Ruijie Reyee RG-EG Series Router

Implementation Cookbook

Document Version: V1.4
Date: 2023-11-03

Copyright

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 Reyee: https://www.ruijienetworks.com/products/reyee
- 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

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 Mbps 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 V2	5 (PoE supported)	100	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 300 Router mode: 32
RG-EG105G V2	5	100	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 300 Router mode: 32
RG-EG105GW	5	100 (recommended number of wireless terminals: 60)	500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	Router mode: 32

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG210G-E	10	200	1000 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-EG210G-P	10 (PoE supported)	200	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-EG105GW(T)	5	100	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	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

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG105GW-X	5	180	1200 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	Router mode: 64
RG-EG305GH-P-E	5	300	1500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-EG310GH-E	10	300	1500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-EG310GH-P-E	10	300	1500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150

1.2 LED Indicators

LED Indicator	Status	Description
SYS	Flashing	Fast flashing (at 8 Hz): The router is starting up. Slow flashing (at 0.5 Hz): The network is unreachable. One long flash followed by three short flashes (at 0.8 Hz): The router is faulty. Flashing twice consecutively (at 0.8 Hz): ● The router is restoring factory settings. ● The router is upgrading the software. Note: Do not power off the router in this case.
	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	● Mesh pairing is not implemented. ● Wireless relay is not set up.
	Flashing alternately	Mesh pairing is in progress.
	Three bars on	● The mesh signal strength is high. ● The wireless relay signal strength is high.
	Two bars on	● The mesh signal strength is medium. ● The wireless relay signal strength is medium.
	One bar on	● The mesh signal strength is low. ● The wireless relay signal strength is low.

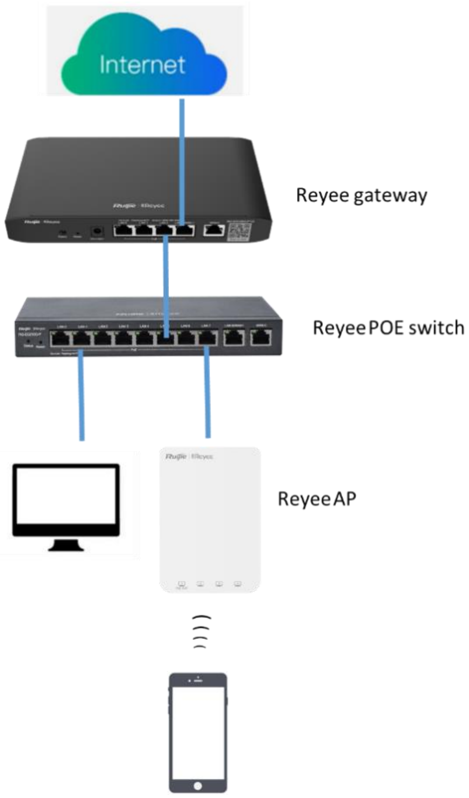
1.3 Button

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

2 Getting Started

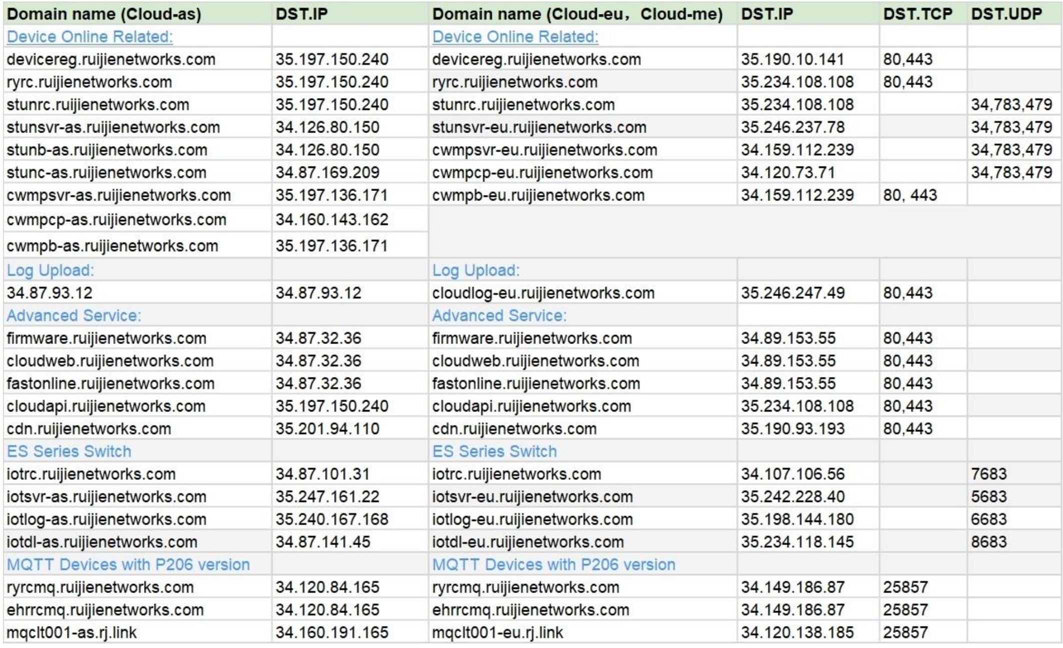
2.1 Network Planning

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	
ehrrcmq.ruijienetworks.com	34.120.84.165	ehrrcmq.ruijienetworks.com	34.149.186.87	25857	
mqclt001-as.rj.link	34.160.191.165	mqclt001-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.

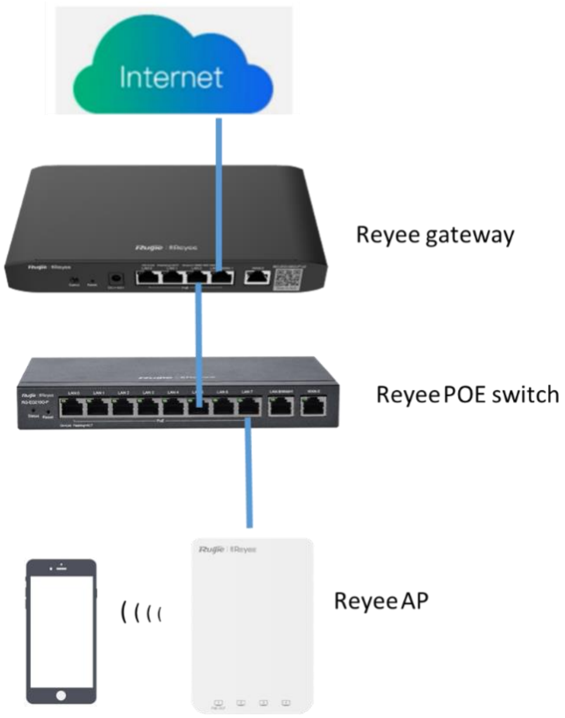
2.2.3 Installation Steps

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

2.3 Quick Provisioning

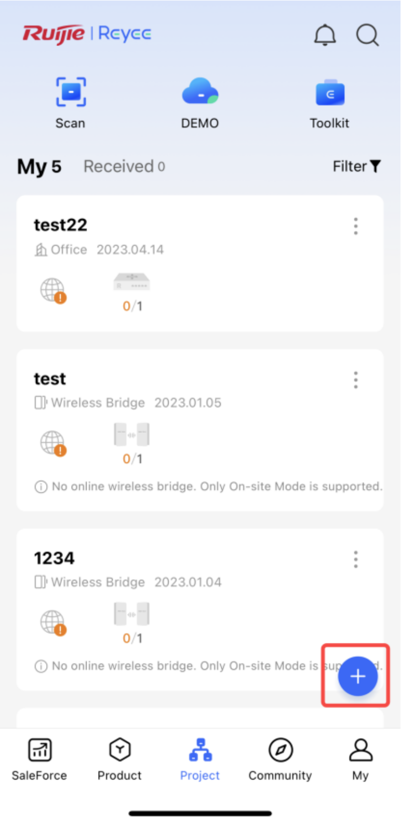
2.3.1 Quick Provisioning Through Ruijie Cloud App

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

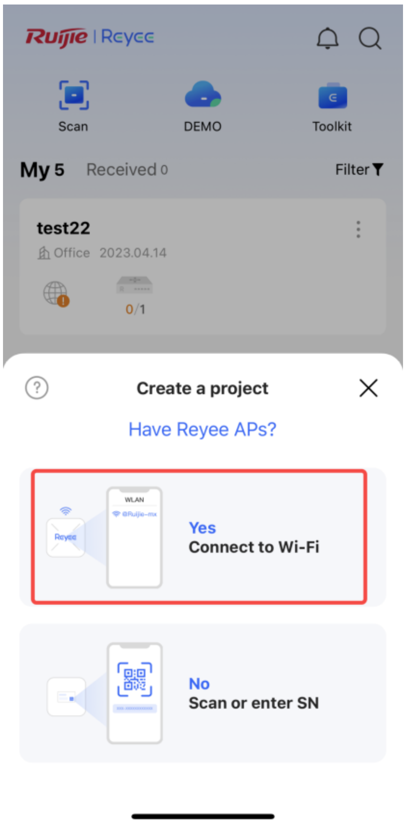


Connect the devices through Ruijie Cloud App for configuration and remote maintenance.

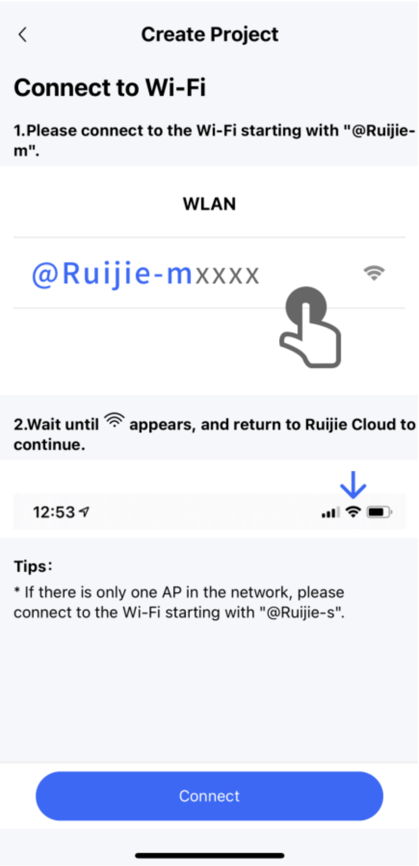
(1) Open Ruijie Cloud App, click **Create a Project,** and select **Connect to Wi-Fi**.



No online wireless bridge. Only On-site Mode is supported.



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



Connect to Wi-Fi

1.Please connect to the Wi-Fi starting with "@Ruijie-m".

2.Wait until appears, and return to Ruijie Cloud to continue.

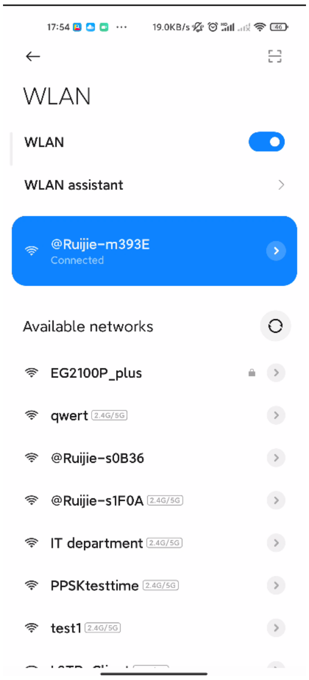
Tips:

* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".

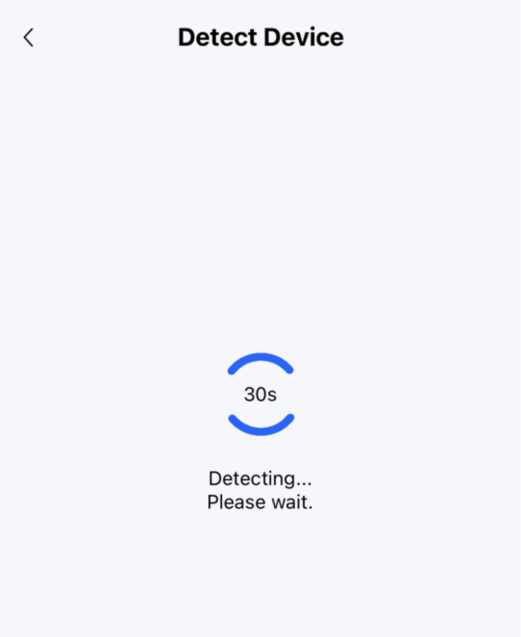
Note

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

(3) Click **Connect** and access SSID **@Ruijie-mxxxx**.

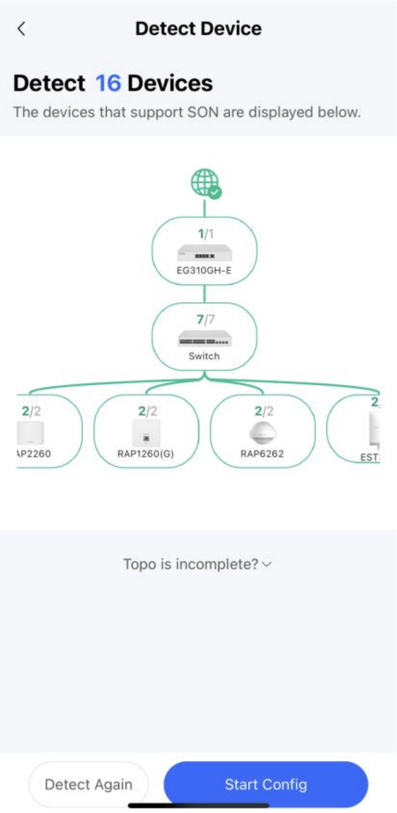


(4) After you access SSID **@Ruijie-mxxxx SSID**, Ruijie Cloud App will generate the topology and detect all devices on the SON.



Detecting...
Please wait.

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

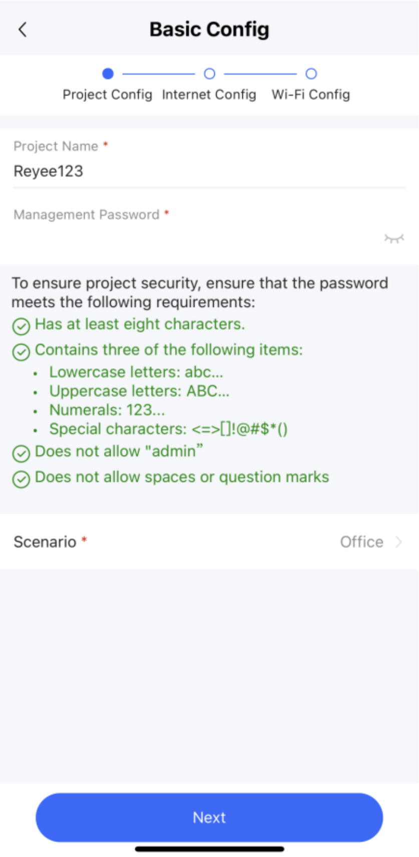


Detect Device

Detect 16 Devices

The devices that support SON are displayed below.

(6) Click Start Config to perform basic configuration of this project. Set Project Name and Management Password.



Basic Config

Project Name *
Reyee123

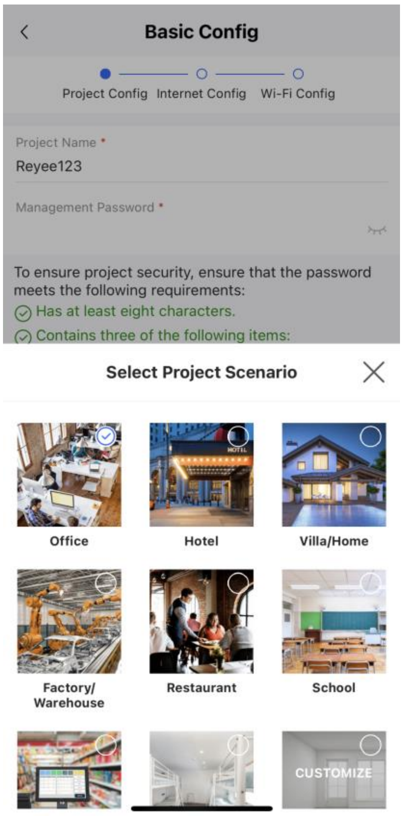
Management Password *

To ensure project security, ensure that the password meets the following requirements:

- ✓ Has at least eight characters.
- ✓ Contains three of the following items:
  - Lowercase letters: abc...
  - Uppercase letters: ABC...
  - Numerals: 123...
  - Special characters: <=>[]!@#$*()
- ✓ Does not allow "admin”
- ✓ Does not allow spaces or question marks

Scenario * Office

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



Basic Config

Project Config Internet Config Wi-Fi Config

Project Name *

Reyee123

Management Password *

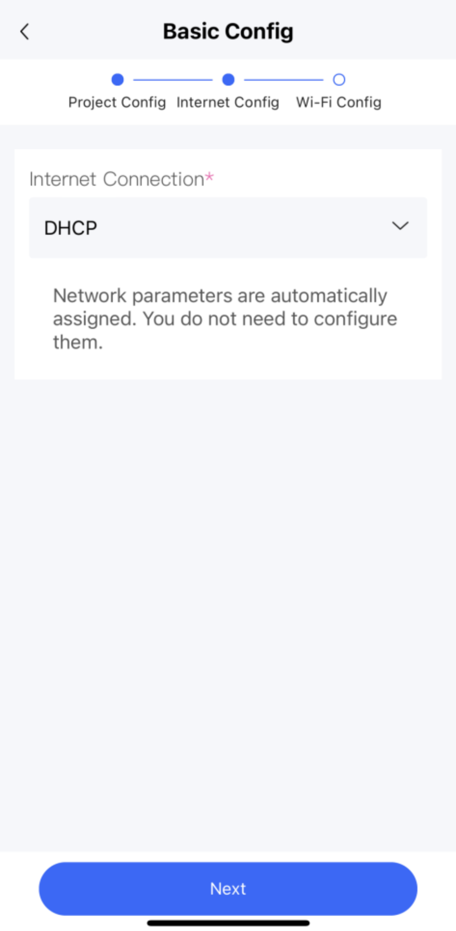
To ensure project security, ensure that the password meets the following requirements:

Has at least eight characters.

Contains three of the following items:

Select Project Scenario

(8) Configure the Internet. For WAN configuration, you can choose **PPPoE**, **DHCP**, or **Static IP**.



Basic Config

Project Config Internet Config Wi-Fi Config

Internet Connection*

DHCP

Network parameters are automatically assigned. You do not need to configure them.

(9) Configure the SSID.

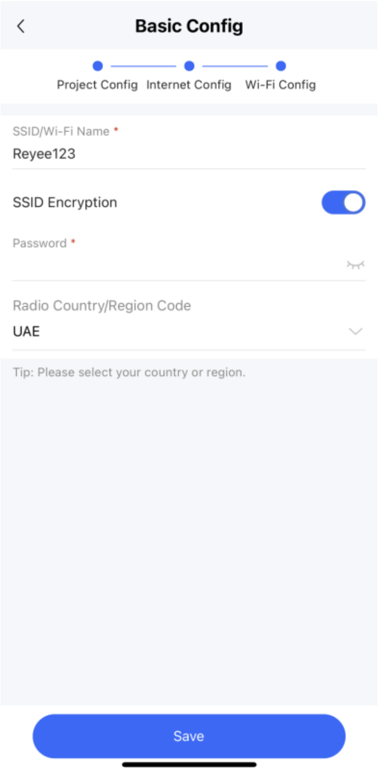
a Enter the name of the SSID.

b Configure it as open to allow clients to access this SSID.

c Configure the password for this SSID.

d Select the region code.

e The configuration will be synchronized to the network.



Basic Config

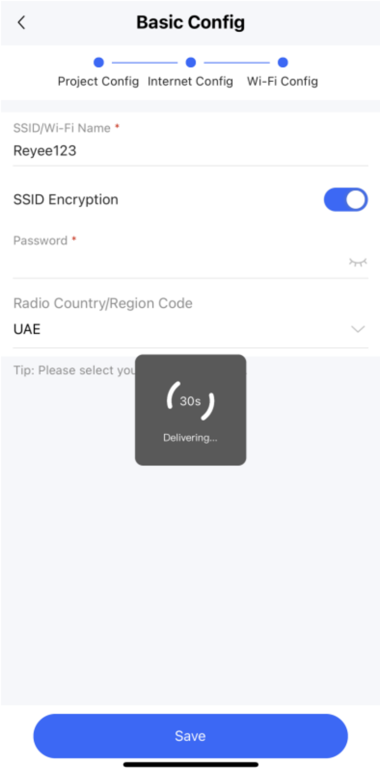
SSID/Wi-Fi Name *
Reyee123

SSID Encryption

Password *

Radio Country/Region Code
UAE

Tip: Please select your country or region.



Basic Config

SSID/Wi-Fi Name *
Reyee123

SSID Encryption

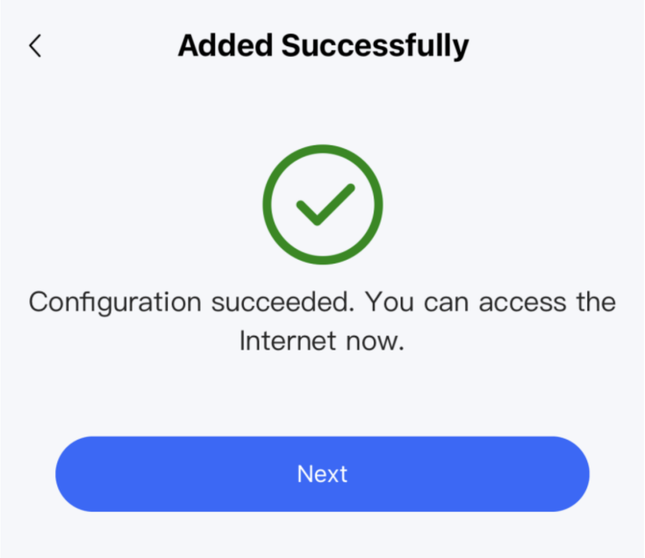
Password *

Radio Country/Region Code
UAE

Tip: Please select you

30s
Delivering...

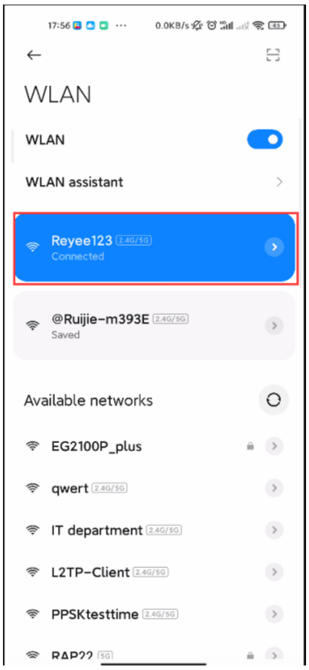
(10) After about 3s, Ruijie Cloud App will prompt that the configuration is delivery succeed.



Added Successfully

Configuration succeeded. You can access the Internet now.

(11) Connect to the SSID created just now to manage the whole network on Cloud App.



17:56 ··· 0.0KB/s

WLAN

WLAN

WLAN assistant

Reyee123 2.4G/5G
Connected

@Ruijie-m393E 2.4G/5G
Saved

Available networks

EG2100P_plus

qwert 2.4G/5G

IT department 2.4G/5G

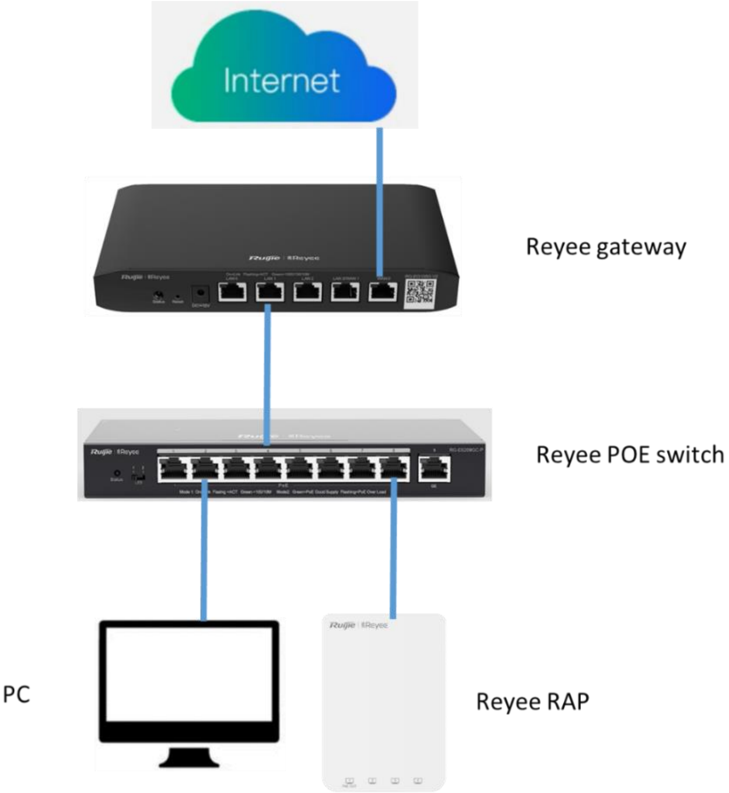
L2TP-Client 2.4G/5G

PPSKtesttime 2.4G/5G

RAP22 5G

2.3.2 Quick Provisioning Through Reyee Eweb

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

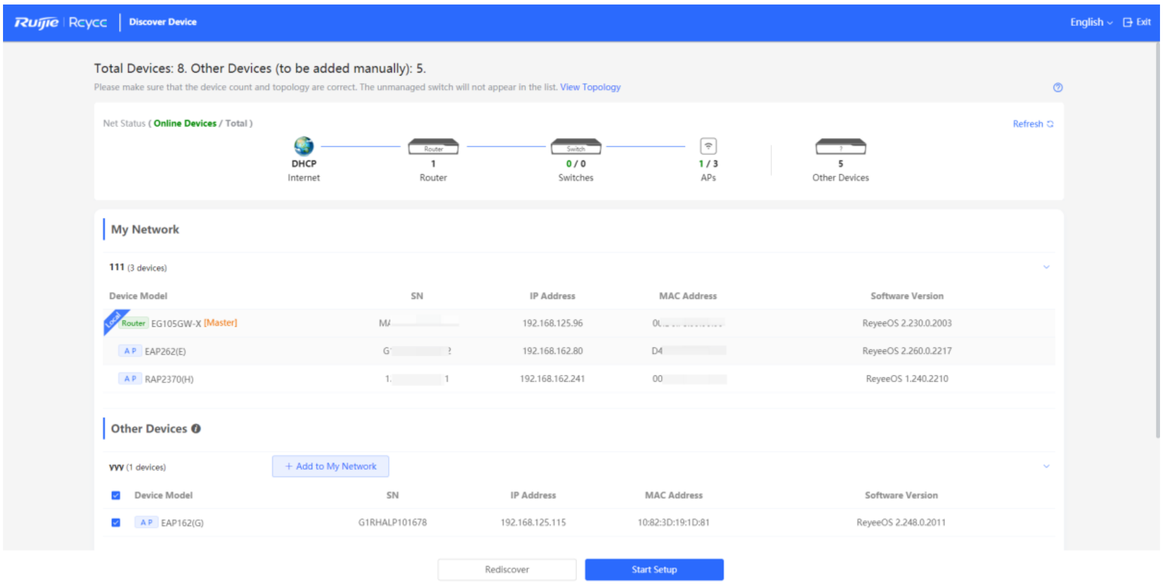


You can use a web management system to configure and maintain the Reyee router.

(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.



Total Devices: 8. Other Devices (to be added manually): 5.

Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list. View Topology

Net Status (Online Devices / Total)

Refresh

DHCP Internet	1 Router	0 / 0 Switches	1 / 3 APs	5 Other Devices

My Network

111 (3 devices)

Device Model	SN	IP Address	MAC Address	Software Version
Local Router EG105GW-X [Master]	M/[redacted]	192.168.125.96	0[redacted]	ReyeeOS 2.230.0.2003
A P EAP262(E)	G[redacted]2	192.168.162.80	D4[redacted]	ReyeeOS 2.260.0.2217
A P RAP2370(H)	1.[redacted]1	192.168.162.241	00[redacted]	ReyeeOS 1.240.2210

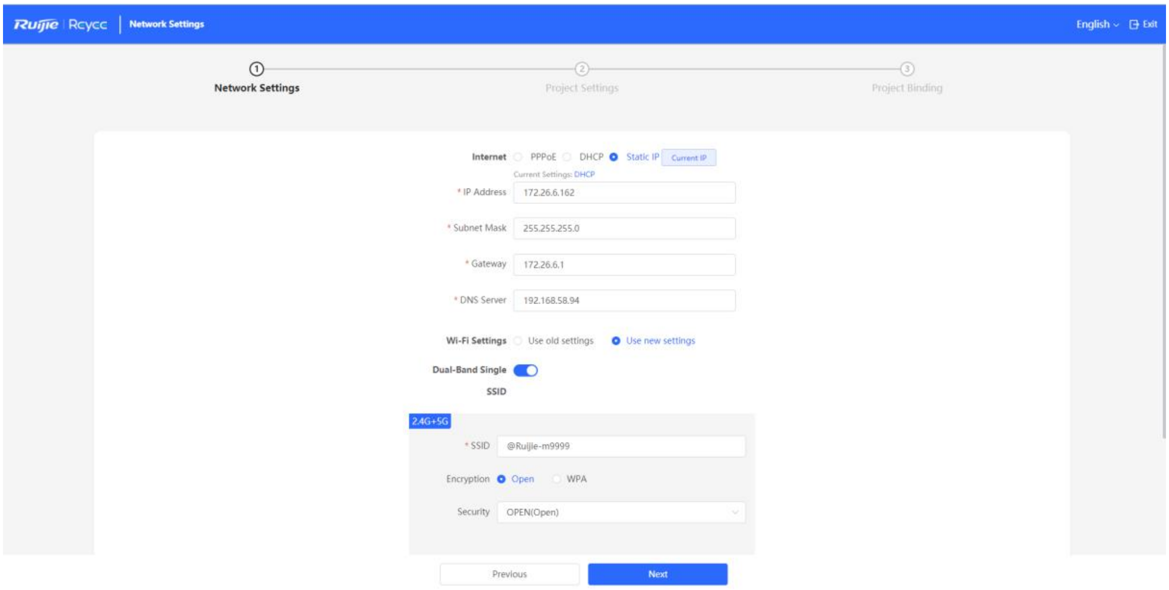
Other Devices

yyy (1 devices)

+ Add to My Network

☑	Device Model	SN	IP Address	MAC Address	Software Version
☑	A P EAP162(G)	G1RHALP101678	192.168.125.115	10:82:3D:19:1D:81	ReyeeOS 2.248.0.2011

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



Internet ○ PPPoE ○ DHCP ● Static IP Current IP

Current Settings: DHCP

* IP Address 172.26.6.162

* Subnet Mask 255.255.255.0

* Gateway 172.26.6.1

* DNS Server 192.168.58.94

Wi-Fi Settings ○ Use old settings ● Use new settings

Dual-Band Single SSID ●

2.4G+5G

* SSID @Ruijie-m9999

Encryption ● Open ○ WPA

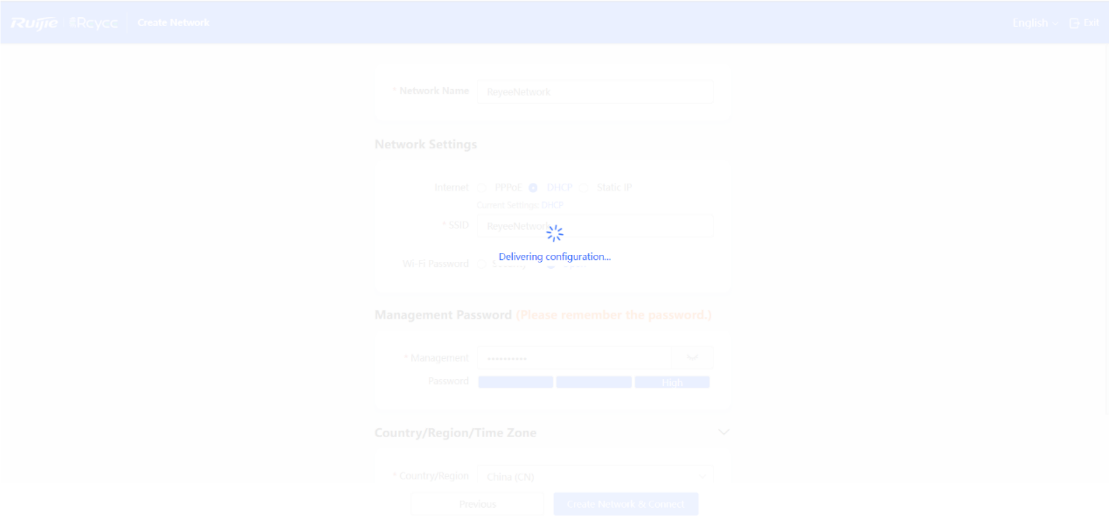
Security OPEN(Open)

a Enter the network name, and configure the Internet access mode of this network.

b Enter the password of the SSID or configure the SSID as open.

c Select the country/region.

(4) Click **Create Network & Connect**. The configuration will be delivered and activated.



Network Name: ReyeeNetwork

Network Settings

Internet: ○ PPPoE ● DHCP ○ Static IP

Current Settings: DHCP

SSID: ReyeeNetwork

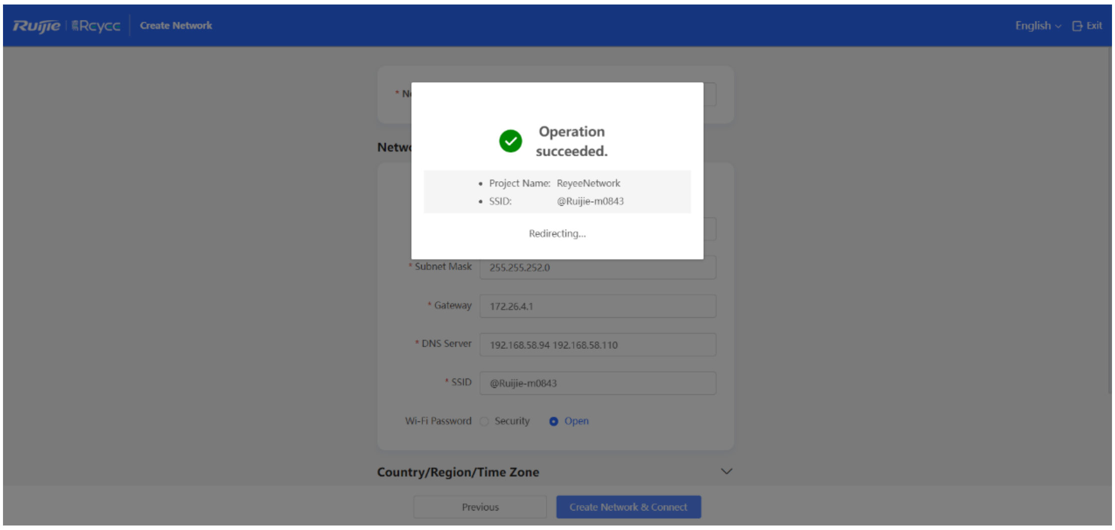
Delivering configuration...

Management Password (Please remember the password.)

Country/Region/Time Zone

Country/Region: China (CN)

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



Operation succeeded.

- Project Name: ReyeeNetwork
- SSID: @Ruijie-m0843

Redirecting...

Subnet Mask: 255.255.252.0

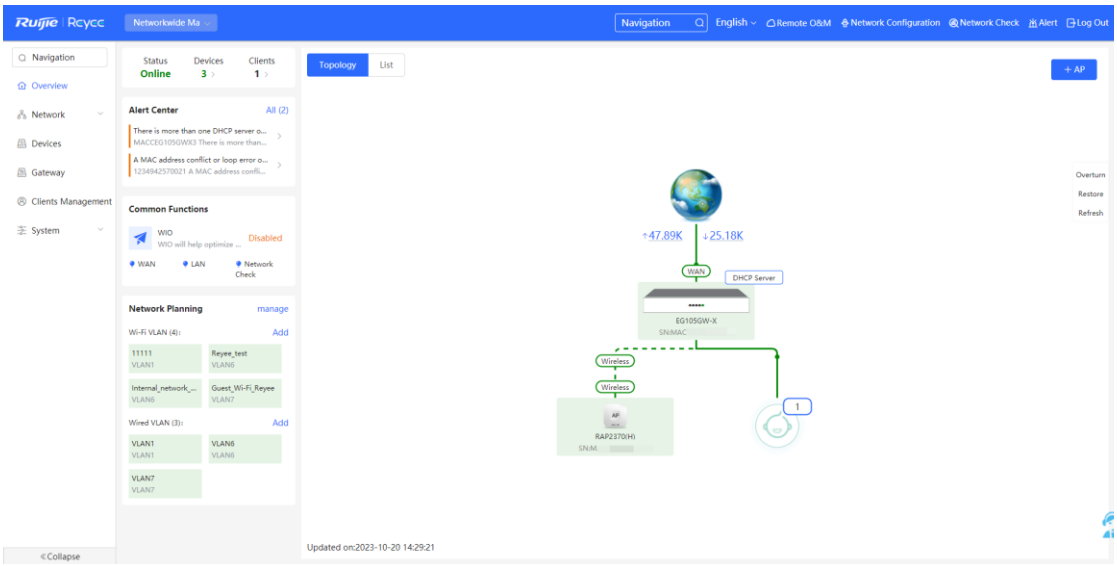
Gateway: 172.26.4.1

DNS Server: 192.168.58.94 192.168.58.110

SSID: @Ruijie-m0843

Wi-Fi Password: ○ Security ● Open

Country/Region/Time Zone



Status: Online Devices: 3 Clients: 1

Alert Center All (2)

There is more than one DHCP server o...
MACCEG105GWX3 There is more than...

A MAC address conflict or loop error o...
1234942570021 A MAC address confli...

Common Functions

WIO Disabled
WIO will help optimize ...

Network Planning

Wi-Fi VLAN (4):

11111 VLAN1	Reyee_test VLAN6
Internal_network_... VLAN6	Guest_Wi-Fi_Reyee VLAN7

Wired VLAN (3):

VLAN1 VLAN1	VLAN6 VLAN6
VLAN7 VLAN7	

Updated on:2023-10-20 14:29:21

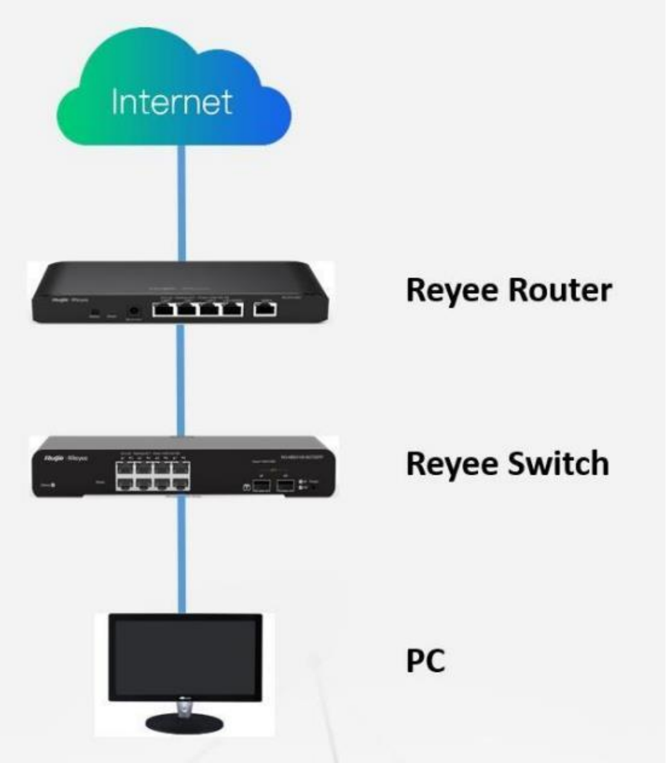
3 Device Management

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.

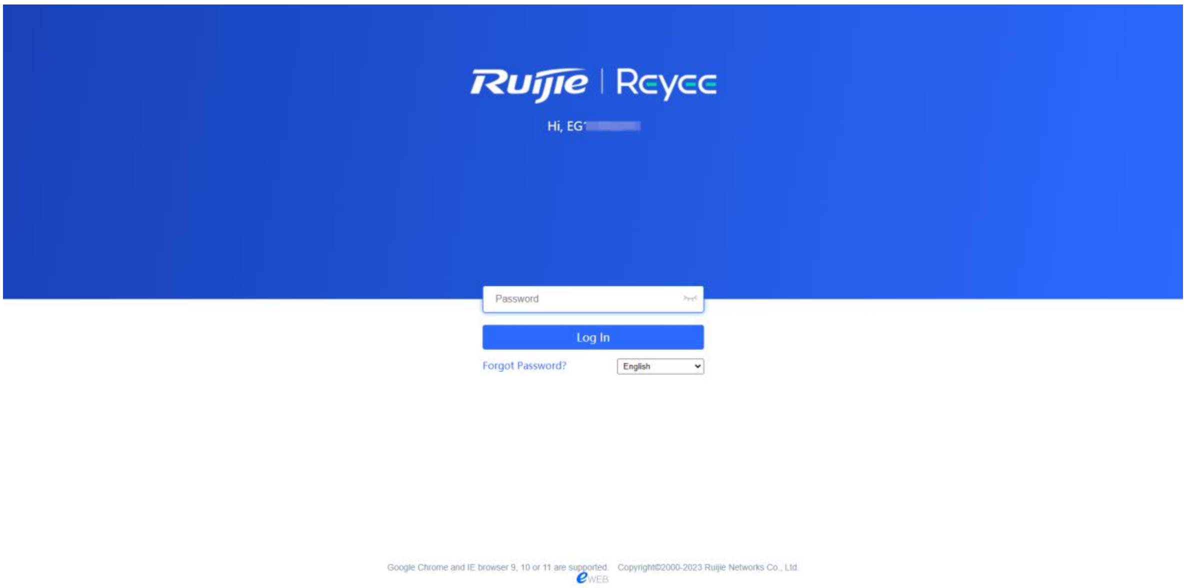
Reyee routers support both web interface management and remote management through life-time-free Ruijie Cloud App and Ruijie Cloud platform. You can view the network status, modify the configuration, and troubleshoot faults easily.

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**.



Hi, EG[redacted]

Google Chrome and IE browser 9, 10 or 11 are supported. Copyright©2000-2023 Ruijie Networks Co., Ltd.

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

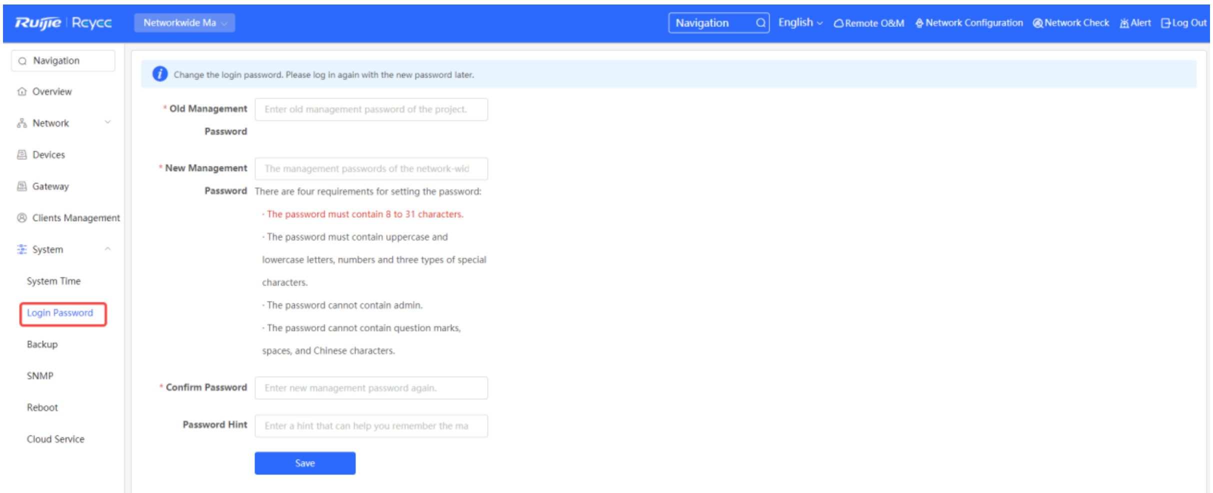
Change your password regularly to ensure account security.

(1) Log into the web management system by using the default IP address.

(2) Choose **System > Login Password**.

(3) Enter the old password and new password.

(4) Click **Save**.



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

* Old Management Password: Enter old management password of the project.

* New Management Password: The management passwords of the network-wid

There are four requirements for setting the password:

- The password must contain 8 to 31 characters.
- The password must contain uppercase and lowercase letters, numbers and three types of special characters.
- The password cannot contain admin.
- The password cannot contain question marks, spaces, and Chinese characters.

* Confirm Password: Enter new management password again.

Password Hint: Enter a hint that can help you remember the ma

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

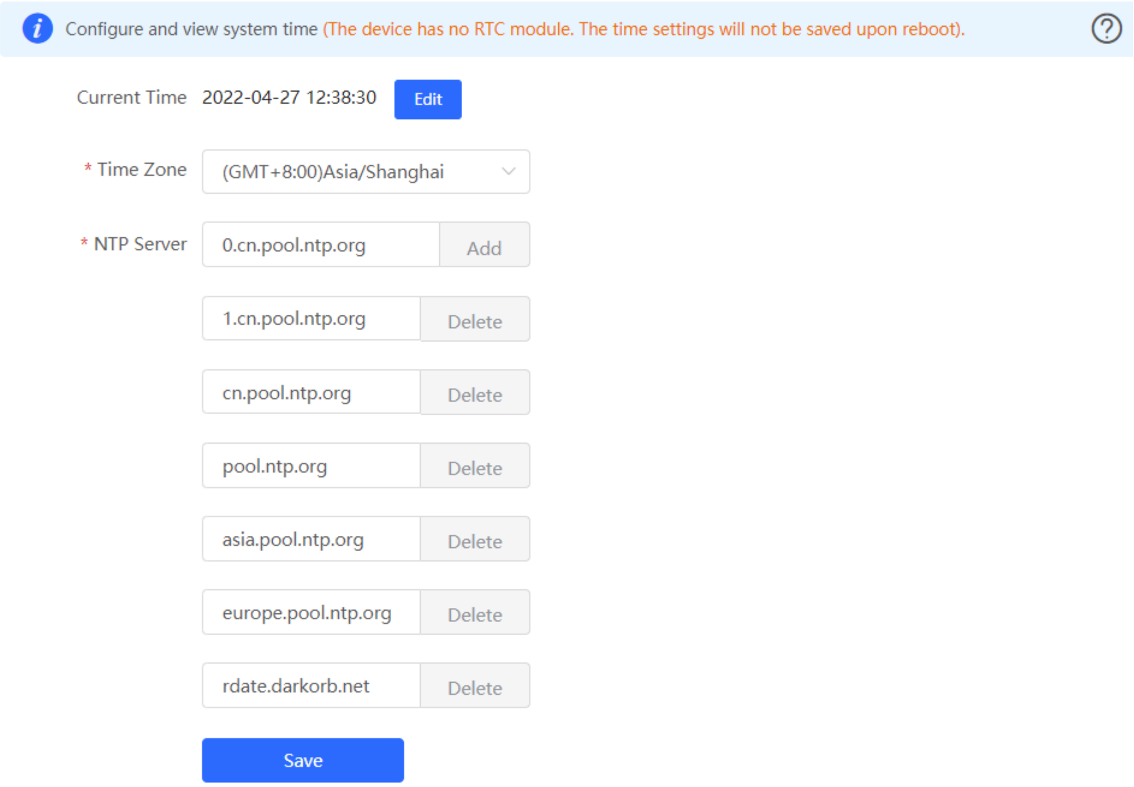
Caution

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

1.cn.pool.ntp.org

cn.pool.ntp.org

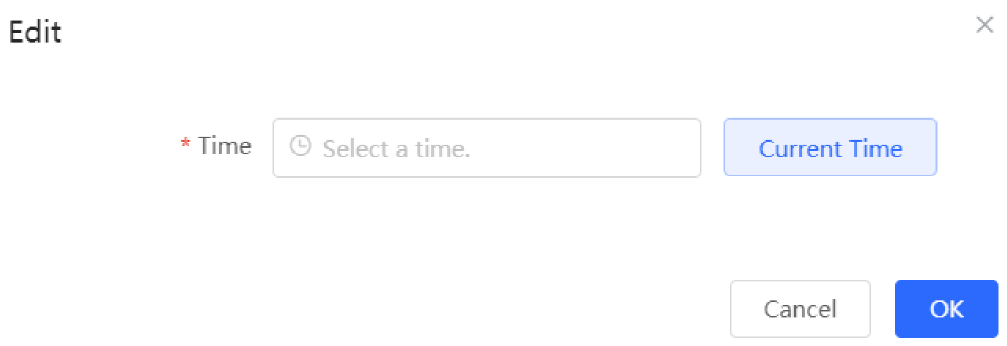
pool.ntp.org

asia.pool.ntp.org

europe.pool.ntp.org

rdate.darkorb.net

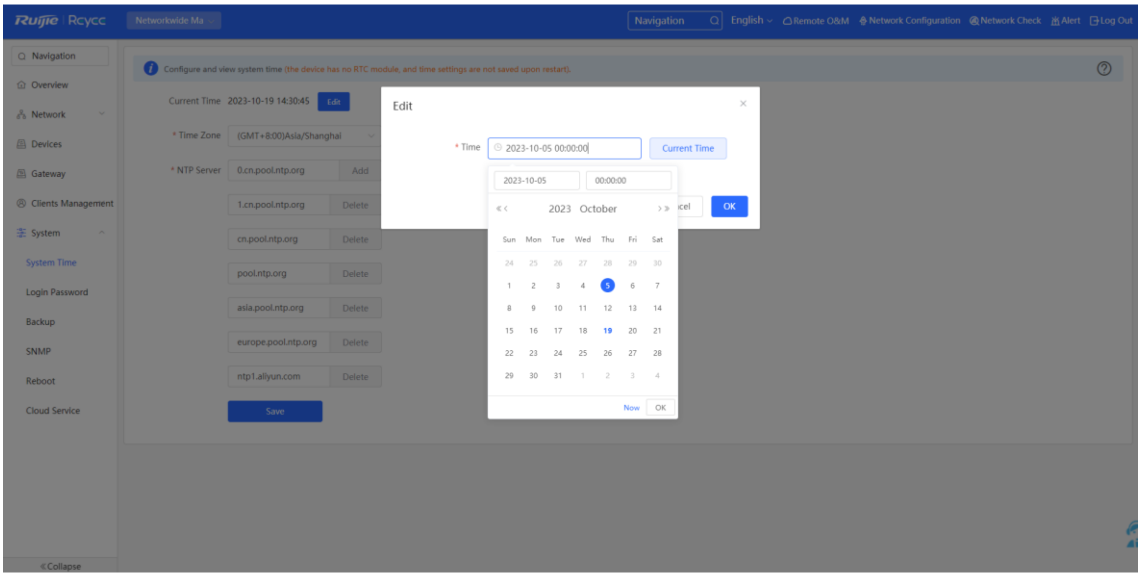
Choose **Current Time** > **Edit** > **Current Time**. The current system time will be filled in automatically.

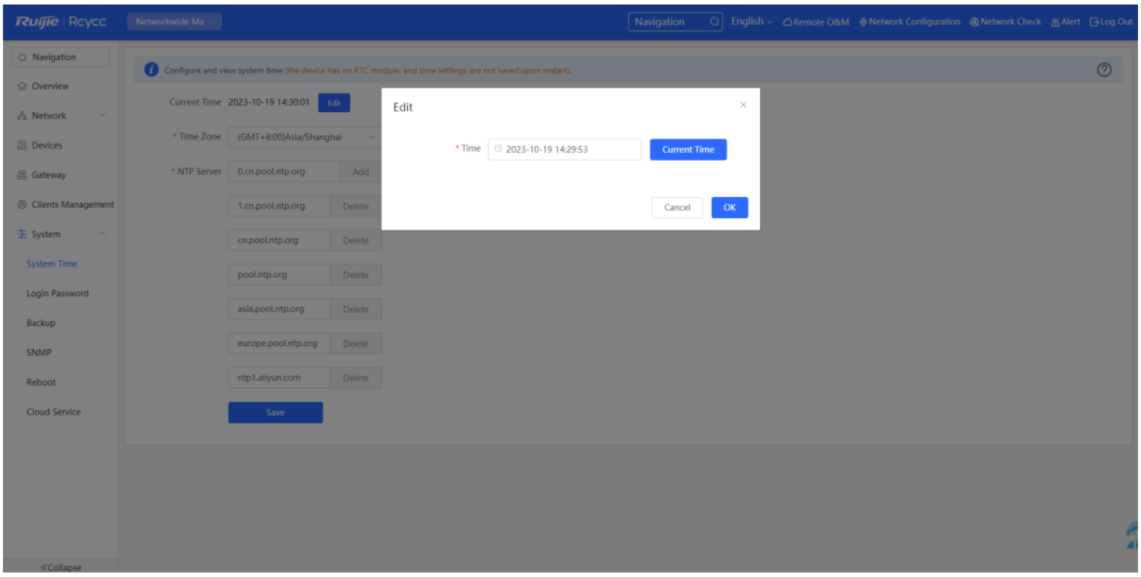


Edit

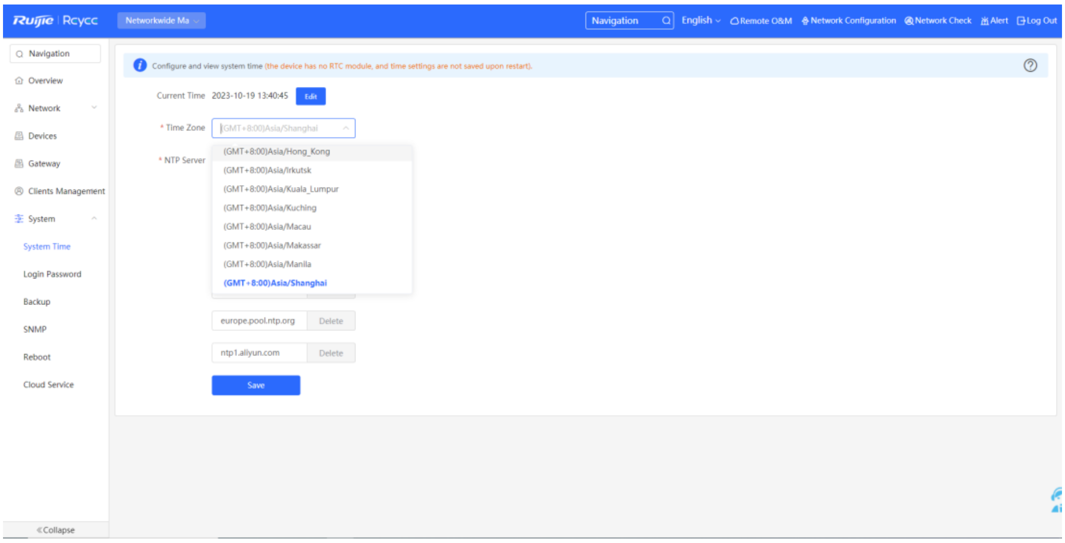
* Time Select a time.

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

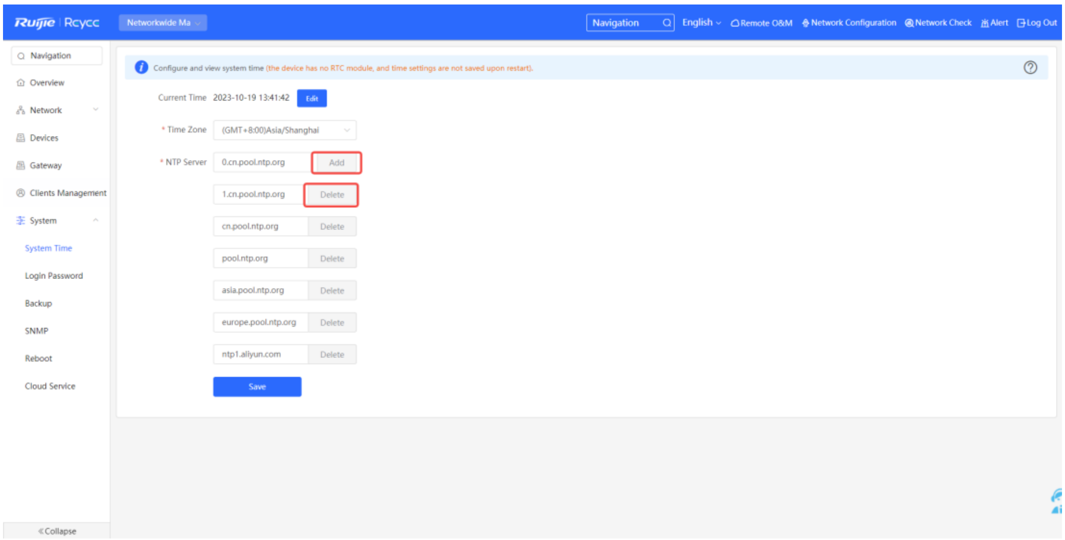




- Manually select a value from the **Time Zone** drop-down list box.



- Add or delete the NTP server.



Configure and view system time (the device has no RTC module, and time settings are not saved upon restart).

Current Time 2023-10-19 13:41:42

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

* NTP Server 0.cn.pool.ntp.org

1.cn.pool.ntp.org

cn.pool.ntp.org

pool.ntp.org

asia.pool.ntp.org

europe.pool.ntp.org

ntp1.aliyun.com

3.4 Configuring Upgrade

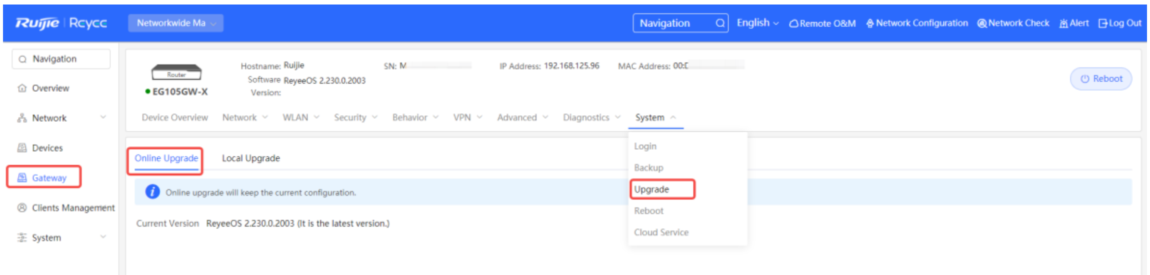
To use new features, upgrade the router to the latest version. There are two methods of upgrading routers: online upgrade and local upgrade.

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**.



EG105GW-X

Hostname: Ruijie

Software Version: ReyeeOS 2.230.0.2003

SN: [redacted]

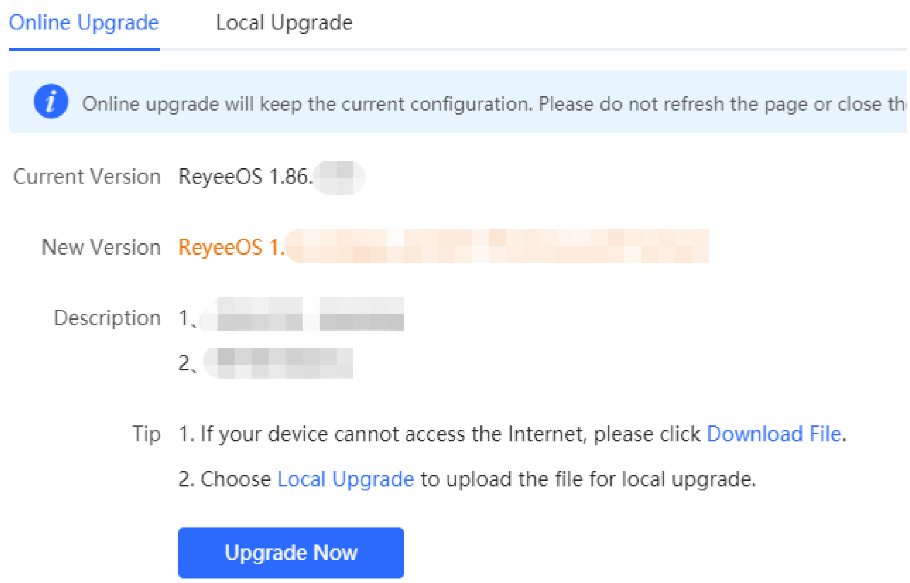
IP Address: 192.168.125.96

MAC Address: [redacted]

Online upgrade will keep the current configuration.

Current Version ReyeeOS 2.230.0.2003 (It is the latest version.)

- 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 will keep the current configuration. Please do not refresh the page or close th

Current Version ReyeeOS 1.86.[redacted]

New Version ReyeeOS 1.[redacted]

Description 1、[redacted]
2、[redacted]

Tip 1. If your device cannot access the Internet, please click Download File.
2. Choose Local Upgrade to upload the file for local upgrade.

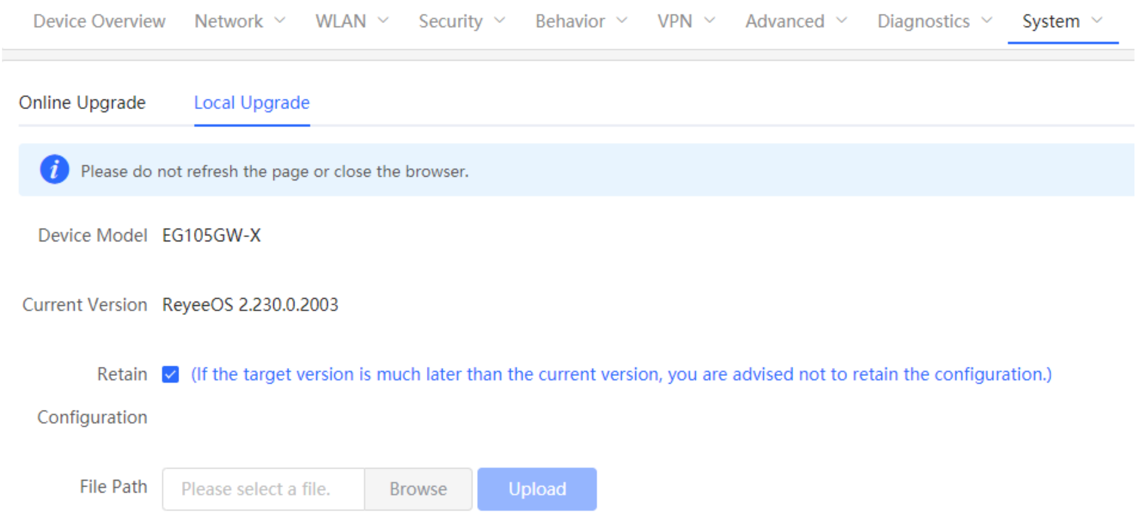
3.4.2 Local Upgrade

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**.



Please do not refresh the page or close the browser.

Device Model EG105GW-X

Current Version ReyeeOS 2.230.0.2003

Retain Configuration ☑ (If the target version is much later than the current version, you are advised not to retain the configuration.)

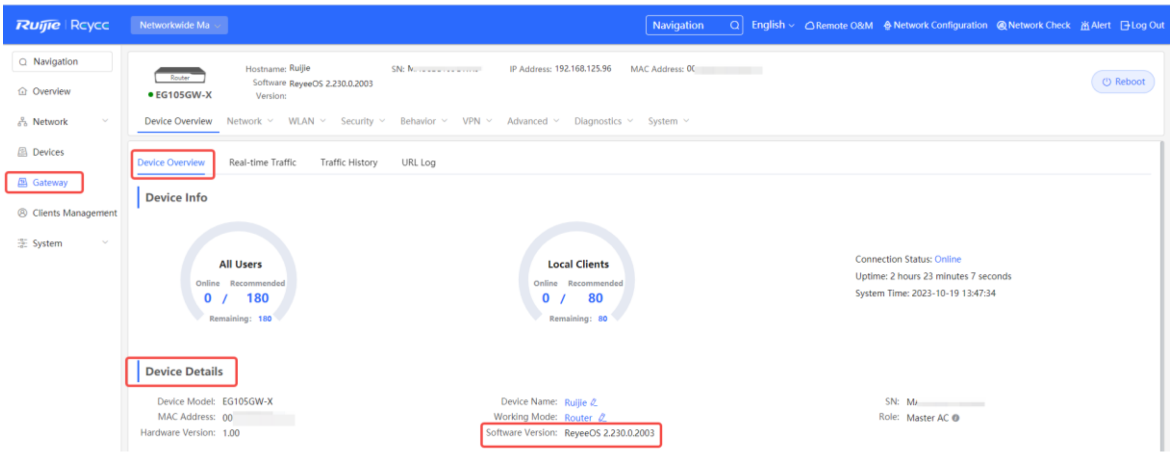
File Path Please select a file.

(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** > **Device 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.



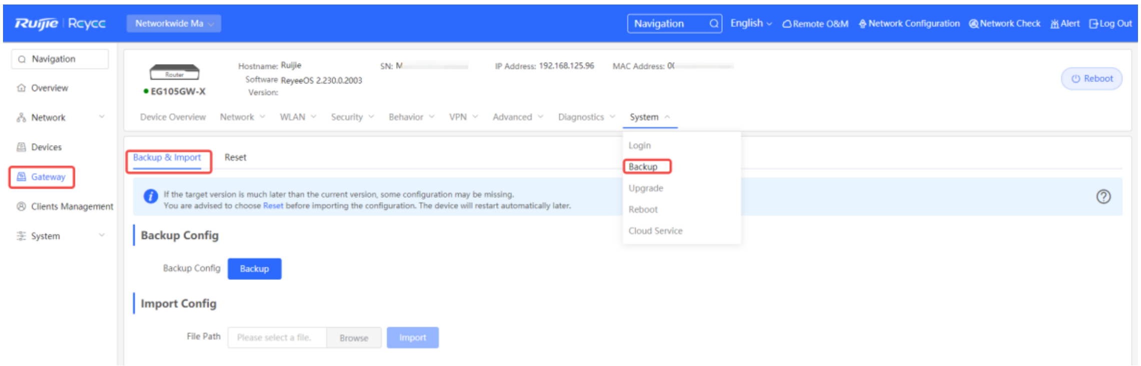
Hostname: Ruijie
Software Version: ReyeeOS 2.230.0.2003
IP Address: 192.168.125.96
Connection Status: Online
Uptime: 2 hours 23 minutes 7 seconds
System Time: 2023-10-19 13:47:34
Device Model: EG105GW-X
Hardware Version: 1.00
Device Name: Ruijie
Working Mode: Router
Software Version: ReyeeOS 2.230.0.2003
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** > **Backup > Backup & Import**.



If the target version is much later than the current version, some configuration may be missing.
You are advised to choose Reset before importing the configuration. The device will restart automatically later.

(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.

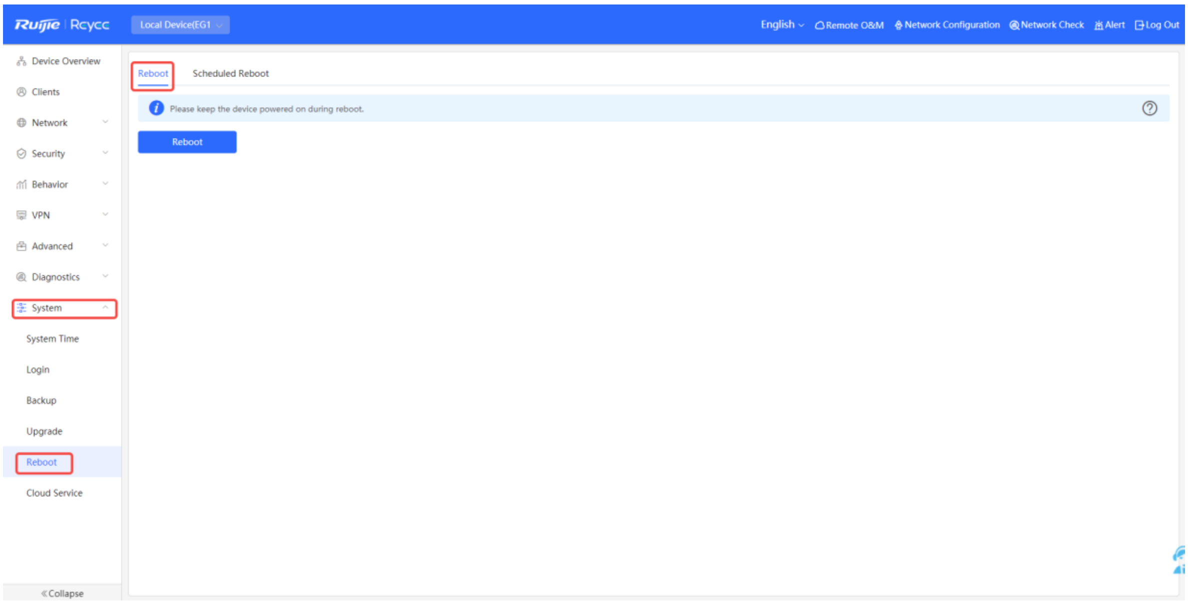
You are advised to restore the settings before importing the configuration. The router will restart automatically if you restore it.

3.6 Configuring Restart

3.6.1 Restarting the Current Device

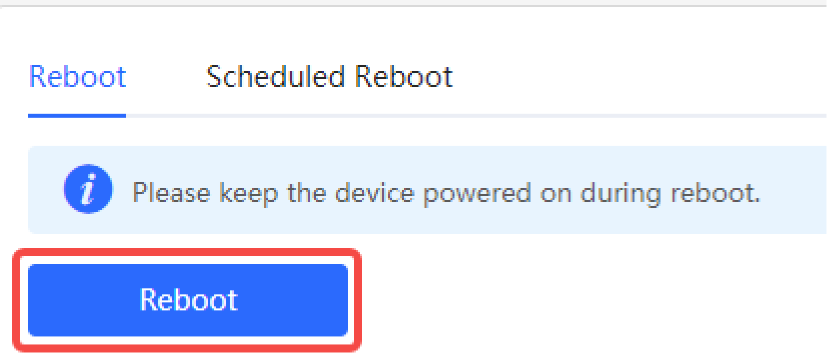
- Switch to the **Local Device** mode.

Choose **System** > **Reboot**



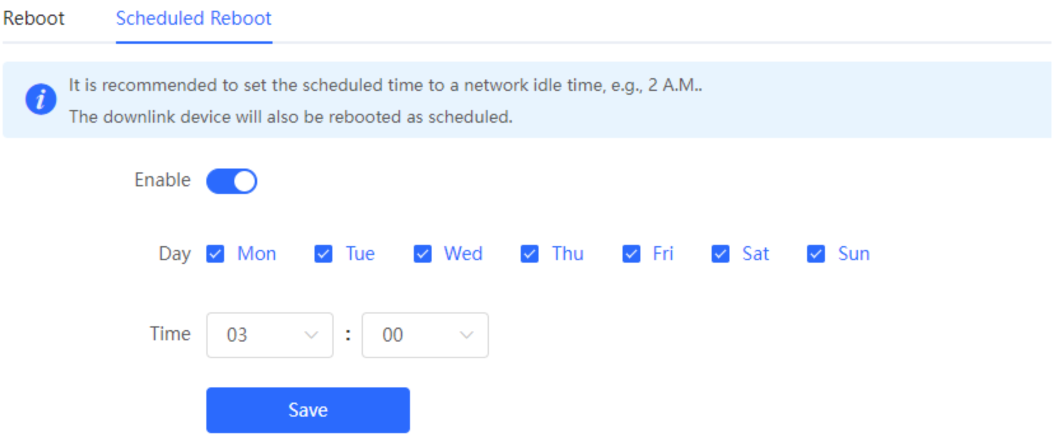
Please keep the device powered on during reboot.

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.



Please keep the device powered on during reboot.

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



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.

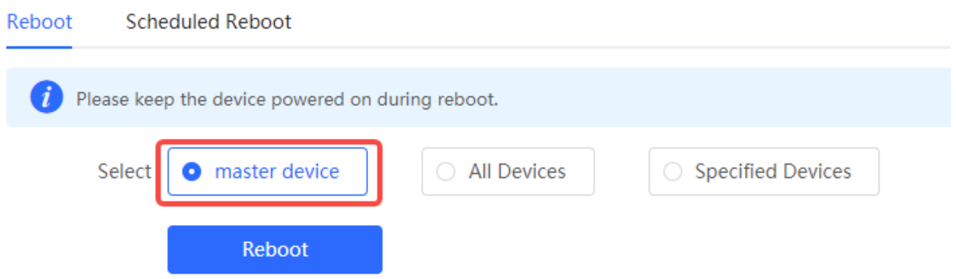
Enable: on

Day ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Time 03 : 00

- Switch to the **Network** mode.

Choose **System** > **Reboot** > **Reboot**. Select **master device** to restart the current device.

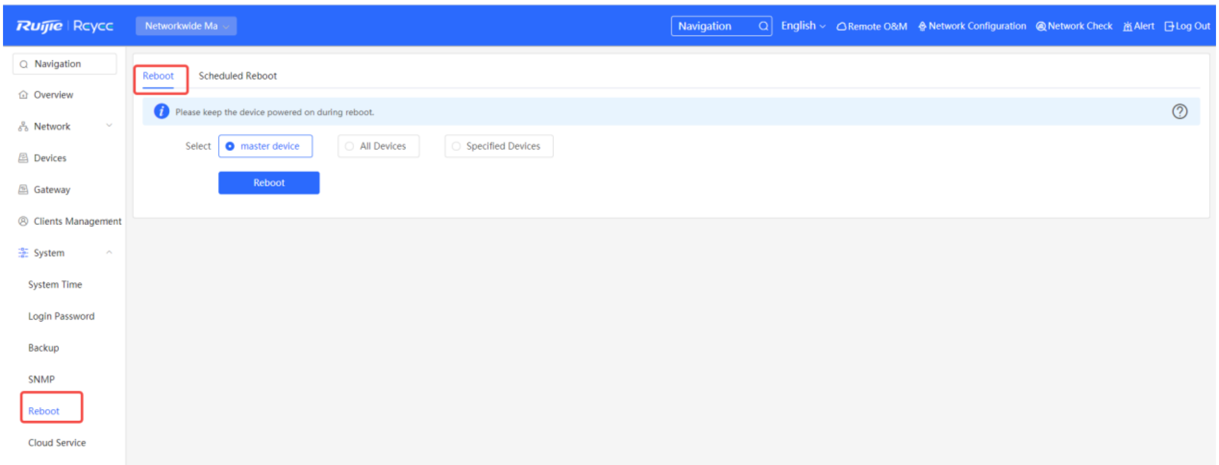


Please keep the device powered on during reboot.

Select ● master device ○ All Devices ○ Specified Devices

3.6.2 Restarting All Devices on the Network

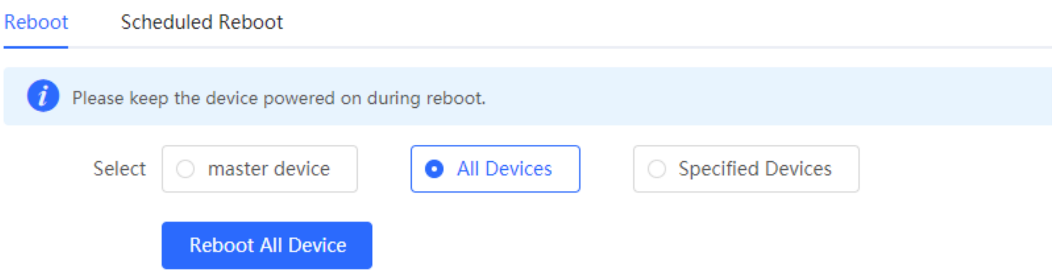
Switch to the **Network** mode. Choose **System** > **Reboot** > **Reboot**.



Please keep the device powered on during reboot.

Select ● master device ○ All Devices ○ Specified Devices

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



Please keep the device powered on during reboot.

Select ○ master device ● All Devices ○ Specified Devices

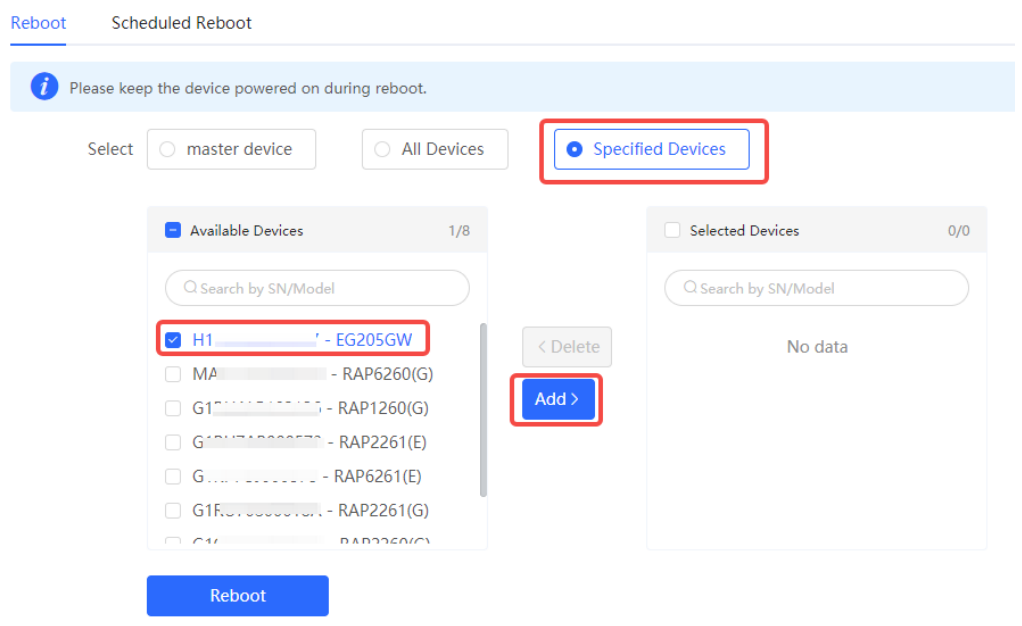
Caution

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

Please keep the device powered on during reboot.

Select ○ master device ○ All Devices ● Specified Devices

☑ Available Devices 1/8

Search by SN/Model

☑ H1[redacted] - EG205GW
□ MA[redacted] - RAP6260(G)
□ G1[redacted] - RAP1260(G)
□ G[redacted] - RAP2261(E)
□ G[redacted] - RAP6261(E)
□ G1[redacted] - RAP2261(G)

< Delete
Add >

□ Selected Devices 0/0

Search by SN/Model

No data

Reboot

3.6.4 Configuring Scheduled Restart

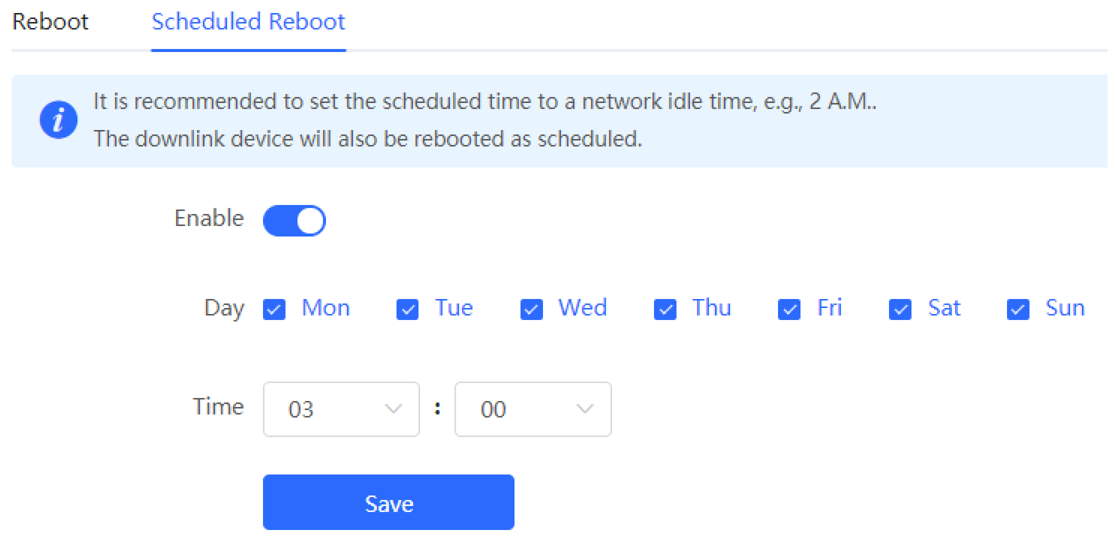
Confirm that the system time is accurate to avoid network interruption caused by device restart at an incorrect time point. For details about how to configure the system time, see section 3.3 Configuring the System Time.

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

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

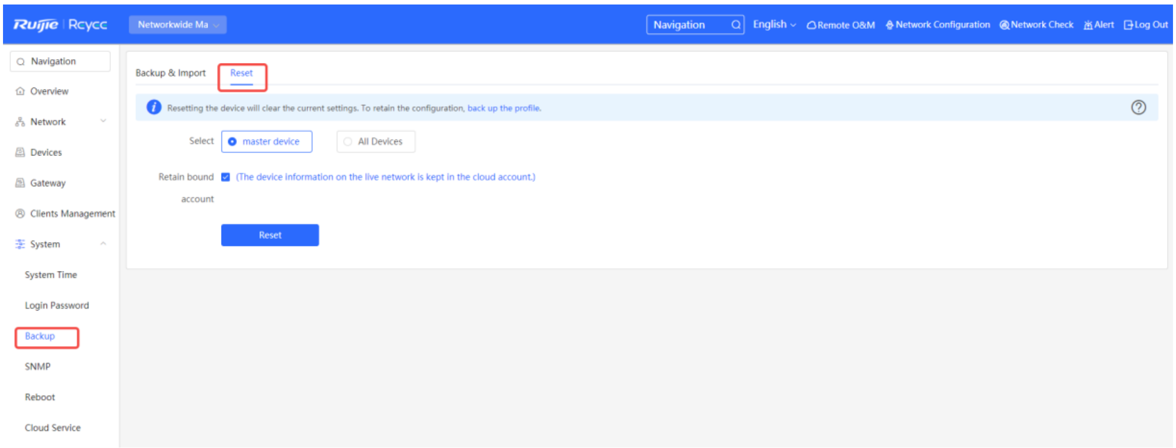
3.7 Restoring Factory Settings

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** > **Backup** > **Reset**.



Resetting the device will clear the current settings. To retain the configuration, back up the profile.

Select ● master device ○ All Devices

Retain bound account ☑ (The device information on the live network is kept in the cloud account.)

(3) Select the target device.

- **Master Device**: Select **Master Device**. Only the local device is restored.
- **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

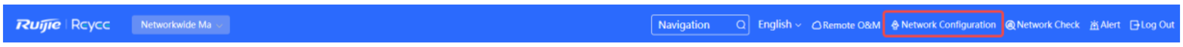
Perform network configuration to connect the router to the Internet quickly.

Three Internet access modes are available:

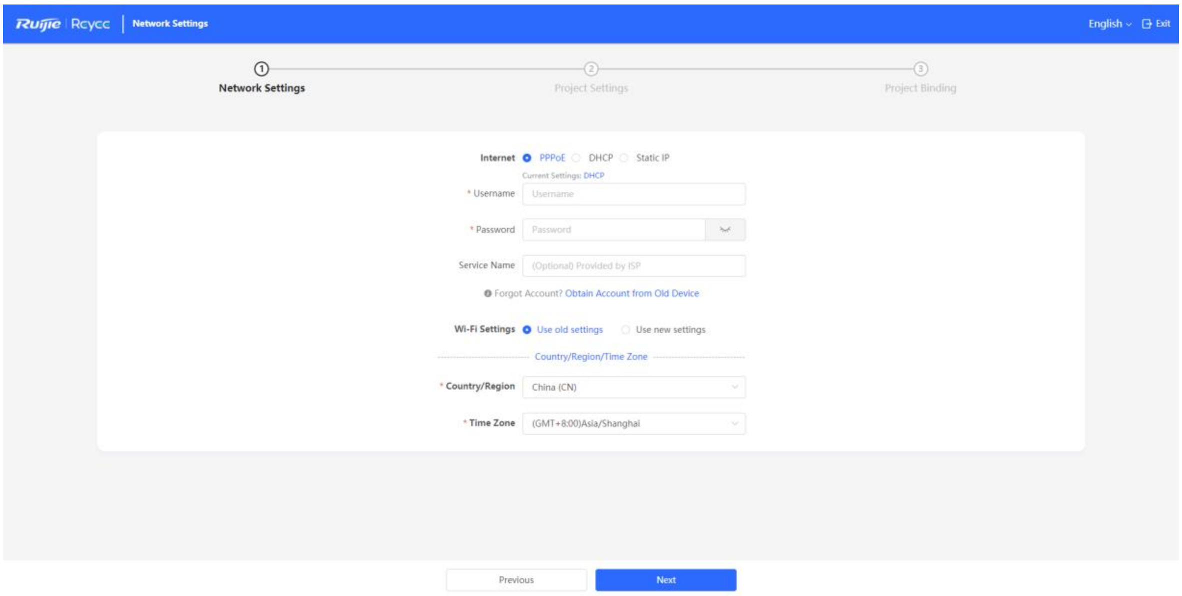
- PPPoE
- DHCP
- Static IP address

4.1.1 PPPoE Configuration Through a WAN Port

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



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



Internet ● PPPoE ○ DHCP ○ Static IP

Current Settings: DHCP

* Username Username

* Password Password

Service Name (Optional) Provided by ISP

Forgot Account? Obtain Account from Old Device

Wi-Fi Settings ● Use old settings ○ Use new settings

Country/Region/Time Zone

* Country/Region China (CN)

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

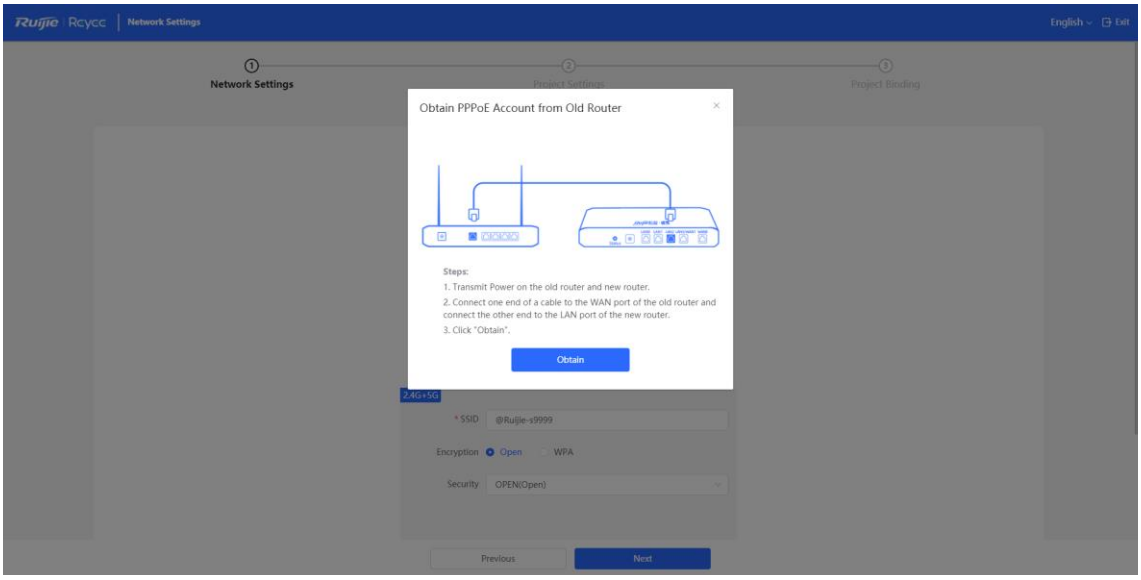
(2) Enter your **Username** and **Password** obtained from an ISP. **Service Name** is optional.

(3) If you forget the password from the ISP, click **Obtain Account from Old Device.**

(4) Click **Next**, and configure **Network Name** and **Password.**

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

(6) After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb.



Obtain PPPoE Account from Old Router

Steps:

1. Transmit Power on the old router and new router.

2. Connect one end of a cable to the WAN port of the old router and connect the other end to the LAN port of the new router.

3. Click "Obtain".

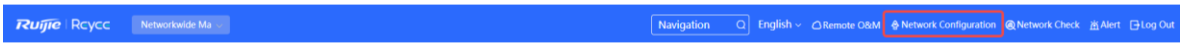
* SSID @Ruijie-s9999

Encryption ● Open ○ WPA

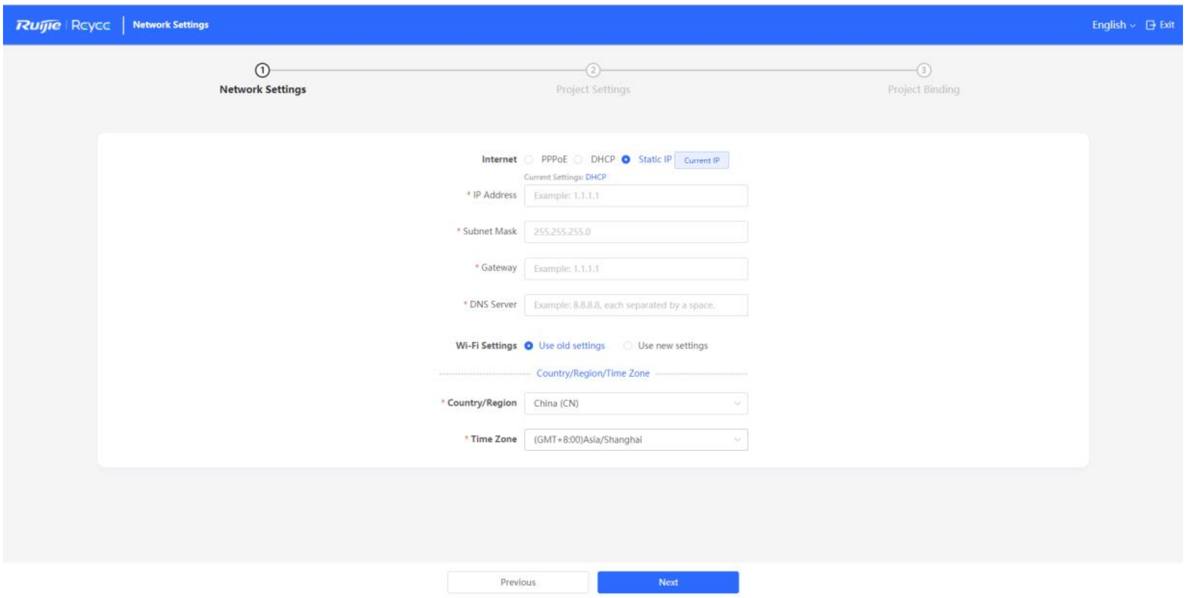
Security OPEN(Open)

4.1.2 Static IP Address Configuration Through a WAN Port

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



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



Internet ○ PPPoE ○ DHCP ● Static IP

Current Settings: DHCP

* IP Address Example: 1.1.1.1

* Subnet Mask 255.255.255.0

* Gateway Example: 1.1.1.1

* DNS Server Example: 8.8.8.8, each separated by a space.

Wi-Fi Settings ● Use old settings ○ Use new settings

* Country/Region China (CN)

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

(3) Configure an IP address, a subnet mask, a gateway IP address, and a DNS server address.

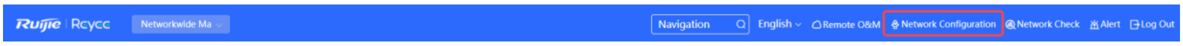
(4) Click **Next**, and configure **Network Name** and **Password.**

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

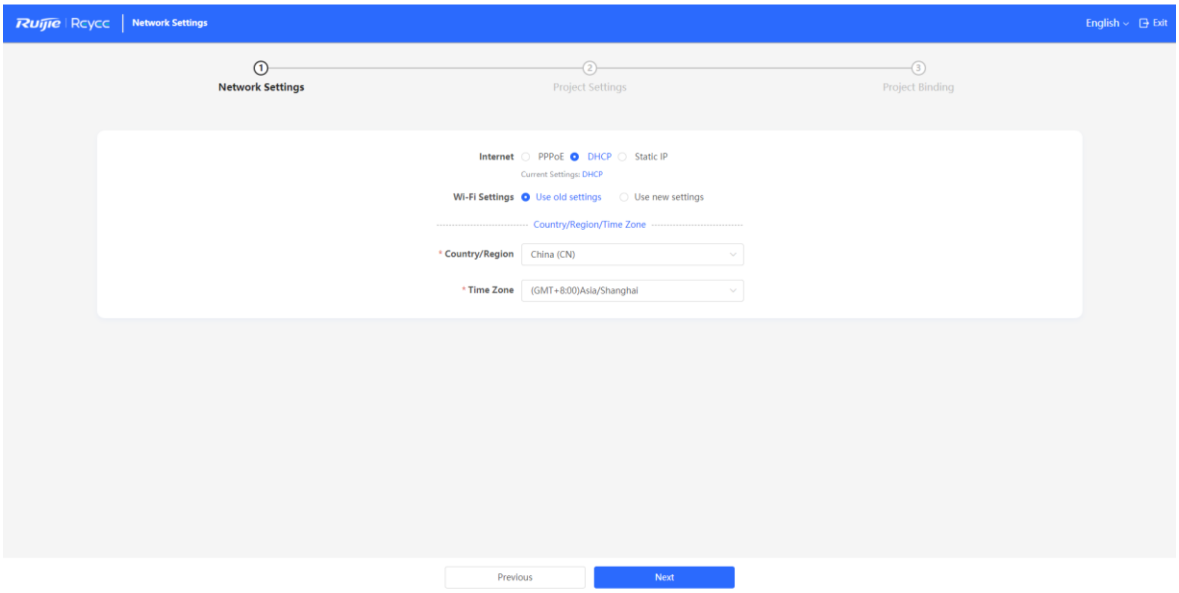
(6) After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb.

4.1.3 DHCP Configuration Through a WAN Port

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



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



Internet ○ PPPoE ● DHCP ○ Static IP

Current Settings: DHCP

Wi-Fi Settings ● Use old settings ○ Use new settings

* Country/Region: China (CN)

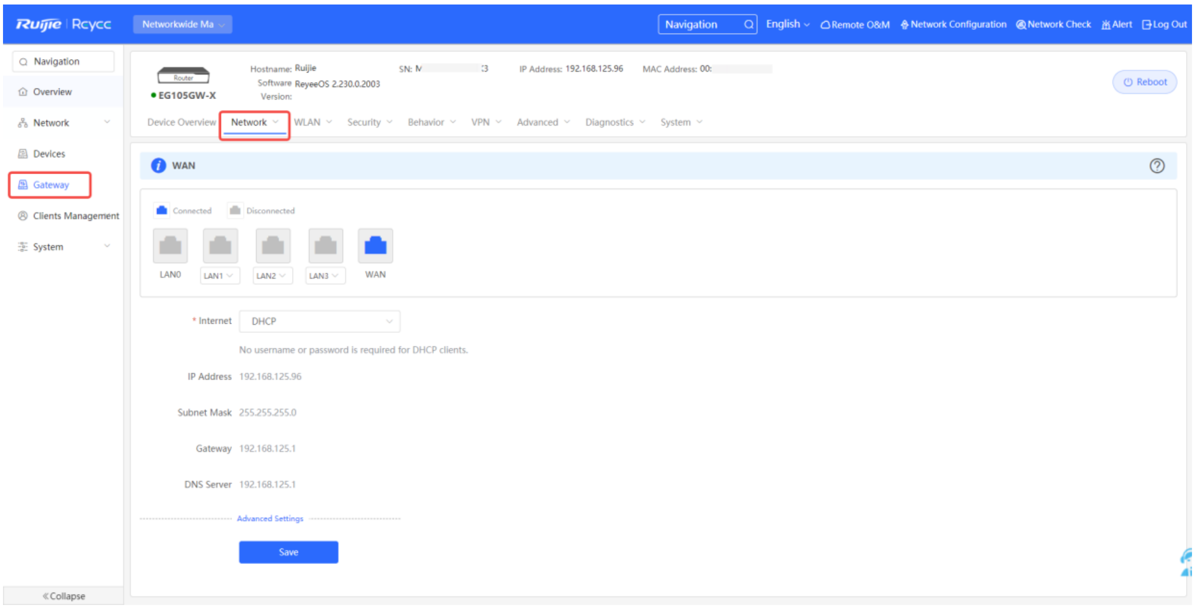
* Time Zone: (GMT+8:00)Asia/Shanghai

(3) Click **Next**, and configure **Network Name** and **Password**.

(4) 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**.



● EG105GW-X

Hostname: Ruijie

Software Version: ReyeeOS 2.230.0.2003

SN: M[redacted]3

IP Address: 192.168.125.96

MAC Address: 00:[redacted]

* Internet: DHCP

No username or password is required for DHCP clients.

IP Address: 192.168.125.96

Subnet Mask: 255.255.255.0

Gateway: 192.168.125.1

DNS Server: 192.168.125.1

4.2 AP Management

Note

- To manage the downlink AP, enable self-organizing network (SON) discovery (see section 4.2.1 Switching the Working Mode). 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 Reyee 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.

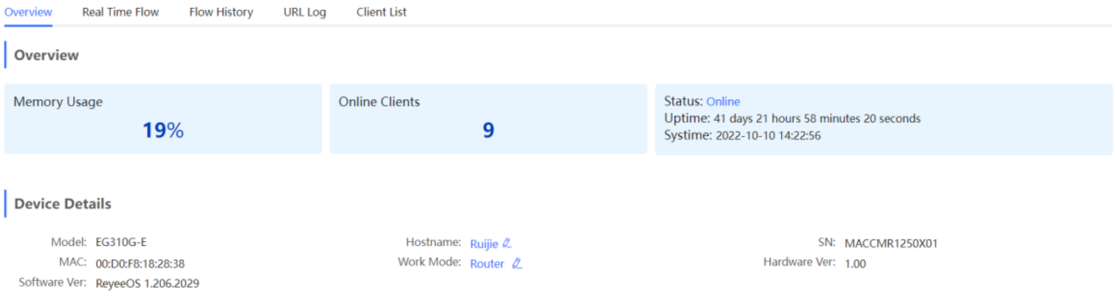
3. Configuration Steps

Choose **Local Device > Device Overview > Device Overview**.

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.



Overview

Memory Usage 19%

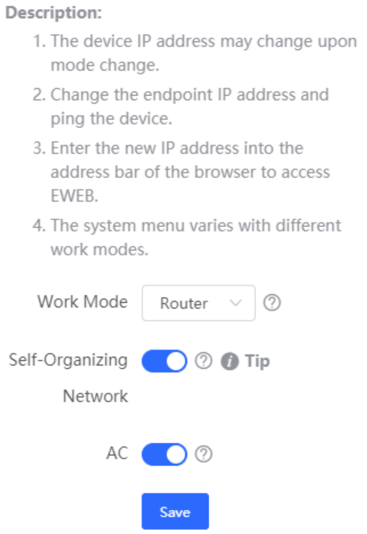
Online Clients 9

Status: Online
Uptime: 41 days 21 hours 58 minutes 20 seconds
Systime: 2022-10-10 14:22:56

Device Details

Model: EG310G-E
MAC: 00:D0:F8:18:28:38
Software Ver: ReyeeOS 1.206.2029
Hostname: Ruijie
Work Mode: Router
SN: MACCMR1250X01
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: Router

Self-Organizing Network: ●

AC: ●

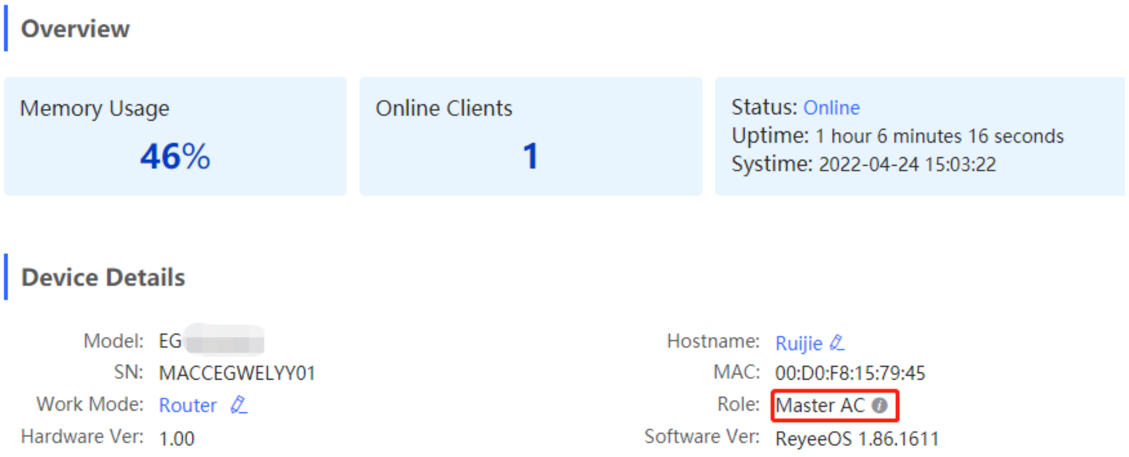
4. Viewing the Self-Organizing Role

Choose **Local Device > Device Overview > Device Overview**.

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	Online Clients	Status: Online Uptime: 1 hour 6 minutes 16 seconds Systime: 2022-04-24 15:03:22
46%	1	

Device Details

Model: EG[redacted]
SN: MACCEGWELYY01
Work Mode: Router
Hardware Ver: 1.00

Hostname: Ruijie
MAC: 00:D0:F8:15:79:45
Role: Master AC
Software Ver: ReyeeOS 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.

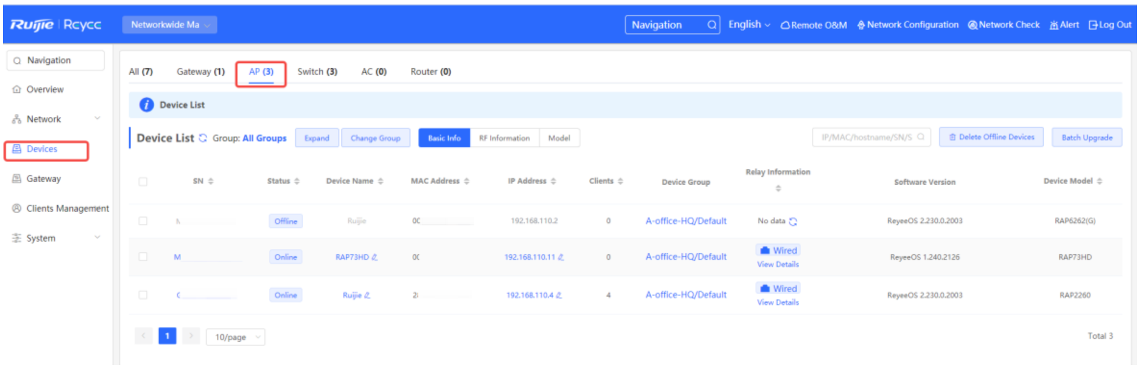
Note

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.

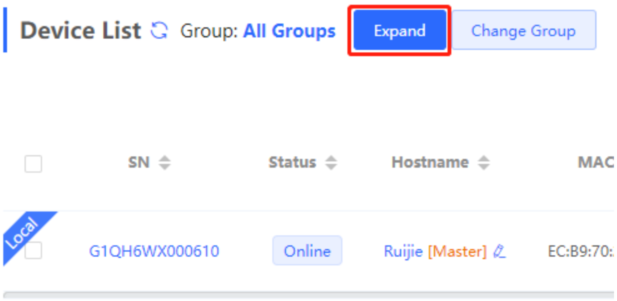


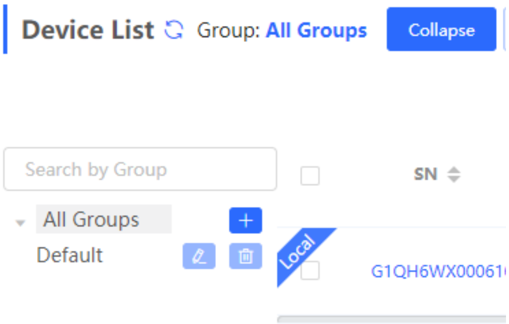
Device List Group: All Groups

□	SN	Status	Device Name	MAC Address	IP Address	Clients	Device Group	Relay Information	Software Version	Device Model
□	[redacted]	Offline	Ruijie	[redacted]	192.168.110.2	0	A-office-HQ/Default	No data	ReyeeOS 2.230.0.2003	RAP6262(G)
□	[redacted]	Online	RAP73HD	[redacted]	192.168.110.11	0	A-office-HQ/Default	Wired View Details	ReyeeOS 1.240.2126	RAP73HD
□	[redacted]	Online	Ruijie	[redacted]	192.168.110.4	4	A-office-HQ/Default	Wired View Details	ReyeeOS 2.230.0.2003	RAP2260

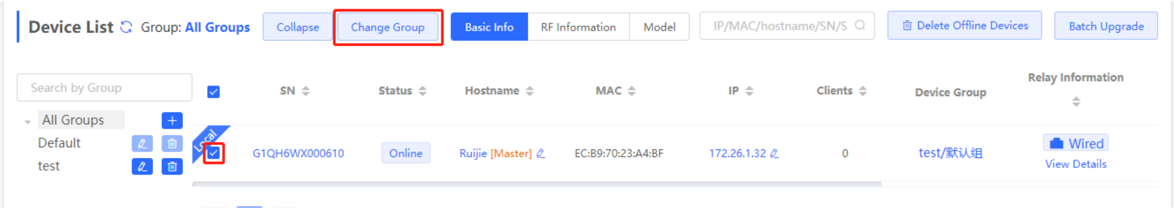
1 10/page Total 3

(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.

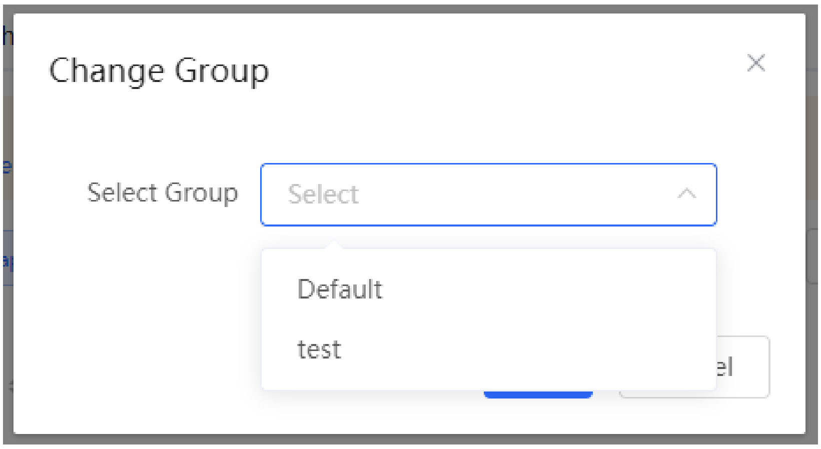




(3) Click a group name in the left. All devices in the group are displayed. One device can belong to only one group. By default, all devices belong to the default group. Select a device from the device list and click **Change Group** to migrate the selected device to the specified group. After a device 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.



☑	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information
☑	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:23:A4:BF	172.26.1.32	0	test/默认组	Wired View Details



4.2.3 Configuring Wi-Fi

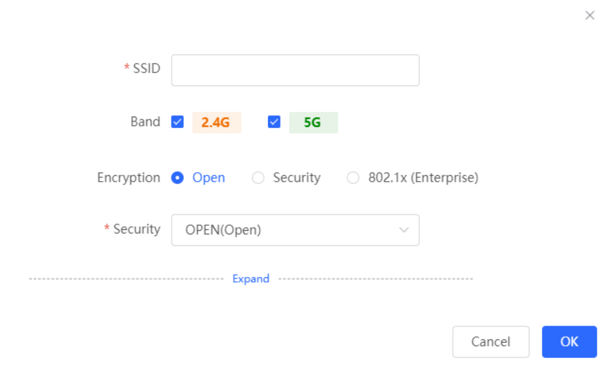
Switch to the **Network** mode. Choose **Network** > **Wi-Fi** > **Wi-Fi Settings**.

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

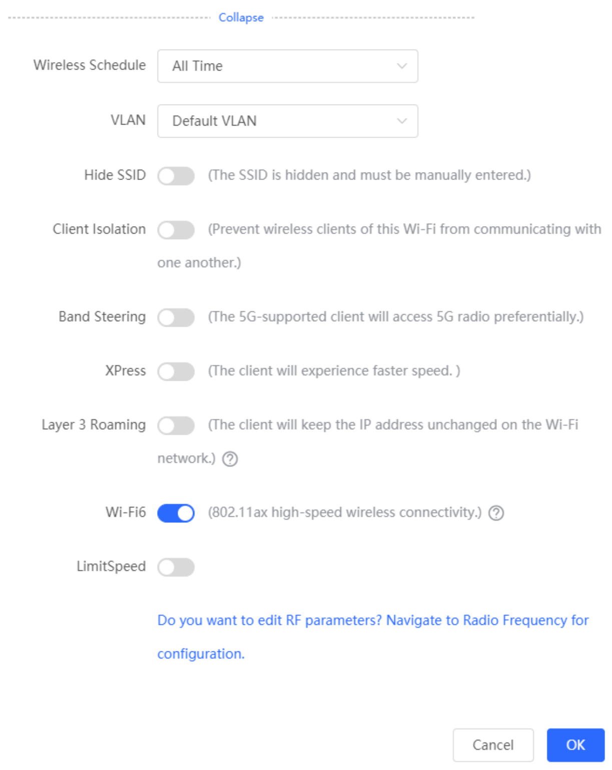
Click **Expand** to configure Wi-Fi parameters.

Caution

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



- * SSID
- Band ☑ 2.4G ☑ 5G
- Encryption ● Open ○ Security ○ 802.1x (Enterprise)
- * Security OPEN(Open)



- 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 the IP address unchanged on the Wi-Fi network.)
- Wi-Fi6 (802.11ax high-speed wireless connectivity.)
- LimitSpeed

Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.

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.

Parameter	Description
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.
Security	Select an encryption mode for wireless network connections. The options are as follows: ● 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.
Effective Time	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.

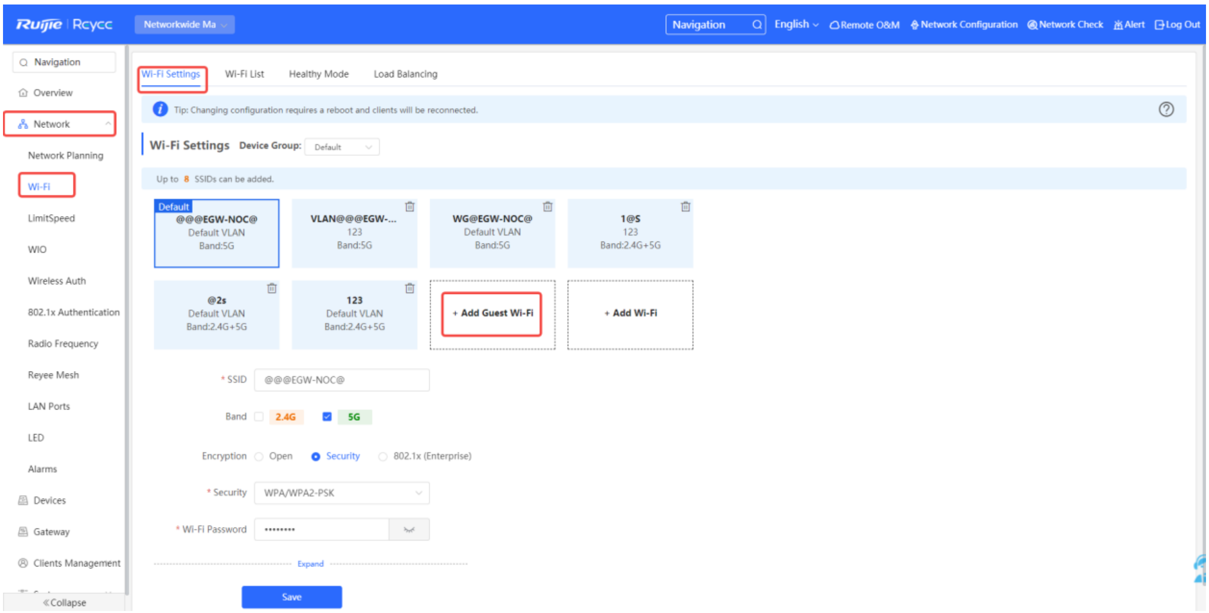
Parameter	Description
Layer-3 Roaming	Layer 3 roaming enables clients to keep their IP addresses unchanged when the clients are associated with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
802.11r	After this feature is enabled, roaming time is reduced to achieve fast transition. If a STA used is not compliant with IEEE 802.11r, the STA may fail to access the Wi-Fi network.
Wi-Fi6	Wi-Fi 6 provides wireless users with faster network access speed and optimized network access experience. 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.

4.2.4 Configuring Guest Wi-Fi

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

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 **Expand** to configure the wireless schedule of guest Wi-Fi and more Wi-Fi parameters. For details, see section 4.2.3 Configuring Wi-Fi. Click **Save**. Guests can access the Internet through Wi-Fi after entering the SSID and password.



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

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

Default @@@EGW-NOC@ Default VLAN Band:5G

VLAN@@@EGW-... 123 Band:5G

WG@EGW-NOC@ Default VLAN Band:5G

1@S 123 Band:2.4G+5G

@2s Default VLAN Band:2.4G+5G

123 Default VLAN Band:2.4G+5G

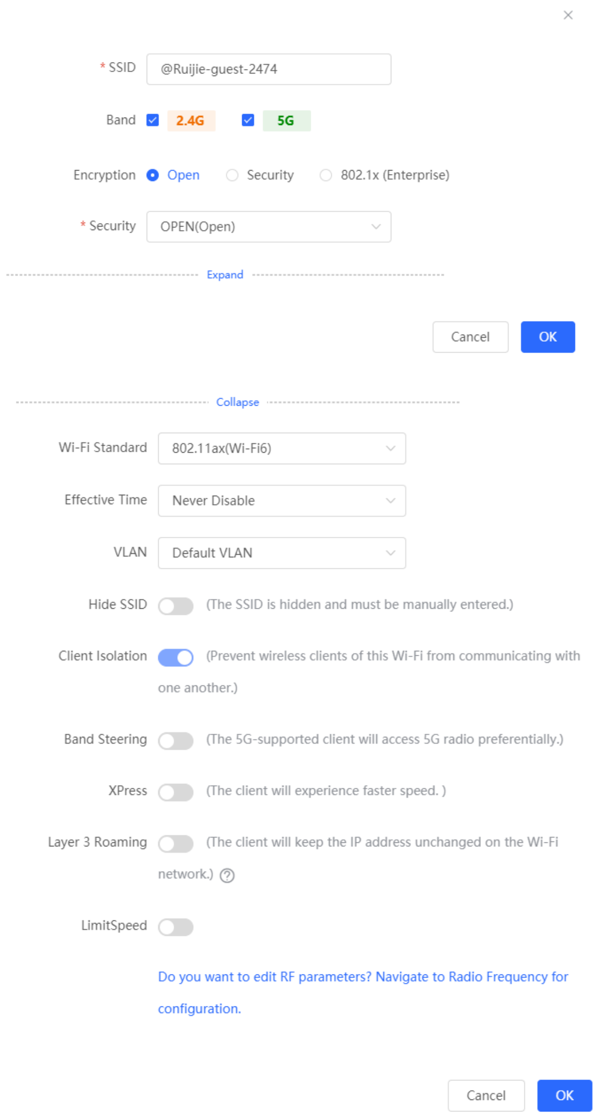
* SSID @@@EGW-NOC@

Band □ 2.4G ☑ 5G

Encryption ○ Open ● Security ○ 802.1x (Enterprise)

* Security WPA/WPA2-PSK

* Wi-Fi Password ••••••••



* SSID: @Ruijie-guest-2474

Band: ☑ 2.4G ☑ 5G

Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(Open)

Wi-Fi Standard: 802.11ax(Wi-Fi6)

Effective Time: Never Disable

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 the IP address unchanged on the Wi-Fi network.)

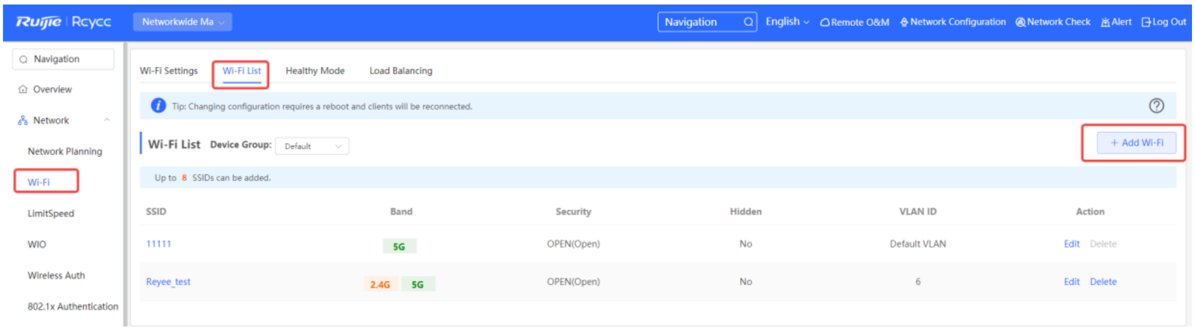
LimitSpeed

Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.

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 Wi-Fi**, enter the SSID and password, and click **OK** to create a Wi-Fi network. Click **Expand** to configure more Wi-Fi parameters. For details, see section 4.2.3 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.

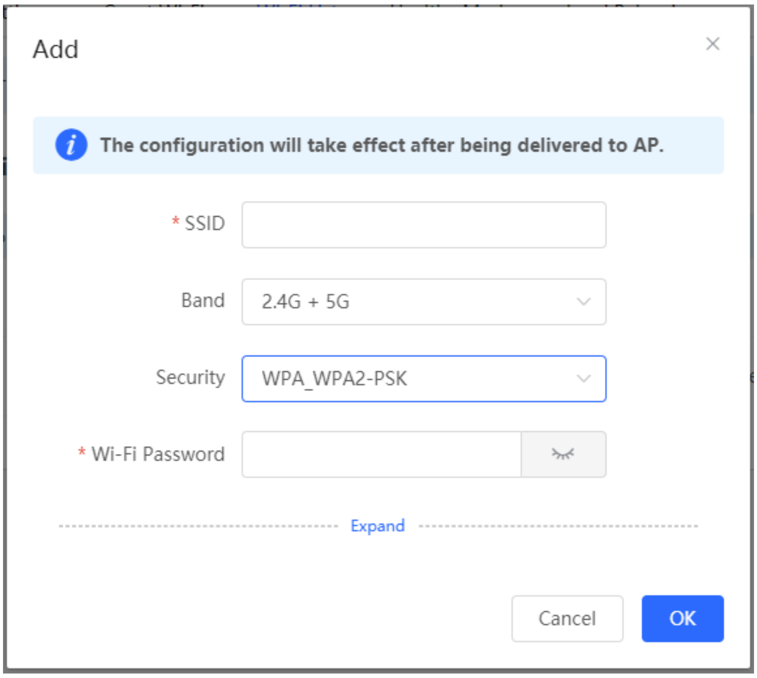


Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
11111	5G	OPEN(Open)	No	Default VLAN	Edit Delete
Reyee_test	2.4G 5G	OPEN(Open)	No	6	Edit Delete



Add

The configuration will take effect after being delivered to AP.

* SSID

Band: 2.4G + 5G

Security: WPA_WPA2-PSK

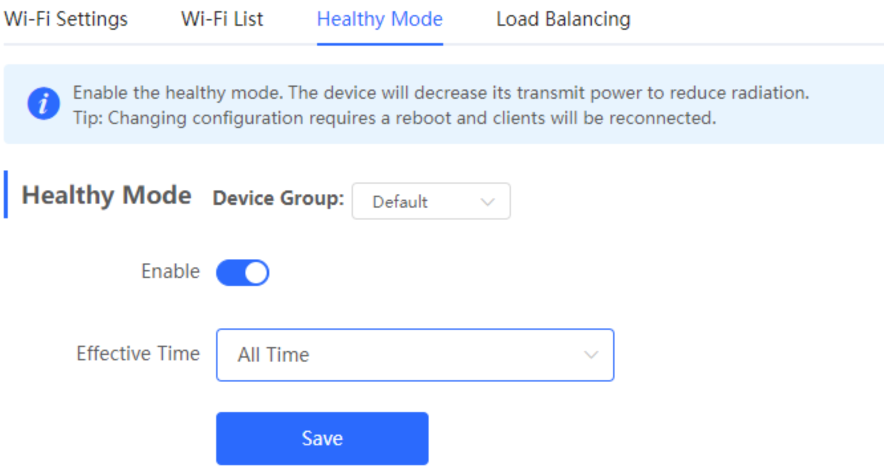
* Wi-Fi Password

4.2.6 Healthy Mode

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

Enable the healthy mode and select the effective time 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.



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

Healthy Mode Device Group: Default

Enable: on

Effective Time: All Time

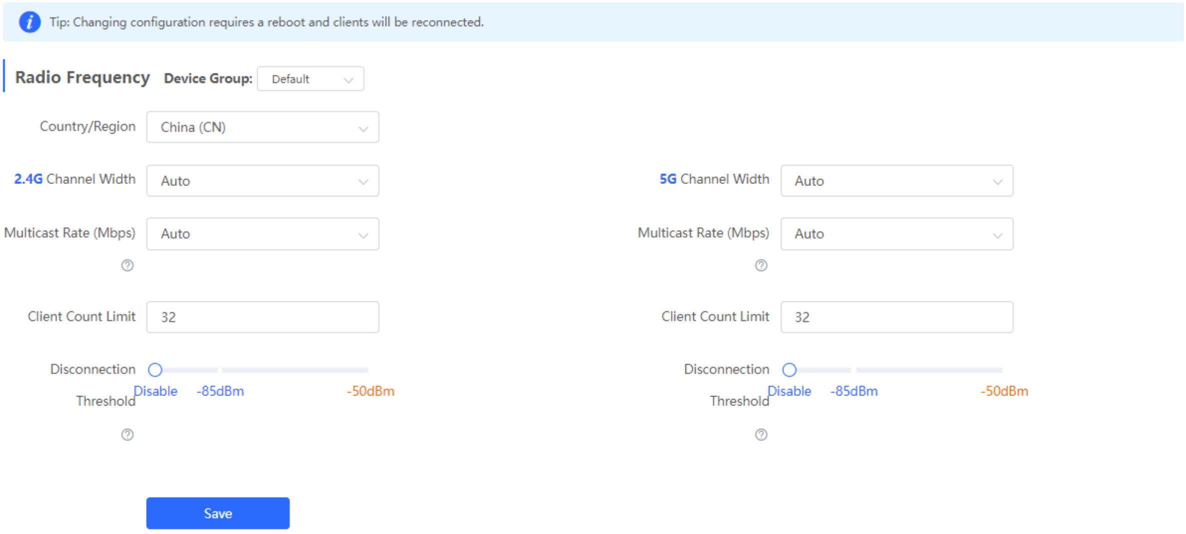
4.2.7 RF Settings

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.



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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

Multicast Rate (Mbps): Auto

Client Count Limit: 32

Disconnection Threshold: Disable -85dBm -50dBm

5G Channel Width: Auto

Multicast Rate (Mbps): Auto

Client Count Limit: 32

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.
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.

Parameter	Description
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 Blocklist or Allowlist

1. Overview

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

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

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

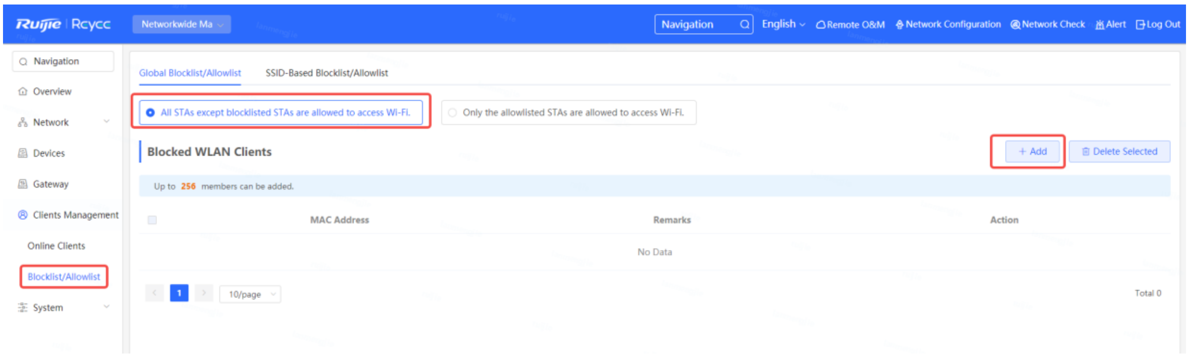
Caution

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

2. Configuring a Global Blocklist or Allowlist

Switch to the Network mode. Choose **Clients Management > Blocklist/Allowlist > Global Blocklist/Allowlist**.

Select the blocklist or allowlist mode and click Add to add a client to the blocklist or allowlist. 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 blocklist are forced offline and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the router.



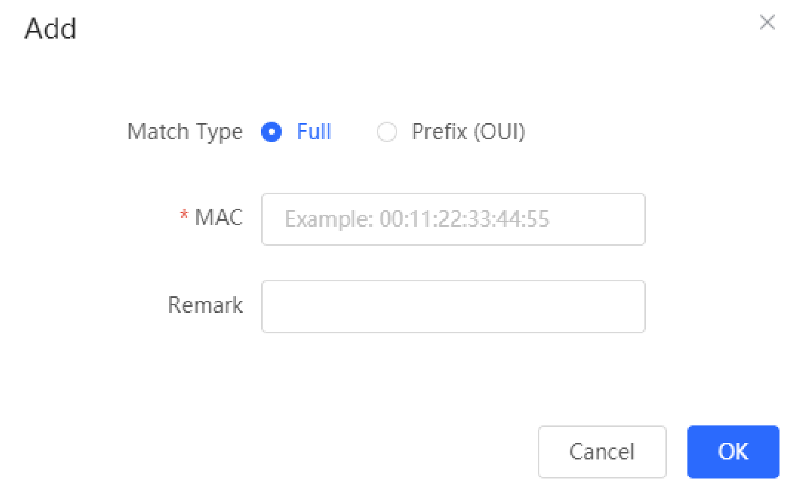
● All STAs except blocklisted STAs are allowed to access Wi-Fi. ○ Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 256 members can be added.

□	MAC Address	Remarks	Action
No Data			

Total 0



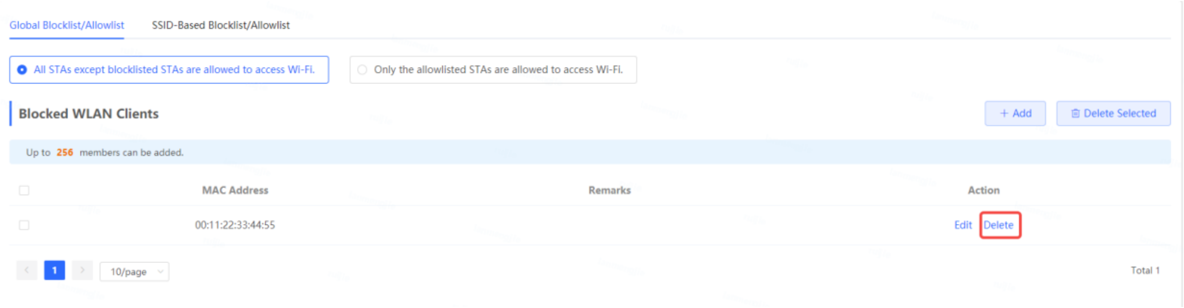
Add

Match Type ● Full ○ Prefix (OUI)

* MAC Example: 00:11:22:33:44:55

Remark

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



● All STAs except blocklisted STAs are allowed to access Wi-Fi. ○ Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 256 members can be added.

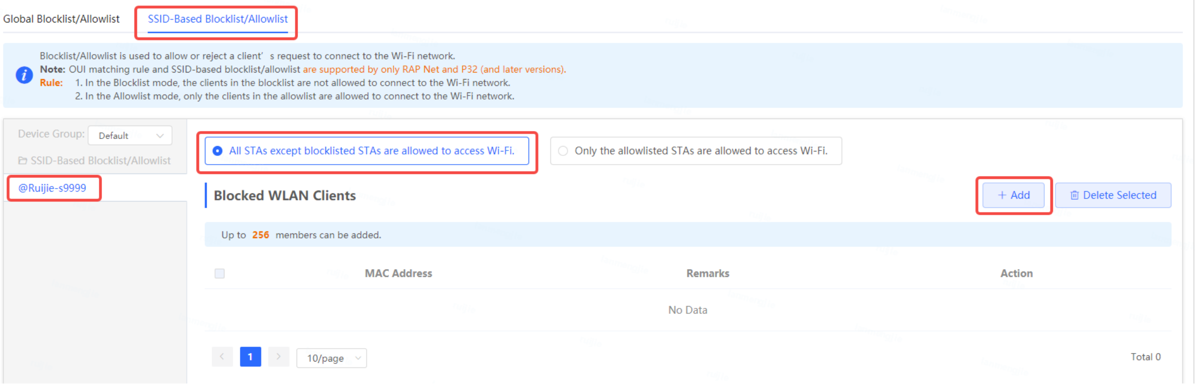
□	MAC Address	Remarks	Action
□	00:11:22:33:44:55		Edit Delete

Total 1

3. Configuring an SSID-based Blocklist or Allowlist

Switch to the Network mode. Choose **Clients Management > Blocklist/Allowlist > SSID-Based Blocklist/Allowlist**.

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



Global Blocklist/Allowlist
SSID-Based Blocklist/Allowlist
Device Group: Default
SSID-Based Blocklist/Allowlist
@Ruijie-s9999
+ Add
Delete Selected
10/page
Total 0

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

● All STAs except blocklisted STAs are allowed to access Wi-Fi. ○ Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 256 members can be added.

□	MAC Address	Remarks	Action
		No Data	

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:

- **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.
- **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.

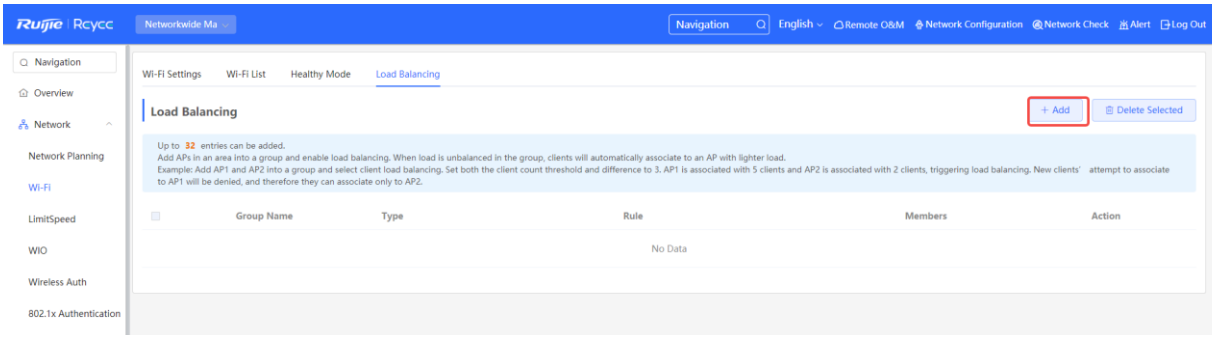
Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with five clients and AP2 is associated with two clients, triggering load balancing. New clients' attempt to associate with AP1 will be denied, so they can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

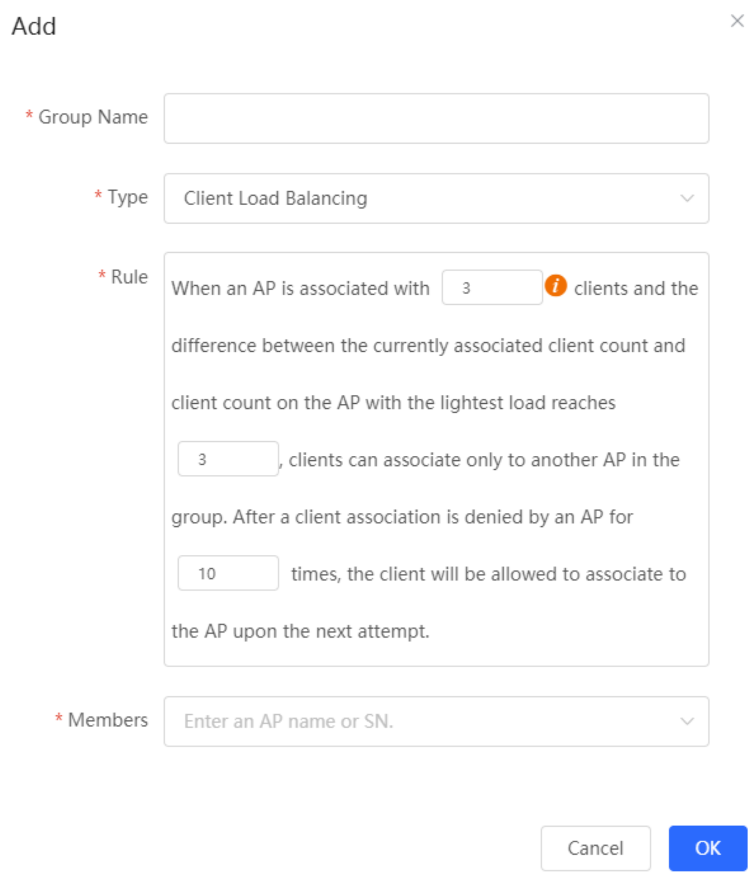
Click **Add**. In the dialog box that appears, set **Type** to **Client Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.



Load Balancing

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

□	Group Name	Type	Rule	Members	Action
			No Data		



Add

* Group Name

* Type: Client Load Balancing

* Rule: When an AP is associated with 3 clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches 3, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.

* Members: Enter an AP name or SN.

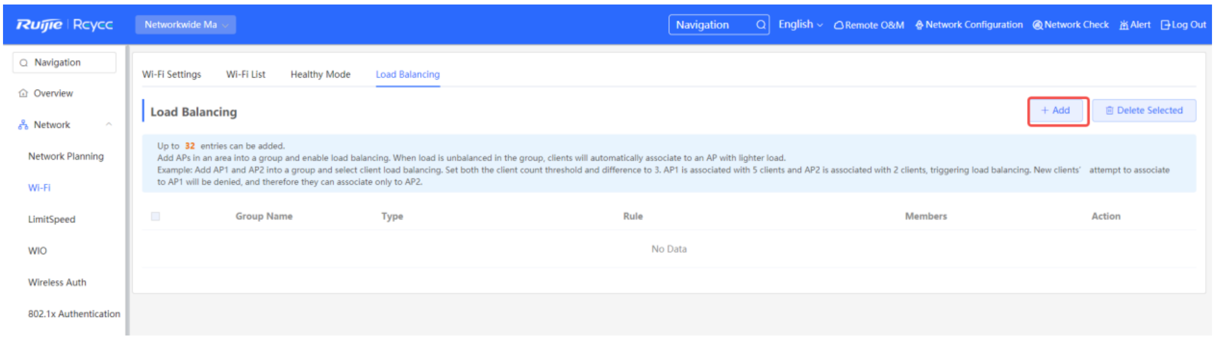
Table 4-3 **Client Load Balancing Configuration**

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

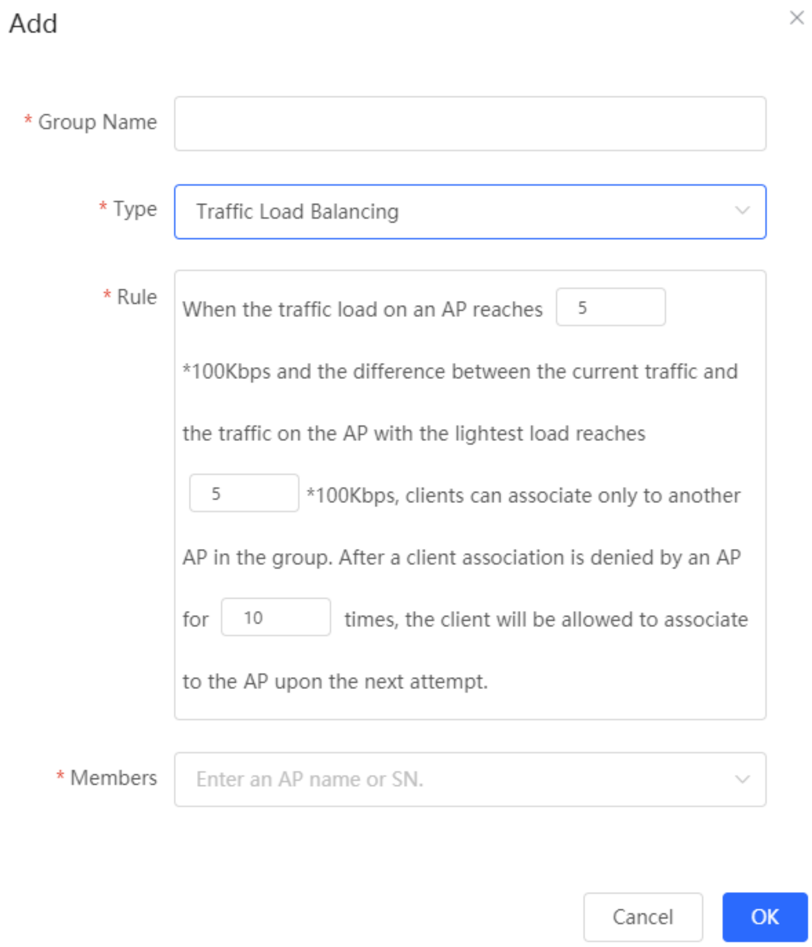
Click **Add**. In the dialog box that appears, set **Type** to **Traffic Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.



Load Balancing

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

☐	Group Name	Type	Rule	Members	Action
No Data					



Add

* Group Name

* Type: Traffic Load Balancing

* Rule: When the traffic load on an AP reaches 5 *100Kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches 5 *100Kbps, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.

* Members: Enter an AP name or SN.

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**.

Parameter	Description
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 kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches 500 kbps, 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 One-Click Wireless Optimization

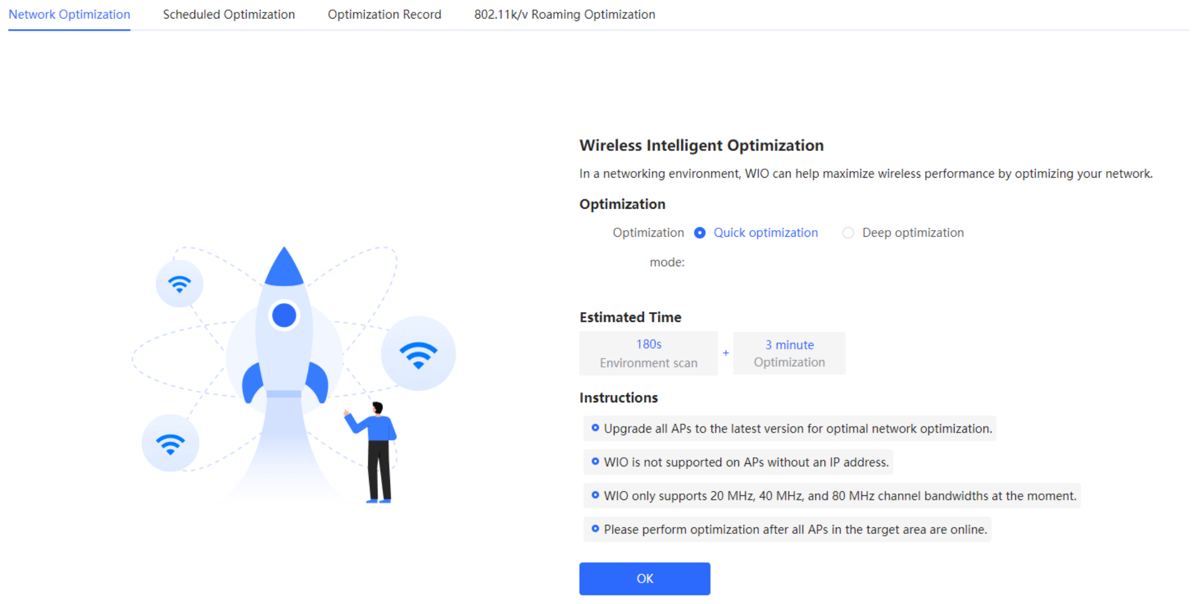
Select the optimization mode, the system automatically optimize the wireless network.

Caution

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

Choose **Network** > **WIO** >> **Network Optimization**.

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



Wireless Intelligent Optimization

In a networking environment, WIO can help maximize wireless performance by optimizing your network.

Optimization

Optimization mode: ● Quick optimization ○ Deep optimization

Estimated Time

180s Environment scan + 3 minute Optimization

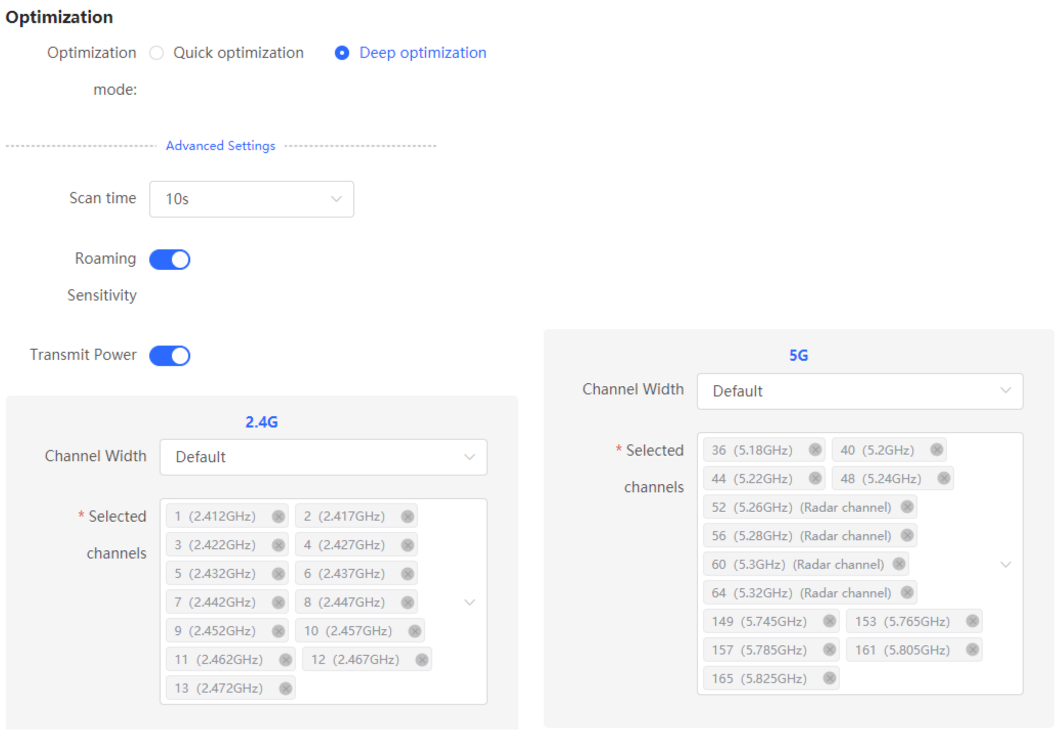
Instructions

- Upgrade all APs to the latest version for optimal network optimization.
- WIO is not supported on APs without an IP address.
- WIO only supports 20 MHz, 40 MHz, and 80 MHz channel bandwidths at the moment.
- Please perform optimization after all APs in the target area are online.

Table 4-5 Description of Tuning Mode

Parameter	Description
Quick optimization	In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power.
Deep optimization	In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand Advanced Settings to configure the scanning time, channel bandwidth and channels. Scanning time: Indicates the time for scanning channels during the optimization. 2.4G Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. Selected channels: Indicates the channels to be optimized. 5G Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. Selected channels: Indicates the channels to be optimized.

When the **Optimization Mode** is configured as **Deep optimization**, expand the **Advanced Settings** to set the scanning time, channel bandwidth and selected channels.



Optimization

Optimization mode: ○ Quick optimization ● Deep optimization

Advanced Settings

Scan time: 10s

Roaming Sensitivity: on

Transmit Power: on

2.4G

Channel Width: Default

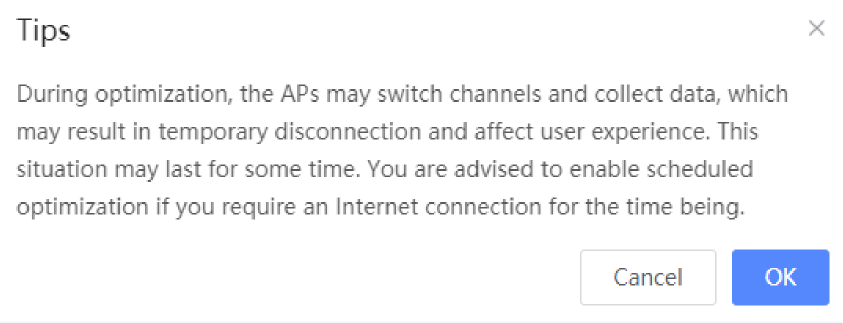
* Selected channels: 1 (2.412GHz), 2 (2.417GHz), 3 (2.422GHz), 4 (2.427GHz), 5 (2.432GHz), 6 (2.437GHz), 7 (2.442GHz), 8 (2.447GHz), 9 (2.452GHz), 10 (2.457GHz), 11 (2.462GHz), 12 (2.467GHz), 13 (2.472GHz)

5G

Channel Width: Default

* Selected channels: 36 (5.18GHz), 40 (5.2GHz), 44 (5.22GHz), 48 (5.24GHz), 52 (5.26GHz) (Radar channel), 56 (5.28GHz) (Radar channel), 60 (5.3GHz) (Radar channel), 64 (5.32GHz) (Radar channel), 149 (5.745GHz), 153 (5.765GHz), 157 (5.785GHz), 161 (5.805GHz), 165 (5.825GHz)

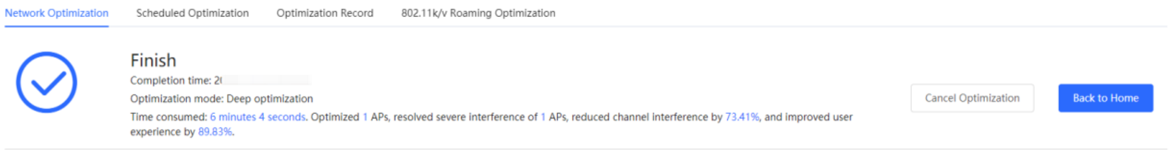
(2) Confirm the tips, and Click **OK**.



Tips

During optimization, the APs may switch channels and collect data, which may result in temporary disconnection and affect user experience. This situation may last for some time. You are advised to enable scheduled optimization if you require an Internet connection for the time being.

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



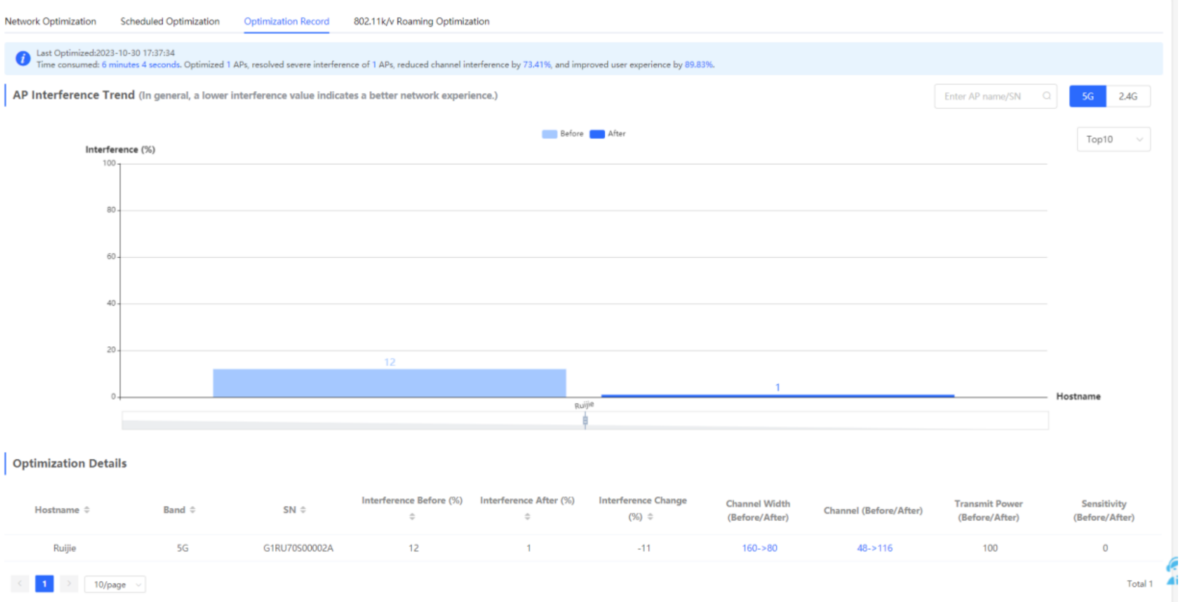
Finish

Completion time: 2(

Optimization mode: Deep optimization

Time consumed: 6 minutes 4 seconds. Optimized 1 APs, resolved severe interference of 1 APs, reduced channel interference by 73.41%, and improved user experience by 89.83%.

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



Last Optimized:2023-10-30 17:37:34
Time consumed: 6 minutes 4 seconds. Optimized 1 APs, resolved severe interference of 1 APs, reduced channel interference by 73.41%, and improved user experience by 89.83%.

AP Interference Trend (In general, a lower interference value indicates a better network experience.)

Optimization Details

Hostname	Band	SN	Interference Before (%)	Interference After (%)	Interference Change (%)	Channel Width (Before/After)	Channel (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)
Ruijie	5G	G1RU70S00002A	12	1	-11	160->80	48->116	100	0

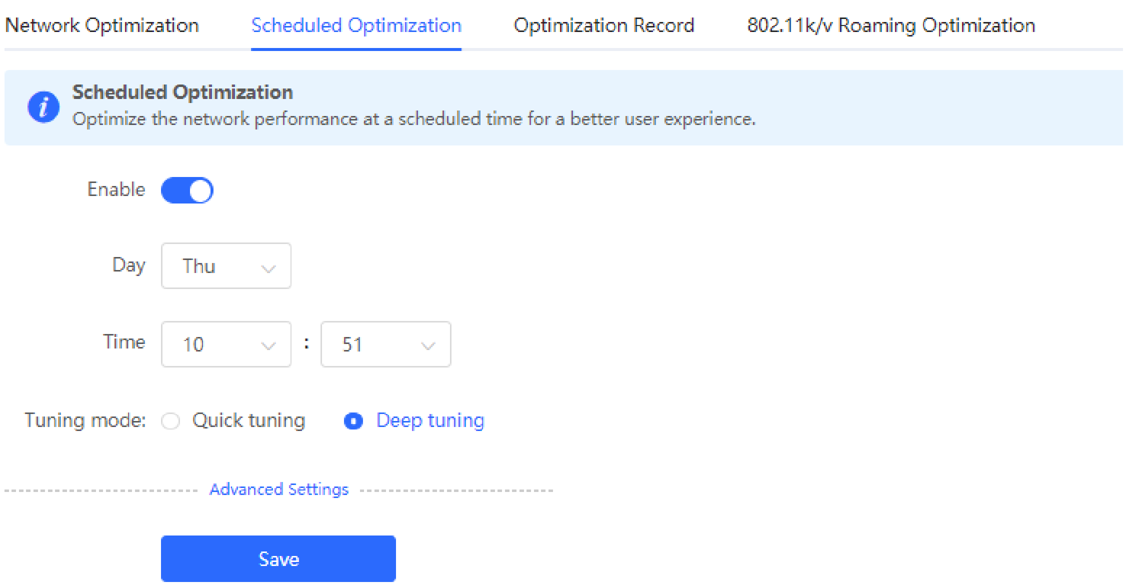
4.2.11 Scheduled Wireless Optimization

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 the idle periods.

⚠ **Caution**

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

Choose **Network** > **WIO >> Scheduled Optimization**.



Scheduled Optimization

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

Enable: ●

Day: Thu

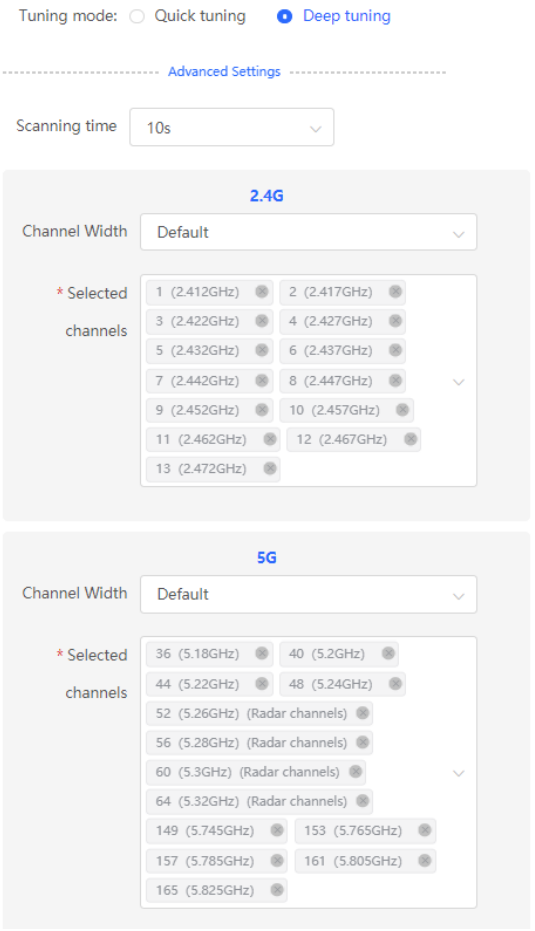
Time: 10 : 51

Tuning mode: ○ Quick tuning ● Deep tuning

(1) Configure the scheduled time.

(2) Select the optimization mode.

(3) (Optional) When the Tuning Mode is configured as Deep optimization, expand the Advanced Settings to set the scanning time, channel bandwidth and selected channels.


Tuning mode: ○ Quick tuning ● Deep tuning

Scanning time: 10s

2.4G

Channel Width: Default

* Selected channels: 1 (2.412GHz), 2 (2.417GHz), 3 (2.422GHz), 4 (2.427GHz), 5 (2.432GHz), 6 (2.437GHz), 7 (2.442GHz), 8 (2.447GHz), 9 (2.452GHz), 10 (2.457GHz), 11 (2.462GHz), 12 (2.467GHz), 13 (2.472GHz)

5G

Channel Width: Default

* Selected channels: 36 (5.18GHz), 40 (5.2GHz), 44 (5.22GHz), 48 (5.24GHz), 52 (5.26GHz) (Radar channels), 56 (5.28GHz) (Radar channels), 60 (5.3GHz) (Radar channels), 64 (5.32GHz) (Radar channels), 149 (5.745GHz), 153 (5.765GHz), 157 (5.785GHz), 161 (5.805GHz), 165 (5.825GHz)

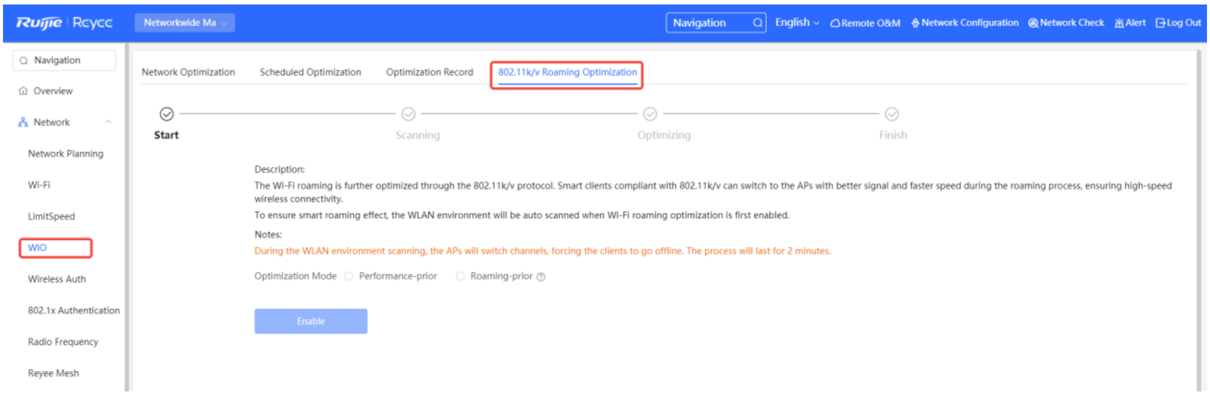
(4) Click **Save**.

4.2.12 Wi-Fi Roaming Optimization (802.11k/v)

Wi-Fi roaming is further optimized through the 802.11k/802.11v protocol. Smart endpoints compliant with IEEE 802.11k/v can switch association to the access points with better signal and faster speed, thereby ensuring high-speed wireless connectivity.

To ensure high quality of smart roaming service, the WLAN environment will be automatically scanned when Wi-Fi roaming optimization is first enabled.

Choose **Network** > **WIO** > **802.11k/v Roaming Optimization**.



Description:

The Wi-Fi roaming is further optimized through the 802.11k/v protocol. Smart clients compliant with 802.11k/v can switch to the APs with better signal and faster speed during the roaming process, ensuring high-speed wireless connectivity.

To ensure smart roaming effect, the WLAN environment will be auto scanned when Wi-Fi roaming optimization is first enabled.

Notes:

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

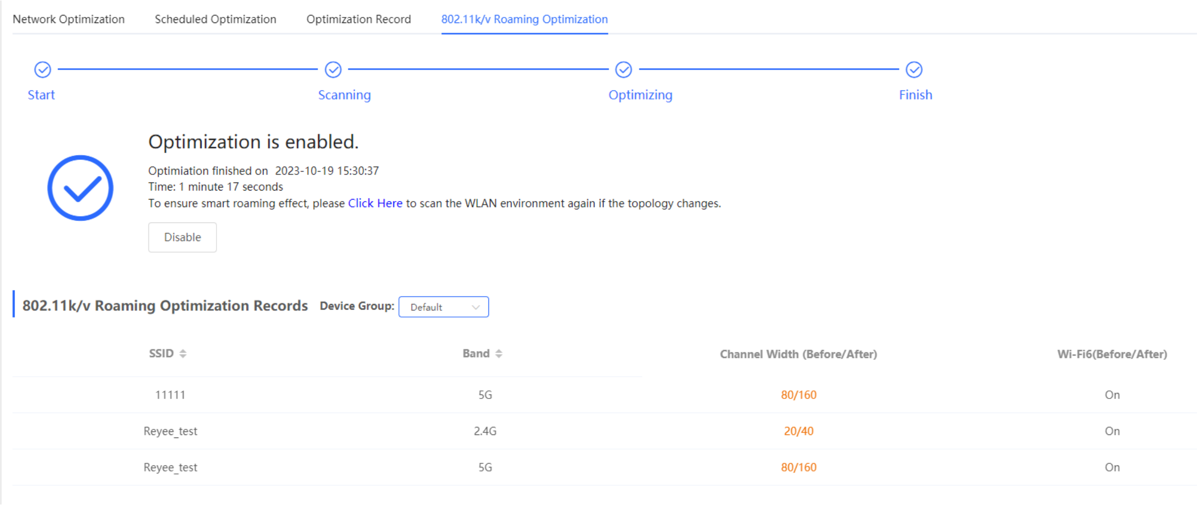
Optimization Mode ○ Performance-prior ○ Roaming-prior

Caution

During the optimization, the clients may be forced offline. Please proceed with caution.

Select **Optimization Mode**, and click **Enable** and the optimization starts.

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



Optimization is enabled.

Optimiation finished on 2023-10-19 15:30:37

Time: 1 minute 17 seconds

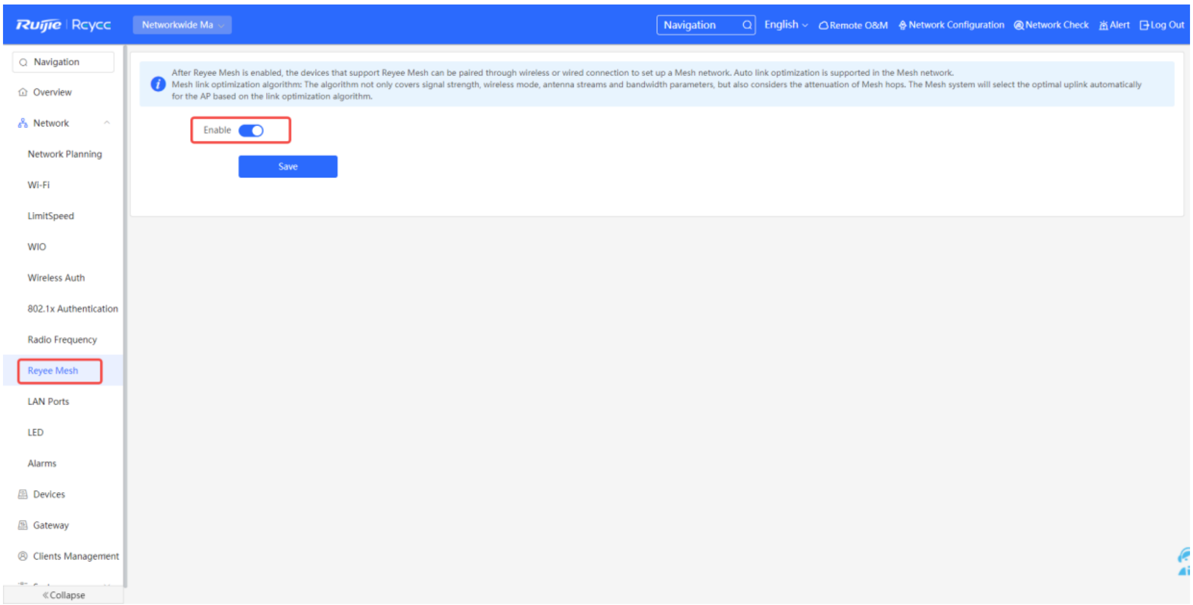
To ensure smart roaming effect, please Click Here to scan the WLAN environment again if the topology changes.

802.11k/v Roaming Optimization Records Device Group: Default

SSID	Band	Channel Width (Before/After)	Wi-Fi6(Before/After)
11111	5G	80/160	On
Reyee_test	2.4G	20/40	On
Reyee_test	5G	80/160	On

4.2.13 Enabling Reyee Mesh

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



After Reyee Mesh is enabled, the devices that support Reyee Mesh can be paired through wireless or wired connection to set up a Mesh network. Auto link optimization is supported in the Mesh network.
Mesh link optimization algorithm: The algorithm not only covers signal strength, wireless mode, antenna streams and bandwidth parameters, but also considers the attenuation of Mesh hops. The Mesh system will select the optimal uplink automatically for the AP based on the link optimization algorithm.

Enable: on

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

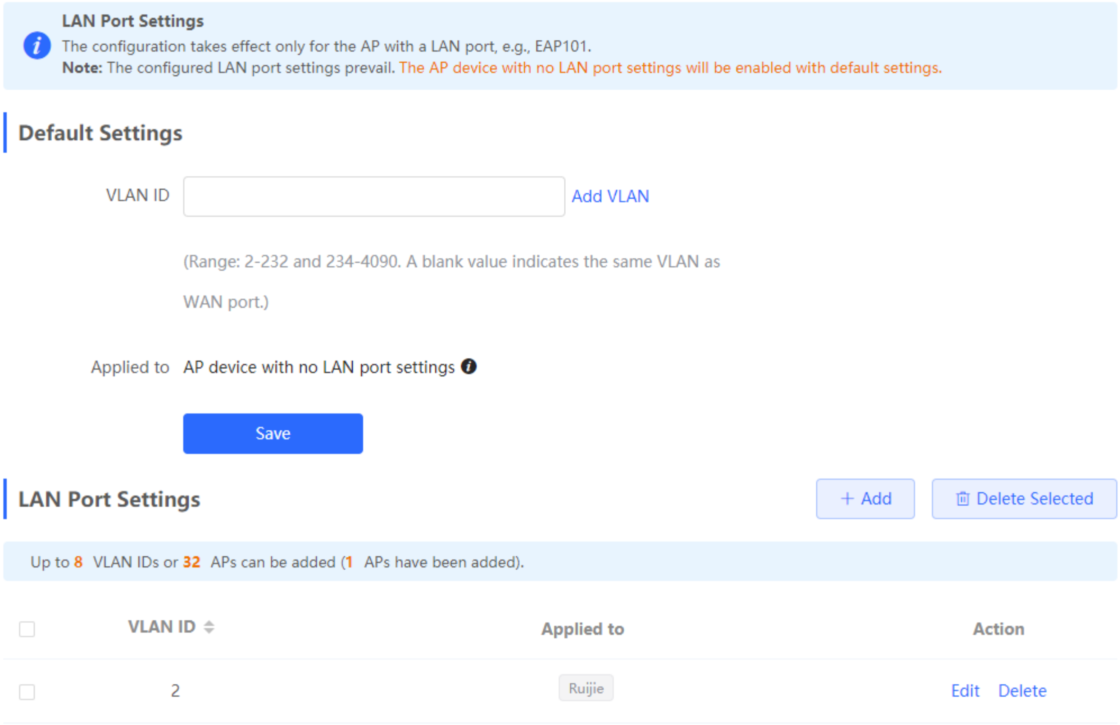
- Make sure that the new router is around the primary router and there are fewer obstacles between them.
- If three or more routers are added for mesh networking, repeat step 2 to 4. You can add eight devices in a batch at one time.

4.2.14 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

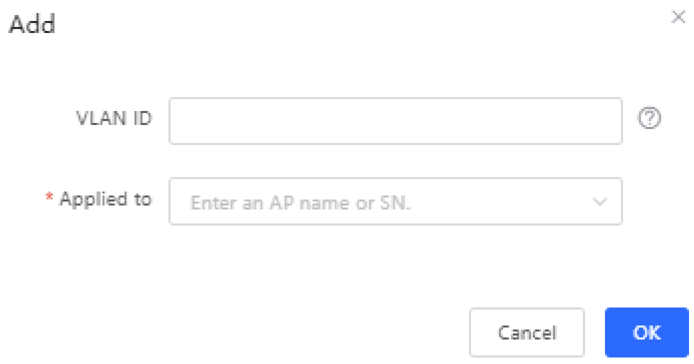
LAN Port Settings

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

□	VLAN ID	Applied to	Action
□	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:

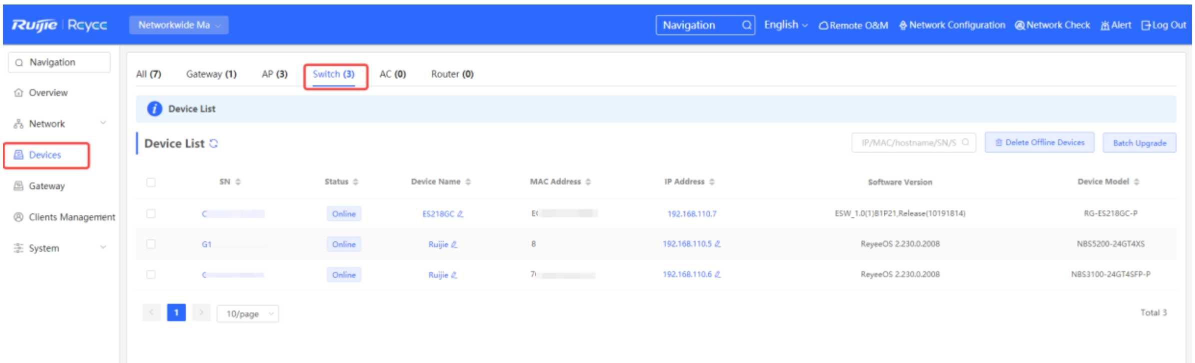
* Applied to: Enter an AP name or SN.

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

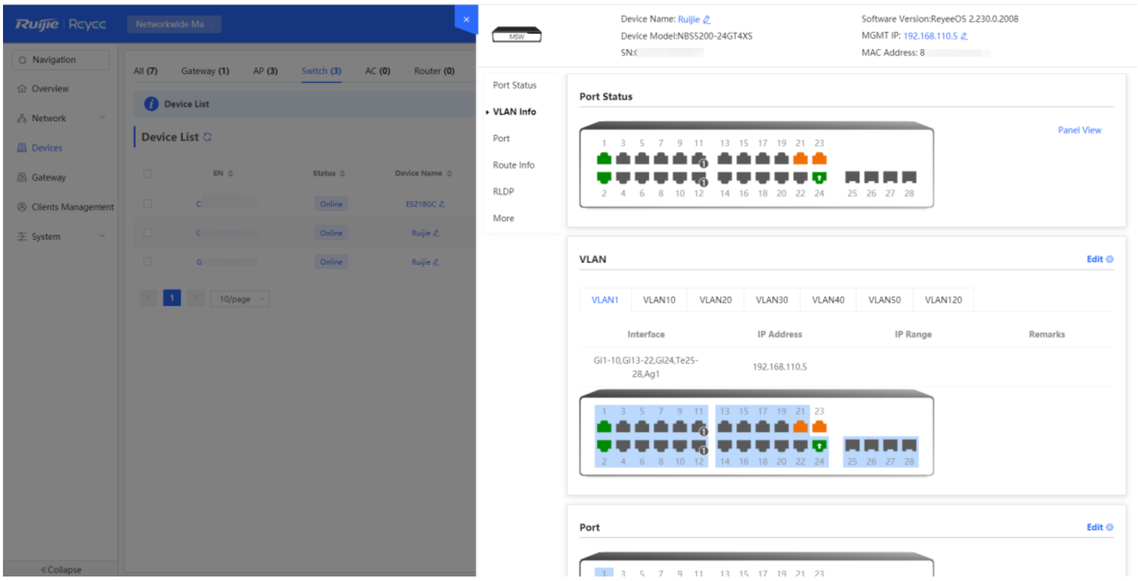
Switch List includes all switches that are managed by the router. The information includes the switch’s host name, IP address, MAC address, status, model, software version, and SN. You can check AP categories by clicking ⇕ .



Device List

SN	Status	Device Name	MAC Address	IP Address	Software Version	Device Model
C	Online	ES218GC	E(	192.168.110.7	ESW_1.0(1)B1P21,Release(10191814)	RG-ES218GC-P
G1	Online	Ruijie	8	192.168.110.5	ReyeeOS 2.230.0.2008	NBS5200-24GT4XS
C	Online	Ruijie	7	192.168.110.6	ReyeeOS 2.230.0.2008	NBS3100-24GT4SFP-P

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



Device Name: Ruijie
Device Model:NBS5200-24GT4XS
SN:(

Software Version:ReyeeOS 2.230.0.2008
MGMT IP: 192.168.110.5
MAC Address: 8

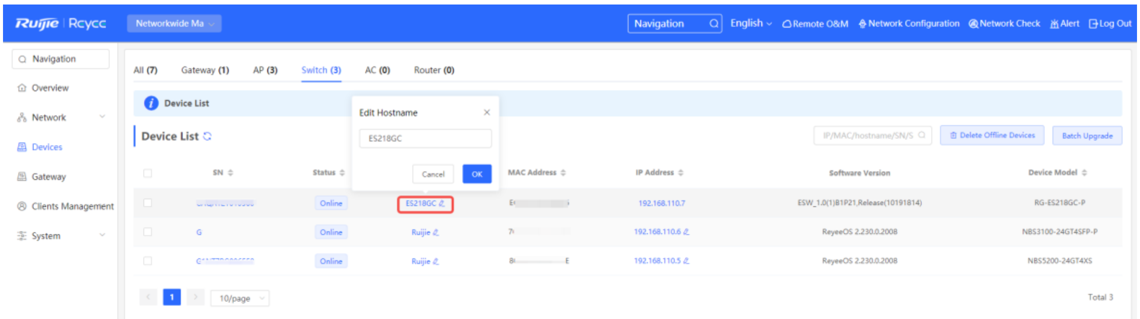
Port Status

VLAN

Interface	IP Address	IP Range	Remarks
Gi1-10,Gi13-22,Gi24,Te25-28,Ag1	192.168.110.5		

Port

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



Edit Hostname

ES218GC

Device List

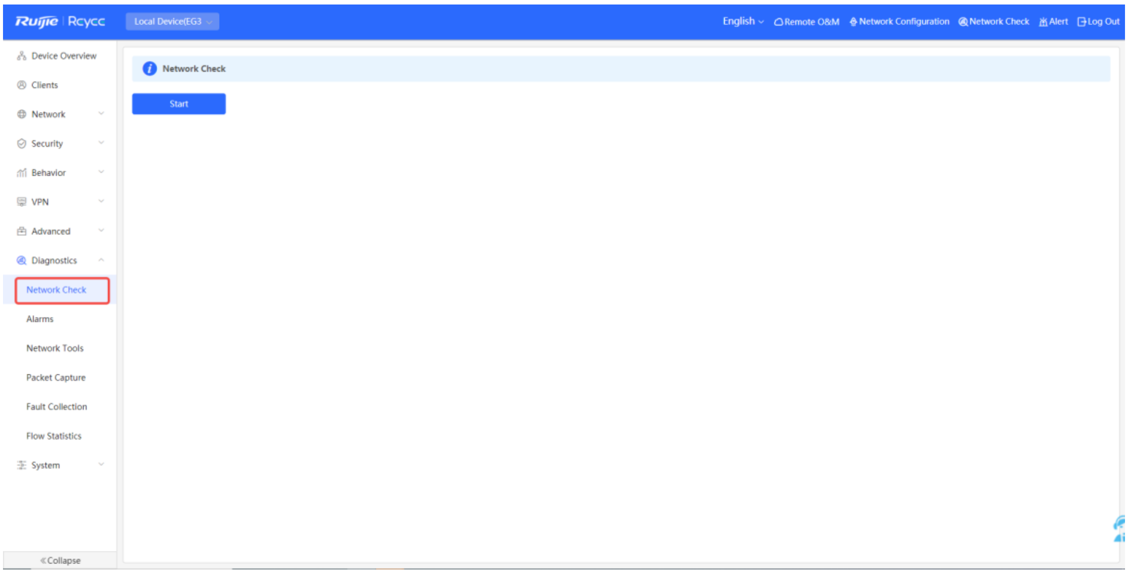
SN	Status	Device Name	MAC Address	IP Address	Software Version	Device Model
	Online	ES218GC	E(	192.168.110.7	ESW_1.0(1)B1P21,Release(10191814)	RG-ES218GC-P
G	Online	Ruijie	7	192.168.110.6	ReyeeOS 2.230.0.2008	NBS3100-24GT4SFP-P
G	Online	Ruijie	8 E	192.168.110.5	ReyeeOS 2.230.0.2008	NBS5200-24GT4XS

4.4 Diagnostics

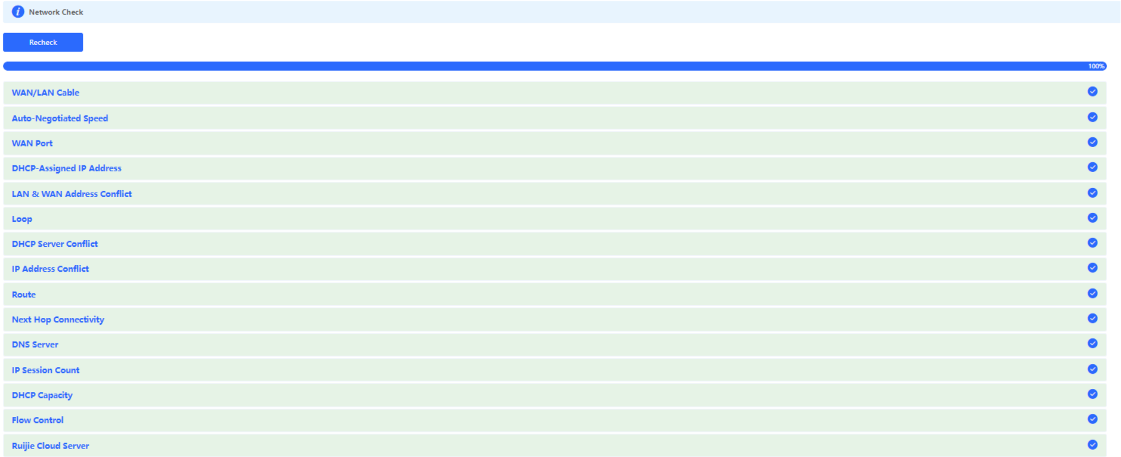
4.4.1 Network Check

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.

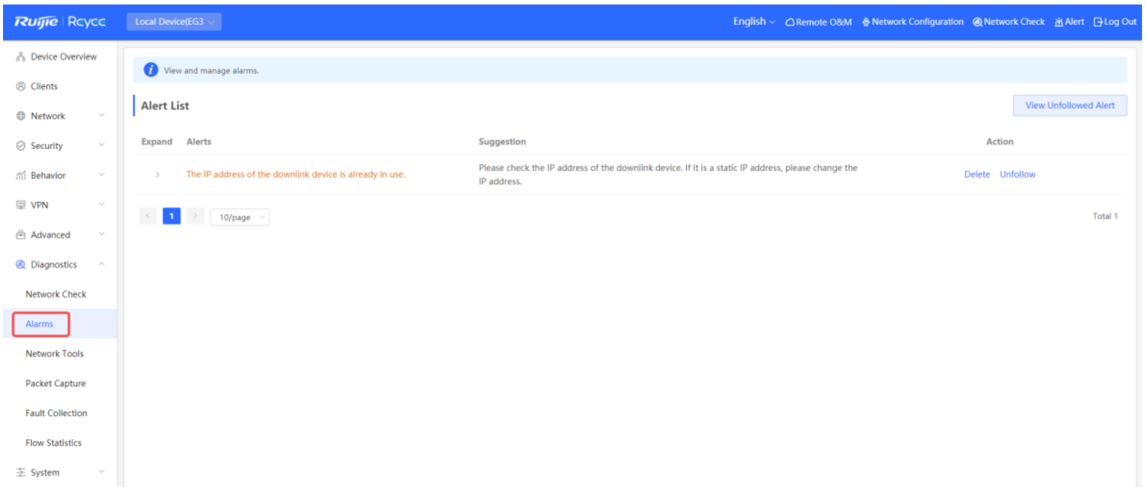


WAN/LAN Cable ✓
Auto-Negotiated Speed ✓
WAN Port ✓
DHCP-Assigned IP Address ✓
LAN & WAN Address Conflict ✓
Loop ✓
DHCP Server Conflict ✓
IP Address Conflict ✓
Route ✓
Next Hop Connectivity ✓
DNS Server ✓
IP Session Count ✓
DHCP Capacity ✓
Flow Control ✓
Ruijie Cloud Server ✓

4.4.2 Alarms

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

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



View and manage alarms.

Alert List

Expand	Alerts	Suggestion	Action
›	The IP address of the downlink device is already in use.	Please check the IP address of the downlink device. If it is a static IP address, please change the IP address.	Delete Unfollow

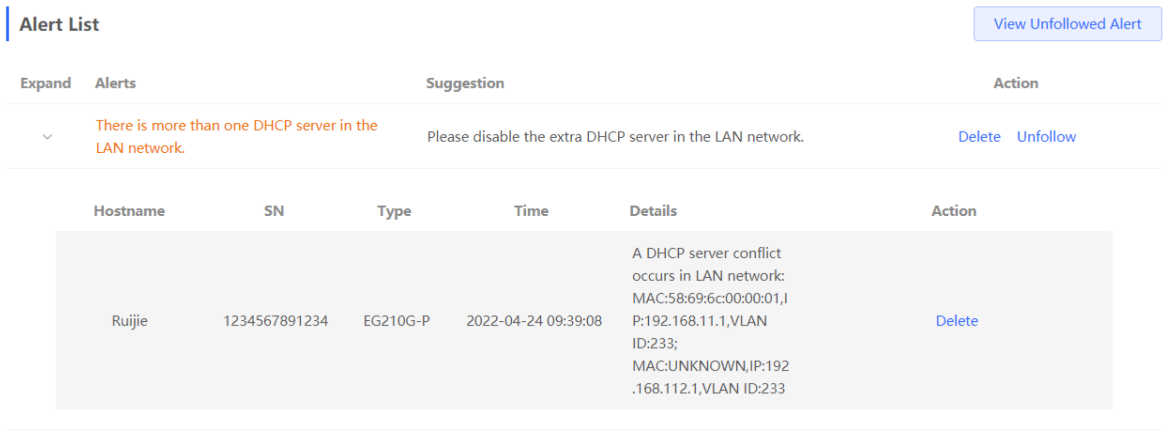
Total 1

(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.



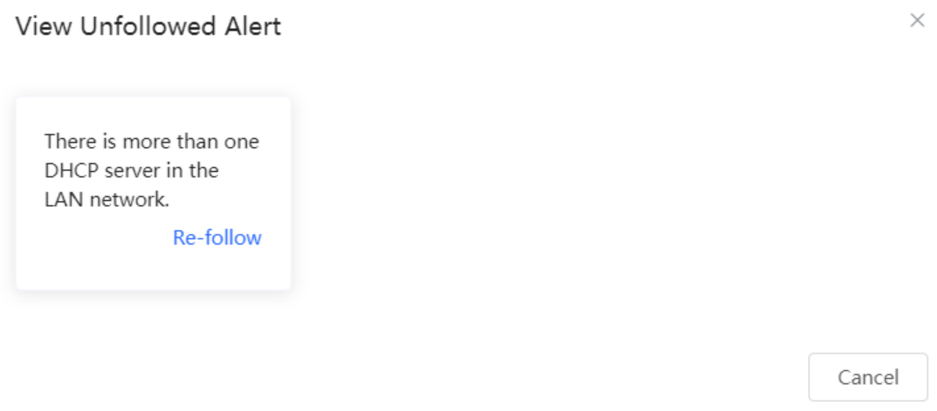
Alert List

View Unfollowed Alert

Expand	Alerts	Suggestion	Action
⌄	There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.	Delete Unfollow

Hostname	SN	Type	Time	Details	Action
Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,IP:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192.168.112.1,VLAN ID:233	Delete

(3) Click **View Unfollowed Alert** to view the unfollowed alarm. You can follow the alarm again in the pop-up window.

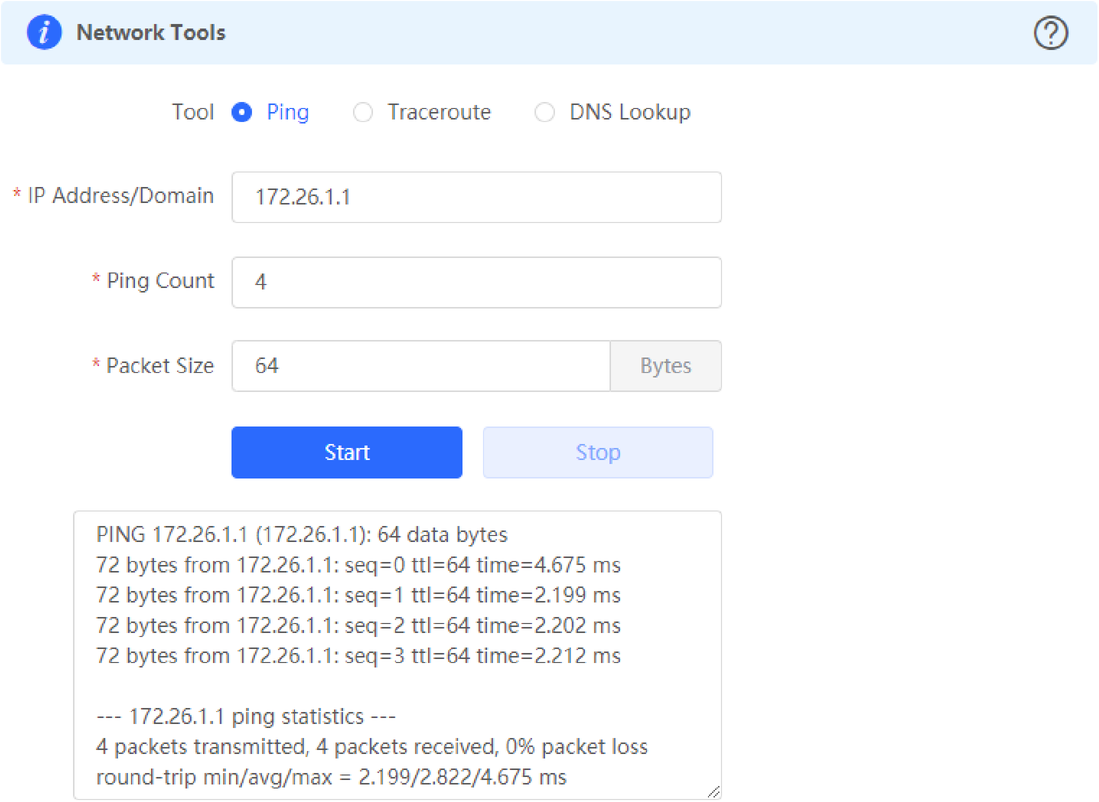


View Unfollowed Alert

There is more than one DHCP server in the LAN network.

4.4.3 Network Tools

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



Tool ● Ping ○ Traceroute ○ DNS Lookup

* IP Address/Domain: 172.26.1.1

* Ping Count: 4

* Packet Size: 64 Bytes

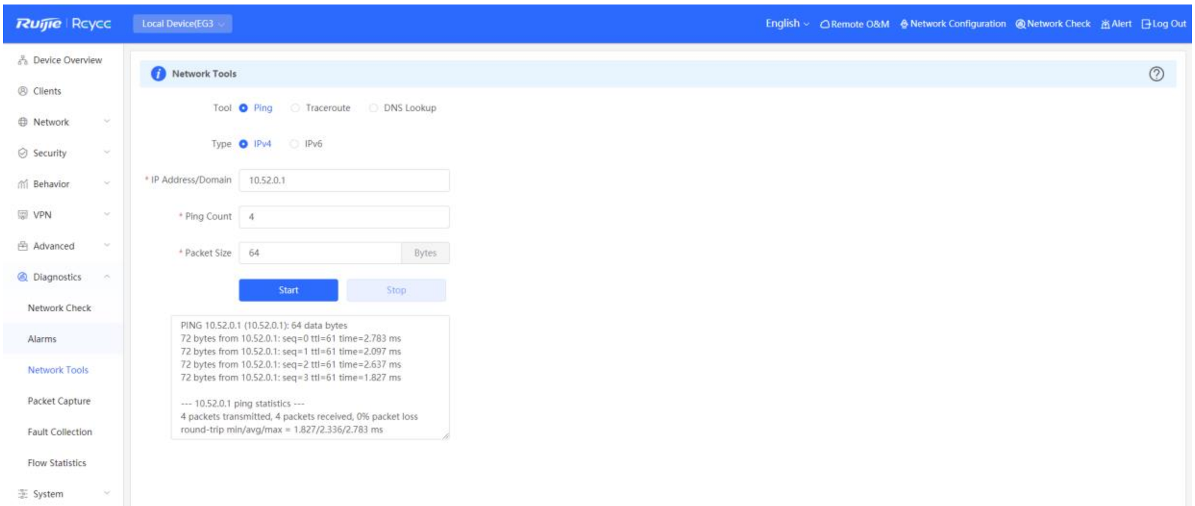
```
PING 172.26.1.1 (172.26.1.1): 64 data bytes
72 bytes from 172.26.1.1: seq=0 ttl=64 time=4.675 ms
72 bytes from 172.26.1.1: seq=1 ttl=64 time=2.199 ms
72 bytes from 172.26.1.1: seq=2 ttl=64 time=2.202 ms
72 bytes from 172.26.1.1: seq=3 ttl=64 time=2.212 ms

--- 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.



Tool ● Ping ○ Traceroute ○ DNS Lookup

Type ● IPv4 ○ IPv6

* IP Address/Domain: 10.52.0.1

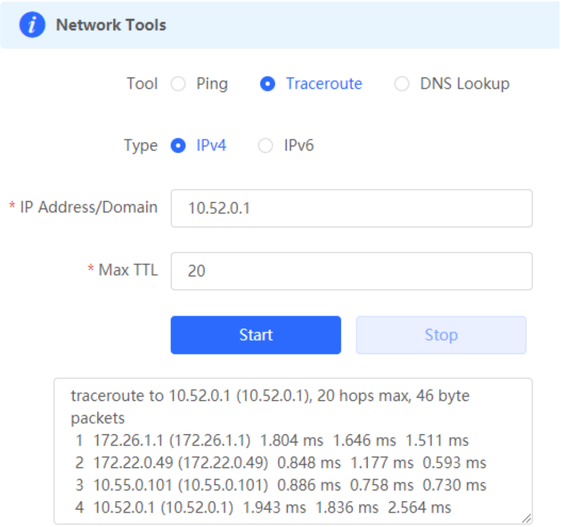
* Ping Count: 4

* Packet Size: 64 Bytes

```
PING 10.52.0.1 (10.52.0.1): 64 data bytes
72 bytes from 10.52.0.1: seq=0 ttl=61 time=2.783 ms
72 bytes from 10.52.0.1: seq=1 ttl=61 time=2.097 ms
72 bytes from 10.52.0.1: seq=2 ttl=61 time=2.637 ms
72 bytes from 10.52.0.1: seq=3 ttl=61 time=1.827 ms

--- 10.52.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.827/2.336/2.783 ms
```

2. Traceroute Tool

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



Tool ○ Ping ● Traceroute ○ DNS Lookup

Type ● IPv4 ○ IPv6

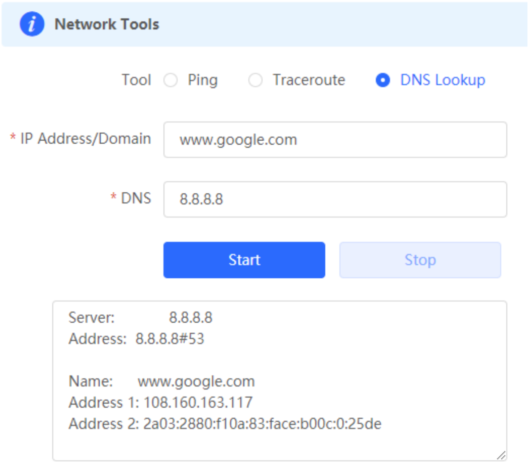
* IP Address/Domain: 10.52.0.1

* Max TTL: 20

```
traceroute to 10.52.0.1 (10.52.0.1), 20 hops max, 46 byte
packets
 1  172.26.1.1 (172.26.1.1)  1.804 ms  1.646 ms  1.511 ms
 2  172.22.0.49 (172.22.0.49)  0.848 ms  1.177 ms  0.593 ms
 3  10.55.0.101 (10.55.0.101)  0.886 ms  0.758 ms  0.730 ms
 4  10.52.0.1 (10.52.0.1)  1.943 ms  1.836 ms  2.564 ms
```

3. DNS Lookup Tool

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



Tool ○ Ping ○ Traceroute ● DNS Lookup

* IP Address/Domain: www.google.com

* DNS: 8.8.8.8

```
Server:         8.8.8.8
Address:  8.8.8.8#53

Name:     www.google.com
Address 1: 108.160.163.117
Address 2: 2a03:2880:f10a:83:face:b00c:0:25de
```

4.4.4 Packet Obtaining

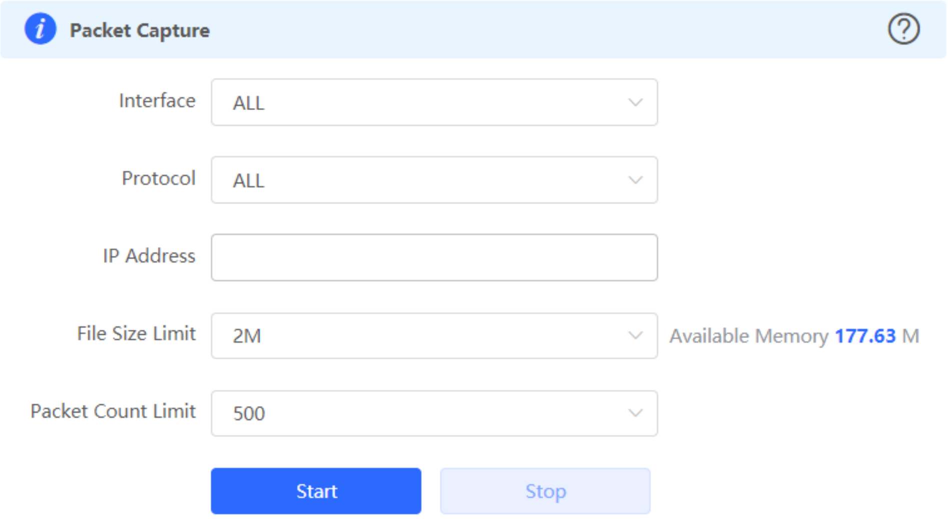
Switch to the **Local** mode. Choose **Diagnostics** > **Packet Capture**.

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: ALL

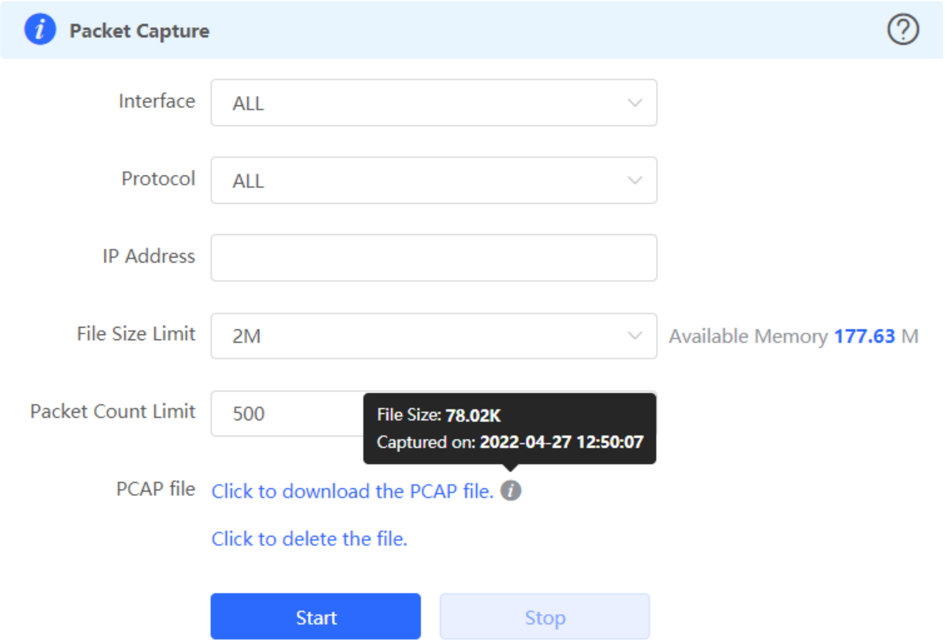
Protocol: ALL

IP Address:

File Size Limit: 2M Available Memory 177.63 M

Packet Count Limit: 500

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: ALL

Protocol: ALL

IP Address:

File Size Limit: 2M Available Memory 177.63 M

Packet Count Limit: 500

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

PCAP file: Click to download the PCAP file.

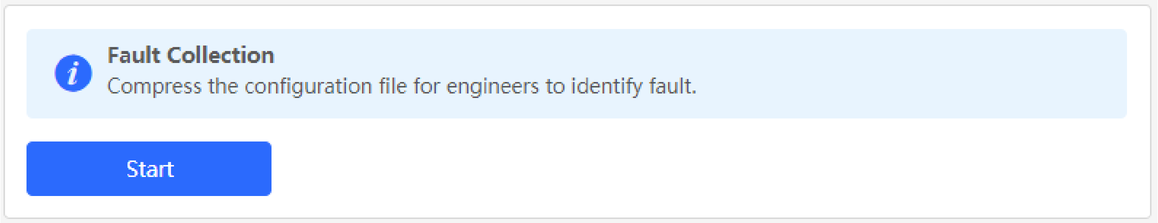
Click to delete the file.

- **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.



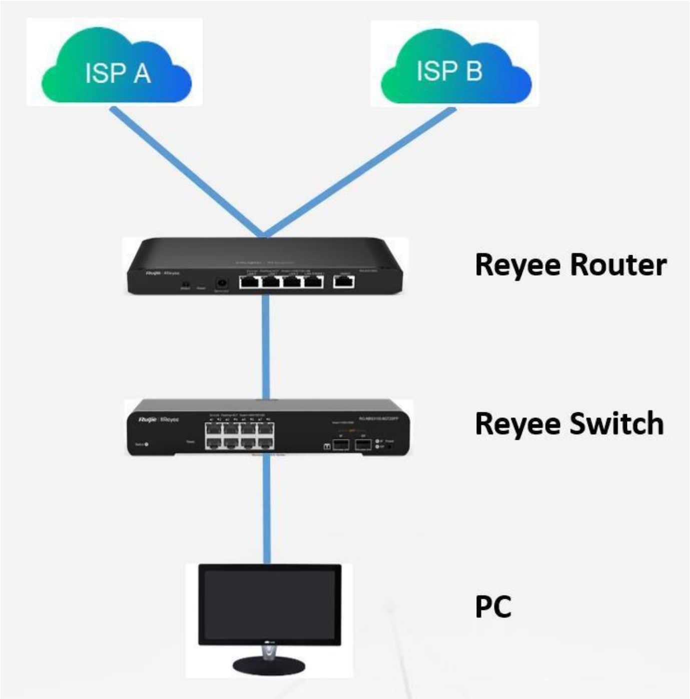
Fault Collection

Compress the configuration file for engineers to identify fault.

Compress the configuration file for engineers to identify faults.

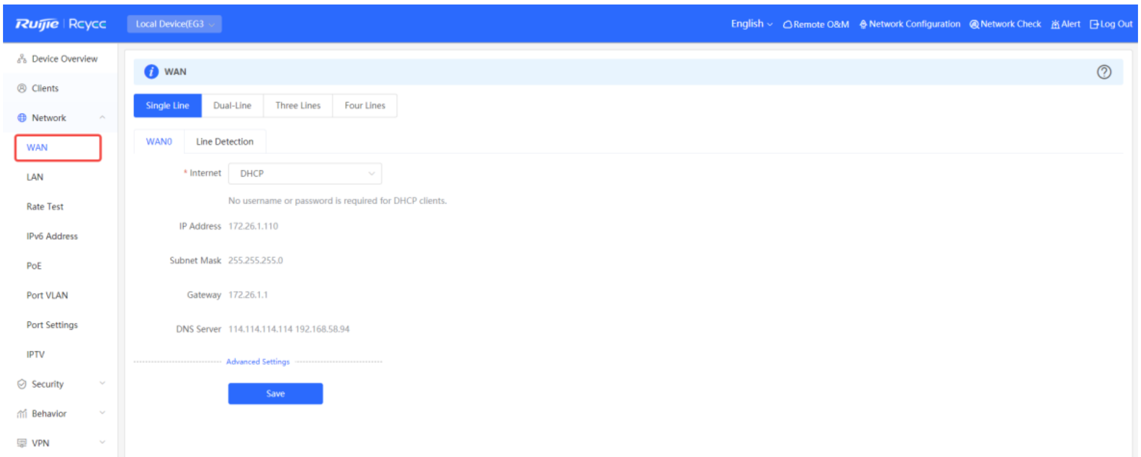
4.5 WAN Load Balancing

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**.



* Internet: DHCP

No username or password is required for DHCP clients.

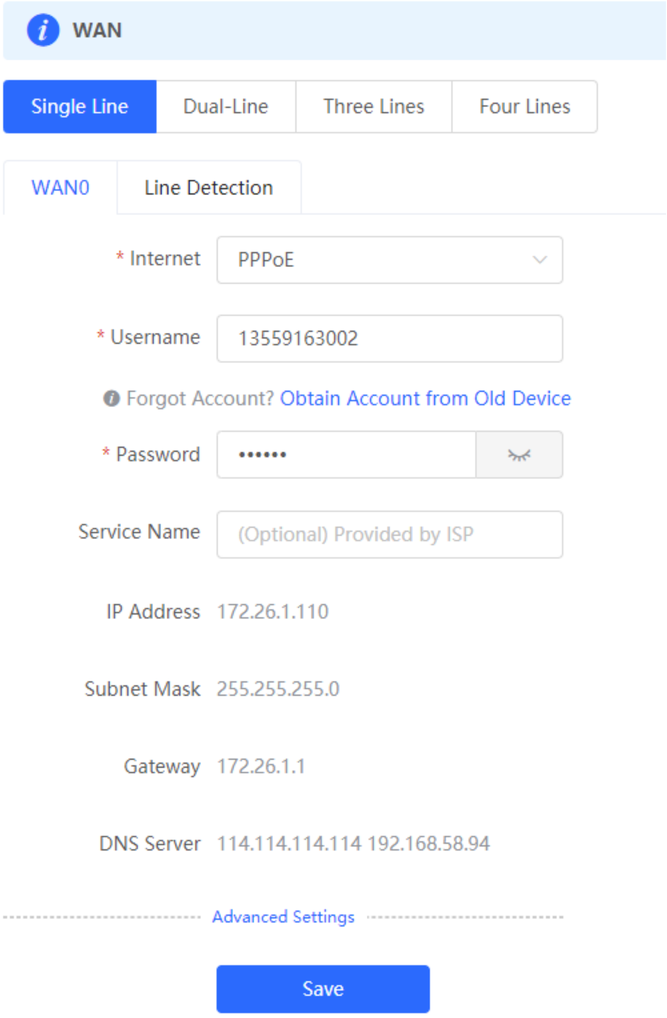
IP Address: 172.26.1.110

Subnet Mask: 255.255.255.0

Gateway: 172.26.1.1

DNS Server: 114.114.114.114 192.168.58.94

(2) Configure **WAN** accordingly.



* Internet: PPPoE

* Username: 13559163002

Forgot Account? Obtain Account from Old Device

* Password: ••••••

Service Name: (Optional) Provided by ISP

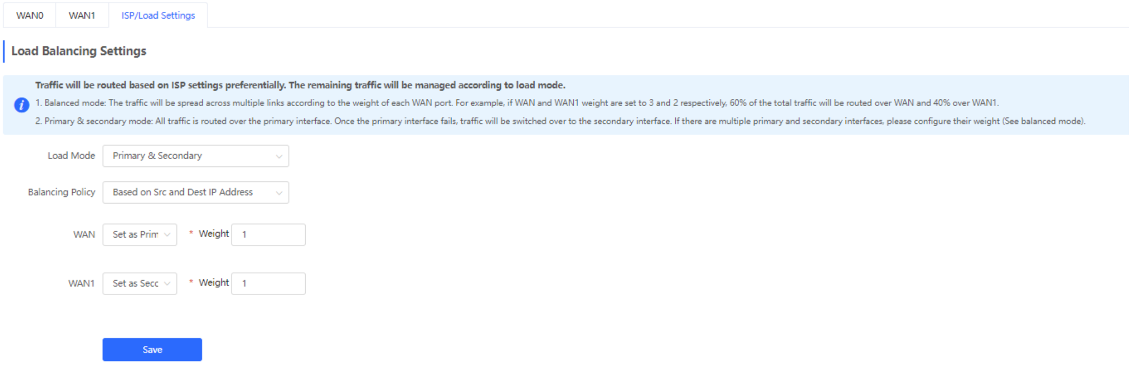
IP Address: 172.26.1.110

Subnet Mask: 255.255.255.0

Gateway: 172.26.1.1

DNS Server: 114.114.114.114 192.168.58.94

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



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

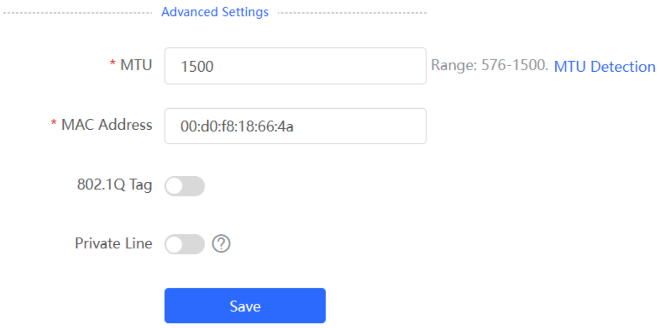
- **Balanced mode:** Traffic will be transmitted across multiple links according to the weight of each WAN port. For example, if weights of **WAN** and **WAN1** are set to 3 and 2 respectively, 60% of the total traffic will be routed over **WAN** and 40% over **WAN1**.
- **Primary & secondary mode:** 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 Modifying the MTU

Choose **Local Device** >**Network** > **WAN** > **WAN0** > **Advanced Settings**.

4.6.1 Modifying the MTU

MTU specifies the maximum transmission unit allowed to pass a WAN port. By default, the MTU of a WAN port is 1500 bytes. Sometimes, large data packets are limited in transmission speed or prohibited in the ISP network, leading to slow network speed or even network disconnection. If this occurs, you can set the MTU to a smaller value.



* MTU: 1500 Range: 576-1500. MTU Detection

* MAC Address: 00:d0:f8:18:66:4a

802.1Q Tag

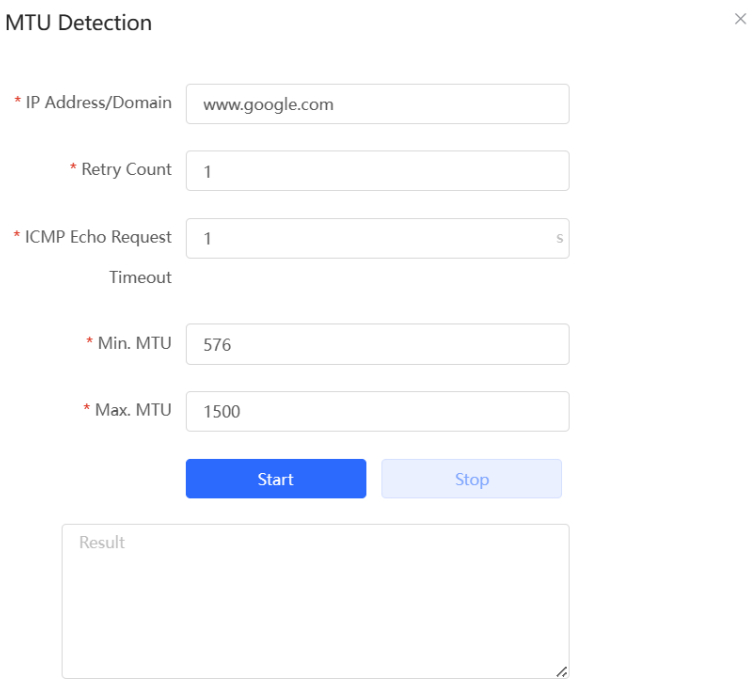
Private Line

If the MTU value is unknown, click **MTU Detection** to configure the one-click MTU detection, and adjust the MTU settings based on the results obtained from MTU detection.

4.6.2 Detecting the MTU

Click **MTU Detection** to configure the one-click MTU detection to determine the MTU between two communication devices.

Enter the destination IP/domain name, retry count, ICMP echo request timeout, minimum MTU, maximum MTU, and click **Start** to start the detection.



MTU Detection

* IP Address/Domain: www.google.com

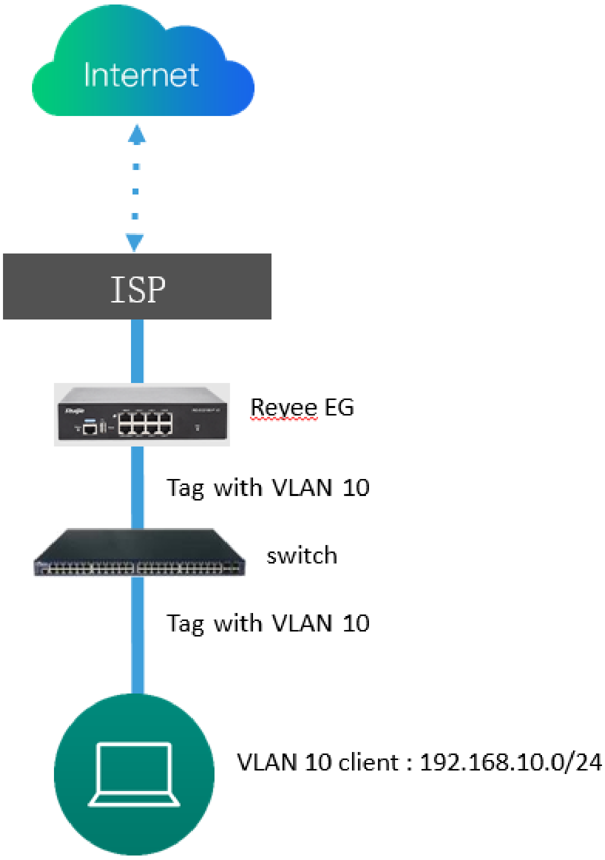
* Retry Count: 1

* ICMP Echo Request Timeout: 1 s

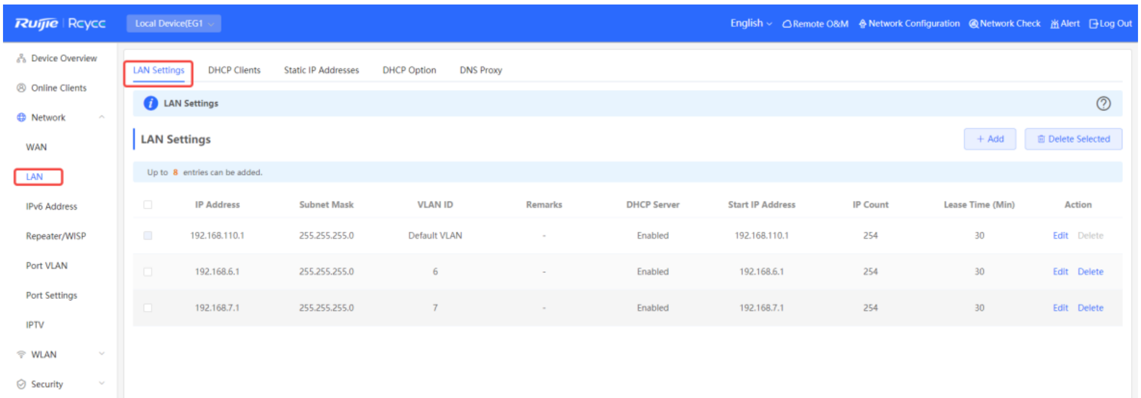
* Min. MTU: 576

* Max. MTU: 1500

4.7 Port VLAN



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

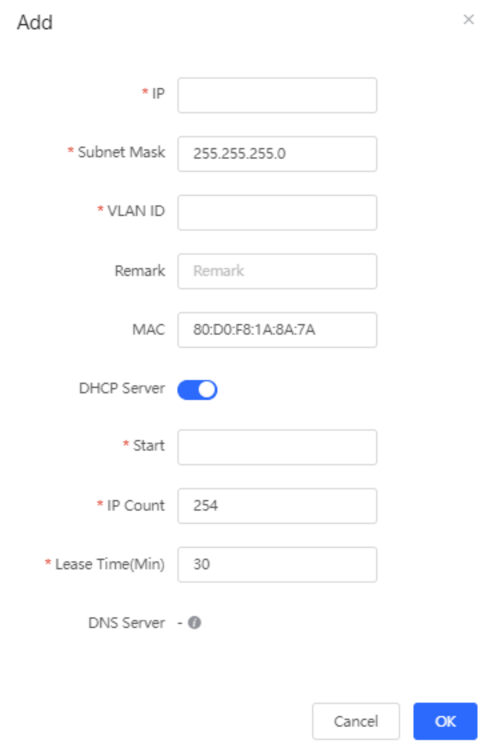


LAN Settings

LAN Settings

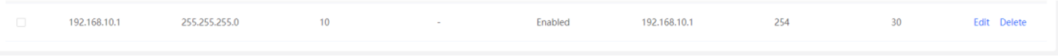
Up to 8 entries can be added.

□	IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
□	192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete



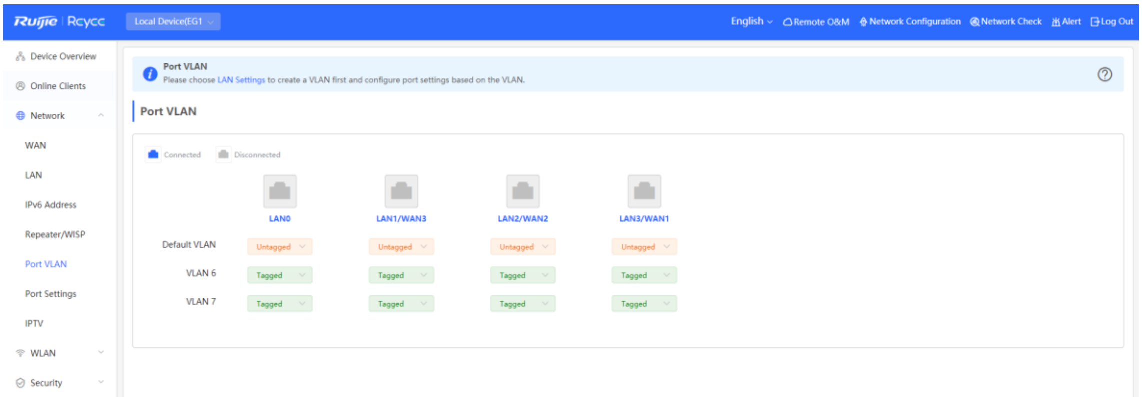
* IP	
* Subnet Mask	255.255.255.0
* VLAN ID	
Remark	Remark
MAC	80:D0:F8:1A:8A:7A
DHCP Server	●
* Start	
* IP Count	254
* Lease Time(Min)	30
DNS Server	-

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



□	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.

Port VLAN

	LAN0	LAN1/WAN3	LAN2/WAN2	LAN3/WAN1
Default VLAN	Untagged	Untagged	Untagged	Untagged
VLAN 6	Tagged	Tagged	Tagged	Tagged
VLAN 7	Tagged	Tagged	Tagged	Tagged

- **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.

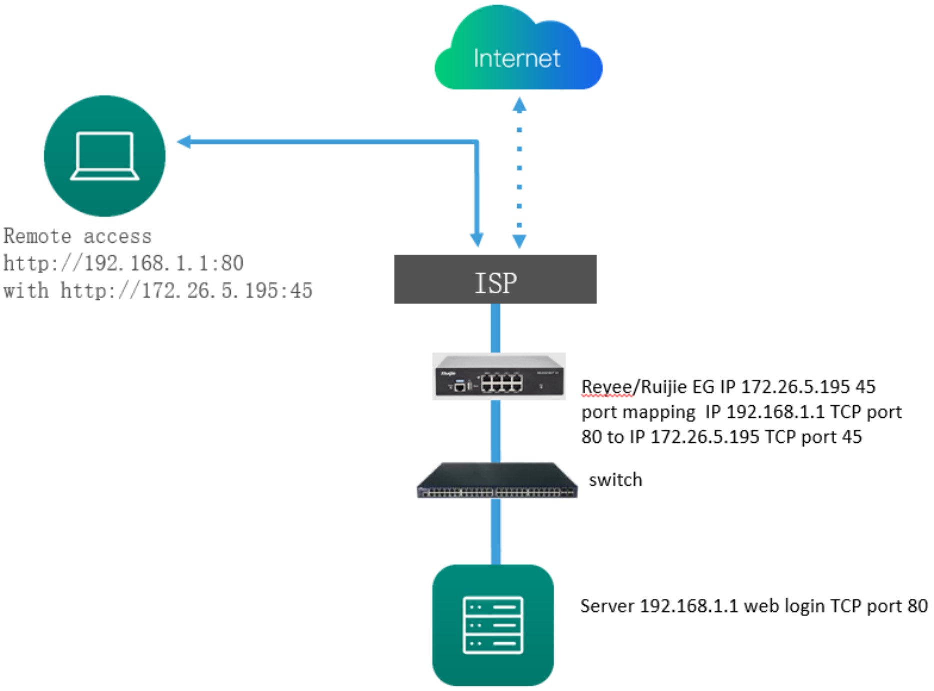
4.8 Port Mapping

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.

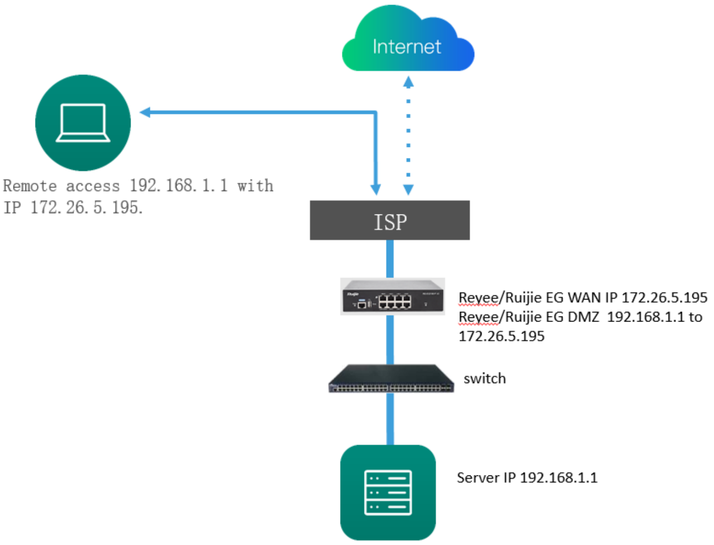
  Port mapping enables users to access cameras or computers on their home networks when they are in companies or on a business trip.


Internet
Remote access
http://192.168.1.1:80
with http://172.26.5.195:45
ISP
Reyee/Ruijie EG IP 172.26.5.195 45
port mapping IP 192.168.1.1 TCP port
80 to IP 172.26.5.195 TCP port 45
switch
Server 192.168.1.1 web login TCP port 80

- 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.

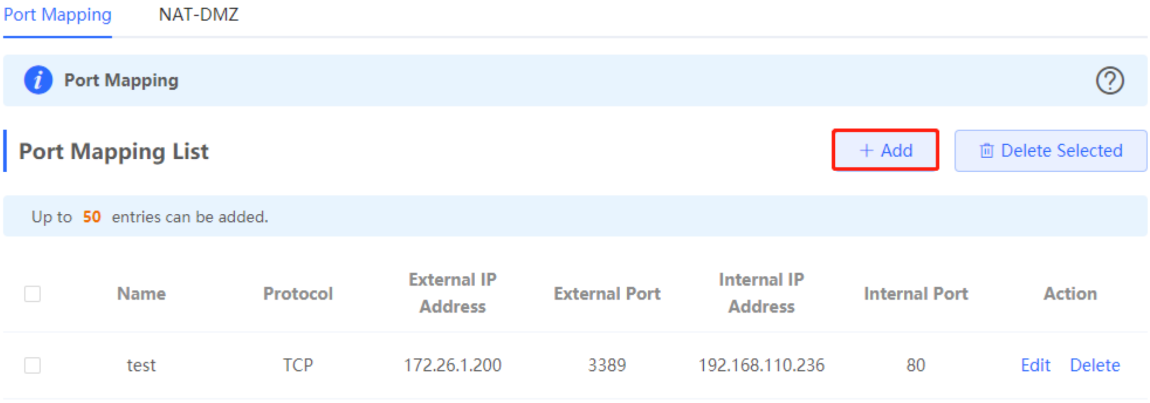
Port mapping or DMZ is used when an external network user wants to access the LAN server, for example, access a server deployed on the intranet when the user is in the enterprise or on a business trip.


Internet
Remote access 192.168.1.1 with IP 172.26.5.195.
ISP
Reyee/Ruijie EG WAN IP 172.26.5.195
Reyee/Ruijie EG DMZ 192.168.1.1 to 172.26.5.195
switch
Server IP 192.168.1.1

4.8.1 Configuring Port Mapping

(1) Switch to the **Local** mode. Choose **Advanced** > **Port Mapping** > **Port Mapping**.

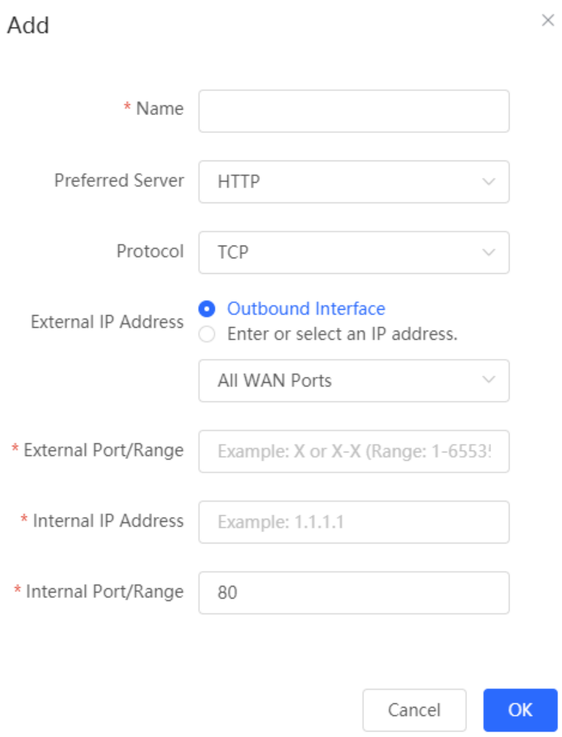
(2) Click **Add**. In the dialog box that appears, enter the rule name, service type, protocol type, external port/range, internal server IP address, and internal port/range. You can create a maximum of 50 port mapping rules.



Port Mapping List

Up to 50 entries can be added.

□	Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Action
□	test	TCP	172.26.1.200	3389	192.168.110.236	80	Edit Delete



Add

* Name

Preferred Server: HTTP

Protocol: TCP

External IP Address: ● Outbound Interface ○ Enter or select an IP address.

All WAN Ports

* External Port/Range: Example: X or X-X (Range: 1-6553!

* Internal IP Address: Example: 1.1.1.1

* Internal Port/Range: 80

Table 4-6 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.
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.

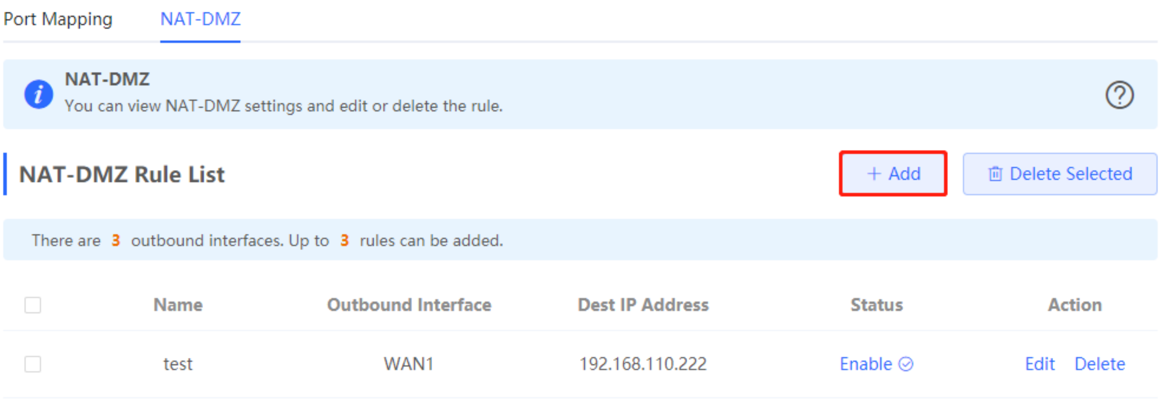
Parameter	Description
Internal Port/Range	Specify the service port number of the internal server to be mapped to the WAN port, that is, the port number of the application that provides Internet access, such as port 8080 of the web service. You can enter a port number or a port range, such as 1050-1060. 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.



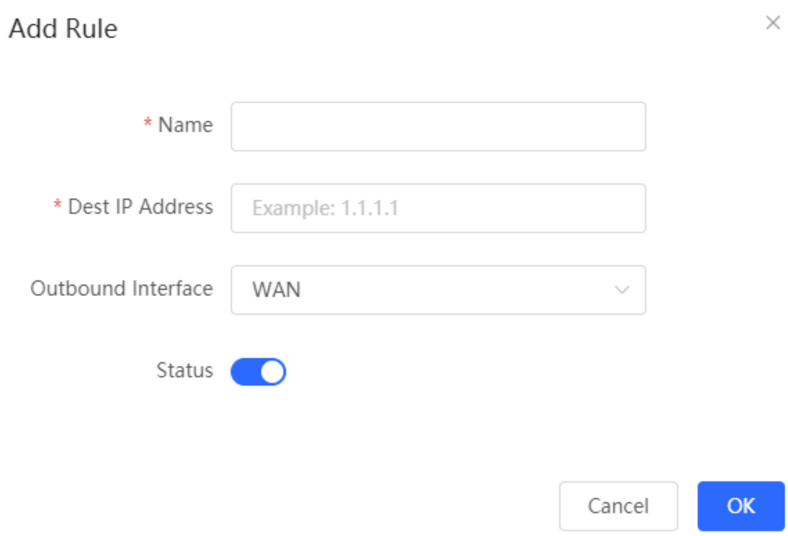
NAT-DMZ

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

NAT-DMZ Rule List

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

□	Name	Outbound Interface	Dest IP Address	Status	Action
□	test	WAN1	192.168.110.222	Enable ✓	Edit Delete



Add Rule

* Name

* Dest IP Address: Example: 1.1.1.1

Outbound Interface: WAN

Status: ●

Table 4-7 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.

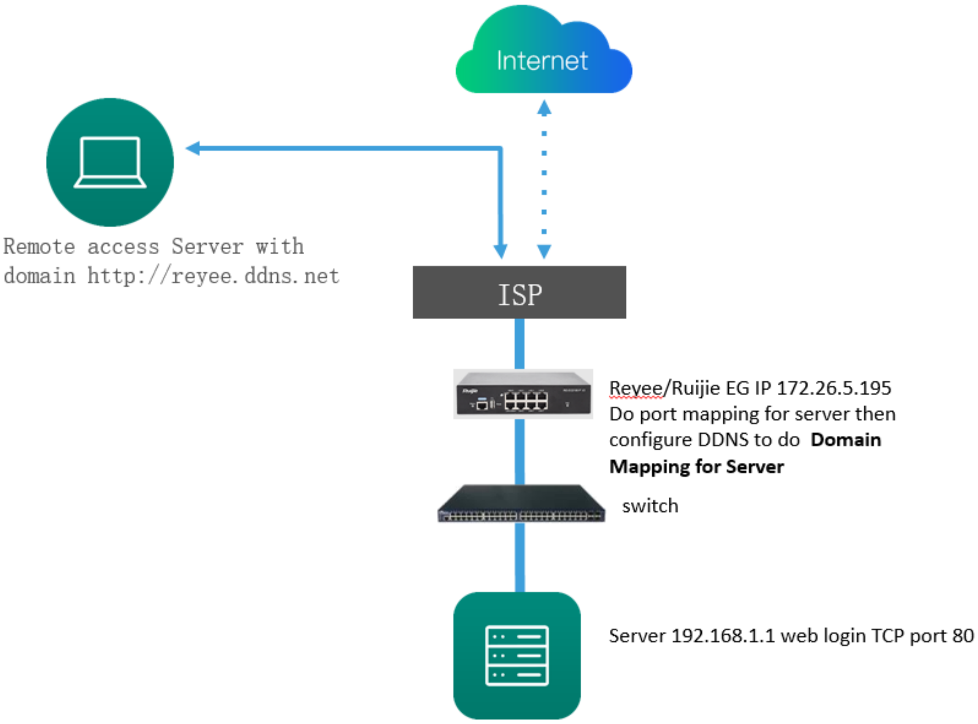
⚠ **Caution**

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

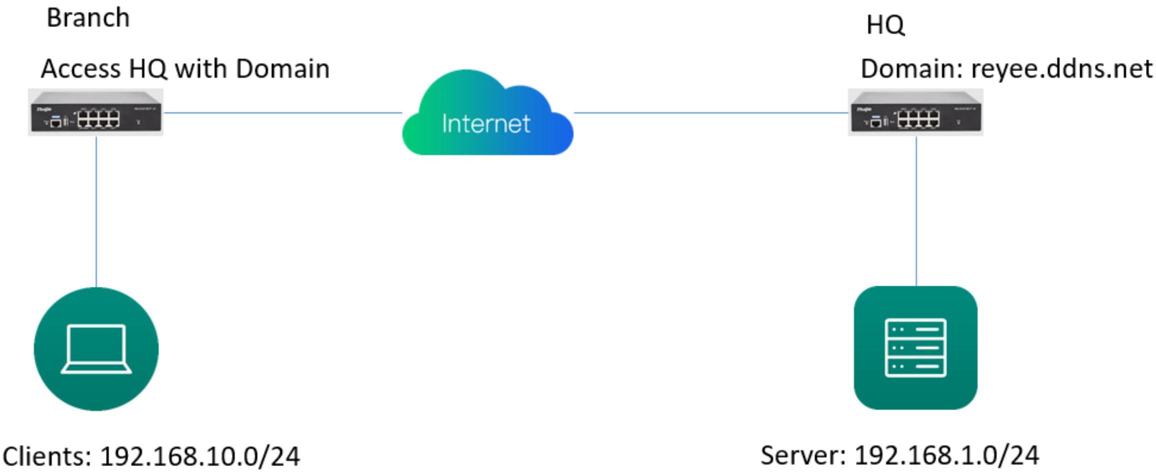
4.9 Dynamic DNS

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

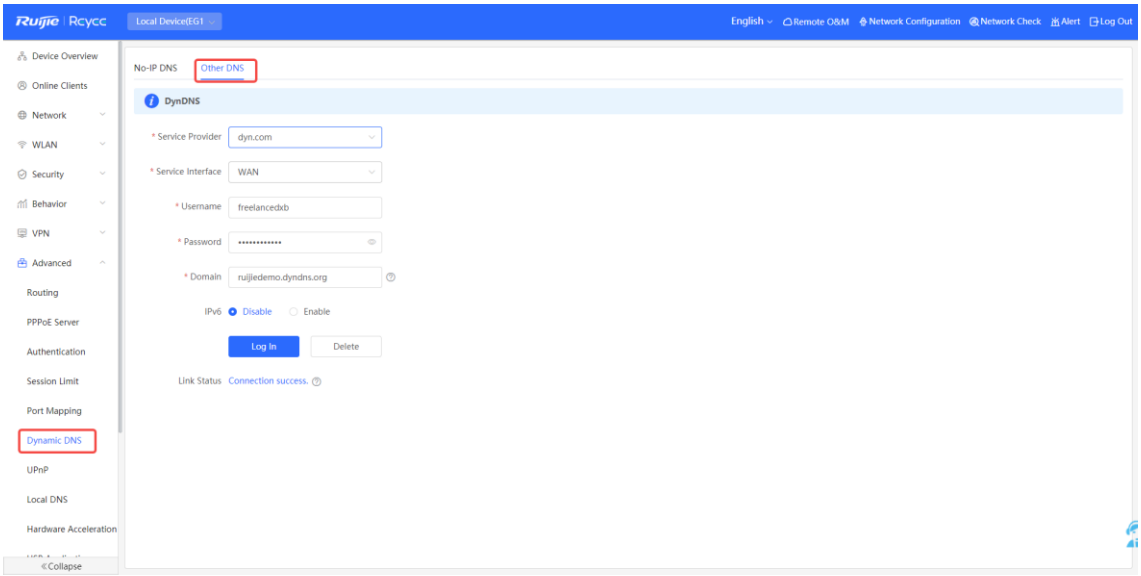

Internet
Remote access Server with
domain http://reyee.ddns.net
ISP
Reyee/Ruijie EG IP 172.26.5.195
Do port mapping for server then
configure DDNS to do **Domain
Mapping for Server**
switch
Server 192.168.1.1 web login TCP port 80

- VPN connection with the domain name



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

There are two DDNS servers you can choose to connect: NO-IP DNS, and Other DNS.



DynDNS

* Service Provider: dyn.com

* Service Interface: WAN

* Username: freelancedxb

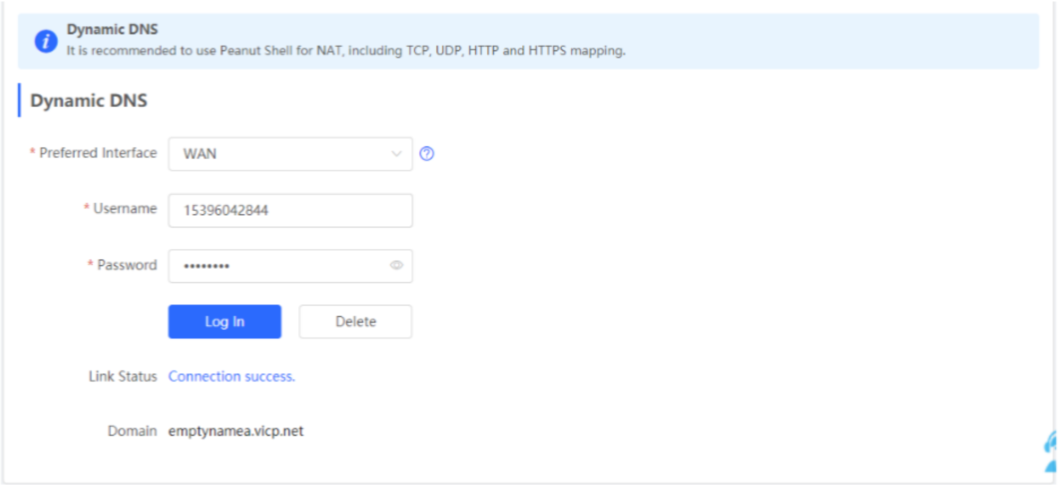
* Password: ••••••••••••

* Domain: ruijiedemo.dyndns.org

IPv6 ● Disable ○ Enable

Link Status: Connection success.

(2) You can use the value of **Domain** to access the intranet server or headquarters device.



Dynamic DNS
It is recommended to use Peanut Shell for NAT, including TCP, UDP, HTTP and HTTPS mapping.

Dynamic DNS

* Preferred Interface: WAN

* Username: 15396042844

* Password: ••••••••

Link Status: Connection success.

Domain: emptynamea.vicp.net

4.10 Wi-Fi Authentication

4.10.1 Overview

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

The Wi-Fi authentication function of the device uses the Portal authentication technology to implement information display and user management. After users connect to Wi-Fi, the traffic will not be directly routed to the Internet. Wi-Fi users must pass authentication on 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.

4.10.2 Getting Started

(1) Before you enable Wi-Fi authentication, ensure that the wireless signal is stable and users can connect to Wi-Fi and surf the Internet normally. The wireless SSID used for authentication in the network should be set to the open state. Encryption may lead to exceptions during Connect Wi-Fi via WeChat authentication.

(2) If the IP address of an AP in the network is within the authentication scope, add the AP as the authentication-free user. For details, see Section 4.10.10 Authentication-Free.

- In a Layer 2 network, add the MAC address of the AP to the authentication-free MAC address allowlist.
- In a Layer 3 network, add the IP address of the AP to the authentication-free IP address allowlist.

4.10.3 WeChat Authentication

1. Overview

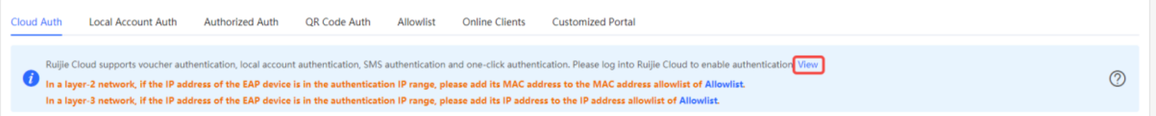
The EG device is connected to the MACC authentication server on the cloud. After Wi-Fi users connect to Wi-Fi, a Portal page pops up. The users need to jump to WeChat and follow the WeChat official account before they can access the Internet. WeChat authentication is applicable to the shopping mall scenario,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

2. Getting Started

(1) Connect Wi-Fi via WeChat is a Layer 2 protocol. Ensure that the authentication device can obtain the MAC addresses of the wireless users.

- The gateway address of the 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 the 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 NOC MACC platform before you enable the authentication function on the device. Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication, and one-click authentication. Please log into Ruijie Cloud to enable authentication.



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

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 allowlist of Allowlist.

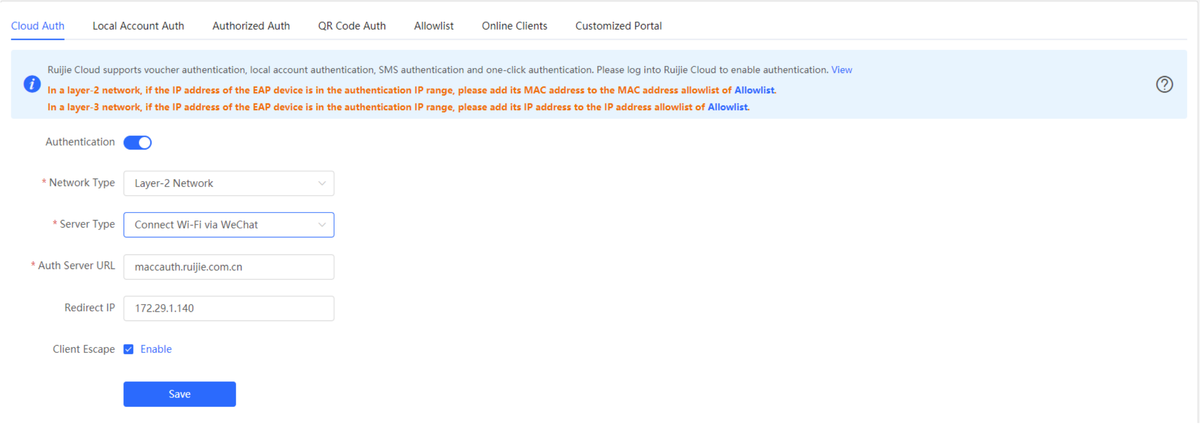
In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address allowlist of Allowlist.

3. Configuration Steps

Choose **Local Device** > **Advanced** > **Authentication** > **Cloud Auth**.

(1) Enable WeChat authentication for Internet access.

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



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

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 allowlist of Allowlist.

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 allowlist of Allowlist.

Authentication: on

* Network Type: Layer-2 Network

* Server Type: Connect Wi-Fi via WeChat

* Auth Server URL: maccauth.ruijie.com.cn

Redirect IP: 172.29.1.140

Client Escape: ☑ Enable

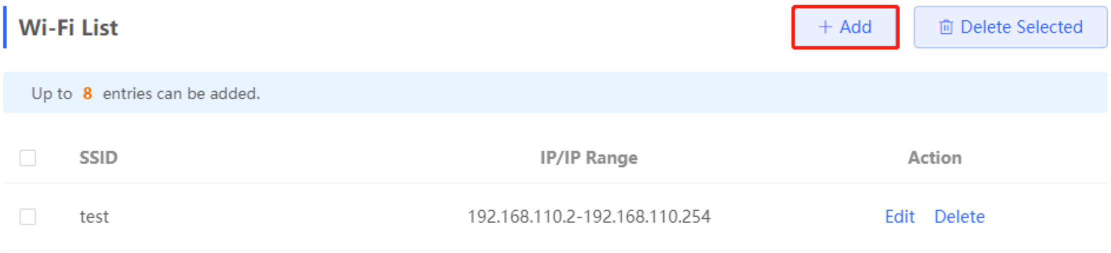
Table 4-8 WeChat authentication configuration

Parameter	Description
Network Type	The default value is **Layer-2 Network**. Select a network type based on the actual network environment. As Connect Wi-Fi via WeChat is a Layer 2 protocol, in a Layer 3 network environment, you need to connect downlink devices to the current authentication device through the DHCP relay and deploy the DHCP address pool for the authentication-engaged network segments in 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**.
Server Type	Select **Connect Wi-Fi via WeChat**.
Auth Server URL	After you complete the MACC server configuration, the MACC server returns a URL. The device sends an authentication request to this URL.
Redirect IP	The redirect IP address corresponds to a menu or link address set in the official account. The default value is 118.31.178.137. Generally, you do not need to change the value. After the user is redirected to the WeChat official account, the user needs to visit this IP address before the subsequent authentication steps can continue. Change the value to an IP address in a not used LAN network segment, if required. For details, see Troubleshooting.
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 started automatically.

(2) Configure the authentication scope.

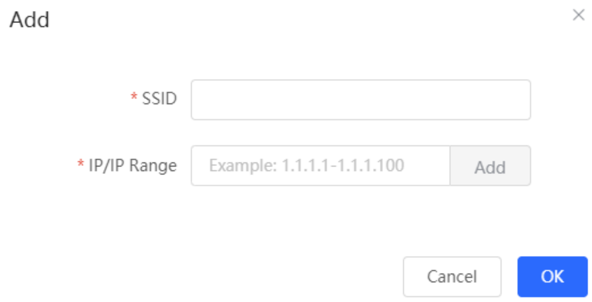
Click **Add** on the current page. In the dialog box that appears, enter the VLAN and IP address range that needs authentication, and click **OK**.

For clients that do not need authentication, such as printers, computers, or some users, set **IP/IP Range** to authentication-free, so that these clients can directly access the Internet. For details, see Section 4.10.10 Authentication-Free.



Up to 8 entries can be added.

□	SSID	IP/IP Range	Action
□	test	192.168.110.2-192.168.110.254	Edit Delete



* SSID

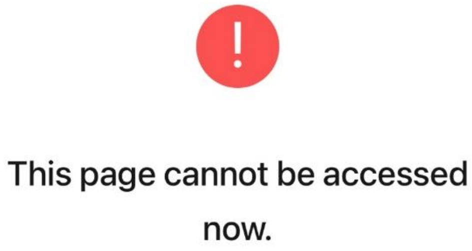
* IP/IP Range: Example: 1.1.1.1-1.1.1.100

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 4.10.11 Online Authenticated User Management.

5. Troubleshooting

When the user clicks the authentication menu or link in the official account during WeChat authentication, the message **This page cannot be accessed now.** pops up, leading to authentication failure.



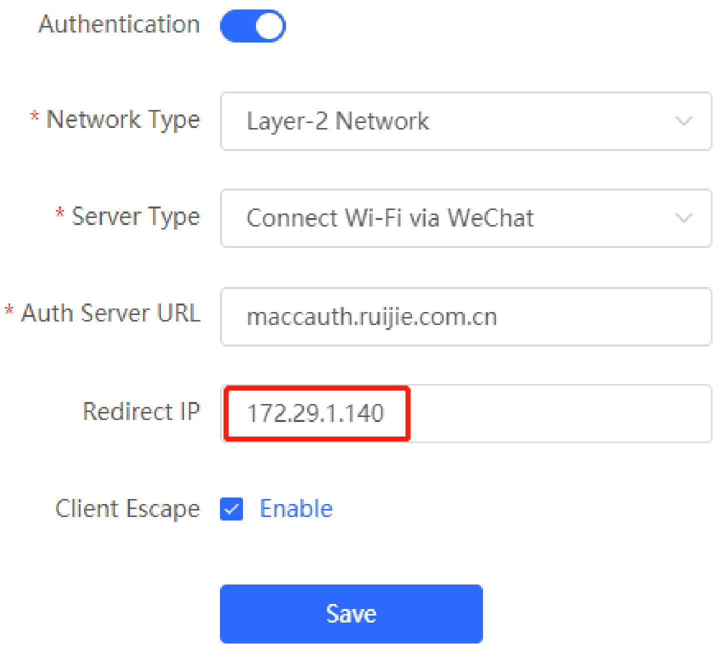
This page cannot be accessed now.

Cause: The link address set in the official account authentication entry in 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 in the LAN. For example, if the network segment 172.29.0.0 is not used in 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 in the LAN, WeChat authentication will fail.



Authentication: On

* Network Type: Layer-2 Network

* Server Type: Connect Wi-Fi via WeChat

* Auth Server URL: maccauth.ruijie.com.cn

Redirect IP: 172.29.1.140

Client Escape: ☑ Enable

4.10.4 Enterprise WeChat Authentication

1. Overview

Similar to WeChat authentication, Wi-Fi users need to jump 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 employee clients and guest clients in the enterprise environment.

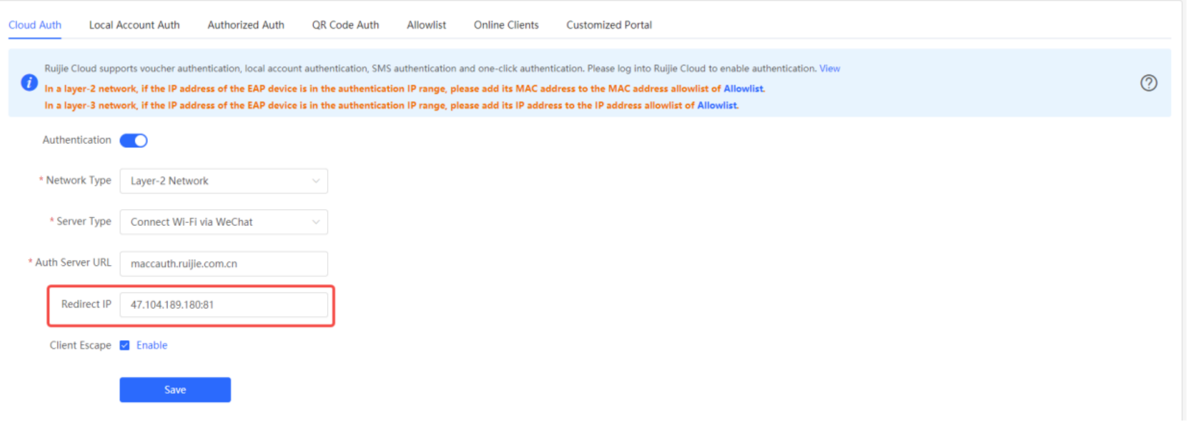
2. Getting Started

Same as those in Section 4.10.3 WeChat Authentication. Before you enable enterprise WeChat authentication, complete relevant configurations on the enterprise WeChat console and NOC MACC platform.

3. Configuration Steps

Choose **Local Device** > **Advanced** > **Authentication** > **Cloud Auth**.

The configuration steps are similar to those in WeChat authentication, with major difference in that the official account redirection IP address in enterprise WeChat authentication should be set to 47.104.189.180:81. For details, see Section 4.10.3 WeChat Authentication.



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

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 allowlist of Allowlist.

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 allowlist of Allowlist.

Authentication: on

* Network Type: Layer-2 Network

* Server Type: Connect Wi-Fi via WeChat

* Auth Server URL: maccauth.ruijie.com.cn

Redirect IP: 47.104.189.180:81

Client Escape: ☑ Enable

4. Employee Authentication

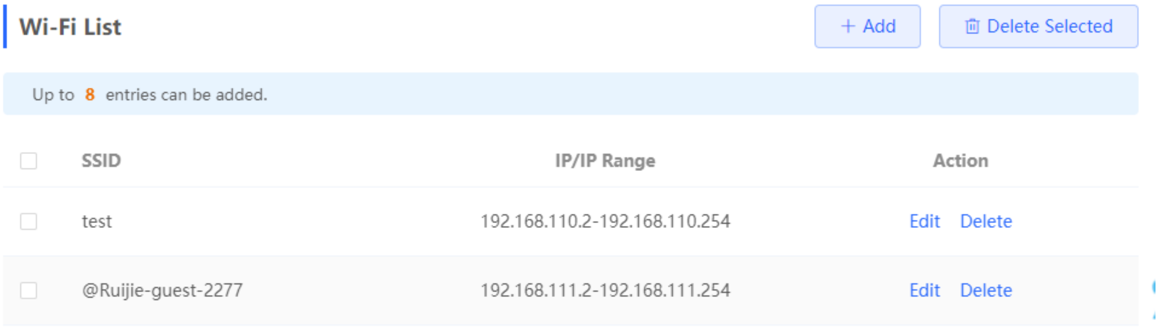
Make sure that the employee has joined the enterprise WeChat organization. When the employee connects the mobile phone to Wi-Fi, the employee is automatically redirected to the enterprise WeChat for authentication. After the employee opens the enterprise WeChat, employee needs to enter the **Workspace** menu of the enterprise WeChat and click the authentication app created by the administrator to obtain Internet access permission. After the authentication success message pops up, 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 poor compatibility. If this occurs, users can manually open the enterprise WeChat and continue follow-up operations.

5. Guest Authentication

Guest access to the Internet via Wi-Fi should be authorized by the receptionist. After a guest connects to the guest Wi-Fi, the authentication QR code pops up. 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.

It should be noted that 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 connection and guest connection, respectively.



Up to 8 entries can be added.

□	SSID	IP/IP Range	Action
□	test	192.168.110.2-192.168.110.254	Edit Delete
□	@Ruijie-guest-2277	192.168.111.2-192.168.111.254	Edit Delete

4.10.5 WiFiDog 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 pops up. The users need to enter the account and password to pass authentication before they can access the Internet. According to the authentication configuration on the MACC server, you can set the authentication mode to SMS authentication, fixed account authentication, or account-free one-click login.

2. Getting Started

(1) WiFiDog is a Layer 2 protocol. Ensure that the authentication device can obtain the MAC addresses of the wireless users.

- The gateway address of the 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 the wireless users and obtain MAC addresses of the wireless users. In this scenario, you need to set Network Type to Layer-3 Network.

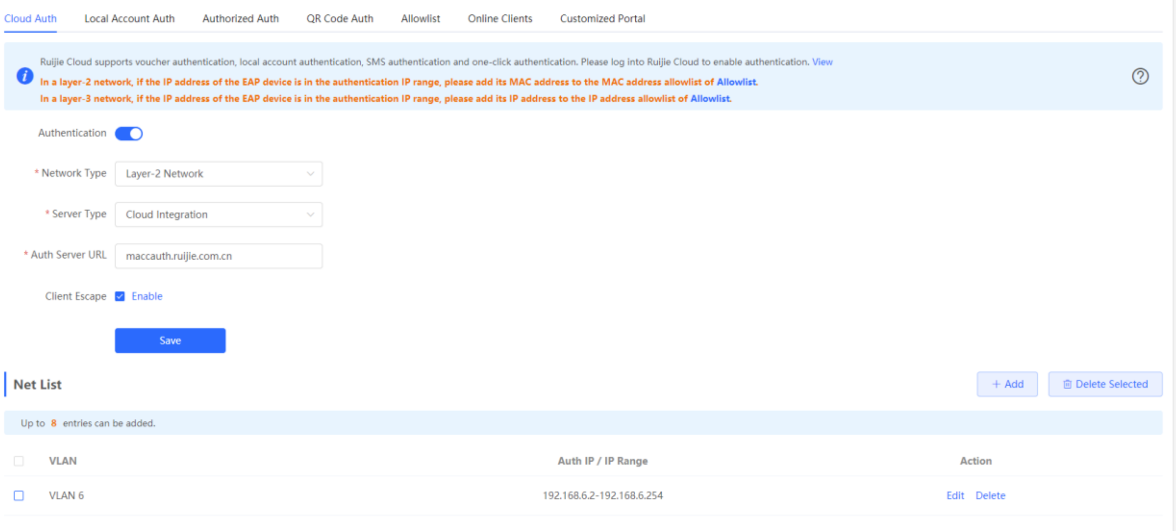
(2) Complete the corresponding configuration on the NOC MACC platform before you enable the authentication function on the device. If SMS authentication is used, you also need to configure the SMS gateway.

3. Configuration Steps

Choose **Local Device** > **Advanced** > **Authentication** > **Cloud Auth**.

(1) Turn on **Authentication**.

(2) Set **Server Type** to **Cloud Integration**, configure **Network Type**, **Auth Server URL**, **Client Escape**, and **IP/IP Range**, and click **Save**.



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

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 allowlist of Allowlist.

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 allowlist of Allowlist.

Authentication: ●

* Network Type: Layer-2 Network

* Server Type: Cloud Integration

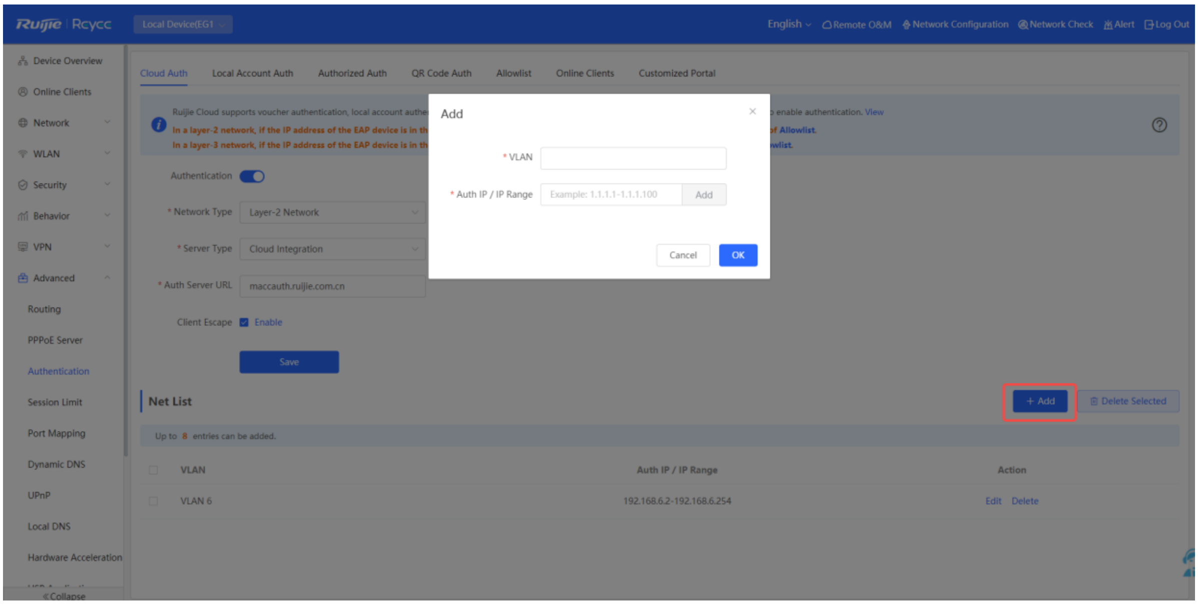
* Auth Server URL: maccauth.ruijie.com.cn

Client Escape: ☑ Enable

Up to 8 entries can be added.

□	VLAN	Auth IP / IP Range	Action
□	VLAN 6	192.168.6.2-192.168.6.254	Edit Delete

(3) In the **Wi-Fi List** area, click **Add**. In the displayed dialog box, enter the Wi-Fi network name and the IP address/range to be authenticated and click **OK**.



Ruijie Cloud supports voucher authentication, local account authe… enable authentication. View

In a layer-2 network, if the IP address of the EAP device is in th… of Allowlist.

In a layer-3 network, if the IP address of the EAP device is in th… wlist.

Authentication: ON

* Network Type: Layer-2 Network

* Server Type: Cloud Integration

* Auth Server URL: maccauth.ruijie.com.cn

Client Escape: ☑ Enable

Add

* VLAN:

* Auth IP / IP Range: Example: 1.1.1.1-1.1.1.100 Add

Up to 8 entries can be added.

□	VLAN	Auth IP / IP Range	Action
□	VLAN 6	192.168.6.2-192.168.6.254	Edit Delete

Table 4-9 Description of WiFiDog Authentication Configuration

Parameter	Description
Network Type	The default value is **Layer-2 Network**. Set the parameter based on the actual network environment.
Server Type	Select **Cloud Integration** from the drop-down list.
Auth Server URL	After completing the configuration at the MACC server end, the MACC server returns a URL. The device sends authentication requests to the URL during authentication.
Client Escape	After the client escape function is enabled, if an exception occurs on the authentication server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication.
SSID	Specify the name of a Wi-Fi network, to which clients connect. A maximum of eight Wi-Fi network names can be configured.
IP/IP Range	Specify the IP address range to be authenticated. You can enter a single IP address (such as 192.168.112.2) or an IP address range (such as 192.168.112.2–192.168.112.254). A maximum of five IP address ranges can be configured.

4. Verifying Configuration

After a mobile phone connects to a specific Wi-Fi, the Portal authentication page pops up automatically.

If the authentication mode configured on the MACC server is SMS authentication, the user needs to enter the mobile number to obtain an Internet access password and enter the password to complete authentication.

If the authentication mode configured on the MACC server is account-free one-click authentication, the user can directly access the Internet after clicking the corresponding button on the page.

If the authentication mode configured on the MACC server is fixed account login, the user can access the Internet after entering the account and password configured on the cloud.

After successful connection, you can choose **Advanced** > **Authentication** > **Online Clients** to view information about this authenticated user. For details, see Section 4.10.11 Online Authenticated User Management.

4.10.6 Configuring Third-Party Authentication

Note

This feature is supported on RG-EG310GH-E, RG-EG305GH-P-E and EG310GH-P-E running ReyeeOS 2.237 or later.

1. Overview

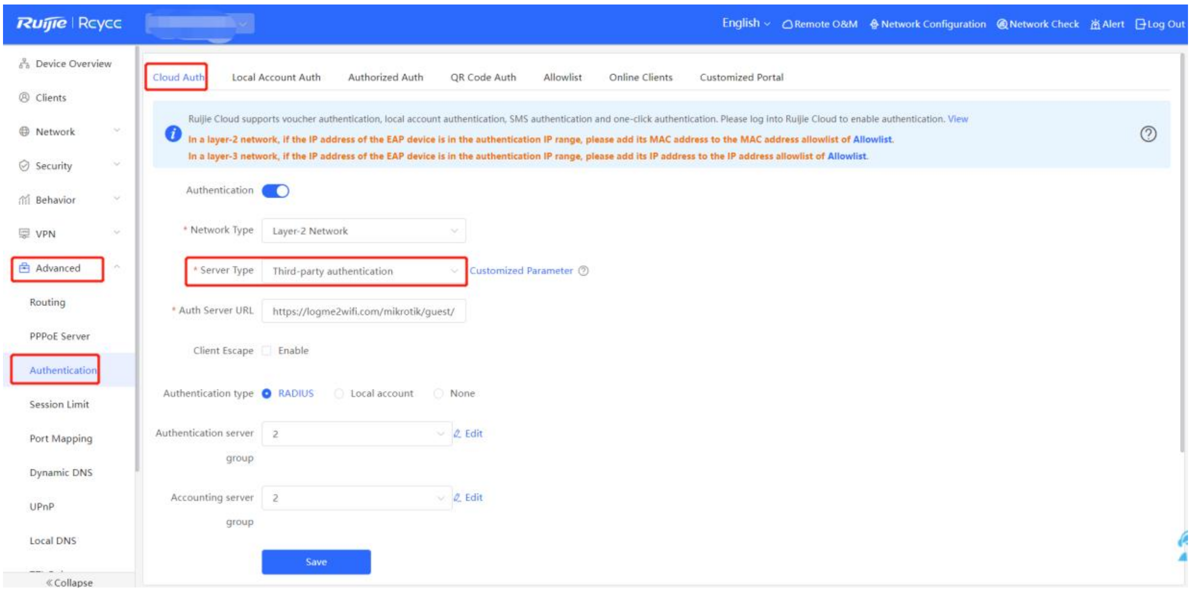
Reyee EG series gateway devices can interwork with WISPr-compliant external authentication servers. After a wireless client is connected to the Wi-Fi network, a Portal page pops up. The wireless client needs to be authenticated before it can access the Internet. Based on the services provided by different authentication servers, you can choose RADIUS authentication, local account authentication, or no authentication for third-party authentication.

2. Getting Started

- Ensure that the authentication server can obtain the MAC address of the wireless client:
  - The gateway address of the wireless client to be authenticated is deployed on the authentication server.
  - If the gateway address of the wireless client to be authenticated is not deployed on the authentication server, then the device must act as a DHCP server to assign an IP address to the wireless client in order to obtain its MAC address. In this scenario, the **Network Type** must be set to **Layer 3 Network**.
- Complete relevant configurations on the third-party authentication platform, and then enable the Wi-Fi authentication feature on the device. For specific configurations, see the configuration manual of relevant third-party authentication platforms.

3. Configuration Steps

Choose **Advanced** > **Authentication** > **Cloud Auth**.



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

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 allowlist of Allowlist.

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 allowlist of Allowlist.

Authentication: on

* Network Type: Layer-2 Network

* Server Type: Third-party authentication

* Auth Server URL: https://logme2wifi.com/mikrotik/guest/

Client Escape: □ Enable

Authentication type: ● RADIUS ○ Local account ○ None

Authentication server group: 2

Accounting server group: 2

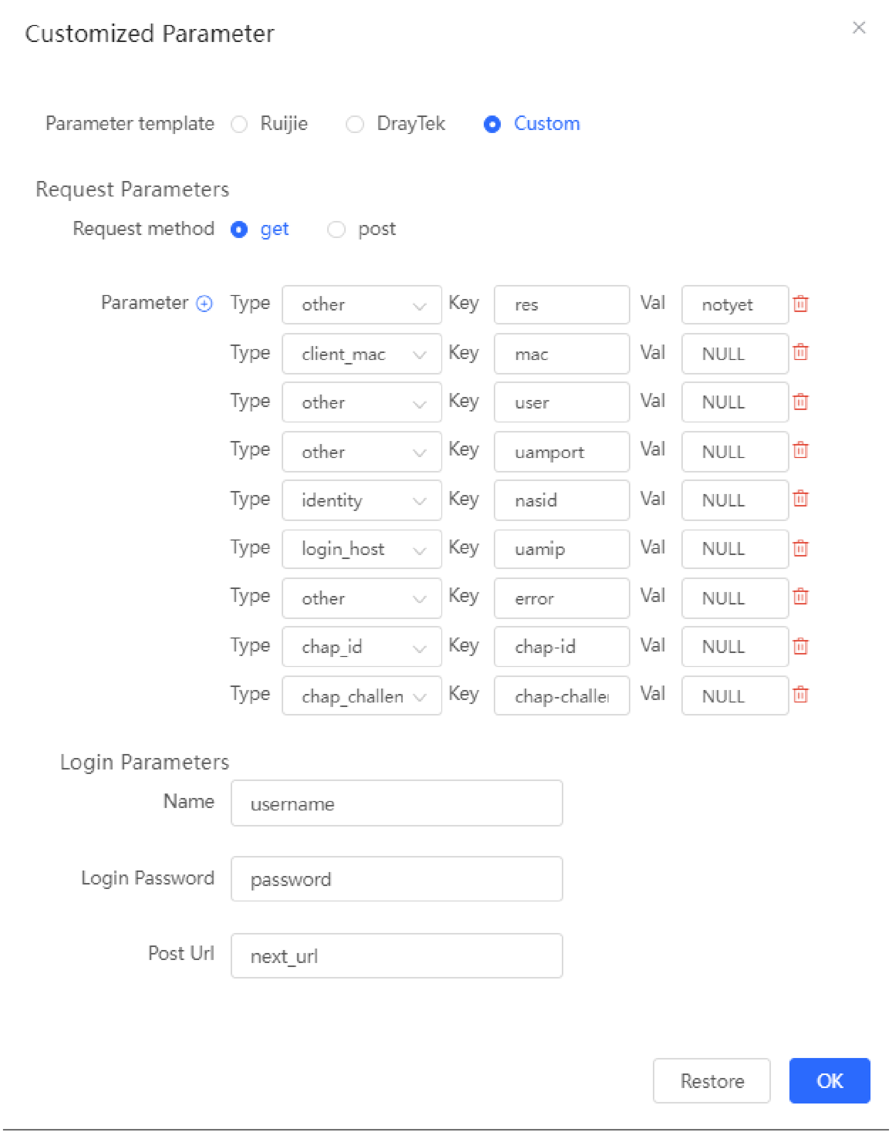
(1) Toggle on **Authentication**.

(2) Set **Server Type** to **Third-party Authentication**, configure **Auth Server URL**, **Client Escape** and **Authentication Type**, and click **Save**.

Table 4-10 Description of Third-Party Authentication Configuration Parameters

Parameter	Description
Network Type	The default value is **Layer-2 Network**. Set the parameter based on the actual network environment.
Server Type	Select **Third-party authentication** from the drop-down list.
Auth Server URL	After completing the configuration on the third-party authentication server, the third-party authentication server returns a URL. The device sends authentication requests to the URL during authentication.
Client Escape	After the client escape function is enabled, if an exception occurs on the authentication server or the RADIUS server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication.
Authentication Type	Types of third-party authentication, which include: ● **RADIUS**: The wireless client is authenticated by the RADIUS server. ● **Local account**: The wireless client is authenticated based on local username and password. ● **None**: No authentication is required for the wireless client.
Auth Server Group	Name of the authentication server group. This parameter is mandatory when the **Authentication Type** is set to **RADIUS**. You can configure the authentication server group in the global management mode by going to **Network-wide** > **802.1X Authentication** > **RADIUS Server Management**.
Accounting Server Group	Name of the accounting server group. This parameter is mandatory when the **Authentication Type** is set to **RADIUS**. You can configure the accounting server group in the global management mode by going to **Network-wide** > **802.1X Authentication** > **RADIUS Server Management**.

(3) (Optional) Considering the different HTTP parameters and request methods required by different third-party authentication platforms, you can customize third-party authentication parameters.



Customized Parameter

Parameter template ○ Ruijie ○ DrayTek ● Custom

Request Parameters

Request method ● get ○ post

Parameter Type other Key res Val notyet

Type client_mac Key mac Val NULL

Type other Key user Val NULL

Type other Key uamport Val NULL

Type identity Key nasid Val NULL

Type login_host Key uamip Val NULL

Type other Key error Val NULL

Type chap_id Key chap-id Val NULL

Type chap_challen Key chap-challe Val NULL

Login Parameters

Name username

Login Password password

Post Url next_url

Table 4-11 Description of Custom Third-Party Authentication Parameters

Parameter	Description
Parameter template	The built-in parameter template. Default parameters are used when the **Parameter Template** is set to **Ruijie** or **DrayTek**. When the **Parameter Template** is set to **Custom**, the parameters can be customized.
Request method	The HTTP request methods used for requesting the portal page.

Parameter	Description
Parameter	Parameters in the parameter template for requesting the portal page: ● When the parameter type is not other, the Val field is invalid, and the default value NULL can be used. The Reyee EG gateway device will automatically populate the value of this parameter. ● When the parameter type is **other**, you need to enter a value in the **Val** field. Parameters include: ● nas_ip: IP address of the Reyee EG series gateway device. Example: 10.52.48.7. ● nas_mac: MAC address of the Reyee EG series gateway device. Example: 11:22:33:44:55:66. ● client_ip: IP address of the wireless client to be authenticated. Example: 192.168.110.5. ● client_mac: MAC address of the wireless client to be authenticated. Example: 11:22:33:44:55:66. ● orig_url: Original URL accessed by the wireless client to be authenticated. Example: https://www.baidu.com. ● login_url: Login interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_login. ● logout_url: Logout interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_logout. ● ssid: SSID or VLAN name associated with the wireless client to be authenticated. Example: VLAN233. ● login_host: IP address of the login interface on the Reyee EG series gateway device. Example: 192.168.110.1:2060. ● other: other custom field. Multiple custom fields are supported.
Login Parameters	Custom fields of the login interface received by the Reyee EG series gateway devices from the third-party authentication platform, including: ● **Username**: username. ● Login Password: password. ● **Post Url**: URL to which the wireless client is redirected after successful authentication.

4. Verifying Configuration

Connect your smartphone to the specific Wi-Fi network to verify that the portal page pops up automatically.

Connect to different authentication platforms to view services provided by these authentication platforms.

After the connection is successful, view the details of the wireless client by going to **Advanced** > **Authentication** > **Online Clients**. For details, see 4.10.11 Online Authenticated User Management.

4.10.7 Local Account Authentication

1. Overview

The device is connected to the local authentication server, and user identity is verified based on the account and password. Local account authentication is applicable to the wireless office network environment.

2. Getting Started

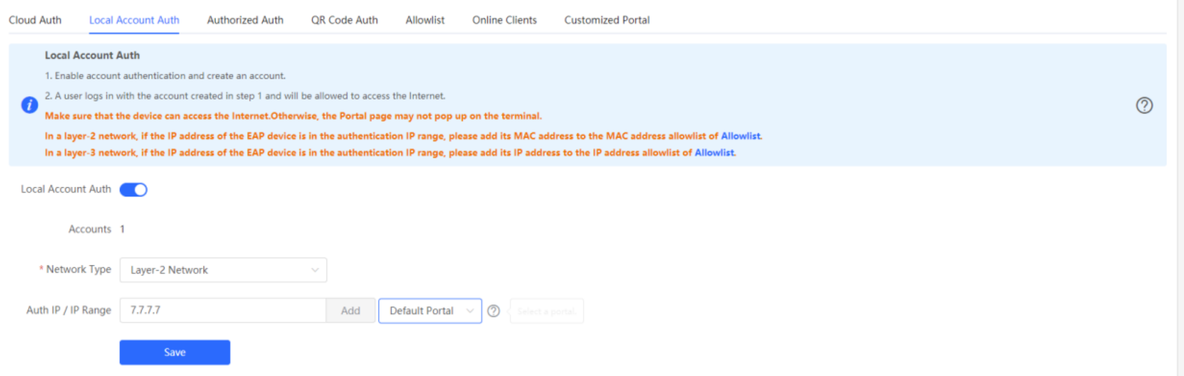
Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **Local Device** > **Advanced** > **Authentication** > **Local Account Auth**.

(1) Enable account authentication.

Turn on **Local Account Auth**, enter the IP address range of clients to be authenticated, and click **Save**. After account authentication is enabled, clients in the specified IP address range can access the Internet only after passing authentication.



Local Account Auth

1. Enable account authentication and create an account.

2. A user logs in with the account created in step 1 and will be allowed to access the Internet.

Make sure that the device can access the Internet.Otherwise, the Portal page may not pop up on the terminal.

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 allowlist of Allowlist.

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 allowlist of Allowlist.

Local Account Auth: on

Accounts 1

* Network Type: Layer-2 Network

Auth IP / IP Range: 7.7.7.7

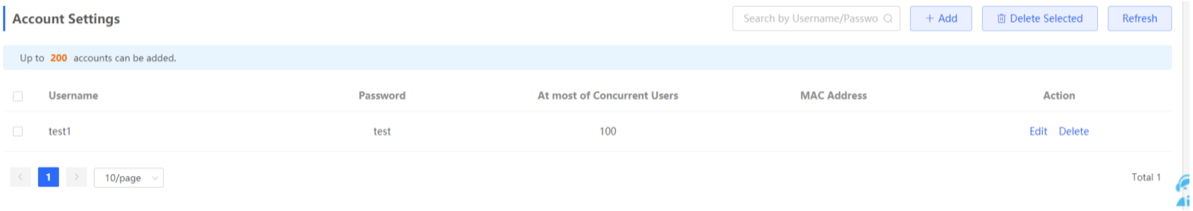
Note

You can select the default portal page or a customized portal page for local account authentication. See 4.10.12 Portal Customization for customizing a portal page.

(2) Configure an authentication account.

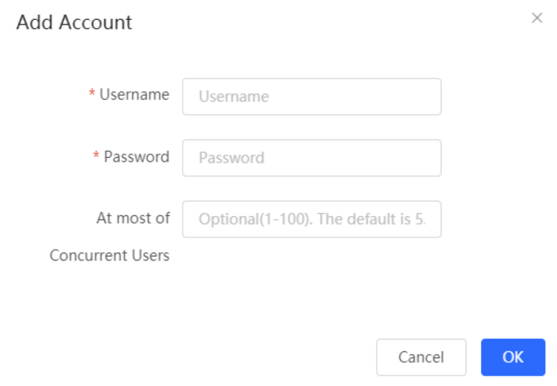
Click **Add** to configure an authentication account for Internet access. Multiple clients can access the Internet using the same account and password. The **Concurrent Users** parameter specifies the maximum number of users allowed to access the Internet using the same account.

After a **Wi-Fi user** passes authentication using an account, the IP address of the authenticated user is displayed in the **IP** column next to the account. The account list records a maximum of five latest device IP addresses using the same account.



Up to 200 accounts can be added.

□	Username	Password	At most of Concurrent Users	MAC Address	Action
□	test1	test	100		Edit Delete



Add Account

* Username: Username

* Password: Password

At most of Concurrent Users: Optional(1-100). The default is 5.

4. Verifying Configuration

After a client connects to the specific Wi-Fi, the authentication page pops up automatically. The user can normally access the Internet only after entering the account and password configured on the local server on the authentication page. You can choose **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 4.10.11 Online Authenticated User Management.

4.10.8 Authorized Guest Authentication

1. Overview

The device is connected to the local authentication server. After a guest connects to Wi-Fi, the guest can access the Internet after the specified authorization IP user or account and password authentication user scans the QR code that pops up for guest authentication. For example, in the wireless office network, users in the employee network segment are authorized to scan the guest authentication QR code for users in the guest network segment.

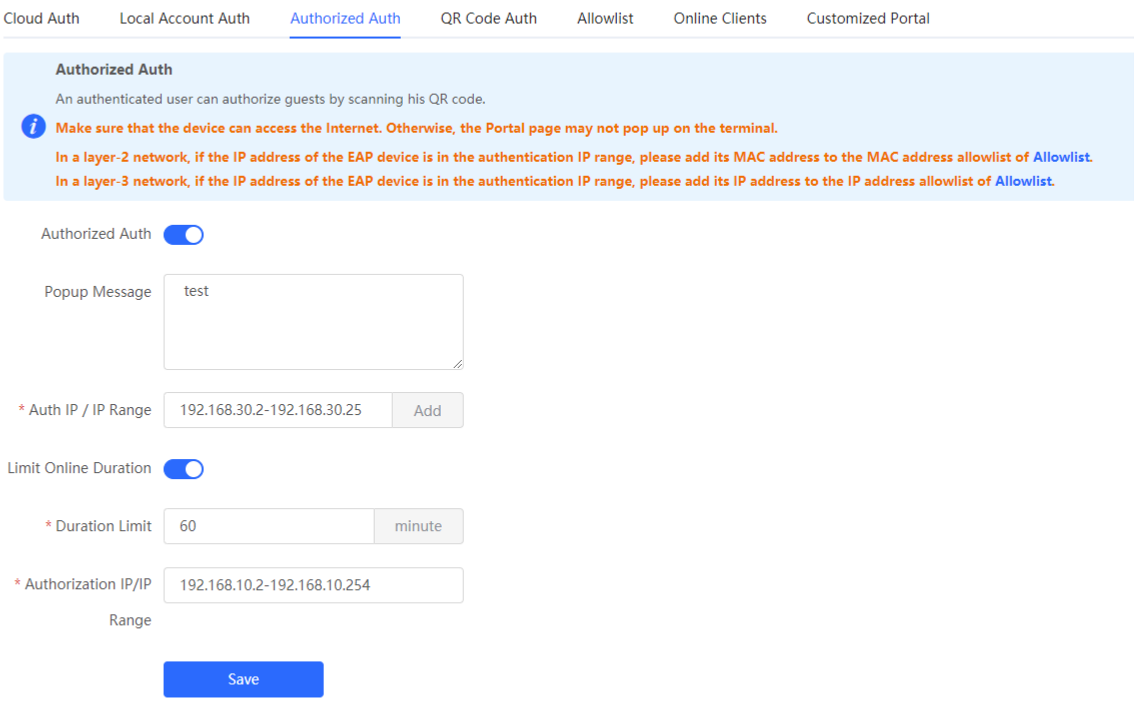
2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **Local Device** > **Advanced** > **Authentication** > **Authorized Auth**.

Turn on **Authorized Auth**, configure **Popup Message**, **Auth IP / IP Range**, **Authorization IP/IP Range**, and **Limit Online Duration**, and click **Save**.



Authorized Auth

An authenticated user can authorize guests by scanning his QR code.

Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.

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 allowlist of Allowlist.

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 allowlist of Allowlist.

Authorized Auth: on

Popup Message: test

* Auth IP / IP Range: 192.168.30.2-192.168.30.25 Add

Limit Online Duration: on

* Duration Limit: 60 minute

* Authorization IP/IP Range: 192.168.10.2-192.168.10.254

Table 4-12 **Authorized guest authentication configuration**

Parameter	Description
Popup Message	Specify the text to be displayed on the pop-up QR code page.
Auth IP / IP Range	Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication.
Limit Online Duration	Specify whether to limit the online duration of guests. After you enable this function, you need to configure **Duration Limit**. If the online duration of a guest exceeds the specified value, the guest can continue Internet access only after re-authorization. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration.
Duration Limit	Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authorized for login again.
Authorization IP/IP Range	Specify the IP address range of authorization users. Users in this range can scan the QR code to authorize guests.

4. Verifying Configuration

After a guest connects to Wi-Fi, the QR code authentication page pops up. The guest can access the Internet after the specified authorization user scans this QR code. You can choose **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 4.10.11 Online Authenticated User Management.

4.10.9 Guest Authentication Through QR Code Scanning

1. Overview

Guests scan the specified QR code to access the Internet. For example, in the wireless office network, guests scan the pasted QR code to access the Internet after they connect to Wi-Fi.

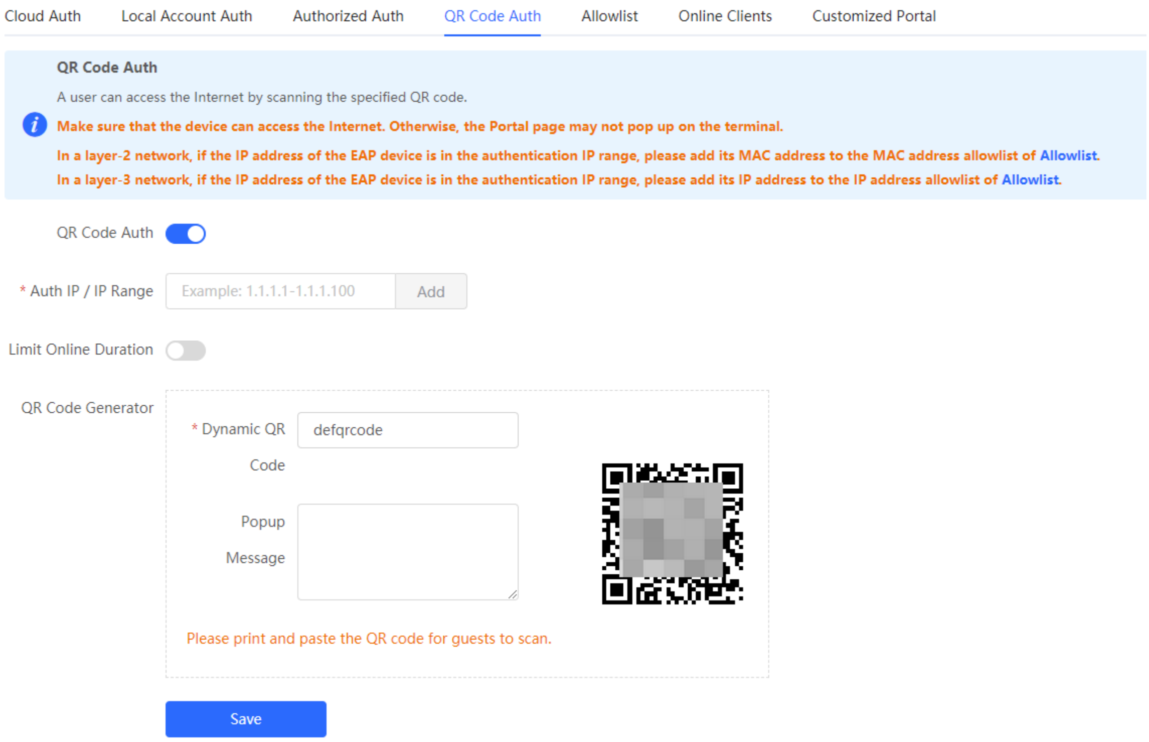
2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **Local Device** > **Advanced** > **Authentication** > **QR Code Auth**.

Turn on **QR Code Auth**, configure **Auth IP / IP Range**, **Limit Online Duration**, and **QR Code Generator**, and click **Save**.



QR Code Auth

A user can access the Internet by scanning the specified QR code.

Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.

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 allowlist of Allowlist.

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 allowlist of Allowlist.

QR Code Auth: On

* Auth IP / IP Range: Example: 1.1.1.1-1.1.1.100

Limit Online Duration: Off

QR Code Generator

* Dynamic QR Code: defqrcode

Popup Message:

Please print and paste the QR code for guests to scan.

Table 4-13 Guest authentication through QR code scanning configuration

Parameter	Description
Auth IP / IP Range	Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication.
Limit Online Duration	Specify whether to limit the online duration of guests. After you enable this function, you need to configure **Duration Limit**. If the online duration of a guest exceeds the specified value, the guest needs to scan the QR code again before continuing Internet access. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration.
Duration Limit	Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authenticated.
Dynamic QR Code	The dynamic QR code is used to generate a QR code image. After the dynamic QR code is updated, the QR code image changes and the previous image becomes invalid. You can print and paste the generated QR code image, which can be scanned by guests to access the Internet.
Popup Message	Specify the QR code prompt message displayed on the page after a guest scans the QR code.

4. Verifying Configuration

After a client connects to Wi-Fi, the guest can scan the QR code to pass authentication and access the Internet. You can choose **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 4.10.11 Online Authenticated User Management.

4.10.10 Authentication-Free

1. Overview

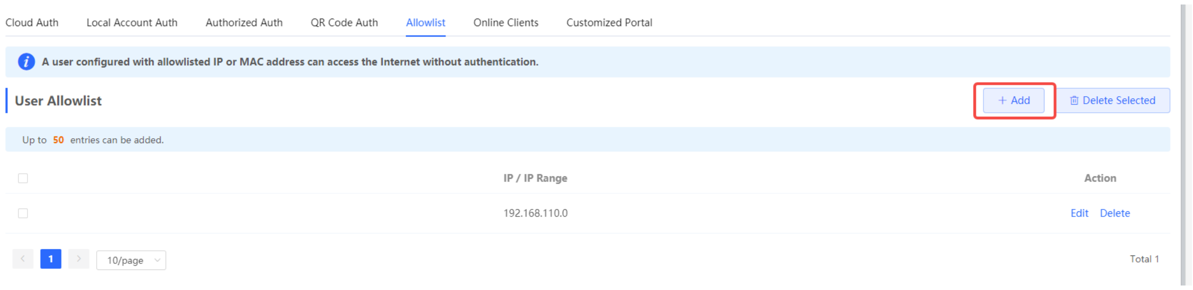
After IP addresses or MAC addresses are configured for authentication-free users, they can directly access the Internet without passing authentication. Traffic from all the users in the blocklist is blocked.

2. Configuring an Authentication-Free User

Choose **Local Device** > **Advanced** > **Authentication** > **Allowlist** > **User Allowlist**.

Authentication-free user: Users in the specified IP address range can directly access the Internet without passing authentication.

Click **Add** to configure the IP address range for authentication-free users. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). A maximum of 50 entries are supported.



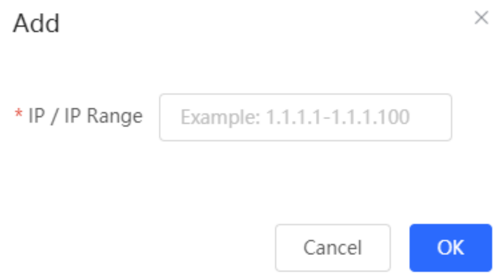
A user configured with allowlisted IP or MAC address can access the Internet without authentication.

User Allowlist

Up to 50 entries can be added.

□	IP / IP Range	Action
□	192.168.110.0	Edit Delete

Total 1



Add

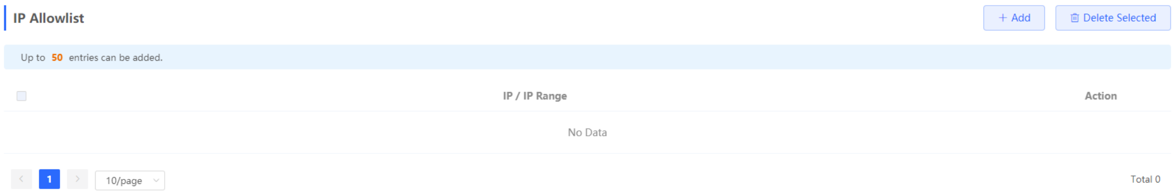
* IP / IP Range: Example: 1.1.1.1-1.1.1.100

3. Configuring Extranet IP Addresses for Authentication-Free

Choose **Local Device** > **Advanced** > **Authentication** > **Allowlist** > **IP Allowlist**.

Extranet IP address for authentication-free: Specify the IP addresses that can be assessed by all users including unauthenticated users.

Click **Add** to configure extranet IP addresses that can be assessed by users without authentication. A maximum of 50 entries are supported.

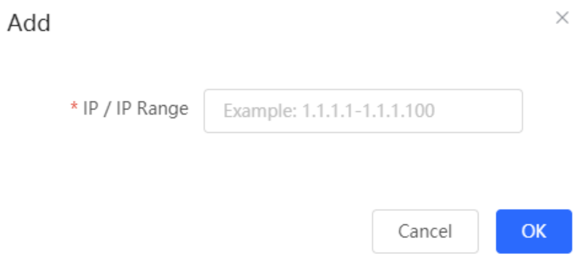


IP Allowlist

Up to 50 entries can be added.

□	IP / IP Range	Action
	No Data	

Total 0



Add

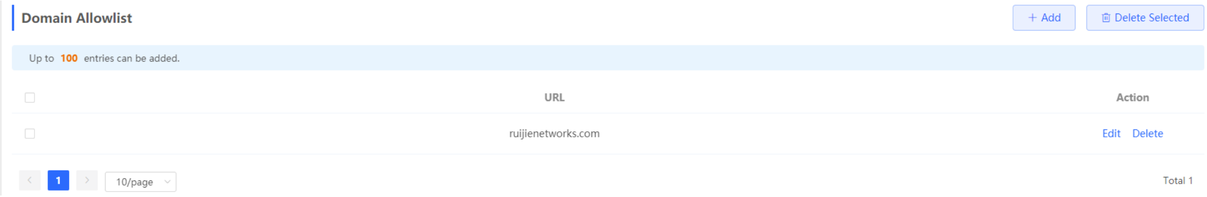
* IP / IP Range: Example: 1.1.1.1-1.1.1.100

4. Configuring a Domain Allowlist

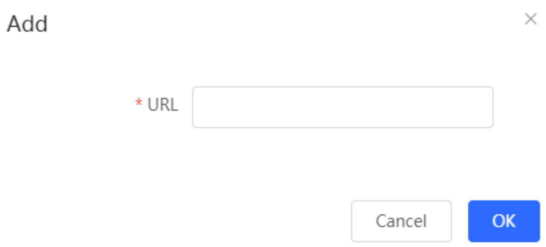
Choose **Local Device** > **Advanced** > **Authentication** > **Allowlist** > **Domain Allowlist**.

Domain Allowlist: Specify the URLs that can be accessed without authentication.

Click **Add**. In the dialog box that appears, enter the authentication-free URLs, and then click OK. When the destination URL of the user is in the **Domain Allowlist**, traffic from the user will be permitted directly, regardless of whether the user passes authentication. A maximum of 100 entries are supported.



□	URL	Action
□	ruijienetworks.com	Edit Delete

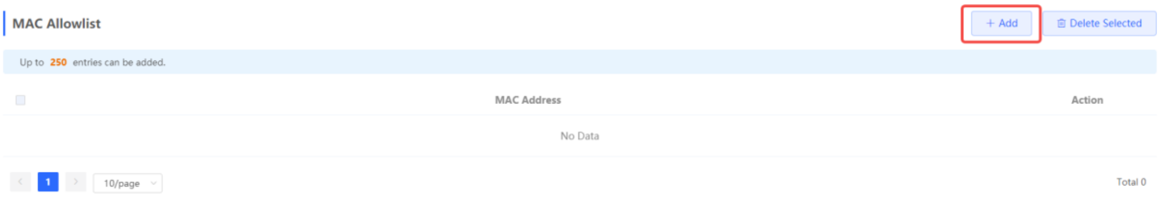


5. Configuring a MAC Allowlist

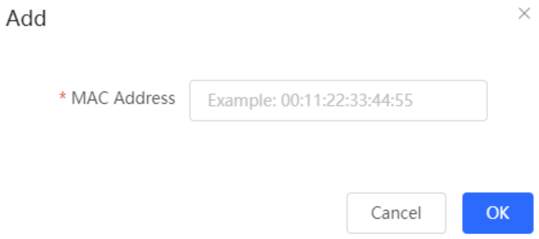
Choose **Local Device** > **Advanced** > **Authentication** > **Allowlist** > **MAC Allowlist**.

MAC Allowlist: Clients whose MAC addresses are in the allowlist can access the Internet through Wi-Fi without the need for authentication.

Click **Add**. In the dialog box that appears, enter the MAC addresses of authentication-free users, and then click **OK**. A maximum of 250 entries are supported.



□	MAC Address	Action
	No Data	

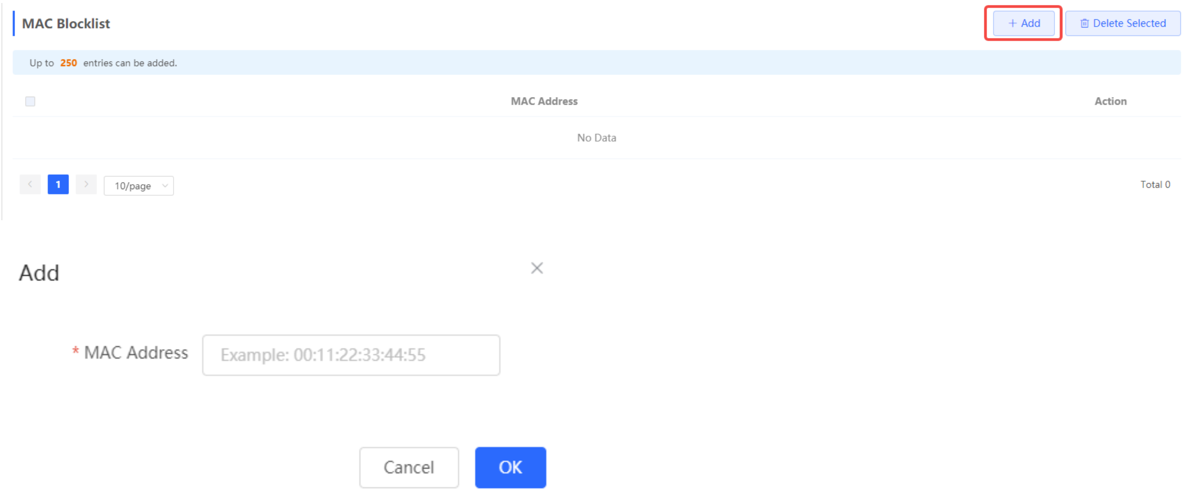


6. Configuring a User MAC Blocklist

Choose **Local Device** > **Advanced** > **Authentication** > **Allowlist** > **MAC Blocklist**.

MAC Blocklist: Clients whose MAC addresses are in the blocklist are prohibited from accessing the Internet.

Click **Add**. In the dialog box that appears, enter the MAC addresses of users in the blocklist, and then click **OK**. A maximum of 250 entries are supported.

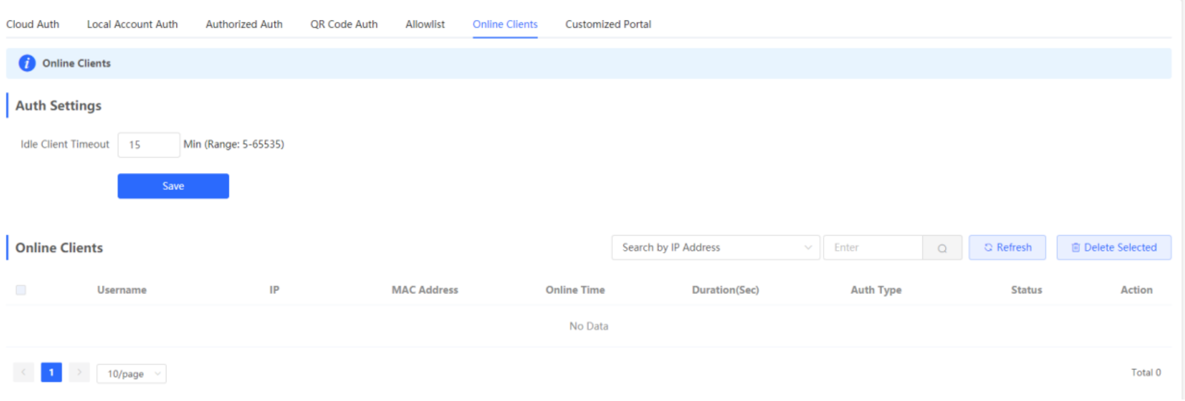


4.10.11 Online Authenticated User Management

1. Configuring the Idle Client Timeout Period

Choose **Local Device** > **Advanced** > **Authentication** > **Online Clients**.

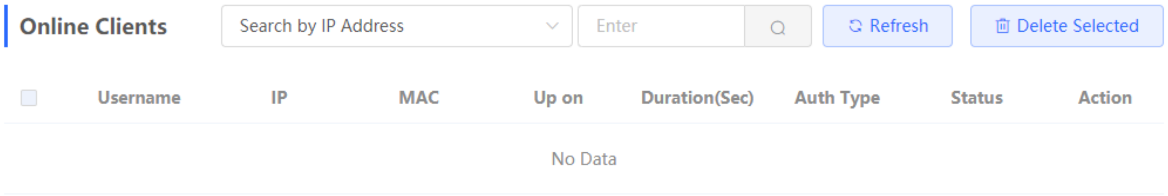
You can configure the idle client timeout period. The default value is 15 minutes. If no traffic from an online user passes through the device within the specified period, the device will force the user offline. The user can continue Internet access only after re-authentication.



Idle Client Timeout 15 Min (Range: 5-65535)

2. Kicking a User Offline

The online client list displays information about all the current online clients, including the client IP address, client MAC address, login time, and authentication mode. You can find the 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 kick the client off and disconnect the Wi-Fi connection of the client.

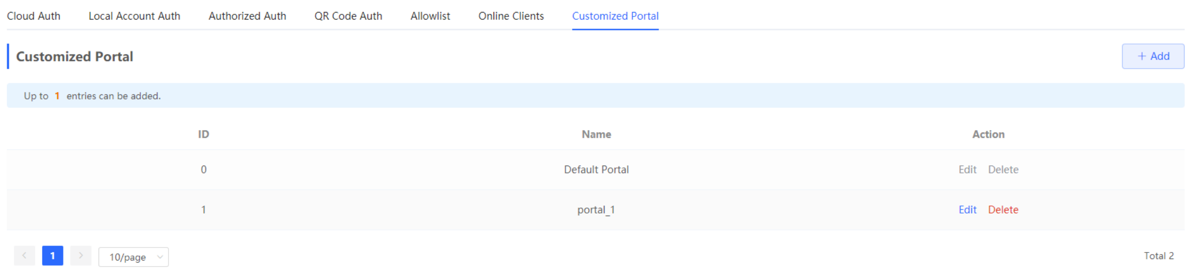


4.10.12 Portal Customization

Choose **Local Device** > **Advanced** > **Authentication** > **Customized Portal**.

Customize the information on a portal page as required through a captive portal. A customized portal page is used for local account authentication.

The system has a piece of default portal information. Click **Edit** to customize the portal information.

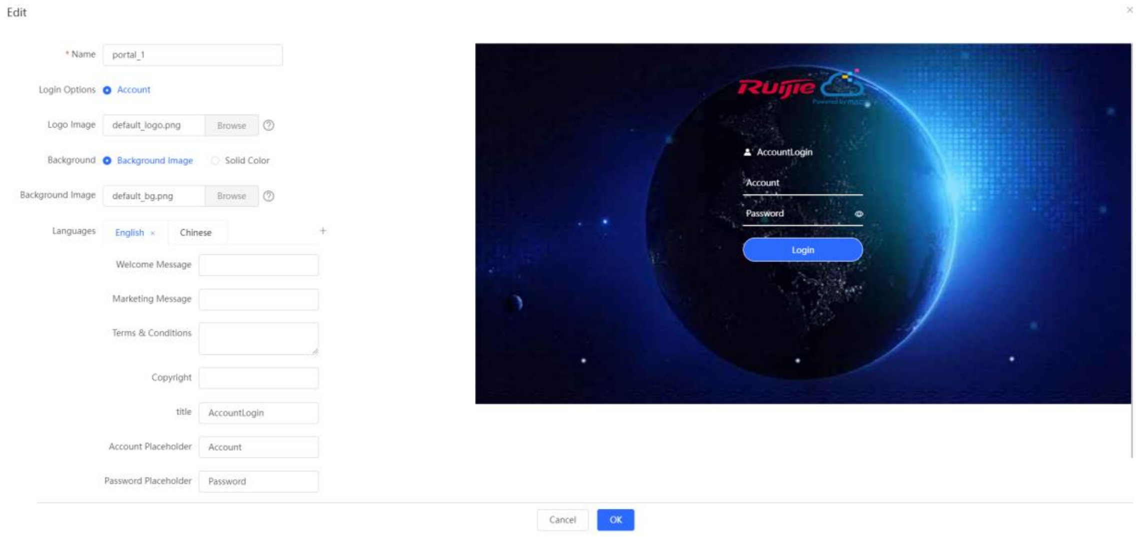


Customized Portal

Up to 1 entries can be added.

ID	Name	Action
0	Default Portal	Edit Delete
1	portal_1	Edit Delete

Total 2



* Name: portal_1

Login Options: ● Account

Logo Image: default_logo.png

Background: ● Background Image ○ Solid Color

Background Image: default_bg.png

Languages: English × Chinese +

Welcome Message:

Marketing Message:

Terms & Conditions:

Copyright:

title: AccountLogin

Account Placeholder: Account

Password Placeholder: Password

4.11 Wireless Authentication

Note

The function is supported by EG310G-E, EG305GH-E, and EG310GH-E.

4.11.1 Overview

Use the wireless authentication function to perform authentication configuration for the AP connected to the gateway. After users connect to the Wi-Fi signals released by the AP, the traffic will not be directly routed to the Internet. Wi-Fi users must pass authentication before accessing network resources.

Note

- The EG series router supports egress authentication. When an EG router is used independently, you are advised to use the authentication function of the router. Log in to the Eweb of the EG router. Choose **Local Device** > **Advanced** > **Authentication**. For details, see 4.10 Wi-Fi Authentication.
- When the EG router connects to the AP, the **Wireless Auth** action entry point appears on the **Network** page but not on the **Local Device** page.

4.11.2 Configuring Captive Portal on Ruijie Cloud

1. Prerequisites

If you want to configure **SMS Authentication** on Ruijie Cloud, please add a Twilio account first.

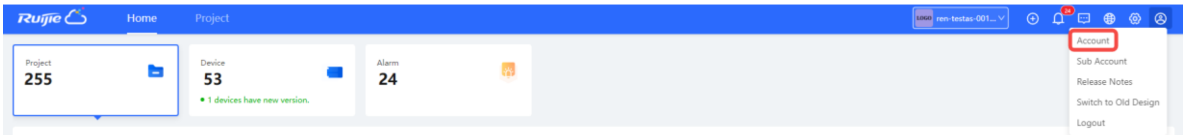
A Twilio account has been applied for from the Twilio official website (https://www.twilio.com/login).

Note

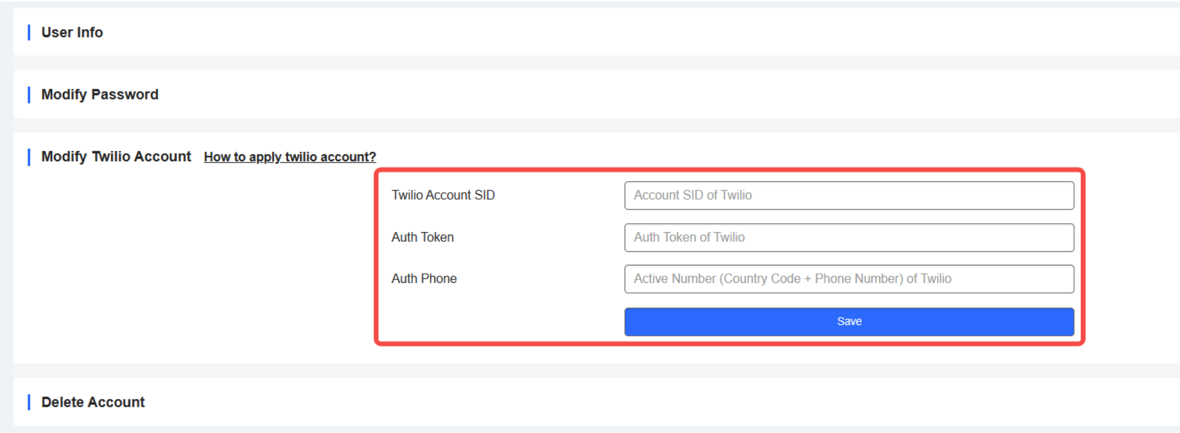
A Twilio account is used to send the SMS verification code.

Configuration Steps

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



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



User Info

Modify Password

Modify Twilio Account How to apply twilio account?

Twilio Account SID: Account SID of Twilio

Auth Token: Auth Token of Twilio

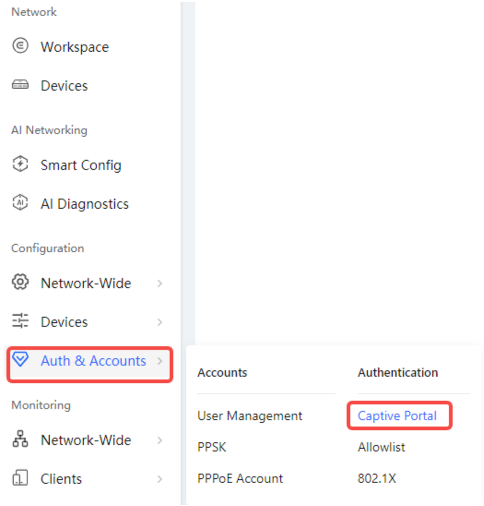
Auth Phone: Active Number (Country Code + Phone Number) of Twilio

Save

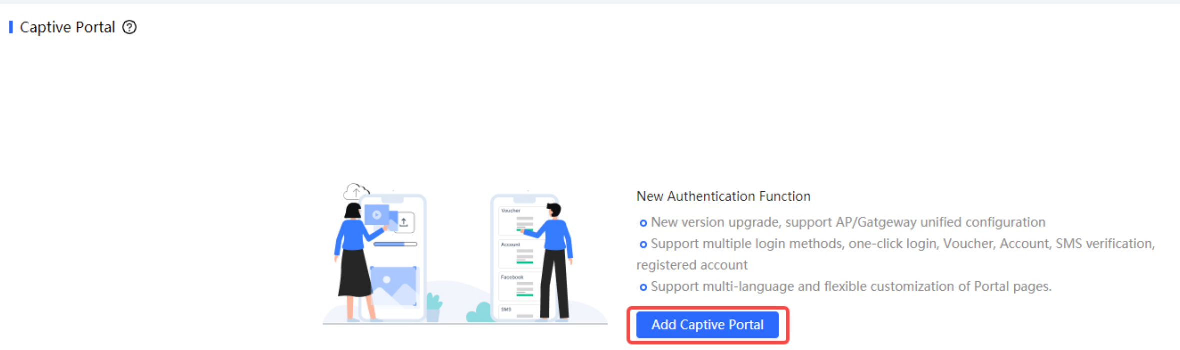
Delete Account

2. Configuring a Portal Page

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



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

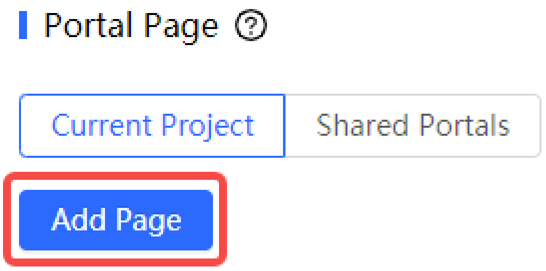


Captive Portal

New Authentication Function

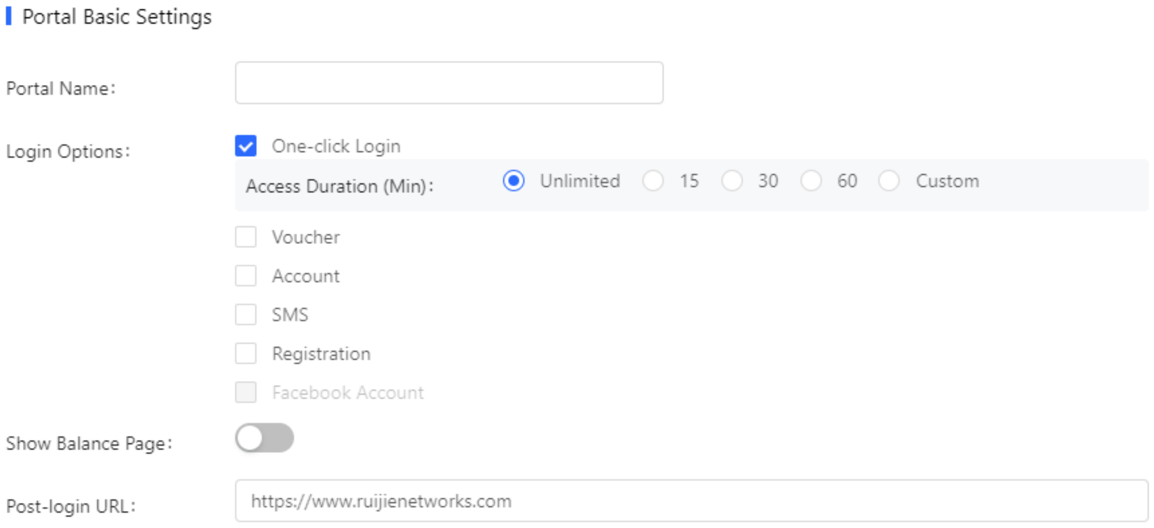
- New version upgrade, support AP/Gatgeway unified configuration
- Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account
- Support multi-language and flexible customization of Portal pages.

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



Portal Page

(4) Configure basic information of the portal template.



Portal Basic Settings

Portal Name:

Login Options: ☑ One-click Login

Access Duration (Min): ● Unlimited ○ 15 ○ 30 ○ 60 ○ Custom

☐ Voucher

☐ Account

☐ SMS

☐ Registration

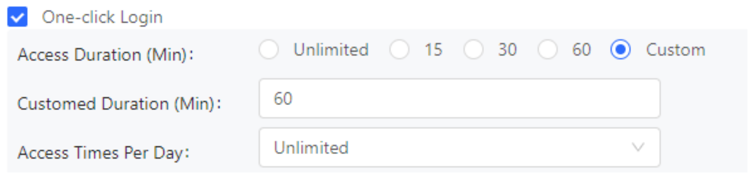
☐ Facebook Account

Show Balance Page:

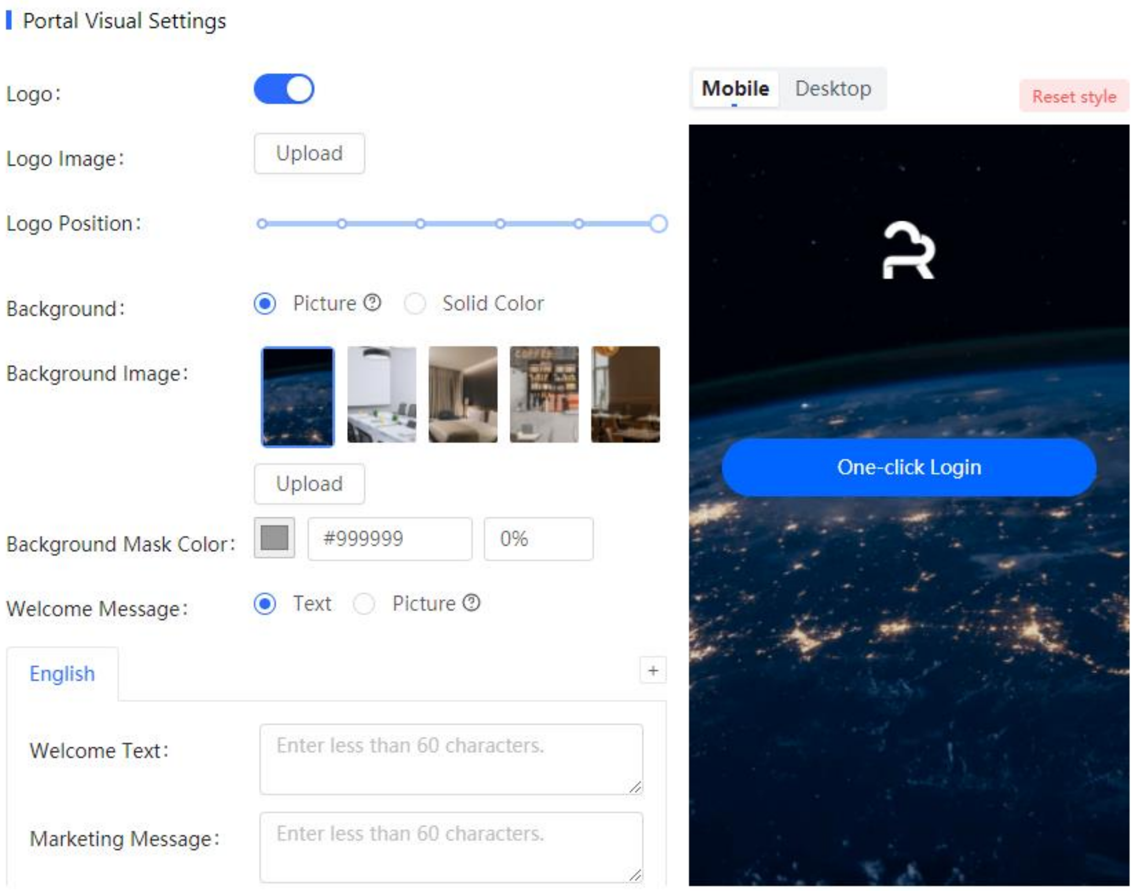
Post-login URL: https://www.ruijienetworks.com

Table 4-14 Basic Information of the Portal Settings

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

Parameter	Description
Login Options	Indicates the option to perform the desired action. ● **One-click Login**: indicates login without the username and password. You can set **Access Duration** and **Access Times Per Day**.  ☑ One-click Login Access Duration (Min): ○ Unlimited ○ 15 ○ 30 ○ 60 ● Custom Customed Duration (Min): 60 Access Times Per Day: Unlimited ● **Voucher**: indicates login with a random eight-digit password. ● **Account**: indicates login with the account and password. ● **SMS**: indicates login with the phone number and code. ● **Registration**: Facebook Account: indicates login with the Facebook account.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) Configure visual settings of the portal template.



Portal Visual Settings

Logo: ●

Logo Image: Upload

Logo Position:

Background: ● Picture ○ Solid Color

Background Image:

Upload

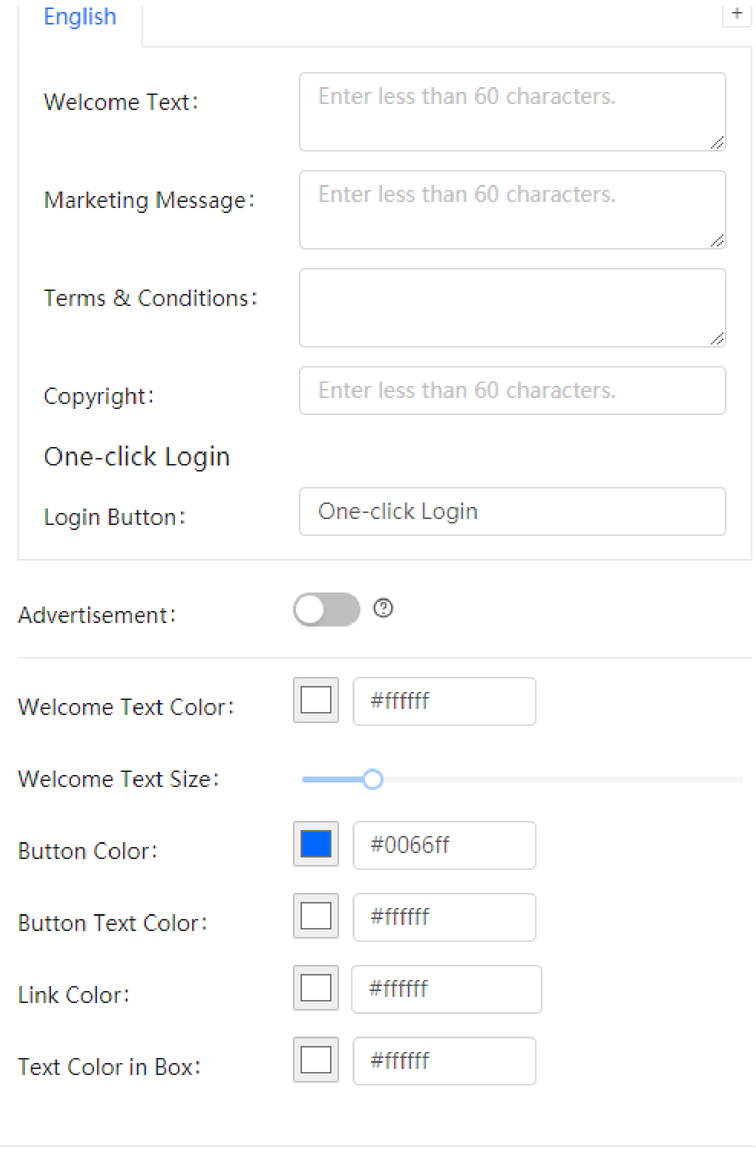
Background Mask Color: #999999 0%

Welcome Message: ● Text ○ Picture

English

Welcome Text: Enter less than 60 characters.

Marketing Message: Enter less than 60 characters.



English +

Welcome Text: Enter less than 60 characters.

Marketing Message: Enter less than 60 characters.

Terms & Conditions:

Copyright: Enter less than 60 characters.

One-click Login

Login Button: One-click Login

Advertisement: ⓘ

Welcome Text Color: □ #ffffff

Welcome Text Size:

Button Color: 🟦 #0066ff

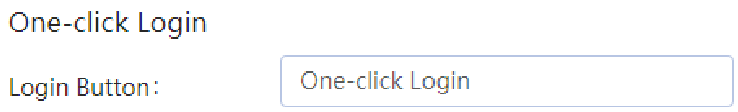
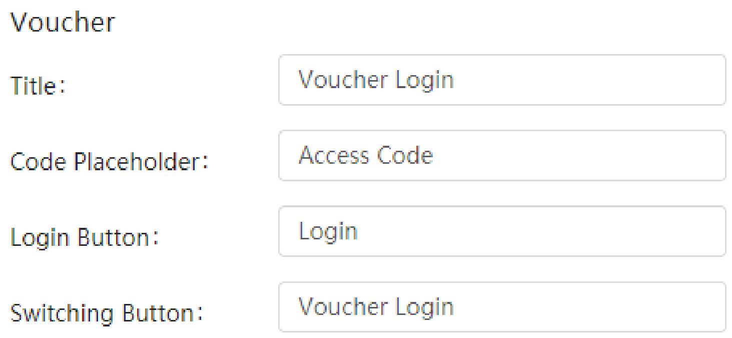
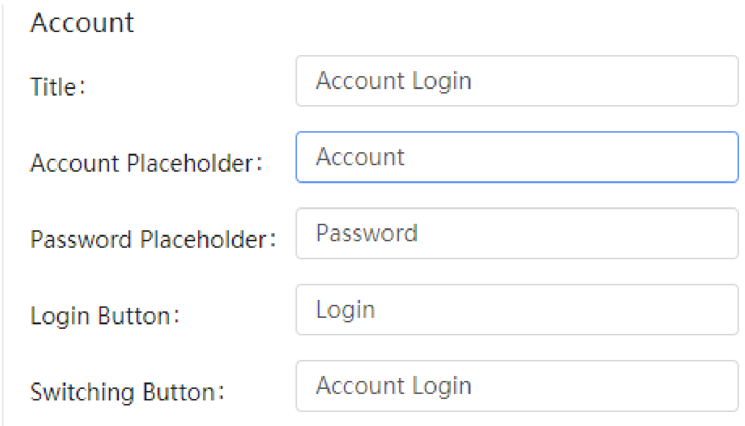
Button Text Color: □ #ffffff

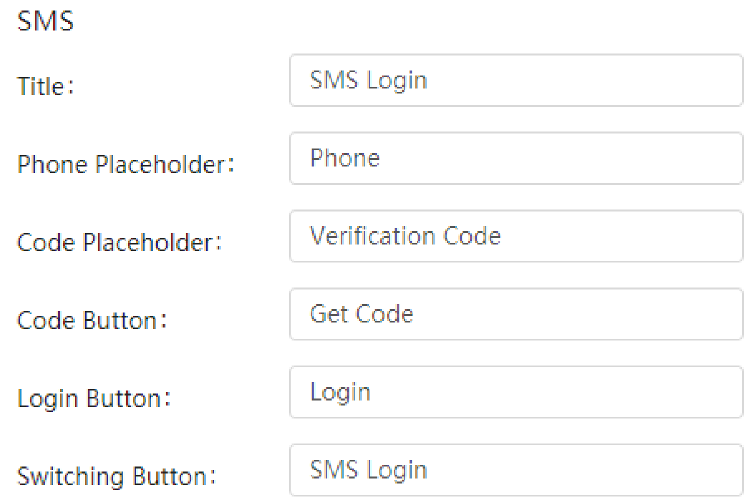
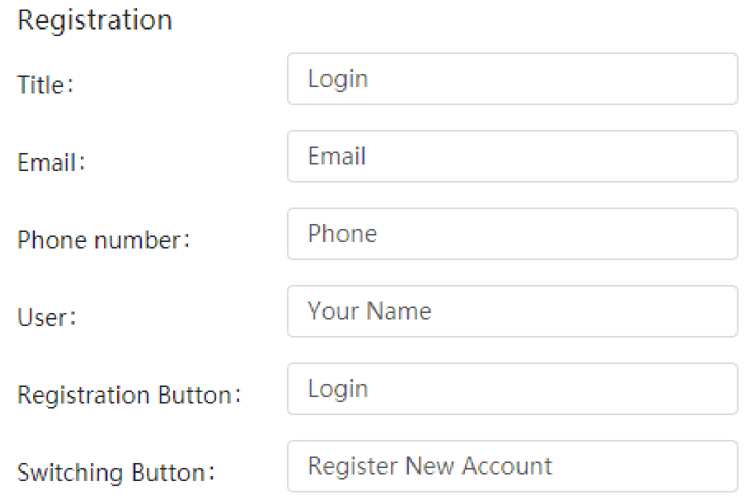
Link Color: □ #ffffff

Text Color in Box: □ #ffffff

Table 4-15 Visual Settings of the Portal Page

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When **Logo** is set to **Image**, upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.
Background Image	When **Background** is set to **Image**, upload the background image or select the default image.
Background Mask Color	When **Background** is set to **Solid Color**, configure the background color. The default value is **#ffffff**.
Welcome Message	Select the welcome message with the image or text.

Language	Select the language of the portal page and configure the content displayed on the portal page as required. You can click + to add portal pages in other languages. ● Welcome Text: Select the welcome message with the image or text. ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● One-click Login: After One-click Login is enabled, you can customize the button name displayed on the portal page, which is set to One-click Login by default.  One-click Login Login Button: One-click Login ● Voucher Login: After Voucher Login is enabled, you can customize the names of controls related to voucher authentication.  Voucher Title: Voucher Login Code Placeholder: Access Code Login Button: Login Switching Button: Voucher Login ● Account Login: After Account Login is enabled, you can customize the names of the controls related to account authentication.  Account Title: Account Login Account Placeholder: Account Password Placeholder: Password Login Button: Login Switching Button: Account Login ● SMS Login: After SMS Login is enabled, you can customize the names of the controls related to SMS authentication.

Parameter	Description
	 SMS Title: SMS Login Phone Placeholder: Phone Code Placeholder: Verification Code Code Button: Get Code Login Button: Login Switching Button: SMS Login ● Registration: After Registration is enabled, you can customize the names of the controls related to register new account.  Registration Title: Login Email: Email Phone number: Phone User: Your Name Registration Button: Login Switching Button: Register New Account
Advertisement	Select whether to display the advertisement.
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Text Size	Select the welcome text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

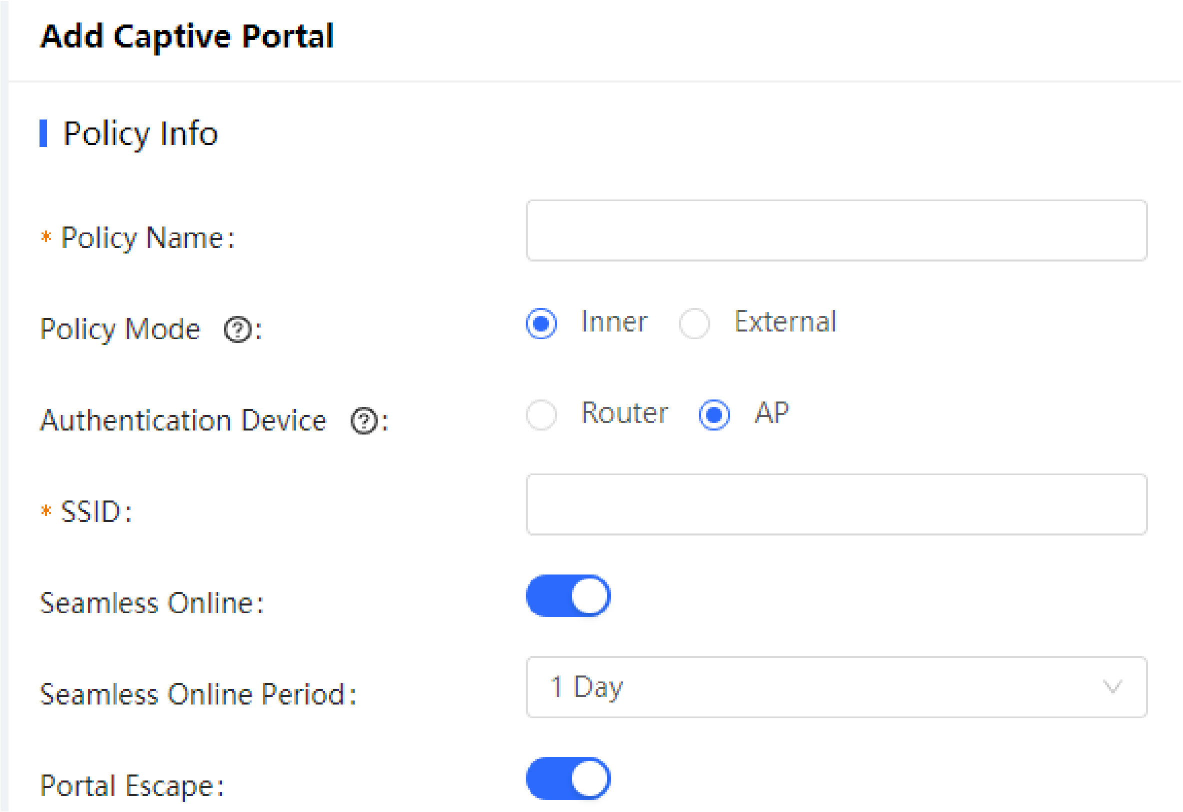
(6) After the configuration, click **OK** to save the portal template configurations.

3. Configuring Policy Info

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

Note

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



Add Captive Portal

Policy Info

* Policy Name:

Policy Mode ⓘ: ● Inner ○ External

Authentication Device ⓘ: ○ Router ● AP

* SSID:

Seamless Online: ●

Seamless Online Period: 1 Day

Portal Escape: ●

Table 4-16 Basic Information of the Captive Portal

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

Parameter	Description
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the NAS. Router: A router or gateway acts as the NAS responsible for performing authentication at the gateway exit. Reyee AP Authentication: RAP/EWR, ReyeeOS 1.219 or later version. Reyee EG WiFiDog Authentication: EG/EGW, ReyeeOS 1.202 or later version. Reyee EG Local Authentication: EG210G-E, EG210G-P-E, EG310GH-E, EG310GH-P-E, EG305GH-E, EG305GH-P-E, ReyeeOS 1.230 or later version. This parameter is not required if the policy mode is Local.
Network	Indicates the wired network that requires authentication. Enter the network segment in this field. Users connecting to the wired network corresponding to this network segment must be authenticated. This parameter is required if the Authentication Device is Router.
SSID	Indicates the network name of the Wi-Fi network that requires authentication. Users connecting to this wireless network must be authenticated. This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
Portal Page	Indicates the portal page that is displayed after portal authentication. Click Current Project to select the portal page for an existing project. Click Shared Portals to select an existing portal page. Click Add Page to customize a portal page.

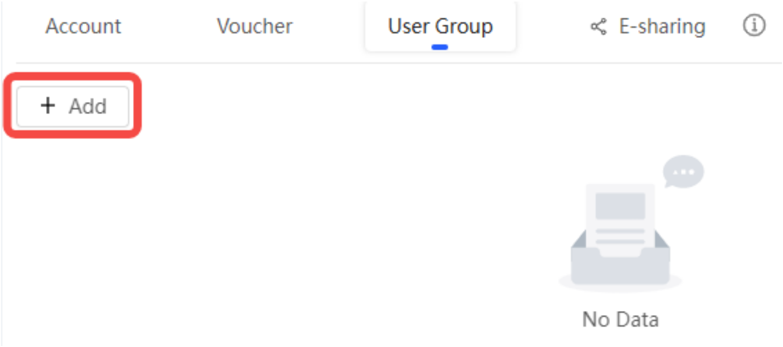
4. (Optional) Adding a Voucher

If the **Login Options** is **Voucher**, you should configure a voucher as the following steps.

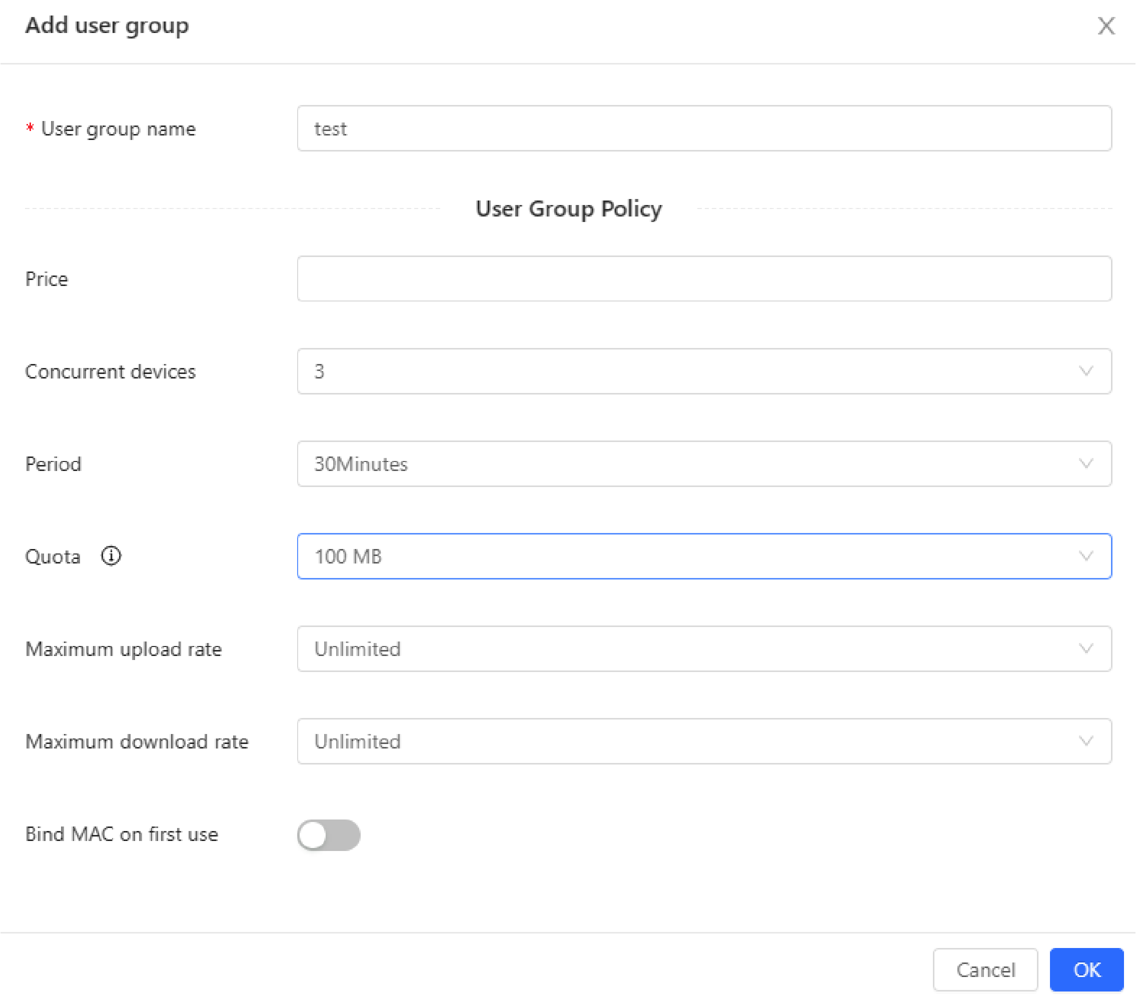
(1) Log in to Ruijie Cloud, choose **Project** > **Authentication** > **User Management**, **and** select a network in this account**.**

(2) Configure a user group.

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



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


Add user group

* User group name: test

User Group Policy

Price:

Concurrent devices: 3

Period: 30Minutes

Quota: 100 MB

Maximum upload rate: Unlimited

Maximum download rate: Unlimited

Bind MAC on first use

User Group Name: indicates the user group name.

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

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

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

Quota: indicates the maximum amount of data transfer.

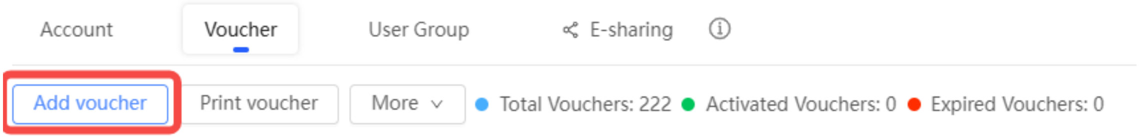
Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

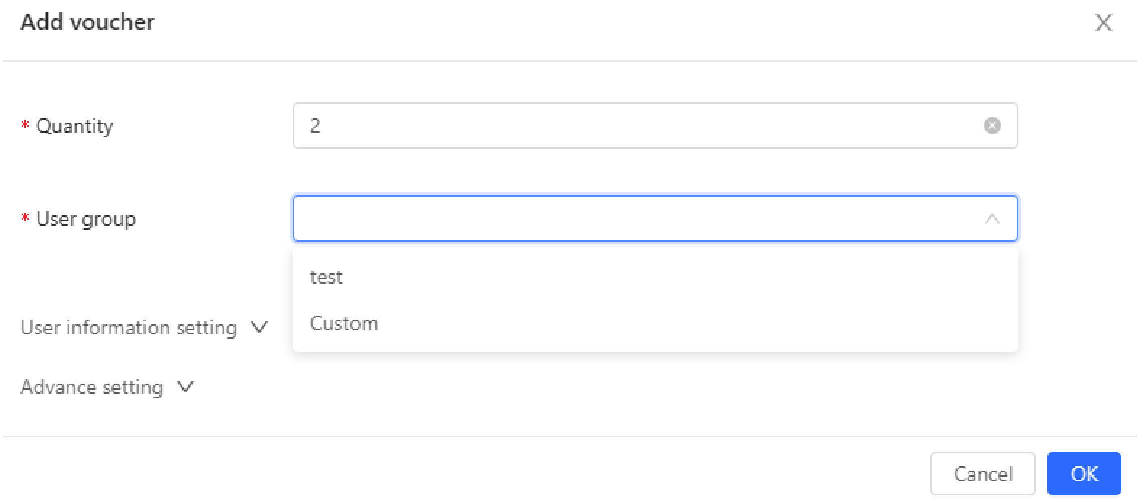
Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) Configure a voucher.

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



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



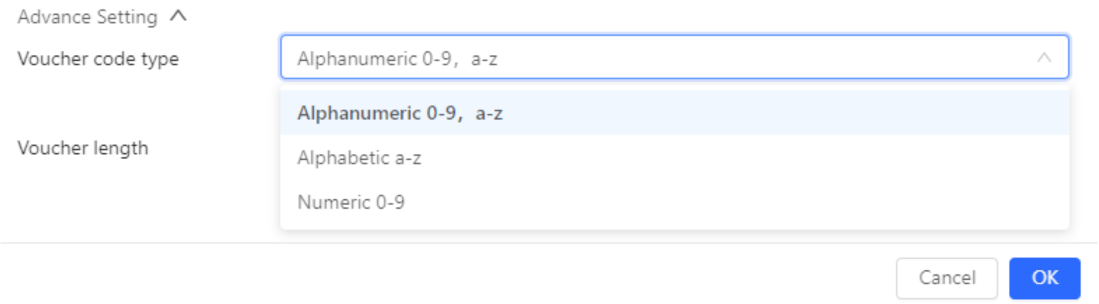
Quantity: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the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

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

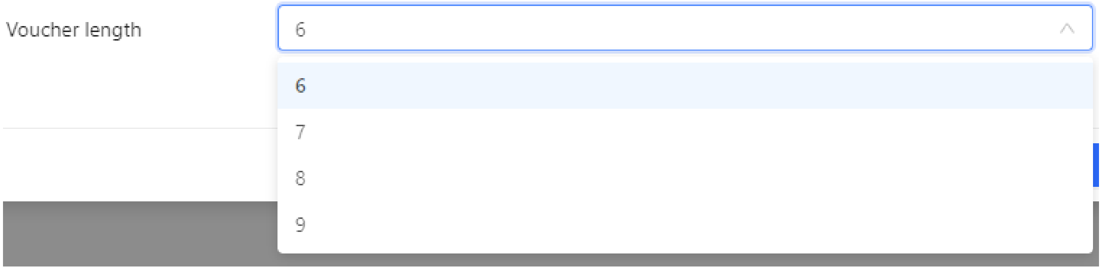
User information setting: Configure user information, which is optional.

Advance setting:

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



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



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

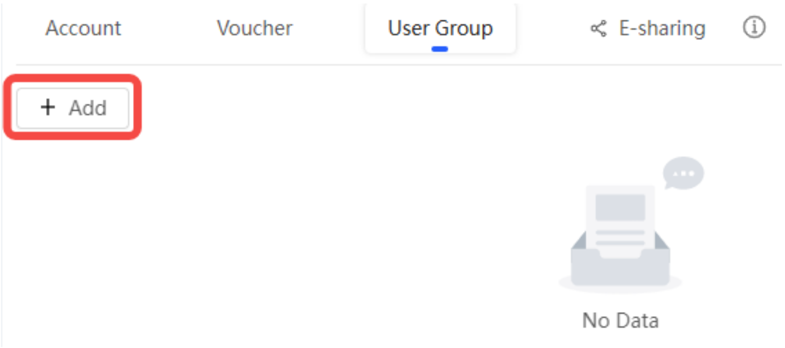
5. (Optional) Adding an Account

If the Login Options is **Account**, you should add accounts as the following steps. following steps.

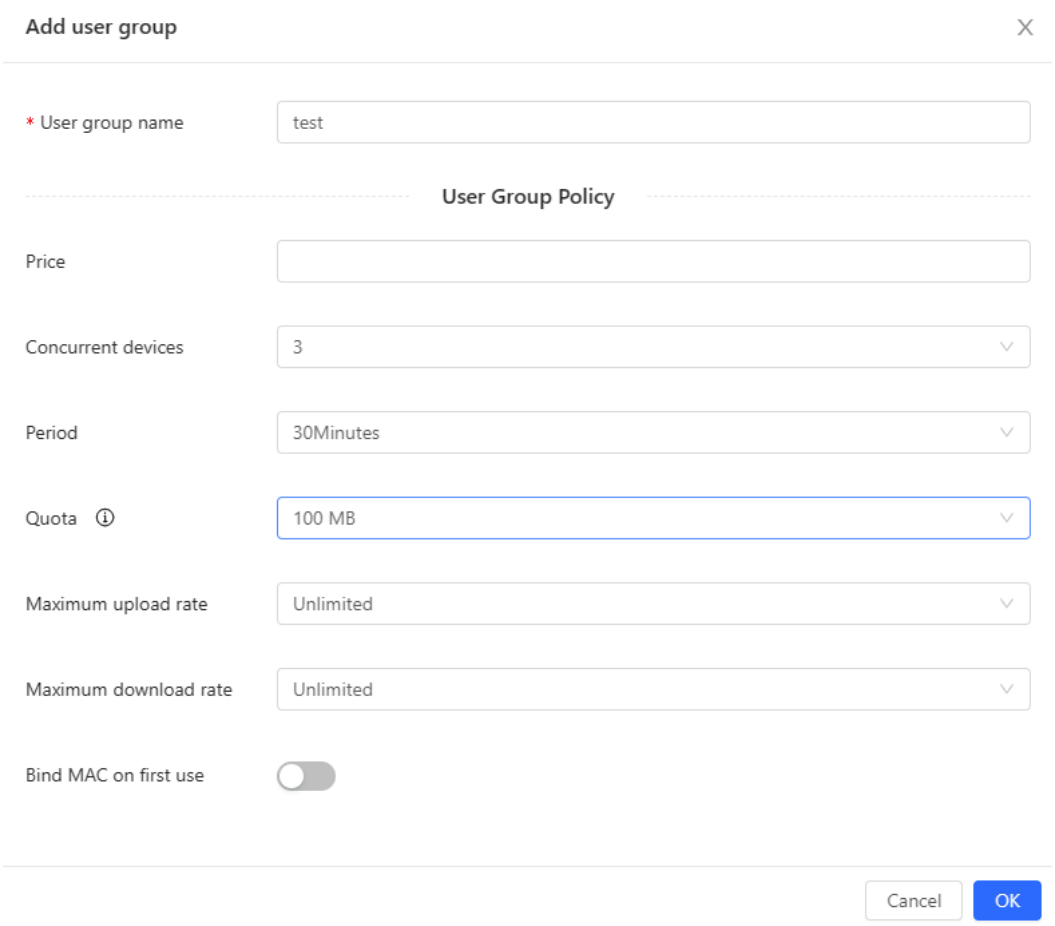
(1) Log in to Ruijie Cloud, choose **Project** > **Authentication** > **User Management**, and select a network in this account**.**

(2) Configure a user group.

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



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



Add user group

* User group name: test

User Group Policy

Price:

Concurrent devices: 3

Period: 30Minutes

Quota: 100 MB

Maximum upload rate: Unlimited

Maximum download rate: Unlimited

Bind MAC on first use: ○

User Group Name: indicates the user group name.

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

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

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

Quota: indicates the maximum amount of data transfer.

Maximum upload rate: indicates the maximum upload rate.

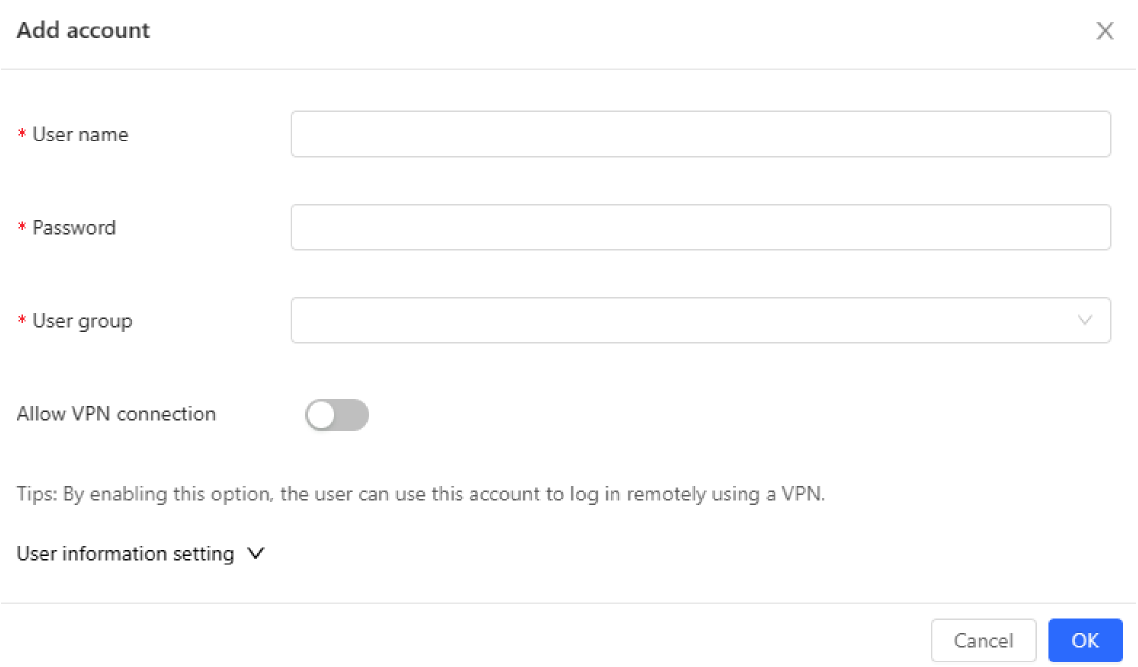
Maximum download rate: indicates the maximum download rate.

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

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

- Adding an account manually

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



Add account

* User name

* Password

* User group

Allow VPN connection

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

User information setting

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

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

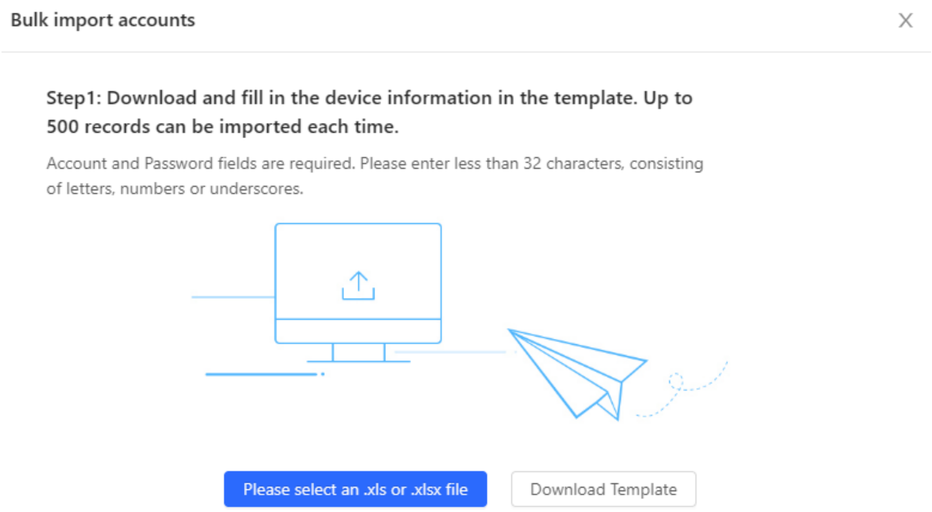
User group: **Select a created user group from the drop-down list. If the created user group does not meet the requirements, click Custom to create a user group.**

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

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

- Adding accounts through batch import

a Click **Bulk import**.



Bulk import accounts

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

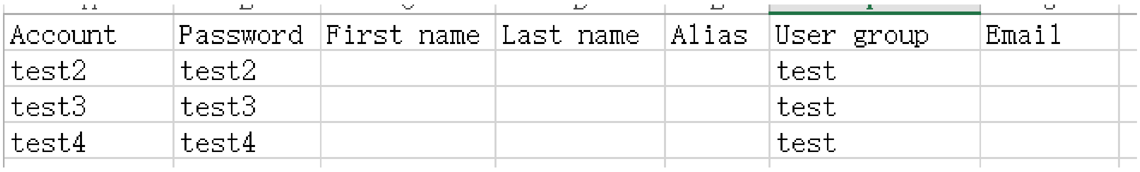
Account and Password fields are required. Please enter less than 32 characters, consisting of letters, numbers or underscores.

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

c Edit the template and save it.

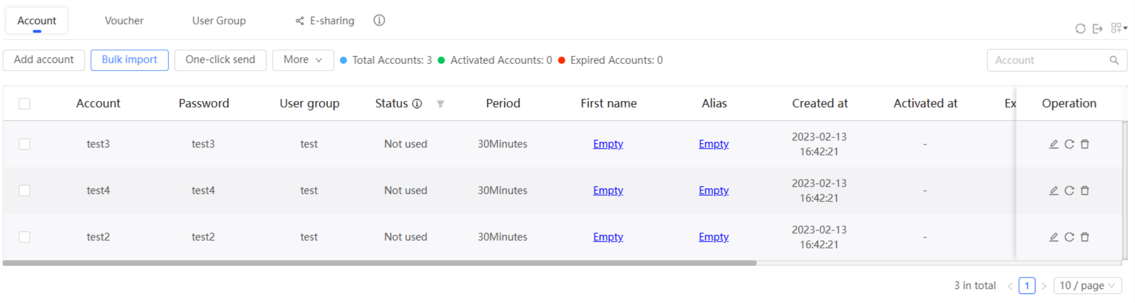
Note

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



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

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



Total Accounts: 3 Activated Accounts: 0 Expired Accounts: 0

□	Account	Password	User group	Status	Period	First name	Alias	Created at	Activated at	Ex	Operation
□	test3	test3	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		
□	test4	test4	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		
□	test2	test2	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		

3 in total < 1 > 10 / page

4.11.3 Configuring an Authentication-Free Account on Eweb Management System

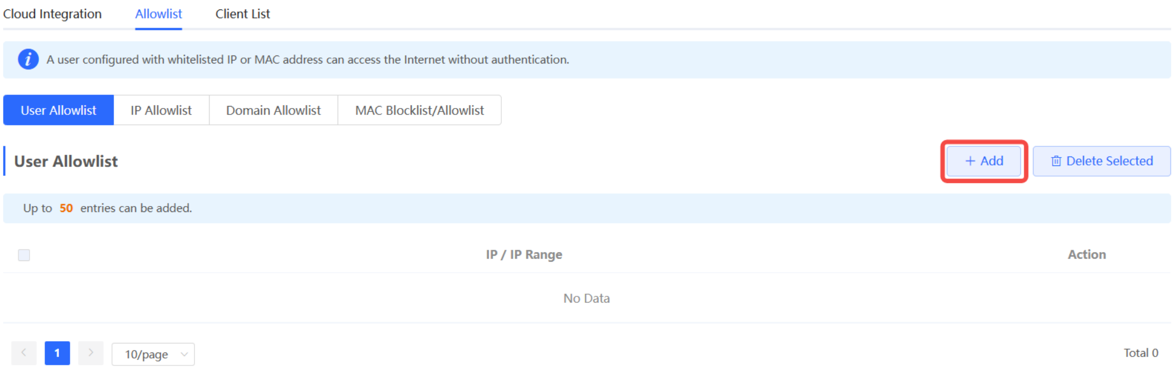
1. Configuring an Authentication-Free Account

The authentication-free user can access the Internet without authentication.

Choose **Networkwide Management** > **Network** > **Wireless Auth** > **Allowlist**.

(1) Click **User Allowlist**.

(2) Click **Add**.



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

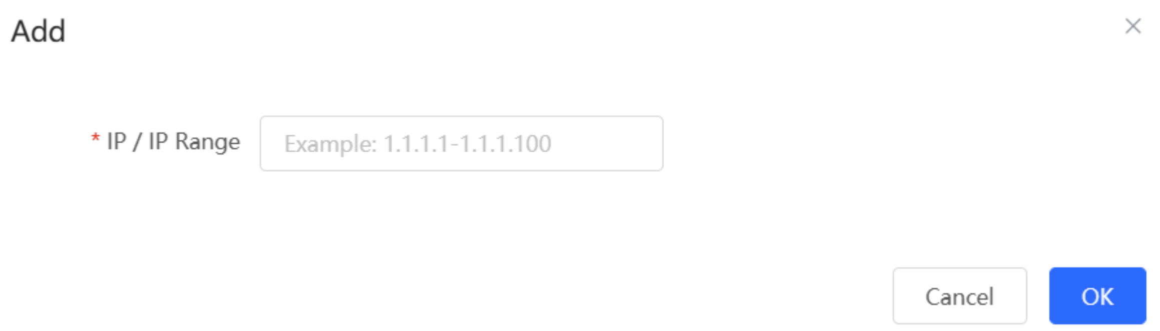
User Allowlist

Up to 50 entries can be added.

□	IP / IP Range	Action
	No Data	

< 1 > 10/page Total 0

(3) Configure the IP address or IP address range for authentication-free users.



(4) Click **OK**.

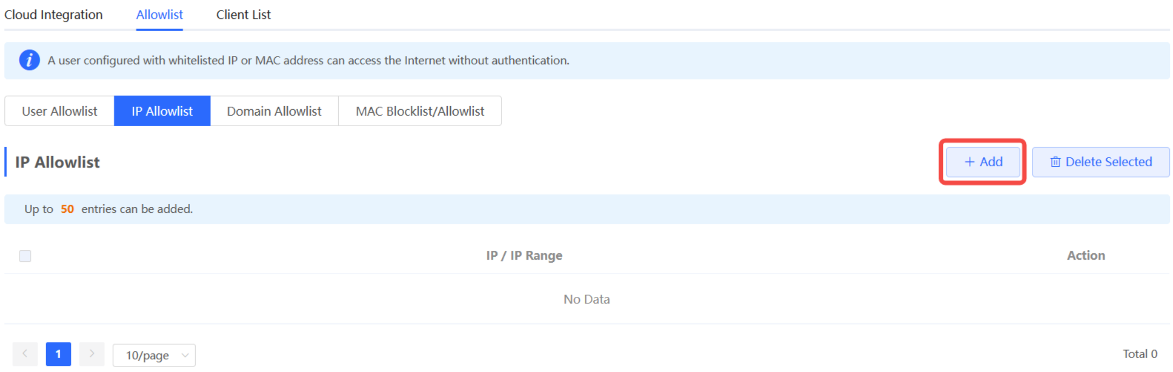
2. Configuring Authentication-Free External IP Addresses

After configuration, the user can access the authentication-free external IP address without authentication.

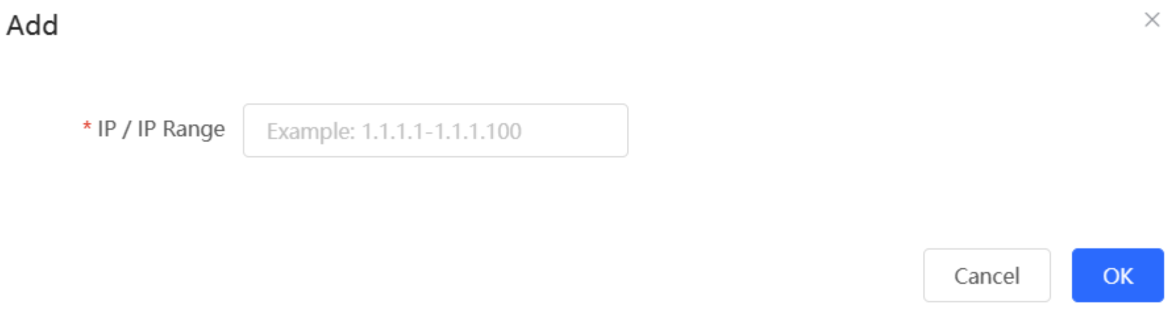
Choose **Networkwide Management > Network** > **Wireless Auth** > **Allowlist**.

(1) Click **IP Allowlist**.

(2) Click **Add**.



(3) Configure authentication-free external IP address or IP address range.



(4) Click **OK**.

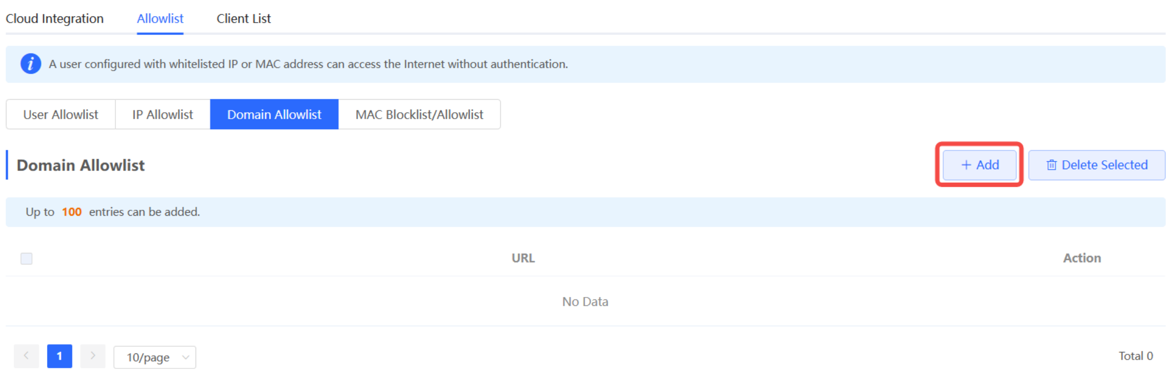
3. Configuring a Domain Allowlist

The user can access the URL in the domain allowlist without authentication.

(1) Choose **Networkwide Management > Network > Wireless Auth > Allowlist.**

(2) Click **Domain Allowlist**.

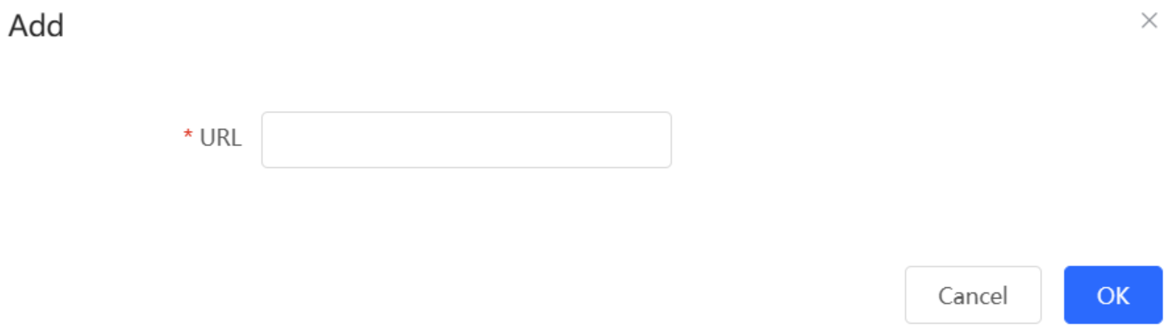
(3) Click **Add**.



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

Up to 100 entries can be added.

(4) Configure authentication-free domains.



(5) Click **OK**.

4. Configuring a MAC Address Blocklist and Allowlist

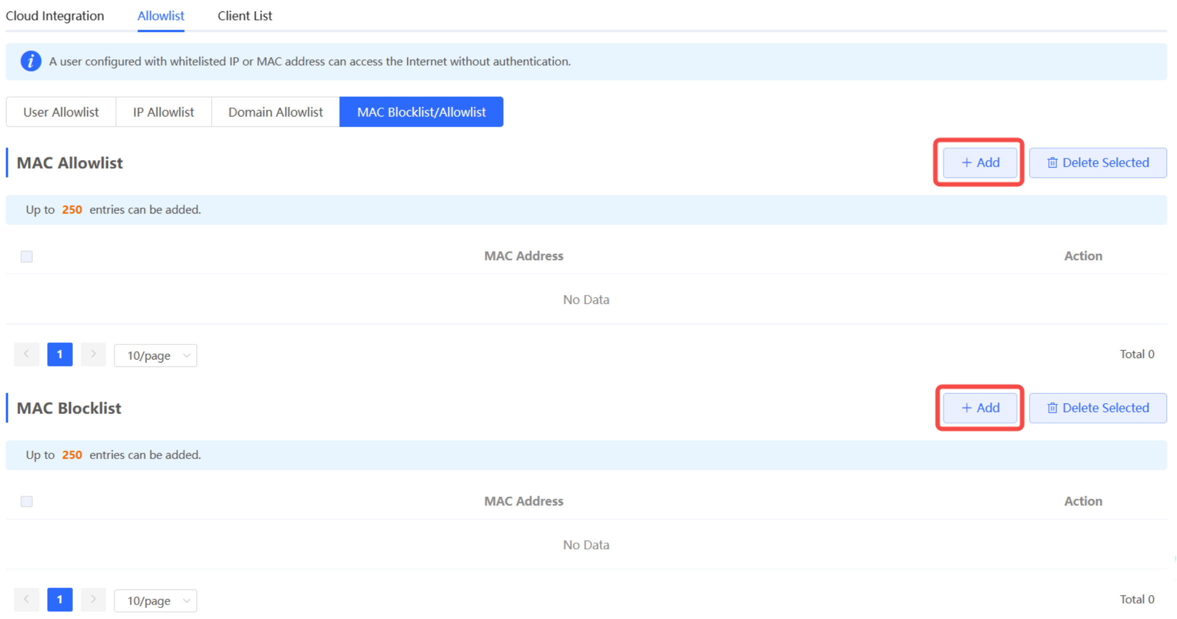
After configuration, the STA with an Allowlist MAC address can access the Internet without authentication while the STA with a blocklist MAC address is forbidden to access the Internet.

(1) Choose **Networkwide Management > Network > Wireless Auth > Allowlist**.

(2) Click **MAC Blocklist/Allowlist**.

(3) Configure a MAC address allowlist.

a Click **Add** on the **MAC Allowlist** page.



Cloud Integration | Allowlist | Client List

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

User Allowlist | IP Allowlist | Domain Allowlist | MAC Blocklist/Allowlist

MAC Allowlist + Add | Delete Selected

Up to 250 entries can be added.

□	MAC Address	Action
	No Data	

1 10/page Total 0

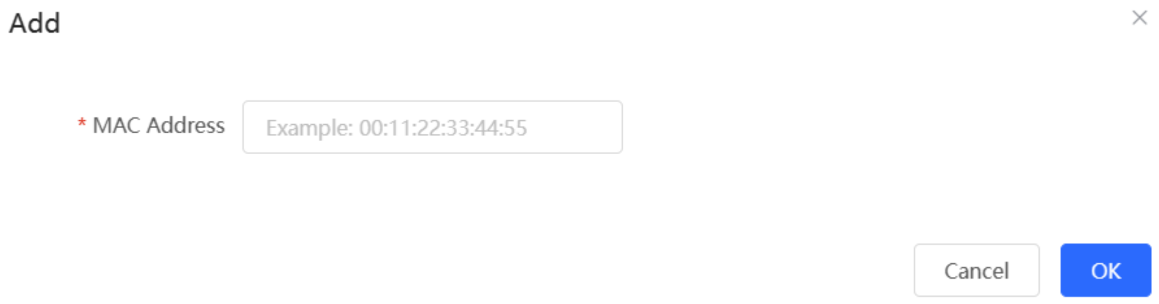
MAC Blocklist + Add | Delete Selected

Up to 250 entries can be added.

□	MAC Address	Action
	No Data	

1 10/page Total 0

b Add the MAC address to the allowlist.



Add

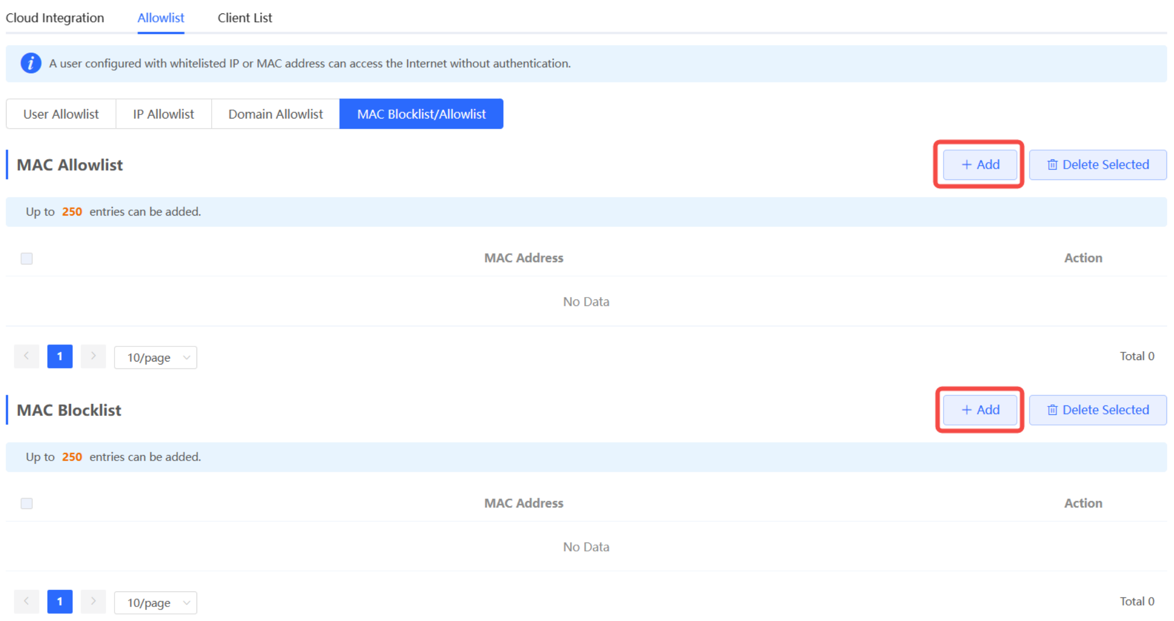
* MAC Address Example: 00:11:22:33:44:55

Cancel OK

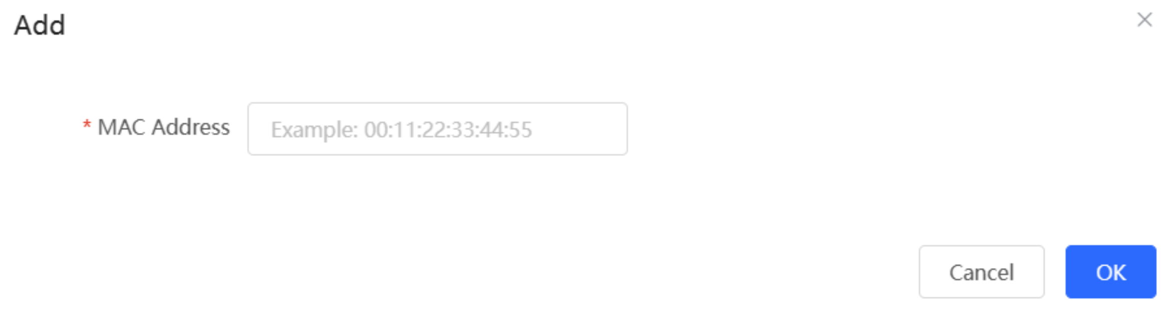
c Click **OK**.

(4) Configure a MAC address blocklist.

a Click **Add** on the **MAC Blocklist** page.



b Add the MAC address to the blocklist.

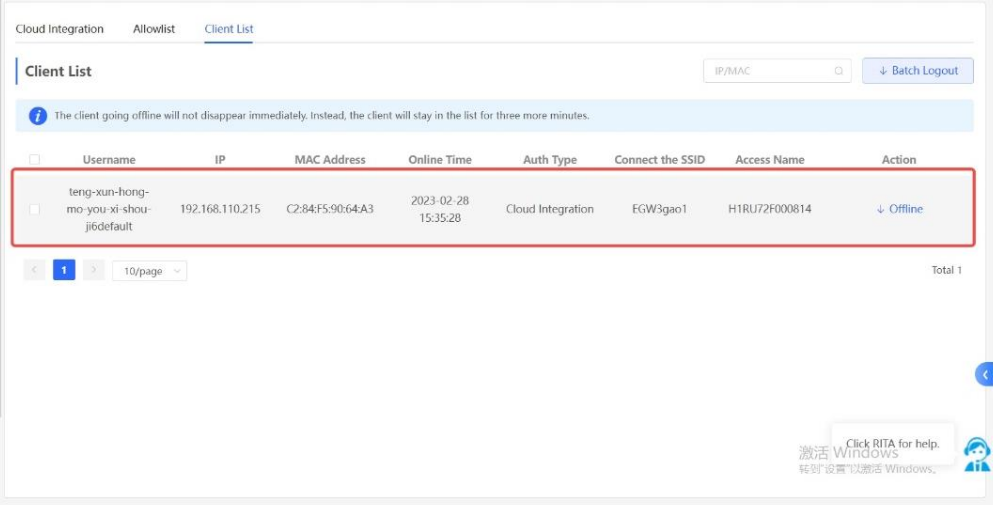


c Click **OK**.

4.11.4 Checking Authentication User List Eweb Management System

Check authentication users in the list view.

Choose **Networkwide Management>Network > Wireless Auth** > **Client List**.



Client List

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

□	Username	IP	MAC Address	Online Time	Auth Type	Connect the SSID	Access Name	Action
□	teng-xun-hong-mo-you-xi-shou-ji6default	192.168.110.215	C2:84:F5:90:64:A3	2023-02-28 15:35:28	Cloud Integration	EGW3gao1	H1RU72F000814	↓ Offline

Click **Offline** in the **Action** column to disconnect users to release network resources.

4.12 Configuring SNMP

Note

This feature is only supported on RG-EG105GW-X and RG-EG205GW.

4.12.1 Overview

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

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

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

4.12.2 Global Configuration

1. Overview

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

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

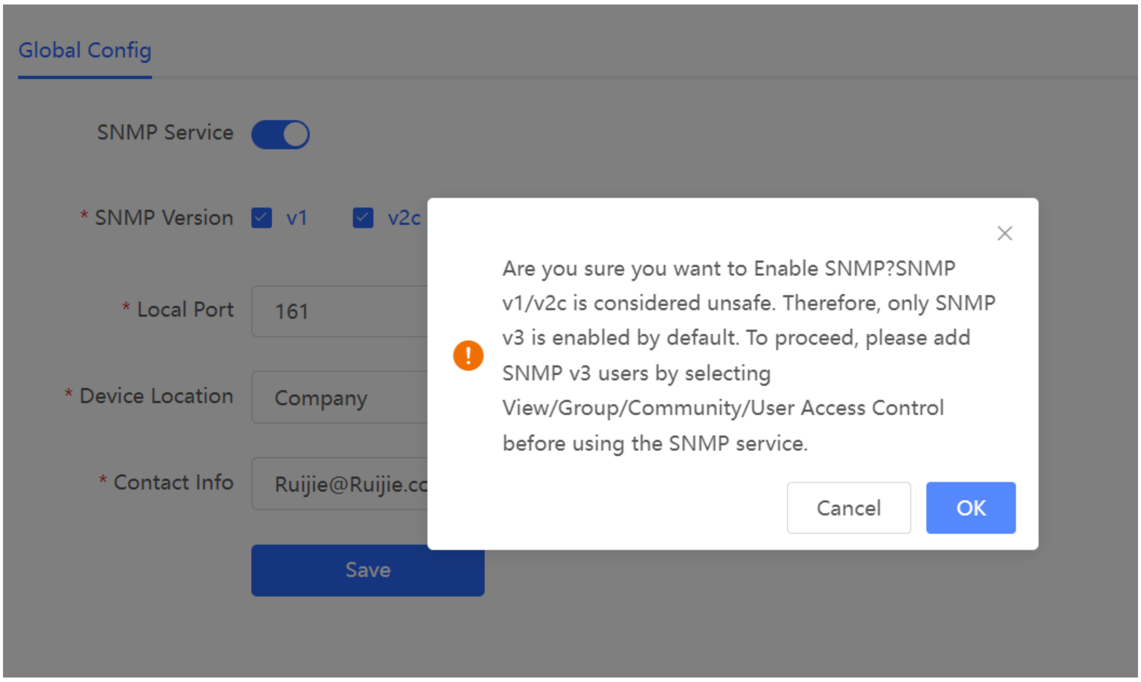
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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

2. Configuration Steps

[Networkwide Management] System > **SNMP** > **Global Config**

(1) Enable the SNMP service.



Global Config

SNMP Service

* SNMP Version ☑ v1 ☑ v2c

* Local Port 161

* Device Location Company

* Contact Info Ruijie@Ruijie.co

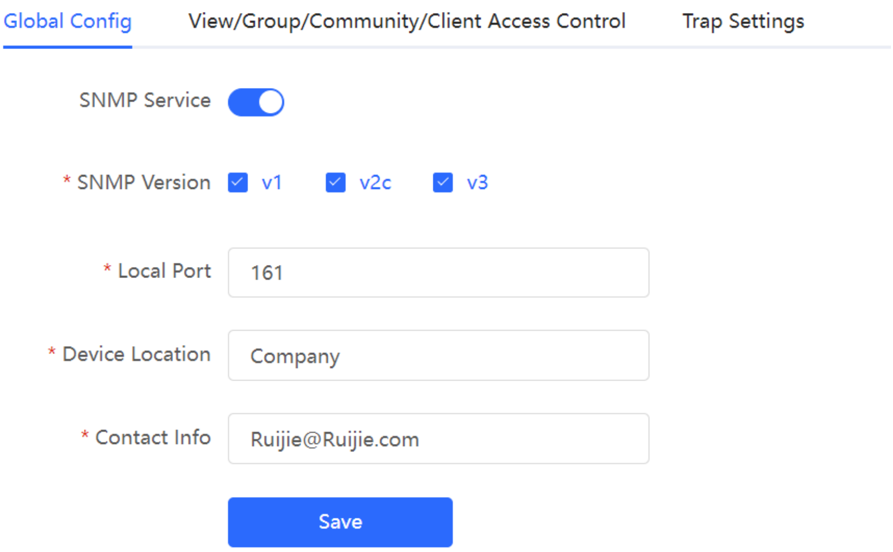
Save

Are you sure you want to Enable SNMP?SNMP v1/v2c is considered unsafe. Therefore, only SNMP v3 is enabled by default. To proceed, please add SNMP v3 users by selecting View/Group/Community/User Access Control before using the SNMP service.

Cancel OK

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

(2) Set SNMP service global configuration parameters.



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

SNMP Service

* SNMP Version ☑ v1 ☑ v2c ☑ v3

* Local Port 161

* Device Location Company

* Contact Info Ruijie@Ruijie.com

Save

Table 4-17 **Global Configuration Parameters**

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

(3) Click **Save**.

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

4.12.3 View/Group/Community/User Access Control

1. Configuring Views

- Overview

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

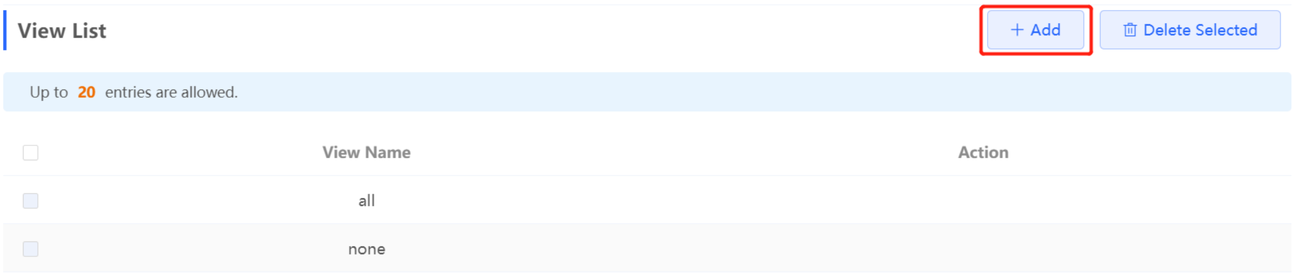
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

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

- Configuration Steps

[Networkwide Management] System > **SNMP** > **View/Group/Community/Client Access Control**

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



View List

Up to 20 entries are allowed.

□	View Name	Action
□	all	
□	none	

(2) Configure basic information of a view.

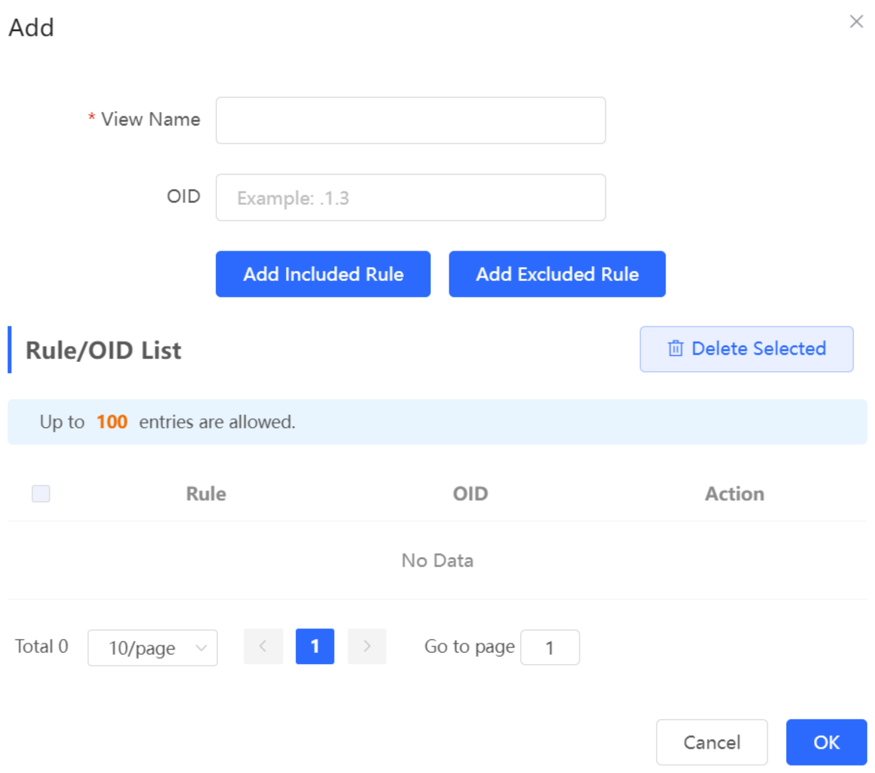


Table 4-18 **View Configuration Parameters**

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

Note

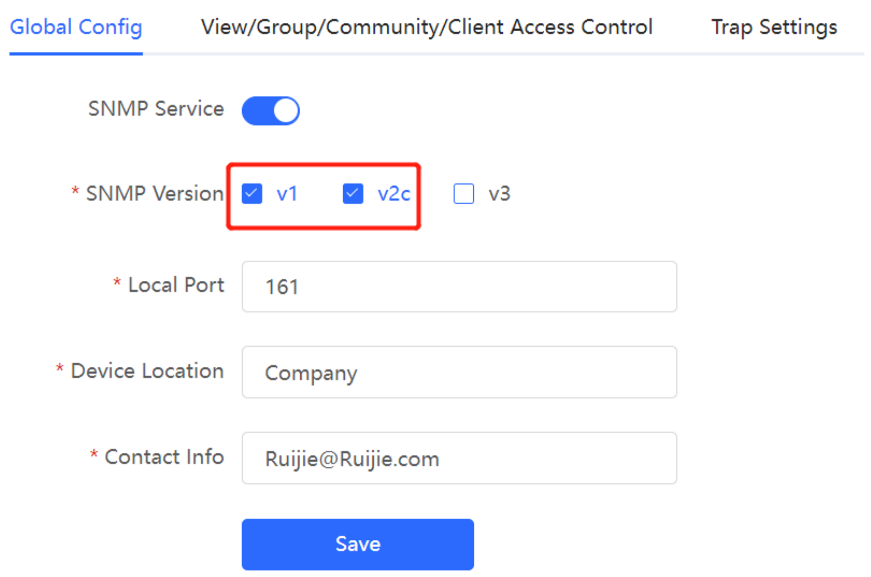
A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1/v2c Users

- Overview

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



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

SNMP Service: On

* SNMP Version: ☑ v1 ☑ v2c □ v3

* Local Port: 161

* Device Location: Company

* Contact Info: Ruijie@Ruijie.com

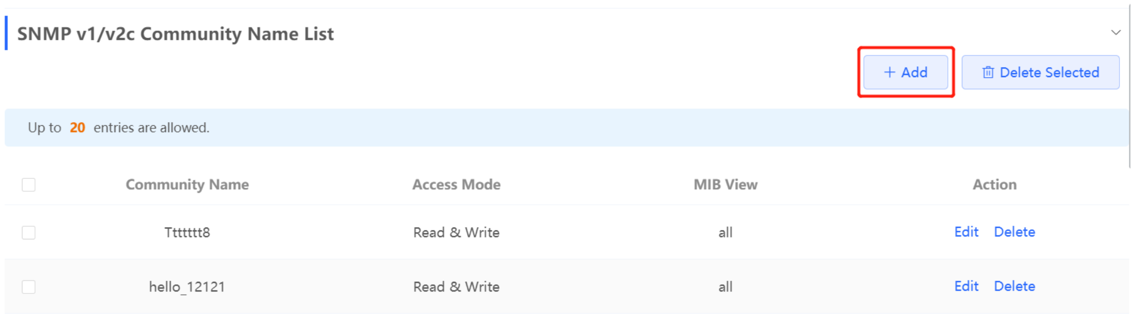
Note

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

- Configuration Steps

[Networkwide Management] System > **SNMP** > **View/Group/Community/Client Access Control**

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

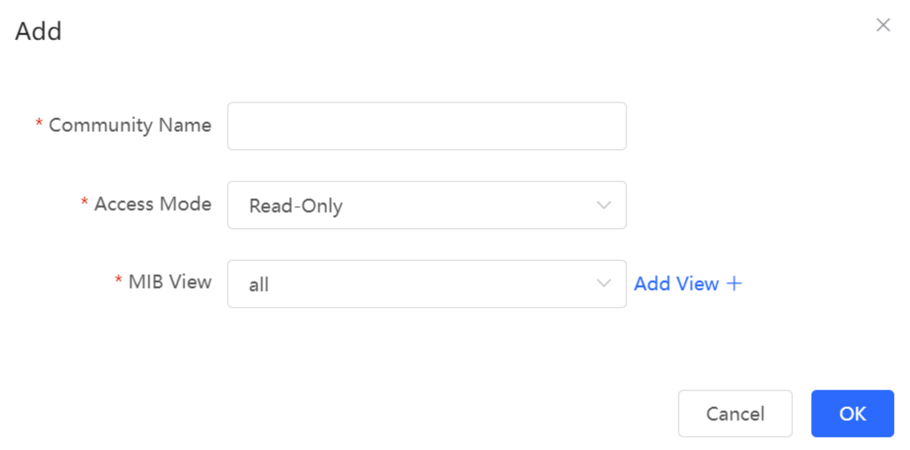


SNMP v1/v2c Community Name List

Up to 20 entries are allowed.

□	Community Name	Access Mode	MIB View	Action
□	Tttttt8	Read & Write	all	Edit Delete
□	hello_12121	Read & Write	all	Edit Delete

(2) Add a v1/v2c user.



Add

* Community Name

* Access Mode: Read-Only

* MIB View: all

Table 4-19 v1/v2c User Configuration Parameters

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

Note

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

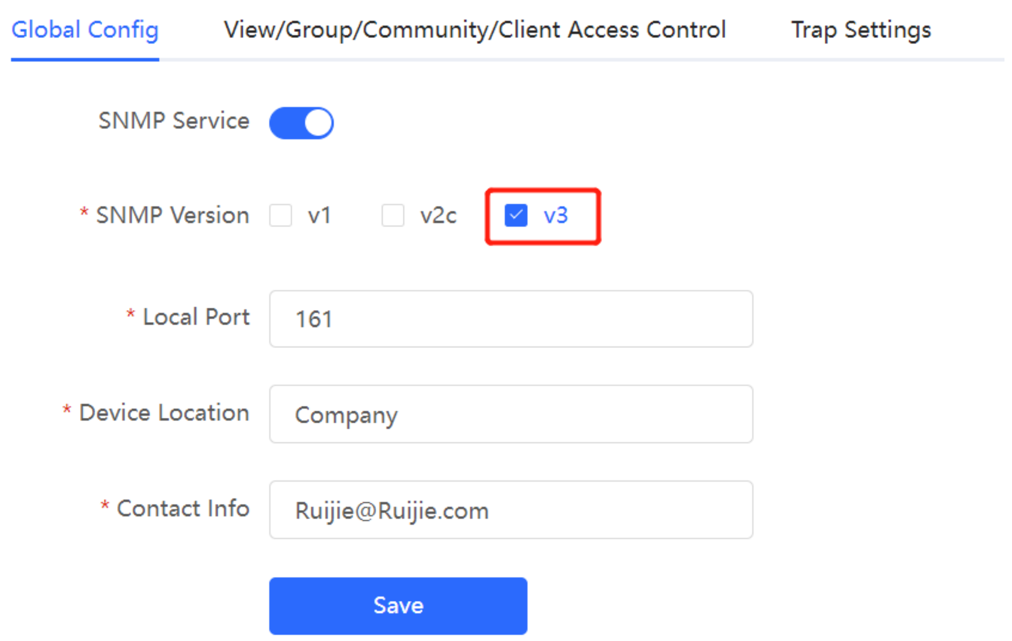
3. Configuring v3 Groups

- Overview

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

- Prerequisites

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



SNMP Service ●

* SNMP Version □ v1 □ v2c ☑ v3

* Local Port 161

* Device Location Company

* Contact Info Ruijie@Ruijie.com

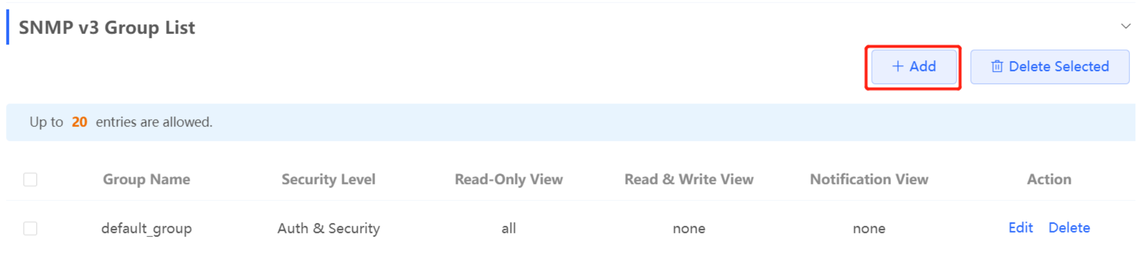
Note

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

- Configuration Steps

[Networkwide Management] System > **SNMP** > **View/Group/Community/Client Access Control**

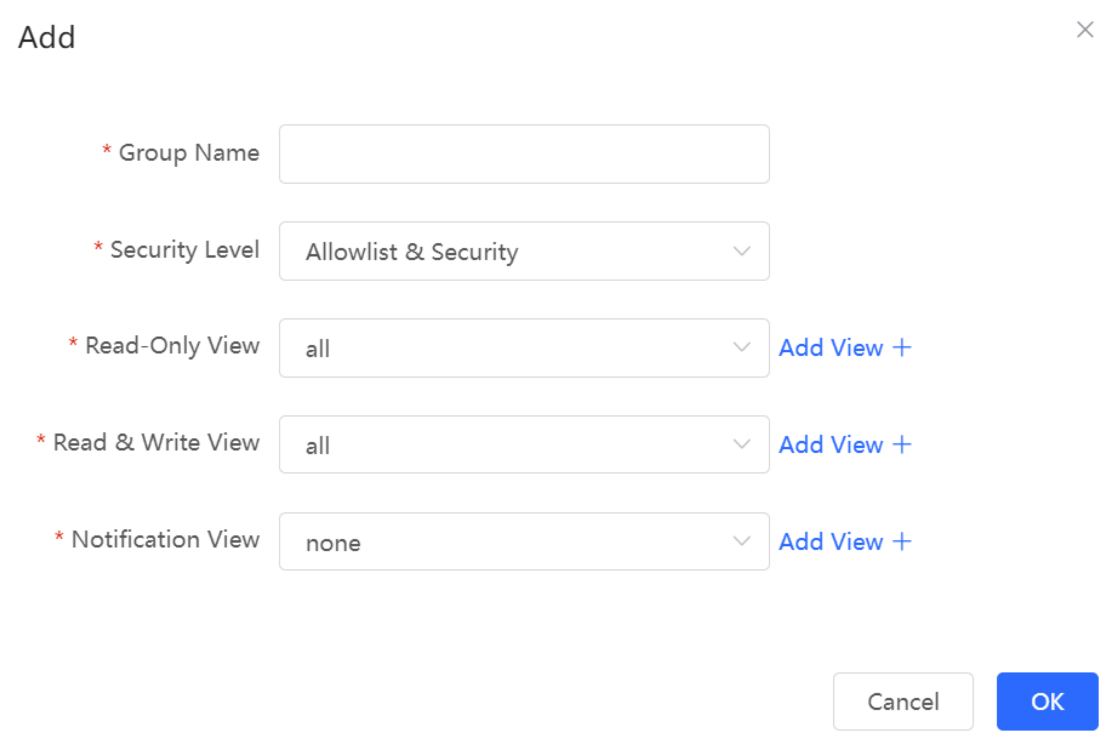
(1) Click **Add** in the **SNMP v3 Group List** pane to create a group.



Up to 20 entries are allowed.

□	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
□	default_group	Auth & Security	all	none	none	Edit Delete

(2) Configure v3 group parameters.



Add

* Group Name

* Security Level: Allowlist & Security

* Read-Only View: all

* Read & Write View: all

* Notification View: none

Table 4-20 v3 Group Configuration Parameters

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

⚠ **Note**

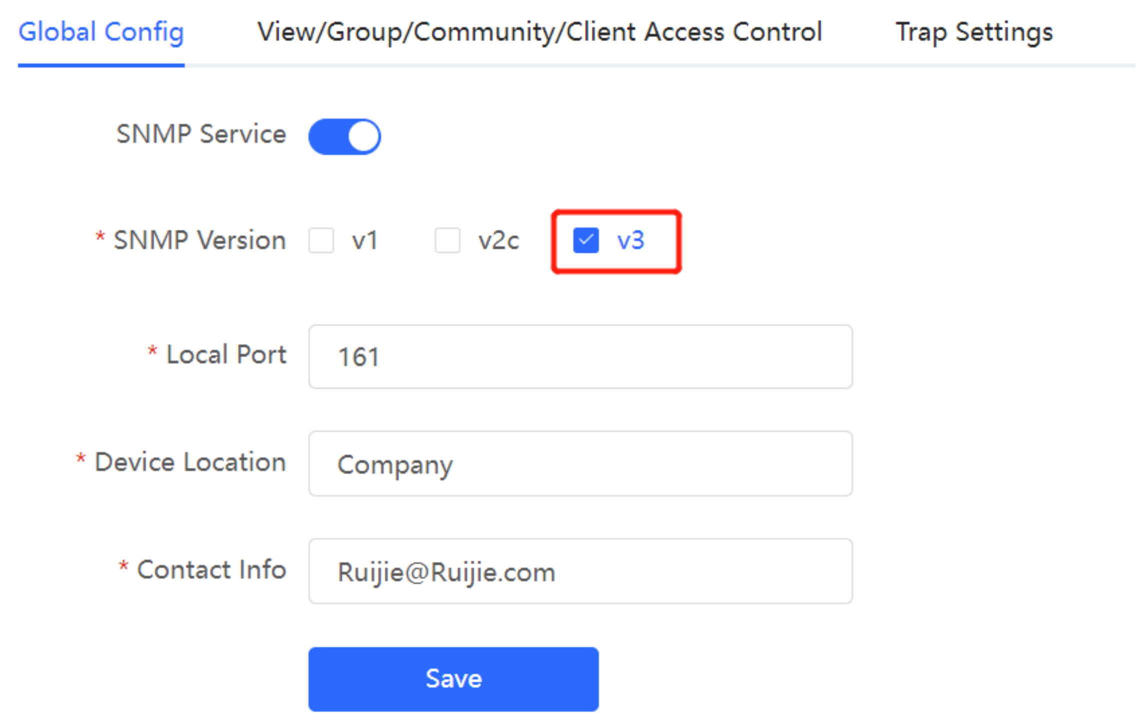
- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

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



SNMP Service: on

* SNMP Version: □ v1 □ v2c ☑ v3

* Local Port: 161

* Device Location: Company

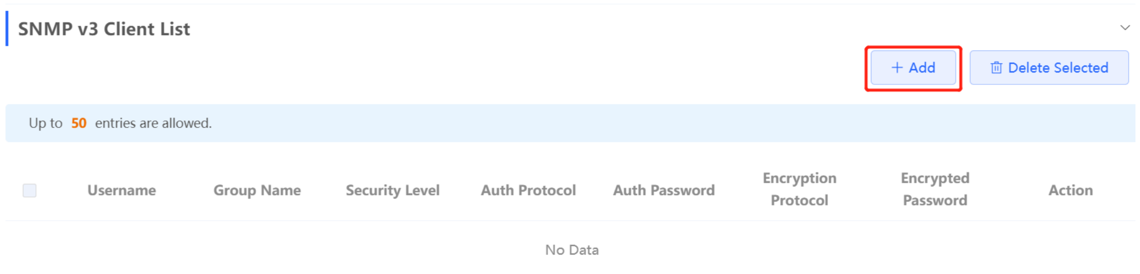
* Contact Info: Ruijie@Ruijie.com

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

- Configuration Steps

[Networkwide Management] System > **SNMP** > **View/Group/Community/Client Access Control**

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

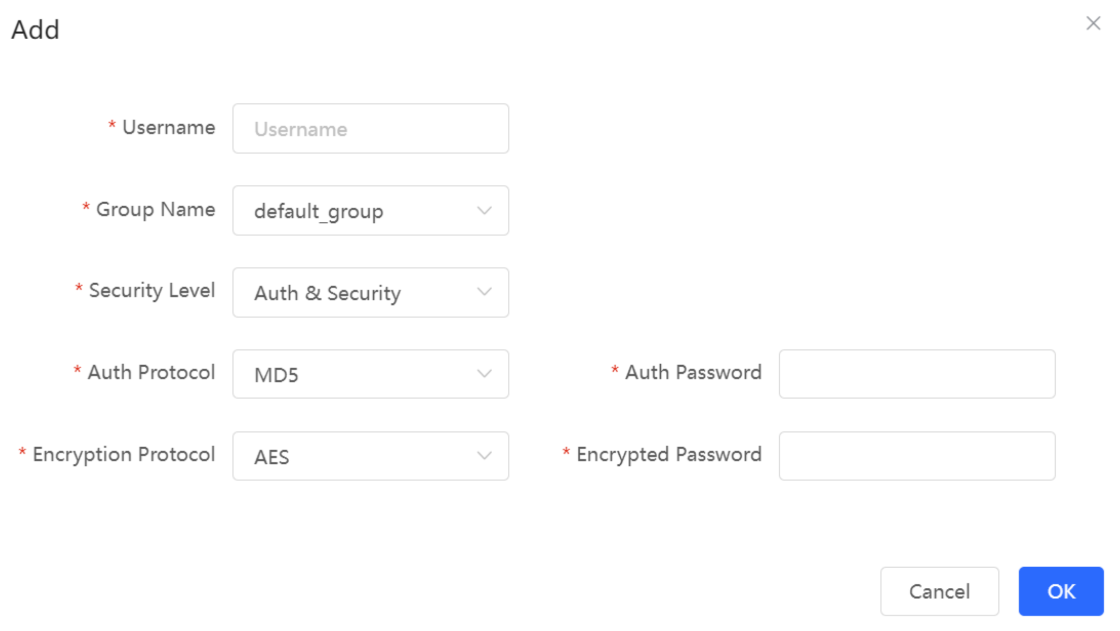


Up to 50 entries are allowed.

□	Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action

No Data

(2) Configure v3 user parameters.



Add

* Username: Username
* Group Name: default_group
* Security Level: Auth & Security
* Auth Protocol: MD5
* Auth Password:
* Encryption Protocol: AES
* Encrypted Password:

Table 4-21 v3 User Configuration Parameters

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

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

⚠ **Note**

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

4.12.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

- Application Scenario

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

- Configuration Specification

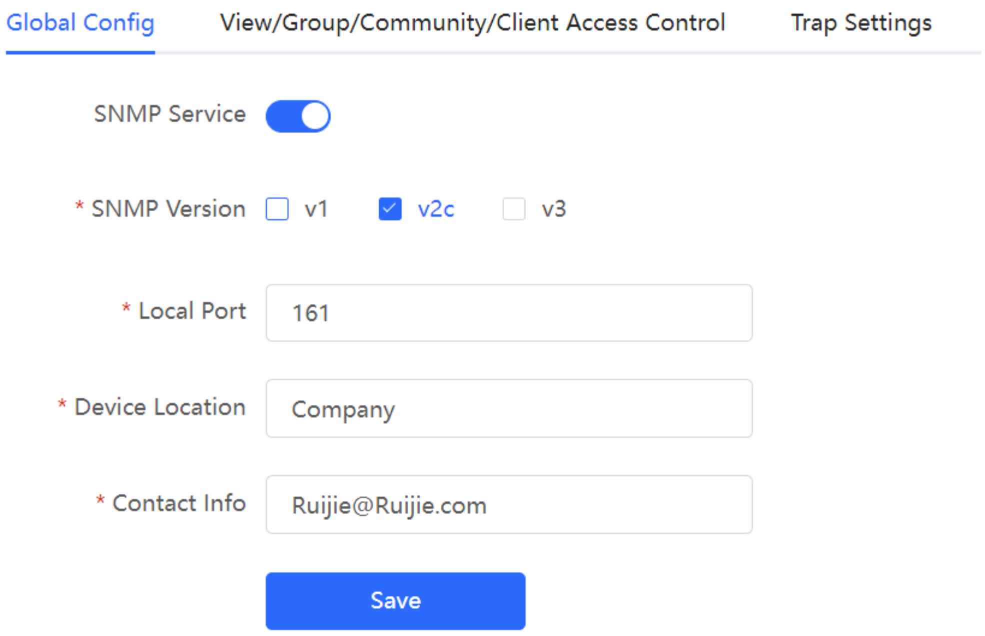
According to the user’s application scenario, the requirements are shown in the following table:

Table 4-22 User Requirement Specification

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

- Configuration Steps

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



SNMP Service: on

* SNMP Version: □ v1 ☑ v2c □ v3

* Local Port: 161

* Device Location: Company

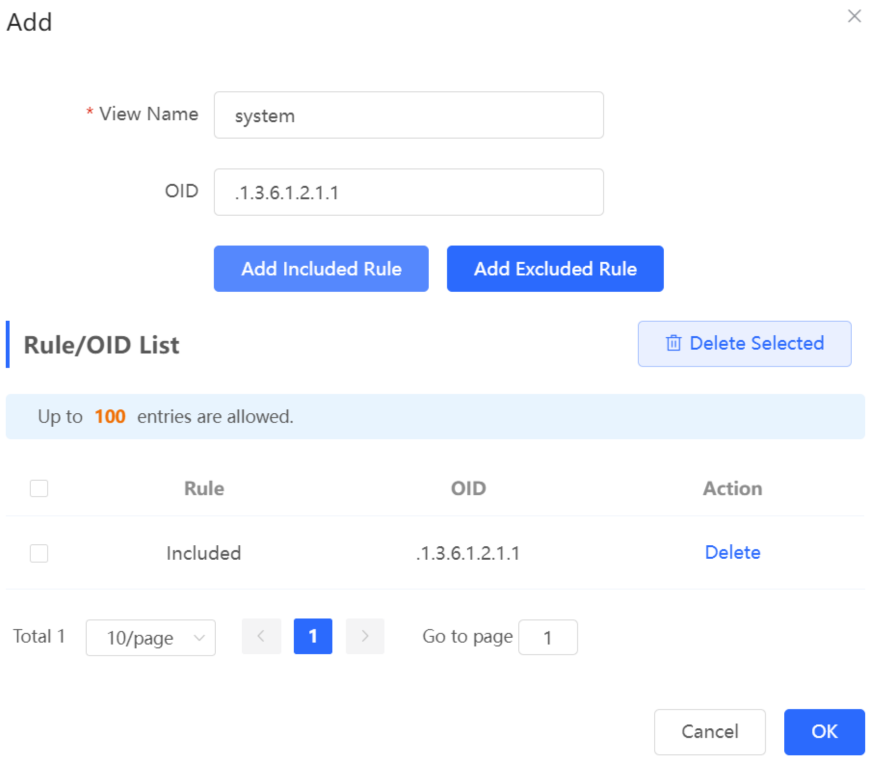
* Contact Info: Ruijie@Ruijie.com

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

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

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

c Click **OK**.



* View Name: system

OID: .1.3.6.1.2.1.1

Up to 100 entries are allowed.

□	Rule	OID	Action
□	Included	.1.3.6.1.2.1.1	Delete

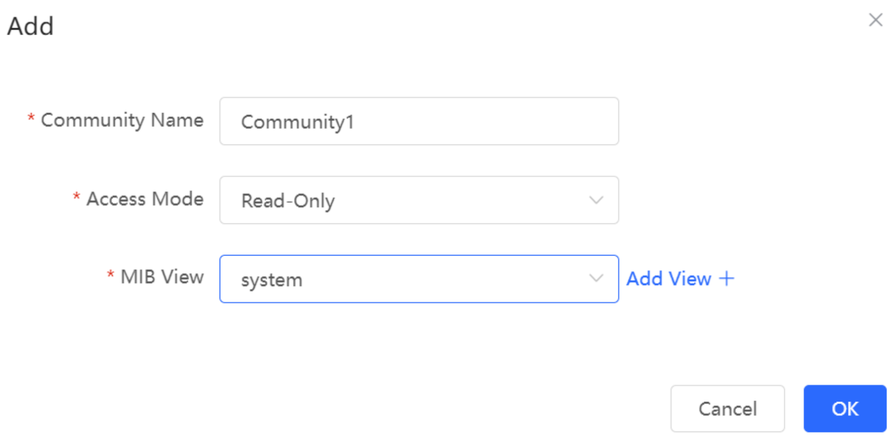
Total 1

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

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

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

c Click **OK**.



Add

* Community Name: Community1

* Access Mode: Read-Only

* MIB View: system

2. Configuring SNMP v3

- Application Scenario

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

- Configuration Specification

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

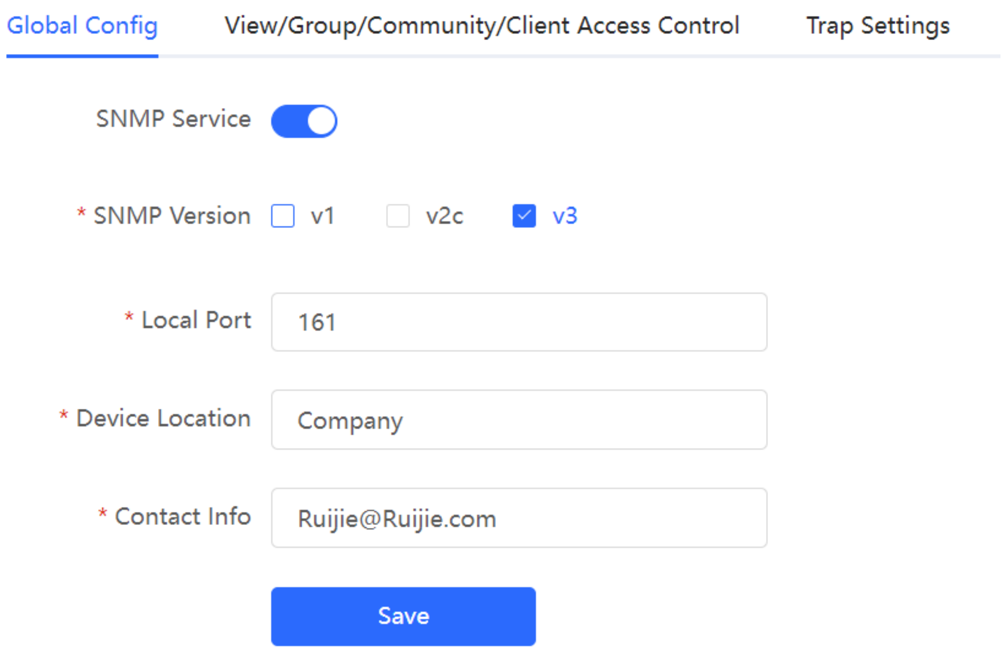
Table 4-23 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.

Item	Description
Configuring v3 Users	User name: v3_user Group name: group Security level: authentication and encryption Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123
Version	For SNMP v3, the default port number is 161.

- Configuration Steps

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



SNMP Service: on

* SNMP Version: □ v1 □ v2c ☑ v3

* Local Port: 161

* Device Location: Company

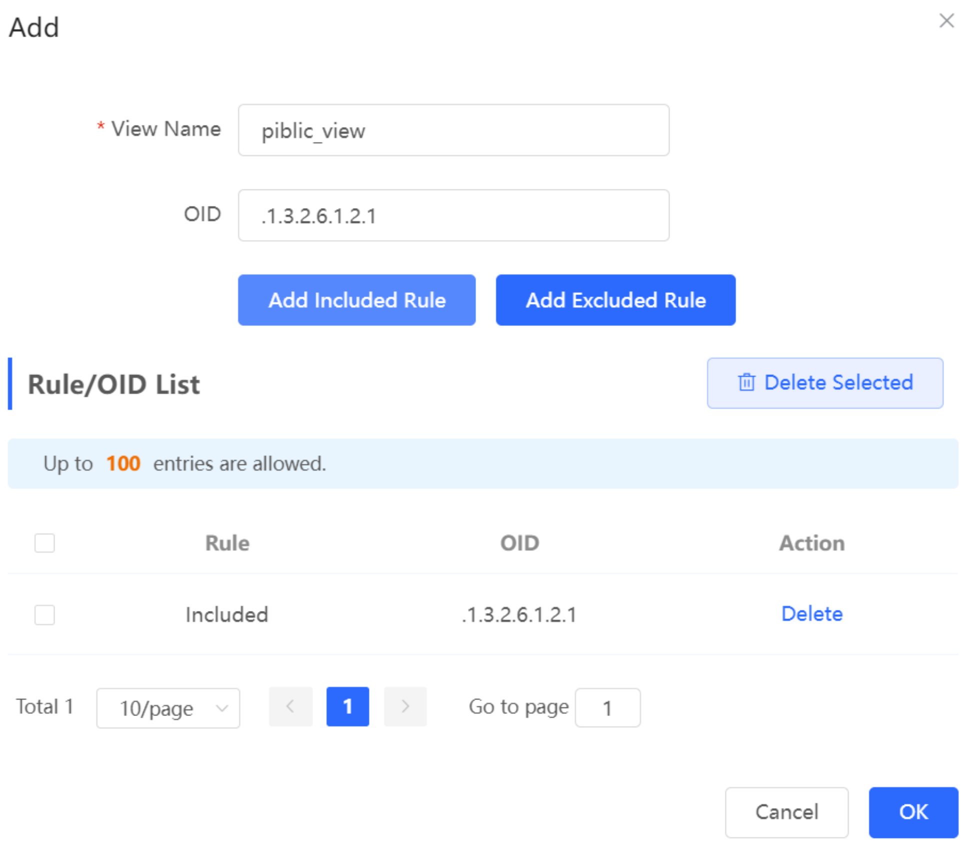
* Contact Info: Ruijie@Ruijie.com

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

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

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

c Click **OK**.



Add

* View Name: piblic_view

OID: .1.3.2.6.1.2.1

Rule/OID List

Up to 100 entries are allowed.

□	Rule	OID	Action
□	Included	.1.3.2.6.1.2.1	Delete

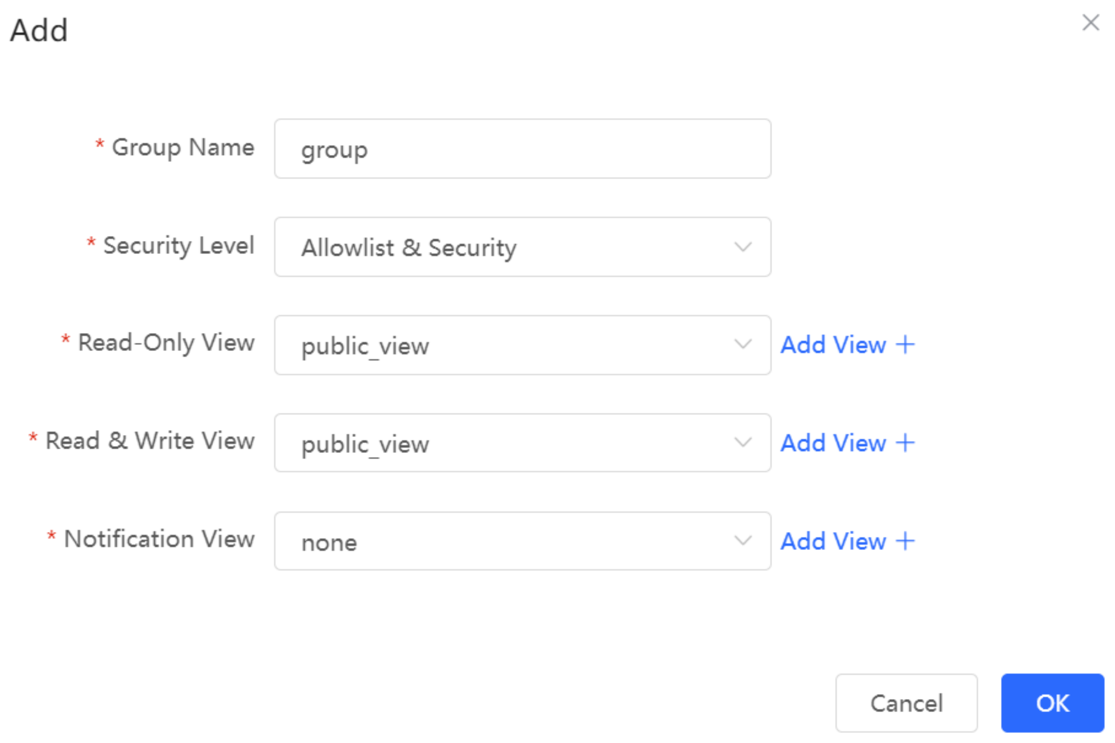
Total 1 10/page < 1 > Go to page 1

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

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

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

c Click **OK**.



Add

* Group Name: group

* Security Level: Allowlist & Security

* Read-Only View: public_view

* Read & Write View: public_view

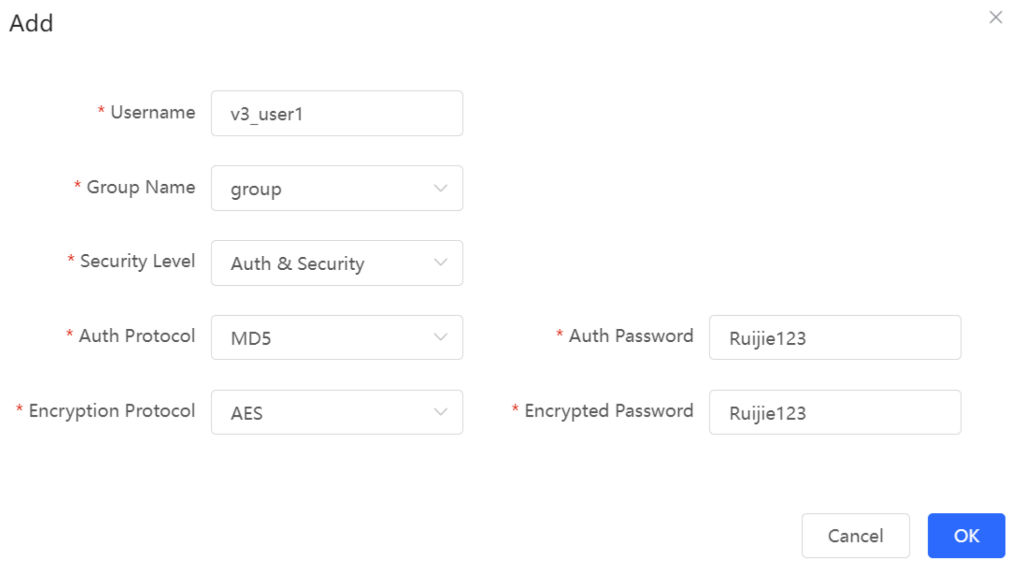
* Notification View: none

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

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

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

c Click **OK**.



Add

* Username: v3_user1

* Group Name: group

* Security Level: Auth & Security

* Auth Protocol: MD5

* Auth Password: Ruijie123

* Encryption Protocol: AES

* Encrypted Password: Ruijie123

4.12.5 Configuring Trap Service

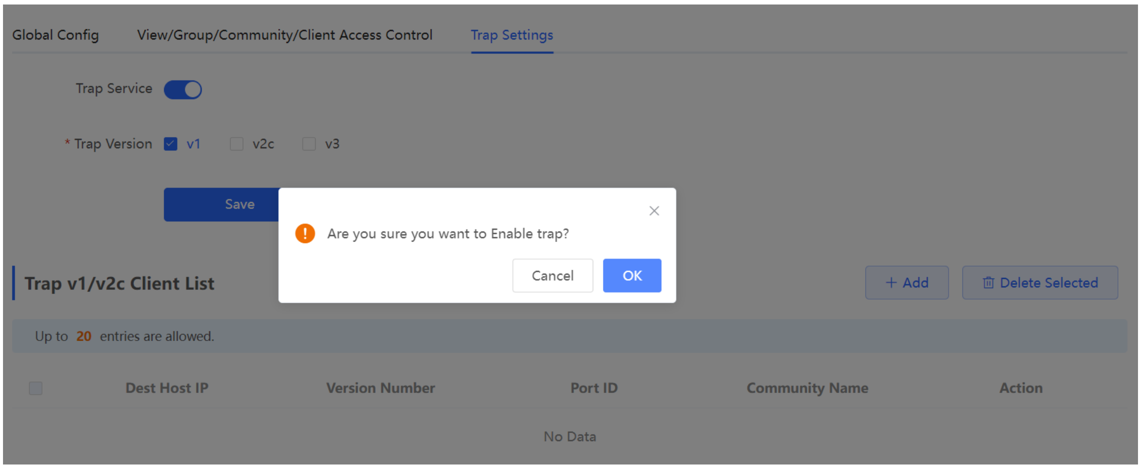
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring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

1. Enabling Trap Service

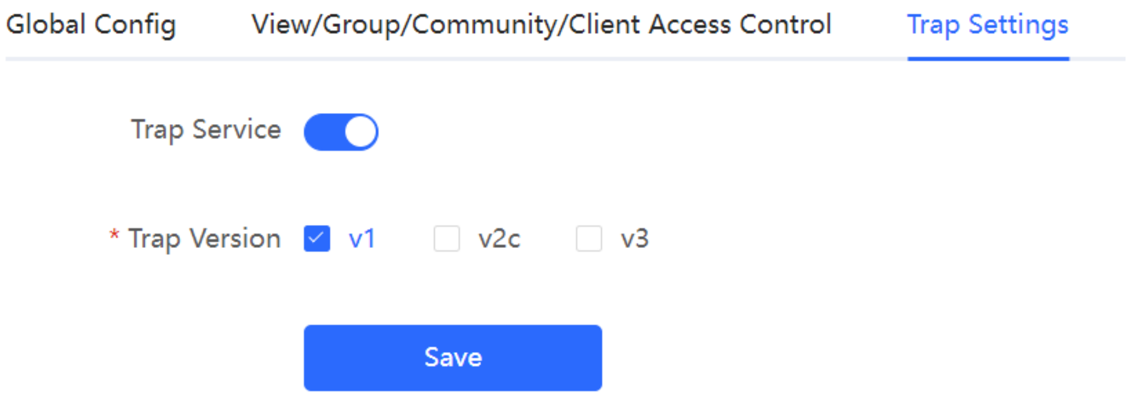
Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

[Networkwide Management] System > **SNMP** > **Trap Setting**

(1) Enable the trap service.



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


Global Config
View/Group/Community/Client Access Control
Trap Settings
Trap Service
* Trap Version ☑ v1 □ v2c □ v3
Save

(2) Set the trap version.

The trap versions include v1, v2c, and v3.

(3) Click **OK**.

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

2. Configuring Trap v1/v2c Users

- Overview

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

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

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

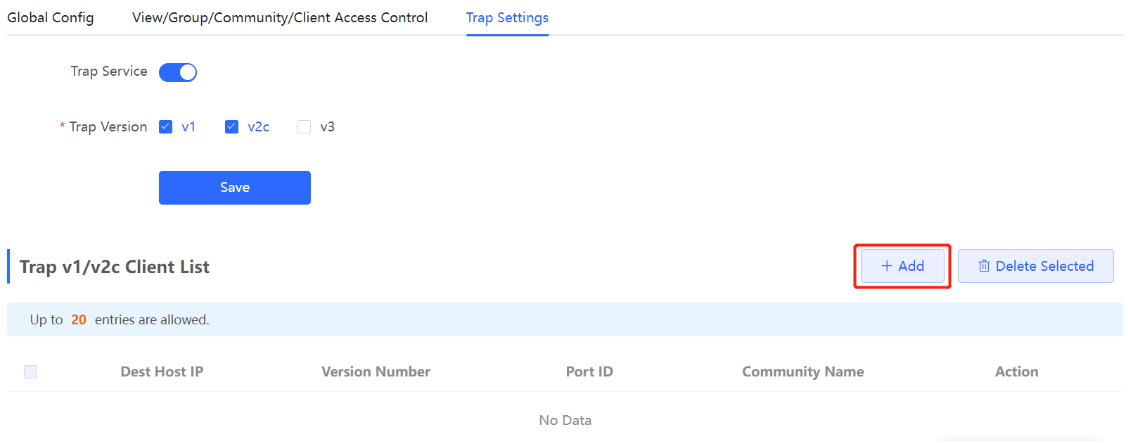
- Prerequisites

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

- Procedure

[Networkwide Management] System > **SNMP** > **Trap Setting**

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



Trap Service: on

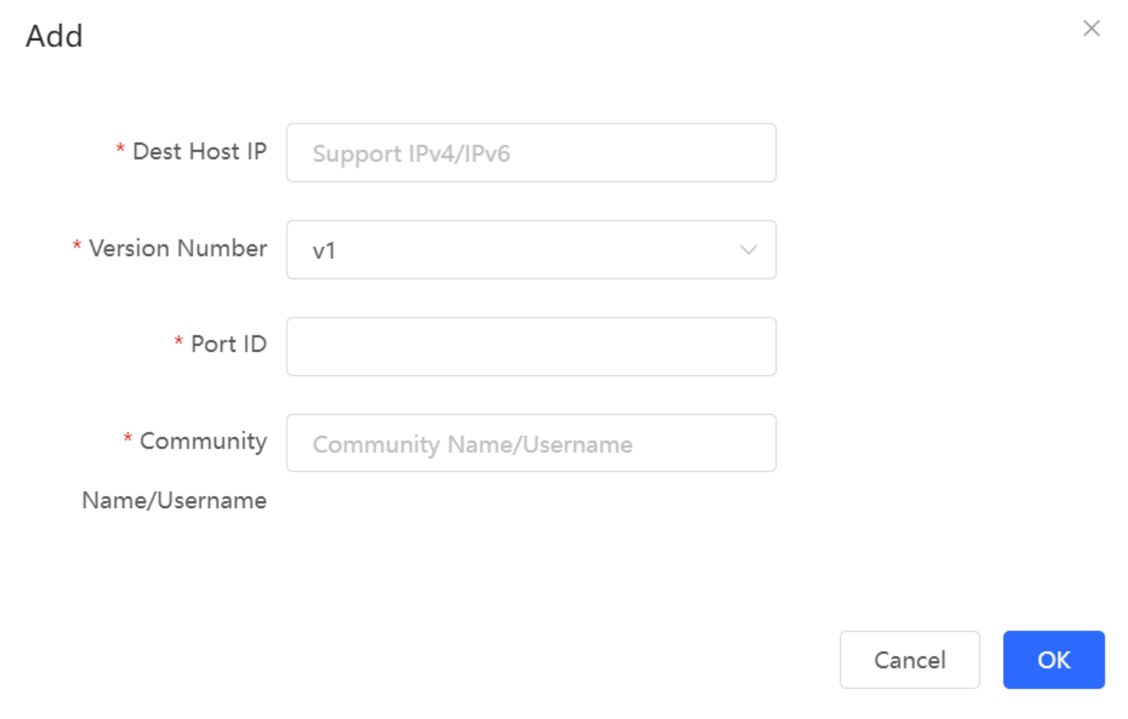
* Trap Version ☑ v1 ☑ v2c □ v3

Trap v1/v2c Client List

Up to 20 entries are allowed.

□	Dest Host IP	Version Number	Port ID	Community Name	Action
No Data					

(2) Configure trap v1/v2c user parameters.



* Dest Host IP: Support IPv4/IPv6

* Version Number: v1

* Port ID:

* Community Name/Username: Community Name/Username

Table 4-24 Trap v1/v2c User Configuration Parameters

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

⚠ **Note**

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

(3) Click **OK**.

1. Configuring Trap v3 Users

- Overview

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

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

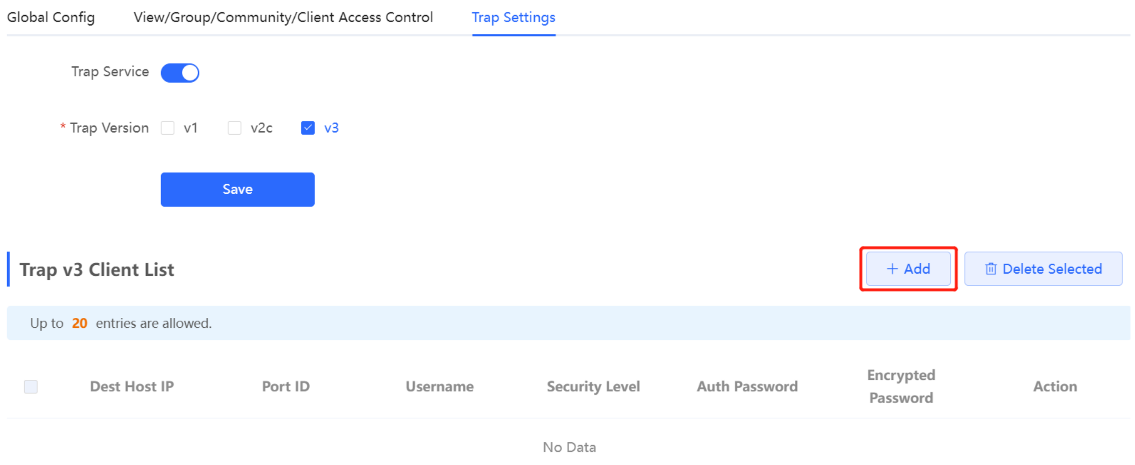
- Prerequisites

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

- Configuration Steps

[Networkwide Management] System > **SNMP** > **Trap Setting**

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



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

Trap Service: on

* Trap Version □ v1 □ v2c ☑ v3

Save

Trap v3 Client List

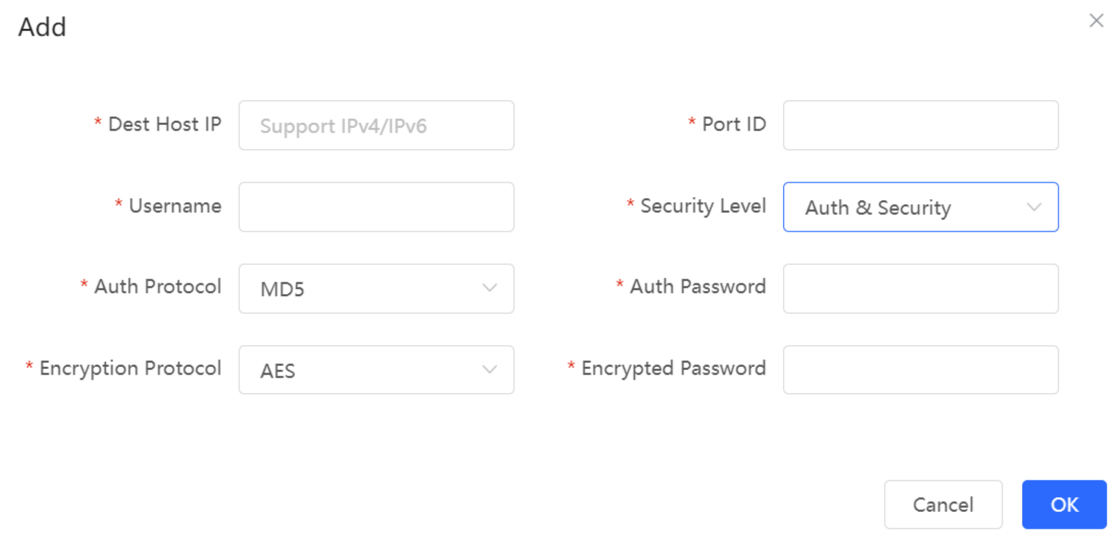
+ Add | Delete Selected

Up to 20 entries are allowed.

□	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action

No Data

(2) Configure trap v3 user parameters.



Add

* Dest Host IP: Support IPv4/IPv6

* Port ID:

* Username:

* Security Level: Auth & Security

* Auth Protocol: MD5

* Auth Password:

* Encryption Protocol: AES

* Encrypted Password:

Cancel | OK

Table 4-25 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.
Username	Name of the trap v3 user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.

Parameter	Description
Security Level	Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

⚠ **Note**

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

4.12.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

- Application Scenarios

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

- Configuration Specification

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

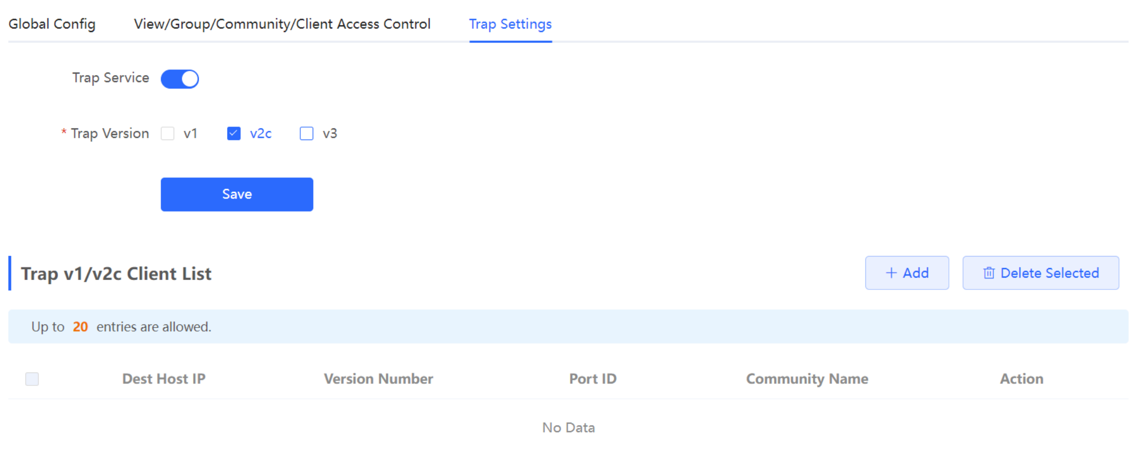
Table 4-26 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port number is 166.

Item	Description
Version	Select the v2 version.
Community name/User name	Trap_user

- Configuration Steps

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



Trap Service ●

* Trap Version □ v1 ☑ v2c □ v3

Trap v1/v2c Client List

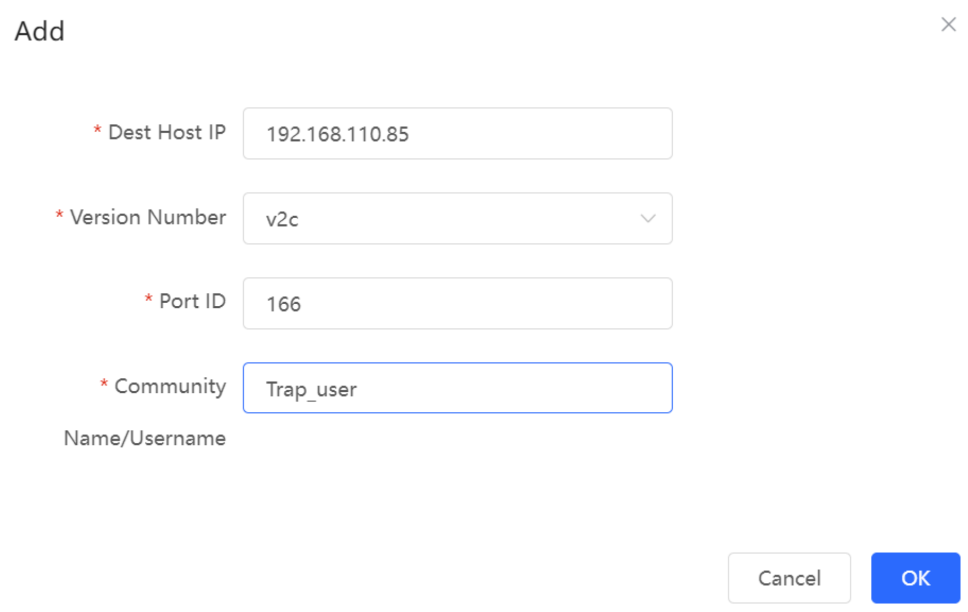
Up to 20 entries are allowed.

□	Dest Host IP	Version Number	Port ID	Community Name	Action

No Data

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

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



Add

* Dest Host IP: 192.168.110.85

* Version Number: v2c

* Port ID: 166

* Community Name/Username: Trap_user

1. Configuring Trap v3

- Application Scenarios

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

- Configuration Specification

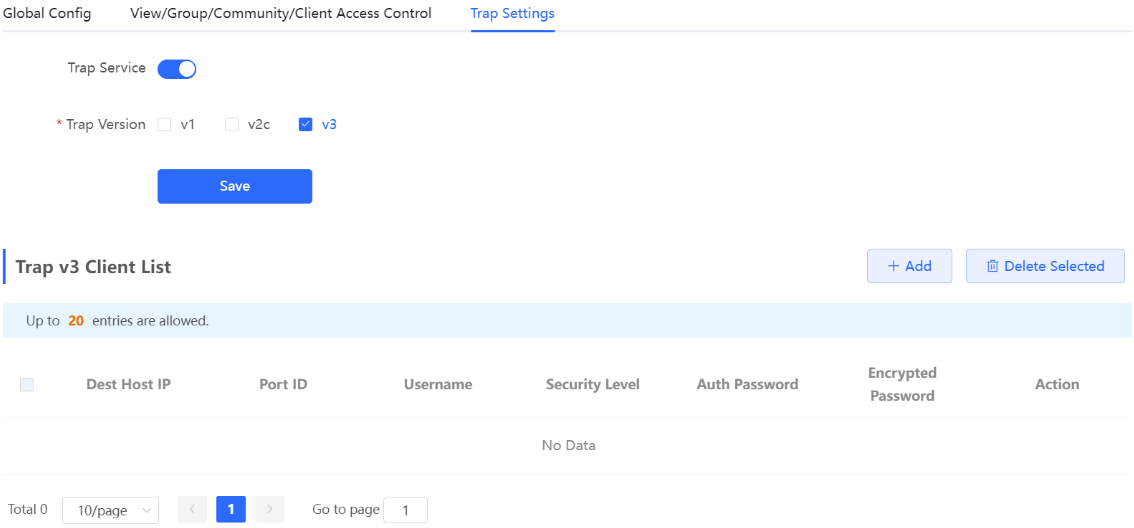
According to the user's application scenario, the requirements are shown in the following table:

Table 4-27 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.87, and the port number is 167.
Version and user name	Select the v3 version and trapv3_user for the user name.
Authentication protocol/authentication password Encryption protocol/encryption password	Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123

- Configuration Steps

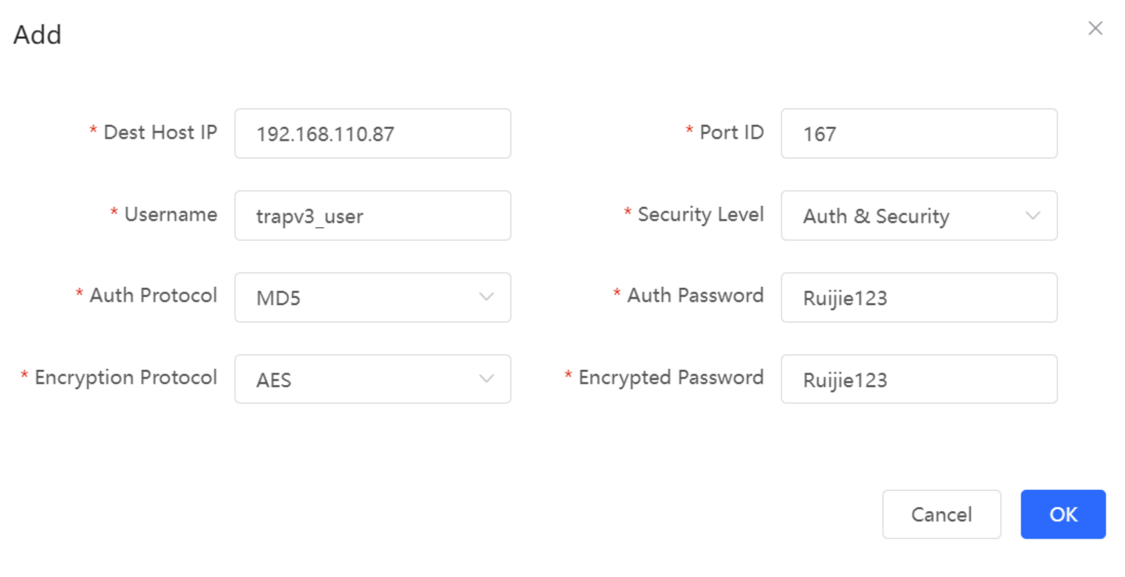
(5) Select the v3 version in the **Trap Setting** interface and click **Save**.



□	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
No Data							

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

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



Add

* Dest Host IP	192.168.110.87	* Port ID	167
* Username	trapv3_user	* Security Level	Auth & Security
* Auth Protocol	MD5	* Auth Password	Ruijie123
* Encryption Protocol	AES	* Encrypted Password	Ruijie123

4.13 Configure IEEE 802.1X authentication

Note

This feature is only supported on RG-EG105GW-X and RG-EG205GW.

4.13.1 Overview

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

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

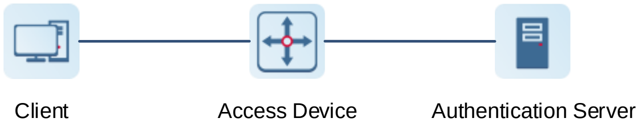
The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

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

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

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

Figure 4-1 Typical Architecture of 802.1X Network



- The client is usually an endpoint device which can initiate 802.1X authentication through the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL) on the local area network.

- The access device is usually a network device (AP or switching device) that supports the IEEE 802.1X protocol. It provides an interface for clients to access the local area network, which can be a physical or a logical interface.

Note

- The RG-EG gateway device itself does not support the IEEE 802.1X authentication, and can only serve as the primary device to support 802.1X global configuration and deliver the configuration to APs and switching devices on the entire network.
- To achieve IEEE 802.1X authentication, ensure that the network includes an AP or switching device.

- The authentication server can realize user authentication, authorization, and accounting. Usually a RADIUS server is used as the authentication server.

4.13.2 Configuring 802.1X Globally

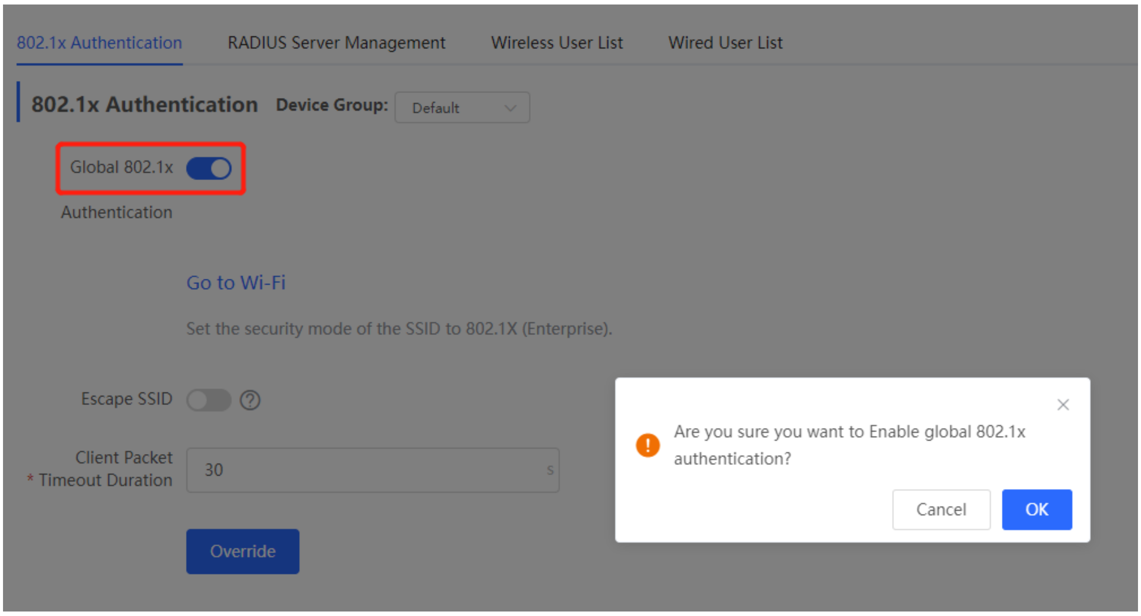
The gateway device supports the 802.1X global configuration, and can synchronously deliver the configuration to APs and switching devices on the network.

[Networkwide Management] Network > **802.1x Authentication**

(1) Click the **802.1x Authentication** tab to configure global configuration for 802.1x wireless authentication.

(2) Select the authentication device group, and enable the global 802.1x authentication.

You will be prompted to enable this feature or not. Click **Yes**.

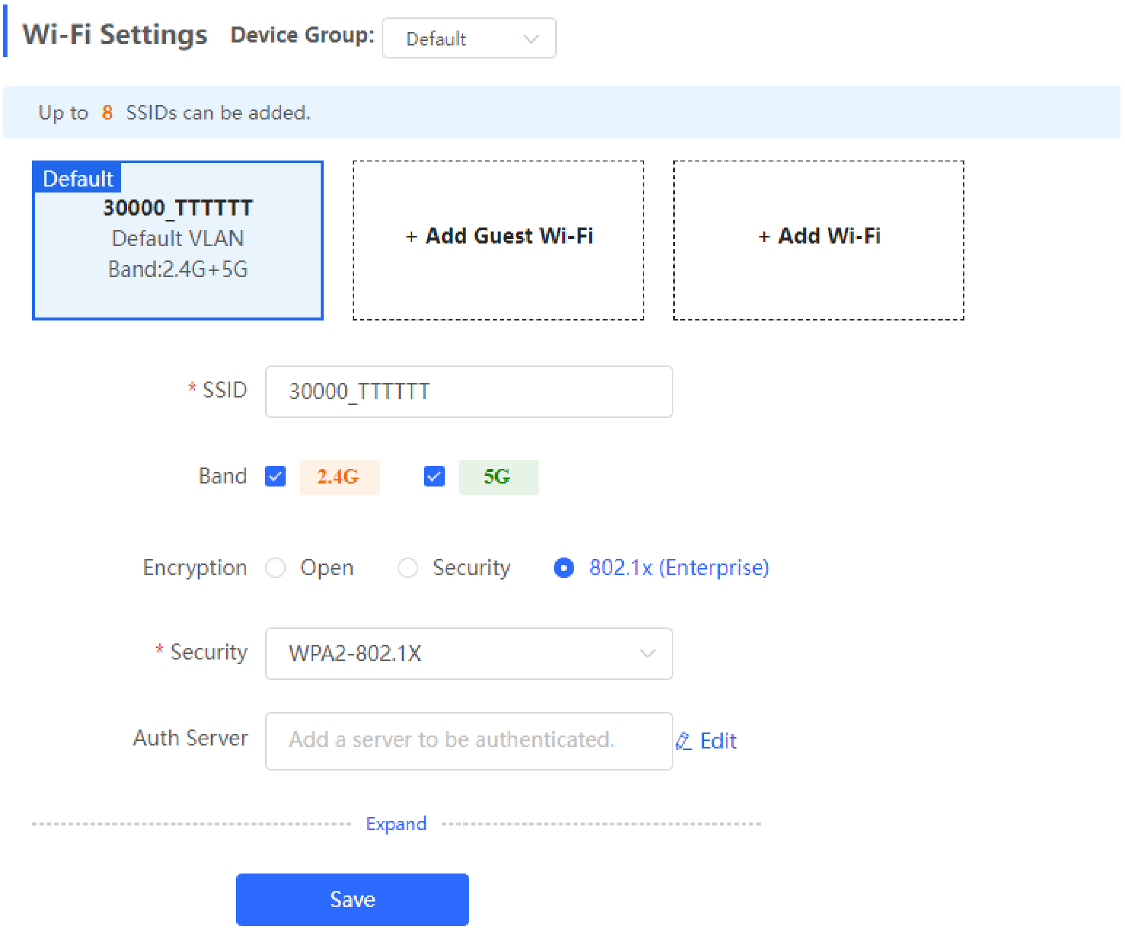


Set the security mode of the SSID to 802.1X (Enterprise).

Client Packet Timeout Duration: 30 s

Are you sure you want to Enable global 802.1x authentication?

(3) Click **Go to Wi-Fi,** and set the encryption method of SSID to **802.1x (Enterprise)**.



Wi-Fi Settings **Device Group:** Default

Up to 8 SSIDs can be added.

Default **30000_TTTTTT** Default VLAN Band:2.4G+5G	+ **Add Guest Wi-Fi**	+ **Add Wi-Fi**

* SSID: 30000_TTTTTT

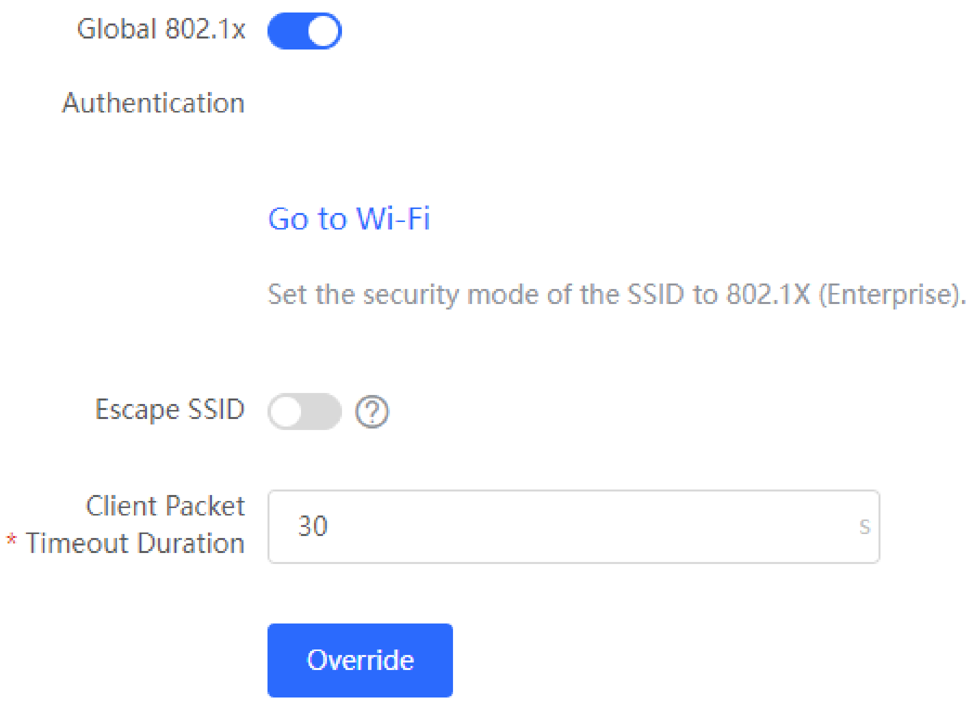
Band: ☑ 2.4G ☑ 5G

Encryption: ○ Open ○ Security ● 802.1x (Enterprise)

* Security: WPA2-802.1X

Auth Server: Add a server to be authenticated. Edit

(4) Configure global parameters.



Global 802.1x Authentication: ● (on)

Go to Wi-Fi

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

Escape SSID: ○ (off) ?

* Client Packet Timeout Duration: 30 s

Parameter	Description
Escape SSID	Once this feature is enabled, when the authentication server is unavailable, the system will create a temporary Wi-Fi network for users. If this function is enabled, it is necessary to set the Escape SSID, encryption type, and Wi-Fi password.
Re-authentication	Once this feature is enabled, the system regularly re-authenticates users. Users who do not match the information on the server will be automatically disconnected. If this function is enabled, it is necessary to set the re-authentication cycle, which is 3600 seconds by default.
Client Packet Timeout Duration	The timeout period for the switching device to wait for the authentication server to send an EAP response message. The default value is 30 seconds.

(5) Click **Override**.

4.13.3 Configuring the RADIUS Server

1. Prerequisites

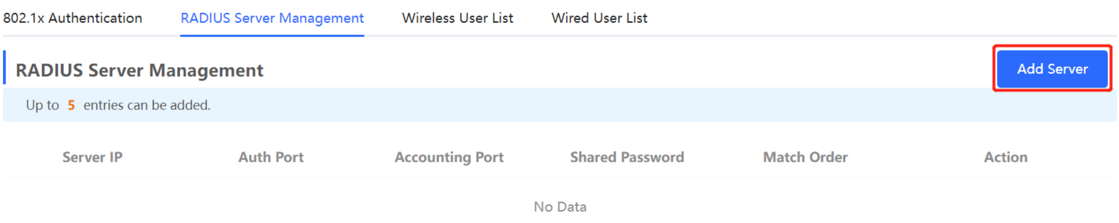
Before configuration, ensure that the RADIUS server is ready, and that the IP address and shared key of the RADIUS server are configured.

2. Configuration Steps

[Networkwide Management] Network > **802.1x Authentication**

(1) Click the **RADIUS Server Management** tab.

(2) Click **Add Server** to configure related server parameters.

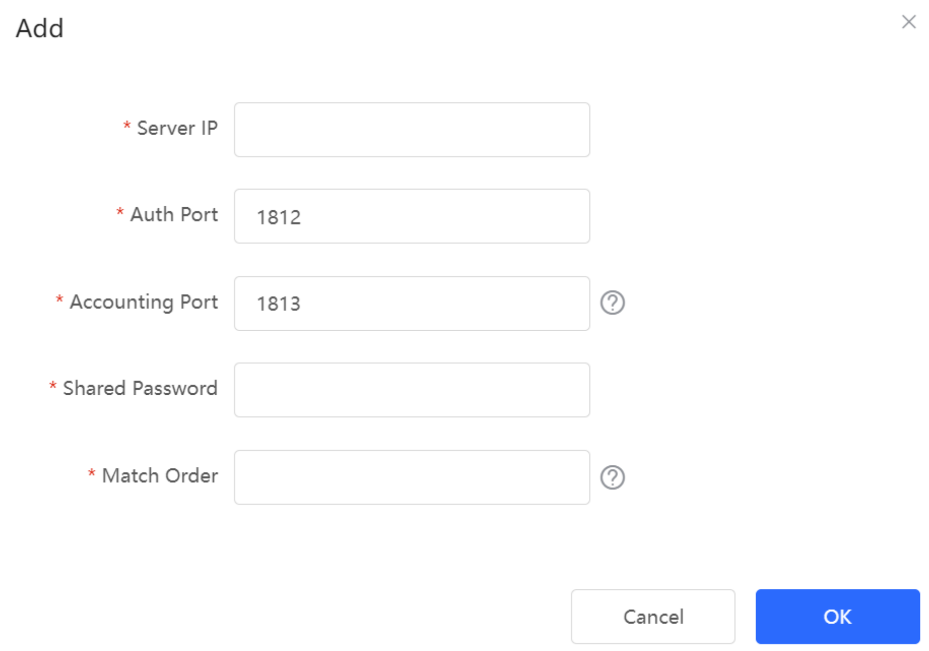


RADIUS Server Management

Up to 5 entries can be added.

Server IP	Auth Port	Accounting Port	Shared Password	Match Order	Action

No Data



Add

* Server IP

* Auth Port: 1812

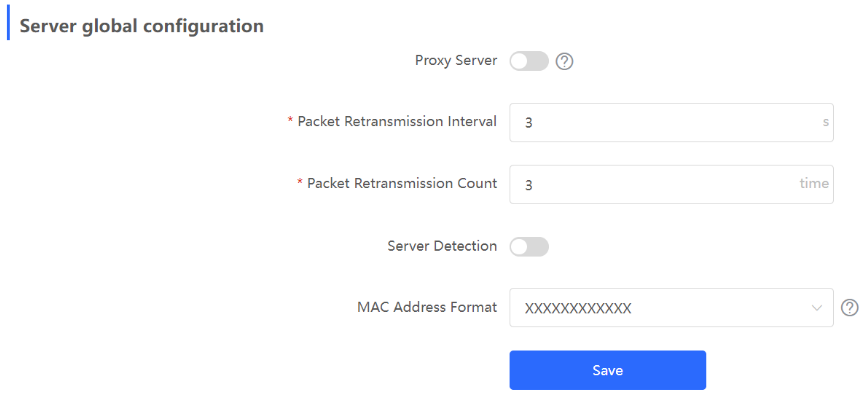
* Accounting Port: 1813

* Shared Password

* Match Order

Parameter	Description
Server IP	IP address of the RADIUS server.
Auth Port	The port number for the RADIUS server to perform user authentication.
Accounting Port	The port number for the RADIUS server to perform user accounting.
Shared Password	Shared key of the RADIUS server.
Match Order	The system supports up to five RADIUS servers. A larger value indicates a higher priority.

(3) Enter the server global configuration parameters, and click **Save**.



Server global configuration

Proxy Server: ○

* Packet Retransmission Interval: 3 s

* Packet Retransmission Count: 3 time

Server Detection: ○

MAC Address Format: XXXXXXXXXXXX

Parameter	Description
Proxy Server	After this function is enabled, local device will act as a proxy for the RADIUS server to send RADIUS messages.

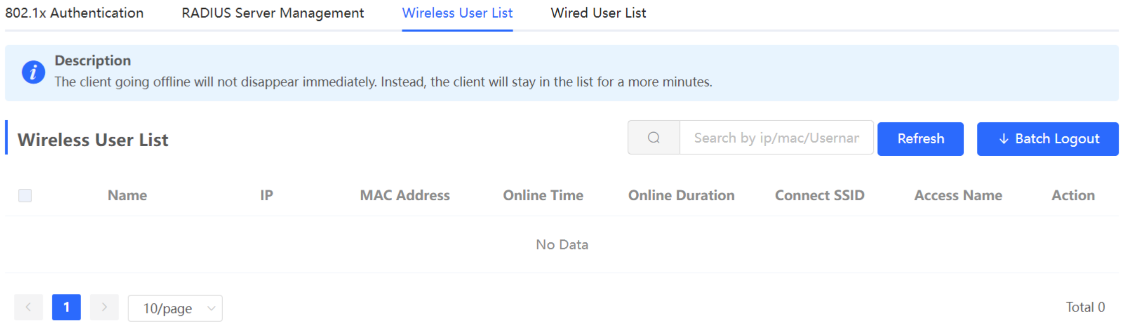
Parameter	Description
Packet Retransmission Interval	Configure the interval during which the device sends a request to a RADIUS server before confirming that the RADIUS server is unreachable.
Packet Retransmission Count	Configure the number of times that the device sends requests to a RADIUS server before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

4.13.4 Checking Authentication User List

When the 802.1x feature is configured on the entire network, and a terminal is authenticated and connected to the network, you can view the list of authenticated users.

[Networkwide Management] Network > **802.1x Authentication**

Click **Wireless User List** or **Wired User List** to view specific user information.



Description

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

Wireless User List

□	Name	IP	MAC Address	Online Time	Online Duration	Connect SSID	Access Name	Action
No Data								

Total 0

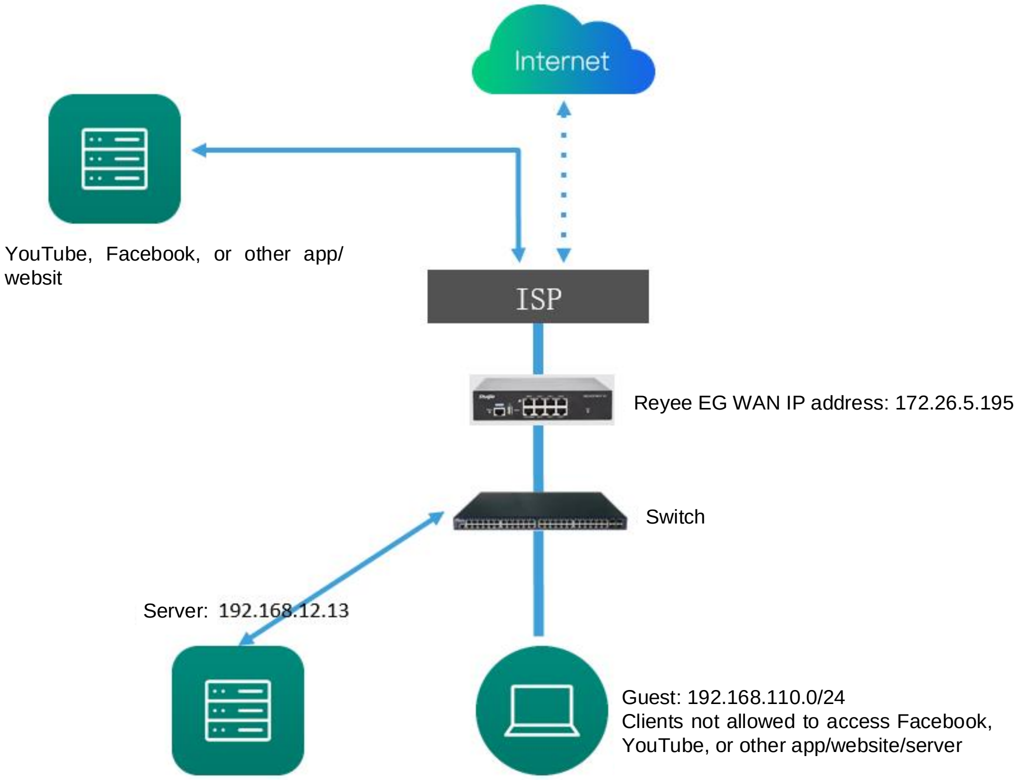
Click **Refresh** to view the latest user list.

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

4.14 Behavior

4.14.1 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.


Internet
YouTube, Facebook, or other app/ websit
ISP
Reyee EG WAN IP address: 172.26.5.195
Switch
Server: 192.168.12.13
Guest: 192.168.110.0/24
Clients not allowed to access Facebook, YouTube, or other app/website/server

4.14.2 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**.

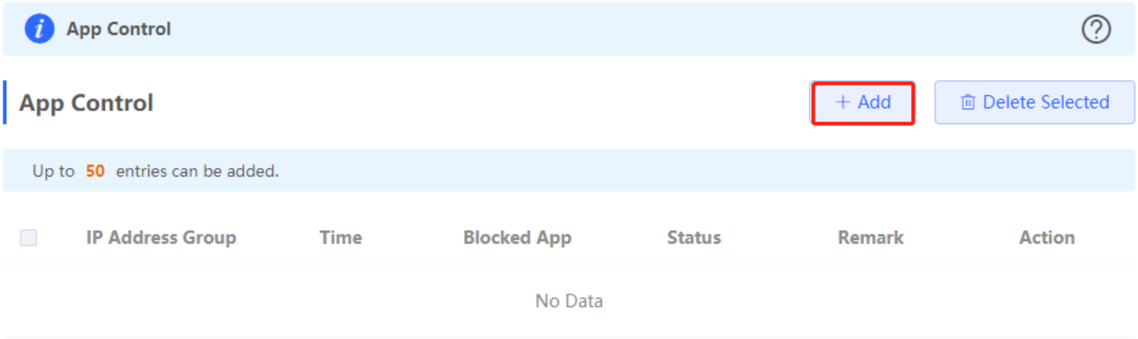
(2) Switch the application library.

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

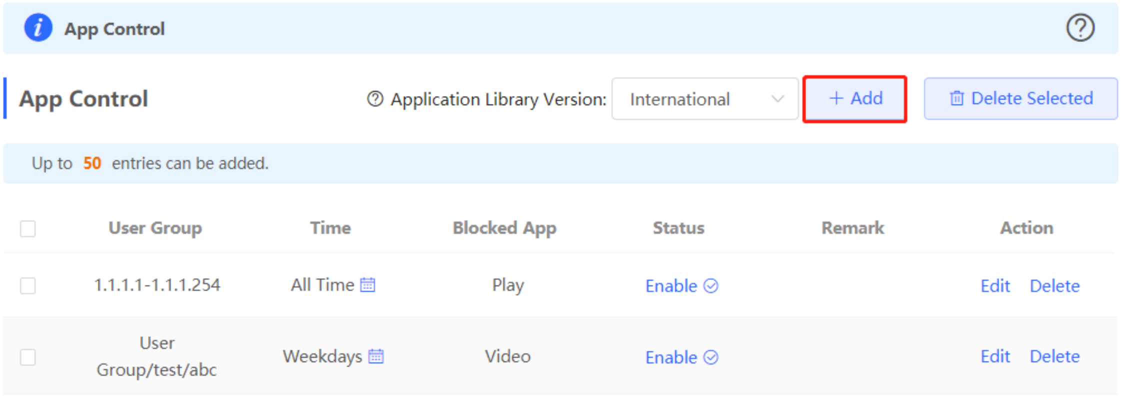
Up to 50 entries can be added.

□	IP Address Group	Time	Blocked App	Status	Remark	Action

No Data

(3) Configure App Control.

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



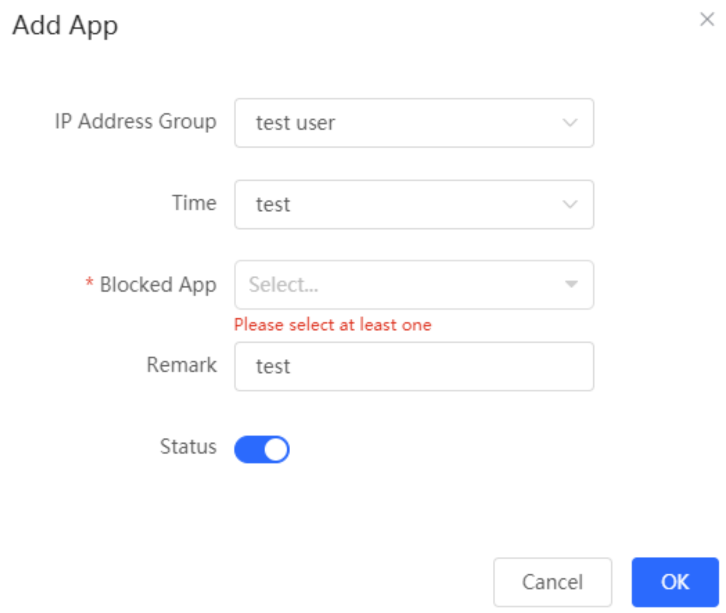
App Control

App Control

Application Library Version: International

Up to 50 entries can be added.

□	User Group	Time	Blocked App	Status	Remark	Action
□	1.1.1.1-1.1.1.254	All Time	Play	Enable ✓		Edit Delete
□	User Group/test/abc	Weekdays	Video	Enable ✓		Edit Delete



Add App

IP Address Group: test user

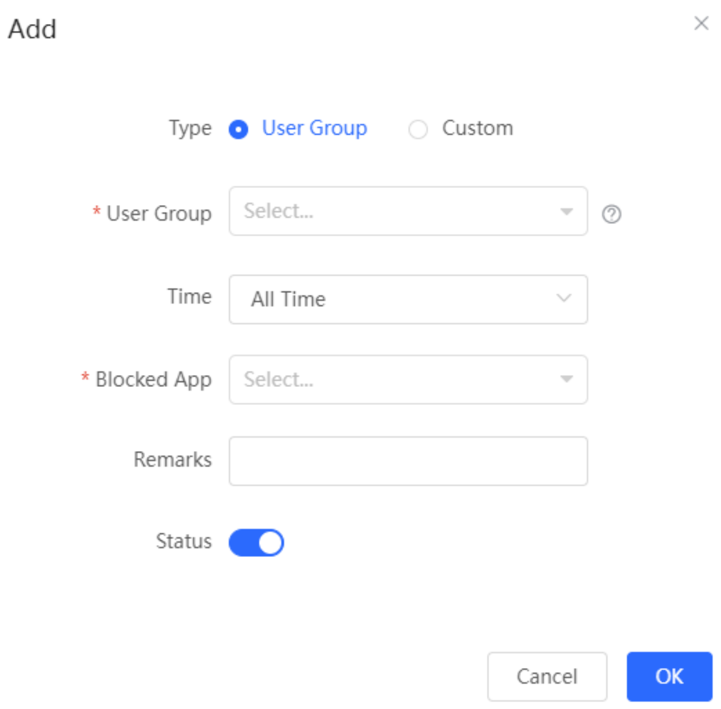
Time: test

* Blocked App: Select...

Please select at least one

Remark: test

Status: On



Add

Type ● User Group ○ Custom

* User Group Select...

Time All Time

* Blocked App Select...

Remarks

Status

Parameter	Description
Type	● **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	Select the users managed by the policy from the list of user groups. 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.
IP Address Group	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.
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.

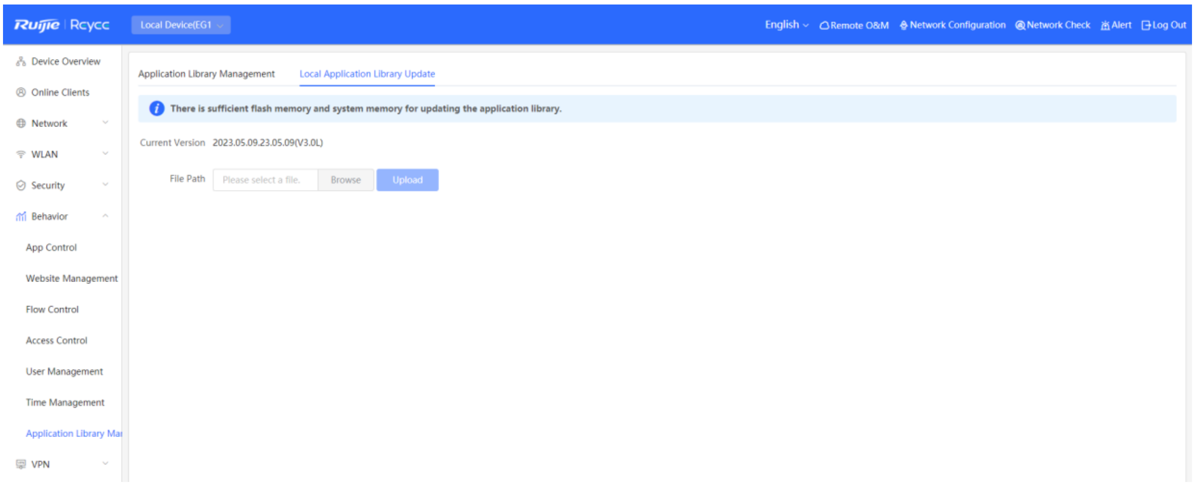
2. Upgrading the Application Library

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 > Application Library Management > 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.



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

Current Version 2023.05.09.23.05.09(V3.0L)

File Path Please select a file.

(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**.

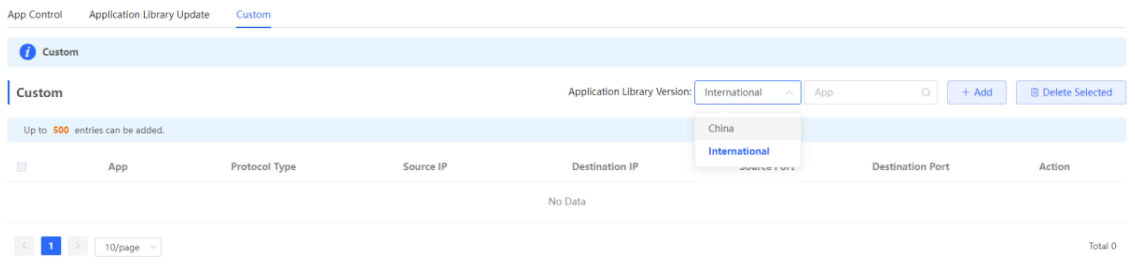
(2) Switch the application library.

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.

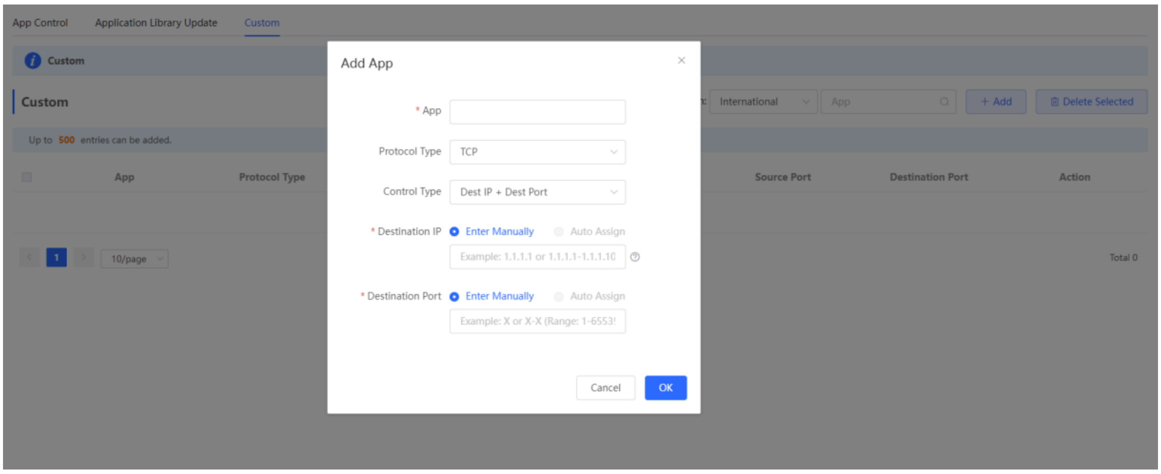
Click **Application Library Version** and select a version. In the displayed dialog box, click **OK**. Wait for a period of time for the system to complete switching.

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

Note

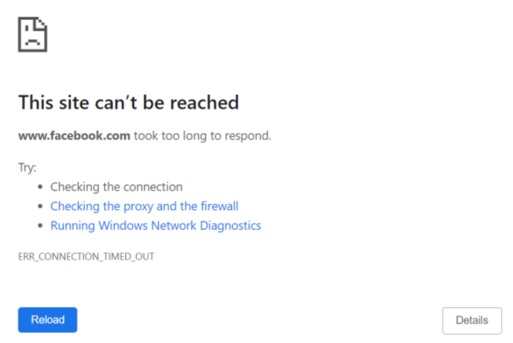
- If **Control Type** is set to **Src IP + Src Port**, you need to set the source IP address and source port.
- If **Control Type** is set to **Dest IP + Dest Port**, you need to set the destination IP address and destination port.
- If **Control Type** is set to **Src IP + Dest IP**, you need to set 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 1. Configuring App Control.

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

4.14.3 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**.

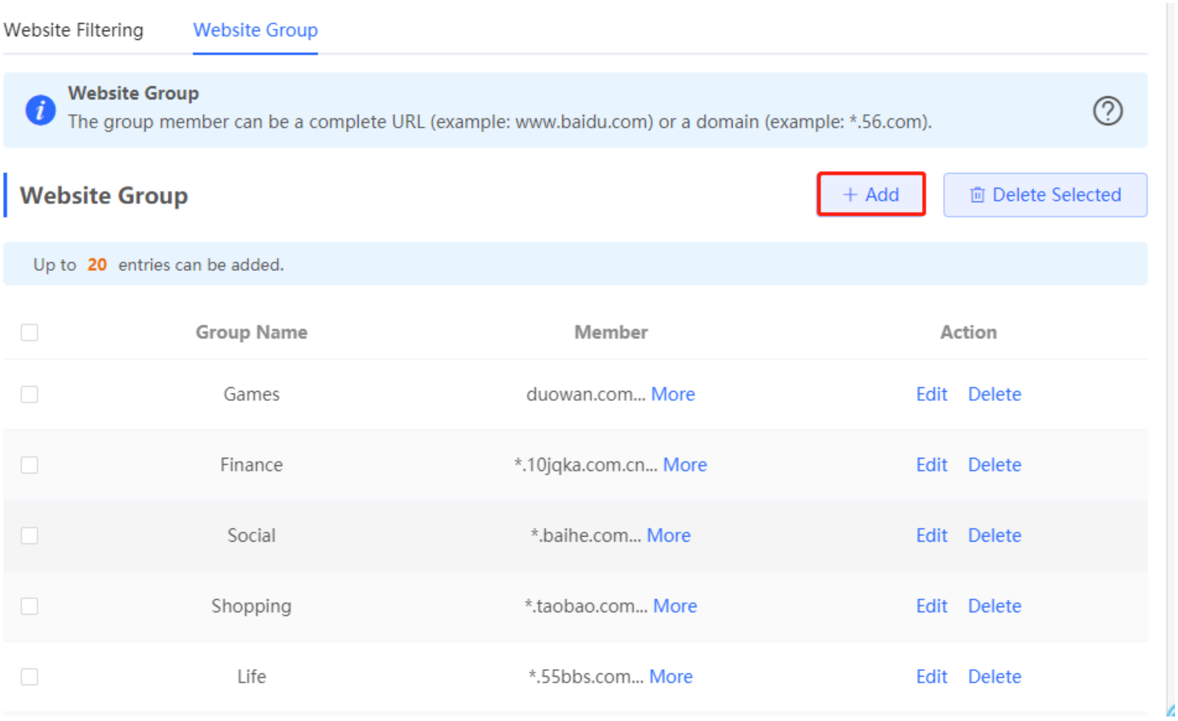
(2) Configure website groups.

a 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.

b 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.

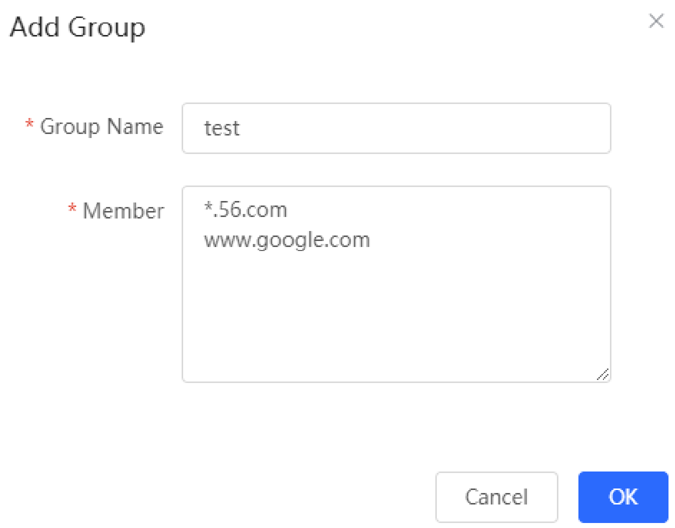


Website Group
The group member can be a complete URL (example: www.baidu.com) or a domain (example: *.56.com).

Website Group

Up to 20 entries can be added.

□	Group Name	Member	Action
□	Games	duowan.com... More	Edit Delete
□	Finance	*.10jqka.com.cn... More	Edit Delete
□	Social	*.baihe.com... More	Edit Delete
□	Shopping	*.taobao.com... More	Edit Delete
□	Life	*.55bbs.com... More	Edit Delete



Add Group

* Group Name: test

* Member:
*.56.com
www.google.com

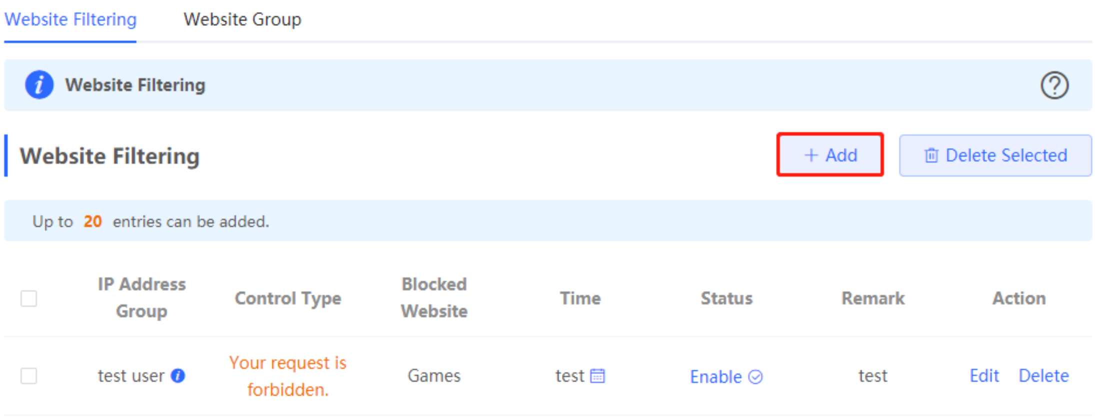
Parameter	Description
Group Name	Configure a unique name for a website group. The name can be a string of 1 to 64 characters.
Member	Specify members in the website group. You can enter multiple websites in a batch. The group member can be a complete URL (such as www.baidu.com) or keyword in the URL (domain 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.



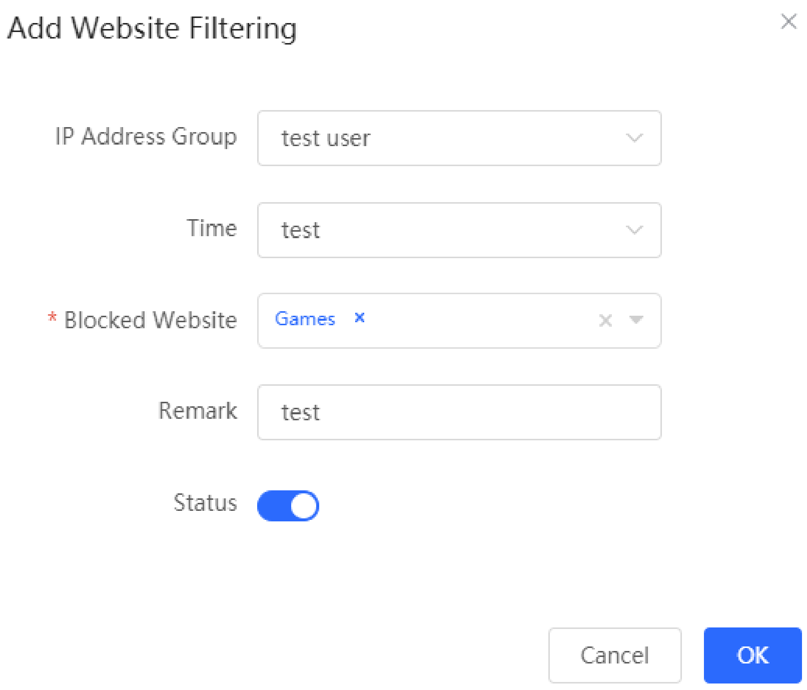
Website Filtering Website Group

Website Filtering

Website Filtering + Add Delete Selected

Up to 20 entries can be added.

□	IP Address Group	Control Type	Blocked Website	Time	Status	Remark	Action
□	test user	Your request is forbidden.	Games	test	Enable	test	Edit Delete



Add Website Filtering

IP Address Group: test user

Time: test

* Blocked Website: Games ×

Remark: test

Status: ●

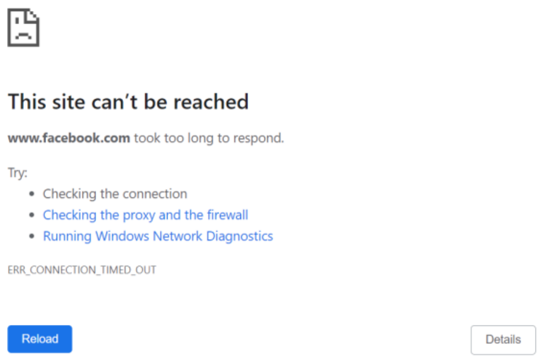
Cancel OK

Parameter	Description
Type	● **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	Select the users managed by the policy from the list of user groups. If all members in the user group are selected, the policy takes effect for the

Parameter	Description
	user group and is also valid for new members added to this group.
IP Address Group	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.
Time	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.
Blocked Website	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.
Remark	Enter the rule description.
Status	Specify whether to enable the website filtering rule.

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

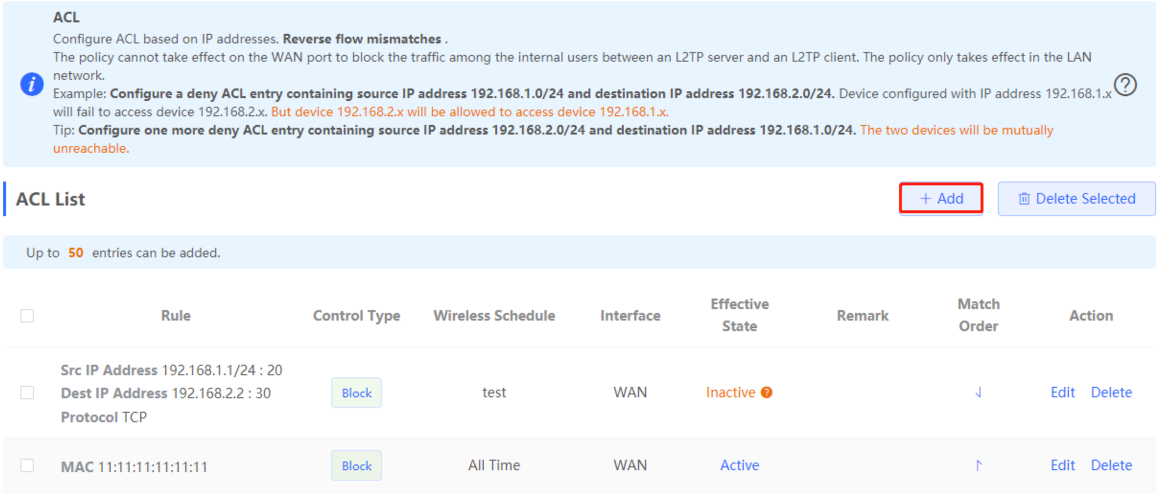
ERR_CONNECTION_TIMED_OUT

4.14.4 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.

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

Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
□	**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
□	**MAC** 11:11:11:11:11:11	Block	All Time	WAN	Active		↑	Edit Delete

Table 4-28 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.

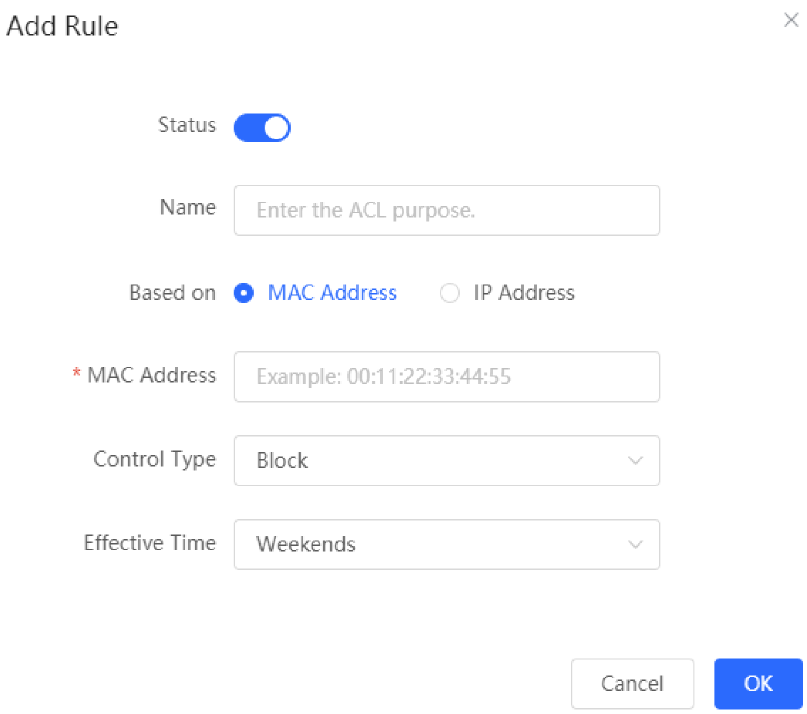
(2) Configure a MAC address-based ACL rule.

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

Status: ●

Name: Enter the ACL purpose.

Based on: ● MAC Address ○ IP Address

* MAC Address: Example: 00:11:22:33:44:55

Control Type: Block

Effective Time: Weekends

Table 4-29 MAC Address-based ACL Configuration

Parameter	Description
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.
Name	Enter the rule description, which is used to uniquely identify a rule.
MAC Address	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. ● Allow: Permit the data packets matching the conditions. ● Block: Drop the data packets matching the conditions.
Effective Time	You can select a time range from the drop-down list box, or select **Custom** and manually enter the specific time range.

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

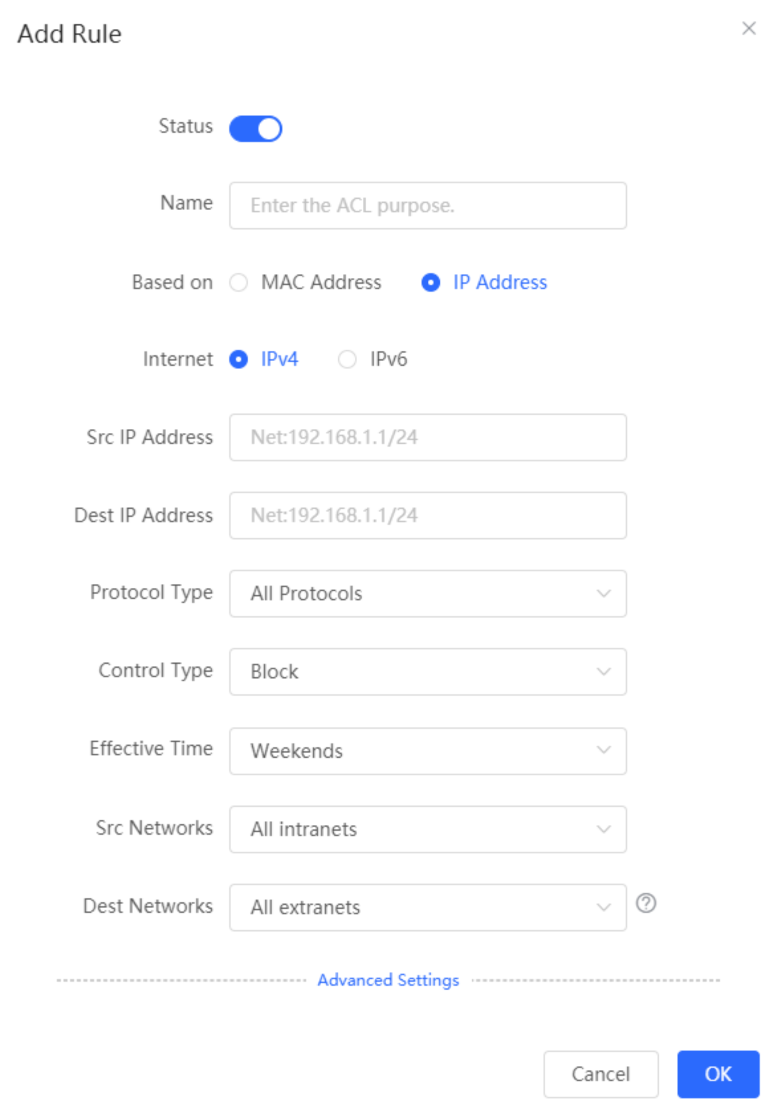
IP address-based ACL rules enable the device to match data flows based on the source IP address, destination IP address, and protocol number.

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

Status: On

Name: Enter the ACL purpose.

Based on: ○ MAC Address ● IP Address

Internet: ● IPv4 ○ IPv6

Src IP Address: Net:192.168.1.1/24

Dest IP Address: Net:192.168.1.1/24

Protocol Type: All Protocols

Control Type: Block

Effective Time: Weekends

Src Networks: All intranets

Dest Networks: All extranets

Table 4-30 IP Address-based ACL Configuration

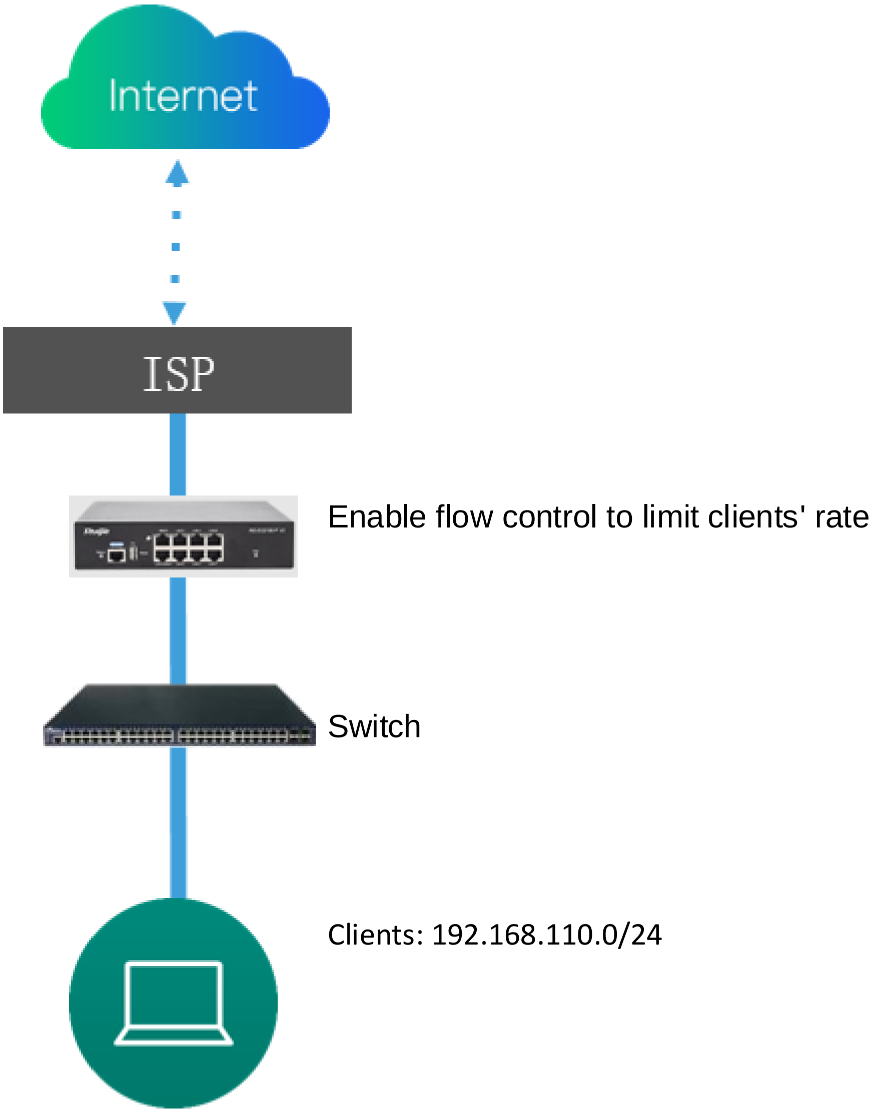
Parameter	Description
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.

Parameter	Description
Name	Enter the rule description, which is used to uniquely identify a rule.
Internet	Format of the IP address. Both IPv4 and IPv6 address formats are supported.
Src IP Address	Enter the source IP address 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:	Enter the destination IP address 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 **All Protocols**, **TCP**, **UDP**, **ICMP**, and **TCP&UDP**.
Control Type	Specify the method for processing data packets matching conditions. ● 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.
Effective Time	You can select a time range from the drop-down list box, or select **Custom** and manually enter the specific time range.
Src Networks	Indicate the source interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Intranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.
Dest Networks	Indicate the destination interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Extranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.

4.15 Flow Control

4.15.1 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.


Internet
ISP
Enable flow control to limit clients' rate
Switch
Clients: 192.168.110.0/24

4.15.2 Smart Flow Control

1. Overview

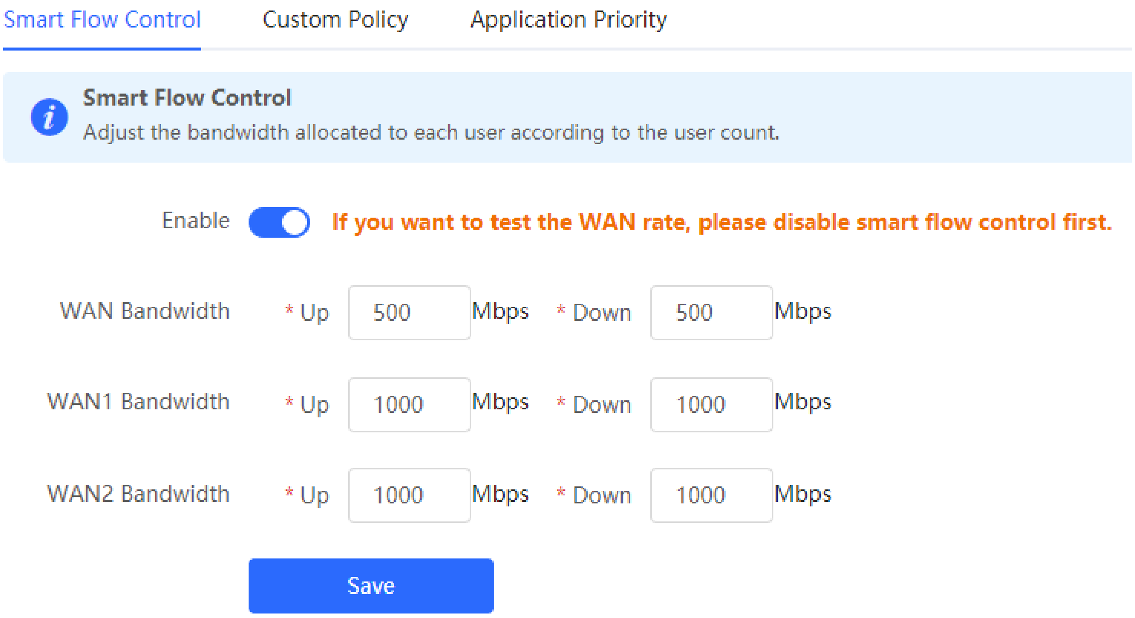
To limit uplink and downlink traffic bandwidth of device ports (such as WAN and WAN 1), you can enable smart flow control. After the line bandwidth is configured for a port, the uplink and downlink traffic of the port will be limited within the specified range. In addition, per-user bandwidth must be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

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 500 Mbps * Down 500 Mbps

WAN1 Bandwidth * Up 1000 Mbps * Down 1000 Mbps

WAN2 Bandwidth * Up 1000 Mbps * Down 1000 Mbps

Table 4-31 **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 Mbps.

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

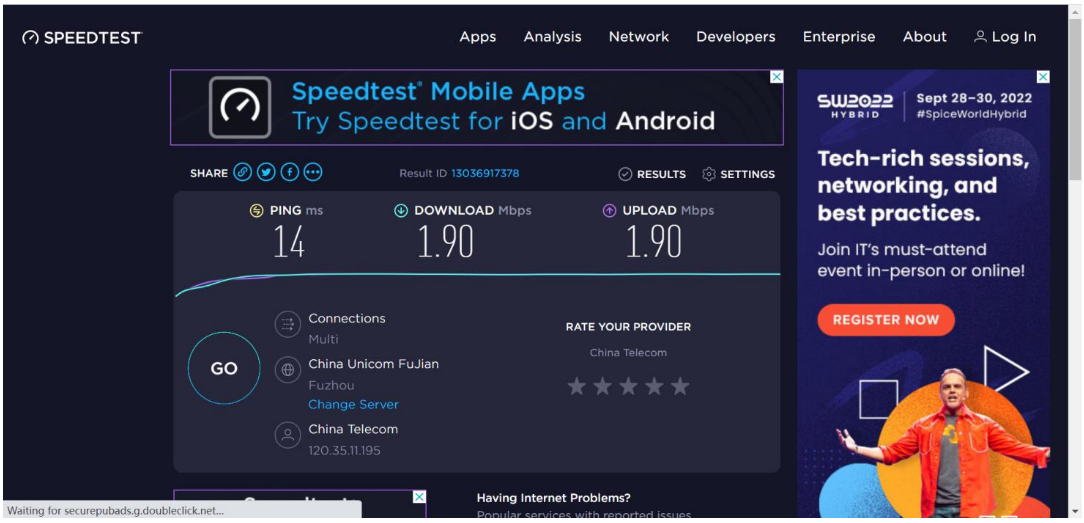
Note

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 Mbps.



SPEEDTEST

Apps Analysis Network Developers Enterprise About Log In

Speedtest® Mobile Apps
Try Speedtest for iOS and Android

SHARE Result ID 13036917378 RESULTS SETTINGS

PING ms 14
DOWNLOAD Mbps 1.90
UPLOAD Mbps 1.90

GO

Connections
Multi

China Unicom FuJian
Fuzhou
Change Server

China Telecom
120.35.11.195

RATE YOUR PROVIDER
China Telecom
★★★★★

SW2022 HYBRID Sept 28–30, 2022 #SpiceWorldHybrid
Tech-rich sessions, networking, and best practices.
Join IT's must-attend event in-person or online!
REGISTER NOW

Having Internet Problems?
Popular services with reported issues

Waiting for securepubads.g.doubleclick.net...

4.15.3 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.

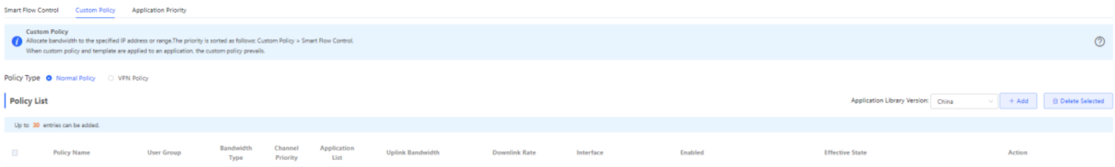
2. Getting Started

Before you configure a custom policy, enable smart flow control. For details, see section 4.15.2 Smart Flow Control.

3. Configuration Steps

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

(1) Set **Policy Type**.



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 Type ● Normal Policy ○ VPN Policy

Policy List

Application Library Version: China + Add Delete Selected

Up to 30 entries can be added.

□	Policy Name	User Group	Bandwidth Type	Channel Priority	Application List	Uplink Bandwidth	Downlink Rate	Interface	Enabled	Effective State	Action

Note

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

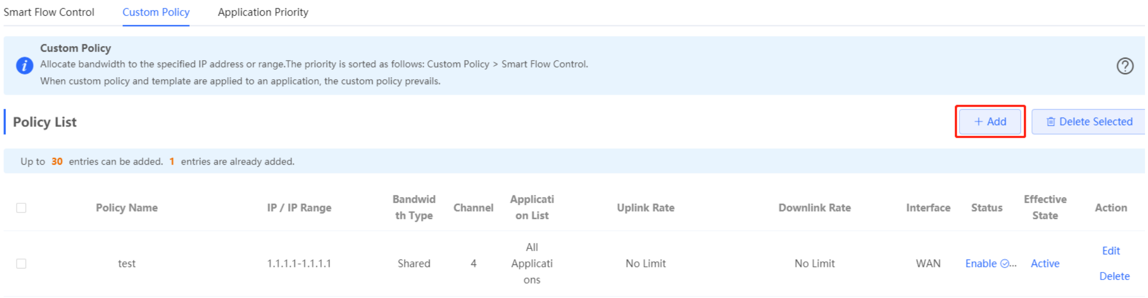
(2) Switch the application library.

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 4.15.4 Application Priority), and the old application control policy may take ineffective (see section 4.14.2 App Control). Proceed with caution.



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

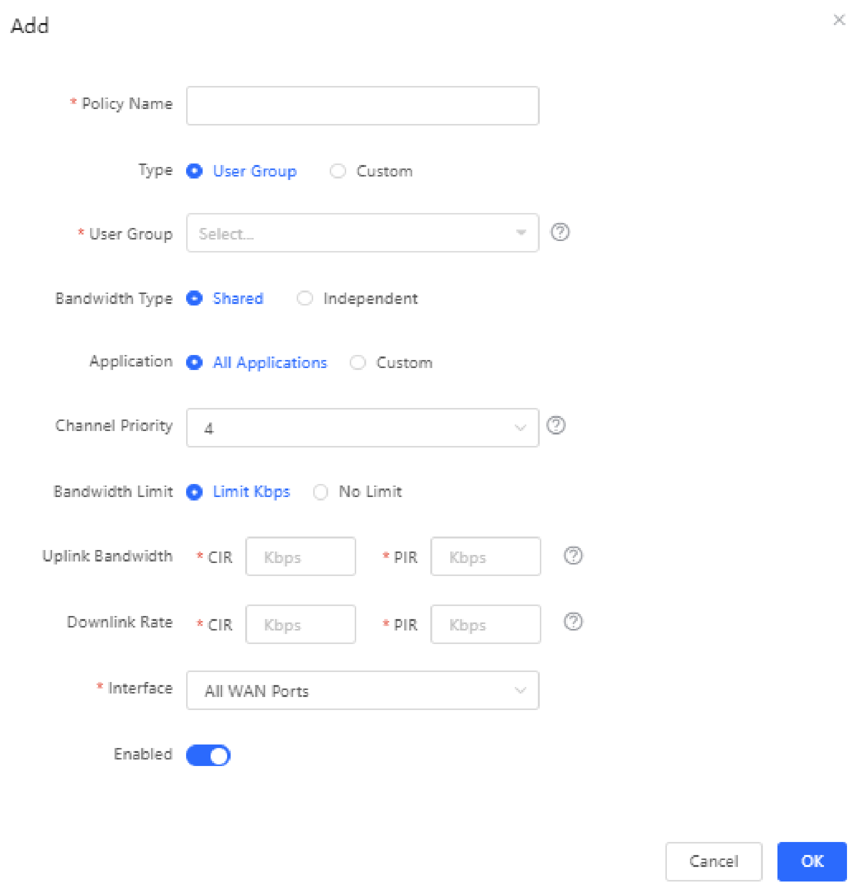
Up to 30 entries can be added. 1 entries are already added.

□	Policy Name	IP / IP Range	Bandwidth Type	Channel	Application List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
□	test	1.1.1.1-1.1.1.1	Shared	4	All Applications	No Limit	No Limit	WAN	Enable ⊘...	Active	Edit Delete

(3) Set a custom policy.

- Set a custom normal policy.

a 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 Select...

Bandwidth Type ● Shared ○ Independent

Application ● All Applications ○ Custom

Channel Priority 4

Bandwidth Limit ● Limit Kbps ○ No Limit

Uplink Bandwidth * CIR Kbps * PIR Kbps

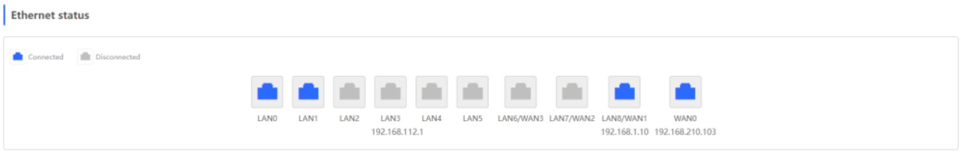
Downlink Rate * CIR Kbps * PIR Kbps

* Interface All WAN Ports

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: ● **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	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. 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.  Ethernet status Connected Disconnected LAN0 LAN1 LAN2 LAN3 192.168.112.1 LAN4 LAN5 LAN6/WAN3 LAN7/WAN2 LAN8/WAN1 192.168.1.10 WAN0 192.168.210.103
Bandwidth Type	● **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	When **Bandwidth Type** is set to **Shared**, the flow control policy can be configured to take effect only on specified applications. ● **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. Traffic of the selected applications is limited by the policy.
Channel Priority	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. 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 4.15.4 Application Priority.
Bandwidth Limit	Configure whether to limit the bandwidth. ● **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	Configure the uplink or downlink data transmission rate, in kbps. ● **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

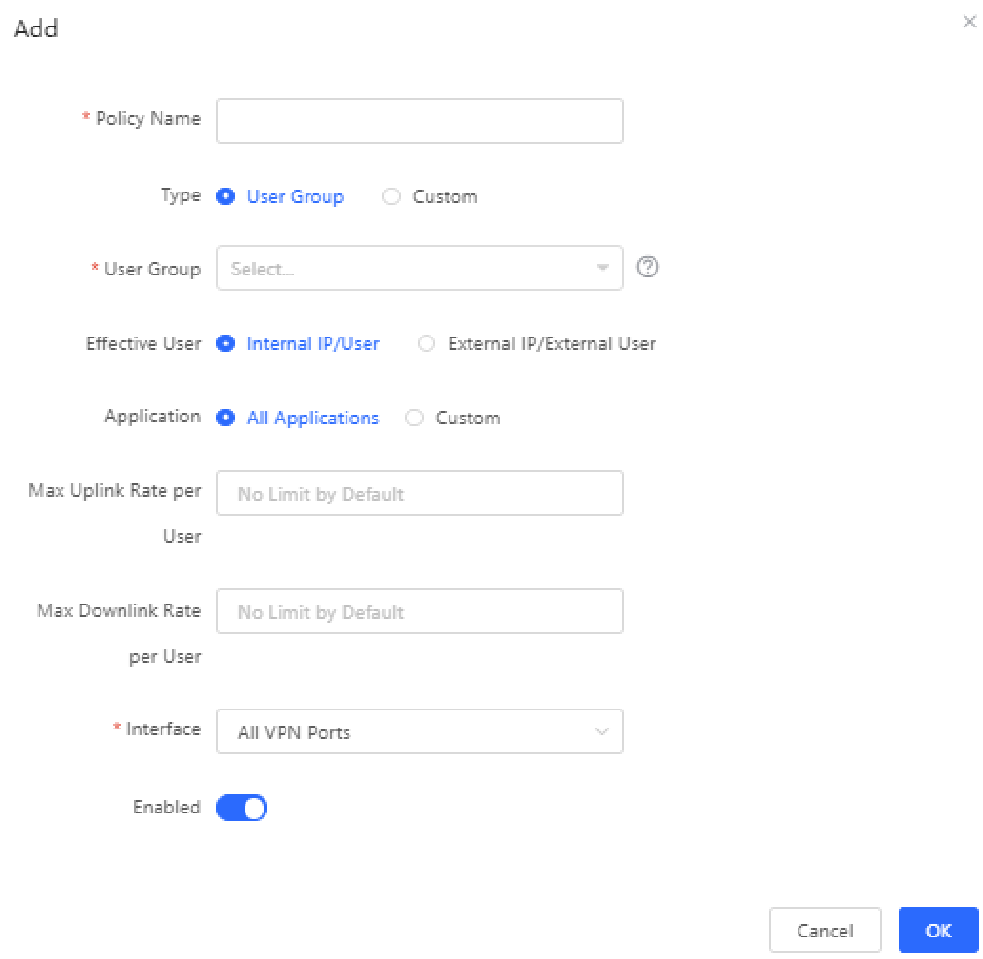
After switching the application library version, you may need to reconfigure the application list.

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 Select...

Effective User ● Internal IP/User ○ External IP/External User

Application ● All Applications ○ Custom

Max Uplink Rate per User No Limit by Default

Max Downlink Rate per User No Limit by Default

* Interface All VPN Ports

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: ● **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: ● **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: ● 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. ● **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 Max Downlink Rate per User	Configure the maximum uplink or downlink data transmission rate when multiple users share the bandwidth, in kbps. It is optional and can be configured only when **Bandwidth Type** is set to **Independent**. The rate is not limited by default.

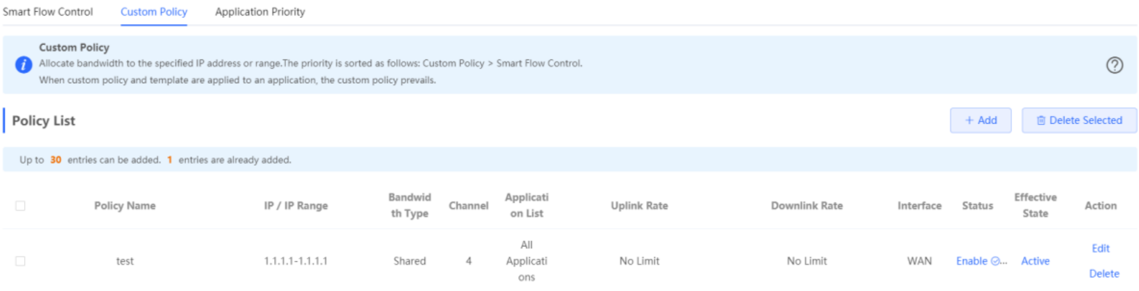
Parameter	Description
Interface	Specify the VPN port on which the policy takes effect. When it is set to **All VPN Ports**, the policy is applied to all traffic of the VPN type.
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.

c Click OK.

(4) 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**.

- Normal policy list



Custom Policy

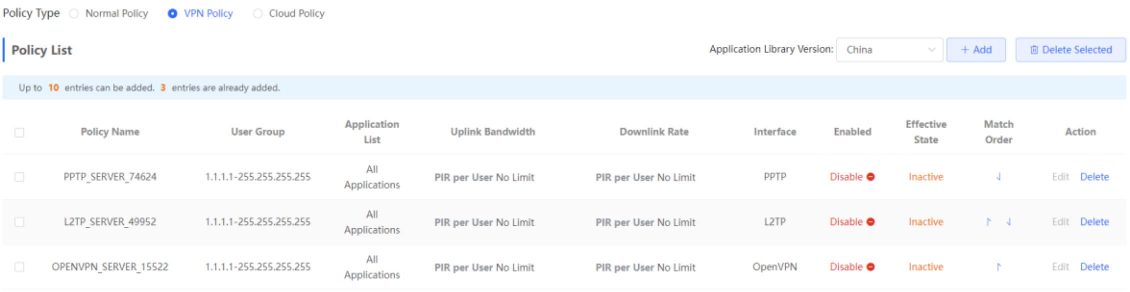
Allocate bandwidth to the specified IP address or range.The priority is sorted as follows: Custom Policy > Smart Flow Control.

When custom policy and template are applied to an application, the custom policy prevails.

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

□	Policy Name	IP / IP Range	Bandwidth Type	Channel	Application List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
□	test	1.1.1.1-1.1.1.1	Shared	4	All Applications	No Limit	No Limit	WAN	Enable ⊘...	Active	Edit Delete

- VPN policy list


Policy Type ○ Normal Policy ● VPN Policy ○ Cloud Policy

Application Library Version: China

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

□	Policy Name	User Group	Application List	Uplink Bandwidth	Downlink Rate	Interface	Enabled	Effective State	Match Order	Action
□	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
□	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
□	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 4-32 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.

Parameter	Description
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.
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.

4.15.4 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

- Before you configure an application priority, enable smart flow control. For details, see section 4.15.2 Smart Flow Control.
- Confirm that the appropriate application library is selected on the **Custom Policy** page (see section 4.15.3 Custom Policies).

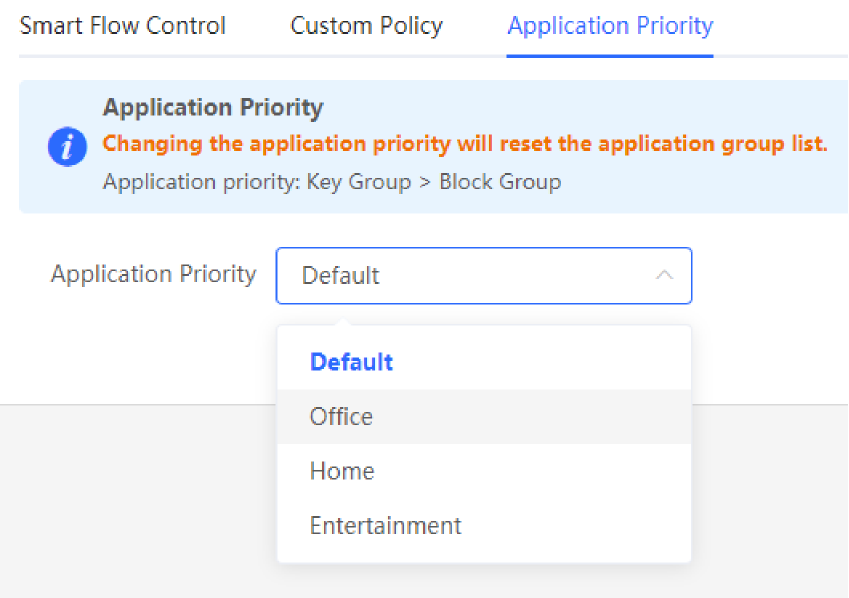
3. Configuration Steps

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.



Application Priority

Changing the application priority will reset the application group list.

Application priority: Key Group > Block Group

Application Priority: Default

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.

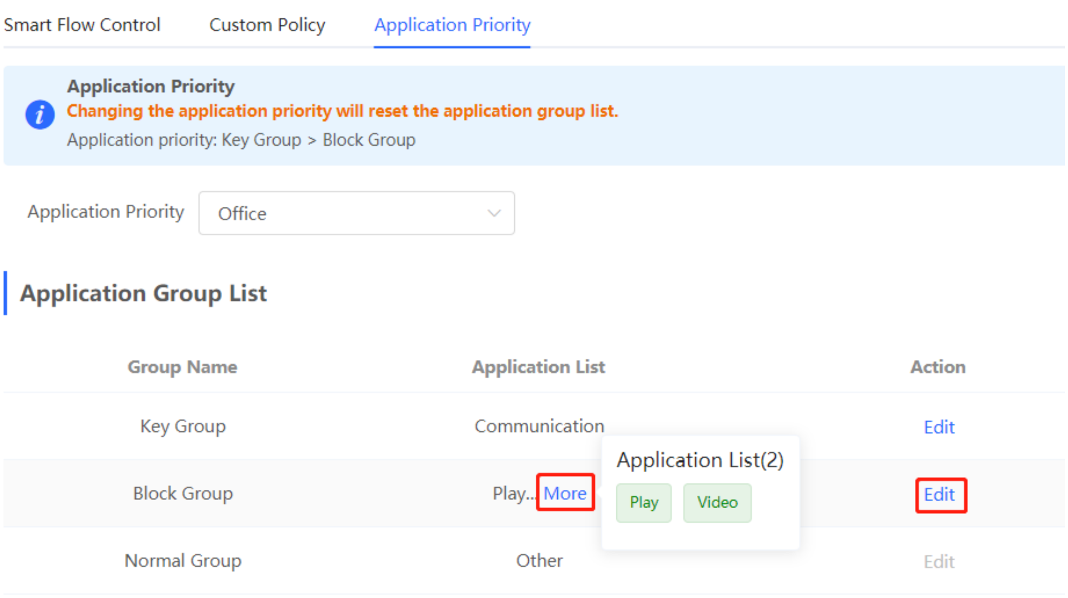
(2) Create an application group list.

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.



Application Priority

Changing the application priority will reset the application group list.

Application priority: Key Group > Block Group

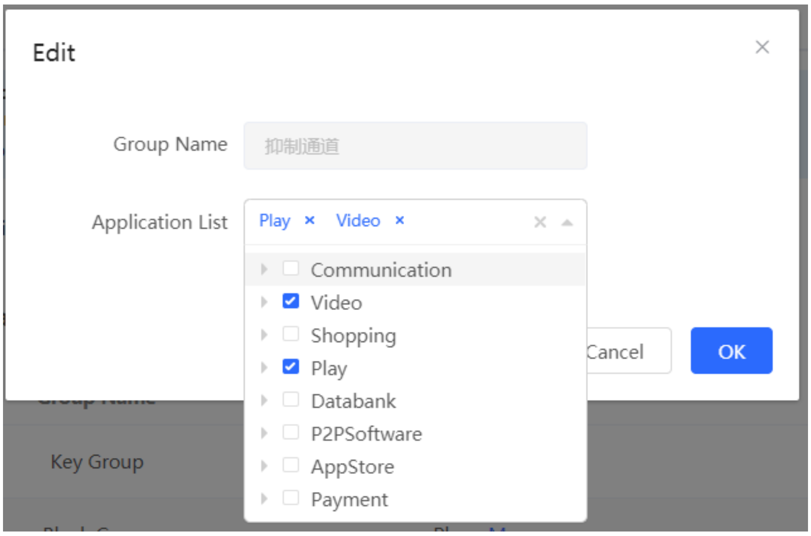
Application Priority: Office

Application Group List

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

Application List(2)

Play Video



Edit

Group Name: 抑制通道

Application List: Play × Video ×

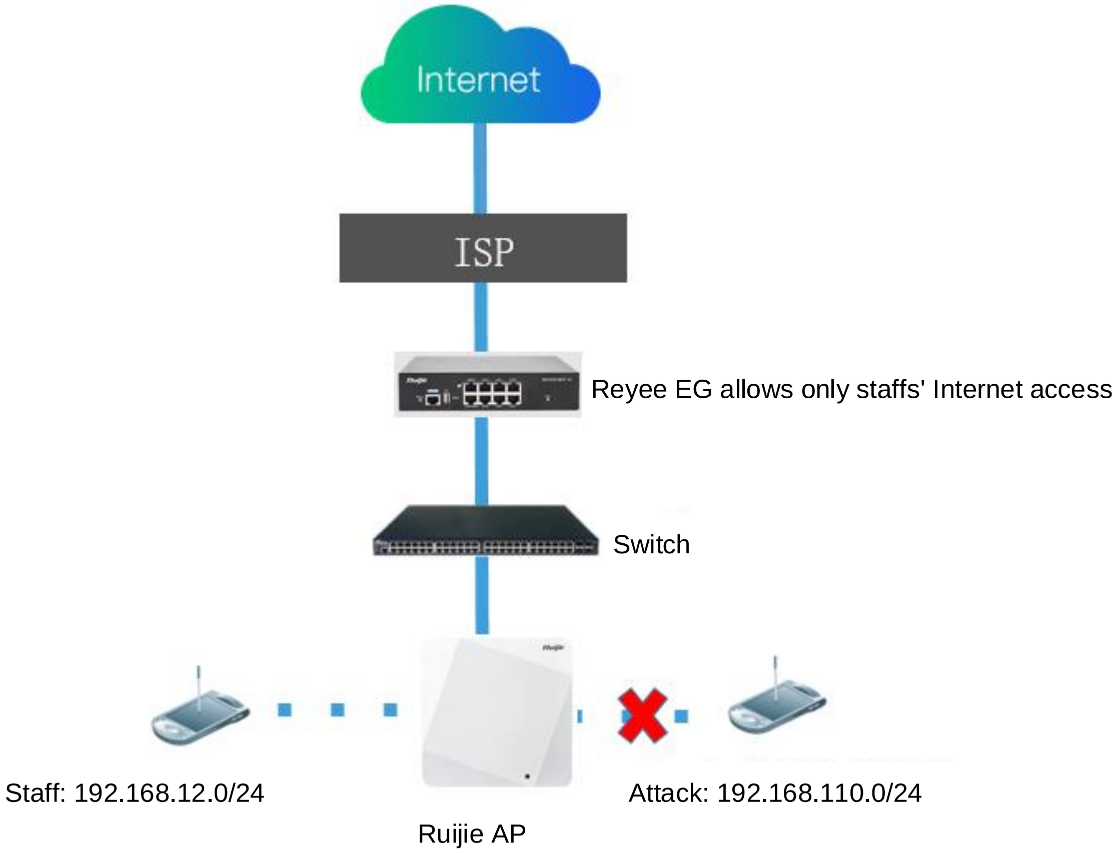
- □ Communication
- ☑ Video
- □ Shopping
- ☑ Play
- □ Databank
- □ P2PSoftware
- □ AppStore
- □ Payment

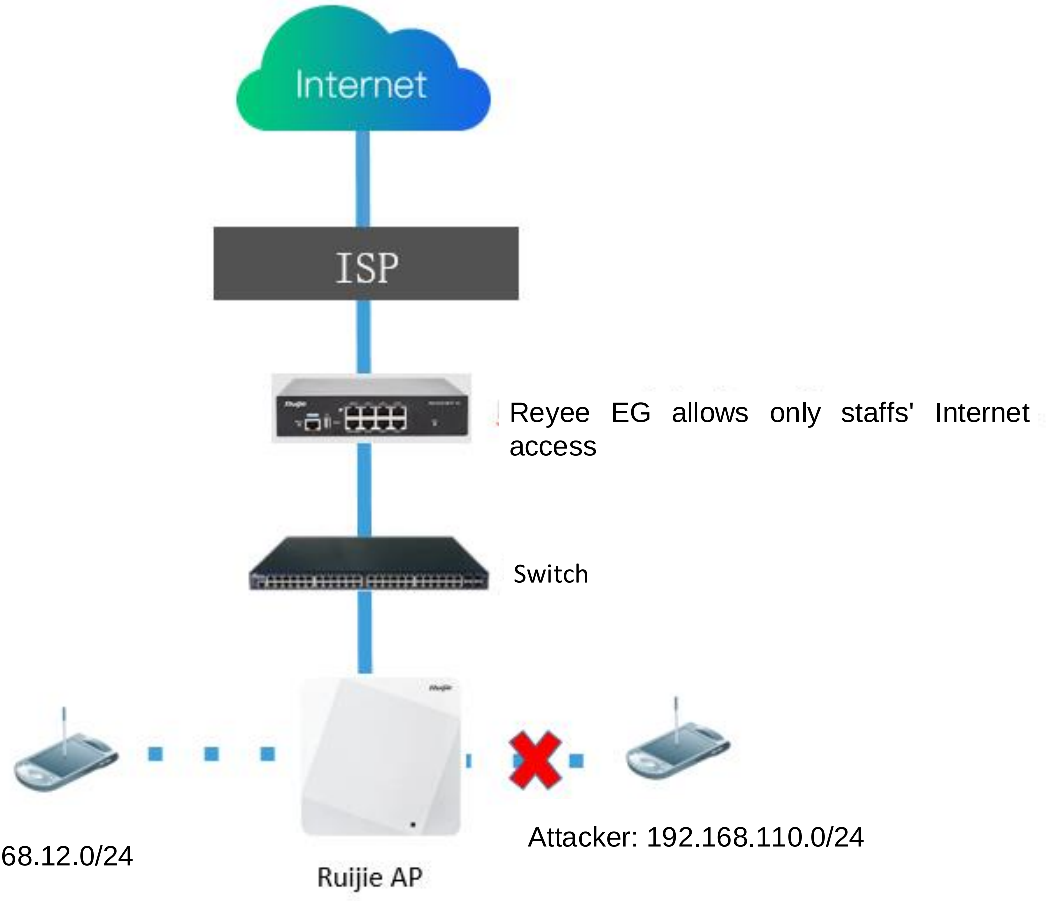
Caution

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

4.16 Security

4.16.1 Application Scenario




Internet
ISP
Reyee EG allows only staffs' Internet access
Switch
Staff: 192.168.12.0/24
Ruijie AP
Attacker: 192.168.110.0/24

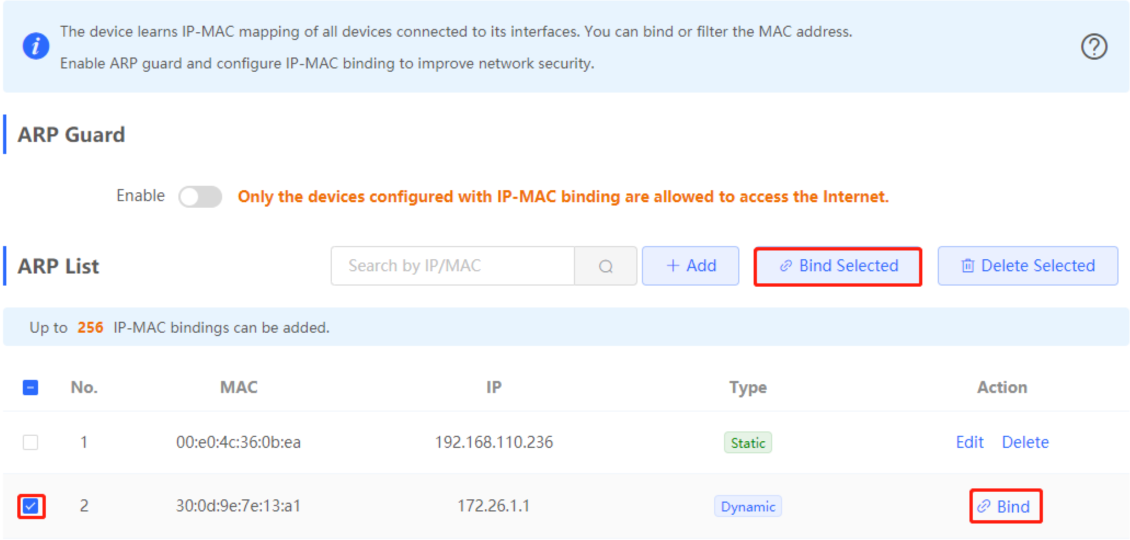
4.16.2 Configuring the ARP List and ARP Guard

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.



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.

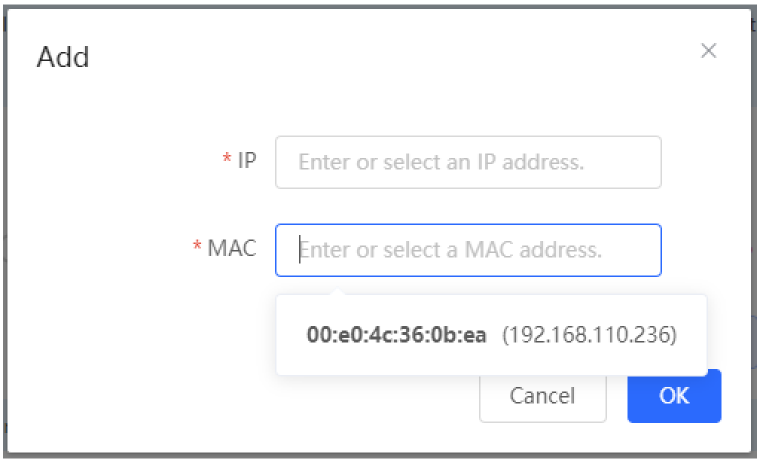
ARP List

Search by IP/MAC | + Add | Bind Selected | Delete Selected

Up to 256 IP-MAC bindings can be added.

☐	No.	MAC	IP	Type	Action
☐	1	00:e0:4c:36:0b:ea	192.168.110.236	Static	Edit Delete
☑	2	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	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.



Add

* IP: Enter or select an IP address.

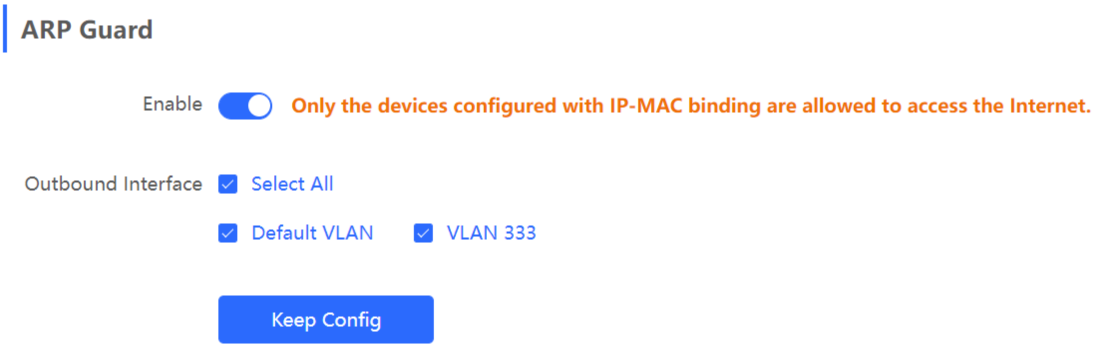
* MAC: Enter or select a MAC address.

00:e0:4c:36:0b:ea (192.168.110.236)

Cancel | OK

(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

Keep Config

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.

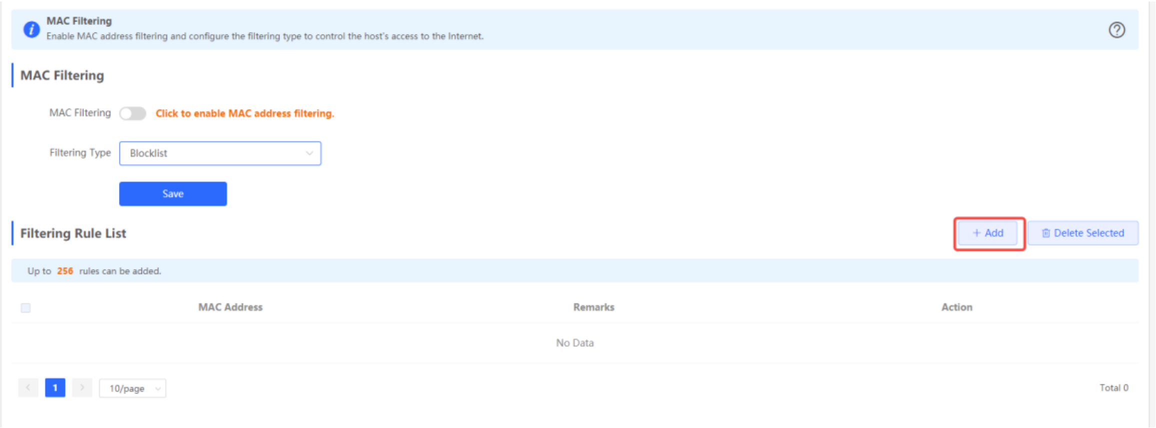
4.16.3 Configuring MAC Address Filtering

You can enable MAC address filtering and configure an allowlist or blocklist to effectively control Internet access from LAN hosts.

- Allowlist: Allow only hosts whose MAC addresses are in the filter rule list to access the Internet.
- Blocklist: Prevent hosts whose MAC addresses are in the filter rule list from accessing the Intern

(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

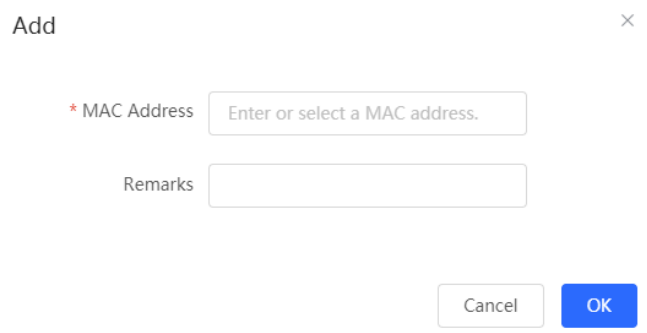
MAC Filtering: Click to enable MAC address filtering.

Filtering Type: Blocklist

Filtering Rule List

Up to 256 rules can be added.

	MAC Address	Remarks	Action
	No Data		

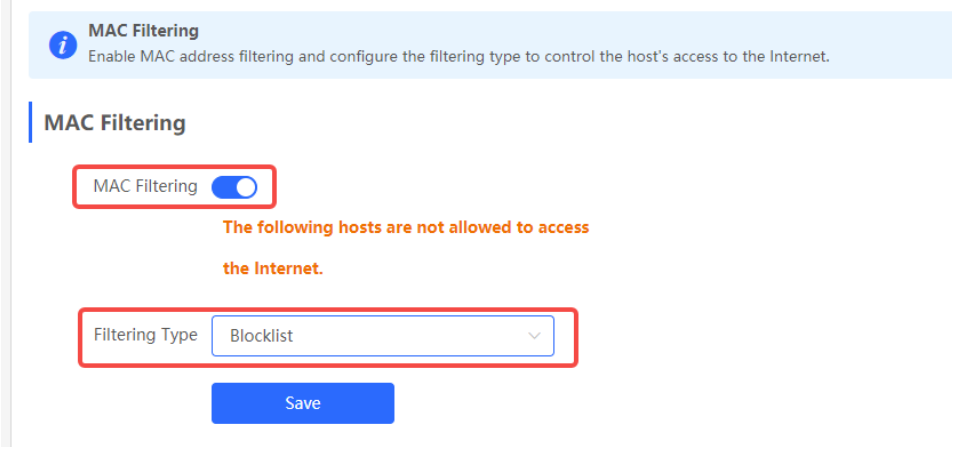


Add

* MAC Address: Enter or select a MAC address.

Remarks:

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



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

MAC Filtering

MAC Filtering: The following hosts are not allowed to access the Internet.

Filtering Type: Blocklist

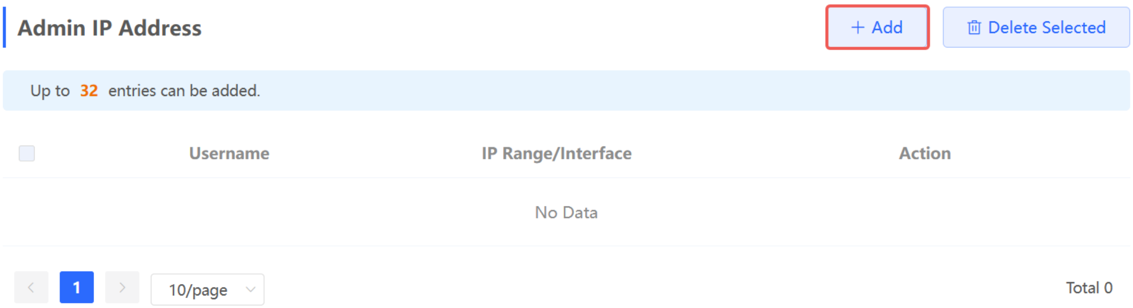
4.17 Configuring Device Security

4.17.1 Configuring an Admin IP Address

Admin IP addresses are exempt from the ping prohibition function. Packets sent from admin IP addresses can pass through and will not be discarded.

Choose **Local Device** > **Security > Local Security > Security Zone > Admin IP Address.**

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

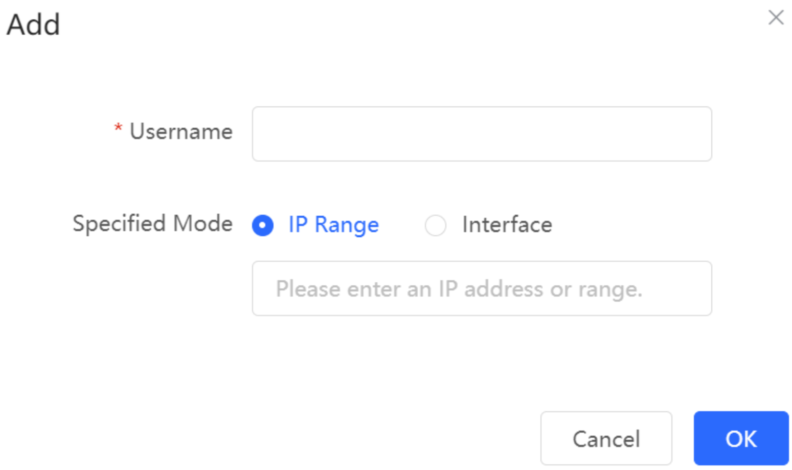


Up to 32 entries can be added.

□	Username	IP Range/Interface	Action
		No Data	

Total 0

1. **Configuring an Admin IP Address (Based on an IP Address)**



* Username

Specified Mode ● IP Range ○ Interface

Please enter an IP address or range.

(1) Configure a name for the admin IP address.

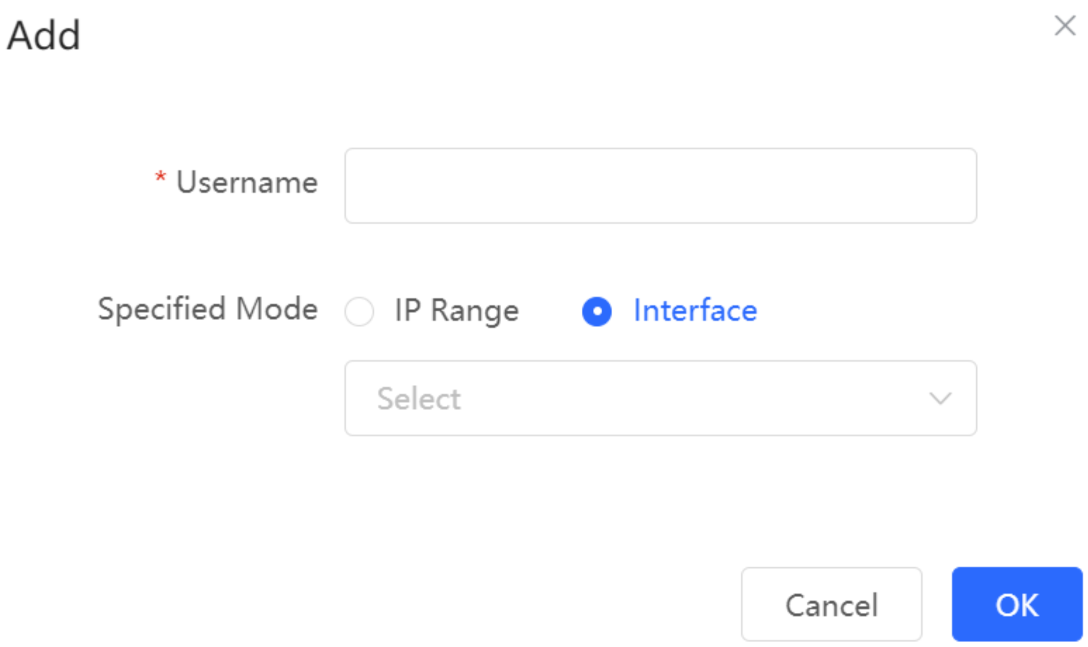
The name is a string of 1–32 characters.

(2) Set **Specific Mode** to **IP Range**.

(3) Configure an IP address.

You can specify a single P address or an IP address range.

2. Configuring an Admin IP Address (Based on a Port)



(1) Configure a name for the admin IP address.

The name is a string of 1–32 characters.

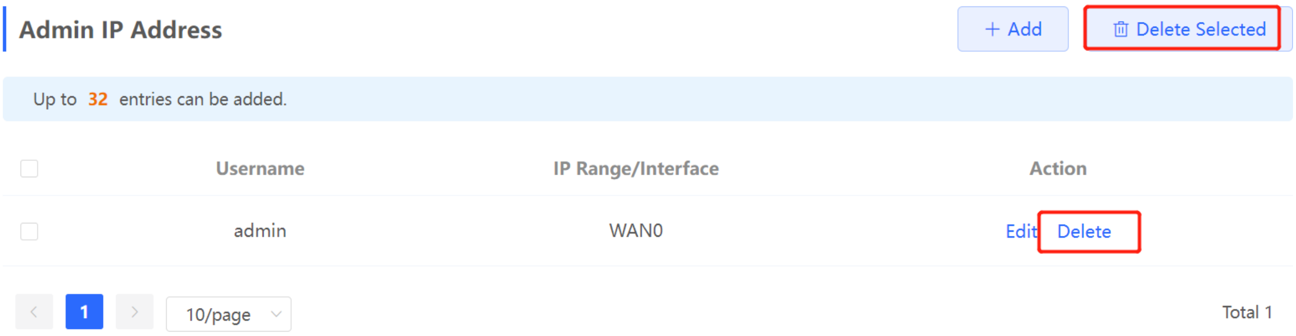
(2) Set **Specific Mode** to **Interface**.

(3) Specify the port.

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

3. Deleting an Admin IP Address

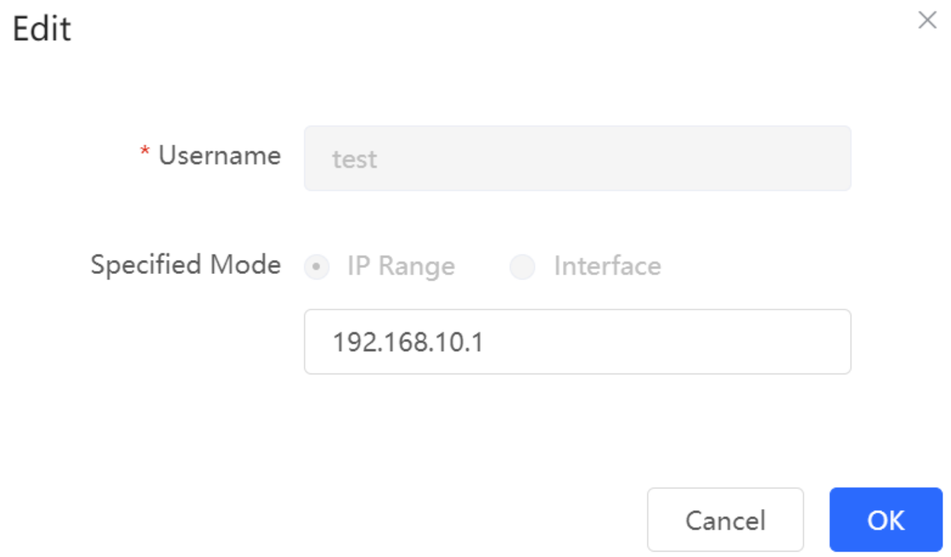
- Select an entry and click **Delete** to delete information about the admin IP address.
- Select multiple entries and click **Delete Selected** to bulk delete selected entries.



□	Username	IP Range/Interface	Action
□	admin	WAN0	Edit Delete

4. Editing Information About an Admin IP Address

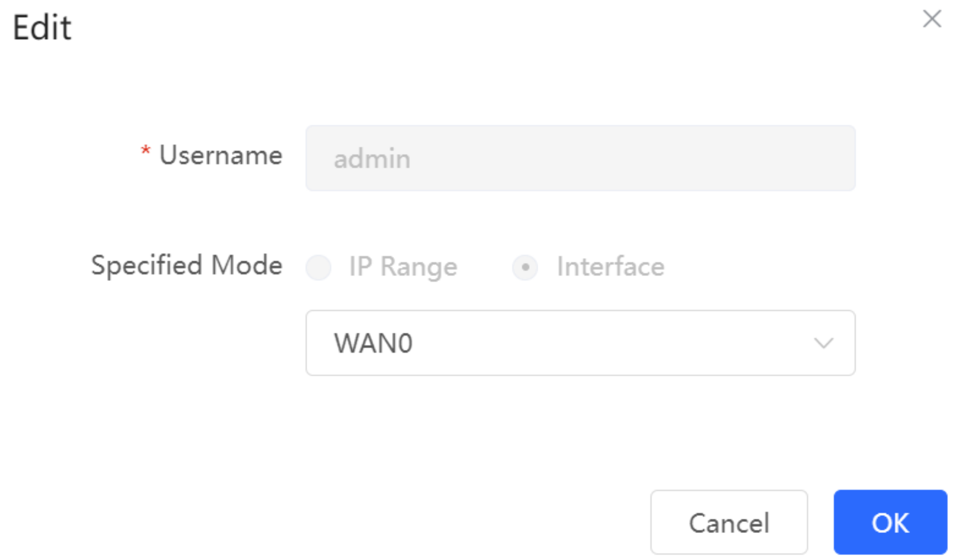
You cannot modify the name and specified mode of an admin IP address but modify the IP address range or port in the specified mode.


Edit

* Username: test

Specified Mode: ● IP Range ○ Interface

192.168.10.1


Edit

* Username: admin

Specified Mode: ○ IP Range ● Interface

WAN0

4.17.2 Configuring Security Zones

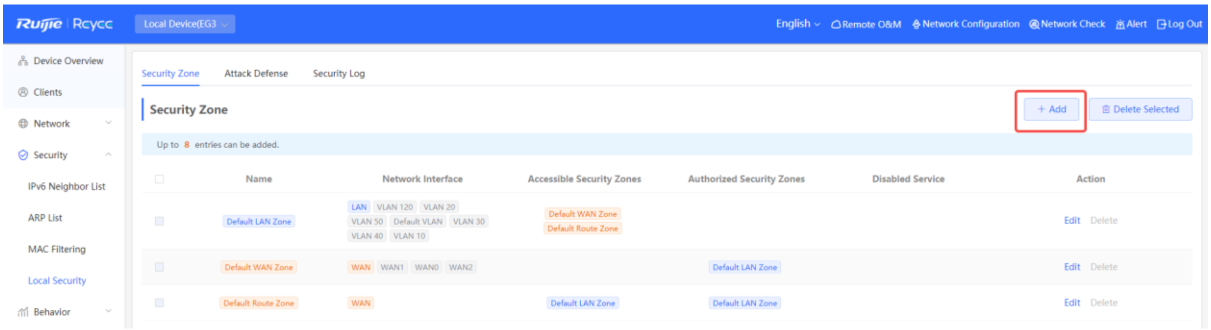
Note

- This feature is not supported on RG-EG105G-P-L.
- For devices that do not support SNMP, the SNMP service cannot be disabled in a LAN zone.

A security zone is a logical zone consisting of a group of systems that trust each other and share the same security protection requirements. Generally, a security zone consists of a group of interfaces. Networks formed by interfaces in the same security zone share the same security attributes. Each interface can only belong to one security zone.

- Up to eight security zones can be added.
- Pre-defined security zones include:
  - Pre-defined LAN zone: By default, all VLANs are mapped to the pre-defined LAN zone.
  - Pre-defined WAN zone: By default, all WAN interfaces are mapped to the pre-defined WAN zone.

Choose **Security** > **Local Security** > **Security Zone.**



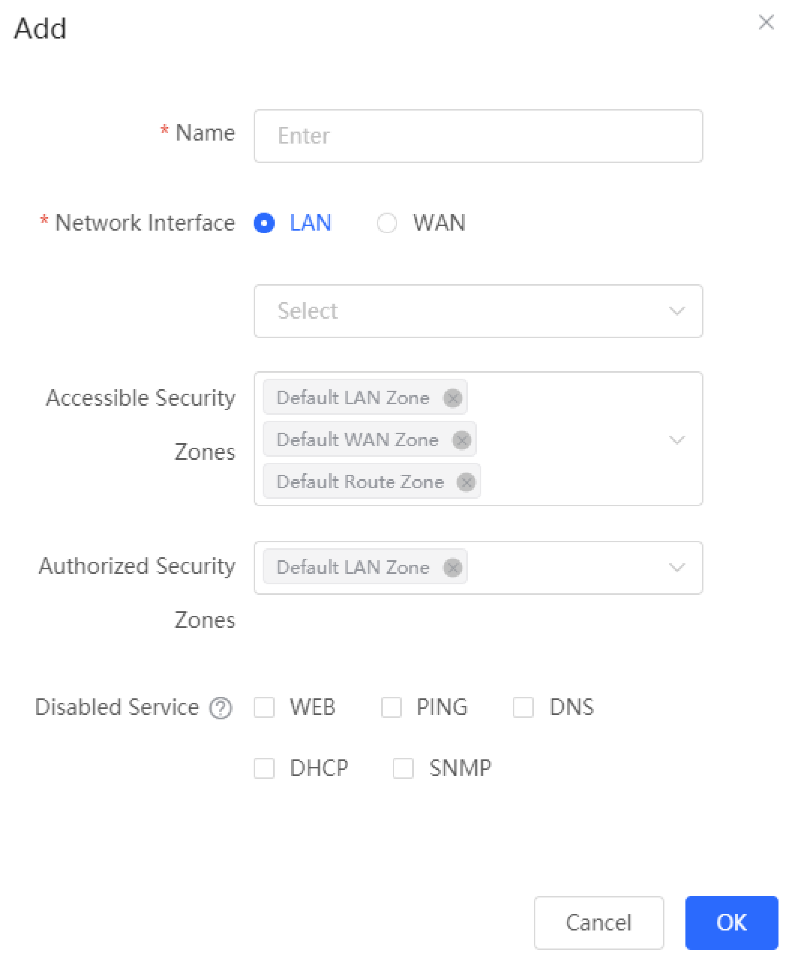
Security Zone

Up to 8 entries can be added.

□	Name	Network Interface	Accessible Security Zones	Authorized Security Zones	Disabled Service	Action
□	Default LAN Zone	LAN VLAN 120 VLAN 20 VLAN 50 Default VLAN VLAN 30 VLAN 40 VLAN 10	Default WAN Zone Default Route Zone			Edit Delete
□	Default WAN Zone	WAN WAN1 WAN0 WAN2		Default LAN Zone		Edit Delete
□	Default Route Zone	WAN	Default LAN Zone	Default LAN Zone		Edit Delete

(1) Click **Add**.

(2) Configure parameters for the security zone.


Add

* Name: Enter

* Network Interface: ● LAN ○ WAN

Select

Accessible Security Zones: Default LAN Zone, Default WAN Zone, Default Route Zone

Authorized Security Zones: Default LAN Zone

Disabled Service: □ WEB □ PING □ DNS □ DHCP □ SNMP

Table 4-33 Description of Security Zone Configuration Parameters

Parameter	Description
Name	Name of the security zone.

Parameter	Description
Network Interface	Interfaces mapped to the security zone, including LAN and WAN. LAN refers to VLAN, and WAN refers to WAN interfaces. Note: After a new security zone is created and VLANs or WAN interfaces are mapped to this new security zone, the VLANs or WAN interfaces will be removed from the pre-defined LAN zone or pre-defined WAN zone.
Accessible Security Zones	Other security zones to which this security zone can access.
Authorized Security Zones	Other security zones that can access this security zone.
Disabled Service	Services disabled for the security zone.

(3) Click **OK**.

4.17.3 Configuring Session Attack Prevention

1. Overview

- Session Attack Prevention
  In a session attack, an attacker sends heavy traffic to the device. In this case, the device has to consume many resources when creating connections. To reduce the impact of the attack, you can limit the rate of creating sessions.
- Flood Attack Prevention
  In a flood attack, an attacker sends tremendous abnormal packets to a device. As a result, the device uses a large amount of resources to handle the packets. This causes the device performance to deteriorate or the system to break down.

  If the value of TCP SYN and other TCP Flood parameters is too small, the authentication function and access to local web pages will be affected.

  If the value of UDP Flood parameter is too small, the DHCP address allocation, DNS domain name resolution, and VPN functionalities will be affected.

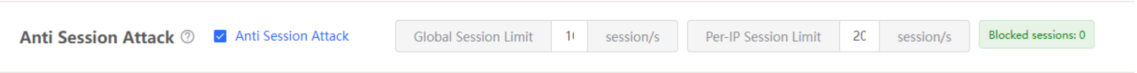
  You are advised to set the value to be greater than the load capacity of the local device.
- Suspicious Packet Attack Prevention

  In a suspicious packet attack, an attacker sends tremendous error packets to the device. When the host or server handles the error packets, its system will crash.

2. Configuring Session Attack Prevention

Choose **Local Device** > **Security** > **Local Security** > **Attack Defense**.

(1) Enable **Anti Session Attack.**



Anti Session Attack ⓘ ☑ Anti Session Attack Global Session Limit 1(session/s Per-IP Session Limit 2C session/s Blocked sessions: 0

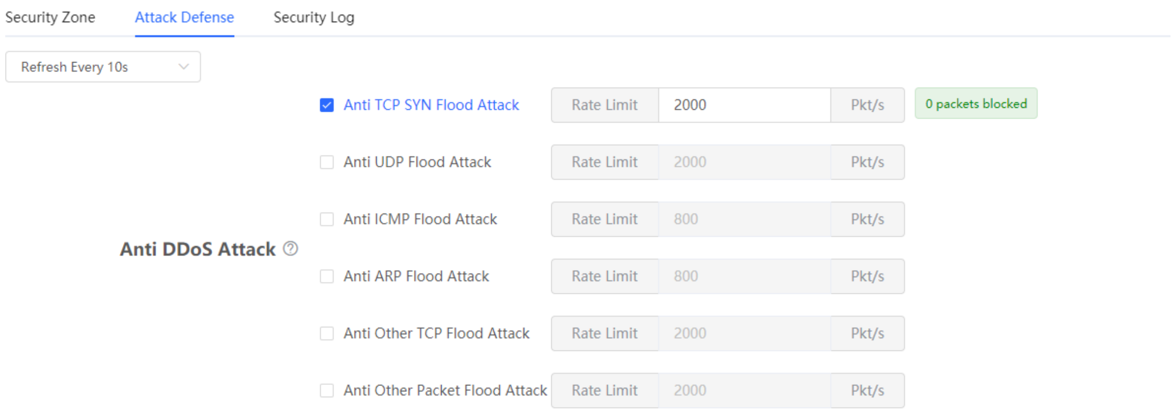
(2) Configure the session creation rate limit, including global and per-IP values.

(3) Click **Save**.

3. Configuring DDoS Attack Prevention

Choose **Local Device** > **Security** > **Local Security** > **Attack Defense**.

(1) Select required attack prevention types and enable this feature.



Security Zone | Attack Defense | Security Log

Refresh Every 10s

Anti DDoS Attack

☑ Anti TCP SYN Flood Attack — Rate Limit 2000 Pkt/s — 0 packets blocked

□ Anti UDP Flood Attack — Rate Limit 2000 Pkt/s

□ Anti ICMP Flood Attack — Rate Limit 800 Pkt/s

□ Anti ARP Flood Attack — Rate Limit 800 Pkt/s

□ Anti Other TCP Flood Attack — Rate Limit 2000 Pkt/s

□ Anti Other Packet Flood Attack — Rate Limit 2000 Pkt/s

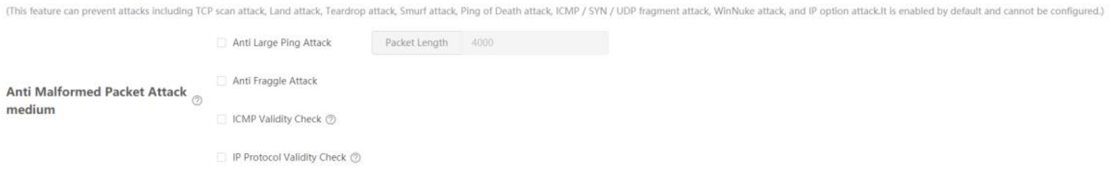
(2) Configure rate limiting.

(3) Click **Save**.

4. Configuring Suspicious Packet Attack Prevention

Choose **Local Device** > **Security** > **Local Security** > **Attack Defense**.

(1) Select required attack prevention types and validity check types to enable this feature.



(This feature can prevent attacks including TCP scan attack, Land attack, Teardrop attack, Smurf attack, Ping of Death attack, ICMP / SYN / UDP fragment attack, WinNuke attack, and IP option attack.It is enabled by default and cannot be configured.)

Anti Malformed Packet Attack medium

□ Anti Large Ping Attack — Packet Length 4000

□ Anti Fraggle Attack

□ ICMP Validity Check

□ IP Protocol Validity Check

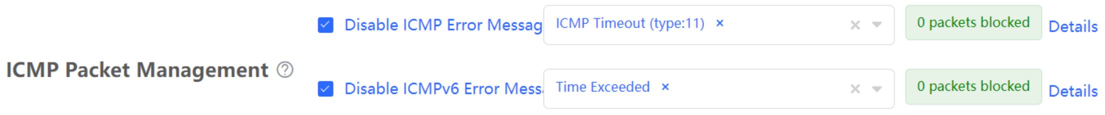
(2) To enable large ping attack prevention, enter the packet length.

(3) Click **Save**.

5. Configuring Packet Receiving and Sending Control

Choose **Local Device** > **Security** > **Local Security** > **Attack Defense**.

(1) Select the packet types that are prohibited from being sent by the device. Select at least one packet type.

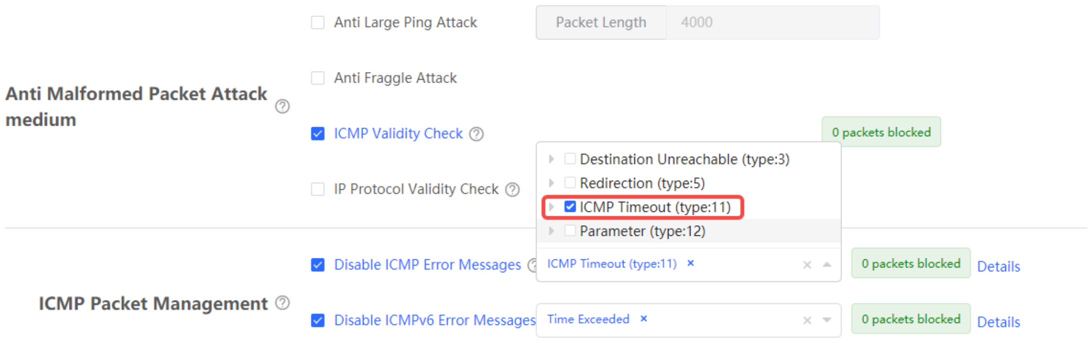


ICMP Packet Management

☑ Disable ICMP Error Messag — ICMP Timeout (type:11) × — 0 packets blocked — Details

☑ Disable ICMPv6 Error Mess — Time Exceeded × — 0 packets blocked — Details

- Enable **Disable ICMP Error Messages**. You can select **ICMP Timeout**, **Destination Unreachable**, **Redirection**, and **Parameter**.



Anti Malformed Packet Attack medium

□ Anti Large Ping Attack — Packet Length: 4000

□ Anti Fraggle Attack

☑ ICMP Validity Check — 0 packets blocked

□ IP Protocol Validity Check

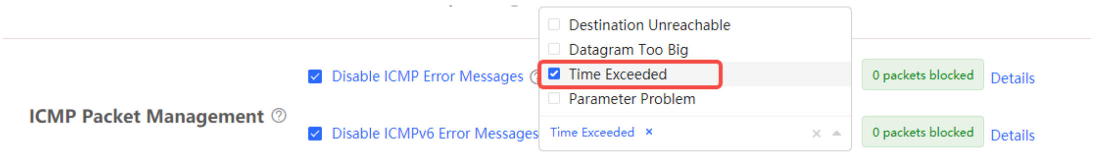
- □ Destination Unreachable (type:3)
- □ Redirection (type:5)
- ☑ ICMP Timeout (type:11)
- □ Parameter (type:12)

ICMP Packet Management

☑ Disable ICMP Error Messages — ICMP Timeout (type:11) — 0 packets blocked — Details

☑ Disable ICMPv6 Error Messages — Time Exceeded — 0 packets blocked — Details

- Enable **Disable ICMPv6 Error Message**. You can select **Destination Unreachable**, **Datagram too Big**, **Time Exceeded**, and **Parameter Problem**.



ICMP Packet Management

- □ Destination Unreachable
- □ Datagram Too Big
- ☑ Time Exceeded
- □ Parameter Problem

☑ Disable ICMP Error Messages — 0 packets blocked — Details

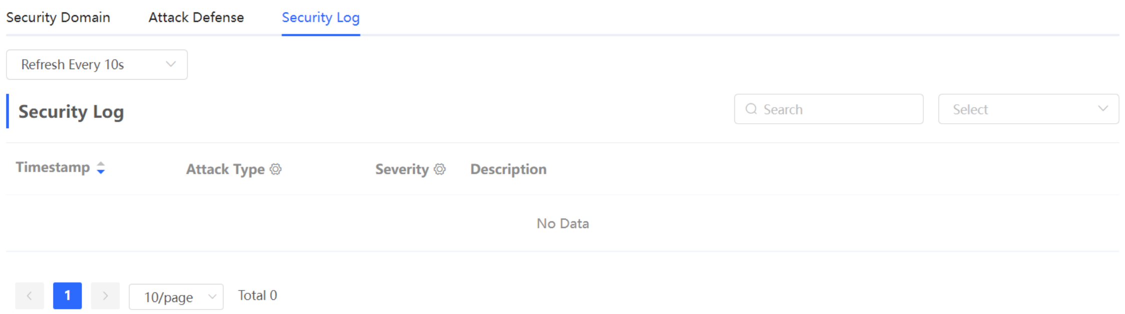
☑ Disable ICMPv6 Error Messages — Time Exceeded — 0 packets blocked — Details

(2) Click **Save**.

4.17.4 Checking the Security Log

Choose **Local Device** > **Security** > **Local Security** >**Security Log**.

Check defense results of the device against various attacks on the **Security Log** page.



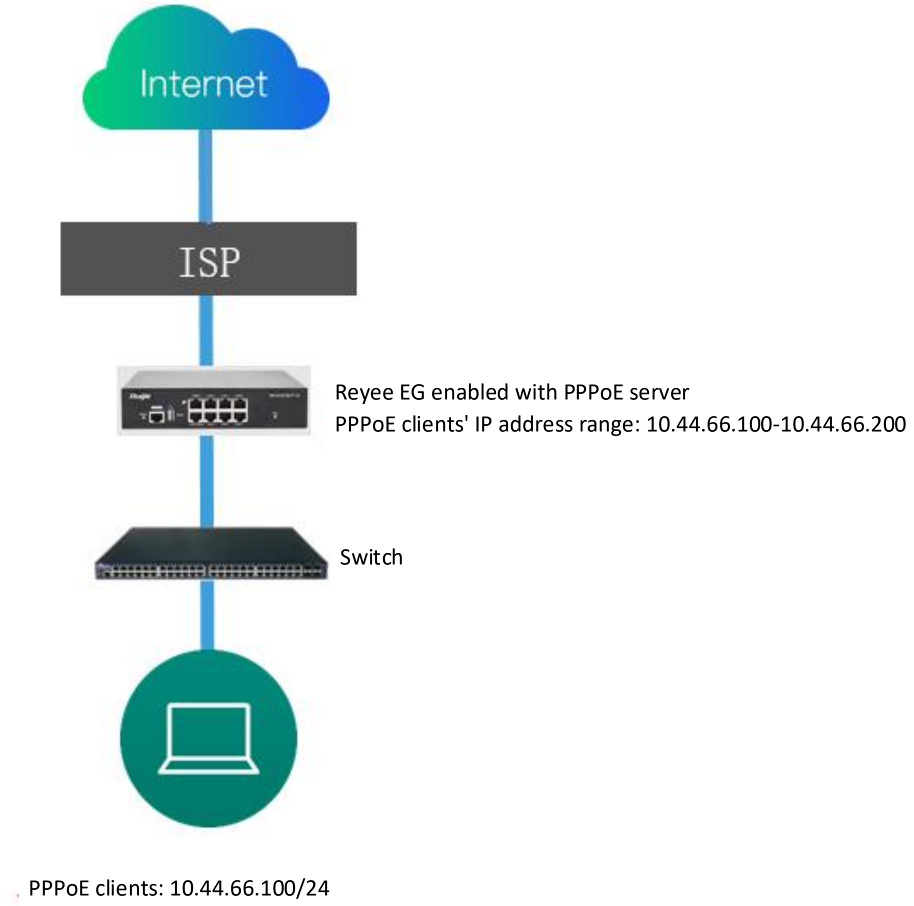
Security Log

Timestamp	Attack Type	Severity	Description
No Data			

4.18 Configuring the PPPoE Server

4.18.1 Application Scenario

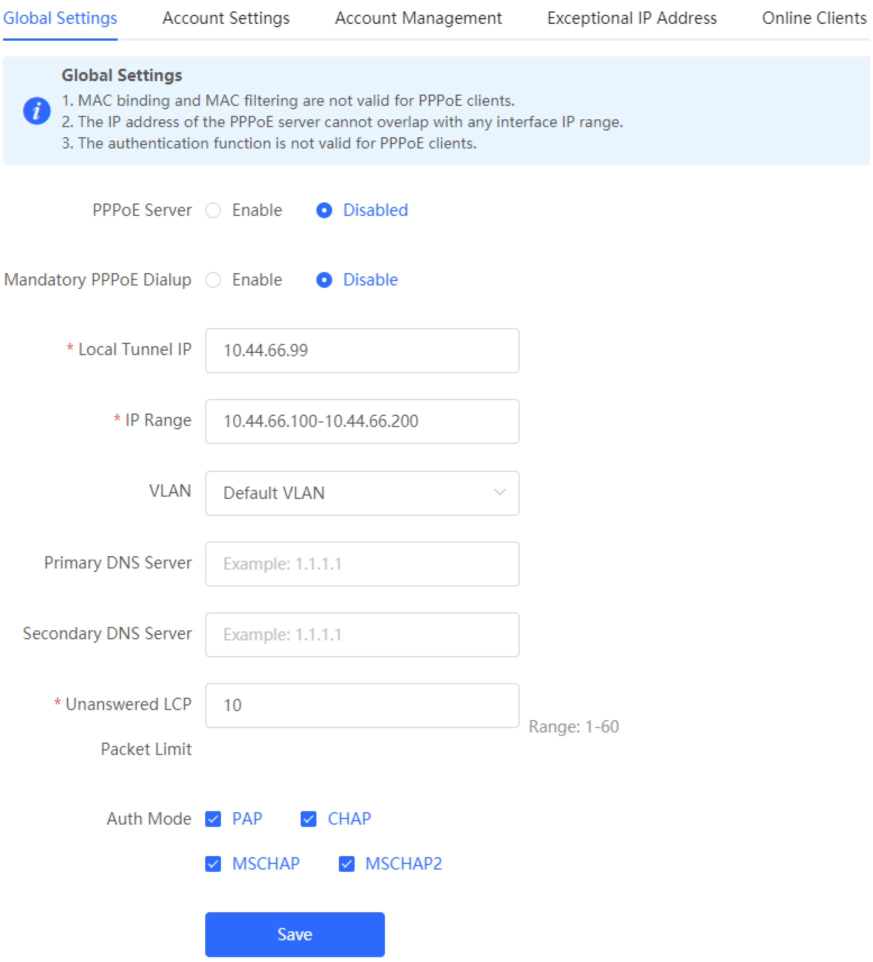
Point-to-Point Protocol over Ethernet (PPPoE) is a network tunneling protocol that encapsulates PPP frames into Ethernet frames. When the router functions as a PPPoE server, it provides the access service to LAN users and supports bandwidth management.


Internet
ISP
Reyee EG enabled with PPPoE server
PPPoE clients' IP address range: 10.44.66.100-10.44.66.200
Switch
PPPoE clients: 10.44.66.100/24

4.18.2 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

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: 10.44.66.99

* IP Range: 10.44.66.100-10.44.66.200

VLAN: Default VLAN

Primary DNS Server: Example: 1.1.1.1

Secondary DNS Server: Example: 1.1.1.1

* Unanswered LCP Packet Limit: 10 Range: 1-60

Auth Mode ☑ PAP ☑ CHAP ☑ MSCHAP ☑ MSCHAP2

Table 4-34 PPPoE Server Configuration

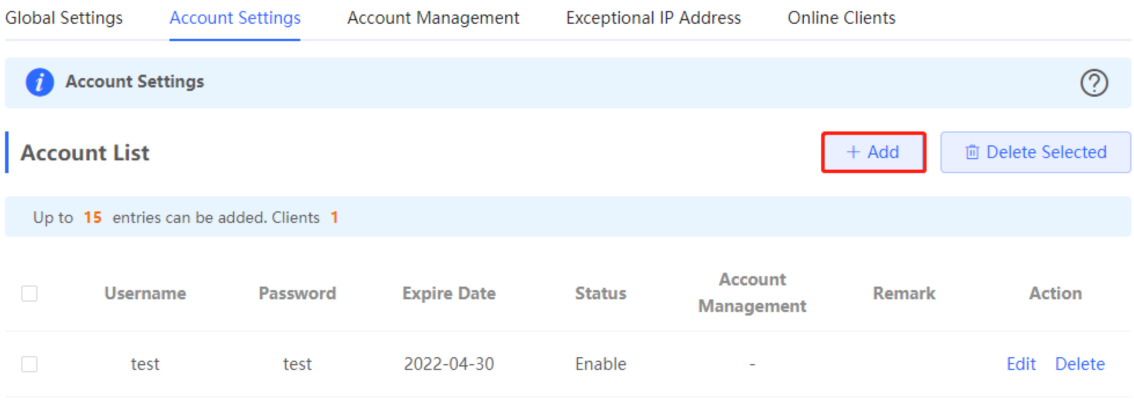
Parameter	Description
PPPoE Server	Specify whether to enable the PPPoE server function.
Mandatory PPPoE Dialup	Specify whether LAN users must access the Internet through dialing.
Local Tunnel IP	Set the P2P address of the PPPoE server.
IP Range	Specify the IP address range that can be allocated by the 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.

4.18.3 Configuring a PPPoE User Account

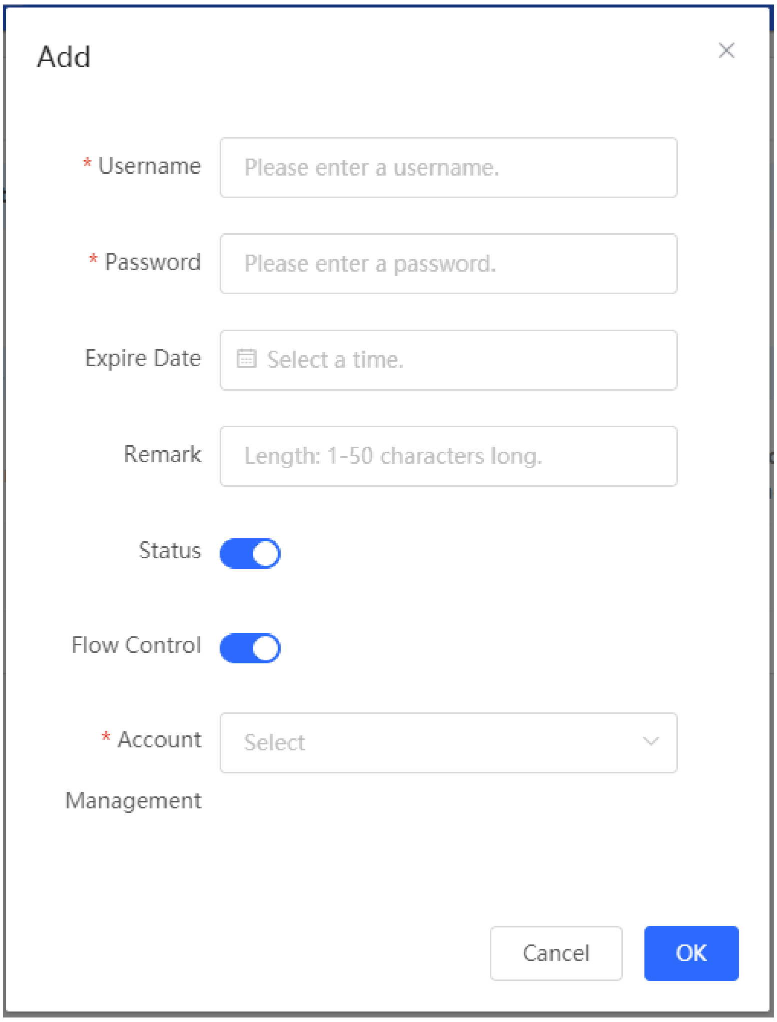
Switch to the **Local** mode. Choose **Advanced** > **PPPoE Server** > **Account Settings**.

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.



Up to 15 entries can be added. Clients 1

□	Username	Password	Expire Date	Status	Account Management	Remark	Action
□	test	test	2022-04-30	Enable	-		Edit Delete



Add

* Username: Please enter a username.

* Password: Please enter a password.

Expire Date: Select a time.

Remark: Length: 1-50 characters long.

Status: ●

Flow Control: ●

* Account Management: Select

Table 4-35 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.

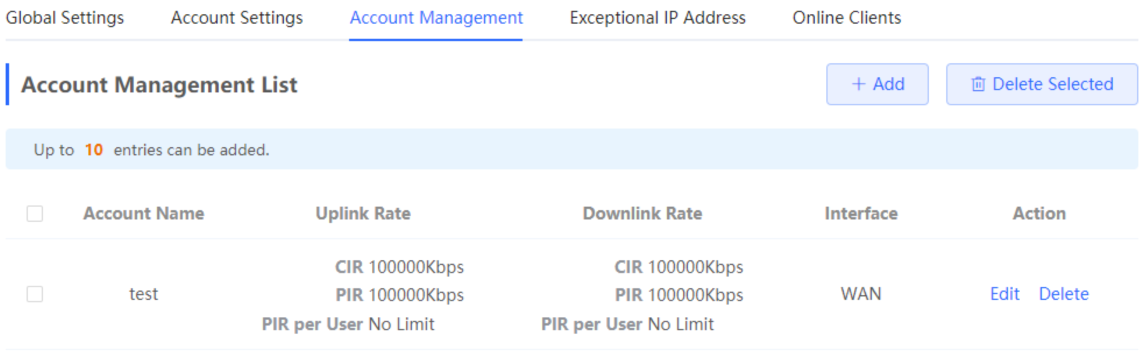
Parameter	Description
Flow Control	Specify whether to apply flow control on the account. If flow control is enabled, you need to configure flow control policies for PPPoE authentication users. If smart flow control is disabled, **Flow Control** must be disabled. To enable **Flow Control**, enable smart flow control first. For details on how to configure smart flow control, see section 4.15.2 Smart Flow Control.
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 4.18.4 Configuring a Flow Control Package.

4.18.4 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 4.15.2 Smart Flow Control.

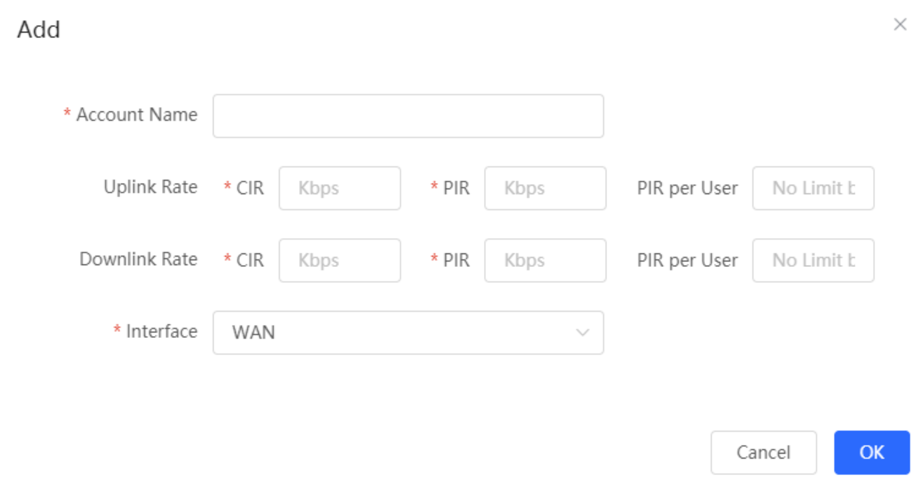
Click **Add** to create a flow control package. Created flow control packages are displayed in the **Account Management List**. You can modify or delete the packages.



Account Management List

Up to 10 entries can be added.

□	Account Name	Uplink Rate	Downlink Rate	Interface	Action
□	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 b

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

* Interface WAN

Table 4-36 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.

4.18.5 Configuring Exceptional IP Addresses

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

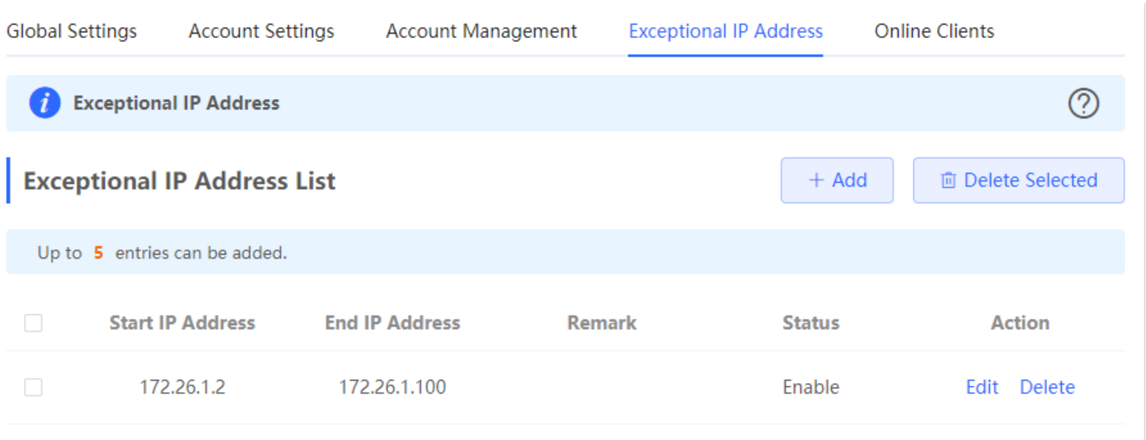
To configure clients with some IP addresses in a specific VLAN to access the Internet without passing account and password authentication, you can configure these IP addresses as exceptional IP addresses on the device enabled with the PPPoE server.

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.

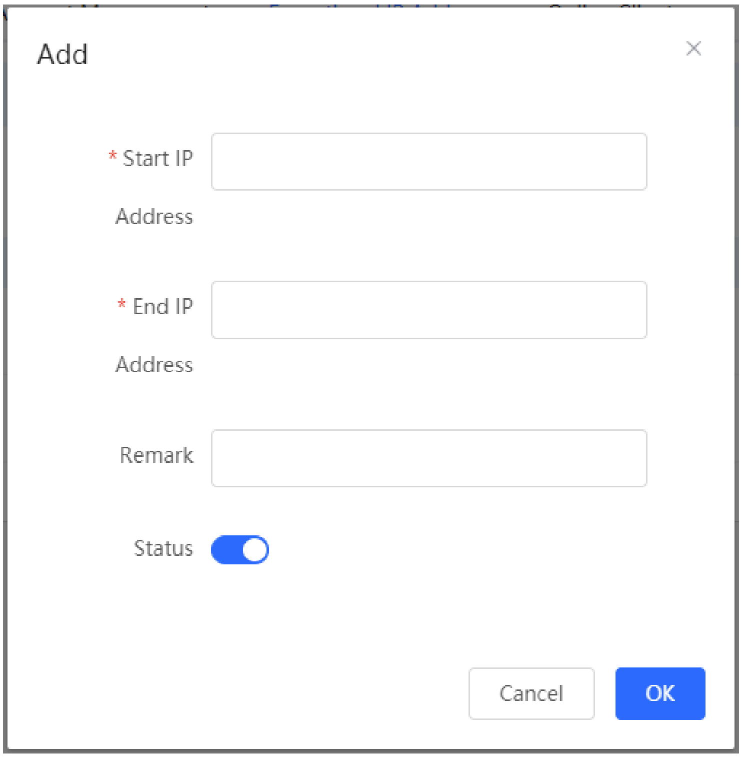
Remark: indicates the description of an exceptional IP address.

Status: indicates whether an exceptional IP address is valid.



Up to 5 entries can be added.

□	Start IP Address	End IP Address	Remark	Status	Action
□	172.26.1.2	172.26.1.100		Enable	Edit Delete



* Start IP Address

* End IP Address

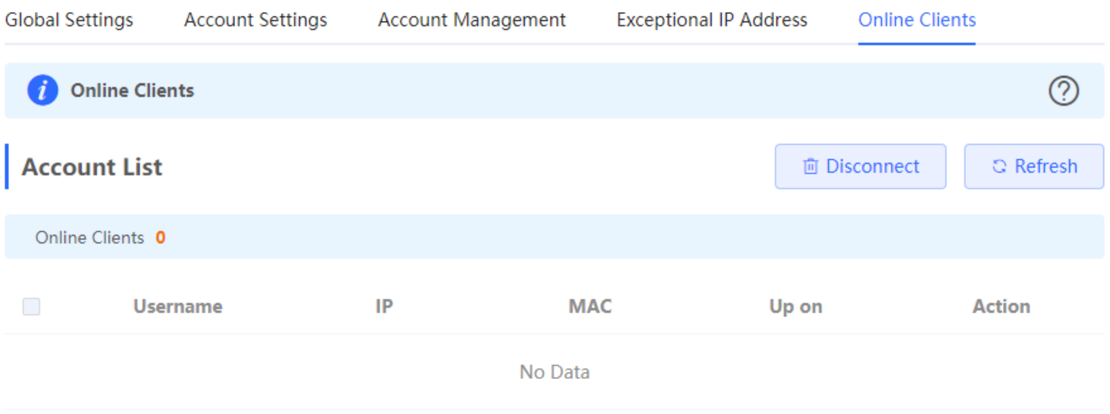
Remark

Status

4.18.6 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.



Online Clients 0

□	Username	IP	MAC	Up on	Action
			No Data		

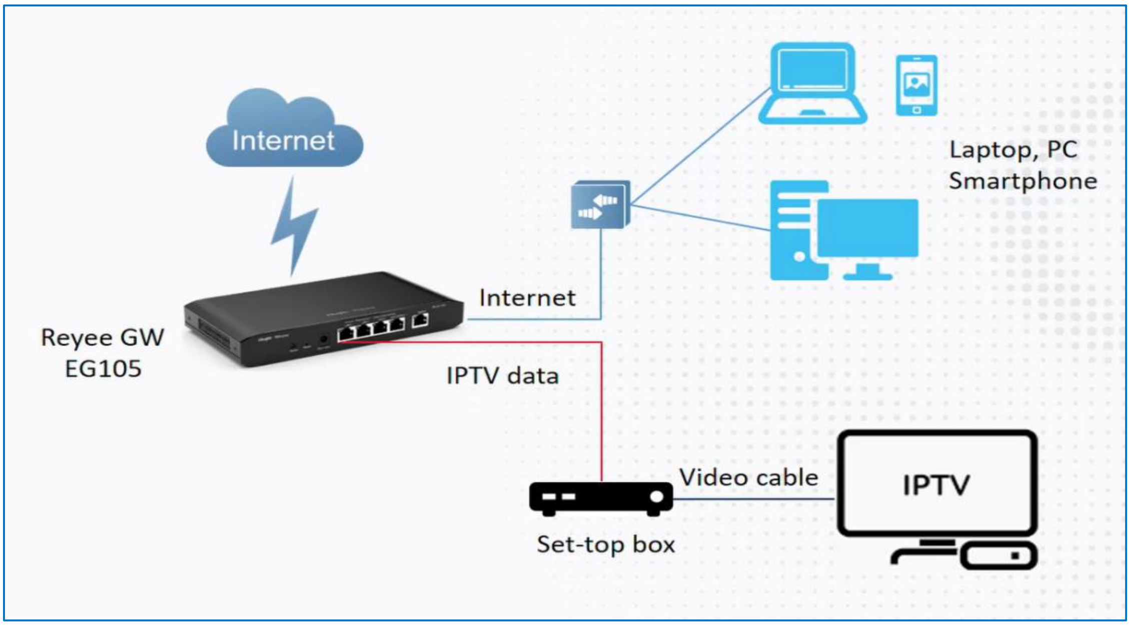
Table 4-37 PPPoE Online User Information

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.

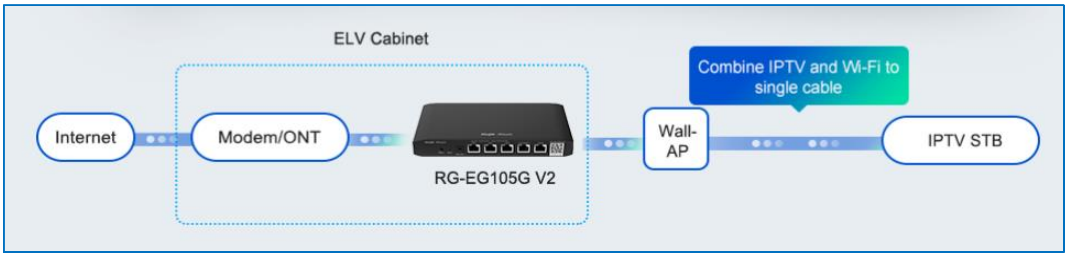
4.19 IPTV

4.19.1 Application Scenario

- **Scenario 1: Dual-WAN Scenario**



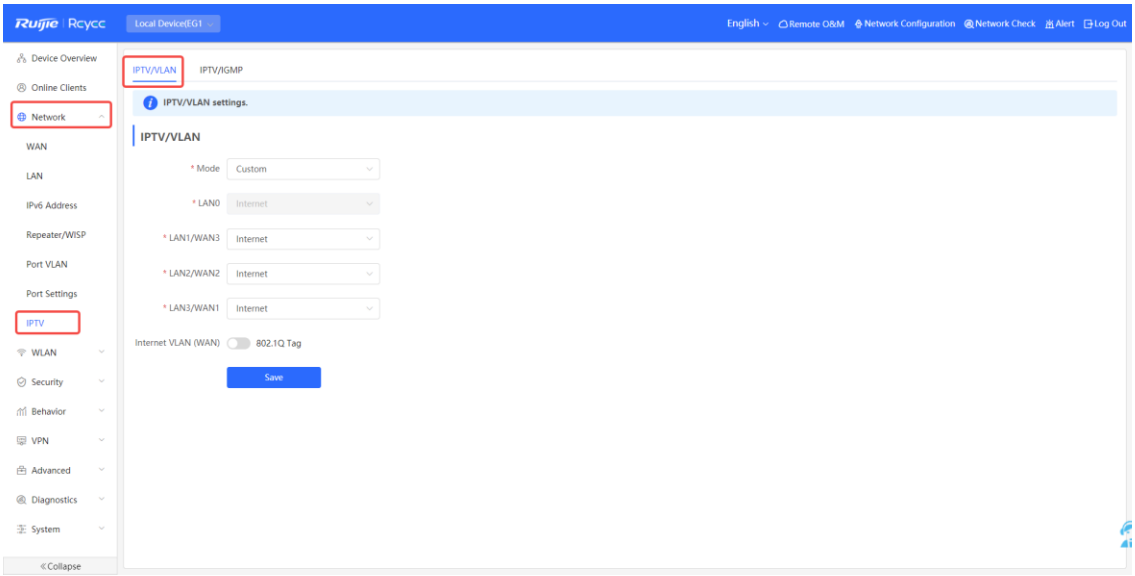
- **Scenario 2: Single-WAN Scenario**



4.19.2 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 Reyee 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**.



IPTV/VLAN settings.

IPTV/VLAN

* Mode: Custom

* LAN0: Internet

* LAN1/WAN3: Internet

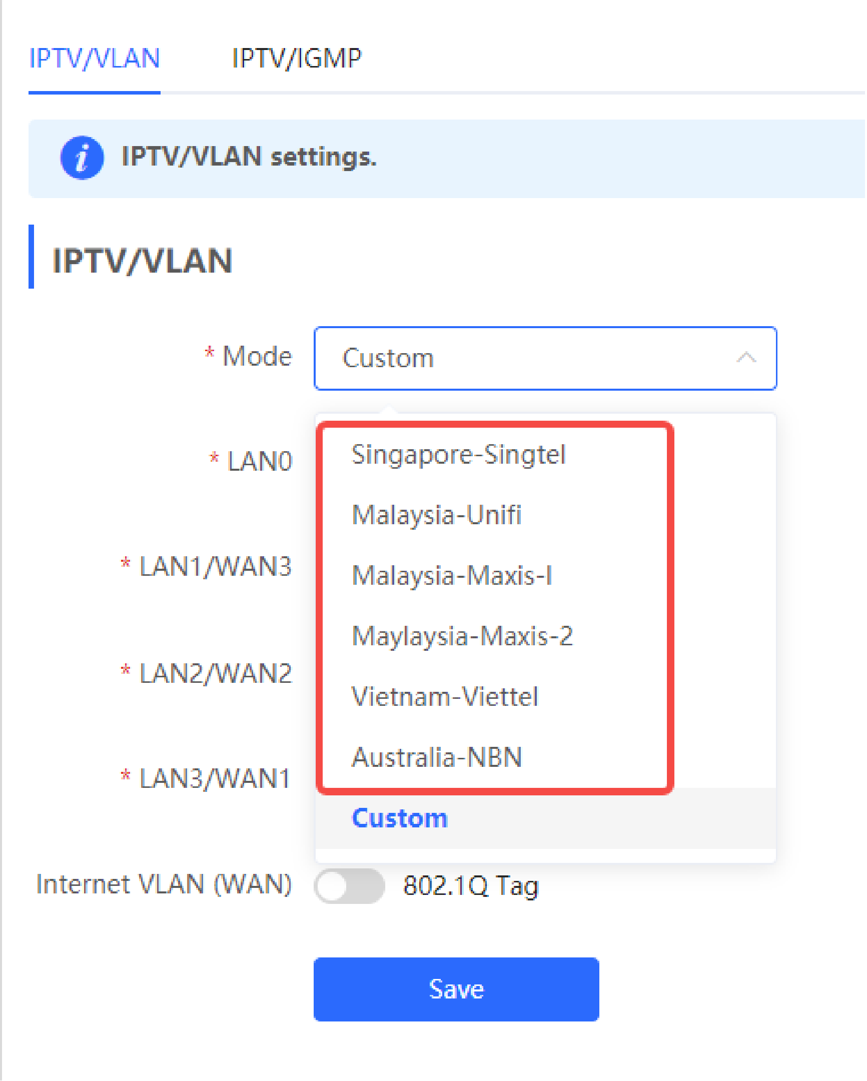
* LAN2/WAN2: Internet

* LAN3/WAN1: Internet

Internet VLAN (WAN): 802.1Q Tag

(3) Configure **IPTV VLAN ID** or **IP-Phone VLAN ID**.

- If you are in following regions listed in the red box, you can choose the mode directly.



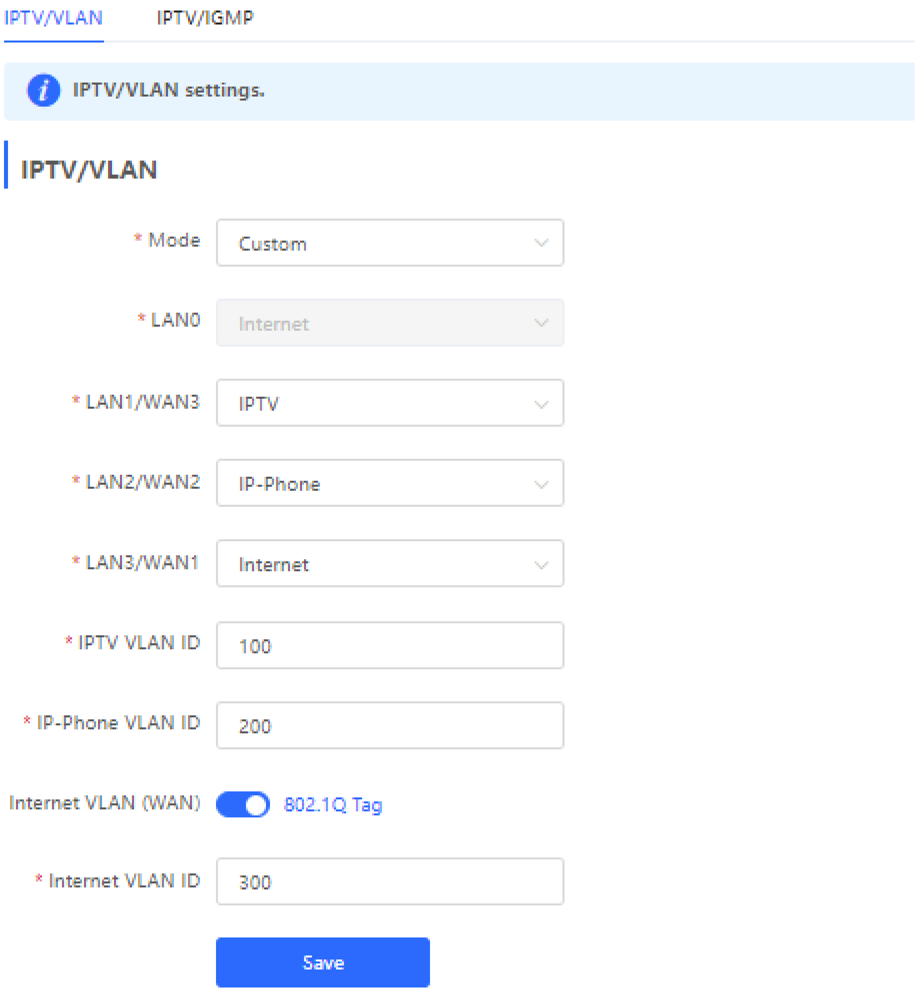
IPTV/VLAN IPTV/IGMP

IPTV/VLAN settings.

IPTV/VLAN

* Mode: Custom

- 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 settings.

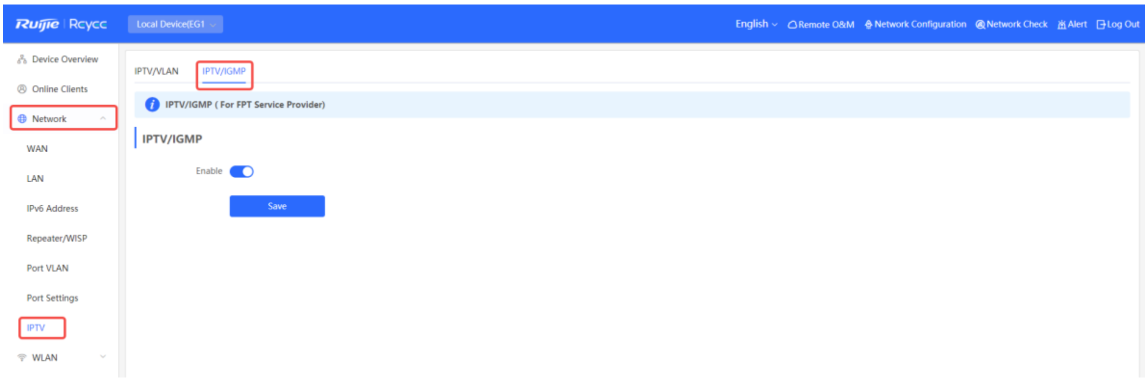
IPTV/VLAN

* Mode: Custom
* LAN0: Internet
* LAN1/WAN3: IPTV
* LAN2/WAN2: IP-Phone
* LAN3/WAN1: Internet
* IPTV VLAN ID: 100
* IP-Phone VLAN ID: 200
Internet VLAN (WAN): 802.1Q Tag
* Internet VLAN ID: 300

4.19.3 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**.

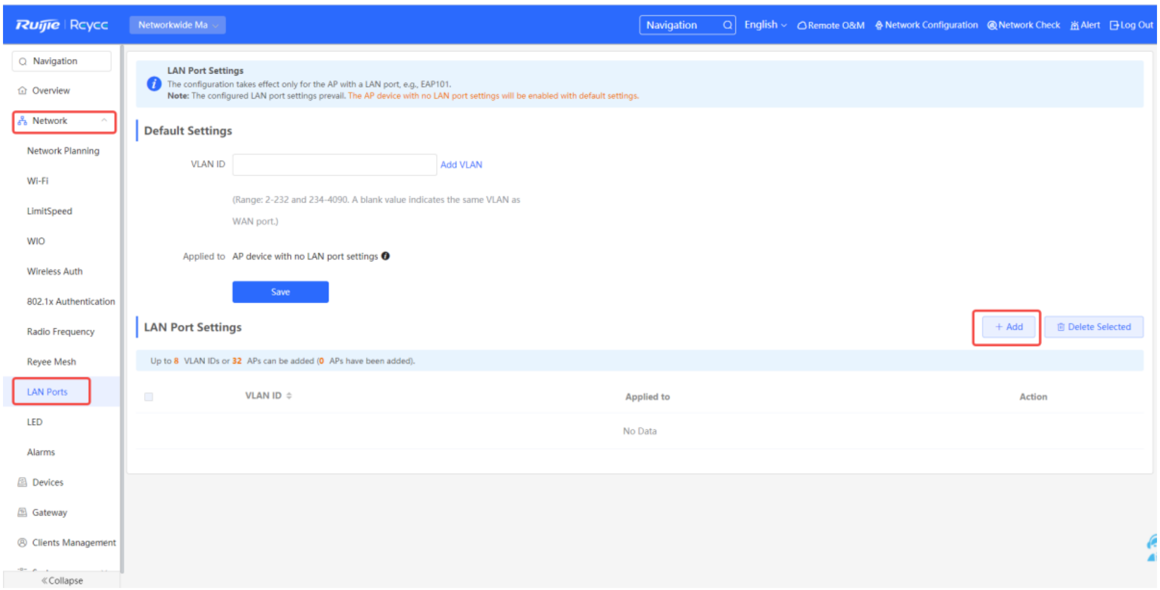


IPTV/IGMP (For FPT Service Provider)

IPTV/IGMP

Enable: on

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



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

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

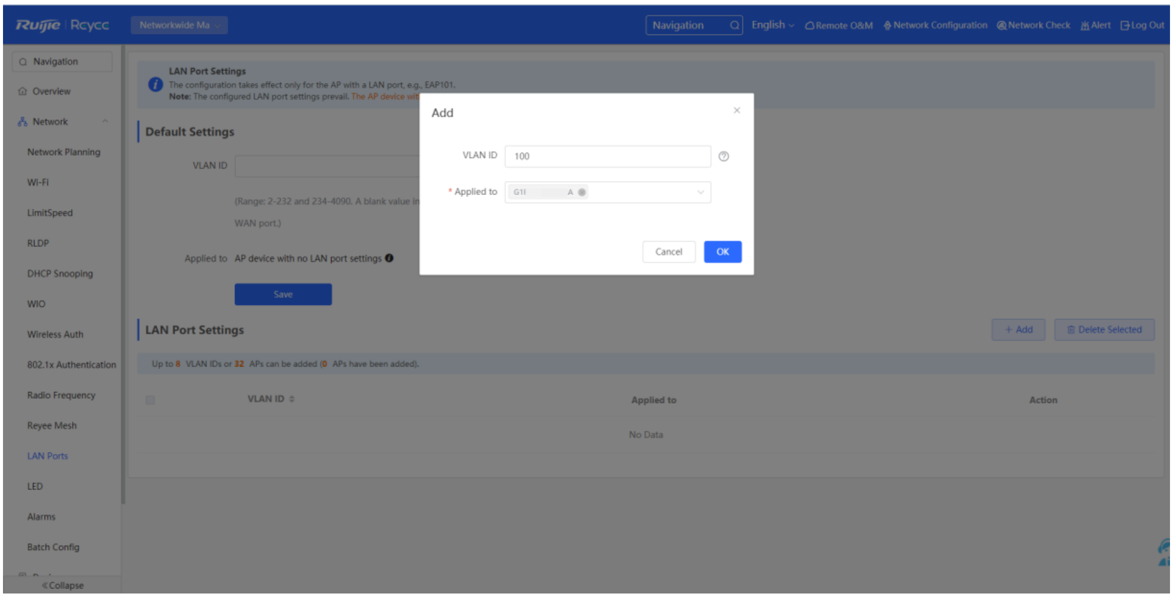
Applied to AP device with no LAN port settings

LAN Port Settings

Up to 8 VLAN IDs or 32 APs can be added (0 APs have been added).

No Data

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



Add

VLAN ID 100

* Applied to G11 A

Caution

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

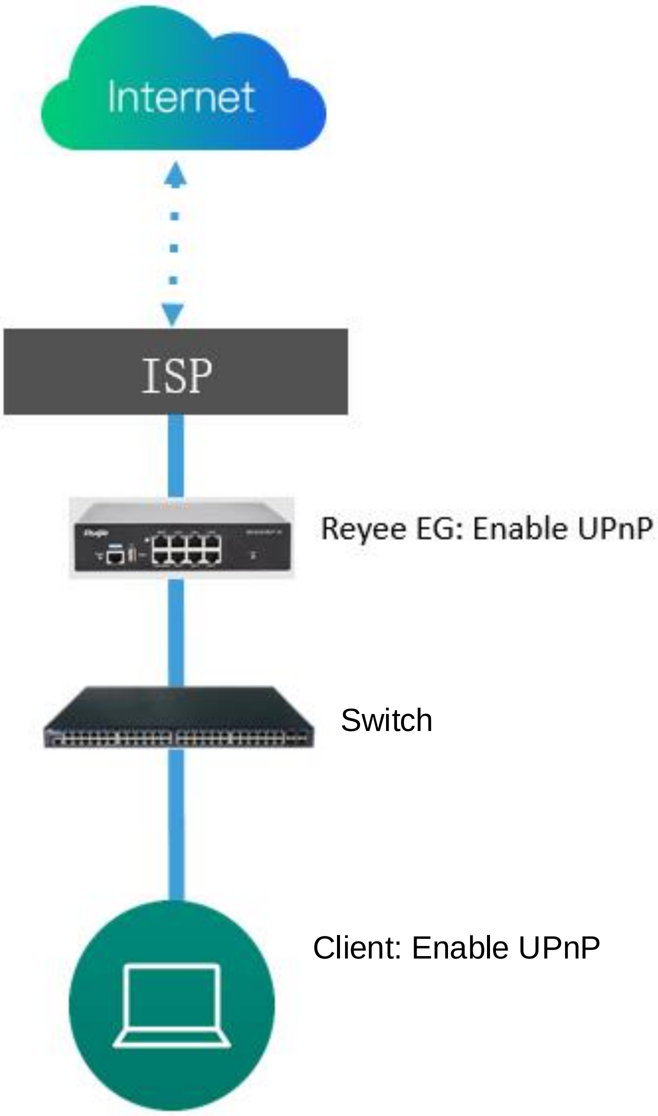
4.20 UPnP

4.20.1 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:

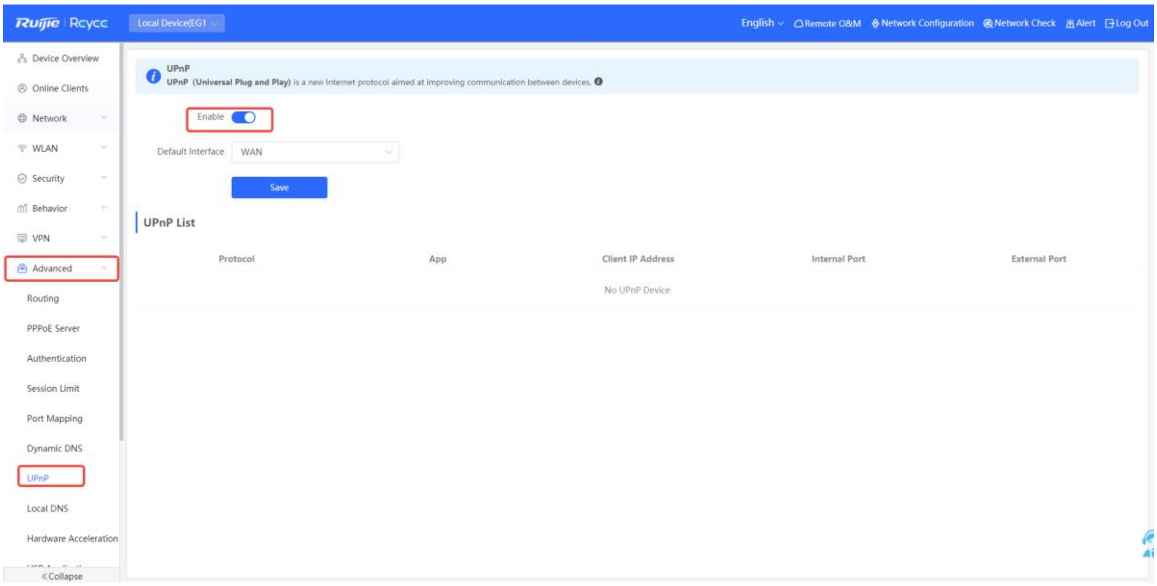
- The device must be enabled with UPnP.
- The operating system of internal hosts must support UPnP.
- Applications must support UPnP.



4.20.2 Procedure

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



UPnP

UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving communication between devices.

Enable

Default Interface WAN

Save

UPnP List

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

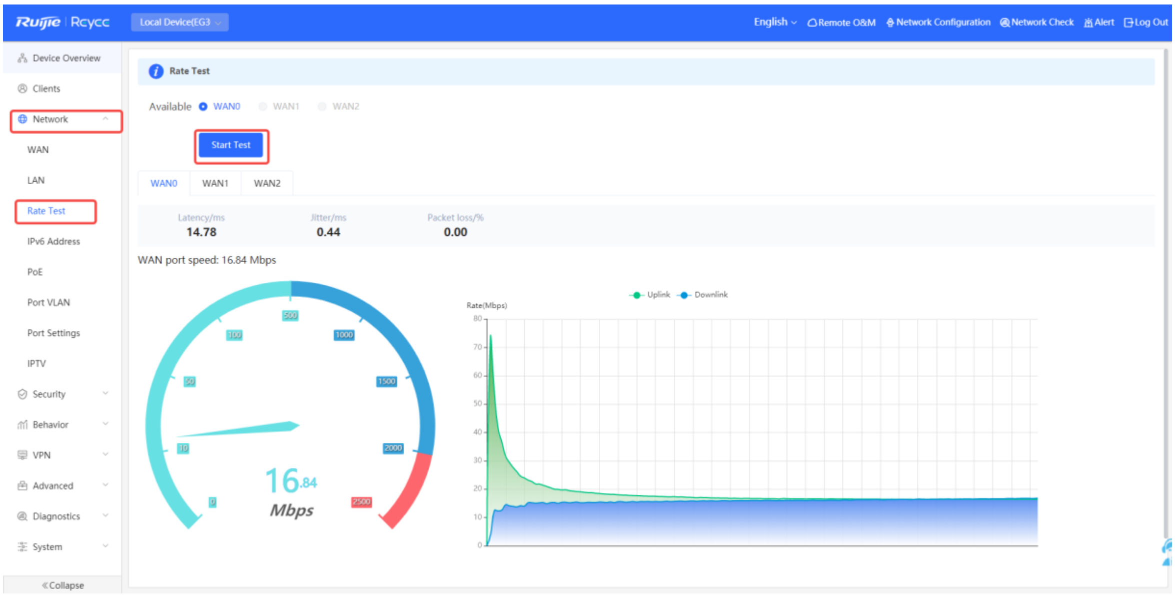
4.21 Configuring Rate Test

Note

Only EG3XX series devices (such as EG310G-E) support this function.

You can use the rate test function to easily monitor the transmission rate of individual ports. In the case of ports with low transmission rates, you can identify and address potential issues to ensure that service quality remains high.

Choose **Local Device** > **Network** > **Rate Test**.



Rate Test

Available ● WAN0 ○ WAN1 ○ WAN2

Start Test

Latency/ms	Jitter/ms	Packet loss/%
14.78	0.44	0.00

WAN port speed: 16.84 Mbps

(1) Select the WAN port to be tested. You can click **Select All** to select all WAN ports for the rate test.

(2) Click **Start Test**.

After the rate test is complete, the system will display the test results, including latency, jitter, and packet loss.

4.22 Configuring IPv6

4.22.1 IPv6 Overview

Internet Protocol Version 6 (IPv6) is the next-generation IP protocol designed by Internet Engineering Task Force (IETF) to substitute IPv4. It is used to compensate insufficient IPv4 network addresses.

4.22.2 IPv6 Basics

1. IPv6 Address Format

IPv6 extends 32-bit IPv4 address into 128 bits, providing wider address space than IPv4.

The basic format of an IPv6 address is X:X:X:X:X:X:X:X. It is represented as eight groups of four hexadecimal digits (0-9, A-F), each group representing16 bits. The groups are separated by colons (:). In this format, each X represents a group of four hexadecimal digits.

Samples of IPv6 addresses are 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:0:1, and 1080:0:0:0:8:800:200C:417A.

The digit 0 in an IPv6 address can be suppressed as follows:

- Leading zeros in each 16-bit field are suppressed. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be suppressed to 2001:CD:34:78:A:B:1200:2100.
- The long sequence of consecutive all-zero fields in some IPv6 addresses can be replaced with two colons (::). For example, 800:0:0:0:0:0:0:1 can be represented as 800::1. The two colons (::) can be used only when all the 16 bits in a group are 0s, and it can appear only once in an IPv6 address.

2. IPv6 Prefix

IPv6 addresses are typically composed of two logical parts:

- Network prefix: *n* bits, corresponding to the network ID in IPv4 addresses
- interface ID: (128 – *n*) bits, corresponding to the host ID in IPv4 addresses

A slash (/) is used to separate the length of network prefix from an IPv6 address. For example, 12AB::CD30:0:0:0:0/60 indicates that the 60-bit network prefix in the address is used for route selection. IPv6 prefixes can be obtained from the IPv6 DHCP server, along with IPv6 addresses. A downlink DHCP server can also automatically obtain IPv6 prefixes from its uplink DHCP server.

3. Special IPv6 Addresses

There are some special IPv6 addresses:

fe80::/8: loopback address, similar to the IPv4 address 169.254.0.0/16

fc00::/7: local address, similar to IPv4 addresses 10.0.0.0/8, 172.16.0.0/16, and 192.168.0.0/16

ff00::/12: multicast address, similar to the IPv4 address 224.0.0.0/8

4. NAT66

IPv6-to-IPv6 Network Address Translation (NAT66) is a process of converting the IPv6 address in the IPv6 data packet header into another IPv6 address. NAT66 can be implemented by converting the prefix in an IPv6 address in an IPv6 data packet header into another IPv6 address prefix. NAT66 enables mutual access between an internal network and an external public network.

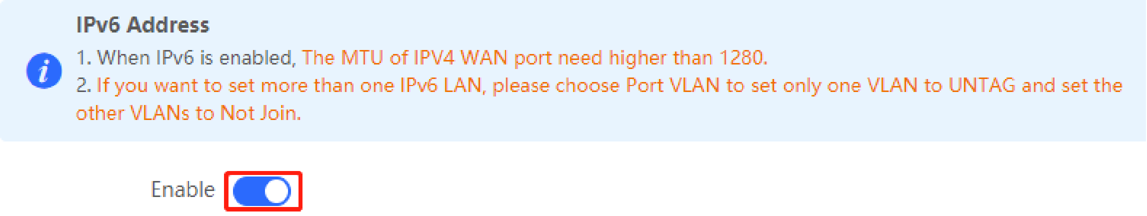
4.22.3 IPv6 Address Allocation Modes

- Manual configuration: IPv6 addresses, prefixes, and other network parameters are configured manually.
- Stateless Address Autoconfiguration (SLAAC): The link-local address is generated based on the interface ID, and the IPv6 address is automatically allocated based on the prefix information in the Router Advertisement (RA) packet.
- Stateful address allocation (DHCPv6): Two DHCPv6 allocation methods are as follows:
  - Automatic DHCPv6 allocation: The DHCPv6 server automatically allocates IPv6 addresses, prefixes, and other network parameters.
  - Automatic allocation of DHCPv6 Prefix Delegations (PDs): The lower-layer network device submits a prefix allocation application to the upper-layer network device. The upper-layer network device allocates an appropriate address prefix to the lower-layer device. The lower-layer device further divides the obtained prefix (usually less than 64 bits) into 64-bit prefixed subnet segments and advertises the address prefixes to the user link directly connected to the IPv6 host through the RA packet, implementing automatic address configuration for hosts.

4.22.4 Enabling the IPv6 Function

Choose **Local Device** > **Network** > **IPv6 Address**.

Turn on **Enable** to enable the IPv6 function.



IPv6 Address

1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.

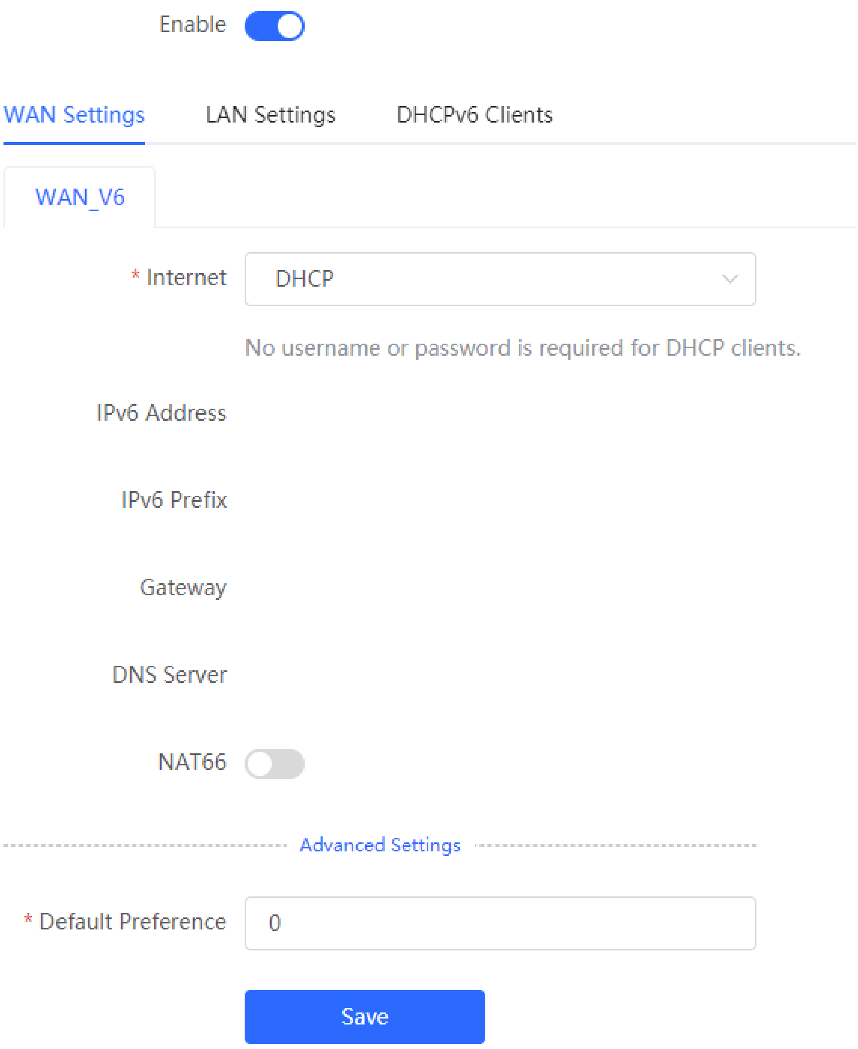
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to UNTAG and set the other VLANs to Not Join.

Enable

4.22.5 Configuring an IPv6 Address for the WAN Port

Choose **Local Device** > **Network** > **IPv6 Address** > **WAN Settings**.

After you enable the IPv6 function, you can set related parameters on the **WAN Settings** tab. The number of **WAN_V6** tabs indicates the number of WAN ports on the current device.



Enable

* Internet: DHCP

No username or password is required for DHCP clients.

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

NAT66

* Default Preference: 0

Table 4-38 IPv6 address configuration for WAN port

Parameter	Description
Internet	Configure a method for the WAN port to obtain an IPv6 address. ● **DHCP**: The current device functions as the DHCPv6 client, and it applies for an IPv6 address and prefix from the uplink network device. ● **Static IP**: You need to manually configure a static IPv6 address, gateway address, and DNS server. ● **Null**: The IPv6 function is disabled on the WAN port.
IPv6 Address	When **Internet** is set to **DHCP**, the automatically obtained IPv6 address is displayed. When **Internet** is set to **Static IP**, you need to configure this parameter manually.
IPv6 Prefix	When **Internet** is set to **DHCP,** the IPv6 address prefix automatically obtained by the current device is displayed.

Parameter	Description
Gateway	When **Internet** is set to **DHCP**, the automatically obtained gateway address is displayed. When **Internet** is set to **Static IP**, you need to configure this parameter manually.
DNS Server	When **Internet** is set to **DHCP**, the automatically obtained DNS server address is displayed. When **Internet** is set to **Static IP**, you need to configure this parameter manually.
NAT66	If the current device cannot access the Internet through DHCP or cannot obtain the IPv6 prefix, you need to enable the NAT66 function to allocate IPv6 addresses to clients on the internal network.
Default Preference	Set the default route preference for the current line. A smaller value indicates a higher preference. For the same destination address, the route with the highest preference is selected as the optimal route.

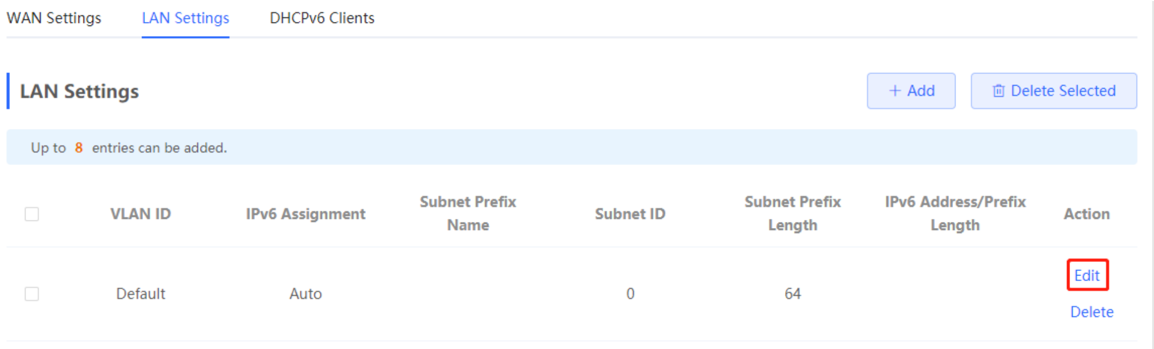
⚠ **Caution**

The RG-EG105G and RG-EG105G-P does not support the NAT66 function.

4.22.6 Configuring an IPv6 Address for the LAN Port

Choose **Local Device** > **Network** > **IPv6 Address** > **LAN Settings**.

When the device accesses the Internet through DHCP, it can obtain LAN port IPv6 addresses from the uplink device and allocate IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the uplink device cannot allocate an IPv6 address prefix to the device, you need to manually configure an IPv6 address prefix for the LAN port and enable the NAT66 function to allocate IPv6 addresses to the clients in the LAN. For details, see Section 4.22.5 Configuring an IPv6 Address for the WAN Port.



LAN Settings

Up to 8 entries can be added.

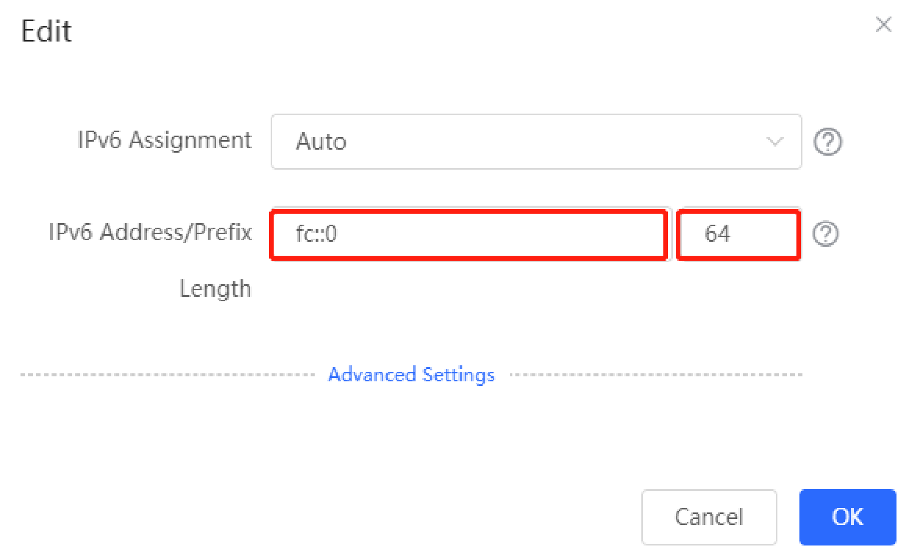
□	VLAN ID	IPv6 Assignment	Subnet Prefix Name	Subnet ID	Subnet Prefix Length	IPv6 Address/Prefix Length	Action
□	Default	Auto		0	64		Edit Delete

Click **Edit** next to the default VLAN, and set **IPv6 Address/Prefix Length** to a local address with no more than 64 bits. This address is also used as the IPv6 address prefix.

You can use either of the following methods to allocate IPv6 addresses to clients:

- **Auto**: Allocate IPv6 addresses to clients in DHCPv6 or SLAAC mode.
- **DHCPv6**: Allocate IPv6 addresses to clients through DHCPv6.
- **SLAAC**: Allocate IPv6 addresses to clients through SLAAC.
- **Null**: Do not allocate addresses to clients.

You should select an allocation method based on the protocol supported by clients on the internal network. If you are not sure about the supported protocol, select **Auto**.

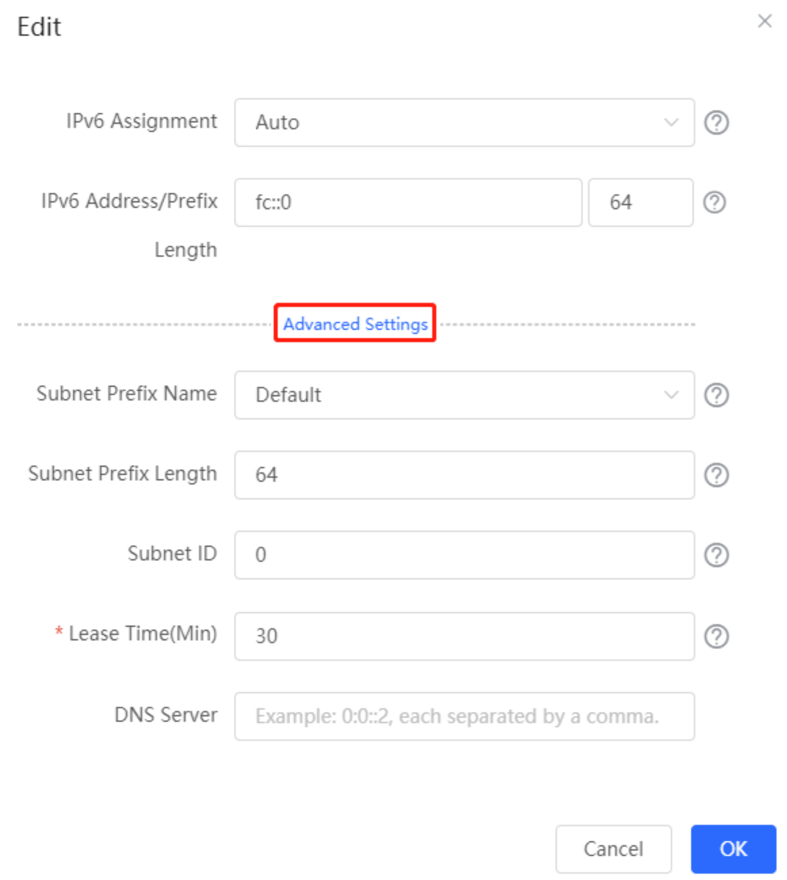


Edit

IPv6 Assignment: Auto

IPv6 Address/Prefix Length: fc::0 / 64

Click **Advanced Settings** to configure more address attributes.



Edit

IPv6 Assignment: Auto

IPv6 Address/Prefix Length: fc::0 / 64

Subnet Prefix Name: Default

Subnet Prefix Length: 64

Subnet ID: 0

* Lease Time(Min): 30

DNS Server: Example: 0:0::2, each separated by a comma.

Table 4-39 **IPv6 address configuration for LAN port**

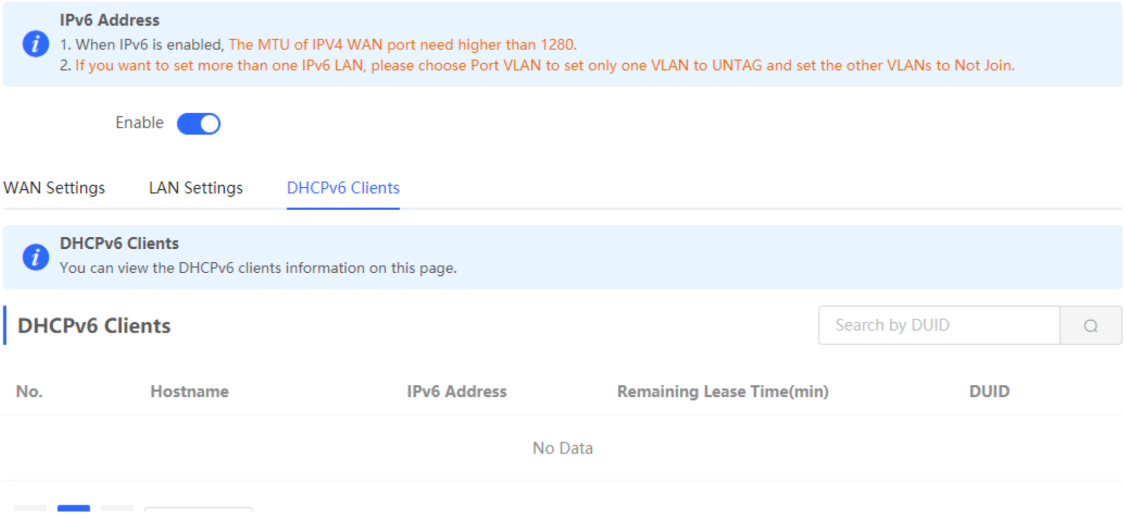
Parameter	Description
Subnet Prefix Name	Specify the interface from which the prefix is obtained, such as **WAN_V6** or **WAN1_V6**. By default, the device obtains prefixes from all interfaces.
Subnet Prefix Length	Specify the length of the subnet prefix. The value is in the range of 48 to 64.
Subnet ID	Configure the subnet ID in the hexadecimal format. The value 0 indicates auto increment.
Lease Time(Min)	Set the lease of the IPv6 address, in minutes.
DNS Server	Configure the IPv6 DNS server address.

4.22.7 Viewing the DHCPv6 Client

Choose **Local Device** > **Network** > **IPv6 Address** > **DHCPv6 Clients**.

When the device functions as a DHCPv6 server to allocate IPv6 addresses to clients, you can view the information about the client that obtains an IPv6 address from the device on the current page. The client information includes the host name, IPv6 address, remaining lease time, and DHCPv6 Unique Identifier (DUID).

Enter the DUID in the search bar and click 🔍 to quickly find relative information of the specified DHCPv6 client.



IPv6 Address
1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to UNTAG and set the other VLANs to Not Join.

Enable ●

DHCPv6 Clients
You can view the DHCPv6 clients information on this page.

DHCPv6 Clients

Search by DUID 🔍

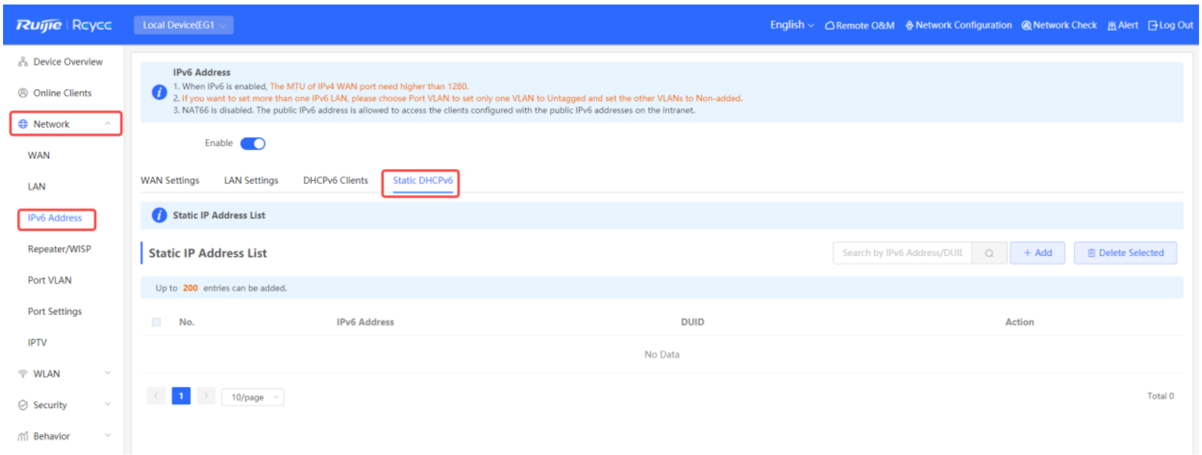
No.	Hostname	IPv6 Address	Remaining Lease Time(min)	DUID
No Data				

- Click **Convert to Static IP** to convert the IP binding of a client with an IP address to static binding. Then the DHCP server assigns a static IP address to the client.
- Click **Bind Selected** to convert the IP binding of multiple clients with IP addresses to static binding. Then the DHCP server assigns static IP addresses to the clients.

4.22.8 Configuring the Static DHCPv6 Address

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

Choose **Local Device** > **Network** > **IPv6 Address** > **Static DHCPv6**.



IPv6 Address
1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.
3. NAT66 is disabled. The public IPv6 address is allowed to access the clients configured with the public IPv6 addresses on the intranet.

Enable ●

Static IP Address List

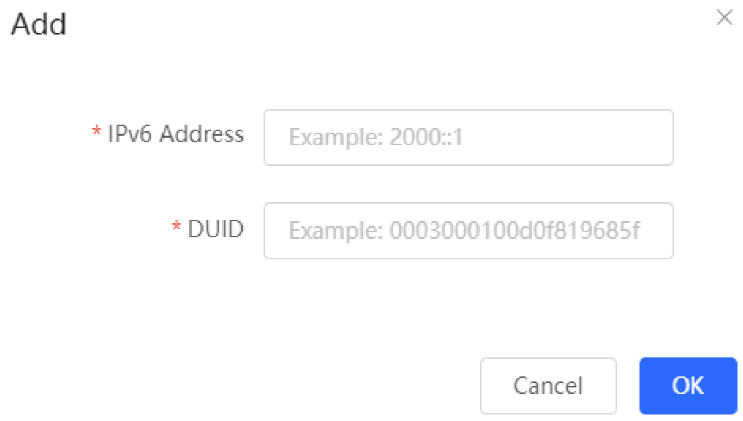
Static IP Address List

Up to 200 entries can be added.

No.	IPv6 Address	DUID	Action
No Data			

Total 0

(1) Click **Add**.



* IPv6 Address: Example: 2000::1

* DUID: Example: 0003000100d0f819685f

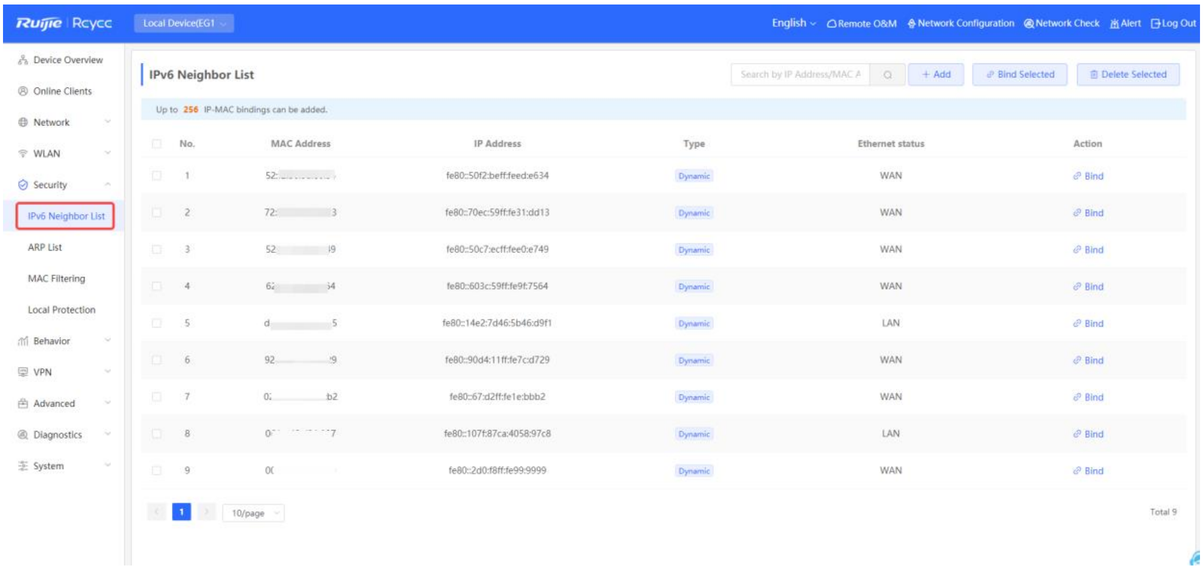
(2) Enter the IPv6 address and DUID.

(3) Click **OK**.

4.22.9 Configuring the IPv6 Neighbor List

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

Choose **Local Device** > **Security** > **IPv6 Neighbor List.**



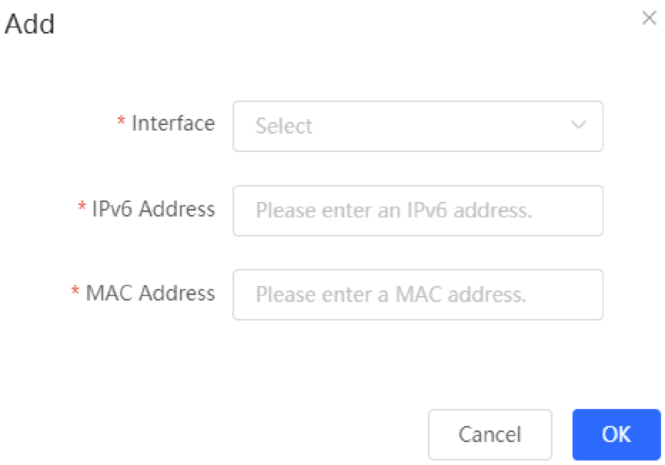
IPv6 Neighbor List

Up to 256 IP-MAC bindings can be added.

No.	MAC Address	IP Address	Type	Ethernet status	Action
1	52:[redacted]	fe80::50f2:beff:feed:e634	Dynamic	WAN	Bind
2	72:[redacted]3	fe80::70ec:59ff:fe31:dd13	Dynamic	WAN	Bind
3	52[redacted]9	fe80::50c7:ecff:fee0:e749	Dynamic	WAN	Bind
4	6[redacted]4	fe80::603c:59ff:fe9f:7564	Dynamic	WAN	Bind
5	d[redacted]5	fe80::14e2:7d46:5b46:d9f1	Dynamic	LAN	Bind
6	92[redacted]9	fe80::90d4:11ff:fe7c:d729	Dynamic	WAN	Bind
7	0[redacted]b2	fe80::67:d2ff:fe1e:bbb2	Dynamic	WAN	Bind
8	0[redacted]7	fe80::107f:87ca:4058:97c8	Dynamic	LAN	Bind
9	0[redacted]	fe80::2d0:f8ff:fe99:9999	Dynamic	WAN	Bind

Total 9

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



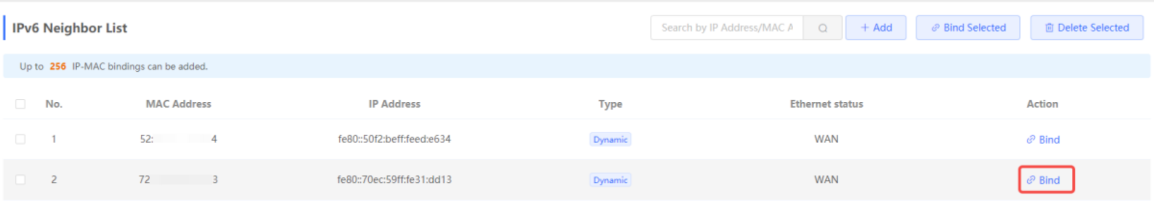
Add

* Interface: Select

* IPv6 Address: Please enter an IPv6 address.

* MAC Address: Please enter a MAC address.

(2) Select the MAC address and IP address to be bound, and click **Bind** in the **Action** column to bind the IP address to the MAC address to prevent ND attacks.



IPv6 Neighbor List

Up to 256 IP-MAC bindings can be added.

No.	MAC Address	IP Address	Type	Ethernet status	Action
1	52:[redacted]4	fe80::50f2:beff:feed:e634	Dynamic	WAN	Bind
2	72[redacted]3	fe80::70ec:59ff:fe31:dd13	Dynamic	WAN	Bind

5 VPN

5.1 Configuring IPsec VPN

5.1.1 Overview

1. IPsec Overview

IP Security (IPsec) is a Layer 3 tunnel encryption protocol defined by the IETF. IPsec is used to provide end-to-end encryption and verification services in the network to provide high quality and interoperability for data transmission over the network and ensure transmission security by using cryptographic algorithms. The communicating parties obtain the following security services at the IP layer through encryption and data source authentication:

- Confidentiality: The IPsec sender encrypts packets before transmitting the packets over the network.
- Data integrity: The IPsec receiver authenticates packets received from the sender to ensure that data is not tampered with during the transmission.
- Data authentication: The IPsec receiver authenticates whether the sender of IPsec packets is valid.
- Anti-replay: The IPsec receiver detects and denies expired or repeated packets.
- The IPsec protocol is widely used for communication between the HQ and branches of an organization. Currently, the device can be deployed as the IPsec server or client. A secure tunnel is established between the HQ and each branch based on the IPsec protocol to ensure the confidentiality of data transmission and improve network security.

2. IKE Overview

IPsec provides secure communication between two endpoints, which are called IPsec peers. Security Association (SA) is the establishment of shared security attributes between the peers to support secure communication. An SA may include attributes such as: security protocol used by the peers, characteristics of data flows to be protected, encapsulation mode of data transmitted between the peers, encryption and authentication algorithms, keys for secure data conversion and transmission, and the SA lifetime. When you configure IPsec, you can use the Internet Key Exchange (IKE) protocol to establish an SA. IKE provides automatically negotiated keys for establishing and maintaining SAs, simplifying IPsec usage and management.

3. IPsec Security Policy

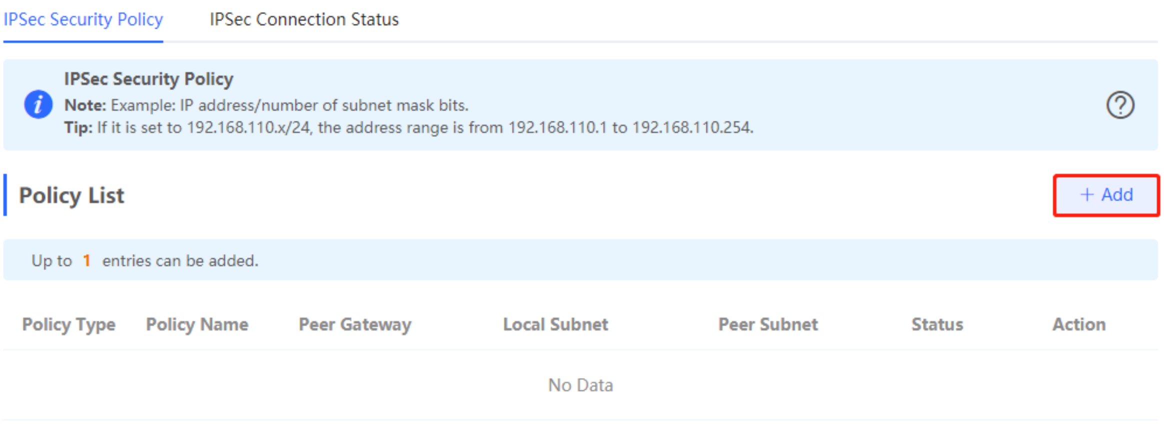
IPsec security policies define security proposals (equivalent to SA) for data flows. You can configure matching security policies on both parties engaged in the communication to establish IPsec tunnels between the IPsec client and the IPsec server, protecting the communication data. An IPsec security policy consists of two parts: basic settings and advanced settings. Advanced settings are optional and include the specific IKE policy and connection policy. You can keep the default settings unless otherwise specified. For details, see the Configuration Steps below.

5.1.2 Configuring the IPsec Server

Choose **Local Device** > **VPN** > **IPsec** > **IPsec Security Policy**.

1. Basic Settings

Click **Add**. In the dialog box that appears, set **Policy Type** to **Server**, enter the policy name and local subnet range, set the pre-shared key, and click **OK**.



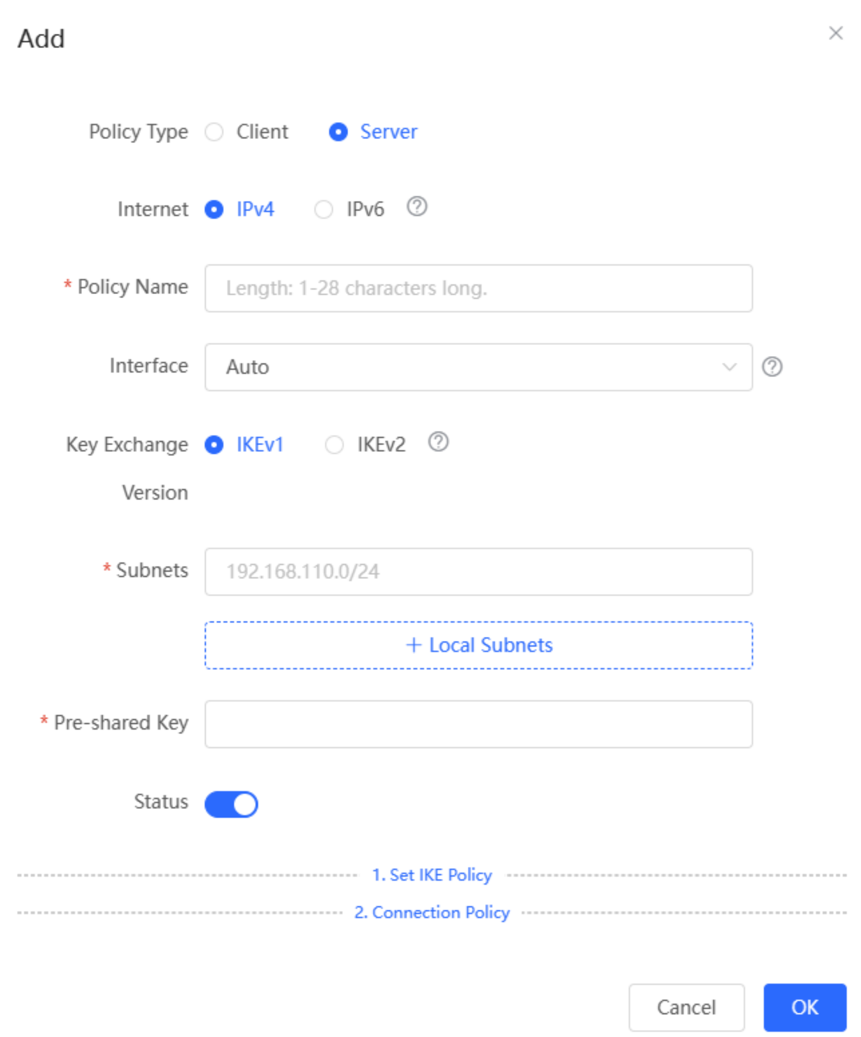
IPSec Security Policy | IPSec Connection Status

IPSec Security Policy
Note: Example: IP address/number of subnet mask bits.
Tip: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.

Policy List + Add

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
No Data						



Add

Policy Type ○ Client ● Server

Internet ● IPv4 ○ IPv6

* Policy Name: Length: 1-28 characters long.

Interface: Auto

Key Exchange Version ● IKEv1 ○ IKEv2

* Subnets: 192.168.110.0/24

+ Local Subnets

* Pre-shared Key:

Status: on

1. Set IKE Policy

2. Connection Policy

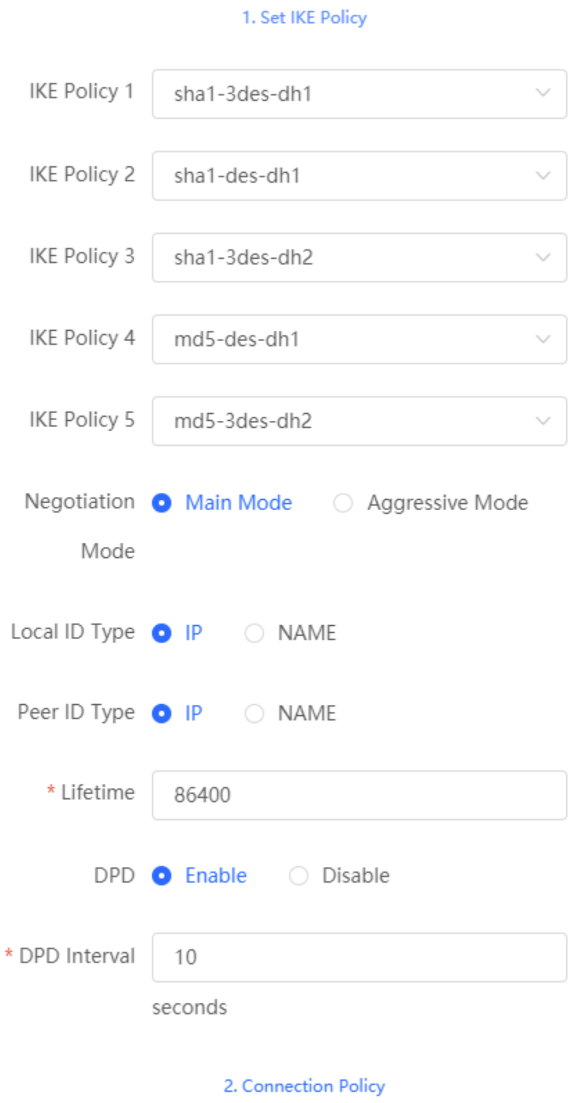
Cancel OK

Table 5-1 **IPsec server basic settings**

Parameter	Description
Policy Name	Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters.
Interface	Select a local WAN port from the drop-down list box. The **Peer Gateway** parameter set for the communication peer (IPsec client) must use the IP address of the WAN port specified here. In the multi-line scenario, you are advised to set this parameter to **Auto**.
Key Exchange Version	Select the IKE version for SA negotiation. There are two options available: ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. ○ Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. ○ Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair.
Local Subnet	Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask.
Pre-shared Key	Specify the same pre-shared key as the credential for authentication between communicating parties. For higher security, different peers must be configured with different pre-shared keys. That is, a pair of interface bound to the IPsec server and peer gateway of the IPsec client must be configured with the same unique pre-shared key.
Status	Specify whether to enable the security policy.

2. Advanced Settings (Phase 1)

Click **1. Set IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.



1. Set IKE Policy

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 Mode: ● Main Mode ○ Aggressive Mode

Local ID Type: ● IP ○ NAME

Peer ID Type: ● IP ○ NAME

* Lifetime: 86400

DPD: ● Enable ○ Disable

* DPD Interval: 10 seconds

2. Connection Policy

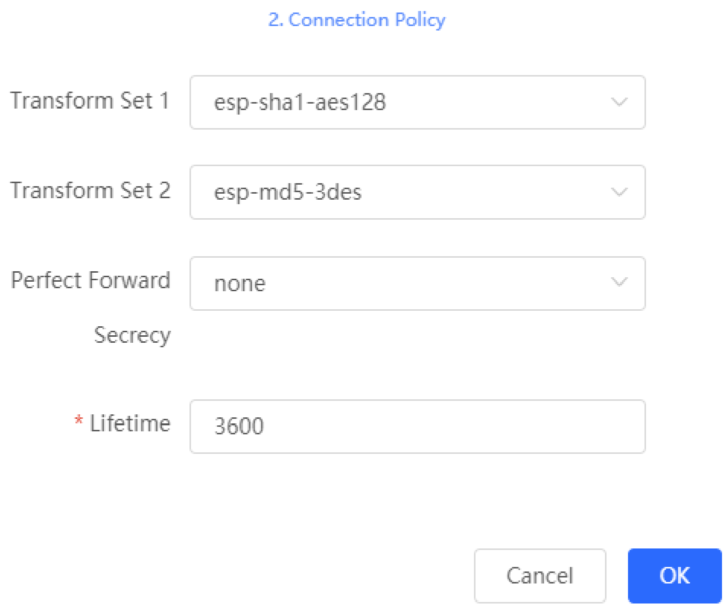
Table 5-2 IPsec server IKE policy configuration

Parameter	Description
IKE Policy	Select the hash algorithm, encryption algorithm, and Diffie-Hellman (DH) group ID used by the IKE protocol. An IKE policy is composed of the three parameters. You can set five sets of IKE policies. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy. ● Hash algorithm: ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group
Negotiation Mode	Select **Main Mode** or **Aggressive Mode**. The negotiation mode on the IPsec server and IPsec client must be the same. ● Main Mode: Generally, this mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● Aggressive Mode: The public network IP addresses obtained by ADSL dial-up users are not fixed and an NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to **NAME** as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security.

Parameter	Description
Local/Peer ID Type	Specify the ID type of the local or peer device. The local ID type of the peer device must be the same as the peer ID type of the local device. ● IP: The IP address is used as the identity ID. The IDs of the local and peer devices are generated automatically. ● NAME: The host character string is used as the identity ID. The IDs of the local and peer devices are generated automatically. When the IP address is not fixed, you need to set **Local ID Type** to **NAME** and modify the peer device settings accordingly. In this case, you also need to configure the host character string that is used as the identity ID.
Local/Peer ID	When the local or peer ID type is set to **NAME**, you also need to host character string that is used as the identity ID. The local ID of the peer device must be the same as peer ID of the local device.
Lifetime	Specify the lifetime of the IKE SA. (The negotiated IKE SA lifetime prevails.) You are advised to use the default value.
DPD	Specify whether to enable Dead Peer Detection (DPD) to detect the IPsec neighbor status. After DPD is enabled, if the receiver does not receive IPsec encrypted packets from the peer within the DPD detection interval, DPD query will be triggered and the receiver actively sends a request packet to detect whether the IKE peer exists. You are advised to configure DPD when links are unstable.
DPD Interval	Specify the DPD detection interval. That is, the interval for triggering DPD query. You are advised to keep the default setting.

3. Advanced Settings (Phase 2)

Click **2. Connection Policy** to expand the configuration items. Keep the default settings unless otherwise specified.



2. Connection Policy

Transform Set 1: esp-sha1-aes128

Transform Set 2: esp-md5-3des

Perfect Forward Secrecy: none

* Lifetime: 3600

Table 5-3 IPsec server connection policy configuration

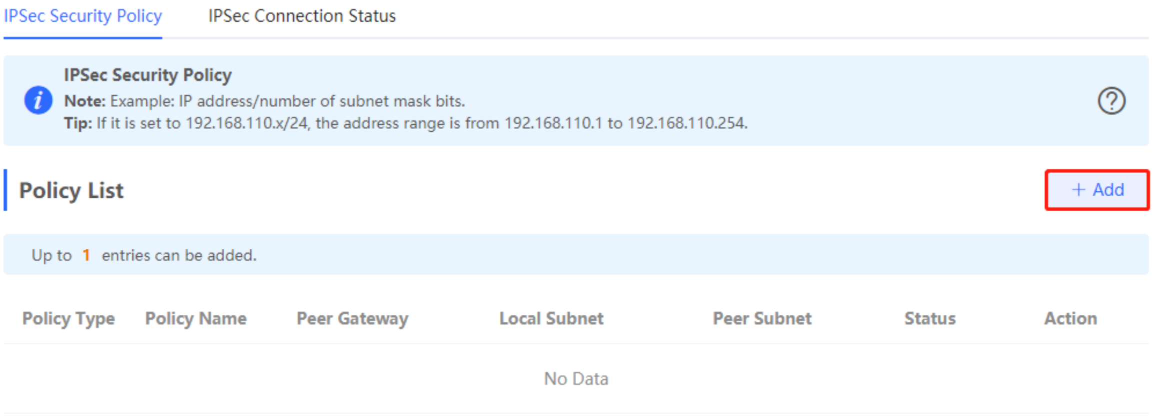
Parameter	Description
Transform Set	Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the IPsec server and IPsec client must be the same. ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: o sha1: SHA-1 HMAC o md5: MD5 HMAC ● Encryption algorithm: o des: DES algorithm using 56-bit keys o 3des: 3DES algorithm using 168-bit keys o aes-128: AES algorithm using 128-bit keys o aes-192: AES algorithm using 192-bit keys o aes-256: AES algorithm using 256-bit keys

Parameter	Description
Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) is a security feature that can guarantee the security of other keys when one key is cracked, because there is no derivative relationship among the keys. After PFS is enabled, temporary private key exchange is performed when an IKE negotiation is initiated using a security policy. If PFS is configured on the local device, it must also be configured on the peer device that initiates negotiation and the DH group specified on the local and peer devices must be the same. Otherwise, negotiation will fail. ● none: Disable PFS. ● d1: 768-bit DH group ● d2: 1024-bit DH group ● d5: 1536-bit DH group By default, PFS is disabled.

5.1.3 Configuring the IPsec Client

Choose **Local Device** > **VPN** > **IPsec** > **IPsec Security Policy**.

Click **Add**. In the dialog box that appears, set **Policy Type** to **Client**, enter the policy name, peer gateway, local subnet range, and peer subnet range, set the pre-shared key, and click **OK**.



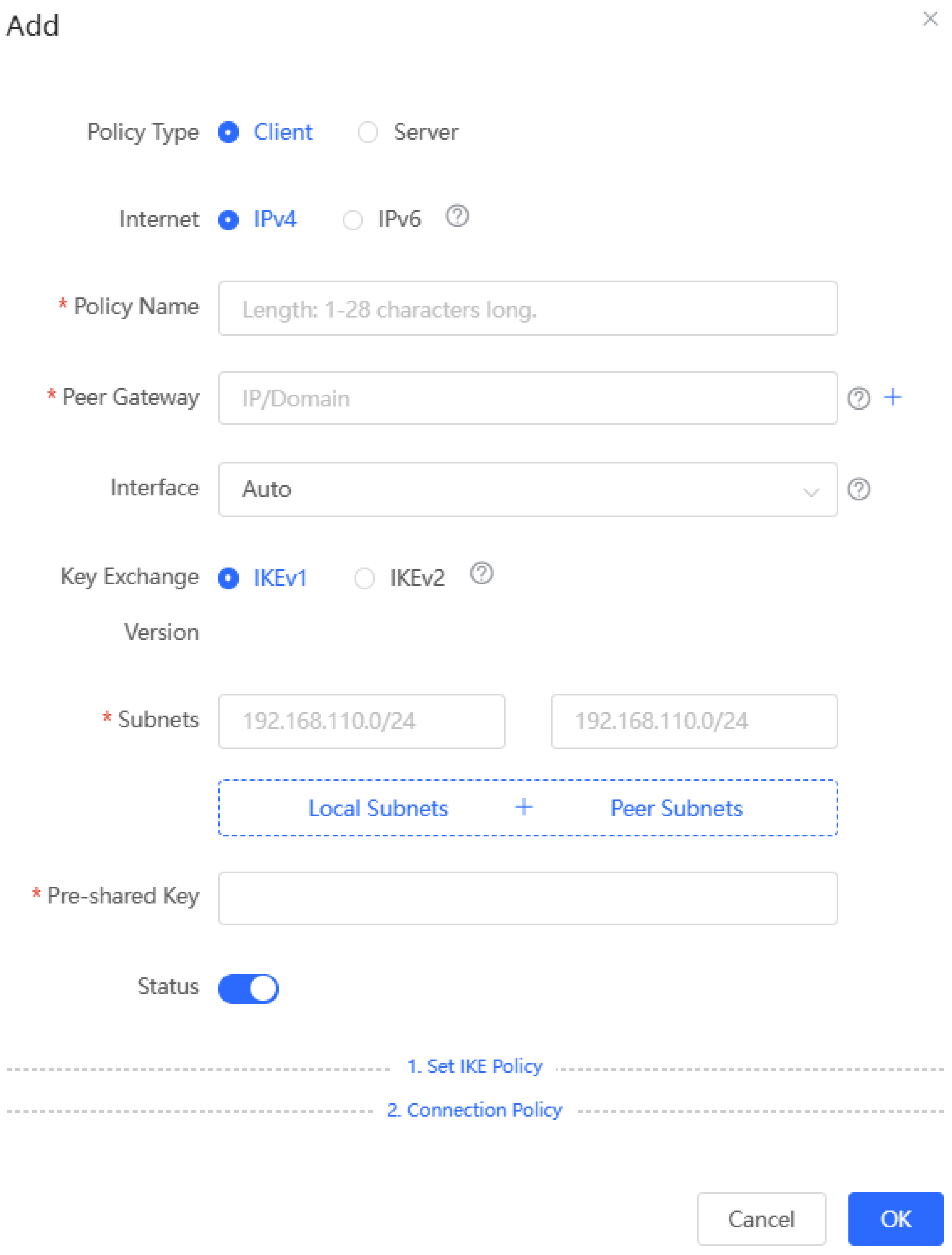
IPSec Security Policy

Note: Example: IP address/number of subnet mask bits.

Tip: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
No Data						



Add

Policy Type ● Client ○ Server

Internet ● IPv4 ○ IPv6

* Policy Name: Length: 1-28 characters long.

* Peer Gateway: IP/Domain

Interface: Auto

Key Exchange Version ● IKEv1 ○ IKEv2

* Subnets: 192.168.110.0/24 192.168.110.0/24

* Pre-shared Key:

Status: On

Table 5-4 IPsec client basic settings

Parameter	Description
Policy Name	Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters.

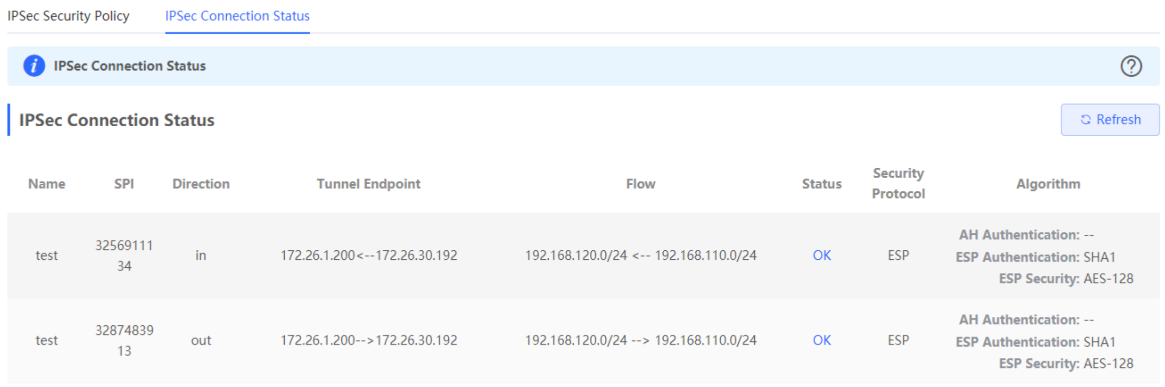
Parameter	Description
Peer Gateway	Enter the IP address or domain name of the peer device.
Interface	Select a WAN port used locally from the drop-down list box. In the multi-line scenario, you are advised to set this parameter to **Auto**.
Key Exchange Version	Select the IKE version for SA negotiation. There are two options available: ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. ○ Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. ○ Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair.
Local Subnet	Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask.
Peer Subnet	Specify the peer subnet address range for the data flows to be protected, that is, the LAN port network segment of the client. The value is the combination of IP address and subnet mask.
Pre-shared Key	Configure the pre-shared key the same as that on the IPsec server.
Status	Specify whether to enable the security policy.

You can configure advanced parameters by referring to the corresponding settings on the IPsec server. For details, see Advanced Settings (Phase 1) and Advanced Settings (Phase 2).

5.1.4 Viewing the IPsec Connection Status

Choose **Local Device** > **VPN** > **IPsec** > **IPsec Connection Status**.

You can view the IPsec tunnel connection status on the current page.



IPSec Security Policy IPSec Connection Status

IPSec Connection Status

IPSec Connection Status

Refresh

Name	SPI	Direction	Tunnel Endpoint	Flow	Status	Security Protocol	Algorithm
test	3256911134	in	172.26.1.200<--172.26.30.192	192.168.120.0/24 <-- 192.168.110.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
test	3287483913	out	172.26.1.200-->172.26.30.192	192.168.120.0/24 --> 192.168.110.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128

Table 5-5 IPsec tunnel connection status information

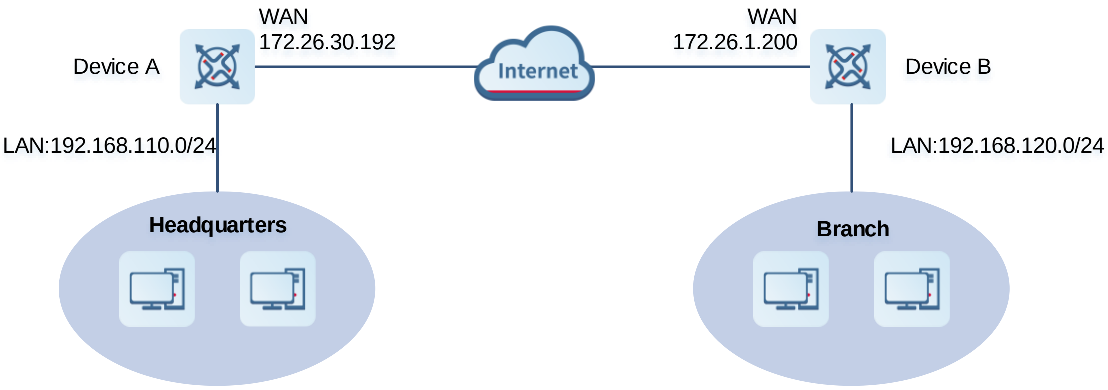
Parameter	Description
Name	Indicate the security policy name on the IPsec server or client.
SPI	Indicate the Security Parameter Index (SPI) of the IPsec connection, used to associate the received IPsec data packets with the corresponding SA. The SPI of each IPsec connection must be unique.
Direction	Indicate the direction of the IPsec connection. The value **in** indicates inbound, and the value **out** indicates outbound.
Tunnel Client	Indicate the gateway addresses on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel.
Flow	Indicate the subnet range on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel.
Status	Indicate the IPsec tunnel connection status.
Security Protocol	Indicate the security protocol used by the IPsec connection.
Algorithm	Indicate the encryption algorithm and authentication algorithm used by the IPsec connection.

5.1.5 Typical Configuration Example

1. Networking Requirements

The HQ and branch of an enterprise are connected through the Internet. An IPsec tunnel needs to be established between the HQ gateway and branch gateway to ensure the confidentiality of transmitted data.

2. Networking Diagram



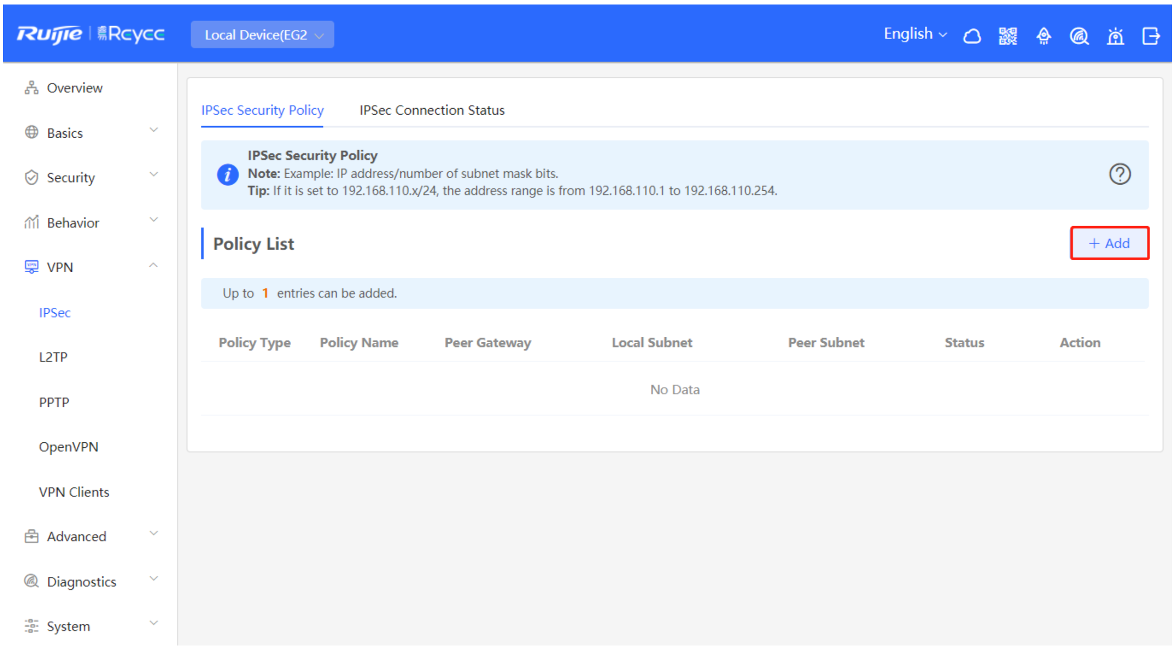
3. Configuration Roadmap

- Configure the HQ gateway Device A as the IPsec server.
- Configure the branch gateway Device B as the IPsec client.

4. Configuration Steps

(1) Configure the HQ gateway.

a Log in to the web management system and choose VPN > IPsec > IPsec Security Policy to access the IPsec Security Policy page.



IPSec Security Policy
Note: Example: IP address/number of subnet mask bits.
Tip: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.

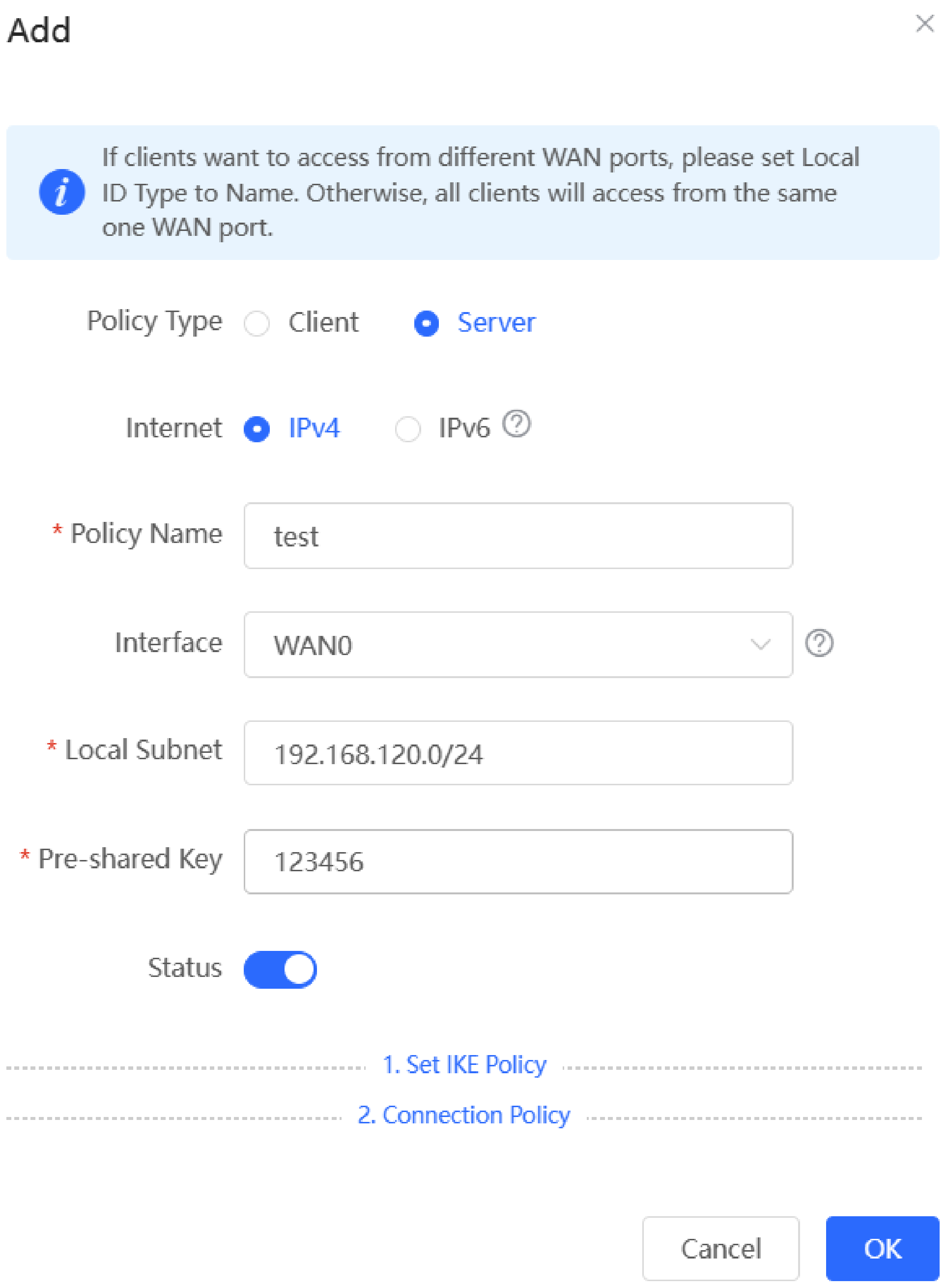
Policy List

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
No Data						

b Click Add. In the dialog box that appears, set Policy Type to Server, enter the policy name, select the bound interface, and configure the local subnet to be accessed through IPsec and the pre-shared key.

If the device connects to other EG devices in the Reyee network, you are advised to keep the default settings in IKE phase 1 and phase 2. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.



Add

If clients want to access from different WAN ports, please set Local ID Type to Name. Otherwise, all clients will access from the same one WAN port.

Policy Type ○ Client ● Server

Internet ● IPv4 ○ IPv6

* Policy Name: test

Interface: WAN0

* Local Subnet: 192.168.120.0/24

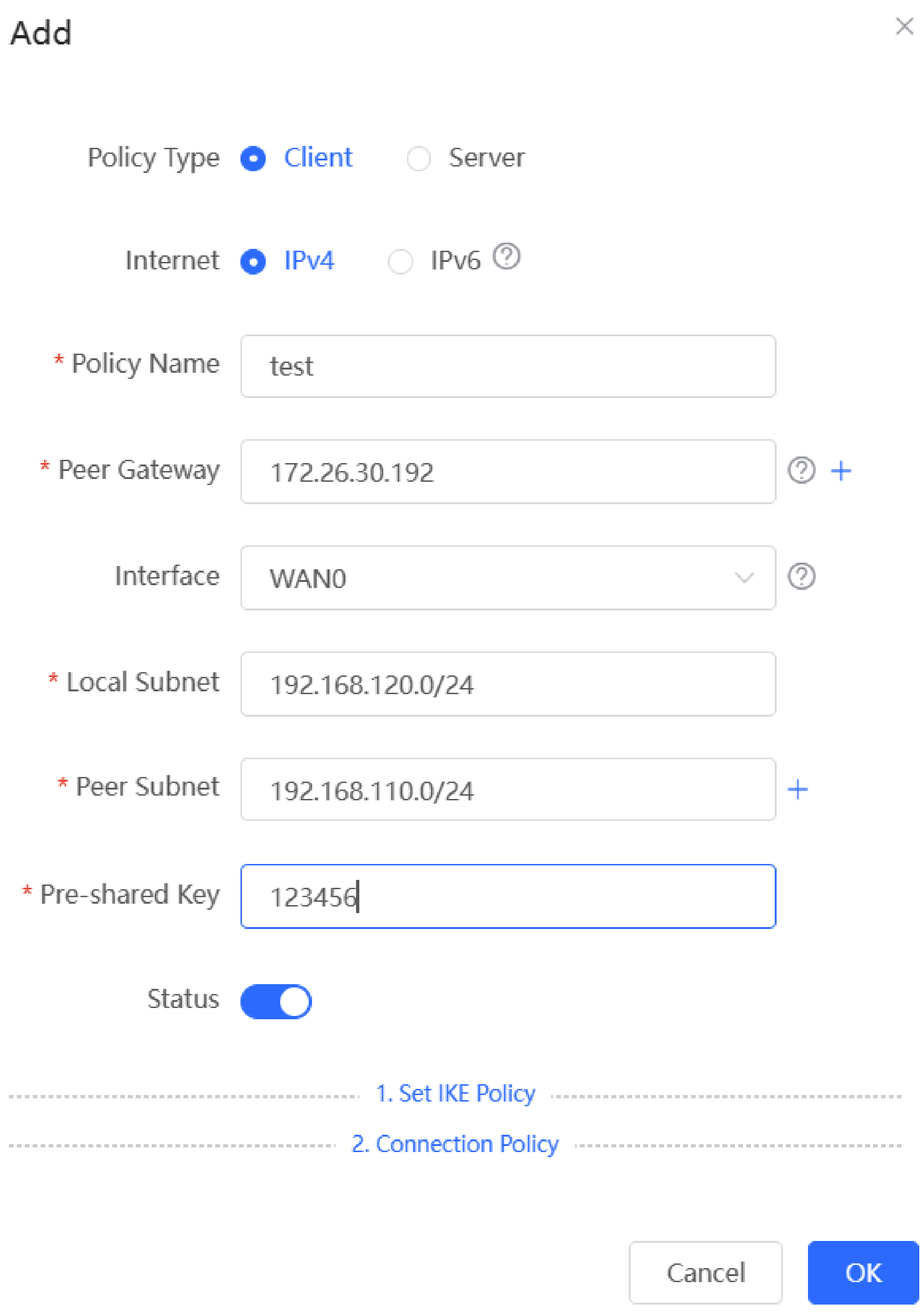
* Pre-shared Key: 123456

Status: On

(2) Configure the branch gateway.

a Log in to the web management system and access the IPsec Security Policy page.

b Click Add. In the dialog box that appears, set Policy Type to Client, enter the policy name, select the peer gateway (WAN port address or domain name of the HQ gateway), and configure the local subnet that needs to access the peer subnet and the pre-shared key the same as that on the HQ gateway. Keep the other phase 1 and phase 2 parameters consistent with those on the IPsec server.



Add

Policy Type ● Client ○ Server

Internet ● IPv4 ○ IPv6

* Policy Name: test

* Peer Gateway: 172.26.30.192

Interface: WAN0

* Local Subnet: 192.168.120.0/24

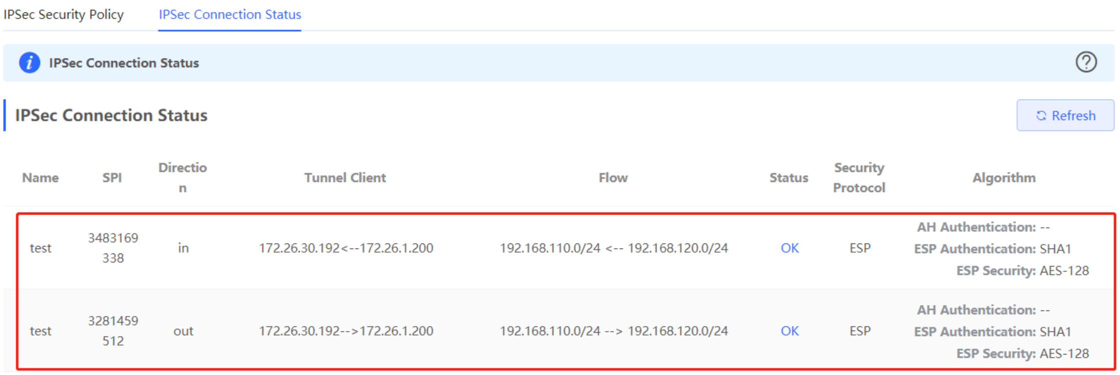
* Peer Subnet: 192.168.110.0/24

* Pre-shared Key: 123456

Status: On

5. Verifying Configuration

(1) Log in to the web management system of the HQ or branch gateway and choose **VPN** > **IPsec** > **IPsec Connection Status**. You can view the IPsec connection status between the HQ and branch.



IPSec Connection Status

IPSec Connection Status

Name	SPI	Direction	Tunnel Client	Flow	Status	Security Protocol	Algorithm
test	3483169338	in	172.26.30.192<--172.26.1.200	192.168.110.0/24 <-- 192.168.120.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
test	3281459512	out	172.26.30.192-->172.26.1.200	192.168.110.0/24 --> 192.168.120.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128

(2) Perform ping test between clients on the two ends that need to access each other. The clients can successfully ping and access each other.

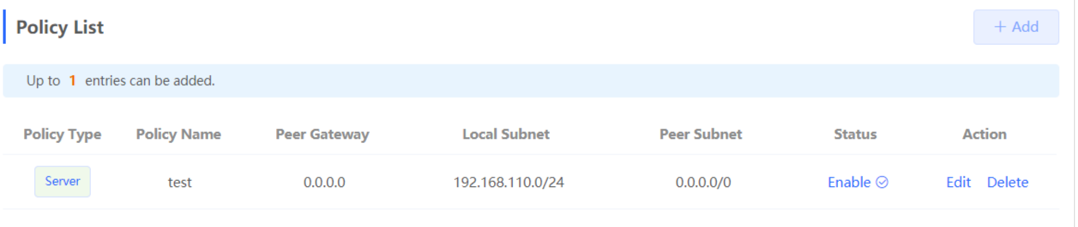
5.1.6 Solution to IPsec VPN Connection Failure

(1) Run the ping command to test the connectivity between the client and server. For details, see Section 4.4.3 Network Tools. If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.

Click **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section 4.4.3 Network Tools.

(2) Confirm that the configurations on the IPsec server and IPsec client are correct.

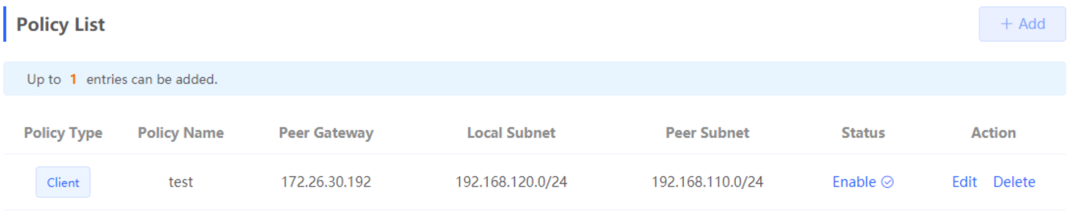
Choose **VPN** > **IPsec** > **IPsec Security Policy** and confirm that the security policies configured on the two ends are matching.



Policy List

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
Server	test	0.0.0.0	192.168.110.0/24	0.0.0.0/0	Enable ✓	Edit Delete

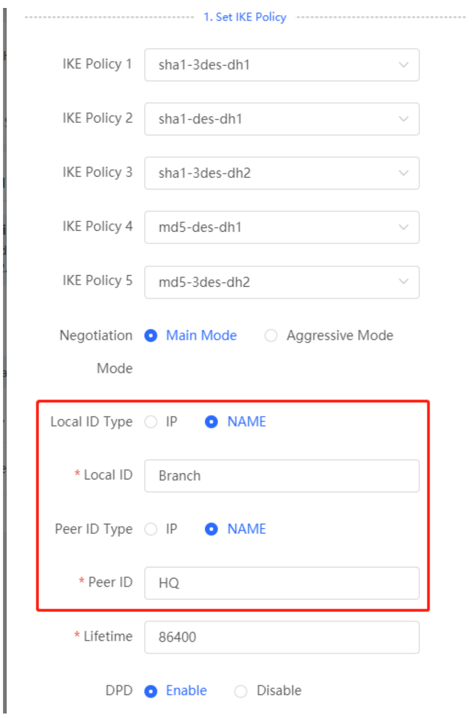


Policy List

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
Client	test	172.26.30.192	192.168.120.0/24	192.168.110.0/24	Enable ✓	Edit Delete

(3) Check whether the WAN IP address of your HQ EG is a public IP address. If not, you need to configure DMZ or port mapping (UDP 500 and 4500 used as IPsec VPN port) on your egress gateway and set **Local ID Type** to **NAME** on HQ and branch gateways.



1. Set IKE Policy

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 Mode: ● Main Mode ○ Aggressive Mode

Local ID Type: ○ IP ● NAME

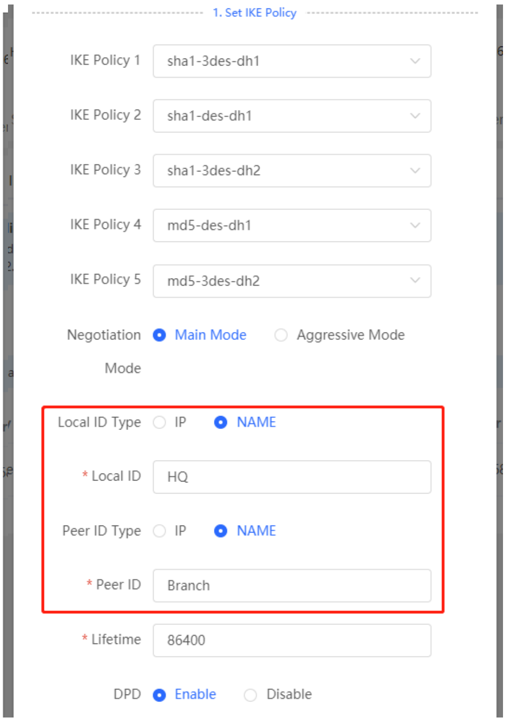
* Local ID: Branch

Peer ID Type: ○ IP ● NAME

* Peer ID: HQ

* Lifetime: 86400

DPD: ● Enable ○ Disable



1. Set IKE Policy

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 Mode: ● Main Mode ○ Aggressive Mode

Local ID Type: ○ IP ● NAME

* Local ID: HQ

Peer ID Type: ○ IP ● NAME

* Peer ID: Branch

* Lifetime: 86400

DPD: ● Enable ○ Disable

5.2 Configuring L2TP VPN

5.2.1 Overview

Layer Two Tunneling Protocol (L2TP) is a virtual tunneling protocol, usually used in virtual private networks.

The L2TP protocol does not provide encryption and reliability verification functions, but it can work with a security protocol to implement encrypted data transmission. L2TP is frequently used with IPsec to encapsulate packets using L2TP before encapsulating packets using IPsec. This combination implements user verification and address allocation through L2TP and ensures communication security through IPsec.

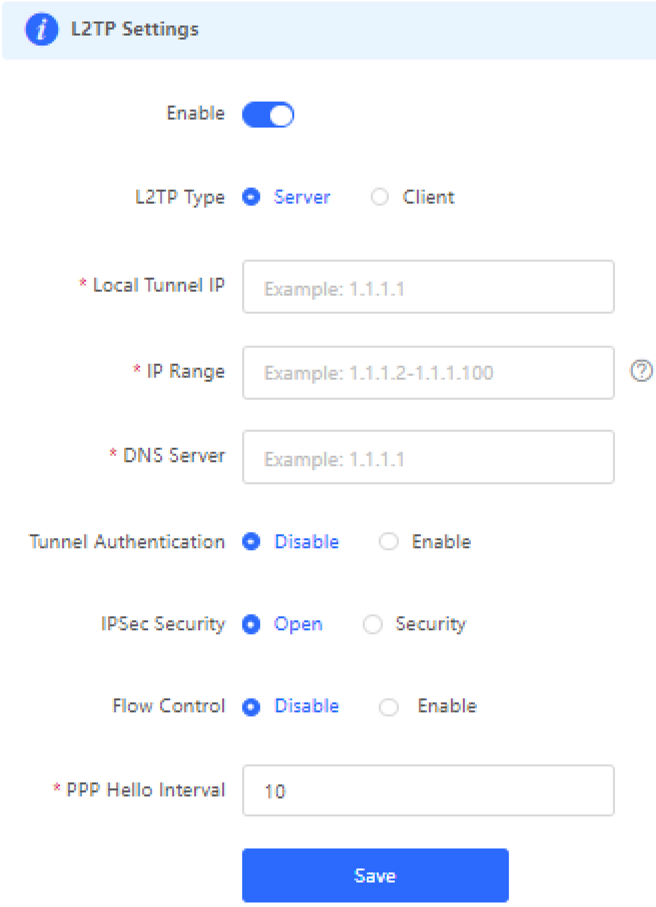
L2TP VPN can be used to establish secure tunnels between the enterprise HQ and branches and allow traveling employees to access the HQ. Currently, the device can be deployed as the L2TP server or client.

5.2.2 Configuring the L2TP Server

1. Basic Settings of L2TP Server

Choose **Local Device** > **VPN** > **L2TP** > **L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Server**, set L2TP server parameters, and click **Save**.



L2TP Settings

Enable

L2TP Type ● Server ○ Client

* Local Tunnel IP Example: 1.1.1.1

* IP Range Example: 1.1.1.2-1.1.1.100

* DNS Server Example: 1.1.1.1

Tunnel Authentication ● Disable ○ Enable

IPSec Security ● Open ○ Security

Flow Control ● Disable ○ Enable

* PPP Hello Interval 10

Table 5-6 L2TP server configuration

Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address.
IP Range	Specify the address pool used by the L2TP server to allocate IP addresses to clients.
DNS Server	Specify the DNS server address pushed by the L2TP server to clients.

Parameter	Description
Tunnel Authentication	Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to configure a tunnel authentication key. By default, tunnel authentication is disabled. The tunnel authentication request can be initiated by clients. If tunnel authentication is enabled on one end, a tunnel to the peer can be established only when tunnel authentication is also enabled on the peer and consistent keys are configured on the two ends. Otherwise, the local end will automatically shut down the tunnel connection. If tunnel authentication is disabled on both ends, no authentication key is required for tunnel establishment. When a PC functions as the client to access the L2TP server, you are advised not to enable tunnel authentication on the L2TP server.
IPsec Security	Specify whether to encrypt the tunnel. If you select **Security**, the device encrypts the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode. If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first. The IPsec encryption configuration on the L2TP server and client must be consistent. For details, see Configuring the L2TP over IPsec Server.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 4.15.2 Smart Flow Control.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.

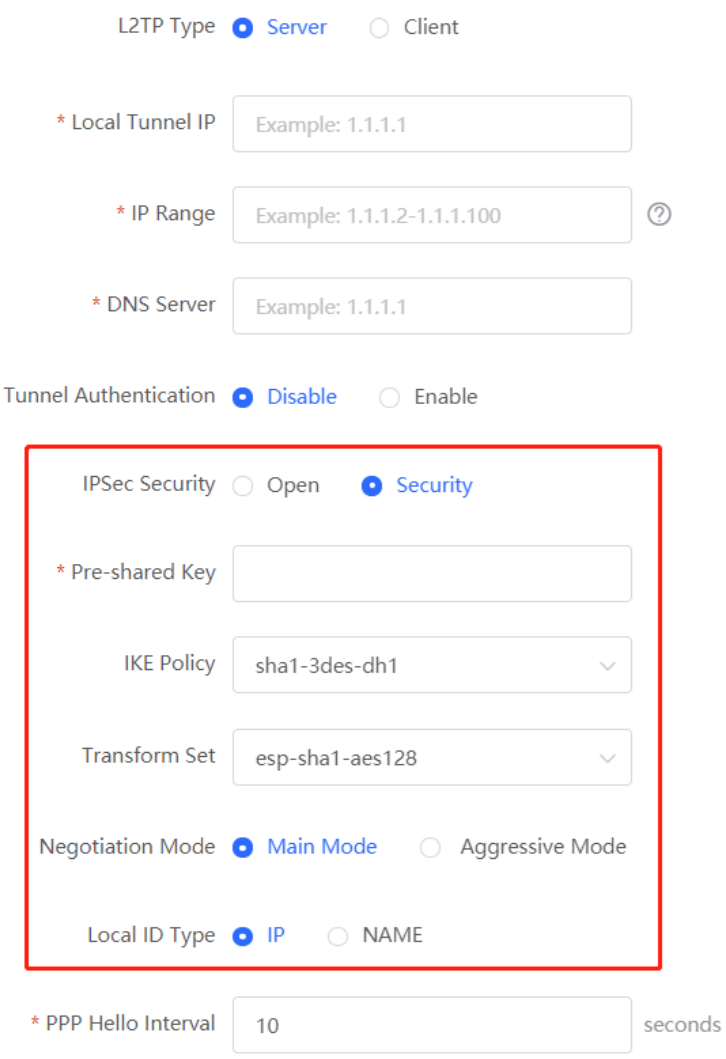
⚠ **Caution**

The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring the L2TP over IPsec Server

Choose **Local Device** > **VPN** > **L2TP** > **L2TP Settings**.

After you complete Basic Settings of L2TP Server, enable IPsec encryption on the L2TP server to guarantee communication security. For details on the IPsec configuration, see Section 5.1 Configuring IPsec VPN.



L2TP Type ● Server ○ Client

* Local Tunnel IP: Example: 1.1.1.1

* IP Range: Example: 1.1.1.2-1.1.1.100

* DNS Server: Example: 1.1.1.1

Tunnel Authentication ● Disable ○ Enable

IPSec Security ○ Open ● Security

* Pre-shared Key:

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

Table 5-7 L2TP over IPsec server configuration

Parameter	Description
Pre-shared Key	Specify the same unique pre-shared key as the credential for mutual authentication between the server and client.

Parameter	Description
IKE Policy	Select the encryption algorithm, hash algorithm, and DH group ID used by the IKE protocol. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy. The IKE policies on the server and client must be consistent. ● Hash algorithm: ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group
Transform Set	Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the server and client must be the same. ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: ○ sha1: SHA-1 HMAC ○ md5: MD5 HMAC ● Encryption algorithm: ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys

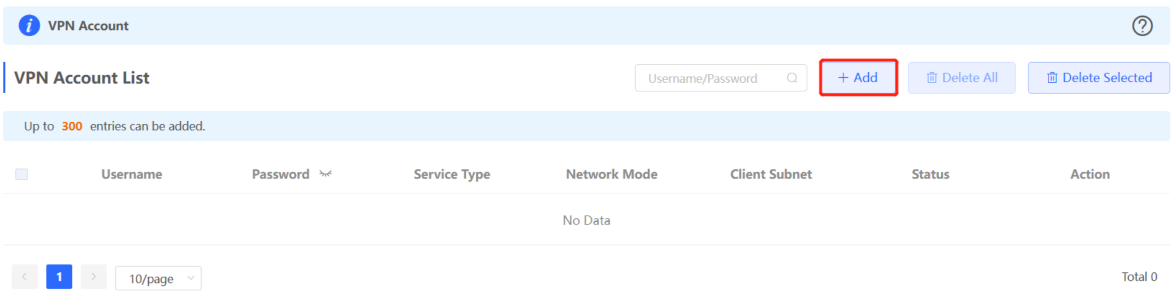
Parameter	Description
Negotiation Mode	Select **Main Mode** or **Aggressive Mode**. The negotiation mode on the server and client must be the same. ● Main Mode: This mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● Aggressive Mode: The public network IP addresses obtained by ADSL dial-up users are not fixed and an NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to **NAME** as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security.
Local ID Type	Specify the ID type of the local device. The peer ID of the client must be the same as local ID of the server. ● IP: The IP address is used as the identity ID. The ID of the local device is generated automatically. ● NAME: The host character string is used as the identity ID. The ID of the local device is generated automatically. In this case, you also need to configure the host character string that is used as the identity ID. When the WAN port IP address of the server is a private network address, you need to set **Local ID Type** to **NAME** and configure DMZ on the external device. When the IP address is not fixed, you need to set **Local ID Type** to **NAME** and modify the peer device settings accordingly.
Local ID	When **Local ID Type** is set to **NAME**, the host character string is used as the identity ID. The peer ID of the client must be the same as local ID of the server.

3. Configuring L2TP User

Choose **Local Device** > **VPN** > **VPN Account**

Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **L2TP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.



VPN Account

VPN Account List

Username/Password

+ Add

Delete All

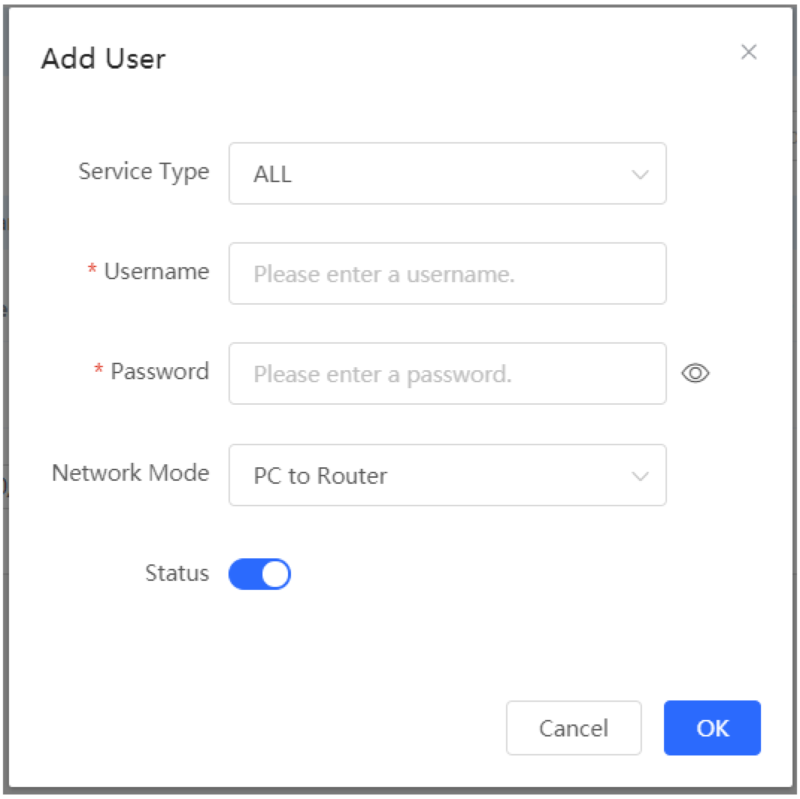
Delete Selected

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: ALL

* Username: Please enter a username.

* Password: Please enter a password.

Network Mode: PC to Router

Status: on

Cancel OK

Table 5-8 L2TP user configuration

Parameter	Description
Username/Password	Specify the name and password of the L2TP user allowed to dial up to connect to the L2TP server. The username and password are used to establish a connection between the server and client.
Network Mode	● PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. ● Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up.

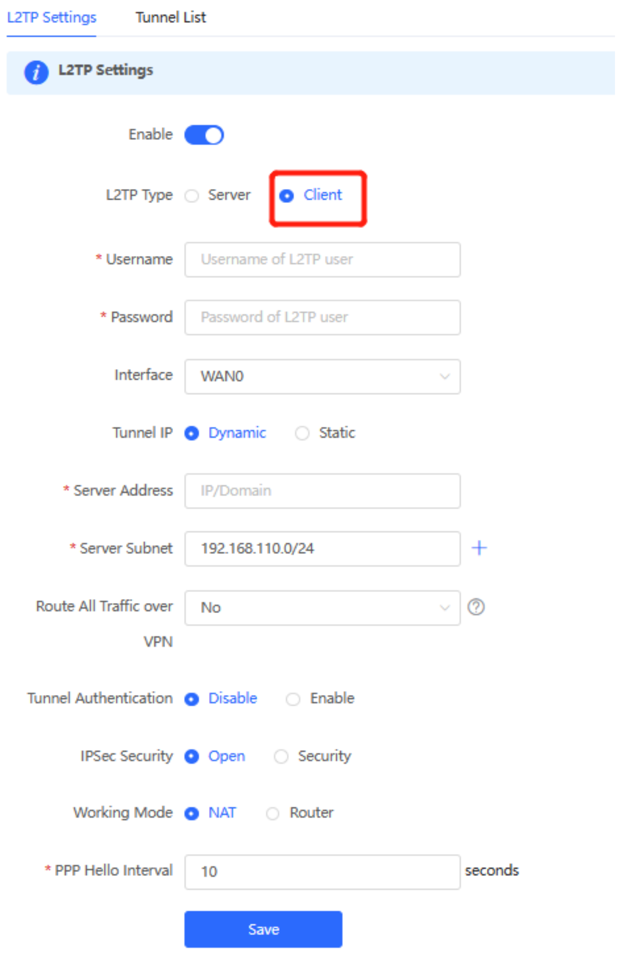
Parameter	Description
Client Subnet	Specify the IP address range used by the LAN on the peer end of the L2TP tunnel. Generally, the Client Subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.) For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router. Note: When the Network Mode is set to Router to Router, you can click + to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.
Status	Specify whether to enable the user account.

5.2.3 Configuring the L2TP Client

1. Basic Settings of L2TP Client

Choose **Local Device** > **VPN** > **L2TP** > **L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Client**, set L2TP client parameters, and click **Save**.



Enable: On

L2TP Type: ○ Server ● Client

* Username: Username of L2TP user

* Password: Password of L2TP user

Interface: WAN0

Tunnel IP: ● Dynamic ○ Static

* Server Address: IP/Domain

* Server Subnet: 192.168.110.0/24 +

Route All Traffic over VPN: No

Tunnel Authentication: ● Disable ○ Enable

IPSec Security: ● Open ○ Security

Working Mode: ● NAT ○ Router

* PPP Hello Interval: 10 seconds

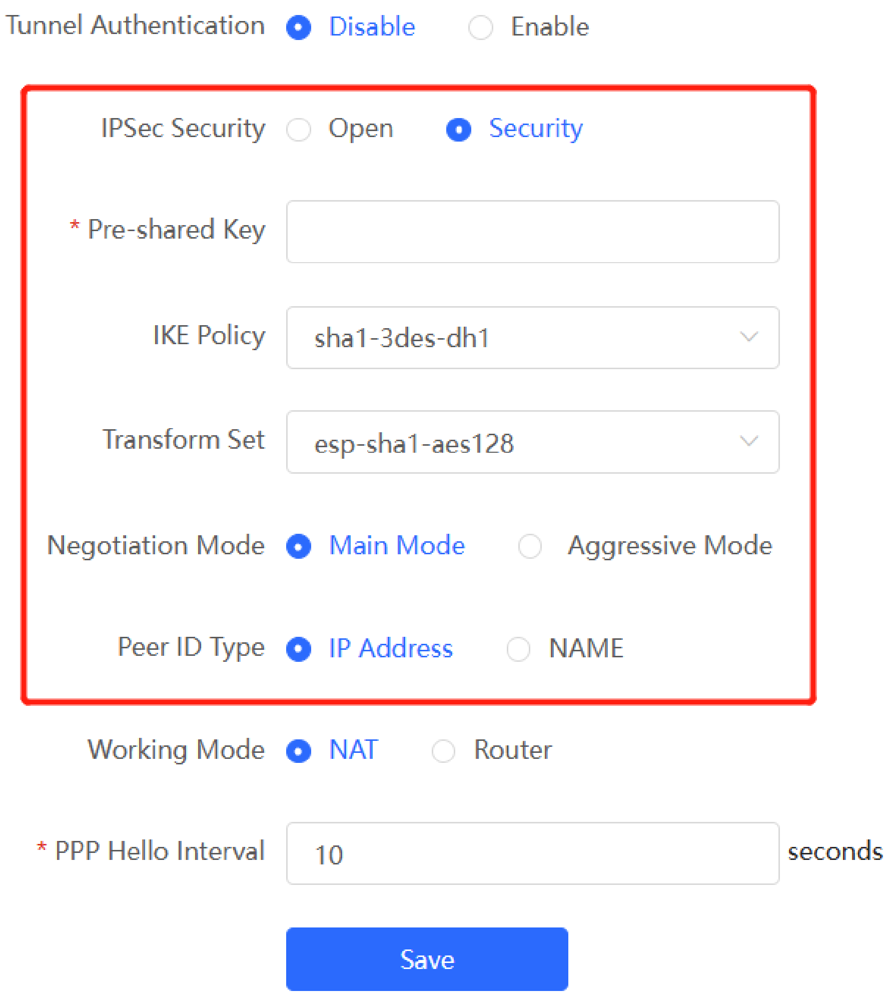
Table 5-9 L2TP client configuration

Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the L2TP tunnel. The values must be the same as those configured on the L2TP server.
Interface	Specify the WAN port used by the client.
Tunnel IP	Specify the virtual IP address of the VPN tunnel client. If you select **Dynamic**, the client obtains an IP address from the server address pool. If you select **Static**, manually configure an idle static address within the range of the server address pool as the local tunnel IP address.
Server Address	Enter the WAN port IP address or domain name of the server. This address must be a public network IP address.
Server Subnet	Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client.
Route ALL Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
Tunnel Authentication	Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to enter tunnel authentication key the same as that configured on the server. By default, tunnel authentication is disabled. To protect tunnel security, you are advised to enable tunnel authentication.
IPsec Security	Specify whether to encrypt the tunnel. If you select **Security**, the device Enable the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode. The IPsec encryption configuration on the server and client must be consistent. For details, see Configuring the L2TP over IPsec Client.
Working Mode	● NAT: Perform NAT traversal on the data packet passing through the L2TP tunnel. That is, replace the source IP address of the data packet with the local virtual IP address of the L2TP tunnel. In NAT mode, the server cannot access the LAN where the client resides. ● Router: Only route the data packet passing through the L2TP tunnel. In router mode, the server can access the LAN where the client resides.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.

2. Configuring the L2TP over IPsec Client

Choose **Local Device** > **VPN** > **L2TP** > **L2TP Settings**.

After you complete Basic Settings of L2TP Client, enable IPsec encryption on the L2TP client to guarantee communication security. The IPsec encryption configuration on the server and client must be consistent. For details, see Configuring the L2TP over IPsec Server.



Tunnel Authentication ● Disable ○ Enable

IPSec Security ○ Open ● Security

* Pre-shared Key

IKE Policy: sha1-3des-dh1

Transform Set: esp-sha1-aes128

Negotiation Mode ● Main Mode ○ Aggressive Mode

Peer ID Type ● IP Address ○ NAME

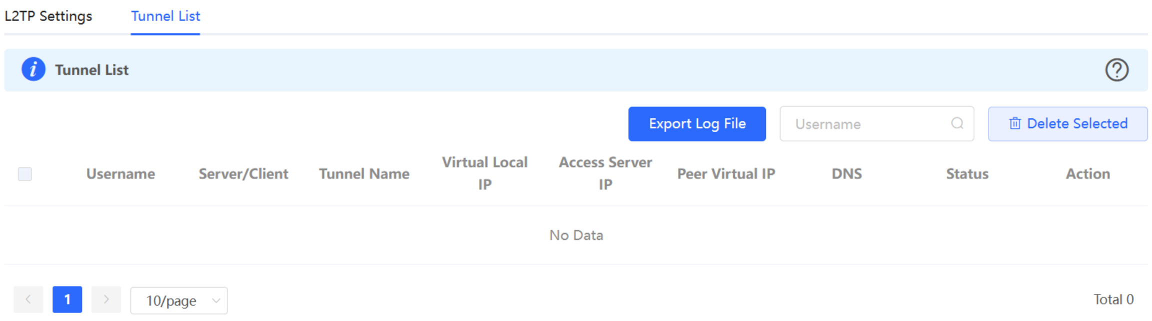
Working Mode ● NAT ○ Router

* PPP Hello Interval: 10 seconds

5.2.4 Viewing the L2TP Tunnel Information

Choose **Local Device** > **VPN** > **L2TP** > **Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the L2TP tunnel establishment status.



□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Status	Action
No Data									

Table 5-10 L2TP tunnel information

Parameter	Description
Username	Indicate the username used by the client for identity authentication.
Server/Client	Indicate the role of the current device, which is client or server.
Tunnel Name	Indicate the name of the vNIC generated by L2TP.
Virtual Local IP	Indicate the local virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server.
Access Server IP	Indicate the real IP address of the peer connecting to the L2TP tunnel.
Peer Virtual IP	Indicate the peer virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server.
DNS	Indicate the DNS server address allocated by the L2TP server.

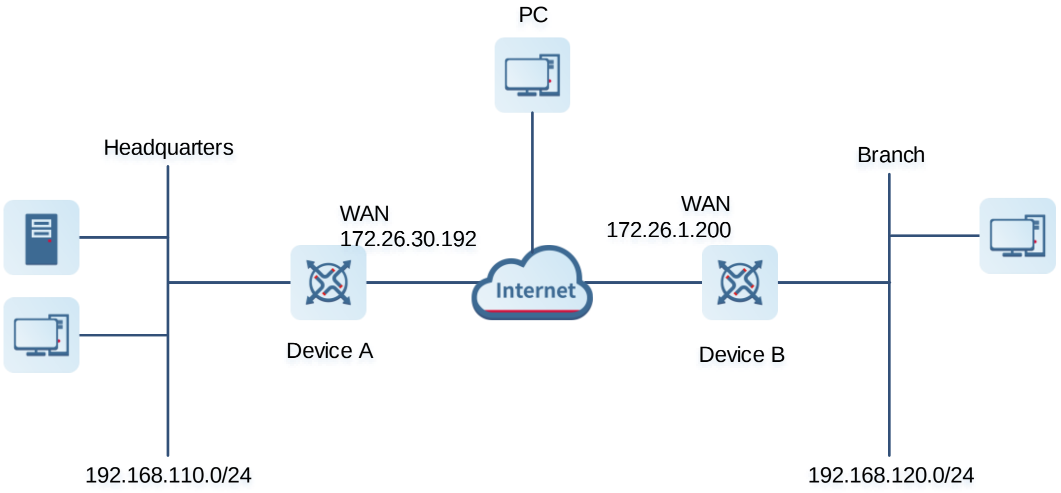
5.2.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish an L2TP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through L2TP VPN.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the L2TP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the L2TP server.
- Configure the branch gateway Device B as the L2TP client.
- Configure the PC of the traveling employee as the L2TP client.

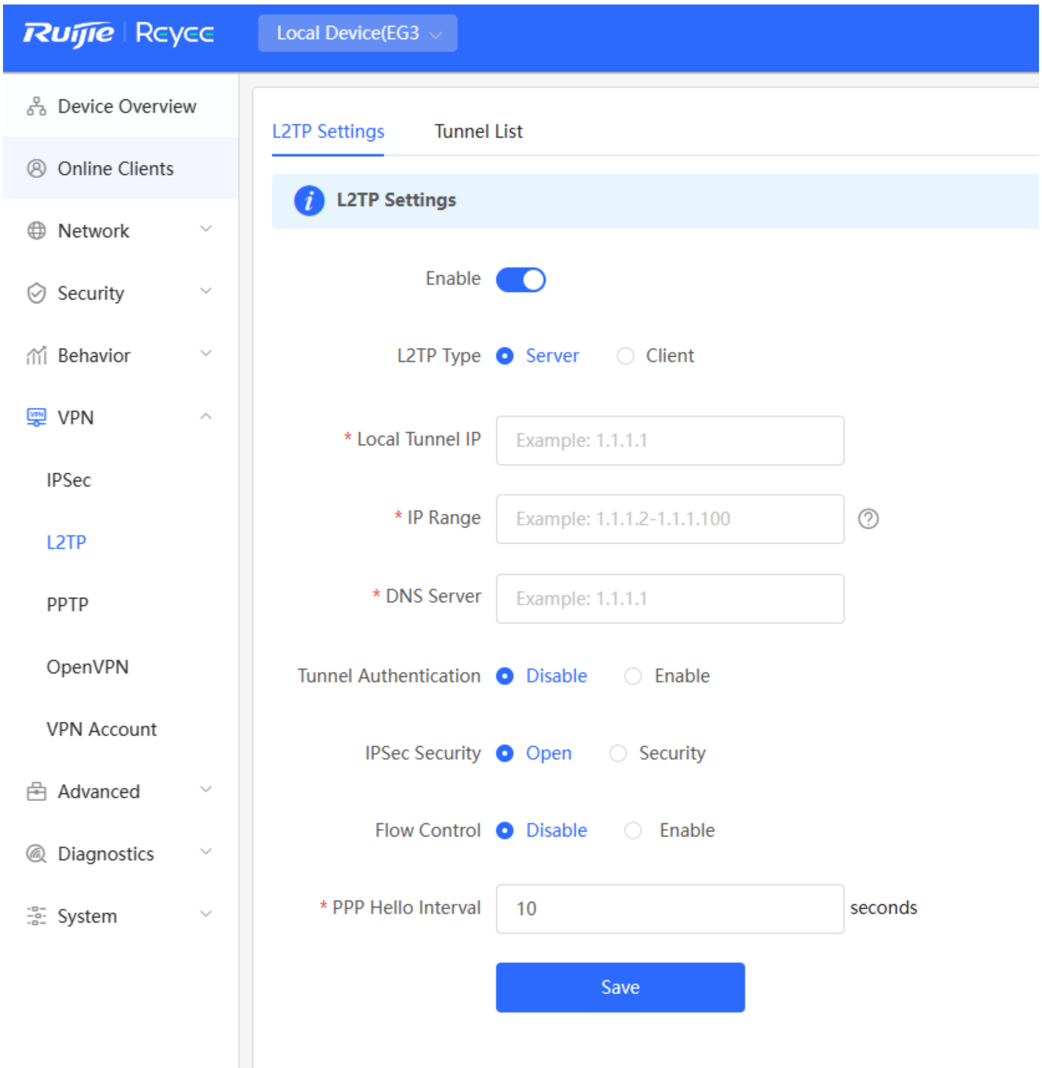
4. Configuration Steps

(1) Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

a Log in to the web management system and choose **VPN** > **L2TP** > **L2TP Settings** to access the L2TP Settings page.



L2TP Settings

Enable: ●

L2TP Type: ● Server ○ Client

* Local Tunnel IP: Example: 1.1.1.1

* IP Range: Example: 1.1.1.2-1.1.1.100

* DNS Server: Example: 1.1.1.1

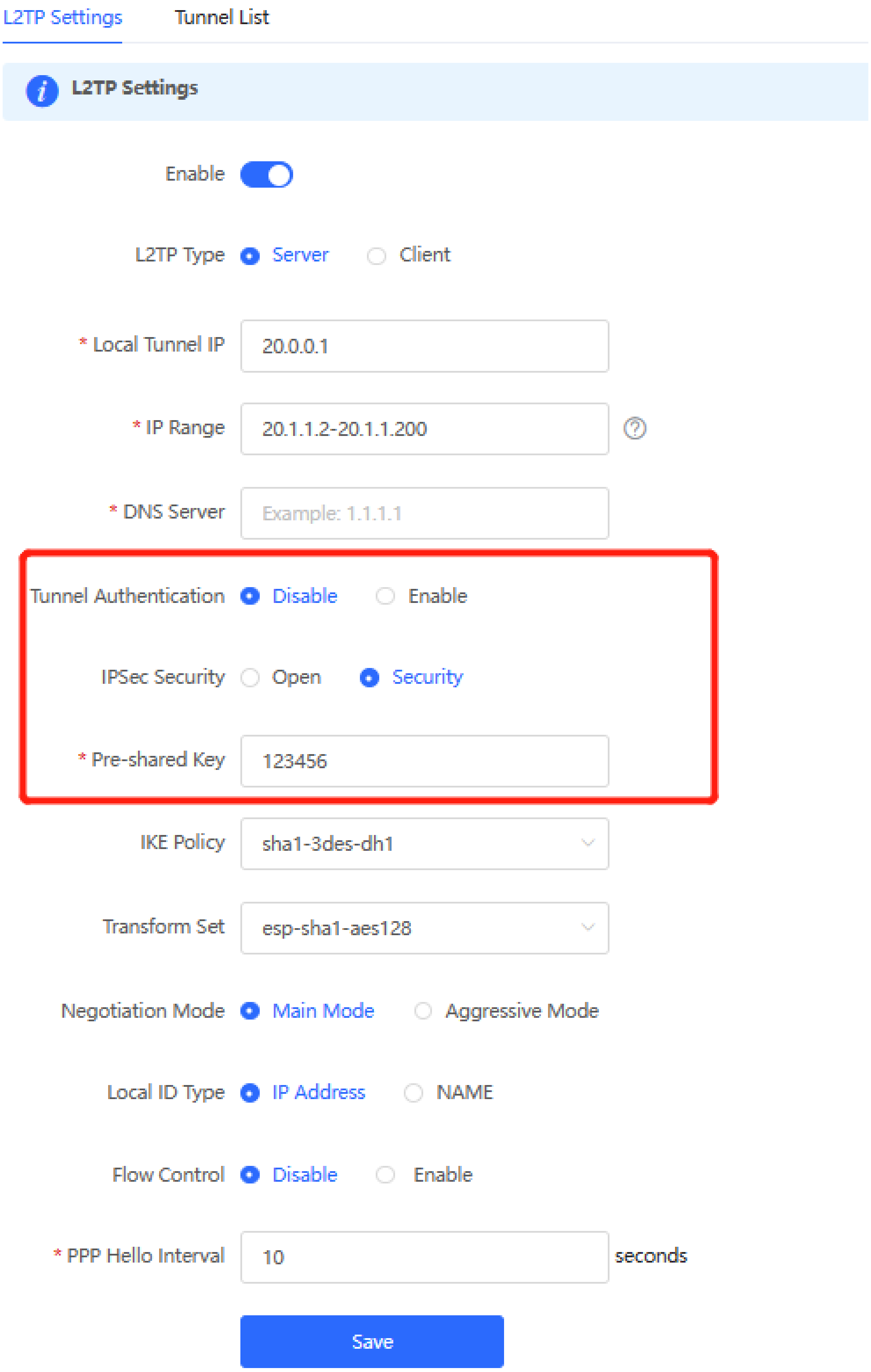
Tunnel Authentication: ● Disable ○ Enable

IPSec Security: ● Open ○ Security

Flow Control: ● Disable ○ Enable

* PPP Hello Interval: 10 seconds

b Turn on the L2TP function, set L2TP Type to Server, enter the local tunnel address, address pool IP address range, and DNS server address, specify whether to enable IPsec encryption and tunnel authentication, and click Save.



L2TP Settings | Tunnel List

L2TP Settings

Enable: ●

L2TP Type: ● Server ○ Client

* Local Tunnel IP: 20.0.0.1

* IP Range: 20.1.1.2-20.1.1.200

* DNS Server: Example: 1.1.1.1

Tunnel Authentication: ● Disable ○ Enable

IPSec Security: ○ Open ● Security

* Pre-shared Key: 123456

IKE Policy: sha1-3des-dh1

Transform Set: esp-sha1-aes128

Negotiation Mode: ● Main Mode ○ Aggressive Mode

Local ID Type: ● IP Address ○ NAME

Flow Control: ● Disable ○ Enable

* PPP Hello Interval: 10 seconds

Table 5-11 L2TP server configuration

Parameter	Description
Local Tunnel IP	Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address.
IP Range	Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients.
DNS Server	Enter an available DNS server address.
Tunnel Authentication	By default, tunnel authentication is disabled. After this function is enabled, the server and client can be connected only when they use the same tunnel key. You can keep tunnel authentication disabled.
IPsec Security	Specify whether to encrypt the L2TP tunnel using the IPsec protocol. You are advised to select **Security** to guarantee data security. If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first.
Pre-shared Key	Enter the key for IPsec authentication. The client can access the server only when the same pre-shared key is configured on the client.
IKE Policy Transform Set Negotiation Mode Local ID Type Local ID	Keep the default settings unless otherwise specified.
PPP Hello Interval	Keep the default settings unless otherwise specified.

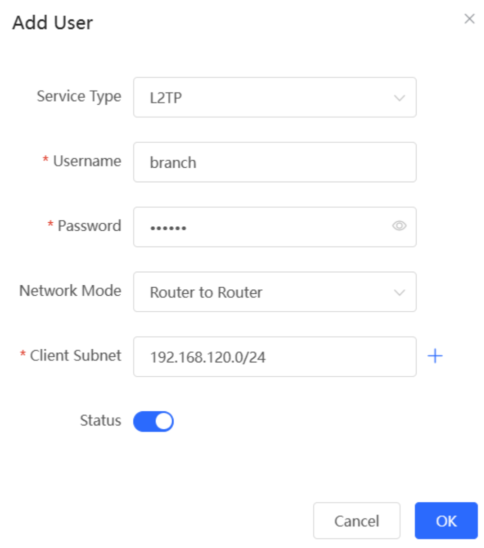
c Choose **VPN** > **VPN Account** and add L2TP user accounts for the traveling employee and branch employee to access the HQ.

For the traveling employee account, set **Network Mode** to **PC to Router**.

For the branch employee account, set **Network Mode** to **Router to Router** and **Peer Subnet** to the LAN network segment of the branch gateway, which is 192.168.120.0/24.

Caution

The LAN network segments of the server and client cannot overlap.



Add User

Service Type: L2TP

* Username: branch

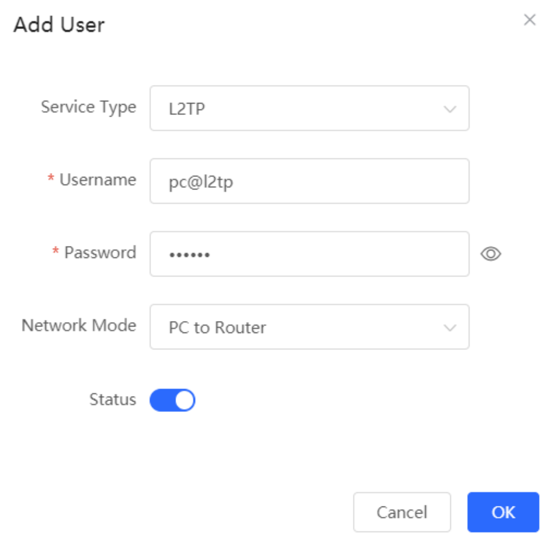
* Password: ••••••

Network Mode: Router to Router

* Client Subnet: 192.168.120.0/24

Status: On

Cancel OK



Add User

Service Type: L2TP

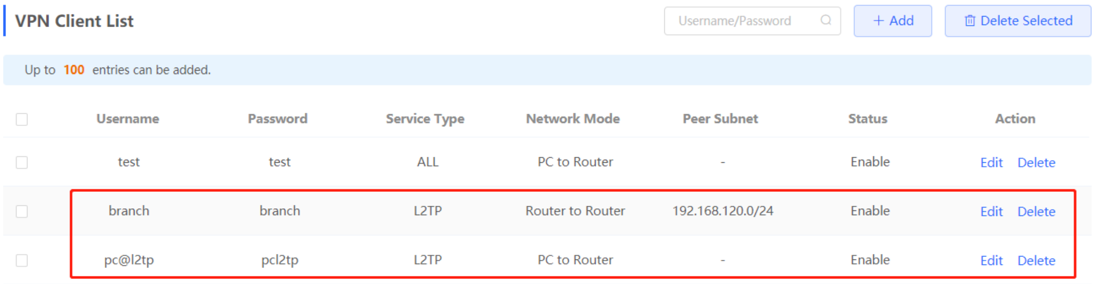
* Username: pc@l2tp

* Password: ••••••

Network Mode: PC to Router

Status: On

Cancel OK



VPN Client List

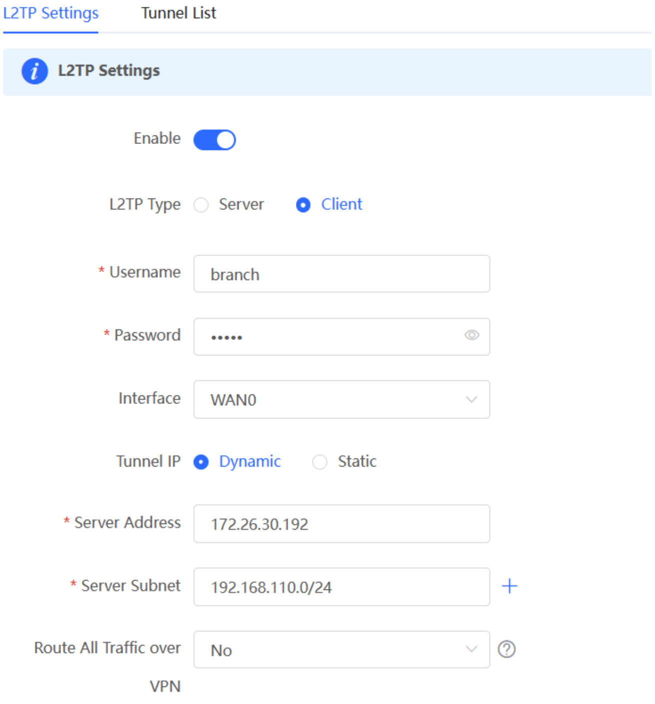
Up to 100 entries can be added.

□	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
□	test	test	ALL	PC to Router	-	Enable	Edit Delete
□	branch	branch	L2TP	Router to Router	192.168.120.0/24	Enable	Edit Delete
□	pc@l2tp	pcl2tp	L2TP	PC to Router	-	Enable	Edit Delete

(2) Configure the branch gateway.

a Log in to the web management system and access the L2TP Settings page.

b Turn on the L2TP function, set L2TP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.



L2TP Settings | Tunnel List

L2TP Settings

Enable: On

L2TP Type: ○ Server ● Client

* Username: branch

* Password: •••••

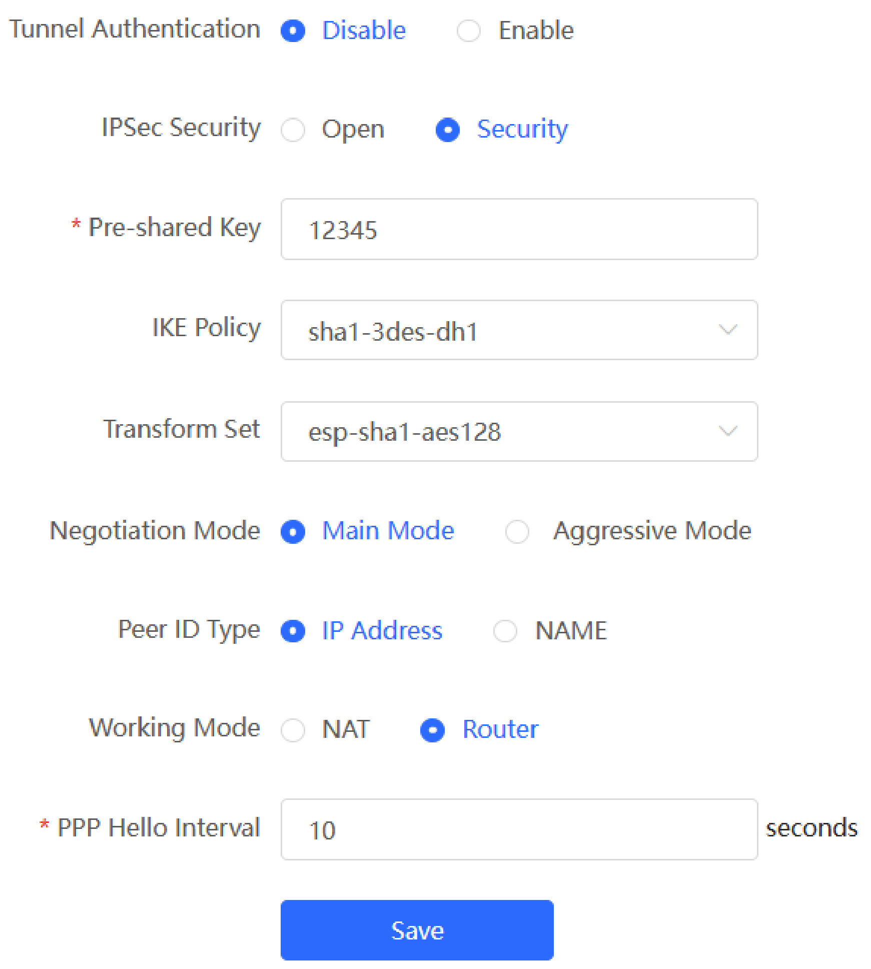
Interface: WAN0

Tunnel IP: ● Dynamic ○ Static

* Server Address: 172.26.30.192

* Server Subnet: 192.168.110.0/24

Route All Traffic over VPN: No



Tunnel Authentication ● Disable ○ Enable

IPSec Security ○ Open ● Security

* Pre-shared Key 12345

IKE Policy sha1-3des-dh1

Transform Set esp-sha1-aes128

Negotiation Mode ● Main Mode ○ Aggressive Mode

Peer ID Type ● IP Address ○ NAME

Working Mode ○ NAT ● Router

* PPP Hello Interval 10 seconds

Table 5-12 L2TP client configuration

Parameter	Description
Username/Password	Enter the username and password configured on the server.
Interface	Select the WAN port on the client to establish a tunnel with the server.
Tunnel IP	Select **Dynamic** to automatically obtain the tunnel IP address. You can also select Static and enter an IP address in the address pool of the server.
Server Address	Enter the WAN port address of the server, which is 172.26.30.192.
Server Subnet	Enter the LAN network segment (LAN port IP address range) of the server, which is 192.168.110.0/24.
Tunnel Authentication	The value must be the same as that on the server. In this example, you need to disable tunnel authentication.

Parameter	Description
IPsec Security	The value must be the same as that on the server. In this example, you need to set this parameter to **Security**.
Pre-shared Key	Enter the pre-shared key configured on the server.
IKE Policy Transform Set Negotiation Mode Peer ID Type Peer ID	The settings must be the same as those on the server. Set **Peer ID Type** to the same value as that of **Local ID Type** on the server.
Working Mode	If the HQ wants to access the LAN of the branch, set this parameter to **Router**.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. Keep the default settings.

(3) Configure the PC of the traveling employee.

Note

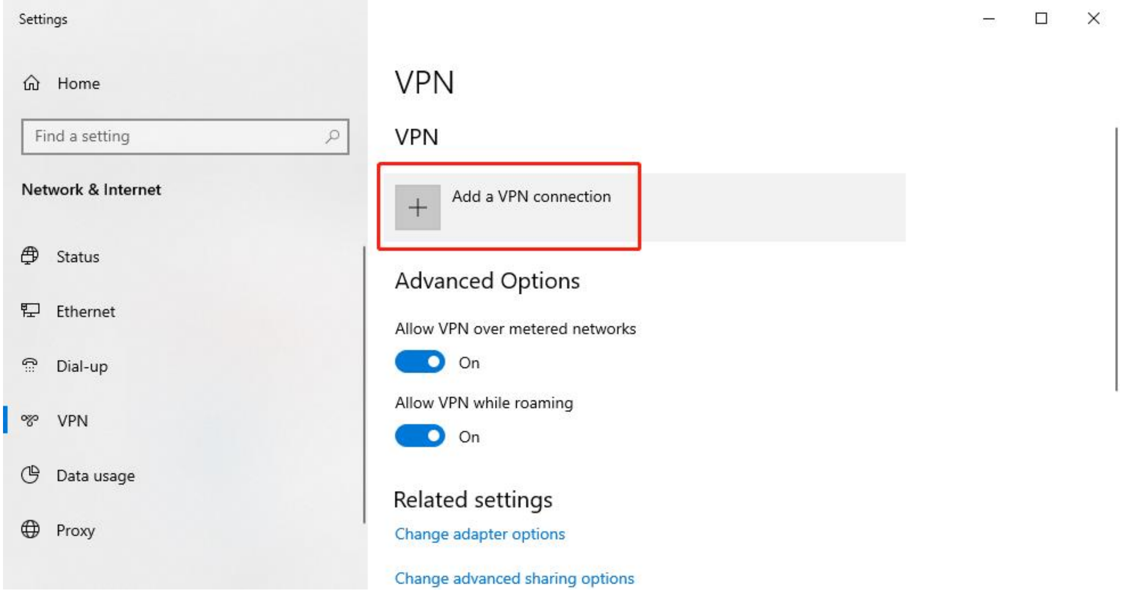
Configure the PC of a traveling employee as the L2TP client. The following uses the PC running Windows 10 operating system as an example.

The Windows XP (shorted as XP) system and Windows 7/Windows 10 (shorted as Win7/10) system differ in their support for L2TP VPN: To enable L2TP VPN in the XP system, you need to modify the service registries. L2TP is supported in the Win7/10 system by default, without the need to modify registries.

Neither the Win7/Win10 system nor the XP system supports L2TP tunnel authentication. Therefore, tunnel authentication must be disabled on the server.

Apple mobile phones support L2TP over IPsec but do not support IPsec encryption for L2TP dial-up.

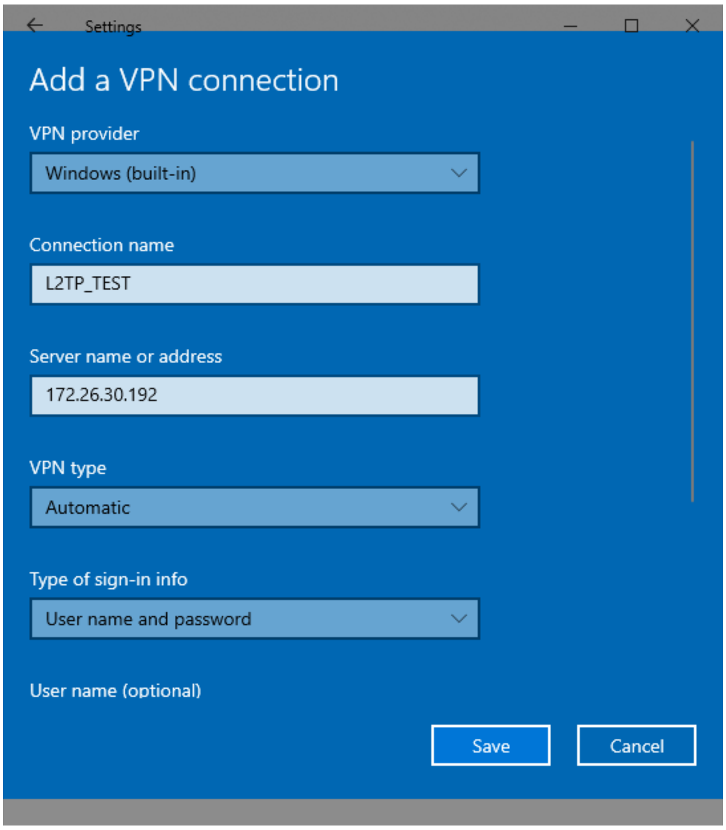
a Choose **Settings** > **Network & Internet** > **VPN** to access the VPN page.



Allow VPN over metered networks: On

Allow VPN while roaming: On

b Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows**, enter the connection name and server address or domain name, and click **Save**.



VPN provider: Windows (built-in)

Connection name: L2TP_TEST

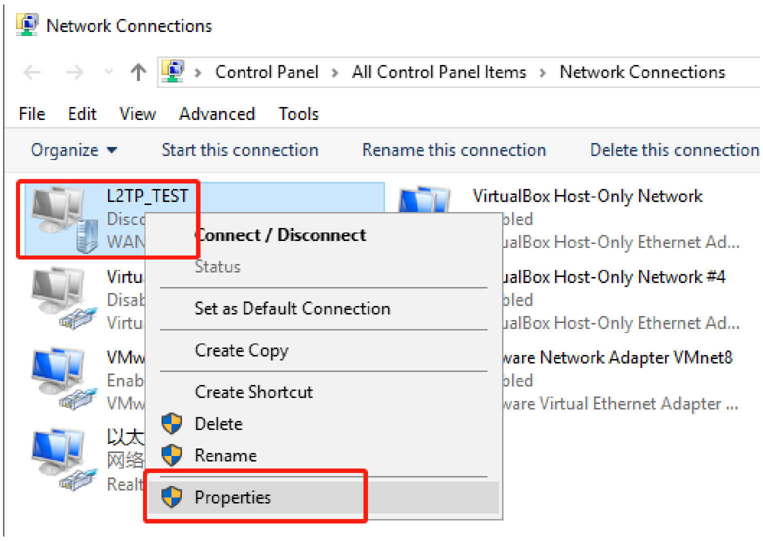
Server name or address: 172.26.30.192

VPN type: Automatic

Type of sign-in info: User name and password

User name (optional)

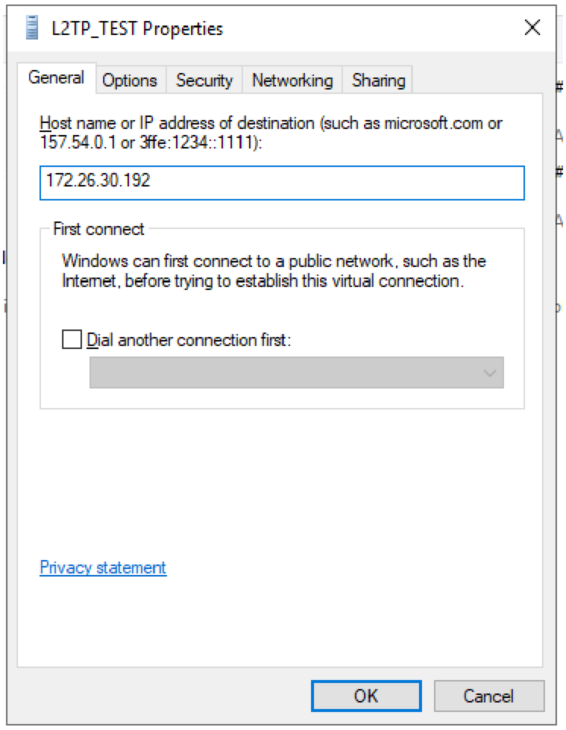
c Right-click the created VPN connection named **L2TP_TEST** and select Properties to view the properties of the network connection.


Network Connections
Control Panel > All Control Panel Items > Network Connections
File Edit View Advanced Tools
Organize Start this connection Rename this connection Delete this connection
L2TP_TEST
Disco
WAN
Virtu
Disab
Virtu
VMw
Enab
VMw
以太
网络
Realt
VirtualBox Host-Only Network
bled
ualBox Host-Only Ethernet Ad...
ualBox Host-Only Network #4
bled
ualBox Host-Only Ethernet Ad...
vare Network Adapter VMnet8
bled
vare Virtual Ethernet Adapter ...
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties

d In the dialog box that appears, click the **Security tab**, and set **Type of VPN** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** and **Data encryption** to **Optional encryption (connect even if no encryption)**.

If IPsec encryption is not enabled on the L2TP server, select **Unencrypted password (PAP)** and click **OK**. Skip Step e .

If IPsec encryption is enabled on the L2TP server, perform Step e .


L2TP_TEST Properties

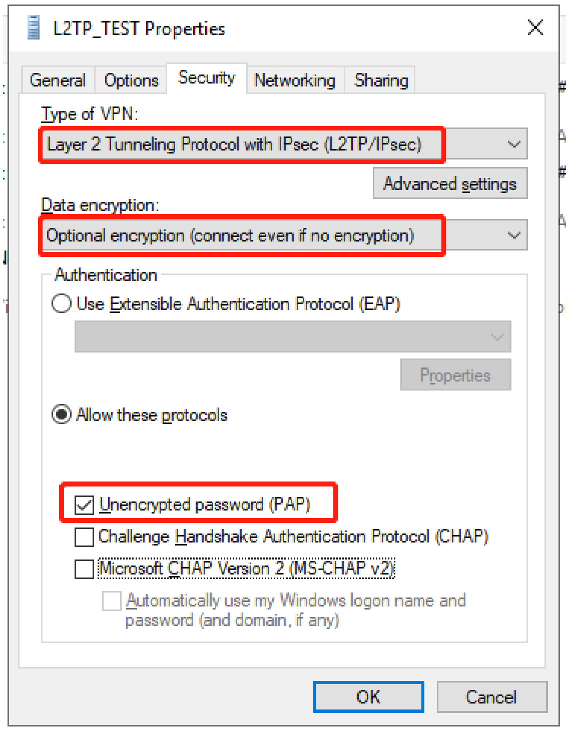
Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

172.26.30.192

First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

□ Dial another connection first:



L2TP_TEST Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Advanced settings

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

☑ Unencrypted password (PAP)

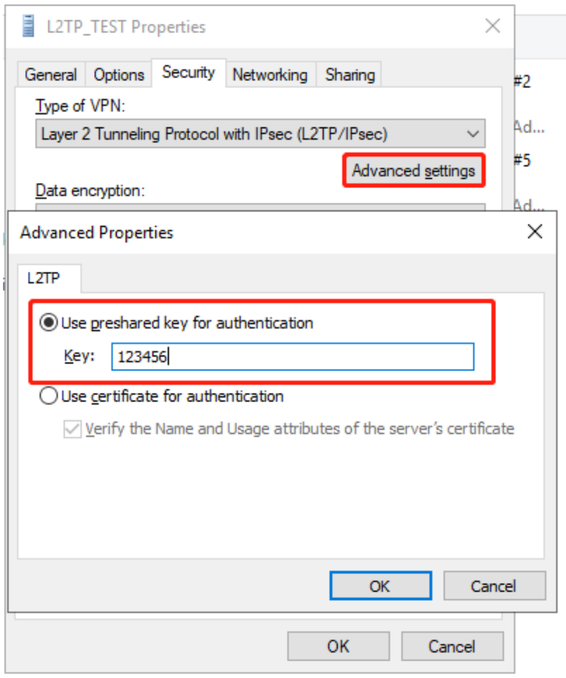
□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

OK Cancel

e If IPsec encryption is enabled on the server, select **CHAP** and **MS-CHAP v2** as the identity authentication protocols and click **Advanced settings**. In the dialog box that appears, configure the pre-shared key the same as that on the server. After completing the configuration, click **OK**.



L2TP_TEST Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Advanced settings

Data encryption:

Advanced Properties

L2TP

● Use preshared key for authentication

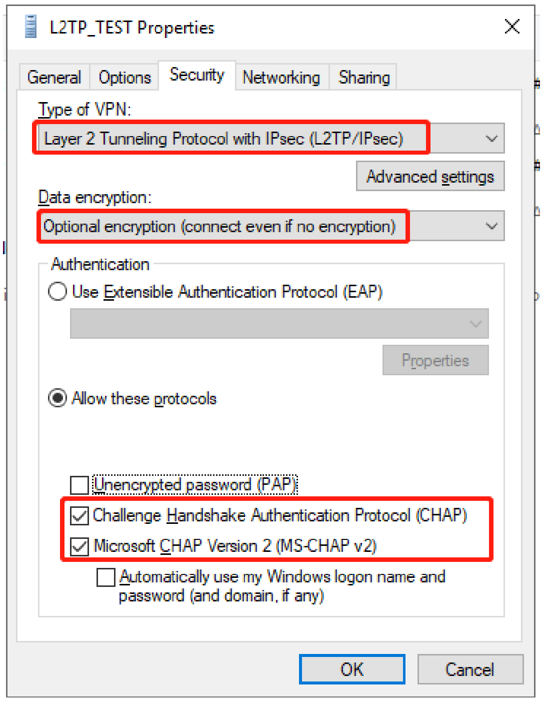
Key: 123456

○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate

OK Cancel

OK Cancel



L2TP_TEST Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Advanced settings

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

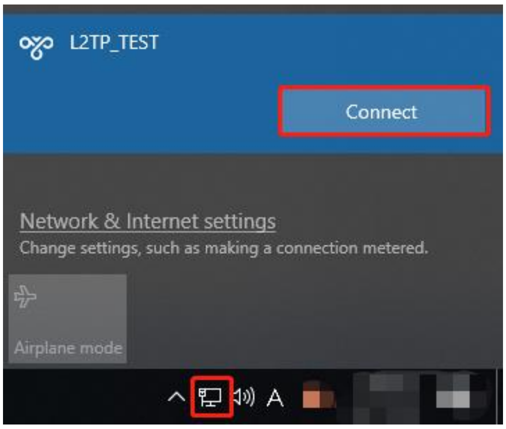
□ Automatically use my Windows logon name and password (and domain, if any)

OK Cancel

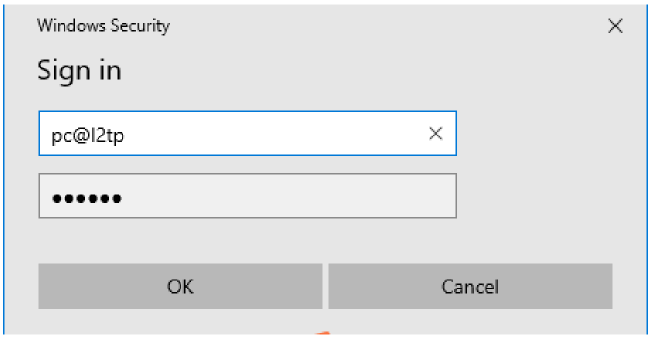
Note

The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

f After the L2TP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon 🖳 in the task bar, select the created L2TP VPN connection, and click Connect. In the dialog box that appears, enter the username and password configured on the server.



L2TP_TEST
Connect
Network & Internet settings
Change settings, such as making a connection metered.
Airplane mode



Windows Security

Sign in

pc@l2tp

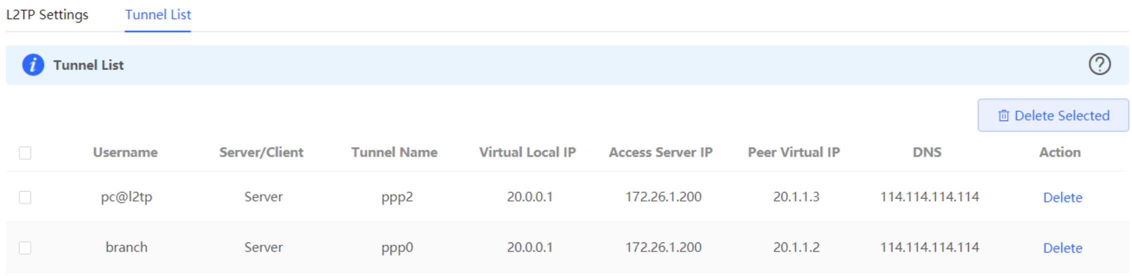
••••••

OK Cancel

5. Verifying Configuration

(1) After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:



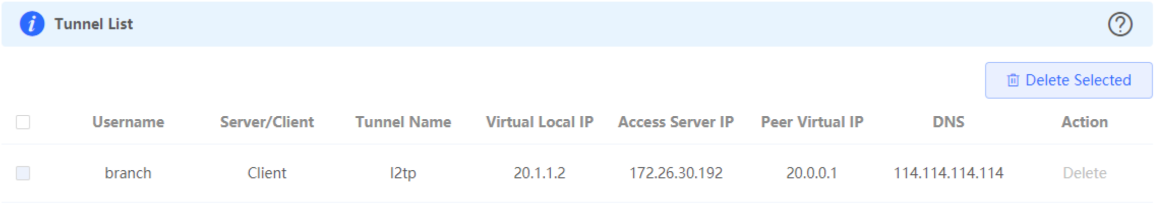
L2TP Settings | Tunnel List

Tunnel List

🗑 Delete Selected

□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	pc@l2tp	Server	ppp2	20.0.0.1	172.26.1.200	20.1.1.3	114.114.114.114	Delete
□	branch	Server	ppp0	20.0.0.1	172.26.1.200	20.1.1.2	114.114.114.114	Delete

Branch:

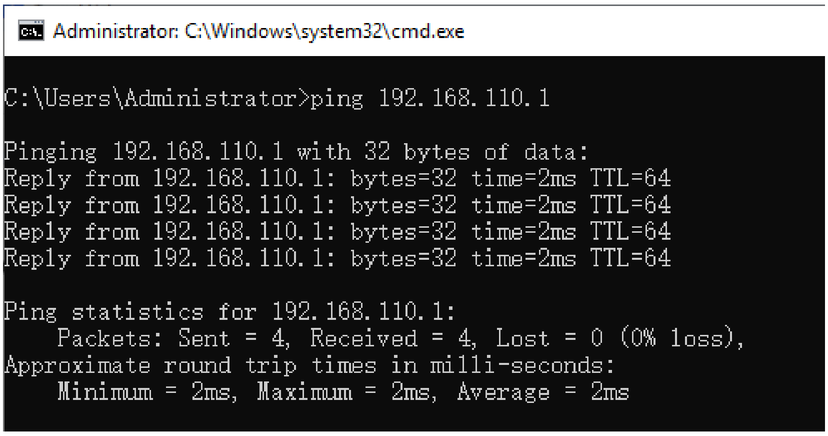


Tunnel List

🗑 Delete Selected

□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	branch	Client	l2tp	20.1.1.2	172.26.30.192	20.0.0.1	114.114.114.114	Delete

(2) Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.



Administrator: C:\Windows\system32\cmd.exe

```
C:\Users\Administrator>ping 192.168.110.1

Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

5.2.6 Solution to L2TP VPN Connection Failure

(1) Run the ping command to test the connectivity between the client and server. For details, see Section4.4.3 Network Tools. If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.

(2) Choose **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section 4.4.3 Network Tools.

(3) Check whether the username and password used by the client are the same as those configured on the server.

(4) Check whether the WAN port IP address of your HQ EG is a public network IP address. If not, you need to configure DMZ on your egress gateway.

5.3 Configuring PPTP VPN

5.3.1 Overview

Point-to-Point Tunneling Protocol (PPTP) is an enhanced security protocol designed based on the Point-to-Point Protocol (PPP). It allows an enterprise to use private tunnels to expand its enterprise network over the public network. PPTP relies on the PPP protocol to implement security functions such as encryption and identity authentication. Generally, PPTP works with Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv1/v2), or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) for identity authentication and Microsoft Point-to-Point Encryption (MPPE) for encryption to improve security.

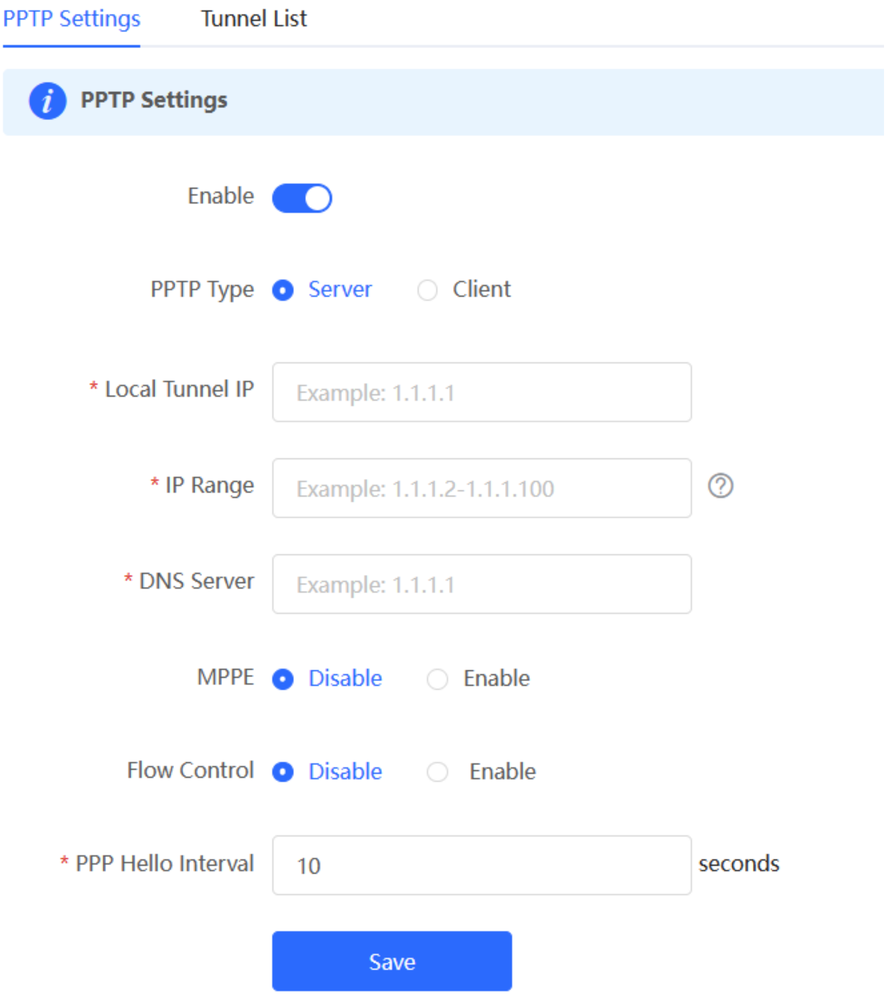
Currently, the device can be deployed as the PPTP server or client. It supports MPPE for encryption MSCHAP-v2 for identity authentication, and does not support EAP authentication.

5.3.2 Configuring the PPTP Service

1. Configuring the PPTP Server

Choose **Local Device** > **VPN** > **PPTP** > **PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Server**, configure PPTP server parameters, and click **Save**.



PPTP Settings Tunnel List

PPTP Settings

Enable: On

PPTP Type: ● Server ○ Client

* Local Tunnel IP: Example: 1.1.1.1

* IP Range: Example: 1.1.1.2-1.1.1.100

* DNS Server: Example: 1.1.1.1

MPPE: ● Disable ○ Enable

Flow Control: ● Disable ○ Enable

* PPP Hello Interval: 10 seconds

Table 5-13 PPTP server configuration

Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address.
IP Range	Specify the address pool used by the PPTP server to allocate IP addresses to clients.
DNS Server	Specify the DNS server address pushed by the PPTP server to clients.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. After MPPE is enabled on the server: If **Data encryption** is set to **Optional encryption** on the client, the server and client can be connected but the server does not encrypt packets. If **Data encryption** is set to **Require encryption** on the client, the server and client can be connected and the server encrypts packets. If **Data encryption** is set to **No encryption allowed** on the client, the server and client cannot be connected. If MPPE is disabled on the server but the client requires encryption, the server and client connection fails. By default, MPPE is disabled on the server. After you enable MPPE, the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 4.15.2 Smart Flow Control.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.

⚠ **Caution**

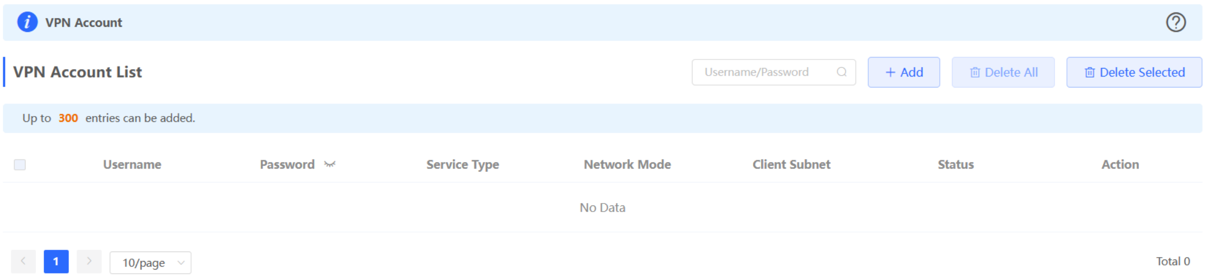
The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring PPTP User

Choose **Local Device** > **VPN** > **VPN Account**.

Only user accounts added to the VPN client list are allowed to dial up to connect to the PPTP server. Therefore, you need to manually configure user accounts for clients to access the PPTP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **PPTP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.



VPN Account

VPN Account List

Username/Password

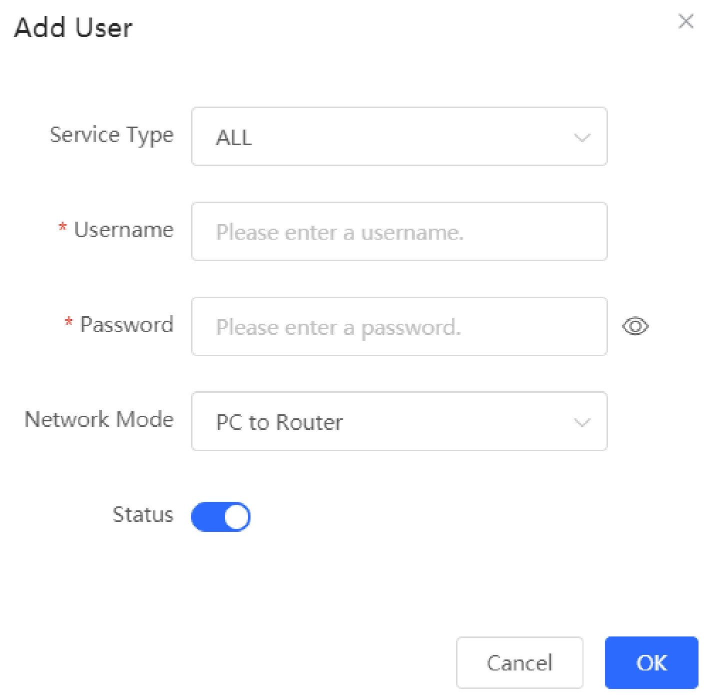
+ Add · Delete All · Delete Selected

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: ALL

* Username: Please enter a username.

* Password: Please enter a password.

Network Mode: PC to Router

Status: ●

Cancel · OK

Table 5-14 PPTP user configuration

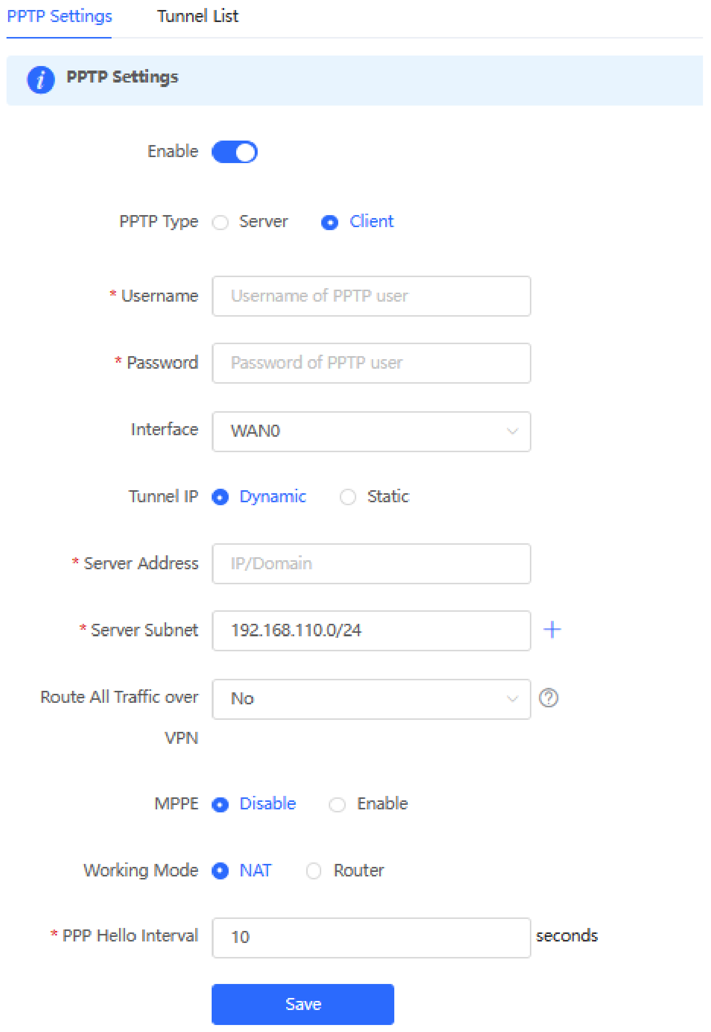
Parameter	Description
Username/Password	Specify the name and password of the PPTP user allowed to dial up to connect to the PPTP server. The username and password are used to establish a connection between the server and client.
Network Mode	● PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. ● Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up.

Parameter	Description
Client Subnet	Specify the IP address range used by the LAN on the peer end of the PPTP tunnel. Generally, the peer subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.) For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router. Note: When the Network Mode is set to Router to Router, you can click + to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.
Status	Specify whether to enable the user account.

5.3.3 Configuring the PPTP Client

Choose **Local Device** > **VPN** > **PPTP** > **PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Client**, configure PPTP client parameters, and click **Save**.



PPTP Settings

Enable: On

PPTP Type: ○ Server ● Client

* Username: Username of PPTP user

* Password: Password of PPTP user

Interface: WAN0

Tunnel IP: ● Dynamic ○ Static

* Server Address: IP/Domain

* Server Subnet: 192.168.110.0/24 +

Route All Traffic over VPN: No

MPPE: ● Disable ○ Enable

Working Mode: ● NAT ○ Router

* PPP Hello Interval: 10 seconds

Table 5-15 PPTP client configuration

Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the PPTP tunnel. The values must be the same as those configured on the PPTP server.
Interface	Specify the WAN port used by the client.
Tunnel IP	Specify the virtual IP address of the VPN tunnel client. If you select **Dynamic**, the client obtains an IP address from the server address pool. If you select **Static**, manually configure an idle static address within the range of the server address pool as the local tunnel IP address.
Server Address	Enter the WAN port IP address or domain name of the server. This address must be a public network IP address.
Server Subnet	Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the server.
Working Mode	NAT: The client can access the server network, but the server cannot access the client network. Router: The server can access the client network.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after a PPTP tunnel is established. You are advised to retain the default configuration.

5.3.4 Viewing the PPTP Tunnel Information

Choose **Local Device** > **VPN** > **PPTP** > **Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the PPTP tunnel establishment status.

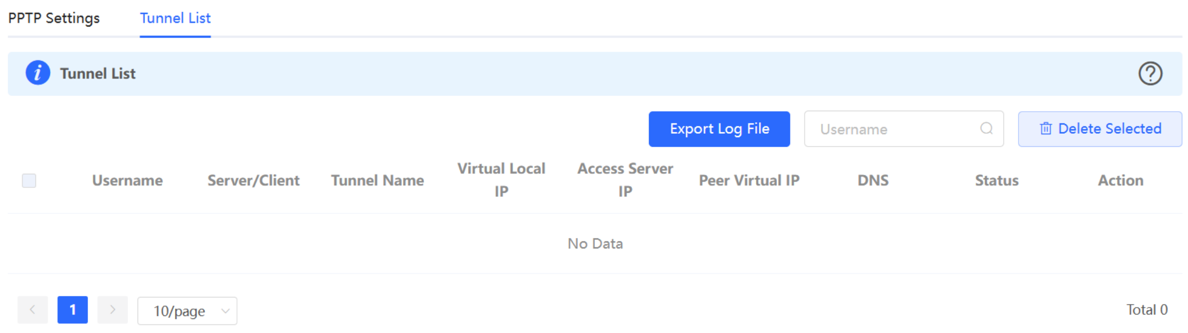


Table 5-16 PPTP tunnel information

Parameter	Description
Username	Indicate the username used by the client for identity authentication.
Server/Client	Indicate the role of the current device, which is client or server.
Tunnel Name	Indicate the name of the vNIC generated by PPTP.
Virtual Local IP	Indicate the local virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server.
Access Server IP	Indicate the real IP address of the peer connecting to the PPTP tunnel.
Peer Virtual IP	Indicate the peer virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server.
DNS	Indicate the DNS server address allocated by the PPTP server.

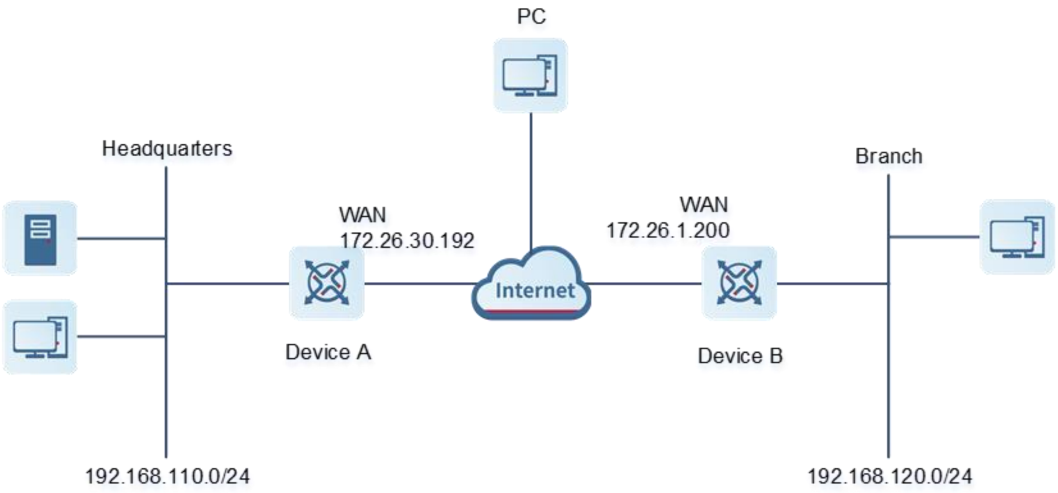
5.3.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish a PPTP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through PPTP dial-up.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the PPTP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the PPTP server.
- Configure the branch gateway Device B as the PPTP client.
- Configure the PC of the traveling employee as the PPTP client.

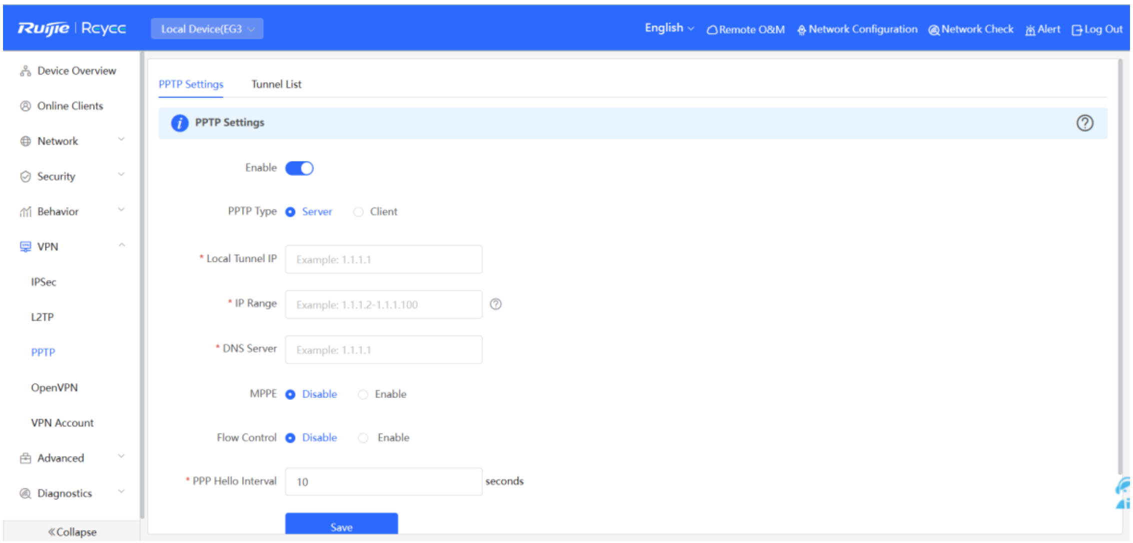
4. Configuration Steps

(1) Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

a Log in to the web management system and choose VPN > PPTP > PPTP Settings to access the PPTP Settings page.



PPTP Settings

Enable: ●

PPTP Type: ● Server ○ Client

* Local Tunnel IP: Example: 1.1.1.1

* IP Range: Example: 1.1.1.2-1.1.1.100

* DNS Server: Example: 1.1.1.1

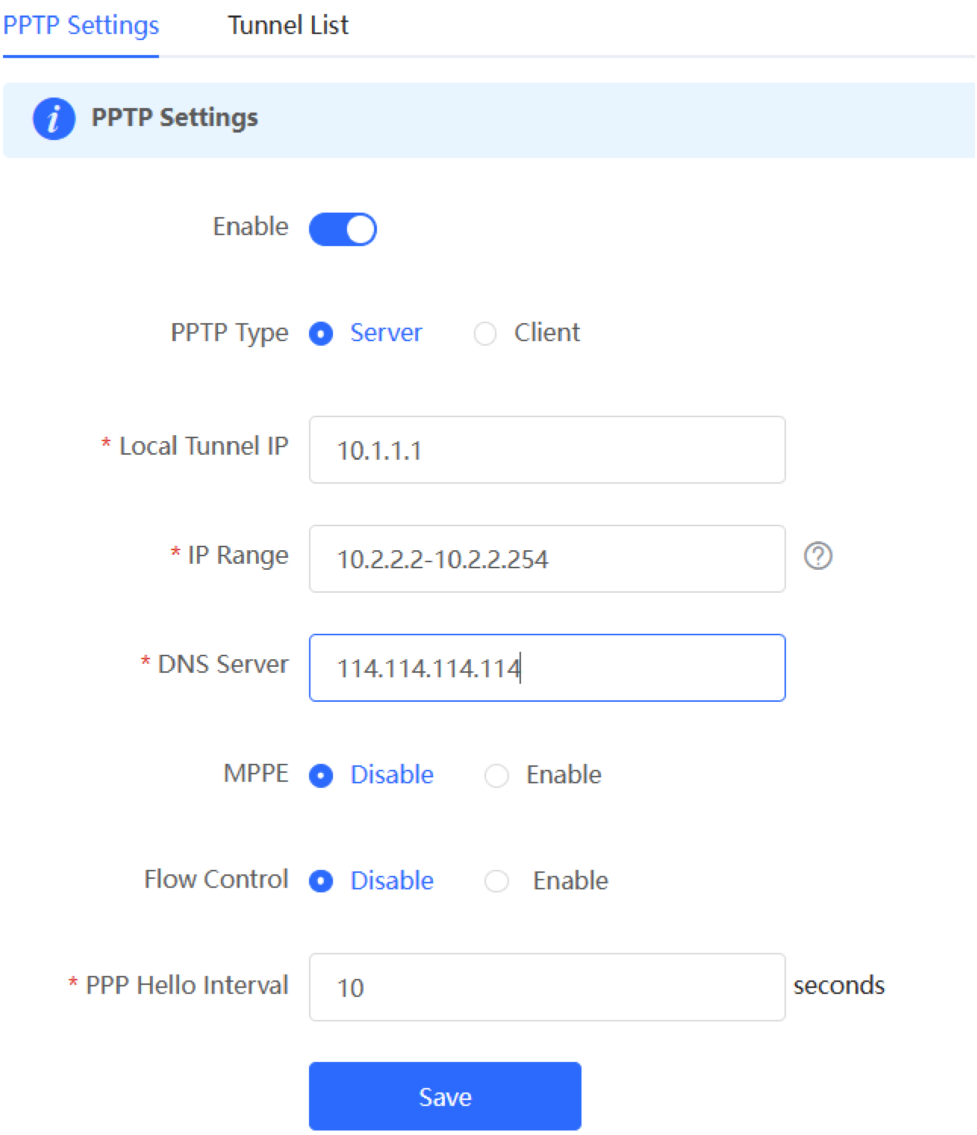
MPPE: ● Disable ○ Enable

Flow Control: ● Disable ○ Enable

* PPP Hello Interval: 10 seconds

Save

b Turn on the PPTP function, set PPTP Type to Server, enter the local tunnel address, address pool IP address range, and DNS server address, specify whether to enable MPPE encryption, and click Save.



PPTP Settings | Tunnel List

PPTP Settings

Enable: ON

PPTP Type: ● Server ○ Client

* Local Tunnel IP: 10.1.1.1

* IP Range: 10.2.2.2-10.2.2.254

* DNS Server: 114.114.114.114

MPPE: ● Disable ○ Enable

Flow Control: ● Disable ○ Enable

* PPP Hello Interval: 10 seconds

Table 5-17 PPTP server configuration

Parameter	Description
Local Tunnel IP	Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address.
IP Range	Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients.
DNS Server	Enter an available DNS server address.

Parameter	Description
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the client. After you enable MPPE, the device security is improved but the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.
Flow control	Flow control is disabled by default.
PPP Hello Interval	Keep the default settings unless otherwise specified.

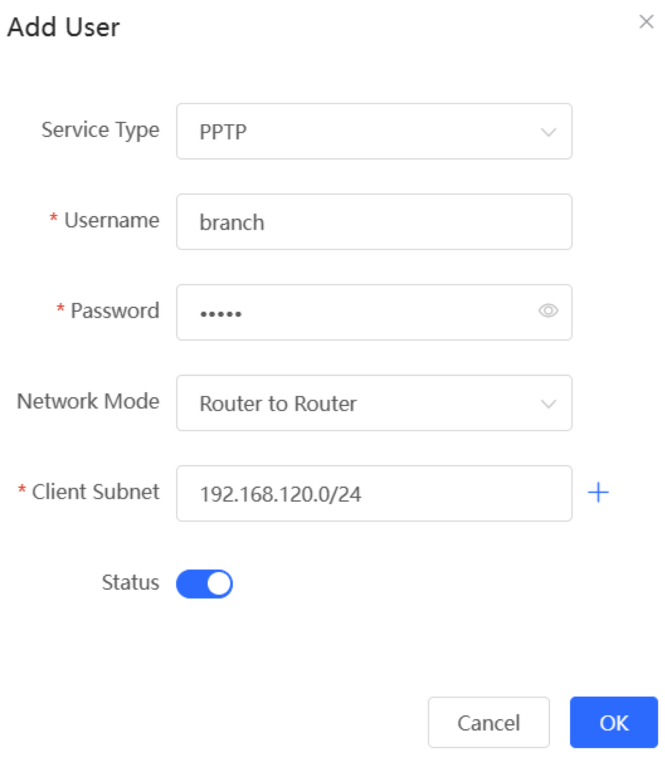
c Choose **VPN** > **VPN Account** and add PPTP user accounts for the traveling employee and branch employee to access the HQ.

For the traveling employee account, set **Network Mode** to **PC to Router**.

For the branch employee account, set **Network Mode** to **Router to Router** and C**lient Subnet** to the LAN network segment of the branch gateway.

⚠ **Caution**

The LAN network segments of the server and client cannot overlap.



Add User

Service Type: PPTP

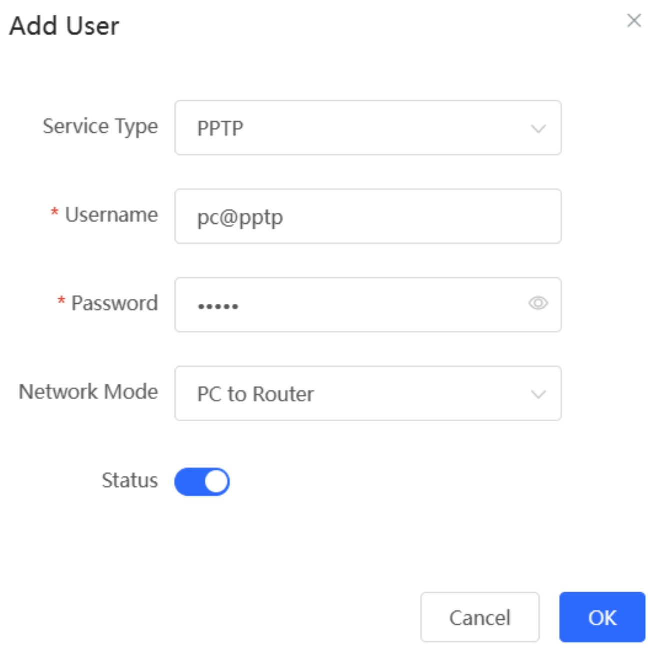
* Username: branch

* Password: •••••

Network Mode: Router to Router

* Client Subnet: 192.168.120.0/24

Status: ●



Add User

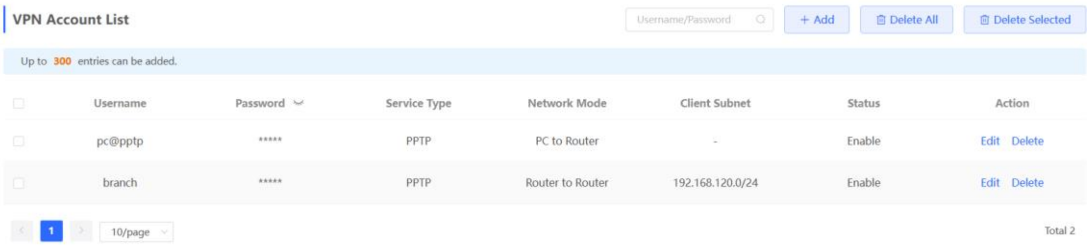
Service Type: PPTP

* Username: pc@pptp

* Password: •••••

Network Mode: PC to Router

Status: ●



VPN Account List

Up to 300 entries can be added.

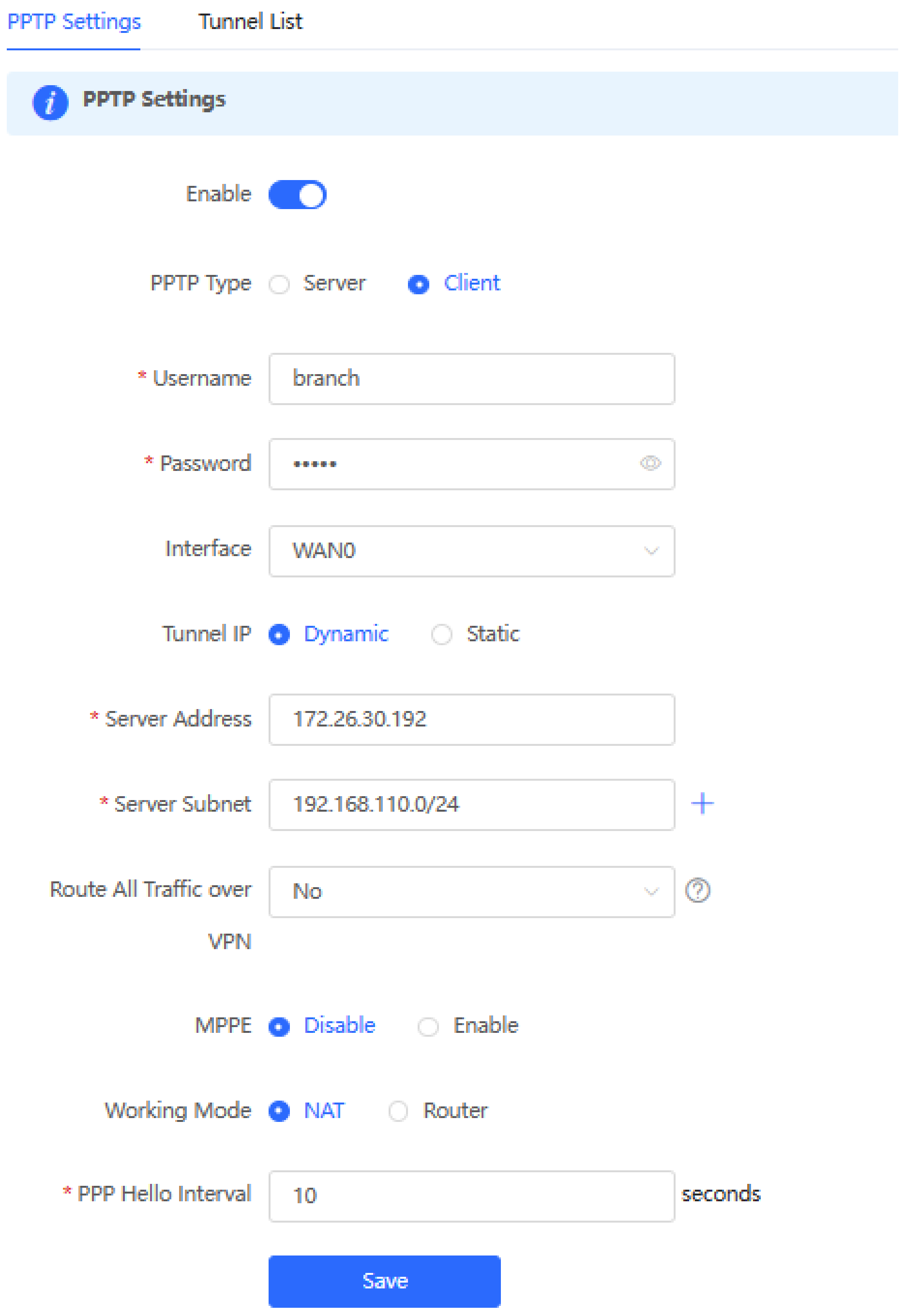
□	Username	Password	Service Type	Network Mode	Client Subnet	Status	Action
□	pc@pptp	*****	PPTP	PC to Router	-	Enable	Edit Delete
□	branch	*****	PPTP	Router to Router	192.168.120.0/24	Enable	Edit Delete

Total 2

(2) Configure the branch gateway.

a Log in to the web management system and access the PPTP Settings page.

b Turn on the PPTP function, set PPTP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.



Enable: On

PPTP Type: ○ Server ● Client

* Username: branch

* Password: •••••

Interface: WAN0

Tunnel IP: ● Dynamic ○ Static

* Server Address: 172.26.30.192

* Server Subnet: 192.168.110.0/24

Route All Traffic over VPN: No

MPPE: ● Disable ○ Enable

Working Mode: ● NAT ○ Router

* PPP Hello Interval: 10 seconds

Table 5-18 **PPTP client configuration**

Parameter	Description
Username/Password	Enter the username and password configured on the server.
Interface	Select the WAN port on the client to establish a tunnel with the server.

Parameter	Description
Tunnel IP	Select **Dynamic** to automatically obtain the tunnel IP address. You can also select **Static** and enter an IP address in the address pool of the server.
Server Address	Enter the WAN port address of the server.
Server Subnet	Enter the LAN network segment (LAN port IP address range) of the server.
MPPE	The value must be the same as that on the server.
Working Mode	If the HQ wants to access the LAN of the branch, set this parameter to **Router**.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed. Keep the default settings.

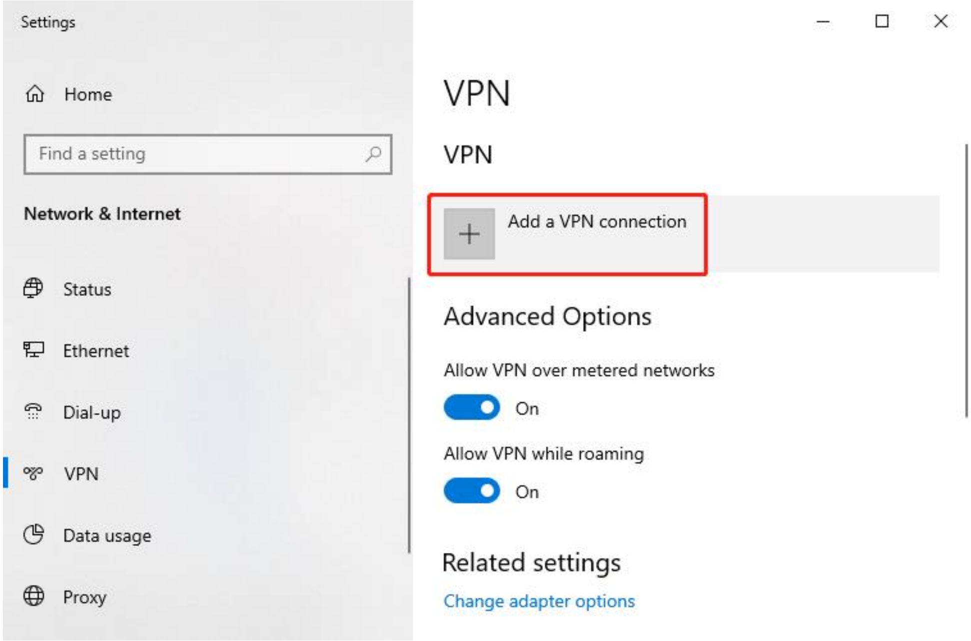
(3) Configure the PC of the traveling employee.

Note

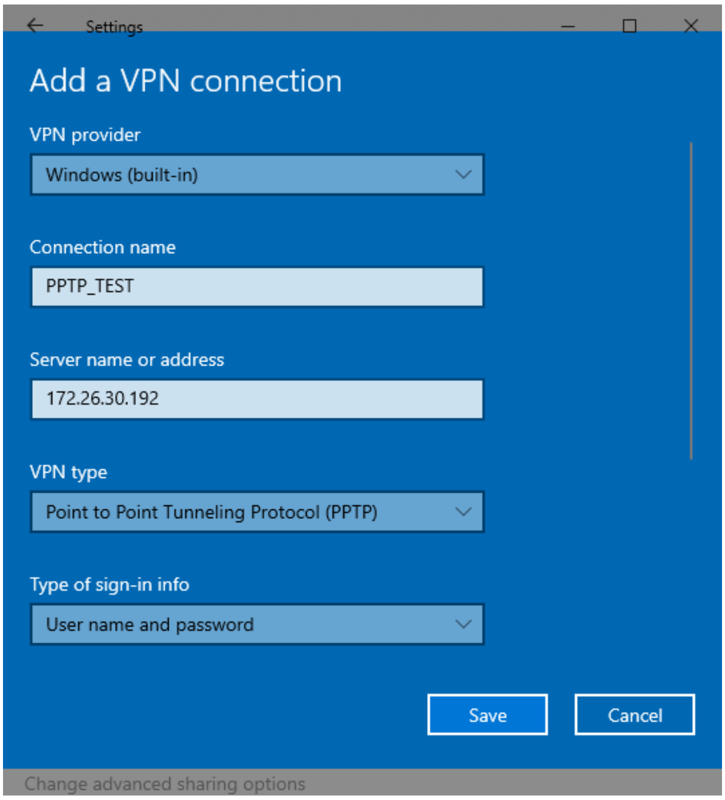
Configure the PC of a traveling employee as the PPTP client. The following uses the PC running Windows 10 operating system as an example.

Enable ports 1723 (PPTP) and 47 (GRE) on the PC firewall.

a Choose Settings > Network & Internet > VPN to access the VPN page.



b Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows** and VPN type to **Point to Point Tunneling Protocol (PPTP)**, enter the connection name and server address or domain name, and click **Save**.



Add a VPN connection

VPN provider: Windows (built-in)

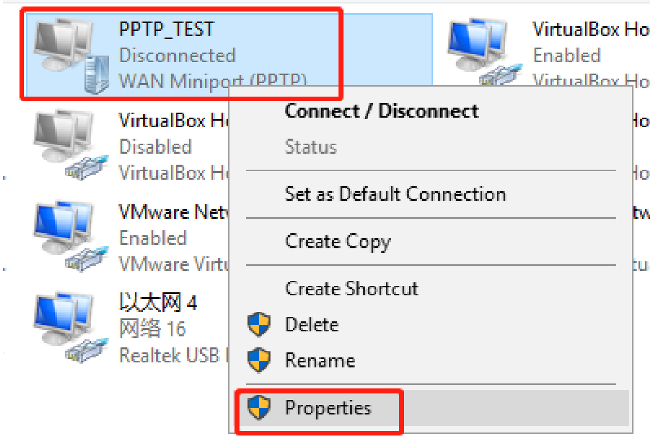
Connection name: PPTP_TEST

Server name or address: 172.26.30.192

VPN type: Point to Point Tunneling Protocol (PPTP)

Type of sign-in info: User name and password

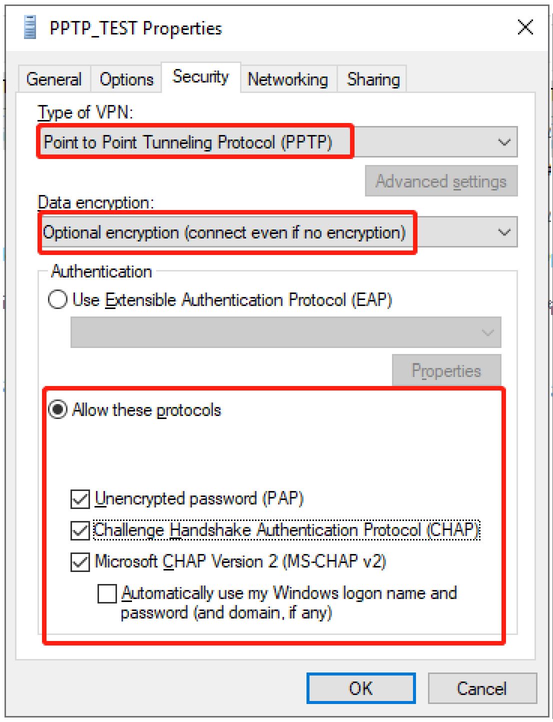
c Right-click the created VPN connection named **PPTP_TEST** and select Properties to view the properties of the network connection.



d In the dialog box that appears, click the **Security** tab.

If MPPE is not enabled on the PPTP server, set **Data encryption** to **Optional encryption** or **No encryption allowed** and use PAP, CHAP, or MS-CHAP v2 for identity authentication, as shown in the following figure on the left.

If MPPE is enabled on the PPTP server, set **Data encryption** to **Require encryption** or **Maximum strength encryption** and use MS-CHAP v2 for identity authentication, as shown in the following figure on the right.



PPTP_TEST Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Point to Point Tunneling Protocol (PPTP)

Advanced settings

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

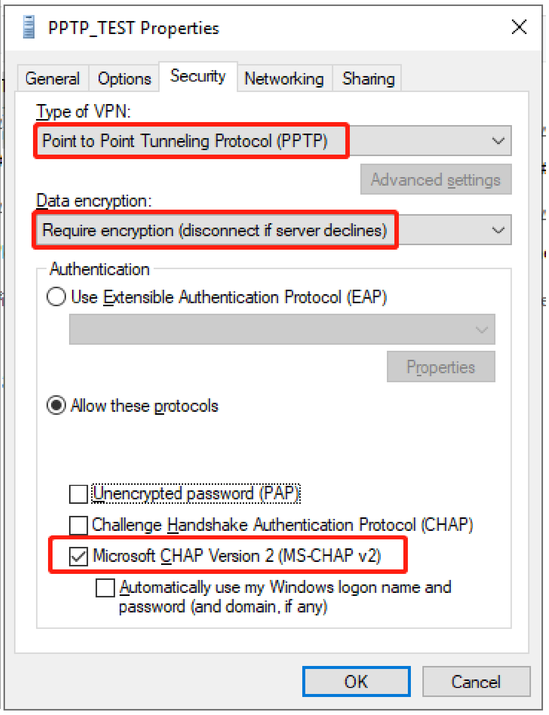
☑ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

OK Cancel



PPTP_TEST Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Point to Point Tunneling Protocol (PPTP)

Advanced settings

Data encryption:

Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

OK Cancel

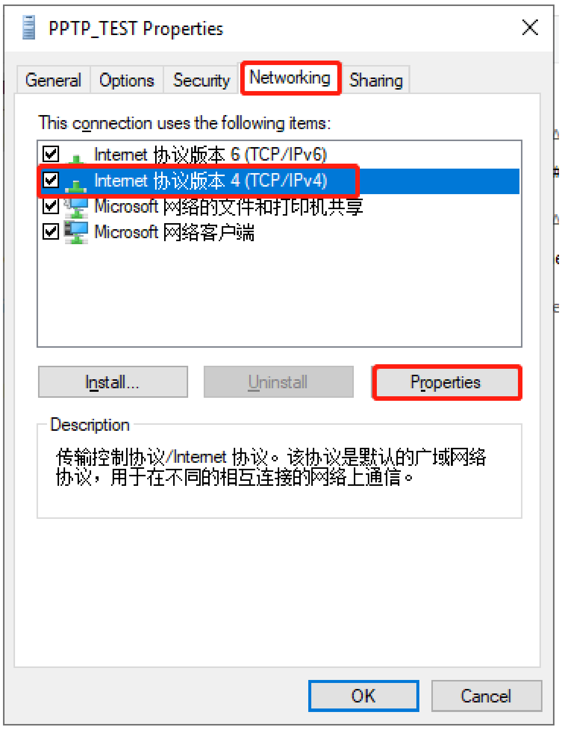
Note

The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

e When the PC functions as a dial-up client, configure the PC by using either of the following methods:

o Add a route to the VPN peer network segment on the PC as the administrator.

o In the **Properties** dialog box of the local VPN connection, select **Use default gateway on remote network**. After the VPN connection is successful, all data flows from the PC to the Internet are routed to the VPN tunnel. The following figures show the detailed configuration.

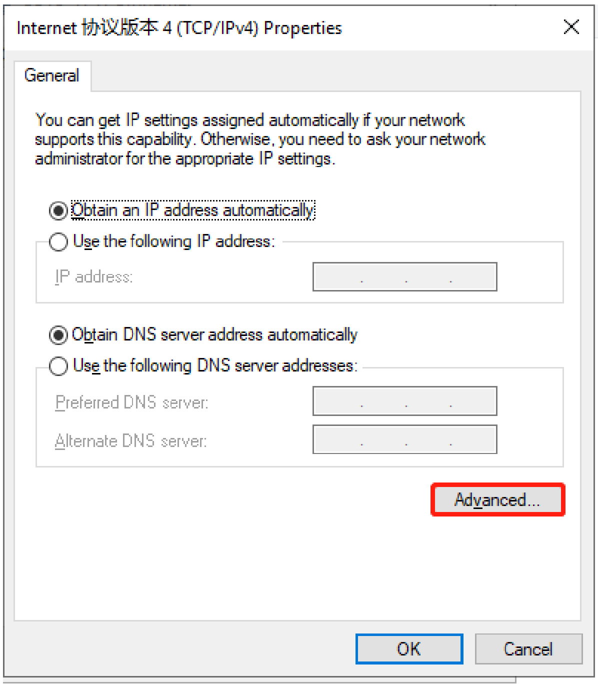


This connection uses the following items:

- ☑ Internet 协议版本 6 (TCP/IPv6)
- ☑ Internet 协议版本 4 (TCP/IPv4)
- ☑ Microsoft 网络的文件和打印机共享
- ☑ Microsoft 网络客户端

Description

传输控制协议/Internet 协议。该协议是默认的广域网络协议，用于在不同的相互连接的网络上通信。



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

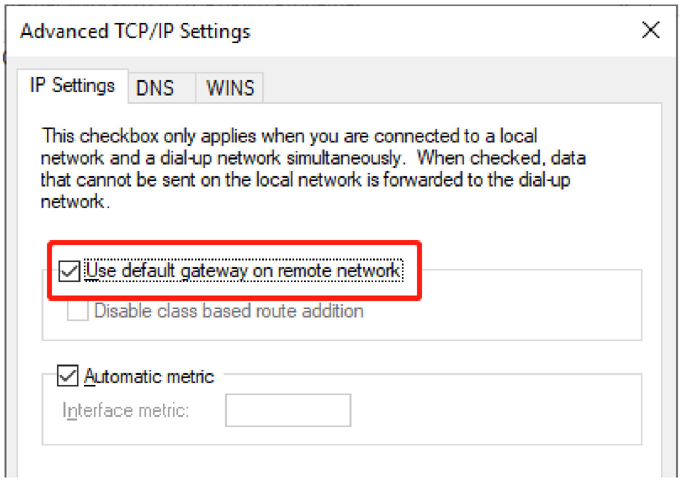
IP address: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .



Advanced TCP/IP Settings

IP Settings | DNS | WINS

This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

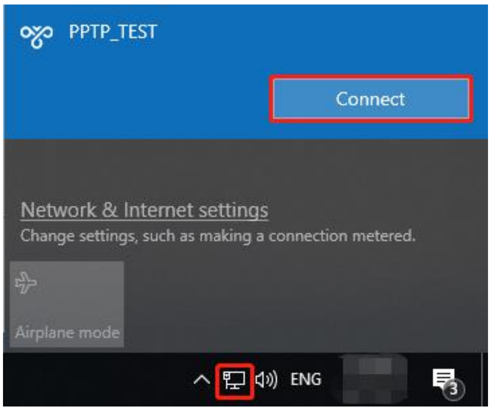
☑ Use default gateway on remote network

□ Disable class based route addition

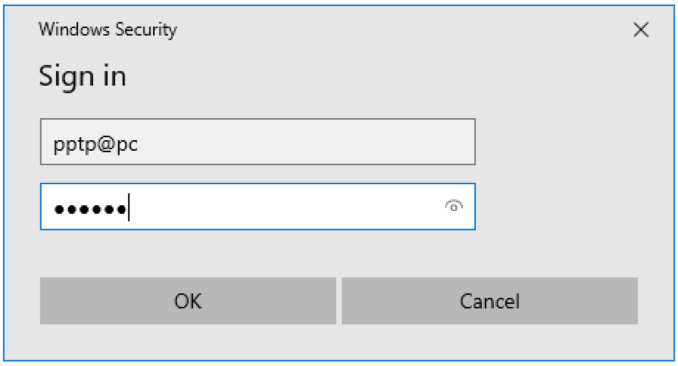
☑ Automatic metric

Interface metric:

f After the PPTP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon in the task bar, select the PPTP VPN connection, and click **Connect**. In the dialog box that appears, enter the username and password configured on the server.



PPTP_TEST
Connect
Network & Internet settings
Change settings, such as making a connection metered.
Airplane mode
ENG



Windows Security

Sign in

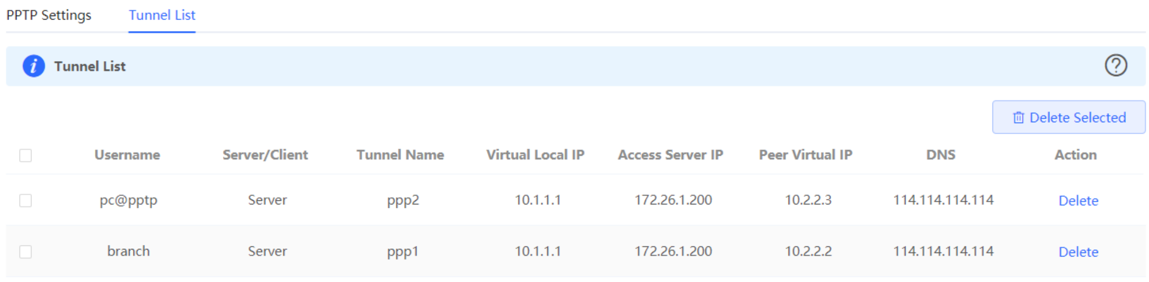
pptp@pc

••••••

5. Verifying Configuration

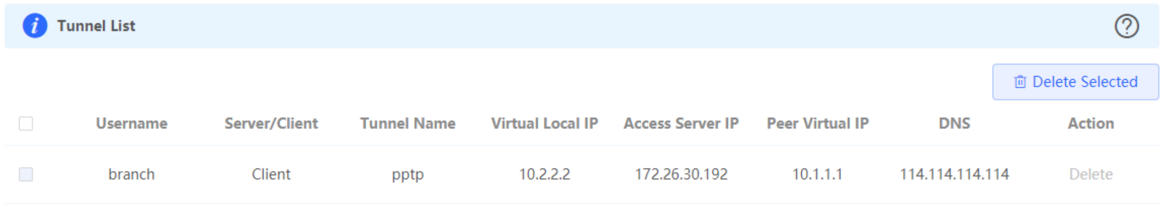
(1) After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:



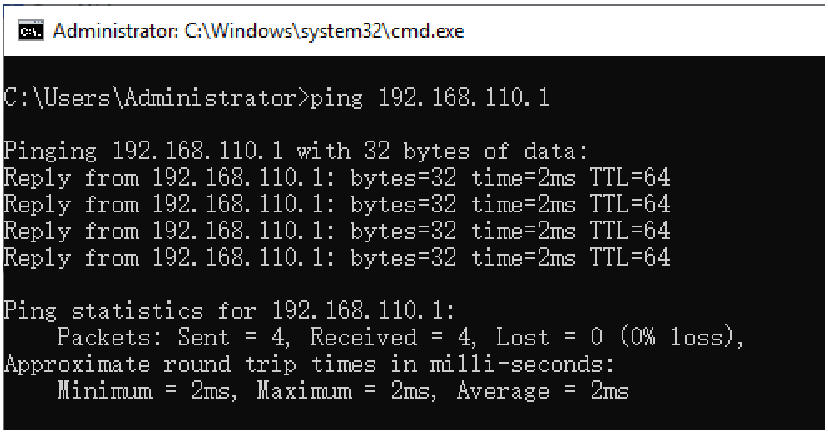
□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	pc@pptp	Server	ppp2	10.1.1.1	172.26.1.200	10.2.2.3	114.114.114.114	Delete
□	branch	Server	ppp1	10.1.1.1	172.26.1.200	10.2.2.2	114.114.114.114	Delete

Branch:



□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	branch	Client	pptp	10.2.2.2	172.26.30.192	10.1.1.1	114.114.114.114	Delete

(2) Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.



```
C:\Users\Administrator>ping 192.168.110.1

Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

5.3.6 Solution to PPTP VPN Connection Failure

(1) iPhones and other IOS devices do not support PPTP VPN. Please use L2TP VPN instead

(2) Run the ping command to test the connectivity between the client and server. For details, see Section 4.4.3 Network Tools. If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails. Check the network connection between the two EGs.

(3) Choose **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section 4.4.3 Network Tools.

(4) Check whether the username and password used by the client are the same as those configured on the server.

(5) Check whether the WAN port IP address of your HQ EG is a public network IP address. If not, please configure DMZ on your egress gateway.

5.4 Configuring OpenVPN

⚠ **Caution**

- The RG-EG105G does not support the OpenVPN function.
- IPTV connection is not supported only in the Chinese environment. To connect to IPTV in the Chinese environment, switch the system language.

5.4.1 Overview

1. OpenVPN Overview

Due to security considerations or cross-NAT communication needs, private channels need to be established between enterprises or between individual and enterprise. OpenVPN is used to establish Layer 2 or Layer 3 VPN tunnels by using the vNIC. OpenVPN supports flexible client authorization modes, supports authentication through certificate or username and password, and allows users to connect to VPN virtual interfaces through the firewall. It is easier to use than other types of VPN technologies. OpenVPN can run in the Linux, xBSD, Mac OS X, and Windows 2000/XP systems. The device can establish VPN connections to PCs, Android/Apple mobile phones, routers, and Linux devices, and it is compatible with most OpenVPN products in the market.

OpenVPN connections can traverse most proxy servers and can function well in the NAT environment. The OpenVPN server can push the following network configuration to clients: IP address, routes, and DNS settings.

2. Certificate Overview

The major advantage of OpenVPN lies in its high security, but OpenVPN security requires the support of certificates.

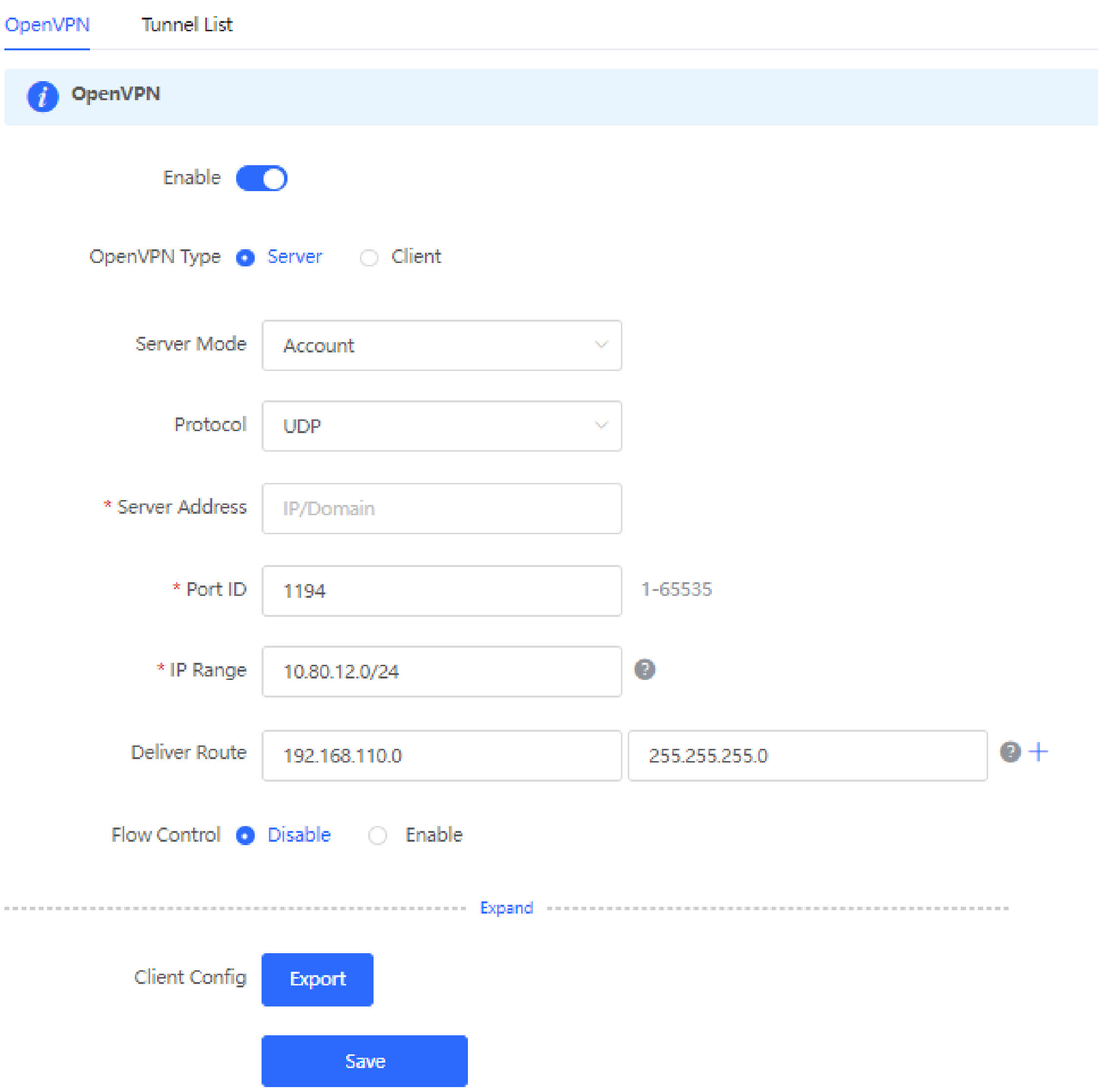
The OpenVPN client supports certificates **ca.crt**, **ca.key**, **client.crt**, and **client.key** and the OpenVPN server supports certificates **ca.crt**, **ca.key**, **server.crt**, and **server.key**.

5.4.2 Configuring the OpenVPN Server

Choose **Local Device** > **VPN** > **OpenVPN**.

1. Basic Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Server**, set other parameters, and click **Save**. After the basic settings are completed, you can view the tunnel information of the server in the tunnel list.



OpenVPN

Enable: On

OpenVPN Type: ● Server ○ Client

Server Mode: Account

Protocol: UDP

* Server Address: IP/Domain

* Port ID: 1194 1-65535

* IP Range: 10.80.12.0/24

Deliver Route: 192.168.110.0 255.255.255.0

Flow Control: ● Disable ○ Enable

Client Config: Export

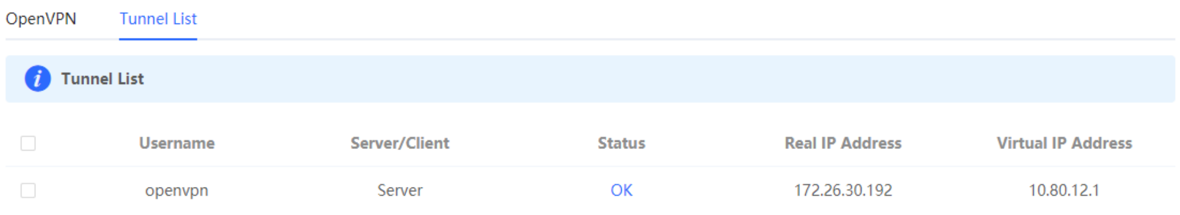
Table 5-19 OpenVPN server basic settings

Parameter	Description
Server Mode	Select a server authentication mode. The options are **Account**, **Certificate**, and **Account & Certificate**. ● Account: Enter the correct username and password and upload the CA certificate on the client to connect to the server. The configuration is simple. ● Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client to connect to the server. ● Account & Certificate: Upload the CA certificate and client certificate and enter the correct username, password, and private key. This mode is applicable to scenarios with high security requirements.

Parameter	Description
Protocol	Select a protocol for all OpenVPN communications based on a single IP port. The options are **UDP** and **TCP**. The default value is **UDP**, which is recommended. When you select a protocol, pay attention to the network status between two encrypted tunnel ends. If high latency or heavy packet loss occurs, select **TCP** as the underlying protocol.
Server Address	Specify the server address for client connection. You can set this parameter to a domain name.
Port ID	Specify the port used by the OpenVPN service process. Internet Assigned Numbers Authority (IANA) specifies port 1194 as the official port for the OpenVPN service. If the port is in use or disabled in the local network, the server log prompts port binding failure and you are asked to change the port number.
IP Range	Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to **10.80.12.0/24**, the VPN virtual address of the server is 10.80.12.1.
Deliver Route	Specify the VPN dial-up line for clients to access the LAN network segment of the server. The server informs clients that want to access the server LAN of the route information. You can configure a maximum of three routes.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 4.15.2 Smart Flow Control.
Client Config	Click **Export** to export the parameter configuration of the client connected to the server in the .tar compressed package. The decompressed information is used for setting the OpenVPN client. In account mode, the compressed package contains the configuration file **client.ovpn**, CA certificate **ca.crt**, and CA private key **ca.key**. If certificate authentication is configured, the compressed package contains the configuration file **client.ovpn**, CA certificate **ca.crt**, CA private key **ca.key**, client certificate **client.cart**, and client private key **client.key**. If TLS authentication is enabled, the compressed package contains the TLS identity authentication key **tls.key** apart from the preceding files. For details on TLS authentication, see Advanced Settings.
Server Log	Click **Export** to export server log files, including the server start time and client dial-up logs.

Caution

The IP address range of the device cannot overlap the network segment of the LAN port on the device.

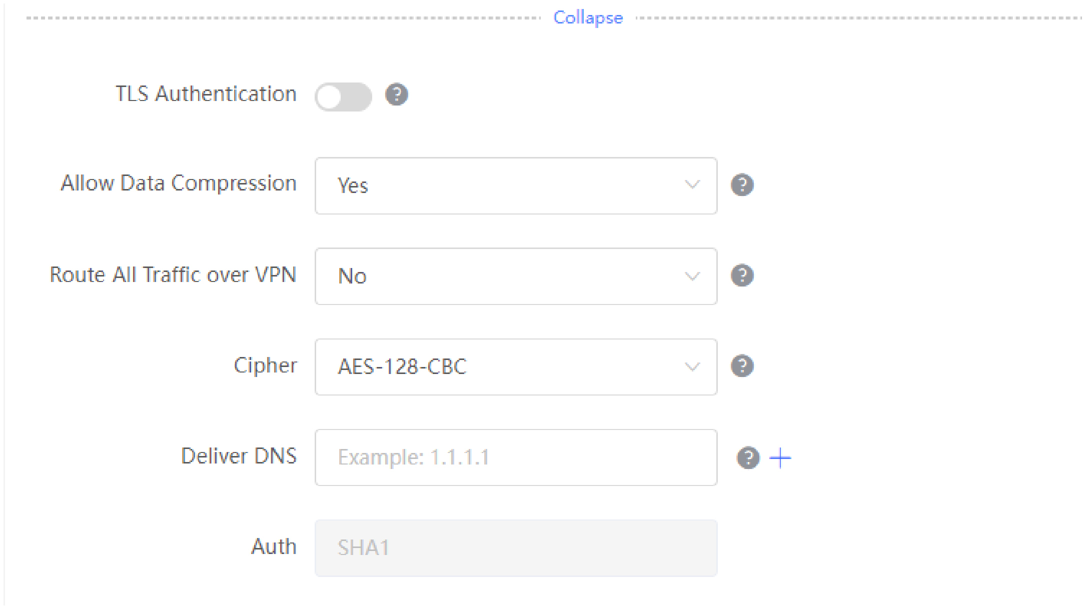


Tunnel List

□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	openvpn	Server	OK	172.26.30.192	10.80.12.1

2. Advanced Settings

Click **Expand** to configure the advanced parameters. Keep the default settings unless otherwise specified.



TLS Authentication: off

Allow Data Compression: Yes

Route All Traffic over VPN: No

Cipher: AES-128-CBC

Deliver DNS: Example: 1.1.1.1

Auth: SHA1

Table 5-20 OpenVPN server advanced settings

Parameter	Description
TLS Authentication	Specify the TLS key for enhanced OpenVPN security by allowing the communicating parties to possess the shared key before TLS handshake. After TLS authentication is enabled, you must import the TLS key on the client. (The version of the peer OpenVPN client must be higher than 2.40.)
Allow Data Compression	Specify whether to enable data compression. If this function is enabled, transmitted data is compressed using the LZO algorithm. Data compression saves bandwidth but consumes certain CPU resources. The setting on the client must be the same as that on the server. Otherwise, the connection fails.

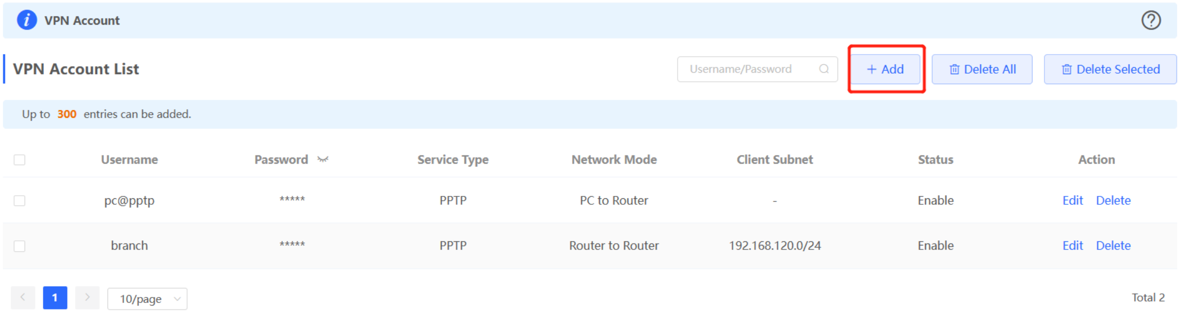
Parameter	Description
Route All Traffic over VPN	Specify whether to route all traffic over VPN. After this function is enabled, all the traffic is routed over the VPN tunnel. This means that the VPN tunnel is the default route.
Cipher	Select the data encryption mode before data transmission to ensure that even data packets are intercepted during transmission, the leaked data cannot be interpreted. If this parameter is set to **Auto** on the server, you can set this parameter to any option on the client. If a specific encryption algorithm is configured on the server, you must select the same encryption algorithm on the client. Otherwise, the connection fails.
Deliver DNS	Specify the DNS server address pushed by the server to clients. Currently, the device can push the DNS server address to Windows clients only.
Auth	Specify the MD5 algorithm used by the server. The server will inform the clients of this information. The default value is **SHA1**.

3. Configuring OpenVPN User

Choose **Local Device** > **VPN** > **VPN Account**.

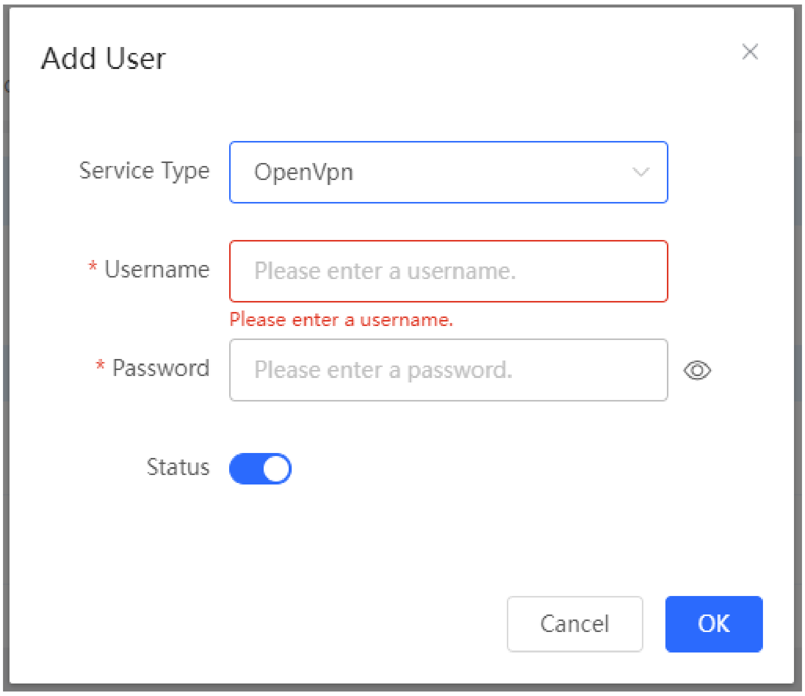
Only user accounts added to the VPN client list are allowed to dial up to connect to the OpenVPN server. Therefore, you need to manually configure user accounts for clients to access the OpenVPN server.

Click **Add**. In the dialog box that appears, set **Service Type** to **OpenVpn**, enter the username and password, and click **OK**. The **Status** parameter specifies whether to enable the user account.



Up to 300 entries can be added.

□	Username	Password	Service Type	Network Mode	Client Subnet	Status	Action
□	pc@pptp	*****	PPTP	PC to Router	-	Enable	Edit Delete
□	branch	*****	PPTP	Router to Router	192.168.120.0/24	Enable	Edit Delete



Add User

Service Type: OpenVpn

* Username: Please enter a username.

Please enter a username.

* Password: Please enter a password.

Status: ●

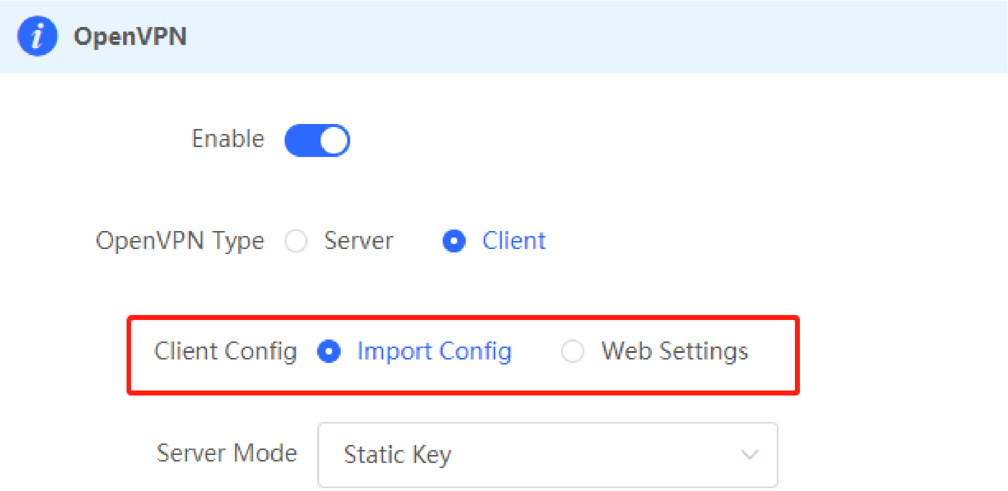
5.4.3 Configuring the OpenVPN Client

Choose **Local Device** > **VPN** > **OpenVPN**.

Currently, you can configure the device as the OpenVPN client in either of the following methods:

Web Settings: Configure OpenVPN client on the web page. This method is used when the device is connected to a non-EG server.

Import Config: Manually import the configuration file. This method is used when the device is connected to a similar device. The client configuration file **client.ovpn** can be directly exported from the connected OpenVPN server.



OpenVPN

Enable: ●

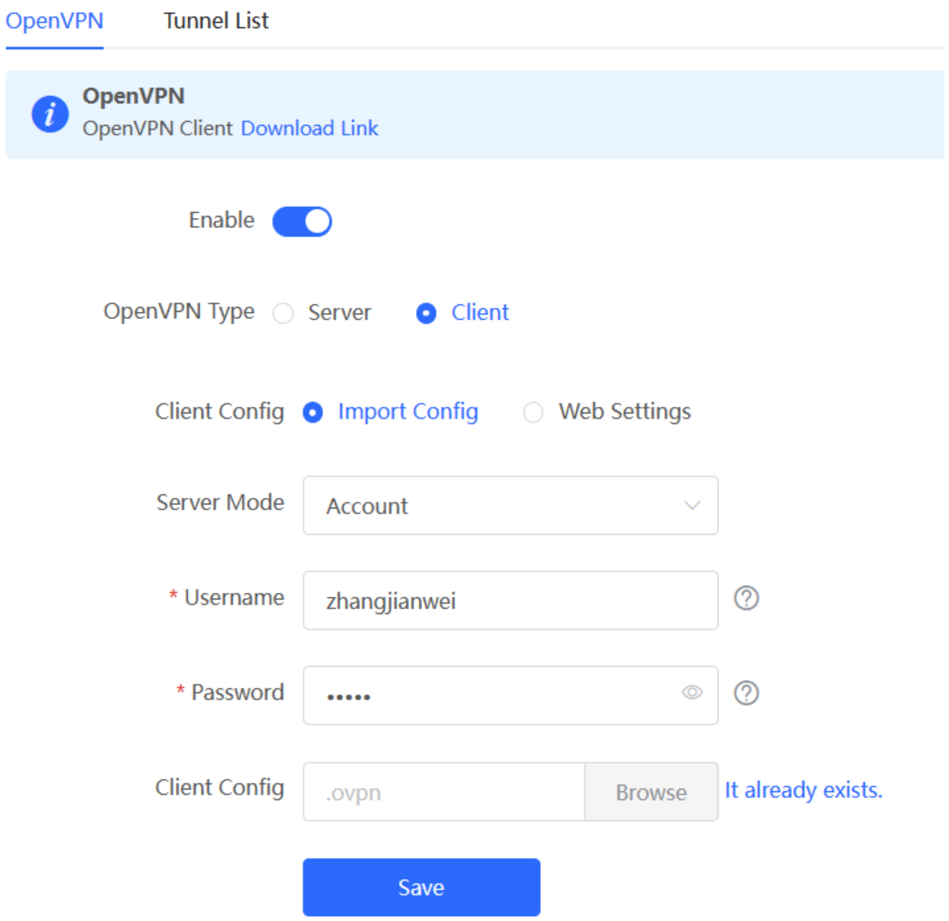
OpenVPN Type: ○ Server ● Client

Client Config: ● Import Config ○ Web Settings

Server Mode: Static Key

1. Import Config

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Import Config**, select a server mode, set relevant parameters, and click **Browse** to import the client configuration file. Then, click **Save** to make the configuration take effect.



Enable ●

OpenVPN Type ○ Server ● Client

Client Config ● Import Config ○ Web Settings

Server Mode: Account

* Username: zhangjianwei

* Password: •••••

Client Config: .ovpn Browse It already exists.

Table 5-21 OpenVPN client configuration in Import Config method

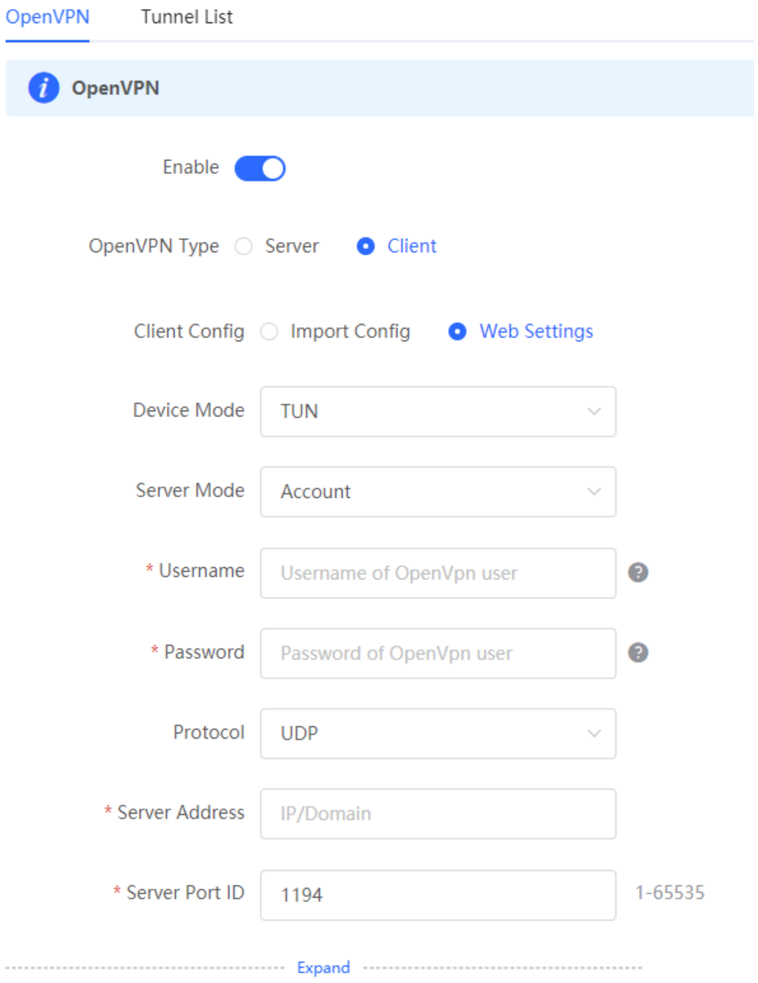
Parameter	Description
Server Mode	Select a server authentication mode. The options are Account, Certificate, Account & Certificate and Pre-Shared Key. ● Account: Enter the correct username and password and upload the CA certificate on the client. The CA certificate information is embedded in the client configuration file. ● Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client. All the information is embedded in the client configuration file. ● Account & Certificate: Enter the correct username, password, and private key and upload the CA certificate, and client certificate on the client. The information of the CA certificate, client certificate, and private key is embedded in the client configuration file. ● Pre-Shared Key: Upload the pre-shared key file apart from the client configuration file.

Parameter	**Description**
Username & Password	Enter the username and password configured on the server.
Client Config	Click Browse, select the client configuration file exported from the server, and upload the file.
Pre-Shared Key	Click Browse, select the pre-shared key file, and upload the file.
Working Mode	This parameter is available only when Server Mode is set to Pre-Shared Key. NAT: The client can access the server network, but the server cannot access the client network. Router: The server can access the client network.
Client Log	Click Export to export the client log file.

2. Web Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Web Settings**, configure parameters such as **Device Mode** and **Device Mode**, and click **Save** to make the configuration take effect.

(1) Basic Settings



Enable ●

OpenVPN Type ○ Server ● Client

Client Config ○ Import Config ● Web Settings

Device Mode: TUN

Server Mode: Account

* Username: Username of OpenVpn user

* Password: Password of OpenVpn user

Protocol: UDP

* Server Address: IP/Domain

* Server Port ID: 1194 1-65535

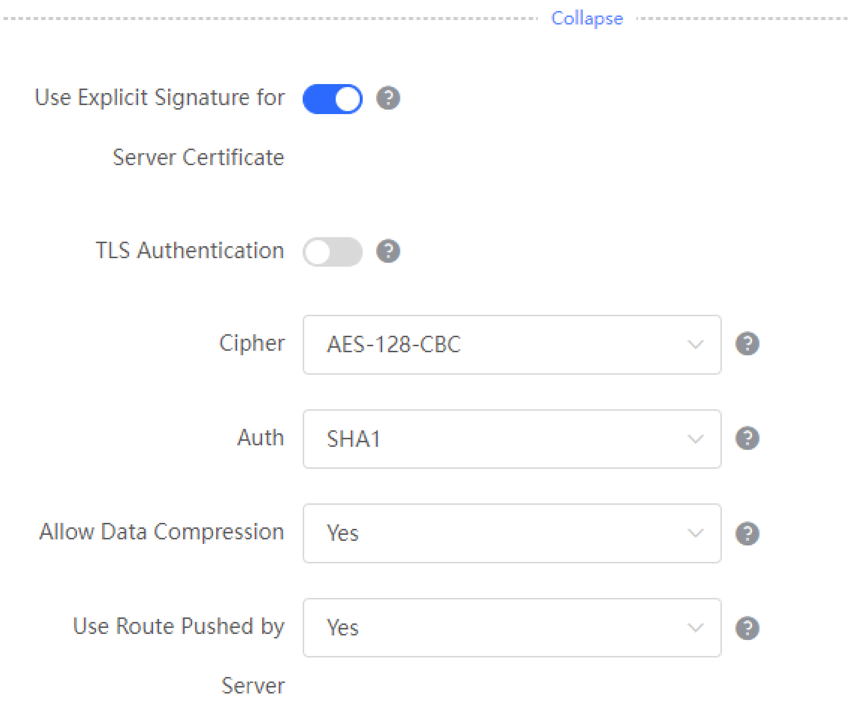
Table 5-22 OpenVPN client configuration in Web Settings method

Parameter	Description
Device Mode	Specify the mode of the EG device that functions as a client. The options are **TUN** and **TAP**. The value must be the same as that configured on the server. When the EG device works as a server, it supports the TUN mode only.
Server Mode	Select a client authentication mode. The options are **Account**, **Certificate**, and **Account & Certificate**. ● Account: Enter the correct username and password and upload the CA certificate on the client. ● Certificate: Upload the correct CA certificate, client certificate, and private key file on the client. ● Account & Certificate: Enter the correct username and password, and upload the CA certificate, client certificate, and private key file on the client.

Parameter	Description
Protocol	Select the protocol running on the device. The options are **UDP** and **TCP**. The value must be the same as that configured on the server.
Server Address	Enter the address or domain name of the server to be connected.
Server Port ID	Enter the port number of the server to be connected.
CA Certificate	Click **Browse**, select the CA certificate file with the file name extension **.ca**, and upload the file.
Client Key	Click **Browse**, select the client private file with the file name extension **.key**, and upload the file.
Client Certificate	Click **Browse**, select the client certificate file with the file name extension **.crt**, and upload the file.
Client Certificate Key	Specify the client certificate key if the client certificate provided by the server (such as the MikroTik server) is encrypted twice.
Client Log	Click **Export** to export the client log file.

(2) Advanced Settings

Click **Expand** to configure the advanced parameters. Keep the default settings unless otherwise specified.



Use Explicit Signature for Server Certificate: on

TLS Authentication: off

Cipher: AES-128-CBC

Auth: SHA1

Allow Data Compression: Yes

Use Route Pushed by Server: Yes

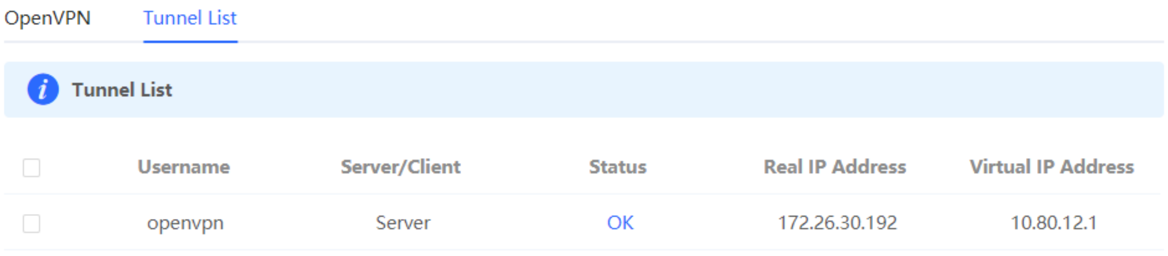
Table 5-23 OpenVPN client configuration in Web Settings method

Parameter	Description
Use Explicit Signature for Server Certificate	Specify whether to verify the server certificate using explicit signature. By default, this function is enabled. If the server certificate does not use explicit signature, for example, the MikroTik server, you need to disable this function. Otherwise, the connection fails.
TLS Authentication	Specify whether to enable TLS authentication for the server. If this function is enabled, you need to upload the TLS certificate file.
Cipher	Select a data compression algorithm. The value must be the same as that configured on the server. Otherwise, the connection fails.
Auth	Select an MD5 algorithm for data packet verification. The options are **SHA1**, **MD5**, **SHA256**, and **NULL**. The value must be the same as that configured on the server. Otherwise, the connection fails.
Allow Data Compression	Specify whether to allow data compression. After this function is enabled, the transmitted data can be compressed by using the LZO algorithm. The value must be the same as that configured on the server.
Use Route Pushed by Server	Specify whether to use the routes pushed by the server. If this function is disabled, the device cannot accept the routes pushed by the server. If the server needs to access LAN devices, you must set this parameter to **Yes**.

5.4.4 Viewing the OpenVPN Tunnel Information

Choose **Local Device** > **VPN** > **OpenVPN** > **Tunnel List**.

After the server and client are configured, you can view the OpenVPN tunnel connection status. If the tunnel is established successfully, the client tunnel information is displayed in the tunnel list of the server.



□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	openvpn	Server	OK	172.26.30.192	10.80.12.1

Table 5-24 OpenVPN tunnel information

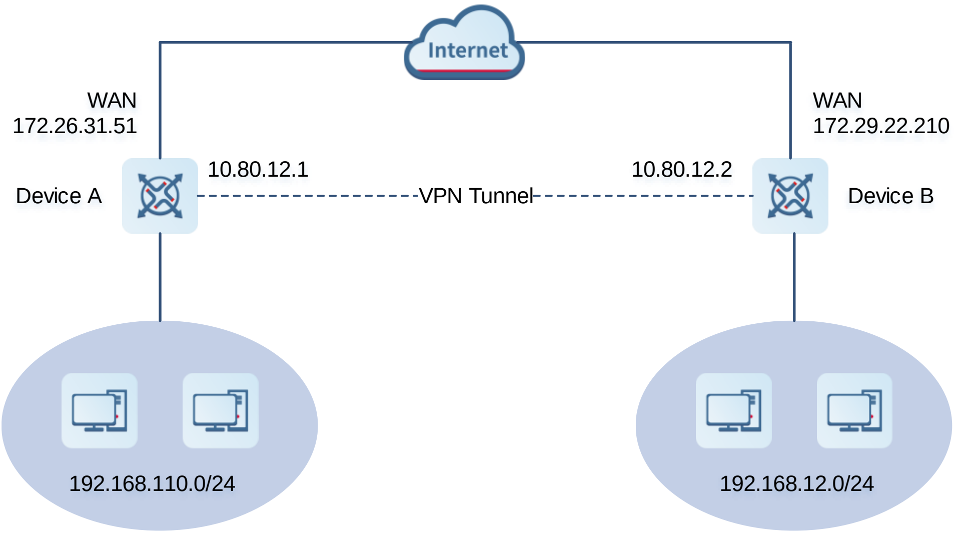
Parameter	Description
Username	Indicate the username used by the client for identity authentication. By default, the username displayed on the server is **openvpn**.
Server/Client	Indicate the role of the local end of the tunnel, which can be client or server.
Status	Indicate the tunnel establishment status.
Real IP Address	Indicate the real IP address used by the local end to connect to the VPN.
Virtual IP Address	Indicate the local virtual IP address of the tunnel. The virtual IP address of the OpenVPN client is allocated by the OpenVPN server.

5.4.5 Typical Configuration Example

1. Networking Requirements

The enterprise wants to allow the client network to dial up to the server through OpenVPN, implementing mutual access between the server and client.

2. Networking Diagram



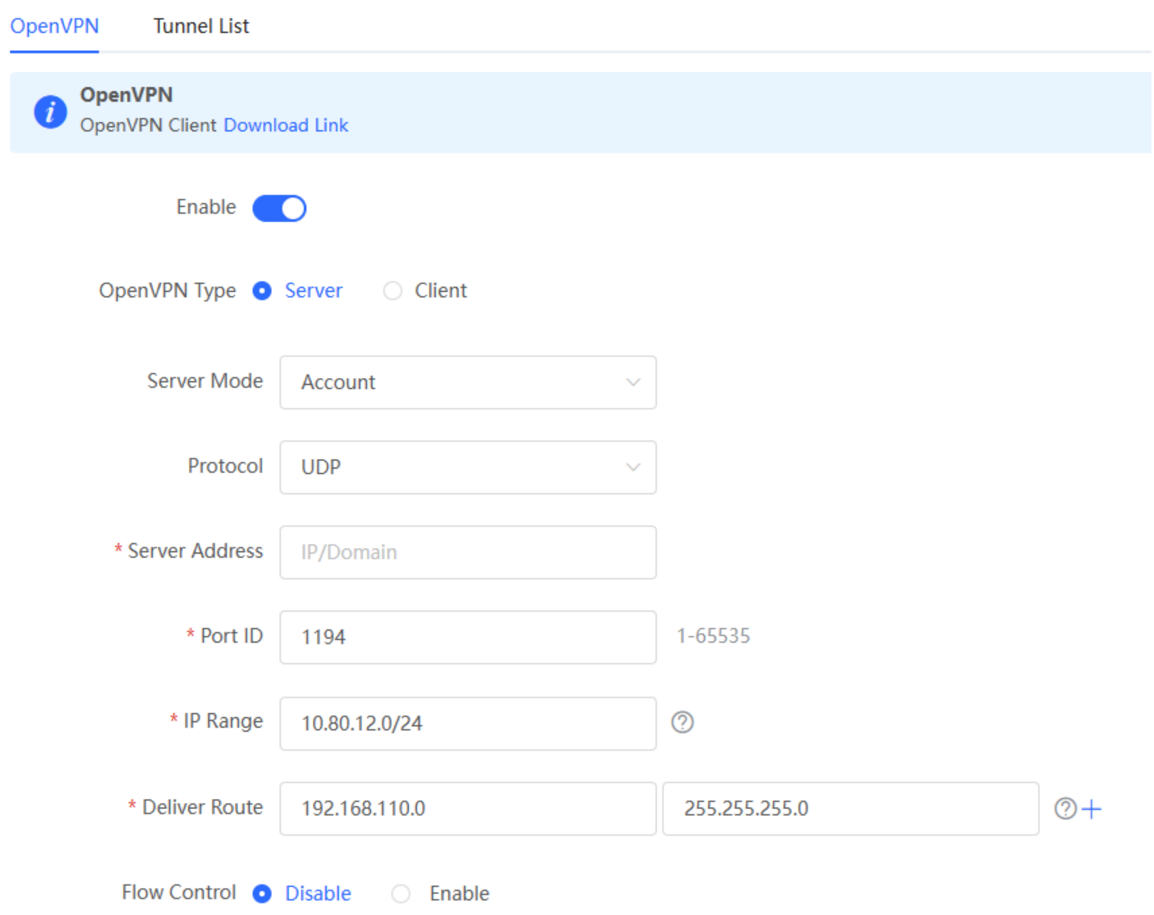
3. Configuration Roadmap

- Configure Device A as the OpenVPN server.
- Configure Device B as the OpenVPN client.
- The server needs to push the local LAN network segment to the client to allow the client to access the server in the LAN.

4. Configuration Steps

(1) Configure Device A.

a Log in to the web management system and choose **VPN > OpenVPN > OpenVPN** to access the OpenVPN page.



Enable: ●

OpenVPN Type: ● Server ○ Client

Server Mode: Account

Protocol: UDP

* Server Address: IP/Domain

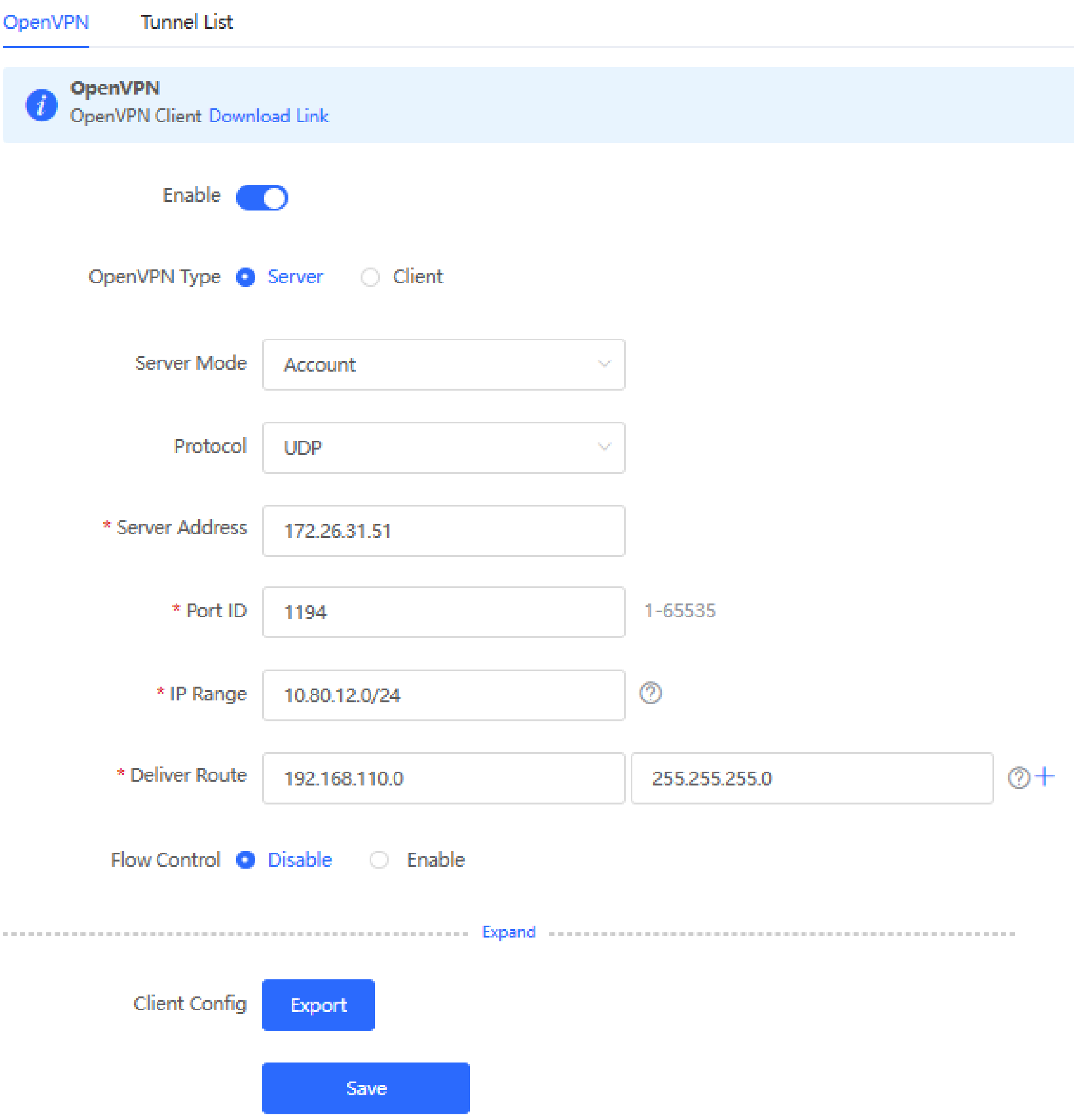
* Port ID: 1194 1-65535

* IP Range: 10.80.12.0/24

* Deliver Route: 192.168.110.0 255.255.255.0

Flow Control: ● Disable ○ Enable

b Turn on Enable to enable the OpenVPN function, set OpenVPN Type to Server, select a server mode and protocol, enter the port number (1194 by default) and server address (external IP address of the local device), and click **Save**.



OpenVPN
OpenVPN Client Download Link

Enable: on

OpenVPN Type: ● Server ○ Client

Server Mode: Account

Protocol: UDP

* Server Address: 172.26.31.51

* Port ID: 1194 1-65535

* IP Range: 10.80.12.0/24

* Deliver Route: 192.168.110.0 255.255.255.0

Flow Control: ● Disable ○ Enable

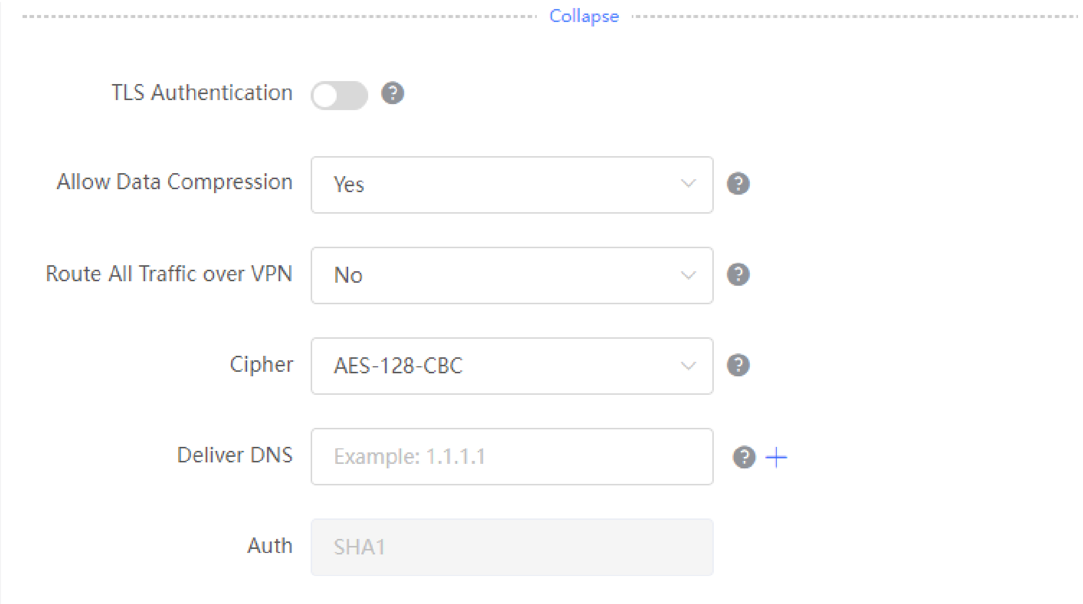
Client Config

Table 5-25 OpenVPN server configuration

Parameter	Description
Server Mode	Select an authentication mode. In this example, select **Account**. In scenarios with high security requirements, select **Account & Certificate**.
Protocol	Select **UDP** unless otherwise specified. When the network status between two encrypted tunnel ends is poor, such as high latency or heavy packet loss, select **TCP**.
Server Address	Enter the WAN port address of the server, which is **172.26.31.51**.

Parameter	Description
Port ID	The default value is **1194**. Keep the default value unless otherwise specified. If the port is in use of disabled in the current network, change to an available port number.
IP Range	Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to **10.80.12.0/24**, the VPN virtual address of the server is 10.80.12.1.
Deliver Route	Add routes to the corresponding network segment if the client wants to the LAN network segment where the server resides.

c Click Expand to configure more advanced parameters. If the device connects to other EG devices in the Reyee network, you are advised to keep the default values for advanced settings. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.



TLS Authentication: off

Allow Data Compression: Yes

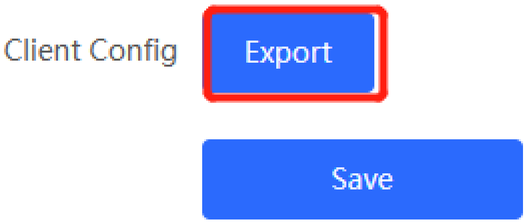
Route All Traffic over VPN: No

Cipher: AES-128-CBC

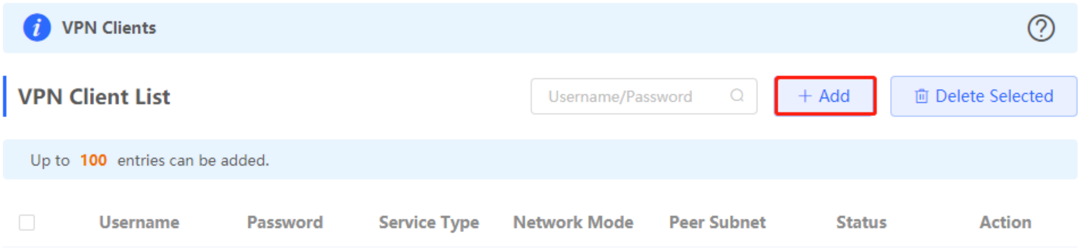
Deliver DNS: Example: 1.1.1.1

Auth: SHA1

d Click **Export** to export the compressed package of the client parameter configuration. Download the compressed package to the local device and decompress it for setting the OpenVPN client in subsequent steps.



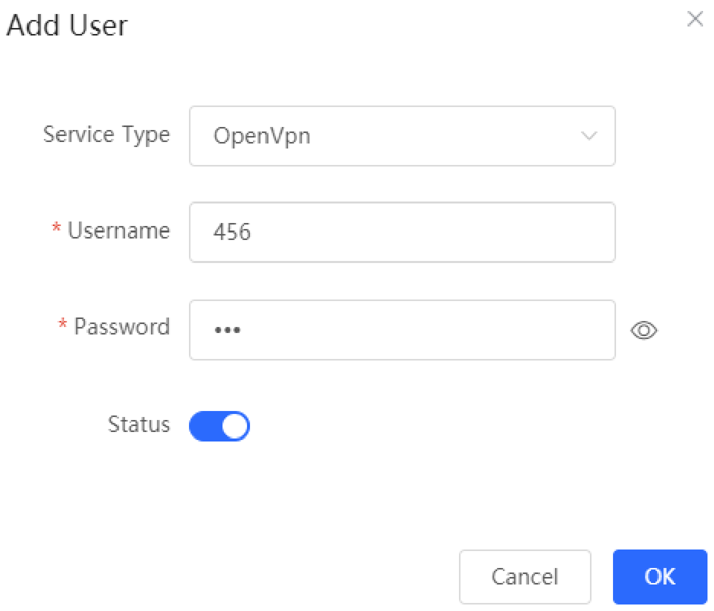
e Choose **VPN** > **VPN Account** and add an OpenVPN user account.



VPN Client List

Up to 100 entries can be added.

□	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action



Add User

Service Type: OpenVpn

* Username: 456

* Password: •••

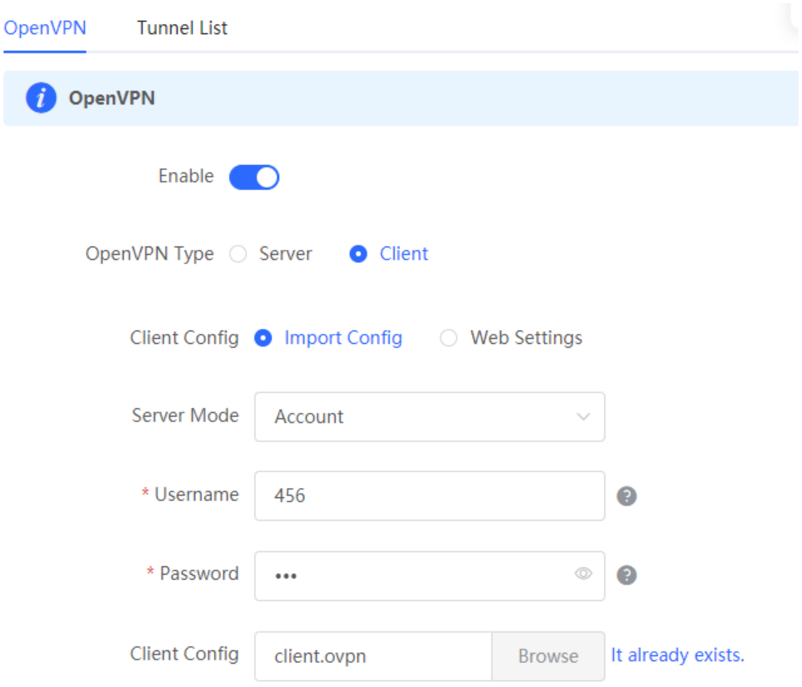
Status: ●

(2) Configure Device B.

a Log in to the web management system and access the OpenVPN page.

b Turn on Enable to enable the OpenVPN function and set OpenVPN Type to Client. Two methods are available for configuring the client. The Import Config method is recommended.

Import Config:



OpenVPN Tunnel List

OpenVPN

Enable: on

OpenVPN Type: ○ Server ● Client

Client Config: ● Import Config ○ Web Settings

Server Mode: Account

* Username: 456

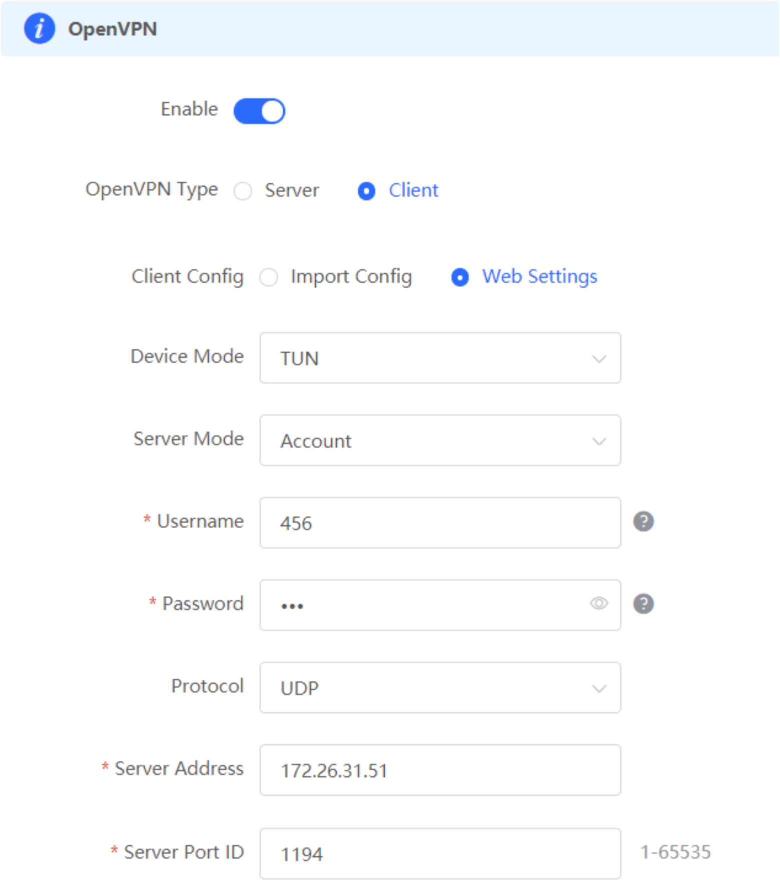
* Password: •••

Client Config: client.ovpn Browse It already exists.

Table 5-26 OpenVPN client configuration in Import Config method

Parameter	Description
Client Config	Select Import Config.
Server Mode	The value must be the same as that on the server. In this example, select **Account**.
Username & Password	Enter the username and password configured on the server.
Client Config	Click **Browse**, select the client configuration file exported from the server, and upload the file.

Web Settings:



OpenVPN

Enable ●

OpenVPN Type ○ Server ● Client

Client Config ○ Import Config ● Web Settings

Device Mode TUN

Server Mode Account

* Username 456

* Password •••

Protocol UDP

* Server Address 172.26.31.51

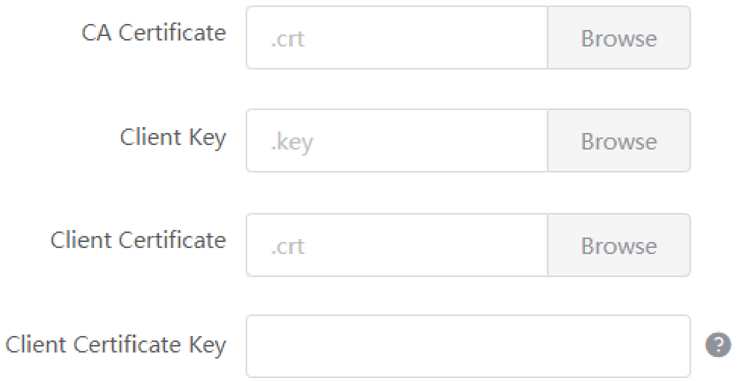
* Server Port ID 1194 1-65535

Table 5-27 OpenVPN client configuration in Web Settings method

Parameter	Description
Client Config	Select Web Settings.
Device Mode	The value must be the same as that on the server. In this example, select **TUN**.
Server Mode	The value must be the same as that on the server. In this example, select **Account**.
Username & Password	Enter the username and password configured on the server.
Protocol	The value must be the same as that on the server. In this example, select **UDP**.
Server Address	Enter the public network IP address of the server, which is **172.26.31.51**.
Server Port ID	Enter the port number used by the server, such as **1194**.

Import the corresponding files according to the value of **Server Mode**.

If **Server Mode** is set to **Certificate** or **Account & Certificate**, you need to import the CA certificate file, client certificate file, and client private key file. If **Server Mode** is set to **Account**, you only need to import the CA certificate file. If the client certificate is encrypted, you also need to enter the pre-shared key specified by **Client Certificate Key**.



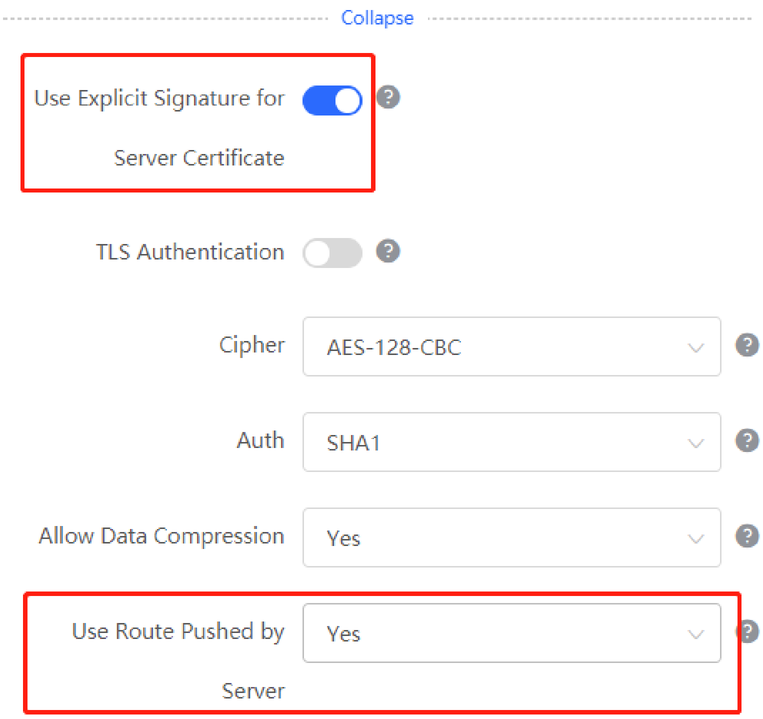
CA Certificate: .crt Browse

Client Key: .key Browse

Client Certificate: .crt Browse

Client Certificate Key: ?

Click **Expand** to configure more parameters. Configure **Use Route Pushed by Server** to specify whether to accept routes pushed by the server. The value must be the same as that on the server. If the client is connected to a non-EG device, such as MikroTik server outside China, you need to turn off **Use Explicit Signature for Server Certificate**.



Collapse

Use Explicit Signature for Server Certificate: ● ?

TLS Authentication: ○ ?

Cipher: AES-128-CBC ?

Auth: SHA1 ?

Allow Data Compression: Yes ?

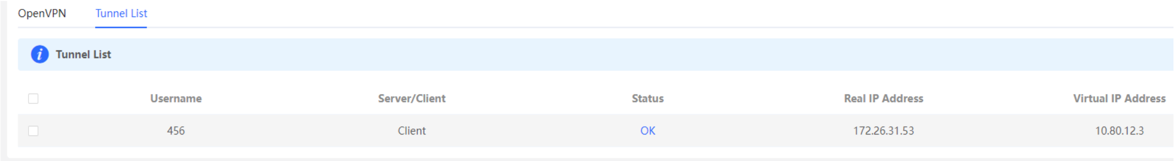
Use Route Pushed by Server: Yes ?

c After the configuration is completed, click Save to make the configuration take effect.

5. Verifying Configuration

After the server and client are configured, view the two tunnel end information in the tunnel list.

Client:

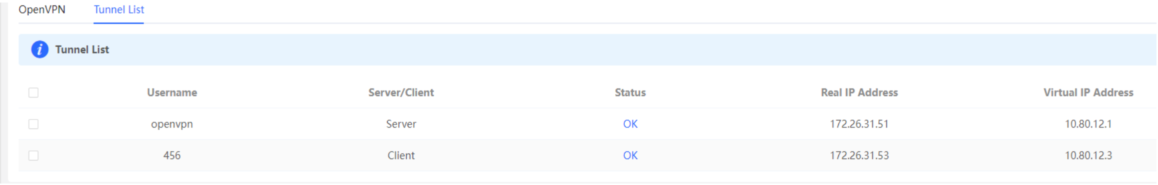


OpenVPN Tunnel List

Tunnel List

□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	456	Client	OK	172.26.31.53	10.80.12.3

Server:



OpenVPN Tunnel List

Tunnel List

□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	openvpn	Server	OK	172.26.31.51	10.80.12.1
□	456	Client	OK	172.26.31.53	10.80.12.3

6 Advanced Solution

6.1 Reyee Flow Control Solution

6.1.1 Application Scenario

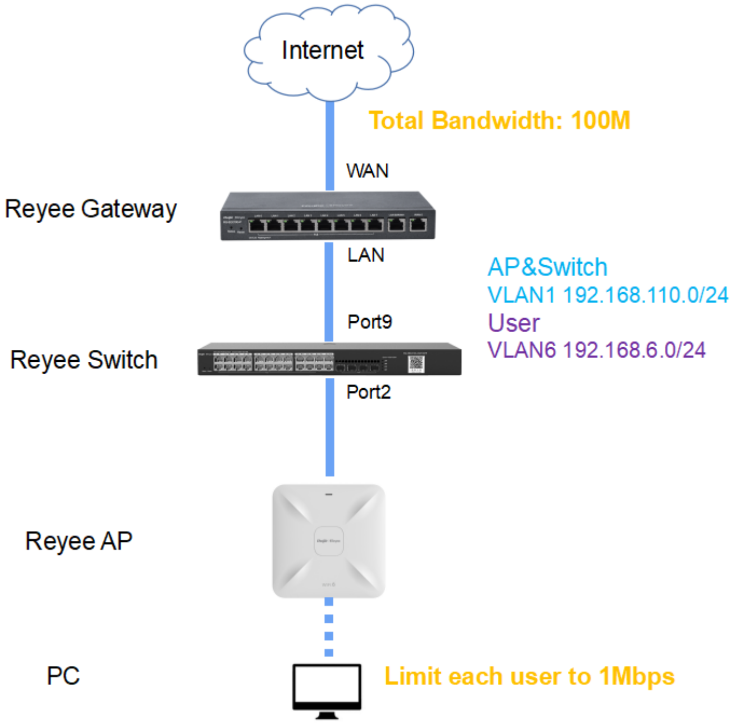
Flow control is used for setting rate limits of download and upload rates for the clients. With flow control configured, the router can protect the network bandwidth from being occupied by some clients.

6.1.2 Configuration Example

Requirement

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

Network Topology



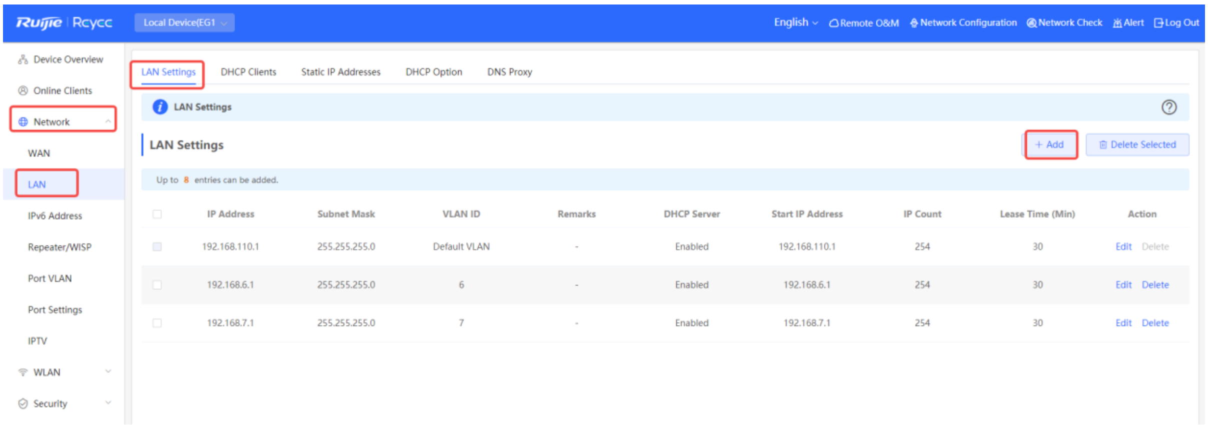
Network Description

- 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 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.**

(1) 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.

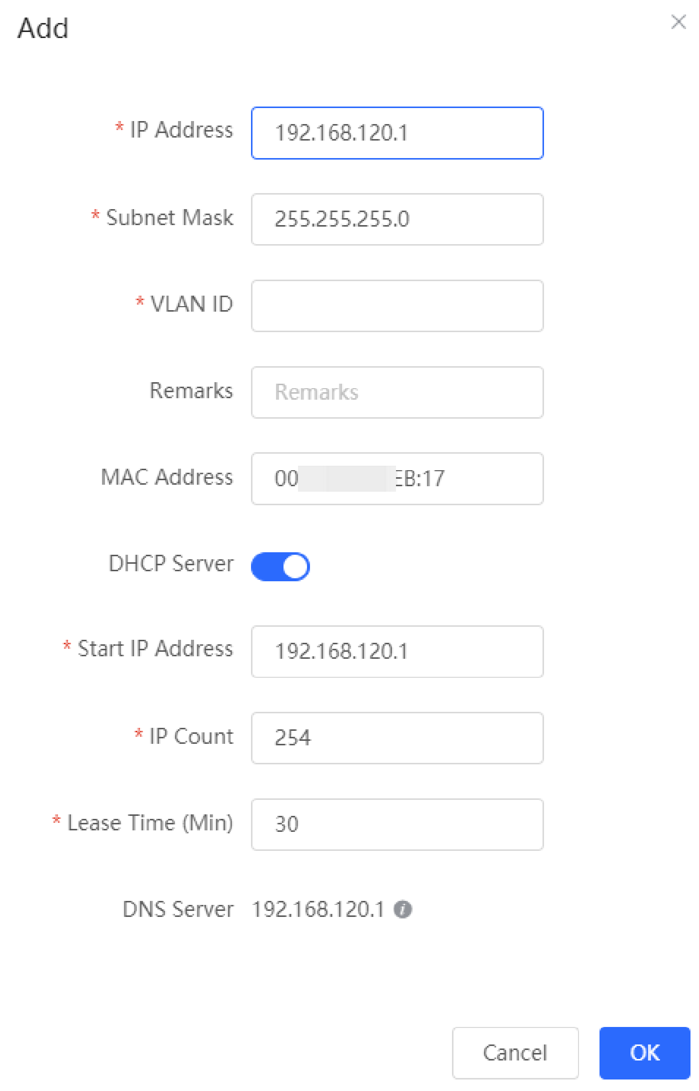


LAN Settings

LAN Settings

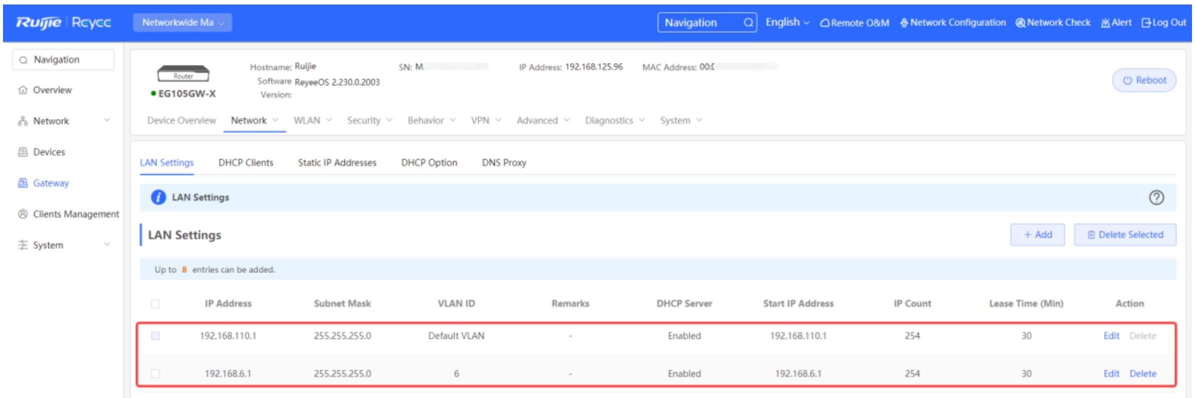
Up to 8 entries can be added.

□	IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
□	192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete



Add

* IP Address	192.168.120.1
* Subnet Mask	255.255.255.0
* VLAN ID	
Remarks	Remarks
MAC Address	00[redacted]B:17
DHCP Server	●
* Start IP Address	192.168.120.1
* IP Count	254
* Lease Time (Min)	30
DNS Server	192.168.120.1



Hostname: Ruijie
Software Version: ReyeeOS 2.230.0.2003
SN: M[redacted]
IP Address: 192.168.125.96
MAC Address: 00:[redacted]

LAN Settings

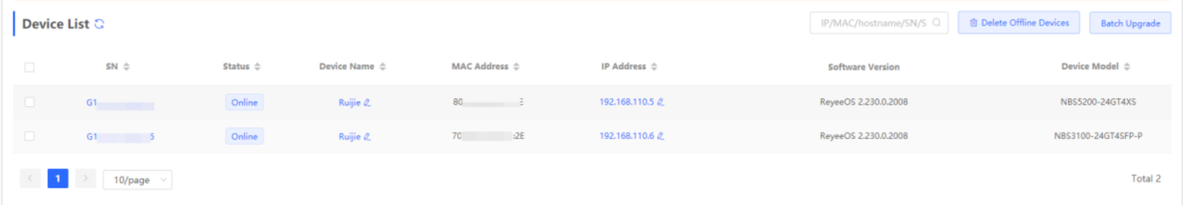
Up to 8 entries can be added.

□	IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	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**.



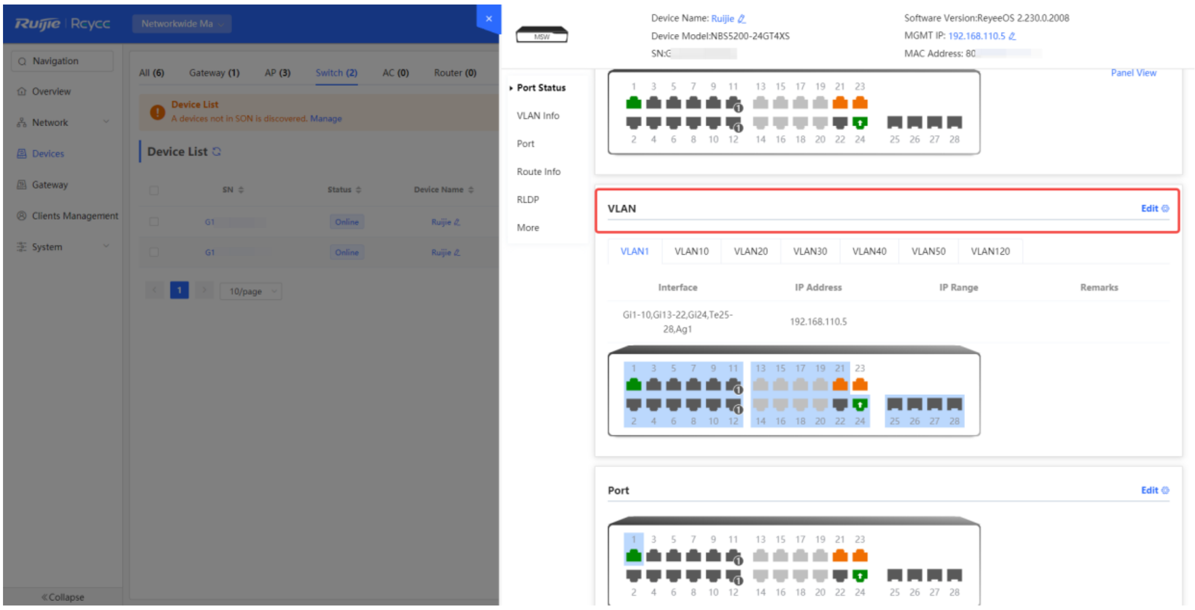
Device List

□	SN	Status	Device Name	MAC Address	IP Address	Software Version	Device Model
□	G1[redacted]	Online	Ruijie	80[redacted]	192.168.110.5	ReyeeOS 2.230.0.2008	NBS5200-24GT4XS
□	G1[redacted]5	Online	Ruijie	70[redacted]:2E	192.168.110.6	ReyeeOS 2.230.0.2008	NBS3100-24GT4SFP-P

Total 2

(3) Select a device from **Device List** and access the configuration page.

(4) In the **VLAN** pane, select a VLAN and click **Edit** to configure the VLAN.

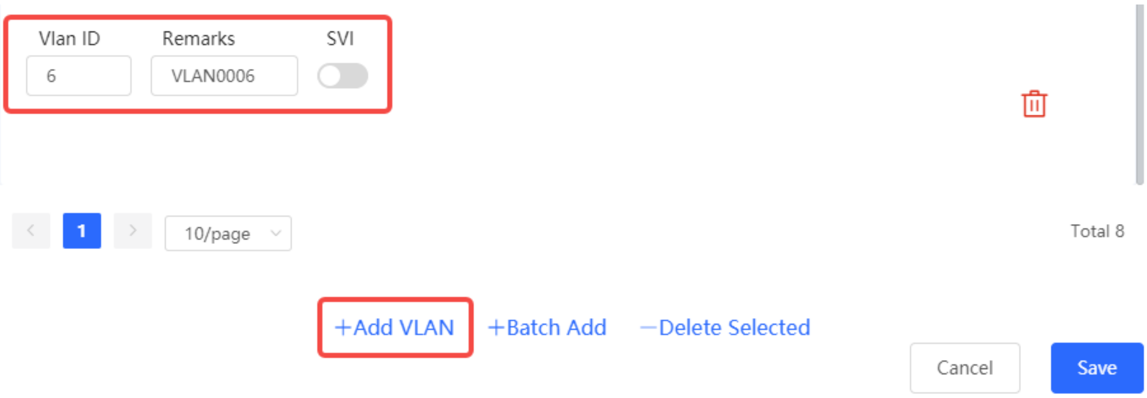


Device Name: Ruijie
Device Model:NBS5200-24GT4XS
SN:G[redacted]
Software Version:ReyeeOS 2.230.0.2008
MGMT IP: 192.168.110.5
MAC Address: 80[redacted]

VLAN

Interface	IP Address	IP Range	Remarks
Gi1-10,Gi13-22,Gi24,Te25-28,Ag1	192.168.110.5		

(5) Click **Add VLAN** to create VLAN 6 on the switch.

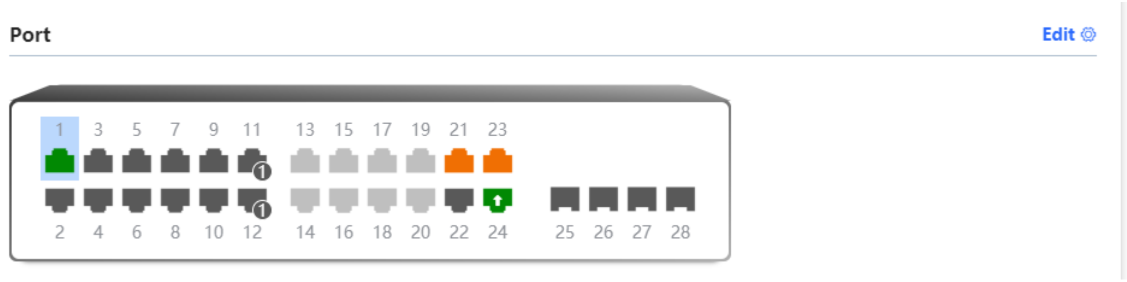


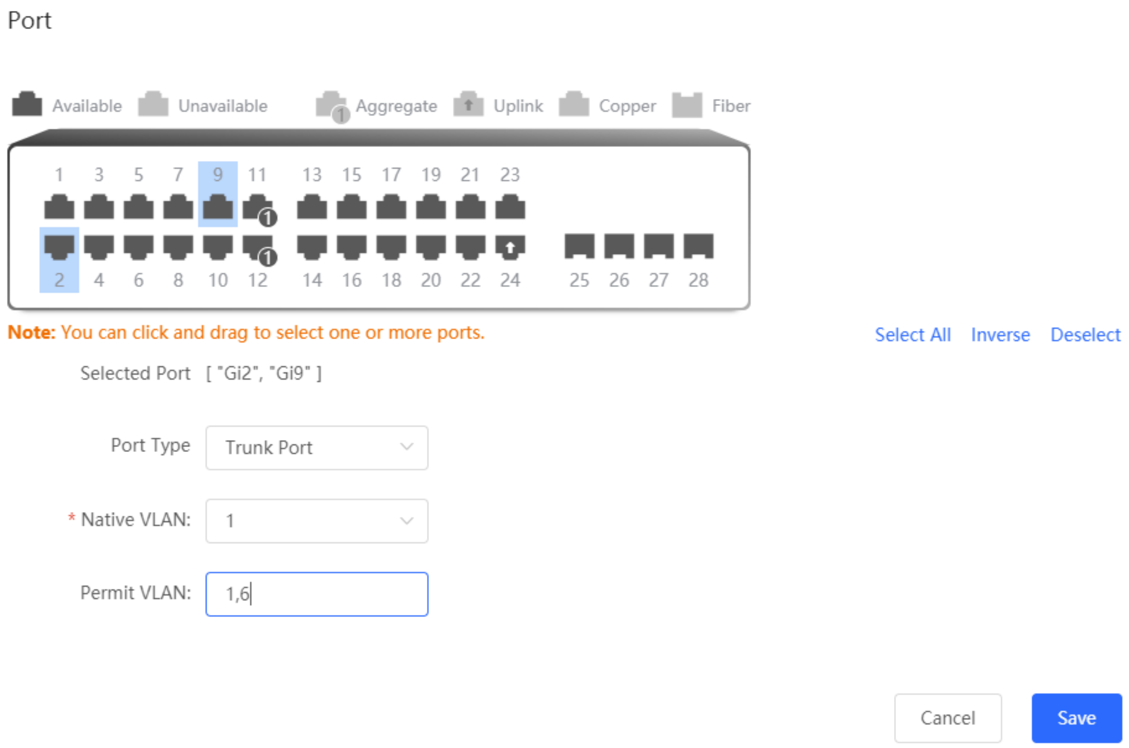
Vlan ID: 6

Remarks: VLAN0006

SVI

(6) 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.





Note: You can click and drag to select one or more ports.

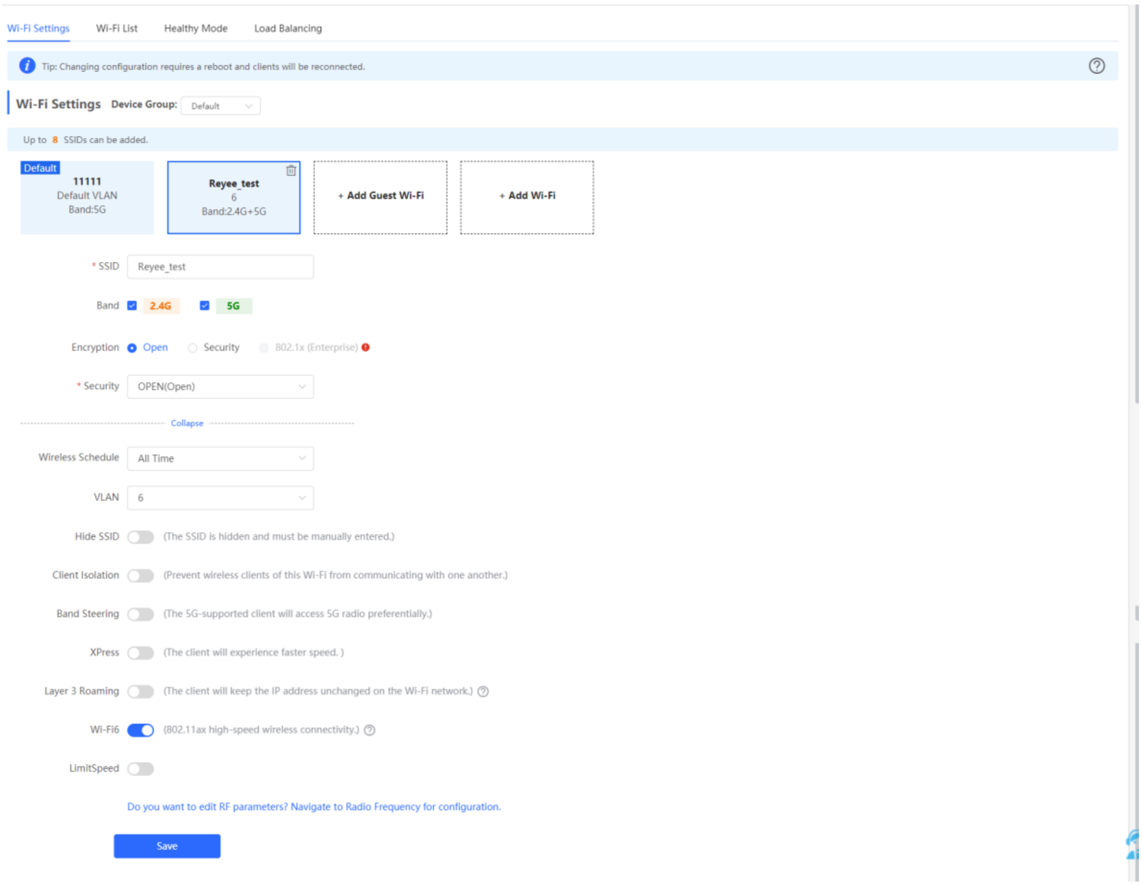
Selected Port ["Gi2", "Gi9"]

Port Type: Trunk Port

* Native VLAN: 1

Permit VLAN: 1,6

(7) 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.



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

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

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

Default 11111 Default VLAN Band:5G | Reyee_test 6 Band:2.4G+5G | + Add Guest Wi-Fi | + Add Wi-Fi

* SSID: Reyee_test

Band: ☑ 2.4G ☑ 5G

Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(Open)

Collapse

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.)

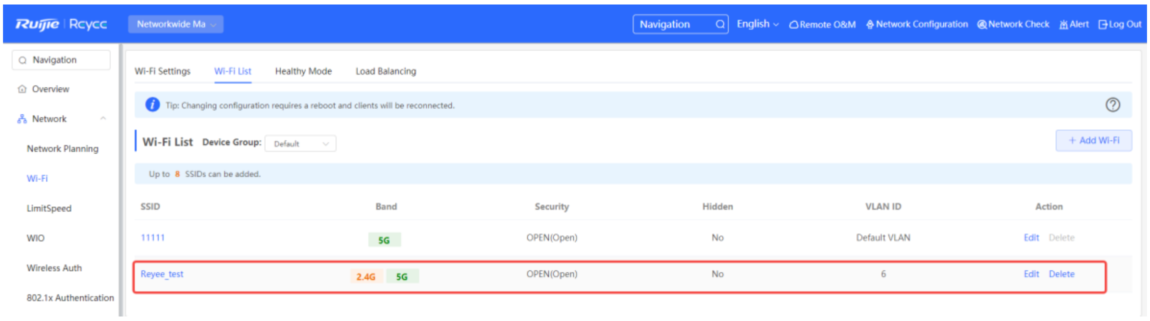
Layer 3 Roaming: (The client will keep the IP address unchanged on the Wi-Fi network.)

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

LimitSpeed

Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.

Save



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

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

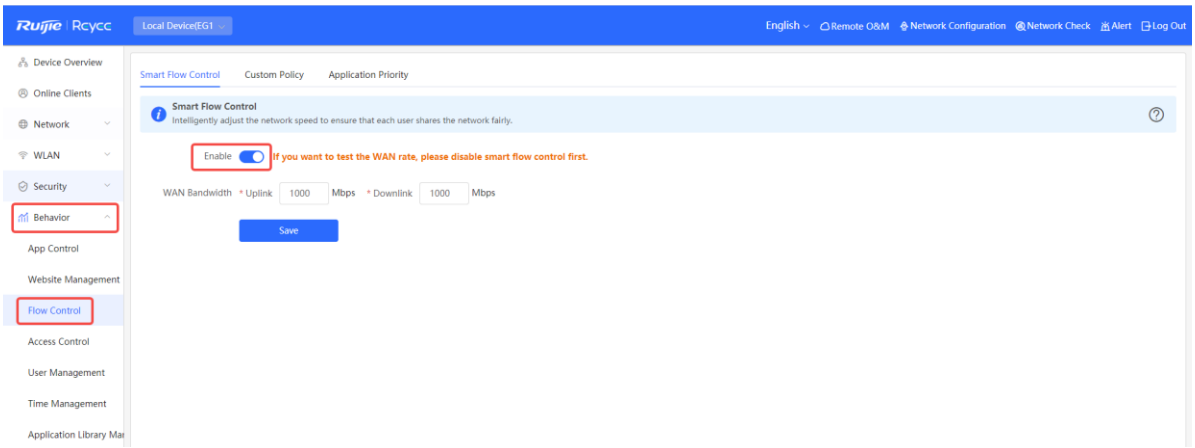
Wi-Fi List Device Group: Default + Add Wi-Fi

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
11111	5G	OPEN(Open)	No	Default VLAN	Edit Delete
Reyee_test	2.4G 5G	OPEN(Open)	No	6	Edit Delete

2. Configure smart flow control.

(1) Switch to the Local mode. Choose **Behavior > Flow Control** and enable Smart Flow Control.



Smart Flow Control | Custom Policy | Application Priority

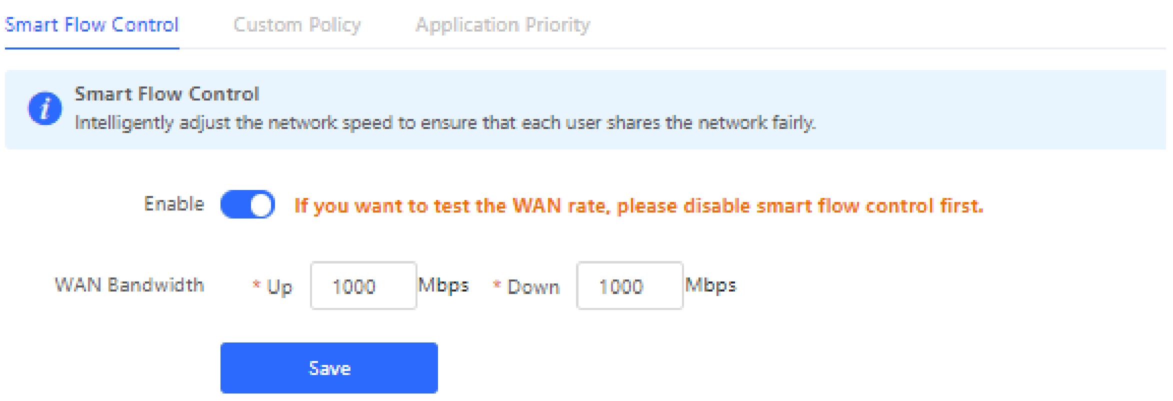
Smart Flow Control
Intelligently adjust the network speed to ensure that each user shares the network fairly.

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

WAN Bandwidth * Uplink 1000 Mbps * Downlink 1000 Mbps

Save

(2) Fill in the uplink and downlink WAN bandwidth as 100 Mbps and click **Save**.



Smart Flow Control

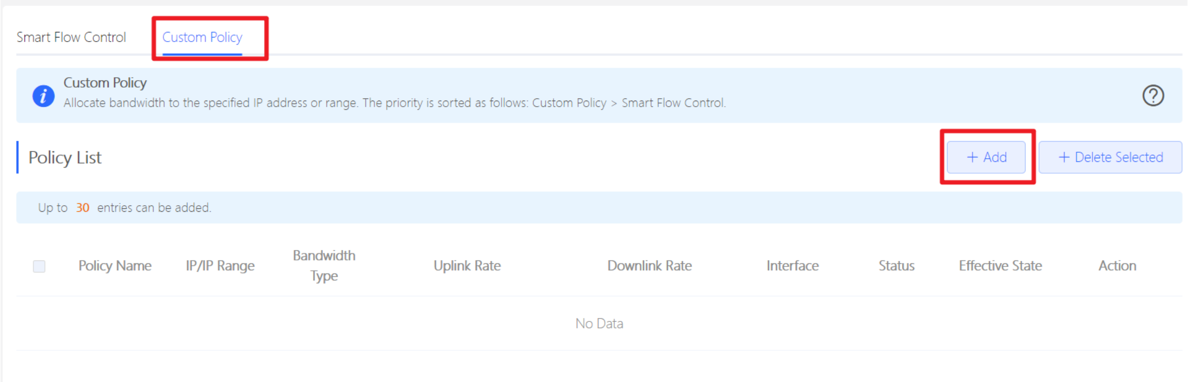
Intelligently adjust the network speed to ensure that each user shares the network fairly.

Enable

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

WAN Bandwidth * Up 1000 Mbps * Down 1000 Mbps

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



Custom Policy

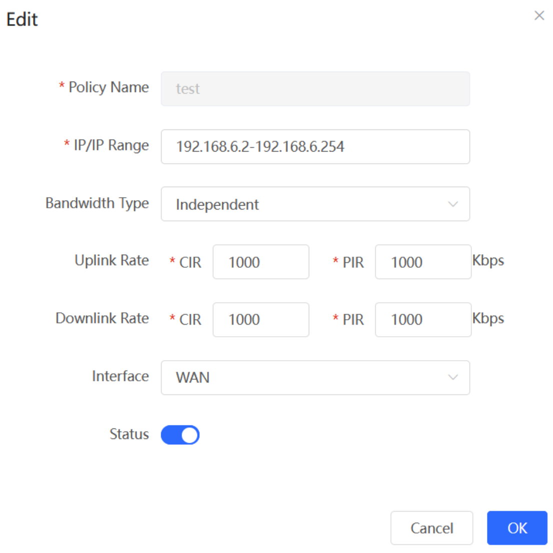
Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.

Policy List

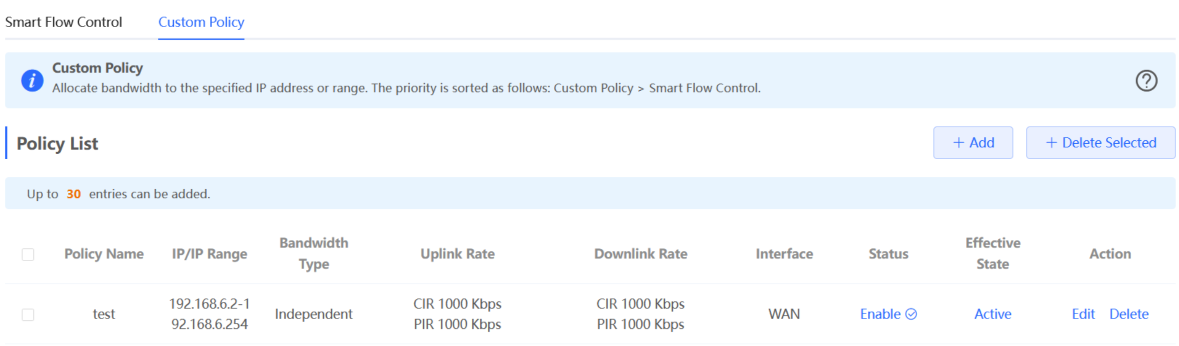
Up to 30 entries can be added.

□	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
No Data									

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



* Policy Name	test
* IP/IP Range	192.168.6.2-192.168.6.254
Bandwidth Type	Independent
Uplink Rate	* CIR 1000 * PIR 1000 Kbps
Downlink Rate	* CIR 1000 * PIR 1000 Kbps
Interface	WAN
Status	



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

Policy List

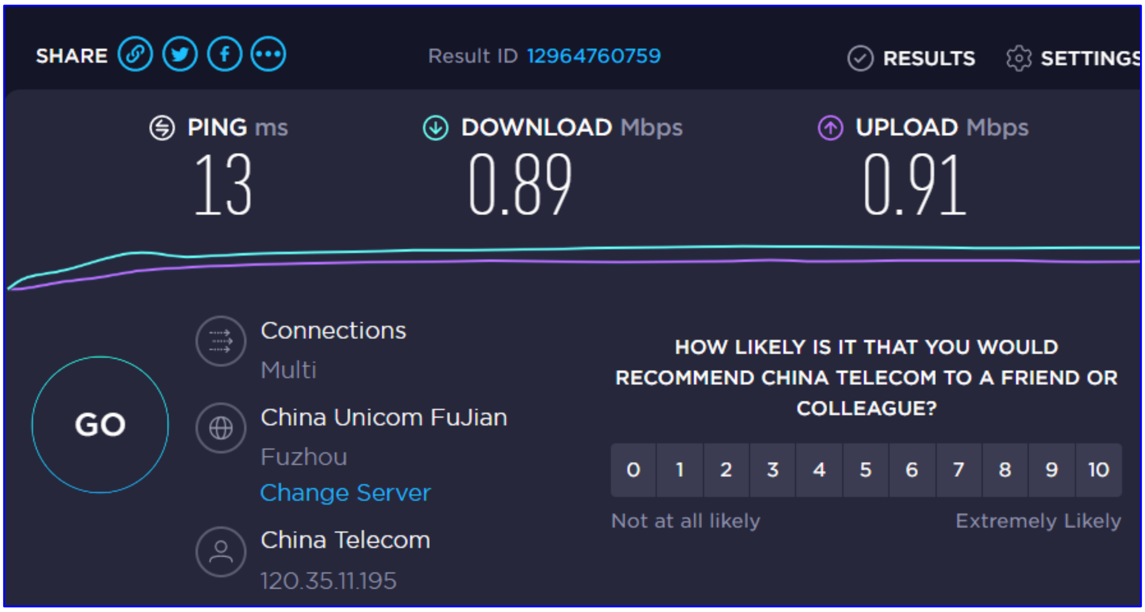
Up to 30 entries can be added.

□	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
□	test	192.168.6.2-1 92.168.6.254	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.

6.1.3 Configuration Verification

Use Speed test tool to check that each user is limited up to 1 Mbps.



Result ID 12964760759

PING ms 13

DOWNLOAD Mbps 0.89

UPLOAD Mbps 0.91

Connections
Multi

China Unicom FuJian
Fuzhou

China Telecom
120.35.11.195

6.2 Reyee Cloud Authentication Solution

6.2.1 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.

6.2.2 Application Scenario

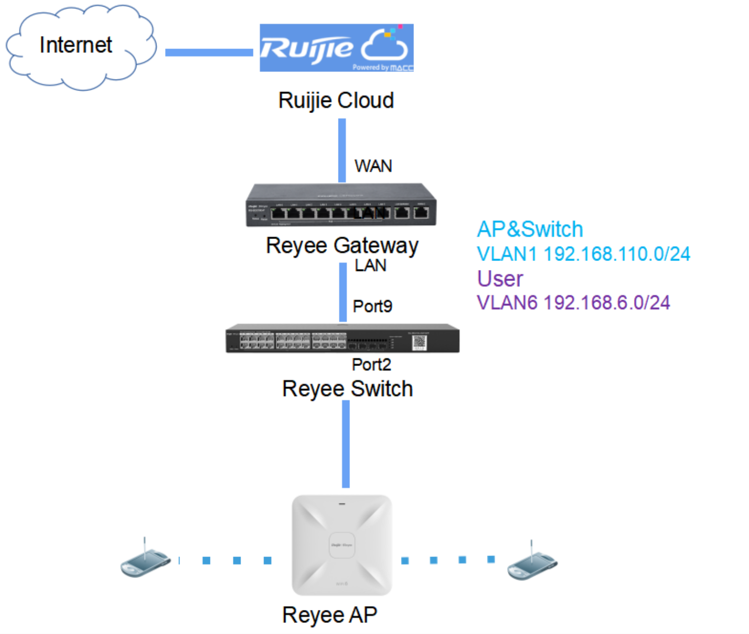
Portal authentication, also known as web authentication, is usually deployed in a guest-access network (such as a hotel or a coffee shop) to control clients' Internet access.

6.2.3 Configuration Example

Requirement

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

Network Topology



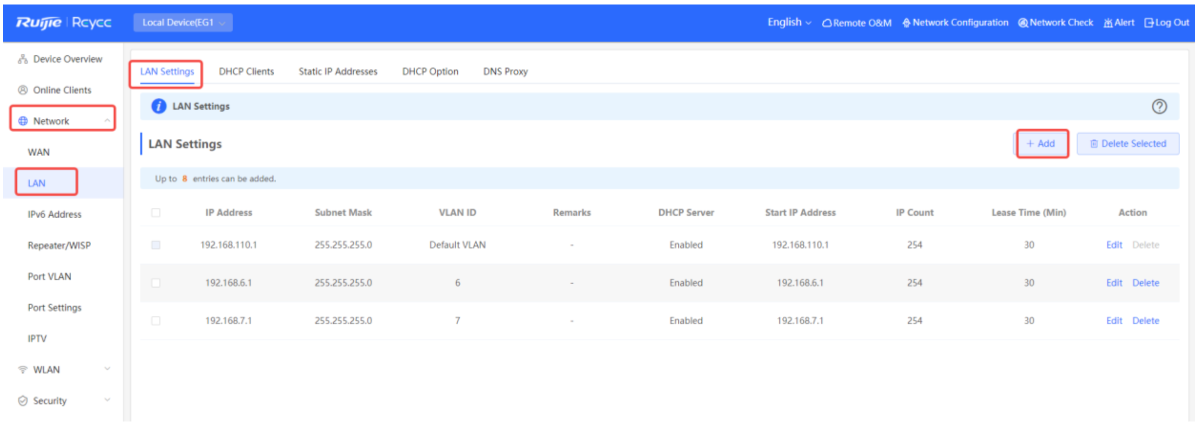
Network Description

- 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 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.

(1) 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.

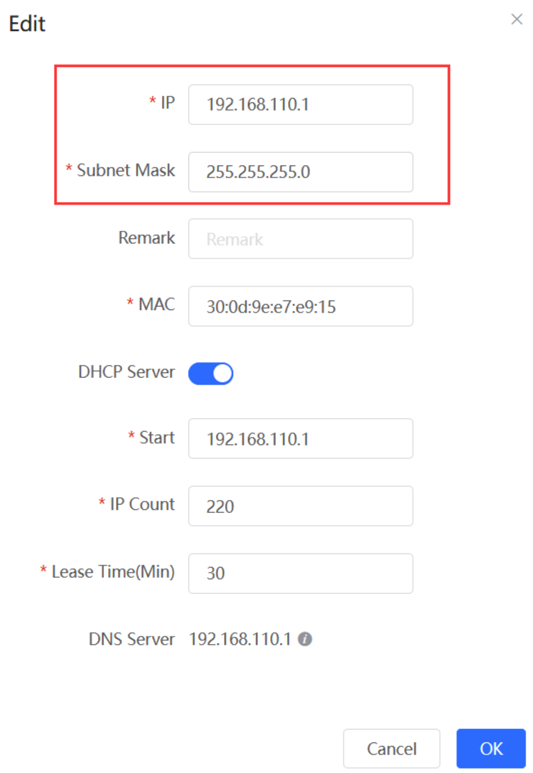


LAN Settings

LAN Settings

Up to 8 entries can be added.

□	IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
□	192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete



* IP: 192.168.110.1

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: 30:0d:9e:e7:e9:15

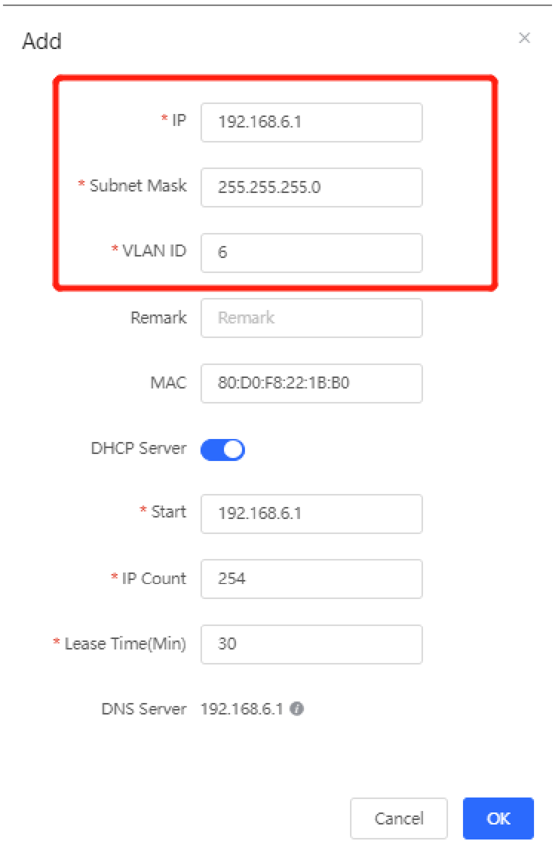
DHCP Server: ●

* Start: 192.168.110.1

* IP Count: 220

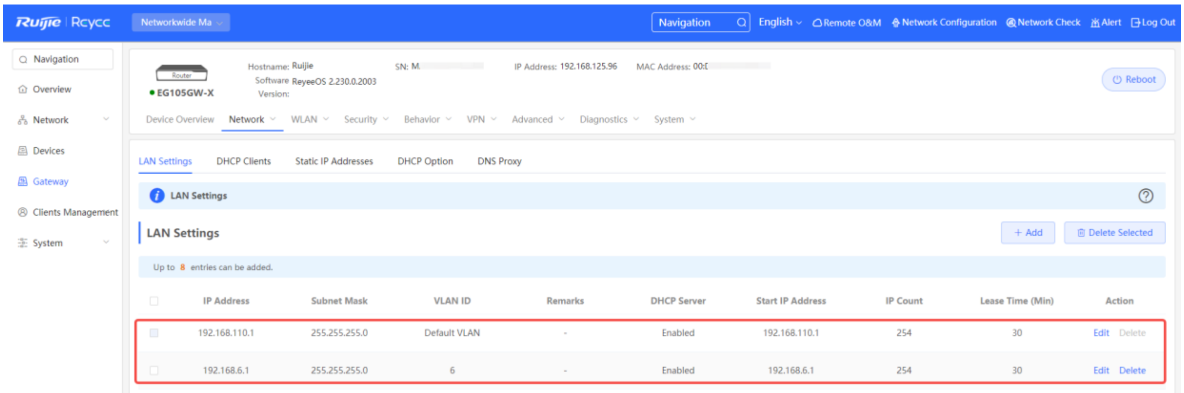
* Lease Time(Min): 30

DNS Server: 192.168.110.1



Add

* IP	192.168.6.1
* Subnet Mask	255.255.255.0
* VLAN ID	6
Remark	Remark
MAC	80:D0:F8:22:1B:B0
DHCP Server	●
* Start	192.168.6.1
* IP Count	254
* Lease Time(Min)	30
DNS Server	192.168.6.1



● EG105GW-X

Hostname: Ruijie
Software Version: ReyeeOS 2.230.0.2003
SN: M[redacted]
IP Address: 192.168.125.96
MAC Address: 00:[redacted]

LAN Settings

LAN Settings

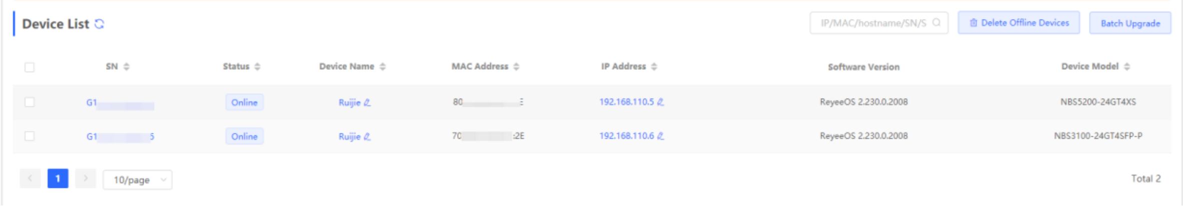
Up to 8 entries can be added.

□	IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	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**.



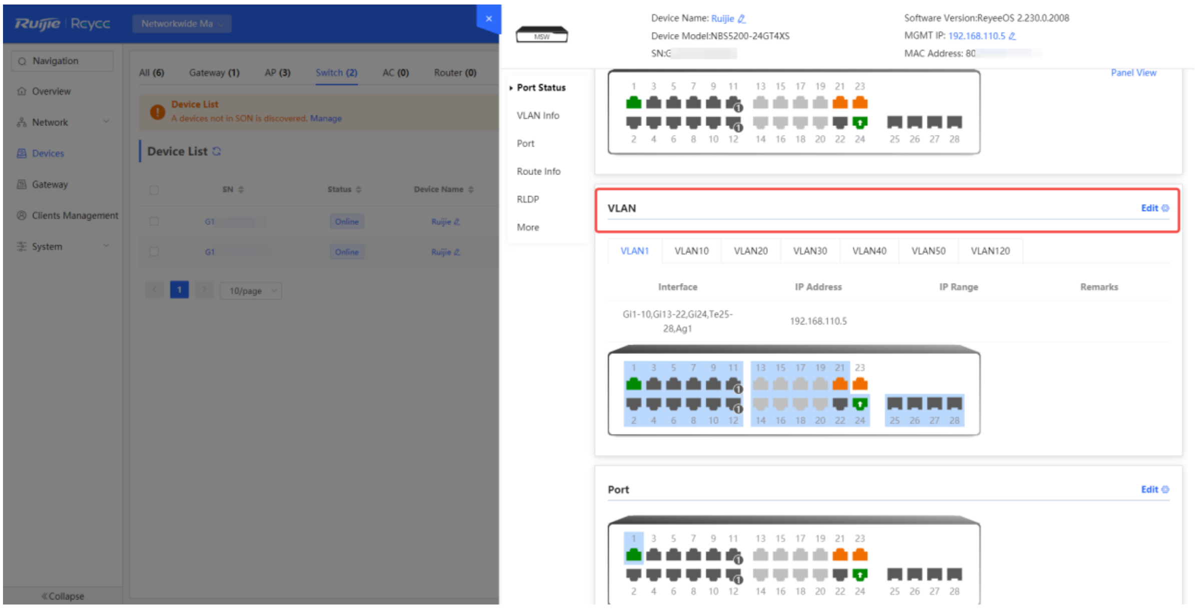
Device List

□	SN	Status	Device Name	MAC Address	IP Address	Software Version	Device Model
□	G1[redacted]	Online	Ruijie	80[redacted]E	192.168.110.5	ReyeeOS 2.230.0.2008	NBS5200-24GT4XS
□	G1[redacted]5	Online	Ruijie	70[redacted]:2E	192.168.110.6	ReyeeOS 2.230.0.2008	NBS3100-24GT4SFP-P

Total 2

(3) Select a device from **Device List** and access the configuration page.

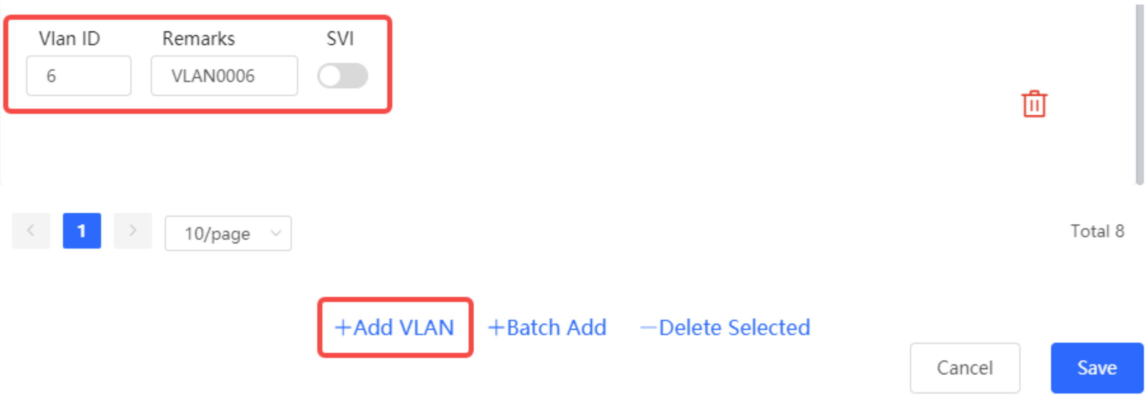
(4) In the **VLAN** pane, select a VLAN and click **Edit** to configure the VLAN.



Device Name: Ruijie
Device Model:NBS5200-24GT4XS
SN:G[redacted]
Software Version:ReyeeOS 2.230.0.2008
MGMT IP: 192.168.110.5
MAC Address: 80[redacted]

Interface	IP Address	IP Range	Remarks
Gi1-10,Gi13-22,Gi24,Te25-28,Ag1	192.168.110.5		

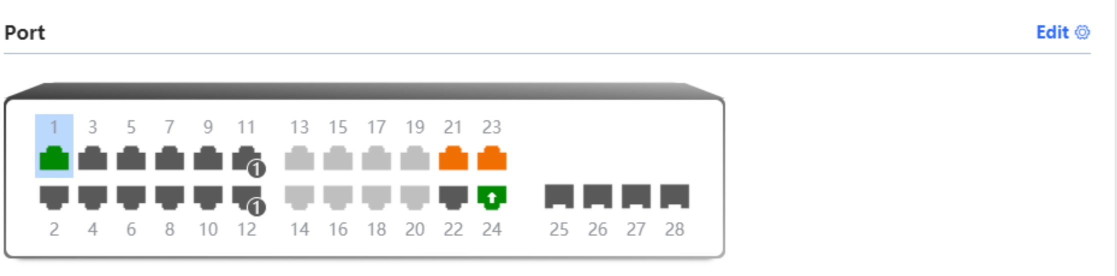
(5) Click **Add VLAN** to create VLAN 6 on the switch.

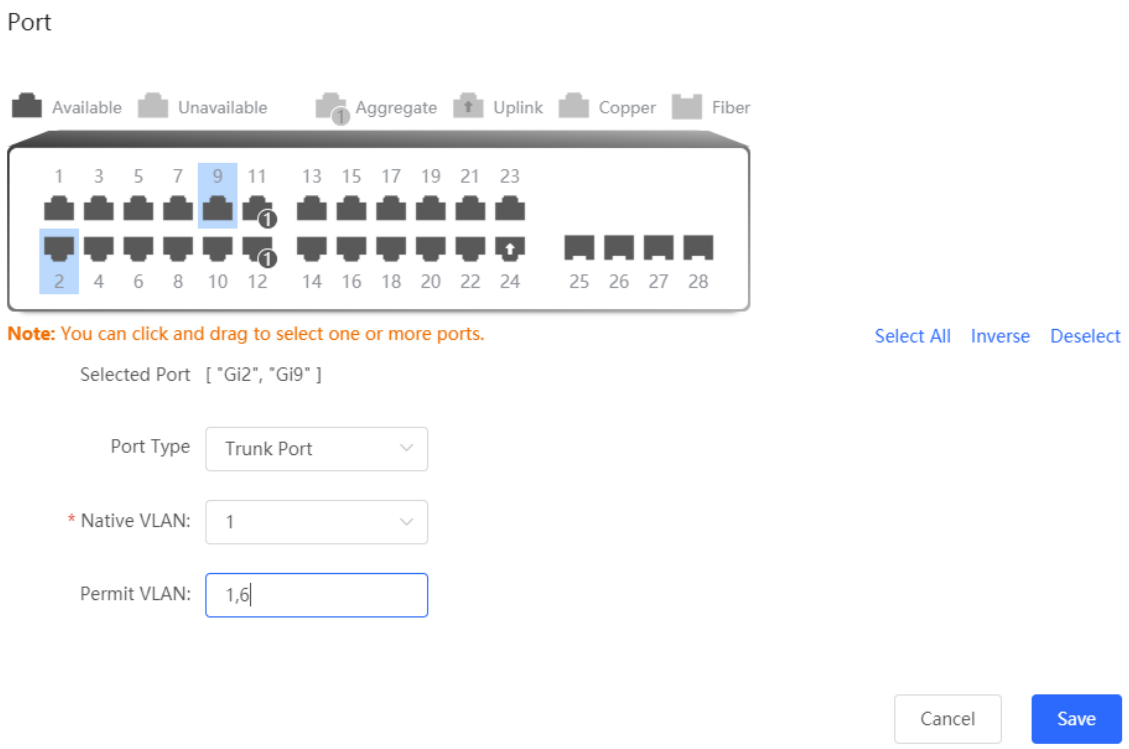


Vlan ID	Remarks	SVI
6	VLAN0006	○

Total 8

(6) 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.





Note: You can click and drag to select one or more ports.

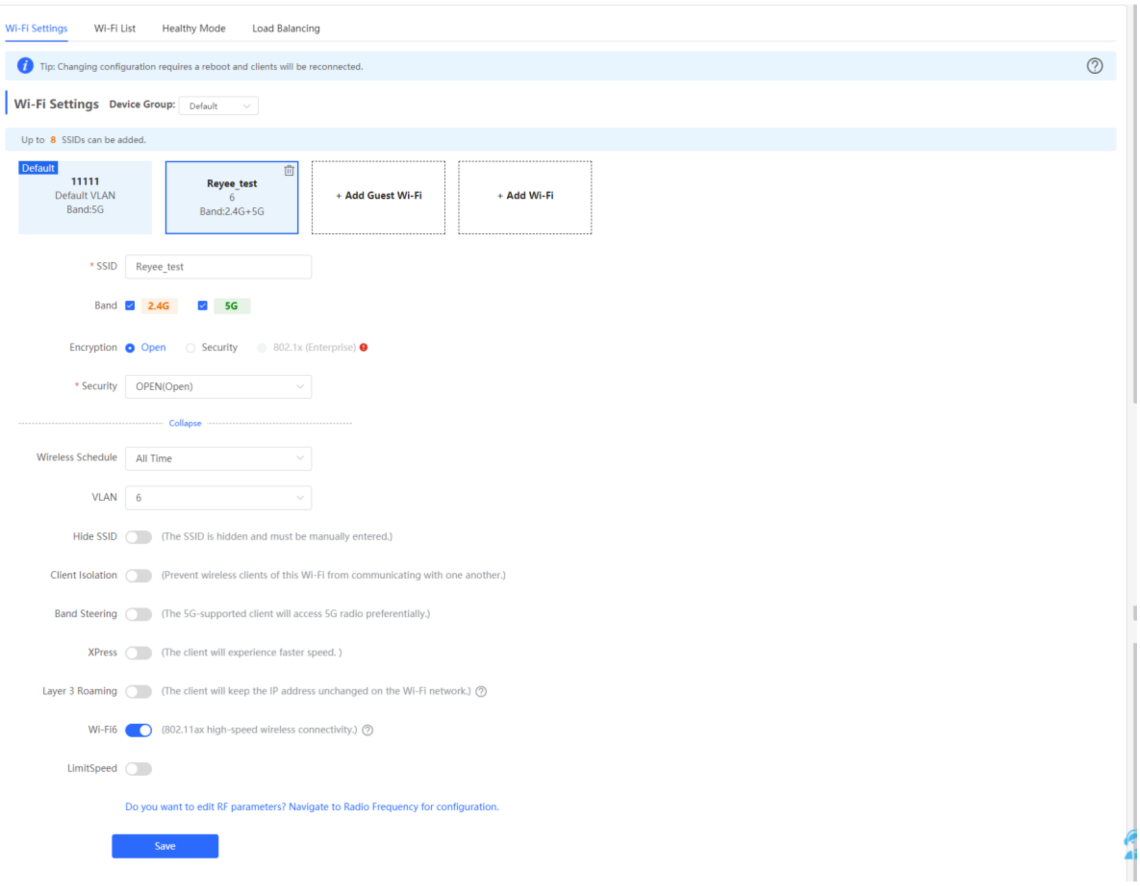
Selected Port ["Gi2", "Gi9"]

Port Type: Trunk Port

* Native VLAN: 1

Permit VLAN: 1,6

(7) 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.



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

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

* SSID: Reyee_test

Band: ☑ 2.4G ☑ 5G

Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(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.)

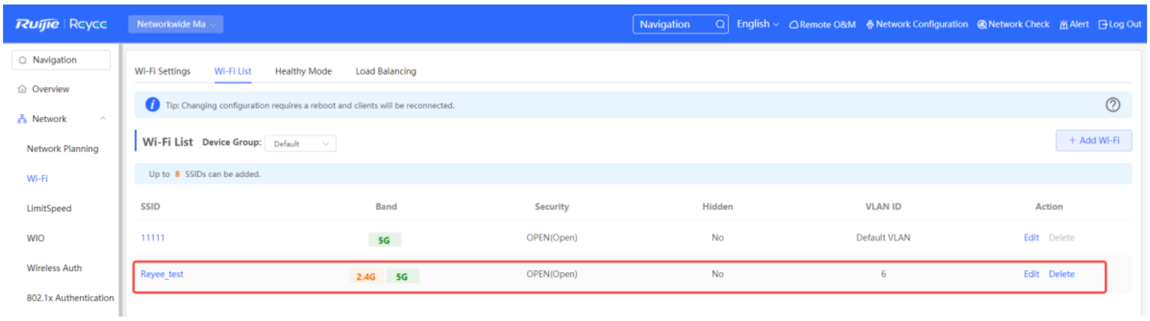
XPress (The client will experience faster speed.)

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

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

LimitSpeed

Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.



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

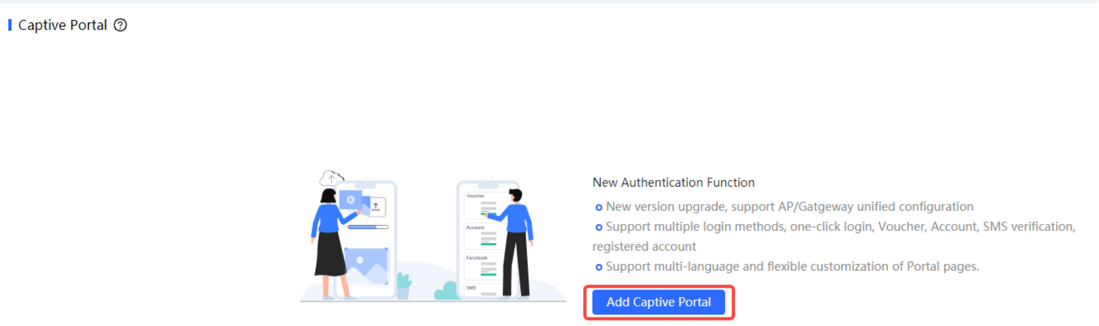
Wi-Fi List Device Group: Default + Add Wi-Fi

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
11111	5G	OPEN(Open)	No	Default VLAN	Edit Delete
Reyee_test	2.4G 5G	OPEN(Open)	No	6	Edit Delete

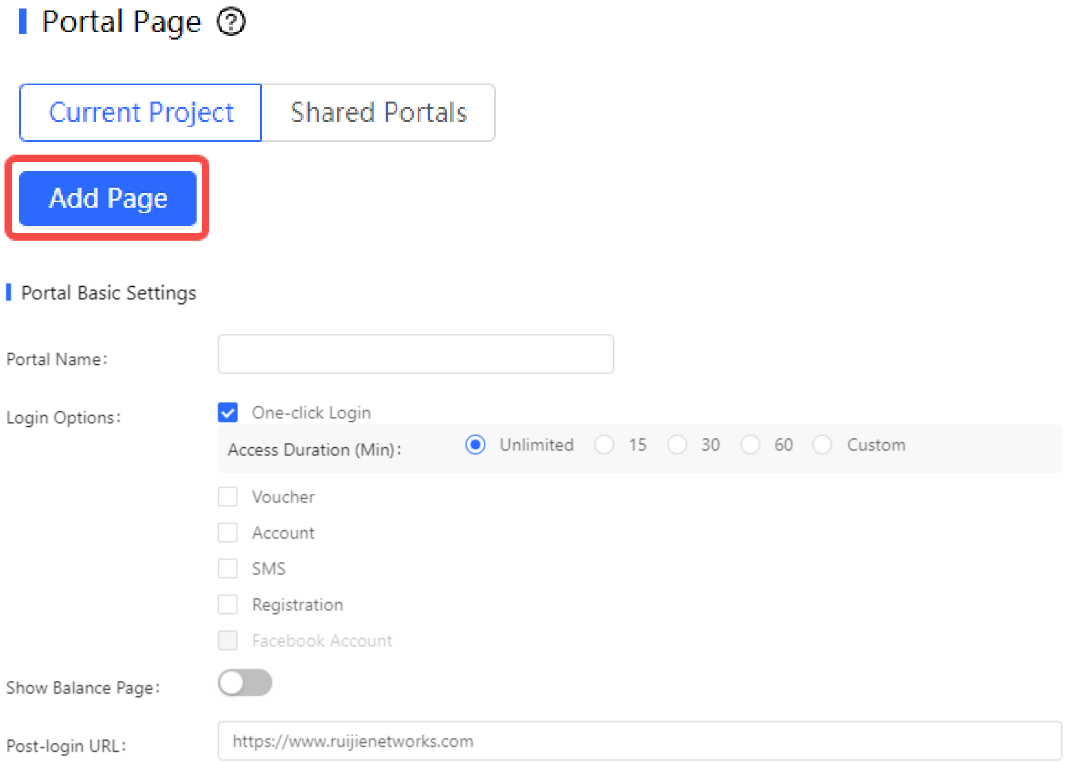
2. **Configure cloud authentication.**

(1) Login to Ruijie Cloud, choose **Configuration** > **Auth & Accounts > Authentication** > **Captive Portal** to access the captive portal page, and click **Add Page** to create a portal template and edit the captive portal template.



New Authentication Function

- New version upgrade, support AP/Gatgeway unified configuration
- Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account
- Support multi-language and flexible customization of Portal pages.



Portal Name:

Login Options: ☑ One-click Login

Access Duration (Min): ● Unlimited ○ 15 ○ 30 ○ 60 ○ Custom

□ Voucher

□ Account

□ SMS

□ Registration

□ Facebook Account

Show Balance Page:

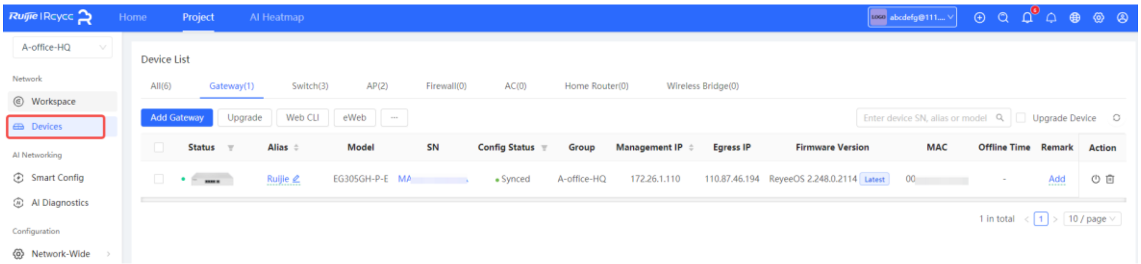
Post-login URL: https://www.ruijienetworks.com

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.

(2) Make sure that the Reyee EG is online on Ruijie Cloud.



Device List

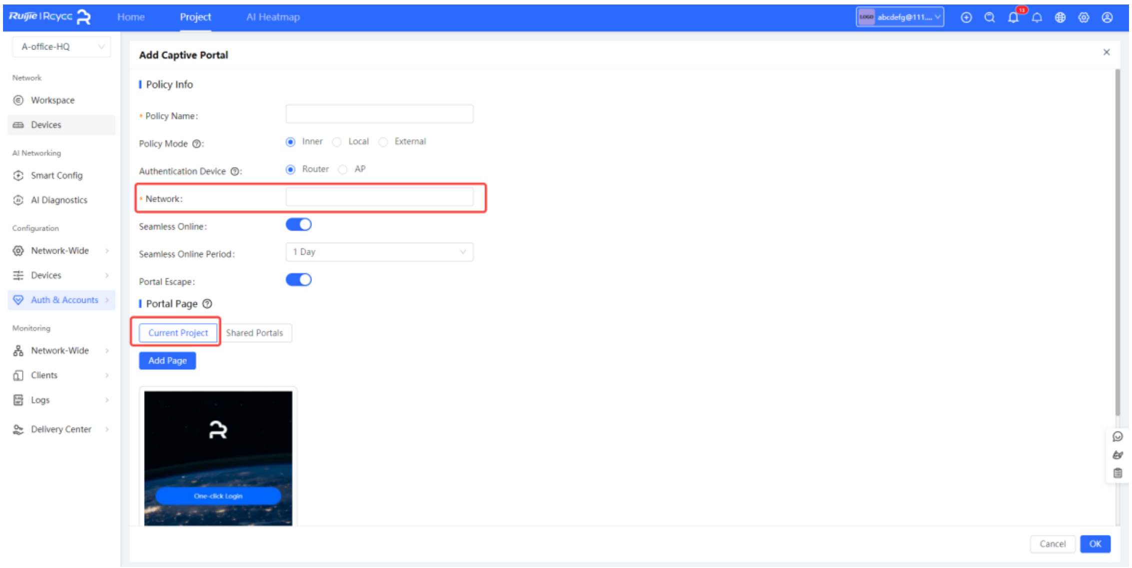
All(6) Gateway(1) Switch(3) AP(2) Firewall(0) AC(0) Home Router(0) Wireless Bridge(0)

Add Gateway | Upgrade | Web CLI | eWeb | ··· — Enter device SN, alias or model — □ Upgrade Device

	Status	Alias	Model	SN	Config Status	Group	Management IP	Egress IP	Firmware Version	MAC	Offline Time	Remark	Action
□	●	Ruijie	EG305GH-P-E	MA[redacted]	● Synced	A-office-HQ	172.26.1.110	110.87.46.194	ReyeeOS 2.248.0.2114 Latest	00[redacted]	-	Add	

1 in total < 1 > 10 / page

(3) Click **Add Captive Portal** to configure authentication on Ruijie Cloud. Set **Network** as **VLAN6** for authentication, and select a portal template to be used. Then click **OK** to save all configurations.



Add Captive Portal

Policy Info

* Policy Name:

Policy Mode: ● Inner ○ Local ○ External

Authentication Device: ● Router ○ AP

* Network:

Seamless Online: on

Seamless Online Period: 1 Day

Portal Escape: on

Portal Page

Current Project | Shared Portals

Add Page

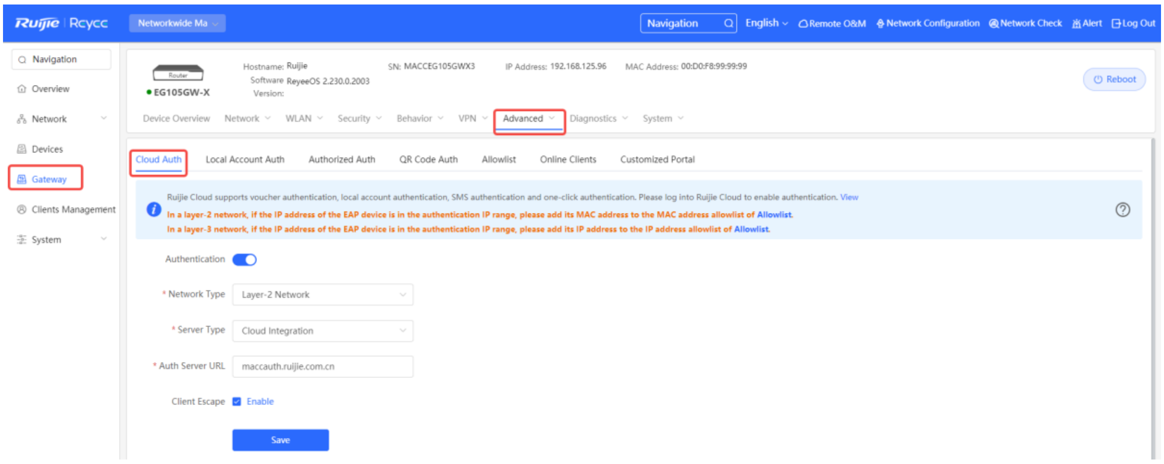
Cancel | OK

Note

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

6.2.4 Configuration Verification

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



Hostname: Ruijie
Software Version: ReyeeOS 2.230.0.2003
SN: MACCEG105GWX3
IP Address: 192.168.125.96
MAC Address: 00:D0:F8:99:99:99

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

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 allowlist of Allowlist.

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 allowlist of Allowlist.

Authentication: On

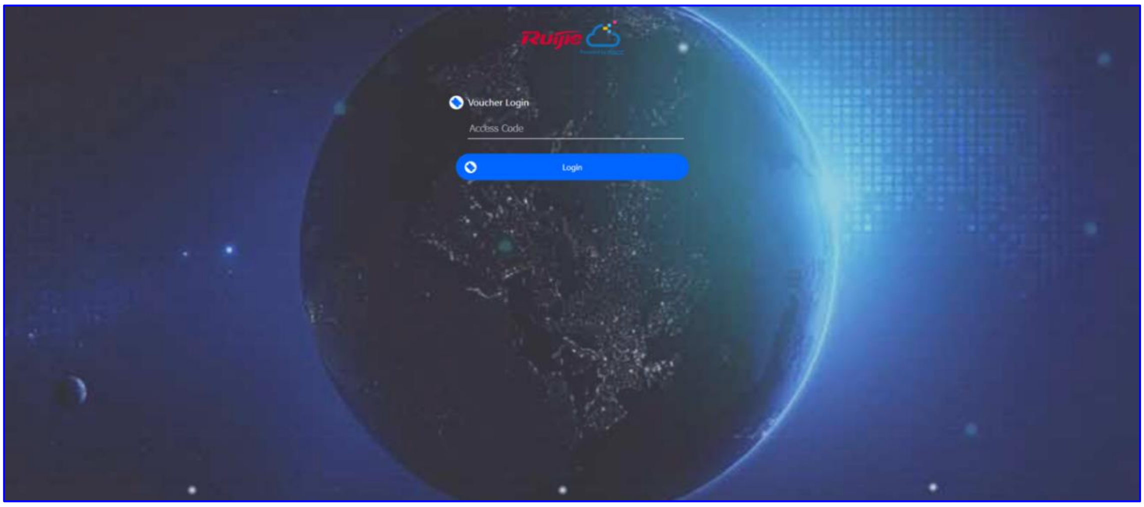
* Network Type: Layer-2 Network

* Server Type: Cloud Integration

* Auth Server URL: maccauth.ruijie.com.cn

Client Escape: ☑ Enable

(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.



6.3 Reyee Guest Wi-Fi Solution

6.3.1 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.

6.3.2 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.

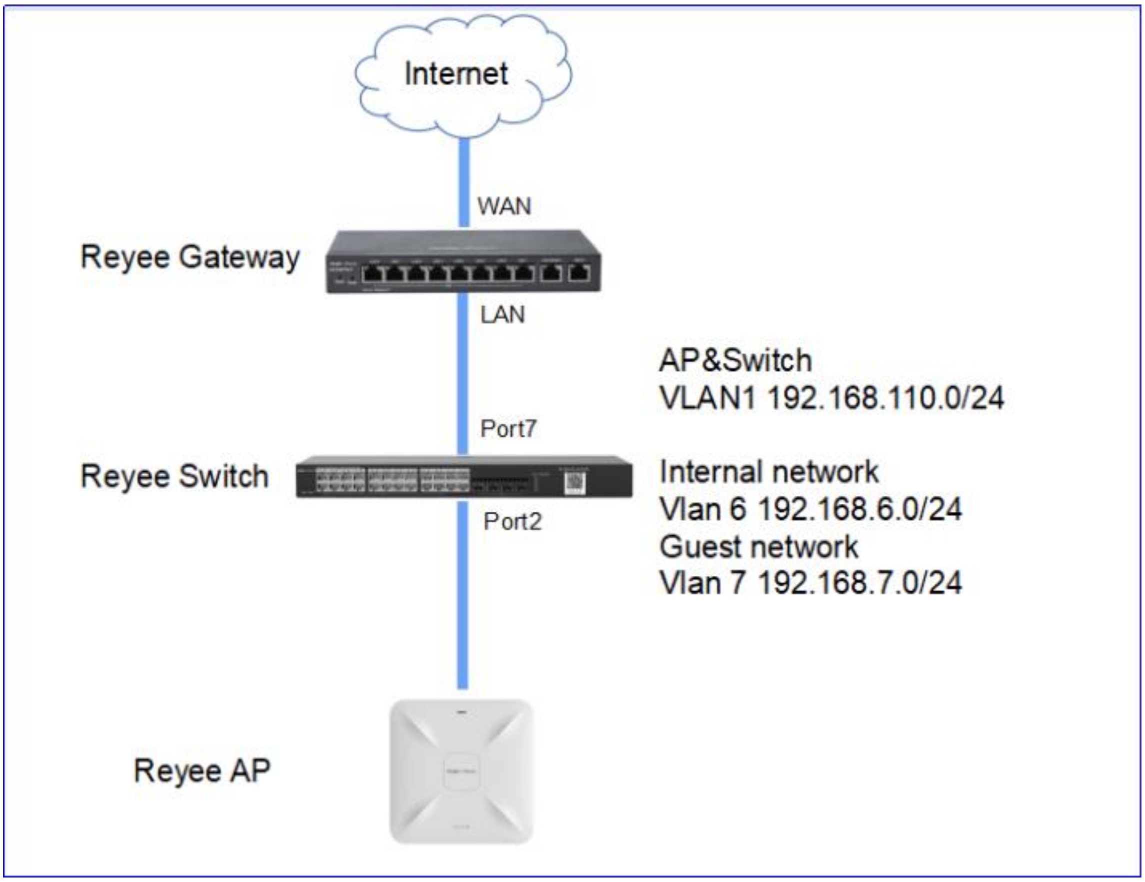
6.3.3 Configuration Example

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



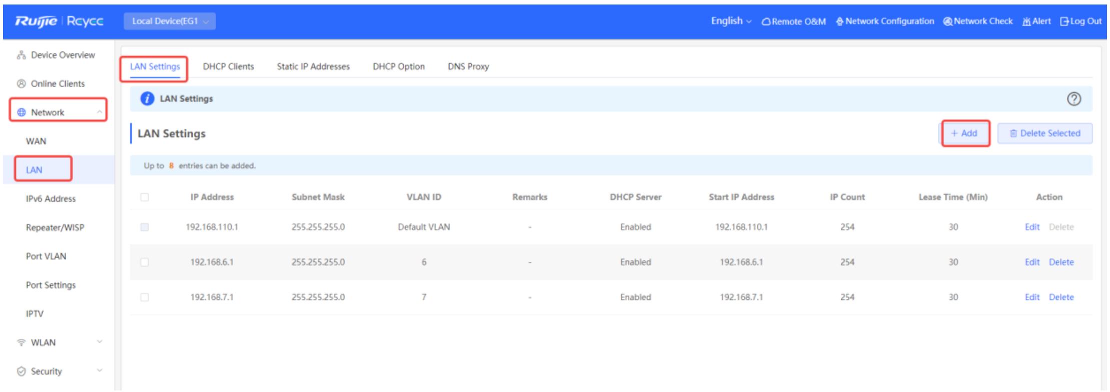
Network Description

- 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**.



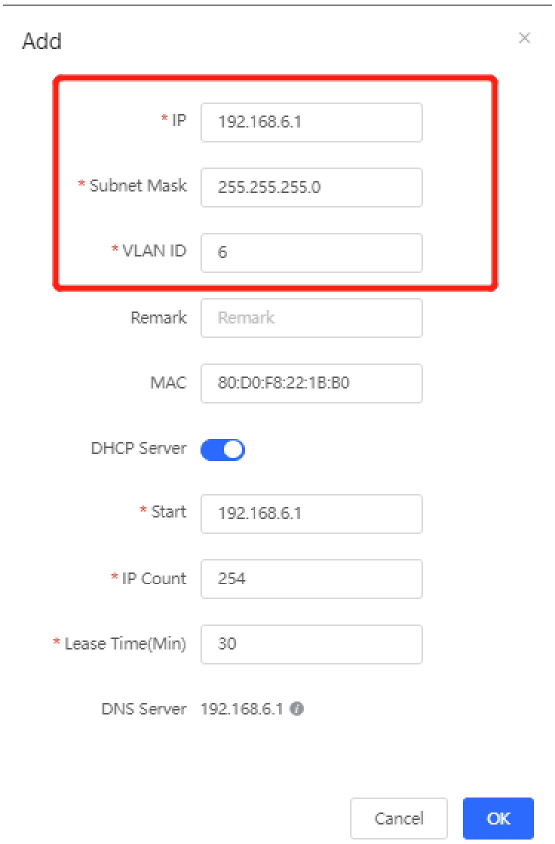
LAN Settings

LAN Settings

Up to 8 entries can be added.

□	IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
□	192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete

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



Add

* IP: 192.168.6.1

* Subnet Mask: 255.255.255.0

* VLAN ID: 6

Remark: Remark

MAC: 80:D0:F8:22:1B:B0

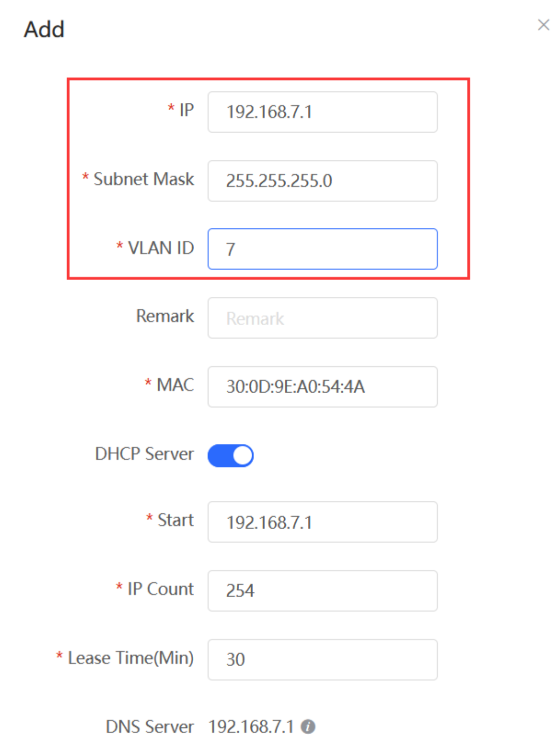
DHCP Server: on

* Start: 192.168.6.1

* IP Count: 254

* Lease Time(Min): 30

DNS Server: 192.168.6.1



Add

* IP: 192.168.7.1

* Subnet Mask: 255.255.255.0

* VLAN ID: 7

Remark: Remark

* MAC: 30:0D:9E:A0:54:4A

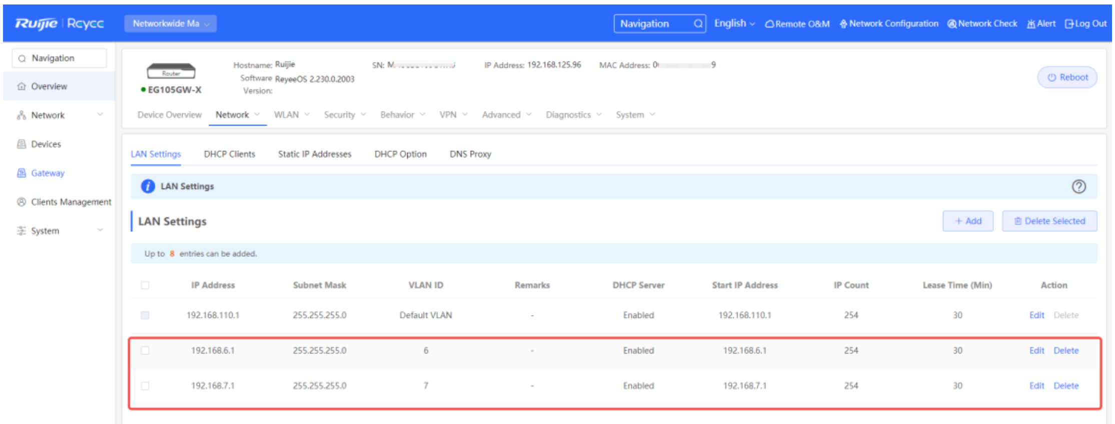
DHCP Server: on

* Start: 192.168.7.1

* IP Count: 254

* Lease Time(Min): 30

DNS Server: 192.168.7.1



● EG105GW-X
Hostname: Ruijie
Software Version: ReyeeOS 2.230.0.2003
SN: M[redacted]
IP Address: 192.168.125.96
MAC Address: 0[redacted]9

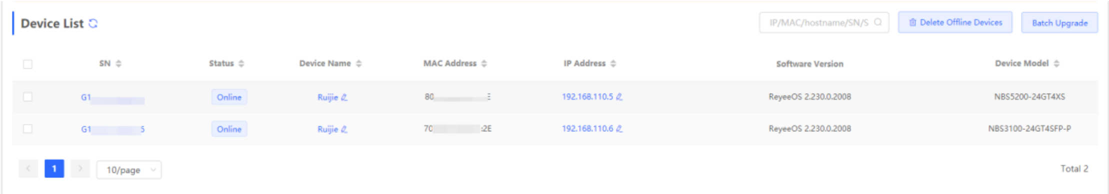
LAN Settings

Up to 8 entries can be added.

IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete

(2) Configure VLANs for a switch.

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



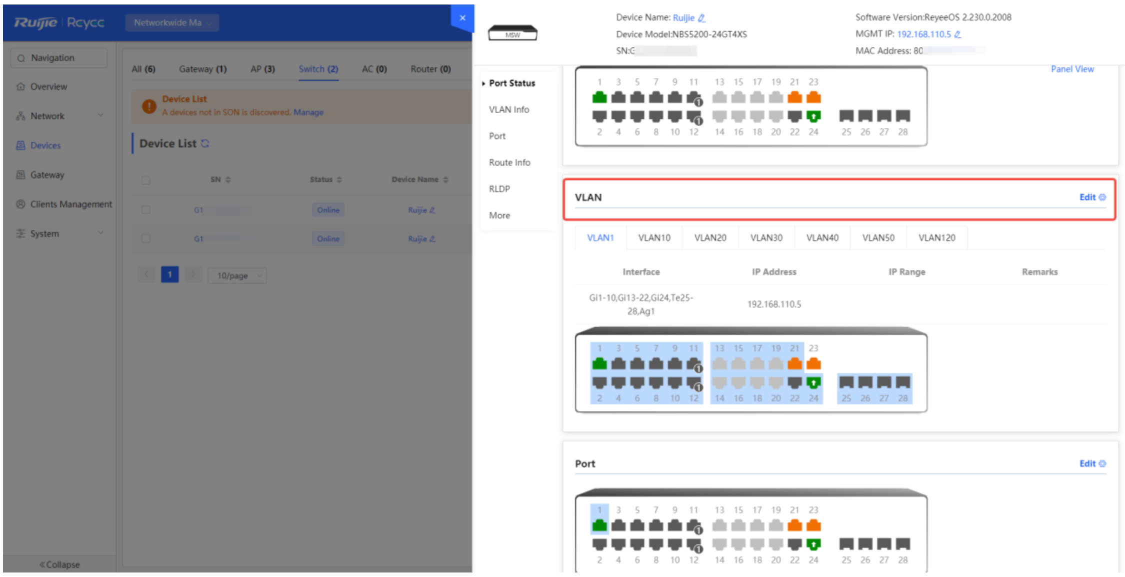
Device List

SN	Status	Device Name	MAC Address	IP Address	Software Version	Device Model
G1[redacted]	Online	Ruijie	80[redacted]E	192.168.110.5	ReyeeOS 2.230.0.2008	NBS5200-24GT4XS
G1[redacted]5	Online	Ruijie	70[redacted]2E	192.168.110.6	ReyeeOS 2.230.0.2008	NBS3100-24GT4SFP-P

1 10/page Total 2

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

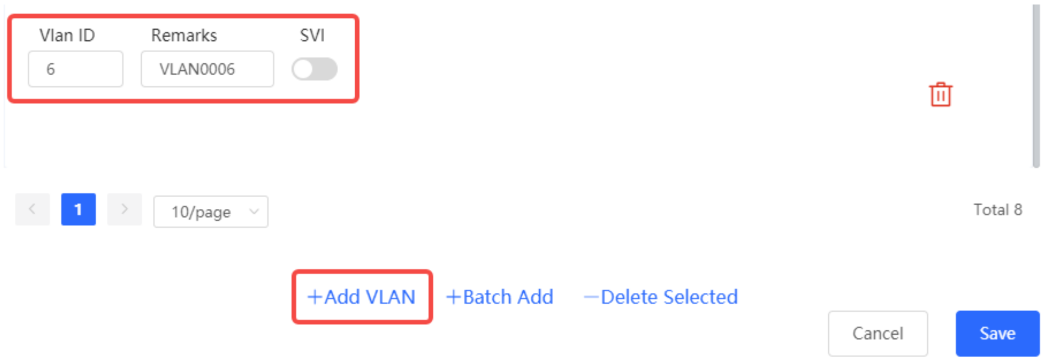
c In the **VLAN** pane, select a VLAN and click **Edit** to configure the VLAN.



Device Name: Ruijie
Device Model:NBS5200-24GT4XS
SN:G[redacted]
Software Version:ReyeeOS 2.230.0.2008
MGMT IP: 192.168.110.5
MAC Address: 80[redacted]

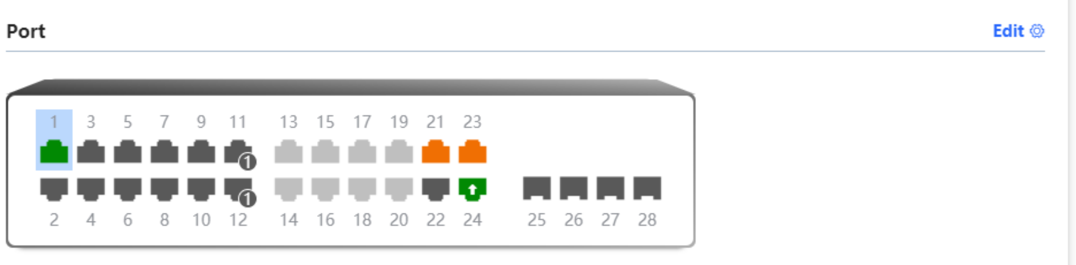
Interface	IP Address	IP Range	Remarks
Gi1-10,Gi13-22,Gi24,Te25-28,Ag1	192.168.110.5		

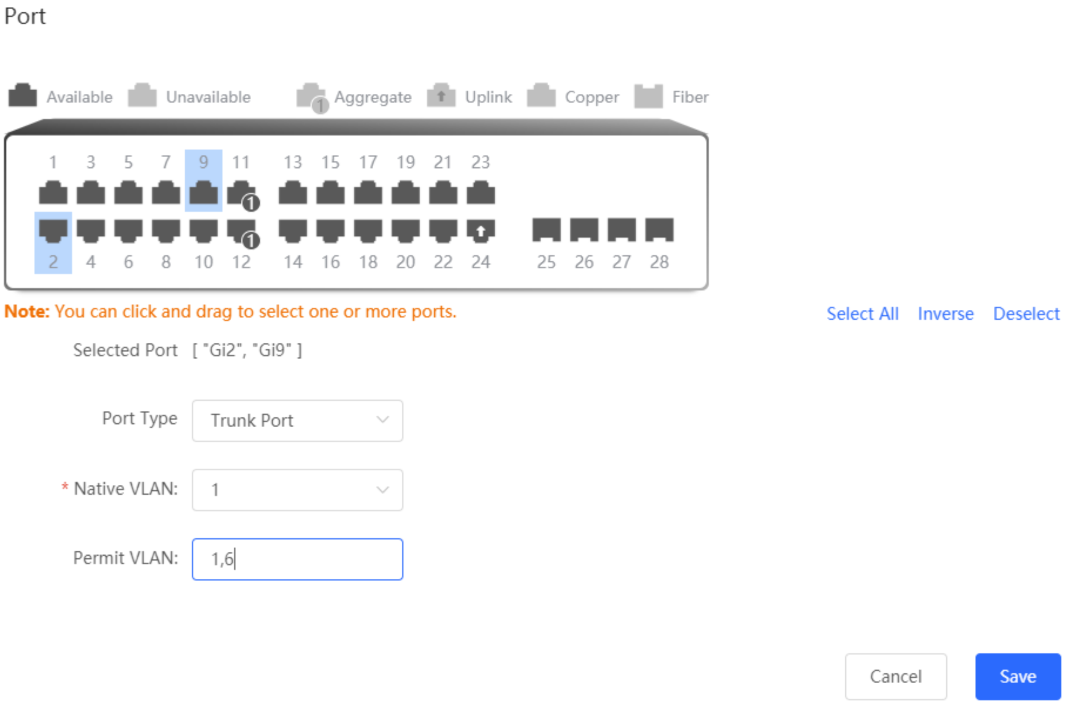
d Click **Add VLAN** to create VLAN 6 on the switch.



Vlan ID	Remarks	SVI
6	VLAN0006	○

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.





Note: You can click and drag to select one or more ports.

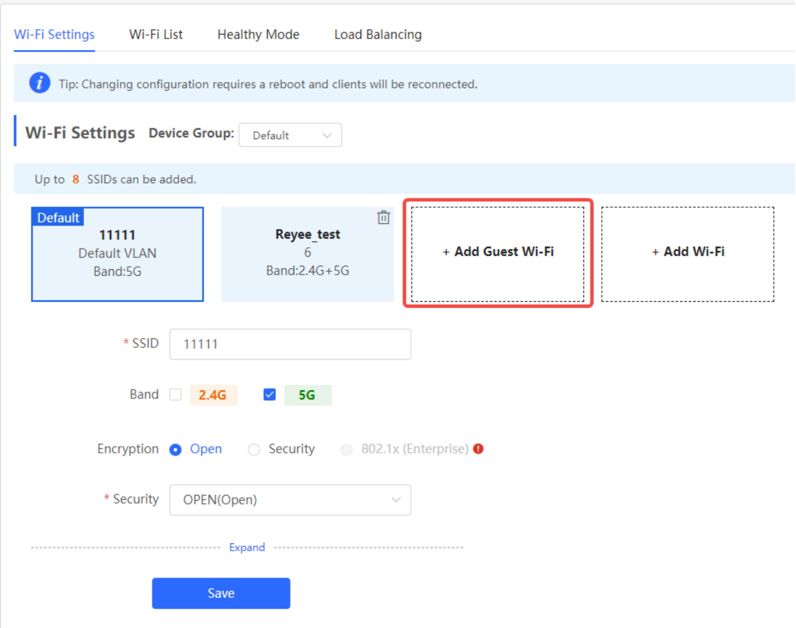
Selected Port ["Gi2", "Gi9"]

Port Type: Trunk Port

* Native VLAN: 1

Permit VLAN: 1,6

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



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

Wi-Fi Settings Device Group: Default

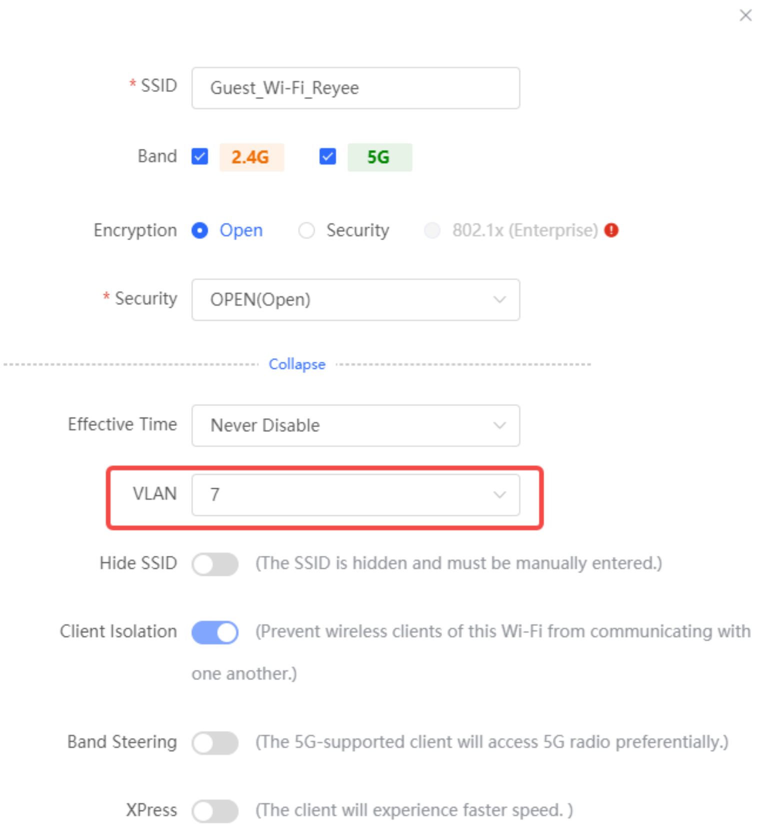
Up to 8 SSIDs can be added.

* SSID: 11111

Band: □ 2.4G ☑ 5G

Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(Open)



* SSID: Guest_Wi-Fi_Reyee

Band: ☑ 2.4G ☑ 5G

Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(Open)

Effective Time: Never Disable

VLAN: 7

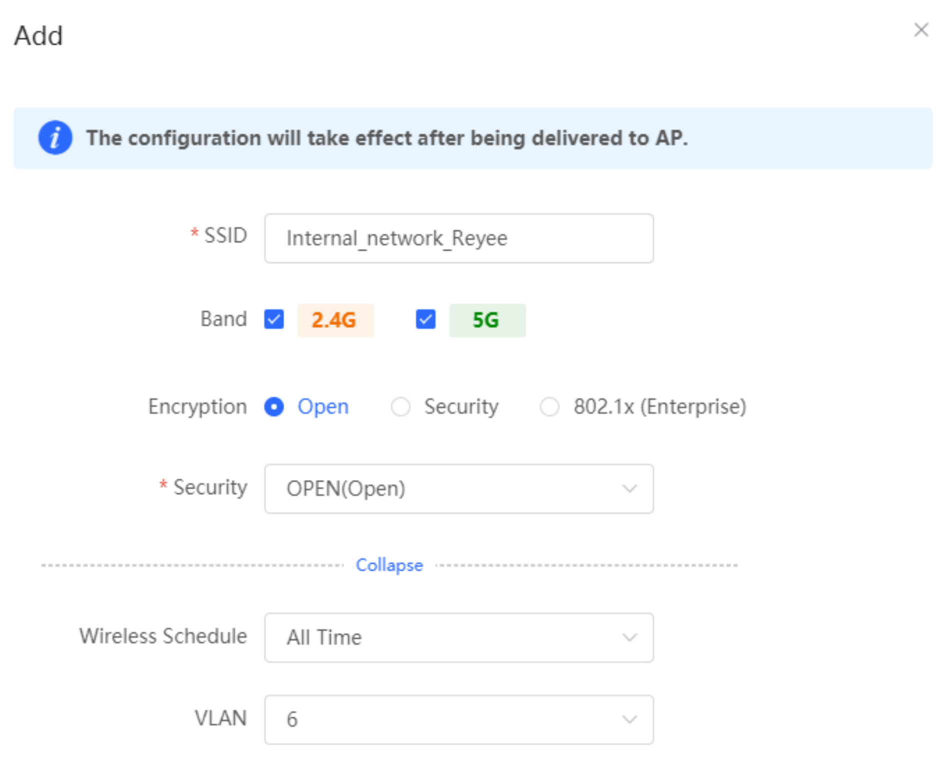
Hide SSID: off (The SSID is hidden and must be manually entered.)

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

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

XPress: off (The client will experience faster speed.)

(4) Choose **Network** > **Wi-Fi** > **Wi-Fi List** > **Add Wi-Fi**, 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

The configuration will take effect after being delivered to AP.

* SSID: Internal_network_Reyee

Band: ☑ 2.4G ☑ 5G

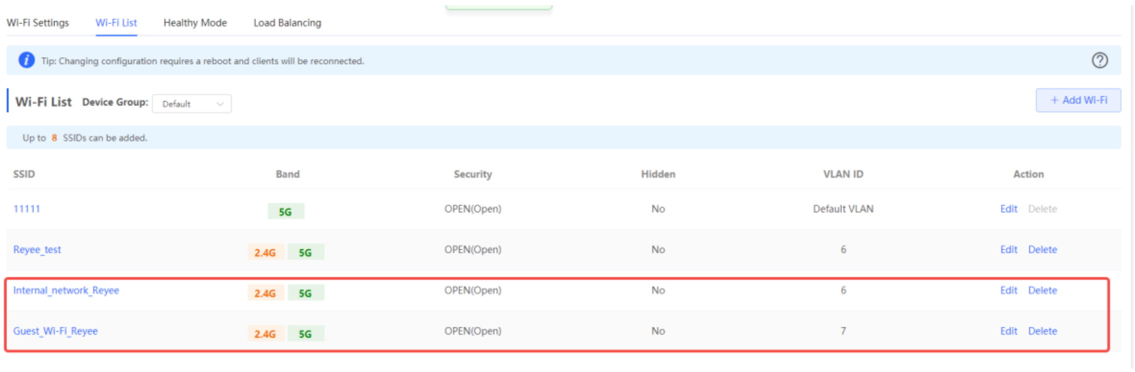
Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(Open)

Collapse

Wireless Schedule: All Time

VLAN: 6



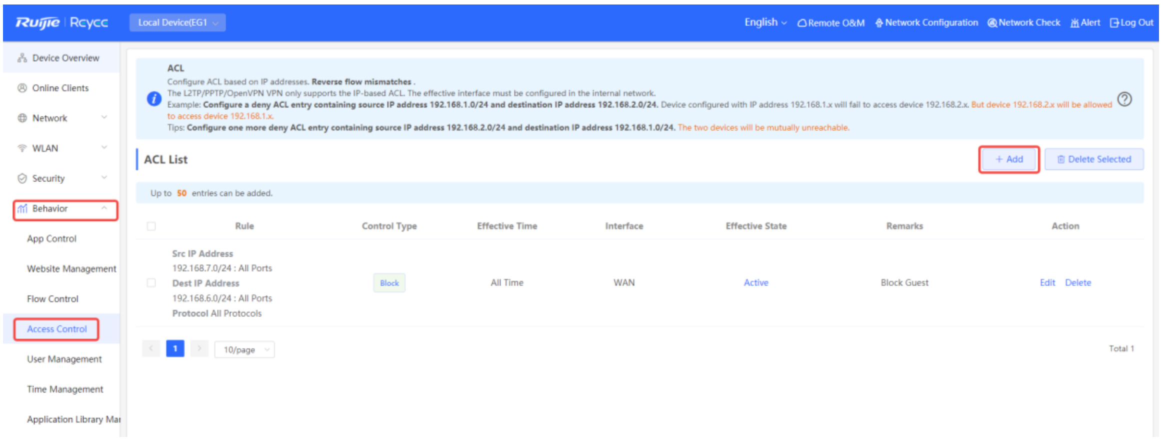
Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
11111	5G	OPEN(Open)	No	Default VLAN	Edit Delete
Reyee_test	2.4G 5G	OPEN(Open)	No	6	Edit Delete
Internal_network_Reyee	2.4G 5G	OPEN(Open)	No	6	Edit Delete
Guest_Wi-Fi_Reyee	2.4G 5G	OPEN(Open)	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.



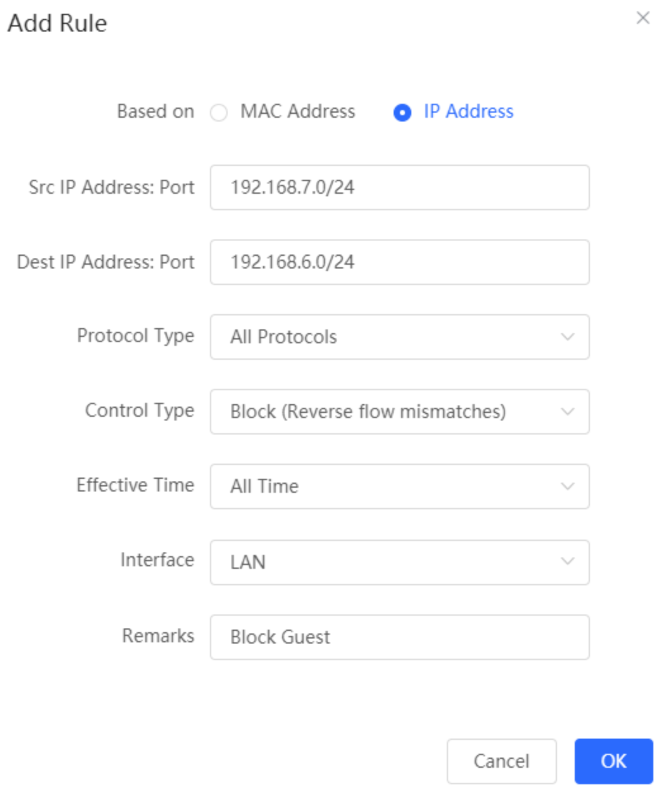
ACL
Configure ACL based on IP addresses. **Reverse flow mismatches .**
The L2TP/PPTP/OpenVPN VPN only supports the IP-based ACL. The effective interface must be configured in the internal network.
Example: **Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 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.
Tips: **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

Up to 50 entries can be added.

□	Rule	Control Type	Effective Time	Interface	Effective State	Remarks	Action
□	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	WAN	Active	Block Guest	Edit Delete

1 10/page Total 1



Add Rule

Based on ○ MAC Address ● IP Address

Src IP Address: Port: 192.168.7.0/24

Dest IP Address: Port: 192.168.6.0/24

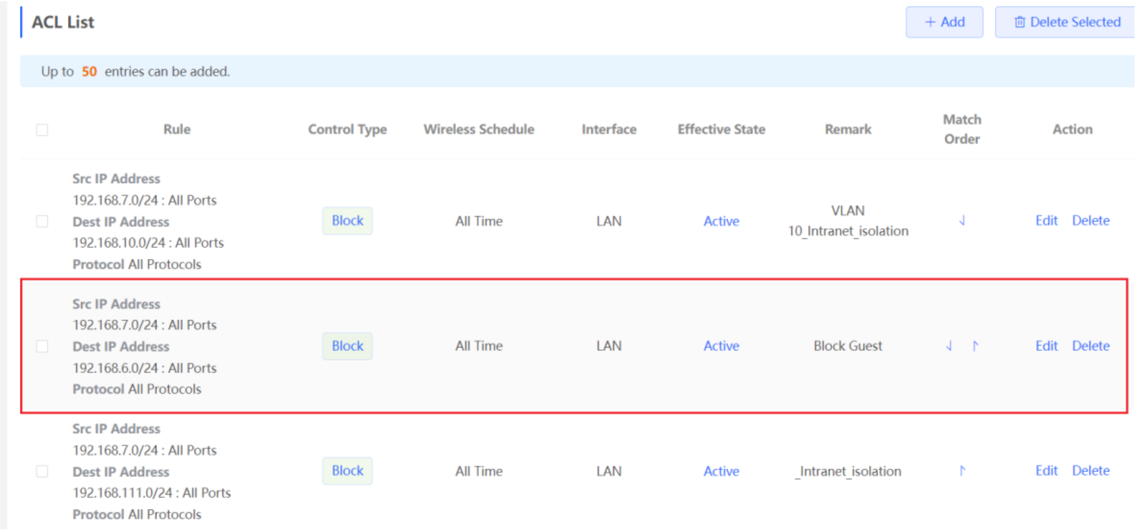
Protocol Type: All Protocols

Control Type: Block (Reverse flow mismatches)

Effective Time: All Time

Interface: LAN

Remarks: Block Guest



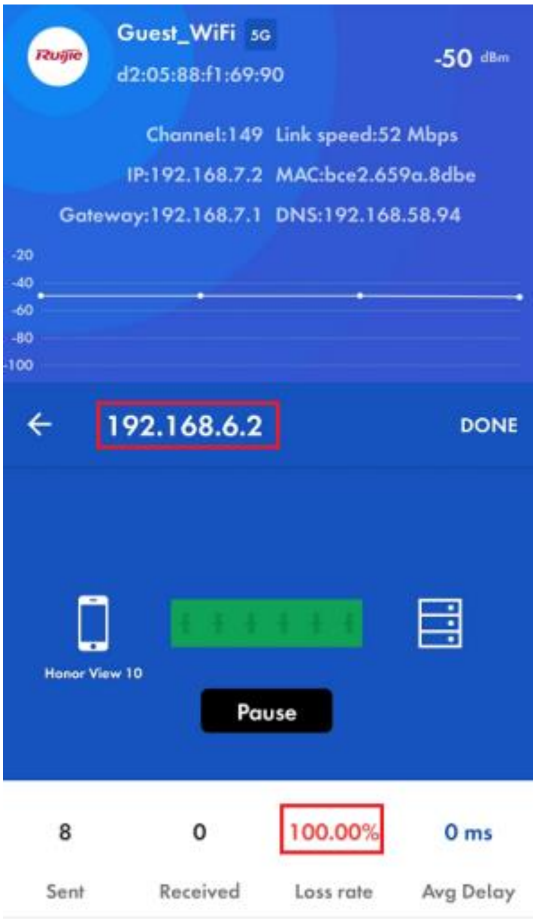
ACL List

Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
□	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
□	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
□	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.



Guest_WiFi 5G
d2:05:88:f1:69:90
-50 dBm
Channel:149 Link speed:52 Mbps
IP:192.168.7.2 MAC:bce2.659a.8dbe
Gateway:192.168.7.1 DNS:192.168.58.94

192.168.6.2

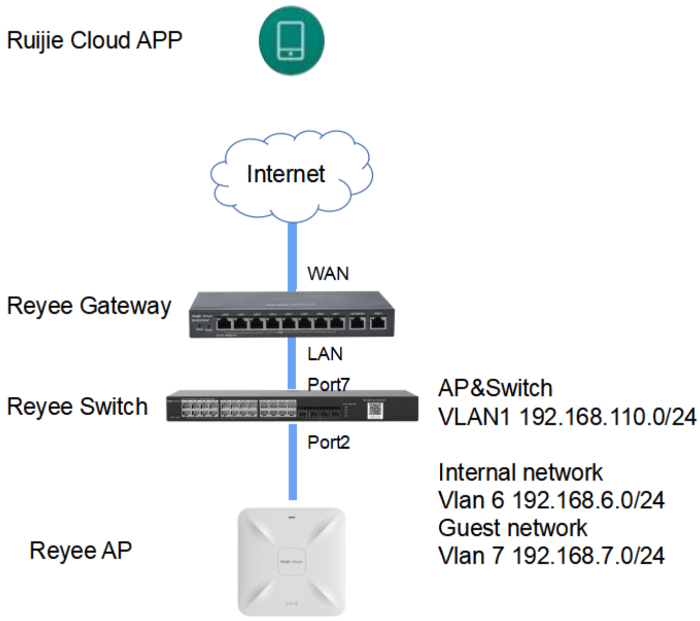
8	0	100.00%	0 ms
Sent	Received	Loss rate	Avg Delay

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

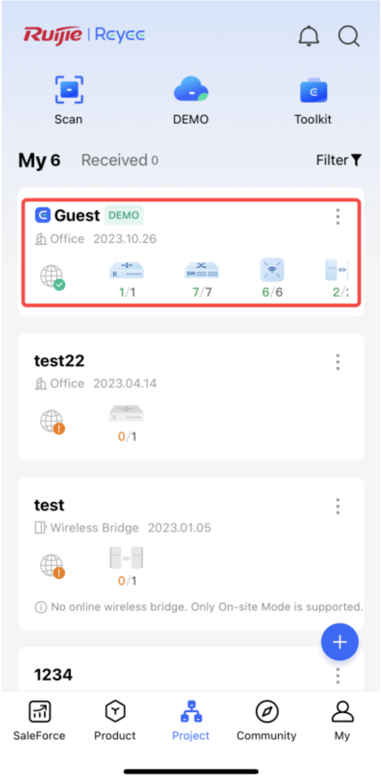


Network Description

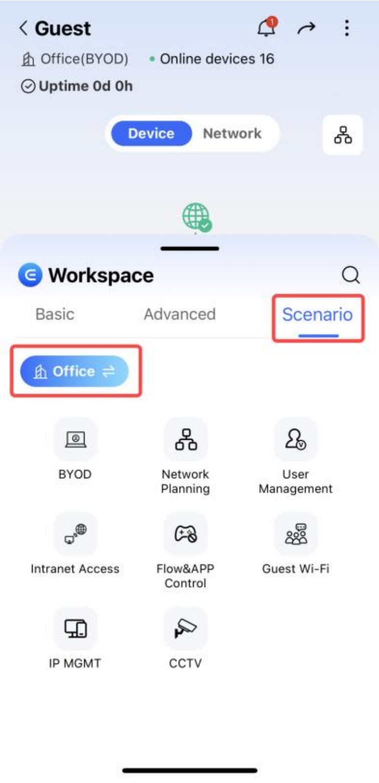
- The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.
- The Reyee AP and switch obtain IP addresses on the network segment of VLAN 1 for Internet access.
- Internal users obtain IP addresses on the network segment of VLAN 6 for Internet access and guests obtain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

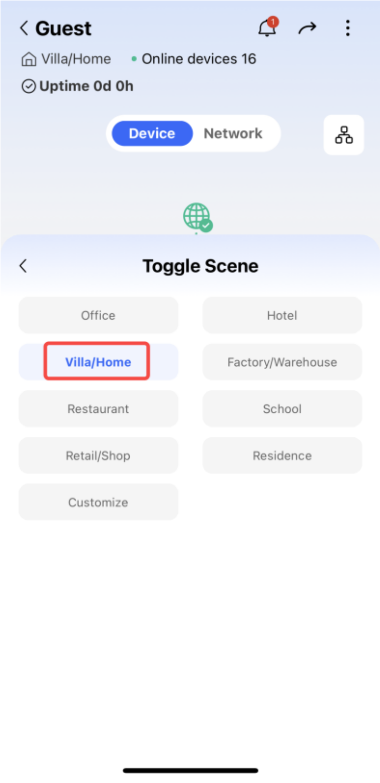
Configuration Steps

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

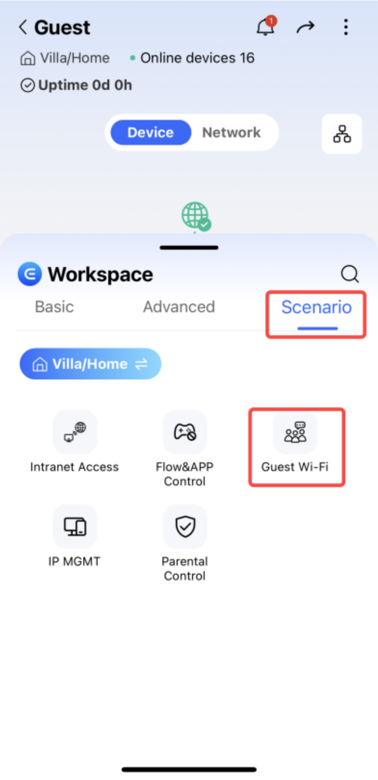


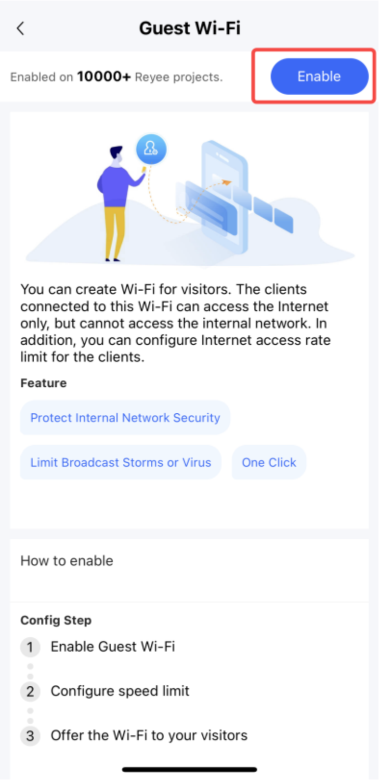
(2) Select **Villa/Home** under **Scenario**. You can see the **Guest Wi-Fi** button.





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





Enabled on **10000+** Reyee projects.

You can create Wi-Fi for visitors. The clients connected to this Wi-Fi can access the Internet only, but cannot access the internal network. In addition, you can configure Internet access rate limit for the clients.

Feature

Protect Internal Network Security

Limit Broadcast Storms or Virus

One Click

How to enable

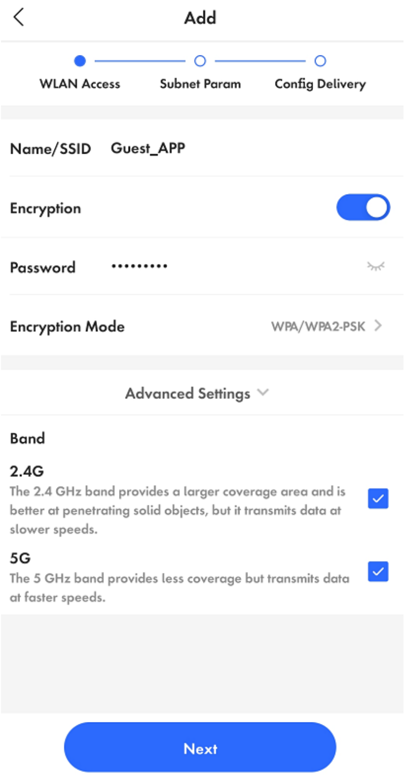
Config Step

1 Enable Guest Wi-Fi

2 Configure speed limit

3 Offer the Wi-Fi to your visitors

(4) 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.



Name/SSID Guest_APP

Encryption

Password •••••••••

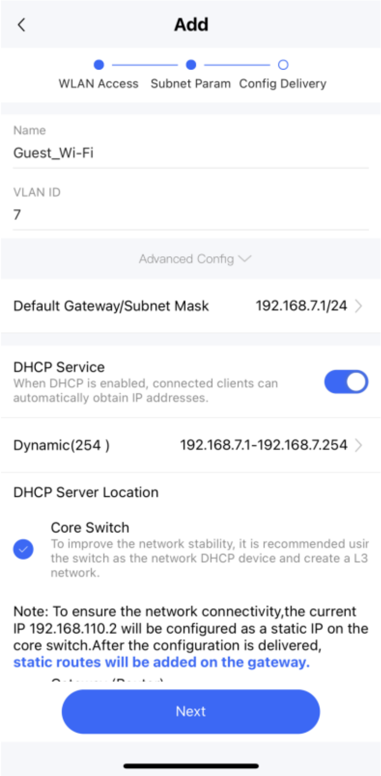
Encryption Mode WPA/WPA2-PSK

Advanced Settings

Band

2.4G
The 2.4 GHz band provides a larger coverage area and is better at penetrating solid objects, but it transmits data at slower speeds. ☑

5G
The 5 GHz band provides less coverage but transmits data at faster speeds. ☑



Name
Guest_Wi-Fi

VLAN ID
7

Default Gateway/Subnet Mask 192.168.7.1/24

DHCP Service
When DHCP is enabled, connected clients can automatically obtain IP addresses.

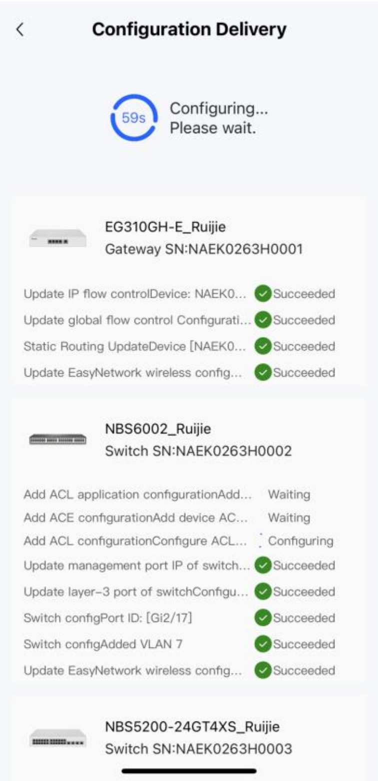
Dynamic(254) 192.168.7.1-192.168.7.254

DHCP Server Location

● Core Switch
To improve the network stability, it is recommended usir the switch as the network DHCP device and create a L3 network.

Note: To ensure the network connectivity,the current IP 192.168.110.2 will be configured as a static IP on the core switch.After the configuration is delivered, static routes will be added on the gateway.

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



Configuring...
Please wait.

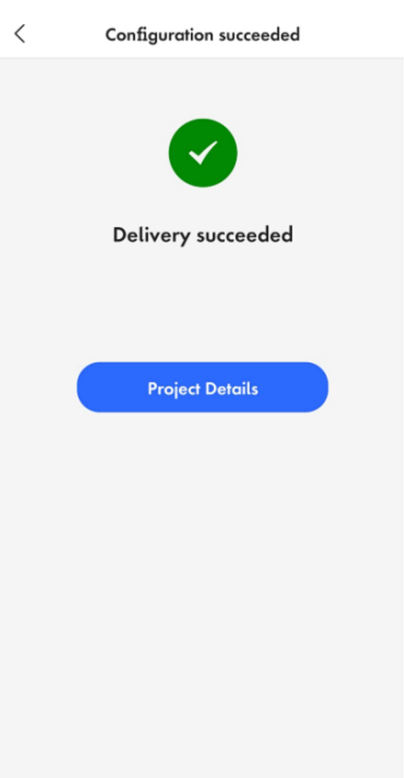
EG310GH-E_Ruijie
Gateway SN:NAEK0263H0001

Update IP flow controlDevice: NAEK0... Succeeded
Update global flow control Configurati... Succeeded
Static Routing UpdateDevice [NAEK0... Succeeded
Update EasyNetwork wireless config... Succeeded

NBS6002_Ruijie
Switch SN:NAEK0263H0002

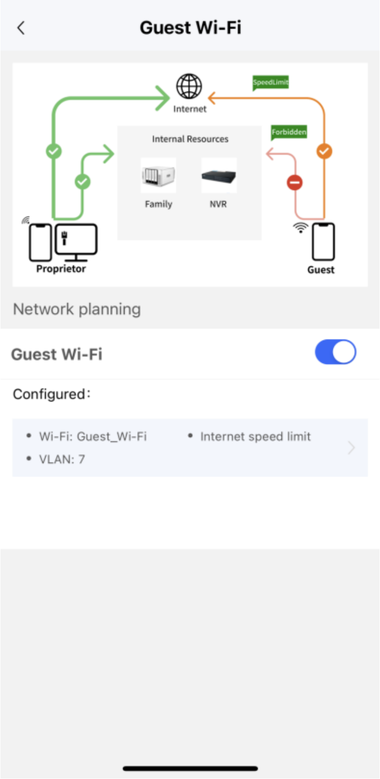
Add ACL application configurationAdd... Waiting
Add ACE configurationAdd device AC... Waiting
Add ACL configurationConfigure ACL... Configuring
Update management port IP of switch... Succeeded
Update layer-3 port of switchConfigu... Succeeded
Switch configPort ID: [Gi2/17] Succeeded
Switch configAdded VLAN 7 Succeeded
Update EasyNetwork wireless config... Succeeded

NBS5200-24GT4XS_Ruijie
Switch SN:NAEK0263H0003



Configuration succeeded

Delivery succeeded



Guest Wi-Fi

Network planning

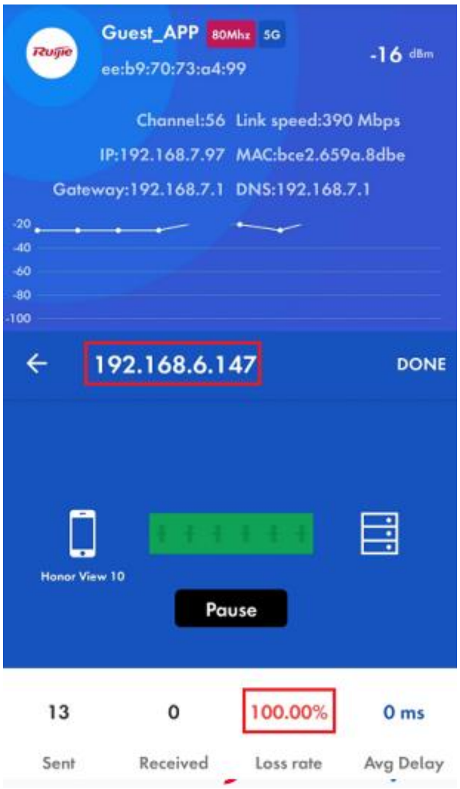
Guest Wi-Fi

Configured:

- Wi-Fi: Guest_Wi-Fi
- VLAN: 7
- Internet speed limit

Configuration Verification

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



Guest_APP 80Mhz 5G

ee:b9:70:73:a4:99

-16 dBm

Channel:56 Link speed:390 Mbps

IP:192.168.7.97 MAC:bce2.659a.8dbe

Gateway:192.168.7.1 DNS:192.168.7.1

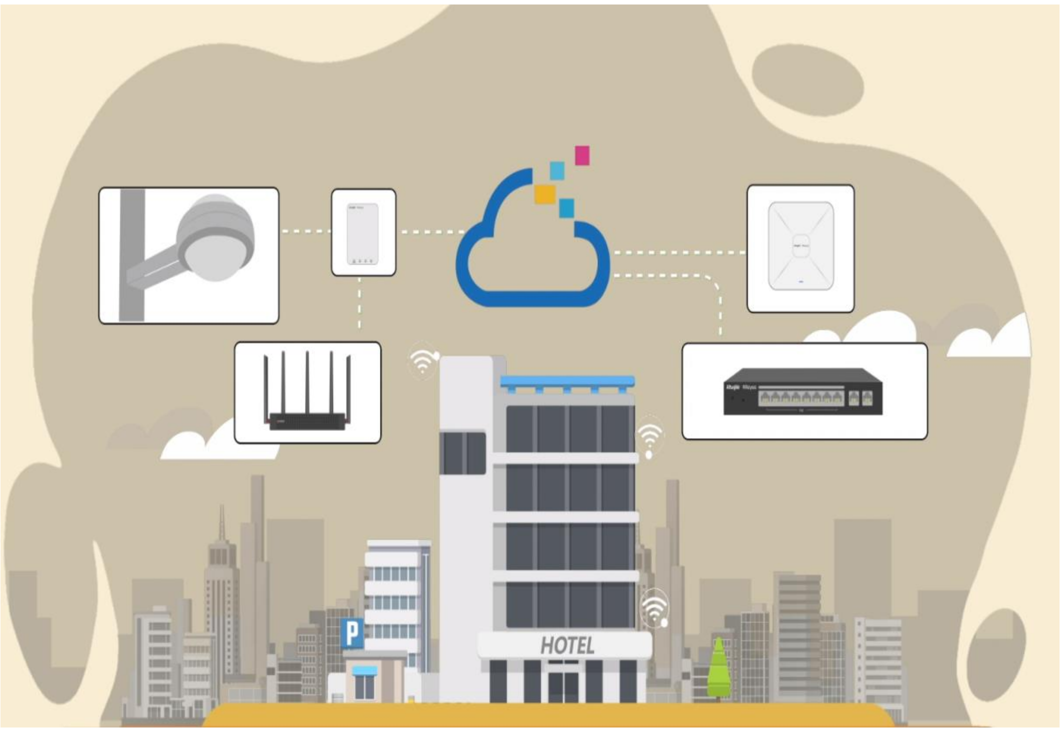
192.168.6.147

13	0	100.00%	0 ms
Sent	Received	Loss rate	Avg Delay

6.4 Reyee Economic Hotel Network Solution

6.4.1 Application Scenario

Reyee 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 Mbps at 2.4GHz, 1201 Mbps at 5 GHz, and up to 1775 Mbps per AP. The wall AP provides a LAN port at the front to facilitate the expansion of IPTV terminals, IP phones, and other terminals.

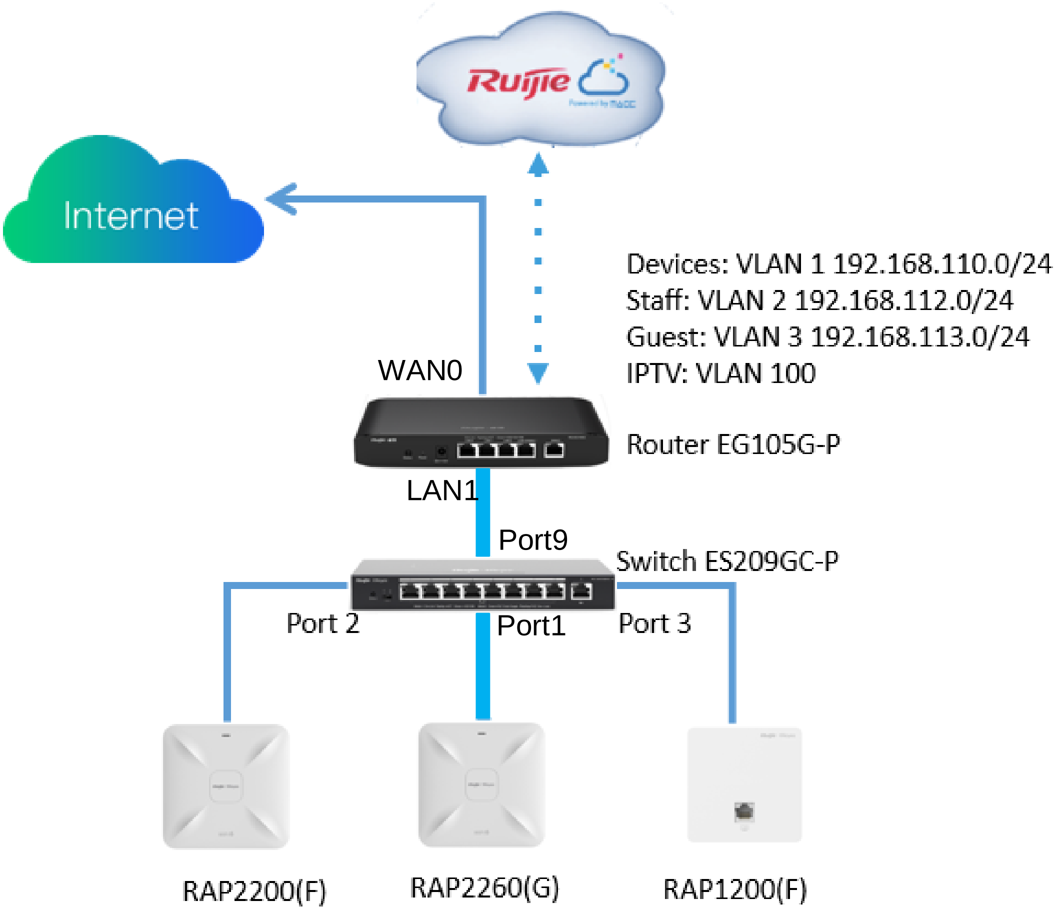


6.4.2 Configuration Example

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



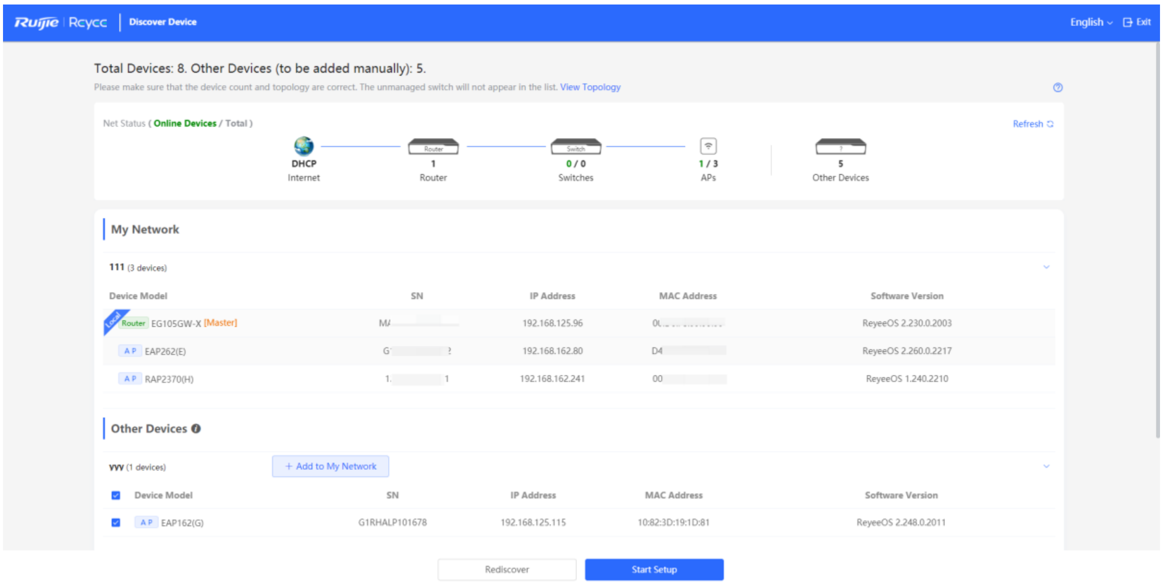
Devices List

Type	Model	Function
Router	EG105G-P	● 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.



Total Devices: 8. Other Devices (to be added manually): 5.

Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list. View Topology

Net Status (Online Devices / Total)

DHCP	1	0 / 0	1 / 3	5
Internet	Router	Switches	APs	Other Devices

My Network

111 (3 devices)

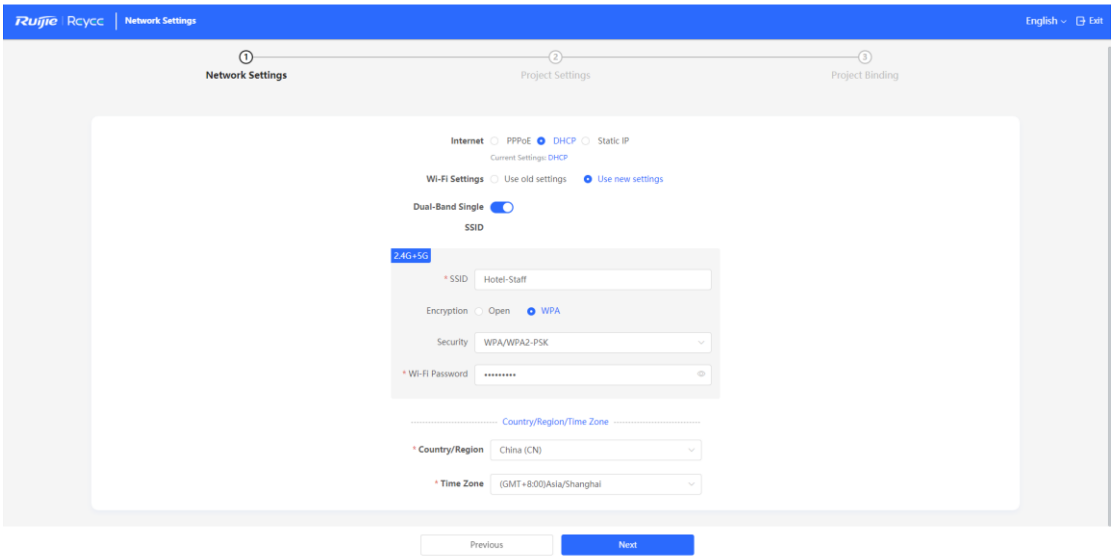
Device Model	SN	IP Address	MAC Address	Software Version
Local Router EG105GW-X [Master]	[redacted]	192.168.125.96	[redacted]	ReyeeOS 2.230.0.2003
A P EAP262(E)	[redacted]	192.168.162.80	[redacted]	ReyeeOS 2.260.0.2217
A P RAP2370(H)	[redacted]	192.168.162.241	[redacted]	ReyeeOS 1.240.2210

Other Devices

yyy (1 devices) + Add to My Network

☑ Device Model	SN	IP Address	MAC Address	Software Version
☑ A P EAP162(G)	G1RHALP101678	192.168.125.115	10:82:3D:19:1D:81	ReyeeOS 2.248.0.2011

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



Internet ○ PPPoE ● DHCP ○ Static IP

Current Settings: DHCP

Wi-Fi Settings ○ Use old settings ● Use new settings

Dual-Band Single SSID ●

2.4G+5G

* SSID: Hotel-Staff

Encryption ○ Open ● WPA

Security: WPA/WPA2-PSK

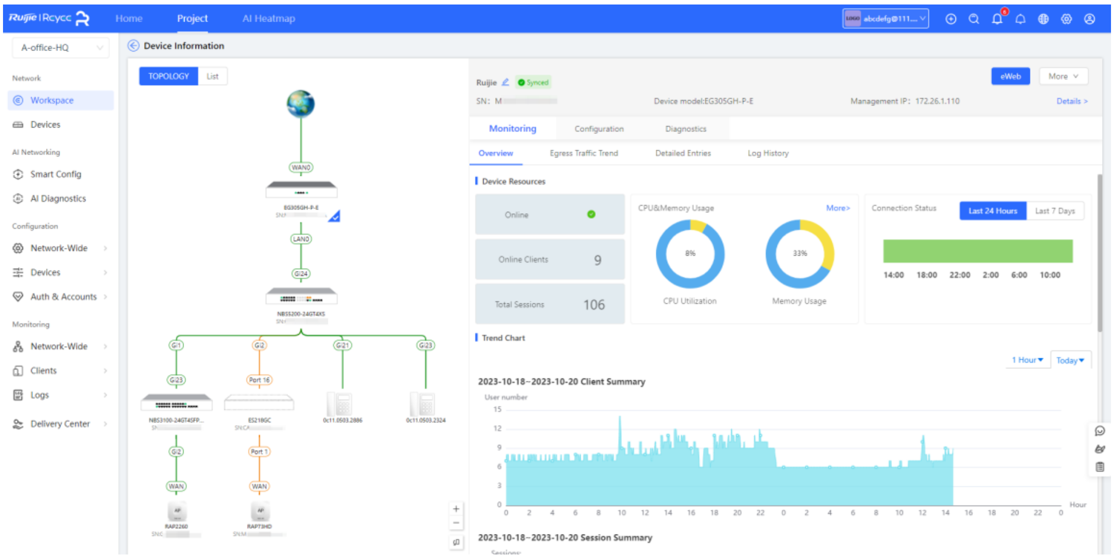
* Wi-Fi Password: •••••••••

Country/Region/Time Zone

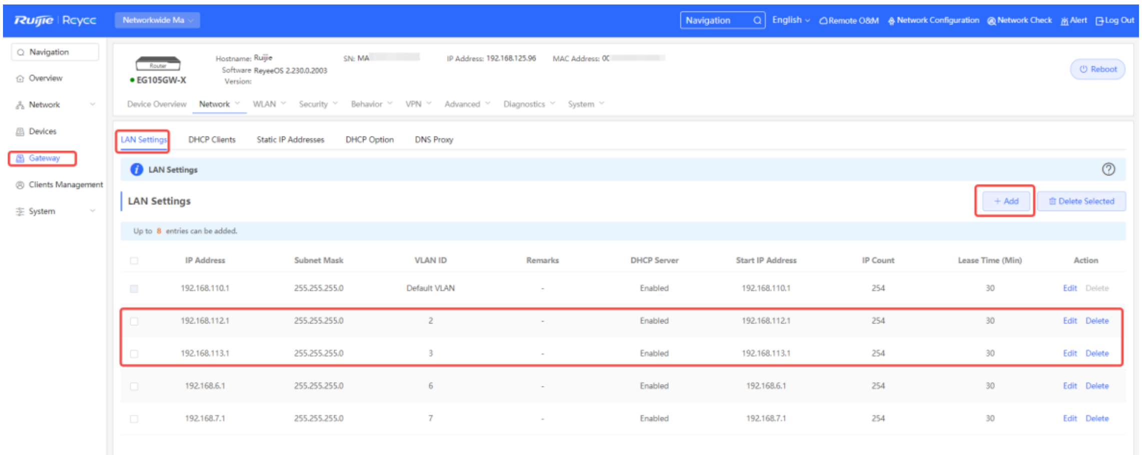
* Country/Region: China (CN)

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

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.

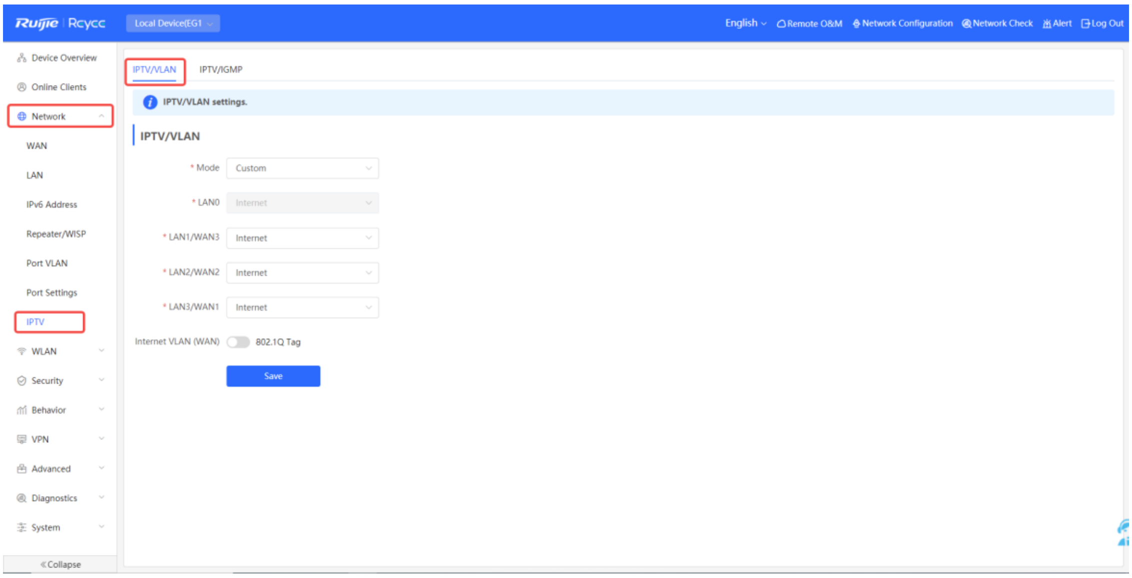


LAN Settings

Up to 8 entries can be added.

	IP Address	Subnet Mask	VLAN ID	Remarks	DHCP Server	Start IP Address	IP Count	Lease Time (Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
□	192.168.112.1	255.255.255.0	2	-	Enabled	192.168.112.1	254	30	Edit Delete
□	192.168.113.1	255.255.255.0	3	-	Enabled	192.168.113.1	254	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
□	192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete

(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 settings.

IPTV/VLAN

* Mode: Custom

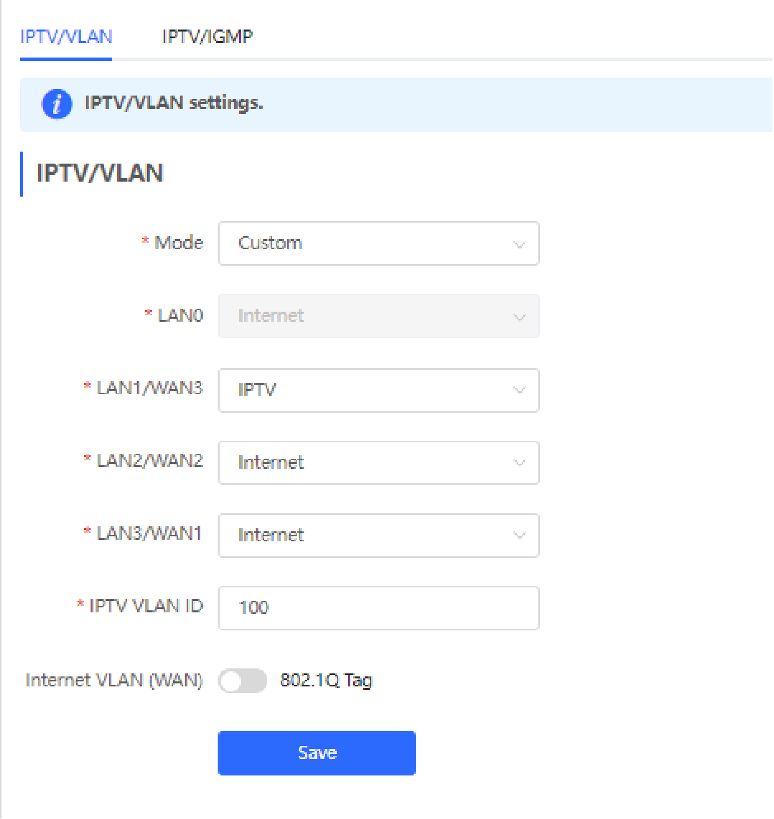
* LAN0: Internet

* LAN1/WAN3: Internet

* LAN2/WAN2: Internet

* LAN3/WAN1: Internet

Internet VLAN (WAN): 802.1Q Tag

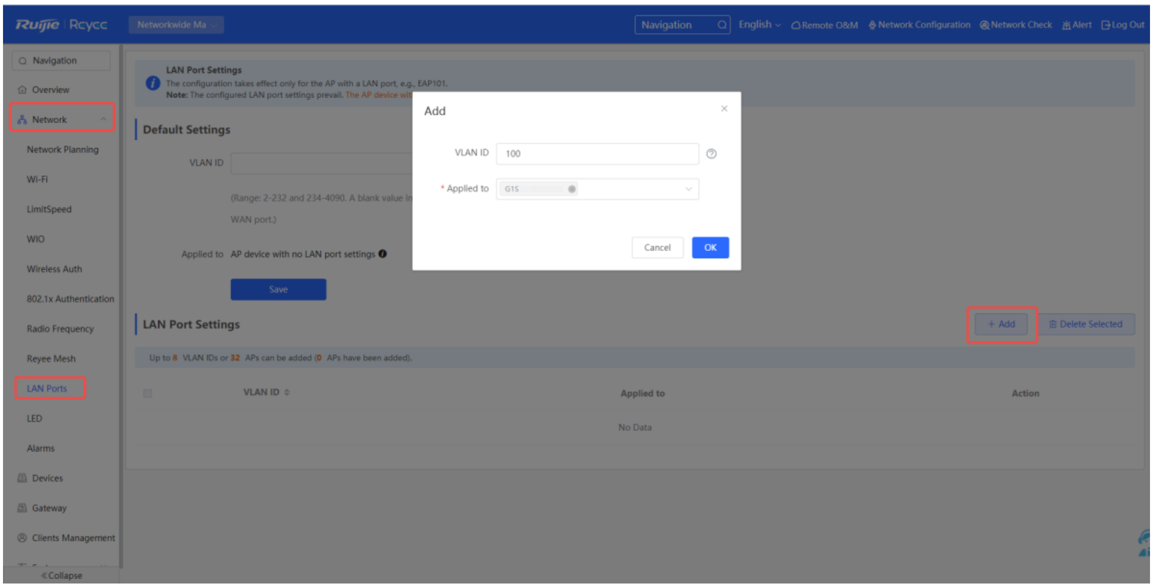


IPTV/VLAN settings.

IPTV/VLAN

- * Mode: Custom
- * LAN0: Internet
- * LAN1/WAN3: IPTV
- * LAN2/WAN2: Internet
- * LAN3/WAN1: Internet
- * IPTV VLAN ID: 100
- Internet VLAN (WAN): 802.1Q Tag

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



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 wit

Default Settings

VLAN ID
(Range: 2-232 and 234-4090. A blank value in
WAN port.)
Applied to: AP device with no LAN port settings

LAN Port Settings

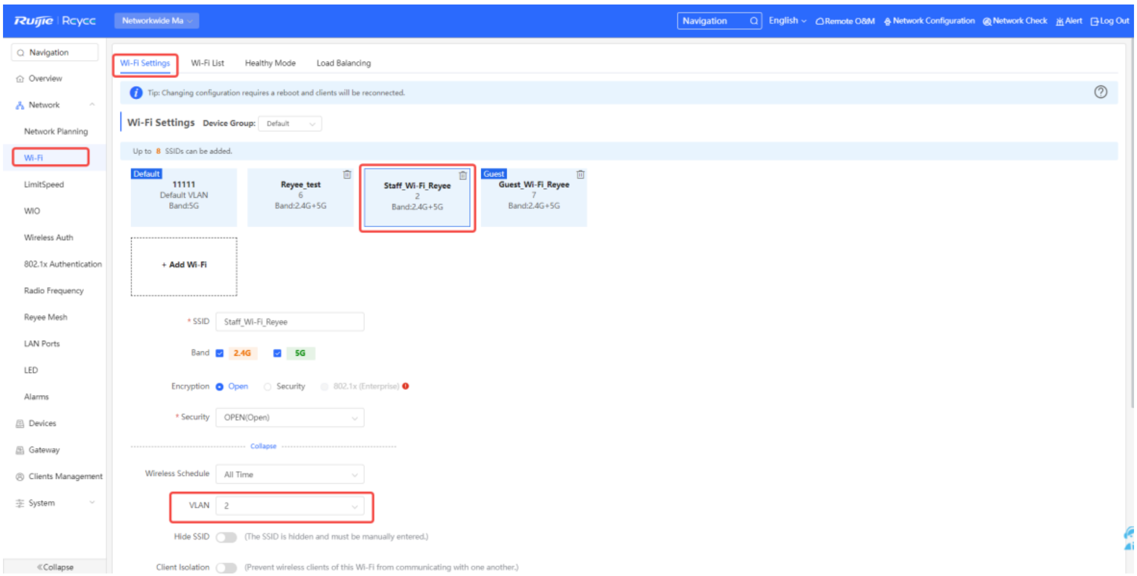
Up to 8 VLAN IDs or 32 APs can be added (0 APs have been added).

VLAN ID	Applied to	Action
No Data		

Add

- VLAN ID: 100
- * Applied to: G1S

(6) Choose **Network >Wi-Fi** > **Wi-Fi Settings**, configure Wi-Fi for staffs and guests, and select VLAN 2 for staffs.



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

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

11111 Default VLAN Band:5G

Reyee_test 6 Band:2.4G+5G

Staff_Wi-Fi_Reyee 2 Band:2.4G+5G

Guest_Wi-Fi_Reyee 7 Band:2.4G+5G

* SSID: Staff_Wi-Fi_Reyee

Band: ☑ 2.4G ☑ 5G

Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(Open)

Wireless Schedule: All Time

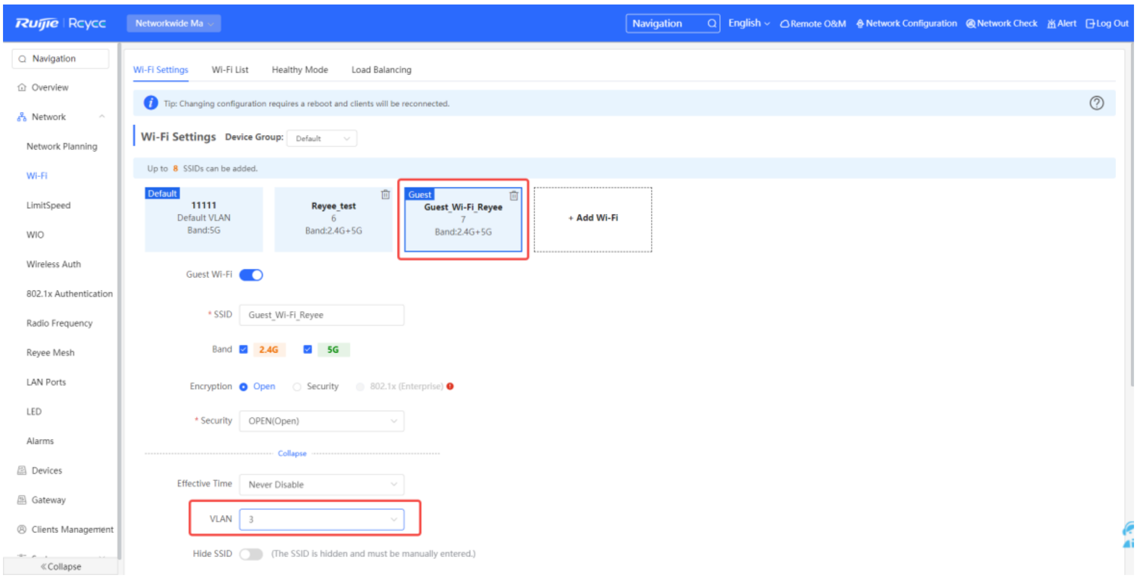
VLAN: 2

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.)

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

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



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

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

11111 Default VLAN Band:5G

Reyee_test 6 Band:2.4G+5G

Guest_Wi-Fi_Reyee 7 Band:2.4G+5G

Guest Wi-Fi: on

* SSID: Guest_Wi-Fi_Reyee

Band: ☑ 2.4G ☑ 5G

Encryption: ● Open ○ Security ○ 802.1x (Enterprise)

* Security: OPEN(Open)

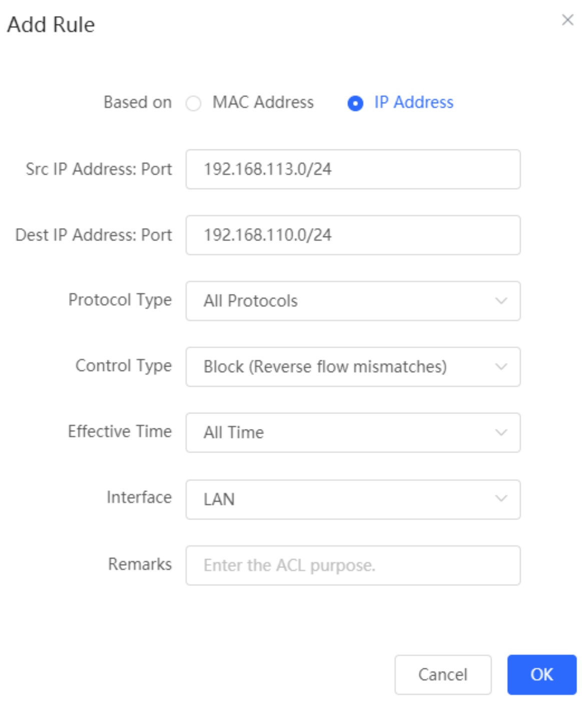
Effective Time: Never Disable

VLAN: 3

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

(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 Address ● IP Address

Src IP Address: Port: 192.168.113.0/24

Dest IP Address: Port: 192.168.110.0/24

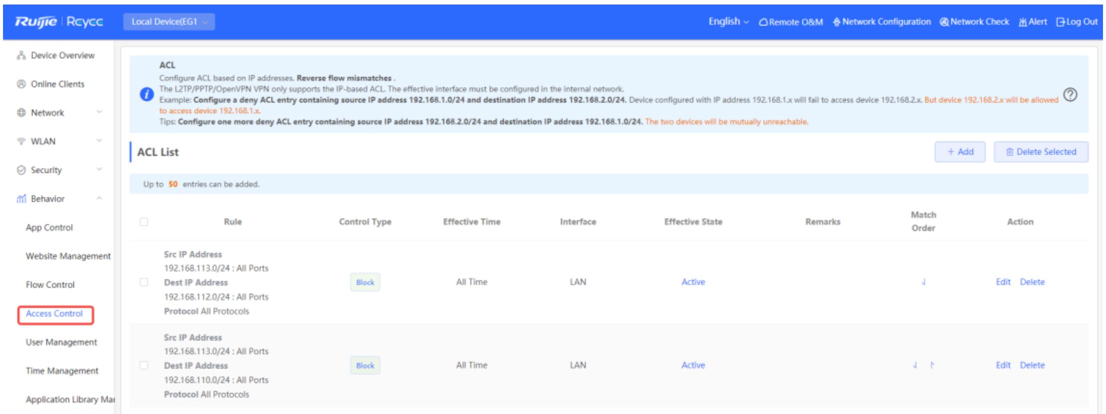
Protocol Type: All Protocols

Control Type: Block (Reverse flow mismatches)

Effective Time: All Time

Interface: LAN

Remarks: Enter the ACL purpose.



ACL

Configure ACL based on IP addresses. **Reverse flow mismatches** .
The L2TP/PPTP/OpenVPN VPN only supports the IP-based ACL. The effective interface must be configured in the internal network.
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.
Tips: **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.

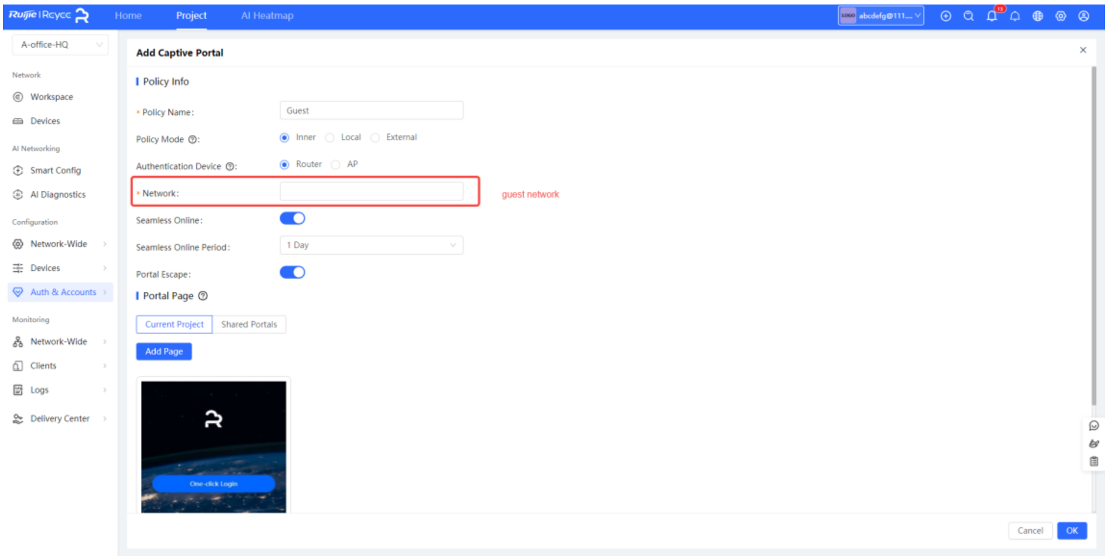
ACL List

Up to 50 entries can be added.

□	Rule	Control Type	Effective Time	Interface	Effective State	Remarks	Match Order	Action
□	**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
□	**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 Choose **Project > Configuration > Auth&Account > Authentication > Captive Portal**, and select the network for guests to configure wireless authentication.



Add Captive Portal

Policy Info

* Policy Name: Guest

Policy Mode: ● Inner ○ Local ○ External

Authentication Device: ● Router ○ AP

* Network:

guest network

Seamless Online: on

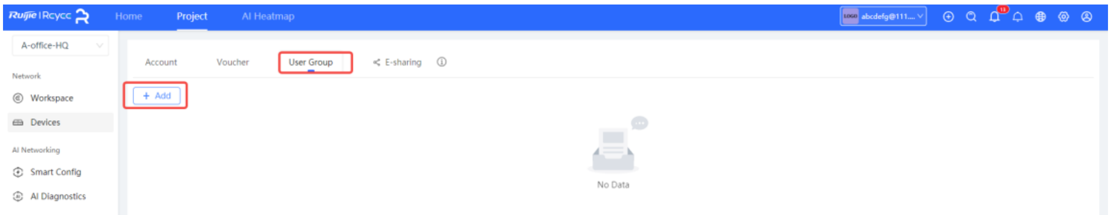
Seamless Online Period: 1 Day

Portal Escape: on

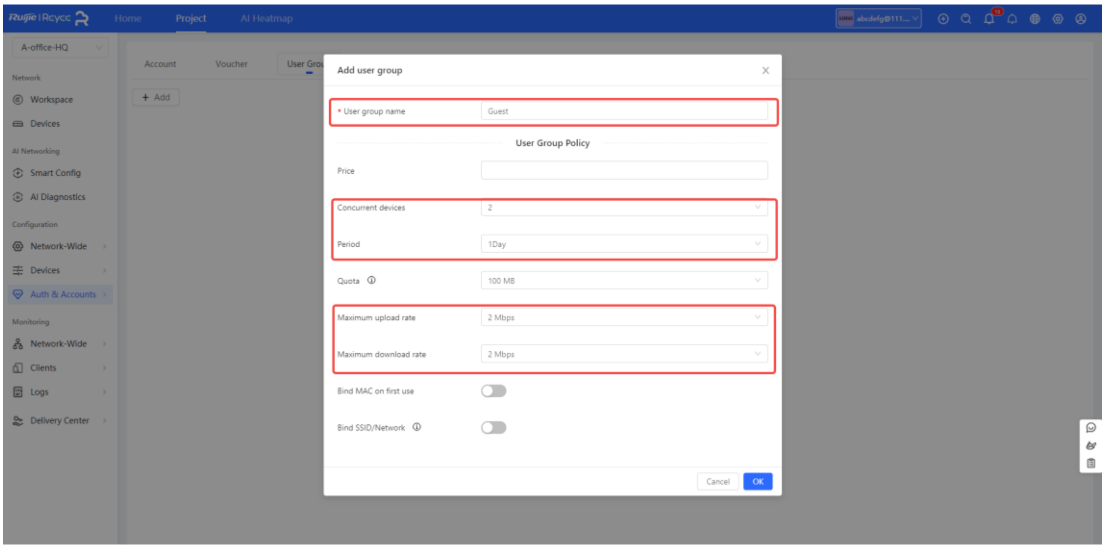
Portal Page

b Add the voucher for guests.

Choose **Configuration > Auth&Account > Authentication > User Management > User Group** and add a group for guests.



Example: Set Concurrent Devices to 2, Period to 1 Day, and Upload Speed and Download Speed to 2 Mbps.



Add user group

* User group name: Guest

User Group Policy

Price:

Concurrent devices: 2

Period: 1Day

Quota: 100 MB

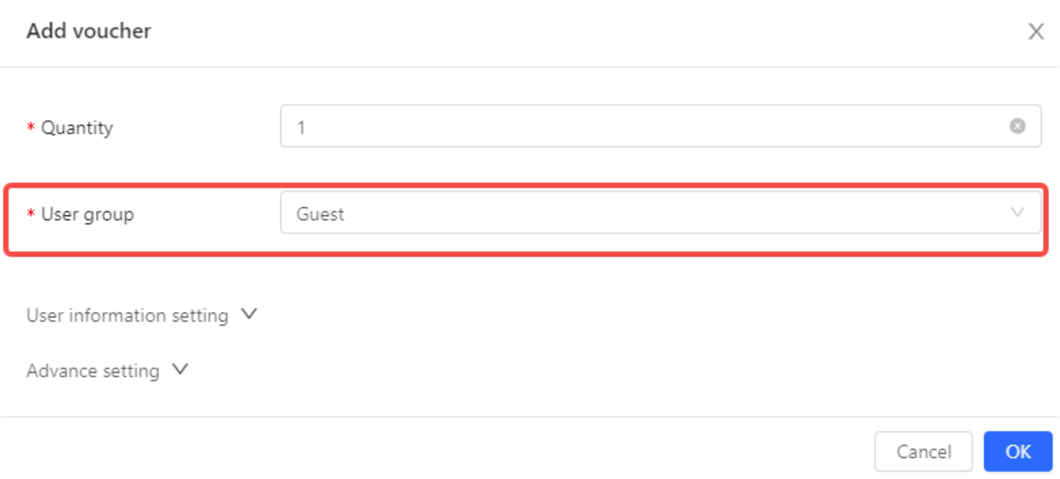
Maximum upload rate: 2 Mbps

Maximum download rate: 2 Mbps

Bind MAC on first use: off

Bind SSID/Network: off

Choose **Configuration > Auth&Account > Authentication > User Management > Voucher** and add a voucher for guests.

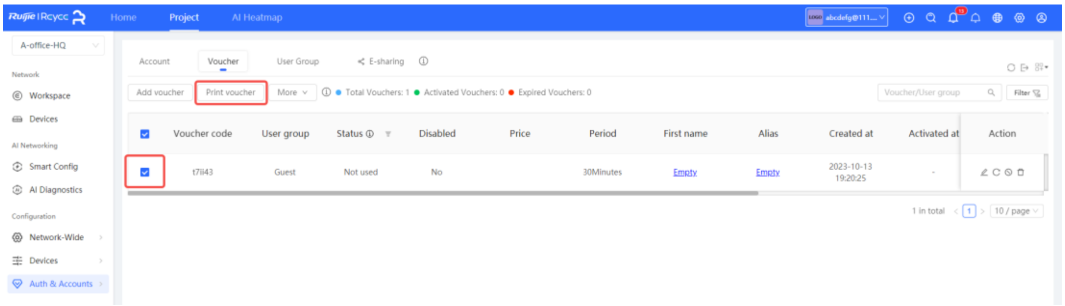


Add voucher

* Quantity: 1

* User group: Guest

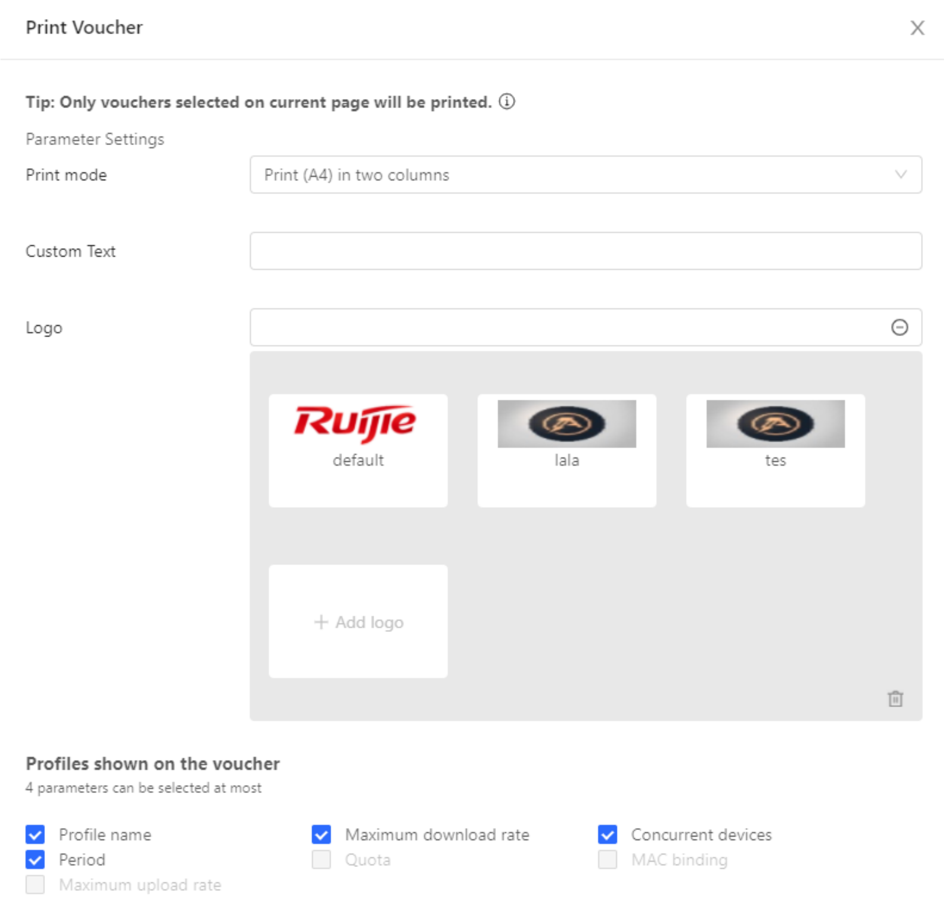
c Click **Print Voucher** to obtain the code for guests.



Total Vouchers: 1 ● Activated Vouchers: 0 ● Expired Vouchers: 0

☑	Voucher code	User group	Status	Disabled	Price	Period	First name	Alias	Created at	Activated at	Action
☑	t7ii43	Guest	Not used	No		30Minutes	Empty	Empty	2023-10-13 19:20:25	-	

1 in total 1 10 / page



Print Voucher

Tip: Only vouchers selected on current page will be printed.

Parameter Settings

Print mode: Print (A4) in two columns

Custom Text:

Logo:

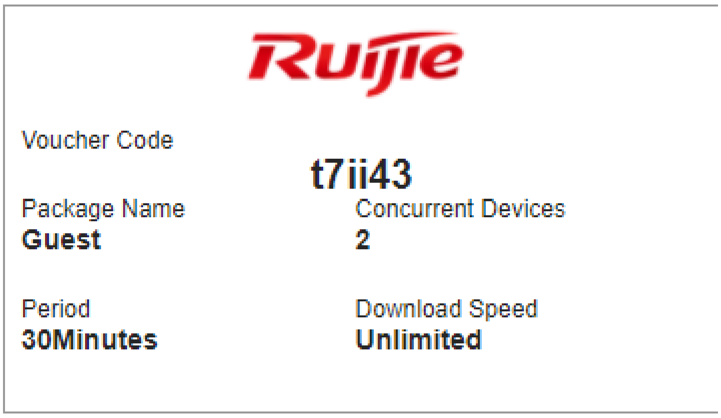
Profiles shown on the voucher

4 parameters can be selected at most

☑ Profile name ☑ Maximum download rate ☑ Concurrent devices

☑ Period □ Quota □ MAC binding

□ Maximum upload rate



Voucher Code

t7ii43

Package Name
Guest

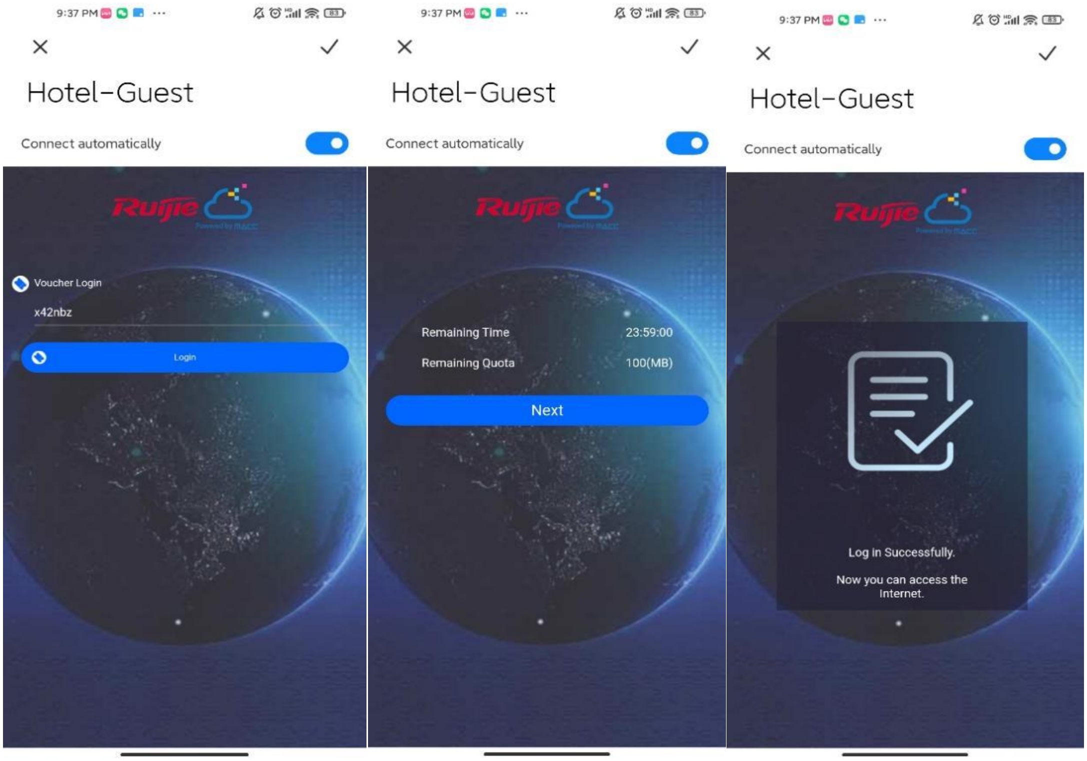
Concurrent Devices
2

Period
30Minutes

Download Speed
Unlimited

6.4.3 Configuration Verification

Connect guest Wi-Fi. You can see that the internal IP address 192.168.110.1 cannot be accessed.



9:37 PM

Hotel-Guest

Connect automatically

Voucher Login

x42nbz

Login

9:37 PM

Hotel-Guest

Connect automatically

Remaining Time 23:59:00

Remaining Quota 100(MB)

Next

9:37 PM

Hotel-Guest

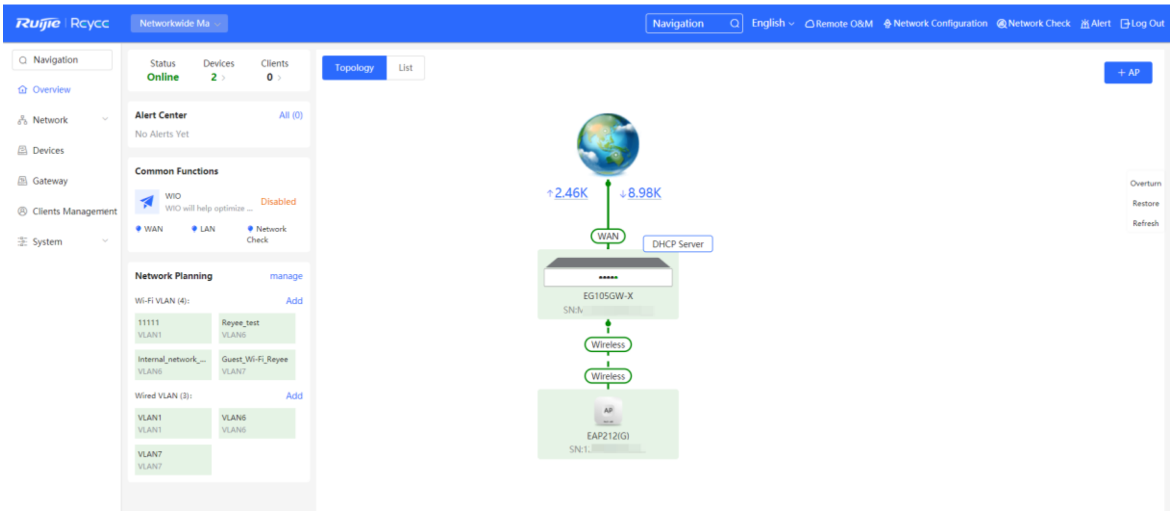
Connect automatically

Log in Successfully.

Now you can access the Internet.

7 Appendix: Surveillance

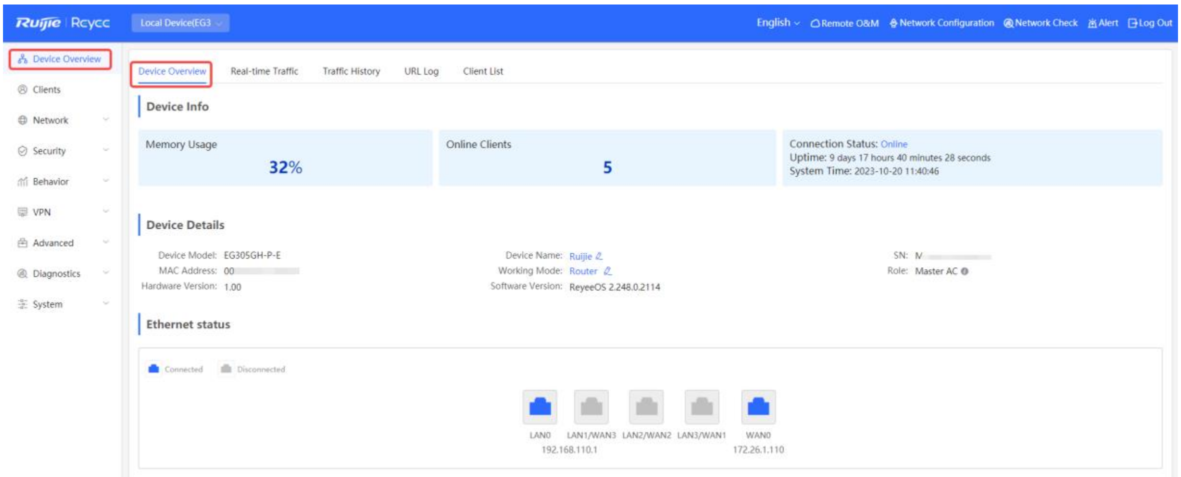
The overview page displays **Device Info**, **Wi-Fi**, **Network Planning**, and **Topology**.



7.1 Device Info

Choose **Local Device > Device Overview > Device Overview**. One the **Device Details** page, the model, host name, IP address, MAC address, software version, and SN of the router are displayed.

In the **Device Info** pane, the memory usage, online client count, status, uptime, and system time are displayed.



Device Info

Memory Usage 32%

Online Clients 5

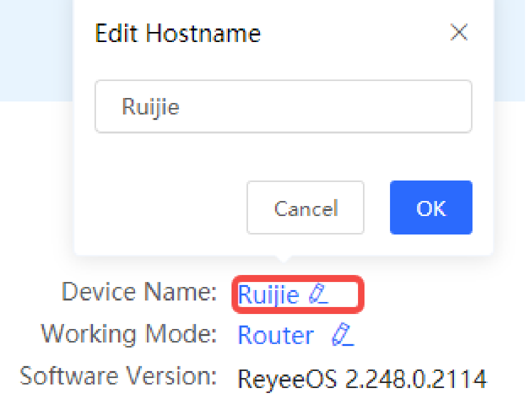
Connection Status: Online
Uptime: 9 days 17 hours 40 minutes 28 seconds
System Time: 2023-10-20 11:40:46

Device Details

Device Model: EG305GH-P-E
MAC Address: 00[redacted]
Hardware Version: 1.00
Device Name: Ruijie
Working Mode: Router
Software Version: ReyeeOS 2.248.0.2114
SN: M[redacted]
Role: Master AC

Ethernet status

- The **Online** status indicates the SON status of the Reyee devices but not Ruijie Cloud.
- You can click **Device Name** to modify the device name.

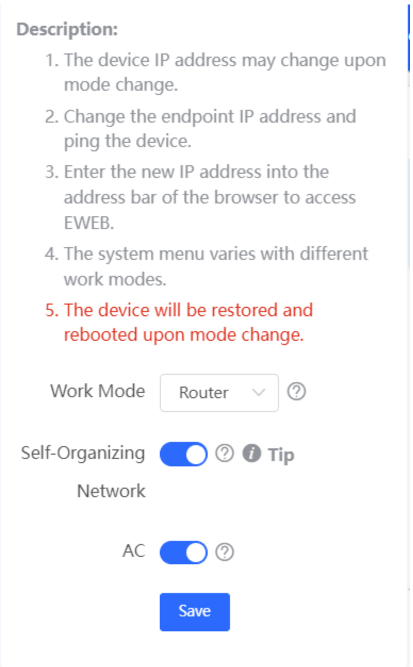


Device Name: Ruijie

Working Mode: Router

Software Version: ReyeeOS 2.248.0.2114

- Click **Work Mode** to switch the device mode. Two modes are available: **Router** and **AC** modes. The default mode is **Router**.



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.
5. The device will be restored and rebooted upon mode change.

Work Mode: Router

Self-Organizing Network: On

AC: On

  - **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.

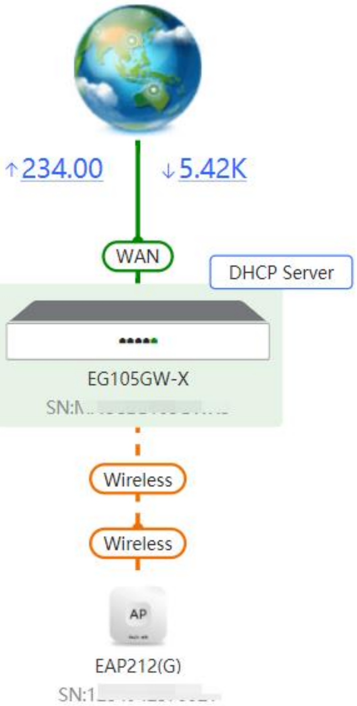
Wi-Fi

Primary Wi-Fi: 11111
Security: No

Guest Wi-Fi: Guest_Wi-Fi_Reyee
Security: No

7.3 Network Topology

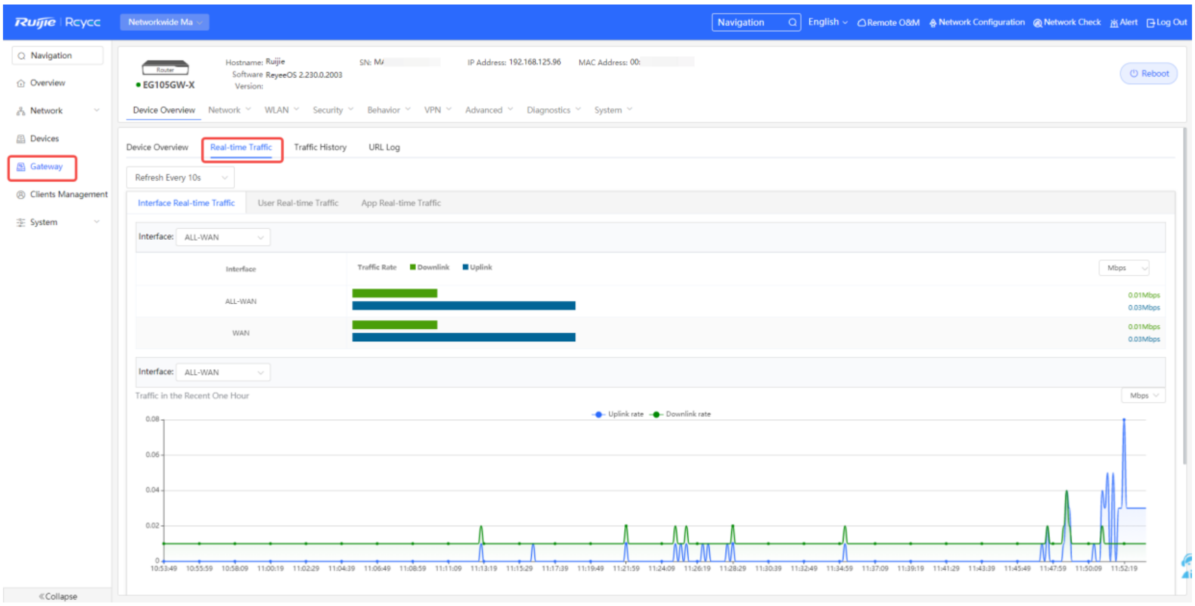
The **Topology** page displays the topology and connected status of the network.



7.4 Real-Time Flow

Choose **Gateway > Device Overview > Real Time Traffic**.

Check real-time traffic flows based on ports, users, and apps, including uplink and downlink flows. The default unit is Mbps. You can change it to be bps and Kbps.



Hostname: Ruijie
SN: MA
Software Version: ReyeeOS 2.230.0.2003
IP Address: 192.168.125.96
MAC Address: 00:
Refresh Every 10s
Interface: ALL-WAN
Interface: ALL-WAN

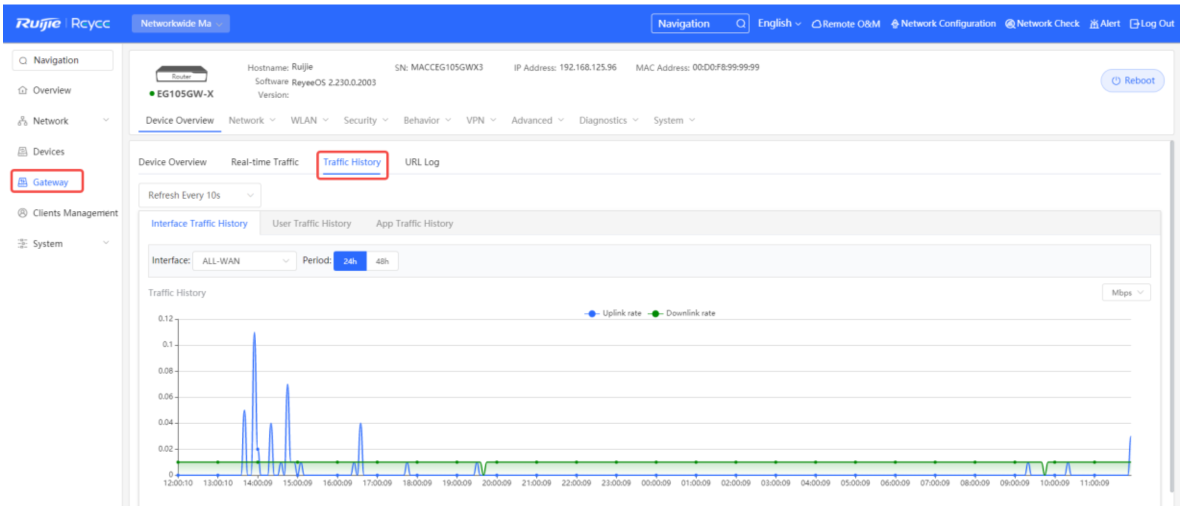
7.5 Traffic History

Note

This feature is supported by R202 and later versions.

Choose **Gateway > Device Overview** > **Traffic History**.

Check historical traffic flow based on ports, users, and apps, including uplink and downlink flows.



Hostname: Ruijie
SN: MACCEG105GWX3
Software Version: ReyeeOS 2.230.0.2003
IP Address: 192.168.125.96
MAC Address: 00:D0:F8:99:99:99
Refresh Every 10s
Interface: ALL-WAN Period: 24h 48h

7.6 URL Logs

URL logs are URL access records of devices on the internal network, including the URL, access count, and audit result.

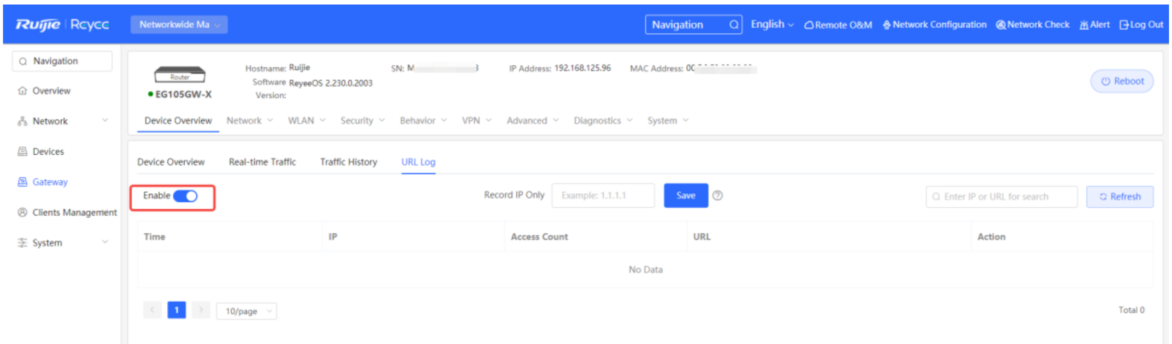
Note

This feature is supported by only EG3xx series routers such as EG310G-E.

(1) Choose **Gateway > Device Overview** > **URL Log**.

(2) Enable URL logging.

Toggle the switch to **Enable** and click **OK** in the dialog box.



Hostname: Ruijie
Software Version: ReyeeOS 2.230.0.2003
SN: M[redacted]
IP Address: 192.168.125.96
MAC Address: 0C[redacted]

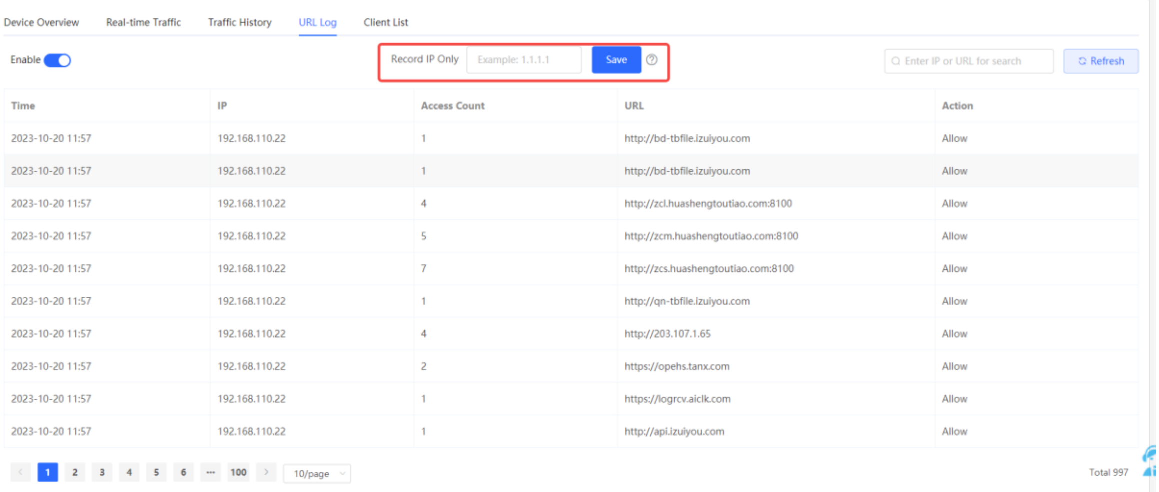
Enable
Record IP Only: Example: 1.1.1.1
Enter IP or URL for search

Time	IP	Access Count	URL	Action
No Data				

1 · 10/page · Total 0

(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**.



Enable
Record IP Only: Example: 1.1.1.1
Enter IP or URL for search

Time	IP	Access Count	URL	Action
2023-10-20 11:57	192.168.110.22	1	http://bd-tbfile.izuiyou.com	Allow
2023-10-20 11:57	192.168.110.22	1	http://bd-tbfile.izuiyou.com	Allow
2023-10-20 11:57	192.168.110.22	4	http://zcl.huashengtoutiao.com:8100	Allow
2023-10-20 11:57	192.168.110.22	5	http://zcm.huashengtoutiao.com:8100	Allow
2023-10-20 11:57	192.168.110.22	7	http://zcs.huashengtoutiao.com:8100	Allow
2023-10-20 11:57	192.168.110.22	1	http://qn-tbfile.izuiyou.com	Allow
2023-10-20 11:57	192.168.110.22	4	http://203.107.1.65	Allow
2023-10-20 11:57	192.168.110.22	2	https://opehs.tanx.com	Allow
2023-10-20 11:57	192.168.110.22	1	https://logrcv.aiclk.com	Allow
2023-10-20 11:57	192.168.110.22	1	http://api.izuiyou.com	Allow

1 2 3 4 5 6 ··· 100 · 10/page · Total 997

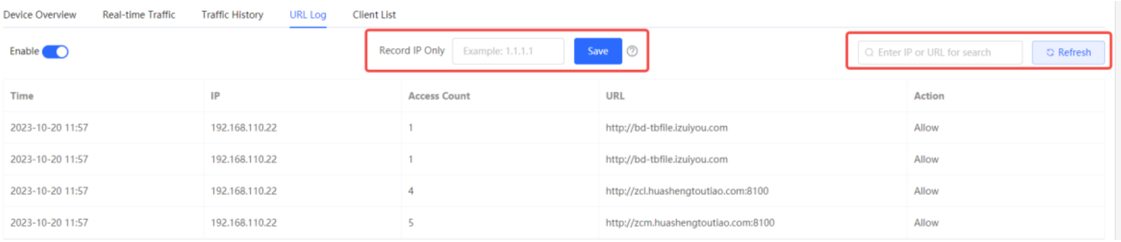
Note

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.



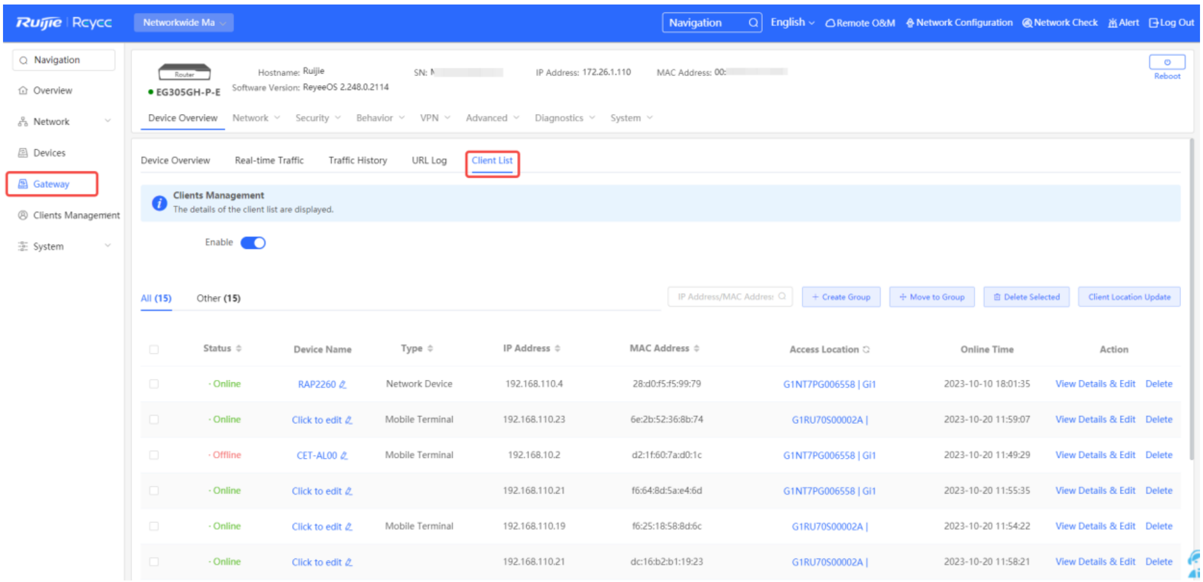
Enable
Record IP Only: Example: 1.1.1.1
Enter IP or URL for search

Time	IP	Access Count	URL	Action
2023-10-20 11:57	192.168.110.22	1	http://bd-tbfile.izuiyou.com	Allow
2023-10-20 11:57	192.168.110.22	1	http://bd-tbfile.izuiyou.com	Allow
2023-10-20 11:57	192.168.110.22	4	http://zcl.huashengtoutiao.com:8100	Allow
2023-10-20 11:57	192.168.110.22	5	http://zcm.huashengtoutiao.com:8100	Allow

7.7 Client List

Choose **Gateway** > **Device Overview** > **Client List**.

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.



● EG305GH-P-E

Hostname: Ruijie

Software Version: ReyeeOS 2.248.0.2114

SN: [redacted]

IP Address: 172.26.1.110

MAC Address: 00:[redacted]

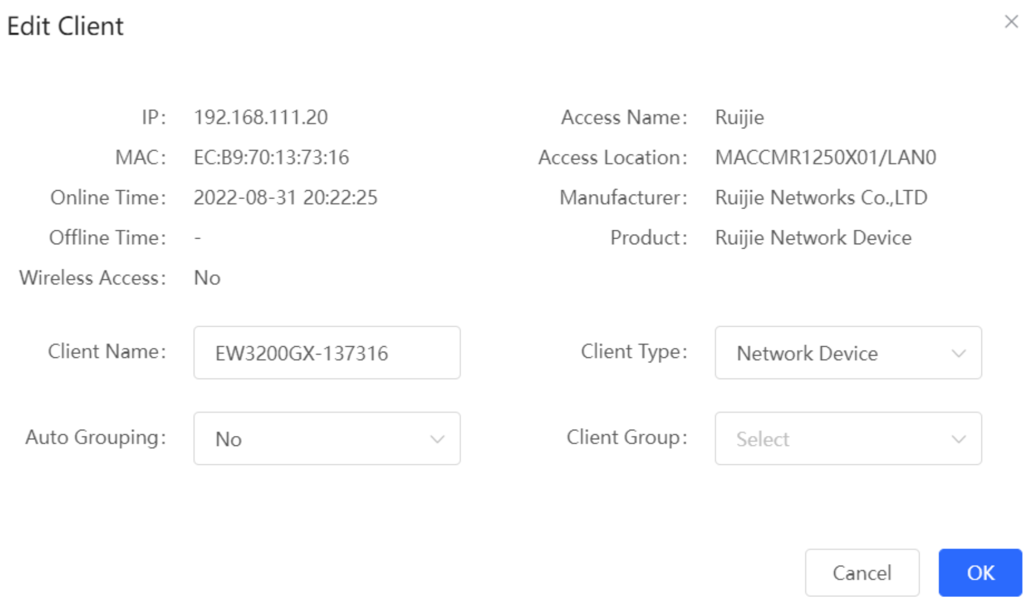
Clients Management

The details of the client list are displayed.

Enable ●

All (15) Other (15)

□	Status	Device Name	Type	IP Address	MAC Address	Access Location	Online Time	Action
□	· Online	RAP2260	Network Device	192.168.110.4	28:d0:f5:f5:99:79	G1NT7PG006558 | Gi1	2023-10-10 18:01:35	View Details & Edit Delete
□	· Online	Click to edit	Mobile Terminal	192.168.110.23	6e:2b:52:36:8b:74	G1RU70S00002A |	2023-10-20 11:59:07	View Details & Edit Delete
□	· Offline	CET-AL00	Mobile Terminal	192.168.10.2	d2:1f:60:7a:d0:1c	G1NT7PG006558 | Gi1	2023-10-20 11:49:29	View Details & Edit Delete
□	· Online	Click to edit		192.168.110.21	f6:64:8d:5a:e4:6d	G1NT7PG006558 | Gi1	2023-10-20 11:55:35	View Details & Edit Delete
□	· Online	Click to edit	Mobile Terminal	192.168.110.19	f6:25:18:58:8d:6c	G1RU70S00002A |	2023-10-20 11:54:22	View Details & Edit Delete
□	· Online	Click to edit		192.168.110.21	dc:16:b2:b1:19:23	G1RU70S00002A |	2023-10-20 11:58:21	View Details & Edit Delete



Edit Client

IP: 192.168.111.20

MAC: EC:B9:70:13:73:16

Online Time: 2022-08-31 20:22:25

Offline Time: -

Wireless Access: No

Access Name: Ruijie

Access Location: MACCMR1250X01/LAN0

Manufacturer: Ruijie Networks Co.,LTD

Product: Ruijie Network Device

Client Name: EW3200GX-137316

Client Type: Network Device

Auto Grouping: No

Client Group: Select