

Ruijie Reyee RG-EG Series Router

FAQs



Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

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



and other Ruijie network logos are trademarks of Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

 **Note**

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

 **Specification**

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

3. Note

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

Contents

Preface	I
Contents	3
1 FAQs About Login	9
1.1 What Is the Default Management IP Address of Reyee EG Routers?	9
1.2 How Do I Log In to a Reyee EG Router?	9
1.3 How Do I Log In to a Reyee EG Router Through Ruijie Cloud App?.....	9
1.4 What Can I Do If I Fail to Log In to the Eweb Management System?	11
2 FAQs About the Password	13
2.1 What Is the Default Login Password of Reyee EG Routers?.....	13
2.2 How Do I Change the Device's Login Password?.....	13
2.3 What Can I Do If I Forget the Password?.....	15
3 FAQs About Network Access	16
3.1 What Should I Do If a PPPoE Connection Fails to Be Set Up?	16
3.2 What Should I Do If the Device Cannot Obtain an IP Address Through DHCP?	18
3.3 What Should I Do If Internet Access Is Slow?	19
3.4 What Should I Do If I Cannot Access the Internet?.....	19
4 FAQs About SON	21
4.1 What Is SON?	21
4.2 Which Devices Can Act as the Master Device on the SON?	21
4.3 How Many Devices Can the SON Support?.....	21
4.4 What Is the Priority of Devices During Master Device Election of the SON?	22
4.5 How Is SON Enabled on a Device?.....	22
4.6 How Is SON Disabled on a Device?.....	23

4.7 How Does the SON Perform Device Discover?	24
4.8 Does the SON Configuration Change If the Master Device Is Disconnected?	24
4.9 Does the SON Support the Preemption Mode?	24
4.10 What Is the IP Address of the Master Device on the SON?	25
4.11 What Is the Difference Between the Default SSID @Ruijie-s and @Ruijie-m?	25
4.12 How Is a Device Specified as the Master Device?.....	25
4.13 How Does the Master Device Add a New Device to the Network?.....	26
4.14 The SON Has Been Configured Successfully, but Devices Still Cannot Be Online on Ruijie Cloud. Why?	27
5 FAQs About Wireless Configuration.....	28
5.1 What Can I Do If SSID Configuration on Ruijie Cloud Fails to Be Synchronized to a Reyee Device?	28
5.2 How Are Radio Settings Adjusted When the Wireless Network Quality Is Low?	29
5.2.1 Optimizing the Radio Channel	30
5.2.2 Optimizing the Channel Width	30
5.2.3 Configuring the Disconnection Threshold.....	31
5.2.4 Configuring the Client Limit.....	32
5.2.5 Configuring the Roaming Sensitivity.....	32
5.3 Can Reyee EG Routers Support Wi-Fi?.....	34
6 FAQs About Guest Wi-Fi	35
6.1 What Is Guest Wi-Fi?	35
6.2 How Do I Configure Guest Wi-Fi on Ruijie Cloud App?	35
6.3 What Can I Do If the System Displays the Message that "The configuration is only supported on the project with gateway?"	37
7 FAQs About Flow Control.....	38

7.1 What Is Flow Control?	38
7.2 How Do I Configure Flow Control?	38
7.3 How Is Flow Control Configured for Specific Users on a Reyee EG Router?	39
7.4 What Can I Do If the Custom Policy of Flow Control Do Not Take Effect?.....	40
8 FAQs About VPN.....	42
8.1 How Is IPsec VPN Configured on a Reyee EG Router?	42
8.2 Can I Use a Reyee EG Router to Establish an IPsec VPN with Devices of Other Brands or Ruijie EG Routers?	46
8.3 Can Reyee EG Routers Support IKEv2?	46
8.4 What Can I Do If Reyee EG Routers Cannot Connect to the IPsec VPN?.....	46
8.5 How Do I Configure PPTP VPN on a Reyee EG Router?	48
8.5.1 Client-to-Site Scenario Configuration	49
8.5.2 Site-to-Site Scenario Configuration	57
8.6 Can a Reyee EG Router Establish a PPTP VPN with Third-Party Devices or Ruijie EG Routers?	59
8.7 Can PPTP VPN Be Connected on an iPhone or Mac?	60
8.8 What Can I Do If a Reyee EG Router Fails to Connect the PPTP VPN?	60
8.9 What Can I Do If I Fail to Connect PPTP VPN on a PC or an iPhone?	60
8.10 What Can I Do If I Have Connected VPN, but Cannot Access Internal Devices of the Headquarters?	61
8.11 Why I Fail to Access the Internet After Connecting the VPN?	62
8.12 Can a Reyee EG Router Be Enabled with PPTP and IPsec Simultaneously?	63
8.13 Can a Reyee EG Router Be Enabled with PPTP and L2TP Simultaneously?	63
8.14 How Do I Configure L2TP VPN on a Reyee EG Router?	63
8.14.1 Client-to-Site Scenario Configuration	64

8.14.2 Site-to-Site Scenario Configuration	73
8.15 Can a Reyee EG Router Establish an L2TP VPN with Third-Party Devices or Ruijie EG Routers?	75
8.16 What Can I Do If a Reyee EG Router Fails to Connect the L2TP VPN?	75
8.17 What Can I Do If I Fail to Connect L2TP VPN on a PC?	76
8.18 Can a Reyee EG Router Be Enabled with L2TP and IPsec Simultaneously?	76
8.19 How Do I Configure L2TP over IPsec VPN on a Reyee EG Router?	76
8.19.2 Client-Side Configuration	81
8.19.3 Branch-Side Configuration	88
8.20 Can a Reyee EG Router Establish an L2TP over IPsec VPN with Third-Party Devices or Ruijie EG Routers?	89
8.21 Can Branches Connect to Each Other?	89
8.22 What Can I Do If I Fail to Connect L2TP over IPsec VPN on a Reyee EG Router?	90
9 FAQs About DDNS	92
9.1 What Is DDNS?	92
9.2 Which DDNS Service Providers Are Available for Reyee Devices?	92
9.3 To Which Scenarios Are DDNS Applied?	92
10 FAQs About Behavior Strategy	95
10.1 What Should I Do If the Behavior Strategy Does Not Take Effect?	95
10.2 How Do I Configure the Users That Are Allowed to Access Only Certain Websites/Apps? ..	95
10.3 How Do I Configure Different Users to Access Different Websites/Apps?	95
10.4 How Is the Access/Blocking Time Customized for Websites/Apps?	95
10.5 How Many Behavior Strategies Can Be Created?	96
11 FAQs About Authentication	97
11.1 What Should I Do If Local Account Authentication Does Not Take Effect?	97

11.2 How Is Local Account Authentication Configured on a Reyee Router?.....	97
11.3 How Many Users Are Supported for One Account?.....	99
11.4 How Is Authorized Authentication Configured on a Reyee Router?	99
11.5 Why Authorized Authentication Does Not Take Effect?.....	102
11.6 How Is QR Code Authentication Configured on a Reyee Router?	102
11.7 What Should I Do If QR Code Authentication Does Not Take Effect?	104
12 FAQs About IPTV	105
12.1 How Can I Configure IPTV on a Reyee EG Router?	105
12.2 What Can I Do If the IPTV Device Does Not Work After the IPTV Device Is Connected to the Reyee EG Router?	108
12.3 What Can I Do If the IPTV Service Is Frozen Frequently After the IPTV Device Is Connected to the Reyee EG Router?	108
13 FAQs About the Mesh Function	108
13.1 Can Wired Mesh Switch to Wireless Mesh?	108
13.2 The Master Device Has Been Powered Off, Will the Slave Device Automatically Connect to the Master Device When It Is Powered On Again?.....	109
13.3 What Should I Do If It Takes a Long Time for the Slave Device to Reconnect to the Master Device After the Master Device Has Restarted?	109
13.4 Why the SSID and Channel Cannot Be Changed on the Slave Device After a Mesh Network Is Set Up Successfully?.....	109
13.5 What Should I Do If a Mesh Network Fails to Be Set Up?.....	109
14 FAQs About Parameters of Reyee Routers	110
14.1 Where Can I Find All Parameters of Reyee Routers?	110
14.2 What Is the Maximum Number of Concurrent Clients on a Reyee Router?	110
14.3 How Many Devices Can a Router Manage in AC or Gateway Mode?	110

14.4 What Is the Difference Between the AC Mode and Router Mode for a Reyee EG Router?111

1 FAQs About Login

1.1 What Is the Default Management IP Address of Reyee EG Routers?

For Reyee EG Routers, the default management IP address is 192.168.110.1, 10.44.77.254, or 10.44.77.253.

1.2 How Do I Log In to a Reyee EG Router?

- Log in to the device in wired mode.

Connect a PC to a LAN port of the EG router, and then log in to the EG router with the IP address 192.168.110.1 in DHCP mode or 10.44.77.254 in static mode.

- Log in to the EG router in wireless mode.

If a Reyee AP is deployed on your network, you can connect the default SSID **@Ruijie-mXXXX** of the Reyee AP, and log in to EG router with the IP address 10.44.77.253 or 10.44.77.254.

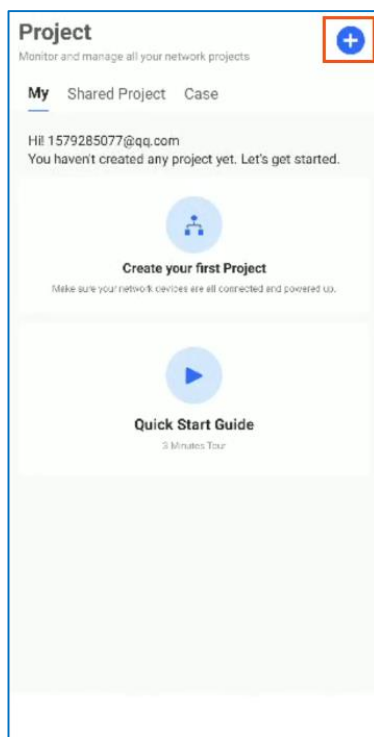
1.3 How Do I Log In to a Reyee EG Router Through Ruijie Cloud App?

Ruijie Cloud App provides a quick start to create a network and add devices.

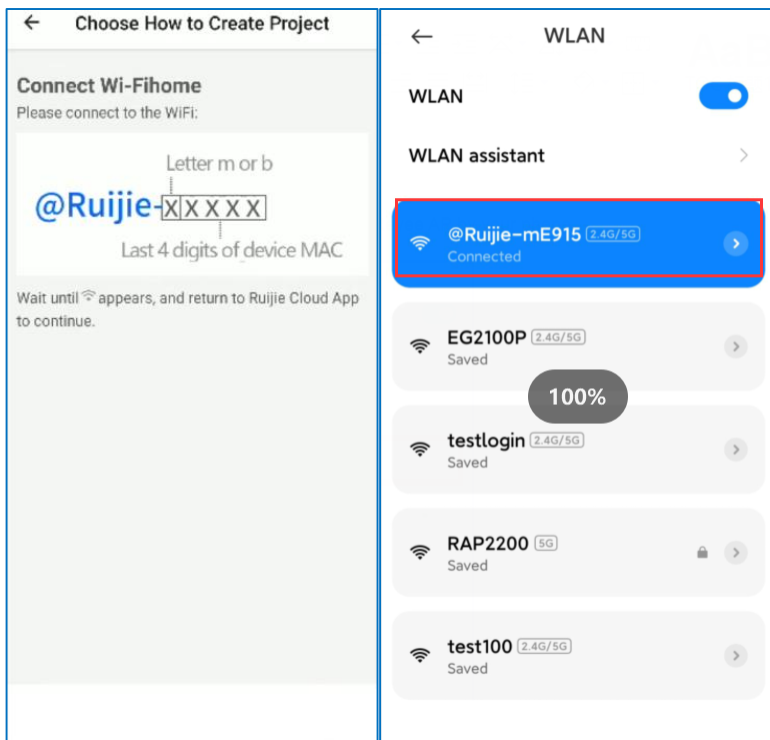
Download Ruijie Cloud App by visiting <https://cloud-as.ruijienetworks.com/admin3/mobileApp>.

Perform the following steps:

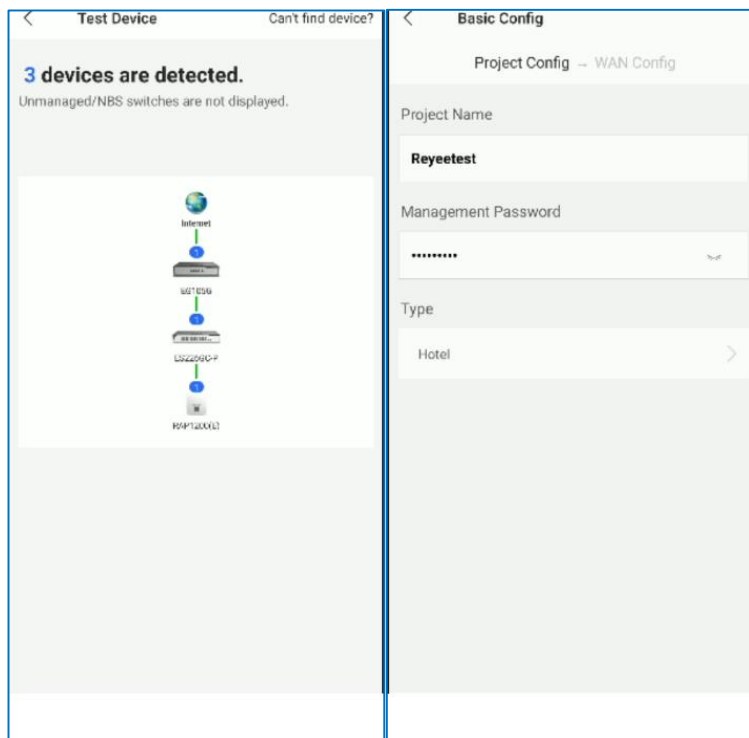
- (1) Connect a WAN port of an EG router to the Internet and connect other Reyee devices on the same network.
- (2) Create a project.



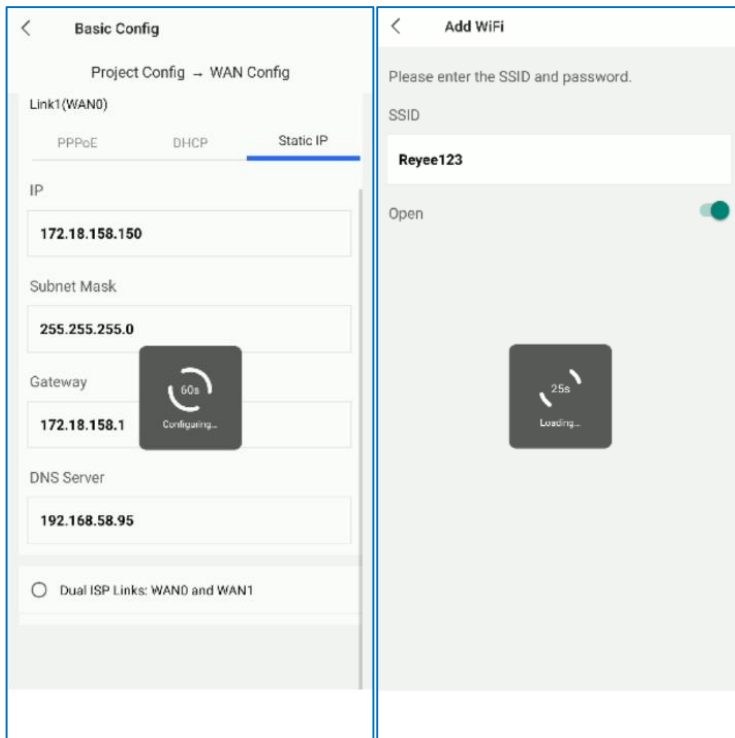
- (3) Connect to the default SSID **@Ruijie-mxxxx** of a Reyee AP through your phone.



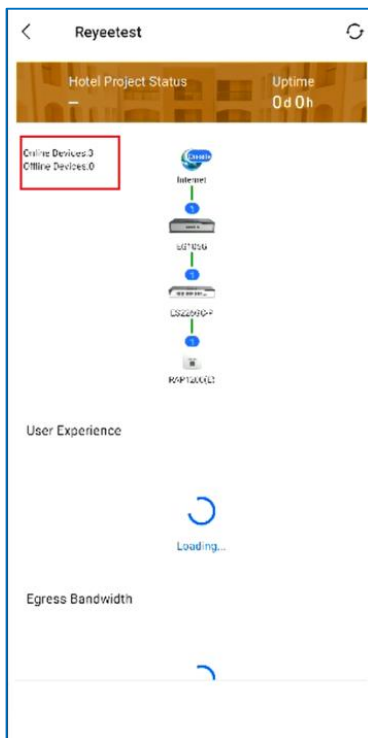
- (4) Check whether devices are detected.
- (5) Name the project and enter the management password.



- (6) Finish the WAN configuration and wireless configuration.



After the configuration, you can check that devices are all online. Then you can log in to the device through Ruijie Cloud.



1.4 What Can I Do If I Fail to Log In to the Eweb Management System?

- (1) Check that the network cable is properly connected to the LAN port of the device and the corresponding LED indicator blinks or is steady on.

- (2) Before accessing the configuration GUI, configure automatic IP address assignment (recommended), so that the server with DHCP enabled can automatically assign an IP address to the PC. To allocate a static IP address to the PC, set the IP address of the PC on the same network segment as the IP address of the management interface.
- (3) Run the **ping** command to test the connectivity between the PC and the device.
- (4) If the fault persists, restore the device to factory settings.

2 FAQs About the Password

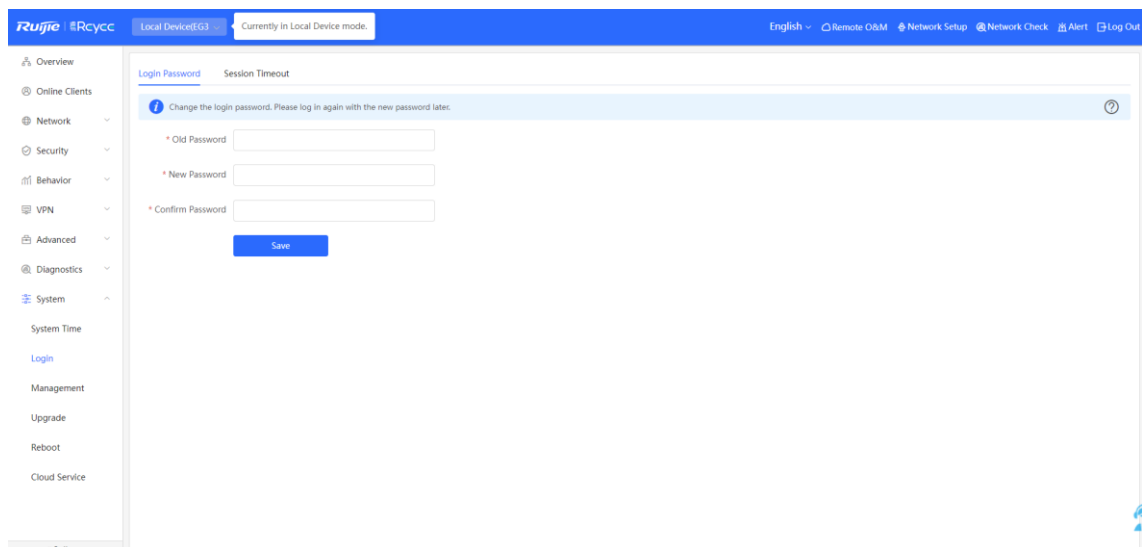
2.1 What Is the Default Login Password of Reyee EG Routers?

Enter the default password **admin** if you log into a Reyee device with a software version earlier than P20 for the first time. For P20 and later versions, the password is not required upon first login.

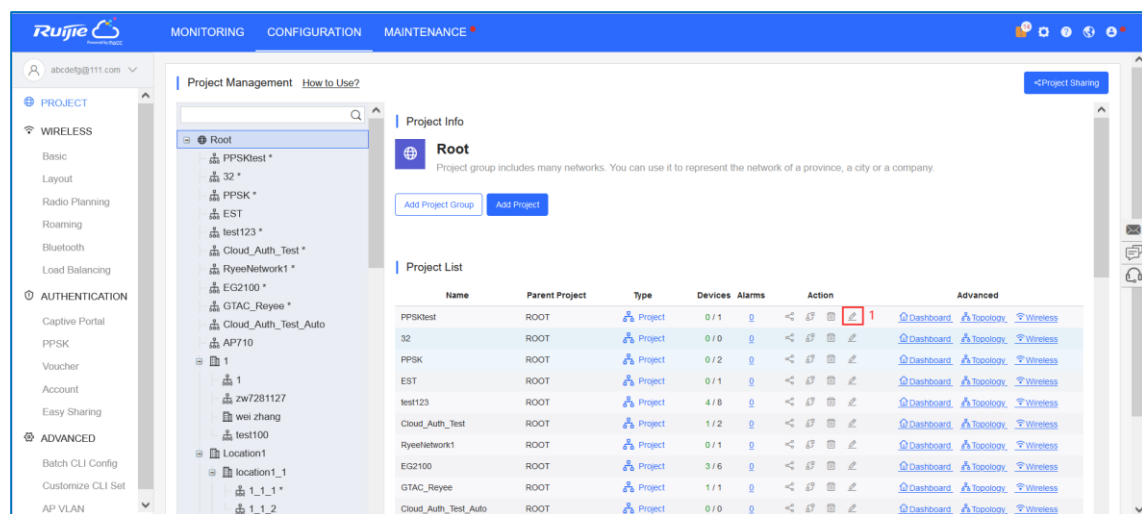
2.2 How Do I Change the Device's Login Password?

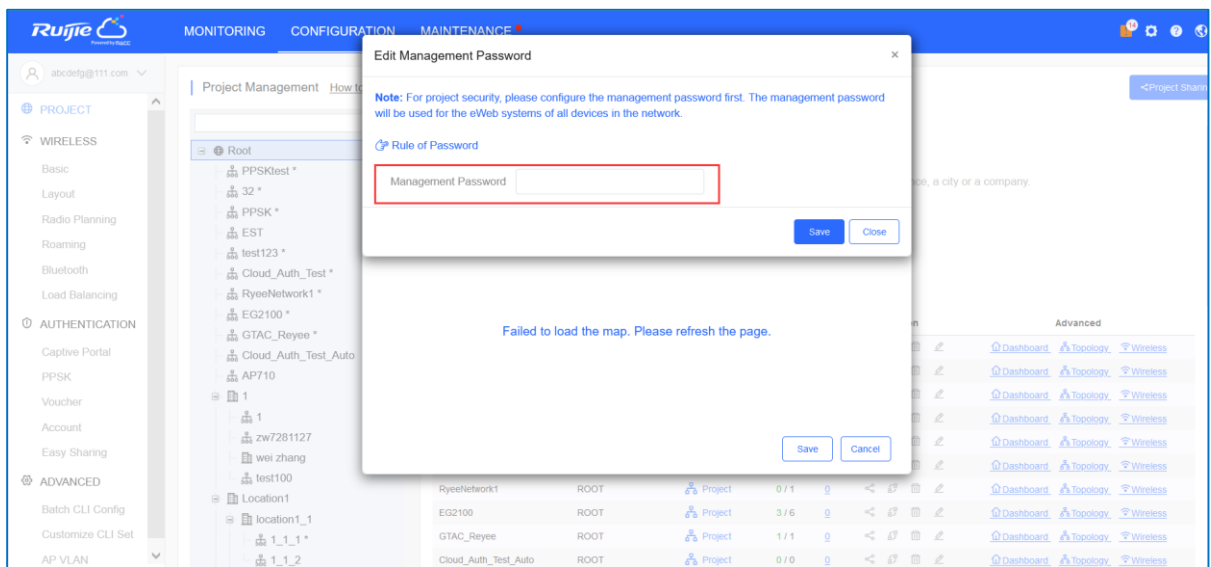
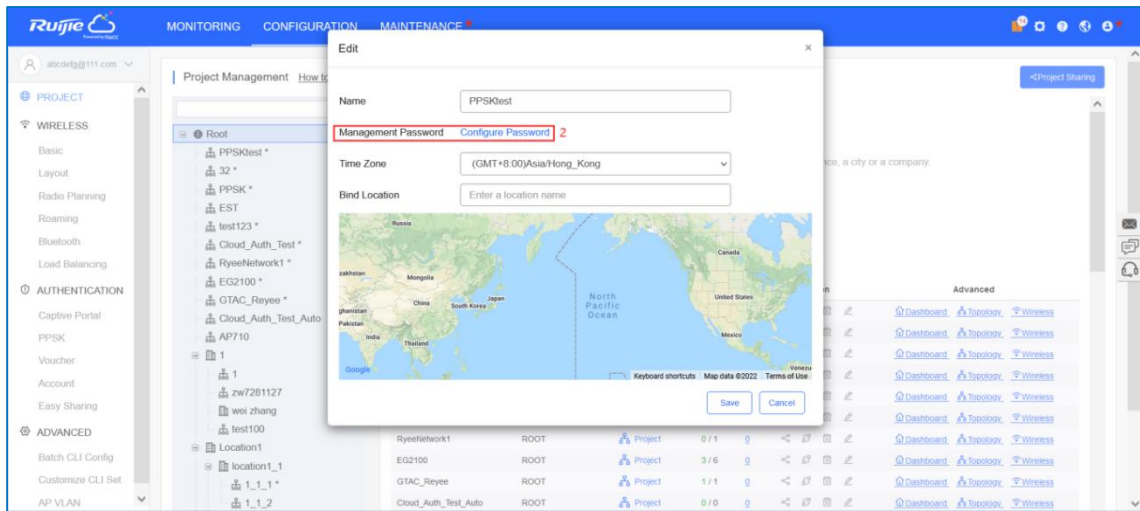
There are three ways to change the device's login password.

- Log in to the Eweb of the device and choose **System** > **Login** to change the device password.

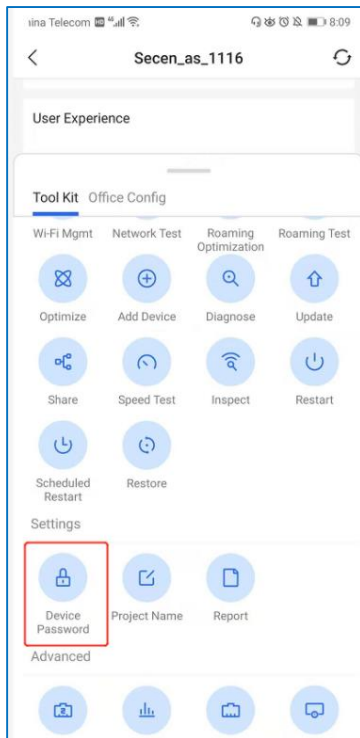


- If the device is online on Ruijie Cloud, you can change the management password on the Eweb of Cloud App.





- Change the password through Ruijie Cloud App.



⚠ Caution

Reyee devices on a network use the same login password.

2.3 What Can I Do If I Forget the Password?

- If you manage your Reyee device on Ruijie Cloud, you can change the password through Ruijie Cloud.
- If the Reyee device is not deployed on Ruijie Cloud, you can press the reset button on the device for more than 5s to restore factory settings.

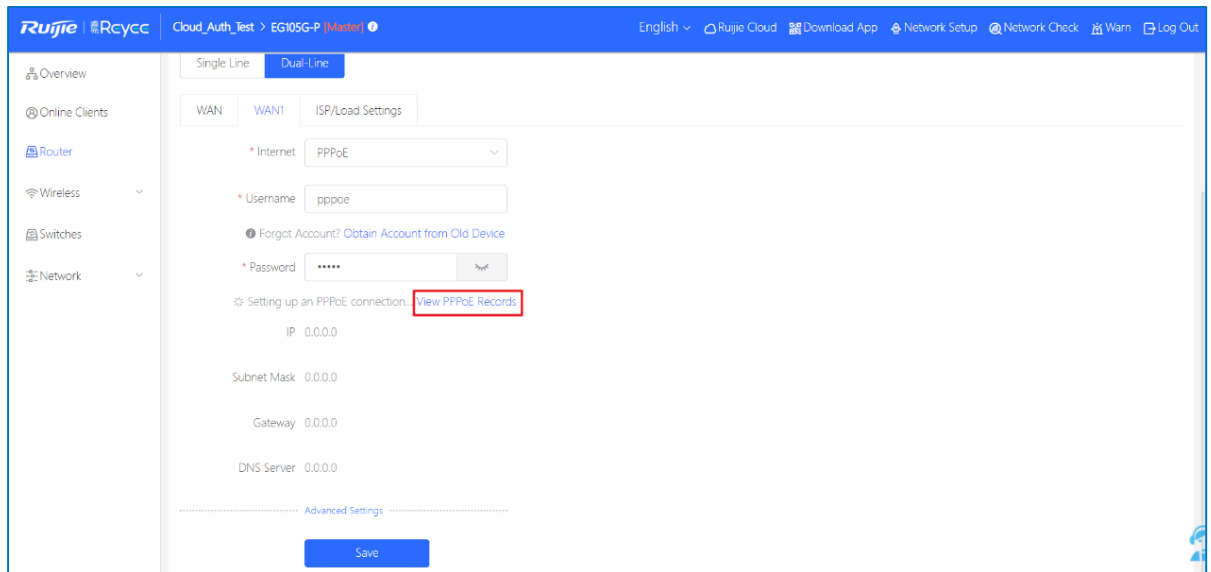
⚠ Caution

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

3 FAQs About Network Access

3.1 What Should I Do If a PPPoE Connection Fails to Be Set Up?

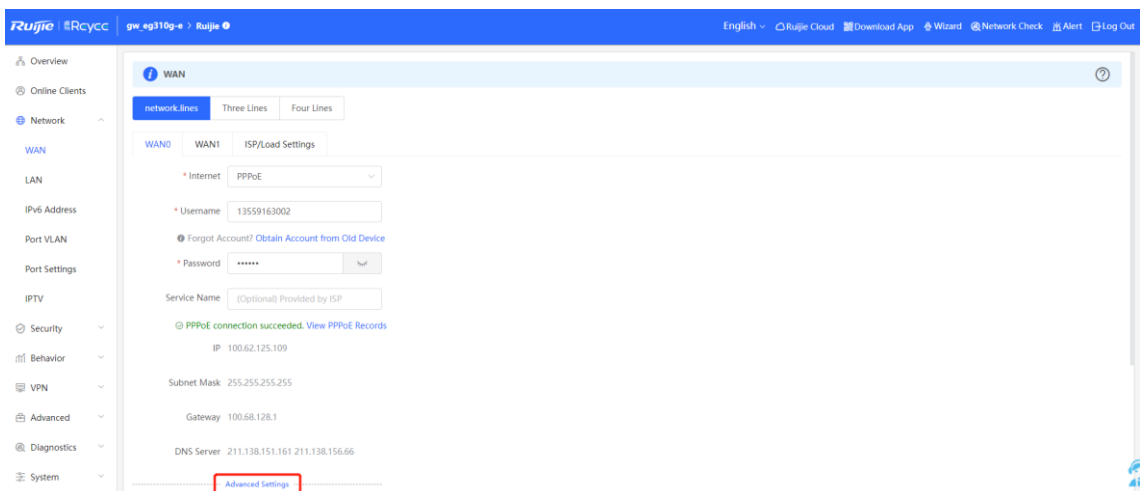
- (1) Check PPPoE records to obtain connection logs.
 - a Choose **Network > WAN**.
 - b Select the target WAN port and click **View PPPoE Records**.



- (2) Check whether the PPPoE account and password are correct.
- (3) Check whether the IP address assigned by the ISP conflicts with the IP address configured on the router.
- (4) Check whether the MTU setting of the device meets requirements of the ISP.

The default MTU is 1480. If the default value does not meet requirements, you can perform the following steps to change it:

- a Choose **Network > WAN**.
- b Select the target WAN port and click **Advanced Settings**. In the expanded section, set an MTU.



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

* MTU

* MAC

802.1Q Tag

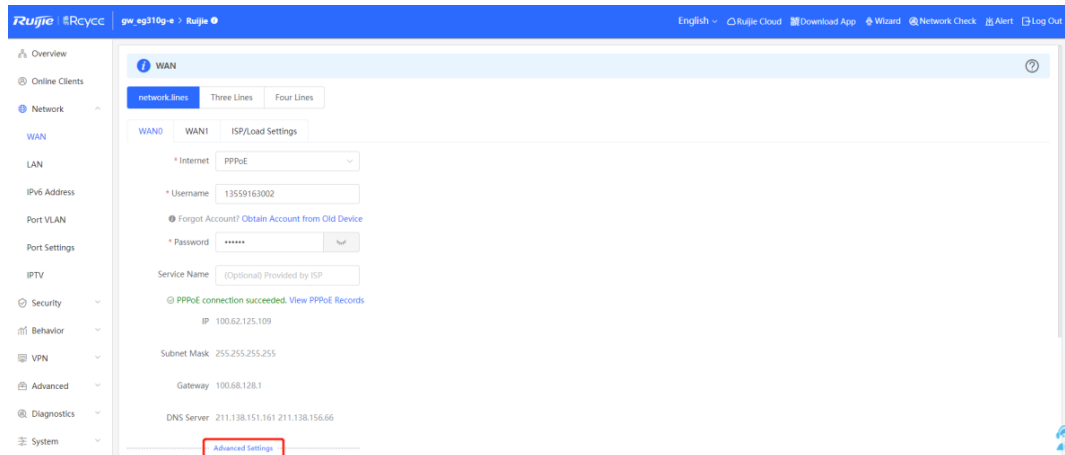
* VLAN ID

Private Line ?

(5) Check whether the VLAN tag needs to be configured for PPPoE.

There is no VLAN tag for PPPoE by default. You can perform the following steps to configure it:

- a Choose **Network > WAN**.
- b Select the target WAN port and click **Advanced Settings**. In the expanded section, enable **802.1Q Tag** and set a VLAN ID.



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

* MTU

* MAC

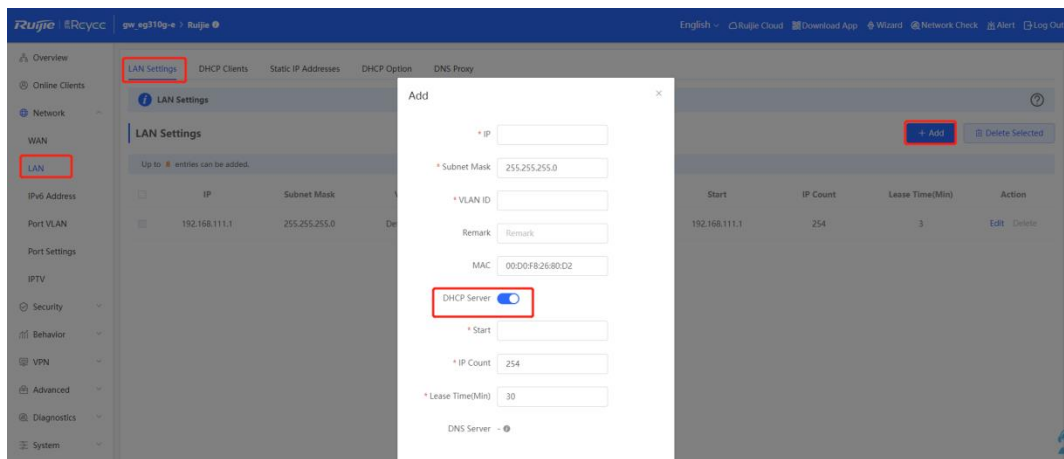
802.1Q Tag

* VLAN ID

Private Line ?

3.2 What Should I Do If the Device Cannot Obtain an IP Address Through DHCP?

- (1) Check the DHCP server configuration.
 - o Check whether the DHCP service is enabled.
 - o Check whether the corresponding DHCP address pool is configured.
 - o Check whether the number of IP addresses in the DHCP address pool is sufficient.



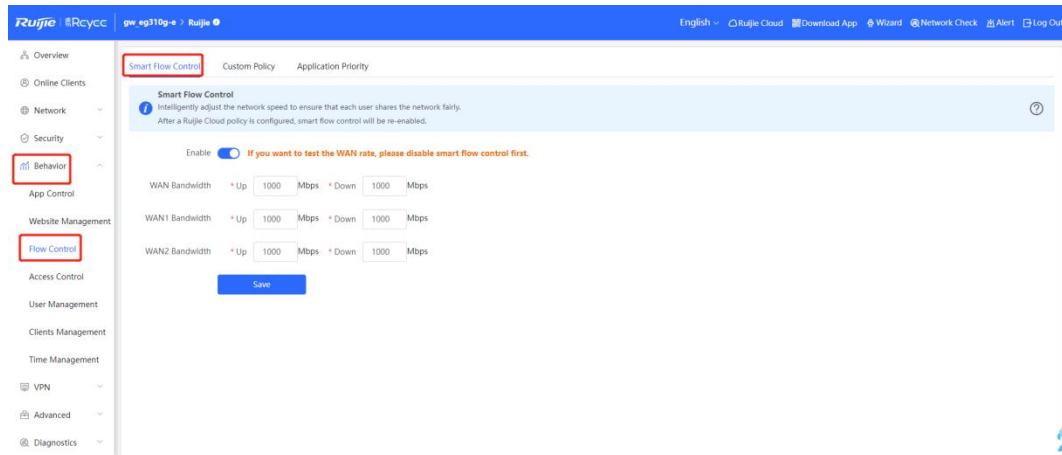
- (2) If switches are deployed, check whether the VLAN, access port, and trunk port are configured correctly.
- (3) If DHCP snooping is configured, check whether the port where the DHCP server is located is configured as a trusted port.

3.3 What Should I Do If Internet Access Is Slow?

Compare test speed results of a PC connected directly to the ISP router or modem and a PC connected to a Reyee device. If the results are the same, the ISP router or modem may fail. If the results are different, perform the following steps.

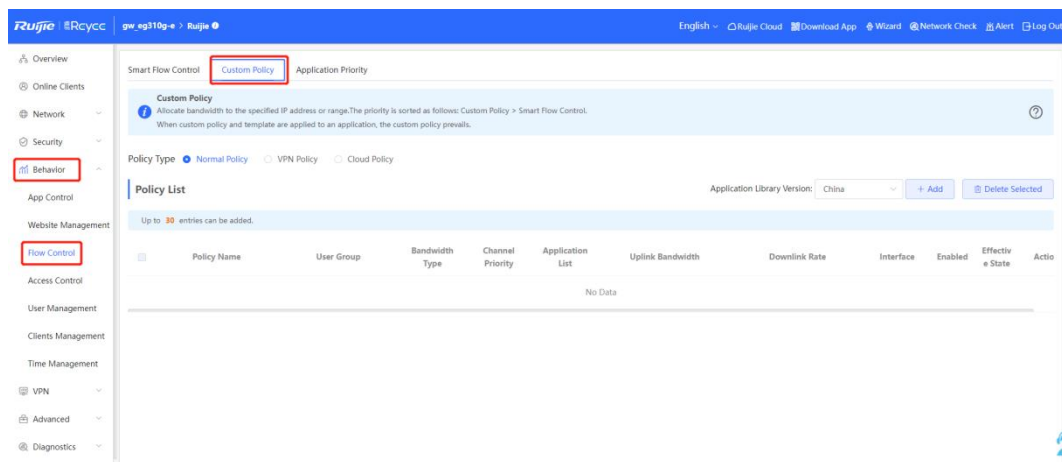
- (1) Check whether **Smart Flow Control** is enabled. If so, disable it.

Choose **Behavior > Flow Control > Smart Flow Control**.



- (2) Check whether **Custom Policy** is configured. If so, add it or disable it.

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



- (3) Replace the network cable for testing.

If the wireless speed is still slow, please continue with the following steps to [Change Wireless Channel, Transmit Power, and Channel Width for the Reyee AP](#). You may change the 2.4 GHz channel width to 40 MHz and 5 GHz channel width to 80 MHz, and try to change a better terminal to perform wireless speed test.

3.4 What Should I Do If I Cannot Access the Internet?

- (1) Check whether the PC or phone obtains the correct IP address.

If the device's IP address is 169.254.x.x or 0.0.0.0, the device does not obtain a correct IP address.

- a End the wired or wireless connection and then reconnect the device.

- b Restart the device.
- (2) Solve this problem according to section [3.2 What Should I Do If the Device Cannot Obtain an IP Address Through DHCP?](#).
- (3) If the device obtains the correct IP address, change the DNS server address to 8.8.8.8 or 8.8.4.4.
- (4) Remove and reinstall the network cable between the gateway or router and ISP.

If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

4 FAQs About SON

4.1 What Is SON?

Self-Organizing Networking (SON) eliminates product limitations and realizes auto-discovery, auto-networking, and auto-configuration between routers, switches, and wireless APs without the need for controllers or Internet access. You can quickly complete device deployment and configuration, remote management, and operation and maintenance of the entire network with Ruijie Cloud App, which greatly reduces the investment of device, labor, and time cost during wireless network construction.

4.2 Which Devices Can Act as the Master Device on the SON?

All EG series routers except the Reyee RG-EG3230/3250 router can act as master devices on the SON.

4.3 How Many Devices Can the SON Support?

The number of devices that can be managed on the SON depends on the maximum number of devices managed by the master device.

The Reyee RG-EG router used as the master device can manage different numbers of devices in AC mode and router mode. The capacity varies with models.

Model	Management capacity	
	AC mode	Router mode
RG-EG105G	300	32
RG-EG105G-P	300	32
RG-EG210G-P	500	150
RG-EG105GW	N/A	32
EG105G V2	300	32
EG105G-P V2	300	32
EG210G-E	500	150
RG-EG305GH-P-E	500	150
RG-EG310GH-E	500	150
RG-EG310GH-P-E	500	150
EG209GS	500	150
RG-EG105GW(T)	N/A	32

Model	Management capacity	
	AC mode	Router mode
RG-EG105GW-X	N/A	64

4.4 What Is the Priority of Devices During Master Device Election of the SON?

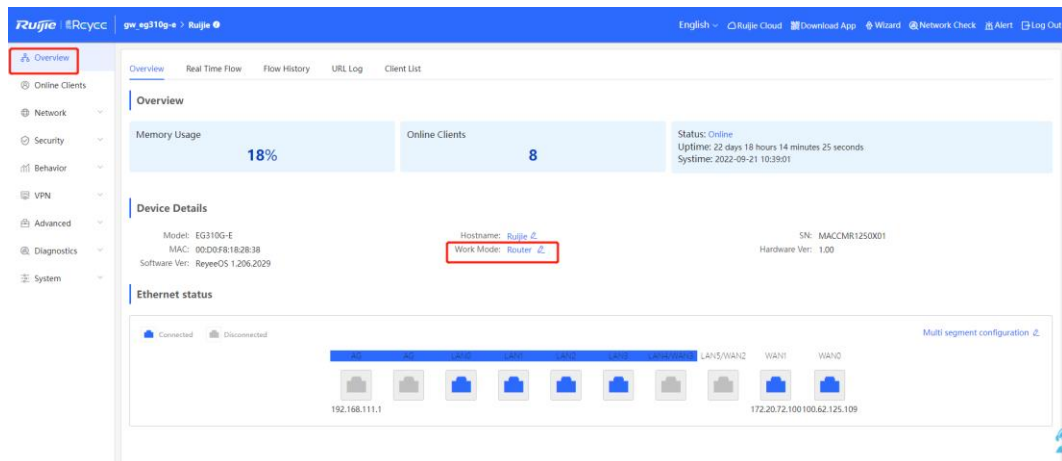
- (1) For different types of devices, the EG in AC mode, EG in router mode, AP in router mode, AP in AP mode, and NBS switch are in descending order of priority.
- (2) For devices of the same type and different models, the priority is related to the CPU, memory, and other parameters (for example, AP radio number) of the device. A larger parameter value indicates a higher priority.
- (3) For devices of the same type and model, a larger MAC address indicates a higher priority.

Caution

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

4.5 How Is SON Enabled on a Device?

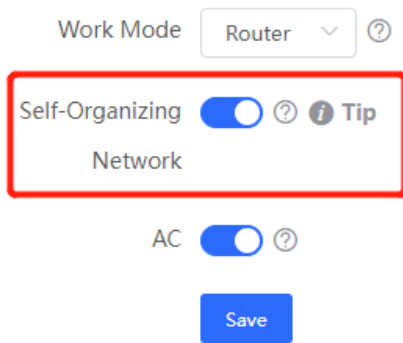
- (1) Click **Overview** and switch **Work Mode** in the **Device Details** pane.



- (2) Enable **Self-Organizing Network** and click **Save**.

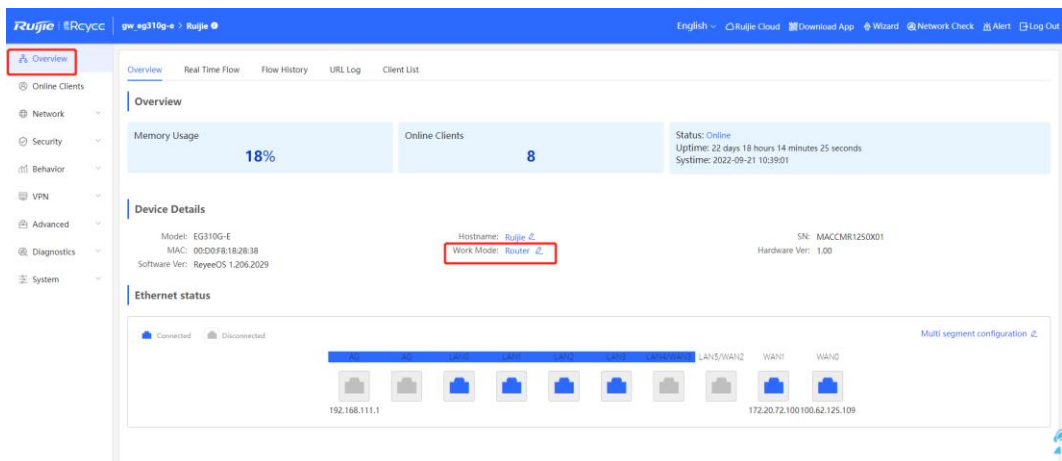
Description:

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.



4.6 How Is SON Disabled on a Device?

- (1) Click **Overview** and switch **Work Mode** in the **Device Details** pane.



- (2) Disable **Self-Organizing Network** and click **Save**.

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 ?

Self-Organizing ?

Network

4.7 How Does the SON Perform Device Discover?

Device discovery is based on Layer 2 broadcast, so all devices must be deployed at the same layer without VLAN or port isolation configuration.

⚠ Caution

The SON establishment does not require a device to access the Internet.

4.8 Does the SON Configuration Change If the Master Device Is Disconnected?

The master device will be re-elected after the old master device is disconnected. The configuration does not change during re-election.

4.9 Does the SON Support the Preemption Mode?

Preemption means that a device with a higher priority is added to a stable network, and the master device will change accordingly. When an EG device is added to RAP networking:

- After the master device is successfully elected, the EG router is added and will become the new master device.
- Preemption time: 7s to 8s

⚠ Caution

An EG router can only act as the master device and cannot be preempted.

4.10 What Is the IP Address of the Master Device on the SON?

The IP address of the master device is 10.44.77.253.

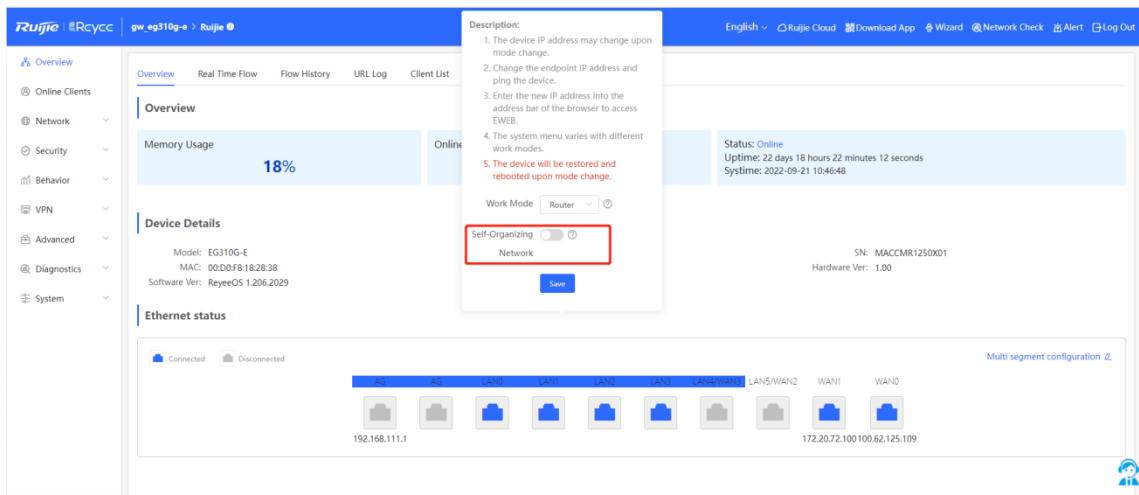
4.11 What Is the Difference Between the Default SSID @Ruijie-s and @Ruijie-m?

@Ruijie-m is generated after the SON established successfully, while @Ruijie-s is generated on a standalone device.

4.12 How Is a Device Specified as the Master Device?

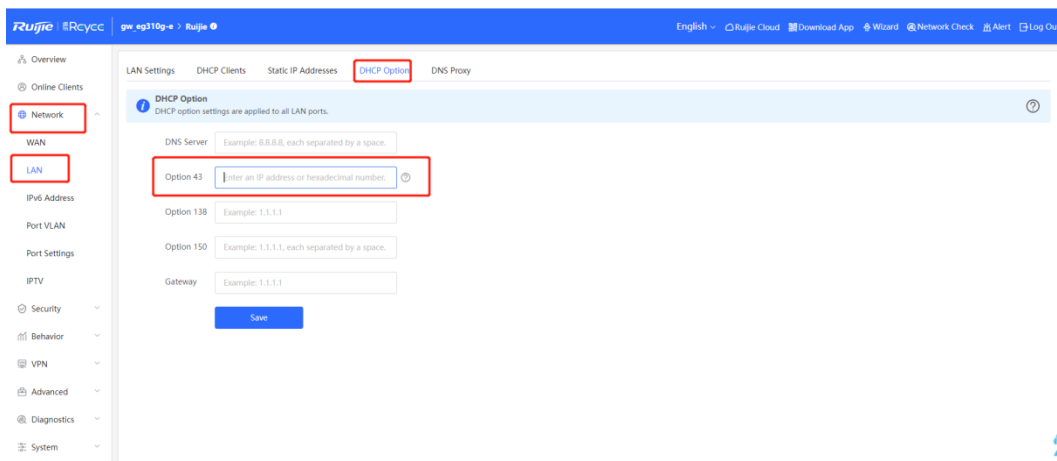
A Reyee EG is required to act as a DHCP server and has SON disabled.

- (1) Disable SON on the DHCP server. The DHCP server will work in standalone mode.



- (2) Configure DHCP Option 43 on the DHCP server: Option 43: #RJ#Master IP.

Example: The master device's IP address is 192.168.100.1, and Option 43 is #RJ#192.168.100.1.

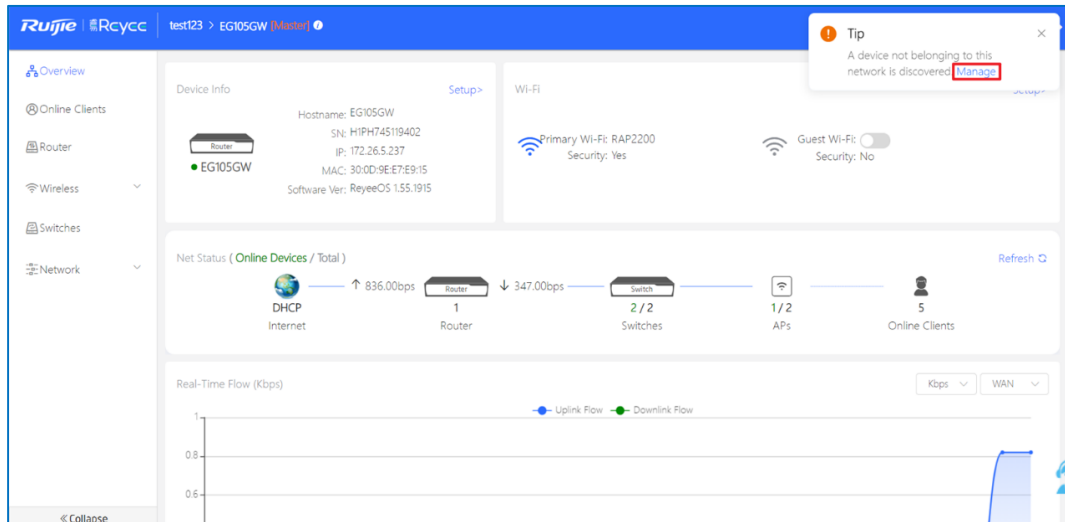


Caution

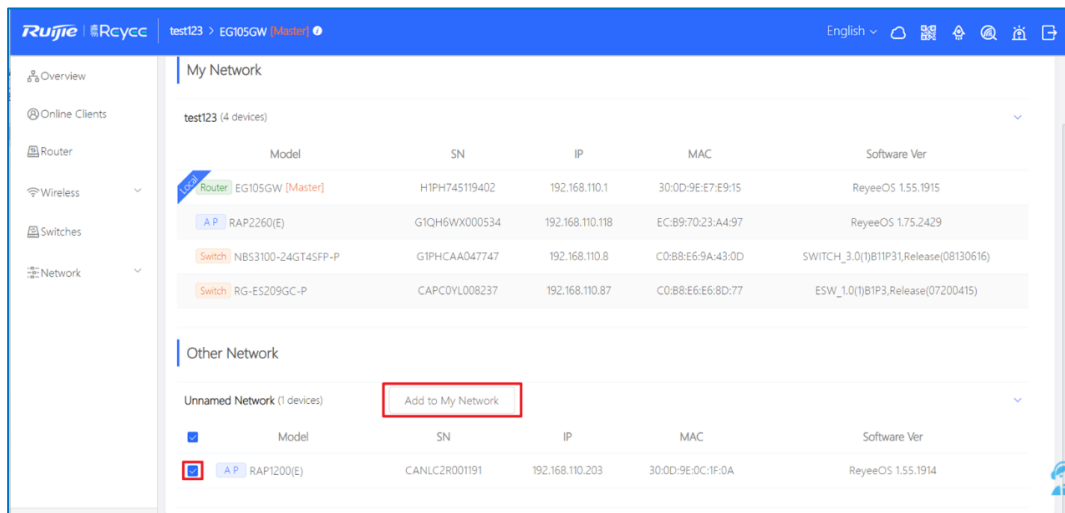
Option 43: When #RJ#Master IP is configured on the device, the SON function cannot be enabled. To enable the SON function, you need to delete the Option 43 configuration.

4.13 How Does the Master Device Add a New Device to the Network?

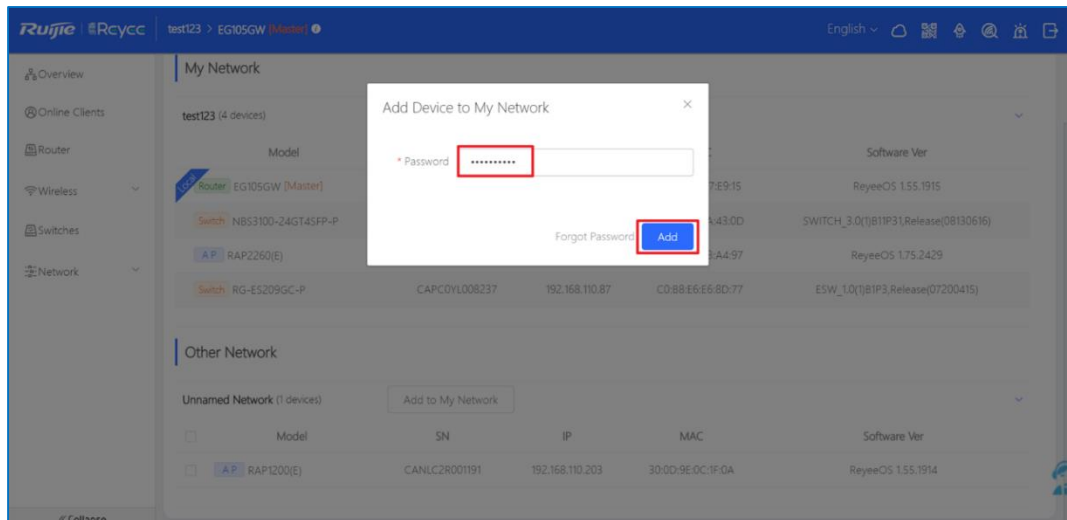
- (1) If the default configuration of the new device is retained, the master device will add it to its own network automatically.
- (2) If the configuration of the new device has been changed, you need to add it to the SON manually on the web page of the master device.
 - a Click **Manage** of **Tip** in the top right corner.



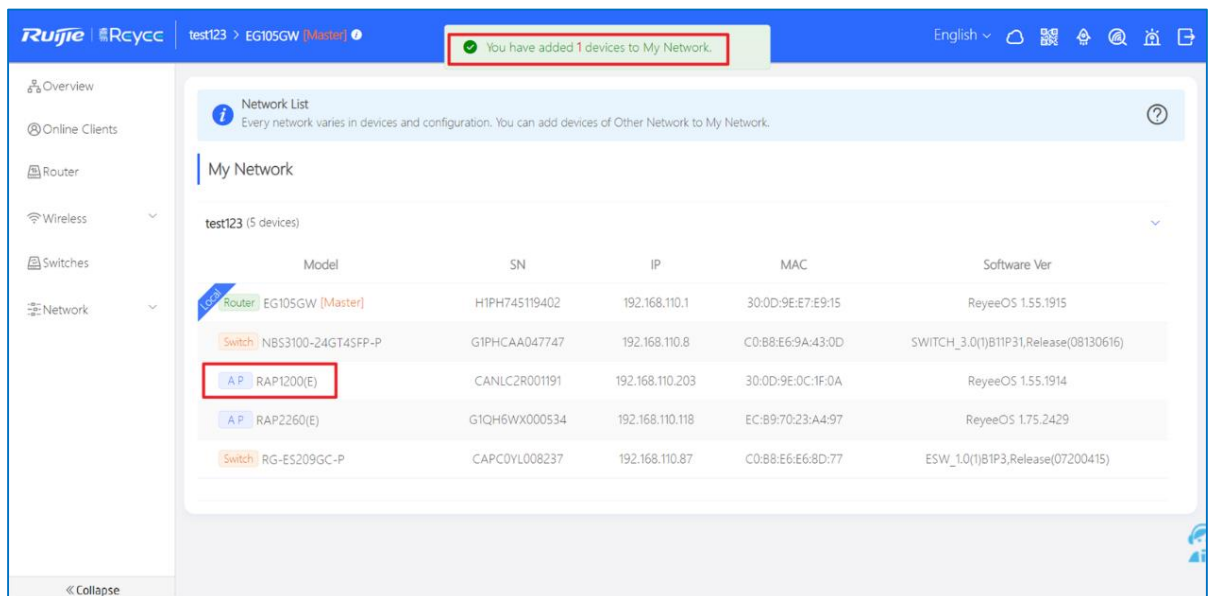
- b Select the device you want to add and click **Add to My Network**.



- c Fill in the password of the device and click **Add**.



The device is added successfully.



4.14 The SON Has Been Configured Successfully, but Devices Still Cannot Be Online on Ruijie Cloud. Why?

- (1) Check whether the firmware is the latest. If not, upgrade the firmware.

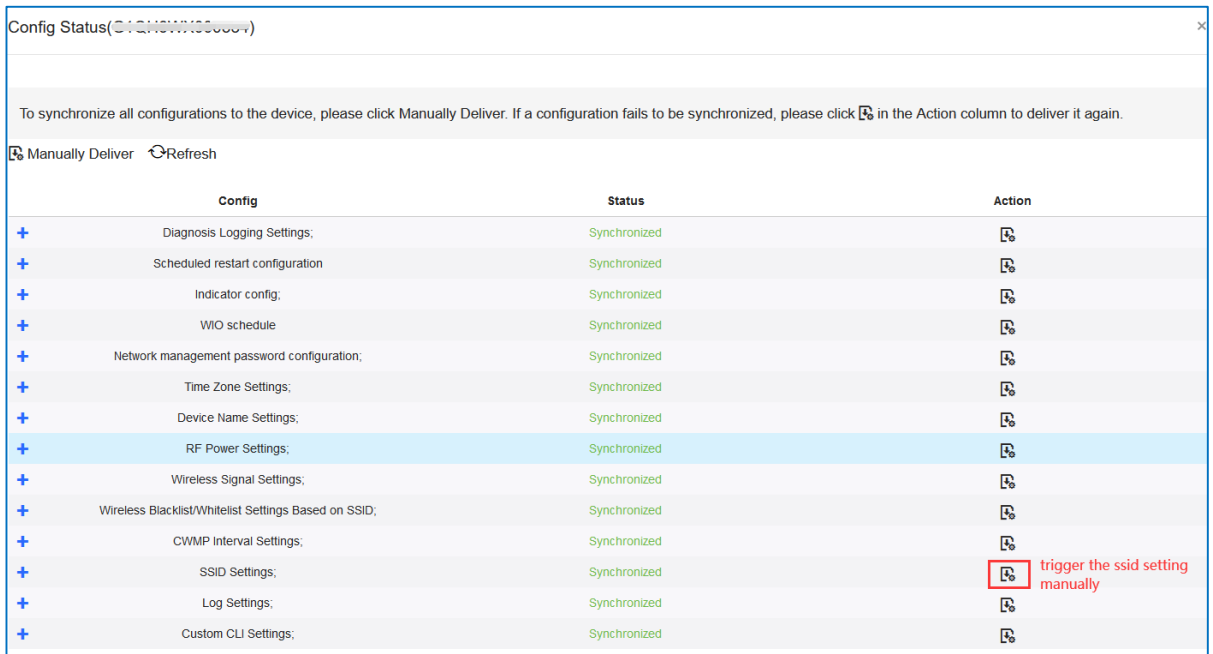
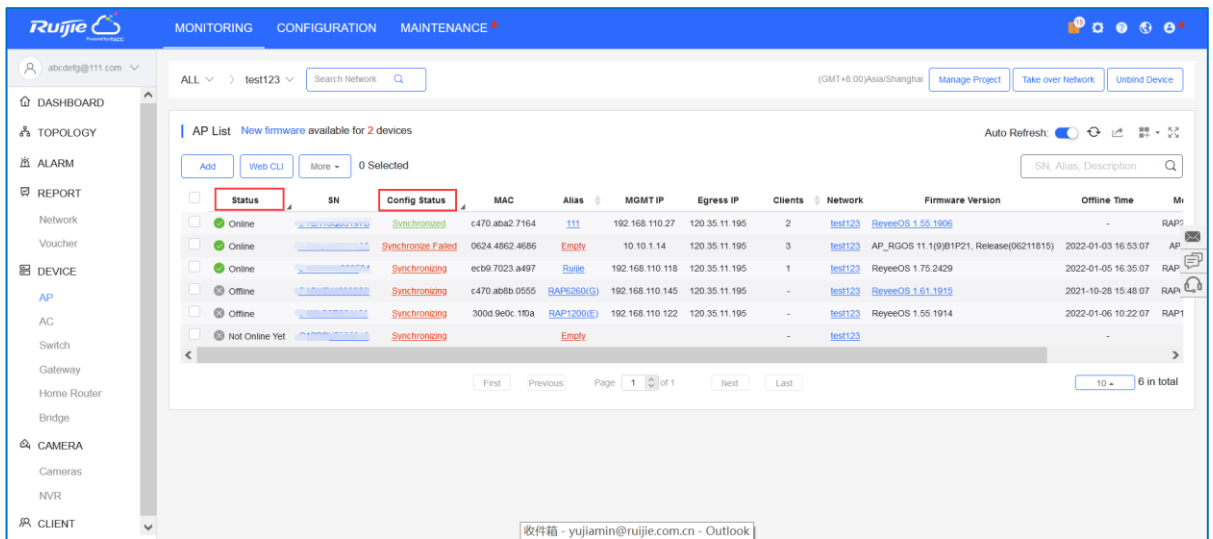
Ping the cloud's default URL (devicereg.ruijienetworks.com) on the device. If the ping operation fails, check the device's DNS configuration and network connectivity. For details, see [What Should I Do If I Cannot Access the Internet?](#).

- (2) Reset the device.

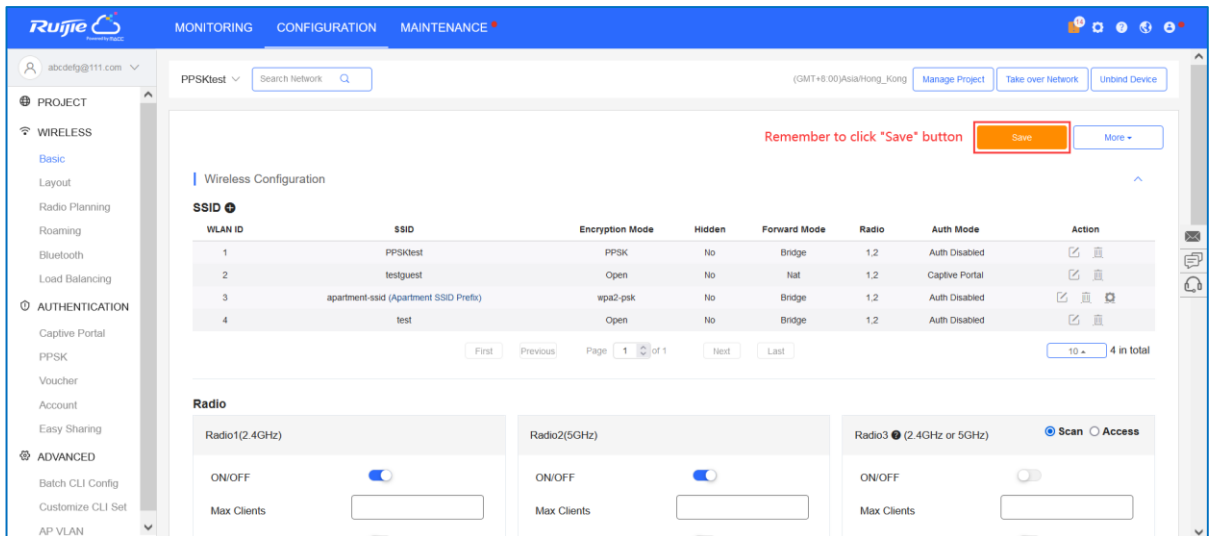
5 FAQs About Wireless Configuration

5.1 What Can I Do If SSID Configuration on Ruijie Cloud Fails to Be Synchronized to a Reyeer Device?

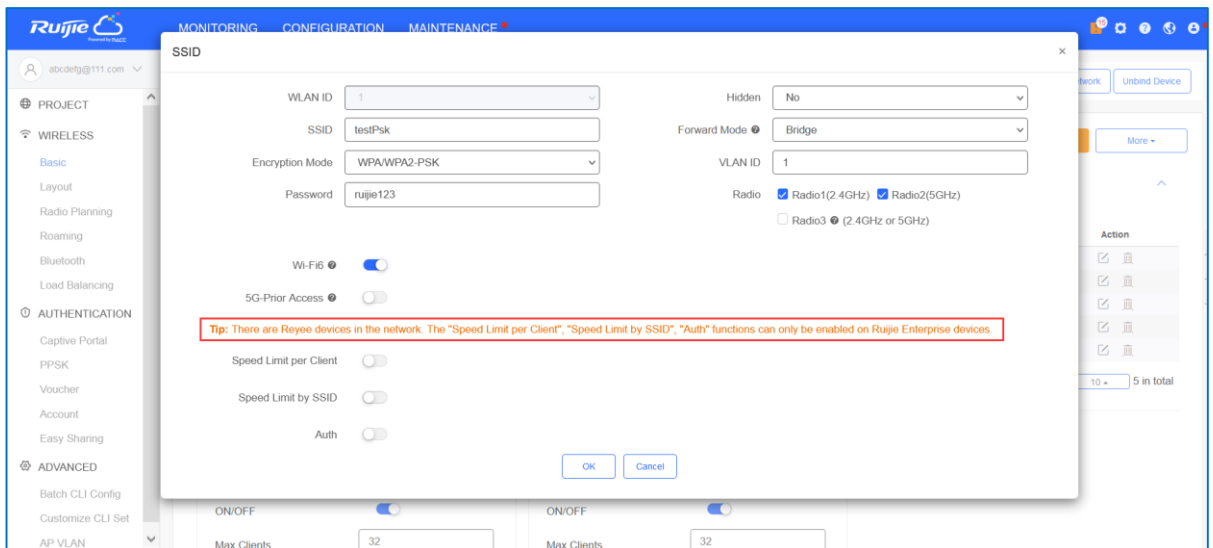
- (1) Check **Status** and **Config Status** of the AP. If the AP status is offline, the cloud does not deliver the configurations to the device. If the AP is online and the value of **Config Status** is **Synchronizing**, you can trigger the configuration synchronization manually.



- (2) Check whether the SSID configuration is saved successfully. Click **Save** and check the device configuration again.



- (3) Check whether the AP version is the latest one. If not, upgrade it.
- (4) If the configured features are not supported by the Reye device, configurations are not synchronized to the Reye device.



5.2 How Are Radio Settings Adjusted When the Wireless Network Quality Is Low?

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

Caution

After optimization, settings of the Wi-Fi network are reset, and clients need to reconnect to the W-Fi network. Therefore, exercise caution when performing this operation.

5.2.1 Optimizing the Radio Channel

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

Choose the best channel identified by Wi-Fi MOHO or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. More devices in a channel mean more serious interference.

Note

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

Radio Frequency

Country/Region China (CN)

2.4G Channel Width Auto

Client Count Limit 32

Kick-off Threshold Disable -75dBm -50dBm

2.4G Channel Auto

Transmit Power Auto

Roaming Sensitivity 1 (2.412GHz)

5G Channel Width Auto

Client Count Limit 32

Kick-off Threshold Disable -75dBm -50dBm

5G Channel Auto

Transmit Power Auto Lower Low Medium High

Roaming Sensitivity Low 20% 40% 60% 80% High

Caution

- The channel and transmit power of each AP must be modified on the AP.

5.2.2 Optimizing the Channel Width

Choose **Wireless > Radio Frequency**.

If the interference is severe, select a lower channel width to avoid network freezing. The AP supports the channel width of 20 MHz and 40 MHz. You are advised to select 20 MHz channel width. After changing the channel width, click **Save** to make the configuration take effect immediately.

Caution

In SON mode, the channel width settings will be synchronized to all devices on the network.

Radio Frequency

Country/Region	China (CN)		
2.4G Channel Width	Auto	5G Channel Width	Auto
Client Count Limit	Auto	Client Count Limit	32
Kick-off Threshold	20MHz 40MHz	Kick-off Threshold	Disable -75dBm -50dBm
2.4G Channel	Auto	5G Channel	Auto
Transmit Power	Auto Lower Low Medium High	Transmit Power	Auto Lower Low Medium High
Roaming Sensitivity	Low 20% 40% 60% 80% High	Roaming Sensitivity	Low 20% 40% 60% 80% High

Save

5.2.3 Configuring the Disconnection Threshold

Choose **Wireless > Radio Frequency**.

The farther a client is away from an AP, the lower the signal strength is. When the signal strength is lower than the threshold, the client will be disconnected and has to select a nearer Wi-Fi signal.

Radio Frequency

Country/Region	China (CN)		
2.4G Channel Width	Auto	5G Channel Width	Auto
Client Count Limit	32	Client Count Limit	32
Kick-off Threshold	Disable -75dBm -50dBm	Kick-off Threshold	Disable -75dBm -50dBm
2.4G Channel	Auto	5G Channel	Auto
Transmit Power	Auto Lower Low Medium High	Transmit Power	Auto Lower Low Medium High
Roaming Sensitivity	Low 20% 40% 60% 80% High	Roaming Sensitivity	Low 20% 40% 60% 80% High

Save

Caution

In SON mode, the disconnection threshold settings will be synchronized to all devices on the network.

5.2.4 Configuring the Client Limit

Choose **Wireless > Radio Frequency**.

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

Radio Frequency

<p>Country/Region China (CN) ▾</p> <p>2.4G Channel Width Auto ▾</p> <p>Client Count Limit 32</p> <p>Kick-off Threshold ⓘ ○ Disable -75dBm -50dBm </p> <p>2.4G Channel Auto ▾</p> <p>Transmit Power ⓘ ○ Auto Lower Low Medium High </p> <p>Roaming Sensitivity ⓘ ○ Low 20% 40% 60% 80% High </p>	<p>5G Channel Width Auto ▾</p> <p>Client Count Limit 32</p> <p>Kick-off Threshold ⓘ ○ Disable -75dBm -50dBm </p> <p>5G Channel Auto ▾</p> <p>Transmit Power ⓘ ○ Auto Lower Low Medium High </p> <p>Roaming Sensitivity ⓘ ○ Low 20% 40% 60% 80% High </p>
--	--

Save

i Note

In SON mode, the client limit refers to the maximum number of clients connected to all Wi-Fi networks. If you want to specify the client limit for one single AP, group the AP and configure the client limit for this group. Alternatively, proceed with the configuration in standalone mode.

5.2.5 Configuring the Roaming Sensitivity

Choose **Wireless > Radio Frequency**.

The roaming sensitivity enables the device to proactively disconnect a client from the Wi-Fi network when the client is far away. In this case, the client has to re-select the nearest signal, thereby improving the sensitivity of wireless roaming. A higher roaming sensitivity level indicates a smaller wireless signal coverage. To improve the signal quality for a client moving within more than one Wi-Fi coverage, improve the roaming sensitivity level. You are advised to keep the default settings.

Radio Frequency

Country/Region	<input type="text" value="China (CN)"/>		
2.4G Channel Width	<input type="text" value="Auto"/>	5G Channel Width	<input type="text" value="Auto"/>
Client Count Limit	<input type="text" value="32"/>	Client Count Limit	<input type="text" value="32"/>
Kick-off Threshold	<input type="range" value="Disable -75dBm -50dBm"/>	Kick-off Threshold	<input type="range" value="Disable -75dBm -50dBm"/>
2.4G Channel	<input type="text" value="Auto"/>	5G Channel	<input type="text" value="Auto"/>
Transmit Power	<input type="range" value="Auto Lower Low Medium High"/>	Transmit Power	<input type="range" value="Auto Lower Low Medium High"/>
Roaming Sensitivity	<input type="range" value="Low 20% 40% 60% 80% High"/>	Roaming Sensitivity	<input type="range" value="Low 20% 40% 60% 80% High"/>

(1) Configuring WIO

Choose **Wireless > WIO**.

Check **I have read the notes**, and click **Network Optimization** to optimize the wireless network. You are advised to set a scheduled task to optimize the wireless network in the early hours of the morning or when the network is idle.

Caution

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

[Network Optimization](#)

[Optimization Record](#)



Description:

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

Notes:

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

I have read the notes.

Scheduled Optimization



Scheduled Optimization

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

Enable

Day

Time :

Save

5.3 Can Reyee EG Routers Support Wi-Fi?

No, other Reyee EGs except EG105GW support Wi-Fi.

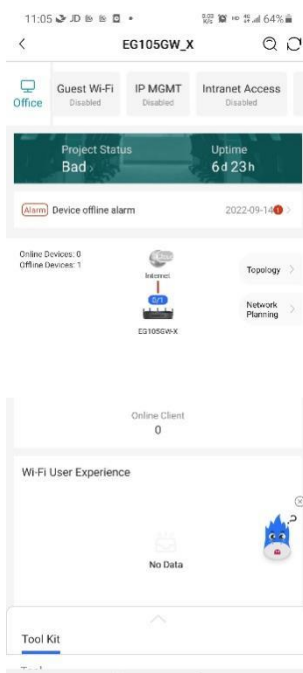
6 FAQs About Guest Wi-Fi

6.1 What Is Guest Wi-Fi?

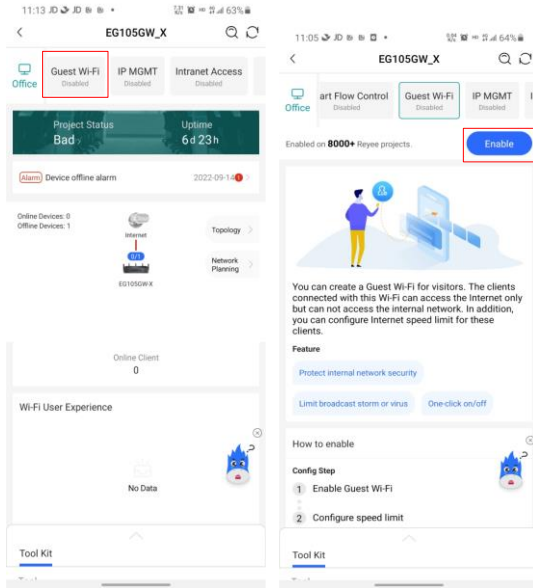
The guest Wi-Fi network can provide guests with an independent Internet access environment, which is isolated from the network connected to main terminals. By creating a guest Wi-Fi network, guest devices are allowed to access the internet, but are not allowed to connect to the internal network.

6.2 How Do I Configure Guest Wi-Fi on Ruijie Cloud App?

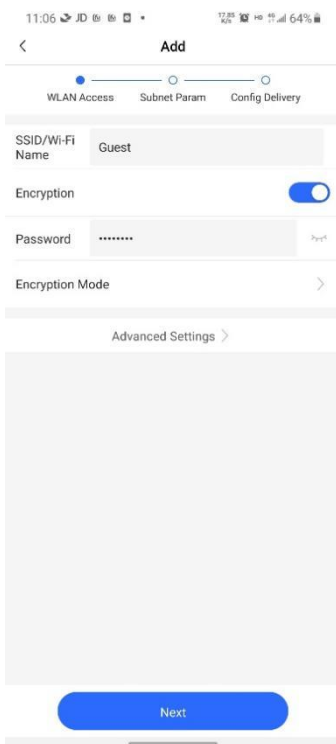
(1) Click the project you want to set for your guest Wi-Fi.



(2) Find out **Guest Wi-Fi** on the toolbar and click the **Enable** button.



- (3) On the **Guest Wi-Fi** page, set the SSID, password, rate limit, VLAN ID, and IP address pool for the guest Wi-Fi, and click **Save**.

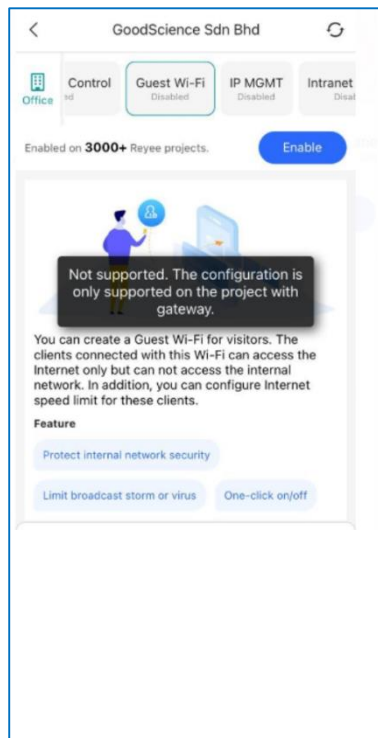


⚠ Caution

- All these configurations have their default settings, but you also can customize them.
- Configuring guest Wi-Fi on the Eweb is of no use.
- For the guest Wi-Fi, ACLs needs to be configured on a Reyee EG.

6.3 What Can I Do If the System Displays the Message that "The configuration is only supported on the project with gateway?"

When using the guest Wi-Fi function, ensure that there is an EG router in the project. This is because ACLs need to be configured on the EG router.



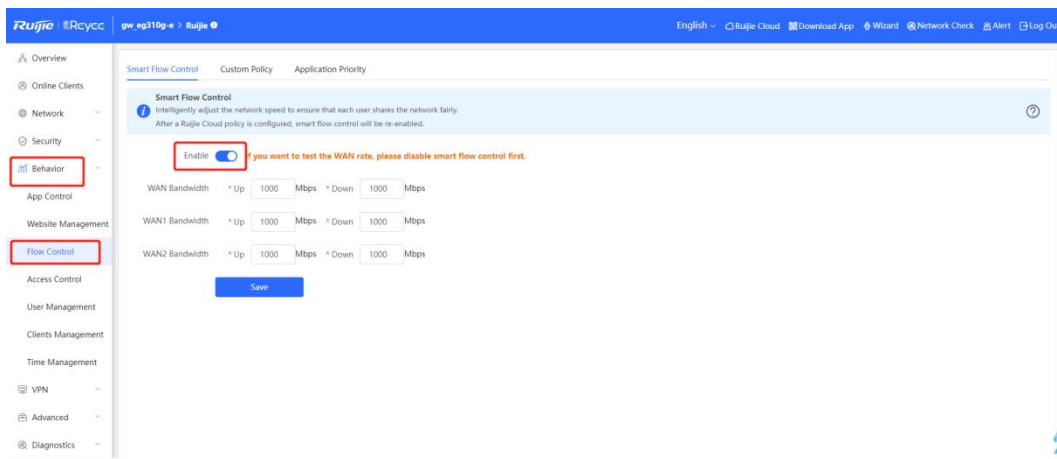
7 FAQs About Flow Control

7.1 What Is Flow Control?

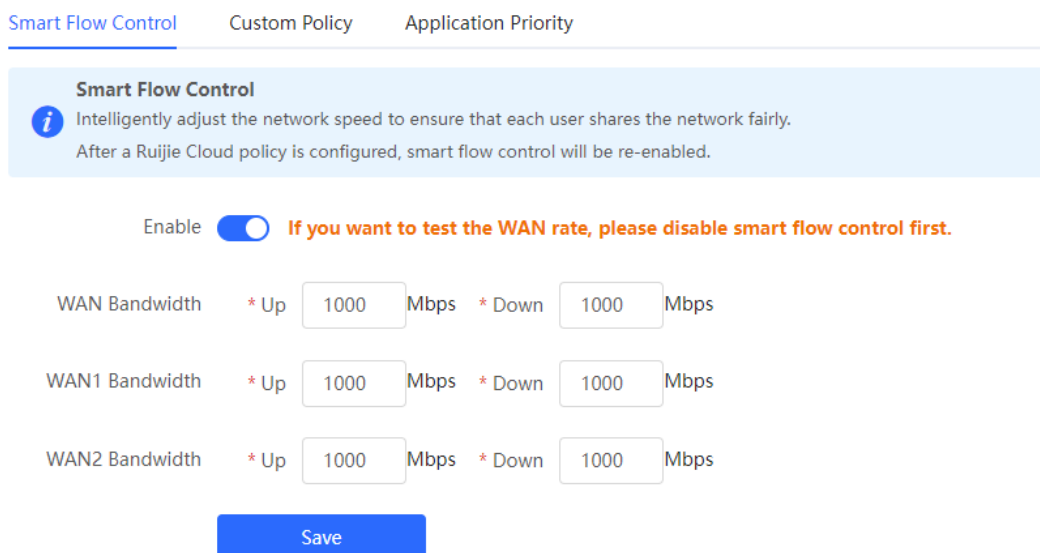
Reyee Smart Flow Control is used to avoid congestion by optimizing users' traffic. When the total user traffic is lower than the maximum WAN bandwidth, the rate limit policy is not applied. Each user will get the required bandwidth. However, when the total user traffic exceeds the maximum WAN bandwidth, the user-based rate limit will take effect. The total WAN bandwidth will be equally allocated to every user.

7.2 How Do I Configure Flow Control?

- (1) Choose **Behavior > Flow Control > Smart Flow Control**, and then enable **Smart Flow Control**.



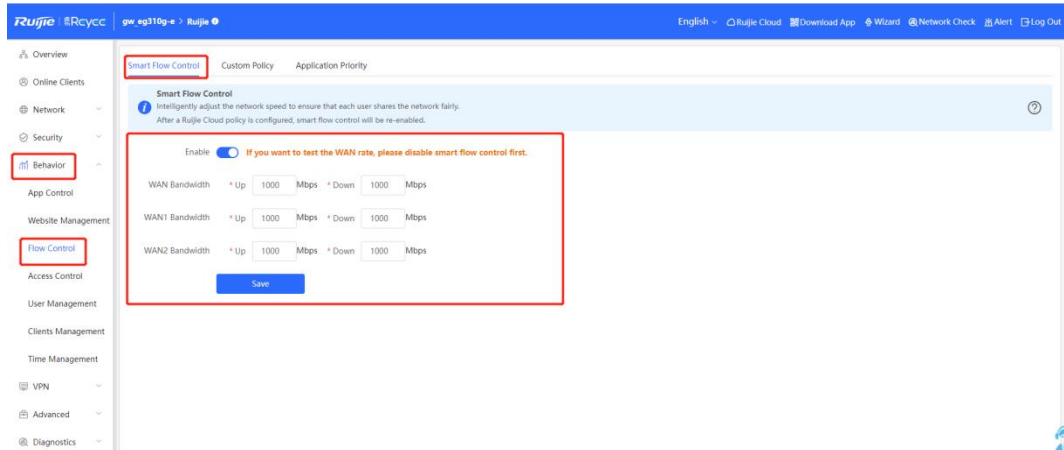
- (2) Fill in the WAN bandwidth and save the configuration.



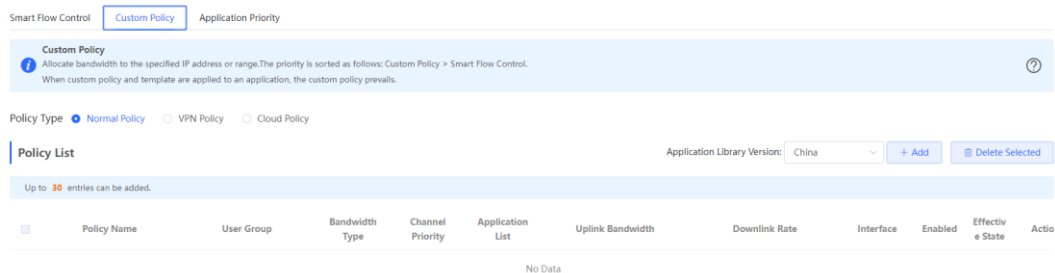
7.3 How Is Flow Control Configured for Specific Users on a Reyee EG Router?

Perform the following steps:

- (1) Configure a smart flow control policy.
 - a Choose **Behavior > Flow Control > Smart Flow Control**.
 - b Enable **Smart flow control**.
 - c Set the uplink and downlink rate limit for the WAN port and click **Save**.



- (2) After step1 is finished, **Custom Policy** will be displayed. Click **Add** to add a policy.



- (3) Fill in **Policy Name**, **IP range**, **Bandwidth Type**, and **Rate**.

×

Add

* Policy Name

Type User Group Custom

* User Group ?

Bandwidth Type Shared Independent

Application All Applications Custom

Channel Priority ?

Bandwidth Limit Limit Kbps No Limit

Uplink Bandwidth * CIR * PIR ?

Downlink Rate * CIR * PIR ?

* Interface

Enabled

Smart Flow Control Custom Policy

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

Policy List + Add + Delete Selected

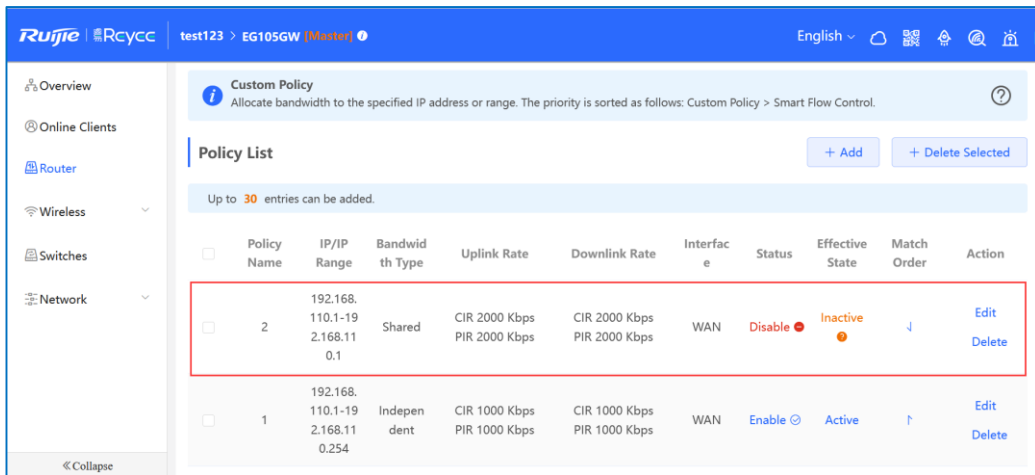
Up to 30 entries can be added.

<input type="checkbox"/>	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
<input type="checkbox"/>	test	192.168.100.2-192.168.100.100	Shared	CIR 10000 Kbps PIR 10000 Kbps	CIR 10000 Kbps PIR 10000 Kbps	WAN	Enable ?	Active	Edit Delete

- ⚠ Caution**
- **Bandwidth Type: Shared** means that all IP addresses share the total bandwidth. **Independent** means that the rate limit is set per IP address.
 - **CIR:** indicates the committed information rate.
 - **PIR:** indicates the peak information rate.

7.4 What Can I Do If the Custom Policy of Flow Control Do Not Take Effect?

- (1) Check the status of the policy.



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

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

Up to 30 entries can be added.

<input type="checkbox"/>	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Match Order	Action
<input type="checkbox"/>	2	192.168.110.1-192.168.110.254	Shared	CIR 2000 Kbps PIR 2000 Kbps	CIR 2000 Kbps PIR 2000 Kbps	WAN	Disable ●	Inactive ●	↓	Edit Delete
<input type="checkbox"/>	1	192.168.110.1-192.168.110.254	Independent	CIR 1000 Kbps PIR 1000 Kbps	CIR 1000 Kbps PIR 1000 Kbps	WAN	Enable ☺	Active ●	↑	Edit Delete

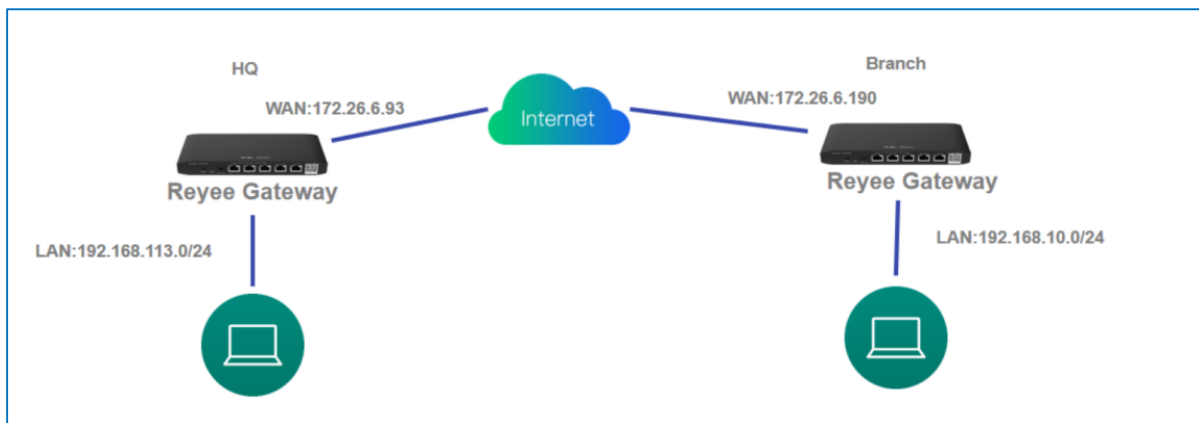
- (2) Check whether the user's IP address is in the range defined by **IP/IP Range** of the policy.
- (3) Check the configuration.
 - If you select **Shared Bandwidth Type**, all IP addresses share the total bandwidth;
 - If you select **Independent Bandwidth Type**, the rate limit is set per IP address.

8 FAQs About VPN

8.1 How Is IPsec VPN Configured on a Reyee EG Router?

IPsec VPN is used for site-to-site scenarios. For example, three branches of a company are distributed in three different places of the Internet. Each branch uses a gateway to establish tunnels with each other, and data between company intranets (several PCs) is securely exchanged through the IPsec VPN tunnel established by the gateways.

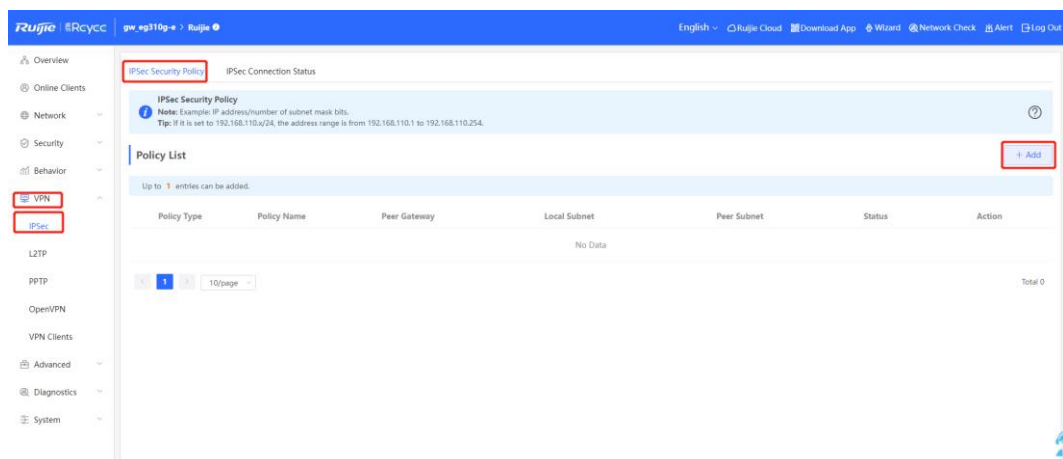
An IPsec VPN is applied to the following scenario.



Perform the following steps to configure IPsec VPN.

(1) Headquarters side:

- a Log in to a Reyee EG router with the default IP address of 192.168.110.1.
- b Choose **VPN > IPsec > IPsec Security Policy**, and then click **Add** to add a policy.



- c Configure the IPsec VPN policy.

Add ×

i 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

* Policy Name

Interface ⓘ

* Local Subnet

* Pre-shared Key

Status

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

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

Cancel

OK

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

	Authentication	Encryption	DH Group
IKE Policy 1	<input type="text" value="sha1"/>	<input type="text" value="3des"/>	<input type="text" value="dh1"/>
IKE Policy 2	<input type="text" value="sha1"/>	<input type="text" value="des"/>	<input type="text" value="dh1"/>
IKE Policy 3	<input type="text" value="sha1"/>	<input type="text" value="3des"/>	<input type="text" value="dh2"/>
IKE Policy 4	<input type="text" value="md5"/>	<input type="text" value="des"/>	<input type="text" value="dh1"/>
IKE Policy 5	<input type="text" value="md5"/>	<input type="text" value="3des"/>	<input type="text" value="dh2"/>

Negotiation Main Mode Aggressive Mode
Mode

Local ID Type IP NAME

Peer ID Type IP NAME

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

..... 2. Connection Policy

Transform Set 1

Transform Set 2

Perfect Forward

Secrecy

* Lifetime

(2) Branch side:

- a Log in to a Reyeeg EG router with the default IP address of 192.168.110.1.
- b Choose **VPN > IPsec > IPsec Security Policy**, and then click **Add** to add a policy.
- c Configure the IPsec policy, and ensure that the IKE policy and connection policy are the same on both sides.

Add ×

Policy Type Client Server

* Policy Name

* Peer Gateway +

Interface ?

* Local Subnet

* Peer Subnet +

* Pre-shared Key

Status

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

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

Negotiation Main Mode Aggressive Mode

Mode

Local ID Type IP NAME

Peer ID Type IP NAME

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

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

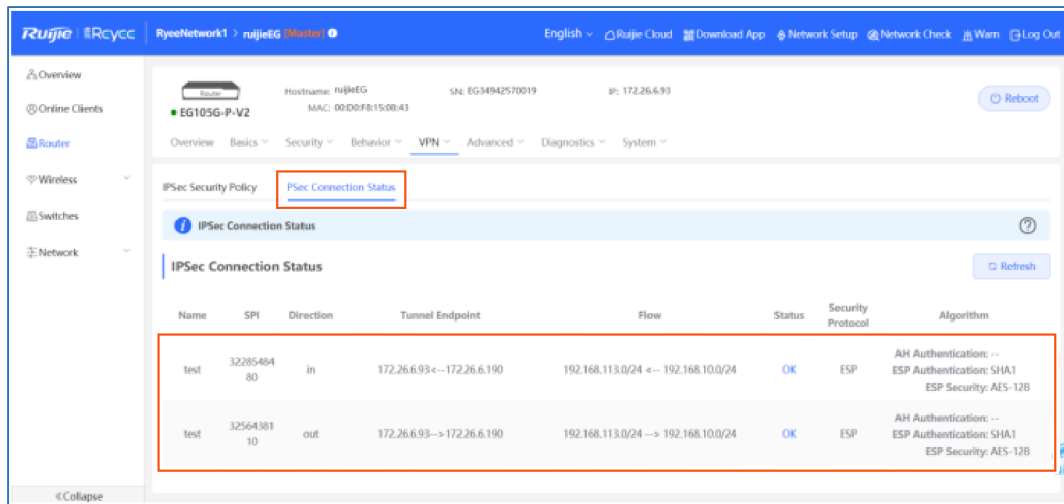
Transform Set 1

Transform Set 2

Perfect Forward Secrecy

* Lifetime

- d Check the IPsec connection status.



⚠ Caution

If the EG router on the headquarters has no public IP address configured on external devices that want to access the EG router of the headquarters, you need to configure port mapping on external devices and configure **Local ID Type** as **NAME** on EG routers of the headquarters and branches.

8.2 Can I Use a Reyee EG Router to Establish an IPsec VPN with Devices of Other Brands or Ruijie EG Routers?

- A Reyee EG router can establish an IPsec VPN with other Ruijie EG routers.
- A Reyee EG router can establish an IPsec VPN with IPsec-capable devices of other brands.

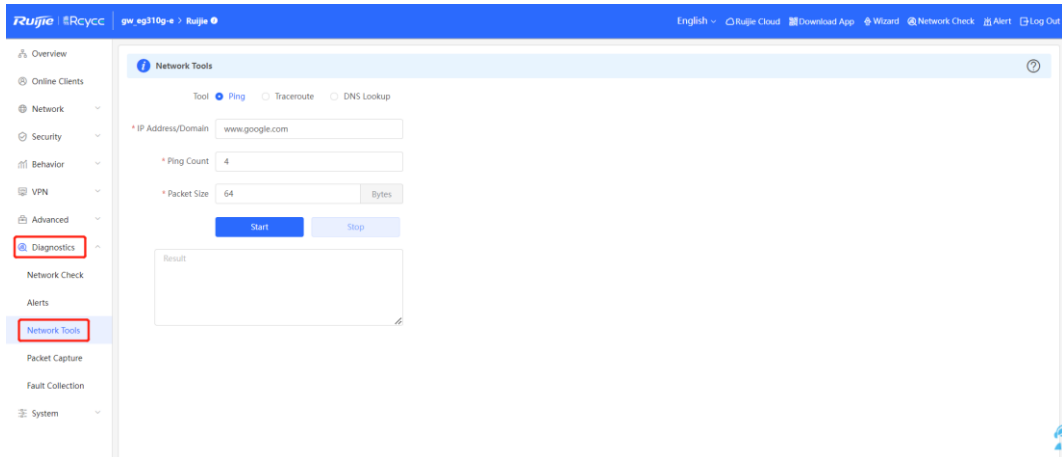
8.3 Can Reyee EG Routers Support IKEv2?

Reyee EG routers support only IKEv1 but not IKEv2.

8.4 What Can I Do If Reyee EG Routers Cannot Connect to the IPsec VPN?

- (1) Check whether the EG router of a branch can ping the EG router of the headquarters. If not, check the network connection between two EG routers.

Choose **Diagnostics > Network Tools** and start the ping operation.



- (2) Check whether the settings are correct according to 12.1 How Can I Configure IPTV on a Reyee EG Router?.
- (3) Check whether the WAN IP address of the EG router of the headquarters is a public IP address. If not, , configure DMZ or port mapping (IPsec VPN use UDP ports 500 and 4500) on your external device and configure **Local ID Type** as **NAME** on devices of the headquarters and branches.

1. Set IKE Policy

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

Negotiation Main Mode Aggressive Mode

Mode

Local ID Type IP **NAME**

* Local ID

Peer ID Type IP **NAME**

* Peer ID

* Lifetime

DPD **Enable** Disable

* DPD Interval

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

	Authentication	Encryption	DH Group
IKE Policy 1	<input type="text" value="sha1"/>	<input type="text" value="3des"/>	<input type="text" value="dh1"/>
IKE Policy 2	<input type="text" value="sha1"/>	<input type="text" value="des"/>	<input type="text" value="dh1"/>
IKE Policy 3	<input type="text" value="sha1"/>	<input type="text" value="3des"/>	<input type="text" value="dh2"/>
IKE Policy 4	<input type="text" value="md5"/>	<input type="text" value="des"/>	<input type="text" value="dh1"/>
IKE Policy 5	<input type="text" value="md5"/>	<input type="text" value="3des"/>	<input type="text" value="dh2"/>

Negotiation Main Mode Aggressive Mode

Mode

Local ID Type IP NAME

* Local ID

Peer ID Type IP NAME

* Peer ID

* Lifetime

DPD Enable Disable

* DPD Interval

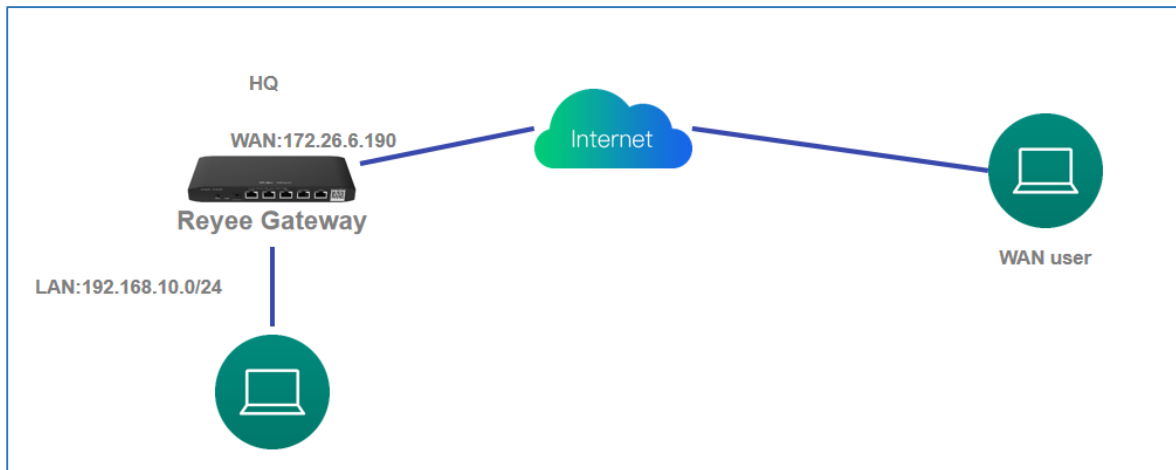
If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

8.5 How Do I Configure PPTP VPN on a Reyee EG Router?

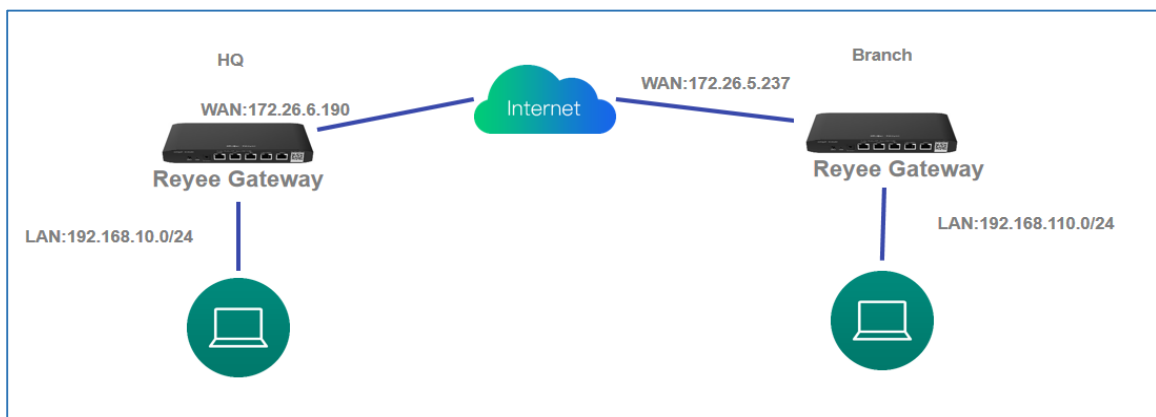
PPTP VPN is typically applied to client-to-site and site-to-site scenarios. For example, clients work from home and need to access company servers through PPTP VPN tunnels. Another example is that a company has three branches that are distributed in three different places of the Internet, and branches need to establish tunnels by using the gateways.

PPTP VPN is applied to the following scenarios.

- Client-to-site scenario



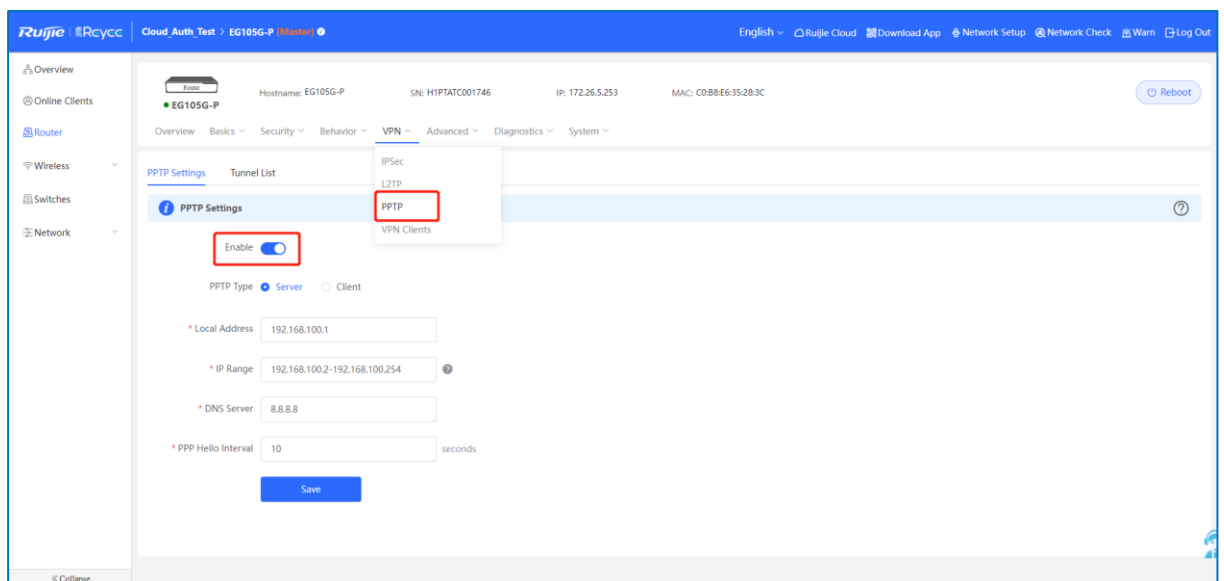
- Site-to-site scenario



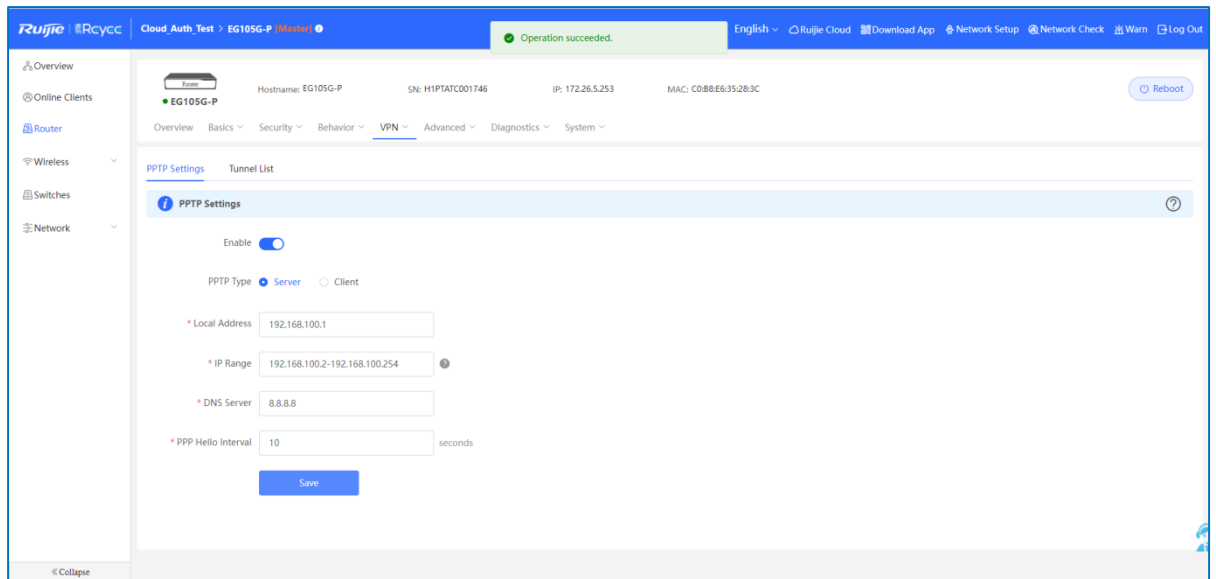
8.5.1 Client-to-Site Scenario Configuration

(1) Headquarters side:

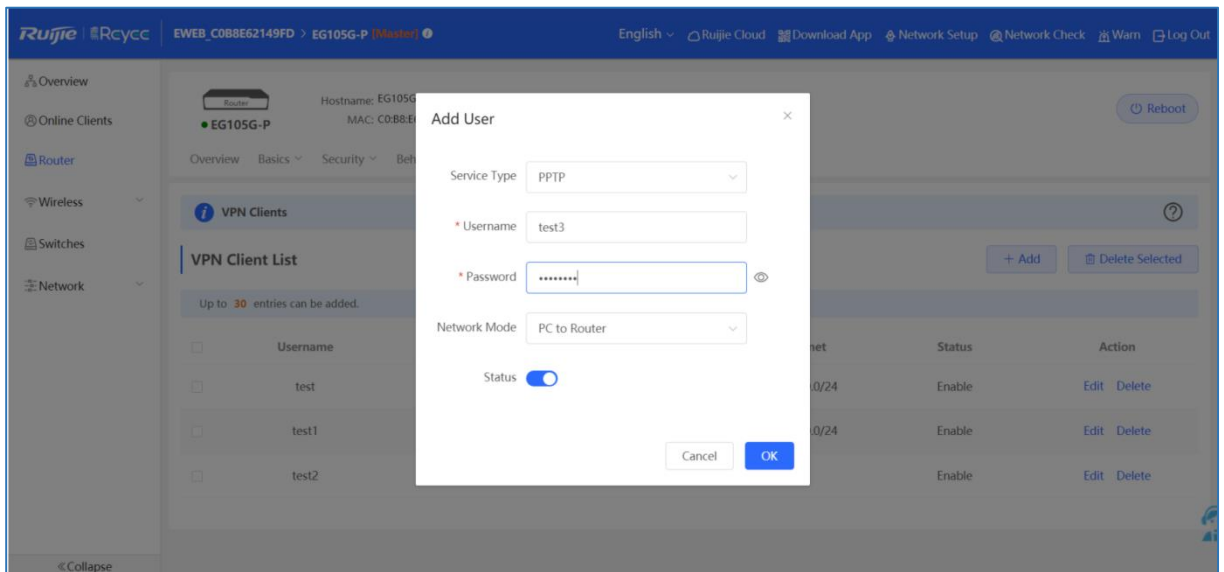
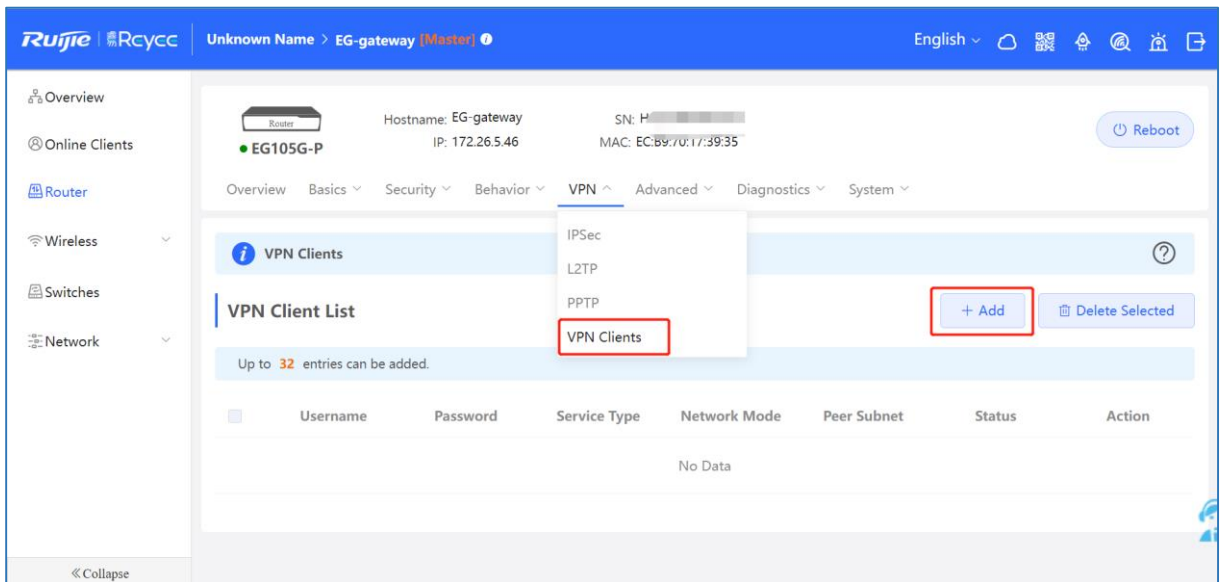
- Log in to a Reyee EG router with the default IP address of 192.168.110.1.
- Choose **VPN > PPTP** and enable PPTP.



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



d Configure VPN clients.

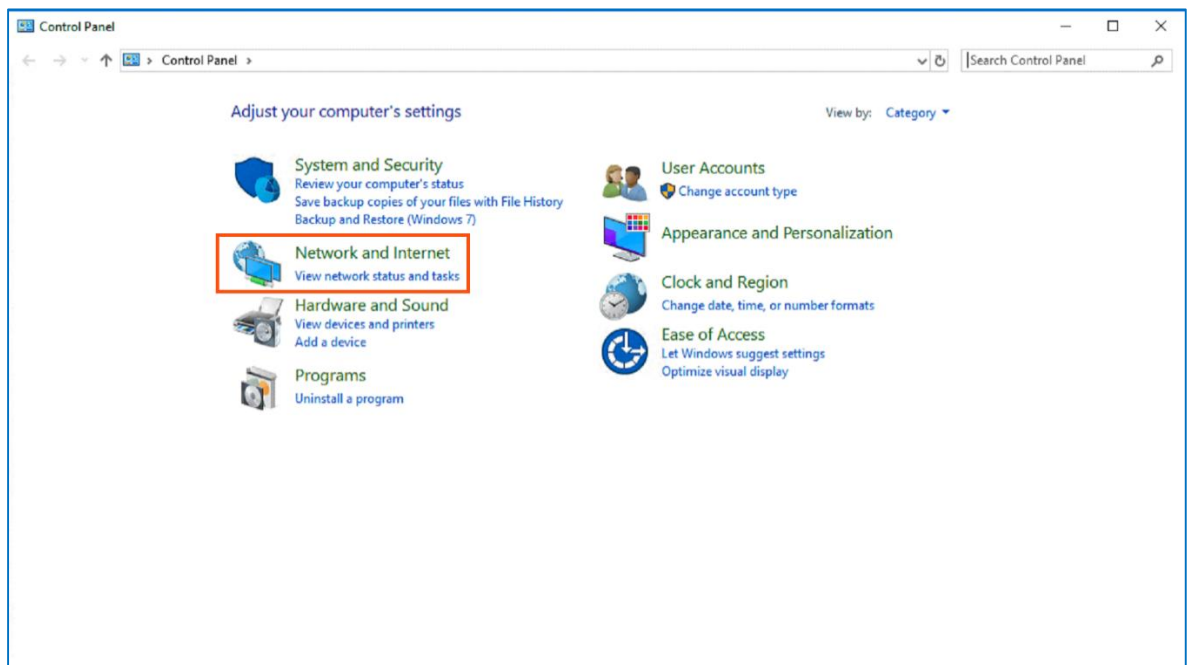
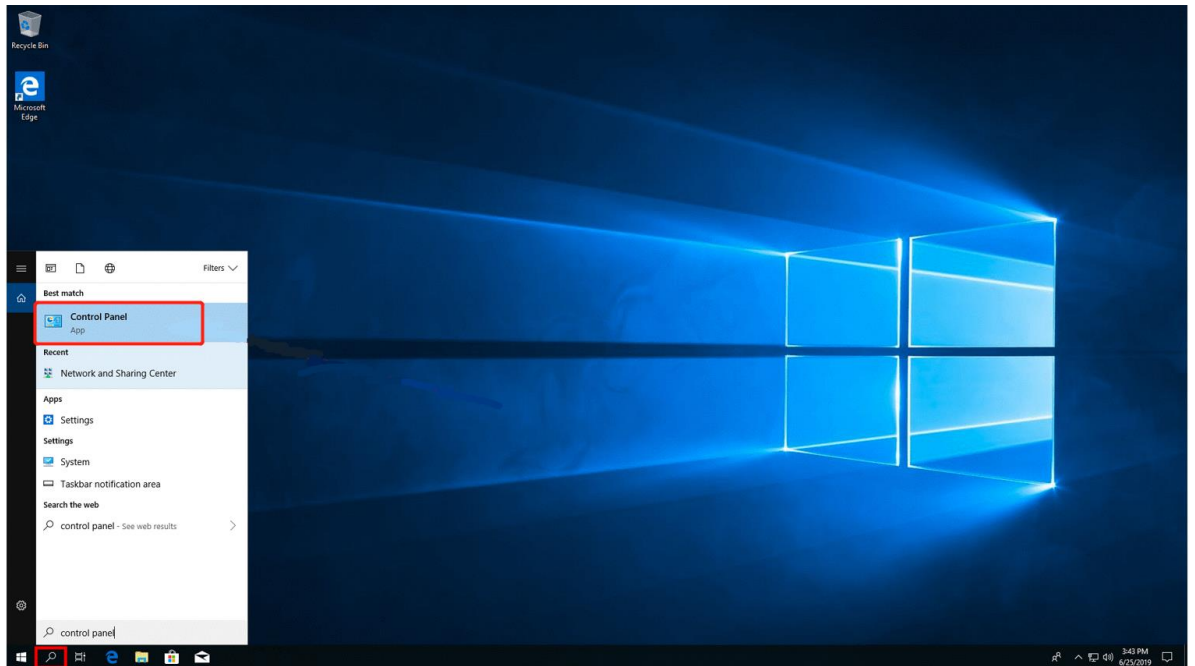


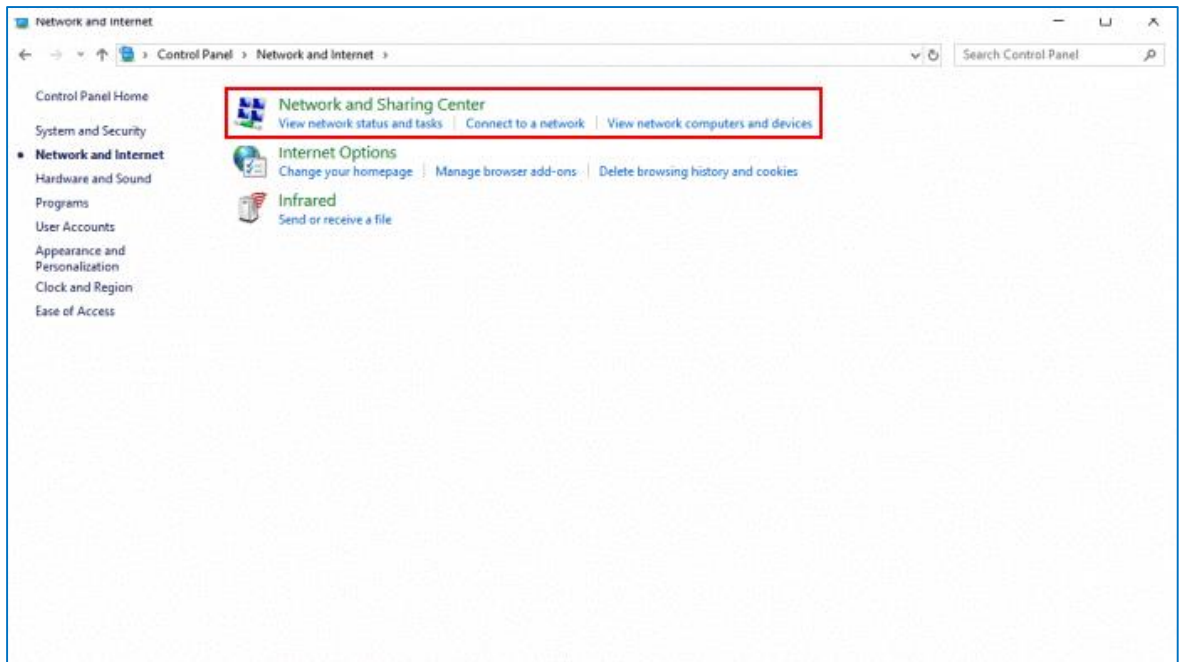
⚠ Caution

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

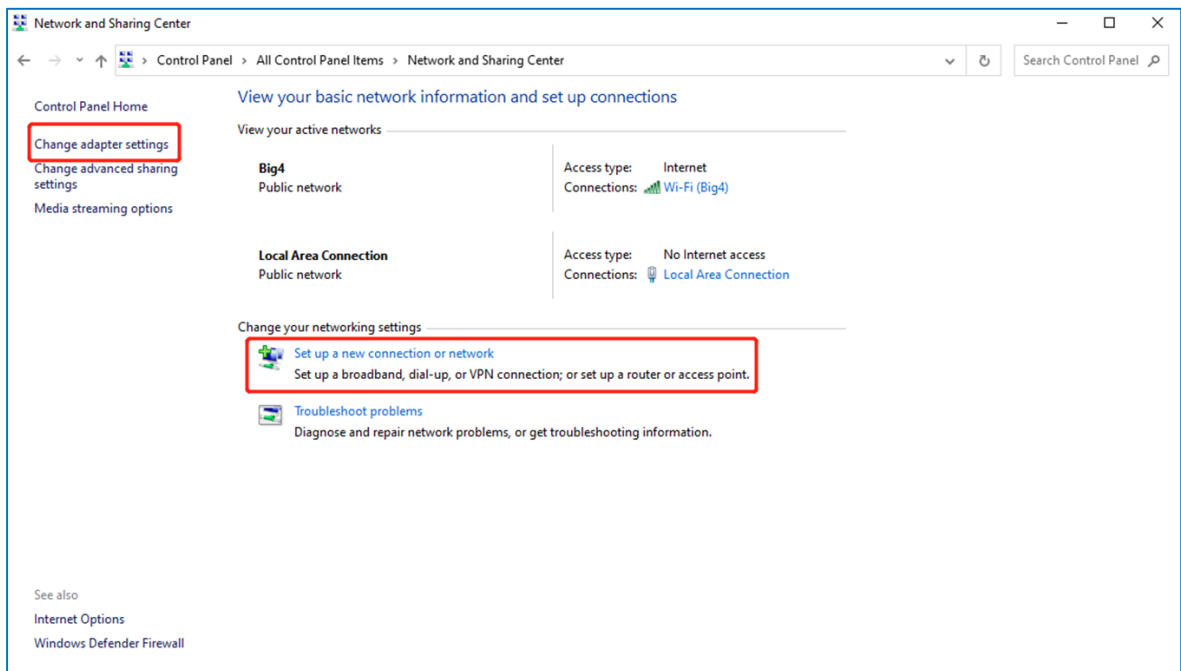
(2) Client side (Windows 10 is used as an example):

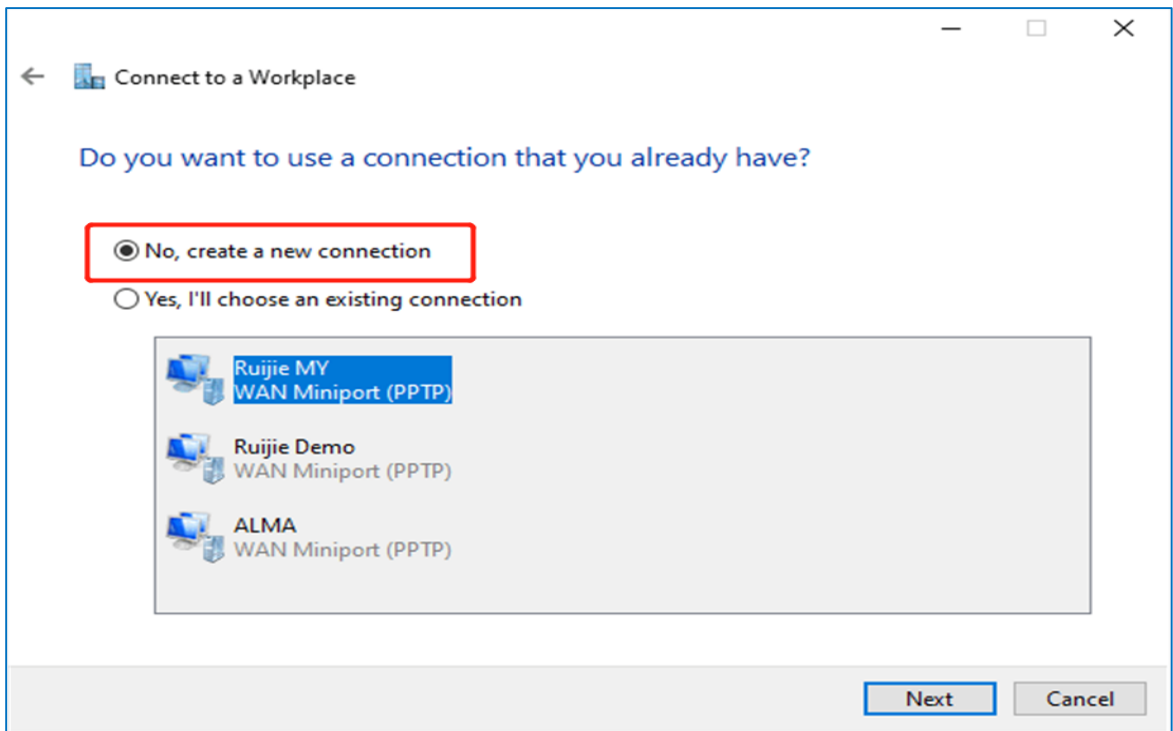
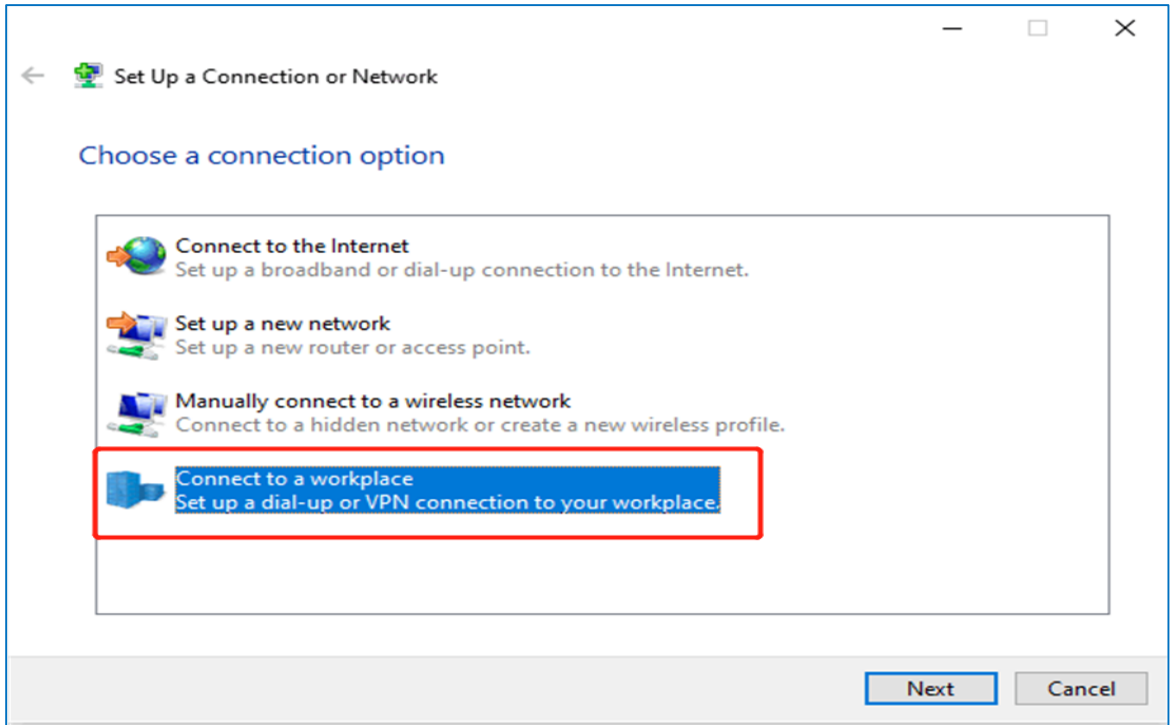
- a Choose **Control Panel > Network and Internet > Network and Sharing Center**.

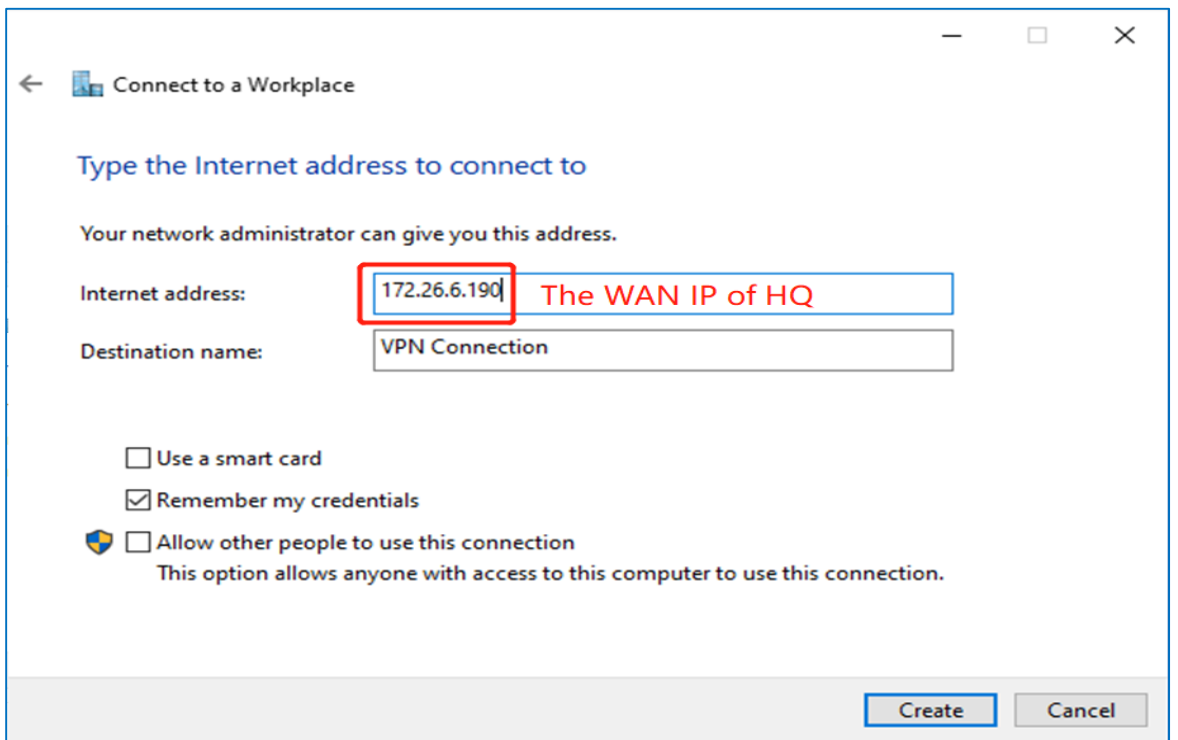
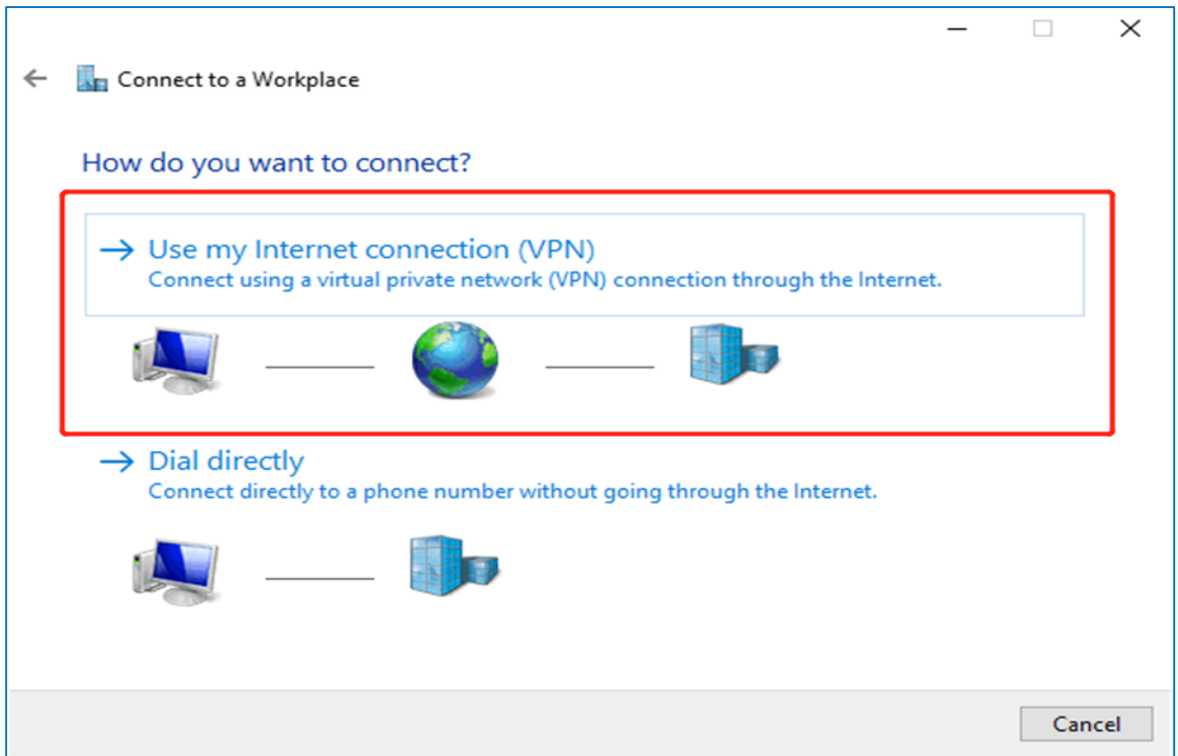




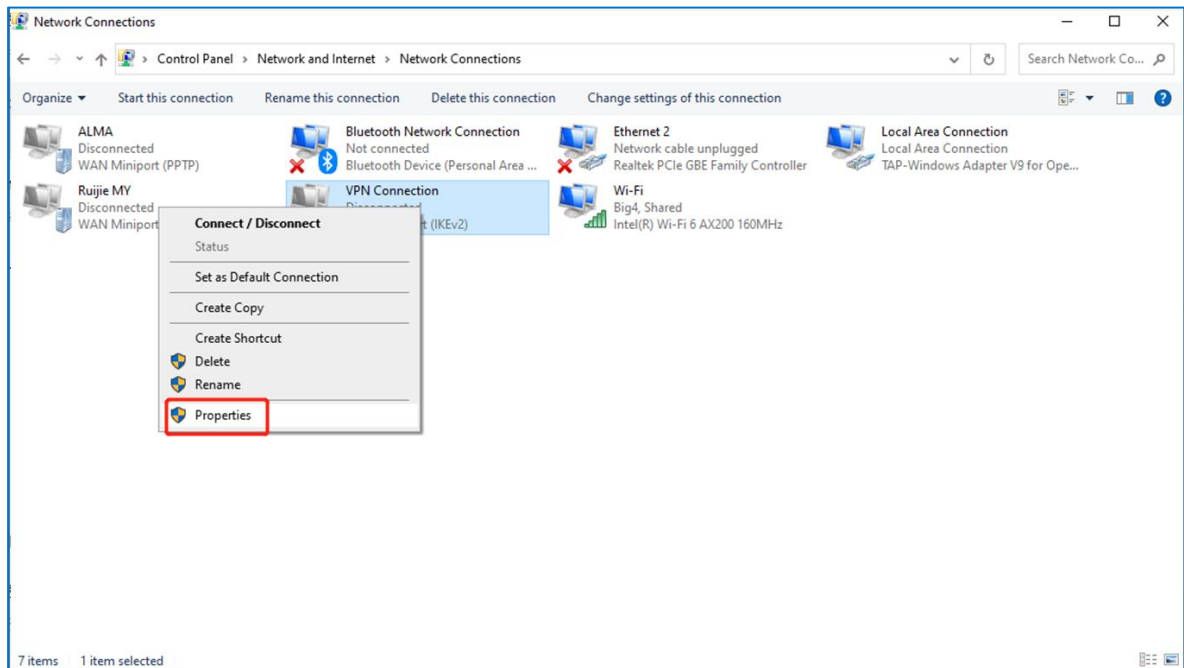
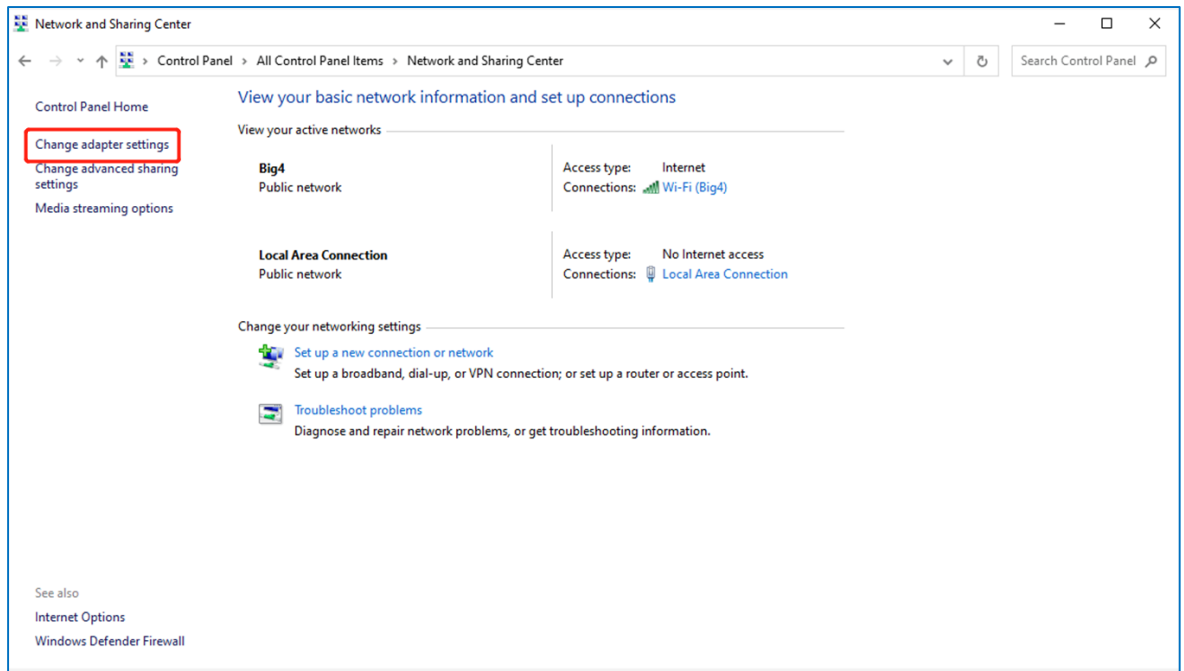
b Configure a VPN connection.

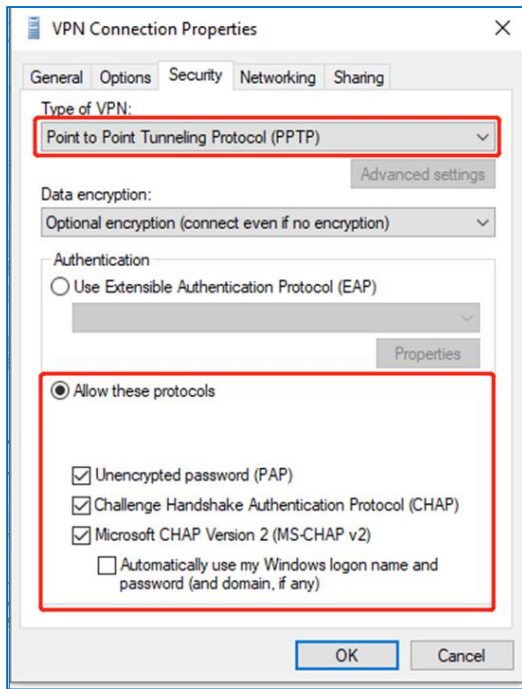




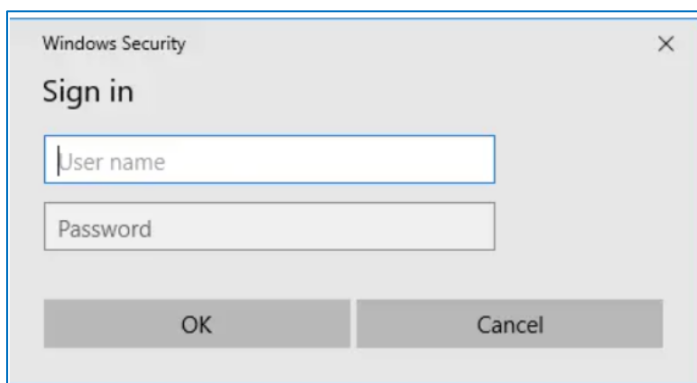
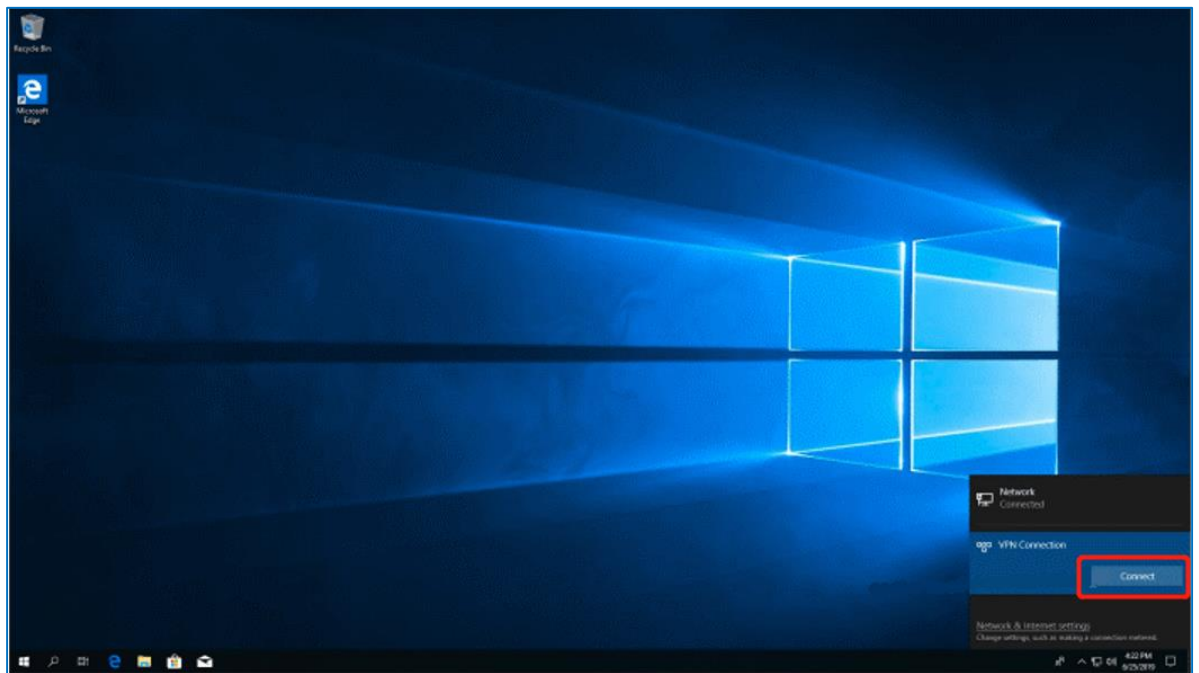


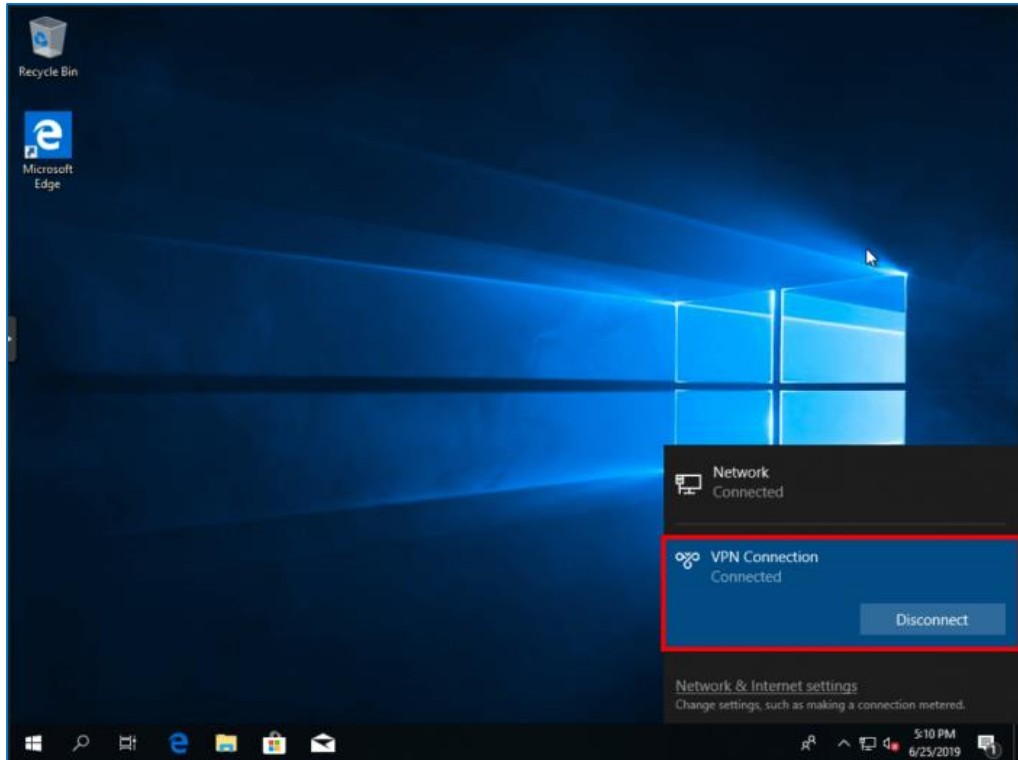
- c. Change the adapter configuration.





d Check the VPN connection status.

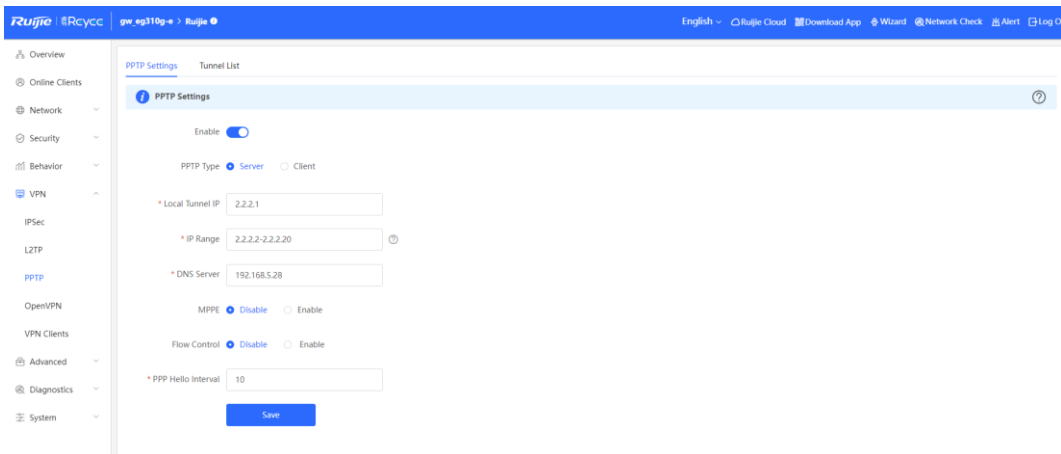




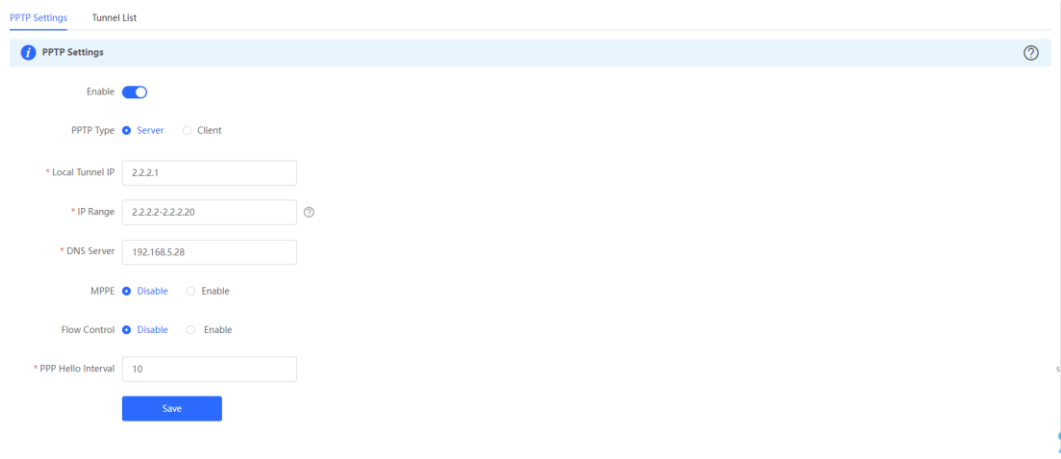
8.5.2 Site-to-Site Scenario Configuration

(1) Headquarters side:

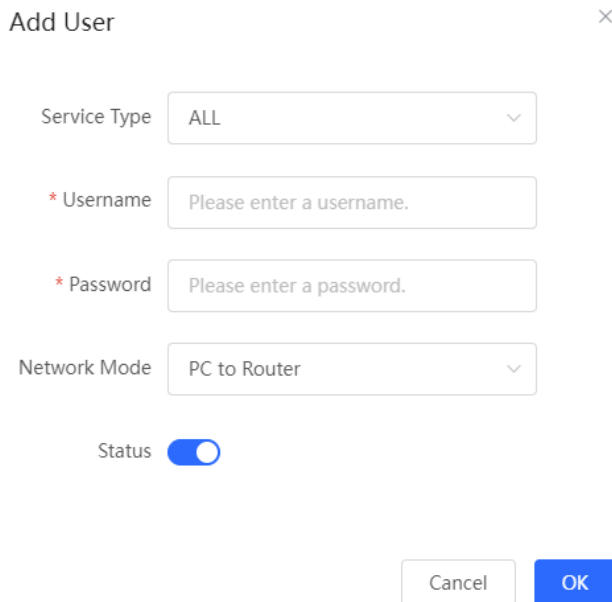
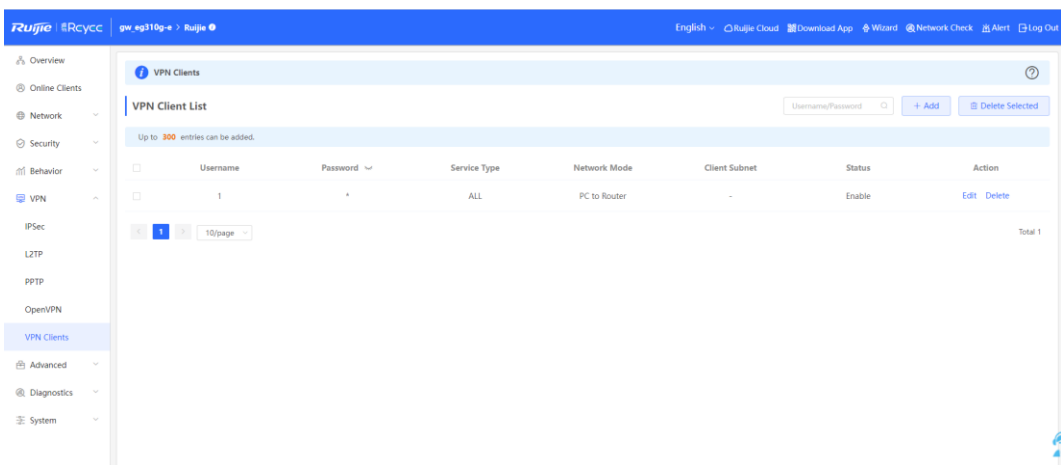
- a Log in to a Reyee EG router with the default IP address of 192.168.110.1.
- b Choose **VPN > PPTP**, enable **PPTP**, and set **PPTP Type** to **Server**.



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



d Configure the VPN client.

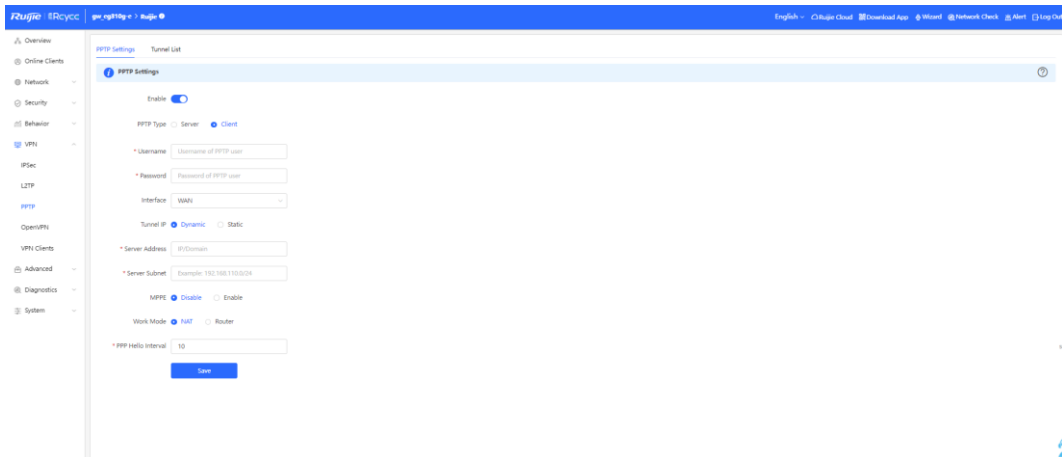


Caution

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

(2) Branch side:

- a Log in to a Reyee EG router with the default IP address of 192.168.110.1.
- b Click **VPN > PPTP**, enable **PPTP**, and set **PPTP Type** to **Client**.



Caution

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

(3) Check the VPN connection status.

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

8.6 Can a Reyee EG Router Establish a PPTP VPN with Third-Party Devices or Ruijie EG Routers?

A Reyee EG router can establish a PPTP VPN with PPTP-capable third-party devices. In this case, the Ruijie EG router cannot function as the PPTP client.

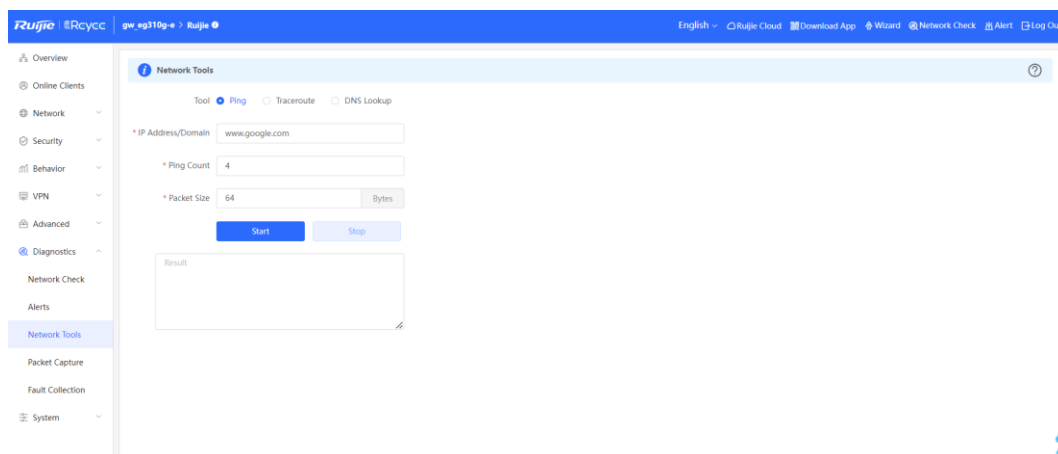
8.7 Can PPTP VPN Be Connected on an iPhone or Mac?

PPTP VPN cannot be connected on an iPhone, Mac, or iPad.

8.8 What Can I Do If a Reyee EG Router Fails to Connect the PPTP VPN?

- (1) Check whether the EG router of the branch can ping the EG router of the headquarters. If the ping fails, check the network connection between two EG routers.

Choose **Diagnostics > Network Tools** and start the ping operation.



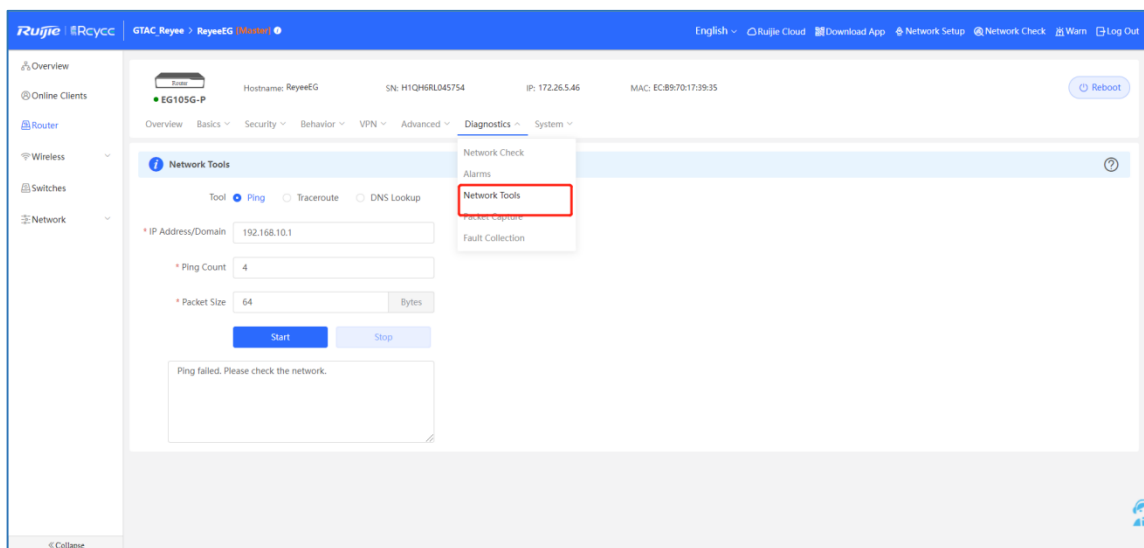
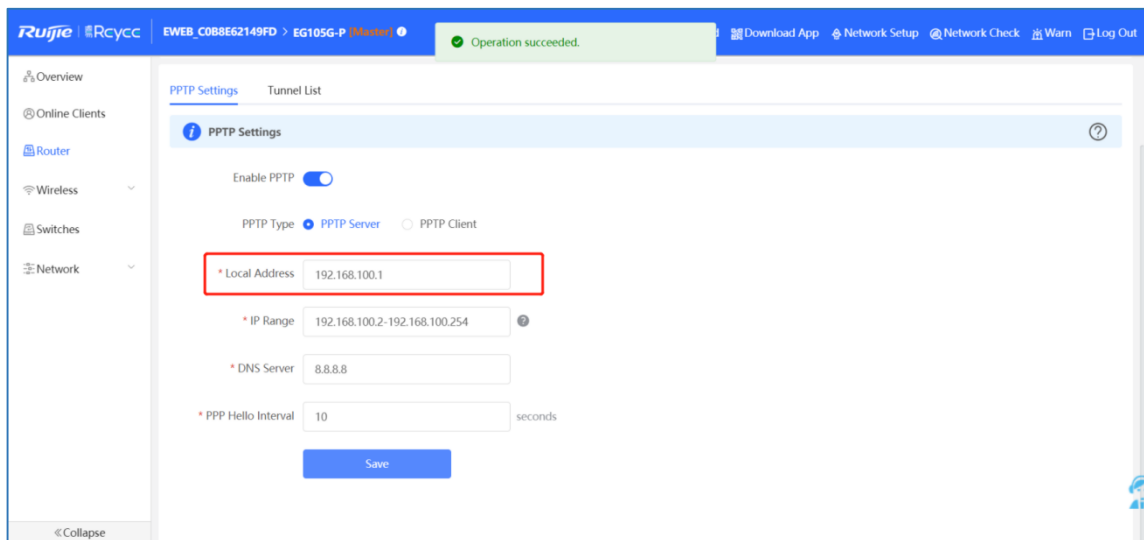
- (2) Check whether the username and password of VPN client settings of the headquarters are correct.
- (3) Check whether the settings are correct according to [8.5 How Do I Configure PPTP VPN on a Reyee EG Router?](#)
- (4) Check whether the WAN IP address of the EG router of the headquarters is a public IP address. If not, configure DMZ on your external device.
- (5) If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

8.9 What Can I Do If I Fail to Connect PPTP VPN on a PC or an iPhone?

- (1) iPhone and other iOS devices do not support PPTP. You can use L2TP instead.
- (2) Check whether PC settings are correct according to [8.5.1 Client-to-Site Scenario Configuration](#).
- (3) Check whether the PC can ping the EG router of the headquarters. If the ping operation fails, check the network connection on your PC.
- (4) Check whether the WAN IP address of the EG router of the headquarters is the public IP address. If not, configure DMZ on your external device.
- (5) If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

8.10 What Can I Do If I Have Connected VPN, but Cannot Access Internal Devices of the Headquarters?

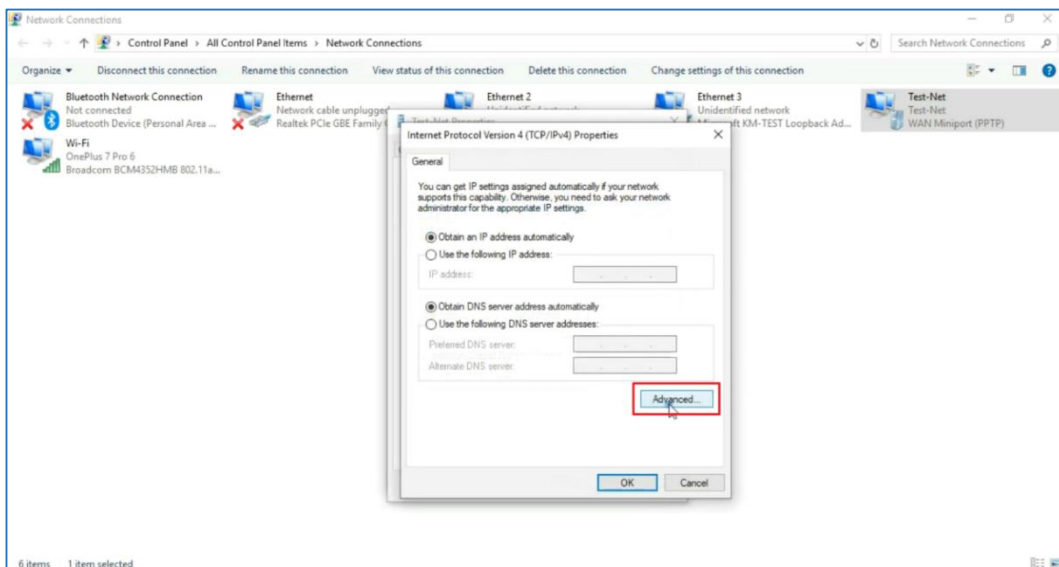
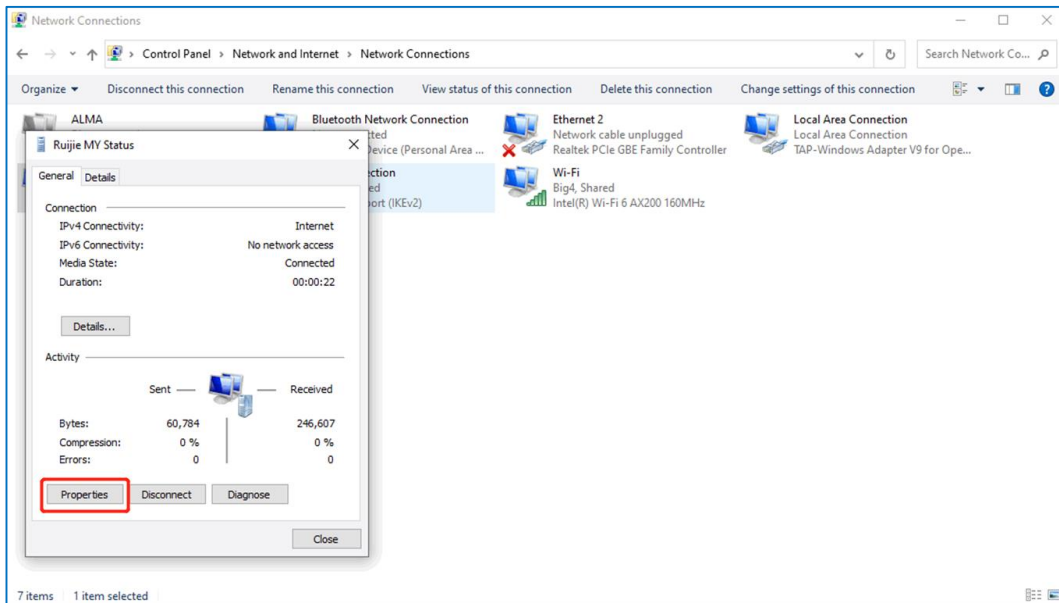
- (1) Perform tracer on the internal device's IP address of the headquarters on your PC to check the hop where packets are lost.
- (2) If the local IP address on the EG router is reachable but the IP address of the internal device is unreachable, ping the IP address of the internal device of the headquarters on the EG router.

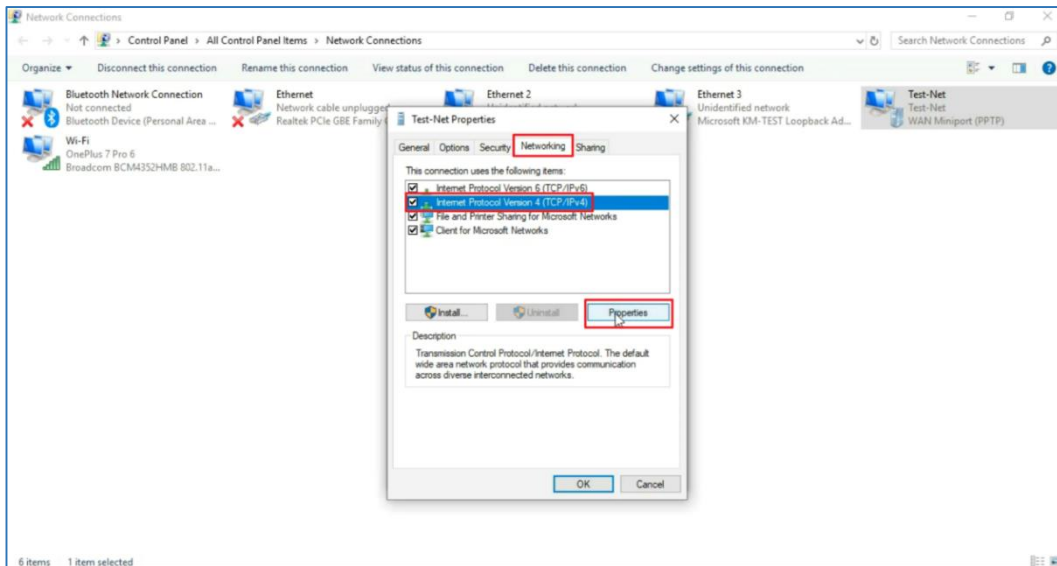


- (3) If the EG router is unreachable, check whether the firewall on the server that wants to access the EG is enabled.
- (4) If you have disabled the firewall on your server but the EG router is still unreachable, check internal network settings of the headquarters, such as VLAN and route settings.
- (5) If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

8.11 Why I Fail to Access the Internet After Connecting the VPN?

- (1) Deselect **use default gateway on remote network** on the PC. Double-click the VPN adapter to access **Properties**.





Click **OK** three times in sequence to save the configuration.

(2) Then disconnect VPN and reconnect it once again.

8.12 Can a Reyee EG Router Be Enabled with PPTP and IPsec Simultaneously?

A Reyee EG router cannot be enabled PPTP and IPsec simultaneously.

8.13 Can a Reyee EG Router Be Enabled with PPTP and L2TP Simultaneously?

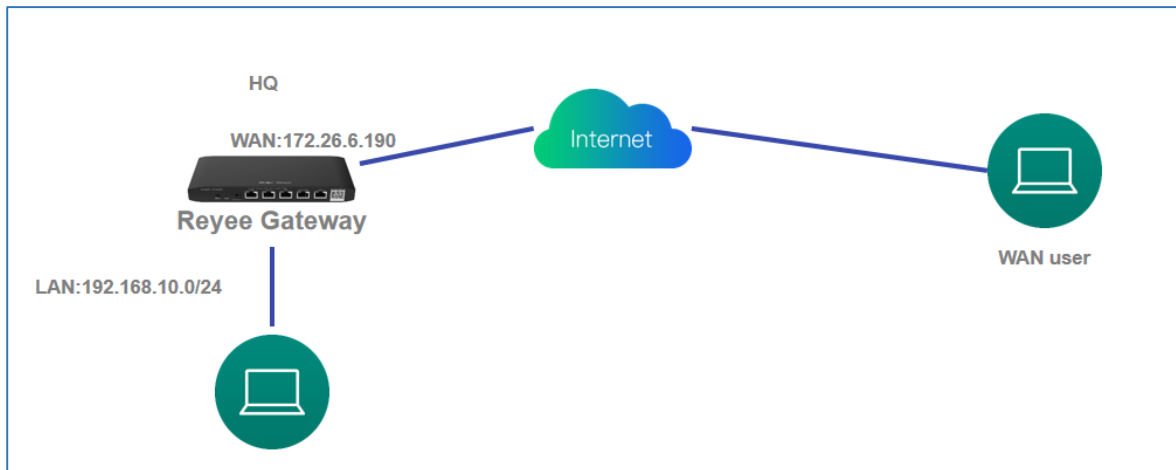
A Reyee EG router cannot be enabled PPTP and L2TP simultaneously on a branch, but it can be enabled PPTP and L2TP simultaneously on the headquarters.

8.14 How Do I Configure L2TP VPN on a Reyee EG Router?

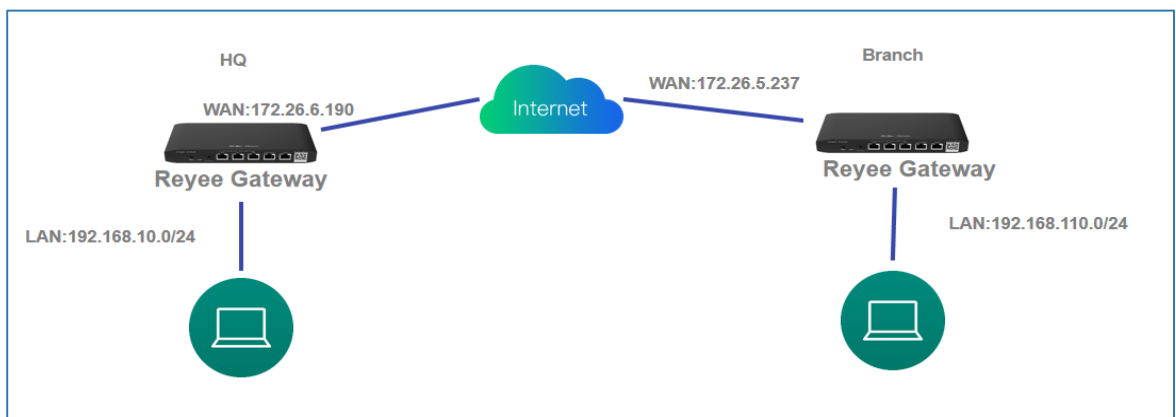
L2TP VPN is typically applied to client-to-site and site-to-site scenarios. For example, clients work from home and need to access company servers through L2TP VPN tunnels. Another example is that a company has three branches that are distributed in three different places of the Internet, and branches need to establish tunnels by using the gateways.

L2TP VPN applies to the following scenarios.

- Client-to-site scenario



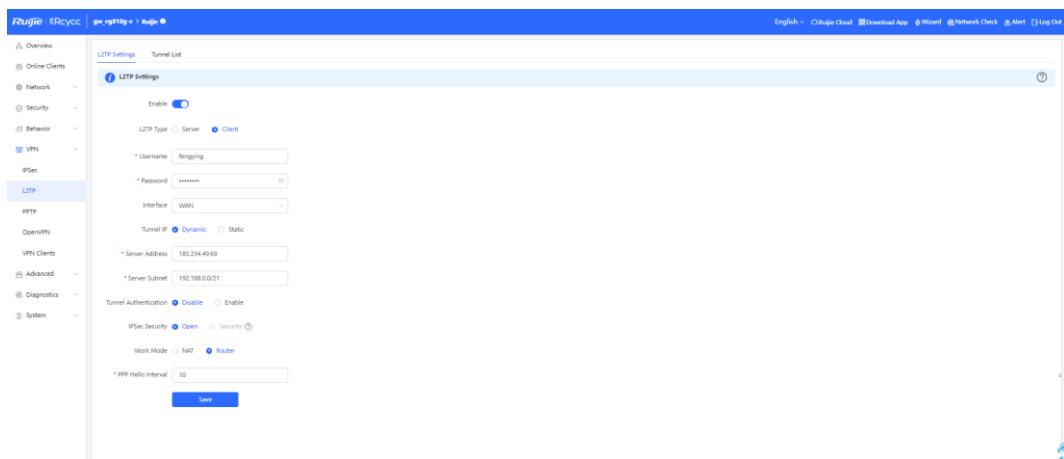
- Site-to-site scenario



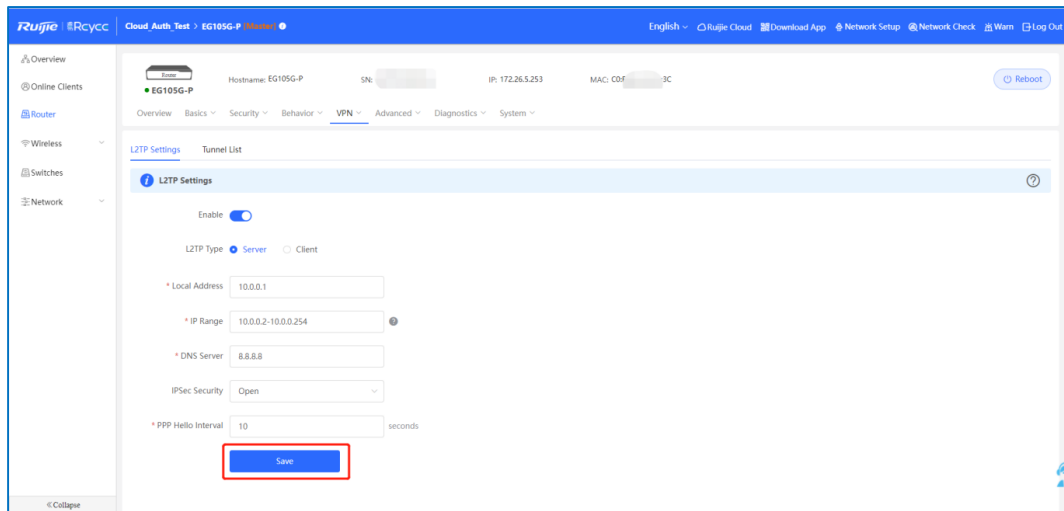
8.14.1 Client-to-Site Scenario Configuration

(1) Headquarters side:

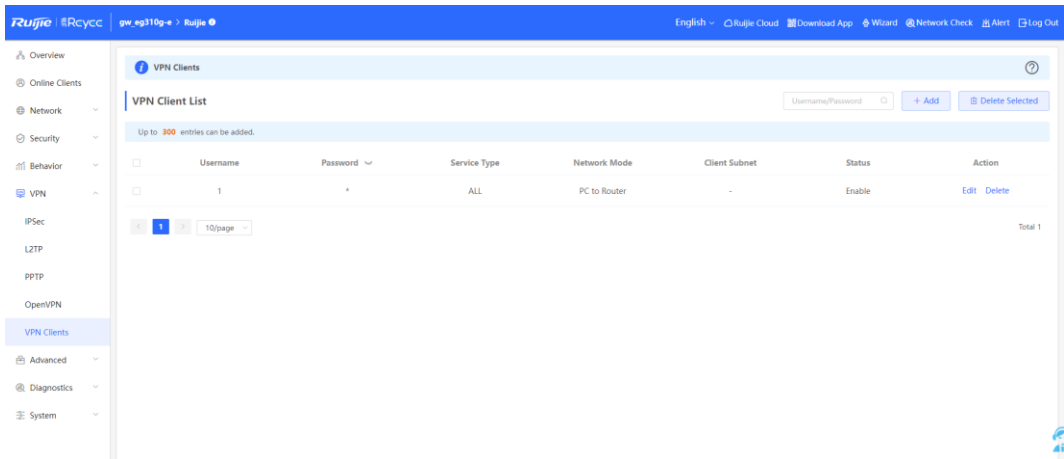
- Log in to a Reyee EG router with the default IP address of 192.168.110.1.
- Choose **VPN > L2TP** and enable L2TP.



- Perform L2TP configuration and click **Save**.



d Choose **VPN > VPN Clients** to configure VPN clients.



Add User ×

Service Type

* Username

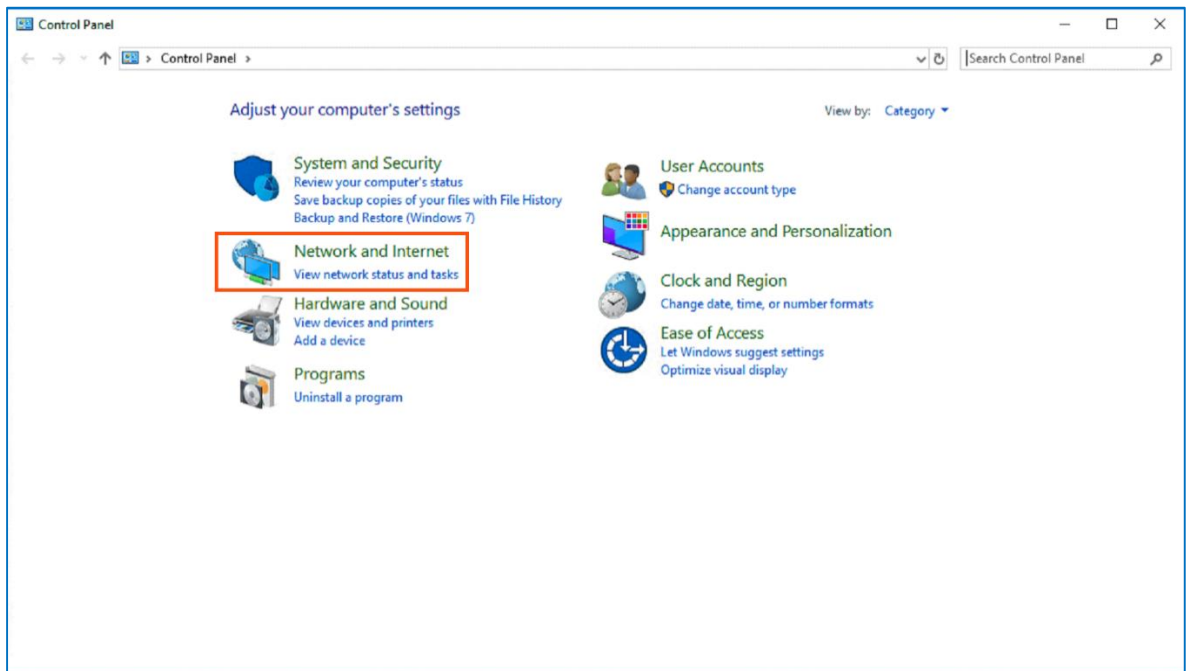
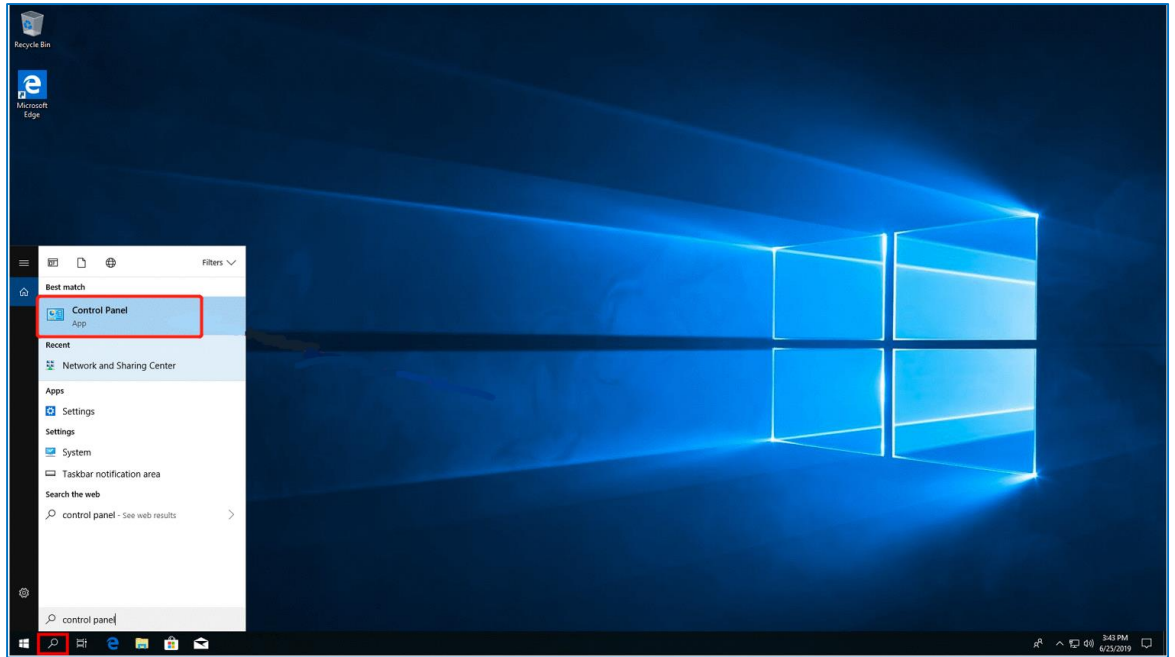
* Password

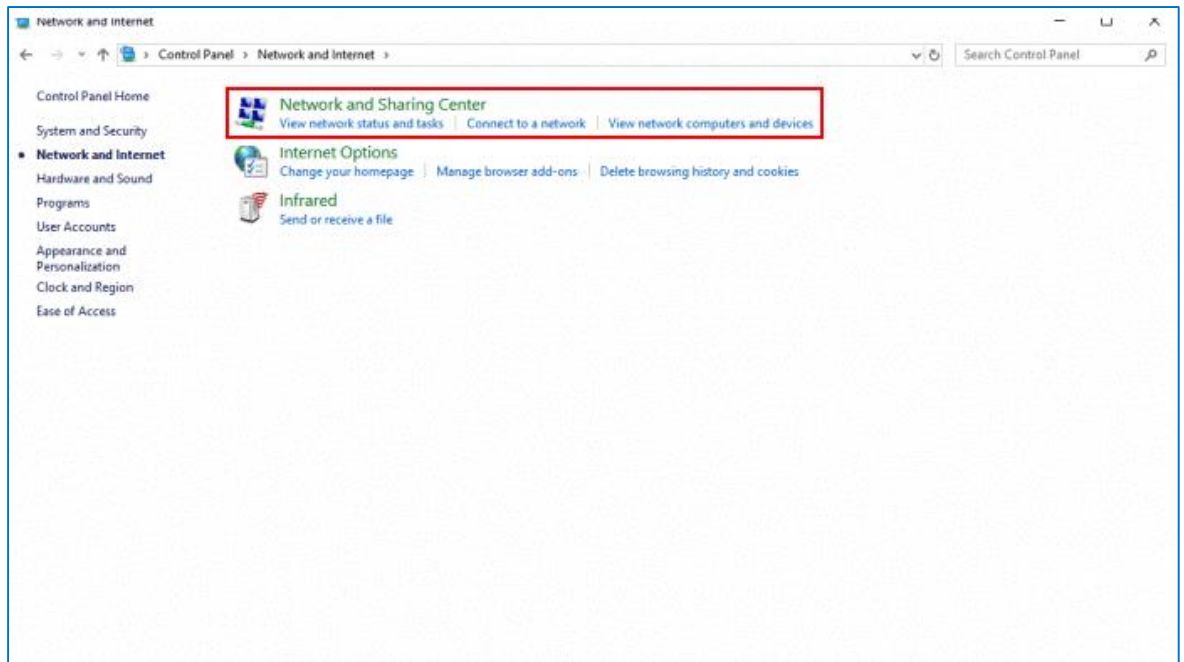
Network Mode

Status

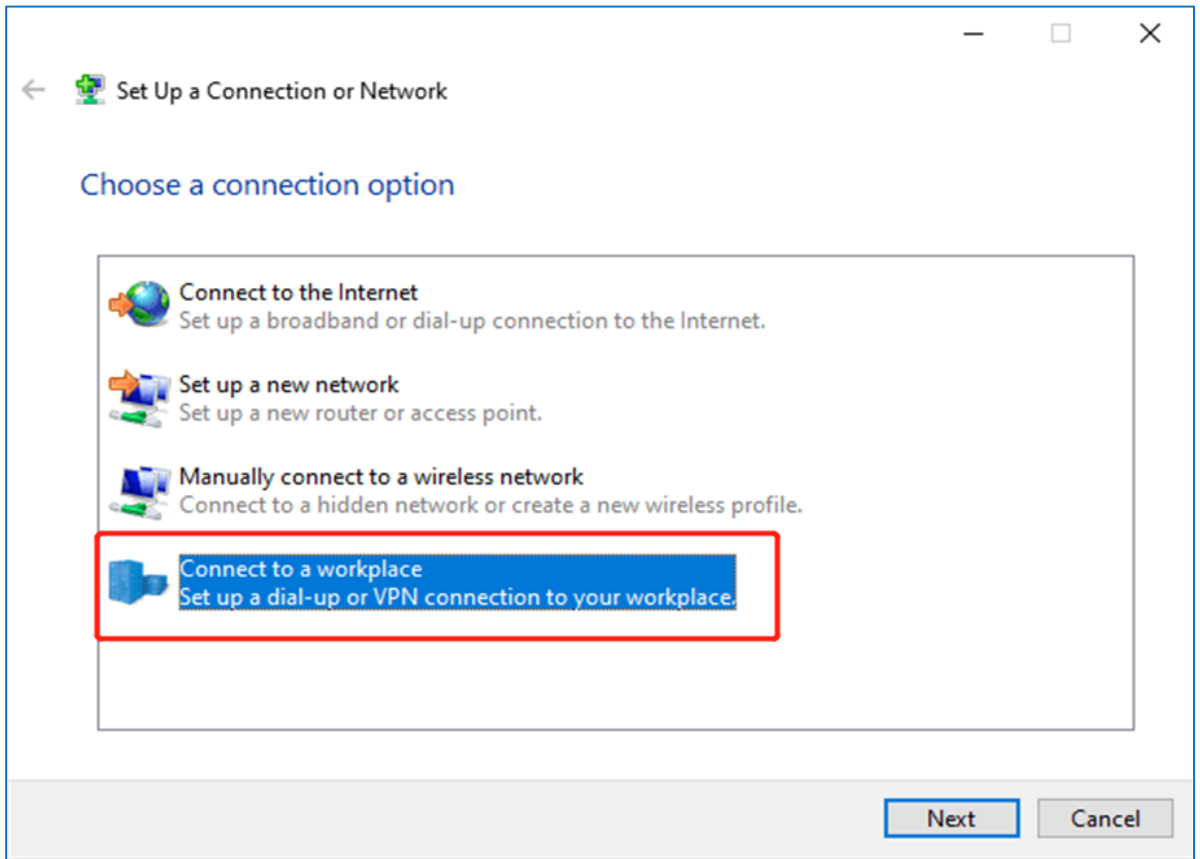
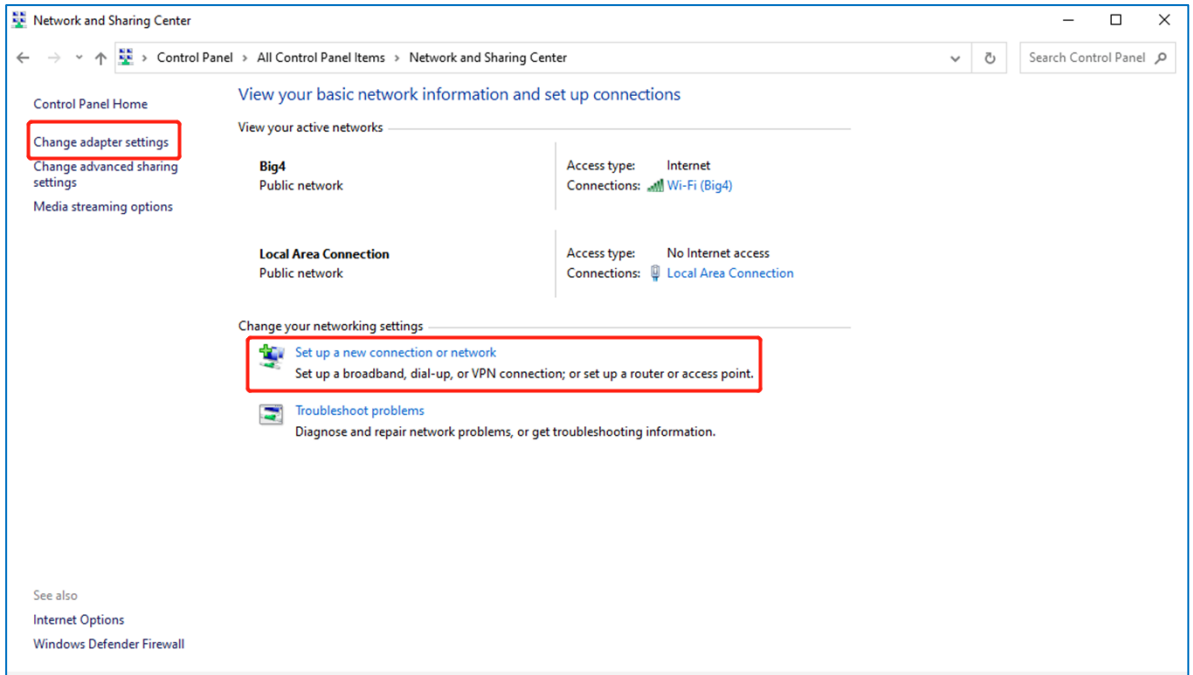
(2) Client side (Windows 10 is used as an example):

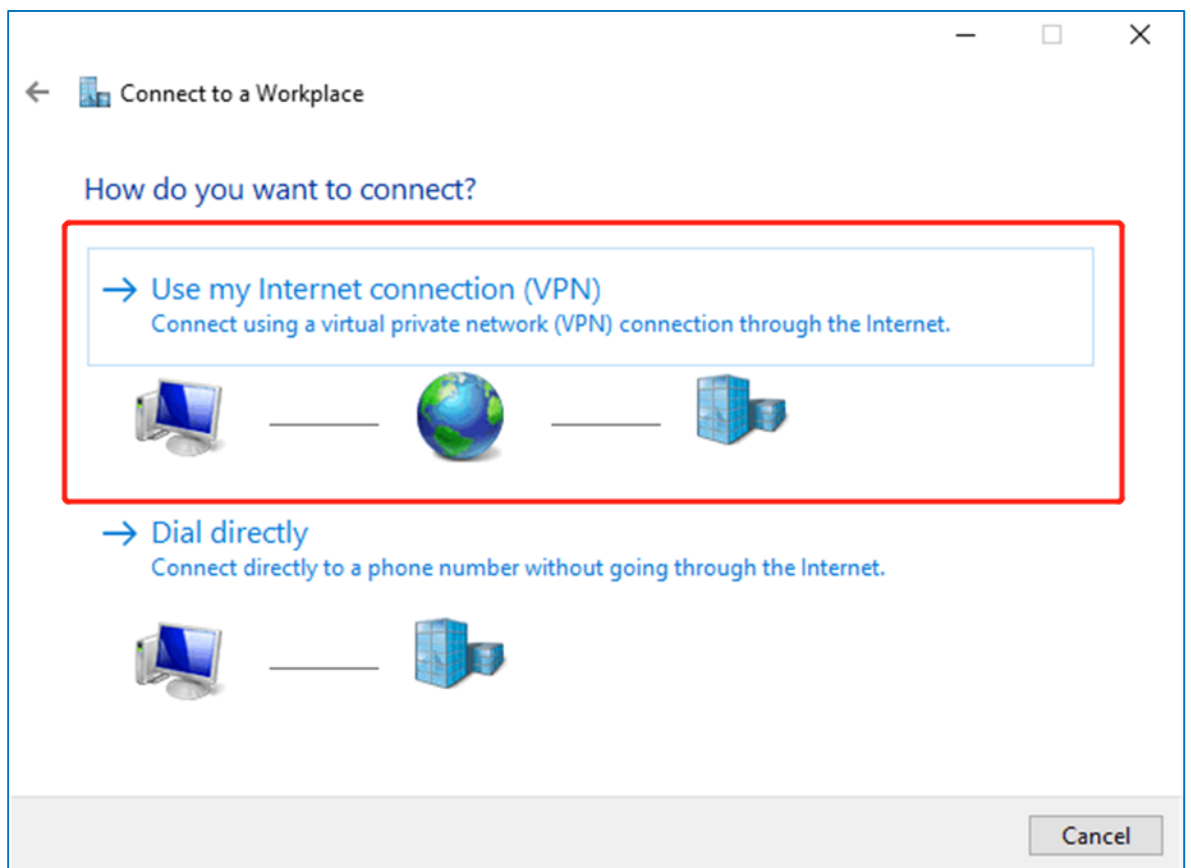
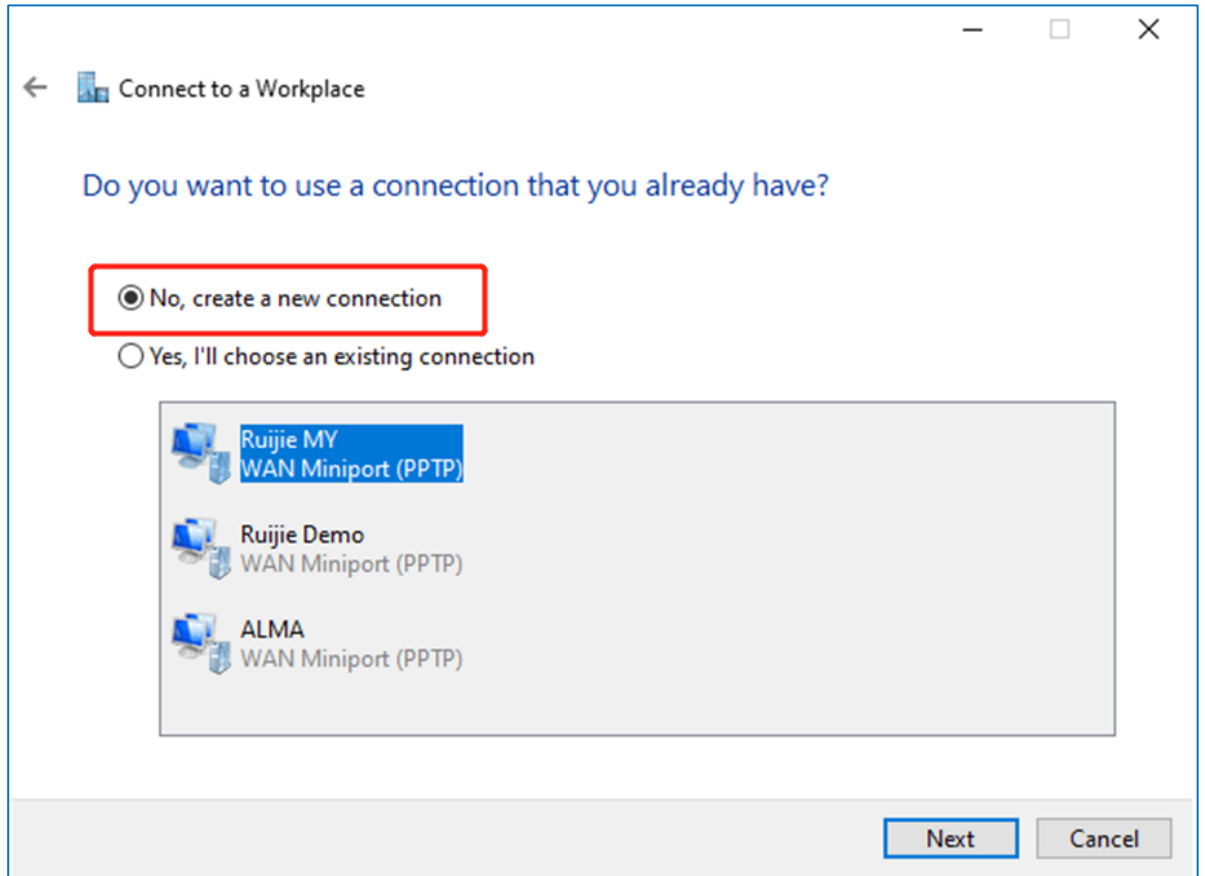
a Choose **Control Panel > Network and Internet > Network and Sharing Center**.

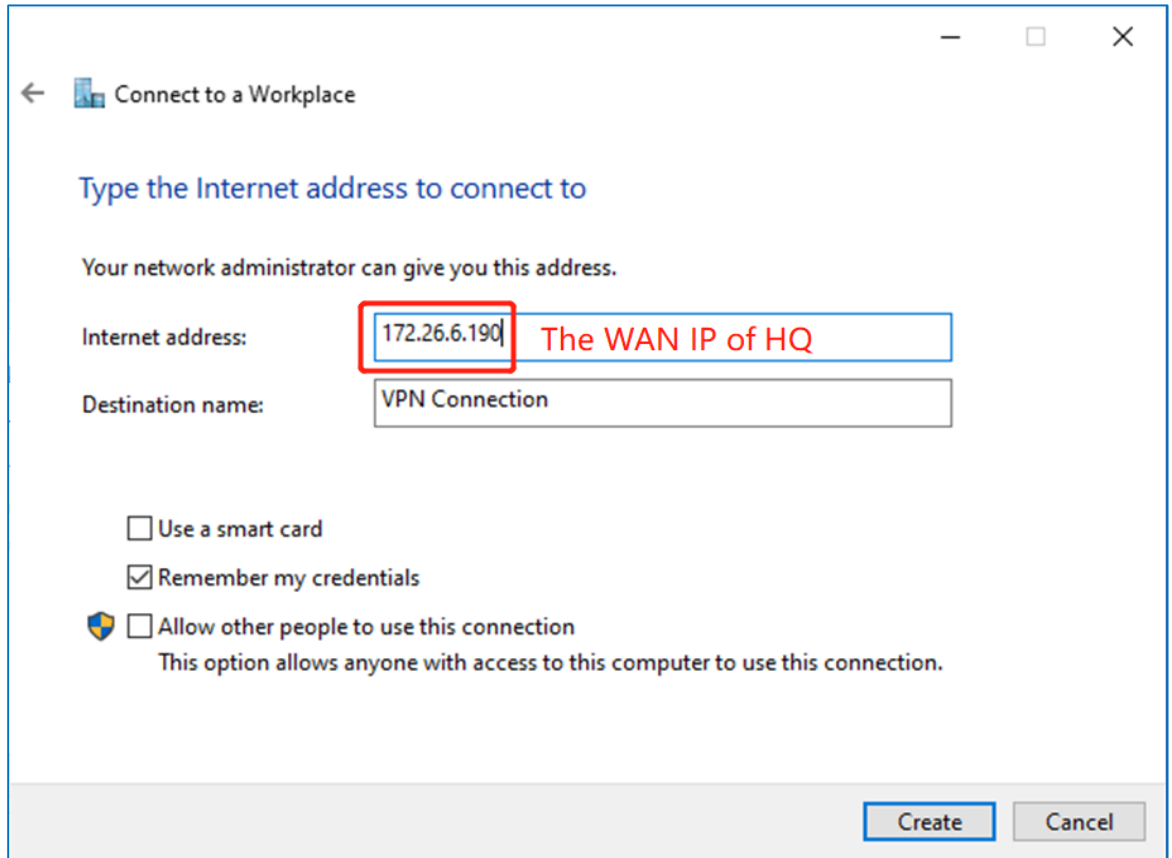




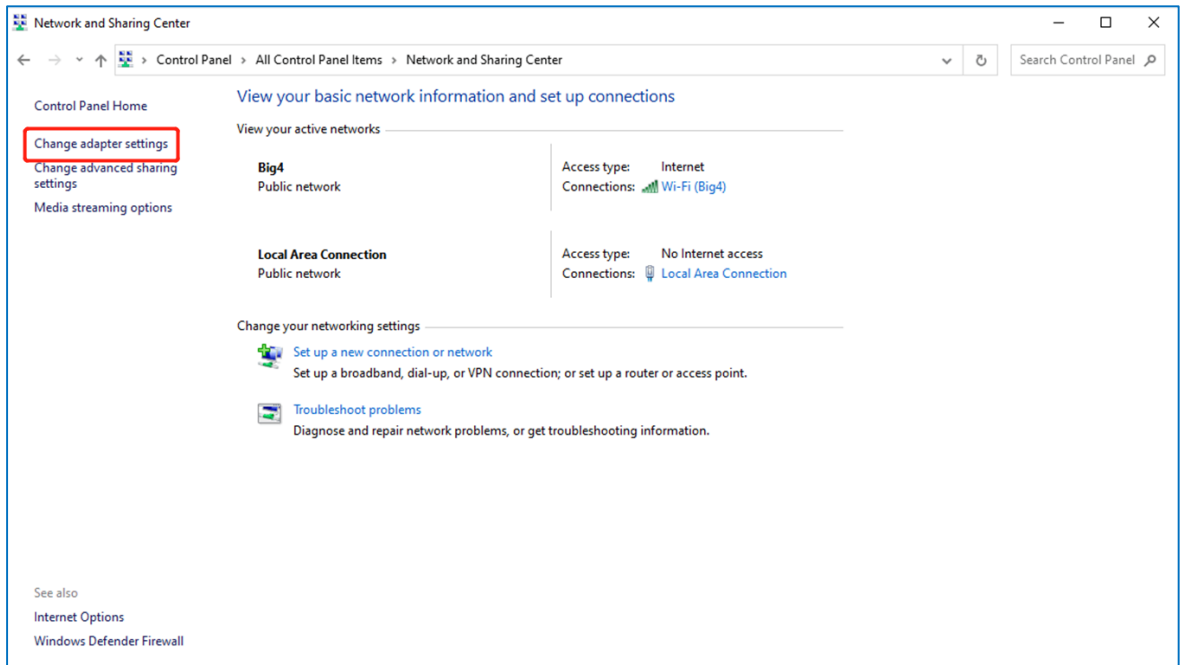
- b. Configure a VPN connection.

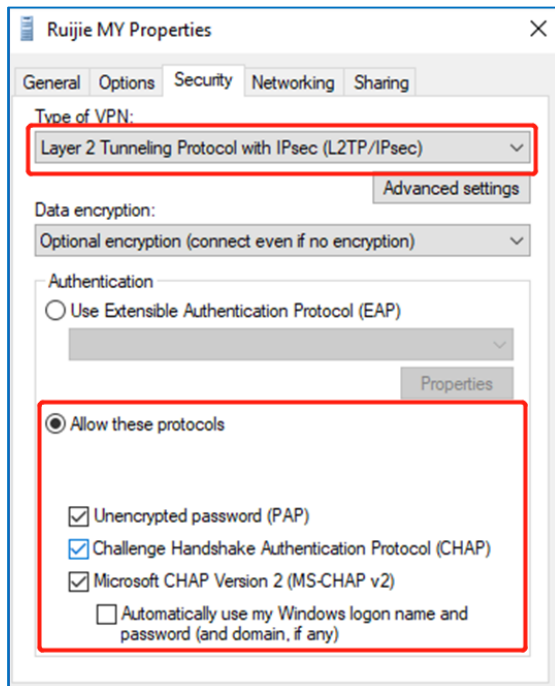
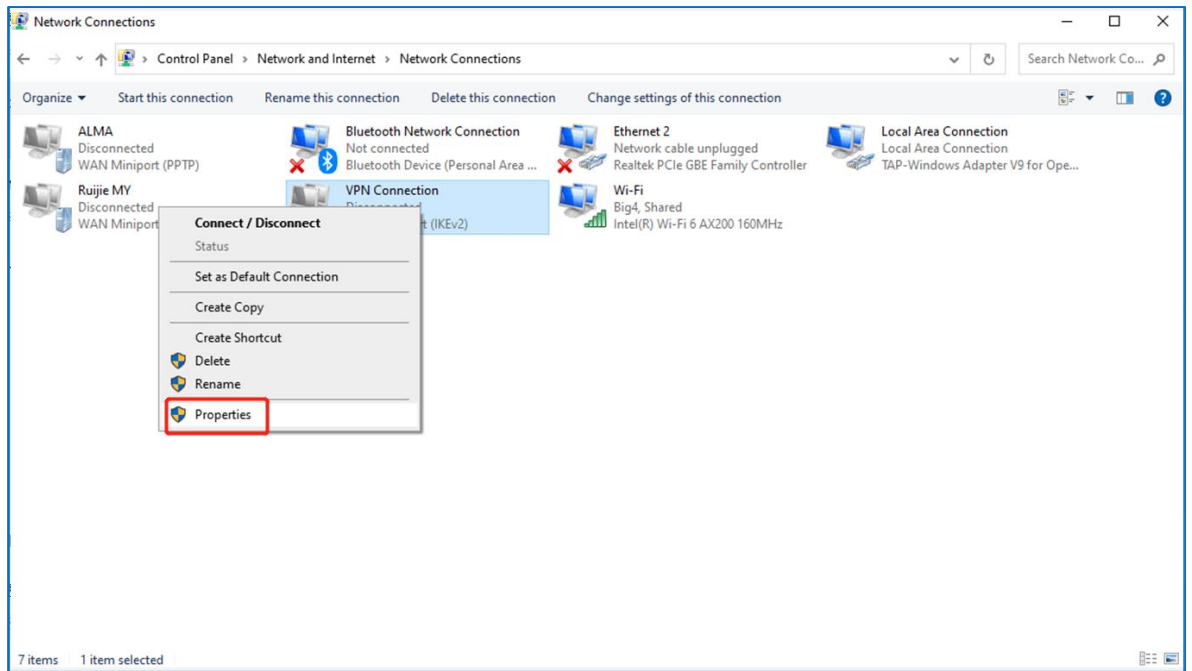




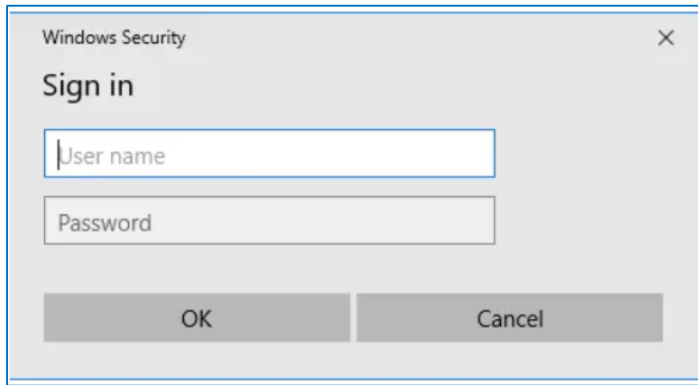
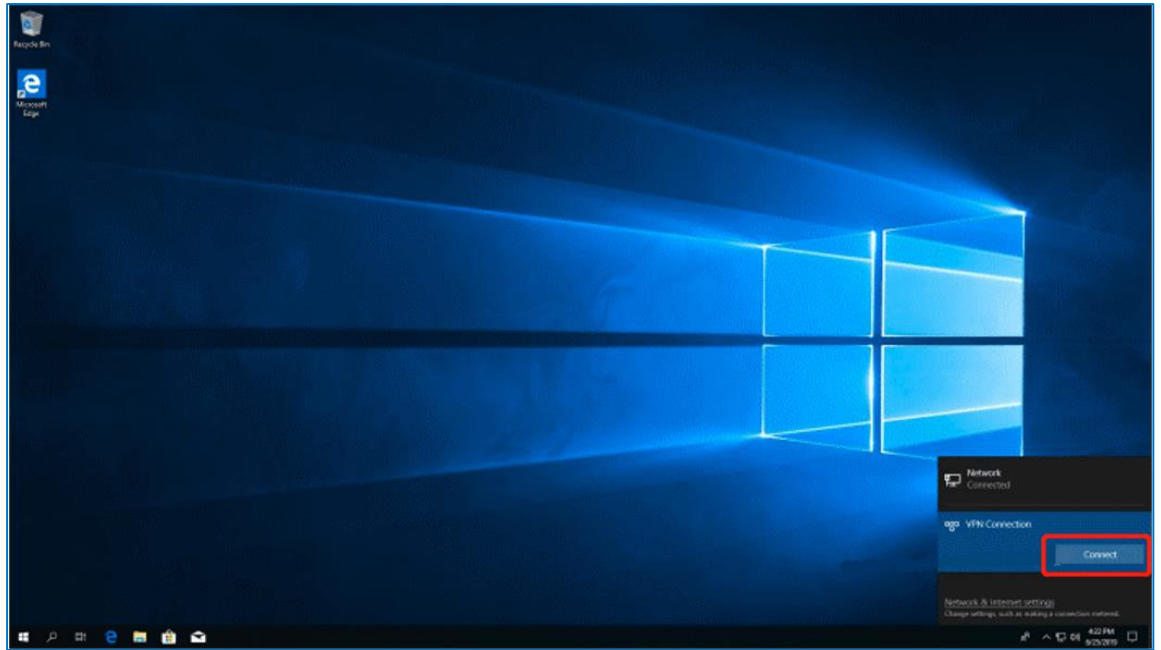


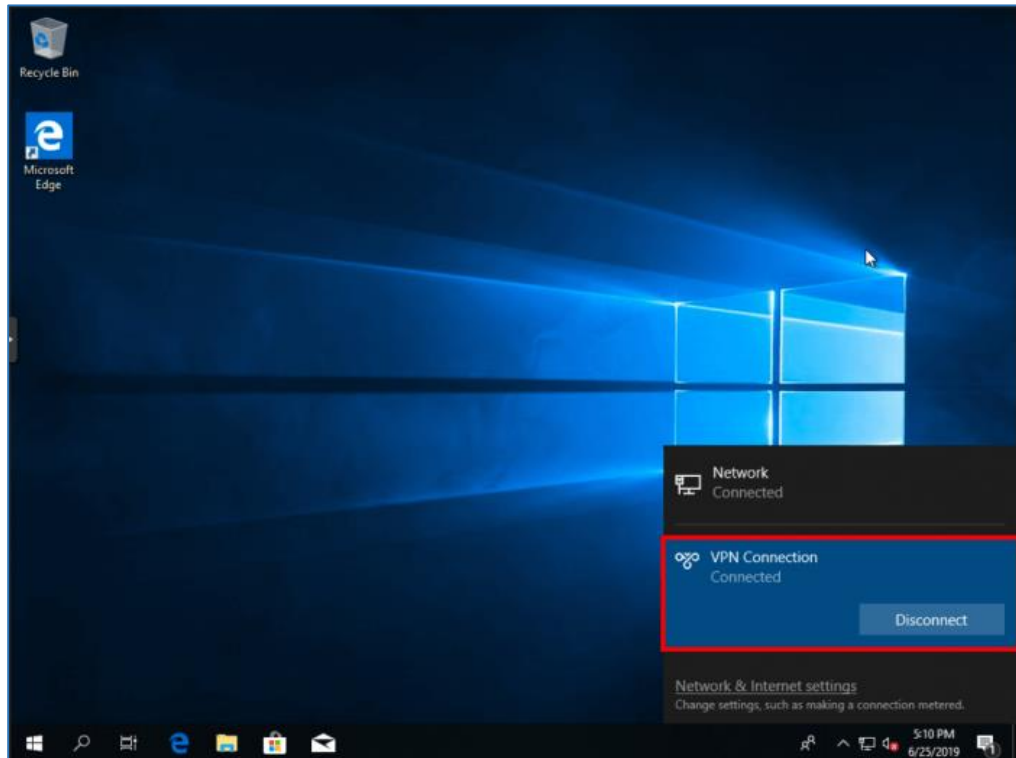
c Change adapter's setting.





d Check the VPN connection status.

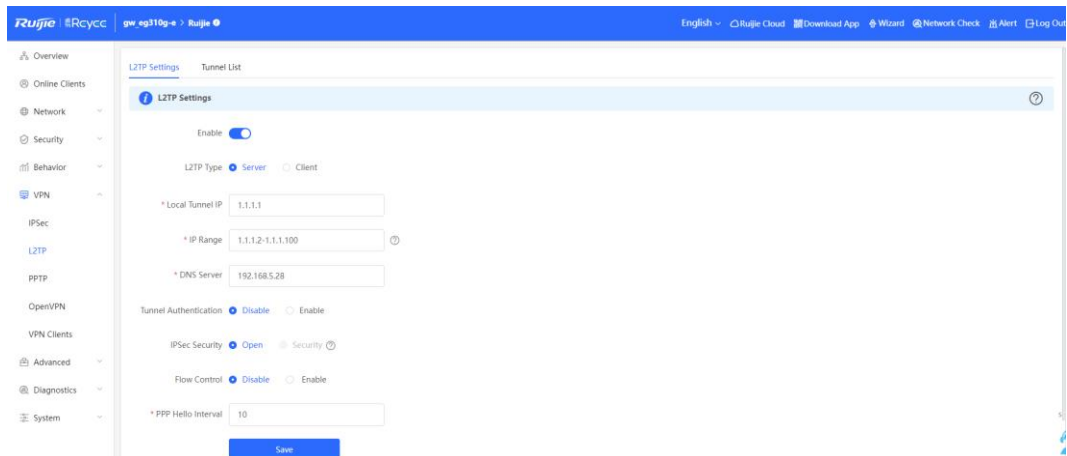




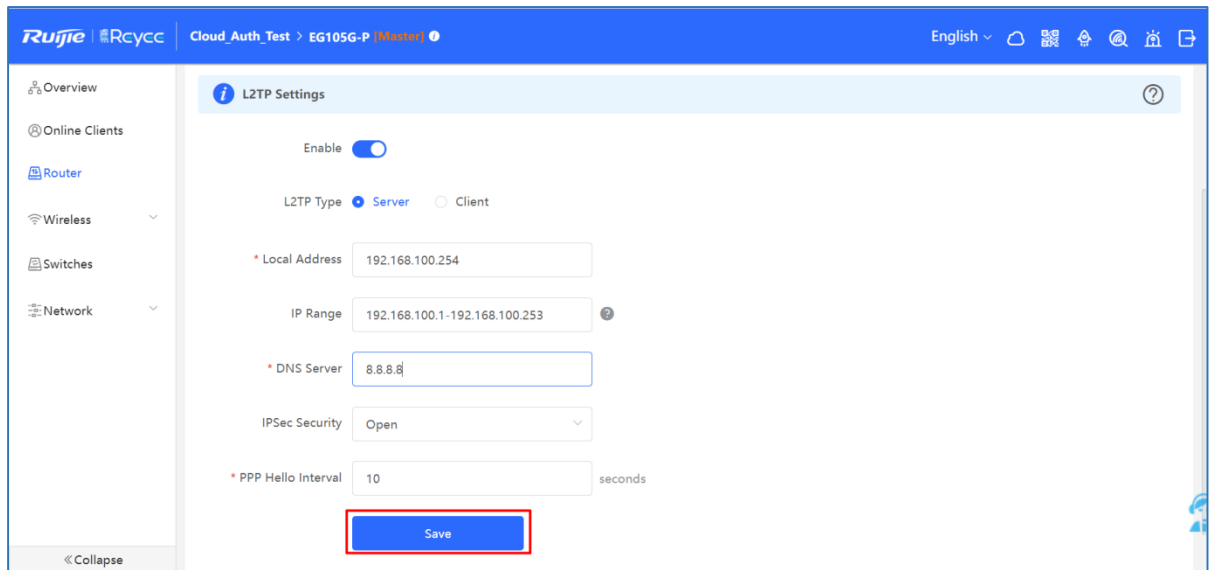
8.14.2 Site-to-Site Scenario Configuration

(1) On the HQ side:

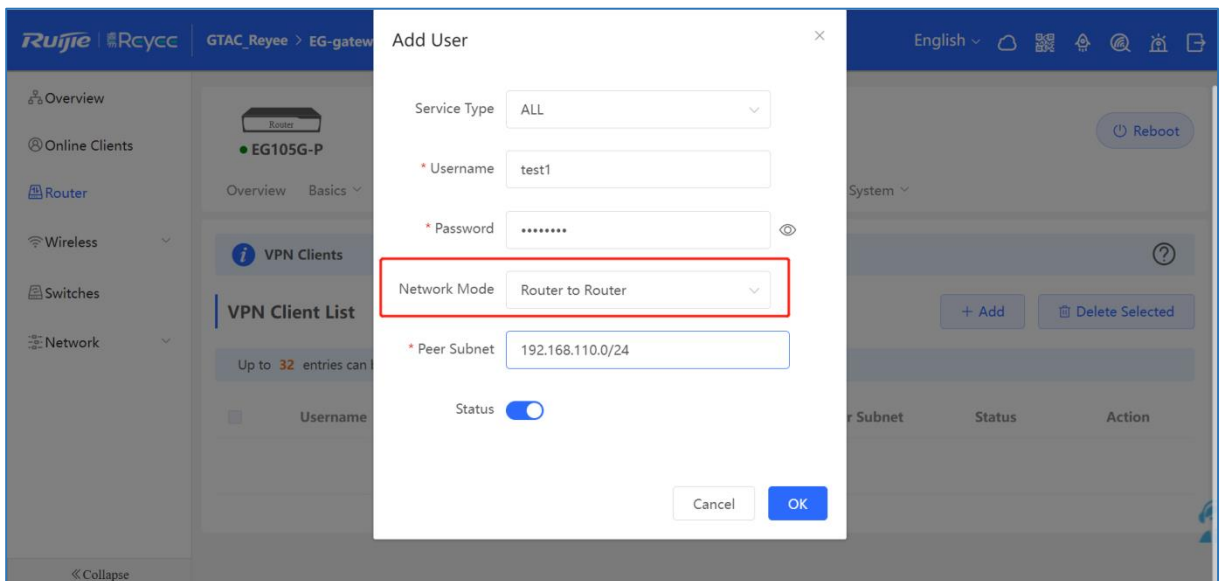
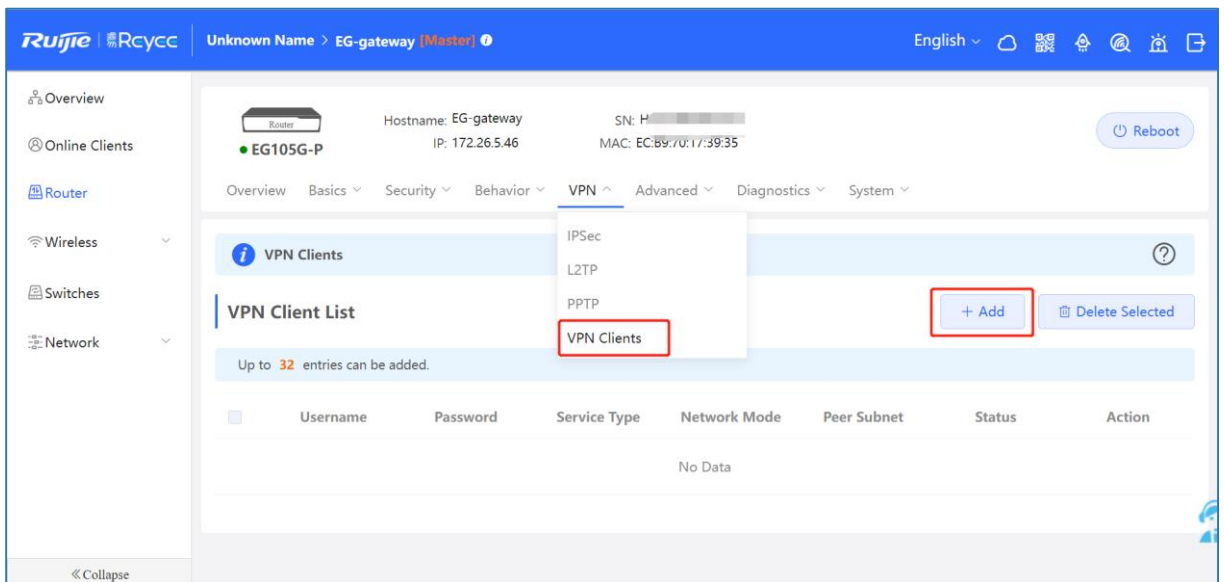
- a Log in to a Reyee EG router with the default IP address of 192.168.110.1.
- b Choose **SVPN > L2TP**, enable **L2TP**, and set **L2TP Type** to **Server**.



- c Perform L2TP configuration and click **Save**.



d Configure a VPN client.

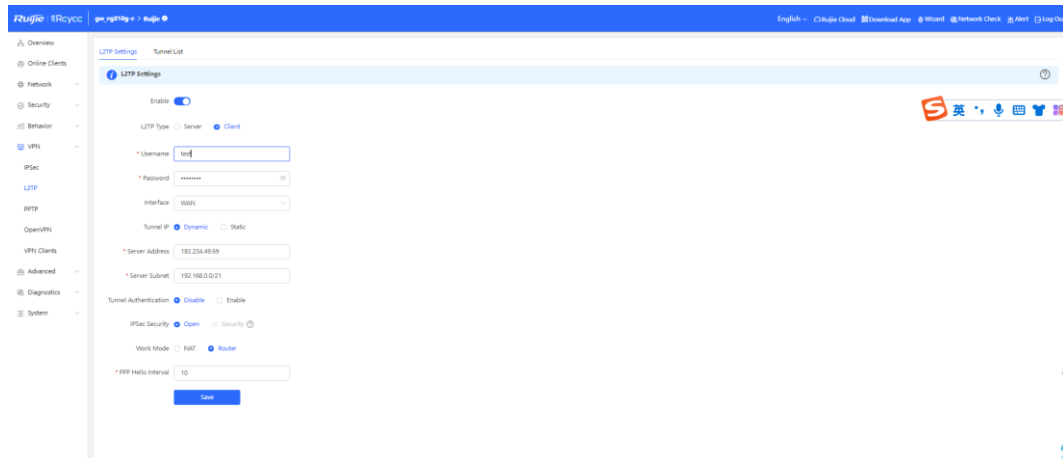


Caution

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

(2) Branch side:

- a Log in to a Ruijie EG router with the default IP address of 192.168.110.1
- b Choose **VPN > L2TP**, enable **L2TP**, and set **L2TP Type** to **Client**.



Caution

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

(3) Check the VPN connection status.

	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input type="checkbox"/>	test1	Client	l2tp	192.168.30.1	172.26.6.190	192.168.30.254	8.8.8.8	Delete

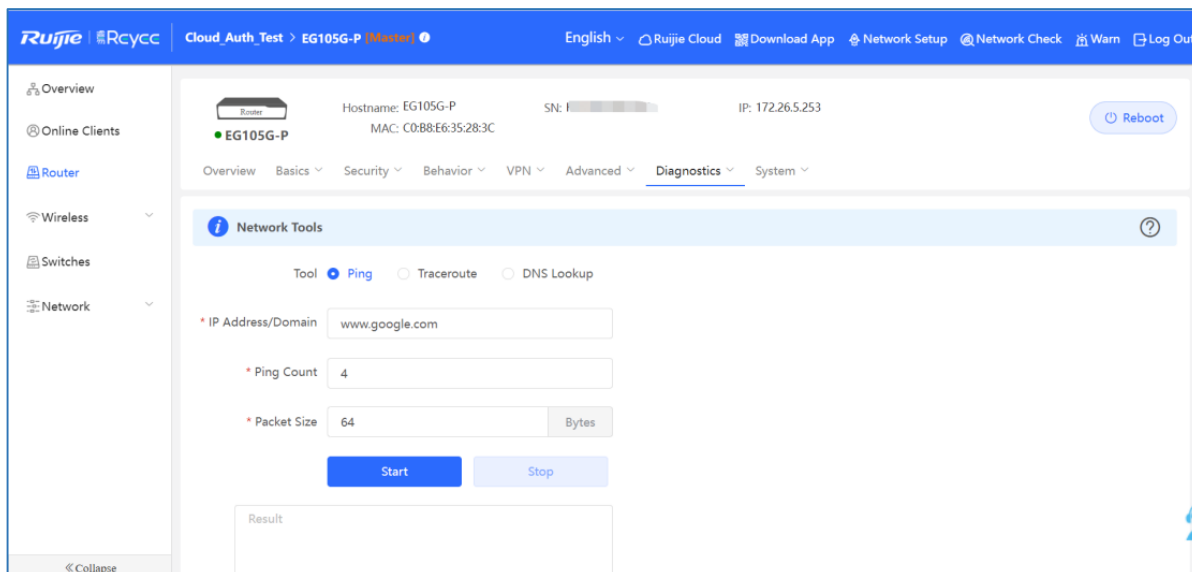
8.15 Can a Ruijie EG Router Establish an L2TP VPN with Third-Party Devices or Ruijie EG Routers?

A Ruijie EG router can establish a L2TP VPN with L2TP-capable third-party devices and Ruijie EG routers.

8.16 What Can I Do If a Ruijie EG Router Fails to Connect the L2TP VPN?

(1) Check whether the EG router of the branch can ping the EG router of the headquarters. If the ping fails, check the network connection between two EG routers

Choose **Diagnostics > Network Tools** and start the ping operation.



- (2) Check whether the username and password of VPN client settings of the headquarters are correct.
- (3) Check whether the settings are correct according to [8.14 How Do I Configure L2TP VPN on a Reyee EG Router?](#).
- (4) Check whether the WAN IP address of the EG router of the headquarters is a public IP address. If not, configure DMZ on your external device.

If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

8.17 What Can I Do If I Fail to Connect L2TP VPN on a PC?

- (1) Check whether PC settings are correct according to 8.14.1 Client-to-Site Scenario Configuration.
- (2) Check whether the PC can ping the EG router of the headquarters. If the ping operation fails, check the network connection on your PC.
- (3) Check whether the WAN IP address of the EG router of the headquarters is a public IP address. If not, configure DMZ on your external device.

If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

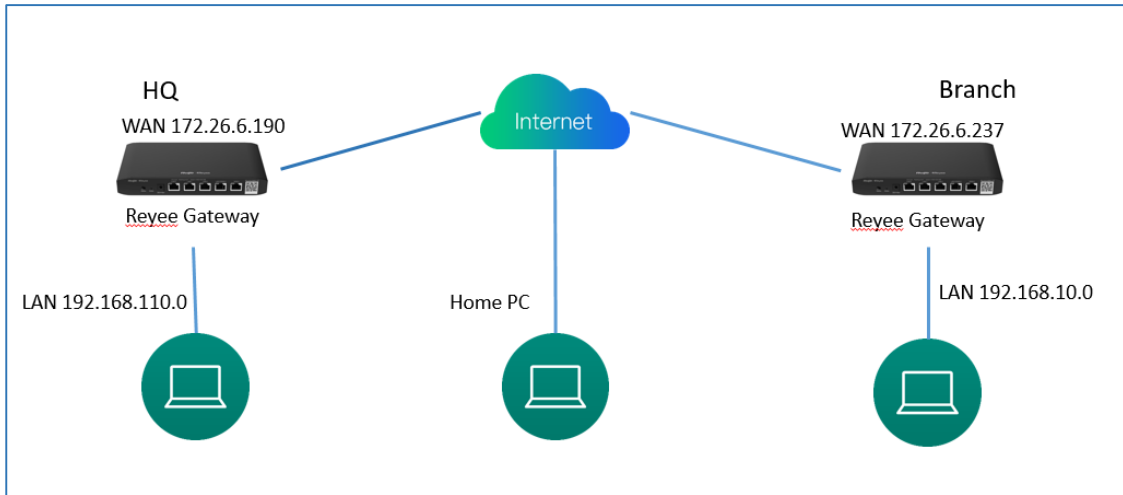
8.18 Can a Reyee EG Router Be Enabled with L2TP and IPsec Simultaneously?

A Reyee EG router can be enabled with L2TP over IPsec.

8.19 How Do I Configure L2TP over IPsec VPN on a Reyee EG Router?

L2TP over IPsec VPN is typically applied to client-to-site and site-to-site scenarios. For example, three branches of a company are distributed in three different places of the Internet, and branches need to establish tunnels by using the gateways. Data between the company intranets (several PCs) is securely exchanged through the L2TP over IPsec VPN tunnel established by these gateways, and employees who work at home can access company data through L2TP over IPsec VPN tunnels.

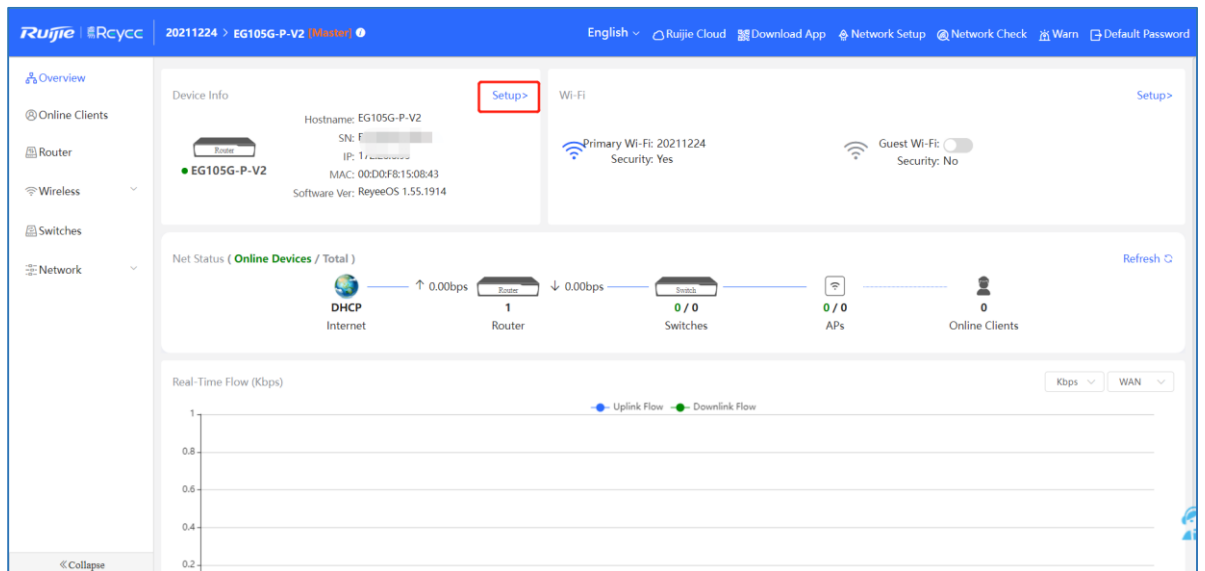
L2TP over IPsec VPN is applied to the following scenarios.

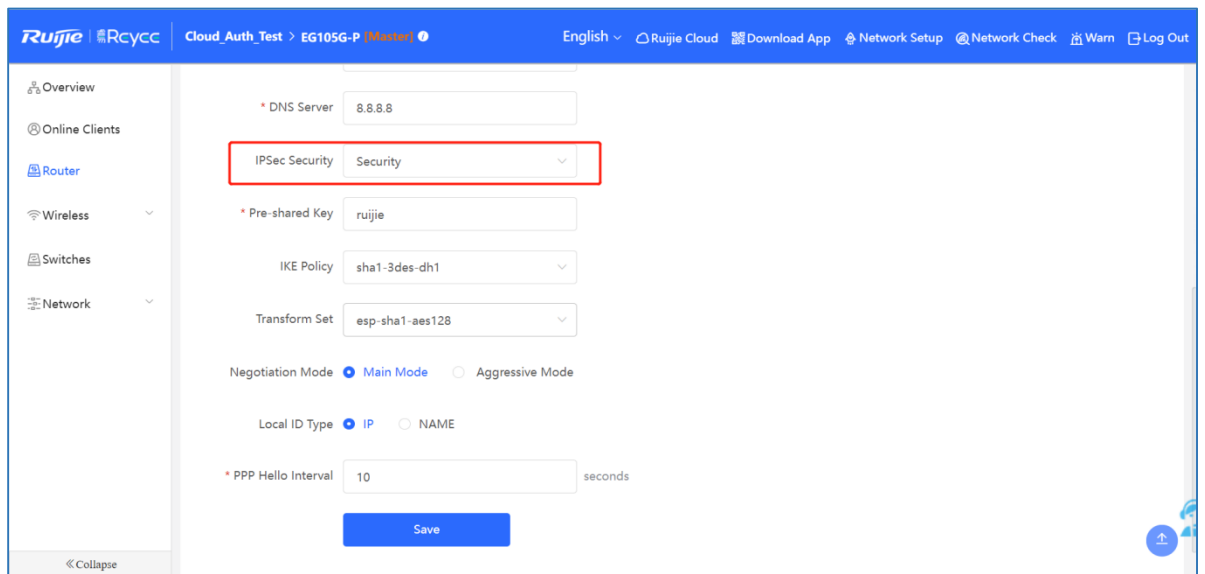
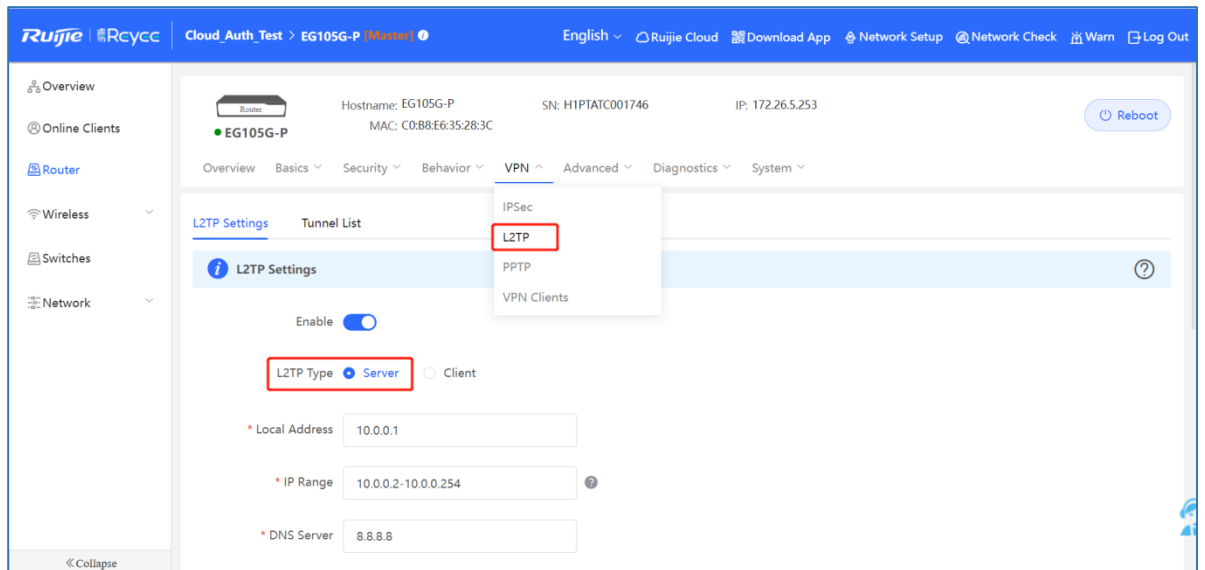


Perform the following steps to configure an L2TP over IPsec VPN.

(1) Headquarters side:

- a Log in to a Reeye EG router with the default IP address of 192.168.110.1.
- b Choose Setup > VPN > L2TP and select IPsec Security.

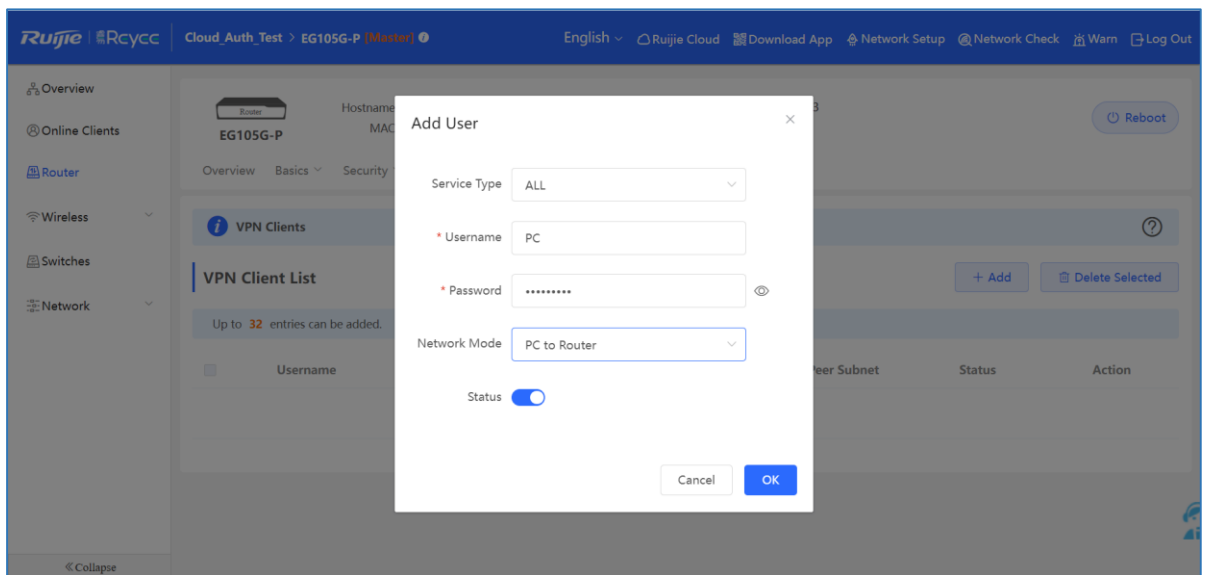
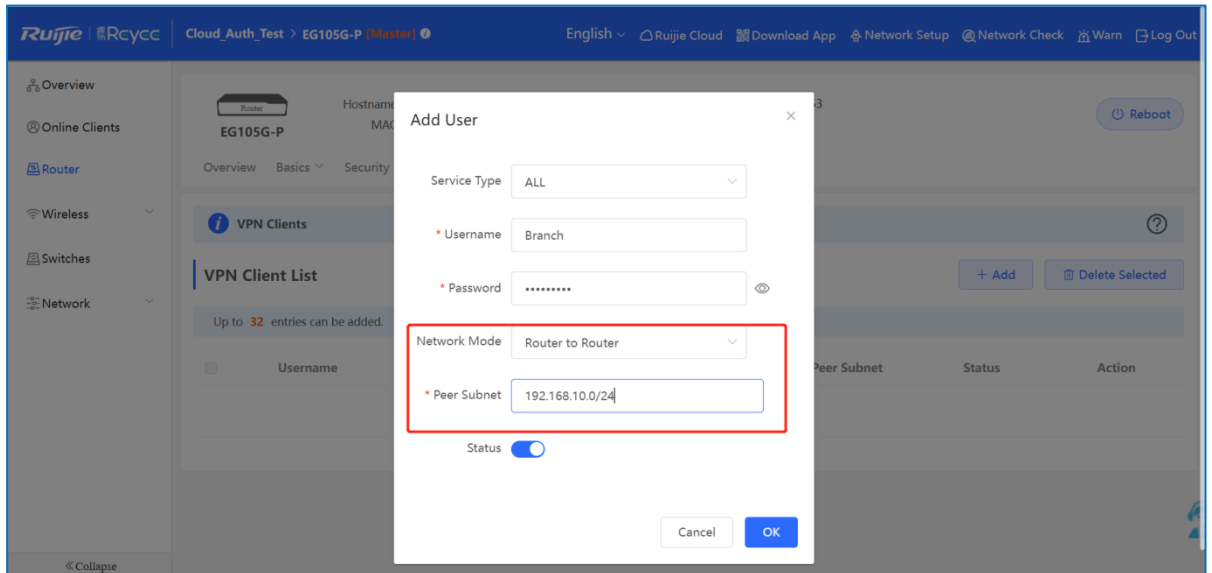
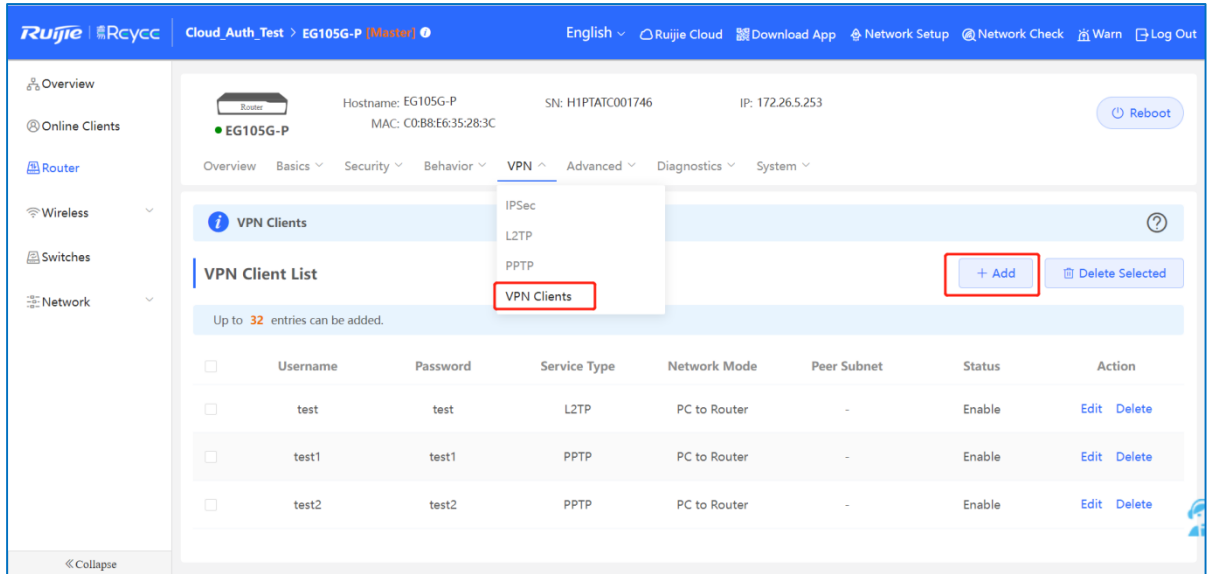





Caution

- **PPP Hello Interval:** Enter the interval between hello messages on a PPP over IPsec connection.
- **IPsec Auth:** Whether IPsec is used on a tunnel.
- **Pre-shared Key:** A pre-shared key is required for IPsec encryption.
- **Local ID Type:** When the WAN port of the headquarters is configured with a public IP address, select **IP**. When the WAN port of the headquarters is configured with a private IP address, select **Name** and configure DMZ on the external device.

c Configure VPN clients: one is for the branch EG and the other is for the PC.



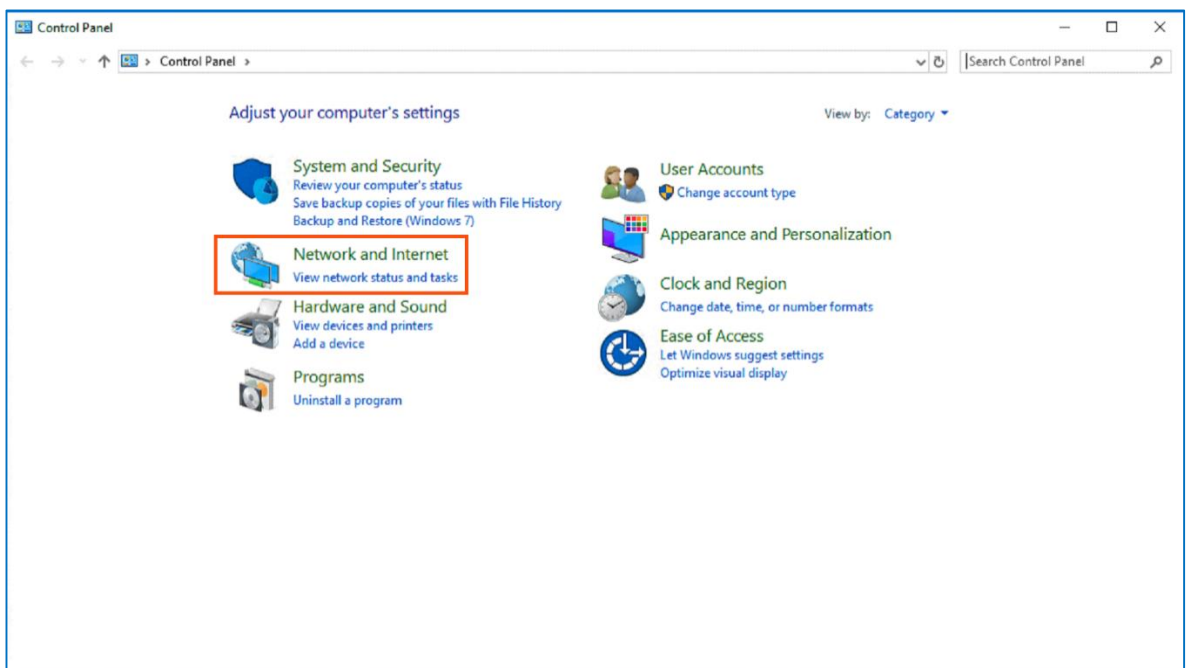
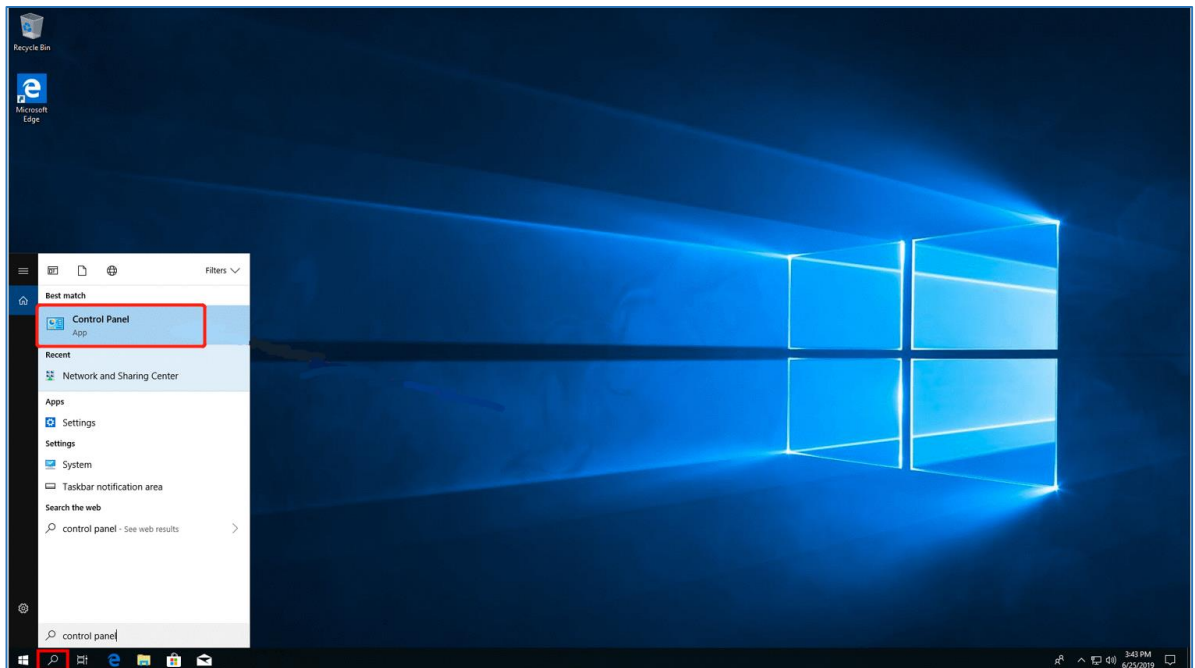
 Instruction

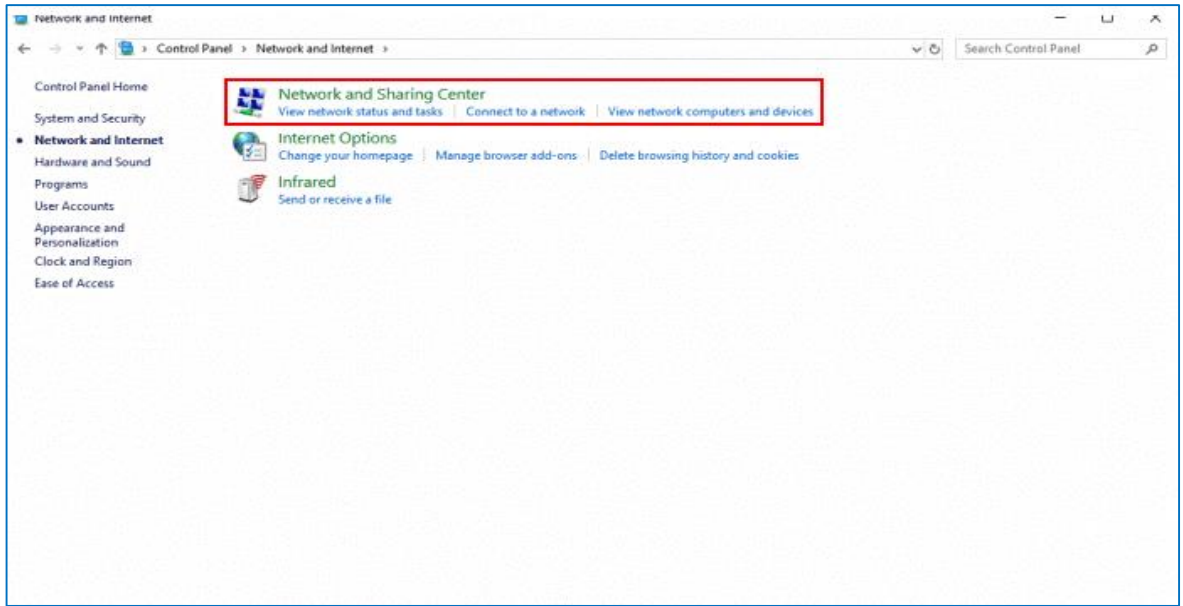
- **PC to Router:** The connection is established between a PC and a terminal.
 - **Router to Router:** A direct, non-shared, and secure connection is set up between two terminals.
-

8.19.2 Client-Side Configuration

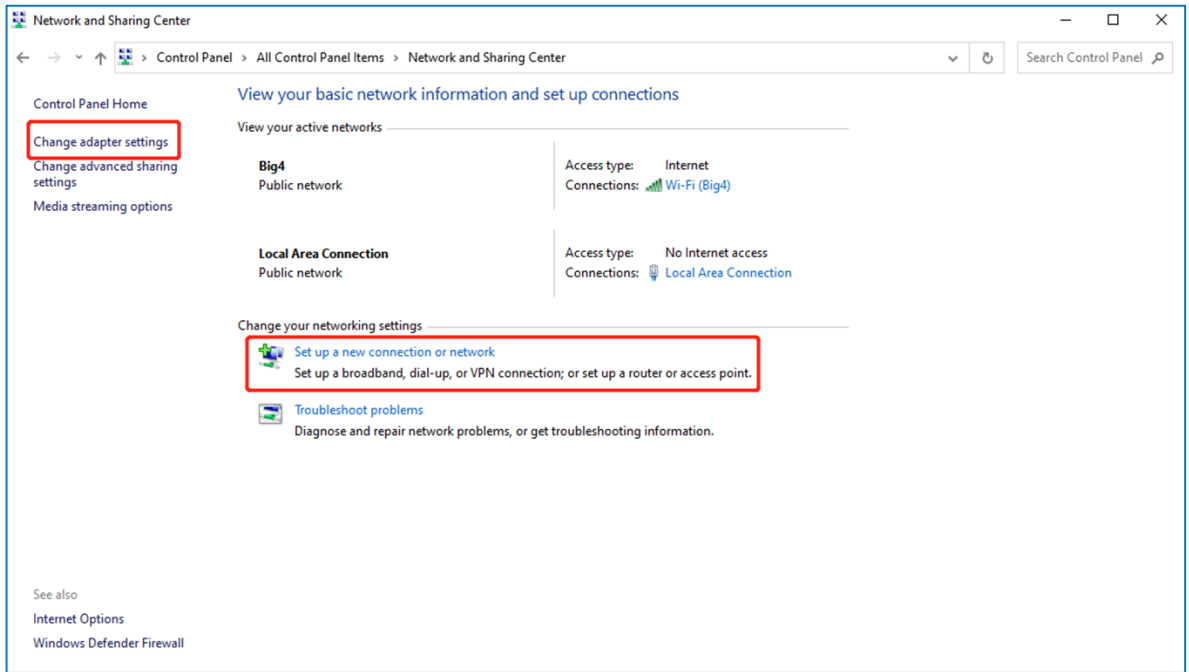
The following example describes how to configure a client on the Windows 10 system.

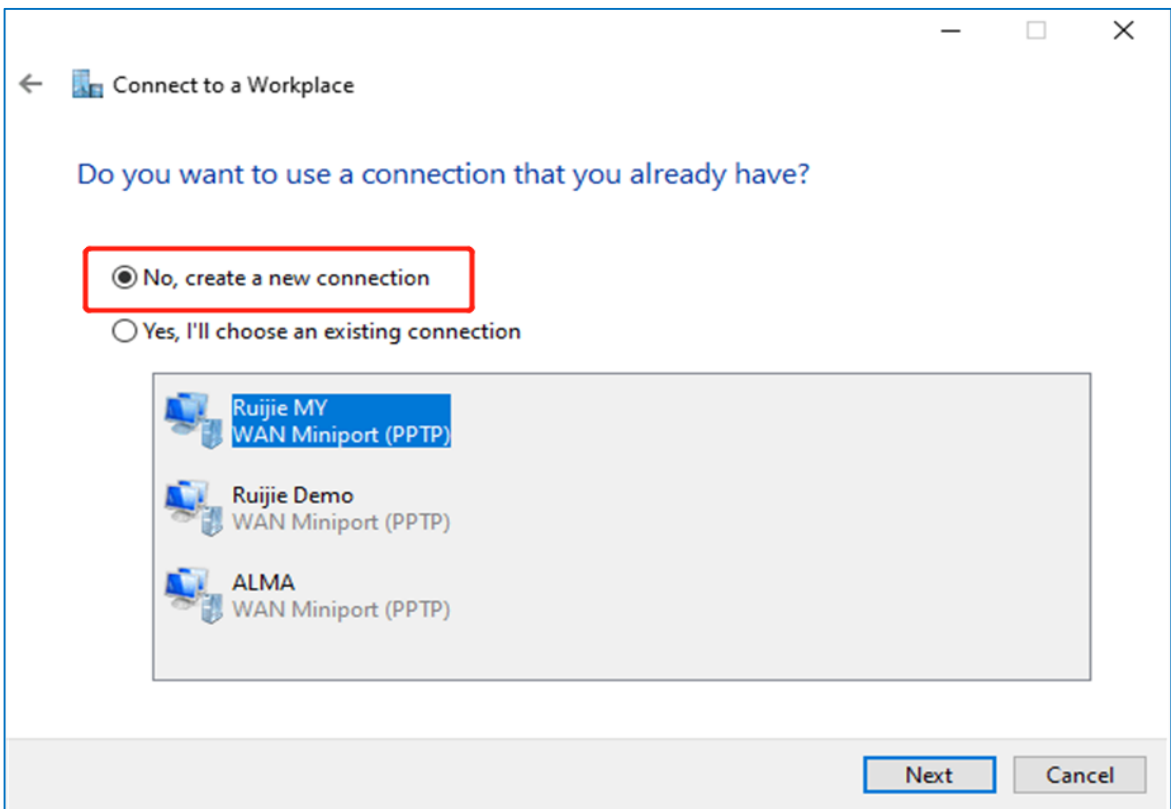
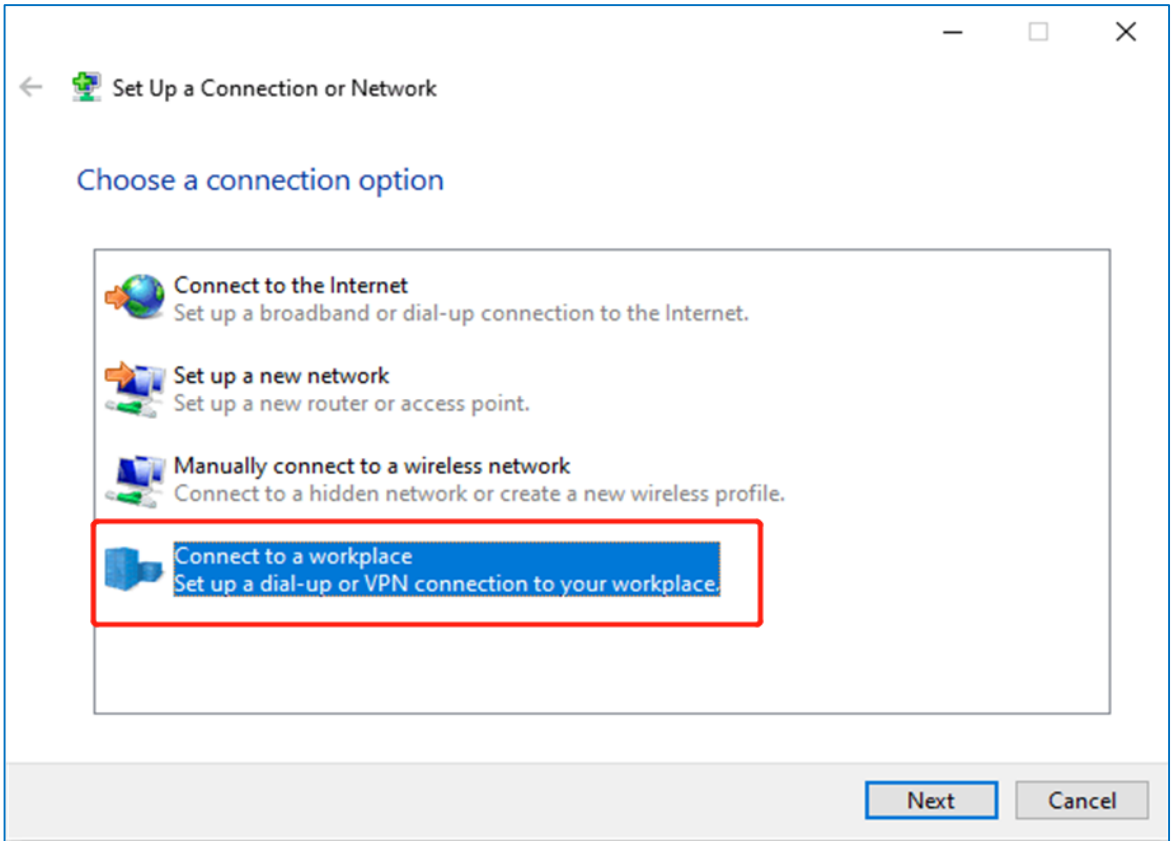
- (1) Choose **Control Panel > Network and Internet > Network and Sharing Center**.

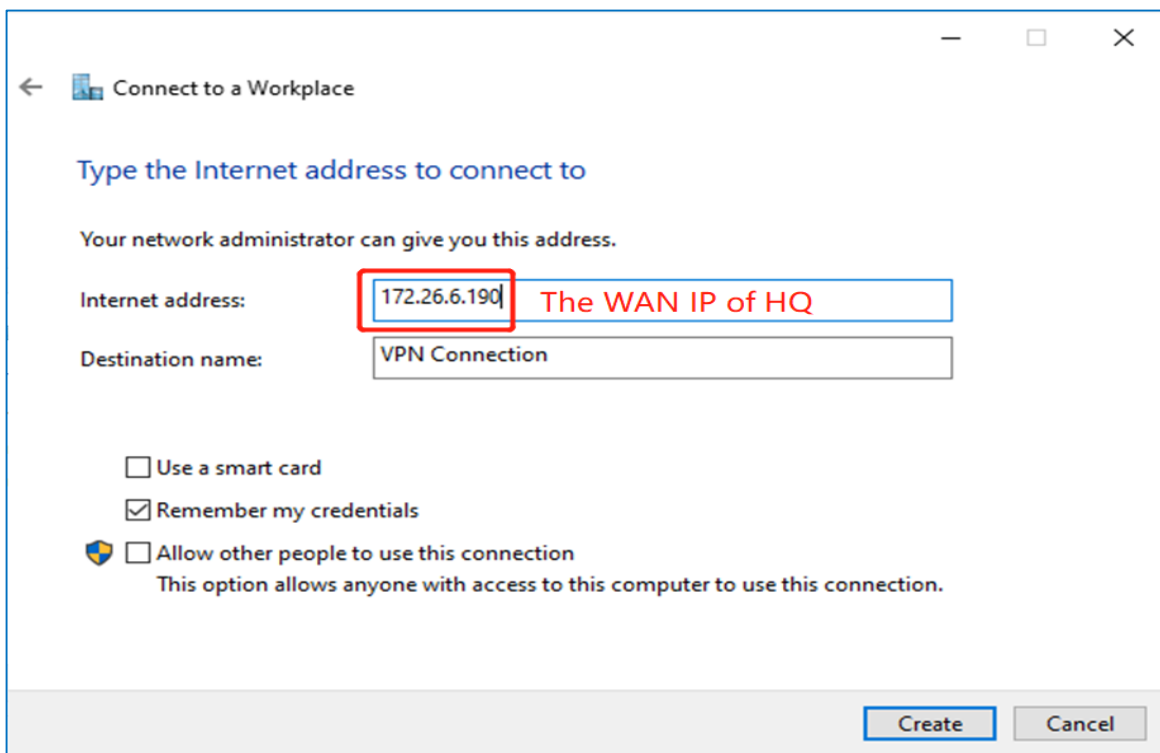
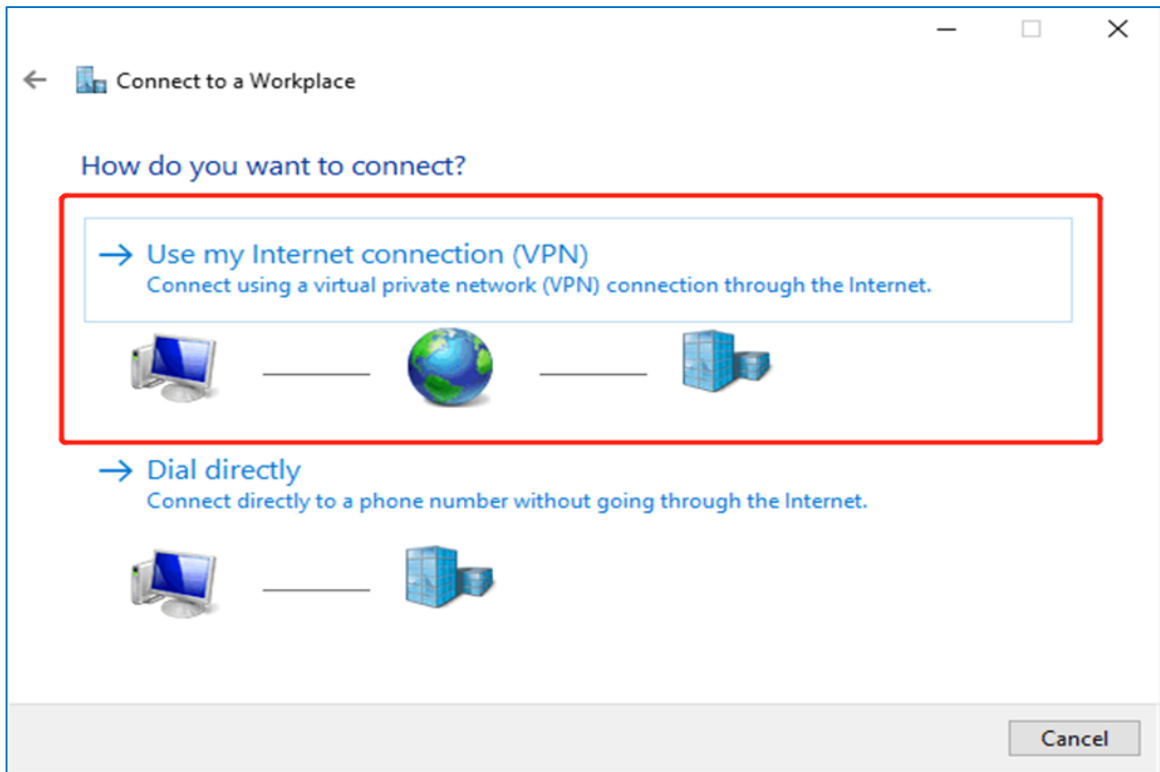




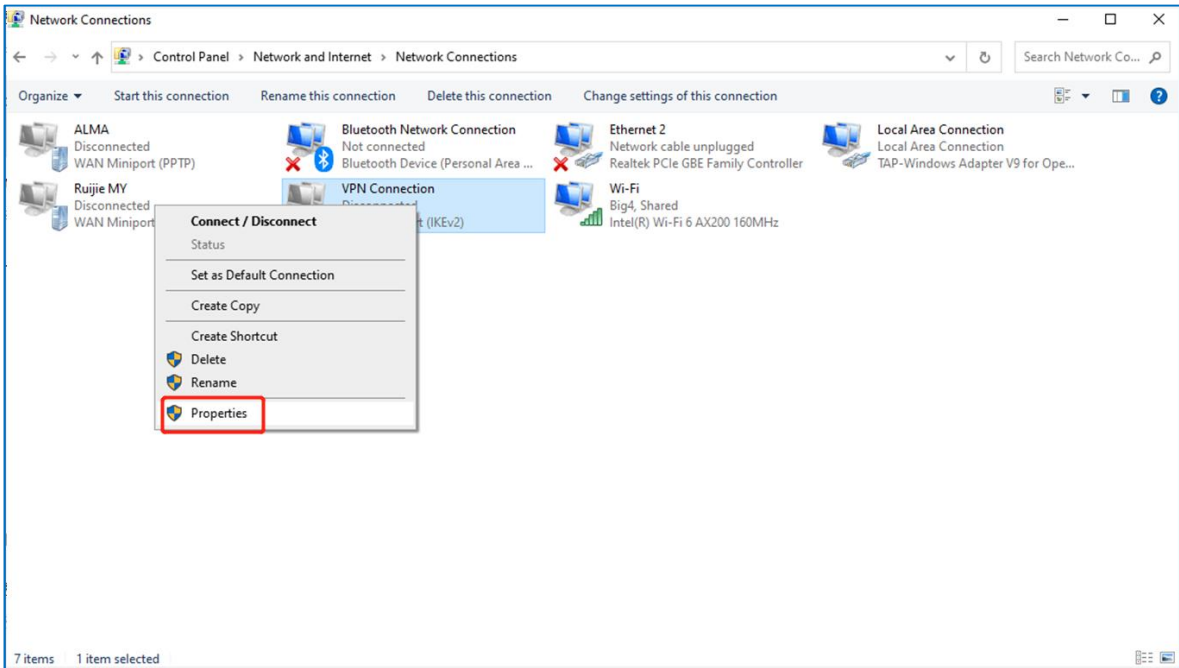
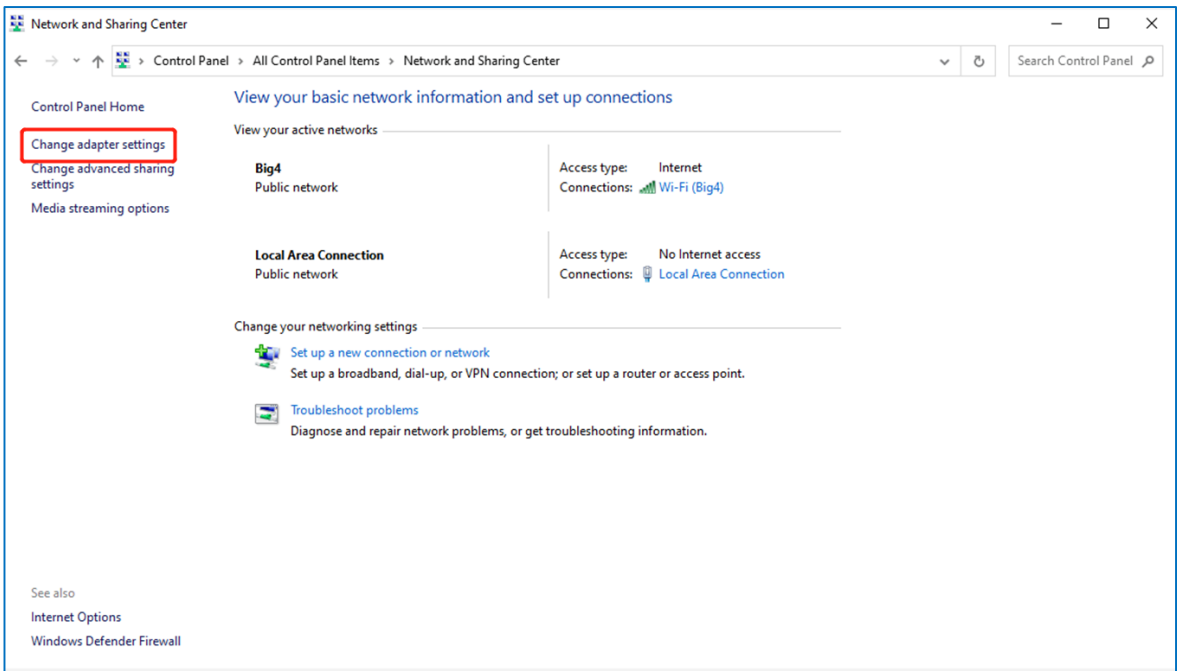
(2) Configure a VPN connection.

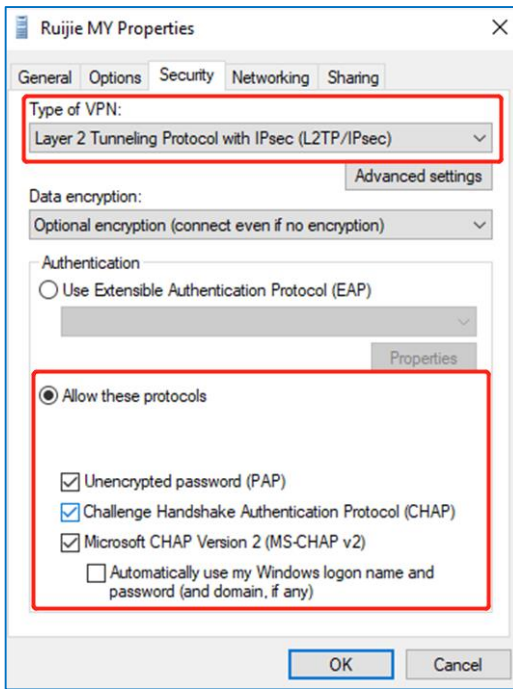




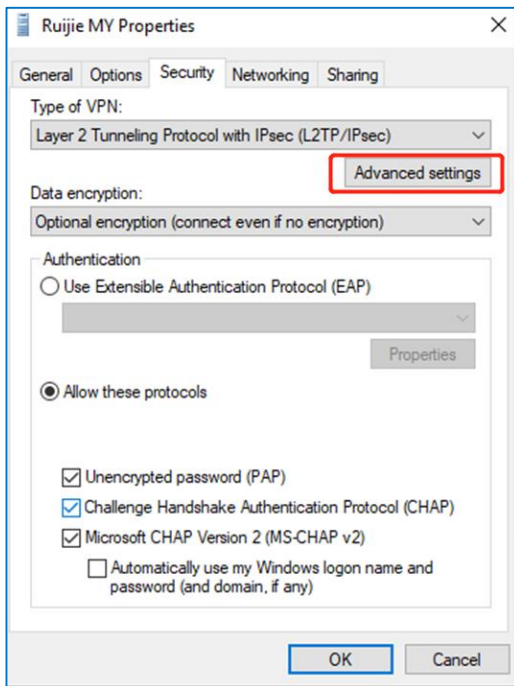


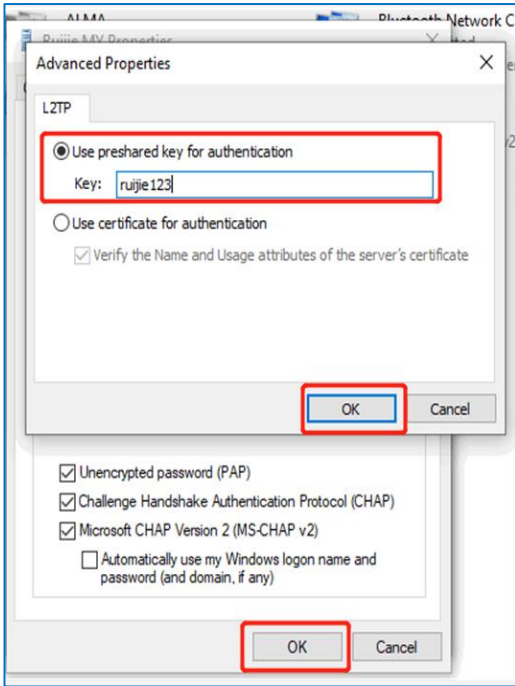
(3) Change the adapter configuration.



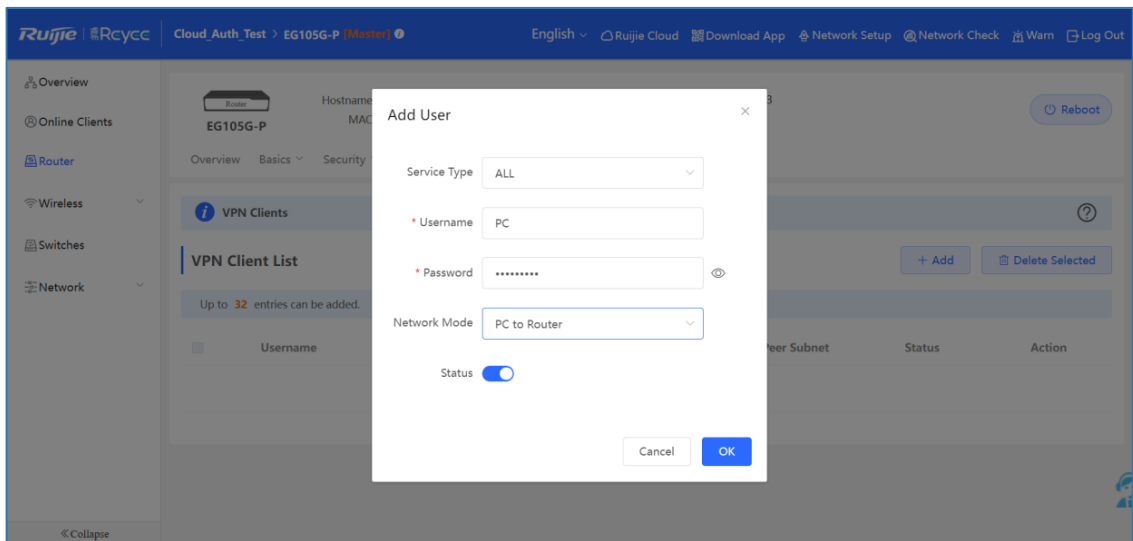


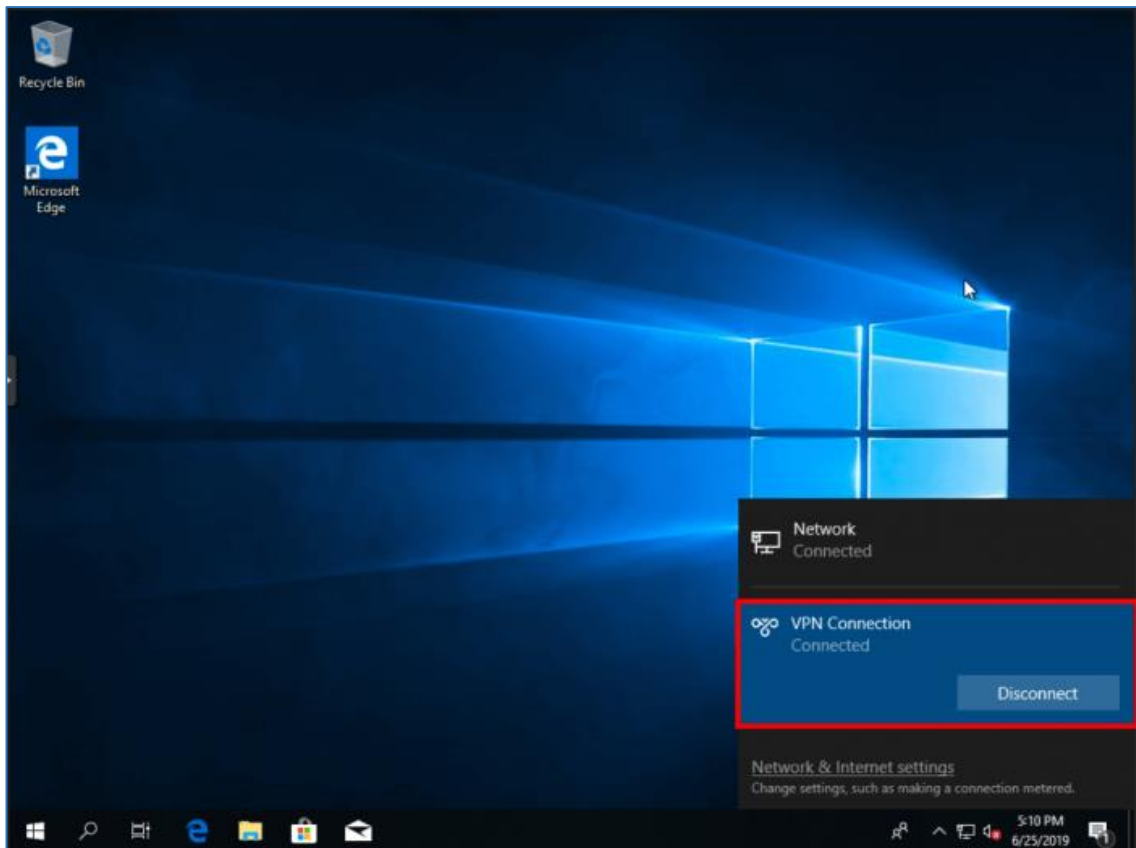
(4) Click **Advanced Settings** to configure the pre-shared password.





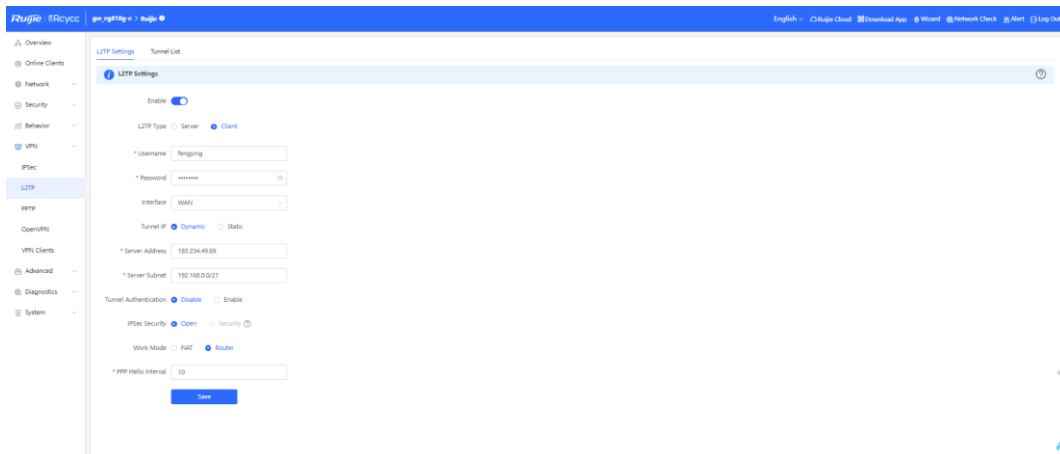
(5) Set **Network Mode** to **PC to Router** to connect the VPN.



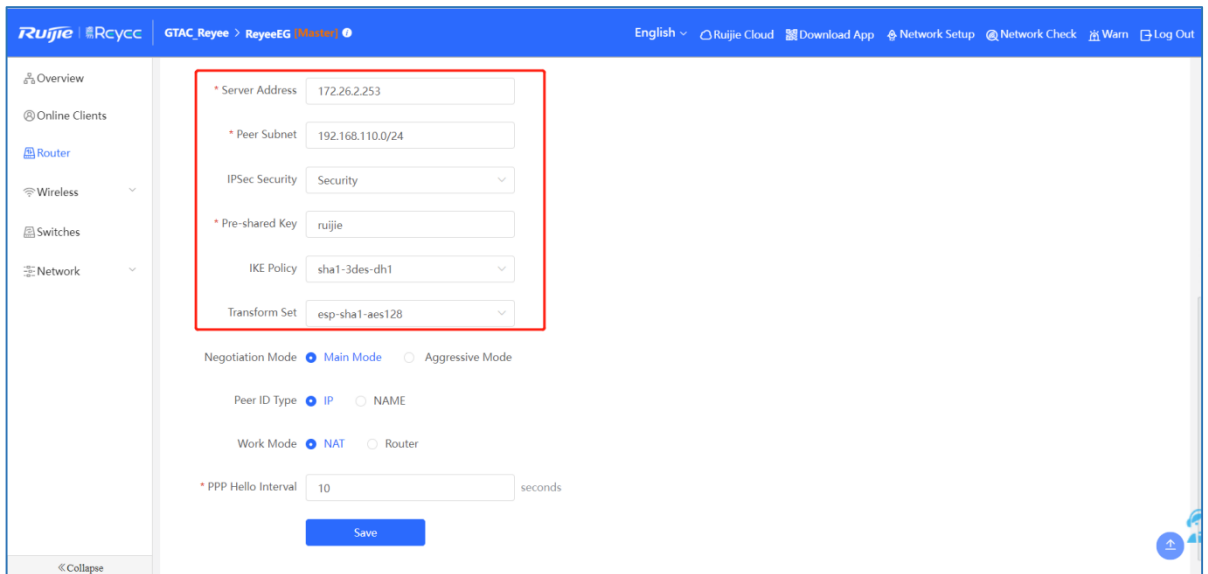


8.19.3 Branch-Side Configuration

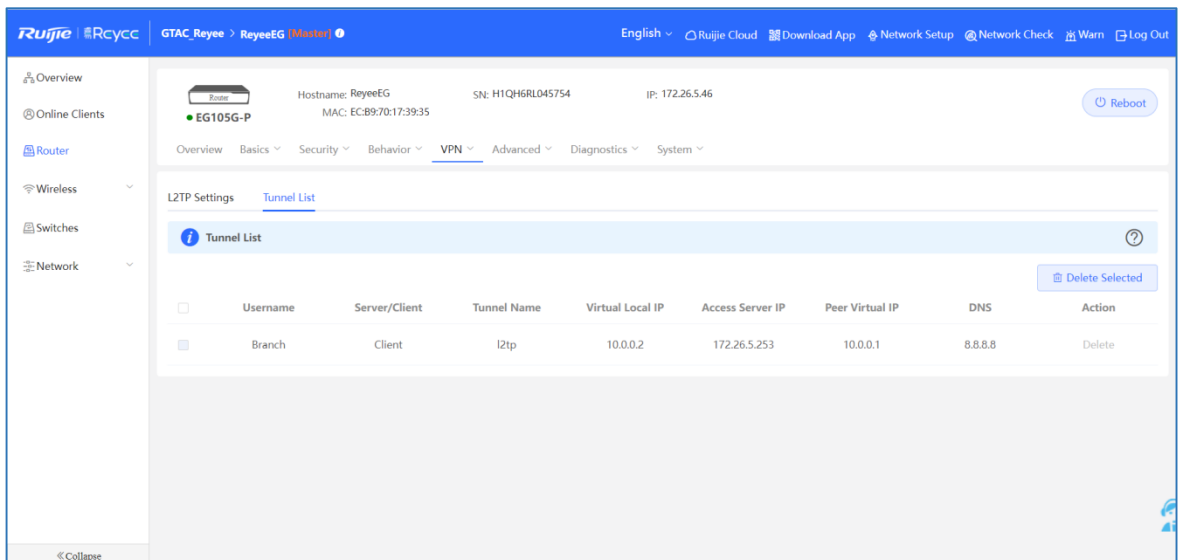
- (1) Log in to a Reyee EG router with the default IP address of 192.168.110.1.
- (2) Choose **VPN > L2TP** and enable IPsec.



- (3) Configure IPsec and ensure that the pre-share password, IKE policy, and transform set are the same at both ends.



(4) Check the status of L2TP over IPsec connection.

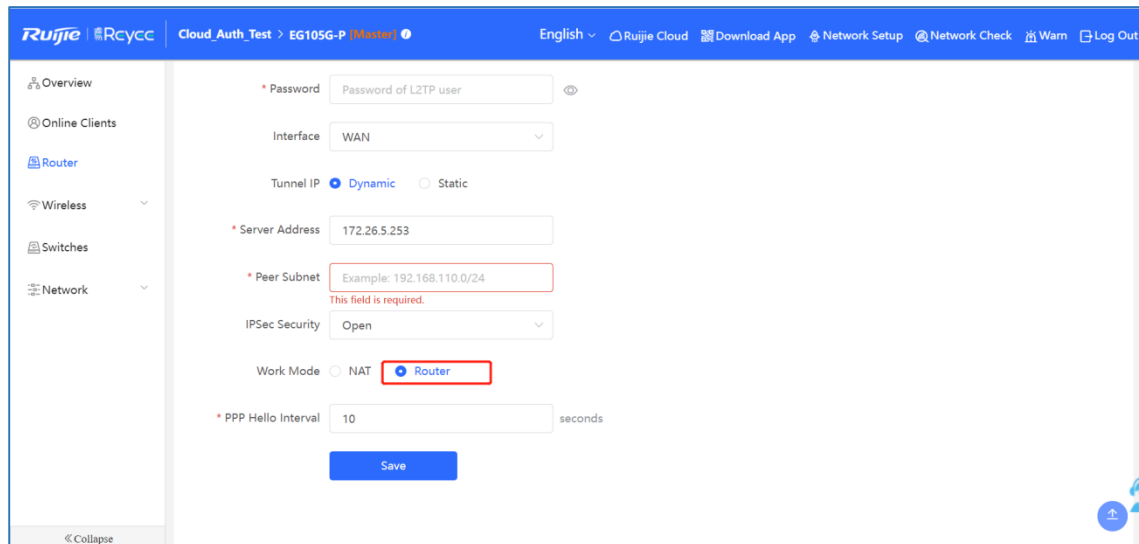


8.20 Can a Reyee EG Router Establish an L2TP over IPsec VPN with Third-Party Devices or Ruijie EG Routers?

A Reyee EG router can establish an L2TP over IPsec VPN with third-party devices that support L2TP over IPsec and Ruijie EG routers.

8.21 Can Branches Connect to Each Other?

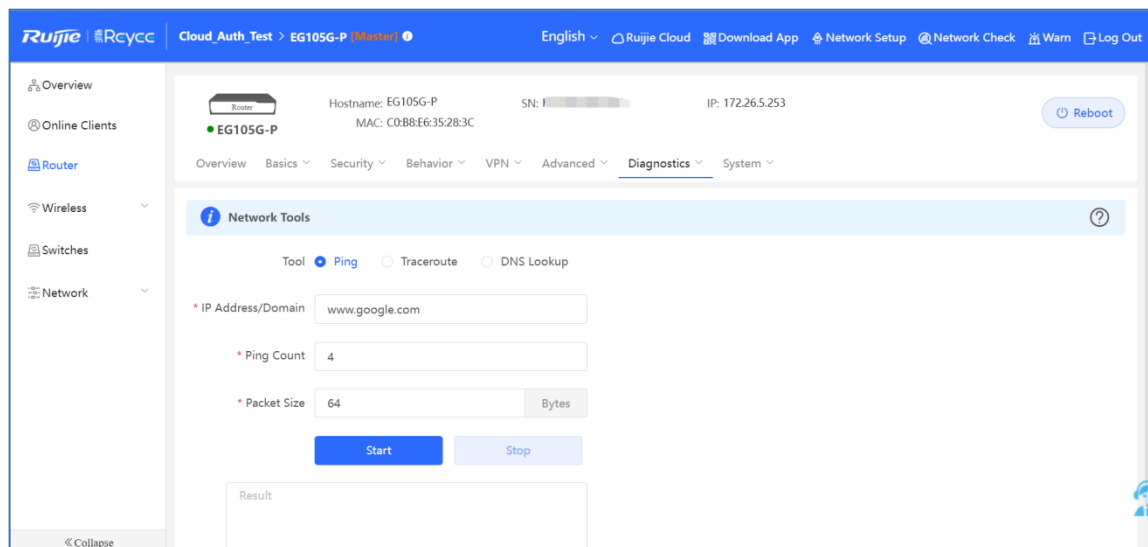
Yes, you can set **Work Mode** to **Router**. Then the branches can connect to each other.



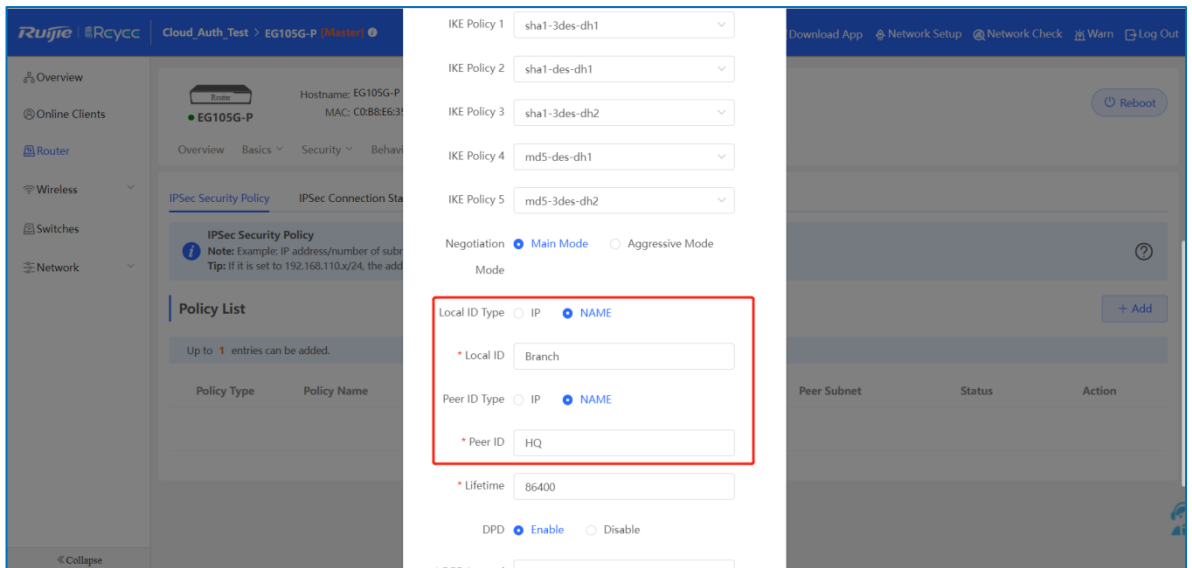
8.22 What Can I Do If I Fail to Connect L2TP over IPsec VPN on a Reyee EG Router?

- (1) Check whether the EG router of the branch can ping the EG router of the headquarters. If the ping operation fails, check the network connection between two EG routers.

Choose **Diagnostics > Network Tools** and start the ping operation.



- (2) Check whether PC settings are correct according to [8.19 How Do I Configure L2TP over IPsec VPN on a Reyee EG Router?](#).
- (3) Check whether the WAN IP address of the EG router of the headquarters is the public IP address. If not, configure DMZ on your external device and set **Local ID Type** to **Name** on EG routers of the headquarters and branches.



If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

9 FAQs About DDNS

9.1 What Is DDNS?

Dynamic DNS (DDNS) allows users on the Internet to gain access to resources on a local network when the Internet address of the local network is constantly changing. The resources mainly include the web server, Webcam, and a PC for remote control operation.

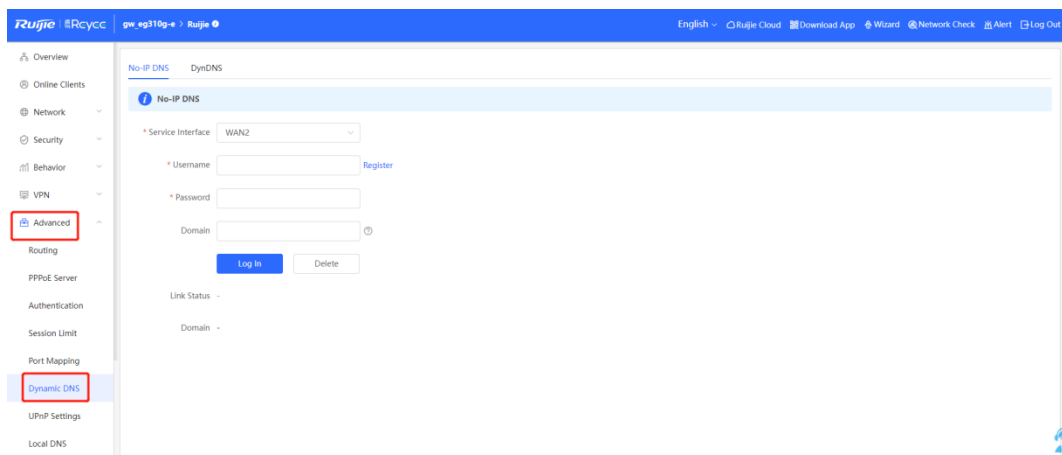
9.2 Which DDNS Service Providers Are Available for Reyee Devices?

Reyee devices support No-IP DNS, DynDNS, and Ruijie DDNS.

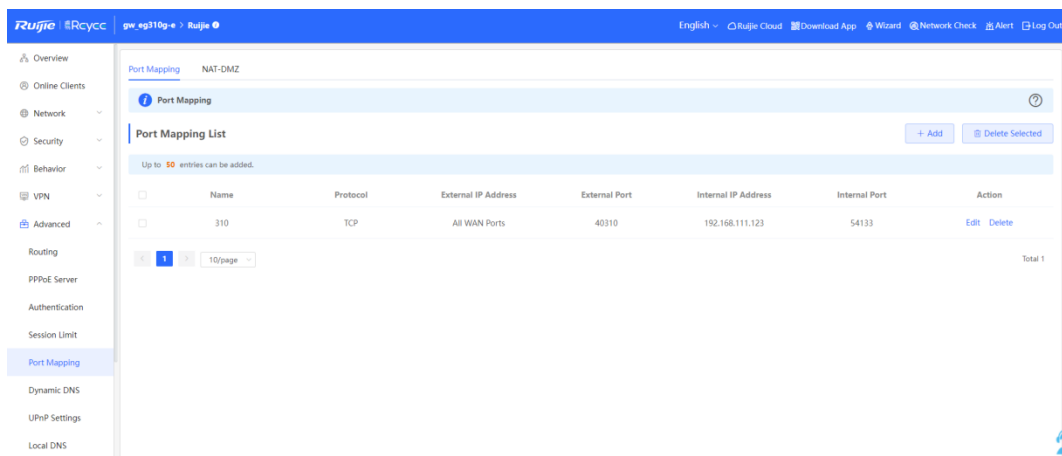
9.3 To Which Scenarios Are DDNS Applied?

(1) Access intranet servers or cameras through domain names.

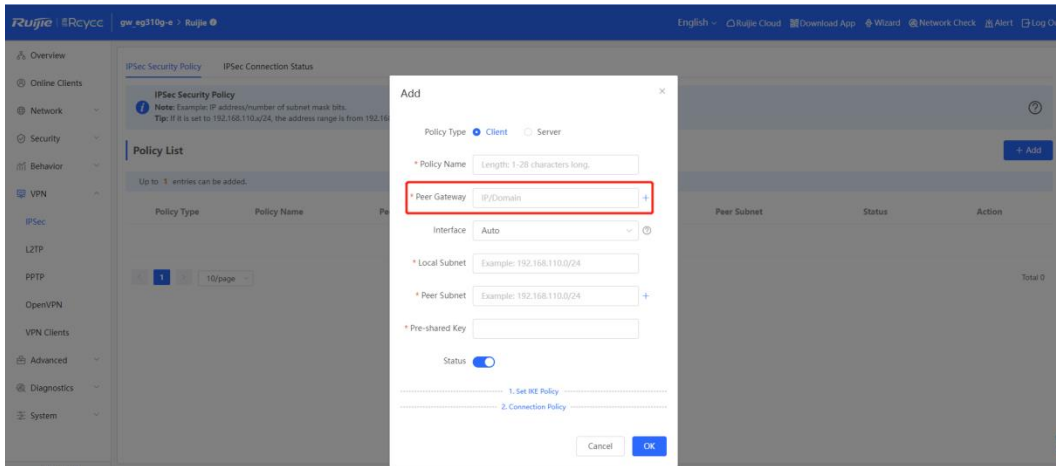
a Choose **Advanced > Dynamic DNS** and configure DDNS on a Reyee device.



b Choose **Advanced > Port Mapping** and configure port mapping on a Reyee device. Port mapping can map TCP/UDP ports to the corresponding ports on the intranet device.



(2) Choose **VPN > IPSec VPN** to configure a VPN client to connect to the VPN server through domain names.

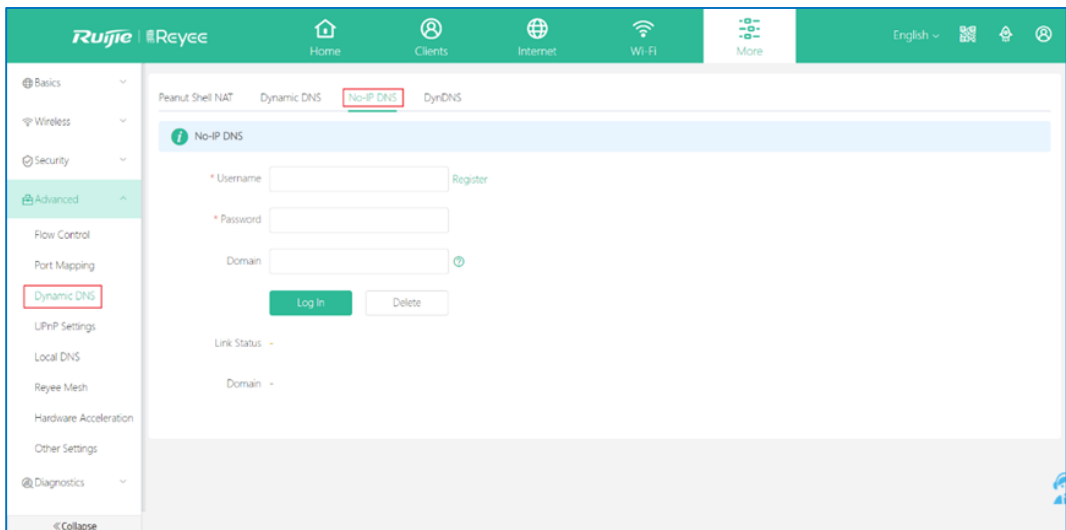


(3) Log in to the web interface of the device.

For the Reycce EW router, you can configure DDNS and enable **Remote Access** on the web page. Then you can log in the web interface through DDNS domain names.

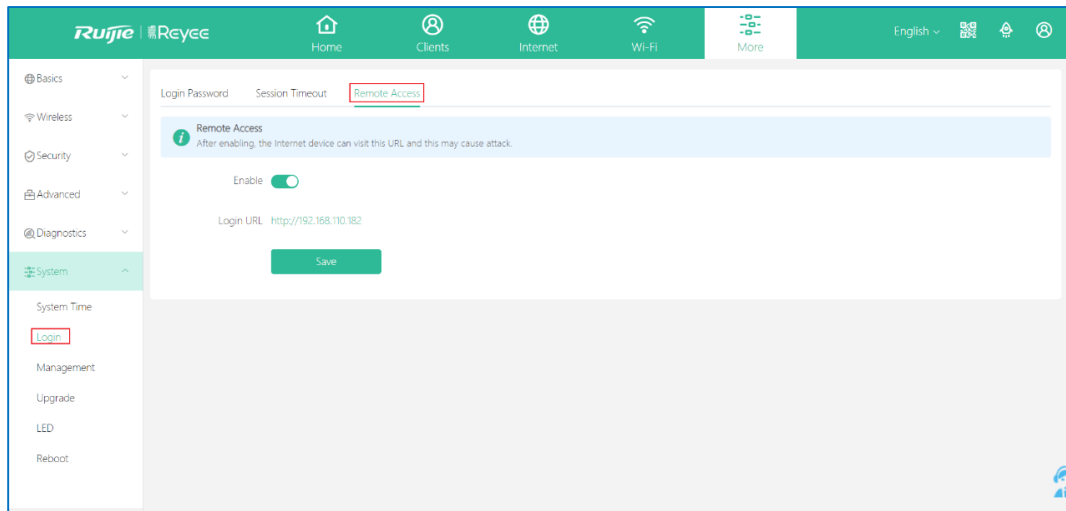
a Configure DDNS on the Reycce device.

Choose **More > Advanced > Dynamic DNS**.



b Enable **Remote Access**.

Choose **More > System > Login > Remote Access**.



⚠ Caution

The web interface of the ReyeE EG router is inaccessible through the DDNS domain name. This is because the ReyeE EG router does not support web interface access through the WAN port's IP address.

10 FAQs About Behavior Strategy

10.1 What Should I Do If the Behavior Strategy Does Not Take Effect?


- (1) Check whether IP addresses that need to be blocked are added to **IP Address Group**.
- (2) Check whether the current time is within the range of the strategy time that you have scheduled before.
- (3) Check whether the apps or websites that need to be blocked are selected.

 **Caution**

The value of **Time** for behavior strategy means the time when this strategy takes effect.

10.2 How Do I Configure the Users That Are Allowed to Access Only Certain Websites/Apps?


The Reyee EG router does not provide the whitelist function, so it cannot limit the users that access certain websites or apps.

 **Caution**

Ruijie EG device routers do not support the whitelist function.

10.3 How Do I Configure Different Users to Access Different Websites/Apps?

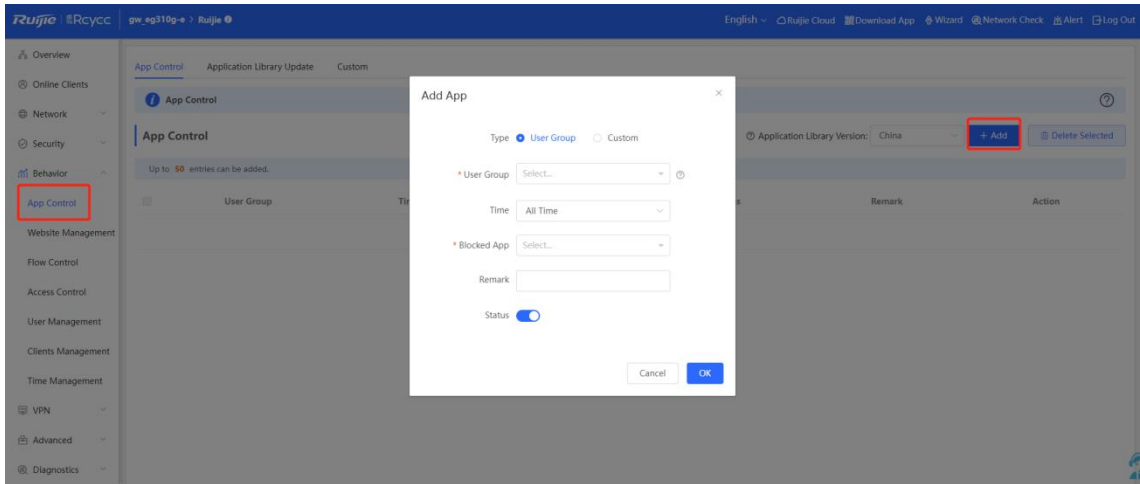
- (1) Create different behavior strategies for different users.
- (2) Customize the IP address or IP address range and websites/apps separately for different users with different behavior strategies.

 **Caution**

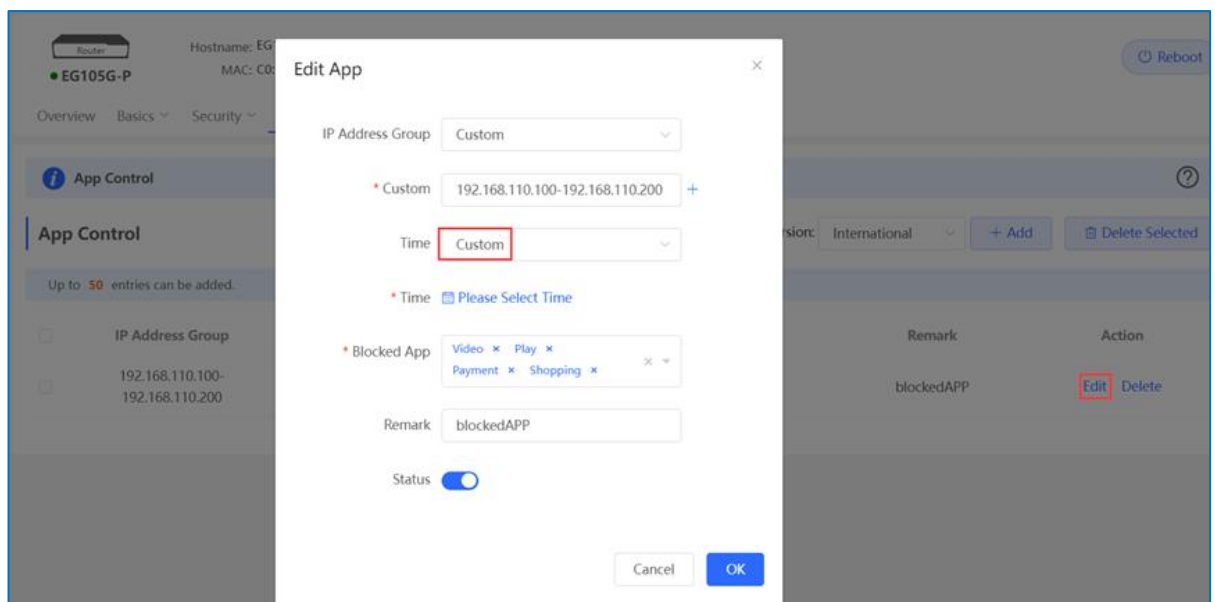
Up to 20 behavior strategies can be added on a Reyee router.

10.4 How Is the Access/Blocking Time Customized for Websites/Apps?

- (1) Click **App Control/ Website Management**, and then Click **Add** to add a behavior strategy.



(2) Select **Custom** from the **Time** drop-down list box and select the time range.



⚠ Caution

The value of **Time** for behavior strategy means the time when this strategy takes effect.

10.5 How Many Behavior Strategies Can Be Created?

Up to 20 behavior strategies can be added on a Reycs router.

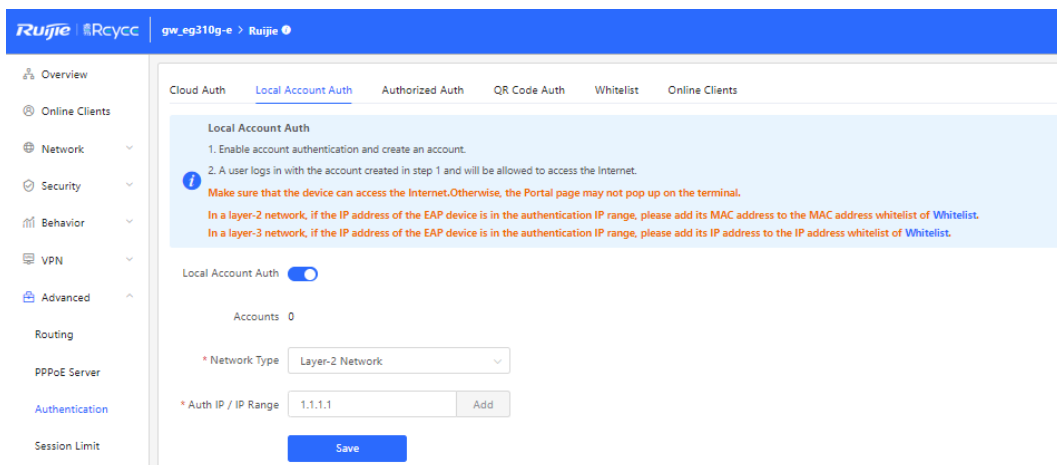
11 FAQs About Authentication

11.1 What Should I Do If Local Account Authentication Does Not Take Effect?

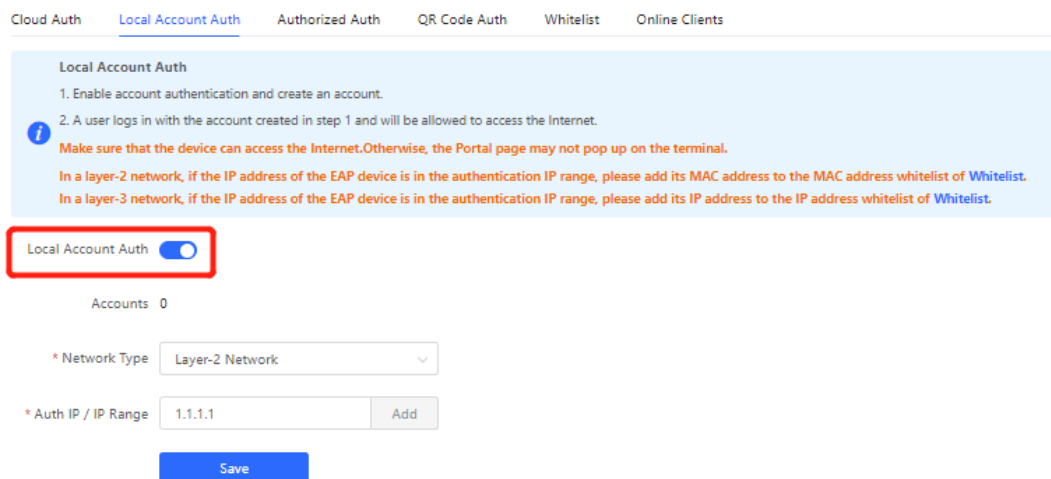
- (1) Check whether the router can access the Internet. Otherwise, the portal page may be not displayed on the terminal.
- (2) Check whether the IP address is in the range of **Auth IP / IP Range**. If not, add the IP address to the range.
- (3) Check whether the IP address is added to the whitelist. The IP address in the whitelist does not need to be authenticated.
- (4) Check whether the username and password of your account are correct.

11.2 How Is Local Account Authentication Configured on a Reyeer Router?

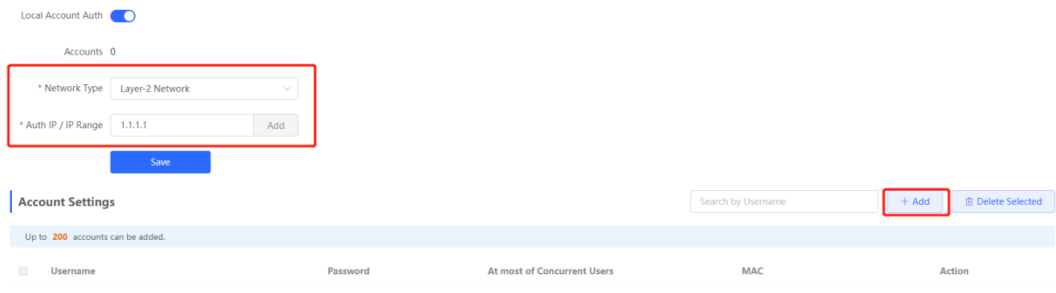
- (1) Choose **Advanced > Authentication > Local Account Auth**.



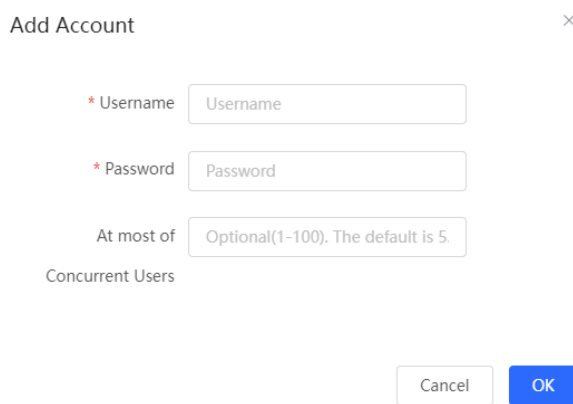
- (2) Enable **Local Account Auth** on the web page of the Reyeer router.



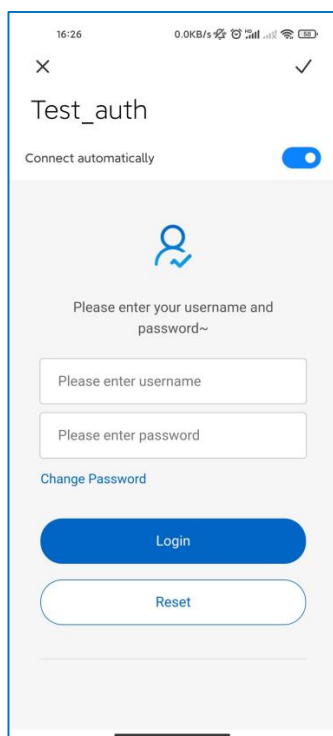
- (3) Select a network type. Enter an authentication IP address or IP range and click **Add**. Click **Save** to add a local account.



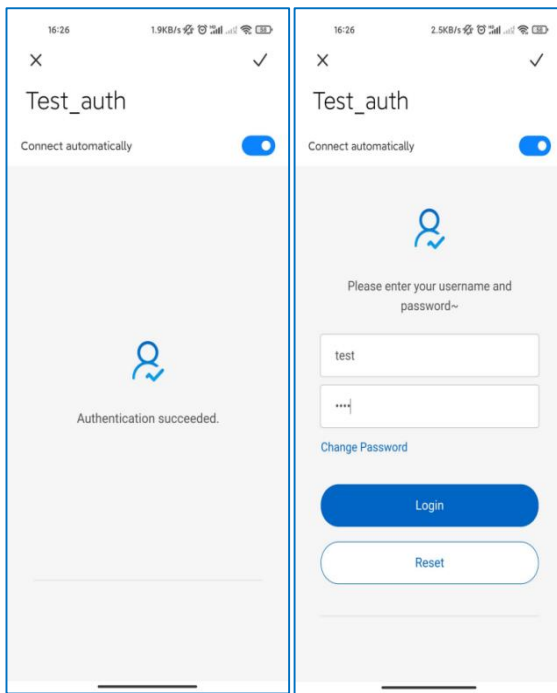
- (4) Click **Add** in the **Account Settings** pane. In the displayed **Add Account** window, configure the username and password for the local account and click **OK**.



- (5) When the client with the specified authentication IP address or in the authentication IP range tries to access the Internet, the authentication page is displayed.



(6) The user is allowed to access the Internet after the correct username and password are entered.



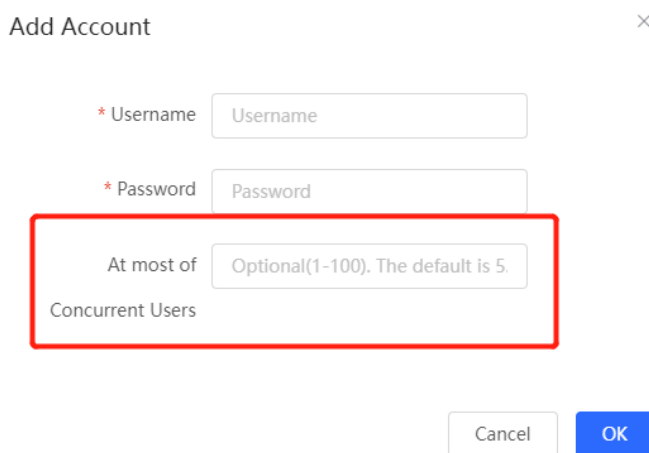
Caution

Up to five authentication IP addresses or ranges can be added for local account authentication.

11.3 How Many Users Are Supported for One Account?

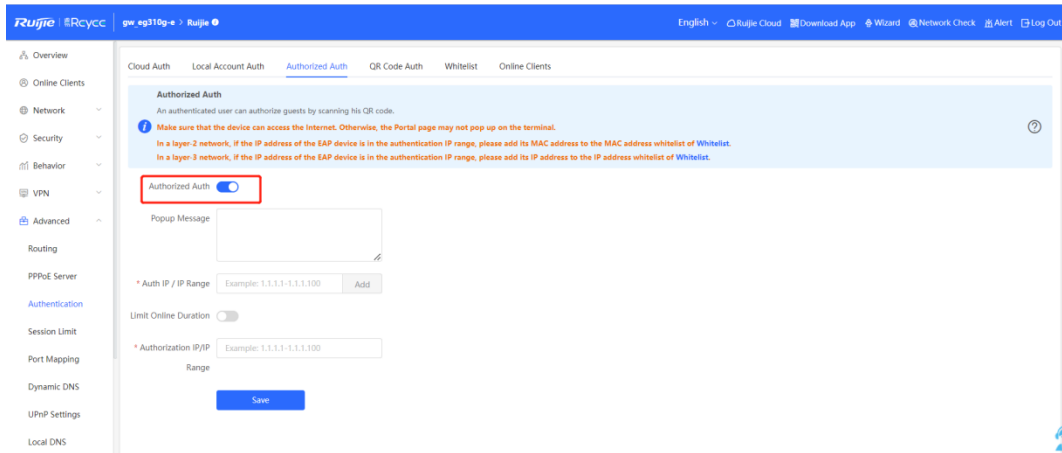
Set **Maximum Clients** to limit the number of clients supported by each account. The value ranges from 1 to 100. The default value is 5.

For example, if the value is set to 6, the account supports up to six clients. If the seventh user logs in on this account, the first user will be removed from the user list.

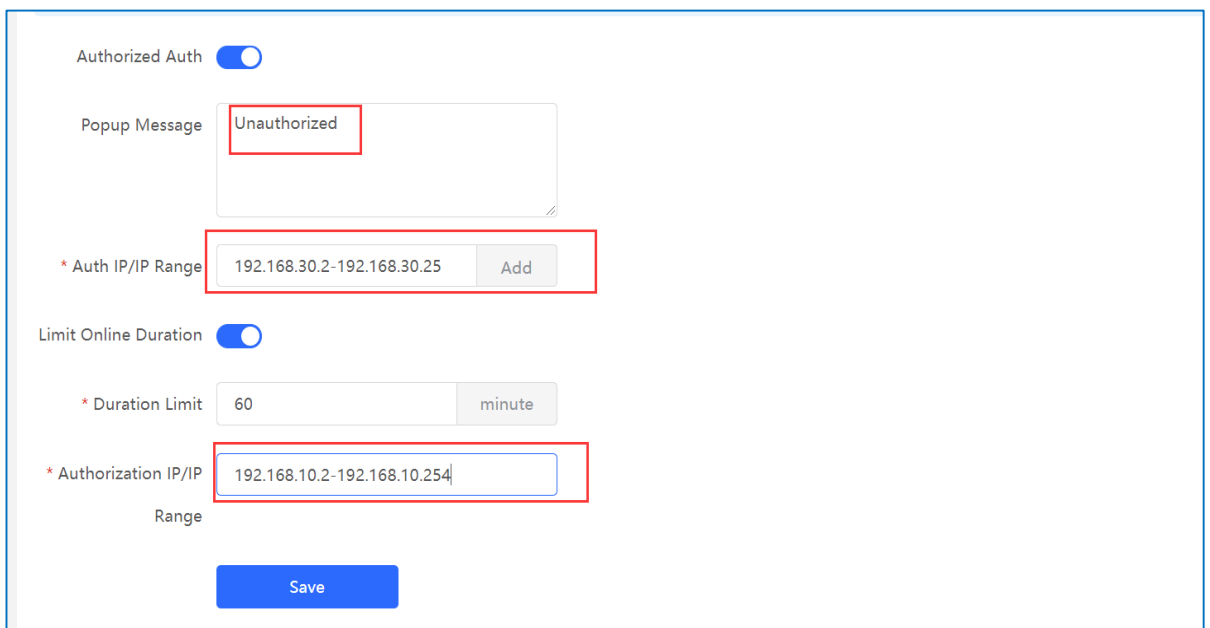


11.4 How Is Authorized Authentication Configured on a Reyee Router?

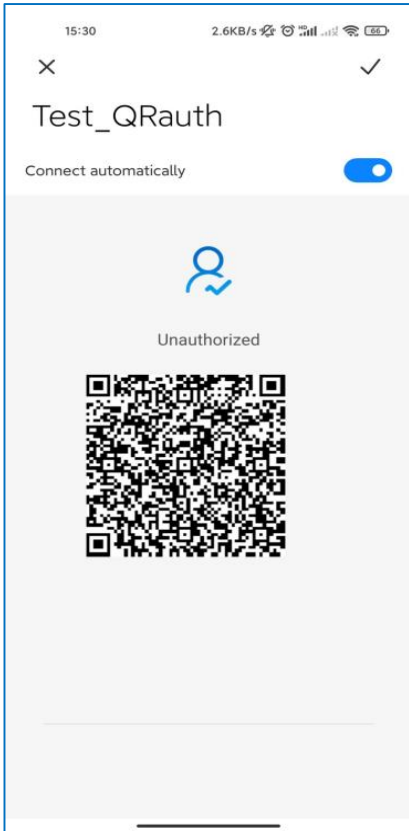
- (1) Choose **Advanced > Authentication > Authorized Auth**.
- (2) Enable **Authorized Auth** on the web page of the Reyee router.



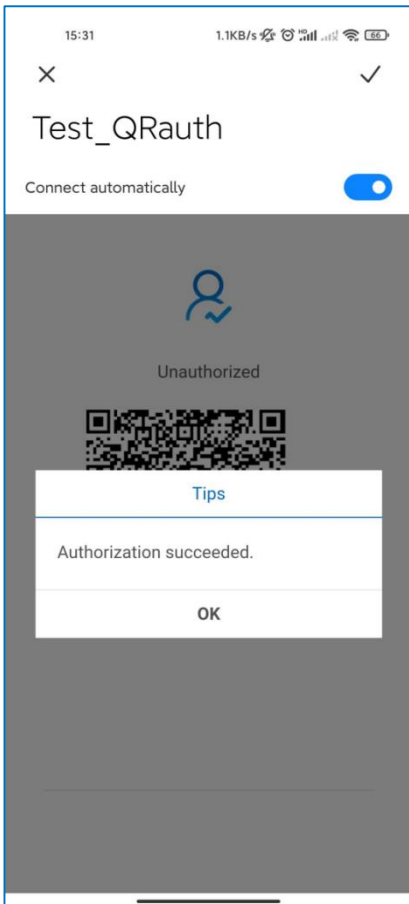
(3) Enter the IP address or IP address range of authorized authentication. A message is displayed.



(4) When the client with the specified authentication IP address or in the authentication IP range tries to access the Internet, the QR code authentication page is displayed.



- (5) The user is allowed to access the Internet after the terminal with the authorized IP address or local account scans the QR code.



Caution

If an IP address is specified in **Local Account Auth**, the user can still perform authorization even though the IP address is excluded from the authentication IP address range.

11.5 Why Authorized Authentication Does Not Take Effect?

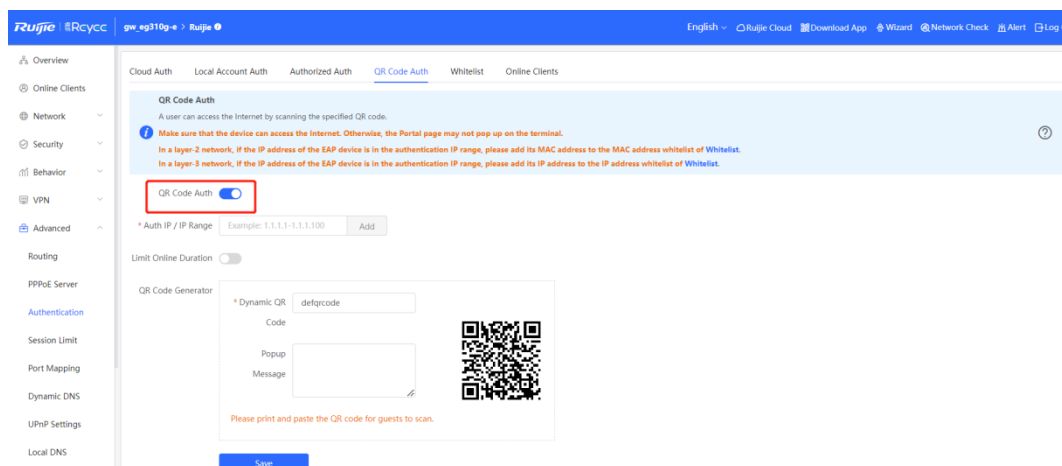
- (1) Check whether the IP address of the authorized user is included in the range of **Authorization IP / IP range** or the authorized user is a local account user. If not, the user is not authorized.
- (2) Check whether the IP address is included in the range of **Auth IP/IP Range**. If not, the user is not authorized.
- (3) Check whether the IP address is added to the whitelist. The IP address in the whitelist is not authenticated.

Caution

If an IP address is specified in **Local Account Auth**, the user can still perform authorization even though the IP address is excluded from the authentication IP address range.

11.6 How Is QR Code Authentication Configured on a Reye Router?

- (1) Choose **Advanced > Authentication > QR Code Auth**.
- (2) Enable **QR Code Auth** on the web page of the Reye router.



- (3) Enter the IP address or IP address range of authorization, duration limit for users, and popup message.

QR Code Auth

* Auth IP / IP Range

Limit Online Duration

QR Code Generator

* Dynamic QR

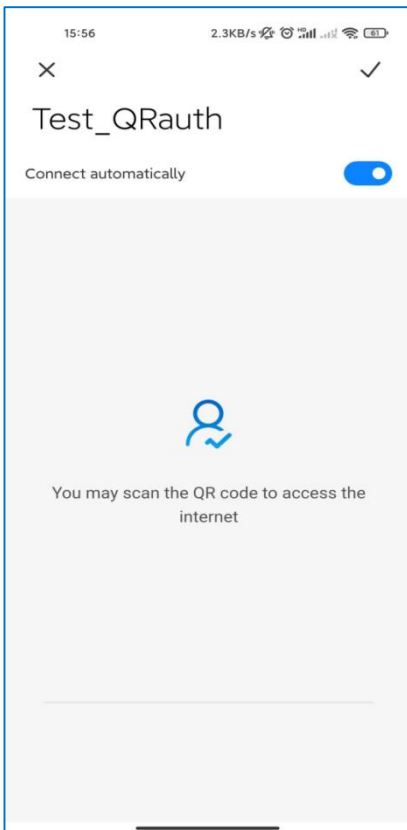
Code

Popup Message

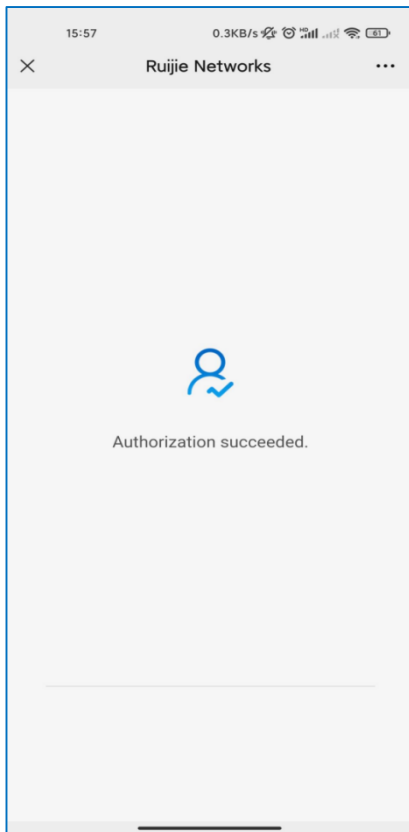



Please print and paste the QR code for guests to scan.

(4) When the client with the specified authentication IP address or in the authentication IP address range tries to access the Internet, the QR code authentication page is displayed.



(5) The user is allowed to access the Internet after the correct QR code is scanned.



 Caution

The QR code needs to be updated if the dynamic QR code has changed.

11.7 What Should I Do If QR Code Authentication Does Not Take Effect?

- (1) Check whether the IP address is included in the range of **Authorization IP / IP Range**. If not, QR code authentication does not take effect.
- (2) Check whether the QR code you scan is correct or the latest. The QR code needs to be updated if the dynamic QR code has changed.

12 FAQs About IPTV

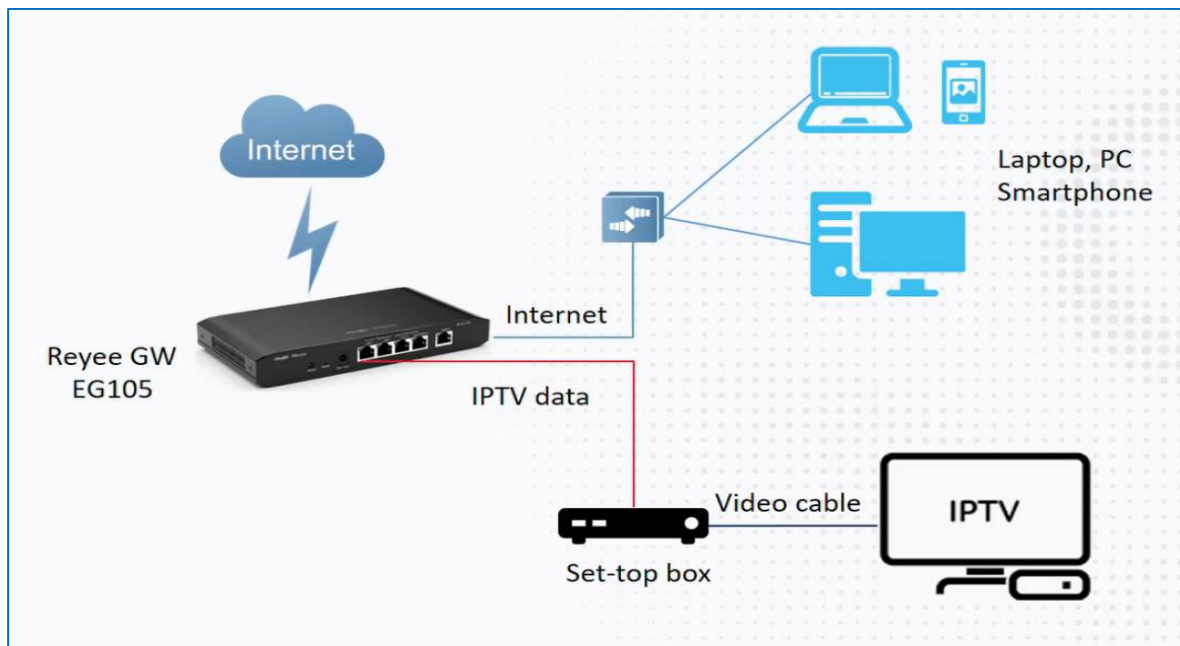
12.1 How Can I Configure IPTV on a Reyee EG Router?

The IPTV service applies to the following two scenarios.

The Reyee EG router supports IPTV functions. There are two scenarios based on network cables.

Scenario 1: Dual-WAN scenario

Two network cables are used to carry IPTV and network flows, respectively.



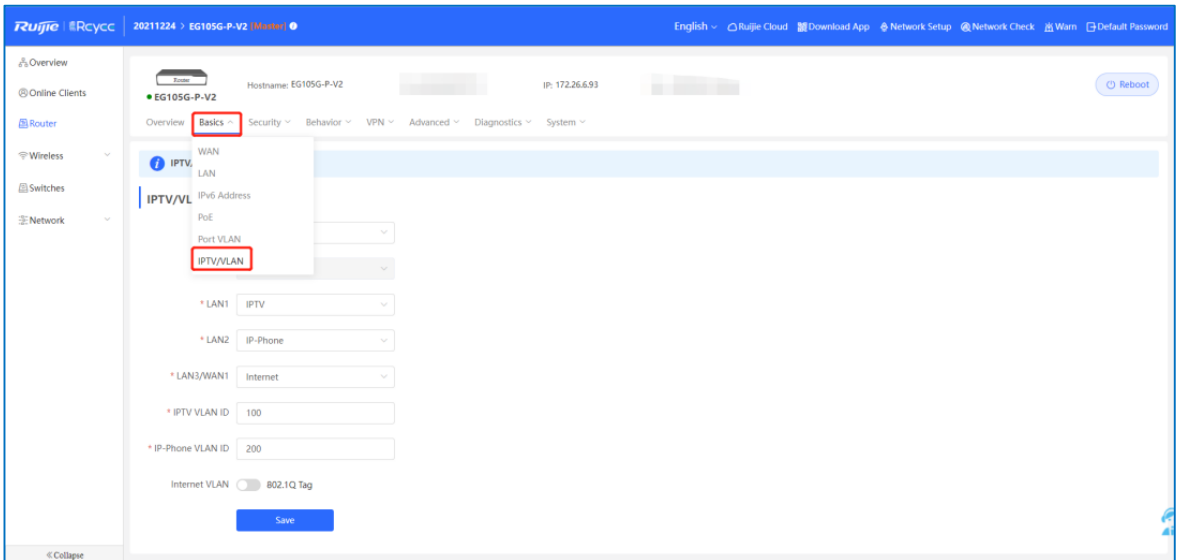
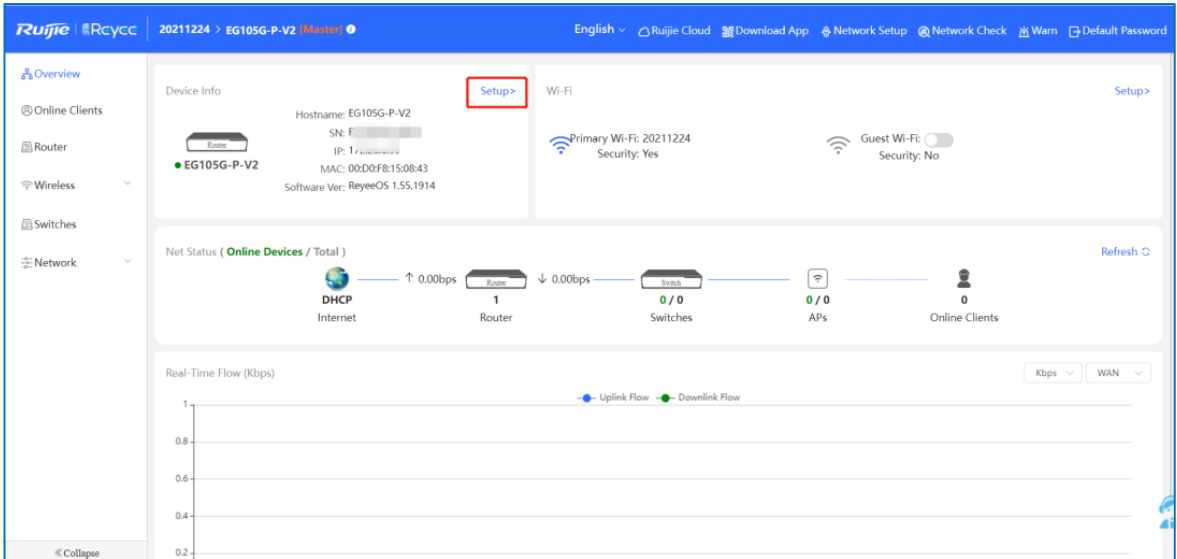
Scenario 2: Single-WAN scenario

A network cable carries both IPTV and network flows.



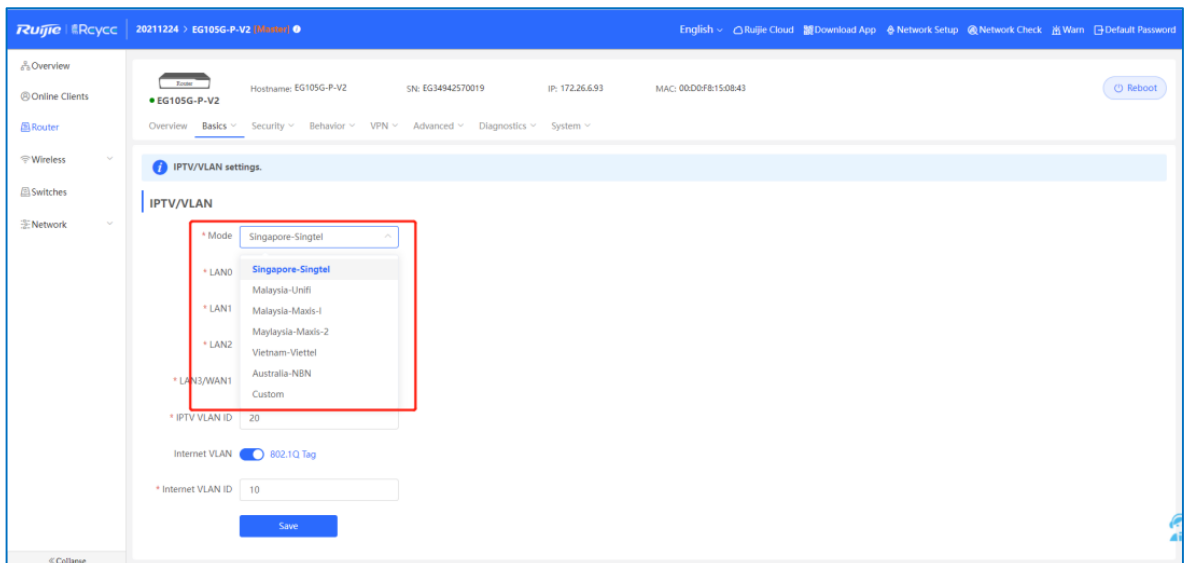
Perform the following steps to configure IPTV.

- (1) Connect the ISP cable to 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 router and use the EG router to access the Internet according to the wizard.
- (2) Choose **Network > IPTV**.

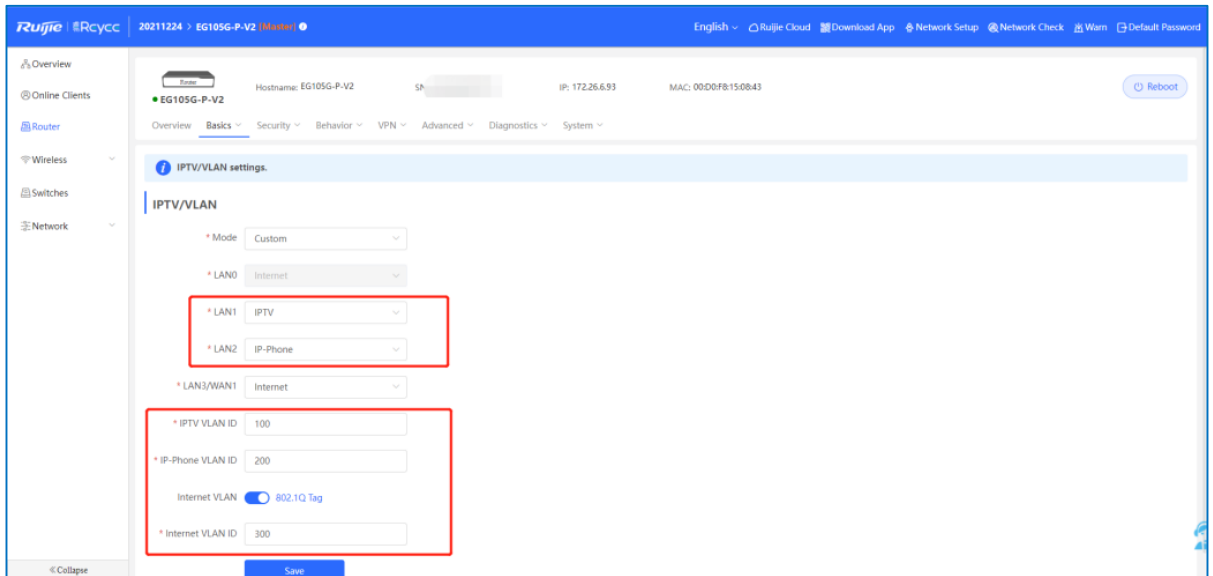


(3) Configure the VLAN ID for the IPTV device or IP phone.

- If you are in any of the following regions in red box, you can select the mode directly.

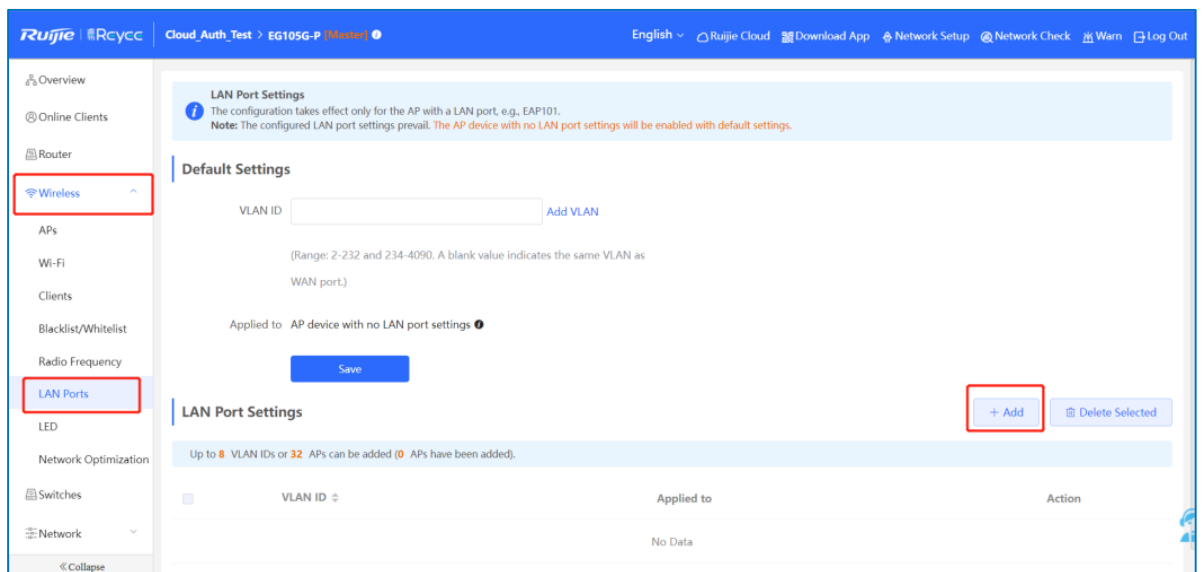


- If you are not in any of these regions, select **Custom**, contact with the ISP for the IPTV settings, and connect the IPTV device and IP phone with LAN ports. For example, the VLAN IDs for the IPTV device, IP phone, and Internet are 100, 200, and 300, respectively.

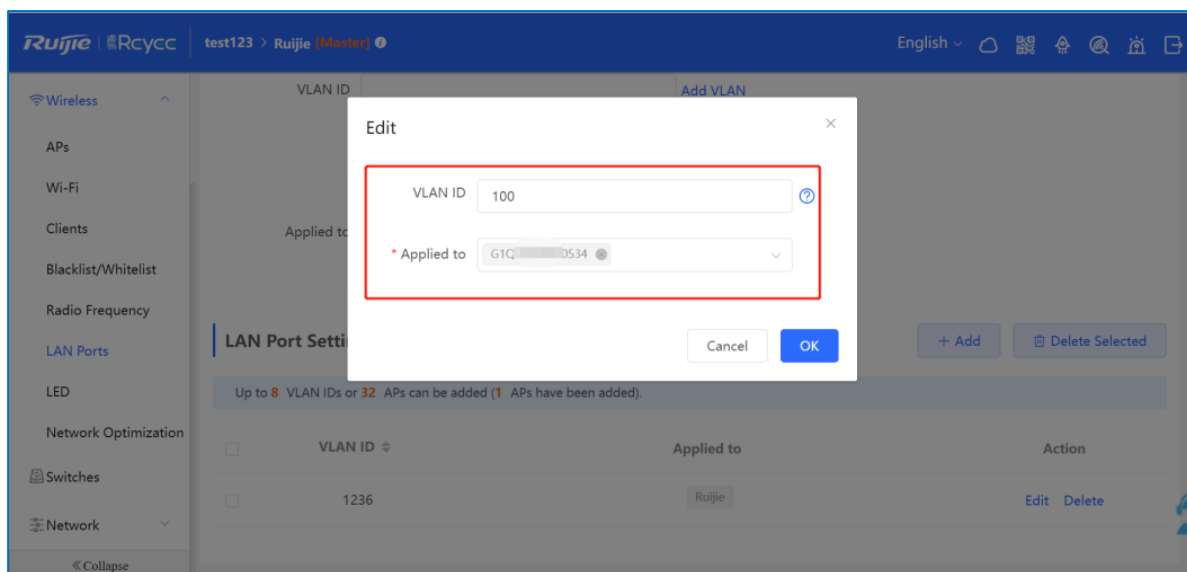


- (4) In scenario 2, after IPTV configuration is performed on a Reyeeg EG router, configure VLAN ID 100 for the IPTV device on a VLAN port of a wall AP. In scenario 1, ignore this step.

- a Choose **Wireless > LAN Ports > Add**.



- b Set the VLAN ID to 100 and apply it to the wall AP.



⚠ Caution

Firmware EG_3.0(1)B11P55 or later can support IPTV.

12.2 What Can I Do If the IPTV Device Does Not Work After the IPTV Device Is Connected to the Reyeeg EG Router?

- (1) Check whether the IPTV device restarts properly.
- (2) Check whether settings are correct according to [12.1 How Can I Configure IPTV on a Reyeeg EG Router?](#)
- (3) Contact the ISP to check whether there are any errors for the IPTV function.
- (4) If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

12.3 What Can I Do If the IPTV Service Is Frozen Frequently After the IPTV Device Is Connected to the Reyeeg EG Router?

- (1) Check whether the IPTV device works properly and restart it.
- (2) Contact the ISP to check whether there are any errors for the IPTV function.
- (3) Restart the Reyeeg EG router.
- (4) If the fault persists, start a live chat with Ruijie technical support: [Ruijie Support](#).

13 FAQs About the Mesh Function

13.1 Can Wired Mesh Switch to Wireless Mesh?

Yes, after a wired mesh connection has been established successfully, the wired mesh mode will automatically switch to the wireless mesh mode if you disconnect the network cable between routers.

13.2 The Master Device Has Been Powered Off, Will the Slave Device Automatically Connect to the Master Device When It Is Powered On Again?

When the master device is powered off, the slave device will detect the master device continuously. When the master device is powered on again, the slave device will detect it and connect to the master device once again.

13.3 What Should I Do If It Takes a Long Time for the Slave Device to Reconnect to the Master Device After the Master Device Has Restarted?

Check whether the wireless channel of the master device is one of the following: CH52, CH56, CH60, CH64, CH100, CH104, CH108, CH112, CH116, CH120, CH124, CH128, CH132, CH136, and CH140I. If so, try to change the wireless channel of the master device to another channel.

13.4 Why the SSID and Channel Cannot Be Changed on the Slave Device After a Mesh Network Is Set Up Successfully?

You cannot change the SSID and channel on the slave device, but can change them on the master device. When the master device's configuration changes, the slave device's configuration will change accordingly.

13.5 What Should I Do If a Mesh Network Fails to Be Set Up?

- (1) Check the distance between the two devices. When a mesh network is established for the first time, the slave device should be within two meters of the master device in an unobstructed environment.
- (2) When a slave device is moved to a location where Wi-Fi coverage is required, there is no more than one wall between the slave device and master device. If more than two walls exist between the two devices, the mesh network may fail to be established.

14 FAQs About Parameters of Reyee Routers

14.1 Where Can I Find All Parameters of Reyee Routers?

Refer to the link

<https://community.ruijienetworks.com/forum.php?mod=viewthread&tid=1820&page=1&extra=#pid2844>.

14.2 What Is the Maximum Number of Concurrent Clients on a Reyee Router?

Model	Maximum Number of Clients
RG-EG105G	100
RG-EG105G-P	100
RG-EG210G-P	200
RG-EG105GW	100 (recommended number of wireless terminals: 60)
RG-EG105G V2	100
RG-EG105G-P V2	100
RG-EG210G-E	200
RG-EG305GH-P-E	300
RG-EG310GH-E	300
RG-EG310GH-P-E	300
EG209GS	200
RG-EG105GW(T)	100
RG-EG105GW-X	150

14.3 How Many Devices Can a Router Manage in AC or Gateway Mode?

Model	Management capacity	
	AC mode	Router mode
RG-EG105G	300	32
RG-EG105G-P	300	32

Model	Management capacity	
	AC mode	Router mode
RG-EG210G-P	500	150
RG-EG105GW	N/A	32
EG105G V2	300	32
EG105G-P V2	300	32
EG210G-E	500	150
RG-EG305GH-P-E	500	150
RG-EG310GH-E	500	150
RG-EG310GH-P-E	500	150
EG209GS	500	150
RG-EG105GW(T)	N/A	32
RG-EG105GW-X	N/A	64

14.4 What Is the Difference Between the AC Mode and Router Mode for a Reyee EG Router?

- The AC mode has a higher SON priority and capacity to manage devices than the router mode.
- The Reyee EG router in AC mode does not support most features and can be used to manage device only.