

Ruijie Reyee RG-EG Series Router

Implementation Cookbook



Copyright

Copyright © 2022 Ruijie Networks

All rights are reserved in this document and this statement.

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



and other Ruijie networks logos are trademarks of Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Official website of Ruijie Reye: <https://www.ruijienetworks.com/products/revee>
- Technical Support Website: <https://www.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	Choose System > Time .

2. Signs

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

Warning

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

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

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

Contents

Preface	I
1 Product Introduction	9
1.1 Models	9
1.2 LED Indicators	12
1.3 Button.....	13
2 Getting Started	14
2.1 Network Planning.....	14
2.2 Installing the Router.....	15
2.2.1 Safety Suggestions.....	15
2.2.2 Installation Site Requirement.....	16
2.2.3 Installation Steps.....	18
2.3 Quick Provisioning	18
2.3.1 Quick Provisioning Through Ruijie Cloud App.....	18
2.3.2 Quick Provisioning Through Reyee Eweb.....	25
3 Device Management	28
3.1 Login	28
3.2 Configuring the Login Password.....	29
3.3 Configuring the System Time	30
3.4 Configuring Upgrade.....	32
3.4.1 Online Upgrade.....	32
3.4.2 Local Upgrade.....	33
3.5 Backing Up or Restoring the Configuration	34
3.6 Configuring Restart.....	34

3.6.1 Restarting the Current Device	34
3.6.2 Restarting All Devices on the Network	36
3.6.3 Restarting Specified Devices.....	36
3.6.4 Configuring Scheduled Restart.....	37
3.7 Restoring Factory Settings	38
4 Common Settings.....	39
4.1 Network Access Setting.....	39
4.1.1 PPPoE Configuration Through a WAN Port	39
4.1.2 Static IP Address Configuration Through a WAN Port	41
4.1.3 DHCP Configuration Through a WAN Port.....	42
4.2 AP Management	43
4.2.1 Switching the Working Mode	43
4.2.2 Configuring AP Groups	45
4.2.3 Configuring Wi-Fi	47
4.2.4 Configuring Guest Wi-Fi	50
4.2.5 Adding More Wi-Fi Networks	51
4.2.6 Healthy Mode.....	52
4.2.7 RF Settings	52
4.2.8 Configuring a Wi-Fi Blacklist or Whitelist.....	54
4.2.9 Configuring AP Load Balancing.....	56
4.2.10 Wireless Network Optimization in One-Click Mode.....	59
4.2.11 Enabling Reye Mesh.....	61
4.2.12 Configuring a LAN Port of a Downlink AP	62
4.3 Switch Settings	64

4.4 Diagnostics	65
4.4.1 Network Check.....	65
4.4.2 Alarms	66
4.4.3 Network Tools	67
4.4.4 Packet Obtaining.....	69
4.4.5 Fault Collection	71
4.5 WAN Load Balancing.....	71
4.6 Port VLAN	74
4.7 VPN.....	76
4.7.1 PPTP VPN	76
4.7.2 L2TP VPN	90
4.7.3 IPsec VPN.....	103
4.7.4 L2TP Over IPsec VPN	107
4.7.5 Open VPN.....	119
4.8 Port Mapping.....	125
4.8.1 Configuring Port Mapping.....	127
4.8.2 Configuring NAT-DMZ.....	129
4.9 Dynamic DNS	130
4.10 Authentication	132
4.10.1 Application Scenario	132
4.10.2 Cloud Authentication.....	134
4.10.3 Local Account Authentication.....	138
4.10.4 Authorized Authentication	141
4.10.5 QR Code Authentication	143

4.10.6 Whitelist.....	144
4.10.7 Online Clients.....	145
4.10.8 WeChat Authentication	146
4.10.9 Enterprise WeChat Authentication.....	150
4.11 Behavior.....	152
4.11.1 Application Scenario.....	152
4.11.2 App Control.....	152
4.11.3 Website Management	158
4.11.4 Access Control	162
4.12 Flow Control.....	166
4.12.1 Application Scenario	166
4.12.2 Smart Flow Control	167
4.12.3 Custom Policies	169
4.12.4 Application Priority	176
4.13 Security.....	179
4.13.1 Application Scenario	179
4.13.2 Configuring the ARP List and ARP Guard	180
4.13.3 Configuring MAC Address Filtering	182
4.13.4 Configuring Device Security	183
4.14 Configuring the PPPoE Server.....	185
4.14.1 Application Scenario	185
4.14.2 Global Settings.....	185
4.14.3 Configuring a PPPoE User Account	187
4.14.4 Configuring a Flow Control Package	189

4.14.5 Configuring Exceptional IP Addresses	190
4.14.6 Checking Online Users	191
4.15 IPTV	192
4.15.1 Application Scenario	192
4.15.2 Dual-WAN Configuration	193
4.15.3 Single-WAN Configuration	195
4.16 UPnP	197
5 Advanced Solution	200
5.1 Reeye Flow Control Solution	200
5.1.1 Application Scenario	200
5.1.2 Configuration Example	200
5.1.3 Configuration Verification	207
5.2 Reeye Cloud Authentication Solution	207
5.2.1 Working Principle	207
5.2.2 Application Scenario	208
5.2.3 Configuration Example	208
5.2.4 Configuration Verification	216
5.3 Reeye Guest Wi-Fi Solution	217
5.3.1 Working Principle	217
5.3.2 Application Scenario	217
5.3.3 Configuration Example	217
5.4 Reeye Economic Hotel Network Solution	230
5.4.1 Application Scenario	230
5.4.2 Configuration Example	231

5.4.3 Configuration Verification.....	241
6 FAQ	242
6.1 Reeye Password FAQ (Collection).....	242
6.2 Ruijie Cloud Reeye EG authentication FAQ (Collection)	242
6.3 Reeye Mesh FAQ (Collection).....	242
6.4 Reeye IPTV FAQ (Collection).....	242
6.5 Reeye Authentication FAQ (Collection).....	242
6.6 Reeye Behavior Strategy FAQ (Collection).....	242
6.7 Reeye DDNS FAQ (Collection)	242
6.8 Reeye VPN FAQ ((collection)).....	242
6.9 Reeye Flow Control FAQ (Collection)	242
6.10 Reeye Guest Wi-Fi FAQ (Collection)	242
6.11 Reeye Wireless Configuration FAQ (Collection).....	242
6.12 Reeye Self-Organizing Network (SON) FAQ (Collection).....	242
6.13 Reeye series Devices Parameters Tables	242
6.14 Reeye Parameter Consultation FAQ (Collection)	242
7 Appendix: Surveillance.....	243
7.1 Device Info.....	243
7.2 Wi-Fi Information	245
7.3 Network Status.....	245
7.4 Real-Time Flow.....	245
7.5 Flow History	245
7.6 URL Logs.....	246
7.7 Online Clients.....	247

1 Product Introduction

Reyee RG-EG series router is a cloud managed router designed for villas and smart home, restaurants, small offices, and homestay hotels. It is affordable, small, and easy to use, providing 500–600 Mbit/s bandwidth and supporting up to 200 clients.

RG-EG series routers provide industry-leading auto-discovery and auto-networking for routers, switches, and wireless devices.

RG-EG series routers can perform per-port VLAN configuration to achieve port isolation, and integrate with smart flow control to achieve comprehensive network planning and perform local and remote network diagnosis.

1.1 Models

The RG-EG series routers come in five models.

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG105G-P	5 (PoE supported)	100	500 Mbit/s asymmetric bandwidth (flow control disabled) 300 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32
RG-EG105G-P V2	5 (PoE supported)	100	500 Mbit/s asymmetric bandwidth (flow control disabled) 600 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG105G	5	100	500 Mbit/s asymmetric bandwidth (flow control disabled) 300 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32
RG-EG105G V2	5	100	600 Mbit/s asymmetric bandwidth (flow control disabled) 500 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32
RG-EG105GW	5	100 (recommended number of wireless terminals: 60)	500 Mbit/s asymmetric bandwidth (flow control disabled) 300 Mbit/s asymmetric bandwidth (flow control enabled)	Router mode: 32
RG-EG210G-E	10	200	1 Gbit/s asymmetric bandwidth (flow control disabled) 1 Gbit/s asymmetric bandwidth (flow control enabled)	AC mode: 500 Router mode: 150

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG210G-P	10 (PoE supported)	200	600 Mbit/s asymmetric bandwidth (flow control disabled) 500 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 500 Router mode: 150
RG-105GW(T)	5	100	600 Mbit/s (1500 bytes, NAT + flow audit) 400 Mbit/s (1500 bytes, NAT + authentication, application identification, flow audit, and flow control)	No. of Manageable Devices (AP + NBS Switches, Router Mode, including this device): 32 No. of Manageable Devices (AP + NBS Switches, Wired Repeater Mode, including this device): N/A No. of Manageable Devices (AP + NBS Switches, Wired Repeater Mode, including this device): 32 No. of Manageable Devices (ES Switches): 128

1.2 LED Indicators

LED Indicator	Status	Description
SYS	Flashing	<p>Fast flashing (at 8 Hz): The router is starting up.</p> <p>Slow flashing (at 0.5 Hz): The network is unreachable.</p> <p>One long flash followed by three short flashes (at 0.8 Hz): The router is faulty.</p> <p>Flashing twice consecutively (at 0.8 Hz):</p> <ul style="list-style-type: none"> ● The router is restoring factory settings. ● The router is upgrading the software. <p>Note: Do not power off the router in this case.</p>
	Solid on	The router is functioning properly.
	Off	The router is not powered on.
Port	Flashing	The port is connected and is sending/receiving traffic.
	Solid on	The port is connected and is not sending/receiving traffic.
	Off	No link is detected for this port.
Mesh	Off	<ul style="list-style-type: none"> ● Mesh pairing is not implemented. ● Wireless relay is not set up.
	Flashing alternately	Mesh pairing is in progress.
	Three bars on	<ul style="list-style-type: none"> ● The mesh signal strength is high. ● The wireless relay signal strength is high.
	Two bars on	<ul style="list-style-type: none"> ● The mesh signal strength is medium. ● The wireless relay signal strength is medium.
	One bar on	<ul style="list-style-type: none"> ● The mesh signal strength is low. ● The wireless relay signal strength is low.

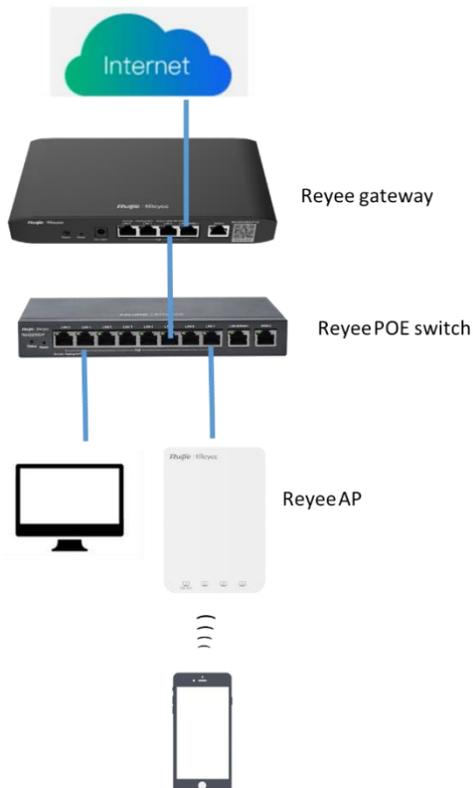
1.3 Button

Button	Description
Reset	<p>Press the Reset button for less than 2 seconds to restart the device.</p> <p>Press the Reset button for over 5 seconds to restore the router to factory settings. (Release the button when the system status LED blinks).</p> <p>The default management IP address is http://192.168.110.1.</p>
Mesh Button	Press the Mesh button for less than 2 seconds to perform mesh pairing.

2 Getting Started

2.1 Network Planning

The following figure shows a typical topology of a Reyee router.



The DHCP server has two address pools on the Reyee router: 192.168.110.0/24 in VLAN 1 for devices of this network and 192.168.10.0/24 in VLAN 10 for clients of this network.

The following ports are used for Ruijie Cloud management. To bring devices to go online on Ruijie Cloud, ensure that these ports are available and data flows are permitted on the network.

Domain name (Cloud-as)	DST.IP	Domain name (Cloud-eu, Cloud-me)	DST.IP	DST.TCP	DST.UDP
Device Online Related:		Device Online Related:			
devicereg.ruijienetworks.com	35.197.150.240	devicereg.ruijienetworks.com	35.190.10.141	80,443	
ryrc.ruijienetworks.com	35.197.150.240	ryrc.ruijienetworks.com	35.234.108.108	80,443	
stunrc.ruijienetworks.com	35.197.150.240	stunrc.ruijienetworks.com	35.234.108.108		34,783,479
stunsvr-as.ruijienetworks.com	34.126.80.150	stunsvr-eu.ruijienetworks.com	35.246.237.78		34,783,479
stunb-as.ruijienetworks.com	34.126.80.150	cwmpsvr-eu.ruijienetworks.com	34.159.112.239		34,783,479
stunc-as.ruijienetworks.com	34.87.169.209	cwmpcp-eu.ruijienetworks.com	34.120.73.71		34,783,479
cwmpsvr-as.ruijienetworks.com	35.197.136.171	cwmpb-eu.ruijienetworks.com	34.159.112.239	80, 443	
cwmpcp-as.ruijienetworks.com	34.160.143.162				
cwmpb-as.ruijienetworks.com	35.197.136.171				
Log Upload:		Log Upload:			
34.87.93.12	34.87.93.12	cloudlog-eu.ruijienetworks.com	35.246.247.49	80,443	
Advanced Service:		Advanced Service:			
firmware.ruijienetworks.com	34.87.32.36	firmware.ruijienetworks.com	34.89.153.55	80,443	
cloudweb.ruijienetworks.com	34.87.32.36	cloudweb.ruijienetworks.com	34.89.153.55	80,443	
fastonline.ruijienetworks.com	34.87.32.36	fastonline.ruijienetworks.com	34.89.153.55	80,443	
cloudapi.ruijienetworks.com	35.197.150.240	cloudapi.ruijienetworks.com	35.234.108.108	80,443	
cdn.ruijienetworks.com	35.201.94.110	cdn.ruijienetworks.com	35.190.93.193	80,443	
ES Series Switch		ES Series Switch			
iotrc.ruijienetworks.com	34.87.101.31	iotrc.ruijienetworks.com	34.107.106.56		7683
iotsvr-as.ruijienetworks.com	35.247.161.22	iotsvr-eu.ruijienetworks.com	35.242.228.40		5683
iotlog-as.ruijienetworks.com	35.240.167.168	iotlog-eu.ruijienetworks.com	35.198.144.180		6683
iotdl-as.ruijienetworks.com	34.87.141.45	iotdl-eu.ruijienetworks.com	35.234.118.145		8683
MQTT Devices with P206 version		MQTT Devices with P206 version			
ryrcmq.ruijienetworks.com	34.120.84.165	ryrcmq.ruijienetworks.com	34.149.186.87	25857	
ehrcmq.ruijienetworks.com	34.120.84.165	ehrcmq.ruijienetworks.com	34.149.186.87	25857	
mqcIt001-as.rj.link	34.160.191.165	mqcIt001-eu.rj.link	34.120.138.185	25857	

2.2 Installing the Router

2.2.1 Safety Suggestions

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

1. Installation

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

2. Movement

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

3. Electricity

- Observe local regulations and specifications when performing electric operations. The operators must be qualified.
- Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp or wet ground or floor.
- Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.
- Try to avoid maintaining the switch that is powered on alone.

- Make a careful check before you cut off the power supply.
- Do not place the equipment in a damp location. Do not let any liquid enter the chassis.

4. Static Discharge Damage Prevention

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

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

5. Laser

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

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

2.2.2 Installation Site Requirement

The installation site must meet the following requirement to ensure normal working and a prolonged durable life Reyee EG series routers.

1. Ventilation

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

2. Temperature and Humidity

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

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

In an environment with a high humidity, insulating materials may have bad insulation or even leaking electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.

In an environment with a low humidity, insulating strips may dry and shrink. Static electricity may occur easily and endanger circuits on the device.

In an environment with a high temperature, the router is subject to more serious harm. Its performance may degrade significantly and various hardware faults may occur.

3. Cleanness

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

4. Grounding

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

- Lightning Grounding

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

- EMC Grounding

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

5. EMI

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

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

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

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

signal interfaces caused by over-voltage or over-current of lightning.

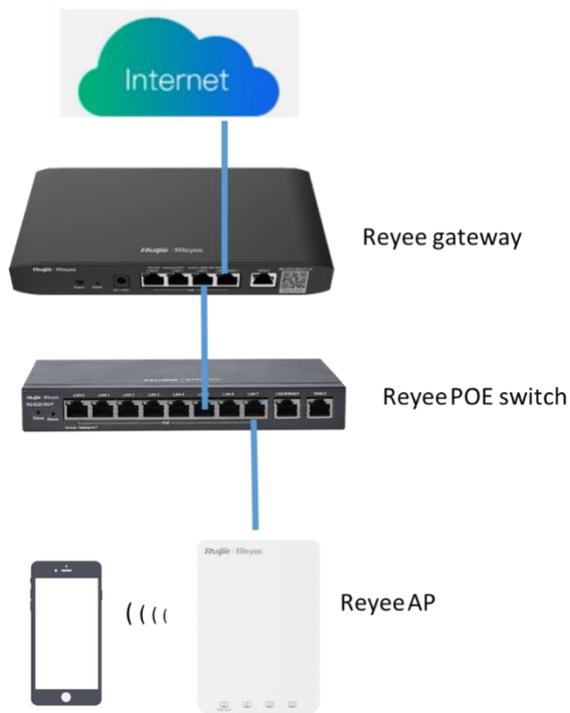
2.2.3 Installation Steps

For details about installation steps, see *Hardware Installation and Reference Guide*.

2.3 Quick Provisioning

2.3.1 Quick Provisioning Through Ruijie Cloud App

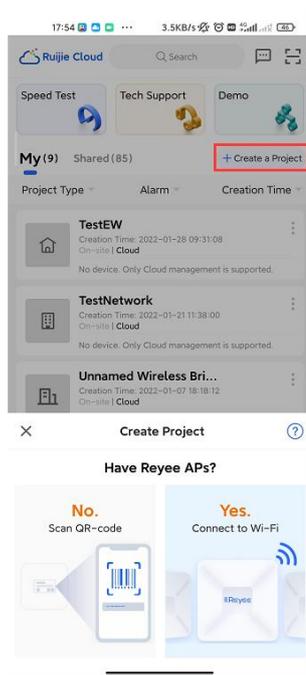
The Reyee router is often used with a Reyee PoE switch and a Reyee RAP.



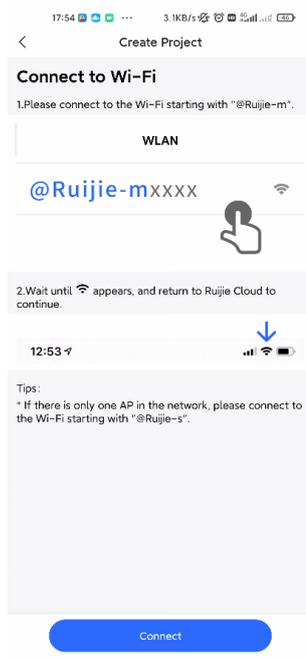
Connect the devices through Ruijie Cloud App for configuration and remote maintenance.

(1) Create a project.

- a Open Ruijie Cloud App, click **Create a Project**, and select **Connect to Wi-Fi**.



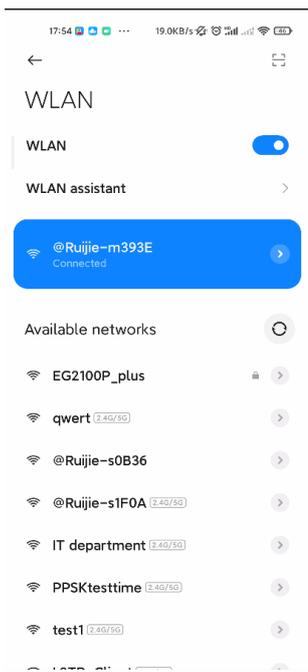
- b After you click **Yes**, Ruijie Cloud App will ask you to connect SSID **@Ruijie-mxxxx**.



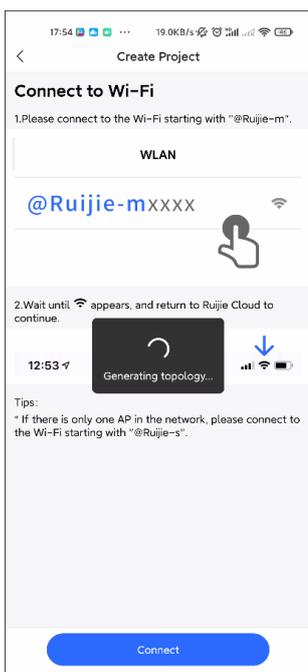
i Note

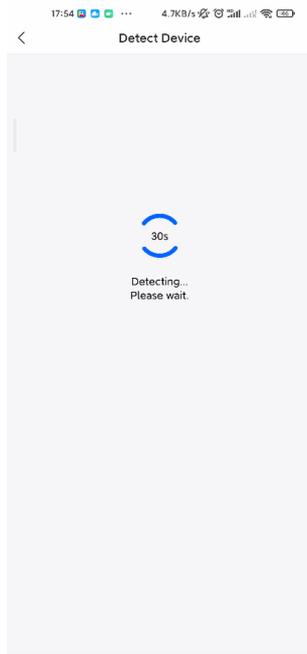
@Ruijie-mxxxx is generated after network self-organization established successfully, while **@Ruijie-sxxxx** is generated on a standalone device. **xxxx** is the last four digits of the MAC address of a device.

- c Click **Connect** and access SSID **@Ruijie-mxxxx**.



- d After you access SSID **@Ruijie-mxxxx SSID**, Ruijie Cloud App will generate the topology and detect all devices on the SON.

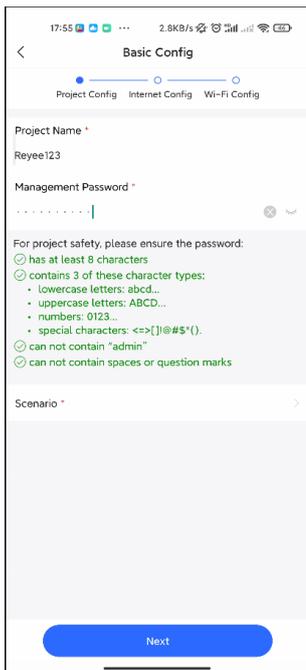




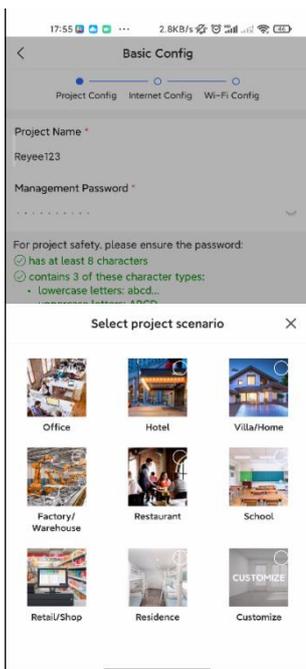
- e After all devices are detected, Cloud App will display them and show the topology.



- (2) Click **Start Config** to perform basic configuration of this project.
- a Set **Project Name** and **Management Password**.

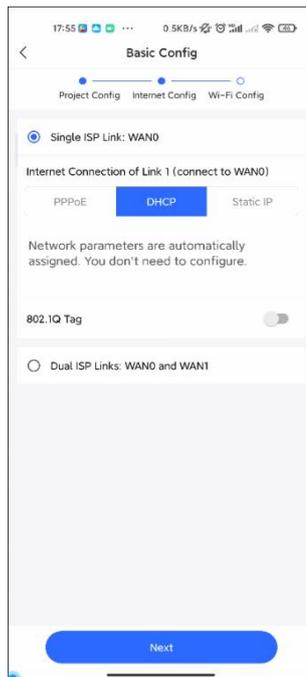


b Select the scenario of this project based on your requirement.

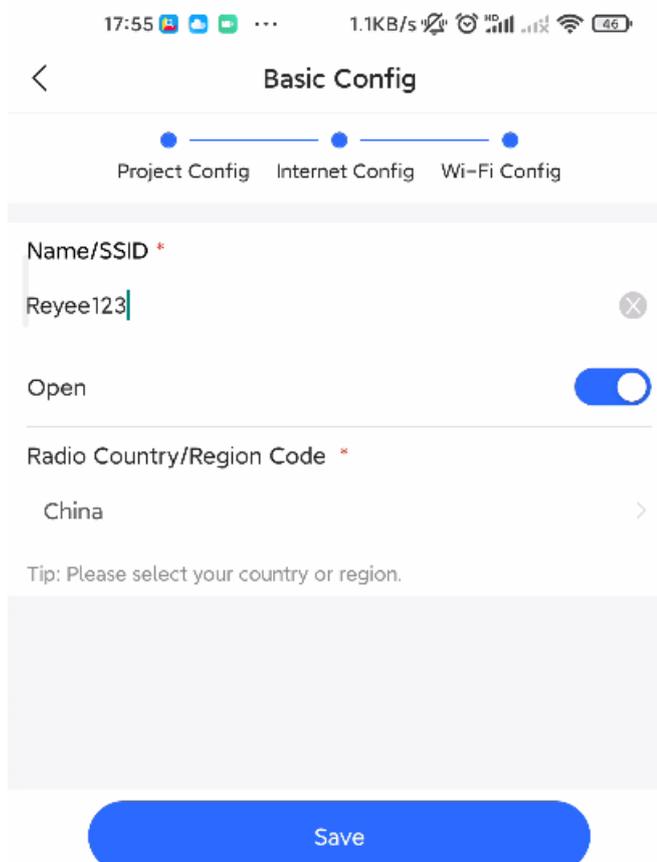


(3) Configure the Internet.

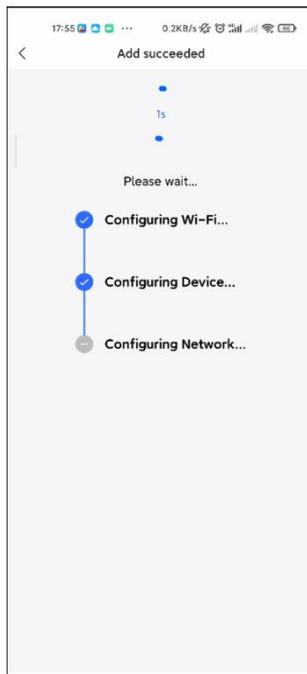
For WAN configuration, you can choose **PPPoE**, **DHCP**, or **Static IP**.



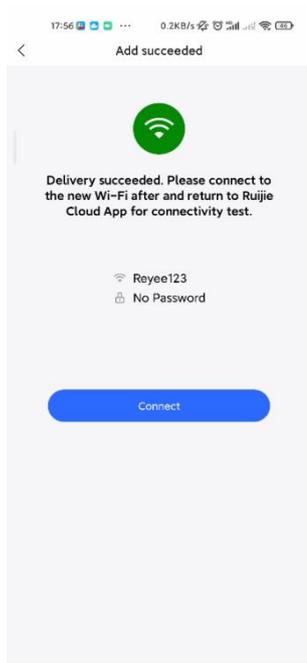
- (4) Configure the SSID.
- Enter the name of the SSID.
 - Configure it as open to allow clients to access this SSID.
 - Configure the password for this SSID.
 - Select the region code.



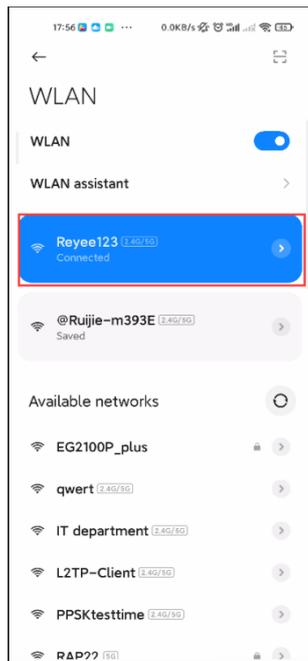
- e The configuration will be synchronized to the network.



- f After about 3s, Ruijie Cloud App will prompt that the configuration is delivery succeed.

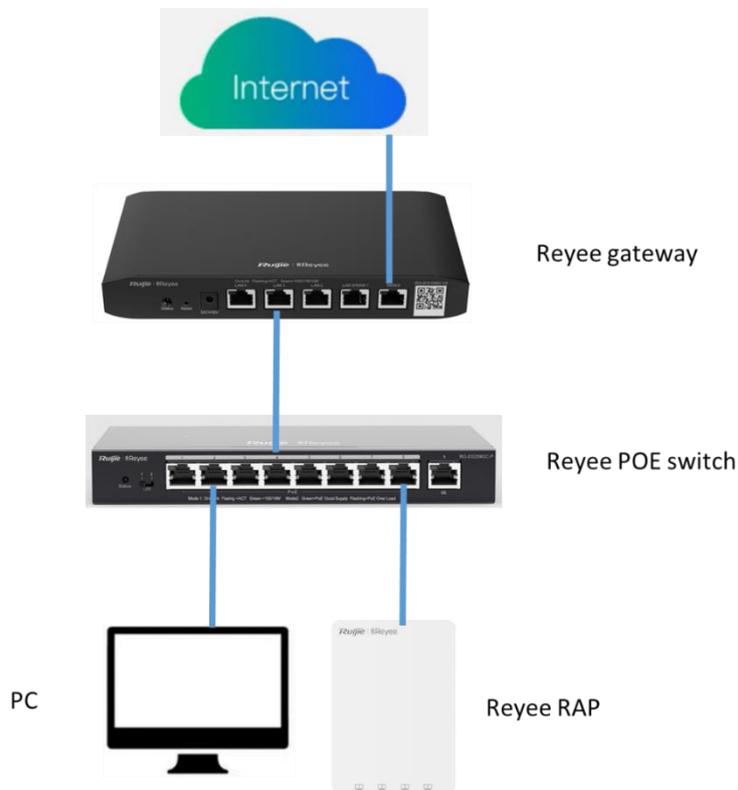


- g Connect to the SSID created just now to manage the whole network on Cloud App.



2.3.2 Quick Provisioning Through Reyee Eweb

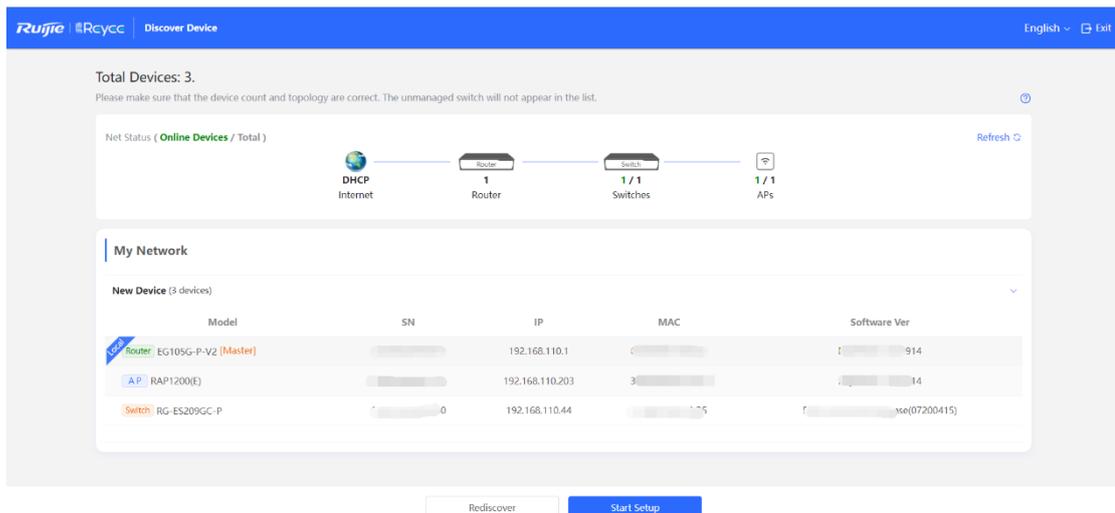
The Reyee router is often used with a Reyee PoE switch and a Reyee RAP.



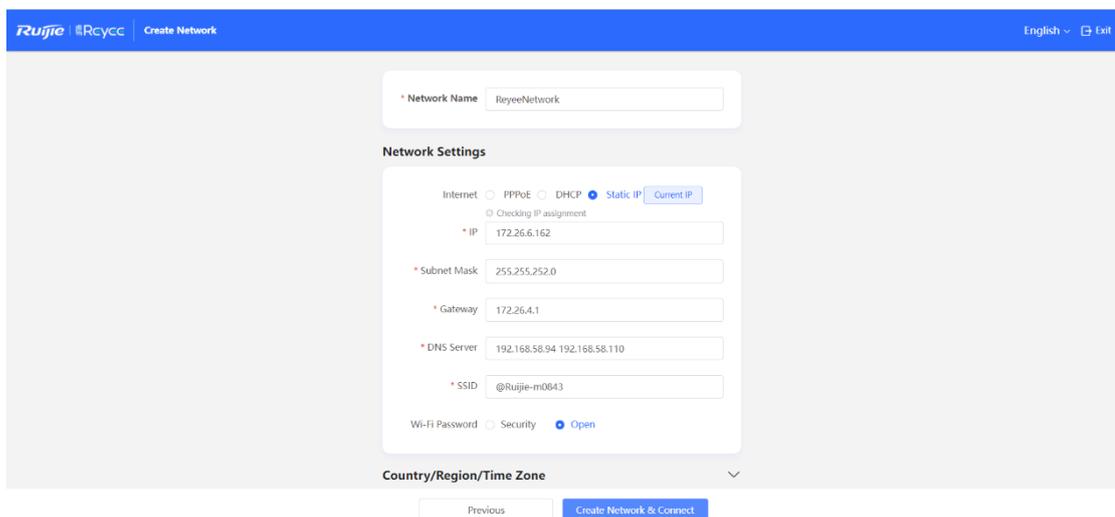
You can use a web management system to configure and maintain the Reyee router.

- (1) Connect a PC to a PoE switch, set the IP address of PC to the static IP address 192.168.110.x.
- (2) Enter 192.168.110.1 in the address bar of the browser to log in to the Eweb of the EG.

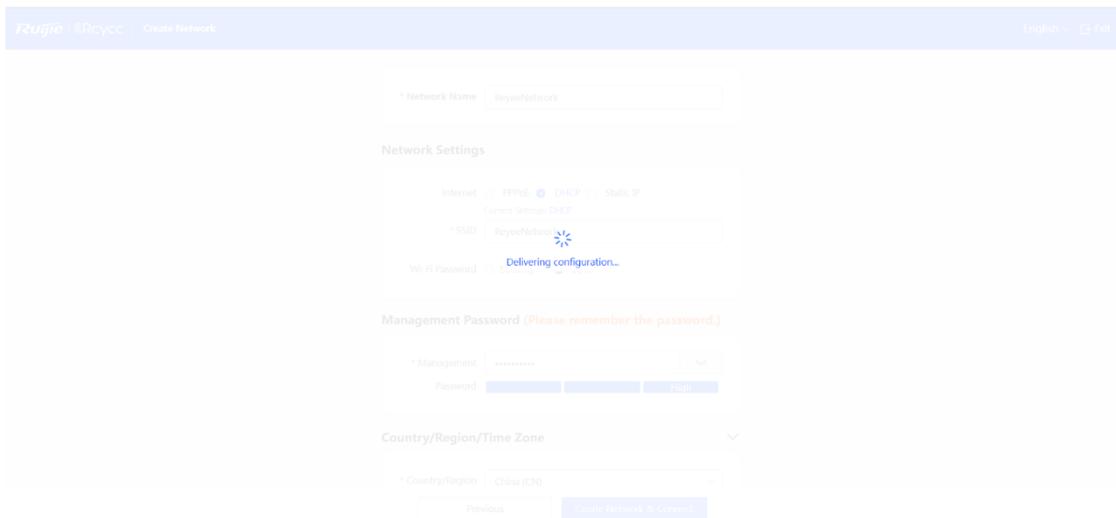
All devices on the network will be displayed in Eweb.



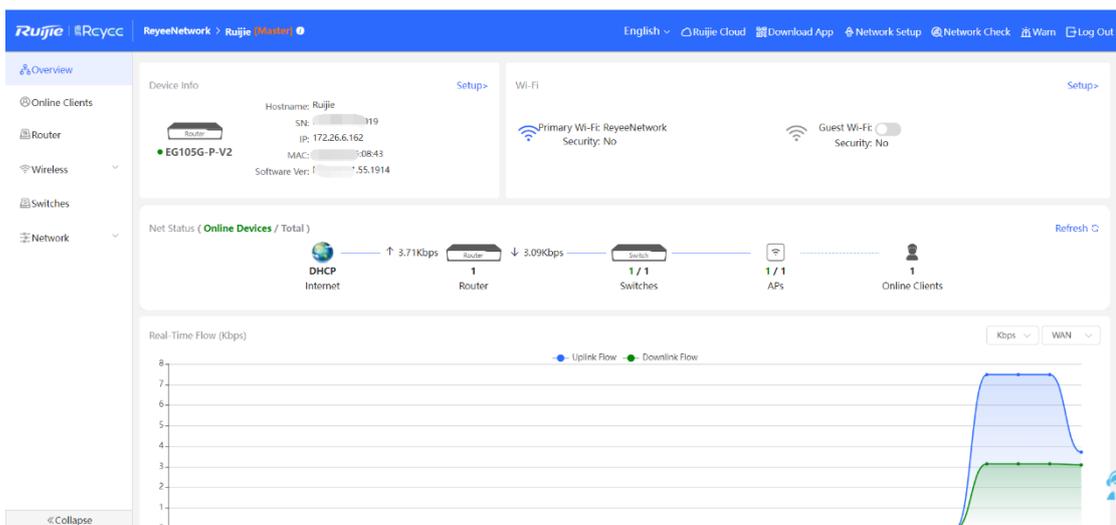
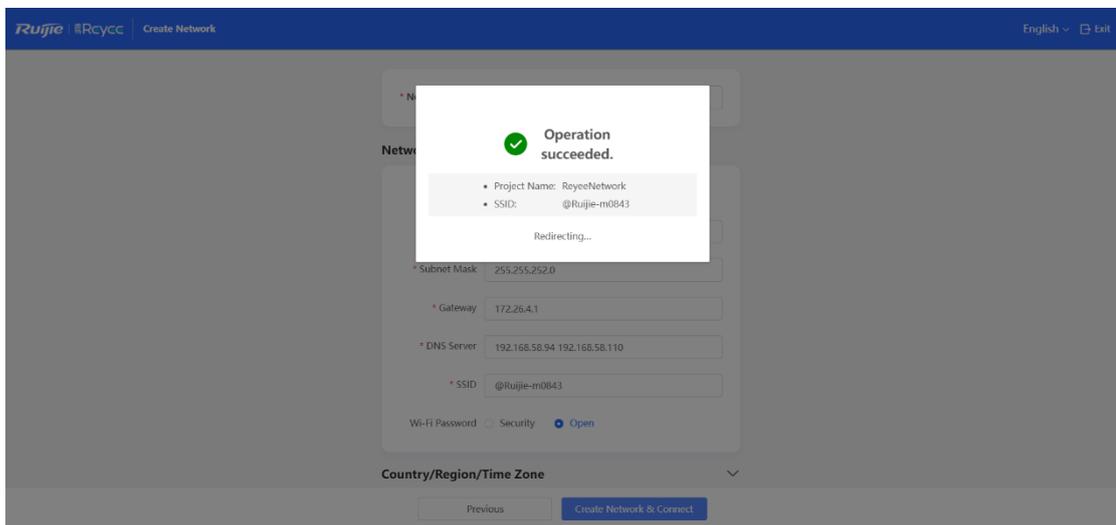
- (3) Click **Start Setup** to perform quick start of the network.



- Enter the network name, and configure the Internet access mode of this network.
 - Enter the password of the SSID or configure the SSID as open.
 - Select the country/region.
- (4) Click **Create Network & Connect**. The configuration will be delivered and activated.



After the configuration has been delivered and activated, you can access the **Overview** page to manage the SON of Reyee devices.



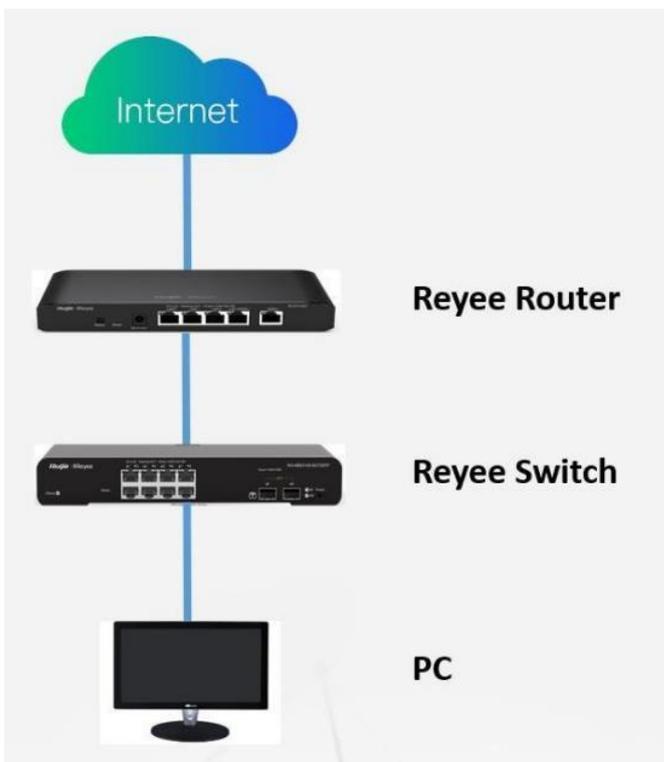
3 Device Management

3.1 Login

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

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

You can access the Eweb management system of an access or aggregation switch through a PC browser to manage and configure the device.



1. Set PC's IP assignment mode to obtain IP addresses automatically.
2. Visit <http://192.168.110.1> through Microsoft Chrome.
3. Enter the password on the login page and click **Login**.

The default password is **admin**.



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

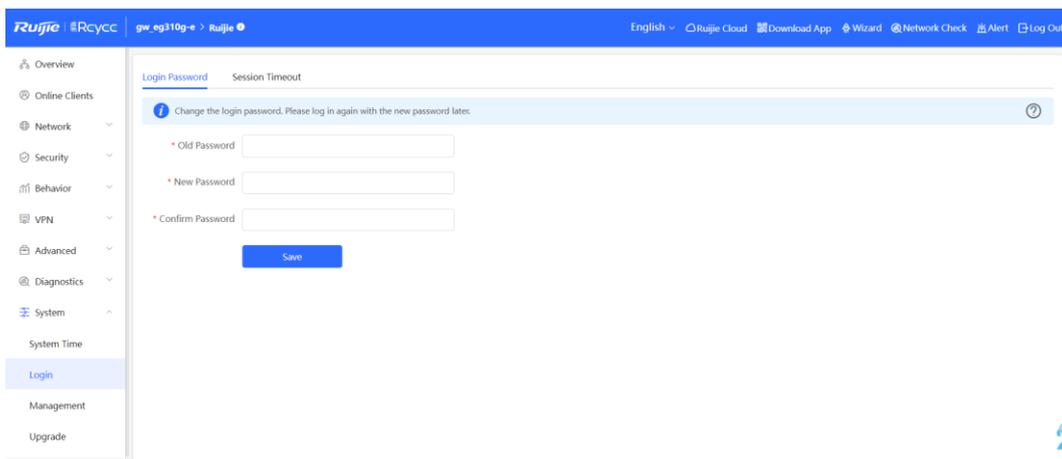
The default login password for all Reyee devices is **admin**.

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

3.2 Configuring the Login Password

Change your password regularly to ensure account security.

- (1) Log into the web management system by using the default IP address.
- (2) Choose **System > Login > Login Password**.
- (3) Enter the old password and new password.
- (4) Click **Save**.



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

Caution

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

3.3 Configuring the System Time

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 the time is still incorrect, click **Edit** to manually set the time. In addition, the device supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server as required.

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

Current Time 2022-04-27 12:38:30

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

* NTP Server

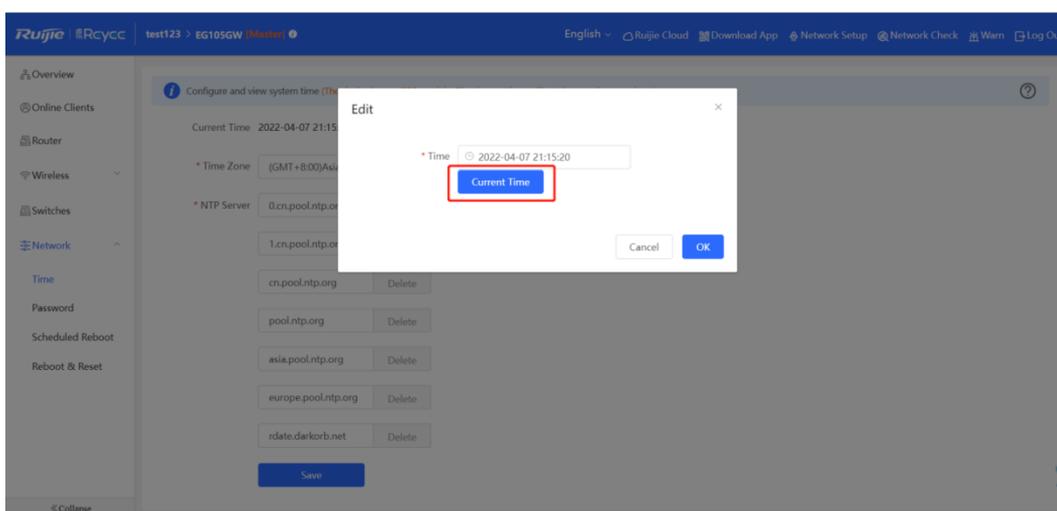
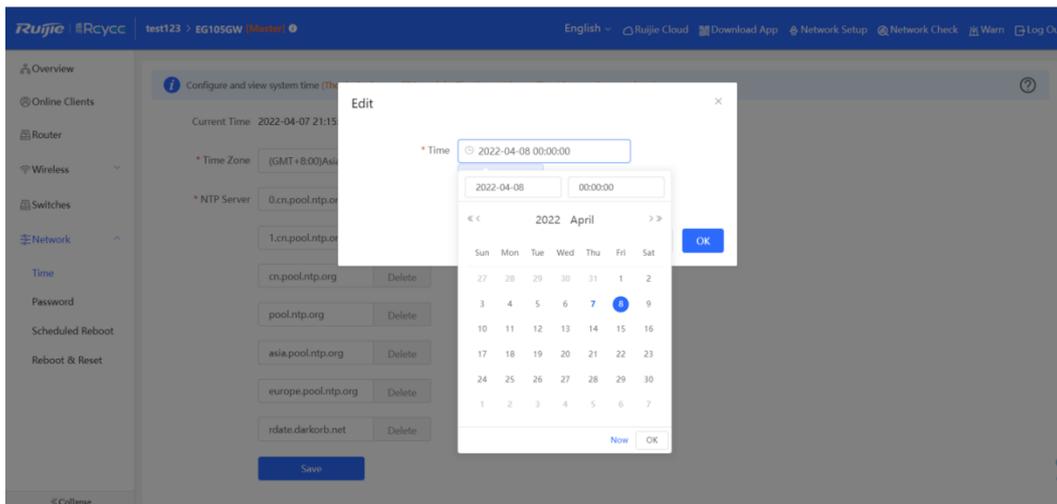
0.cn.pool.ntp.org	<input type="button" value="Add"/>
1.cn.pool.ntp.org	<input type="button" value="Delete"/>
cn.pool.ntp.org	<input type="button" value="Delete"/>
pool.ntp.org	<input type="button" value="Delete"/>
asia.pool.ntp.org	<input type="button" value="Delete"/>
europa.pool.ntp.org	<input type="button" value="Delete"/>
rdate.darkorb.net	<input type="button" value="Delete"/>

Choose **Current Time > Edit > Current Time**. The current system time will be filled in automatically.

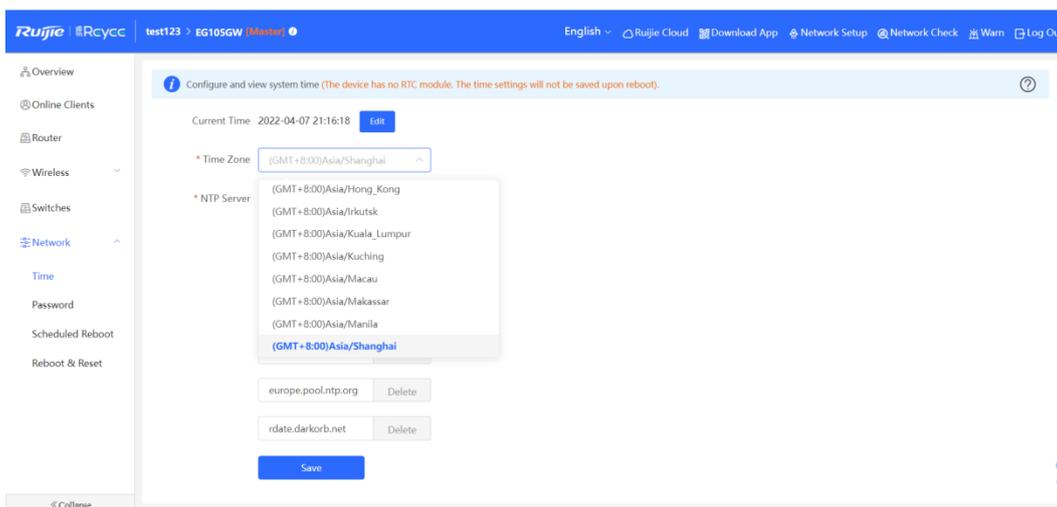
Edit ×

* Time

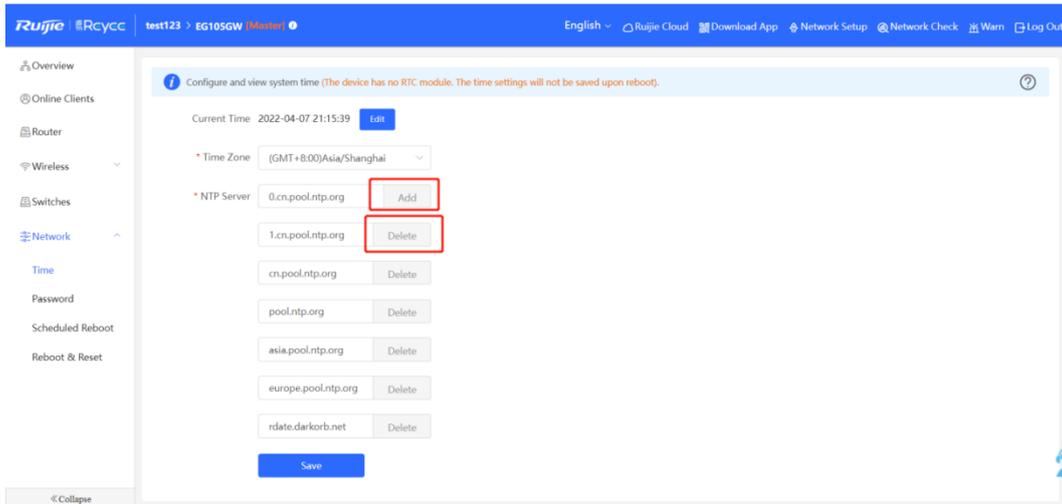
- Manually edit the current time or click **current time** to synchronize the current time automatically.



- Manually select a value from the **Time Zone** drop-down list box.



- Add or delete the NTP server.



3.4 Configuring Upgrade

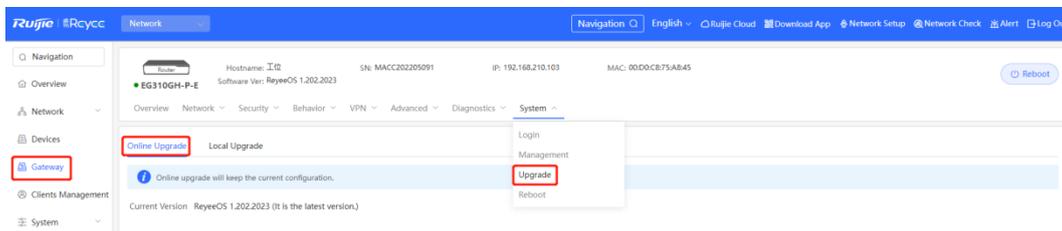
To use new features, upgrade the router to the latest version. There are two methods of upgrading routers: online upgrade and local upgrade.

3.4.1 Online Upgrade

The router that is connected to the Internet can be upgraded online.

Log in to the Eweb of the device.

(1) Choose **Gateway > System > Upgrade > Online Upgrade**.



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

[Online Upgrade](#) Local Upgrade

i Online upgrade will keep the current configuration. Please do not refresh the page or close the browser.

Current Version ReyeeOS 1.86.1229

New Version **ReyeeOS 1.86.1230**

Description 1. **Fix the issue of the system not starting normally after the upgrade.**
2. **Fix the issue of the system not starting normally after the upgrade.**

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

3.4.2 Local Upgrade

Upgrade the router by uploading a local upgrade package.

Confirm the target version and download the upgrade package from the official website.

- (1) Log in to the Eweb of the router.
- (2) Choose **Gateway > System > Upgrade > Local Upgrade**.

Overview Network Security Behavior VPN Advanced Diagnostics **System**

Online Upgrade [Local Upgrade](#)

i Please do not refresh the page or close the browser.

Model EG105G-P-V2

Current Version ReyeeOS 1.86.1929

Keep Config (If the target version is much later than the current version, it is recommended not to keep the configuration.)

File Path

- (3) Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file.
- (4) After the file is uploaded successfully, the system displays upgrade package information and asks for the upgrade. Click **OK** to start the upgrade.
- (5) After the upgrade is complete, choose **Gateway > Overview** and check whether the current version is consistent with the target version in the **Device Details** pane.
 - If versions are consistent, the upgrade is successful.
 - If versions are inconsistent, the upgrade fails. Try again or contact RITA.

The screenshot shows the 'Overview' page of the Ruijie Eweb interface. At the top, there are navigation tabs: Overview, Network, Security, Behavior, VPN, Advanced, Diagnostics, and System. The 'Overview' section displays three key metrics: Memory Usage at 65%, Online Clients at 3, and Status as Online. Below this, the 'Device Details' section lists various attributes: Model (EG105G-P-V2), MAC (00:D0:F8:15:08:43), Hardware Ver (1.00), Hostname (EG105G-P-V2), Work Mode (Router), Software Ver (ReyeeOS 1.86.1929), SN (M...), and Role (Master AC).

3.5 Backing Up or Restoring the Configuration

Back up the configuration to restore the configuration quickly in the case of a failure.

- (1) Log into the Eweb of the router.
- (2) Choose **Gateway > System > Management**.

The screenshot shows the 'Backup & Import' page in the Ruijie Eweb interface. The page has a blue header with the Ruijie logo and navigation options. A sidebar on the left contains a navigation menu with options like Overview, Network, Devices, Gateway, Clients Management, and System. The main content area shows the 'Backup & Import' section with a 'Reset' button. Below this, there is a warning message: 'If the target version is much later than the current version, some configuration may be missing. It is recommended to choose Reset before importing the configuration. The device will be rebooted automatically later.' The 'Backup Config' section has a 'Backup' button, and the 'Import Config' section has a 'File Path' input field with 'Browse' and 'Import' buttons.

- (3) Click **Backup** to download a configuration file locally.
- (4) To restore the configuration, click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The router will restart.

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

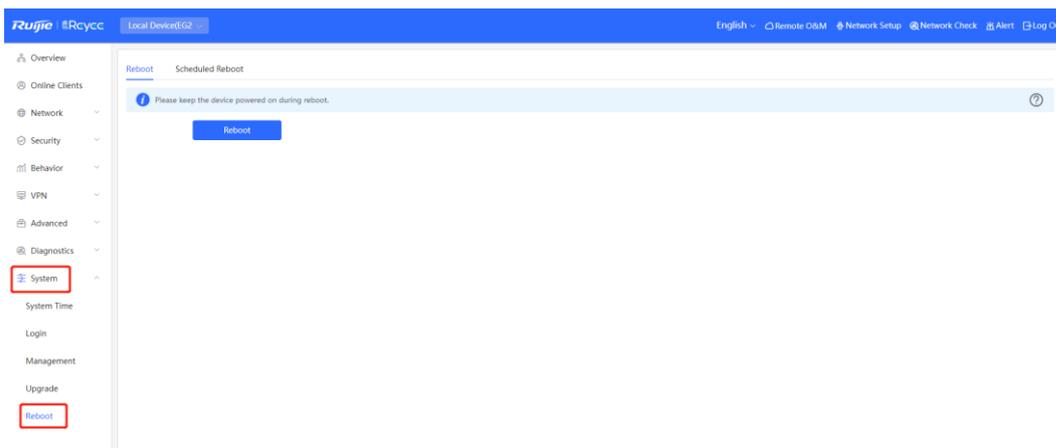
You are advised to restore the settings before importing the configuration. The router will restart automatically if you restore it.

3.6 Configuring Restart

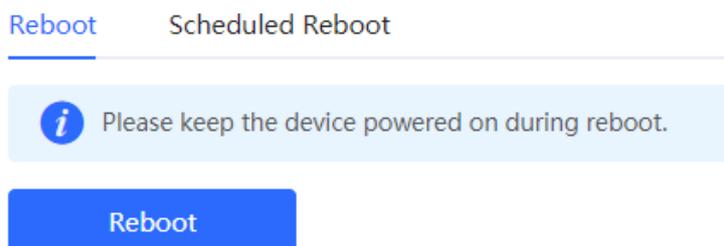
3.6.1 Restarting the Current Device

- Switch to the **Local Device** mode.

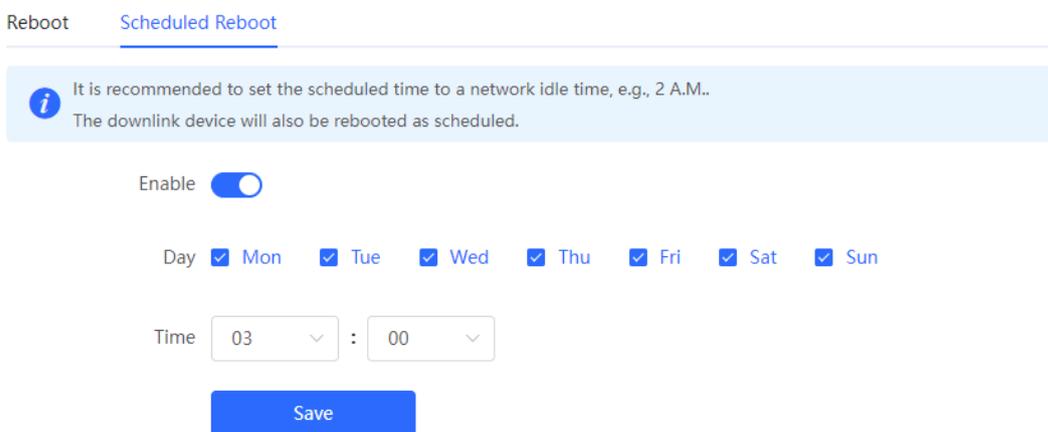
Choose **System > Reboot**.



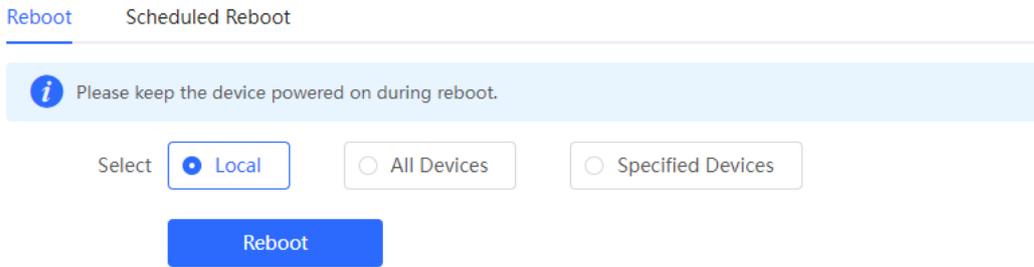
Click **Reboot**. The device will restart immediately. Do not refresh or close the page during restart. After the device restarts, you will be redirected to the login page.



Click **Scheduled Reboot**. Enable this feature and select the scheduled restart time. The device will restart as scheduled.

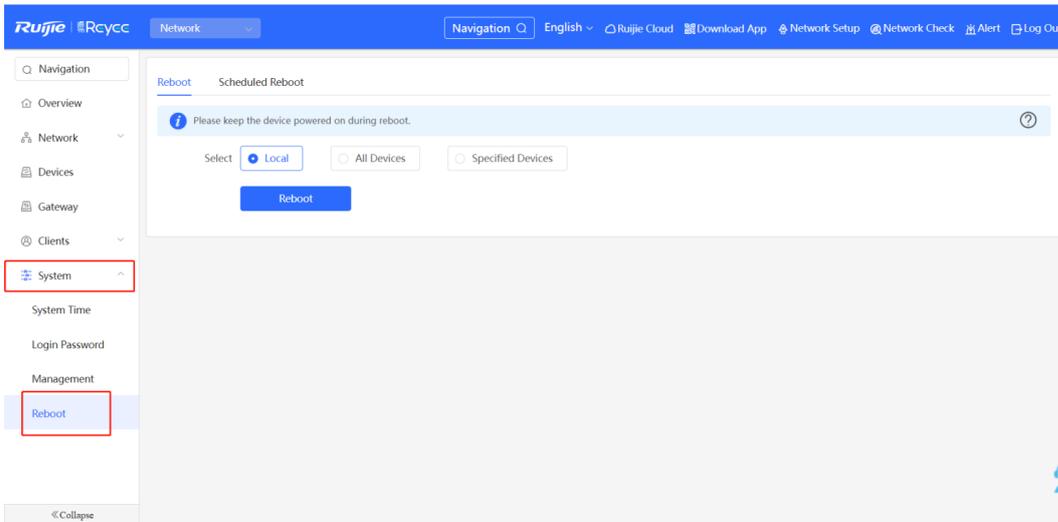


- Switch to the **Network** mode.
 - Choose **System > Reboot > Reboot**. Select **Local** to restart the current device.

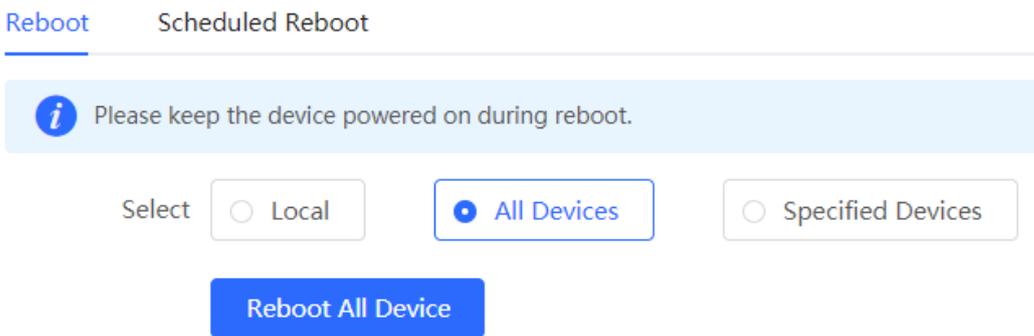


3.6.2 Restarting All Devices on the Network

Switch to the **Network** mode. Choose **System > Reboot > Reboot**.



Select **All Devices**, and click **Reboot All Device** to restart all devices on the network.



Caution

The operation takes some time and affects the entire network. Therefore, exercise caution when performing this operation.

3.6.3 Restarting Specified Devices

Switch to the **Network** mode. Choose **System > Reboot > Reboot**.

Click **Specified Devices**, select required devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** list on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will restart.

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

1234567891234 - EG210G-P

< Delete

Add >

Selected Devices 0/0

Search by SN/Model

No data

Reboot

3.6.4 Configuring Scheduled Restart

Confirm that the system time is accurate to avoid network interruption caused by device restart at an incorrect time point. For details about how to configure the system time, see section [3.3 Setting and Displaying System Time](#).

Choose **System > Reboot > Scheduled Reboot**.

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

Caution

The operation affects the entire network. Therefore, exercise caution when performing this operation.

Reboot Scheduled Reboot

i 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 03 : 00

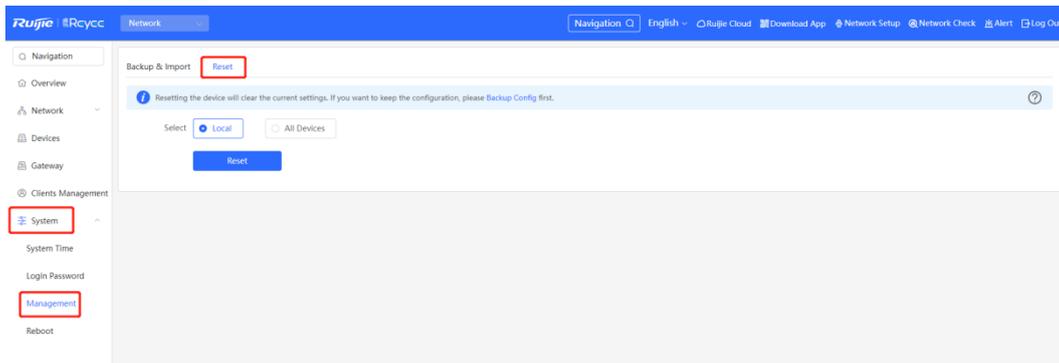
Save

3.7 Restoring Factory Settings

Restore the device to factory settings and the default password.

The operation deletes all current configuration. You are advised to back up the configuration before restoring factory settings.

- (1) Log in to the Eweb of the device.
- (2) Choose **System > Management > Reset**.



- (3) Select the target device.
 - o **Local**: Select **Local**. Only the local device is restored.
 - o **All Devices**: Select **All Devices**. All devices on the network are restored.
- (4) Click **Reset** to restore the selected devices to factory settings.

4 Common Settings

4.1 Network Access Setting

Perform network configuration to connect the router to the Internet quickly.



Three Internet access modes are available:

- PPPoE
- DHCP
- Static IP address

4.1.1 PPPoE Configuration Through a WAN Port

(1) Click **Wizard** to access the configuration wizard page.



Set **Internet** to **PPPoE** in the **Network Settings** pane.

* Network Name

Network Settings

Internet PPPoE DHCP Static IP
Current Settings: DHCP

* Username

* Password

Service Name

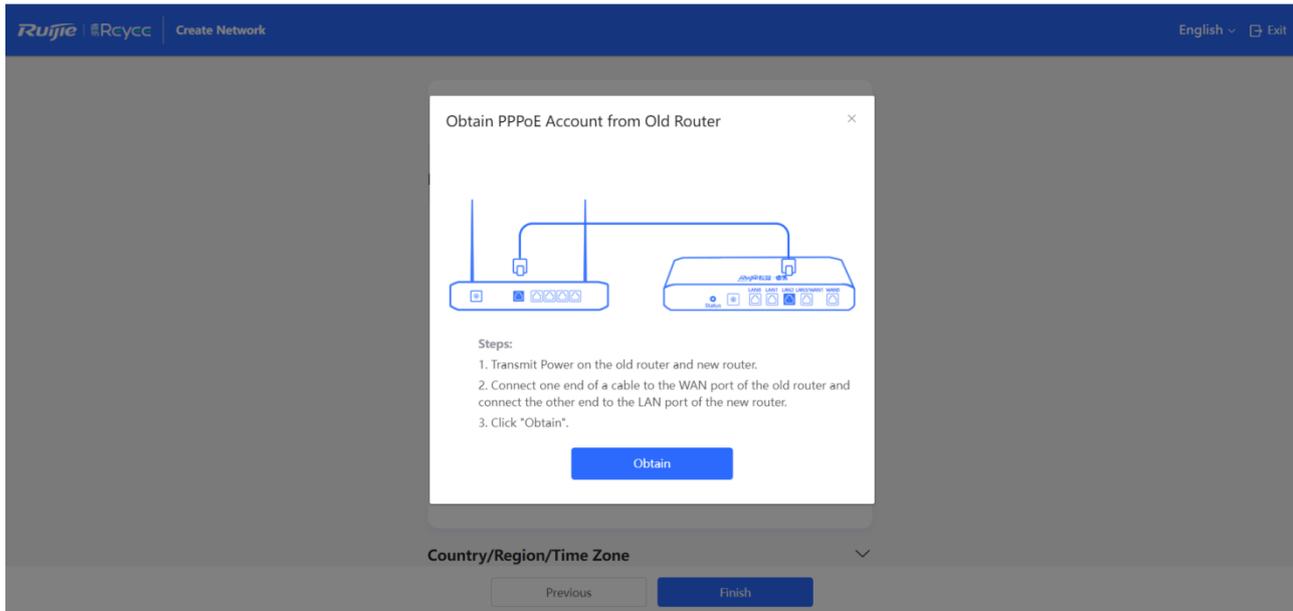
[Forgot Account? Obtain Account from Old Device](#)

Country/Region/Time Zone

* Country/Region

* Time Zone

- (2) Enter your **Username** and **Password** obtained from an ISP. **Service Name** is optional.
- (3) If you forget the password from the ISP, click **Obtain Account from Old Device**.
- (4) Click **Create Network & Connect**. The router initiates a connection with the Internet.
- (5) After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb.



4.1.2 Static IP Address Configuration Through a WAN Port

- (1) Click **Wizard** to access the configuration wizard page.



- (2) Set **Internet** to **Static IP** in the **Network Settings** pane.

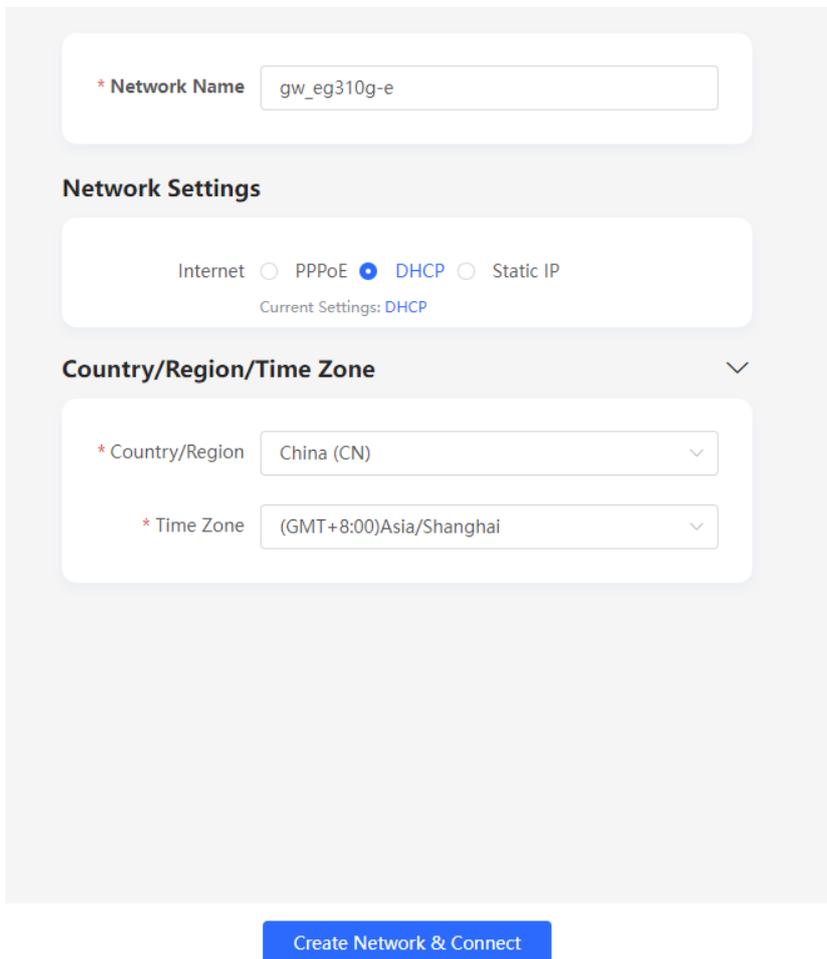
- (3) Configure an IP address, a subnet mask, a gateway IP address, and a DNS server address.
- (4) Click **Create Network & Connect**. The router initiates a connection with the Internet.
- (5) After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb.

4.1.3 DHCP Configuration Through a WAN Port

- (1) Click **Wizard** to access the configuration wizard page.



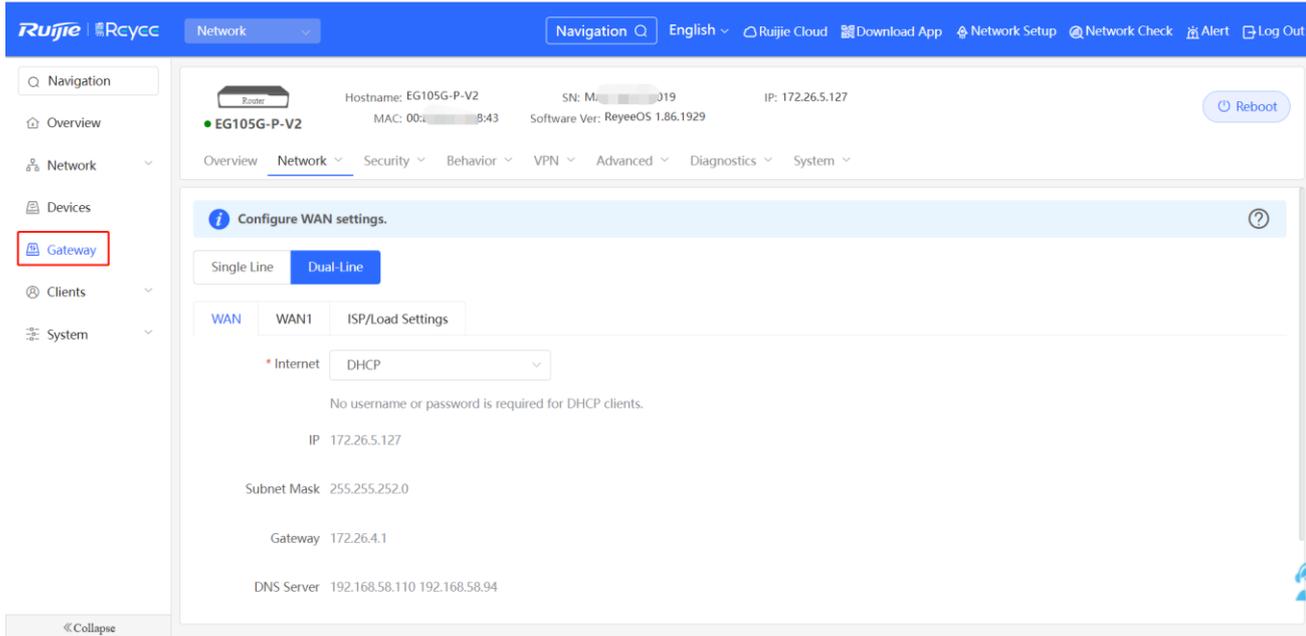
- (2) Set **Internet** to **DHCP** in the **Network Settings** pane.

A screenshot of the DHCP configuration wizard interface. At the top, there is a text input field for '* Network Name' with the value 'gw_eg310g-e'. Below this is the 'Network Settings' section, which contains radio buttons for 'Internet', 'PPPoE', 'DHCP', and 'Static IP'. The 'DHCP' radio button is selected, and the text 'Current Settings: DHCP' is displayed below it. The next section is 'Country/Region/Time Zone', which has a dropdown arrow to its right. It contains two dropdown menus: '* Country/Region' with the value 'China (CN)' and '* Time Zone' with the value '(GMT+8:00)Asia/Shanghai'. At the bottom of the form is a blue button labeled 'Create Network & Connect'.

- (3) Click **Create Network & Connect**. The router initiates a connection with the Internet.

After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb. You can perform WAN configuration through the following page.

Choose **Gateway > Network > WAN**.



4.2 AP Management

Note

- To manage the downlink AP, enable self-organizing network (SON) discovery (see section [错误!未找到引用源。错误!未找到引用源。](#)). The wireless settings are synchronized to all wireless devices on the network by default. You can configure groups to limit the device scope under wireless management. For details, see section 4.2.2 [Configuring AP Groups](#).
- Except the RG-EG105GW and RG-105GW(T), other Reye routers do not send Wi-Fi signals. Wireless settings need to be delivered to make downlink APs take effect.

4.2.1 Switching the Working Mode

1. Working Mode

- Router mode

The device supports routing functions such as route-based forwarding and network address translation (NAT), VPN, and behavior management. It can allocate addresses to downlink devices, forward network data based on routes, and perform NAT operations.

In router mode, the device can access the network through Point-to-Point Protocol over Ethernet (PPPoE) dialing, dynamic IP address, and static IP address. It can also directly connect to a fiber-to-the-home (FTTH) network cable or an uplink device to provide network access and manage downlink devices.

- AC mode

The device supports Layer 2 forwarding only. The device does not provide routing and Dynamic Host Configuration Protocol (DHCP) server functions. By default, a WAN port obtains an IP address through DHCP. The AC mode is applicable to the scenario where the network is working normally. In AC mode, the device serves as the management controller to access the network in bypass mode and manage APs.

2. SON Discovery

When configuring a working mode, you can configure whether to enable the SON discovery function. This function is enabled by default.

After the SON discovery function is enabled, the device can be discovered on a network and discover other devices on the network. Devices interconnect with each other based on the device status and synchronize global configuration. You can log in to the web management page of any device on the network to check information about all devices on 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 SON discovery function is disabled, the device will not be discovered on the network and runs in standalone mode. After logging in to the web page, you can configure and manage only the current login device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the SON discovery function.

Note

In AC mode, the SON discovery function is enabled by default.

After the SON discovery function is enabled, you can view the self-organizing role of the device on the **Device Details** page.

The menus on the web page vary depending on whether the SON discovery function is enabled. For details, see section [1.7 Switching Between Management Pages](#).

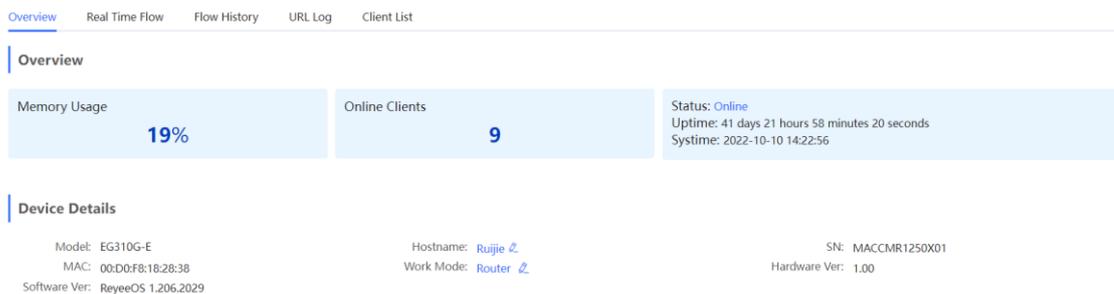
3. Configuration Steps

Choose Overview > Device Details.

Click the current working mode to edit the working mode.

Caution

After you switch the working mode, the device will restore factory settings and restart. Proceed with caution.



The screenshot shows a web interface with a navigation bar at the top containing 'Overview', 'Real Time Flow', 'Flow History', 'URL Log', and 'Client List'. The 'Overview' section is active and displays three key metrics: 'Memory Usage' at 19%, 'Online Clients' at 9, and 'Status: Online' with 'Uptime: 41 days 21 hours 58 minutes 20 seconds' and 'System: 2022-10-10 14:22:56'. Below this is the 'Device Details' section, which lists: Model: EG310G-E, MAC: 00:D0:F8:18:28:38, Software Ver: ReyeeOS 1.206.2029, Hostname: Ruijie, Work Mode: Router, SN: MACCMR1250X01, and Hardware Ver: 1.00.

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

Network

AC ?

Save

4. Viewing the Self-Organizing Role

Choose Local Device > Overview > Device Details.

After the SON discovery function is enabled, you can view the self-organizing role of the device on the Device Details page.

Master AP/AC: The device functions as an AC to manage downlink devices.

Slave AP: The device connects to the AC in self-organizing mode and is managed by the AC. Slave APs are uniformly managed by the master AP or AC. Some wireless network configurations cannot be modified separately in local mode, and must be delivered by the master AP or AC.

Overview

Memory Usage

46%

Online Clients

1

Status: Online

Uptime: 1 hour 6 minutes 16 seconds

System: 2022-04-24 15:03:22

Device Details

Model: EG ██████████

SN: MACCEGWELY01

Work Mode: Router ?

Hardware Ver: 1.00

Hostname: Ruijie ?

MAC: 00:D0:F8:15:79:45

Role: Master AC ?

Software Ver: ReyeOS 1.86.1611

4.2.2 Configuring AP Groups

1. Overview

After SON network discovery is enabled, the device can work as the master AP or AC to batch configure and manage its downlink APs by group. Before you configure APs, assign them to different groups.

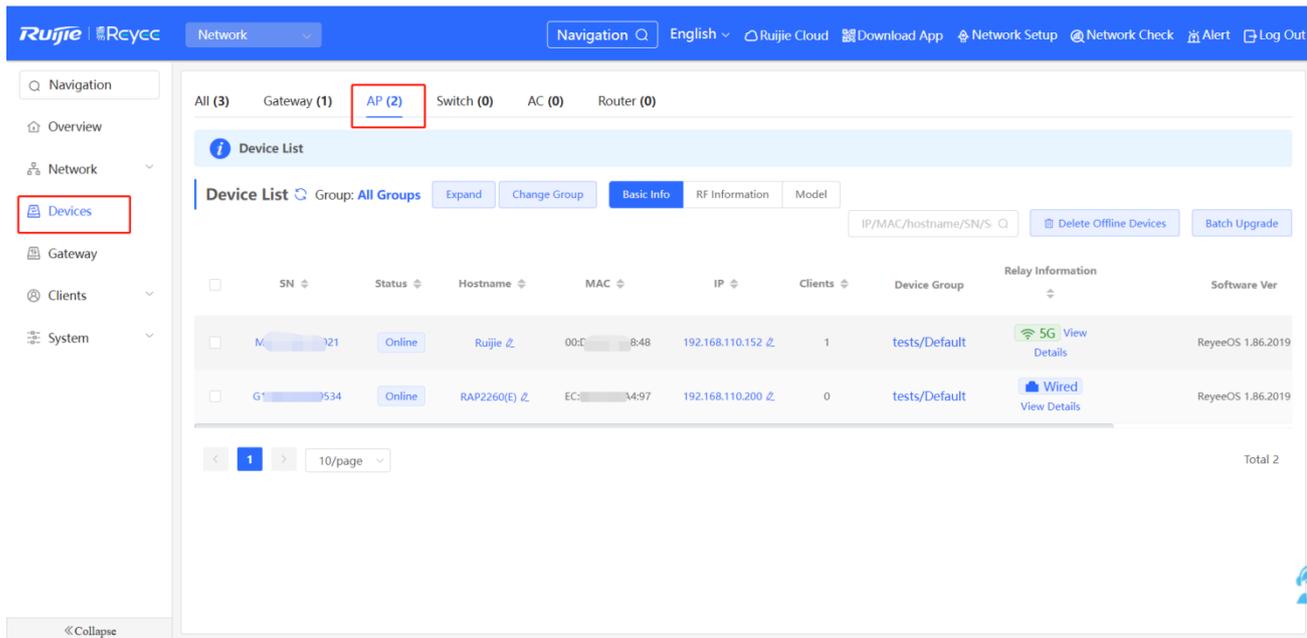
Note

If you specify groups when configuring the wireless network, the configuration takes effect on wireless devices in the specified groups.

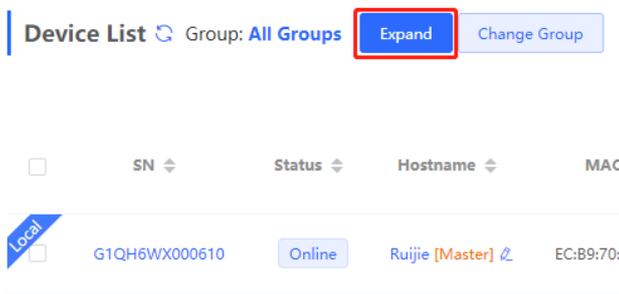
2. Configuration Steps

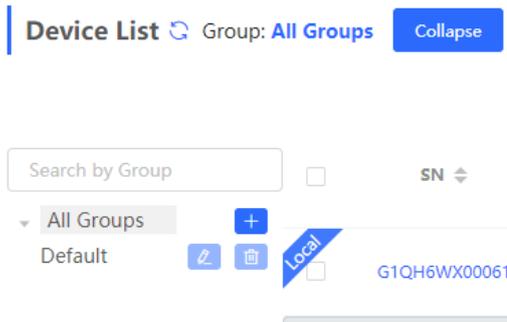
Switch to the **Network** mode. Choose **Devices > AP**.

- (1) View the information of all APs on the current network, including basic information, RF information, and model. Click the SN of an AP to configure the AP separately.

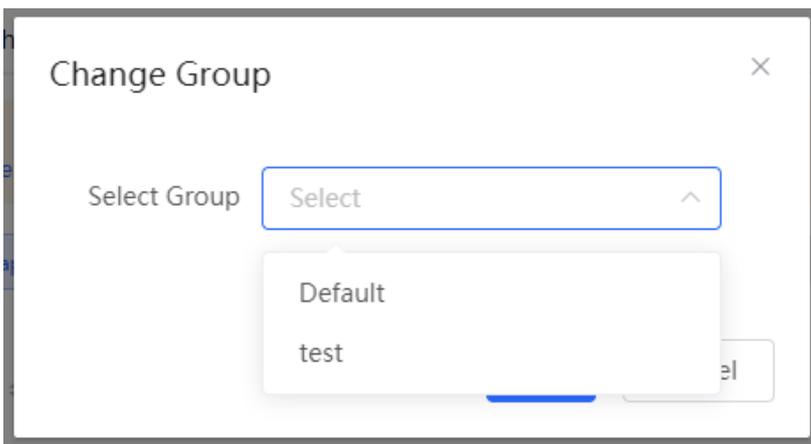
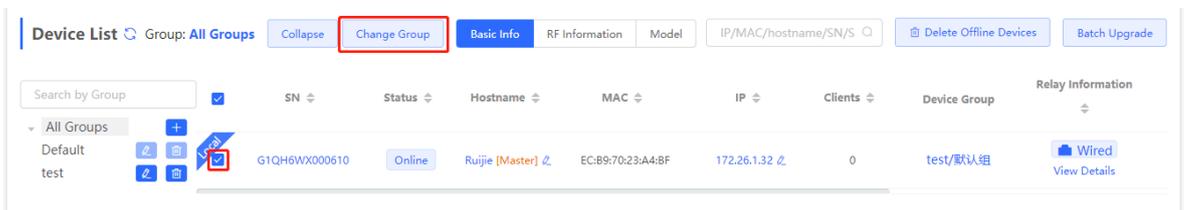


- (2) Click **Expand**. Information about all the current groups is displayed on the left of the list. Click **+** to create a group. You can create a maximum of eight groups. Select the target group and click **✎** to modify the group name or click **🗑** to delete the group. You cannot modify the name of the default group or delete the default group.





- (3) Click a group name in the left. All devices in the group are displayed. One device can belong to only one group. By default, all devices belong to the default group. Select a device from the device list and click **Change Group** to migrate the selected device to the specified group. After a device is moved to the specified group, the device will use the configuration for the new group. Click **Delete Offline Devices** to remove offline devices from the list.



4.2.3 Configuring Wi-Fi

Switch to the **Network** mode. Choose **Network > Wi-Fi > Wi-Fi Settings**.

Enter the SSID and Wi-Fi password, select the frequency band used by the Wi-Fi signal, and click **Save**.

Click **Advanced Settings** to configure Wi-Fi parameters.

 **Caution**

Configuration modification will cause the wireless configuration to be reset, resulting in logout of connected clients. Exercise caution when performing this operation.

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

Wi-Fi Settings Device Group: Default 

* SSID

Band 2.4G + 5G 

Security Open 

[Collapse](#)

Wireless Schedule All Time 

VLAN Default VLAN 

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

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 his IP address unchanged in this Wi-Fi network.)

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

Table 4-1 Wireless Network Configuration

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
SSID Encoding	If the SSID does not contain Chinese, this item will be hidden. If the SSID contains Chinese, this item will be displayed. You can select UTF-8 or GBK.
Band	Set the band used by Wi-Fi signals. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band as needed. The default value is 2.4G + 5G , indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.

Parameter	Description
Security	<p>Select an encryption mode for wireless network connections. The options are as follows:</p> <ul style="list-style-type: none"> ● Open: The device can associate with Wi-Fi without a password. ● WPA-PSK/WPA2-PSK: Wi-Fi Protected Access (WPA) or WPA2 is used for encryption. ● WPA_WPA2-PSK (recommended): WPA2-PSK or WPA-PSK is used for encryption.
Wi-Fi Password	Specify the password for interconnection with the wireless network. The password is a string of 8 to 16 characters.
Wireless Schedule	Specify the period during which Wi-Fi is enabled. When this parameter is set, users can only connect to Wi-Fi during this period.
VLAN	Set the VLAN to which Wi-Fi signals belong. You can select a VLAN from the available VLANs, or click Add New VLAN and go to the LAN Settings page to add a VLAN.
Hide SSID	Enabling SSID hiding can prevent unauthorized users' access to Wi-Fi, improving security. However, mobile phones or computers cannot find the SSID after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current SSID before you enable this function.
Client Isolation	With client isolation enabled, clients associated with Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.
Band Steering	Band steering allows 5G-capable clients to select 5 GHz Wi-Fi preferentially. You can enable this function only when Band is set to 2.4G + 5G .
XPress	XPress enables the device to send game packets preferentially, providing more stable wireless network for games.
Layer-3 Roaming	Layer 3 roaming enables clients to keep their IP addresses unchanged when the clients are associated with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
Wi-Fi6	<p>Wi-Fi 6 provides wireless users with faster network access speed and optimized network access experience.</p> <p>This function is valid only on 802.11ax-capable APs and routers. Clients must also support 802.11ax to experience high-speed network access empowered by Wi-Fi 6. If clients do not support Wi-Fi 6, disable this function.</p>

4.2.4 Configuring Guest Wi-Fi

Switch to the **Network** mode. Choose **Network > Wi-Fi > Guest Wi-Fi**.

Guest Wi-Fi is a wireless network provided for guests, and is disabled by default. Client isolation is enabled for guest Wi-Fi by default, and cannot be disabled. In this case, clients associating with guest Wi-Fi are mutually isolated, and they can only access the Internet through Wi-Fi. This improves network access security. You can configure a wireless schedule for the guest network. After the specified schedule expires, the guest network will become unreachable.

Enable guest Wi-Fi and set the guest SSID and password. Click **Advanced Settings** to configure the wireless schedule of guest Wi-Fi and more Wi-Fi parameters. For details, see section [4.2.2 Configuring Wi-Fi](#). Click **Save**. Guests can access the Internet through Wi-Fi after entering the SSID and password.

Wi-Fi Settings **Guest Wi-Fi** Wi-Fi List Healthy Mode Load Balancing

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

Guest Wi-Fi Device Group:

Enable

* SSID

Band

Security

..... 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 his IP address unchanged in this Wi-Fi network.)

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

4.2.5 Adding More Wi-Fi Networks

Switch to the **Network** mode. Choose **Network > Wi-Fi > Wi-Fi List**, and select the device group which you want to add more Wi-Fi networks.

Click **Add**, enter the SSID and password, and click **OK** to create a Wi-Fi network. Click **Advanced Settings** to configure more Wi-Fi parameters. For details, see section [4.2.2 Configuring Wi-Fi](#). After a Wi-Fi network is added, clients can find this Wi-Fi network, and Wi-Fi information is displayed in the Wi-Fi list.

Wi-Fi Settings Guest Wi-Fi Wi-Fi List Healthy Mode Load Balancing

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

Wi-Fi List Device Group:

Up to 8 SSIDs can be added.

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

Add ×

i The configuration will take effect after being delivered to AP.

* SSID

Band

Security

* Wi-Fi Password

----- Expand -----

4.2.6 Healthy Mode

Switch to the **Network** mode. Choose **Network > Wi-Fi > Healthy Mode**.

Enable the healthy mode and select a wireless schedule for the mode.

After the healthy mode is enabled, the RF transmit power and Wi-Fi coverage range of the device are reduced in the schedule. This may lead to weak signals and network freezing. You are advised to disable the healthy mode or set the wireless schedule to an idle period.

Wi-Fi Settings Guest Wi-Fi Wi-Fi List **Healthy Mode** Load Balancing

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

Healthy Mode Device Group:

Enable

Wireless Schedule

4.2.7 RF Settings

Switch to the **Network** mode. Choose **Network > Radio Frequency**.

The device can detect the surrounding wireless environment upon power-on and select proper configuration. However, network freezing caused by wireless environment changes cannot be prevented. You can analyze the wireless environment around the APs and routers and manually select proper parameters.

⚠ Caution

Configuration modification will cause the wireless configuration to be reset, resulting in logout of connected clients. Exercise caution when performing this operation.

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 32 Client Count Limit 32

Disconnection Threshold Disable -85dBm -50dBm Disconnection Threshold Disable -85dBm -50dBm

Save

Table 4-2 RF Configuration

Parameter	Description
Country/Region	Wi-Fi channels stipulated by each country may be different. To ensure that clients can find Wi-Fi signals, select the country or region where the device is located.
2.4G/5G Channel Width	A lower bandwidth indicates a more stable network, and a higher bandwidth indicates less interference. In case of severe interference, select a low bandwidth to prevent network freezing to a certain extent. The 2.4 GHz band supports 20 MHz and 40 MHz bandwidths. The 5 GHz band supports 20 MHz, 40 MHz, and 80 MHz bandwidths. By default, the value is Auto , indicating that the bandwidth is selected automatically based on the environment.

Parameter	Description
Client Count Limit	If a large number of users are connected to an AP or a router, the wireless network performance of the AP or router may be degraded, affecting users' Internet access experience. When this parameter is set and the number of access users reaches the specified value, the AP or router rejects access of new users. If clients require high bandwidth, you can adjust this parameter to a smaller value. You are advised to keep the default value unless otherwise specified.
Disconnection Threshold	When multiple Wi-Fi signals are available, you can set this parameter to optimize the wireless signal quality. When a client is far away from the wireless device and the wireless signal strength of the end user is lower than this value, the Wi-Fi connection is ended. In this case, the client has to select a nearer wireless signal. The client is prone to be disconnected if this value is high. To ensure that the client can normally access the Internet, you are advised to set this parameter to Disable or a value smaller than -75 dBm.

 **Note**

- Available wireless channels depend on the country or region code. Select the country or region code based on the country or region of your device.
 - The channel, transmit power, and roaming sensitivity cannot be set globally. You must configure these parameters on devices separately.
-

4.2.8 Configuring a Wi-Fi Blacklist or Whitelist

1. Overview

You can configure the global or SSID-based blacklist and whitelist. MAC addresses can be exactly matched or based on the OUI.

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

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

 **Caution**

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

2. Configuring a Global Blacklist or Whitelist

Switch to the Network mode. Choose Clients Management > Blacklist/Whitelist > Global Blacklist/Whitelist.

Select the blacklist or whitelist mode and click Add to add a client to the blacklist or whitelist. In the Add dialog box, enter the MAC address and remarks of the target client and click OK. If a client is already associated with the router, its MAC address appears automatically. Click the MAC address for automatic input. All clients

in the blacklist are forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the router.

Global Blacklist/Whitelist SSID-Based Blacklist/Whitelist

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

Blocked WLAN Clients + Add Delete Selected

Up to 64 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	AE:4E:11 OUI		Edit Delete
<input type="checkbox"/>	11:22:33:44:55:66		Edit Delete

Add ×

Match Type Full Prefix (OUI)

* MAC

Remark

Cancel OK

If you delete a client from the blacklist, the client is allowed to connect to the Wi-Fi network. If you delete a client from the whitelist, the client is forced offline and not allowed to access the Wi-Fi network.

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

Blocked WLAN Clients + Add Delete Selected

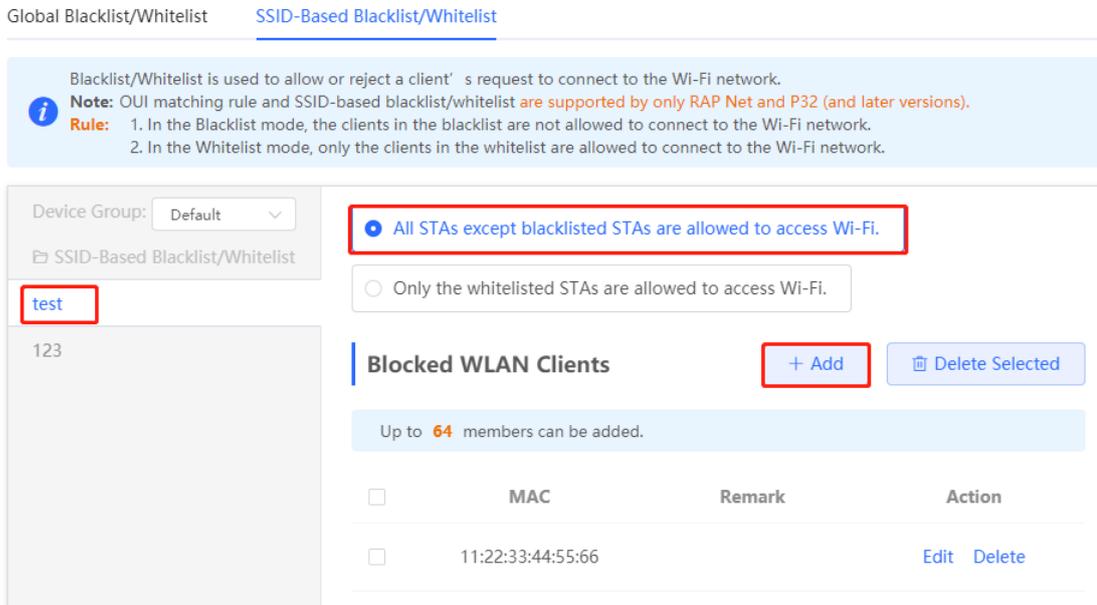
Up to 64 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	AE:4E:11 OUI		Edit Delete
<input type="checkbox"/>	11:22:33:44:55:66		Edit Delete

3. Configuring an SSID-based Blacklist or Whitelist

Switch to the Network mode. Choose Clients Management > Blacklist/Whitelist > SSID-Based Blacklist/Whitelist.

Select a target Wi-Fi network from the left column, select the blacklist or whitelist mode, and click Add to add a client to the blacklist or whitelist. The SSID-based blacklist or whitelist restricts the client's access to the specified Wi-Fi network.



4.2.9 Configuring AP Load Balancing

1. Overview

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

- o **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 of the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.
- o **Traffic Load Balancing:** The load is balanced according to traffic on the APs. When the traffic on an AP is heavy and the traffic difference of 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 five clients and AP2 is associated with two clients, triggering load balancing. New clients' attempt to associate with AP1 will be denied, so they can associate only with AP2.

When a client request is denied by an AP and fails to associate with another AP in the group, the client will keep trying to associate with this AP. If the number of client attempts reaches the specified value, the AP will allow this client, ensuring that the client can normally access the Internet.

2. Configuring Client Load Balancing

Switch to the **Network** mode. Choose **Network > 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.

<input type="checkbox"/>	Group Name	Type	Rule	Members	Action
No Data					

Add

×

* Group Name

* Type

* Rule 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 4-3 Client Load Balancing Configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select Client Load Balancing.

Parameter	Description
Rule	<p>Configure a detailed load balancing rule, including the maximum number of clients allowed to associate with an AP, difference between the currently associated client count and client count on the AP with the lightest load, and number of attempts to access the AP with a full load.</p> <p>By default, when an AP is associated with three 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's association is denied by an AP for 10 times, the client will be allowed to associate with the AP upon the next attempt.</p>
Members	Specify the APs to be added to the AP load balancing group.

3. Configuring Traffic Load Balancing

Switch to the **Network** mode. Choose **Network > 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**.

Wi-Fi Settings Guest Wi-Fi Wi-Fi List Healthy Mode Load Balancing

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.

<input type="checkbox"/>	Group Name	Type	Rule	Members	Action
No Data					

Add×

* Group Name

* Type

* 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

Table 4-4 Traffic Load Balancing Configuration

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

4.2.10 Wireless Network Optimization in One-Click Mode

Switch to the **Network** mode. Choose **Network > WIO**.

On the **Network Optimization** tab, select **I have read the notes** and click **Network Optimization** to perform automatic wireless network optimization in the networking environment. You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to daybreak or an idle period.

Caution

Clients may be disconnected during optimization and the configuration cannot be rolled back after optimization starts. Exercise caution when performing this operation.

Network Optimization Optimization Record

Start Scanning Optimizing Finish

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

Notes:
1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization at night.
2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.
3. The configuration cannot be rolled back once optimization starts.

I have read the notes.

Network Optimization

Scheduled Optimization

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

Enable

Day Sun

Time 03 : 00

Save

After optimization starts, wait for a while until optimization is complete. After optimization ends, click **Cancel Optimization** to restore optimized RF parameters to default values.

Click **View Details** or the **Optimization Record** tab to view the latest optimization record details.

Start Scanning Optimizing Finish

Finish

Optimization finished on 20...
Time: 31 seconds

[View Details](#) [Back](#) [Cancel Optimization](#)

Network Optimization [Optimization Record](#)

Last Optimized: 2022-04-26 15:26:22
You have optimized 1 APs and improved the performance by 12.50%!

[Overview](#) [Details](#)

Hostname	Band	SN	Channel (Before/After)	Channel Width (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)	CCI (Before/After)	ACI (Before/After)	Interference (Before/After)
Ruijie	2.4G	G1QH6WX000 610	1	20	auto/100	80/0	0	0	0
Ruijie	5G	G1QH6WX000 610	36	80	auto/100	78/0	0	0	0

4.2.11 Enabling Reye Mesh

Switch to the **Network** mode. Choose **Network > Reye Mesh**.

Ruijie Rcycc Network

Navigation English Ruijie Cloud Download App Network Set

Navigation

DHCP Snooping

WIO

Radio Frequency

Reye Mesh

LAN Ports

LED

Alerts

Batch Config

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

Enable

[Save](#)

After Reye mesh is enabled, you can set up a mesh network through mesh pairing between the devices that support Reye 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. Reye mesh is enabled on the device by default with firmware ReyeOS 1.86 or later.

Perform the following steps to set up a mesh network:

- (1) Connect the first router to the network and configure it as the primary device.
- (2) Place the second router 2 m (6.56 ft) away from the first router. Power on the second router.
- (3) The system status LED of the second router blinks for 2 to 3 minutes. When the system status LED is solid on, the second router is started up.

- (4) Press the **MESH** button on the first router to perform mesh pairing automatically.

The MESH LEDs on both routers are blinking for about 2 minutes. When the MESH LEDs stop blinking and turn solid white, mesh pairing succeeds.

- (5) Place the second router where you want to have Wi-Fi coverage and then power on the router.

Wait for 3 to 5 minutes until the MESH LED turns solid on. Mesh networking succeeds and you can access the Internet by connecting to the new Wi-Fi network.

Note

- Make sure that the new router is around the primary router and there are fewer obstacles between them.
- If three or more routers are added for mesh networking, repeat step 2 to 4. You can add eight devices in a batch at one time.

4.2.12 Configuring a LAN Port of a Downlink AP

Caution

The configuration takes effect only for a downlink AP with a wired LAN port.

Switch to the **Network** mode. Choose **Network > LAN Ports**.

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"/>	2	Ruijie	Edit Delete

In the **Default Settings** pane, enter the VLAN ID and click **Save** to configure the VLAN to which the AP's LAN port belongs. If the VLAN ID is empty, the LAN port and WAN port belong to the same VLAN.

Click **Add** to add the AP's wired port. Enter a VLAN ID and select an AP.

Add ×

VLAN ID ?

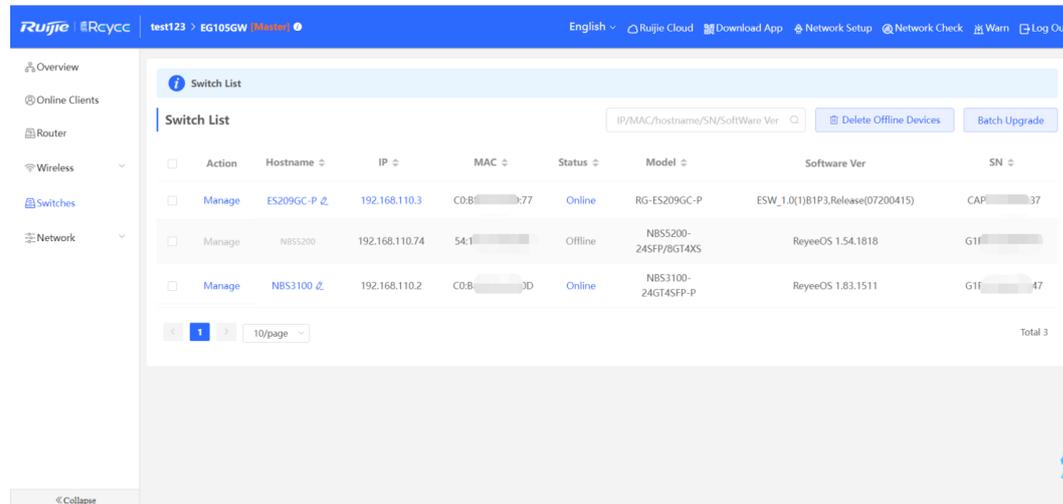
* Applied to ▼

In SON mode, the configuration of AP's wired port applies to all APs that have wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially.

For APs, if no configuration is applied in **LAN Port Settings**, the default configuration of the AP's wired port will take effect.

4.3 Switch Settings

Switch List includes all switches that are managed by the router. The information includes the switch's host name, IP address, MAC address, status, model, software version, and SN. You can check AP categories by clicking .

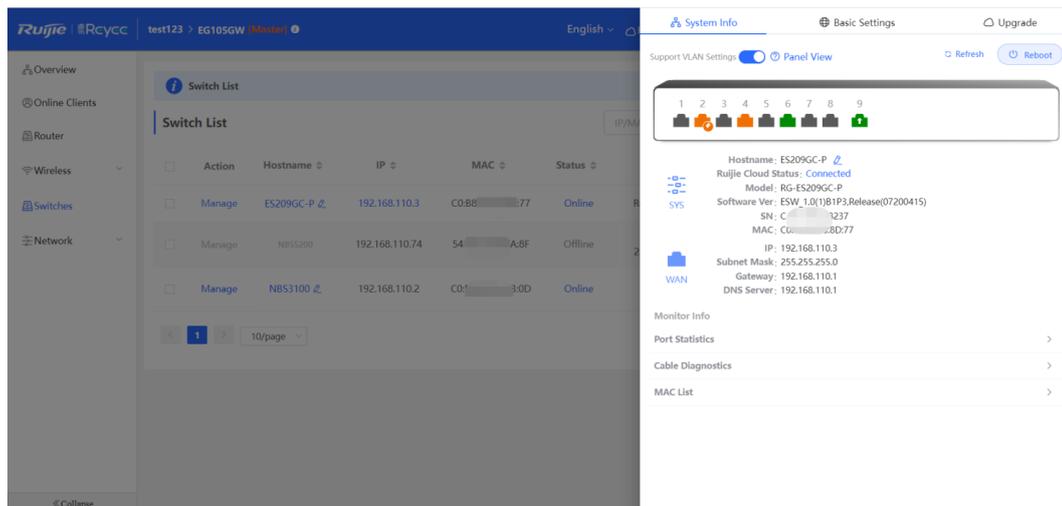


The screenshot shows the Ruijie RCloud interface with the 'Switch List' page. The table contains the following data:

Action	Hostname	IP	MAC	Status	Model	Software Ver	SN
Manage	ES209GC-P	192.168.110.3	CO:88:00:00:00:77	Online	RG-ES209GC-P	ESW_1.0(1)B1P3.Release(07200415)	CAF:00:00:00:00:37
Manage	NBS5200	192.168.110.74	54:10:00:00:00:A8F	Offline	NBS5200-24SFP/8GT4XS	ReyeeOS 1.54.1818	G1F:00:00:00:00:47
Manage	NBS3100	192.168.110.2	CO:88:00:00:00:3D	Online	NBS3100-24GT4SFP-P	ReyeeOS 1.83.1511	G1F:00:00:00:00:47

Navigation: Page 1 of 1, 10/page, Total 3.

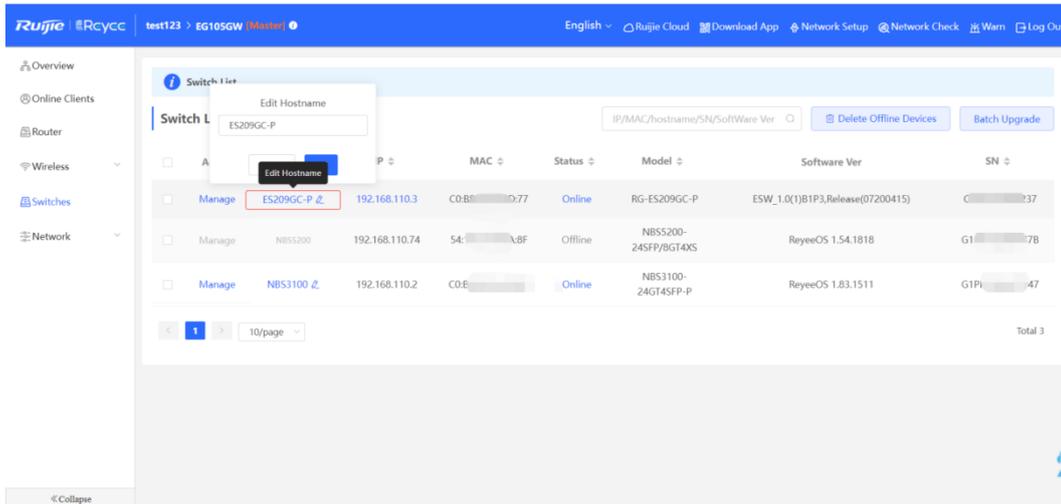
- **Manage:** Go to the detailed configuration page of the switch.



The screenshot shows the detailed configuration page for a switch. The 'System Info' tab is active, displaying the following information:

- Support VLAN Settings: Panel View
- Refresh
- Reboot
- Port Status: 1 (Online), 2 (Online), 3 (Online), 4 (Online), 5 (Online), 6 (Online), 7 (Online), 8 (Online), 9 (Online)
- Hostname: [ES209GC-P](#)
- Ruijie Cloud Status: [Connected](#)
- Model: [RG-ES209GC-P](#)
- Software Ver: [ESW_1.0\(1\)B1P3.Release\(07200415\)](#)
- SN: [C0:88:00:00:00:3237](#)
- MAC: [C0:88:00:00:00:77](#)
- IP: [192.168.110.3](#)
- Subnet Mask: [255.255.255.0](#)
- Gateway: [192.168.110.1](#)
- DNS Server: [192.168.110.1](#)
- Monitor Info: [Monitor Info](#)
- Port Statistics: [Port Statistics](#)
- Cable Diagnostics: [Cable Diagnostics](#)
- MAC List: [MAC List](#)

- **Edit Hostname:** Modify the host name of switch.

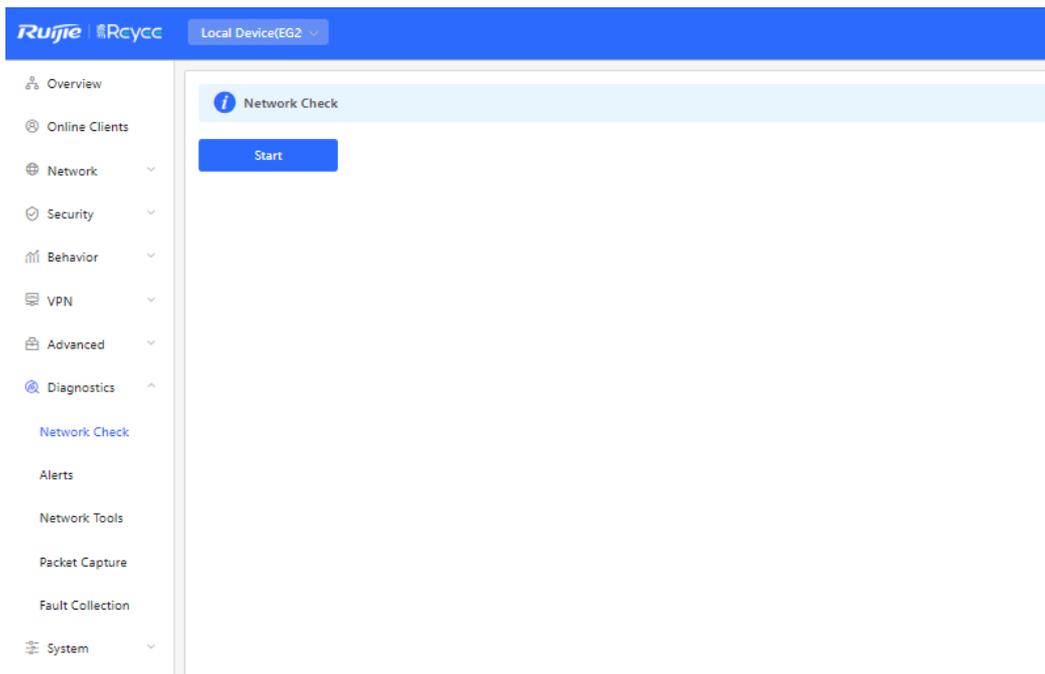


4.4 Diagnostics

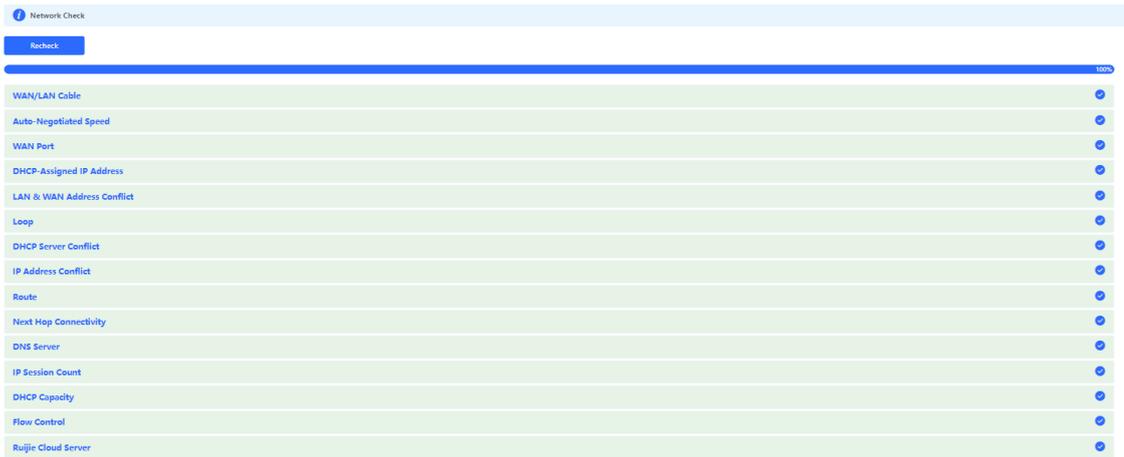
4.4.1 Network Check

You can check your network and resolve the problem on this page.

- (1) Switch to the **Local** mode. Choose **Diagnostics > Network Check**. Click **Start** and click **OK** in the displayed dialog box to start checking the network status.



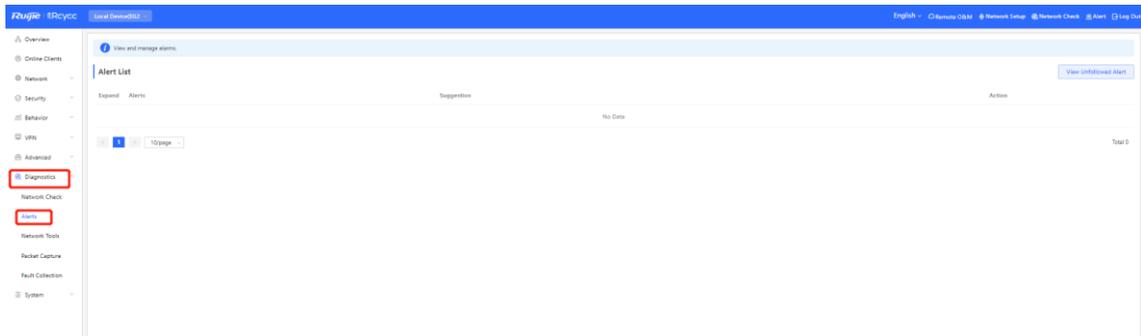
- (2) The result is displayed after network check finishes.



4.4.2 Alarms

The **Alerts** page allows you to query and manage alarms.

- (1) Switch to the **Local** mode. Choose **Diagnostics > Alert**.



- (2) The **Alert List** page displays possible problems on the network environment and device.

All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarms.

Caution

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



- (3) Click **View Unfollowed Alert** 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

4.4.3 Network Tools

Switch to the **Local** mode. Choose **Diagnostics > Network Tools**.

 **Network Tools**


Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* Ping Count

* Packet Size Bytes

```

PING 172.26.1.1 (172.26.1.1): 64 data bytes
72 bytes from 172.26.1.1: seq=0 ttl=64 time=4.675 ms
72 bytes from 172.26.1.1: seq=1 ttl=64 time=2.199 ms
72 bytes from 172.26.1.1: seq=2 ttl=64 time=2.202 ms
72 bytes from 172.26.1.1: seq=3 ttl=64 time=2.212 ms

--- 172.26.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.199/2.822/4.675 ms

```

Select a diagnostic method, enter an IP address or URL, and click **Start**.

- The ping method is used to test the connectivity between the tested device and the specified IP address or URL. If the ping operation fails, the IP address or URL fails to be pinged from the device.
- The traceroute method is used to trace network paths to the specified IP address or URL.
- The DNS lookup method is used to check the DNS server address for URL parsing.

1. Ping Tool

Set **IP Address/Domain**, **Ping Count**, and **Packet Size** on this page, and click **Start**. The ping result will be displayed.

Network Tools

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* Ping Count

* Packet Size

```
PING 8.8.8.8 (8.8.8.8): 64 data bytes
72 bytes from 8.8.8.8: seq=0 ttl=112 time=42.277 ms
72 bytes from 8.8.8.8: seq=1 ttl=112 time=43.100 ms
72 bytes from 8.8.8.8: seq=2 ttl=112 time=43.862 ms
72 bytes from 8.8.8.8: seq=3 ttl=112 time=41.880 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 41.880/42.779/43.862 ms
```

2. Traceroute Tool

Set **IP Address/Domain** and **Max TTL** on this page, and click **Start**. The traceroute result will be displayed.

i Network Tools

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* Max TTL

```
traceroute to 172.26.4.1 (172.26.4.1), 20 hops max, 38 byte packets
 1 172.26.4.1 (172.26.4.1) 1.860 ms 1.624 ms 1.868 ms
```

3. DNS Lookup Tool

This tool is used to resolve the domain name to an IP address.

i Network Tools

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

```
Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

Name: www.google.com
Address 1: 2001::6ca0:a7a7
Address 2: 128.242.240.20
```

4.4.4 Packet Obtaining

Switch to the **Local** mode. Choose **Diagnostics > Packet Capture**.

If the device fails and troubleshooting is required, the packet obtaining result can be analyzed to locate and rectify the fault.

Configure an interface and a protocol, and specify the host IP address to obtain the content in data packets. Select the file size limit and packet count limit to determine the conditions for automatically stopping packet obtaining. If the file size or number of packets reaches the specified threshold, packet obtaining stops and a diagnostic package download link is generated. Click **Start** to execute the packet obtaining command.

 **Caution**

The packet obtaining operation may occupy many system resources, causing network freezing. Therefore, exercise caution when performing this operation.

 **Packet Capture** 

Interface

Protocol

IP Address

File Size Limit Available Memory **177.63 M**

Packet Count Limit

Packet obtaining can be stopped at any time. Then a download link is generated. Click this link to save the packet obtaining result in the PCAP format locally. Use analysis software such as Wireshark to view and analyze the result.

Packet Capture
?

Interface

Protocol

IP Address

File Size Limit Available Memory **177.63 M**

Packet Count Limit

File Size: **78.02K**
 Captured on: **2022-04-27 12:50:07**

PCAP file [Click to download the PCAP file.](#) i

[Click to delete the file.](#)

Start
Stop

- **Interface:** Obtain packets passing through this interface.
- **Protocol:** Obtain packets of this protocol.
- **IP Address:** Obtain packets of this IP address
- **File Size Limit:** Limit the size of a packet.
- **Packet Count Limit:** Limit the packet count. When the packet count reaches the limit, packet obtaining will stop and a download link will be generated.

4.4.5 Fault Collection

Switch to the **Local** mode. Choose **Diagnostics > Fault Collection**.

When the device fails, you need to collect fault information. Click **Start**. Configuration files of the device are packaged into a compressed file. Download the compressed file locally and provide it to R&D personnel for fault locating.

i

Fault Collection

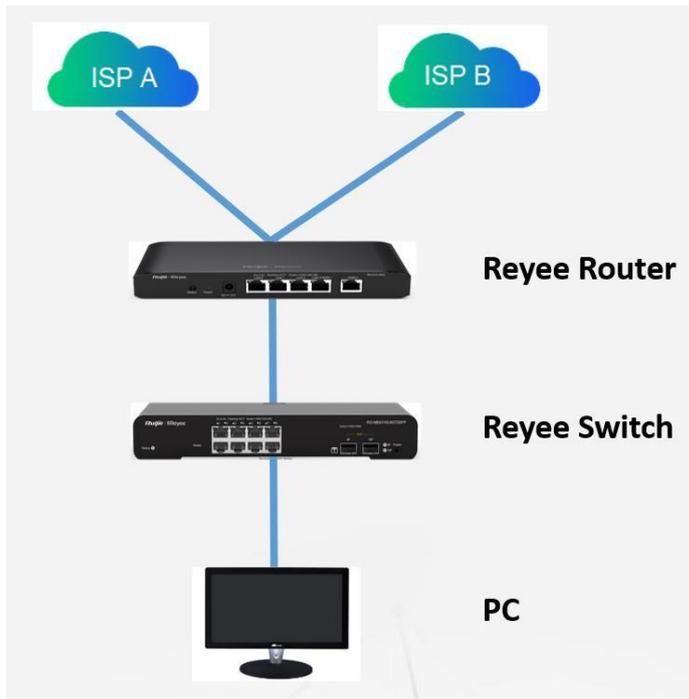
Compress the configuration file for engineers to identify fault.

Start

Compress the configuration file for engineers to identify faults.

4.5 WAN Load Balancing

If there is more than one WAN port, some traffic is routed over the ISP route, and the remaining traffic is balanced according to the load mode.



Prepare two uplink cables for Internet access before configuration.

(1) Switch to the **Local** mode. Choose **Network > WAN**.

The screenshot shows the Ruijie Rcycc web interface. The top navigation bar includes the Ruijie logo, 'Rcycc', and the device identifier 'gw_eg310g-e > Ruijie'. A left sidebar contains a menu with items: Overview, Online Clients, Network (expanded), WAN (selected), LAN, IPv6 Address, Port VLAN, Port Settings, IPTV, Security, Behavior, VPN, Advanced, Diagnostics, and System. The main content area is titled 'WAN' and has tabs for 'network.lines', 'Three Lines', and 'Four Lines'. Under 'network.lines', there are sub-tabs for 'WAN0', 'WAN1', and 'ISP/Load Settings'. The 'WAN1' tab is active, showing configuration for 'Internet' set to 'PPPoE'. Fields include 'Username' (13559163002), 'Password' (masked), and 'Service Name' (Optional) Provided by ISP. A green status message indicates 'PPPoE connection succeeded. View PPPoE Records'. Below this, IP address (100.62.90.190), Subnet Mask (255.255.255.255), Gateway (100.68.128.1), and DNS Server (211.138.151.161, 211.138.156.66) are displayed. A dashed line separates the main settings from 'Advanced Settings'. A blue 'Save' button is at the bottom.

(2) Configure **WAN** accordingly.

WAN0
WAN1
ISP/Load Settings

* Internet PPPoE

* Username 13559163002

[Forgot Account? Obtain Account from Old Device](#)

* Password ***** 👁

Service Name (Optional) Provided by ISP

✔ **PPPoE connection succeeded.** [View PPPoE Records](#)

IP 100.62.90.190

Subnet Mask 255.255.255.255

Gateway 100.68.128.1

DNS Server 211.138.151.161 211.138.156.66

----- [Advanced Settings](#) -----

Save

(3) Select **ISP/Load Settings**, and configure the load mode and interface weight.

WAN0
WAN1
ISP/Load Settings

Load Balancing Settings

Traffic will be routed based on ISP settings preferentially. The remaining traffic will be managed according to load mode.

1. **Balanced mode:** The traffic will be spread across multiple links according to the weight of each WAN port. For example, if WAN and WAN1 weight are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN1.

2. **Primary & secondary mode:** All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface. If there are multiple primary and secondary interfaces, please configure their weight (See balanced mode).

Load Mode Primary & Secondary

Balancing Policy Based on Src and Dest IP Address

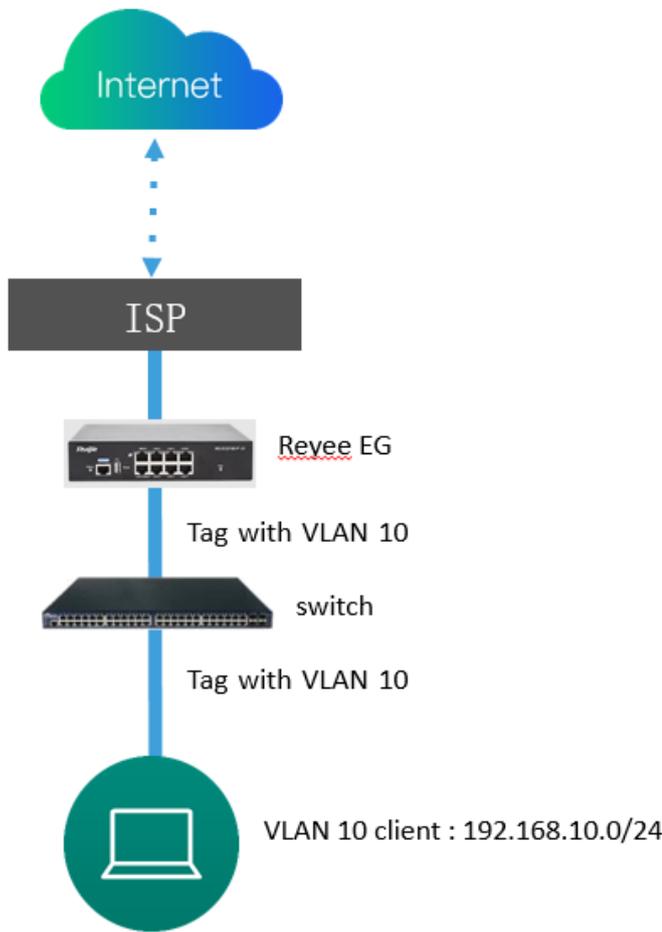
WAN Set as Prim * Weight 1

WAN1 Set as Secc * Weight 1

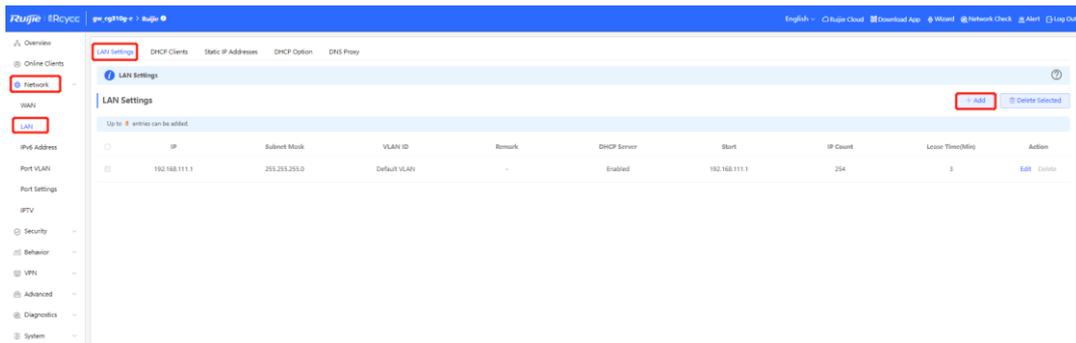
Save

- **Balanced mode:** Traffic will be transmitted across multiple links according to the weight of each WAN port. For example, if weights of **WAN** and **WAN1** are set to 3 and 2 respectively, 60% of the total traffic will be routed over **WAN** and 40% over **WAN1**.
- **Primary & secondary mode:** All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface. If there are multiple primary and secondary interfaces, configure the weights.

4.6 Port VLAN



(1) Switch to the **Local** mode. Choose **Network > LAN** to create a VLAN first.



Add ×

* IP

* Subnet Mask

* VLAN ID

Remark

MAC

DHCP Server

* Start

* IP Count

* Lease Time(Min)

DNS Server - ?

After you configure a LAN successfully, it is displayed in **LAN Settings**.

<input type="checkbox"/>	192.168.10.1	255.255.255.0	10	-	Enabled	192.168.10.1	254	30	Edit	Delete
--------------------------	--------------	---------------	----	---	---------	--------------	-----	----	----------------------	------------------------

(2) Choose **Network > Port VLAN to tag VLAN**. By default, the tagged mode is used for VLANs.

Port VLAN

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

	LAN0	LAN1/WAN3	LAN2/WAN2	LAN3/WAN1
Default VLAN	UNTAG	UNTAG	UNTAG	UNTAG
VLAN 11	TAG	TAG	TAG	TAG
VLAN 12	TAG	TAG	TAG	TAG
VLAN 13 11111	TAG	TAG	TAG	TAG

- o **UNTAG**: If VLAN 10 is set to **UNTAG** on port 2, VLAN 10 will be the native VLAN of port 2. Packets from VLAN 10 are forwarded through port 2 without being tagged with VLAN 10 and all untagged packets on

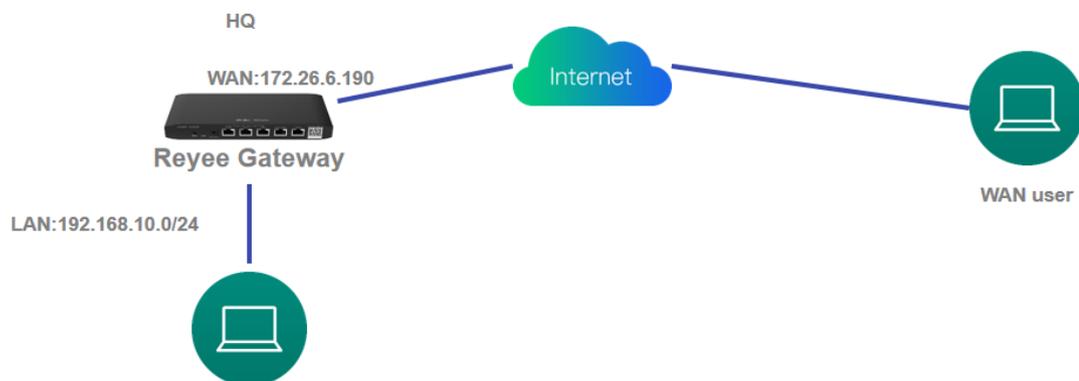
port 2 are considered as the packets from VLAN 10.

- Each port can be configured with only one untagged VLAN.
- The native VLAN of port 1 is the default VLAN and cannot be edited.
- **TAG**: If both VLAN 10 and VLAN 20 are set to **TAG** on port 2, packets from VLAN 10 and VLAN 20 are forwarded through port 2.
- **Not Join**: If both VLAN 10 and VLAN 20 are set to **Not Join** on port 2, port 2 will not receive or transmit packets from VLAN 10 or VLAN 20.

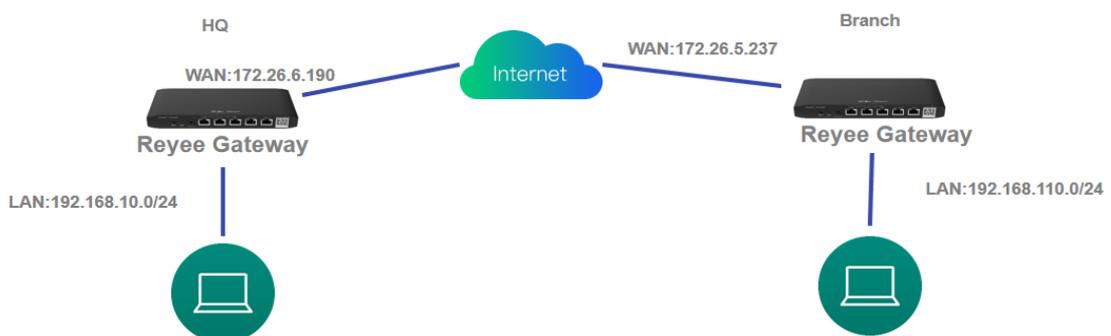
4.7 VPN

Application Scenario

- Client-to-Site Scenario



- Site-to-Site Scenario



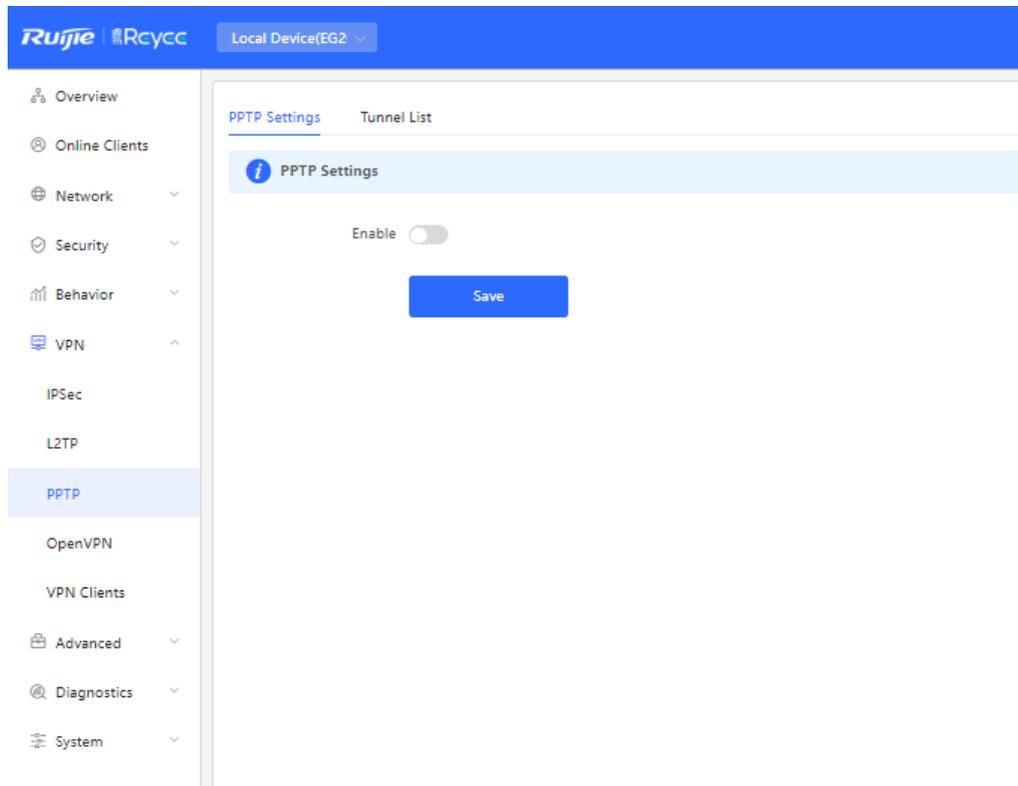
4.7.1 PPTP VPN

PPTP VPN is typically used in client-to-site and site-to-site scenarios. For example, clients work from home and need to access company servers through PPTP VPN tunnels; a company has three branches that are distributed in three different places, and each branch needs to establish a tunnel with each other through a router.

1. Client-to-Site Scenario Configuration

(1) Headquarters side:

- a Log in to the Reyee EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN > PPTP** and enable PPTP.



- c Perform PPTP configuration and click **Save**.

PPTP Settings Tunnel List

PPTP Settings

Enable

PPTP Type Server Client

* Local Tunnel IP

* IP Range ?

* DNS Server

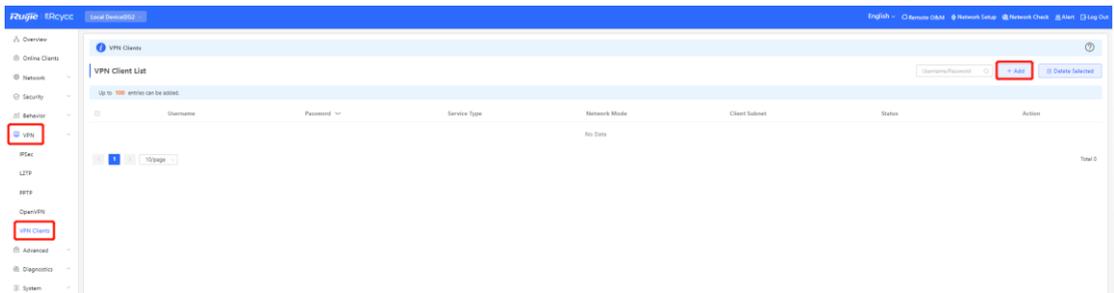
MPPE Disable Enable

Flow Control Disable Enable

* PPP Hello Interval

Save

d Choose **Network > VPN Clients** and configure VPN clients.



Add User ×

Service Type

* Username

* Password

Network Mode

Status

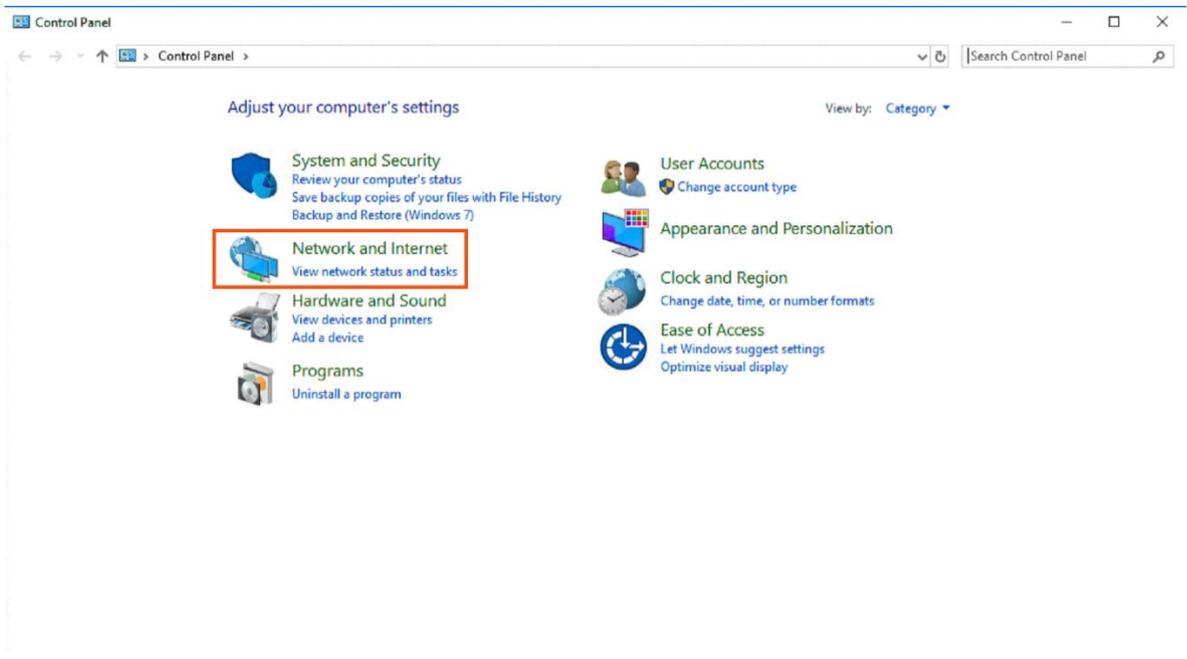
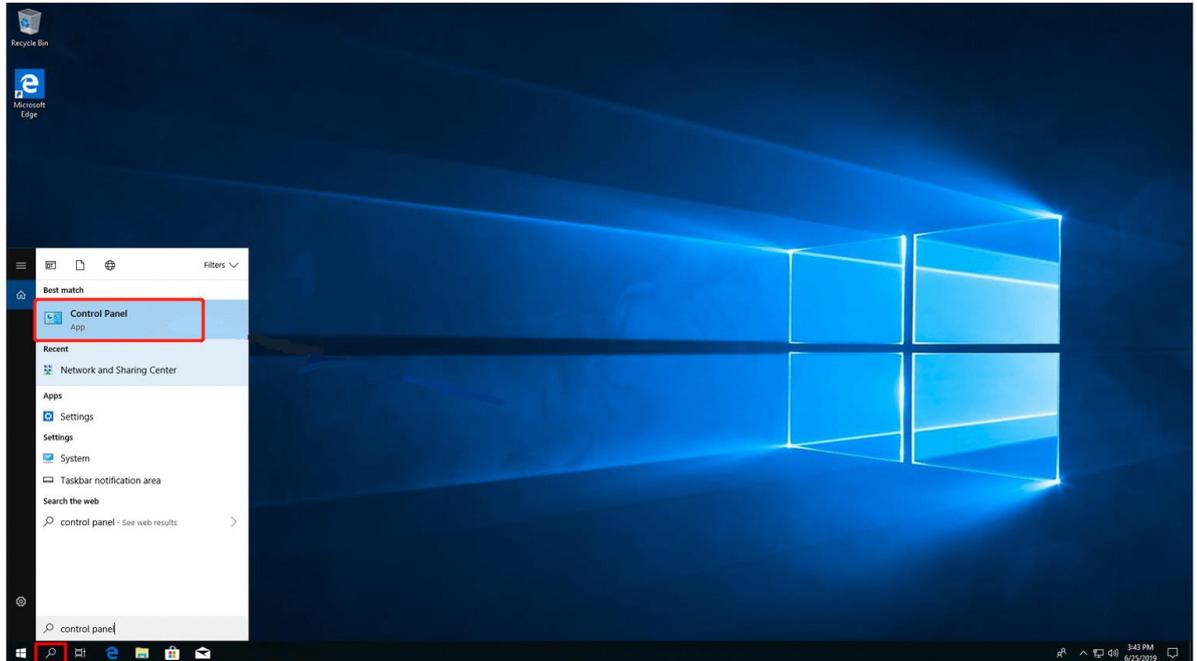
Cancel **OK**

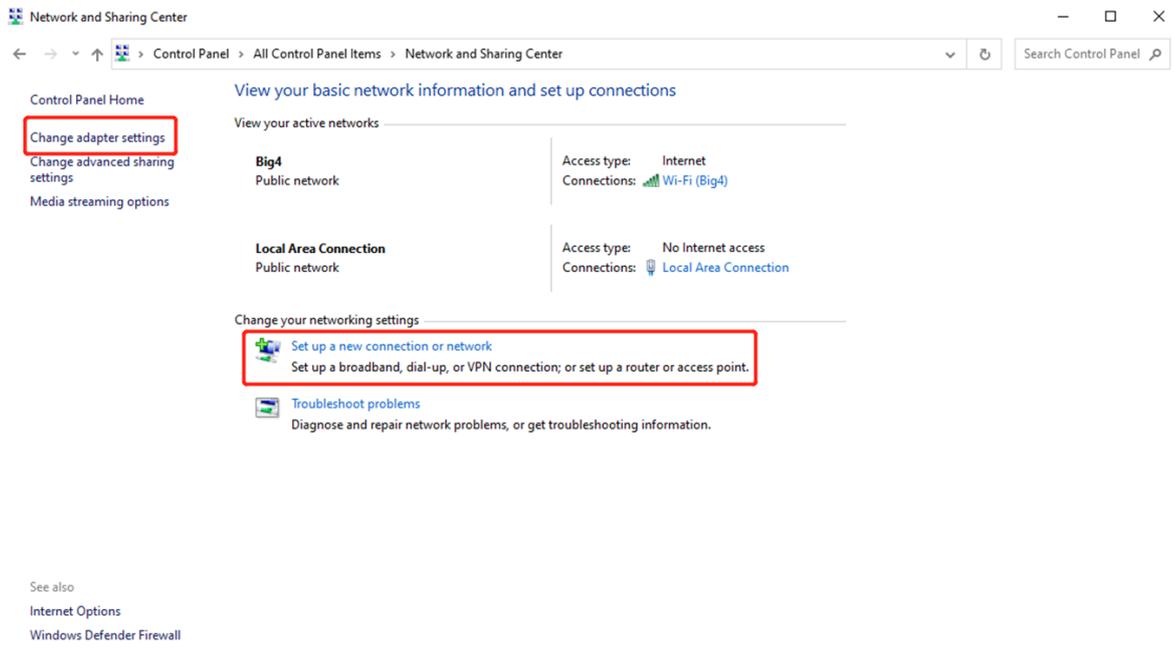
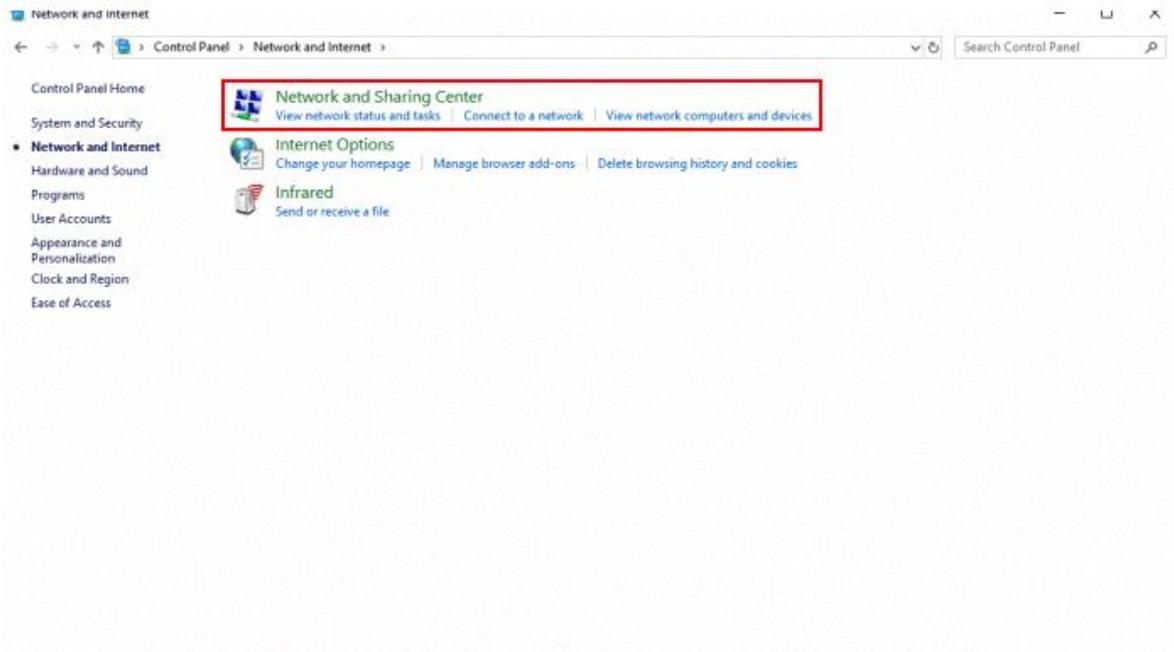
Note

- **Service type:** Select **PPTP**.
- **Network Mode:** Select **Router to Router**.
- **Peer Subnet:** Fill in the internal network segment of the branch. The value and the internal network segment of the headquarters cannot overlap.

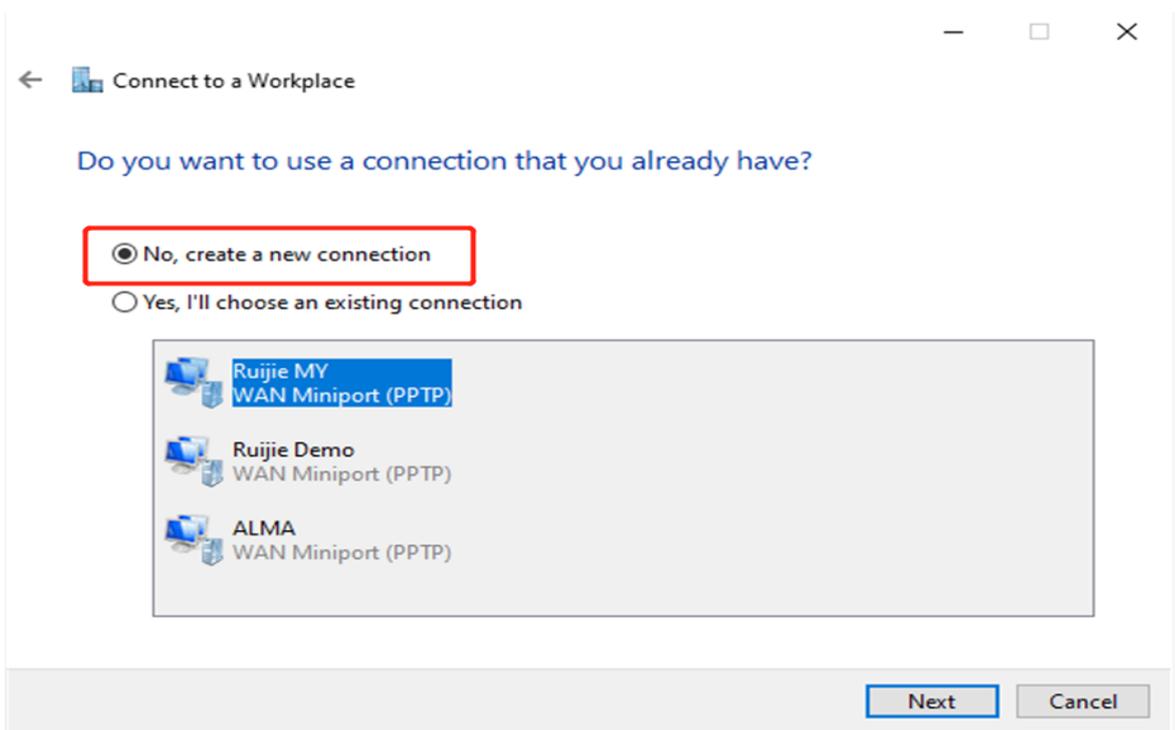
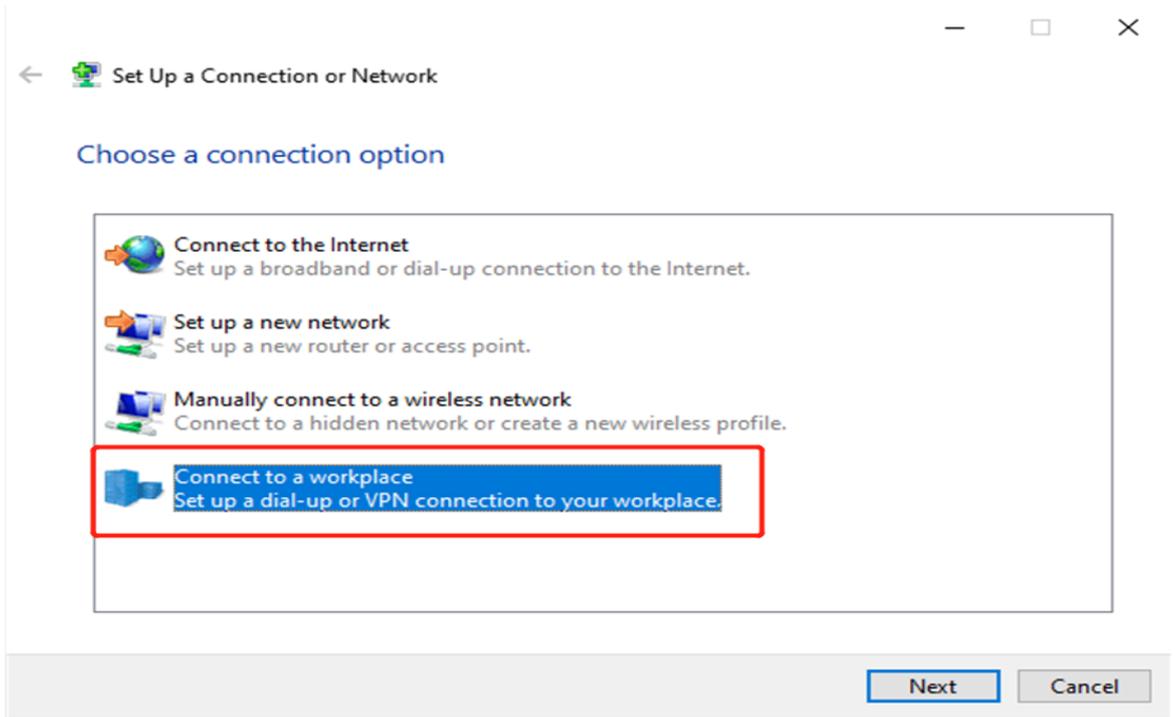
(2) Client side (Windows 10 is used as an example):

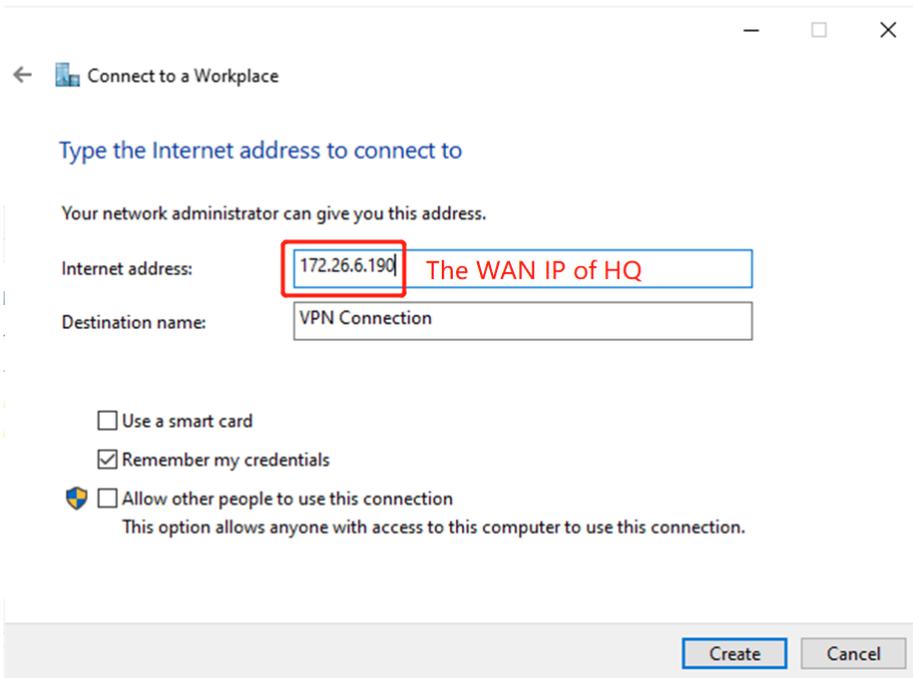
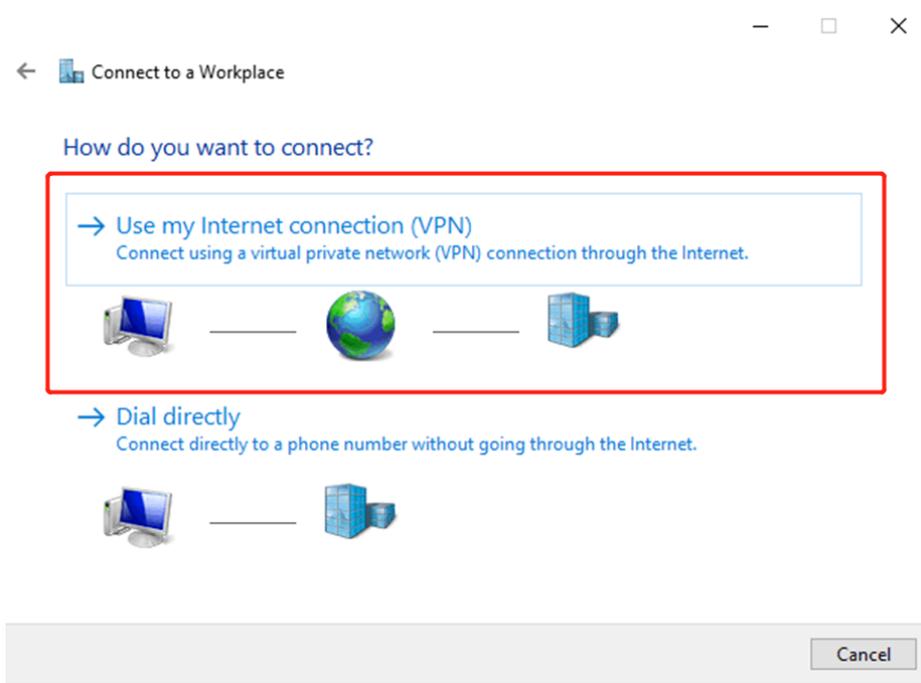
- a Choose **Control Panel > Network and Internet > Network and Sharing Center**.



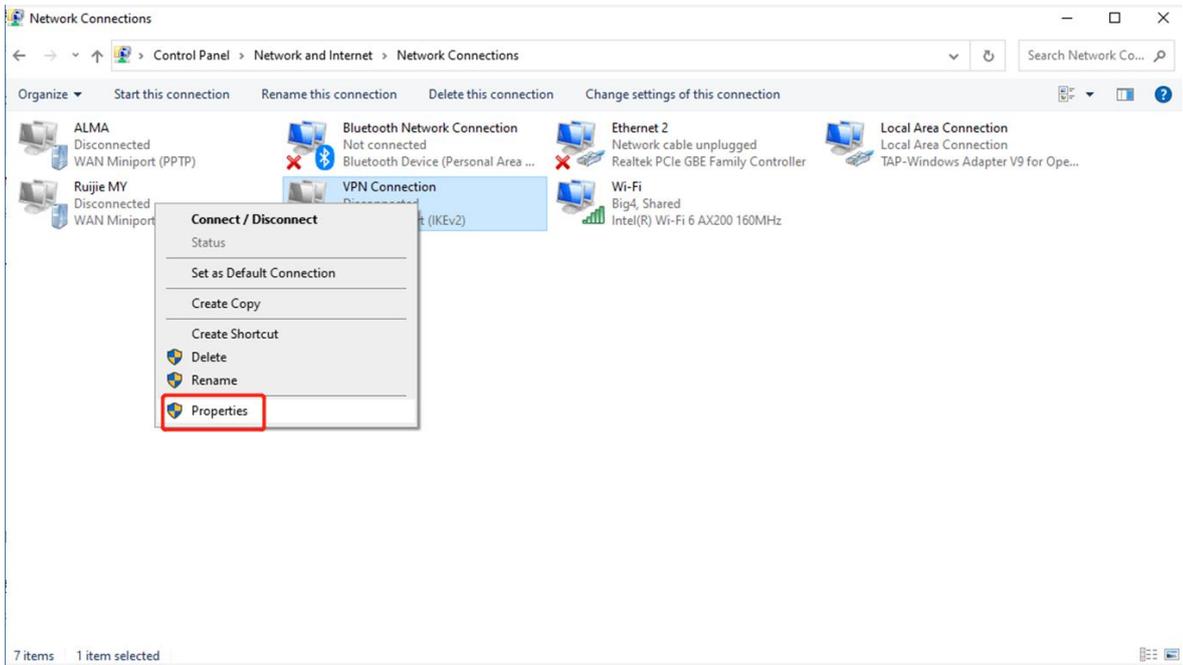
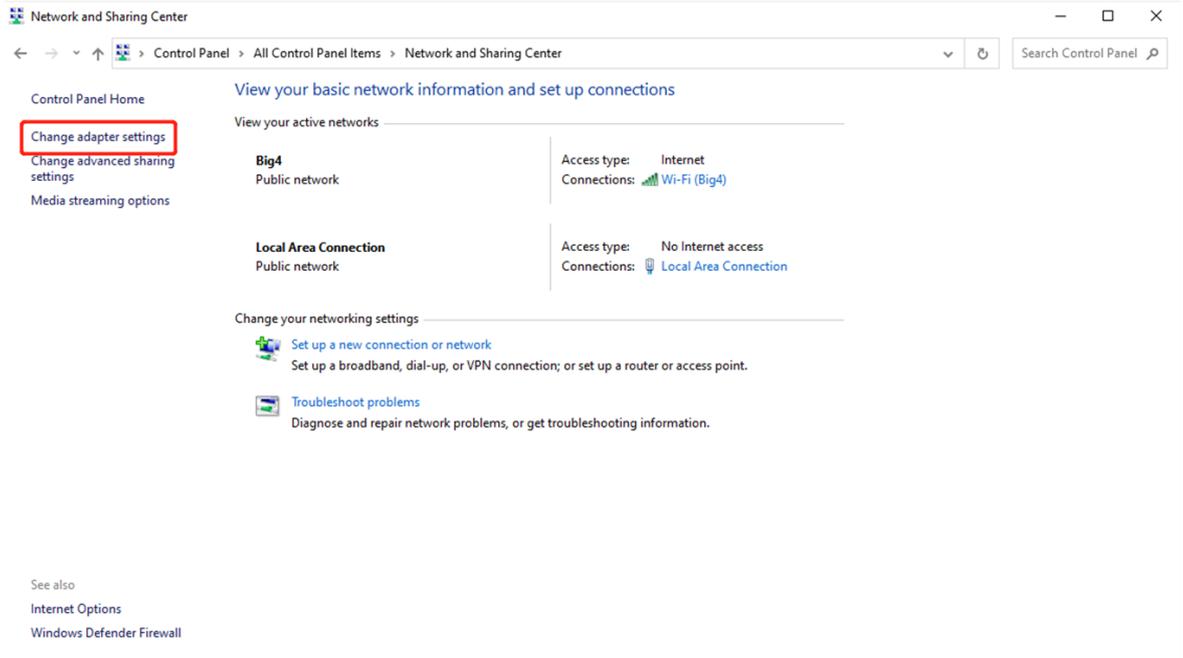


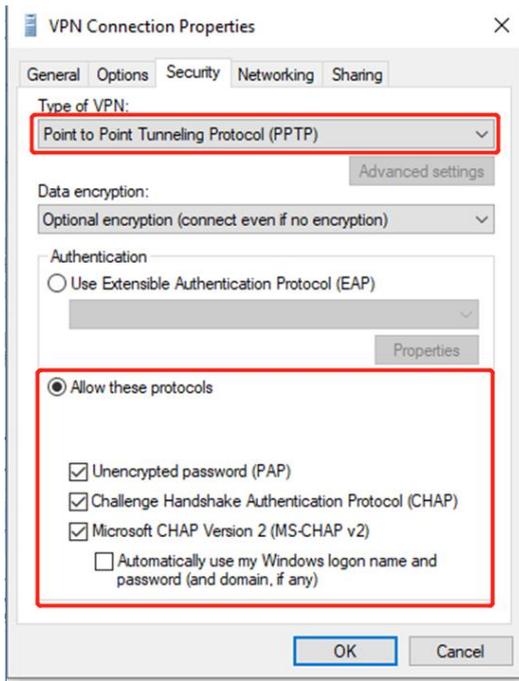
b Configure a VPN connection.



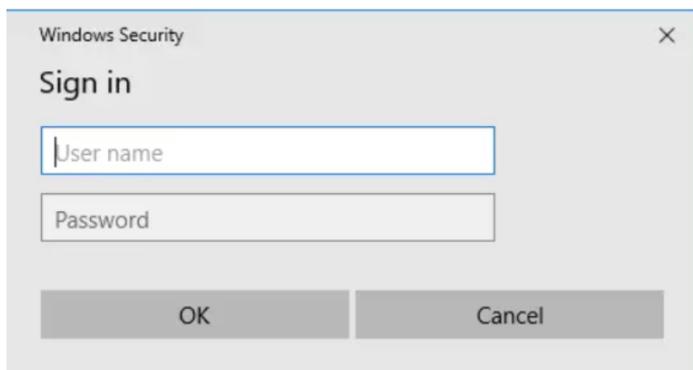
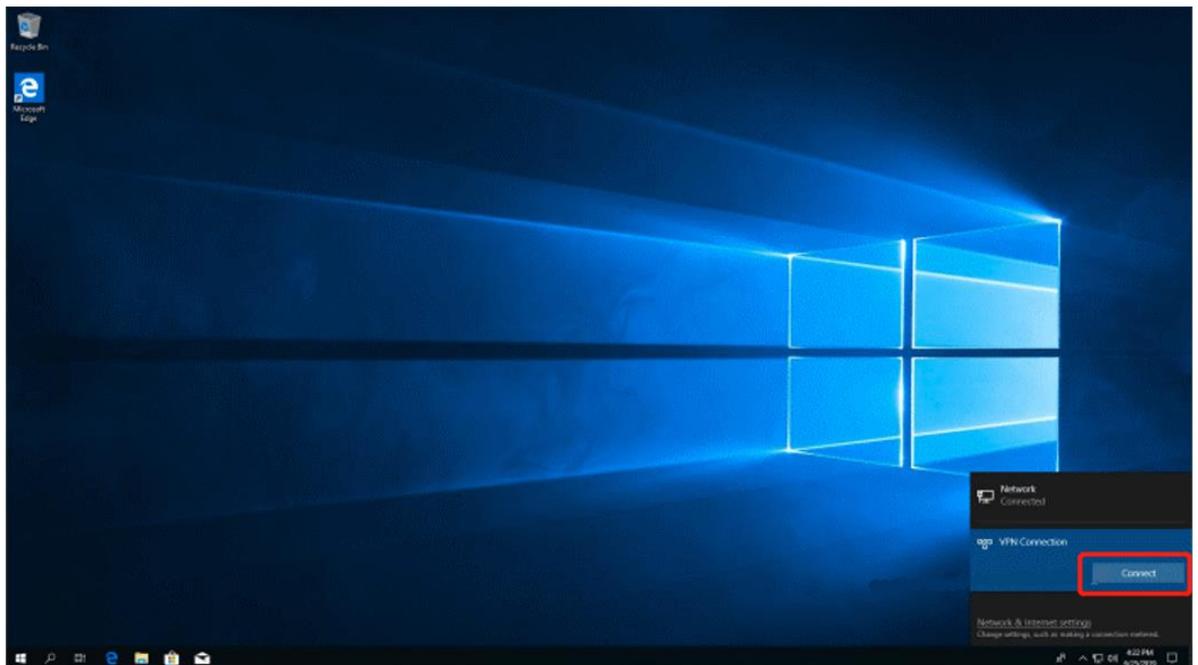


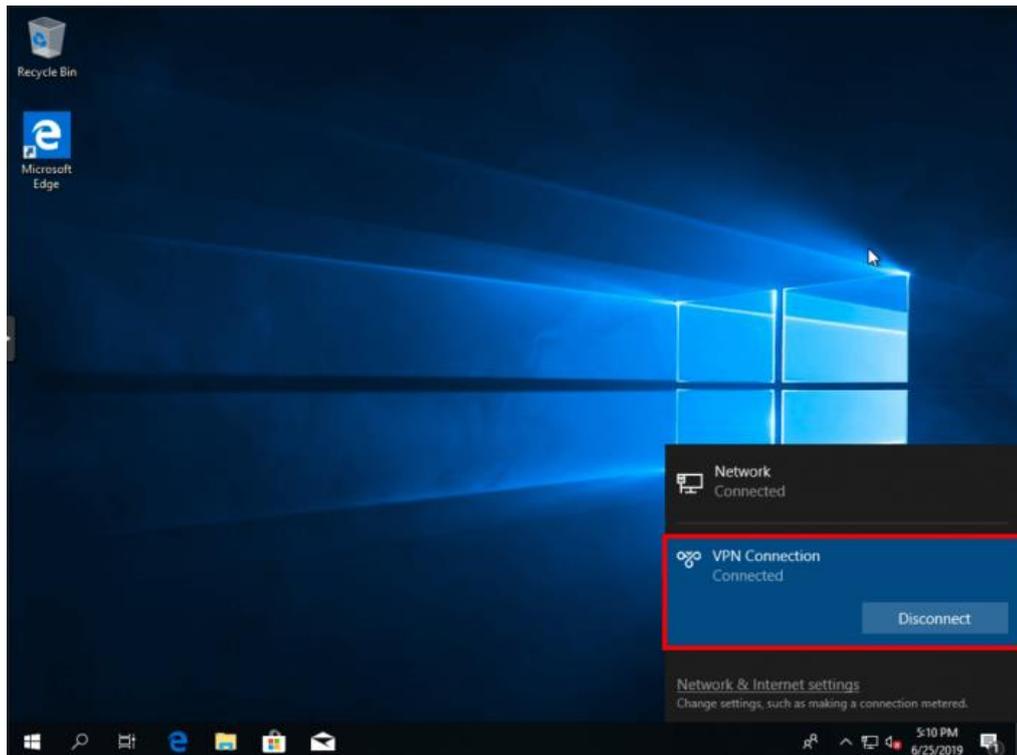
- c Change settings of the adapter.





d Check the VPN connection status.





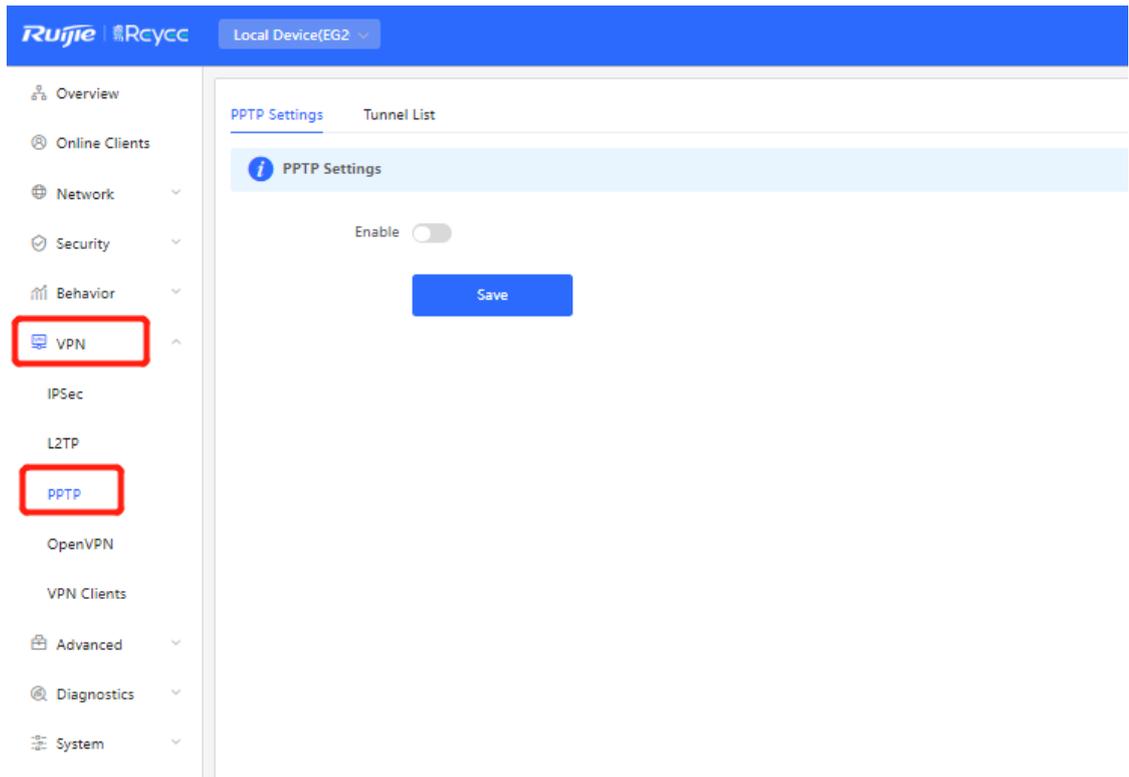
- e If your PC cannot access internal devices (192.168.10.0/24) of the headquarters after the VPN connection is set up, add the following static route on your PC. The IP address 192.168.100.2 is the PC's IP address obtained from the headquarters. Then the PC can access internal devices of the headquarters.

```
C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2
```

2. Site-to-Site Scenario Configuration

(1) Headquarters side:

- a Log in to the Reyeeg EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN > PPTP**.



- c Enable PPTP, set **PPTP Type** to **Server**, perform PPTP configuration, and click **Save**.

PPTP Settings Tunnel List

PPTP Settings

Enable

PPTP Type Server Client

* Local Tunnel IP

* IP Range ?

* DNS Server

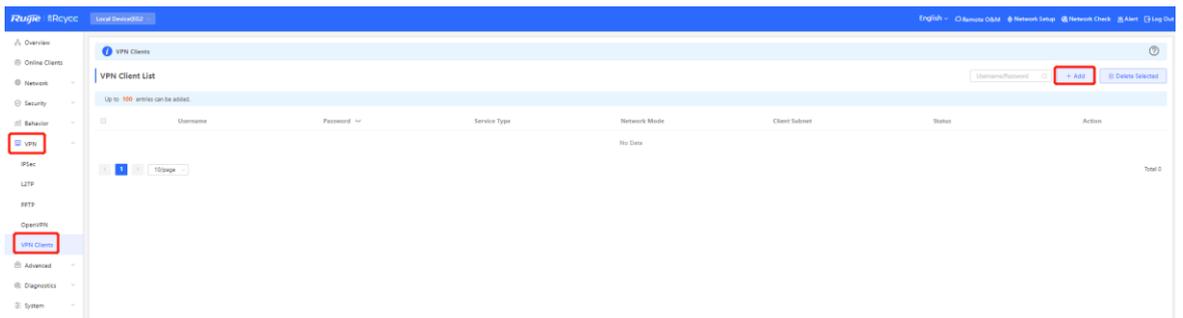
MPPE Disable Enable

Flow Control Disable Enable

* PPP Hello Interval

Save

d Choose **Network > VPN Clients** and configure VPN clients.



Add User ×

Service Type

* Username

* Password

Network Mode

Status

⚠ Caution

The value of **Peer Subnet** is the local IP address range of its branch.

- (2) Branch side:
- a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the **Local** mode. Choose **VPN > PPTP**, enable **PPTP**, and set **PPTP Type** to **Client**.

PPTP Settings Tunnel List

PPTP Settings

Enable

PPTP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

MPPE Disable Enable

Work Mode NAT Router

* PPP Hello Interval

[Save](#)

Caution

- PPTP Type: Select Client.
- Username and Password: Fill in the username and password that have been added in the headquarters.
- Tunnel IP: Select the address in the IP address range of the address pool filled in by the headquarters. If Dynamic is selected, the IP address of the address pool is assigned randomly. If Static is selected, any address in the address pool can be entered without conflicts.
- Server Address: Fill in the WAN port address of the headquarters. The public network IP address is required. Here, a private network address is just for reference.
- Peer Subnet: Specify the internal network segment of the headquarters. The value and internal network segment of the branch cannot overlap.
- Work Mode: Specify whether the headquarters is allowed to access the branch intranet. If so, select Router. If not, select NAT.

c Check the VPN connection status.

PPTP Settings Tunnel List

Tunnel List

[Delete Selected](#)

	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input type="checkbox"/>	test	Server	ppp0	192.168.100.1	172.26.5.237	192.168.100.2	8.8.8.8	Delete

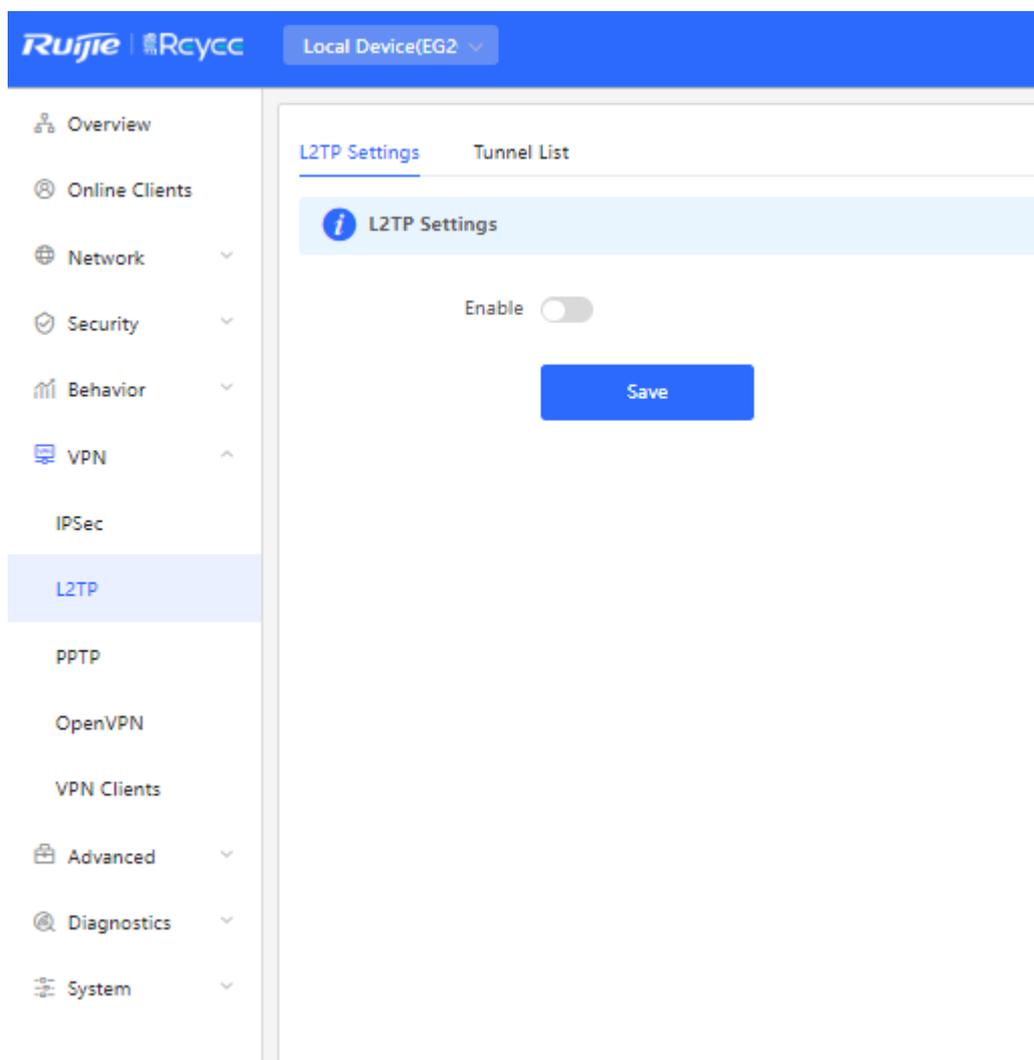
4.7.2 L2TP VPN

L2TP VPN is typically used in client-to-site and site-to-site scenarios. For example, clients work from home and need to access company server through L2TP VPN tunnels; a company has three branches that are distributed in three different places of the Internet, and each branch needs to establish a tunnel with each other through a router.

1. Client-to-Site Scenario Configuration

(1) Headquarters side:

- a Log in to the Reyeeg EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN > L2TP**.



- c Enable L2TP, perform L2TP configuration, and click **Save**.

L2TP Settings Tunnel List

L2TP Settings

Enable

L2TP Type Server Client

* Local Tunnel IP

* IP Range ⓘ

* DNS Server

Tunnel Authentication Disable Enable

IPSec Security Open Security ⓘ

Flow Control Disable Enable

* PPP Hello Interval

Save

d Choose **Local Device > VPN > VPN Clients** and configure VPN clients.

Ruijie Rcycc Local Device:EG3 Currently in Local Device mode English Remote O&M Network Setup Network Check Alert Log Out

Overview
Online Clients
Network
Security
Behavior
VPN
IPSec
L2TP
PPTP
OpenVPN
VPN Clients
Advanced
Diagnostics
System

VPN Clients

VPN Client List Username/Password + Add Delete All Delete Selected

Up to 300 entries can be added.

Username	Password	Service Type	Network Mode	Client Subnet	Status	Action
No Data						

1 10/page Total 0

Add User



Service Type

* Username

* Password

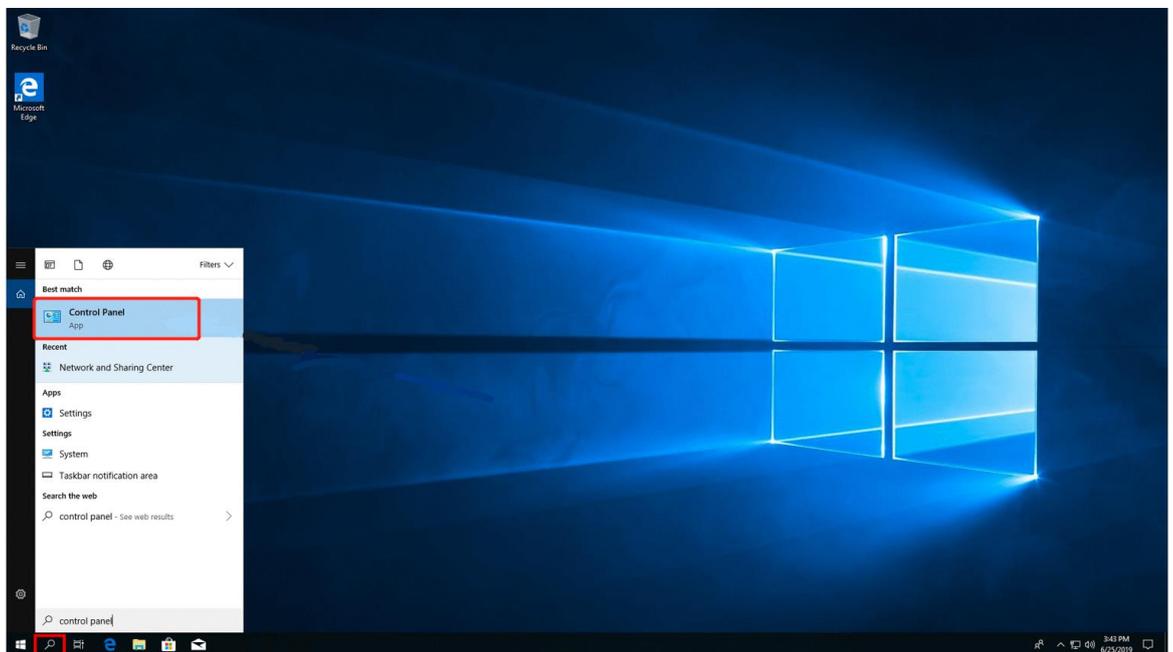
Status

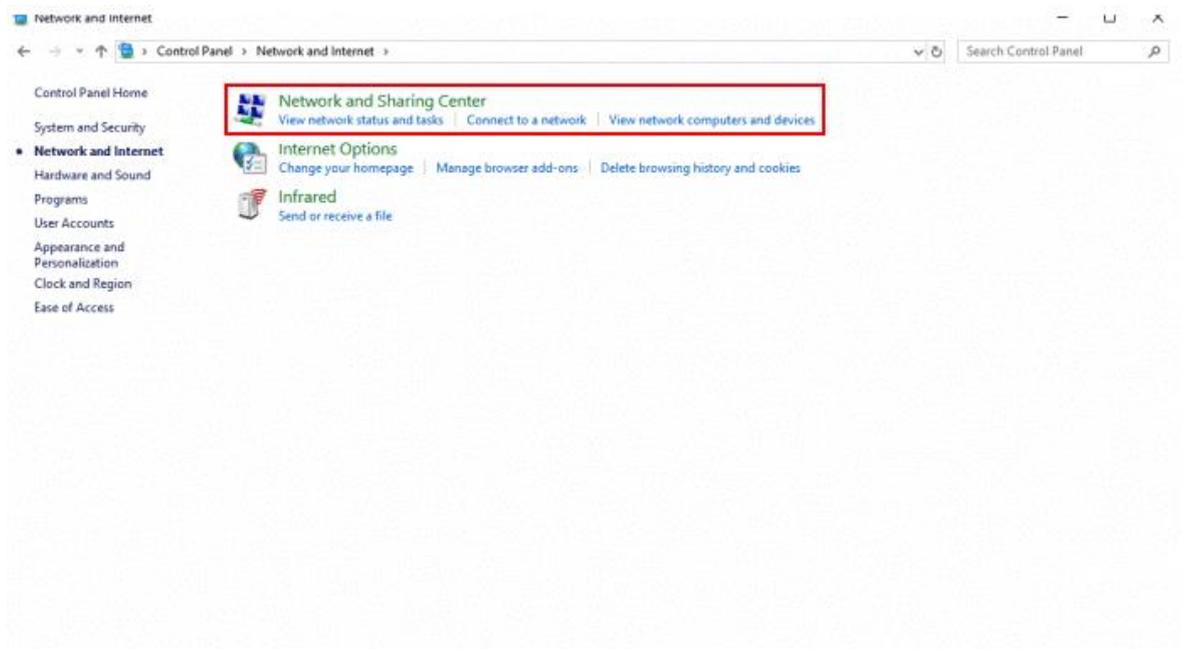
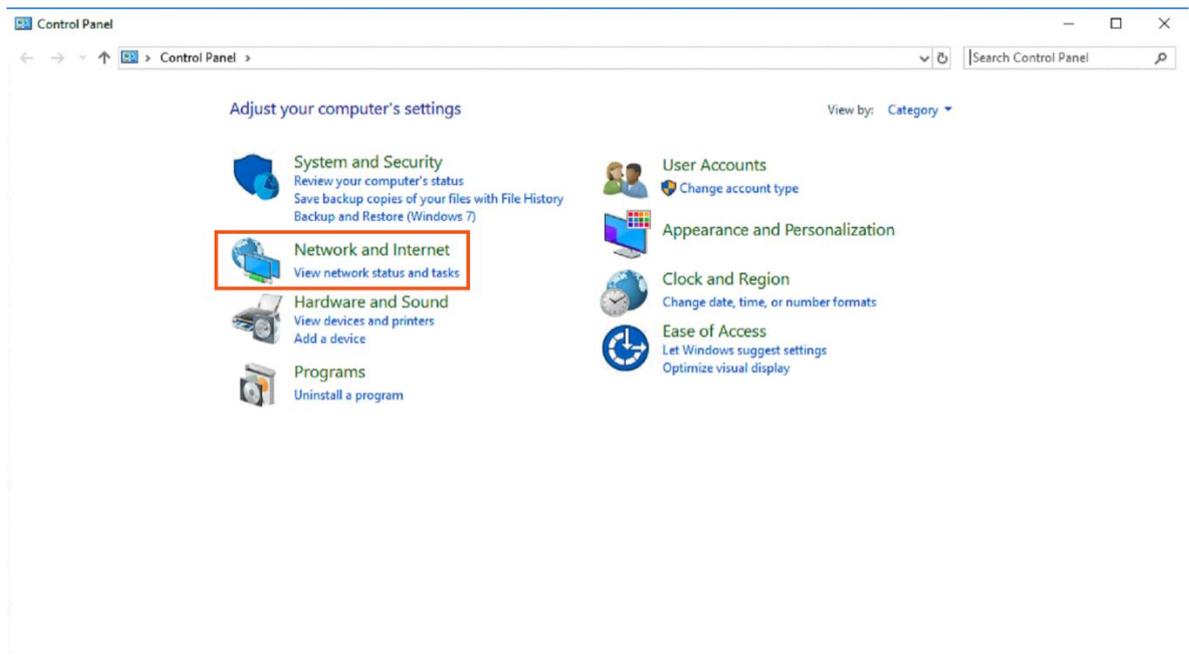
Cancel

OK

(2) Client side (Windows 10 is used as an example):

- a Choose **Control Pane > Network and Internet > Network and Sharing Center**.





b. Configure a VPN connection.

Network and Sharing Center

Control Panel Home

- Change adapter settings
- Change advanced sharing settings
- Media streaming options

View your basic network information and set up connections

View your active networks

Big4 Public network	Access type: Internet Connections: Wi-Fi (Big4)
Local Area Connection Public network	Access type: No Internet access Connections: Local Area Connection

Change your networking settings

- Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
- Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also

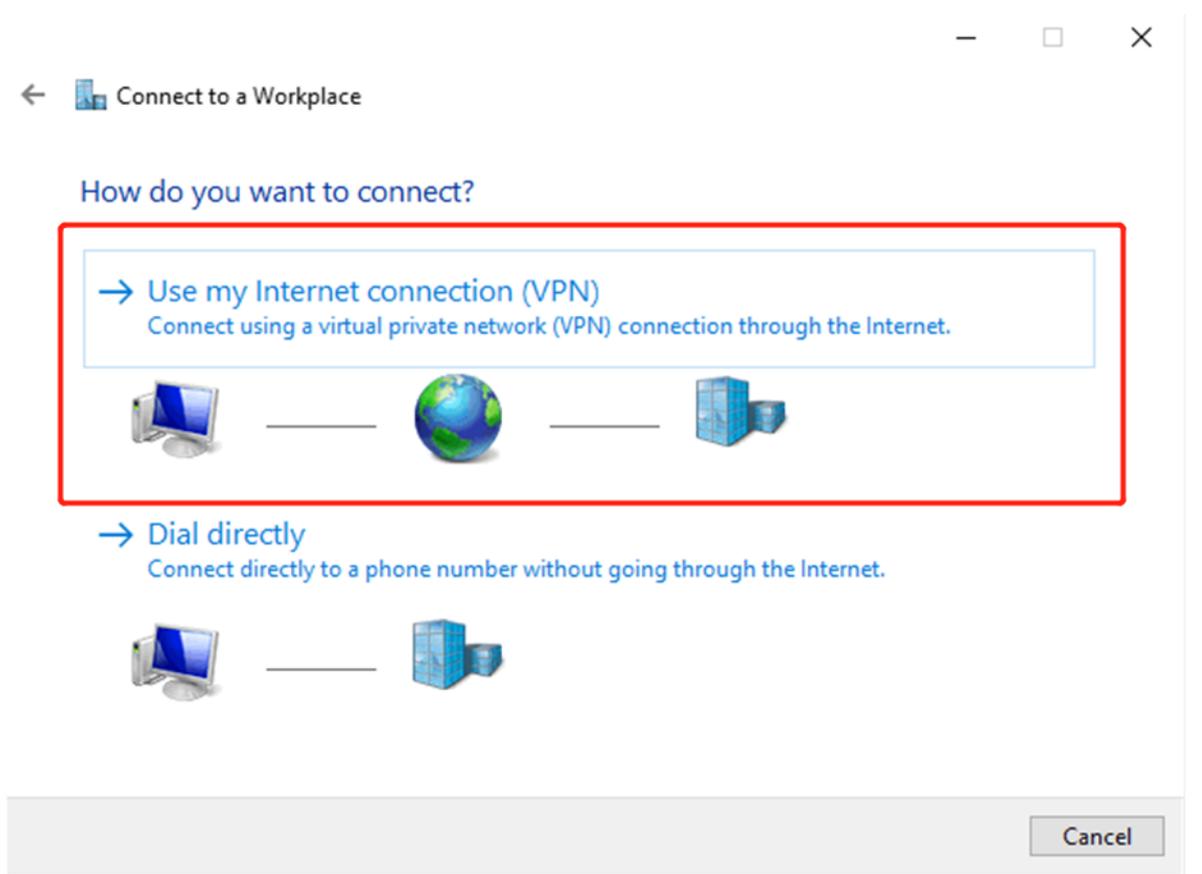
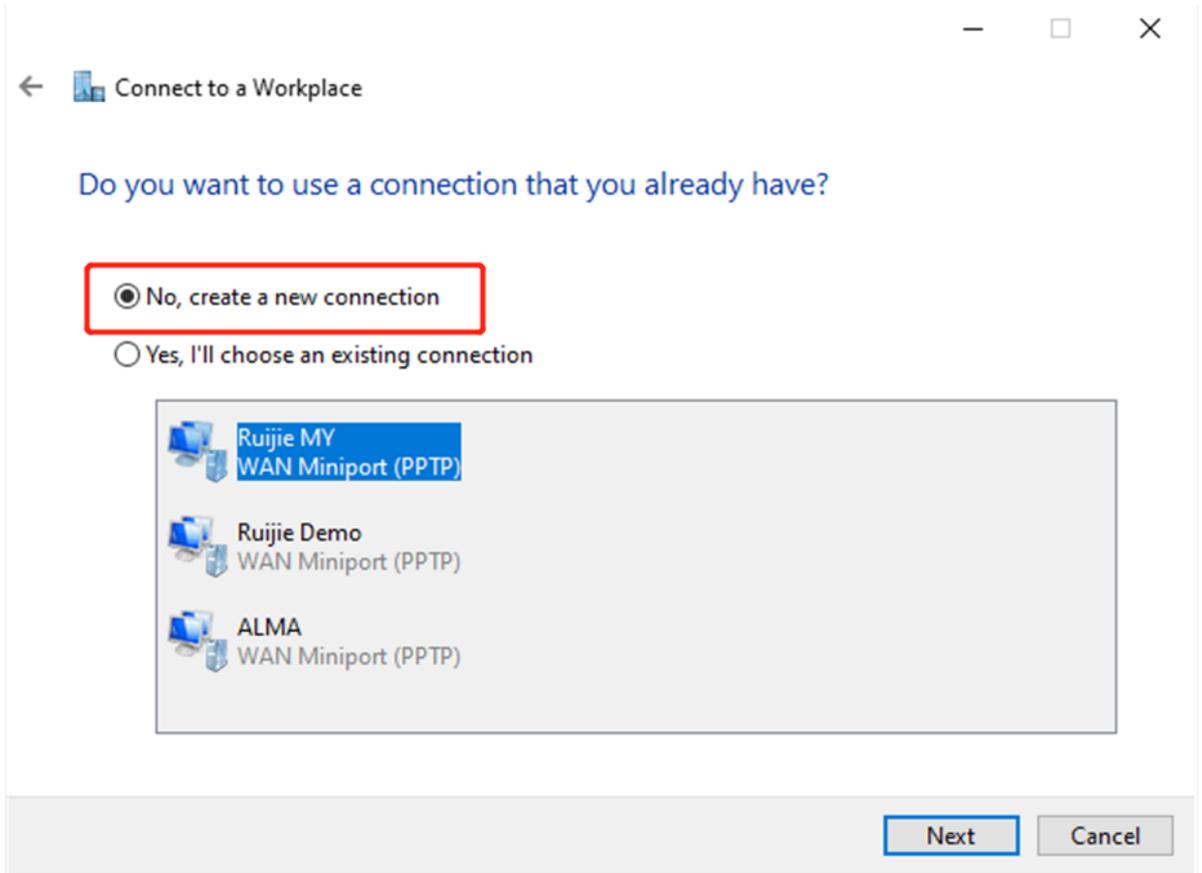
- Internet Options
- Windows Defender Firewall

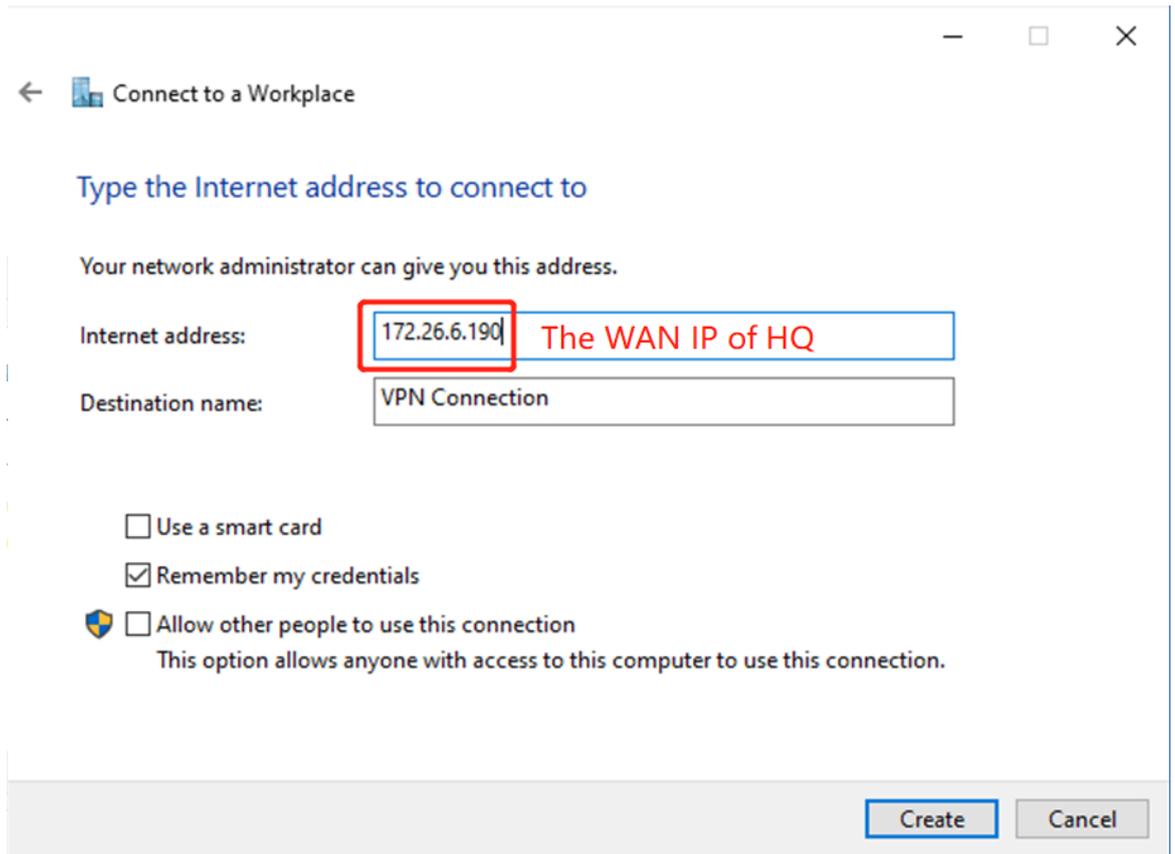
Set Up a Connection or Network

Choose a connection option

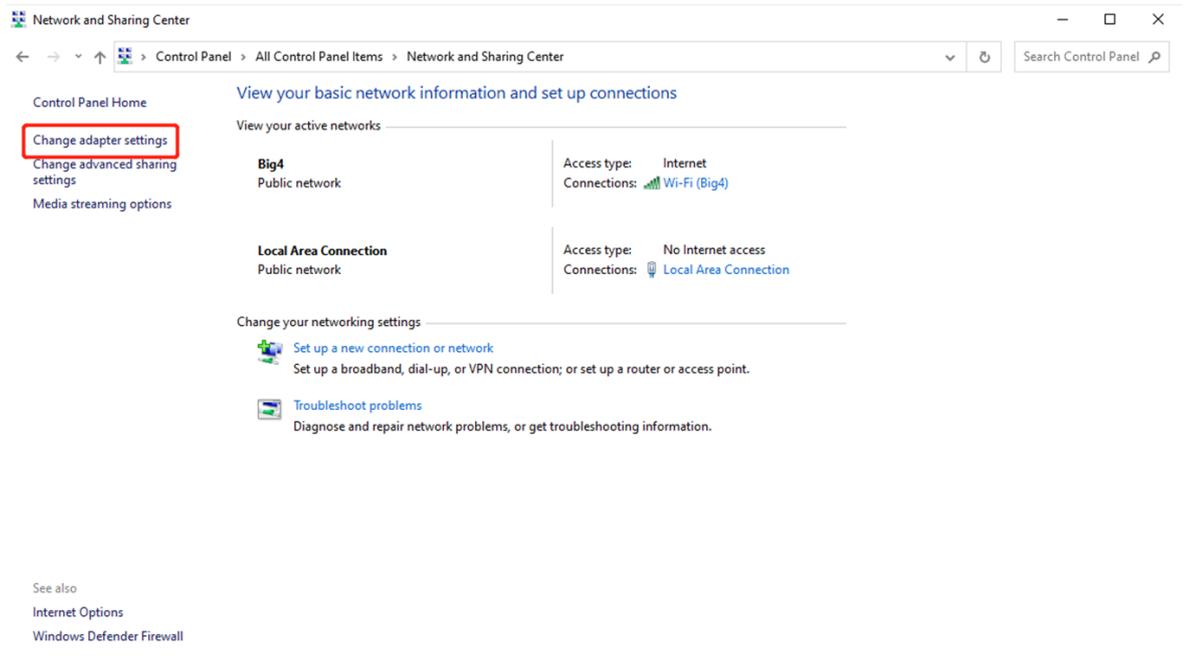
- Connect to the Internet**
Set up a broadband or dial-up connection to the Internet.
- Set up a new network**
Set up a new router or access point.
- Manually connect to a wireless network**
Connect to a hidden network or create a new wireless profile.
- Connect to a workplace**
Set up a dial-up or VPN connection to your workplace.

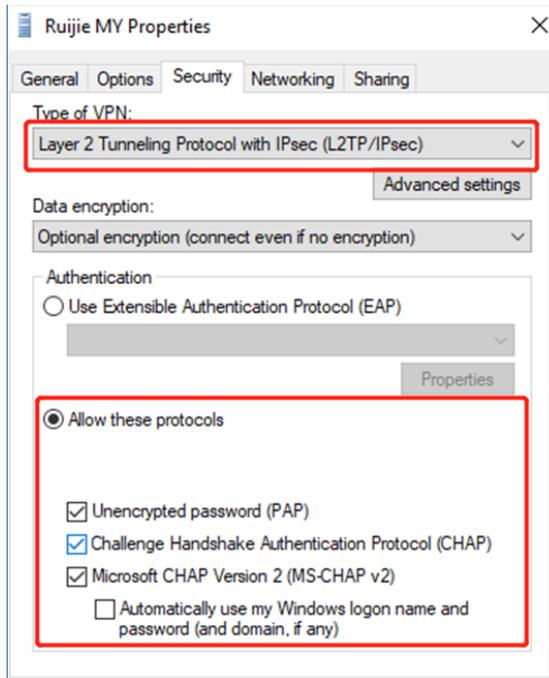
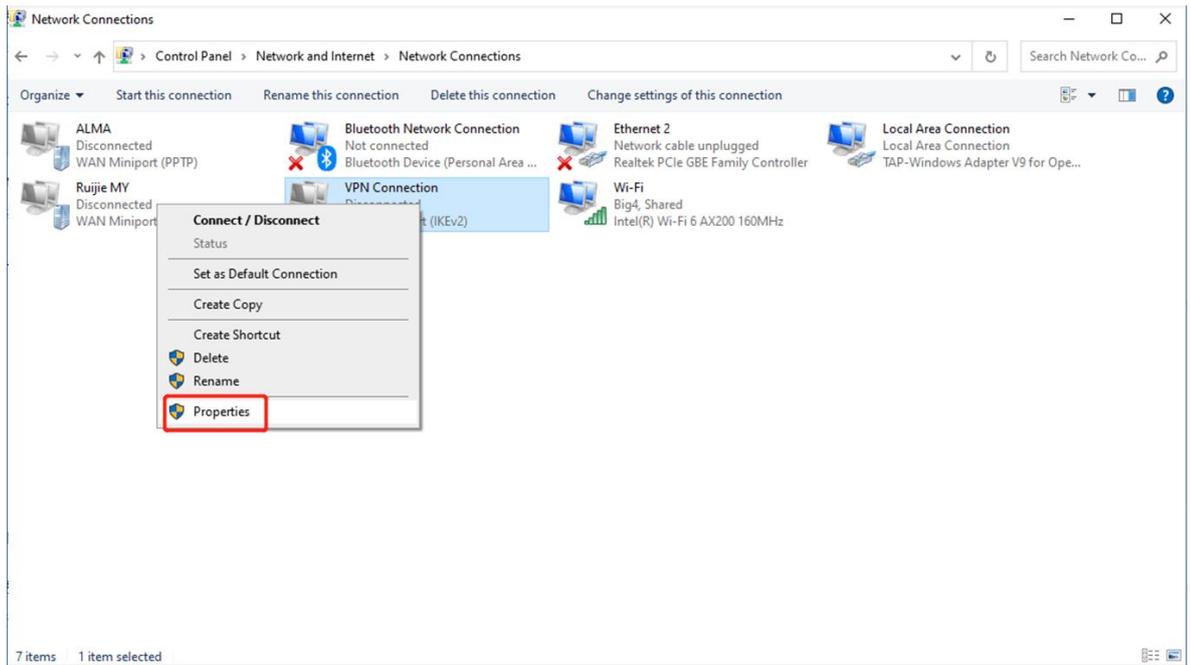
Next Cancel



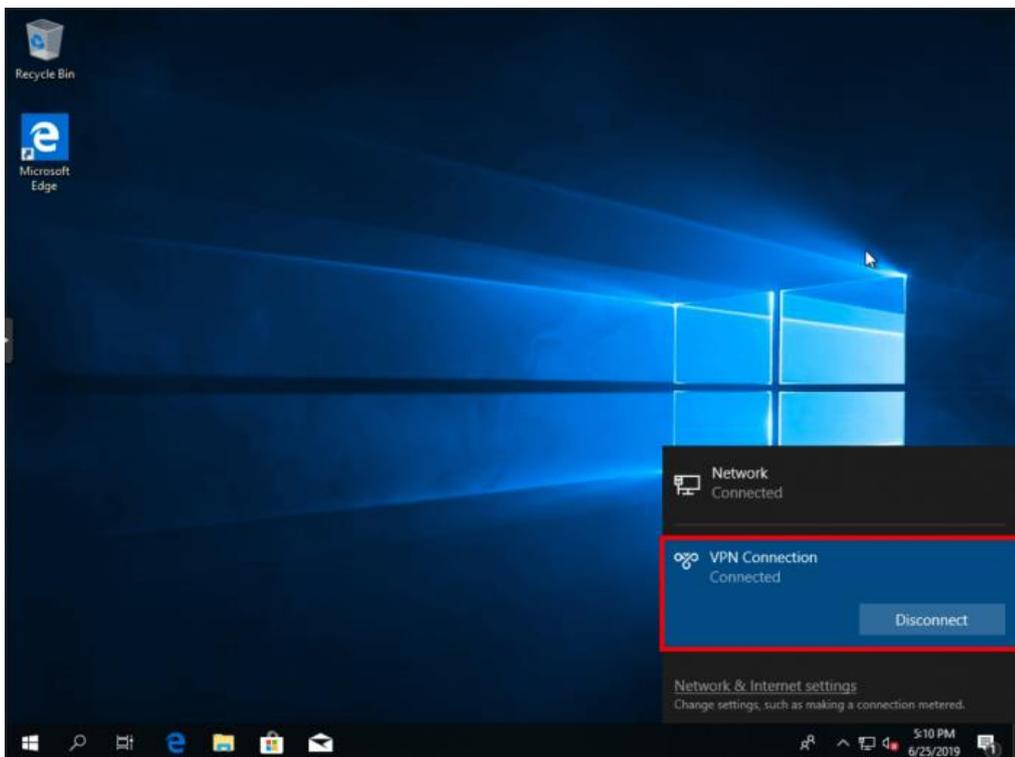
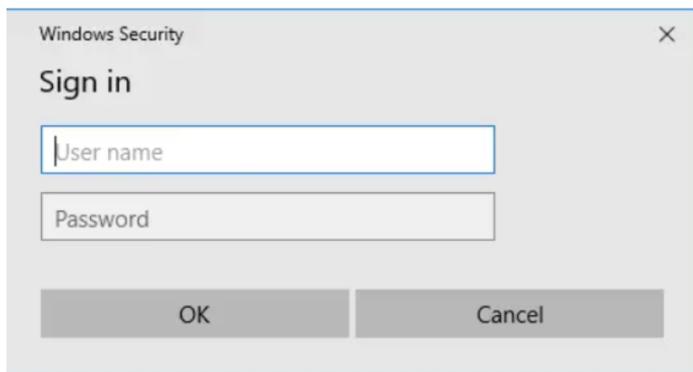
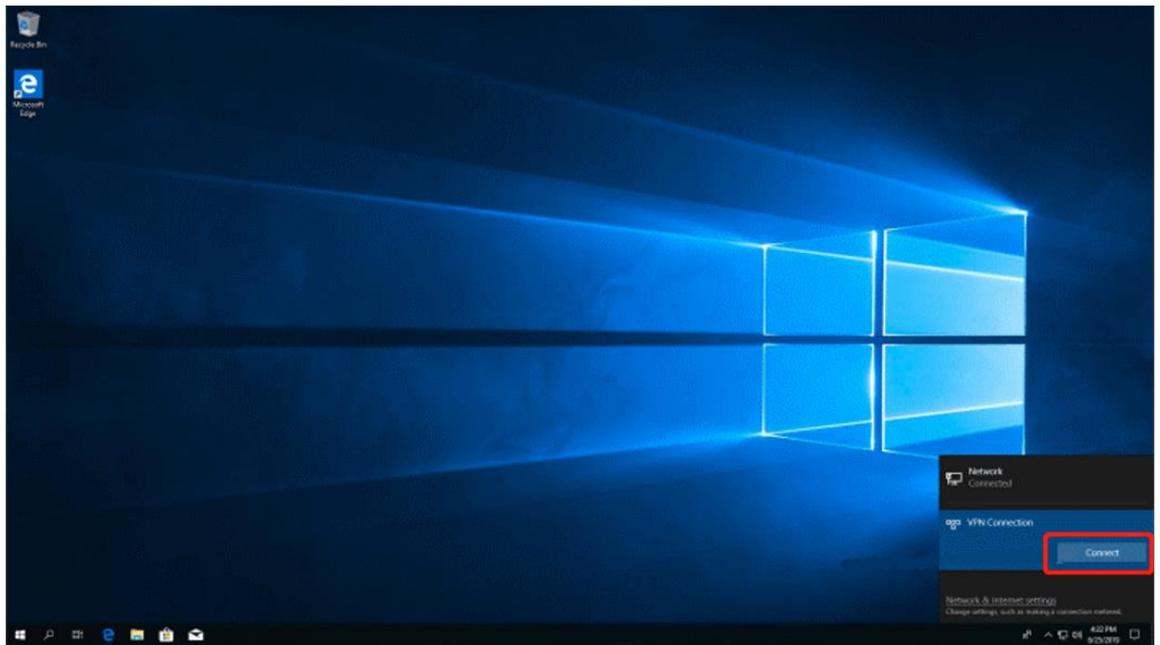


c Change adapter's settings.





d Check the VPN connection status.



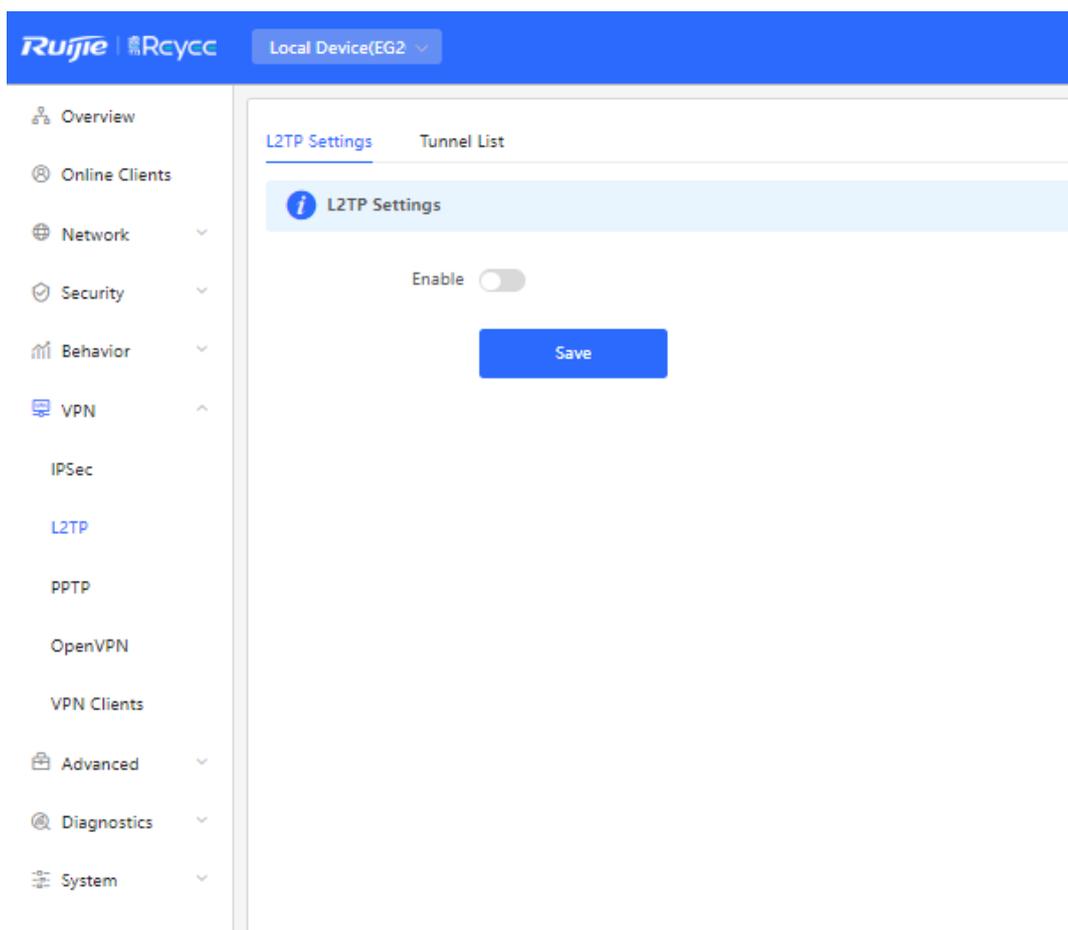
- e If your PC cannot access internal devices (192.168.10.0/24) of the headquarters after the VPN connection is set up, add the following static route on your PC. The IP address 192.168.100.2 is the PC's IP address obtained from the headquarters. Then the PC can access internal devices of the headquarters.

```
C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2
```

2. Site-to-Site Scenario Configuration

(1) Headquarters side:

- a Log in to the Reyee EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN >L2TP**.



- c Enable L2TP, set **L2TP Type** to **Server**, perform L2TP configuration, and click **Save**.

L2TP Settings Tunnel List

L2TP Settings

Enable

L2TP Type Server Client

* Local Tunnel IP

* IP Range ?

* DNS Server

Tunnel Authentication Disable Enable

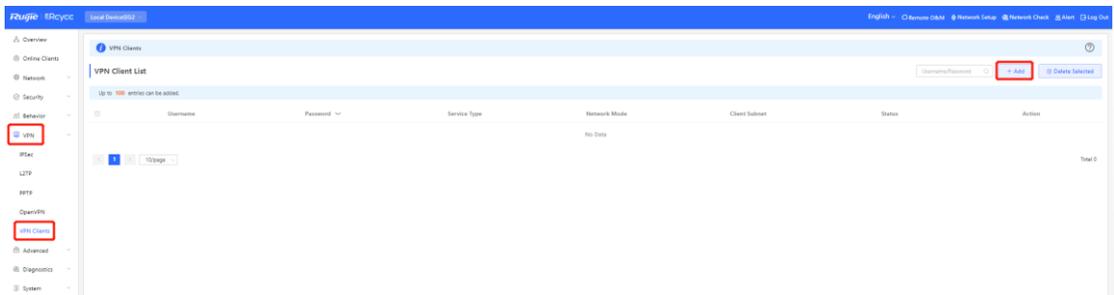
IPSec Security Open Security

Flow Control Disable Enable

* PPP Hello Interval

Save

d Choose **Network > VPN Clients** and configure VPN clients.



Add User×

Service Type

* Username

* Password

Network Mode

* Client Subnet

Status

⚠ Caution

The value of **Peer Subnet** is the local IP address range of its branch.

- (2) Branch side:
- a Log in to the Reyeeg EG with the default IP address of 192.168.110.1.
 - b Switch to the **Local** mode. Choose **Gateway > VPN > L2TP**, enable **L2TP**, and set **L2TP Type** to **Client**.

⚠ Caution

- **NAT:** NAT is applied to incoming L2TP packets (the source IP address is replaced with the local virtual IP address).
- **Router:** Only incoming L2TP packets are routed.

c Check the VPN connection status.

Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
test1	Client	l2tp	192.168.30.1	172.26.6.190	192.168.30.254	8.8.8.8	Delete

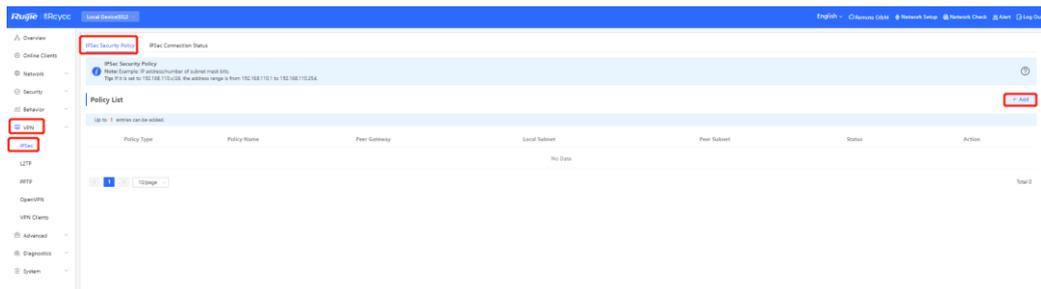
4.7.3 IPsec VPN

IPsec VPN is used for site-to-site scenarios. For example, three branches of a company are distributed in three different places of the internet; each branch uses a router to establish tunnels with each other; data between the company intranets (several PCs) is securely interconnected through the IPsec VPN tunnels established by through these routers.

IPsec VPN only applies to site-to-site scenarios.

(1) Headquarters side:

- a Log in to the Reyee EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN > IPsec > IPsec Security Policy**.



c Configure an IPsec VPN security policy.

Add ×

Policy Type Client **Server**

* Policy Name

Interface ?

* Local Subnet

* Pre-shared Key

Status

----- 1. Set IKE Policy -----
----- 2. Connection Policy -----

----- 1. Set IKE Policy -----

	Authentication	Encryption	DH Group
IKE Policy 1	sha1	3des	dh1
IKE Policy 2	sha1	des	dh1
IKE Policy 3	sha1	3des	dh2
IKE Policy 4	md5	des	dh1
IKE Policy 5	md5	3des	dh2

Negotiation Main Mode Aggressive Mode

Mode

Local ID Type IP NAME

Peer ID Type IP NAME

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

----- 2. Connection Policy -----

Transform Set 1

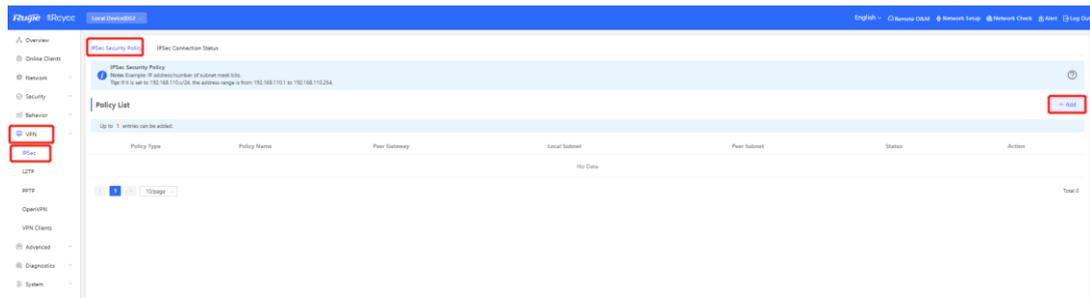
Transform Set 2

Perfect Forward
Secrecy

* Lifetime

(2) Branch side:

- a Log in to the Reyeeg EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN > IPSec > IPSec Security Policy**.



- c Configure an IPsec policy. Ensure that the IKE policy and connection policy are the same on both sides.

Add ×

Policy Type Client Server

* Policy Name

* Peer Gateway +

Interface ?

* Local Subnet

* Peer Subnet +

* Pre-shared Key

Status

----- 1. Set IKE Policy -----

	Authentication	Encryption	DH Group
IKE Policy 1	sha1	3des	dh1
IKE Policy 2	sha1	des	dh1
IKE Policy 3	sha1	3des	dh2
IKE Policy 4	md5	des	dh1
IKE Policy 5	md5	3des	dh2

Negotiation Main Mode Aggressive Mode
Mode

Local ID Type IP NAME

Peer ID Type IP NAME

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

----- 2. Connection Policy -----

Transform Set 1

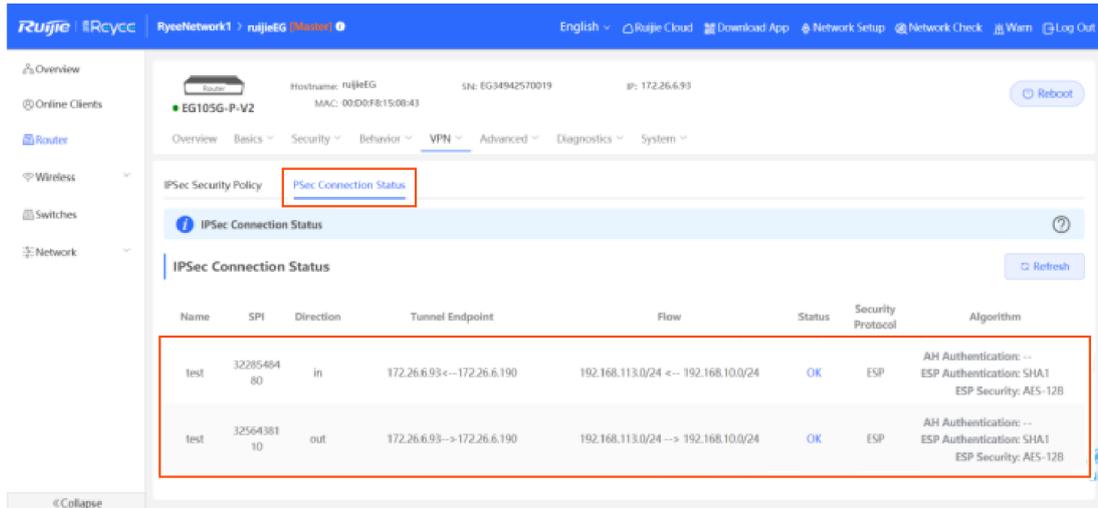
Transform Set 2

Perfect Forward

Secrecy

* Lifetime

d Check the IPsec connection status.



⚠ Caution

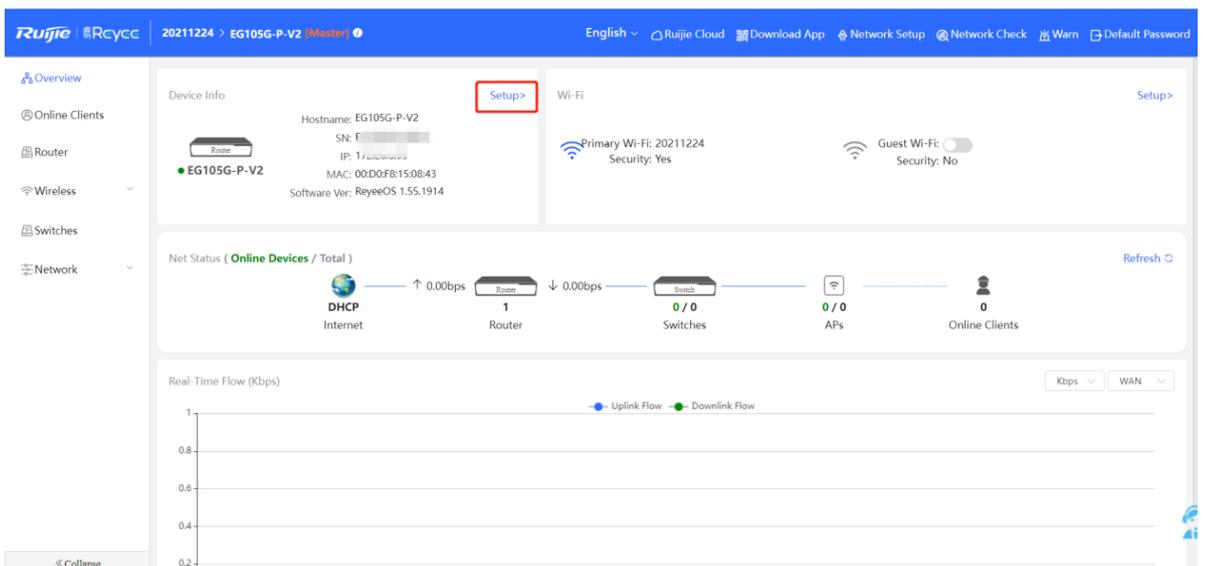
If your headquarters EG has no public IP address configured for other external devices, you need to configure port mapping on external devices and configure **Local ID Type** as **NAME** on devices of the headquarters and branches.

4.7.4 L2TP Over IPsec VPN

L2TP over IPsec VPN is typically used in site-to-site and client-to-site scenarios. For example, three branches of a company are distributed in three different places of the Internet, each branch uses a router to establish tunnels with each other, and data between the company intranets (several PCs) is securely interconnected through L2TP over IPsec VPN tunnels established by these routers, the staff who work at home can access company data through L2TP over IPsec VPN tunnels.

(1) Headquarters side:

- a Log in to the Reyeeg EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN > L2TP** and configure **IPsec Security**.



The screenshot shows the Ruijie Cloud management interface for a device named EG105G-P. The 'VPN' menu is expanded, and 'L2TP' is selected. The 'L2TP Settings' page is displayed with the following configuration:

- Enable:
- L2TP Type: Server Client
- * Local Address: 10.0.0.1
- * IP Range: 10.0.0.2-10.0.0.254
- * DNS Server: 8.8.8.8

The screenshot shows the 'IPsec Security' configuration page in the Ruijie Cloud management interface. The configuration includes:

- * DNS Server: 8.8.8.8
- IPsec Security: Security
- * Pre-shared Key: ruijie
- IKE Policy: sha1-3des-dh1
- Transform Set: esp-sha1-aes128
- Negotiation Mode: Main Mode Aggressive Mode
- Local ID Type: IP NAME
- * PPP Hello Interval: 10 seconds

A 'Save' button is visible at the bottom of the configuration area.

⚠ Caution

- **PPP Hello Interval:** indicates the interval for sending hello messages on the PPP over IPsec connection.
- **IPsec Security:** indicates whether IPsec is used.
- **Pre-shared Key:** indicates the pre-shared key required for IPsec encryption.
- **Local ID Type:** When the WAN port of the headquarters is configured with the public IP address, select **IP**. When the WAN port of the headquarters is configured with the private IP address, select **NAME** and configure DMZ on the external device.

c Configure VPN clients for the branch EG and PC.

The screenshot shows the Ruijie Cloud management interface for a device named EG105G-P. The 'VPN Clients' menu is open, and the 'VPN Client List' page is displayed. A table lists existing clients: 'test' (L2TP, PC to Router), 'test1' (PPTP, PC to Router), and 'test2' (PPTP, PC to Router). A '+ Add' button is highlighted with a red box. A dropdown menu is open over the 'VPN Clients' header, with 'VPN Clients' selected and highlighted with a red box.

Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
test	test	L2TP	PC to Router	-	Enable	Edit Delete
test1	test1	PPTP	PC to Router	-	Enable	Edit Delete
test2	test2	PPTP	PC to Router	-	Enable	Edit Delete

The 'Add User' dialog box is shown with the following configuration: Service Type: ALL, Username: Branch, Password: [masked], Network Mode: Router to Router (highlighted with a red box), Peer Subnet: 192.168.10.0/24, and Status: On. The 'OK' button is highlighted.

The 'Add User' dialog box is shown with the following configuration: Service Type: ALL, Username: PC, Password: [masked], Network Mode: PC to Router, Peer Subnet: [empty], and Status: On. The 'OK' button is highlighted.

⚠ Caution

- **PC to Router:** A connection is established between a PC and a terminal.

- **Router to Router:** A direct, non-shared, and secure connection is set up between two terminals.

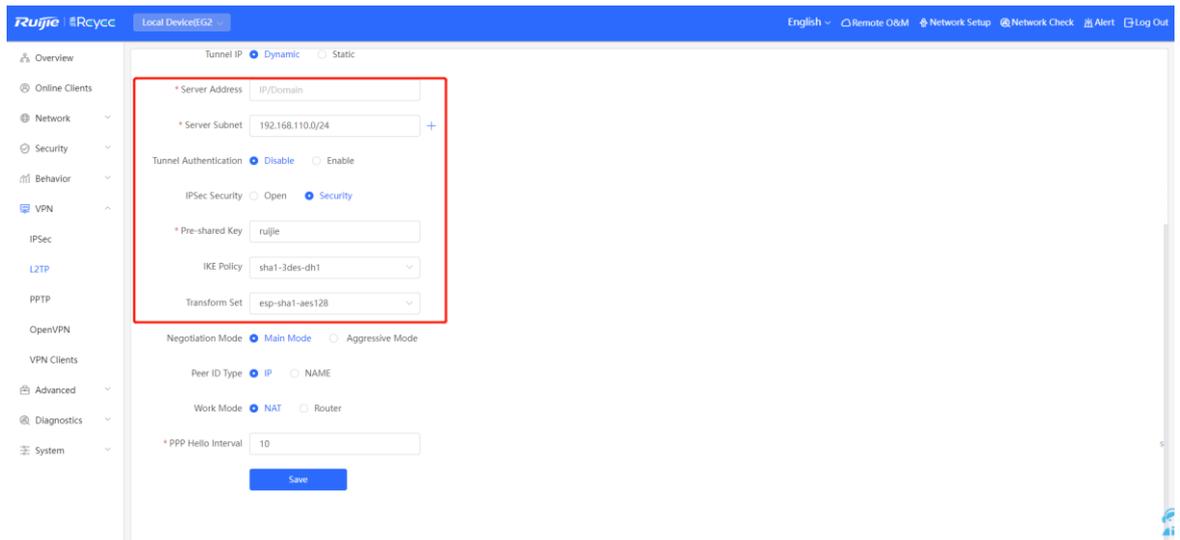
(2) Branch side:

- Log in to the Reyeeg EG with the default IP address of 192.168.110.1.
- Choose **Setup > VPN > L2TP** and enable **IPsec Auth**.

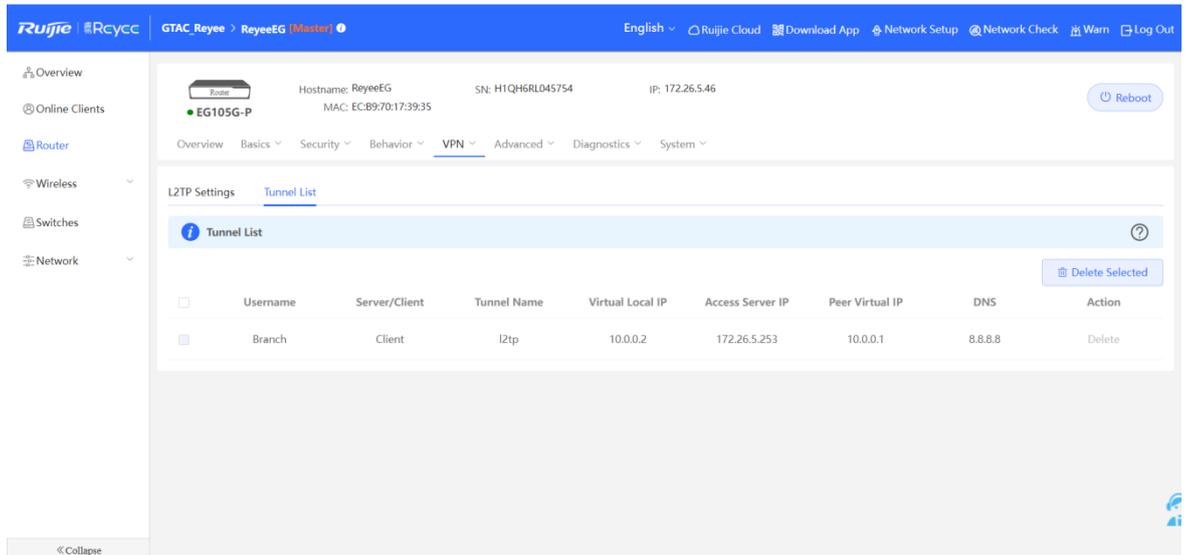
The screenshot shows the Ruijie Reyeeg EG105G-P-V2 web interface. The 'Device Info' section is highlighted with a red box around the 'Setup' button. The 'Net Status' section shows 1 Router and 0 Online Clients. The 'Real-Time Flow' section shows a graph for Uplink and Downlink flows.

The screenshot shows the Ruijie Reyeeg EG105G-P web interface. The 'VPN' menu is open, and 'L2TP' is selected. The 'L2TP Settings' section is visible, with 'Enable' checked, 'L2TP Type' set to 'Client', and 'Username' set to 'Branch'. A red box highlights the 'L2TP' option in the VPN menu.

- Configure an IPsec security, and ensure that the values of **Pre-share Key**, **IKE Policy**, and **Transform Set** are the same on both sides.

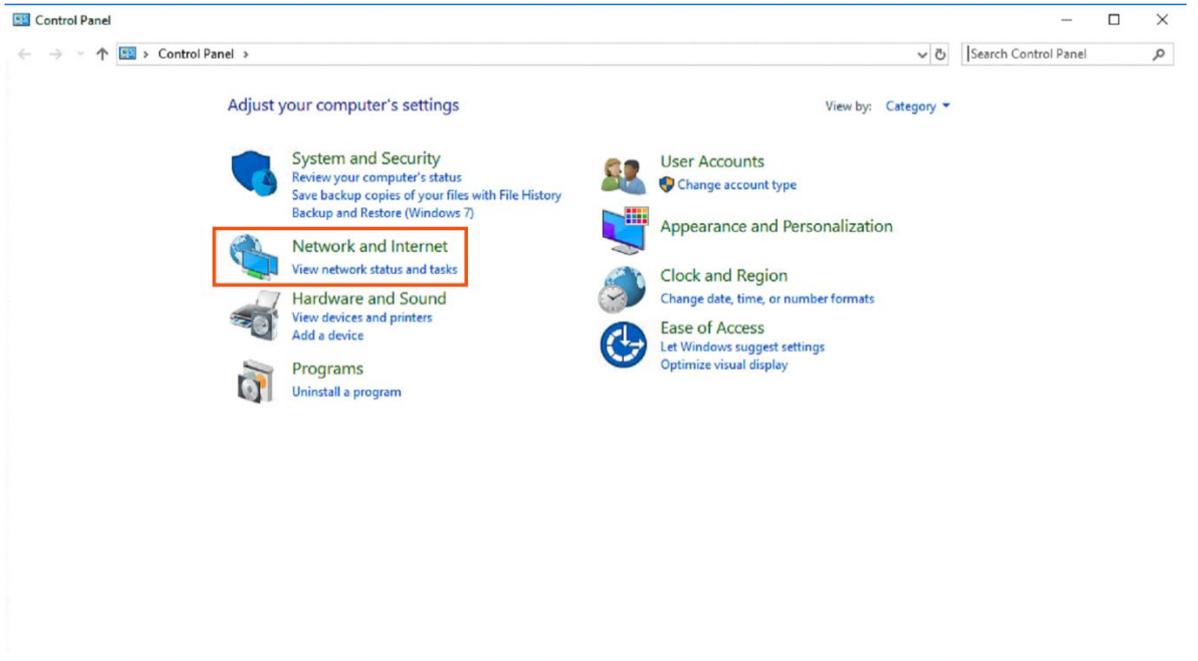
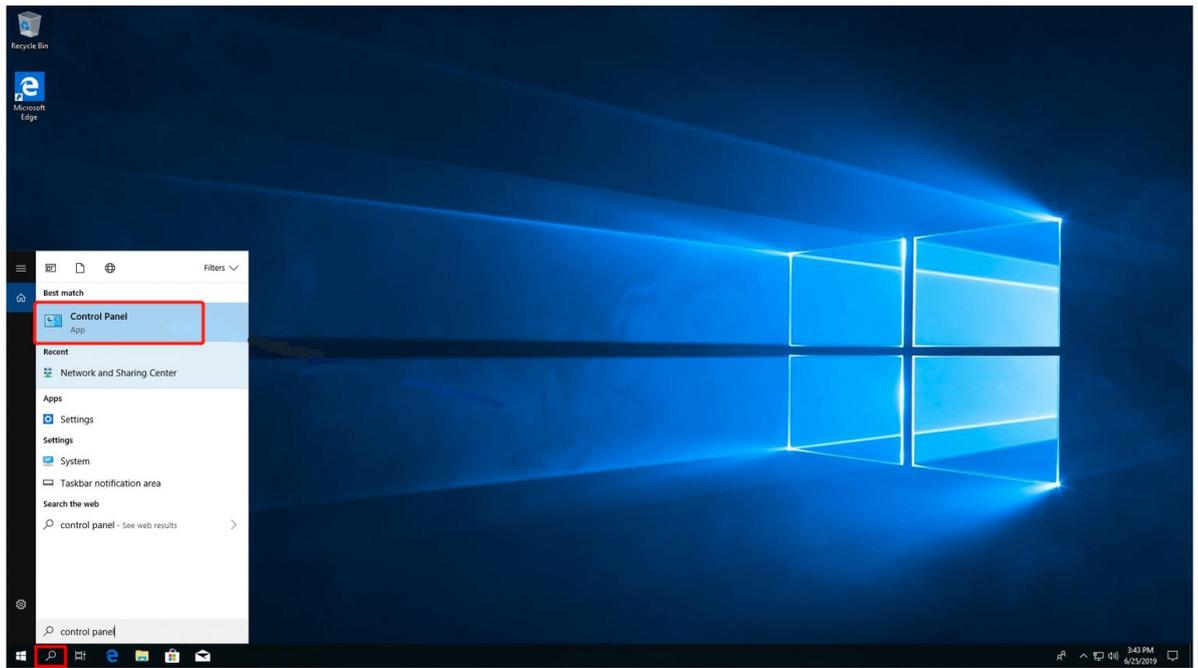


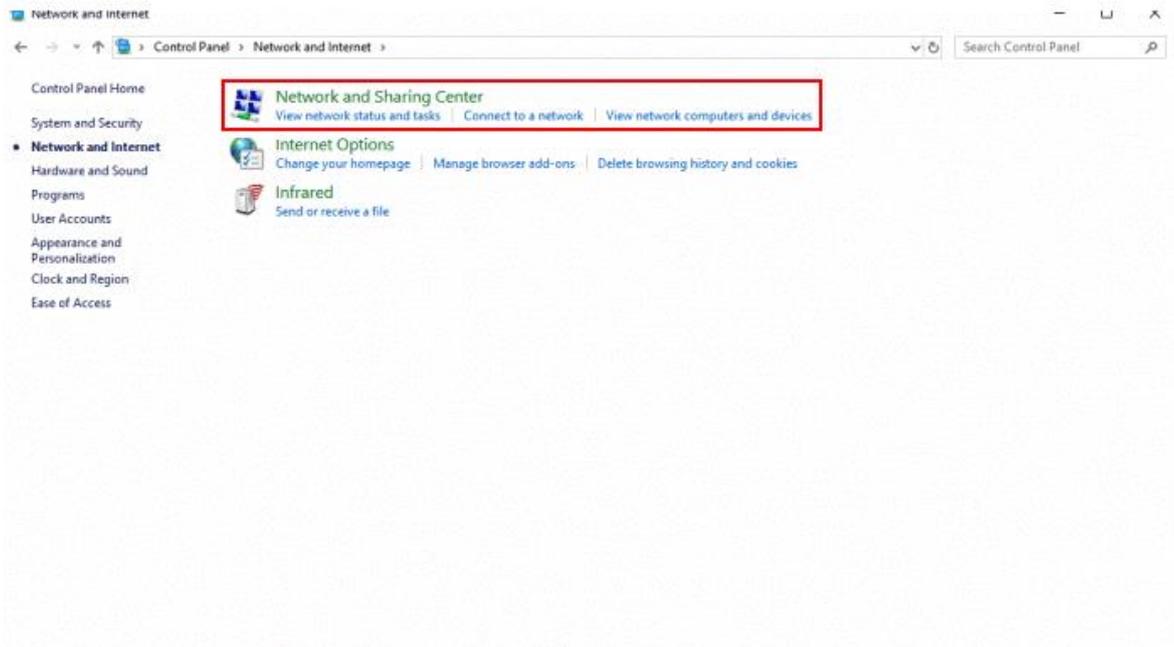
d Check the L2TP over IPsec connection status.



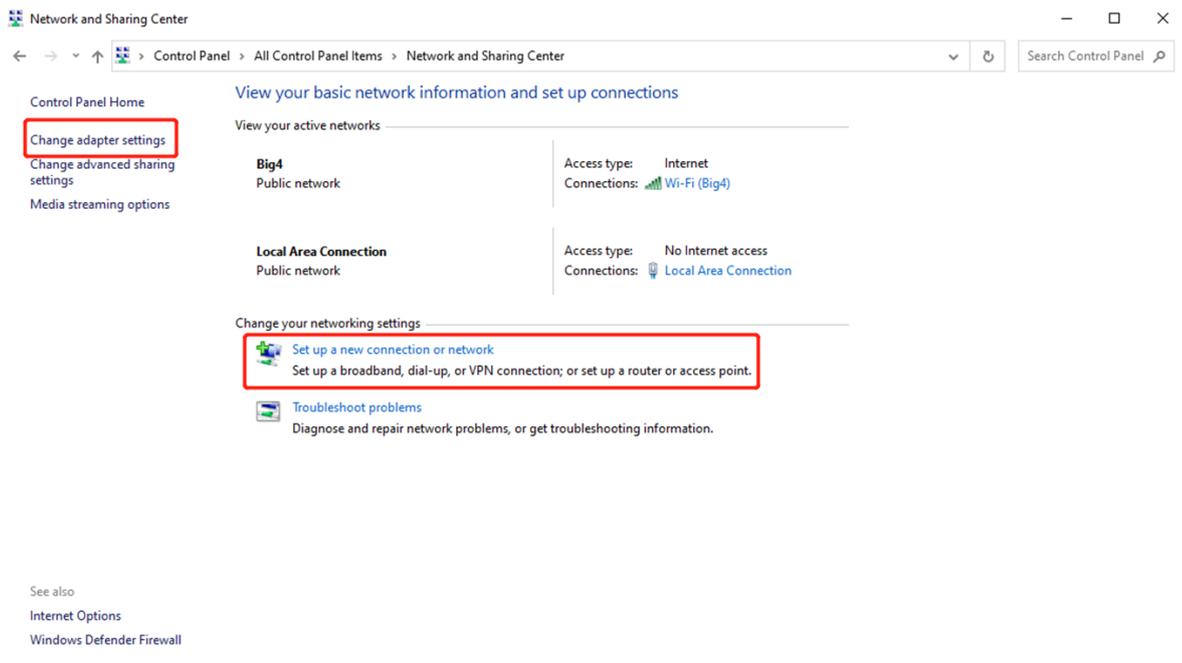
(3) Client side (Windows 10 is used as an example):

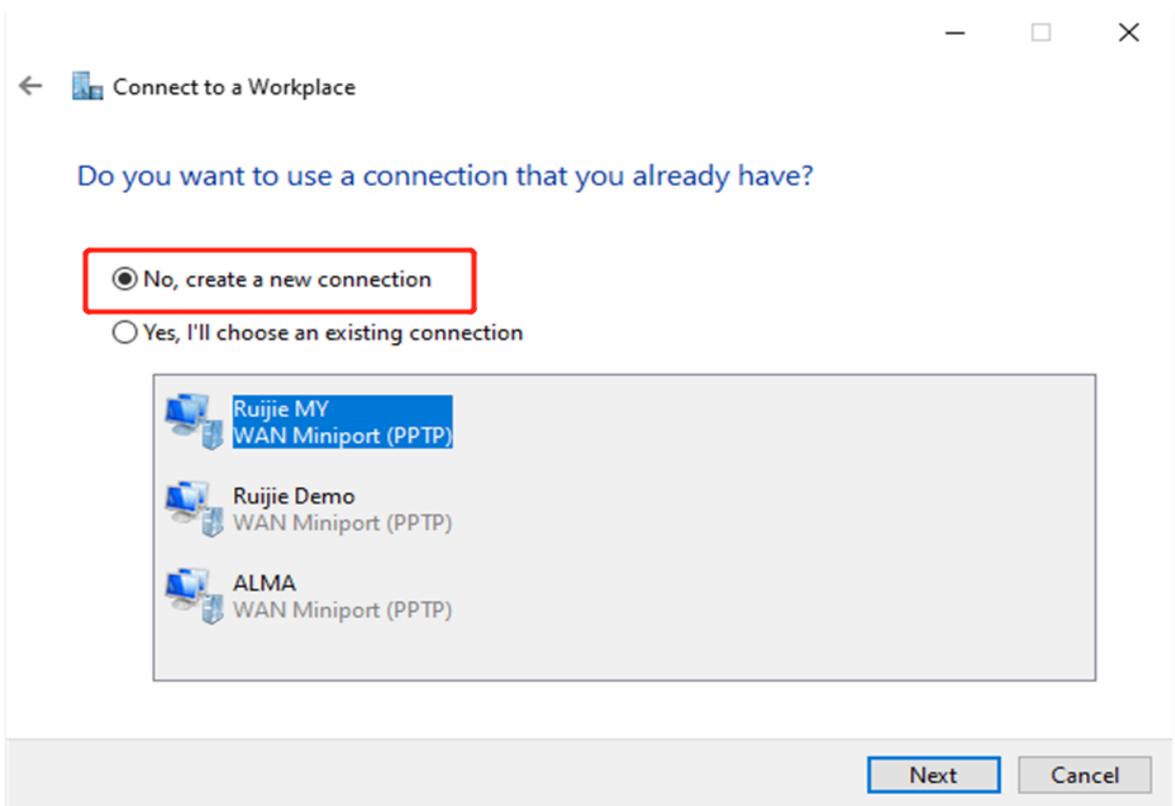
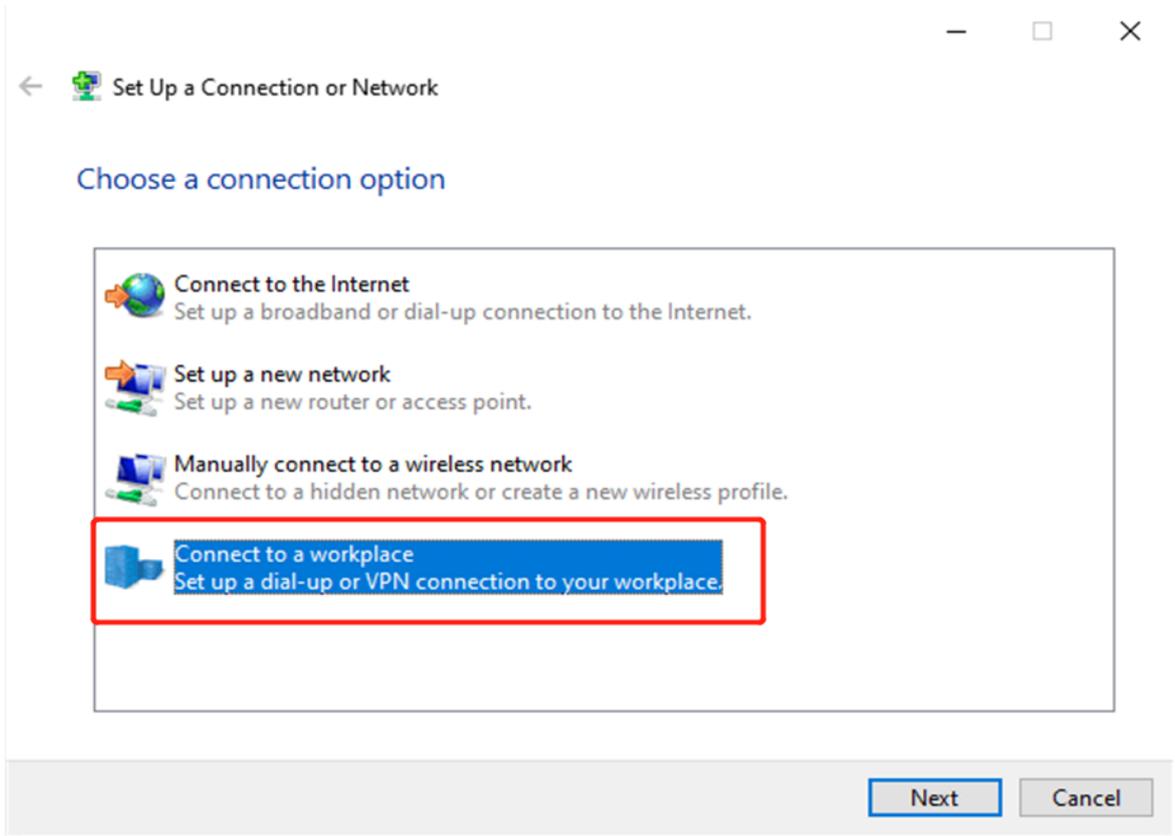
a Choose **Control Panel > Network and Internet > Network and Sharing Center**.

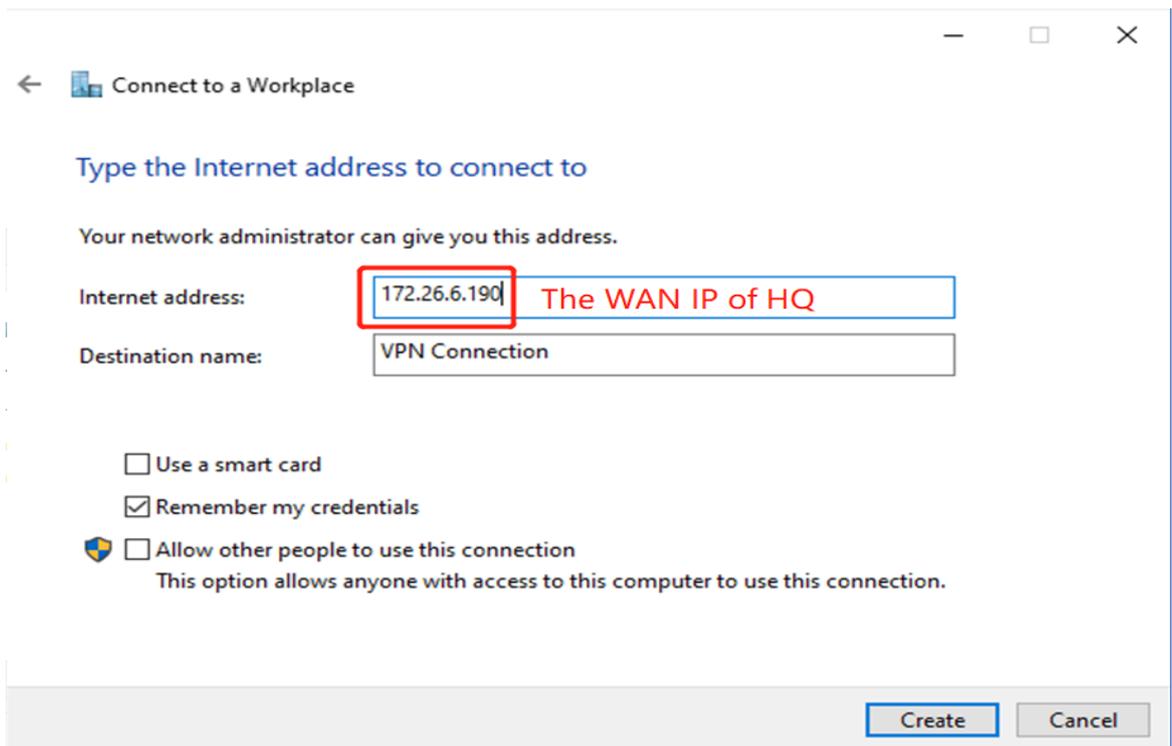
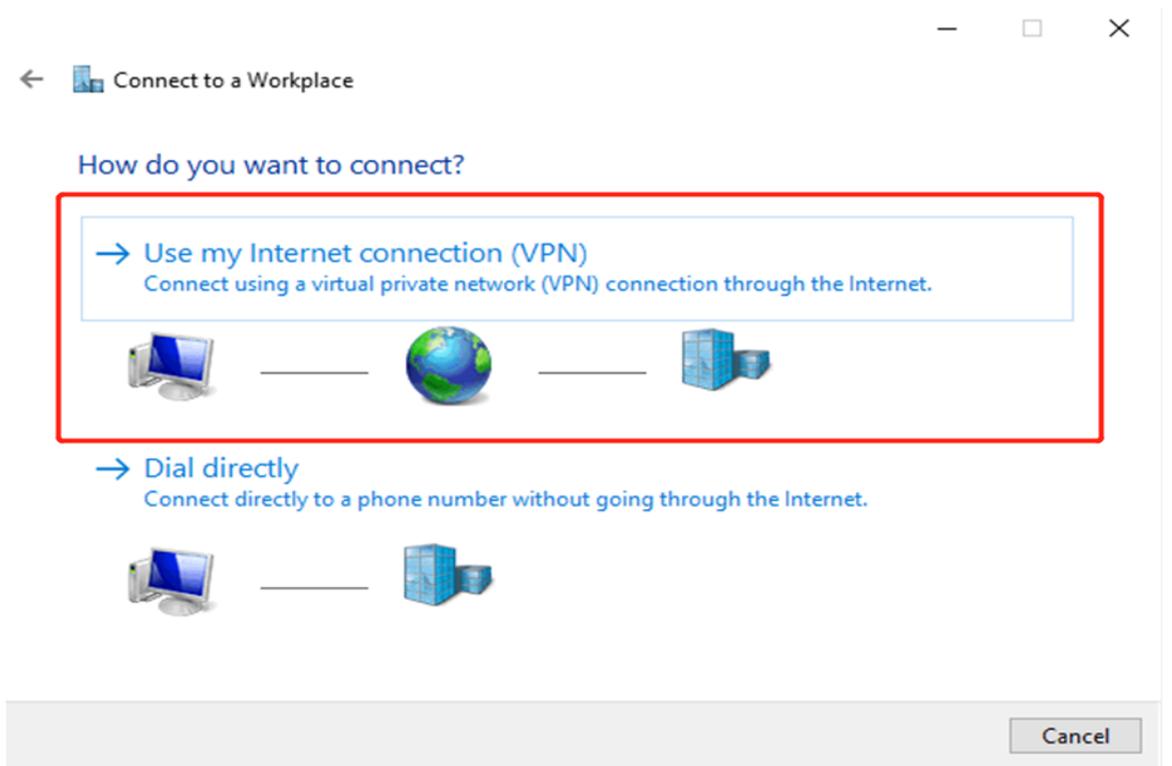




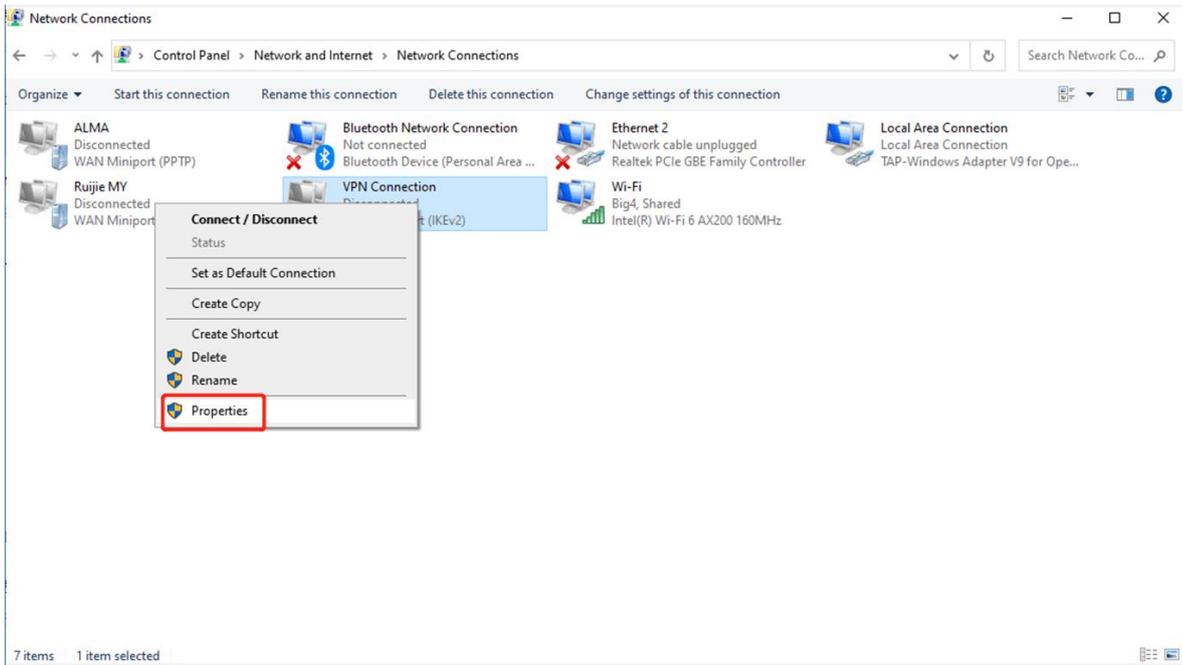
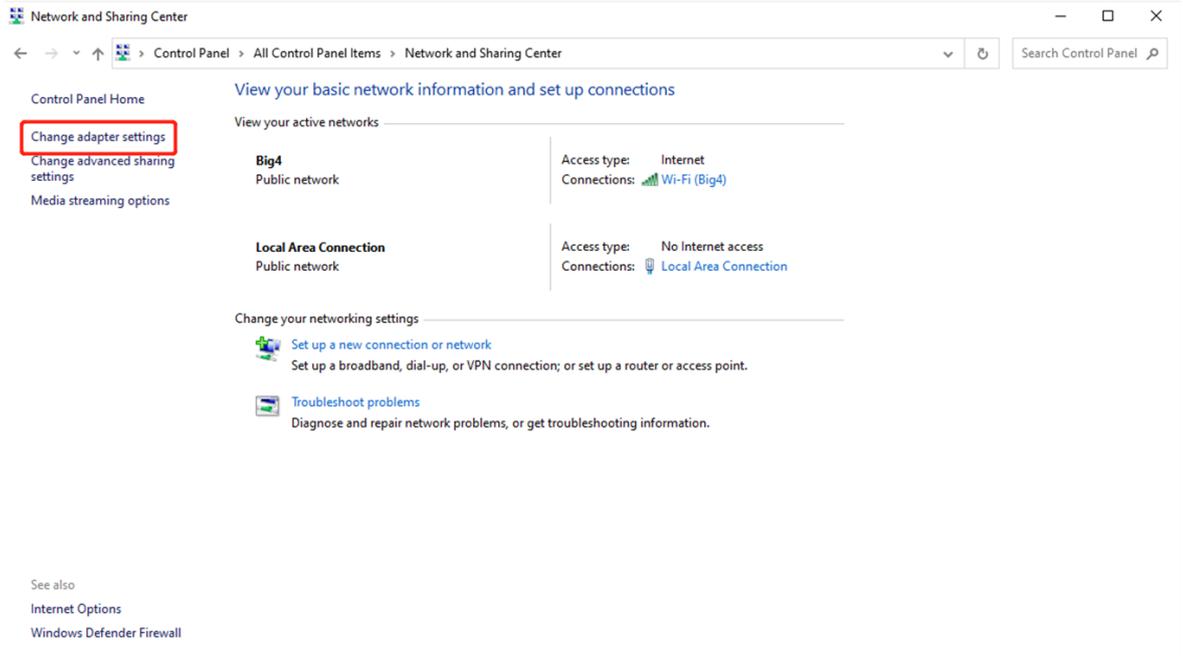
b Configure a VPN connection.

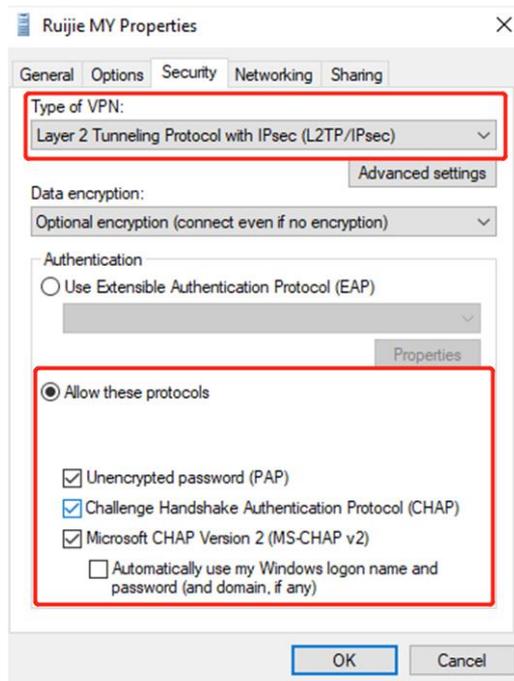




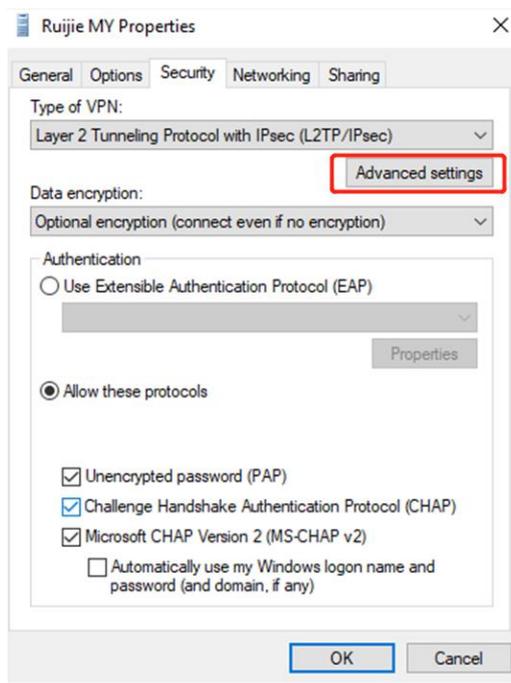


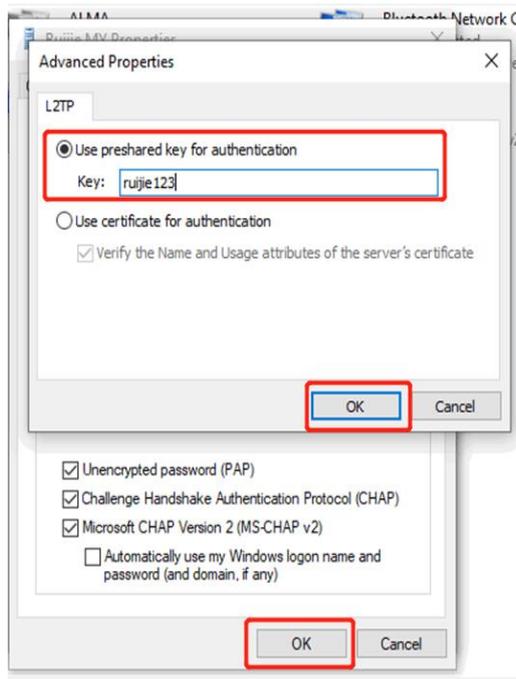
c Change adapter's settings.



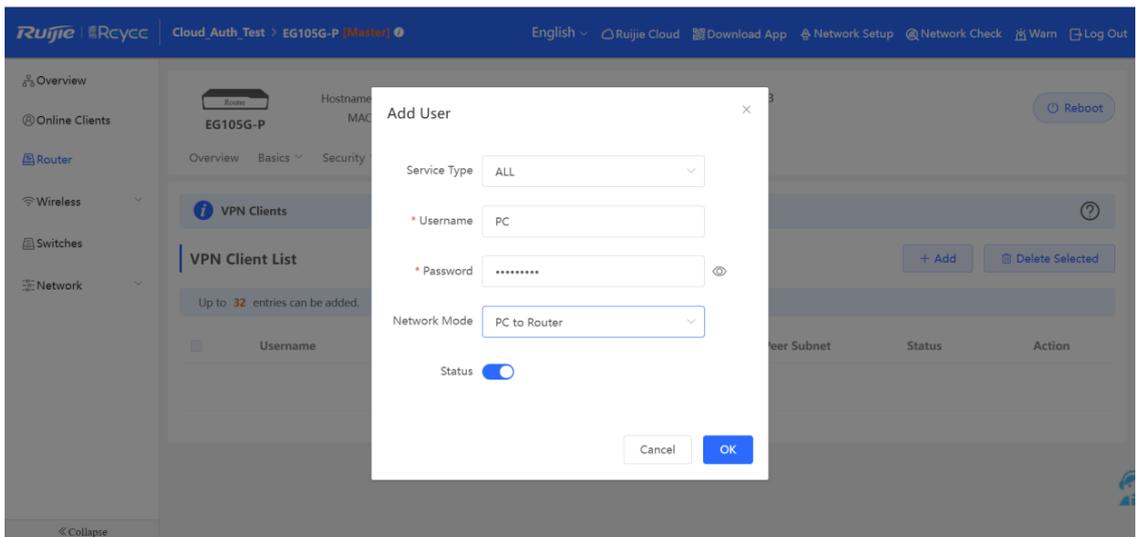


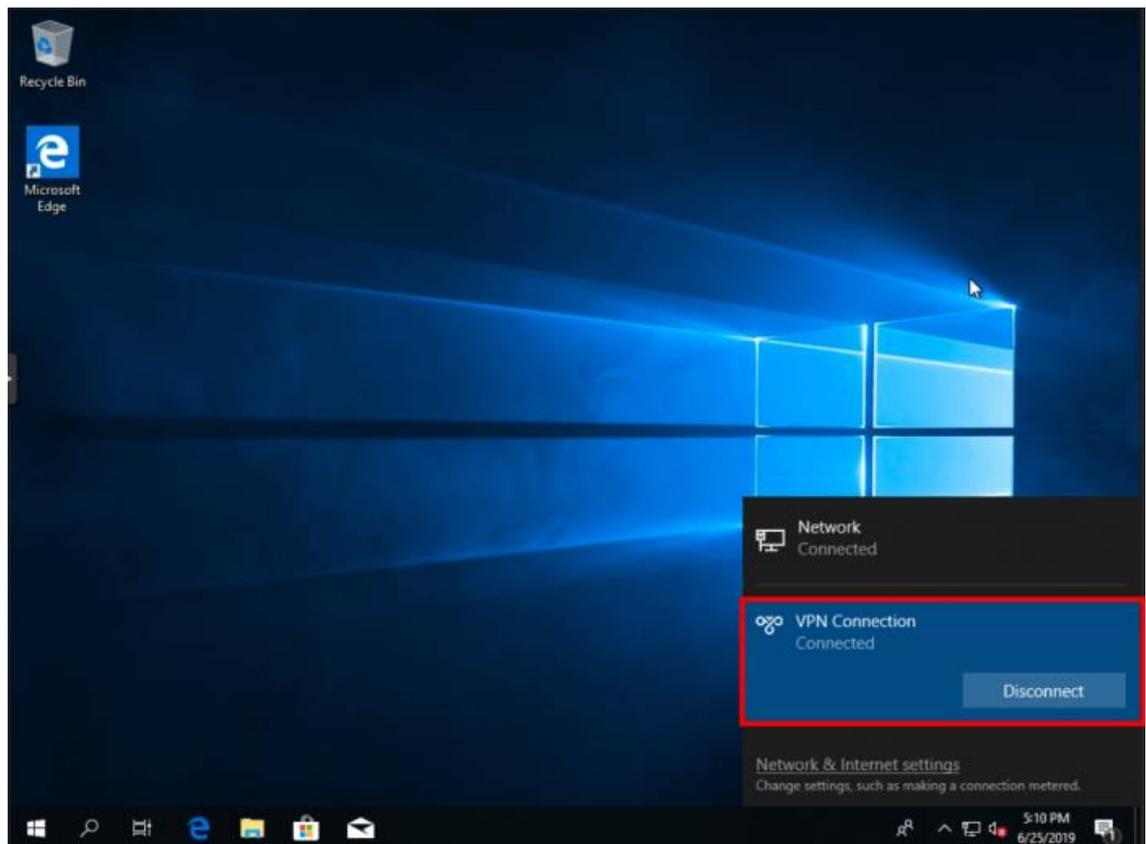
d Click **Advanced Settings** to configure the pre-shared password.





e Set Network Mode to PC to Router.



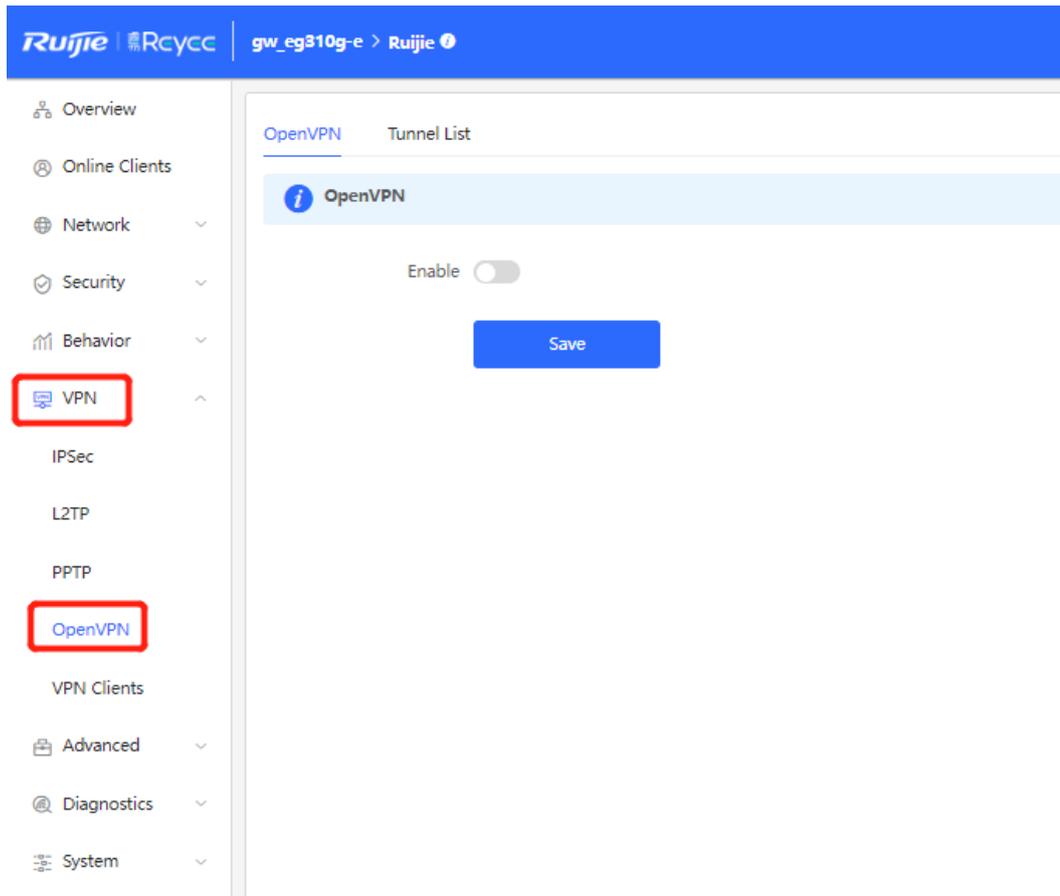


4.7.5 Open VPN

Open VPN is typically used in site-to-site and client-to-site scenarios. Open VPN is an application-layer VPN implementation based on the OpenSSL library. Compared with traditional VPN, open VPN is simple to use. VPN is a virtual private channel or a tunnel that provides secure data transmission between enterprises. Open VPN is full-featured SSL VPN that uses Layer 2 or Layer 3 secure network technology and industrial standard Secure Sockets Layer (SSL) or Transport Layer Security (TLS). SSL and TLS are security protocols that provide security and data integrity for network communications. Open VPN supports flexible client authorization modes, and supports certificates, usernames and passwords, allowing users to connect to the VPN through virtual interfaces. Open VPN is not the web proxy-based application or browser-based access.

(1) Headquarters side:

- a Log in to the Reyeeg EG with the default IP address of 192.168.110.1.
- b Switch to the **Local** mode. Choose **VPN > OpenVPN**.



c Enable **Open VPN** and configure VPN information.

[Collapse](#)

TLS Authentication ?

Allow Data Compression Yes ?

Route All Traffic over VPN Yes ?

Cipher AES-128-CBC ?

Deliver DNS 192.168.5.28 ? +

Auth SHA1

Client Config [Export](#)

[Save](#)

OpenVPN Tunnel List

OpenVPN

Enable

OpenVPN Type Server Client

Server Mode

Protocol

* Server Address

* Port ID 1-65535

* IP Range ?

Deliver Route ? +

Flow Control Disable Enable

----- Expand -----

Client Config

- **OpenVPN Type:** Select **Server** or **Client** as needed
- **Server Mode:** Select an authentication mode.
 - Account: You have to enter the correct account password, and import the CA certificate file on the client.
 - Certificate: You have to import the correct CA certificate, client certificate, and private key file on the client.
 - Account & Certificate: You have to enter the correct account password and import the correct CA certificate, client certificate, and private key file on the client.
 - **Protocol:** Select **TCP** or **UDP**.
- **Server Address:** Enter the WAN IP address or domain name.
- **Port ID:** Use port 1194 by default.
- **IP Range:** Assign IP addresses in the range to clients.
- **Deliver Route:** The route of the client is used when the client accesses the intranet of the server.
- **Advanced configuration:**
 - **TLS authentication:** A VPN connection is secured with the TLS key.
 - **Allow Data Compression:** The value is **Yes** by default.

- **Route All Traffic over VPN:** The value is **No** by default.
 - **Cipher:** You can select a data encryption algorithm. AES-128-CBC is used by default.
 - **Deliver DNS:** A DNS address is assigned to a client.
 - **Auth:** SHA1 is used by default.
- d Click **Save** to save the configuration and click **Export** to export client configuration.

OpenVPN Tunnel List

OpenVPN

Enable

OpenVPN Type Server Client

Server Mode

Protocol

* Server Address

* Port ID 1-65535

* IP Range ?

Deliver Route ? +

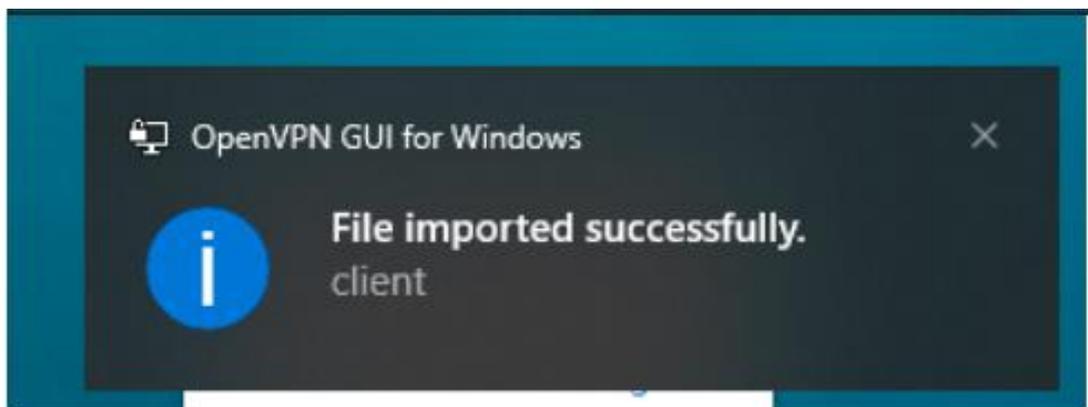
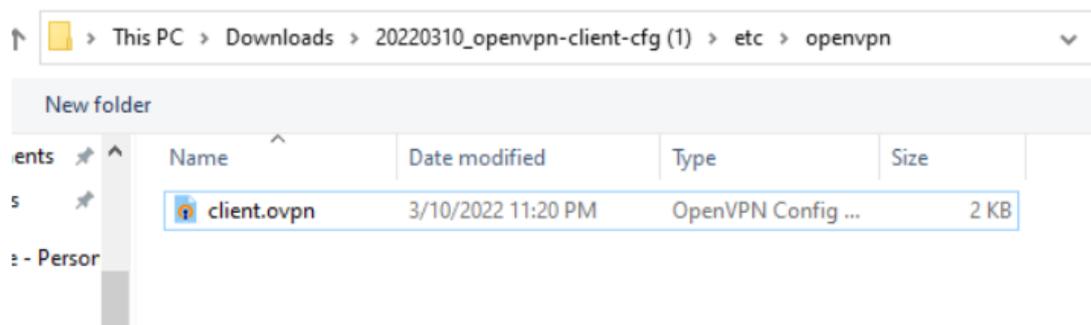
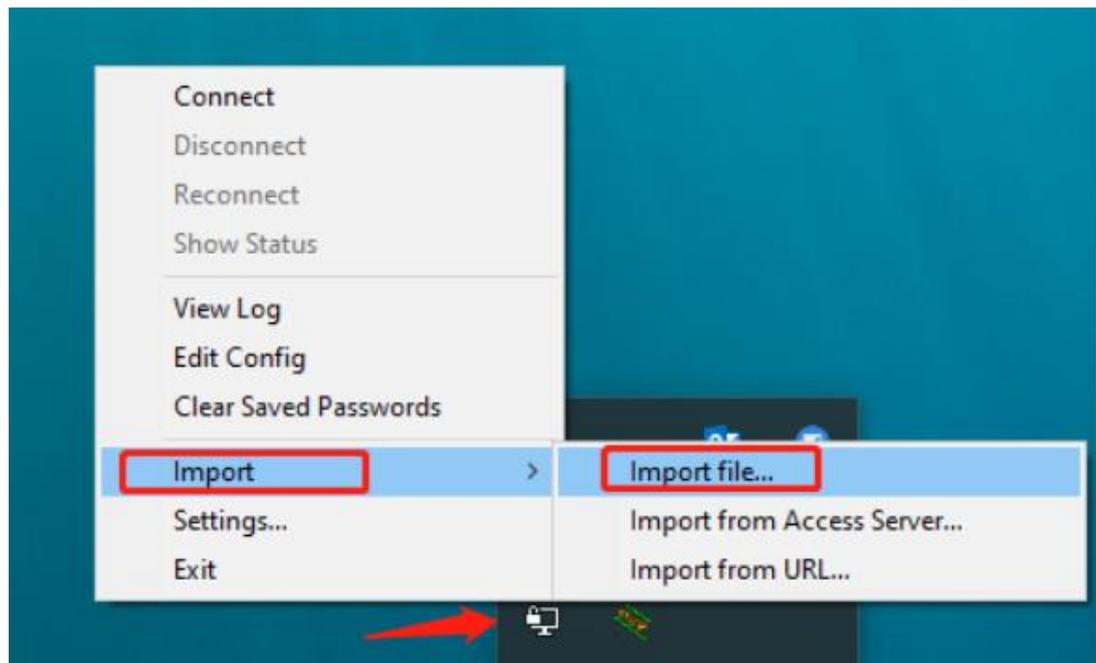
Flow Control Disable Enable

----- Expand -----

Client Config

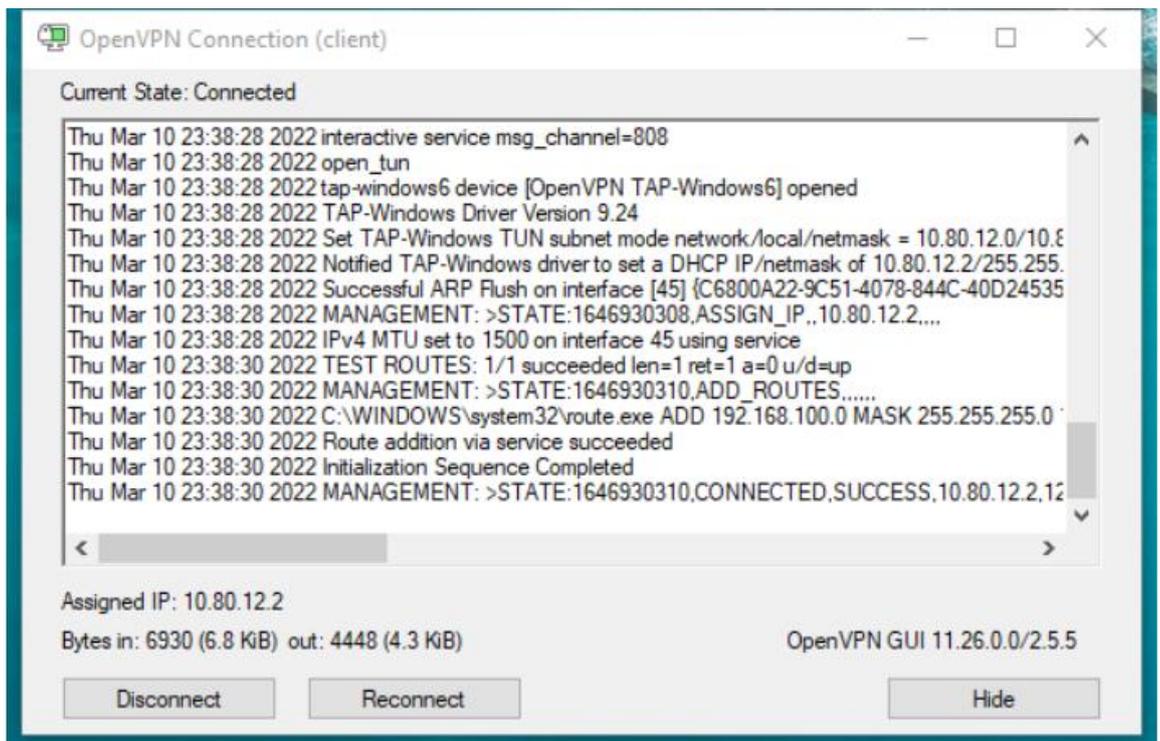
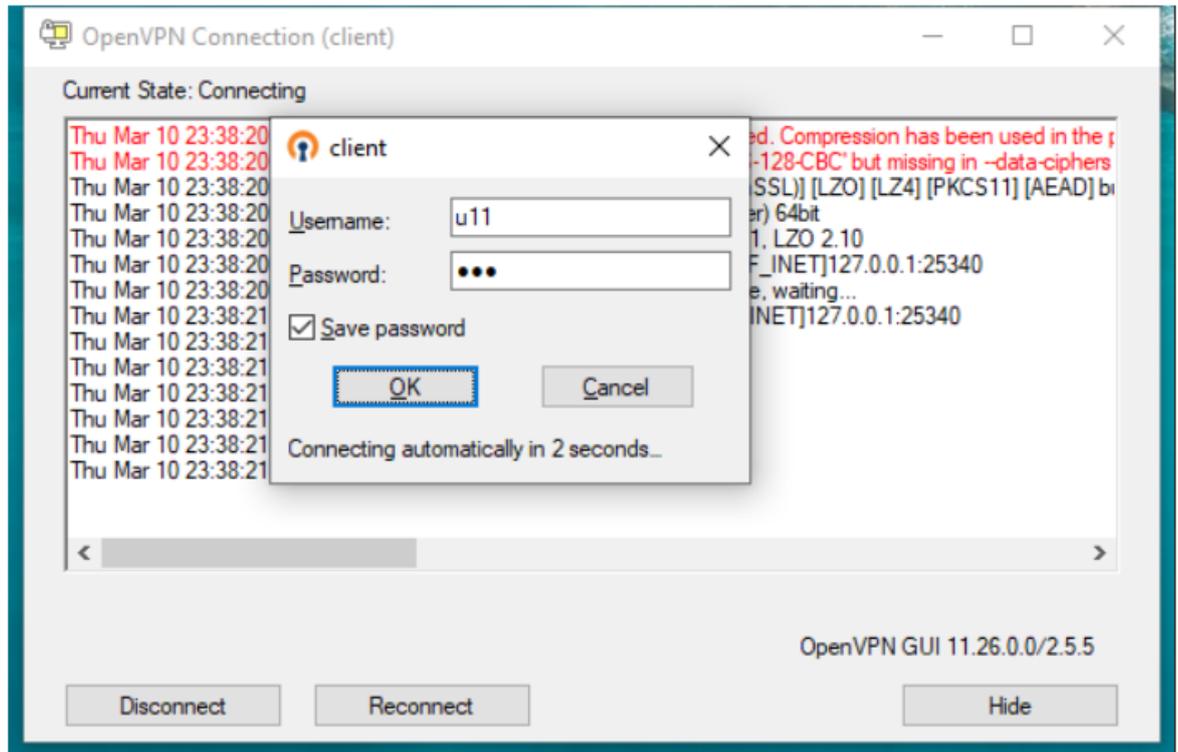
(2) Client side (Windows 10 is used as example):

- Download and install OpenVPN application to your PC.
You can download OpenVPN client at <https://openvpn.net/community-downloads/>. Select a suitable version for your PC.
- Import client configuration to the OpenVPN client after the OpenVPN client is installed on your PC.
 - Export the client configuration on the web page.
 - Right-click **OpenVPN** and choose **Import > Import file...** to import the client configuration on the client.



After the message "File Imported successfully" appears, you can connect to the VPN.

- c Click **OpenVPN** and select **Connect**. If you use the account authentication method, enter your VPN account.



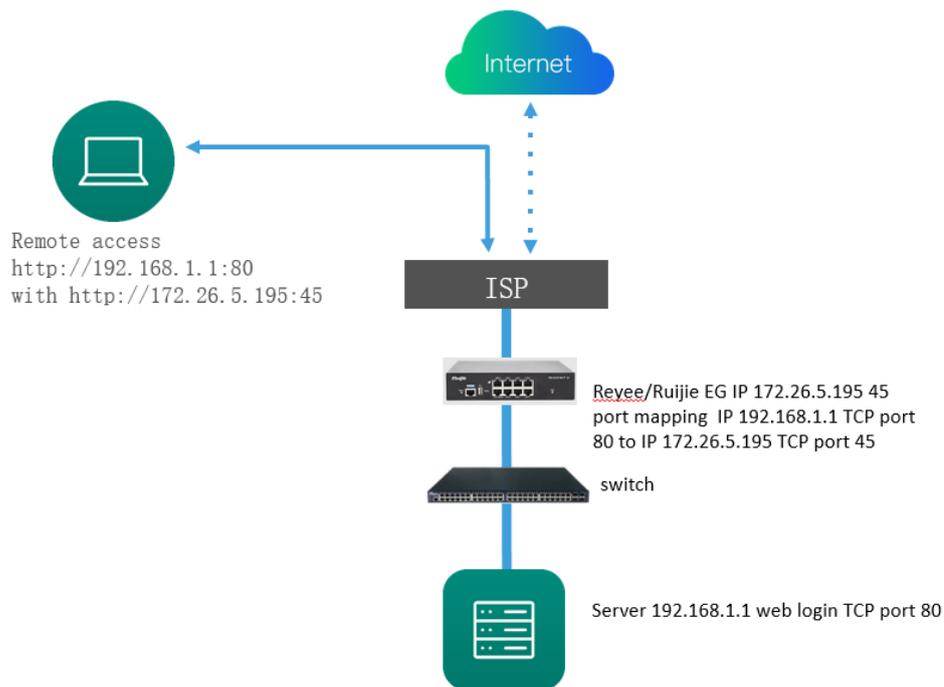
4.8 Port Mapping

Port mapping is used to map the internal server IP address and port number to external IP address so that extranet staffs can access internal servers. The difference between port mapping and DMZ is that port mapping only map one or more ports, but DMZ will map all ports.

- Typical scenario of port mapping

The port mapping function can establish a mapping relationship between the IP address and port number of a WAN port and the IP address and port number of a server on the LAN, so that all access traffic destined for a service port of the WAN port is redirected to the corresponding port of the specified LAN server. This function enables external users to proactively access the service host on the LAN through the IP address and port number of the specified WAN port.

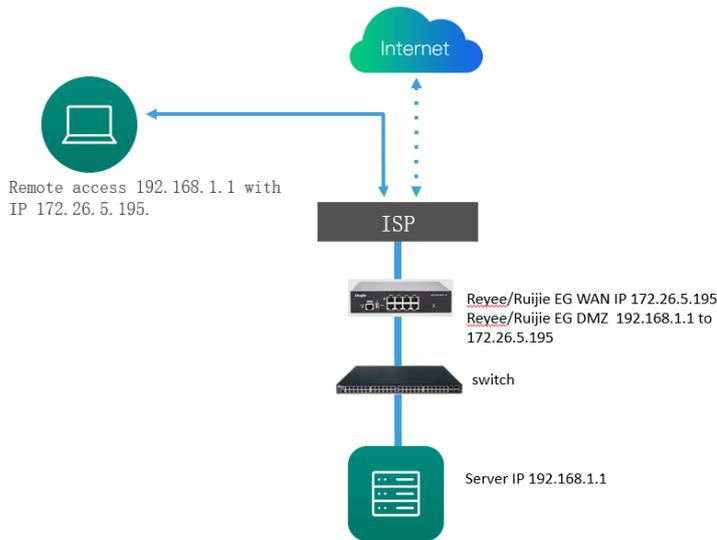
Port mapping enables users to access cameras or computers on their home networks when they are in companies or on a business trip.



- Typical scenario of DMZ

When an incoming data packet does not hit any port mapping entry, the packet is redirected to the LAN server according to the Demilitarized Zone (DMZ) rule. All data packets proactively sent from the Internet to the device are forwarded to the designated DMZ host, realizing LAN server access of external network users. DMZ provides the external network access service while ensuring security of other hosts on the LAN.

Port mapping or DMZ is used when an external network user wants to access the LAN server, for example, access a server deployed on the intranet when the user is in the enterprise or on a business trip.



4.8.1 Configuring Port Mapping

- (1) Switch to the **Local** mode. Choose **Advanced > Port Mapping > Port Mapping**.
- (2) Click **Add**. In the dialog box that appears, enter the rule name, service type, protocol type, external port/range, internal server IP address, and internal port/range. You can create a maximum of 50 port mapping rules.

Port Mapping NAT-DMZ

Port Mapping ⓘ

Port Mapping List + Add Delete Selected

Up to **50** entries can be added.

<input type="checkbox"/>	Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Action
<input type="checkbox"/>	test	TCP	172.26.1.200	3389	192.168.110.236	80	Edit Delete

Add
×

* Name

Preferred Server

Protocol

External IP Address Outbound Interface
 Enter or select an IP address.

* External Port/Range

* Internal IP Address

* Internal Port/Range

Table 4-5 Port Mapping Configuration

Parameter	Description
Name	Enter the description of a port mapping rule, which is used to identify the rule.
Preferred Server	Select the type of a service to be mapped, such as HTTP or FTP. The internal port number commonly used by the service is automatically entered. If the service type is unknown, select Custom .
Protocol	Select the transmission layer protocol type used by a service, such as TCP or UDP. The value ALL indicates that the rule applies to both protocols. The value must comply with the client configuration of the service.
External IP Address	Specify the host address used for accessing the external network. Outbound Interface: You can select All WAN Ports or specify a WAN port. Enter or select an IP address: Select or enter the IP address of a WAN port.

Parameter	Description
External Port/Range	Specify the port number used for Internet access. You need to confirm the port number in the client software, such as the camera monitoring software. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the value of Internal Port/Range must also be a port range.
Internal IP Address	Specify the IP address of the internal server to be mapped to the WAN port, that is, the IP address of the LAN device that provides Internet access, such as the IP address of a network camera.
Internal Port/Range	Specify the service port number of the internal server to be mapped to the WAN port, that is, the port number of the application that provides Internet access, such as port 8080 of the web service. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the number of ports must be the same as that specified in External Port/Range .

- (3) Check whether the external network device can access services on the destination host using the external IP address and external port number.

4.8.2 Configuring NAT-DMZ

- (1) Switch to the **Local** mode. Choose **Advanced > Port Mapping > NAT-DMZ**.
- (2) Click **Add**. Enter the rule name and internal server IP address, select the interface to which the rule applies, specify the rule status, and click **OK**. You can configure only one DMZ rule for an outbound interface.

Port Mapping [NAT-DMZ](#)

NAT-DMZ ?
You can view NAT-DMZ settings and edit or delete the rule.

NAT-DMZ Rule List + Add Delete Selected

There are **3** outbound interfaces. Up to **3** rules can be added.

<input type="checkbox"/>	Name	Outbound Interface	Dest IP Address	Status	Action
<input type="checkbox"/>	test	WAN1	192.168.110.222	Enable ☺	Edit Delete

Add Rule
×

* Name

* Dest IP Address

Outbound Interface WAN ▼

Status

Cancel
OK

Table 4-1 DMZ Rule Configuration

Parameter	Description
Name	Enter the description of a mapping rule, which is identify the rule.
Dest IP Address	Specify the IP address of the DMZ host to which packets are redirected, that is, the IP address of the internal server that can be accessed from the Internet.
Outbound Interface	Specify the WAN port in the DMZ rule. You can configure only one rule for a WAN port.
Status	Specify whether the rule is effective. The rule is effective when Status is enabled.

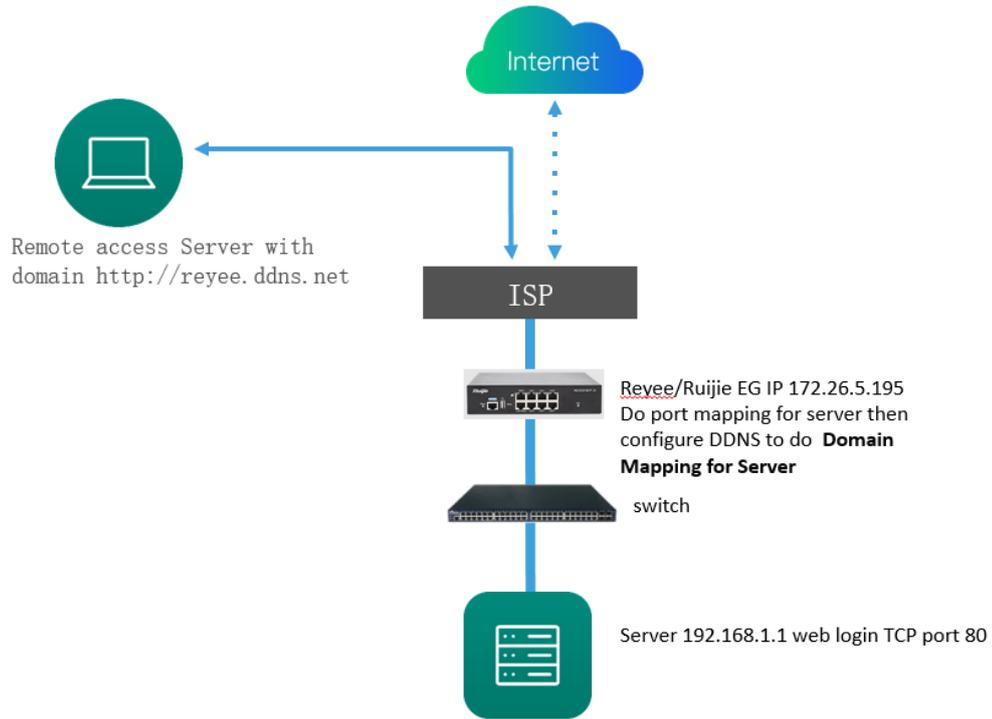
Caution

When both DMZ and port mapping are configured, port mapping takes precedence.

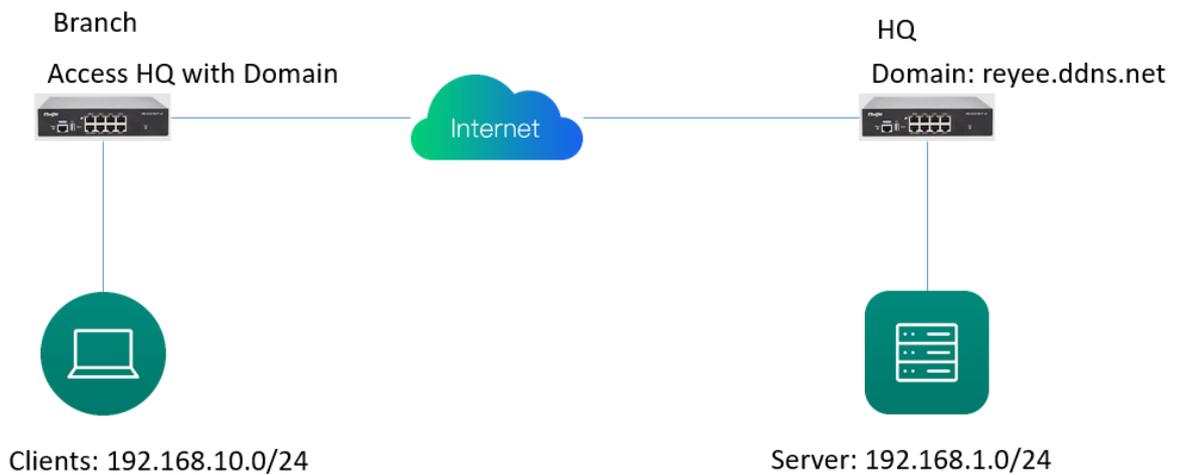
4.9 Dynamic DNS

Dynamic Domain Name Server (DDNS) is to map a user's dynamic IP address to a fixed domain name. Each time a user connects to the network, the client program will transfer the dynamic IP address of the user host to the server program located on a host of a service provider. Then the server program is responsible for providing DNS services and implementing dynamic domain name resolution.

- Server access with the domain name

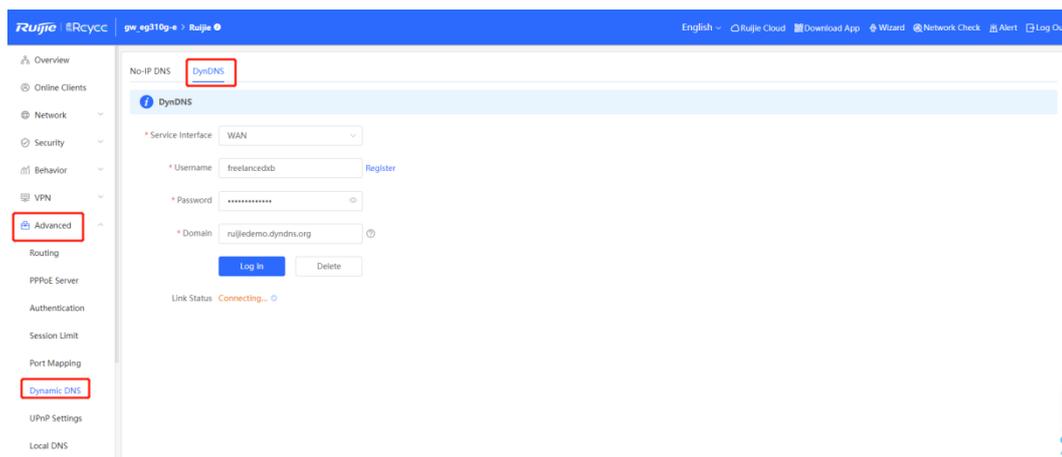


- VPN connection with the domain name

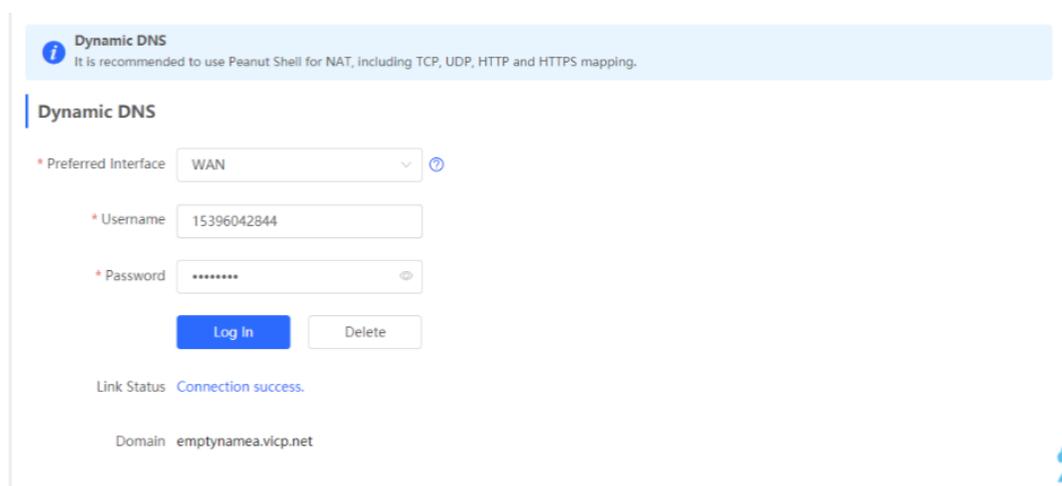


(1) Switch to the **Local** mode. Choose **Advanced > Dynamic DNS**.

There are three DDNS servers you can choose to connect: Peanut Shell DDNS, NO-IP DNS, and DynDNS.



- (2) When Peanut Shell DDNS is used, you are advised to use WeChat or Peanut Shell to scan the QR code to register an account.
- (3) You can use the value of **Domain** to access the intranet server or headquarters device.



4.10 Authentication

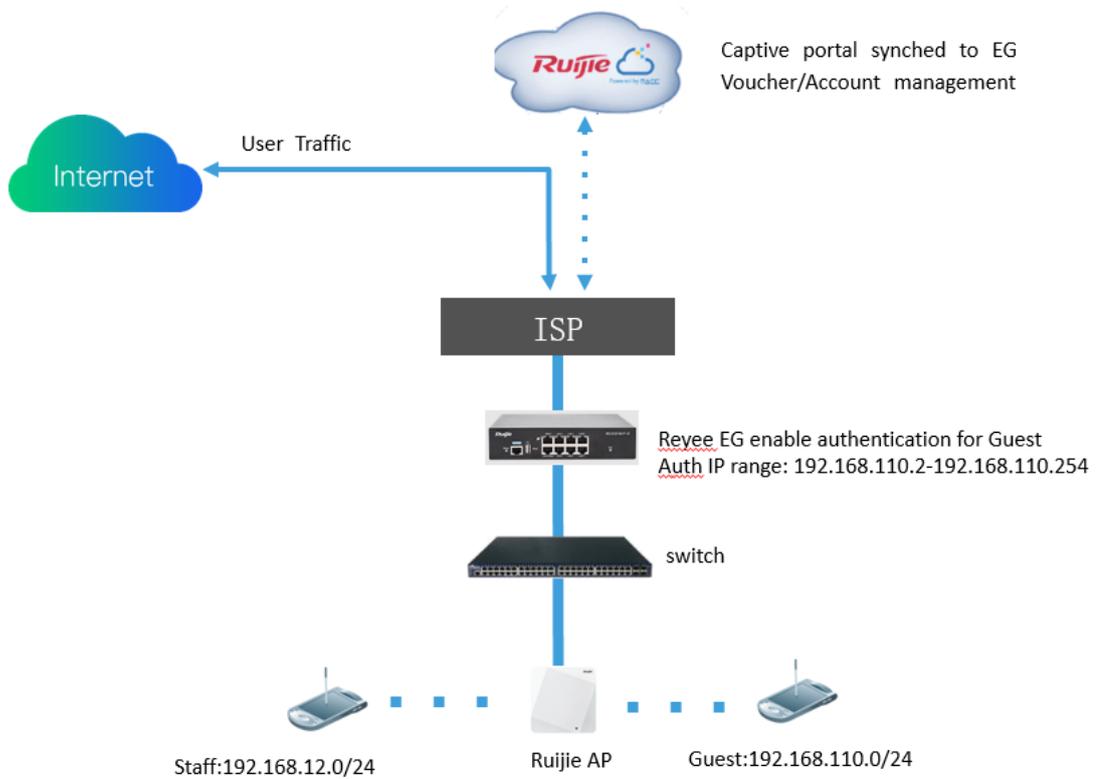
4.10.1 Application Scenario

As wireless networks become popular, Wi-Fi has become one of the marketing means for merchants. Users can connect to Wi-Fi provided by the merchants to surf the Internet after watching advertisements or following WeChat official accounts. In addition, to defend against security vulnerabilities, a wireless office network usually allows only employees to associate with Wi-Fi, so identities of clients need to be verified.

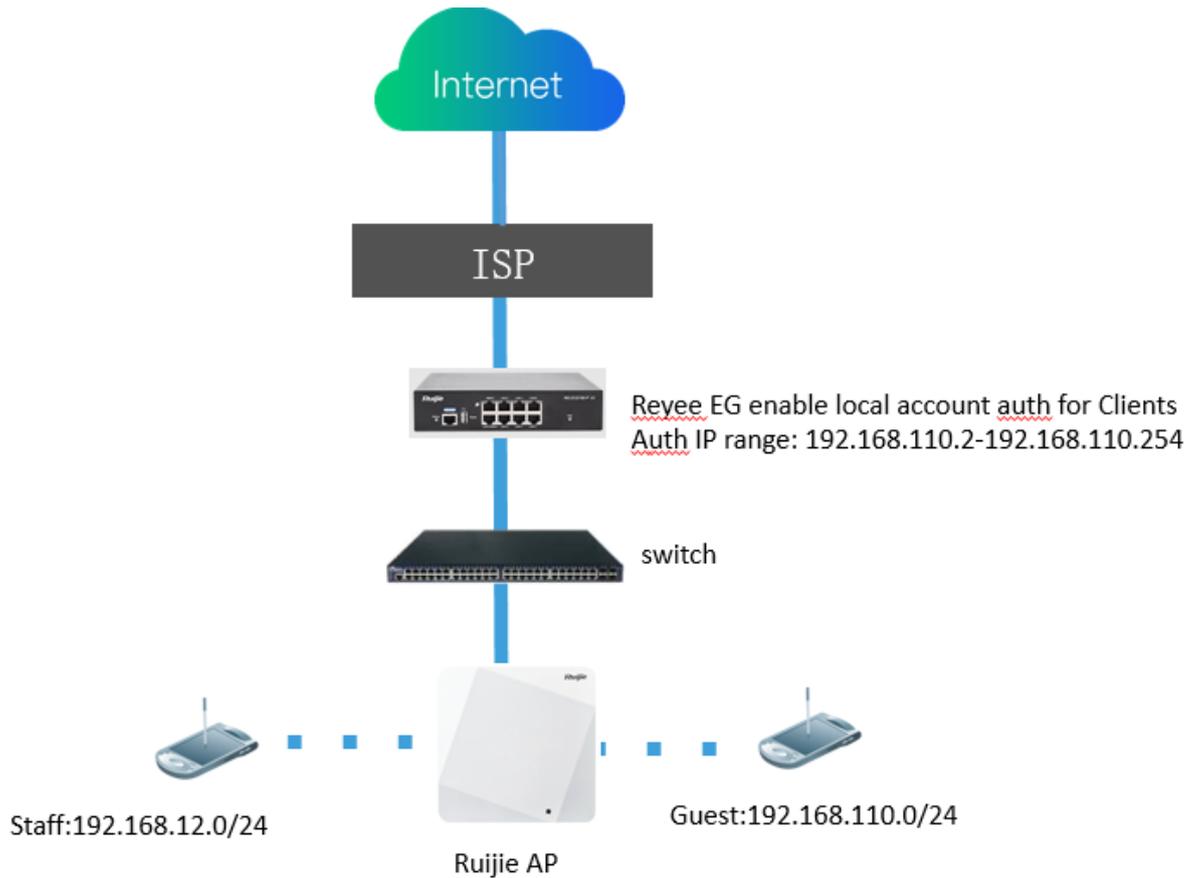
The device uses portal authentication to implement information display and user management. After users connect to Wi-Fi, traffic is not routed to the Internet. Wi-Fi users must pass authentication at the Portal authentication website, and only authenticated users are allowed to use network resources. Merchants or enterprises can customize Portal pages for identity authentication and advertisement display.

- (1) Before you enable Wi-Fi authentication, ensure that wireless signals are stable and users can connect to Wi-Fi and surf the Internet normally. The wireless SSID used for authentication on a network should be set to **open**. Encryption may lead to exceptions during Wi-Fi interconnection through authentication.
- (2) If the IP address of an AP on a network is within the authentication scope, add the AP as the authentication-free user. For details, see section [4.2.10.7 Authentication-Free](#).

- On a Layer 2 network, add the MAC address of the AP to the authentication-free MAC address whitelist.
- On a Layer 3 network, add the IP address of the AP to the authentication-free IP address whitelist.
- **Cloud authentication scenario**



- **Local account authentication scenario**



4.10.2 Cloud Authentication

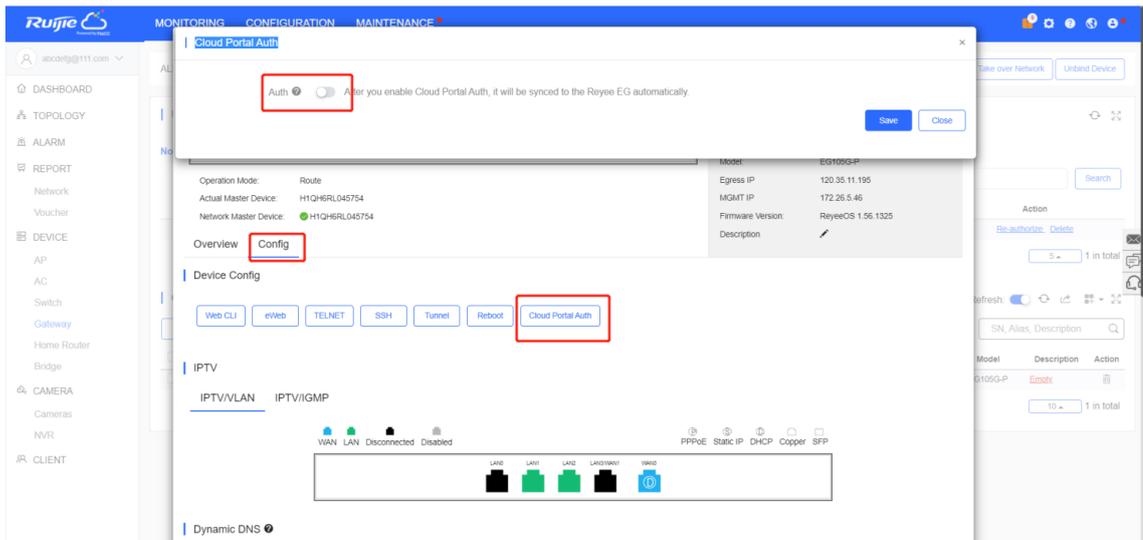
Reyee EG devices support cloud portal authentication, including one-click, voucher, account, SMS (integration with Twilio) authentication modes.

- (1) Configure cloud authentication on the cloud, and click the SN of the EG to access the page of EG details.

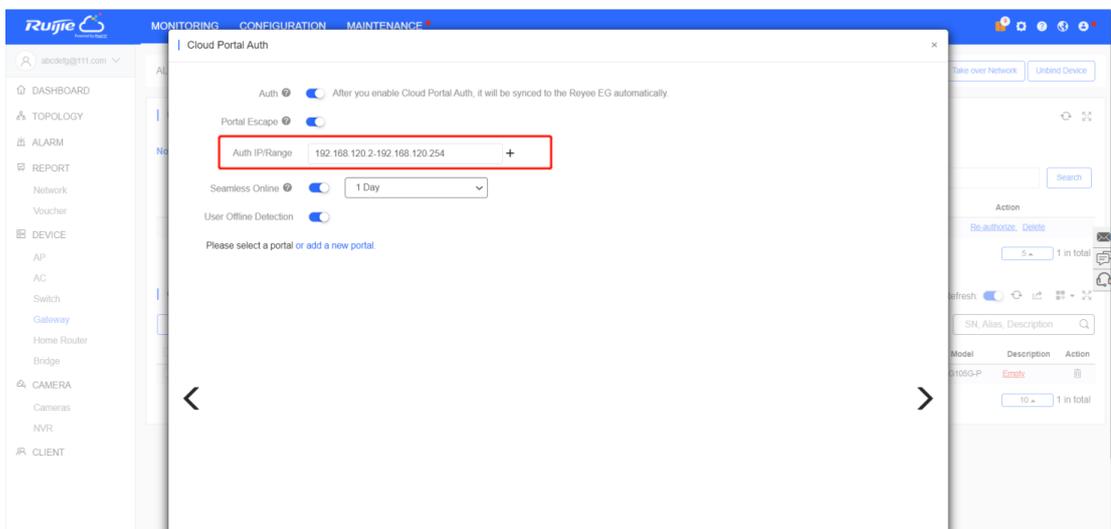
The screenshot shows the 'Gateway List' table in the management interface. The table has columns for Status, SN, Alias, MGMT IP, MAC, Egress IP, Network, Firmware Version, Offline Time, Model, Description, and Action. A single entry is shown, with the SN field highlighted in red.

Status	SN	Alias	MGMT IP	MAC	Egress IP	Network	Firmware Version	Offline Time	Model	Description	Action
Online	1122870173254	Bullie	172.26.5.46	ec29 7017.3935	120.35.11.195	Bullie-Hostel	ReyeeOS 1.56.1325	-	EG105G-P	Empty	

- (2) Choose **Config > Cloud Portal Auth**.



- (3) Enter the value of **Auth IP/Range** for the user that needs to be authenticated before Internet access.

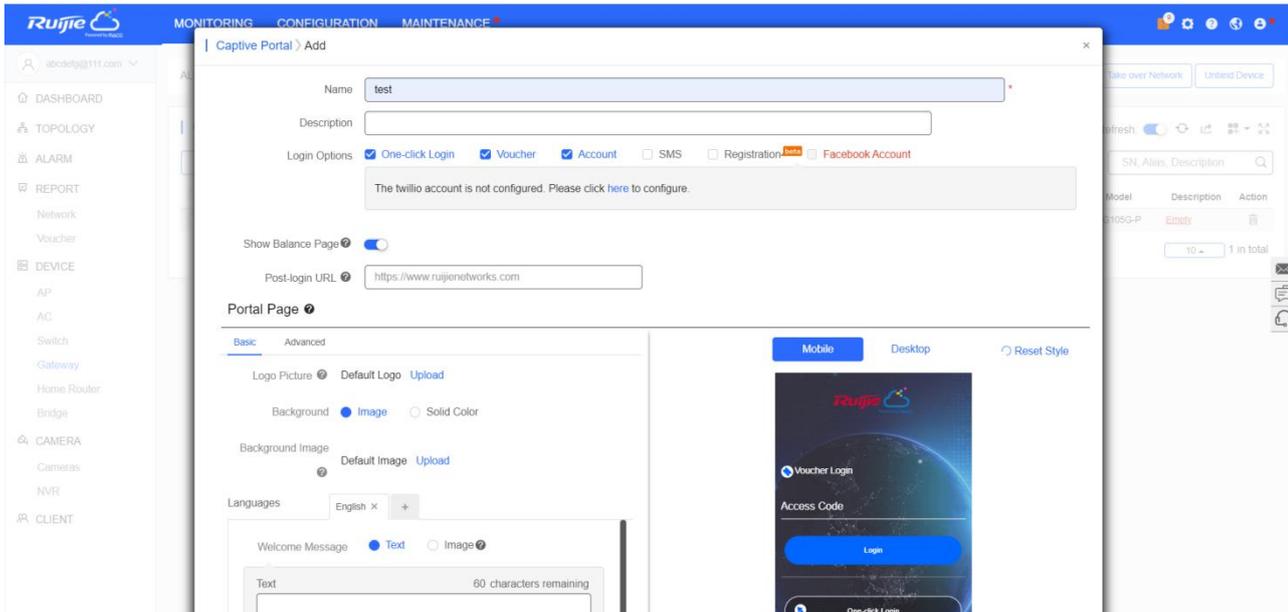


Portal Escape: When the cloud server goes Down, this function enables clients to access the Internet directly without authentication.

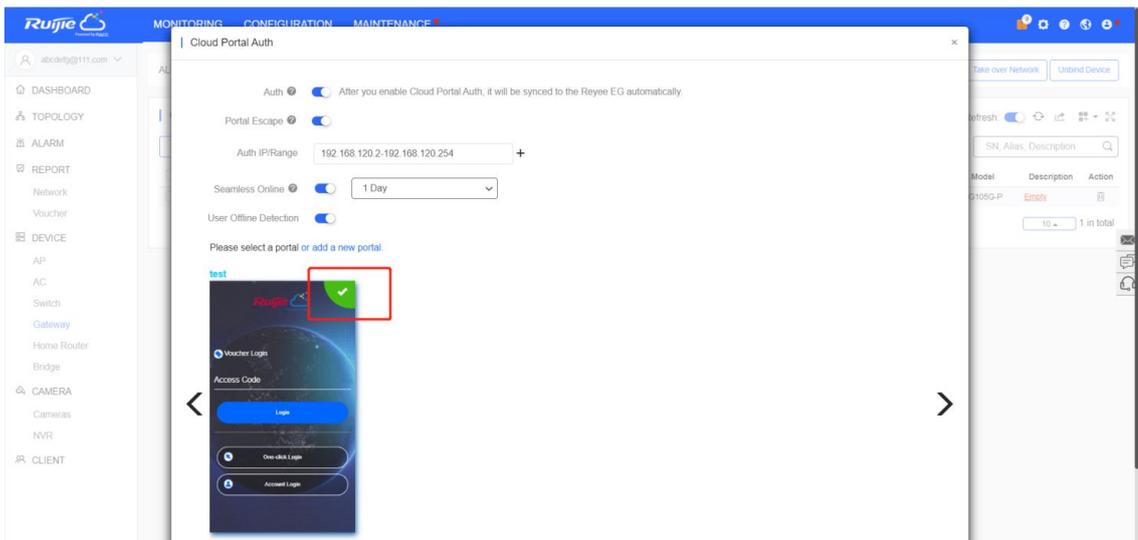
Seamless Online: Users only need to pass the authentication once. If they want to go online again, authentication is not required. After users go online, they do not need to log in again in the specified period. You can choose **1 Day**, **1 Week**, **1 Month**, or **Always**.

User Offline Detection: Users do not access the Internet after the validity period.

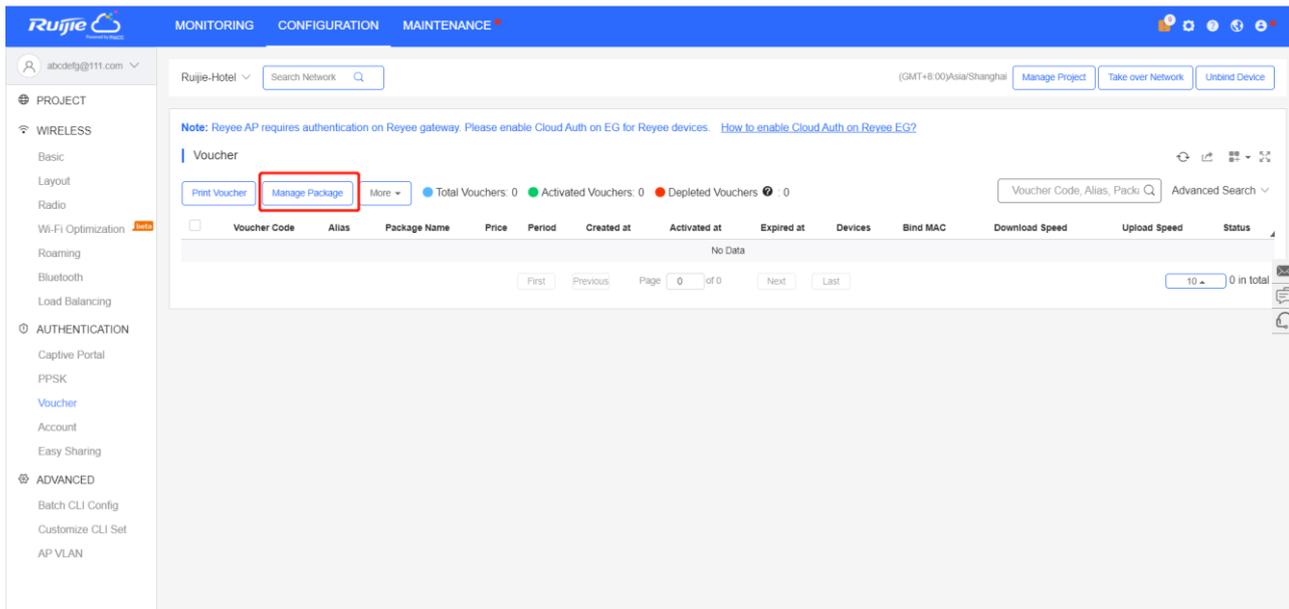
- (4) Click **add a new portal** to add a portal page.



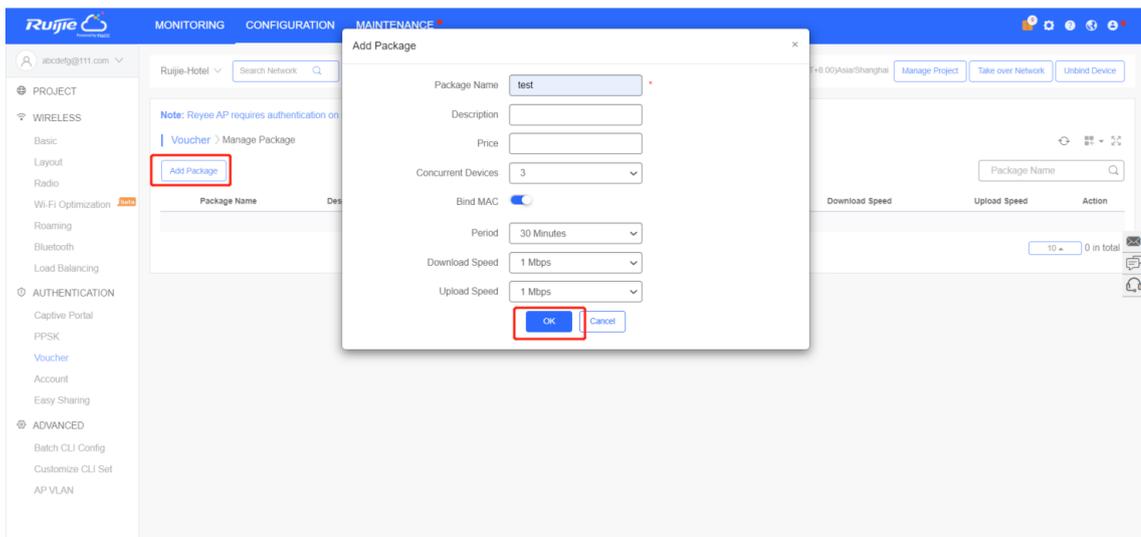
(5) Click the portal page to apply it and click **Save**.



(6) If you use voucher or account authentication, choose **Configuration > Voucher/Account** to add a voucher or an account used for clients. Click **Manage Package** to add a package.



- (7) Click **Add Package** and fill in **Price**, **Concurrent Devices**, **Bind MAC**, **Period**, **Download Speed**, and **Upload Speed**.



- (8) Click **Print Voucher** to add a voucher. Fill in **Quantity** and choose the package you add just now. Then click **Print**.

Print Configuration

* Quantity: 1

Alias: []

* Package: test (Manage Package)

Logo: [Select the logo] (Clear)

Text: [] (0/40)

Print Method: Print in 2 Columns (A4)

Profile Information on Voucher

You can select at most 4 parameters for the voucher.

Package Name: test

Bind MAC: Yes

Concurrent Devices: 3

Period: 30 Minutes

Preview

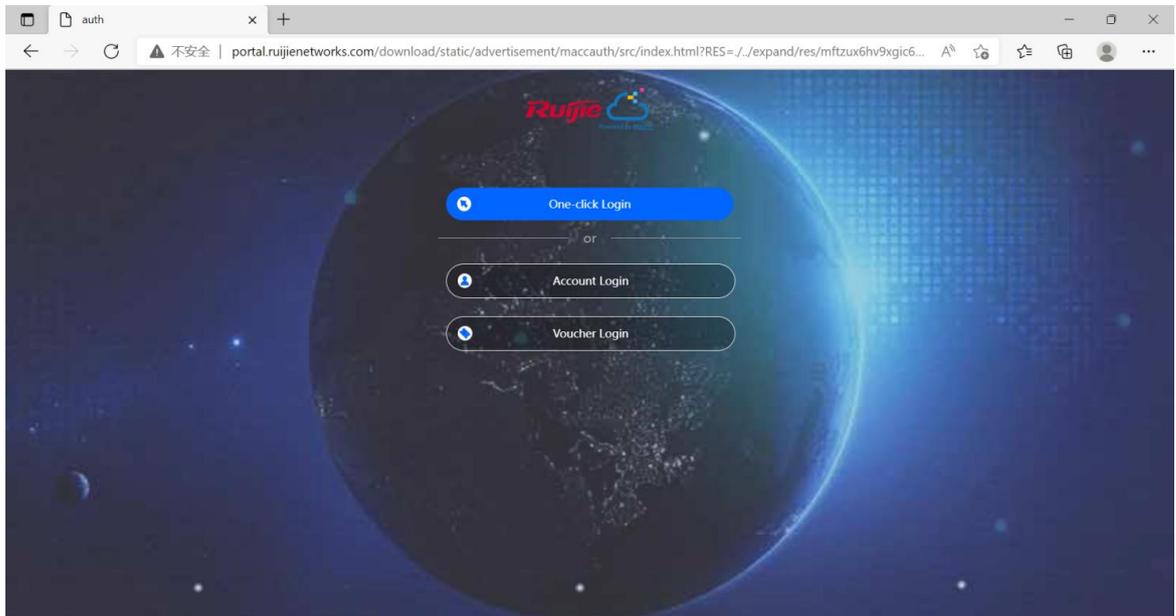
Voucher Code: **XXXXXX**

Print Voucher | Manage Package | More

Total Vouchers: 1 | Activated Vouchers: 0 | Depleted Vouchers: 0

Voucher Code	Alias	Package Name	Price	Period	Created at	Activated at	Expired at	Devices	Bind MAC	Download Speed	Upload Speed	Status
37tc7g	-	test	-	30 Minutes	2022-04-14 21:50:31	-	-	0/3	Yes	1.00 Mbps	1.00 Mbps	Not Activated

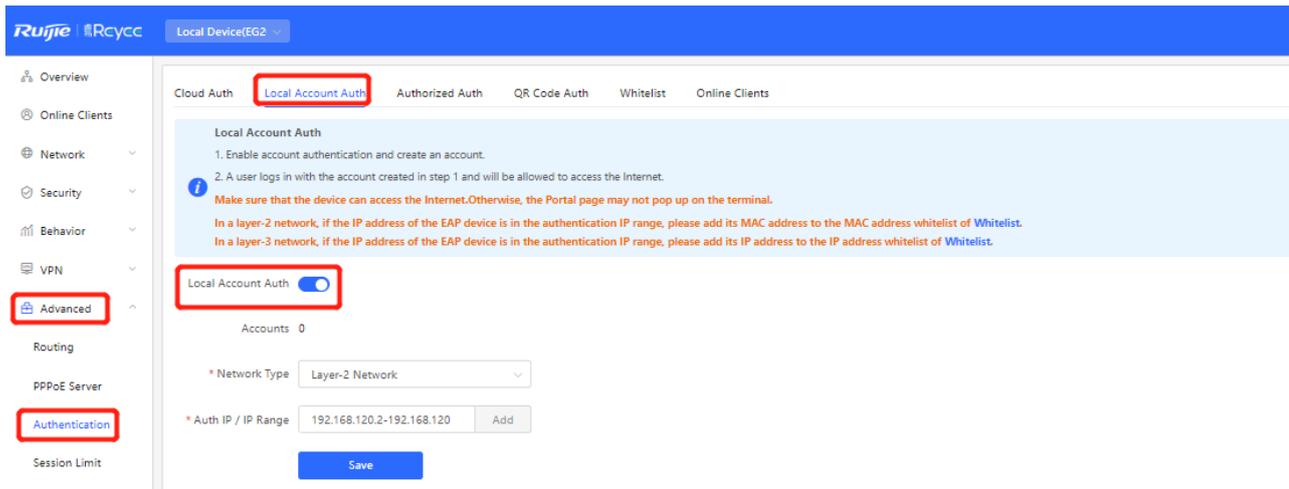
(9) Click **One-Click** to log in and perform authentication on the PC.



4.10.3 Local Account Authentication

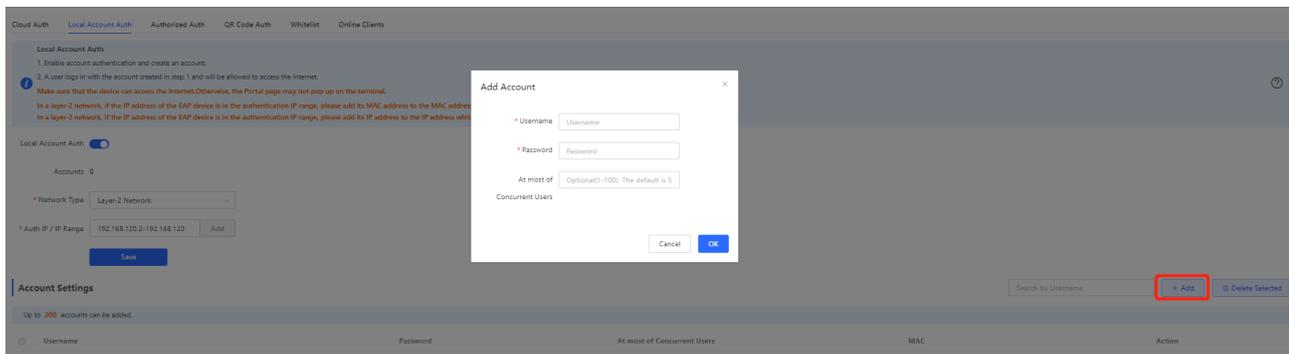
Reyee EG devices provide local account authentication. The portal page and account are all created locally.

- (1) Switch to the **Local** mode. Choose **Advanced > Authentication > Local Account Auth**, enable local account authentication, fill in **Auth IP/IP Range**, and click **Save**.



Auth IP/IP Range: The IP address of a client who needs to be authenticated. The value and other IP addresses for authentication cannot overlap.

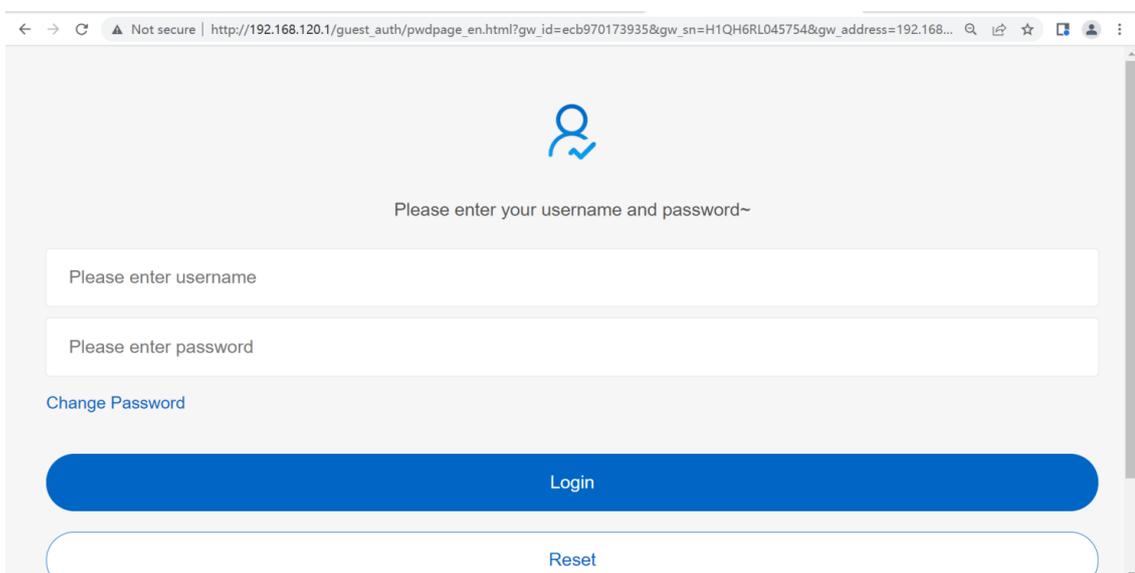
- (2) Add the account used by clients. Up to 200 accounts can be added.



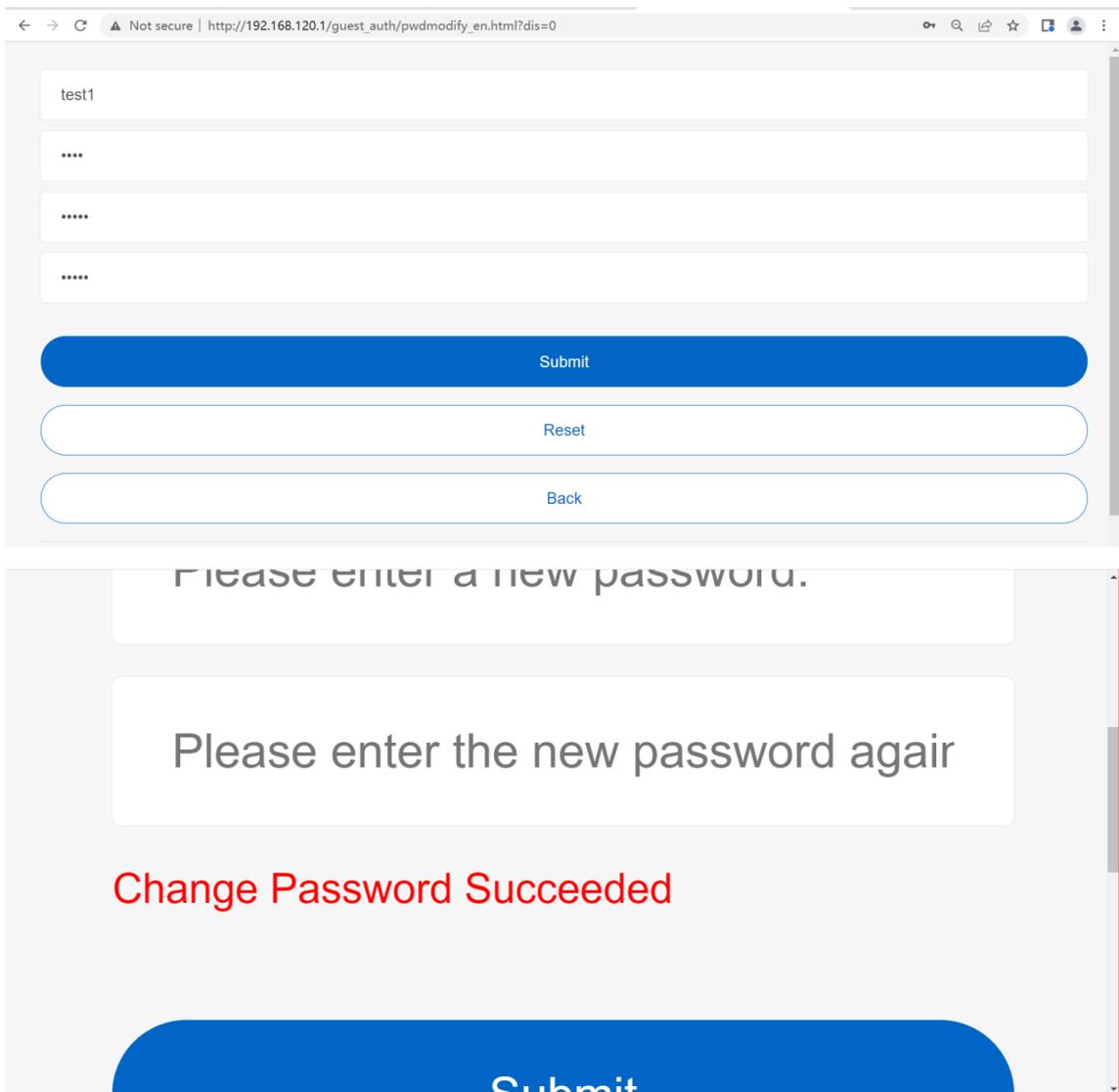
⚠ Caution

The account can be used by multiple clients.

- (3) Perform authentication on the PC. Generally, the portal page is displayed automatically. If the page is not displayed, try to enter 1.1.1.1 to redirect to the portal page. The page is displayed based on your browser language setting.

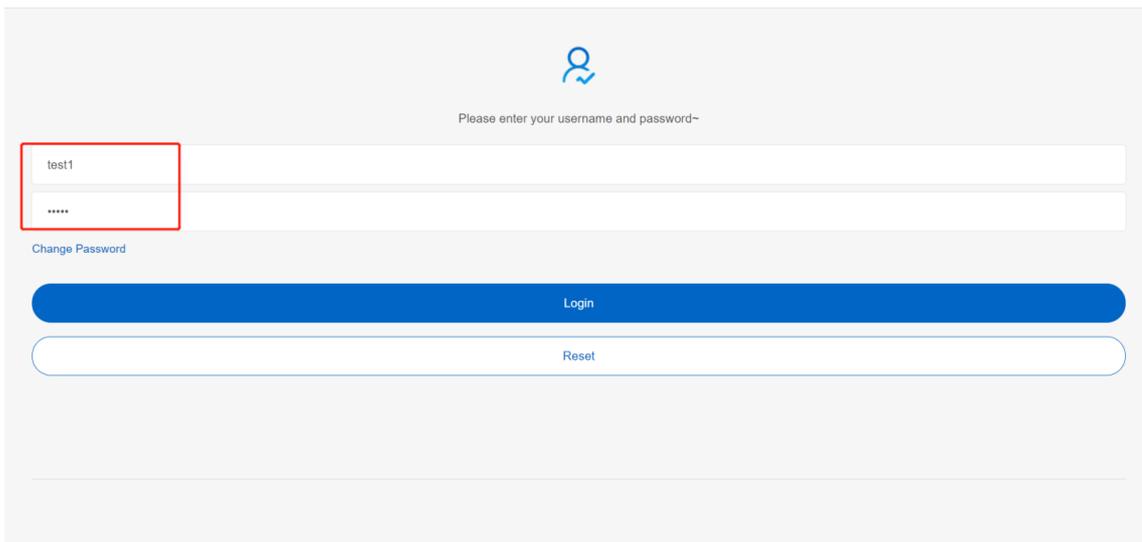


- (4) Enter **username** and **password** obtained from a manager. To change the password, click **Change Password**.

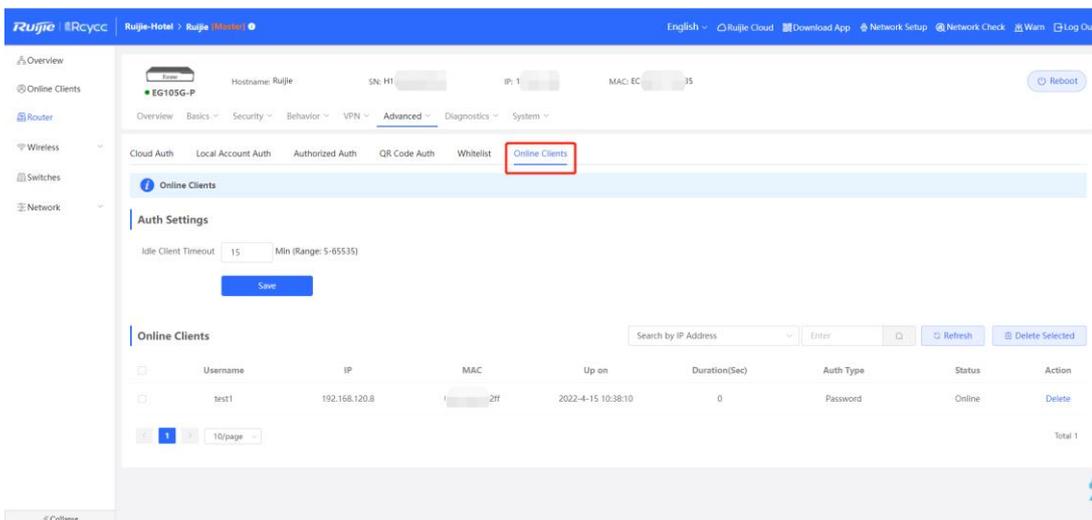


The image shows two screenshots of a web browser interface. The top screenshot displays a form with a text input field containing 'test1', three password input fields (the first is masked with dots), and three buttons: 'Submit' (blue), 'Reset' (white with blue border), and 'Back' (white with blue border). The bottom screenshot shows a confirmation message: 'Please enter a new password.' followed by 'Please enter the new password again' in a white box. Below this is a red message 'Change Password Succeeded' and a blue 'Submit' button.

- (5) Enter the new username and password to log in. The page will appear automatically after you log in, and then you can access the Internet.



(6) Check online information on the EG.



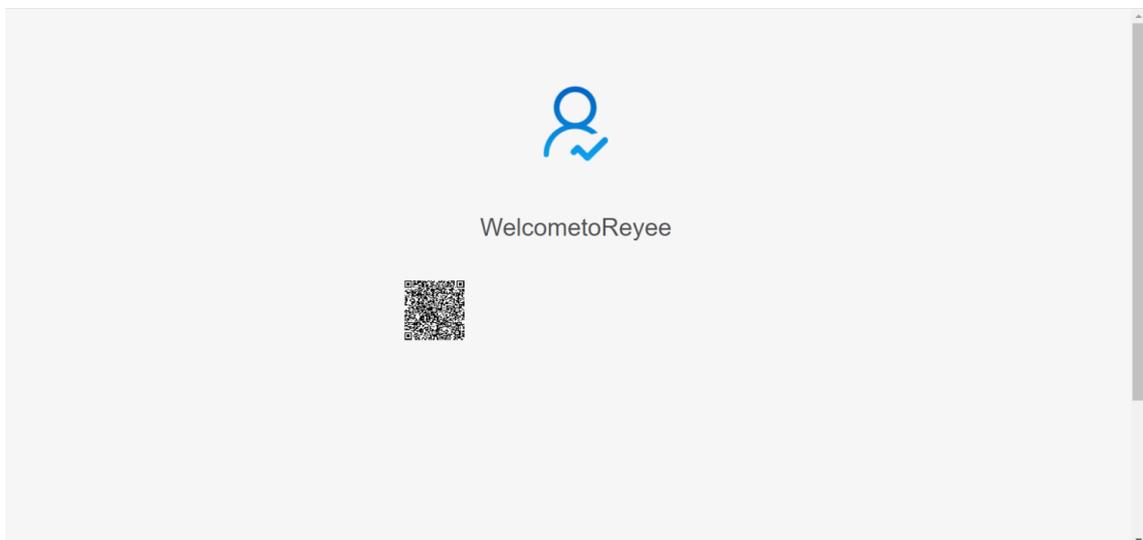
4.10.4 Authorized Authentication

Reyee EG devices supports **Authorized Auth**. When this function is enabled, an authenticated user can authorize guests by scanning the QR code.

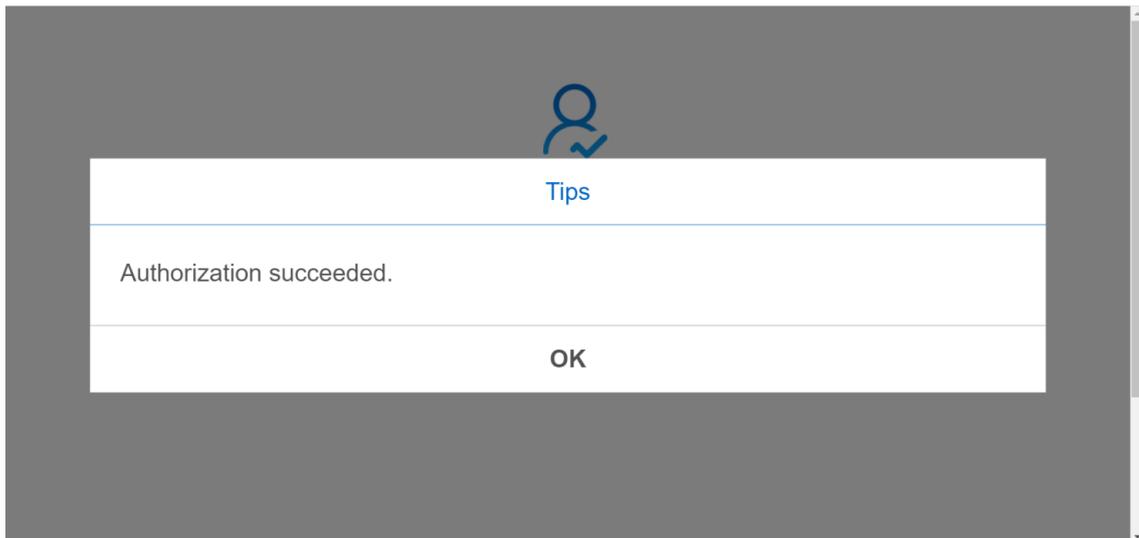
- (1) Switch to the **Local** mode. Choose **Advanced > Authentication > Authorized Auth**, and enable **Authorized Auth**.

The screenshot shows the 'Authorized Auth' configuration page in the Ruijie Rcycc interface. The 'Authorized Auth' toggle is turned on. The 'Auth IP / IP Range' is set to 192.168.110.2-192.168.110. The 'Limit Online Duration' is set to 60 minutes. The 'Authorization IP/IP Range' is set to 192.168.12.2-192.168.12.254. A 'Save' button is located at the bottom of the configuration area.

- **Auth IP/IP Range:** indicates the guest's IP address to be authenticated or range of guests' IP addresses to be authenticated.
 - **Limit Online Duration:** indicates the online duration of a guest.
 - **Authorization IP/IP:** indicates the IP address of the authenticated user.
- (2) The following authentication portal page is displayed automatically after the guest is connected to the Internet.



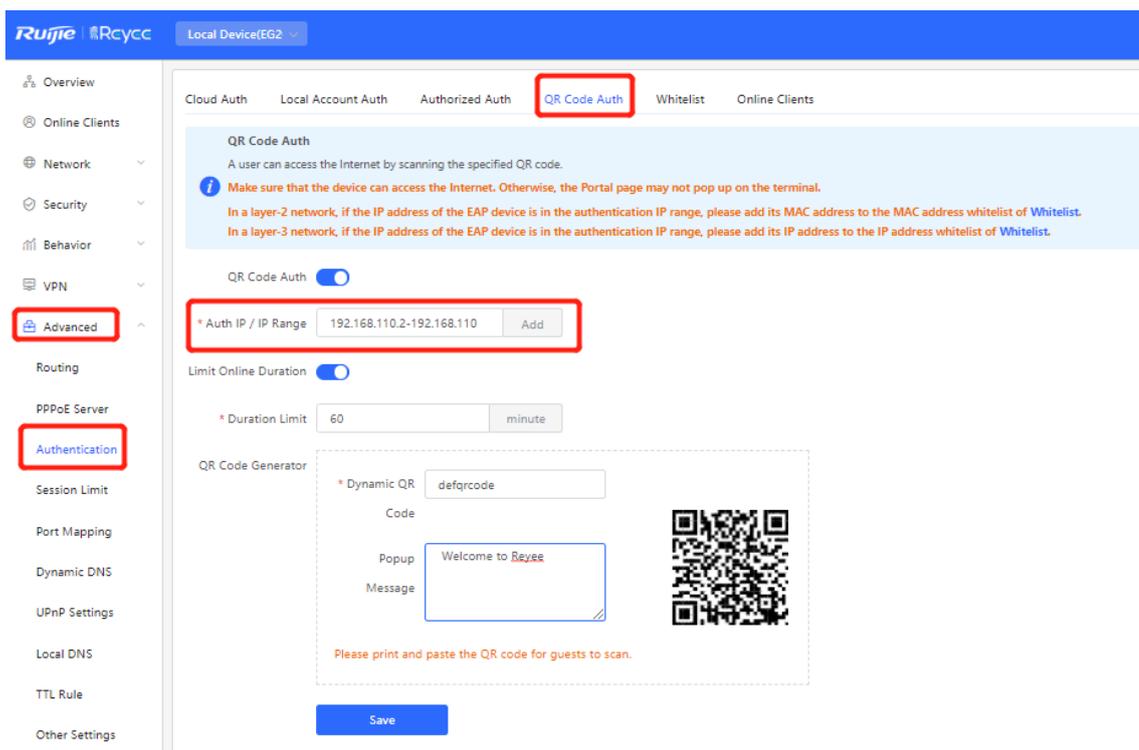
- (3) After the authorized client scans the QR code, the guest is authorized to access the Internet.



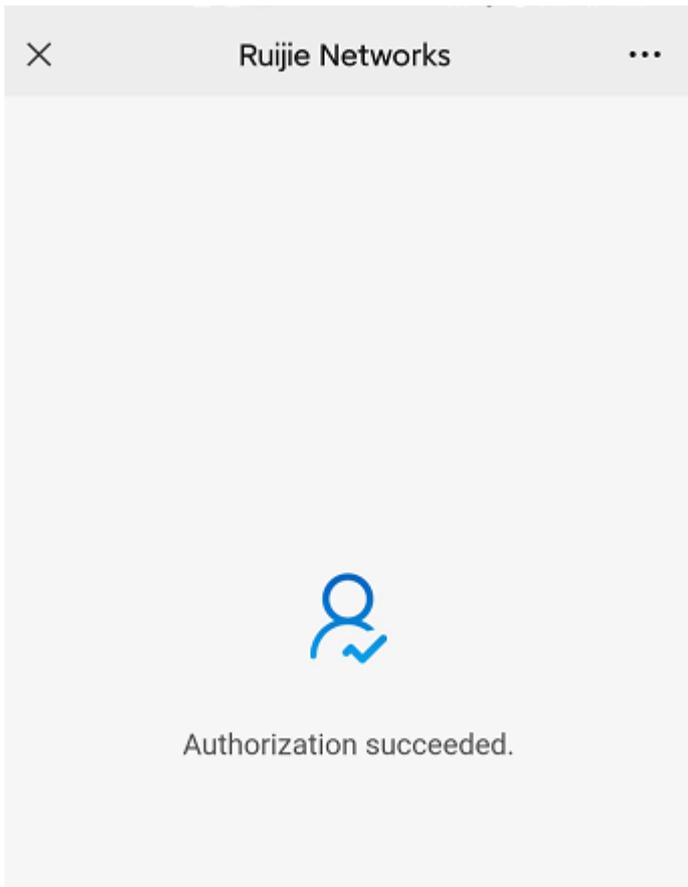
4.10.5 QR Code Authentication

Reyee EG devices support QR code authentication. This function enables a user to access the Internet by scanning the specified QR code.

- (1) Switch to the **Local** mode. Choose **Advanced > Authentication > QR Code Auth**, and enable **QR Code Auth**.



- o **Auth IP / IP Range:** indicates the IP address of a guest.
- o **Limit Online Duration:** indicates the online duration of a guest.
- o **QR Code Generator:** indicates the QR code used for guests to scan.

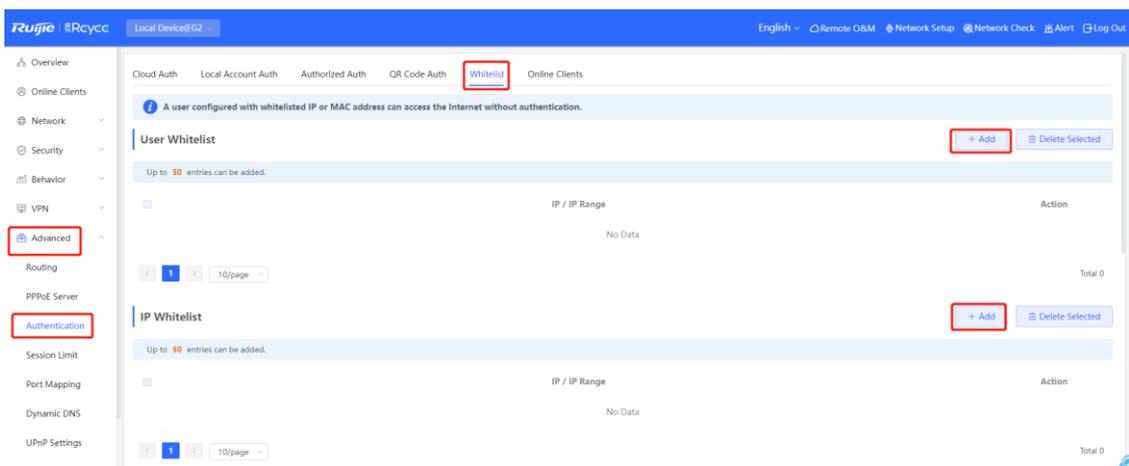


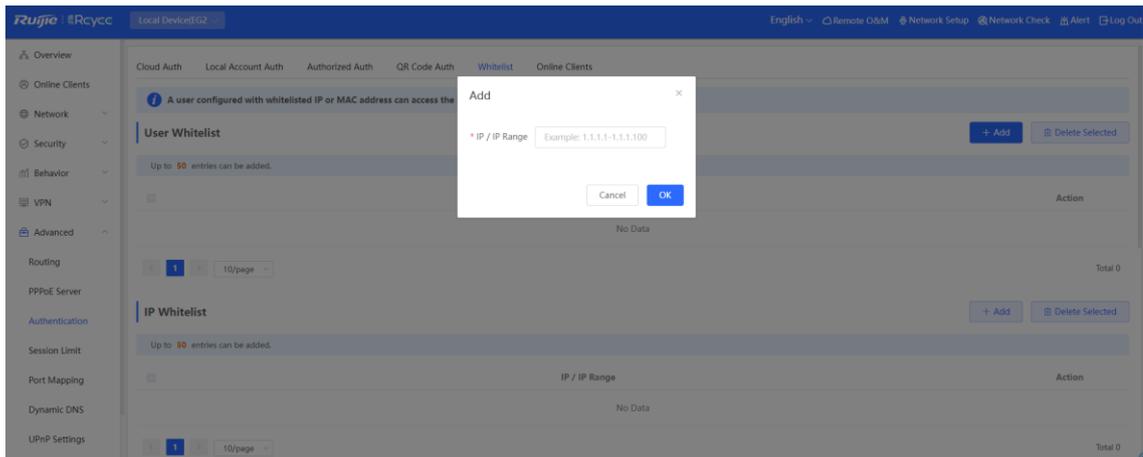
(2) The guest scan the QR code, and then can access the Internet.

4.10.6 Whitelist

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

(1) Switch to the **Local** mode. Choose **Advanced > Authentication > Whitelist**, and add **User Whitelist, IP Whitelist, URL Whitelist, MAC Whitelist, or MAC Blacklist**.





- **User Whitelist:** indicates that users can access the Internet without authentication. Up to 50 entries can be added.
- **IP Whitelist:** indicates that users can access an external IP address without authentication. Up to 50 entries can be added.
- **URL Whitelist:** indicates that users can access a URL without authentication. Up to 100 entries can be added.
- The following URL is the default URL added for cloud authentication.



- **MAC Whitelist:** indicates that a user with the whitelisted MAC address can access the Internet without authentication. Up to 250 accounts can be added.
- **MAC Blacklist:** indicates that a user with the blacklisted MAC address is prevented from accessing the Internet.

4.10.7 Online Clients

1. Configuring the Idle Client Timeout

Switch to the Local mode. Choose Local Device > Advanced > Authentication > Online Clients.

You can configure the idle client timeout. The default value is 15 minutes. If no traffic from an online user passes through the device within the specified period, the device will disconnect the user. The user can access the Internet again only after being re-authenticated.

Cloud Auth Local Account Auth Authorized Auth QR Code Auth Whitelist Online Clients

i **Online Clients**

Auth Settings

Idle Client Timeout Min (Range: 5-65535)

Save

Idle Client Timeout: The idle client will be disconnected after 15 minutes. The value ranges from 5 to 65535, in minutes.

2. Disconnecting a User

The online client list displays information about all the current online clients, including the client IP address, client's MAC address, login time, and authentication mode. You can find client information based on the IP address, MAC address, or username. Find the target client in the online client list and click **Delete** in the **Action** column to delete the client and end the Wi-Fi connection of the client.

Online Clients

▼

Q

↻ Refresh
🗑 Delete Selected

<input type="checkbox"/>	Username	IP	MAC	Up on	Duration(Sec)	Auth Type	Status	Action
No Data								

4.10.8 WeChat Authentication

1. Overview

The EG device is connected to the MACC authentication server on the cloud. After Wi-Fi users connect to Wi-Fi, a Portal page is displayed. Users need to switch to WeChat and follow the WeChat official account before they can access the Internet. WeChat authentication is applicable to the shopping mall scenario, where merchants guide customers to follow their WeChat official accounts through WeChat authentication.

2. Getting Started

- (1) Connect Wi-Fi through WeChat that is a Layer 2 protocol. Ensure that the authentication device can obtain MAC addresses of the wireless users.
 - The gateway address of wireless users to be authenticated is deployed on the authentication device.
 - If the gateway address is not deployed on the authentication device, the device functions as a DHCP server to allocate IP addresses to wireless users and obtain MAC addresses of the wireless users. In this scenario, you need to set **Network Type** to **Layer-3 Network**.
- (2) Complete the corresponding configuration on the WeChat Official Account platform and Ruijie Cloud platform before you enable authentication on the device. Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication, and one-click authentication. Log in to Ruijie Cloud to enable authentication.

Cloud Auth Local Account Auth Authorized Auth QR Code Auth Whitelist Online Clients

Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. [View](#)

i In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist. **?**

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

3. Configuration Steps

- (1) Switch to the **Local** mode. Choose **Advanced > Authentication > Cloud Auth**.
- (2) Enable WeChat authentication for Internet access.

Enable authentication, set **Server Type** to **Connect Wi-Fi via WeChat**, configure **Network Type**, **Auth Server URL**, **Redirect IP**, and **Client Escape**, and click **Save**.

Cloud Auth Local Account Auth Authorized Auth QR Code Auth Whitelist Online Clients

Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. [View](#)

i In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist. **?**

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

Authentication

* Network Type

* Server Type

* Auth Server URL

Redirect IP

Client Escape Enable

Table 4-6 WeChat Authentication Configuration

Parameter	Description
Network Type	<p>The default value is Layer-2 Network. Select a network type based on the actual network environment.</p> <p>Interconnection between Wi-Fi and the WeChat platform is performed on a Layer 2 network. On a Layer 3 network, you need to connect downlink devices to the current authentication device through the DHCP relay agent and deploy the DHCP address pool for authentication-engaged network segments on the authentication device. In this way, the authentication device can obtain MAC addresses of wireless users through DHCP. In this scenario, set this parameter to Layer-3 Network.</p>
Server Type	Select Connect Wi-Fi via WeChat .
Auth Server URL	After you complete MACC server configuration, the MACC server returns a URL. The device sends an authentication request to this URL.
Redirect IP	<p>The value corresponds to a menu or link address configured in the official account. The default value is 118.31.178.137. In most cases, you do not need to change the value.</p> <p>When a user is redirected to the WeChat official account, the user needs to visit this IP address before subsequent authentication.</p>
Client Escape	After this function is enabled, the authentication function is disabled on the device if the authentication server fails, so that all the users can directly access the Internet. After the server recovers, the authentication function is enabled automatically.

(3) Configure the authentication scope.

Click **Add** on the current page. In the dialog box that appears, enter the SSID and IP address range that requires authentication, and click **OK**.

For clients (such as printers, computers, or some users) that do not require authentication, set **IP/IP Range** to authentication-free, so that these clients can directly access the Internet.

Wi-Fi List			+ Add	Delete Selected
Up to 8 entries can be added.				
<input type="checkbox"/>	SSID	IP/IP Range	Action	
<input type="checkbox"/>	test	192.168.110.2-192.168.110.254	Edit	Delete

Add×

* SSID

* IP/IP Range

4. Verifying Configuration

When a mobile phone connects to the specific Wi-Fi, the portal authentication page pops up automatically. The user visits the WeChat page under instructions on the portal authentication page, follows the WeChat official account, clicks the menu or auto reply link to complete authentication. Then the user can normally access the Internet. After successful user authentication, you can choose **Advanced > Authentication > Online Clients** to view information about this authenticated user. For details, see section [错误!未找到引用源。错误!未找到引用源。](#)

5. Troubleshooting

- When a user clicks the authentication menu or link in the official account during WeChat authentication, the message "**This page cannot be accessed now.**" is displayed, leading to an authentication failure.



**This page cannot be accessed
now.**

Cause: The link address configured in the official account authentication entry on the official account Platform is regarded as insecure by Security Center of the WeChat client. When a client sends a request to this address, WeChat blocks this request.

Solution: Change the forced redirection address and the address in the official account authentication menu or link to an IP address not used on the LAN. For example, if the network segment 172.29.0.0 is not used on the LAN, set both the official account redirection IP address and the link address in the official account to 172.29.1.140.

⚠ Caution

If the official account redirection IP address is set to an IP address in a network segment used on the LAN, WeChat authentication will fail.

Authentication

* Network Type

* Server Type

* Auth Server URL

Redirect IP

Client Escape Enable

4.10.9 Enterprise WeChat Authentication

1. Overview

Similar to WeChat authentication, Wi-Fi users need to switch to the enterprise WeChat after connecting to Wi-Fi and complete applet authentication in the workspace before they can access the Internet. Enterprise WeChat authentication can be used to manage Internet access of employees and guests in the enterprise environment.

2. Getting Started

The operations are the same as those in section [错误!未找到引用源。错误!未找到引用源。](#) Before you enable enterprise WeChat authentication, complete relevant configurations on the enterprise WeChat console and Ruijie Cloud platform.

3. Configuration Steps

Switch to the **Local** mode. Choose **Advanced > Authentication > Cloud Auth**.

The configuration steps are similar to those in WeChat authentication. The major difference is that the official account redirection IP address in enterprise WeChat authentication must be set to 47.104.189.180:81. For details, see section [错误!未找到引用源。错误!未找到引用源。](#)

- Cloud Auth
- Local Account Auth
- Authorized Auth
- QR Code Auth
- Whitelist
- Online Clients

Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. [View](#)

i In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of **Whitelist**.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of **Whitelist**.

Authentication

* Network Type

* Server Type

* Auth Server URL

Redirect IP

Client Escape Enable

[Save](#)

Employee Authentication

Make sure that employees have joined the enterprise WeChat organization. When an employee connects a mobile phone to Wi-Fi, the employee is automatically redirected to the enterprise WeChat for authentication. After the employee opens the enterprise WeChat, the employee needs to access the **Workspace** menu of the enterprise WeChat and click the authentication app created by the administrator to obtain an Internet access permission. After the authentication success message is displayed, the employee can access the Internet normally.

The enterprise WeChat may not be started on the portal authentication page on some mobile phones due to low compatibility. In this case, users can manually open the enterprise WeChat and continue follow-up operations.

Guest Authentication

When a guest visits an enterprise, the employee can authorize the guest to connect to the Wi-Fi network of the enterprise. After the guest connects to the guest Wi-Fi, the authentication QR code is displayed. At this time, the authenticated employee scans the QR code using the enterprise WeChat on the mobile phone and enters the guest name. Then the guest can pass authentication and access the Internet normally.

When configuring guest authentication, you need to configure at least two Wi-Fi SSIDs and corresponding network segments in the Wi-Fi list, which are used for employee and guest connections, respectively.

Wi-Fi List

[+ Add](#)
[Delete Selected](#)

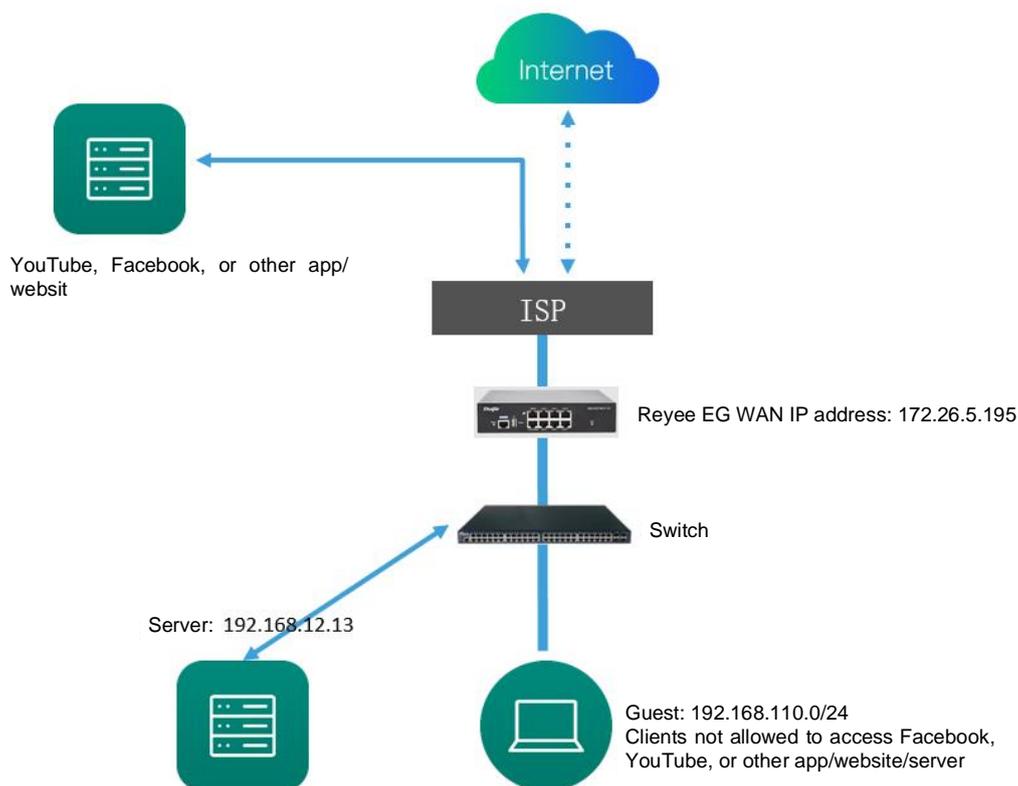
Up to 8 entries can be added.

	SSID	IP/IP Range	Action
<input type="checkbox"/>	test	192.168.110.2-192.168.110.254	Edit Delete
<input type="checkbox"/>	@Ruijie-guest-2277	192.168.111.2-192.168.111.254	Edit Delete

4.11 Behavior

4.11.1 Application Scenario

Online behavior management aims to block or prohibit specific Internet access behaviors of LAN users. Online behavior management is classified into five categories: app control, website filtering, QQ management, flow control, and access control. The effective range of each behavior management policy is flexibly controlled by the specified client IP address and effective time.



4.11.2 App Control

App control aims at controlling the range of specific apps that can be accessed by users. By default, users can access any app. After an app control policy is configured, users on the current network cannot access prohibited apps. App access can be prohibited based on the specified user group and time range. For example, employees on the office network are prohibited from accessing entertainment and game software during work periods to improve network security.

1. Configuring App Control

- (1) Switch to the **Local** mode. Choose **Behavior > App Control**.
- (2) Switch the application library.

The application lists vary depending on regions. Chinese and International versions of the application library are available. Select the version based on the regions.

Click to select **Application Library Version** and click **OK**. The version is switched after a few minutes.

⚠ Caution

- It takes about 1 minute to switch the application library version. Please wait.
- If you switch the application library, the old application control policy may take ineffective. Proceed with caution.

App Control ⓘ

App Control + Add Delete Selected

Up to **50** entries can be added.

<input type="checkbox"/>	IP Address Group	Time	Blocked App	Status	Remark	Action
No Data						

(3) Configure App Control.

Click **Add** to create an App control policy.

App Control ⓘ

App Control ⓘ Application Library Version: International + Add Delete Selected

Up to **50** entries can be added.

<input type="checkbox"/>	User Group	Time	Blocked App	Status	Remark	Action
<input type="checkbox"/>	1.1.1.1-1.1.1.254	All Time 📅	Play	Enable ☑		Edit Delete
<input type="checkbox"/>	User Group/test/abc	Weekdays 📅	Video	Enable ☑		Edit Delete

Add App



IP Address Group

Time

* Blocked App

Please select at least one

Remark

Status

Cancel

OK

Add

Type User Group Custom* User Group Time * Blocked App Remarks Status

Cancel

OK

Parameter	Description
Type	<ul style="list-style-type: none"> ● User Group: The policy is applicable to users in the specified user group. Select the target user group. ● Custom: The policy is applicable to users in the specified IP address range. Enter the managed IP address range manually.
User Group	<p>Select the users managed by the policy from the list of user groups. For details on how to configure a user group list, see section 6.2 User Management.</p> <p>If all members in the user group are selected, the policy takes effect for the user group and is also valid for new members added to this group.</p>
IP Address Group	<p>If the IP address range is restricted by the app control policy and the type of the policy is set to Custom, enter the IP address range manually.</p>

Parameter	Description
Time	Specify the time range under app control. In the specified time range, managed clients cannot access the selected apps in the list of prohibited apps. You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Blocked App	Specify the apps or app groups to be blocked.
Remark	Enter the policy description.
Status	Specify whether to enable the app control policy.

2. Upgrading the Application Library

The app control function relies on the application library, and the application library is updated with the app version. You can upgrade the application library to the latest version on the **Application Library Update** page.

(1) Switch to the Local mode. Choose Behavior > App Control > Application Library Update.

Caution

- Upgrading the application library version takes about 1 minute to take effect. Do not cut off power during the upgrade. You can view the current application library version on the page.
- Perform subsequent operations based on memory information displayed on the page. If the memory is insufficient, you are advised to restart the device and then upgrade the application library.
- After the application library is upgraded, the original app control policy may become invalid. Therefore, exercise caution when performing this operation.

App Control Application Library Update Custom

 There is sufficient flash memory and system memory for updating the application library.

Current Version 2022.08.17.22.08.17(V2.0)

File Path

- (2) Click **Browse**. Select an application library upgrade file.
- (3) Click **Upload** to upload the upgrade file.
- (4) Click **OK**. Wait for the system to automatically complete the upgrade.

3. Configuring Custom Apps

Based on traffic packets of certain websites or apps that are obtained by the device, users can analyze and extract 5-tuple information (protocol, source IP address, source port, destination IP address, and destination port) of the packets. You can define apps that are not in the default application list.

After custom apps are configured successfully, you can configure control policies for custom apps on the app control page to block users from accessing the custom apps on the current network.

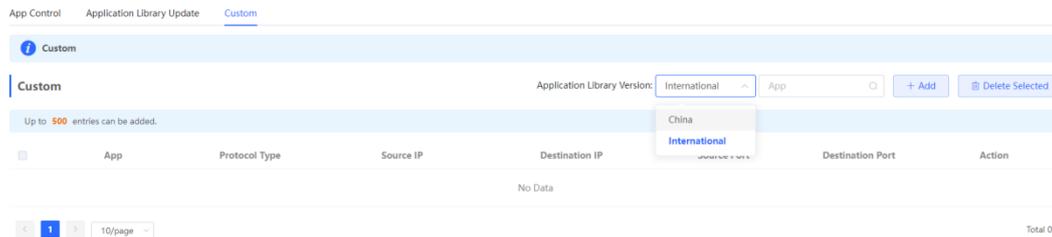
- (1) Switch to the **Local** mode. Choose **Behavior > App Control > Custom**.
- (2) Switch the application library.

The supported app list varies depending on regions. Chinese and international versions of the application library are available. Select an application library version based on the actual region.

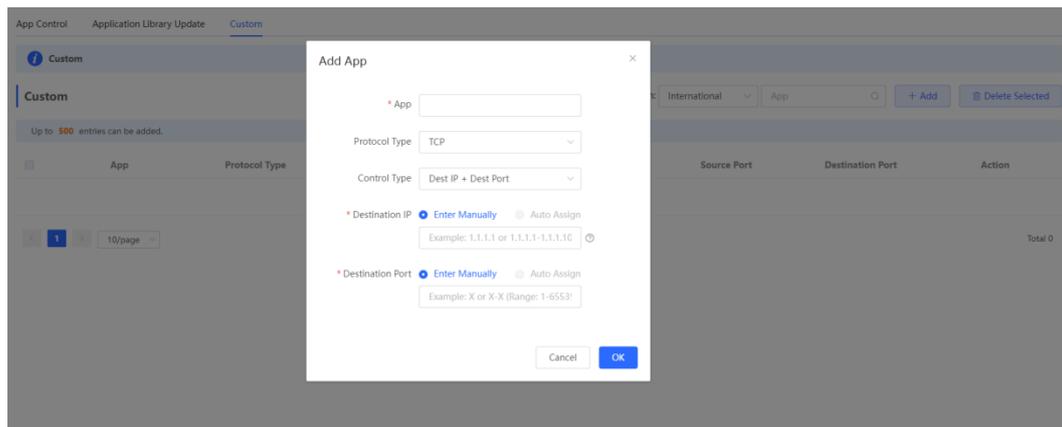
Click **Application Library Version** and select a version. In the displayed dialog box, click **OK**. Wait for a period of time for the system to complete switching.

Caution

- Switching the application library version takes about 1 minute to take effect.
- After the application library version is switched, the original app control policy may become invalid. Therefore, exercise caution when performing this operation.



- (3) Click **Add**. Enter information about a custom app.



Parameter	Description
App	Configure the app name (the name must be unique in the app list).
Protocol Type	Select a protocol type based on the protocol used by obtained packets. It can be set to TCP, UDP, or IP.
Control Type	Select a rule type based on 5-tuple information of extracted packets. It can be set to the following: Src IP + Src Port Dest IP + Dest Port Src IP + Dest IP
Source/Destination IP	Enter the source or destination IP address.

Parameter	Description
Source/Destination Port	Enter the source or destination port number.

Note

- If **Control Type** is set to **Src IP + Src Port**, you need to set the source IP address and source port.
- If **Control Type** is set to **Dest IP + Dest Port**, you need to set the destination IP address and destination port.
- If **Control Type** is set to **Src IP + Dest IP**, you need to set the source and destination IP addresses. The source IP address can be also to **Auto Assign**.

(4) Click **OK**.

4. Verifying the Configuration

Add a policy for rejecting access to Facebook and YouTube according to [错误!未找到引用源。错误!未找到引用源。](#).

Try to access Facebook on the guest PC. Then you will find the access failure.



This site can't be reached

www.facebook.com took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Reload

Details

4.11.3 Website Management

Website management consists of website grouping and filtering. Website grouping refers to the classification of website URLs. You can modify existing website groups or create website groups. Website filtering refers to access control for existing website groups to prohibit users' access to websites in specific groups. Website filtering can be applied based on the specified user group and time range. For example, employees on the office network are prohibited from accessing game websites during work periods to improve network security.

(1) Switch to the **Local** mode. Choose **Behavior > Website Management**.

(2) Configure website groups.

- Click the **Website Group** tab. On the page that appears, all the created website groups are displayed in the list. Find the target group and click **More** in the **Member** column to view all the website URLs in the group. Find the target group and click **Edit** in the **Action** column to modify the member website URLs in the group. Find the target group and click **Delete** in the **Action** column to delete the group.
- Click **Add** to create a website group.

⚠ Caution

If a website filtering rule in a website group is being referenced, the group cannot be deleted from the website group list. To delete this group, modify the website filtering configuration to remove the reference relationship first.

Website Filtering [Website Group](#)

Website Group ?

The group member can be a complete URL (example: www.baidu.com) or a domain (example: *.56.com).

Website Group + Add Delete Selected

Up to **20** entries can be added.

	Group Name	Member	Action
<input type="checkbox"/>	Games	duowan.com... More	Edit Delete
<input type="checkbox"/>	Finance	*.10jqka.com.cn... More	Edit Delete
<input type="checkbox"/>	Social	*.baihe.com... More	Edit Delete
<input type="checkbox"/>	Shopping	*.taobao.com... More	Edit Delete
<input type="checkbox"/>	Life	*.55bbs.com... More	Edit Delete

Add Group ×

* Group Name

* Member

*.56.com
www.google.com

Cancel
OK

Parameter	Description
Group Name	Configure a unique name for a website group. The name can be a string of 1 to 64 characters.

Parameter	Description
Member	Specify members in the website group. You can enter multiple websites in a batch. The group member can be a complete URL (such as www.baidu.com) or keyword in the URL (domain name with a wildcard in front, such as *.baidu.com). The wildcard can only appear at the beginning of a URL, and cannot be in the middle or end of the domain name.

(3) Configure website filtering.

- a Choose **Gateway > Behavior > Website Management > Website Filtering**.
- b Click the **Website Filtering** tab. On the page that appears, all the created website filtering rules are displayed in the list. Click **Edit** to modify rule information and click **Delete** to delete the specific filtering rule.
- c Click **Add** to create a website filtering rule.

Website Filtering Website Group

Website Filtering + Add Delete Selected

Up to 20 entries can be added.

<input type="checkbox"/>	IP Address Group	Control Type	Blocked Website	Time	Status	Remark	Action
<input type="checkbox"/>	test user i	Your request is forbidden.	Games	test 📅	Enable 🔄	test	Edit Delete

Add Website Filtering ✕

IP Address Group

Time

* Blocked Website

Remark

Status

Parameter	Description
Type	<ul style="list-style-type: none"> ● User Group: The policy is applicable to users in the specified user group. Select the target user group. ● Custom: The policy is applicable to users in the specified IP address range. Enter the managed IP address range manually.
User Group	<p>Select the users managed by the policy from the list of user groups. For details on how to configure a user group list, see section 6.2 User Management.</p> <p>If all members in the user group are selected, the policy takes effect for the user group and is also valid for new members added to this group.</p>
IP Address Group	<p>If the IP address range is restricted by the app control policy and the type of the policy is set to Custom, enter the IP address range manually.</p>
Time	<p>Specify the time range under website filtering control. In the specified time range, managed clients cannot access the prohibited websites. You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.</p>
Blocked Website	<p>Configure the type of websites to be blocked. You can select an existing website group. After a website group is selected, users are prohibited from accessing all websites in this group. For details on how to create or modify a website group, see 错误!未找到引用源。.</p>
Remark	<p>Enter the rule description.</p>
Status	<p>Specify whether to enable the website filtering rule.</p>

d Click **OK**.

(4) Try to access Facebook on the guest PC. Then you will find the access fails.



This site can't be reached

www.facebook.com took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Reload

Details

4.11.4 Access Control

Access control enables the device to match data packets passing through the device based on specific rules and to permit or drop data packets in the specified time range. This function controls whether to permit LAN users' access to the Internet and whether to block a specific data flow. The device matches packets based on the MAC address or IP address.

- (1) Switch to the **Local** mode. Choose **Behavior > Access Control**.

The access control rule list displays the created access control rules. Click **Add** to add an access control rule.

ACL
 Configure ACL based on IP addresses. **Reverse flow mismatches** .
 The policy cannot take effect on the WAN port to block the traffic among the internal users between an L2TP server and an L2TP client. The policy only takes effect in the LAN network.

i Example: **Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 192.168.2.0/24.** Device configured with IP address 192.168.1.x will fail to access device 192.168.2.x. **But device 192.168.2.x will be allowed to access device 192.168.1.x.**

Tip: Configure one more deny ACL entry containing source IP address 192.168.2.0/24 and destination IP address 192.168.1.0/24. The two devices will be mutually unreachable.

ACL List + Add + Add Delete Selected

Up to 50 entries can be added.

<input type="checkbox"/>	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
<input type="checkbox"/>	Src IP Address 192.168.1.1/24 : 20 Dest IP Address 192.168.2.2 : 30 Protocol TCP	Block	test	WAN	Inactive ⚠		↓	Edit Delete
<input type="checkbox"/>	MAC 11:11:11:11:11:11	Block	All Time	WAN	Active		↑	Edit Delete

Table 4-9 Access Control Rule Information

Parameter	Description
Effective State	Indicate whether a rule takes effect. If Inactive is displayed, the current system time may be not in the effective time range. Move the cursor to  to view the detailed cause.
Match Order	All the created ACL rules are displayed in the ACL list, with the latest rule listed on the top. The device matches rules according to their sorting in the list. You can manually adjust the rule matching sequence by clicking  or  in the list.
Action	You can modify or delete a rule.

(2) Configure a MAC address-based ACL rule.

MAC address-based ACL rules enable the device to match data packets based on the source MAC address, and are typically used to control Internet access from online users or specific clients.

Set **Based on MAC**, enter the MAC address of a client, select a rule type, set the effective time range, and click **OK**.

 **Note**

MAC address-based ACL rules are valid on WAN ports by default.

Add Rule
×

Based on **MAC** IP

* MAC

Control Type

Wireless Schedule

Remark

Table 4-10 MAC Address-based ACL Configuration

Parameter	Description
MAC	Enter the client's MAC address to be controlled by the ACL rule. After you click the input field, the current client information is displayed. You can click to automatically enter the corresponding MAC address.
Control Type	Specify the method for processing data packets matching conditions. <ul style="list-style-type: none"> ● Allow: Permit the data packets matching the conditions. ● Block: Drop the data packets matching the conditions.
Wireless Schedule	You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Remark	Enter the rule description, which is used to uniquely identify a rule.

(3) Configure an IP address-based ACL rule.

IP address-based ACL rules enable the device to match data flows based on the source IP address, destination IP address, and protocol number.

Set **Based on IP**, enter the source IP address and port of a data flow, set the destination IP address and port of the data flow, select the protocol type, rule type, effective time range, and effective port, and click **OK**.

 **Caution**

IP address-based ACL rules take effect in only one direction. For example, in a rule that defines **Block**, the source IP address segment is 192.168.1.0/24 and the destination IP address segment is 192.168.2.0/24. Based on this rule, the device at 192.168.1.x cannot access the device at 192.168.2.x, but the device at 192.168.2.x can access the device at 192.168.1.x. To block bidirectional access on this network segment, you need to configure another blocking rule with the source IP address segment 192.168.2.0/24 and destination IP address segment 192.168.1.0/24.

L2TP and PPTP VPN support only IP address-based access control, and effective ports must be on the LAN.

Add Rule
×

Based on MAC IP

Src IP Address: Port :

Dest IP Address: Port :

Protocol Type ▾

Control Type ▾

Wireless Schedule ▾

Interface ▾

Remark

Table 4-11 IP Address-based ACL Configuration

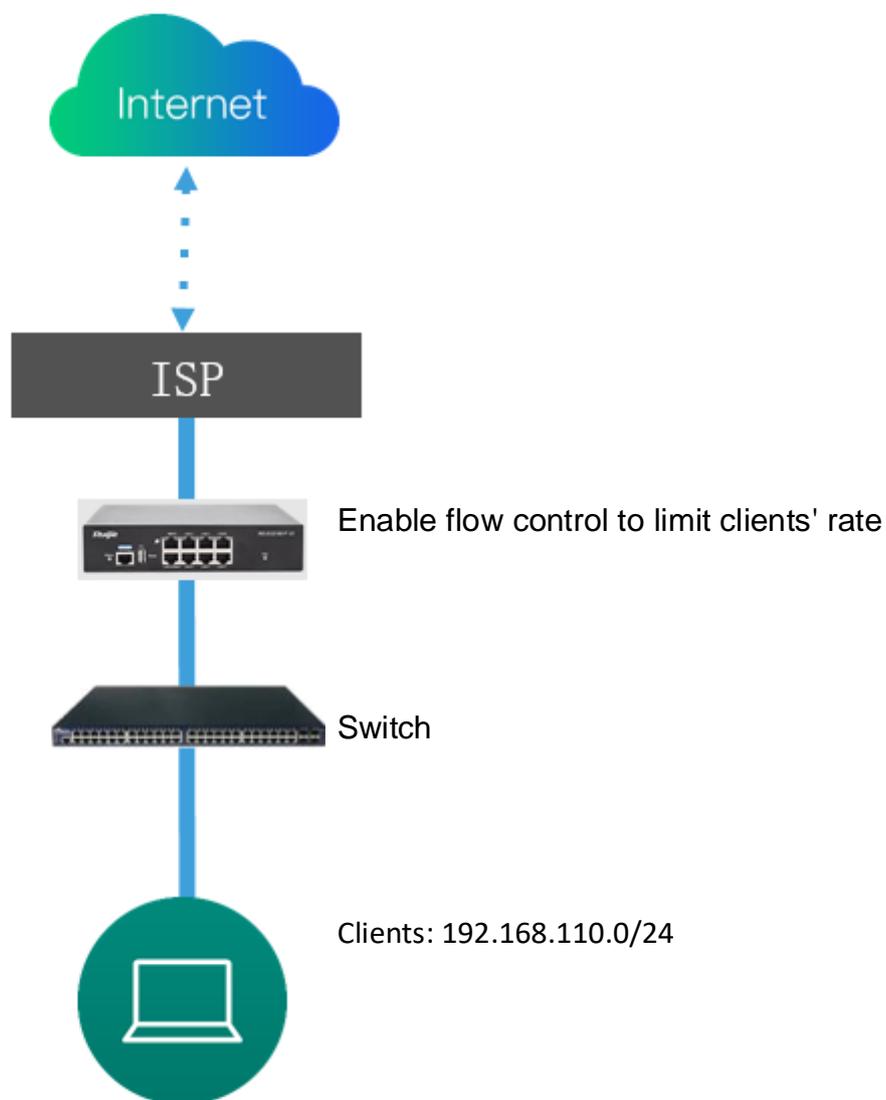
Parameter	Description
Src IP Address: Port	Enter the source IP address and port number for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The source IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24).
Dest IP Address: Port	Enter the destination IP address and port number for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The destination IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24).
Protocol Type	Specify the protocol type for data packet matching. The options are TCP , UDP , and ICMP .
Control Type	Specify the method for processing data packets matching conditions. <ul style="list-style-type: none"> ● Allow: Permit the data packets matching the conditions. ● Block: Drop the data packets matching the conditions. This rule is valid only in one direction, and does not block reverse flows.

Parameter	Description
Wireless Schedule	You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Interface	Select the port to which the rule applies. <ul style="list-style-type: none">● LAN: The rule takes effect on a LAN port to control data packets to the LAN.● WAN: The rule takes effect on a WAN port to control data packets received from or sent to the Internet.
Remark	Enter the rule description, which is used to uniquely identify a rule.

4.12 Flow Control

4.12.1 Application Scenario

Flow control enables the device to classify flows based on rules and process flows using different policies based on their categories. Flow control can be used to guarantee key flows and suppress malicious flows. It can be also used when the bandwidth is insufficient or flows need to be distributed properly.



4.12.2 Smart Flow Control

1. Overview

To limit uplink and downlink traffic bandwidth of device ports (such as WAN and WAN 1), you can enable smart flow control. After the line bandwidth is configured for a port, the uplink and downlink traffic of the port will be limited within the specified range. In addition, per-user bandwidth must be intelligently adjusted according to the number of users so that users can fairly share the bandwidth.

2. Configuration Steps

- (1) Switch to the **Local** mode. Choose **Behavior > Flow Control > Smart Flow Control**.
- (2) Toggle the switch to **Enable** on the **Smart Flow Control** tab and set the line bandwidth based on the bandwidth actually allocated by an ISP. If the device has multiple lines, you can set the bandwidth for these

WAN ports separately.

[Smart Flow Control](#) [Custom Policy](#) [Application Priority](#)



Smart Flow Control

Adjust the bandwidth allocated to each user according to the user count.

Enable **If you want to test the WAN rate, please disable smart flow control first.**

WAN Bandwidth * Up Mbps * Down Mbps

WAN1 Bandwidth * Up Mbps * Down Mbps

WAN2 Bandwidth * Up Mbps * Down Mbps

Save

Table 4-7 Smart Flow Control Configuration

Parameter	Description
Enable	Specify whether to enable the smart flow control function. By default, smart flow control is disabled.
WAN Bandwidth	Set the uplink and downlink bandwidth limits for WAN ports, in Mbit/s.

(3) Click **Save** to make the configuration take effect.

Caution

Enabling flow control will affect network speed testing. To test the network speed, disable flow control first.

Note

Smart flow control can be used to control the line traffic in different networking modes, including bandwidth-based, static IP address, and dynamic IP address.

(4) Perform the speed test. The following figure shows that the guest's upload or download speed falls below 2 Mbit/s.



4.12.3 Custom Policies

1. Overview

Custom policies are used to restrict the traffic with specific IP addresses based on smart flow control, thereby meeting bandwidth requirements of specific users or servers. When creating a custom flow control policy, you can flexibly configure the limited user range, bandwidth limit, limited application traffic, and rate limit mode. A custom policy takes precedence over the smart flow control configuration.

Custom policies are classified into normal policies, MACC policies, and VPN policies based on their application scope:

- Normal policies are used to control common traffic.
- VPN policies are used to control VPN traffic.
- MACC policies are flow control policies configured on the cloud. The web management page only displays the policies. MACC policies cannot be modified on the web management page. To modify an MACC policy, log in to the MACC.

2. Getting Started

Before you configure a custom policy, enable smart flow control. For details, see section [错误!未找到引用源。](#)
[错误!未找到引用源。](#)

3. Configuration Steps

Choose **Gateway > Behavior > Flow Control > Custom Policy**.

(1) Set Policy Type.



Note

The **Cloud Policy** option is displayed in **Policy Type** only after a MACC policy is configured on the MACC.

(2) Switch the application library.

The application lists vary depending on regions. Chinese and International versions of the application library are available. Select the version based on the regions.

Click to select **Application Library Version** and click **OK**. The version is switched after a few minutes.

Caution

- It takes about 1 minute to switch the application library version. Please wait.
- If you switch the application library, the template of the application priority will be reset (see section [6.6.4 Application Priority](#)), and the old application control policy may take ineffective (see section [6.4 App Control](#)). Proceed with caution.

Smart Flow Control **Custom Policy** Application Priority

Custom Policy
 Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.
 When custom policy and template are applied to an application, the custom policy prevails.

Policy List + Add Delete Selected

Up to **30** entries can be added. **1** entries are already added.

<input type="checkbox"/>	Policy Name	IP / IP Range	Bandwidth Type	Channel	Application List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
<input type="checkbox"/>	test	1.1.1.1-1.1.1.1	Shared	4	All Applications	No Limit	No Limit	WAN	Enable	Active	Edit Delete

(1) Set a custom policy.

- Set a custom normal policy.
 - Set **Policy Type** to **Normal Policy** and click **Add** to create a custom normal flow control policy. A maximum of 30 custom normal policies can be configured.

Add
×

* Policy Name

Type User Group Custom

* User Group ?

Bandwidth Type Shared Independent

Application All Applications Custom

Channel Priority ?

Bandwidth Limit Limit Kbps No Limit

Uplink Bandwidth * CIR * PIR ?

Downlink Rate * CIR * PIR ?

* Interface

Enabled

b Configure items related to a normal policy.

Parameter	Description
Policy Name	A policy name uniquely identifies a custom flow control policy. It cannot be modified.
Type	Type of a flow control policy: <ul style="list-style-type: none"> ● User Group: The policy is applied to users in a specified user group. You need to select a user group to be managed. ● Custom: The policy is applied to users in a specified IP address segment. You need to manually enter the IP address range to be managed.
User Group	Select a user to be managed by the policy from the user group list. . If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later).

Parameter	Description
IP/IP Range	<p>Specify the IP address range for the flow control policy to take effect. When Type is set to Custom, enter the IP address manually. You can enter a single IP address or an IP address segment.</p> <p>The IP address range must be within a LAN segment. You can choose Overview > Ethernet status to check the network segment of the current LAN port. For example, the network segment of the LAN port shown in the figure below is 192.168.110.0/24.</p>  <p>The screenshot shows the 'Ethernet status' interface with a legend for 'Connected' (blue) and 'Disconnected' (grey). Below the legend, there are icons for LAN0, LAN1, LAN2, LAN3, LAN4, LAN5, LAN6/WAN3, LAN7/WAN2, LAN8/WAN1, and WAN0. LAN0 and LAN1 are blue, indicating they are connected. LAN2 through LAN5 and LAN6/WAN3 are grey, indicating they are disconnected. LAN7/WAN2, LAN8/WAN1, and WAN0 are also grey. Below the icons, the IP address 192.168.112.1 is shown under LAN3, and 192.168.1.10 and 192.168.210.103 are shown under LAN8/WAN1 and WAN0 respectively.</p>
Bandwidth Type	<ul style="list-style-type: none"> ● Shared: All users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the bandwidth of a single user is not limited. ● Independent: All users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the maximum bandwidth of a single user can be limited.
Application	<p>When Bandwidth Type is set to Shared, the flow control policy can be configured to take effect only on specified applications.</p> <ul style="list-style-type: none"> ● All Applications: The flow control policy takes effect on all applications in the current application library. ● Custom: The flow control policy takes effect only on specified applications in the application list. <p>When Bandwidth Type is set to Independent, some models do not support application selection and the flow control policy takes effect on all applications in the current application library by default.</p> <p>For the models, contact technical support engineers.</p>
Application List	<p>When Application is set to Custom, it specifies the applications on which the policy takes effect. Traffic of the selected applications is limited by the policy.</p>
Channel Priority	<p>Specify the traffic guarantee level. The value ranges from 0 to 7. A smaller value indicates a higher priority and the value 0 indicates the highest priority.</p> <p>Different traffic priority values correspond to different application groups in an application template. The value 2 indicates the key group, value 4 indicates the normal group, and value 6 indicates the suppression group. For the description of application groups in a priority template, see 错误!未找到引用源。错误!未找到引用源。.</p>
Bandwidth Limit	<p>Configure whether to limit the bandwidth.</p> <ul style="list-style-type: none"> ● Limit Kbps: You can set the uplink and downlink bandwidth limits as required. ● No Limit: When the bandwidth is sufficient, the used maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth cannot be guaranteed.

Parameter	Description
Uplink Bandwidth Downlink Rate	<p>Configure the uplink or downlink data transmission rate, in kbit/s.</p> <ul style="list-style-type: none"> ● CIR: Specifies the minimum bandwidth that can be shared by all users when the bandwidth is insufficient. ● PIR: Specifies the total maximum bandwidth that can be occupied by all users when the bandwidth is sufficient. ● PIR per User: Specifies the maximum bandwidth that can be occupied by each user when multiple users share the bandwidth. It is optional and can be configured only when Bandwidth Type is set to Independent. The rate is not limited by default.
Interface	Specify the WAN port on which the policy takes effect. When it is set to All WAN Ports , the policy will be applied to all WAN ports.
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.

 **Caution**

After switching the application library version, you may need to reconfigure the application list.

- c Click **OK**.
- Set a custom VPN policy.
 - a Set **Policy Type** to **VPN Policy** and click **Add** to create a custom VPN flow control policy. A maximum of 10 VPN policies can be configured.

Add
×

* Policy Name

Type User Group Custom

* User Group ?

Effective User Internal IP/User External IP/External User

Application All Applications Custom

Max Uplink Rate per User

Max Downlink Rate per User

* Interface

Enabled

b Configure items related to a VPN policy.

Parameter	Description
Policy Name	A policy name uniquely identifies a custom flow control policy. It cannot be modified.
Type	Type of a flow control policy: <ul style="list-style-type: none"> ● User Group: The policy is applied to users in a specified user group. You need to select a user group to be managed. ● Custom: The policy is applied to users in a specified IP address segment. You need to manually enter the IP address range to be managed.
User Group	Select a user to be managed by the policy from the user group list. If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later).
Effective User	Specify the type of effective users: <ul style="list-style-type: none"> ● Internal IP/User: For a gateway, IP addresses of clients connected to the gateway are internal IP addresses. ● External IP/External User: For a gateway, non-gateway internal IP addresses are external IP addresses, such as the internal IP address of the VPN server. Configuration suggestions are as follows: <ul style="list-style-type: none"> ● When clients are configured to control VPN traffic, select Internal IP/ User to control traffic of internal network users. When the VPN server is configured to control VPN traffic, select External IP/External User to control traffic of external network users. ● For the VPN of the NAT model, the external IP address of the server must be in the IP address segment of the VPN address pool. ● For the VPN in router mode, the IP address segment must be set to IP addresses of restricted users. For the VPN in router mode, to configure flow control on internal IP addresses of clients, set internal IP addresses to the IP addresses of the flow control objects.
Application	When Bandwidth Type is set to Shared , the flow control policy can be configured to take effect only on specified applications. <ul style="list-style-type: none"> ● All Applications: The flow control policy takes effect on all applications in the current application library. ● Custom: The flow control policy takes effect only on specified applications in the application list. When Bandwidth Type is set to Independent , some models do not support application selection and the flow control policy takes effect on all applications in the current application library by default. For the models, contact technical support engineers.
Application List	When Application is set to Custom , it specifies the applications on which the policy takes effect. The traffic of the selected applications is limited by the policy.
Max Uplink Rate per User	Configure the maximum uplink or downlink data transmission rate when multiple users share the bandwidth, in kbit/s.
Max Downlink Rate per User	It is optional and can be configured only when Bandwidth Type is set to Independent . The rate is not limited by default.
Interface	Specify the VPN port on which the policy takes effect. When it is set to All VPN Ports , the policy is applied to all traffic of the VPN type.

Parameter	Description
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.

c Click OK.

(3) View Custom Policies

The current custom policies are displayed in the **Policy List** section. You can modify and delete a custom policy. To delete multiple custom policies in a batch, select the desired policies and click **Delete Selected**.

o Normal policy list

Smart Flow Control **Custom Policy** Application Priority

Custom Policy
 Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control. When custom policy and template are applied to an application, the custom policy prevails.

Policy List + Add Delete Selected

Up to 30 entries can be added. 1 entries are already added.

<input type="checkbox"/>	Policy Name	IP / IP Range	Bandwidth Type	Channel	Application List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
<input type="checkbox"/>	test	1.1.1.1-1.1.1.1	Shared	4	All Applications	No Limit	No Limit	WAN	Enable @...	Active	Edit Delete

o VPN policy list

Policy Type Normal Policy **VPN Policy** Cloud Policy

Policy List Application Library Version: China + Add Delete Selected

Up to 10 entries can be added. 3 entries are already added.

<input type="checkbox"/>	Policy Name	User Group	Application List	Uplink Bandwidth	Downlink Rate	Interface	Enabled	Effective State	Match Order	Action
<input type="checkbox"/>	PPTP_SERVER_74624	1.1.1.1-255.255.255.255	All Applications	PIR per User No Limit	PIR per User No Limit	PPTP	Disable ●	Inactive	↓	Edit Delete
<input type="checkbox"/>	L2TP_SERVER_49952	1.1.1.1-255.255.255.255	All Applications	PIR per User No Limit	PIR per User No Limit	L2TP	Disable ●	Inactive	↑ ↓	Edit Delete
<input type="checkbox"/>	OPENVPN_SERVER_15522	1.1.1.1-255.255.255.255	All Applications	PIR per User No Limit	PIR per User No Limit	OpenVPN	Disable ●	Inactive	↑	Edit Delete

Table 4-8 Policy List Information

Parameter	Description
Application List	Application List contains the applications for which the policy is valid. If Application Library matches Application that is set to Custom and supported by the policy, Custom is displayed in Application List . If not, Custom is displayed.
Status	Whether the current policy is enabled. You can click to edit the status. If Application Library does not match Application that is set to Custom and supported by the policy, you cannot edit Status directly. Click Edit in the action bar to edit the policy or switch the application library.

Parameter	Description
Effective State	Whether the policy is effective in the current system. If Inactive is displayed, check whether the policy is enabled, whether the policy-enabled port exists, and whether Application Library matches Application for which the policy is valid.
Match Order	All the created custom policies are displayed in the policy list, with the latest policy listed on the top. The device matches policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking  or  in the list.
Action	You can modify and delete a custom policy.

4.12.4 Application Priority

1. Overview

After smart flow control is enabled, you can set the application priority to provide guaranteed bandwidth for applications with a high priority and suppress the bandwidth for applications with a low priority. You can predefine a list of applications whose bandwidth needs to be guaranteed preferentially and a list of applications whose bandwidth needs to be suppressed as needed.

Caution

If one application exists in both the custom policy list and application priority list, the custom policy takes effect.

2. Getting Started

- o Before you configure an application priority, enable smart flow control. For details, see section [错误!未找到引用源。错误!未找到引用源。](#)
- o Confirm that the appropriate application library is selected on the **Custom Policy** page (see section [6.6.3 Custom Policies](#)).

3. Configuration Steps

Switch to the Local mode. Choose Behavior > Flow Control > Application Priority.

- (1) Create an application priority template.

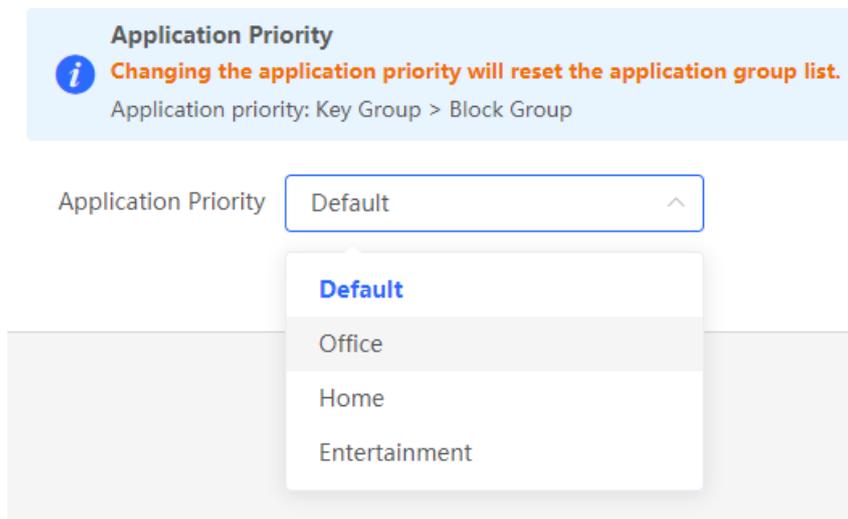
Select a template from the **Application Priority** drop-down list box.

Four application priority templates are predefined to meet needs in different scenarios. You can switch among the templates as needed.

Smart Flow Control

Custom Policy

Application Priority



The application priority templates are as follows:

- **Default:** This template is used during device initialization. The traffic bandwidth is not guaranteed or suppressed for any application.
- **Office:** This template is designed for the office scenario, where application traffic from the office network is guaranteed preferentially.
- **Home:** This template is designed for the home scenario, where application traffic from the home network is guaranteed preferentially.
- **Entertainment:** This template is designed for the entertainment scenario, where application traffic from the entertainment network is guaranteed preferentially.

(2) Create an application group list.

Each default template has three application groups: key group, block group, and normal group. The application priorities of the key group, normal group, and block group are in descending order:

- **Key Group:** Traffic from applications in the application list for this group is guaranteed preferentially.
- **Block Group:** Traffic from applications in the application list for this group is suppressed to preferentially guarantee the traffic from applications with a higher priority.
- **Normal Group:** All the applications in the application library beyond **Key Group** and **Block Group** are included in this group. Traffic from applications in this group are guaranteed after traffic from applications of **Key Group** is guaranteed.

After you select a template, **Key Group**, **Block Group**, **Normal Group**, and the application list for each group in the current template are displayed. You can click **More** to view details of each application list.

You can click **Edit** in the **Action** column next to the key group and block group to edit the application list, allowing traffic from these applications to be guaranteed or suppressed.

Smart Flow Control Custom Policy Application Priority

Application Priority
 **Changing the application priority will reset the application group list.**
Application priority: Key Group > Block Group

Application Priority

Application Group List

Group Name	Application List	Action
Key Group	Communication	Edit
Block Group	Play.. More Play Video	Edit
Normal Group	Other	Edit

Edit ✕

Group Name

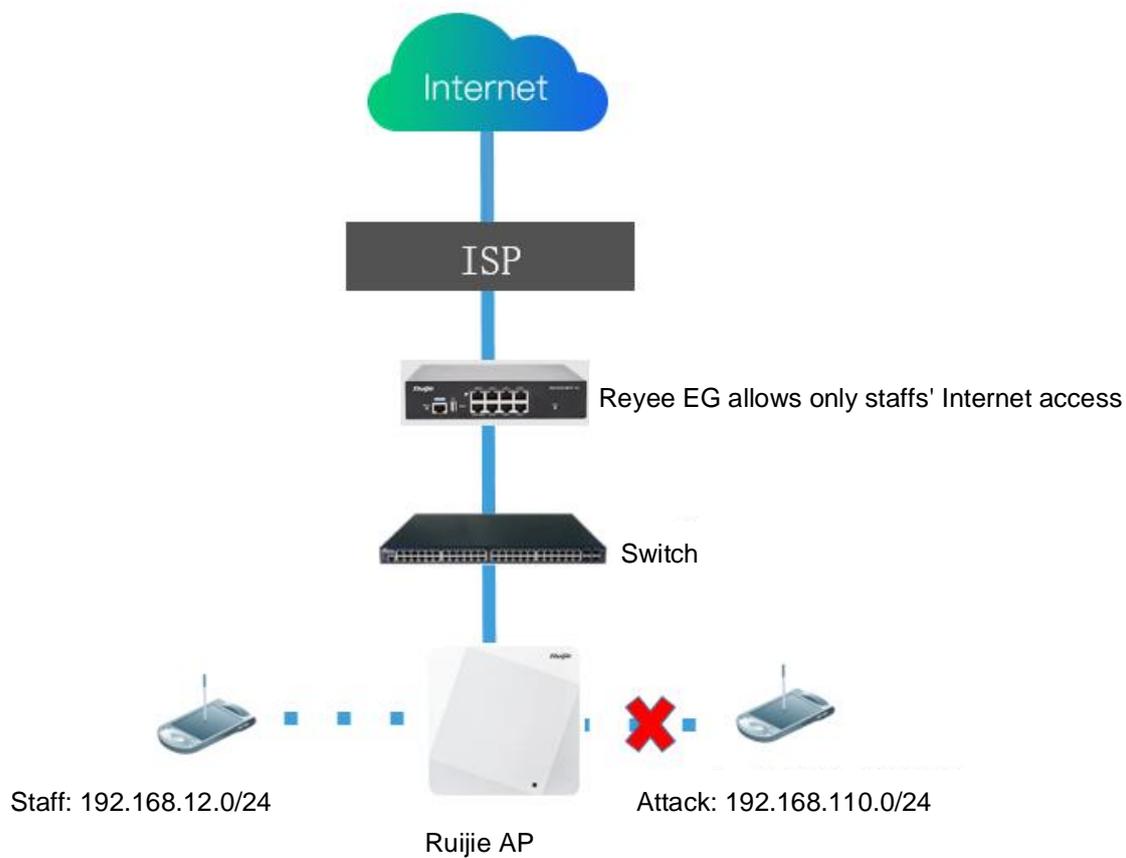
Application List Play ✕ Video ✕ ✕ ▲

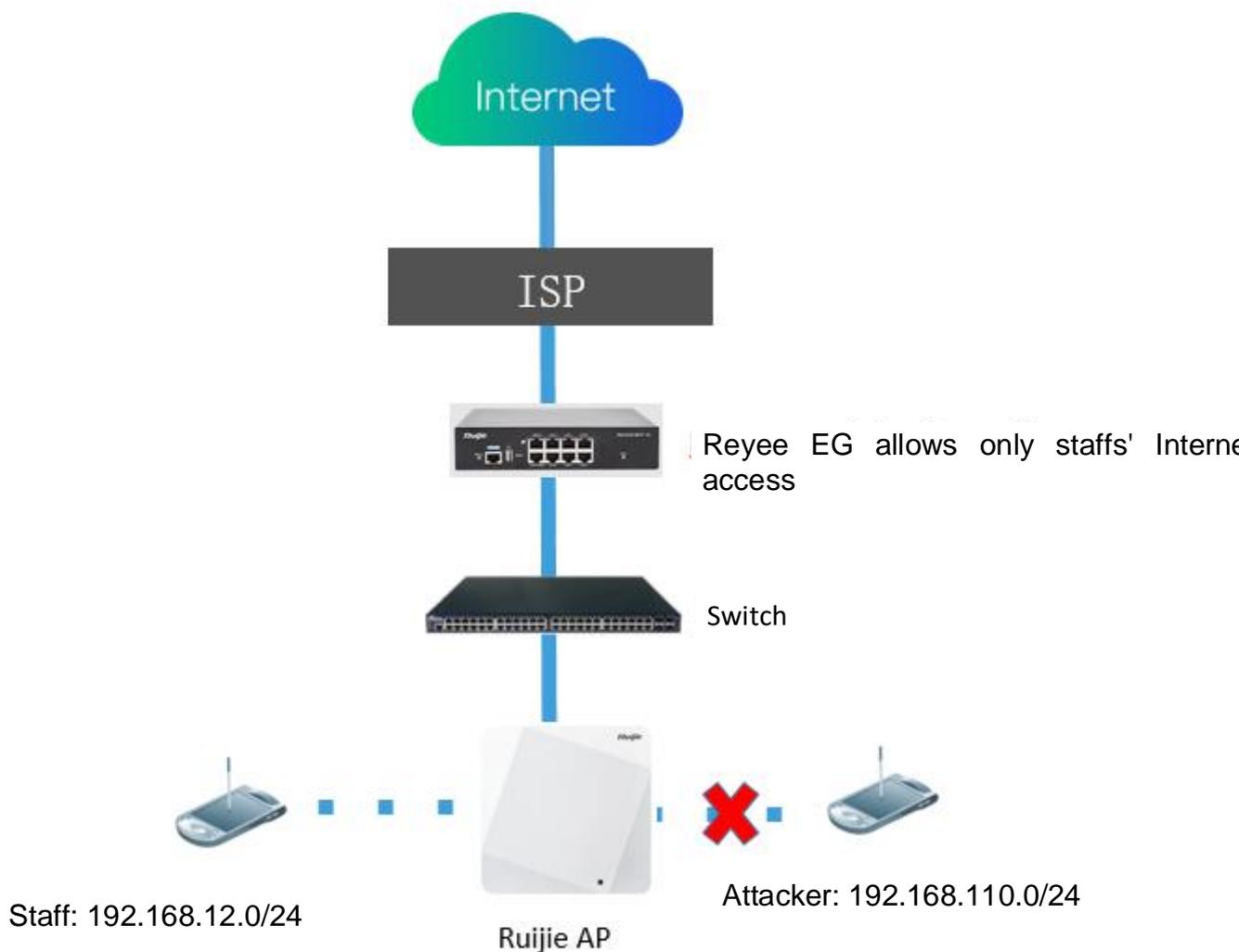
- ▶ Communication
- ▶ Video
- ▶ Shopping
- ▶ Play
- ▶ Databank
- ▶ P2PSoftware
- ▶ AppStore
- ▶ Payment

-  **Caution**
- If you switch the application library, the application list will change.
 - The application list will be reset after you switch the application priority template.

4.13 Security

4.13.1 Application Scenario





4.13.2 Configuring the ARP List and ARP Guard

The device learns IP addresses and MAC addresses of network devices connected to its interfaces and generates ARP entries. You can enable ARP guard and configure IP-MAC binding to restrict Internet access of LAN hosts and improve network security.

- (1) Switch to the **Local** mode. Choose **Security > ARP List**.
- (2) Before enabling ARP guard, you must configure the binding between IP addresses and MAC addresses in either of the following ways:
 - Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them.

i The device learns IP-MAC mapping of all devices connected to its interfaces. You can bind or filter the MAC address.
 Enable ARP guard and configure IP-MAC binding to improve network security. ?

ARP Guard

Enable **Only the devices configured with IP-MAC binding are allowed to access the Internet.**

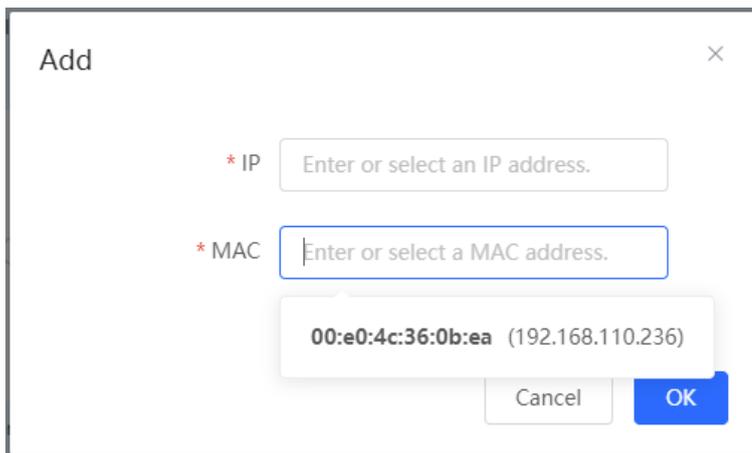
ARP List

Search by IP/MAC

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

No.	MAC	IP	Type	Action
<input type="checkbox"/> 1	00:e0:4c:36:0b:ea	192.168.110.236	Static	Edit Delete
<input checked="" type="checkbox"/> 2	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	<input type="button" value="Bind"/>

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



- (3) Click **Enable** to enable ARP guard.

After ARP guard is enabled, only LAN hosts with IP-MAC binding can access the external network.

ARP Guard

Enable **Only the devices configured with IP-MAC binding are allowed to access the Internet.**

Outbound Interface **Select All**
 Default VLAN **VLAN 333**

Set the range for the function to take effect.

If you check **Select All**, the ARP guard function will take effect on all clients on the LAN. If you select a specified port, the ARP guard function will take effect only on clients connected to the port.

4.13.3 Configuring MAC Address Filtering

You can enable MAC address filtering and configure a whitelist or blacklist to effectively control Internet access from LAN hosts.

- Whitelist: Allow only hosts whose MAC addresses are in the filter rule list to access the Internet.
 - Blacklist: Prevent hosts whose MAC addresses are in the filter rule list from accessing the Internet.
- (1) Switch to the **Local** mode. Choose **Security > MAC Filtering**.
 - (2) Click **Add**. In the dialog box that appears, enter the MAC address and remarks. The text box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the MAC address. Click **OK**. A filter rule is created.

MAC Filtering
Enable MAC address filtering and configure the filtering type to control the host's access to the Internet.

MAC Filtering Click to enable MAC address filtering.

Filtering Type: Blacklist

Save

Filtering Rule List + Add Delete Selected

Up to 80 rules can be added.

	MAC	Remark	Action
	No Data		

Add

* MAC: Enter or select a MAC address.

Remark:

Cancel OK

- (3) Enable MAC address filtering, set **Filtering Type**, and click **Save**.

MAC Filtering

MAC Filtering



The following hosts are not allowed to access the Internet.

Filtering Type

Blacklist

Save

4.13.4 Configuring Device Security

Note

This feature is supported by only R202 and later versions.

1. Overview

Prohibit Ping: This function identifies and directly discards ping packets in the traffic sent to the device, so as to prohibit the ping operation on the device. The device can be pinged from the administrative IP address only.

Admin IP Address: Packets sent from the administrative IP address are allowed to pass through.

2. Enabling the Ping Prohibition Function

Switch to the **Local** mode. Choose **Security > Local Safety**.

The ping prohibition function includes the following:

- If you select **Prohibit LAN**, ping packets sent from all clients on the LAN to the device will be discarded.
- If you select **Prohibit WAN**, ping packets sent from all clients on the WANs to the device will be discarded. Ping packets sent from a client to the device will be responded only after the IP address of the client is contained in **Admin IP Address**. For details on how to configure admin IP addresses, see [Configuring an Admin IP Address](#).

NFPP

Prohibit Ping Prohibit LAN Prohibit WAN

Save

Admin IP Address + Add Delete Selected

Up to 32 entries can be added.

Username	IP Range	Outbound Interface	Action
No Data			

1 / 10/page Total 0

3. Configuring an Admin IP Address

Switch to the **Local** mode. Choose **Security > Local Safety**.

Click **Add**. Then you can configure admin IP address information.

NFPP

Prohibit Ping Prohibit LAN Prohibit WAN

Save

Admin IP Address **+ Add** **Delete Selected**

Up to **32** entries can be added.

<input type="checkbox"/>	Username	IP Range	Outbound Interface	Action
No Data				

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

- Configuring an admin IP address (based on an IP address)

Add ×

* Username

Specified Mode **IP Range** Outbound Interface

- (1) Configure a name for the admin IP address.
The name is a string of 1 to 32 characters.
- (2) Set **Specific Mode** to **IP Range**.
- (3) Configure an IP address.
You can specify a single IP address or an IP address range.

- Configuring an admin IP address (based on a port)

Add ×

* Username

Specified Mode IP Range **Outbound Interface**

- (1) Configure a name for the admin IP address.
The name is a string of 1 to 32 characters.

(2) Set **Specific Mode** to **Outbound Interface**.

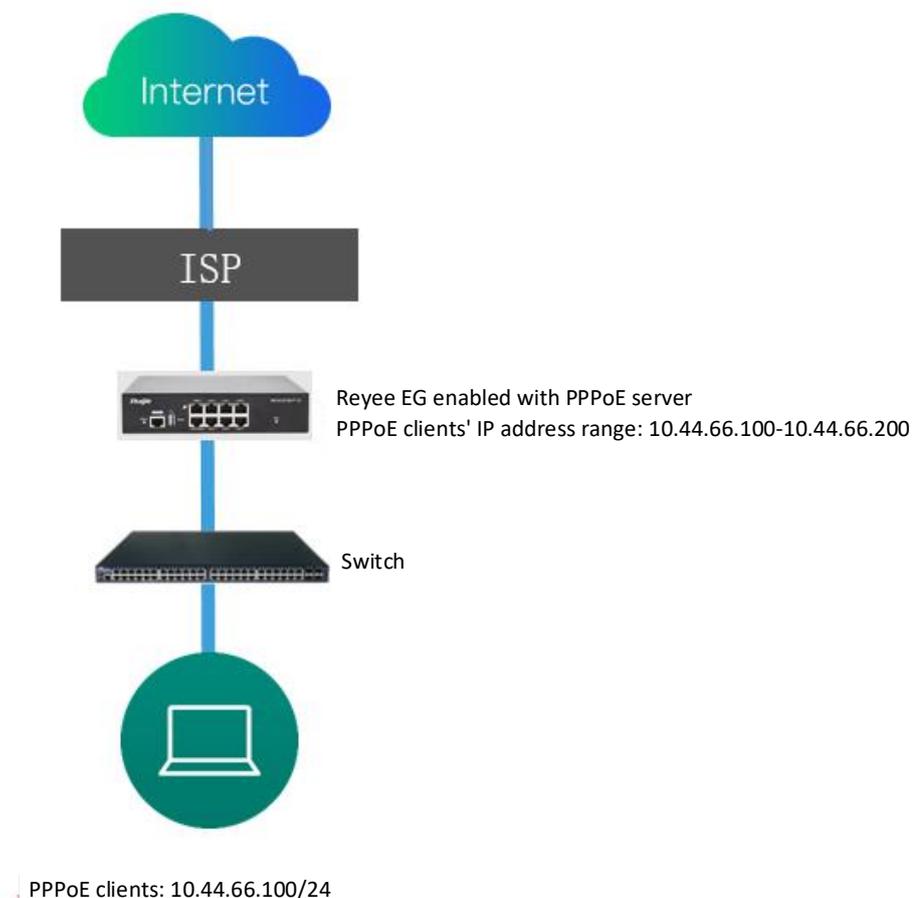
(3) Specify the port.

You can select a LAN port or WAN port as the outbound interface.

4.14 Configuring the PPPoE Server

4.14.1 Application Scenario

Point-to-Point Protocol over Ethernet (PPPoE) is a network tunneling protocol that encapsulates PPP frames into Ethernet frames. When the router functions as a PPPoE server, it provides the access service to LAN users and supports bandwidth management.



4.14.2 Global Settings

Switch to the **Local** mode. Choose **Advanced** > **PPPoE Server** > **Global Settings**.

Set **PPPoE Server** to **Enable** and configure PPPoE server parameters.

Global Settings Account Settings Account Management Exceptional IP Address Online Clients

Global Settings

1. MAC binding and MAC filtering are not valid for PPPoE clients.
 2. The IP address of the PPPoE server cannot overlap with any interface IP range.
 3. The authentication function is not valid for PPPoE clients.

PPPoE Server Enable Disabled

Mandatory PPPoE Dialup Enable Disable

* Local Tunnel IP

* IP Range

VLAN

Primary DNS Server

Secondary DNS Server

* Unanswered LCP Range: 1-60
 Packet Limit

Auth Mode PAP CHAP
 MSCHAP MSCHAP2

Table 4-7 PPPoE Server Configuration

Parameter	Description
PPPoE Server	Specify whether to enable the PPPoE server function.
Mandatory PPPoE Dialup	Specify whether LAN users must access the Internet through dialing.
Local Tunnel IP	Set the P2P address of the PPPoE server.
IP Range	Specify the IP address range that can be allocated by the PPPoE server to authenticated users.
VLAN	Set the VLAN ID of the PPPoE server.
Primary/Secondary DNS Server	Specify the DNS server address delivered to authenticated users.
Unanswered LCP Packet Limit	When the number of LCP packets with no response in one link exceeds the specified value, the PPPoE server automatically disconnects the link.

Parameter	Description
Auth Mode	Select at least one authentication mode among PAP, CHAP, MSCHAP, and MSCHAP2.

4.14.3 Configuring a PPPoE User Account

Switch to the **Local** mode. Choose **Advanced > PPPoE Server > Account Settings**.

Click **Add** to create a PPPoE authentication user account. Created PPPoE authentication user accounts are displayed in the **Account List** section. Find the target account and click **Edit** to modify account information. Find the target account and click **Delete** to delete the account.

Global Settings [Account Settings](#) Account Management Exceptional IP Address Online Clients

Account Settings ?

Account List [+ Add](#) [Delete Selected](#)

Up to **15** entries can be added. Clients **1**

<input type="checkbox"/>	Username	Password	Expire Date	Status	Account Management	Remark	Action
<input type="checkbox"/>	test	test	2022-04-30	Enable	-		Edit Delete

Add
×

* Username

* Password

Expire Date

Remark

Status

Flow Control

* Account

Management

Table 4-8 PPPoE User Account Configuration

Parameter	Description
Username/Password	Set the username and password of the authentication account for Internet access through PPPoE dialing.
Expire Date	Set the expiration date of the authentication account. After the account expires, it can no longer be used for Internet access through PPPoE authentication.
Remark	Enter the account description.
Status	Specify whether to enable this user account. If the account is disabled, the account is invalid and cannot be used for Internet access through PPPoE authentication.

Parameter	Description
Flow Control	Specify whether to apply flow control on the account. If flow control is enabled, you need to configure flow control policies for PPPoE authentication users. If smart flow control is disabled, Flow Control must be disabled. To enable Flow Control , enable smart flow control first. For details on how to configure smart flow control, see section 6.6.2 错误!未找到引用源。 .
Account Management	After flow control is enabled, you need to configure a flow control package for the current account to restrict user bandwidth accordingly. For details on how to configure and view flow control packages, see section 3.12.4 错误!未找到引用源。 .

4.14.4 Configuring a Flow Control Package

Switch to the **Local** mode. Choose **Advanced > PPPoE Server > Account Management**.

If smart flow control is disabled, the flow control package for the account does not take effect. Before you configure a flow control package, enable smart flow control. For details on how to configure smart flow control, see section [6.6.2](#) [错误!未找到引用源。](#) .

Click **Add** to create a flow control package. Created flow control packages are displayed in the **Account Management List**. You can modify or delete the packages.

Global Settings	Account Settings	Account Management	Exceptional IP Address	Online Clients
---------------------------------	----------------------------------	------------------------------------	--	--------------------------------

Account Management List					+ Add	Delete Selected
Up to 10 entries can be added.						
<input type="checkbox"/>	Account Name	Uplink Rate	Downlink Rate	Interface	Action	
<input type="checkbox"/>	test	CIR 100000Kbps PIR 100000Kbps PIR per User No Limit	CIR 100000Kbps PIR 100000Kbps PIR per User No Limit	WAN	Edit Delete	

Add
×

* Account Name

Uplink Rate * CIR Kbps * PIR Kbps PIR per User No Limit t

Downlink Rate * CIR Kbps * PIR Kbps PIR per User No Limit t

* Interface WAN

Table 4-9 PPPoE User Flow Control Package Configuration

Parameter	Description
Account Name	Set the name of the flow control package. When configuring an authentication account, you can select a flow control package based on the name.
Uplink/Downlink CIR	Specify the uplink and downlink committed information rate (CIR) for an authentication account when the bandwidth is insufficient.
Uplink/Downlink PIR	Specify the uplink and downlink peak information rate (PIR) that can be used by an authentication account when the bandwidth is sufficient.
Uplink/Downlink PIR per User	Specify the PIR that can be consumed by each user. This parameter is optional. By default, the PIR per user is not limited.
Interface	Specify the interface to which the flow control package applies.

4.14.5 Configuring Exceptional IP Addresses

Switch to the **Local** mode. Choose **Advanced > PPPoE Server > Exceptional IP Address**.

To configure clients with some IP addresses in a specific VLAN to access the Internet without passing account and password authentication, you can configure these IP addresses as exceptional IP addresses on the device enabled with the PPPoE server.

The created exceptional IP addresses are displayed in **Exceptional IP Address List**. Click **Edit** to modify the exceptional IP address and click **Delete** to delete the exceptional IP address.

Start IP Address/End IP Address: indicates the start or end exceptional IP address.

Remark: indicates the description of an exceptional IP address.

Status: indicates whether an exceptional IP address is valid.

Global Settings Account Settings Account Management Exceptional IP Address Online Clients

Exceptional IP Address ⓘ

Exceptional IP Address List [+ Add](#) [Delete Selected](#)

Up to **5** entries can be added.

<input type="checkbox"/>	Start IP Address	End IP Address	Remark	Status	Action
<input type="checkbox"/>	172.26.1.2	172.26.1.100		Enable	Edit Delete

Add ×

* Start IP
Address

* End IP
Address

Remark

Status

[Cancel](#) [OK](#)

4.14.6 Checking Online Users

Switch to the **Local** mode. Choose **Advanced > PPPoE Server > Online Clients**.

Check information about end users that access the Internet through PPPoE dialing. Click **Disconnect** to disconnect a user from the PPPoE server.

Global Settings Account Settings Account Management Exceptional IP Address Online Clients

Online Clients ?

Account List Disconnect Refresh

Online Clients **0**

<input type="checkbox"/>	Username	IP	MAC	Up on	Action
No Data					

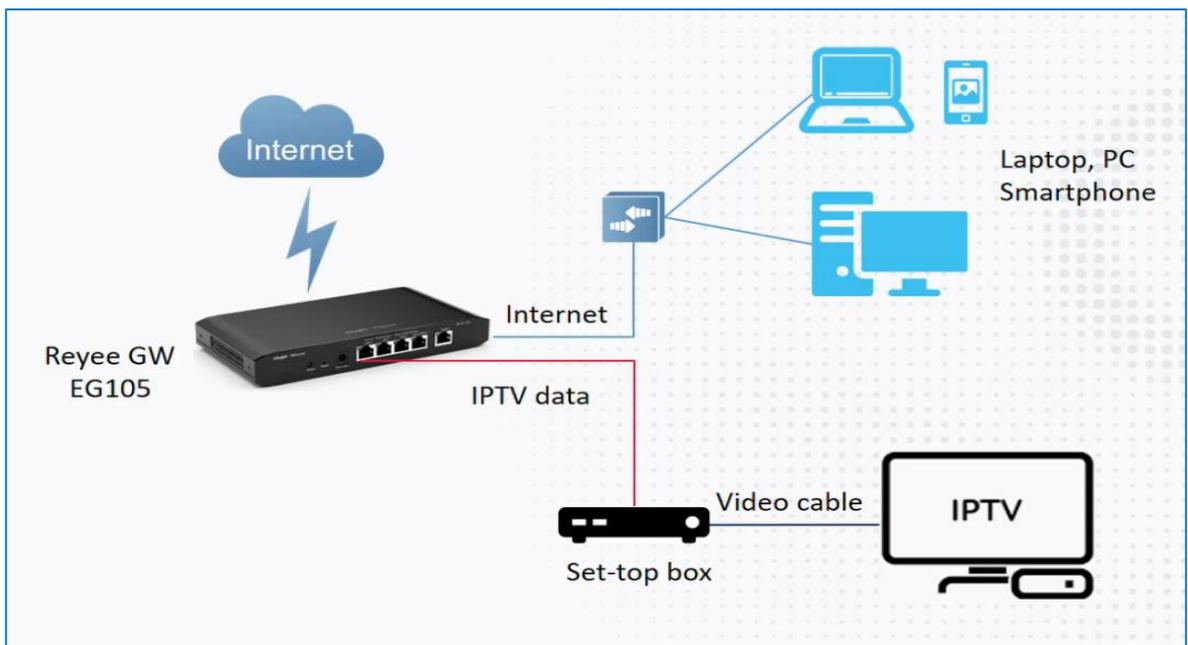
Table 4-10 PPPoE Online User Information

Parameter	Description
Username	Total number of online users that access the Internet through PPPoE dialing.
IP	IP address of the client.
MAC	MAC address of the client.
Up on	Time when the user accesses the Internet.

4.15 IPTV

4.15.1 Application Scenario

- Scenario 1: Dual-WAN Scenario



- Scenario 2: Single-WAN Scenario



4.15.2 Dual-WAN Configuration

- (1) Connect the ISP cable with a WAN port, and connect your PC with a LAN port. Use the default IP address of 192.168.110.1 to log in to the Reyye EG and configure your EG to access the Internet successfully according to the wizard.
- (2) Switch to the **Local** mode. Choose **Network > IPTV > IPTV/VLAN**.

The screenshot shows the Ruijie web management interface. The 'Network' menu is highlighted, and the 'IPTV/VLAN' sub-menu is selected. The configuration page shows various settings for IPTV/VLAN, including Mode (Custom), AG (Internet), and LAN0-LAN3 (Internet). The 'Internet VLAN (WAN)' toggle is also visible.

- (3) Configure **IPTV VLAN ID** or **IP-Phone VLAN ID**.
 - o If you are in following regions listed in the red box, you can choose the mode directly.

IPTV/VLAN IPTV/IGMP

i IPTV/VLAN settings.

IPTV/VLAN

* Mode

* AG
* AG
* AG
* LAN0
* LAN1
* LAN1
Custom

* LAN2

* LAN3

* LAN4/WAN3

* LAN5/WAN2

Internet VLAN (WAN) 802.1Q Tag

Save

- o If you are not in these regions, you can choose **Custom**. Then contact with an ISP for IPTV settings and connect the IPTV and IP phone with LAN ports. For example, the VLAN IDs for IPTV, IP phone, and Internet services are 100, 200, and 300, respectively.

[IPTV/VLAN](#) [IPTV/IGMP](#)

i IPTV/VLAN settings.

IPTV/VLAN

* Mode

* LAN0

* LAN1/WAN3

* LAN2/WAN2

* LAN3/WAN1

* IPTV VLAN ID

* IP-Phone VLAN ID

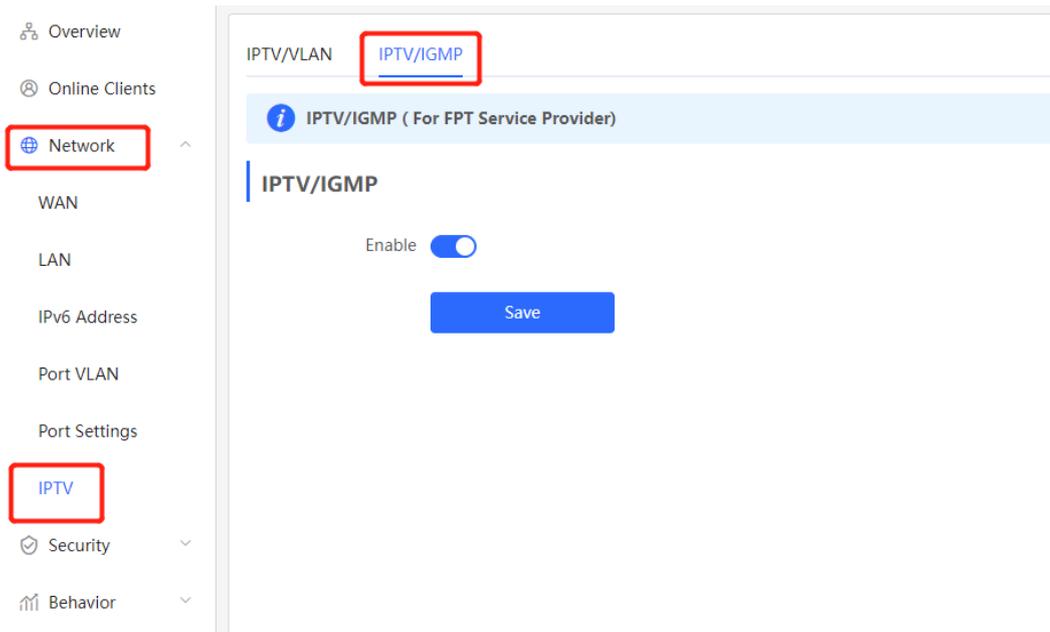
Internet VLAN (WAN) 802.1Q Tag

* Internet VLAN ID

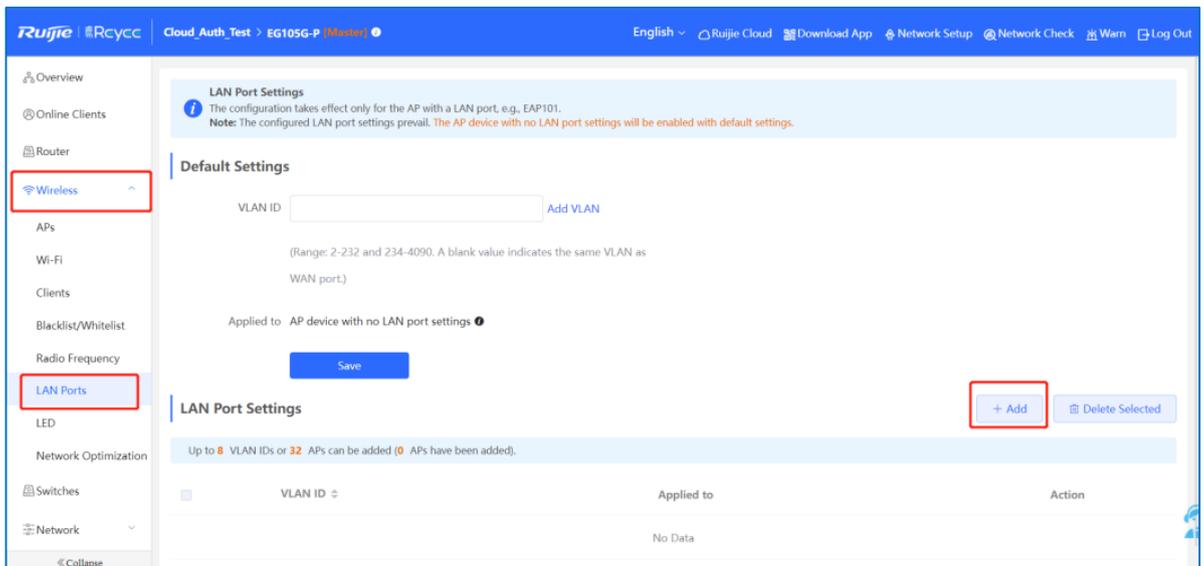
4.15.3 Single-WAN Configuration

After performing IPTV configuration on the Reyee EG that has only one WAN port, you need to configure the IPTV VLAN 100 on the LAN port of the wall AP. If the router has two WAN ports, ignore this step.

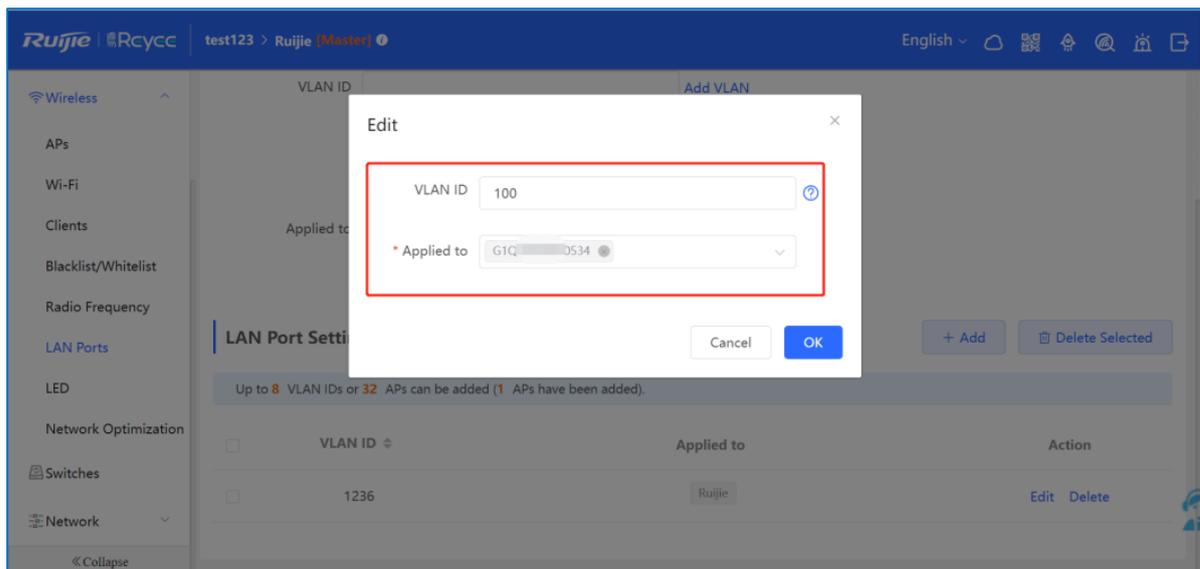
- (1) Log in to the web management system. Choose **Network > IPTV > IPTV/IGMP** and enable **IPTV/IGMP**.



(2) Log in to the web management system of a wall AP. Choose **Wireless > LAN Ports > Add**.



Set the VLAN ID to 100, which is applied to the wall AP.



Caution

IPTV is supported by only Reyyee OS 1.55 and later versions.

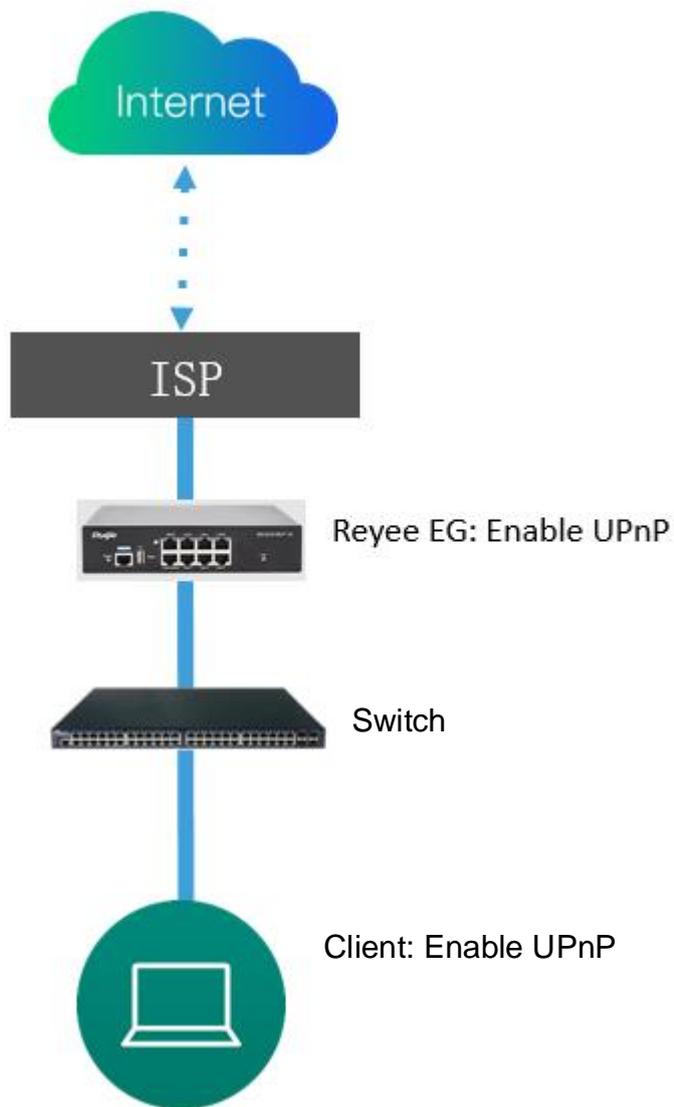
4.16 UPnP

Application Scenario

With the Universal Plug and Play (UPnP) function enabled, the device can switch the port used by the terminal's Internet service according to the terminal's request, achieving NAT conversion. When a terminal on the Internet wants to access resources of the device's intranet, the device can automatically add port mapping entries to realize service transmission across internal and external networks. Common applications that support the UPnP protocol include MSN Messenger, Thunder, BT, and PPLive.

There are three requirements for applying UPnP:

- The device must be enabled with UPnP.
- The operating system of internal hosts must support UPnP.
- Applications must support UPnP.

**Procedure**

- (1) Switch to the **Local** mode. Choose **Advanced > UPnP Settings > Enable** to enable UPnP on your phone or PC.
- (2) The router will automatically detect your device and enable port mapping for the device. Finally you can use the external IP address and port to access your phone or PC service.

The screenshot shows the MikroTik WinBox interface for 'Local DNS Settings'. The left sidebar contains a menu with 'Advanced' and 'UPnP Settings' highlighted. The main content area is titled 'UPnP Settings' and includes a description: 'UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving communication between devices.' Below this, there is an 'Enable' toggle switch (checked) and a 'Default Interface' dropdown menu set to 'lan1'. A 'Save' button is located below the dropdown. Underneath, there is a section titled 'UPnP List' with a table. The table has five columns: 'Protocol', 'App', 'Client IP Address', 'Internal Port', and 'External Port'. The table is currently empty, with the text 'No UPnP Device' centered below the header row.

Protocol	App	Client IP Address	Internal Port	External Port
No UPnP Device				

5 Advanced Solution

5.1 Reeye Flow Control Solution

5.1.1 Application Scenario

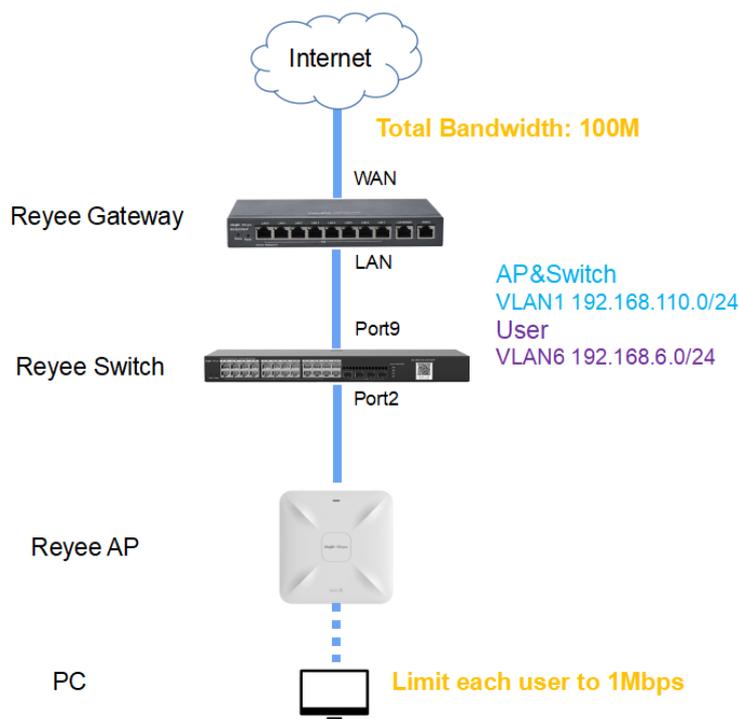
Flow control is used for setting rate limits of download and upload rates for the clients. With flow control configured, the router can protect the network bandwidth from being occupied by some clients.

5.1.2 Configuration Example

Requirement

The total bandwidth of the EG is limited to 100 Mbit/s and the rate of each user on the network segment of VLAN 6 is limited to 1 Mbit/s.

Network Topology

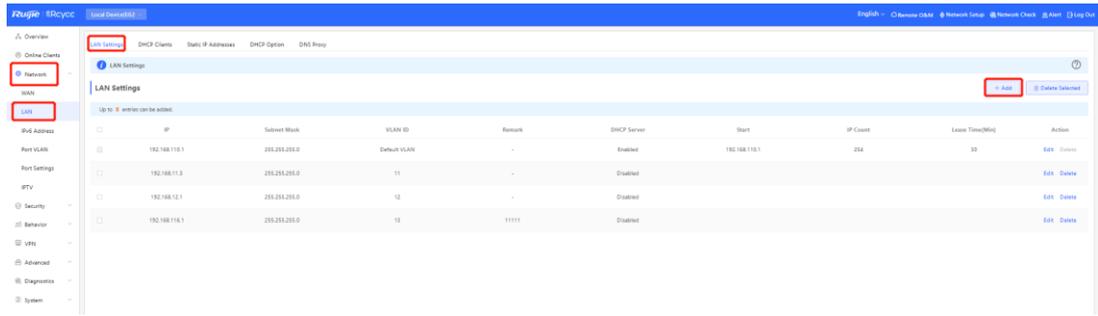


Network Description

- The EG works as a DHCP server to assign IP addresses to users, Reeye AP, and Reeye switch.
- The Reeye AP and switch obtain the IP address 192.168.110.0/24 on the network segment of VLAN 1 for Internet access.
- The users obtain the IP address 192.168.6.0/24 on the network segment in VLAN 6 for Internet access.

Configuration Steps

- (1) Perform basic network configuration.
 - a Switch to the **Local** mode. Choose **Network > LAN > LAN Settings > Add** and perform LAN settings and DHCP address pools of VLAN 1 and VLAN 6 on the router.



Add

X

* IP

* Subnet Mask

* VLAN ID

Remark

MAC

DHCP Server

* Start

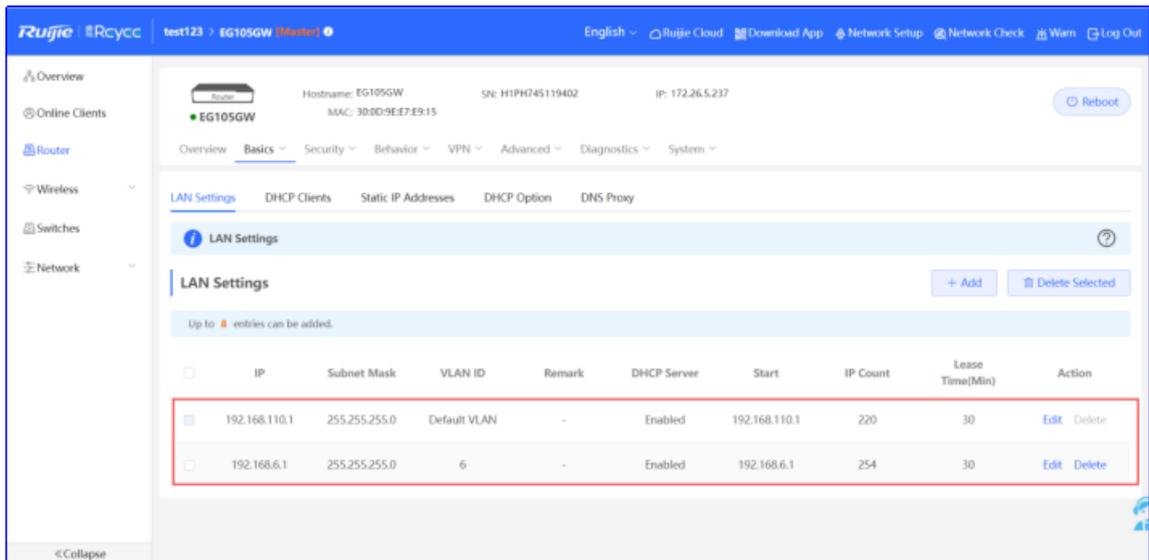
* IP Count

* Lease Time(Min)

DNS Server

Cancel

OK



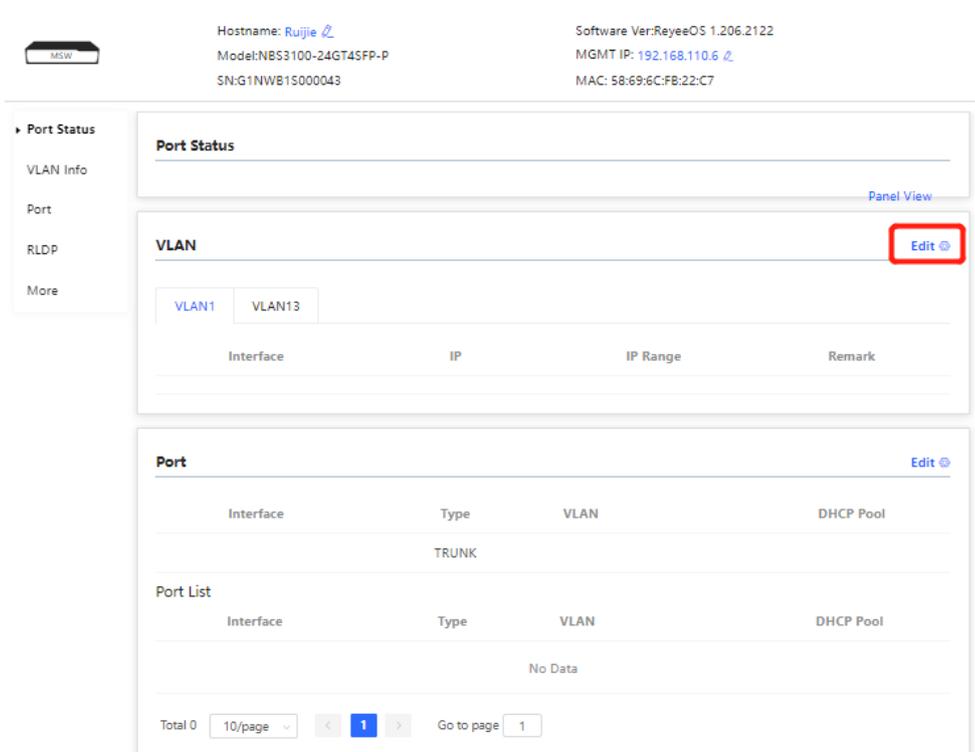
Caution

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

(2) Switch to the **Network** mode. Choose **Device > Switch**.



- a Select a device from **Device List** and access the configuration page.
- b In the **VLAN** pane, select a VLAN and click **Edit** to configure the VLAN.



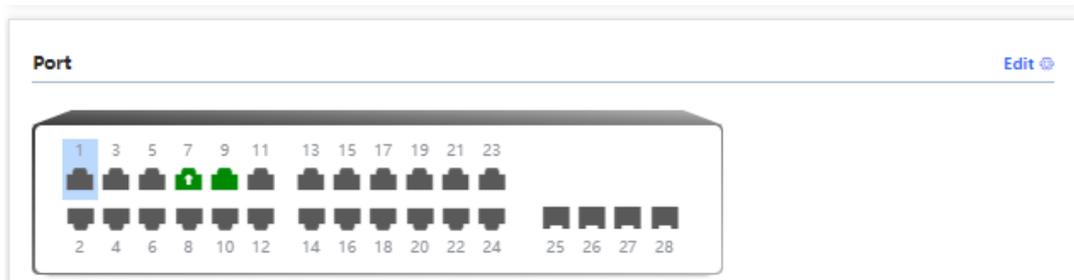
c Click **Add VLAN** to create VLAN 6 on the switch.

VLAN Info

Vlan ID	Remark	
1	VLAN0001	
13	11111	
6		

[+Add VLAN](#) [+Batch Add](#) [-Delete Selected](#)

- d In the **Port** pane, click **Edit**, configure port2 and port9 connected to the AP and EG as trunk ports and configure them to allow packets from VLAN 1 and VLAN 6 to pass through. Then check port settings on the switch.



Port

Available Unavailable Aggregate Uplink Copper Fiber

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

Selected Port ["Gi2"]

Routed Port Not Supported

Port Type

* Access VLAN:

- (3) Switch to the **Network** mode. Choose **Network > Wi-Fi > Wi-Fi Settings**, configure the SSID named **Reyee_test**, and associate VLAN 6 with this SSID.

Ruijie Rcycc Network

Navigation: Overview, Network, Network Planning, Wi-Fi, RLDP, DHCP Snooping, WIO, Radio Frequency, Reyee Mesh, LAN Ports, LED, Alerts, Batch Config, Devices, Gateway, Firewall, Clients Management, System

Wi-Fi Settings

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

Device Group: Default

* SSID: @Ruijie-mBCFA

Band: 2.4G + 5G

Security: Open

Wireless Schedule: All Time

VLAN: 6

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

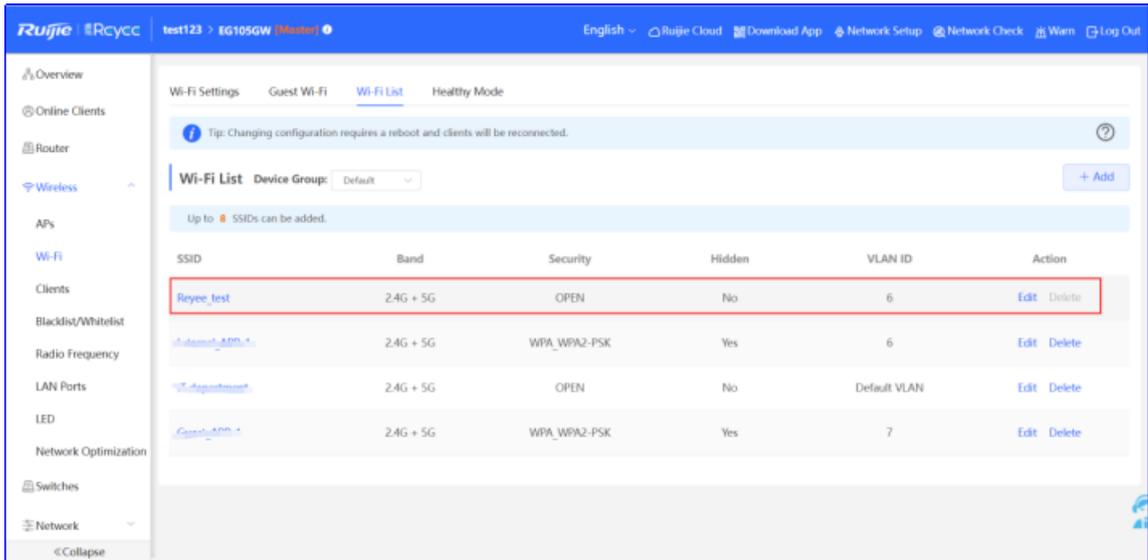
Client Isolation: Prevent wireless clients of this Wi-Fi from communicating with one another.

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

XPress: (The client will experience faster speed.)

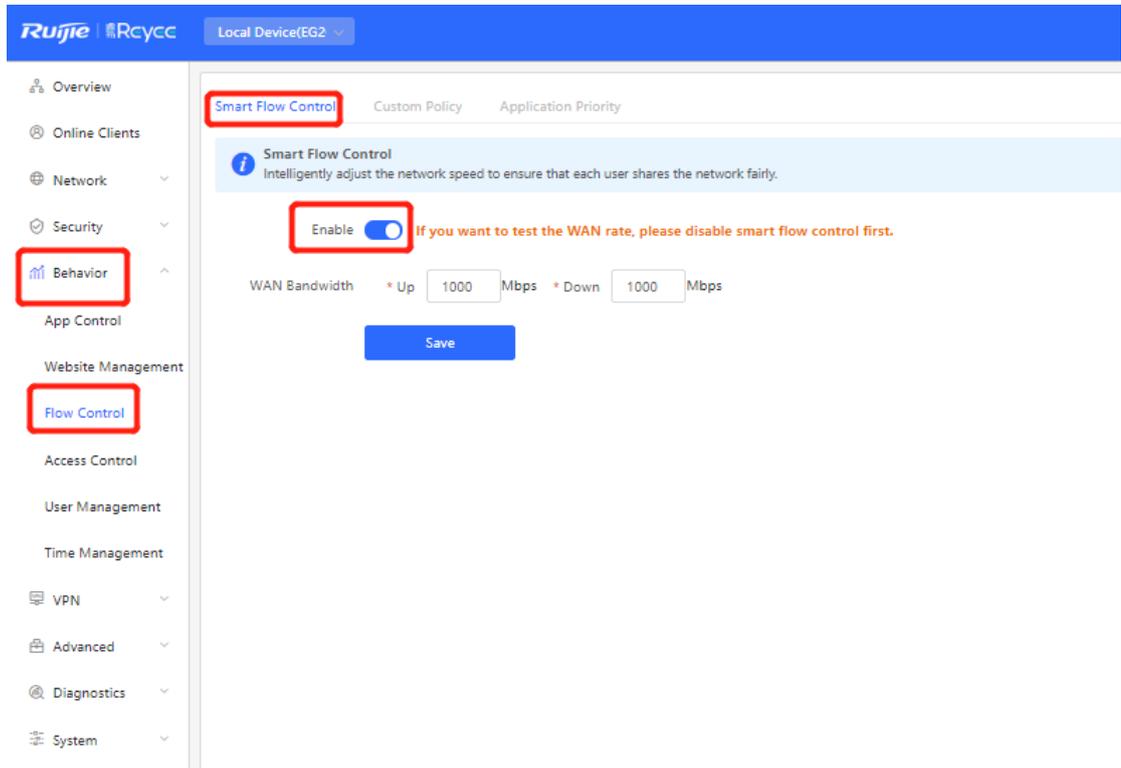
Layer-3 Roaming: (The client will keep his IP address unchanged in this Wi-Fi network.)

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



(4) Configure smart flow control.

a Switch to the **Local** mode. Choose **Behavior** > **Flow Control** and enable **Smart Flow Control**.



b Fill in the uplink and downlink WAN bandwidth as 100 Mbit/s and click **Save**.

Smart Flow Control Custom Policy Application Priority

Smart Flow Control
Intelligently adjust the network speed to ensure that each user shares the network fairly.

Enable **If you want to test the WAN rate, please disable smart flow control first.**

WAN Bandwidth * Up Mbps * Down Mbps

c After Step 2 is performed, **Custom Policy** will be displayed. Click **Add** to add a policy.

Smart Flow Control **Custom Policy**

Custom Policy
Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.

Policy List

Up to 30 entries can be added.

<input type="checkbox"/>	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
No Data									

Set Policy Name, IP Range, Bandwidth Type, Rate, and other parameters.

Edit ×

* Policy Name

* IP/IP Range

Bandwidth Type

Uplink Rate * CIR * PIR Kbps

Downlink Rate * CIR * PIR Kbps

Interface

Status

Smart Flow Control [Custom Policy](#)

Custom Policy
Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.

Policy List + Add + Delete Selected

Up to 30 entries can be added.

<input type="checkbox"/>	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
<input type="checkbox"/>	test	192.168.6.2-192.168.6.254	Independent	CIR 1000 Kbps PIR 1000 Kbps	CIR 1000 Kbps PIR 1000 Kbps	WAN	Enable ☑	Active	Edit Delete

- **Bandwidth Type**
 - **Shared:** indicates that the total bandwidth is shared by all IP addresses.
 - **Independent:** indicates that the rate limit is set for each IP address.
- **CIR:** indicates the committed information rate.
- **PIR:** indicates the peak information rate.

5.1.3 Configuration Verification

Use Speed test tool to check that each user is limited up to 1 Mbit/s.



5.2 Reye Cloud Authentication Solution

5.2.1 Working Principle

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

5.2.2 Application Scenario

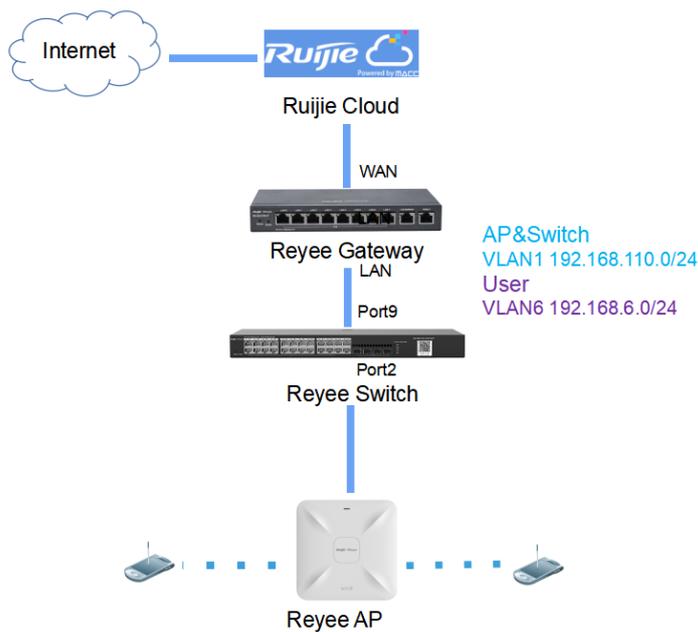
Portal authentication, also known as web authentication, is usually deployed in a guest-access network (such as a hotel or a coffee shop) to control clients' Internet access.

5.2.3 Configuration Example

Requirement

Users need to be authenticated before accessing the Internet. Reyyee AP does not support cloud authentication, and Reyyee EG needs to authenticate users.

Network Topology

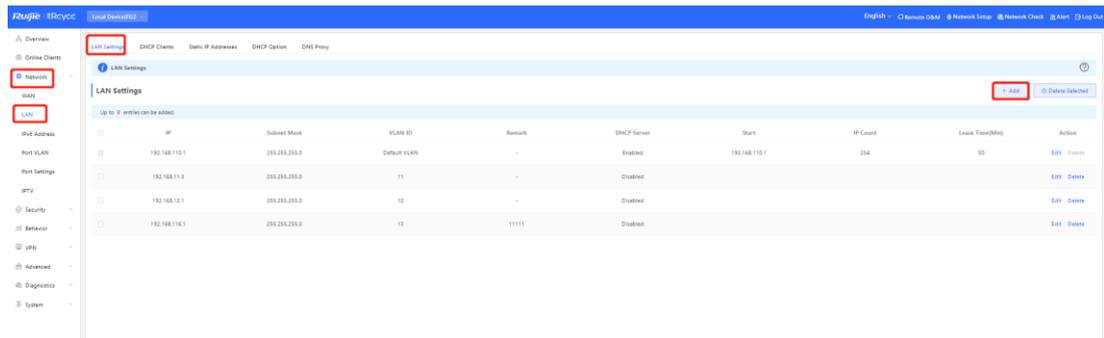


Network Description

- The EG works as a DHCP server to assign IP addresses to users, Reyyee AP, and Reyyee switch.
- The Reyyee AP and switch obtain the IP address 192.168.110.0/24 on the network segment of VLAN 1 for Internet access.
- Users obtain the IP address 192.168.6.0/24 on the network segment of VLAN 6 for Internet access.
- Ruijie Cloud manages and monitors the device and client status and provides captive authentication for clients.

Configuration Steps

- (1) Configure the basic network.
 - a Switch to the **Local** mode. Choose **Network > LAN > LAN Settings > Add**, and configure LAN settings and DHCP pool of VLAN 1 and VLAN 6 on the router.



Edit



* IP

* Subnet Mask

Remark

* MAC

DHCP Server

* Start

* IP Count

* Lease Time(Min)

DNS Server 192.168.110.1 ⓘ

Add
×

* IP

* Subnet Mask

* VLAN ID

Remark

MAC

DHCP Server

* Start

* IP Count

* Lease Time(Min)

DNS Server ⓘ

The screenshot shows the Ruijie RCloud interface for a device named EG105GW. The 'LAN Settings' section is active, displaying a table of configurations. A red box highlights two entries in the table:

IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete
192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete

⚠ Caution

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

(2) Switch to the **Network** mode. Choose **Device > Switch**.

The screenshot shows the 'Device List' table with the following columns: ID, SN, Status, Hardware, MAC, IP, Software Ver, and Model. Two devices are listed:

ID	SN	Status	Hardware	MAC	IP	Software Ver	Model
019A81000001	019A81000001	Online	Switch-C	88D4C79E2C7F	192.168.110.2	ReyOS 1.206.2132	MS110W-24GT48P-F
MAC21000001	MAC21000001	Online	Switch-C	80D0F8221BB0	192.168.110.1	ReyOS 1.206.2116	MS6502

- a Select a device from **Device List** and access the configuration page.
- b In the **VLAN** pane, select a VLAN and click **Edit** to configure the VLAN.

MSW

Hostname: [Ruijie](#)
Model: NBS3100-24GT45FP-P
SN: G1NWB15000043

Software Ver: ReyeOS 1.206.2122
MGMT IP: [192.168.110.6](#)
MAC: 58:69:6C:FB:22:C7

Port Status

VLAN Info

Port

RLDP

More

Port Status [Panel View](#)

VLAN [Edit](#)

VLAN1 | VLAN13

Interface	IP	IP Range	Remark
-----------	----	----------	--------

Port [Edit](#)

Interface	Type	VLAN	DHCP Pool
TRUNK			

Port List

Interface	Type	VLAN	DHCP Pool
No Data			

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

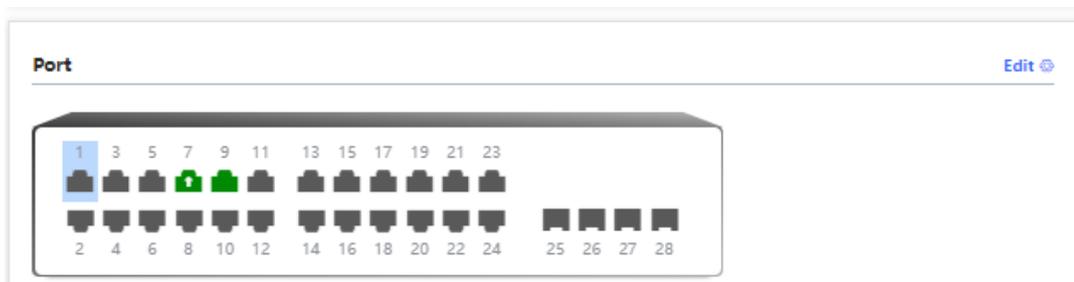
c Click **Add VLAN** to create VLAN 6 on the switch.

VLAN Info

Vlan ID	Remark	
1	VLAN0001	
13	11111	
6		

[+Add VLAN](#) [+Batch Add](#) [-Delete Selected](#)

- d In the **Port** pane, click **Edit**, configure port2 and port9 connected to the AP and EG as trunk ports and configure them to allow packets from VLAN 1 and VLAN 6 to pass through, and check port settings on the device.



Port

Available
 Unavailable
 Aggregate
 Uplink
 Copper
 Fiber

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

Selected Port ["Gi2"]

Routed Port Not Supported

Port Type

* Access VLAN:

- Switch to the **Network** mode. Choose **Network > Wi-Fi > Wi-Fi Settings**, and configure the SSID named **Reyee_test** and associate VLAN 6 with this SSID.

Ruijie RCloud Network

Navigation: Overview, Network, Network Planning, Wi-Fi, RLDP, DHCP Snooping, WIO, Radio Frequency, Reyee Mesh, LAN Ports, LED, Alerts, Batch Config, Devices, Gateway, Firewall, Clients Management, System

Wi-Fi Settings

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

Device Group: Default

* SSID: @Ruijie-mBCFA

Band: 2.4G + 5G

Security: Open

Wireless Schedule: All Time

VLAN: 6

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

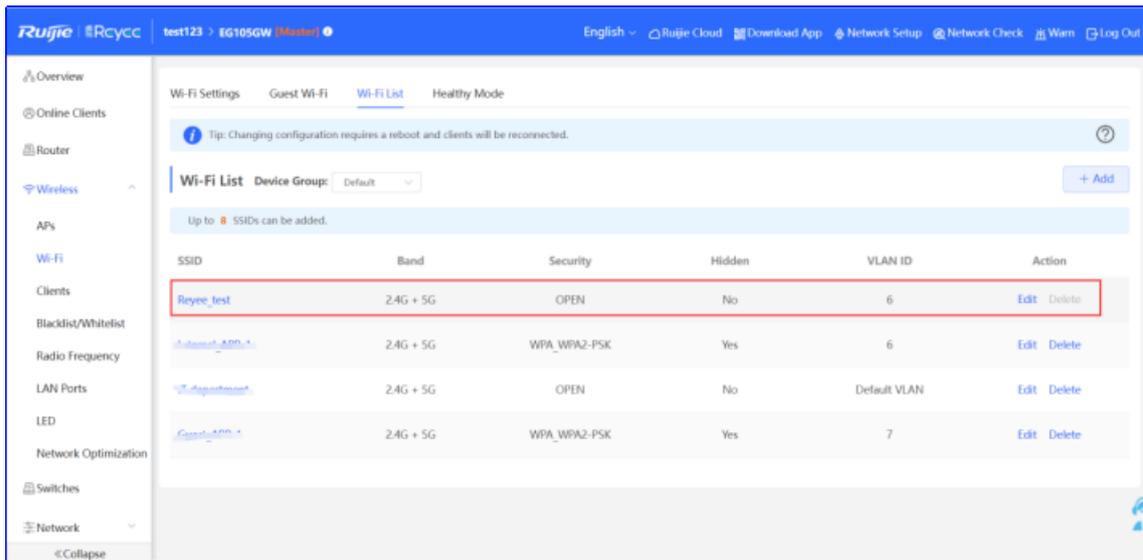
Client Isolation: Prevent wireless clients of this Wi-Fi from communicating with one another.

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

XPress: (The client will experience faster speed.)

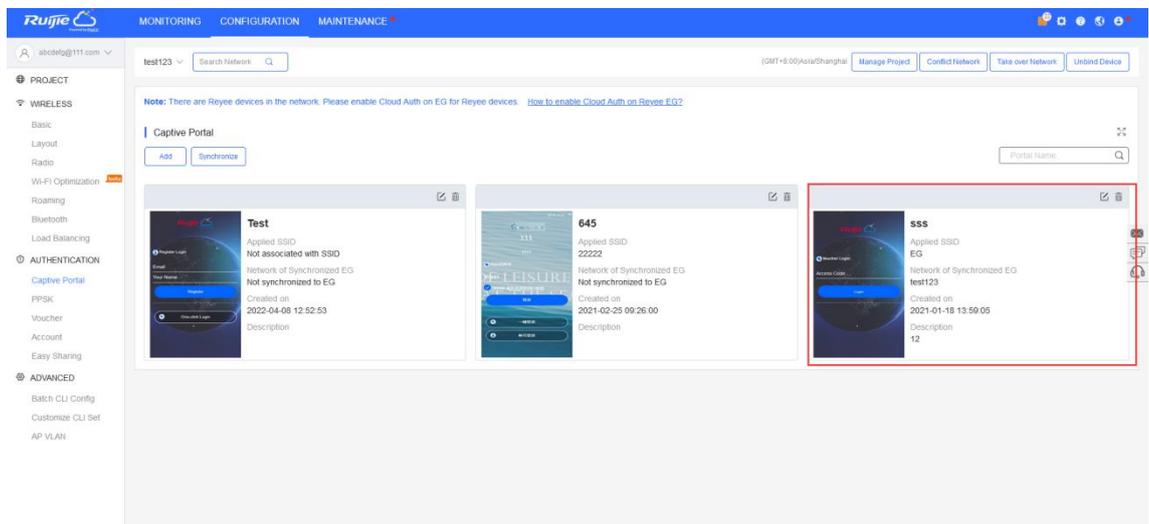
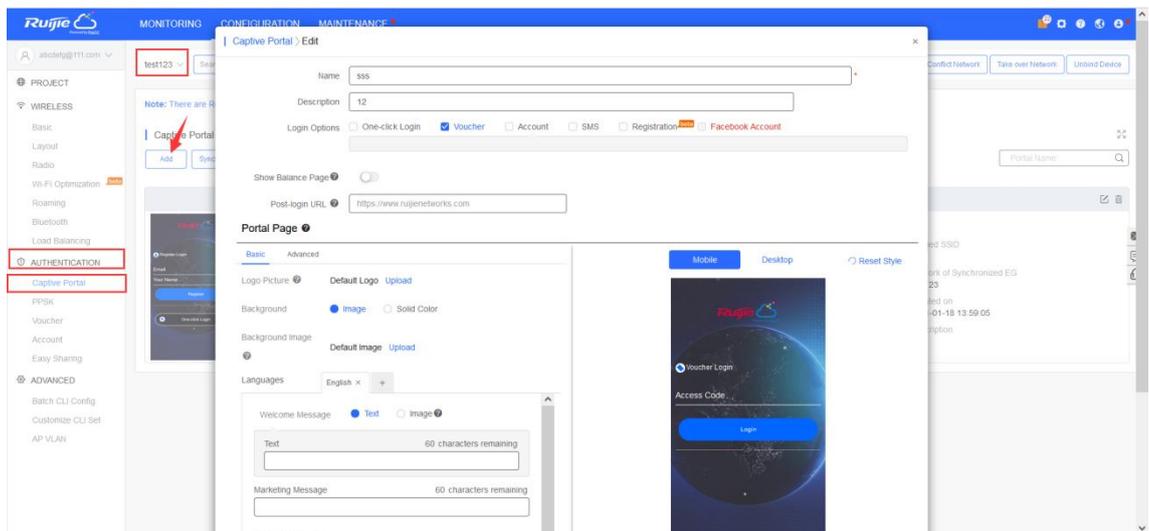
Layer-3 Roaming: (The client will keep his IP address unchanged in this Wi-Fi network.)

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



(4) Configure cloud authentication.

- a Choose **CONFIGURATION > AUTHENTICATION > Captive Portal** to access the captive portal page, and click **Add** to create a portal template and edit the captive portal template.



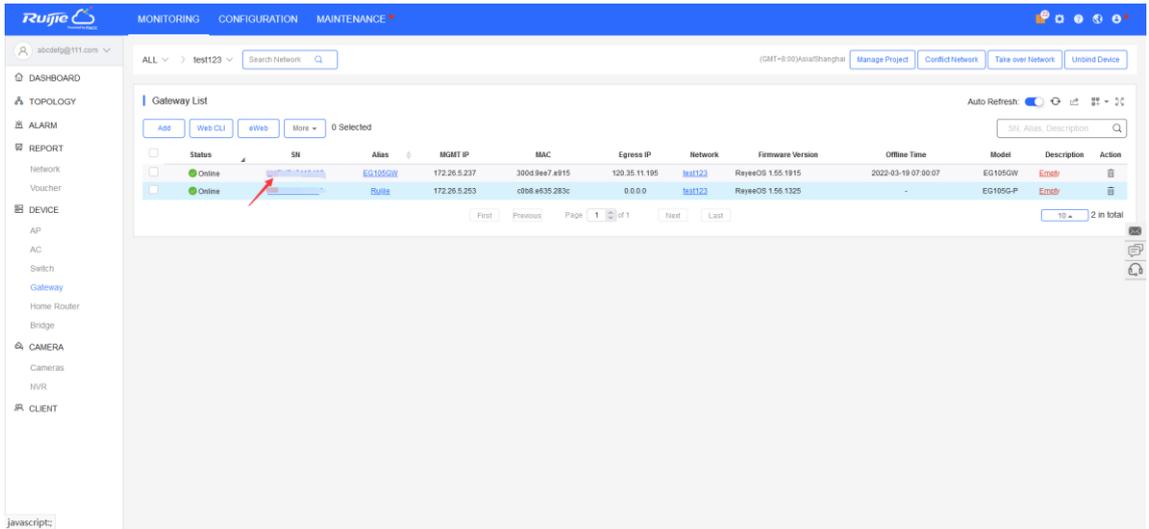
Note

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

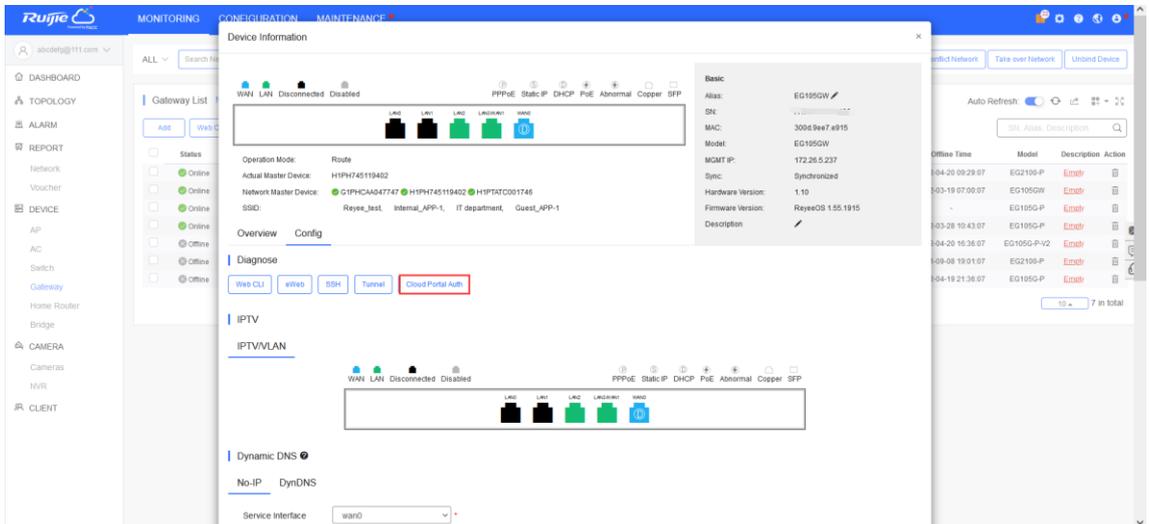
Voucher: indicates login with a random eight-digit password.

Account: indicates login with the account and password.

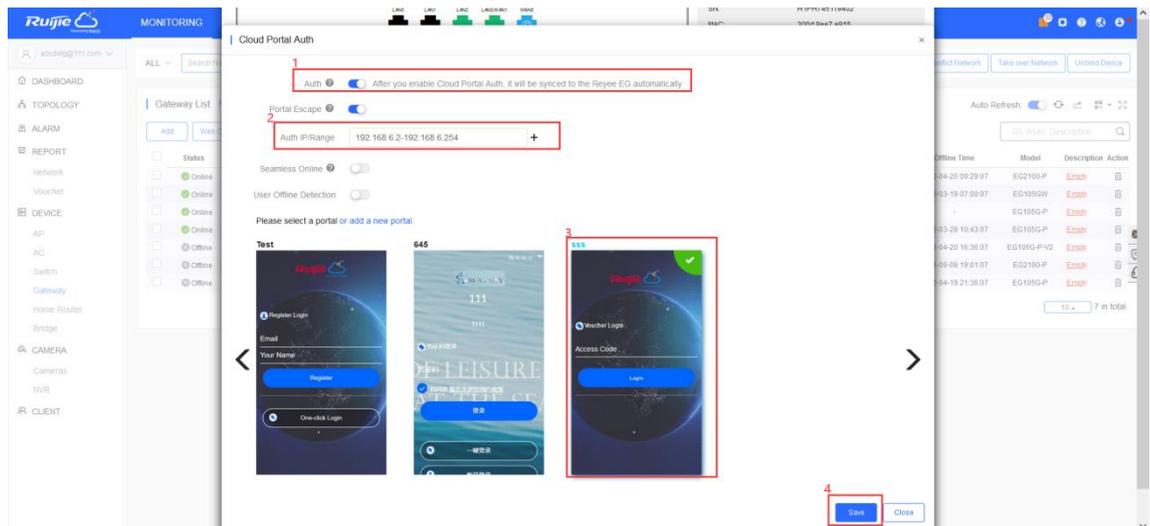
- b Make sure that the Reyee EG is online on Ruijie Cloud. Click its SN in the list to access the configuration page.



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



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

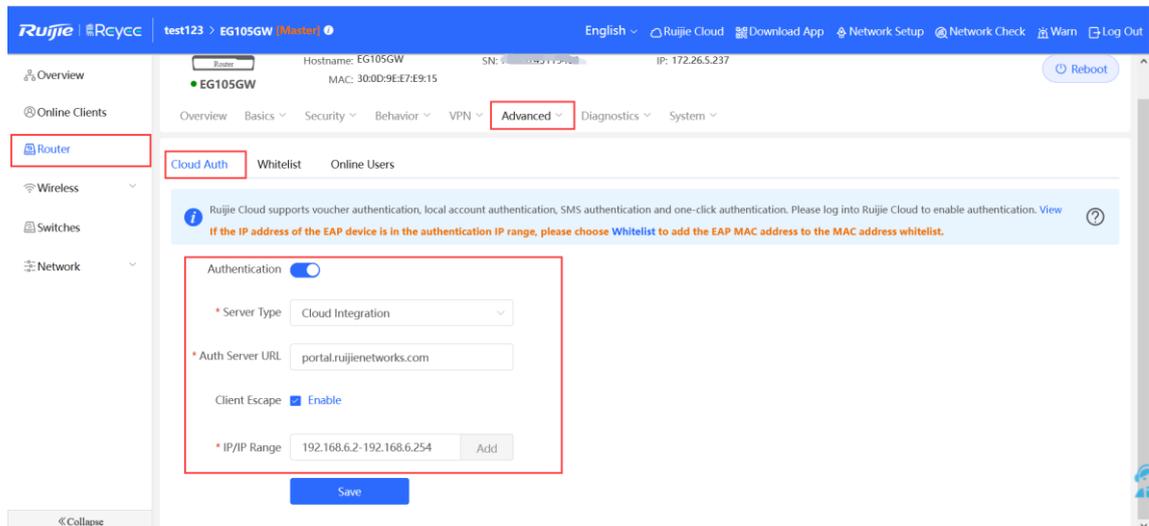


Note

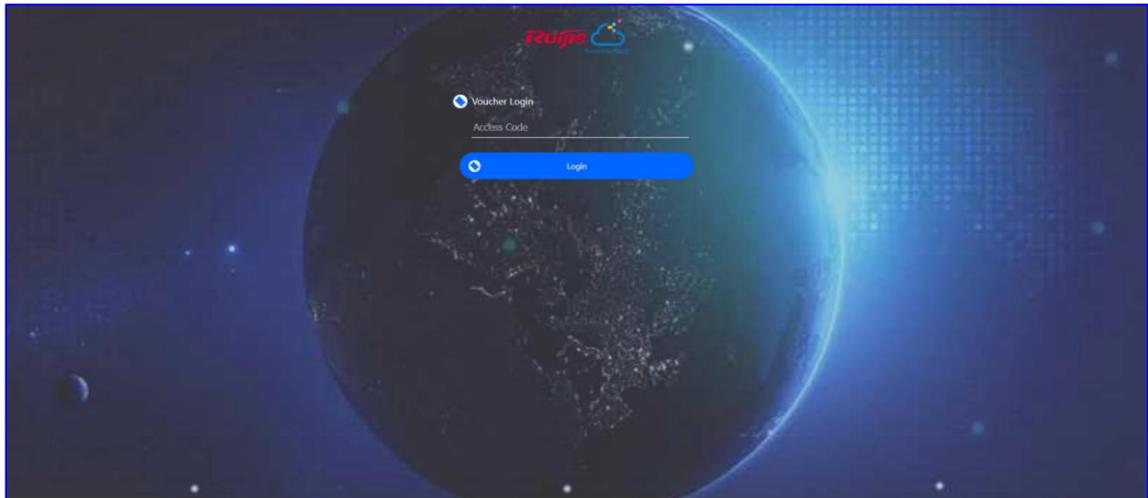
IP addresses of the EG, switch, and AP need to be excluded; otherwise, the switch cannot access the Internet.

5.2.4 Configuration Verification

- (1) Choose **Advanced > LAN > Authentication > Cloud Auth** to check whether the configuration has been synchronized to the EG.



- (2) Users whose IP addresses are in the range of 192.168.6.2 to 192.168.6.254 need to be authenticated before accessing the Internet.



5.3 Reye Guest Wi-Fi Solution

5.3.1 Working Principle

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

5.3.2 Application Scenario

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

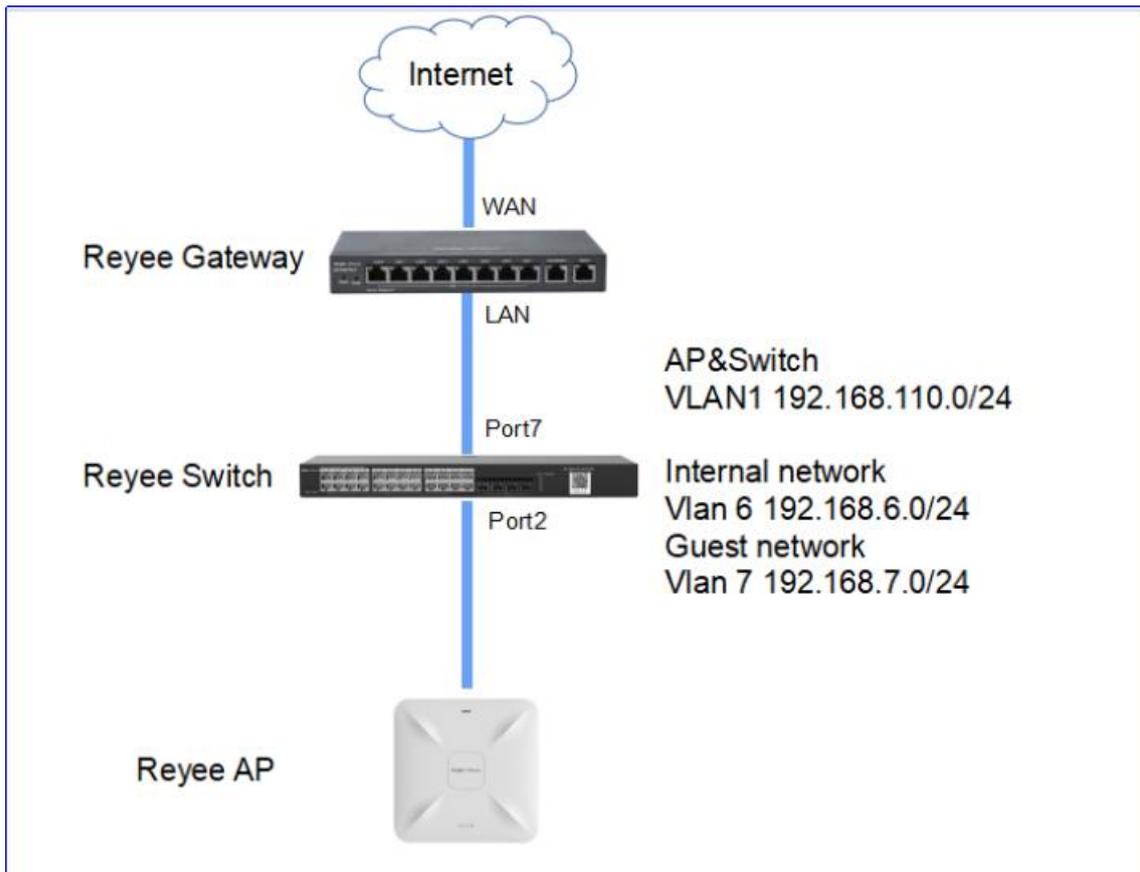
5.3.3 Configuration Example

1. Configuration Through EG's Eweb

Requirement

Guest Wi-Fi is configured for guests on the network segment of VLAN 7 and the guests are not allowed to access the internal network on the network segment of VLAN 6.

Network Topology



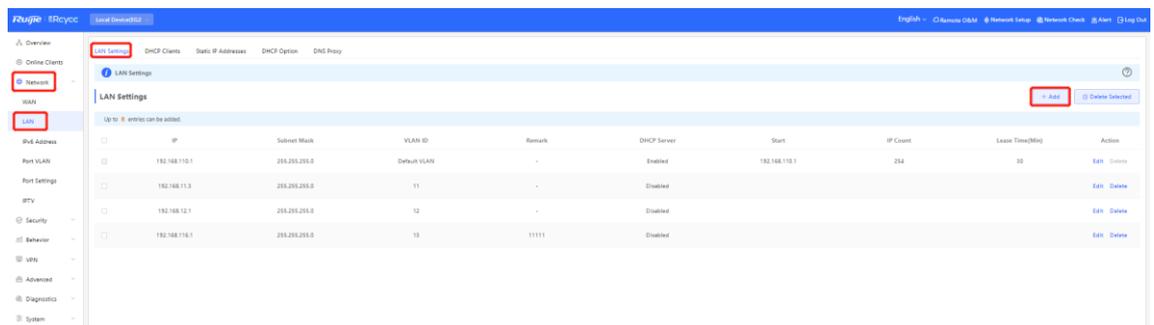
Network Description

- The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.
- The Reyee AP and switch obtain the IP address on the network segment of VLAN 1 for Internet access.
- Internal users obtain IP addresses in the network segment of VLAN 6 for Internet access and guests obtain IP addresses on the network segment of VLAN 7 for Internet access

Configuration Steps

(1) Configure VLAN 6 and VLAN 7 on the router.

a Switch to the **Local** mode. Choose **Network > LAN > LAN Settings > Add**.



b Perform LAN settings and configure DHCP address pools of VLAN 6 and VLAN 7 on the router.

Add ×

* IP

* Subnet Mask

* VLAN ID

Remark

MAC

DHCP Server

* Start

* IP Count

* Lease Time(Min)

DNS Server 192.168.6.1 ⓘ

Add ×

* IP

* Subnet Mask

* VLAN ID

Remark

* MAC

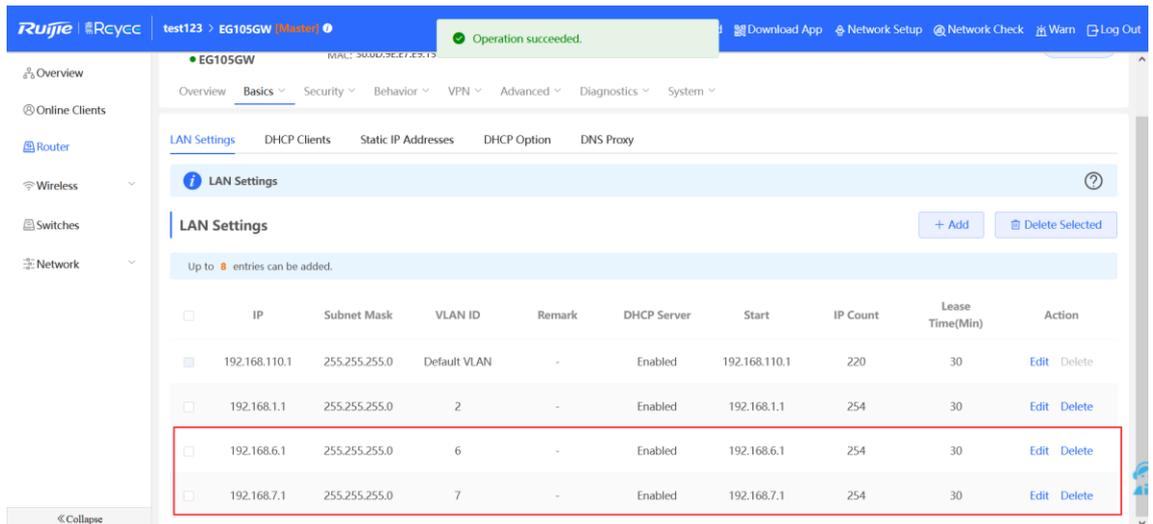
DHCP Server

* Start

* IP Count

* Lease Time(Min)

DNS Server 192.168.7.1 ⓘ



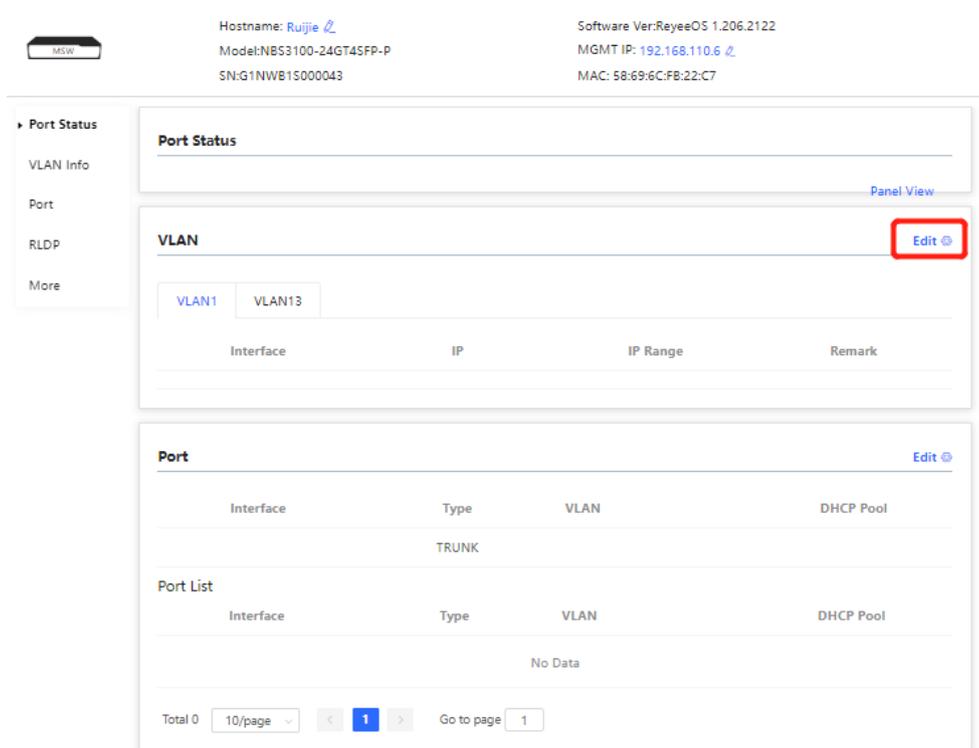
(2) Configure VLANs for a switch.

a Switch to the **Network** mode. Choose **Device > Switch**.



b Select a device from **Device List** and access the configuration page.

c In the **VLAN** pane, select a VLAN and click **Edit** to configure the VLAN.



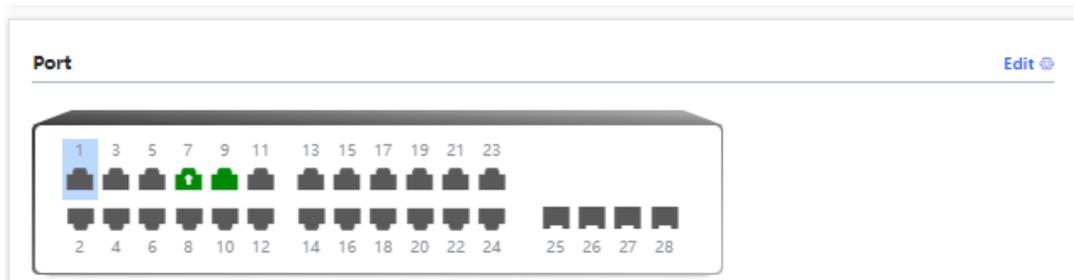
d Click **Add VLAN** to create VLAN 6 on the switch.

VLAN Info

Vlan ID	Remark	
1	VLAN0001	
13	11111	
6		

[+Add VLAN](#) [+Batch Add](#) [-Delete Selected](#)

- e In the **Port** pane, click **Edit**, configure port2 and port9 connected to the AP and EG as trunk ports and configure them to allow packets from VLAN 1 and VLAN 6 to pass through, and check port settings on the device.



Port

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

Selected Port ["Gi2"]

Routed Port Not Supported

Port Type

* Access VLAN:

- Switch to the **Network** mode. Choose **Network > Wi-Fi > Guest Wi-Fi**, and configure a guest Wi-Fi SSID named **Guest_Wi-Fi_Reyee** and associate VLAN 7 with this SSID.

Wi-Fi Settings **Guest Wi-Fi** Wi-Fi List Healthy Mode Load Balancing

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

Guest Wi-Fi Device Group:

Enable

* SSID

Band

Security

* Wi-Fi Password

----- Collapse -----

Effective Time

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 his IP address unchanged in this Wi-Fi network.)

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

- Choose **Network > Wi-Fi > Wi-Fi List > Add**, configure the internal user SSID named **Internal_network_Reyee**, associate VLAN 6 with this SSID, and check Wi-Fi settings in the Wi-Fi list.

Add ×

i The configuration will take effect after being delivered to AP.

* SSID

Band

Security

[Collapse](#)

Wireless Schedule

VLAN

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

Wi-Fi Settings Guest Wi-Fi **Wi-Fi List** Healthy Mode

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

Wi-Fi List Device Group: + Add

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
RAP2	2.4G + 5G	WPA_WPA2-PSK	No	10	Edit Delete
Internal_network_Reyee	2.4G + 5G	WPA_WPA2-PSK	No	6	Edit Delete
Guest_WiFi_Reyee	2.4G + 5G	WPA_WPA2-PSK	No	7	Edit Delete

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

The screenshot shows the Ruijie iEye configuration interface. In the left sidebar, the 'Access Control' menu item is highlighted. The main content area displays the 'ACL List' configuration page. At the top, there is a blue information banner with a tip: 'Tip: Changing configuration requires a reboot and clients will be reconnected.' Below this, the 'ACL List' section shows a table with the header 'Up to 30 entries can be added.' The table is currently empty, displaying 'No Data'. A red box highlights the '+ Add' button in the top right corner of the ACL List section.

Add Rule ✕

Based on MAC IP

Src IP Address: Port :

Dest IP Address: Port :

Protocol Type

Control Type

Effective Time

Interface

Remark

ACL List + Add

Up to 50 entries can be added.

<input type="checkbox"/>	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
<input type="checkbox"/>	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.10.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	VLAN 10_Intranet_isolation	↓	Edit Delete
<input type="checkbox"/>	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.6.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	Block Guest	↓ ↑	Edit Delete
<input type="checkbox"/>	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.111.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	_Intranet_isolation	↑	Edit Delete

Configuration Verification

A guest at 192.1687.2 cannot access the internal network user at 192.168.6.2.

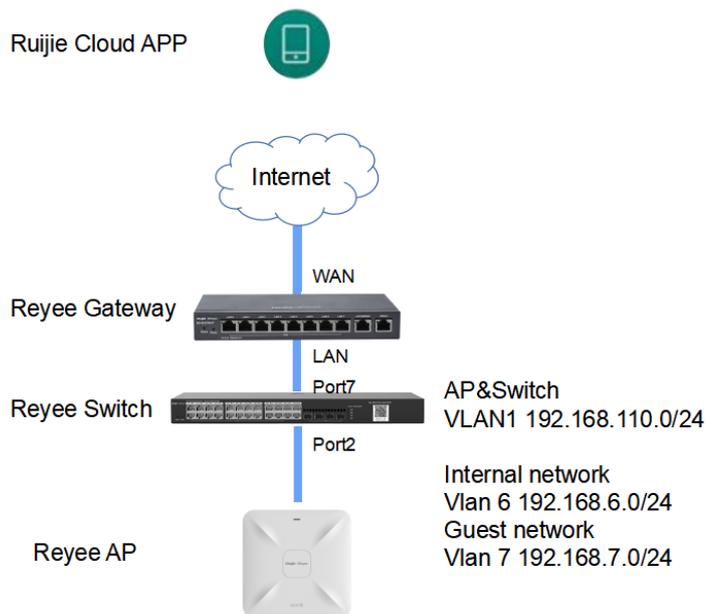


2. Configuration Through Ruijie Cloud APP

Requirement

Guest Wi-Fi through Ruijie Cloud App is configured for guests on the network segment of VLAN 7, who cannot access the internal network on the network segment of VLAN 6. Ruijie Cloud App will deliver the corresponding configuration to the device automatically.

Network Topology

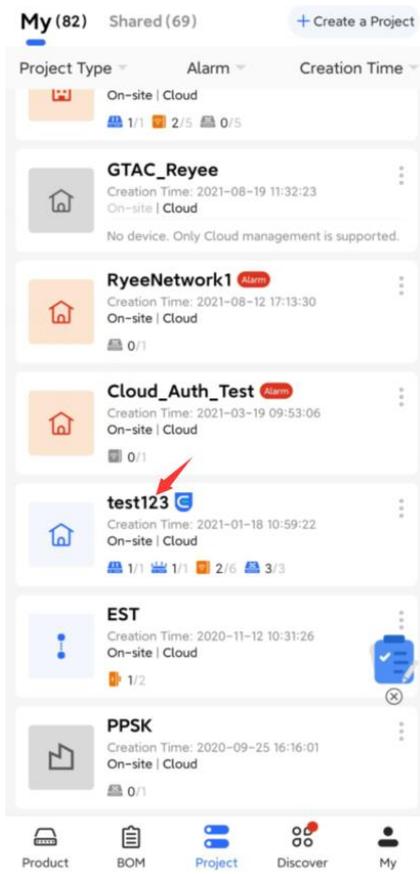


Network Description

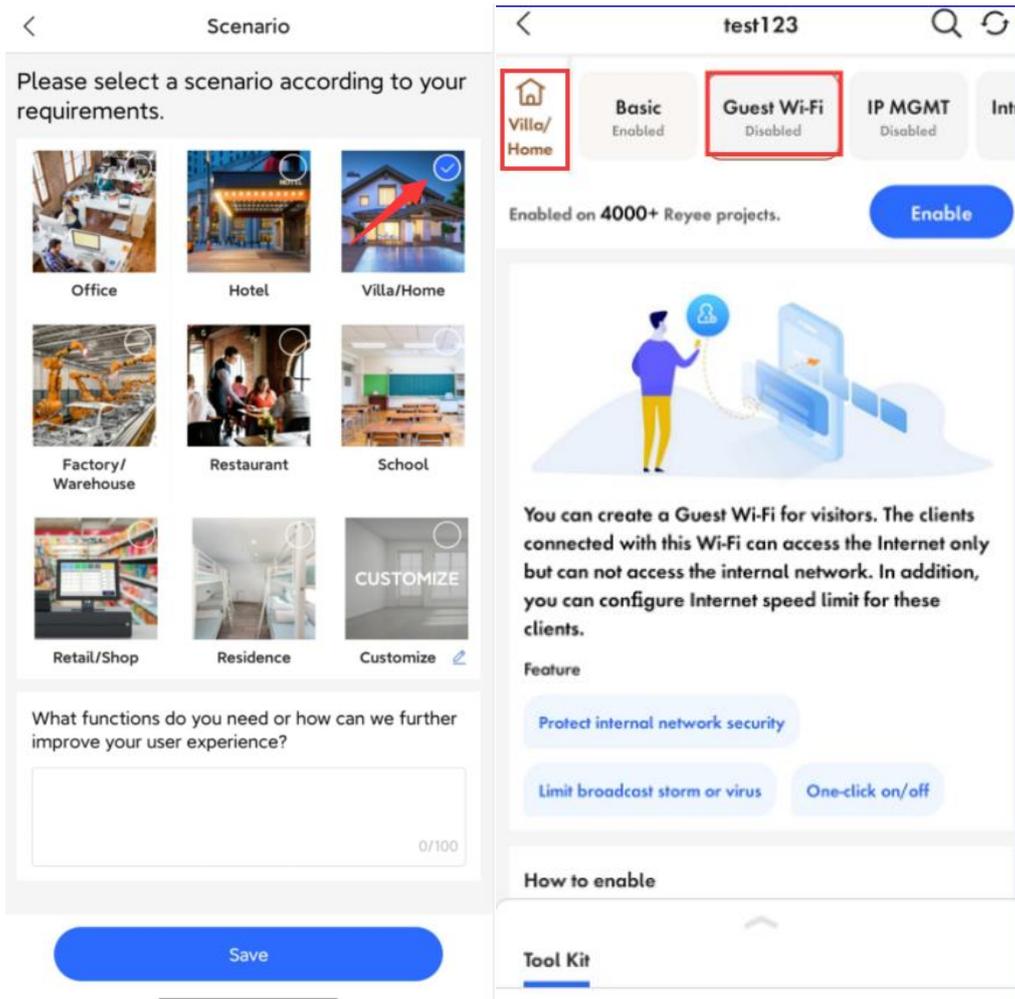
- The EG works as a DHCP server to assign IP addresses to users, Reeye AP, and Reeye switch.
- The Reeye AP and switch obtain IP addresses on the network segment of VLAN 1 for Internet access.
- Internal users obtain IP addresses on the network segment of VLAN 6 for Internet access and guests obtain IP addresses on the network segment of VLAN 7 for Internet access.

Configuration Steps

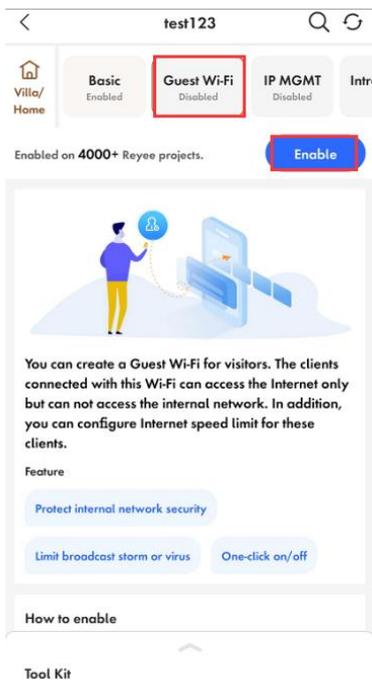
- (1) Log in to your Ruijie Cloud App on the smartphone and access the project with Reeye router and RAP.



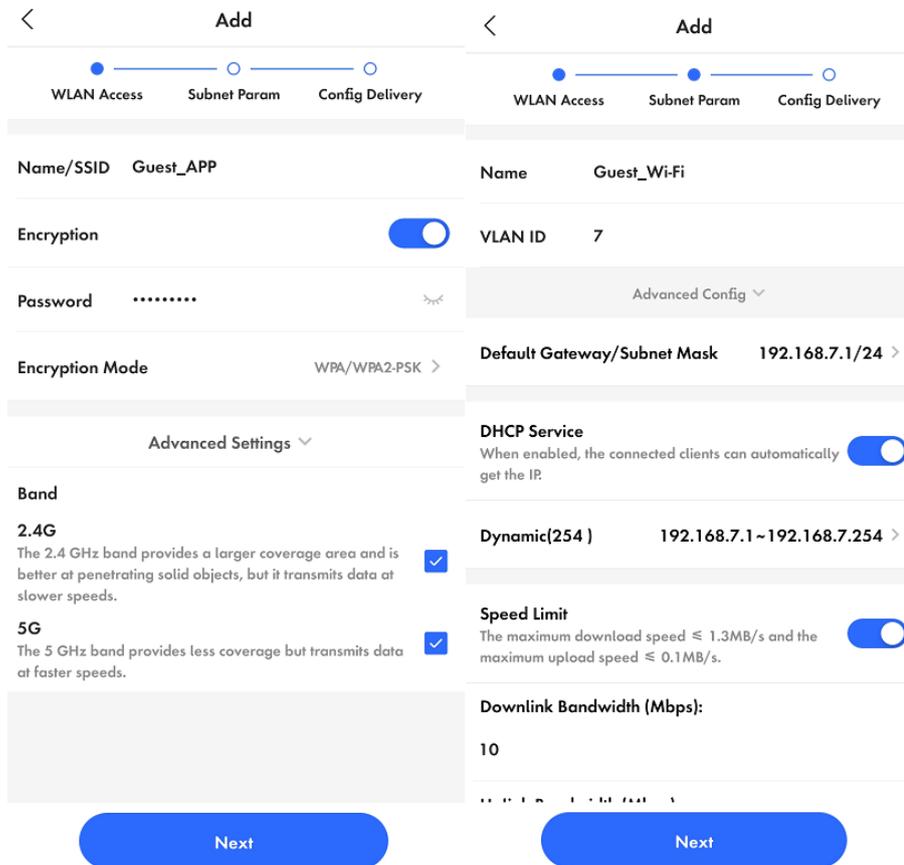
(2) Select **Villa/Home** under **Scenario**. You can see the **Guest Wi-Fi** button.



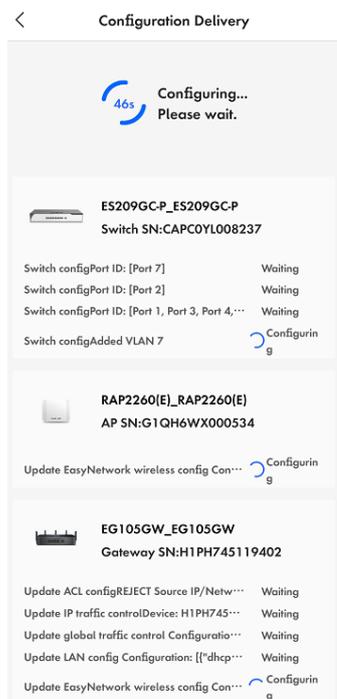
(3) Select **Guest Wi-Fi** and click **Enable** button.

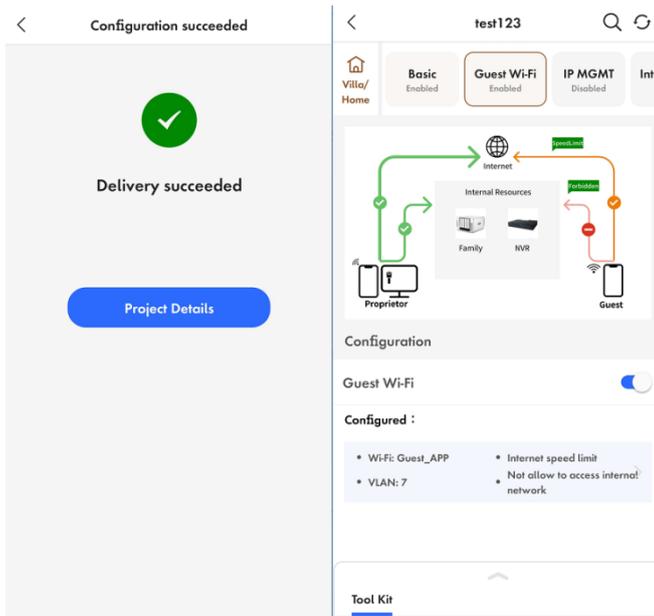


- Modify guest Wi-Fi information, configure an Internal user SSID named **Guest_APP** and associate VLAN 6 with this SSID, and configure a guest Wi-Fi SSID named **Guest_Wi-Fi** and associate VLAN 7 with this SSID. Then Click **Save** to save your configuration.



- Wait around 1 minute for the system to deliver the configuration to the device.





Configuration Verification

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

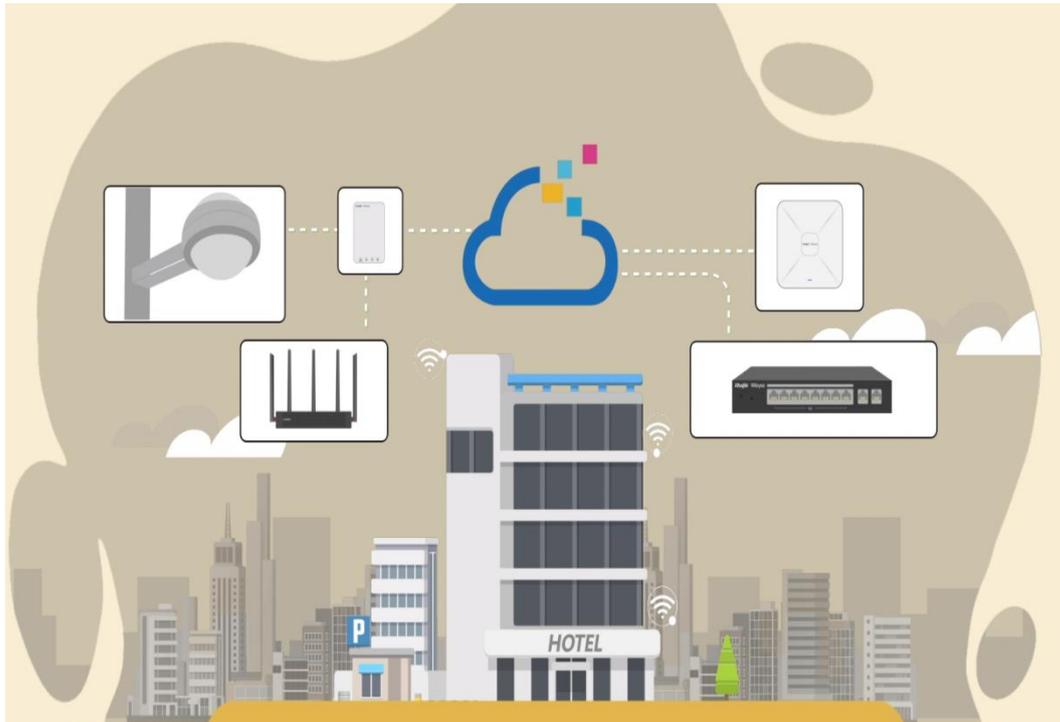


5.4 Reeye Economic Hotel Network Solution

5.4.1 Application Scenario

Reeye economic hotel network solution provides an affordable 5-star Wi-Fi for clients. It can operate concurrently at 2.4 GHz and 5 GHz, providing high-speed wireless access of 574 Mbit/s at 2.4GHz, 1201 Mbit/s at 5 GHz,

and up to 1775 Mbit/s per AP. The wall AP provides a LAN port at the front to facilitate the expansion of IPTV terminals, IP phones, and other terminals.

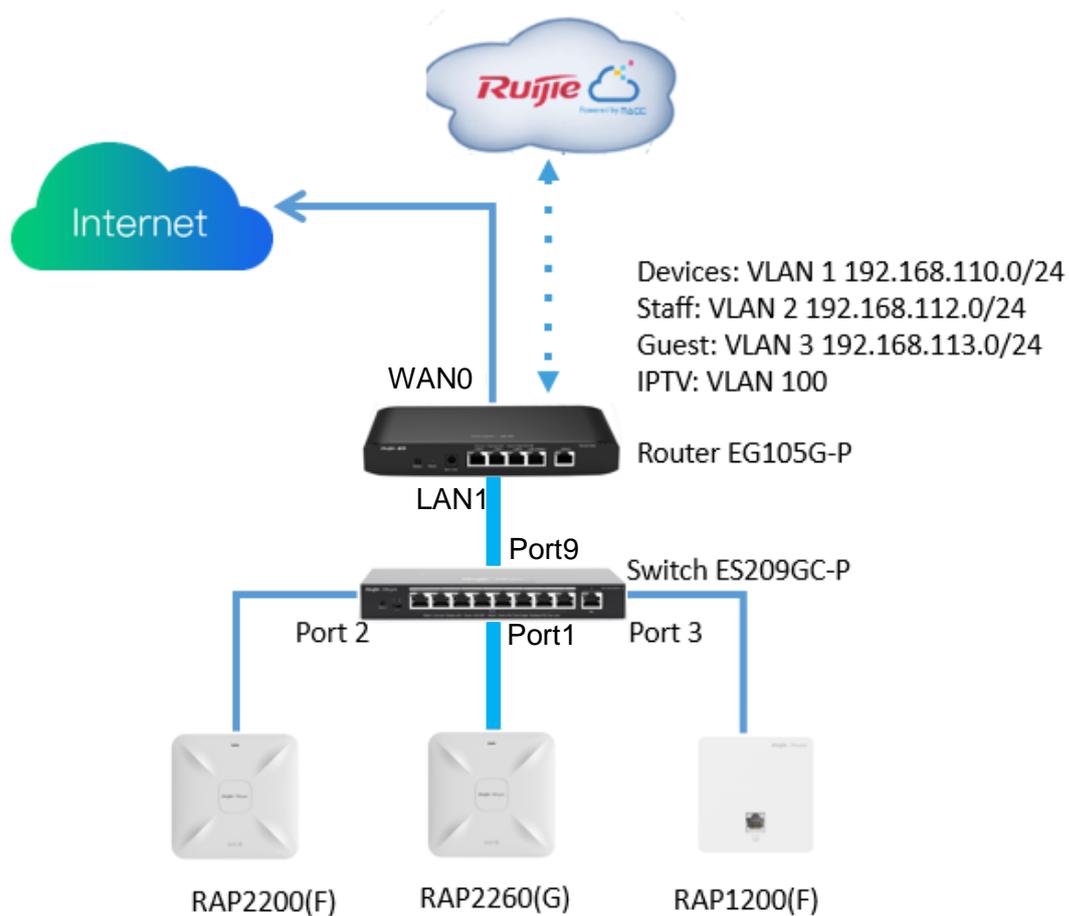


5.4.2 Configuration Example

Requirement

- A wireless network needs to be built for the hotel, and guests need to pass voucher authentication before accessing the Internet and are not allowed to access the internal network of the hotel.
- Wired connections are configured for IPTV.

Network Topology



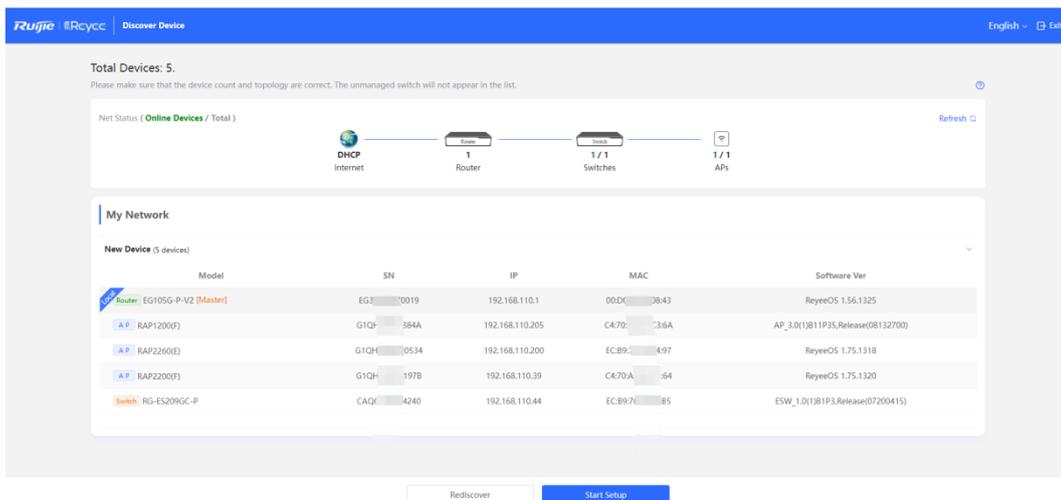
Devices List

Type	Model	Function
Router	EG105G-P	<ul style="list-style-type: none"> Connects to the Internet and works as the DHCP server for downlink devices and clients. Manages the AP and switch locally. Supports voucher authentication with Ruijie Cloud.
Switch	ES209GC-P	Provides wired and PoE connections.
Wall AP	RAP1200(F)	Provides wireless connections for rooms. Provides a wired connection for IPTV.
Indoor AP	RAP2200(F)&RAP2260(G)	Provides wireless connections for the hall and corridor.

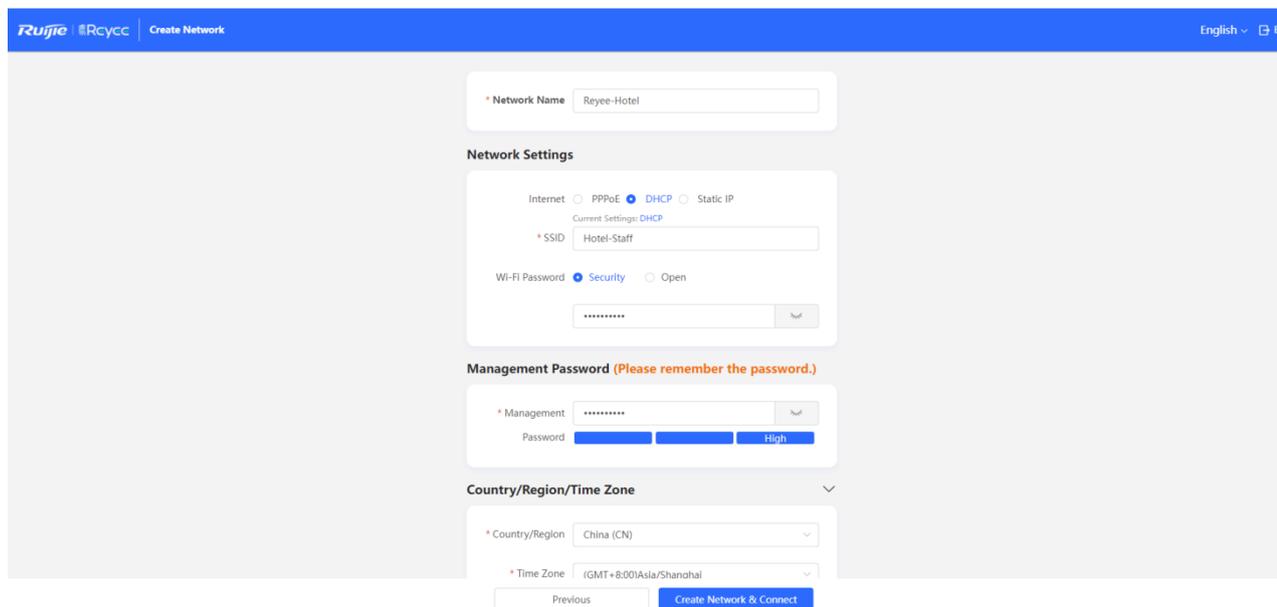
Configuration Steps

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

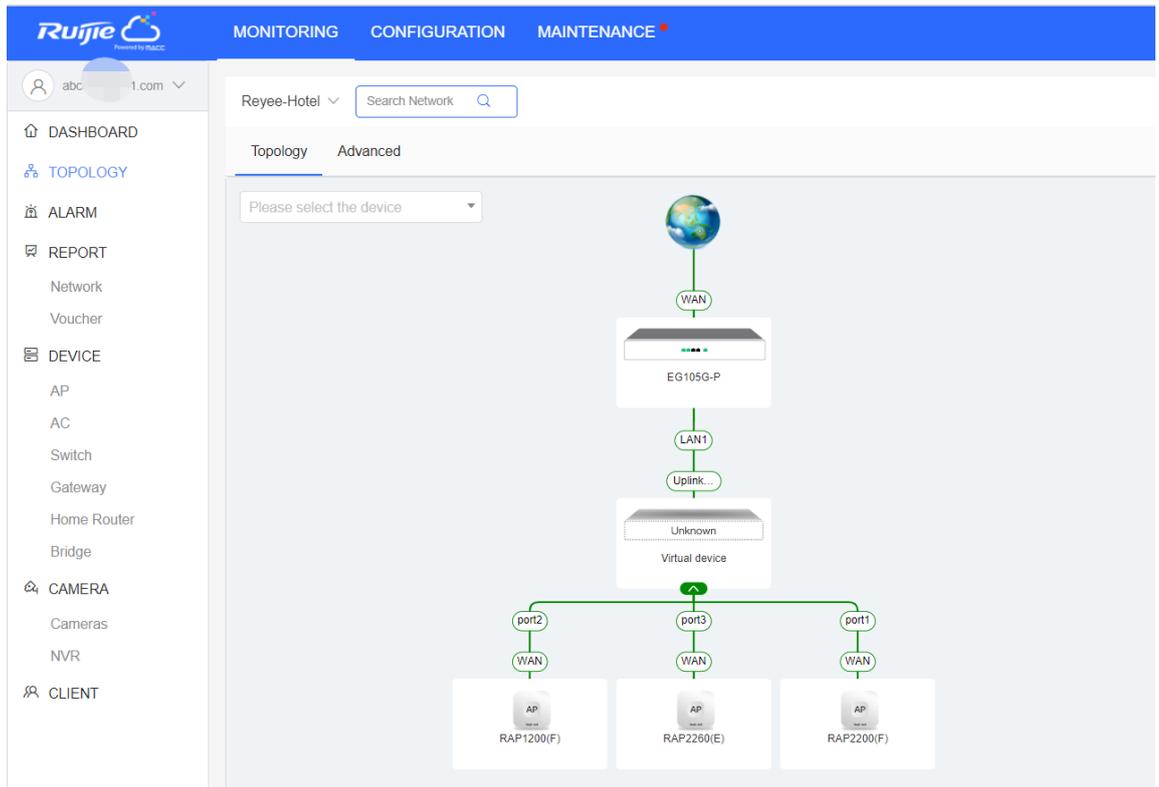
- (2) By default, the IP address of the router is 192.168.110.1. Click **Start Setup** to perform basic network setting.



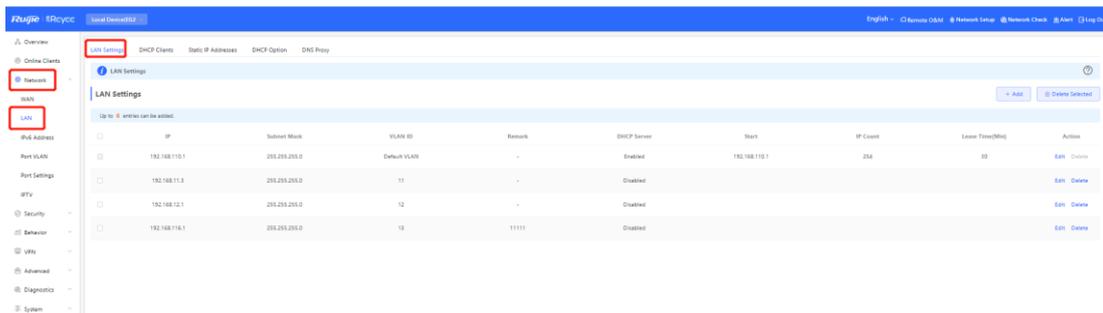
- a Set **Network Name**, **Network Settings**, **SSID** for staffs, and **Management Password**.



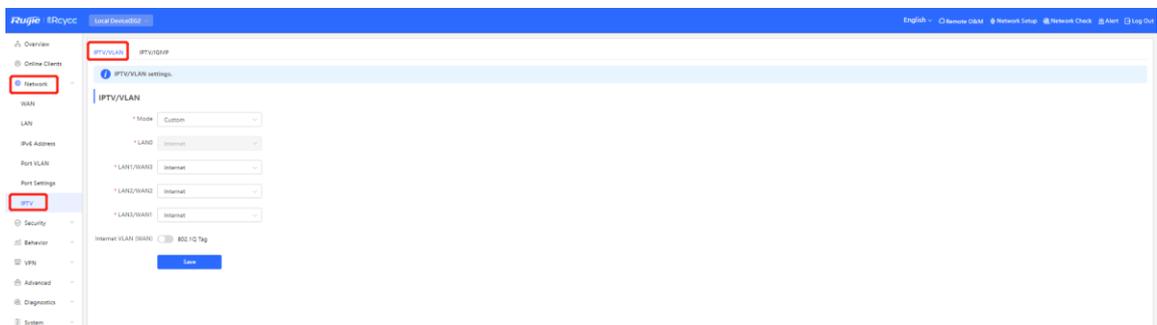
- b Click **Create Network & Connect** to active the configuration and add the devices to Ruijie Cloud.



- (3) Switch to the **Local** mode. Choose **Network > LAN > LAN Settings** to create VLAN 2 and VLAN 3 for staffs and guests.



- (4) Switch to the **Local** mode. Choose **Network > IPTV** to perform IPTV settings obtained from the ISP. For example, the VLAN ID for IPTV is 100.



IPTV/VLAN IPTV/IGMP

i IPTV/VLAN settings.

IPTV/VLAN

* Mode

* LAN0

* LAN1/WAN3

* LAN2/WAN2

* LAN3/WAN1

* IPTV VLAN ID

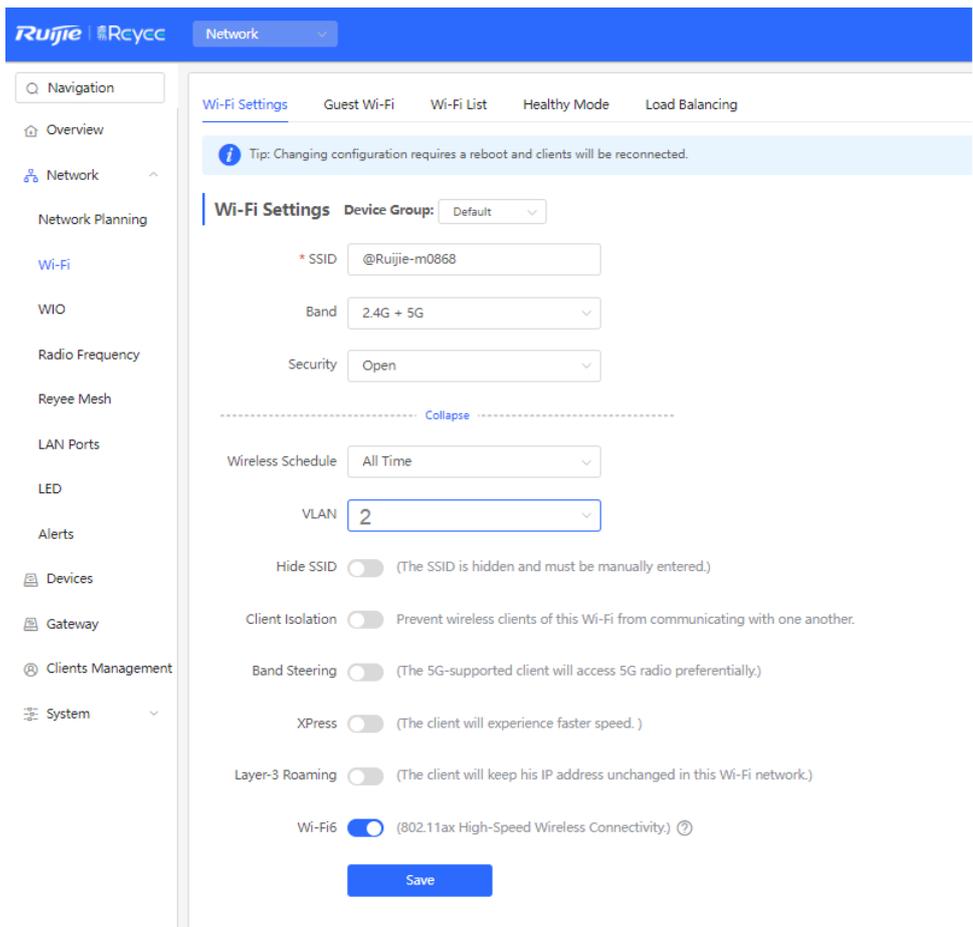
Internet VLAN (WAN) 802.1Q Tag

Save

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

The screenshot shows the Ruijie Rcycc Network Management System interface. The 'LAN Port Settings' page is active, displaying 'Default Settings' with 'VLAN ID' set to 100. An 'Add' dialog box is open, allowing the user to add a new LAN port configuration. The dialog shows 'VLAN ID' as 100 and 'Applied to' as 'Enter an AP name or SN.'. The 'LAN Ports' section in the sidebar is highlighted with a red box, and the '+ Add' button is also highlighted with a red box.

- (6) Choose **Network > Wi-Fi > Wi-Fi Settings**, configure Wi-Fi for staffs and guests, and select VLAN 2 for staffs.



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

Switch to the **Network** mode. Choose **Network > Wi-Fi > Guest Wi-Fi**.

The screenshot shows the Ruijie Rcycc Network configuration interface. The left sidebar contains a navigation menu with the following items: Navigation, Overview, Network, Network Planning, Wi-Fi, RLDP, DHCP Snooping, WIO, Radio Frequency, Reeye Mesh, LAN Ports, LED, Alerts, Batch Config, Devices, Gateway, Firewall, Clients Management, and System. The main content area is titled 'Guest Wi-Fi' and includes a 'Device Group' dropdown set to 'Default'. A tip message states: 'Tip: Changing configuration requires a reboot and clients will be reconnected.' The configuration options are as follows:

- Enable:** (Toggled on)
- * SSID:** @Ruijie-guest-BCFA
- Band:** 2.4G + 5G
- Security:** Open
- Effective Time:** Never Disable
- VLAN:** 13 (11111)
- 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 his IP address unchanged in this Wi-Fi network.)
- Wi-Fi6:** (802.11ax High-Speed Wireless Connectivity.)

A blue 'Save' button is located at the bottom of the configuration area.

- (8) Switch to the **Local** mode. Choose **Behavior > Access Control** and configure an ACL to prevent guests from accessing the internal network.

Add two ACL rules to prevent hosts in VLAN 3 from accessing hosts in VLAN 1 and VLAN 2, and apply them to the LAN port.

Add Rule

Based on MAC IP

Src IP Address: Port :

Dest IP Address: Port :

Protocol Type

Control Type

Effective Time

Interface

Remark

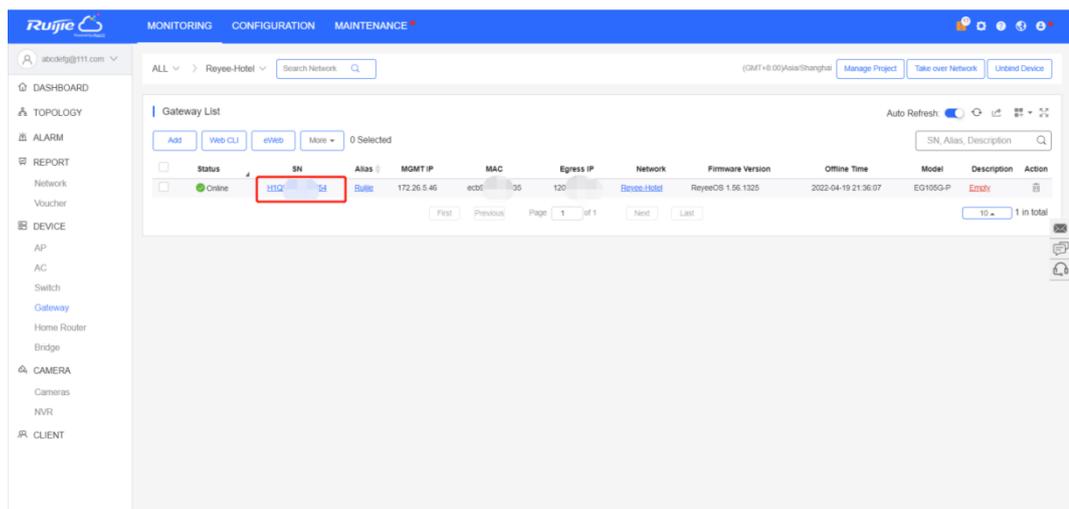
ACL List

Up to 50 entries can be added.

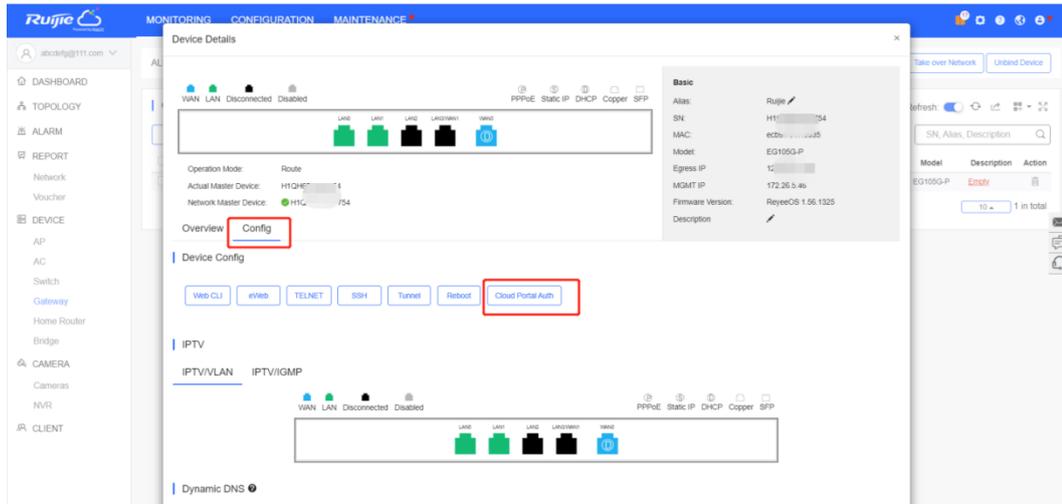
Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
<input type="checkbox"/> Src IP Address 192.168.113.0/24 : All Ports Dest IP Address 192.168.112.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active		↓	Edit Delete
<input type="checkbox"/> Src IP Address 192.168.113.0/24 : All Ports Dest IP Address 192.168.110.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active		↑	Edit Delete

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

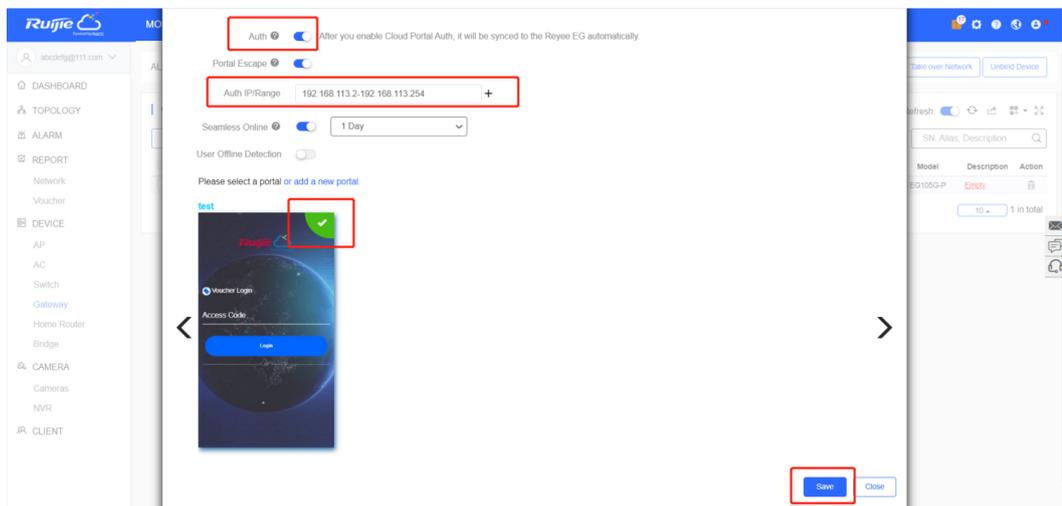
a Click the SN of the EG to access the page of device details.



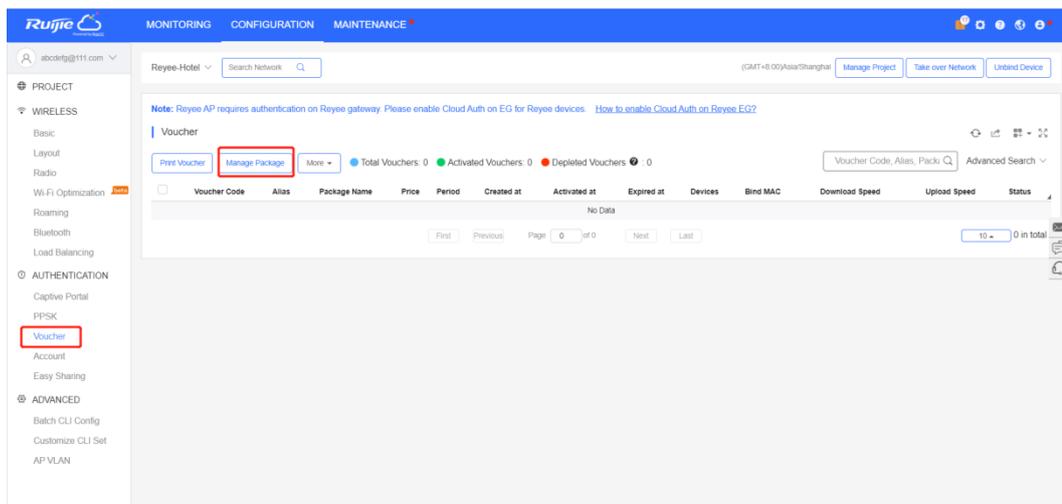
b Choose Config > Cloud Portal Auth.



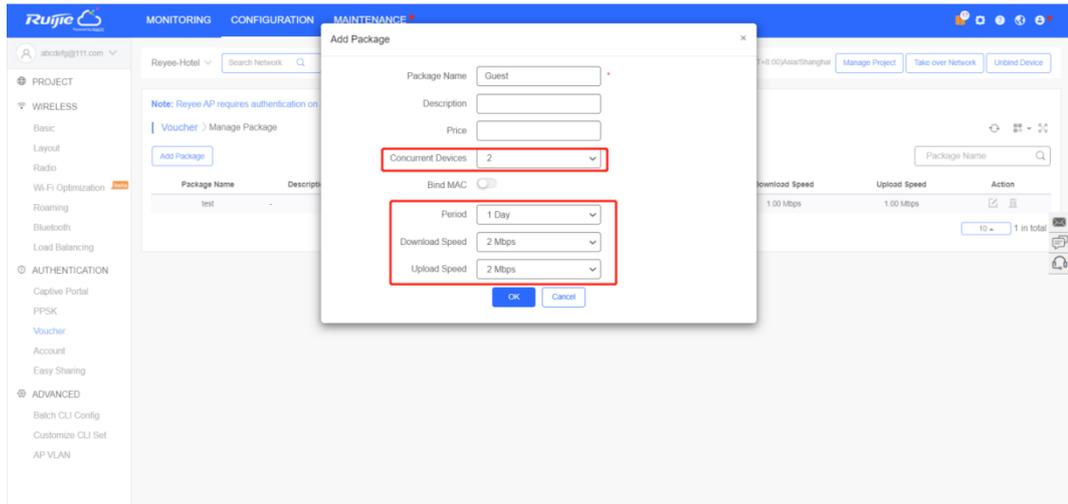
- c Enable authentication and configure IP addresses of guests in the range from 192.168.113.2 to 192.168.113.254.



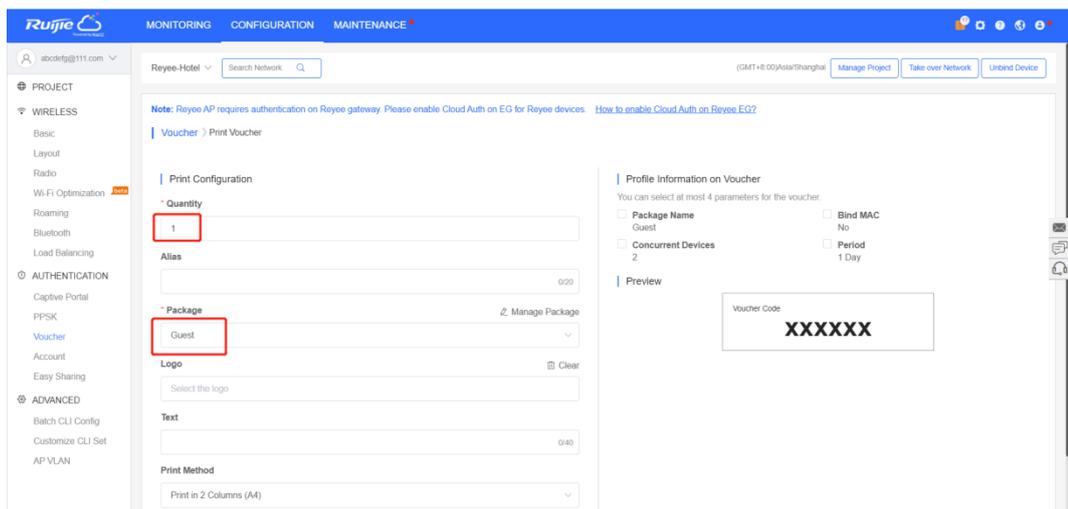
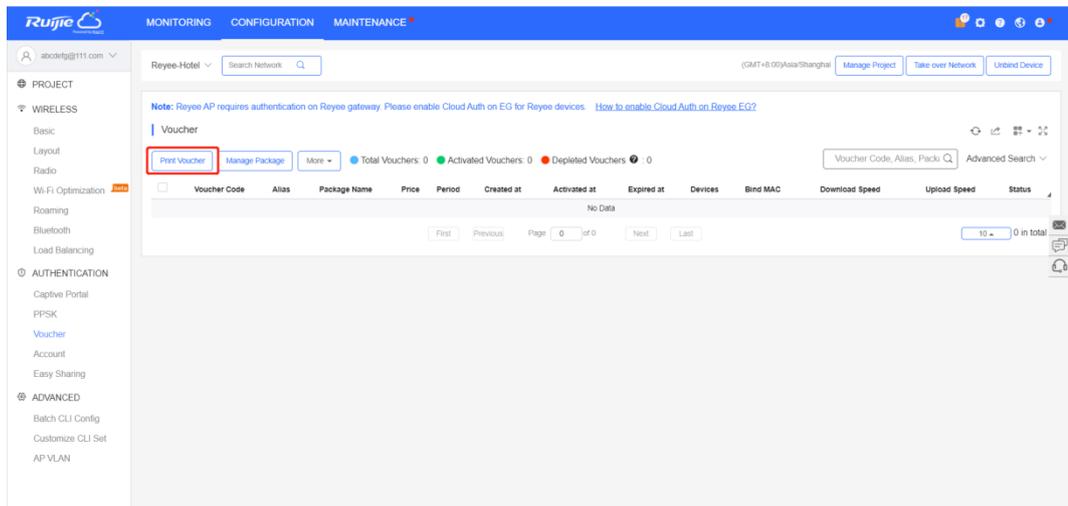
- d Add the voucher package for guests.
Choose **Voucher > Manage Package > Add Package** and add a voucher package for guests.

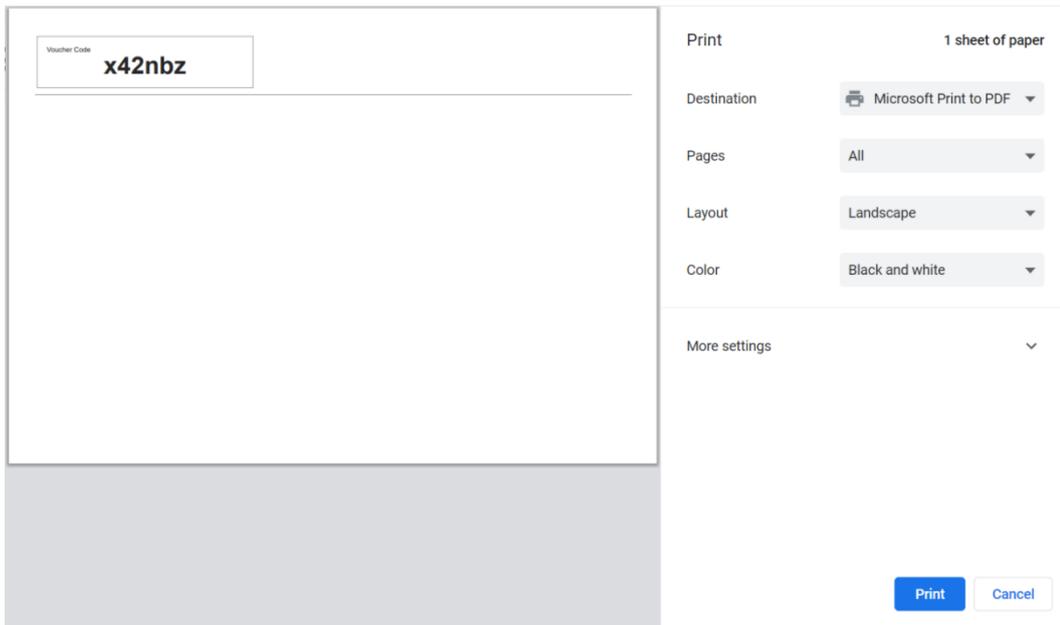


Example: Set Concurrent Devices to 2, Period to 1 Day, and Upload Speed and Download Speed to 2 Mbit/s.



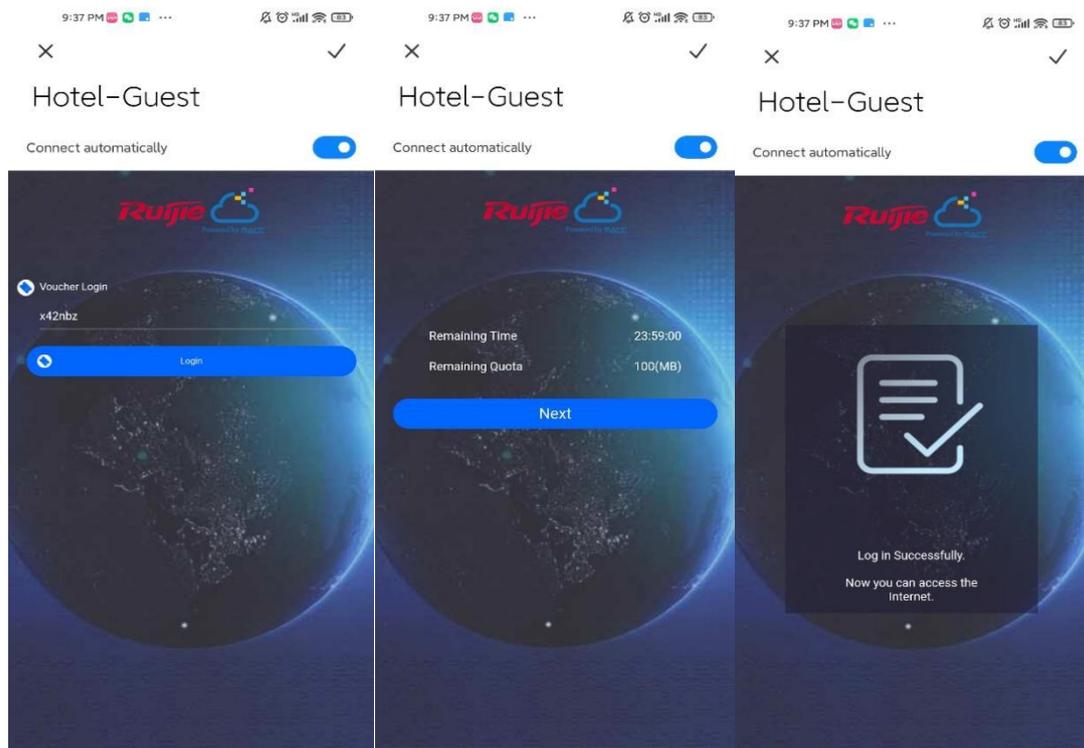
e Click **Print Voucher** to obtain the code for guests.





5.4.3 Configuration Verification

Connect guest Wi-Fi. You can see that the internal IP address 192.168.110.1 cannot be accessed.

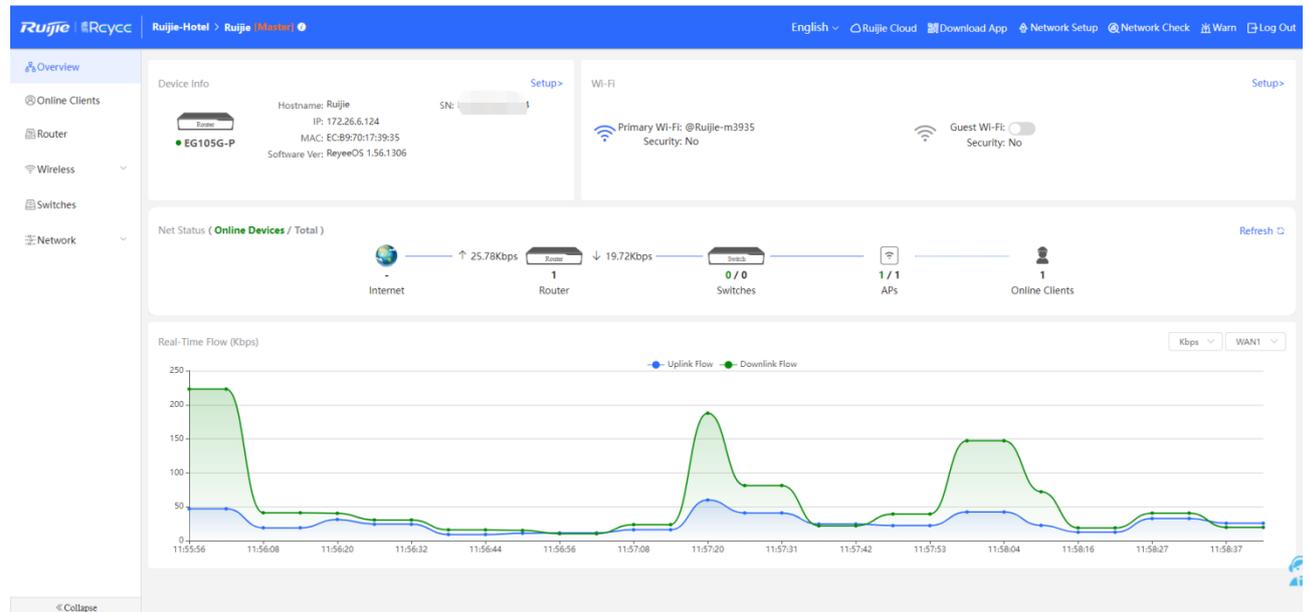


6 FAQ

- 6.1 [Reyee Password FAQ \(Collection\)](#)
- 6.2 [Ruijie Cloud Reyee EG authentication FAQ \(Collection\)](#)
- 6.3 [Reyee Mesh FAQ \(Collection\)](#)
- 6.4 [Reyee IPTV FAQ \(Collection\)](#)
- 6.5 [Reyee Authentication FAQ \(Collection\)](#)
- 6.6 [Reyee Behavior Strategy FAQ \(Collection\)](#)
- 6.7 [Reyee DDNS FAQ \(Collection\)](#)
- 6.8 [Reyee VPN FAQ \(\(collection\)\)](#)
- 6.9 [Reyee Flow Control FAQ \(Collection\)](#)
- 6.10 [Reyee Guest Wi-Fi FAQ \(Collection\)](#)
- 6.11 [Reyee Wireless Configuration FAQ \(Collection\)](#)
- 6.12 [Reyee Self-Organizing Network \(SON\) FAQ \(Collection\)](#)
- 6.13 [Reyee series Devices Parameters Tables](#)
- 6.14 [Reyee Parameter Consultation FAQ \(Collection\)](#)

7 Appendix: Surveillance

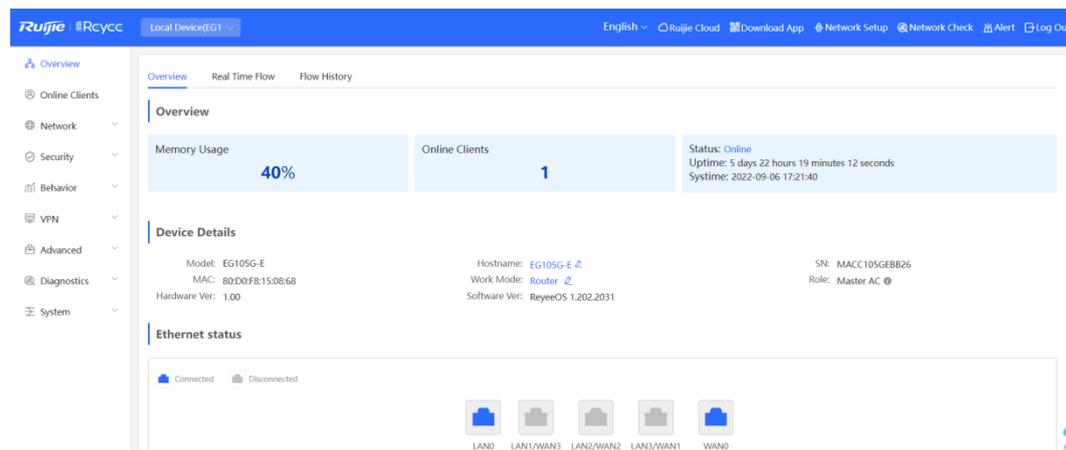
The overview page displays **Device Info**, **Wi-Fi**, **Network Status**, and **Real-Time Flow**.



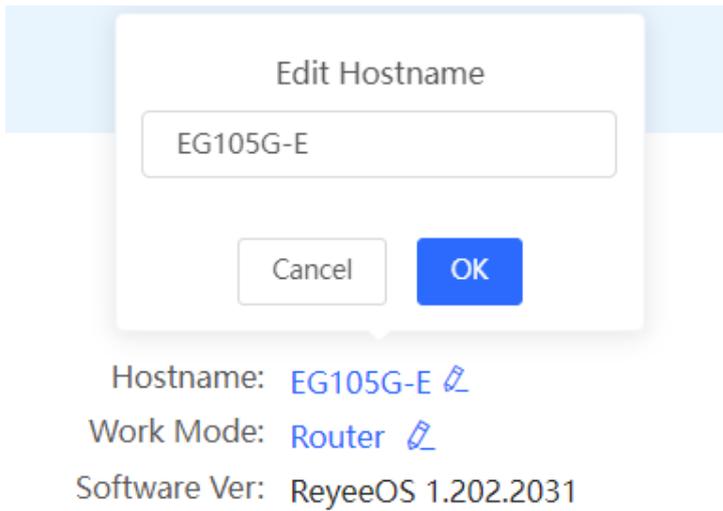
7.1 Device Info

Choose **Overview > Overview**. On the **Device Info** page, the model, host name, IP address, MAC address, software version, and SN of the router are displayed.

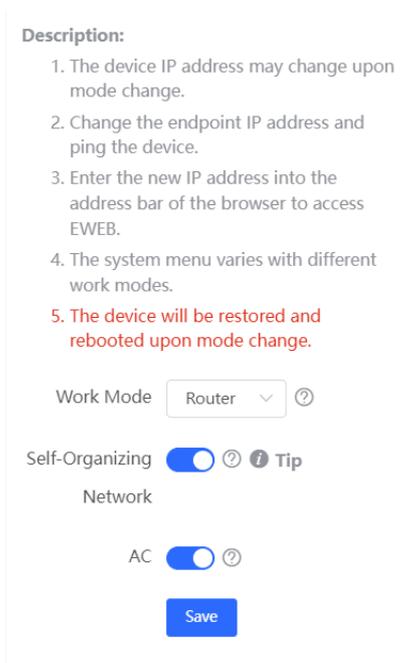
In the **Overview** pane, the memory usage, online client count, status, uptime, and system time are displayed.



- The **Online** status indicates the SON status of the Reye devices but not Ruijie Cloud.
- You can click **Hostname** to modify the device name.



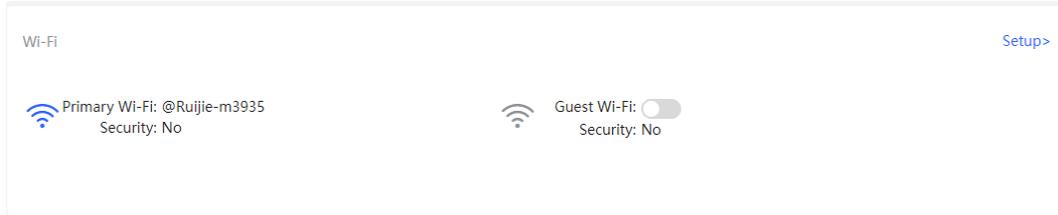
- Click **Work Mode** to switch the device mode. Two modes are available: **Router** and **AC** modes. The default mode is **Router**.



- **Router Mode:** indicates NAT forwarding.
- **AC Mode:** indicates bridge forwarding.
- SON:
 - -If SON is enabled, the device role is displayed.
 - -If SON is disabled, the device works in standalone mode.
 - - SON is enabled by default in AC mode.
- AC:
 - -It is enabled by default. The device works as a virtual AC to manage downlink devices.
 - -When it is disabled, the device must be elected as the AC before managing downlink devices.

7.2 Wi-Fi Information

You can name the Wi-Fi of the network and enable guest Wi-Fi.



Setup: Go to the Wi-Fi setting page.

7.3 Network Status

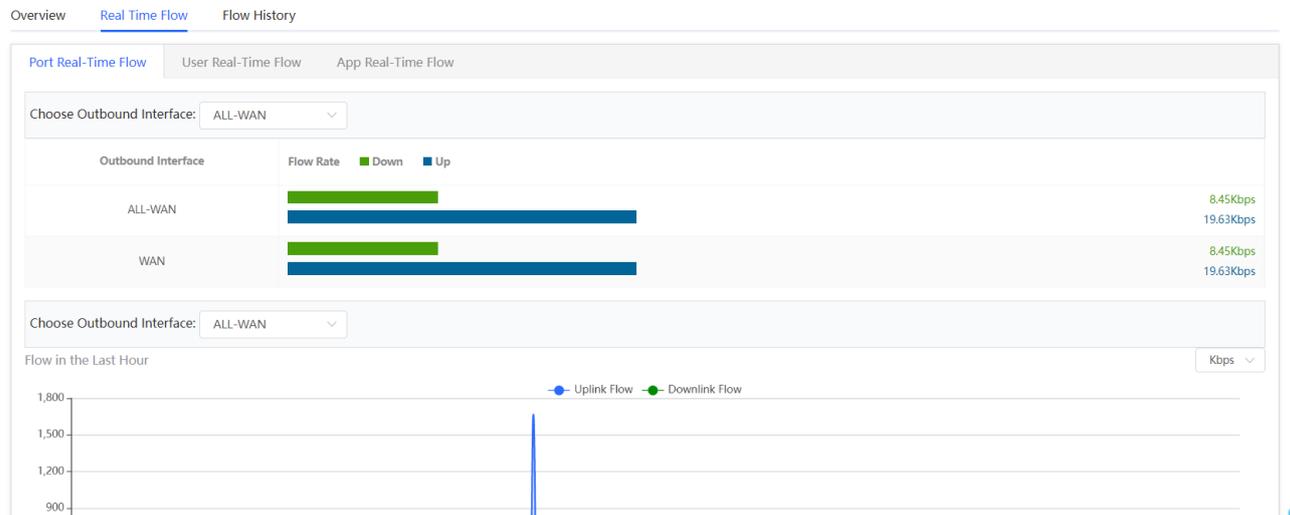
The **Network Status** page displays the topology and connected status of the network.



7.4 Real-Time Flow

Choose **Gateway > Overview > Real Time Flow**. The **Real-Time Flow** page appears.

Check real-time traffic flows based on ports, users, and apps, including uplink and downlink flows. The default unit is kbit/s. You can change it to be bit/s and Mbit/s.



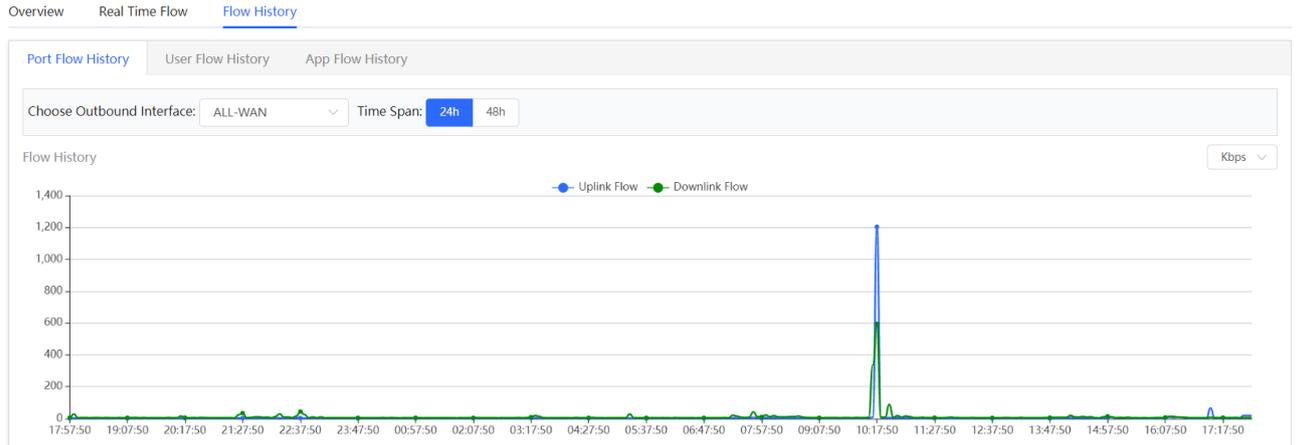
7.5 Flow History

Note

This feature is supported by R202 and later versions.

Choose **Overview > Flow History**. The **Flow History** page appears.

Check historical traffic flow based on ports, users, and apps, including uplink and downlink flows.



7.6 URL Logs

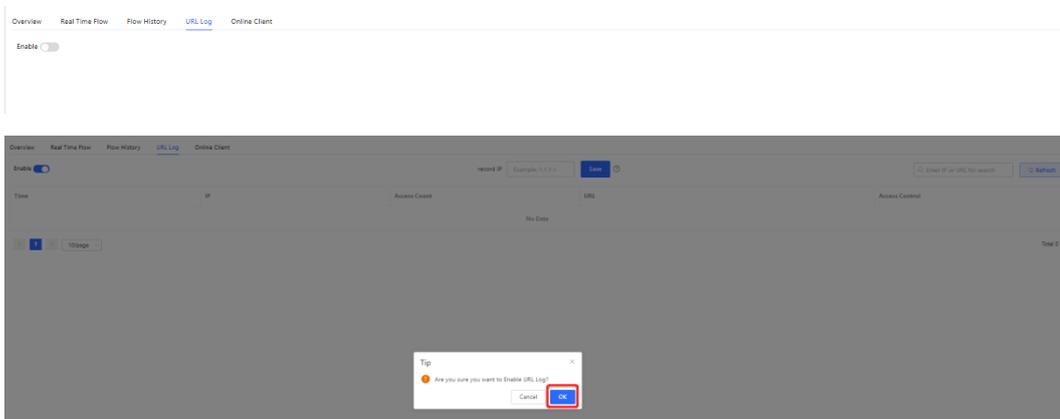
URL logs are URL access records of devices on the internal network, including the URL, access count, and audit result.

Note

This feature is supported by only EG3 series routers such as EG310G-E.

- (1) Choose **Overview > URL Log**.
- (2) Enable URL logging.

Toggle the switch to **Enable** and click **OK** in the dialog box.



- (3) (Optional) Configure an IP address to view its URL access records.

The system logs URL access records of all devices on the internal network by default. To view URL access records of a specific device, configure an IP address in the **record IP** text box and click **Save**.

Time	IP	Access Count	URL	Access Control
2022-06-15 09:26	192.168.33.3	1	http://0000f00e-glink-9222	Allow
2022-06-15 09:26	192.168.33.4	15	http://www.gdsgo.cn	Allow
2022-06-15 09:26	192.168.33.3	1	http://www.baidu.com	Allow
2022-06-15 09:25	192.168.33.4	3	http://120.241.131.85	Allow
2022-06-15 09:25	192.168.33.4	1	http://112.65.8.27	Allow
2022-06-15 09:25	192.168.33.4	5	http://www.tudou.com	Allow
2022-06-15 09:25	192.168.33.4	16	http://www.gdsgo.cn	Allow
2022-06-15 09:25	192.168.33.4	1	http://www.qq.com	Allow
2022-06-15 09:25	192.168.33.4	1	http://182.254.118.119	Allow
2022-06-15 09:25	192.168.33.4	1	http://www.qq.com	Allow

Note

To restore URL access records of all devices on the internal network, clear the **record IP** text box and click **Save**.

- (4) Check URL log details.

A log includes the access time, IP address, and access count.

You can search logs by IP address or URL.



7.7 Online Clients

Choose **Gateway > Overview > Online Clients**. The **Online Clients** page appears.

Select a client from the client list and click **View Details**. You can find the client’s username, type (wired/wireless), IP address, MAC address, current rate, connected Wi-Fi name, and access control status.

✕

Edit Client

IP: 192.168.111.20	Access Name: Ruijie
MAC: EC:B9:70:13:73:16	Access Location: MACCMR1250X01/LAN0
Online Time: 2022-08-31 20:22:25	Manufacturer: Ruijie Networks Co.,LTD
Offline Time: -	Product: Ruijie Network Device
Wireless Access: No	

Client Name: <input type="text" value="EW3200GX-137316"/>	Client Type: <input type="text" value="Network Device"/>
Auto Grouping: <input type="text" value="No"/>	Client Group: <input type="text" value="Select"/>