Ruijie Reyee Series Access Point

Implementation Cookbook

Document Version: V1.3
Date: 2024-02-04

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

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

Warning

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

Note

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

Instruction

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

Specification

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

3. Instruction

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

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

Contents

Preface I

1 Product Introduction 1

1.1 Product List 1

1.2 LED Indicator 4

1.2.1 Reyee Indoor AP 4

1.2.2 Reyee Wall AP 8

1.2.3 Reyee Outdoor AP 10

1.3 Button 14

2 Getting Started 15

2.1 Network Planning 15

2.2 Installation 16

2.2.1 Safety Suggestions 16

2.2.2 Installation Site Requirement 17

2.2.3 Installing the AP 19

2.3 Quick Provisioning 20

2.3.1 Quick Provisioning Through Ruijie Cloud App 20

2.3.2 Quick Provisioning Through Reyee Eweb 33

3 Device Management 37

3.1 Login 37

3.1.1 Case Demonstration 37

3.2 Setting the Login Password 38

3.3 Performing Upgrade and Checking the System Version 39

3.3.1 Online Upgrade 39

3.3.2 Local Upgrade 40

3.4 Configuring Backup and Import 41

3.5 Restoring Factory Settings 41

4 Configuration 43

4.1 Wireless Configuration 43

4.1.1 Wireless Basic Configuration 43

4.1.2 Guest Wi-Fi Configuration 45

4.1.3 Multiple SSID Configuration 47

4.1.4 Healthy Mode 48

4.1.5 Wireless Client List 49

4.1.6 Radio Frequency Configuration 50

4.1.7 Wireless Blocklist/Allowlist Configuration 54

4.1.8 AP Group Configuration 57

4.2 Basic Configuration 59

4.2.1 WAN Port Configuration 59

4.2.2 LAN Port Configuration 61

4.3 Wireless Authentication 65

4.3.1 Overview 65

4.3.2 Configuring One-click Login on Ruijie Cloud 66

4.3.3 Configuring Voucher Authentication on Ruijie Cloud 70

4.3.4 Configuring Account Authentication on Ruijie Cloud 78

4.3.5 Configuring SMS Authentication on Ruijie Cloud 86

4.3.6 Configuring an Authentication-Free User List on Eweb Management System 92

4.3.7 Displaying Authenticated Users on Eweb Management System 95

4.3.8 Displaying Authenticated Users on Ruijie Cloud 96

4.4 Configuring 802.1X Authentication 96

4.4.1 Overview 96

4.4.2 Configuring 802.1X Authentication 97

4.4.3 Viewing Wireless User List 101

4.4.4 Viewing Wired User List 102

4.5 Advanced Configuration 102

4.5.1 ARP List 102

4.5.2 Local DNS 103

4.5.3 PoE Configuration 104

4.5.4 Port Flow Control Configuration 105

4.6 Operation and Maintenance 105

4.6.1 Network Check 105

4.6.2 Alarms 106

4.6.3 Network Tools 107

4.6.4 Fault Collection 109

4.6.5 System 109

4.7 Configuring SNMP 115

4.7.1 Overview 115

4.7.2 Global Configuration 115

4.7.3 View/Group/Community/User Access Control 117

4.7.4 SNMP Service Typical Configuration Examples 126

4.7.5 Configuring Trap Service 131

4.7.6 Trap Service Typical Configuration Examples 136

5 Advanced Solution Guide 140

5.1 Reyee Flow Control Solution 140

5.1.1 Application Scenario 140

5.1.2 Configuration Case 140

5.2 Reyee Cloud Authentication Solution 147

5.2.1 Working Principle 147

5.2.2 Application Scenario 147

5.2.3 Configuration Case 147

5.3 Reyee Guest Wi-Fi Solution 155

5.3.1 Working Principle 155

5.3.2 Application Scenario 156

5.3.3 Configuration Case 156

5.4 Reyee SON 169

5.4.1 Working Mechanism of Reyee SON 169

5.4.2 Reyee SON Configuration 172

5.4.3 SON Troubleshooting 174

5.5 Reyee Economic Hotel Network Solution 174

5.5.1 Application Scenario 174

5.5.2 Configuration Case 175

6 Reyee FAQ 185

6.1 Reyee Password FAQ (Collection) 185

6.2 Reyee Guest WiFi FAQ (Collection) 185

6.3 Reyee Wireless Configuration FAQ (Collection) 185

6.4 Reyee Self-Organizing Network (SON) FAQ (Collection) 185

6.5 Reyee series Devices Parameters Tables 185

6.6 Reyee Parameter Consultation FAQ (Collection) 185

7 Appendix: Monitoring 186

7.1 Memory Usage 186

7.2 Device Status 186

7.3 AP Working Mode 186

7.4 Checking the SON Status 188

7.5 Online Clients 189

7.6 Device Information 189

7.7 Wireless Information 189

7.8 Ethernet Status 190

1 Product Introduction

Reyee cloud-managed access points (APs) have high performance for indoor, outdoor, and wall scenarios. In conformance with 802.11ac Wave 2, Reyee cloud-managed series APs support Multi-user Multiple Input, Multiple Output (MU-MIMO) dual-stream technology.

Reyee APs are easy to install and maintain with the industrial design.

Good Performance Based on Dual-band Wi-Fi

The AP supports 2.4GHz and 5GHz dual-band communication, providing the rate of 400 Mbit/s at 2.4 GHz, 867 Mbit/s at 5 GHz, and up to 1267 Mbit/s per AP. It can provide 5 GHz frequency band with less interference, wider channel, and faster speed for terminals, allowing users to enjoy excellent wireless experience.

Seamless Layer 3 Roaming

The AP supports Layer 3 roaming on a complex Layer 3 network. When users move across Layer 3 networks, seamless roaming can be achieved without service interruption.

SON Support

Self-Organizing Networking (SON) eliminates product limitations and realizes auto-discovery, auto-networking, and auto-configuration between routers, switches, and wireless APs without the need for controllers or Internet access. The mobile app allows you to quickly complete device deployment and configuration, remote management, operation and maintenance (O&M) of the entire network, which greatly reduces the investment of device, labor, and time cost during wireless network construction.

1.1 Product List

Model	Recommended Coverage	Recommended Number of Clients	WLAN ID	SON Number	Spatial Streams
RG-RAP1200(F)	20 meters	40 = 8 (2.4 GHz) + 32 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP1200(P)	20 meters	80 = 16 (2.4 GHz) + 64 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2200(F)	30 meters	48 = 16 (2.4 GHz) + 32 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO

Model	Recommended Coverage	Recommended Number of Clients	WLAN ID	SON Number	Spatial Streams
RG-RAP2200(E)	30 meters	80 = 16 (2.4 GHz) + 64 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2260(G)	30 meters	100 = 16 (2.4 GHz) + 84 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2260(E)	30 meters	120 = 16 (2.4 GHz) + 104 (5 GHz)	8	300	2.4 GHz 4x4 MIMO 5 GHz 4x4 MIMO
RG-EAP602	2.4 GHz 40 meters 5 GHz 150 meters	96 = 32 (2.4 GHz) + 64 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP6260(G)	2.4 GHz 50 meters 5 GHz 150 meters	100 = 16 (2.4 GHz) + 84 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5G GHz 2x2 MIMO
RG-RAP6262(G)	2.4 GHz 50 meters 5 GHz 150 meters	100 = 16 (2.4 GHz) + 84 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP6202(G)	2.4 GHz 50 meters 5 GHz 150 meters	96 = 32 (2.4 GHz) + 64 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2260	2.4 GHz 40 meters 5 GHz	110 = 16 (2.4 GHz) + 94 (5 GHz)	8	300	2.4 GHz 2x2MIMO 5 GHz 2x2MIMO

Model	Recommended Coverage	Recommended Number of Clients	WLAN ID	SON Number	Spatial Streams
	70 meters				
RG-RAP6262	2.4 GHz 50 meters 5 GHz 150 meters	80 = 16 (2.4 GHz) + 64 (5 GHz)	8	300	2.4 GHz 2x2MIMO 5 GHz 2x2MIMO
RG-RAP2260(H)	2.4 GHz 40 meters 5 GHz 70 meters	130 = 16 (2.4 GHz) + 114 (5 GHz)	8	300	2.4 GHz 4x4 MIMO 5 GHz 4x4 MIMO
RG-RAP6260(H)	2.4 GHz 50 meters 5 GHz 150 meters	120 = 16 (2.4 GHz) + 104 (5 GHz)	8	300	2.4 GHz 4x4 MIMO 5 GHz 4x4 MIMO
RG-RAP6260(H)-D	2.4 GHz 100 meters 5 GHz 300 meters	130 = 16 (2.4 GHz) + 114(5 GHz)	8	300	2.4 GHz 4 x 4 MIMO 5 GHz: 4 x 4 MIMO
RG-RAP1260	2.4 GHz 30 meters 5 GHz 30 meters	110 = 16 (2.4 GHz) + 94(5 GHz)	8	300	2.4 GHz 2 x 2 MIMO 5 GHz 2 x 2 MIMO
RG-RAP1261	2.4 GHz 30 meters 5 GHz 30 meters	110 = 16 (2.4 GHz) + 94(5 GHz)	8	300	2.4 GHz 2 x 2 MU-MIMO 5 GHz 2 x 2 MU-MIMO
RG-RAP2266	2.4 GHz 40 meters	110 = 16 (2.4 GHz) + 94(5	8	300	2.4 GHz 2 x 2 MIMO

Model	Recommended Coverage	Recommended Number of Clients	WLAN ID	SON Number	Spatial Streams
	5 GHz 70 meters	GHz)			5 GHz 3 x 3 MIMO
RG-RAP73HD	2.4 GHz 40 meters 5 GHz 70 meters 6 GHz 70 meters	250 = 16 (2.4 GHz) + 114(5 GHz) +120(6 GHz)	8	300	2.4 GHz: 4x4 MU-MIMO 5 GHz: 4x4 MU-MIMO 6 GHz: 4x4 MU-MIMO
RG-RAP1201	2.4 GHz 10 meters 5 GHz 15 meters	40 = 8 (2.4 GHz) + 32 (5 GHz)	8	300	2.4 GHz: 2x2 MIMO 5 GHz: 2x2 MIMO
RG-RAP52-OD	2.4 GHz 50 meters 5 GHz 150 meters	96 = 32 (2.4 GHz) + 64 (5 GHz)	8	300	2.4 GHz: 2x2 MIMO 5 GHz: 2x2 MIMO

Note

The above coverage data is based on ideal conditions with straight distance and no obstacles. The real coverage distance is subject to the real environment.

1.2 LED Indicator

1.2.1 Reyee Indoor AP

Reyee indoor APs include RG-RAP2200(E), RG-RAP2200(F), RG-RAP2260(E), RG-RAP2260(G), RG-RAP2260, RG-RAP2260(H), RG-RAP2266 and RG-RAP73HD.

RG-RAP2200(E)/RG-RAP2200(F)/RG-RAP2260(E)/RG-RAP2260(G)

LED Indicator	State	Frequency	Meaning
LED indicator	Off	N/A	The AP is not receiving power.
	Blinking	0.5 Hz	The AP is functioning properly but an alarm is generated.
	Fast blinking	10 Hz	Possible cases: ● Restoring factory settings ● Upgrading the firmware ● Restoring the image file ● Initializing the device
	Solid green	N/A	The AP is functioning properly with no alarms.

RG-RAP2260

LED Indicator	Status	Description
LED Indicator	Solid blue	The AP is functioning properly with no alarms.
	Off	The AP is not receiving power.
	Fast flashing	The AP is starting up.
	Slow flashing (at 0.5 Hz)	The network is unreachable.
	Flashing twice in succession	Possible cases: ● The AP is restoring the factory settings. ● The AP is upgrading the software. **Caution** Do not power off the device in this case.
	One long flash followed by three short flashes.	Other faults occur.

RG-RAP2260(H)

LED Indicator	Status	Description
LED Indicator	Off	The AP is not receiving power.
	Slow Blinking	The AP is functioning properly but an alarm is generated.
	Fast blinking	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. ● Handling alarms automatically. ● Starting up the access point.
	Solid blue	The AP is functioning properly with no alarms.

RG-RAP2266

LED Indicator	Status	Description
LED Indicator	Solid blue	The access point is operating normally with no alarms.
	Off	The access point is not receiving power.
	Fast flashing	The access point is starting up.
	Slow flashing (at 0.5 Hz)	The network is unreachable.
	Flashing twice in succession	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. **Caution** Do not power off the access point in this case.
	One long flash followed by three short flashes.	A fault occurs.

RG-RAP73HD

LED Indicator	Status	Description
LED Indicator	Solid Blue	The AP is operating normally with no alarms.
	Off	The AP is not powered on.
	Fast Flashing	The AP is starting up.
	Slow Flashing (at 0.5 Hz)	The network is unconnected.
	Flashing Twice in Succession	Possible cases: ● The AP is restoring factory settings. ● The AP is recovering automatically by upgrading the firmware. Note: Do not power off the AP in this case.
	One Long Flash Followed by Three Short Flashes	Other fault occurs.

1.2.2 Reyee Wall AP

Reyee wall APs include RG-RAP1200(F), RG-RAP1200(P), RG-RAP1260, RG-RAP1201 and RG-RAP1261.

RG-RAP1200(F)/ RG-RAP1200(P)

LED Indicator	State	Frequency	Meaning
LED indicator	Off	N/A	The AP is powered off.
	Slow blinking	0.5 Hz	The AP is functioning properly but an alarm is generated.

LED Indicator	State	Frequency	Meaning
	Fast blinking	10 Hz	Possible cases: ● Restoring factory settings ● Upgrading the firmware ● Self-repairing ● Initializing the AP ● The PoE OUT port is overloaded.
	Solid green	NA	The AP is functioning properly with no alarms.

RG-RAP1260

LED Indicator	Status	Description
LED Indicator	Off	The access point is not receiving power.
	Slow Blinking (at 0.5 Hz)	The access point is operating normally but there is an alarm generated.
	Fast Blinking (at 2 Hz)	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. ● Handling alarms automatically. ● Starting up the access point.
	Solid White	The access point is operating normally without alarms.

RG-RAP1261

LED Indicator	Status	Description
LED Indicator	Off	The access point is not receiving power.
	Fast flashing (at 8 Hz)	The access point is starting up.
	Solid on	The access point functions properly.

	Slow flashing (at 0.5 Hz)	The network is unreachable.
	Flashing twice in succession	The access point is being upgraded. Do not power off the access point.

RG-RAP1201

LED Indicator	Status	Description
LED	Off	The access point is NOT receiving power.
	Fast blinking (blinks eight times per second)	The access point is starting up.
	Steady white	The access point is functioning properly.
	Slow blinking (blinks twice per second)	The access point is not connected to the Internet.
	Blinks twice consecutively	The access point is upgrading. Do not power it off.

1.2.3 Reyee Outdoor AP

Reyee outdoor APs include RG-EAP602, RG-RAP6260(G), RG-RAP6262(G), RG-RAP6202(G), RG-RAP6262, RG-RAP6260(H), RG-RAP6260(H)-D, and RG-RAP52-OD.

RG-EAP602/RG-RAP6260(G)

LED Indicator	State	Frequency	Meaning
LED indicator	Off	N/A	The AP is not receiving power.
	Slow blinking	0.5 Hz	The AP is normal but is not connected to Ruijie Cloud.
	Fast blinking	10 Hz	Possible cases: ● Restoring factory settings ● Upgrading the firmware Restoring the image file ● Initializing the device

LED Indicator	State	Frequency	Meaning
	Solid Blue	On	The AP is functioning properly with no alarms.

RG-RAP6262(G)/RG-RAP6202(G)

LED Indicator	State	Meaning
Wi-Fi (green)	Blinking	Data is transmitted by Wi-Fi.
	Solid on	Wi-Fi is enabled and no data is transmitted.
	Off	Wi-Fi is disabled.
SYS (blue)	Fast blinking	The AP is being initialized.
	Slow blinking (0.5 Hz)	The Internet is unreachable.
	Blinking twice	● Restore factory settings. ● Upgrade the firmware and restore the image file. **Caution** Do not power off the device in this case.
	A long blink and three short blinks	Other faults occur.
	Solid on	The AP is working properly with no alarm.
	Off	The AP is powered off.
LAN 1 (green)	Blinking	The port is Up and data is transmitted.
	Solid on	The port is Up and no data is transmitted.
	Off	The port is Down.
LAN 2 (green)	Blinking	The port is Up and data is transmitted.
	Solid on	The port is Up and no data is transmitted.
	Off	The port is Down.

RG-RAP6262

LED Indicator	State	Meaning
Wi-Fi LED (Green)	Flashing	Data is transmitted by Wi-Fi.
	Solid on	Wi-Fi is enabled and no data is transmitted.
	Off	Wi-Fi is disabled.
System Status LED (Blue)	Fast flashing	The access point is starting up.
	Slow flashing (at 0.5 Hz)	The network is unreachable.
	Flashing twice in succession	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. ● Handling alarms automatically. Note: Do not power off the access point in this case.
	Solid on	The access point is functioning properly.
	Off	The access point is not receiving power.
LAN Port Status LED (Green)	Flashing	The port has made a successful link and is sending/receiving traffic.
	Solid on	The port has made a successful link and is not sending/receiving traffic.
	Off	No link is detected for the port.
SFP Port Status LED (Green)	Flashing	The port has made a successful link and is sending/receiving traffic.
	Solid on	The port has made a successful link and is not sending/receiving traffic.
	Off	No link is detected for the port.

RG-RAP6260(H)/RG-RAP6260(H)-D

LED Indicator	State	Meaning
LED Indicator	Off	The access point is not receiving power.
	Slow Blinking	The access point is operating normally but there is an alarm generated.
	Fast Blinking	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. ● Handling alarms automatically. ● Starting up the access point.
	Solid Blue	The access point is operating normally with no alarms.

RG-RAP52-OD

LED Indicator	Status	Description
LED Indicator	Solid blue	The device is operating normally.
	Off	The device is NOT receiving power.
	Fast blinking	The device is starting up.
	Slow blinking (at a two-second interval)	The device is not connected to the Internet.
	Blinking twice	● The device is resetting. ● The device is upgrading. ● The device is recovering. ⚠ **Caution** Do not power off the device when the LED is in this state.

1.3 Button

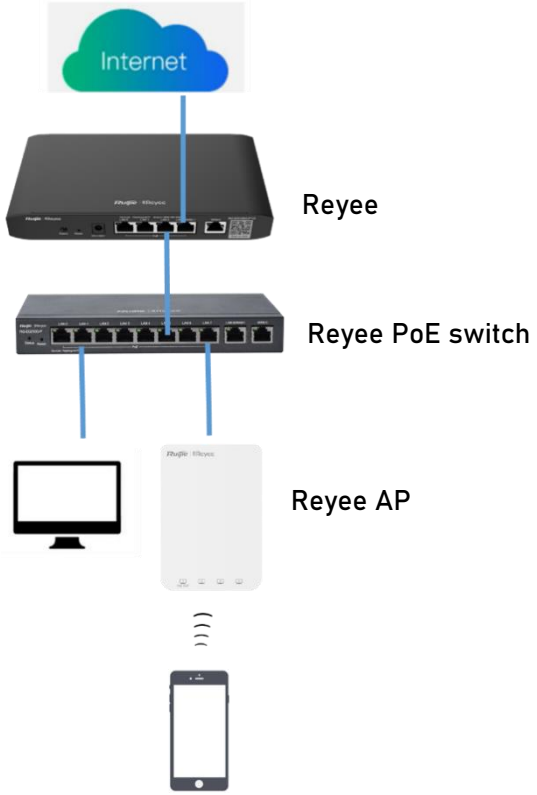
Model	Button		Meaning
All AP	Reset	Pressing this button for less than 2 seconds	Restart the AP.
		Pressing this button for more than 5 seconds	Restore factory defaults.

2 Getting Started

2.1 Network Planning

The DHCP server has two address pools on the egress gateway:

- 192.168.110.0/24 in VLAN 1 for devices on this network
- 192.168.10.0/24 in VLAN 10 for clients on this network



The following ports are used for Ruijie Cloud management. To connect devices on Ruijie Cloud, ensure that these ports are available and data streams are permitted on the network.

Cloud	Domain name	DST.TCP	DST.UDP
Cloud-as	devicereg.ruijienetworks.com	80,443	
	ryrc.ruijienetworks.com	80,443	
	stunrc.ruijienetworks.com		3478,3479
	stunsvr-as.ruijienetworks.com		3478,3479
	cwmpsvr-as.ruijienetworks.com	80,443	
	34.87.93.12	80,443	
	firmware.ruijienetworks.com	80,443	
	cloudweb.ruijienetworks.com	80,443	
	fastonline.ruijienetworks.com	80,443	
	cloudapi.ruijienetworks.com	80,443	
	cdn.ruijienetworks.com	80,443	
	iotrc.ruijienetworks.com		7683
	iotsvr-as.ruijienetworks.com		5683
	iotlog-as.ruijienetworks.com		6683
	iotdl-as.ruijienetworks.com		8683

Cloud	Domain name	DST.TCP	DST.UDP
Cloud-eu	devicereg.ruijienetworks.com	80,443	
	ryrc.ruijienetworks.com	80,443	
	stunrc.ruijienetworks.com		3478,3479
	stunsvr-eu.ruijienetworks.com		3478,3479
	cwmpsvr-eu.ruijienetworks.com	80,443	
	cloudlog-eu.ruijienetworks.com	80,443	
	firmware.ruijienetworks.com	80,443	
	cloudweb.ruijienetworks.com	80,443	
	fastonline.ruijienetworks.com	80,443	
	cloudapi.ruijienetworks.com	80,443	
	cdn.ruijienetworks.com	80,443	
	iotrc.ruijienetworks.com		7683
	iotsvr-eu.ruijienetworks.com		5683
	iotlog-eu.ruijienetworks.com		6683
	iotdl-eu.ruijienetworks.com		8683

Cloud	Domain name	DST.TCP	DST.UDP
Cloud-ru	devicereg.ruijienetworks.com	80,443	
	ryrc.ruijienetworks.com	80,443	
	stunrc.ruijienetworks.com		3478,3479
	stunsvr-ru.ruijienetworks.com		3478,3479
	cwmpsvr-ru.ruijienetworks.com	80,443	
	130.193.40.202	80,443	
	firmware.ruijienetworks.com	80,443	
	cloudweb.ruijienetworks.com	80,443	
	fastonline.ruijienetworks.com	80,443	
	cloudapi.ruijienetworks.com	80,443	
	cdn.ruijienetworks.com	80,443	
	iotrc.ruijienetworks.com		7683
	iotsvr-ru.ruijienetworks.com		5683
	iotlog-ru.ruijienetworks.com		6683
	iotdl-ru.ruijienetworks.com		8683

2.2 Installation

2.2.1 Safety Suggestions

To avoid personal injury and equipment damage, read safety suggestions carefully before you install each device. The following safety suggestions do not cover all possible dangers.

1. Installation

- Keep the chassis clean and free from any dust.
- Do not place devices in a walking area.
- Do not wear loose clothes or accessories that may be hooked or caught by devices during installation and maintenance.

2. Movement

- Do not frequently move devices.
- When moving devices, keep the balance and avoid hurting legs and feet or straining the back.
- Before moving devices, turn off all power supplies and dismantle all power modules.

3. Electricity

- Observe local regulations and specifications when performing electric operations. The operators must be qualified.
- Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp or wet ground or floor.
- Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.
- Try to avoid maintaining the switch that is powered on alone.
- Make a careful check before you cut off the power supply.
- Do not place the equipment in a damp location. Do not let any liquid enter the chassis.

4. Static Discharge Damage Prevention

To prevent damage from static electricity, pay attention to the following points:

- Properly ground grounding screws on the back panel of the device; use a three-wire single-phase socket with the protective earth wire (PE) as the AC power socket.
- Prevent indoor dusts.
- Ensure proper humidity conditions.

5. Laser

Some devices support varying models of optical modules that are Class I laser products sold on the market. Improper use of optical modules may cause damage. Therefore, pay attention to the following points when you use them:

- When a fiber transceiver is working, ensure that the port has been connected to an optical fiber or is covered with a dust cap, to keep out dust and avoid burns.
- When the optical module is working, do not pull out the fiber cable or look directly into a transceiver. The transceiver emit laser light that can damage your eyes.

2.2.2 Installation Site Requirement

The installation site must meet the following requirement to ensure normal working and a prolonged durable life of Reyee APs.

1. Ventilation

When installing devices, reserve at least 10 cm distances from both sides and the back plane of the cabinet at ventilation openings to ensure good ventilation. After cables have been connected, bundle or place the cables on the cabling rack to prevent them from blocking the air inlets. It is recommended that the device be cleaned at regular intervals. In particular, avoid dust from blocking the screen mesh on the back of the cabinet.

2. Temperature and Humidity

To ensure normal operation and prolong the service life of the AP, keep proper temperature and humidity in the equipment room.

If the temperature and humidity in the equipment room do not meet the requirements for a long time, the AP may be damaged.

- In an environment with a high humidity, insulating materials may have bad insulation or even leaking electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.
- In an environment with a low humidity, insulating strips may dry and shrink. Static electricity may occur easily and endanger circuits on the device.
- In an environment with a high temperature, the AP is subject to more serious harm. Its performance may degrade drastically and various hardware faults may occur.

3. Cleanness

Dust poses a severe threat to the running of the AP. The indoor dust falling on the AP may be adsorbed by the static electricity, causing bad contact of the metallic joint. Such electrostatic adsorption may occur more easily when the relative humidity is low. This affects the lifecycle of the AP and causes communication faults.

4. Grounding

A good grounding system is the basis for stable and reliable operation of the device, preventing lightning strokes and resisting interference. Carefully check the grounding conditions at the installation site according to the grounding requirements, and perform grounding operations properly as required.

Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, down conductor, and connector to the grounding system, which usually shares the power reference ground and ground cable. The lightning discharge ground is targeted for the facility.

EMC Grounding

The grounding required for EMC design includes the shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The resistance of earth wires should be less than 1 Ω.

5. EMI

Electro-Magnetic Interference (EMI), from either outside or inside the device or application system, affects the system in the conductive ways such as capacitive coupling, inductive coupling, and electromagnetic radiation.

There are two types of electromagnetic interference: radiated interference and conducted interference, depending on the type of the transmission path.

When the energy, often RF energy, from a component arrives at a sensitive component through the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conducted interference results from an electromagnetic wire or signal cable connection between the source and the sensitive component, along which cable the interference conducts from one unit to another. Conducted interference often affects the power supply of the device, but can be controlled by a filter. Radiated interference may affect any signal path in the device and is difficult to shield.

- For the TN AC power supply system, the single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through filtering circuits.
- Do not use the grounding device of the device cannot be used for an electrical device or anti-lightning grounding device. In addition, the grounding device of the device must be deployed far away from the grounding device of the electrical device and anti-lightning grounding device.
- Keep the device away from the high-power radio transmitter, radar transmitting station, and high-frequency large-current device.
- Take measures to shield static electricity.

- Lay interface cables inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device signal interfaces caused by over-voltage or over-current of lightning.

2.2.3 Installing the AP

For how to install the AP, refer to the hardware installation manual of each AP.

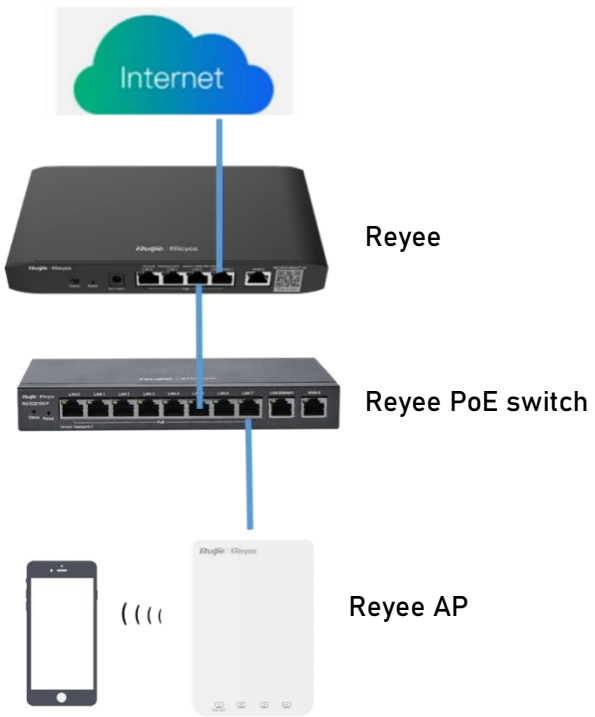
Model	Link of Hardware Installation Manual
RG-RAP1200(F)	https://www.ruijienetworks.com/resources/preview/76609
RG-RAP1200(P)	https://www.ruijienetworks.com/resources/preview/76610
RG-RAP2200(F)	https://www.ruijienetworks.com/resources/preview/76612
RG-RAP2200(E)	https://www.ruijienetworks.com/resources/preview/76611
RG-RAP2260(G)	https://www.ruijienetworks.com/resources/preview/76769
RG-RAP2260(E)	https://www.ruijienetworks.com/resources/preview/76806
RG-EAP602	https://www.ruijienetworks.com/resources/preview/76616
RG-RAP6260(G)	https://www.ruijienetworks.com/resources/preview/76770
RG-RAP6262(G)	https://www.ruijienetworks.com/resources/preview/77058
RG-RAP6202G	https://www.ruijienetworks.com/resources/preview/77243
RG-RAP2260	https://www.ruijienetworks.com/resources/preview/77449
RG-RAP6262	https://www.ruijienetworks.com/resources/preview/77494
RG-RAP2260(H)	https://www.ruijienetworks.com/resources/preview/77409
RG-RAP6260(H)	https://www.ruijienetworks.com/resources/preview/77410
RG-RAP6260(H)-D	Ruijie Reyee RG-RAP6260(H)-D Access Point Hardware Installation and Reference Guide (V1.0) - Ruijie Networks
RG-RAP1260	Ruijie Reyee RG-RAP1260 Access Point Hardware Installation and Reference Guide (V1.0) - Ruijie Networks
RG-RAP1261	Ruijie Reyee RG-RAP1261 Access Point Hardware Installation and Reference Guide (V1.0) - Ruijie Networks
RG-RAP2266	Ruijie Reyee RG-RAP2266 Access Point Hardware Installation and Reference Guide (V1.0) - Ruijie Networks

Model	Link of Hardware Installation Manual
RG-RAP73HD	Ruijie Reyee RG-RAP73HD Access Point Hardware Installation and Reference Guide (V1.0) - Ruijie Networks
RG-RAP1201	Ruijie Reyee RG-RAP1201 Access Point Hardware Installation and Reference Guide(V1.0) - Ruijie Networks
RG-RAP52-OD	https://www.ruijienetworks.com/resources/preview/rg-rap52-od-hardware-installation-and-reference-guide

2.3 Quick Provisioning

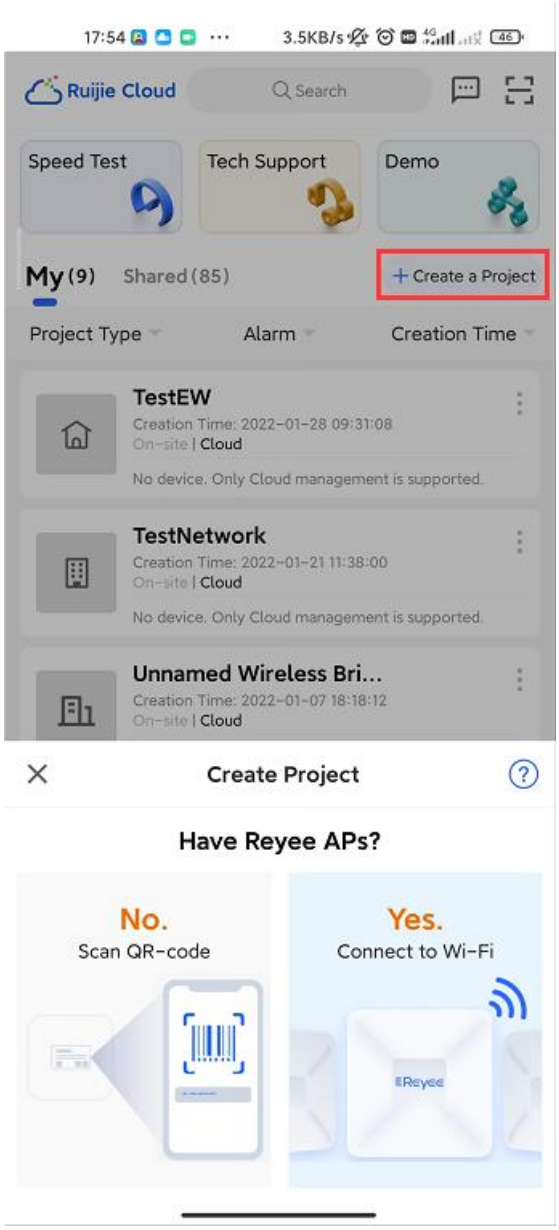
2.3.1 Quick Provisioning Through Ruijie Cloud App

The network topology shown below includes the Reyee gateway, Reyee PoE switch, and Reyee AP.



1. Creating a Project

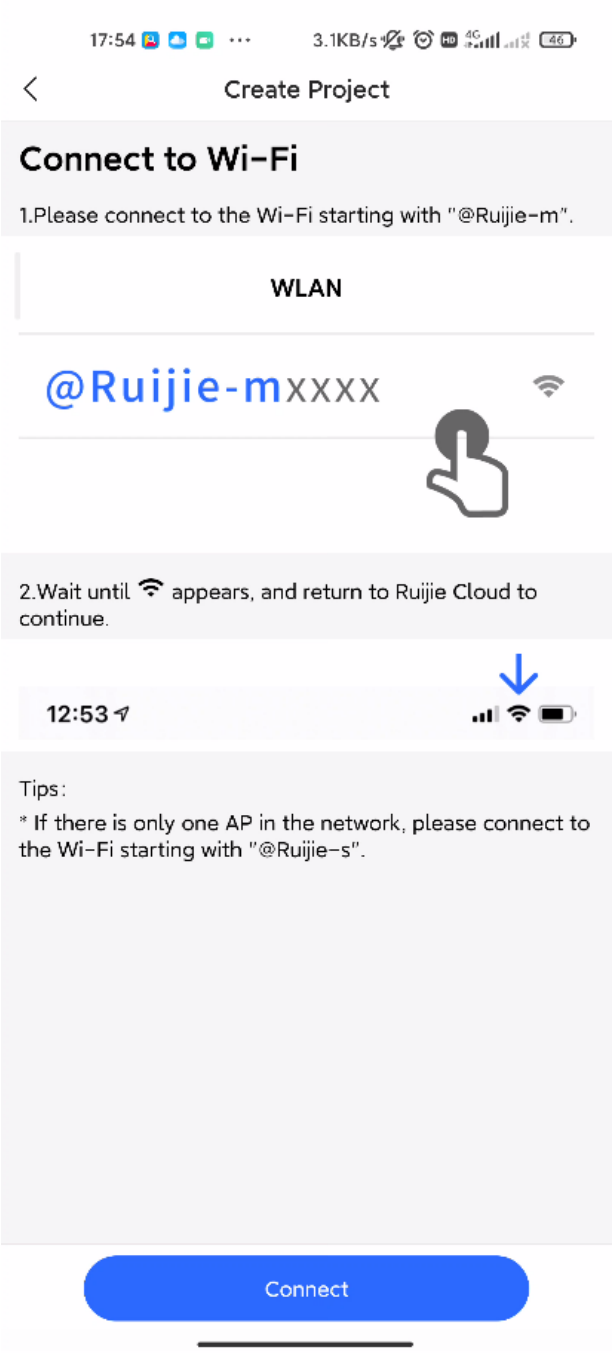
(1) Open Ruijie Cloud App, tap **Create a Project**, and select **Connect to Wi-Fi**.



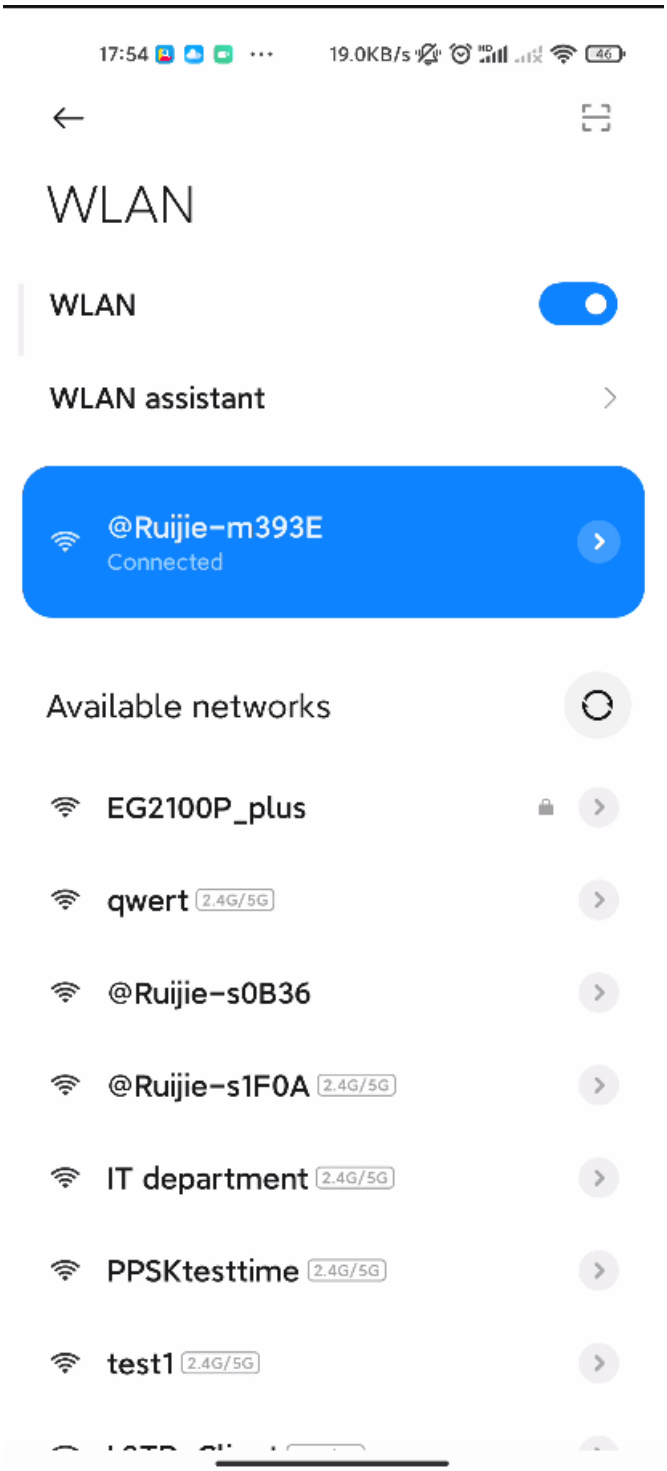
Tap **Yes**. Ruijie Cloud App asks you to connect **@Ruijie-m***xxxx* SSID.

Instruction

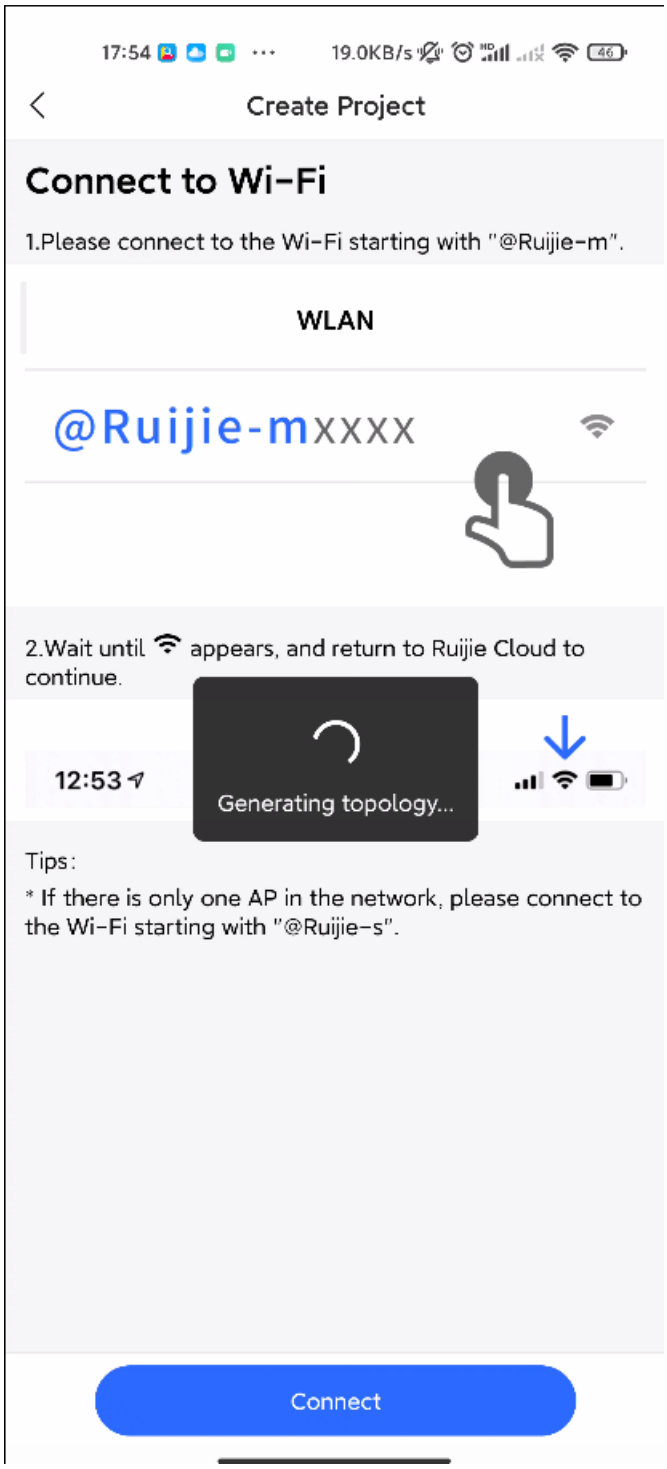
@Ruijie-m*xxxx* is generated after the SON is established successfully. **@Ruijie-s***xxxx* is generated on a standalone device, where *xxxx* is the last four digits of MAC address of the AP.

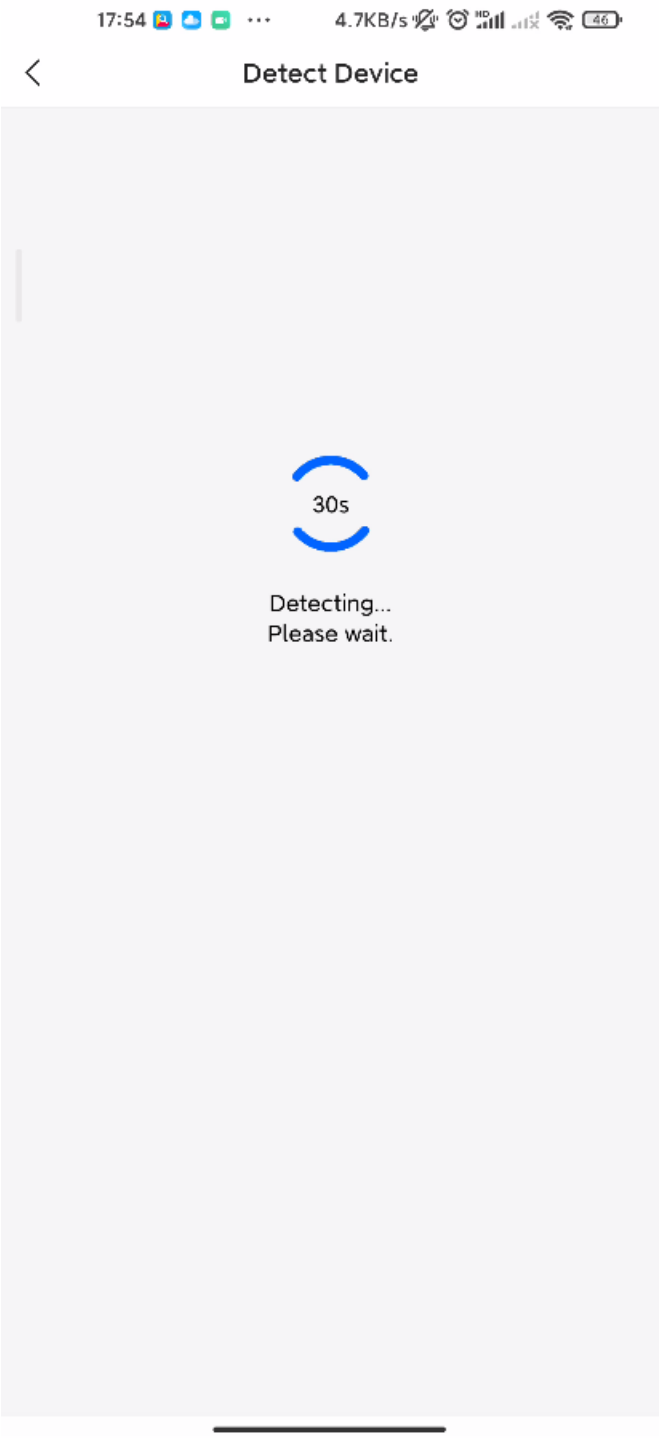


(2) Connect the SSID **@Ruijie-m***xxxx* on your phone.

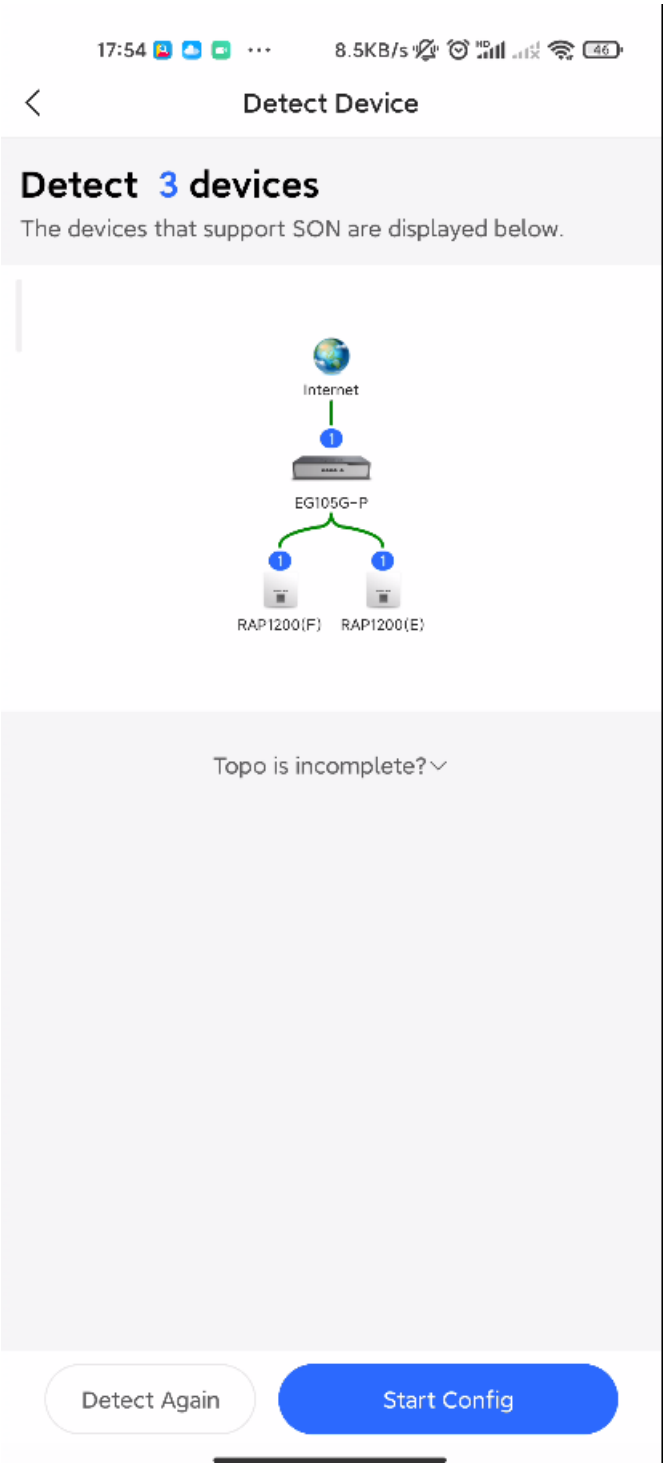


After the phone is connected to the SSID **@Ruijie-m***xxxx*, return to Ruijie Cloud App. The Cloud App will generate the topology and detect all devices on this SON.


17:54
19.0KB/s
Create Project
Connect to Wi-Fi
1.Please connect to the Wi-Fi starting with "@Ruijie-m".
WLAN
@Ruijie-mxxxx
2.Wait until appears, and return to Ruijie Cloud to continue.
12:53
Generating topology...
Tips:
* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".
Connect



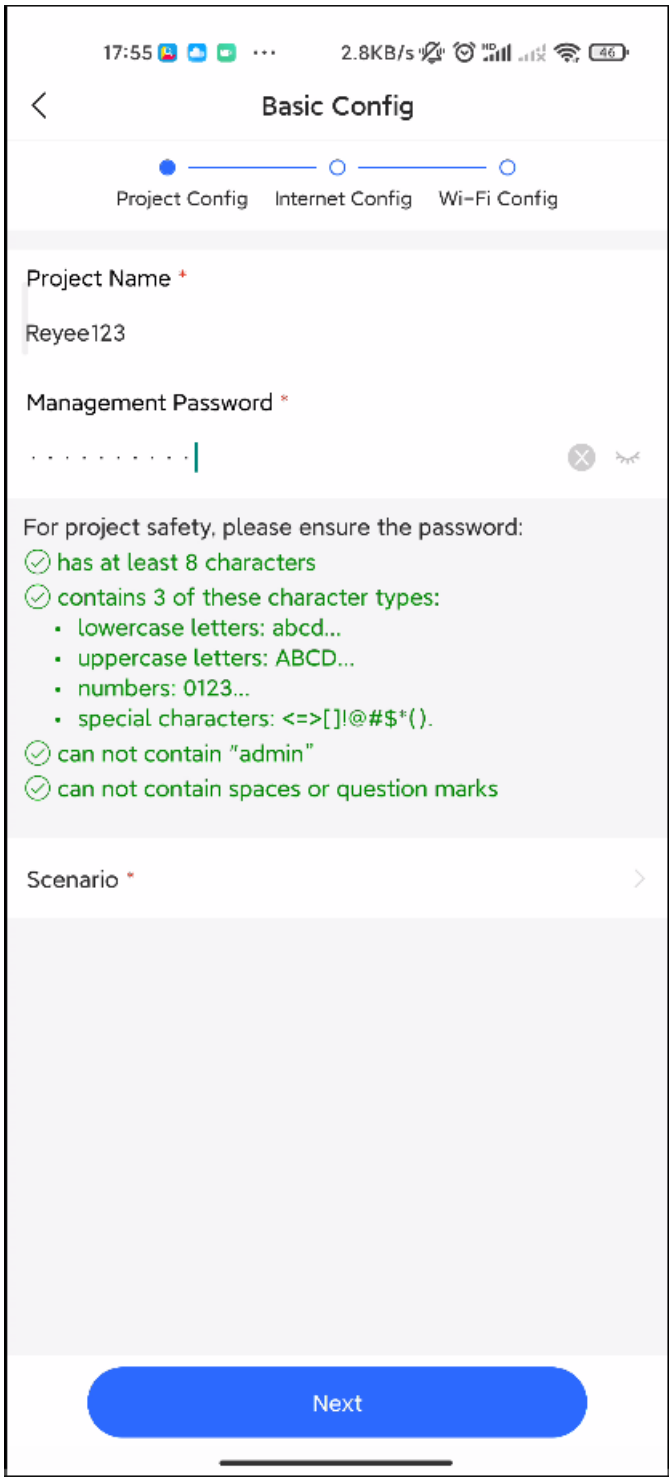
After all devices are detected, Ruijie Cloud App will display them and show the topology.



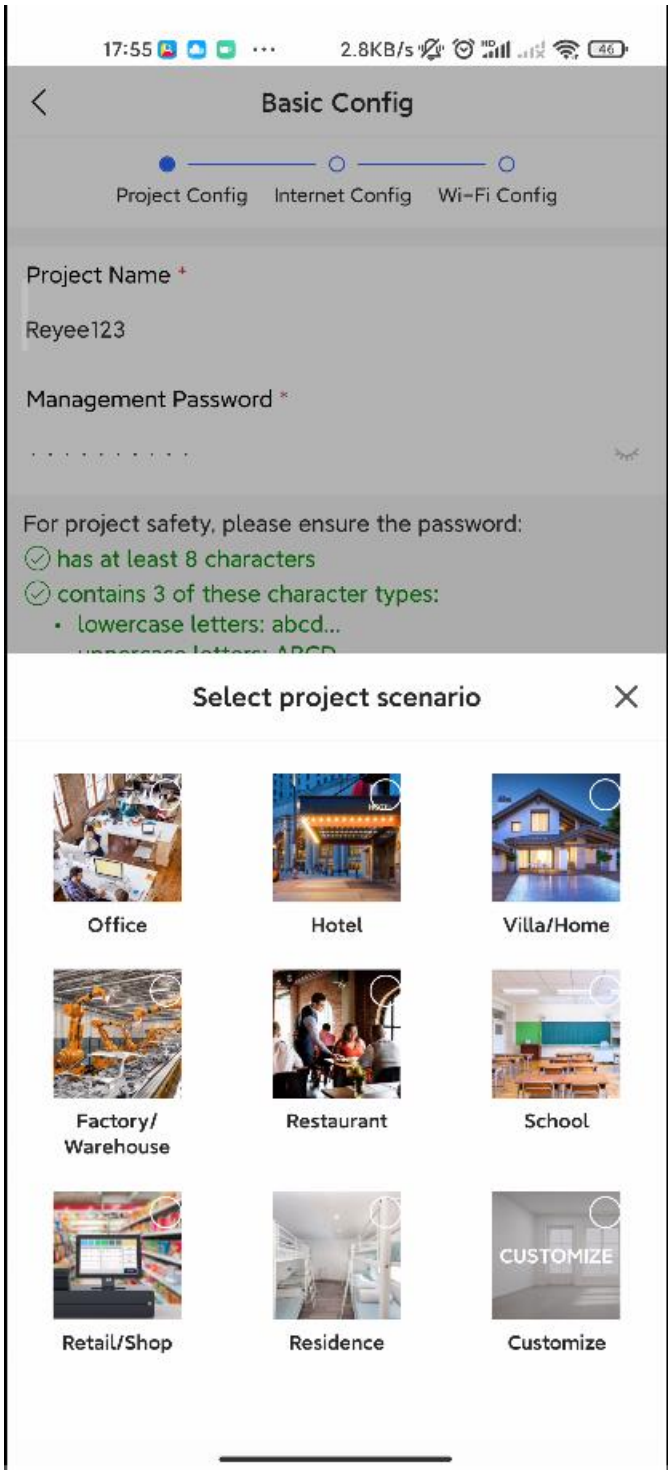
(3) Click **Start Config** to perform basic configuration of this project.

2. Configuring the Project

(1) Enter **Project Name** and **Management Password**.

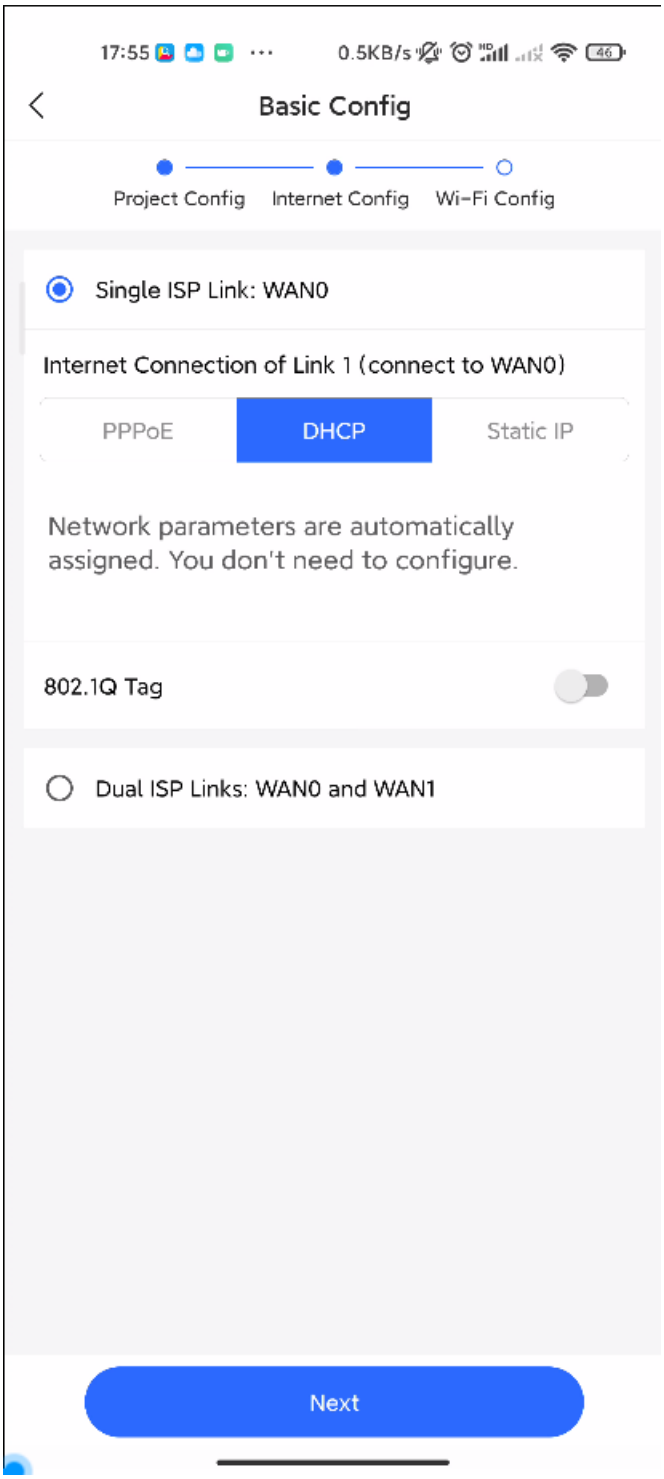


(2) Select the scenario of this project based on your requirement.



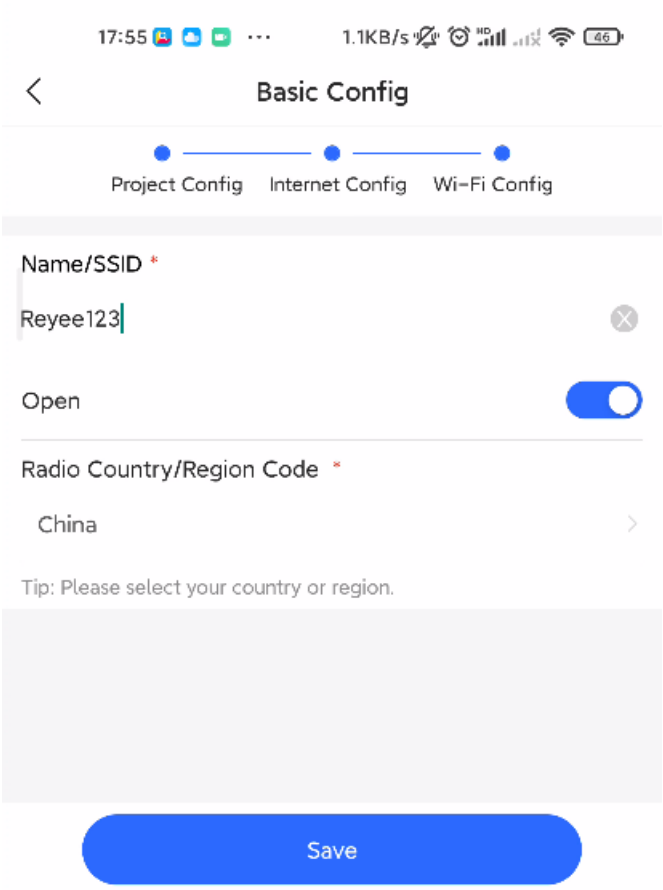
3. Configuring the Internet

For WAN configuration, you can select **PPPoE**, **DHCP**, or **Static IP**.

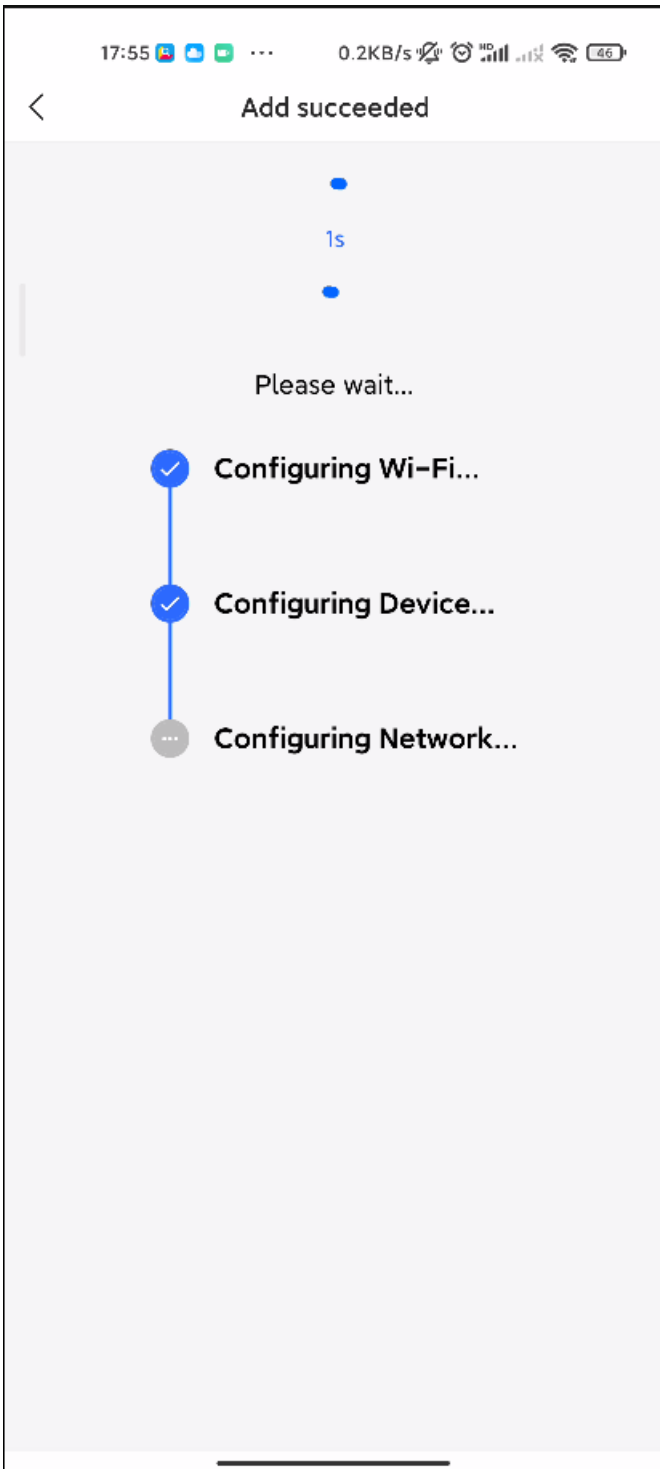


4. Configuring the SSID

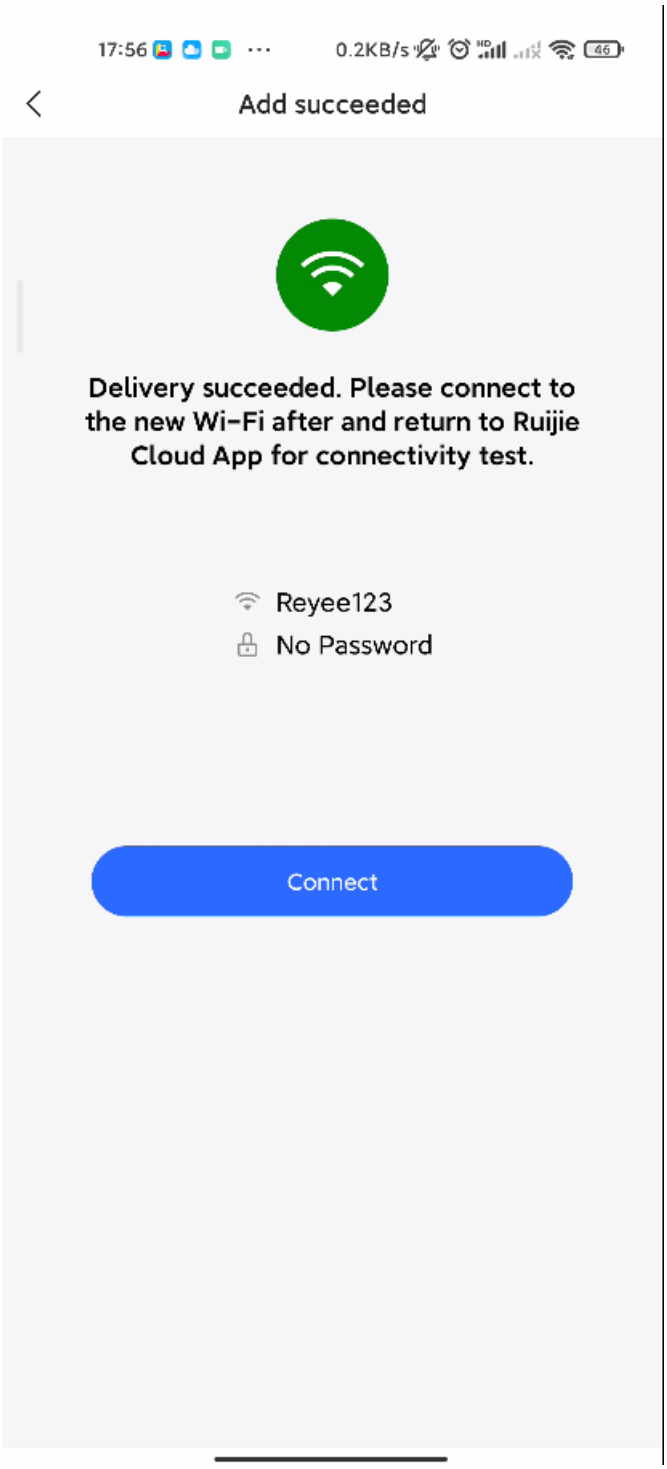
For SSID settings, enter the name of the SSID and enable **Open** or configure the password for this SSID. Then select the region code and click **Save**.



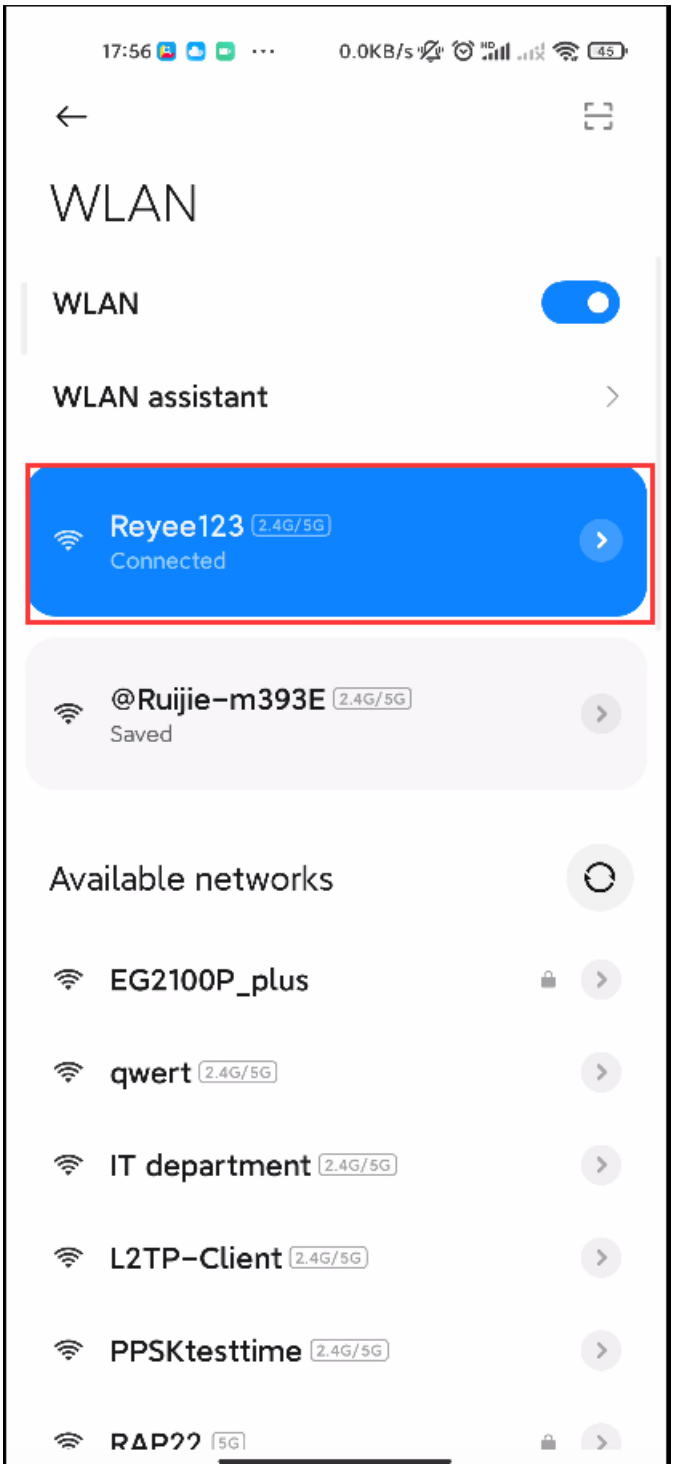
The configuration will be synchronized to the network.



Ruijie Cloud App displays that the configuration is delivered successfully about 3s later.

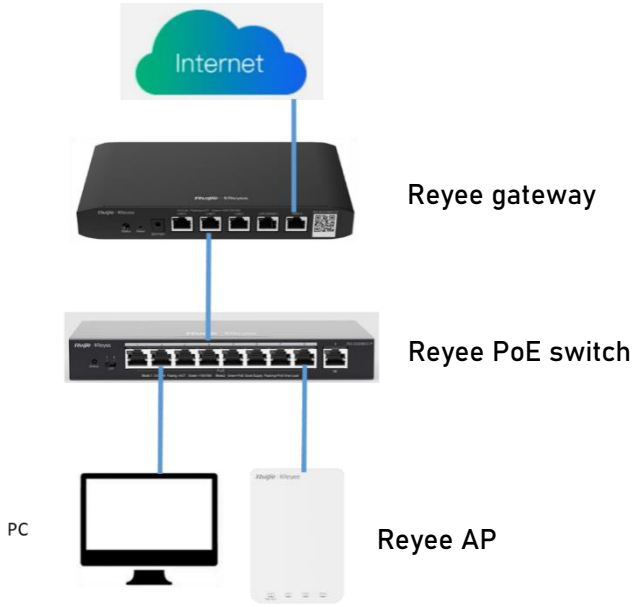


Connect to the SSID created to manage the entire network on Cloud App.



2.3.2 Quick Provisioning Through Reyee Eweb

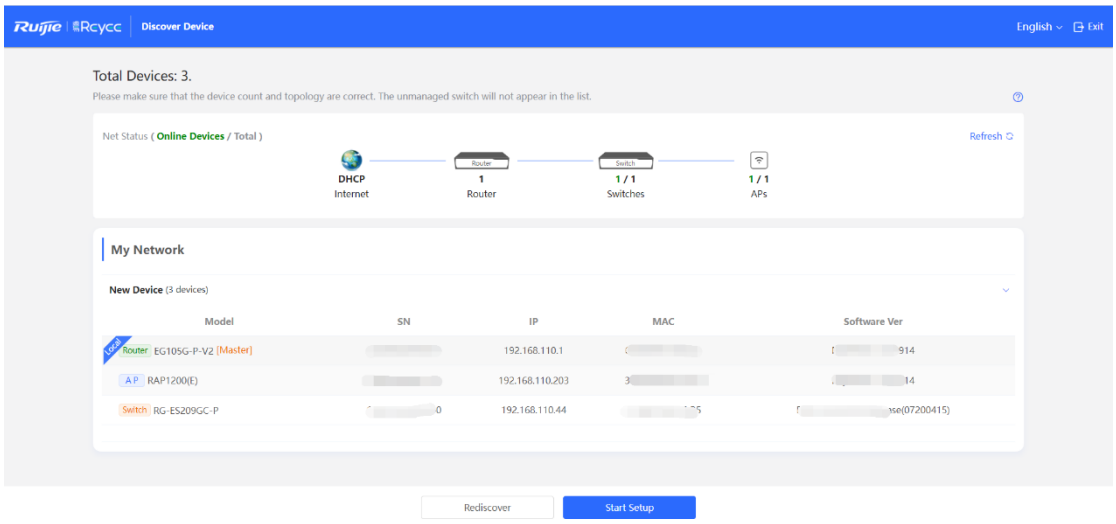
The network topology shown below includes the Reyee gateway, Reyee POE switch, and Reyee RAP.



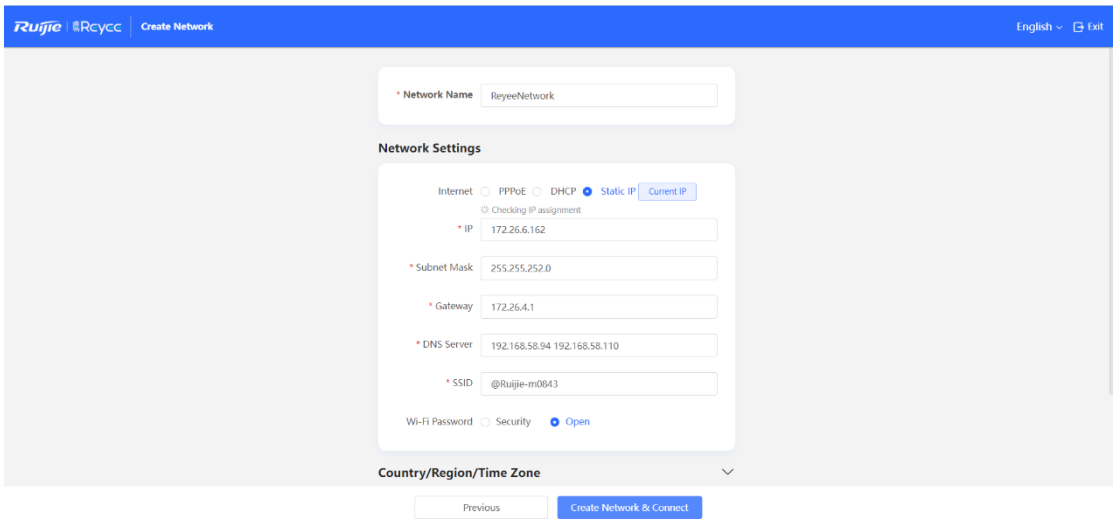
(1) Connect a PC to the POE switch, set the IP address of the PC to the static IP address 192.168.110.*x* (*x* is an integer between 2 and 254) and the subnet mask to 255.255.255.0, and enter 192.168.110.1 in the browser address bar to log in to the Eweb of the EG.

All devices on this network will be displayed in the Eweb.

(2) Click **Start Setup** to perform quick start of the network.

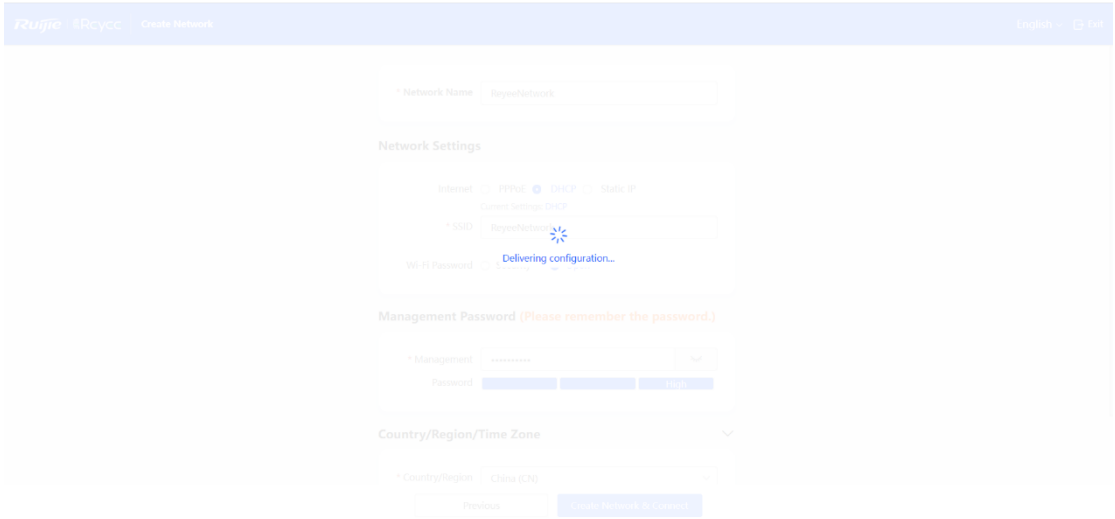


(3) To finish quick start of the network, enter the network name, configure the Internet access mode of the network and enter the password of the SSID or enable **Open**. Then select **Country/Region/Time Zone**.

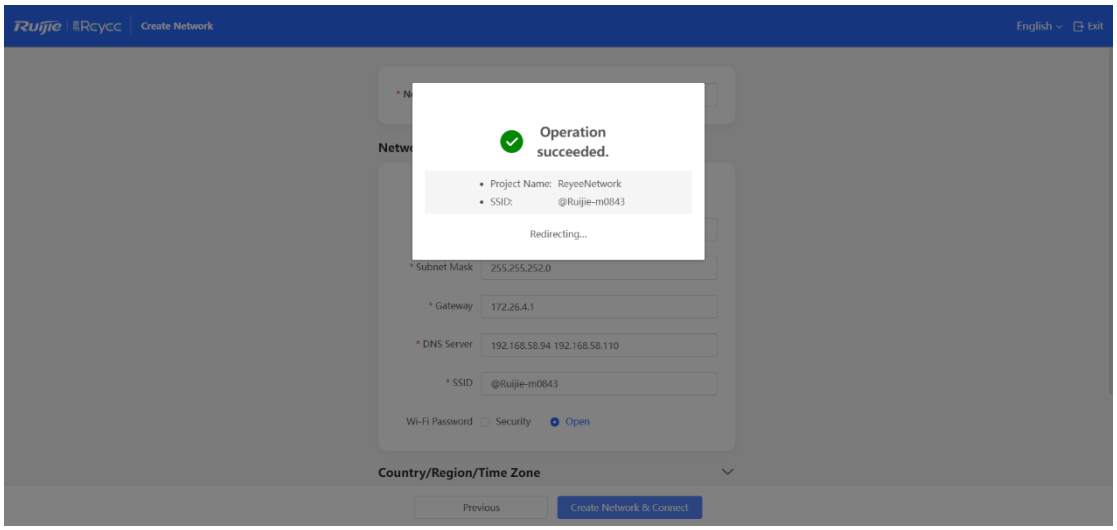


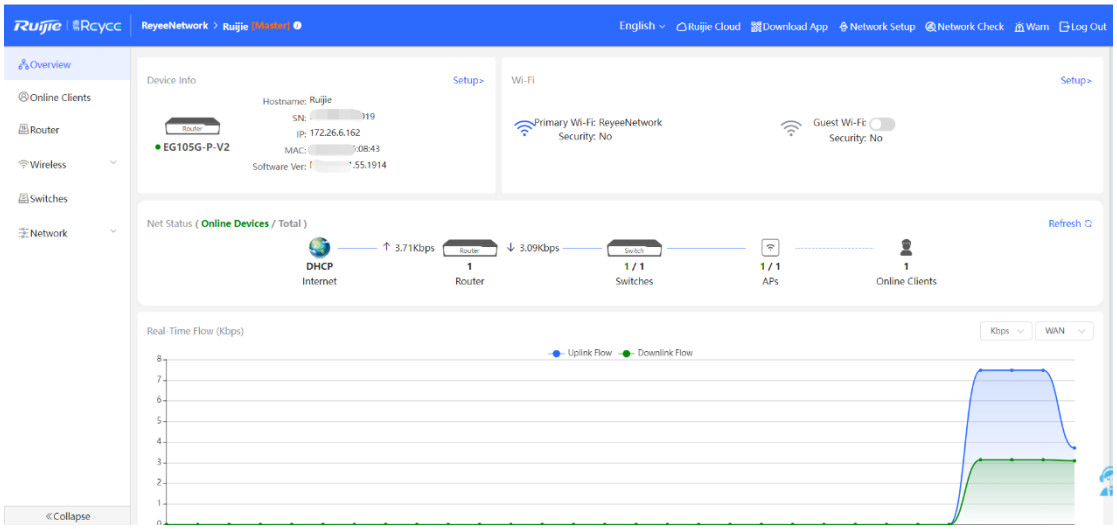
(4) Click **Create Network & Connect**.

The configuration will be delivered and activated.



After the configuration has been delivered and activated, you can access the overview interface to manage the SON of Reyee devices.


Create Network
English
Exit
Operation succeeded.
Project Name: ReyeeNetwork
SSID: @Ruijie-m0843
Redirecting...
Subnet Mask 255.255.252.0
Gateway 172.26.4.1
DNS Server 192.168.58.94 192.168.58.110
SSID @Ruijie-m0843
Wi-Fi Password Security Open
Country/Region/Time Zone
Previous
Create Network & Connect


ReyeeNetwork > Ruijie (Master)
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Device Info
Setup>
Hostname: Ruijie
IP: 172.26.6.162
EG105G-P-V2
Wi-Fi
Setup>
Primary Wi-Fi: ReyeeNetwork
Security: No
Guest Wi-Fi:
Security: No
Net Status (Online Devices / Total)
Refresh
3.71Kbps
3.09Kbps
DHCP
Internet
1
Router
1 / 1
Switches
1 / 1
APs
1
Online Clients
Real-Time Flow (Kbps)
Kbps
WAN
Uplink Flow
Downlink Flow

3 Device Management

3.1 Login

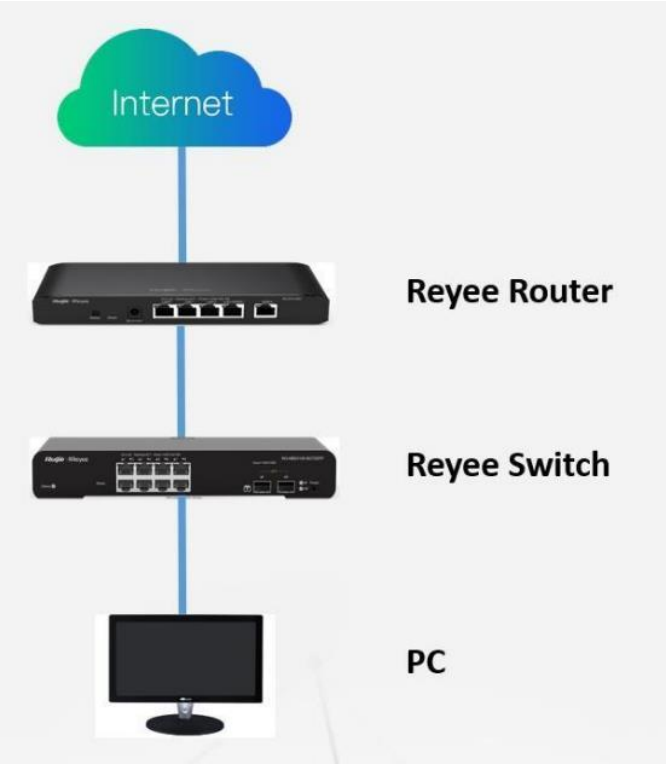
Eweb is a web-based network management system used to manage or configure devices. You can access Eweb through a browser such as Google Chrome. Web-based management involves a web server and a web client. The web server, which is integrated in a device, is used to receive and process requests from the client, and to return processing results to the web client. The web client usually refers to a browser, such as Google Chrome, IE, or Firefox.

The Reyee managed switches support both web interface management and remote management through life-time-free Ruijie Cloud App and Ruijie Cloud platform. You can view the network status, modify the configuration, and troubleshoot faults easily.

3.1.1 Case Demonstration

Network Topology

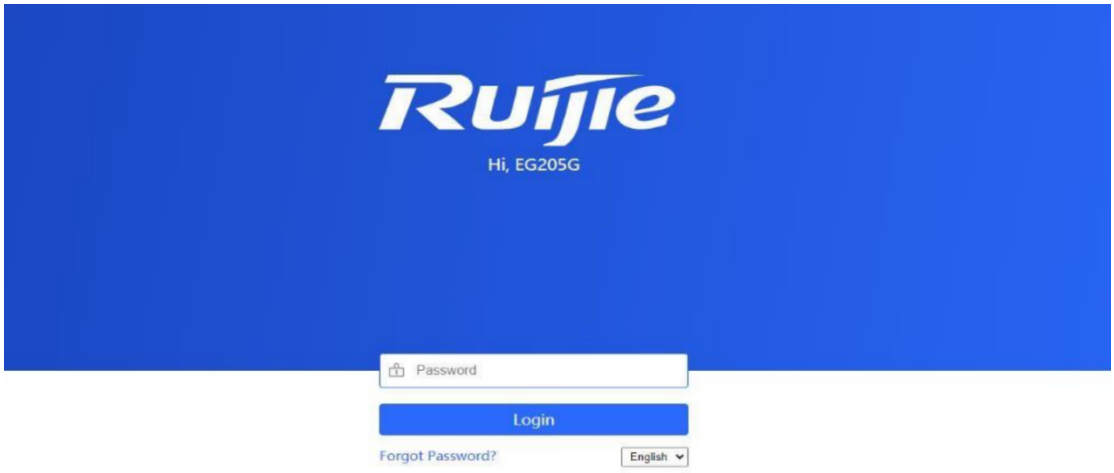
In the following figure, you can access the Eweb management system of an access or aggregation switch through a PC browser to manage and configure the device.



(1) Set PC's IP assignment mode to obtain the IP address automatically.

(2) Visit http://192.168.110.1 by Chrome browser.

(3) Enter the password on the login page and click **Login**.



For the Reyee EG, you may use either 192.168.110.1 or 10.44.77.254 to access it.

For the Reyee switch, you may use 10.44.77.200 to access it.

For the Reyee AP, you may use either 192.168.120.1 or 10.44.77.254 to access it.

For the EST, you may use 10.44.77.254 to access it.

The default login password for all Reyee devices is **admin**.

You may visit https://10.44.77.253 to log in to the master device of the Reyee network.

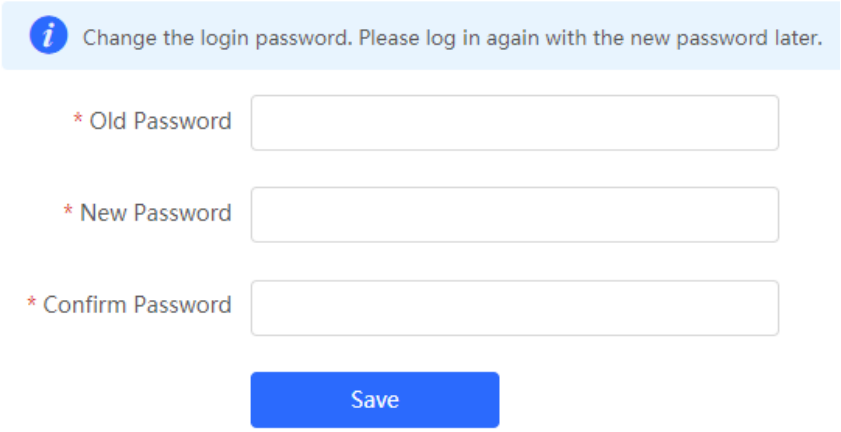
3.2 Setting the Login Password

Choose **System** > **Login** > **Login Password**.

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

Note

In SON mode, the login password of all devices on the network will be changed synchronously.



3.3 Performing Upgrade and Checking the System Version

Note

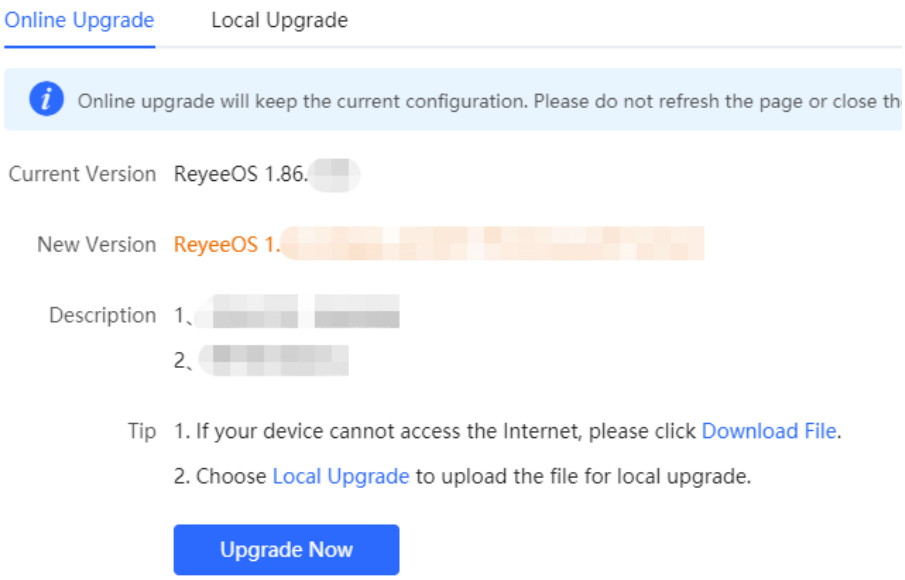
- You are advised to back up the configuration before upgrading the AP.
- After being upgraded, the AP will restart. Therefore, exercise caution when performing this operation.

3.3.1 Online Upgrade

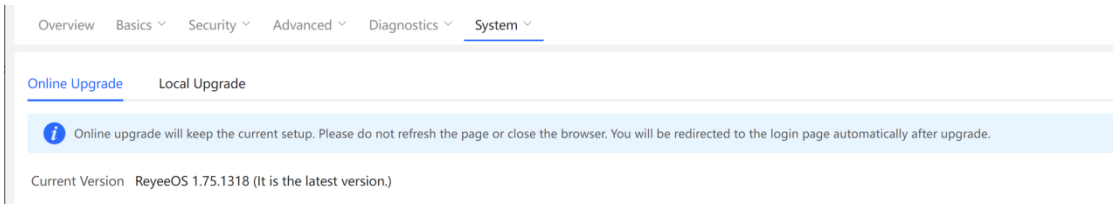
- In SON mode, select **Local Device** and choose **System** > **Upgrade** > **Online Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Online Upgrade**.

You can view the current system version.

- If a new version is available, you can click **Upgrade Now** for an upgrade. The upgrade operation does not affect the current configuration, but the AP will restart after being upgraded successfully. Do not refresh the page or close the browser during the upgrade. You will be redirected to the login page automatically after the upgrade.



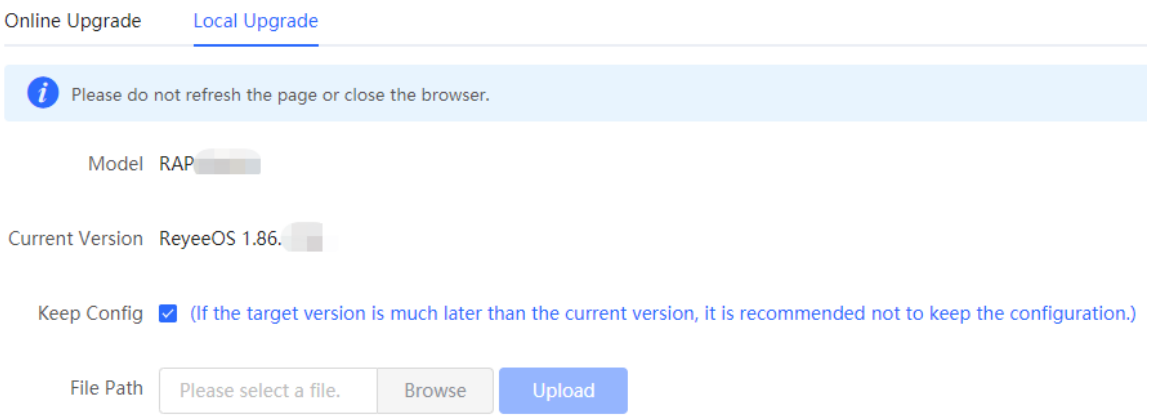
- If there is no new version, a massage is displayed, indicating that the current version is the latest.



3.3.2 Local Upgrade

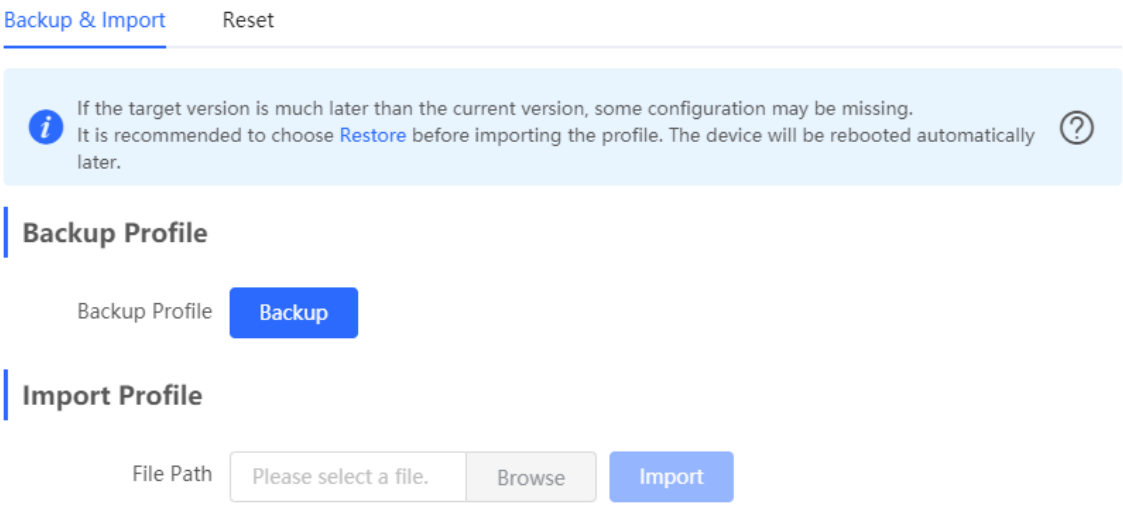
- In SON mode, select **Local Device** mode and choose **System** > **Upgrade** > **Local Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Local Upgrade**.

You can view the current software version, hardware version, and device model. To upgrade the device with the configuration retained, check **Keep Config**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. After the AP is uploaded successfully, the system will display upgrade package information and asks you to upgrade the AP. Click **OK** to start the upgrade.



3.4 Configuring Backup and Import

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



You can import a configuration file to the AP or export the current configuration of the AP.

- 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 AP will restart.

  If the target version is much later than the current version, some configuration may be missing.

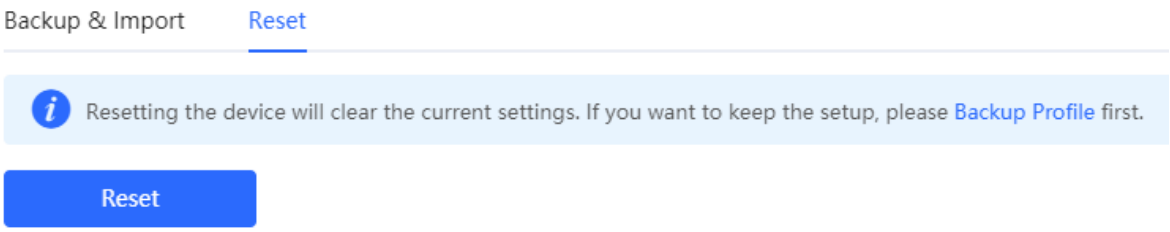
  You are advised to restore the settings before importing the configuration. The AP will restart automatically if you restore it.

3.5 Restoring Factory Settings

- In SON mode, select **Local Device** mode and choose **System** > **Management** > **Reset**.

- In standalone mode, choose **System** > **Management** > **Reset**.

Click **Reset** to restore the AP to factory defaults.



Note

The operation will clear all configuration of the AP. To retain the current configuration, back up the configuration first (see 3.4 Configuring Backup and Import). Therefore, exercise caution when performing this operation.

4 Configuration

4.1 Wireless Configuration

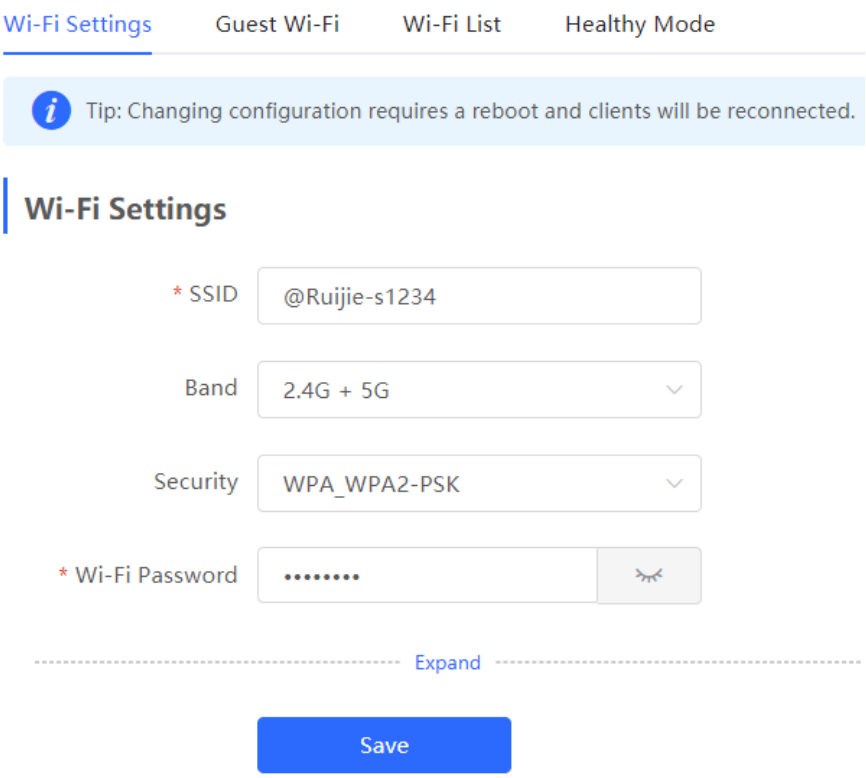
4.1.1 Wireless Basic Configuration

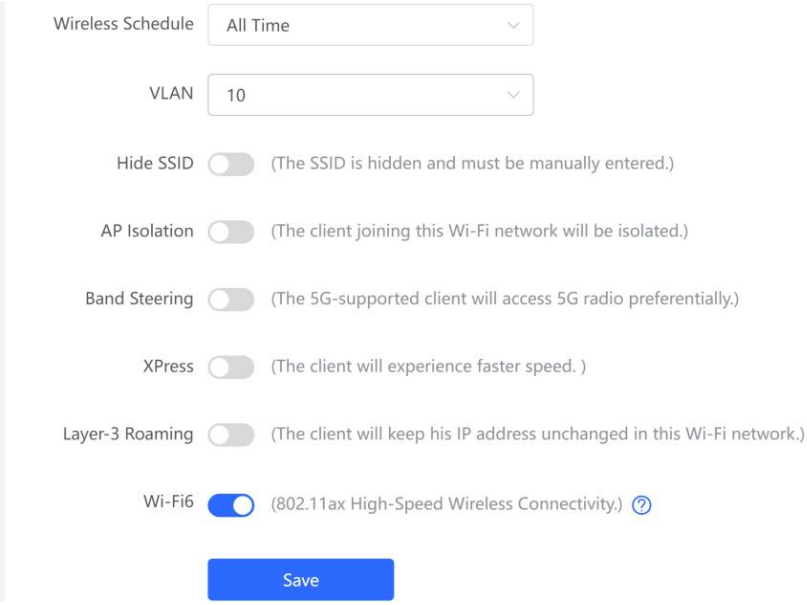
- SON mode
  - To configure the master Wi-Fi, select **Network** and choose **Network** > **Wi-Fi** > **Wi-Fi Settings**.
  - To configure other Wi-Fi, select **Network** and choose **Network** > **Wi-Fi** > **Wi-Fi List**. Then select the target Wi-Fi in the list and click **Edit** in the action bar.
- Standalone mode
  - To configure the master Wi-Fi, choose **WLAN > Wi-Fi > Wi-Fi Settings**.
  - To configure other Wi-Fi, choose **WLAN** > **Wi-Fi** > **Wi-Fi List**. Then select the target Wi-Fi in the list and click **Edit** in the action bar.

Set parameters of the Wi-Fi network and click **Save**.

Note

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.





SSID: indicates the Wi-Fi name.

Band: indicates the band, which is **2.4G**, **5G**, or **2.4G + 5G**.

Security: indicates the security authentication mode, which is **Open**, **WPA-PSK**, **WPA2-PSK**, or **WPA_WPA2-PSK**.

Wireless Schedule: indicates the time when Wi-Fi takes effect.

Hide SSID: disables or enables SSID broadcasting.

AP Isolation: indicates that the SSID-based client will be isolated.

Band Steering: detects clients capable of 5 GHz and steers them to that frequency. 2.4 GHz is available for legacy clients. Enabling this function is not recommended if most clients only support 2.4 GHZ.

XPress: enables faster speed for clients.

Layer-3 Roaming: A client will keep the IP address unchanged on the Wi-Fi network. Layer 3 roaming can be enabled on Reyee APs here, and Ruijie Cloud only supports Ruijie APs.

Wi-Fi 6: Some wireless adapters of old versions may be incompatible. The end points accessing the Wi-Fi 6 network must support 802.11ax.

4.1.2 Guest Wi-Fi Configuration

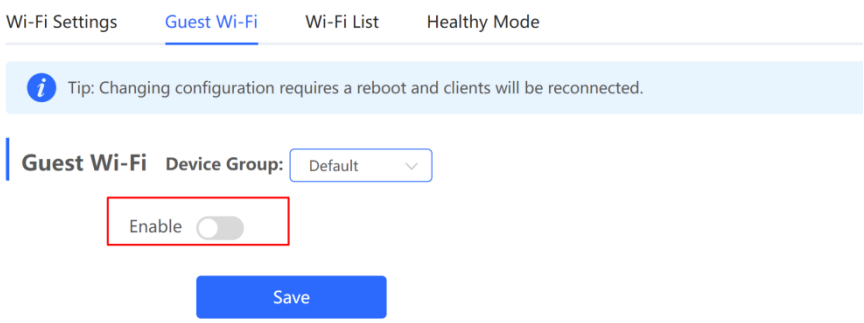
This Wi-Fi network is provided for guests and is disabled by default. It supports client isolation, that is, clients are isolated from each other. The clients can only access the Internet by Wi-Fi, but cannot access each other, improving security. The guest Wi-Fi network can be disabled as scheduled.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

Procedure

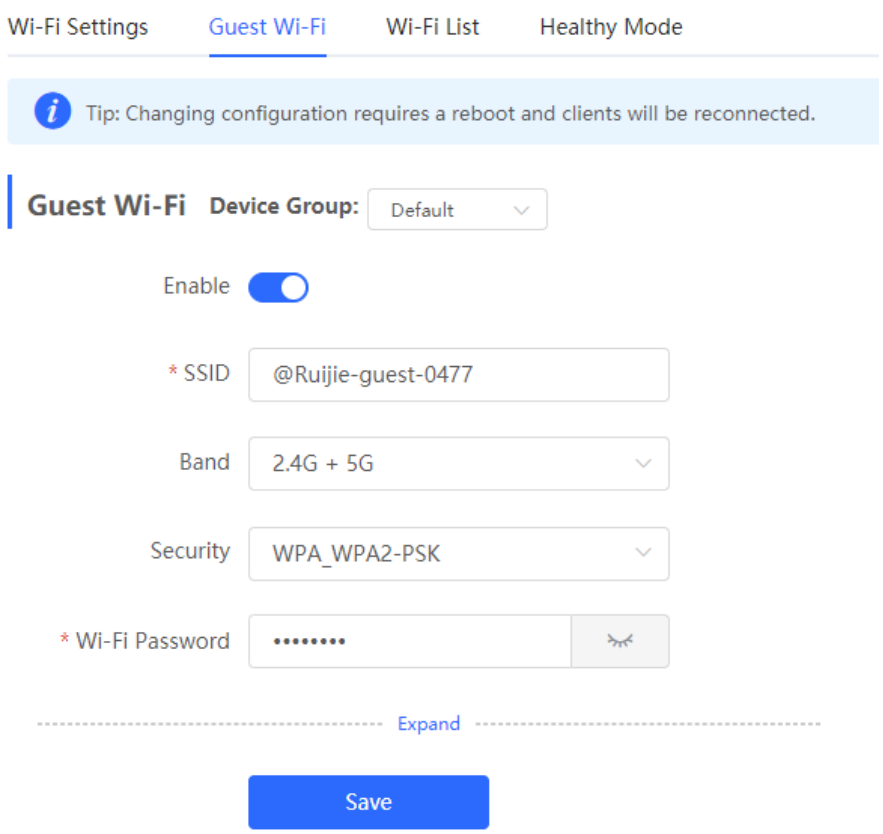
(1) Access the **Guest Wi-Fi** page.

- In SON mode, select **Network** mode and choose **Network** > **Wi-Fi** > **Guest Wi-Fi**.
- In standalone mode, choose **WLAN** > **Wi-Fi** > **Guest Wi-Fi**.

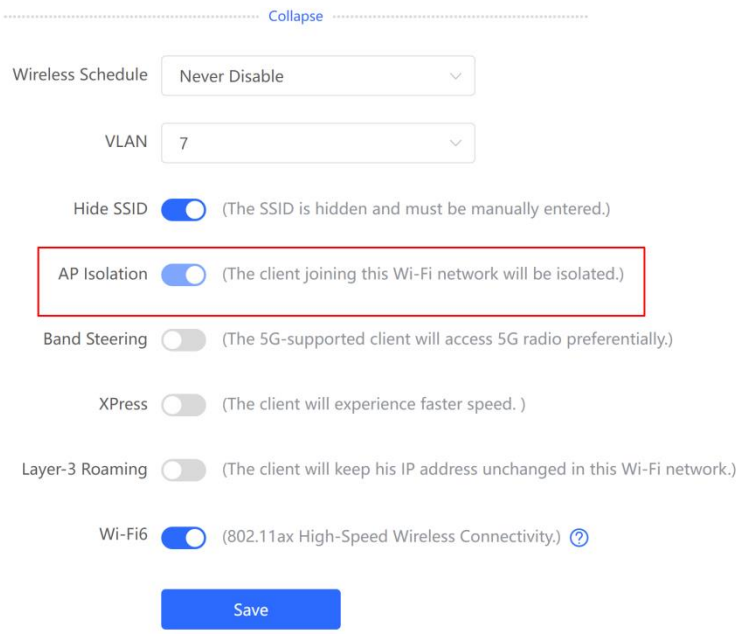
The guest Wi-Fi is disabled by default.



(2) Enable **Guest Wi-Fi** and enter the SSID and Wi-Fi password.



(3) Click **Expand** to configure the validity time and other Wi-Fi features in the expanded settings. Click **Save**. The guest Wi-Fi network will be created. Guests can access the guest Wi-Fi network by entering the SSID and Wi-Fi password.



Instruction

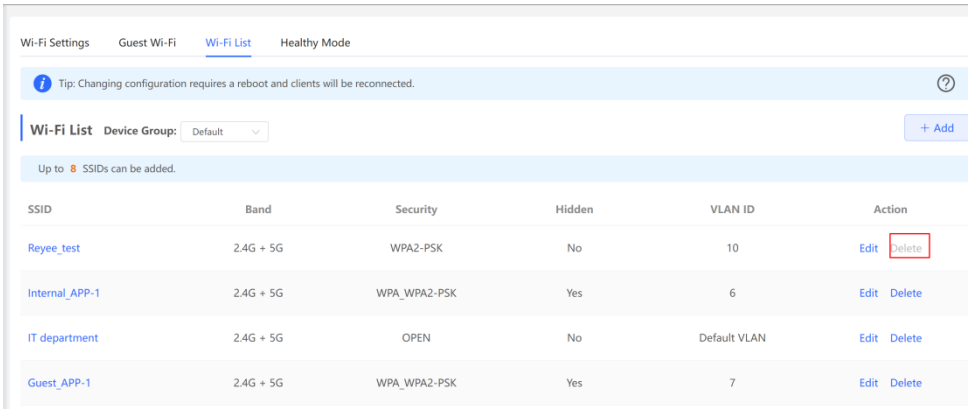
AP isolation is enabled by default and cannot be modified.

Set the wireless schedule. The guest Wi-Fi will be enabled only at this schedule. When the time expires, the guest Wi-Fi will be disabled.

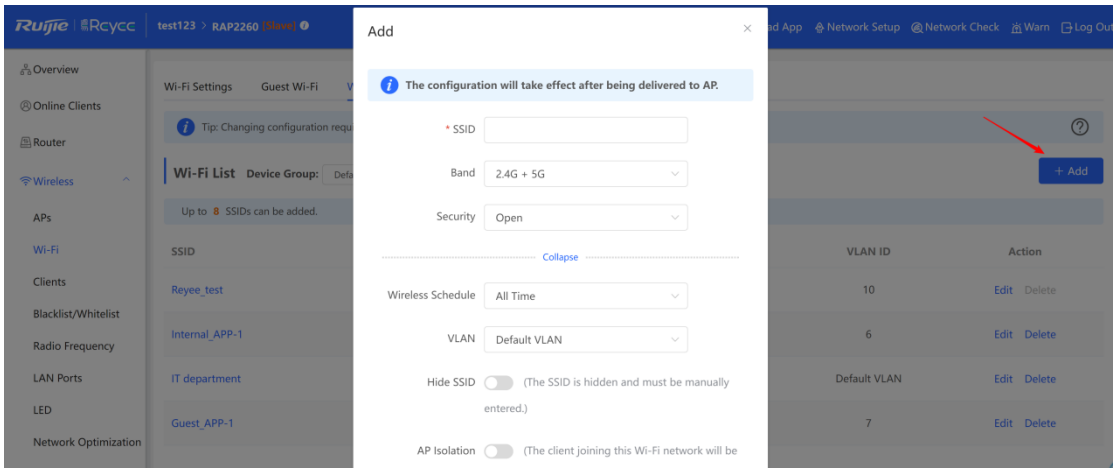
4.1.3 Multiple SSID Configuration

- In SON mode, select **Network** mode and choose **Network** > **Wi-Fi** > **Wi-Fi List**.
- In standalone mode, choose **WLAN** > **Wi-Fi** > **Wi-Fi List**.

Wi-Fi List displays all Wi-Fi networks. The primary Wi-Fi is also listed here and cannot be deleted.



- To reconfigure an existing Wi-Fi network, click **Edit**, set parameters in the displayed dialog box, and click **OK**. After changing the configuration, restart the device. Then your network will be reconnected.
- To add a Wi-Fi network, click **Add**, configure parameters in the displayed dialog box, and click **OK** to save the configuration.



4.1.4 Healthy Mode

Healthy Mode allows you to enable the healthy mode and set a schedule.

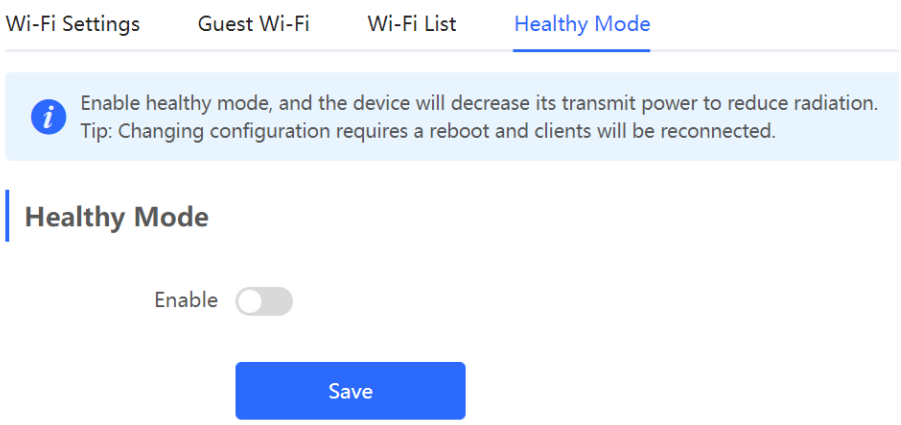
- The healthy mode may reduce signal strength and cause network suspension. You are advised to disable it or enable it when the network is idle.
- After the healthy mode is enabled, the AP will decrease its transmit power to reduce radiation.
- After changing the configuration, restart the device. Then your network will be reconnected.
- Router radiation is much lower than common radiation, which does not cause damage to the human body.

Procedure

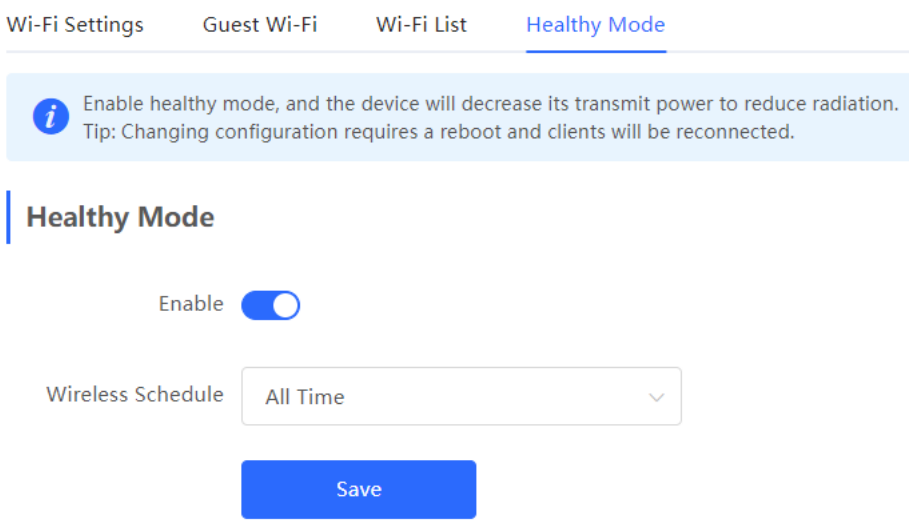
(1) Access the **Healthy Mode** page.

- In SON mode, select **Network** and choose **Network** > **Wi-Fi** > **Healthy Mode**.
- In standalone mode, choose **WLAN** > **Wi-Fi** > **Healthy Mode**.

(2) Click **Enable** to enable the healthy mode.



(3) Set the validity time for the healthy mode, and click **Save**.



4.1.5 Wireless Client List

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

Check information about all wireless clients connected to the Wi-Fi network. You can click **Advanced Search** to search clients by SN and MAC address.

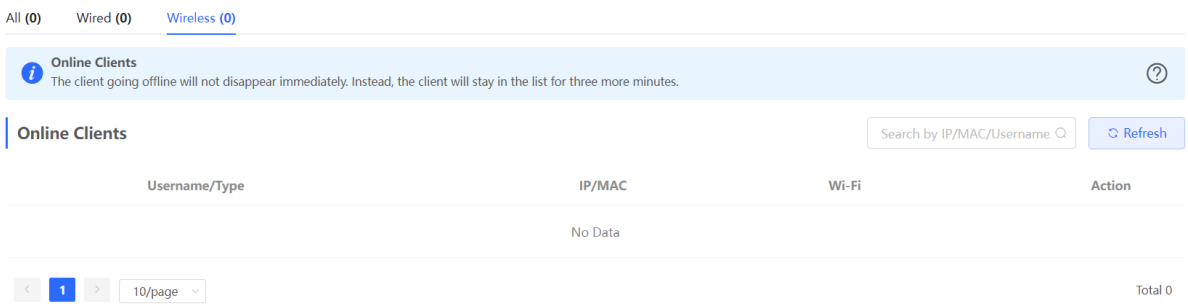


Table 4-1 Description of Wireless Client Information

Item	Description
Username/Type	Name and type of the client.
IP/MAC	IPv4 address and MAC address of the client.
Wi-Fi	Name of the Wi-Fi network associated with the client.
Action	Click **Add to Blocklist** to disconnect a client and prevent the client from accessing the Wi-Fi network.

4.1.6 Radio Frequency Configuration

- SON mode:
  - To configure the master device, select **Network** and choose **Network > Radio Frequency**.
  - To configure the slave device, select **Devices**, select the target device in the device list, and choose **SN** > **Radio Frequency**.
- In standalone mode, choose **WLAN > Radio Frequency**.

  Select the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. More devices in a channel indicate more severe interference.

Instruction

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

Configure radio frequency parameters on the **Radio Frequency** page and click **Save**.

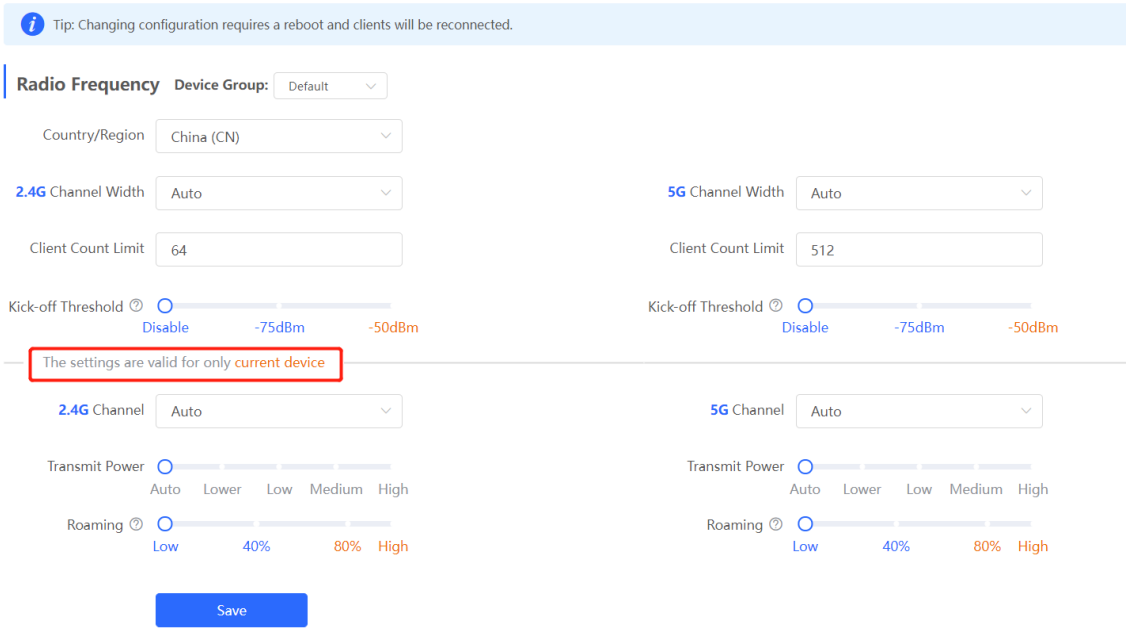


Table 4-2 Description of Radio Frequency Information

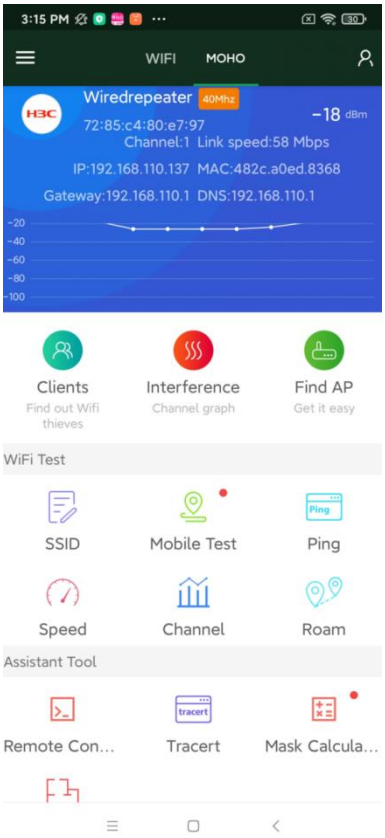
Item	Description
Country/Region	Set this parameter according to your location.
2.4G Channel Width/5G	Different products and different regions may have different

Item	Description
Channel Width	channel width. If the interference is severe, select a lower channel width to avoid network suspension. The AP supports the channel width of 20 MHz and 40 MHz. You are advised to select 20 MHz channel width. After changing the channel width, click **Save** to make the configuration take effect immediately.
Client Count Limit	Limit the number of connected clients. The AP that is associated with a large number of clients has lower performance, affecting user experience. After the threshold is configured, new clients over the threshold are not allowed to access the Wi-Fi network. You can reduce the threshold if bandwidth is required per client. You are advised to keep the default settings unless there are special cases.
Kick-off Threshold	A farther distance where the client is away from the AP indicates a lower signal strength. When the signal strength is lower than the threshold, the client will be disconnected. In this case, select a nearer Wi-Fi signal.
2.4G Channel/5G Channel	In **Auto** mode, the AP will automatically select the best channel according to the environmental interference. You can also select the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. More devices in a channel indicate more severe interference.
Transmit Power:	**Lower** means 25%, **Low** means 50%, **Medium** means 75%, and **High** means 100%. A larger value indicates a wider coverage. A greater transmit power indicates a larger coverage and brings more severe interference to surrounding wireless routers. In a high-density scenario, you are advised to set a small transmit power. The **Auto** mode is recommended, indicating automatic adjustment of the transmit power.
Roaming Sensitivity	Roaming sensitivity is the rate at which a device selects and switches to the nearest available AP, offering a better signal. A higher roaming sensitivity level indicates a poorer Wi-Fi coverage. If the device does not roam, select a low roaming sensitivity level.

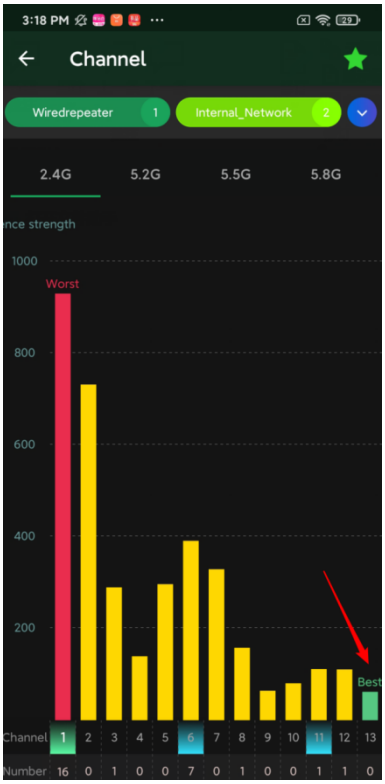
Item	Description
	If the device roams, increase the roaming sensitivity level to obtain a better signal. A lower level indicates a greater coverage and less frequent roaming. Advantage: The connection is retained. Disadvantage: The signal may be poor. A higher level indicates a poorer coverage and more frequent roaming. Advantage: The device will send a strong signal. Disadvantage: The connection will be ended when roaming occurs.

Wireless Optimization Example

Enable Wi-Fi Moho when the SSID is connected and click **Channel** to check the current environmental channel utilization.



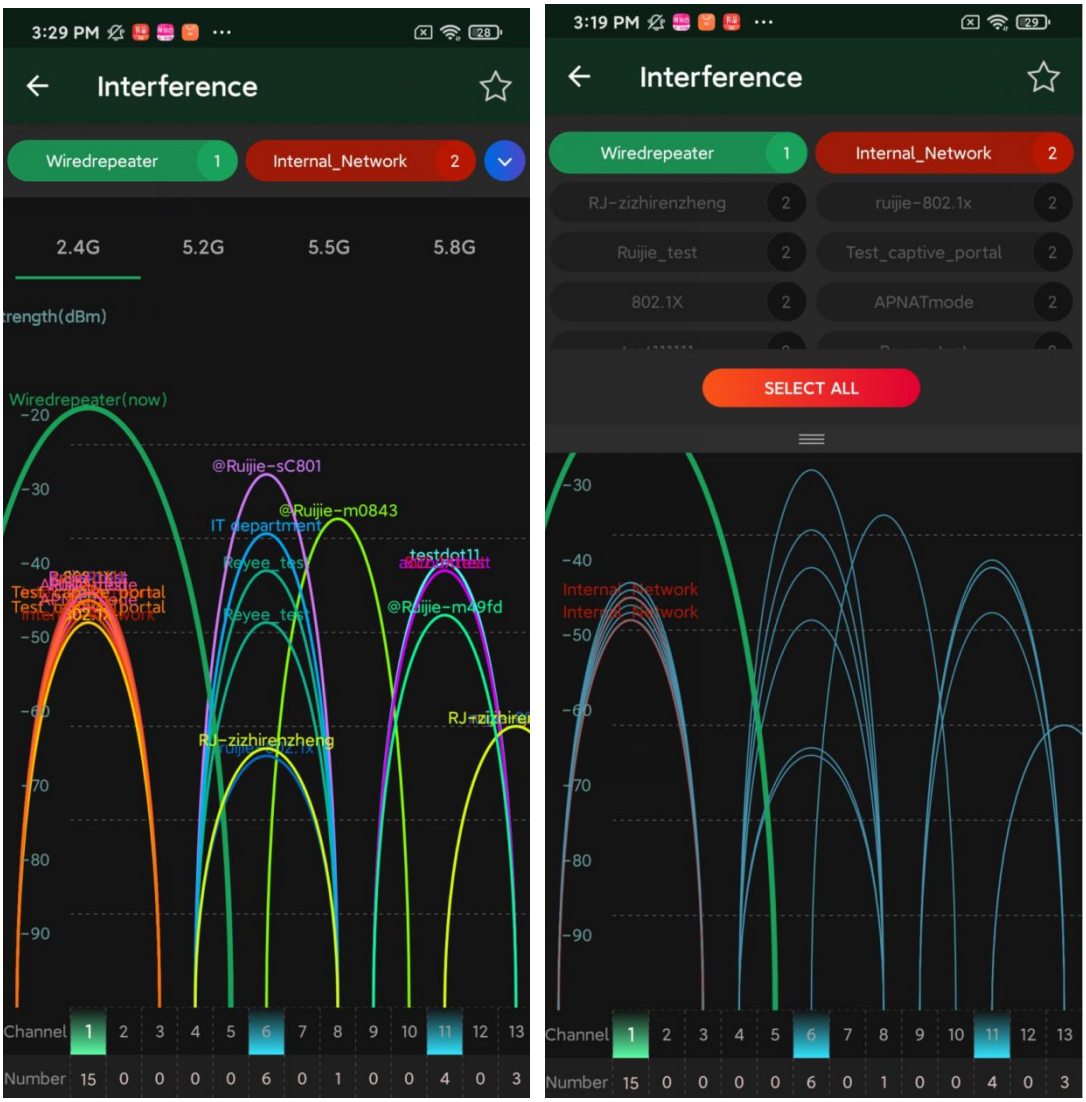
In the following figure, devices are centralized in channel 1 under 2.4 GHz, and channel 13 is the best.



To learn the SSID that belongs to a channel, click **Interference**.

The green color represents the currently connected SSID. You can select the remaining SSIDs on the top to view the channel.

When your wireless speed is slow or during deployment, you can use Wi-Fi Moho to check the configuration. Then select the channel with the least interference.



4.1.7 Wireless Blocklist/Allowlist Configuration

You can configure the global or SSID-based blocklist and allowlist. The MAC address can be matched exactly or based on the OUI.

- 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 allowed 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.

1. Configuring a Global Blocklist or Allowlist

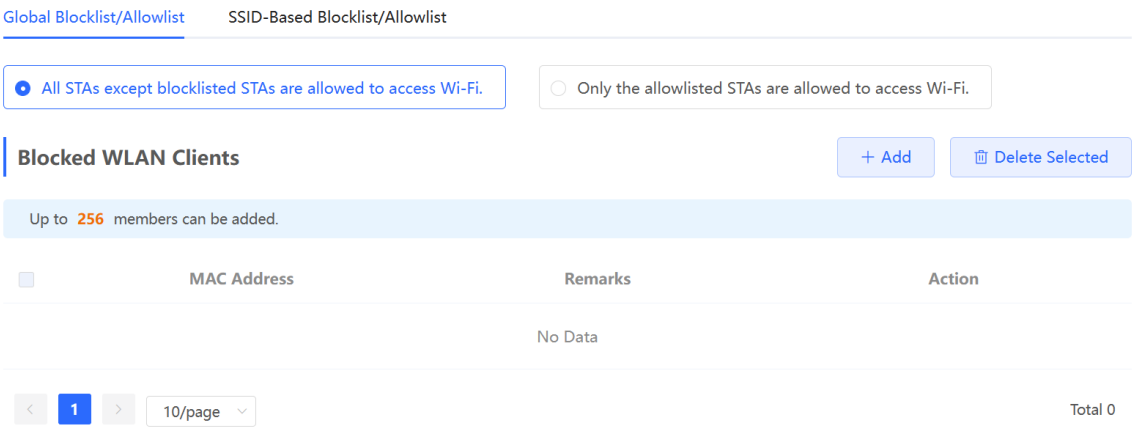
(1) Access the **Global Blocklist/Allowlist** page.

- In SON mode, select **Network** and choose **Clients** > **Blocklist/Allowlist** > **Global Blocklist/Allowlist**.
- In standalone mode, choose **WLAN** > **Blocklist/Allowlist** > **Global Blocklist/Allowlist**.

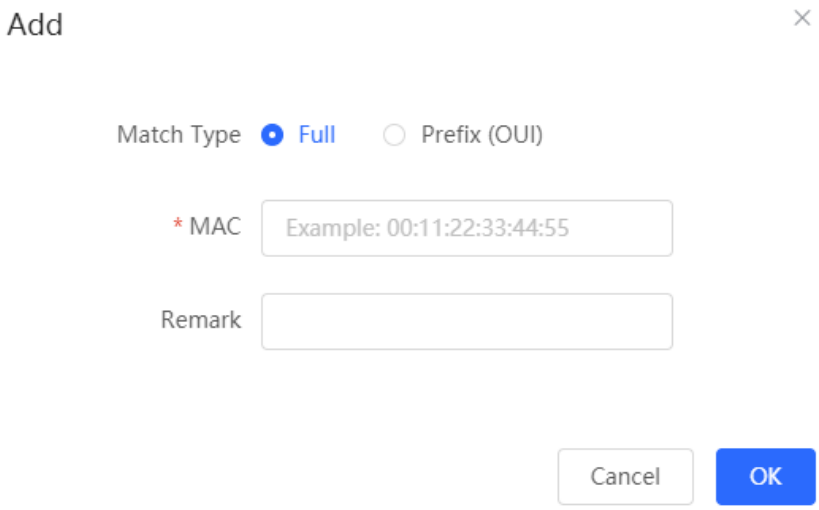
(2) Select the blocklist or allowlist mode and click **Add** to add a client to a blocklist or allowlist.

Note

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



(3) In the **Add** window, enter the MAC address and remarks of the target client and click **OK**. If a client is already associated with the AP, its MAC address is displayed automatically. Click the MAC address. All clients in the blocklist are disconnected and prevented from accessing the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the AP.



2. Configuring an SSID-based Blocklist or Allowlist

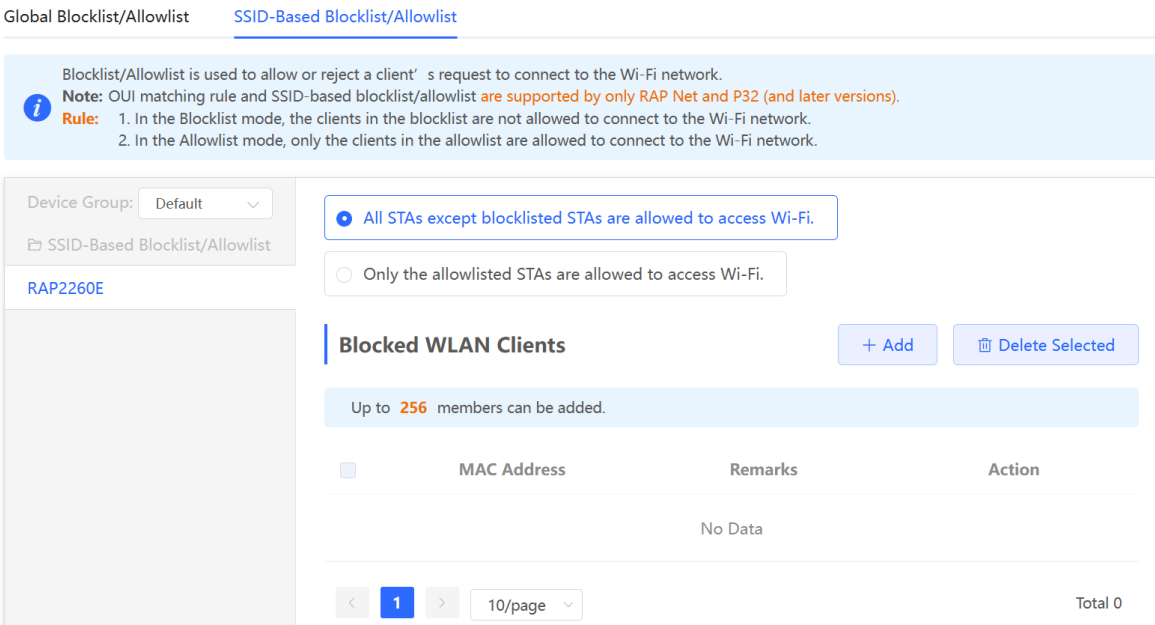
Note

Only RAP Net and P32 (and later versions) support OUI matching and SSID-based blocklist or allowlist.

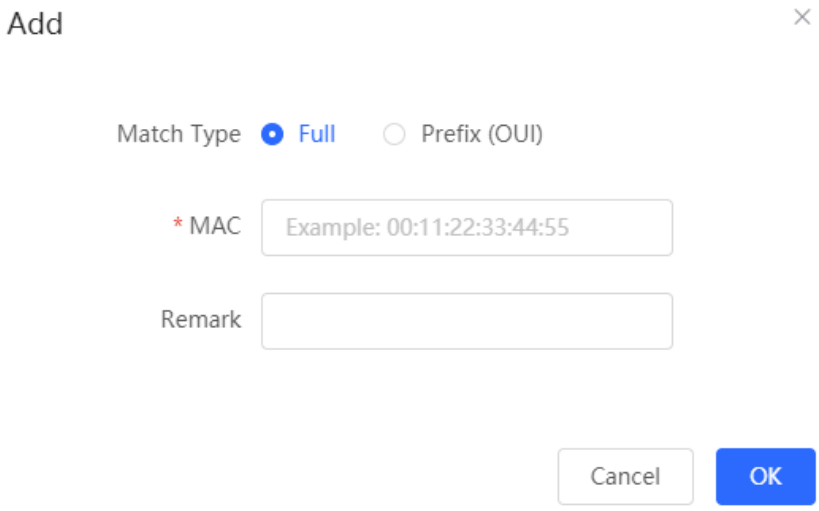
(1) Access the **SSID-Based Blocklist/Allowlist** page.

- In SON mode, select **Network** and choose **Clients** > **Blocklist/Allowlist** > **SSID-Based Blocklist/Allowlist**.
- In standalone mode, choose **WLAN** > **Blocklist/Allowlist** > **SSID-Based Blocklist/Allowlist**.

(2) Select a target Wi-Fi network from the left column and select the blacklist or allowlist mode



(3) Click **Add** to add a client to a blacklist or allowlist. The SSID-based blacklist or allowlist will restrict or allow the client's access to the specified Wi-Fi network.



4.1.8 AP Group Configuration

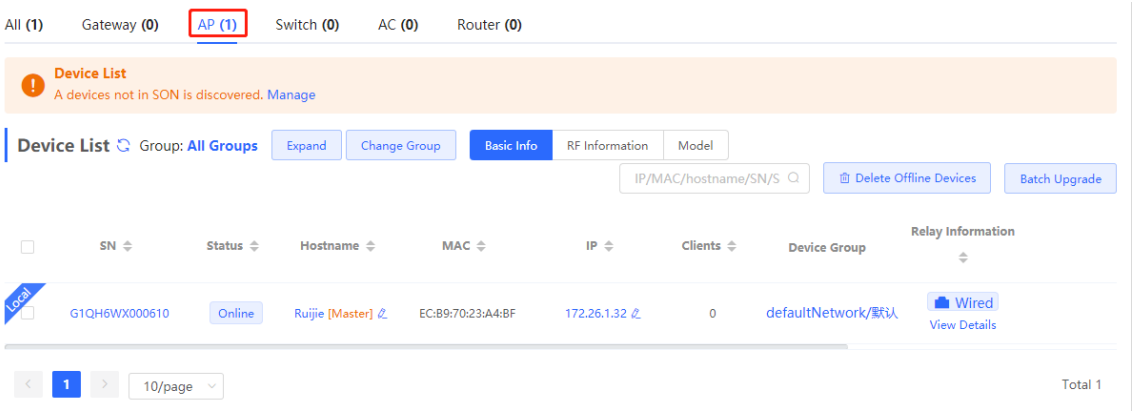
After the SON is enabled, the device can act as the master AP or AC to perform batch configuration and management on the downlink APs in a group. Aps need to be grouped before the configuration is delivered.

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.

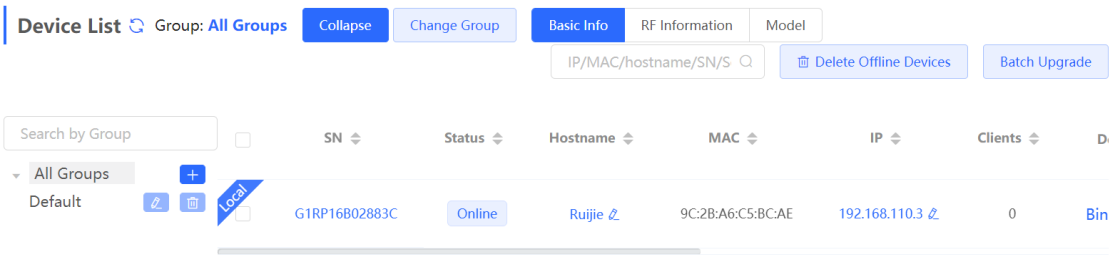
In **Network** mode, choose **Devices** > **AP**.

Check information about all APs on the live network, including basic information, RF information, and models. You can click **SN** to configure the device.



You can configure AP groups, and APs can be upgraded, deleted, or moved to other groups.

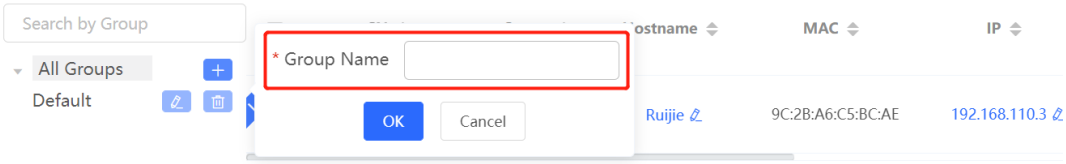
- Click **Expand** to view all groups on the left part of the **AP List** page. A device can only belong to a group. By default, all devices belong to the default group. The default group cannot be deleted and its name cannot be edited.



After clicking **Expand**, you can add or delete a group, edit the group name, or click the group name.

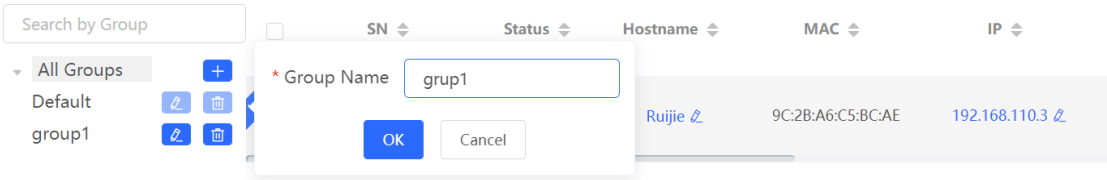
- Add a group. Up to eight groups can be added.

Click +, enter the group name, and click **OK** to create a group.



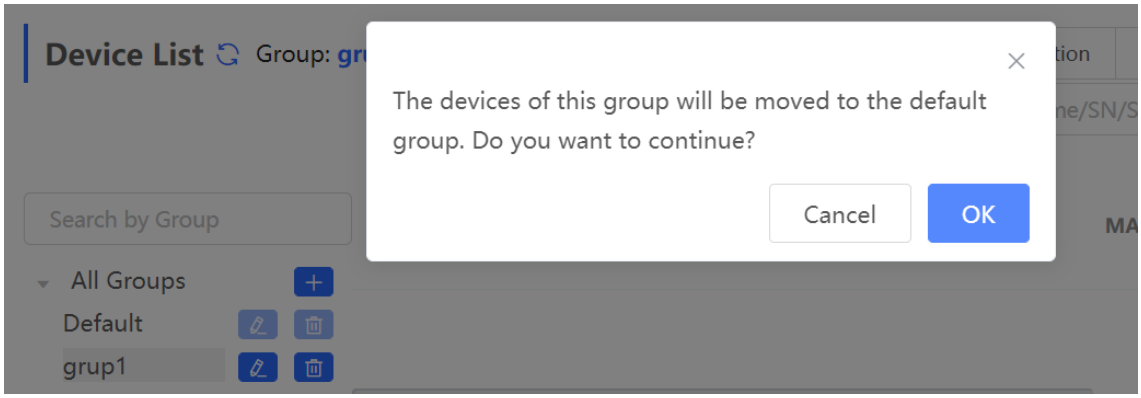
- Edit the group name.

  Click , change the group name, and click **OK**.



- Delete a group.

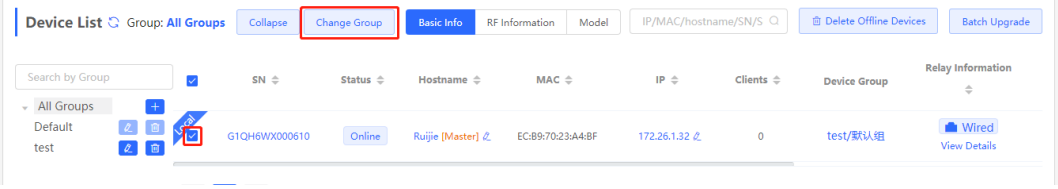
  Click . Then click **OK** in the displayed window.



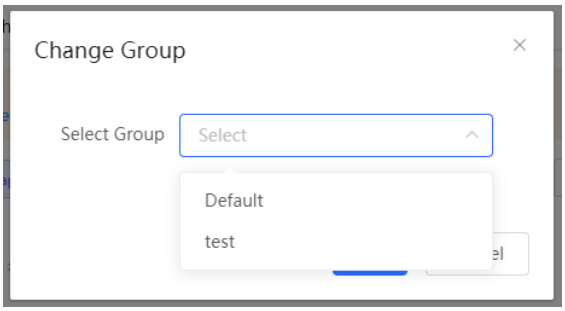
- Click the group name on the left part to view all devices in this group.

- Change the group that the device belongs to.

  a Select one or more offline devices in **Device list** and click **Change Group**.



  b Select a new group for the target device and click **OK**. Then the device will apply the configuration of this group.



- Delete offline devices.

  Select one or more offline devices in **Device list** and click **Delete Offline Devices** to remove devices from the list.

- Upgrade devices.

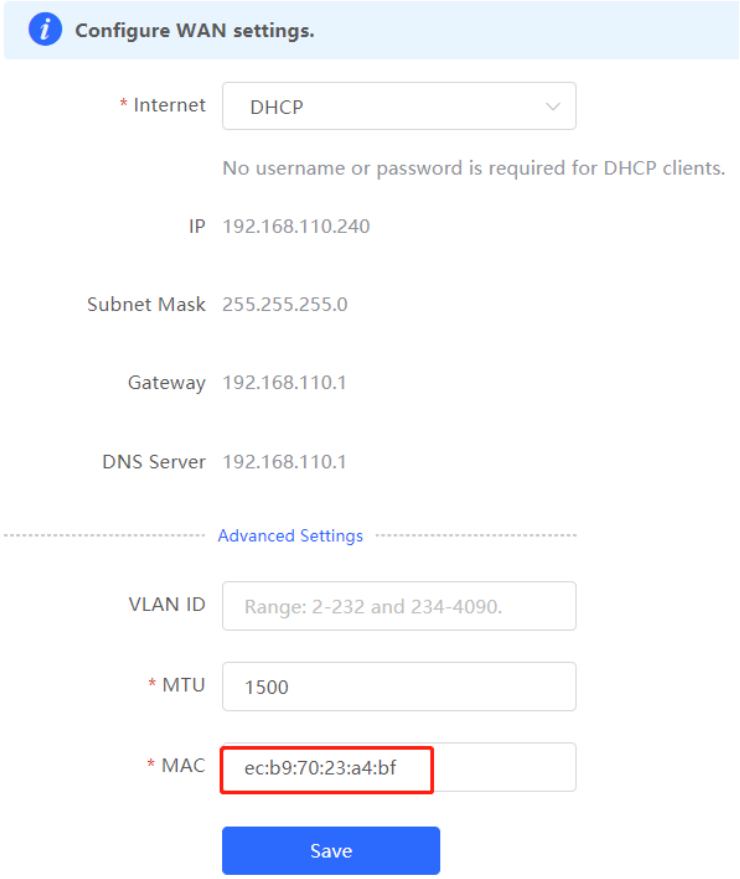
  Select one or more devices in **Device list** and click **Batch Upgrade** to upgrade devices in batches.

4.2 Basic Configuration

4.2.1 WAN Port Configuration

- In SON mode, select **Local Device** and choose **Network** > **WAN**.
- In standalone mode, choose **Network** > **WAN**.

Set parameters of WAN port configuration and click **Save**.



Internet: Select the Internet access mode after confirming with the ISP. You can select **PPPoE**, **DHCP**, or **Static IP**.

- **PPPoE**: Access the Internet by using the broadband account provided by the ISP.
- **DHCP**: Access the Internet by using the dynamic IP address provided by the ISP.
- **Static IP**: Access the Internet by using a static IP address provided by the ISP.

  When **Internet** is set to **Static IP**, **IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server** are mandatory.

VLAN ID: The value ranges from 2 to 232 and 234 to 4090.

MTU: Maximum transmission unit (MTU) allowed by a WAN port. The default value is 1500 bytes. In some scenarios, large data packets need to be rate-limited or prevented. As a result, the network speed is low or even the network is disconnected. In this case, you can configure a small MTU.

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

Note

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. You do not need to change the default MAC address unless in special cases.

4.2.2 LAN Port Configuration

1. VLAN Settings of a Port

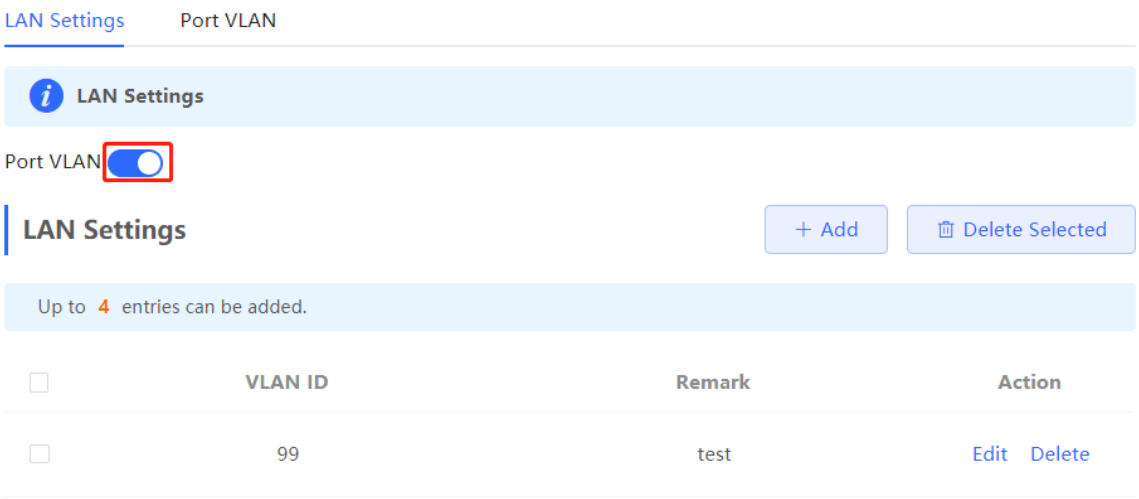
Note

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

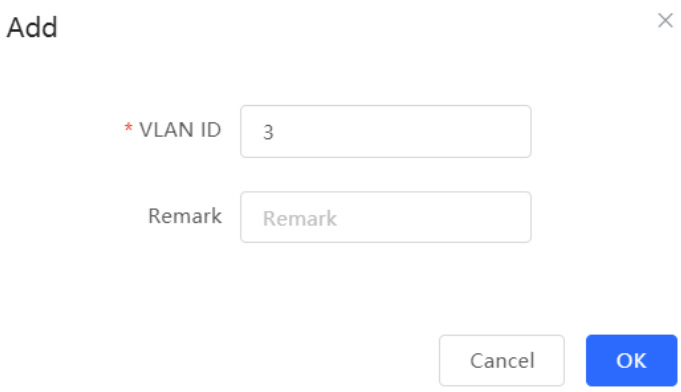
(1) Access the **LAN** page.

- In SON mode, select **Local Device** mode and choose **Network** > **LAN**.
- In standalone mode, choose **Network** > **LAN**.

(2) On the **LAN Settings** tab page, enable **Port VLAN**, and click **OK** in the displayed dialog box.

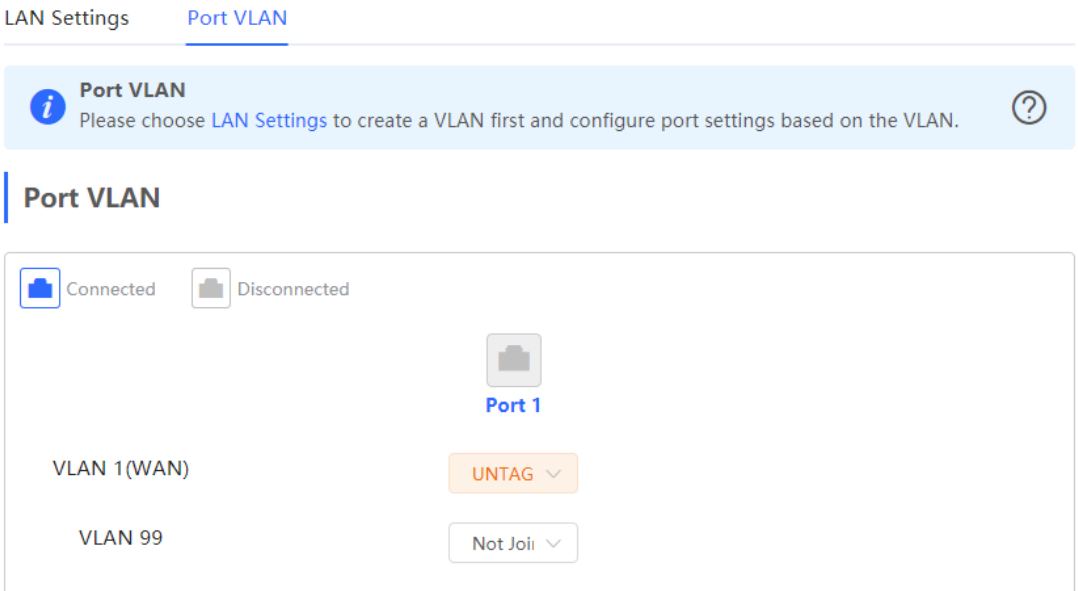


(3) Click **Add**. Enter the VLAN ID and description, and click **OK** to create a VLAN. The added VLAN is used to set the VLAN to which a port belongs.



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

- **UNTAG**: Configure the VLAN as the native VLAN of the port. That is, when receiving a packet from this VLAN, the port removes the VLAN tag from the packet and forwards the packet. When receiving an untagged packet, the port adds the VLAN tag to the packet and forwards the packet through the VLAN. Only one VLAN can be configured as an untagged VLAN on each port.
- **TAG**: Configure the VLAN as an allowed VLAN of the port. The VLAN cannot be the native VLAN. That is, VLAN packets carry the original VLAN tag when being forwarded by the port.
- **Not Join**: Configure the port not to allow packets from this VLAN to pass through. For example, if port 2 is not added to VLAN 10 and VLAN 20, port 2 does not receive or send packets from or to VLAN 10 and VLAN 20.



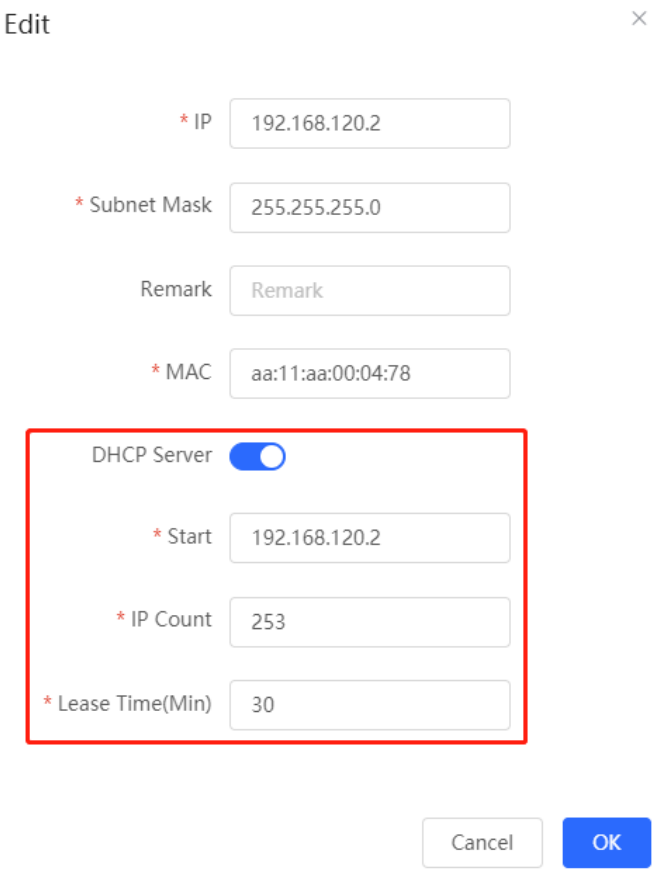
2. DHCP Server Configuration

Note

- This function is only available in router mode.
- If the DHCP server function is disabled on all devices of a 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.

- In SON mode, select **Local Device** and choose **Network** > **LAN**.
- In standalone mode, choose **Network** > **LAN**.

On the **LAN Settings** tab page, click **ADD**, set parameters of the DHCP server, and click **OK**.



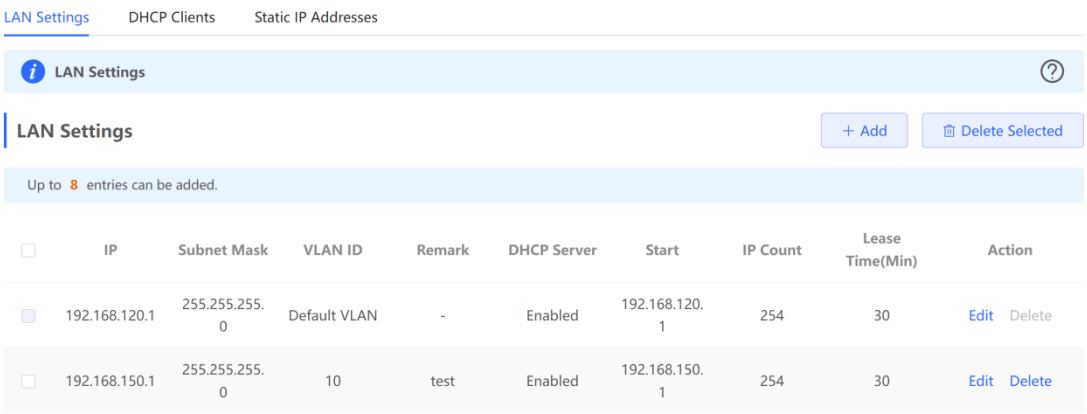
DHCP server: The DHCP server function is enabled by default in router mode. You are advised to enable the function if the device is used as the sole router on a network. When multiple routers are connected to the upper-layer device through LAN ports, disable this function.

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.

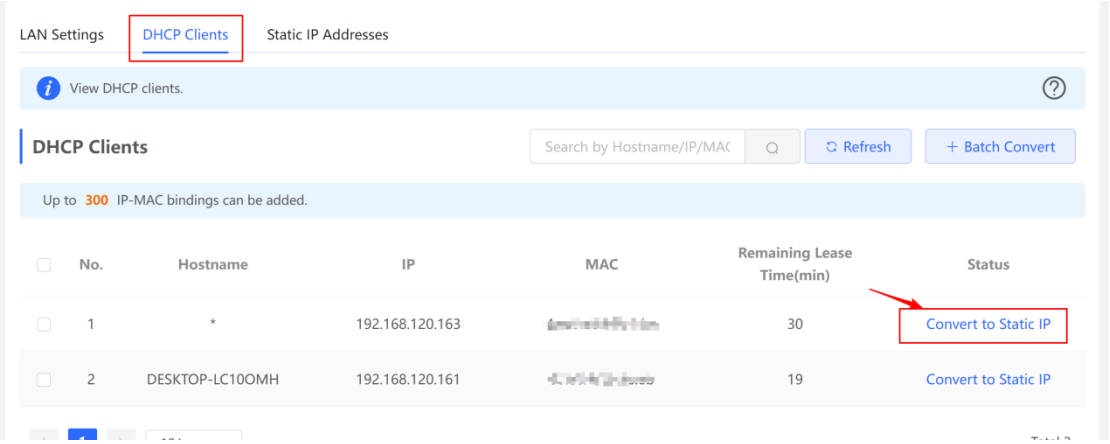
IP Count: Enter the number IP addresses in the address pool.

Lease Time(Min): Enter the address lease time. 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 time expires. After the client connection is restored, the client can request an IP address again. The default lease time is 30 minutes.

After the DHCP server is configured, you can check the configuration on the LAN Settings tab page. You can click **Edit** to change the DHCP server configuration.



Switch to the **DHCP Clients** tab page to 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.



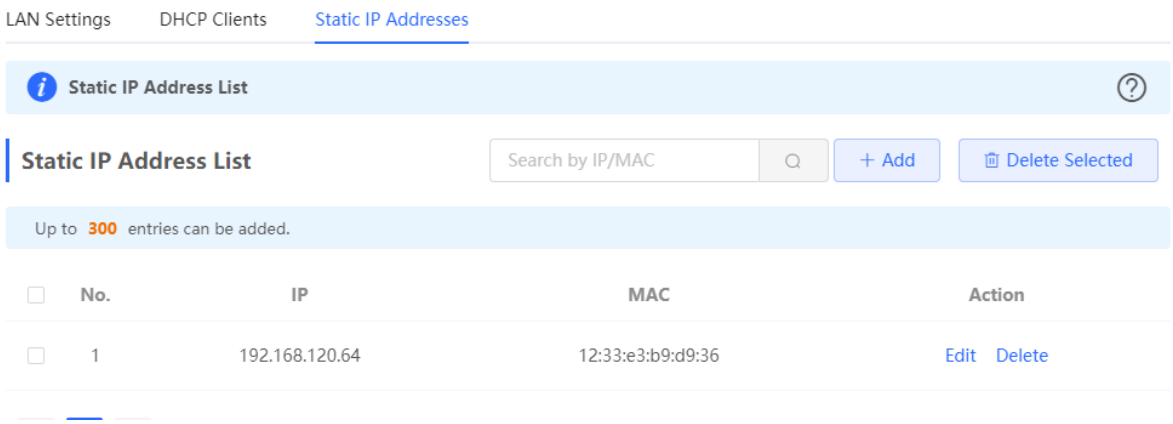
3. Binding Static IP Addresses

Note

This function is only available in router mode.

- In SON mode, select **Local Device** and choose **Network** > **LAN** > **Static IP Addresses**.
- In standalone mode, choose **Network** > **LAN** > **Static IP Addresses**.

Click **Add**. In the displayed dialog box of static IP address bindings, 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. You can click **Edit** to modify IP address and MAC address.



4.3 Wireless Authentication

Caution

This function is supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, and RG-RAP6262.

4.3.1 Overview

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

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

The following four authentication modes are supported:

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

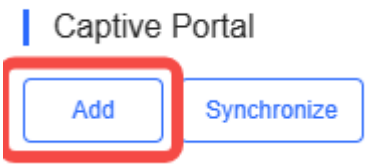
Two or more authentication modes can be configured in a portal template. When multiple authentication modes are configured, users can select an authentication mode on the portal page.

4.3.2 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** > **Authentication** > **Captive Portal**, and select a network that needs to configure wireless authentication.

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



(3) Configure basic information of the portal template.

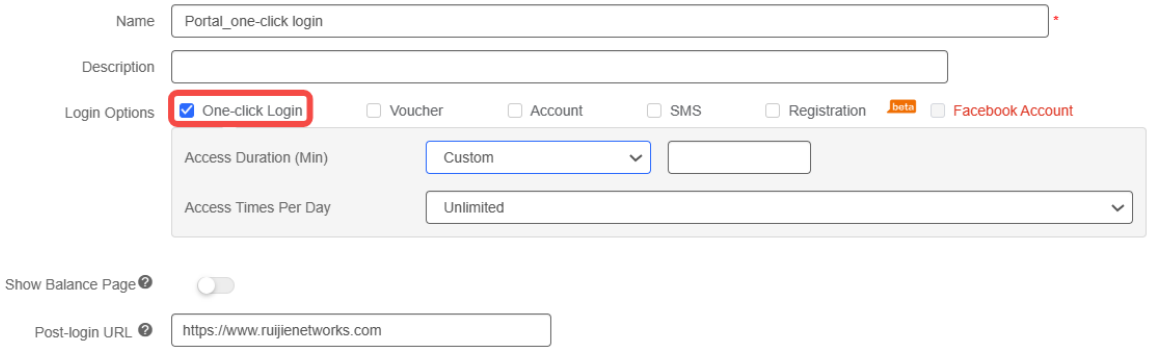


Table 4-3 Basic Information of the Portal Template

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

(4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

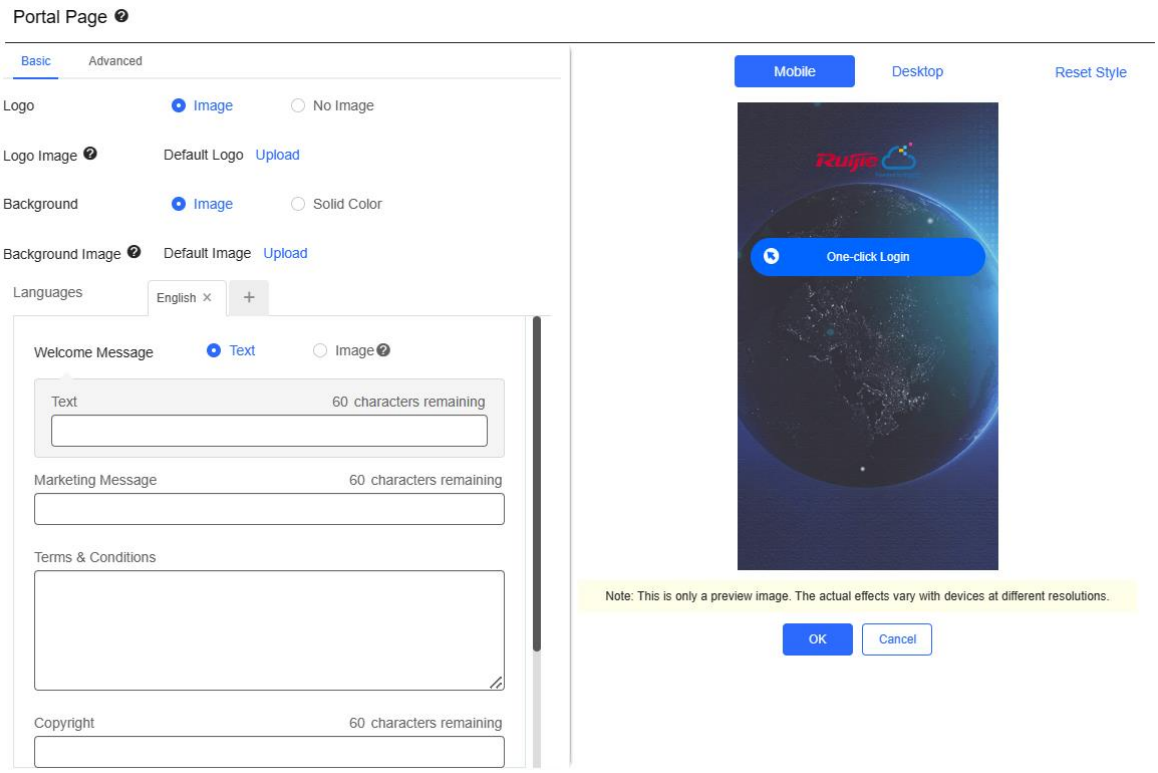


Table 4-4 Basic Information of the Portal Page

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
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 Color	When **Background** is set to **Solid Color**, configure the background color. The default value is **#ffffff**.
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.

Parameter	Description
	● 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. 

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.

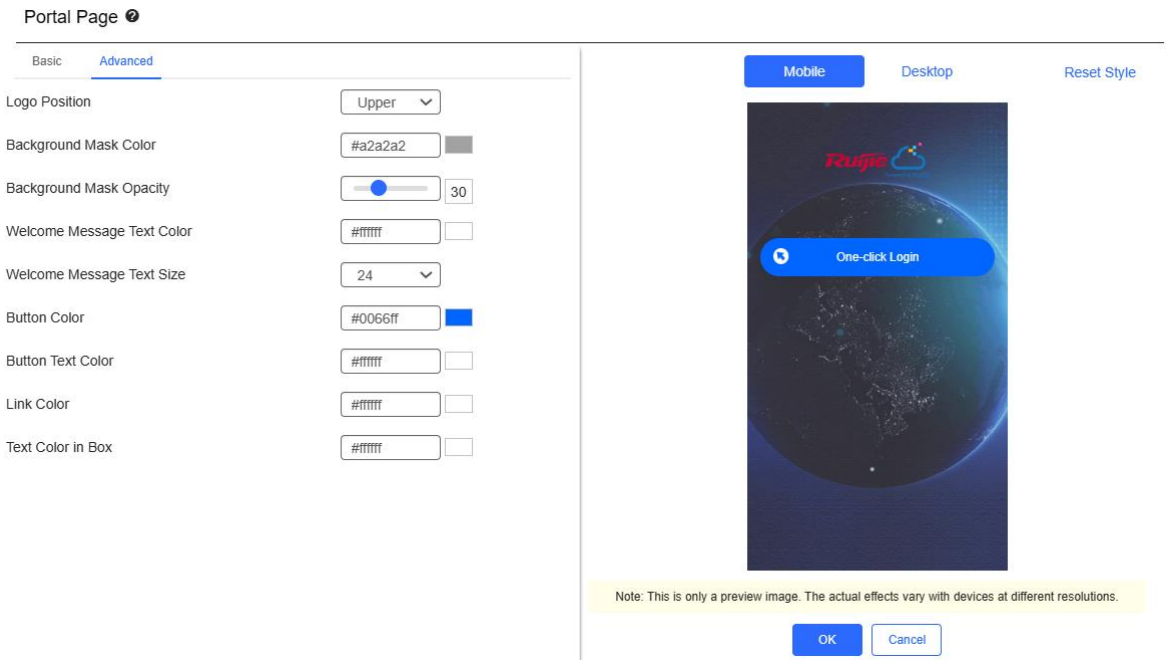


Table 4-5 Advanced Information of the Portal Page

Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background Mask Color	Select the background mask color. The default value is #a2a2a2.
Background Mask Opacity	Select the background mask opacity (0-100).
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.

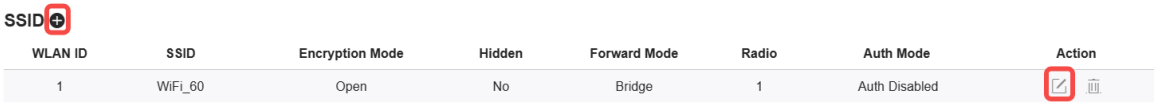
Parameter	Description
Welcome Message Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

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

2. Enabling One-click Login for an SSID

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **SSID**, and select a network that needs to configure wireless authentication.

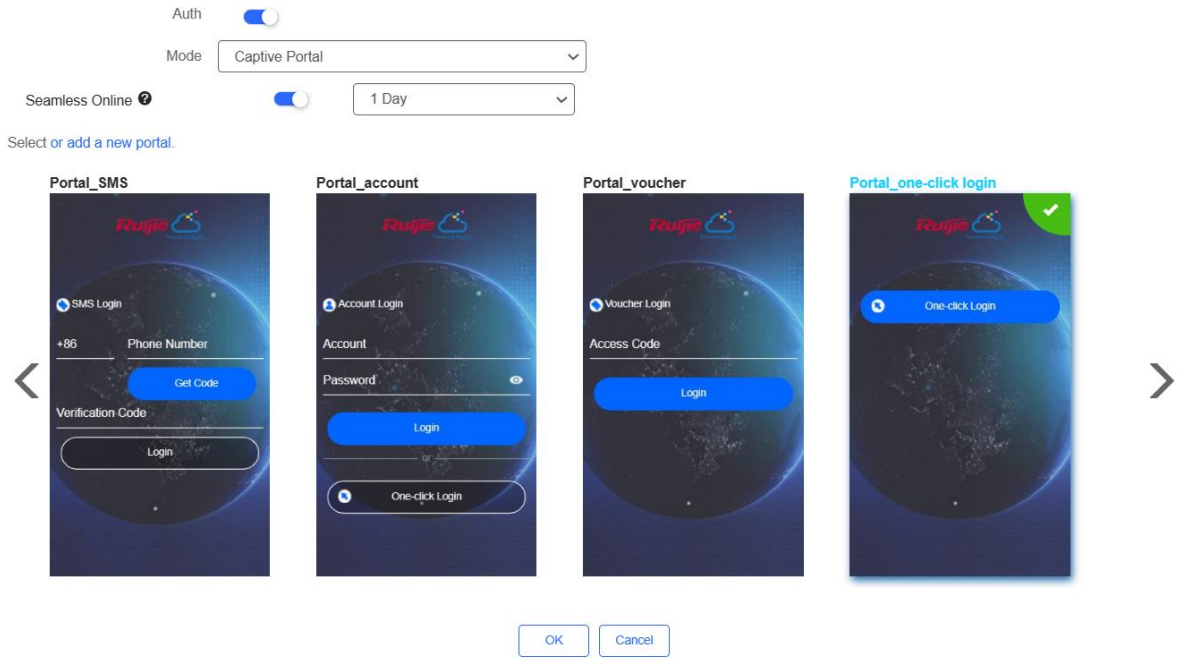
(2) If the SSID that needs to enable wireless authentication is not created, click to open the SSID configuration page. If the SSID that needs to enable wireless authentication is created, click in the **Action** column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.



(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

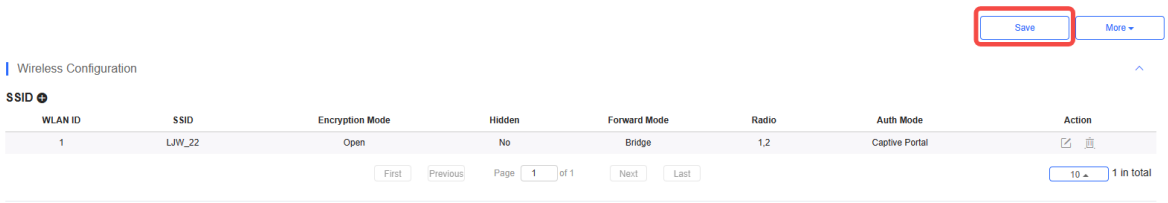
Note

When Encryption Mode is set to a value other than WPA2-Enterprise(802.1x), Auth is available and you can select whether to perform wireless authentication.



- **Mode**: Set it to **Captive Portal**.
- **Seamless Online**: Determine whether to enable **Seamless Online** as required, which is enabled by default. After **Seamless Online** is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- **Select or add a new portal**: Select a portal template with the authentication mode set to **One-click Login**. If the configured template does not meet the requirements, click **or add a new portal** to create a portal template.

(4) Click **Save** for the configuration to take effect.

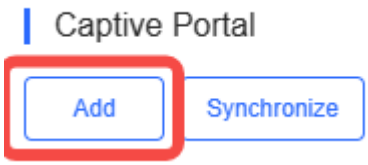


4.3.3 Configuring Voucher Authentication on Ruijie Cloud

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

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

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



(3) Configure basic information of the portal template.

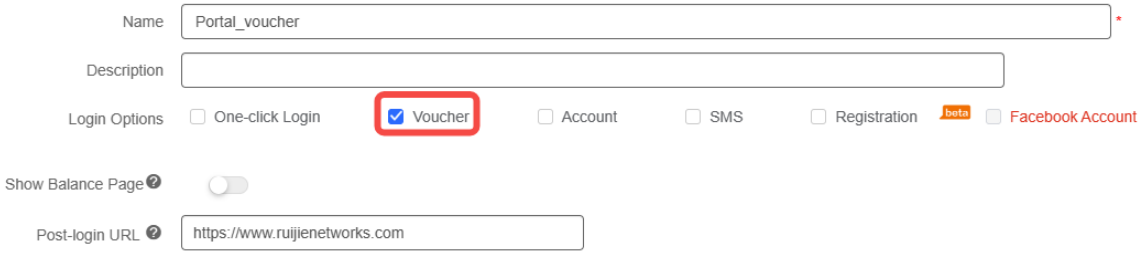


Table 4-6 Basic Information of the Portal Template

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

(4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

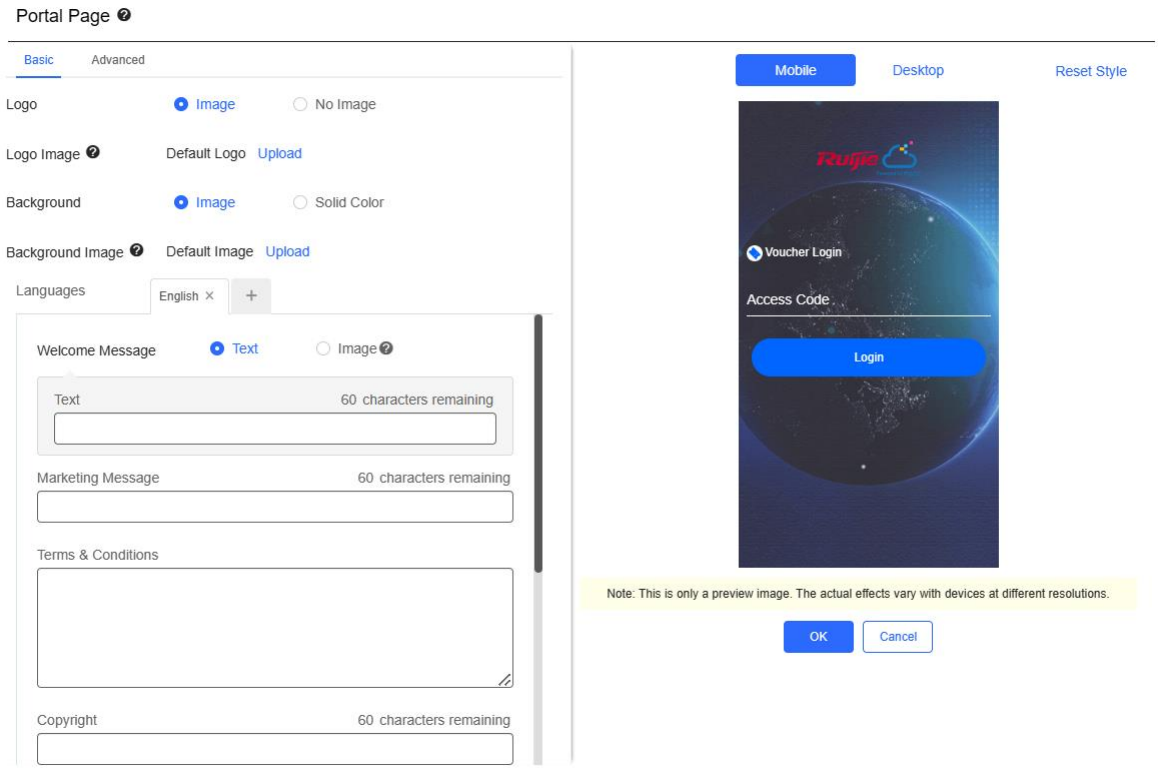
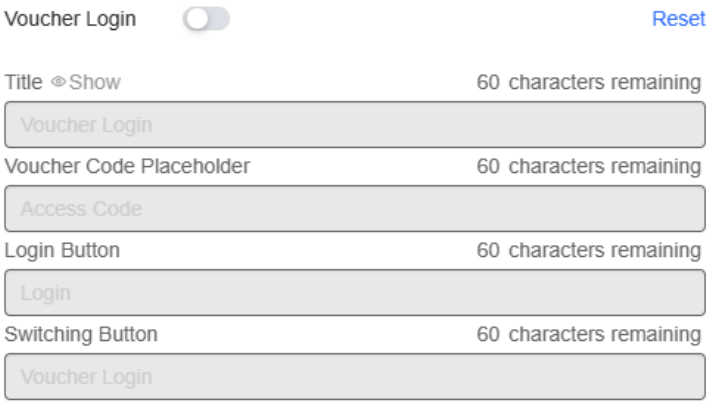


Table 4-7 Basic Information of the Portal Page

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
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 Color	When **Background** is set to **Solid Color**, configure the background color. The default value is **#ffffff**.
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.

Parameter	Description
	● Voucher Login: After **Voucher Login** is enabled, you can customize the names of controls related to voucher authentication. 

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.

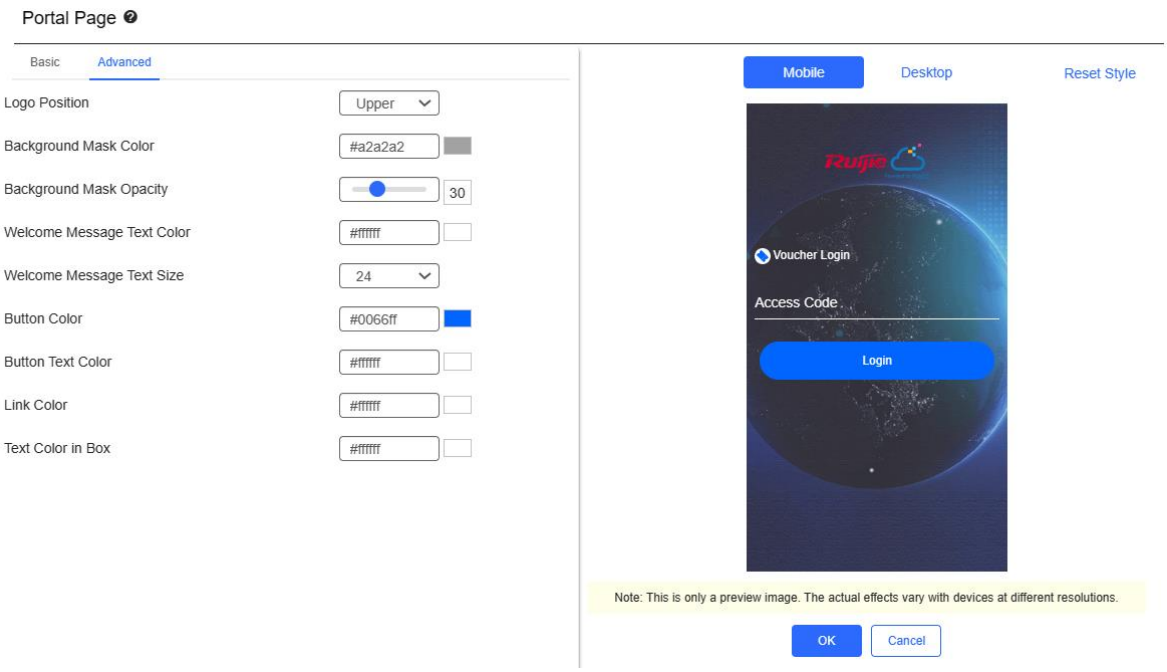


Table 4-8 Advanced Information of the Portal Page

Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background Mask Color	Select the background mask color. The default value is #a2a2a2.
Background	Select the background mask opacity (0-100).

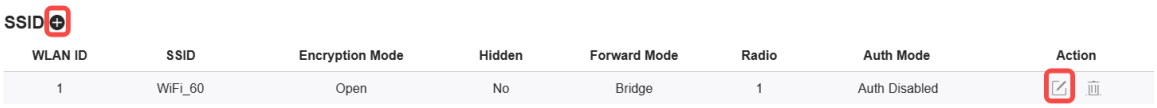
Parameter	Description
Mask Opacity	
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

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

2. Enabling Voucher Authentication for an SSID

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **SSID**, and select a network that needs to configure wireless authentication.

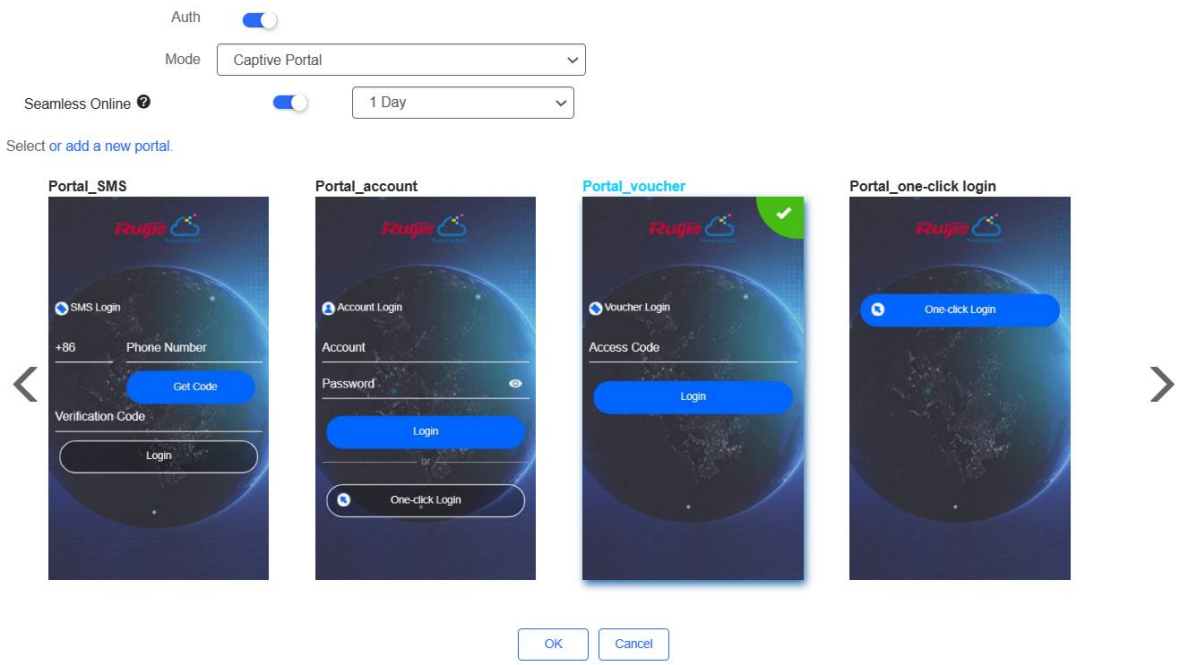
(2) If the SSID that needs to enable wireless authentication is not created, click to open the SSID configuration page. If the SSID that needs to enable wireless authentication is created, click in the **Action** column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.



(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

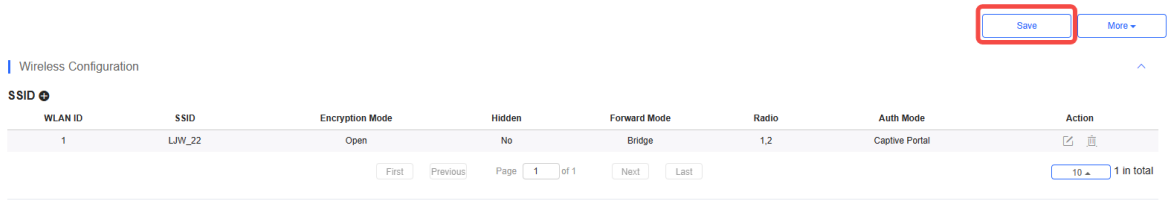
Note

When Encryption Mode is set to a value other than WPA2-Enterprise(802.1x), Auth is available and you can select whether to perform wireless authentication.



- **Mode**: Set it to **Captive Portal**.
- **Seamless Online**: Determine whether to enable **Seamless Online** as required, which is enabled by default. After **Seamless Online** is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- **Select or add a new portal**: Select a portal template with the authentication mode set to **Voucher**. If the configured template does not meet the requirements, click **or add a new portal** to create a portal template.

(4) Click **Save** for the configuration to take effect.

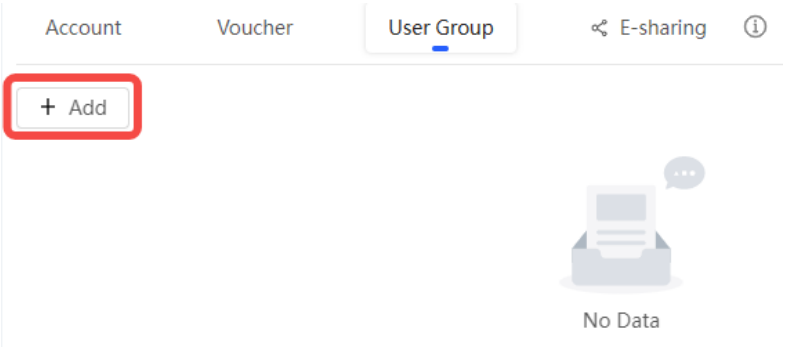


3. Adding a Voucher

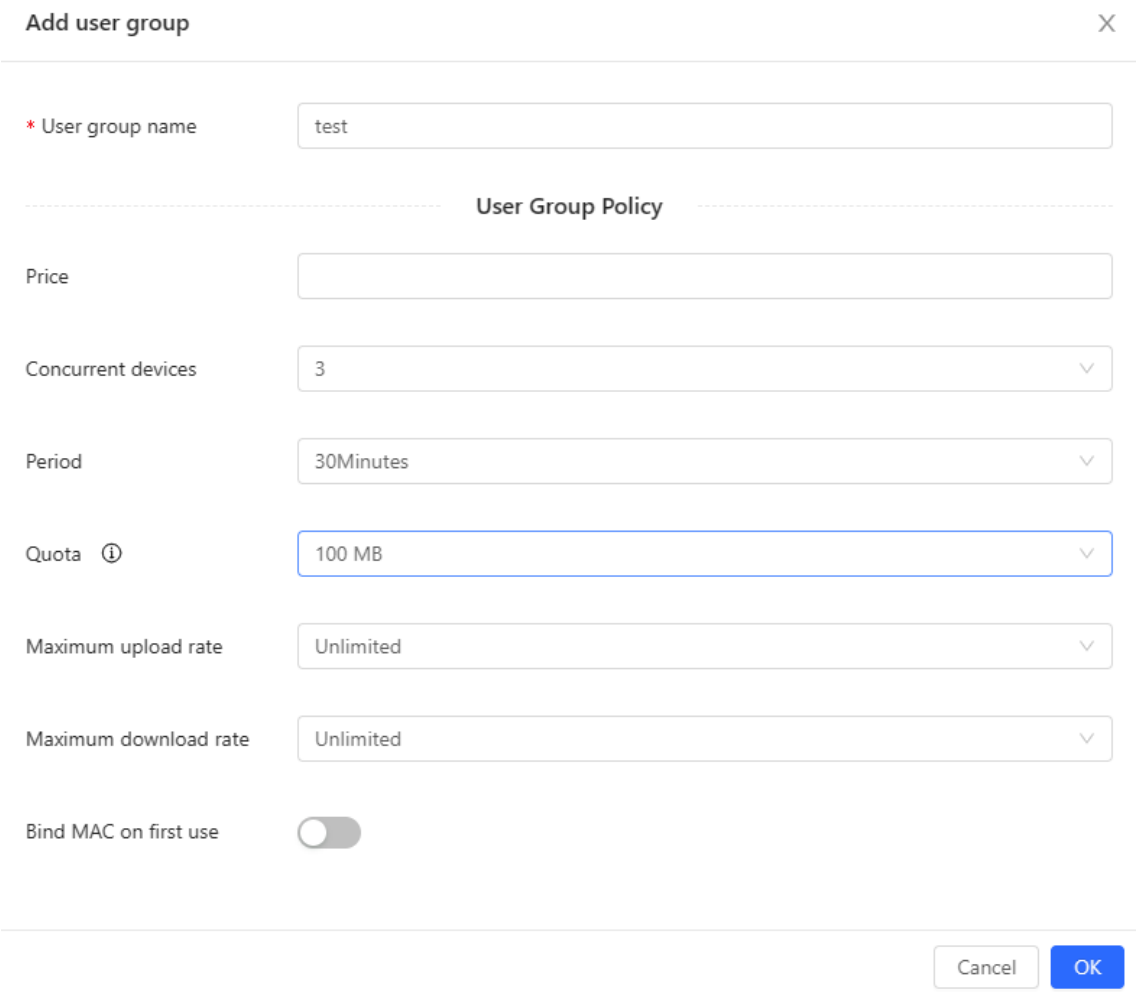
(1) Log in to Ruijie Cloud, choose **Project** > **Authentication** > **User Management**, **and** select a network in this account**.**

(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.

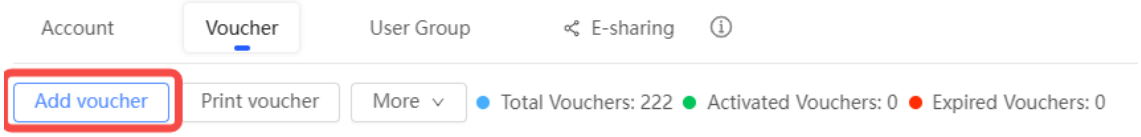
Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

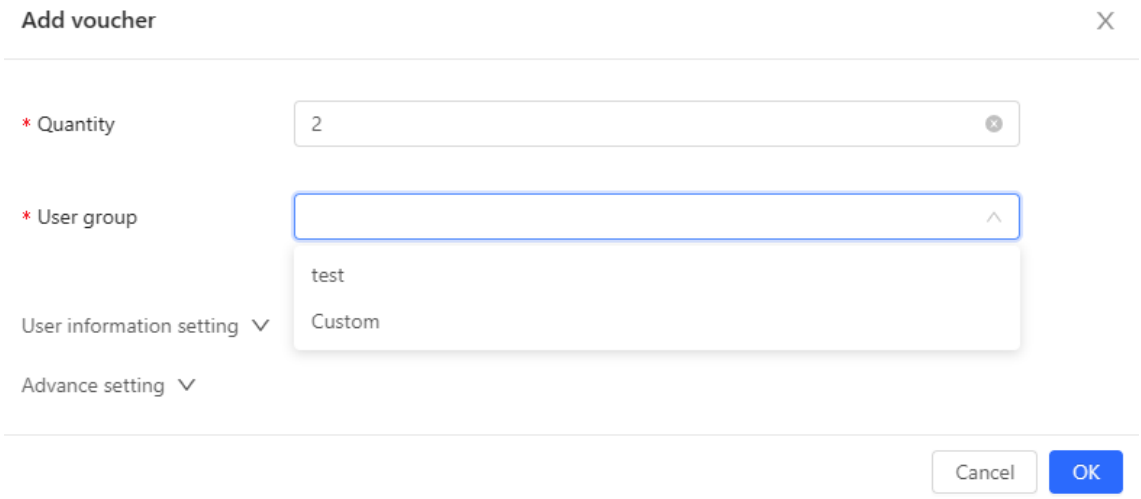
Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) Configure a voucher.

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



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



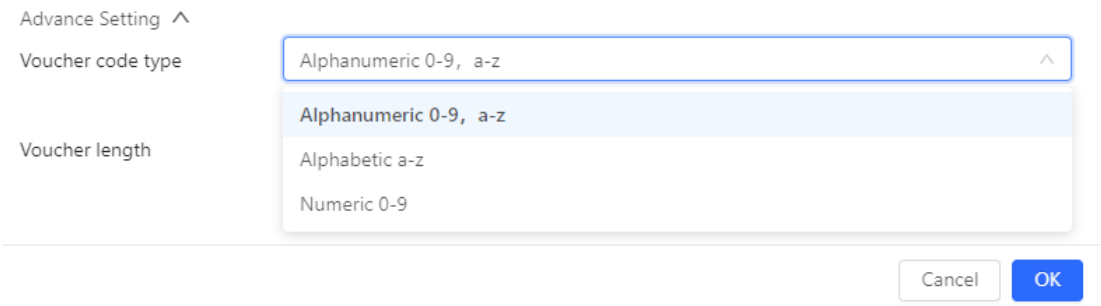
Quantity: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the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

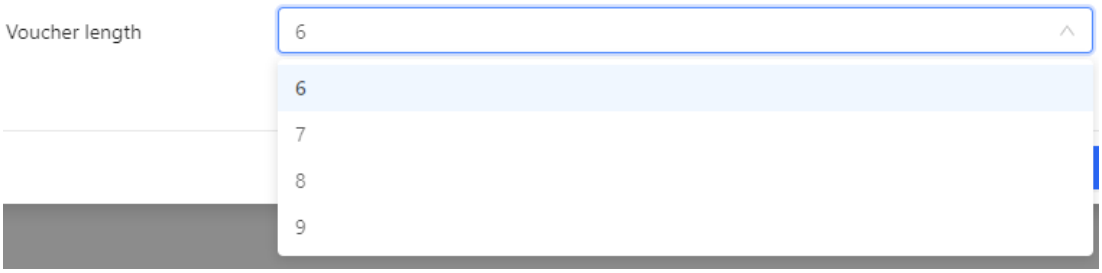
User information setting: Configure user information, which is optional.

Advance setting:

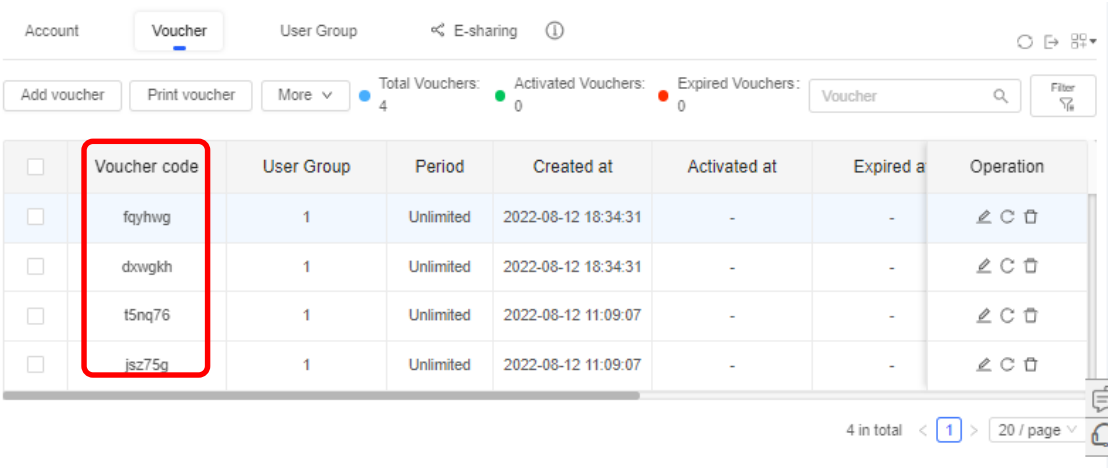
- **Voucher code type**: Set the value to Alphanumeric 0-9, a-z, Alphabetic a-z, or Numeric 0-9.



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



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

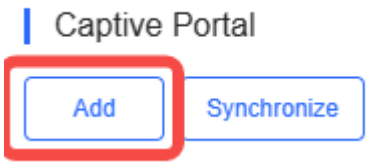


4.3.4 Configuring Account Authentication on Ruijie Cloud

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

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

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



(3) Configure basic information of the portal template.

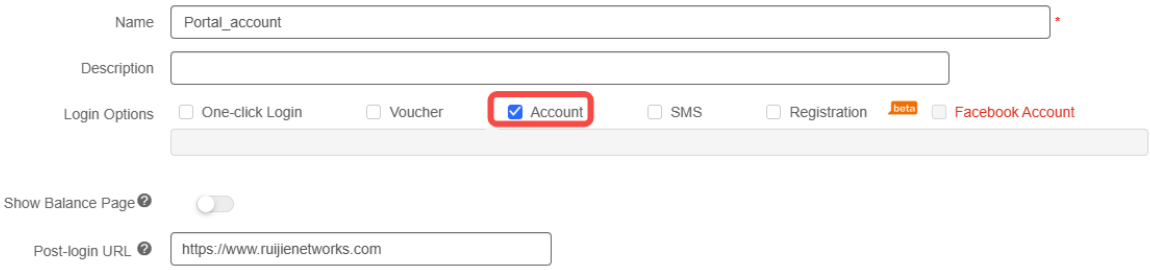


Table 4-9 Basic Information of the Portal Template

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

(4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

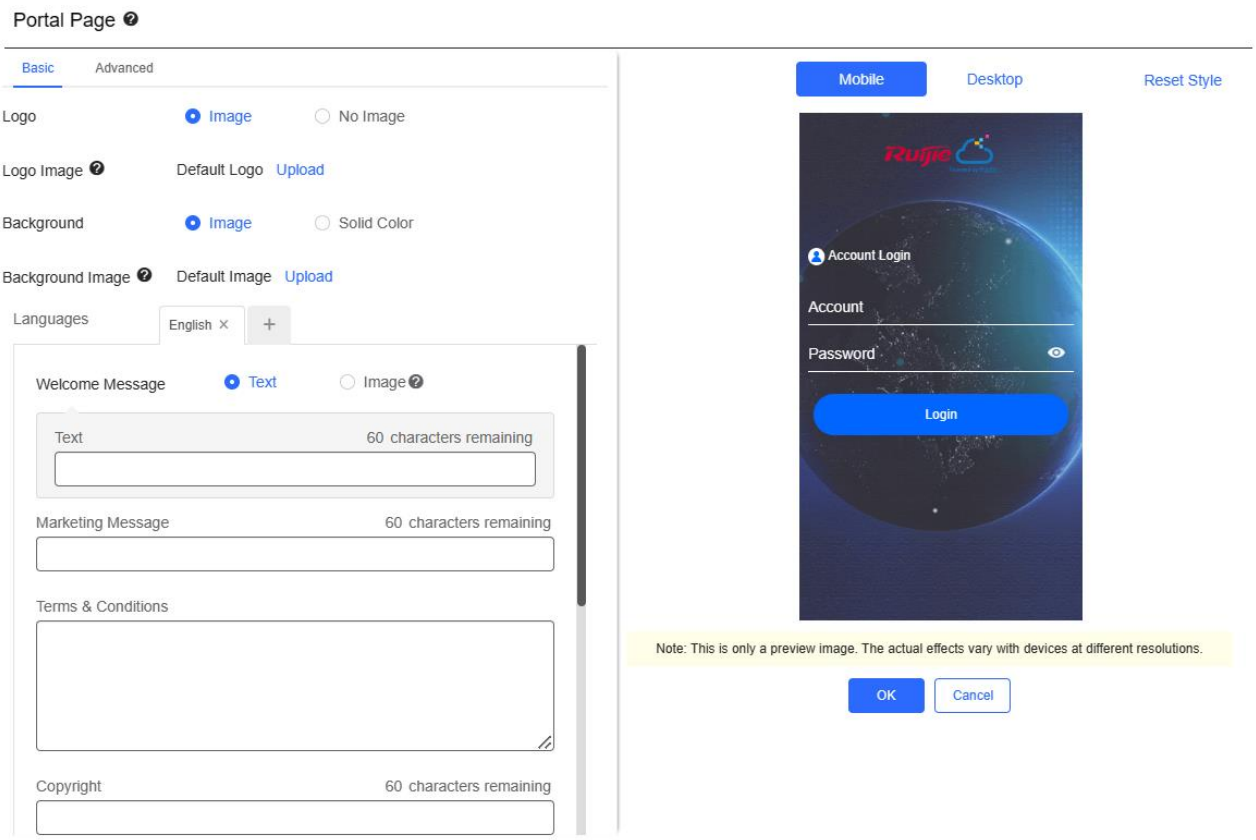
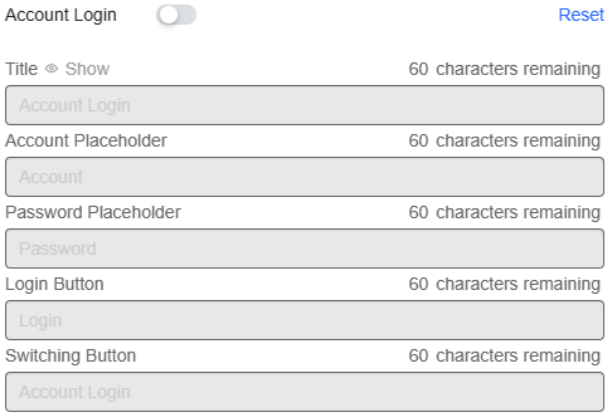


Table 4-10 Basic Information of the Portal Page

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
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 Color	When **Background** is set to **Solid Color**, configure the background color. The default value is **#ffffff**.
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.

Parameter	Description
	● Copyright: Enter the copyright. ● Account Login: After **Account Login** is enabled, you can customize the names of the controls related to account authentication. 

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.

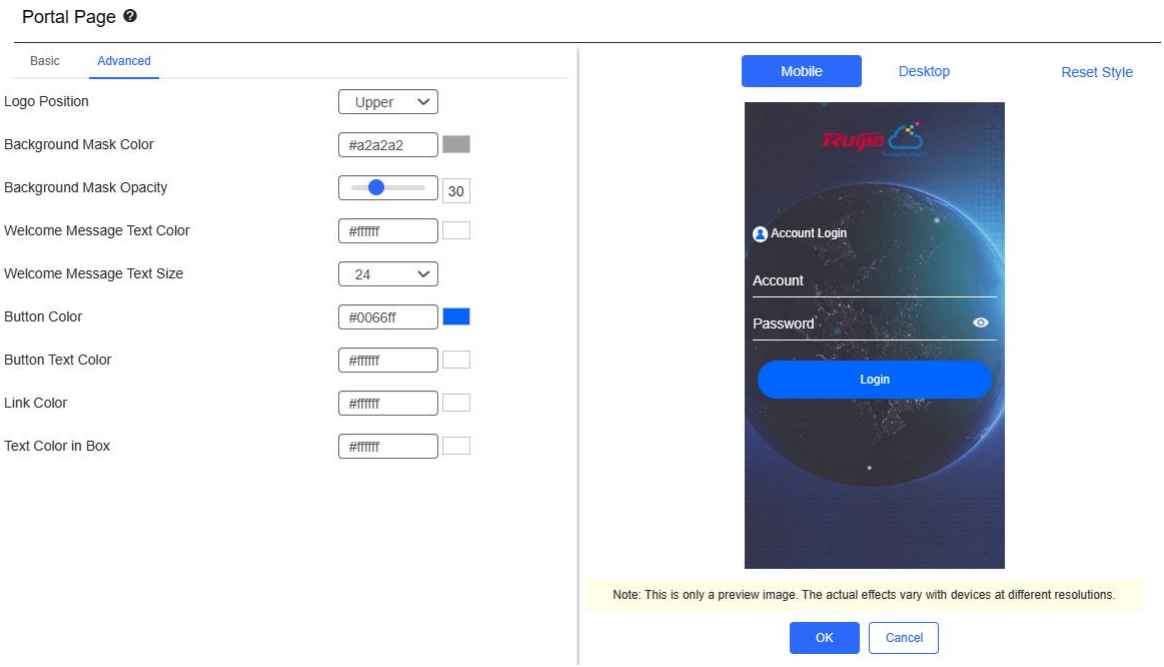


Table 4-11 Advanced Information of the Portal Page

Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background mask color. The default value is

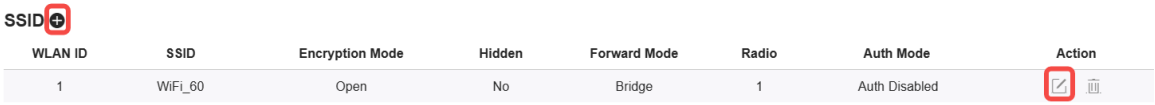
Parameter	Description
Mask Color	#a2a2a2.
Background Mask Opacity	Select the background mask opacity (0-100).
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

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

2. Enabling Account Authentication for an SSID

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **SSID**, and select a network that needs to configure wireless authentication.

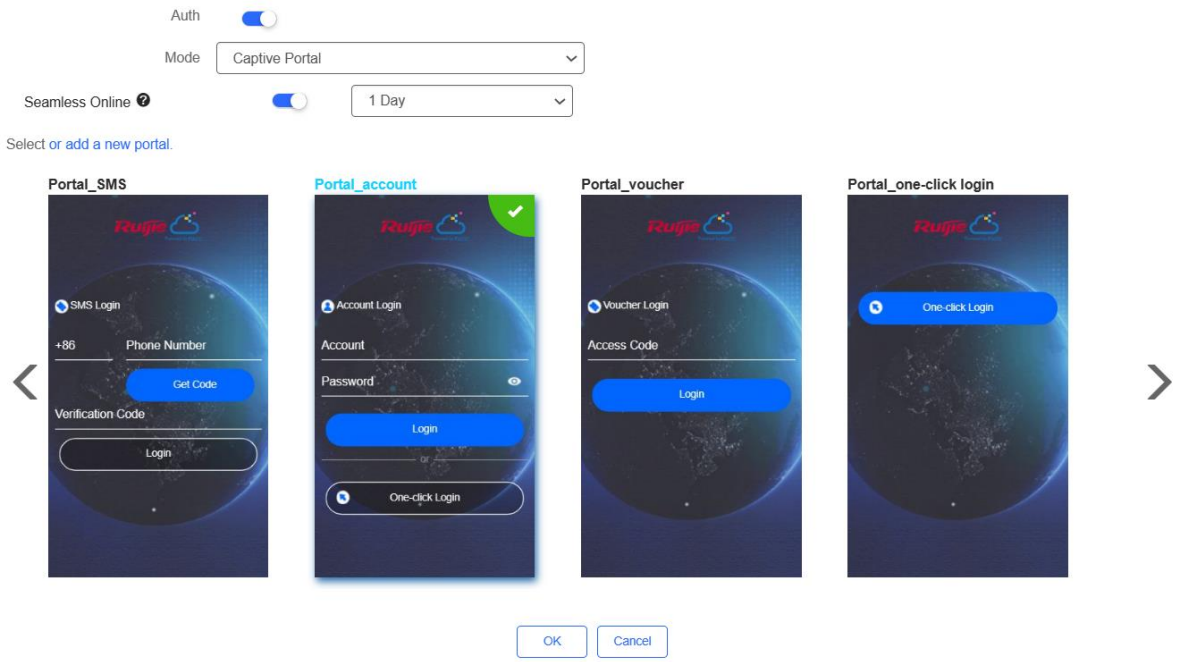
(2) If the SSID that needs to enable wireless authentication is not created, click to open the SSID configuration page. If the SSID that needs to enable wireless authentication is created, click in the **Action** column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.



(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

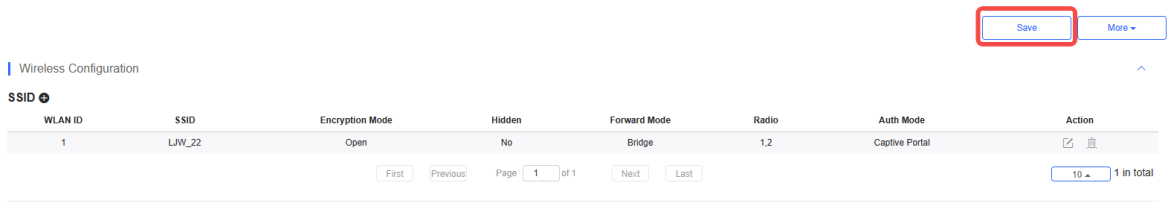
Note

When Encryption Mode is set to a value other than WPA2-Enterprise(802.1x), Auth is available and you can select whether to perform wireless authentication.



- **Mode**: Set it to **Captive Portal**.
- **Seamless Online**: Determine whether to enable **Seamless Online** as required, which is enabled by default. After **Seamless Online** is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- **Select or add a new portal**: Select a portal template with the authentication mode set to **Account**. If the configured template does not meet the requirements, click **or add a new portal** to create a portal template.

(4) Click **Save** for the configuration to take effect.

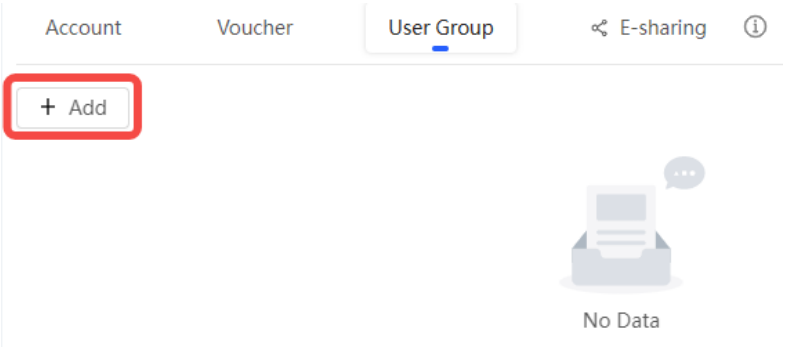


3. Adding an Account

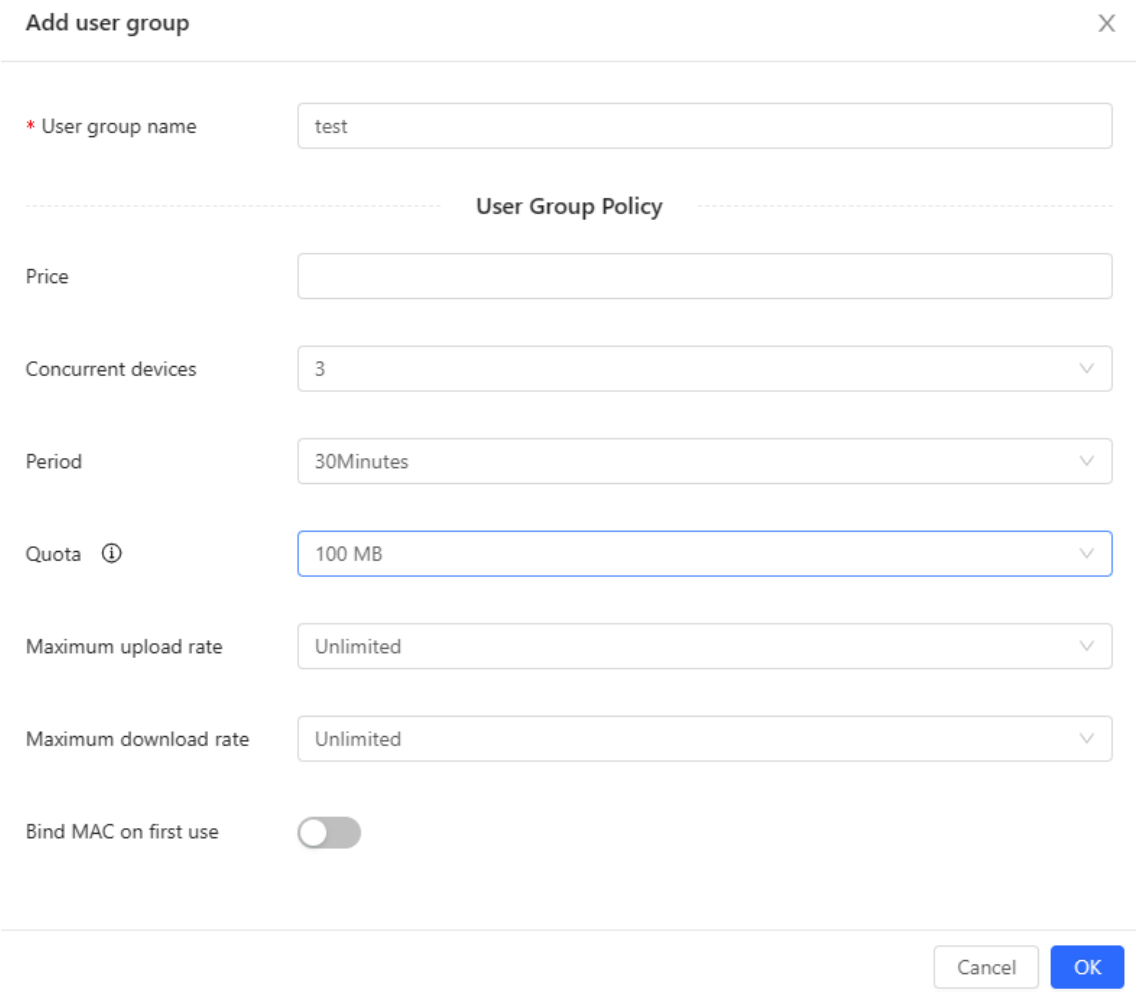
(1) Log in to Ruijie Cloud, choose **Project** > **Authentication** > **User Management**, **and** select a network in this account**.**

(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.

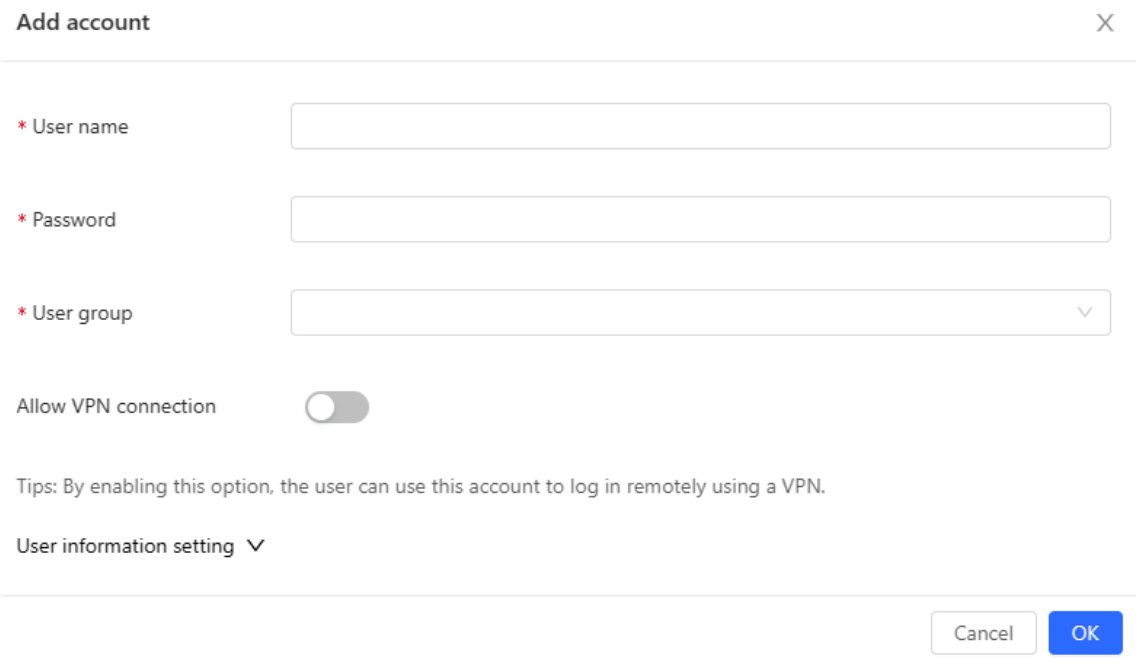
Maximum download rate: indicates the maximum download rate.

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.

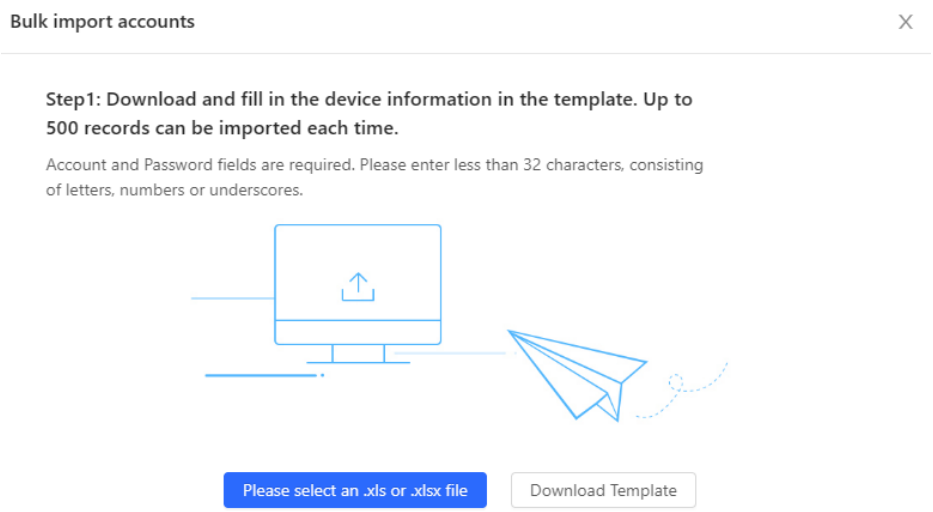
User group: **Select a created user group from the drop-down list. If the created user group does not meet the requirements, click Custom to create a user group.**

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.

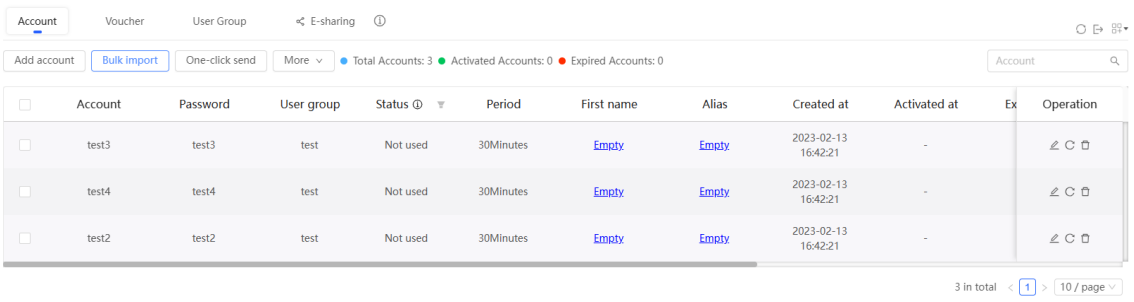
c Edit the template and save it.

Note

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

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

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



4.3.5 Configuring SMS Authentication on Ruijie Cloud

1. Adding a Twilio Account

Prerequisites

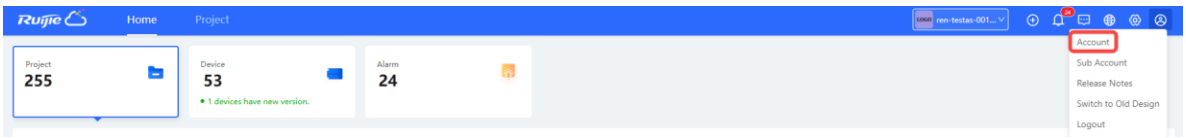
A Twilio account has been applied for from the Twilio official website (https://www.twilio.com/login).

Note

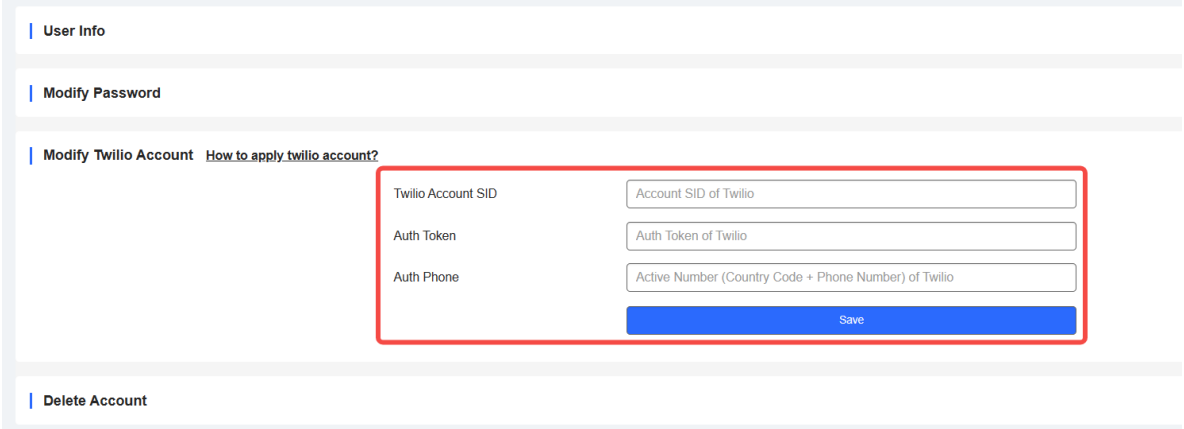
A Twilio account is used to send the SMS verification code.

Configuration Steps

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



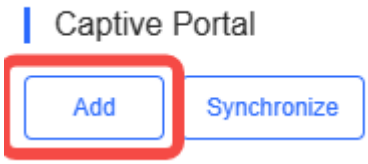
(2) Add Twilio account information and click **Save**.



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

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

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



(3) Configure basic information of the portal template.

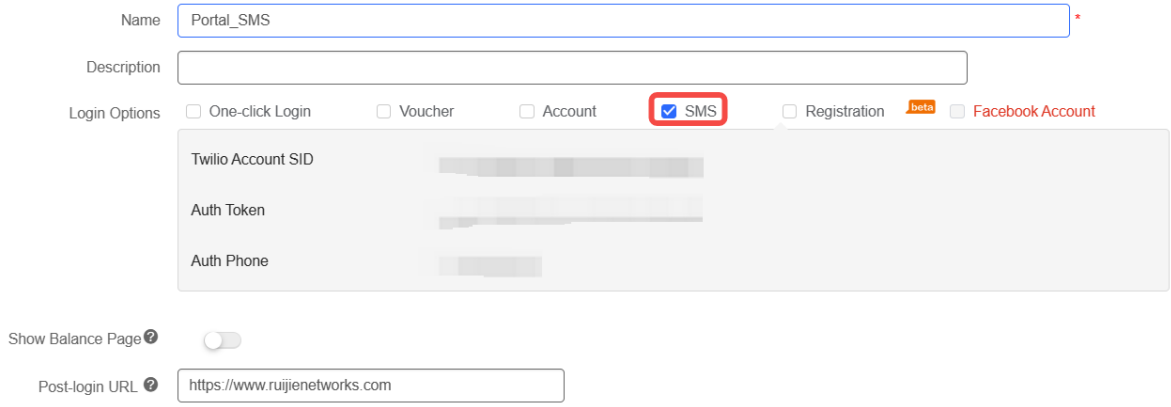


Table 4-12 Basic Information of the Portal Template

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

(4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

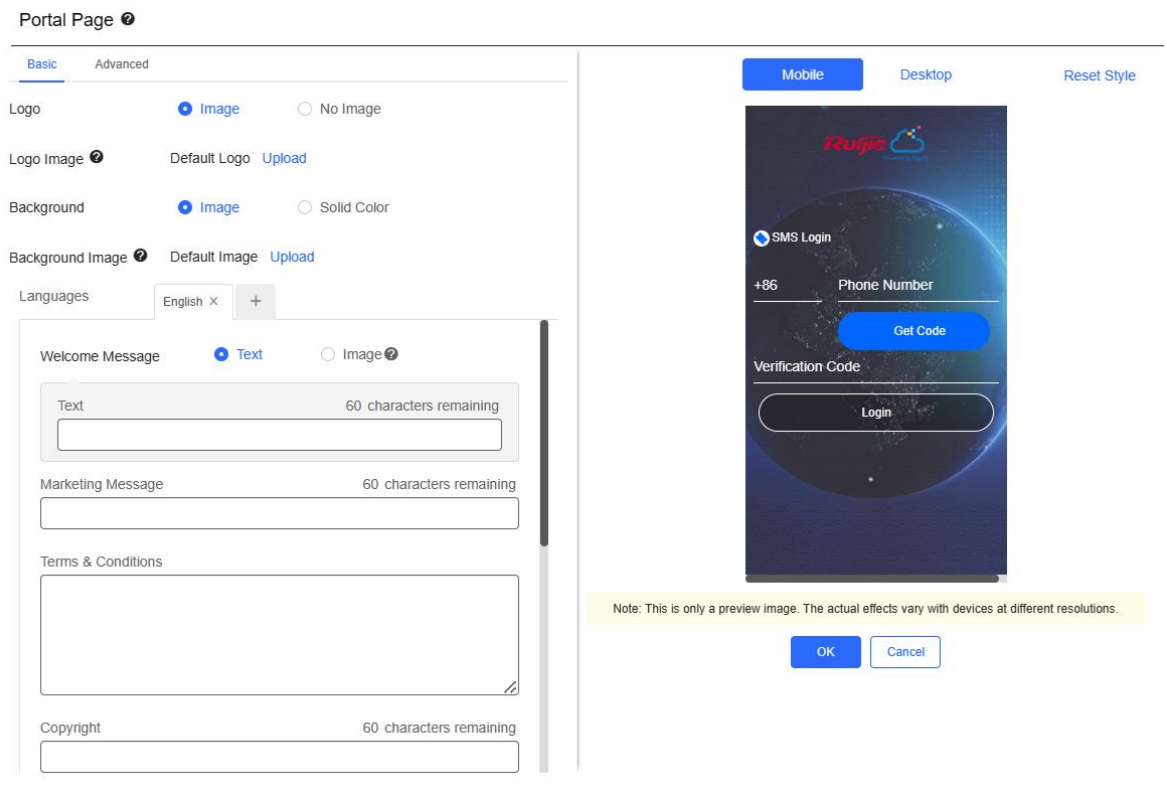
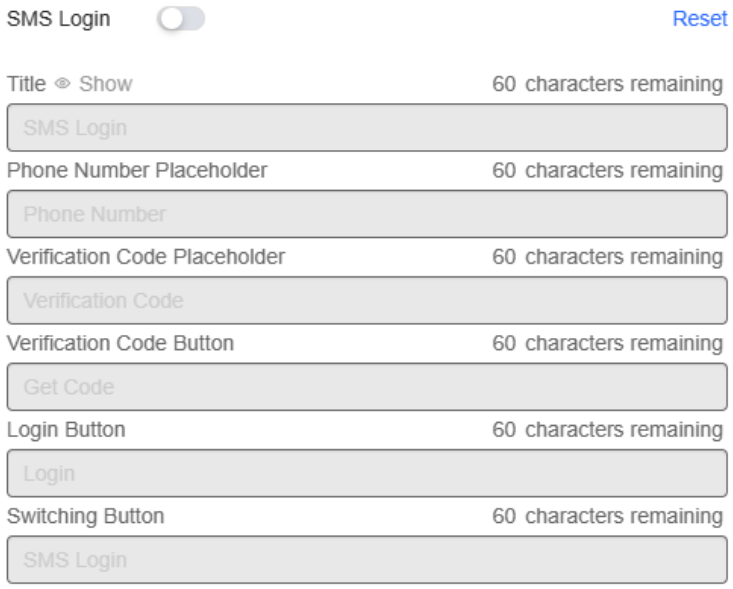


Table 4-13 Basic Information of the Portal Page

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
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 Color	When **Background** is set to **Solid Color**, configure the background color. The default value is **#ffffff**.
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.

Parameter	Description
	● SMS Login: After **SMS Login** is enabled, you can customize the names of the controls related to SMS authentication. 

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.

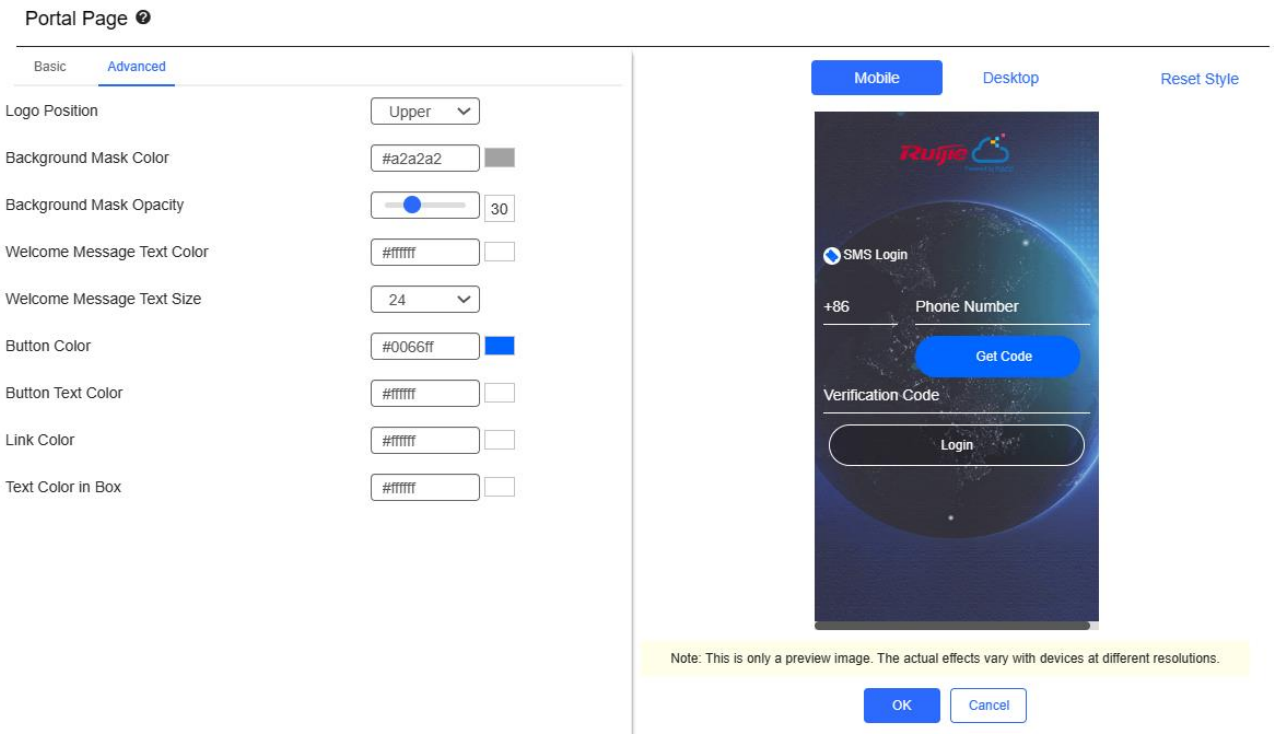


Table 4-14 Advanced Information of the Portal Page

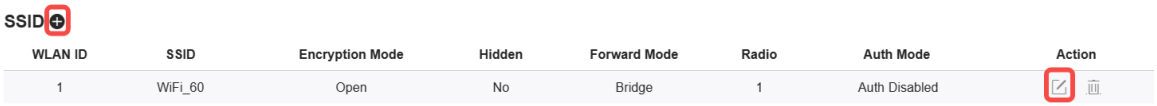
Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background Mask Color	Select the background mask color. The default value is #a2a2a2.
Background Mask Opacity	Select the background mask opacity (0-100).
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

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

3. Enabling SMS Authentication for an SSID

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **SSID**, and select a network that needs to configure wireless authentication.

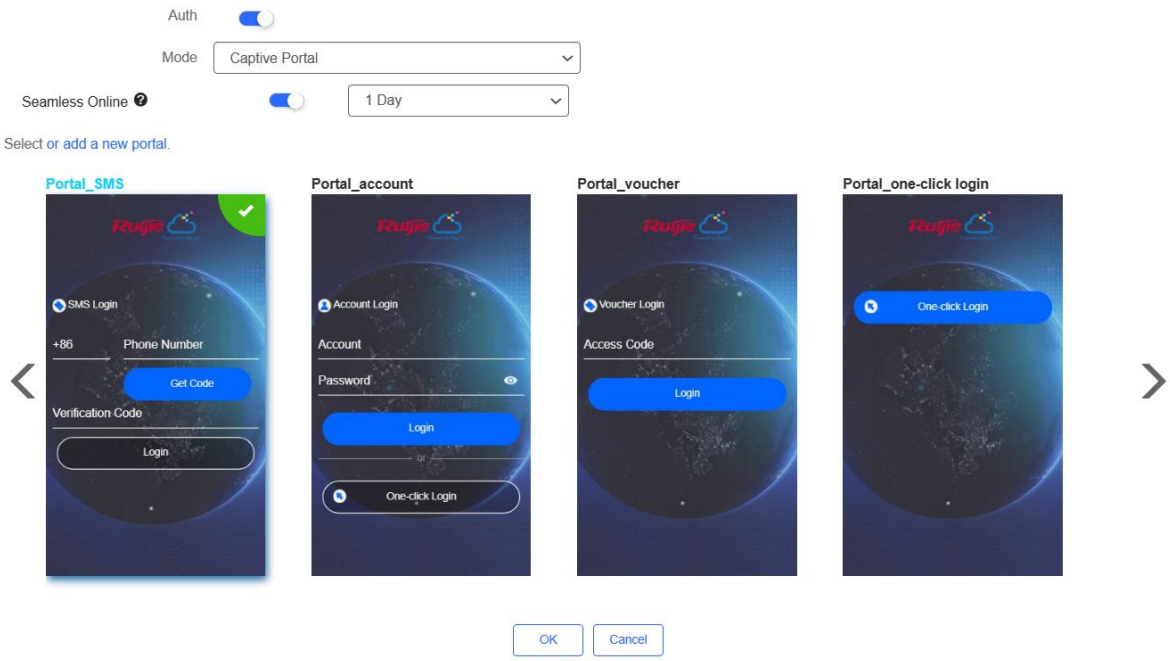
(2) If the SSID that needs to enable wireless authentication is not created, click to open the SSID configuration page. If the SSID that needs to enable wireless authentication is created, click in the **Action** column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.



(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

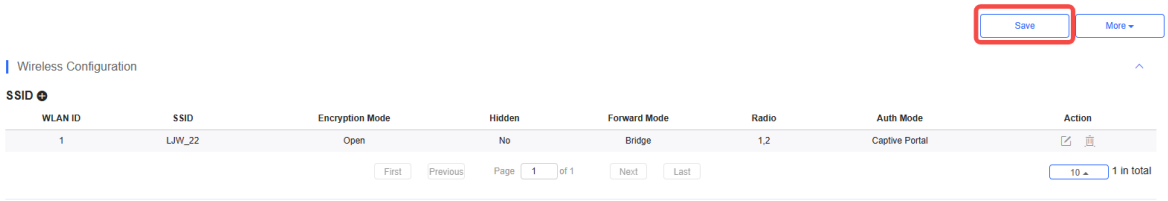
Note

When Encryption Mode is set to a value other than WPA2-Enterprise(802.1x), Auth is available and you can select whether to perform wireless authentication.



- **Mode**: Set it to **Captive Portal**.
- **Seamless Online**: Determine whether to enable **Seamless Online** as required, which is enabled by default. After **Seamless Online** is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- **Select or add a new portal**: Select a portal template with the authentication mode set to **SMS**. If the configured template does not meet the requirements, click **or add a new portal** to create a portal template.

(4) Click **Save** for the configuration to take effect.



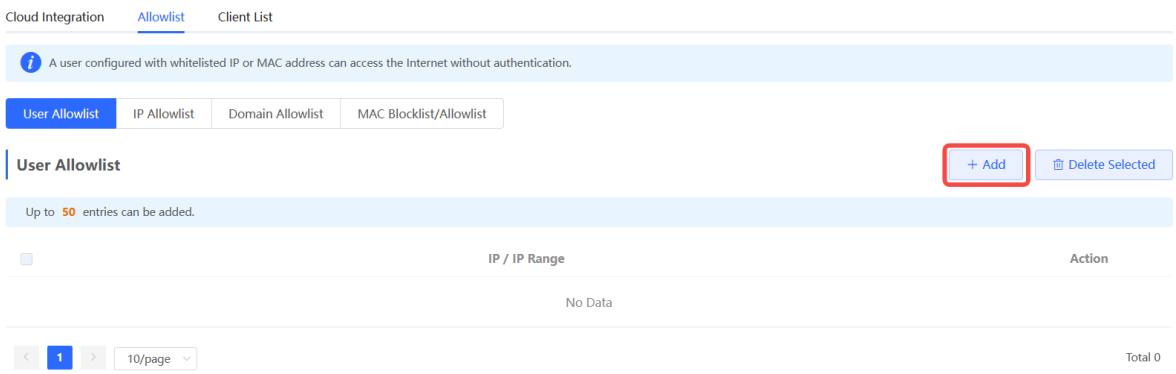
4.3.6 Configuring an Authentication-Free User List on Eweb Management System

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

1. Configuring an Authentication-Free User

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

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

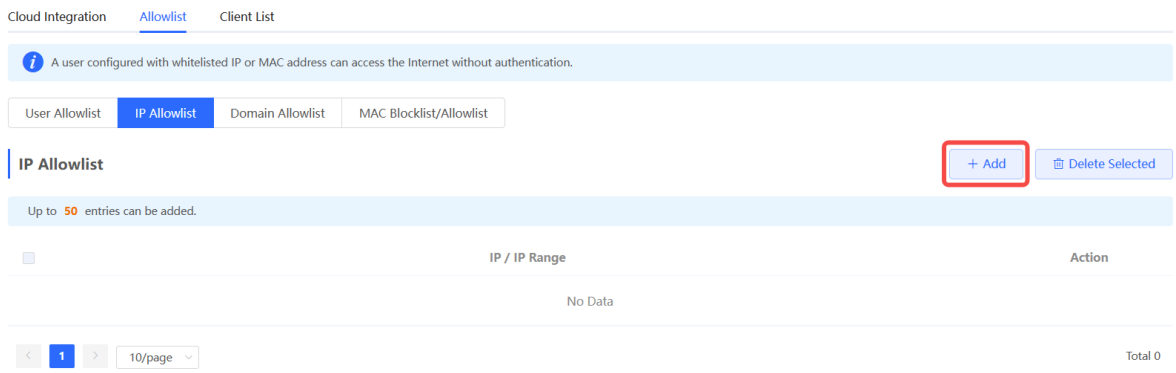


(3) Configure an STA IP address or IP address range. After the configuration, click **OK** to save the configurations.

2. Configuring an Authentication-Free Public IP Address

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

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

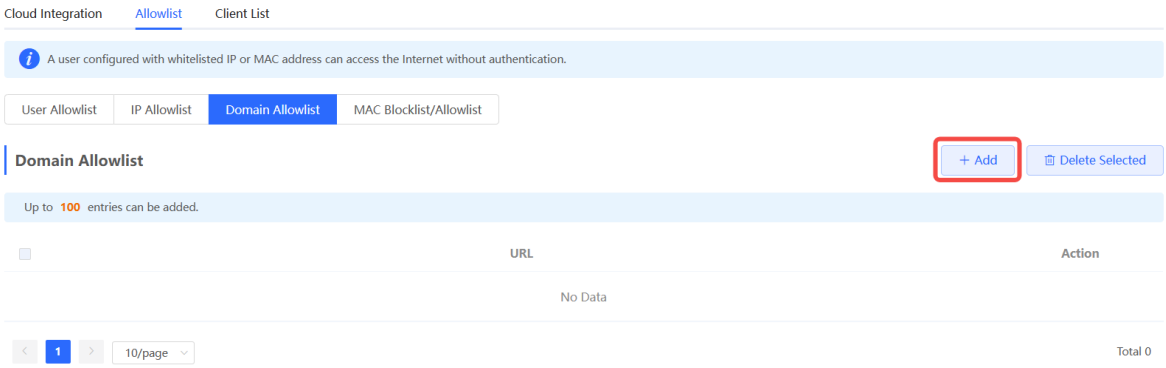


(3) Configure a public IP address or public IP address range. After the configuration, click **OK** to save the configurations.

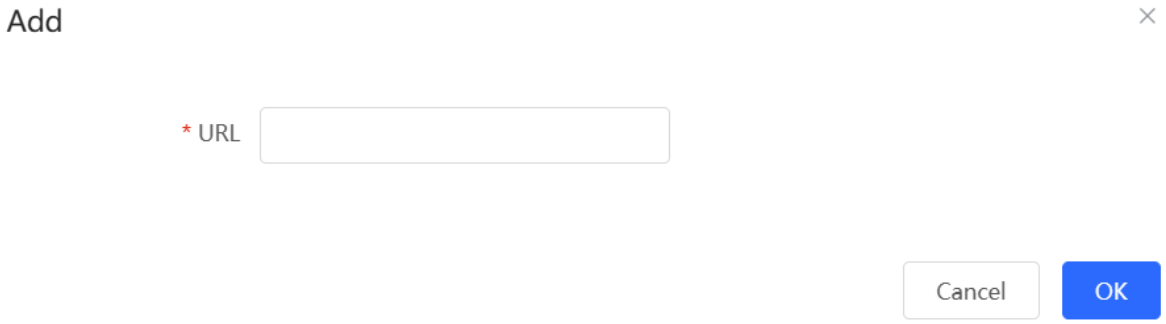
3. Configuring a Domain Name Allowlist

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

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



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

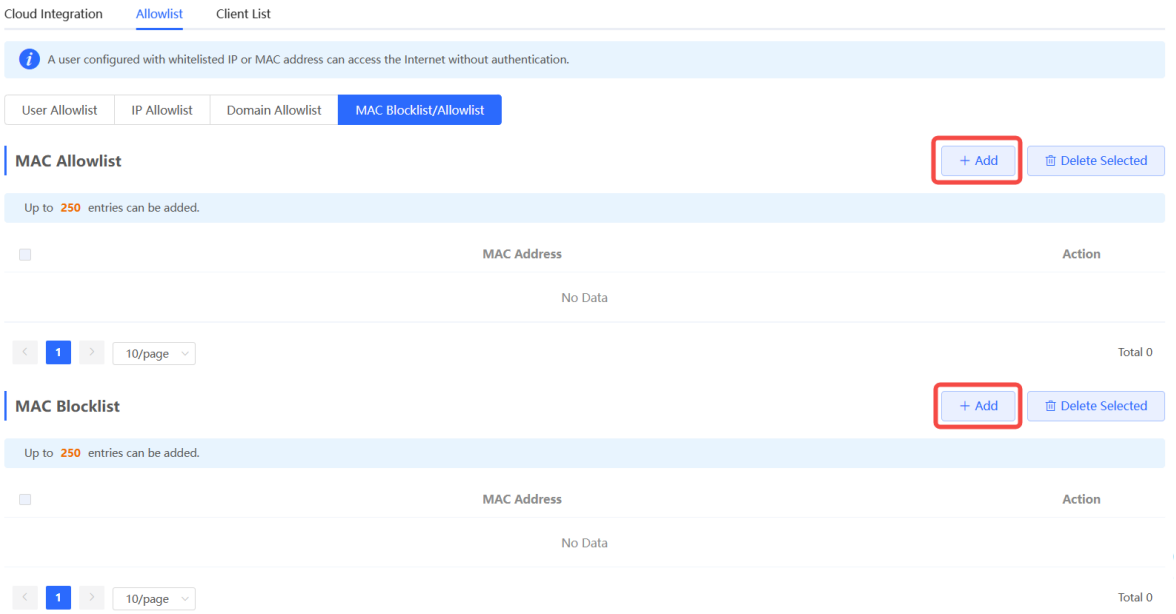


4. Configuring a MAC Address Allowlist and Blocklist

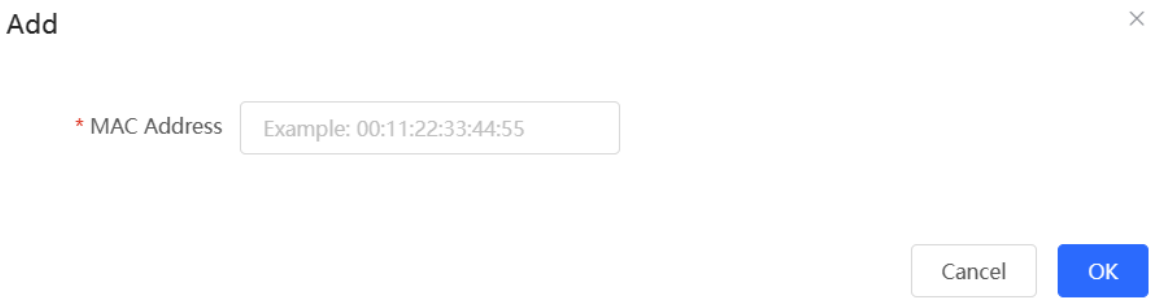
STAs whose MAC addresses are added to the MAC address allowlist can access the network without authentication, and STAs whose MAC addresses are added to the MAC address blocklist are forbidden to access the network.

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

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



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

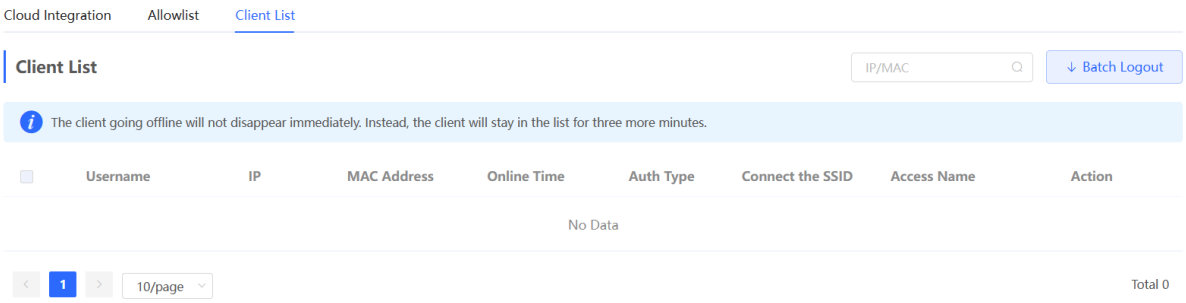


4.3.7 Displaying Authenticated Users on Eweb Management System

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

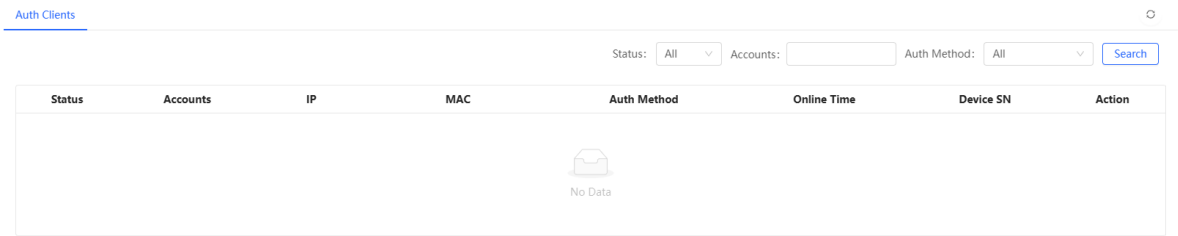
Note

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



4.3.8 Displaying Authenticated Users on Ruijie Cloud

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



4.4 Configuring 802.1X Authentication

Caution

The functions mentioned in this chapter are supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260, and RG-RAP6262.

4.4.1 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.

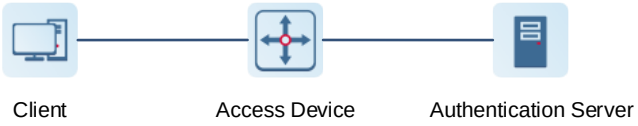
The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

- 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 4-1 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.

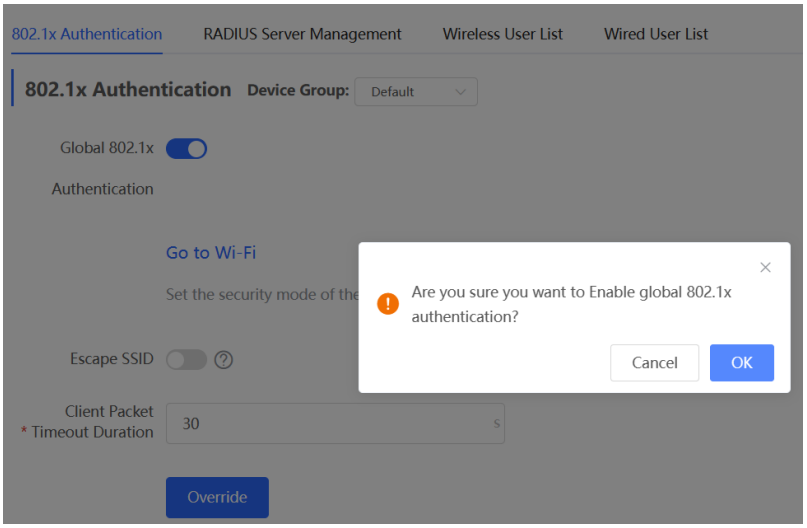
Note

The RG-RAP APs only support the authentication.

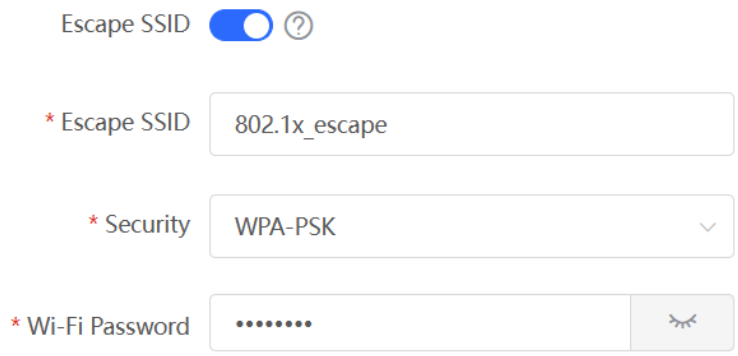
4.4.2 Configuring 802.1X Authentication

(1) To access the configuration page, perform the following operations: **In Network mode, choose Network > 802.1x Authentication.**

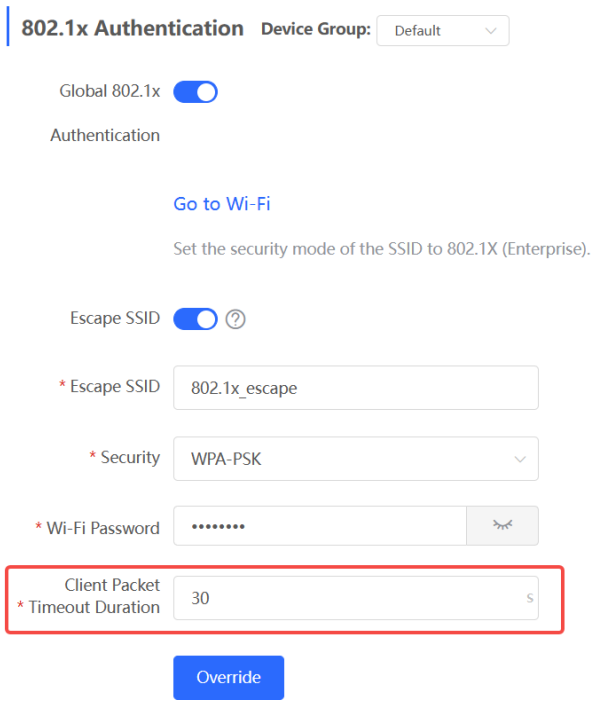
(2) Click **Global 802.1x.** A pop-up window is displayed. Click **OK**.



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.



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:

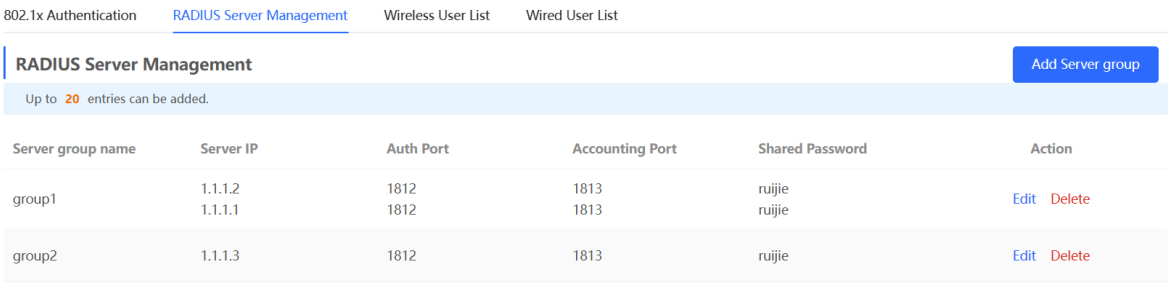
- The RADIUS server is ready and the following configurations have been completed.
  - A username and a password have been added for client login.
  - The firewall has been disabled. Otherwise, authentication messages may be blocked, leading to authentication failure.
  - The IP address of the device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

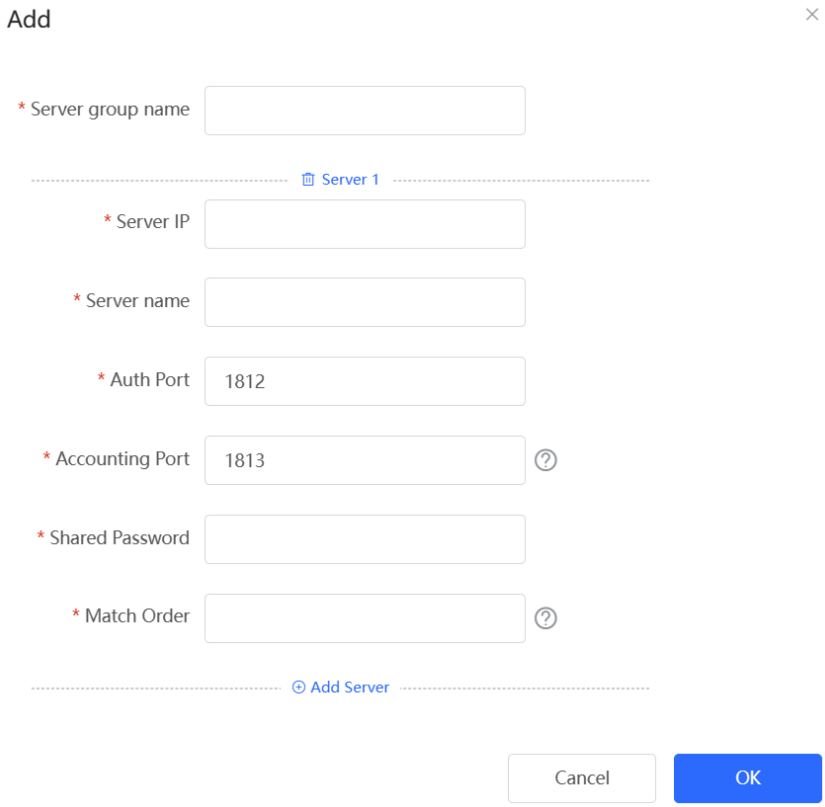


Table 4-15 Server Group Parameters

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.
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**.

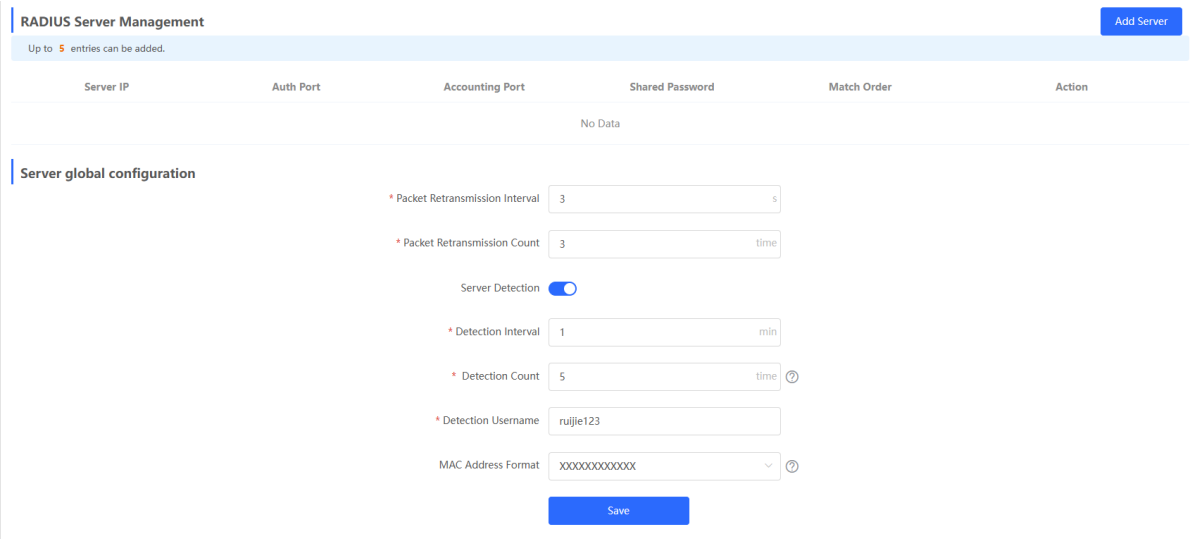


Table 4-16 Server Global Configuration Parameters

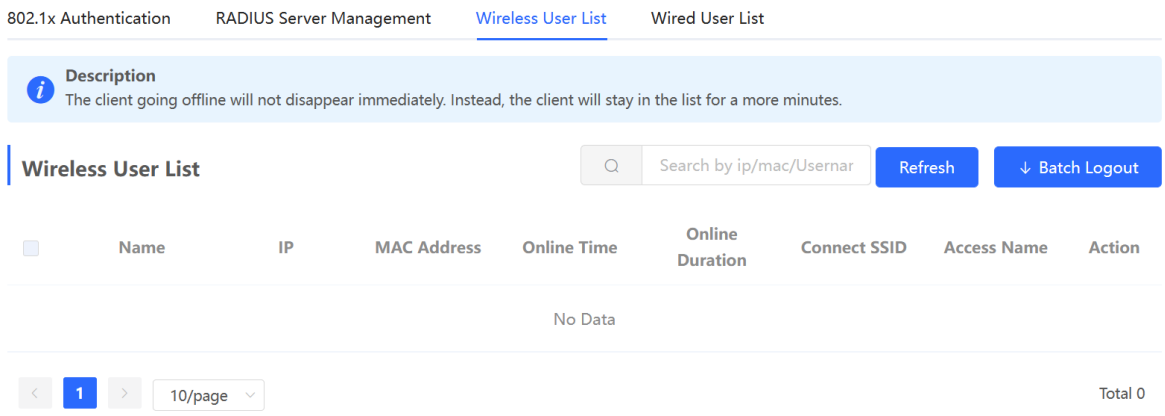
Parameter	Description
Packet Retransmission Interval	Configure the interval during which the device sends a request to a RADIUS server before confirming that the RADIUS server is unreachable.
Packet Retransmission	Configure the number of times that the device sends requests to a RADIUS server before confirming that the

Parameter	Description
Count	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

4.4.3 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**.

To access the configuration page, perform the following operations: **In Network mode, choose Network > 802.1x Authentication > Wireless User List.**



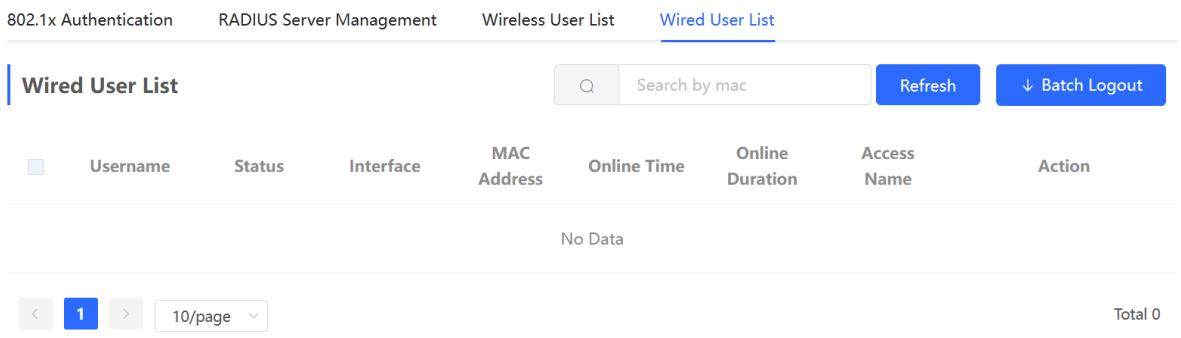
Click **Refresh** to view the latest user list.

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.

4.4.4 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**.

In Network mode, choose Network > 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.

4.5 Advanced Configuration

4.5.1 ARP List

Note

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

ARP List displays the mapping relationship between IP addresses and MAC addresses.

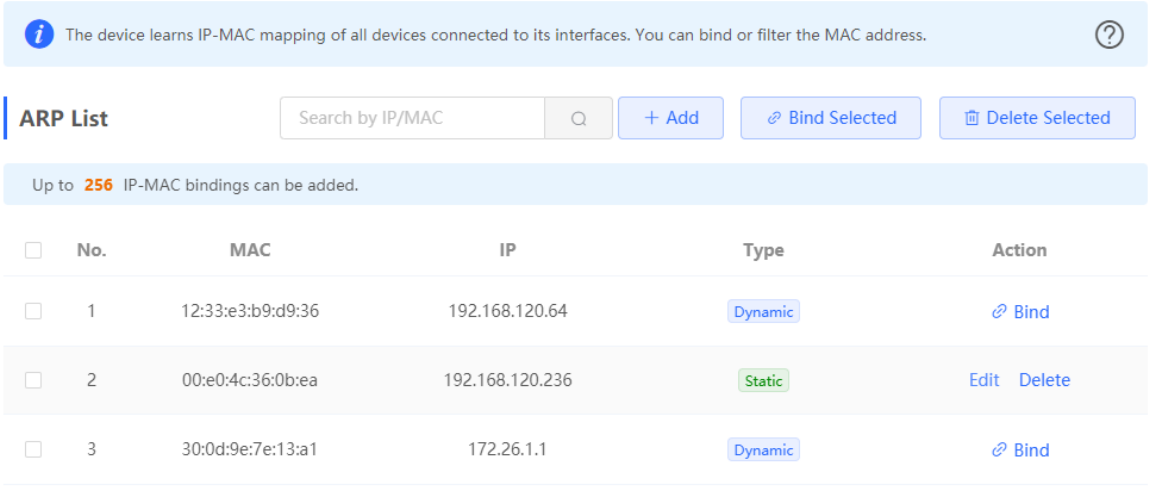
The device learns the IP and MAC addresses of network devices connected to ports of the device and generates ARP entries. You can bind ARP mappings to improve network security.

- In SON mode, select **Local Device** and choose **Advanced** > **Local DNS**.
- In standalone mode, choose **Advanced** > **Local DNS**.

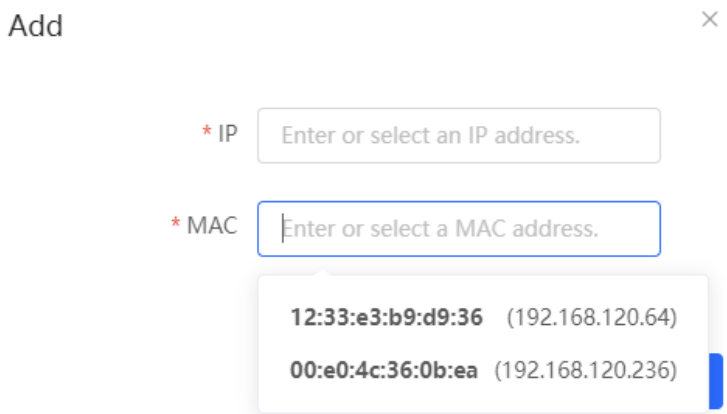
In **Local Device** mode, choose **Security** > **ARP List**.

ARP mappings can be bound in two ways:

- 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.



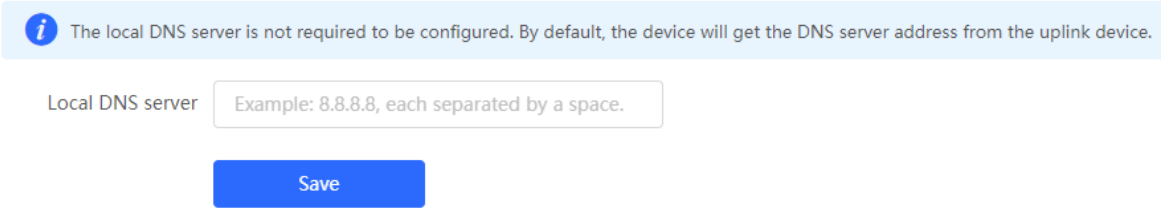
- Click **Add**, enter the IP address and MAC address to be bound, and click **OK**. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the address mapping.



4.5.2 Local DNS

- In SON mode, select **Local Device** and choose **Advanced** > **Local DNS**.
- In standalone mode, choose **Advanced** > **Local DNS**.

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



4.5.3 PoE Configuration

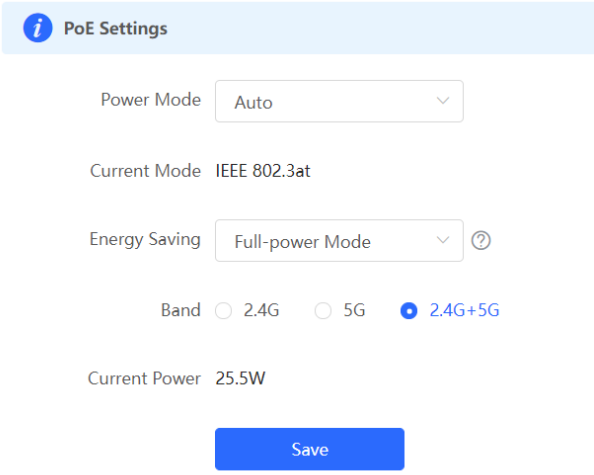
Note

Only some devices support this function.

The **PoE Settings** page allows you to configure the PoE mode.

- In SON mode, select **Local Device** mode and choose **Advanced** > **PoE Settings**.
- In standalone mode, choose **Advanced** > **PoE Settings**.

Set parameters on the **PoE Settings** page and click **Save**.



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

Current Mode: indicates the current PoE mode.

Energy Saving: indicates the energy saving mode. In rate-limiting mode, the device is rate-limited. In flow-limiting mode, the spatial stream in each band is halved.

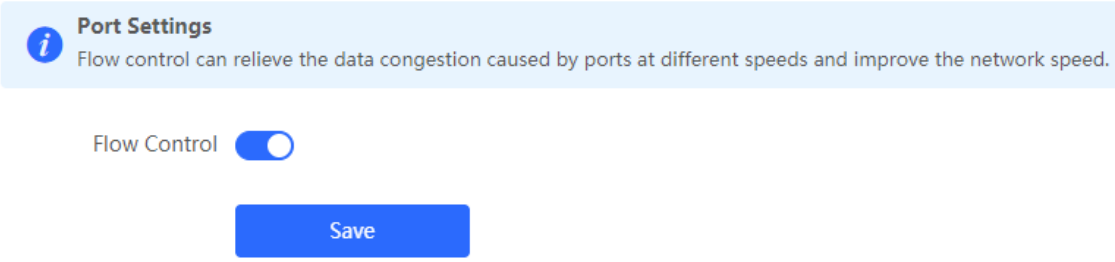
Band: indicates the band type.

Current Power: indicates the current power.

4.5.4 Port Flow Control Configuration

- In SON mode, select **Local Device** mode and choose **Advanced** > **Port Settings**.
- In standalone mode, choose **Advanced** > **Port Settings**.

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



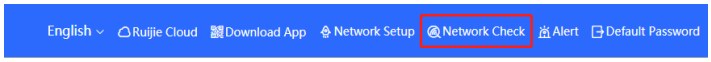
4.6 Operation and Maintenance

4.6.1 Network Check

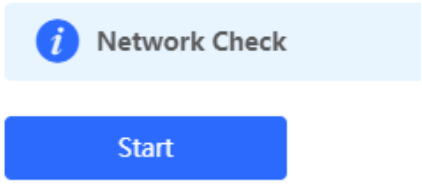
When a network error occurs, perform **Network Check** to identify the fault and take the suggested action.

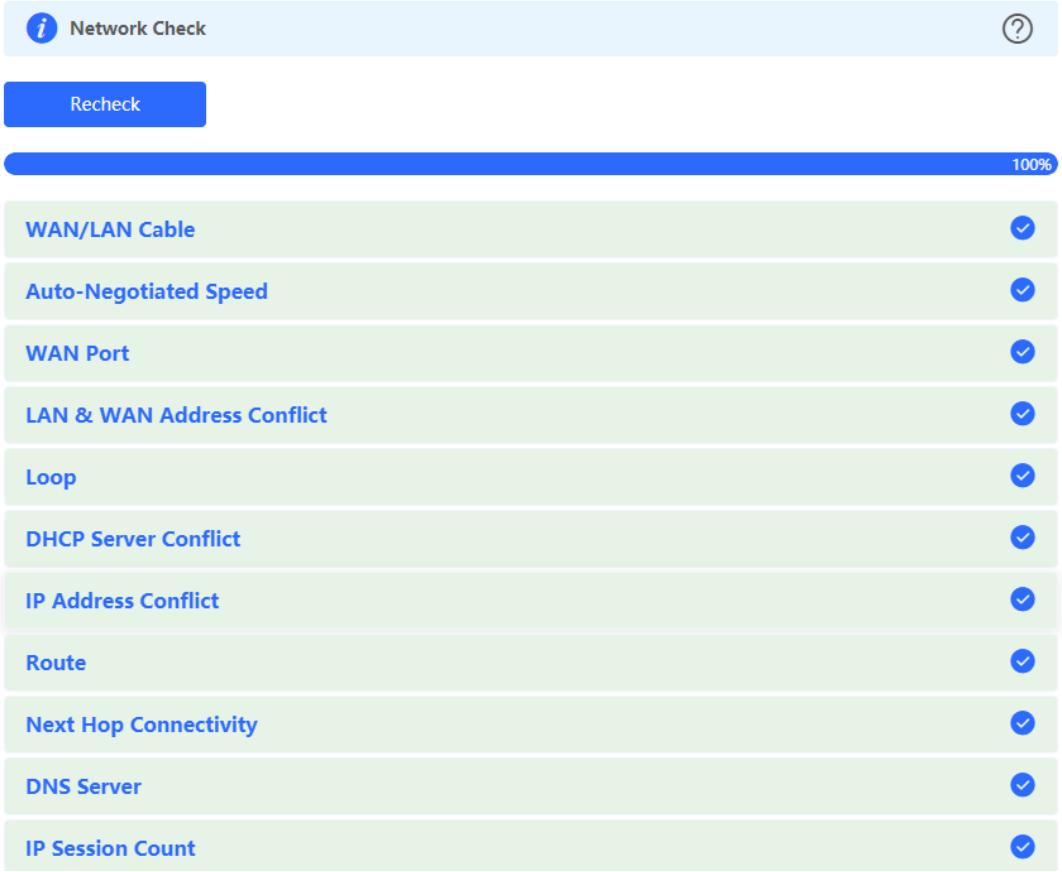
(1) Go to the **Network Check** page.

- In SON mode, select **Local Device**. Then click  in the navigation bar or choose **Diagnostics** > **Network Check**.
- In standalone mode, click  in the navigation bar or choose **Diagnostics** > **Network Check**.

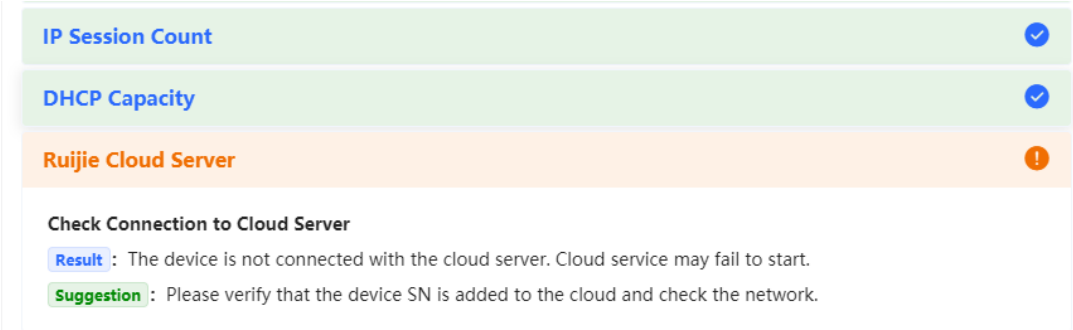


(2) Click **Start** to perform the network check and check the result.





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



4.6.2 Alarms

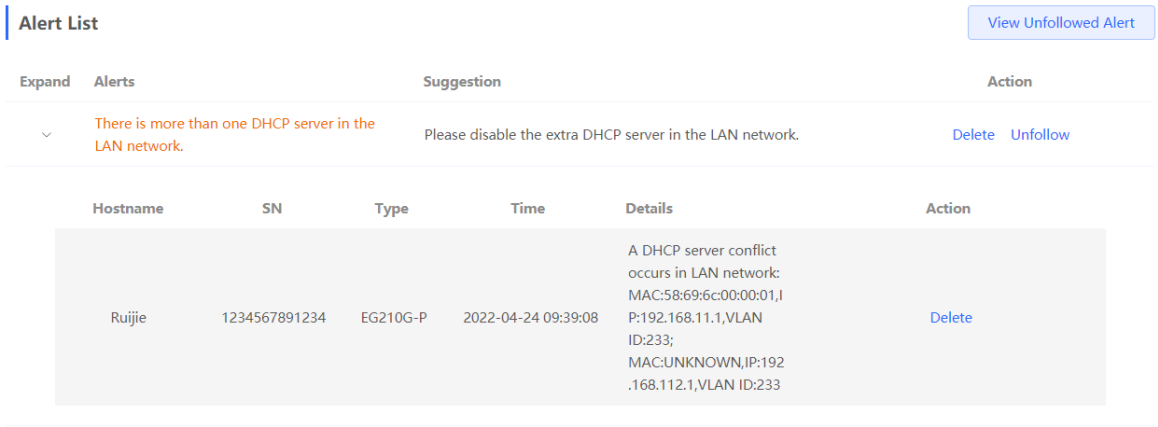
Choose **Network** (**Diagnostics**) > **Alerts**.

The **Alerts** page displays possible problems in the network environment and on the device. You can delete or unfollow alarms.

Note

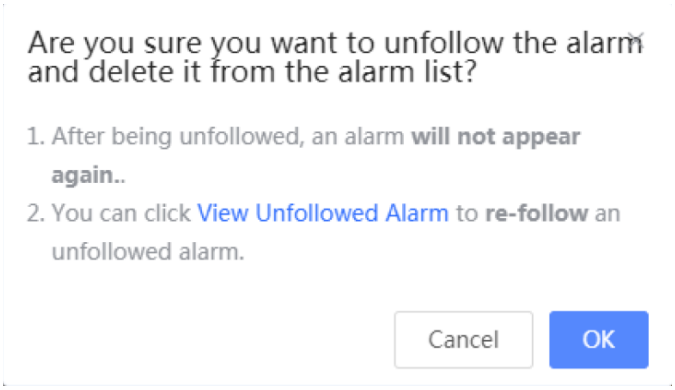
- After you click **Delete**, the alarm will reappear if the warning occurs. After clicking **Unfollow**, the alarm will never appear.
- When a type of alarms is unfollowed, the device will not discover and process all alarms of this type in a timely manner. Therefore, exercise caution when performing this operation.

All types of alarms are followed by default.



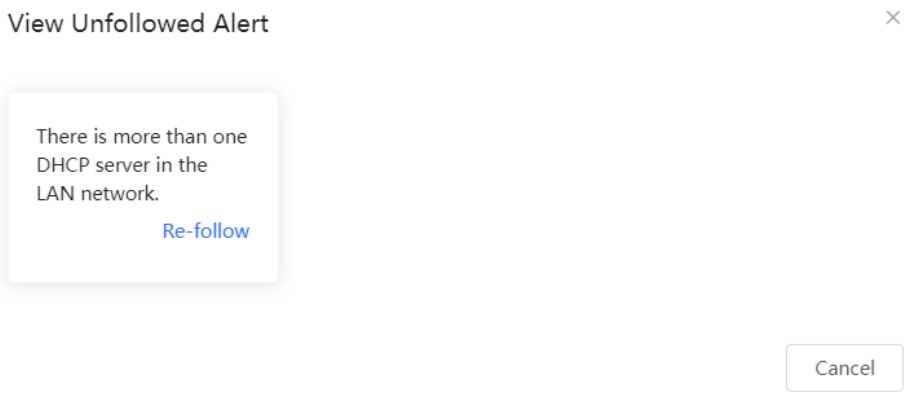
- Unfollow an alarm.

  Click **Unfollow** in the **Action** column. Then click **OK** in the displayed window to unfollow this type of alarms.



- Re-follow the alarm.

  Click **View Unfollowed Alert** to view the unfollowed alarm. Then click **Re-follow** to follow the alarm again in the displayed window.



4.6.3 Network Tools

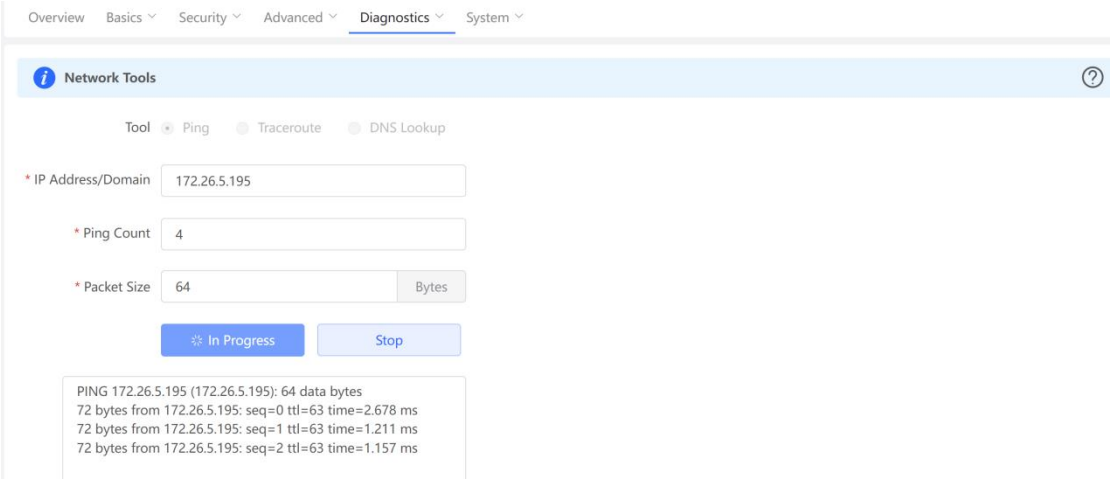
- In SON mode, select **Local Device** and choose **Diagnostics** > **Network Tools**.

- In standalone mode, choose **Diagnostics** > **Network Tools**.

Network tools includes **Ping**, **Traceroute**, and **DNS Lookup**.

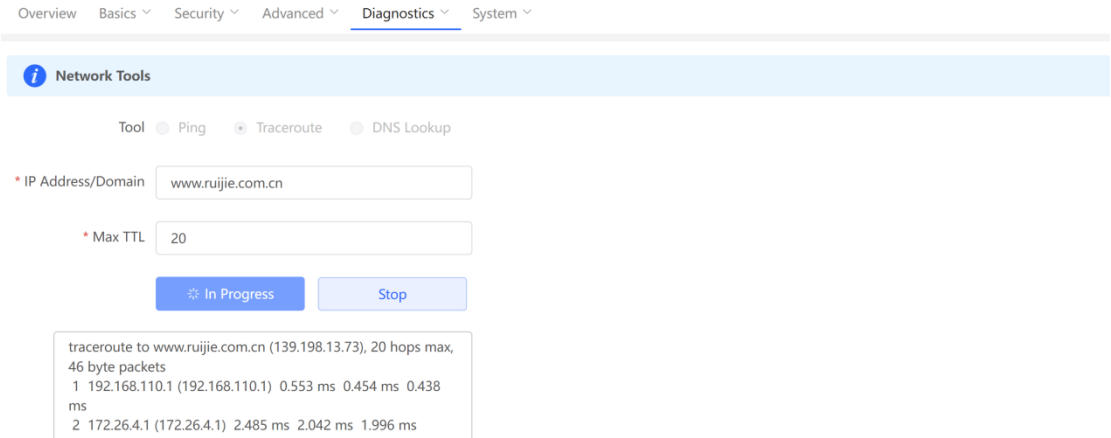
- **Ping**: Test whether the IP address or domain name is reachable.

  Enter the IP address or URL and click **Start** to test the connectivity between the AP and the IP address or URL. The message "Ping failed" indicates that the IP address or URL is inaccessible.



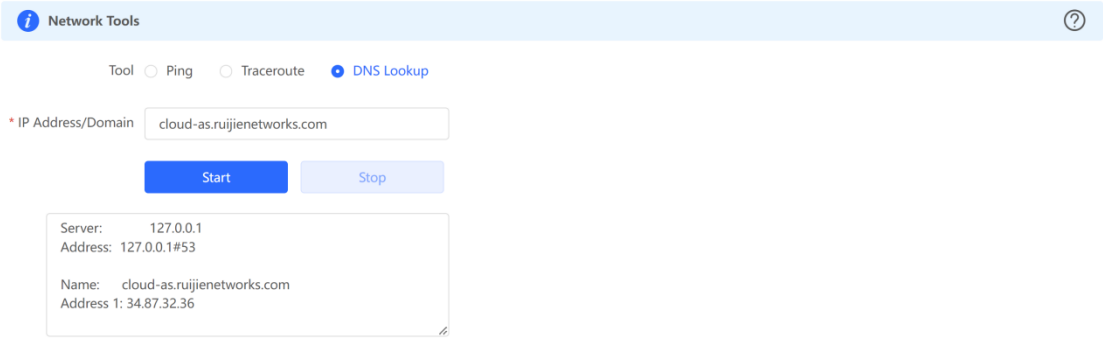
- **Traceroute**: Count the number of hops, displaying communication links from one point to another point and the time taken for each hop.

  Enter the IP address or URL, fill in **MAX TTL**, and click **Start** to display the network path to a specific IP address or URL.



- **DNS Lookup**: Display the DNS server address used to resolve a URL.

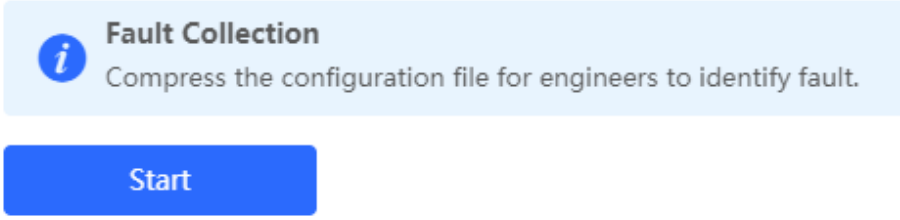
  Enter the IP address or URL and click **Start**.



4.6.4 Fault Collection

- In SON mode, select **Local Device** and choose **Diagnostics** > **Fault Collection**.
- In standalone mode, choose **Diagnostics** > **Fault Collection**.

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



4.6.5 System

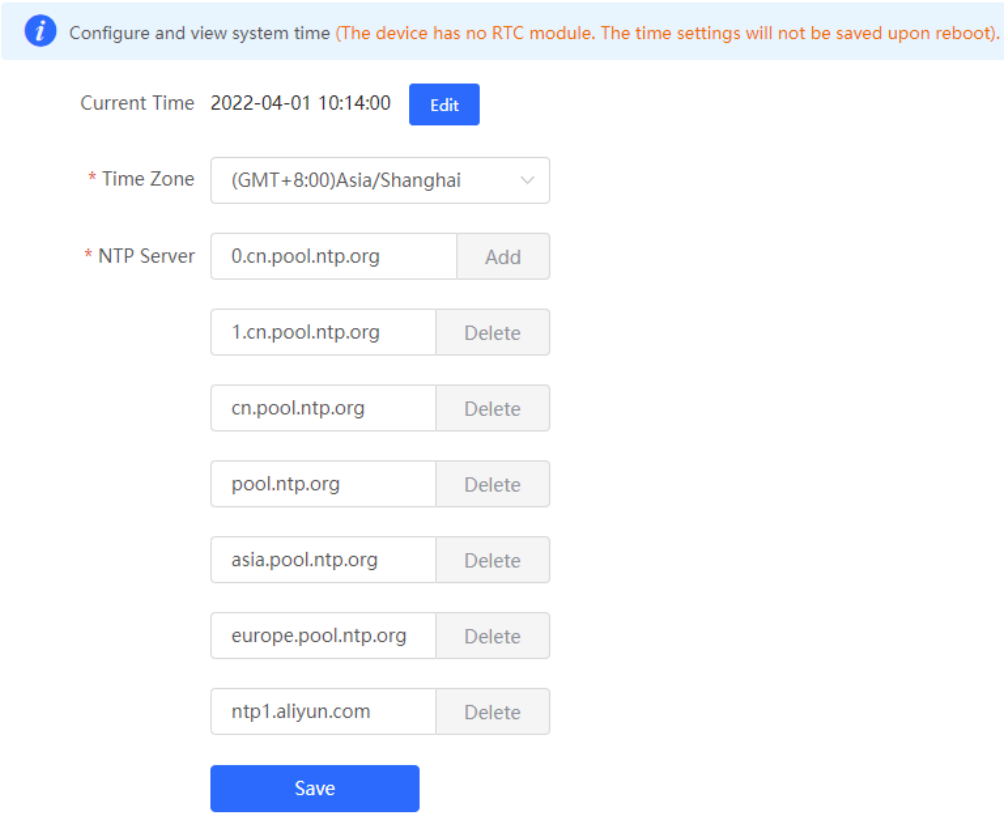
1. Setting the System Time

Note

In SON mode, the system time of all devices on the network will be changed synchronously.

Choose **System** > **System Time**.

Set parameters of the system time and click **Save**.



Current 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 the time is still incorrect, click **Edit** to manually set the time.
- If the time is not set or synchronized with a time server, the device will start with the manufacturing time.

Time Zone: Select the time zone based on your address.

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

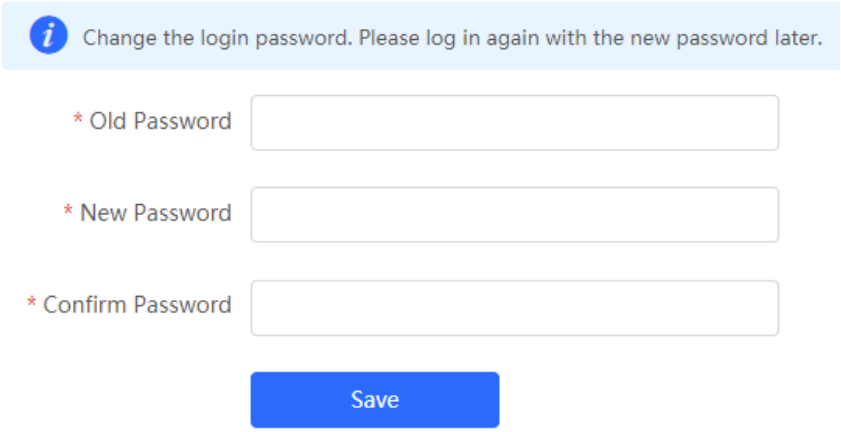
2. Setting the Login Password

Choose **System** > **Login** > **Login Password**.

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

Note

In SON mode, the login password of all devices on the network will be changed synchronously.

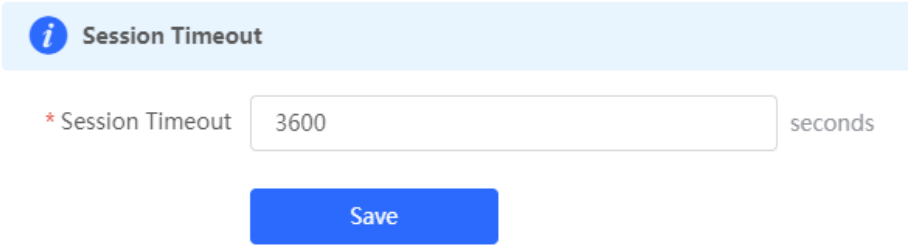


3. Setting the Timeout of the Login Page

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

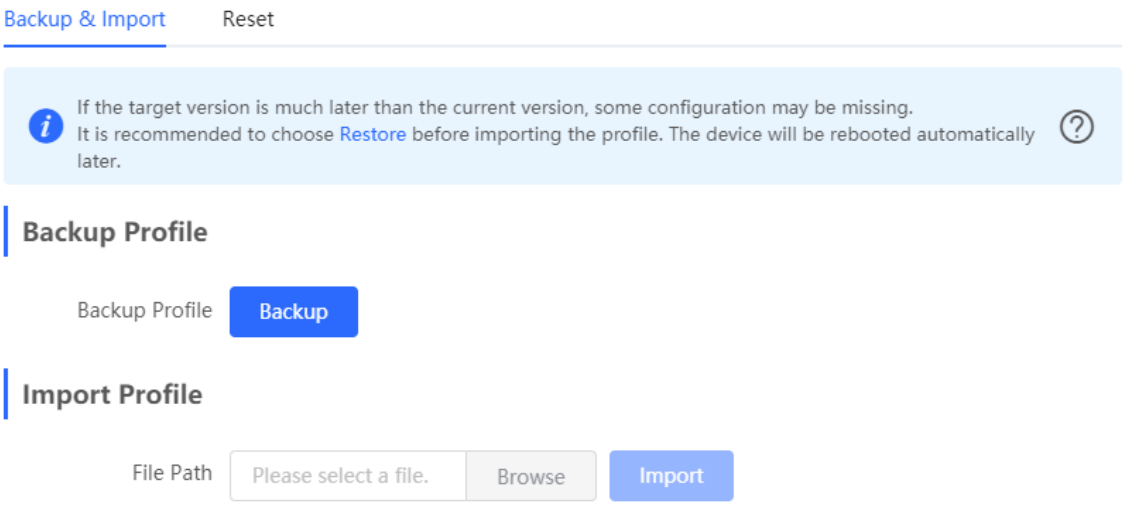
- In SON mode, select **Local Device** mode and choose **System** > **Login** > **Session Timeout**.
- In standalone mode, choose **System** > **Login** > **Session Timeout**.

Set the timeout of the login page and click **Save**. The value ranges from 600 to 7200 seconds.



4. Backup/Import Configuration

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



You can import a configuration file to AP or export the current configuration of the AP.

- 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 AP will restart.

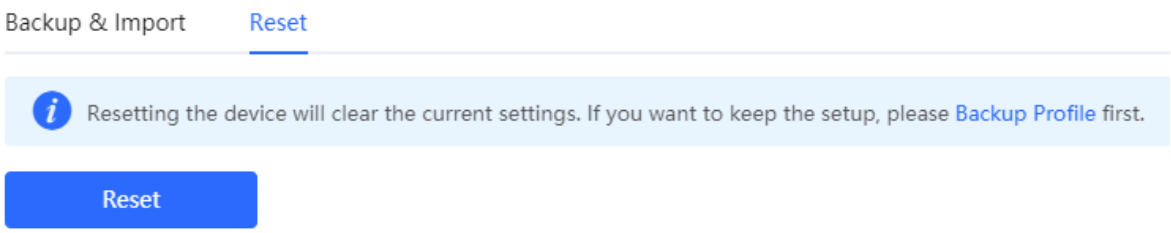
  If the target version is much later than the current version, some configuration may be missing.

  You are advised to restore the settings before importing the configuration. The AP will restart automatically if you restore it.

5. Reset

Choose **System** > **Management** > **Reset**.

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



Note

The operation will clear all configuration of the current device. To retain the current configuration, first back up the configuration (see 4. Backup/Import Configuration). Therefore, exercise caution when performing this operation.

6. Upgrade

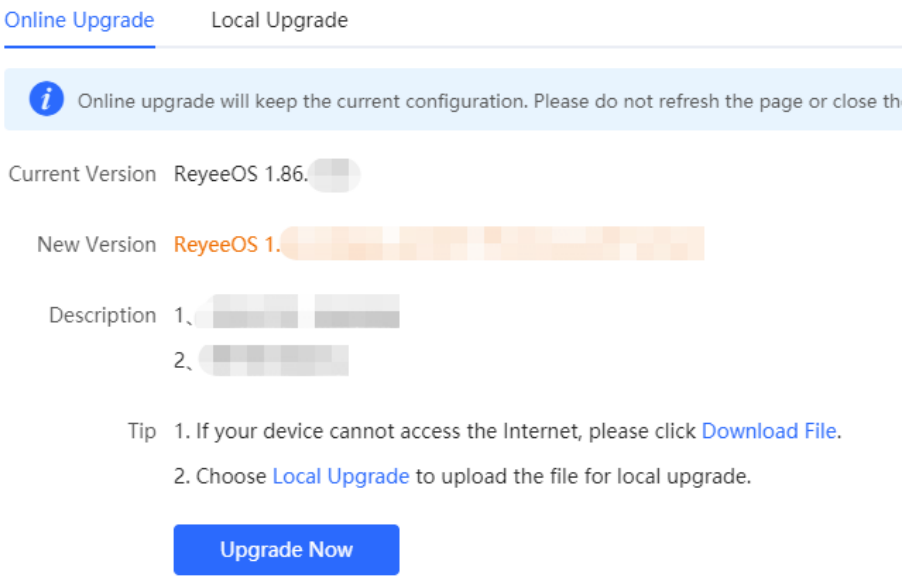
There are two modes: **Online Upgrade** and **Local Upgrade**.

Online Upgrade

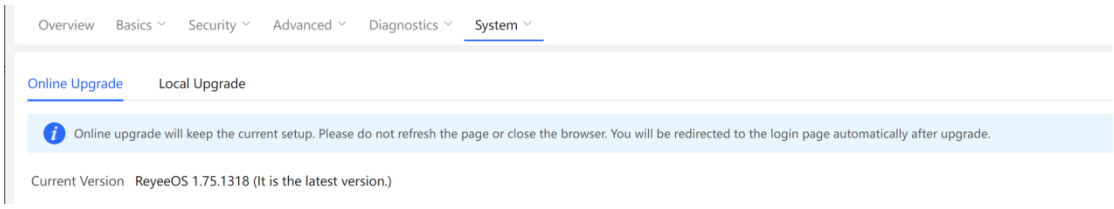
- In SON mode, select **Local Device** mode and choose **System** > **Upgrade** > **Online Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Online Upgrade**.

You can view the current system version.

- If a new version is available, you can click **Upgrade Now** for an upgrade. The upgrade operation does not affect the current configuration, but the AP will restart after being upgraded successfully. Do not refresh the page or close the browser during the upgrade. You are redirected to the login page automatically after the upgrade.



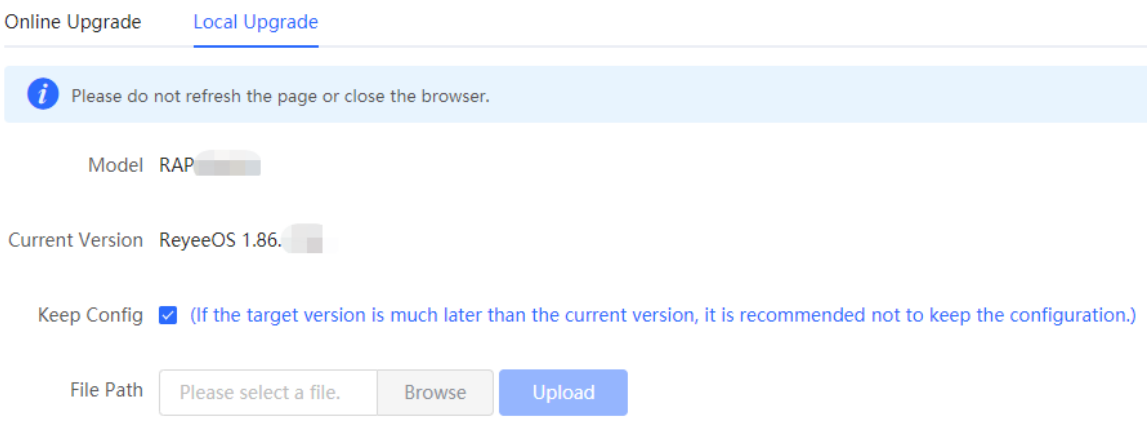
- If there is no new version, the system displays a message indicating that the current version is the latest.



Local Upgrade

- In SON mode, select **Local Device** mode and choose **System** > **Upgrade** > **Local Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Local Upgrade**.

You can view the current software version, hardware version, and device model. To upgrade the device with the configuration retained, check **Keep Config**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. After the file is uploaded successfully, the system displays upgrade package information and asks for the upgrade. Click **OK** to start the upgrade.



7. Restarting the Device

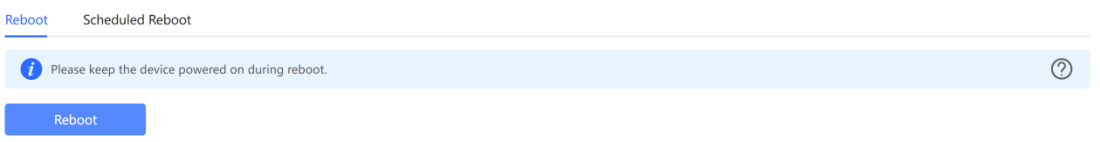
- In SON mode, select **Local Device** mode and choose **System** > **Reboot**.
- In standalone mode, choose **System** > **Reboot**.

You can restart the device immediately or set a scheduled restart.

- Restart the device immediately.

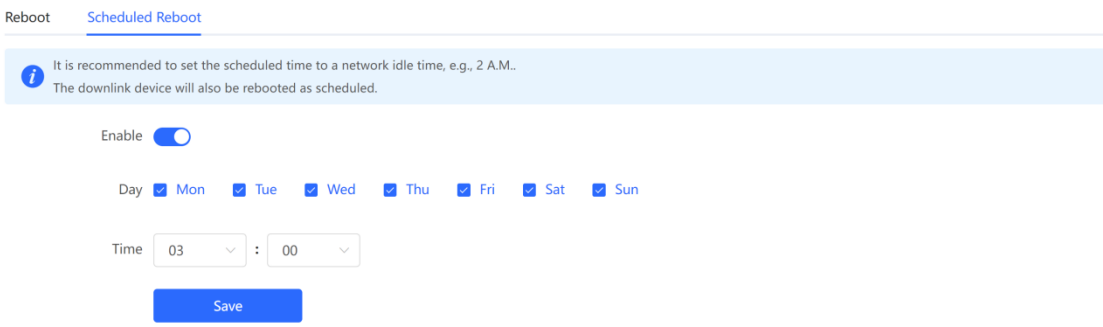
  On the **Reboot** tab page, click **Reboot** and click **OK** in the confirmation box. **Reboot** allows you to restart the device immediately.

  The device is restarted, and you need to log into the Eweb management system again after the restart. Do not refresh the page or close the browser during the restart. After the device is successfully restarted, you will be redirected to the login page of the Eweb management system.



- Set a scheduled reboot.

  Switch to the **Scheduled Reboot** tab page, enable scheduled reboot, set the scheduled day and time, and click **Save**.



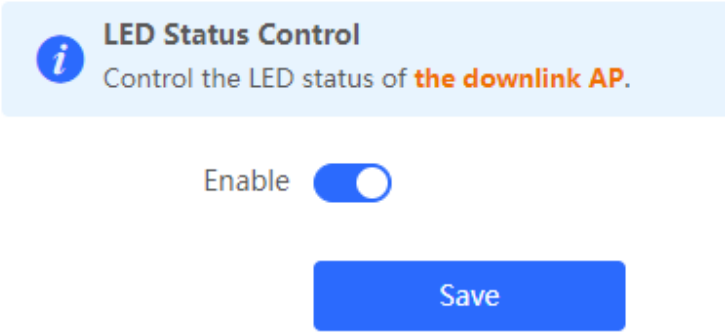
8. AP LED

Note

The **LED Status Control** function is not supported in the standalone mode (the SON is not enabled).

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

Enable or disable the LED of all downlink APs on the network and click **Save**.



4.7 Configuring SNMP

Caution

The functions mentioned in this chapter are supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260, and RG-RAP6262.

4.7.1 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.

4.7.2 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.

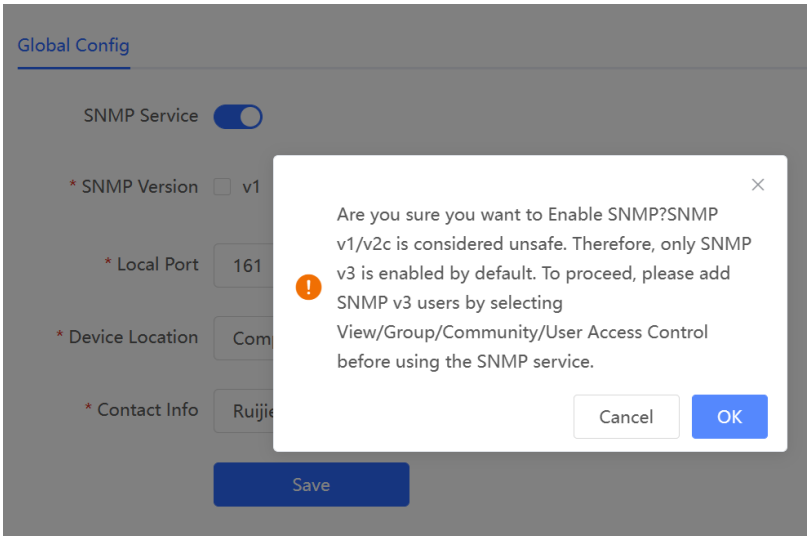
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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

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

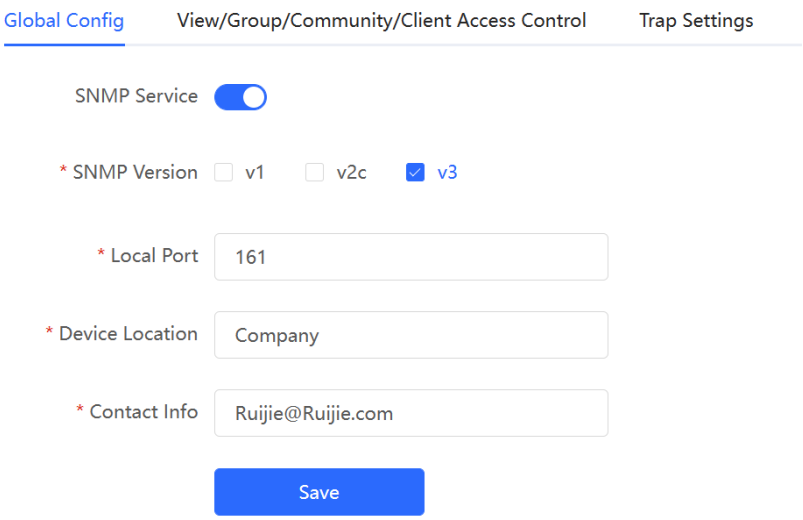


Table 4-17 Global Configuration Parameters

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.

4.7.3 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.

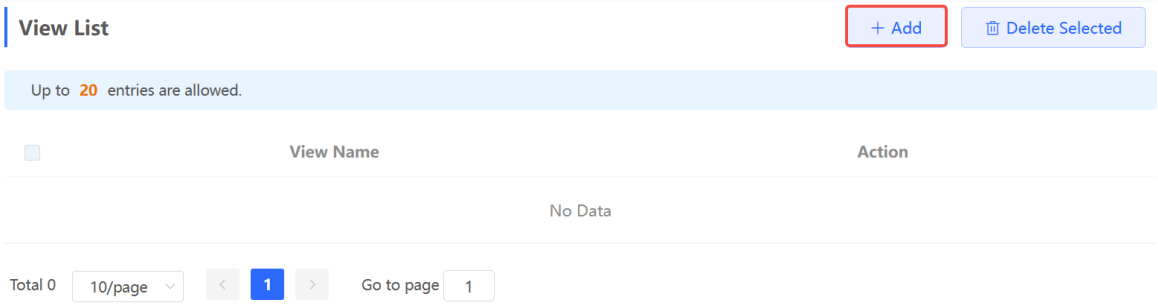
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

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

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

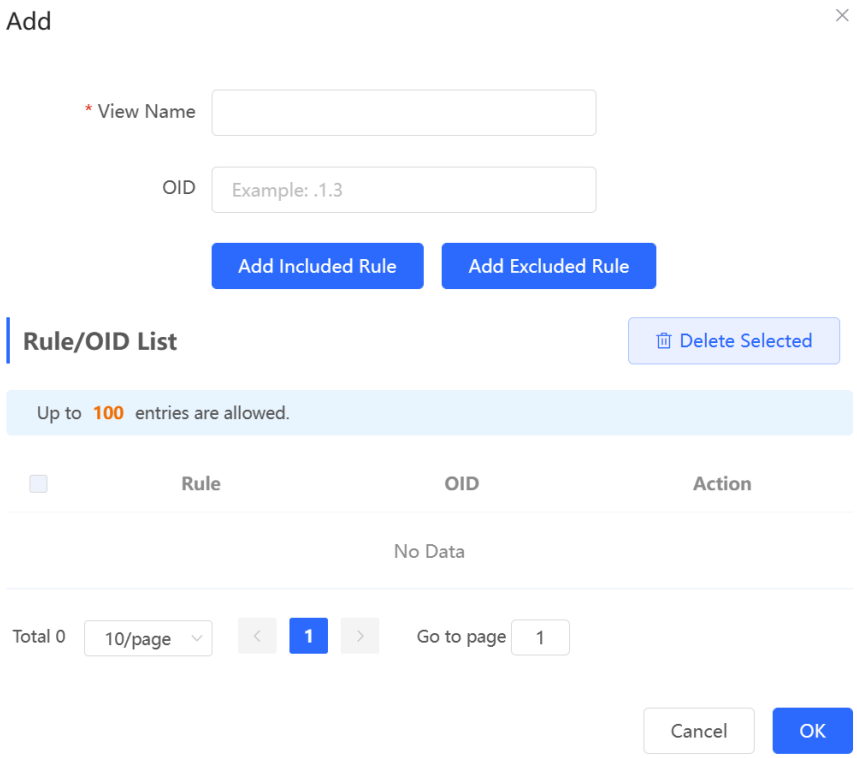


Table 4-18 View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.

Parameter	Description
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

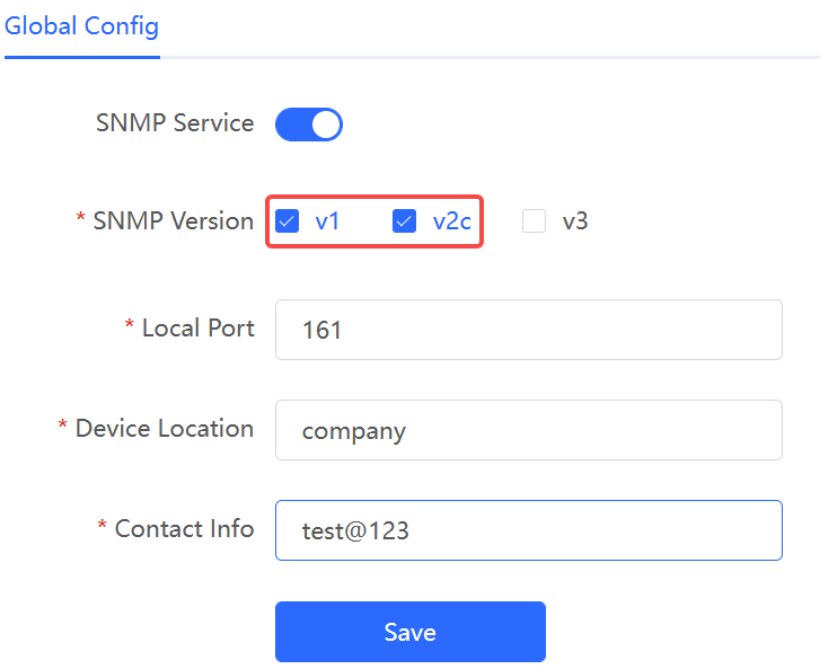
A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1/v2c Users

- Overview

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



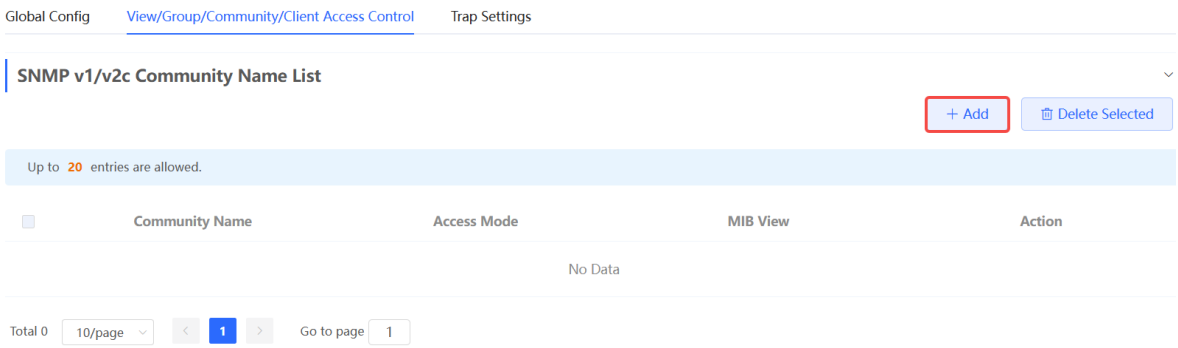
Note

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

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

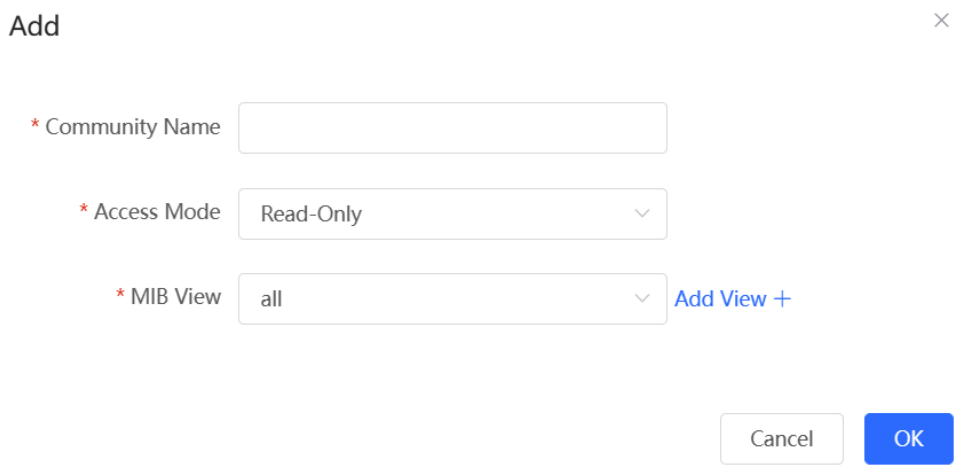


Table 4-19 v1/v2c User Configuration Parameters

Parameter	Description
Community Name	At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and

Parameter	Description
	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**.

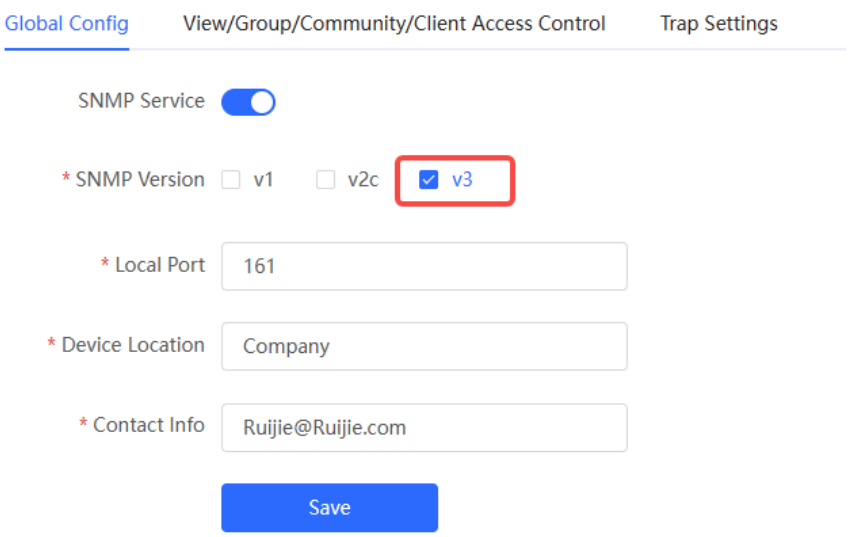
3. Configuring v3 Groups

- 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.



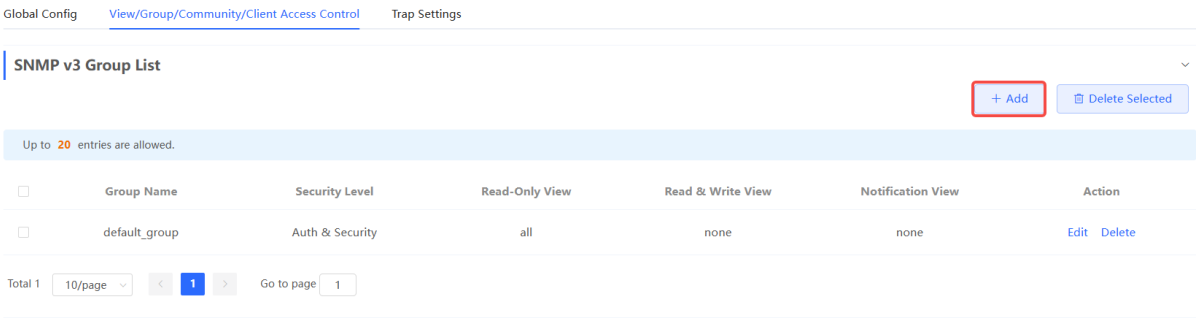
Note

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

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

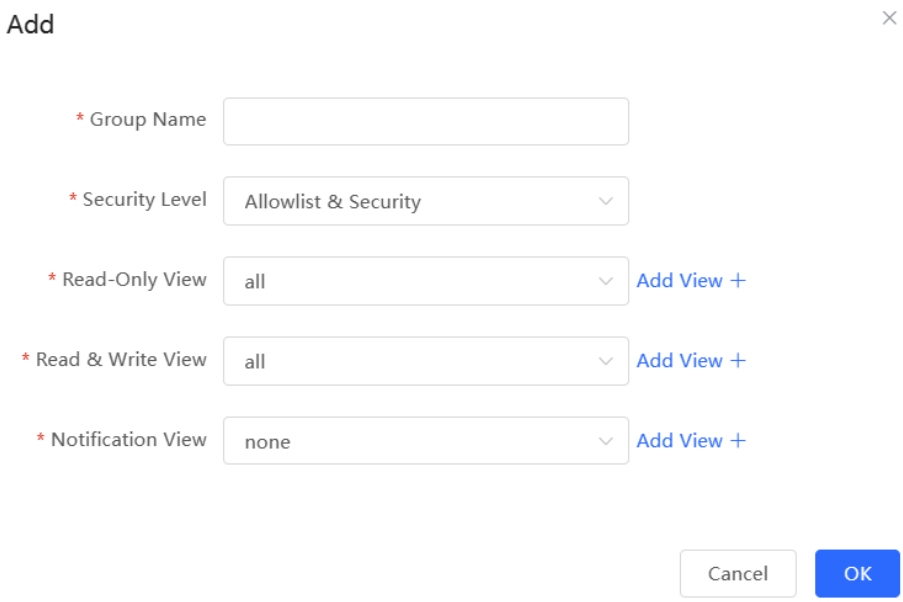


Table 4-20 v3 Group Configuration Parameters

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

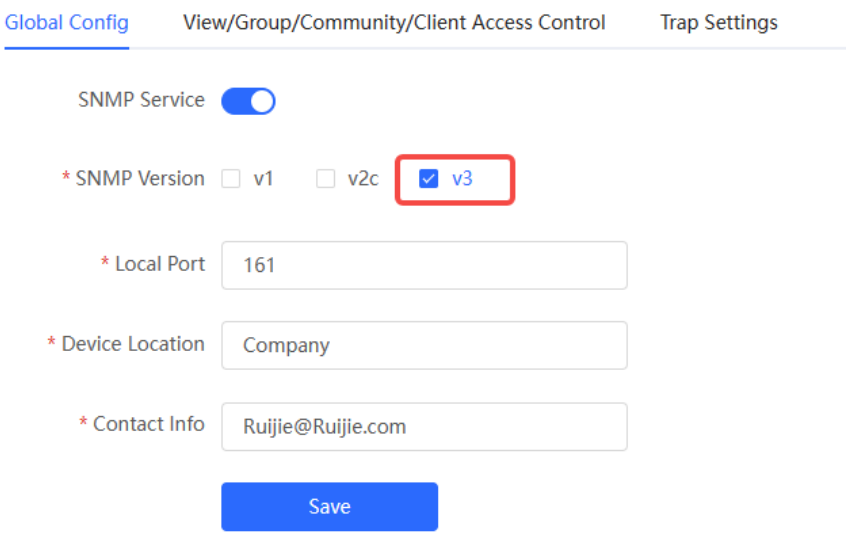
- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

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



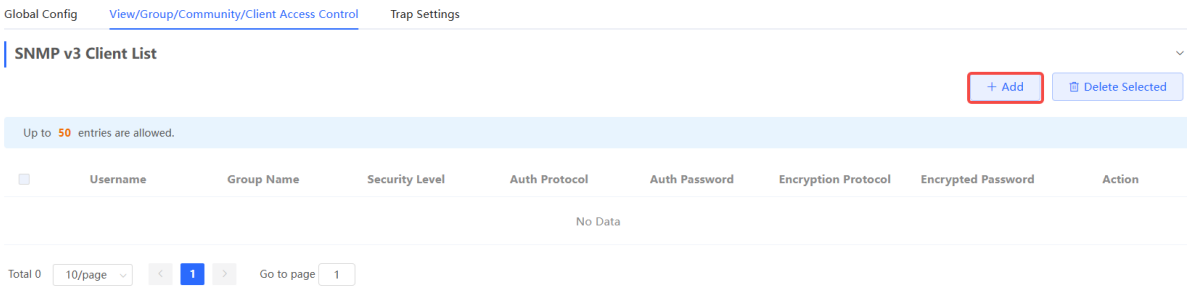
Note

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

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

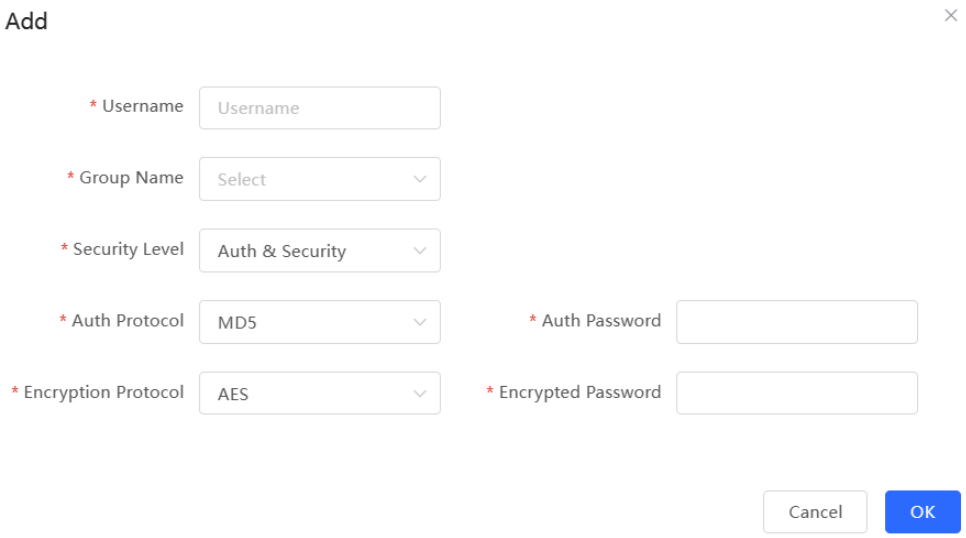


Table 4-21 v3 User Configuration Parameters

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

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

4.7.4 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

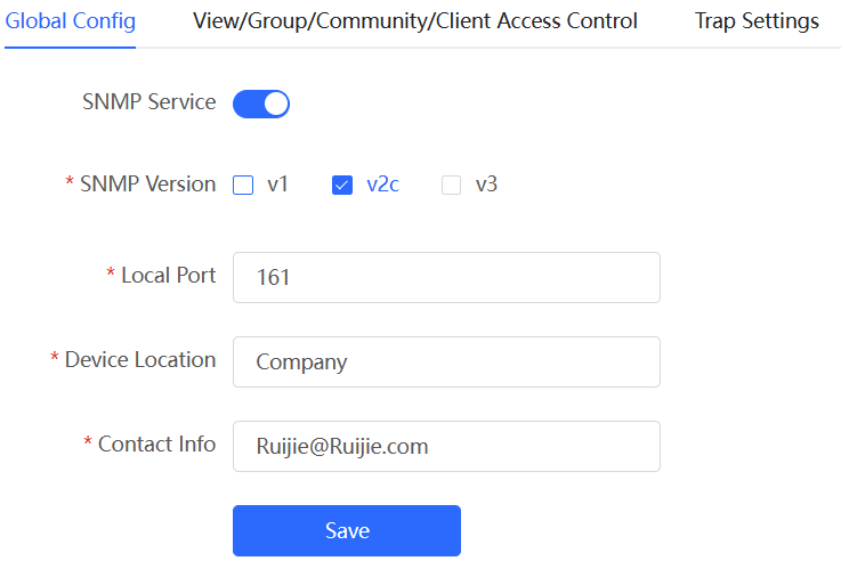
According to the user's application scenario, the requirements are shown in the following table:

Table 4-22 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

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

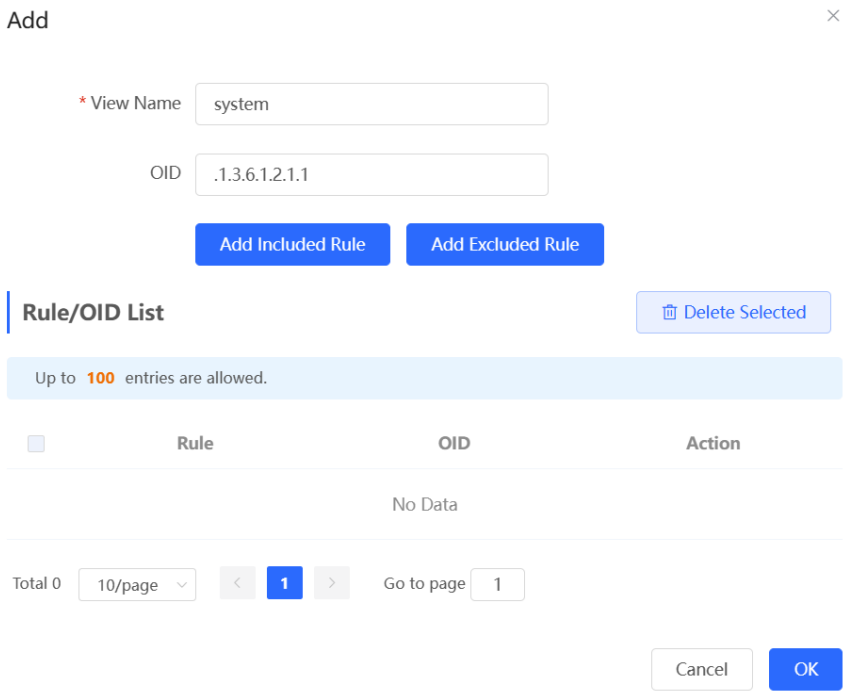


(2) Add a view on the **View/Group/Community/Client Access Control** interface.

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**.

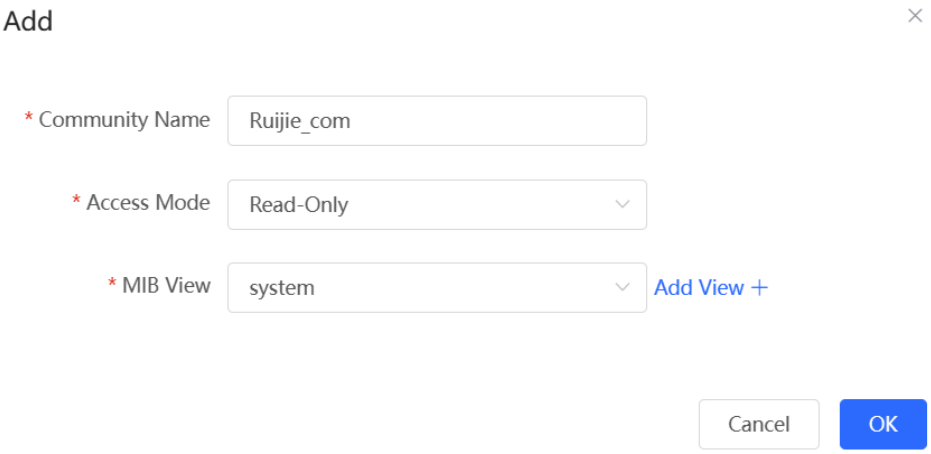


(3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.

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

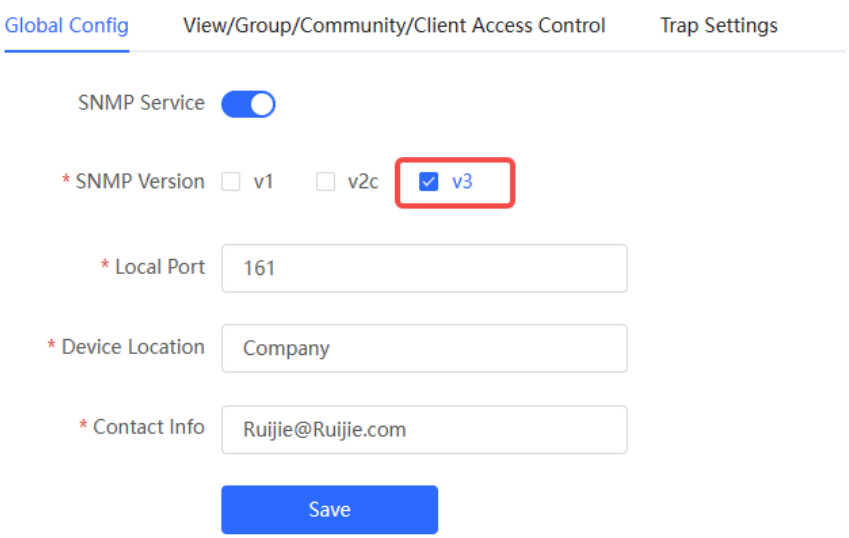
According to the user's application scenario, the requirements are shown in the following table:

Table 4-23 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**.

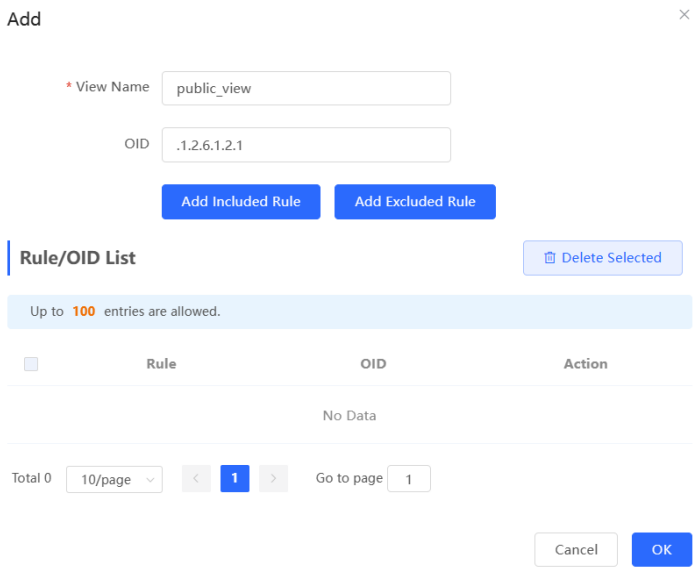


(2) Add a view on the **View/Group/Community/Client Access Control** interface.

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**.

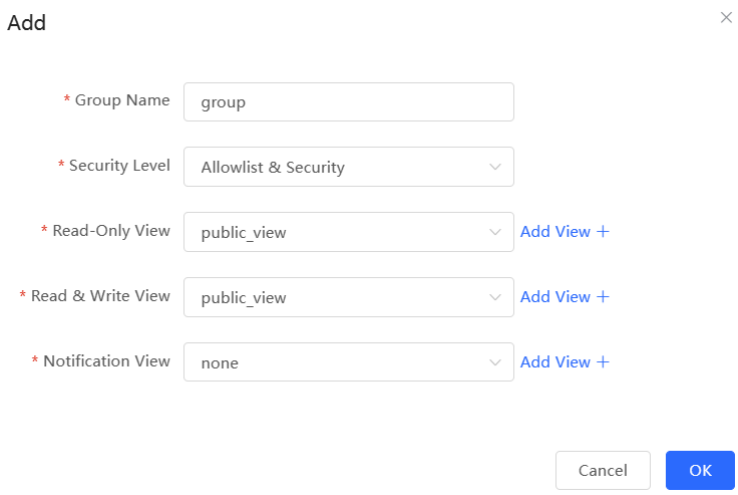


(3) On the **View/Group/Community/Client Access Control** interface, add an SNMP v3 group.

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**.

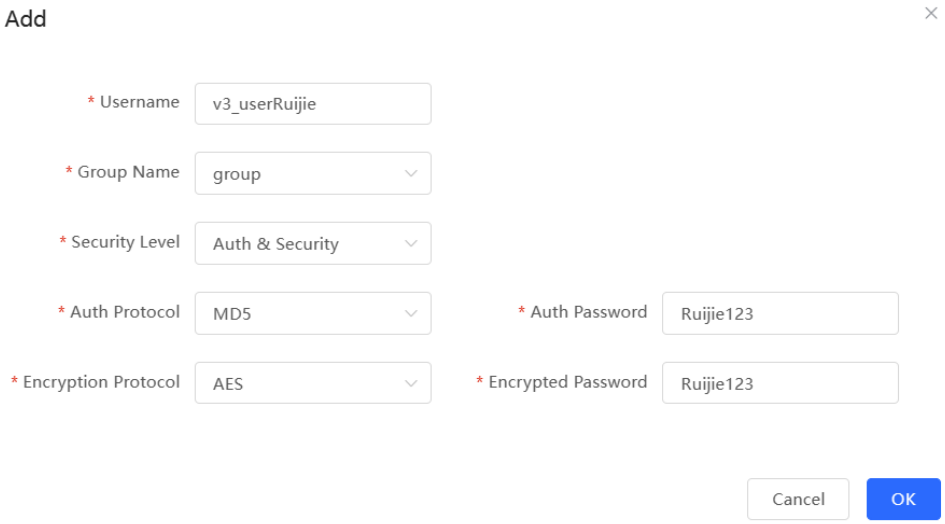


(4) On the **View/Group/Community/Client Access Control** interface, add an SNMP v3 user.

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**.



4.7.5 Configuring Trap Service

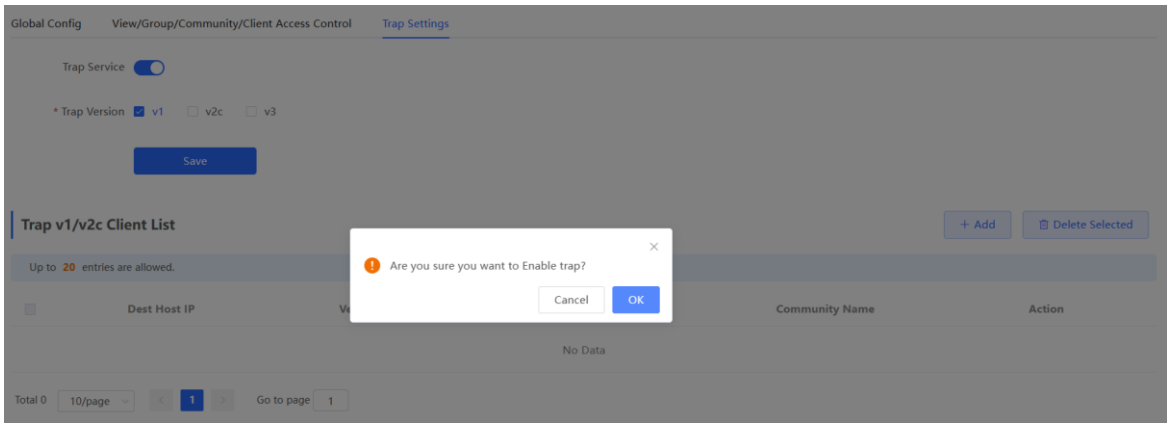
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring 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.

In **Network** mode, choose **System** > **SNMP** > **Trap Settings**

(1) Enable the trap service.



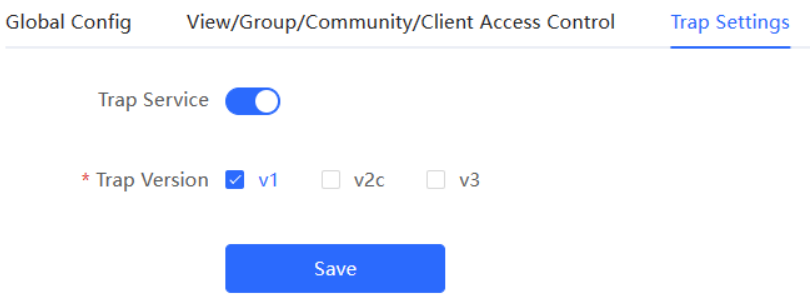
When the trap service is enabled for the first time, the system will pop up a prompt message. Click **OK**.

(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.

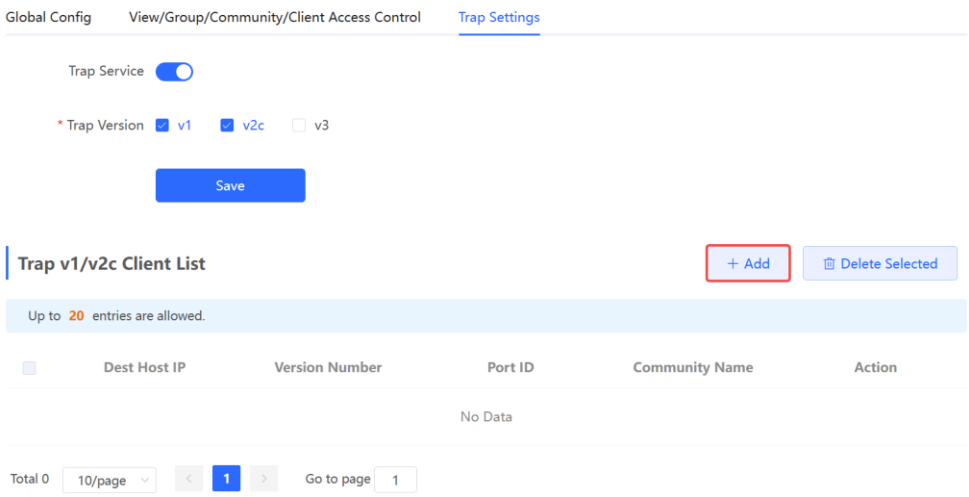
- Prerequisites

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

- Configuration Steps

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

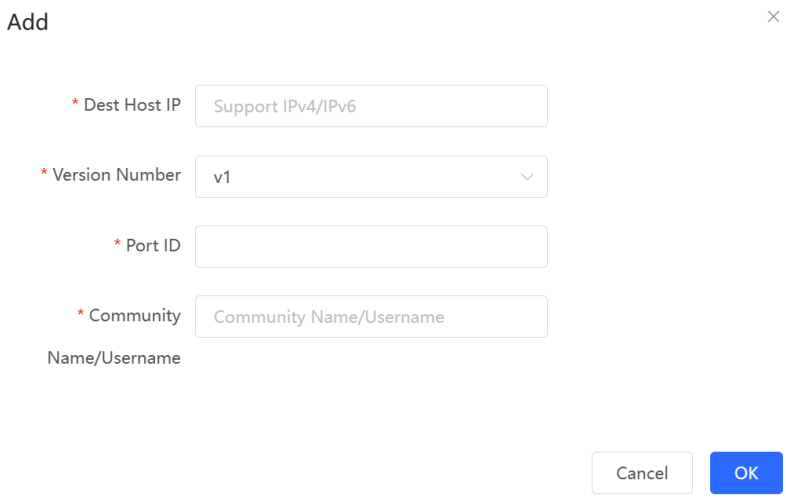


Table 4-24 Trap v1/v2c User Configuration Parameters

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.

Parameter	Description
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.

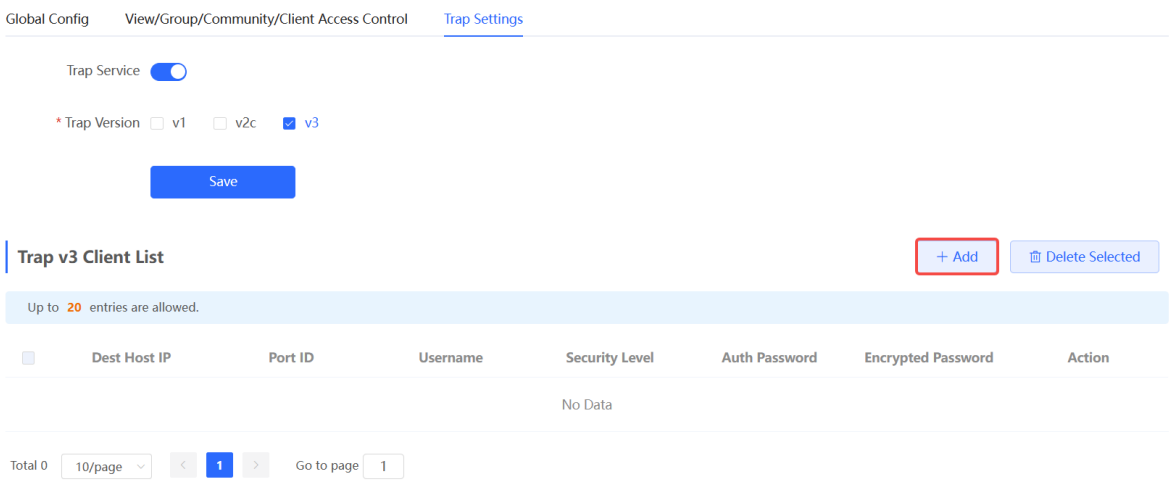
- Prerequisites

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

- Configuration Steps

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

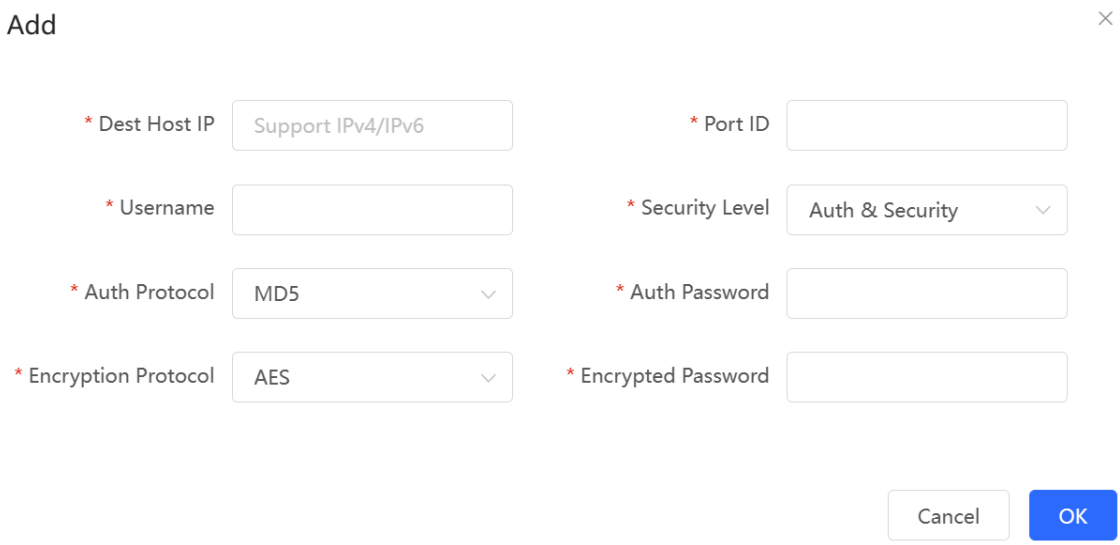


Table 4-25 Trap v3 User Configuration Parameters

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.
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.

Parameter	Description
	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**.

4.7.6 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

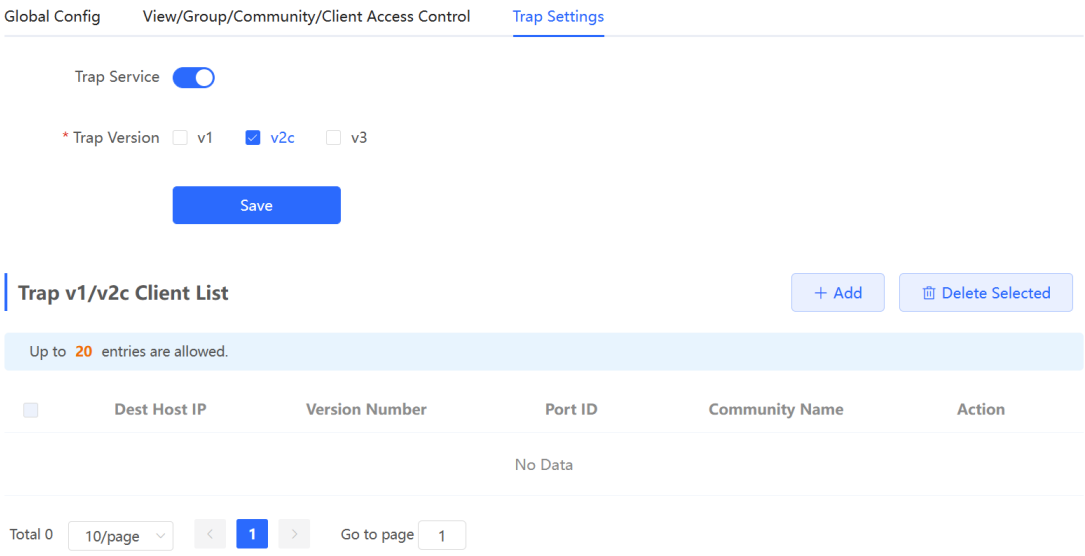
According to the user's application scenario, the requirements are shown in the following table:

Table 4-26 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

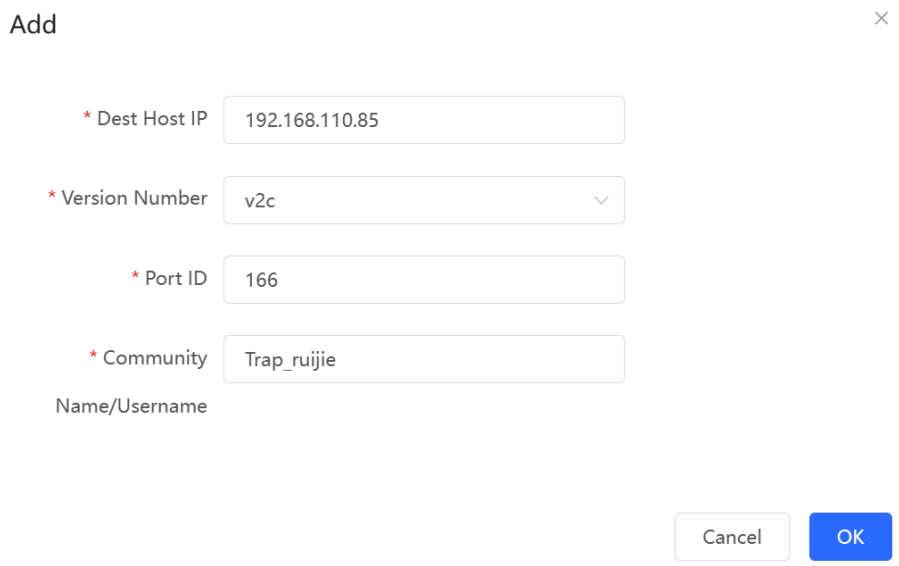
- Configuration Steps

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



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

(4) 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

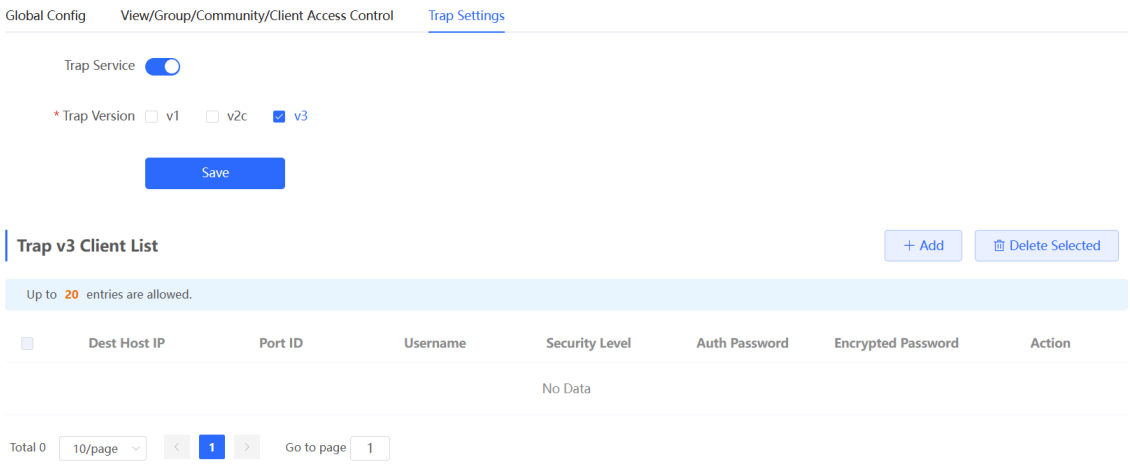
According to the user's application scenario, the requirements are shown in the following table:

Table 4-27 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

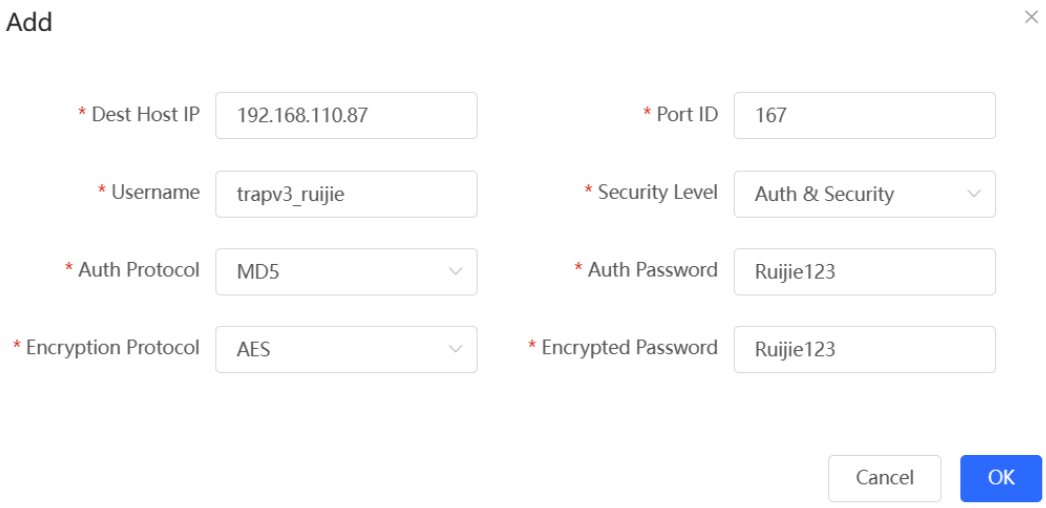
- Configuration Steps

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



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

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



5 Advanced Solution Guide

5.1 Reyee Flow Control Solution

5.1.1 Application Scenario

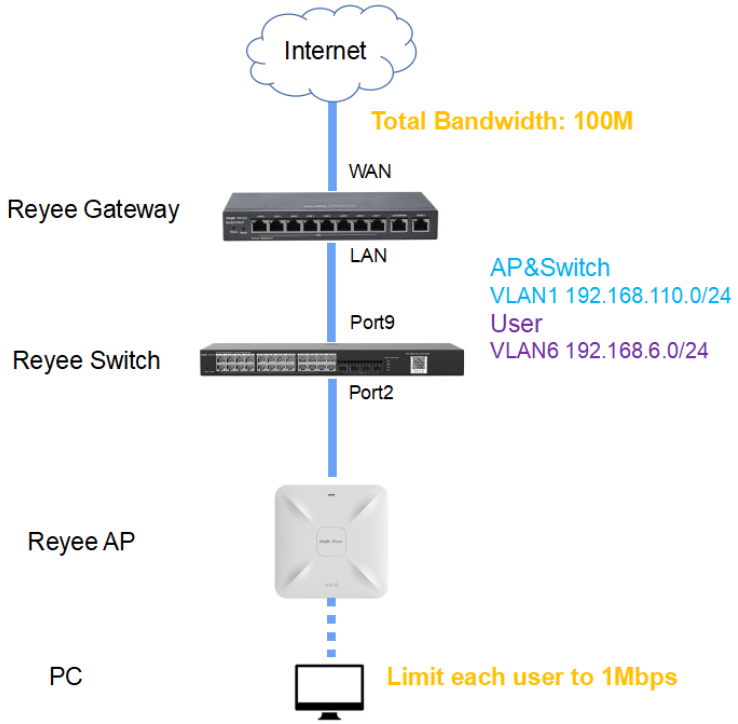
Flow control is used for setting the rate limit of download and upload for the clients, and protects the network bandwidth from being occupied by some clients.

5.1.2 Configuration Case

Requirement

The total bandwidth of the EG egress needs to be limited to 100 Mbit/s and the rate of each user in VLAN 6 to 1 Mbit/s.

Network Topology



Network Description:

The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

The AP and switch obtain IP addresses on network segment 192.168.110.0/24 in VLAN 1 for Internet access.

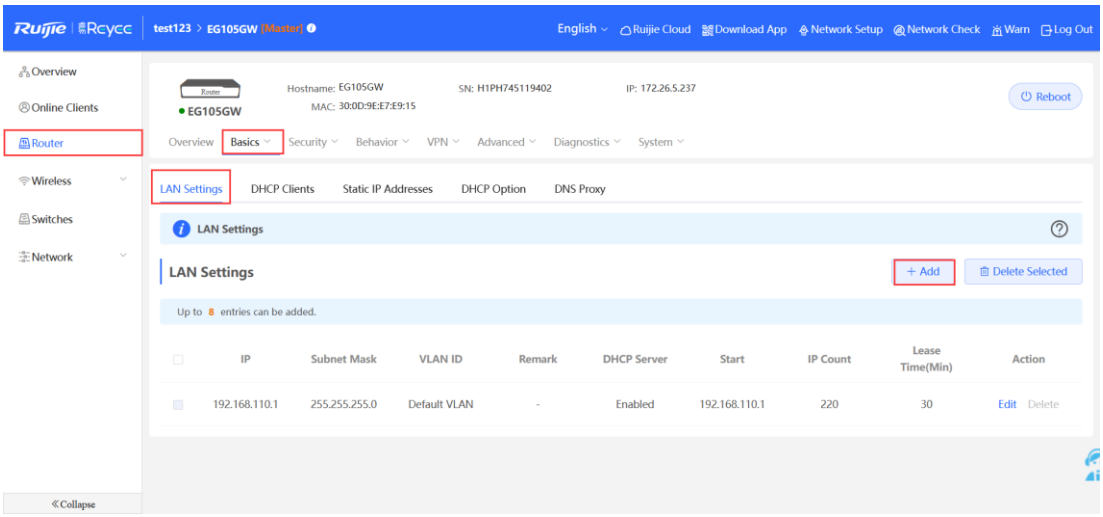
Users obtain IP addresses on network segment 192.168.6.0/24 in VLAN 6 for Internet access.

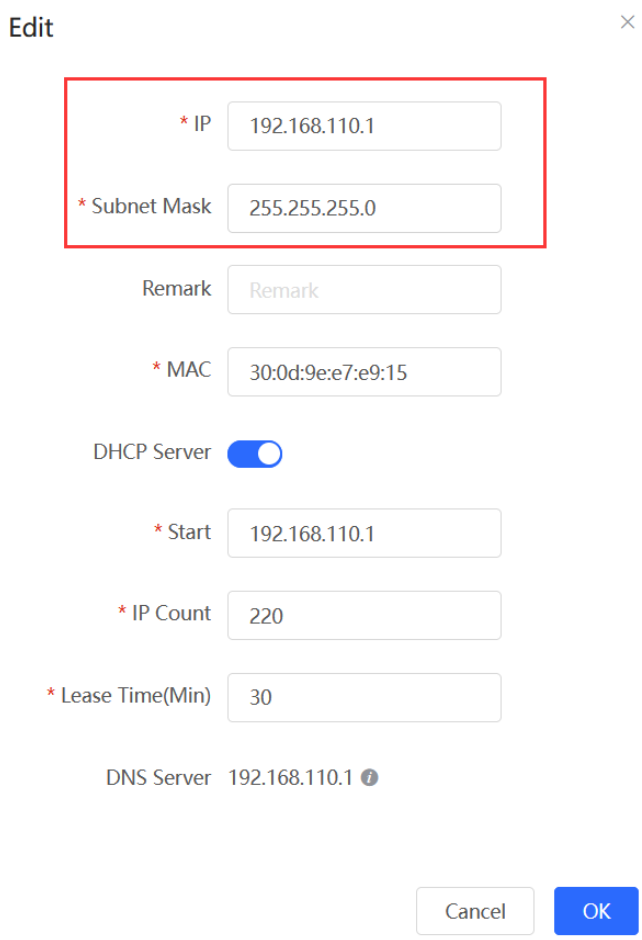
Configuration Steps

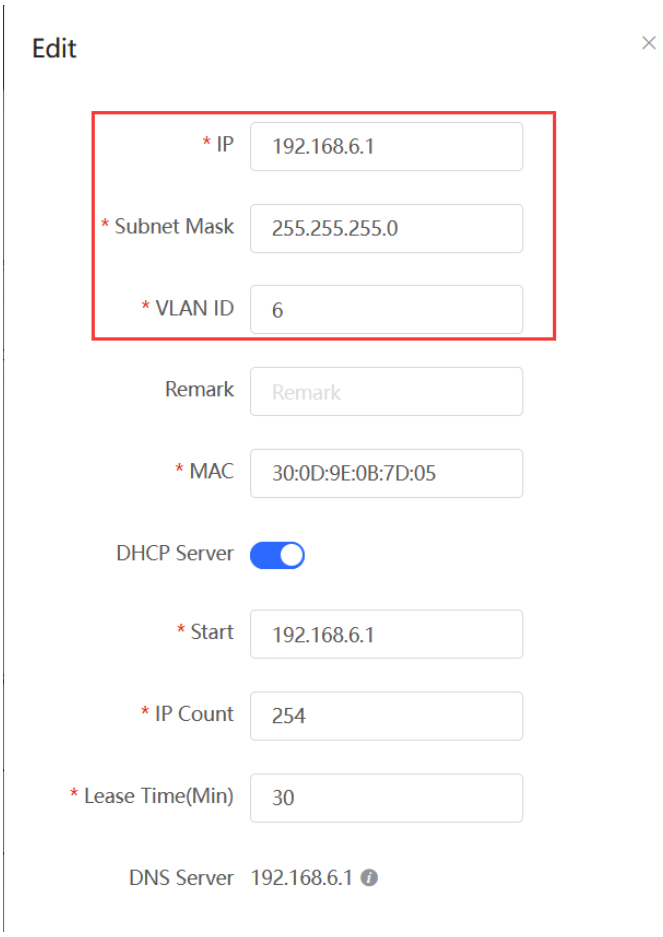
The configuration steps include configuring the basic network, enabling smart flow control, and configuring a customized policy.

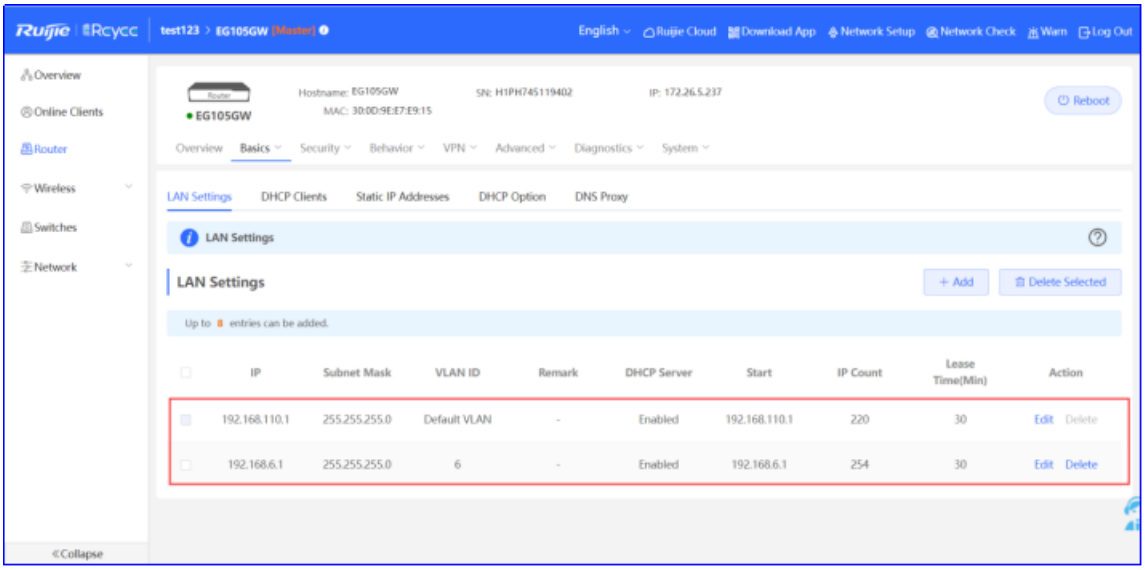
(1) Configure the basic network.

a Choose **Router** > **Basics** > **LAN** > **LAN Settings** > **Add**. Configure LAN settings and a DHCP pool for VLAN 1 and VLAN 6 on the EG.





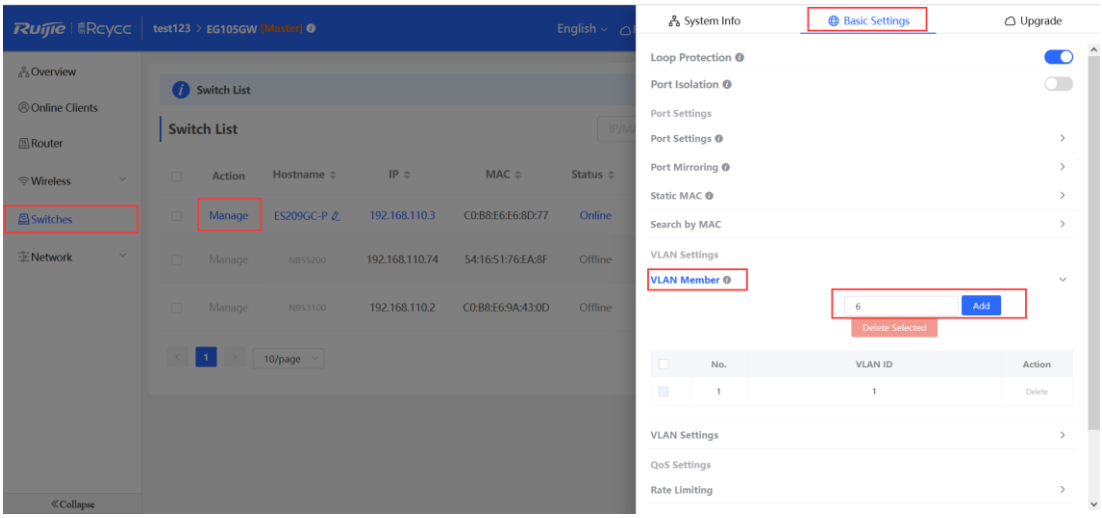


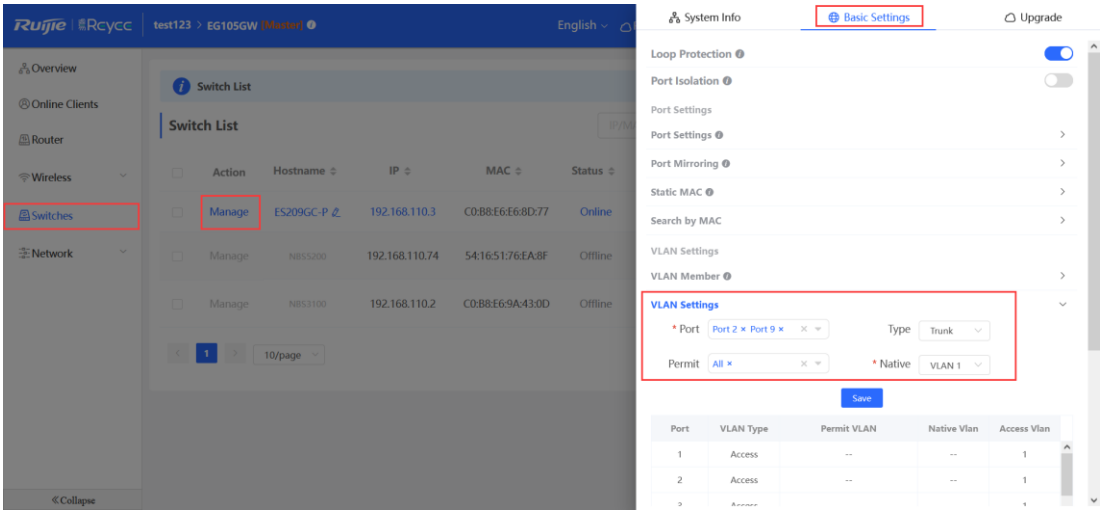


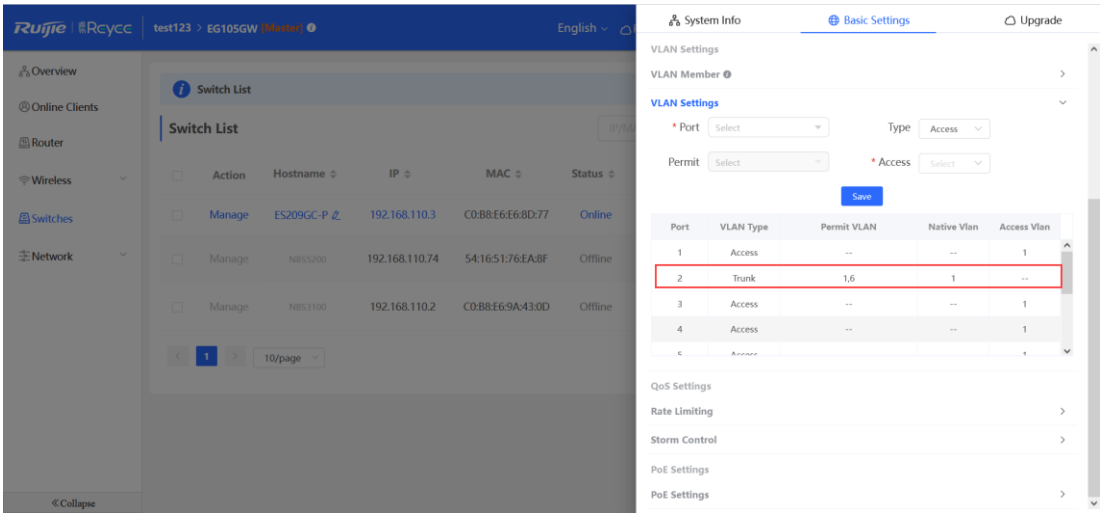
Note

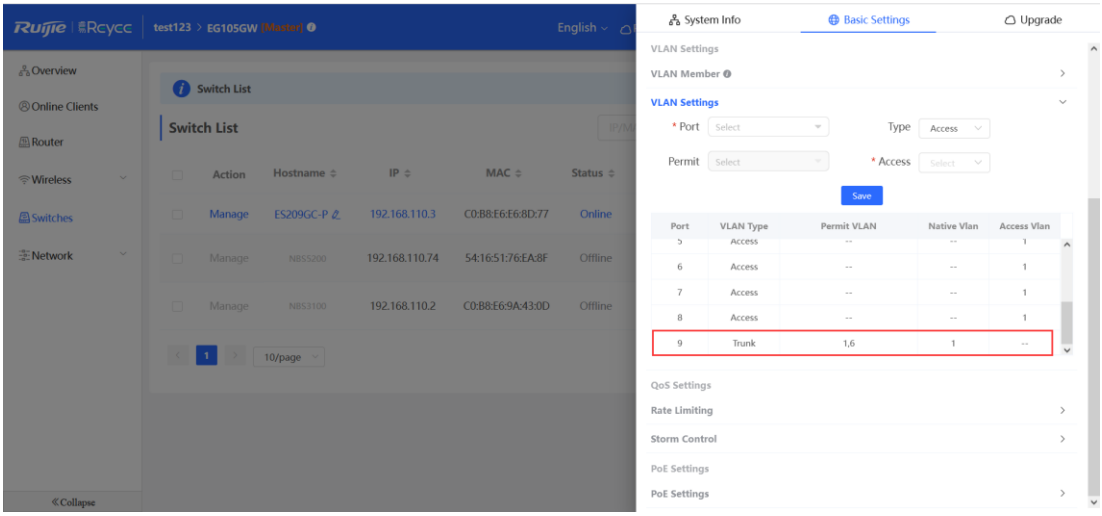
The network segment 192.168.110.0/24 is configured for VLAN 1.

b Choose **Switches** > **Manage** > **Basic Settings** > **VLAN Member** to create VLAN 6 on the switch, and click **VLAN Settings** to configure port 2 and port 9 connected to the AP and EG as trunk ports and allow packets from VLAN 1 and VLAN 6 to pass through. Then check port settings on the switch.

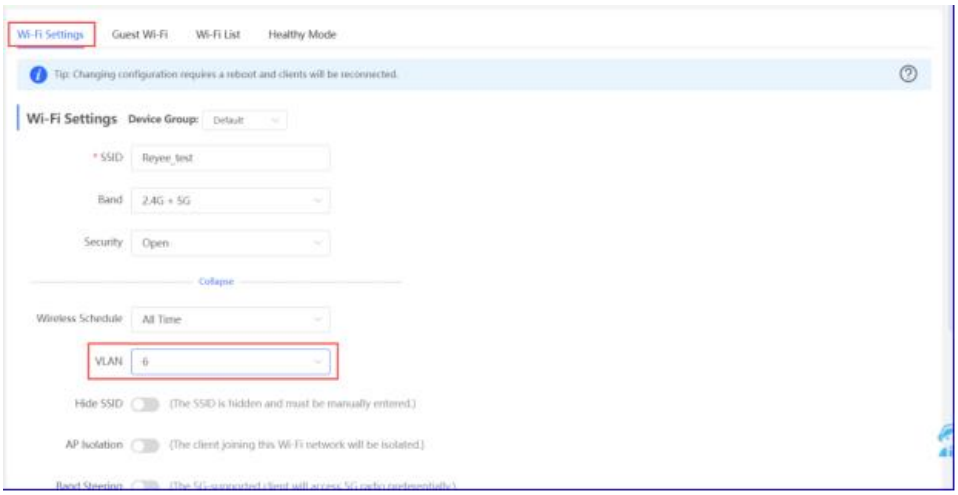


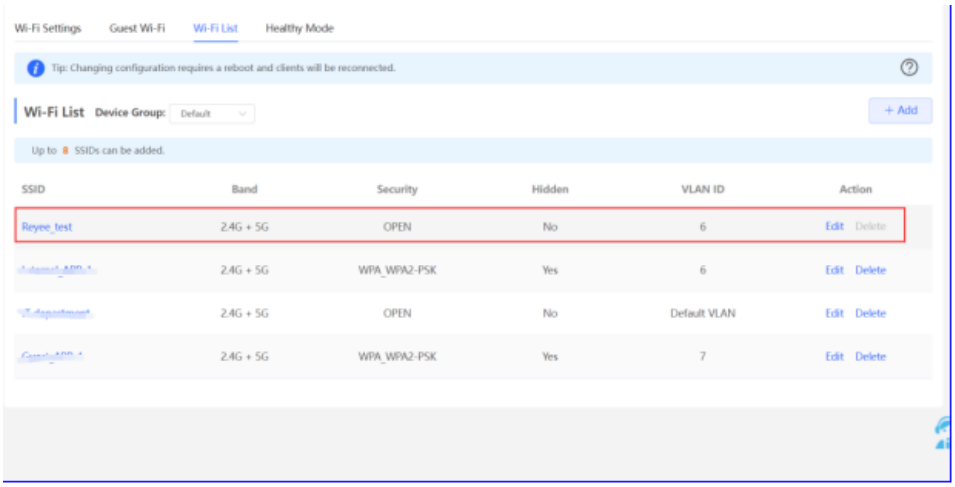






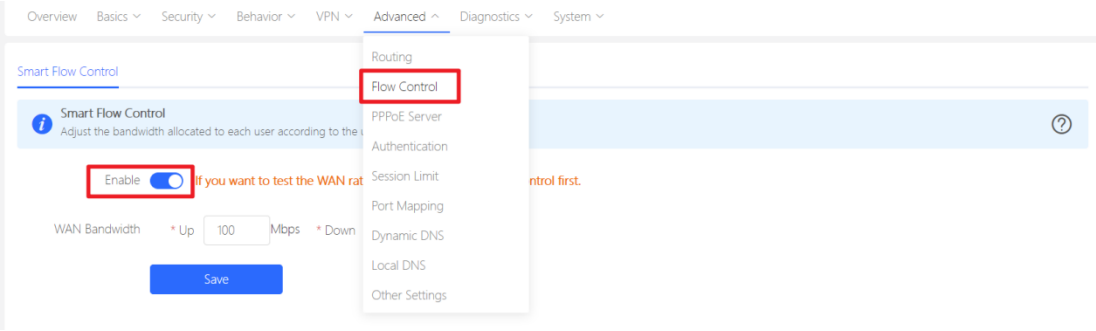
c Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Configure the SSID named **Reyee_test** and associate VLAN 6 with the SSID.



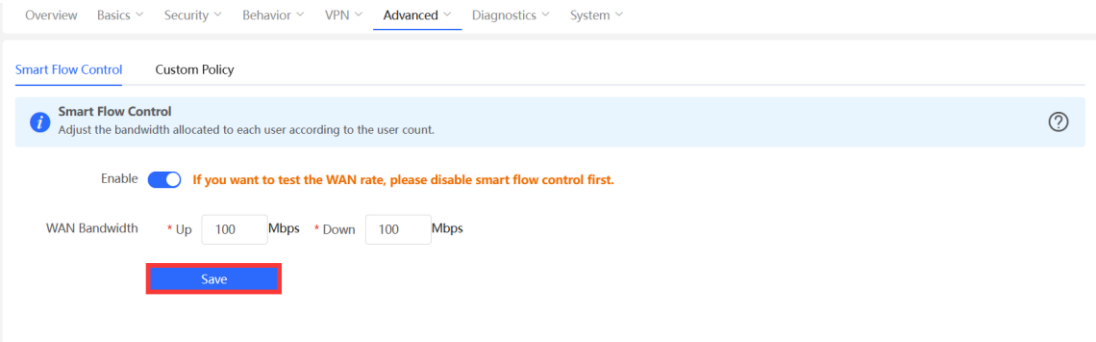


(2) Configure **Smart Flow Control** and a customized policy.

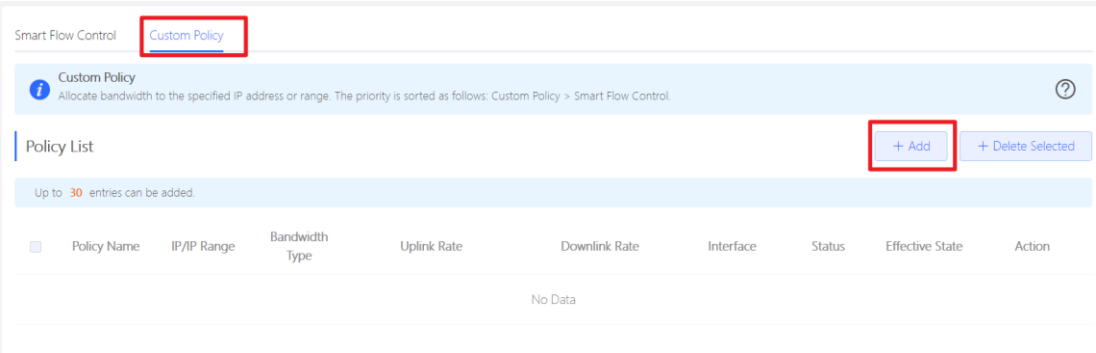
a Choose **Router** > **Advanced** > **Flow Control** and enable **Smart Flow Control**.



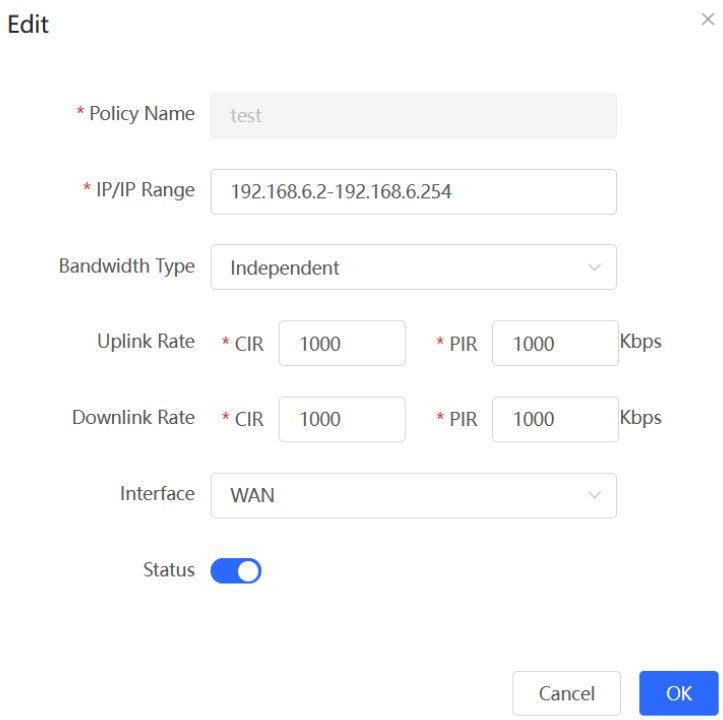
b Set uplink and downlink WAN bandwidth to 100 Mbit/s and click **Save** to save the configuration.

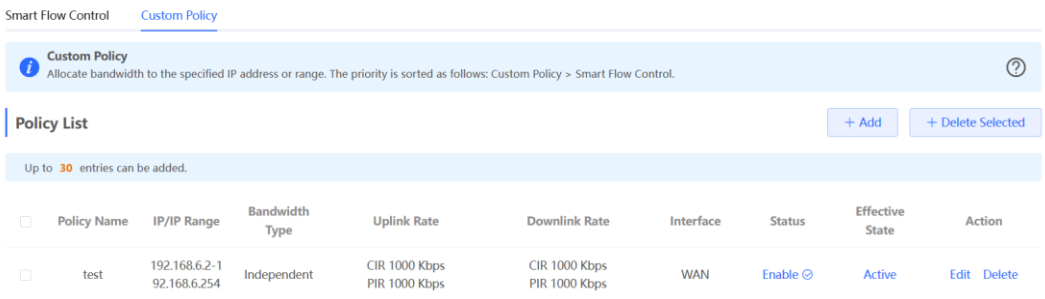


c After the previous step is complete, **Custom Policy** will be displayed. Click **Add** to add a policy.



d Set **Policy Name**, **IP range**, **Bandwidth Type**, **Rate**, and other parameters.



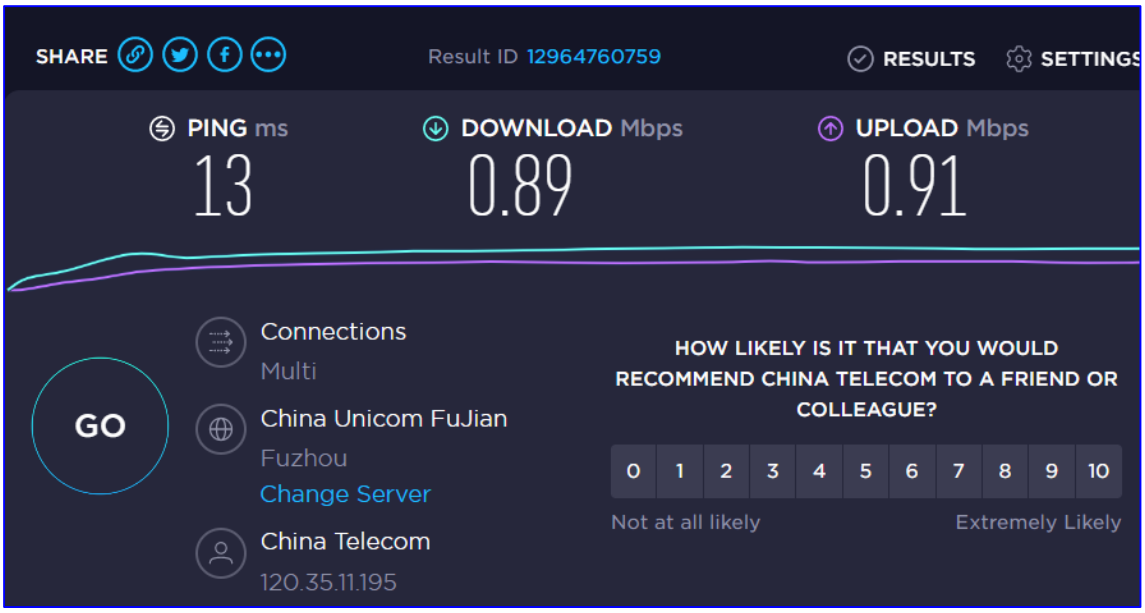


Bandwidth Type: **Shared** indicates that all IP addresses share the total bandwidth. **Independent** indicates that the rate limit is set for each IP address.

Uplink Rate/**Downlink Rate**: **CIR** means the committed information rate. **PIR** means the peak information rate.

Configuration Verification

Use the speed test tool to check that each user is limited to 1 Mbit/s.



5.2 Reyee Cloud Authentication Solution

5.2.1 Working Principle

Cloud authentication allows you to control users' access to the wireless network. The configuration will be synchronized from the cloud to the local EG. In portal authentication, all the clients' HTTP requests will be redirected to an authentication page first. The clients are required for authentication, payment, acceptance of the end-user license agreement, acceptable use policy, survey completion, or other valid credentials. Then they can visit the Internet after successful authentication.

5.2.2 Application Scenario

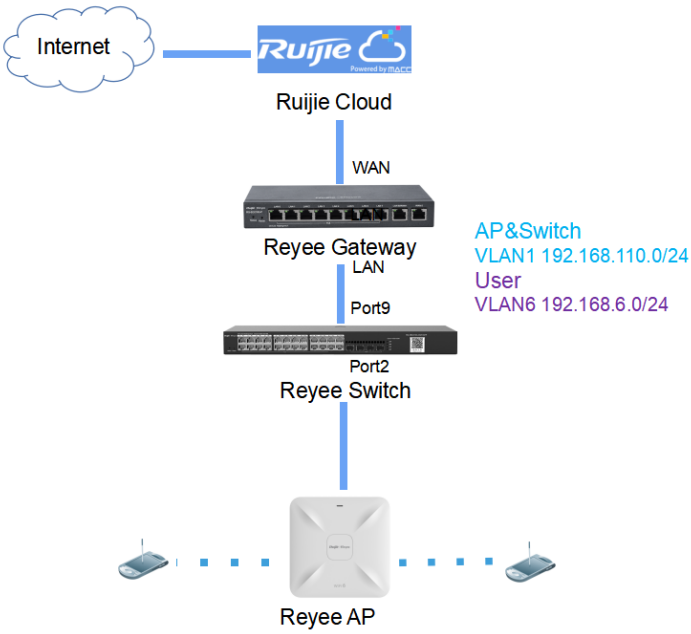
Portal authentication, also known as web authentication, is usually deployed on a guest-access network (such as a hotel or a coffee shop) to control the clients' Internet access.

5.2.3 Configuration Case

Requirement

Users need to be authenticated first before being allowed to access the Internet. A Reyee AP does not support cloud authentication, so a Reyee EG is required.

Network Topology



Network Description:

The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

The AP and switch obtain IP addresses on network segment 192.168.110.0/24 in VLAN 1 for Internet access

Users obtain IP addresses on network segment 192.168.6.0/24 in VLAN 6 for Internet access.

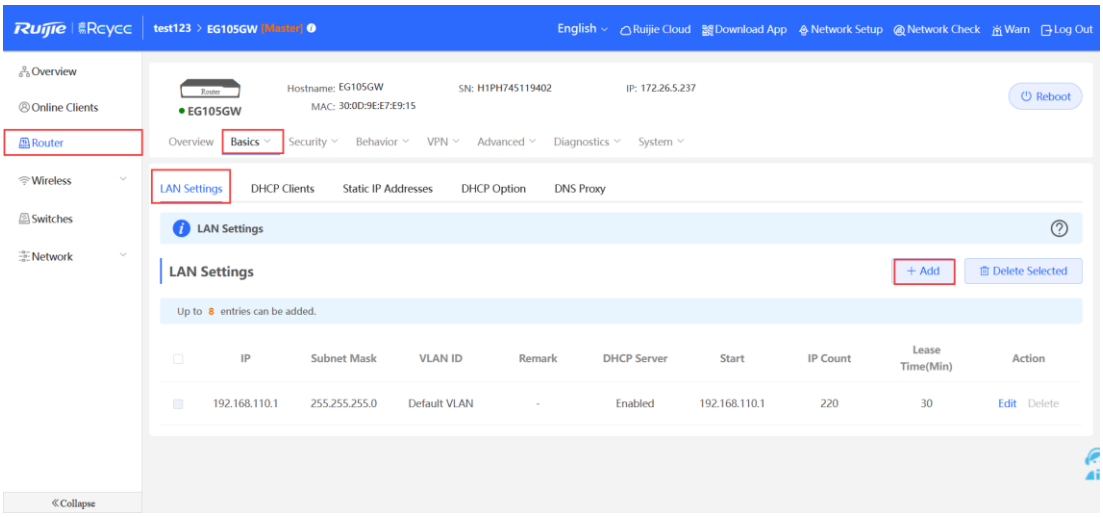
Ruijie Cloud manages and monitors devices and clients and provides captive authentication for clients.

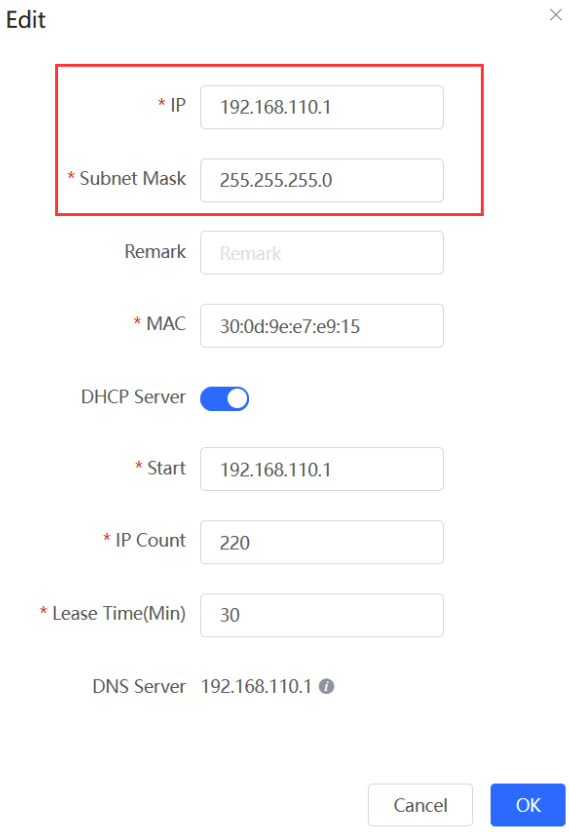
Configuration Steps

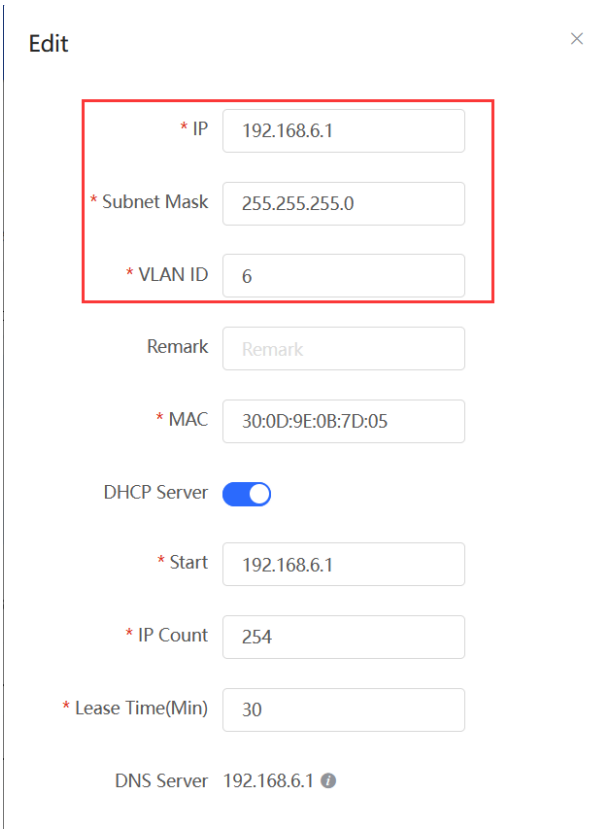
The configuration steps include configuring the basic network and cloud authentication.

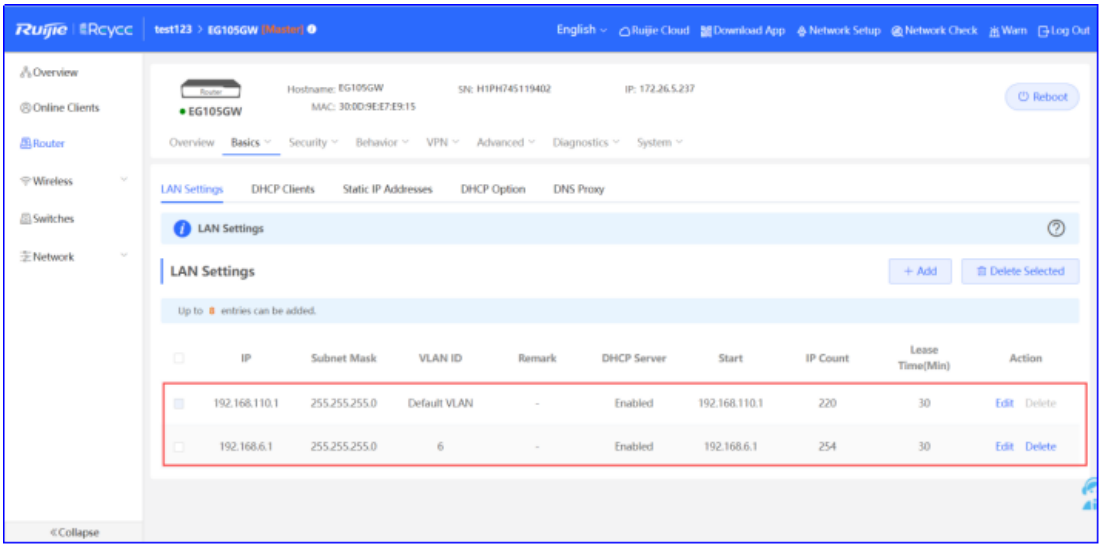
(1) Configure the basic network.

a Choose **Router** > **Basics** > **LAN** > **LAN Settings** > **Add**. Configure LAN settings and a DHCP pool for VLAN 1 and VLAN 6 on the EG.


test123 > EG105GW [Master]
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
EG105GW
Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: H1PH745119402
IP: 172.26.5.237
Reboot
Overview
Basics
Security
Behavior
VPN
Advanced
Diagnostics
System
LAN Settings
DHCP Clients
Static IP Addresses
DHCP Option
DNS Proxy
LAN Settings
LAN Settings
+ Add
Delete Selected
Up to 8 entries can be added.
IP
Subnet Mask
VLAN ID
Remark
DHCP Server
Start
IP Count
Lease Time(Min)
Action
192.168.110.1
255.255.255.0
Default VLAN
-
Enabled
192.168.110.1
220
30
Edit
Delete


Edit
* IP
192.168.110.1
* Subnet Mask
255.255.255.0
Remark
Remark
* MAC
30:0d:9e:e7:e9:15
DHCP Server
* Start
192.168.110.1
* IP Count
220
* Lease Time(Min)
30
DNS Server
192.168.110.1
Cancel
OK

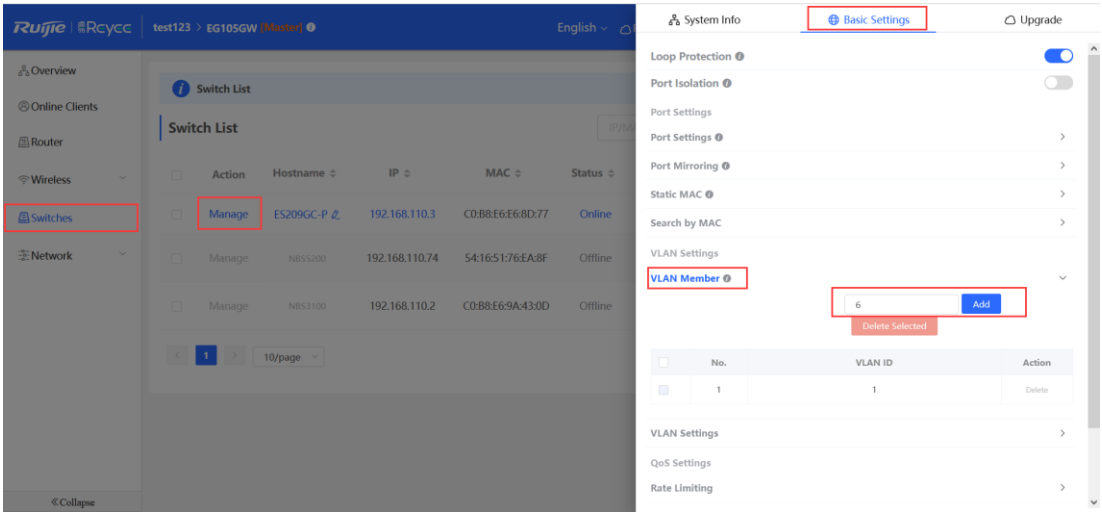


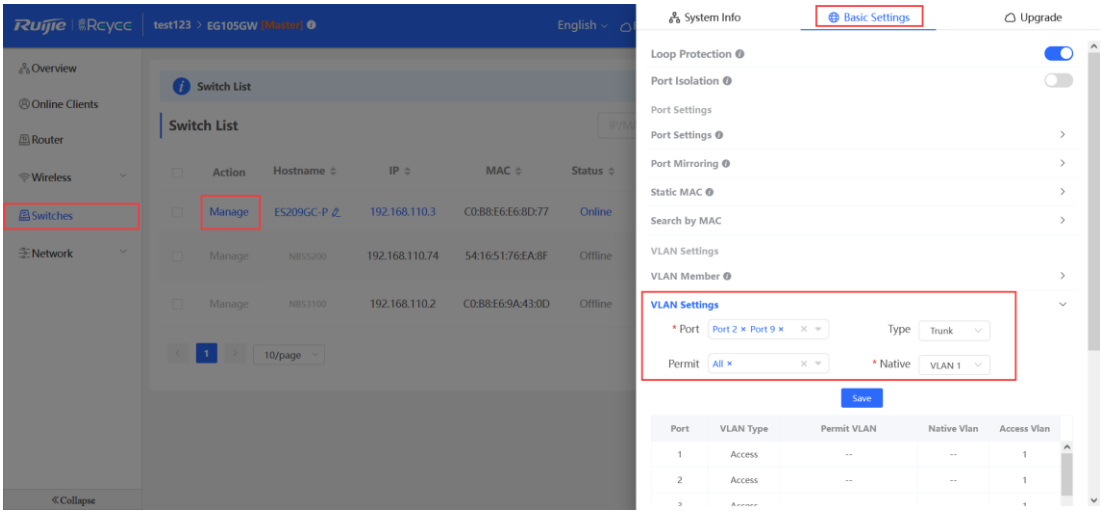


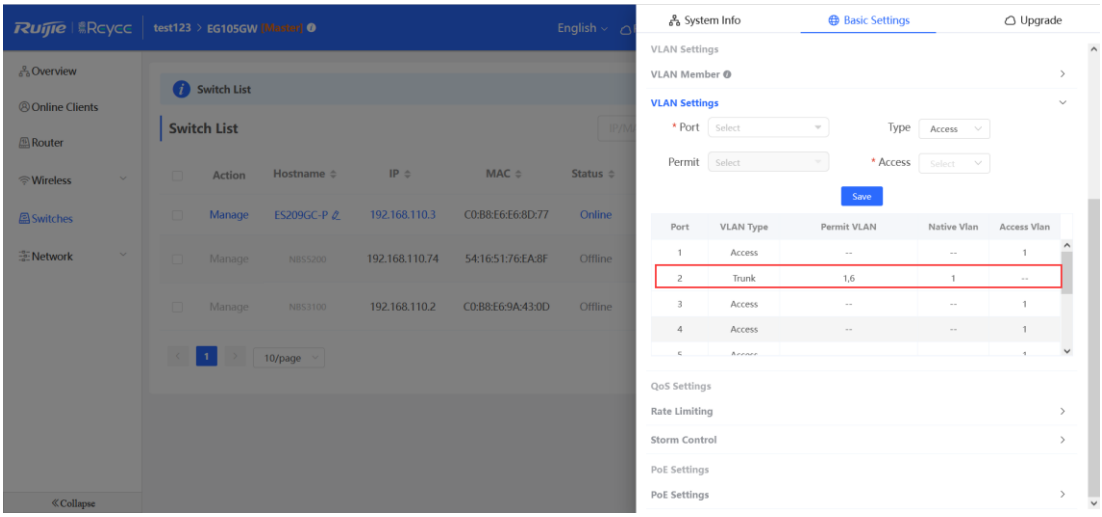
Instruction

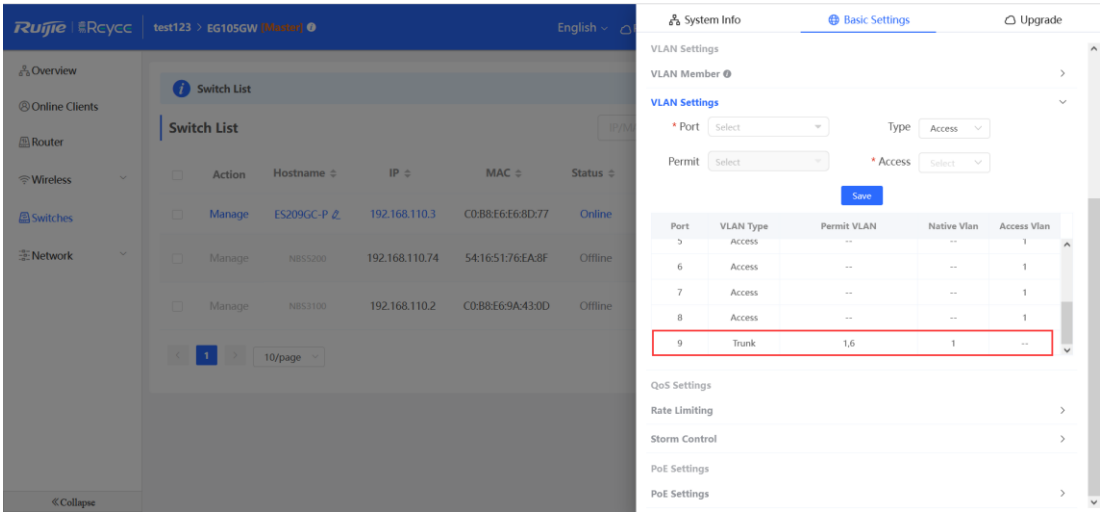
The network segment 192.168.110.0/24 is configured for VLAN 1.

b Choose **Switches** > **Manage** > **Basic Settings** > **VLAN Member** to create VLAN 6 on the switch, and click **VLAN Settings** to configure port 2 and port 9 connected to the AP and EG as trunk ports and allow packets from VLAN 1 and VLAN 6 to pass through. Then check port settings on the switch.

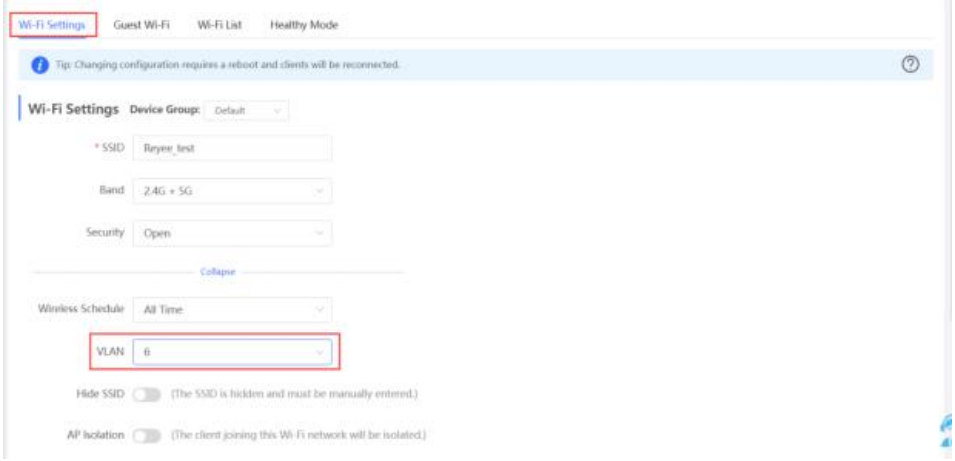

test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Switch List
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
Manage
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
Manage
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
Offline
10/page
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
6
Add
Delete Selected
No.
VLAN ID
Action
1
1
Delete
VLAN Settings
QoS Settings
Rate Limiting

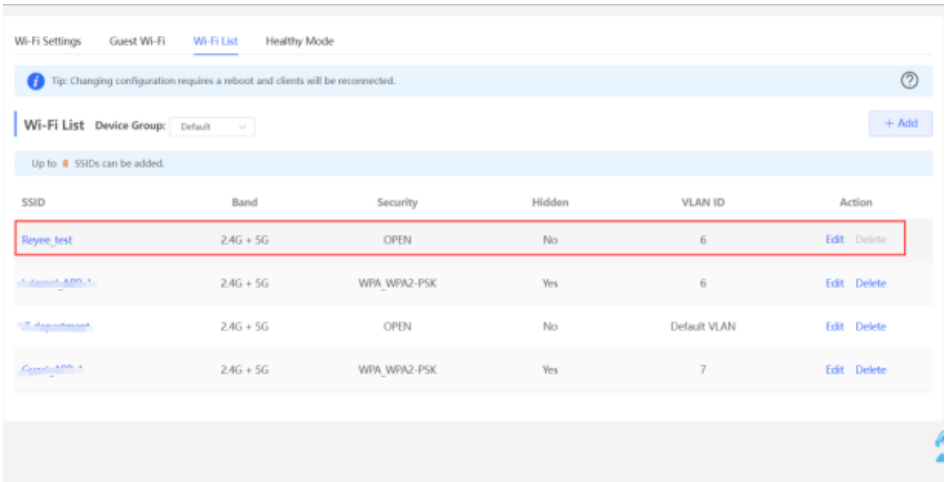

test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Switch List
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
Manage
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
Manage
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
Offline
10/page
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
VLAN Settings
* Port
Port 2 × Port 9 ×
Type
Trunk
Permit
All ×
* Native
VLAN 1
Save
Port
VLAN Type
Permit VLAN
Native Vlan
Access Vlan
1
Access
--
--
1
2
Access
--
--
1


test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Switch List
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
Manage
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
Manage
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
Offline
10/page
System Info
Basic Settings
Upgrade
VLAN Settings
VLAN Member
VLAN Settings
* Port
Select
Type
Access
Permit
Select
* Access
Select
Save
Port
VLAN Type
Permit VLAN
Native Vlan
Access Vlan
1
Access
--
--
1
2
Trunk
1,6
1
--
3
Access
--
--
1
4
Access
--
--
1
QoS Settings
Rate Limiting
Storm Control
PoE Settings
PoE Settings



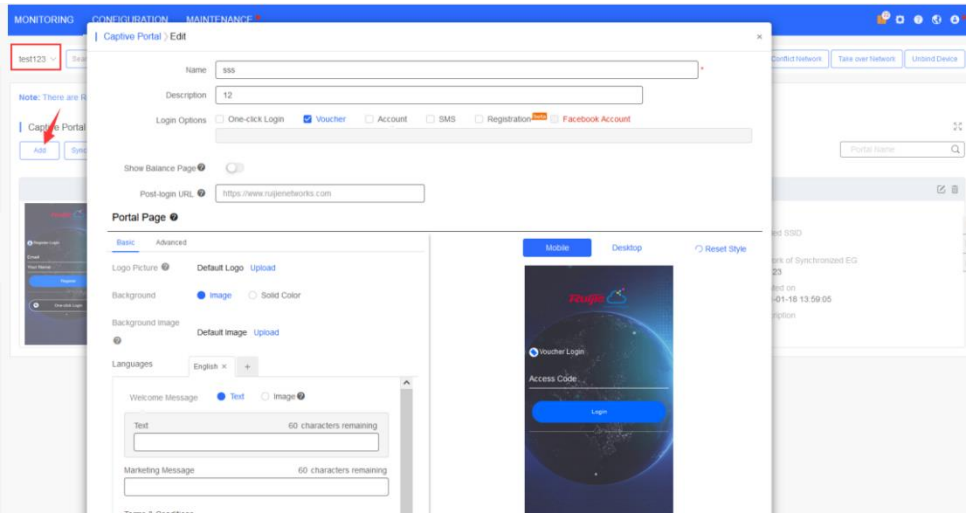
c Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**, configure a SSID named **Reyee test** and associate VLAN 6 with the SSID.

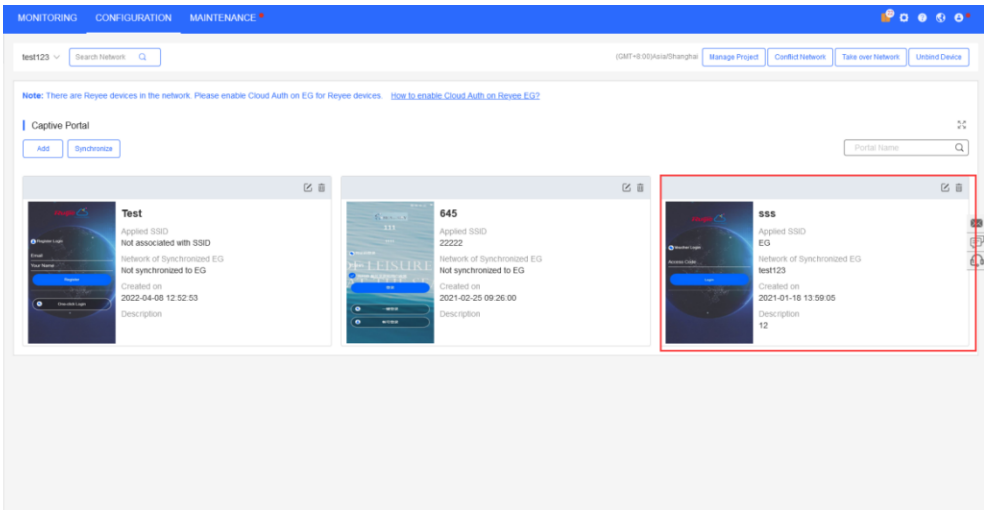




(2) Configure cloud authentication.

a Choose **CONFIGURATION** > **AUTHENTICATION** > **Captive Portal** to access the **Captive Portal** page, select a network in this account, and click **Add** to create a new portal template and edit the captive portal template.



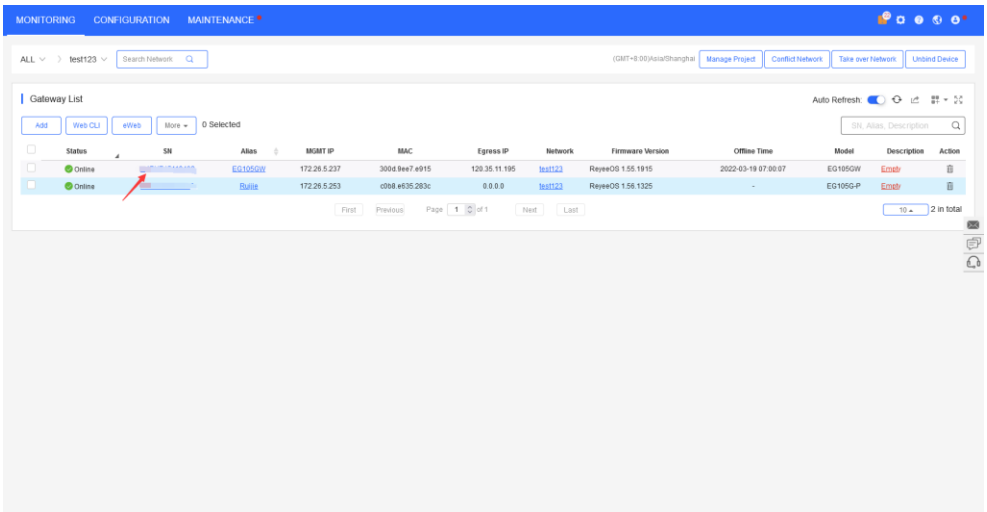


One-click Login: Log in without the username and password. **Access Duration** and **Access Times per day** can be configured.

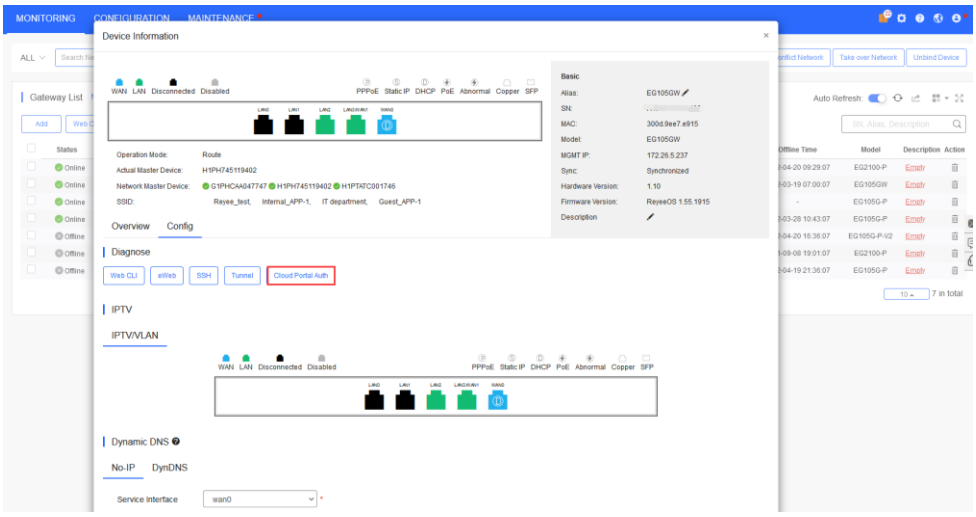
Voucher: Log in with a random eight-digit password.

Account: Log in with the account and password.

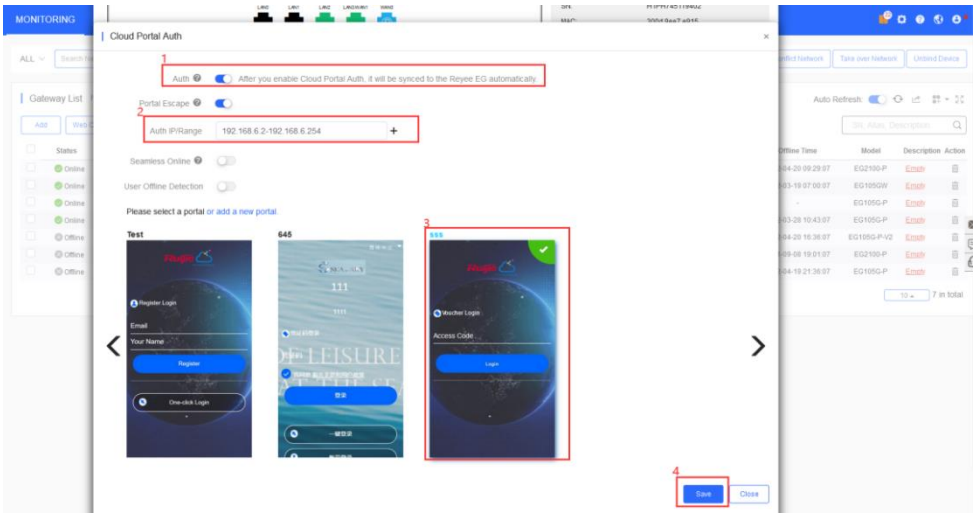
b Choose **MONITORING > DEVICE** > **Gateway**. Ensure that the Reyee EG is online on Ruijie Cloud and click its SN in the list to access the configuration page.



c Click **Cloud portal Auth** to configure authentication on Ruijie Cloud.



d Enable **Auth**, set **Auth IP Range 192.168.6.2-192.168.6.254** for authentication, and select a portal template to be used. Then click **Save** to save all configurations.

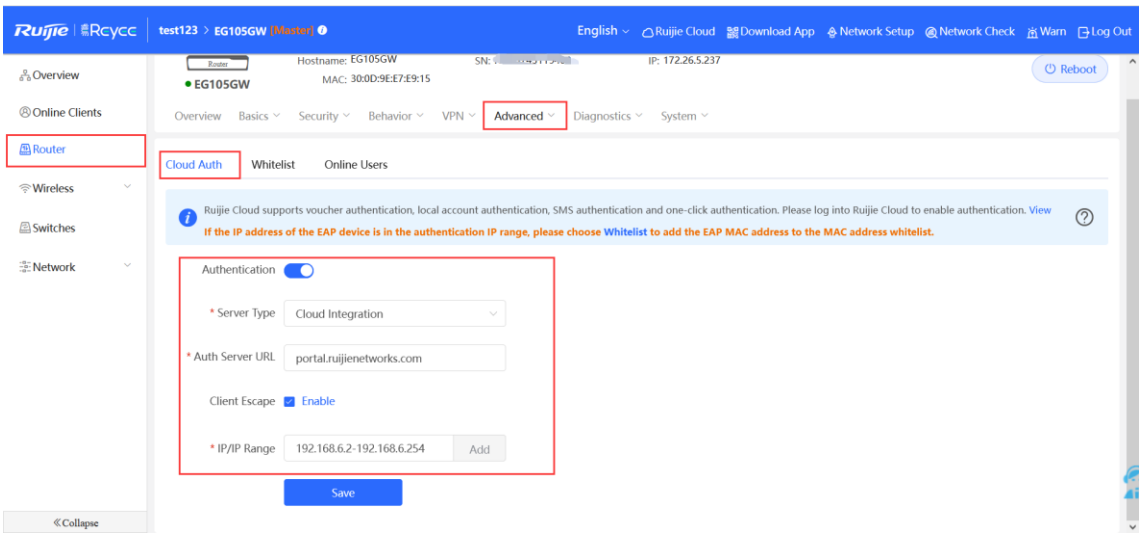


Note

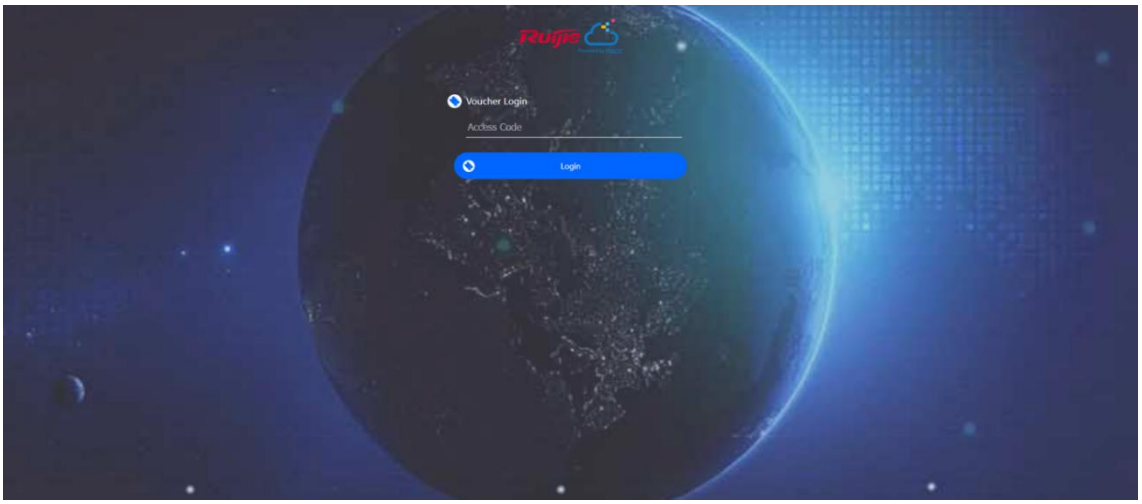
The IP addresses of the EG, switch, and AP need to be excluded; otherwise, the EG, switch, and AP cannot access the Internet.

Configuration Verification

Choose **Router** > **Advanced** > **LAN** > **Authentication** > **Cloud Auth**. Check whether the configuration is synchronized to the EG.



Users whose IP addresses are in the range from 192.168.6.2 to 192.168.6.254 IP need to be authenticated before accessing the Internet.



5.3 Reyee Guest Wi-Fi Solution

5.3.1 Working Principle

A single Internet entrance can be created by using guest Wi-Fi. The devices that are allowed to access guest Wi-Fi can access the Internet but cannot access the home Wi-Fi.

5.3.2 Application Scenario

Guest Wi-Fi provides secure Wi-Fi access for guests to share your home or office network. When someone visits your house, apartment, or workplace, you can enable guest Wi-Fi for them. You can set different access options for guest users, ensuring security and privacy of the main network.

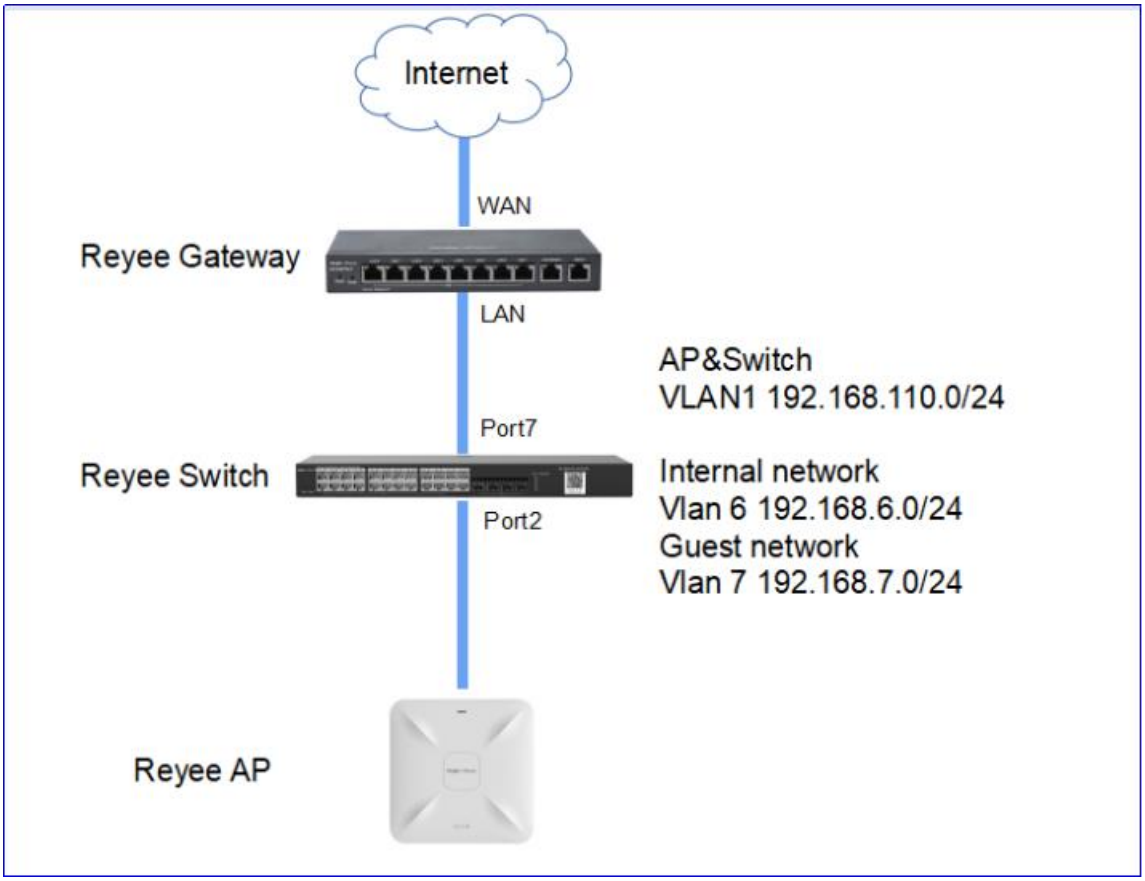
5.3.3 Configuration Case

1. Configuration Through EG's Eweb

Requirement

Guest Wi-Fi needs to be configured for guests in VLAN 7, so the guests are not allowed to access the internal network in VLAN 6.

Network Topology



Network Description:

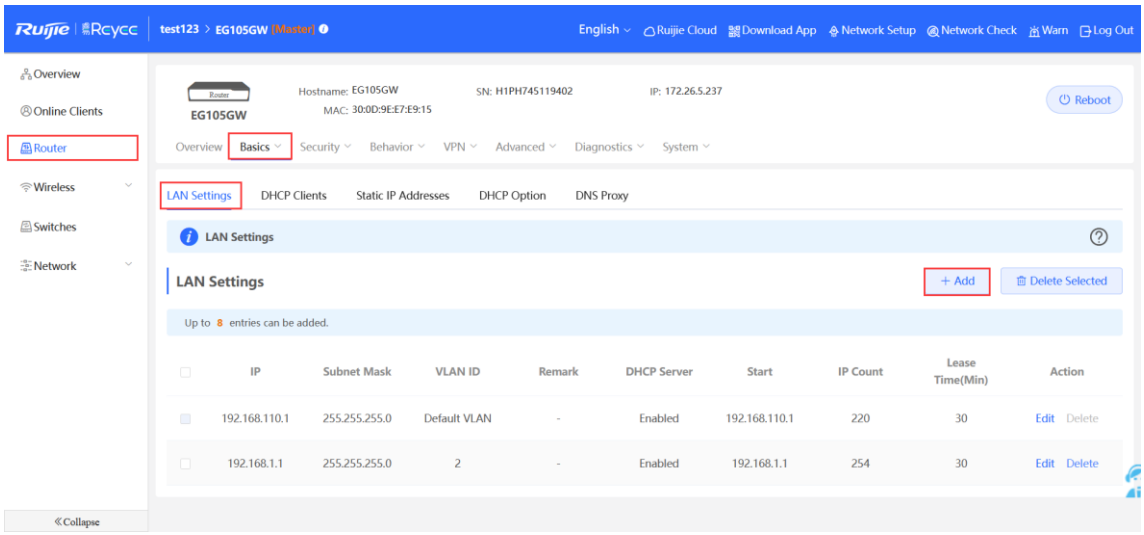
The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

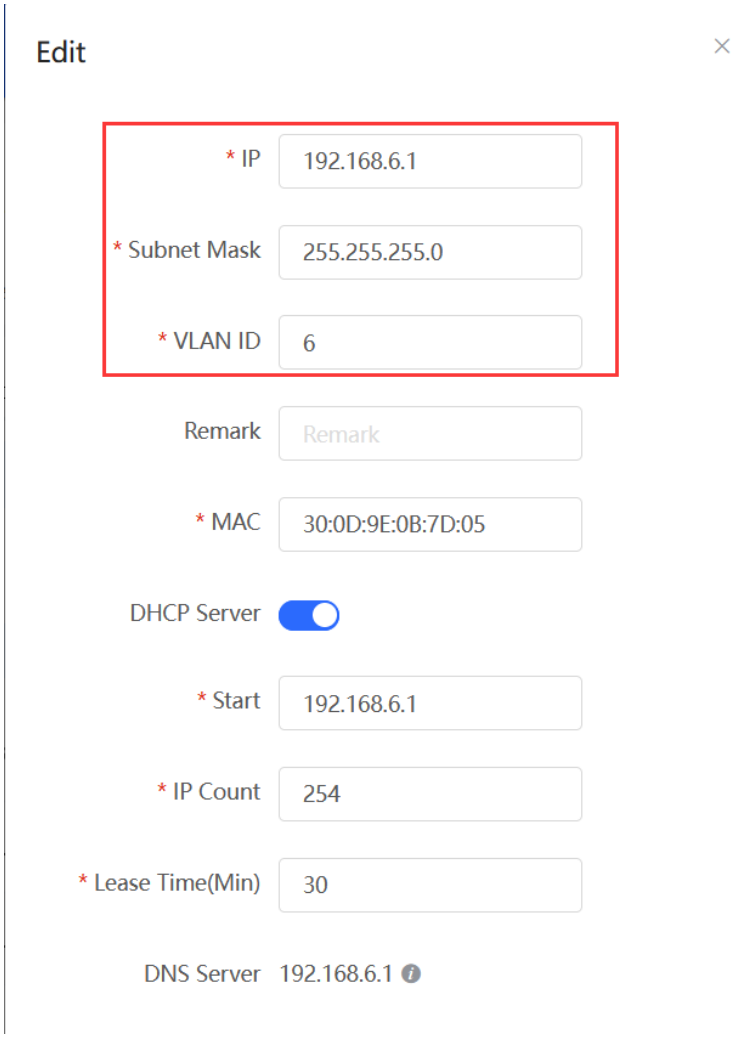
The AP and switch obtain IP addresses in VLAN 1 for Internet access.

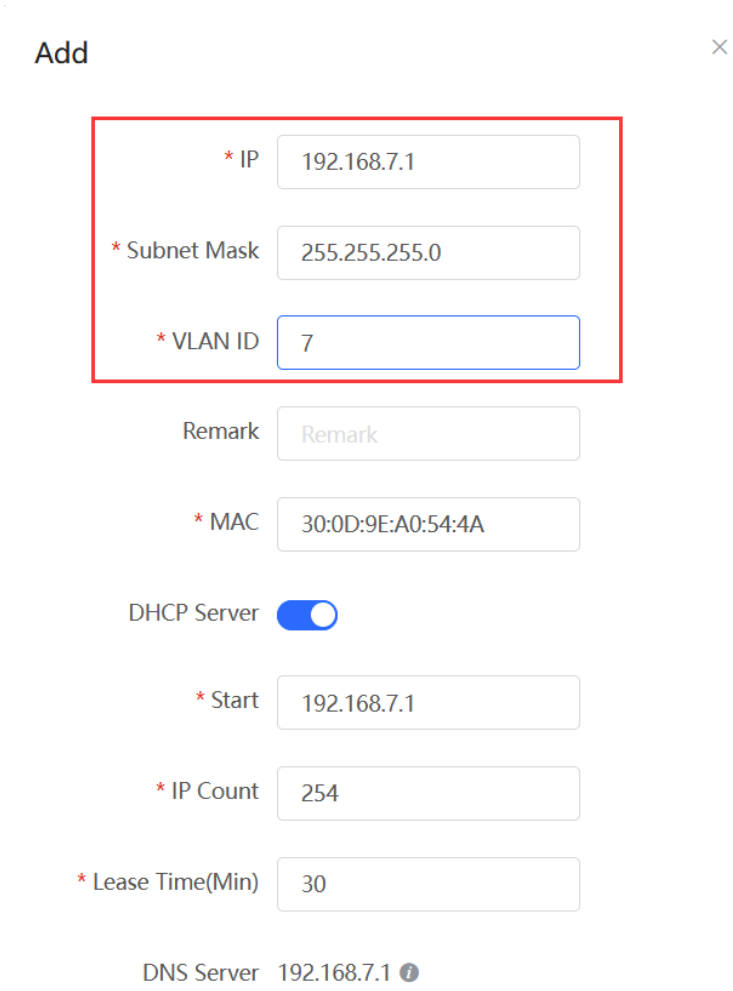
Internal users obtain IP addresses on the network segment in VLAN 6 for Internet access, and guests obtain IP addresses on the network segment in VLAN 7 for Internet access.

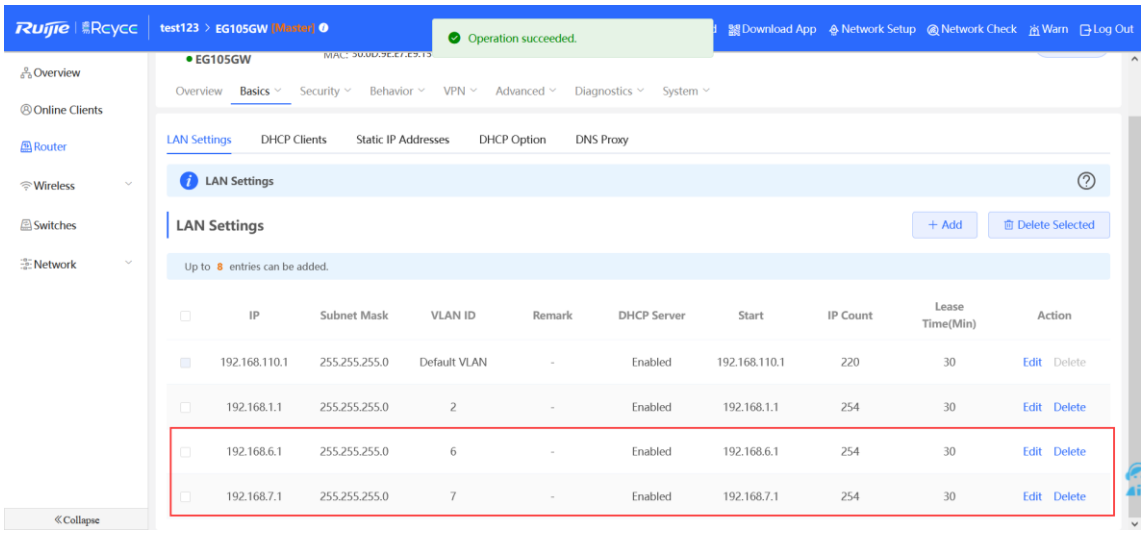
Configuration Steps

(1) Choose **Router** > **Basics** > **LAN** > **LAN Settings** > **Add**. Configure LAN settings and a DHCP pool for VLAN 6 and VLAN 7 on the EG.

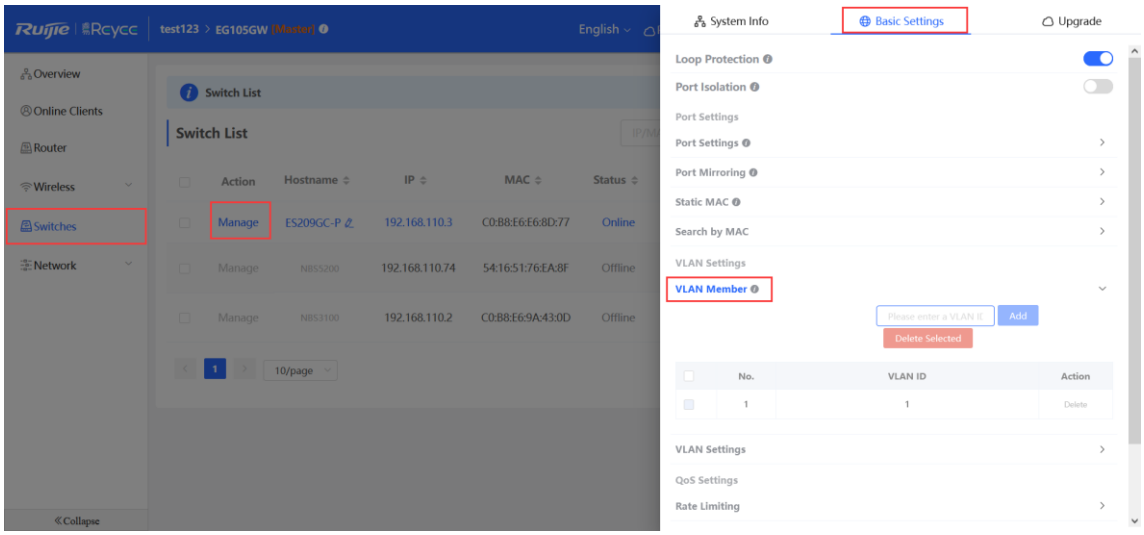


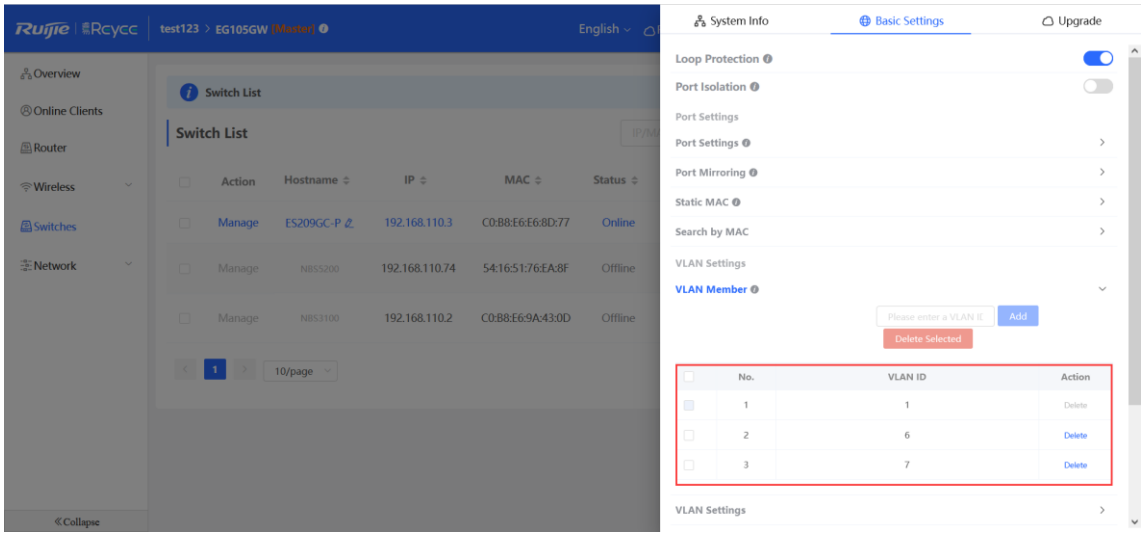


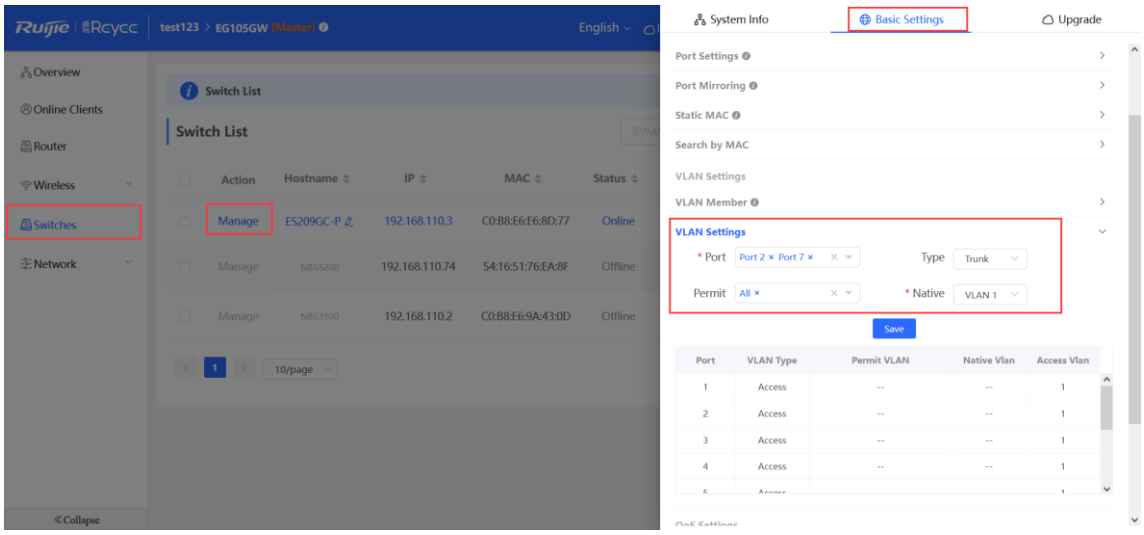


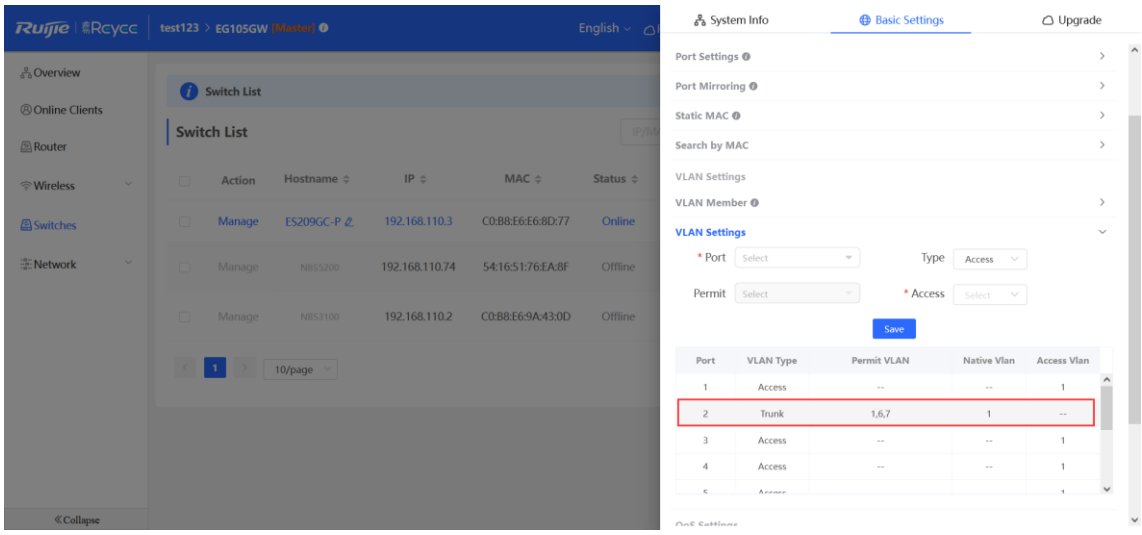


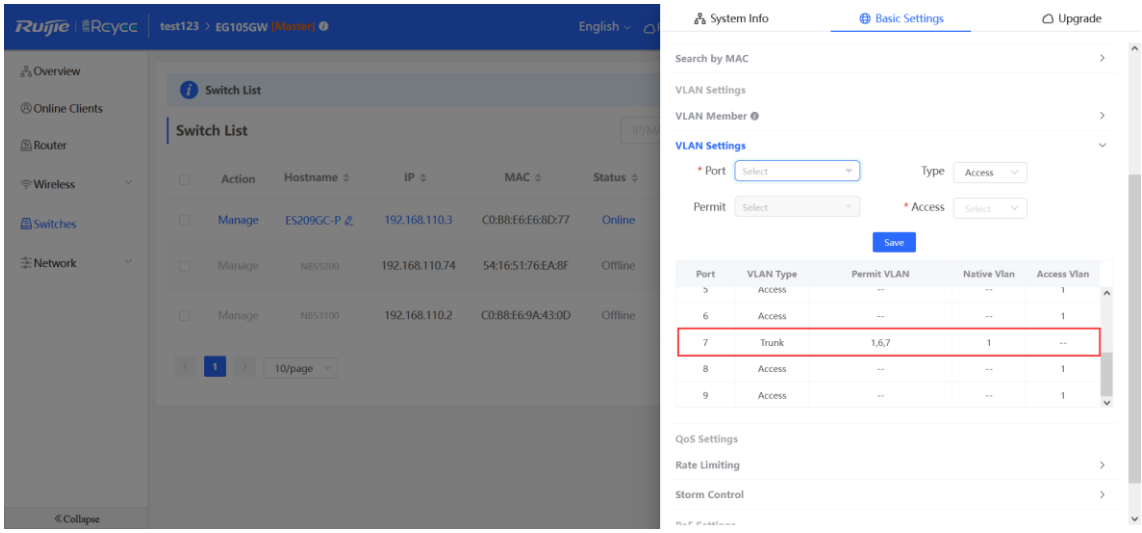
(2) Choose **Switches** > **Manage** > **Basic Settings** > **VLAN Member** to create VLAN 6 and VLAN 7 on the switch, and click **VLAN Settings** to configure port 2 and port 7 connected to the AP and EG as trunk ports and allow packets from VLAN 1, VLAN 6, and VLAN 7 to pass through. Then check port settings on the switch.


test123 > EG105GW [Master]
English
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
192.168.110.74
54:16:51:76:EA:8F
Offline
192.168.110.2
C0:B8:E6:9A:43:0D
10/page
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
Add
Delete Selected
No.
VLAN ID
Action
Delete
QoS Settings
Rate Limiting

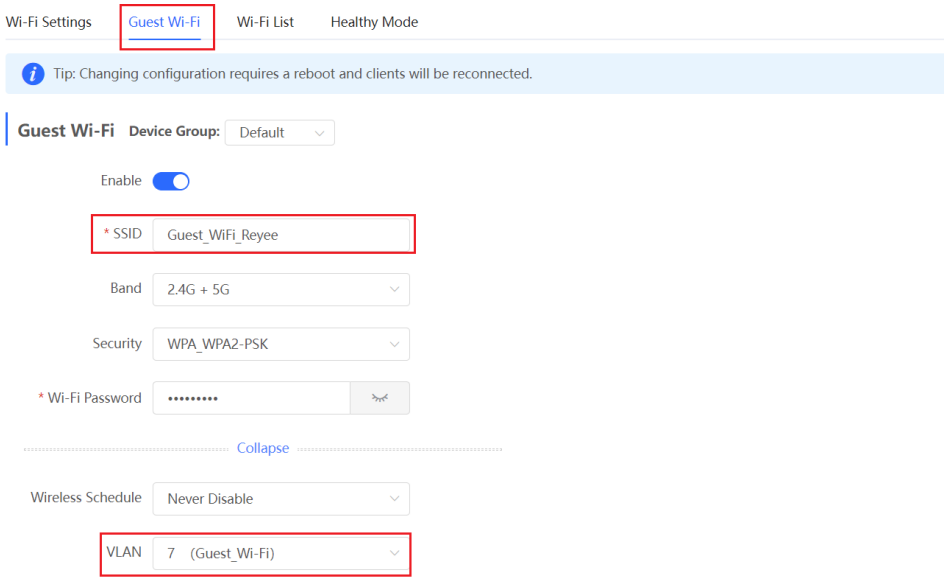

test123 > EG105GW [Master]
English
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
192.168.110.74
54:16:51:76:EA:8F
Offline
192.168.110.2
C0:B8:E6:9A:43:0D
10/page
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
Add
Delete Selected
No.
VLAN ID
Action
1
1
2
6
3
7
Delete


test123 > EG105GW [Master]
English
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
192.168.110.74
54:16:51:76:EA:8F
Offline
192.168.110.2
C0:B8:E6:9A:43:0D
10/page
System Info
Basic Settings
Upgrade
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
VLAN Settings
* Port
Port 2 × Port 7 ×
Type
Trunk
Permit
All ×
* Native
VLAN 1
Save
Port
VLAN Type
Permit VLAN
Native Vlan
Access Vlan
Access

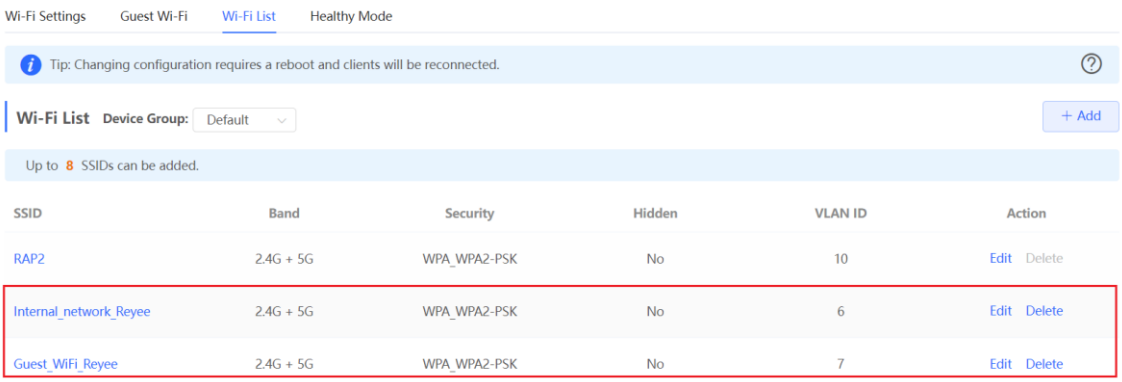




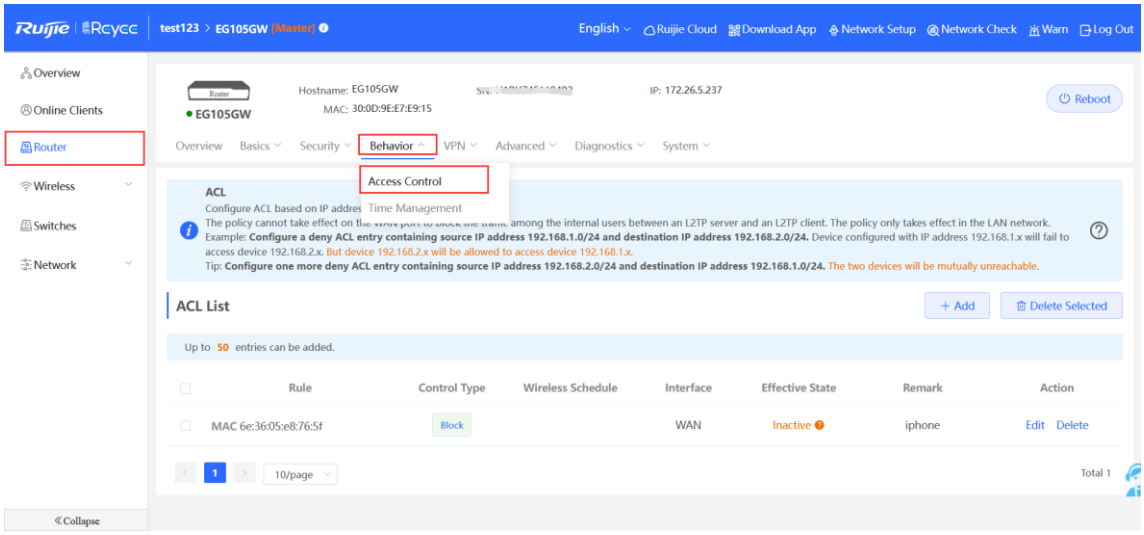
(3) Choose **WLAN > Wi-Fi > Guest Wi-Fi**, configure a guest Wi-Fi SSID named **Guest_WiFi_Reyee** and associate VLAN 7 with the SSID.

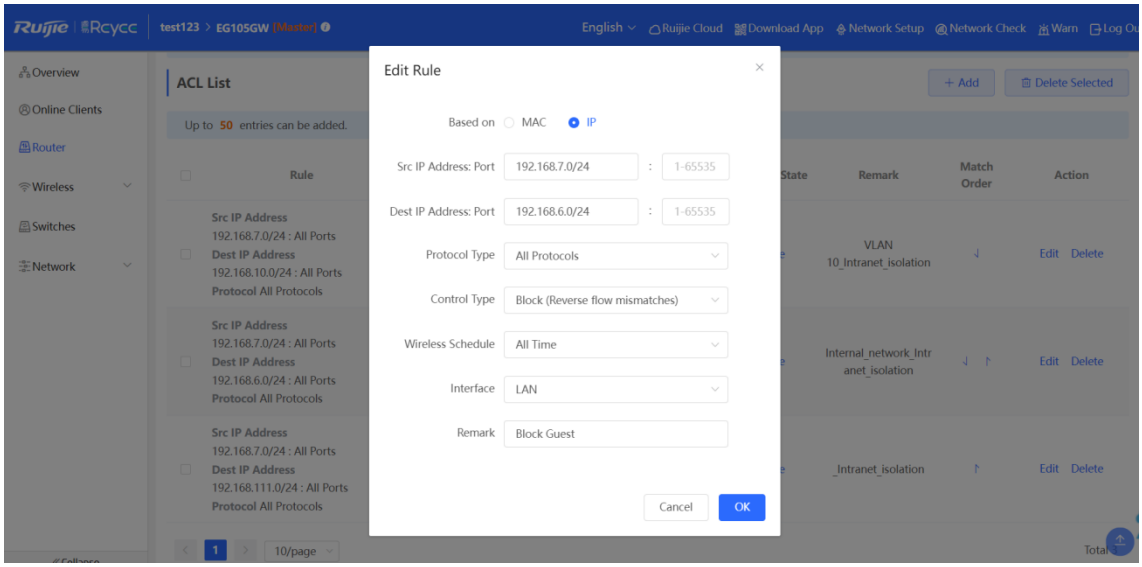


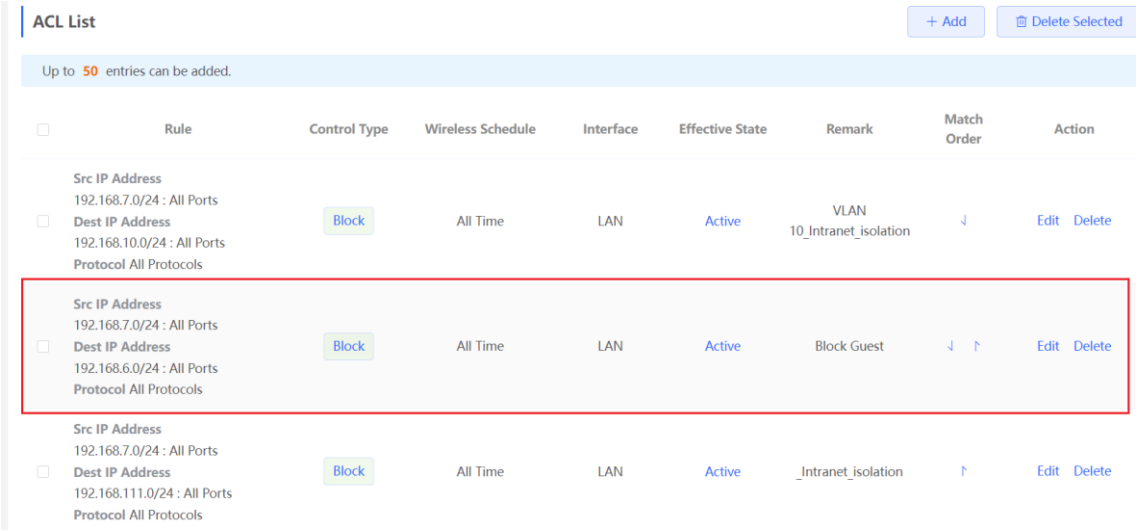
(4) Choose **WLAN** > **Wi-Fi** > **Wi-Fi List** > **Add**, configure the SSID named **Internal_network_Reyee** for internal users, configure VLAN6 for this SSID, and check Wi-Fi settings in **Wi-Fi List**.



(5) Choose **Router** > **Behavior** > **Access Control**, configure an ACL to block traffic from guests on network segment 192.168.7.0/24 in VLAN 7 to internal users on network segment 192.168.6.0/24 in VLAN 6, and apply the ACL to a LAN interface on the EG.







Configuration Verification

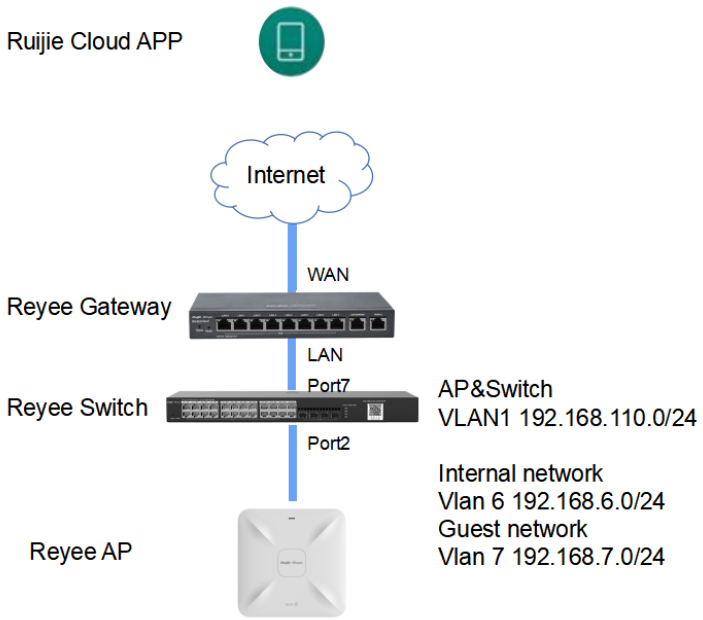
Guests at 192.1687.2 cannot access the internal users at 192.168.6.2.

2. Configuration Through Ruijie Cloud App

Requirement

Guest Wi-Fi needs to be configured through Ruijie Cloud App for guests in VLAN 7, so guests are not allowed to access the internal network in VLAN 6. Ruijie Cloud App will deliver the corresponding configuration to the gateway, switch, and AP automatically.

Network Topology



Network Description:

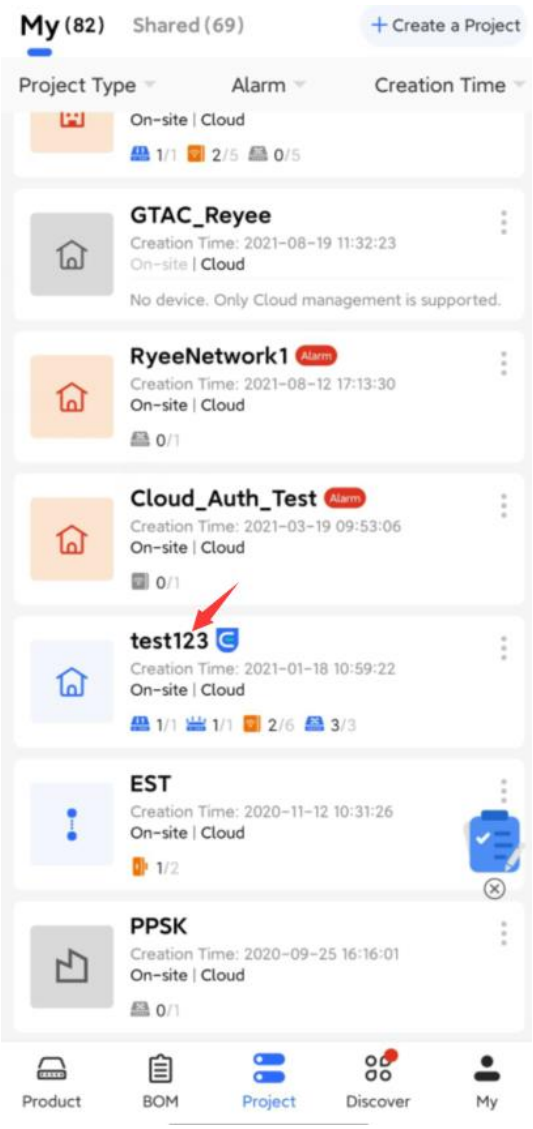
The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

The AP and switch obtain IP addresses in VLAN 1 for Internet access.

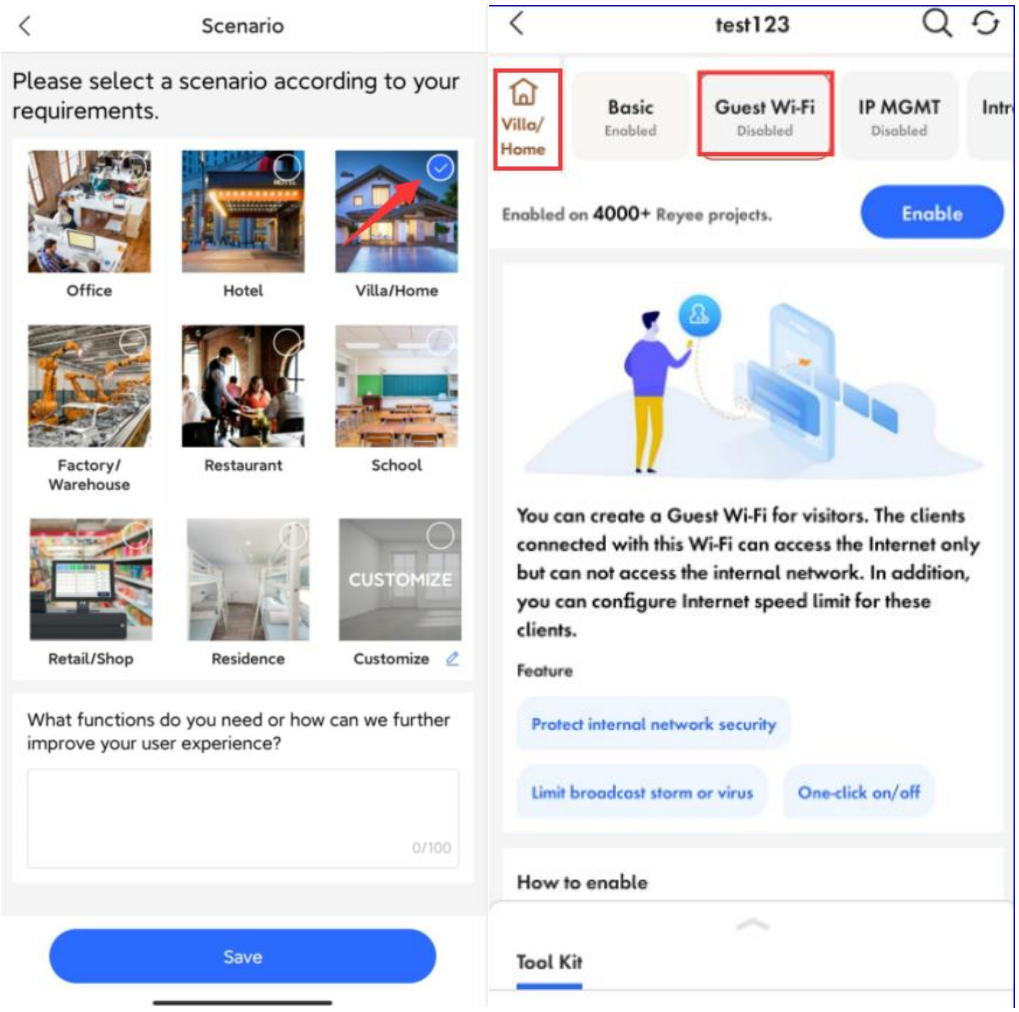
Internal users obtain IP addresses in VLAN 6 for Internet access, and guests obtain IP addresses in VLAN 7 for Internet access.

Configuration Steps

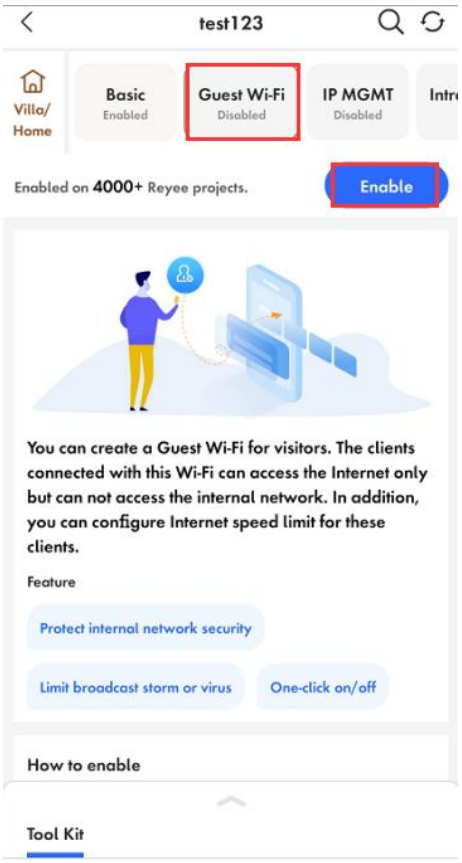
(1) Log in to your Ruijie Cloud App on your smartphone, and then access the project through Reyee gateway and RAP.



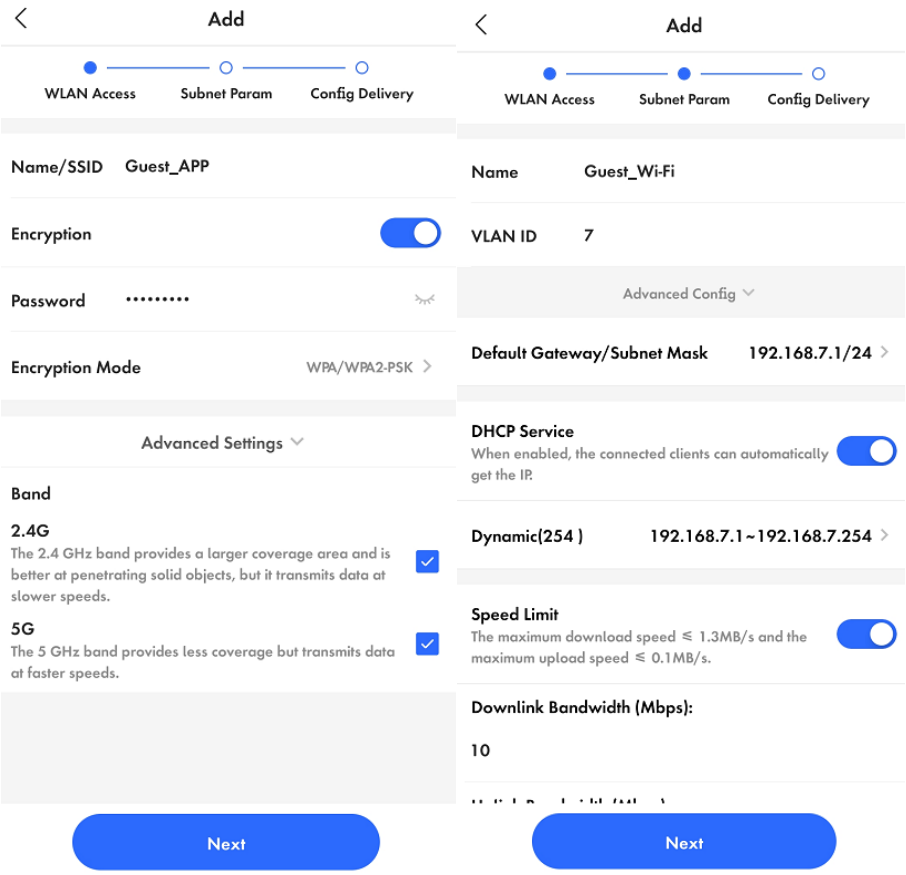
(2) Choose **Villa/Home**. Then you can check the **Guest Wi-Fi** button.



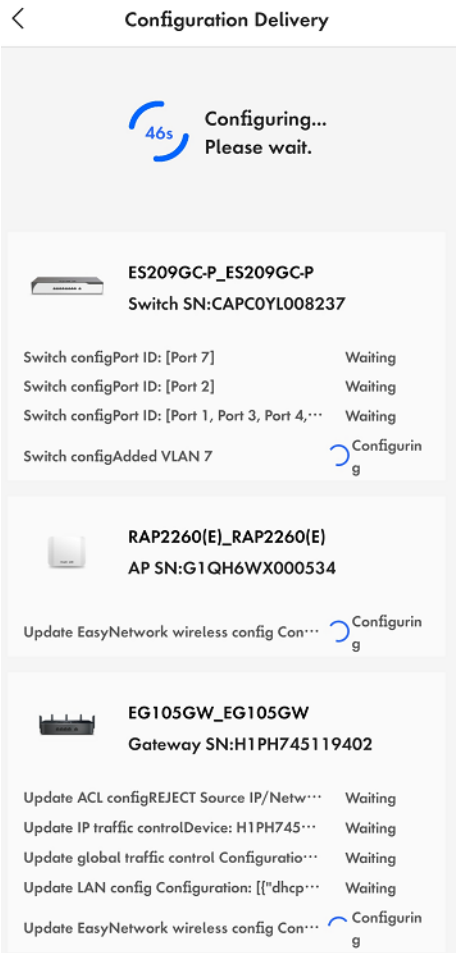
(3) Select **Guest Wi-Fi** and click **Enable**.

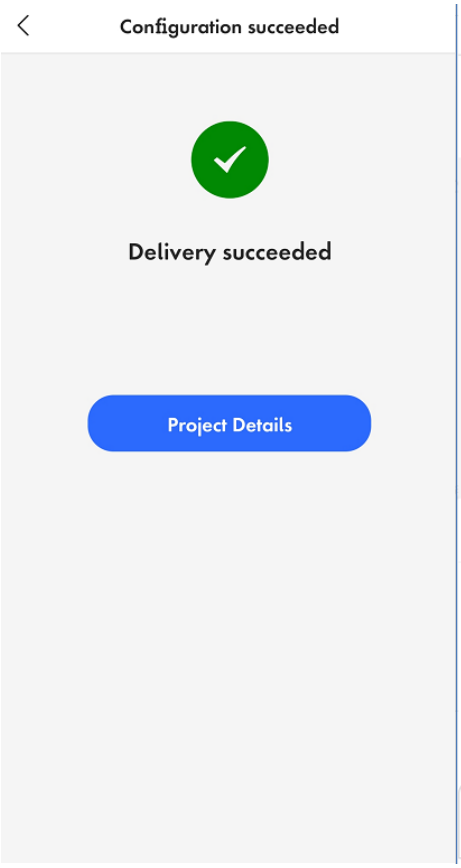


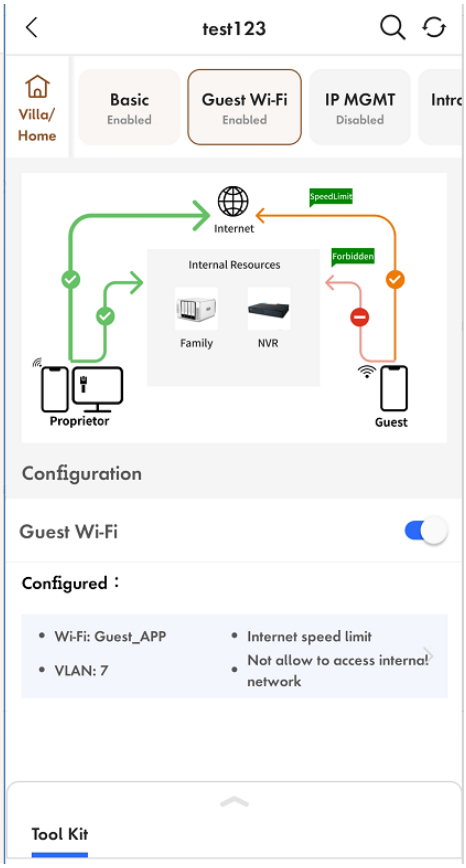
(4) Modify guest Wi-Fi information, configure an internal user SSID named **Guest_APP** and associate VLAN 6 with this SSID, configure a guest Wi-Fi SSID named **Guest_WiFi** and associate VLAN 7 with this SSID, and Click **Save** to save your configuration.



(5) Wait for about 1 minute for the system to deliver the configuration to the device.


Configuration Delivery
46s
Configuring...
Please wait.
ES209GC-P_ES209GC-P
Switch SN:CAPC0YL008237
Switch configPort ID: [Port 7] Waiting
Switch configPort ID: [Port 2] Waiting
Switch configPort ID: [Port 1, Port 3, Port 4,··· Waiting
Switch configAdded VLAN 7 Configuring
RAP2260(E)_RAP2260(E)
AP SN:G1QH6WX000534
Update EasyNetwork wireless config Con··· Configuring
EG105GW_EG105GW
Gateway SN:H1PH745119402
Update ACL configREJECT Source IP/Netw··· Waiting
Update IP traffic controlDevice: H1PH745··· Waiting
Update global traffic control Configuratio··· Waiting
Update LAN config Configuration: [{"dhcp··· Waiting
Update EasyNetwork wireless config Con··· Configuring


Configuration succeeded
Delivery succeeded
Project Details


test123
Villa/ Home
Basic Enabled
Guest Wi-Fi Enabled
IP MGMT Disabled
Internet
SpeedLimit
Internal Resources
Forbidden
Family
NVR
Proprietor
Guest
Configuration
Guest Wi-Fi
Configured :
Wi-Fi: Guest_APP
VLAN: 7
Internet speed limit
Not allow to access internal network
Tool Kit

Configuration Verification

The guest at 192.168.7.97 cannot access the internal user at 192.168.6.147.

5.4 Reyee SON

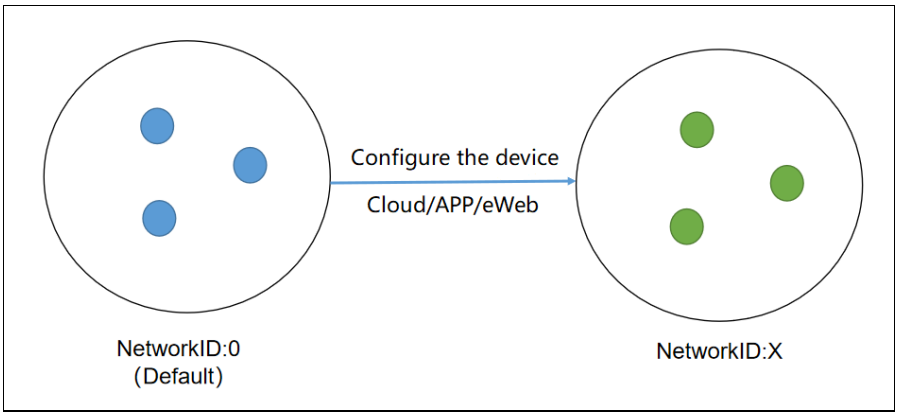
SON eliminates product limitations and realizes auto-discovery, auto-networking, and auto-configuration between routers, switches, and wireless APs without the need for controllers or Internet access. With mobile APP, you can quickly complete device deployment and configuration, remote management, O&M of the entire network, which greatly reduces the investment of the device, labor, and time cost during wireless network construction.

5.4.1 Working Mechanism of Reyee SON

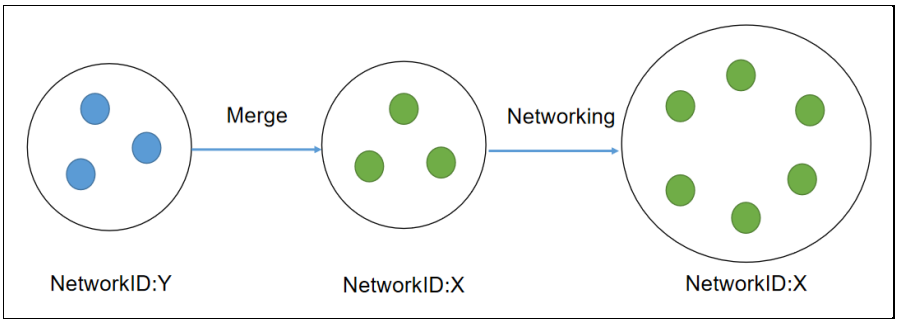
1. Network ID

Every device has its own network ID.
Only devices with the same network ID can be added to a network.
Different network IDs of devices are required to be merged before the devices are added to the same network.
The network ID is 0 by default.
After the device is configured, it will have a new network ID (non-zero value).

After configuration:



Merge:



2. Protocol

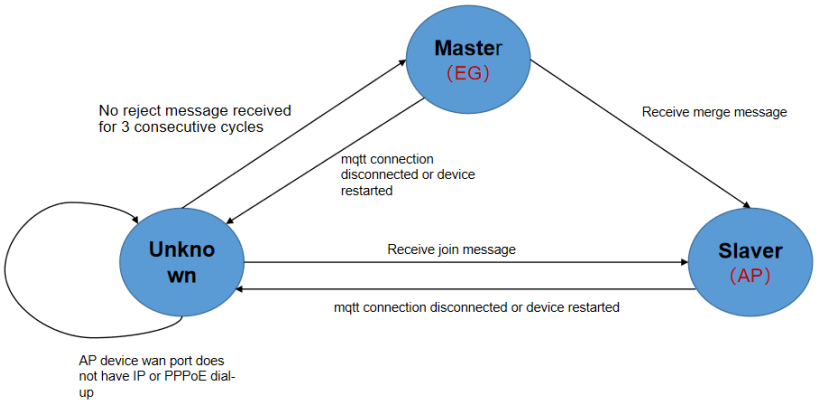
Easydisc

Easydisc provides neighbor discovery, master election, and notification of master changes. Easydisc is a proprietary protocol and uses UDP port numbers 43561 and 43562 for communication.

MQTT

MQTT collects information about network devices and STAs, and synchronizes the configuration.
MQTT is a standard protocol and uses TCP port number 1883 for communication.

3. Easydisc - Role



4. Easydisc - Packets

Packet types:

Declare: In Initial state, the device broadcasts Declare packets and sends its own priority and other related information.

Reject: When receiving a decade packet in unicast mode, the device with a higher priority sends a Reject packet according to the election priority.

Join: The Join packet is broadcast by the master. When other devices in initial state receive the packet, they will connect to the master according to master information in it.

Conflict: The master sends a Conflict packet in unicast mode when receiving a Join packet from another master. As a result, the slave cannot resolve the packet according to the conflict handling algorithm.

Merge: The master sends a Merge packet in unicast mode when receiving a Join packet from other master devices. In this case, the master combines Join packets from other masters according to the conflict handling algorithm.

Hello: All devices start broadcasting Hello packets after the role status is confirmed for neighbor discovery.

5. Master Election

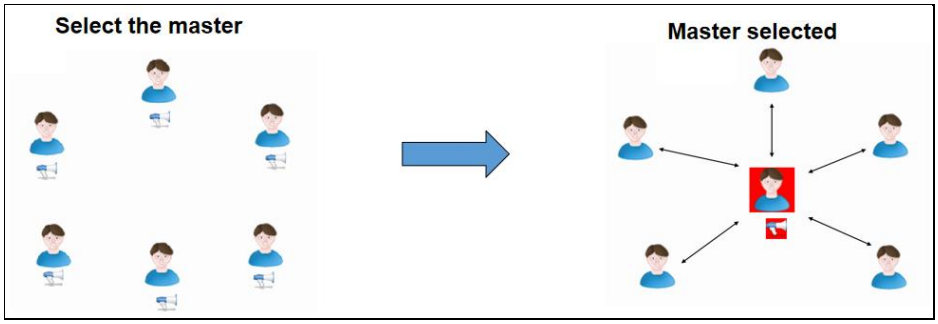
Priority:

(1) EG > AP > switch

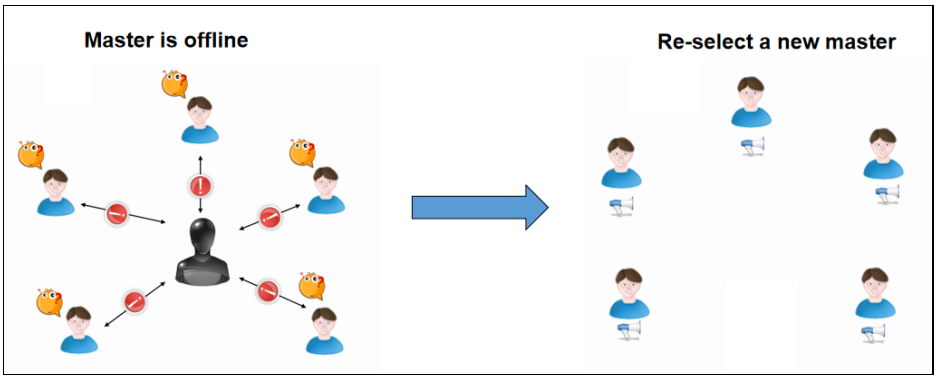
(2) Device model: device CPU/memory/other information (AP radio number)

(3) When the priorities are the same, the device with a larger MAC address will be the master.

Select the master.



Re-select the master.



6. Master Preemption Mechanism

If a device with a higher priority joins a network, the master device will change. The new device will send a Merge packet to the master device.

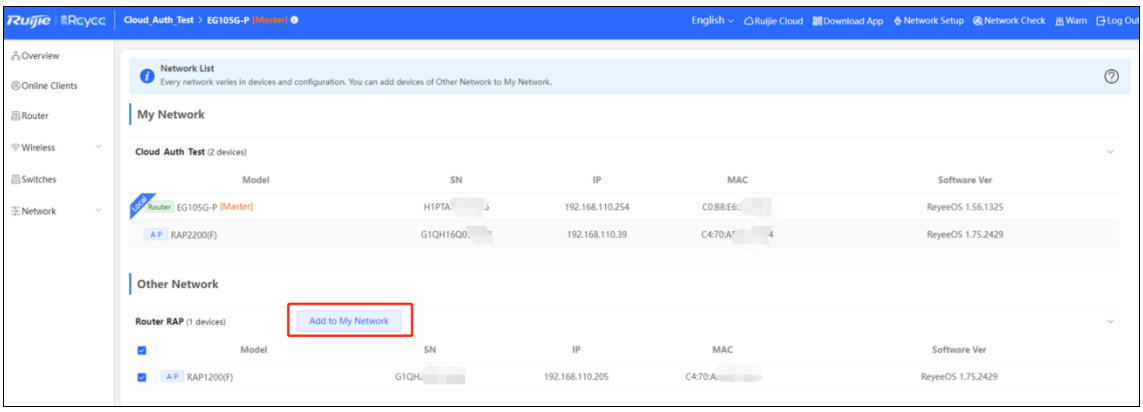
- For AP networking, after the master is selected, if a new EG is added, the EG will become the master.
  Preemption time: 7-8s
- For AP networking, after the master is selected, if a new AP with a higher priority is added, the preemption is delayed.

  Preemption time: Preemption starts after the master is powered on for 36 hours and the new device is powered on for 5 minutes. Otherwise, preemption starts after the new device is powered on for 30 minutes.
- For networking with the AP and switch, after the master is selected, if a new EG is added, the EG will become the master.

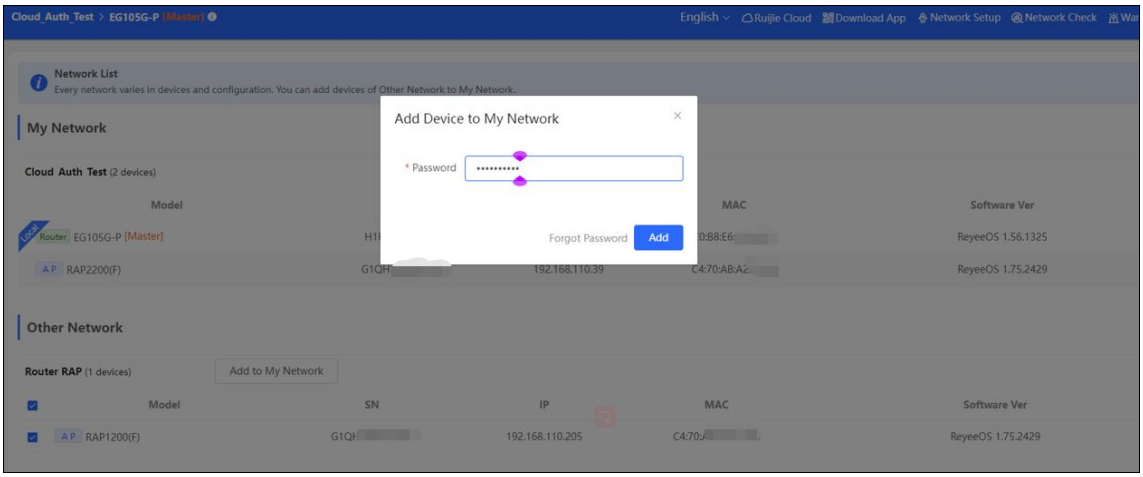
5.4.2 Reyee SON Configuration

1. Neighbor Discovery

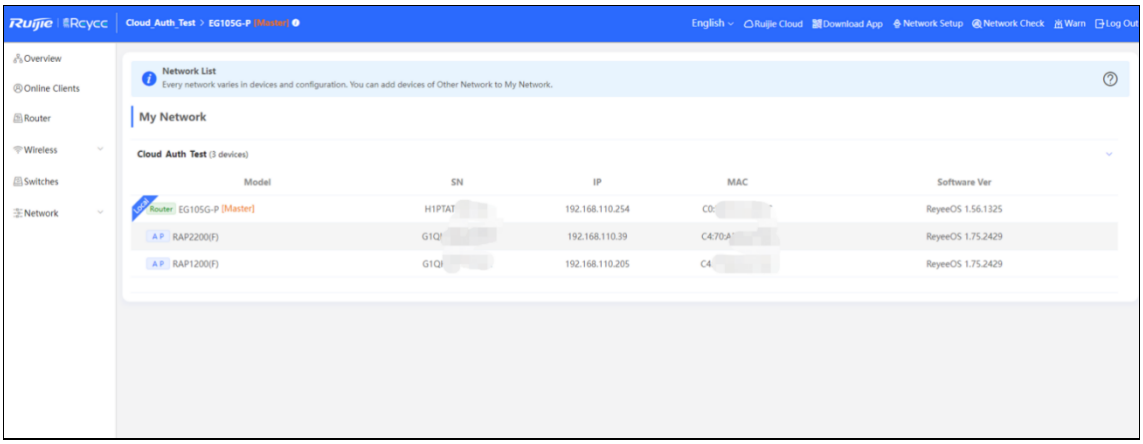
Add devices of other networks to **My Network**.



Enter the device password.

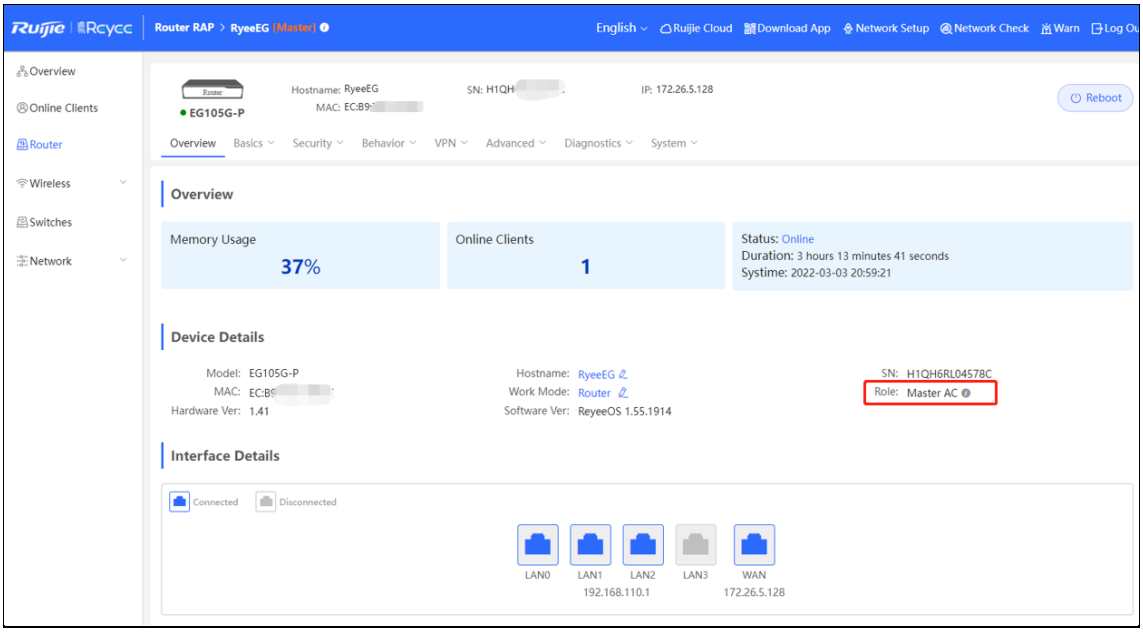


The device is added to the network.

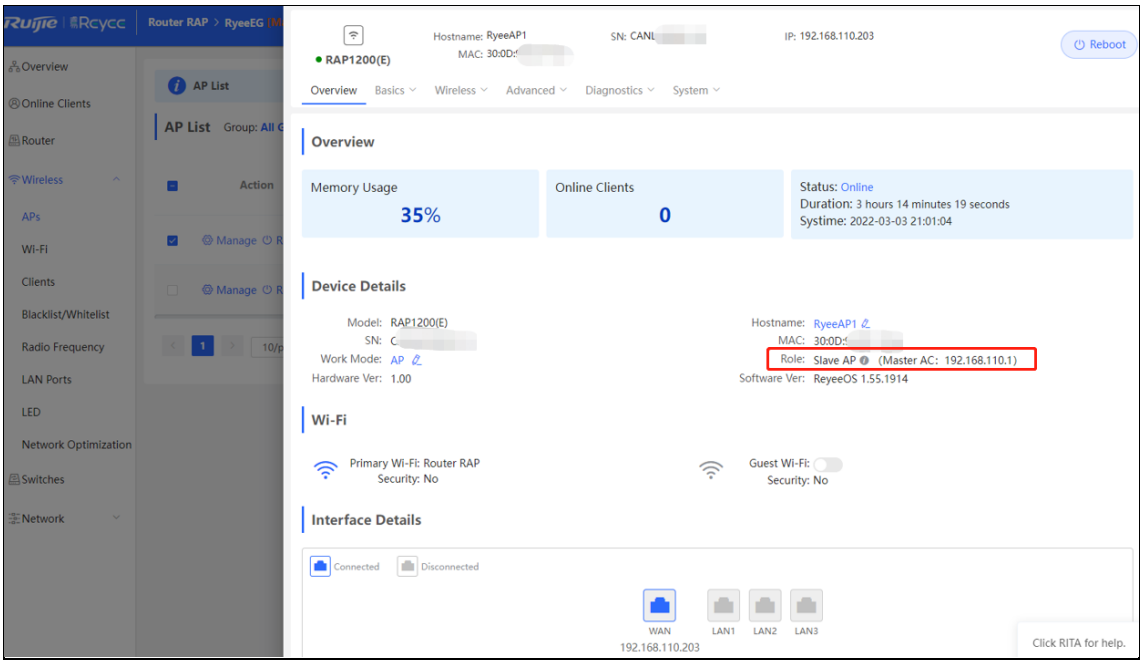


2. Device Networking Role

Master:



Slave:



5.4.3 SON Troubleshooting

Fault Symptom

The SON fails.

Cause

There are multiple masters, and more than one @Ruijie-mxxx SSID can be viewed.

Layer 2 broadcast becomes ineffective.

Solution

Check whether the devices are connected to and join the same network.

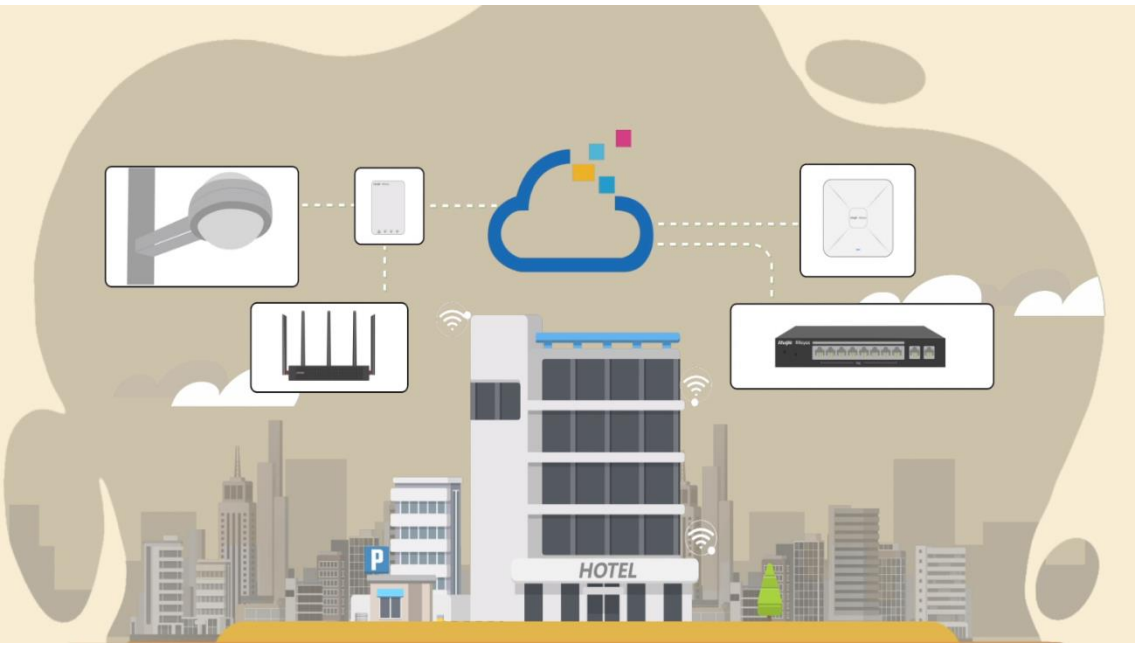
Check whether there are some configurations such as VLAN and port isolation.

Check whether the SON is disabled.

5.5 Reyee Economic Hotel Network Solution

5.5.1 Application Scenario

Reyee economic hotel network solution provides an affordable 5-star Wi-Fi for clients. The AP can operate concurrently at 2.4 GHz and 5 GHz, providing high-speed wireless access of 574 Mbit/s at 2.4 GHz, 1201 Mbit/s at 5 GHz, and up to 1775 Mbit/s. The wall AP provides a LAN port at the front to facilitate expansion of IPTV devices, IP phones, and other terminals.



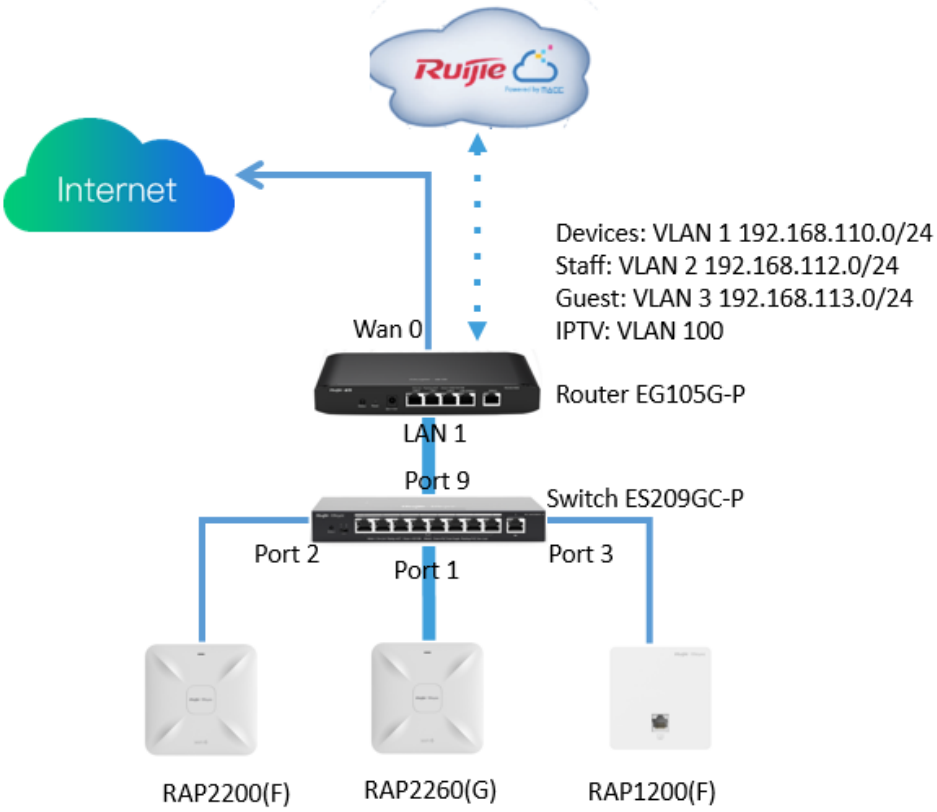
5.5.2 Configuration Case

Requirement

(1) On the wireless network for the hotel scenario, guests need to pass voucher authentication before accessing the Internet and are not allowed to access the internal network of the hotel.

(2) Wired connections are provided for IPTV.

Network Topology



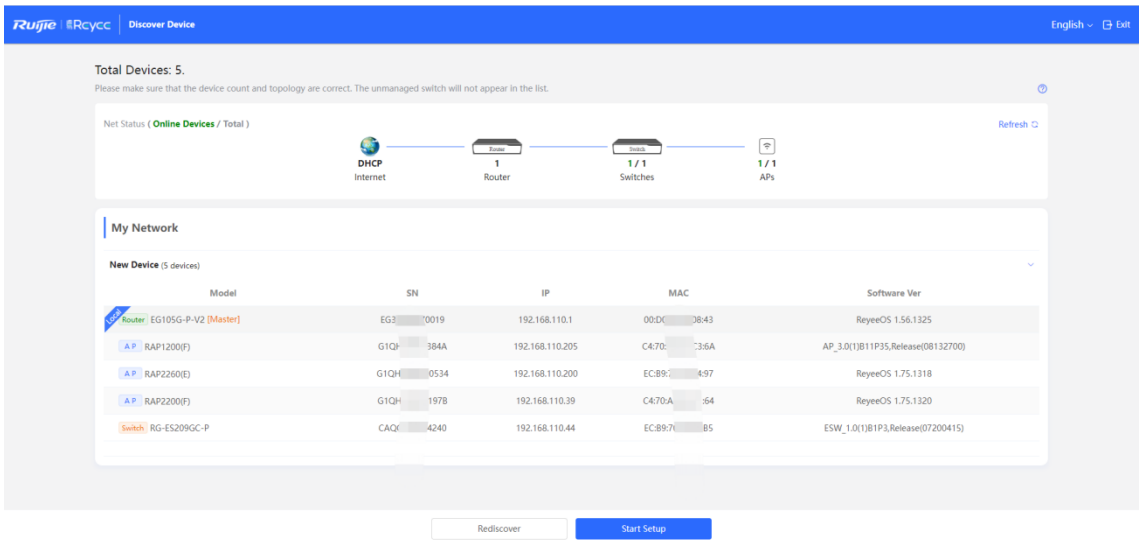
Devices List

Type	Model	Function
Gateway	EG105G-P	Connects to the Internet and works as the DHCP server for downlink devices and clients. Manages APs and switches locally. Supports voucher authentication with Ruijie Cloud.
Switch	ES209GC-P	Provides wired and PoE connections.
Wall AP	RAP1200(F)	Provides wireless connections for rooms. Provides wired connections for IPTV.
Indoor AP	RAP2200(F)&RAP2260(G)	Provides wireless connections for the hall and corridor.

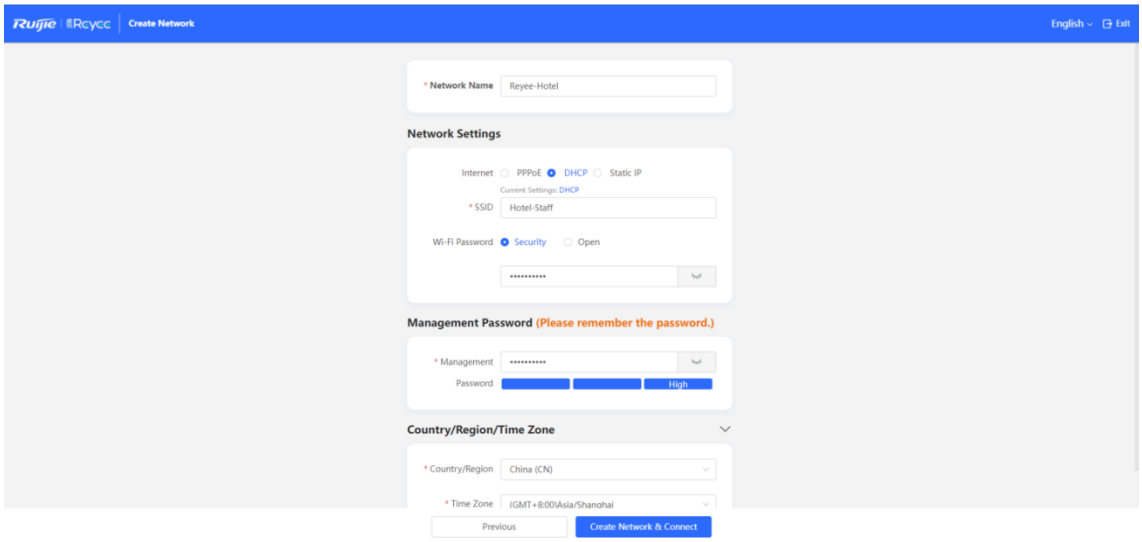
Configuration Steps

(1) Power on and connect to the device according to the topology.

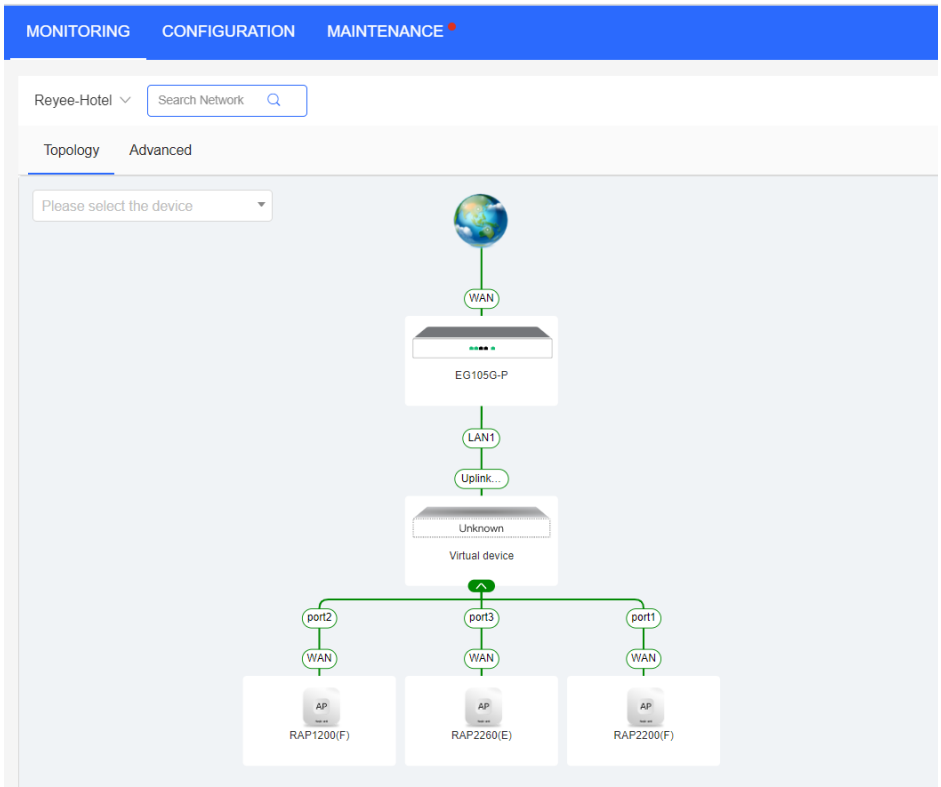
(2) The IP address of the access gateway is 192.168.110.1. Configure basic network settings according to **Start Setup**.



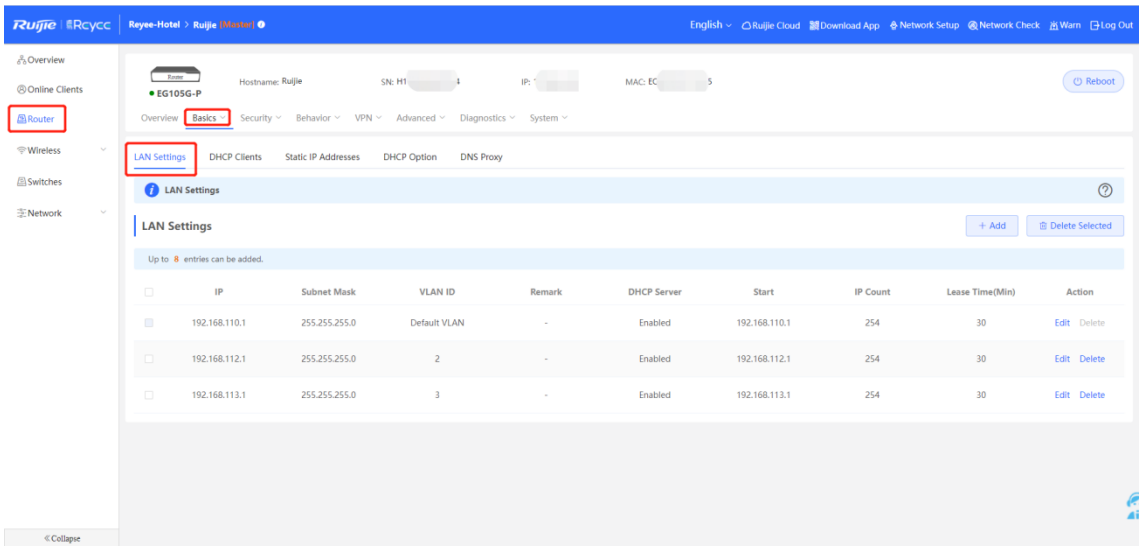
Set **Network Name**, **Network Settings**, and **SSID** for staffs and set **Management Password**.



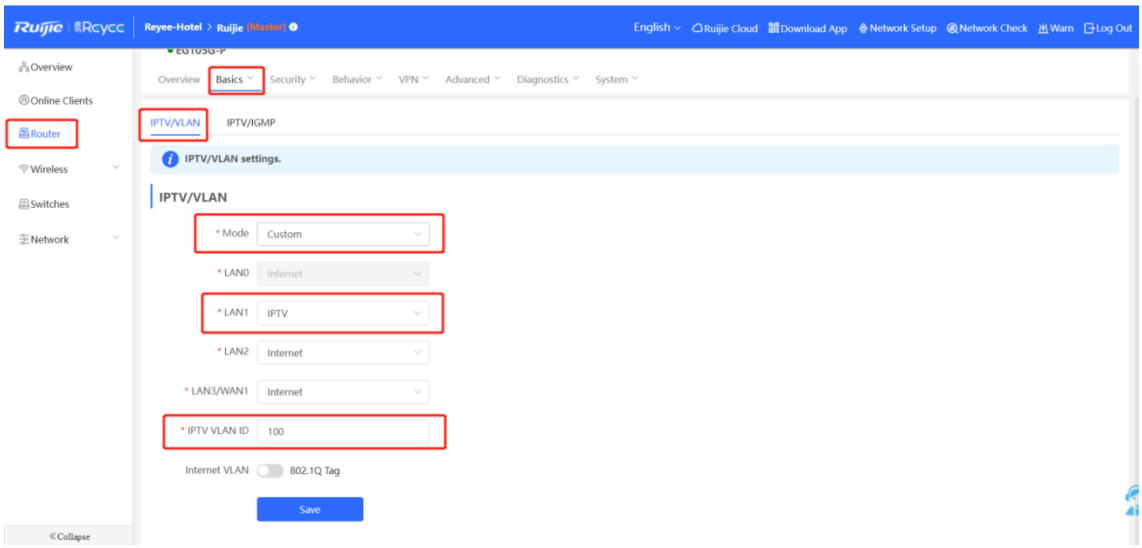
Click **Create Network & Connect** to activate the configuration and add devices to Ruijie Cloud.



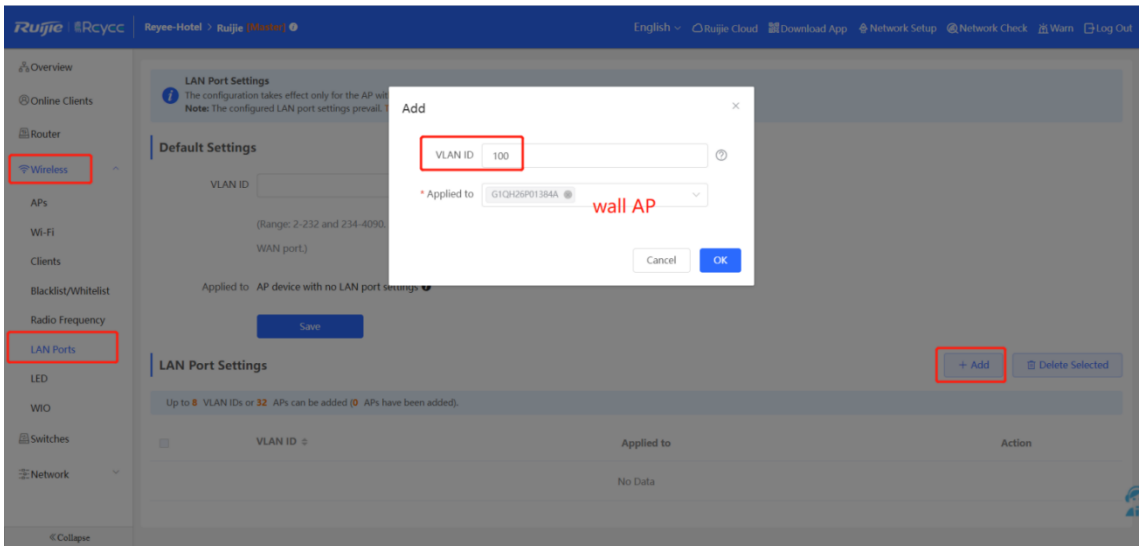
(3) Choose **Router > Basic > LAN** to create VLAN 2 and VLAN 3 for staffs and guests.



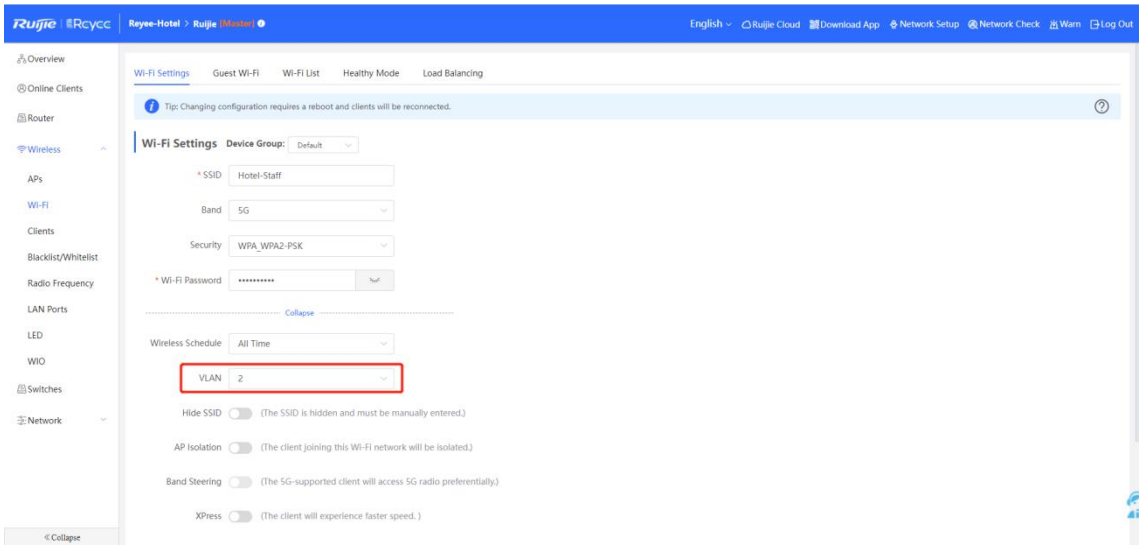
(4) Choose **Router > Basic > IPTV** to configure IPTV settings obtained from the ISP. For example, the IPTV VLAN ID is 100. Perform the operation as follows.



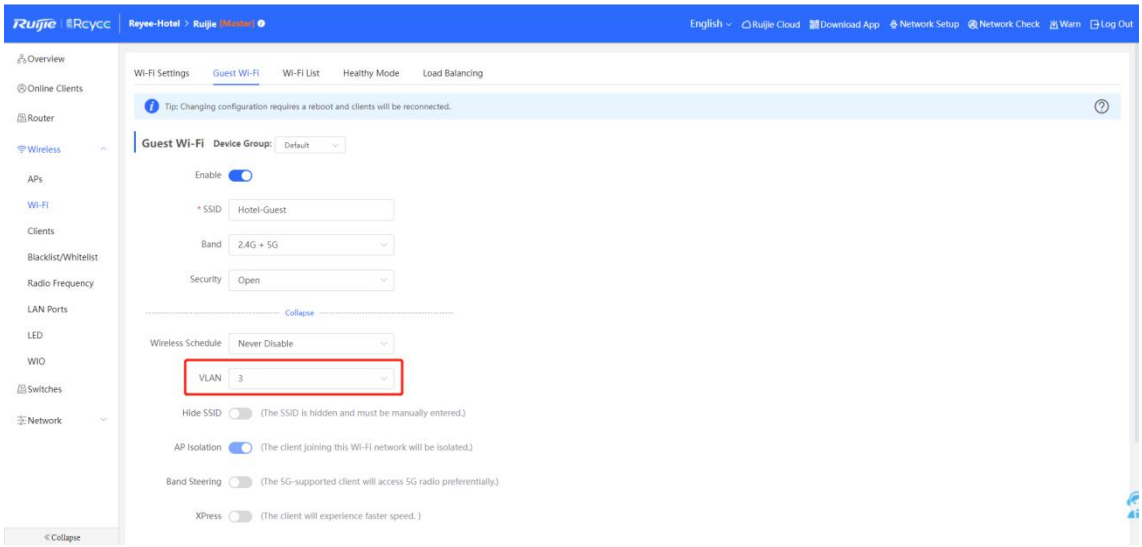
(5) Choose **WLAN > LAN Ports > Add** to configure VLAN 100 for IPTV. If default VLAN 1 is used, ignore this step.



(6) Choose **WLAN > Wi-Fi** to configure Wi-Fi for staffs and guests. Select VLAN 2 for staffs.

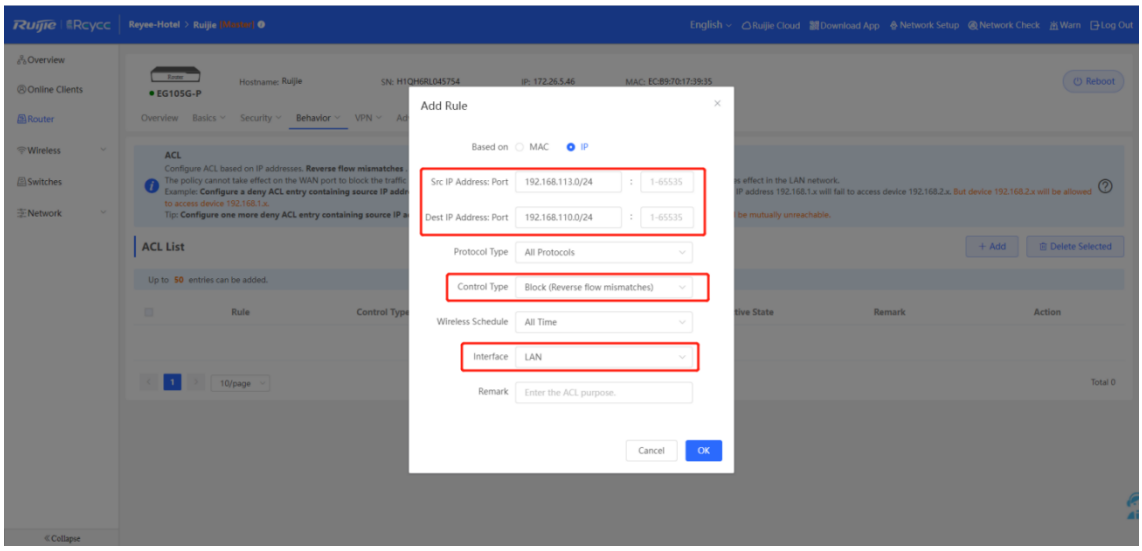


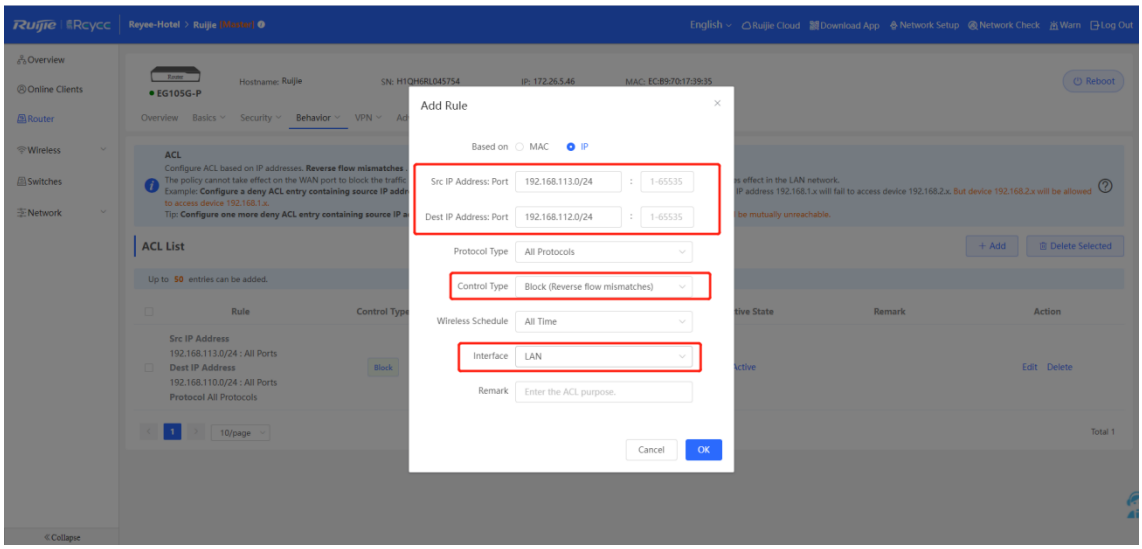
(7) Enable guest Wi-Fi, and select VLAN 3 for it.

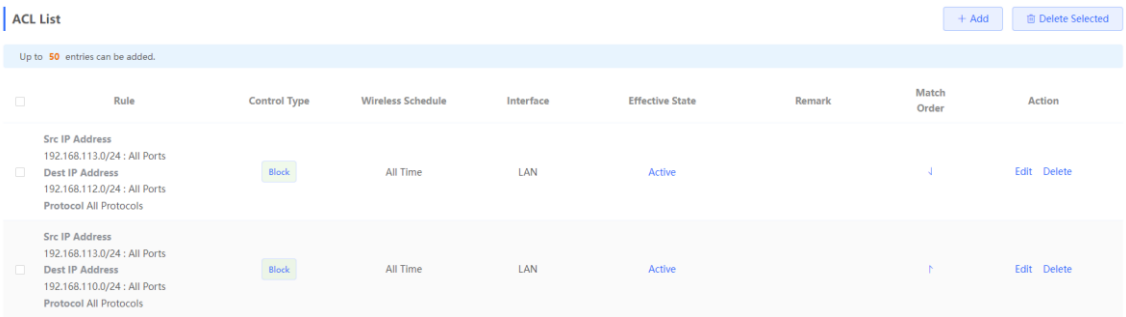


(8) Choose **Router > Behavior > Access Control**. Configure ACLs to block guests from accessing the internal network.

Add two ACLs and apply them to a LAN port to block devise in VLAN 3 from accessing users in VLAN 1 and VLAN 2.



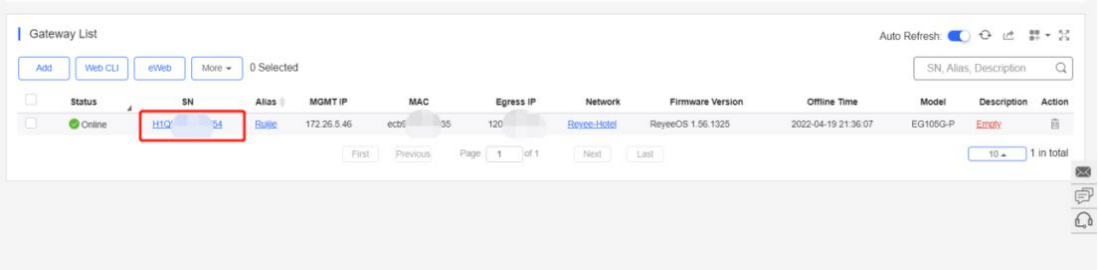




(9) Log in to Cloud web to configure Cloud voucher authentication for guests.

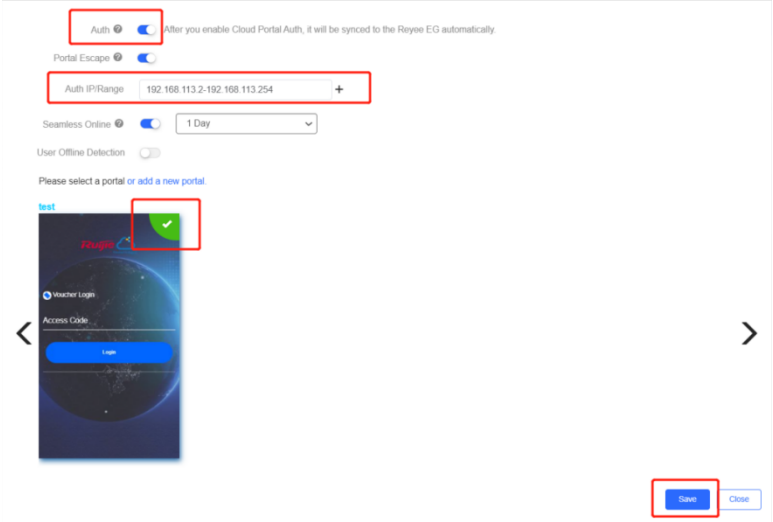
a Choose **MONITORING** > **DEVICE** > **Gateway**.

b Click the SN of the EG to access the page of device details.



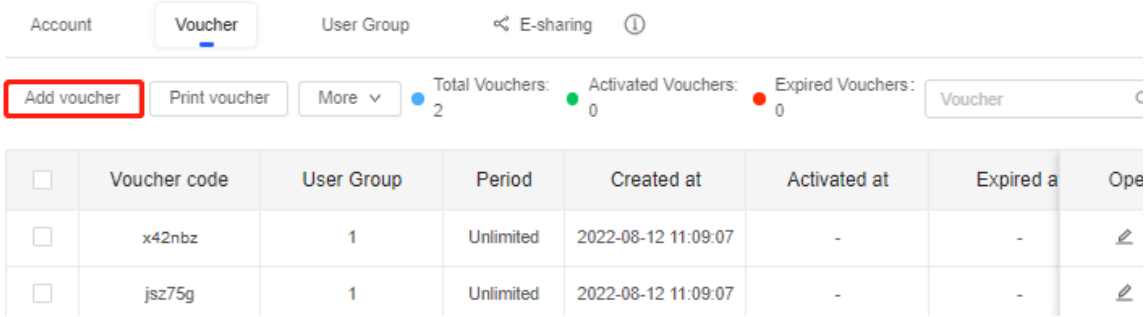
c Choose **Config** > **Cloud Portal Auth**.

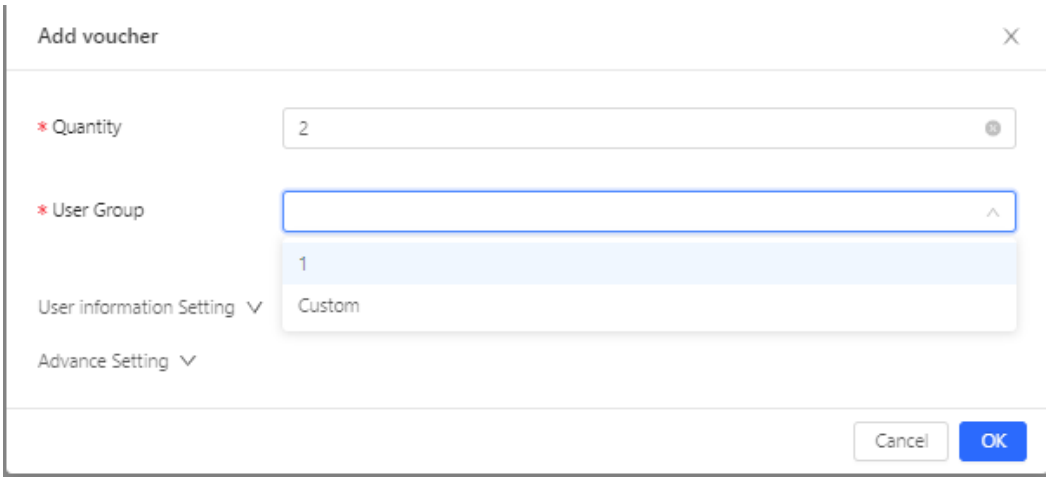
d Enable **Auth** and configure guests' IP address range from 192.168.113.2 to 192.168.113.254.



e Add the voucher for guests.

Choose **CONFIGURATION** > **AUTHENTICATION** > **User Management**, switch to the **Voucher** tab page, click **Add voucher** to configure **Quantity** and **User Group** of the voucher for guests. After the voucher is added, obtain the voucher code for guests from the **Voucher code** column in the voucher list.





Quantity: Enter the quantity of vouchers.

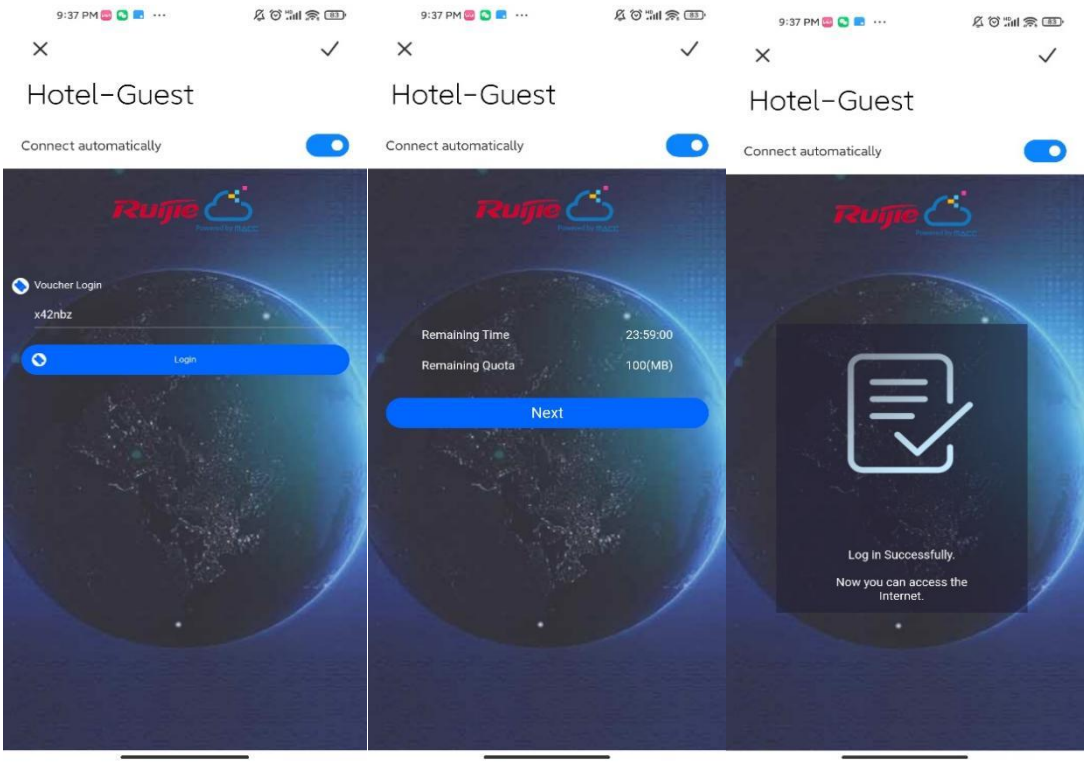
User Group: Select an existing user group or click **Custom** to customize a new user group.

User information Setting: Set user information.

Advance Setting: Set **Voucher code type** and **Voucher length**. **Voucher code type** can be set to **Alphanumeric 0-9, a-z**, **Alphabetic a-z**, or **Numeric 0-9**. **Voucher length** can be set to 6 to 9.

Configuration Verification

Connect guest Wi-Fi. Then you can view that the internal IP address 192.168.110.1 cannot be accessed.



6 Reyee FAQ

6.1 Reyee Password FAQ (Collection)

6.2 Reyee Guest WiFi FAQ (Collection)

6.3 Reyee Wireless Configuration FAQ (Collection)

6.4 Reyee Self-Organizing Network (SON) FAQ (Collection)

6.5 Reyee series Devices Parameters Tables

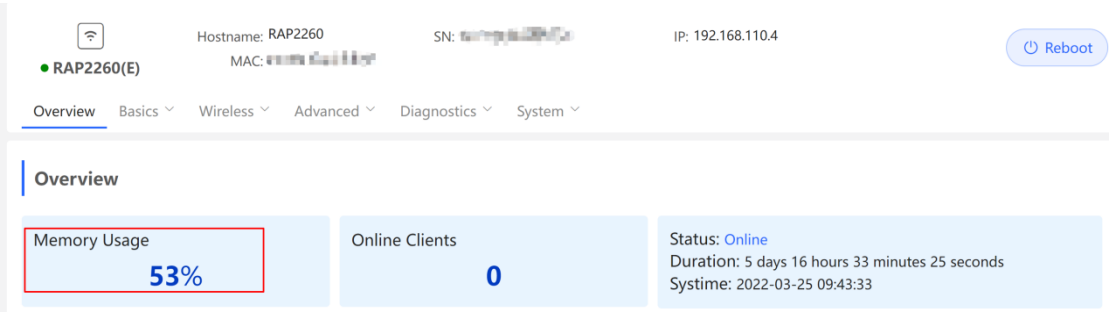
6.6 Reyee Parameter Consultation FAQ (Collection)

7 Appendix: Monitoring

7.1 Memory Usage

- In SON mode, select **Local Device** and select **Overview**.
- In standalone mode, select **Overview**.

Check the memory usage in the **Overview** area.

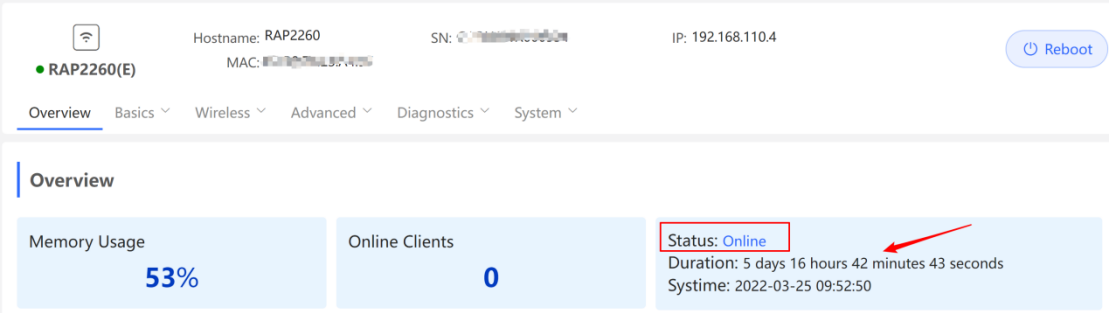


The valid memory usage is between 40% and 70%. When there are no clients, the reason for a high usage is that the memory usage is pre-allocated.

7.2 Device Status

- In SON mode, select **Local Device** and select **Overview**.
- In standalone mode, select **Overview**.

Check the device status in the **Overview** area.



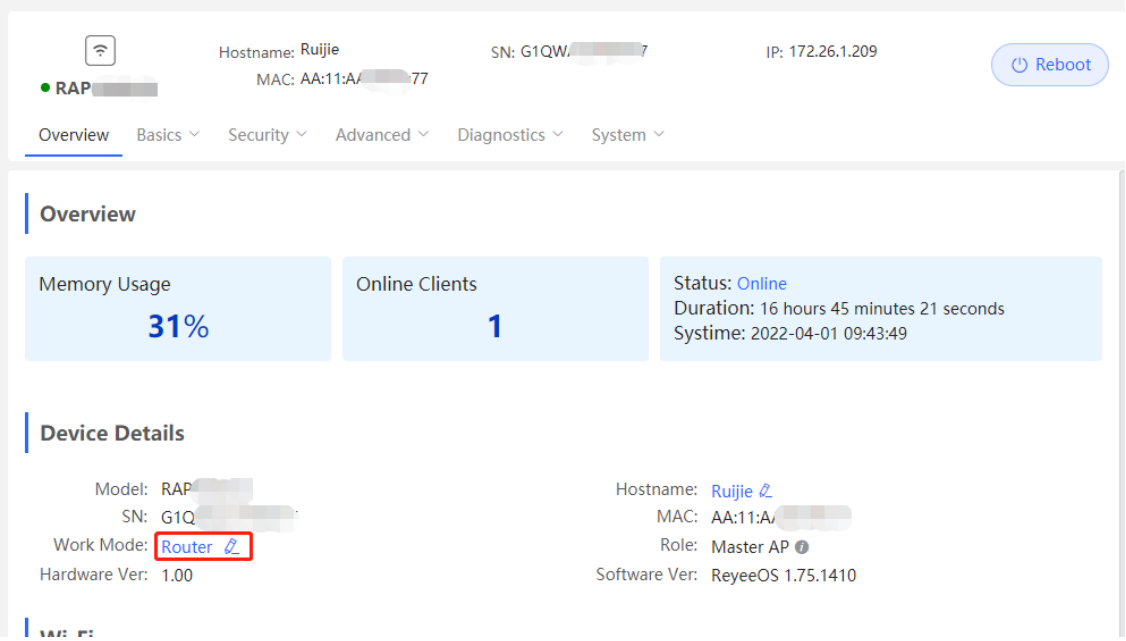
Status: indicates the device status. Check whether the device is online. **Online** means the SON feature of the Reyee device and is irrelevant to Ruijie Cloud.

Duration: indicates the online duration.

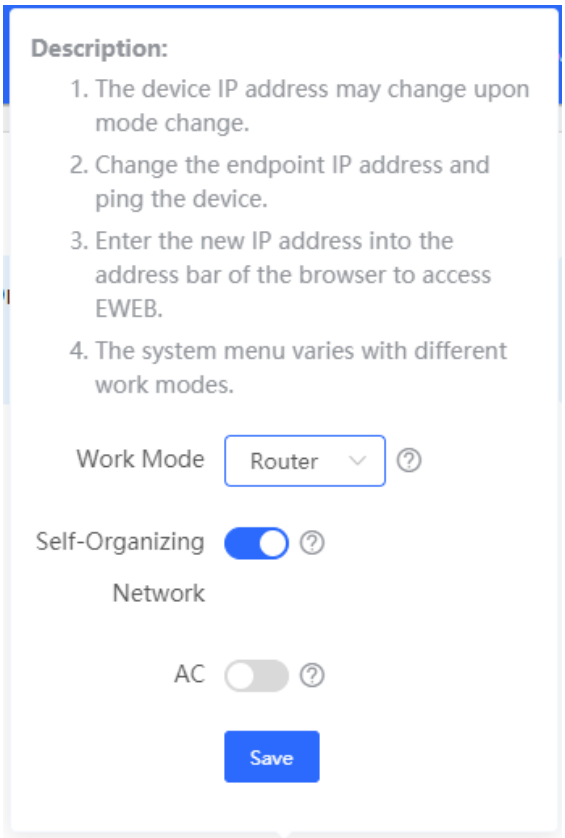
7.3 AP Working Mode

- In SON mode, select **Local Device** and choose **Overview** > **Device Details**.
- In standalone mode, choose **Overview** > **Device Details**.

Click the current working mode to access the working mode configuration page.



Set parameters of the working mode and click **Save**.



Working Mode: An AP can work in **AP** mode or **Router** mode.

- **Router**: indicates NAT forwarding. The AP in **Router** mode supports networking, network-wide configuration, and AP-specific radio functions.
- **AP**: indicates bridge forwarding.

Self-Organizing Network: If this function is enabled, the device role will be displayed. If it is disabled, the device works in standalone mode.

AC: When **Working Mode** is set to **Router** and **Self-Organizing Network** is enabled, this parameter is available. You can enable or disable the AC function. After the AC function is enabled, the device in 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 SON mode and then manage downlink devices.

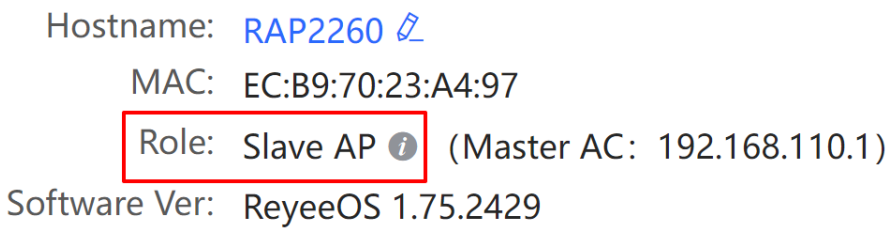
Note

After SON discovery is enabled, you can check the role of the device in SON mode.

7.4 Checking the SON Status

In SON mode, select **Local Device** and choose **Overview** > **Device Details**.

View the device role.



There are four types of role:

- **Master AP/AC**: The device can manage downlink devices.
- **Slave AP/Device**: The device has been managed by an AC.
- **Unknown**: The device failed to join an SON and works as a common AP.
- **Standalone**: The device has not joined an SON.

Instruction

If the role is incorrect, press **F5** to refresh the page.

Ruijie EG3230/3250 and Reyee ES switches cannot act as the master.

The priority of SON networking is as follows:

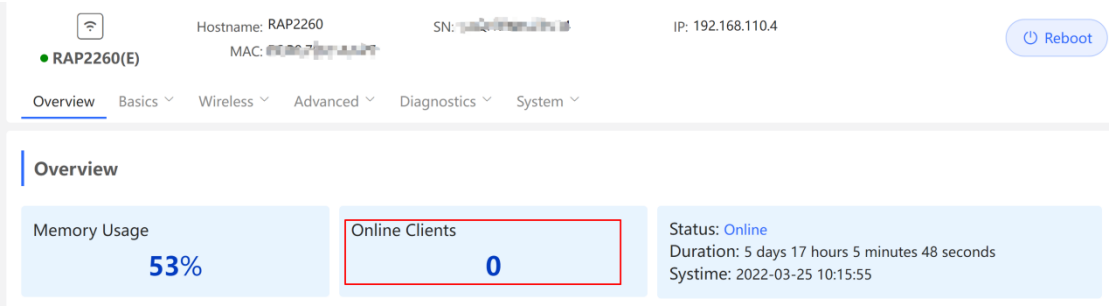
- Different models: EG (AC mode) > EG (router mode) > AP (router mode) > AP (AP mode) > switch
- Device CPU/Memory/other information (AP radio number): If devices have the same type but different models, a large parameter value indicates a higher priority of the device.

- Same model: If devices have the same type and models, a larger MAC address indicates a higher priority of the device.\

7.5 Online Clients

- In SON mode, select **Local Device** and select **Overview**.
- In standalone mode, select **Overview**.

View the number of online clients in the **Overview** area.



7.6 Device Information

- In SON mode, select **Local Device** and choose **Overview** > **Device Details**.
- In standalone mode, choose **Overview** > **Device Details**.

Check the device information.

7.7 Wireless Information

- In SON mode, select **Local Device** and choose **Overview** > **Wi-Fi**.
- In standalone mode, choose **Overview** > **Wi-Fi**.

Check wireless information.

7.8 Ethernet Status

- In SON mode, select **Local Device** and choose **Overview** > **Ethernet status**.
- In standalone mode, choose **Overview** > **Ethernet status**.

Check the interface details.