

Ruijie Reyee RG-RAP Series Access Points

ReyeeOS 2.262

Web-based Configuration Guide



Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademarks including , are owned by Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Audience

This document is intended for:

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

Technical Support

- Official website of Ruijie Reyee: <https://www.ruijienetworks.com/products/reyee>
- Technical support website: <https://ruijienetworks.com/support>
- Case portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

 **Note**

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

 **Specification**

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

3. Note

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

Contents

Preface	I
1 Fast Internet Access	1
1.1 Configuration Environment Requirements	1
1.1.1 PC	1
1.2 Default Configuration	1
1.3 Login to Eweb	1
1.3.1 Connecting to the Access Point	1
1.3.2 Configuring the IP Address of the Management Client	2
1.3.3 Logging in to the Web Page	2
1.4 Work Mode.....	3
1.4.1 AP Mode.....	3
1.4.2 Router Mode	4
1.4.3 Wireless Repeater Mode	4
1.5 Configuration Wizard (Router Mode).....	4
1.5.1 Getting Started.....	4
1.5.2 Configuration Steps	5
1.6 Configuration Wizard (AP Mode).....	8
1.6.1 Getting Started.....	8
1.6.2 Configuration Steps	8
1.7 Configuration Wizard (Wireless Repeater Mode).....	9

1.7.1 Getting Started.....	9
1.7.2 Configuration Steps	9
1.8 Introduction to the Eweb GUI	11
1.8.1 Single Management Webpage	11
1.8.2 Dual Management Webpages	14
2 Network Monitoring	1
2.1 Viewing the Network Information.....	1
2.2 Adding Network Devices.....	4
2.2.1 Wired Connection	4
2.2.2 AP Mesh.....	5
2.3 Managing Network Devices.....	14
2.4 Configuring Network Planning	16
2.4.1 Configuring Wired VLAN.....	17
2.4.2 Configuring Wi-Fi VLAN.....	19
2.5 Troubleshooting Fault Alerts.....	21
3 Wi-Fi Network Settings	23
3.1 Configuring AP Groups.....	23
3.1.1 Overview	23
3.1.2 Procedures.....	23
3.2 Configuring SSID and Wi-Fi Password	25
3.3 Hiding the SSID	27

3.3.1 Overview	27
3.3.2 Configuration Steps	27
3.4 Checking Wireless Clients	28
3.5 Configuring Wi-Fi Band.....	30
3.6 Configuring Band Steering	31
3.7 Configuring Wi-Fi 6	32
3.8 Configuring Layer-3 Roaming.....	32
3.9 Configuring AP Isolation	33
3.10 Configuring 802.11r	34
3.11 Adding a Wi-Fi Network.....	35
3.12 Configuring a Guest Wi-Fi	35
3.12.1 Overview	35
3.12.2 Configuration Steps	35
3.13 Configuring Wireless Rate Limiting	36
3.13.1 Overview	36
3.13.2 Configuration Steps	37
3.14 Configuring Wi-Fi Blocklist or Allowlist	40
3.14.1 Overview	40
3.14.2 Configuration Steps	41
3.15 Optimizing Wi-Fi Network	42
3.15.1 Overview	42

3.15.2 Getting Started.....	42
3.15.3 Optimizing the Radio Channel.....	43
3.15.4 Optimizing the Channel Width.....	44
3.15.5 Optimizing the Transmit Power.....	45
3.15.6 Configuring the Multicast Rate	46
3.15.7 Configuring the Client Limit	47
3.15.8 Configuring the Kick-off Threshold	48
3.15.9 Configuring the Roaming Sensitivity	49
3.15.10 Configuring Access Threshold.....	50
3.15.11 Configuring Response RSSI Threshold	51
3.15.12 Configuring WIO	52
3.15.13 Configuring Wi-Fi Roaming Optimization (802.11k/v)	56
3.16 Configuring Healthy Mode	58
3.17 Configuring XPress.....	58
3.18 Configuring Wireless Schedule	59
3.19 Enabling Reyee Mesh	60
3.20 Configuring AP Load Balancing	60
3.20.1 Overview	60
3.20.2 Configuring Client Load Balancing	61
3.20.3 Configuring Traffic Load Balancing.....	62
3.21 Wireless Authentication	64

3.21.1 Overview	64
3.21.2 Configuring One-click Login on Ruijie Cloud.....	65
3.21.3 Configuring Voucher Authentication on Ruijie Cloud	69
3.21.4 Configuring Account Authentication on Ruijie Cloud.....	77
3.21.5 Configuring SMS Authentication on Ruijie Cloud.....	85
3.21.6 Configuring an Authentication-Free User List on Eweb Management System.....	92
3.21.7 Displaying Authenticated Users on Eweb Management System	95
3.21.8 Displaying Authenticated Users on Ruijie Cloud	95
3.22 Configuring 802.1X Authentication.....	95
3.22.1 Overview	96
3.22.2 Configuring 802.1X Authentication	97
3.22.3 Viewing Wireless User List	101
3.22.4 Viewing Wired User List.....	102
4 Network Settings.....	103
4.1 Switching Work Mode	103
4.1.1 Work Mode.....	103
4.1.2 Self-Organizing Network Discovery.....	103
4.1.3 Configuration Steps	104
4.1.4 Viewing Device Role.....	105
4.2 Configuring Internet Connection Type (IPv4).....	106
4.3 Configuring Internet Connection Type (IPv6).....	107

4.4 Configuring LAN Port.....	107
4.5 Configuring Repeater Mode	108
4.5.1 Wired Repeater.....	109
4.5.2 Wireless Repeater	109
4.6 Creating a VLAN.....	112
4.7 Configuring Port VLAN	114
4.8 Changing MAC Address	116
4.9 Changing MTU.....	117
4.10 Configuring DHCP Server	117
4.10.1 DHCP Server	118
4.10.2 Configuring the DHCP Server Function	118
4.10.3 Displaying Online DHCP Clients	119
4.10.4 Displaying the DHCP Static IP Address List.....	120
4.11 Link Aggregation.....	121
4.12 Configuring DNS.....	121
4.13 Hardware Acceleration	122
4.14 Configuring Port Flow Control	122
4.15 Configuring ARP Binding.....	123
4.16 Configuring LAN Ports.....	124
4.17 IPv6 Settings.....	125
4.17.1 Overview	125

4.17.2 IPv6 Basic.....	125
4.17.3 IPv6 Address Assignment Methods.....	126
4.17.4 Enabling IPv6.....	127
4.17.5 Configuring the IPv6 Address for the WAN Port.....	128
4.17.6 Configuring the IPv6 Address for the LAN Port.....	130
4.17.7 Viewing DHCPv6 Clients.....	132
4.17.8 Configuring the Static DHCPv6 Address.....	133
4.17.9 Configuring the IPv6 Neighbor List.....	133
5 System Settings	135
5.1 PoE	135
5.2 PoE Settings.....	135
5.3 Setting the Login Password.....	136
5.4 Setting the Session Timeout Duration.....	137
5.5 Setting and Displaying System Time.....	138
5.6 Configuring SNMP	139
5.6.1 Overview	139
5.6.2 Global Configuration	140
5.6.3 View/Group/Community/User Access Control.....	141
5.6.4 SNMP Service Typical Configuration Examples.....	151
5.6.5 Configuring Trap Service	156
5.6.6 Trap Service Typical Configuration Examples.....	161

5.7 Configuring Reboot.....	164
5.7.1 Rebooting the Current Device	165
5.7.2 Rebooting All Devices in the Network.....	165
5.7.3 Rebooting the Specified Device	166
5.8 Configuring Scheduled Reboot.....	168
5.8.1 Configuring Scheduled Reboot for the Current Device	168
5.9 Configuring Backup and Import.....	169
5.10 Restoring Factory Settings	169
5.10.1 Restoring the Current Device to Factory Settings.....	169
5.10.2 Restoring All Devices to Factory Settings	170
5.11 Performing Upgrade and Checking System Version	171
5.11.1 Online Upgrade.....	171
5.11.2 Local Upgrade	171
5.12 Switching System Language	172
5.13 Configuring LED Status Control	172
6 Network Diagnosis Tools	174
6.1 Network Check.....	174
6.2 Network Tools.....	175
6.3 Alarms	177
6.4 Fault Collection	178
7 FAQs	179

7.1 Login Failure	179
7.2 Factory Setting Restoration	179
7.3 Password Loss.....	179

1 Fast Internet Access

1.1 Configuration Environment Requirements

1.1.1 PC

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

1.2 Default Configuration

Table 1-1 Default Web Configuration

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

1.3 Login to Eweb

1.3.1 Connecting to the Access Point

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

- Wired Connection

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

- Wireless Connection

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

1.3.2 Configuring the IP Address of the Management Client

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

Caution

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

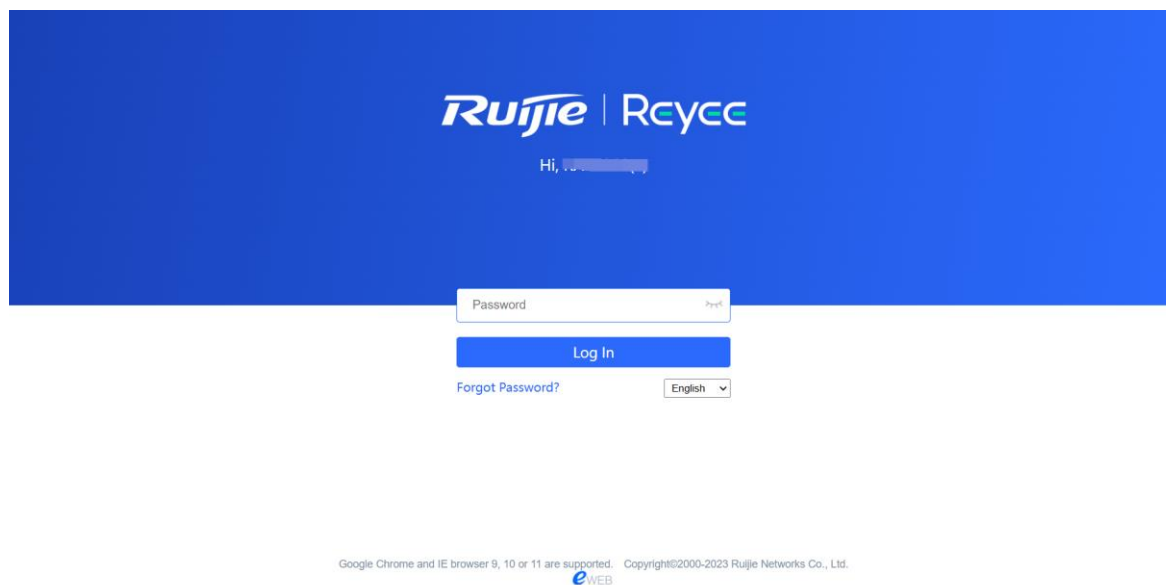
1.3.3 Logging in to the Web Page

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

Note

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

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



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

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

Caution

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

1.4 Work Mode

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

1.4.1 AP Mode

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

1.4.2 Router Mode

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

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

⚠ Caution

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

1.4.3 Wireless Repeater Mode

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

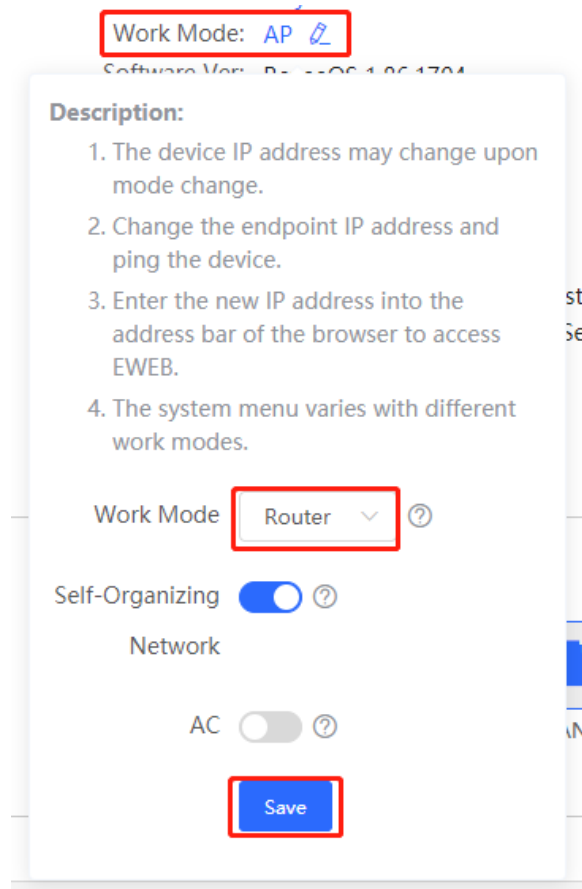
1.5 Configuration Wizard (Router Mode)

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

1.5.1 Getting Started

- (1) Connect the device to a power supply and connect the port of the device to an upstream device with an Ethernet cable. Or you can connect an Ethernet cable to the device.
- (2) Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet access may fail due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection type:
 - Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
 - In the PPPoE mode, a username, a password, and possibly a service name are needed.
 - In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.

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



1.5.2 Configuration Steps

1. Add a Device to Network

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

i Note

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

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

Ruijie | Reycce | Discover Device English Exit

Total Devices: 1.
Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.

Net Status (**Online Devices** / Total) Refresh

Internet — Router (0) — Switches (0 / 0) — APs (1 / 1)

My Network

test (1 devices)

	Model	SN	IP	MAC	Software Ver
Local A.P. RA	[Master]	G1Q 0477	19 .2	AA:1 :4:77	ReyeeOS 1.

Rediscover Start Setup

2. Creating a Network Project

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

- (1) **Network Name:** Identify the network where the device is located.
- (2) **Internet:** Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).
 - **DHCP:** The access point detects whether it can obtain an IP address via DHCP by default. If the access point connects to the Internet successfully, you can click **Next** without entering an account.
 - **PPPoE:** Click **PPPoE**, and enter the username, password, and service name. Click **Next**.
 - **Static IP:** Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.
- (3) **SSID and Wi-Fi Password:** The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.
- (4) **Management Password:** The password is used for logging in to the management page.

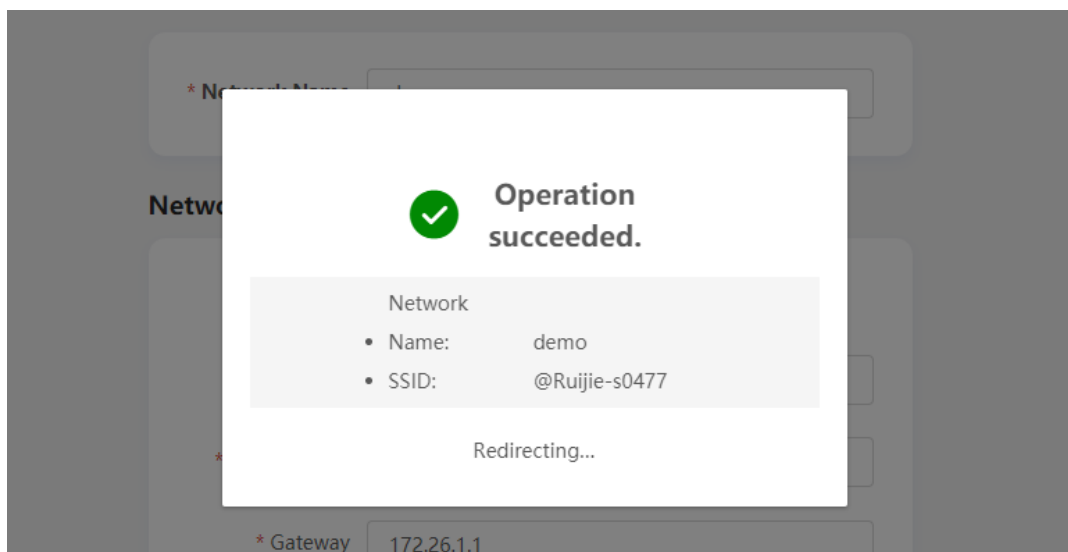
- (5) **Country/Region:** The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- (6) **Time Zone:** Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.

The screenshot shows the 'Create Network' configuration page. At the top, there is a blue header with the Ruijie logo, 'Rcycc c', and 'Create Network' text. On the right side of the header, there are 'English' and 'Exit' options. The main content area is divided into several sections:

- * Network Name:** A text input field with the placeholder text 'Example: XX hotel.'
- Network Settings:** A section containing:
 - Internet connection type: Radio buttons for 'Internet', 'PPPoE', 'DHCP' (selected), and 'Static IP'. Below 'DHCP' is a small icon and the text 'Checking IP assignment'.
 - * SSID: A text input field.
 - Wi-Fi Password: Radio buttons for 'Security' and 'Open' (selected).
- Management Password (Please remember the password.):** A section with a text input field containing 'Please remember the management pass' and a toggle for visibility.
- Country/Region/Time Zone:** A section with two dropdown menus:
 - * Country/Region: Set to 'China (CN)'. A downward arrow is visible to the right.
 - * Time Zone: Set to '(GMT+8:00)Asia/Shanghai'. A downward arrow is visible to the right.

At the bottom of the form, there are two buttons: 'Previous' and 'Create Network & Connect'.

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



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

i Note

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

1.6 Configuration Wizard (AP Mode)

1.6.1 Getting Started

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

1.6.2 Configuration Steps

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

The screenshot shows the 'Create Network' configuration wizard in the Ruijie Rcycc web interface. The interface is in English and includes an 'Exit' button. The configuration steps are as follows:

- Network Name:** A text input field with the placeholder text 'Example: XX hotel.'
- Network Settings:**
 - Internet:** Radio buttons for 'DHCP' (selected) and 'Static IP'.
 - SSID:** A text input field containing '@Ruijie-s0477'.
 - Wi-Fi Password:** Radio buttons for 'Security' (selected) and 'Open', followed by a password input field with masked characters and a 'Show/Hide' icon.
- Management Password (Please remember the password.):** A text input field with the placeholder text 'Please remember the management pas:' and a 'Show/Hide' icon.
- Country/Region/Time Zone:**
 - Country/Region:** A dropdown menu set to 'China (CN)'.
 - Time Zone:** A dropdown menu set to '(GMT+8:00)Asia/Shanghai'.

At the bottom of the form is a blue button labeled 'Create Network & Connect'.

1.7 Configuration Wizard (Wireless Repeater Mode)

1.7.1 Getting Started

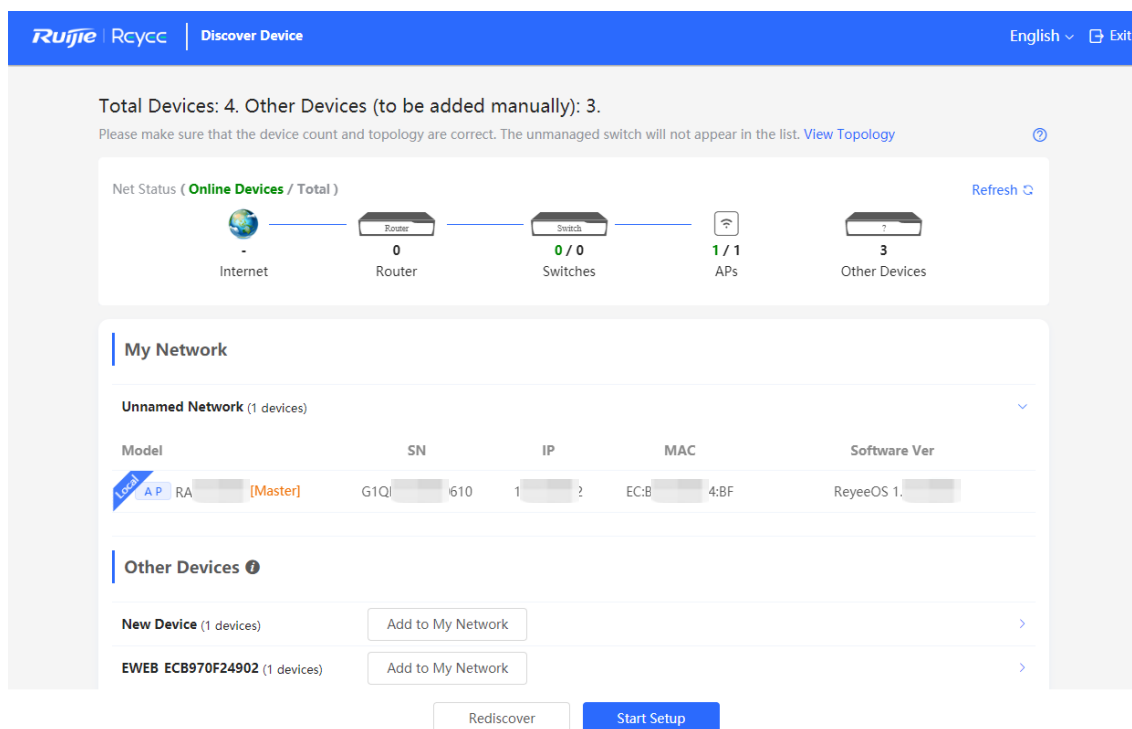
- Before configuring the wireless repeater mode, configure the primary router and test that the primary router can access the Internet.
- Place the device where it can discover at least two-bar Wi-Fi signal of the primary router.

Caution

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

1.7.2 Configuration Steps

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



The screenshot shows the Ruijie Rcycc web interface. At the top, there is a blue header with the Ruijie logo, 'Rcycc', and 'Discover Device'. On the right, there are links for 'English' and 'Exit'. Below the header, the main content area displays network status and device discovery options.

Total Devices: 4. Other Devices (to be added manually): 3.
Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list. [View Topology](#)

Net Status (Online Devices / Total)

Category	Online Devices	Total
Internet	-	-
Router	0	0
Switches	0 / 0	0 / 0
APs	1 / 1	1 / 1
Other Devices	3	3

My Network

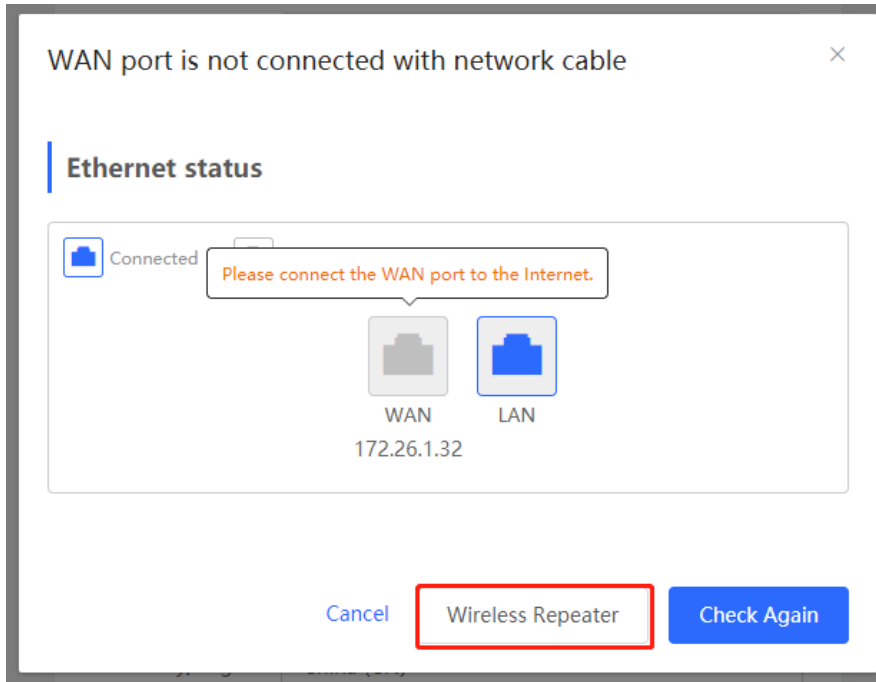
Unnamed Network (1 devices)

Model	SN	IP	MAC	Software Ver
A.P. RA [Master]	G1QI 610	1 ?	EC:B 4:BF	ReyeeOS 1.

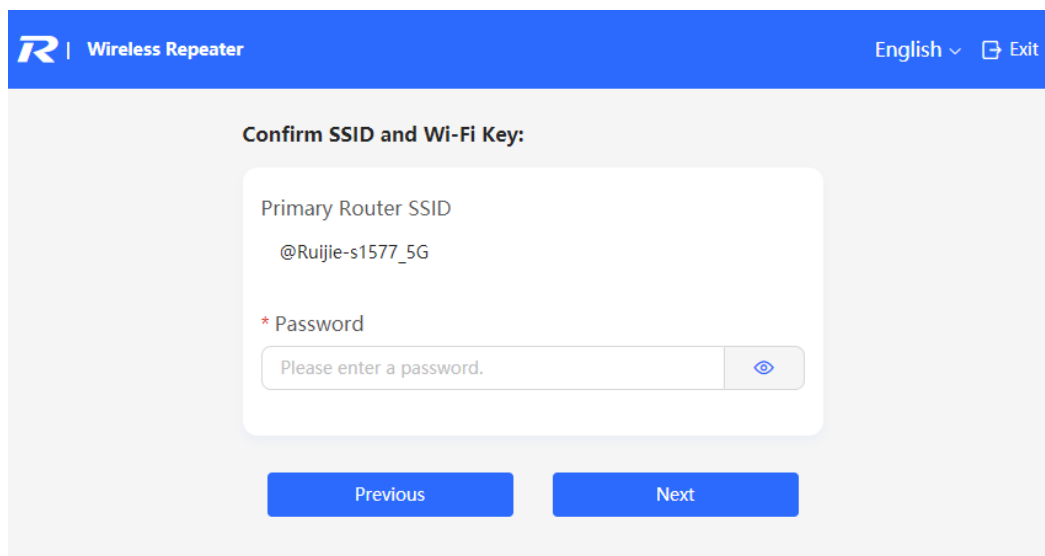
Other Devices

- New Device (1 devices)**
- EWEB ECB970F24902 (1 devices)**

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



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



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

The screenshot shows the 'Local Router Wi-Fi' configuration interface. At the top, there is a blue header with the Ruijie logo and 'Wireless Repeater' text, along with 'English' and 'Exit' options. The main content area is titled 'Local Router Wi-Fi' and contains a form with three sections: 'New Wi-Fi' (selected) and 'Same as Primary Router Wi-Fi' (unselected); '* SSID (2.4G)' with a text input field containing '@Ruijie-s1577_5G_plus'; '* SSID (5G)' with a text input field containing '@Ruijie-s1577_5G_plus_5G'; and '* Wi-Fi Password' with a text input field containing '12345678' and a toggle switch that is turned on. At the bottom of the form are two blue buttons: 'Previous' and 'Save'.

1.8 Introduction to the Eweb GUI

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

As to the RG-RAP2260(G), 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 models, please refer to Dual Management Webpages.

As to other RAP models, please refer to Single Management Webpage.

Note

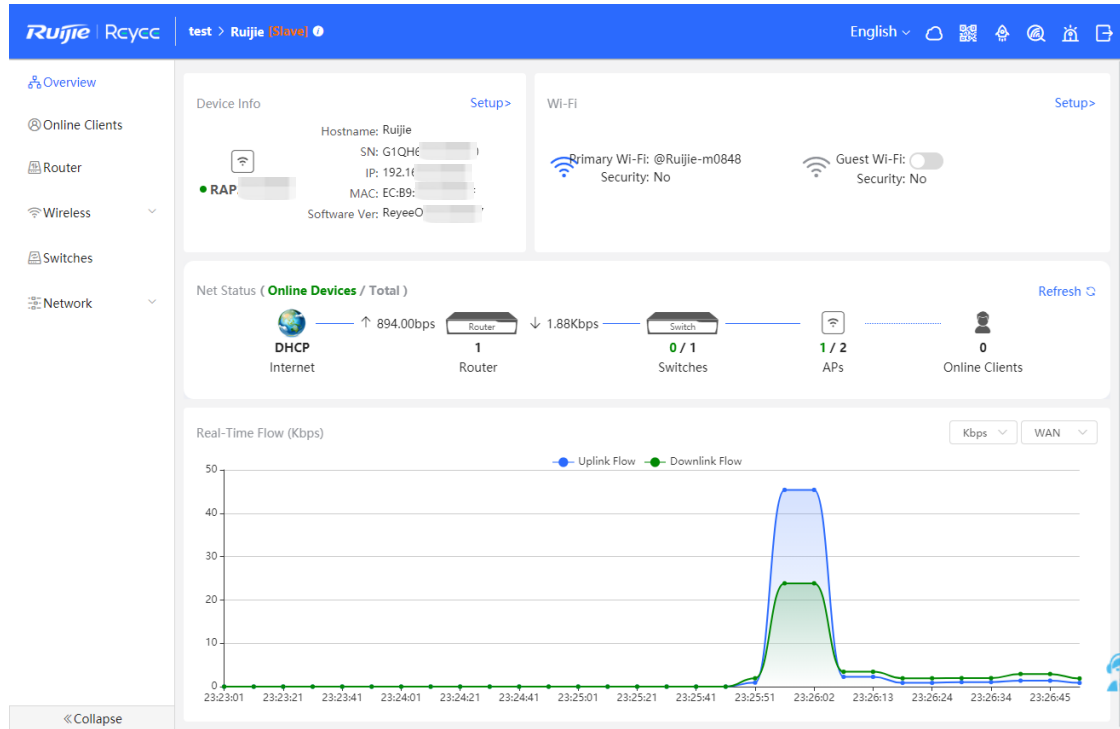
When the self-organizing network is enabled, the Eweb GUI is subject to the master device in the network. If the master device supports the dual management webpages, the slave device also displays the dual management webpages.

1.8.1 Single Management Webpage

1. Network-wide Management

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

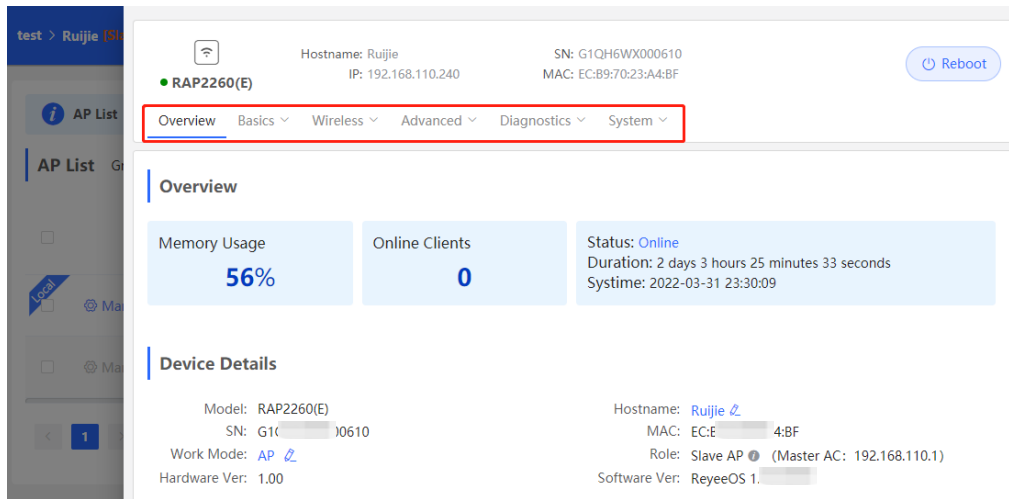
routers exist in the network), switch management configuration, and network-wide management configuration (time, password, network-wide reboot, and other system settings).



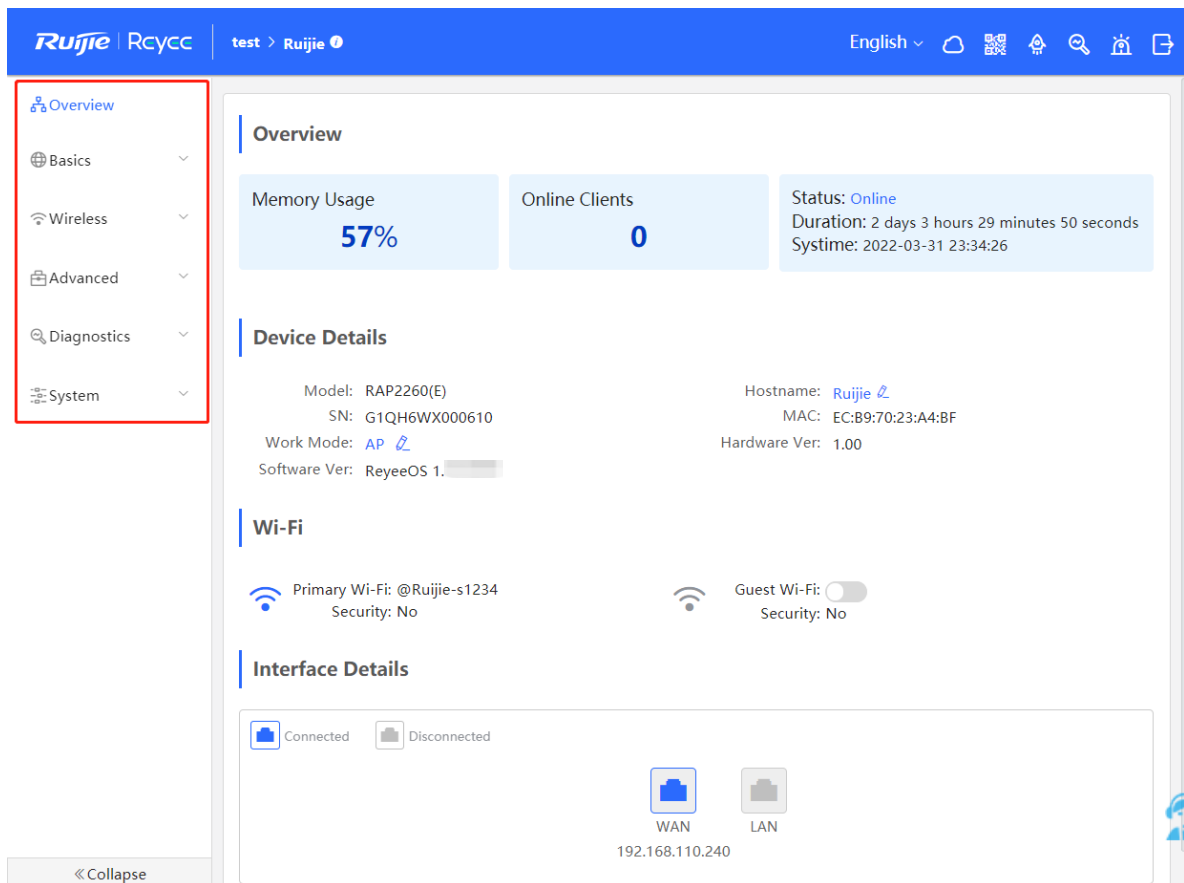
2. Standalone Management

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





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



1.8.2 Dual Management Webpages

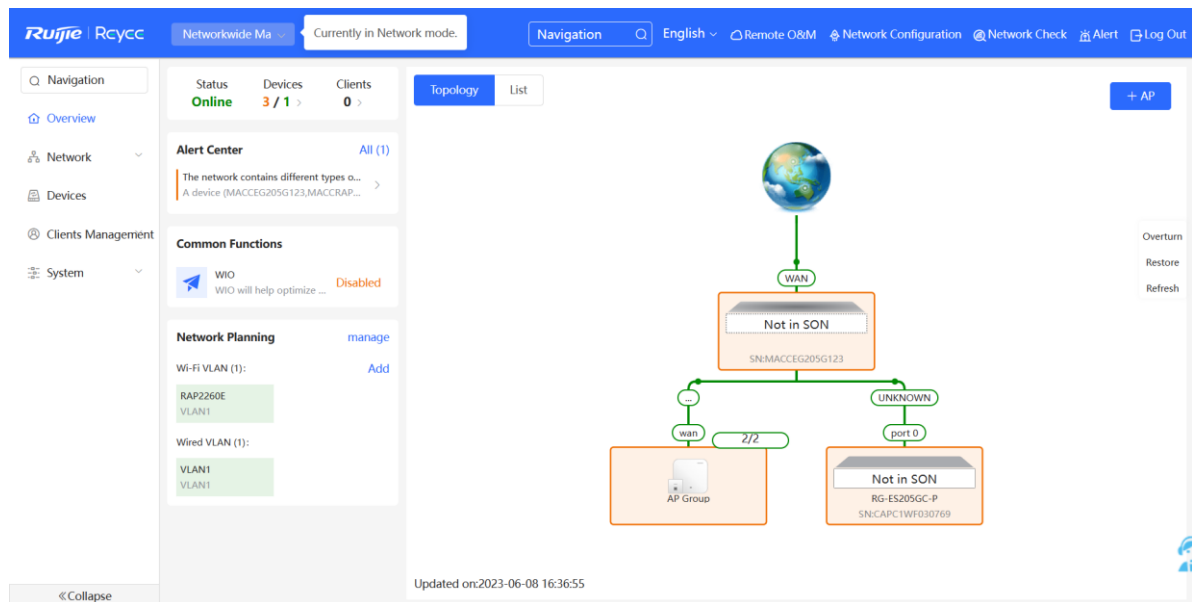
1. Introducing the Management Mode

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

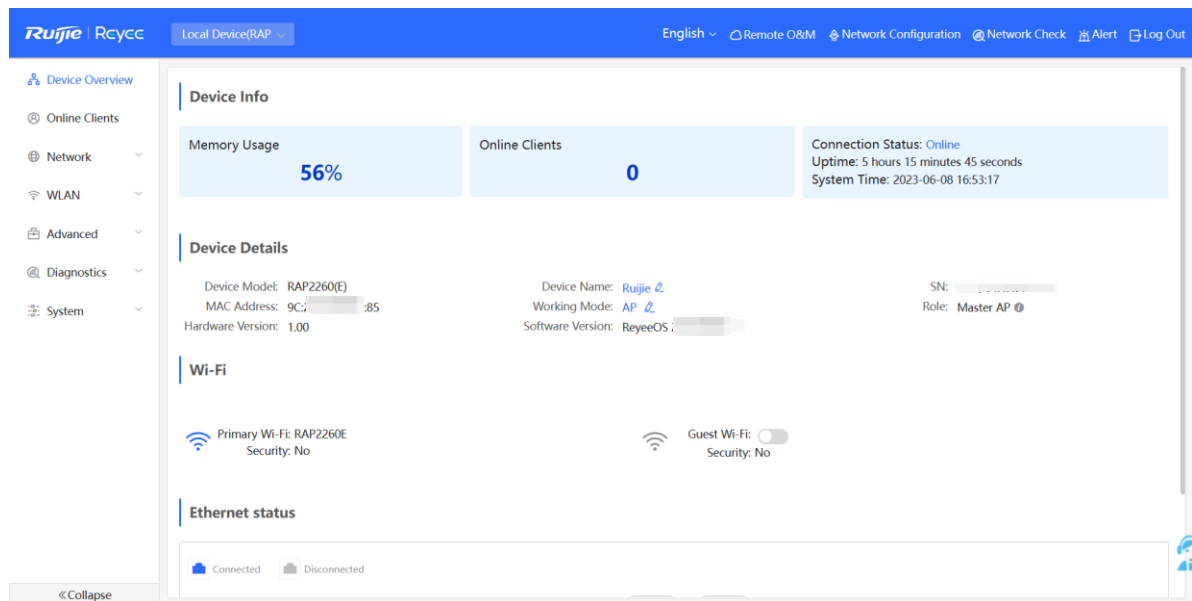
If the self-organizing network is enabled, the device can work in the network mode and the local device mode. The two modes can be switched on the Web page.

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

Network mode webpage

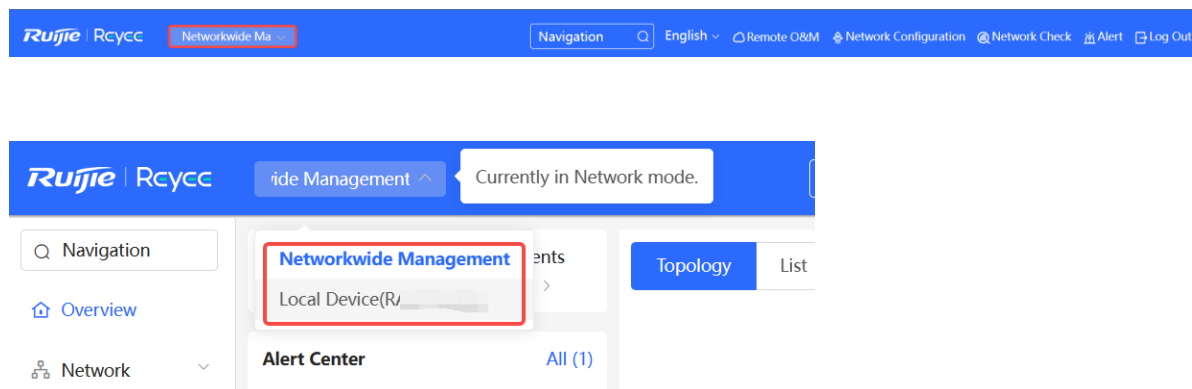


Local Device mode webpage



2. Switching the Management Mode


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



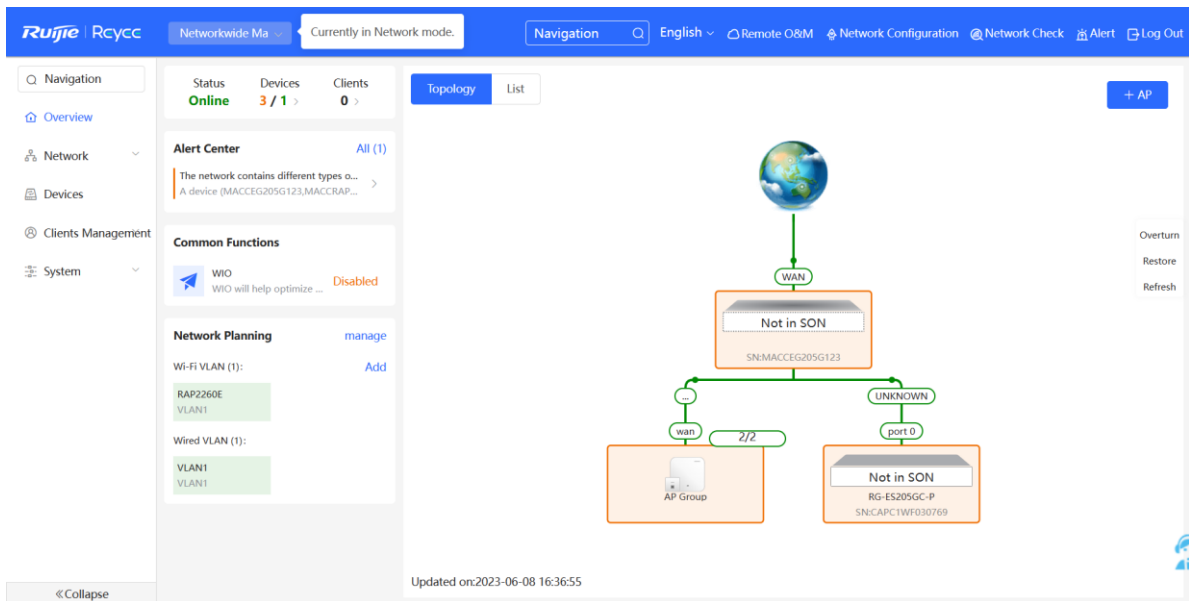
2 Network Monitoring

⚠ Caution

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

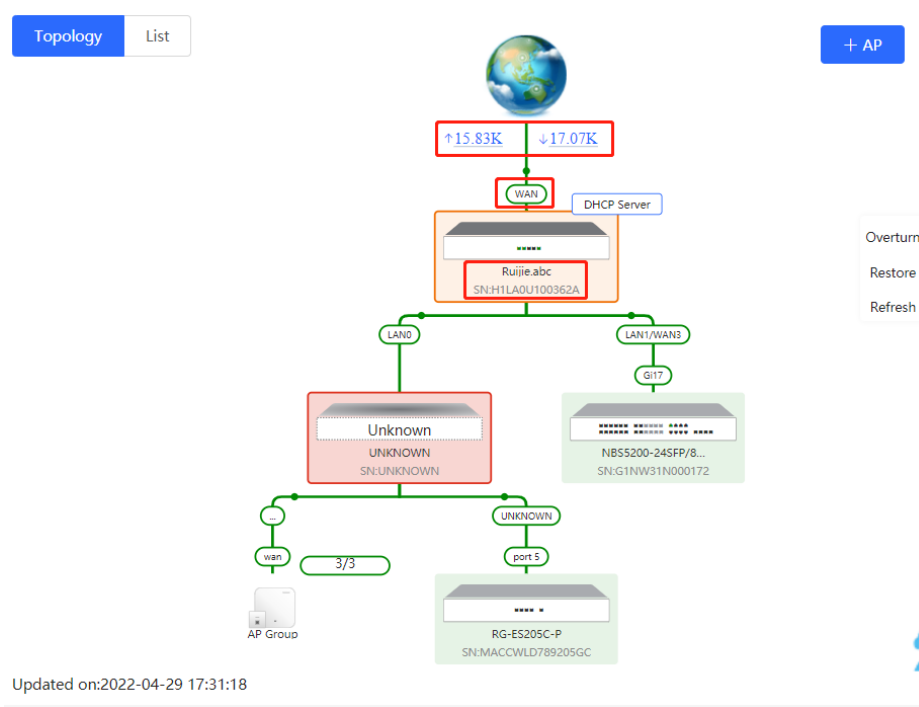
In **Network** mode, select  **Overview**.

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

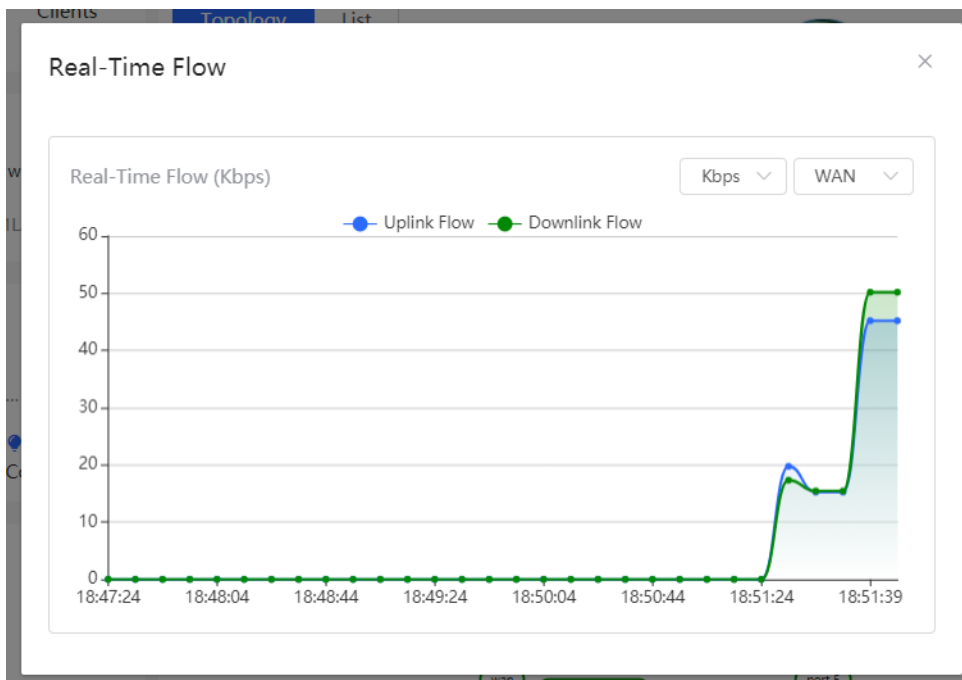



2.1 Viewing the Network Information

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



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



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

The screenshot displays the Ruijie network management interface. On the left, a network topology diagram shows a central switch connected to various devices. The main panel shows the switch's details: Hostname: Ruijie.abc, Model: EG205G, SN: H1LA0U100362A, Software Ver: ReyeeOS, MGMT IP: 192.168.110.1, and MAC: 00:7...d:85. Below this, the 'Port Status' section shows indicators for LAN0, LAN1, LAN2, WAN1, and WAN. The 'VLAN' section includes a table for the Default VLAN:

Interface	IP	IP Range	Remark
LAN0,1	192.168.110.1	192.168.110.1-192.168.110.254	

At the bottom left, it indicates 'Updated on: 2022-04-29 17:31:18'.

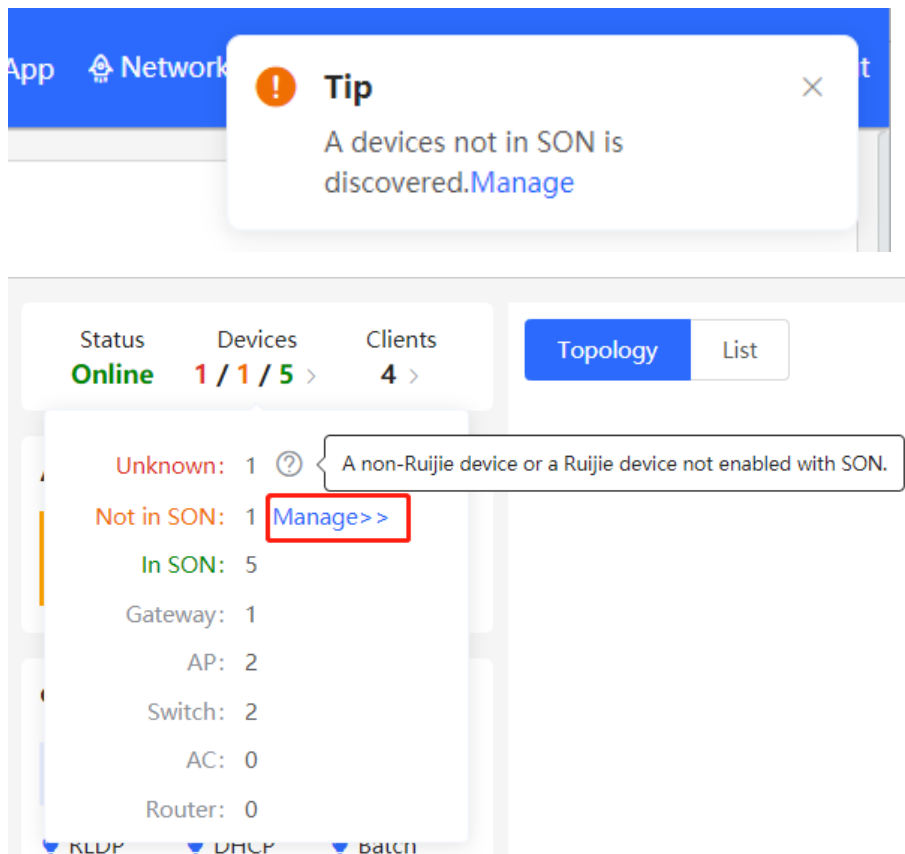
- The update time of the topology is displayed at the bottom left corner. Click **Refresh** to update the topology to the latest status. Please wait for a few minutes for the update.

This screenshot focuses on the topology view of the Ruijie network management interface. It shows a central switch connected to a WAN port and two LAN ports (LAN0 and LAN1/WAN3). The WAN port is labeled with traffic statistics: ↑ 14.05K and ↓ 22.45K. The switch is identified as Ruijie.abc with SN: H1LA0U100362A and is marked as a DHCP Server. On the right side, there are control buttons: 'Overturn', 'Restore', and 'Refresh' (which is highlighted with a red border). A '+ AP' button is also visible in the top right corner.

2.2 Adding Network Devices

2.2.1 Wired Connection

- (1) If a new device is connected to the device in the network through wired connection, a prompt message will pop up, indicating that a device not in SON (Self-Organizing Network) is discovered. The number (in orange) of devices that are not in SON is displayed under the **Devices** at the top left corner of the page. Click **Manage** to add the device to the current network.



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

Network List
Every network varies in devices and configuration. You can add devices of Other Network to My Network.

My Network

AA (1 devices)

Device Model	SN	IP Address	MAC Address	Software Version
Local A P RAP2260(E) [Master]	G1Q[]705B	192.168.125.187	9C:2[]B:85	ReyeeOS []7

Other Network

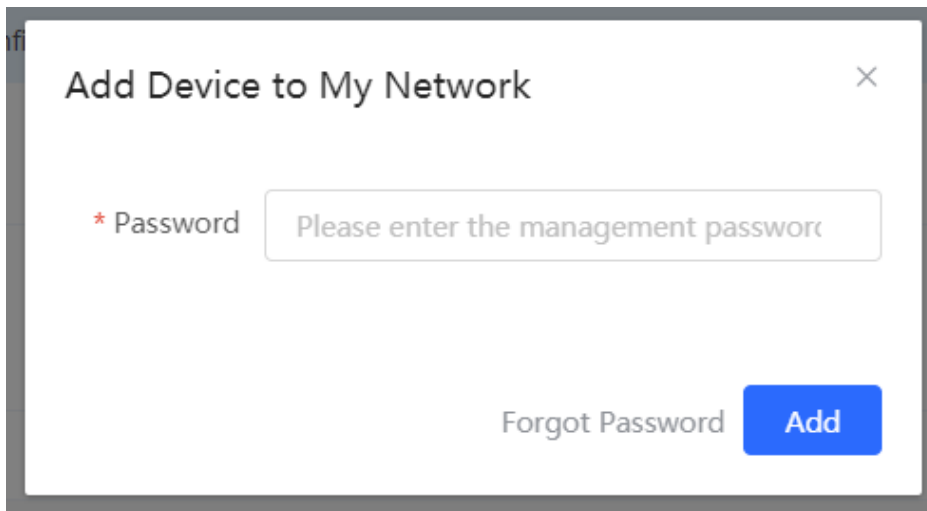
111 (1 devices) + Add to My Network

Device Model	SN	IP Address	MAC Address	Software Version
<input checked="" type="checkbox"/> A P RAP2200(E)	MAC[]0E0	192.168.125.210	00:L[]8:48	ReyeeOS []

lhf (1 devices) + Add to My Network

Unnamed Network (1 devices) + Add to My Network

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



2.2.2 AP Mesh

Note
This function is not supported by RG-RAP1200(F) and RG-RAP2200(F).

1. Overview

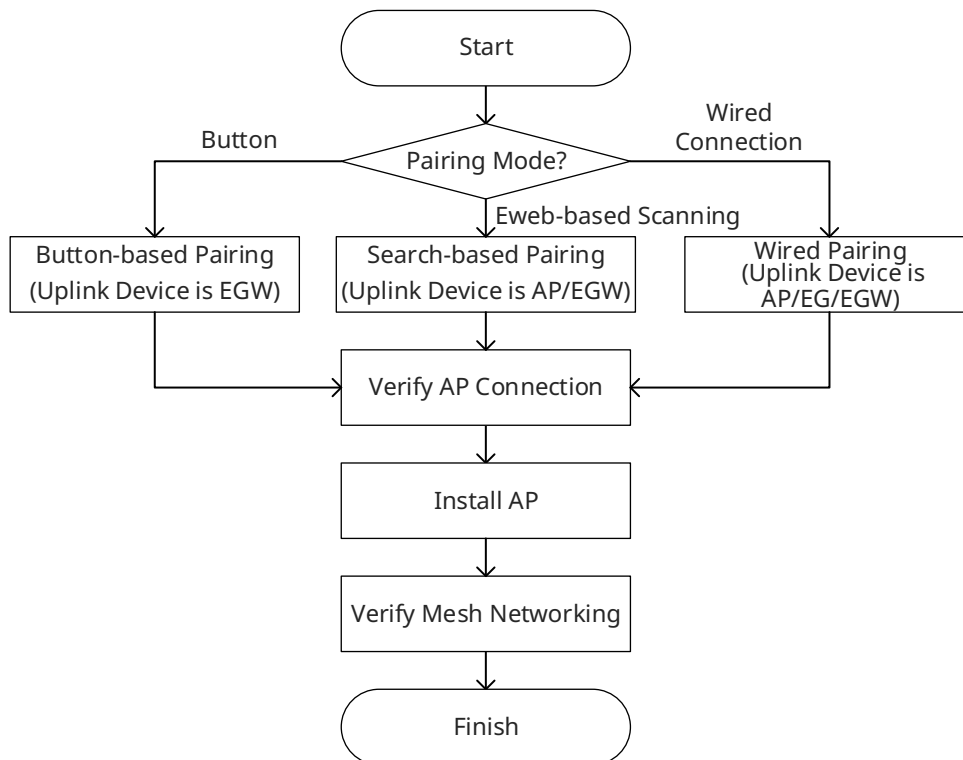
After being powered on and enabled with Mesh (see 3.19__ for details), a Mesh-capable new AP can be paired with other Mesh-capable wireless devices on the target network through

multiple ways. Then the AP will be synchronized its Wi-Fi configuration with other devices automatically. Mesh networking addresses pain points such as complex wireless networking and cabling. A new AP can be connected to any uplink wireless device among AP, EG router, and EGW router in the following ways:

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

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

2. Configuration Procedure




3. Configuration Steps for Button-based Pairing (Uplink Device is an EGW Router)

⚠ Caution

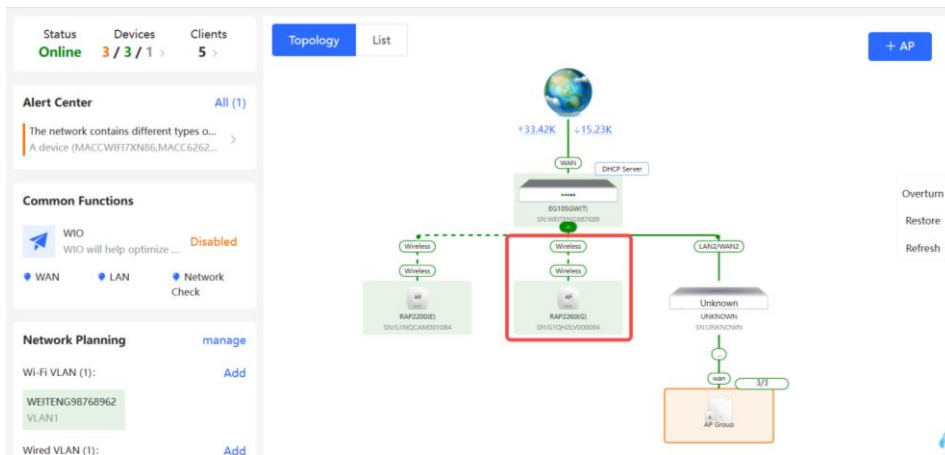
- Only EG105GW-X and EG105GW(T) support button-based pairing and each router can be paired with up to 15 new APs.
- The new AP must be in factory status.

- It can be scanned only when the live network is enabled with Mesh (see [3.19 Enabling Reyee Mesh](#) for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

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

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

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




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

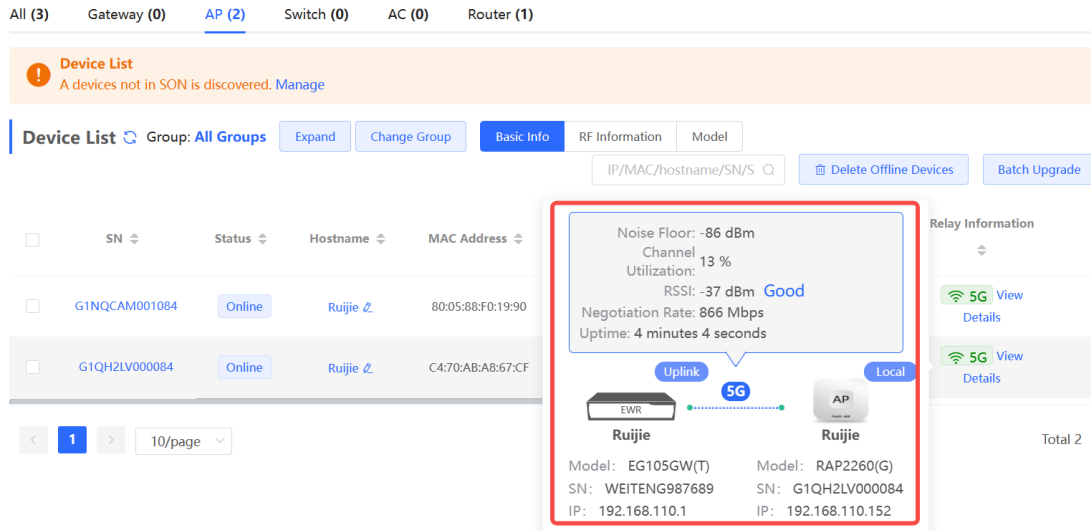
(5) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices** > **AP**. Make sure that the new AP is online and the corresponding entry contains icon



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

SN	Status	Hostname	MAC Address	IP Address	Clients	Device Group	Relay Information
G1NQCAM001084	Online	Ruijie_2	80D5:88F0:19:90	192.168.110.31	0	egw默认/Default	5G View Details
G1QH2LV000084	Online	Ruijie_2	C470:AB:A8:67:CF	192.168.110.152	0	egw默认/Default	5G View Details

Click **View Details** following the  icon to obtain information about the uplink device and RSSI.



The screenshot shows a network monitoring interface. At the top, there are tabs for 'All (3)', 'Gateway (0)', 'AP (2)', 'Switch (0)', 'AC (0)', and 'Router (1)'. Below this is a 'Device List' section with a warning icon and the text 'A devices not in SON is discovered. Manage'. The main area shows a table of devices with columns for SN, Status, Hostname, and MAC Address. Two devices are listed, both with status 'Online'. A detailed view of one device is shown, highlighting the 'Uplink' and 'Local' connections. The detailed view includes the following information:

- Noise Floor: -86 dBm
- Channel Utilization: 13 %
- RSSI: -37 dBm **Good**
- Negotiation Rate: 866 Mbps
- Uptime: 4 minutes 4 seconds

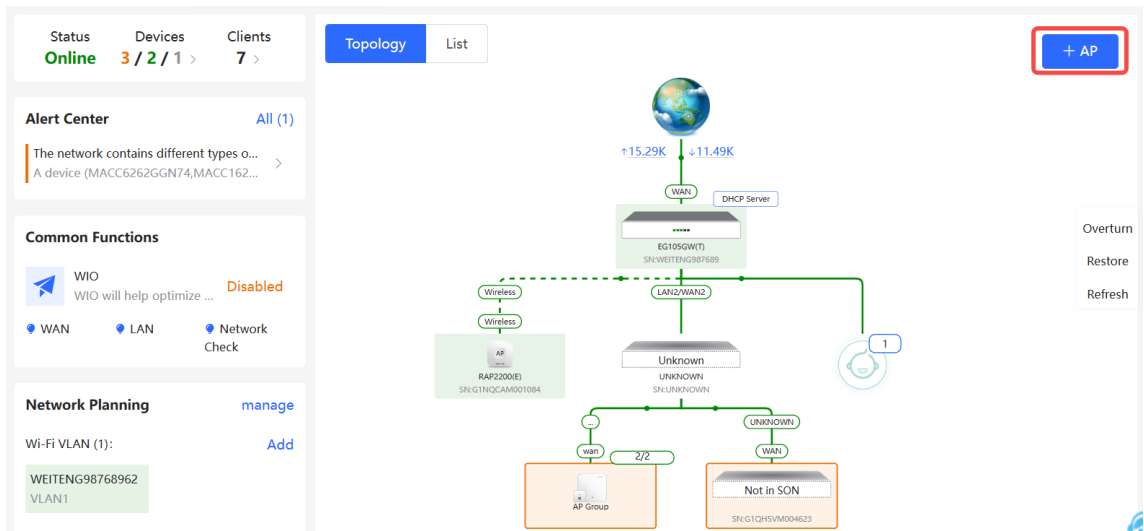
The detailed view also shows a diagram of the uplink connection between an EWR (EGW Router) and an AP (Access Point), both labeled 'Ruijie'. The EWR has Model: EG105GW(T), SN: WEITENG987689, and IP: 192.168.110.1. The AP has Model: RAP2260(G), SN: G1QH2LV000084, and IP: 192.168.110.152.

4. Configuration Steps for Search-based Pairing (Uplink Device is an AP or EGW Router)

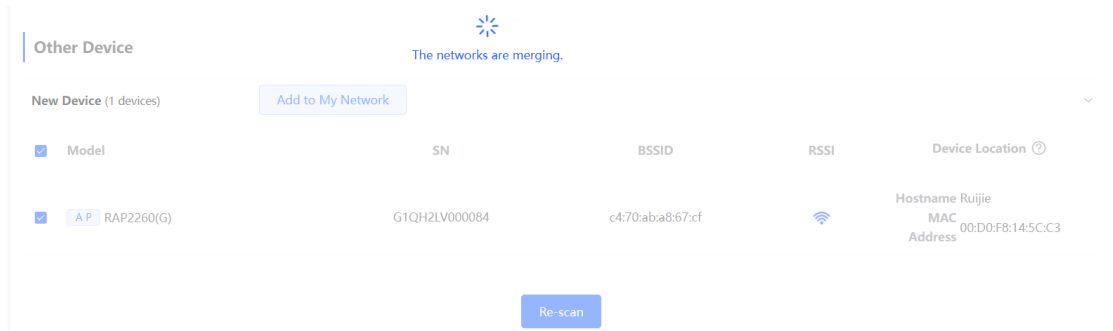
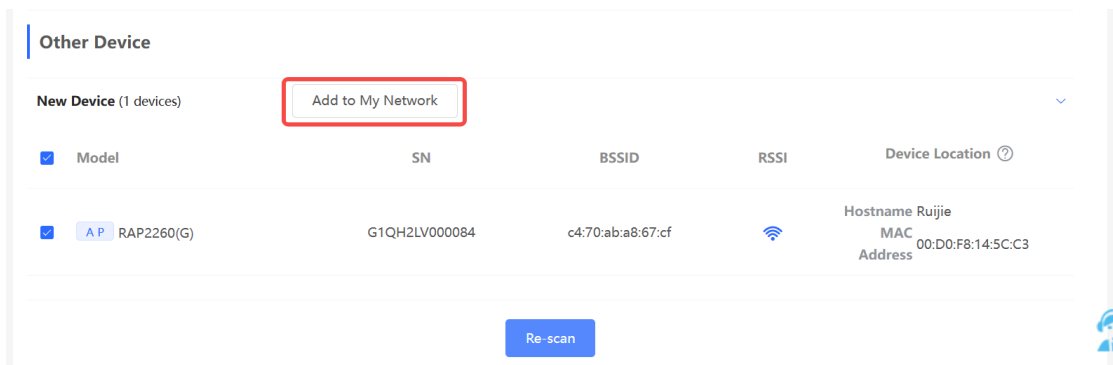
Caution

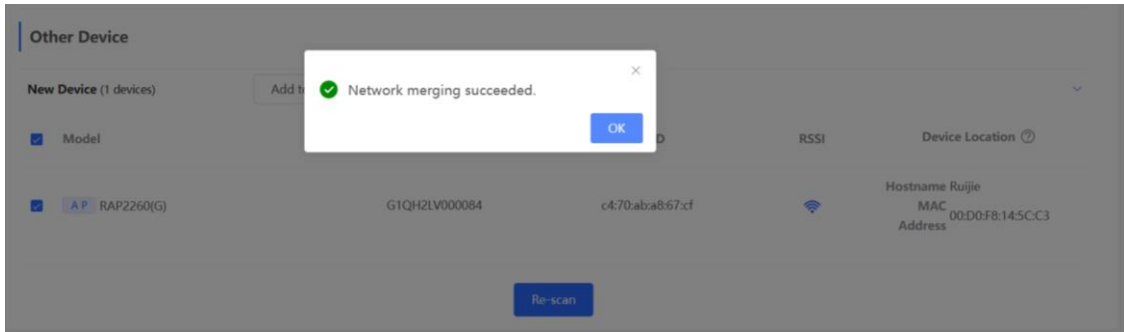
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.19__ for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

- (1) Power on the new AP and place it near the AP or EGW router on the target network.
- (2) Log in to the Eweb of a device on the target network. In **Network** mode, click **+AP** in the upper right corner of the **Overview** page to scan the APs in other networks not plugged in with Ethernet cables.

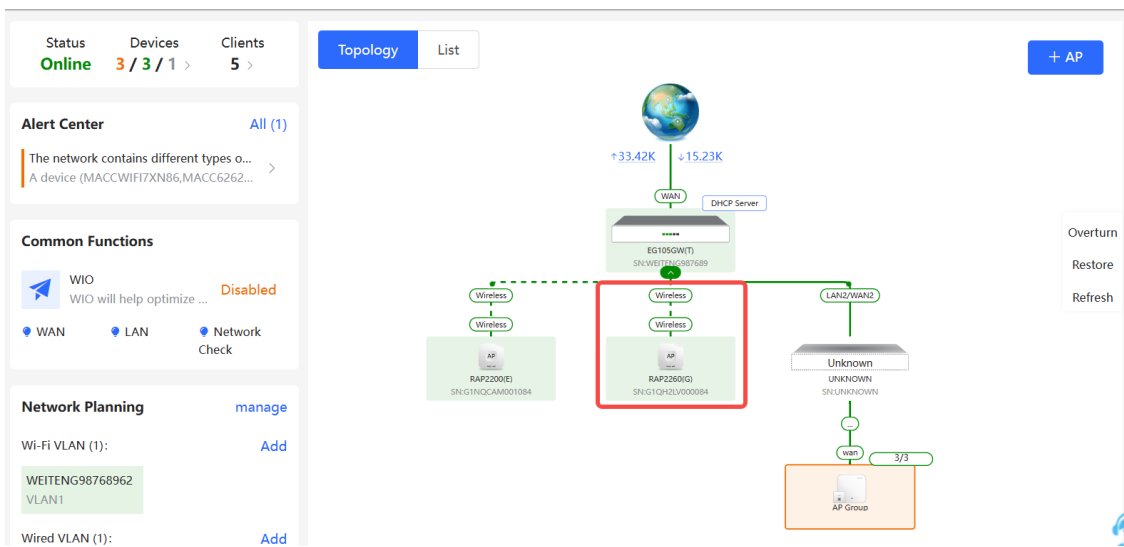


(3) Select the APs to be added and click **Add to My Network**. No more than eight APs are allowed at a time. Wait until network merging finishes.





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




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

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



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

SN	Status	Hostname	MAC Address	IP Address	Clients	Device Group	Relay Information
G1NQCAM001084	Online	Rujjie	8005:88:F0:19:90	192.168.110.31	0	egw默认/Default	5G View Details
G1QH2LV000084	Online	Rujjie	C470:AB:A8:67:CF	192.168.110.152	0	egw默认/Default	5G View Details

Click **View Details** following the  icon to obtain information about the uplink device and RSSI.

All (3) Gateway (0) **AP (2)** Switch (0) AC (0) Router (1)

Device List
A devices not in SON is discovered. [Manage](#)

Device List Group: All Groups Expand Change Group Basic Info RF Information Model

IP/MAC/hostname/SN/S Delete Offline Devices Batch Upgrade

SN	Status	Hostname	MAC Address
G1NQCAM001084	Online	Ruijie	80:05:88:F0:19:90
G1QH2LV000084	Online	Ruijie	C4:70:AB:A8:67:CF

Noise Floor: -86 dBm
Channel Utilization: 13 %
RSSI: -37 dBm **Good**
Negotiation Rate: 866 Mbps
Uptime: 4 minutes 4 seconds

Uplink 5G Local

EWR Ruijie AP Ruijie

Model: EG105GW(T) Model: RAP2260(G)
SN: WEITENG987689 SN: G1QH2LV000084
IP: 192.168.110.1 IP: 192.168.110.152

Relay Information

5G View Details

5G View Details

Total 2

5. Configuration Steps for Wired Pairing (Uplink Device is an AP, EG Router, or EGW Router)

Caution

- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see [3.19 Enabling Reyee Mesh](#) for details).

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

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

Navigation Overview Network **Devices** Gateway Clients Management System

All (2) Gateway (0) **AP (1)** Switch (0) AC (0) Router (1)

Device List
A devices not in SON is discovered. [Manage](#)

Device List IP/MAC/hostname/SN/S Delete Offline Devices Batch Upgrade

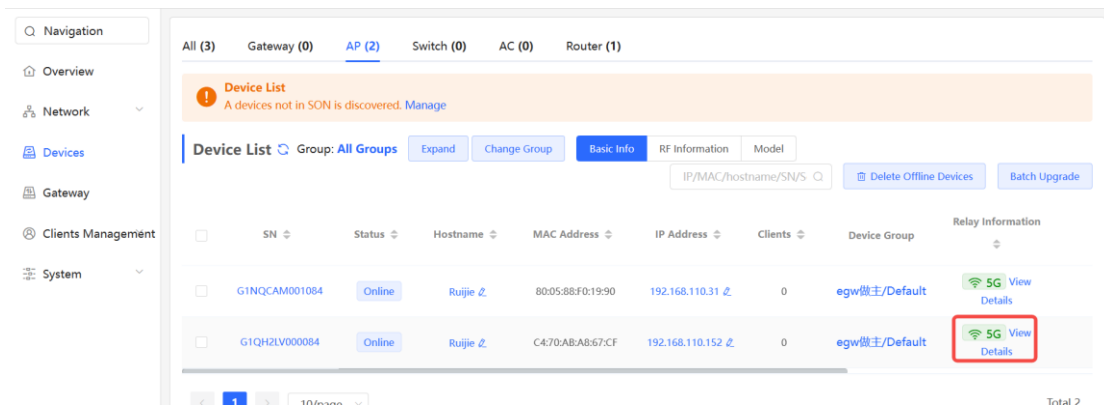
SN	Status	Hostname	MAC Address	IP Address	Software Ver	Model
WEITENG987689	Online	Ruijie [Master]	00:D0:F8:14:5C:C3	10.18.108.1	ReyeeOS	EG105GW(T)
G1NQCAM001084	Online	Ruijie	80:05:88:F0:19:90	192.168.110.31	ReyeeOS	RAP2200(E)

Total 2

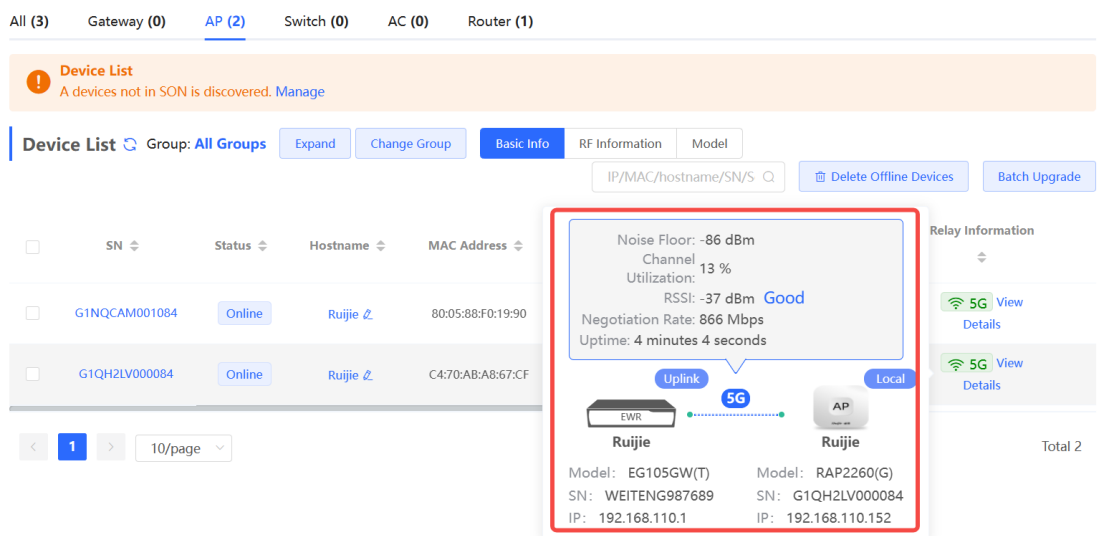
- (3) Unplug the Ethernet cable, power off the new AP, and install it as planned.
- (4) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices > AP**. Make sure that the new AP is online and the corresponding entry contains icon



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



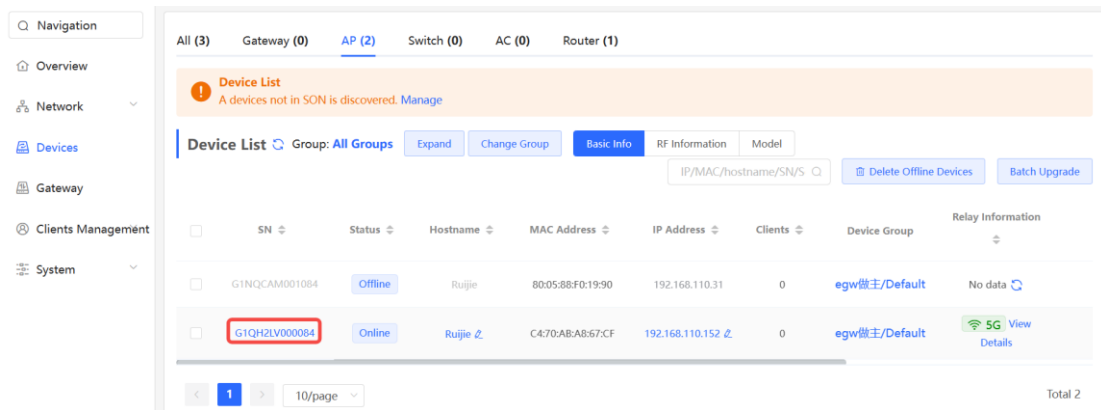
Click **View Details** following the  icon to obtain information about the uplink device and RSSI.



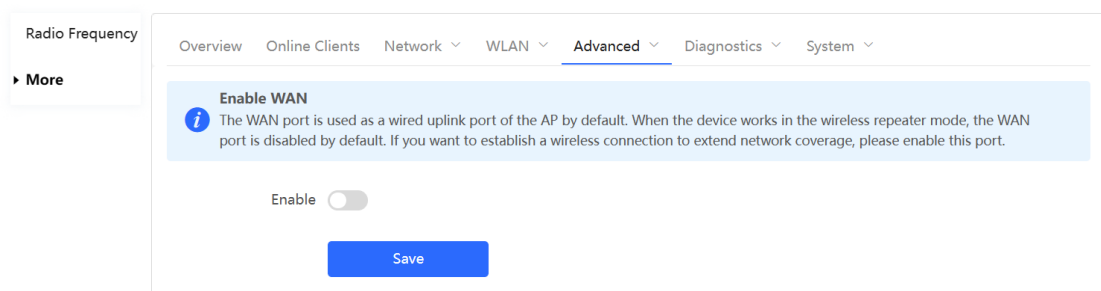
6. Enabling WAN Port

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

- (1) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices > AP** and click the serial number of the Mesh AP with the WAN port to be enabled.



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

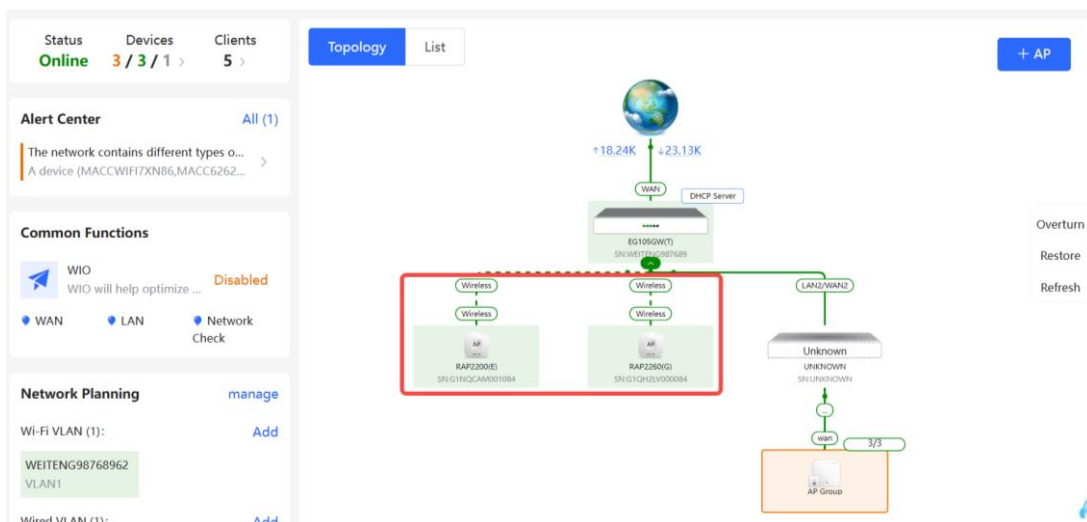


7. Querying Mesh APs and Mesh Details

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

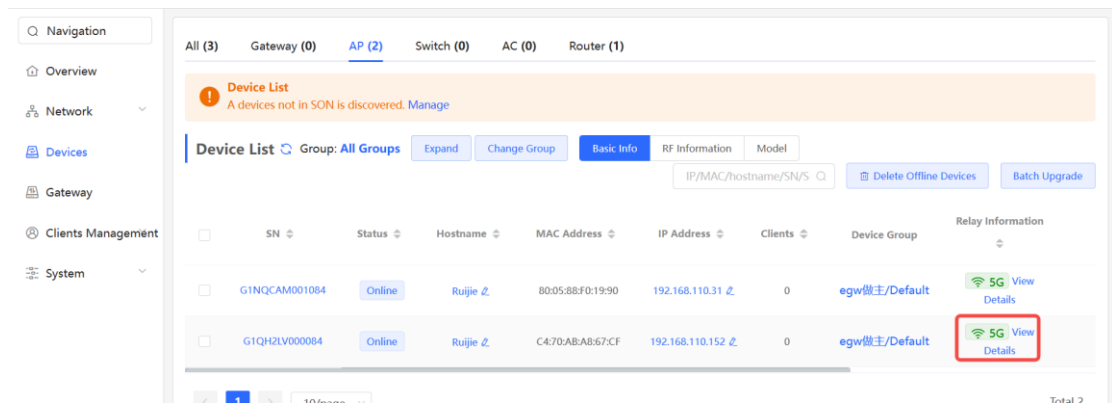
(2) Query Mesh APs.

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



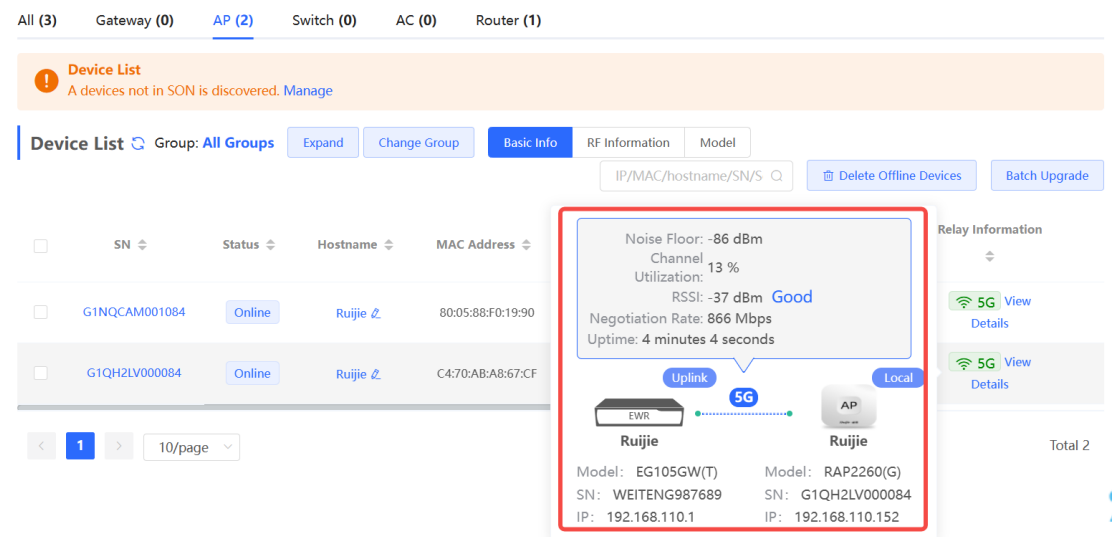
- Method 2: In **Network** mode, choose **Devices > AP**. If an entry contains icon 

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



(3) Query Mesh networking details.

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



2.3 Managing Network Devices

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

<input type="checkbox"/>	SN	Status	Hostname	MAC	IP	Software Ver	Model
<input type="checkbox"/>	MACCWLD789205GC	Online	rujije	78:11:22:33:44:55	192.168.110.226	ESW_	RG-ES205C-P
<input checked="" type="checkbox"/>	H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1	ReyeeOS	EG205G
<input type="checkbox"/>	G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	192.168.110.89	ReyeeOS	NBS5200-24SFP/8GT4XS
<input type="checkbox"/>	1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152	AP	RAP2200(E)
<input type="checkbox"/>	G1QH2LV00090C	Online	Ruijie	C4:70:AB:A8:69:17	192.168.110.102	ReyeeOS	RAP2260(G)

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

Hostname: Ruijie
Model: NBS5200-24SFP/8GT4XS
SN: G1NW31N000172
Software Ver: ReyeeOS
MGMT IP: 11.1.1.89
MAC: 00:D3:F8:15:08:5B

Port Status

VLAN

Interface	IP	IP Range	Remark
Gi2,Gi4,Gi6,Gi17-24,Te25-28,Ag1-4,Ag8	11.1.1.89		

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

Topology	List	IP/MAC/hostname/SN/S	Delete Offline Devices	Batch Upgrade		
SN	Status	Hostname	MAC	IP	Software Ver	Model
MACCWLD789205GC	Online	ruijie	78:11:22:33:44:55	192.168.110.226		RG-ES205C-P
H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1		EG205G
G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	11.1.1.89		NB55200-245FP/8GT4XS
G1QH2LV00090C	Offline	Ruijie	C4:70:AB:A8:69:17	192.168.110.102		RAP2260(G)
1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152		RAP2200(E)
MACCS22376524	Online	Ruijie	00:10:F8:75:33:72	192.168.110.200		EAP602

2.4 Configuring Network Planning

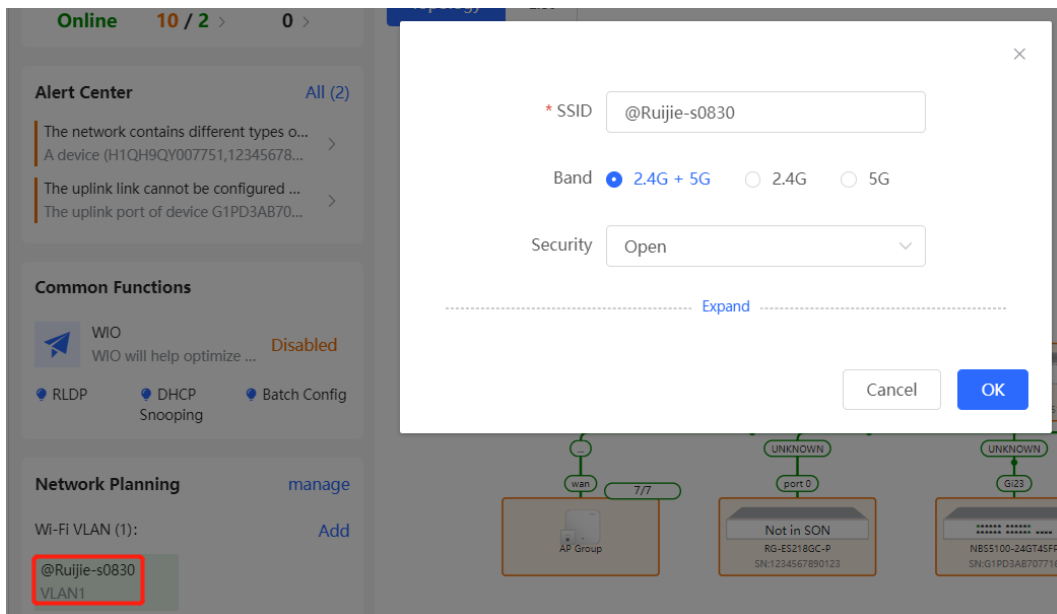
The **Overview** page displays the configuration of **Network Planning** at the bottom left corner, including **Wi-Fi VLAN** and **Wired VLAN**.

The screenshot shows the Network Monitoring Overview page. On the left, there is a sidebar with 'Status' (Online 10/2), 'Devices' (10/2), and 'Clients' (0). Below this is an 'Alert Center' with two alerts and 'Common Functions' including WIO (Disabled), RLD, DHCP Snooping, and Batch Config. The 'Network Planning' section is highlighted with a red box and contains:

- Wi-Fi VLAN (1):** @Ruijie-s0830, VLAN1
- Wired VLAN (3):** VLAN0001 (VLAN1), VLAN0002 (VLAN2), VLAN0003 (VLAN3)

The main area displays a network topology diagram with a central 'WAN' node connected to several 'UNKNOWN' nodes. A 'Not in SON' node is also present. A notification at the top right states 'A devices not in SON is discovered. Manage'. On the right side, there are buttons for 'Overturn', 'Restore', and 'Refresh'. The bottom of the diagram is updated on 2022-12-12 10:19:51.

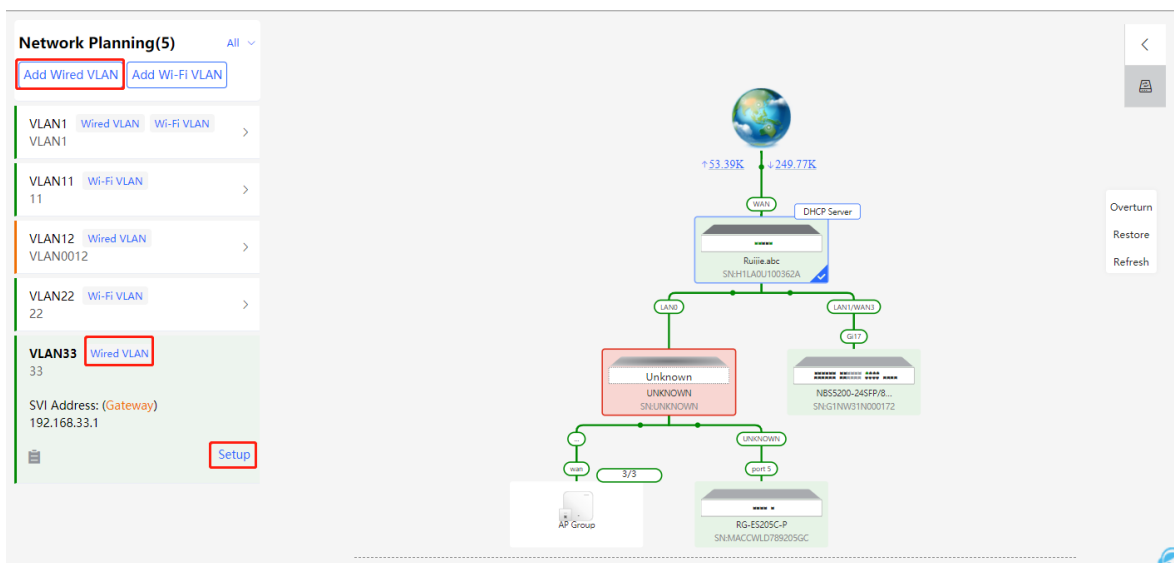
- Click **manage** to go to the **Network Planning** page for configuration (**Network > Network Planning**). You can add or edit the **Network Planning** configuration for the live network.
- Click **Add** to configure **Wi-Fi VLAN** or **Wired VLAN** for the live network.
- Click the SSID to edit the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



2.4.1 Configuring Wired VLAN

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

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



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

Configure Network Planning/Add Wired VLAN

1 Configure VLAN Parameters 2 Configure Wired Access 3 Confirm Config Delivery

Description:

* VLAN ID:

Address Pool Gateway

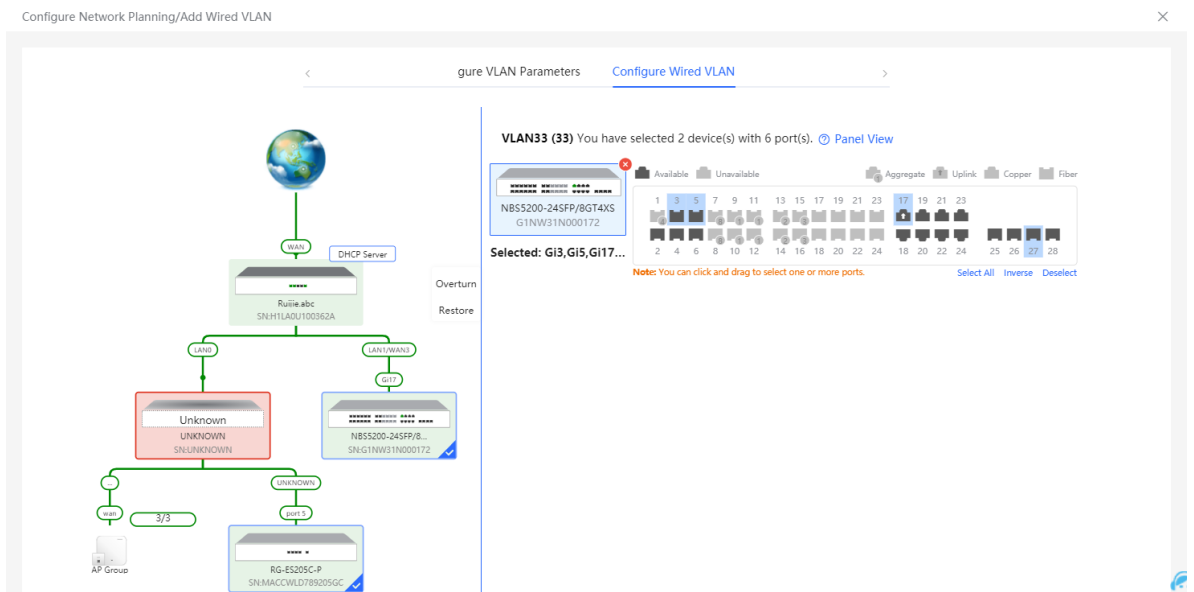
Server

Gateway/Mask: /

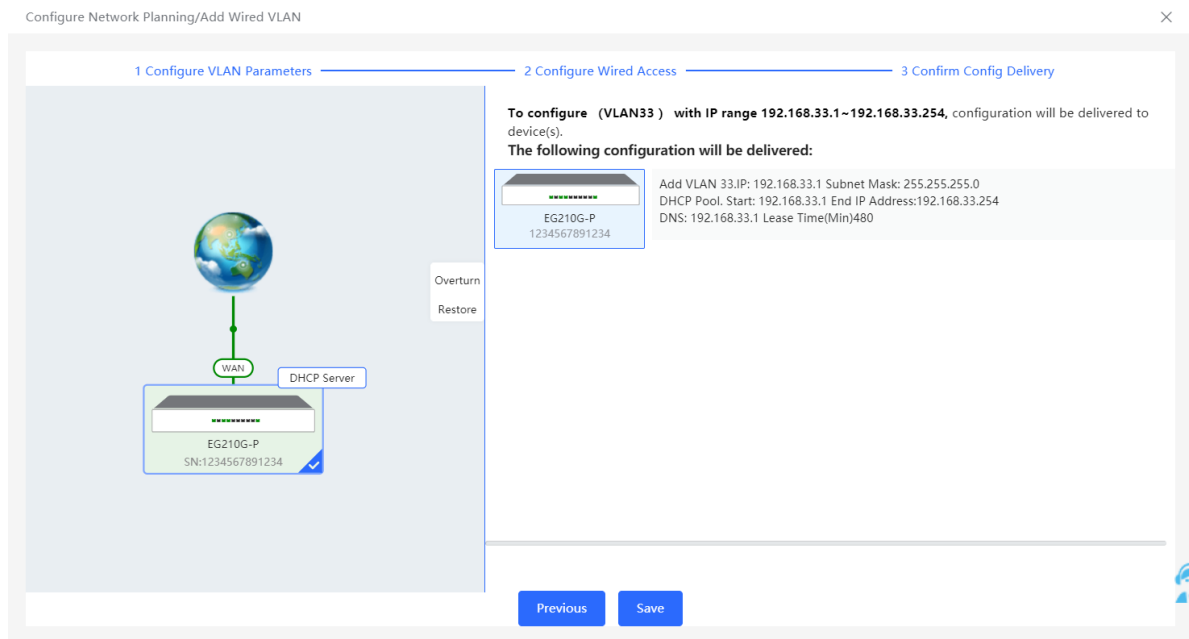
DHCP Pool:

IP Range: -

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



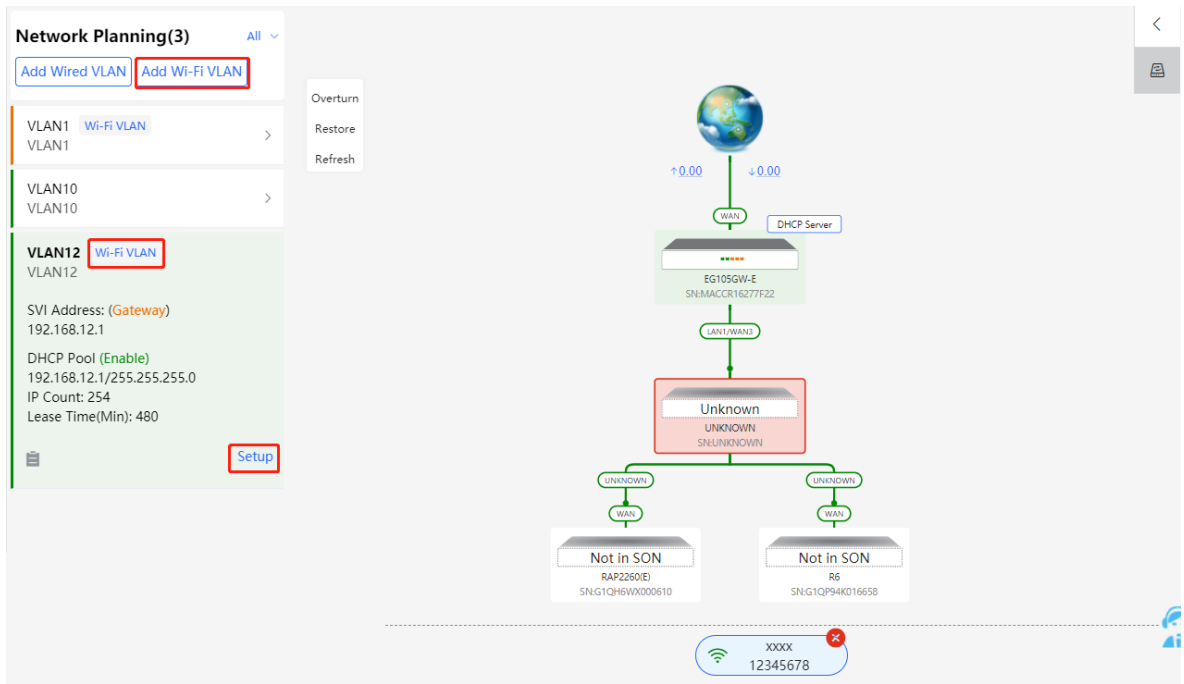
- (4) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



2.4.2 Configuring Wi-Fi VLAN

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

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

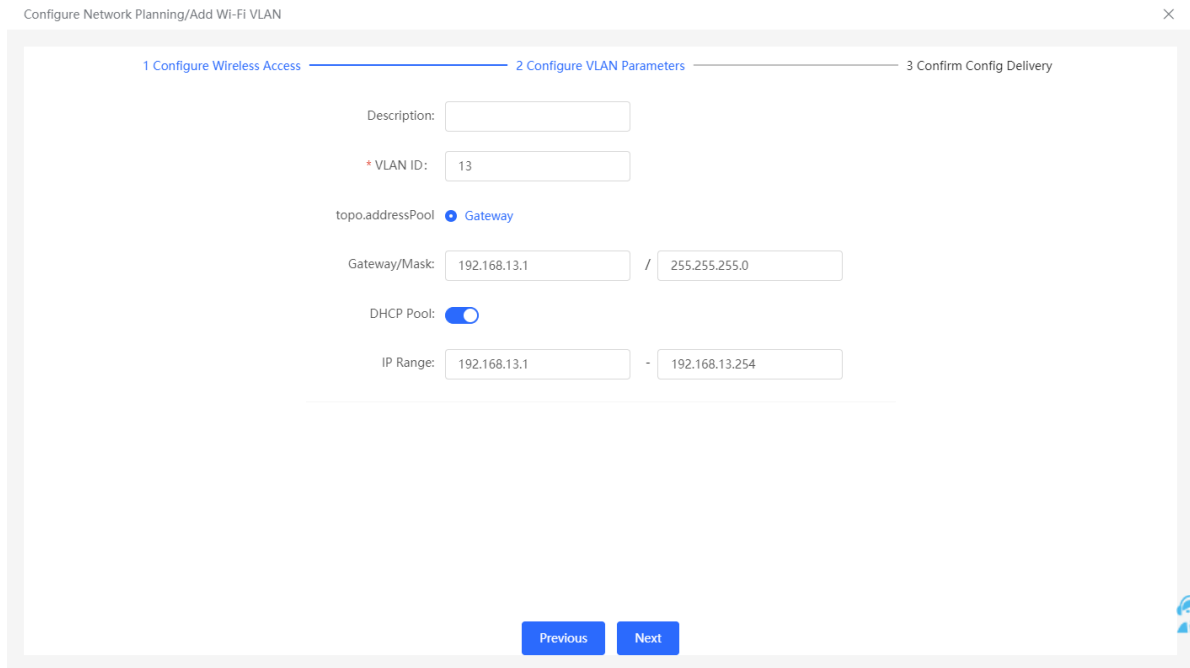


(2) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.

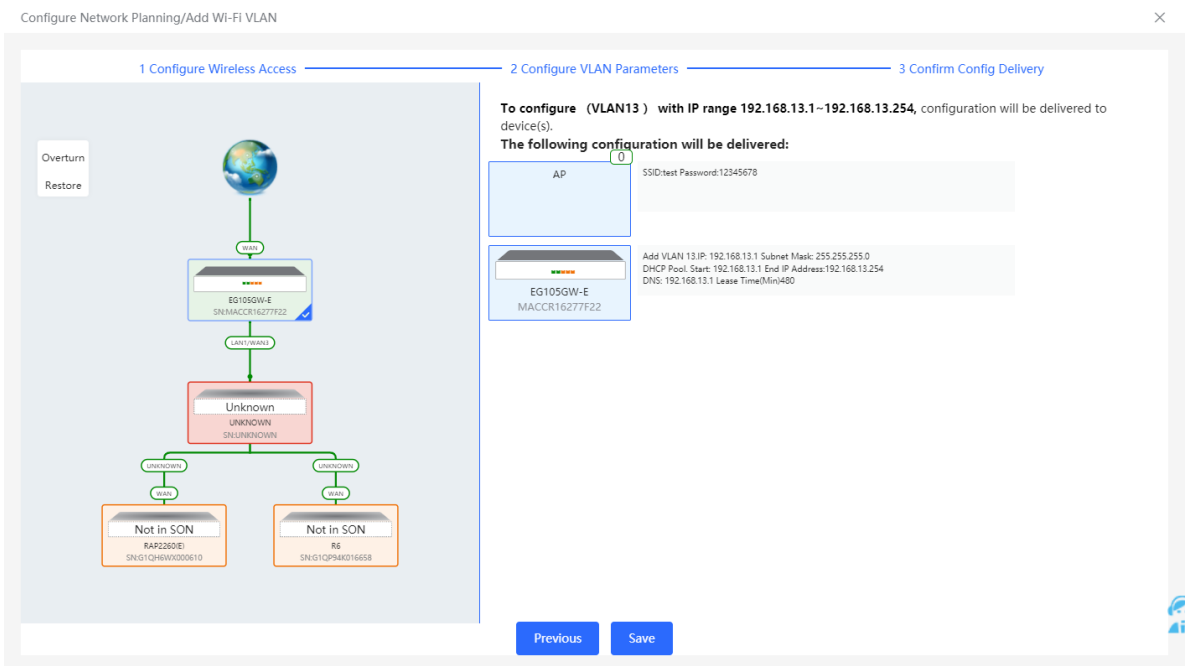
The configuration screen is titled 'Configure Network Planning/Add Wi-Fi VLAN'. It has three steps: 1. Configure Wireless Access, 2. Configure VLAN Parameters, and 3. Confirm Config Delivery. The current step is '1. Configure Wireless Access'. It contains the following fields and options:

- Information: The configuration will take effect after being delivered to AP.
- * SSID: [Empty text box]
- Band: 2.4G + 5G, 2.4G, 5G
- Security: Open (dropdown menu)
- Wireless Schedule: All Time (dropdown menu)
- Hide SSID: (The SSID is hidden and must be manually entered.)
- Client Isolation: Prevent wireless clients of this Wi-Fi from communicating with one another.
- Band Steering: (The 5G-supported client will access 5G radio preferentially.)
- XPress: (The client will faster speed.)
- Next button

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



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



2.5 Troubleshooting Fault Alerts

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

The screenshot shows a network monitoring interface with a blue header. On the left, there's a sidebar with navigation icons. The main area displays a network topology. At the top, it shows 'Status Online', 'Devices 1 / 1 / 5', and 'Clients 4'. Below this is the 'Alert Center' with a red border, containing the message: 'The gateway is not configured with a VLAN. The downlink port of device H1LA0U1...'. To the right of the alert center are 'Common Functions' (WIO, RLDP, DHCP Snooping, Batch Config) and 'Network Planning' (Setup). The topology shows a central 'Gateway' device (Ruijie abc, SN:H1LA0U100362A) connected to a 'WAN' (Earth icon) and a 'LAN2' (Unknown device). The 'LAN1/WAN3' port of the gateway is connected to a 'Switch' (NB55200-24SFP/8..., SN:G1NW31N000172). This switch is connected to a 'port 5' (Unknown device) and a 'WAN' (Earth icon). The 'port 5' device is connected to another 'Switch' (RG-ES205C-P, SN:MACCWLD789205GC). An 'AP Group' is also shown. On the right side of the topology, there are buttons for 'Overturn', 'Restore', and 'Refresh'. The bottom right corner shows 'Updated on:2022-04-29 17:31:18'.

This is a partial screenshot of the network monitoring interface, showing the 'Alert Center' and 'Network Planning' sections. The 'Alert Center' contains the same alert message as in the previous screenshot. The 'Network Planning' section shows 'Wi-Fi VLAN (1):' with '默认组_lgh' and 'VLAN1', and 'Wired VLAN (2):' with 'VLAN1' and 'VLAN0012'.

The screenshot shows the 'Alerts' section of the network monitoring interface. It features a blue header with an 'Alerts' icon. Below the header, there's a 'Current Alert' section with the message: 'The downlink port LAN1/WAN3 of device H1LA0U100362A is not allowed to be configured with allowed VLAN 12.' Below this is a 'Solution:' section with the text: 'Please configure the LAN IP address.' To the right of the alert message are buttons for 'Overturn' and 'Restore'. Below the alert section is a network topology diagram. The diagram shows a central 'Gateway' device (Ruijie abc, SN:H1LA0U100362A) connected to a 'WAN' (Earth icon) and a 'LAN2' (Unknown device). The 'LAN1/WAN3' port of the gateway is connected to a 'Switch' (NB55200-24SFP/8..., SN:G1NW31N000172). This switch is connected to a 'port 5' (Unknown device) and a 'WAN' (Earth icon). The 'port 5' device is connected to another 'Switch' (RG-ES205C-P, SN:MACCWLD789205GC). An 'AP Group' is also shown. On the right side of the topology, there are buttons for 'Overturn' and 'Restore'.

3 Wi-Fi Network Settings

Note

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

3.1 Configuring AP Groups

3.1.1 Overview

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


Note

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

3.1.2 Procedures

For RG-RAP2260(G), 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 models: In **Network** mode, choose  **Devices > AP**

For other RAP models, choose  **WLAN > APs**

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

The screenshot shows the 'Device List' page. At the top, there are navigation tabs: 'All (1)', 'Gateway (0)', 'AP (1)', 'Switch (0)', 'AC (0)', and 'Router (0)'. Below the tabs is a warning message: 'Device List: A devices not in SON is discovered. Manage'. The main content area has a header with 'Device List', a refresh icon, and 'Group: All Groups'. There are buttons for 'Expand', 'Change Group', 'Basic Info', 'RF Information', and 'Model'. A search bar contains 'IP/MAC/hostname/SN/S'. There are also buttons for 'Delete Offline Devices' and 'Batch Upgrade'. Below this is a table with columns: SN, Status, Hostname, MAC, IP, Clients, Device Group, and Relay Information. A single device is listed with SN 'G1QH6WX000610', Status 'Online', Hostname 'Ruijie [Master]', MAC 'EC:B9:70:23:A4:BF', IP '172.26.1.32', Clients '0', and Device Group 'defaultNetwork/默认'. A 'Local' tag is on the left. At the bottom, there is a pagination control showing '1' of 10 per page and a 'Total 1' count.

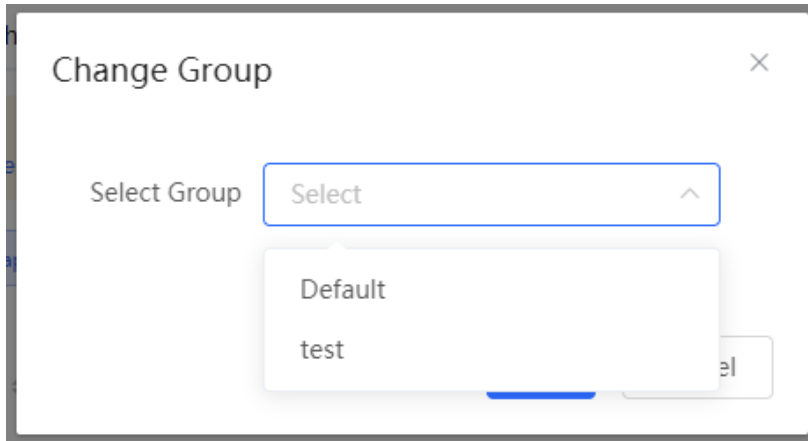
(1) Click **Expand** to view all groups on the left part of the **Device List** page. Click to create a new group. Up to 8 groups can be added. You can click to edit the group name and click to delete the group. The default group cannot be deleted and its name cannot be edited.

This close-up shows the 'Device List' header. It includes 'Device List', a refresh icon, 'Group: All Groups', and two buttons: 'Expand' (highlighted with a red box) and 'Change Group'.

This close-up shows the group selection area. It features a search bar 'Search by Group', a refresh icon, and 'SN'. Below is a dropdown menu with 'All Groups' selected. There are buttons for '+', 'edit', and 'delete'. A 'Local' tag is visible next to a device entry with SN 'G1QH6WX000610'.





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

Device List		Group: All Groups	Collapse	Change Group	Basic Info	RF Information	Model	IP/MAC/hostname/SN/S	Delete Offline Devices	Batch Upgrade
Search by Group	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information		
All Groups										
Default										
test	G1QH6WX000610	Online	Ruijie [Master]	ECB9:70:23:A4:BF	172.26.1.32	0	test/默认组	Wired View Details		



3.2 Configuring SSID and Wi-Fi Password

(1) Go to the page for configuration.

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

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

Caution

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

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

Default

rtk-11111
Default VLAN
Band:2.4G+5G

+ Add Guest Wi-Fi

+ Add Wi-Fi

* SSID

Band 2.4G 5G

Encryption Open Security 802.1x (Enterprise)

* Security

Expand

Save

Table 3-1 Wireless network configuration

Parameter	Description
SSID	The name displayed when a wireless client searches for a wireless network.
Band	The frequency band used for wireless data transmission. 2.4GHz and 5GHz frequency bands are supported. The 5GHz frequency band offers a faster transmission rate and less interference compared to the 2.4GHz frequency band, but it has weaker signal coverage and wall penetration. The frequency band can be selected according to actual needs. The default band is 2.4GHz+5GHz, on which Wi-Fi transmits on both the 2.4GHz and 5GHz bands.
Encryption	The encryption methods for wireless network connection. The following three encryption methods are supported: <ul style="list-style-type: none"> ● Open: A password is not required to connect to the Wi Fi network. There are two options: "OPEN (Open)" and "OWE (Enhanced Open)". ● Security: Options include WPA-PSK, WPA/WPA2-PSK, WPA2-PSK, WPA2-PSK/WPA3-SAE, and WPA3-SAE ● 802.1X (Enterprise): Options include WPA-802.1X, WPA/WPA2-802.1X,

Parameter	Description
	and WPA2-802.1X
Wi-Fi Password	When the encryption method is Encrypt, a Wi-Fi password needs to be entered. The password for connecting to the wireless network, consisting of 8-16 characters.
Server group	When the encryption method is 802.1x (Enterprise), a wireless server group needs to be selected. The server group for user authentication, authorization, and accounting is usually a RADIUS server.





3.3 Hiding the SSID

3.3.1 Overview

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

3.3.2 Configuration Steps

(1) Go to the page for configuration.

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

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

Caution

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

Wi-Fi Settings Device Group: Default

Up to **8** SSIDs can be added.

<p>Default</p> <p>rtk-11111</p> <p>Default VLAN</p> <p>Band:2.4G+5G</p>	<p>+ Add Guest Wi-Fi</p>	<p>+ Add Wi-Fi</p>
---	--------------------------	--------------------

* SSID

Band **2.4G** **5G**

Encryption **Open** Security 802.1x (Enterprise)

* Security

..... Collapse

Wireless Schedule

VLAN

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

3.4 Checking Wireless Clients

For RG-RAP2260(G), 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 models:

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

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

For other RAP models:

Choose **WLAN > Clients**

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

Wireless Client List
Refresh
Advanced Search

Username	MAC	IP	SN	Duration	RSSI	Rate	Band	SSID	Channel	Action
NULL	72:58:52:40	192.168.110.194	G1QH6WX000610	2022-04-01 09:40:36	-66	24M	5G	@Ruijie-s1234	64	Add to Blacklist

All (1) Wired (0) Wireless (1)

Online Clients ?

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

Online Clients
Search by IP/MAC/Username
Refresh

Username/Type	Access Location	IP/MAC	Current Rate	Wi-Fi
2.4G	G1QH6WX000610	172.26.1.73 62:cf:2f:84:bd:d0	Up:0.00bps Down:0.00bps	Channel:13 RSCP:-87 Duration:7 minutes 55 seconds Negotiation Rate:1M





Table 3-2 Description of Wireless Client Information

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

Item	Description
Current Rate	Uplink and downlink data rate.

3.5 Configuring Wi-Fi Band

(1) Go to the page for configuration.

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

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

Wi-Fi Settings Device Group:

Up to 8 SSIDs can be added.

Default

rtk-11111
Default VLAN
Band:2.4G+5G

+ Add Guest Wi-Fi

+ Add Wi-Fi

* SSID

Band 2.4G 5G

Encryption Open Security 802.1x (Enterprise)

* Security

Expand

3.6 Configuring Band Steering

⚠ Caution

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

(1) Go to the page for configuration.

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

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

Wi-Fi Settings Device Group:

Up to 8 SSIDs can be added.

<p>Default</p> <p>rtk-11111</p> <p>Default VLAN</p> <p>Band:2.4G+5G</p>	<p>+ Add Guest Wi-Fi</p>	<p>+ Add Wi-Fi</p>
--	--------------------------	--------------------

* SSID

Band 2.4G 5G

Encryption Open Security 802.1x (Enterprise)

* Security





..... Expand

3.7 Configuring Wi-Fi 6

Caution

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

(1) Go to the page for configuration.

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

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

[Collapse](#)

Wireless Schedule

VLAN


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

Client Isolation Prevent wireless clients of this Wi-Fi from communicating with one another.

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

XPress (The client will experience faster speed.)



Layer 3 Roaming (The client will keep the IP address unchanged on the Wi-Fi network.)

Wi-Fi6 (802.11ax high-speed wireless connectivity.) 

3.8 Configuring Layer-3 Roaming

(1) Go to the page for configuration.

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

- Method 2: Choose  **Network** ( **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.
- (2) Click **Expand**, turn on **Layer 3 Roaming** in the expanded settings and click **Save**. The client will keep the IP address unchanged in this Wi-Fi network, improving roaming experience across VLANs.

----- Collapse -----

Wireless Schedule

VLAN


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

Client Isolation Prevent wireless clients of this Wi-Fi from communicating with one another.

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





XPress (The client will experience faster speed.)

Layer 3 Roaming (The client will keep the IP address unchanged on the Wi-Fi network.)

Wi-Fi6 (802.11ax high-speed wireless connectivity.) 

3.9 Configuring AP Isolation

(1) Go to the page for configuration.

- Method 1: Choose  **Network** ( **WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
 - Method 2: Choose  **Network** ( **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.
- (2) Click **Expand**, turn on **AP Isolation** in the expanded settings and click **Save**. The clients joining in this Wi-Fi network will be isolated. The clients associated with the same access point cannot access each other.

----- Collapse -----

Wireless Schedule

VLAN





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

Client Isolation Prevent wireless clients of this Wi-Fi from communicating with one another.

3.10 Configuring 802.11r

The 802.11r feature is supported only when the encryption type is either WPA2-PSK or WPA2-802.1X.

(1) To access the configuration page, perform the following operations:

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

(2) Click to expand Advanced Settings. Enable **802.11r**, and click **Save**. After this feature is enabled, roaming time is reduced to achieve fast transition.

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

Client Isolation (Prevent wireless clients of this Wi-Fi from communicating with one another.)

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

XPress (The client will experience faster speed.)

Layer 3 Roaming (The client will keep the IP address unchanged on the Wi-Fi network.) ?

Wi-Fi6 (802.11ax high-speed wireless connectivity.) ?

802.11r (After this feature is enabled, roaming time is reduced to achieve fast transition.) ?





over the air

LimitSpeed

[Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.](#)

3.11 Adding a Wi-Fi Network

(1) Go to the page for configuration.

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

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

×

* SSID

Band **2.4G** **5G**

Encryption **Open** **Security** **802.1x (Enterprise)**

* Security

..... [Expand](#)

3.12 Configuring a Guest Wi-Fi

3.12.1 Overview

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

3.12.2 Configuration Steps

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

Click **Add Guest Wi-Fi** to configure the SSID and password of the Guest Wi-Fi. Click **Expand** to configure the effective time period and other Wi-Fi features in the expanded settings. Click

Save, and the guest Wi-Fi network will be created. Guests can access the guest Wi-Fi network by entering the SSID and Wi-Fi password.

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

Default
@Ruijie-s0830
Default VLAN
Band:2.4G + 5G

+ Add Guest Wi-Fi

+ Add Wi-Fi

* SSID @Ruijie-guest-21E1

Band 2.4G 5G

Encryption Open Security 802.1x (Enterprise)

* Security OPEN(Open)

Expand

Cancel OK

3.13 Configuring Wireless Rate Limiting

⚠ Caution

This function is supported by only RG-RAP2260(G), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP1260, RG-RAP2266, RG-RAP2260, and RG-RAP6262.

3.13.1 Overview

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

- **Client-based rate limiting:** This function allows you to limit the rate based on the MAC address of the client, so as to limit or guarantee the bandwidth required by specific clients.
- **SSID-based rate limiting:** This function provides two rate limiting modes for a specified SSID: **Rate Limit Per User** and **Rate Limit All Users**. **Rate Limit Per User** means that all clients connected to the SSID use the same rate limit. **Rate Limit All Users** means that the configured rate limit value is evenly allocated to all clients connected to the SSID. The rate

limit value of each client dynamically changes with the number of clients connected to the SSID.

- AP-based rate limiting: This function limits the client rates based on the whole network. All clients connected to the network will work according to the configured rate limit value.
- Packet-based rate limiting: This function limits the client rates based on the downlink broadcast and multicast packets. The device supports rate limiting for specific broadcast packets (such as ARP and DHCP), multicast packets (such as MDNS and SSDP), or all types of broadcast and multicast packets. If network stalling remains during network access and there is no client with large traffic, you are advised to adjust the rate between 1 kbps and 512 kbps.

3.13.2 Configuration Steps

1. Configuring Client-based Rate Limiting

Choose  **Network** ( **WLAN**) > **LimitSpeed** > **Client-based Rate Limiting**.

(1) Enable Wireless Rate Limiting.

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

Wireless Rate Limiting

Client-based Rate Limiting Wi-Fi-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

Client-based Rate Limiting
The rate limiting mode based on wireless clients can limit or provide the bandwidth for specific clients.

Client-based Rate Limiting + Add Delete Selected

Up to 512 entries can be added.

<input type="checkbox"/>	Client MAC	Uplink Rate Limit	Downlink Rate Limit	Remarks	Action
No Data					

< 1 > 10/page Total 0

Add ×

* Client MAC

Uplink Rate



Limit Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate

Limit Current: Kbps. Range: 1-1700000 Kbps

Remarks

2. Configuring SSID-based Rate Limiting

Method 1: Choose  **Network** ( **WLAN**) > **LimitSpeed** > **SSID-based Rate Limiting**.


(1) Enable Wireless Rate Limiting.

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

Wireless Rate Limiting

Client-based Rate Limiting SSID-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting


SSID-based Rate Limiting

 This function provides rate limit per user and dynamic rate limiting for a specified SSID. Rate Limit per User indicates that all clients connected to the SSID use the same rate limit. Rate Limit All Users indicates that all clients connected to the SSID share the rate limit in average. The priority of this function is lower than that of client-based rate limiting.

SSID-based Rate Limiting Device Group: Default [Are you sure you want to add a Wi-Fi? Click to go.](#)

SSID	Uplink Rate Limit	Downlink Rate Limit	Action
333	Rate Limit All Users 1111K bps	No Limit	Edit Disable
111	No Limit	No Limit	Edit Disable
wbctest	No Limit	No Limit	Edit Disable
@Ruijie-guest-6D85	Rate Limit All Users 111K bps	Rate Limit Per User 2M bps	Edit Disable

Edit ×

Uplink Rate Limit **Rate Limit Per User** Rate Limit All Users 

Rate Limit No Limit by Default. Kbps

Current: Kbps. Range: 1-1700000 Kbps





Downlink Rate Limit **Rate Limit Per User** Rate Limit All Users

Rate Limit No Limit by Default. Kbps

Current: Kbps. Range: 1-1700000 Kbps

Method 2:

(1) To access the configuration page, perform the following operations:

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

- Click to expand Advanced Settings. Enable **LimitSpeed**, set the uplink and downlink rate limit modes and rate limits, and click **Save**.

OKC (After this feature is enabled, complete 802.1X authentication is not required for roaming.)

LimitSpeed

Uplink Rate Limit Rate Limit Per User Rate Limit All Users

Rate Limit

Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate Limit Rate Limit Per User Rate Limit All Users

Rate Limit

Current: Kbps. Range: 1-1700000 Kbps

[Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.](#)

3. Configuring AP-based Rate Limiting

Choose **Network** (**WLAN**) > **LimitSpeed** > **AP-based Rate Limiting**.

- Enable Wireless Rate Limiting.
- Set the uplink and downlink rate limit modes to **Rate Limit Per User**, configure the rate limit values, and click **OK**.

Wireless Rate Limiting

Client-based Rate Limiting Wi-Fi-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

AP-based Rate Limiting
 This function provides client rate limiting based on the whole network. All devices connected to the network use the preset rate limiting value. The priority of this function is lower than that of client-based rate limiting and SSID-based rate limit per user.

AP-based Rate Limiting

Uplink Rate Limit No Limit Rate Limit Per User

Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate Limit No Limit Rate Limit Per User

Current: Kbps. Range: 1-1700000 Kbps

- Wechat texts, voice messages and webpage services: 1 Mbps to 2 Mbps.
- Real-time video calls and HD videos: 2 Mbps to 4 Mbps.
- Ultra HD/4K/Blue-ray videos and live videos: 5 Mbps to 10 Mbps.
- Other: You are not advised to set the value to 20 Mbps. It may affect the Internet experience of other users in the internal network.

4. Configuring Packet-based Rate Limiting

Choose  **Network ( WLAN) > LimitSpeed > Packet-based Rate Limiting.**


(1) Enable Wireless Rate Limiting.

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

Wireless Rate Limiting

Client-based Rate Limiting Wi-Fi-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

Packet-based Rate Limiting

 This function allows users to limit the downlink rate for broadcast and multicast packets. If the internet access is still slow and unstable when no client needs large amounts of traffic, you are advised to set the rate ranging from 1 Kbps to 512 Kbps. Smaller rate brings better network improvement.
[wqos.mcDescTip](#)

Packet-based Rate Limiting

Broadcast Rate Limiting Disable Limit All Limit Part

ARP Packet DHCP Packet

Multicast Rate Limiting Disable Limit All Limit Part

MDNS Packet SSDP Packet

* Rate Limit Kbps

Current: 0 Kbps. Range: 1-1700000 Kbps

3.14 Configuring Wi-Fi Blocklist or Allowlist

3.14.1 Overview

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

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

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

Caution

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

3.14.2 Configuration Steps

1. Configuring a Global Blocklist/Allowlist

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

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

Global Blocklist/Allowlist
SSID-Based Blocklist/Allowlist

All STAs except blocklisted STAs are allowed to access Wi-Fi.

Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

+ Add
Delete Selected

Up to 256 members can be added.

<input type="checkbox"/>	MAC Address	Remarks	Action
No Data			

<
1
>
10/page

Total 0

Add
×

Match Type **Full** Prefix (OUI)

* MAC

Remark

Cancel
OK

2. Configuring an SSID-based Blocklist/Allowlist

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

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

Global Blocklist/Allowlist SSID-Based Blocklist/Allowlist

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

Device Group: Default ▾

SSID-Based Blocklist/Allowlist

RAP2260E

All STAs except blocklisted STAs are allowed to access Wi-Fi.

Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients + Add Delete Selected

Up to 256 members can be added.

<input type="checkbox"/>	MAC Address	Remarks	Action
No Data			

< 1 > 10/page ▾ Total 0

3.15 Optimizing Wi-Fi Network

3.15.1 Overview

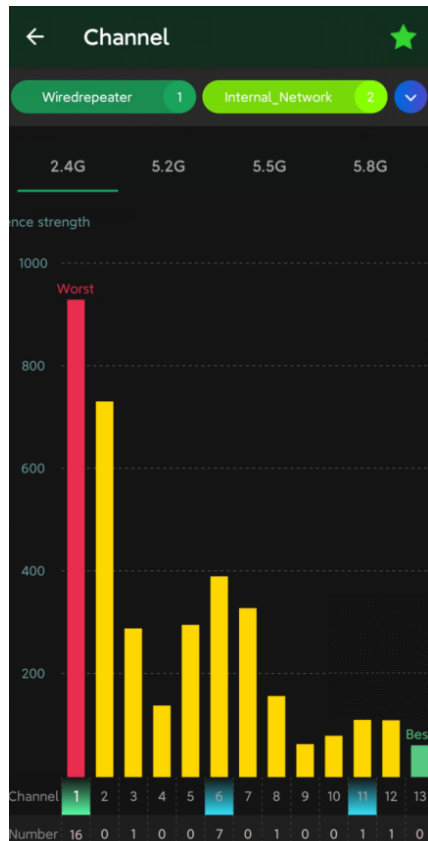
The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point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

Caution

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




3.15.2 Getting Started

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



3.15.3 Optimizing the Radio Channel

For RG-RAP2260(G), 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 models:

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

For other RAP models:

- Configure the master device. Choose  **WLAN** > **Radio Frequency**
- Configure the slave device. Choose  **WLAN** > **APs** > Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**

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

Note

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

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Multicast Rate (Mbps): Auto

Multicast Rate (Mbps): Auto

Client Count Limit: 64

Client Count Limit: 36 (5.18GHz), 40 (5.2GHz), 44 (5.22GHz), 48 (5.24GHz), 52 (5.26GHz), 56 (5.28GHz), 60 (5.3GHz)

Disconnection Threshold: Disable, -85dBm, -65dBm

Disconnection Threshold: 48 (5.24GHz), 52 (5.26GHz), 56 (5.28GHz), 60 (5.3GHz)

The settings are valid for only current device

2.4G Channel: Auto

5G Channel: Auto

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

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

Roaming: Low, 40%, 80%, High

Roaming: Low, 40%, 80%, High

3.15.4 Optimizing the Channel Width

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

A network with a lower channel width is more stable, while a network with a higher channel width is susceptible to interference. If the interference is severe, choose a lower channel width to avoid network stalling to a certain extent. The access point supports the channel width of 20 MHz and 40 MHz in the 2.4 GHz channel, and the channel width of 20 MHz and 40 MHz and 80 MHz and 160 MHz in the 5 GHz channel.

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

Caution

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

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width Auto **5G Channel Width** Auto

Multicast Rate (Mbps): Auto Multicast Rate (Mbps): Auto

Client Count Limit: 64 Client Count Limit: 20MHz

Disconnection Threshold: Disable -85dBm -65dBm Disconnection Threshold: Disable -85dBm -65dBm




The settings are valid for only **current device**

2.4G Channel Auto **5G Channel** Auto

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

3.15.5 Optimizing the Transmit Power

For RG-RAP2260(G), 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 models:

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

For other RAP models:

- Configure the master device. Choose  **WLAN > Radio Frequency**
- Configure the slave device. Choose  **WLAN > APs** > Select the target device in the device list and click **Manage > WLAN > Radio Frequency**

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

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

Multicast Rate (Mbps): Auto

Client Count Limit: 64

Disconnection Threshold: Disable -85dBm -65dBm

5G Channel Width: Auto

Multicast Rate (Mbps): Auto (Dropdown menu: 20MHz, 40MHz, 80MHz, 160MHz)

Client Count Limit: 64

Disconnection Threshold: Disable -85dBm -65dBm

The settings are valid for only **current device**

2.4G Channel: Auto

5G Channel: Auto

Transmit Power: Auto Lower Low Medium High

Roaming: Low 40% 80% High

Access Threshold: Disable -85dBm -65dBm

3.15.6 Configuring the Multicast Rate

⚠ Caution

This function is supported by only RG-RAP2260(G), 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.

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

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

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Multicast Rate (Mbps): Auto

Multicast Rate (Mbps): Auto

Client Count Limit: 64

Client Count Limit: OFDM 6, OFDM 9, OFDM 12, OFDM 18, OFDM 24, OFDM 36, OFDM 48

Disconnection Threshold: Disable, -85dBm, -65dBm

Disconnection Threshold: Disable, -85dBm, -65dBm

The settings are valid for only current device

2.4G Channel: Auto

5G Channel: Auto

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

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

3.15.7 Configuring the Client Limit

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

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

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Multicast Rate (Mbps): Auto

Multicast Rate (Mbps): Auto

Client Count Limit: 64

Client Count Limit: 512

Disconnection Threshold: Disable, -85dBm, -65dBm

Disconnection Threshold: Disable, -85dBm, -65dBm

The settings are valid for only current device

2.4G Channel: Auto

5G Channel: Auto

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

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

Note


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

3.15.8 Configuring the Kick-off Threshold

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

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

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

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

Radio Frequency Device Group:

Country/Region

2.4G Channel Width **5G** Channel Width

Multicast Rate (Mbps) Multicast Rate (Mbps)

Client Count Limit Client Count Limit

Disconnection Threshold Disconnection Threshold

The settings are valid for only **current device**

2.4G Channel **5G** Channel




Transmit Power Transmit Power

Caution


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

3.15.9 Configuring the Roaming Sensitivity

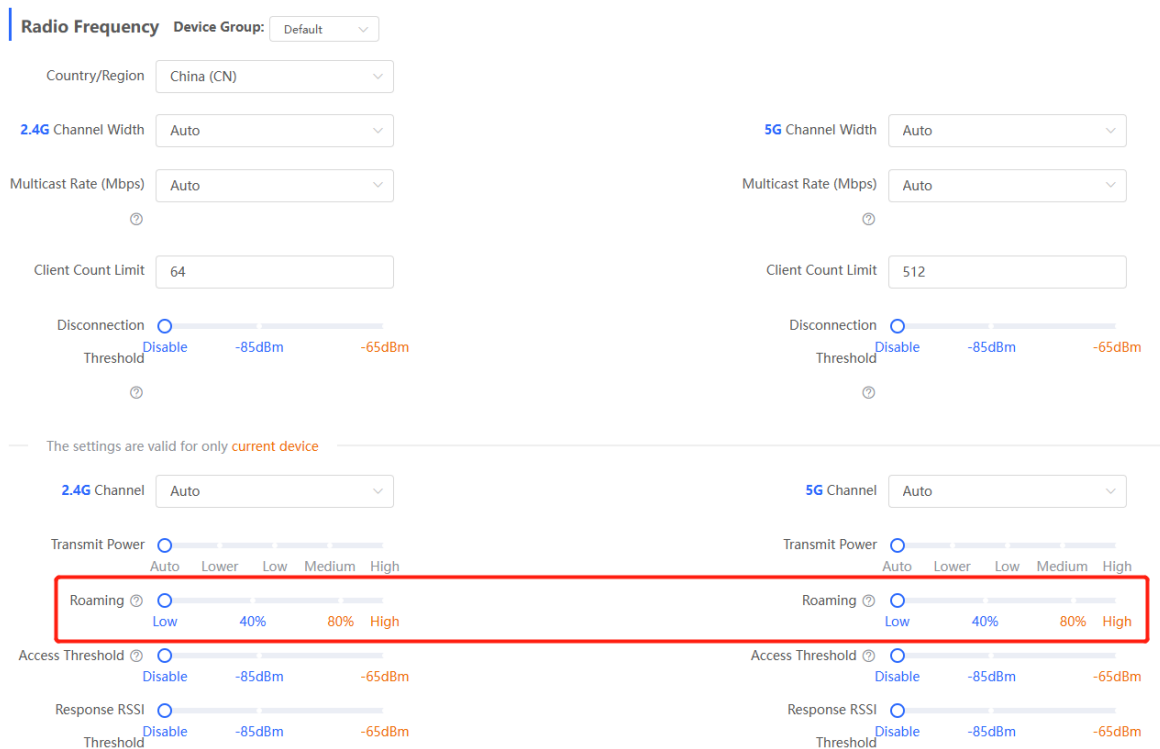
For RG-RAP2260(G), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

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

For other RAP models:

- Configure the master device. Choose  **WLAN** > **Radio Frequency**
- Configure the slave device. Choose  **WLAN** > **APs** > Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**




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




The screenshot shows the configuration interface for Radio Frequency settings. It is divided into two columns for 2.4G and 5G configurations. The 'Roaming' setting is highlighted with a red box. The 'Roaming' slider is set to 'Low', with '40%' and '80%' markers visible. Other settings include Country/Region (China (CN)), Channel Width (Auto), Multicast Rate (Mbps) (Auto), Client Count Limit (64 for 2.4G, 512 for 5G), Disconnection Threshold (Disable, -85dBm, -65dBm), Transmit Power (Auto, Lower, Low, Medium, High), Access Threshold (Disable, -85dBm, -65dBm), and Response RSSI Threshold (Disable, -85dBm, -65dBm). A note at the bottom states 'The settings are valid for only current device'.

3.15.10 Configuring Access Threshold

For RG-RAP2260(G), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP1261, RG-RAP1260, RG-RAP2260 and RG-RAP6262 models:

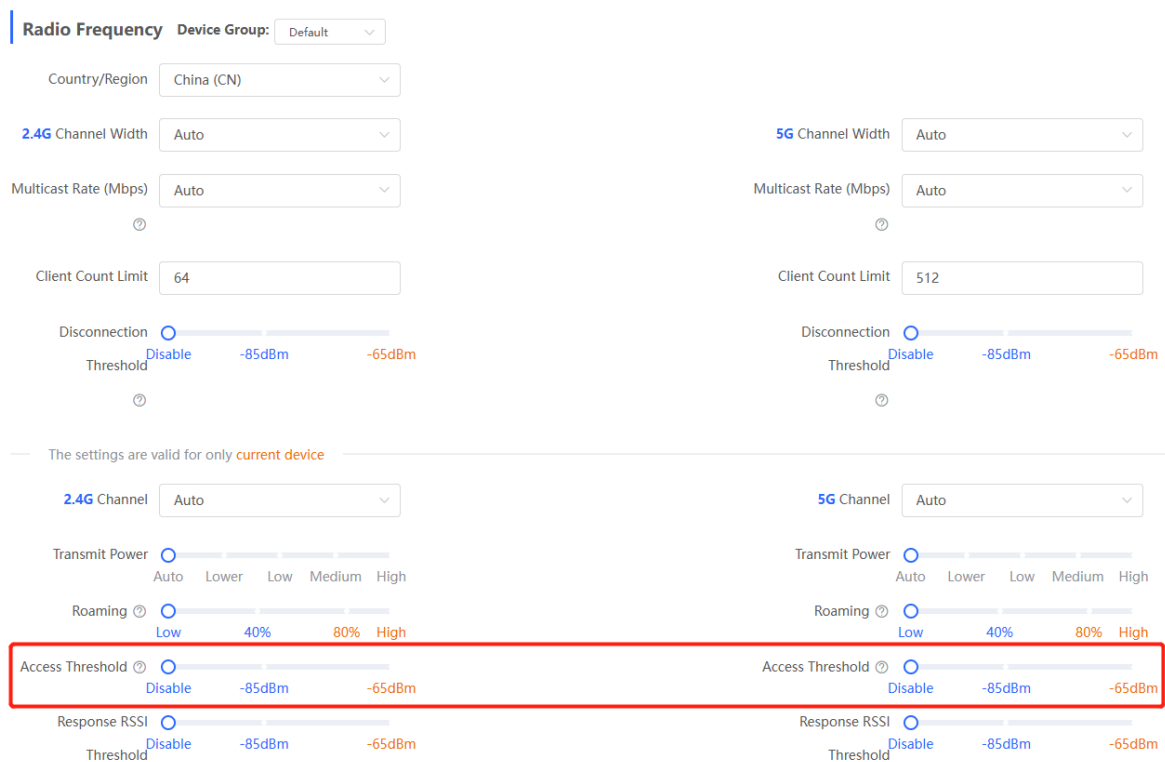
- Configure the master device. Choose  **Network** ( **WLAN**) > **Radio Frequency**
- Configure the slave device. Choose  **Devices** > Select the target device in the device list and click **SN** > **Radio Frequency**

For other RAP models:

- Configure the master device. Choose  **WLAN** > **Radio Frequency**

Configure the slave device. Choose  **WLAN** > **APs** > Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**

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



The screenshot displays the 'Radio Frequency' configuration page. At the top, there is a 'Device Group' dropdown set to 'Default'. Below this, the page is divided into two columns for 2.4G and 5G settings. Each column includes dropdowns for 'Country/Region' (set to 'China (CN)'), 'Channel Width' (set to 'Auto'), and 'Multicast Rate (Mbps)' (set to 'Auto'). There are also input fields for 'Client Count Limit' (64 for 2.4G, 512 for 5G) and sliders for 'Disconnection Threshold' (set to 'Disable'). A note states 'The settings are valid for only current device'. The bottom section contains sliders for 'Transmit Power' (set to 'Auto'), 'Roaming' (set to 'Low'), 'Access Threshold' (set to 'Disable'), and 'Response RSSI Threshold' (set to 'Disable'). A red rectangular box highlights the 'Access Threshold' settings for both 2.4G and 5G channels.

3.15.11 Configuring Response RSSI Threshold

For RG-RAP2260(G), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP1261, RG-RAP1260, RG-RAP2260 and RG-RAP6262 models:

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

For the other RAP models:

- Configure the master device. Choose **WLAN** > **Radio Frequency**

Configure the slave device. Choose **WLAN** > **APs** > Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**

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

The screenshot displays the 'Radio Frequency' configuration page. At the top, there is a 'Device Group' dropdown set to 'Default'. Below this, the 'Country/Region' is set to 'China (CN)'. The page is split into two columns for 2.4G and 5G settings. For 2.4G, 'Channel Width' and 'Multicast Rate (Mbps)' are both set to 'Auto', and 'Client Count Limit' is 64. For 5G, 'Channel Width' and 'Multicast Rate (Mbps)' are both set to 'Auto', and 'Client Count Limit' is 512. Both columns feature a 'Disconnection Threshold' slider with markers for 'Disable', '-85dBm', and '-65dBm'. A note states 'The settings are valid for only current device'. Below this, there are sliders for '2.4G Channel', '5G Channel', 'Transmit Power' (with markers for Auto, Lower, Low, Medium, High), 'Roaming' (with markers for Low, 40%, 80%, High), and 'Access Threshold'. The 'Response RSSI Threshold' slider at the bottom is highlighted with a red box, showing markers for 'Disable', '-85dBm', and '-65dBm'.

3.15.12 Configuring WIO

For RG-RAP2260(G), 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 models: In **Network** mode, choose  **Network > WIO**

For the other RAP models: Choose  **WLAN > WIO**

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

Caution

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

Table 3-3 Description of Tuning Mode

Parameter	Description
Quick tuning	In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power.
Deep tuning	<p>In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand Advanced Settings to configure the scanning time, channel bandwidth and channels.</p> <ul style="list-style-type: none"> ● Scanning time: Indicates the time for scanning channels during the optimization. ● Roaming Sensitivity: The roam sensitivity can be optimized based on the actual environment to ensure fast roaming of wireless devices. ● Transmit power: Increasing the transmit power enhances both the strength and coverage of the wireless signal, but it may also introduce interference to surrounding wireless networks. With this feature enabled, the AP will automatically adjust the transmit power based on the environment. ● 2.4G <ul style="list-style-type: none"> ○ Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized. ● 5G

Parameter	Description
	<ul style="list-style-type: none"> ○ Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized.

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

[Network Optimization](#)
 [Scheduled Optimization](#)
 [Optimization Record](#)
 [802.11k/v Roaming Optimization](#)



Wireless Intelligent Optimization

In a network environment, we will optimize your network to maximize wireless performance. Please use it after all APs in the optimization area are fully online.

Optimization configuration

Tuning mode: Quick tuning Deep tuning

Estimated time consumed

180s Environment scan + 3 minute Optimization configuration

OK

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

[Network Optimization](#)
 [Scheduled Optimization](#)
 [Optimization Record](#)
 [802.11k/v Roaming Optimization](#)



Wireless Intelligent Optimization

In a network environment, we will optimize your network to maximize wireless performance. Please use it after all APs in the optimization area are fully online.

Optimization configuration

Tuning mode: Quick tuning Deep tuning

..... [Advanced Settings](#)

..... [Advanced Settings](#)

Scan time

Roaming

Sensitivity

Transmit Power

2.4G

Channel Width

* Selected channels

1 (2.412GHz) <input type="checkbox"/>	2 (2.417GHz) <input type="checkbox"/>
3 (2.422GHz) <input type="checkbox"/>	4 (2.427GHz) <input type="checkbox"/>
5 (2.432GHz) <input type="checkbox"/>	6 (2.437GHz) <input type="checkbox"/>
7 (2.442GHz) <input type="checkbox"/>	8 (2.447GHz) <input type="checkbox"/>
9 (2.452GHz) <input type="checkbox"/>	10 (2.457GHz) <input type="checkbox"/>
11 (2.462GHz) <input type="checkbox"/>	12 (2.467GHz) <input type="checkbox"/>
13 (2.472GHz) <input type="checkbox"/>	

5G

Channel Width

* Selected channels

36 (5.18GHz) <input type="checkbox"/>	40 (5.2GHz) <input type="checkbox"/>
44 (5.22GHz) <input type="checkbox"/>	48 (5.24GHz) <input type="checkbox"/>
52 (5.26GHz) (Radar channel) <input type="checkbox"/>	
56 (5.28GHz) (Radar channel) <input type="checkbox"/>	
60 (5.3GHz) (Radar channel) <input type="checkbox"/>	
64 (5.32GHz) (Radar channel) <input type="checkbox"/>	
149 (5.745GHz) <input type="checkbox"/>	153 (5.765GHz) <input type="checkbox"/>
157 (5.785GHz) <input type="checkbox"/>	161 (5.805GHz) <input type="checkbox"/>
165 (5.825GHz) <input type="checkbox"/>	

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

Click **Back to homepage** to perform wireless optimization again.

[Network Optimization](#) [Scheduled Optimization](#) [Optimization Record](#) [802.11k/v Roaming Optimization](#)



Finish

Optimization completion time: 2023-06-12 11:10:44

Tuning mode: Quick tuning

Time consumed: 36 seconds, optimized 1 APs, resolved severe interference on 1 APs, resulting in a 0.00% decrease in overall channel interference and an 0.00% improvement in overall network experience.

Cancel Optimization

Back to homepage

Optimization details

Search Name/SN

5G 2.4G

Hostname	Band	SN	Channel Width (Before/After)	Channel (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)
Ruijie	5G	1234942571121	160->80	64->36	auto	0

< 1 > 10/page Total 1

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

[Network Optimization](#) [Scheduled Optimization](#) [Optimization Record](#) [802.11k/v Roaming Optimization](#)



Finish

Optimization completion time: 2023-06-12 11:10:44

Tuning mode: Quick tuning

Time consumed: 36 seconds, optimized 1 APs, resolved severe interference on 1 APs, resulting in a 0.00% decrease in overall channel interference and an 0.00% improvement in overall network experience.

Cancel Optimization

Optimization Record

[Network Optimization](#) [Scheduled Optimization](#) [Optimization Record](#) [802.11k/v Roaming Optimization](#)

Last Optimized:2023-06-12 11:10:44
Time consumed: 36 seconds, optimized 1 APs, resolved severe interference on 1 APs, resulting in a 0.00% decrease in overall channel interference and an 0.00% improvement in overall network experience.

Optimization details

Search Name/SN

5G 2.4G

Hostname	Band	SN	Channel Width (Before/After)	Channel (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)
Ruijie	5G	1234942571121	160->80	64->36	auto	0

< 1 > 10/page Total 1

You are advised to set a scheduled task to optimize the wireless network in the early hours of the morning or when the network is idle.

Network Optimization Scheduled Optimization Optimization Record 802.11k/v Roaming Optimization

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

Enable

Day Mon

Time 00 : 00

Tuning mode: Quick tuning Deep tuning


Save

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

Caution

This function is not supported by RG-RAP1200(F) and RG-RAP2200(F).

For RG-RAP2260(G), 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 models: In **Network** mode, choose  **Network > WIO > Wi-Fi Roaming Optimization (802.11k/v)**.

For the other RAP models: Choose  **WLAN > WIO > Wi-Fi Roaming Optimization (802.11k/v)**.

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

Caution

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

Network Optimization Scheduled Optimization Optimization Record 802.11k/v Roaming Optimization

Start — Scanning — Optimizing — Finish

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

Notes:
 During the WLAN environment scanning, the APs will switch channels, forcing the clients to go offline. The process will last for 2 minutes.

Optimization Mode Performance-prior Roaming-prior ?

Enable

Table 3-4 Optimization Mode

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

Network Optimization Scheduled Optimization Optimization Record 802.11k/v Roaming Optimization

Start — Scanning — Optimizing — Finish

802.11k/v Roaming Optimization Scanning

Start: 2023-06-12 11:17:11
 Expected Time: 2 minute

10%

Network Optimization Scheduled Optimization Optimization Record 802.11k/v Roaming Optimization

Start — Scanning — Optimizing — Finish

Optimization is enabled.

Optimization finished on 2023-06-12 11:17:47
 Time: 36 seconds
 To ensure smart roaming effect, please [Click Here](#) to scan the WLAN environment again if the topology changes.


Disable

3.16 Configuring Healthy Mode

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

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

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

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

Healthy Mode Device Group: Default





Enable

Effective Time All Time

Save

3.17 Configuring XPress

(1) Go to the page for configuration.

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

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

Collapse

Wireless Schedule

VLAN

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

Client Isolation Prevent wireless clients of this Wi-Fi from communicating with one another.

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

XPress (The client will experience faster speed.)

3.18 Configuring Wireless Schedule

(1) Go to the page for configuration.

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

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

* SSID

Band 2.4G + 5G 2.4G 5G

Security

Collapse

Wireless Schedule


VLAN

Hide SSID manually

Client Isolation Wi-Fi from


3.19 Enabling Reyee Mesh

For RG-RAP2260(G), 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 models: In **Network** mode, choose  **Network > Reyee Mesh**

For the other RAP models: Choose  **WLAN > APs > Manage > Advanced > Reyee Mesh**

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

 After enabling Reyee Mesh, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh.

Enable

Save

3.20 Configuring AP Load Balancing

Caution

This function is supported by only RG-RAP series access points.

3.20.1 Overview

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

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

Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated

with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only with AP2.

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

3.20.2 Configuring Client Load Balancing

Choose  **Network** ( **WLAN**) > **Wi-Fi** > **Load Balancing**.

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

Load Balancing
+ Add
Delete Selected

Up to **32** entries can be added.
 Add APs in an area into a group and enable load balancing. When load is unbalanced in the group, clients will automatically associate to an AP with lighter load.
 Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only to AP2.


	Group Name	Type	Rule	Members	Action
No Data					

Add
×

* Group Name

* Type

* Rule

When an AP is associated with  clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches , clients can associate only to another AP in the group. After a client association is denied by an AP for times, the client will be allowed to associate to the AP upon the next attempt.

* Members

Cancel
OK

Table 3-5 Client load balancing configuration

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

3.20.3 Configuring Traffic Load Balancing

Choose  **Network** ( **WLAN**) > **Wi-Fi** > **Load Balancing**.

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

Load Balancing + Add Delete Selected

Up to **32** entries can be added.
 Add APs in an area into a group and enable load balancing. When load is unbalanced in the group, clients will automatically associate to an AP with lighter load.
 Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only to AP2.

	Group Name	Type	Rule	Members	Action
No Data					

Add
×

* Group Name

* Type Traffic Load Balancing ▼

* Rule

When the traffic load on an AP reaches *100Kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches *100Kbps, clients can associate only to another AP in the group. After a client association is denied by an AP for times, the client will be allowed to associate to the AP upon the next attempt.

* Members Enter an AP name or SN. ▼

Cancel
OK

Table 3-6 Traffic load balancing configuration

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

Parameter	Description
Members	Specify the APs to be added to the AP load balancing group.

3.21 Wireless Authentication

Caution

This function is supported by only RG-RAP2260(G), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP1261, RG-RAP1260, RG-RAP2260, and RG-RAP6262.

3.21.1 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 blacklist) to access the network without authentication. The AP forbids STAs whose MAC addresses are added to the MAC address blacklist configured on the Eweb management system from accessing the network. For other users or domain names, the AP redirects them to the portal authentication page. Users need to complete identity verification on the portal page.

The following four authentication modes are supported:

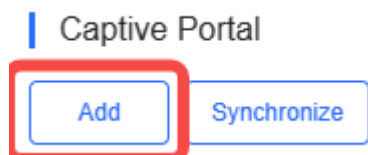
- One-click Login: indicates login without the username and password.
- Voucher: indicates login with a random eight-digit password.
- Account: indicates login with the account and password.
- SMS: indicates login with the phone number and code.

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

3.21.2 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.

Name

Description

Login Options One-click Login Voucher Account SMS Registration Facebook Account

Access Duration (Min)

Access Times Per Day

Show Balance Page

Post-login URL

Table 3-7 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.

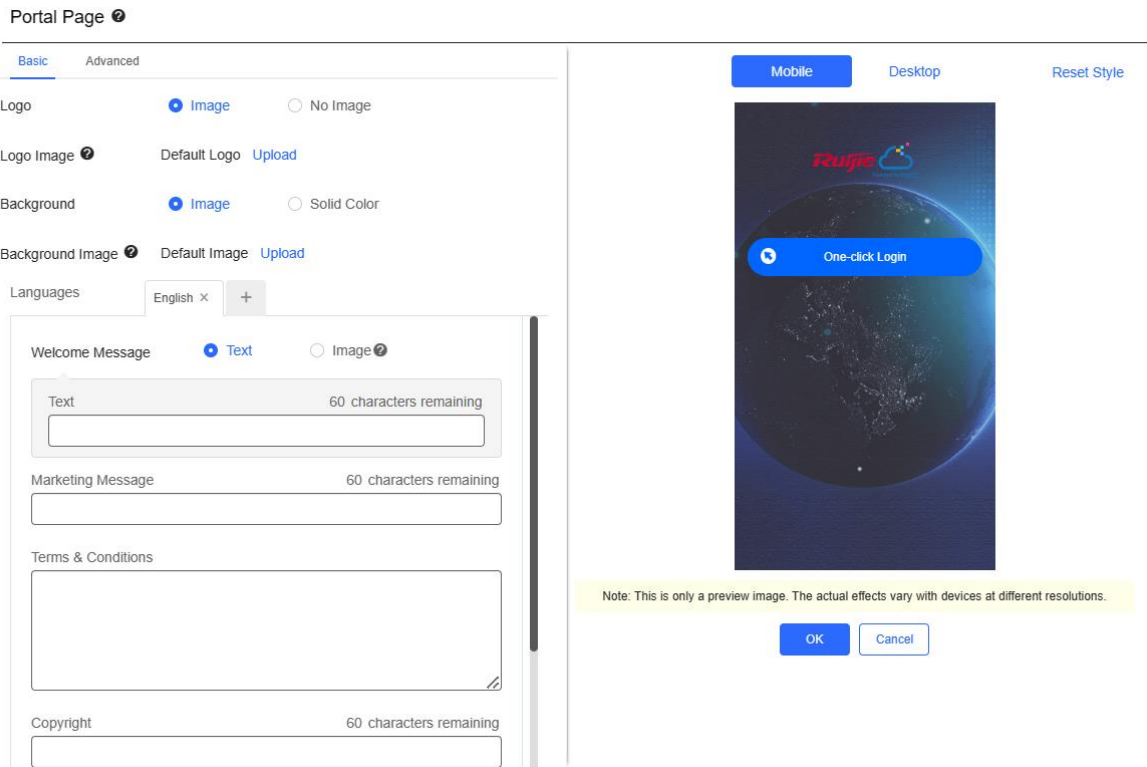



Table 3-8 Basic Information of the Portal Page

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. <ul style="list-style-type: none"> ● Welcome Message: Select the welcome message with the image or text. ● Marketing message: Enter the marketing message.

Parameter	Description
	<ul style="list-style-type: none"> ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● One-click Login: After One-click Login is enabled, you can customize the button name displayed on the portal page, which is set to One-click Login by default. <p>One-click Login <input type="checkbox"/> Reset</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Switching Button 45 characters remaining</p> <p style="text-align: center; border: 1px solid #ccc; padding: 2px;">One-click Login</p> </div>

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

Portal Page ⊕

Basic Advanced

Logo Position Upper ▾

Background Mask Color #a2a2a2

Background Mask Opacity 30

Welcome Message Text Color #ffffff

Welcome Message Text Size 24 ▾

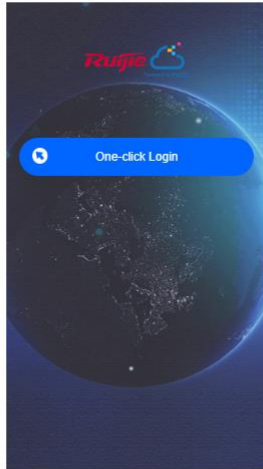
Button Color #0066ff

Button Text Color #ffffff

Link Color #ffffff

Text Color in Box #ffffff

Mobile Desktop Reset Style



Note: This is only a preview image. The actual effects vary with devices at different resolutions.

OK Cancel

Table 3-9 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	Select the welcome message text color. The default value is #ffffff.


Parameter	Description
Color	
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.

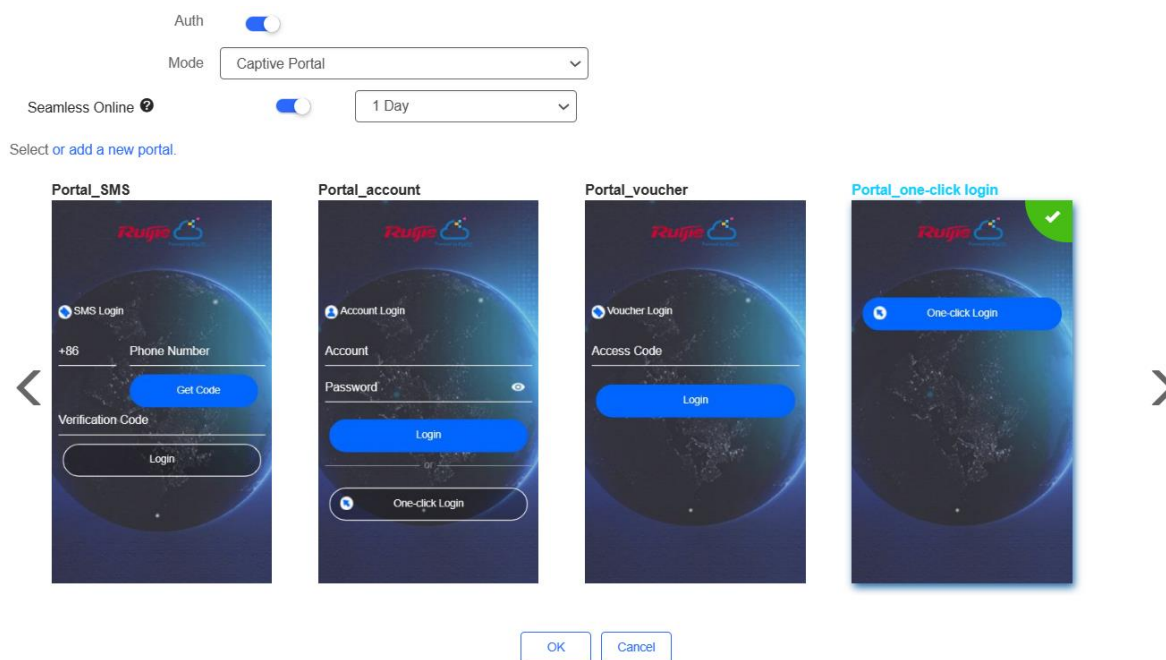
SSID 

WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	WIFI_60	Open	No	Bridge	1	Auth Disabled	 

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

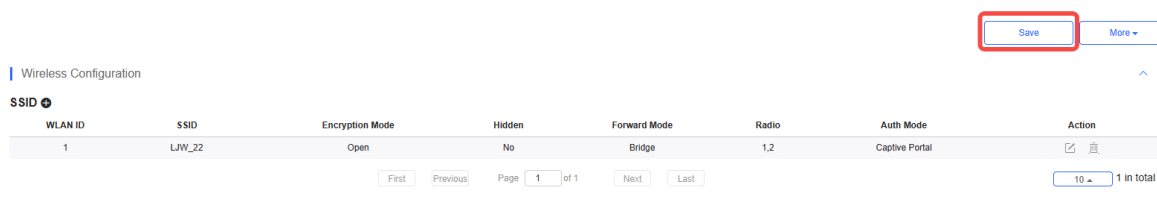
Note

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.

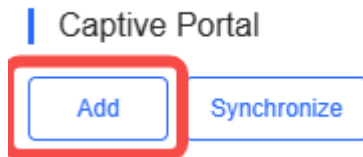
(4) Click **Save** for the configuration to take effect.



3.21.3 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.

Name

Description

Login Options One-click Login Voucher Account SMS Registration Facebook Account

Show Balance Page

Post-login URL

Table 3-10 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.

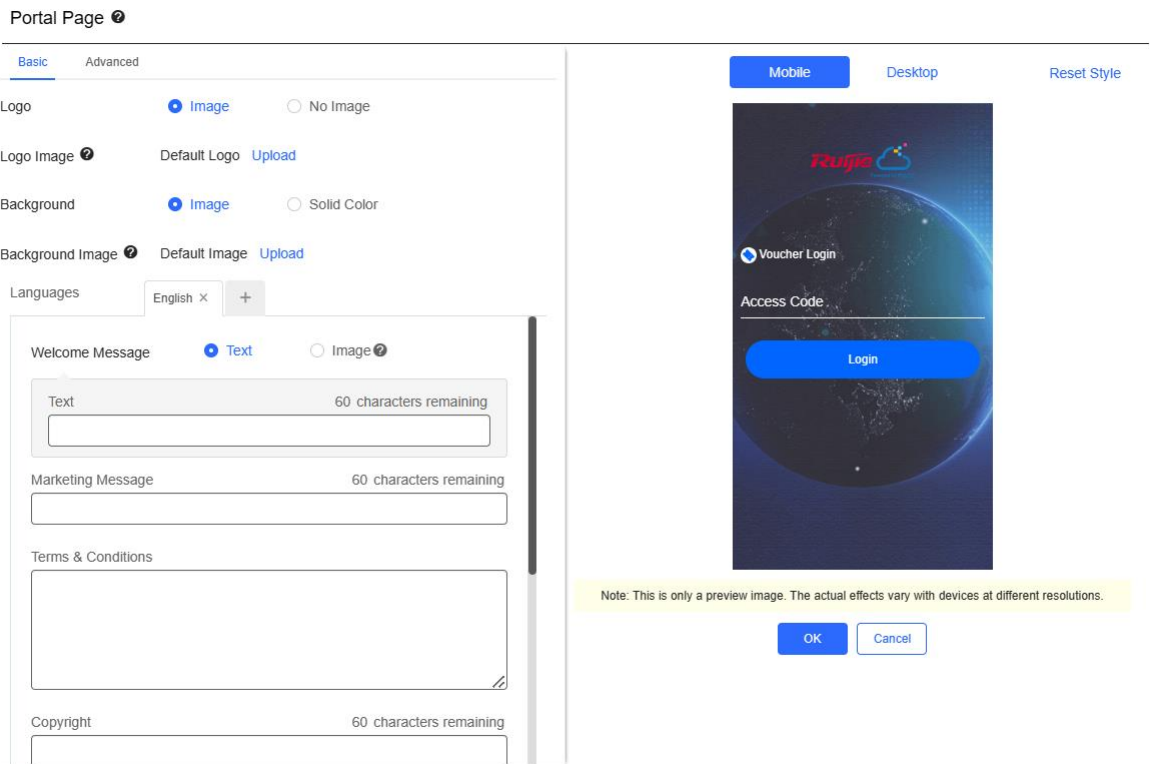



Table 3-11 Basic Information of the Portal Page

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. <ul style="list-style-type: none"> ● Welcome Message: Select the welcome message with the image or text. ● Marketing message: Enter the marketing message.

Parameter	Description
	<ul style="list-style-type: none"> ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● Voucher Login: After Voucher Login is enabled, you can customize the names of controls related to voucher authentication. <p>Voucher Login <input type="checkbox"/> Reset</p> <p>Title <input type="text" value="Show"/> 60 characters remaining <input type="text" value="Voucher Login"/></p> <p>Voucher Code Placeholder 60 characters remaining <input type="text" value="Access Code"/></p> <p>Login Button 60 characters remaining <input type="text" value="Login"/></p> <p>Switching Button 60 characters remaining <input type="text" value="Voucher Login"/></p>

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

Portal Page

Basic **Advanced**

Logo Position

Background Mask Color

Background Mask Opacity

Welcome Message Text Color

Welcome Message Text Size

Button Color

Button Text Color

Link Color

Text Color in Box

Mobile Desktop [Reset Style](#)

Note: This is only a preview image. The actual effects vary with devices at different resolutions.

Table 3-12 Advanced Information of the Portal Page



Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).


Parameter	Description
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.

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.

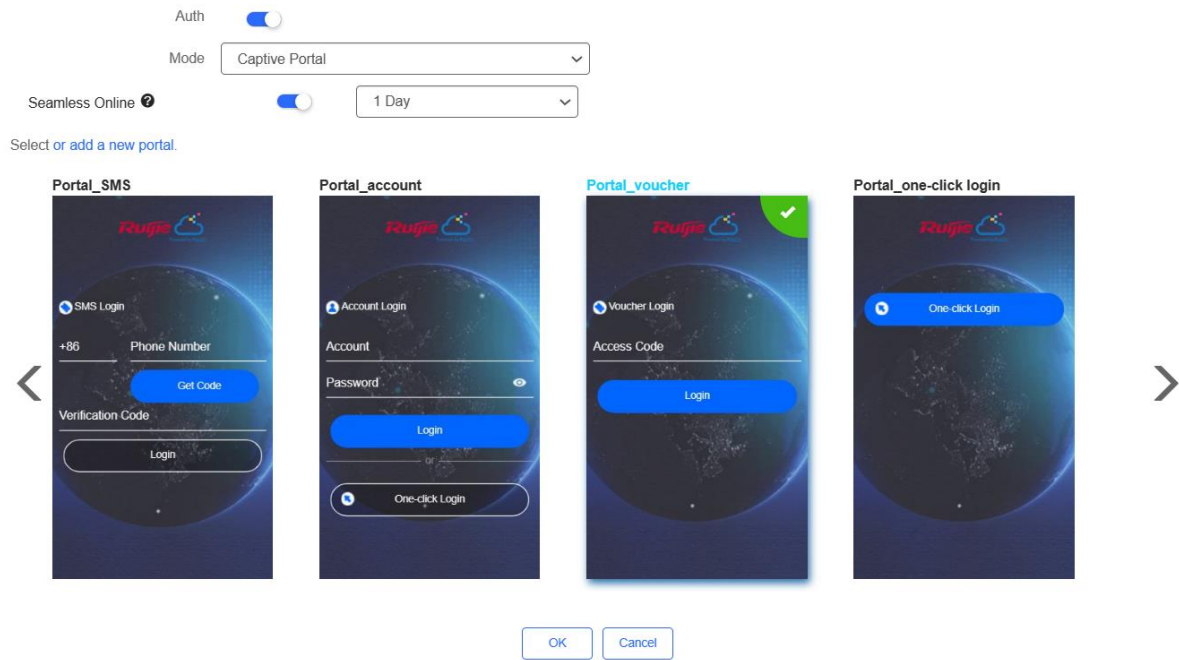
SSID 

WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	WIFI_60	Open	No	Bridge	1	Auth Disabled	 

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

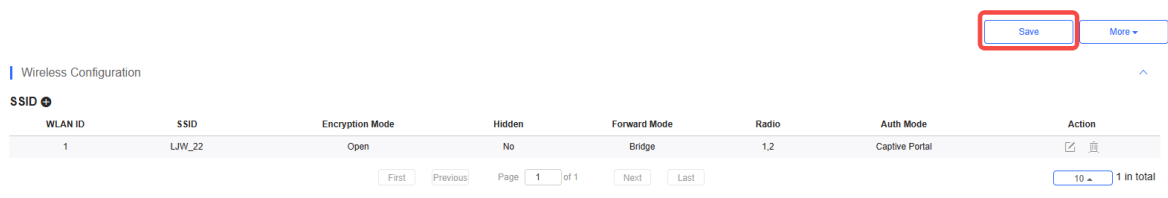
Note

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.



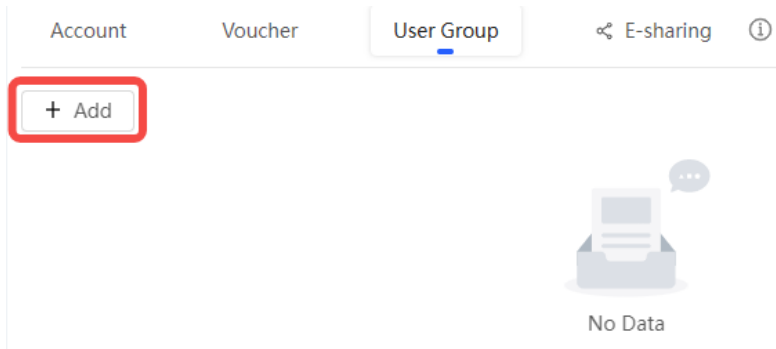
- **Mode:** Set it to **Captive Portal**.
- **Seamless Online:** Determine whether to enable **Seamless Online** as required, which is enabled by default. After **Seamless Online** is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- **Select 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**.

Add user group X

* User group name

User Group Policy

Price

Concurrent devices

Period

Quota ⓘ

Maximum upload rate

Maximum download rate

Bind MAC on first use

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.

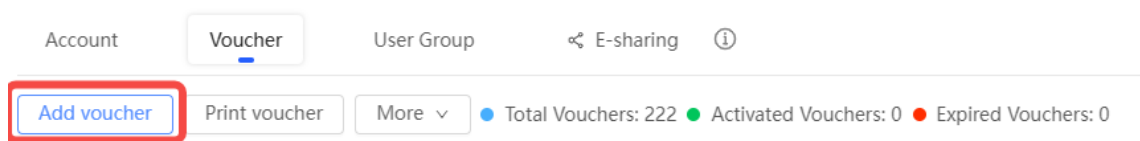
Maximum upload rate: indicates the maximum upload rate.

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:

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

Advance Setting ^

Voucher code type: Alphanumeric 0-9, a-z

Voucher length: Alphanumeric 0-9, a-z

Alphabetic a-z

Numeric 0-9

Cancel OK

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

Voucher length: 6

6

7

8

9

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

Account Voucher User Group E-sharing

Add voucher Print voucher More Total Vouchers: 4 Activated Vouchers: 0 Expired Vouchers: 0

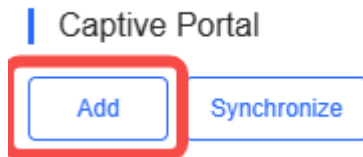
<input type="checkbox"/>	Voucher code	User Group	Period	Created at	Activated at	Expired at	Operation
<input type="checkbox"/>	fqyhwyg	1	Unlimited	2022-08-12 18:34:31	-	-	✎ ⌂ 🗑
<input type="checkbox"/>	dxwgkxh	1	Unlimited	2022-08-12 18:34:31	-	-	✎ ⌂ 🗑
<input type="checkbox"/>	t5nq76	1	Unlimited	2022-08-12 11:09:07	-	-	✎ ⌂ 🗑
<input type="checkbox"/>	jsz75g	1	Unlimited	2022-08-12 11:09:07	-	-	✎ ⌂ 🗑

4 in total < 1 > 20 / page

3.21.4 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.

Name *

Description

Login Options One-click Login Voucher Account SMS Registration beta Facebook Account

Show Balance Page

Post-login URL

Table 3-13 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.

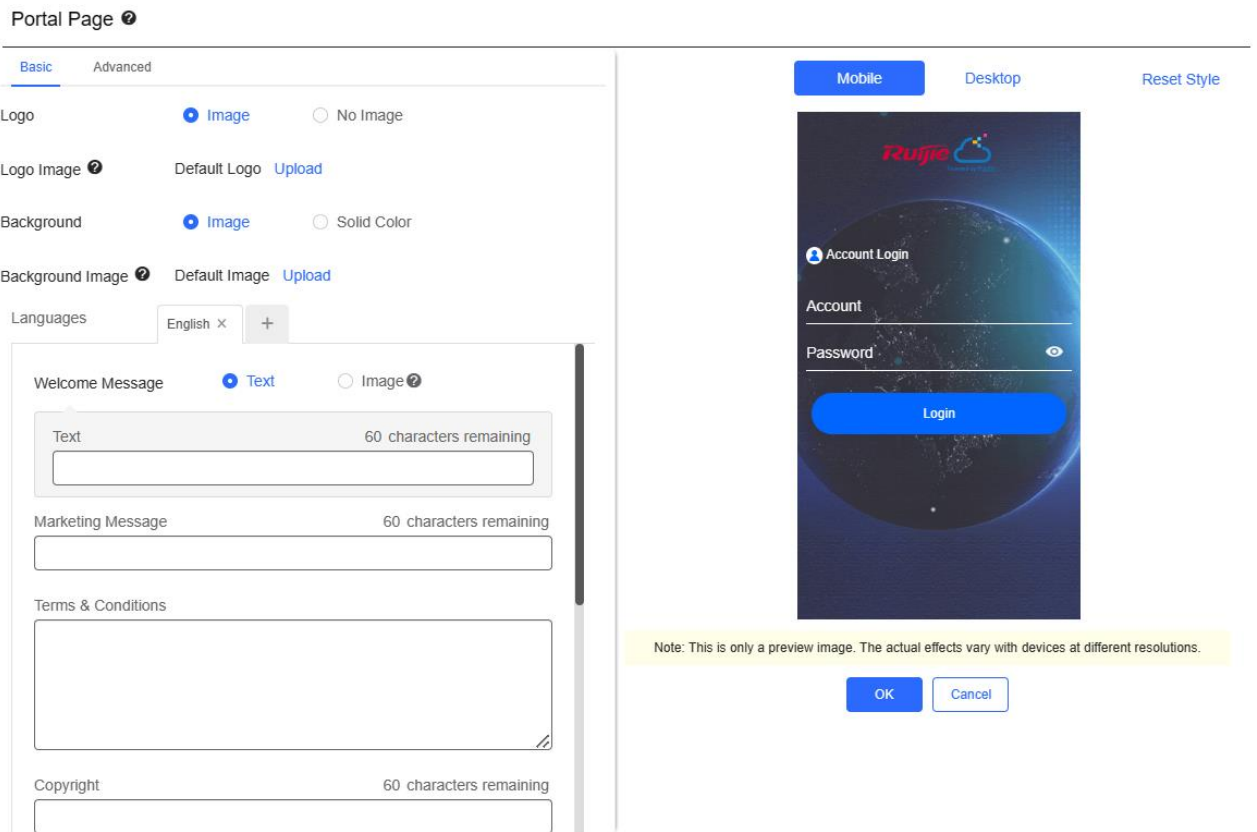



Table 3-14 Basic Information of the Portal Page

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. <ul style="list-style-type: none"> ● Welcome Message: Select the welcome message with the image or text.

Parameter	Description
	<ul style="list-style-type: none"> ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● Account Login: After Account Login is enabled, you can customize the names of the controls related to account authentication. <p>Account Login <input type="checkbox"/> Reset</p> <p>Title <input type="text" value="Show"/> 60 characters remaining <input type="text" value="Account Login"/></p> <p>Account Placeholder 60 characters remaining <input type="text" value="Account"/></p> <p>Password Placeholder 60 characters remaining <input type="text" value="Password"/></p> <p>Login Button 60 characters remaining <input type="text" value="Login"/></p> <p>Switching Button 60 characters remaining <input type="text" value="Account Login"/></p>

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

Portal Page

Basic **Advanced**

Logo Position

Background Mask Color

Background Mask Opacity

Welcome Message Text Color

Welcome Message Text Size

Button Color

Button Text Color

Link Color

Text Color in Box

Mobile Desktop [Reset Style](#)

Note: This is only a preview image. The actual effects vary with devices at different resolutions.



Table 3-15 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.

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.

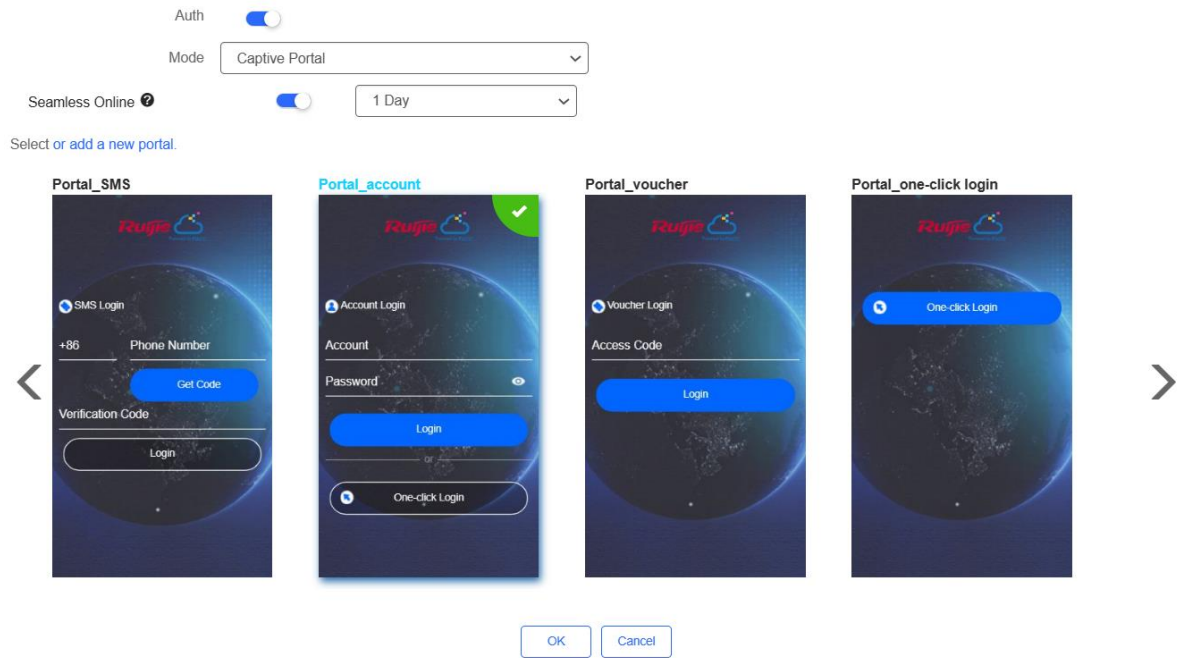
(2) If the SSID that needs to enable wireless authentication is not created, click  to open the SSID configuration page. If the SSID that needs to enable wireless authentication is created, click  in the **Action** column. The following content only describes configurations related to wireless authentication.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

SSID 							
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	WiFi_60	Open	No	Bridge	1	Auth Disabled	 

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

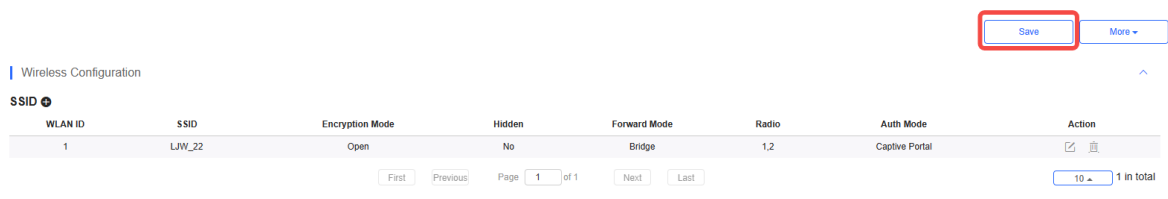
Note

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.

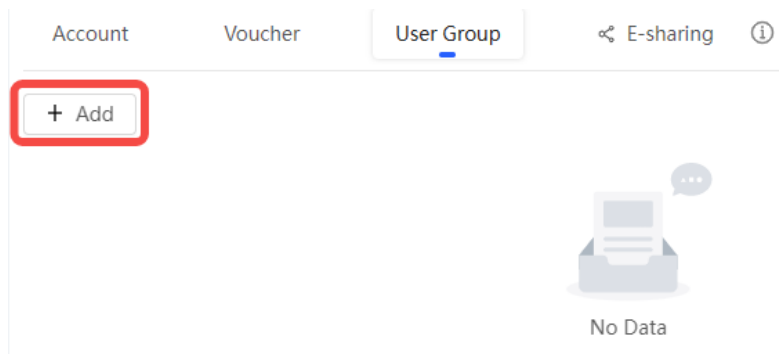
(4) Click **Save** for the configuration to take effect.



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**.

Add user group
✕

* User group name

User Group Policy

Price

Concurrent devices

Period

Quota ⓘ

Maximum upload rate

Maximum download rate

Bind MAC on first use

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**.

Add account
✕

* User name

* Password

* User group

Allow VPN connection

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

User information setting ▼

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**.

Bulk import accounts X

Step1: Download and fill in the device information in the template. Up to 500 records can be imported each time.

Account and Password fields are required. Please enter less than 32 characters, consisting of letters, numbers or underscores.



Please select an .xls or .xlsx file

Download Template

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.

Account
Voucher
User Group
E-sharing

Add account
Bulk import
One-click send
More
Total Accounts: 3
Activated Accounts: 0
Expired Accounts: 0

<input type="checkbox"/>	Account	Password	User group	Status	Period	First name	Alias	Created at	Activated at	Ex	Operation
<input type="checkbox"/>	test3	test3	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		⌵ ⌵ ⌵
<input type="checkbox"/>	test4	test4	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		⌵ ⌵ ⌵
<input type="checkbox"/>	test2	test2	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		⌵ ⌵ ⌵

3 in total
1
>
10 / page

3.21.5 Configuring SMS Authentication on Ruijie Cloud

1. Adding a Twilio Account


Prerequisites

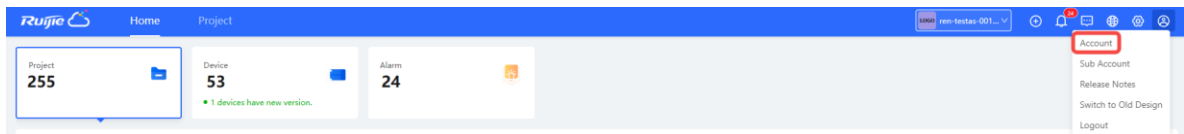
A Twilio account has been applied for from the Twilio official website (<https://www.twilio.com/login>).

Note

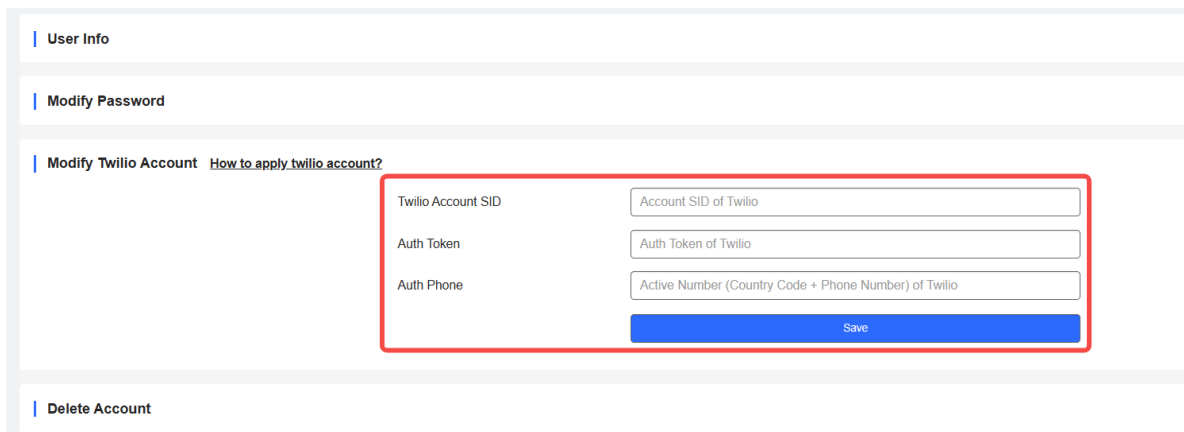
A Twilio account is used to send the SMS verification code.

Configuration Steps

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



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

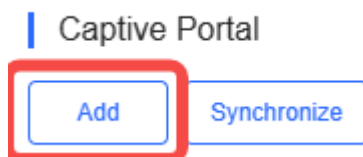


The screenshot shows the 'Modify Twilio Account' section of the Ruijie Cloud interface. It includes a link 'How to apply twilio account?'. The form contains three input fields: 'Twilio Account SID' (with placeholder 'Account SID of Twilio'), 'Auth Token' (with placeholder 'Auth Token of Twilio'), and 'Auth Phone' (with placeholder 'Active Number (Country Code + Phone Number) of Twilio'). A blue 'Save' button is located below the fields. The 'Delete Account' option is visible at the bottom of the section.

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.

Name

Description

Login Options One-click Login Voucher Account SMS Registration beta Facebook Account

Twilio Account SID

Auth Token

Auth Phone

Show Balance Page

Post-login URL

Table 3-16 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.

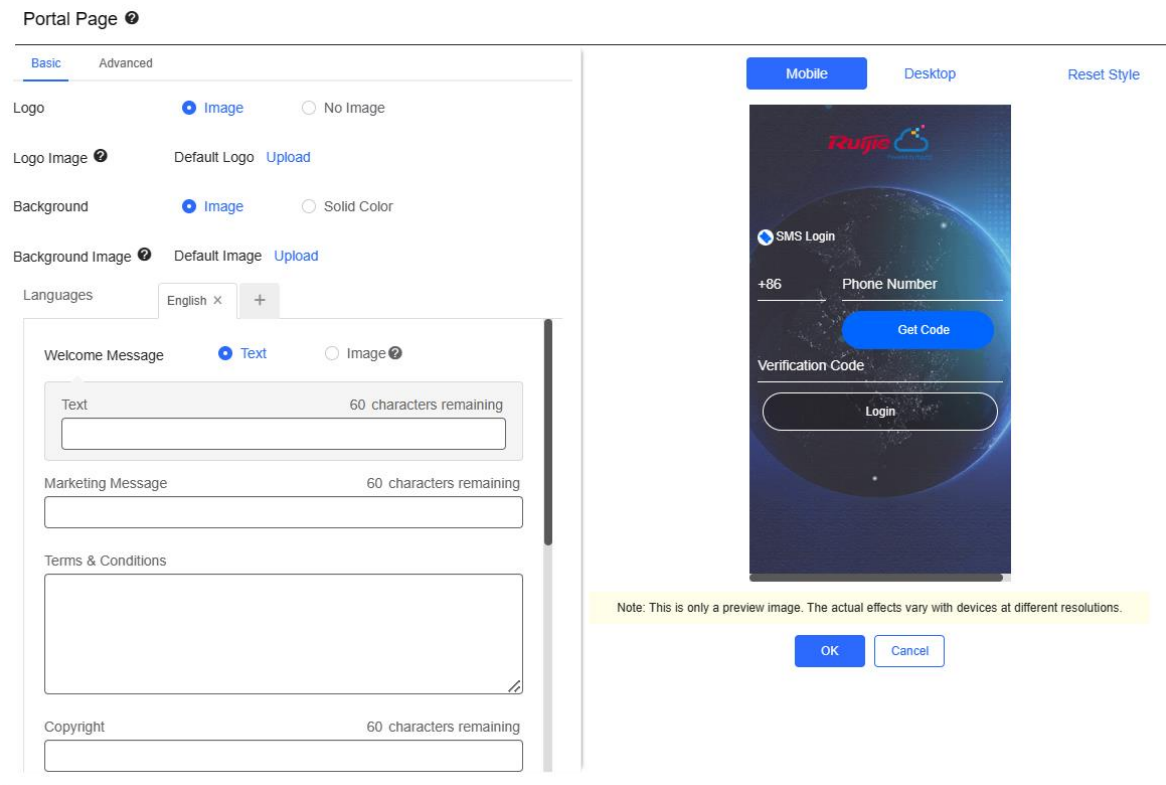



Table 3-17 Basic Information of the Portal Page

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. <ul style="list-style-type: none"> ● Welcome Message: Select the welcome message with the image or text. ● Marketing message: Enter the marketing message.

Parameter	Description
	<ul style="list-style-type: none"> ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● SMS Login: After SMS Login is enabled, you can customize the names of the controls related to SMS authentication. <p>SMS Login <input type="checkbox"/> Reset</p> <p>Title <input type="text" value="SMS Login"/> 60 characters remaining</p> <p>Phone Number Placeholder <input type="text" value="Phone Number"/> 60 characters remaining</p> <p>Verification Code Placeholder <input type="text" value="Verification Code"/> 60 characters remaining</p> <p>Verification Code Button <input type="text" value="Get Code"/> 60 characters remaining</p> <p>Login Button <input type="text" value="Login"/> 60 characters remaining</p> <p>Switching Button <input type="text" value="SMS Login"/> 60 characters remaining</p>

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

Portal Page ⓘ

Basic Advanced

Logo Position

Background Mask Color

Background Mask Opacity

Welcome Message Text Color

Welcome Message Text Size

Button Color

Button Text Color

Link Color

Text Color in Box

Mobile Desktop [Reset Style](#)

Note: This is only a preview image. The actual effects vary with devices at different resolutions.



Table 3-18 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.

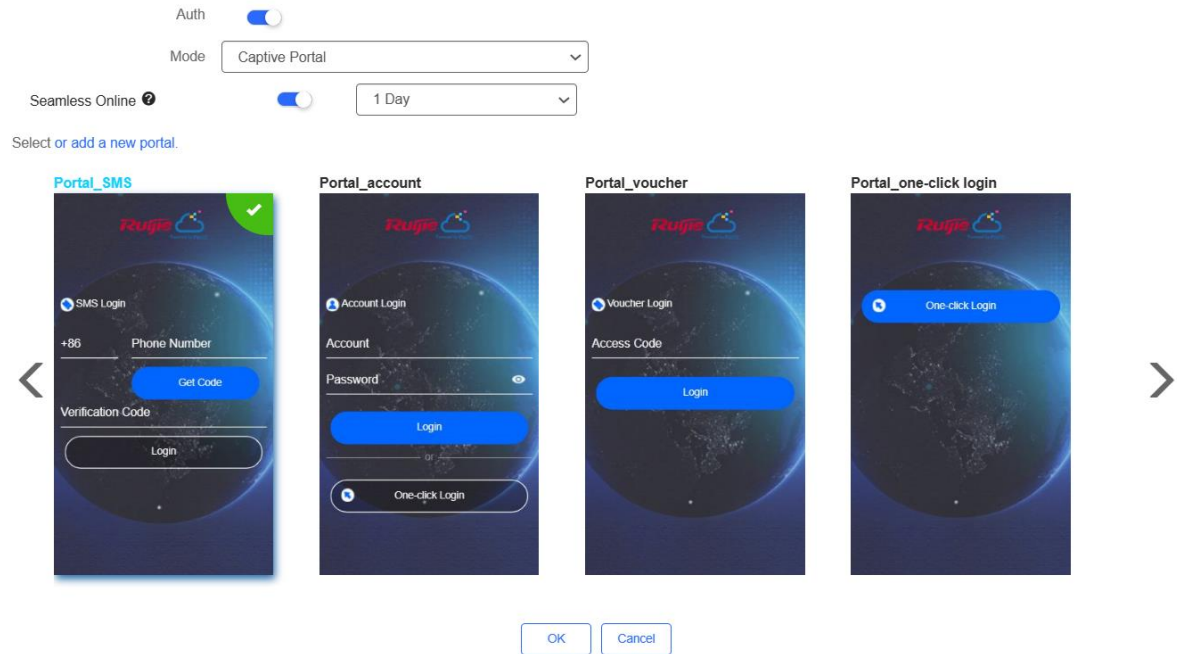
(2) If the SSID that needs to enable wireless authentication is not created, click  to open the SSID configuration page. If the SSID that needs to enable wireless authentication is created, click  in the **Action** column. The following content only describes configurations related to wireless authentication.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

SSID 							
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	WiFi_60	Open	No	Bridge	1	Auth Disabled	 

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

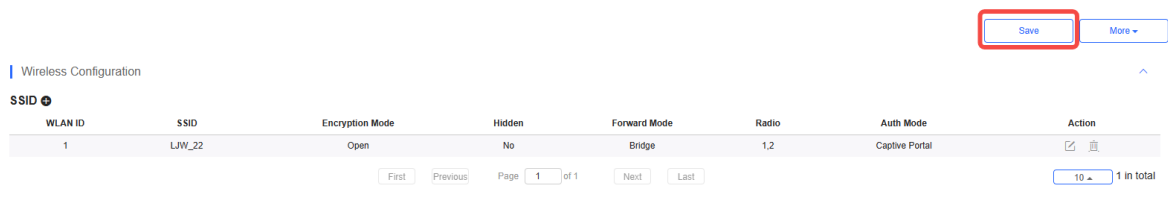
Note

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.



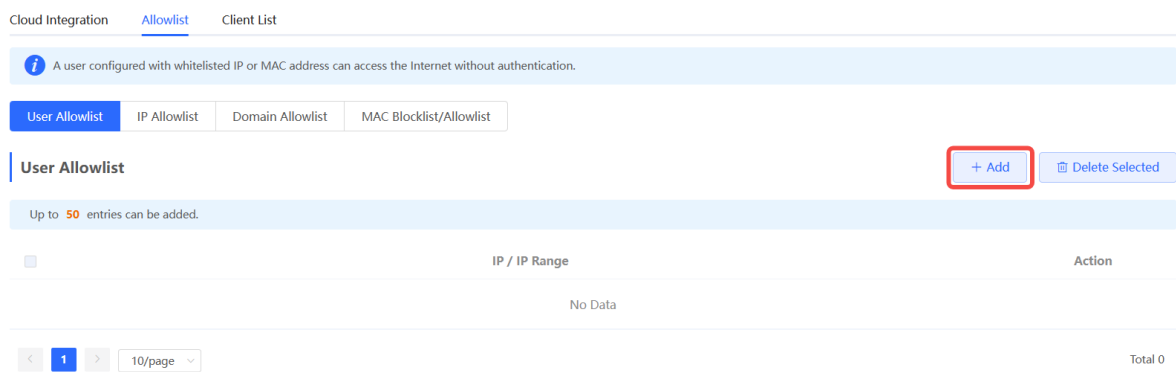
3.21.6 Configuring an Authentication-Free User List on Eweb Management System

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.



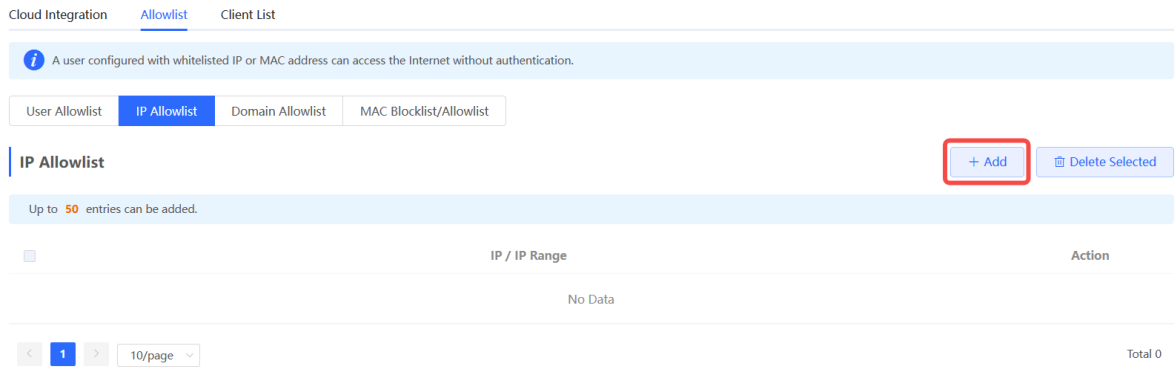
(3) Configure an STA IP address or IP address range. After the configuration, click **OK** to save the configurations.



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.



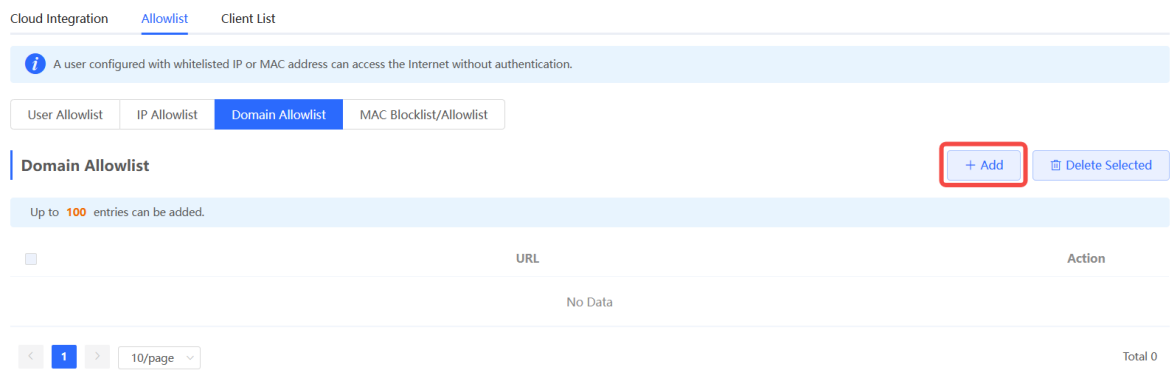
(3) Configure a public IP address or public IP address range. After the configuration, click **OK** to save the configurations.



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**.

Add ×

* URL


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.

Cloud Integration [Allowlist](#) Client List

 A user configured with whitelisted IP or MAC address can access the Internet without authentication.

User Allowlist IP Allowlist Domain Allowlist **MAC Blocklist/Allowlist**

MAC Allowlist

Up to 250 entries can be added.

<input type="checkbox"/>	MAC Address	Action
No Data		

< 1 > 10/page Total 0

MAC Blocklist

Up to 250 entries can be added.

<input type="checkbox"/>	MAC Address	Action
No Data		

< 1 > 10/page Total 0

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

Add ×

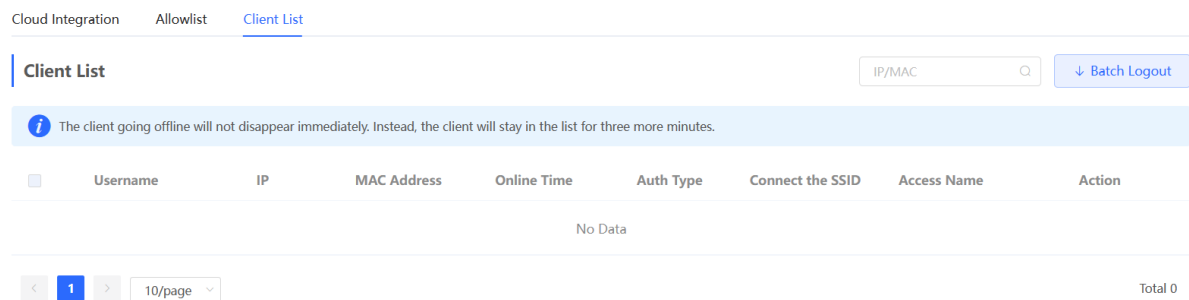
* MAC Address

3.21.7 Displaying Authenticated Users on Eweb Management System

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

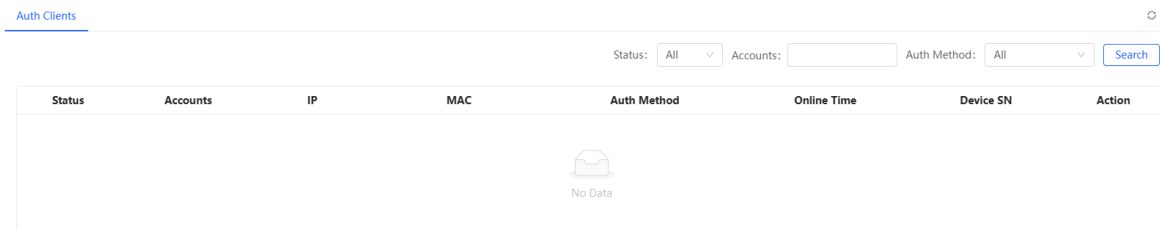
Note

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



3.21.8 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.



3.22 Configuring 802.1X Authentication

Caution

The functions mentioned in this chapter are supported by only RG-RAP2260(G), 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.

3.22.1 Overview

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

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

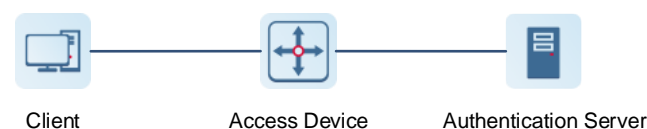
The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

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

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

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

Figure 3-1 Typical Architecture of 802.1X Network




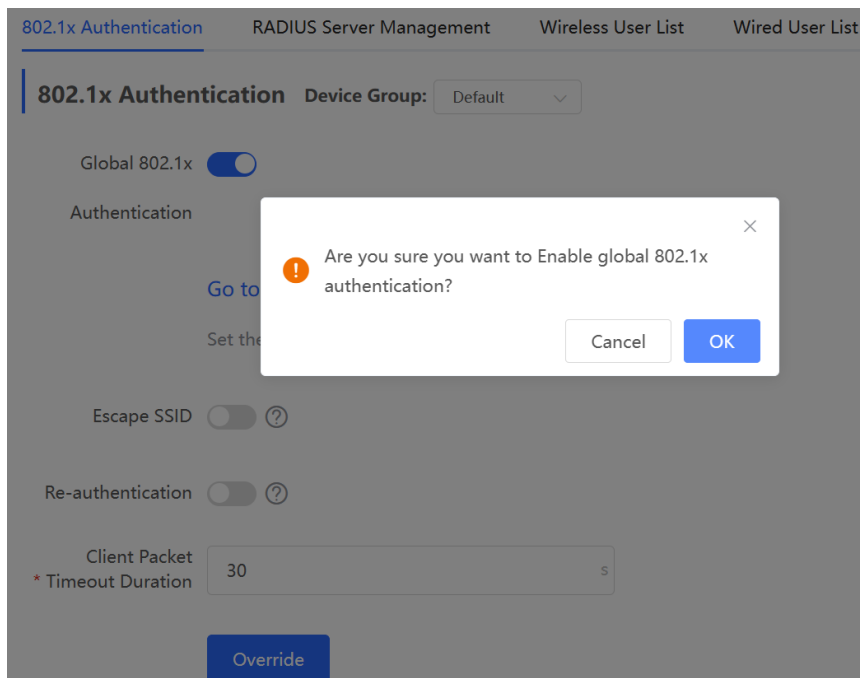
- The client is usually an endpoint device which can initiate 802.1X authentication through the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL) on the local area network.
- The access device is usually a network device (AP or switching device) that supports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

Note


The RG-RAP APs only support the authentication.

3.22.2 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.

Escape SSID 

* Escape SSID

* Security

* Wi-Fi Password 

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

⚠ Caution

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

Re-authentication 

* Re-auth Interval

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.

802.1x Authentication Device Group:

Global 802.1x

Authentication

[Go to Wi-Fi](#)

Set the security mode of the SSID to 802.1X (Enterprise).

Escape SSID 

Re-authentication 

Client Packet
* Timeout Duration s

Override

(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**.

802.1x Authentication [RADIUS Server Management](#) Wireless User List Wired User List

RADIUS Server Management Add Server group

Up to 20 entries can be added.

Server group name	Server IP	Auth Port	Accounting Port	Shared Password	Action
group1	1.1.1.2	1812	1813	rujije	Edit Delete
	1.1.1.1	1812	1813	rujije	
group2	1.1.1.3	1812	1813	rujije	Edit Delete

You can click [+ Add Server](#) to add multiple servers to a server group, and click [Server](#) to delete a selected server.

Add ×

* Server group name

[Server 1](#)

* Server IP

* Server name

* Auth Port

* Accounting Port ?

* Shared Password

* Match Order ?

[+ Add Server](#)

Table 3-19 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**.

RADIUS Server Management
Add Server

Up to 5 entries can be added.

Server IP	Auth Port	Accounting Port	Shared Password	Match Order	Action
No Data					

Server global configuration

- * Packet Retransmission Interval s
- * Packet Retransmission Count time
- Server Detection
- * Detection Interval min
- * Detection Count time ⓘ
- * Detection Username
- MAC Address Format ⓘ

Save

Table 3-20 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

Parameter	Description
	is unreachable.
Packet Retransmission Count	Configure the number of times that the device sends requests to a RADIUS server before confirming that the RADIUS server is unreachable.
Server Detection	If this function is enabled, it is necessary to set the server detection cycle, server detection times, and server detection username. Determines the server status and whether to enable functions such as the escape function.
MAC Address Format	Configure the format of the MAC address used in attribute 31 (Calling-Station-ID) of a RADIUS message. The following formats are supported: <ul style="list-style-type: none"> ● Dotted hexadecimal format. For example, 00d0.f8aa.bbcc. ● IETF format. For example: 00-D0-F8-AA-BB-CC. ● Unformatted (default). For example: 00d0f8aabbcc


3.22.3 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.**

802.1x Authentication RADIUS Server Management Wireless User List Wired User List

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

Wireless User List [Refresh](#) [Batch Logout](#)

<input type="checkbox"/>	Name	IP	MAC Address	Online Time	Online Duration	Connect SSID	Access Name	Action
No Data								

< **1** > 10/page Total 0

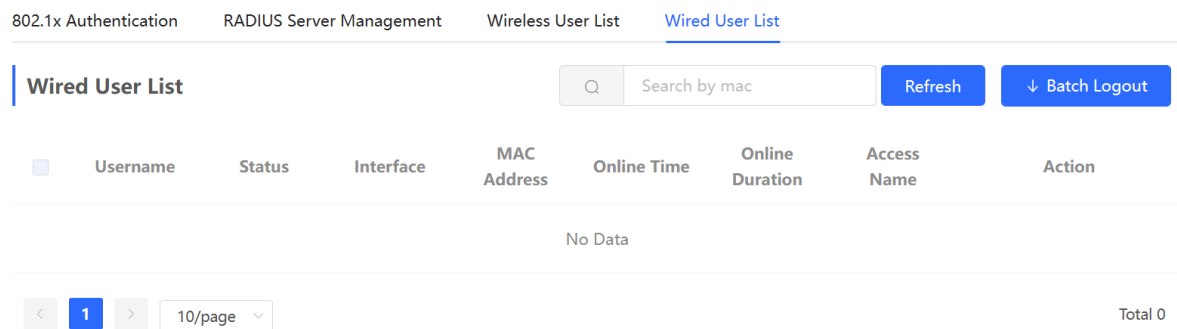
Click **Refresh** to view the latest user list.

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

3.22.4 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**.



The screenshot shows the 'Wired User List' page in a web-based configuration interface. At the top, there are navigation tabs: '802.1x Authentication', 'RADIUS Server Management', 'Wireless User List', and 'Wired User List' (which is selected). Below the tabs, the page title is 'Wired User List'. There is a search bar with a magnifying glass icon and the text 'Search by mac'. To the right of the search bar are two buttons: 'Refresh' and 'Batch Logout'. Below the search bar is a table with the following columns: 'Username', 'Status', 'Interface', 'MAC Address', 'Online Time', 'Online Duration', 'Access Name', and 'Action'. The table is currently empty, displaying 'No Data'. At the bottom of the page, there is a pagination control showing '1' in a blue box, indicating the current page, and '10/page' in a dropdown menu. On the far right, it says 'Total 0'.


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

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

4 Network Settings

Note

This chapter takes the currently logged in device as an example to describe the entry of each function setting page. If you need to configure other devices in the network, please refer to the following path to enter the configuration page of the corresponding device, and then configure the function:

- For RG-RAP2260(G), 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: Click **Manage Network Device**.
 - For the other RAP models: Choose  **WLAN > APs** > Select the target device in the device list and click **Manage**.
-

4.1 Switching Work Mode

4.1.1 Work Mode

See [Work Mode](#) for details.

4.1.2 Self-Organizing Network Discovery

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

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


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

4.1.3 Configuration Steps

Note

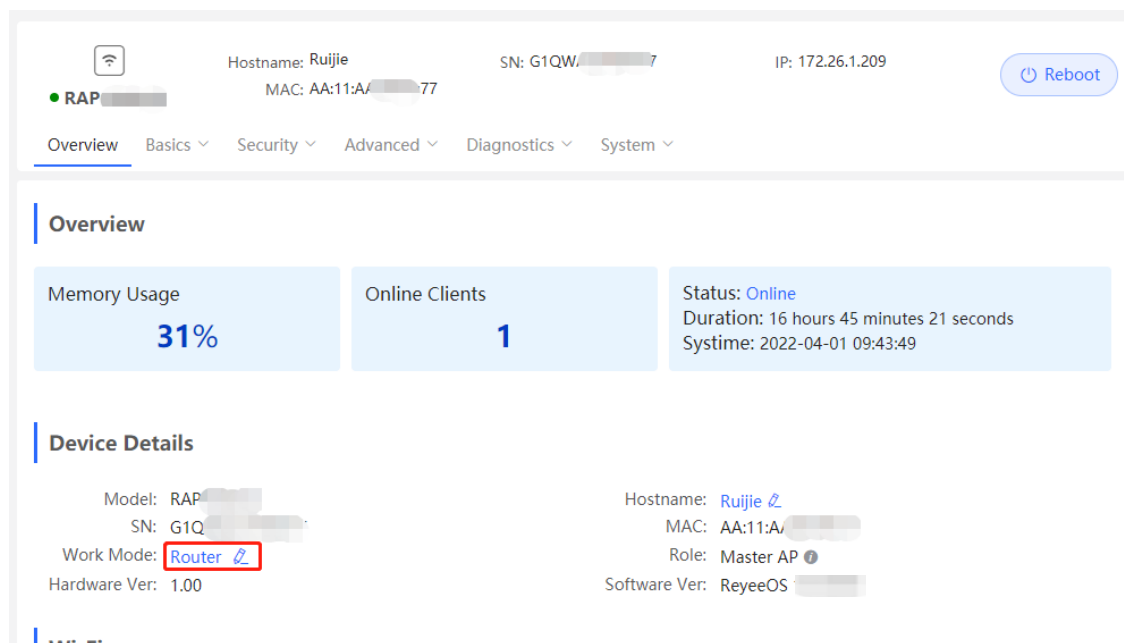
If you need to switch the work mode to wireless bridging mode, please see [Wireless Repeater Mode](#) for details.

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Overview > Device Details**

For other RAP models: Choose ( **WLAN > APs > Manage**)  **Overview > Device Details**

Click the current work mode to change the work mode.



The screenshot shows the Ruijie web management interface for a device. At the top, there is a header with a Wi-Fi icon, Hostname: Ruijie, SN: G1QW/..., IP: 172.26.1.209, and a Reboot button. Below the header is a navigation menu with tabs: Overview, Basics, Security, Advanced, Diagnostics, and System. The main content area is divided into two sections: Overview and Device Details. The Overview section shows Memory Usage at 31%, Online Clients at 1, and Status: Online with a duration of 16 hours 45 minutes 21 seconds and a system time of 2022-04-01 09:43:49. The Device Details section shows Model: RAP..., SN: G1Q..., Work Mode: Router (highlighted with a red box), Hardware Ver: 1.00, Hostname: Ruijie, MAC: AA:11:A..., Role: Master AP, and Software Ver: ReyeOS.

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

Description:

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

Work Mode ?

Self-Organizing ?

Network


AC ?

⚠ Caution

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

4.1.4 Viewing Device Role

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Overview > Device Details**

For other RAP models: Choose ( **WLAN > APs > Manage**)  **Overview > Device Details**

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

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

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

Device Details

Model: RAP2261(E)
MAC Address: 58:69:6C:22:08:30
Hardware Ver: 1.00

Hostname: Ruijie [↗](#)
Work Mode: Router [↗](#)
Software Ver: ReyeOS 1 [↗](#)

SN: MACCR10825107
Role: Master AP [?](#)

4.2 Configuring Internet Connection Type (IPv4)

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > WAN > WAN**

For other RAP models: Choose ( **WLAN > APs > Manage >**)  **Network > WAN > WAN**

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

WAN

* Internet

No username or password is required for DHCP clients.

IP Address 192.168.111.210

Subnet Mask 255.255.255.0

Gateway 192.168.111.1

DNS Server 192.168.111.1

[Advanced Settings](#)

Save

The device supports the following Internet connection types:

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

4.3 Configuring Internet Connection Type (IPv6)

Caution

This function is supported by only RG-RAP2260(G), 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 in the AP mode.

In **Local Device** mode, choose  **Network > WAN > WAN_V6 Settings**.

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

WAN [WAN_V6 Settings](#)

* Internet

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

The device supports the following Internet connection types:


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

4.4 Configuring LAN Port

Caution

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

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > LAN > LAN Settings**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **Network > LAN > LAN Settings**

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

LAN Settings DHCP Clients Static IP Addresses

LAN Settings + Add Delete Selected

Up to 8 entries can be added.

<input type="checkbox"/>	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
<input type="checkbox"/>	192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	Edit Delete

×

Edit

* IP

* Subnet Mask

Remark

* MAC

DHCP Server


4.5 Configuring Repeater Mode

 **Caution**

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

4.5.1 Wired Repeater

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > Repeater Mode**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **Network > Repeater Mode**

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


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

Caution

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

The device is working in **Router** mode.

Access Point Wireless Repeater

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

Wired Repeater

Check


4.5.2 Wireless Repeater

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

Note

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

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > Repeater Mode**

For other RAP models: Choose ( **WLAN > APs > Manage >**)  **Network > Repeater Mode**

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

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

Router Access Point **Wireless Repeater**

 • This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.

• The local device will work as a secondary device.

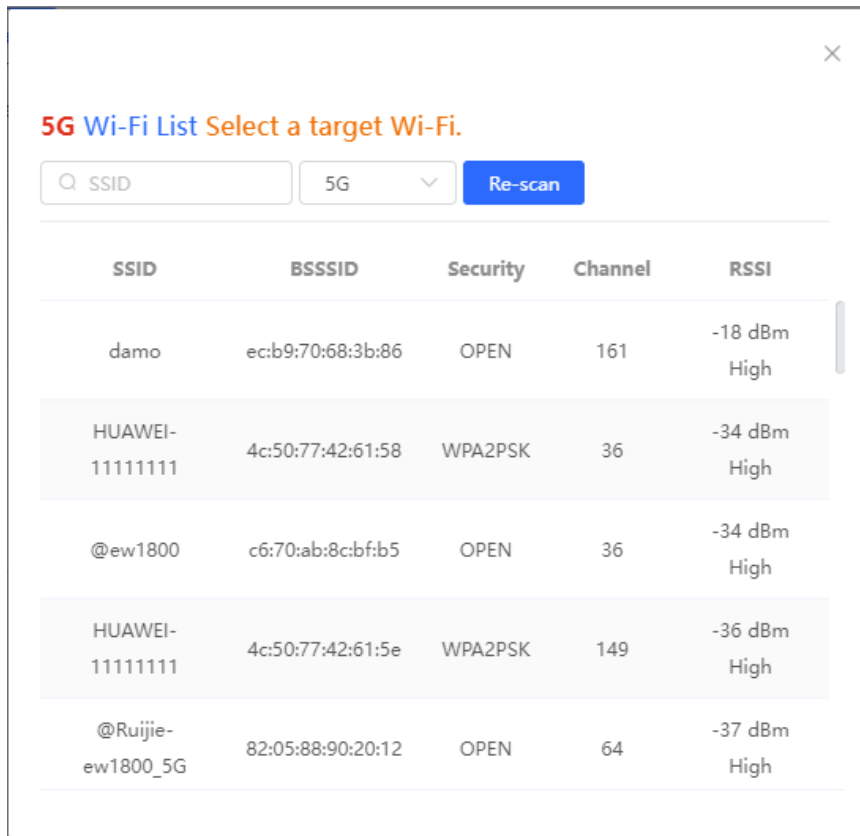
• It is recommended to select a 5G Wi-Fi of the primary device.

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

Wireless Repeater

Primary Device _____

* SSID



- (2) Select the Wi-Fi signal of the upper-layer device that you want to extend. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.
- (3) Configure Local Router Wi-Fi. You can select New Wi-Fi or Same as Primary Router Wi-Fi.
 - If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the router are automatically synchronized with those on the primary router. Generally, clients merge Wi-Fi signals with the same name into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.
 - If **New Wi-Fi** is selected, you can set a local Wi-Fi name and password. Clients will search out different Wi-Fi signals.

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

Router
 Access Point
 Wireless Repeater

i

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

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

Wireless Repeater

Primary Device _____

* SSID @ew1800

Local Device _____

Local Router Wi-Fi **New Wi-Fi** Same as Primary Router Wi-Fi

* SSID(2.4G)

* SSID(5G)

Wi-Fi Password

⚠ Caution


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

4.6 Creating a VLAN

⚠ Caution

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

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > LAN > LAN Settings**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **Network > LAN > LAN Settings**

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

LAN Settings DHCP Clients Static IP Addresses

LAN Settings + Add Delete Selected

Up to 8 entries can be added.

<input type="checkbox"/>	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
<input type="checkbox"/>	192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	Edit Delete

Add ×

* IP

* Subnet Mask

* VLAN ID

Remark

* MAC

DHCP Server

Table 4-1 VLAN Configuration

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

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

 **Caution**

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

4.7 Configuring Port VLAN

 **Caution**

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

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > LAN**

For other RAP models: Choose ( **WLAN > APs > Manage >**)  **Network > LAN**

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

LAN Settings Port VLAN

i LAN Settings

Port VLAN

LAN Settings
+ Add
Delete Selected

Up to 4 entries can be added.

	VLAN ID	Remark	Action
<input type="checkbox"/>	99	test	Edit Delete

(1) 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.

Add
×

* VLAN ID

Remark

Cancel
OK

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

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

LAN Settings

Port VLAN

i **Port VLAN**
 Please choose [LAN Settings](#) to create a VLAN first and configure port settings based on the VLAN. ?

Port VLAN

Connected


Disconnected

Port 1

VLAN 1(WAN)	<div style="border: 1px solid #ccc; padding: 2px 5px; background-color: #fff9c4; display: inline-block;">UNTAG ▾</div>
VLAN 99	<div style="border: 1px solid #ccc; padding: 2px 5px; display: inline-block;">Not Joli ▾</div>

4.8 Changing MAC Address

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > WAN > WAN**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **Network > WAN > WAN**

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

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

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

Caution

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

----- Advanced Settings -----


VLAN ID

* MTU

* MAC

4.9 Changing MTU

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > WAN > WAN**

For other RAP models: Choose ( **WLAN > APs > Manage >**)  **Network > WAN > WAN**

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

----- Advanced Settings -----

VLAN ID

* MTU

* MAC

4.10 Configuring DHCP Server

Caution


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



4.10.1 DHCP Server

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

4.10.2 Configuring the DHCP Server Function

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > LAN > LAN Settings**

For other RAP models: Choose ( **WLAN > APs > Manage >**)  **Network > LAN > LAN Settings**

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

Caution

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

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

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

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

Edit
×

* IP

* Subnet Mask

Remark

* MAC


DHCP Server

* Start

* IP Count

* Lease Time(Min)

4.10.3 Displaying Online DHCP Clients

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > LAN > DHCP Clients**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **Network > LAN > DHCP Clients**

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

LAN Settings **DHCP Clients** Static IP Addresses

i View DHCP clients. ?


DHCP Clients Search by Hostname/IP/MAC

Up to **300** IP-MAC bindings can be added.

<input type="checkbox"/>	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
<input type="checkbox"/>	1	nova-f5a...G-97	192.168.120.172	42:11:26:...	23	Convert to Static IP
<input type="checkbox"/>	2	no-7d2c...G-12	192.168.120.35	72:26:e8:...	13	Convert to Static IP
<input type="checkbox"/>	3	R1...	192.168.120.236	00:e0:4:...	19	Convert to Static IP

4.10.4 Displaying the DHCP Static IP Address List

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Network > LAN > Static IP Addresses**

For other RAP models: Choose ( **WLAN > APs > Manage >**)  **Network > LAN > Static IP Addresses**

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

LAN Settings DHCP Clients **Static IP Addresses**

i Static IP Address List ?

Static IP Address List Search by IP/MAC

Up to **300** entries can be added.

<input type="checkbox"/>	No.	IP	MAC	Action
<input type="checkbox"/>	1	192.168.120.64	12:33:e3:b9:d9:36	Edit Delete

4.11 Link Aggregation

Caution

The function is supported by only RG-RAP2260(H).

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

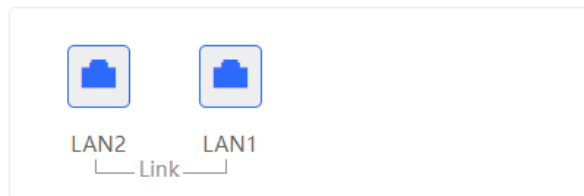
Link Aggregation can improve the throughput in the network and deal with link congestion.



Link Aggregation

Please enable 802.3ad link aggregation on the client and connect it to port LAN2,LAN1.


Link Aggregation



Save


4.12 Configuring DNS

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Advanced** > **Local DNS**

For other RAP models: Choose ( **WLAN** > **APs** > **Manage** >)  **Advanced** > **Local DNS**

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

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

Local DNS server

Save


4.13 Hardware Acceleration

Caution

This function is supported by only RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260, and RG-RAP6262.

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

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


 **Hardware Acceleration**
After Hardware Acceleration is enabled, the Internet access speed will be improved and clients will not be rate-limited.

Enable

Save

4.14 Configuring Port Flow Control

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Advanced** > **Port Settings**

For other RAP models: Choose ( **WLAN** > **APs** > **Manage** >)  **Advanced** > **Port Settings**

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

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

Flow Control

[Save](#)

4.15 Configuring ARP Binding

⚠ Caution

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

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

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose **Security > ARP List**

For other RAP models: Choose (**WLAN > APs > Manage >**) **Security > ARP List**

ARP mappings can be bound in two ways:

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

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

ARP List

Up to **256** IP-MAC bindings can be added.

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

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

Add ×

* IP

* MAC

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

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

4.16 Configuring LAN Ports

Caution

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

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

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

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

LAN Port Settings

The configuration takes effect only for the AP with a LAN port, e.g., EAP101.
Note: The configured LAN port settings prevail. The AP device with no LAN port settings will be enabled with default settings.

Default Settings

VLAN ID [Add VLAN](#)

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

Applied to AP device with no LAN port settings

[Save](#)

LAN Port Settings [+ Add](#) [Delete Selected](#)

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

	VLAN ID ↕	Applied to	Action
<input type="checkbox"/>	5	Ruijie	Edit Delete

4.17 IPv6 Settings

Caution

This function is supported only by RG-RAP2260(G), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1260, RG-RAP1261 and RG-RAP6262 in the router mode.

4.17.1 Overview

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

4.17.2 IPv6 Basic

1. IPv6 Address Format

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

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

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

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

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

2. IPv6 Prefix

An IPv6 address consists of two parts:

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

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

3. Special IPv6 Address

There are also some special IPv6 addresses, for example:

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

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

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

4. NAT66

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

4.17.3 IPv6 Address Assignment Methods

- Manual configuration: The IPv6 address/prefix and other network configuration parameters are manually configured.
- Stateless Address Autoconfiguration (SLAAC): The link local address is generated based on the interface ID, and then the local address is automatically configured based on the prefix information contained in the route advertisement packet.
- Stateful address autoconfiguration, that is, DHCPv6: DHCPv6 is divided into the following two types:
 - DHCPv6 autoconfiguration: The DHCPv6 server automatically configures the IPv6 address/prefix and other network configuration parameters.


- o DHCPv6 Prefix Delegation (PD): The lower-layer network device sends a prefix allocation application to the upper-layer network device. The upper-layer network device assigns an appropriate address prefix to the lower-layer device. The lower-layer device automatically subdivides the obtained prefix (generally less than 64 bits in length) into subnet segments with 64-bit prefix length, and then advertises the subdivided address prefixes to the user link directly connected to the IPv6 host through the route to realize automatic address configuration of the host.

4.17.4 Enabling IPv6

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

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


IPv6 Address

 1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

Tips



 Are you sure you want to enable IPv6 address?

Cancel

OK

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

IPv6 Address

1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings
LAN Settings
DHCPv6 Clients
Static DHCPv6

* Internet

IPv6 Address


IPv6 Prefix

Gateway

DNS Server

NAT66

4.17.5 Configuring the IPv6 Address for the WAN Port

In **Local Device** mode, choose  **Network > IPv6 Address > WAN Settings**.
 Configure the IPv6 address for the WAN port, and click **Save**.

IPv6 Address

1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings
LAN Settings
DHCPv6 Clients
Static DHCPv6

* Internet

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

NAT66

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

Parameter	Description
Internet	<p>Specify the method for obtaining an IPv6 address for the WAN port.</p> <ul style="list-style-type: none"> ● DHCP: The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device. ● Static IP: If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server. ● Null: The IPv6 function is disabled on the current WAN port.
IPv6 Address	<p>If Internet is set to DHCP, the automatically obtained IPv6 address is displayed.</p> <p>If Internet is set to Static IP, you need to manually configure this parameter.</p>
IPv6 Prefix	<p>If Internet is set to DHCP and the current device obtains the IPv6 address prefix from the upstream device. The obtained IPv6 address prefix is displayed.</p>
Gateway	<p>If Internet is set to DHCP, the automatically obtained gateway address is displayed.</p> <p>If Internet is set to Static IP, you need to manually configure this parameter.</p>
DNS Server	<p>If Internet is set to DHCP, the automatically obtained DNS server address is displayed.</p> <p>If Internet is set to Static IP, you need to manually configure this parameter.</p>
NAT66	<p>If the current device cannot access the Internet in DHCP mode or cannot obtain the IPv6 address prefix, you must enable NAT66 to assign the IPv6 address to an intranet client.</p>

4.17.6 Configuring the IPv6 Address for the LAN Port

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

When the device accesses the network in DHCP mode, the upstream device can assign an IPv6 address to the LAN port, and assign IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the upstream device cannot assign an IPv6 address prefix to the current device, you need to manually configure an IPv6 address prefix for the LAN port, and assign IPv6 addresses to the clients in the LAN by enabling the NAT66 function (see [4.17.5 Configuring the IPv6 Address for the WAN Port](#)).

IPv6 Address

1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings **LAN Settings** DHCPv6 Clients Static DHCPv6

LAN Settings + Add Delete Selected

Up to 8 entries can be added.

	VLAN ID	IPv6 Assignment	Subnet Prefix Name	Subnet ID	Subnet Prefix Length	IPv6 Address/Prefix Length	Action
<input type="checkbox"/>	Default	Auto		0	64		Edit Delete

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

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

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

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

Edit ×

IPv6 Assignment ?

IPv6 Address/Prefix ?

Length

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

Edit ×

IPv6 Assignment ?

IPv6 Address/Prefix ?

Length

[Advanced Settings](#)

Subnet Prefix Name ?

Subnet Prefix Length ?

Subnet ID ?

* Lease Time (Min) ?

DNS Server


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

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


4.17.7 Viewing DHCPv6 Clients

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

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

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


IPv6 Address


 1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings LAN Settings DHCPv6 Clients Static DHCPv6

DHCPv6 Clients

 You can view the DHCPv6 clients information on this page.

DHCPv6 Clients Search by IPv6 Address/DUID  [+ Batch Convert](#)

<input type="checkbox"/>	No.	Hostname	IPv6 Address	Remaining Lease Time(min)	DUID	Status
No Data						

< **1** > 10/page Total 0

4.17.8 Configuring the Static DHCPv6 Address

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

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

IPv6 Address

1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings LAN Settings DHCPv6 Clients Static DHCPv6

Static IP Address List

Static IP Address List Search by IPv6 Address/DUID

Up to 200 entries can be added.

<input type="checkbox"/>	No.	IPv6 Address	DUID	Action
No Data				

Total 0

(1) Click **Add**.

Add ×

* IPv6 Address

* DUID

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

(3) Click **OK**.

4.17.9 Configuring the IPv6 Neighbor List

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

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

IPv6 Neighbor List Search by IP Address/MAC A + Add Bind Selected Delete Selected

Up to 256 IP-MAC bindings can be added.

No.	MAC Address	IP Address	Type	Ethernet status	Action
1	58:69:6c:22:08:30	fe80::5a69:6cff:fe22:830	Dynamic	WAN	Bind
2	42:93:d6:46:2e:ab	fe80::5e1a:a95:3ed7:9be4	Dynamic	LAN	Bind
3	f8:e4:3b:13:21:6f	fe80::9120:5120:d4df:562b	Dynamic	LAN	Bind

< 1 > 10/page Total 3

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

Add ×

* Interface

* IPv6 Address

* MAC Address

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

IPv6 Neighbor List Search by IP Address/MAC A + Add Bind Selected Delete Selected

Up to 256 IP-MAC bindings can be added.

No.	MAC Address	IP Address	Type	Ethernet status	Action
1	58:69:6c:22:08:30	fe80::5a69:6cff:fe22:830	Dynamic	WAN	Bind
2	42:93:d6:46:2e:ab	fe80::5e1a:a95:3ed7:9be4	Dynamic	LAN	Bind
3	f8:e4:3b:13:21:6f	fe80::9120:5120:d4df:562b	Dynamic	LAN	Bind

< 1 > 10/page Total 3


5 System Settings

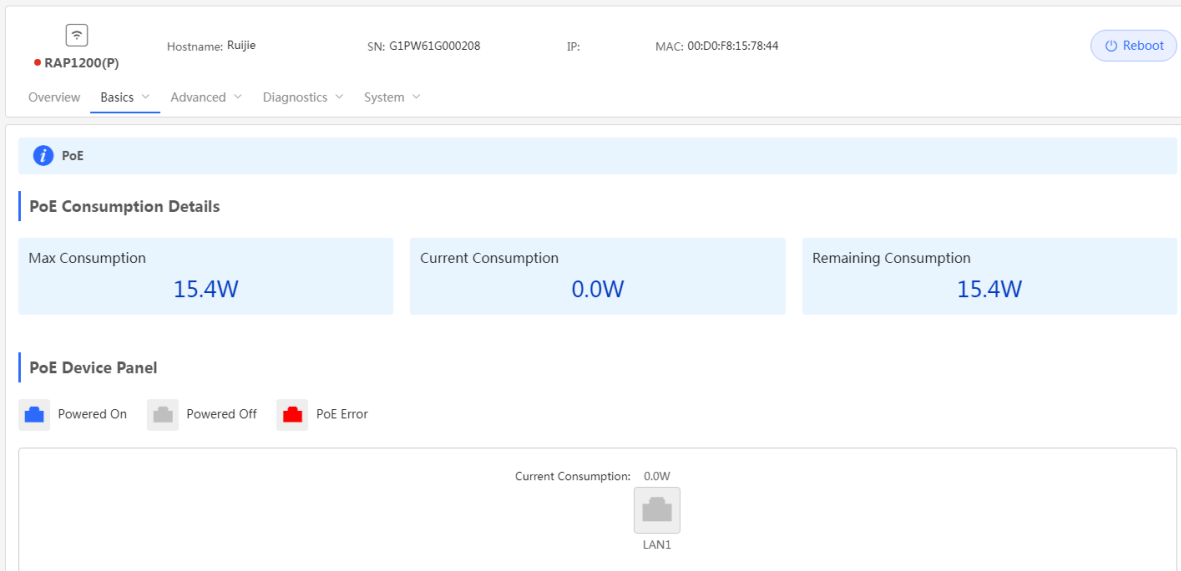
5.1 PoE

Caution

Only RG-RAP1200(P) supports this function.

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

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



Hostname: Rujjie SN: G1PW61G000208 IP: MAC: 00:D0:F8:15:78:44 [Reboot](#)




Overview Basics Advanced Diagnostics System

PoE


PoE Consumption Details

Max Consumption	Current Consumption	Remaining Consumption
15.4W	0.0W	15.4W

PoE Device Panel

 Powered On  Powered Off  PoE Error

Current Consumption: 0.0W

 LAN1

5.2 PoE Settings

Caution

This function is supported by only RG-RAP2260(G), 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.

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

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

i **PoE Settings**

Power Mode

Current Mode IEEE 802.3bt

Energy Saving ?

Band 2.4G 5G 2.4G+5G

Current Power 51W

5.3 Setting the Login Password


For RG-RAP2260(G), 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 models:


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

choose  **System > Login Password**

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

For other RAP models:

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

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

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

⚠ Caution

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

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

* Old Password

* New Password

* Confirm Password


Save

5.4 Setting the Session Timeout Duration

For RG-RAP2260(G), 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 models:


If the device works in self-organizing network mode, and **Local Device** mode webpage is

displayed, choose  **System > Login**

In standalone mode: Choose  **System > Login > Session Timeout**

For other RAP models:

In self-organizing network mode: Choose  **WLAN > APs > Manage > System > Login > Session Timeout**

In standalone mode: Choose  **System > Login > Session Timeout**

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

i Session Timeout

* Session Timeout seconds


[Save](#)

5.5 Setting and Displaying System Time

For RG-RAP2260(G), 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 models:


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

choose  **System > System Time**

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

For other RAP models:


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

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

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

Caution

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

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

Current Time 2022-04-01 10:14:00 [Edit](#)

* Time Zone

* NTP Server [Add](#)

[Delete](#)

[Delete](#)

[Delete](#)

[Delete](#)

[Delete](#)

[Delete](#)

[Save](#)

5.6 Configuring SNMP

Caution

The functions mentioned in this chapter are supported by only RG-RAP2260(G), 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.

5.6.1 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.

5.6.2 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.

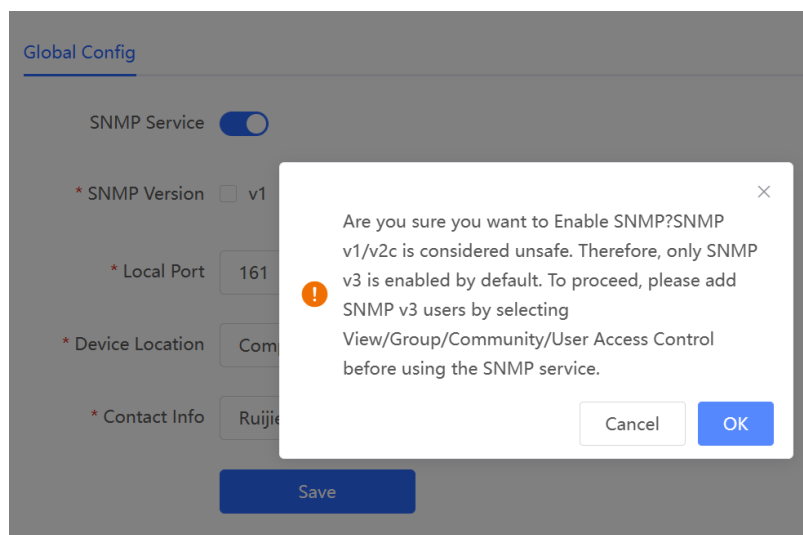
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Table 5-1 Global Configuration Parameters

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

(3) Click **Save**.

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

5.6.3 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.

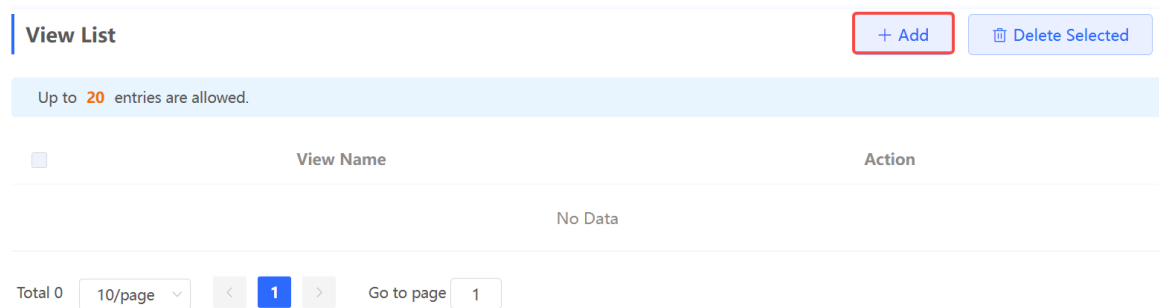
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

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.



View List + Add Delete Selected

Up to 20 entries are allowed.

<input type="checkbox"/>	View Name	Action
No Data		

Total 0 10/page < 1 > Go to page 1

(2) Configure basic information of a view.

Add
×

* View Name

OID

Add Included Rule
Add Excluded Rule

Rule/OID List
Delete Selected

Up to **100** entries are allowed.

	Rule	OID	Action
No Data			

Total 0
10/page
< 1 >
Go to page
1

Cancel
OK

Table 5-2 View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.
Type	There are two types of rules: included and excluded rules. <ul style="list-style-type: none"> ● 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.

Global Config

SNMP Service

* SNMP Version v1 v2c v3

* Local Port


* Device Location

* Contact Info

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.

Global Config [View/Group/Community/Client Access Control](#) Trap Settings

SNMP v1/v2c Community Name List + Add Delete Selected

Up to 20 entries are allowed.

Community Name	Access Mode	MIB View	Action
No Data			

Total 0 10/page < 1 > Go to page 1

(2) Add a v1/v2c user.

Add ×

* Community Name

* Access Mode Read-Only ▼

* MIB View all ▼ [Add View +](#)

Cancel OK

Table 5-3 v1/v2c User Configuration Parameters

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

⚠ Caution

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

(3) Click **OK**.

3. Configuring v3 Groups

- Overview

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

- Prerequisites

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

[Global Config](#) [View/Group/Community/Client Access Control](#) [Trap Settings](#)

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

i 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.

Global Config [View/Group/Community/Client Access Control](#) Trap Settings

SNMP v3 Group List + Add Delete Selected

Up to 20 entries are allowed.

<input type="checkbox"/>	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
<input type="checkbox"/>	default_group	Auth & Security	all	none	none	Edit Delete

Total 1 10/page < 1 > Go to page 1

(2) Configure v3 group parameters.

Add ×

* Group Name

* Security Level Allowlist & Security ▼

* Read-Only View all ▼ [Add View +](#)

* Read & Write View all ▼ [Add View +](#)

* Notification View none ▼ [Add View +](#)

Cancel OK

Table 5-4 v3 Group Configuration Parameters

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

Parameter	Description
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.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

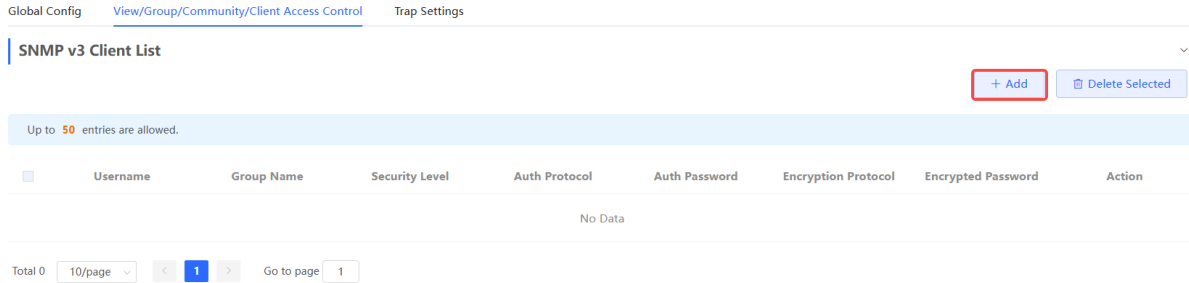
Note

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.

Add ×

* Username

* Group Name

* Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

Table 5-5 v3 User Configuration Parameters

Parameter	Description
Username	<p>Username</p> <p>At least 8 characters.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Admin, public or private community names are not allowed.</p> <p>Question marks, spaces, and Chinese characters are not allowed.</p>

Parameter	Description
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	<p>Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512.</p> <p>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.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.</p>
Encryption Protocol, Encrypted Password	<p>Encryption protocols supported: DES/AES/AES192/AES256.</p> <p>Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption.</p>

 **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.

No.	Device Model	IP	engineID	Action
1			80	Copy

Total 1

5.6.4 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 5-6 User Requirement Specification

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

- Configuration Steps

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

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

- (2) Add a view on the **View/Group/Community/Client Access Control** interface.
- Click **Add** in the **View List** pane to add a view.
 - Enter the view name and OID in the pop-up window, and click **Add Included Rule**.
 - Click **OK**.

Add ×

* View Name

OID

Rule/OID List

Up to 100 entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
No Data			

Total 0

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

Add
×

* Community Name

* Access Mode

* MIB View [Add View +](#)

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 5-7 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.
Configuring v3 Users	User name: v3_user Group name: group Security level: authentication and encryption

Item	Description
	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**.

[Global Config](#) [View/Group/Community/Client Access Control](#) [Trap Settings](#)

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

(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**.

Add
×

* View Name

OID

Add Included Rule
Add Excluded Rule

Rule/OID List Delete Selected

Up to **100** entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
No Data			

Total 0 < 1 > Go to page

Cancel
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**.

Add
×

* Group Name

* Security Level

* Read-Only View Add View +

* Read & Write View Add View +

* Notification View Add View +

Cancel
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**.

Add ×

* Username

* Group Name

* Security Level

* Auth Protocol * Auth Password


* Encryption Protocol * Encrypted Password

5.6.5 Configuring Trap Service

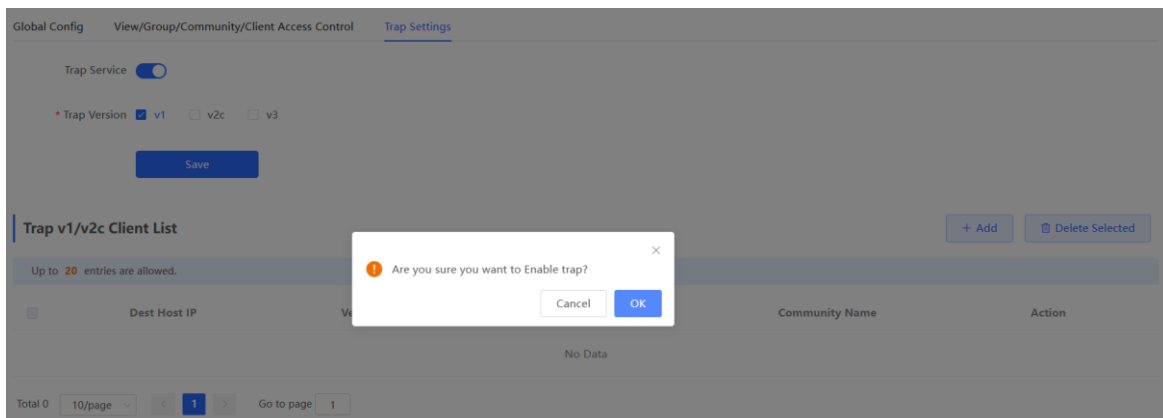
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring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



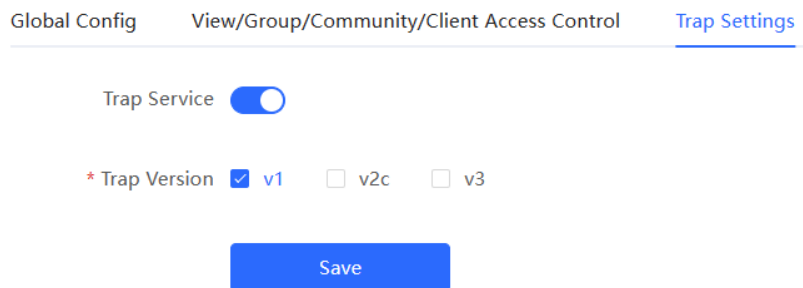
When the trap service is enabled for the first time, the system will pop up a prompt message. Click **OK**.

(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 v1/v2c 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.

Global Config View/Group/Community/Client Access Control **Trap Settings**

Trap Service

* Trap Version v1 v2c v3

Save

Trap v1/v2c Client List + Add Delete Selected

Up to 20 entries are allowed.

<input type="checkbox"/>	Dest Host IP	Version Number	Port ID	Community Name	Action
No Data					

Total 0 Go to page

(2) Configure trap v1/v2c user parameters.

Add ×

* Dest Host IP

* Version Number

* Port ID

* Community
Name/Username

Table 5-8 Trap v1/v2c User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Version Number	Trap version, including v1 and v2c.
Port ID	The port range of the trap peer device is 1 to 65535.
Community Name/Username	Community name of the trap user. At least 8 characters. It must contain at least three character categories, including

Parameter	Description
	<p>uppercase and lowercase letters, digits, and special characters.</p> <p>Admin, public or private community names are not allowed.</p> <p>Question marks, spaces, and Chinese characters are not allowed.</p>

⚠ 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.

Global Config View/Group/Community/Client Access Control **Trap Settings**

Trap Service

* Trap Version v1 v2c v3

Save

Trap v3 Client List **+ Add** **Delete Selected**

Up to 20 entries are allowed.

<input type="checkbox"/>	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
No Data							

Total 0 Go to page

(2) Configure trap v3 user parameters.

Add ×

* Dest Host IP * Port ID

* Username * Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

Table 5-9 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.
Username	Name of the trap v3 user. At least 8 characters. It must contain at least three character categories, including

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

 **Caution**

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

(3) Click **OK**.

5.6.6 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 5-10 User Requirement Specification

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

- Configuration Steps

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

Global Config View/Group/Community/Client Access Control Trap Settings

Trap Service

* Trap Version v1 v2c v3

Save

Trap v1/v2c Client List + Add Delete Selected

Up to 20 entries are allowed.

<input type="checkbox"/>	Dest Host IP	Version Number	Port ID	Community Name	Action
No Data					

Total 0 < 1 > Go to page

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

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

Add
×

* Dest Host IP

* Version Number

* Port ID

* Community

Name/Username

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 5-11 User Requirement Specification

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

- Configuration Steps

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

Global Config View/Group/Community/Client Access Control [Trap Settings](#)

Trap Service

* Trap Version v1 v2c v3

Save

Trap v3 Client List [+ Add](#) [Delete Selected](#)

Up to 20 entries are allowed.

<input type="checkbox"/>	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
No Data							

Total 0

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

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

Add ×

* Dest Host IP * Port ID

* Username * Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

5.7 Configuring Reboot


Caution

- Do not cut off power during system reboot to avoid device damage.
- Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.


- Rebooting the device affects the network. Therefore, exercise caution when performing this operation.
-

5.7.1 Rebooting the Current Device

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **System > Reboot > Reboot**

For other RAP models:

In self-organizing network mode: Choose  **WLAN > APs > Reboot**

In standalone mode: Choose  **System > Reboot > Reboot**

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


 Please keep the device powered on during reboot.

Reboot

5.7.2 Rebooting All Devices in the Network

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


For RG-RAP2260(G), 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 models: In **Network** mode, choose  **System > Reboot > Reboot**

For other RAP models: Choose  **Network > Reboot & Reset > Reboot**

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

Reboot Scheduled Reboot

 Please keep the device powered on during reboot.

Select Local All Devices Specified Devices

Reboot All Device

 **Caution**

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

5.7.3 Rebooting the Specified Device

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

For RG-RAP2260(G), 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 models: In **Network** mode, choose  **System > Reboot > Reboot**

For other RAP models:  **Network > Reboot & Reset > Reboot**

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

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

Reboot Scheduled Reboot

i Please keep the device powered on during reboot.

Select Local All Devices Specified Devices

Available Devices 1/1

Search by SN/Model

G1QH6WX000610 - RAP2260(E)

Selected Devices 0/0

Search by SN/Model

No data

Reboot Scheduled Reboot

i Please keep the device powered on during reboot.

Select Local All Devices Specified Devices

Available Devices 0/0

Search by SN/Model

No data

Selected Devices 1/1

Search by SN/Model

G1QH6WX000610 - RAP2260(E)


167

5.8 Configuring Scheduled Reboot

5.8.1 Configuring Scheduled Reboot for the Current Device

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


For RG-RAP2260(G), 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 models: Choose  **System > Reboot > Scheduled Reboot**

For other RAP models:

To configure scheduled reboot for the current device, choose ( **WLAN > APs > Manage >**)

 **System > Reboot > Scheduled Reboot**

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

Caution

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

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

Reboot [Scheduled Reboot](#)



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

Enable


Day Mon Tue Wed Thu Fri Sat Sun

Time :

Save

5.9 Configuring Backup and Import

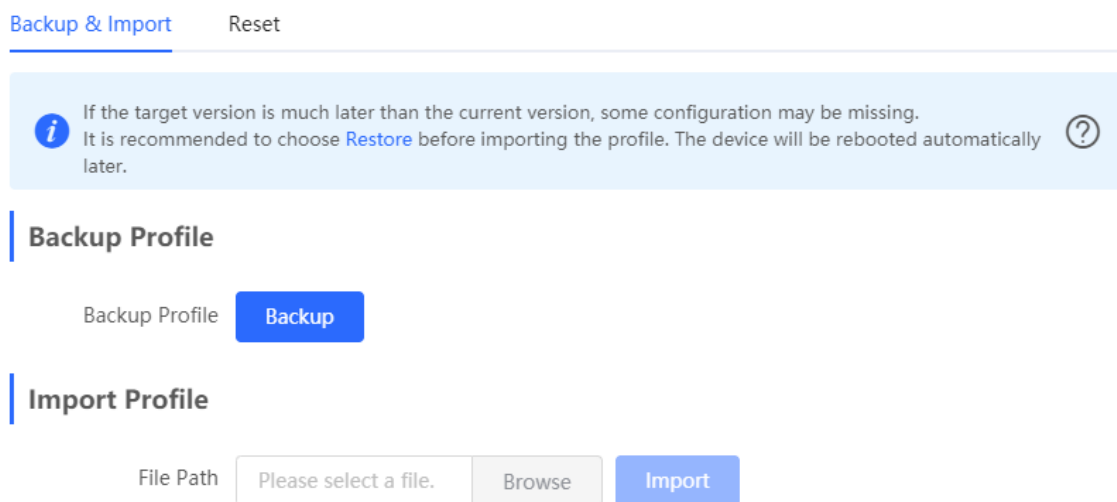
For RG-RAP2260(G), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260

and RG-RAP6262 models: Choose  **System > Backup > Backup & Import**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **System > Backup > Backup & Import**

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

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



[Backup & Import](#) [Reset](#)

i If the target version is much later than the current version, some configuration may be missing. It is recommended to choose [Restore](#) before importing the profile. The device will be rebooted automatically later. **?**

Backup Profile

Backup Profile [Backup](#)


Import Profile

File Path [Browse](#) [Import](#)

5.10 Restoring Factory Settings

5.10.1 Restoring the Current Device to Factory Settings


For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **System > Backup > Reset**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **System > Backup > Reset**

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

Backup & Import [Reset](#)

 Resetting the device will clear the current settings. If you want to keep the setup, please [Backup Profile](#) first.

[Reset](#)

⚠ Caution

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

5.10.2 Restoring All Devices to Factory Settings


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

For RG-RAP2260(G), 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 models: In **Network** mode, choose **System > Backup > Reset**

For other RAP models: Choose  **Network > Reboot & Reset > Restore**

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

Backup & Import [Reset](#)

 Resetting the device will clear the current settings. If you want to keep the configuration, please [Backup Config](#) first.

Select Local All DevicesOption **Unbind Account** (The devices of this account will be removed from Ruijie Cloud and will not be managed by this account).[Reset All Devices](#)

⚠ Caution

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


5.11 Performing Upgrade and Checking System Version

Caution

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

5.11.1 Online Upgrade


For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **System > Upgrade > Online Upgrade**

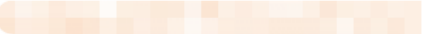
For other RAP models: Choose ( **WLAN > APs > Manage >**  **System > Upgrade > Online Upgrade**



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

[Online Upgrade](#) Local Upgrade

 Online upgrade will keep the current configuration. Please do not refresh the page or close the page.

Current Version ReyeeOS 1. 

New Version **ReyeeOS 1.** 


Description 1. 
 2. 

Tip 1. If your device cannot access the Internet, please click [Download File](#).
 2. Choose [Local Upgrade](#) to upload the file for local upgrade.

[Upgrade Now](#)

5.11.2 Local Upgrade


For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **System > Upgrade > Local Upgrade**


For other RAP models: Choose ( **WLAN** > **APs** > **Manage** >  **System** > **Upgrade** > **Local Upgrade**

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

Online Upgrade Local Upgrade

 Please do not refresh the page or close the browser.

Model RAP 

Current Version ReyeeOS 1. 

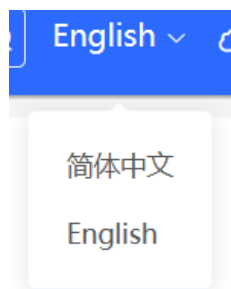
Keep Config (If the target version is much later than the current version, it is recommended not to keep the configuration.)

File Path

5.12 Switching System Language

Choose  in the upper right corner of the Web page.

Click a required language to switch the system language.





5.13 Configuring LED Status Control

Caution

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

For RG-RAP2260(G), 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 models: Choose  **Network** > **LED**

For other RAP models: Choose  **WLAN** > **LED**

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



LED Status Control

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


Enable

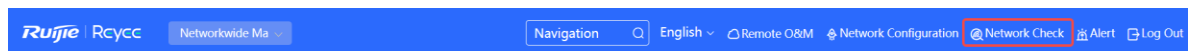
Save

6 Network Diagnosis Tools

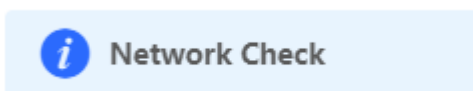
6.1 Network Check

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

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



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



Network Check ⓘ ?

Recheck

100%

- WAN/LAN Cable ✓
- Auto-Negotiated Speed ✓
- WAN Port ✓
- LAN & WAN Address Conflict ✓
- Loop ✓
- DHCP Server Conflict ✓
- IP Address Conflict ✓
- Route ✓
- Next Hop Connectivity ✓
- DNS Server ✓
- IP Session Count ✓

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

IP Session Count ✓

DHCP Capacity ✓

Ruijie Cloud Server !


Check Connection to Cloud Server

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

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

6.2 Network Tools

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Diagnostics > Network Tools**

For other RAP models: Choose ( **WLAN > APs > Manage >**  **Diagnostics > Network Tools**

- The Ping tool tests the connectivity between the access point and the IP address or URL.

The message "Ping failed" indicates that the access point cannot reach the IP address or URL.

- The Traceroute tool displays the network path to a specific IP address or URL.
- The DNS Lookup tool displays the DNS server address used to resolve a URL.

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

Network Tools

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Ping Count

* Packet Size Bytes

```

PING www.baidu.com (163.177.151.109): 64 data bytes
72 bytes from 163.177.151.109: seq=0 ttl=51 time=18.896 ms
72 bytes from 163.177.151.109: seq=1 ttl=51 time=18.686 ms
72 bytes from 163.177.151.109: seq=2 ttl=51 time=18.284 ms
72 bytes from 163.177.151.109: seq=3 ttl=51 time=20.310 ms
                    
```

Network Tools

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Max TTL

```

traceroute to www.baidu.com (163.177.151.109), 20 hops
max, 46 byte packets
 1 192.168.111.1 (192.168.111.1) 0.621 ms 0.536 ms 0.548 ms
 2 172.20.74.1 (172.20.74.1) 2.271 ms 9.091 ms 8.565 ms
 3 172.20.255.109 (172.20.255.109) 2.974 ms 6.424 ms
10.932 ms
 4 * * *
 5 172.22.0.249 (172.22.0.249) 1.902 ms 1.453 ms 1.081 ms
 6 112.111.60.97 (112.111.60.97) 3.215 ms 3.290 ms 2.794 ms
 7 218.104.229.69 (218.104.229.69) 2.890 ms 2.639 ms
                    
```

Network Tools

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

```

Server:      127.0.0.1
Address:    127.0.0.1#53

Name:      www.baidu.com
www.baidu.com canonical name = www.a.shifen.com
Name:      www.a.shifen.com
Address 1: 163.177.151.109
Address 2: 163.177.151.110
www.baidu.com canonical name = www.a.shifen.com
                    
```

6.3 Alarms

For RG-RAP2260(G), 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 models: In **Network** mode, choose  **Network > Alarms**

For other RAP models: Choose ( **WLAN > APs > Manage >**)  **Diagnostics > Alarms**

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

Caution

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

Alert List					View Unfollowed Alert
Expand	Alerts	Suggestion		Action	
▼	There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.		Delete	Unfollow
Hostname	SN	Type	Time	Details	Action
Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,I P:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192.168.112.1,VLAN ID:233	Delete

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

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

Cancel

OK

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

View Unfollowed Alert




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

[Re-follow](#)

Cancel

6.4 Fault Collection

For RG-RAP2260(G), 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 models: In **Local Device** mode, choose  **Diagnostics > Fault Collection**

For RAP models: Choose ( **WLAN > APs > Manage >**  **Diagnostics > Fault Collection**

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



Fault Collection

Compress the configuration file for engineers to identify fault.

Start

7 FAQs

7.1 Login Failure

➤ What can I do when I failed to log in to the Eweb management system?

Perform the following steps:

- (1) Check that the Ethernet cable is properly connected to the LAN port of the device.
- (1) Before accessing the setup page, you are advised to choose **Auto** for the device enabled with DHCP service to assign an IP address to the PC. If you want to configure a static IP address for the PC, please make sure the IP address of the PC and the LAN port are in the same IP range. The default IP address of the LAN port is 10.44.77.254, and the subnet mask is 255.255.255.0. The IP address of the PC should be set to 10.44.77.X (X is an integer between 2 and 254), and the subnet mask is 255.255.255.0.)
- (2) Run the **Ping** command to check the connectivity between the PC and the device. If the ping fails, please check the network settings.
- (3) If the login failure persists, restore the device to factory settings.

7.2 Factory Setting Restoration

➤ How can I restore the device to factory settings?

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

7.3 Password Loss

➤ What can I do when I forget the password?

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