RG-OCE-Network Manager

User Guide

Document Version: V1.1
Date: July 02, 2025

Copyright

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

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

Warning

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

Caution

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

Note

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

Specification

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

3. Note

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

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

1 Product Introduction

1.1 RG OCE Network Manager (OCE-NM) Service Overview

The Ruijie OCE (Omni-Control Engine) is an easy and efficient on-premises network management solution for enterprise office, manufactory, K12 school, ISP and MSP to provide management features on local. The solutions include device deployment, monitoring, network optimization, and operational life cycle management; providing customers with plug-and-play deployment and operation and maintenance (O&M). It satisfies needs of automatic RF planning and user experience monitoring. Moreover, it supports flexible wireless Wi-Fi management, including secure Private Pre-Shared Key (PPSK) authentication (one person, one machine, and one password), and third-party devices monitoring.

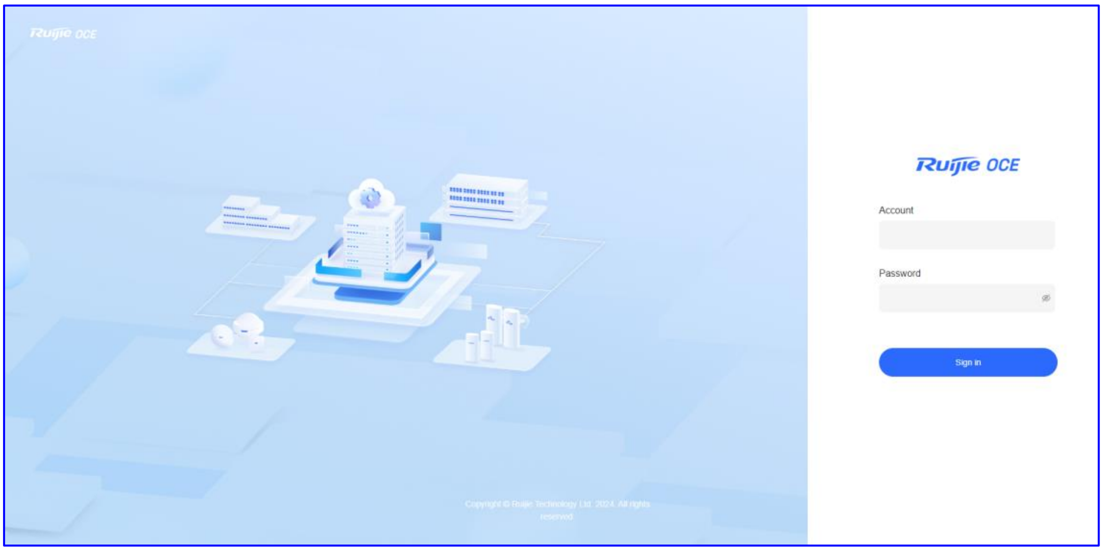
1.2 Key Features

- Centralized Management
  - RG OCE-NM can conduct configuration and management of all APs, switches, routers and gateway devices in one cloud management platform.
  - Auto-Configured Network and VLAN visualization help administrator deploy the wired and wireless network quickly and easily.
  - Support 3rd-party devices monitoring based on SNMP protocol.
- Network Monitoring
  - Rich data statistics, device / client status monitoring and network report
  - Network topology and real time user experience monitoring
- Multi-tenancy and Sub-account Management
  - Perfection for Managed Service Business, integrated with multi-accounts management feature.
  - Easy to create different role permissions for sub-account, including Admin, Employee and Guest Role.
- Zero-provisioning
  - With plug-n-play, RG OCE-NM allows administrator to provision new network devices in their existing network automatically without manual intervention.

2 Quick Start

2.1 How to Login RG OCE-NM

(1) Visit your customized domain for On-Premises service.


Ruijie OCE
Ruijie OCE
Account
Password
Sign in
Copyright © Ruijie Technology Ltd. 2024. All rights reserved

(2) Input the Admin account and Click **Sign in** to login directly.

2.2 Adding a Project

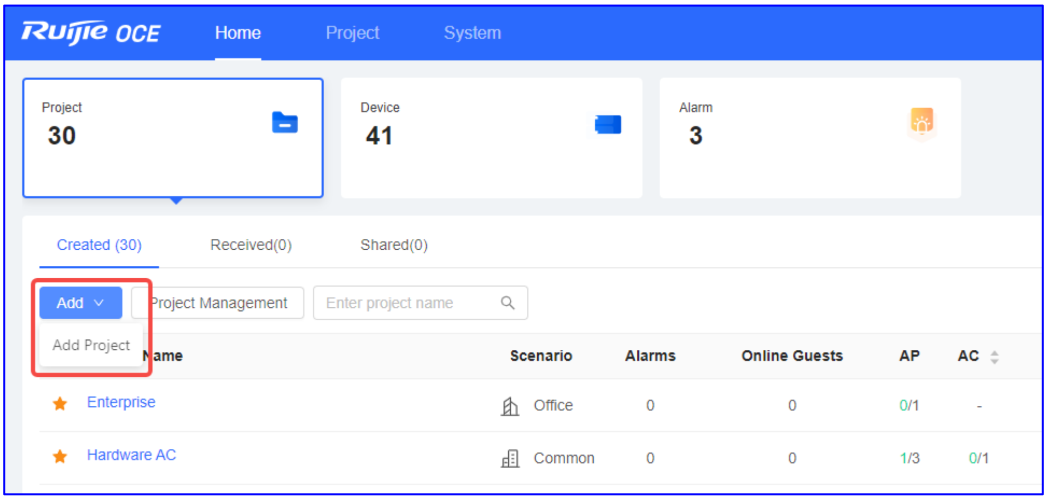
A project group includes many networks, and is usually used to represent the network of a province, a city, or a company.

Note

Adding devices to a project group is not supported. The project group is used to manage multiple projects.

Procedure

(1) Choose **Home** > **PROJECT**> **Add** > **Add Project**



Project 30

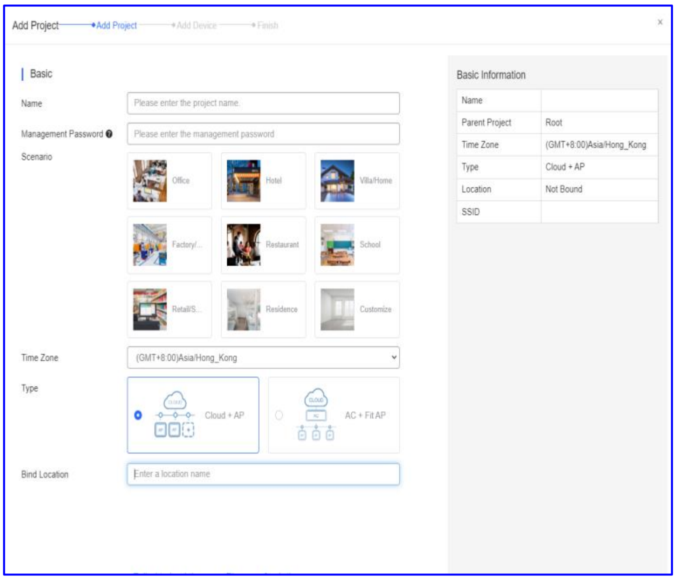
Device 41

Alarm 3

Created (30) Received(0) Shared(0)

	Name	Scenario	Alarms	Online Guests	AP	AC
★	Enterprise	Office	0	0	0/1	-
★	Hardware AC	Common	0	0	1/3	0/1

(2) Set basic parameters of the project. Then click **Next**.



Basic

Name: Please enter the project name.

Management Password: Please enter the management password

Scenario

Time Zone: (GMT+8:00)Asia/Hong_Kong

Type: ● Cloud + AP ○ AC + Fit AP

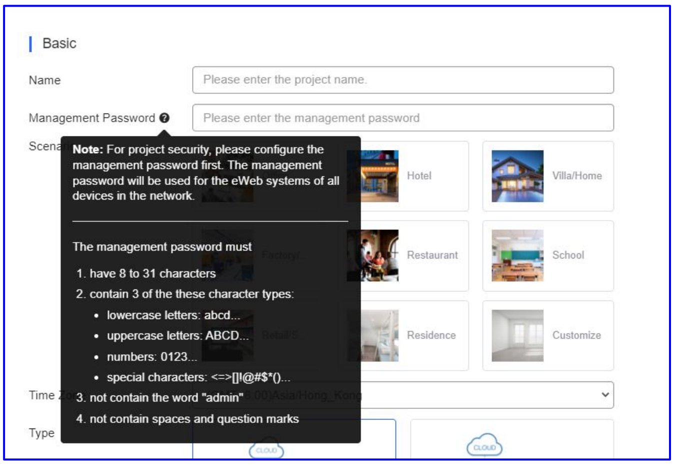
Bind Location: Enter a location name

Basic Information

Name	
Parent Project	Root
Time Zone	(GMT+8:00)Asia/Hong_Kong
Type	Cloud + AP
Location	Not Bound
SSID	

Name: indicates the name of a project. The value is a string of up to 32 characters, including letters, numerals, or underscores (_).

Management Password: indicates the management password.



Basic

Name: Please enter the project name.

Management Password: Please enter the management password

Note: For project security, please configure the management password first. The management password will be used for the eWeb systems of all devices in the network.

The management password must

1. have 8 to 31 characters
2. contain 3 of the these character types:
   - lowercase letters: abcd...
   - uppercase letters: ABCD...
   - numbers: 0123...
   - special characters: <=>[]!@#$*()...
3. not contain the word "admin"
4. not contain spaces and question marks

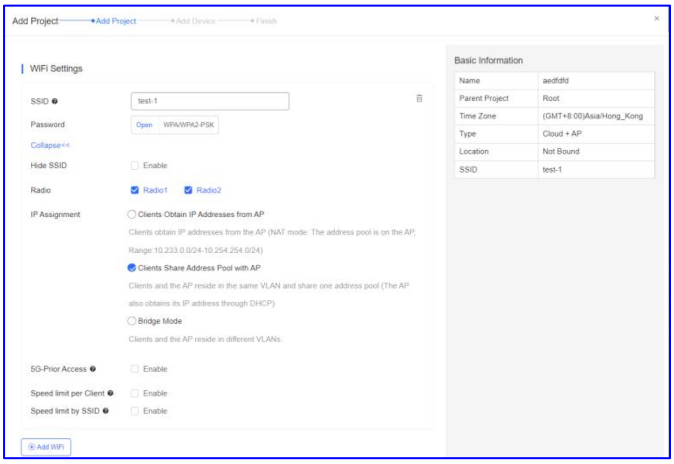
Scenario: indicates the scenario that suits the customer's actual scenario.

Time Zone: indicates the time zone where the current customer is located.

Type: indicates the type of the project. If there is an AC in the project, select **AC + Fit AP**.

Bind Location: indicates the location of the project.

(3) Set Wi-Fi parameters. Then click **Save & Next**.



WiFi Settings

SSID: test-1

Password: Open | WPA/WPA2-PSK

Hide SSID: □ Enable

Radio: ☑ Radio1 ☑ Radio2

IP Assignment:
○ Clients Obtain IP Addresses from AP
Clients obtain IP addresses from the AP (NAT mode: The address pool is on the AP, Range:10.233.0.0/24-10.254.254.0/24)
● Clients Share Address Pool with AP
Clients and the AP reside in the same VLAN and share one address pool (The AP also obtains its IP address through DHCP)
○ Bridge Mode
Clients and the AP reside in different VLANs.

5G-Prior Access: □ Enable

Speed limit per Client: □ Enable

Speed limit by SSID: □ Enable

Basic Information

Name	aedfdfd
Parent Project	Root
Time Zone	(GMT+8:00)Asia/Hong_Kong
Type	Cloud + AP
Location	Not Bound
SSID	test-1

SSID: indicates the WLAN name of a project.

Password: indicates the SSID encryption method and password.

Hide SSID: indicates that the SSID is hidden or broadcast.

Radio: indicates the radio that needs to be enabled.

IP Assignment: indicates the mode in which clients obtain IP addresses.

5G-prior Access: indicates that clients are connected to the 5 GHz frequency band preferentially. Legacy clients are connected to2.4 GHz frequency band.

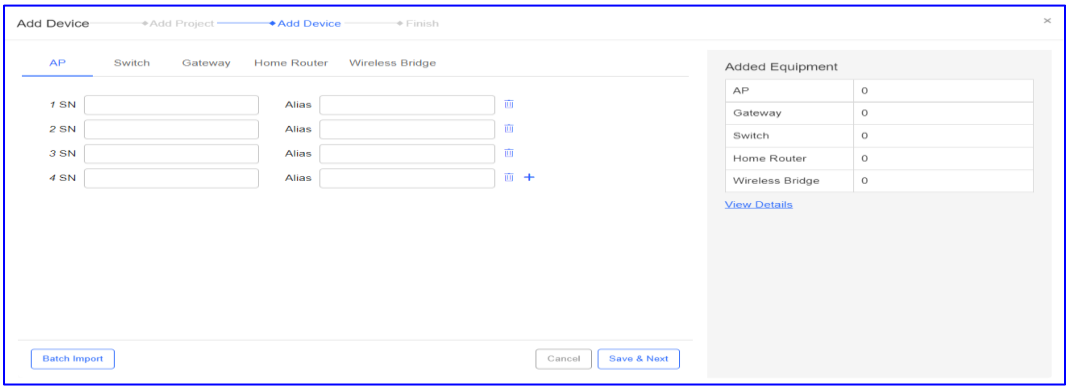
Speed limit per Client: indicates channel width control for each user who connects to this Wi-Fi.

Speed limit by SSID: indicates channel width control for the total traffic on this SSID.

(4) Add devices manually or through batch import.

- Option 1: Add devices manually.

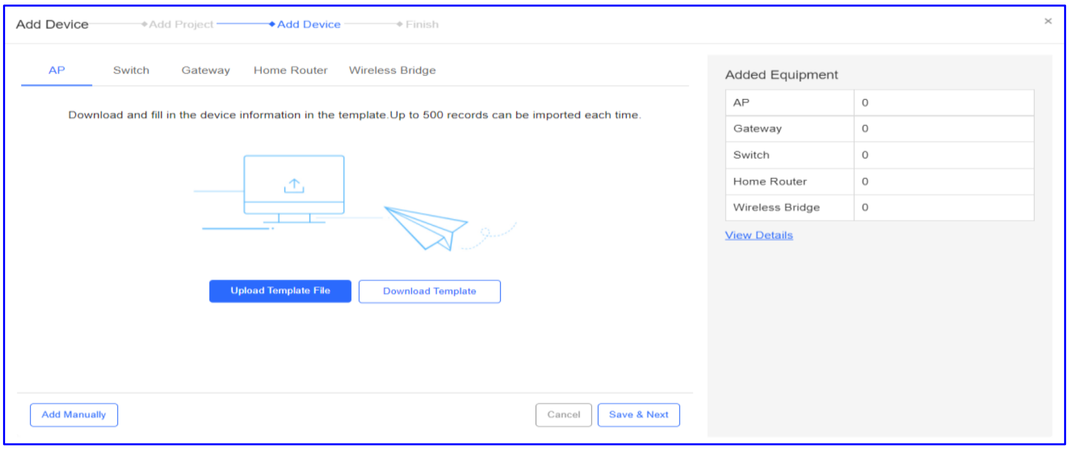
Enter the device SN and alias.



Added Equipment

AP	0
Gateway	0
Switch	0
Home Router	0
Wireless Bridge	0

- Option 2: Add devices through batch import. In the template, up to 500 records can be imported each time.



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

Added Equipment

AP	0
Gateway	0
Switch	0
Home Router	0
Wireless Bridge	0

a Click **Batch Import**.

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

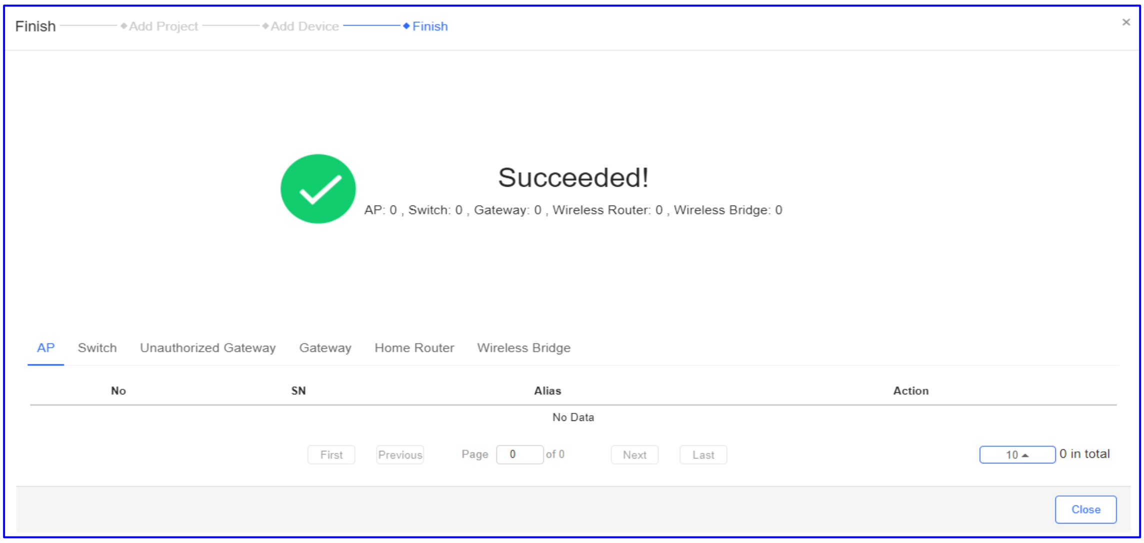
c Fill in the device SN and alias in the template and save it.

d Click **Upload Template File** to upload the edited template file.

e Click the **Import** button.

(5) After devices are added, click **Save & Next**.

The project is added successfully.



Succeeded!

AP: 0 , Switch: 0 , Gateway: 0 , Wireless Router: 0 , Wireless Bridge: 0

No	SN	Alias	Action
		No Data	

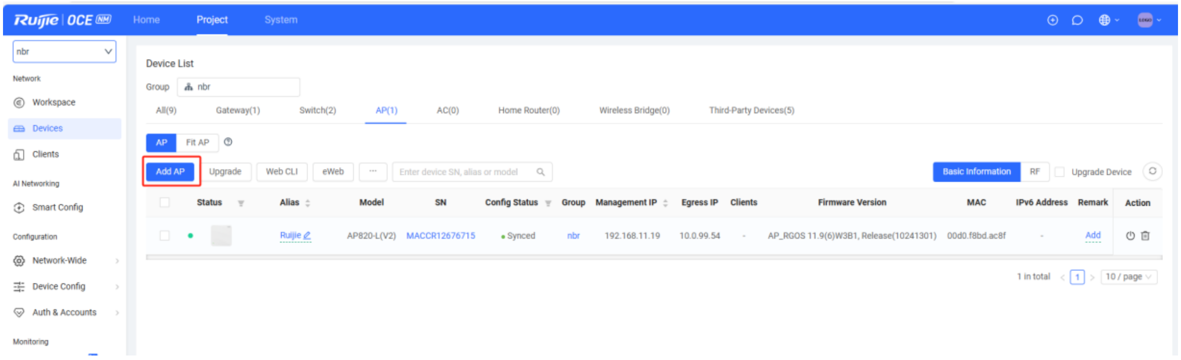
2.3 Adding a Device

2.3.1 Adding Ruijie Devices

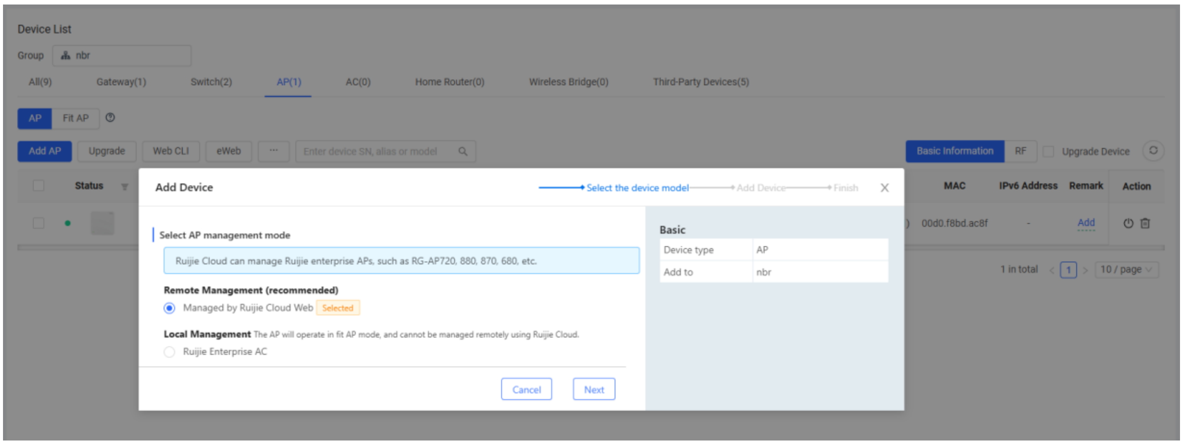
1. Method 1 (Recommended)

Public cloud redirection to OCE (requires both the device and the OCE server to have internet access).

On the **Device List** page, click the device type tab, and add the corresponding device, such as a wireless AP.



	Status	Alias	Model	SN	Config Status	Group	Management IP	Egress IP	Clients	Firmware Version	MAC	IPv6 Address	Remark	Action
□	●	Ruijie	AP820-L(V2)	MACCR12676715	● Synced	nbr	192.168.11.19	10.0.99.54	-	AP_RGOS 11.9(6)W3B1, Release(10241301)	00d0.f8bd.ac8f	-	Add	



Add Device

Select AP management mode

Ruijie Cloud can manage Ruijie enterprise APs, such as RG-AP720, 880, 870, 680, etc.

Remote Management (recommended)

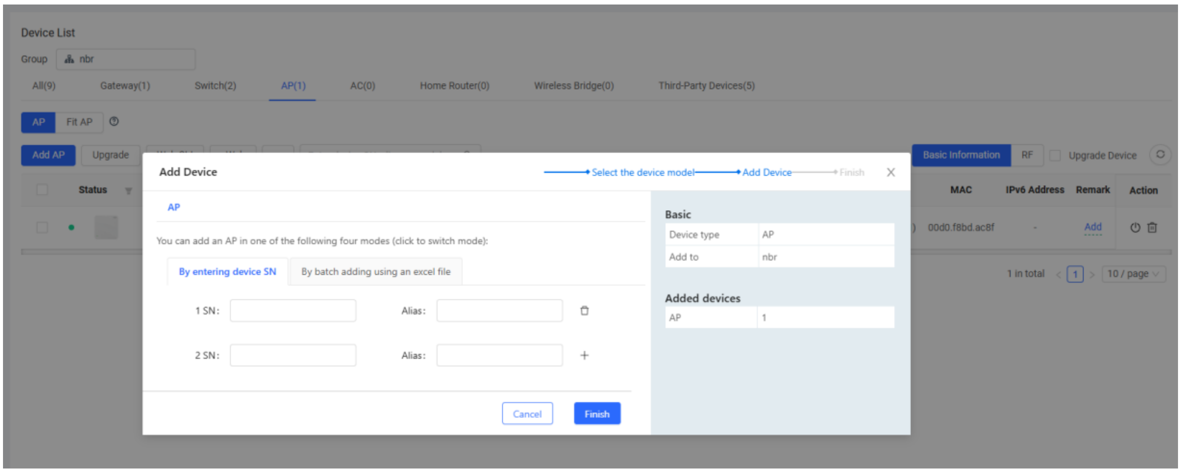
● Managed by Ruijie Cloud Web Selected

Local Management The AP will operate in fit AP mode, and cannot be managed remotely using Ruijie Cloud.

○ Ruijie Enterprise AC

Basic

Device type	AP
Add to	nbr



Add Device

AP

You can add an AP in one of the following four modes (click to switch mode):

By entering device SN | By batch adding using an excel file

1 SN: Alias:

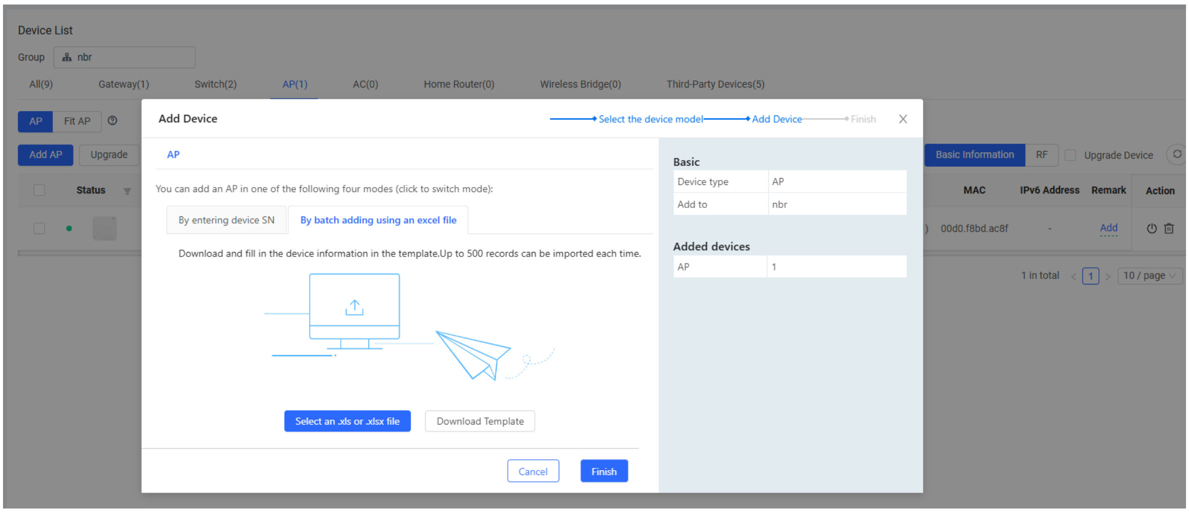
2 SN: Alias:

Basic

Device type	AP
Add to	nbr

Added devices

AP	1



Add Device

AP

You can add an AP in one of the following four modes (click to switch mode):

By entering device SN | By batch adding using an excel file

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

Basic

Device type	AP
Add to	nbr

Added devices

AP	1

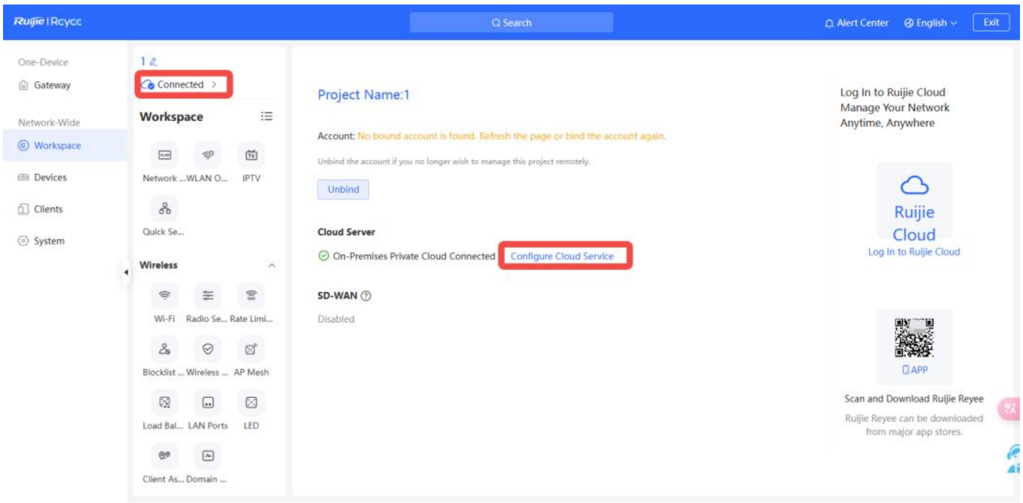
You can add devices by entering the device SN or by batch importing devices.

2. Method 2

Change cloud address on Device eWeb or CLI.

- eWeb example

1. Choose ☁ **Connected** > **Configure Cloud Service**.



Project Name:1

Account: No bound account is found. Refresh the page or bind the account again.

Unbind the account if you no longer wish to manage this project remotely.

Cloud Server

On-Premises Private Cloud Connected

SD-WAN

Disabled

Log In to Ruijie Cloud Manage Your Network Anytime, Anywhere

Scan and Download Ruijie Reyee

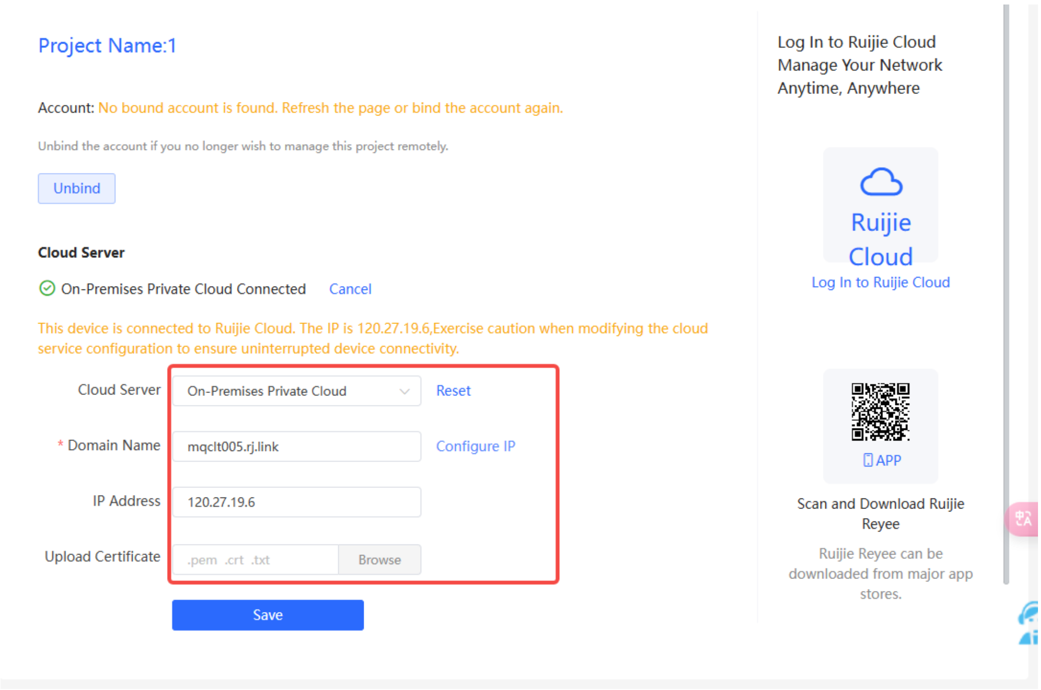
Ruijie Reyee can be downloaded from major app stores.

2. Select **On-Premises Private Cloud** from the drop-down list in the **Cloud Server** field.

Enter a domain name for the OCE Network Manager in the **Domain Name** field.

(Optional) Set an IP address for the OCE Network Manager. You are not advised to set an IP address, as the IP address may change.

(Optional) Upload the certificate. The certificate file needs to be exported from the OCE Network Manager.



Project Name:1

Account: No bound account is found. Refresh the page or bind the account again.

Unbind the account if you no longer wish to manage this project remotely.

Cloud Server

On-Premises Private Cloud Connected

This device is connected to Ruijie Cloud. The IP is 120.27.19.6,Exercise caution when modifying the cloud service configuration to ensure uninterrupted device connectivity.

Cloud Server: On-Premises Private Cloud

* Domain Name: mqclt005.rj.link

IP Address: 120.27.19.6

Upload Certificate: .pem .crt .txt

Log In to Ruijie Cloud Manage Your Network Anytime, Anywhere

Scan and Download Ruijie Reyee

Ruijie Reyee can be downloaded from major app stores.

- CLI example

```
ruijie(config)#cwmp
ruijie(config-cwmp)#acs url http://xxx.oce.domain/service/acs
ruijie(config-cwmp)#cpe inform interval 30
ruijie(config-cwmp)#exit
ruijie(config-cwmp)#save
```

3. FAQs

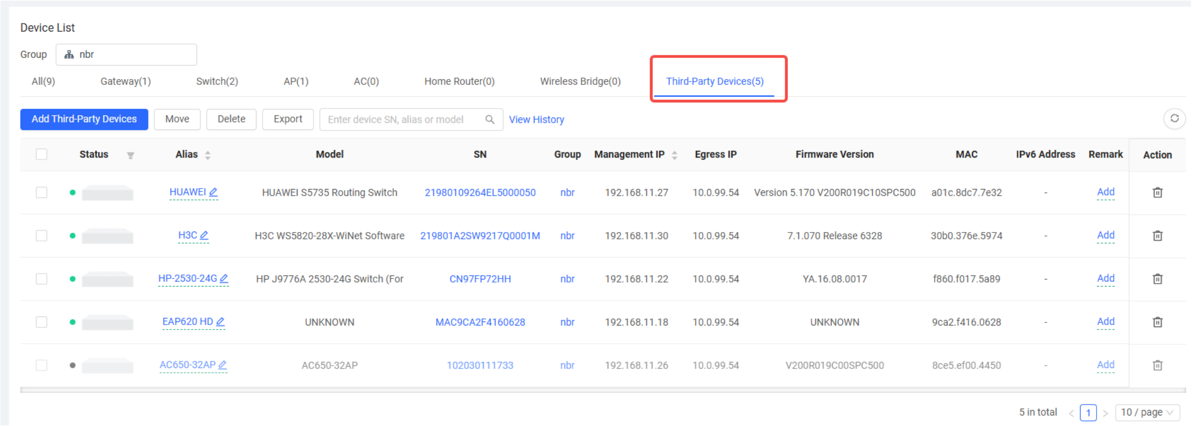
Q: Why is the domain name mapping not taking effect after modification?

A: Check whether an IP address is configured for the cloud server. Remove the IP address and test again.

2.3.2 Adding Third-Party Devices

You can scan and add devices on the LAN using the SNMP v2/v3 protocol. Third-party devices should have SNMP enabled and be configured with the same community name as the OCE server.

To add third-party devices, switch to the **Third-Party Devices** tab and click **Add Third-Party Devices**.



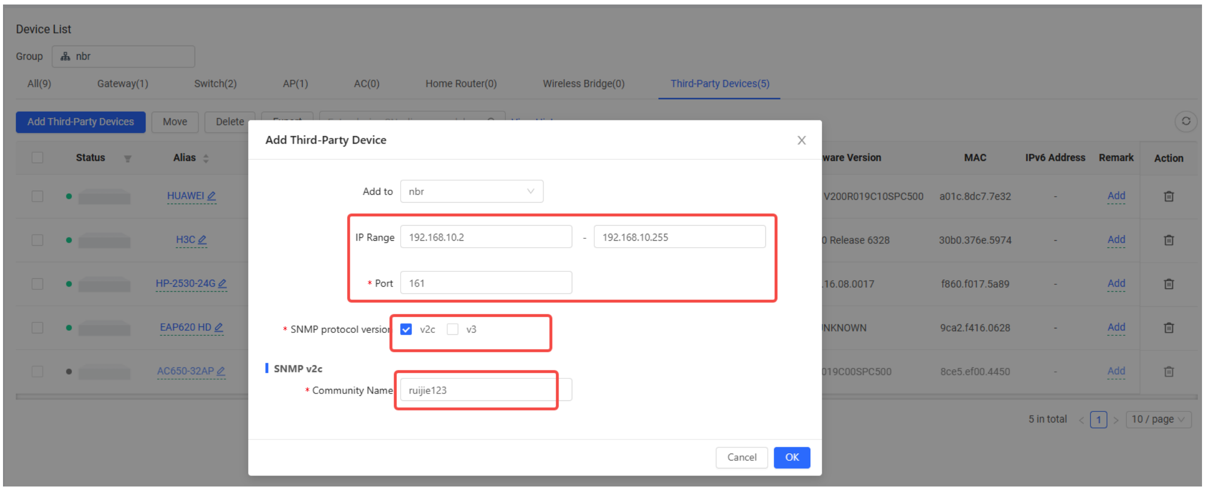
Device List

Group: nbr

All(9) | Gateway(1) | Switch(2) | AP(1) | AC(0) | Home Router(0) | Wireless Bridge(0) | Third-Party Devices(5)

□	Status	Alias	Model	SN	Group	Management IP	Egress IP	Firmware Version	MAC	IPv6 Address	Remark	Action
□	●	HUAWEI	HUAWEI S5735 Routing Switch	21980109264EL5000050	nbr	192.168.11.27	10.0.99.54	Version 5.170 V200R019C10SPC500	a01c.8dc7.7e32	-	Add	🗑
□	●	H3C	H3C WS5820-28X-WiNet Software	219801A2SW9217Q0001M	nbr	192.168.11.30	10.0.99.54	7.1.070 Release 6328	30b0.376e.5974	-	Add	🗑
□	●	HP-2530-24G	HP J9776A 2530-24G Switch (For	CN97FP72HH	nbr	192.168.11.22	10.0.99.54	YA.16.08.0017	f860.f017.5a89	-	Add	🗑
□	●	EAP620 HD	UNKNOWN	MAC9CA2F4160628	nbr	192.168.11.18	10.0.99.54	UNKNOWN	9ca2.f416.0628	-	Add	🗑
□	●	AC650-32AP	AC650-32AP	102030111733	nbr	192.168.11.26	10.0.99.54	V200R019C00SPC500	8ce5.ef00.4450	-	Add	🗑

5 in total < 1 > 10 / page



Add Third-Party Device

Add to: nbr

IP Range: 192.168.10.2 - 192.168.10.255

* Port: 161

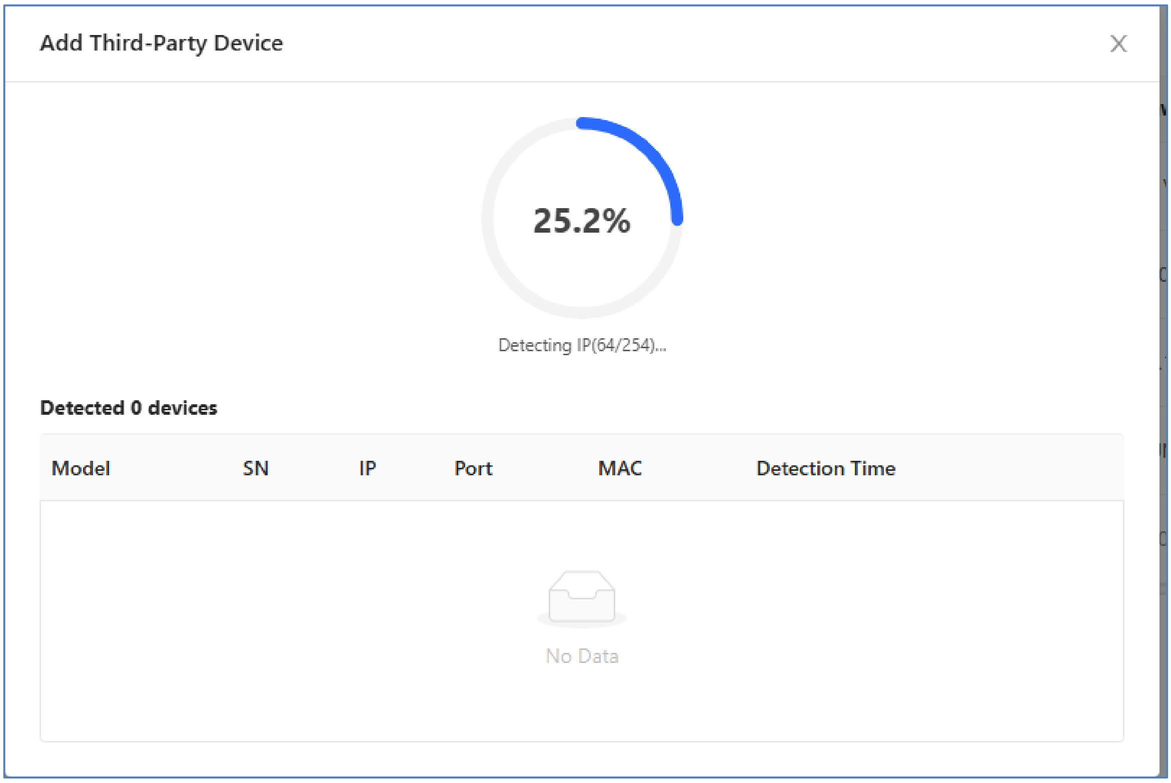
* SNMP protocol version: ☑ v2c □ v3

SNMP v2c

* Community Name: ruijie123

IP Range: Indicates the IP range where the device is located.
Port: Indicates the SNMP port. The default value is 161.
SNMP protocol version: Indicates the SNMP protocol version. SNMP v2 and SNMP v3 are supported.
Community Name: Indicates the SNMP community name.

Click **OK**. The RG-OCE will scan the devices on this network. Any new devices discovered will be automatically added to the device list.



Add Third-Party Device

25.2%

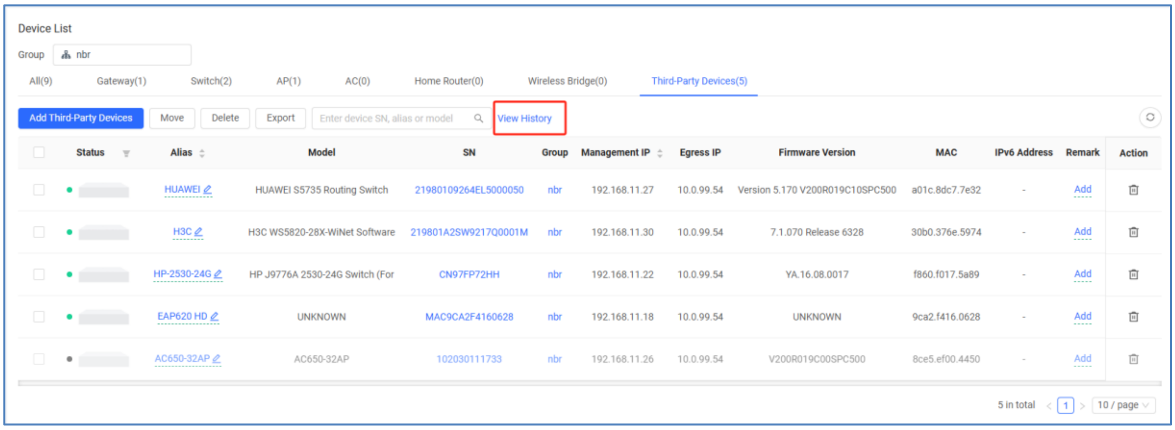
Detecting IP(64/254)...

Detected 0 devices

Model	SN	IP	Port	MAC	Detection Time

No Data

Click **View History** to view device discovery history and device details.



Device List

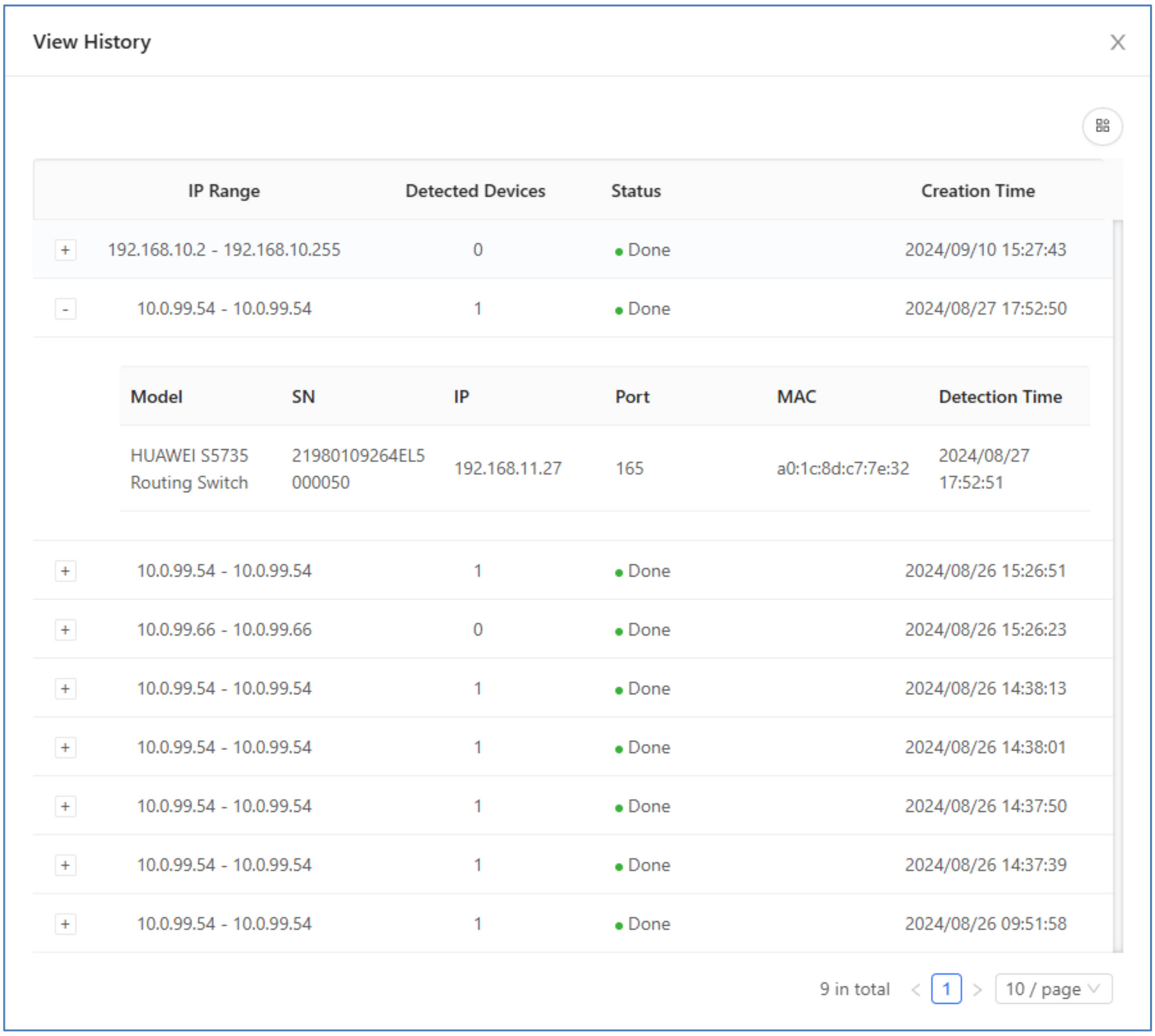
Group: nbr

All(9) Gateway(1) Switch(2) AP(1) AC(0) Home Router(0) Wireless Bridge(0) Third-Party Devices(5)

Add Third-Party Devices | Move | Delete | Export | Enter device SN, alias or model | View History

□	Status	Alias	Model	SN	Group	Management IP	Egress IP	Firmware Version	MAC	IPv6 Address	Remark	Action
□	●	HUAWEI	HUAWEI S5735 Routing Switch	21980109264EL5000050	nbr	192.168.11.27	10.0.99.54	Version 5.170 V200R019C10SPC500	a01c.8dc7.7e32	-	Add	🗑
□	●	H3C	H3C WS5820-28X-WiNet Software	219801A2SW9217Q0001M	nbr	192.168.11.30	10.0.99.54	7.1.070 Release 6328	30b0.376e.5974	-	Add	🗑
□	●	HP-2530-24G	HP J9776A 2530-24G Switch (For	CN97FP72HH	nbr	192.168.11.22	10.0.99.54	YA.16.08.0017	f860.f017.5a89	-	Add	🗑
□	●	EAP620 HD	UNKNOWN	MAC9CA2F4160628	nbr	192.168.11.18	10.0.99.54	UNKNOWN	9ca2.f416.0628	-	Add	🗑
□	●	AC650-32AP	AC650-32AP	102030111733	nbr	192.168.11.26	10.0.99.54	V200R019C00SPC500	8ce5.ef00.4450	-	Add	🗑

5 in total < 1 > 10 / page



View History

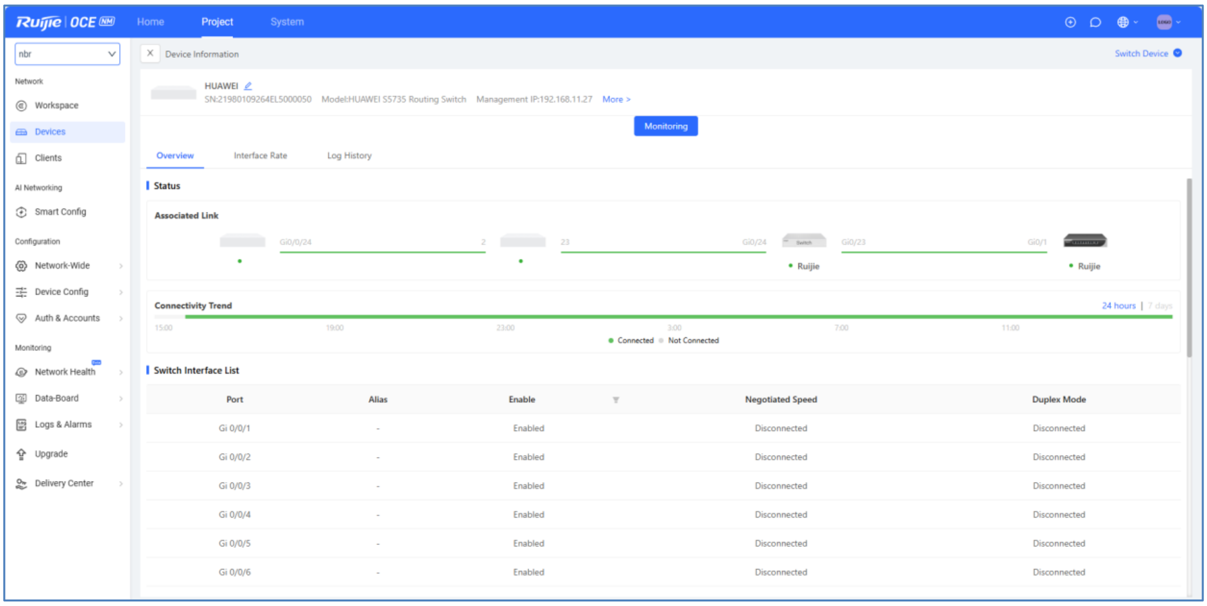
	IP Range	Detected Devices	Status	Creation Time
+	192.168.10.2 - 192.168.10.255	0	● Done	2024/09/10 15:27:43
-	10.0.99.54 - 10.0.99.54	1	● Done	2024/08/27 17:52:50

Model	SN	IP	Port	MAC	Detection Time
HUAWEI S5735 Routing Switch	21980109264EL5000050	192.168.11.27	165	a0:1c:8d:c7:7e:32	2024/08/27 17:52:51

	IP Range	Detected Devices	Status	Creation Time
+	10.0.99.54 - 10.0.99.54	1	● Done	2024/08/26 15:26:51
+	10.0.99.66 - 10.0.99.66	0	● Done	2024/08/26 15:26:23
+	10.0.99.54 - 10.0.99.54	1	● Done	2024/08/26 14:38:13
+	10.0.99.54 - 10.0.99.54	1	● Done	2024/08/26 14:38:01
+	10.0.99.54 - 10.0.99.54	1	● Done	2024/08/26 14:37:50
+	10.0.99.54 - 10.0.99.54	1	● Done	2024/08/26 14:37:39
+	10.0.99.54 - 10.0.99.54	1	● Done	2024/08/26 09:51:58

9 in total < 1 > 10 / page

After a third-party device is successfully added, you can view its details, including the interface list and status.



Device Information

HUAWEI

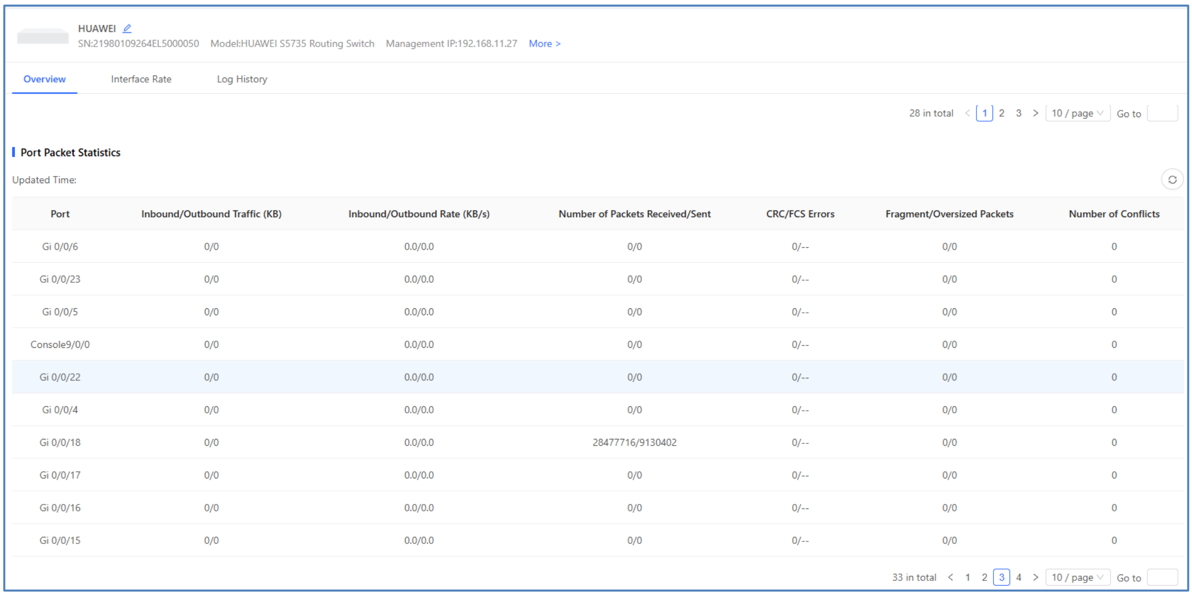
SN:21980109264EL5000050 Model:HUAWEI S5735 Routing Switch Management IP:192.168.11.27 More >

Status

Switch Interface List

Port	Alias	Enable	Negotiated Speed	Duplex Mode
Gi 0/0/1	-	Enabled	Disconnected	Disconnected
Gi 0/0/2	-	Enabled	Disconnected	Disconnected
Gi 0/0/3	-	Enabled	Disconnected	Disconnected
Gi 0/0/4	-	Enabled	Disconnected	Disconnected
Gi 0/0/5	-	Enabled	Disconnected	Disconnected
Gi 0/0/6	-	Enabled	Disconnected	Disconnected

Interface packet statistics:



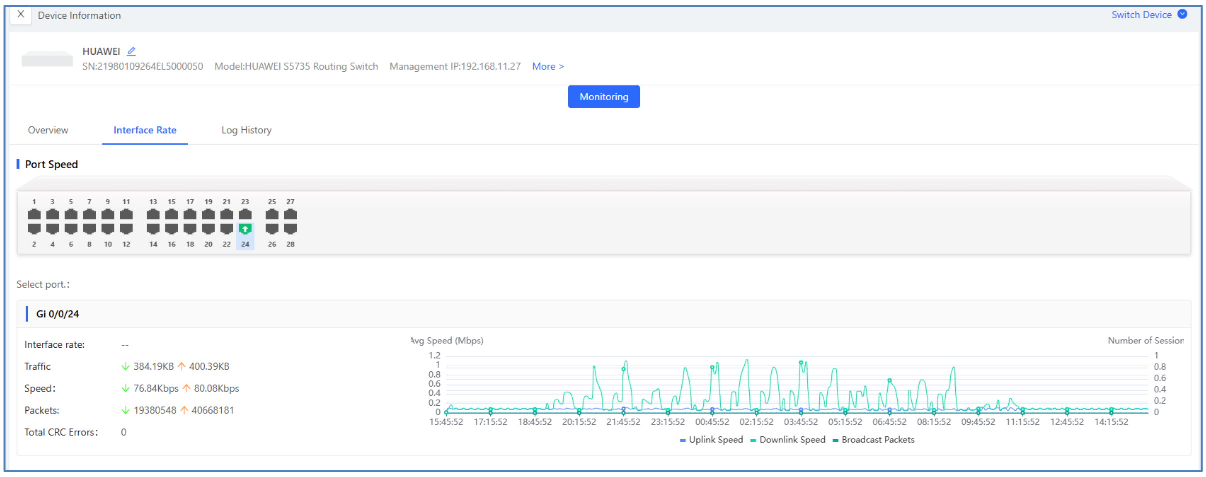
HUAWEI
SN:21980109264EL5000050 Model:HUAWEI S5735 Routing Switch Management IP:192.168.11.27 More >

Port Packet Statistics

Updated Time:

Port	Inbound/Outbound Traffic (KB)	Inbound/Outbound Rate (KB/s)	Number of Packets Received/Sent	CRC/FCS Errors	Fragment/Oversized Packets	Number of Conflicts
Gi 0/0/6	0/0	0.0/0.0	0/0	0/--	0/0	0
Gi 0/0/23	0/0	0.0/0.0	0/0	0/--	0/0	0
Gi 0/0/5	0/0	0.0/0.0	0/0	0/--	0/0	0
Console9/0/0	0/0	0.0/0.0	0/0	0/--	0/0	0
Gi 0/0/22	0/0	0.0/0.0	0/0	0/--	0/0	0
Gi 0/0/4	0/0	0.0/0.0	0/0	0/--	0/0	0
Gi 0/0/18	0/0	0.0/0.0	28477716/9130402	0/--	0/0	0
Gi 0/0/17	0/0	0.0/0.0	0/0	0/--	0/0	0
Gi 0/0/16	0/0	0.0/0.0	0/0	0/--	0/0	0
Gi 0/0/15	0/0	0.0/0.0	0/0	0/--	0/0	0

Interface rate trends:



HUAWEI
SN:21980109264EL5000050 Model:HUAWEI S5735 Routing Switch Management IP:192.168.11.27 More >

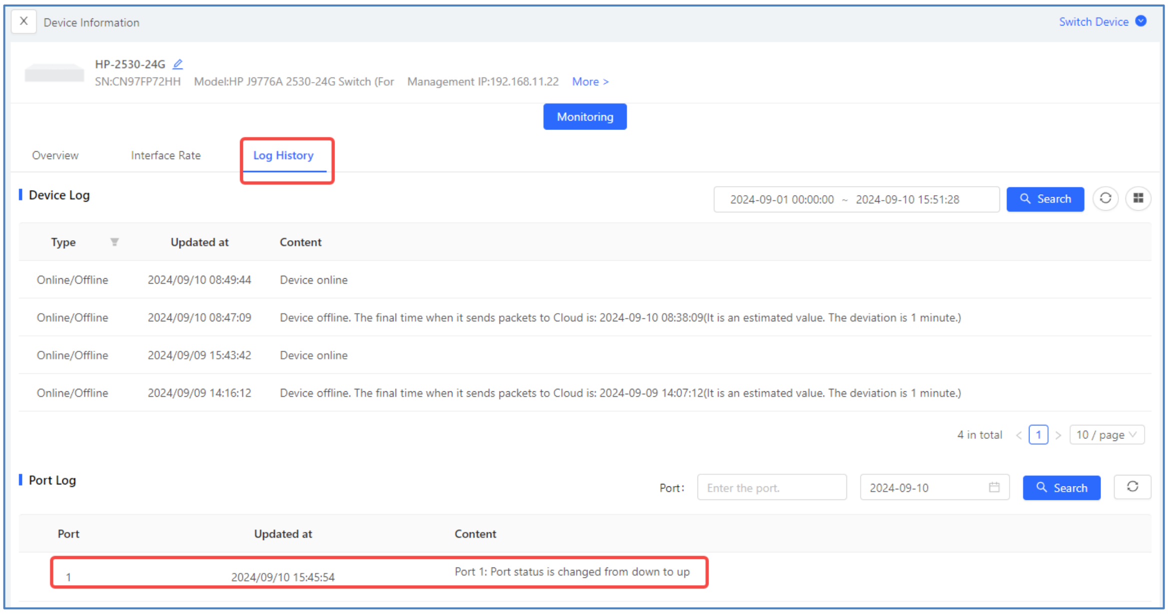
Port Speed

Select port.:

Gi 0/0/24

Interface rate: --
Traffic ↓ 384.19KB ↑ 400.39KB
Speed: ↓ 76.84Kbps ↑ 80.08Kbps
Packets: ↓ 19380548 ↑ 40668181
Total CRC Errors: 0

Device online/offline history and port events (Up/Down): The SNMP device offline detection mechanism checks the SNMP GET message every 5 minutes. If there is no response, the device is considered offline.



HP-2530-24G
SN:CN97FP72HH Model:HP J9776A 2530-24G Switch (For Management IP:192.168.11.22 More >

Device Log

2024-09-01 00:00:00 ~ 2024-09-10 15:51:28

Type	Updated at	Content
Online/Offline	2024/09/10 08:49:44	Device online
Online/Offline	2024/09/10 08:47:09	Device offline. The final time when it sends packets to Cloud is: 2024-09-10 08:38:09(It is an estimated value. The deviation is 1 minute.)
Online/Offline	2024/09/09 15:43:42	Device online
Online/Offline	2024/09/09 14:16:12	Device offline. The final time when it sends packets to Cloud is: 2024-09-09 14:07:12(It is an estimated value. The deviation is 1 minute.)

Port Log

Port: Enter the port. 2024-09-10

Port	Updated at	Content
1	2024/09/10 15:45:54	Port 1: Port status is changed from down to up

3 Networking

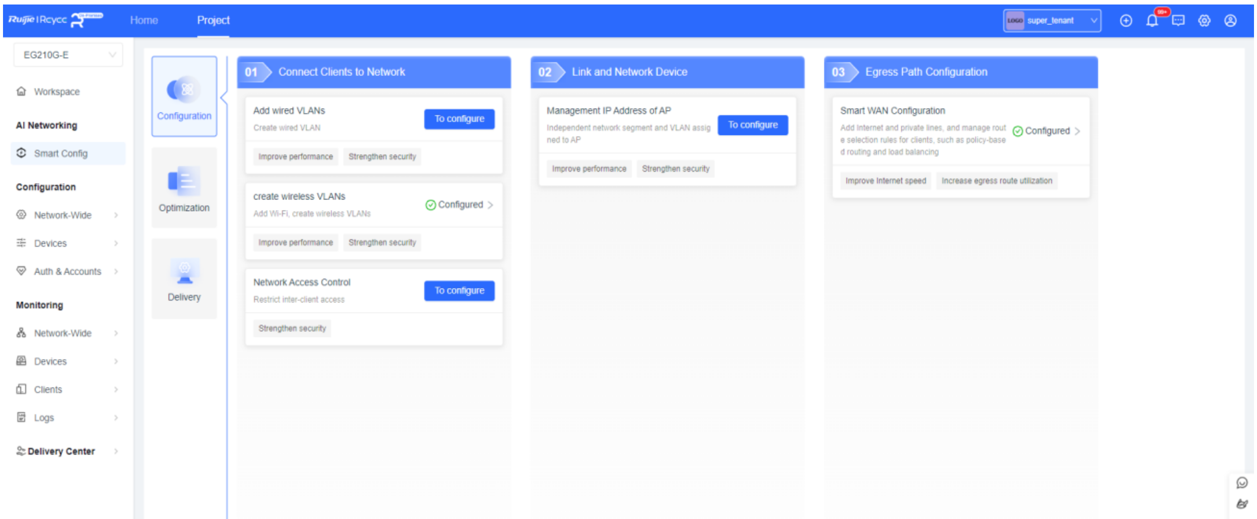
3.1 Smart Config

3.1.1 Configuration

(1) Project > Smart Config, click **Configuration**.

You can create wired and wireless VLANs, and perform ACL, AP VLAN, and WAN configurations on the page that is displayed.

Click To configure under the item that you want to configure. You will be redirected to the corresponding **configuration** page.

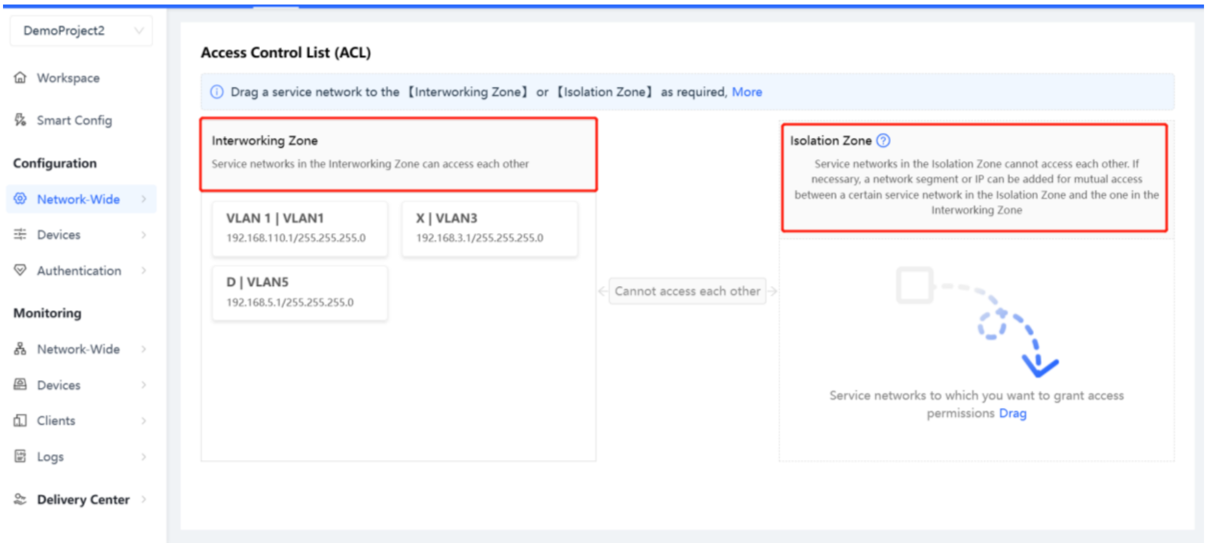


ACL configuration is used as an example to illustrate the configuration steps.

First, click **To configure**. The ACL page is displayed. On the page that is displayed, click **To configure** to start the configuration.

You can use this ACL feature to assign a service network to the **Interworking Zone** or the **Isolation Zone**, depending on the access control rights you want to assign to this service network. Service networks in the Interworking Zone can access each other,while those in the Isolation Zone cannot. Service networks in the interneworking Zone cannot access those in the Isolation Zone, and vice versa. You can restrict the access control rights of a service network by dragging it from the Interworking Zone to the Isolation Zone, and then clicking **Save**.

By clicking **No IP** under a service network in the Isolation Zone, you can set an IP address or an IP address range that is allowed to access this service network.



Access Control List (ACL)

Drag a service network to the 【Interworking Zone】 or 【Isolation Zone】 as required, More

Interworking Zone

Service networks in the Interworking Zone can access each other

VLAN 1 | VLAN1 192.168.110.1/255.255.255.0

X | VLAN3 192.168.3.1/255.255.255.0

D | VLAN5 192.168.5.1/255.255.255.0

Cannot access each other

Isolation Zone

Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for mutual access between a certain service network in the Isolation Zone and the one in the Interworking Zone

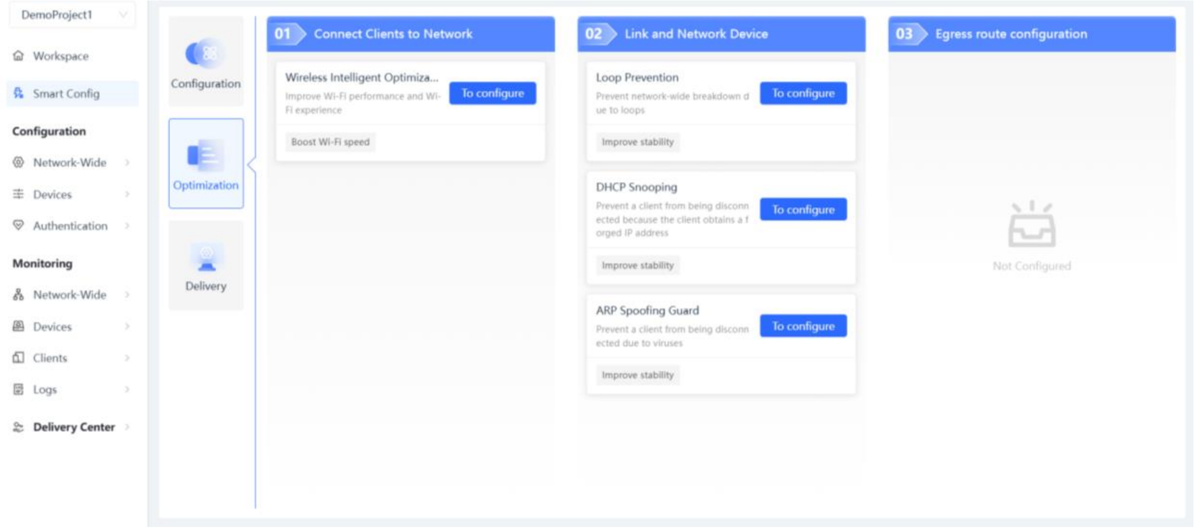
Service networks to which you want to grant access permissions Drag

3.1.2 Optimization

On the **Optimization** page, you can configure features such as Wi-Fi optimization, loop prevention, DHCP snooping, and ARP spoofing guard.

Click **To configure** under the item that you want to configure. You will be redirected to the corresponding configuration page.

WIO configuration is used as an example to illustrate the configuration steps.
First, click **To configure**. The WIO page is displayed. On the page that is displayed, click **Enable Wi-Fi Optimization**, and then click **Optimize Now**.
The system will perform the network optimization. After the optimization is complete, you can check the results by scrolling down the page.
You can set the time for scheduled optimization by clicking **Optimization Schedule**, and then clicking **Save** to save the configuration.



01 Connect Clients to Network

Wireless Intelligent Optimiza... Improve Wi-Fi performance and Wi-Fi experience — Boost Wi-Fi speed

02 Link and Network Device

Loop Prevention: Prevent network-wide breakdown due to loops — Improve stability

DHCP Snooping: Prevent a client from being disconnected because the client obtains a forged IP address — Improve stability

ARP Spoofing Guard: Prevent a client from being disconnected due to viruses — Improve stability

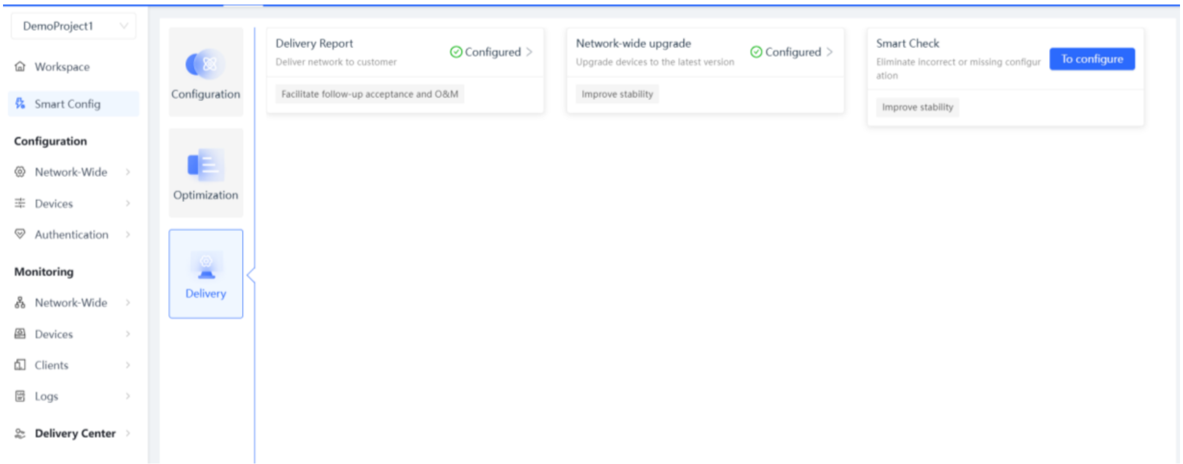
03 Egress route configuration

3.1.3 Delivery

You can perform a network-wide smart check, view reports and update devices by clicking **Delivery**.
Click **To configure** under the item that you want to configure. You will be redirected to the corresponding configuration page.
Smart Check is used as an example to illustrate the configuration steps.

First, click **To configure**. Click **Check Now.**

The system will perform the smart check. After the check is complete, you can click **View Report** to view the project report.



4 Network Configuration

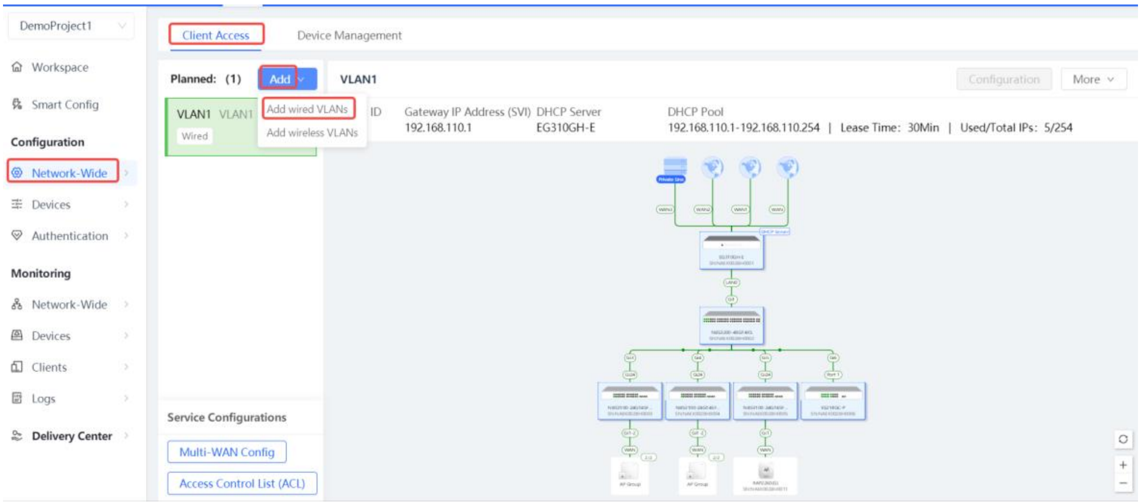
4.1 Creating a Wired VLAN

4.1.1 Overview

Different clients exist on a network, such as PCs and cameras. When a camera is running, broadcast or abnormal traffic often occurs, imposing negative effects on the service network. The administrator wants to isolate the broadcast and abnormal traffic of the camera from the running service network.

4.1.2 Configuration Steps

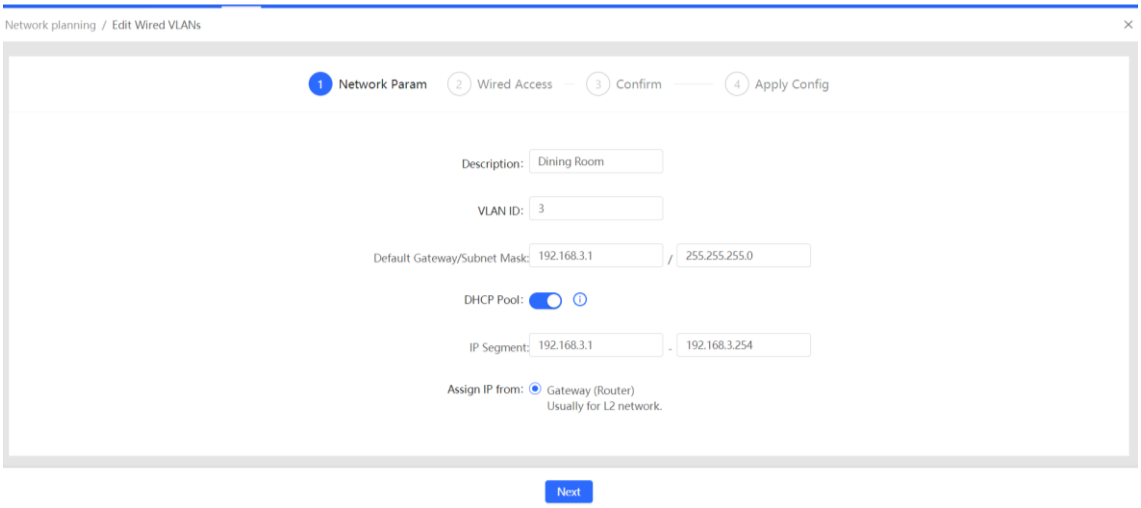
(1) Adding a wired VLAN: Click **Add** and select **Add wired VLANs** to add wired VLAN configuration for the current network, or select an existing wired VLAN and click **Configuration**.



VLAN1

ID	Gateway IP Address (SVI)	DHCP Server	DHCP Pool
	192.168.110.1	EG310GH-E	192.168.110.1-192.168.110.254 | Lease Time: 30Min | Used/Total IPs: 5/254

(2) Setting service parameters: Set the VLAN for wired access and create a Dynamic Host Configuration Protocol (DHCP) address pool for devices in the VLAN to automatically obtain IP addresses. The gateway can serve as the address pool server to assign addresses to access clients. If a core switch supporting the address pool function is deployed on a network, you can configure the switch as the address pool server. After configuring service parameters, click **Next**.



Network planning / Edit Wired VLANs

Description: Dining Room

VLAN ID: 3

Default Gateway/Subnet Mask: 192.168.3.1 / 255.255.255.0

DHCP Pool: ●

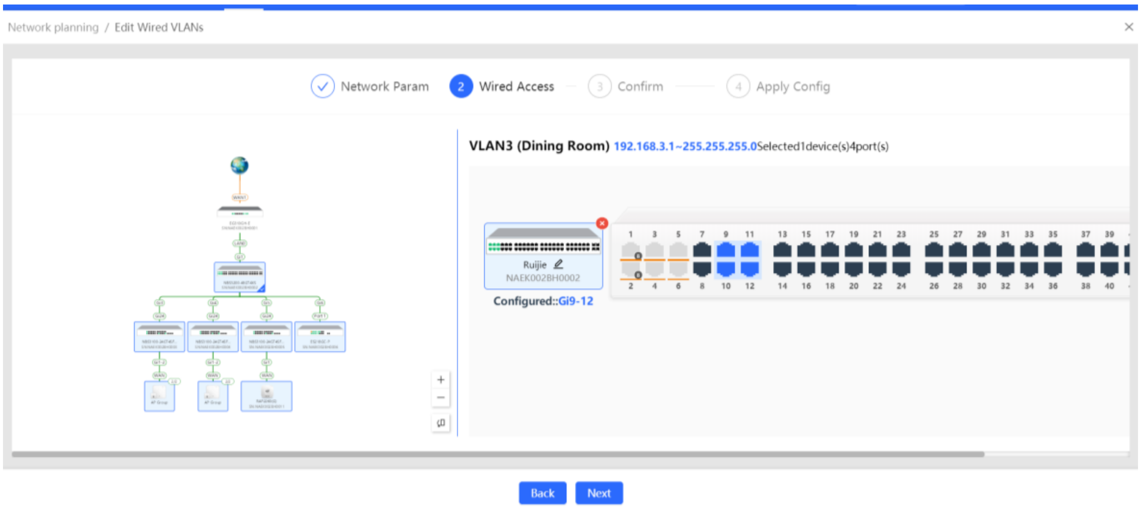
IP Segment: 192.168.3.1 - 192.168.3.254

Assign IP from: ● Gateway (Router)
Usually for L2 network.

The following table lists the description of parameters.

Parameter	Description
Description	Enter the VLAN description, for example, Office PC.
VLAN ID	The VLAN ID can be set to any value from 2 to 232 and from 234 to 4060, except the used value.
Default Gateway/Subnet Mask	After the VLAN ID is configured, the value of the default gateway or the subnet mask will be updated automatically 1s later.
DHCP Pool	You are advised to keep the default configuration. If the DHCP pool is disabled, a camera or PC needs to be manually configured with a static IP address. The deployment location of the IP address pool can be selected as needed. Generally, the gateway used as the DHCP server is applicable to a Layer 2 network, and the core switch used as the DHCP server is applicable to a Layer 3 network.
IP Segment	The parameter is available only when the DHCP pool is enabled. When the VLAN ID is configured, the IP segment will be updated automatically 1s later.
Assign IP from	The parameter is available only when the DHCP pool is enabled. You are advised to keep the default configuration.

(3) Select the interface for connecting the camera in the topology on the left, and select the port to connect the camera from port icons on the right. The port icon will change from gray-black to blue. Click Next.

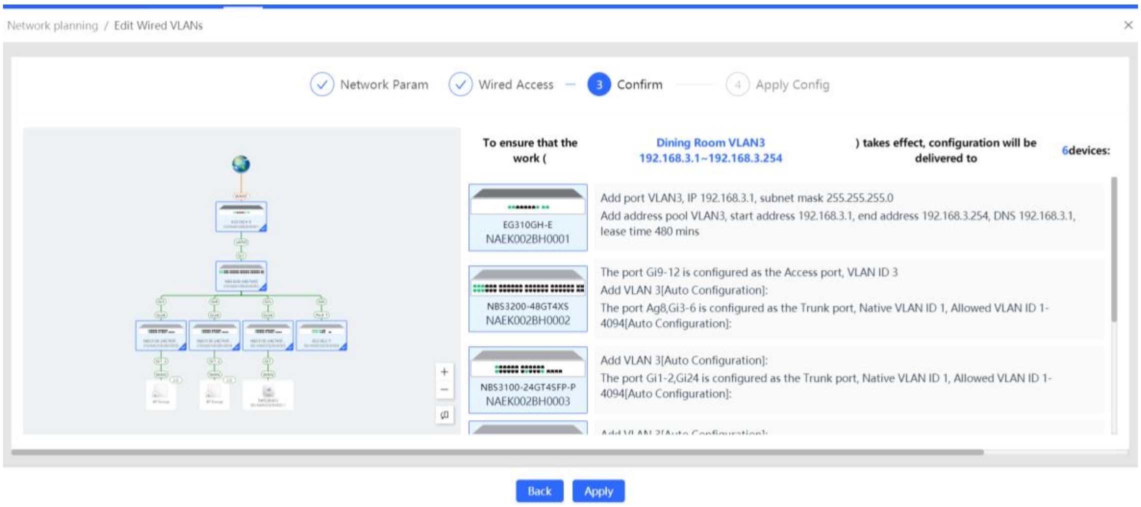


VLAN3 (Dining Room) 192.168.3.1~255.255.255.0Selected1device(s)4port(s)

NAEK002BH0002

Configured::Gi9-12

(4) Click Apply. The configuration will be delivered to the gateway and the switch, and takes effect.



To ensure that the work (Dining Room VLAN3 192.168.3.1~192.168.3.254) takes effect, configuration will be delivered to 6devices:

EG310GH-E NAEK002BH0001

Add port VLAN3, IP 192.168.3.1, subnet mask 255.255.255.0

Add address pool VLAN3, start address 192.168.3.1, end address 192.168.3.254, DNS 192.168.3.1, lease time 480 mins

NBS3200-48GT4XS NAEK002BH0002

The port Gi9-12 is configured as the Access port, VLAN ID 3

Add VLAN 3[Auto Configuration]:

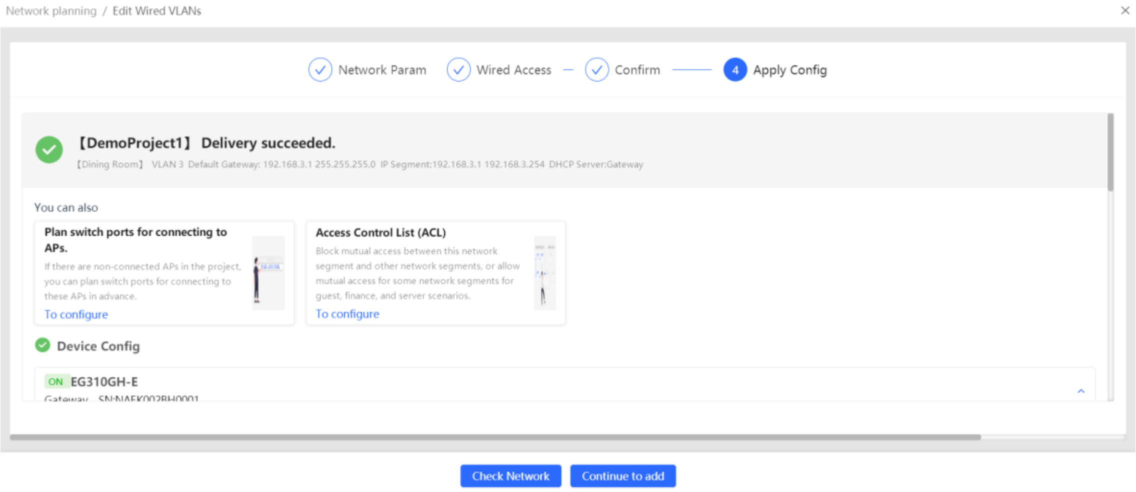
The port Ag8,Gi3-6 is configured as the Trunk port, Native VLAN ID 1, Allowed VLAN ID 1-4094[Auto Configuration]:

NBS3100-24GT4SFP-P NAEK002BH0003

Add VLAN 3[Auto Configuration]:

The port Gi1-2,Gi24 is configured as the Trunk port, Native VLAN ID 1, Allowed VLAN ID 1-4094[Auto Configuration]:

(5) The service network is added successfully when the message indicating delivery success is displayed.



【DemoProject1】 Delivery succeeded.

【Dining Room】 VLAN 3 Default Gateway: 192.168.3.1 255.255.255.0 IP Segment:192.168.3.1 192.168.3.254 DHCP Server:Gateway

You can also

Plan switch ports for connecting to APs.

If there are non-connected APs in the project, you can plan switch ports for connecting to these APs in advance.

To configure

Access Control List (ACL)

Block mutual access between this network segment and other network segments, or allow mutual access for some network segments for guest, finance, and server scenarios.

To configure

Device Config

ON EG310GH-E

Gateway SN:NAEK002BH0001

4.1.3 FAQs

1. Why Do I Classify VLANs?

(1) Reducing resource waste caused by broadcast traffic

In monitoring, door control, IPTV, and other scenarios, the heavy broadcast traffic of different services can easily affect each other, causing network jamming. Broadcast domains need to be isolated to reduce the bandwidth occupied by broadcast packets and avoid broadcast storms.

①There are broadcast packets of various network protocols, such as Address Resolution Protocol (ARP) requests for querying MAC addresses of identified devices, and DHCP requests for requesting IP addresses. When there are considerable clients on the network, broadcast packets will occupy numerous bandwidth resources, causing resource waste. VLANs can isolate broadcast domains and reduce bandwidth resource waste.

②In monitoring, door control, broadcast system, and other scenarios, broadcast or multicast packets (devices that do not support multicasting will process multicast packets as broadcast packets) are usually used. Therefore, separate VLANs need to be configured for monitoring and video (such as IPTV) devices to isolate such traffic from common service traffic.

(2) Facilitating management

After VLANs are classified based on departments, policies can be conveniently configured for different departments and enterprise intranets can be better managed.

In hotel scenarios, there may be Internet access by guests, conference room and banquet network, reception office network, and monitoring network. The reception office network involves the check-in/refund handling. In enterprise office scenarios, different departments may have different intranet access permissions and different security requirements. It is necessary to classify VLANs by user category and configure access control lists (ACLs) and other policies to meet different service requirements.

(3) Ensuring intranet security

①In a LAN, device information can be easily captured, and even data may be stolen, imposing security risks. After VLANs are configured, LANs can be divided into different VLANs to narrow down the broadcast scope of different packets, thereby enhancing information security.

For example, in the enterprise office scenario, configuring a guest VLAN can greatly reduce security threats imposed by visitors to the intranet.

②Some virus software identifies other devices in the same VLAN through scanning in broadcast mode, and spreads viruses to the other devices in the same VLAN. Classifying VLANs can restrict the spread within the same VLAN.

For example, in the primary and middle school scenarios, teachers' Internet access devices and teaching devices can be added to different VLANs to prevent the spread of viruses on a teacher's PC to the teaching devices.

In conclusion, on the enterprise network, hotel network, school network, multi-client network, and monitoring and IPTV service networks, classify VLANs to improve the network experience and security.

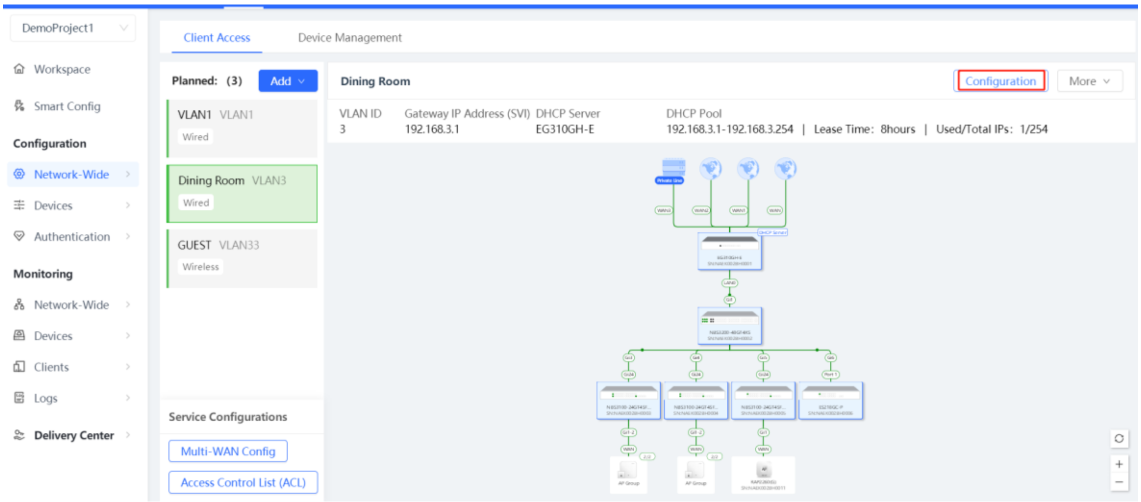
2. How Do I Set the Lease Time of DHCP Addresses?

Purpose of Lease Period

When clients are online, they renew the lease automatically when 1/2 or 7/8 of the lease period has elapsed. If the lease is not renewed because a client goes offline or other problems arise, the client can continue to use the original IP address after reconnection before the lease period expires. For example, if the lease period is 24 hours and a client goes offline, the client can still use the original IP address after re-login within one day. If the lease period expires, the IP address will be returned to the address pool. When the client connects to the network again, it will obtain an address again. In general scenarios, keep the default value for the lease period. If the address pool has sufficient addresses, set the lease period to a smaller value; if the addresses are sufficient, set the lease period to a larger value.

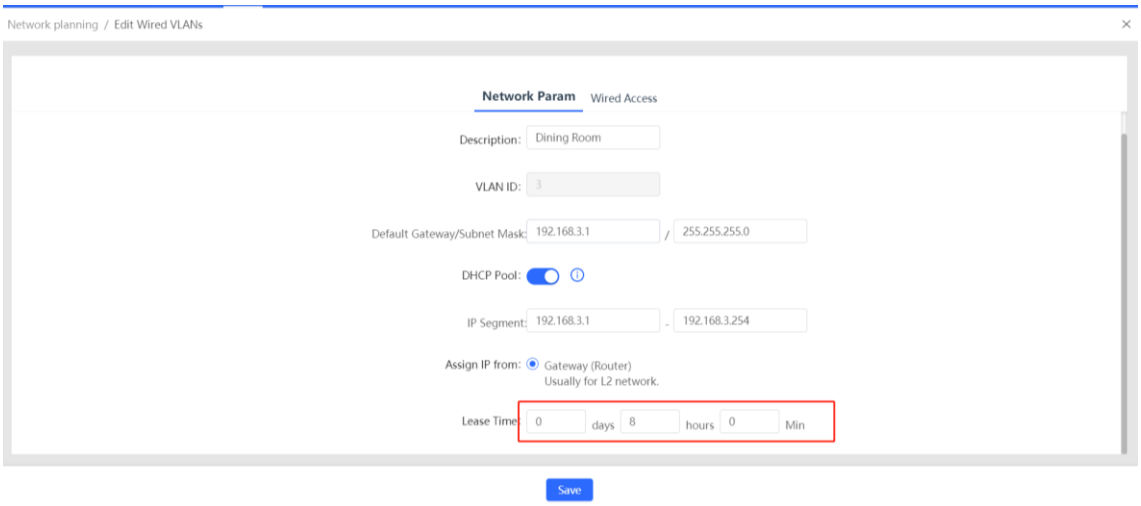
Configuration Steps

(1) Choose **Configuration** > **Network-Wide** > **Planned**, select a VLAN, and then click **Configuration** at the upper right corner.



VLAN ID	Gateway IP Address (SVI)	DHCP Server	DHCP Pool
3	192.168.3.1	EG310GH-E	192.168.3.1-192.168.3.254 | Lease Time: 8hours | Used/Total IPs: 1/254

(2) Enter the lease period and click **Save**.



Description: Dining Room

VLAN ID: 3

Default Gateway/Subnet Mask: 192.168.3.1 / 255.255.255.0

DHCP Pool: ●

IP Segment: 192.168.3.1 - 192.168.3.254

Assign IP from: ● Gateway (Router)
Usually for L2 network.

Lease Time: 0 days 8 hours 0 Min

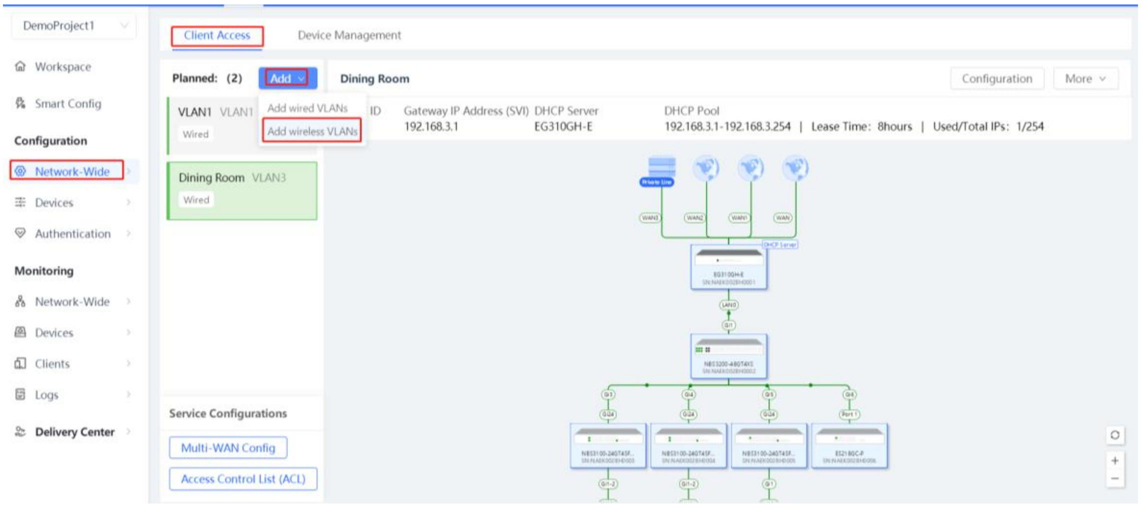
4.2 Creating a Wireless VLAN

4.2.1 Overview

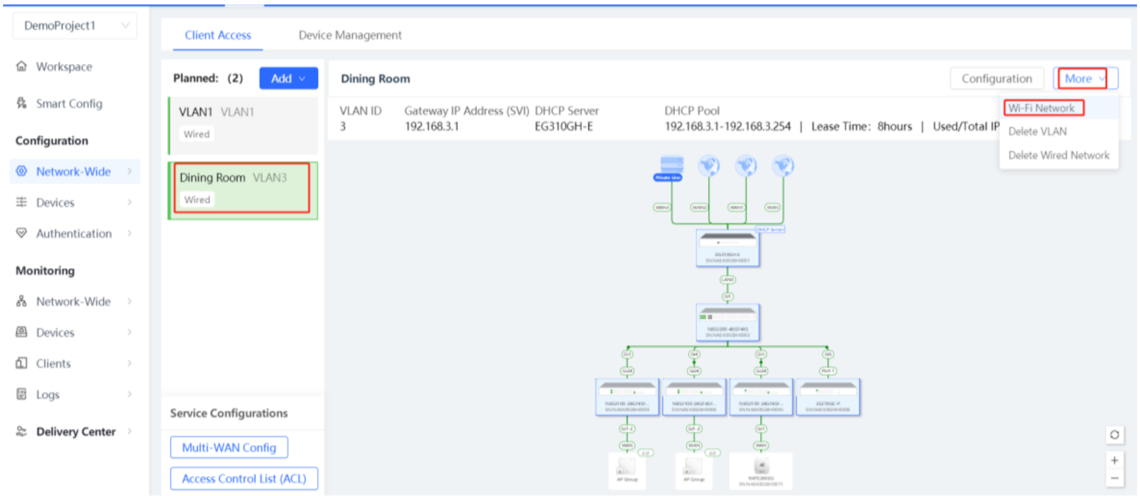
To manage the Wi-Fi usage of different user groups (such as company employees and external guests) separately, the company wants to provide separate Wi-Fi access for guests, and isolate the IP segment used by the guests' terminals and the VLAN to which they belong from company employees.

4.2.2 Configuration Steps

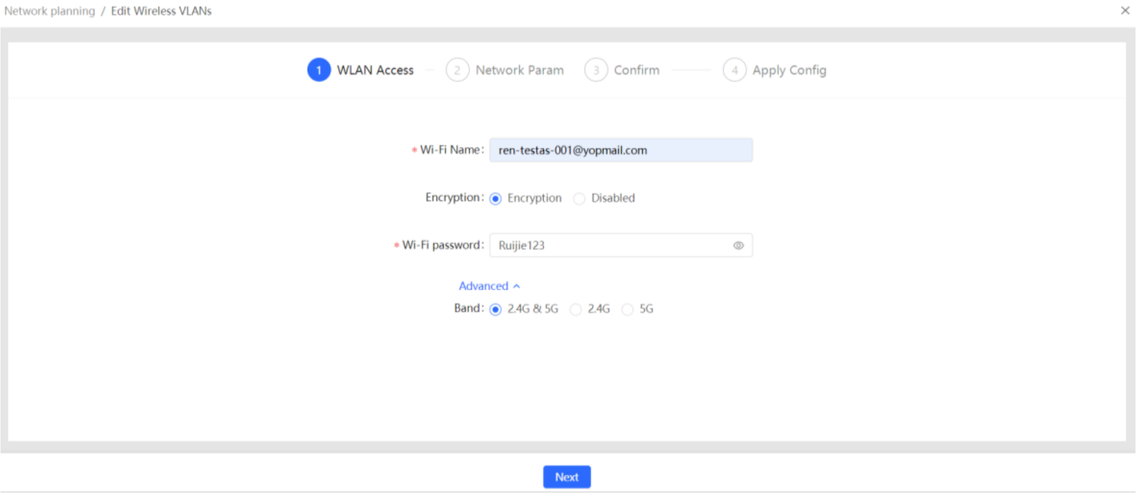
(1) Adding a wireless VLAN: Click **Add** and select **Add wireless VLANs** to add wireless VLAN configuration for the current network.



Alternatively, select an existing wired VLAN and click **More** and select **Wi-Fi Network** to add a Wi-Fi network based on the current wired VLAN.



(2) Setting Wi-Fi service parameters: Set Wi-Fi information first, such as the Wi-Fi name and password.



* Wi-Fi Name: ren-testas-001@yopmail.com

Encryption: ● Encryption ○ Disabled

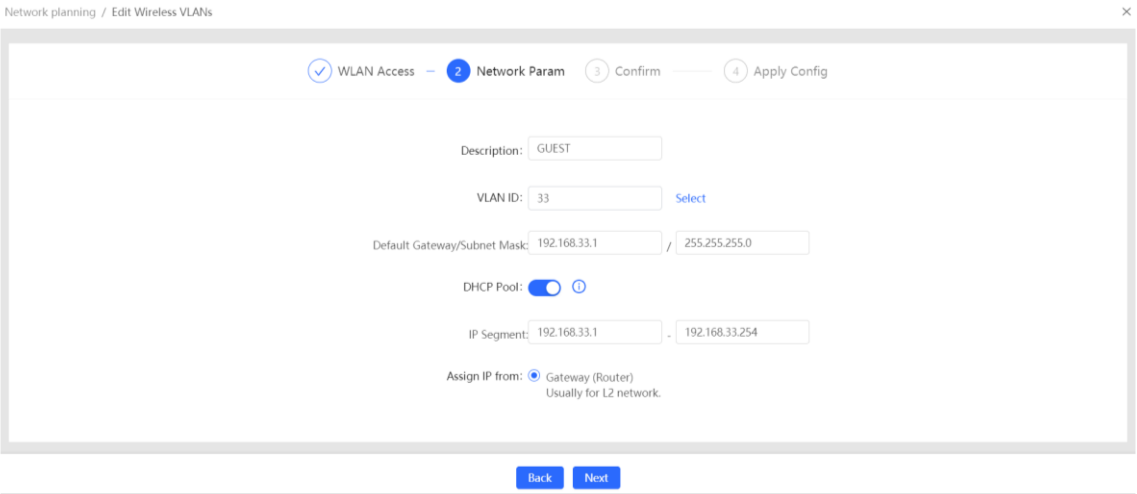
* Wi-Fi password: Ruijie123

Band: ● 2.4G & 5G ○ 2.4G ○ 5G

The following table lists the description of parameters.

Parameter	Description
SSID	Enter a string of less than 32 charters, including letters, numerals, spaces, and special characters (-_@&.). If spaces are contained, it cannot be longer than characters. For example, set SSID to Guest.
Encryption	You are advised to encrypt the network to prevent other clients from accessing the network. If an open network is required, click Disabled.
Password	Enter the password with a string of 8 to 16 characters, containing letters, numbers and special characters (<=>[]!@#$*().). For example, set Password to Ruijie123.
Advanced Settings > Band	The value is 2.4G & 5G, 2.4G, or 5G. The default value is 2.4G & 5G.

(3) Configuring the VLAN for wired access: Create a DHCP address pool for devices in the VLAN to automatically obtain IP addresses. The gateway can serve as the address pool server to assign addresses to access clients. If a core switch supporting the address pool function is deployed on a network, you can configure the switch as the address pool server. After configuring service parameters, click **Next**.



Description: GUEST

VLAN ID: 33 Select

Default Gateway/Subnet Mask: 192.168.33.1 / 255.255.255.0

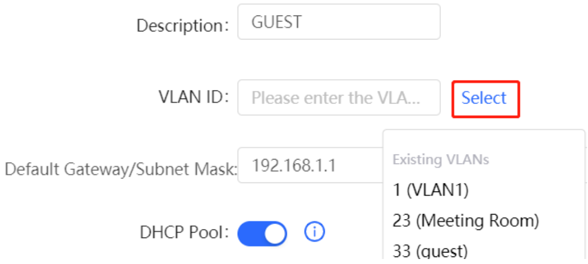
DHCP Pool: ● ⓘ

IP Segment: 192.168.33.1 - 192.168.33.254

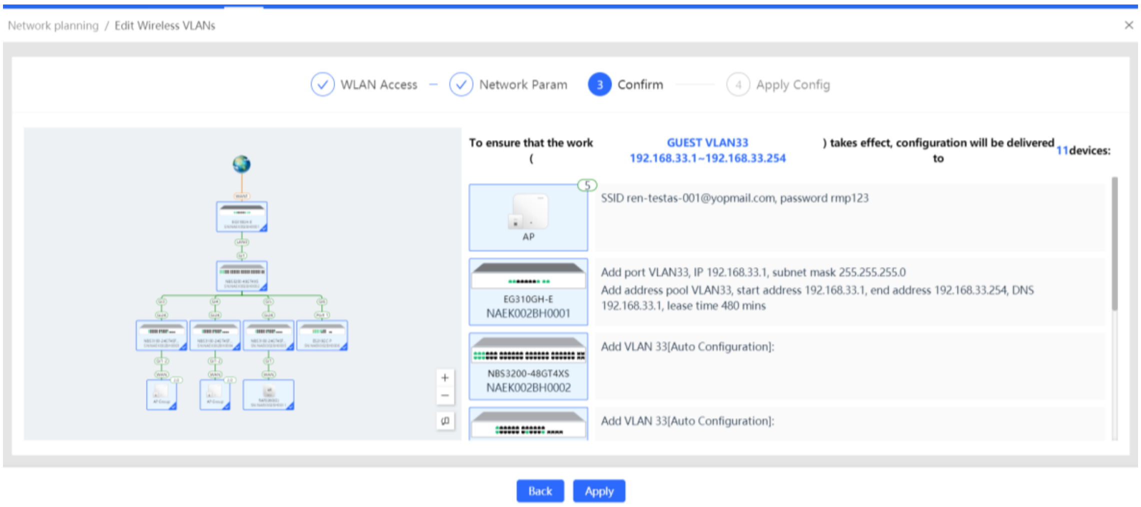
Assign IP from: ● Gateway (Router)
Usually for L2 network.

The following table lists the description of parameters.

Parameter	Description
Description	Enter the description of the guest VLAN.

Parameter	Description
VLAN ID	The VLAN ID can be set to any value from 2 to 232 and from 234 to 4060. If the service network created is used for both wired and wireless client access, and the corresponding wired service network (such as a wired network for guests) exists, click **Select** to select a VLAN ID from **Existing VLANs**, and then click it to add a wireless network based on the wired service network.  Description: GUEST VLAN ID: Please enter the VLA... Select Default Gateway/Subnet Mask: 192.168.1.1 DHCP Pool: ⓘ Existing VLANs 1 (VLAN1) 23 (Meeting Room) 33 (guest)
Default Gateway/Subnet Mask	When the VLAN ID is configured, the value of the default gateway or the subnet mask will be updated automatically 1s later.
DHCP Pool	You are advised to keep the default configuration. If the DHCP pool is disabled, a camera or PC needs to be manually configured with a static IP address. The deployment location of the IP address pool can be selected as needed. Generally, the gateway used as the DHCP server is applicable to a Layer 2 network, and the core switch used as the DHCP server is applicable to a Layer 3 network.
IP Segment	The parameter is available only when the DHCP pool is enabled. After the VLAN ID is configured, the IP segment will be updated automatically 1s later.
Assign IP from	The parameter is available only when the DHCP pool is enabled. You are advised to keep the default configuration.

(4) Confirm the WLAN network configuration and click Apply. The configuration will be delivered to the gateway, switch, and AP, and takes effect.



To ensure that the work (GUEST VLAN33 192.168.33.1~192.168.33.254) takes effect, configuration will be delivered to 11devices:

SSID ren-testas-001@yopmail.com, password rmp123

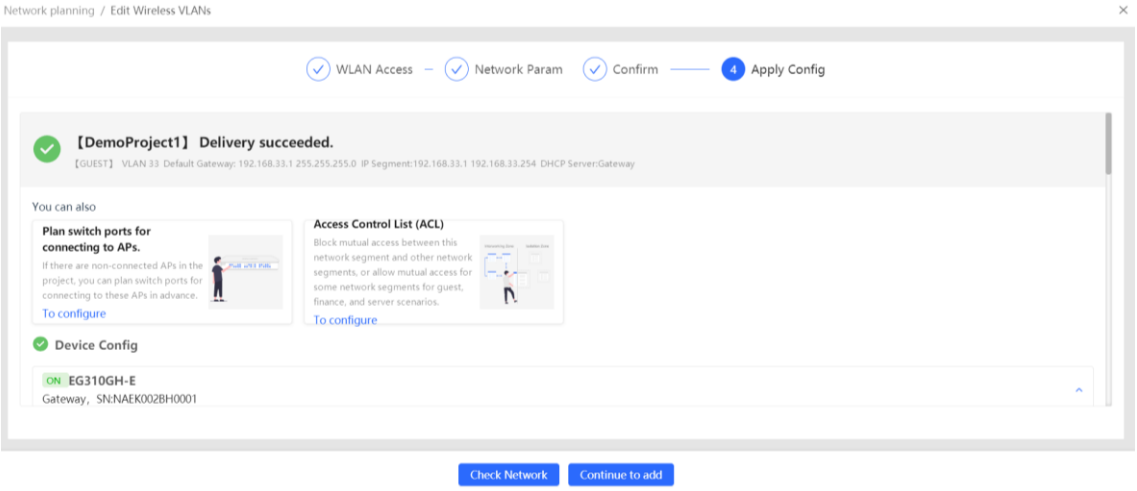
Add port VLAN33, IP 192.168.33.1, subnet mask 255.255.255.0

Add address pool VLAN33, start address 192.168.33.1, end address 192.168.33.254, DNS 192.168.33.1, lease time 480 mins

Add VLAN 33[Auto Configuration]:

Add VLAN 33[Auto Configuration]:

(5) The service network is added successfully when the message indicating delivery success is displayed.



【DemoProject1】 Delivery succeeded.

【GUEST】 VLAN 33 Default Gateway: 192.168.33.1 255.255.255.0 IP Segment:192.168.33.1 192.168.33.254 DHCP Server:Gateway

You can also

Plan switch ports for connecting to APs.

If there are non-connected APs in the project, you can plan switch ports for connecting to these APs in advance.

To configure

Access Control List (ACL)

Block mutual access between this network segment and other network segments, or allow mutual access for some network segments for guest, finance, and server scenarios.

To configure

Device Config

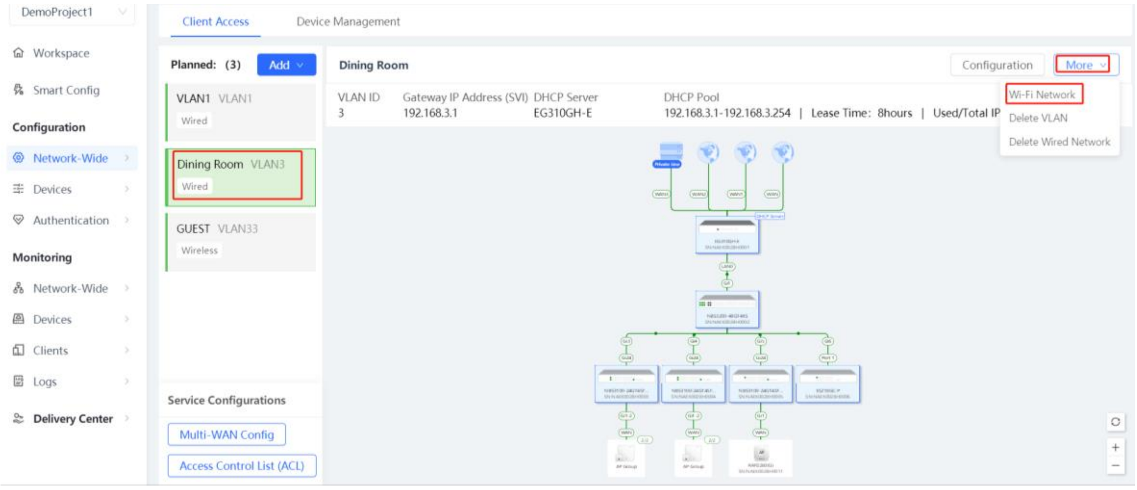
ON EG310GH-E

Gateway, SN:NAEK002BH0001

4.2.3 FAQs

1. How Do I Add the Names of Multiple Wi-Fi Networks to the Same VLAN?

When multiple Wi-Fi signals need to be added to the same VLAN, you can select the VLAN, to which Wi-Fi signals need to be added, in the service map in the middle, click **More** and select **Wi-Fi Network**, add Wi-Fi information, and deliver the configuration.



VLAN ID 3

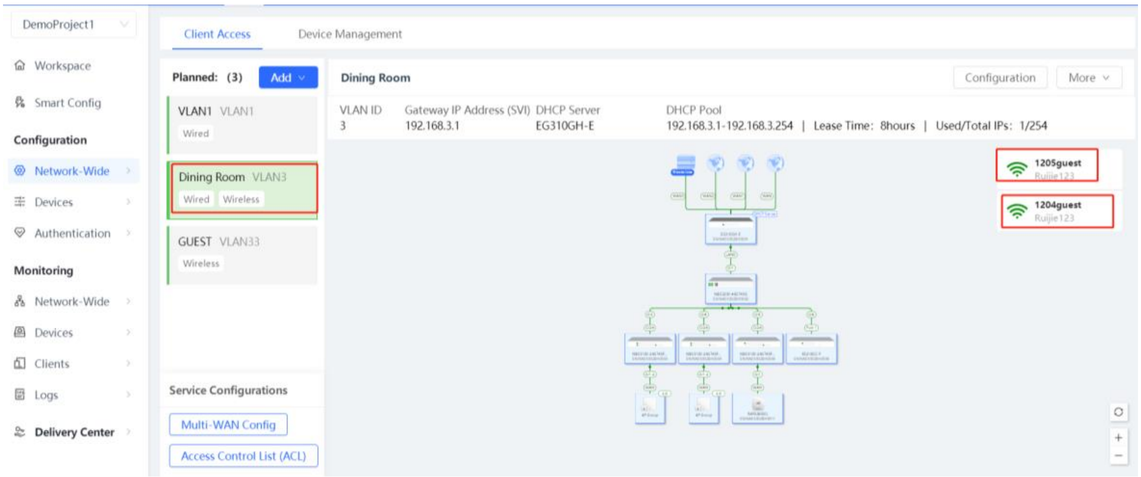
Gateway IP Address (SVI) 192.168.3.1

DHCP Server EG310GH-E

DHCP Pool 192.168.3.1-192.168.3.254 | Lease Time: 8hours | Used/Total IP

2. How Do I Add the Names of Multiple Wi-Fi Networks to Different VLANs?

When multiple Wi-Fi networks need to be added to different VLANs, add wireless networks multiple times by referring to 4.2.2 Configuration Steps.



VLAN ID 3 | Gateway IP Address (SVI) 192.168.3.1 | DHCP Server EG310GH-E | DHCP Pool 192.168.3.1-192.168.3.254 | Lease Time: 8hours | Used/Total IPs: 1/254

4.3 Configuring the AP Management Service Network (AP Management VLAN)

4.3.1 Demand

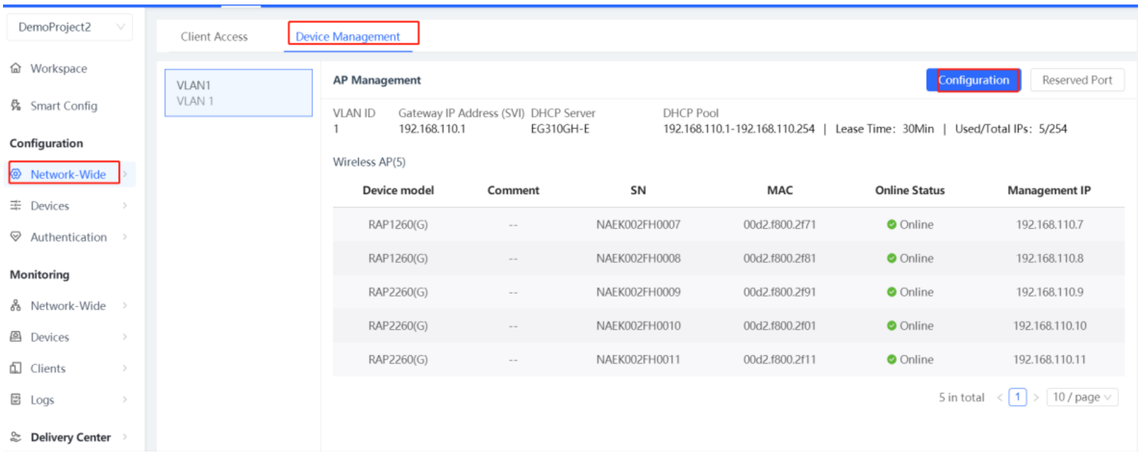
Multiple access points (APs) are deployed on the network to transmit wireless network signals. One separate VLAN needs to be configured for management packets of the APs. Configuring a separate management service network can avoid AP go-offline due to the complex environment on the service network, thereby enhancing the stability.

Ruijie Cloud can automatically detect switch ports, to which APs are connected, and users do not need to record them in advance, simplifying the difficulty in modifying and managing VLANs.

4.3.2 Configuration Steps

1. Configuring an AP Management VLAN

(1) Choose **Network-Wide** > **Network** > **VLAN** > **Device Management**. Information about APs on the network is displayed, including the management VLAN, device models, SNs, management IP addresses, MAC addresses, and online status. Click **Configuration** to configure the AP management service network.



VLAN ID 1 | Gateway IP Address (SVI) 192.168.110.1 | DHCP Server EG310GH-E | DHCP Pool 192.168.110.1-192.168.110.254 | Lease Time: 30Min | Used/Total IPs: 5/254

Wireless AP(5)

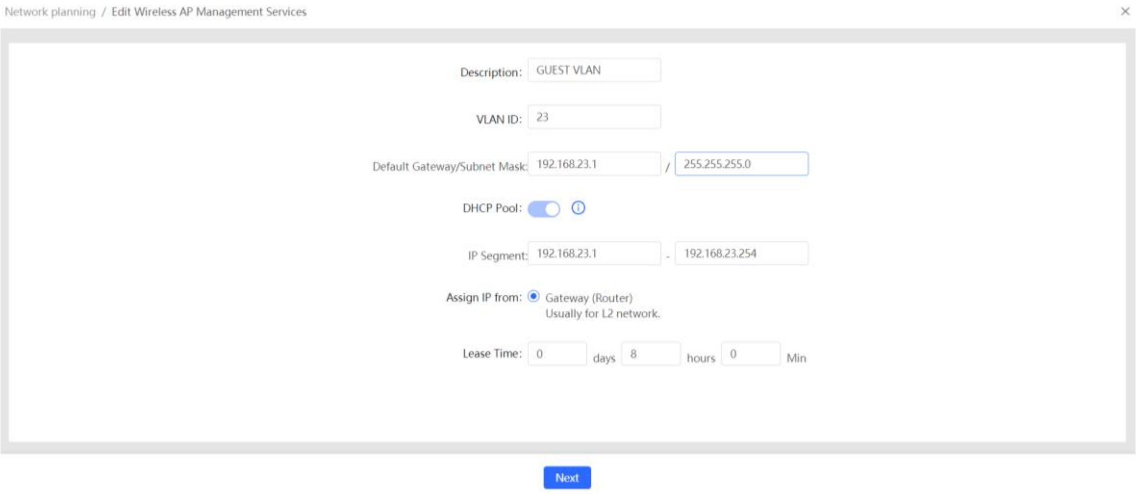
Device model	Comment	SN	MAC	Online Status	Management IP
RAP1260(G)	--	NAEK002FH0007	00d2.f800.2f71	● Online	192.168.110.7
RAP1260(G)	--	NAEK002FH0008	00d2.f800.2f81	● Online	192.168.110.8
RAP2260(G)	--	NAEK002FH0009	00d2.f800.2f91	● Online	192.168.110.9
RAP2260(G)	--	NAEK002FH0010	00d2.f800.2f01	● Online	192.168.110.10
RAP2260(G)	--	NAEK002FH0011	00d2.f800.2f11	● Online	192.168.110.11

5 in total < 1 > 10 / page

(2) Enter the description, set **VLAN ID** to **23**, and wait about 1 second. The default gateway/subnet mask and IP address segment will be automatically updated. You can select the deployment location of the IP address pool based on actual requirements: In general, the gateway serves as the DHCP server in Layer-2 network scenarios, and the core switch serves as the DHCP server in Layer-3 network scenarios. Click **Save**.

Caution

- You are advised to use default configurations for other parameters. Do not disable the DHCP address pool. Otherwise, IP addresses cannot be assigned to APs and you have to configure static IP addresses to the APs manually one by one.
- In **Description**, enter the description of the current service network for differentiation from other service networks.
- The VLAN ID can be set to any value in the range of 2 to 232 and 234 to 4060 except the numbers used by existing VLAN IDs.



Description: GUEST VLAN

VLAN ID: 23

Default Gateway/Subnet Mask: 192.168.23.1 / 255.255.255.0

DHCP Pool: ●

IP Segment: 192.168.23.1 - 192.168.23.254

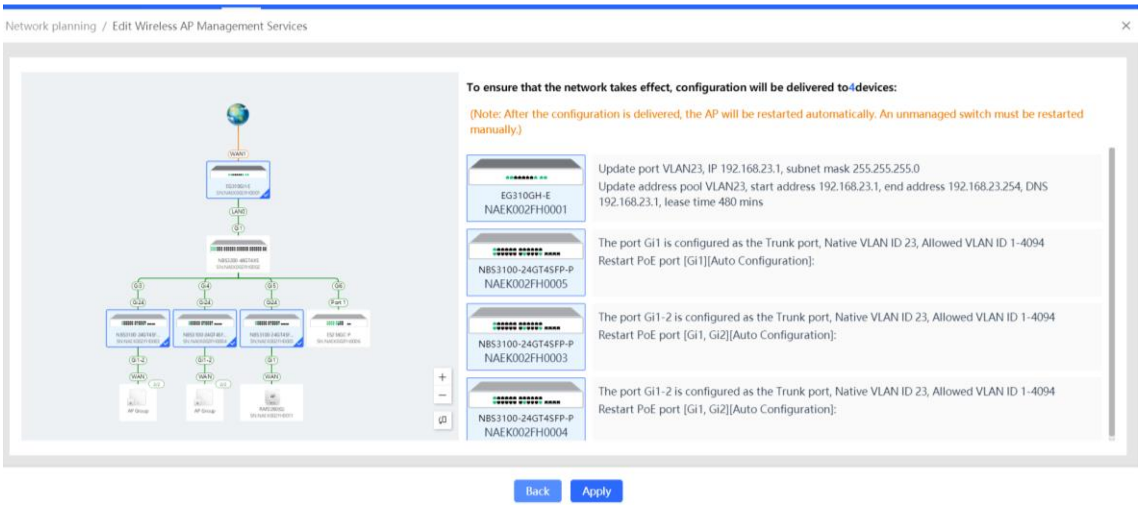
Assign IP from: ● Gateway (Router)
Usually for L2 network.

Lease Time: 0 days 8 hours 0 Min

(3) Click **Apply**. The configuration is delivered to the gateways and switches and takes effect. Wait till the prompt "Delivery succeeded" is displayed, indicating that the service network is added.

Note

After the configuration delivery is completed, PoE ports on the switches that are connected to the APs will be restarted to restart the APs. If there are configuration-free switches on the network, restart the APs manually.

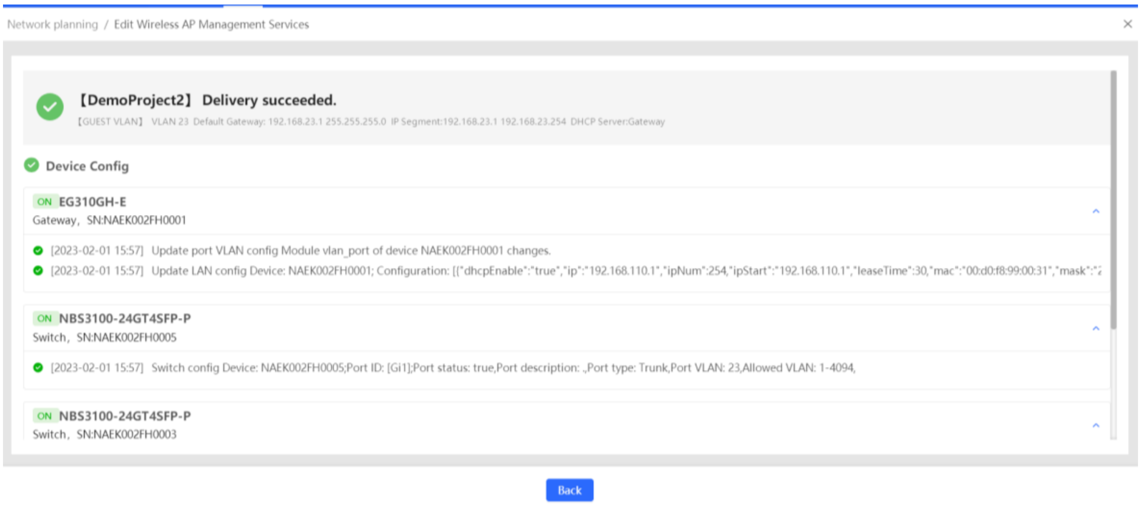


To ensure that the network takes effect, configuration will be delivered to4devices:

(Note: After the configuration is delivered, the AP will be restarted automatically. An unmanaged switch must be restarted manually.)

EG310GH-E NAEK002FH0001	Update port VLAN23, IP 192.168.23.1, subnet mask 255.255.255.0 Update address pool VLAN23, start address 192.168.23.1, end address 192.168.23.254, DNS 192.168.23.1, lease time 480 mins
NBS3100-24GT4SFP-P NAEK002FH0005	The port Gi1 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 1-4094 Restart PoE port [Gi1][Auto Configuration]:
NBS3100-24GT4SFP-P NAEK002FH0003	The port Gi1-2 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 1-4094 Restart PoE port [Gi1, Gi2][Auto Configuration]:
NBS3100-24GT4SFP-P NAEK002FH0004	The port Gi1-2 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 1-4094 Restart PoE port [Gi1, Gi2][Auto Configuration]:

(4) The AP management network configuration is delivered.



【DemoProject2】 Delivery succeeded.

【GUEST VLAN】 VLAN 23 Default Gateway: 192.168.23.1 255.255.255.0 IP Segment:192.168.23.1 192.168.23.254 DHCP Server:Gateway

Device Config

ON EG310GH-E
Gateway, SN:NAEK002FH0001

```
[2023-02-01 15:57] Update port VLAN config Module vlan_port of device NAEK002FH0001 changes.
[2023-02-01 15:57] Update LAN config Device: NAEK002FH0001; Configuration: [{"dhcpEnable":"true","ip":"192.168.110.1","ipNum":254,"ipStart":"192.168.110.1","leaseTime":30,"mac":"00:d0:f8:99:00:31","mask":"
```

ON NBS3100-24GT4SFP-P
Switch, SN:NAEK002FH0005

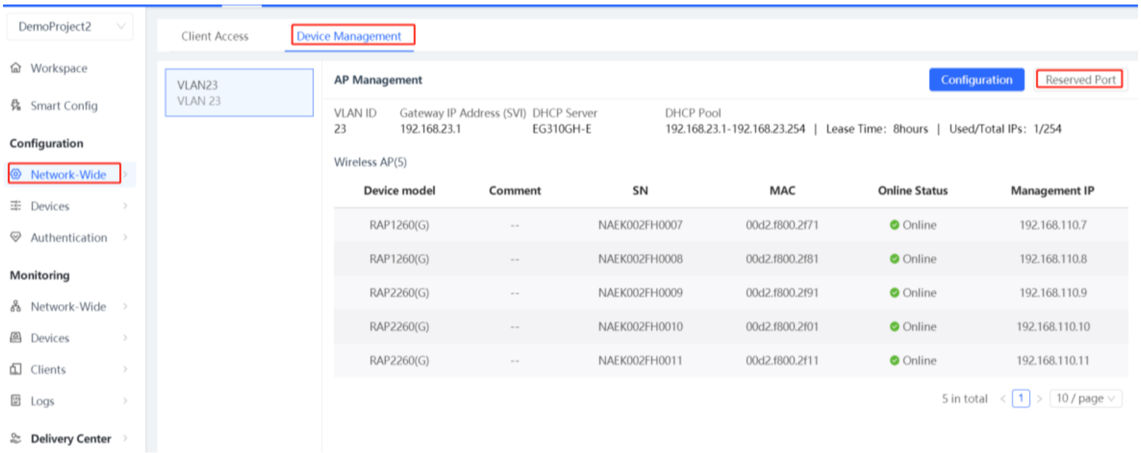
```
[2023-02-01 15:57] Switch config Device: NAEK002FH0005;Port ID: [Gi1];Port status: true,Port description: ,Port type: Trunk,Port VLAN: 23,Allowed VLAN: 1-4094,
```

ON NBS3100-24GT4SFP-P
Switch, SN:NAEK002FH0003

2. Configuring a Reserved Port for an AP (applicable to the scenario in which APs are not connected)

If an AP is not connected to the network, you can reserve a switch port for the AP.

(1) Choose **Network-Wide** > **VLAN** > **Device Management** > **Reserved Port**.



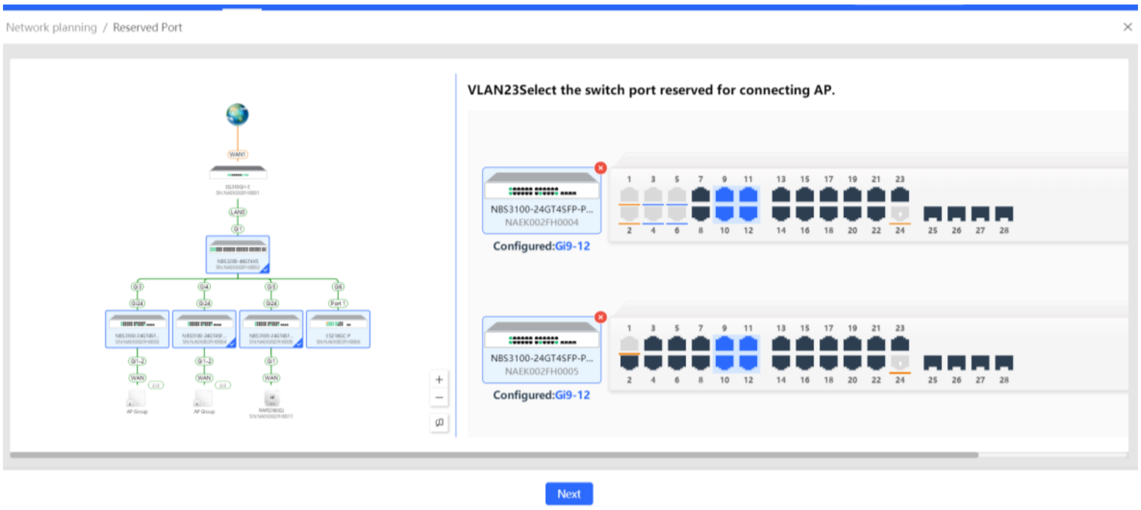
AP Management

VLAN ID	Gateway IP Address (SVI)	DHCP Server	DHCP Pool
23	192.168.23.1	EG310GH-E	192.168.23.1-192.168.23.254 | Lease Time: 8hours | Used/Total IPs: 1/254

Wireless AP(5)

Device model	Comment	SN	MAC	Online Status	Management IP
RAP1260(G)	--	NAEK002FH0007	00d2.f800.2f71	● Online	192.168.110.7
RAP1260(G)	--	NAEK002FH0008	00d2.f800.2f81	● Online	192.168.110.8
RAP2260(G)	--	NAEK002FH0009	00d2.f800.2f91	● Online	192.168.110.9
RAP2260(G)	--	NAEK002FH0010	00d2.f800.2f01	● Online	192.168.110.10
RAP2260(G)	--	NAEK002FH0011	00d2.f800.2f11	● Online	192.168.110.11

(2) Click the switch for connecting to an AP (you can select multiple switches) in the topology on the left, and select the port reserved for AP wired connection on the switch on the port icon panel on the right. The port icon changes from dark gray to blue. Click **Next**.



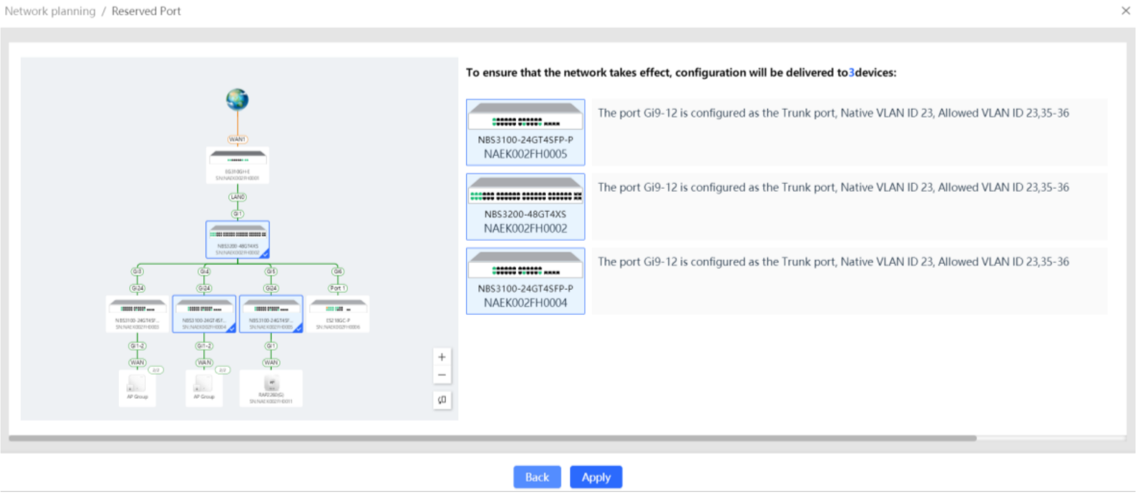
Network planning / Reserved Port

VLAN23Select the switch port reserved for connecting AP.

NBS3100-24GT4SFP-P...
NAEK002FH0004
Configured:Gi9-12

NBS3100-24GT4SFP-P...
NAEK002FH0005
Configured:Gi9-12

(3) Click **Apply**. The configuration is delivered to the switch and takes effect. Wait till the prompt "Delivery succeeded" is displayed, indicating that the reserved port is configured successfully.



Network planning / Reserved Port

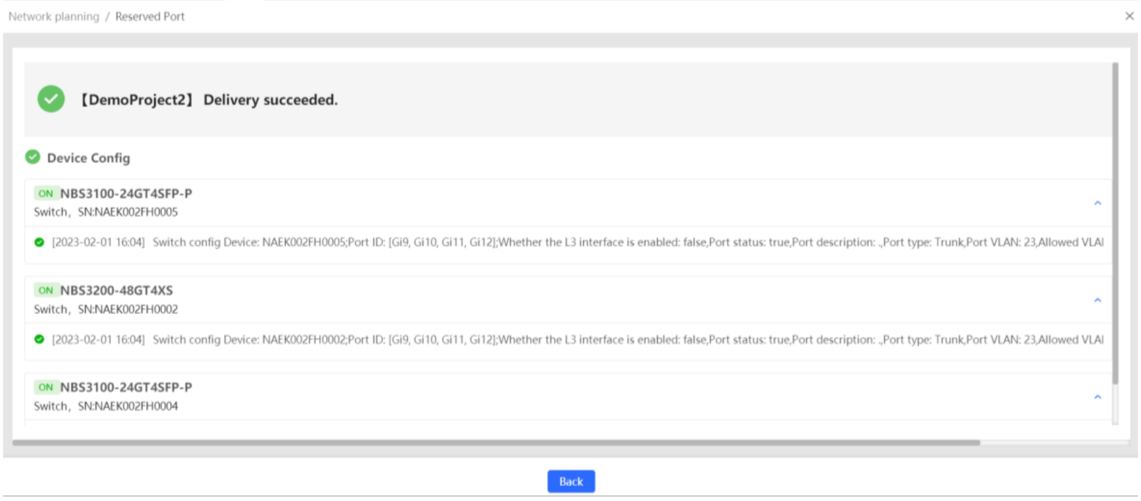
To ensure that the network takes effect, configuration will be delivered to3devices:

NBS3100-24GT4SFP-P
NAEK002FH0005
The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23,35-36

NBS3200-48GT4XS
NAEK002FH0002
The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23,35-36

NBS3100-24GT4SFP-P
NAEK002FH0004
The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23,35-36

(4) The port configuration is delivered successfully.



Network planning / Reserved Port

【DemoProject2】 Delivery succeeded.

Device Config

ON NBS3100-24GT4SFP-P
Switch, SN:NAEK002FH0005

[2023-02-01 16:04] Switch config Device: NAEK002FH0005;Port ID: [Gi9, Gi10, Gi11, Gi12];Whether the L3 interface is enabled: false,Port status: true,Port description: .,Port type: Trunk,Port VLAN: 23,Allowed VLAI

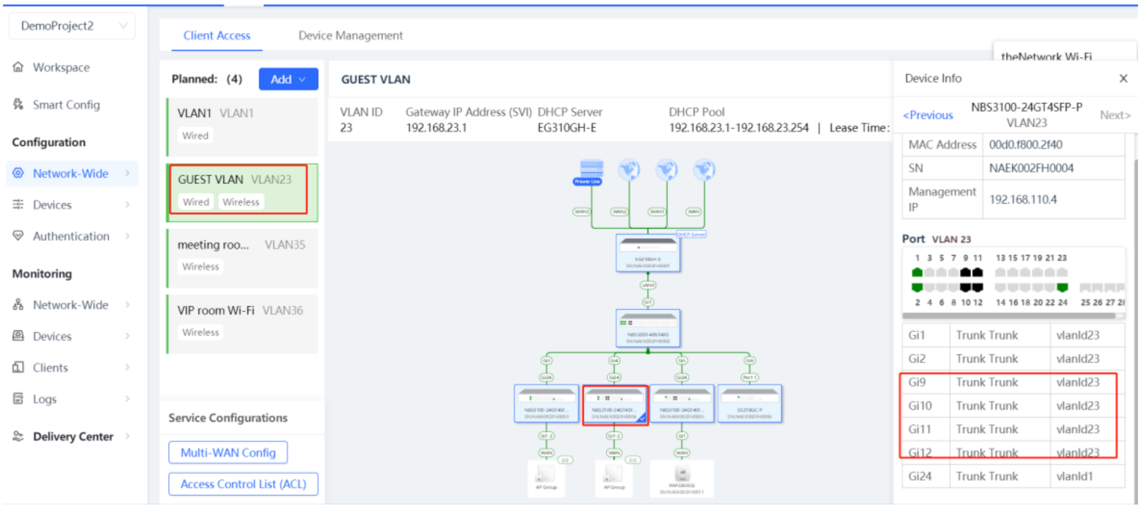
ON NBS3200-48GT4XS
Switch, SN:NAEK002FH0002

[2023-02-01 16:04] Switch config Device: NAEK002FH0002;Port ID: [Gi9, Gi10, Gi11, Gi12];Whether the L3 interface is enabled: false,Port status: true,Port description: .,Port type: Trunk,Port VLAN: 23,Allowed VLAI

ON NBS3100-24GT4SFP-P
Switch, SN:NAEK002FH0004

3. Verification

Check information about the configured AP management service network on the service map page. IP addresses obtained by APs belong to the 192.168.23.0/24 network segment.



GUEST VLAN

VLAN ID: 23 | Gateway IP Address (SVI): 192.168.23.1 | DHCP Server: EG310GH-E | DHCP Pool: 192.168.23.1-192.168.23.254 | Lease Time:

NBS3100-24GT4SFP-P
VLAN23

MAC Address	00d0.f800.2f40
SN	NAEK002FH0004
Management IP	192.168.110.4

Port VLAN 23

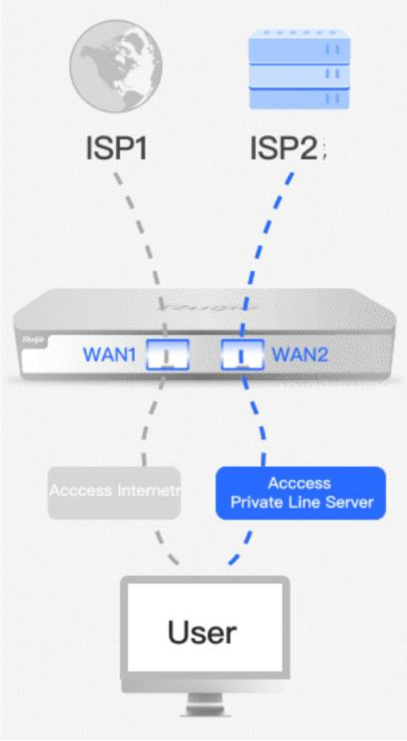
Gi1	Trunk Trunk	vlanId23
Gi2	Trunk Trunk	vlanId23
Gi9	Trunk Trunk	vlanId23
Gi10	Trunk Trunk	vlanId23
Gi11	Trunk Trunk	vlanId23
Gi12	Trunk Trunk	vlanId23
Gi24	Trunk Trunk	vlanId1

4.4 Multi-WAN

4.4.1 Overview

1. Applicable Scenarios

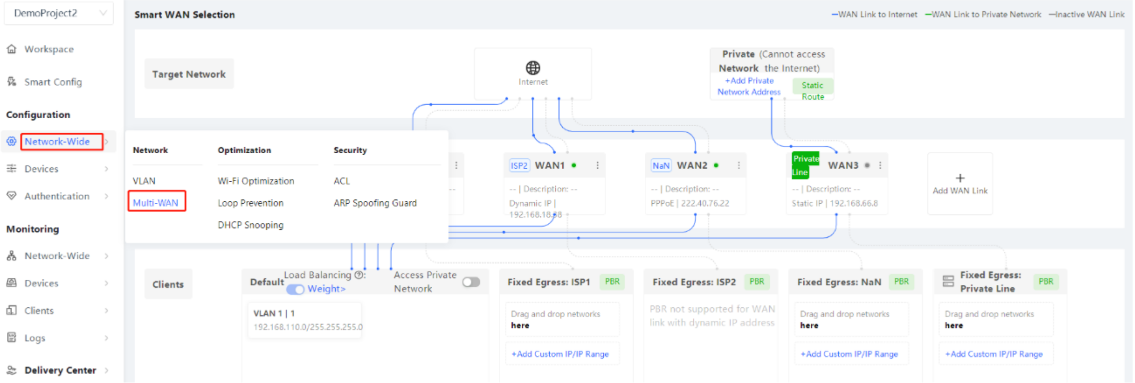
When a gateway is connected to multiple extranet lines, the multi-WAN function can be configured to meet different requirements. This function mainly applies to the following three scenarios:



- Traffic from different users is transmitted through different egresses: IP traffic from some intranet users can be transmitted through a fixed extranet line.
- Bandwidth superimposition (load balancing): The gateway automatically distributes egress traffic to multiple extranet lines to achieve the bandwidth superimposition effect.
- Private line for access to the private line server: A private network refers to a network that cannot access the Internet, such as e-government private networks. The access traffic of a device on the intranet to private line resources needs to be transmitted through the private line egress, while the Internet access traffic needs to be transmitted through other egresses.

2. Configuration Page

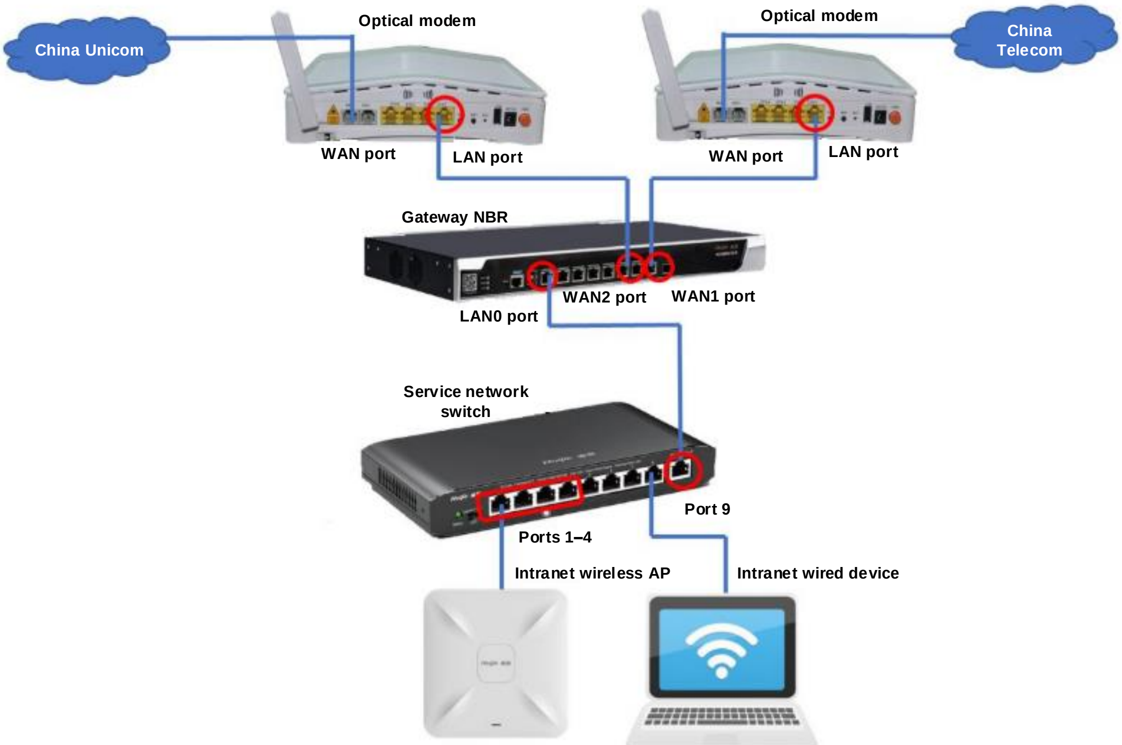
Choose **Network-Wide** > **Multi-WAN** to go to the **Smart WAN Selection** page.



4.4.2 Multi-WAN Bandwidth Superimposition

1. Demand

A company's network connects to two broadband Internet access lines. The bandwidths need to be superimposed to meet the Internet access needs of multiple users.



Load balancing is automatically conducted on traffic from all devices on the intranet and the traffic is distributed to the WAN1 and WAN2 ports.

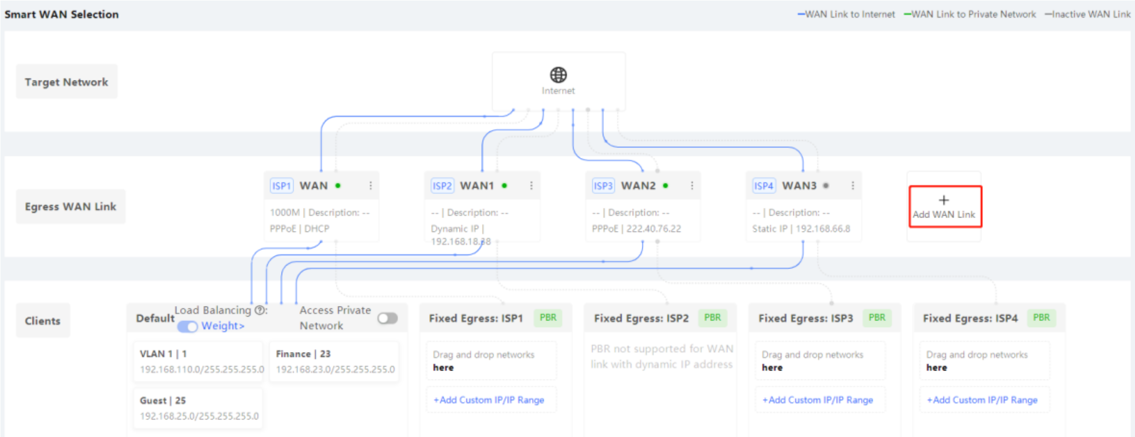
2. Configuration Ideas

(1) Configure WAN ports to access the Internet through dynamic IP addresses, static IP addresses (non-private line), or PPPoE.

(2) Enable load balancing.

3. Configuration Steps

(1) Click **Add WAN Link** to go to the **Multi-WAN Config** page of the gateway.



Smart WAN Selection

—WAN Link to Internet —WAN Link to Private Network —Inactive WAN Link

Target Network

Internet

Egress WAN Link

ISP1 WAN ●
1000M | Description: --
PPPoE | DHCP

ISP2 WAN1 ●
-- | Description: --
Dynamic IP | 192.168.18.88

ISP3 WAN2 ●
-- | Description: --
PPPoE | 222.40.76.22

ISP4 WAN3 ●
-- | Description: --
Static IP | 192.168.66.8

+ Add WAN Link

Clients

Default Load Balancing ⓘ: Weight> Access Private Network

VLAN 1 | 1
192.168.110.0/255.255.255.0

Finance | 23
192.168.23.0/255.255.255.0

Guest | 25
192.168.25.0/255.255.255.0

Fixed Egress: ISP1 PBR
Drag and drop networks **here**
+Add Custom IP/IP Range

Fixed Egress: ISP2 PBR
PBR not supported for WAN link with dynamic IP address

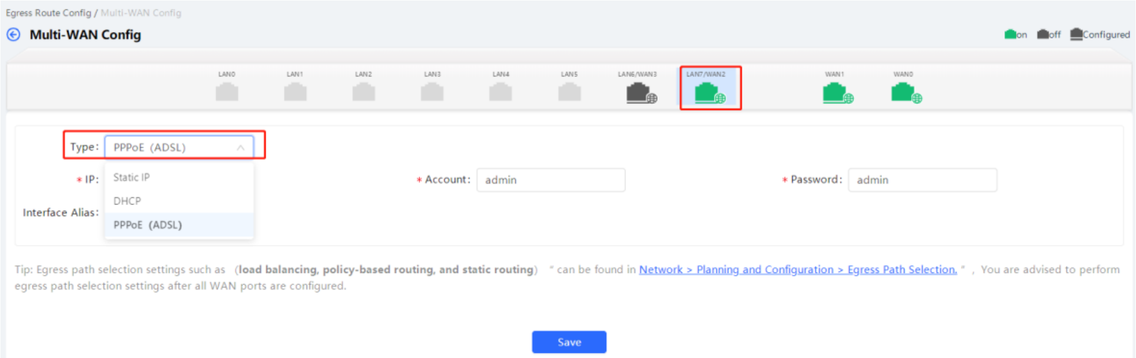
Fixed Egress: ISP3 PBR
Drag and drop networks **here**
+Add Custom IP/IP Range

Fixed Egress: ISP4 PBR
Drag and drop networks **here**
+Add Custom IP/IP Range

(2) Select a WAN port and configure the Internet access type for the WAN port based on the operator's requirements. It can be set to **Static IP**, **DHCP**, or **PPPoE (ADSL)**.Click **Save**.

Note

- If the configuration is inconsistent with the operator's requirements, for example, the account or password is incorrect, the network may be abnormal or disconnected.



Type: PPPoE (ADSL)

* IP:

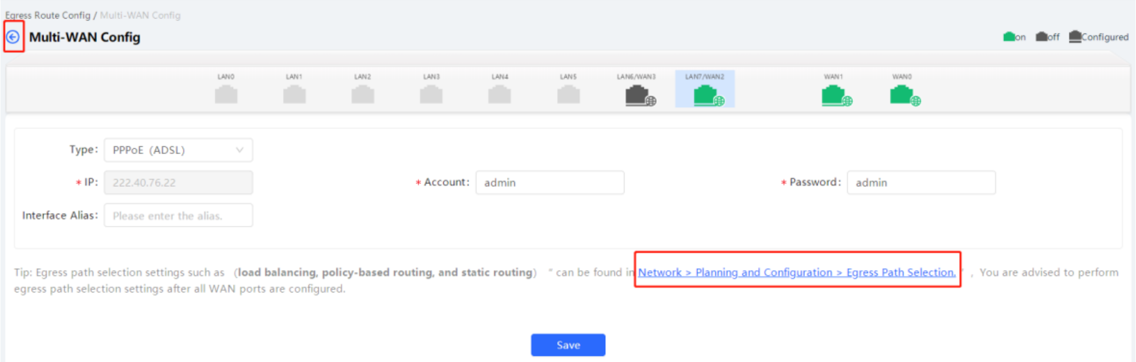
Interface Alias:

* Account: admin

* Password: admin

Tip: Egress path selection settings such as (**load balancing, policy-based routing, and static routing**) " can be found in Network > Planning and Configuration > Egress Path Selection. " , You are advised to perform egress path selection settings after all WAN ports are configured.

(3) Click the back button on the right of **Multi-WAN Config** or click **Network > Planning and Configuration > Egress Path Selection** to return to the **Smart WAN Selection** page.



Type: PPPoE (ADSL)

* IP: 222.40.76.22

Interface Alias: Please enter the alias.

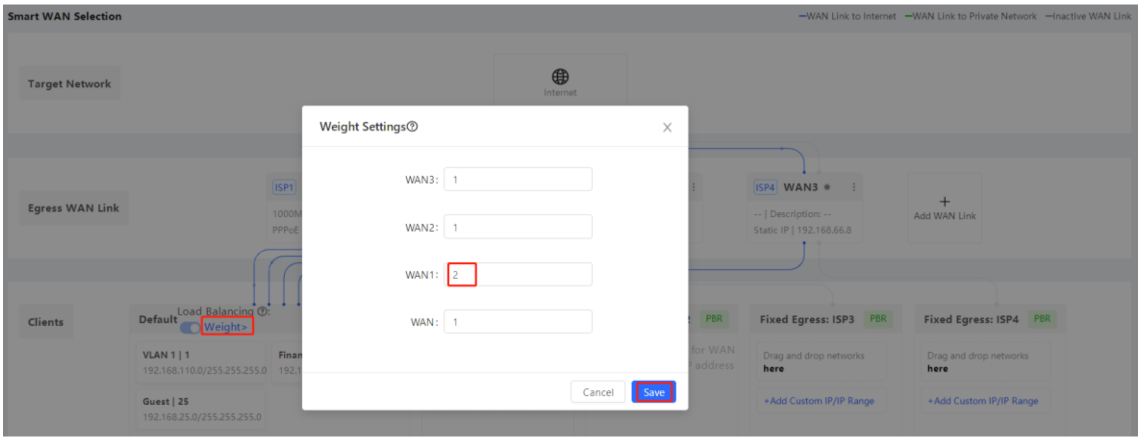
* Account: admin

* Password: admin

Tip: Egress path selection settings such as (**load balancing, policy-based routing, and static routing**) " can be found in Network > Planning and Configuration > Egress Path Selection. " , You are advised to perform egress path selection settings after all WAN ports are configured.

(4) Enable **Load Balancing** and click **Weight** to set the traffic weight.

Configure the load balancing weight based on the actual broadband proportion. The load is balanced based on the configured downlink bandwidth proportion by default. For example, the bandwidth is set to 200 Mbps for WAN1 port and 100 Mbps for other WAN ports. You can set the weight of the WAN1 port to 2 and the weight of other ports to 1. Click **Save**.



Weight Settings

WAN3: 1

WAN2: 1

WAN1: 2

WAN: 1

4.4.3 Configuring Traffic of Different Users to Pass Through Different Lines

1. Demand

A company's network connects to two broadband lines, and traffic from wired office users needs to be transmitted by the WAN2 port and the traffic from the wireless network needs to be transmitted by the WAN1 port. Bandwidth is automatically assigned to other users. The WAN1 port of the gateway is connected to an optical modem of China Telecom and the WAN2 port is connected to an optical modem of China Unicom.

2. Configuration Ideas

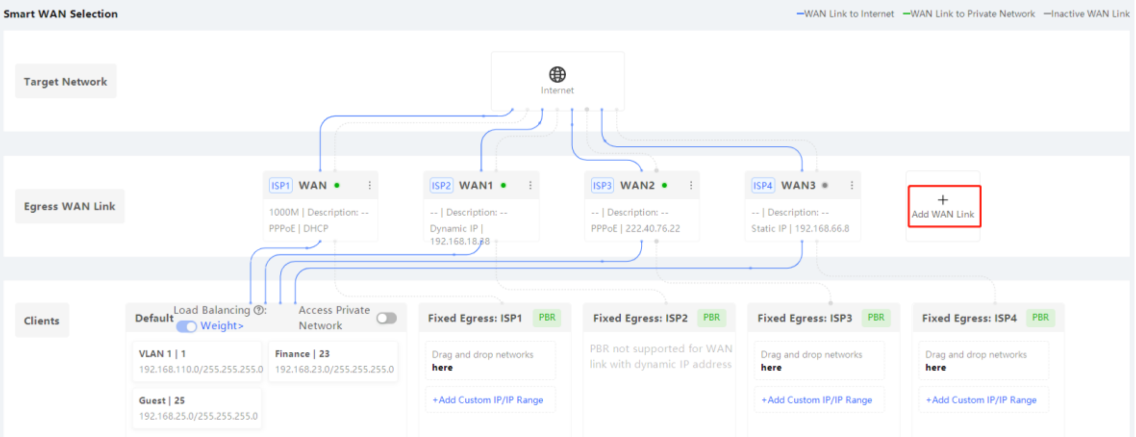
(1) Configure WAN ports to access the Internet through static IP addresses PPPoE.

(2) Configure traffic of different users to pass through different lines.

(3) Bandwidth is automatically assigned to other users.

3. Configuration Steps

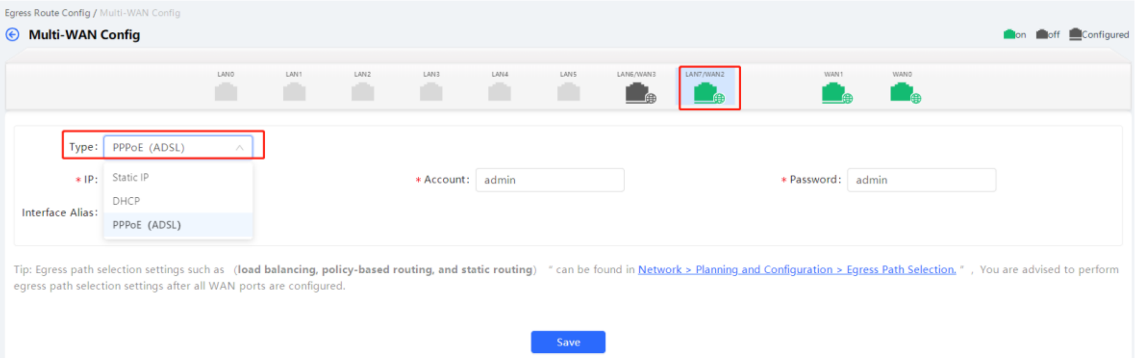
(1) Click **Add WAN Link** to go to the **Multi-WAN Config** page of the gateway.



(2) Select a WAN port and configure the Internet access type for the WAN port based on the operator's requirements. It can be set to **Static IP**, **DHCP**, or **PPPoE (ADSL)**.Click **Save**.

Note

- If the configuration is inconsistent with the operator's requirements, for example, the account or password is incorrect, the network may be abnormal or disconnected.



Type: PPPoE (ADSL)

* IP:

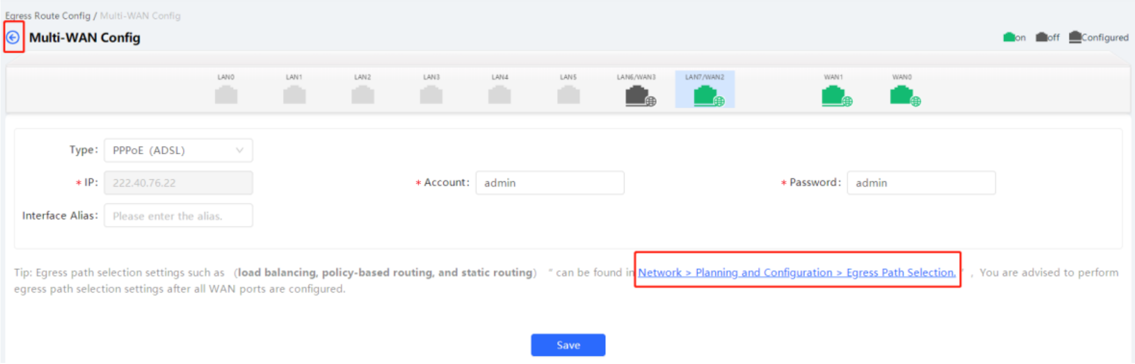
Interface Alias:

* Account: admin

* Password: admin

Tip: Egress path selection settings such as (**load balancing, policy-based routing, and static routing**) " can be found in Network > Planning and Configuration > Egress Path Selection. " , You are advised to perform egress path selection settings after all WAN ports are configured.

(3) Click the back button on the right of **Multi-WAN Config** or click **Network > Planning and Configuration > Egress Path Selection** to return to the **Smart WAN Selection** page.



Egress Route Config / Multi-WAN Config

Multi-WAN Config

Type: PPPoE (ADSL)

* IP: 222.40.76.22

* Account: admin

* Password: admin

Interface Alias: Please enter the alias.

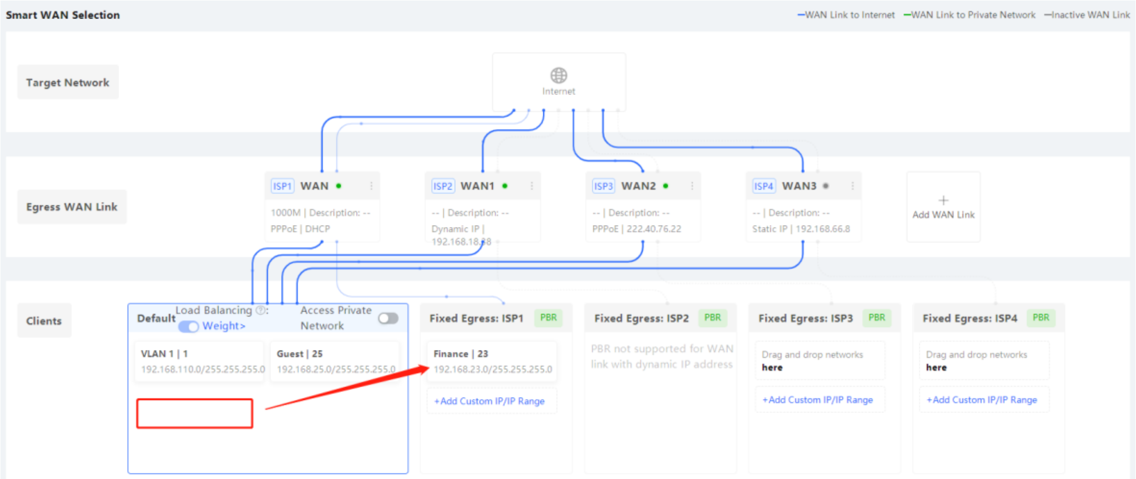
Tip: Egress path selection settings such as (load balancing, policy-based routing, and static routing) " can be found in Network > Planning and Configuration > Egress Path Selection. " , You are advised to perform egress path selection settings after all WAN ports are configured.

(4) Configure a routing policy.

Caution

- Only static IP addresses or PPPoE (ADSL) support the policy-based route (PBR) configuration.

If you need to add a created service network to a fixed line, for example, configure all users in VLAN 23 to access the Internet through the egress of ISP1, select VLAN 23 and drag it to the corresponding service network area, such as **Fixed Egress: ISP1**.



Smart WAN Selection

ISP1 WAN ● 1000M | Description: -- PPPoE | DHCP

ISP2 WAN1 ● -- | Description: -- Dynamic IP | 192.168.18.88

ISP3 WAN2 ● -- | Description: -- PPPoE | 222.40.76.22

ISP4 WAN3 ● -- | Description: -- Static IP | 192.168.66.8

Default Load Balancing: Weight> Access Private Network

VLAN 1 | 1 192.168.110.0/255.255.255.0

Guest | 25 192.168.25.0/255.255.255.0

Fixed Egress: ISP1 PBR

Finance | 23 192.168.23.0/255.255.255.0

+Add Custom IP/IP Range

Fixed Egress: ISP2 PBR

PBR not supported for WAN link with dynamic IP address

Fixed Egress: ISP3 PBR

Drag and drop networks **here**

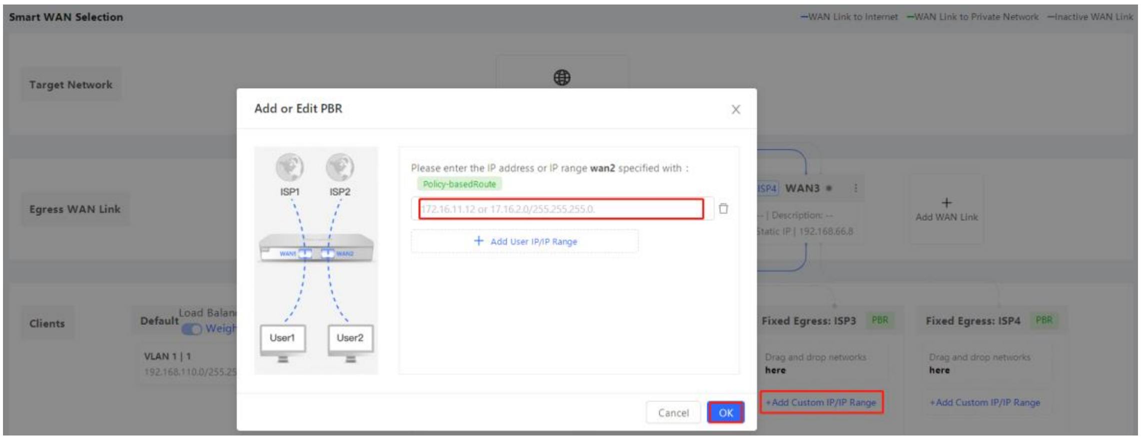
+Add Custom IP/IP Range

Fixed Egress: ISP4 PBR

Drag and drop networks **here**

+Add Custom IP/IP Range

You can also click **Add Custom IP/IP Range**, for example, add an IP address or IP address range for **Fixed Egress: ISP3**.



Add or Edit PBR

Please enter the IP address or IP range **wan2** specified with : Policy-basedRoute

172.16.11.12 or 17.16.2.0/255.255.255.0.

4.4.4 Configuring the Traffic for Accessing a Private Line Server to Go Through a Private Line

1. Demand

A company's network connects to three Internet broadband lines: ISP1, ISP2, and ISP3 lines, and the company has a financial private line. The financial software on the intranet can normally access the financial server through the financial private line and all devices can access the Internet through the ISP lines.

2. Configuration Ideas

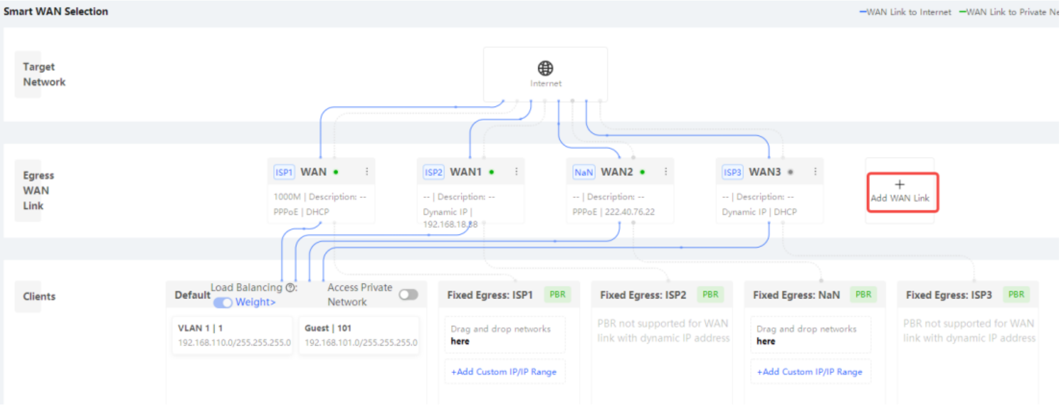
(1) Configure a static IP address for the WAN3 port and select the private line.

(2) There are two policies available for private networks:

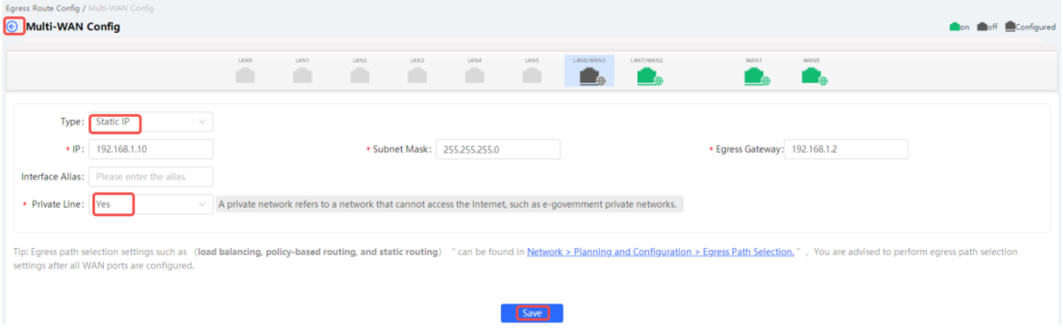
- Specifying the destination network: When all users access the Internet, the traffic for accessing the specified destination network (such as the server IP address) is transmitted through the private line and other traffic is not transmitted through the private line.
- Specifying Intranet users: When specified Intranet users access the Internet, the traffic of the users is transmitted through the private line and the traffic of other users is not transmitted through the private line.

3. Configuration Steps

(1) Click **Add WAN Link** to go to the **Multi-WAN Config** page.



(2) Configure Internet access type for the WAN port based on the operator's requirements. **Type** can be set to **Static IP** for private lines. Set **Private Line** to **Yes**, click **Save**, and then click the back arrow on the right of **Multi-WAN Config** at the upper right corner.



Type: Static IP

* IP: 192.168.1.10 * Subnet Mask: 255.255.255.0 * Egress Gateway: 192.168.1.2

Interface Alias: Please enter the alias.

* Private Line: Yes A private network refers to a network that cannot access the Internet, such as e-government private networks.

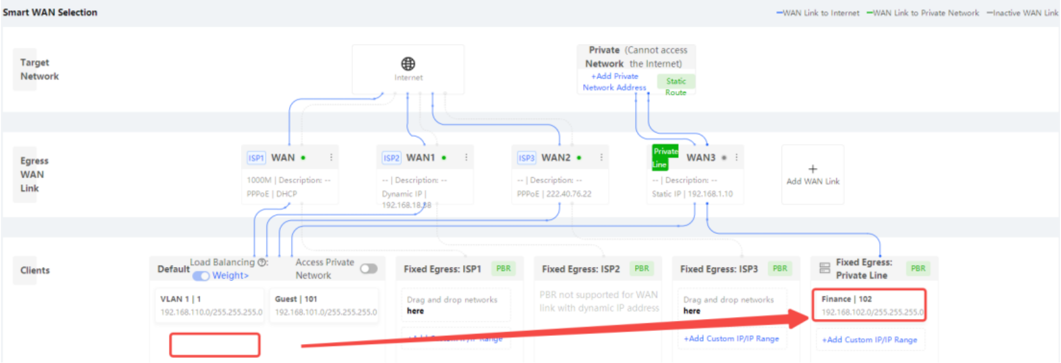
Tip: Egress path selection settings such as (**load balancing, policy-based routing, and static routing**) " can be found in Network > Planning and Configuration > Egress Path Selection. " , You are advised to perform egress path selection settings after all WAN ports are configured.

Save

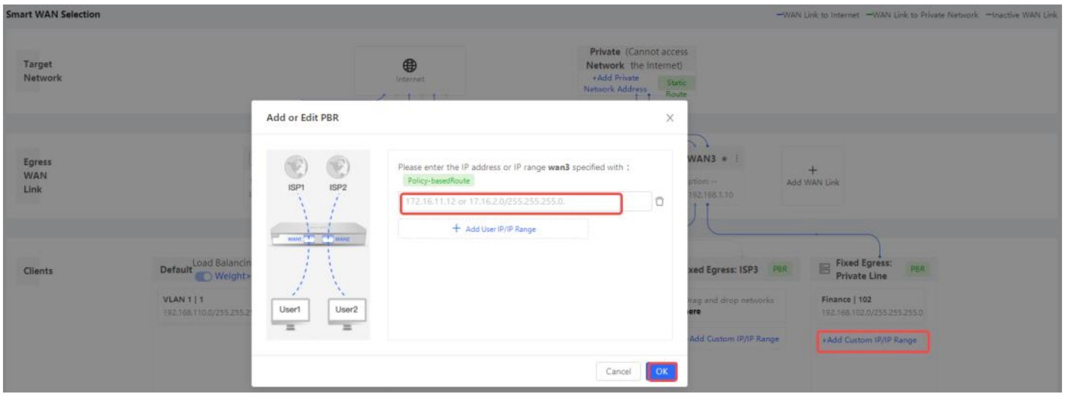
Note

- Private lines can be selected only for static IP addresses. After the private line is enabled, the device will forward traffic according to the policy (specifying users or specifying private line resources) specified for the private line.

(3) Policy 1: Allow some users to only access the private line. You can drag a created VLAN to the **Fixed Egress: Private Line** module.

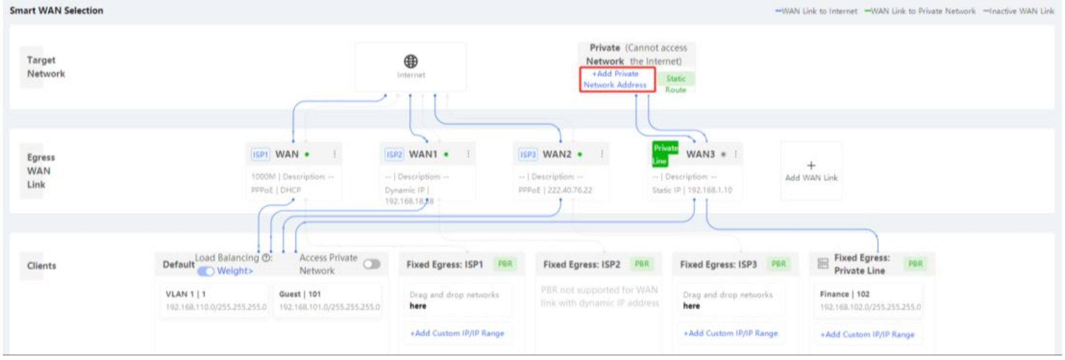


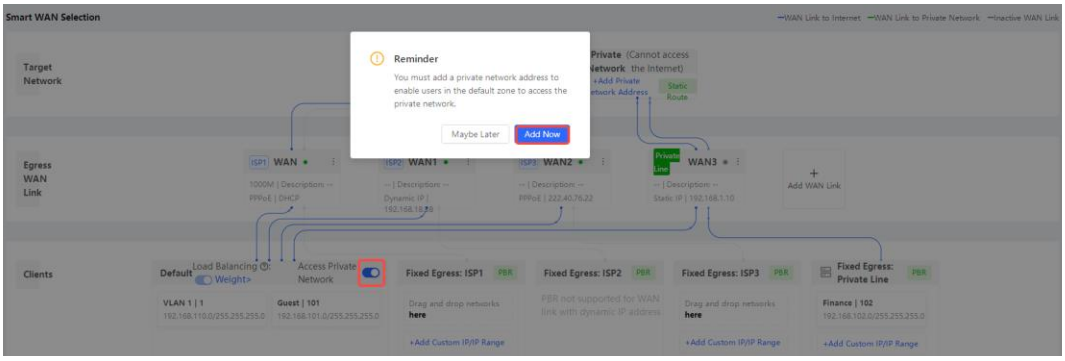
You can also click **Add Custom IP/IP Range** to add an IP address or IP address segment.



(4) Policy 2: Allow the default service network to access the private line.

Click **Add Private Network Address** or set **Access Private Network** to **On** to go to the **Add or Edit Private Network Address** page.





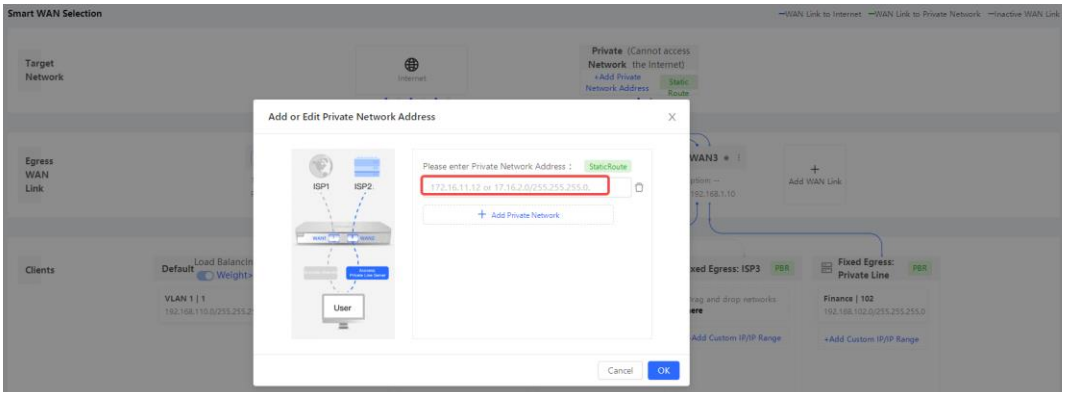
Reminder

You must add a private network address to enable users in the default zone to access the private network.

Edit the destination network specified for the private line (you need to specify the address or address segment of the private line you want to access, such as the tax network or medical network; you can set multiple addresses).

Note

- The address should be as accurate as possible to avoid selecting the private network for the normal Internet access and affecting the normal Internet access service.



Add or Edit Private Network Address

Please enter Private Network Address : 172.16.11.12 or 17.16.2.0/255.255.255.0.

5 Optimization Configuration

5.1 Wi-Fi Optimization

Overview

Wi-Fi optimization is an intelligent and automatic RF optimization scheme tailored for complex scenarios with multiple APs. This function is supported by enterprise APs, most Reyee APs, and EGs. After the device enabled with Wi-Fi optimization collects spatial information, including the SSID, channel, signal strength, and client status (for example, transfer rate, delay, packet loss rate), it analyses information through the intelligent algorithm to provide the optimal network solution (channel and power planning for each AP), and automatically adjusts the configuration of APs on the network.

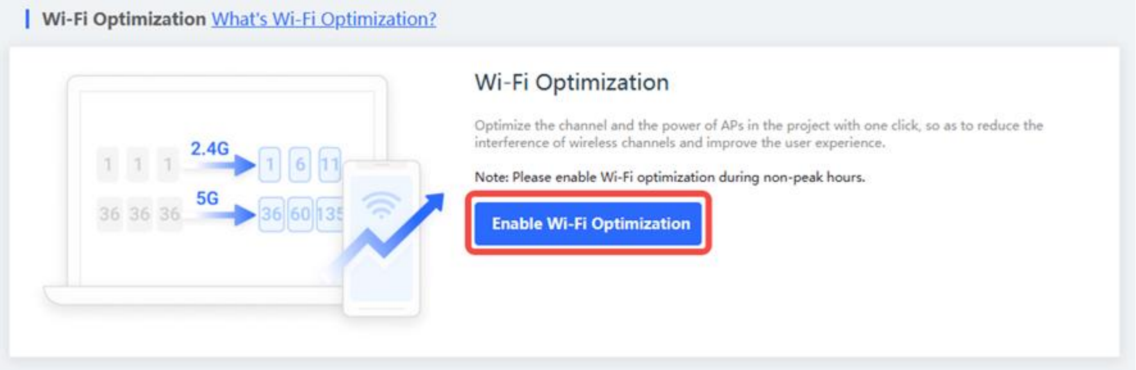
Wi-Fi optimization is applicable to the following scenarios:

- In the scenario where over 100 APs need to be optimized, auto channel optimization does not achieve good roaming effect, and it takes too much time to manually adjust the channel and power.
- In an office with dozens of APs where network connections are unstable for some PCs or phones, clients may experience web buffering and low speed. Wireless network optimization is time- and labor-consuming.

Procedure

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Network-Wide** > **Optimization** > **Wi-Fi Optimization** and select a network in this account.

(2) Click **Enable Wi-Fi optimization**.



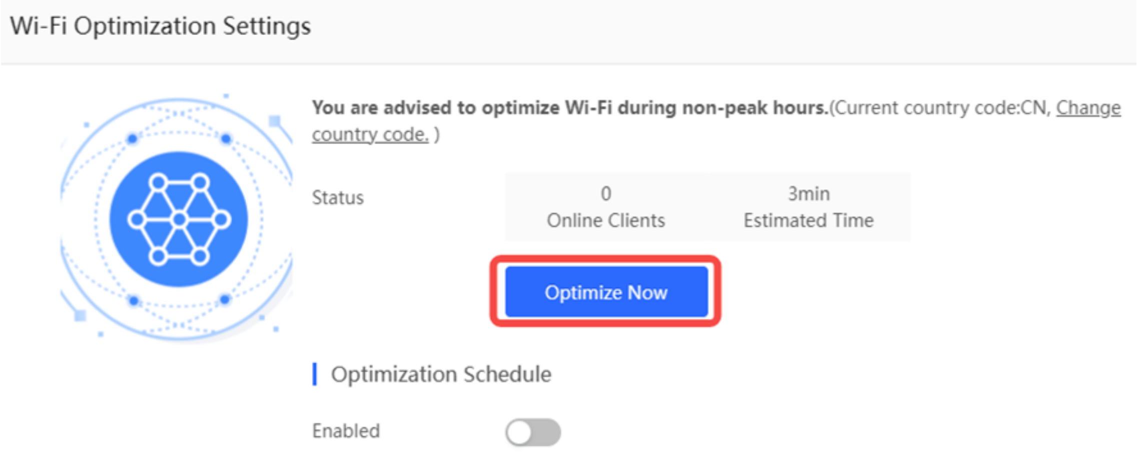
Wi-Fi Optimization What's Wi-Fi Optimization?

Wi-Fi Optimization

Optimize the channel and the power of APs in the project with one click, so as to reduce the interference of wireless channels and improve the user experience.

Note: Please enable Wi-Fi optimization during non-peak hours.

(3) Click **Optimize Now** to start optimization.



Wi-Fi Optimization Settings

You are advised to optimize Wi-Fi during non-peak hours.(Current country code:CN, Change country code.)

Status	0 Online Clients	3min Estimated Time

Optimization Schedule

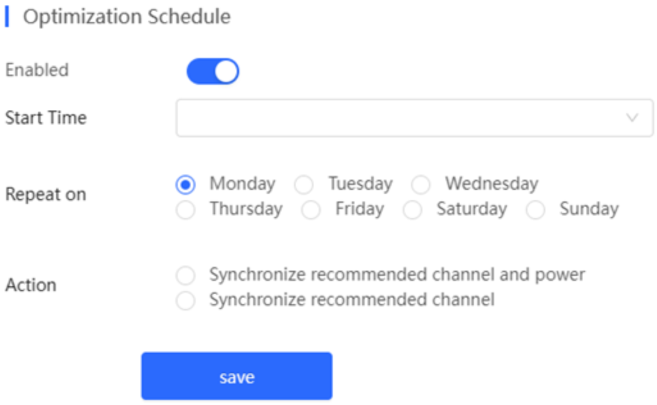
Enabled: Off

Online Clients: indicates the number of all online wireless clients.

Estimated Time: indicates the estimated time to complete optimization.

Optimization Schedule: enables or disables scheduled optimization. You are advised to optimize Wi-Fi during non-peak hours.

If you want set scheduled optimization, enable **Optimization Schedule**, set the optimization time and action, and click **Save**.



Optimization Schedule

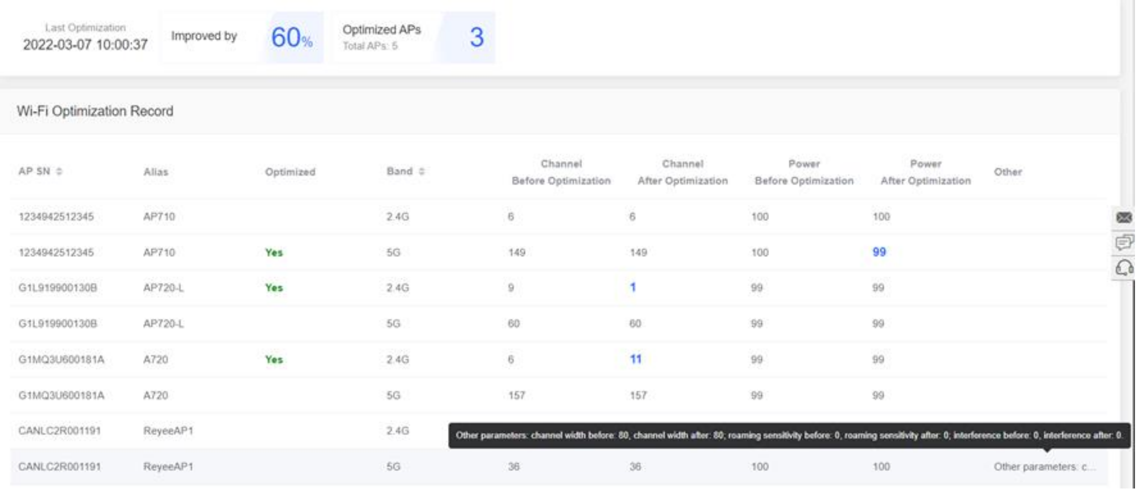
Enabled: On

Start Time:

Repeat on: ● Monday ○ Tuesday ○ Wednesday ○ Thursday ○ Friday ○ Saturday ○ Sunday

Action: ○ Synchronize recommended channel and power ○ Synchronize recommended channel

(4) After the optimization is complete, the browser displays the optimization details.



Last Optimization 2022-03-07 10:00:37

Improved by 60%

Optimized APs 3

Total APs: 5

Wi-Fi Optimization Record

AP SN	Alias	Optimized	Band	Channel Before Optimization	Channel After Optimization	Power Before Optimization	Power After Optimization	Other
1234942512345	AP710		2.4G	6	6	100	100	
1234942512345	AP710	Yes	5G	149	149	100	99	
G1L919900130B	AP720-L	Yes	2.4G	9	1	99	99	
G1L919900130B	AP720-L		5G	60	60	99	99	
G1MQ3U600181A	A720	Yes	2.4G	6	11	99	99	
G1MQ3U600181A	A720		5G	157	157	99	99	
CANLC2R001191	ReyeeAP1		2.4G					
CANLC2R001191	ReyeeAP1		5G	36	36	100	100	Other parameters: c...

Other parameters: channel width before: 80, channel width after: 80; roaming sensitivity before: 0, roaming sensitivity after: 0; interference before: 0, interference after: 0.

Last Optimization: indicates the time of last optimization.

Improved by: indicates the improved device percentage.

Optimized APs: indicates the number of optimized devices.

AP SN: indicates the serial number of an AP.

Alias: indicates the description of an AP.

Optimized: indicates the optimized result.

Band: indicates the optimized wireless band.

Channel Before Optimization: indicates the wireless channel before optimization.

Channel After Optimization: indicates the wireless channel after optimization.

Power Before Optimization: indicates the local power before optimization.

Power after Optimization: indicates the local power after optimization.

Other: indicates other parameters for Reyee devices. The parameters are as follows:

- **Channel width before**: indicates the channel width before optimization.
- **Channel width after**: indicates the channel width after optimization.
- **Roaming sensitivity before**: indicates the roaming sensitivity before optimization.
- **Roaming sensitivity after**: indicates the roaming sensitivity after optimization.
- **Interference before**: indicates the interference before optimization.
- **Interference after**: indicates the interference after optimization.

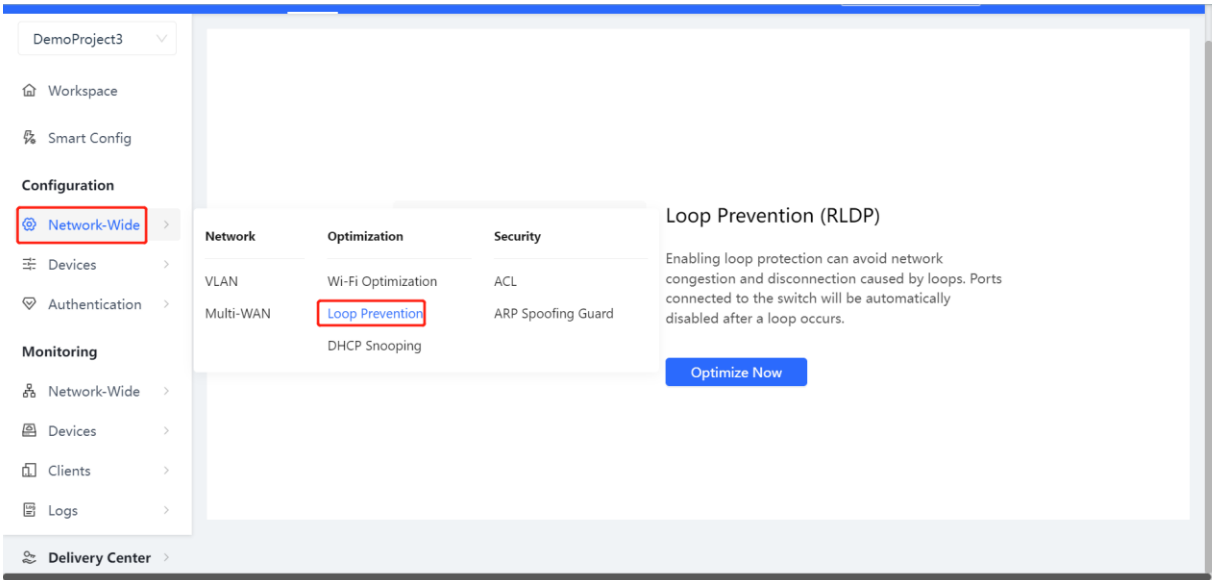
5.2 Loop Prevention

5.2.1 Overview

Enabling loop prevention can avoid network congestion and disconnection caused by loops. Ports connected to the switch will be automatically disabled after a loop occurs.

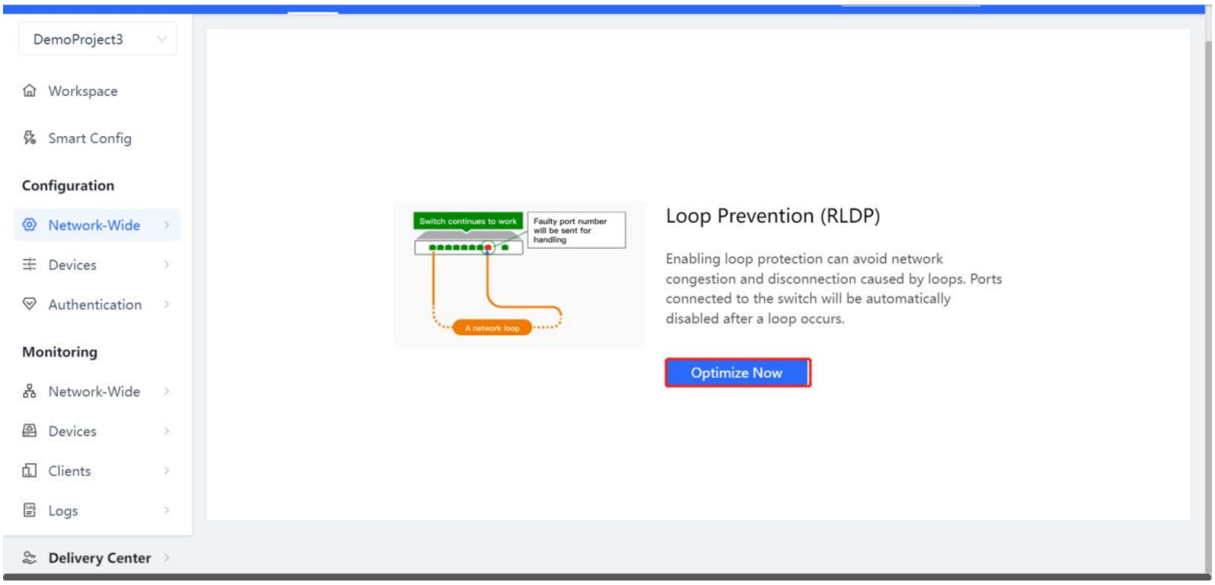
5.2.2 Configuration Steps

Choose **Configuration** > **Network-Wide** > **Optimization** > **Loop Prevention**.



Loop Prevention (RLDP)

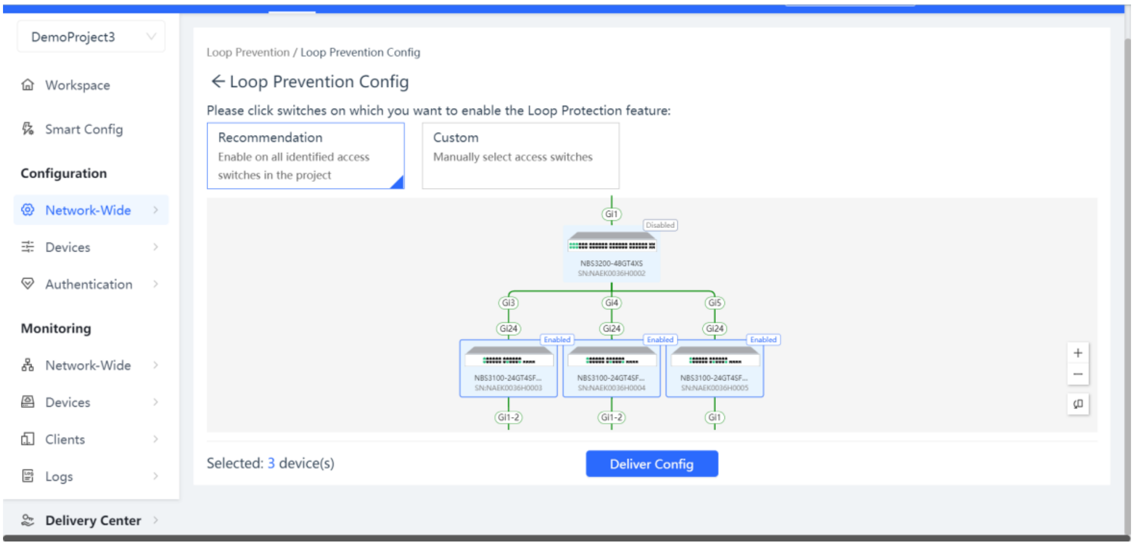
Enabling loop protection can avoid network congestion and disconnection caused by loops. Ports connected to the switch will be automatically disabled after a loop occurs.



Loop Prevention (RLDP)

Enabling loop protection can avoid network congestion and disconnection caused by loops. Ports connected to the switch will be automatically disabled after a loop occurs.

Click **Optimize Now**. You are advised to use the default value. Click **Deliver Config**.



Loop Prevention / Loop Prevention Config

← Loop Prevention Config

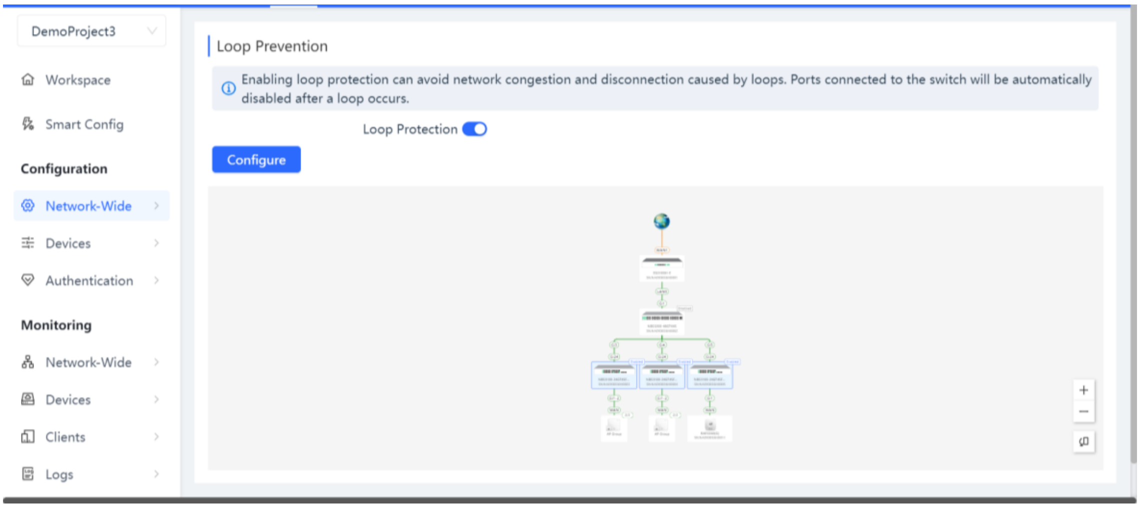
Please click switches on which you want to enable the Loop Protection feature:

Recommendation
Enable on all identified access switches in the project

Custom
Manually select access switches

Selected: 3 device(s)

Deliver Config



Loop Prevention

ⓘ Enabling loop protection can avoid network congestion and disconnection caused by loops. Ports connected to the switch will be automatically disabled after a loop occurs.

Loop Protection ●

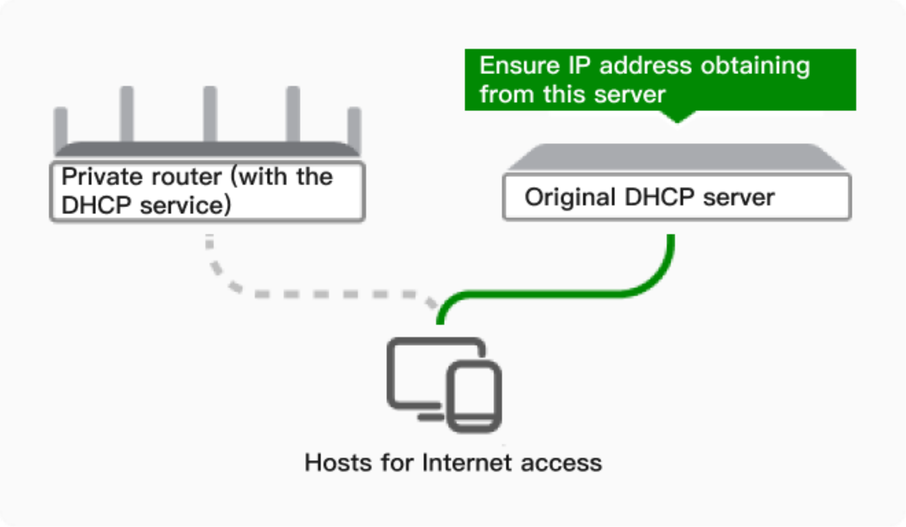
Configure

5.3 DHCP Snooping

5.3.1 Overview

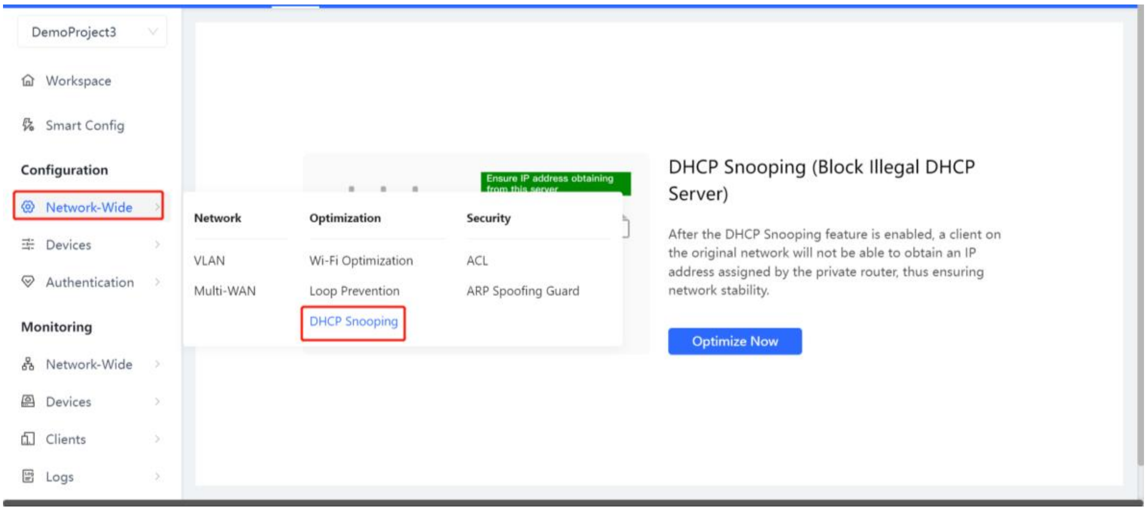
If a private router is connected to the network, some clients may obtain incorrect IP addresses and fail to access the Internet.

After the DHCP Snooping feature is enabled, a client on the original network will not be able to obtain an IP address assigned by the private router, thus ensuring network stability.


Ensure IP address obtaining from this server
Private router (with the DHCP service)
Original DHCP server
Hosts for Internet access

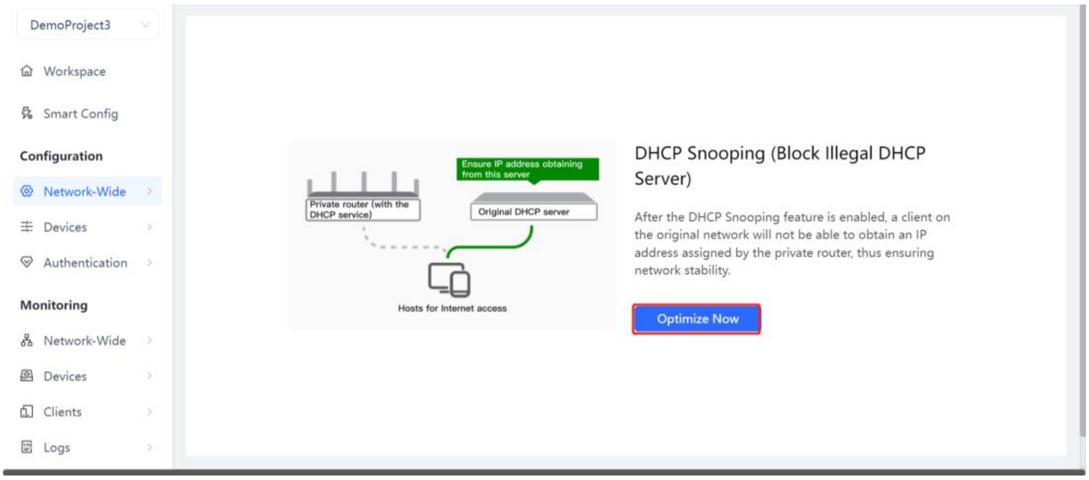
5.3.2 Configuration Steps

Choose **Configuration** > **Network-Wide** > **Optimization** > **DHCP Snooping**.



DHCP Snooping (Block Illegal DHCP Server)

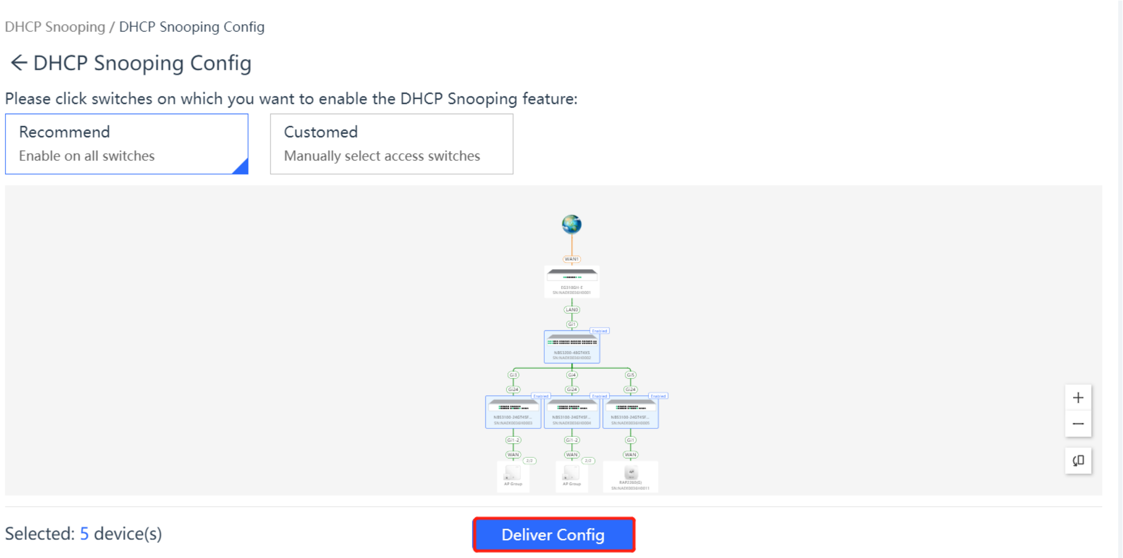
After the DHCP Snooping feature is enabled, a client on the original network will not be able to obtain an IP address assigned by the private router, thus ensuring network stability.



DHCP Snooping (Block Illegal DHCP Server)

After the DHCP Snooping feature is enabled, a client on the original network will not be able to obtain an IP address assigned by the private router, thus ensuring network stability.

Click **Optimize Now**. You are advised to use the default value. Click **Deliver Config**.

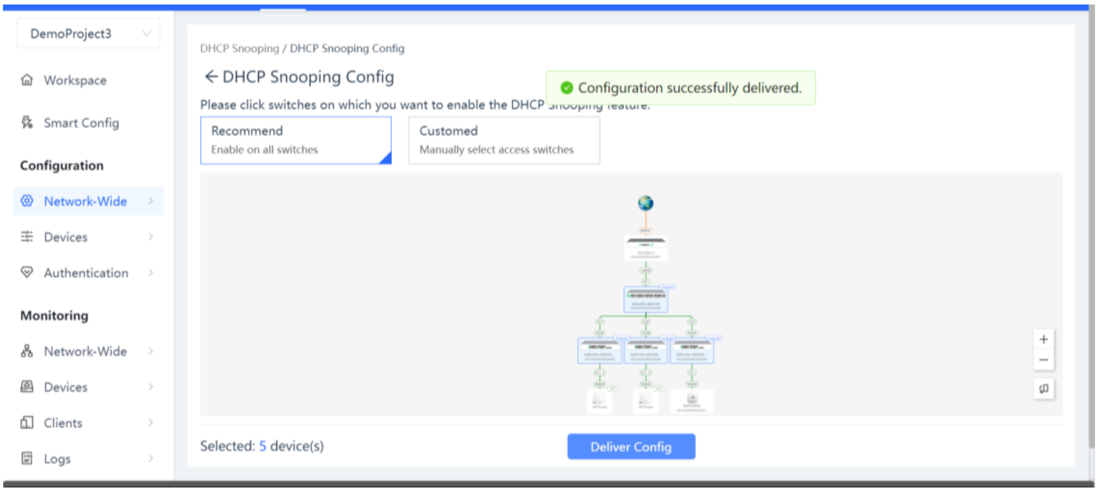


DHCP Snooping / DHCP Snooping Config

← DHCP Snooping Config

Please click switches on which you want to enable the DHCP Snooping feature:

Selected: 5 device(s)



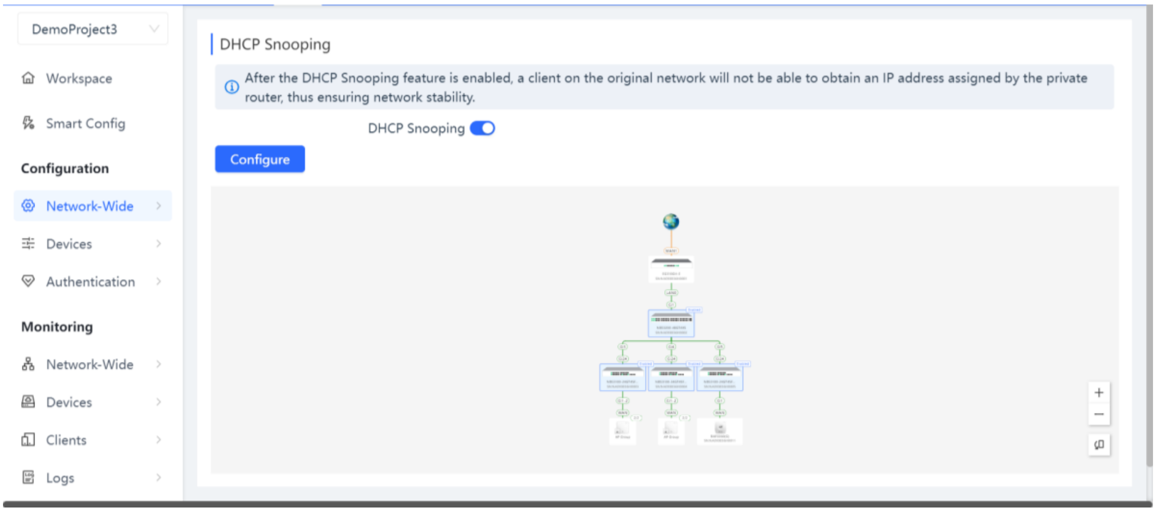
DHCP Snooping / DHCP Snooping Config

← DHCP Snooping Config

Configuration successfully delivered.

Please click switches on which you want to enable the DHCP Snooping feature:

Selected: 5 device(s)



DHCP Snooping

After the DHCP Snooping feature is enabled, a client on the original network will not be able to obtain an IP address assigned by the private router, thus ensuring network stability.

DHCP Snooping ●

5.4 Traffic Control

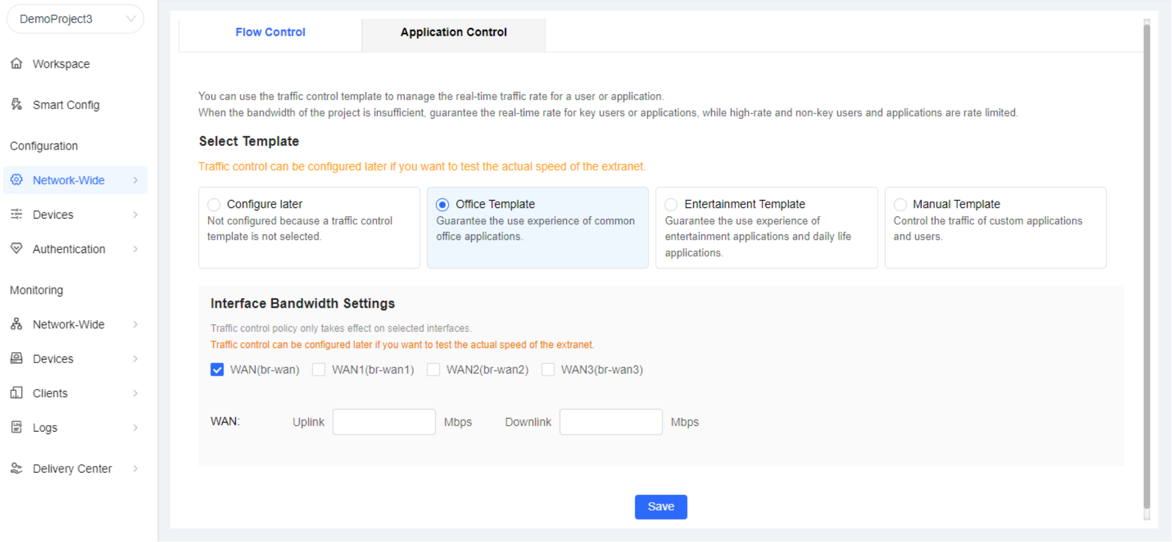
Set real-time traffic rate for a user or an application.

When the bandwidth of the project is insufficient, guarantee the real-time rate for key users or applications, while high-rate and non-key users and applications are rate limited.

You can use the traffic control template to manage the real-time traffic rate for a user or application.

When the bandwidth of the project is insufficient, guarantee the real-time rate for key users or applications, while high-rate and non-key users and applications are rate limited.

1. Click Interface Bandwidth Setting.



You can use the traffic control template to manage the real-time traffic rate for a user or application.
When the bandwidth of the project is insufficient, guarantee the real-time rate for key users or applications, while high-rate and non-key users and applications are rate limited.

Select Template

Traffic control can be configured later if you want to test the actual speed of the extranet.

○ Configure later
Not configured because a traffic control template is not selected.

● Office Template
Guarantee the use experience of common office applications.

○ Entertainment Template
Guarantee the use experience of entertainment applications and daily life applications.

○ Manual Template
Control the traffic of custom applications and users.

Interface Bandwidth Settings

Traffic control policy only takes effect on selected interfaces.
Traffic control can be configured later if you want to test the actual speed of the extranet.

☑ WAN(br-wan) □ WAN1(br-wan1) □ WAN2(br-wan2) □ WAN3(br-wan3)

WAN: Uplink Mbps Downlink Mbps

2. Select a template.

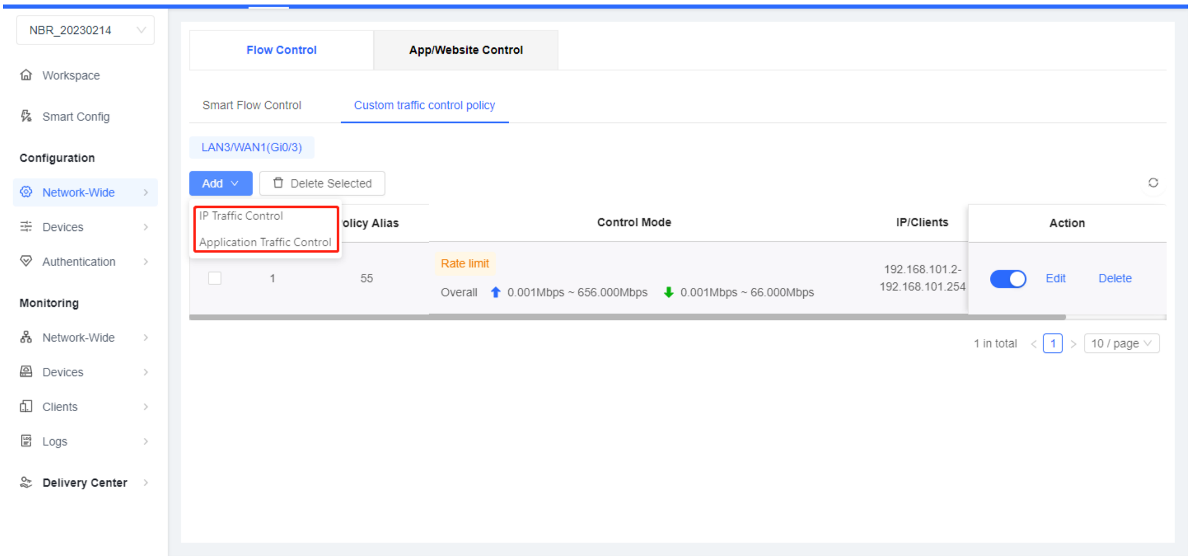
Configure later: indicates that traffic control is disabled.

Office Template: indicates that the embedded smart traffic control policy guarantees the traffic of common office and work applications, and user-defined policies can be added.

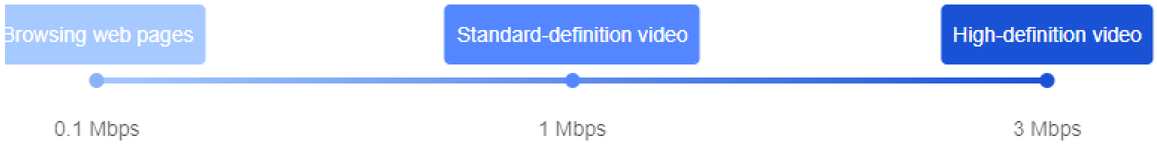
Entertainment Template: indicates that the embedded smart traffic control policy guarantees the traffic of entertainment and common daily life applications, and user-defined policies can be added.

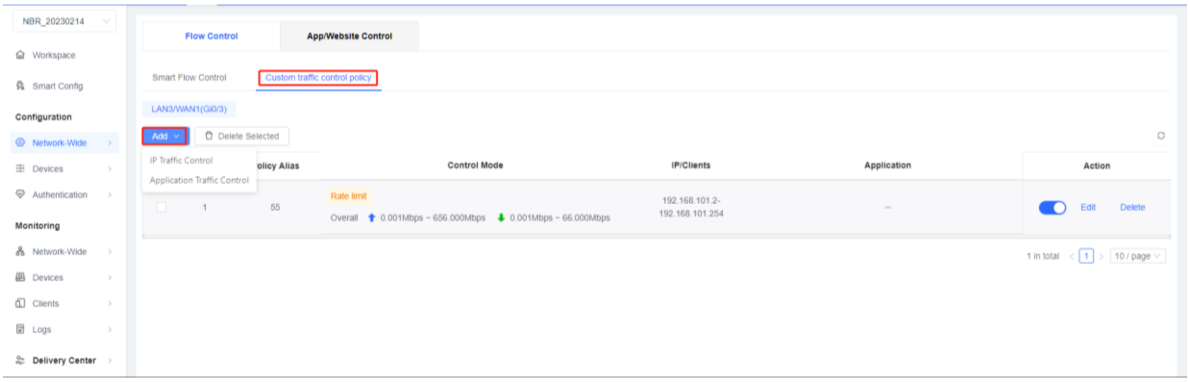
Manual Template: indicates that traffic control settings are customized and a traffic control policy is manually added.

3. Add a custom traffic control policy.



4. Configure a traffic control policy: When the bandwidth reaches 3 Mbps, a user can watch high-definition videos smoothly; when the bandwidth reaches 1 Mbps, a user can watch standard-definition videos smoothly; when the bandwidth reaches 0.1 Mbps, a user can browse Web pages smoothly.





5.4.1 IP Traffic Control

Select IP: Select the IP address range, in which the traffic control policy takes effect.

Select Traffic Control Mode: Select **Rate limit** or **No rate limit**.

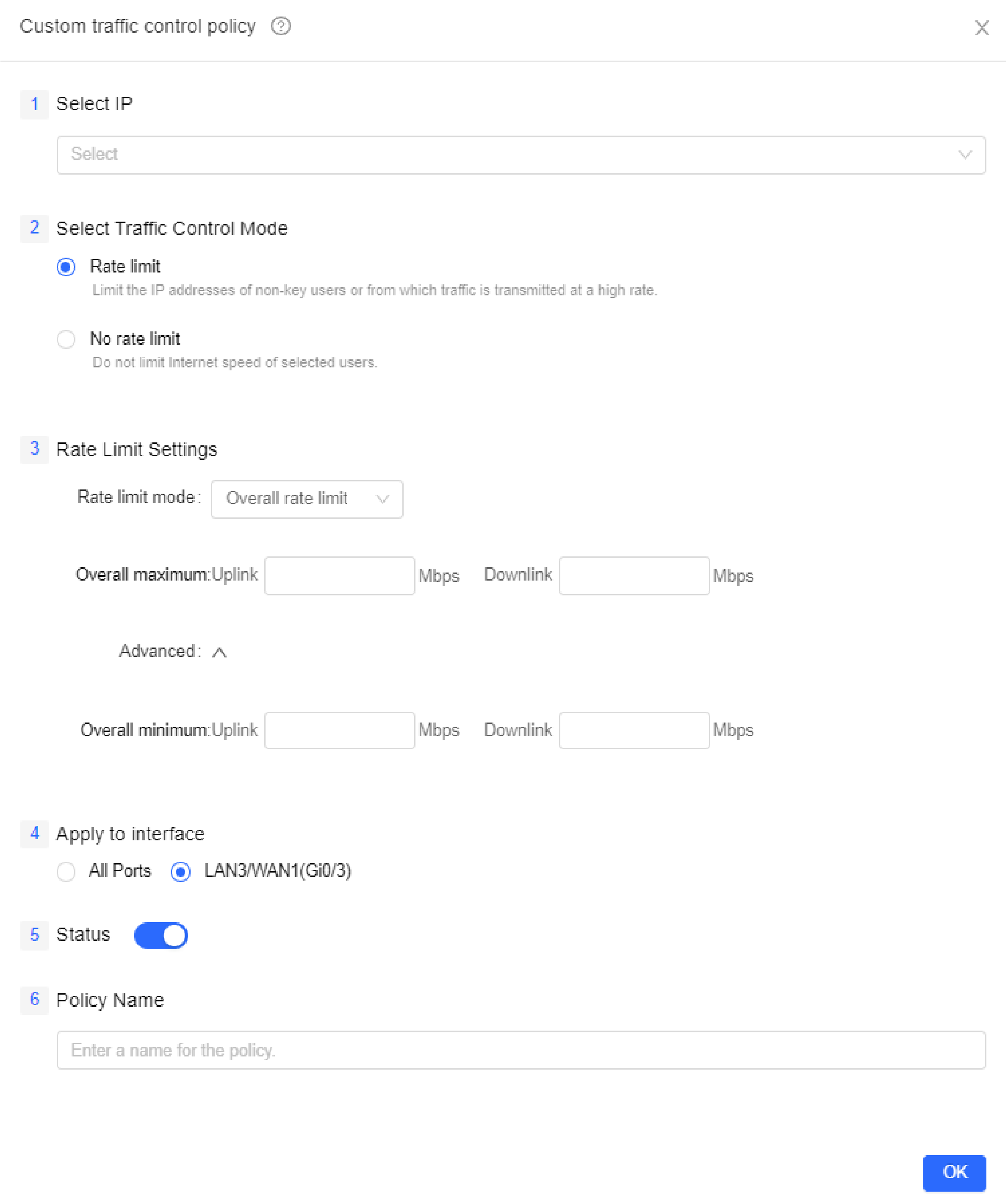
Rate Limit Settings: **Overall rate limit** indicates the overall maximum rate and **Per IP rate limit** indicates the maximum rate for each IP address.

Overall maximum/**Per IP maximum**: indicates the uplink and downlink maximum rates, in Mbps.

Overall minimum in the **Advanced** area: indicates the guaranteed rate for users when the bandwidth is insufficient.

Apply to interface: indicates the port, in which the policy takes effect. You are advised to select **All Ports**.

Policy Name: Configure a name for the policy to facilitate maintenance.



Custom traffic control policy

1 Select IP

Select

2 Select Traffic Control Mode

● Rate limit

Limit the IP addresses of non-key users or from which traffic is transmitted at a high rate.

○ No rate limit

Do not limit Internet speed of selected users.

3 Rate Limit Settings

Rate limit mode: Overall rate limit

Overall maximum: Uplink Mbps Downlink Mbps

Advanced:

Overall minimum: Uplink Mbps Downlink Mbps

4 Apply to interface

○ All Ports ● LAN3/WAN1(Gi0/3)

5 Status

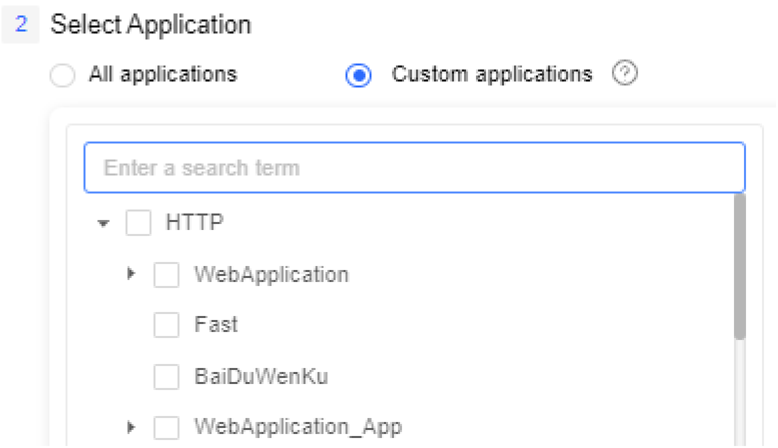
6 Policy Name

Enter a name for the policy.

5.4.2 Application Traffic Control

Select IP: Select the IP address range, in which the traffic control policy takes effect.

Select Application: Select the application whose traffic needs to be controlled. You can enter keywords for search.



2 Select Application

○ All applications ● Custom applications

Enter a search term

□ HTTP

□ WebApplication

□ Fast

□ BaiDuWenKu

□ WebApplication_App

Select Traffic Control Mode: Select **Rate limit** or **No rate limit**.

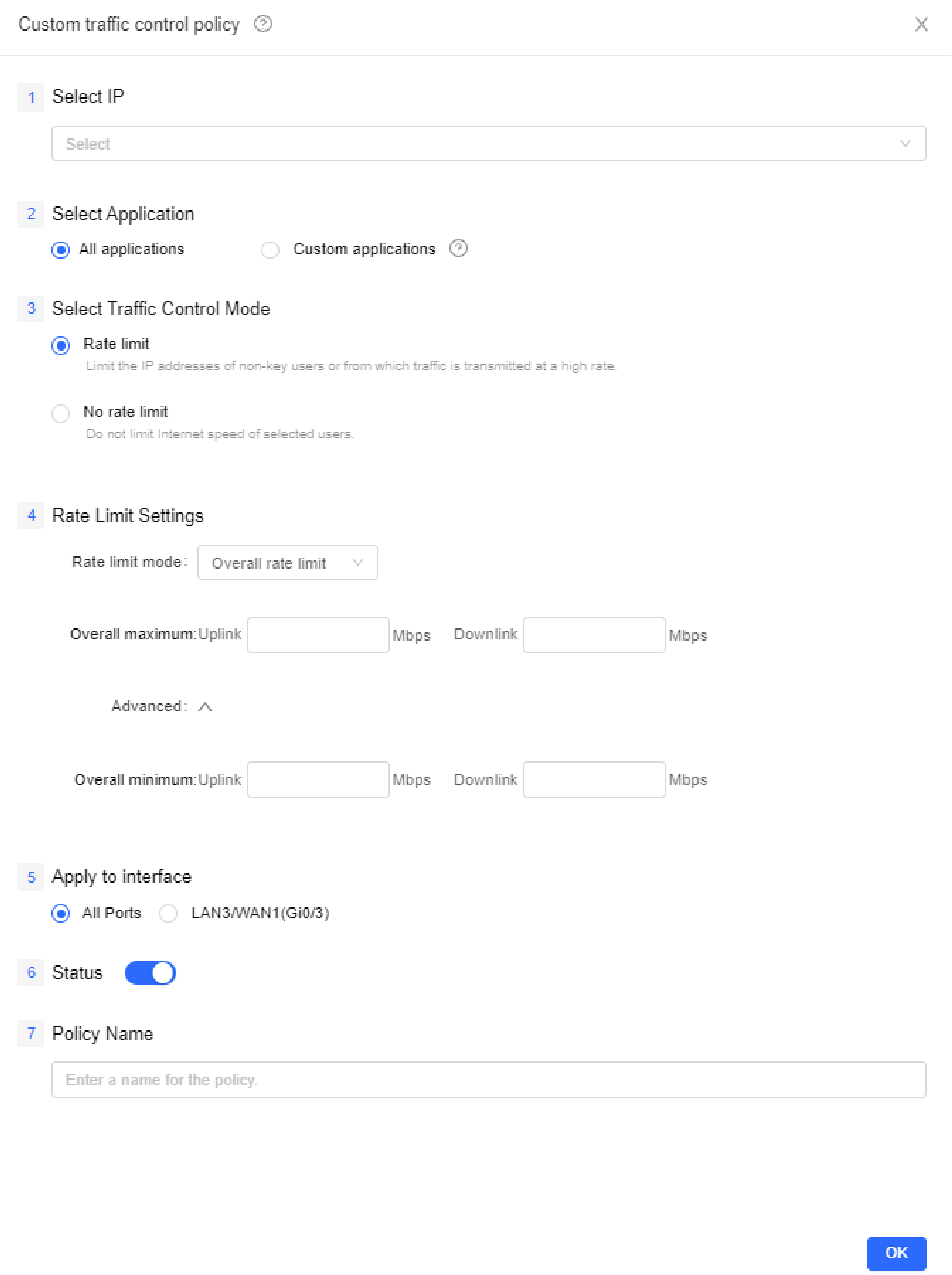
Rate Limit Settings: **Overall rate limit** indicates the overall maximum rate and **Per IP rate limit** indicates the maximum rate for each IP address.

Overall maximum/**Per IP maximum**: indicates the uplink and downlink maximum rates, in Mbps.

Overall minimum in the **Advanced** area: indicates the guaranteed rate for users when the bandwidth is insufficient.

Apply to interface: indicates the port, in which the policy takes effect. You are advised to select **All Ports**.

Policy Name: Configure a name for the policy to facilitate maintenance.



Custom traffic control policy

1 Select IP

Select

2 Select Application

● All applications ○ Custom applications

3 Select Traffic Control Mode

● Rate limit

Limit the IP addresses of non-key users or from which traffic is transmitted at a high rate.

○ No rate limit

Do not limit Internet speed of selected users.

4 Rate Limit Settings

Rate limit mode: Overall rate limit

Overall maximum: Uplink Mbps Downlink Mbps

Advanced:

Overall minimum: Uplink Mbps Downlink Mbps

5 Apply to interface

● All Ports ○ LAN3/WAN1(Gi0/3)

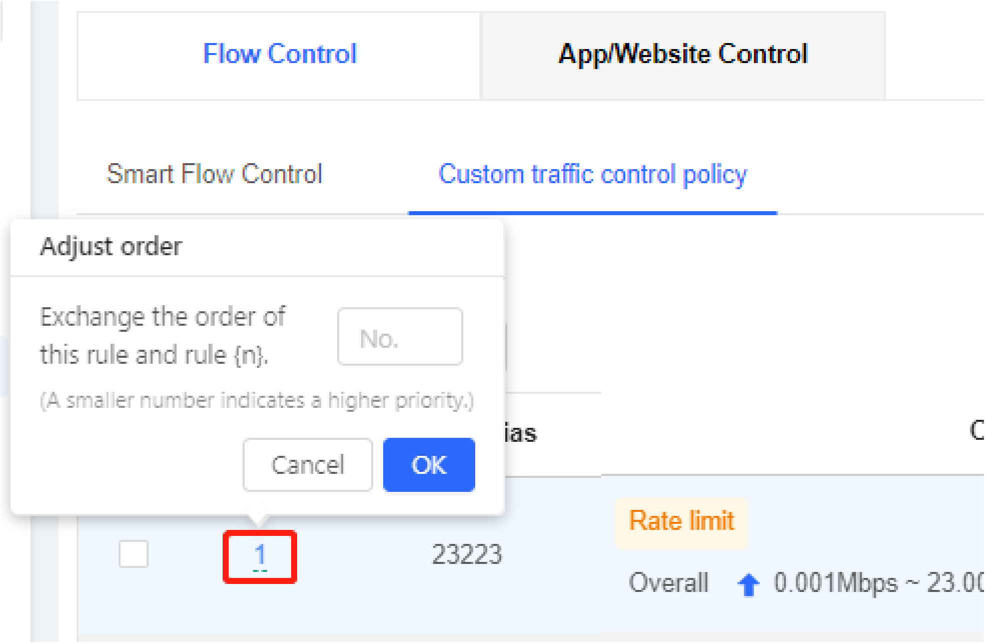
6 Status

7 Policy Name

Enter a name for the policy.

5.4.3 Configuring the Policy Priority

Click the number of a policy to adjust the policy sequence. A smaller number indicates a higher priority.



Adjust order

Exchange the order of this rule and rule {n}. No.

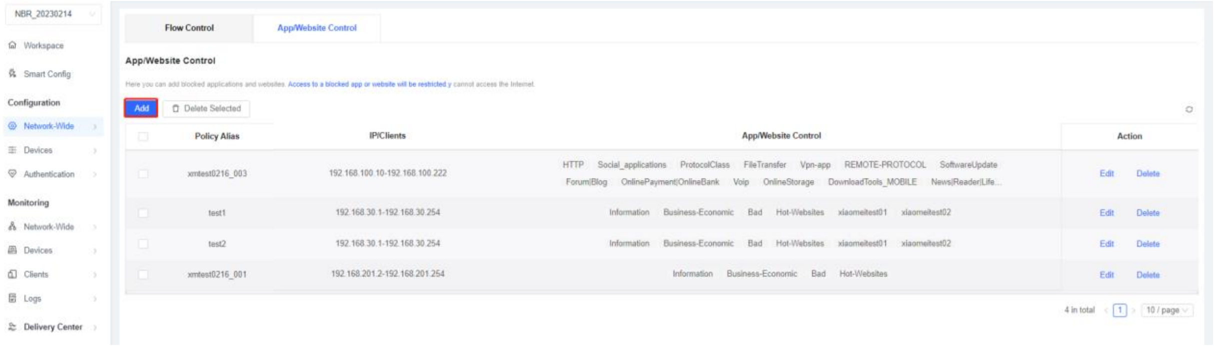
(A smaller number indicates a higher priority.)

□	1	23223	Rate limit Overall 0.001Mbps ~ 23.0(

5.4.4 App/Website Control

Here you can add blocked applications and websites. Access to a blocked app or website will be restricted.

1. Choose **Project** > **Network-Wide** > **Traffic Control** > **App/Website Control** and click **Add**.



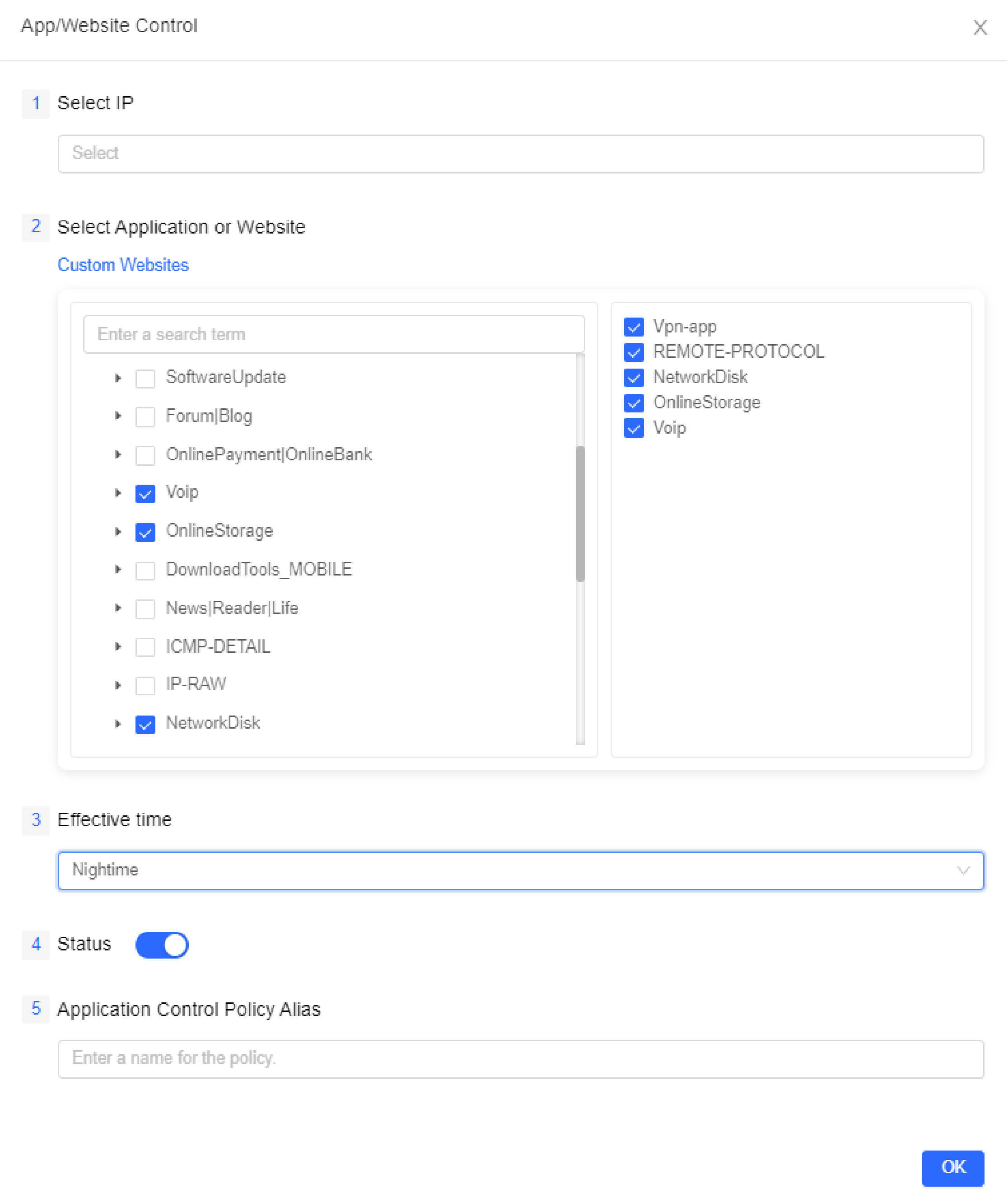
App/Website Control

Here you can add blocked applications and websites. Access to a blocked app or website will be restricted y cannot access the Internet.

□	Policy Alias	IP/Clients	App/Website Control	Action
□	xmtest0216_003	192.168.100.10-192.168.100.222	HTTP Social_applications ProtocolClass FileTransfer Vpn-app REMOTE-PROTOCOL SoftwareUpdate Forum|Blog OnlinePayment|OnlineBank Voip OnlineStorage DownloadTools_MOBILE News|Reader|Life...	Edit Delete
□	test1	192.168.30.1-192.168.30.254	Information Business-Economic Bad Hot-Websites xiaomeitest01 xiaomeitest02	Edit Delete
□	test2	192.168.30.1-192.168.30.254	Information Business-Economic Bad Hot-Websites xiaomeitest01 xiaomeitest02	Edit Delete
□	xmtest0216_001	192.168.201.2-192.168.201.254	Information Business-Economic Bad Hot-Websites	Edit Delete

4 in total < 1 > 10 / page

2. Configure a policy.



App/Website Control

1 Select IP

Select

2 Select Application or Website

Custom Websites

Enter a search term

- □ SoftwareUpdate
- □ Forum|Blog
- □ OnlinePayment|OnlineBank
- ☑ Voip
- ☑ OnlineStorage
- □ DownloadTools_MOBILE
- □ News|Reader|Life
- □ ICMP-DETAIL
- □ IP-RAW
- ☑ NetworkDisk

- ☑ Vpn-app
- ☑ REMOTE-PROTOCOL
- ☑ NetworkDisk
- ☑ OnlineStorage
- ☑ Voip

3 Effective time

Nightime

4 Status ●

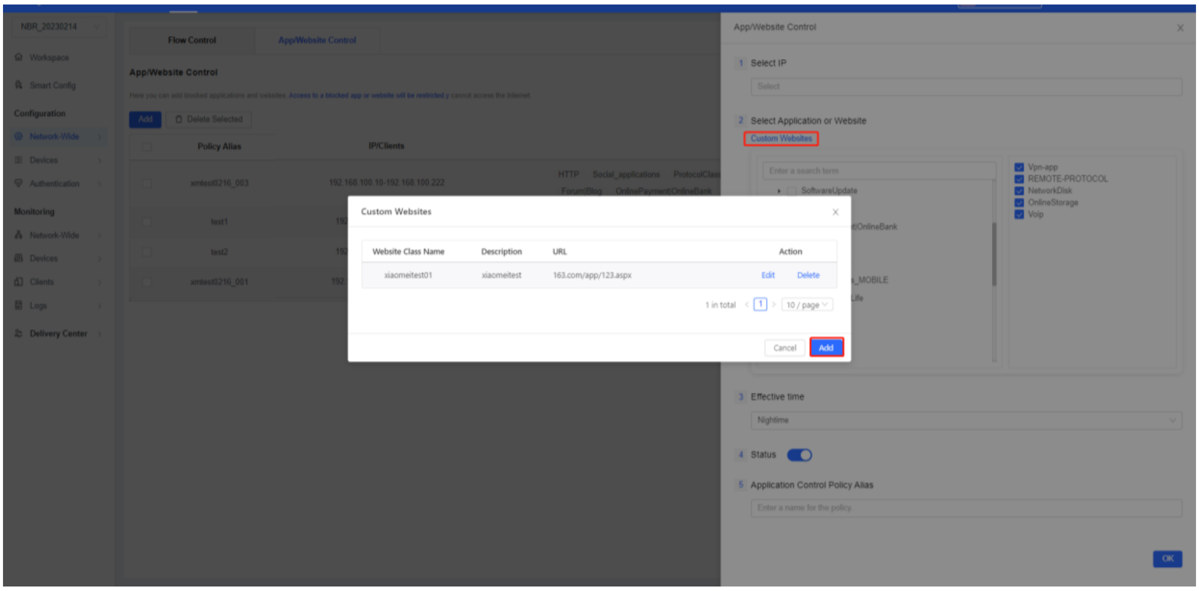
5 Application Control Policy Alias

Enter a name for the policy.

OK

Select IP: Select the IP address range, in which the policy does not take effect.

Select Application or Website: Select an application or website to be blocked. You can click **Custom Websites** to add the website domain name to be blocked.



Custom Websites

Website Class Name	Description	URL	Action
xiaomeitest01	xiaomeitest	163.com/app/123.aspx	Edit Delete

1 in total < 1 > 10 / page

Cancel Add

Note

- URLs support two levels of directories at most, for example, www.ruijie.com.cn/about/summary.aspx.URLs must be separated by either a carriage return character or a comma. URL prefixes such as http:// or https:// are not required.

Effective time: Select the time when the policy takes effect.

Application Control Policy Alias: Enter the policy comment to facilitate maintenance.

6 Security Configuration

6.1 Network Access Control (simplified)

6.1.1 Applicable Scenarios

There are various types of users on the network. To ensure security, some users are banned from accessing each other, such as visitors, finance department, servers, and monitoring devices. Service access control can prohibit mutual access between different network segments.

6.1.2 Models of ACL-Supported Products

Product Type	Device Name	Version
Gateway	EG series EG-E series	
Reyee Switch	NBS5100 series NBS5200 series NBS6002 series NBS7003 series NBS7006 series	ReyeeOS 1.86 or later

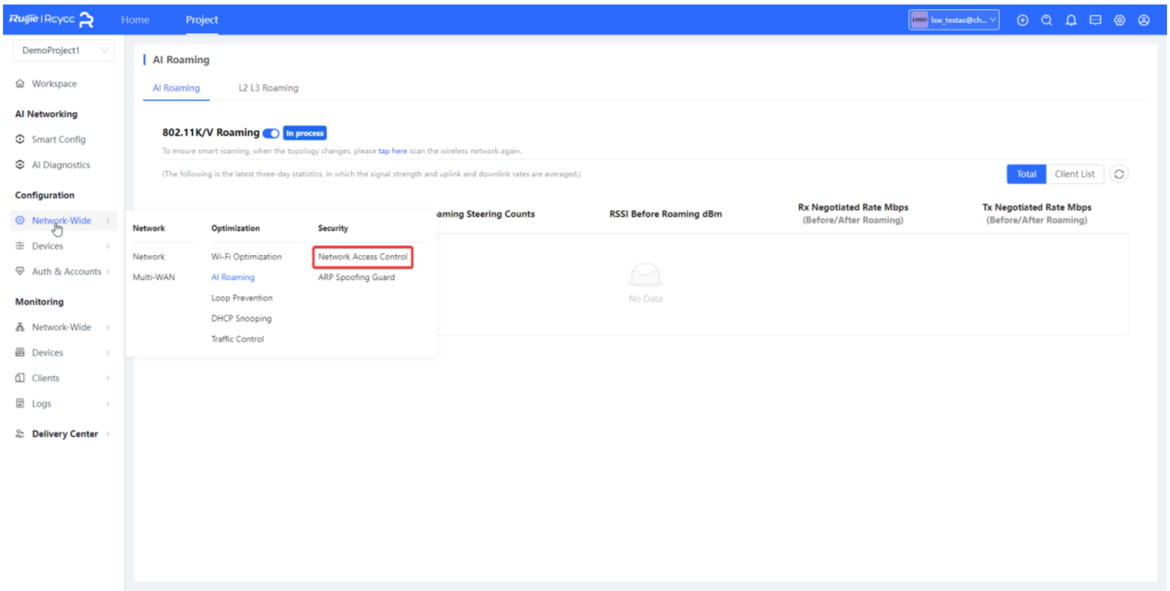
6.1.3 Configuration Steps

1. Creating a Service Network

For details, see 4.1 "Creating a Wired VLAN."

2. Configuring Service Access Control

Choose **Configuration** > **Network-Wide** > **Security** > **Network Access Control**.



(1) Click **To configure** to go to the **Network Access Control** page.

On this page, service networks are divided into two zones based on the access permission of the service networks.

- Interworking Zone

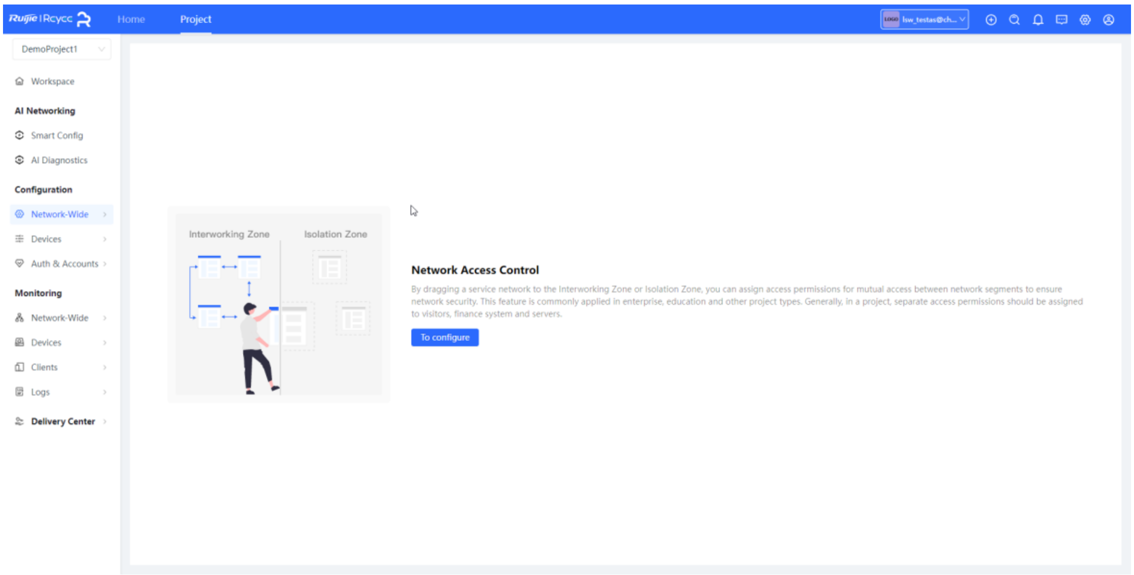
  Service networks in the interworking zone can access each other.

- Isolation Zone

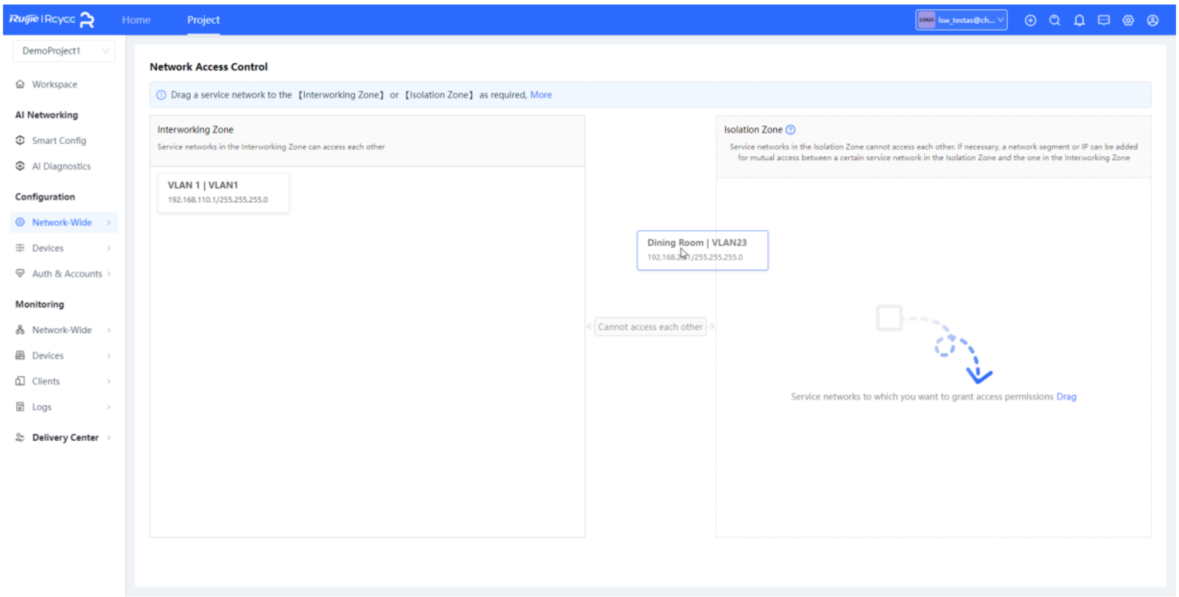
  Service network segments in the isolation zone cannot access those in the interworking zone and vice versa.

  Service network segments in the isolation zone are isolated from each other.

  The ban is bidirectional. For example, if both network segments A and B are banned, A cannot access B, and B cannot access A, either.



By dragging a service network to the Interworking Zone or Isolation Zone, you can assign access permissions for mutual access between network segments to ensure network security. This feature is commonly applied in enterprise, education and other project types. Generally, in a project, separate access permissions should be assigned to visitors, finance system and servers.



Network Access Control

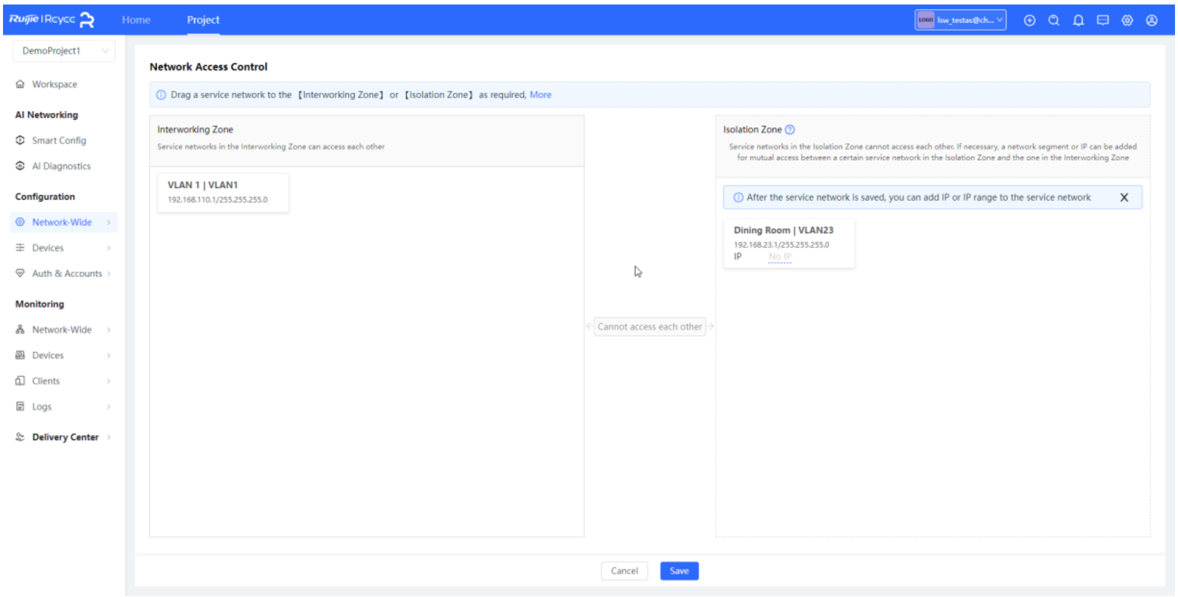
Drag a service network to the 【Interworking Zone】 or 【Isolation Zone】 as required. More

Service networks in the Interworking Zone can access each other

Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for mutual access between a certain service network in the Isolation Zone and the one in the Interworking Zone

Service networks to which you want to grant access permissions Drag

(2) Drag a service network whose access permission needs to be restricted from the interworking zone to the isolation zone and click **Save**.



Network Access Control

Drag a service network to the 【Interworking Zone】 or 【Isolation Zone】 as required. More

Service networks in the Interworking Zone can access each other

Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for mutual access between a certain service network in the Isolation Zone and the one in the Interworking Zone

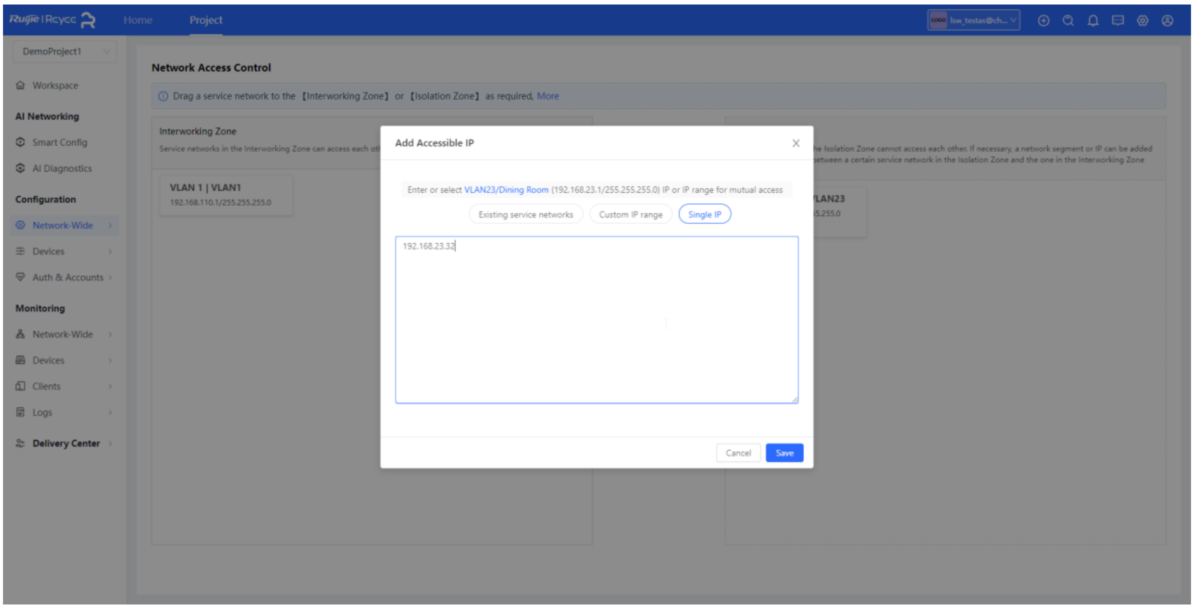
After the service network is saved, you can add IP or IP range to the service network

(3) (Optional) In **Isolation Zone**, click **No IP**.

No IP:

- Exceptional exemption rules have a higher priority than banning rules.
- It is used to exempt a specific IP or network segment, for example, after adding a monitoring network to the isolation zone, you can exempt the administrator IP address and allow it to access other service networks.
- Banning exemption is also bidirectional. For example, if network segment A allows access from IP X, the access from network segment A to IP X and the access from IP X to network segment A are both reachable.

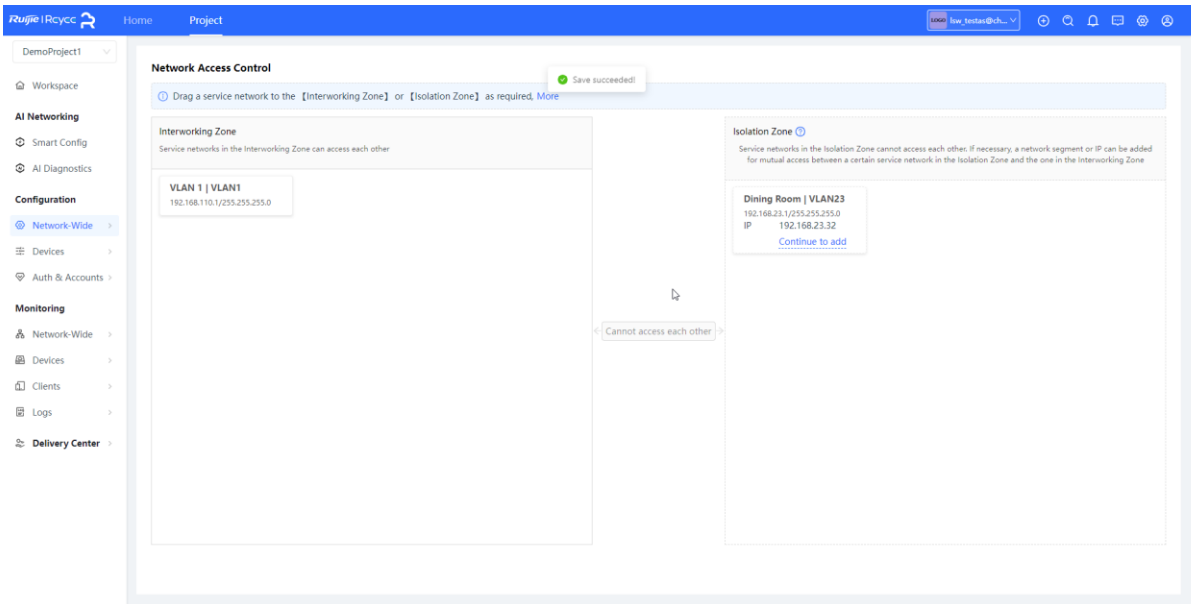
In **Isolation Zone**, select a service network and click **No IP** to go to the **Add Accessible IP** page. Configure the accessible IP address or IP address range and click **Save**.



Add Accessible IP

Enter or select VLAN23/Dining Room (192.168.23.1/255.255.255.0) IP or IP range for mutual access

192.168.23.32



Network Access Control

Save succeeded!

Drag a service network to the 【Interworking Zone】 or 【Isolation Zone】 as required, More

Interworking Zone

Service networks in the Interworking Zone can access each other

VLAN 1 | VLAN1
192.168.110.1/255.255.255.0

Isolation Zone

Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for mutual access between a certain service network in the Isolation Zone and the one in the Interworking Zone

Dining Room | VLAN23
192.168.23.1/255.255.255.0
IP 192.168.23.32

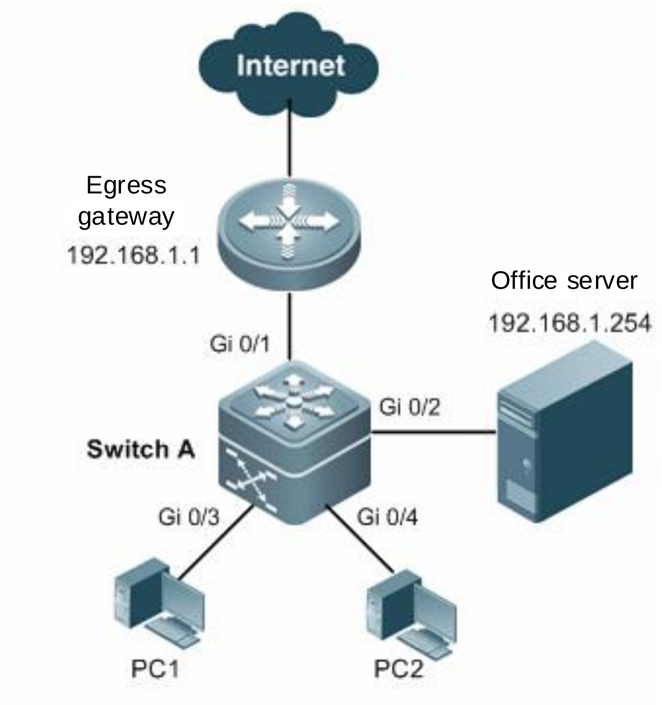
6.2 Gateway Anti-ARP Spoofing Solution

6.2.1 Overview

A user may connect a small wireless router to a network without authorization and its IP address is the same as the IP address of the gateway, or malicious users impersonate the gateway. As a result, users cannot access the Internet.

Gateway anti-ARP spoofing can block ARP packets from non-trusted interfaces and ensure that the real gateway is not forged, and users can access the Internet normally.

Typical Topology of Gateway Anti-ARP Spoofing



6.2.2 Principles

1. ARP

Address Resolution Protocol (ARP) can resolve MAC addresses based on IP addresses. The MAC addresses can be used for data forwarding in a LAN. When a MAC address is needed, host A broadcasts an ARP request to all hosts on the network. The ARP request contains IP information. Host B with the IP address same as that in the request responds to host A with its MAC address. After receiving the MAC address of host B, host A records it in its ARP table. Then, host A will forward data to host B according to the ARP table.

2. Gateway ARP Spoofing

If there are more than one IP address on the network, there is a probability that a wrong MAC address is obtained, resulting in message transmission errors and bringing great security risks.

Gateway ARP spoofing is that the IP address of the gateway is impersonated, causing disconnection of normal network services and malicious interception of user communication.

3. Anti-ARP Spoofing

Switch interfaces block ARP packets that contain the gateway IP address from untrusted interfaces and only the ARP packets from trusted interfaces are forwarded to prevent users from receiving the wrong gateway MAC address.

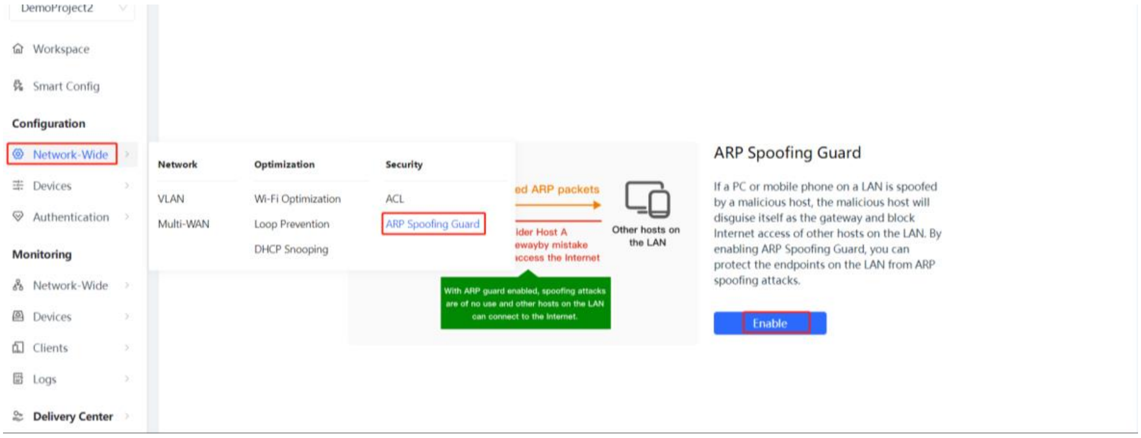
Enable gateway anti-ARP spoofing on the ports (Gi 0/3 and Gi 0/4 in this example) of the access switch (switch A) that are directly connected to PCs. The gateway address is the intranet gateway address and the intranet server address.

6.2.3 Models of Products Supporting the Feature and Topology

Product Type	Device Name	Version
Switch	NBS series	The version is unlimited. You are advised to upgrade the device to the latest version.

6.2.4 Configuration Steps

Choose **Configuration** > **Network-Wide** > **ARP Spoofing Guard** > **Enable**.

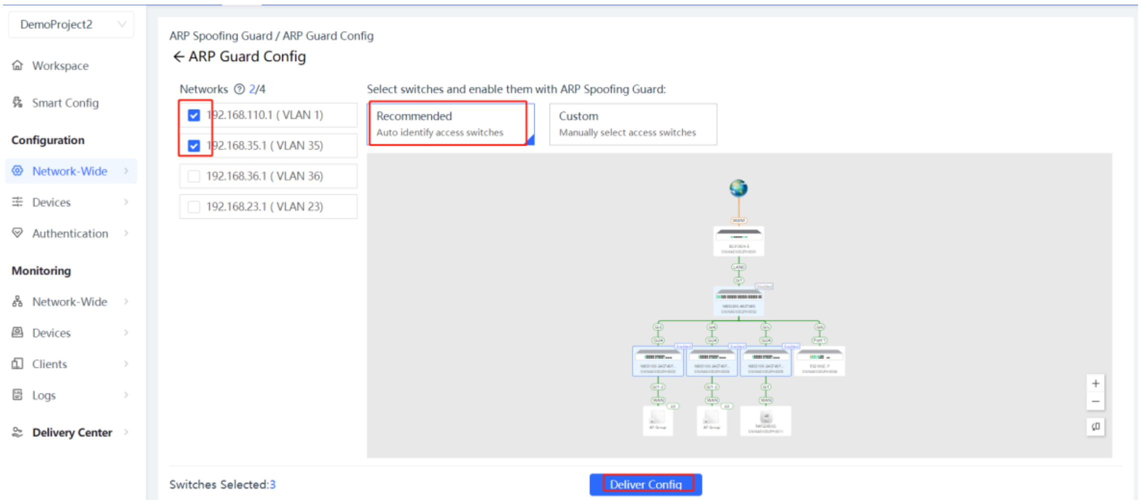


With ARP guard enabled, spoofing attacks are of no use and other hosts on the LAN can connect to the Internet.

ARP Spoofing Guard

If a PC or mobile phone on a LAN is spoofed by a malicious host, the malicious host will disguise itself as the gateway and block Internet access of other hosts on the LAN. By enabling ARP Spoofing Guard, you can protect the endpoints on the LAN from ARP spoofing attacks.

Select the gateway IP address and switch, for which anti-ARP spoofing needs to be configured. The system automatically lists the gateway IP addresses of the service networks. By default (recommended), all access switches of the current network are selected.



ARP Spoofing Guard / ARP Guard Config

← ARP Guard Config

Networks ⓘ 2/4

☑ 192.168.110.1 (VLAN 1)
☑ 192.168.35.1 (VLAN 35)
□ 192.168.36.1 (VLAN 36)
□ 192.168.23.1 (VLAN 23)

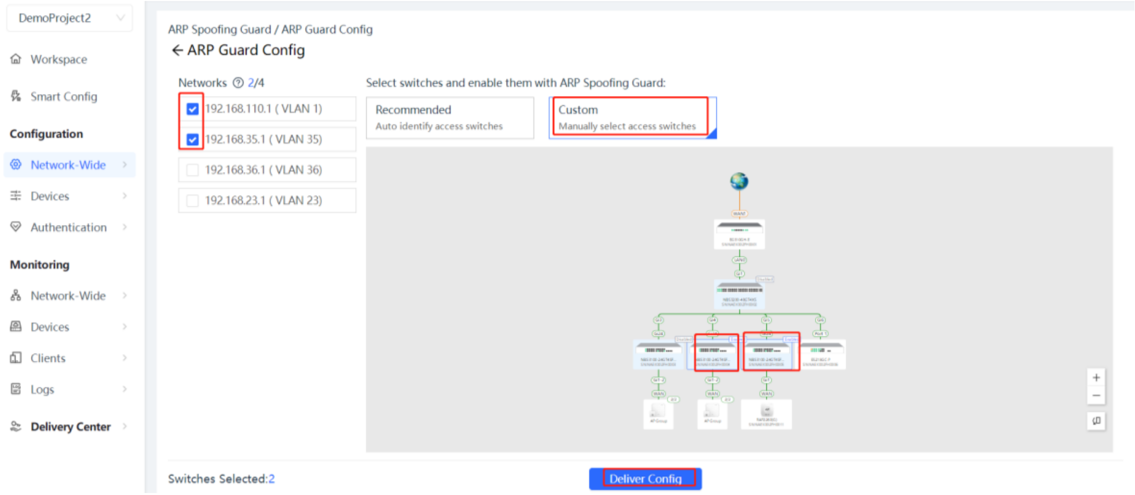
Select switches and enable them with ARP Spoofing Guard:

Recommended
Auto identify access switches

Custom
Manually select access switches

Switches Selected:3

If anti-ARP spoofing does not need to be configured for all access switches, click **Custom**, select the required switches in the topology, and then click **Deliver Config**.



Networks 2/4

☑ 192.168.110.1 (VLAN 1)
☑ 192.168.35.1 (VLAN 35)
□ 192.168.36.1 (VLAN 36)
□ 192.168.23.1 (VLAN 23)

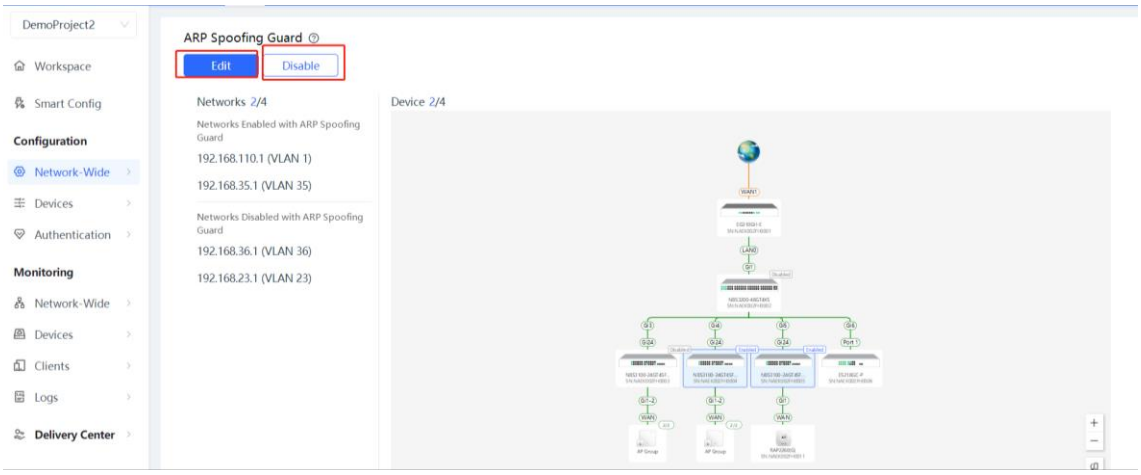
Select switches and enable them with ARP Spoofing Guard:

Recommended — Auto identify access switches

Custom — Manually select access switches

Switches Selected:2

After configuration, IP addresses and switches, for which anti-ARP spoofing is configured, are displayed. If you need to modify the configuration, click **Edit**. If you need to disable anti-ARP spoofing, click **Disable**.



Networks 2/4

Networks Enabled with ARP Spoofing Guard

192.168.110.1 (VLAN 1)

192.168.35.1 (VLAN 35)

Networks Disabled with ARP Spoofing Guard

192.168.36.1 (VLAN 36)

192.168.23.1 (VLAN 23)

Device 2/4

6.2.5 FAQs

1. If a switch is selected for enabling anti-ARP spoofing but the network topology changes, can Ruijie Cloud automatically identify the change and revise the configuration?

   No. After the topology changes, you need to go to the anti-ARP spoofing configuration page and deliver the configuration again.

2. All ports except uplink ports on a switch with anti-ARP spoofing enabled will block the forwarding of ARP packets that carry the gateway IP address. When the uplink ports of the switch change, can Ruijie Cloud automatically identify the change and deliver the configuration?

   No. After the uplink ports change, you need to go to the anti-ARP spoofing page and deliver the configuration again. If the configuration is not re-delivered, some devices fail to obtain gateway information, resulting in network disconnection.

7 General Configuration

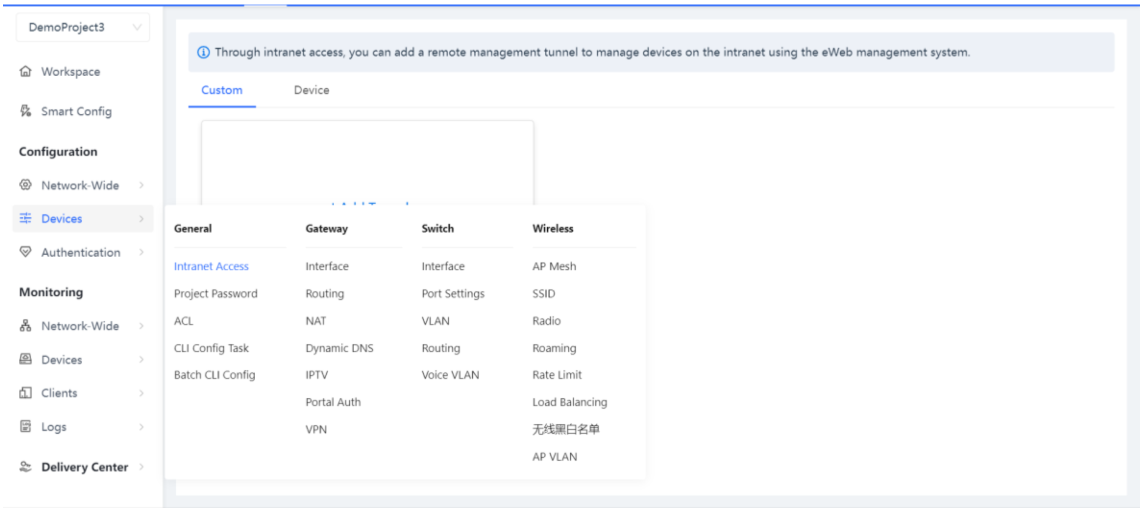
7.1 Intranet Access

7.1.1 Overview

Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.

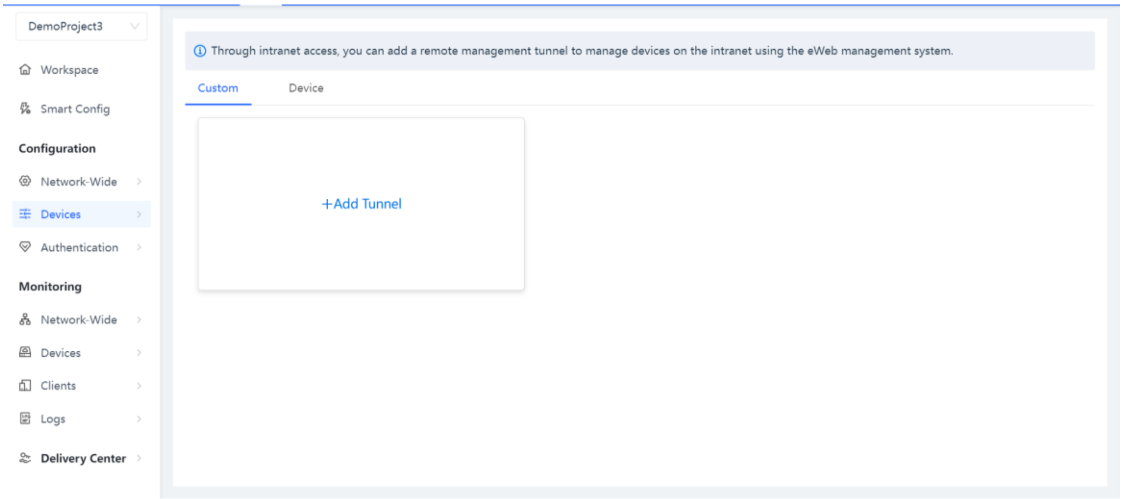
7.1.2 Configuration Steps

Choose **Configuration** > **Devices** > **General** > **Intranet Access**.

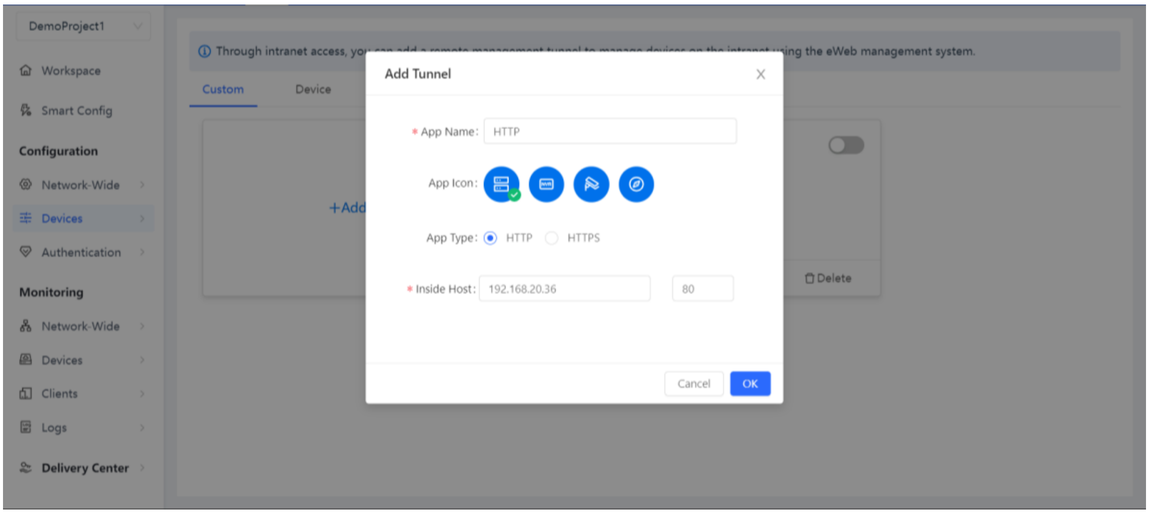


Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.

Click **Add Tunnel** on the **Intranet Access** page. You can create a remote tunnel to access the intranet devices.



Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.



Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.

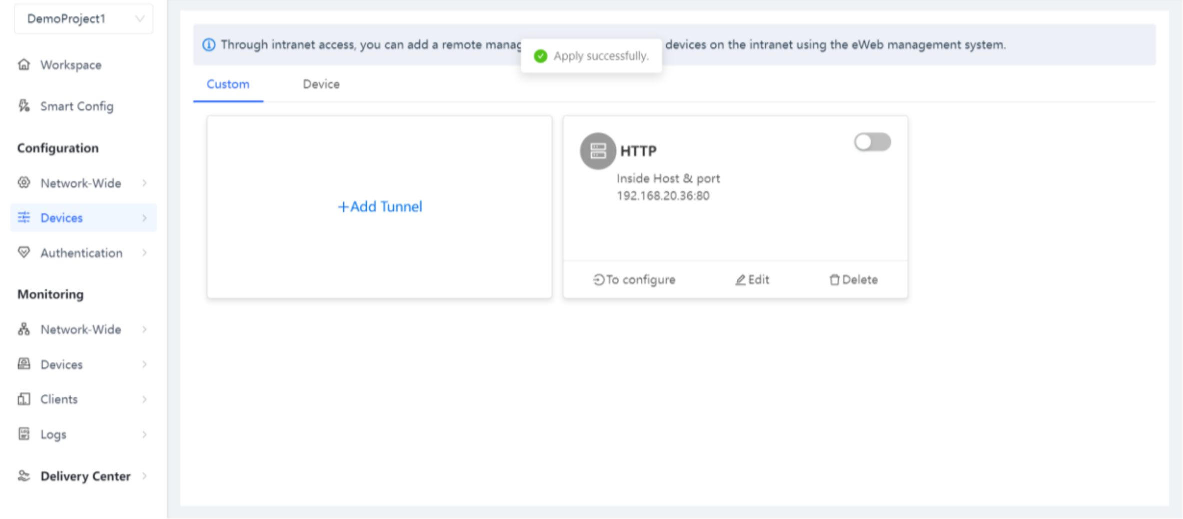
Add Tunnel

* App Name: HTTP

App Icon:

App Type: ● HTTP ○ HTTPS

* Inside Host: 192.168.20.36 80

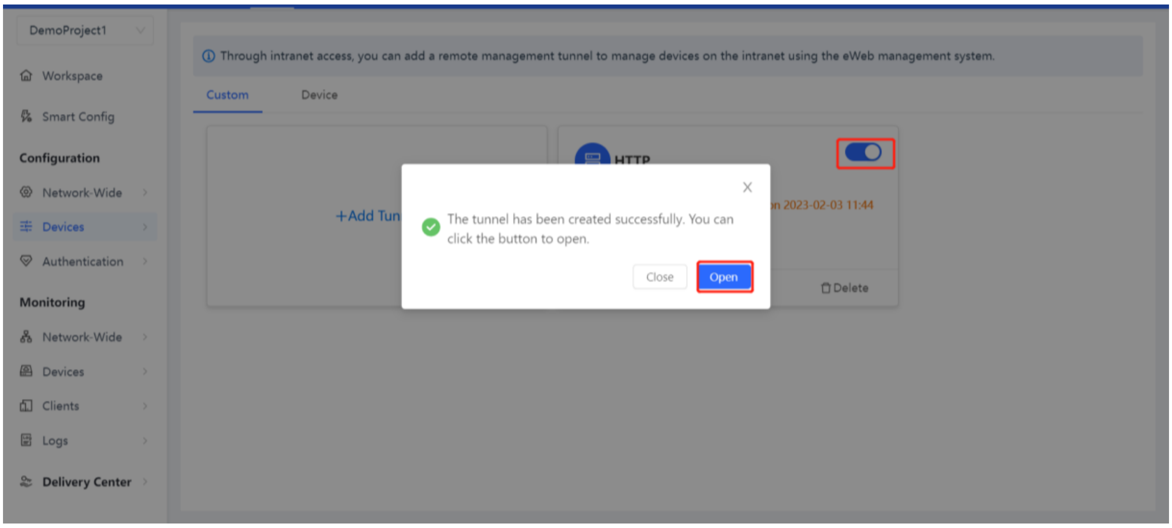


Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.

Apply successfully.

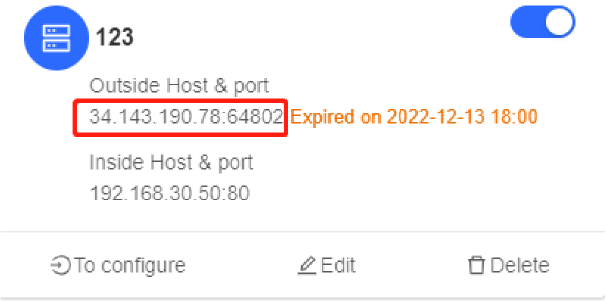
HTTP

Inside Host & port
192.168.20.36:80



Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.

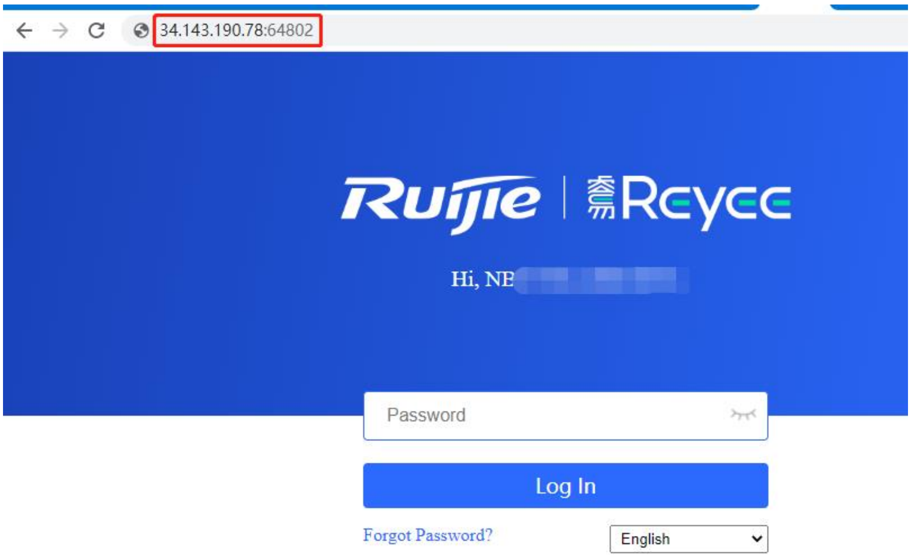
The tunnel has been created successfully. You can click the button to open.



123

Outside Host & port
34.143.190.78:64802 Expired on 2022-12-13 18:00

Inside Host & port
192.168.30.50:80



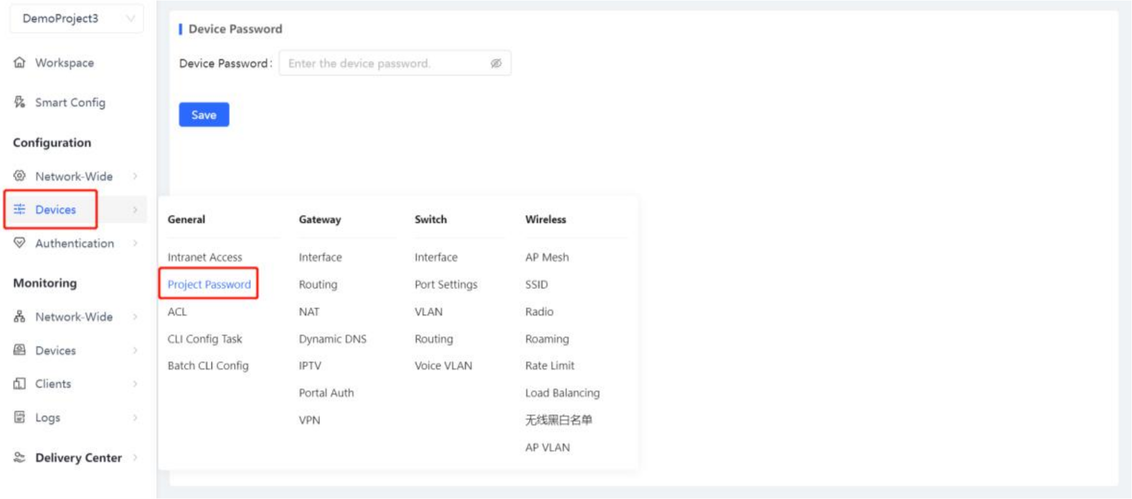
34.143.190.78:64802

Hi, NE[redacted]

7.2 Project Password

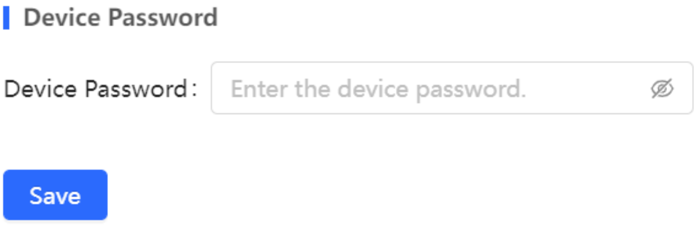
Choose **Configuration** > **Devices** > **General** > **Project Password**.

Enter a new device password and click **Save**.



Device Password

Device Password: Enter the device password.



Device Password

Device Password: Enter the device password.

7.3 ACL

An access control list (ACL) is commonly referred to as packet filter in some documents. An ACL defines a series of permit or deny rules and applies these rules to device interfaces to control packets sent to and from the interfaces, so as to enhance security of the network device.

You can add ACLs based on MAC addresses or IP addresses and bind ACLs to ports.

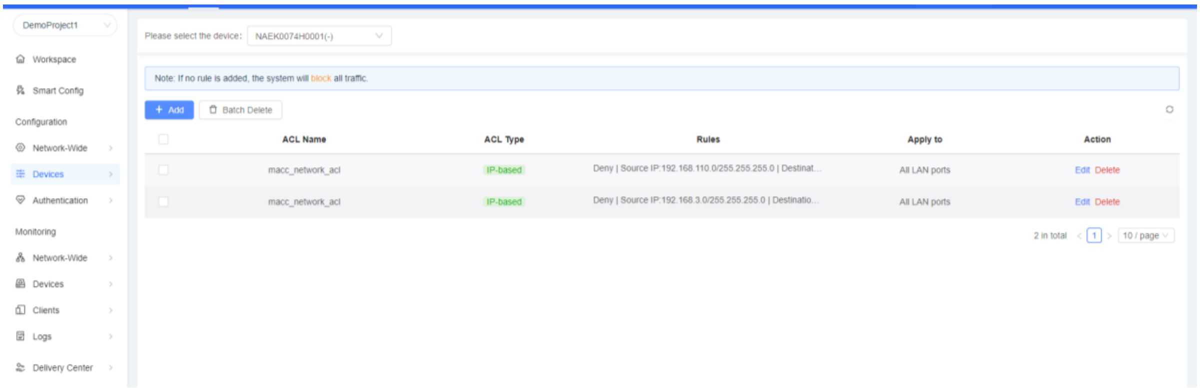
7.3.1 Creating ACL Rules

Choose **Local Device** > **Security** > **ACL** > **ACL List**.

(1) Click **Add** to set the ACL control type, enter an ACL name, select ports and rules.

Based on MAC address: To control the L2 packets entering/leaving the port, and deny or permit specific L2 packets destined to a network.

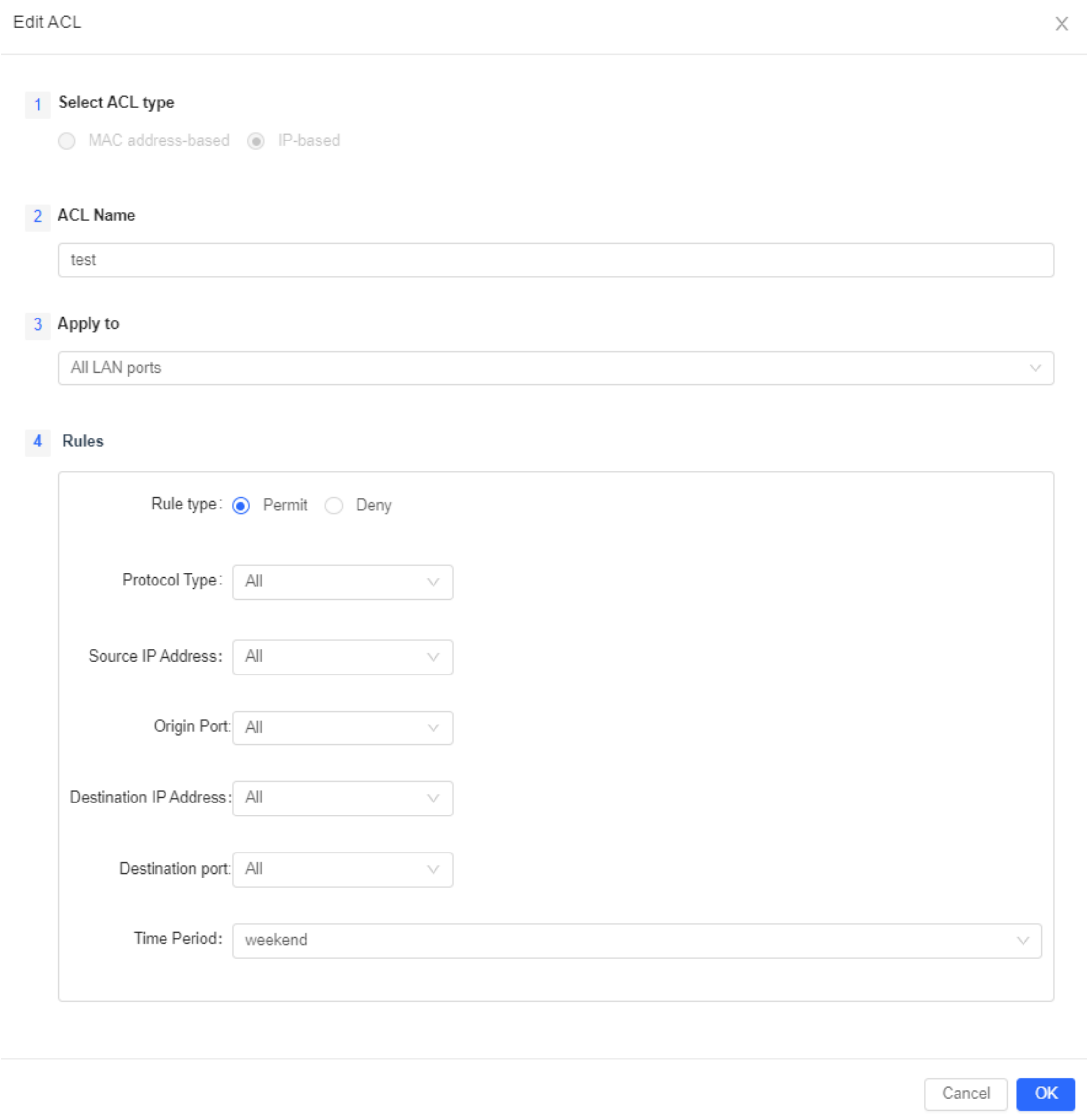
Based on IP address: To control the Ipv4 packets entering/leaving a port, and deny or permit specific Ipv4 packets destined to a network.



Please select the device: NAEK0074H0001(-)

Note: If no rule is added, the system will block all traffic.

□	ACL Name	ACL Type	Rules	Apply to	Action
□	macc_network_acl	IP-based	Deny | Source IP:192.168.110.0/255.255.255.0 | Destinat...	All LAN ports	Edit Delete
□	macc_network_acl	IP-based	Deny | Source IP:192.168.3.0/255.255.255.0 | Destinatio...	All LAN ports	Edit Delete



Edit ACL

1 Select ACL type

○ MAC address-based ● IP-based

2 ACL Name

test

3 Apply to

All LAN ports

4 Rules

Rule type: ● Permit ○ Deny

Protocol Type: All

Source IP Address: All

Origin Port: All

Destination IP Address: All

Destination port: All

Time Period: weekend

Rules: The rules include two actions of **Permit** or **Deny**, and the matching rules of packets.

Table 9-1 Description of ACL Rule Configuration Parameters

Parameter	Description
ACL	Configuring ACL Rules Action Block: If packets match this rule, the packets are denied. Allow: If packets match this rule, the packets are permitted.
IP Protocol Number	Match IP protocol number The value ranges from 0 to 255. Check **All** to match all IP protocols.
Src IP Address	Match the source IP address of the packet. Check **All** to match all source IP addresses.
Dest IP Address	Match the destination IP address of the packet. Check **All** to match all

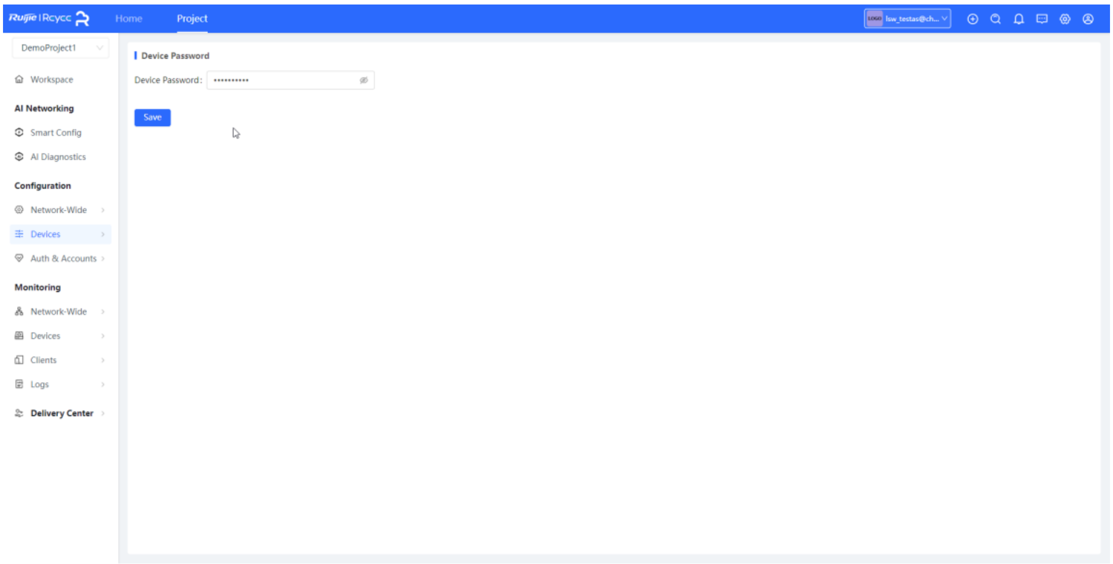
Parameter	Description
	destination IP addresses
EtherType Value	Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check **All** to match all protocol type numbers.
Src Mac	Match the MAC address of the source host. Check **All** to match all source MAC addresses
Dest MAC	Match the MAC address of the destination host. Check **All** to match all destination MAC addresses

Note

- If no rule is added, the system will block all traffic.
- An ACL applied by a port cannot be edited or deleted. To edit, unbind the ACL from the port first.

7.4 Device Password

In this project, password modification only applies to web login passwords, and the login passwords for all devices will be changed to this new password.



Device Password: •••••••••••

7.5 CLI Config Task

7.5.1 Add a CLI Command Set

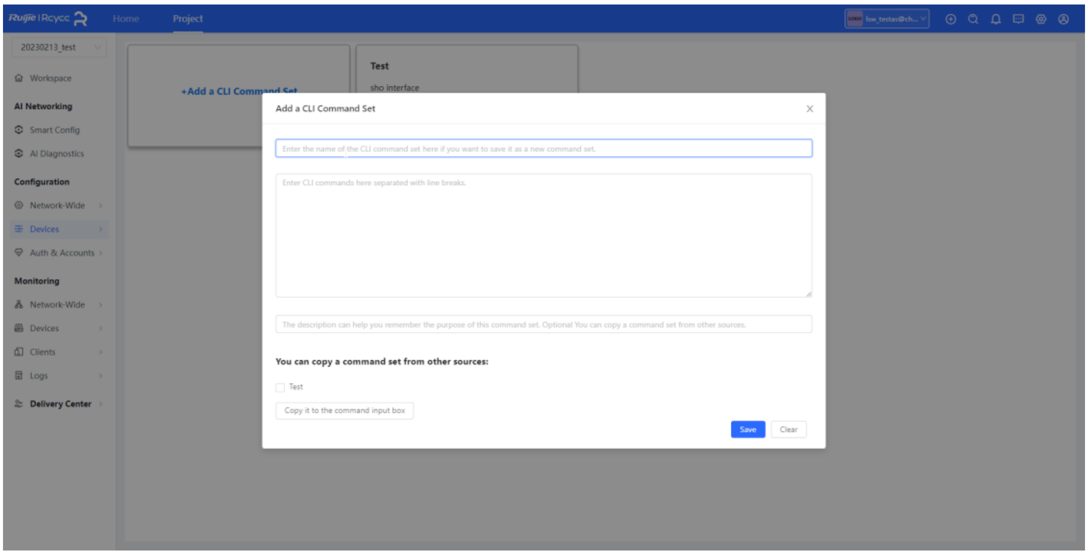
Limitations

The function is only supported on RGOS devices.

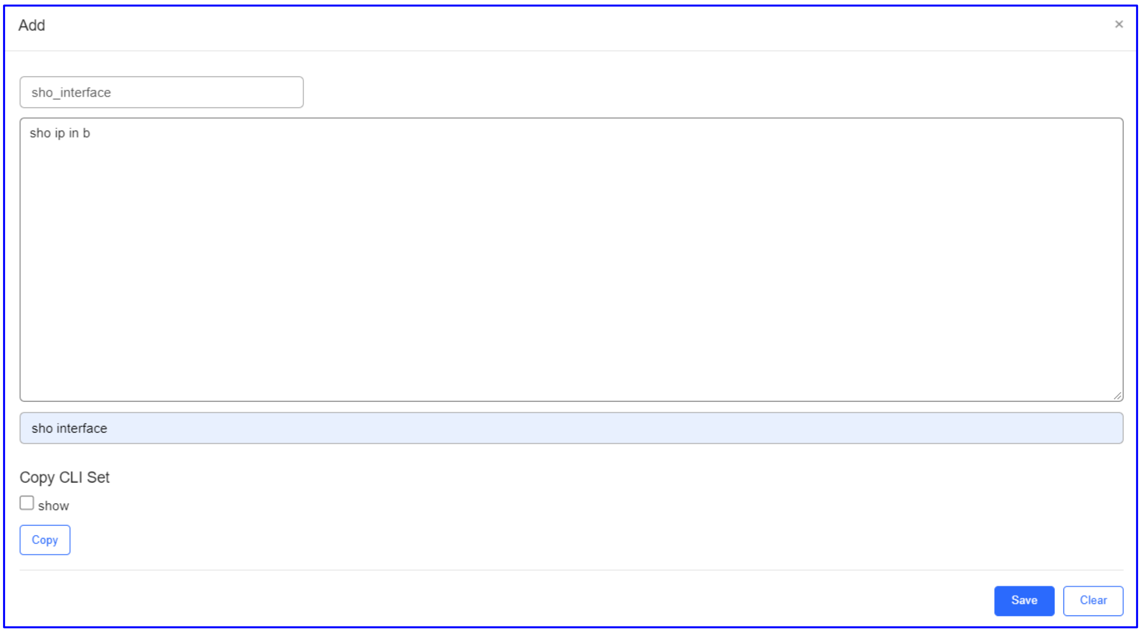
Procedure

(1) Choose **Project** > **Devices** > **CLI Config Task**.

(2) Click **Add a CLI Command Set** to customize a CLI Task.


Ruijie | Rcycc
Home
Project
lsw_testas@ch...
20230213_test
Workspace
AI Networking
Smart Config
AI Diagnostics
Configuration
Network-Wide
Devices
Auth & Accounts
Monitoring
Network-Wide
Devices
Clients
Logs
Delivery Center
+Add a CLI Command Set
Test
sho interface
Add a CLI Command Set
Enter the name of the CLI command set here if you want to save it as a new command set.
Enter CLI commands here separated with line breaks.
The description can help you remember the purpose of this command set. Optional You can copy a command set from other sources.
You can copy a command set from other sources:
Test
Copy it to the command input box
Save
Clear

(3) Enter the set name and commands and click **Save**.



sho_interface

```
sho ip in b
```

sho interface

If the CLI command is the same as another one, you can select the CLI set and click **Copy**.

7.5.2 Batch CLI Configuration

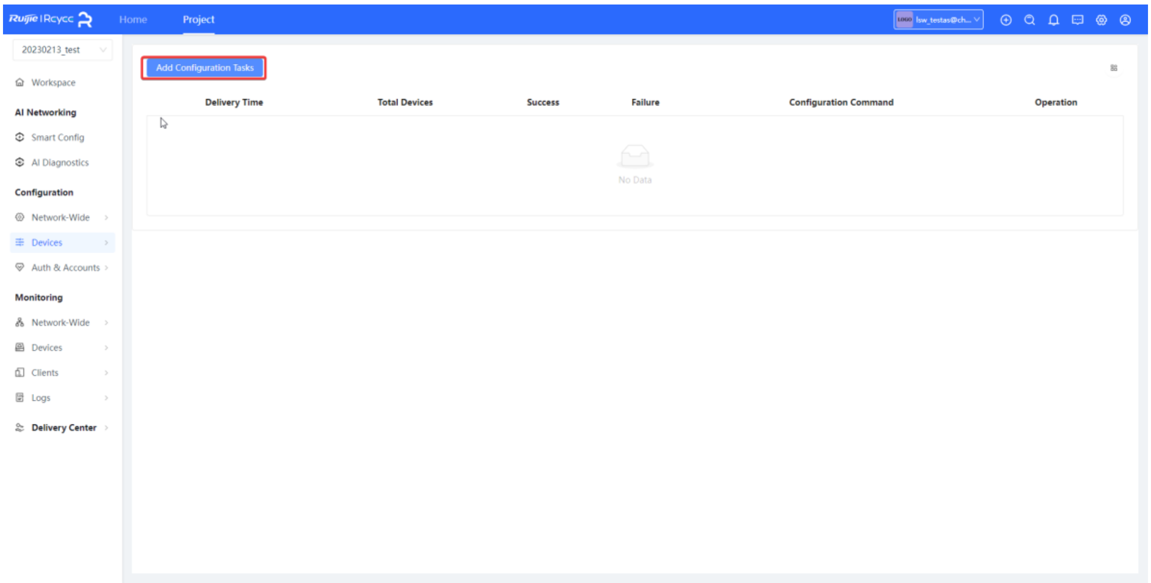
Limitations

The function is only supported on RGOS devices.

Procedure

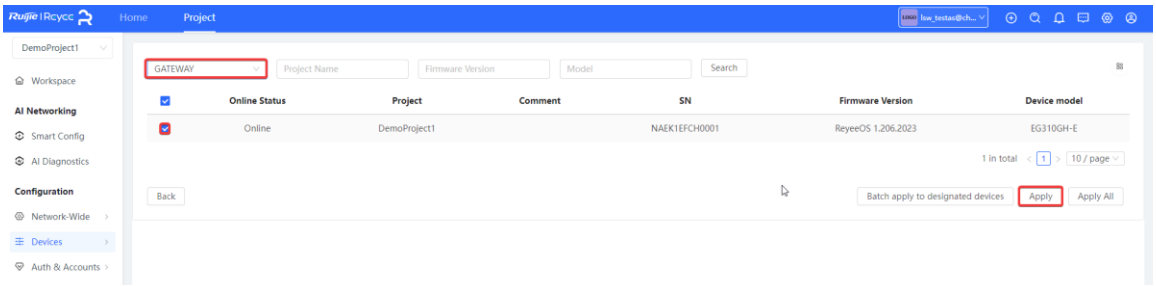
(1) Choose **Project** > **Device** > **Batch CLI Config**.

(2) Click **Add Configuration Tasks**.



Delivery Time	Total Devices	Success	Failure	Configuration Command	Operation

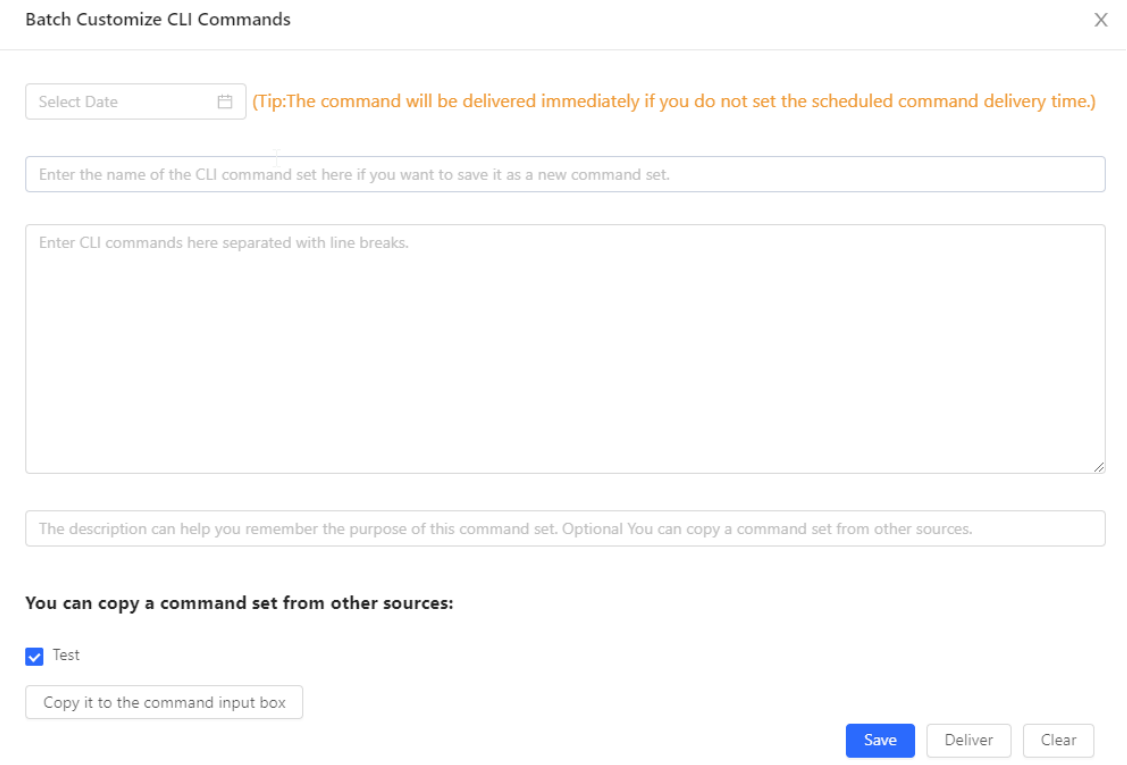
(3) Select one or more devices, and click **Apply**.



☑	Online Status	Project	Comment	SN	Firmware Version	Device model
☑	Online	DemoProject1		NAEK1EFCH0001	ReyeeOS 1.206.2023	EG310GH-E

(4) Set parameters and click **Apply**.

The command will be delivered immediately if you do not set the scheduled command delivery time.



Batch Customize CLI Commands

Select Date (Tip:The command will be delivered immediately if you do not set the scheduled command delivery time.)

Enter the name of the CLI command set here if you want to save it as a new command set.

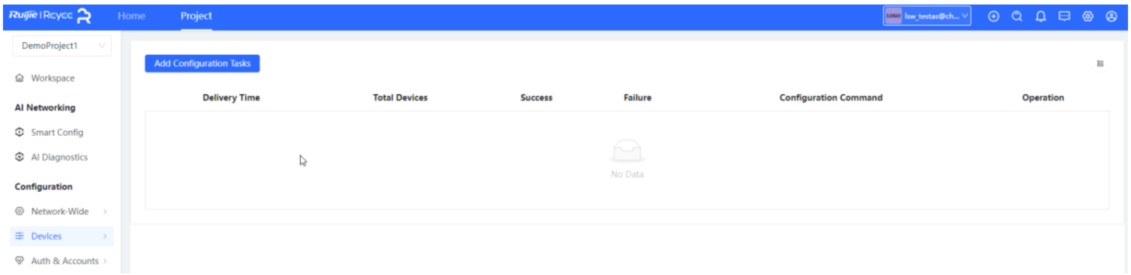
Enter CLI commands here separated with line breaks.

The description can help you remember the purpose of this command set. Optional You can copy a command set from other sources.

You can copy a command set from other sources:

☑ Test

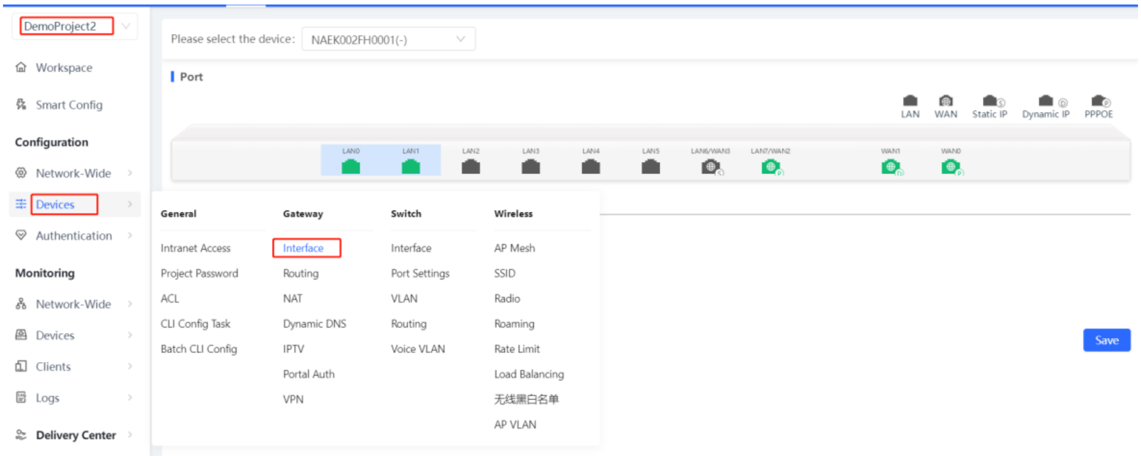
(5) Click **Back** to return to the **Batch CLI Config Status** page.



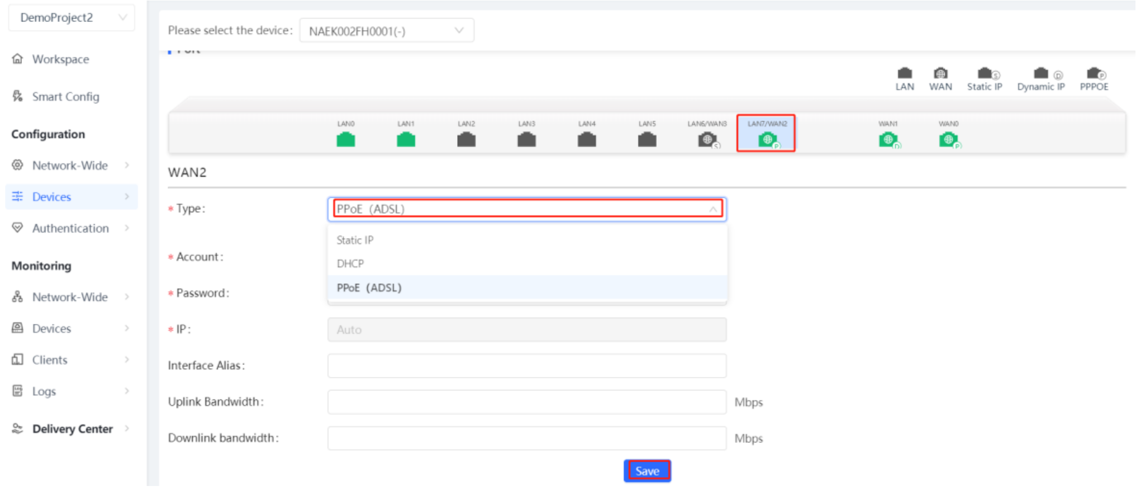
8 Gateway Configuration

8.1 Interface

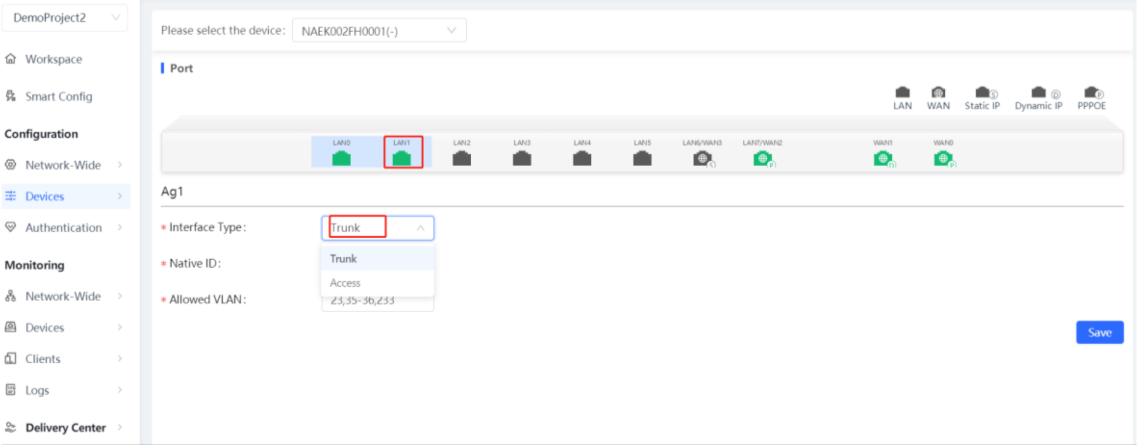
Choose **Project** > **Devices** > **Gateway** > **Interface**. The gateway port page is displayed.



Click a WAN port on the gateway and set the networking mode. Click **Save**.



Click a LAN port on the gateway, and set **Interface Type**, **Native ID**, and **Allowed VLAN** for the LAN port, and then click **Save**.



Please select the device: NAEK002FH0001(-)

Ag1

* Interface Type: Trunk

* Native ID:

* Allowed VLAN: 23,35-36,233

8.2 Routing

8.2.1 Adding a Static Route

1. Introduction

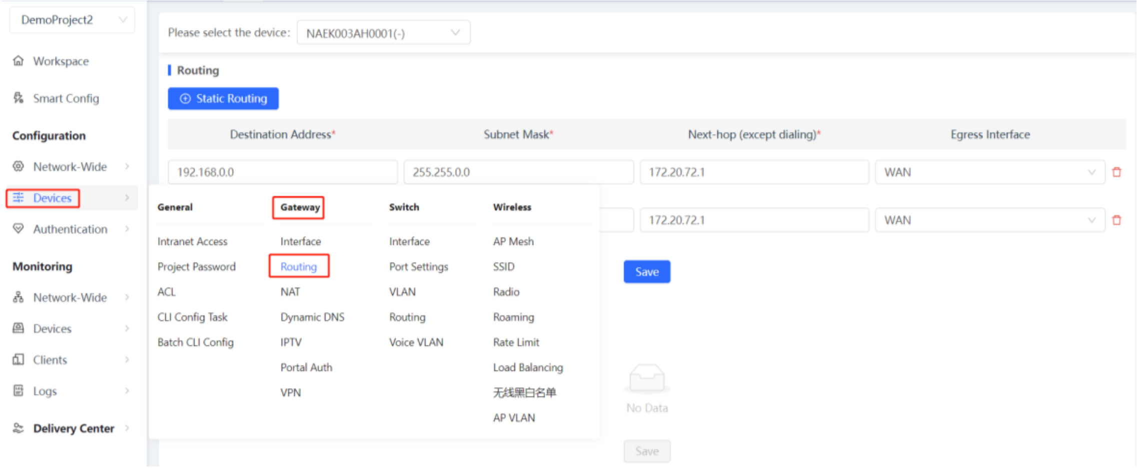
Static routes are manually configured. When a data packet matches a static route, the packet will be forwarded based on the specified forwarding mode.

Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

2. Configuration Steps

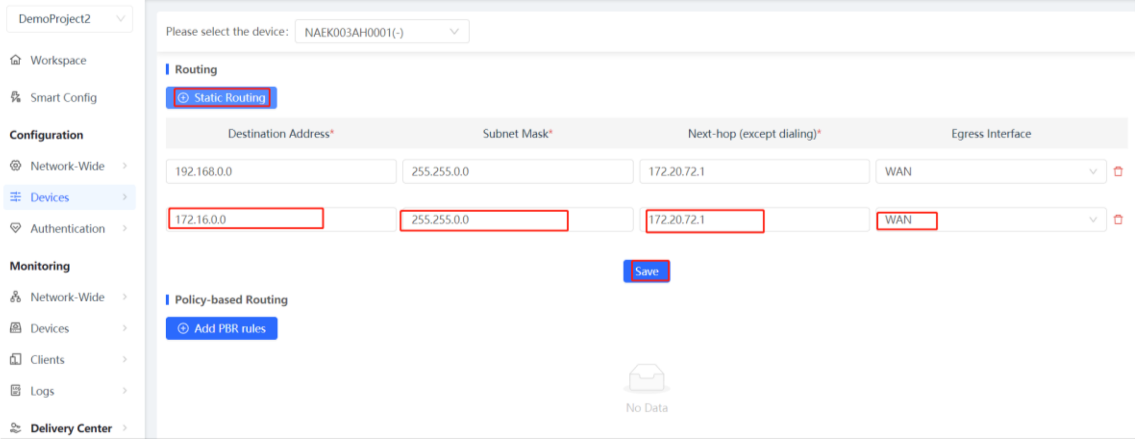
(1) Choose **Device** > **Getaway** > **Routing** to go to the route configuration page.



Please select the device: NAEK003AH0001(-)

Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface
192.168.0.0	255.255.0.0	172.20.72.1	WAN
		172.20.72.1	WAN

(2) Click ⊕ **Static Routing** to add a static route. Click **Save**.



Please select the device: NAEK003AH0001(-)

Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface
192.168.0.0	255.255.0.0	172.20.72.1	WAN
172.16.0.0	255.255.0.0	172.20.72.1	WAN

The following table lists the description of parameters.

Parameter	Description
Destination Address	Specify the destination network to which data packets are to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.
Next-hop Address	Specify the IP address of the next hop in the route for data packets. If the outbound interface accesses the Internet through PPPoE dialing, you do not need to configure the next-hop address.
Egress	Specify the interface that forwards data packets.

8.2.2 Adding PBR

1. Introduction

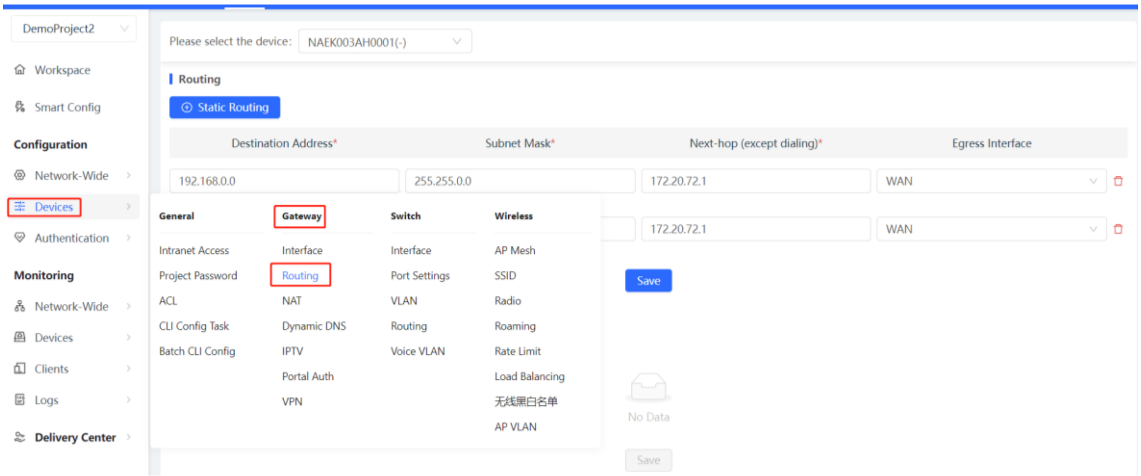
Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets based on configured rules, and then forwards the matched packets according to the specified forwarding policy. PBR enables the device to define rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forward the data packets from a specific interface.

In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data to the external network may be sent to the internal network, resulting in network exceptions. To prevent these exceptions, you need to configure PBR to control data isolation and forwarding on the internal and external networks.

The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing are in descending order of priority.

2. Configuration Steps

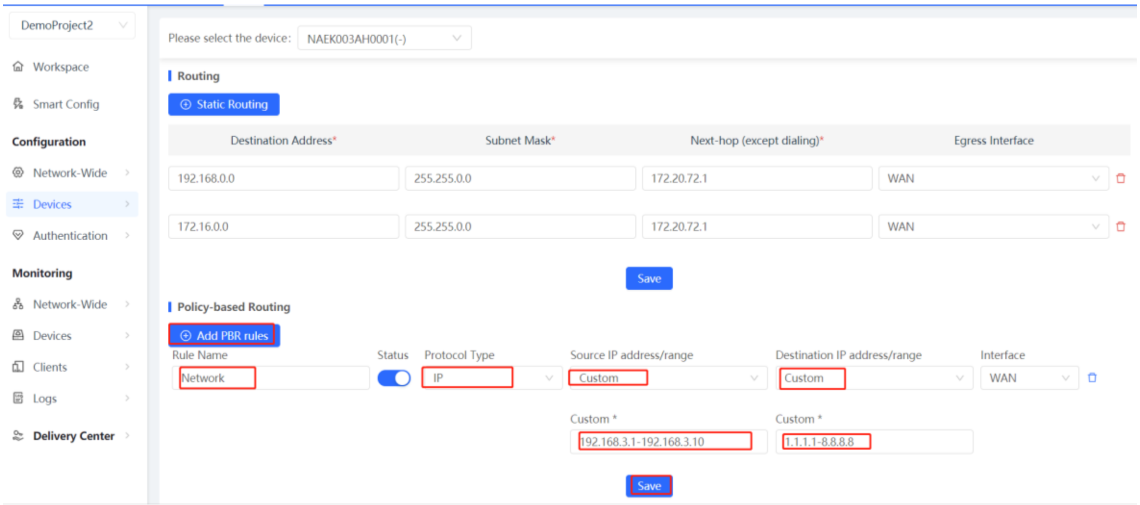
(1) Choose **Device** > **Getaway** > **Routing** to go to the route configuration page.



Please select the device: NAEK003AH0001(-)

Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface
192.168.0.0	255.255.0.0	172.20.72.1	WAN
		172.20.72.1	WAN

(2) Click ⊕ **Add PBR rules** to add a PBR rule. Set parameters and then click **Save**.



Please select the device: NAEK003AH0001(-)

Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface
192.168.0.0	255.255.0.0	172.20.72.1	WAN
172.16.0.0	255.255.0.0	172.20.72.1	WAN

Rule Name	Status	Protocol Type	Source IP address/range	Destination IP address/range	Interface
Network	●	IP	Custom	Custom	WAN
			Custom * 192.168.3.1-192.168.3.10	Custom * 1.1.1.1-8.8.8.8	

The following table lists the description of parameters.

Parameter	Description
Name	Specify the name of a PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Status	Indicate whether to enable the PBR rule. If the value is disabled, this rule does not take effect.
Protocol	Specify the protocol for which the PBR rule is effective. You can set this parameter to **IP**, **ICMP**, **UDP**, **TCP**, or **Custom**.
Source IP/IP Range	Configure the source IP address or IP address range for matching PBR entries. The default value is **All IP Addresses**. **All IP Addresses**: Match all the source IP addresses. **Custom**: Match the source IP addresses in the specified IP address range.
Custom Src IP	When **Src IP/IP Range** is set to **Custom**, you need to enter a single source IP address or a source IP address range.

Parameter	Description
Destination IP/IP Range	Configure the destination IP address or IP address range for matching PBR entries. The default value is **All IP Addresses**. **All IP Addresses**: Match all the destination IP addresses. **Custom**: Match the destination IP addresses in the specified IP address range.
Custom Dest IP	When **Dest IP/IP Range** is set to **Custom**, you need to enter a destination IP address or a destination IP address range.
Port	Specify the interface that forwards data packets based on the hit PBR rule.

8.3 NAT

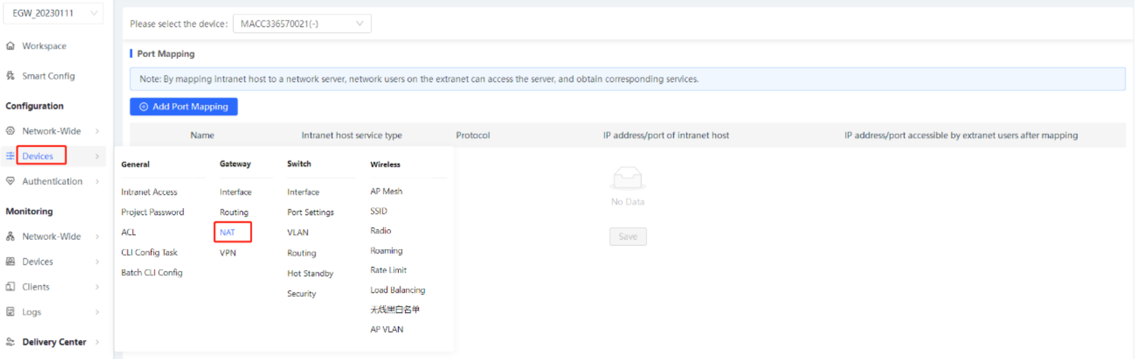
8.3.1 Applicable Scenarios

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

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

8.3.2 Configuration Steps

(1) Choose **Device** > **Gateway** > **NAT** to go to the **Port Mapping** page.



Please select the device: MACC336570021(-)

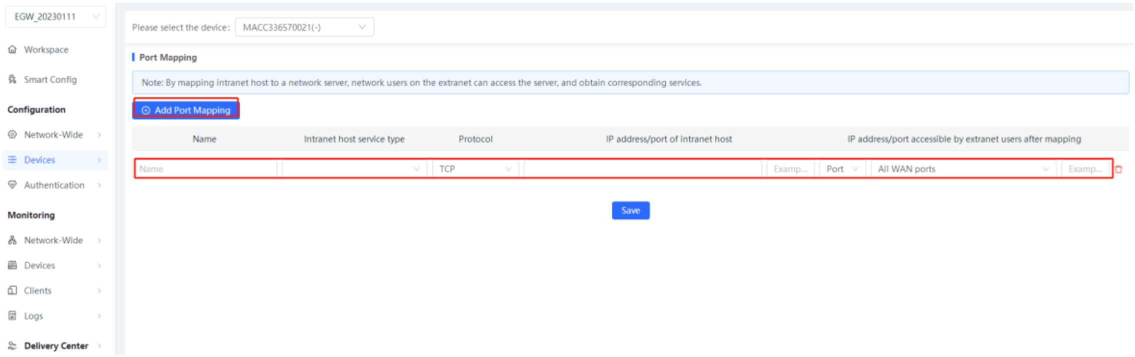
Port Mapping

Note: By mapping intranet host to a network server, network users on the extranet can access the server, and obtain corresponding services.

Name	Intranet host service type	Protocol	IP address/port of intranet host	IP address/port accessible by extranet users after mapping

No Data

(2) Click ⊕**Add Port Mapping**, set parameters, and then click **Save**.

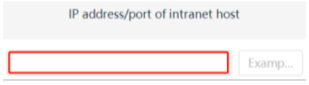
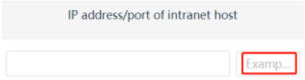
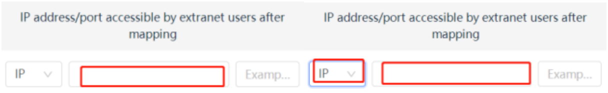


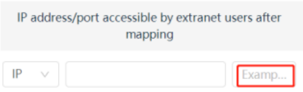
Please select the device: MACC336570021(-)

Port Mapping

Note: By mapping intranet host to a network server, network users on the extranet can access the server, and obtain corresponding services.

The following table lists the description of parameters.

Parameter	Description
Name	Enter the description of a port mapping rule, which is used to identify the rule.
Intranet host service type	Select the transport layer protocol type used by the service, such as TCP or UDP. The value **ALL** indicates that the rule applies to all protocols. The value must comply with the terminal configuration of a service.
Protocol	Select the transport layer protocol type used by the service, such as TCP or UDP. The value **ALL** indicates that the rule applies to all protocols. The value must comply with the terminal configuration of a service.
Internal Server IP	Specify the IP address of the internal server to be mapped to the WAN port, that is, the IP address of the LAN device that provides Internet access, such as the IP address of a network camera. 
Internal Port	Specify the service port number of the internal server to be mapped to a WAN port, that is, the port number of the application that provides Internet access, such as port 8080 of the web service. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the number of ports must be the same as that specified in **External Port/Range**. 
External Server IP	Specify the host address used for Internet access. The default value is the IP address of a WAN port.  IP address/port accessible by extranet users after mapping IP address/port accessible by extranet users after mapping IP Examp... IP Examp...

Parameter	Description
External Port	Specify the port number used for Internet access. You need to confirm the port number in the client software, such as the camera monitoring software. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the value of **Internal Port/Range** must also be a port range.  IP address/port accessible by extranet users after mapping IP Examp...

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

Note

Solution to test failures:

- Modify the value of **External Server IP** and use the new external port number to perform the test again. The possible cause is that the port is blocked by the firewall.
- Enable the remote access permission on the server. The possible cause is that remote access is displayed on the server, resulting in normal internal access but abnormal access across network segments.

8.4 Configuring VPN

1. Overview

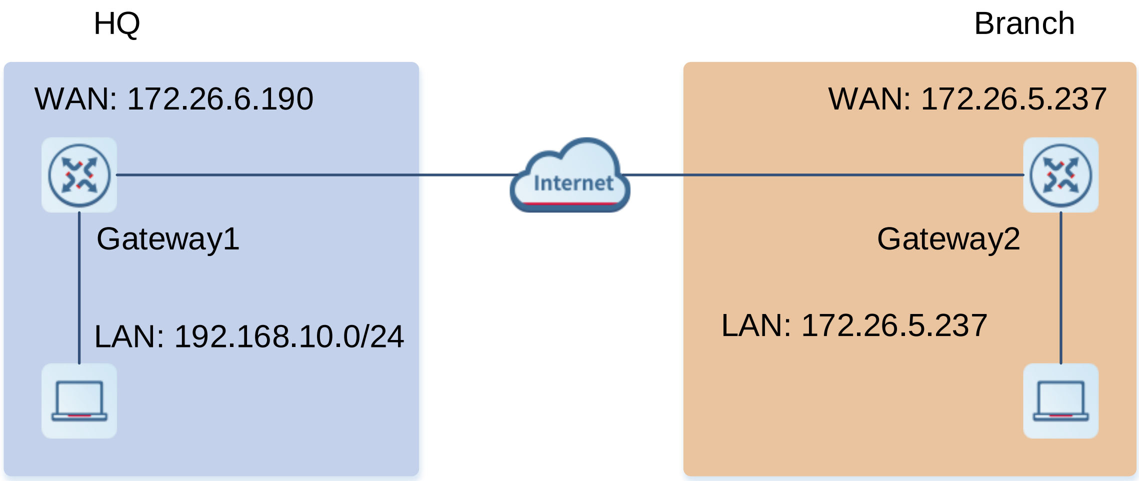
Virtual private network (VPN) is used to build a virtual private network on the public network, and transmit private network traffic on this virtual network.

There are two VPN application scenarios:

- Site-to-Site VPN

  A connection is established between two LANs through a VPN tunnel. Figure 8-1 shows the typical network topology. An enterprise's HQ and branch are connected to the Internet through gateway 1 and gateway 2 respectively. The HQ and branch often send internal confidential data to each other because of business needs. To secure data transmission on the Internet, a VPN tunnel is established between gateway 1 and gateway 2.

Figure 8-1 Typical Network Topology of Site-to-Site VPN



In this scenario, the networks of the HQ and branch are connected to the Internet through fixed gateways, and the networking is relatively fixed. The access is bidirectional, that is, both the branch and HQ may initiate access to the peer end. It is often used for business communication of chain supermarkets, government departments, and banks.

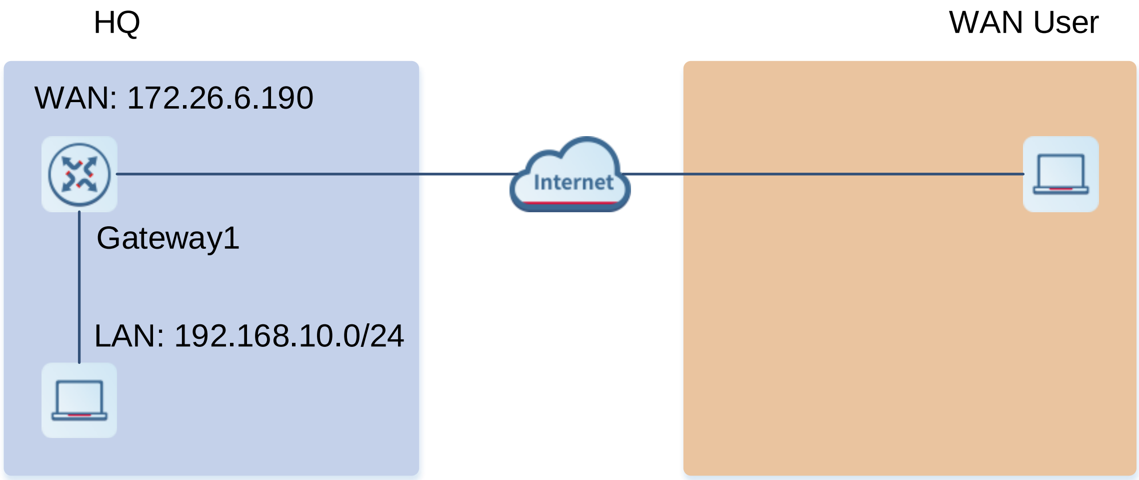
Site-to-site VPN can be implemented in the following ways: PPTP, L2TP, IPSec, and L2TP over IPsec. Ruijie Cloud supports only the IPsec VPN mode.

- Client-to-Site VPN

A connection is established between clients and the enterprise intranet through VPN tunnels. Figure 8-2 shows the typical network topology. Employees on business trips (clients) access the Intranet of the HQ through Internet to transmit data to the HQ and access internal servers. To secure data transmission, a VPN tunnel can be established between a client and the enterprise gateway.

In this scenario, the client address is not fixed and the access is one-way, that is, only the client initiates access to Intranet servers. It is suitable for employees on business trips or employees in temporary offices to remotely access the HQ intranet through mobile phones or PCs.

Figure 8-2 Typical Network Topology of Client-to-Site VPN



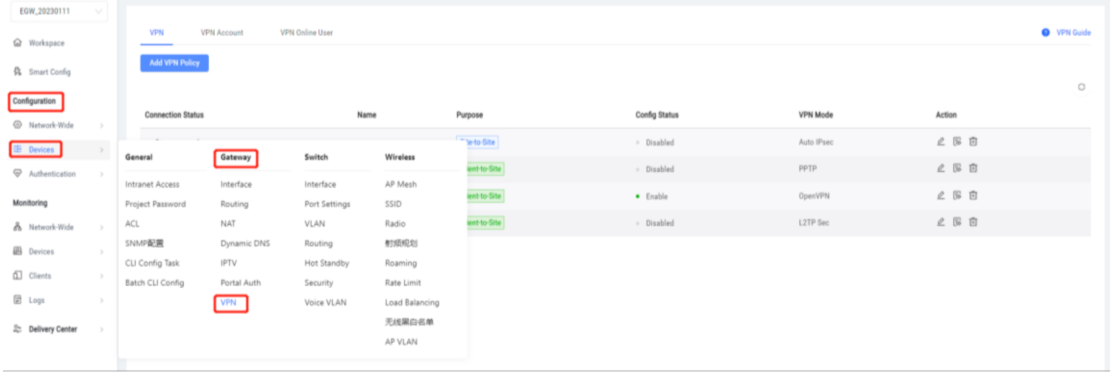
Client-to-site VPN can be implemented in the following ways: PPTP, L2TP, L2TP over VPN, and open VPN.

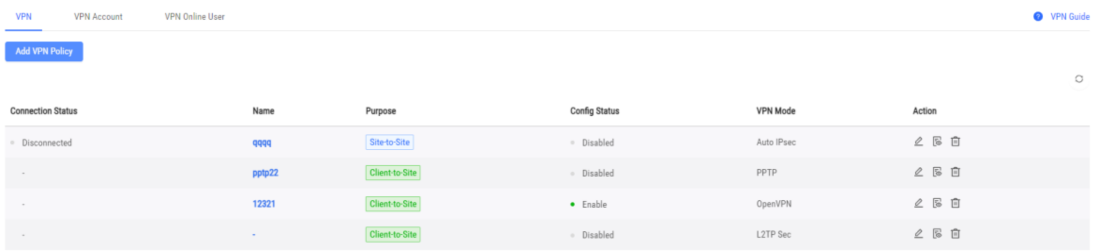
2. Configuring Site-to-Site VPN (Based on IPsec VPN)

(1) Configure VPN for the HQ gateway.

a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.

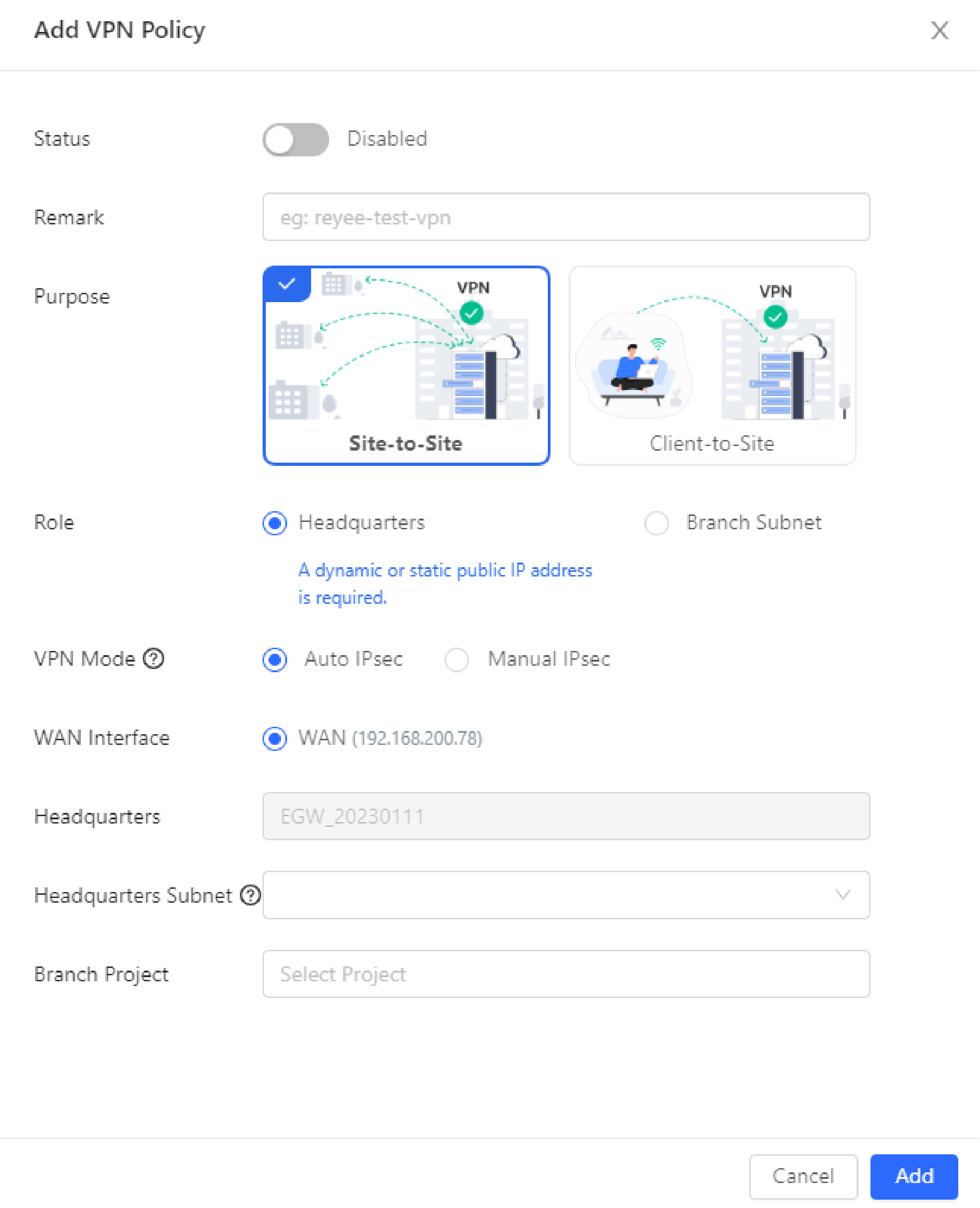
b Choose **Configuration** > **Devices** > **Gateway** > **VPN**.





Connection Status	Name	Purpose	Config Status	VPN Mode	Action
Disconnected	qqqq	Site-to-Site	Disabled	Auto IPsec	
-	pptp22	Client-to-Site	Disabled	PPTP	
-	12321	Client-to-Site	● Enable	OpenVPN	
-	-	Client-to-Site	Disabled	L2TP Sec	

c Click **Add VPN Policy**.



Add VPN Policy

Status ○ Disabled

Remark eg: reyee-test-vpn

Purpose ☑ Site-to-Site | Client-to-Site

Role ● Headquarters ○ Branch Subnet

A dynamic or static public IP address is required.

VPN Mode ● Auto IPsec ○ Manual IPsec

WAN Interface ● WAN (192.168.200.78)

Headquarters EGW_20230111

Headquarters Subnet

Branch Project Select Project

d Set configuration items related to the HQ VPN.

Table 8-1 Configuration Items Related to the HQ VPN

Parameter	Description
Status	Specify whether to enable the VPN policy. Ensure that the VPN policies of both the HQ and branch are enabled so that the VPN between the HQ and branch can be established successfully.
Remark	Provide the description of the VPN policy.

Parameter	Description
Purpose	Specify the VPN usage scenario. Select **Site-to-Site**.
Role	Specify the role of the current gateway. Select **Headquarter** if the HQ gateway needs to be connected.
VPN Mode	Specify the IPSec VPN implementation mode. It can be set to the following: **Auto IPsec**: When the HQ gateway and branch gateway are managed by the same Cloud account, click **Auto IPsec**. When this mode is selected, a VPN tunnel can be automatically established by selecting the HQ gateway and the branch gateway. **Manual IPsec**: When this mode is selected, VPN needs to be manually configured on the HQ gateway or branch gateway so that a connection is established between the branch gateway and HQ gateway.
WAN Interface	
Headquarters	Specify the name of the HQ gateway.
Headquarters Subnet	
Branch Project	Project, to which the branch gateway belongs. Set this parameter when **VPN Mode** is set to **Manual IPsec**.

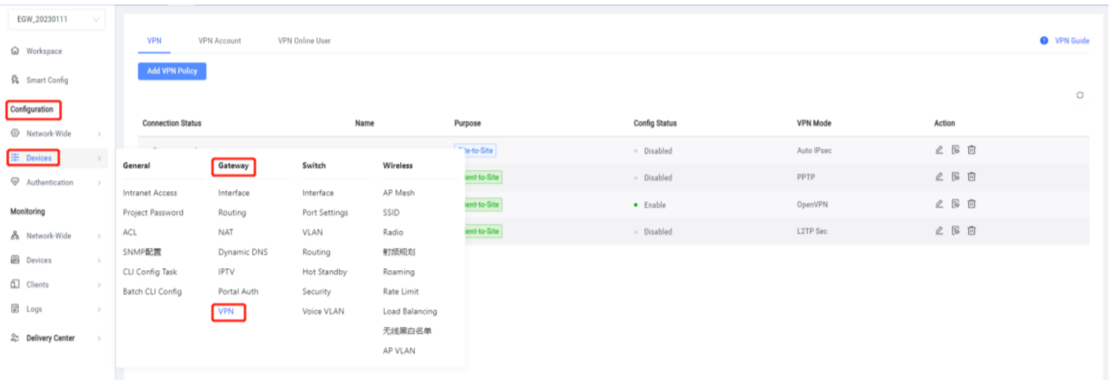
e Click **Add**.

(2) (Optional) Configure VPN for the branch gateway.

When VPN is configured for the HQ gateway, if **VPN Mode** is set to **Manual IPSec**, perform the following operations. If **VPN Mode** is not set to **Auto IPsec**, the following operations are not required.

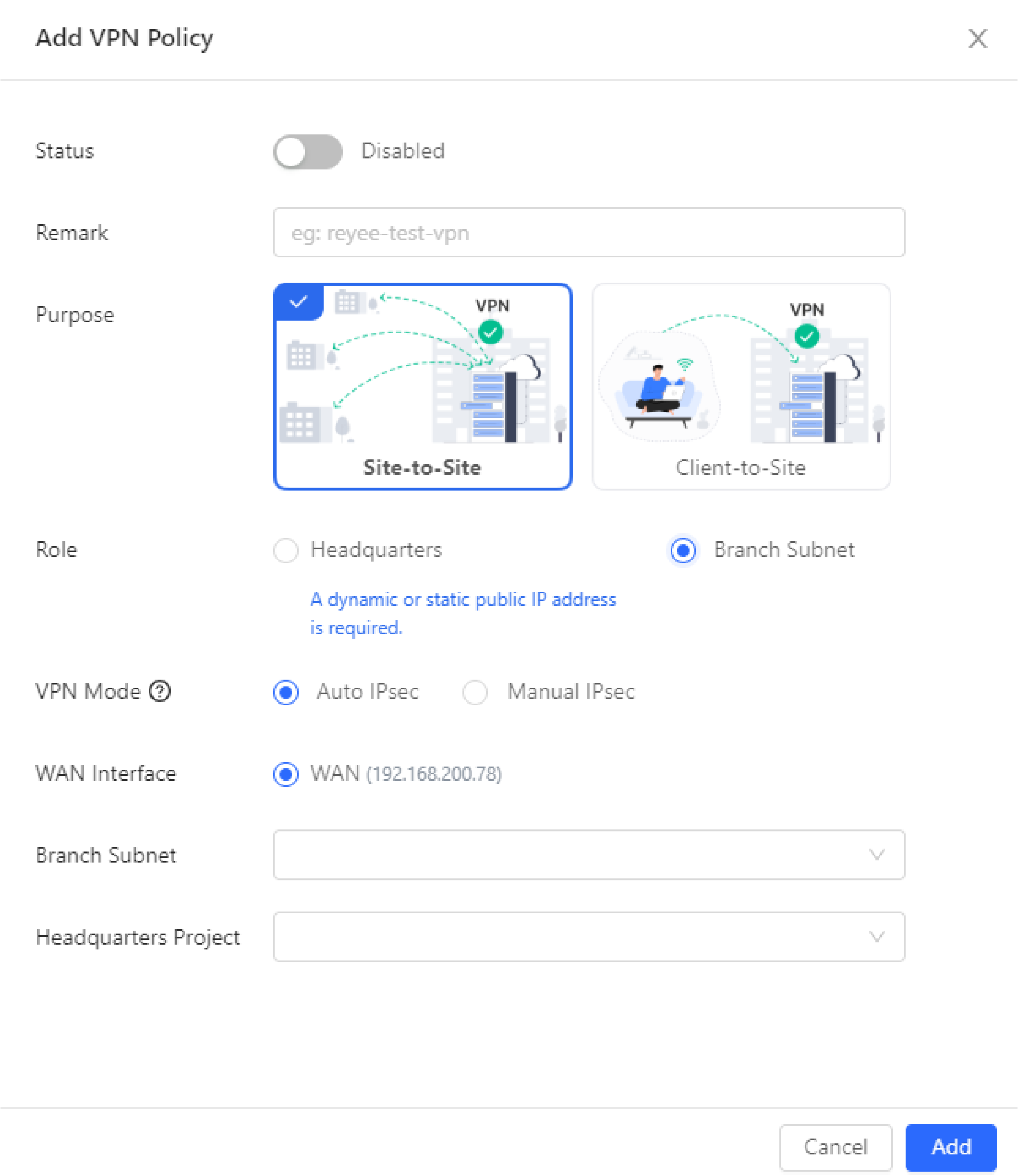
a Log in to Ruijie Cloud and click the project, to which the branch gateway belongs, to go to the configuration page.

b Choose **Configuration** > **Devices** > **Gateway** > **VPN**.



Connection Status	Name	Purpose	Config Status	VPN Mode	Action
		Site-to-Site	Disabled	Auto IPsec	
		Client-to-Site	Disabled	PPTP	
		Client-to-Site	Enable	OpenVPN	
		Client-to-Site	Disabled	L2TP Sec	

c Click **Add VPN Policy**.



Add VPN Policy

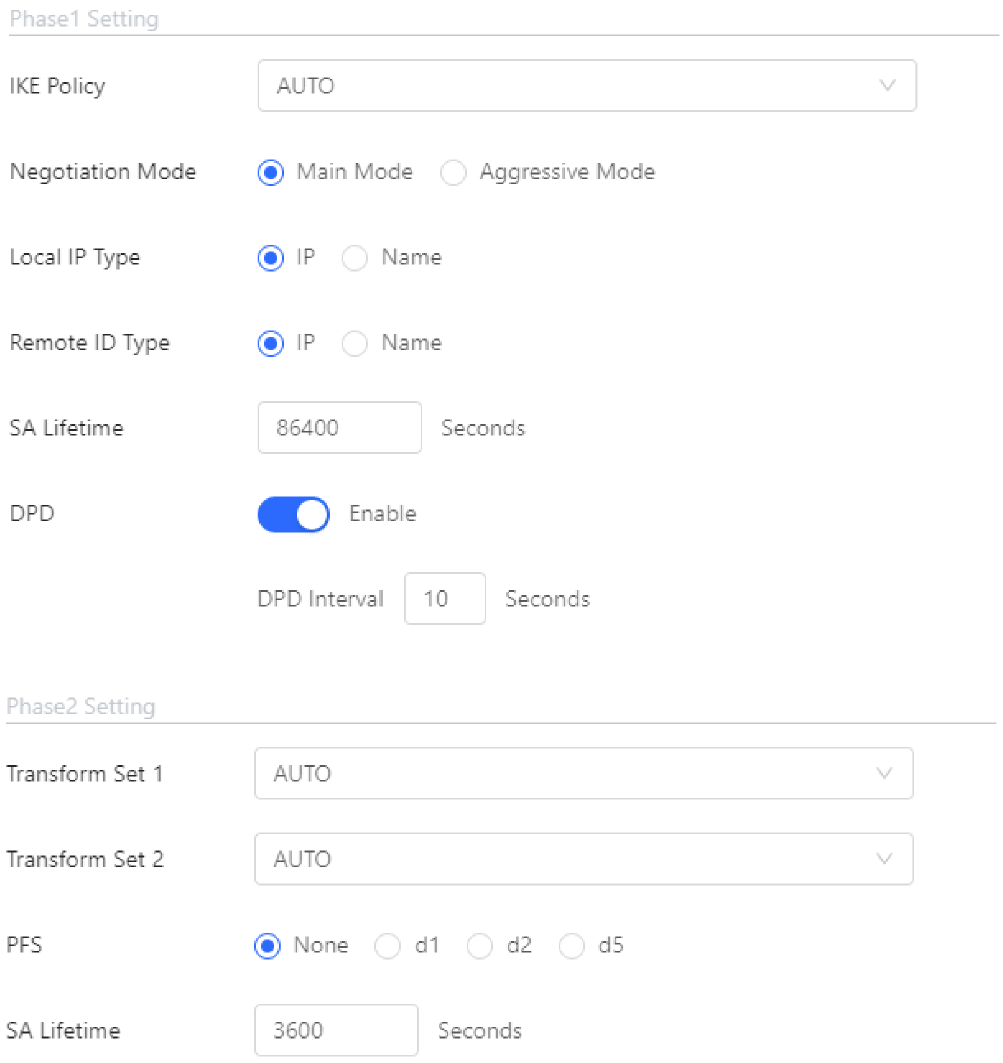
Status	Disabled
Remark	eg: reyee-test-vpn
Purpose	[✓ Site-to-Site] Client-to-Site
Role	○ Headquarters ● Branch Subnet A dynamic or static public IP address is required.
VPN Mode	● Auto IPsec ○ Manual IPsec
WAN Interface	● WAN (192.168.200.78)
Branch Subnet	
Headquarters Project	

d Set configuration items related to the branch VPN.

Table 8-2 Configuration Items Related to the Branch VPN

Parameter	Description
Status	Specify whether to enable the VPN policy. Ensure that the VPN policies of both the HQ and branch are enabled so that the VPN between the HQ and branch can be established successfully.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select **Site-to-Site**.
Role	Specify the role of the current gateway. Select **Branch Subnet** if the branch gateway needs to be connected.
VPN Mode	Auto or Manual
WAN Interface	Select the WAN Interface
Headquarters Subnet	Specify the subnet mask of the HQ gateway. Set this parameter when **VPN Mode** is set to **Manual IPsec**.
Headquarters IP/Domain	Specify the IP address or domain name of the HQ gateway. Set this parameter when **VPN Mode** is set to **Manual IPsec**.
Headquarters	Specify the name of the HQ gateway.
Branch Subnet	Specify the subnet mask of the branch gateway.
Pre-Shared Key	The pre-shared key required for IPsec encryption. Set this parameter when **VPN Mode** is set to **Manual IPsec**.

e (Optional) When **VPN Mode** is set to **Manual IPsec**, click **Advanced Settings** to set items related to Phase1 and Phase2.



Phase1 Setting

IKE Policy: AUTO

Negotiation Mode: ● Main Mode ○ Aggressive Mode

Local IP Type: ● IP ○ Name

Remote ID Type: ● IP ○ Name

SA Lifetime: 86400 Seconds

DPD: Enable

DPD Interval: 10 Seconds

Phase2 Setting

Transform Set 1: AUTO

Transform Set 2: AUTO

PFS: ● None ○ d1 ○ d2 ○ d5

SA Lifetime: 3600 Seconds

f Click **Add**.

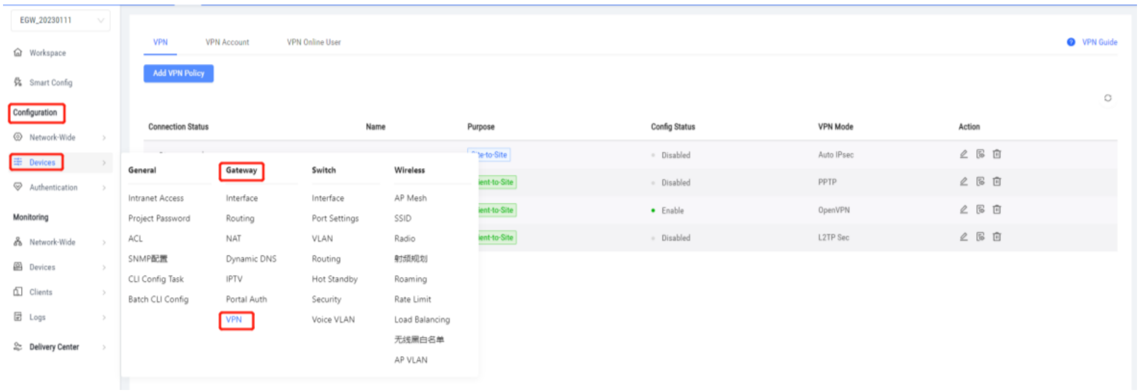
3. Configuring Client-to-Site VPN (Based on PPTP VPN)

Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

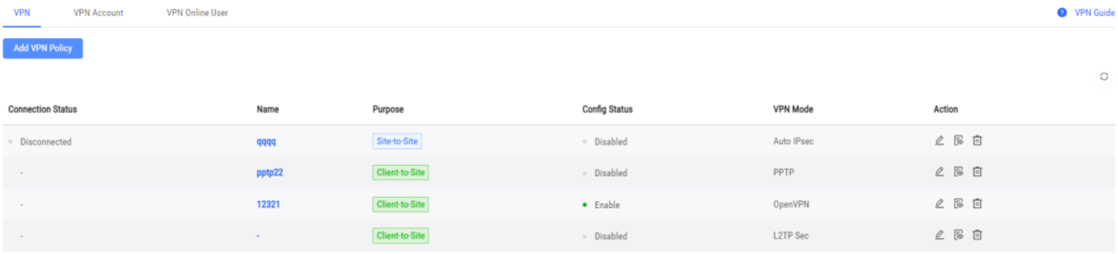
(1) Configure VPN for the HQ gateway.

a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.

b Choose **Configuration** > **Devices** > **Gateway** > **VPN** > **VPN**.

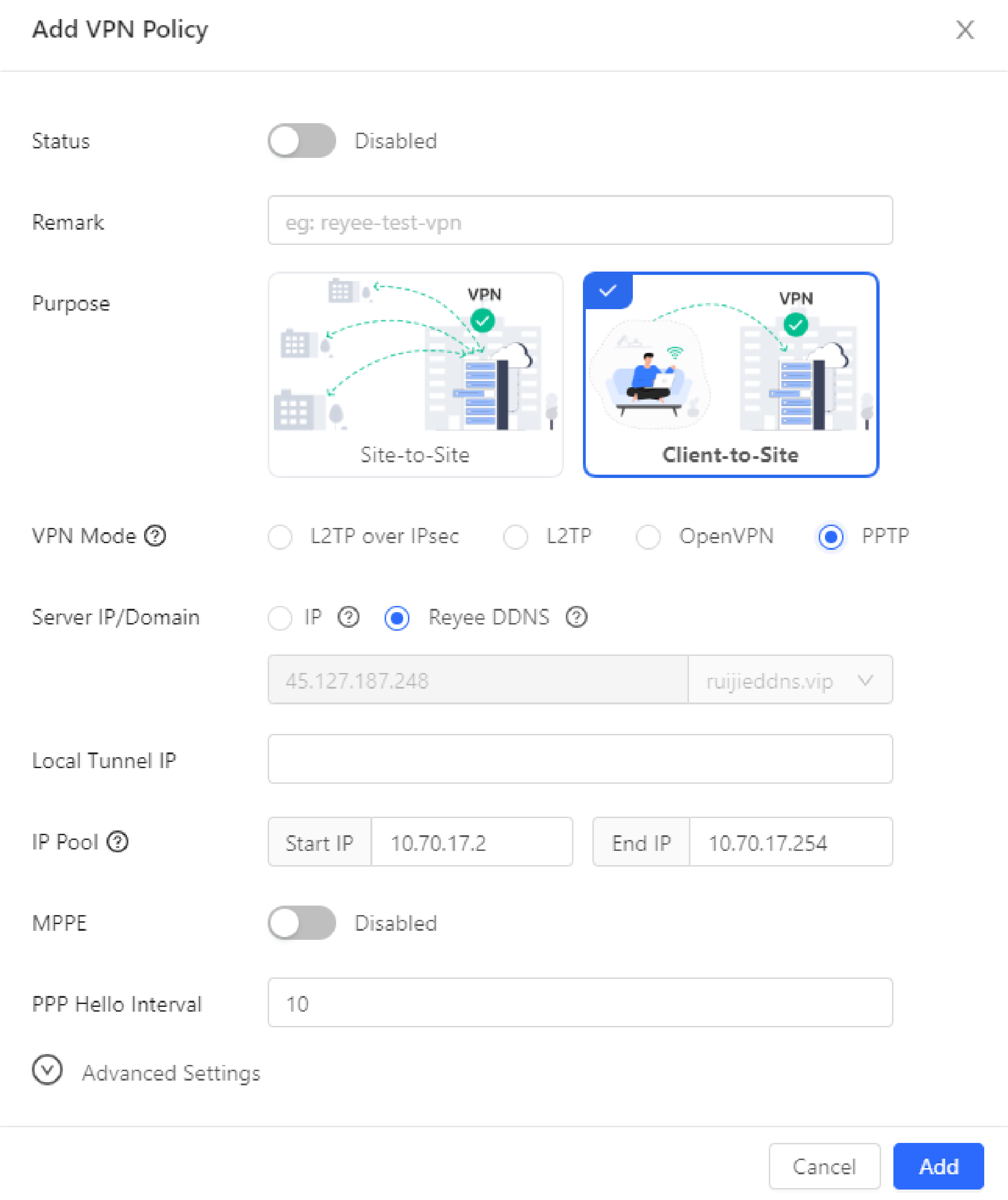


Connection Status	Name	Purpose	Config Status	VPN Mode	Action
		te-to-Site	Disabled	Auto IPsec	
		ient-to-Site	Disabled	PPTP	
		ient-to-Site	● Enable	OpenVPN	
		ient-to-Site	Disabled	L2TP Sec	



Connection Status	Name	Purpose	Config Status	VPN Mode	Action
Disconnected	qqqq	Site-to-Site	Disabled	Auto IPsec	
-	pptp22	Client-to-Site	Disabled	PPTP	
-	12321	Client-to-Site	● Enable	OpenVPN	
-	-	Client-to-Site	Disabled	L2TP Sec	

c Click **Add VPN Policy**.



Add VPN Policy

Status ○ Disabled

Remark eg: reyee-test-vpn

Purpose

VPN Mode ○ L2TP over IPsec ○ L2TP ○ OpenVPN ● PPTP

Server IP/Domain ○ IP ● Reyee DDNS

45.127.187.248 ruijieddns.vip

Local Tunnel IP

IP Pool Start IP 10.70.17.2 End IP 10.70.17.254

MPPE ○ Disabled

PPP Hello Interval 10

Advanced Settings

d Configure the VPN policy for the HQ gateway.

Table 8-3 VPN Configuration Items for the HQ Gateway

Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select **Client-to-Site**.
VPN Mode	Select the mode for implementing client-to-site VPN. Select **PPTP**.

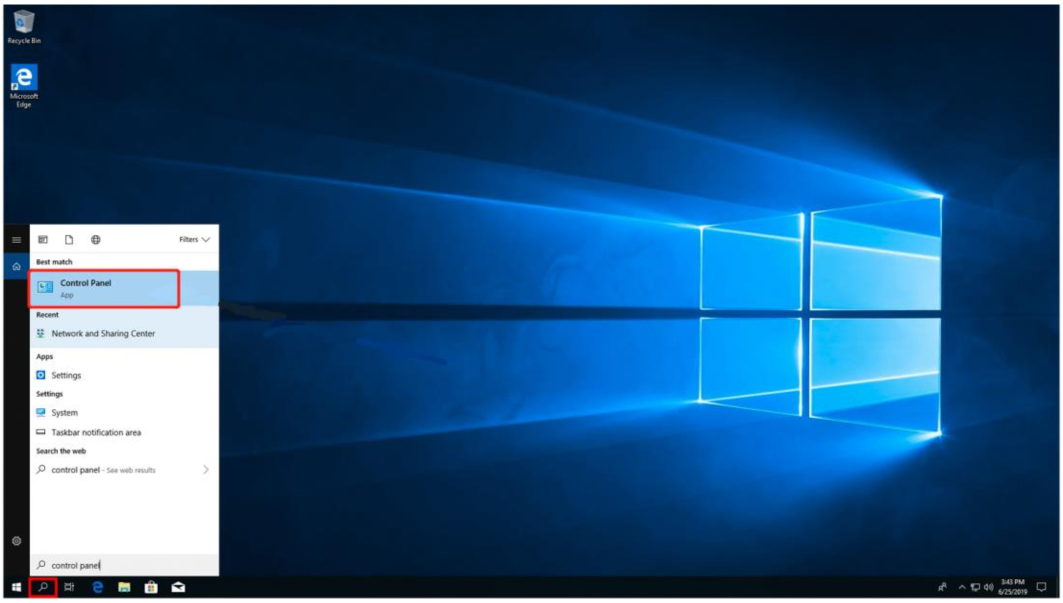
Parameter	Description
Server IP/Domain	Specify the IP address or domain name of the PPTP server.
Local Tunnel IP	Specify the local virtual IP address of the server of the VPN tunnel. After the client dials into the VPN, the client can access the server through this IP address.
IP Pool	Specify the address pool used by the PPTP server to allocate IP addresses to clients. Enter the start IP address and end IP address.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. After MPPE is enabled on the server: If **Data encryption** is set to **Optional encryption** on the client, the server and client can be connected but the server does not encrypt packets. If **Data encryption** is set to **Require encryption** on the client, the server and client can be connected and the server encrypts packets. If **Data encryption** is set to **No encryption allowed** on the client, the server and client cannot be connected. If MPPE is disabled on the server but the client requires encryption, the server and client connection fails. By default, MPPE is disabled on the server. After you enable MPPE, the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.
DNS	Specify the DNS server address pushed by the PPTP server to clients.

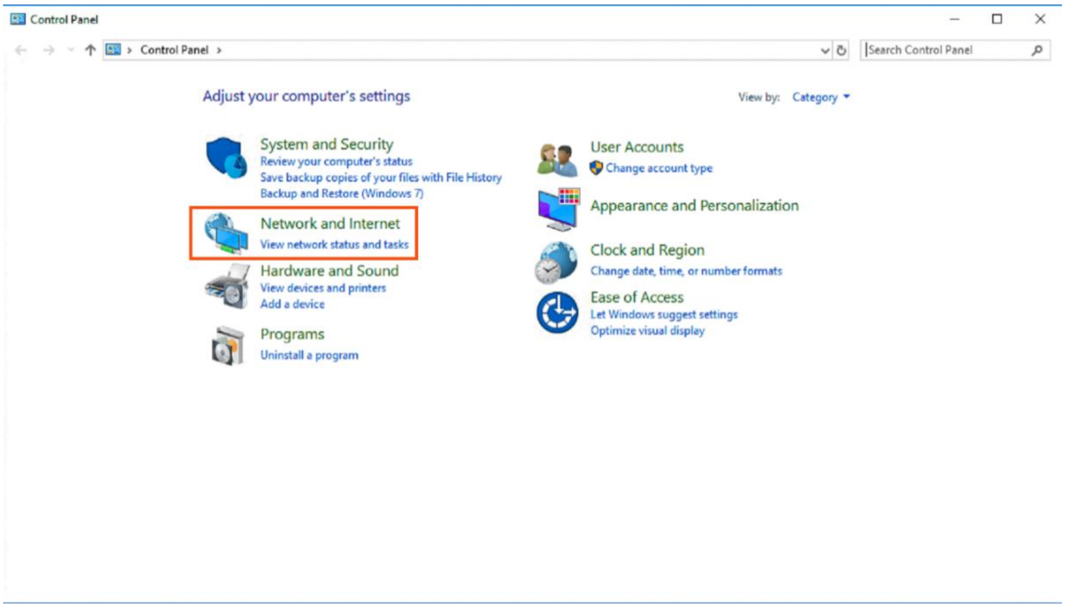
e Click **Add**.

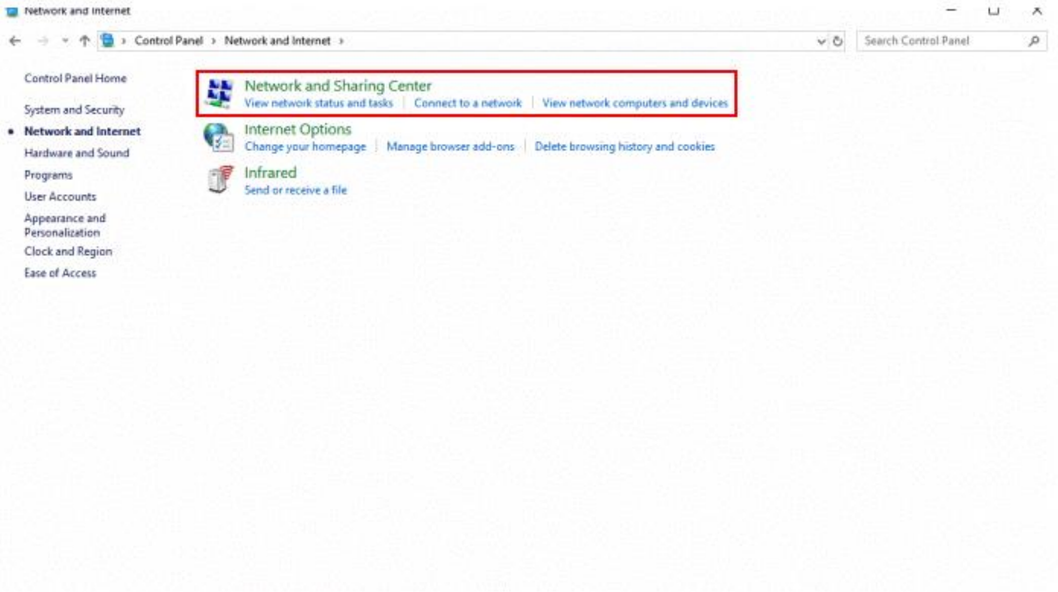
(2) Configure the client.

The following uses a Windows 10 client as an example for description. For the configuration of other clients, click **VPN Guide** at the upper right corner of the configuration page.

a Log in to the Windows client and choose **Control Panel** > **Network and Internet** > **Network and Sharing Center**.


Recycle Bin
Microsoft Edge
Filters
Best match
Control Panel
App
Recent
Network and Sharing Center
Apps
Settings
Settings
System
Taskbar notification area
Search the web
control panel - See web results
control panel
3:43 PM
6/25/2019


Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display



Network and Internet

Control Panel › Network and Internet ›

Search Control Panel

Control Panel Home

System and Security

Network and Internet

Hardware and Sound

Programs

User Accounts

Appearance and Personalization

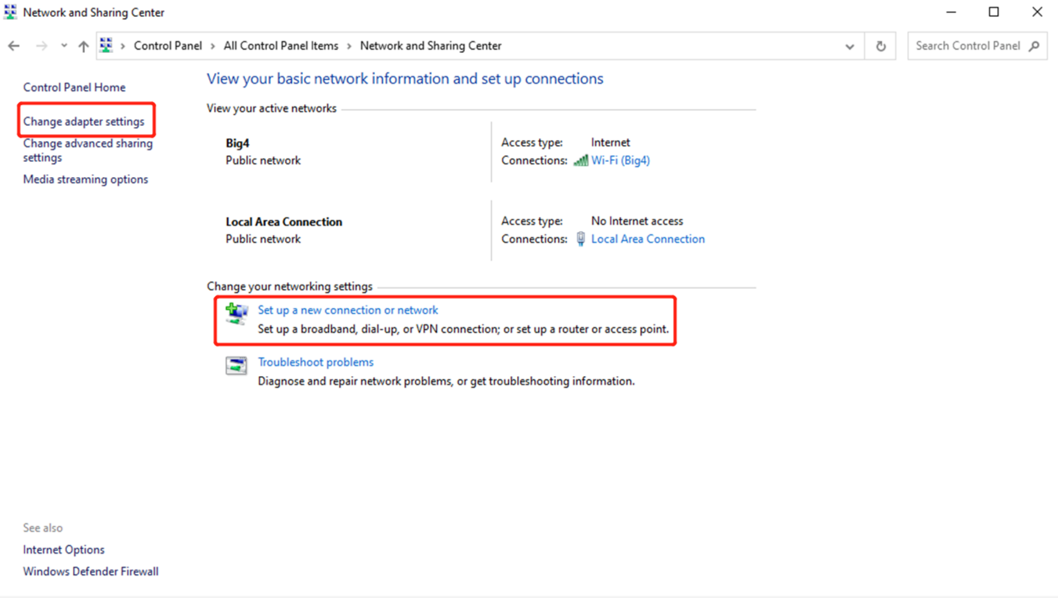
Clock and Region

Ease of Access

Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices

Internet Options
Change your homepage | Manage browser add-ons | Delete browsing history and cookies

Infrared
Send or receive a file



Network and Sharing Center

Control Panel › All Control Panel Items › Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

Media streaming options

View your basic network information and set up connections

View your active networks

Big4
Public network

Access type: Internet
Connections: Wi-Fi (Big4)

Local Area Connection
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

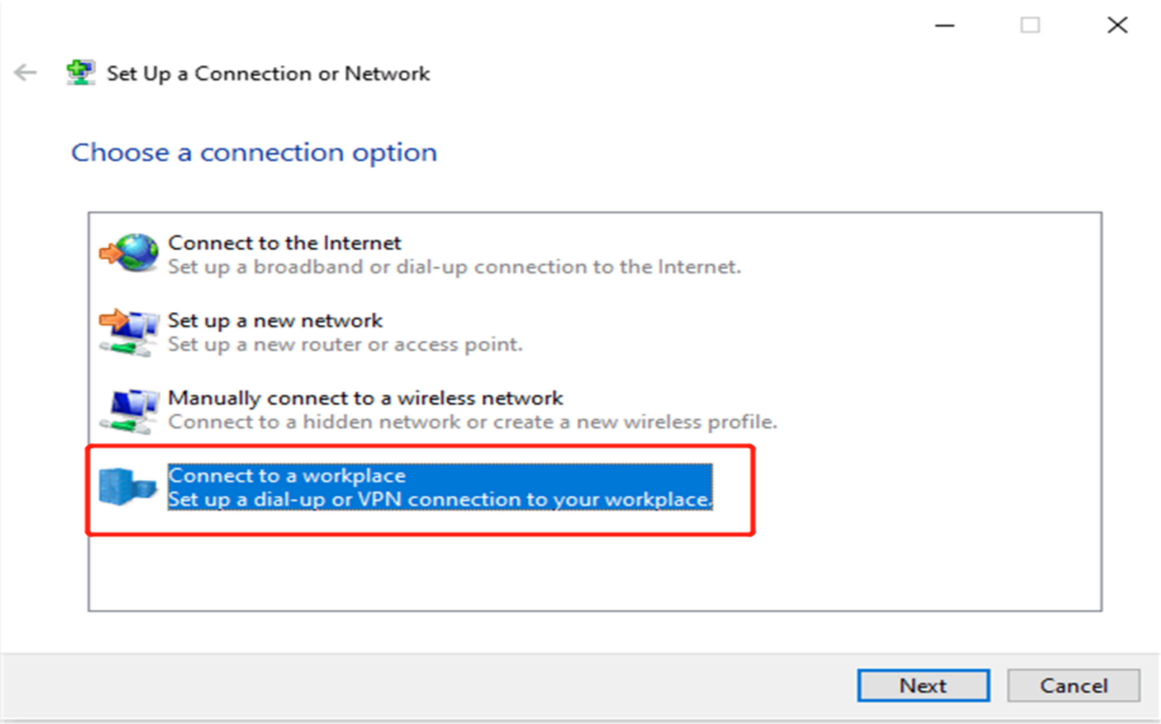
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also

Internet Options

Windows Defender Firewall

b Configure a VPN connection.



Set Up a Connection or Network

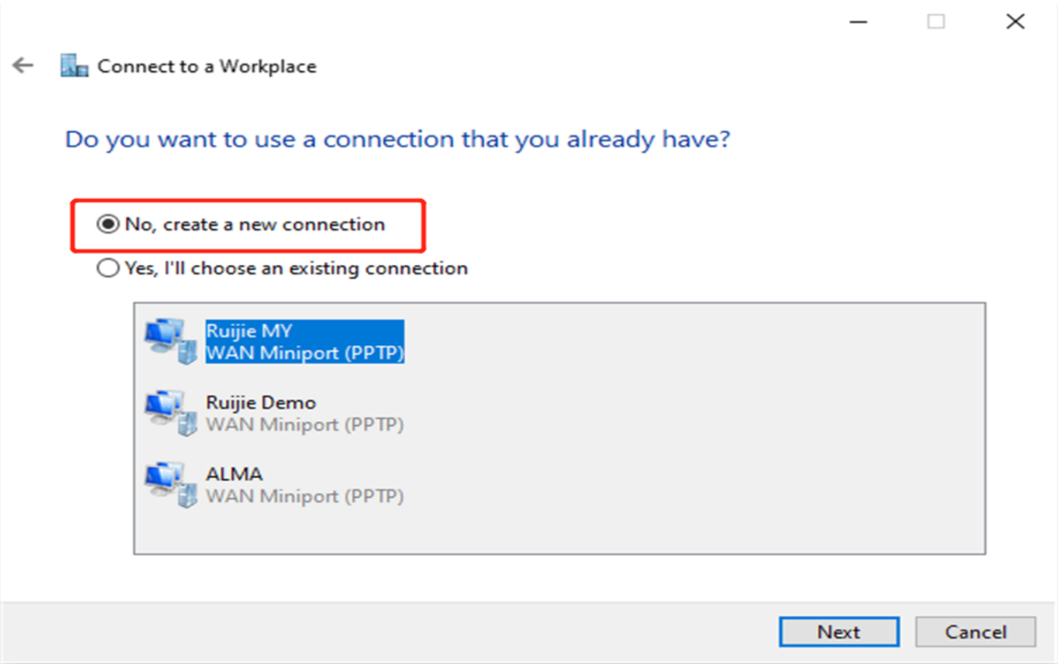
Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.



Connect to a Workplace

Do you want to use a connection that you already have?

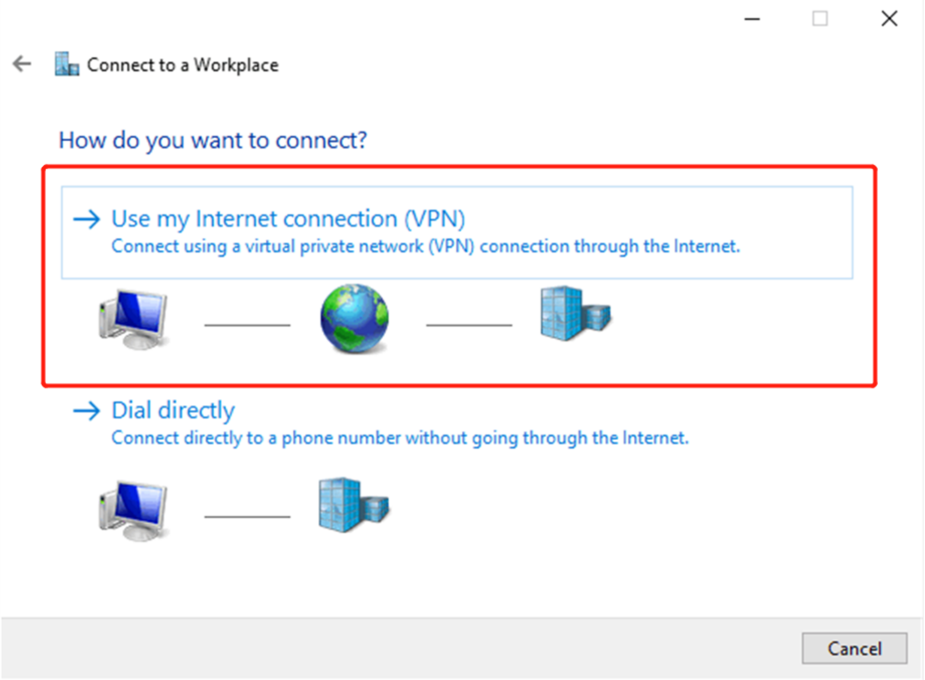
● No, create a new connection

○ Yes, I'll choose an existing connection

Ruijie MY
WAN Miniport (PPTP)

Ruijie Demo
WAN Miniport (PPTP)

ALMA
WAN Miniport (PPTP)

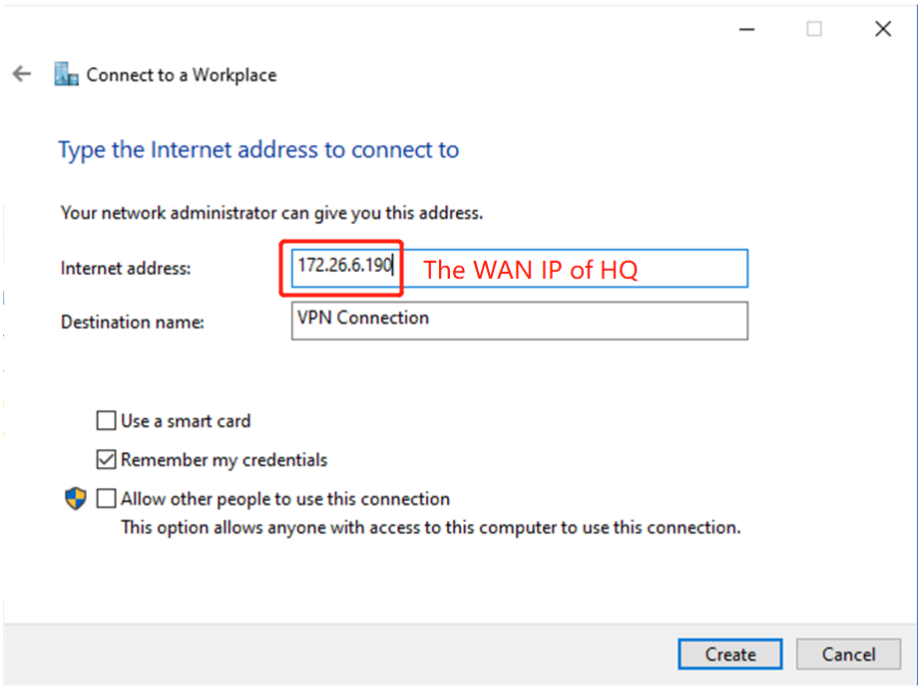


Connect to a Workplace

How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.26.6.190 The WAN IP of HQ

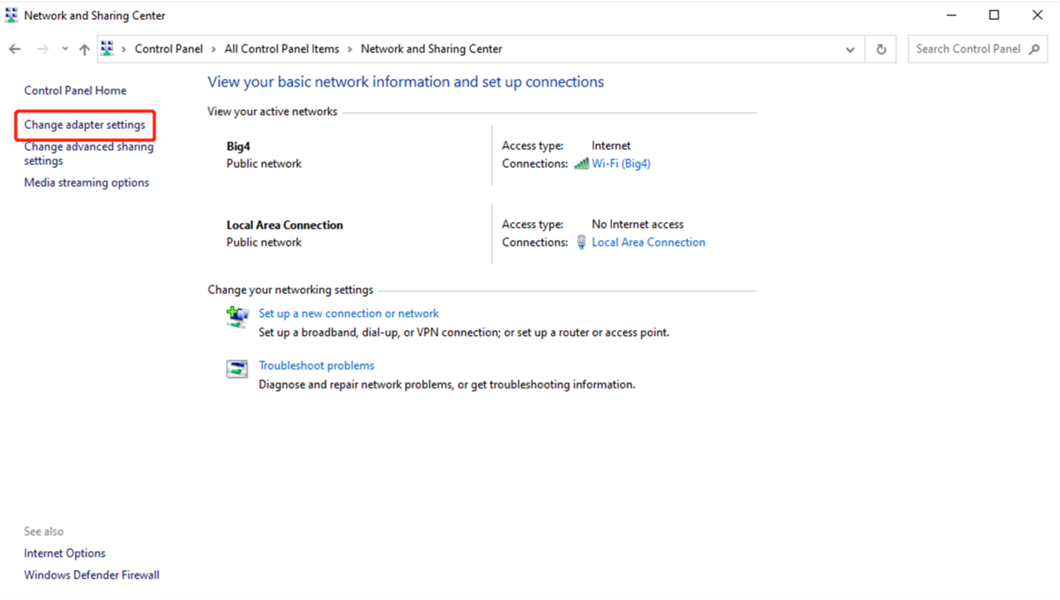
Destination name: VPN Connection

□ Use a smart card

☑ Remember my credentials

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

c Change settings of the adapter.



Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

Media streaming options

View your basic network information and set up connections

View your active networks

Big4
Public network

Access type: Internet
Connections: Wi-Fi (Big4)

Local Area Connection
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

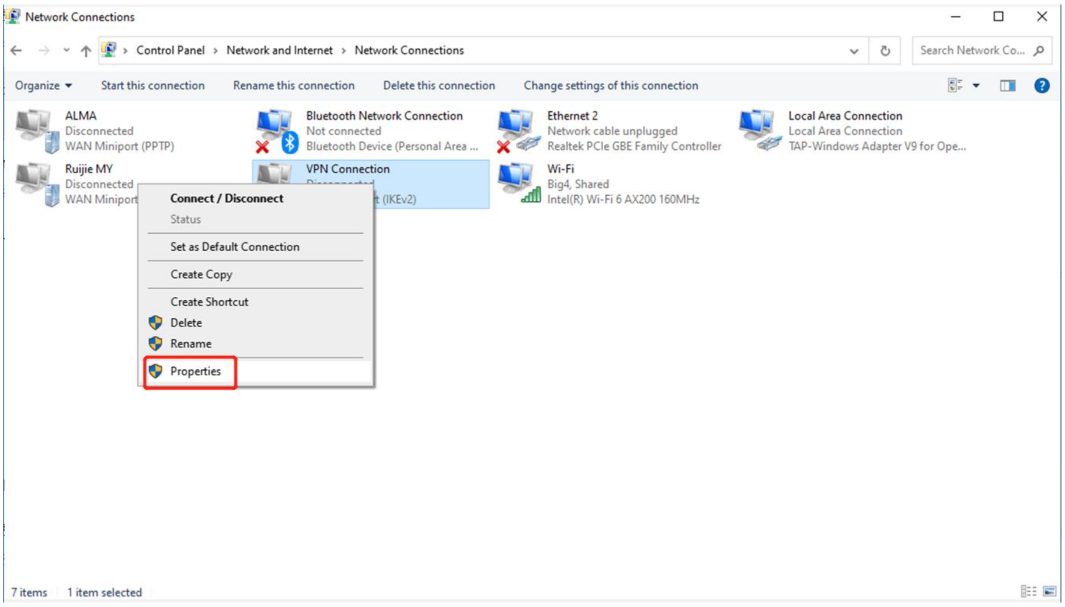
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also

Internet Options

Windows Defender Firewall



Network Connections

Control Panel > Network and Internet > Network Connections

Search Network Co...

Organize ▾ Start this connection Rename this connection Delete this connection Change settings of this connection

ALMA
Disconnected
WAN Miniport (PPTP)

Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

Ethernet 2
Network cable unplugged
Realtek PCIe GBE Family Controller

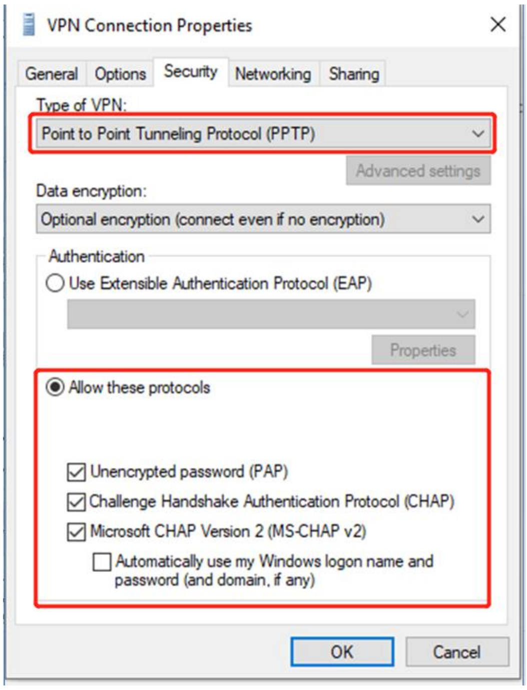
Local Area Connection
Local Area Connection
TAP-Windows Adapter V9 for Ope...

Ruijie MY
Disconnected
WAN Miniport

VPN Connection
Disconnected
(IKEv2)

Wi-Fi
Big4, Shared
Intel(R) Wi-Fi 6 AX200 160MHz

7 items 1 item selected



VPN Connection Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Point to Point Tunneling Protocol (PPTP)

Advanced settings

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

☑ Unencrypted password (PAP)

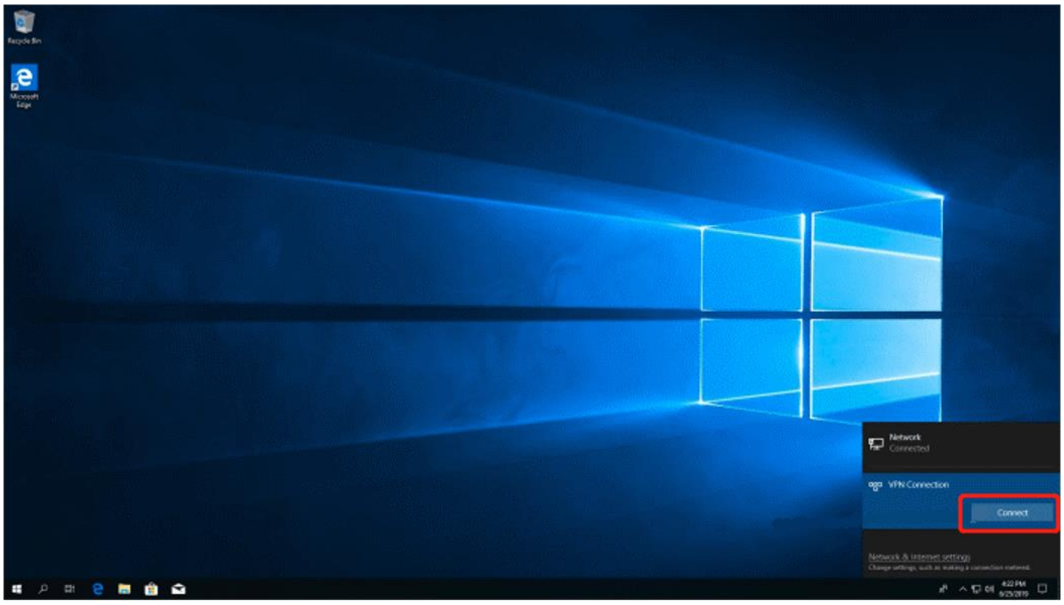
☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

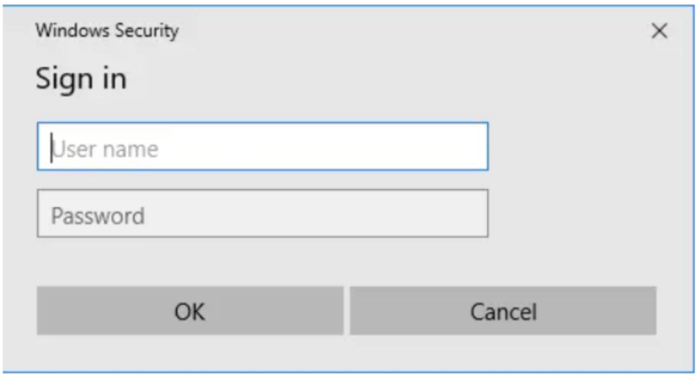
□ Automatically use my Windows logon name and password (and domain, if any)

OK Cancel

d Check the VPN connection status.



Recycle Bin
Microsoft Edge
Network
Connected
VPN Connection
Connect
Network & Internet settings
Change settings, such as making a connection metered.
4:22 PM
9/25/2019



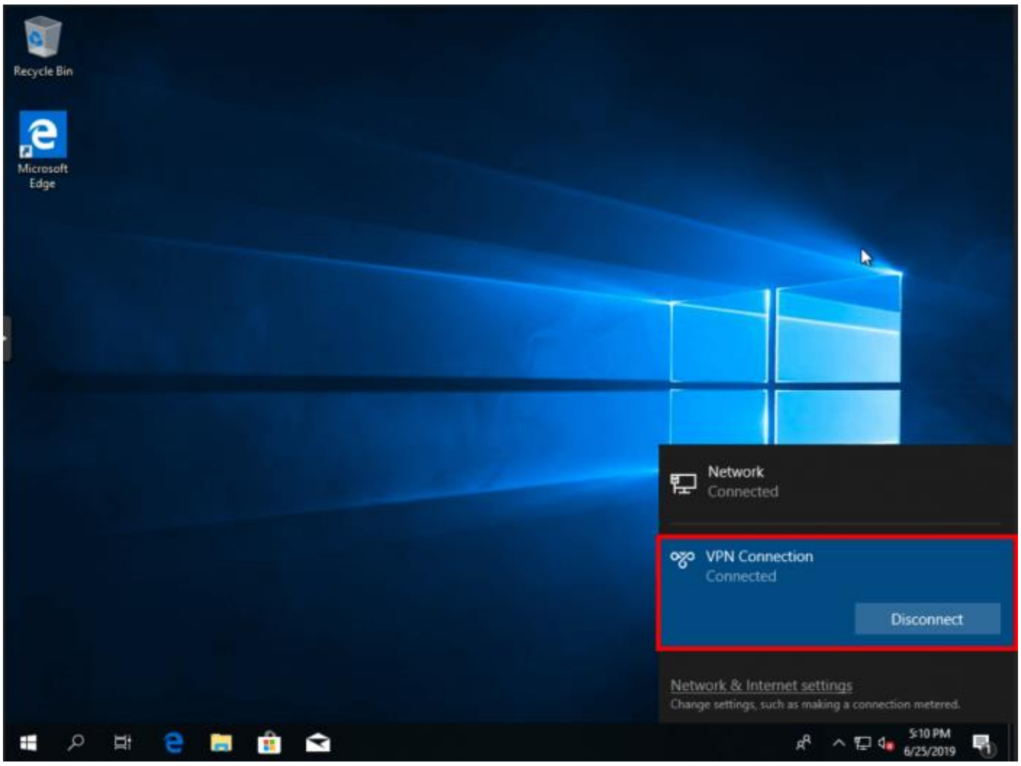
Windows Security

Sign in

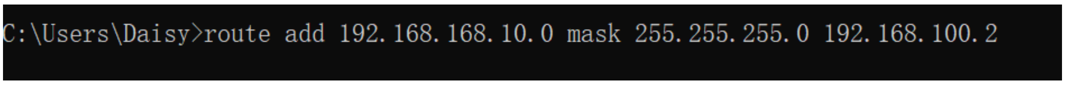
User name

Password

OK Cancel



e If your PC cannot access the internal devices of the HQ after the VPN connection is set up, run the **route add** command and add the static route on your PC. The following figure shows a command example. The IP address in this command is the virtual IP address obtained by the PC from the HQ. Then, the PC can access the internal devices of the HQ.



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

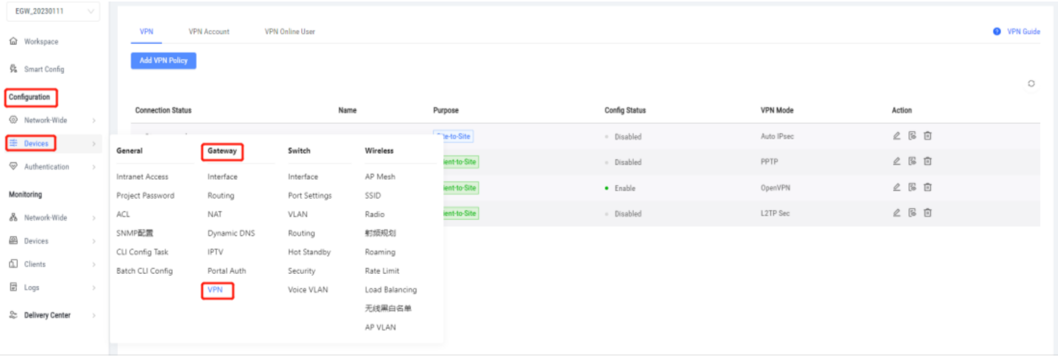
4. Configuring Client-to-Site VPN (Based on L2TP VPN)

Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

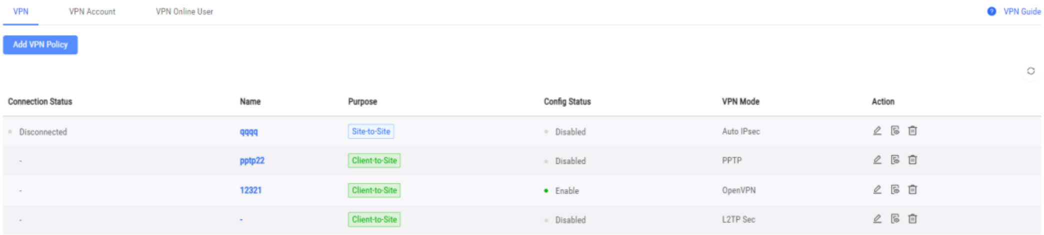
(1) Configure VPN for the HQ gateway.

a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.

b Choose **Configuration** > **Devices** > **Gateway** > **VPN**.

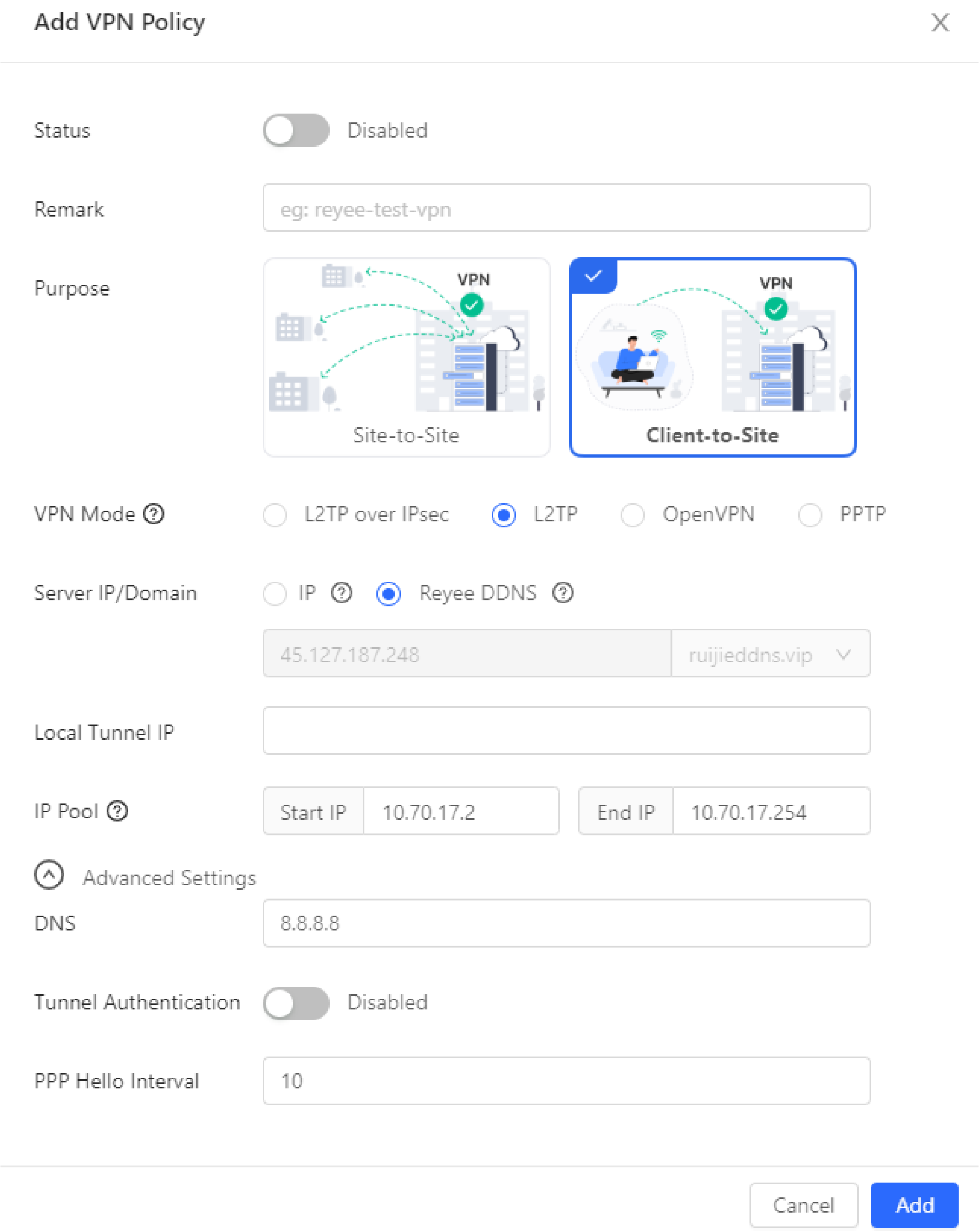


Connection Status	Name	Purpose	Config Status	VPN Mode	Action
		te-to-Site	Disabled	Auto IPsec	
		ient-to-Site	Disabled	PPTP	
		ient-to-Site	● Enable	OpenVPN	
		ient-to-Site	Disabled	L2TP Sec	



Connection Status	Name	Purpose	Config Status	VPN Mode	Action
Disconnected	qqqq	Site-to-Site	Disabled	Auto IPsec	
-	pptp22	Client-to-Site	Disabled	PPTP	
-	12321	Client-to-Site	● Enable	OpenVPN	
-	-	Client-to-Site	Disabled	L2TP Sec	

c Click **Add VPN Policy**.



Add VPN Policy

Status: Disabled

Remark: eg: reyee-test-vpn

Purpose: ○ Site-to-Site ☑ Client-to-Site

VPN Mode: ○ L2TP over IPsec ● L2TP ○ OpenVPN ○ PPTP

Server IP/Domain: ○ IP ● Reyee DDNS

45.127.187.248 ruijieddns.vip

Local Tunnel IP:

IP Pool: Start IP 10.70.17.2 End IP 10.70.17.254

Advanced Settings

DNS: 8.8.8.8

Tunnel Authentication: Disabled

PPP Hello Interval: 10

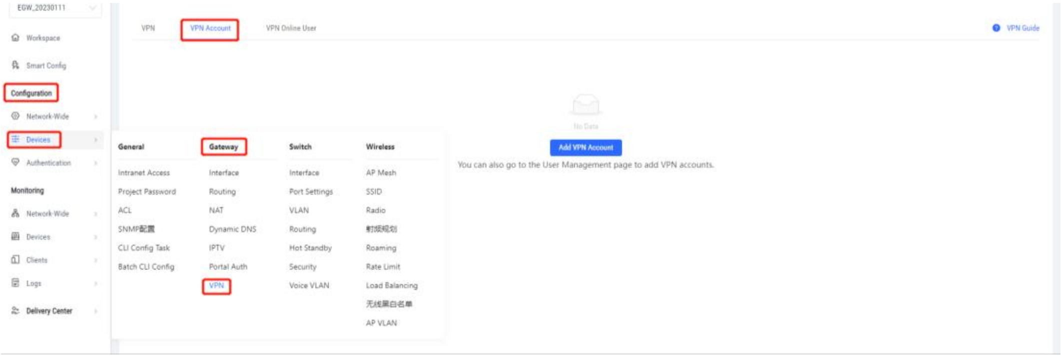
d Configure the VPN policy for the HQ gateway.

Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select **Client-to-Site**.
VPN Mode	Select the mode for implementing client-to-site VPN. Select **L2TP**.
Server IP/Domain	Specify the IP address or domain name of the L2TP server.
Local Tunnel IP	Specify the local virtual IP address of the server of the VPN tunnel. After the client dials into the VPN, the client can access the server through this IP address.
IP Pool	Specify the address pool used by the L2TP server to allocate IP addresses to clients.
DNS	Specify the DNS server address pushed by the L2TP server to clients.
Tunnel Authentication	Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to configure a tunnel authentication key. By default, tunnel authentication is disabled. The tunnel authentication request can be initiated by clients. If tunnel authentication is enabled on one end, a tunnel to the peer can be established only when tunnel authentication is also enabled on the peer and consistent keys are configured on the two ends. Otherwise, the local end will automatically shut down the tunnel connection. If tunnel authentication is disabled on both ends, no authentication key is required for tunnel establishment. When a PC functions as the client to access the L2TP server, you are advised not to enable tunnel authentication on the L2TP server.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.
DNS	Specify the DNS server address pushed by the PPTP server to clients.

(2) Set a VPN account.

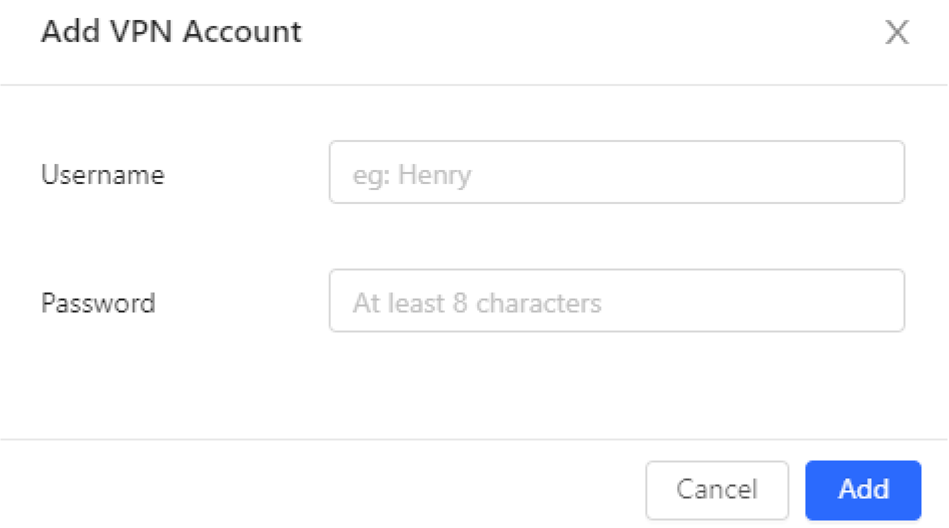
Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

a Choose **Configuration** > **Devices** > **Gateway** > **VPN** > **VPN Account**.



You can also go to the User Management page to add VPN accounts.

b Click **Add VPN Account**.



Add VPN Account

Username: eg: Henry

Password: At least 8 characters

c Configure items related to a VPN account.

Table 8-4 VPN Account Configuration Items

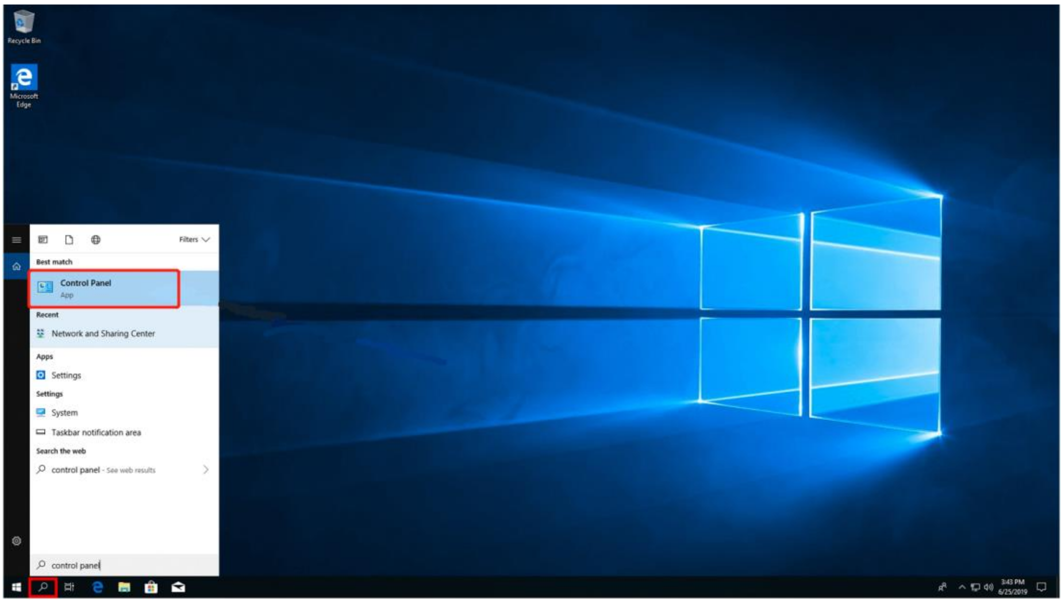
Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

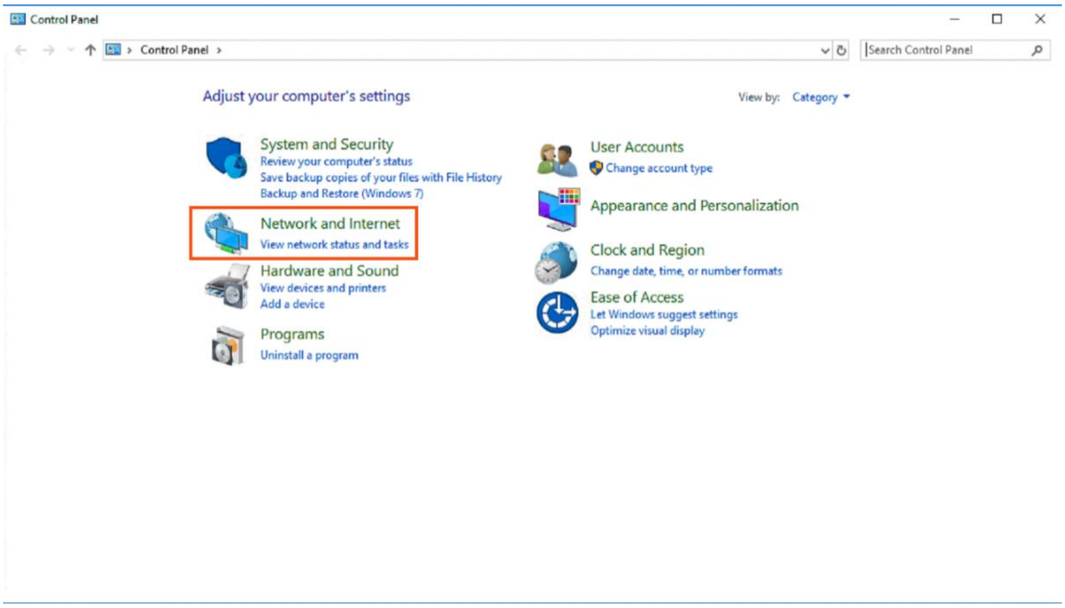
d Click **Add**.

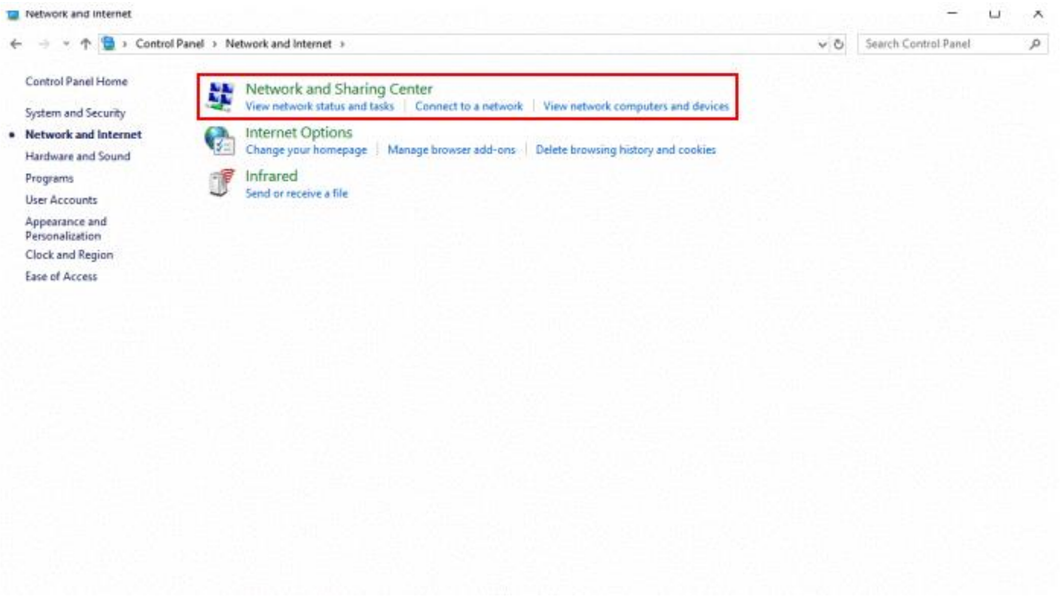
(3) Configure the client.

The following uses a Windows 10 client as an example for description. For the configuration of other clients, click **VPN Guide** at the upper right corner of the configuration page.

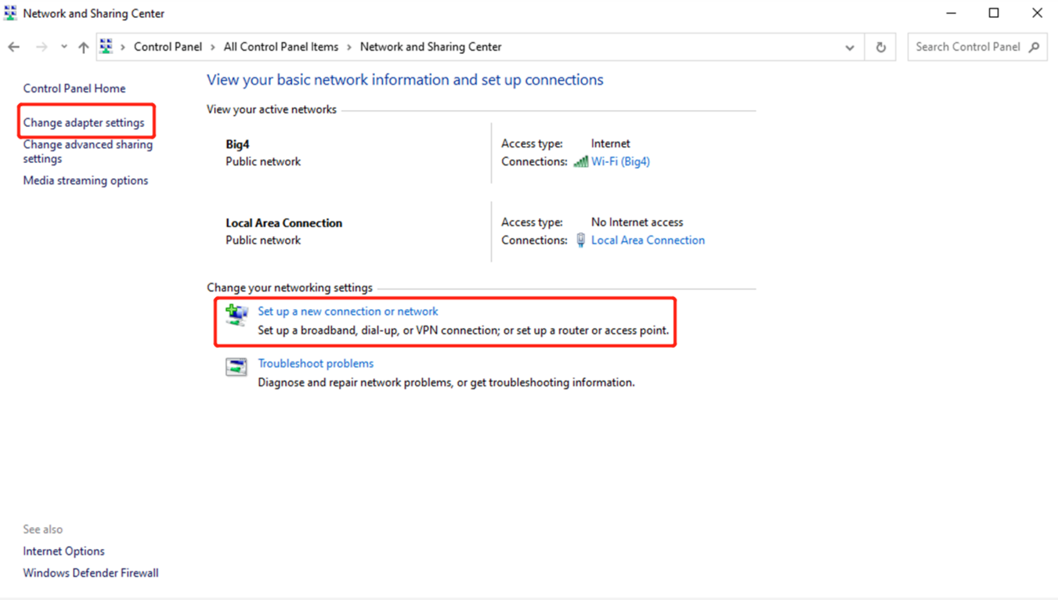
a Choose **Control Pane** > **Network and Internet** > **Network and Sharing Center**.


Recycle Bin
Microsoft Edge
Filters
Best match
Control Panel
App
Recent
Network and Sharing Center
Apps
Settings
Settings
System
Taskbar notification area
Search the web
control panel - See web results
control panel


Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display


Network and Internet
Control Panel › Network and Internet ›
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Internet Options
Change your homepage
Manage browser add-ons
Delete browsing history and cookies
Infrared
Send or receive a file

b Configure a VPN connection.



Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

Media streaming options

View your basic network information and set up connections

View your active networks

Big4
Public network

Access type: Internet
Connections: Wi-Fi (Big4)

Local Area Connection
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

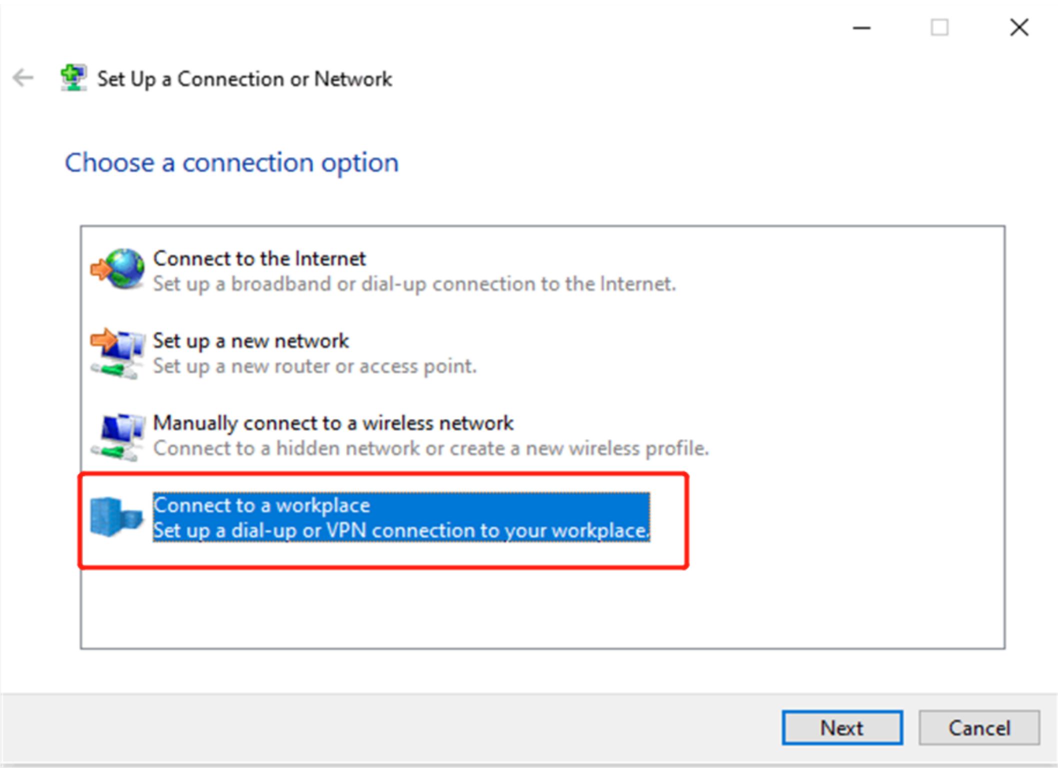
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also

Internet Options

Windows Defender Firewall



Set Up a Connection or Network

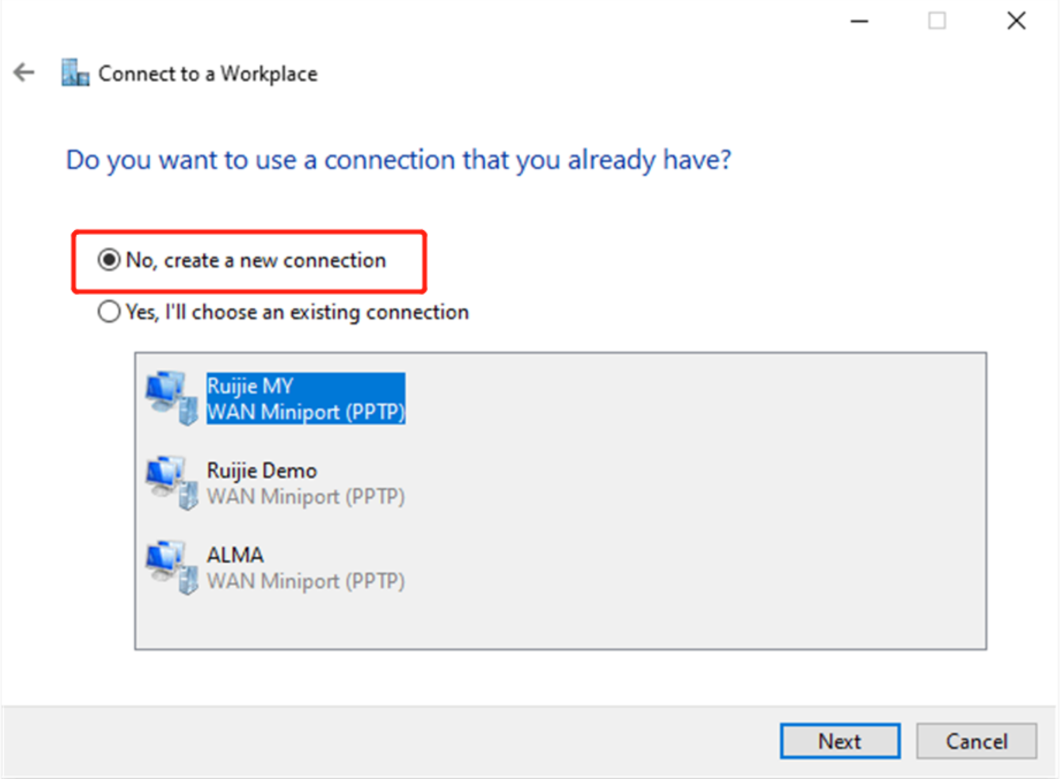
Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.



Connect to a Workplace

Do you want to use a connection that you already have?

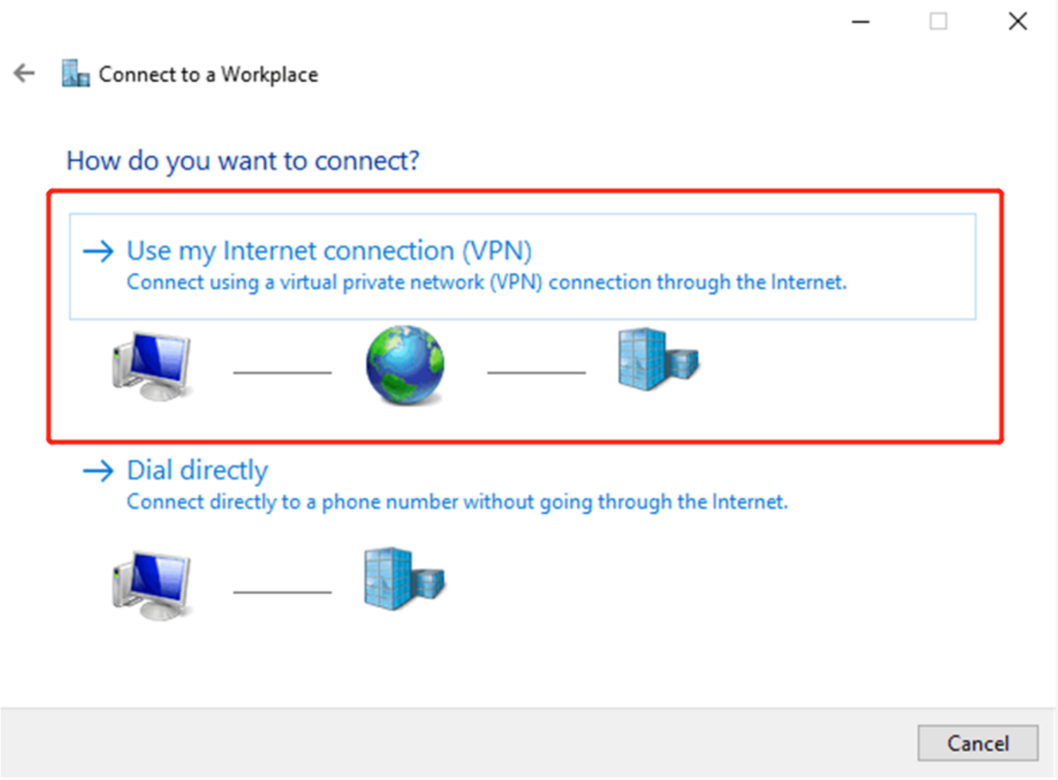
● No, create a new connection

○ Yes, I'll choose an existing connection

Ruijie MY
WAN Miniport (PPTP)

Ruijie Demo
WAN Miniport (PPTP)

ALMA
WAN Miniport (PPTP)

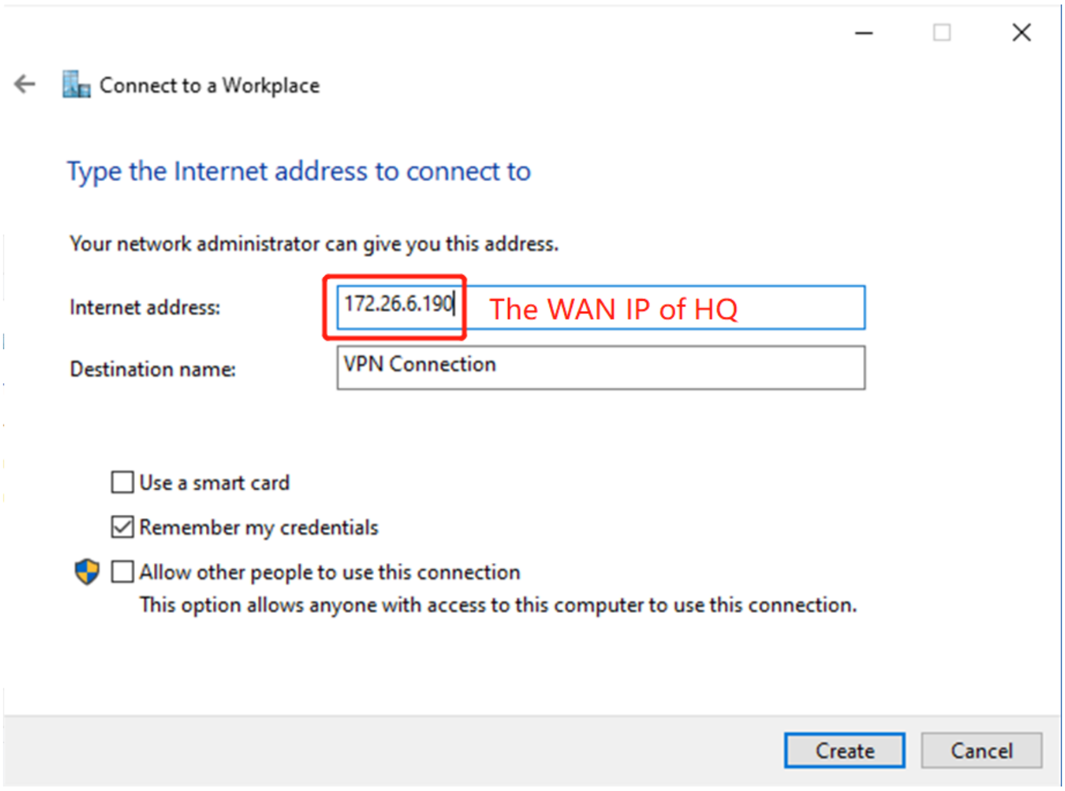


Connect to a Workplace

How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.26.6.190

The WAN IP of HQ

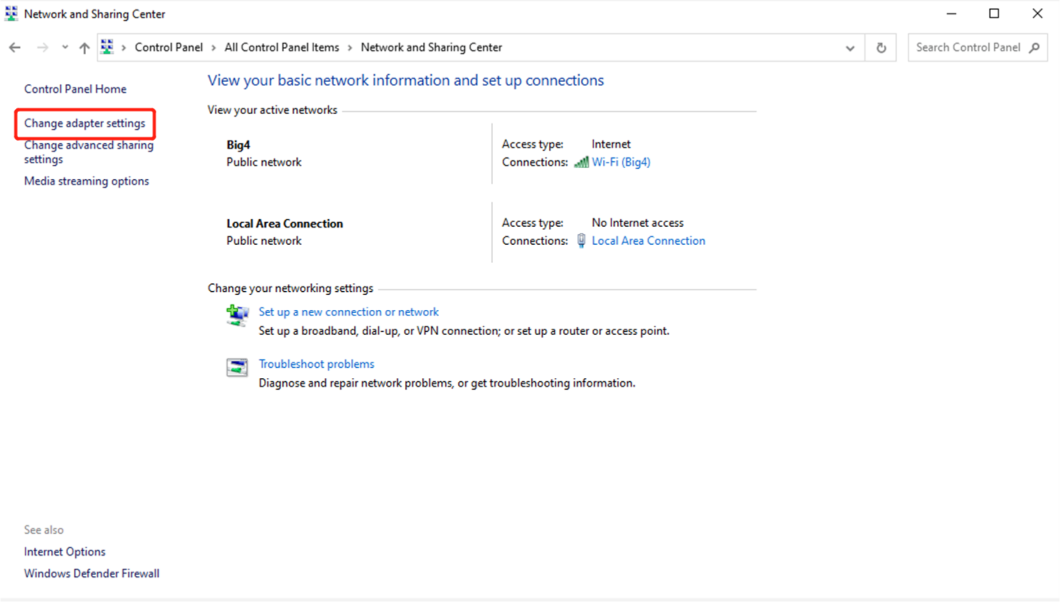
Destination name: VPN Connection

□ Use a smart card

☑ Remember my credentials

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

c Change adapter's settings.



Network and Sharing Center

Control Panel › All Control Panel Items › Network and Sharing Center

View your basic network information and set up connections

View your active networks

Big4
Public network

Access type: Internet
Connections: Wi-Fi (Big4)

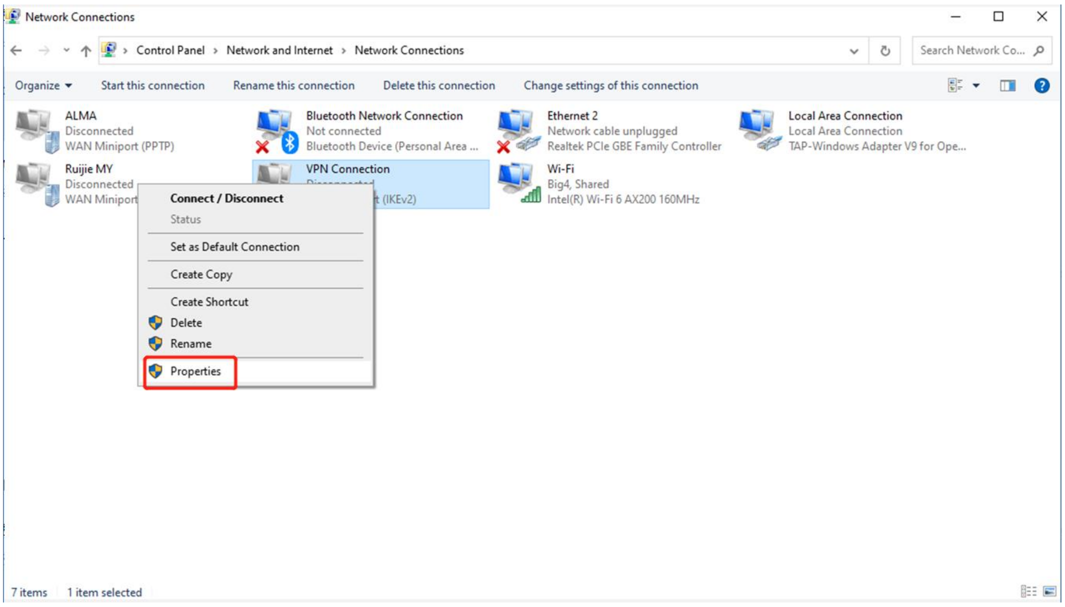
Local Area Connection
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.



Network Connections

Control Panel > Network and Internet > Network Connections

Search Network Co...

Organize ▾ Start this connection Rename this connection Delete this connection Change settings of this connection

ALMA
Disconnected
WAN Miniport (PPTP)

Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

Ethernet 2
Network cable unplugged
Realtek PCIe GBE Family Controller

Local Area Connection
Local Area Connection
TAP-Windows Adapter V9 for Ope...

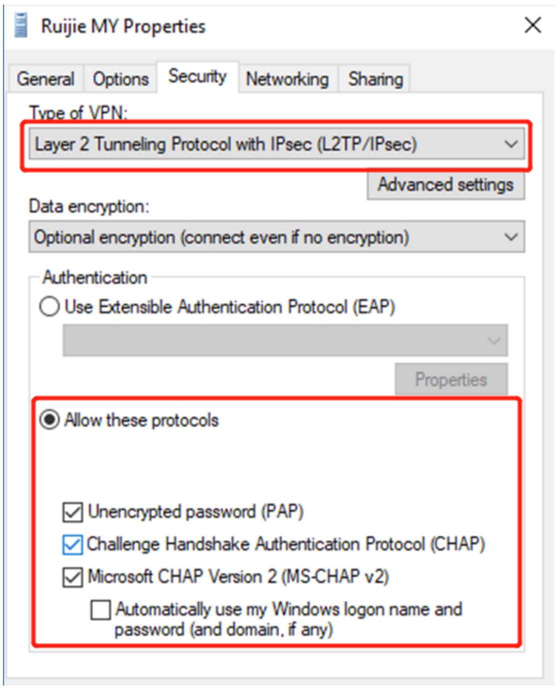
Ruijie MY
Disconnected
WAN Miniport

VPN Connection
(IKEv2)

Wi-Fi
Big4, Shared
Intel(R) Wi-Fi 6 AX200 160MHz

Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties

7 items 1 item selected



Ruijie MY Properties

General Options Security Networking Sharing

Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Advanced settings

Data encryption:
Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

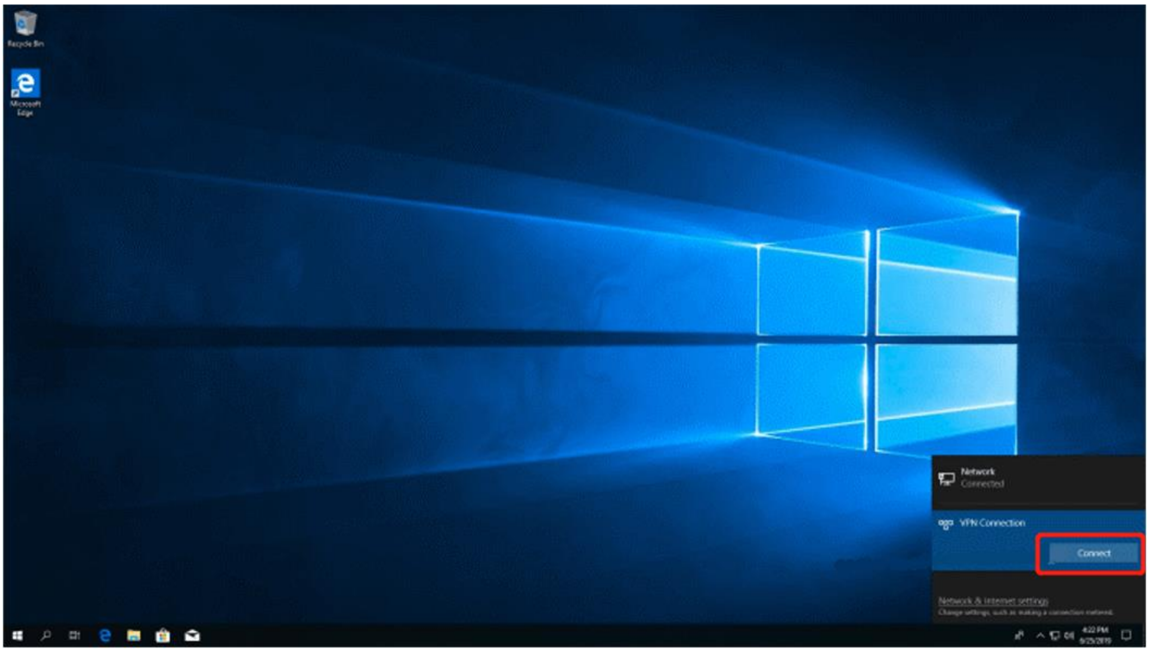
☑ Unencrypted password (PAP)

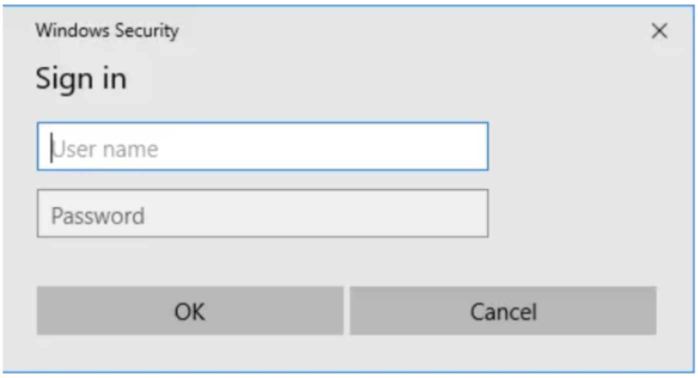
☑ Challenge Handshake Authentication Protocol (CHAP)

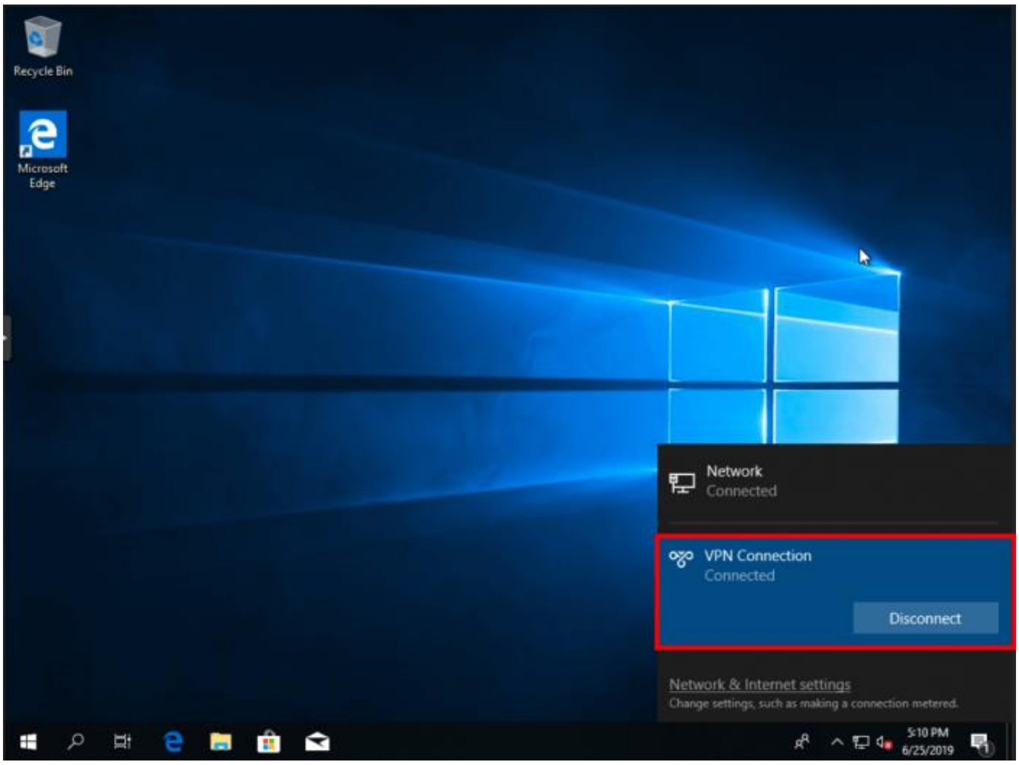
☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

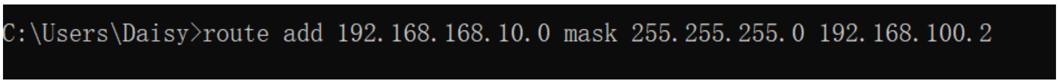
d Check the VPN connection status.


Recycle Bin
Microsoft Edge
Network
Connected
VPN Connection
Connect
Network & Internet settings
Change settings, such as making a connection metered.
4:22 PM
6/25/2019


Windows Security
Sign in
User name
Password
OK
Cancel


Recycle Bin
Microsoft Edge
Network
Connected
VPN Connection
Connected
Disconnect
Network & Internet settings
Change settings, such as making a connection metered.
5:10 PM
6/25/2019

e If your PC cannot access internal devices of the HQ after the VPN connection is set up, run the **route add** command and add the static route on your PC. The following figure shows a command example. The IP address in this command is the virtual IP address obtained by the PC from the HQ. Then, the PC can access the internal devices of the HQ.



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

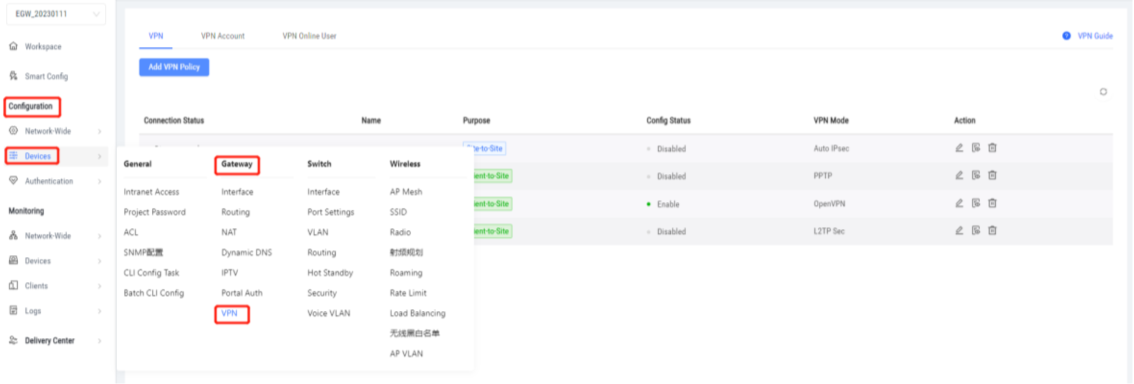
5. Configuring Client-to-Site VPN (Based on L2TP over IPSec VPN)

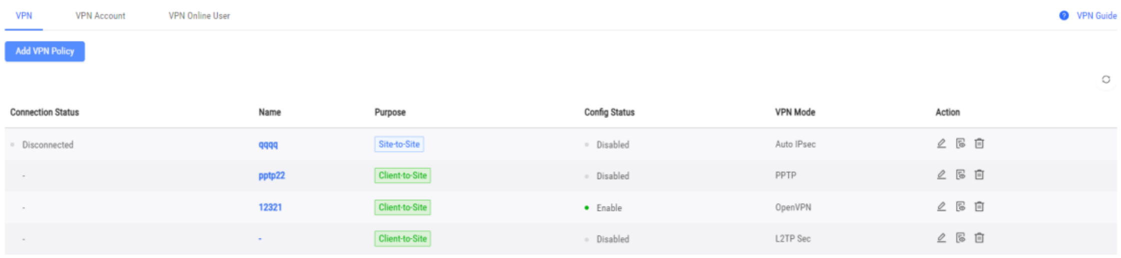
Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

(1) Configure VPN for the HQ gateway.

a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.

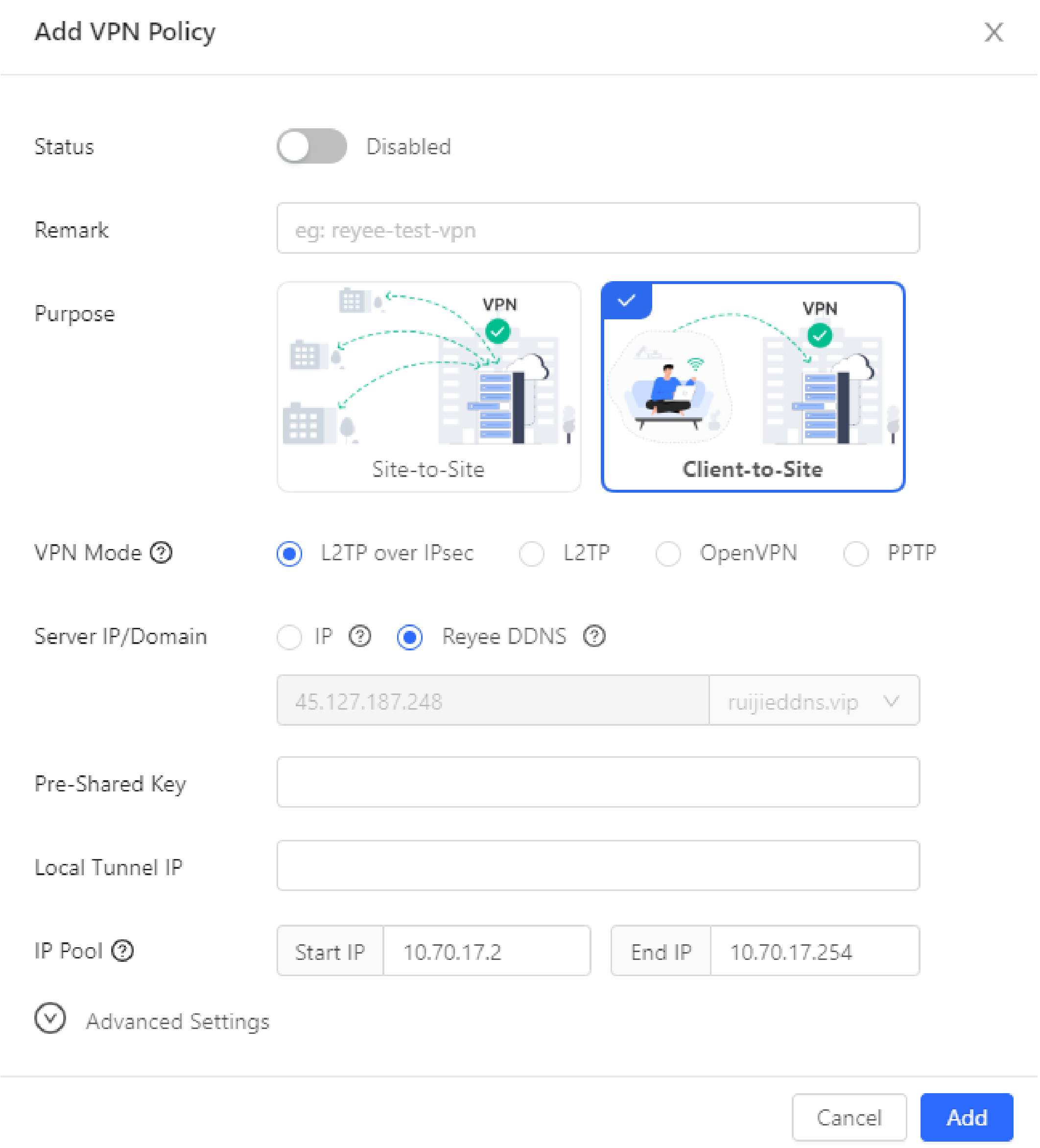
b Choose **Configuration** > **Devices** > **Gateway** > **VPN** > **VPN**.





Connection Status	Name	Purpose	Config Status	VPN Mode	Action
Disconnected	qqqq	Site-to-Site	Disabled	Auto IPsec	
-	pptp22	Client-to-Site	Disabled	PPTP	
-	12321	Client-to-Site	● Enable	OpenVPN	
-	-	Client-to-Site	Disabled	L2TP Sec	

c Click **Add VPN Policy**.



Add VPN Policy

Status: Disabled

Remark: eg: reyee-test-vpn

Purpose: Site-to-Site / ☑ Client-to-Site

VPN Mode: ● L2TP over IPsec ○ L2TP ○ OpenVPN ○ PPTP

Server IP/Domain: ○ IP ● Reyee DDNS

45.127.187.248 ruijieddns.vip

Pre-Shared Key:

Local Tunnel IP:

IP Pool: Start IP 10.70.17.2 End IP 10.70.17.254

Advanced Settings

Cancel Add

d Configure the VPN policy for the HQ gateway.

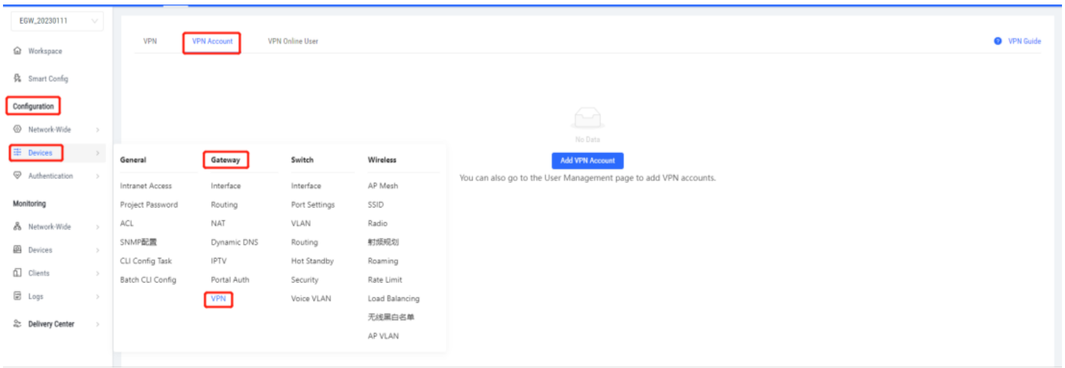
Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select **Client-to-Site**.
VPN Mode	Select the mode for implementing client-to-site VPN. Select **L2TP over IPsec**.
Server IP/Domain	Specify the IP address or domain name of the L2TP server.
Pre-Shared Key	Specify the same unique pre-shared key as the credential for mutual authentication between the server and client.

Parameter	Description
Local Tunnel IP	
IP Pool	Specify the address pool used by the server to allocate IP addresses to clients.
DNS	
Tunnel Authentication	
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP over IPsec VPN is deployed.

(2) Set a VPN account.

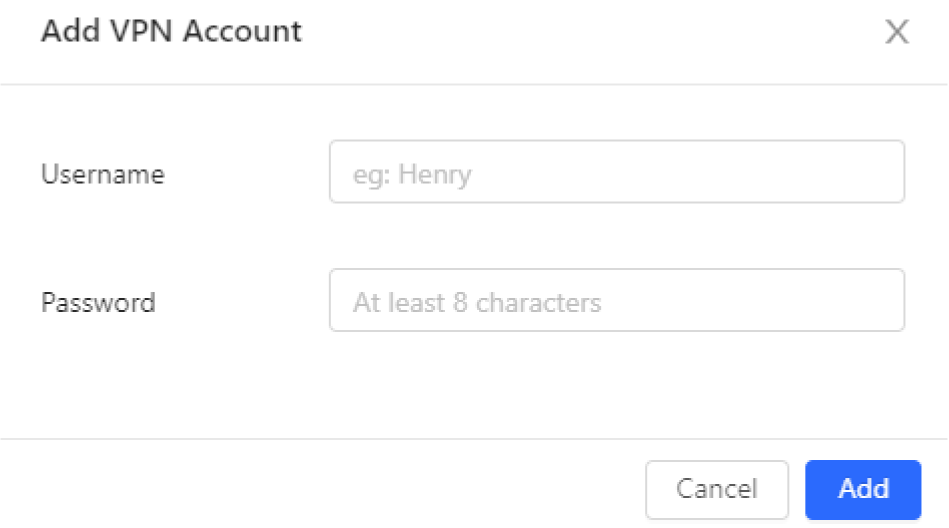
Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

a Choose **Configuration** > **Devices** > **Gateway** > **VPN** > **VPN Account**.



You can also go to the User Management page to add VPN accounts.

b Click **Add VPN Account**.



c Configure items related to a VPN account.

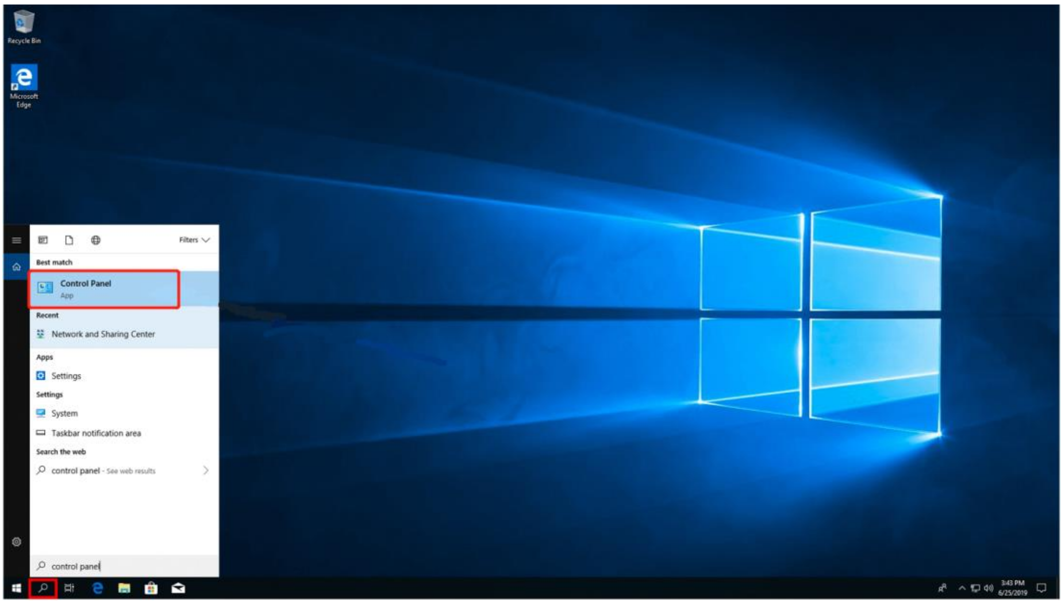
Table 8-5 **VPN Account Configuration Items**

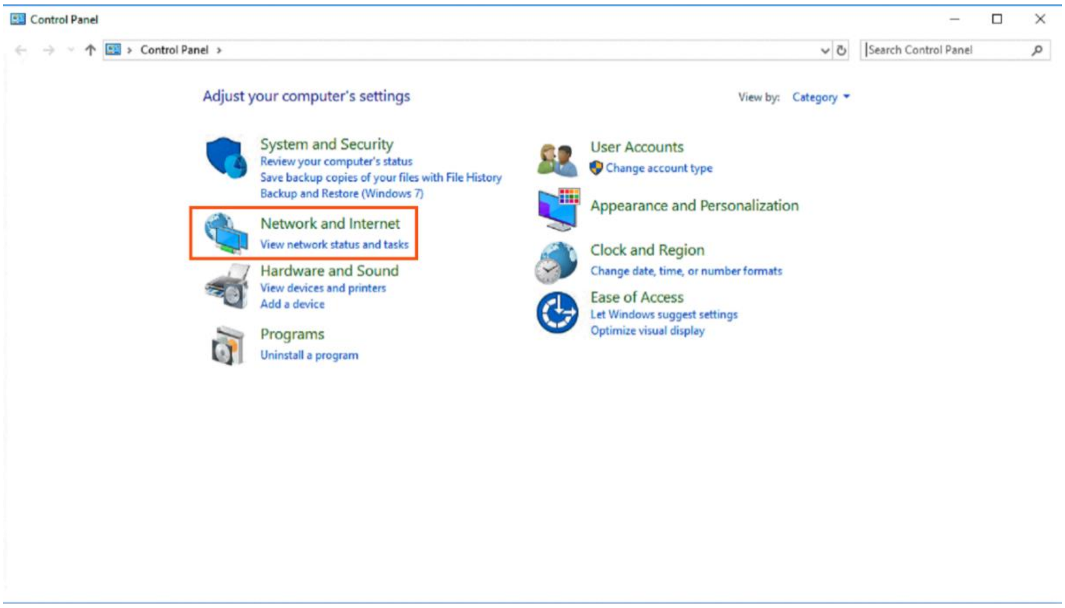
Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

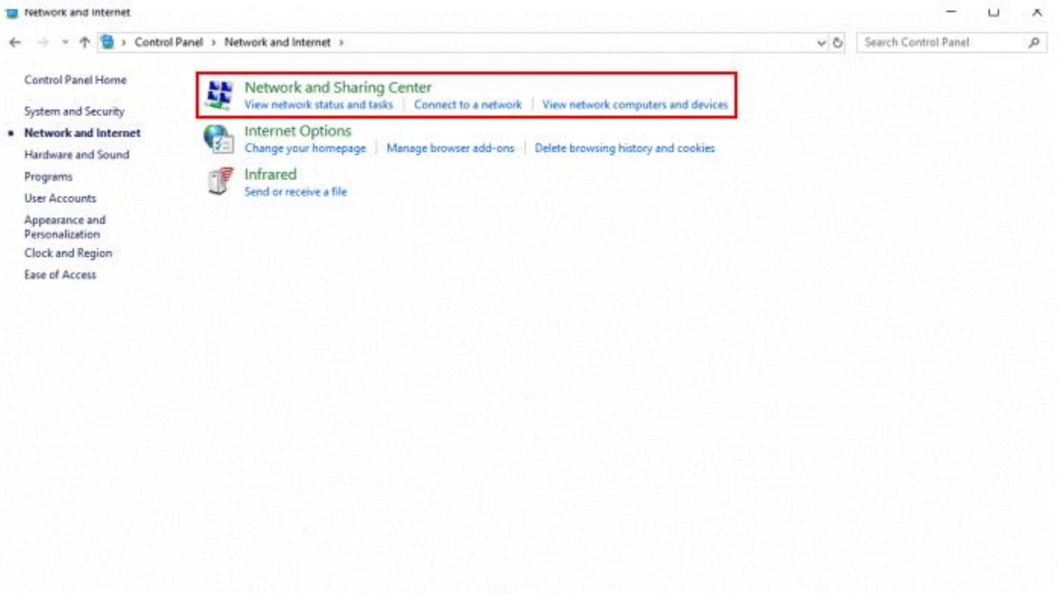
d Click **Add**.

(3) Configure the client.

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




Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display



Network and Internet

Control Panel › Network and Internet ›

Search Control Panel

Control Panel Home

System and Security

- **Network and Internet**

Hardware and Sound

Programs

User Accounts

Appearance and Personalization

Clock and Region

Ease of Access

Network and Sharing Center

View network status and tasks | Connect to a network | View network computers and devices

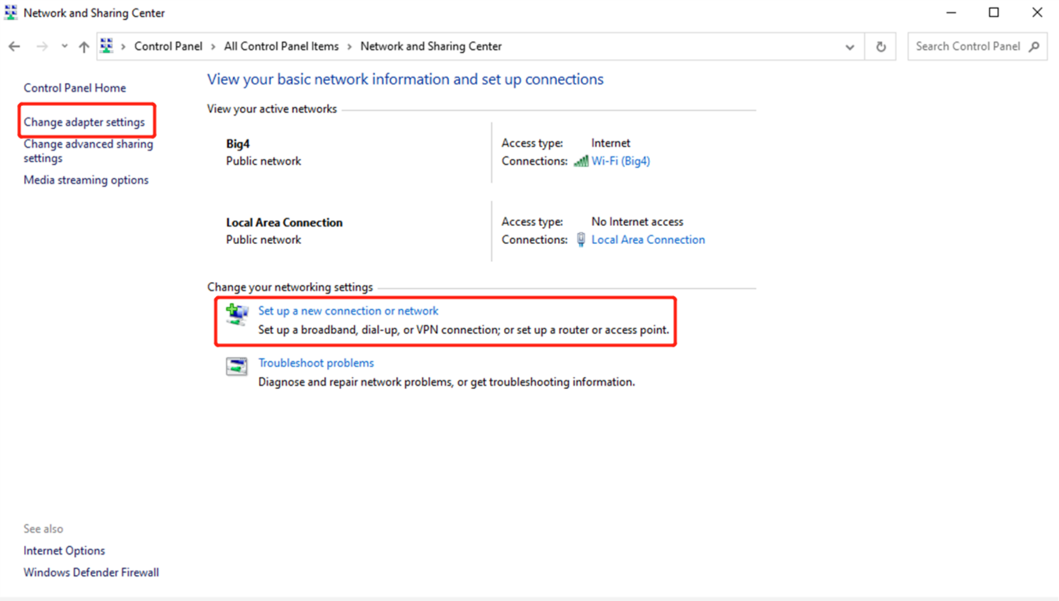
Internet Options

Change your homepage | Manage browser add-ons | Delete browsing history and cookies

Infrared

Send or receive a file

b Configure a VPN connection.



Network and Sharing Center

Control Panel › All Control Panel Items › Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

Media streaming options

View your basic network information and set up connections

View your active networks

Big4
Public network

Access type: Internet
Connections: Wi-Fi (Big4)

Local Area Connection
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network

Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

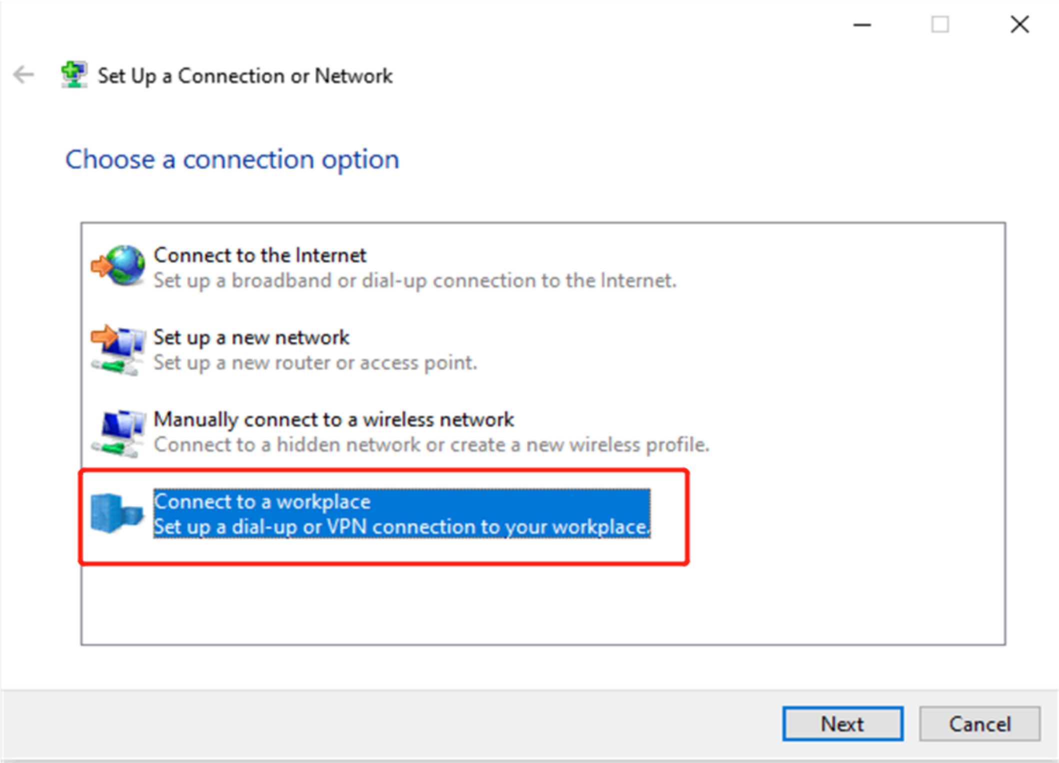
Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

See also

Internet Options

Windows Defender Firewall



Set Up a Connection or Network

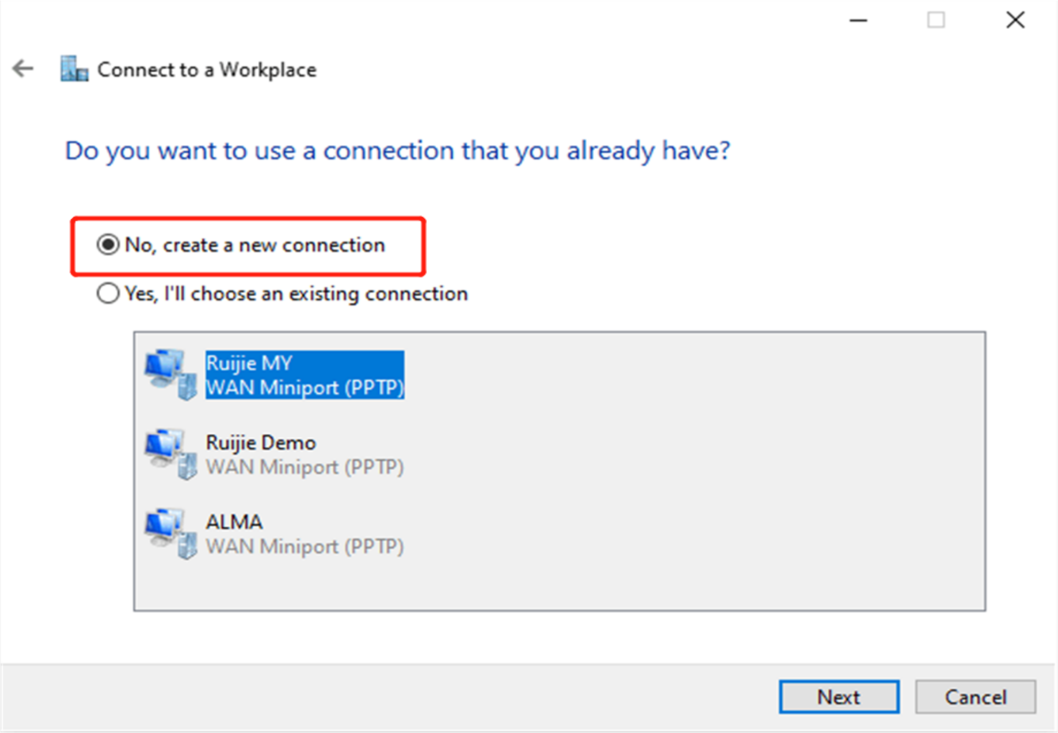
Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.



Connect to a Workplace

Do you want to use a connection that you already have?

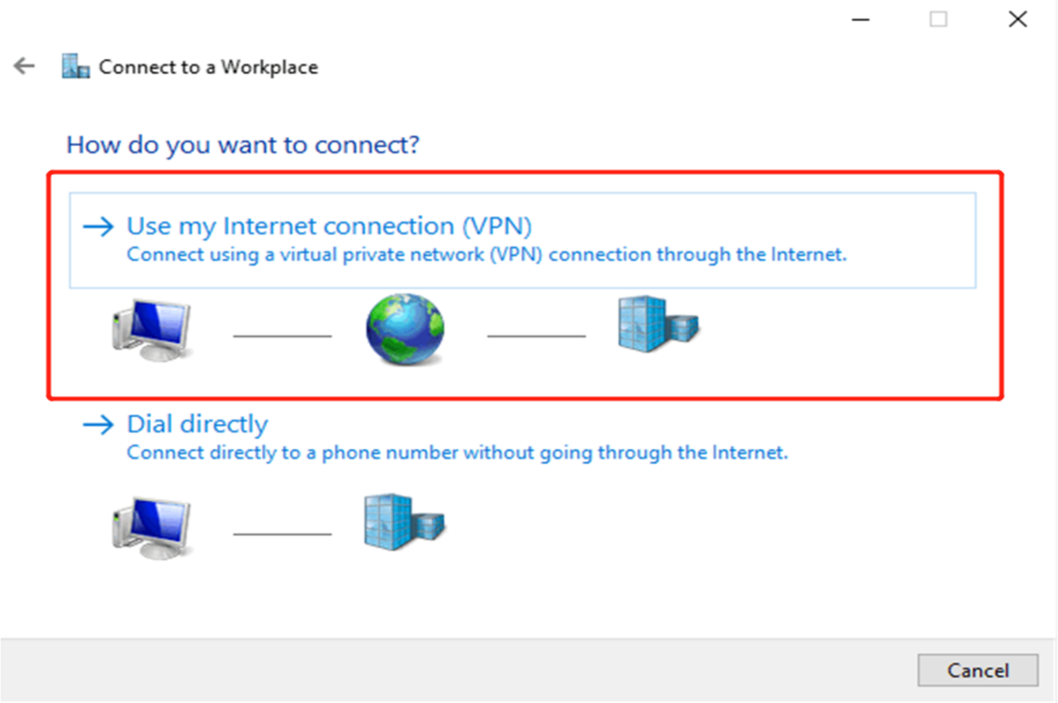
● No, create a new connection

○ Yes, I'll choose an existing connection

Ruijie MY
WAN Miniport (PPTP)

Ruijie Demo
WAN Miniport (PPTP)

ALMA
WAN Miniport (PPTP)

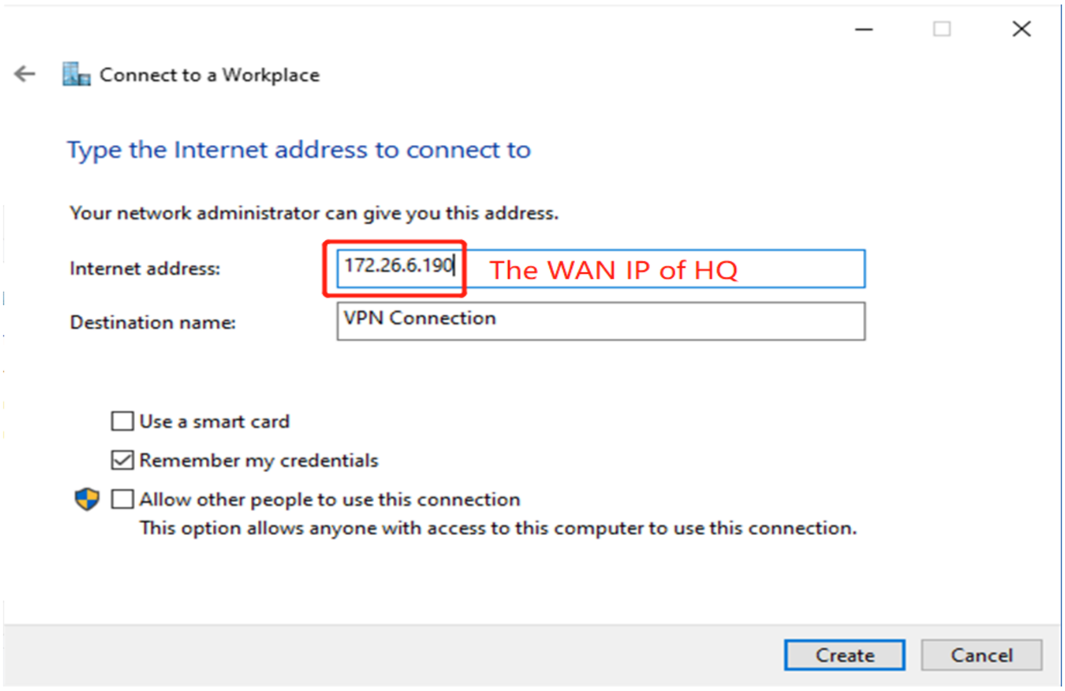


Connect to a Workplace

How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.



Connect to a Workplace

Type the Internet address to connect to

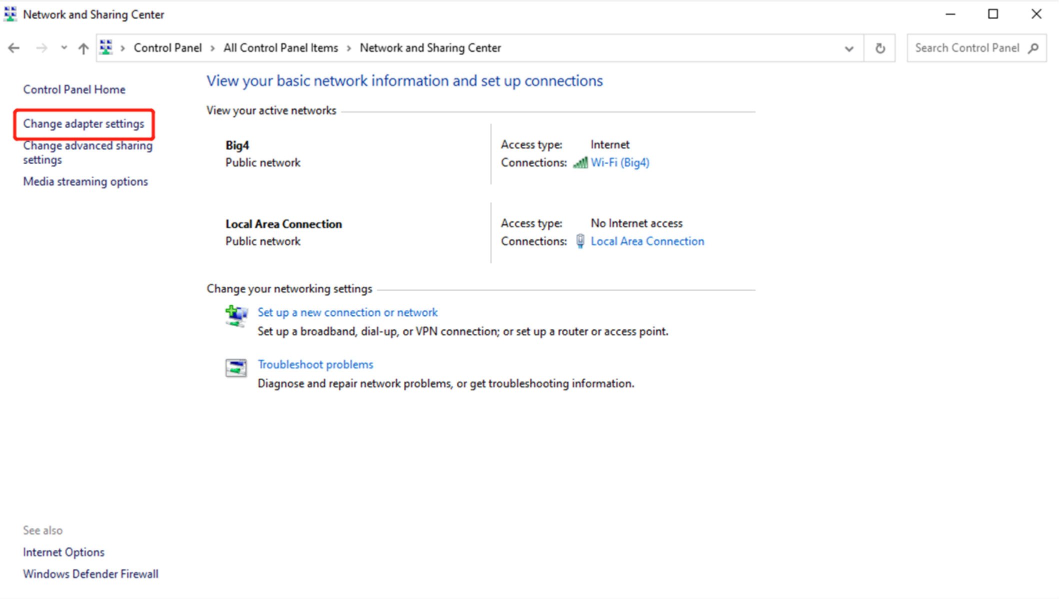
Your network administrator can give you this address.

Internet address: 172.26.6.190 The WAN IP of HQ

Destination name: VPN Connection

□ Use a smart card
☑ Remember my credentials
□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

c Change adapter's settings.


Network and Sharing Center
Control Panel > All Control Panel Items > Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
See also
Internet Options
Windows Defender Firewall

View your basic network information and set up connections

View your active networks

Big4
Public network

Access type: Internet
Connections: Wi-Fi (Big4)

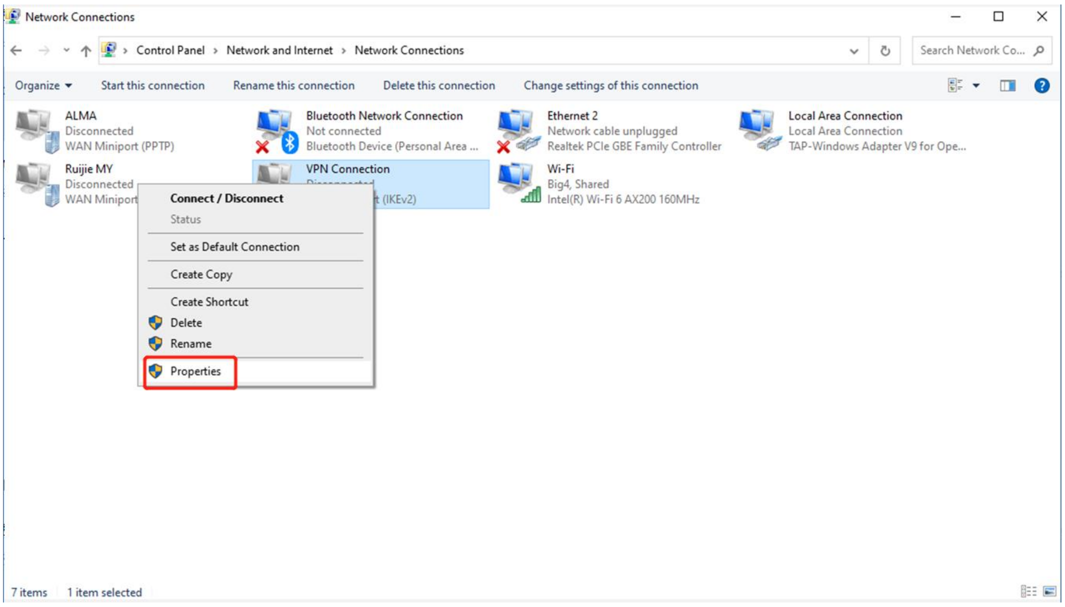
Local Area Connection
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.



ALMA
Disconnected
WAN Miniport (PPTP)

Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

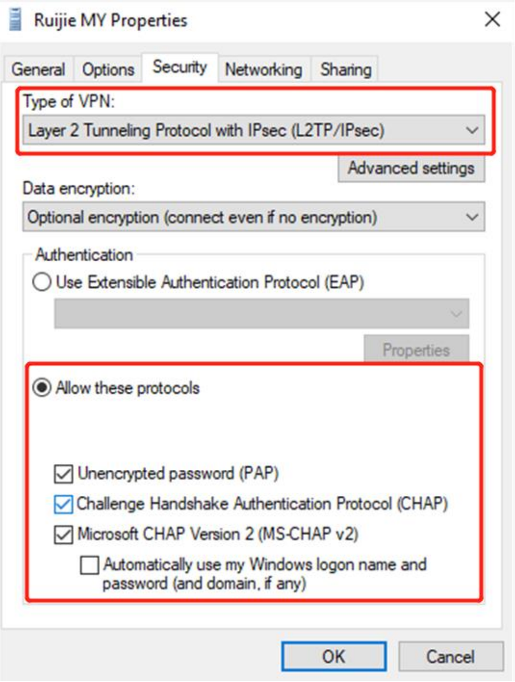
Ethernet 2
Network cable unplugged
Realtek PCIe GBE Family Controller

Local Area Connection
Local Area Connection
TAP-Windows Adapter V9 for Ope...

Ruijie MY
Disconnected
WAN Miniport

VPN Connection
Disconnected
(IKEv2)

Wi-Fi
Big4, Shared
Intel(R) Wi-Fi 6 AX200 160MHz



Ruijie MY Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

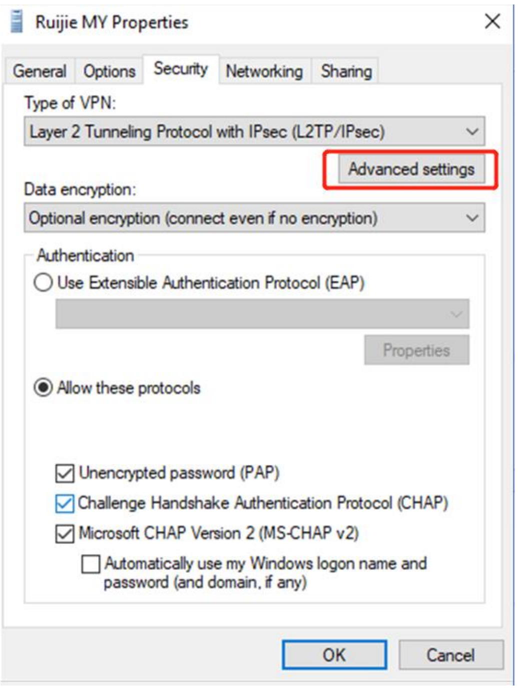
☑ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

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



Ruijie MY Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

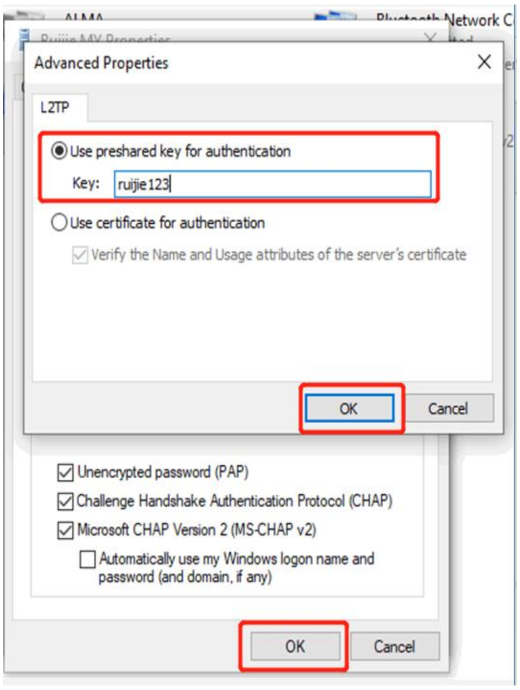
● Allow these protocols

☑ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)



Advanced Properties

L2TP

● Use preshared key for authentication

Key: ruijie123

○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate

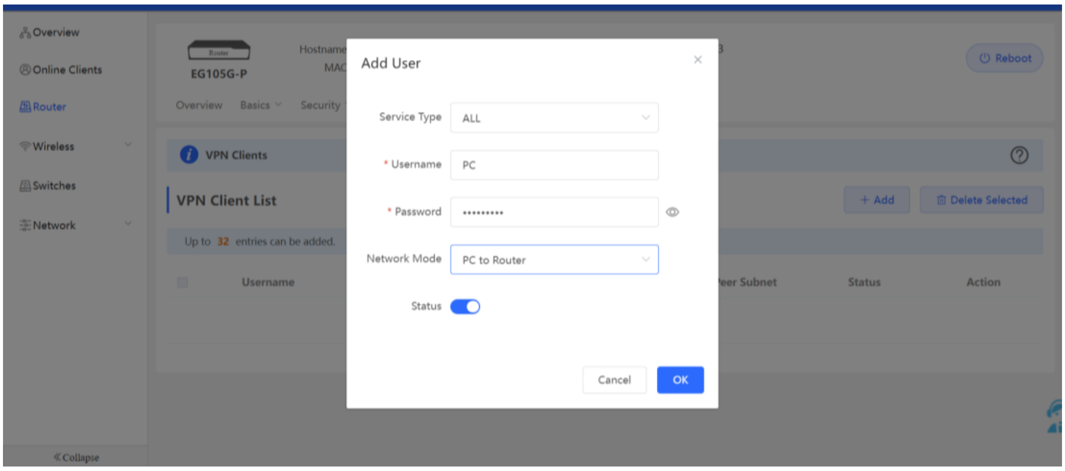
☑ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

e Set **Network Mode** to **PC to Router**.



Add User

Service Type ALL

* Username PC

* Password •••••••••

Network Mode PC to Router

Status ●

VPN Client List

Up to 32 entries can be added.

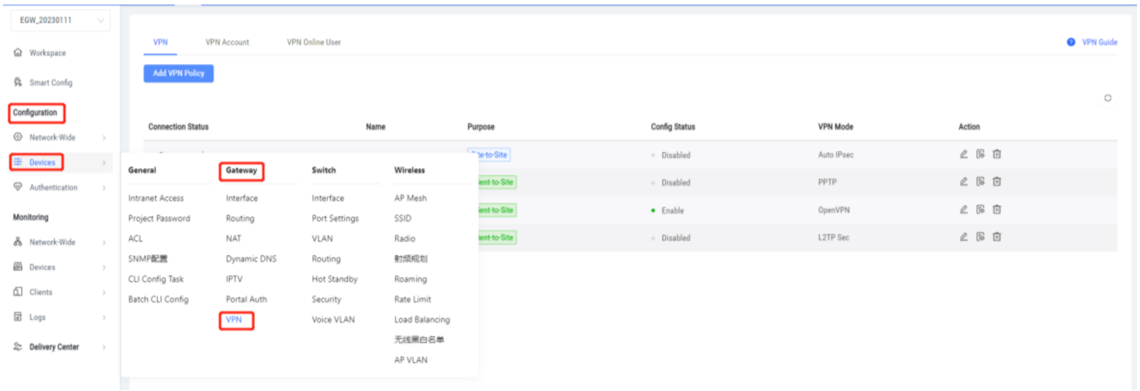
6. Configuring Client-to-Site VPN (Based on Open VPN)

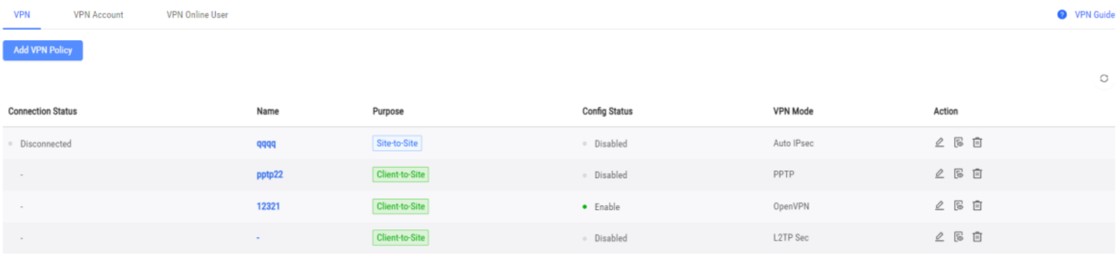
Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

(1) Configure VPN for the HQ gateway.

a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.

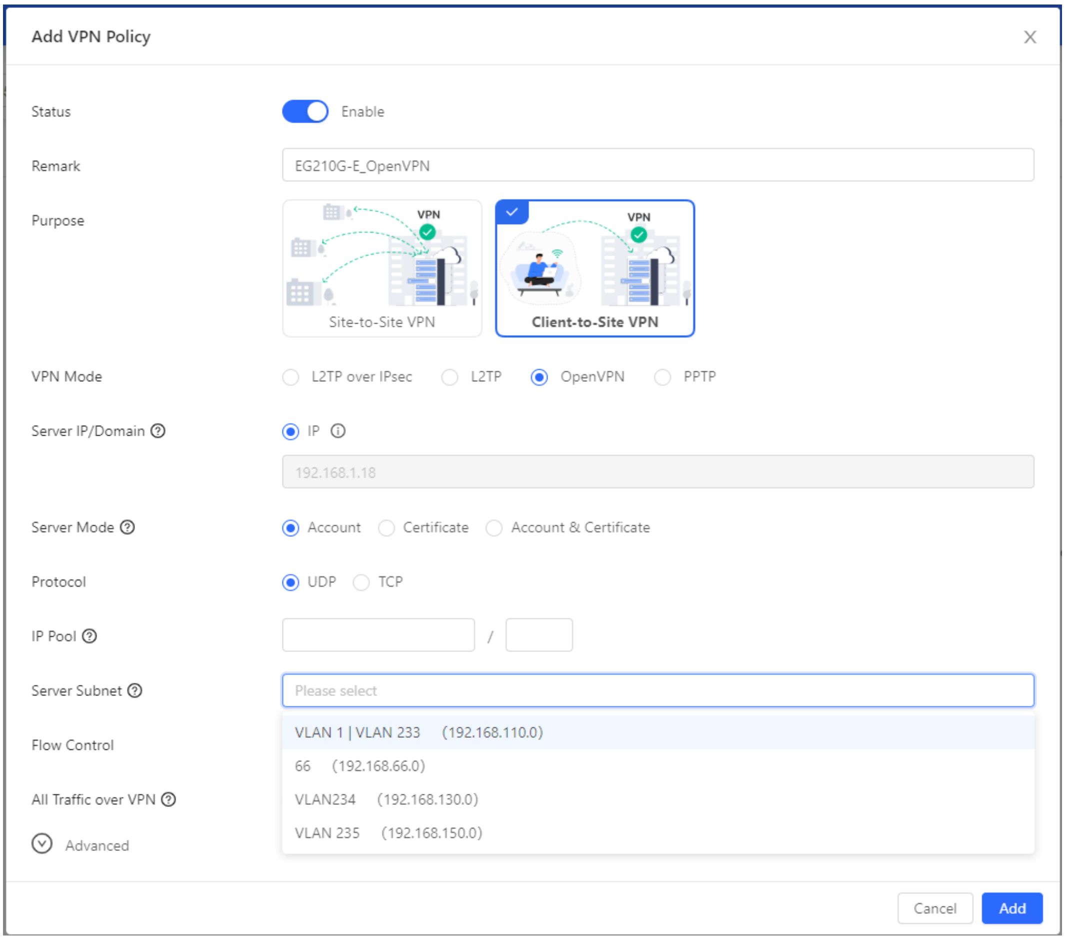
b Choose **Configuration** > **Devices** > **Gateway** > **VPN** > **VPN**.





Connection Status	Name	Purpose	Config Status	VPN Mode	Action
Disconnected	qqqq	Site-to-Site	Disabled	Auto IPsec	
-	pptp22	Client-to-Site	Disabled	PPTP	
-	12321	Client-to-Site	● Enable	OpenVPN	
-	-	Client-to-Site	Disabled	L2TP Sec	

c Click **Add VPN Policy**.



Status: Enable

Remark: EG210G-E_OpenVPN

Purpose: ☑ Client-to-Site VPN

VPN Mode: ○ L2TP over IPsec ○ L2TP ● OpenVPN ○ PPTP

Server IP/Domain: ● IP

192.168.1.18

Server Mode: ● Account ○ Certificate ○ Account & Certificate

Protocol: ● UDP ○ TCP

IP Pool: /

Server Subnet: Please select

VLAN 1 | VLAN 233 (192.168.110.0)
66 (192.168.66.0)
VLAN234 (192.168.130.0)
VLAN 235 (192.168.150.0)

Flow Control

All Traffic over VPN

Advanced

d Configure the VPN policy for the HQ gateway.

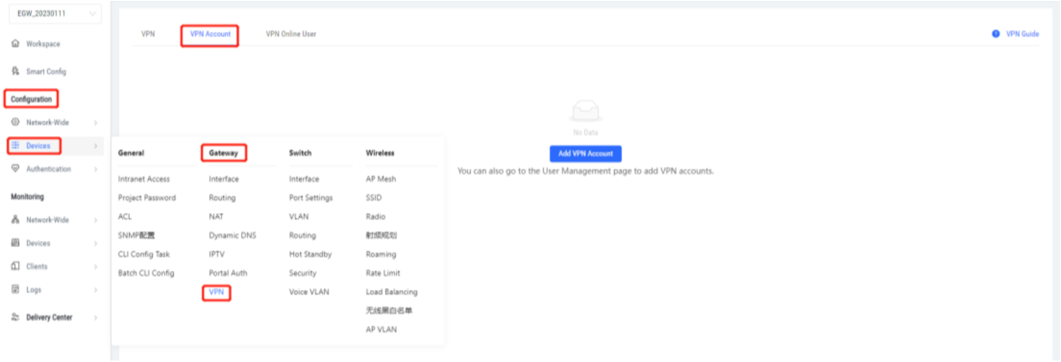
Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select **Client-to-Site**.
VPN Mode	Select the mode for implementing client-to-site VPN. Select **Open VPN**.
Server IP/Domain	Specify the IP address or domain name of the L2TP server.
Server Mode	Select a server authentication mode. The options are **Account** and **Certificate**, ● Account: Enter the correct username and password and upload the CA certificate on the client to connect to the server. The configuration is simple. ● Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client to connect to the server.
Protocol	Select a protocol for all OpenVPN communications based on a single IP port. The options are **UDP** and **TCP**. The default value is **UDP**, which is recommended. When you select a protocol, pay attention to the network status between two encrypted tunnel ends. If high latency or heavy packet loss occurs, select **TCP** as the underlying protocol.
IP Pool	Specify the address pool used by the server to allocate IP addresses to clients.
Server Subnet	
All Traffic over VPN	Specify whether to route all traffic over VPN. After this function is enabled, all the traffic is routed over the VPN tunnel. This means that the VPN tunnel is the default route.
Port ID	
TLS Authentication	
Data Compression	Specify whether to enable data compression. If this function is enabled, transmitted data is compressed using the LZO algorithm. Data compression saves bandwidth but consumes certain CPU resources. The setting on the client must be the same as that on the server. Otherwise, the connection fails.

Parameter	Description
Cipher	Select the data encryption mode before data transmission to ensure that even data packets are intercepted during transmission, the leaked data cannot be interpreted. If this parameter is set to **Auto** on the server, you can set this parameter to any option on the client. If a specific encryption algorithm is configured on the server, you must select the same encryption algorithm on the client. Otherwise, the connection fails.

(2) Create an OpenVPN user.

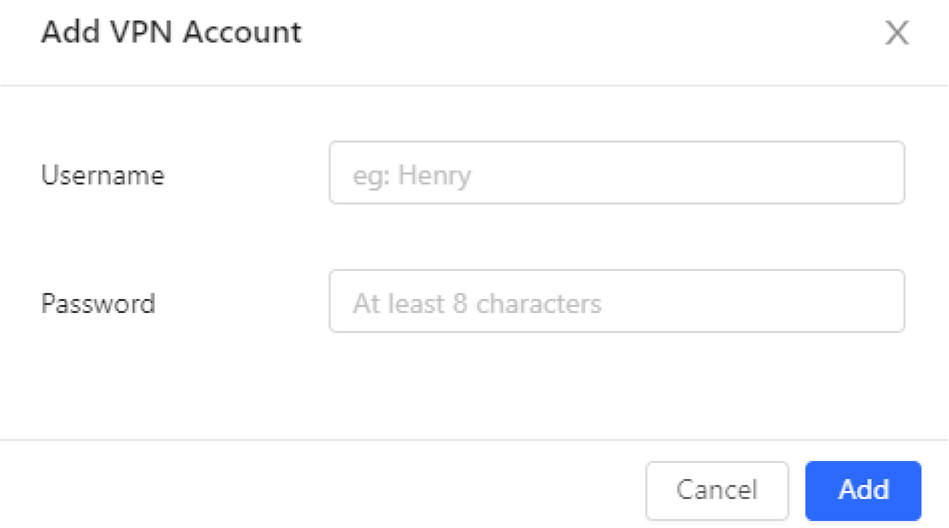
Only user accounts added to the VPN client list are allowed to dial up to connect to the OpenVPN server. Therefore, you need to manually configure user accounts for clients to access the OpenVPN server.

a Choose **Configuration** > **Devices** > **Gateway** > **VPN** > **VPN Account**.



You can also go to the User Management page to add VPN accounts.

b Click **Add VPN Account**.



c Configure items related to a VPN account.

Table 8-6 VPN Account Configuration Items

Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

d Click **Add**.

(3) Configure the client.

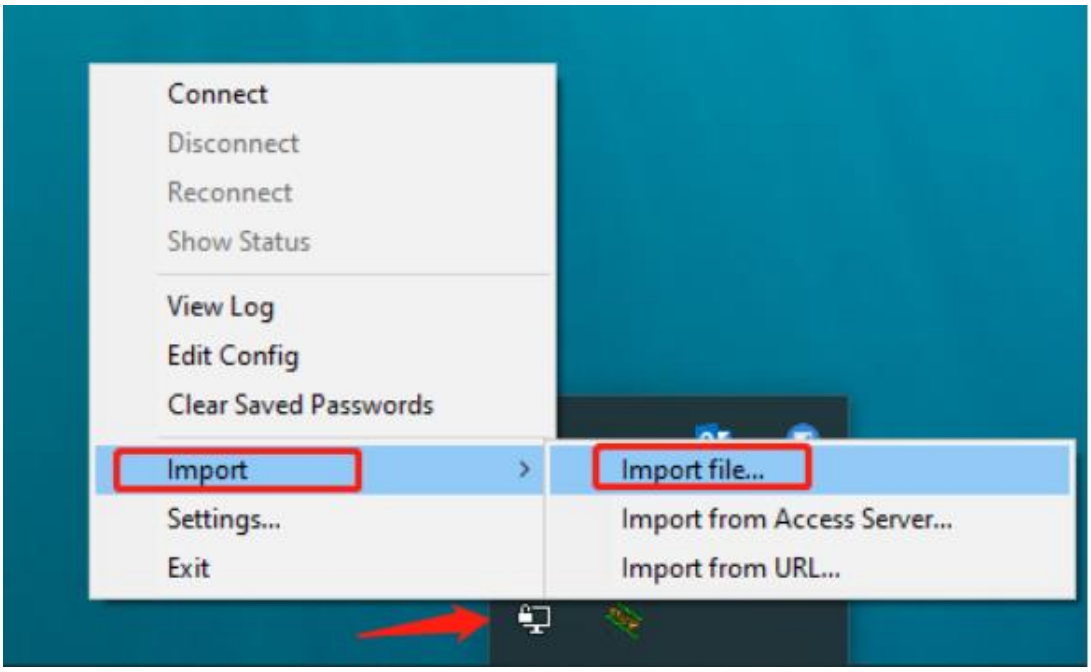
The following uses a Windows 10 client as an example for description. For the configuration of other clients, click **VPN Guide** at the upper right corner of the configuration page.

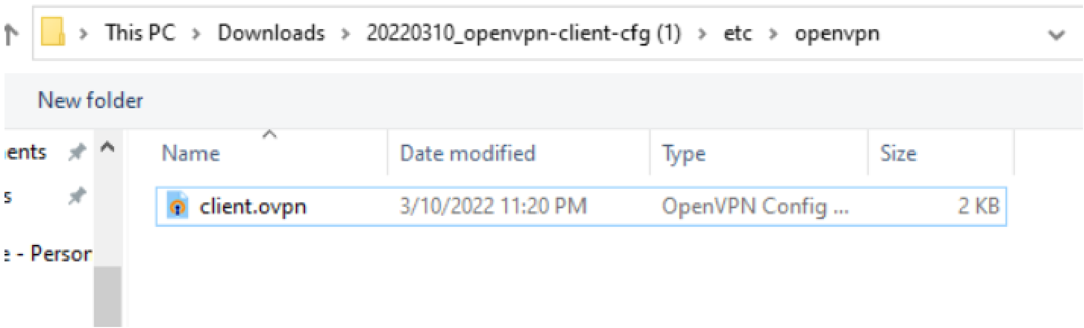
a Download and install OpenVPN application to your PC.

You can download OpenVPN client at https://openvpn.net/community-downloads/. Select a suitable version for your PC.

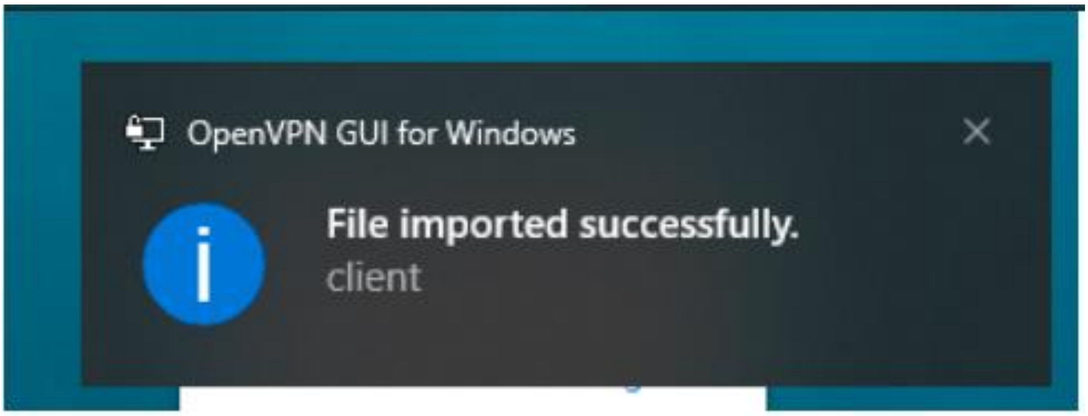
b Import client configuration to the OpenVPN client after the OpenVPN client is installed on your PC.

- Export the client configuration on the web page.
- Right-click **OpenVPN** and choose **Import** > **Import file...** to import the client configuration on the client.




This PC > Downloads > 20220310_openvpn-client-cfg (1) > etc > openvpn
New folder
ents
s
: - Persor

Name	Date modified	Type	Size
client.ovpn	3/10/2022 11:20 PM	OpenVPN Config ...	2 KB



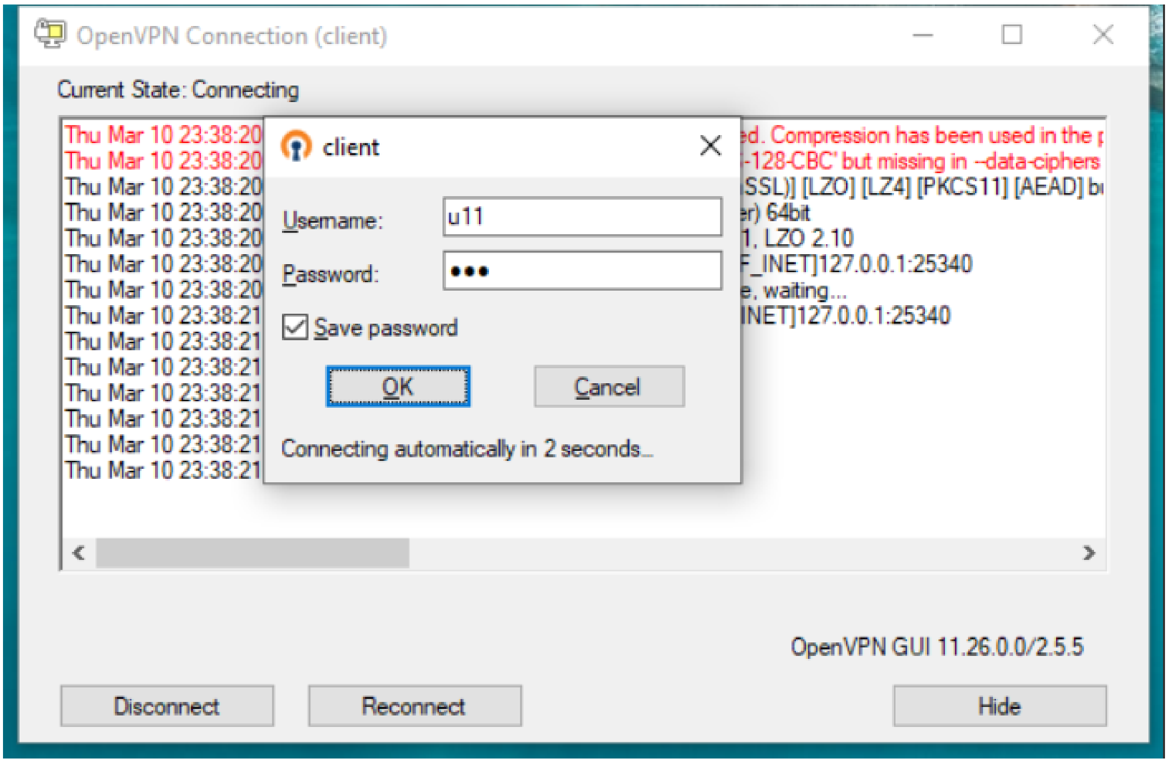
OpenVPN GUI for Windows

File imported successfully.

client

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

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



OpenVPN Connection (client)

Current State: Connecting

```
Thu Mar 10 23:38:20 ...ed. Compression has been used in the p
Thu Mar 10 23:38:20 ...-128-CBC' but missing in --data-ciphers
Thu Mar 10 23:38:20 ...SSL)] [LZO] [LZ4] [PKCS11] [AEAD] bu
Thu Mar 10 23:38:20 ...er) 64bit
Thu Mar 10 23:38:20 ...1, LZO 2.10
Thu Mar 10 23:38:20 ...F_INET]127.0.0.1:25340
Thu Mar 10 23:38:20 ...e, waiting...
Thu Mar 10 23:38:21 ...INET]127.0.0.1:25340
Thu Mar 10 23:38:21
Thu Mar 10 23:38:21
Thu Mar 10 23:38:21
Thu Mar 10 23:38:21
Thu Mar 10 23:38:21
Thu Mar 10 23:38:21
```

client

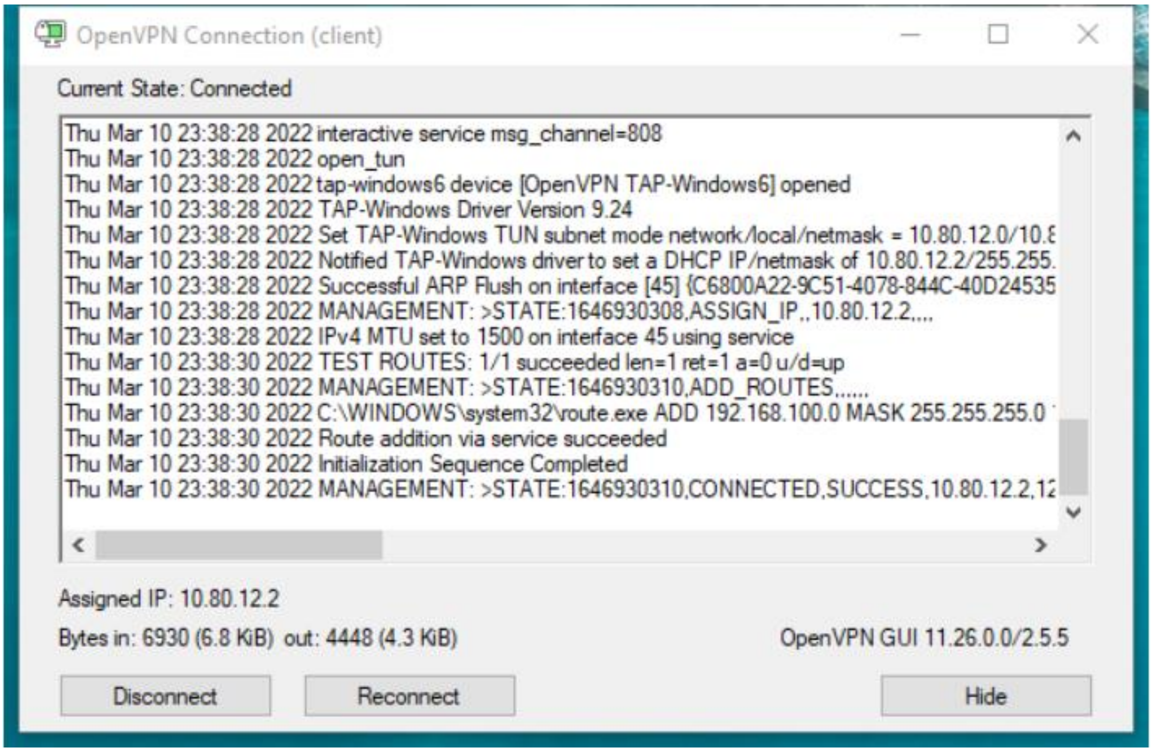
Username: u11

Password: •••

☑ Save password

Connecting automatically in 2 seconds...

OpenVPN GUI 11.26.0.0/2.5.5



Current State: Connected

```
Thu Mar 10 23:38:28 2022 interactive service msg_channel=808
Thu Mar 10 23:38:28 2022 open_tun
Thu Mar 10 23:38:28 2022 tap-windows6 device [OpenVPN TAP-Windows6] opened
Thu Mar 10 23:38:28 2022 TAP-Windows Driver Version 9.24
Thu Mar 10 23:38:28 2022 Set TAP-Windows TUN subnet mode network/local/netmask = 10.80.12.0/10.8
Thu Mar 10 23:38:28 2022 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.80.12.2/255.255.
Thu Mar 10 23:38:28 2022 Successful ARP Flush on interface [45] {C6800A22-9C51-4078-844C-40D24535
Thu Mar 10 23:38:28 2022 MANAGEMENT: >STATE:1646930308,ASSIGN_IP,,10.80.12.2,,,,
Thu Mar 10 23:38:28 2022 IPv4 MTU set to 1500 on interface 45 using service
Thu Mar 10 23:38:30 2022 TEST ROUTES: 1/1 succeeded len=1 ret=1 a=0 u/d=up
Thu Mar 10 23:38:30 2022 MANAGEMENT: >STATE:1646930310,ADD_ROUTES,,,,,,
Thu Mar 10 23:38:30 2022 C:\WINDOWS\system32\route.exe ADD 192.168.100.0 MASK 255.255.255.0
Thu Mar 10 23:38:30 2022 Route addition via service succeeded
Thu Mar 10 23:38:30 2022 Initialization Sequence Completed
Thu Mar 10 23:38:30 2022 MANAGEMENT: >STATE:1646930310,CONNECTED,SUCCESS,10.80.12.2,12
```

Assigned IP: 10.80.12.2

Bytes in: 6930 (6.8 KiB) out: 4448 (4.3 KiB) OpenVPN GUI 11.26.0.0/2.5.5

8.5 Configuring Dynamic DNS

1. Overview

After the dynamic domain name server (DDNS) service is enabled, external users can use a fixed domain name to access service resources on the device over the Internet at any time, without the need to search for the WAN port IP address. The device supports three DDNS protocols: No-IP DNS, and DynDNS.

2. Getting Started

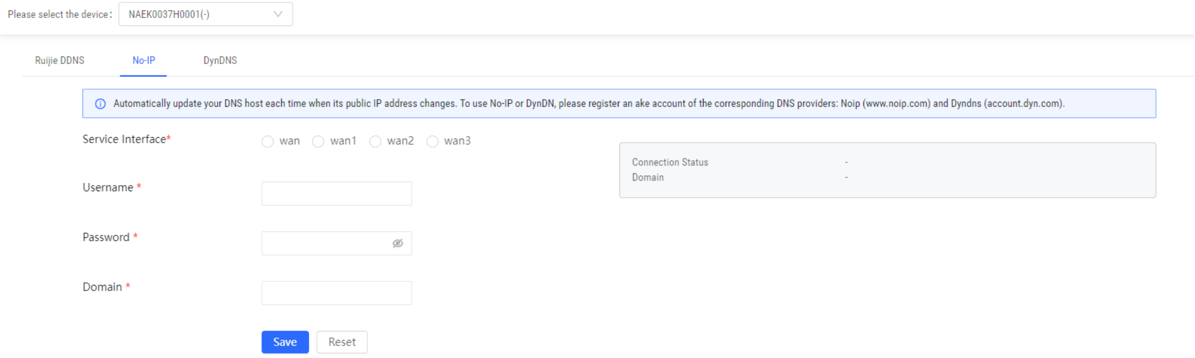
Before you use the DDNS service, you need to register an account and a domain name on the third-party DDNS service provider for this service.

3. Configuration Steps

- Configuring the No-IP

Select the DDNS server with the domain name of www.noip.com.

Choose **Configuration** > **Devices** > **Gateway > Dynamic DNS** > **No-IP**.



Please select the device: NAEK0037H0001(-)

Automatically update your DNS host each time when its public IP address changes. To use No-IP or DynDN, please register an ake account of the corresponding DNS providers: Noip (www.noip.com) and Dyndns (account.dyn.com).

Service Interface* ○ wan ○ wan1 ○ wan2 ○ wan3

Username *

Password *

Domain *

Connection Status -
Domain -

(1) Set configuration items on the **No-IP** tab.

Table 8-7 DDNS login information

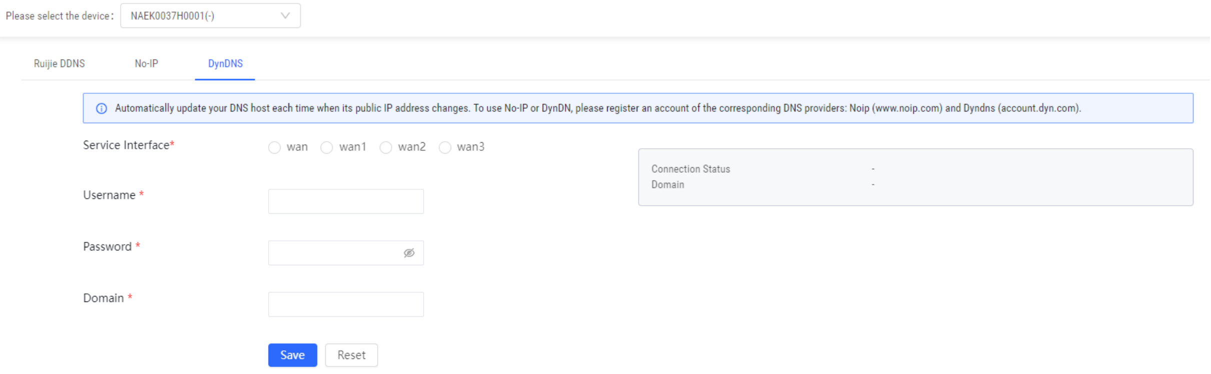
Parameter	Description
Service Interface	One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN port bound to the domain name when multiple WAN ports are available. By default, the service interface is a WAN port.
Username & Password	Enter the username and password of the account registered at the official website of the DDNS service provider. Register at the official website of the DDNS service provider in advance.
Domain	Specify the domain name bound to the service interface IP address. One account can be bound to multiple domain names. You can choose to bind only one domain name to the IP address of the current service interface. Only the selected domain name is parsed to the WAN port IP address.

(2) Click **Save**.

- Configuring the DynDNS

Select the DDNS server with the domain name of www.dyndns.org.

Choose **Configuration** > **Devices** > **Gateway > Dynamic DNS** > **DynDNS**.



Please select the device： NAEK0037H0001(-)

ⓘ Automatically update your DNS host each time when its public IP address changes. To use No-IP or DynDN, please register an account of the corresponding DNS providers: Noip (www.noip.com) and Dyndns (account.dyn.com).

Service Interface* ○ wan ○ wan1 ○ wan2 ○ wan3

Username *

Password *

Domain *

Connection Status -

Domain -

(3) Set configuration items on the **DynDNS** tab.

Table 8-8 DDNS login information

Parameter	Description
Service Interface	One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN port bound to the domain name when multiple WAN ports are available. By default, the service interface is a WAN port.

Parameter	Description
Username & Password	Enter the username and password of the account registered at the official website of the DNS service provider. Register at the official website of the DDNS service provider in advance.
Domain	Specify the domain name bound to the service interface IP address. One account can be bound to multiple domain names. You can choose to bind only one domain name to the IP address of the current service interface. Only the selected domain name is parsed to the WAN port IP address.

(4) Click **Save**.

4. Verifying Configuration

If **Connection Status** is displayed as **Connected**, the server connection is established successfully. After the configuration is completed, ping the domain name from the Internet. The ping succeeds and the domain name is parsed to the WAN port IP address.

8.6 Configuring IPTV

1. Overview

Internet Protocol television (IPTV) is a new technology that uses broadband cable television network and integrates Internet, multimedia, communication, and other technologies to provide home users with a variety of interactive services including digital television. It allows users to enjoy the IPTV service at home.

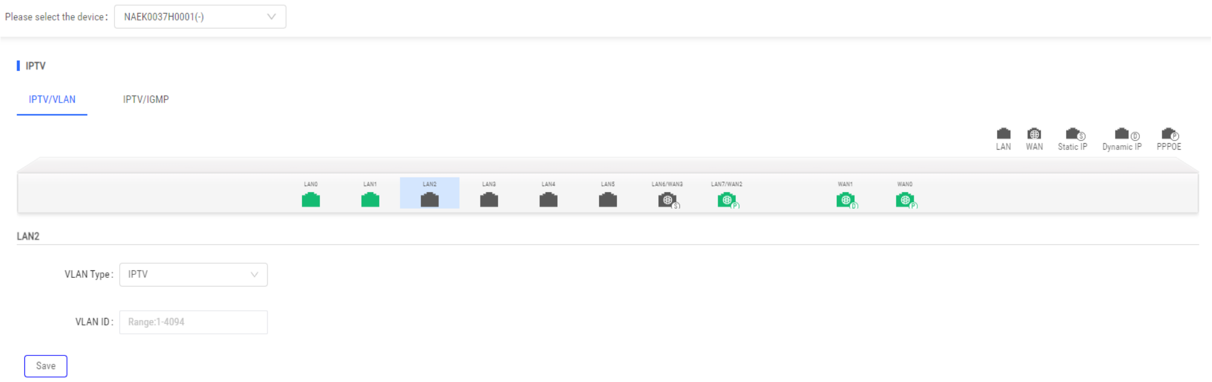
2. Getting Started

- Confirm that the IPTV service is activated.
- Check the local IPTV type: VLAN or IGMP. If the type is VLAN, confirm the VLAN ID. If you cannot confirm the type or VLAN ID, contact the local ISP.

3. Configuration Steps

- Configuring the IPTV Service of the VLAN Type

Choose **Configuration** > **Devices** > **Gateway > IPTV** > **IPTV/VLAN**.



Please select the device: NAEK0037H0001(-)

IPTV

LAN2

VLAN Type: IPTV

VLAN ID: Range:1-4094

(1) Select the port for carrying the IPTV service on the device.

(2) Set **VLAN Type** to **IPTV**.

(3) Enter the VLAN ID provided by the ISP.

(4) Click **Save**.

For example, when you want to connect the IPTV set top box to LAN 3 port of the device and the VLAN ID is 20, the configuration UI is as follows.

After the configuration is completed, confirm that the IPTV set top box is connected to the correct port, for example, LAN 3 in the example.

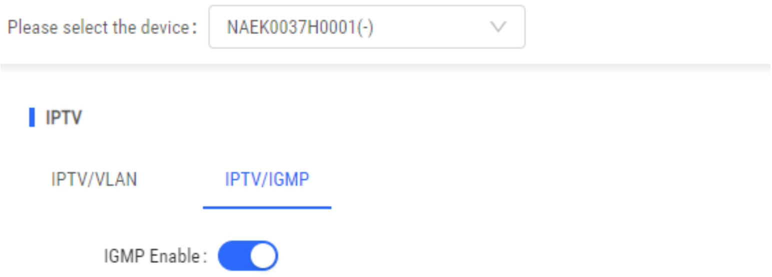
⚠ **Caution**

Enabling this function may lead to network disconnection. Exercise caution when performing this operation.

- Configuring the IPTV Service of the IGMP Type

Choose **Configuration** > **Devices** > **Gateway > IPTV** > **IPTV/IGMP**.

The IGMP type is applicable to the ISP FPT. After you enable IPTV connection, connect the IPTV set top box to any LAN port on the router.



Please select the device: NAEK0037H0001(-)

IGMP Enable: ON

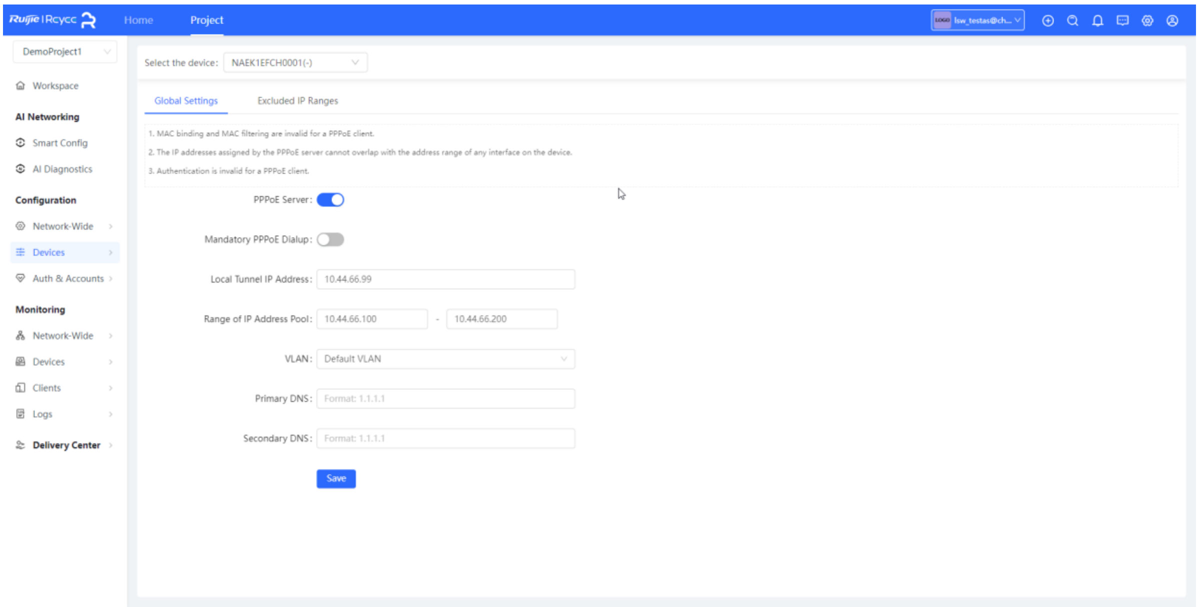
8.7 PPPoE Server

After enabling the PPPoE server, clients connected to the router's downstream need to enter their PPPoE account and password. Once authenticated, they will receive an IP address issued by the router in order to access the internet.

1. MAC binding and MAC filtering are invalid for a PPPoE client.

2. The IP addresses assigned by the PPPoE server cannot overlap with the address range of any interface on the device.

3. Authentication is invalid for a PPPoE client.



Select the device: NAEK1EFCH0001(-)

1. MAC binding and MAC filtering are invalid for a PPPoE client.
2. The IP addresses assigned by the PPPoE server cannot overlap with the address range of any interface on the device.
3. Authentication is invalid for a PPPoE client.

PPPoE Server: on

Mandatory PPPoE Dialup: off

Local Tunnel IP Address: 10.44.66.99

Range of IP Address Pool: 10.44.66.100 - 10.44.66.200

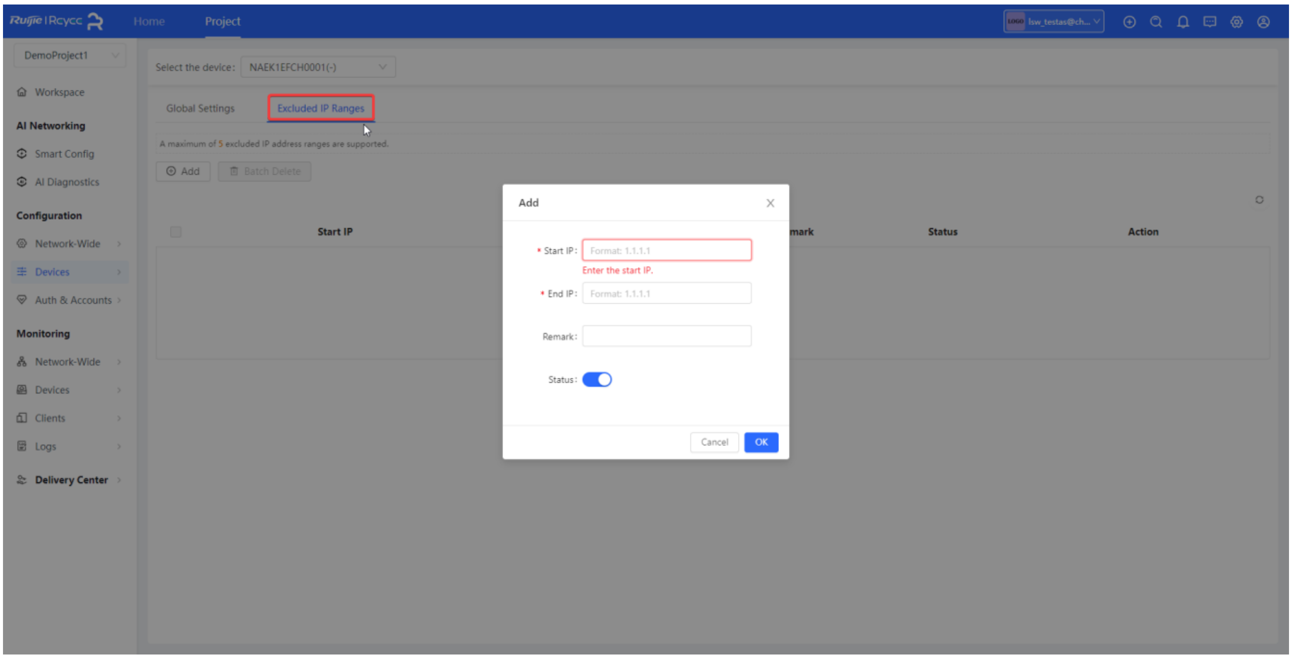
VLAN: Default VLAN

Primary DNS: Format: 1.1.1.1

Secondary DNS: Format: 1.1.1.1

Set exception IP addresses, which will be able to access the internet without having to dial through PPPoE.

A maximum of 5 excluded IP address ranges are supported.



Select the device: NAEK1EFCH0001(-)

A maximum of 5 excluded IP address ranges are supported.

* Start IP: Format: 1.1.1.1

Enter the start IP.

* End IP: Format: 1.1.1.1

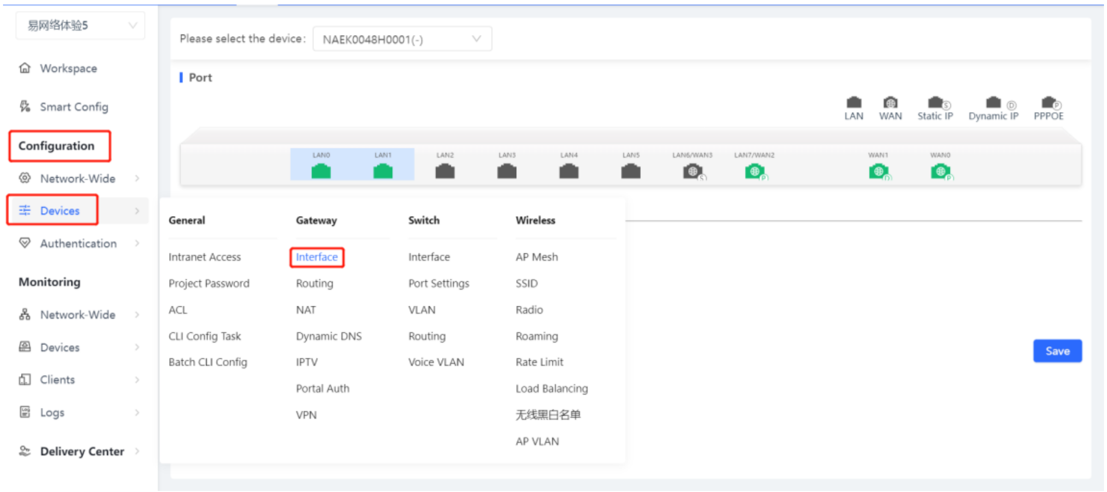
Remark:

Status: on

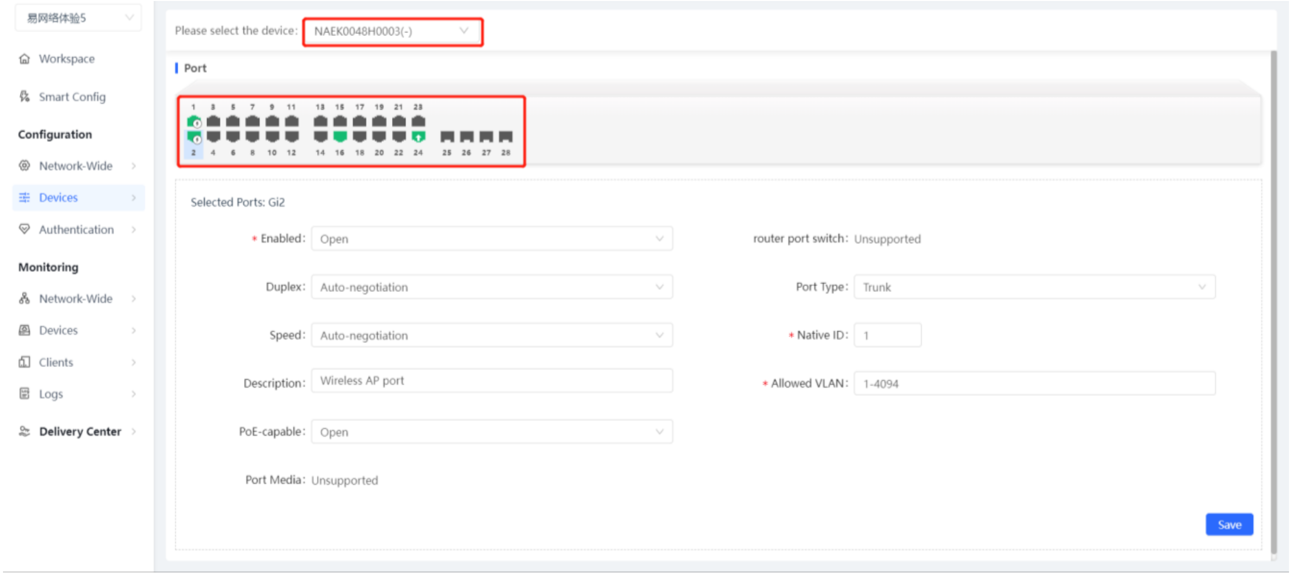
9 Switch Configuration

9.1 Interface

Choose **Configuration** > **Devices** > **Switch** > **Interface** to go to the device network port page.



Select a device, click the port to be configured, configure **Duplex**, **Speed**, **Port Type**, and **PoE-capable** for the port, and then click **Save**.



Please select the device: NAEK0048H0003(-)

Selected Ports: Gi2

* Enabled: Open

router port switch: Unsupported

Duplex: Auto-negotiation

Port Type: Trunk

Speed: Auto-negotiation

* Native ID: 1

Description: Wireless AP port

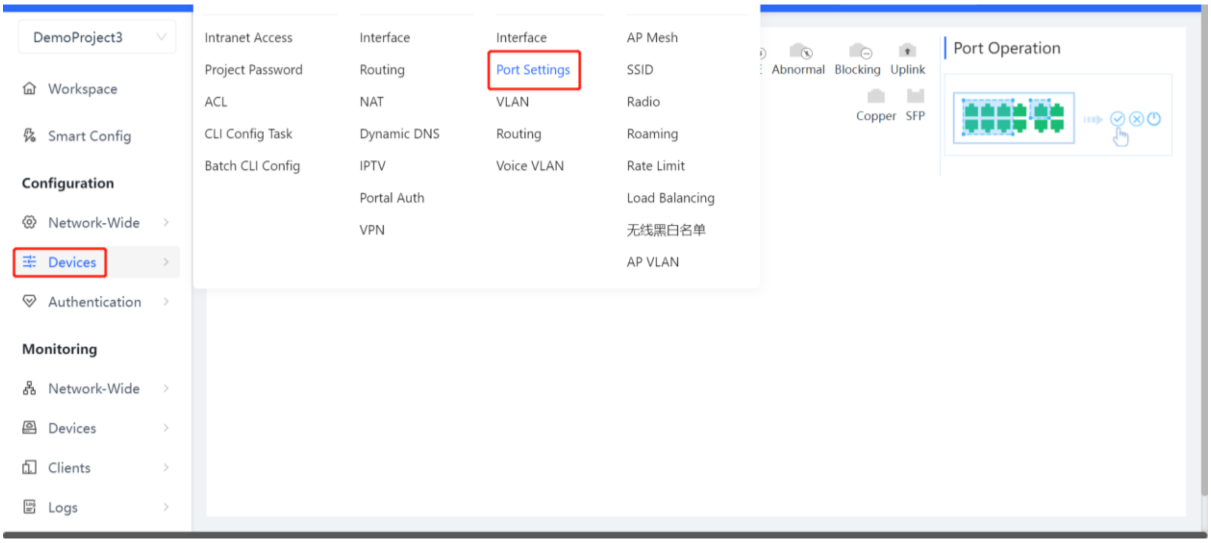
* Allowed VLAN: 1-4094

PoE-capable: Open

Port Media: Unsupported

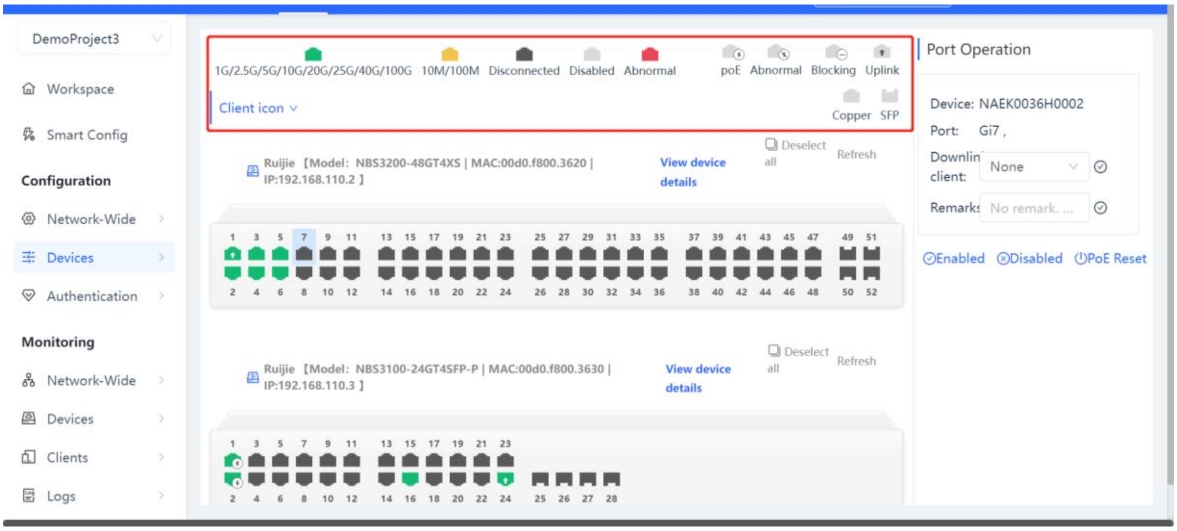
9.2 Port Settings

Choose **Configuration** > **Devices** > **Switch** > **Port Settings**.



9.2.1 Port Status Bar

Port icons in different colors and shapes at the top of the page represent different states and types of the ports. Move the cursor over a port icon. Basic information of the port will be displayed, including **Port Status**, **Port Speed**, and **Rate**.



Ruijie【Model: NBS3200-48GT4XS | MAC:00d0.f800.3620 | IP:192.168.110.2】

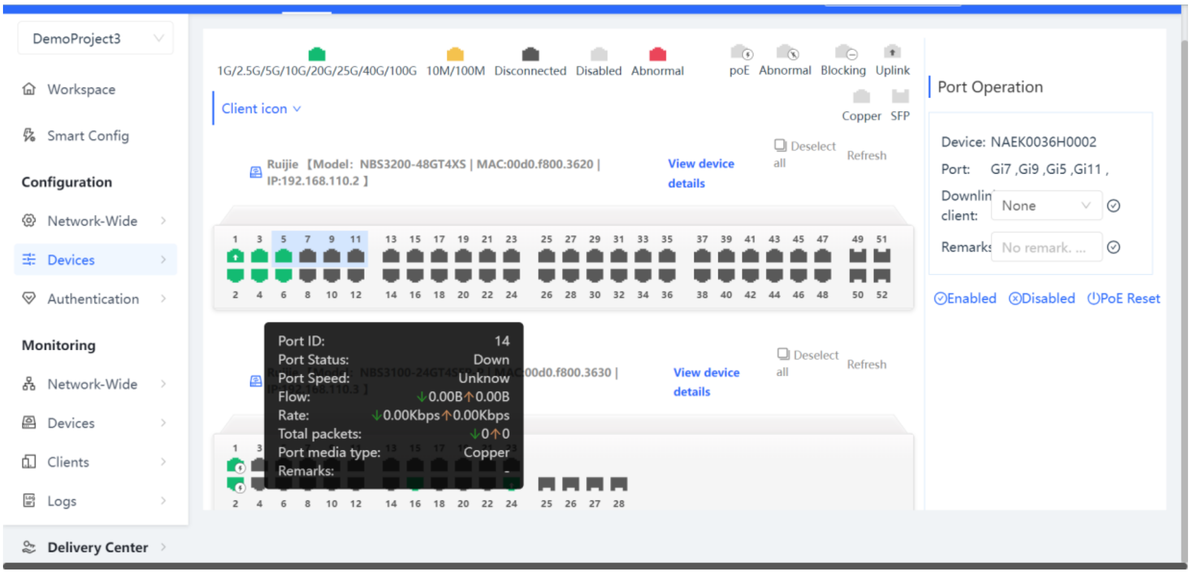
Ruijie【Model: NBS3100-24GT4SFP-P | MAC:00d0.f800.3630 | IP:192.168.110.3】

Device: NAEK0036H0002

Port: Gi7 ,

Downlink client: None

Remarks: No remark. ...



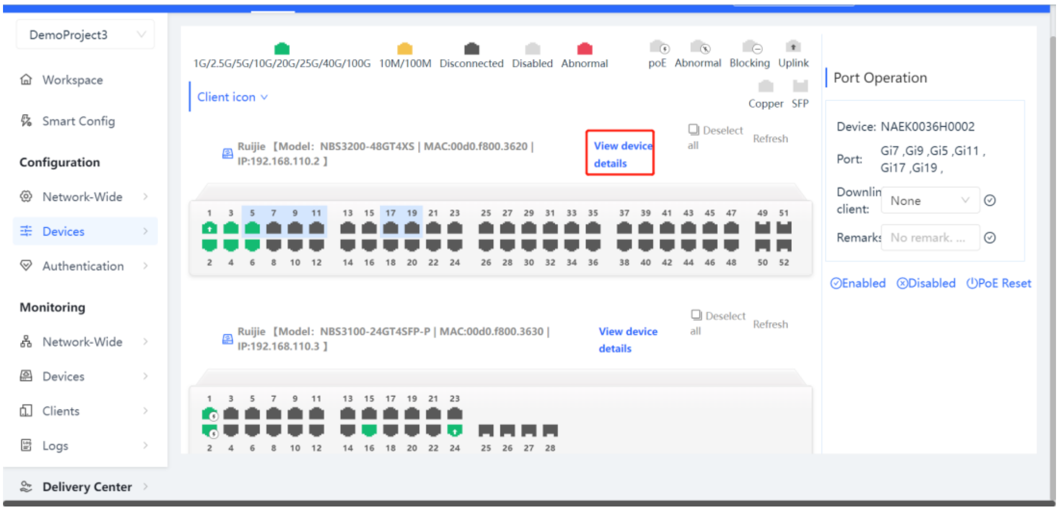
Ruijie【Model: NBS3200-48GT4XS | MAC:00d0.f800.3620 | IP:192.168.110.2 】

Port ID: 14
Port Status: Down
Port Speed: Unknow
Flow: ↓0.00B↑0.00B
Rate: ↓0.00Kbps↑0.00Kbps
Total packets: ↓0↑0
Port media type: Copper
Remarks:

Device: NAEK0036H0002
Port: Gi7 ,Gi9 ,Gi5 ,Gi11 ,
Downlink client: None
Remarks: No remark. ...

9.2.2 Device Information

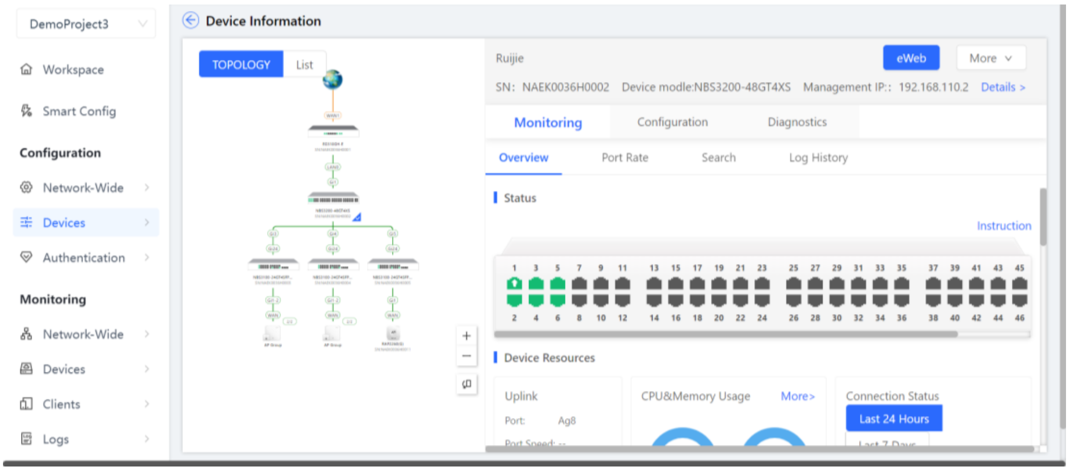
Click **View device details** to go to the **Device Information** page, which displays the device details.



Ruijie【Model: NBS3200-48GT4XS | MAC:00d0.f800.3620 | IP:192.168.110.2 】

Ruijie【Model: NBS3100-24GT4SFP-P | MAC:00d0.f800.3630 | IP:192.168.110.3 】

Device: NAEK0036H0002
Port: Gi7 ,Gi9 ,Gi5 ,Gi11 , Gi17 ,Gi19 ,
Downlink client: None
Remarks: No remark. ...



Ruijie

SN: NAEK0036H0002 Device modle:NBS3200-48GT4XS Management IP:: 192.168.110.2 Details >

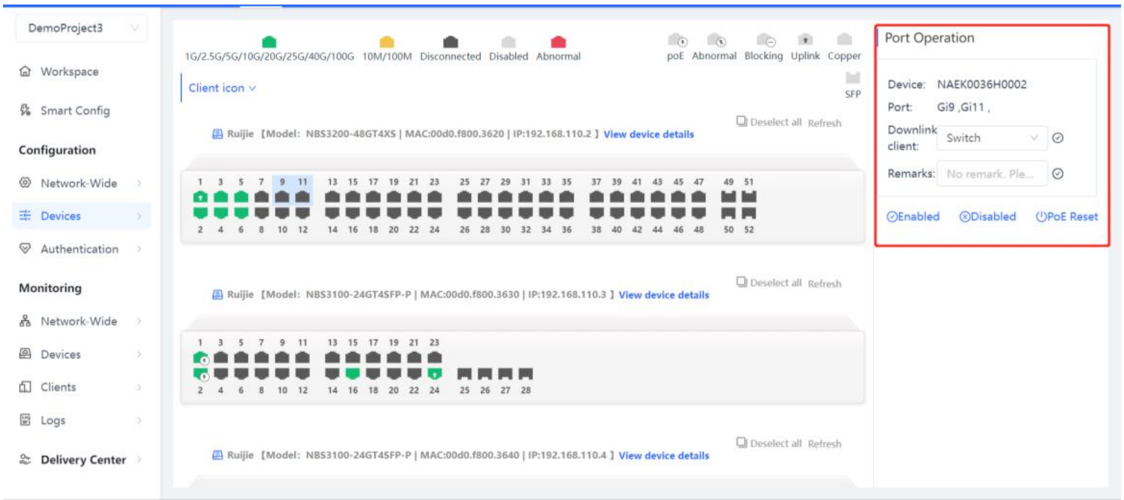
Port: Ag8

Port Speed: --

9.2.3 Port Settings

Select a device and click a port of the device to set the device port.

- To enable the device port, click **Enabled**.
- To disable the device port, click **Disabled**.
- To restart the device port, click **PoE Reset**.


DemoProject3
Workspace
Smart Config
Configuration
Network-Wide
Devices
Authentication
Monitoring
Network-Wide
Devices
Clients
Logs
Delivery Center
1G/2.5G/5G/10G/20G/25G/40G/100G
10M/100M
Disconnected
Disabled
Abnormal
poE
Abnormal
Blocking
Uplink
Copper
SFP
Client icon
Deselect all
Refresh
Ruijie 【Model: NBS3200-48GT4XS | MAC:00d0.f800.3620 | IP:192.168.110.2 】 View device details
Ruijie 【Model: NBS3100-24GT4SFP-P | MAC:00d0.f800.3630 | IP:192.168.110.3 】 View device details
Ruijie 【Model: NBS3100-24GT4SFP-P | MAC:00d0.f800.3640 | IP:192.168.110.4 】 View device details
Port Operation
Enabled
Disabled
PoE Reset

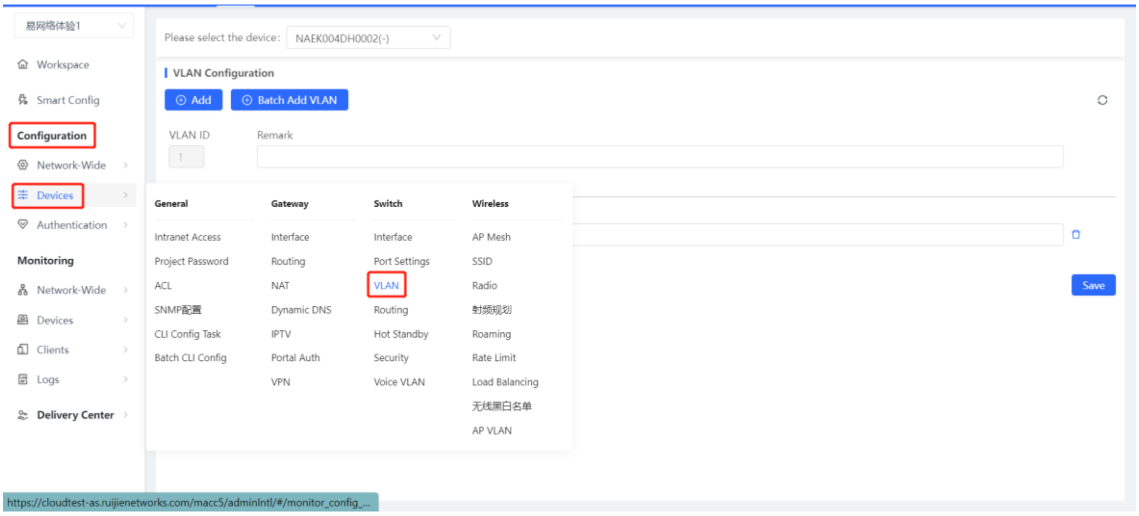
Device: NAEK0036H0002
Port: Gi9 ,Gi11 ,
Downlink client: Switch
Remarks: No remark. Ple...

9.3 Configuring a VLAN for an Interface

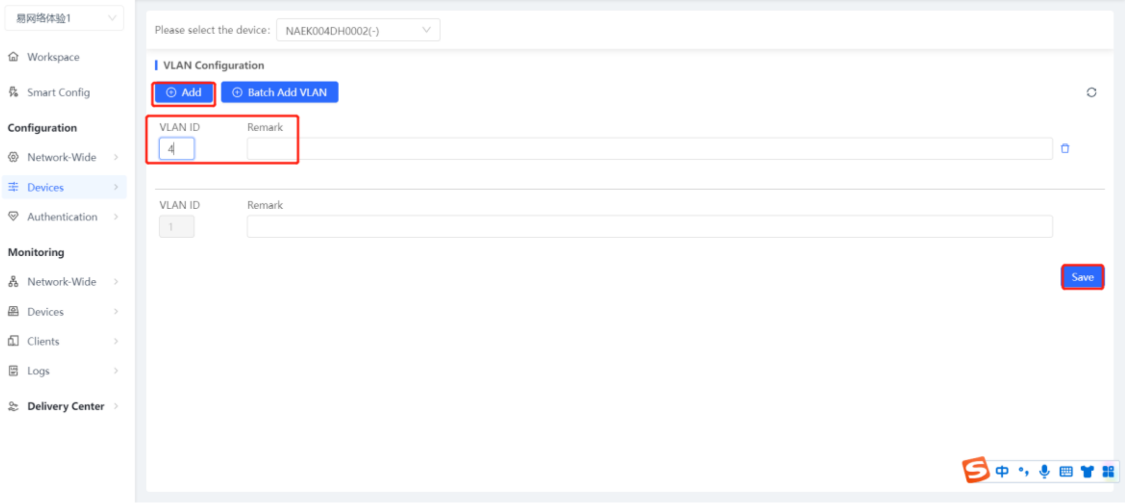
(1) Creating a VLAN

Choose **Configuration** > **Devices** > **Switch** > **VLAN**.

Click **Add**, set **VLAN ID**, and click **Save** to add a VLAN.



Please select the device: NAEK004DH0002(-)
VLAN ID: 1
Remark:



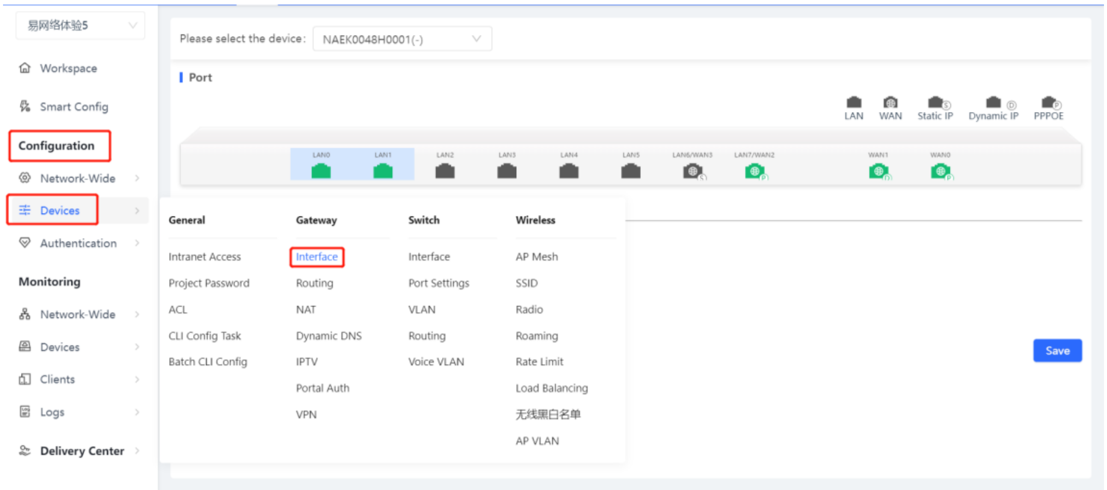
Please select the device: NAEK004DH0002(-)

VLAN Configuration

VLAN ID	Remark
4	
1	

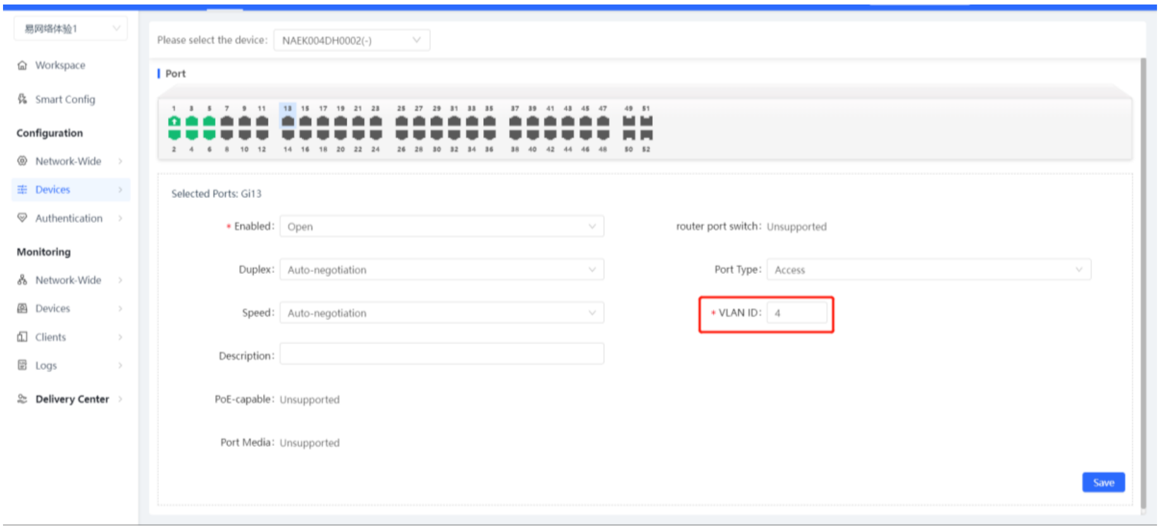
(2) Adding an interface to the VLAN

Choose **Configuration** > **Devices** > **Switch** > **Interface** to go to the device network port page.



Please select the device: NAEK0048H0001(-)

Select a device, click the port to be configured, set **VLAN ID** to the ID of the created VLAN, and then click **Save**.



Please select the device: NAEK004DH0002(-)

Selected Ports: Gi13

* Enabled: Open

router port switch: Unsupported

Duplex: Auto-negotiation

Port Type: Access

Speed: Auto-negotiation

* VLAN ID: 4

Description:

PoE-capable: Unsupported

Port Media: Unsupported

9.4 Routing

9.4.1 Adding a Static Route

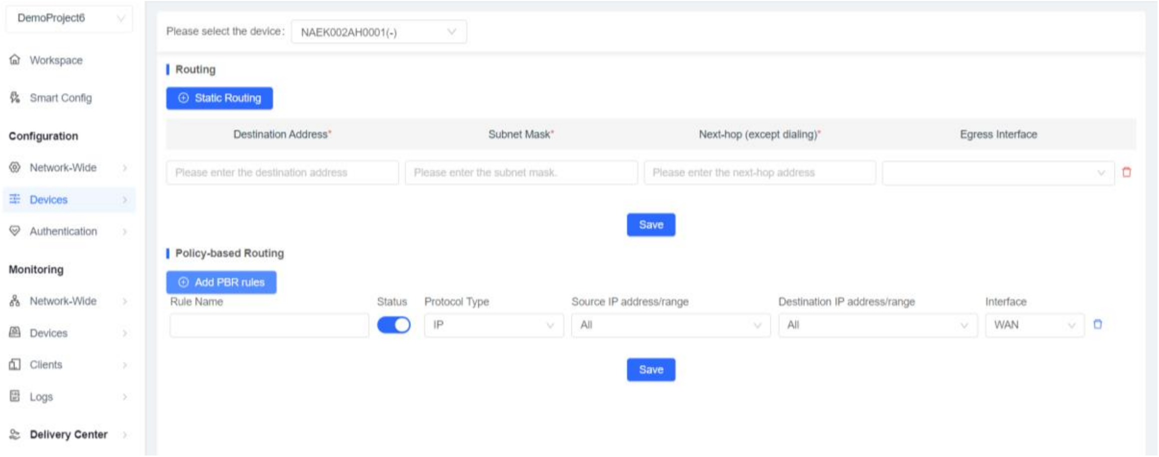
Static routes are manually configured. When a data packet matches a static route, the packet will be forwarded based on the specified forwarding mode.

Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

Procedure

Choose **Project** > **Device** > **Routing**, click **Static Routing**, click **Save**.



Please select the device: NAEK002AH0001(-)

Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface
Please enter the destination address	Please enter the subnet mask.	Please enter the next-hop address	

Rule Name	Status	Protocol Type	Source IP address/range	Destination IP address/range	Interface
	●	IP	All	All	WAN

The following table lists the description of parameters.

Parameter	Description
Destination Address	Specify the destination network to which data packets are to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.
Next-hop Address	Specify the IP address of the next hop in the route for data packets. If the outbound interface accesses the Internet through PPPoE dialing, you do not need to configure the next-hop address.
Egress	Specify the interface that forwards data packets.

9.4.2 Adding PBR

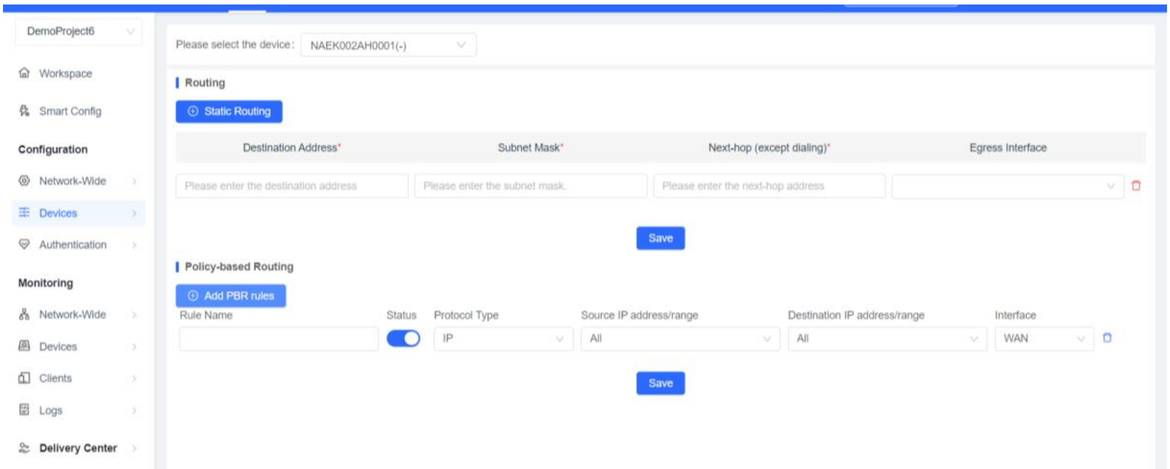
Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets based on configured rules, and then forwards the matched packets according to the specified forwarding policy. PBR enables the device to define rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forward the data packets from a specific interface.

In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data to the external network may be sent to the internal network, resulting in network exceptions. To prevent these exceptions, you need to configure PBR to control data isolation and forwarding on the internal and external networks.

The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing are in descending order of priority.

Procedure

Choose **Project** > **Device** > **Routing**, choose **Add PBR rules**, set parameters, and click **Save**.



Please select the device: NAEK002AH0001(-)

Routing

Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface
Please enter the destination address	Please enter the subnet mask	Please enter the next-hop address	

Policy-based Routing

Rule Name	Status	Protocol Type	Source IP address/range	Destination IP address/range	Interface
	●	IP	All	All	WAN

The following table lists the description of parameters.

Parameter	Description
Rule Name	Specify the name of a PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Status	Indicate whether to enable the PBR rule. If the value is disabled, this rule does not take effect.
Protocol Type	Specify the protocol for which the PBR rule is effective. You can set this parameter to IP, ICMP, UDP, TCP, or Custom.
Source IP/IP Range	Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses. All IP Addresses: Match all the source IP addresses. Custom: Match the source IP addresses in the specified IP address range.

Parameter	Description
Destination IP/IP Range	Configure the destination IP address or IP address range for matching PBR entries. The default value is All IP Addresses. All IP Addresses: Match all the destination IP addresses. Custom: Match the destination IP addresses in the specified IP address range.
Interface	Specify the interface that forwards data packets based on the hit PBR rule.

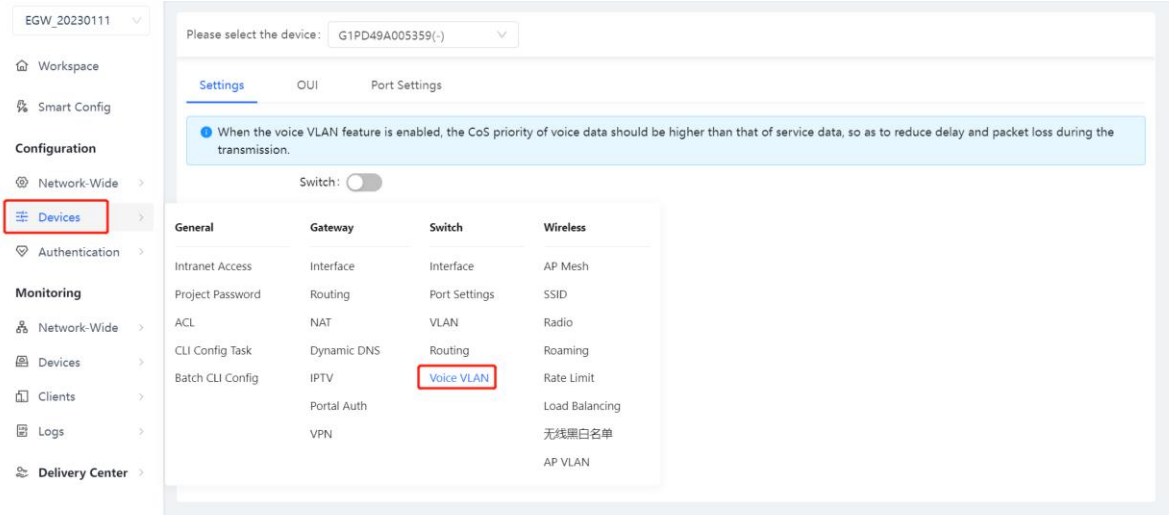
9.5 Voice VLAN

9.5.1 Overview

Voice VLAN is a VLAN specially classified for users' voice data streams. Voice VLAN limits data streams and voice streams to the data VLAN and voice VLAN respectively. When the voice VLAN feature is enabled, the CoS priority of voice data should be higher than that of service data, so as to reduce delay and packet loss during the transmission, thereby improving the voice quality.

9.5.2 Configuration Steps

Choose **Configuration** > **Devices** > **Switch** > **Voice VLAN**.



EGW_20230111

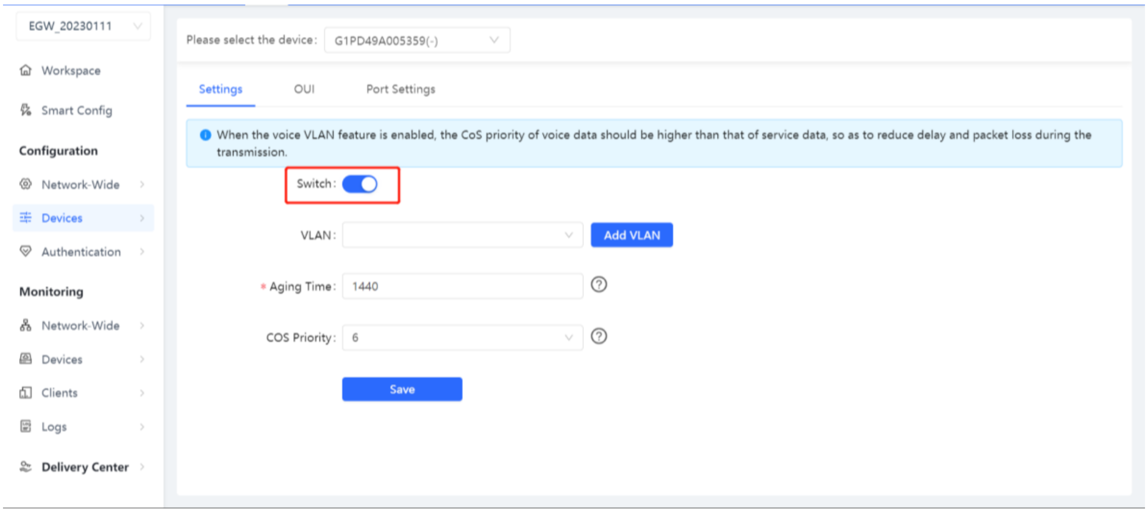
Please select the device: G1PD49A005359(-)

When the voice VLAN feature is enabled, the CoS priority of voice data should be higher than that of service data, so as to reduce delay and packet loss during the transmission.

Switch: ○

1. Voice VLAN Settings

Enable voice VLAN, set **VLAN**, **Aging Time**, and **COS Priority**, and click **Save**.



Please select the device: G1PD49A005359(-)

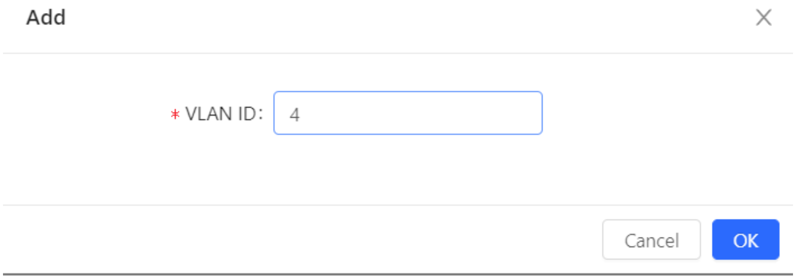
When the voice VLAN feature is enabled, the CoS priority of voice data should be higher than that of service data, so as to reduce delay and packet loss during the transmission.

Switch:

VLAN:

* Aging Time: 1440

COS Priority: 6

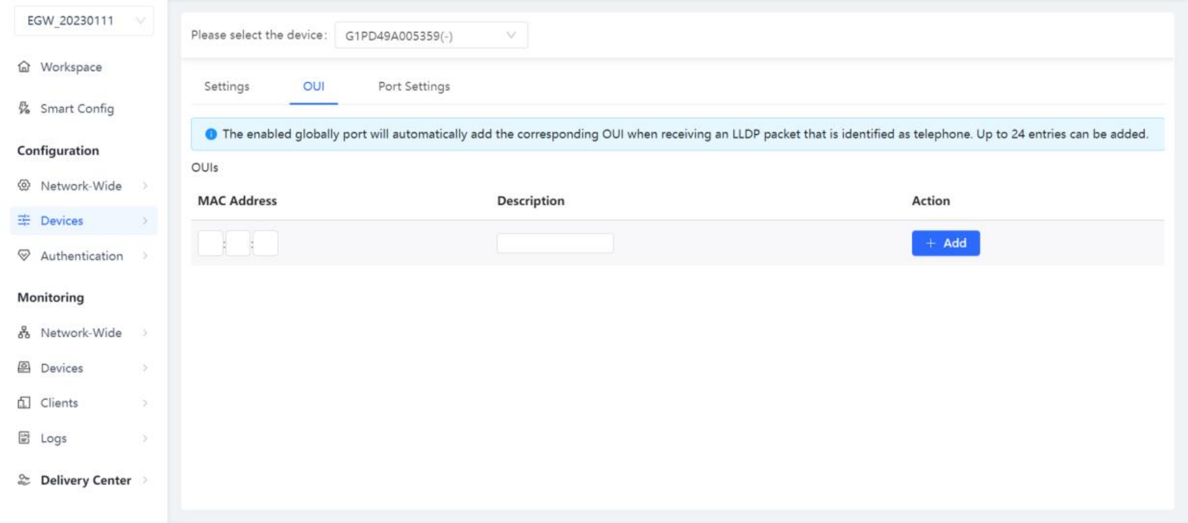


* VLAN ID: 4

2. OUI Settings

The device identifies the source MAC address of the input message and configures the OUI address to identify the voice data stream of the specified voice device. The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

Enter the MAC address and click <Add> to add the OUI address.

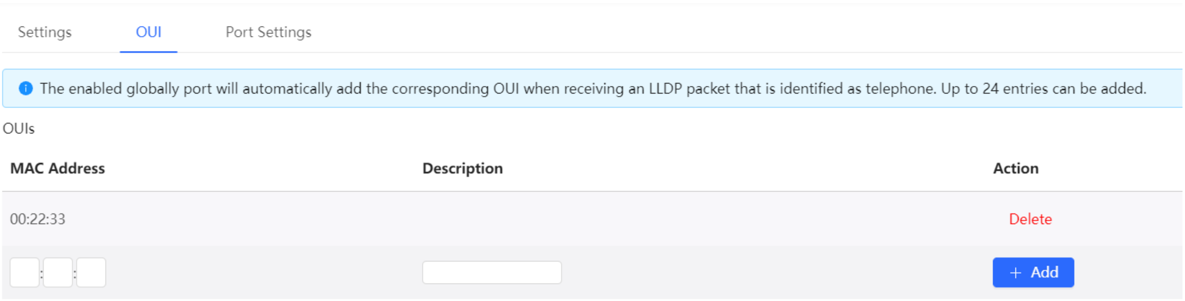


Please select the device: G1PD49A005359(-)

The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone. Up to 24 entries can be added.

OUIs

MAC Address	Description	Action
: :		+ Add



The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone. Up to 24 entries can be added.

OUIs

MAC Address	Description	Action
00:22:33		Delete
: :		+ Add

3. Port Settings

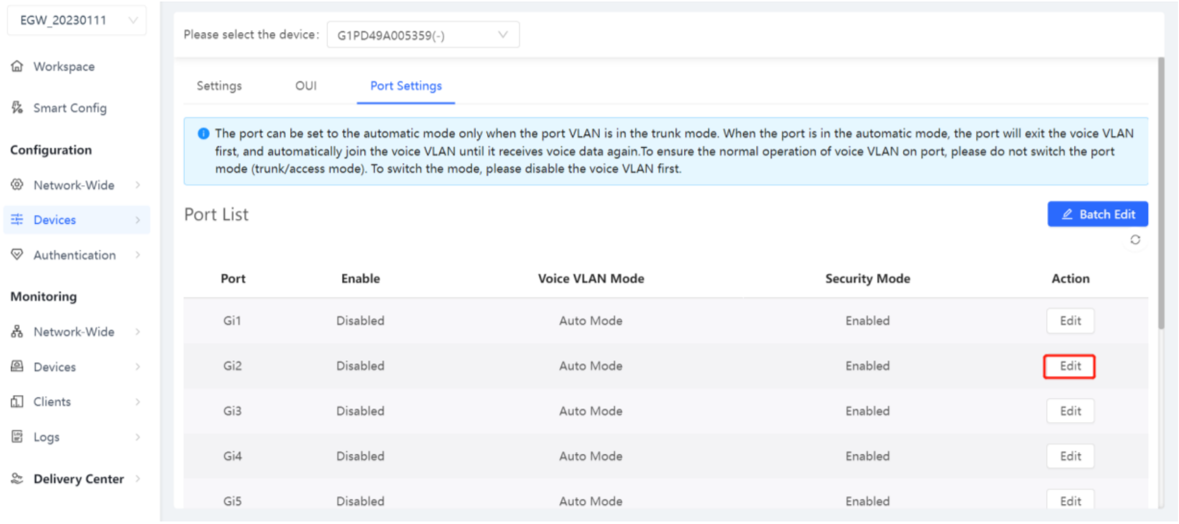
The port can be set to the automatic mode only when the port VLAN is in the trunk mode.

When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

Caution

To ensure the normal operation of voice VLAN on port, please do not switch the port mode (trunk/access mode). To switch the mode, please disable the voice VLAN first.

Select a port and click **Edit**. Configure **Voice VLAN Mode** and **Security Mode** and click **Confirm**.

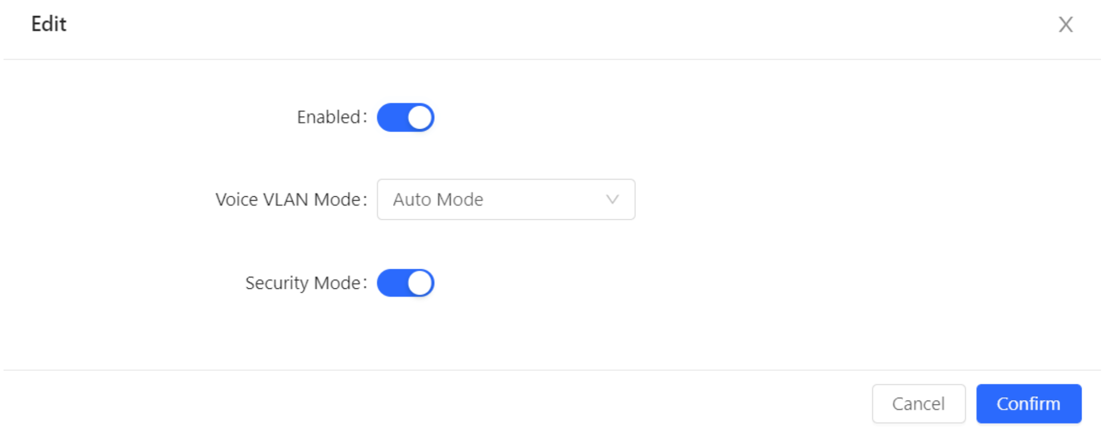


Please select the device: G1PD49A005359(-)

The port can be set to the automatic mode only when the port VLAN is in the trunk mode. When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.To ensure the normal operation of voice VLAN on port, please do not switch the port mode (trunk/access mode). To switch the mode, please disable the voice VLAN first.

Port List

Port	Enable	Voice VLAN Mode	Security Mode	Action
Gi1	Disabled	Auto Mode	Enabled	Edit
Gi2	Disabled	Auto Mode	Enabled	Edit
Gi3	Disabled	Auto Mode	Enabled	Edit
Gi4	Disabled	Auto Mode	Enabled	Edit
Gi5	Disabled	Auto Mode	Enabled	Edit



Enabled: ●

Voice VLAN Mode: Auto Mode

Security Mode: ●

10 Wireless Configuration

10.1 AP Mesh

Overview

- When wired uplink is unavailable in the deployment area, wireless uplink is used for mesh networking to prevent coverage holes.
- An AP automatically scans and selects the best uplink AP. When an uplink fails, the AP will automatically switch to another uplink AP.
- When the wired network fails, a wired AP will automatically switch to the wireless uplink to ensure high availability.

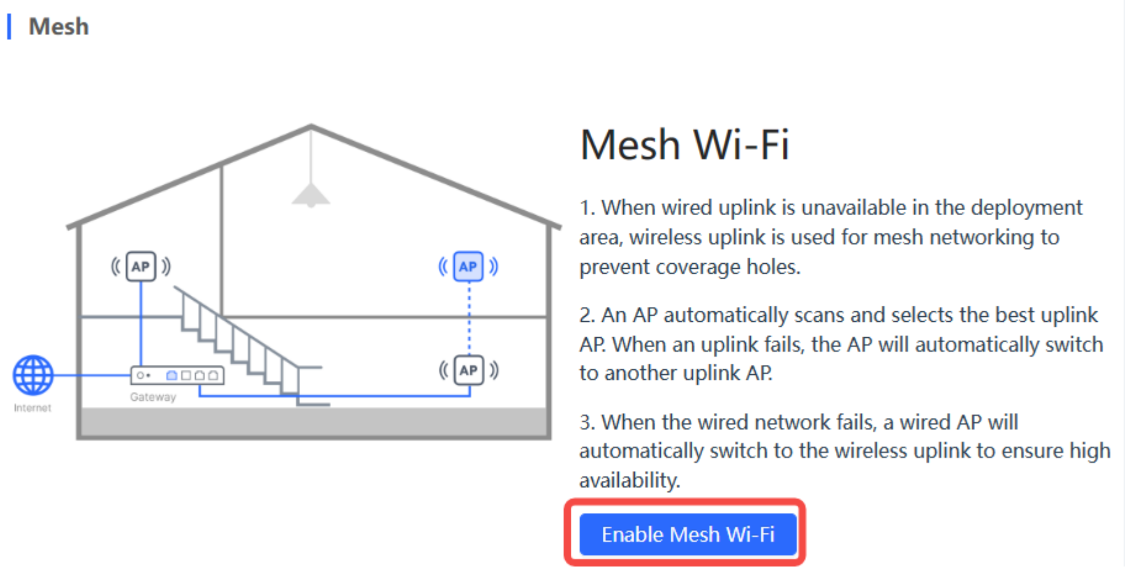
Configuration

(1) Power on all devices.

(2) Place the root AP and Mesh AP within each other's Wi-Fi coverage radius (RSSI > -70 dBm).

(3) Log in to Ruijie Cloud, choose **Configuration** > **Devices** > **Wireless** > **AP mesh**, and select a network in this account.

(4) Confirm that the mesh function (enabled by default) is enabled. If the mesh function is disabled, click **Enable Mesh Wi-Fi**.



Mesh Wi-Fi

1. When wired uplink is unavailable in the deployment area, wireless uplink is used for mesh networking to prevent coverage holes.

2. An AP automatically scans and selects the best uplink AP. When an uplink fails, the AP will automatically switch to another uplink AP.

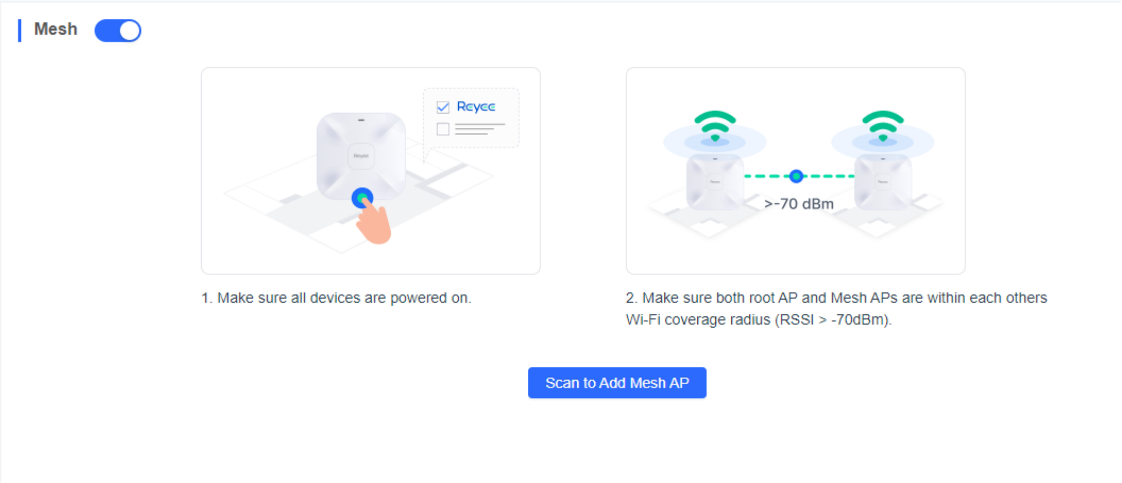
3. When the wired network fails, a wired AP will automatically switch to the wireless uplink to ensure high availability.

(5) Click **Scan to Add Mesh AP**.

Caution

- Up to 8 APs can be paired at a time.
- You are advised to use a maximum of 16 APs to set up a mesh network.
- The Mesh AP must be a Reyee AP.
- The AP is powered on.

- The distance between Root AP and Mesh AP should be less than 2 m.
- A provisioned AP is restored to factory defaults.



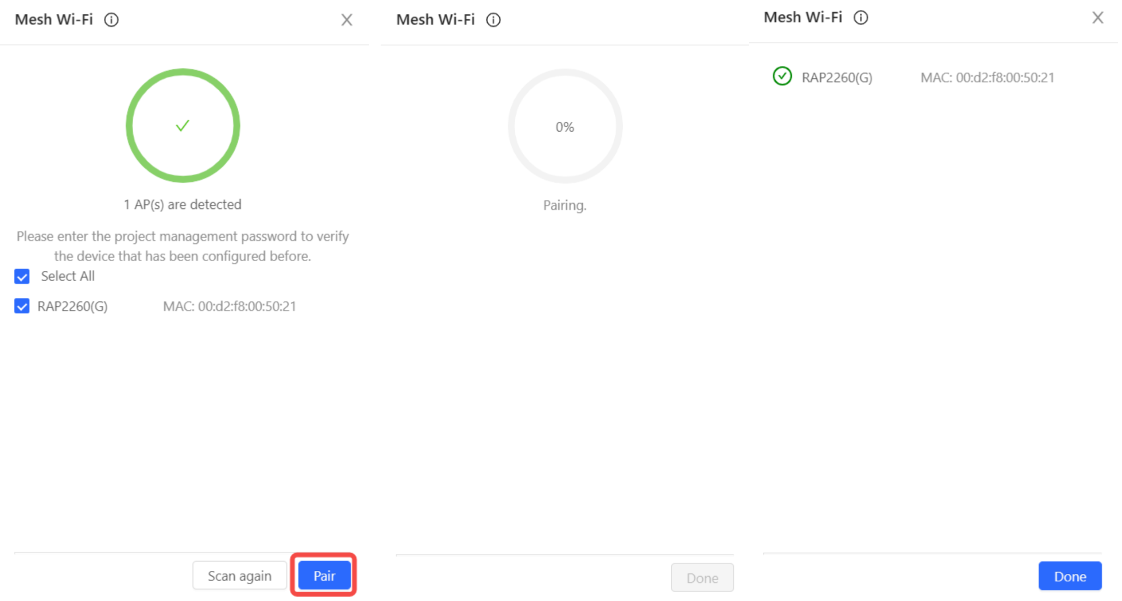
Mesh

1. Make sure all devices are powered on.

2. Make sure both root AP and Mesh APs are within each others Wi-Fi coverage radius (RSSI > -70dBm).

Scan to Add Mesh AP

(6) Select the AP to be paired in the scanning result and click **Pair**. Wait for pairing completion.



Mesh Wi-Fi ⓘ ×

✓

1 AP(s) are detected

Please enter the project management password to verify the device that has been configured before.

☑ Select All

☑ RAP2260(G) MAC: 00:d2:f8:00:50:21

Scan again Pair

Mesh Wi-Fi ⓘ

0%

Pairing.

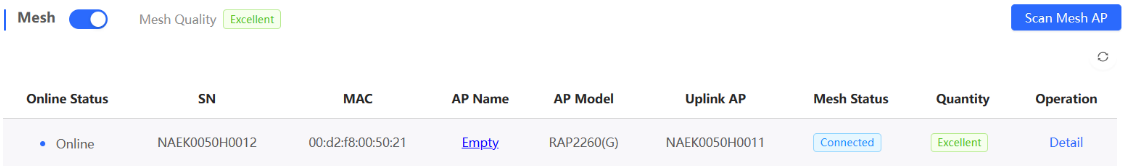
Done

Mesh Wi-Fi ⓘ ×

✓ RAP2260(G) MAC: 00:d2:f8:00:50:21

Done

After pairing, you can view information about the mesh device on the **AP Mesh** page.



Mesh Mesh Quality Excellent Scan Mesh AP

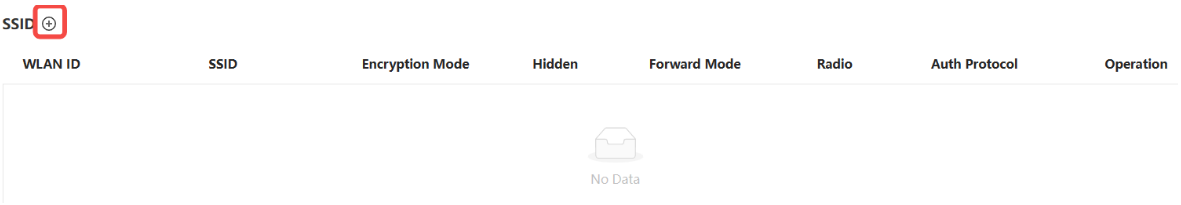
Online Status	SN	MAC	AP Name	AP Model	Uplink AP	Mesh Status	Quantity	Operation
• Online	NAEK0050H0012	00:d2:f8:00:50:21	Empty	RAP2260(G)	NAEK0050H0011	Connected	Excellent	Detail

10.2 SSID

10.2.1 SSID Basic Settings

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **SSID**, and select a network in this account.

(2) On the **SSID** setting page, click ⊕ next to **SSID** to create an SSID for devices on the network.

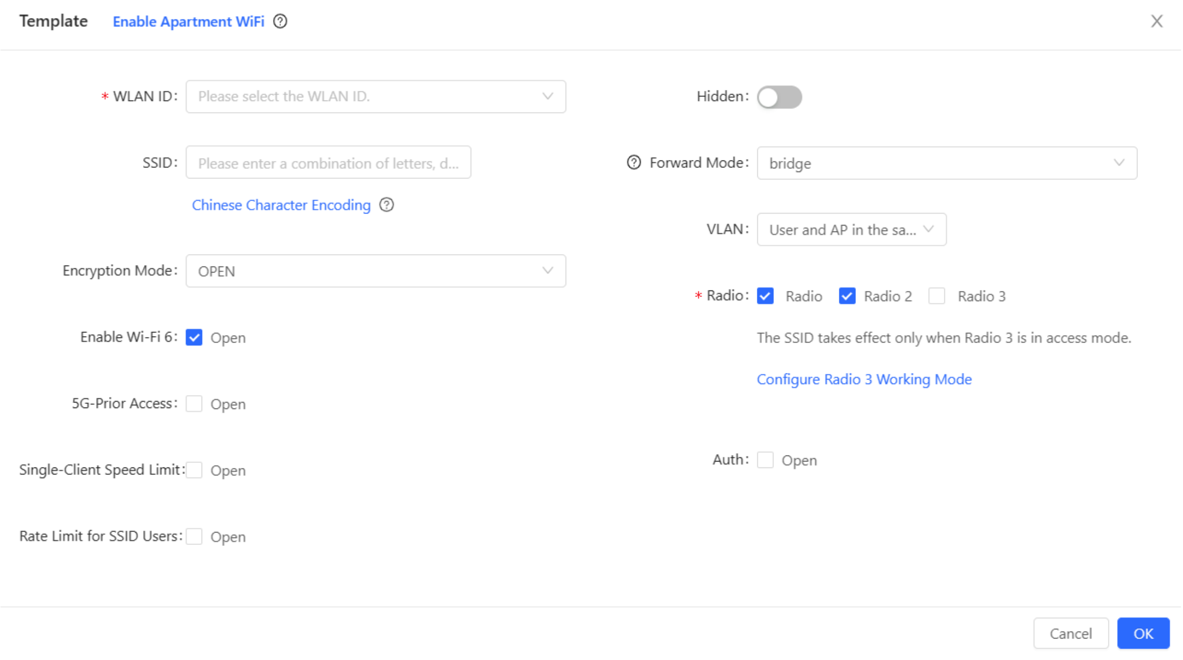


SSID ⊕

WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Protocol	Operation

No Data

(3) On the **SSID** setting page, you can create an SSID and fill in parameters as needed. After configuration, click **OK**.



Template Enable Apartment WiFi ⓘ ×

* WLAN ID: Please select the WLAN ID.

SSID: Please enter a combination of letters, d...

Chinese Character Encoding ⓘ

Encryption Mode: OPEN

Enable Wi-Fi 6: ☑ Open

5G-Prior Access: □ Open

Single-Client Speed Limit: □ Open

Rate Limit for SSID Users: □ Open

Hidden: ○

ⓘ Forward Mode: bridge

VLAN: User and AP in the sa...

* Radio: ☑ Radio ☑ Radio 2 □ Radio 3

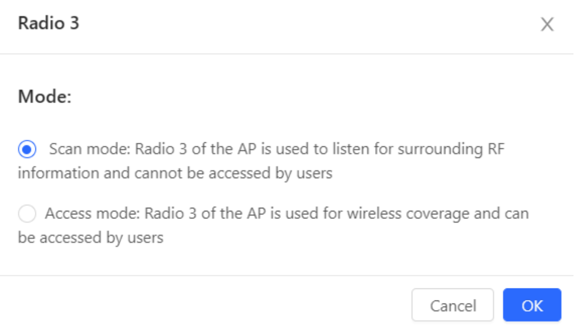
The SSID takes effect only when Radio 3 is in access mode.

Configure Radio 3 Working Mode

Auth: □ Open

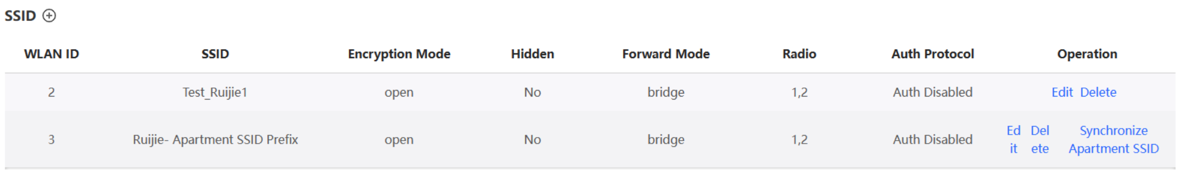
Table 10-1 Description of SSID Configuration Parameters

Parameter	Description
Enable Apartment WiFi	In apartment and quasi-apartment scenarios (AP-based independent SSID scenarios), **Enable Apartment WiFi** can be enabled. Recommended deployment for apartments: Deploy one AP in each room and name each AP using the room number. Each room has an independent SSID.

Parameter	Description
WLAN ID	It indicates the sequence number to represent an SSID. Up to 32 SSIDs are supported, and there may be differences between diverse models.
Hidden	It indicates whether to disable SSID broadcasting.
SSID	In general scenarios (that is, **Enable Apartment WiFi** is disabled), this parameter is valid. It indicates the Wi-Fi name.
SSID prefix	In apartment and quasi-apartment scenarios (that is, **Enable Apartment WiFi** is enabled), this parameter is valid, indicating the Wi-Fi name prefix. The SSID consists of the SSID prefix and AP name (you are advised to name APs after room numbers). For example, when you set **SSID prefix** to **RUIJIE-** and the AP name is 301, the SSID for the AP is RUIJIE-301. Note: Configure the apartment SSID password and alias on the AP details page. The default password is 88888888, which does not affect other SSID passwords. The SSID password here is just the apartment SSID password.
Forward Mode	It indicates the NAT mode or bridge mode. If you are not familiar with the live network design, the NAT mode is recommended. For details, see Configuration Description **of Forward Mode**.
Encryption Mode	The following encryption modes are supported: OPEN, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK, WPA2-Enterprise(802.1x). For details, see Encryption Mode.
Radio	In most cases, Radio1 represents 2.4 GHz and Radio2 represents 5 GHz, and Radio3 represents 2.4 GHz and 5 GHz. (Radio3 is supported on some models.) When you select **Radio3**, you can click **Configure Radio 3 Working Mode**.  Radio 3 Mode: ● Scan mode: Radio 3 of the AP is used to listen for surrounding RF information and cannot be accessed by users ○ Access mode: Radio 3 of the AP is used for wireless coverage and can be accessed by users
Enable Wi-Fi 6	Specify whether to enable **Wi-Fi 6**. On Reyee APs, **Wi-Fi 6** can be enabled based on the SSID. On RGOS APs, **Wi-Fi 6** can only be enabled based on the radio. After **Wi-Fi 6** is enabled, Wi-Fi 6 is applied to the radio corresponding to the SSID.

Parameter	Description
5G-Prior Access	Detect clients capable of 5 GHz and steer them to that frequency, while leaving 2.4 GHz available for legacy clients. Enabling this function is not recommended if most of clients only support 2.4 GHz.
Single-Client Speed Limit	It indicates the upload and download speed limiting for each client on this SSID.
Rate Limit for SSID Users	It indicates the total throughput (upload & download) on this SSID.
Auth	Specify whether to conduct authentication when **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**. After authentication is enabled, the following authentication protocols are supported: WiFiDog and WeChat Connect Wi-Fi (3.X). For details, see **Authentication Configuration Description**.

(4) View the SSID list.

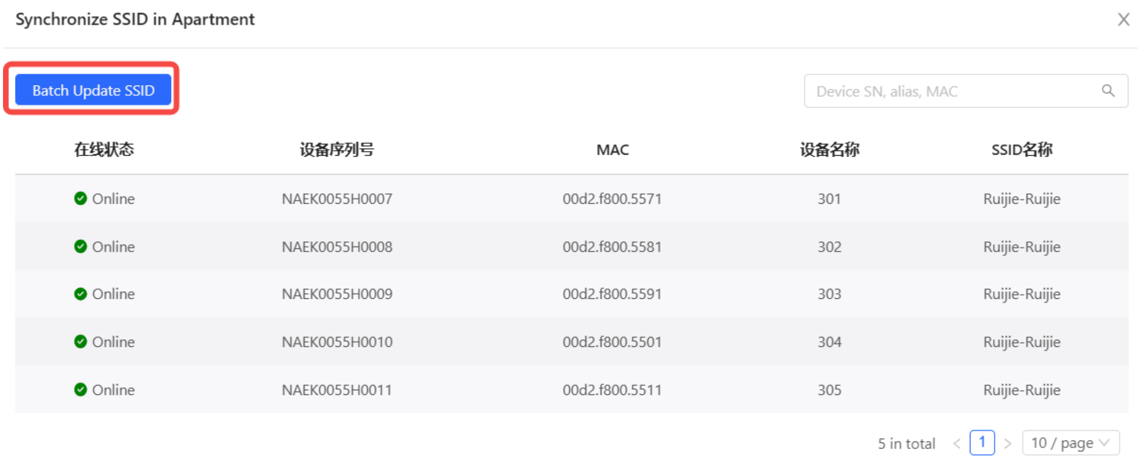


SSID ⊕

WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Protocol	Operation
2	Test_Ruijie1	open	No	bridge	1,2	Auth Disabled	Edit Delete
3	Ruijie- Apartment SSID Prefix	open	No	bridge	1,2	Auth Disabled	Edit Delete Synchronize Apartment SSID

The **Operation** column is described as follows:

- **Edit**: Click this button to modify SSID configuration parameters except WLAN ID.
- **Delete**: Click this button to delete a specified SSID.
- Synchronize Apartment SSID: If the AP name is changed, you must click this button to access the **Synchronize SSID in Apartment** page, and then click the **Batch Update SSID** button to update the SSIDs involved.



Synchronize SSID in Apartment

在线状态	设备序列号	MAC	设备名称	SSID名称
Online	NAEK0055H0007	00d2.f800.5571	301	Ruijie-Ruijie
Online	NAEK0055H0008	00d2.f800.5581	302	Ruijie-Ruijie
Online	NAEK0055H0009	00d2.f800.5591	303	Ruijie-Ruijie
Online	NAEK0055H0010	00d2.f800.5501	304	Ruijie-Ruijie
Online	NAEK0055H0011	00d2.f800.5511	305	Ruijie-Ruijie

1. Configuration Description of Forward Mode

Parameter Description

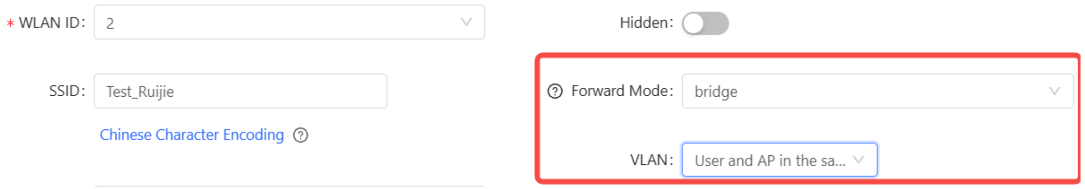
The following forwarding modes are supported: bridge, nat.

- NAT mode: An AP will serve as a router and use the DHCP pool to provide IP addresses for stations (STAs).
  - Common NAT: All devices can be configured with the same address pool. Otherwise, the current or default one will be used, 192.168.23.0/24.
  - Cloud NAT: In NAT roaming scenarios, this mode should be applied. You can configure a range for the cloud NAT address pool. Ruijie Cloud will distribute different address pools to different devices according to the range.

  If SSIDs in both NAT mode and Cloud NAT mode are configured, Ruijie Cloud will only deliver the Cloud NAT pool (that is, assign a pool to each device), but not the NAT pool.
- Bridge mode: An AP will function as a switch and allow all traffic to pass through. You need to specify the VLAN ID for users. The users and AP can use the same VLAN or different VLANs.
  - Users and the AP use the same VLAN: The users and AP share the address pool. It is applicable to the case, in which the address pool of the AP is also a DHCP address pool.
  - Users and the AP use different VLANs: The user VLAN and IP address pool are a part of the local network. It is applicable to the case, in which the local network can separately assign VLANs and addresses to users.

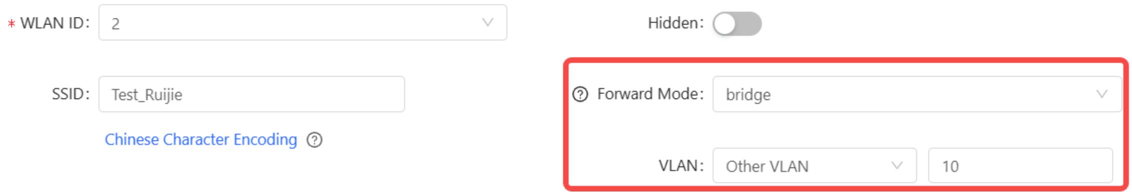
Configuration Example

- **Forward Mode** is set to **bridge** and users and the AP are in the same VLAN.



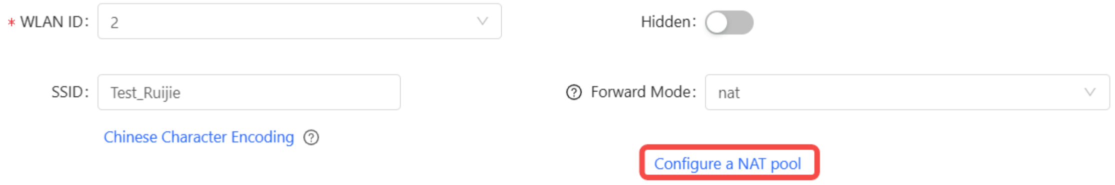
* WLAN ID: 2
Hidden: ○
SSID: Test_Ruijie
Forward Mode: bridge
VLAN: User and AP in the sa...

- **Forward Mode** is set to **bridge** and users and the AP are in different VLANs. The client connected to the SSID will seek the DHCP server with VLAN 10 on the network to obtain the address.



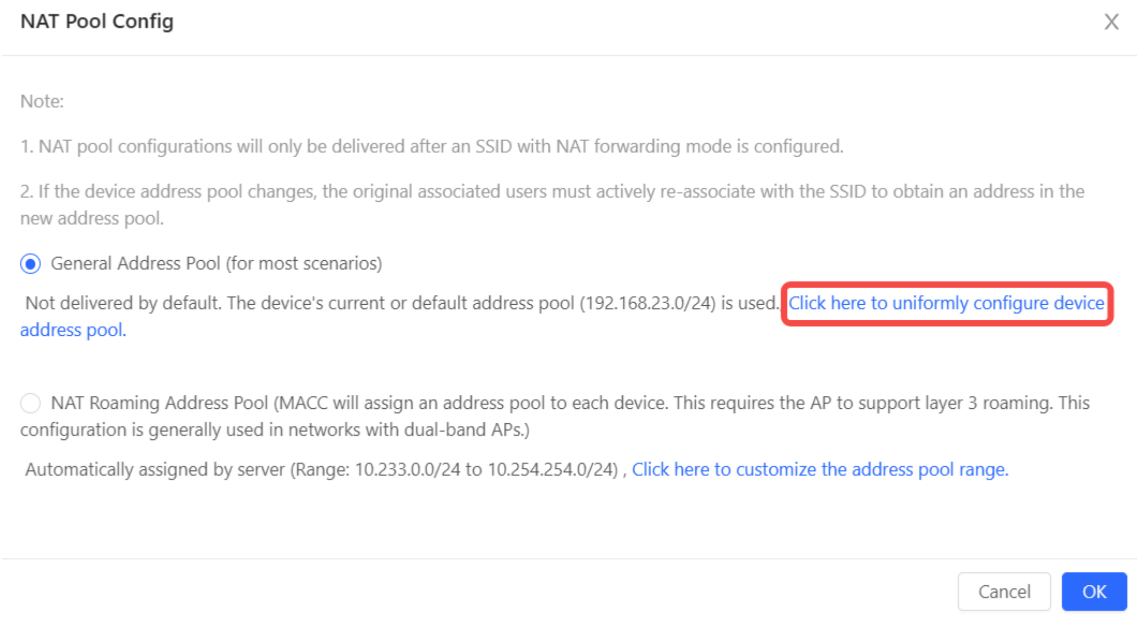
* WLAN ID: 2
Hidden: ○
SSID: Test_Ruijie
Forward Mode: bridge
VLAN: Other VLAN 10

- When the NAT mode is configured, click **Configure a NAT Pool** to access the address pool configuration interface.



* WLAN ID: 2
Hidden: ○
SSID: Test_Ruijie
Forward Mode: nat

- Uniformly configure the device address pool: Select **General Address Pool** and click **Click here to uniformly configure device address pool.** to customize the address pool. After configuration, click **OK**.



NAT Pool Config

Note:

1. NAT pool configurations will only be delivered after an SSID with NAT forwarding mode is configured.

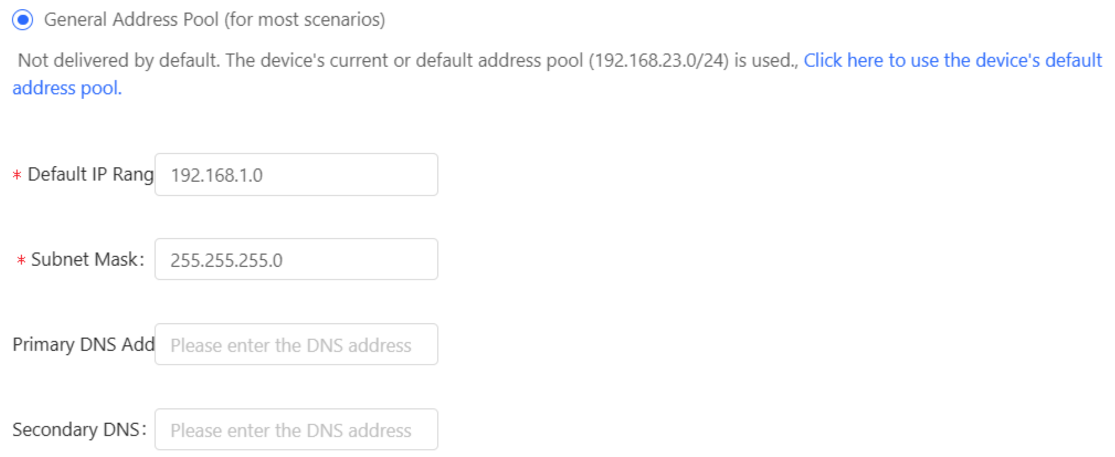
2. If the device address pool changes, the original associated users must actively re-associate with the SSID to obtain an address in the new address pool.

● General Address Pool (for most scenarios)

Not delivered by default. The device's current or default address pool (192.168.23.0/24) is used. Click here to uniformly configure device address pool.

○ NAT Roaming Address Pool (MACC will assign an address pool to each device. This requires the AP to support layer 3 roaming. This configuration is generally used in networks with dual-band APs.)

Automatically assigned by server (Range: 10.233.0.0/24 to 10.254.254.0/24) , Click here to customize the address pool range.

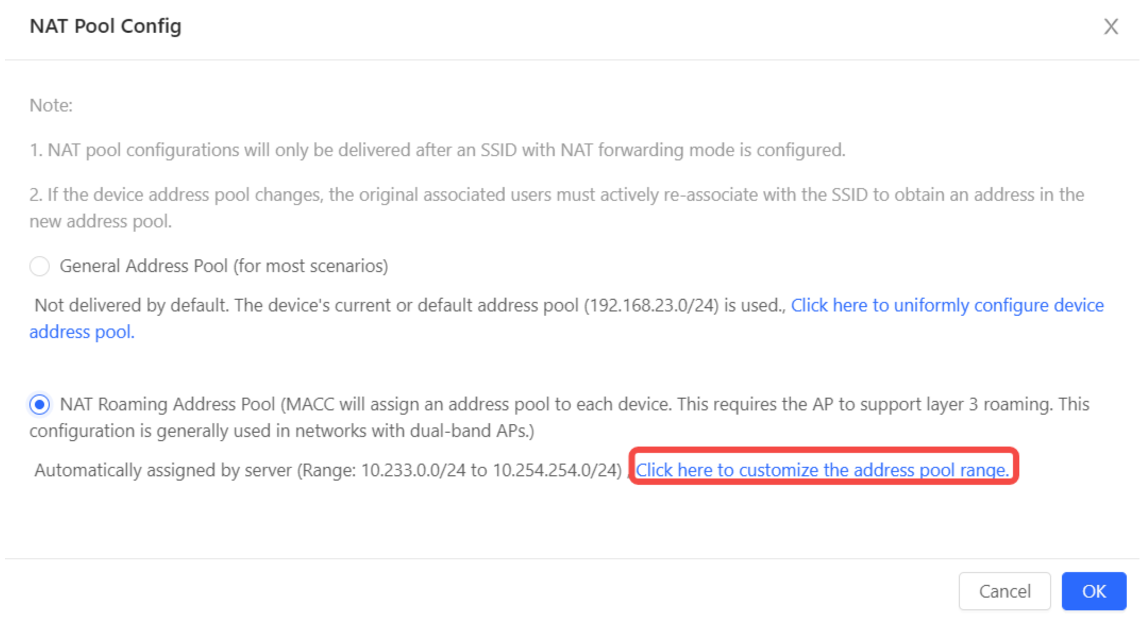


● General Address Pool (for most scenarios)

Not delivered by default. The device's current or default address pool (192.168.23.0/24) is used., Click here to use the device's default address pool.

* Default IP Rang	192.168.1.0
* Subnet Mask:	255.255.255.0
Primary DNS Add	Please enter the DNS address
Secondary DNS:	Please enter the DNS address

- When there are multiple APs on a network and Layer 3 roaming is enabled, select **NAT Roaming Address Pool** Mode and click **Click here to customize the address pool range.** to configure the address pool range. After configuration, click **OK**.



NAT Pool Config

Note:

1. NAT pool configurations will only be delivered after an SSID with NAT forwarding mode is configured.

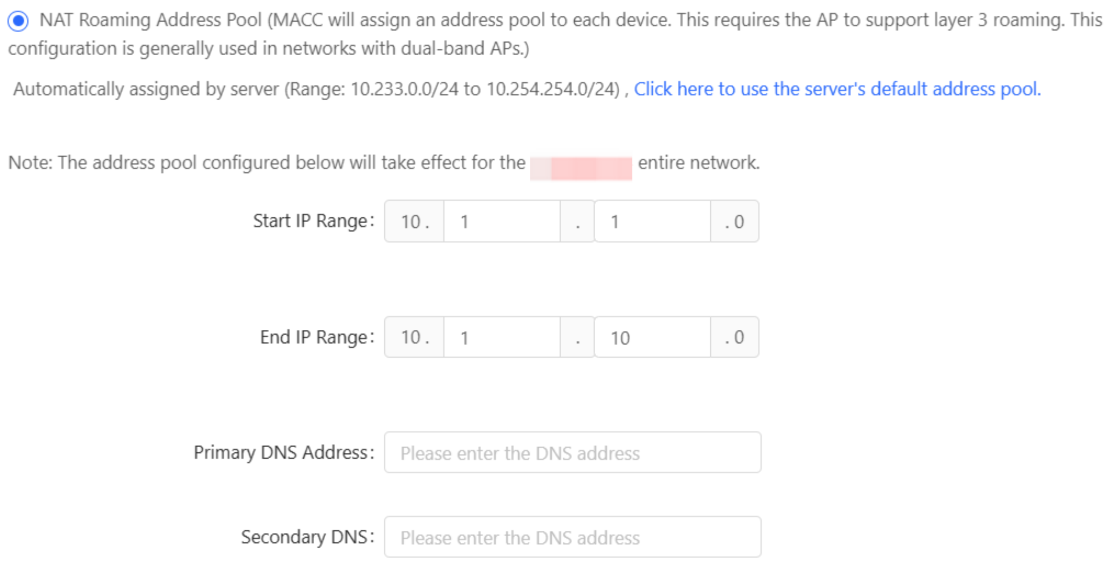
2. If the device address pool changes, the original associated users must actively re-associate with the SSID to obtain an address in the new address pool.

○ General Address Pool (for most scenarios)

Not delivered by default. The device's current or default address pool (192.168.23.0/24) is used., Click here to uniformly configure device address pool.

● NAT Roaming Address Pool (MACC will assign an address pool to each device. This requires the AP to support layer 3 roaming. This configuration is generally used in networks with dual-band APs.)

Automatically assigned by server (Range: 10.233.0.0/24 to 10.254.254.0/24) , Click here to customize the address pool range.



● NAT Roaming Address Pool (MACC will assign an address pool to each device. This requires the AP to support layer 3 roaming. This configuration is generally used in networks with dual-band APs.)

Automatically assigned by server (Range: 10.233.0.0/24 to 10.254.254.0/24) , Click here to use the server's default address pool.

Note: The address pool configured below will take effect for the [redacted] entire network.

Start IP Range: 10 . 1 . 1 . 0

End IP Range: 10 . 1 . 10 . 0

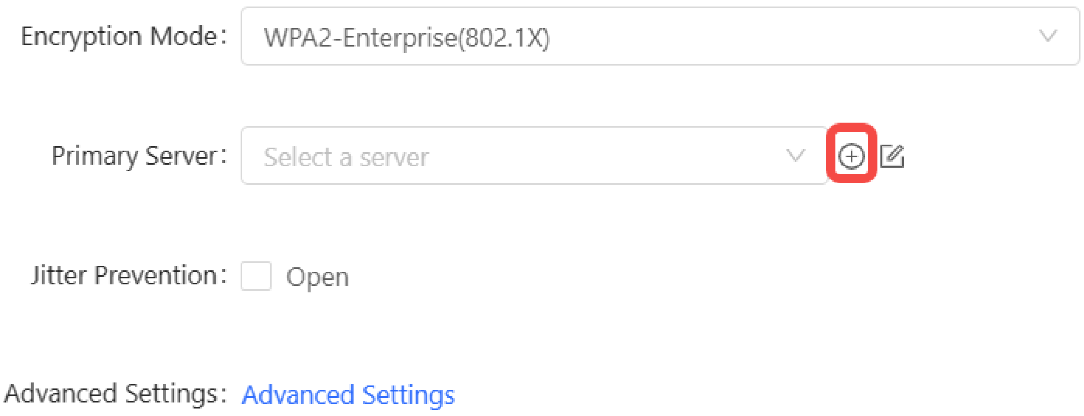
Primary DNS Address: Please enter the DNS address

Secondary DNS: Please enter the DNS address

2. Configuration Description of Encryption Mode

- **OPEN**: Open the SSID. The password is not required.
- **WPA-PSK**: Use the WPA algorithm to encrypt the SSID. The password is required. After **PPSK** is selected, each client connected to the network will be assigned a separate Wi-Fi key and an account.
- **WPA2-PSK**: Use the WPA2 algorithm to encrypt the SSID. The password is required. After **PPSK** is selected, each client connected to the network will be assigned a separate Wi-Fi key and an account.
- **WPA/WPA2-PSK**: Use the WPA/WPA2 algorithm to encrypt the SSID. The password is required. After **PPSK** is selected, each client connected to the network will be assigned a separate Wi-Fi key and an account.
- **WPA2-Enterprise(802.1x)**: 802.1X authentication and the external RADIUS server are required.

a Set **Encryption Mode** to **WPA2-Enterprise(802.1x)** and click ⊕ in the **Primary Server** line.



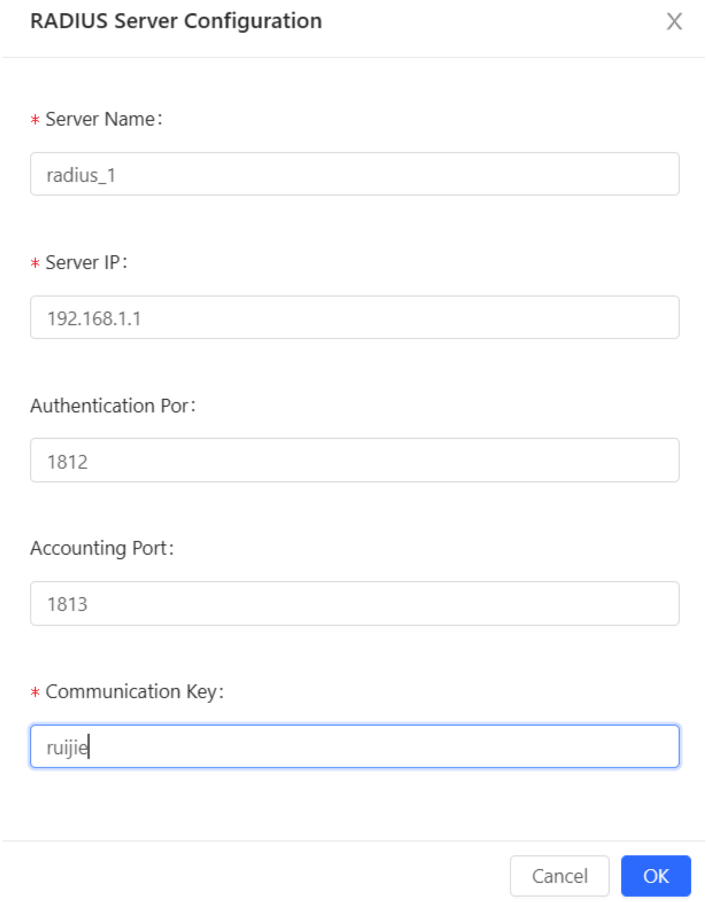
Encryption Mode: WPA2-Enterprise(802.1X)

Primary Server: Select a server

Jitter Prevention: □ Open

Advanced Settings: Advanced Settings

b Set parameters of the standby RADIUS server and click **OK**



RADIUS Server Configuration

* Server Name: radius_1

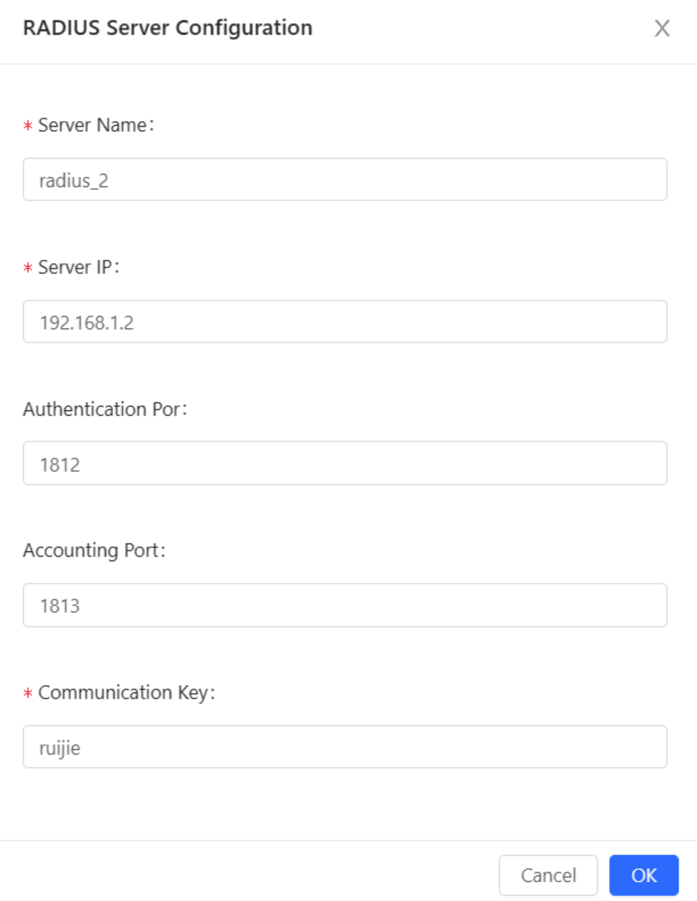
* Server IP: 192.168.1.1

Authentication Por: 1812

Accounting Port: 1813

* Communication Key: ruijie

c If the standby RADIUS server exists, click ⊕ in the **Standby Server** line. Set parameters of the standby RADIUS server and click **OK**



RADIUS Server Configuration

* Server Name: radius_2

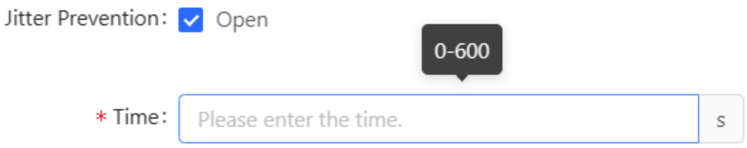
* Server IP: 192.168.1.2

Authentication Por: 1812

Accounting Port: 1813

* Communication Key: ruijie

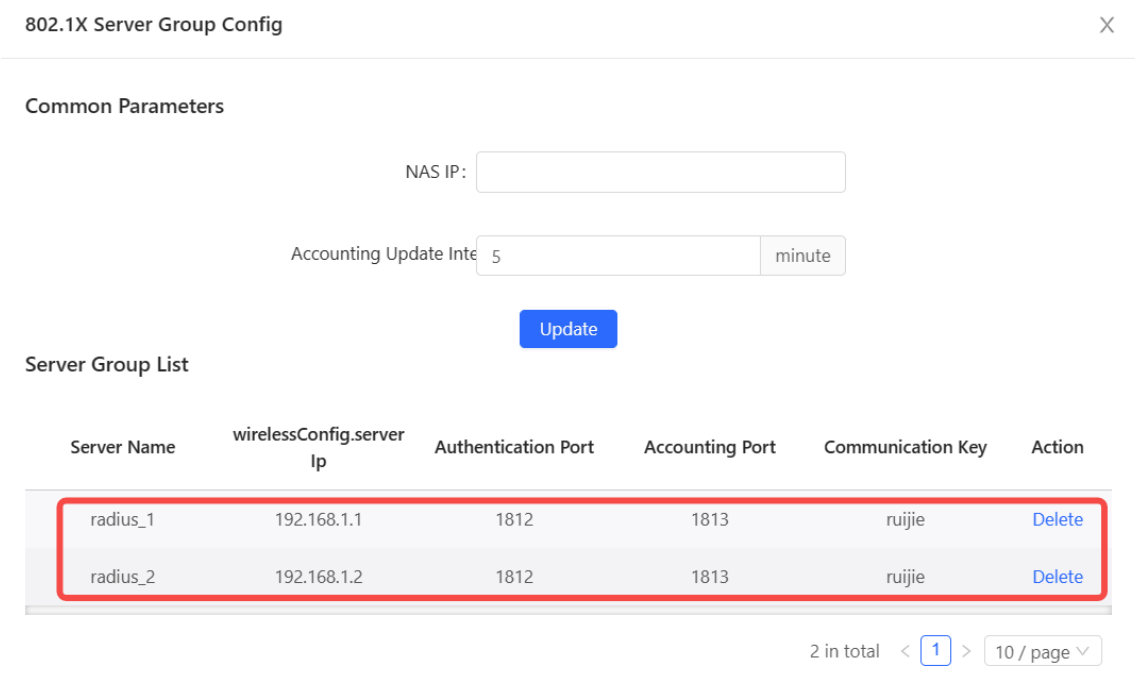
d In order to prevent users from repeatedly requesting authentication in a short period of time, you can enable **Jitter Prevention** and set the jitter prevention duration (0–600s).



Jitter Prevention: ☑ Open

* Time: Please enter the time. s

e Click **Advanced Settings** to check the radius server list.



802.1X Server Group Config

Common Parameters

NAS IP:

Accounting Update Inte 5 minute

Server Group List

Server Name	wirelessConfig.server Ip	Authentication Port	Accounting Port	Communication Key	Action
radius_1	192.168.1.1	1812	1813	ruijie	Delete
radius_2	192.168.1.2	1812	1813	ruijie	Delete

2 in total < 1 > 10 / page

3. Authentication Configuration Description

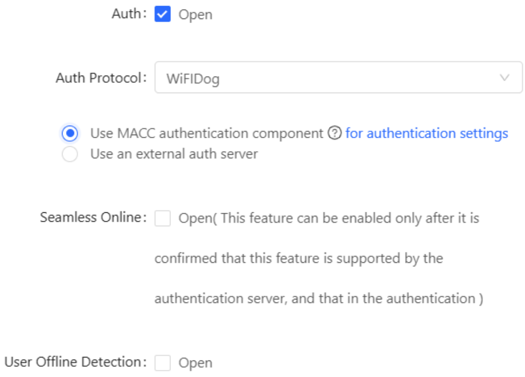
Two authentication protocols are supported:

- **WiFiDog**: The protocol sends random dynamic passwords to users' mobile phones in the form of SMs. When the users use the wireless network, they enter the dynamic passwords on the authentication portal page to complete their identity real name verification, thereby ensuring the security of the wireless network.
- **WeChat Connect Wi-Fi (3.X)**: It is an authentication way that can quickly connect to a Wi-Fi hotspot through WeChat. By scanning the QR code in WeChat, users can quickly connect to the Wi-Fi network provided by merchants for free Internet access. After the connection is successful, a status prompt "Connecting to Wi-Fi" will appear at the top of the main page of users' WeChat. Users can click this prompt to view the merchant's official account and special offer and use online functions and services provided by the merchant.

You can use the authentication component of Ruijie Cloud or an external authentication server for authentication.

- Using the authentication component of Ruijie Cloud

To use the authentication component of Ruijie Cloud, configure authentication for the network on Ruijie Cloud. For details, see 11.1 Captive Portal.



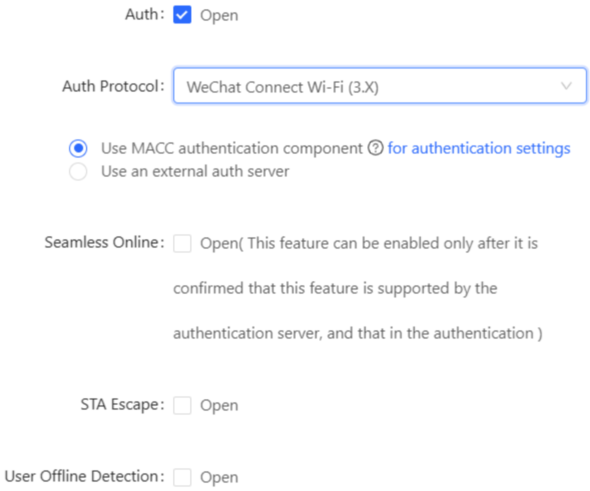
Auth: ☑ Open

Auth Protocol: WiFIDog

● Use MACC authentication component ⓘ for authentication settings
○ Use an external auth server

Seamless Online: □ Open(This feature can be enabled only after it is confirmed that this feature is supported by the authentication server, and that in the authentication)

User Offline Detection: □ Open



Auth: ☑ Open

Auth Protocol: WeChat Connect Wi-Fi (3.X)

● Use MACC authentication component ⓘ for authentication settings
○ Use an external auth server

Seamless Online: □ Open(This feature can be enabled only after it is confirmed that this feature is supported by the authentication server, and that in the authentication)

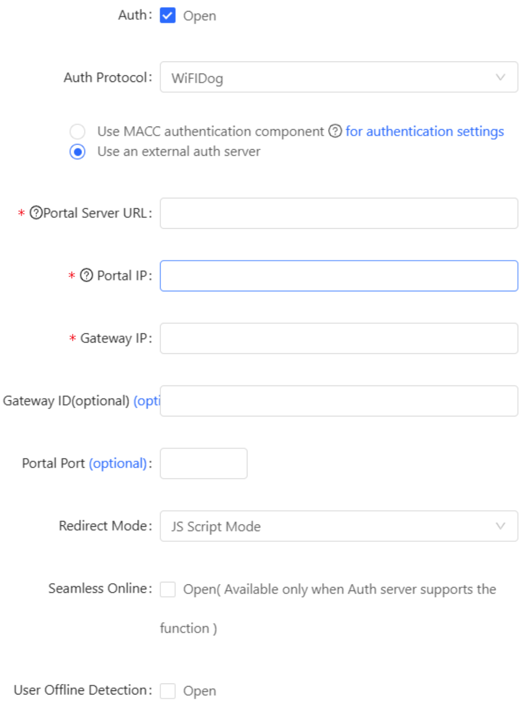
STA Escape: □ Open

User Offline Detection: □ Open

Table 10-2 Description of Authentication Configuration Parameters

Parameter	Description
Auth Protocol	Set it to **WiFiDog** or **WeChat Connect Wi-Fi (3.X)**.
Seamless Online:	Users only need to pass authentication once. If they want to go online again, authentication is not required. After users go online, they do not need to log in again in the specified period. To use this function, ensure that MAB authentication is enabled for the network so that authentication and Internet access can be normally performed.
STA Escape	This parameter is valid when **Auth Protocol** is set to **WeChat Connect Wi-Fi (3.X)**. After the feature is enabled, if the server is unavailable, users can automatically go online when no authentication page is displayed. You are not advised to enable it. Network packet loss can easily trigger escape.
User Offline Detection	After it is enabled, inactive users will go offline automatically. It is disabled by default, indicating that the device uses the default configuration.

- Using an external authentication server



Auth: ☑ Open

Auth Protocol: WiFIDog

○ Use MACC authentication component ⓘ for authentication settings
● Use an external auth server

* ⓘPortal Server URL:

* ⓘ Portal IP:

* Gateway IP:

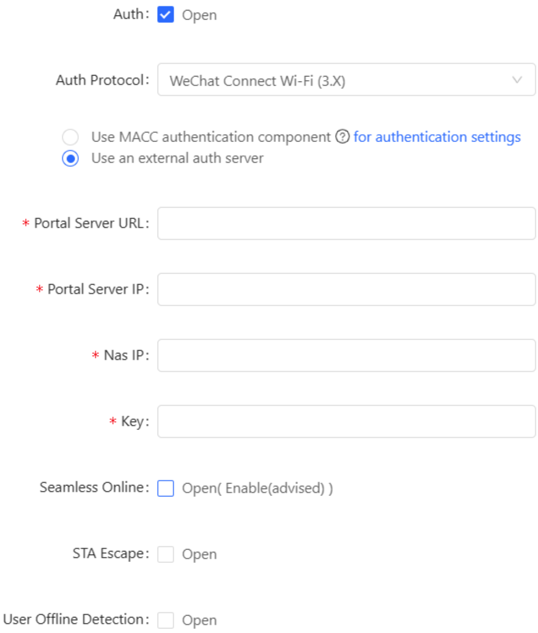
Gateway ID(optional) (opti

Portal Port (optional):

Redirect Mode: JS Script Mode

Seamless Online: □ Open(Available only when Auth server supports the function)

User Offline Detection: □ Open



Auth: ☑ Open

Auth Protocol: WeChat Connect Wi-Fi (3.X)

○ Use MACC authentication component ⓘ for authentication settings
● Use an external auth server

* Portal Server URL:

* Portal Server IP:

* Nas IP:

* Key:

Seamless Online: □ Open(Enable(advised))

STA Escape: □ Open

User Offline Detection: □ Open

Table 10-3 Description of WiFiDog Authentication Configuration Parameters

Parameter	Description
Portal Server URL	It indicates the URL of the external wifidog portal server. After authentication is enabled on the device, unauthenticated users will be redirected to the URL when accessing the Internet.
Portal IP	It indicates the IP address of the portal server. Device communicates with the Portal server configured with this IP address.
Gateway IP	It indicates the gateway IP for wifidog.
Gateway ID	It indicates the gateway ID for wifidog.
Portal Port:	It indicates the port number for landing page redirection.
Redirect Mode	It supports JS Script Mode and HTTP302.
Seamless Online	It indicates seamless authentication on STAs connected to an SSID. The authentication server that supports the seamless feature is required.
User Offline Detection	After it is enabled, inactive users will go offline automatically. It is disabled by default, indicating that the device uses the default configuration.

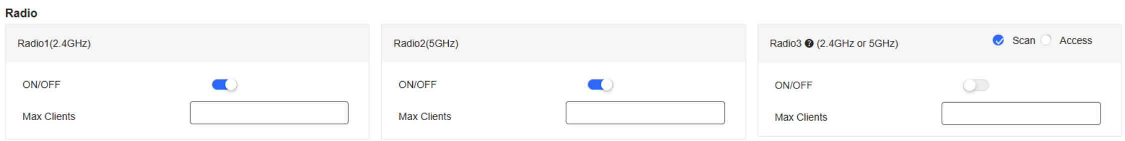
Table 10-4 **Description of WeChat Connect Wi-Fi (3.X) Authentication Configuration Parameters**

Parameter	Description
Portal Server URL	It indicates the URL of the external wifidog portal server. After authentication is enabled on the device, unauthenticated users will be redirected to the URL when accessing the Internet.
Portal IP	It indicates the IP address of the portal server. Device communicates with the Portal server configured with this IP address.
NAS IP	It indicates the source IP address used by the device to send RADIUS packets.
Key	It indicates the communication key.
Seamless Online:	It indicates seamless authentication on STAs connected to an SSID. The authentication server that supports the seamless feature is required.
STA Escape	This parameter is valid when **Auth Protocol** is set to **WeChat Connect Wi-Fi (3.X)**. After the feature is enabled, if the server is unavailable, users can automatically go online when no authentication page is displayed. You are not advised to enable it. Network packet loss can easily trigger escape.
User Offline Detection	After it is enabled, inactive users will go offline automatically. It is disabled by default, indicating that the device uses the default configuration.

10.2.2 Radio Settings

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **SSID**, and select a network in this account.

(2) On the **Radio** setting page, click ⊕ next to **Radio** and set parameters. Up to 3 Radios can be added.



Radio

Radio1(2.4GHz)
ON/OFF: on
Max Clients:

Radio2(5GHz)
ON/OFF: on
Max Clients:

Radio3 (2.4GHz or 5GHz) ● Scan ○ Access
ON/OFF: off
Max Clients:

ON/OFF: If this RF switch is turned off, all SSIDs in this frequency will be disabled and the clients can not access the Internet.

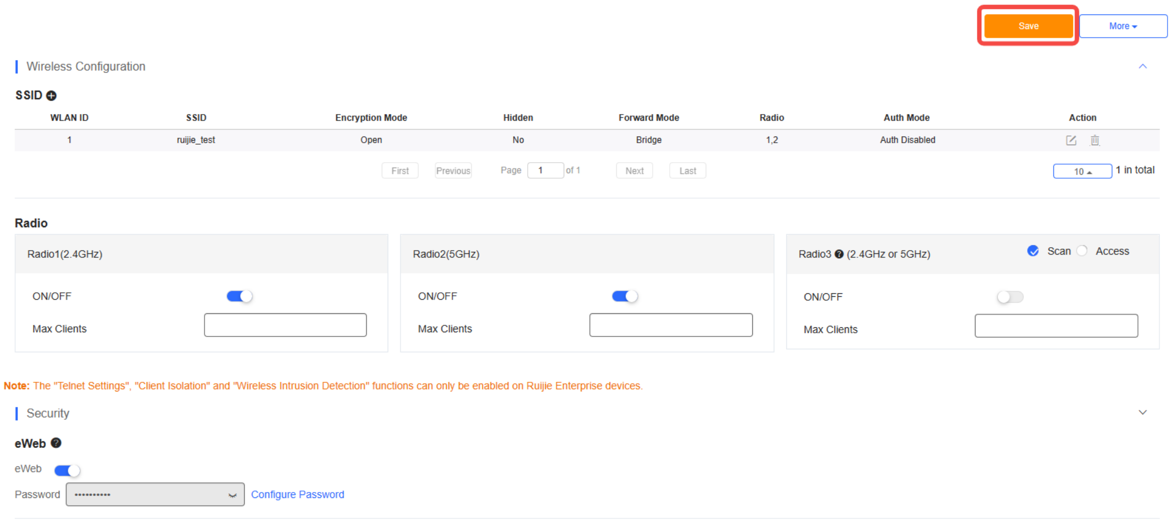
Max Clients: The maximum number of users set will take effect as the maximum number of users if it exceeds the maximum number of users actually supported by the AP; leave it blank to turn off the user limit.

Radio3: It is supported on some models. Supports configuring the operating mode.

Scan: Radio3 is used for collecting RF information around an AP. The client access service is unavailable.

Access: Radio3 is used for wireless coverage. The client access service is available.

(3) After configuration, click **Save**.



Wireless Configuration

SSID

WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	ruijie_test	Open	No	Bridge	1,2	Auth Disabled	

Radio

Radio1(2.4GHz)
ON/OFF
Max Clients

Radio2(5GHz)
ON/OFF
Max Clients

Radio3 (2.4GHz or 5GHz) ● Scan ○ Access
ON/OFF
Max Clients

Note: The "Telnet Settings", "Client Isolation" and "Wireless Intrusion Detection" functions can only be enabled on Ruijie Enterprise devices.

Security

eWeb

eWeb

Password •••••••••• Configure Password

10.3 Radio

Overview

The country code ensures each radio's broadcast frequency bands, interfaces, channels, and transmit power levels conform to country-specific regulations. The frequency bandwidth determines how many non-overlapping channels can be used for your AP to reduce RF interference.

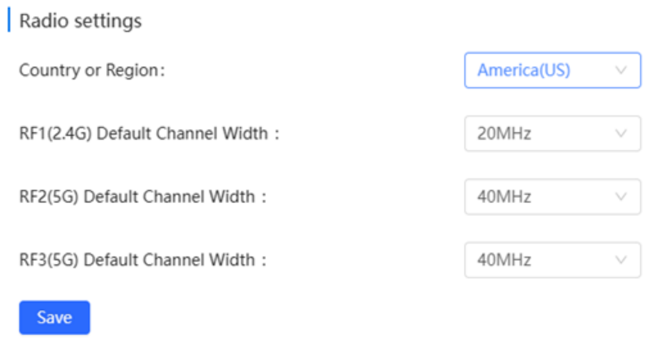
The best practice for user experience is 2.4 GHz in 20 MHz and 5 GHz in 40 MHz.

Procedure

Log in to Ruijie Cloud. Choose **Project** > **Configuration** > **Devices** > **Wireless** > **Radio** and select a network in this account. Set parameters in the **Radio settings** area and **Manual Planning** area.

- **Radio settings**

  Configures parameters in the **Radio settings** area. After configuration, click **Save**.



Radio settings

Country or Region: America(US)

RF1(2.4G) Default Channel Width : 20MHz

RF2(5G) Default Channel Width : 40MHz

RF3(5G) Default Channel Width : 40MHz

Country or Region: Select a country code.

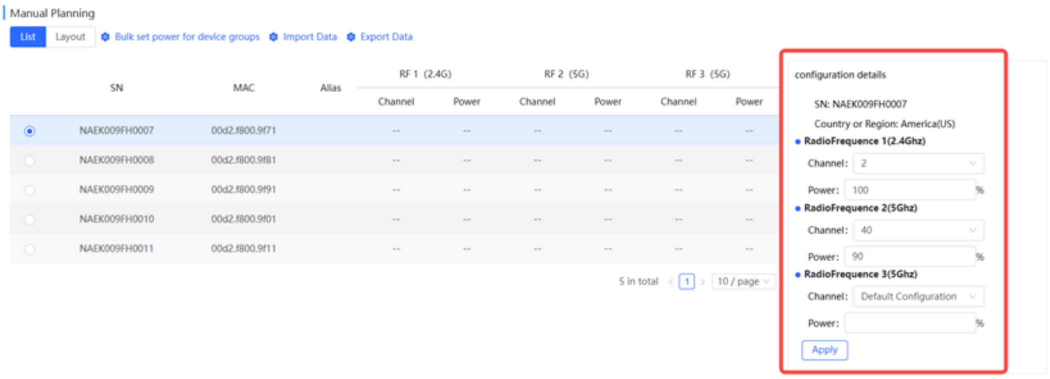
RF1(2.4G) Default Channel Width: Configure the default channel width of RF1.

RF2(5G) Default Channel Width: Configure the default channel width of RF2.

RF3(5G) Default Channel Width: Configure the default channel width of RF3.

- **Manual Planning**

  - Configure a single device: Select an AP and configure the channel and power of radios. After configuration, click **Apply**.



Manual Planning

	SN	MAC	Alias	RF 1 (2.4G)		RF 2 (5G)		RF 3 (5G)	
				Channel	Power	Channel	Power	Channel	Power
●	NAEK009FH0007	00d2.f800.9f71		--	--	--	--	--	--
○	NAEK009FH0008	00d2.f800.9f81		--	--	--	--	--	--
○	NAEK009FH0009	00d2.f800.9f91		--	--	--	--	--	--
○	NAEK009FH0010	00d2.f800.9f01		--	--	--	--	--	--
○	NAEK009FH0011	00d2.f800.9f11		--	--	--	--	--	--

5 in total < 1 > 10 / page

configuration details

SN: NAEK009FH0007

Country or Region: America(US)

- **RadioFrequence 1(2.4Ghz)**

Channel: 2

Power: 100 %

- **RadioFrequence 2(5Ghz)**

Channel: 40

Power: 90 %

- **RadioFrequence 3(5Ghz)**

Channel: Default Configuration

Power: %

SN: indicates the SN of an AP.

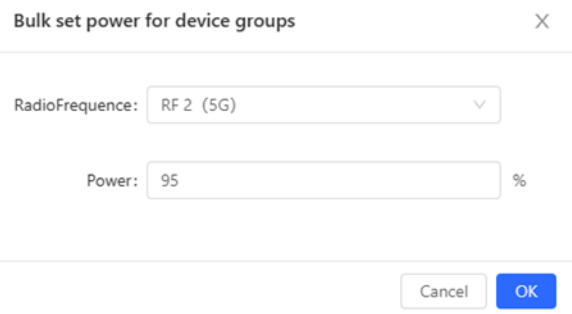
MAC: indicates the MAC address of an AP.

Device Name: indicates the AP name.

RadioFrequence > **Channel**: Check the current channel of radios.

RadioFrequence > **Power**: Check the local power of radios.

- Bulk configure devices (all devices) in a band: Click **Bulk set power for device groups**, select a band, and configure power. After configuration, click **OK**.

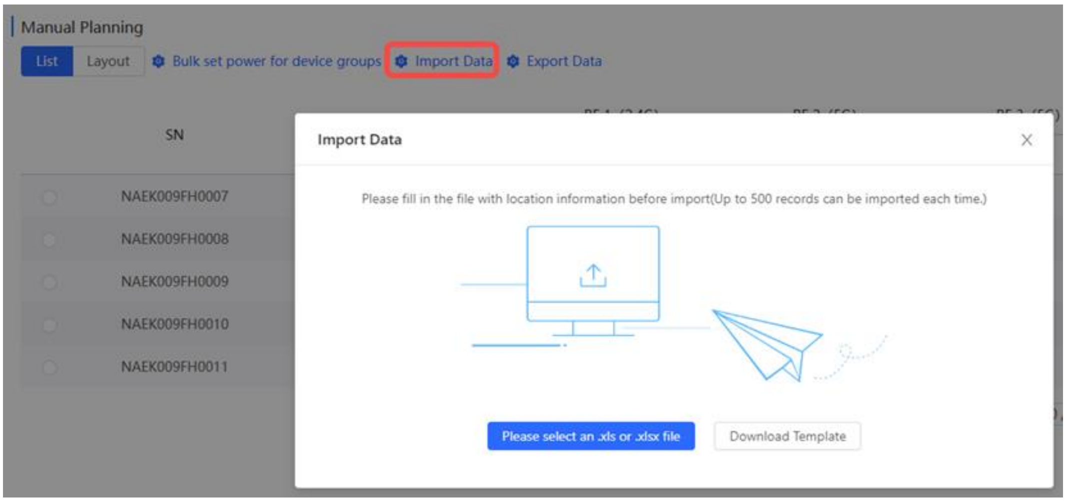


Bulk set power for device groups

RadioFrequence: RF 2 (5G)

Power: 95 %

- Bulk configure devices (specified devices) in multiple bands: Click **Import Data** to go to the configuration import page. Click **Download Template** to download the template and fill in the template (SN is mandatory). After filling, save the file and click **Please select an .xls or .xlsx file** to complete configuration import.

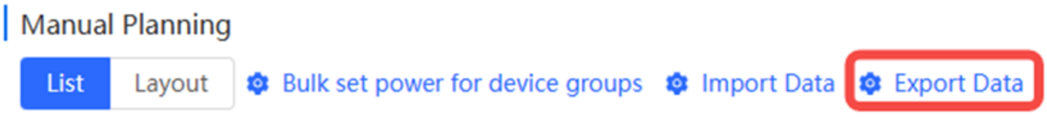


Manual Planning

Import Data

Please fill in the file with location information before import(Up to 500 records can be imported each time.)

- Export current configuration: Click **Export Data** to export configuration data to an .xlsx file.



10.4 Roaming

10.4.1 L2 L3 Roaming

Overview

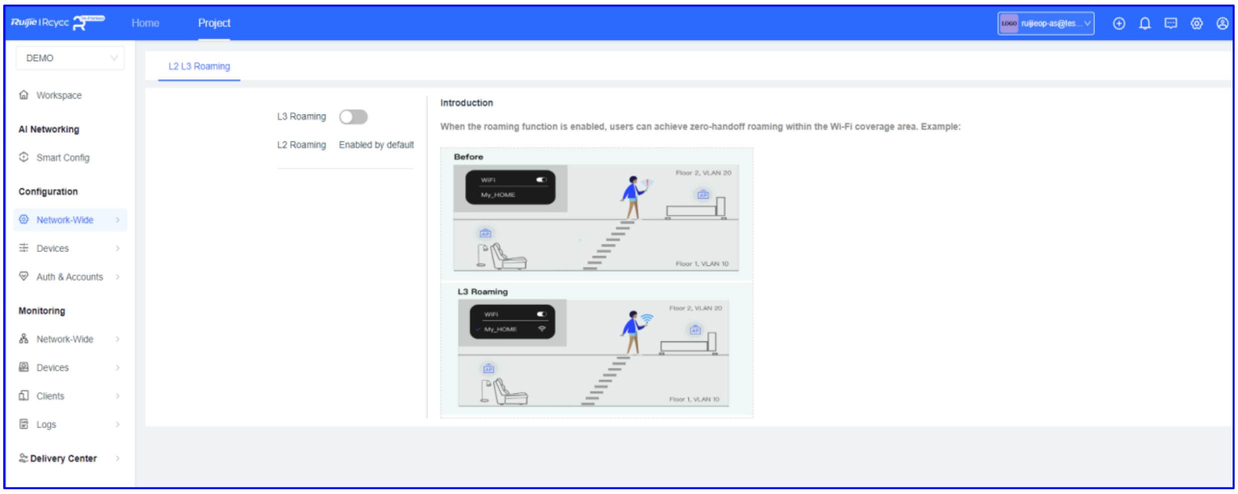
The roaming function on Ruijie Cloud allows a STA from to roam from AP-1 to subnet B of AP-2 seamlessly. You can enable **L3 Roaming** on the **L2 L3 Roaming** page. **L2 Roaming** is enabled by default.

If the sub project uses the same wireless configuration of current project, its L3 Roaming will be enabled at the same time.

Configuration Steps

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Roaming**, and select a network in this account.

(2) On the **L2 L3 Roaming** tab, enable **L3 Roaming**.



L3 Roaming ○

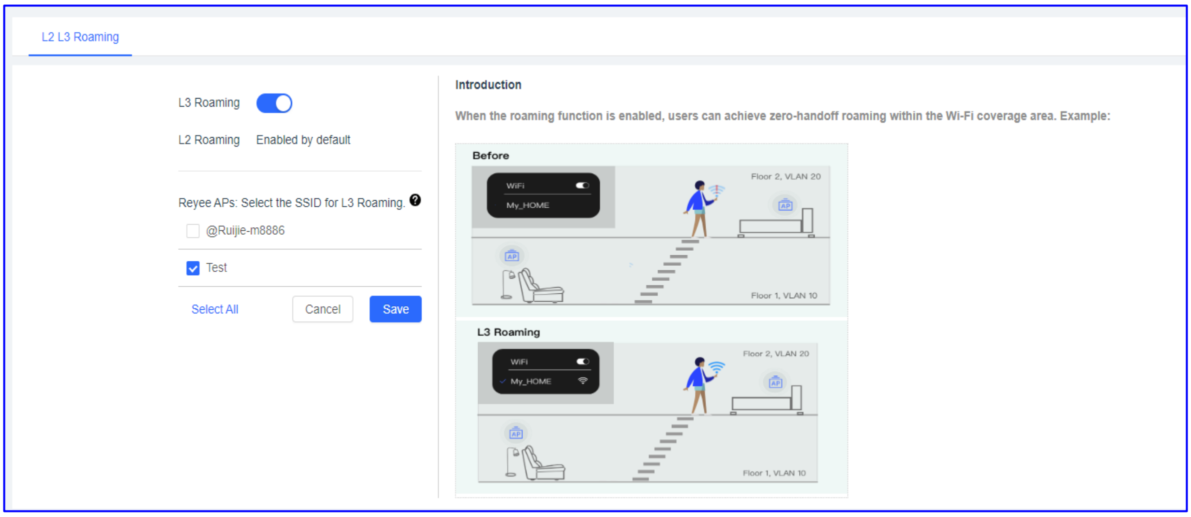
L2 Roaming Enabled by default

Introduction

When the roaming function is enabled, users can achieve zero-handoff roaming within the Wi-Fi coverage area. Example:

(3) If you have completed SSID configuration, select the SSID for L3 Roaming and click **Save**.

(4) After enabling Layer 3 roaming, choose **MONITORING** > **Devices** > **AP**, select a device, and click **Web CLI**. Enter the **Roaming Group Neighbor** command to check roaming group neighbors.



L2 L3 Roaming

L3 Roaming ●

L2 Roaming Enabled by default

Reyee APs: Select the SSID for L3 Roaming.

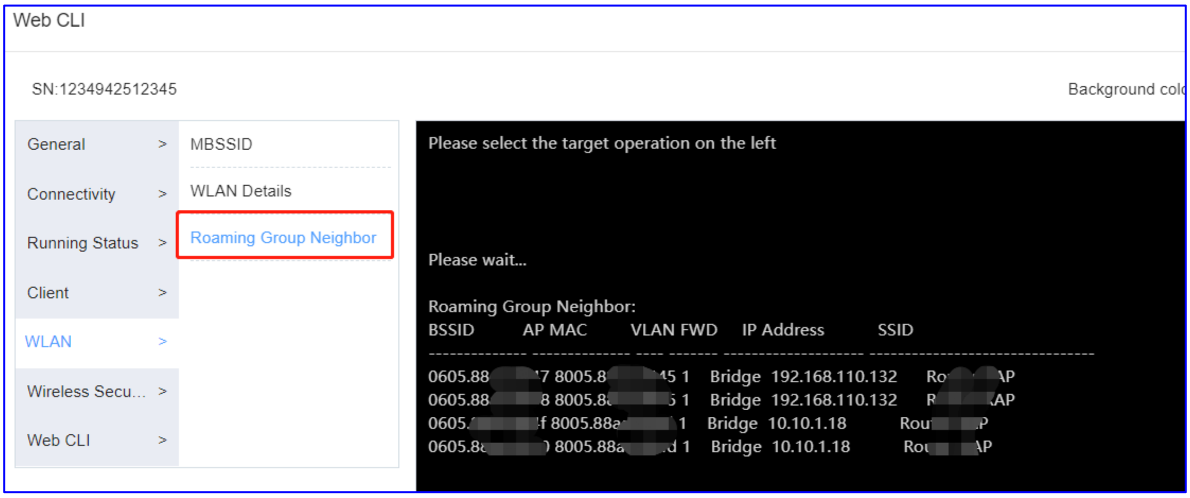
□ @Ruijie-m8886

☑ Test

Select All | Cancel | Save

Introduction

When the roaming function is enabled, users can achieve zero-handoff roaming within the Wi-Fi coverage area. Example:



Web CLI

SN:1234942512345

Background colo

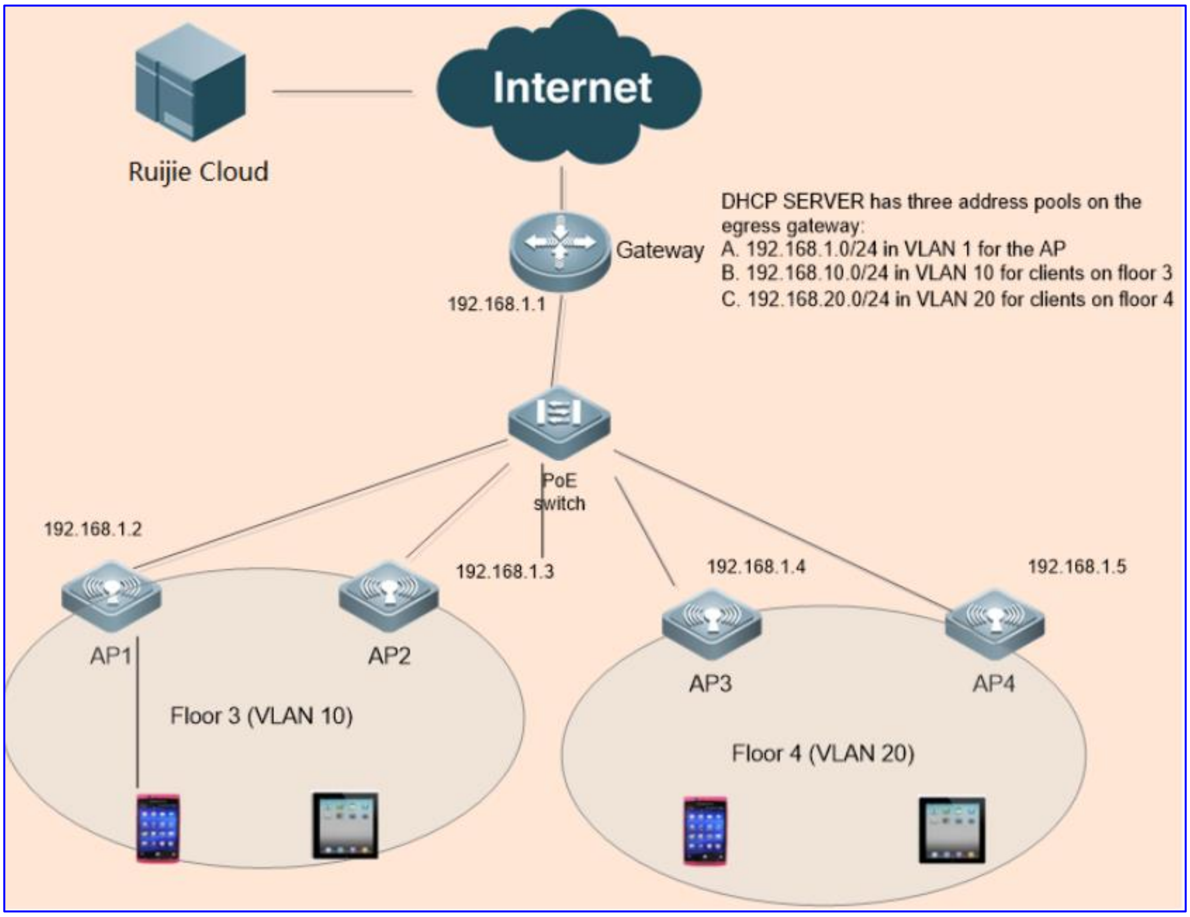
```
Please select the target operation on the left



Please wait...

Roaming Group Neighbor:
BSSID          AP MAC          VLAN FWD   IP Address        SSID
-------------- -------------- ---- ------- ------------------ ------------------------------
0605.88[redacted]7 8005.8[redacted]45 1   Bridge  192.168.110.132    Ro[redacted]AP
0605.88[redacted]8 8005.8[redacted]5 1    Bridge  192.168.110.132    R[redacted]AP
0605.[redacted]f 8005.88a[redacted] 1    Bridge  10.10.1.18        Rou[redacted]P
0605.8[redacted]) 8005.88a[redacted]d 1   Bridge  10.10.1.18        Ro[redacted]AP
```

Layer 3 Roaming Scenario

Scenario

To deploy a network for a new branch, a Wi-Fi network named **SSID-FREE** is provided for external personnel for free. The WLANs for clients on floor 3 and floor 4 are assigned to VLAN 10 and VLAN 20, respectively. The roaming function is supported, and the uplink and downlink rates of all clients are limited to 100 kbit/s.

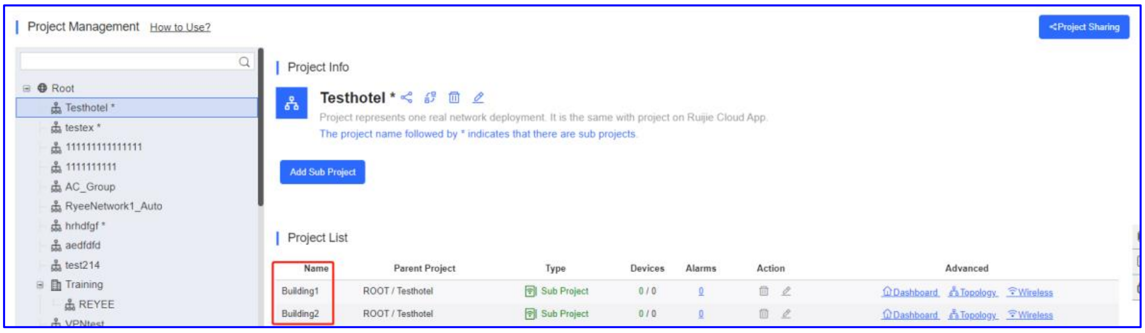
Topology



DHCP SERVER has three address pools on the egress gateway:
A. 192.168.1.0/24 in VLAN 1 for the AP
B. 192.168.10.0/24 in VLAN 10 for clients on floor 3
C. 192.168.20.0/24 in VLAN 20 for clients on floor 4

Configuration

(1) Add two sub-projects under the same project.



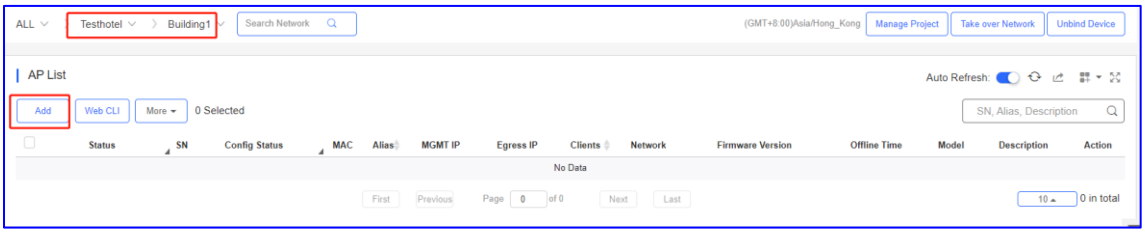
Testhotel *

Project represents one real network deployment. It is the same with project on Ruijie Cloud App.

The project name followed by * indicates that there are sub projects.

Name	Parent Project	Type	Devices	Alarms	Action	Advanced
Building1	ROOT / Testhotel	Sub Project	0 / 0	0		Dashboard Topology Wireless
Building2	ROOT / Testhotel	Sub Project	0 / 0	0		Dashboard Topology Wireless

(2) Add AP1 and AP2 to Building1.



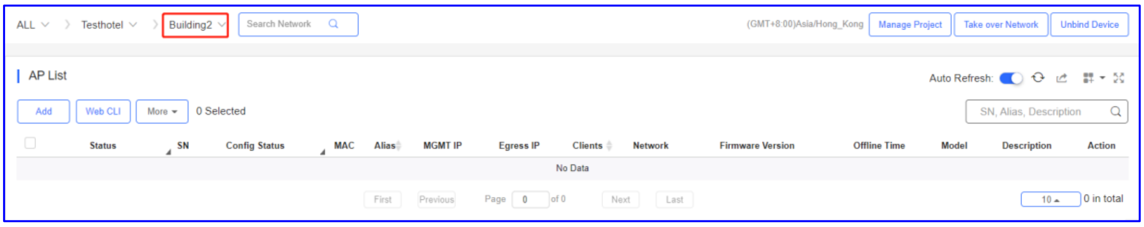
0 Selected

Status	SN	Config Status	MAC	Alias	MGMT IP	Egress IP	Clients	Network	Firmware Version	Offline Time	Model	Description	Action
No Data													

Page 0 of 0

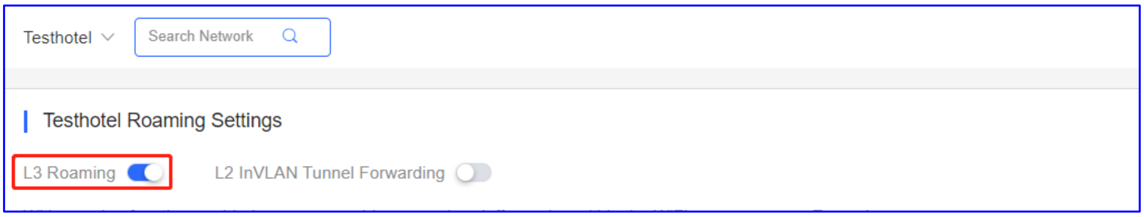
10 0 in total

(3) Add AP3 and AP4 to Building2.



Status	SN	Config Status	MAC	Alias	MGMT IP	Egress IP	Clients	Network	Firmware Version	Offline Time	Model	Description	Action
No Data													

(4) Enable L3 Roaming.

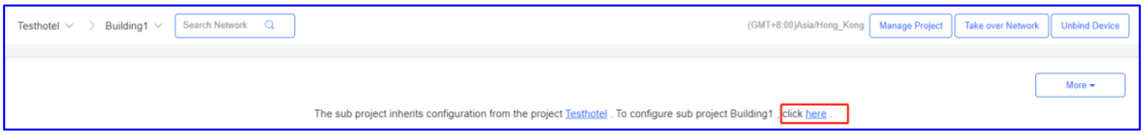


Testhotel Roaming Settings

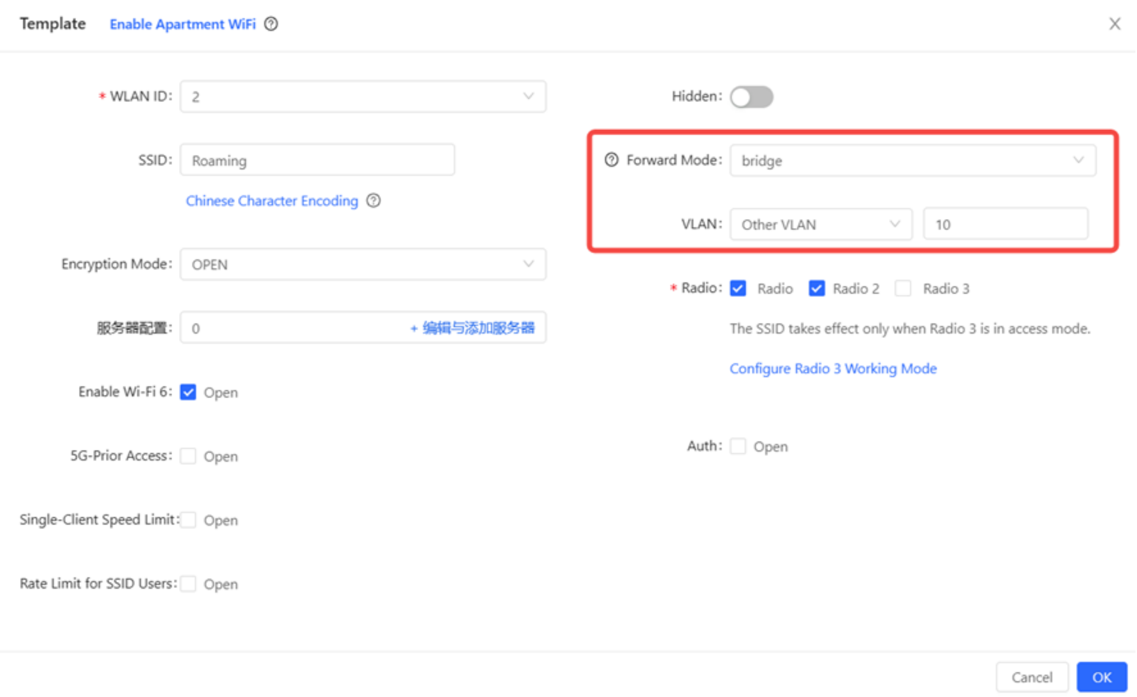
L3 Roaming: on

L2 InVLAN Tunnel Forwarding: off

(5) Configure the SSID for Building1, set **Forward Mode** to **bridge**, and VLAN ID is 10.



The sub project inherits configuration from the project Testhotel . To configure sub project Building1 , click here .



* WLAN ID: 2

SSID: Roaming

Encryption Mode: OPEN

服务器配置: 0

Enable Wi-Fi 6: ☑ Open

5G-Prior Access: □ Open

Single-Client Speed Limit: □ Open

Rate Limit for SSID Users: □ Open

Hidden: off

Forward Mode: bridge

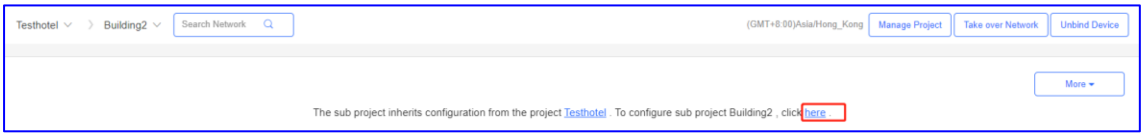
VLAN: Other VLAN 10

* Radio: ☑ Radio ☑ Radio 2 □ Radio 3

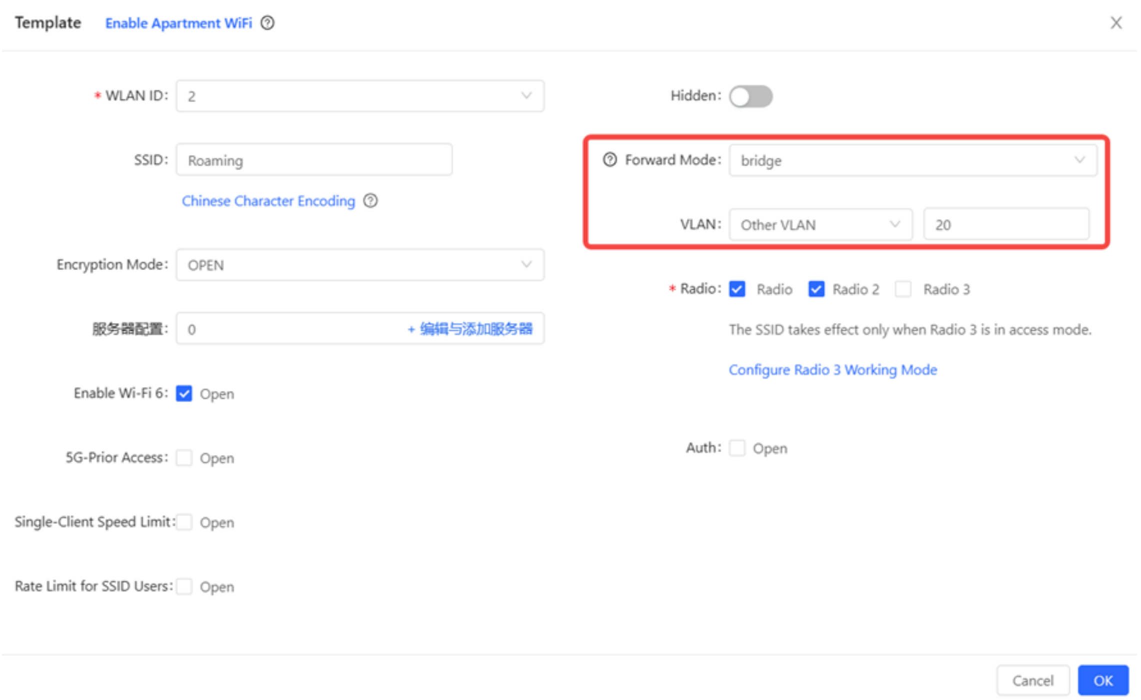
The SSID takes effect only when Radio 3 is in access mode.

Auth: □ Open

(6) Configure the SSID for Building2, set **Forward Mode** to **bridge**, and VLAN ID is 20.



The sub project inherits configuration from the project Testhotel . To configure sub project Building2 , click here .



Template Enable Apartment WiFi ⓘ

* WLAN ID: 2

SSID: Roaming

Chinese Character Encoding ⓘ

Encryption Mode: OPEN

服务器配置: 0 + 编辑与添加服务器

Enable Wi-Fi 6: ☑ Open

5G-Prior Access: □ Open

Single-Client Speed Limit: □ Open

Rate Limit for SSID Users: □ Open

Hidden:

ⓘ Forward Mode: bridge

VLAN: Other VLAN 20

* Radio: ☑ Radio ☑ Radio 2 □ Radio 3

The SSID takes effect only when Radio 3 is in access mode.

Configure Radio 3 Working Mode

Auth: □ Open

(7) Confirm that APs are online.

(8) Configure the gateway.

AP address pool: 192.168.1.0/24.

Client address pool of **Building 1**: 192.168.10.0/24; gateway: 192.168.10.1; VLAN: 10

Client address pool of **Building 2**: 192.168.20.0/24; gateway: 192.168.20.1; VLAN: 20

(9) Configure the PoE switch.

On the port through which the PoE switch is connected to the AP, configure a trunk port with the native ID set to 1 by default, and add VLANs 10 and 20.

Verification

Connect a mobile phone to the Wi-Fi network properly for Internet access.

Connect a mobile phone to the SSID: **Roaming**, and go upstairs from **Building1** to **Building2**. Reconnection and Internet access failures do not occur.

10.5 Rate Limit

10.5.1 Overview

It supports User Rate Limit, Wireless Rate Limit, AP Rate Limit, and Packet Rate Limit. If multiple rate limit modes are configured for one client, their priorities are as follows: **User Rate Limit** > **Wireless Rate Limit** > **AP Rate Limit**.

- User Rate Limit: You can configure wireless STA-based rate limit to limit or guarantee the required bandwidth for specific STAs. The maximum number of supported rules is 512 users.
- Wireless Rate Limit: You can configure per-user rate limit, dynamic rate limit, and other functions for designated SSIDs.
  - Per-user rate limit indicates that all STAs associated with the SSID equally share the rate limit.

  - All-user rate limit indicates that all STAs associated with the SSID equally share the configured rate limit.

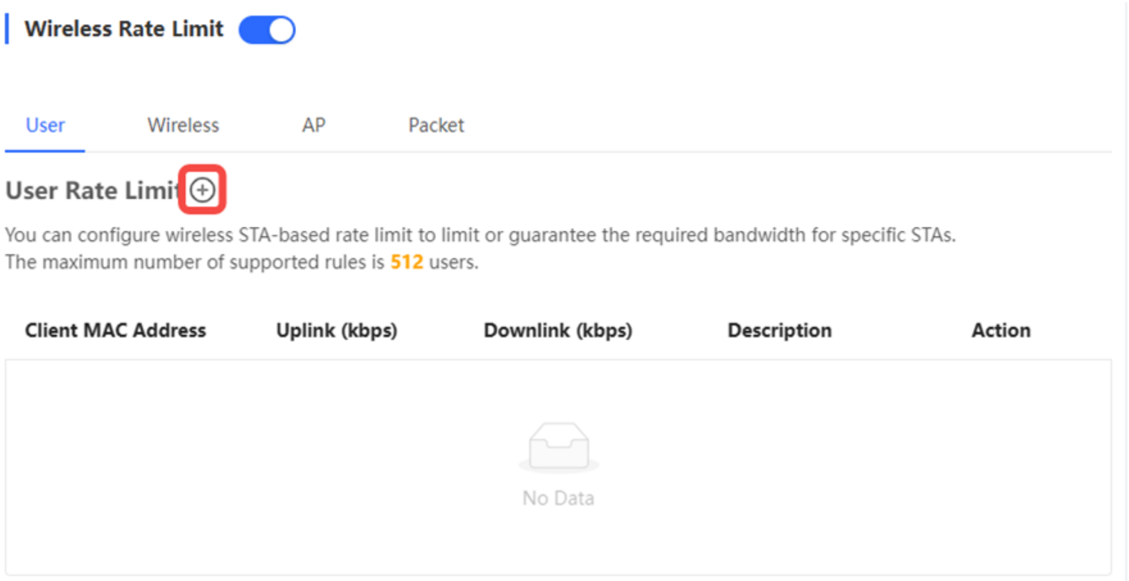
- AP Rate Limit: You can use this function to configure network-wide client rate limit. All clients on the network will share the configured rate limit.
- Packet Rate Limit: You can use this function to set downlink rate limit for broadcast and multicast packets. If the Internet is frozen without heavy traffic during normal use, you are advised to adjust the rate between 1 kbit/s and 512 kbit/s. A lower rate ensures better Internet experience.

10.5.2 User Rate Limit

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Rate Limit**, and select a network in this account.

(2) Confirm that **Wireless Rate Limit** (enabled by default) is enabled.

(3) On the **User** tab, click ⊕ to go to the configuration page.

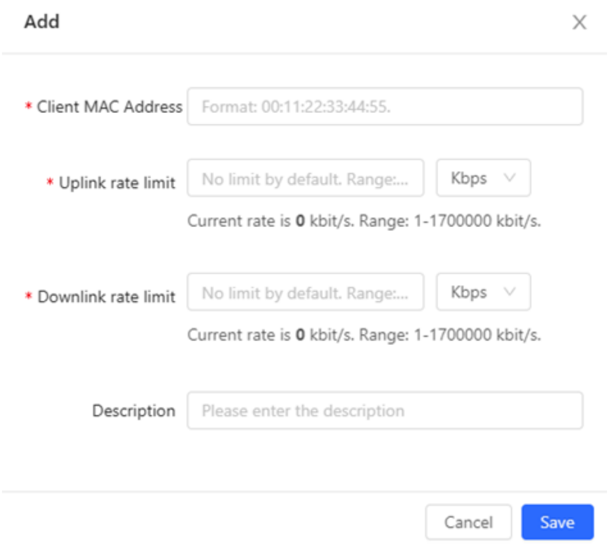


You can configure wireless STA-based rate limit to limit or guarantee the required bandwidth for specific STAs.
The maximum number of supported rules is 512 users.

Client MAC Address	Uplink (kbps)	Downlink (kbps)	Description	Action

No Data

(4) Configure the MAC address of the client whose rate needs to be limited and the rate limit value. After configuration, click **Save**.



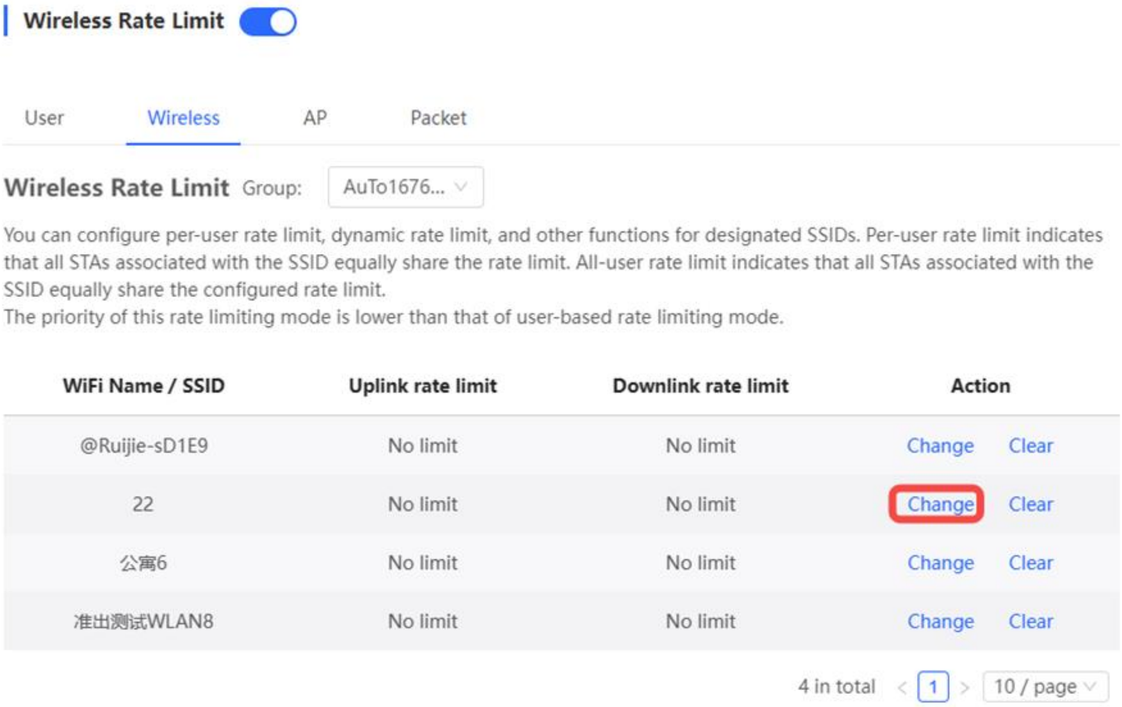
* Client MAC Address	Format: 00:11:22:33:44:55.
* Uplink rate limit	No limit by default. Range:... Kbps Current rate is 0 kbit/s. Range: 1-1700000 kbit/s.
* Downlink rate limit	No limit by default. Range:... Kbps Current rate is 0 kbit/s. Range: 1-1700000 kbit/s.
Description	Please enter the description

10.5.3 Wireless Rate Limit

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Rate Limit**, and select a network in this account.

(2) Confirm that **Wireless Rate Limit** (enabled by default) is enabled.

(3) On the **Wireless** tab, select the Wi-Fi service whose rate needs to be limited and click **Change** in the **Action** column to go to the configuration page.

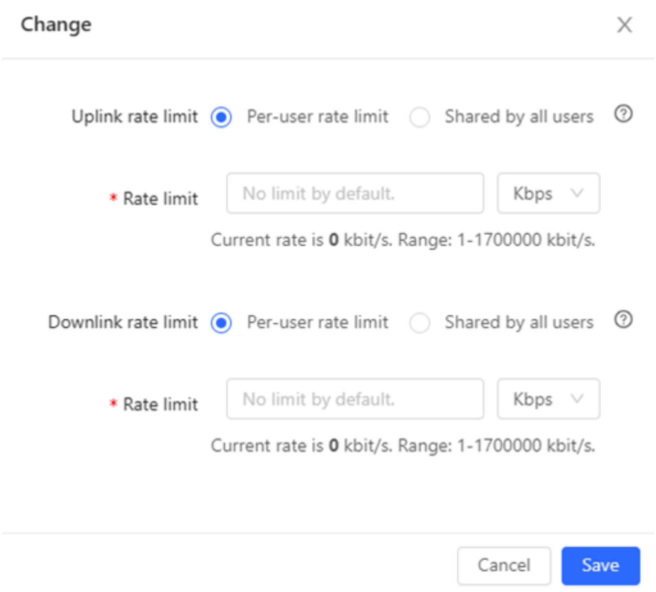


Wireless Rate Limit Group: AuTo1676...

You can configure per-user rate limit, dynamic rate limit, and other functions for designated SSIDs. Per-user rate limit indicates that all STAs associated with the SSID equally share the rate limit. All-user rate limit indicates that all STAs associated with the SSID equally share the configured rate limit.
The priority of this rate limiting mode is lower than that of user-based rate limiting mode.

WiFi Name / SSID	Uplink rate limit	Downlink rate limit	Action
@Ruijie-sD1E9	No limit	No limit	Change Clear
22	No limit	No limit	Change Clear
公寓6	No limit	No limit	Change Clear
准出测试WLAN8	No limit	No limit	Change Clear

(4) Configure the rate limit modes for the uplink and downlink directions and rate limit values. After configuration, click **Save**.



Uplink rate limit ● Per-user rate limit ○ Shared by all users

* Rate limit No limit by default. Kbps

Current rate is **0** kbit/s. Range: 1-1700000 kbit/s.

Downlink rate limit ● Per-user rate limit ○ Shared by all users

* Rate limit No limit by default. Kbps

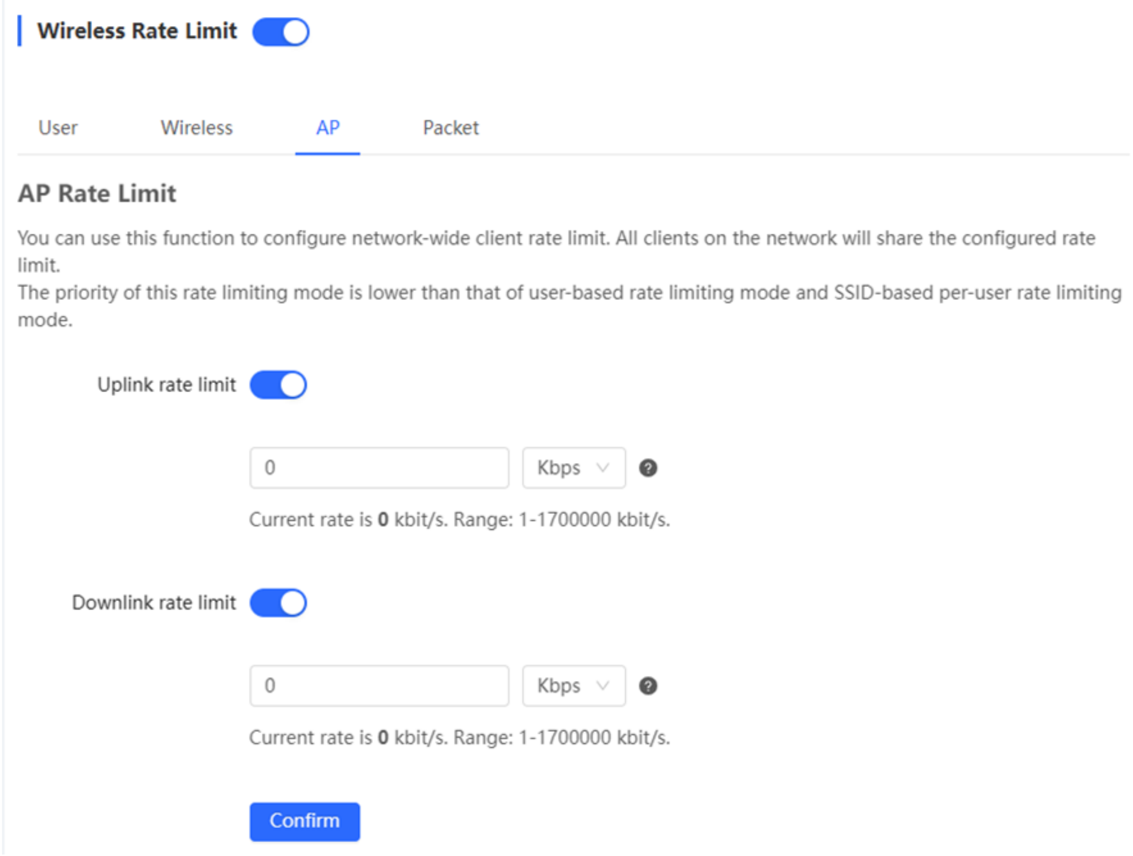
Current rate is **0** kbit/s. Range: 1-1700000 kbit/s.

10.5.4 AP Rate Limit

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Rate Limit**, and select a network in this account.

(2) Confirm that **Wireless Rate Limit** (enabled by default) is enabled.

(3) On the **AP** tab, enable the uplink and downlink rate limit functions and configure the rate limit values. After configuration, click **Confirm**.



Wireless Rate Limit ●

AP Rate Limit

You can use this function to configure network-wide client rate limit. All clients on the network will share the configured rate limit.
The priority of this rate limiting mode is lower than that of user-based rate limiting mode and SSID-based per-user rate limiting mode.

Uplink rate limit ●

0 Kbps

Current rate is **0** kbit/s. Range: 1-1700000 kbit/s.

Downlink rate limit ●

0 Kbps

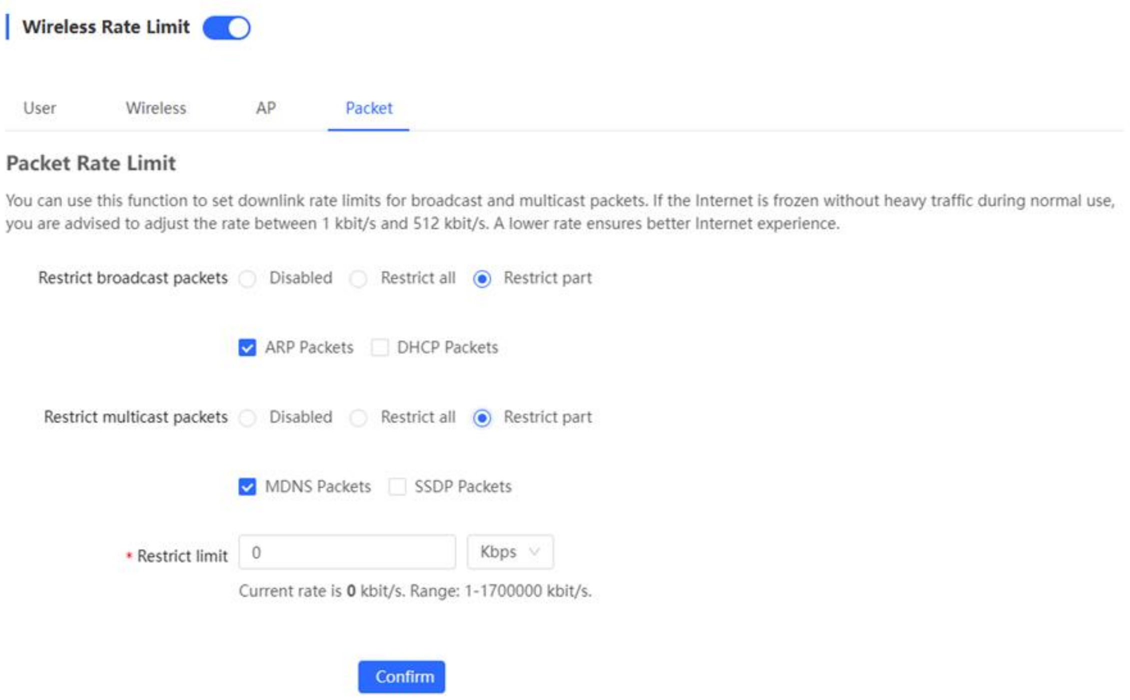
Current rate is **0** kbit/s. Range: 1-1700000 kbit/s.

10.5.5 Packet Rate Limit

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Rate Limit**, and select a network in this account.

(2) Confirm that **Wireless Rate Limit** (enabled by default) is enabled.

(3) On the **Packet** tab, select the type of broadcast/multicast packets whose rate needs to be limited, and configure the rate limit value. After configuration, click **Confirm**.



Wireless Rate Limit

Packet Rate Limit

You can use this function to set downlink rate limits for broadcast and multicast packets. If the Internet is frozen without heavy traffic during normal use, you are advised to adjust the rate between 1 kbit/s and 512 kbit/s. A lower rate ensures better Internet experience.

Restrict broadcast packets ○ Disabled ○ Restrict all ● Restrict part

☑ ARP Packets □ DHCP Packets

Restrict multicast packets ○ Disabled ○ Restrict all ● Restrict part

☑ MDNS Packets □ SSDP Packets

* Restrict limit 0 Kbps

Current rate is **0** kbit/s. Range: 1-1700000 kbit/s.

10.6 Load Balancing

Overview

Load balancing ensures that clients are evenly distributed across member APs, thereby using resources efficiently.

Load balancing can be achieved by assigning all the APs in the same area to the same load balancing group to control the access of wireless clients. For example, there are 15 clients associated with AP1, 10 associated with AP2, and the current threshold configured is 2. The client different between the two APs is 5, which is greater than the threshold. Therefore, subsequent users will be associated with AP2.

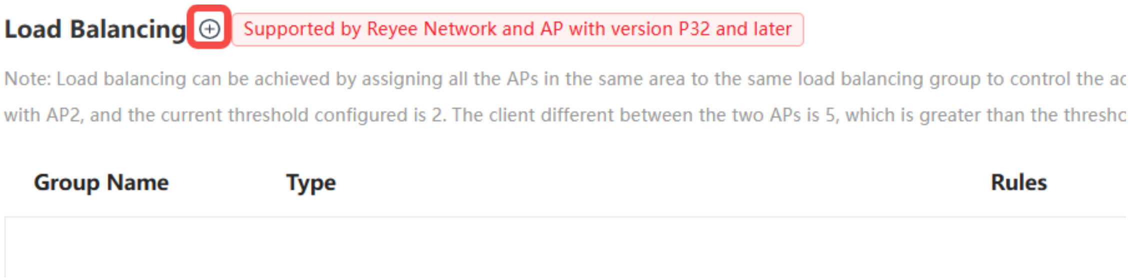
Limitations

Load balancing is supported by Reyee Network and AP with P32 or a higher version, and there must be a Reyee EG on the network.

Procedure

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Load Balancing**, and select a network in this account.

(2) Click ⊕ to add a load balancing group.

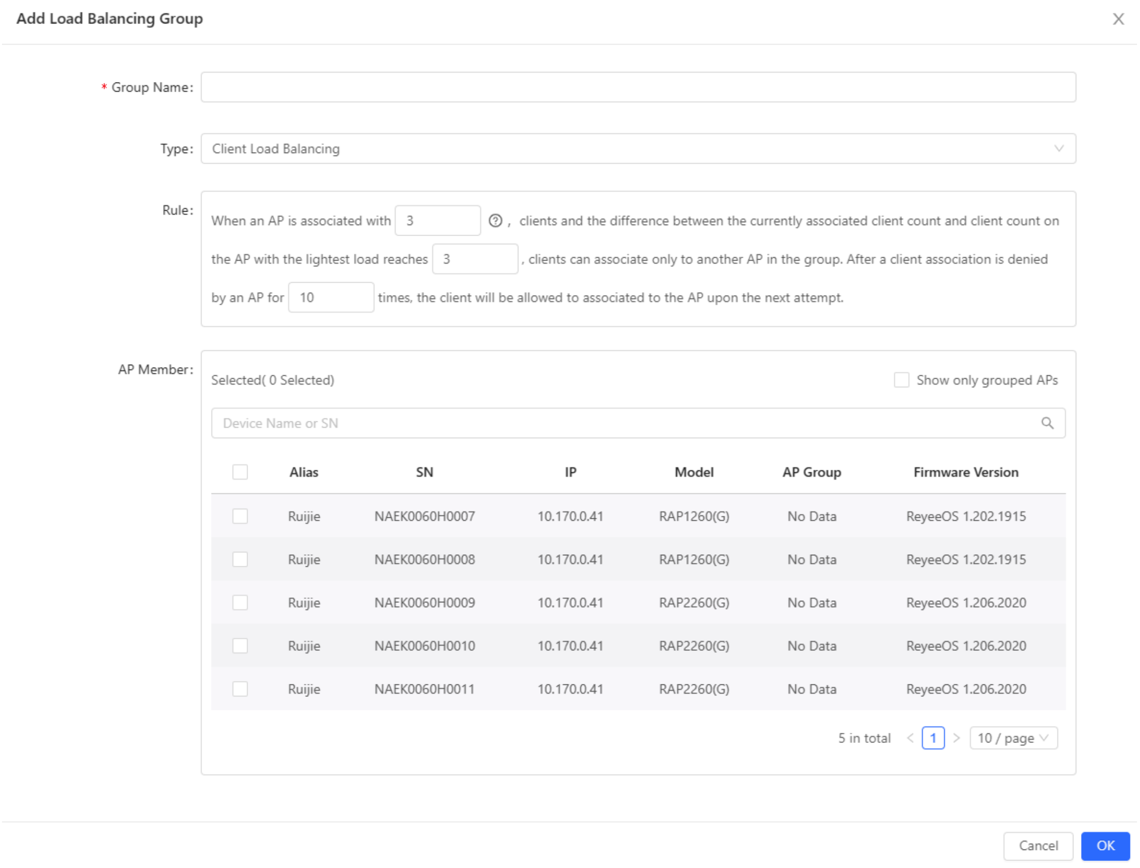


Load Balancing ⊕ Supported by Reyee Network and AP with version P32 and later

Note: Load balancing can be achieved by assigning all the APs in the same area to the same load balancing group to control the ac
with AP2, and the current threshold configured is 2. The client different between the two APs is 5, which is greater than the threshc

Group Name	Type	Rules

(3) Configure parameters for the load balancing group, including **Group Name**, **Type**, **Rule**, and **AP Member**. After configuration, click **OK**.



Add Load Balancing Group

* Group Name:

Type: Client Load Balancing

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

AP Member: Selected(0 Selected) □ Show only grouped APs

Device Name or SN

□	Alias	SN	IP	Model	AP Group	Firmware Version
□	Ruijie	NAEK0060H0007	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915
□	Ruijie	NAEK0060H0008	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915
□	Ruijie	NAEK0060H0009	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020
□	Ruijie	NAEK0060H0010	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020
□	Ruijie	NAEK0060H0011	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020

Group Name: indicates the load balance group name.

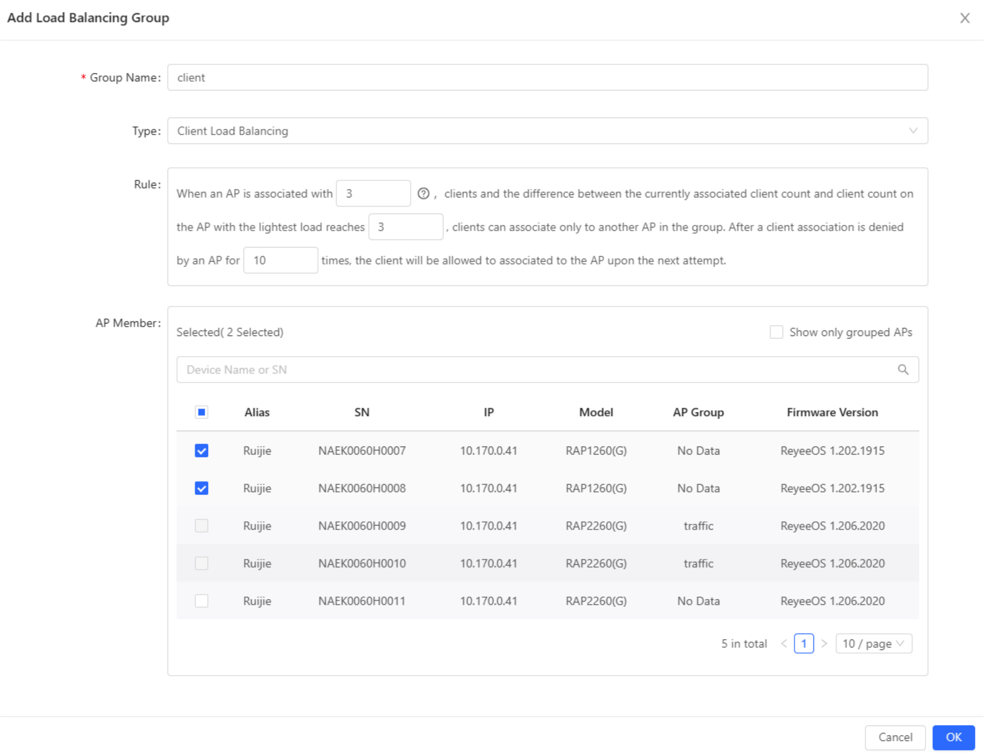
Type: indicates the type of load balancing (client or traffic).

Rule: indicates the rule of load balancing group.

AP Member: indicates the AP added to the group.

Implementation of client and traffic load balancing are as follows:

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



Add Load Balancing Group

* Group Name: client

Type: Client Load Balancing

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

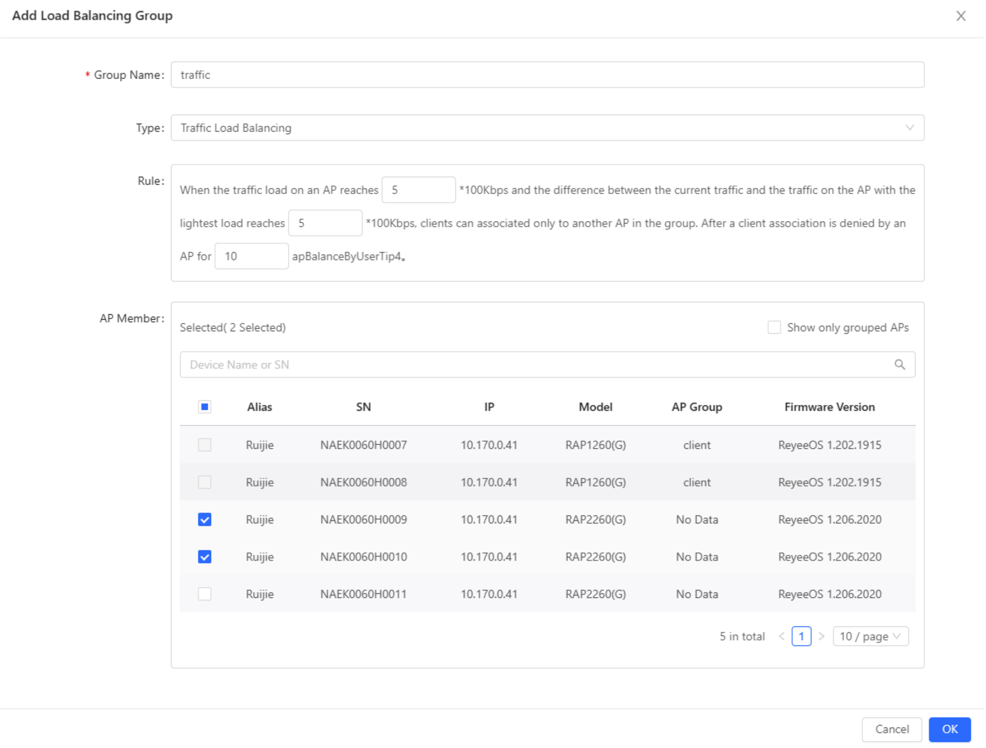
AP Member: Selected(2 Selected) □ Show only grouped APs

Device Name or SN

■	Alias	SN	IP	Model	AP Group	Firmware Version
☑	Ruijie	NAEK0060H0007	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915
☑	Ruijie	NAEK0060H0008	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915
□	Ruijie	NAEK0060H0009	10.170.0.41	RAP2260(G)	traffic	ReyeeOS 1.206.2020
□	Ruijie	NAEK0060H0010	10.170.0.41	RAP2260(G)	traffic	ReyeeOS 1.206.2020
□	Ruijie	NAEK0060H0011	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020

5 in total < 1 > 10 / page

- **Traffic Load Balancing**: When the traffic load on an AP reaches *n* multiplied by 100 kbit/s and the difference between the current traffic and the traffic on the AP with the lightest load reaches *n* multiplied by 100 kbit/s, clients can be associated only with another AP in the group. After a client association is denied by an AP for *n* times, the client will be allowed to be associated with the AP upon the next attempt.



Add Load Balancing Group

* Group Name: traffic

Type: Traffic Load Balancing

Rule: When the traffic load on an AP reaches 5 *100Kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches 5 *100Kbps, clients can associated only to another AP in the group. After a client association is denied by an AP for 10 apBalanceByUserTip4。

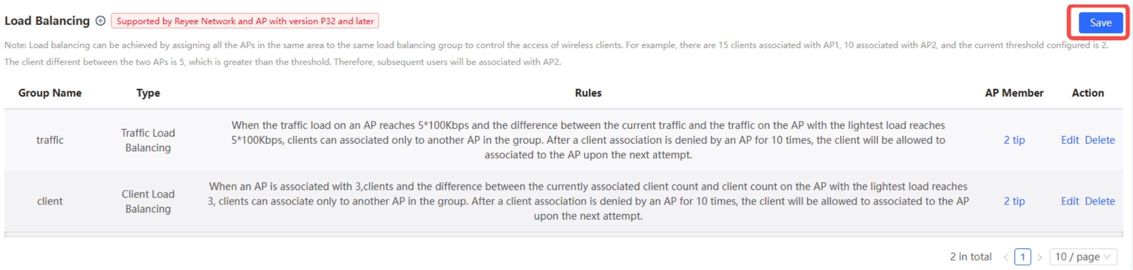
AP Member: Selected(2 Selected) □ Show only grouped APs

Device Name or SN

■	Alias	SN	IP	Model	AP Group	Firmware Version
□	Ruijie	NAEK0060H0007	10.170.0.41	RAP1260(G)	client	ReyeeOS 1.202.1915
□	Ruijie	NAEK0060H0008	10.170.0.41	RAP1260(G)	client	ReyeeOS 1.202.1915
☑	Ruijie	NAEK0060H0009	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020
☑	Ruijie	NAEK0060H0010	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020
□	Ruijie	NAEK0060H0011	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020

5 in total < 1 > 10 / page

(4) After configuring the load balancing group, click **Save** at the upper right corner of the **Load Balancing** page.



Load Balancing ⓘ Supported by Reyee Network and AP with version P32 and later

Save

Note: Load balancing can be achieved by assigning all the APs in the same area to the same load balancing group to control the access of wireless clients. For example, there are 15 clients associated with AP1, 10 associated with AP2, and the current threshold configured is 2. The client different between the two APs is 5, which is greater than the threshold. Therefore, subsequent users will be associated with AP2.

Group Name	Type	Rules	AP Member	Action
traffic	Traffic Load Balancing	When the traffic load on an AP reaches 5*100Kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches 5*100Kbps, clients can associated only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associated to the AP upon the next attempt.	2 tip	Edit Delete
client	Client Load Balancing	When an AP is associated with 3,clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches 3, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associated to the AP upon the next attempt.	2 tip	Edit Delete

2 in total < 1 > 10 / page

The **Action** column is described as follows:

- **Edit**: Click this button to modify configuration parameters except **Group Name**.
- **Delete**: Click this button to delete a specified load balancing group.

After modifying load balancing group parameters or deleting a load balancing group, click **Save** at the upper right corner.

10.7 Client Blocklist and Allowlist

Overview

The purpose of the **Client Blocklist and Allowlist** feature is to deny/allow wireless clients to access Wi-Fi networks. You can configure the global blocklist and allowlist for all Wi-Fi networks or the blocklist and allowlist for a specified SSID. The blocklist and allowlist feature supports matching the MAC address prefixes (OUIs) of clients.

Client Blocklist: Clients on the blocklist are banned from connecting to Wi-Fi networks and clients not on the blocklist are not restricted.

Client Allowlist: When the allowlist is not empty, only clients in the allowlist are allowed to connect to Wi-Fi networks and those not on the allowlist are banned from connecting to the Wi-Fi networks.

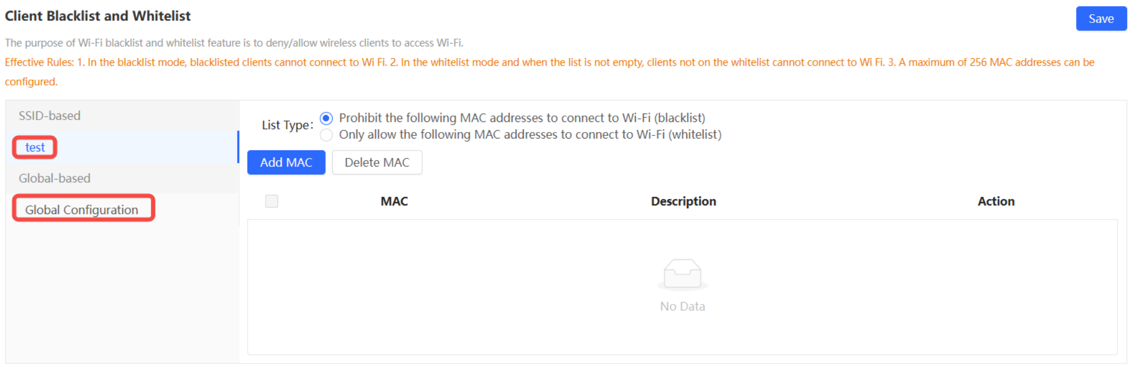
⚠ **Caution**

When the allowlist is empty, the Wi-Fi allowlist does not take effect, that is, all MAC addresses are allowed to connect to Wi-Fi networks.

Configuration Steps

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Client Blocklist and Allowlist**, and select a network in this account.

(2) Select the scope (**SSID-based** or **Global-based**), in which the blocklist or allowlist takes effect, in the list on the left.



Client Blacklist and Whitelist

Save

The purpose of Wi-Fi blacklist and whitelist feature is to deny/allow wireless clients to access Wi-Fi.

Effective Rules: 1. In the blacklist mode, blacklisted clients cannot connect to Wi Fi. 2. In the whitelist mode and when the list is not empty, clients not on the whitelist cannot connect to Wi Fi. 3. A maximum of 256 MAC addresses can be configured.

SSID-based
test
Global-based
Global Configuration

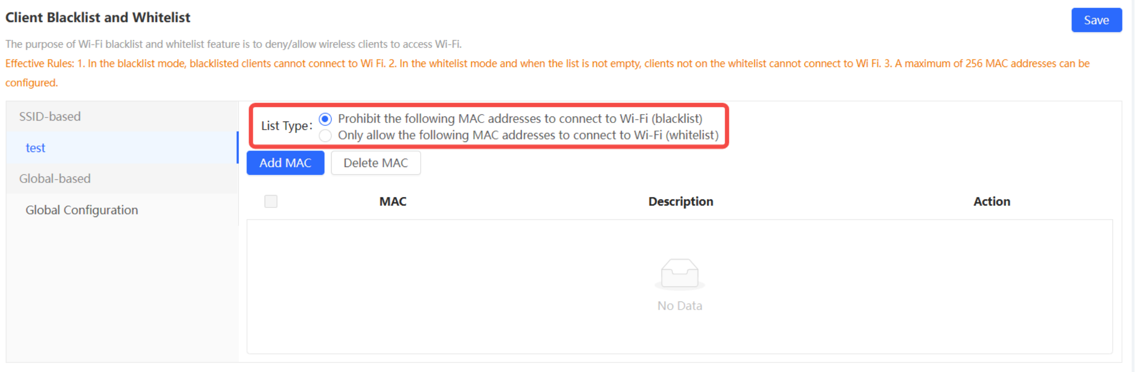
List Type: ● Prohibit the following MAC addresses to connect to Wi-Fi (blacklist)
○ Only allow the following MAC addresses to connect to Wi-Fi (whitelist)

Add MAC Delete MAC

□	MAC	Description	Action

No Data

(3) Select the blocklist/allowlist mode. The default mode is blocklist mode. When you switch the mode, click **OK** in the pop-up prompt box to make the mode take effect.



Client Blacklist and Whitelist

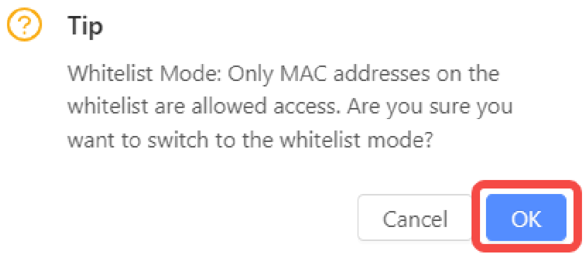
The purpose of Wi-Fi blacklist and whitelist feature is to deny/allow wireless clients to access Wi-Fi.

Effective Rules: 1. In the blacklist mode, blacklisted clients cannot connect to Wi Fi. 2. In the whitelist mode and when the list is not empty, clients not on the whitelist cannot connect to Wi Fi. 3. A maximum of 256 MAC addresses can be configured.

List Type: ● Prohibit the following MAC addresses to connect to Wi-Fi (blacklist)
○ Only allow the following MAC addresses to connect to Wi-Fi (whitelist)

□	MAC	Description	Action

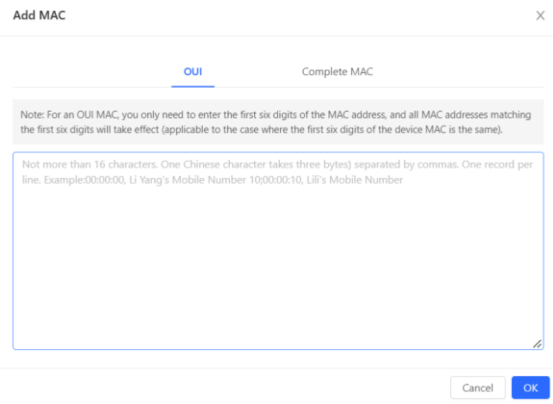
No Data



Tip

Whitelist Mode: Only MAC addresses on the whitelist are allowed access. Are you sure you want to switch to the whitelist mode?

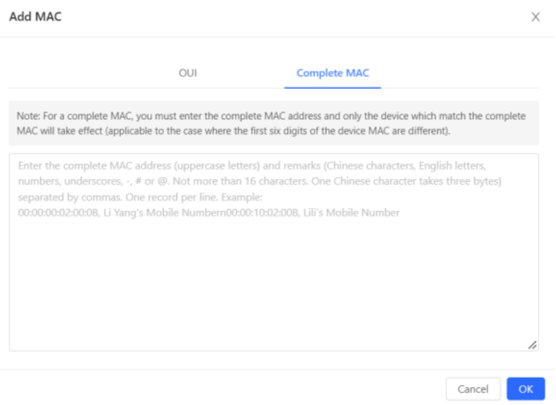
(4) Click **Add MAC**. On the **Add MAC** page, add MAC address prefixes or MAC addresses. After adding, click **OK**.



Add MAC

Note: For an OUI MAC, you only need to enter the first six digits of the MAC address, and all MAC addresses matching the first six digits will take effect (applicable to the case where the first six digits of the device MAC is the same).

Not more than 16 characters. One Chinese character takes three bytes) separated by commas. One record per line. Example:00:00:00, Li Yang's Mobile Number 10;00:00:10, Lili's Mobile Number



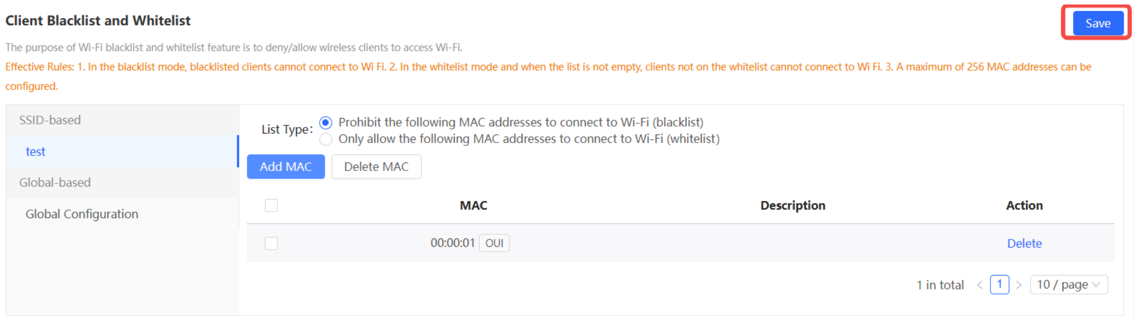
Add MAC

Note: For a complete MAC, you must enter the complete MAC address and only the device which match the complete MAC will take effect (applicable to the case where the first six digits of the device MAC are different).

Enter the complete MAC address (uppercase letters) and remarks (Chinese characters, English letters, numbers, underscores, -, # or @. Not more than 16 characters. One Chinese character takes three bytes) separated by commas. One record per line. Example:
00:00:00:02:00:0B, Li Yang's Mobile Numbern00:00:10:02:00B, Lili's Mobile Number

- OUI: For an OUI MAC, you only need to enter the first six digits of the MAC address, and all MAC addresses matching the first six digits will take effect (applicable to the case where the first six digits of the device MAC is the same).
- Complete MAC: For a complete MAC, you must enter the complete MAC address and only the device which match the complete MAC will take effect (applicable to the case where the first six digits of the device MAC are different).

(5) After completing the blocklist/allowlist configuration, click **Save** at the upper right corner of the **Client Blocklist and Allowlist** page.



Client Blacklist and Whitelist

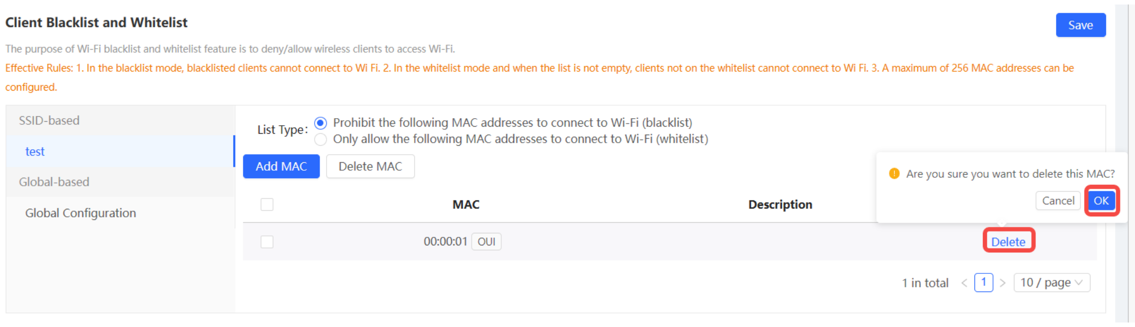
The purpose of Wi-Fi blacklist and whitelist feature is to deny/allow wireless clients to access Wi-Fi.

Effective Rules: 1. In the blacklist mode, blacklisted clients cannot connect to Wi Fi. 2. In the whitelist mode and when the list is not empty, clients not on the whitelist cannot connect to Wi Fi. 3. A maximum of 256 MAC addresses can be configured.

List Type: ● Prohibit the following MAC addresses to connect to Wi-Fi (blacklist) ○ Only allow the following MAC addresses to connect to Wi-Fi (whitelist)

□	MAC	Description	Action
□	00:00:01 OUI		Delete

The **Action** column is described as follows: To delete a rule, click **Delete** in the **Action** column, click **OK** in the pop-up prompt box, and then click **Save** at the upper right corner.



Client Blacklist and Whitelist

The purpose of Wi-Fi blacklist and whitelist feature is to deny/allow wireless clients to access Wi-Fi.

Effective Rules: 1. In the blacklist mode, blacklisted clients cannot connect to Wi Fi. 2. In the whitelist mode and when the list is not empty, clients not on the whitelist cannot connect to Wi Fi. 3. A maximum of 256 MAC addresses can be configured.

List Type: ● Prohibit the following MAC addresses to connect to Wi-Fi (blacklist) ○ Only allow the following MAC addresses to connect to Wi-Fi (whitelist)

Are you sure you want to delete this MAC?

□	MAC	Description	
□	00:00:01 OUI		Delete

10.8 AP VLAN

Overview

This feature can be used to deliver the port VLAN configuration to multiple designated devices.

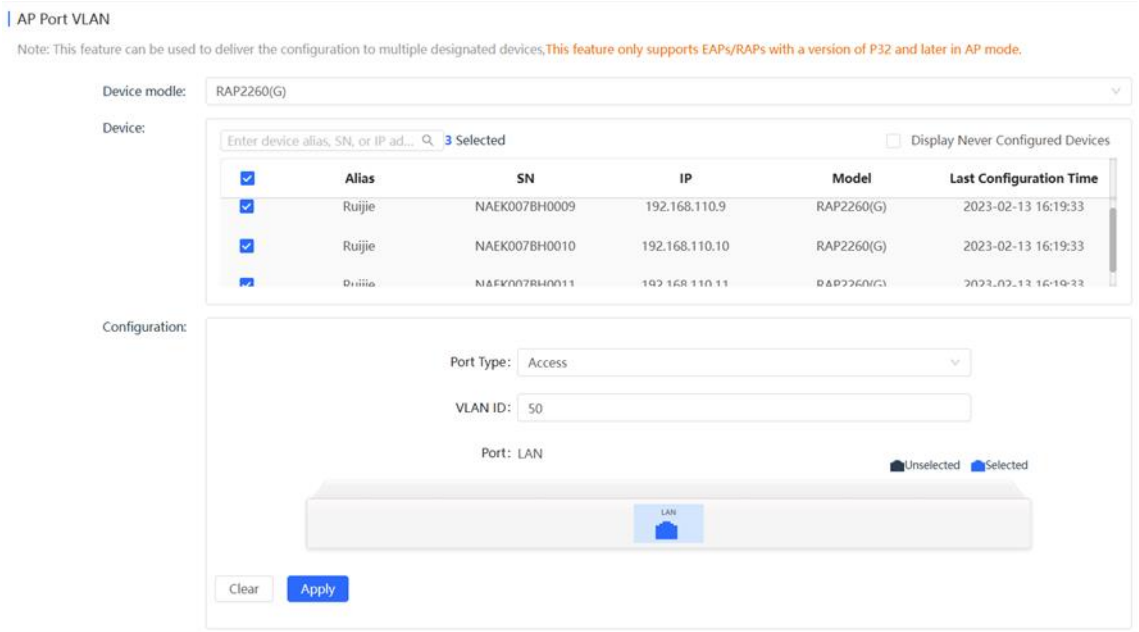
Limitations

This feature only supports EAPs/RAPs with a version of P32 and later in AP mode.

Procedure

(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **AP VLAN**, and select a network in this account.

(2) Set parameters on the **AP Port VLAN** page. After configuration, click **Apply** to deliver the configuration.



AP Port VLAN

Note: This feature can be used to deliver the configuration to multiple designated devices,This feature only supports EAPs/RAPs with a version of P32 and later in AP mode.

Device modle: RAP2260(G)

Device: Enter device alias, SN, or IP ad... 3 Selected □ Display Never Configured Devices

☑	Alias	SN	IP	Model	Last Configuration Time
☑	Ruijie	NAEK007BH0009	192.168.110.9	RAP2260(G)	2023-02-13 16:19:33
☑	Ruijie	NAEK007BH0010	192.168.110.10	RAP2260(G)	2023-02-13 16:19:33
☑	Ruijie	NAEK007BH0011	192.168.110.11	RAP2260(G)	2023-02-13 16:19:33

Configuration:

Port Type: Access

VLAN ID: 50

Port: LAN

Device Model: indicates the AP model.

Device: indicates the device to which the configuration needs to be delivered.

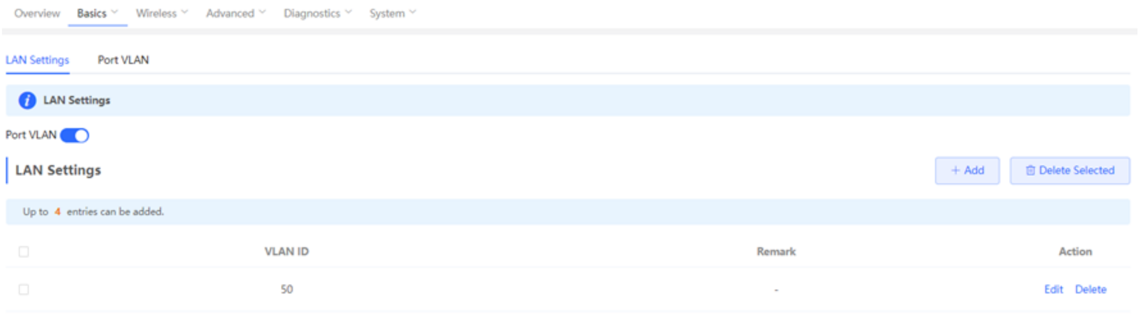
Port Type: indicates the port type, which is access or trunk.

VLAN ID: indicates the VLAN ID of a port.

Selected Ports: Select the port to which the VLAN ID needs to be delivered.

Apply && Clear: Apply the configuration to the device or clear the configuration.

(3) Access the AP's eWeb and check the VLAN ID and port VLAN configuration.



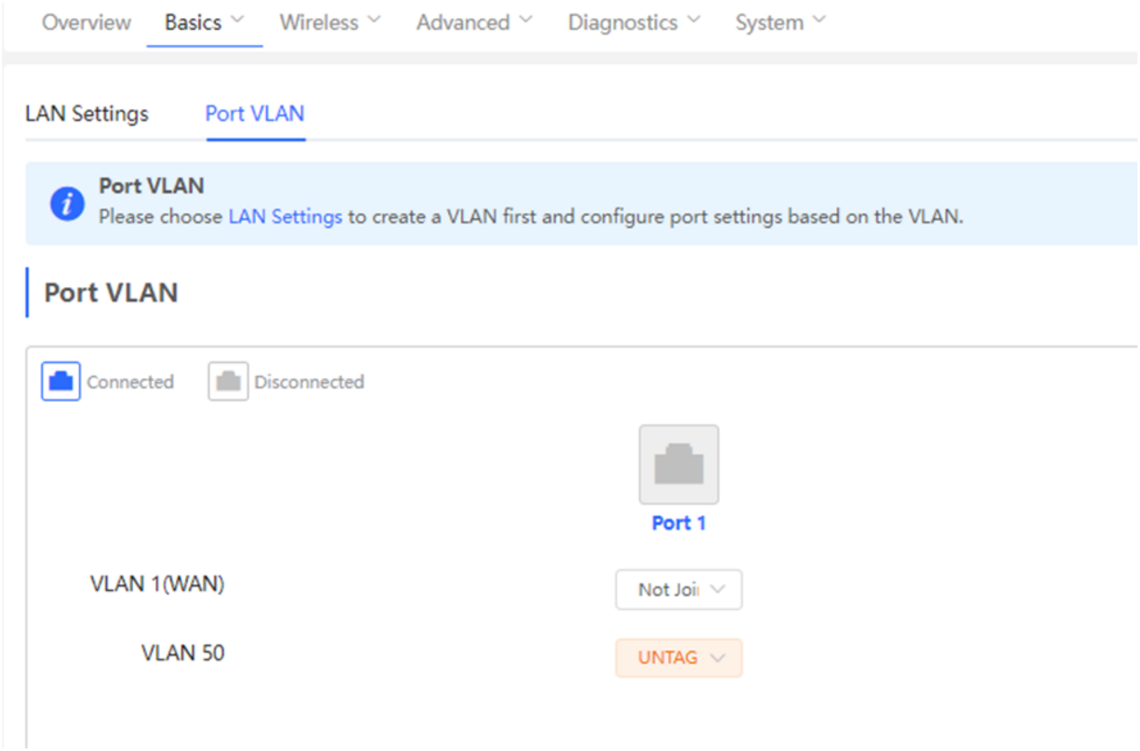
LAN Settings

Port VLAN ●

LAN Settings

Up to 4 entries can be added.

□	VLAN ID	Remark	Action
□	50	-	Edit Delete



Port VLAN

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

Port VLAN

VLAN 1(WAN) Not Joi

VLAN 50 UNTAG

11 Authentication Configuration

11.1 Captive Portal

You can use the Hotspot Policy feature to set authentication policies, including customizing authentication pages, setting authentication network segments, SSID, and other information.

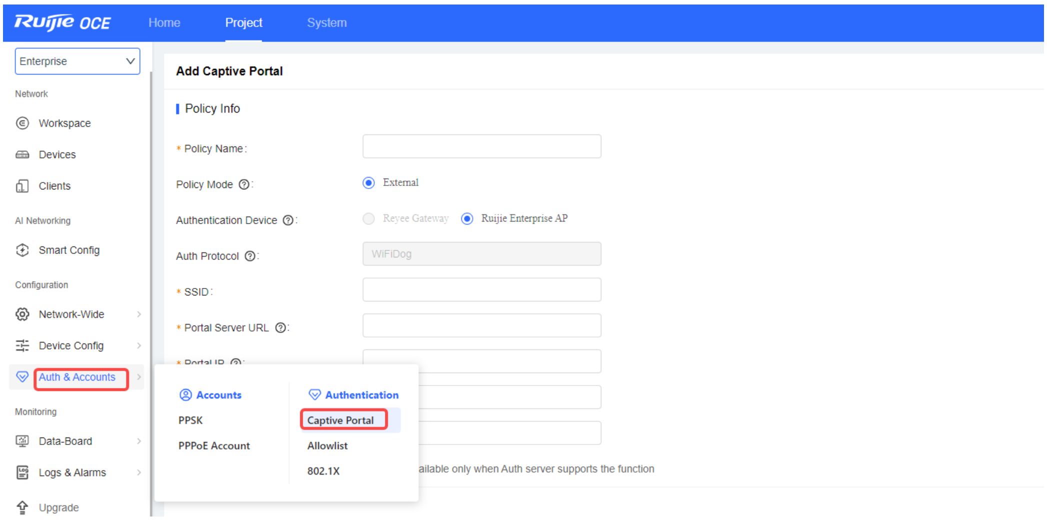
When a user is connected to a wireless or wired network, the system will display a landing or login page that may require authentication, payment, acceptance of an end-user license agreement, acceptable user policy, survey completion, or other valid credentials that both the host and user agree to adhere by.

The network security can be enhanced by configuring the Hotspot policy.

OCE-NM only provide external portal configuration to work with OCE-Identity Manager (IM) to support portal server on local. OCE-IM supports one-click, voucher, account, SMS (integrated with Twilio) authentication modes.

Procedure

(1) Choose **Configuration**> **Auth & Accounts** > **Authentication** > **Captive Portal**.



Add Captive Portal

Policy Info

* Policy Name:

Policy Mode: ● External

Authentication Device: ○ Reyee Gateway ● Ruijie Enterprise AP

Auth Protocol: WiFiDog

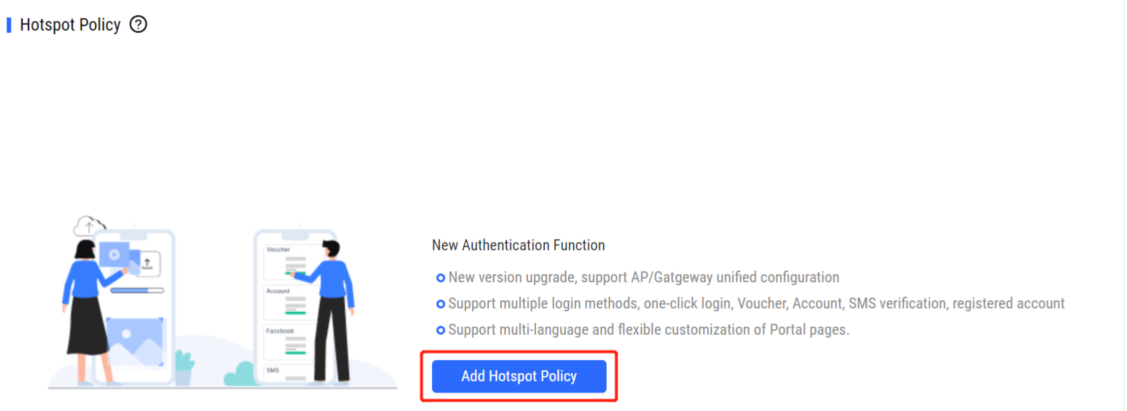
* SSID:

* Portal Server URL:

* Portal IP:

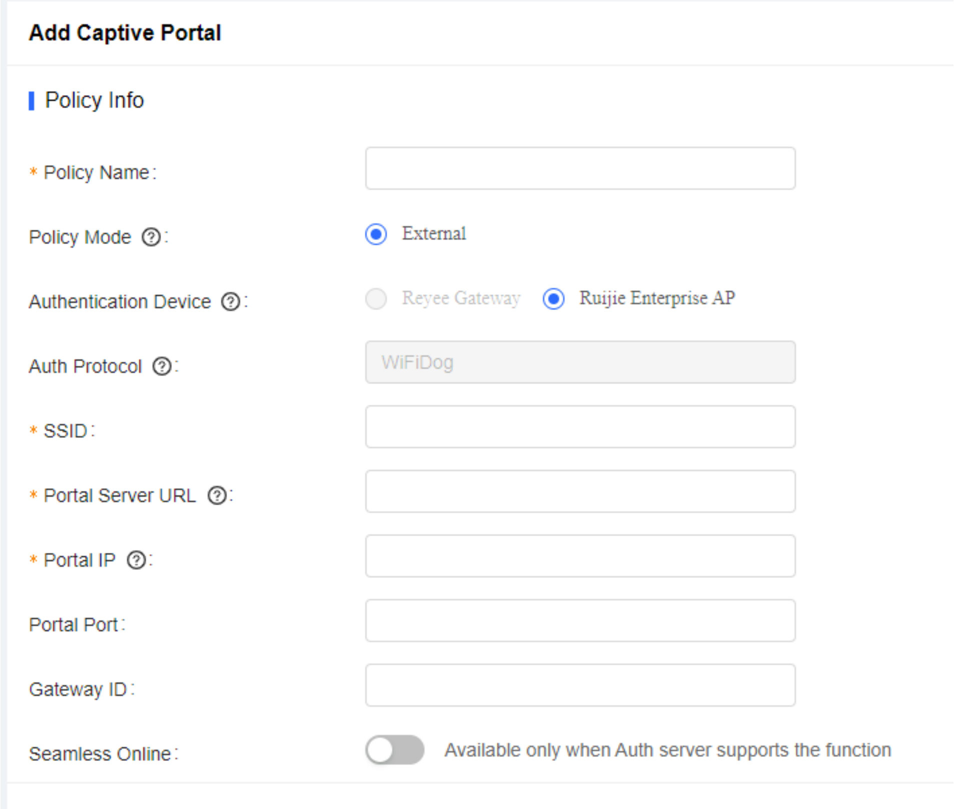
...ailable only when Auth server supports the function

(2) Click **Add Captive Portal** to add a authentication policy.



New Authentication Function

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



Add Captive Portal

Policy Info

* Policy Name:

Policy Mode ⓘ: ● External

Authentication Device ⓘ: ○ Reyee Gateway ● Ruijie Enterprise AP

Auth Protocol ⓘ: WiFiDog

* SSID:

* Portal Server URL ⓘ:

* Portal IP ⓘ:

Portal Port:

Gateway ID:

Seamless Online: Available only when Auth server supports the function

a Configure basic information about the hotspot policy.

Table 11-1 Basic Information About the Hotspot policy

Parameter	Description
Policy name	Indicates the name of a hotspot policy.
Policy Mode	Indicates the authentication mode to which the hotspot policy applies: ● **External**: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.

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

11.2 PPSK

Overview

Per-user PSK (PPSK) is also called as "One Client, One Password". It combines advantages of PSK and 802.1X. Each terminal is bound to a unique Wi-Fi password to ensure secure Wi-Fi.

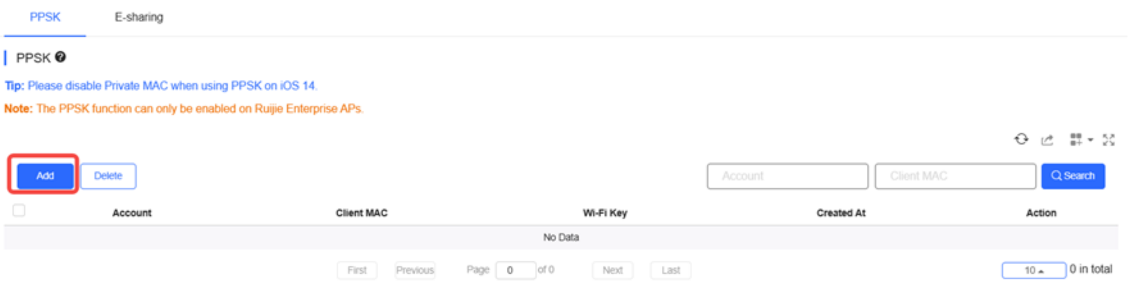
Limitations

- PPSK only supports import of 1500 passwords.
- PPSK is based on MAC address binding of terminals, and multiple devices of the same user also need to log in with different passwords.
- Each AP can only be configured with a PPSK authentication SSID.
- The PPSK password is generated randomly and does not support the customized password format.
- The AP can support PPSK only after being upgrade to B40P2 or a later version.
- There is no validity date for PPSK, which can be used all the time when it is created.
- PPSK can be created manually or through batch import.
- The AP130(L) does not support PPSK.
- Only the sub account user who is assigned with the root group can configure PPSK.

Procedure

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

(2) Click **Add** to go to the PPSK account configuration page.

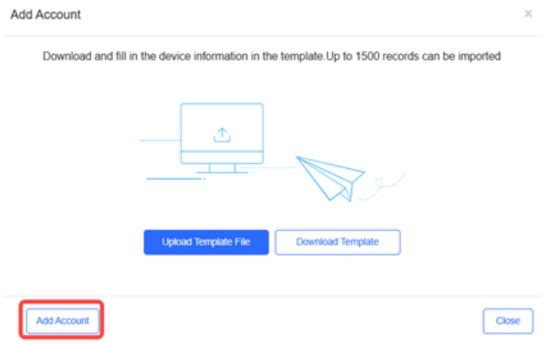


Tip: Please disable Private MAC when using PPSK on iOS 14.

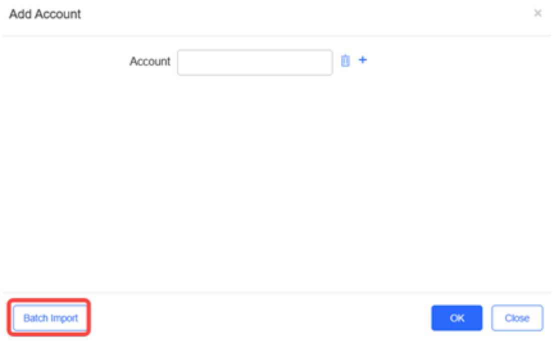
Note: The PPSK function can only be enabled on Ruijie Enterprise APs.

□	Account	Client MAC	Wi-Fi Key	Created At	Action
			No Data		

(3) You can import PPSK accounts in batches to add accounts or add them directly on the page. The default account adding mode is batch import. Click Add Account or Batch Import at the lower left corner of the page to switch the account adding mode.

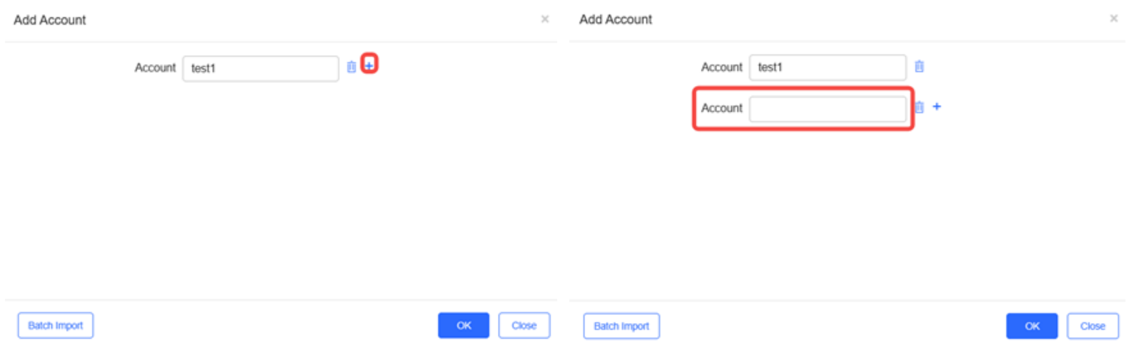


Download and fill in the device information in the template.Up to 1500 records can be imported



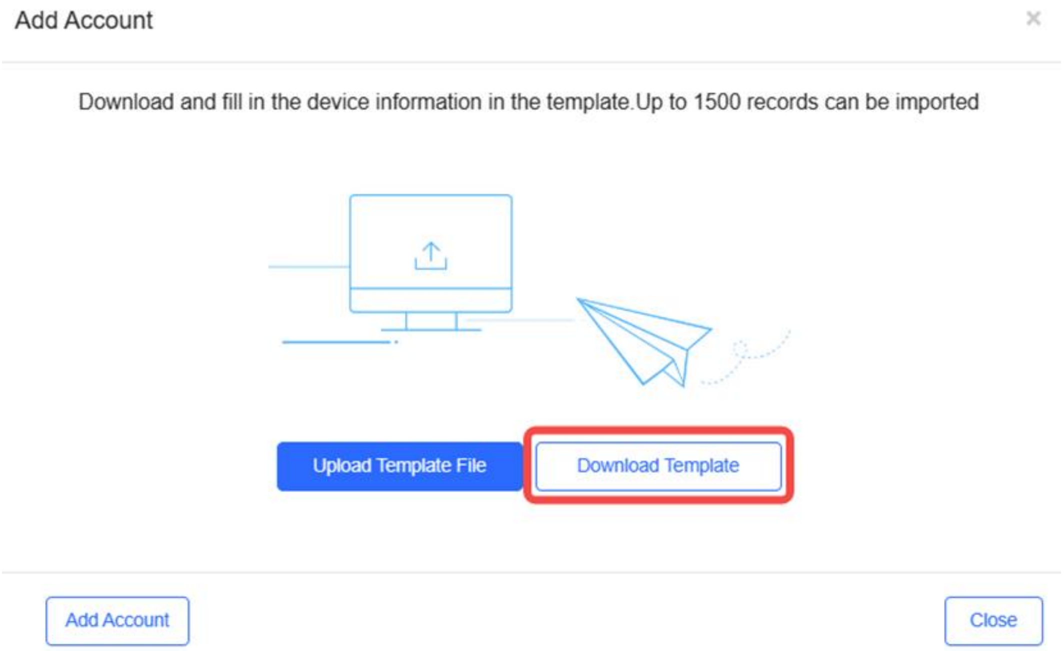
- Adding PPSK accounts manually

  On the **Add Account** page, enter an account name. Click + to add one row. After configuration, click **OK**.



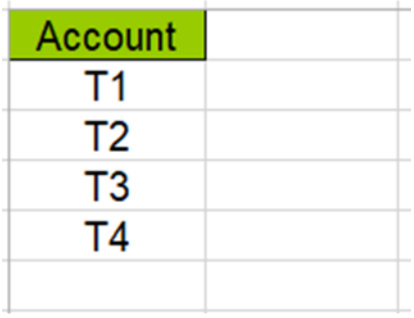
- Adding PPSK accounts through batch import

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



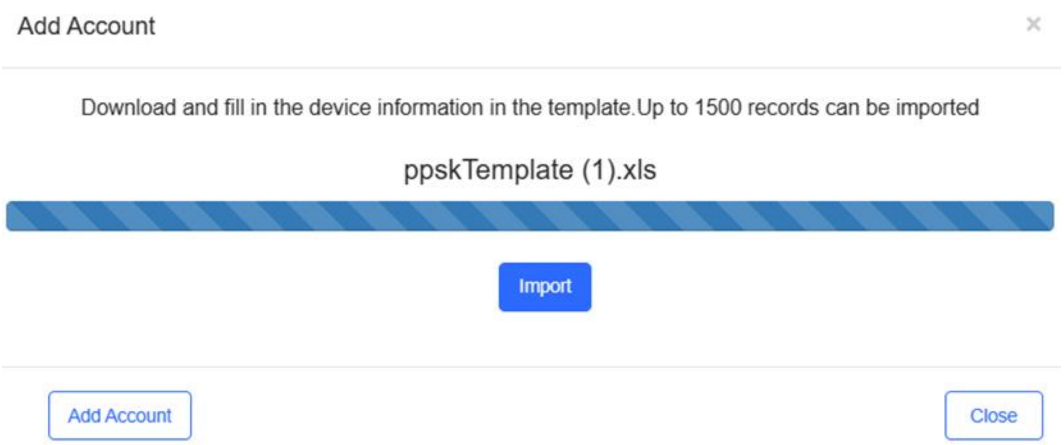
Download and fill in the device information in the template.Up to 1500 records can be imported

b Edit the template and save it.



Account	
T1	
T2	
T3	
T4	

c Click **Upload Template File** to upload the file. After uploading, users are automatically created.

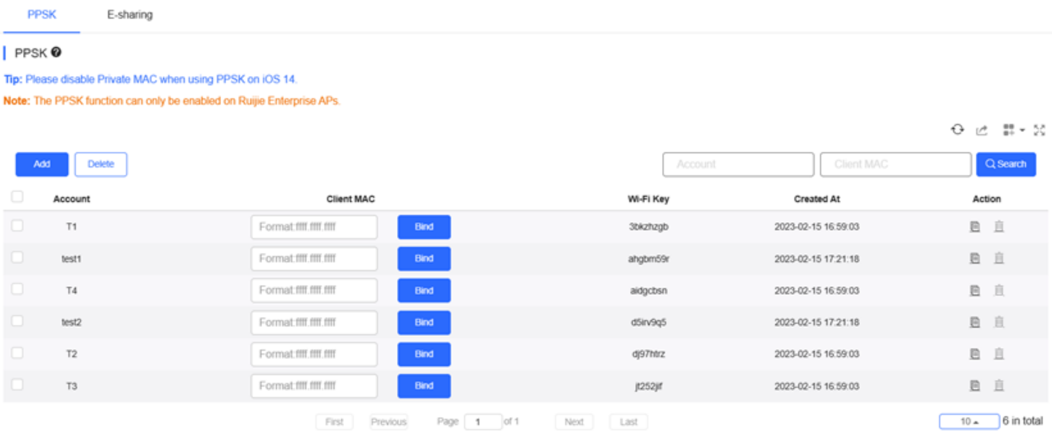


Add Account

Download and fill in the device information in the template.Up to 1500 records can be imported

ppskTemplate (1).xls

(4) View the account list.



PPSK

Tip: Please disable Private MAC when using PPSK on iOS 14.

Note: The PPSK function can only be enabled on Ruijie Enterprise APs.

□	Account	Client MAC		Wi-Fi Key	Created At	Action
□	T1	Format:ffff.ffff.ffff	Bind	3bkzhzgb	2023-02-15 16:59:03	
□	test1	Format:ffff.ffff.ffff	Bind	ahgbm59r	2023-02-15 17:21:18	
□	T4	Format:ffff.ffff.ffff	Bind	aidgcbsn	2023-02-15 16:59:03	
□	test2	Format:ffff.ffff.ffff	Bind	d5irv9q5	2023-02-15 17:21:18	
□	T2	Format:ffff.ffff.ffff	Bind	dj97htrz	2023-02-15 16:59:03	
□	T3	Format:ffff.ffff.ffff	Bind	jt252jif	2023-02-15 16:59:03	

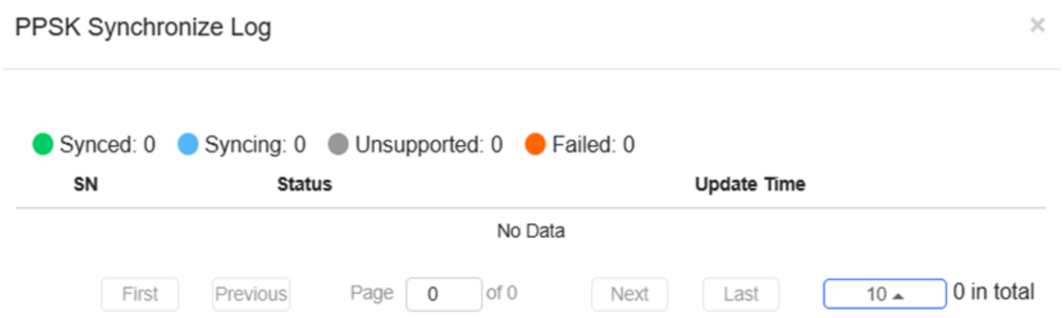
Account: indicates the name of PPSK account.

Client MAC: indicates the client's MAC address for this account.

WiFi Key: indicates the randomly generated 8-digit password for a PPSK account.

Created at: indicates the time when a PPSK account was created.

Action: indicates the **View** or **Delete** action. You can view the account to check the PPSK synchronization log.

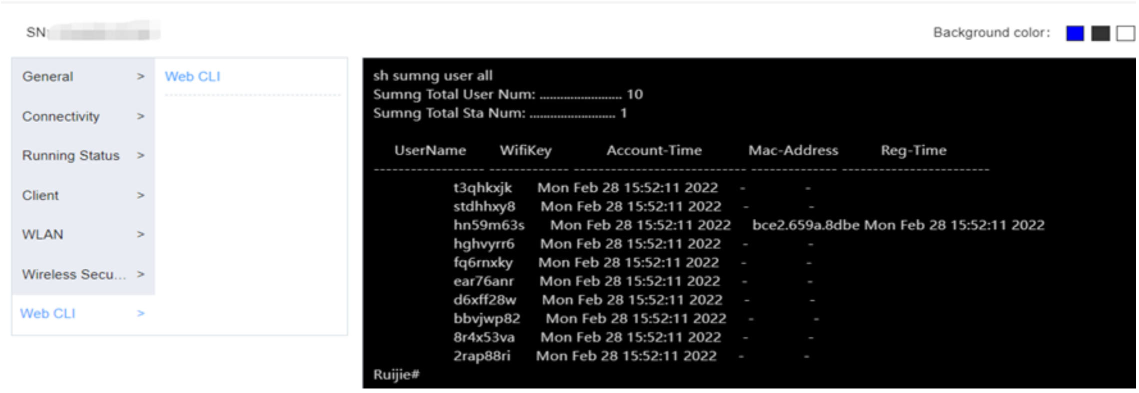


PPSK Synchronize Log

● Synced: 0 ● Syncing: 0 ● Unsupported: 0 ● Failed: 0

SN	Status	Update Time
No Data		

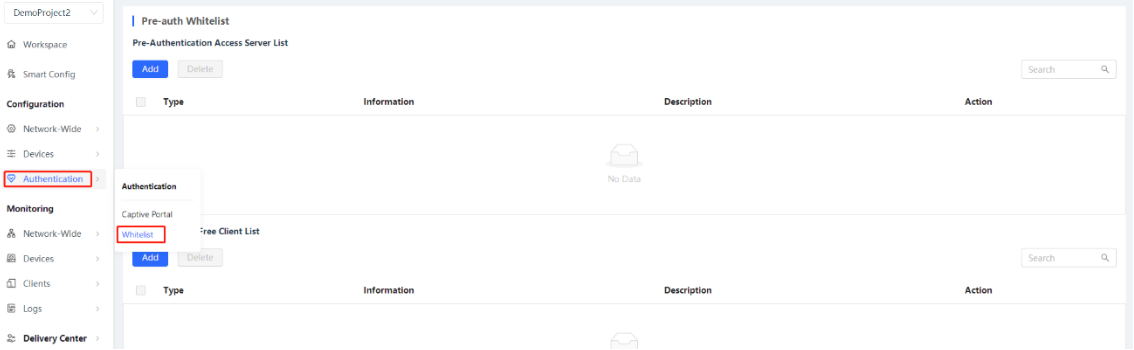
(5) The PPSK key needs to be synchronized to all APs on the same network. Choose **MONITORING** > **Devices** > **AP**, select a device, and click **Web CLI**. Enter the **show sumng user all** command to check whether the PPSK Wi-Fi key is synchronized to the AP.



```
sh sumng user all
Sumng Total User Num: ......................... 10
Sumng Total Sta Num: ......................... 1

   UserName     WifiKey        Account-Time          Mac-Address       Reg-Time
----------------- ------------- -------------------------- ------------- -----------------------
           t3qhkxjk    Mon Feb 28 15:52:11 2022   -           -
           stdhhxy8    Mon Feb 28 15:52:11 2022   -           -
           hn59m63s    Mon Feb 28 15:52:11 2022   bce2.659a.8dbe Mon Feb 28 15:52:11 2022
           hghvyrr6    Mon Feb 28 15:52:11 2022   -           -
           fq6rnxky    Mon Feb 28 15:52:11 2022   -           -
           ear76anr    Mon Feb 28 15:52:11 2022   -           -
           d6xff28w    Mon Feb 28 15:52:11 2022   -           -
           bbvjwp82    Mon Feb 28 15:52:11 2022   -           -
           8r4x53va    Mon Feb 28 15:52:11 2022   -           -
           2rap88ri    Mon Feb 28 15:52:11 2022   -           -
Ruijie#
```

11.3 Allowlist

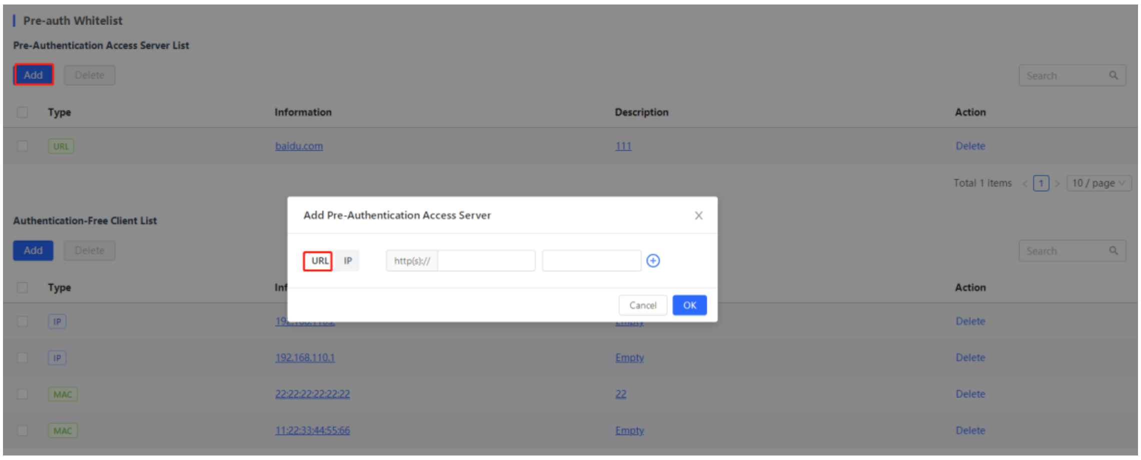
Choose **Authentication** > **Allowlist** to go to the allowlist configuration page.



11.3.1 Pre-Authentication Access Server List

(1) Pre-authentication URL list: It lists websites that can be accessed by users even if the users are not authenticated.

Click **Add** below **Pre-Authentication Access Server List**, select **URL**, and add a website. You can add a description for the website behind the website.

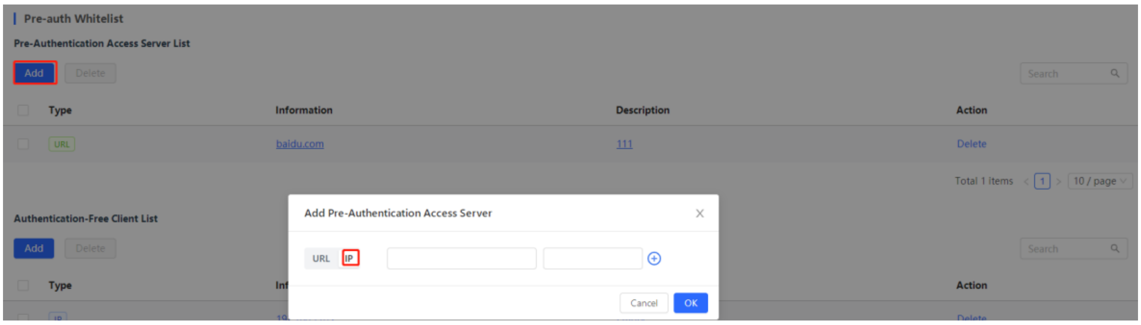

Pre-auth Whitelist
Pre-Authentication Access Server List
Add
Delete
Search
Total 1 items
1
10 / page
Authentication-Free Client List
Add
Delete
Search
Add Pre-Authentication Access Server
URL
IP
http(s)://
Cancel
OK

Type	Information	Description	Action
URL	baidu.com	111	Delete

Type	Information	Description	Action
IP	19[illegible]	[illegible]	Delete
IP	192.168.110.1	Empty	Delete
MAC	22:22:22:22:22:22	22	Delete
MAC	11:22:33:44:55:66	Empty	Delete

(2) Pre-authentication IP list: It lists external network IP addresses that can be accessed by all users including unauthenticated users.

Click **Add** below **Pre-Authentication Access Server List**, select **IP**, and add an IP address. You can add a description for the IP address behind the IP address.



Pre-auth Whitelist

Pre-Authentication Access Server List

Type	Information	Description	Action
URL	baidu.com	111	Delete

Total 1 items

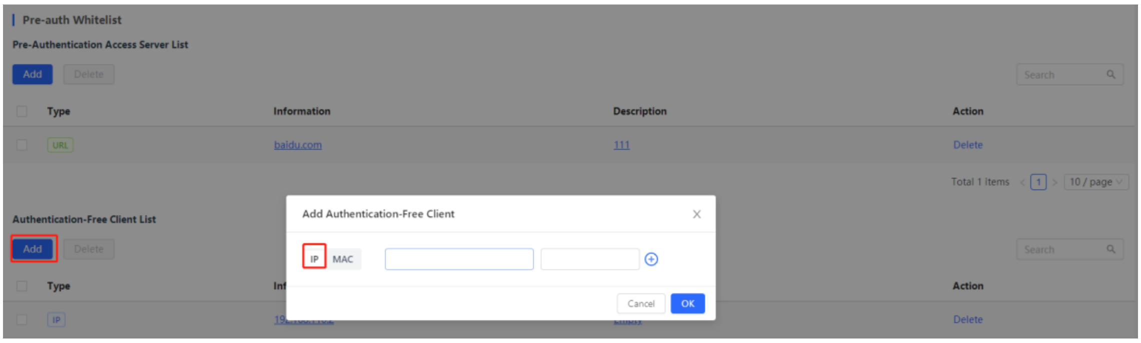
Authentication-Free Client List

Add Pre-Authentication Access Server

11.3.2 Authentication-Free Client List

(1) Authentication-free IP list: IP addresses in the list can access the Internet without authentication.

Click **Add** below **Authentication-Free Client List**, select **IP**, and add an IP address. You can add a description for the IP address behind the IP address.



Pre-auth Whitelist

Pre-Authentication Access Server List

Type	Information	Description	Action
URL	baidu.com	111	Delete

Total 1 items

Authentication-Free Client List

Add Authentication-Free Client

(2) Authentication-free MAC list: MAC addresses in the list can access the Internet without authentication.

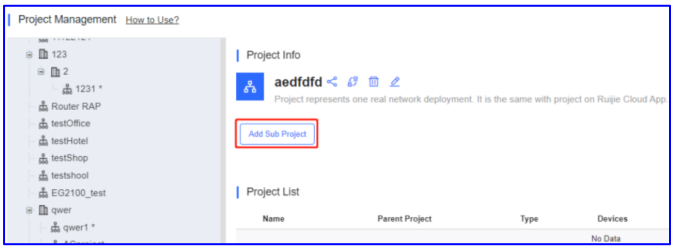
Click **Add** below **Authentication-Free Client List**, select **MAC**, and add a MAC address. You can add a description for the MAC address behind the MAC address.

12 Cloud Account and Project Management

12.1 Adding a Sub Project

(1) Choose **CONFIGURATION** > **PROJECT** and select a project.

(2) Click **Add Sub Project** to add a sub project.

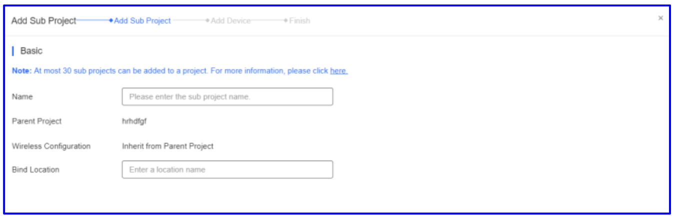


aedfdfd

Project represents one real network deployment. It is the same with project on Ruijie Cloud App.

Name	Parent Project	Type	Devices
			No Data

(3) Set basic parameters of the sub project. Then click **Save & Next**.



Note: At most 30 sub projects can be added to a project. For more information, please click here.

Name: Please enter the sub project name.

Parent Project: hrhdfgf

Wireless Configuration: Inherit from Parent Project

Bind Location: Enter a location name

Name: indicates the name of the sub project. The value is a string of up to 32 characters, including letters, numerals, or underscores (_).

Parent Project: indicates the project to which the sub project belongs.

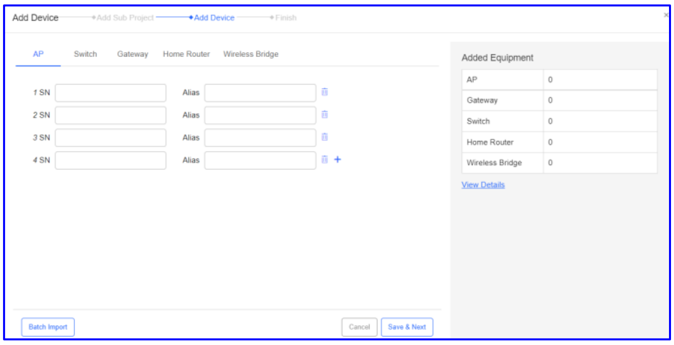
Wireless Configuration: indicates the wireless configuration of the parent project is inherited.

Bind Location: indicates the location of the sub project.

(4) Add devices manually or through batch import.

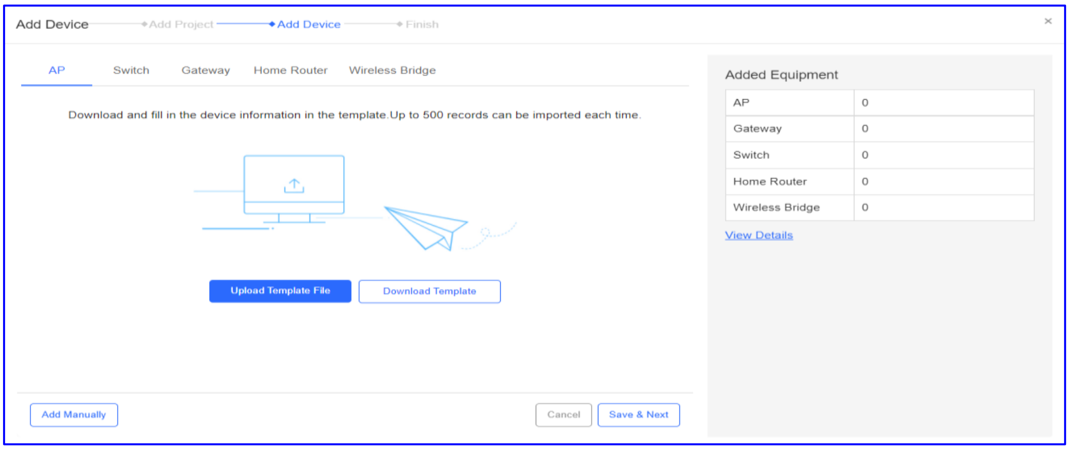
- Option 1: Add devices manually.

  Enter the device SN and alias.



AP	0
Gateway	0
Switch	0
Home Router	0
Wireless Bridge	0

- Option 2: Add devices through batch import. In the template, up to 500 records can be imported each time.



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

Added Equipment

AP	0
Gateway	0
Switch	0
Home Router	0
Wireless Bridge	0

a Click **Batch Import**.

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

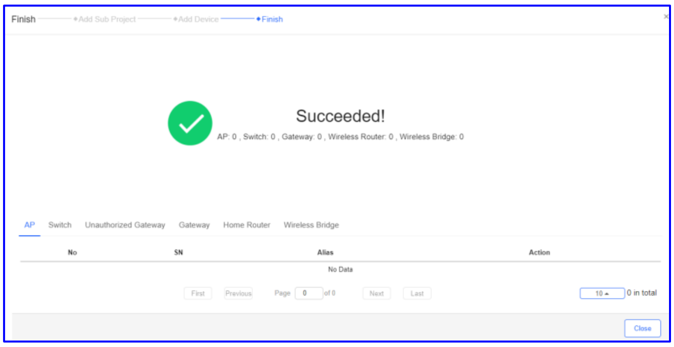
c Fill in the device SN and alias in the template and save it.

d Click **Upload Template File** to upload the edited template file.

e Click the **Import** button.

(5) After the devices are added, click **Save & Next**.

The sub project is added successfully.



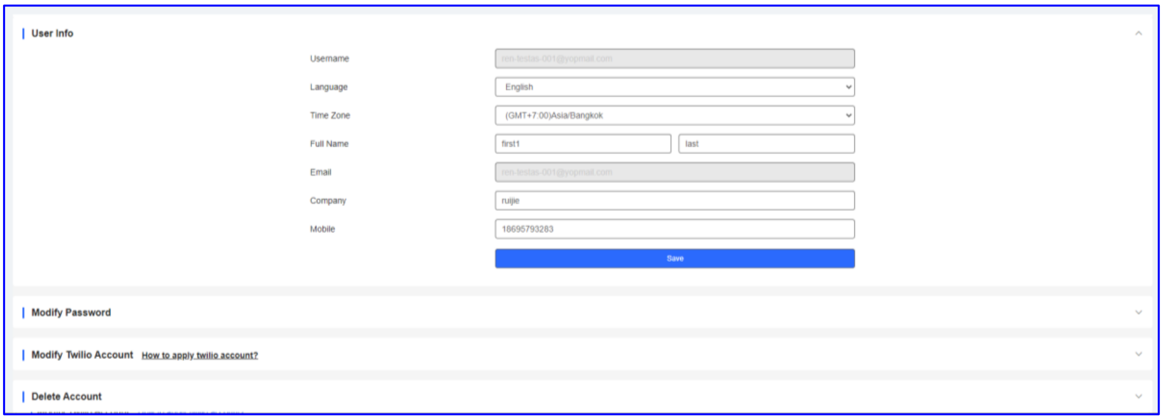
Succeeded!

AP: 0 , Switch: 0 , Gateway: 0 , Wireless Router: 0 , Wireless Bridge: 0

No	SN	Alias	Action
No Data			

12.2 Managing Cloud Login Accounts

Click at the upper right corner and click **Account**.



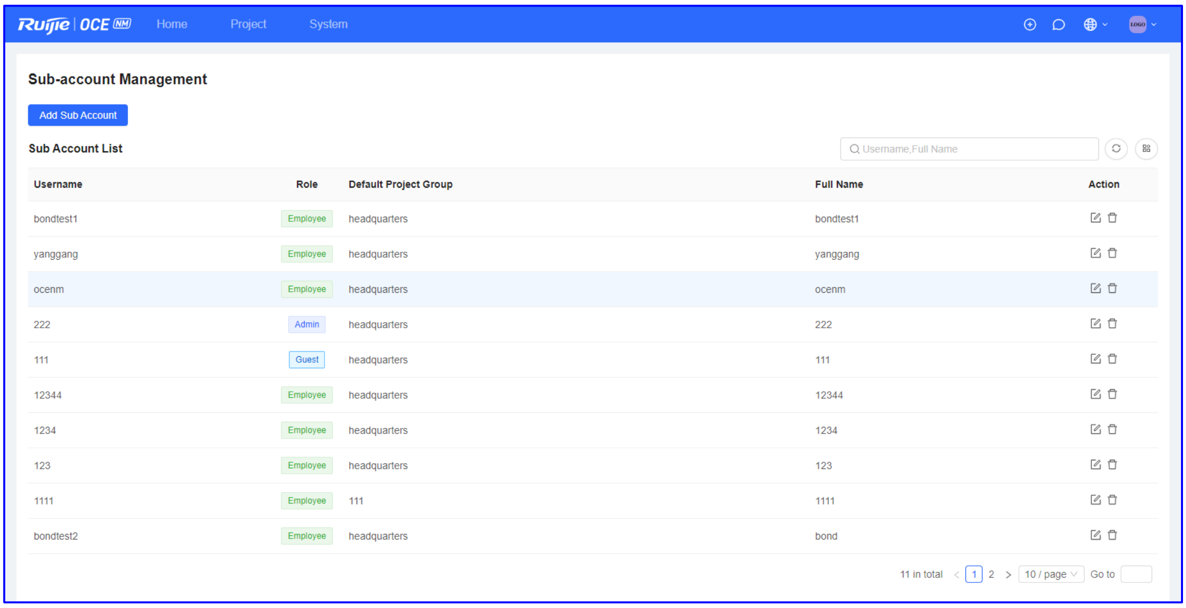
User Info

Username	ren-testas-001@yopmail.com
Language	English
Time Zone	(GMT+7:00)Asia/Bangkok
Full Name	first1 last
Email	ren-testas-001@yopmail.com
Company	ruijie
Mobile	18695793283

12.3 Managing Cloud Sub Accounts

Click 👤 at the upper right corner, and click **Sub Account**.

The **Sub Account List** displays the information of sub accounts. Click ✎ in the **Action** column to edit the sub account. Click 🗑 in the **Action** column to delete the sub account.



Sub-account Management

Sub Account List

Username	Role	Default Project Group	Full Name	Action
bondtest1	Employee	headquarters	bondtest1	✎ 🗑
yanggang	Employee	headquarters	yanggang	✎ 🗑
ocenm	Employee	headquarters	ocenm	✎ 🗑
222	Admin	headquarters	222	✎ 🗑
111	Guest	headquarters	111	✎ 🗑
12344	Employee	headquarters	12344	✎ 🗑
1234	Employee	headquarters	1234	✎ 🗑
123	Employee	headquarters	123	✎ 🗑
1111	Employee	111	1111	✎ 🗑
bondtest2	Employee	headquarters	bond	✎ 🗑

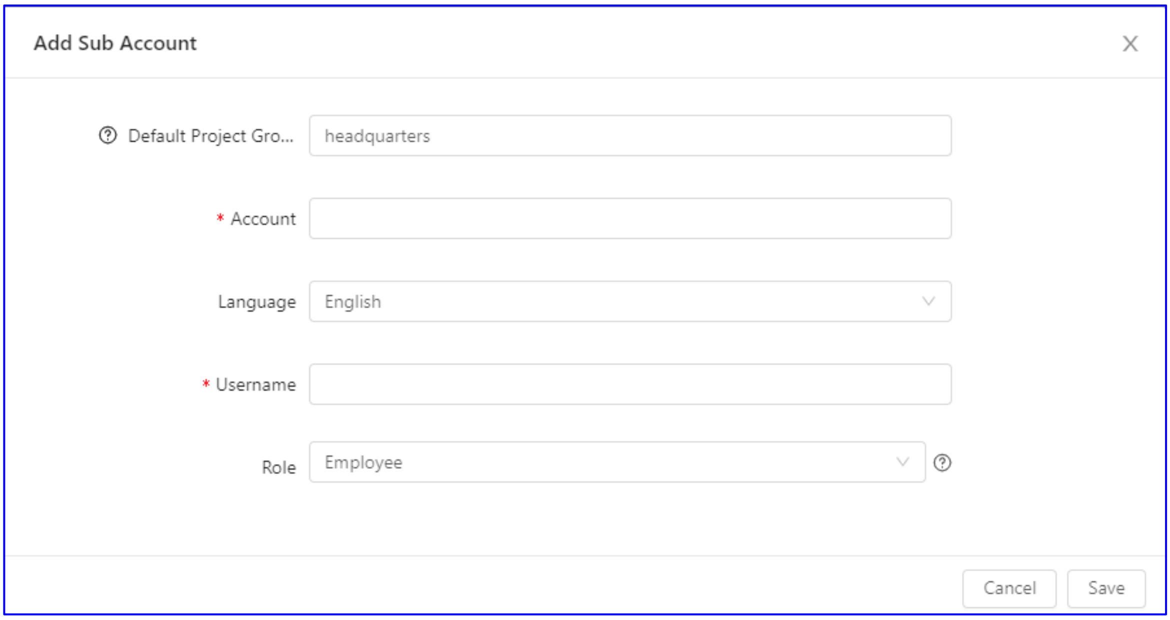
Click **Add Sub Account** to add a new sub account. Select the network, enter the **Account**, **Username** and **Role**, and click **Save**.

Role:

Admin owns the permissions to create an account.

Employee owns the permissions to edit data.

Guest owns the permissions to view data.



Add Sub Account

Default Project Gro... headquarters

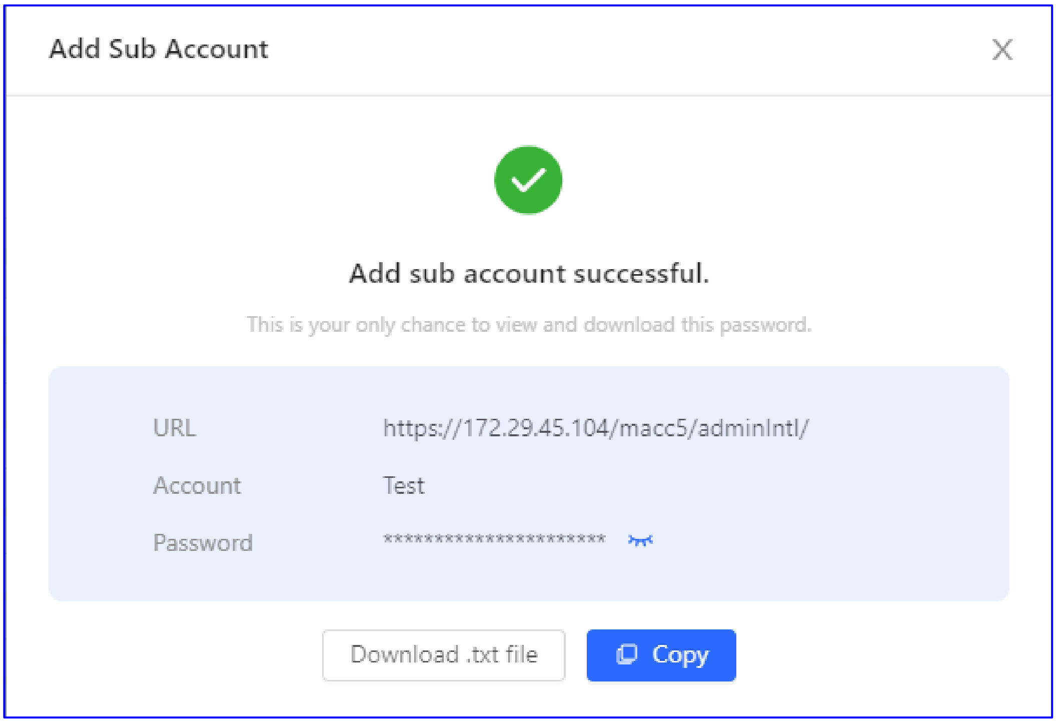
* Account

Language English

* Username

Role Employee

Sub Account password will be auto generated, click **Copy** and share to user. When sub account login first time, system will require to change the password.



Add Sub Account

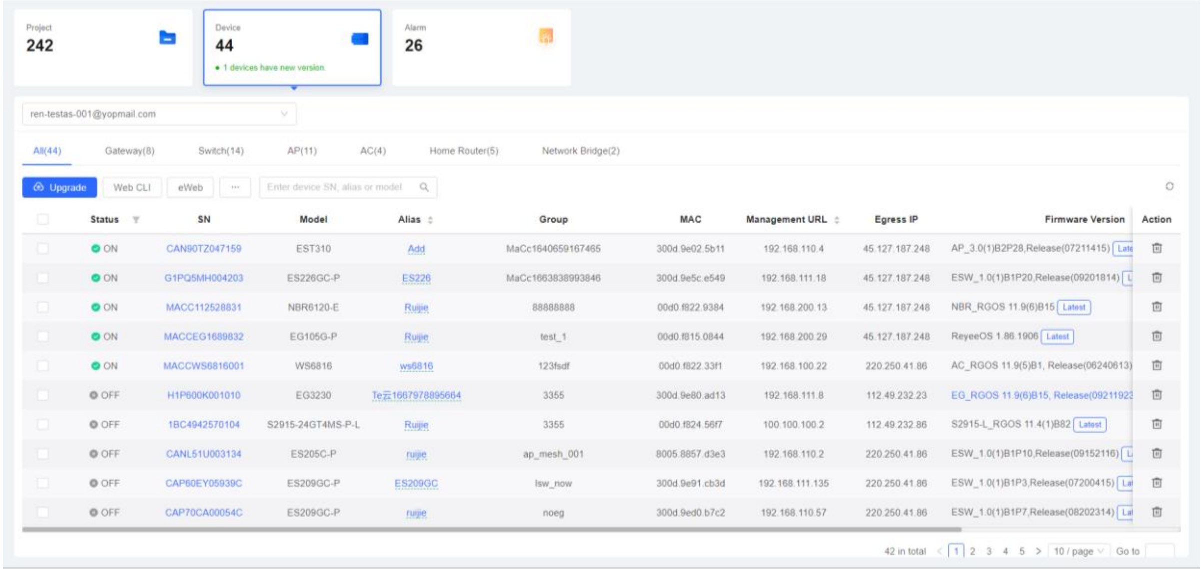
Add sub account successful.

This is your only chance to view and download this password.

URL	https://172.29.45.104/macc5/adminIntl/
Account	Test
Password	**********************

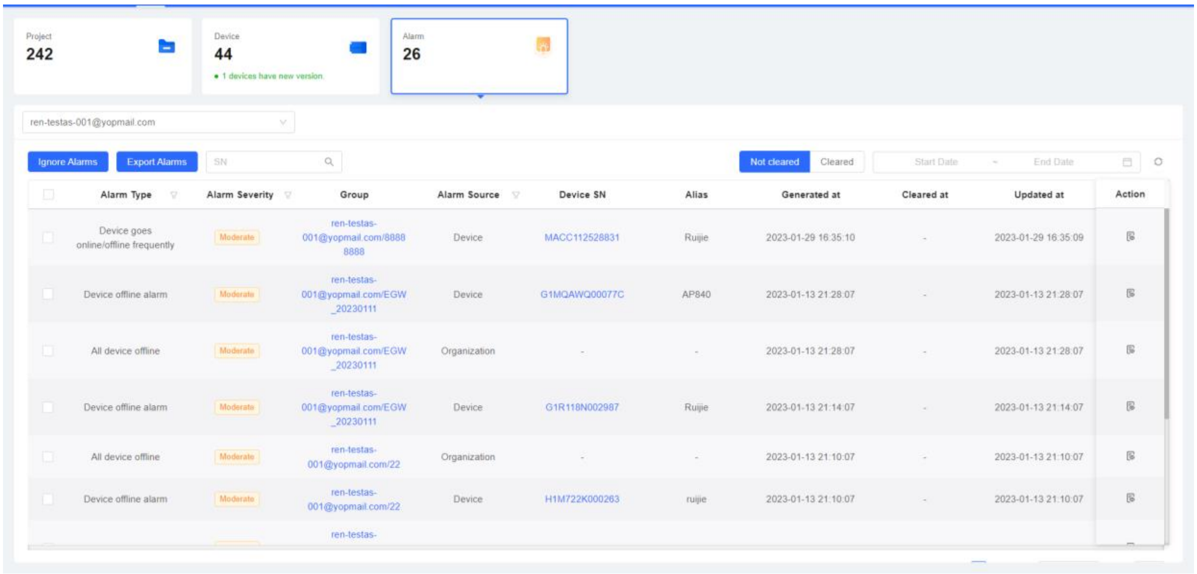
13 Monitoring

13.1 Viewing all the Device



□	Status	SN	Model	Alias	Group	MAC	Management URL	Egress IP	Firmware Version	Action
□	● ON	CAN90TZ047159	EST310	Add	MaCc1640659167465	300d.9e02.5b11	192.168.110.4	45.127.187.248	AP_3.0(1)B2P28,Release(07211415) Late	🗑
□	● ON	G1PQ5MH004203	ES226GC-P	ES226	MaCc1663838993846	300d.9e5c.e549	192.168.111.18	45.127.187.248	ESW_1.0(1)B1P20,Release(09201814) L	🗑
□	● ON	MACC112528831	NBR6120-E	Ruijie	88888888	00d0.f822.9384	192.168.200.13	45.127.187.248	NBR_RGOS 11.9(6)B15 Latest	🗑
□	● ON	MACCEG1689832	EG105G-P	Ruijie	test_1	00d0.f815.0844	192.168.200.29	45.127.187.248	ReyeeOS 1.86.1906 Latest	🗑
□	● ON	MACCWS6816001	WS6816	ws6816	123fsdf	00d0.f822.33f1	192.168.100.22	220.250.41.86	AC_RGOS 11.9(5)B1, Release(06240613)	🗑
□	● OFF	H1P600K001010	EG3230	Te云1667978895664	3355	300d.9e80.ad13	192.168.111.8	112.49.232.23	EG_RGOS 11.9(6)B15, Release(0921192	🗑
□	● OFF	1BC4942570104	S2915-24GT4MS-P-L	Ruijie	3355	00d0.f824.56f7	100.100.100.2	112.49.232.86	S2915-L_RGOS 11.4(1)B82 Latest	🗑
□	● OFF	CANL51U003134	ES205C-P	ruijie	ap_mesh_001	8005.8857.d3e3	192.168.110.2	220.250.41.86	ESW_1.0(1)B1P10,Release(09152116) L	🗑
□	● OFF	CAP60EY05939C	ES209GC-P	ES209GC	lsw_now	300d.9e91.cb3d	192.168.111.135	220.250.41.86	ESW_1.0(1)B1P3,Release(07200415) La	🗑
□	● OFF	CAP70CA00054C	ES209GC-P	ruijie	noeg	300d.9ed0.b7c2	192.168.110.57	220.250.41.86	ESW_1.0(1)B1P7,Release(08202314) La	🗑

13.2 Viewing all the Alarm



□	Alarm Type	Alarm Severity	Group	Alarm Source	Device SN	Alias	Generated at	Cleared at	Updated at	Action
□	Device goes online/offline frequently	Moderate	ren-testas-001@yopmail.com/88888888	Device	MACC112528831	Ruijie	2023-01-29 16:35:10	-	2023-01-29 16:35:09	🗎
□	Device offline alarm	Moderate	ren-testas-001@yopmail.com/EGW_20230111	Device	G1MQAWQ00077C	AP840	2023-01-13 21:28:07	-	2023-01-13 21:28:07	🗎
□	All device offline	Moderate	ren-testas-001@yopmail.com/EGW_20230111	Organization	-	-	2023-01-13 21:28:07	-	2023-01-13 21:28:07	🗎
□	Device offline alarm	Moderate	ren-testas-001@yopmail.com/EGW_20230111	Device	G1R118N002987	Ruijie	2023-01-13 21:14:07	-	2023-01-13 21:14:07	🗎
□	All device offline	Moderate	ren-testas-001@yopmail.com/22	Organization	-	-	2023-01-13 21:10:07	-	2023-01-13 21:10:07	🗎
□	Device offline alarm	Moderate	ren-testas-001@yopmail.com/22	Device	H1M722K000263	ruijie	2023-01-13 21:10:07	-	2023-01-13 21:10:07	🗎
			ren-testas-							

13.3 Viewing Topology

Topology displays the overall network status on the GUI, including the network topology and device status, and offers the project report.

Requirements on the Network Topology

(1) Ensure that devices are online on the Ruijie Cloud and the web CLI is accessible.

(2) A root node that can be an EG or a core switch is required.

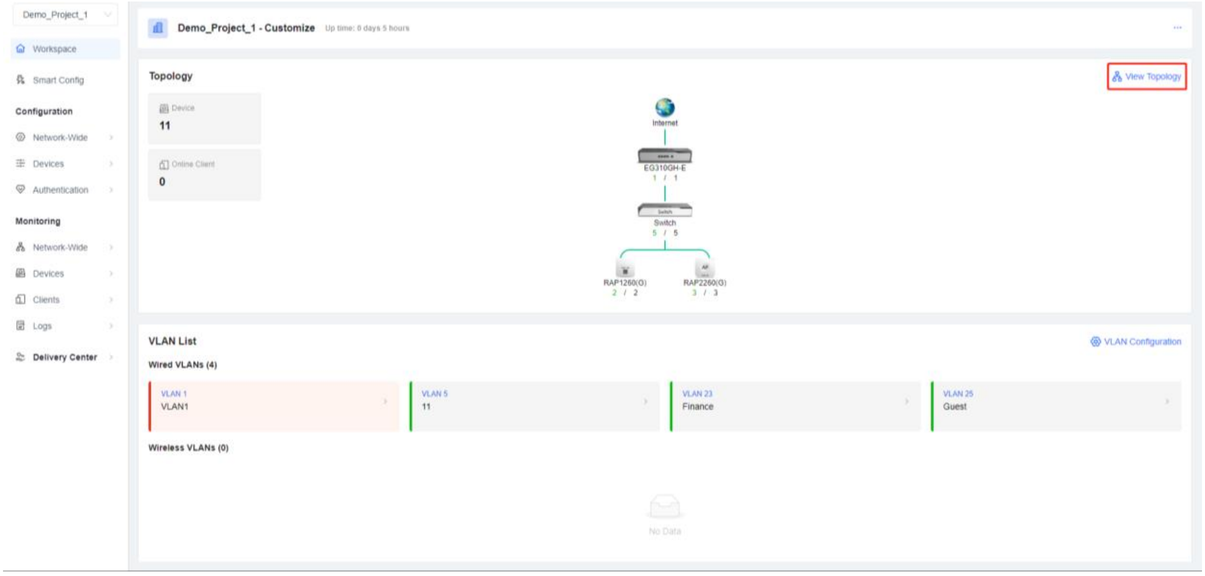
(3) The number of connected devices is calculated based on the root node and the topology is refreshed. Data such as MAC addresses, ARP entries, and routing entries is required.

The topology cannot be displayed in the following situations:

- You cannot access the device web CLI.
- An EG is deployed on the network, but it does not support the **show mac** command or the version is not the latest.
- Multiple switches at the same level together with non-Ruijie products serve as the egress.
- The core switch, access switches, and Aps are deployed. The core switch runs OSPF and has no static routing entries, so its routing table is incomplete.
- Device offline, port change, static route modification, device addition or deletion, etc.
- Switches constitute a network using Virtual Switching Unit (VSU).
- Switches constitute a network using Virtual Router Redundancy Protocol (VRRP).
- Only APs exist in the network group.

Procedure

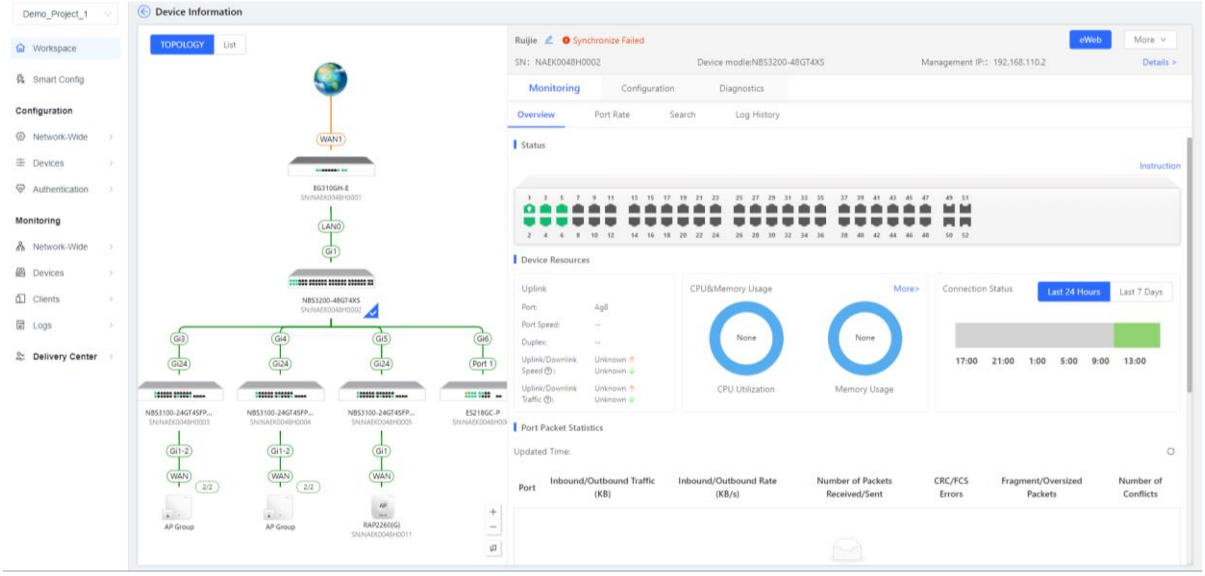
Click **Project** > **Workspace** > **View Topology**



Update Topology: refreshes the topology when devices are added or deleted.

Download Topo: downloads the topology in .png format.

: Click any device in the topology to view or configure the corresponding device.

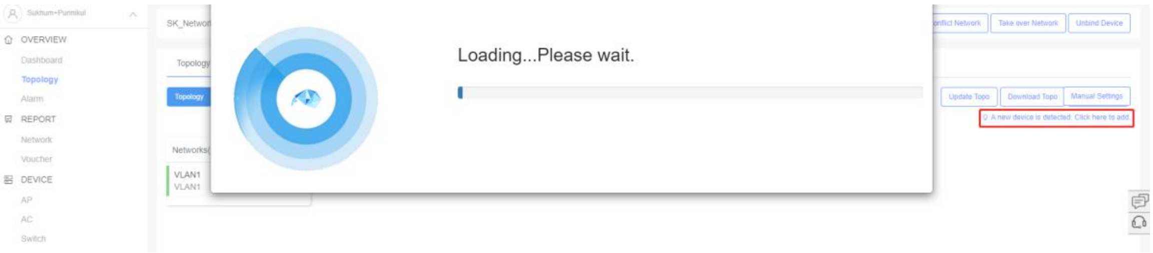


13.4 Detecting Device

Detect Device: After the detection is completed, the detection result will be displayed.

Procedure

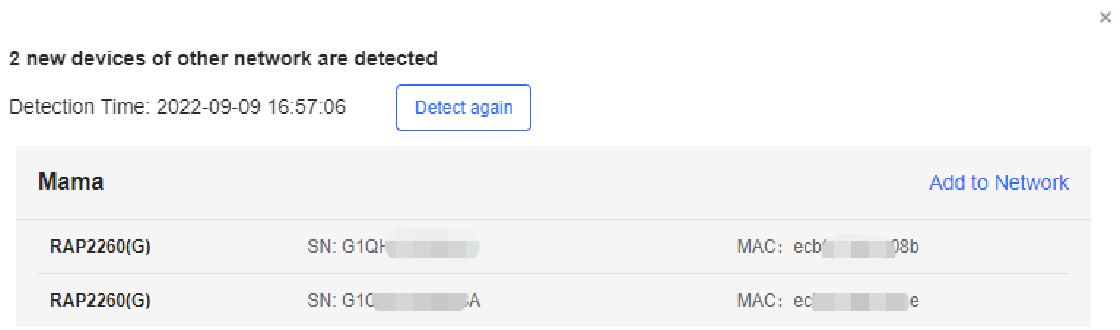
Click **Project** > **Workspace** > **View Topology**, Click Detect Device.



Loading...Please wait.

A new device is detected. Click here to add

After the detection is completed, the detection result will be displayed.



2 new devices of other network are detected

Detection Time: 2022-09-09 16:57:06

Mama Add to Network

RAP2260(G)	SN: G1QH[redacted]	MAC: ecb[redacted]08b
RAP2260(G)	SN: G1([redacted]A	MAC: ec[redacted]e

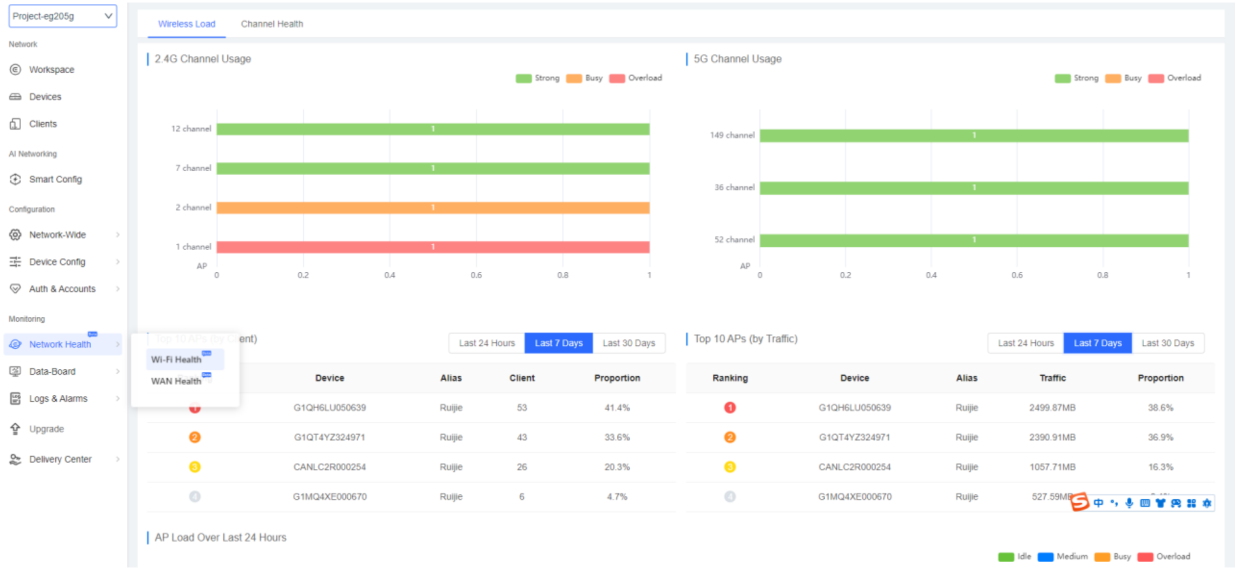
When you add a device to the network, you are required to enter the device password. If the password is incorrect, the system will refuse to add it to the network.

Ruijie Cloud refreshes the topology by default when a device is added to the network. When Ruijie Cloud fails to detect the added devices, click **Detect again** to update the topology.

13.5 Network Health

13.5.1 Wi-Fi Health

You can monitor wireless health, including 2.4 GHz and 5 GHz channel usage, top APs by traffic and clients, and AP load at different times.



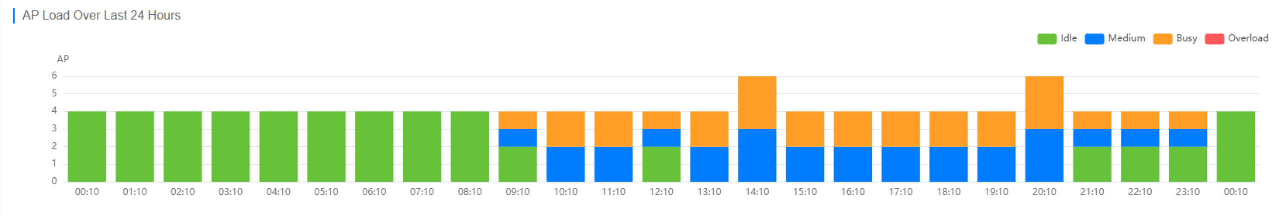
Top 10 APs (by Client)

	Device	Alias	Client	Proportion
1	G1QH6LU050639	Ruijie	53	41.4%
2	G1QT4YZ324971	Ruijie	43	33.6%
3	CANLC2R000254	Ruijie	26	20.3%
4	G1MQ4XE000670	Ruijie	6	4.7%

Top 10 APs (by Traffic)

Ranking	Device	Alias	Traffic	Proportion
1	G1QH6LU050639	Ruijie	2499.87MB	38.6%
2	G1QT4YZ324971	Ruijie	2390.91MB	36.9%
3	CANLC2R000254	Ruijie	1057.71MB	16.3%
4	G1MQ4XE000670	Ruijie	527.59MB	[illegible]

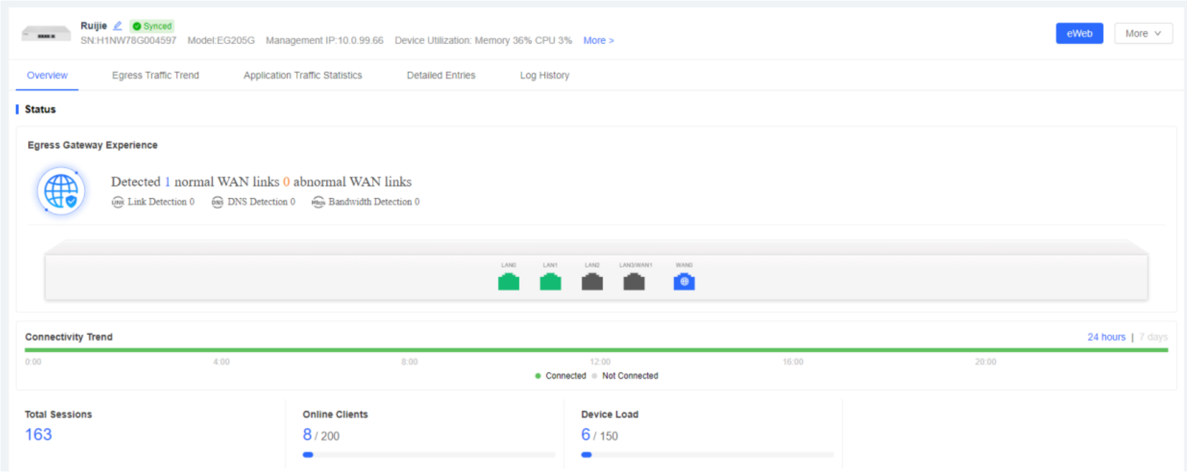
AP Load Over Last 24 Hours



AP Load Over Last 24 Hours

13.5.2 WAN Health

You can view the egress status, including the WAN port status, link, and DNS status, number of sessions, number of online users, top clients by traffic, top applications by traffic, user trend, traffic trend, CPU and memory usage trend, interface IP, and negotiated speed, and so on.



Ruijie Synced
SN:H1NW78G004597 Model:EG205G Management IP:10.0.99.66 Device Utilization: Memory 36% CPU 3% More >

Status

Egress Gateway Experience

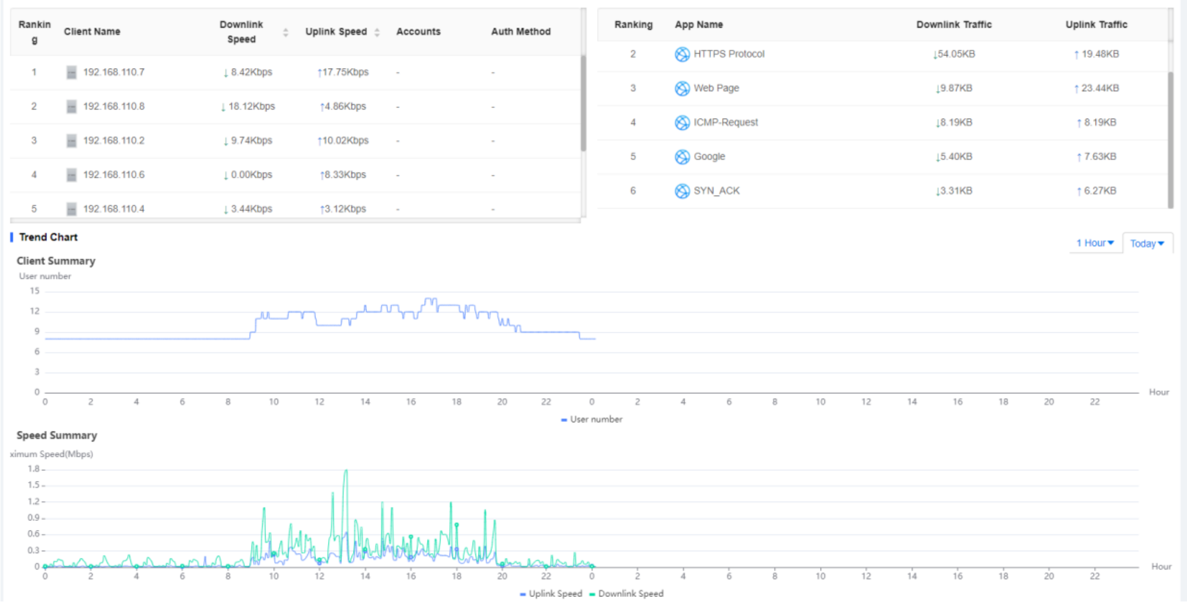
Detected 1 normal WAN links 0 abnormal WAN links
Link Detection 0 DNS Detection 0 Bandwidth Detection 0

Connectivity Trend

Total Sessions
163

Online Clients
8 / 200

Device Load
6 / 150



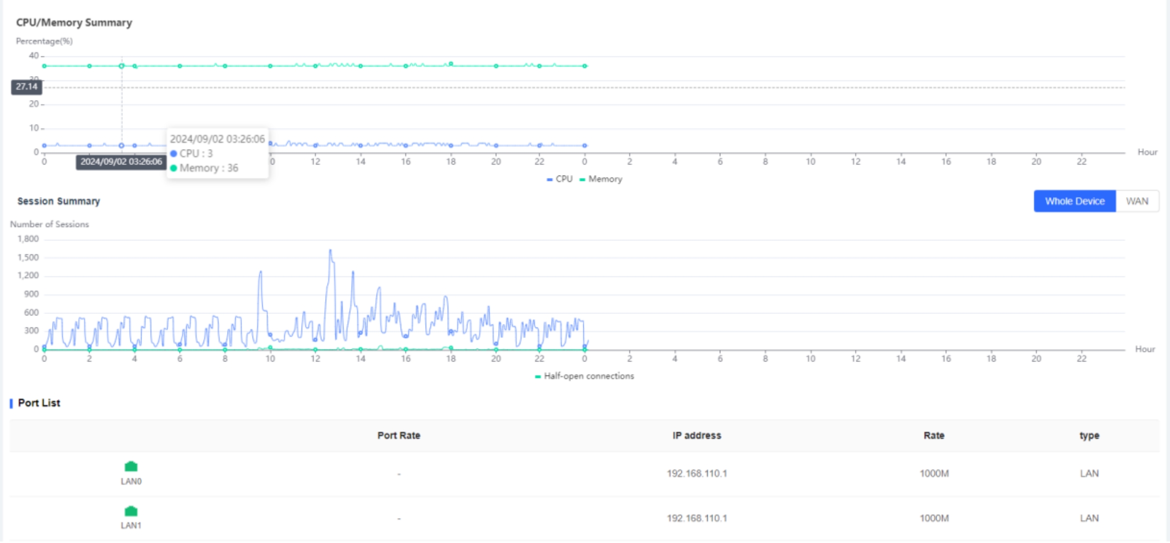
Ranking	Client Name	Downlink Speed	Uplink Speed	Accounts	Auth Method
1	192.168.110.7	↓8.42Kbps	↑17.75Kbps	-	-
2	192.168.110.8	↓18.12Kbps	↑4.86Kbps	-	-
3	192.168.110.2	↓9.74Kbps	↑10.02Kbps	-	-
4	192.168.110.6	↓0.00Kbps	↑8.33Kbps	-	-
5	192.168.110.4	↓3.44Kbps	↑3.12Kbps	-	-

Ranking	App Name	Downlink Traffic	Uplink Traffic
2	HTTPS Protocol	↓54.05KB	↑19.48KB
3	Web Page	↓9.87KB	↑23.44KB
4	ICMP-Request	↓8.19KB	↑8.19KB
5	Google	↓5.40KB	↑7.63KB
6	SYN_ACK	↓3.31KB	↑6.27KB

Trend Chart

Client Summary

Speed Summary



Port List

	Port Rate	IP address	Rate	type
LAN0	-	192.168.110.1	1000M	LAN
LAN1	-	192.168.110.1	1000M	LAN

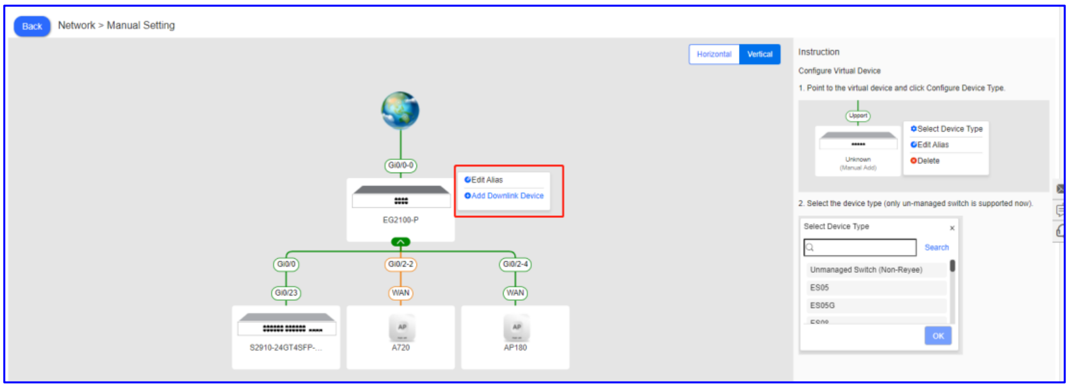
13.6 Edit Topology

Procedure

Click **Project** > **Workspace** > **View Topology** and click **Edit**

Edit: For different devices, you can perform different operations. Hover the mouse over the device to check the operations that can be performed on the device. The following are for reference only.

- For the gateway detected by the network, you can edit the alias of the device or add the downlink device.



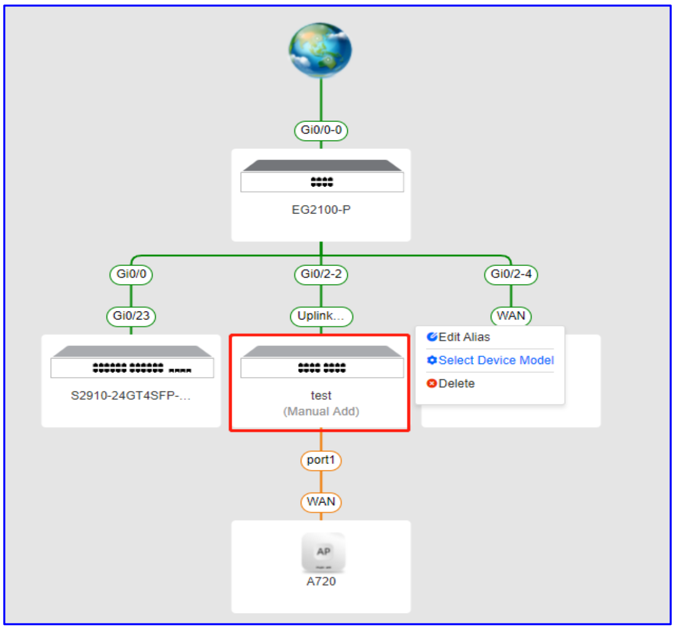
Instruction

Configure Virtual Device

1. Point to the virtual device and click Configure Device Type.

2. Select the device type (only un-managed switch is supported now).

- For the device added manually, you can rename the device, select the device model, or remove the device form the network. The models include Reyee ES series and unmanaged switches (non-Reyee).



13.6.1 Common Troubleshooting

1. **What can I do if the system displays "No Data" in the topology?**

(1) If there is only one AP on the network, the topology cannot be displayed.

(2) The egress device is not the Ruijie device and no core switch is deployed.

(3) Try to refresh the topology manually.

2. **What can I do if there is only an EG in the topology?**

(10) If the version is not the latest one, you need upgrade it to the latest version.

(11) If the web CLI is unavailable, other devices cannot be displayed.

3. **What can I do if some devices are not displayed in the topology?**

(12) **show mac**/**show arp**/**show ip route**: If the output of any of the preceding commands contains the configuration with S*, static bindings exist.

(13) Dynamic routing protocols such as OSPF are configured for the topology.

(14) The switches in the topology are configured with VSU.

4. **What can I do if virtual devices are displayed in the topology?**

(15) The network device is not on the Ruijie Cloud or is offline.

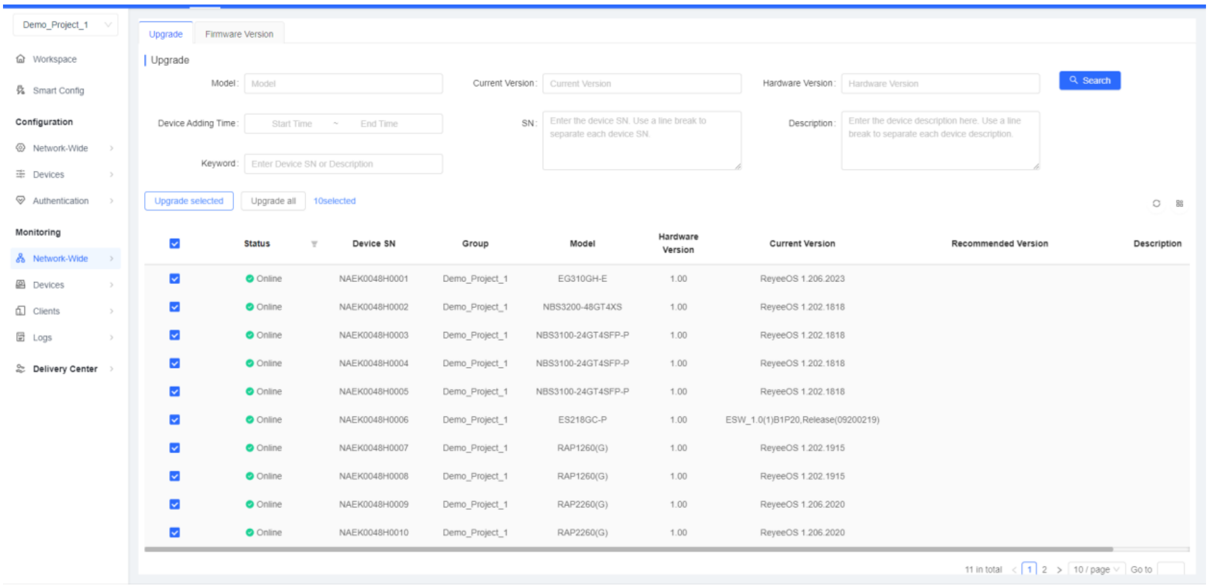
(16) The network device is not the Ruijie device.

(17) If the network device is an unmanaged switch, you are advised to edit the name and the port manually.

13.7 Upgrade

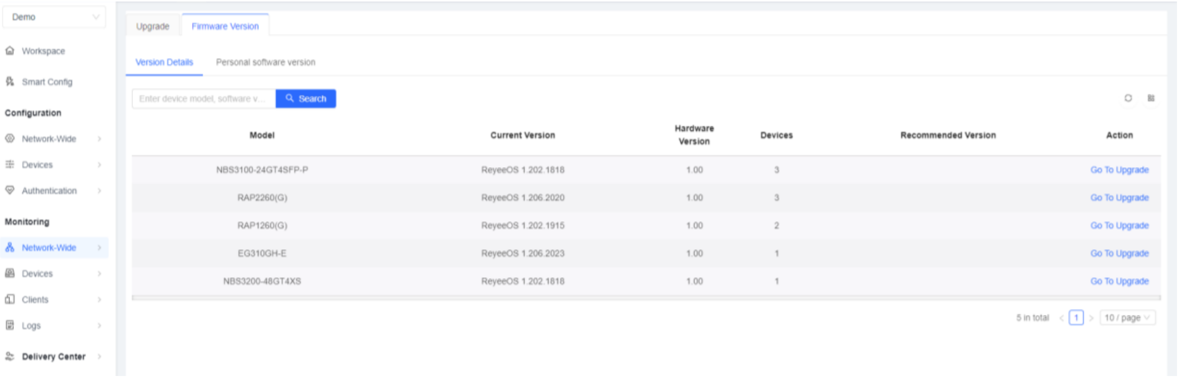
13.7.1 Upgrade

Select products to upgrade the software versions of the products in batches.


Demo_Project_1
Workspace
Smart Config
Configuration
Network-Wide
Devices
Authentication
Monitoring
Network-Wide
Devices
Clients
Logs
Delivery Center
Upgrade
Firmware Version
Upgrade
Model: Model
Current Version: Current Version
Hardware Version: Hardware Version
Search
Device Adding Time: Start Time ~ End Time
SN: Enter the device SN. Use a line break to separate each device SN.
Description: Enter the device description here. Use a line break to separate each device description.
Keyword: Enter Device SN or Description
Upgrade selected
Upgrade all
10selected
11 in total
1
2
10 / page
Go to

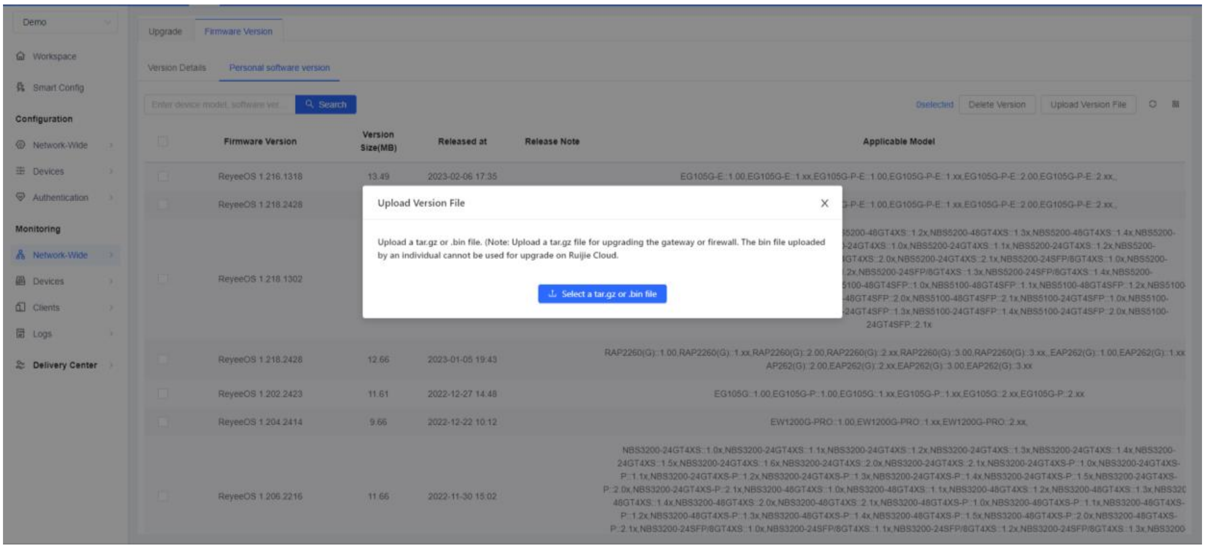
☑	Status	Device SN	Group	Model	Hardware Version	Current Version	Recommended Version	Description
☑	Online	NAEK0048H0001	Demo_Project_1	EG310GH-E	1.00	ReyeeOS 1.206.2023		
☑	Online	NAEK0048H0002	Demo_Project_1	NBS3200-48GT4XS	1.00	ReyeeOS 1.202.1818		
☑	Online	NAEK0048H0003	Demo_Project_1	NBS3100-24GT4SFP-P	1.00	ReyeeOS 1.202.1818		
☑	Online	NAEK0048H0004	Demo_Project_1	NBS3100-24GT4SFP-P	1.00	ReyeeOS 1.202.1818		
☑	Online	NAEK0048H0005	Demo_Project_1	NBS3100-24GT4SFP-P	1.00	ReyeeOS 1.202.1818		
☑	Online	NAEK0048H0006	Demo_Project_1	ES218GC-P	1.00	ESW_1.0(1)B1P20,Release(09200219)		
☑	Online	NAEK0048H0007	Demo_Project_1	RAP1260(G)	1.00	ReyeeOS 1.202.1915		
☑	Online	NAEK0048H0008	Demo_Project_1	RAP1260(G)	1.00	ReyeeOS 1.202.1915		
☑	Online	NAEK0048H0009	Demo_Project_1	RAP2260(G)	1.00	ReyeeOS 1.206.2020		
☑	Online	NAEK0048H0010	Demo_Project_1	RAP2260(G)	1.00	ReyeeOS 1.206.2020		

13.7.2 Firmware Version



Model	Current Version	Hardware Version	Devices	Recommended Version	Action
NBS3100-24GT4SFP-P	ReyeeOS 1.202.1818	1.00	3		Go To Upgrade
RAP2260(G)	ReyeeOS 1.206.2020	1.00	3		Go To Upgrade
RAP1260(G)	ReyeeOS 1.202.1915	1.00	2		Go To Upgrade
EG310GH-E	ReyeeOS 1.206.2023	1.00	1		Go To Upgrade
NBS3200-48GT4XS	ReyeeOS 1.202.1818	1.00	1		Go To Upgrade

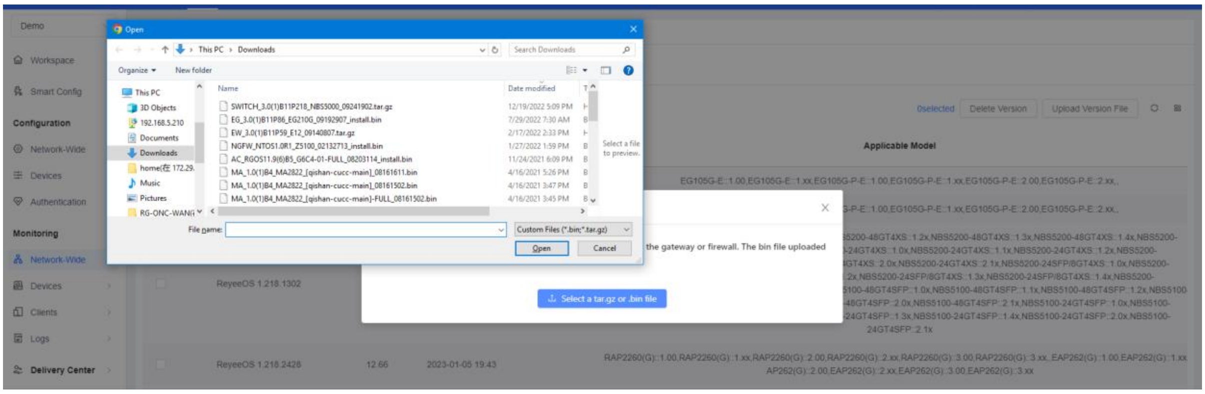
This page lists device version files that are manually uploaded by users.



Firmware Version	Version Size(MB)	Released at	Release Note	Applicable Model
ReyeeOS 1.216.1318	13.49	2023-02-06 17:35		EG105G-E::1.00,EG105G-E::1.xx,EG105G-P-E::1.00,EG105G-P-E::1.xx,EG105G-P-E::2.00,EG105G-P-E::2.xx,,
ReyeeOS 1.218.2428				G-P-E::1.00,EG105G-P-E::1.xx,EG105G-P-E::2.00,EG105G-P-E::2.xx,,
ReyeeOS 1.218.1302				5200-48GT4XS::1.2x,NBS5200-48GT4XS::1.3x,NBS5200-48GT4XS::1.4x,NBS5200- -24GT4XS::1.0x,NBS5200-24GT4XS::1.1x,NBS5200-24GT4XS::1.2x,NBS5200- GT4XS::2.0x,NBS5200-24GT4XS::2.1x,NBS5200-24SFP/8GT4XS::1.0x,NBS5200- 2x,NBS5200-24SFP/8GT4XS::1.3x,NBS5200-24SFP/8GT4XS::1.4x,NBS5200- 5100-48GT4SFP::1.0x,NBS5100-48GT4SFP::1.1x,NBS5100-48GT4SFP::1.2x,NBS5100- 48GT4SFP::2.0x,NBS5100-48GT4SFP::2.1x,NBS5100-24GT4SFP::1.0x,NBS5100- 24GT4SFP::1.3x,NBS5100-24GT4SFP::1.4x,NBS5100-24GT4SFP::2.0x,NBS5100- 24GT4SFP::2.1x
ReyeeOS 1.218.2428	12.66	2023-01-05 19:43		RAP2260(G)::1.00,RAP2260(G)::1.xx,RAP2260(G)::2.00,RAP2260(G)::2.xx,RAP2260(G)::3.00,RAP2260(G)::3.xx,,EAP262(G)::1.00,EAP262(G)::1.xx AP262(G)::2.00,EAP262(G)::2.xx,EAP262(G)::3.00,EAP262(G)::3.xx
ReyeeOS 1.202.2423	11.61	2022-12-27 14:48		EG105G::1.00,EG105G-P::1.00,EG105G::1.xx,EG105G-P::1.xx,EG105G::2.xx,EG105G-P::2.xx
ReyeeOS 1.204.2414	9.66	2022-12-22 10:12		EW1200G-PRO::1.00,EW1200G-PRO::1.xx,EW1200G-PRO::2.xx,
ReyeeOS 1.206.2216	11.66	2022-11-30 15:02		NBS3200-24GT4XS::1.0x,NBS3200-24GT4XS::1.1x,NBS3200-24GT4XS::1.2x,NBS3200-24GT4XS::1.3x,NBS3200-24GT4XS::1.4x,NBS3200- 24GT4XS::1.5x,NBS3200-24GT4XS::1.6x,NBS3200-24GT4XS::2.0x,NBS3200-24GT4XS::2.1x,NBS3200-24GT4XS-P::1.0x,NBS3200-24GT4XS- P::1.1x,NBS3200-24GT4XS-P::1.2x,NBS3200-24GT4XS-P::1.3x,NBS3200-24GT4XS-P::1.4x,NBS3200-24GT4XS-P::1.5x,NBS3200-24GT4XS- P::2.0x,NBS3200-24GT4XS-P::2.1x,NBS3200-48GT4XS::1.0x,NBS3200-48GT4XS::1.1x,NBS3200-48GT4XS::1.2x,NBS3200-48GT4XS::1.3x,NBS320 48GT4XS::1.4x,NBS3200-48GT4XS::2.0x,NBS3200-48GT4XS::2.1x,NBS3200-48GT4XS-P::1.0x,NBS3200-48GT4XS-P::1.1x,NBS3200-48GT4XS- P::1.2x,NBS3200-48GT4XS-P::1.3x,NBS3200-48GT4XS-P::1.4x,NBS3200-48GT4XS-P::1.5x,NBS3200-48GT4XS-P::2.0x,NBS3200-48GT4XS- P::2.1x,NBS3200-24SFP/8GT4XS::1.0x,NBS3200-24SFP/8GT4XS::1.1x,NBS3200-24SFP/8GT4XS::1.2x,NBS3200-24SFP/8GT4XS::1.3x,NBS3200-

Upload Version File

Upload a tar.gz or .bin file. (Note: Upload a tar.gz file for upgrading the gateway or firewall. The bin file uploaded by an individual cannot be used for upgrade on Ruijie Cloud.



Name	Date modified
SWITCH_3.0(1)B11P218_NBS5000_09241902.tar.gz	12/19/2022 5:09 PM
EG_3.0(1)B11P86_EG210G_09192907_install.bin	7/29/2022 7:30 AM
EW_3.0(1)B11P59_E12_09140807.tar.gz	2/17/2022 2:33 PM
NGFW_NTOS1.0R1_Z5100_02132713_install.bin	1/27/2022 1:59 PM
AC_RGOS11.9(6)B5_G6C4-01-FULL_08203114_install.bin	11/24/2021 6:09 PM
MA_1.0(1)B4_MA2822_[qishan-cucc-main]_08161611.bin	4/16/2021 5:26 PM
MA_1.0(1)B4_MA2822_[qishan-cucc-main]_08161502.bin	4/16/2021 3:47 PM
MA_1.0(1)B4_MA2822_[qishan-cucc-main]-FULL_08161502.bin	4/16/2021 3:45 PM

File name:

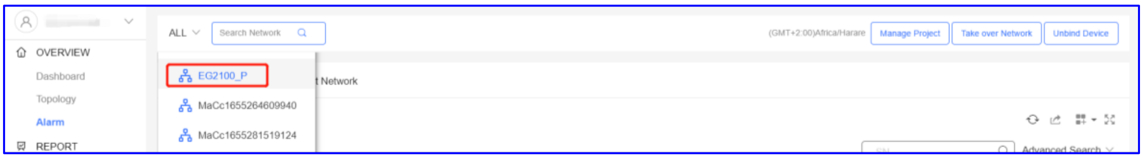
Custom Files (*.bin;*.tar.gz)

13.8 Configuring Alarms

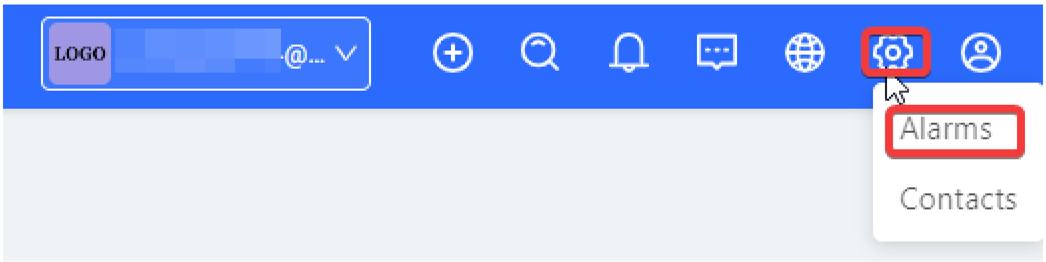
Click ⚙ at the upper right corner, and click **Alarm**. When no alarm is configured, global settings are used. On the **Alarm Settings** page, you can specify whether to enable or disable alarms and how the alarms should be received.

Procedure

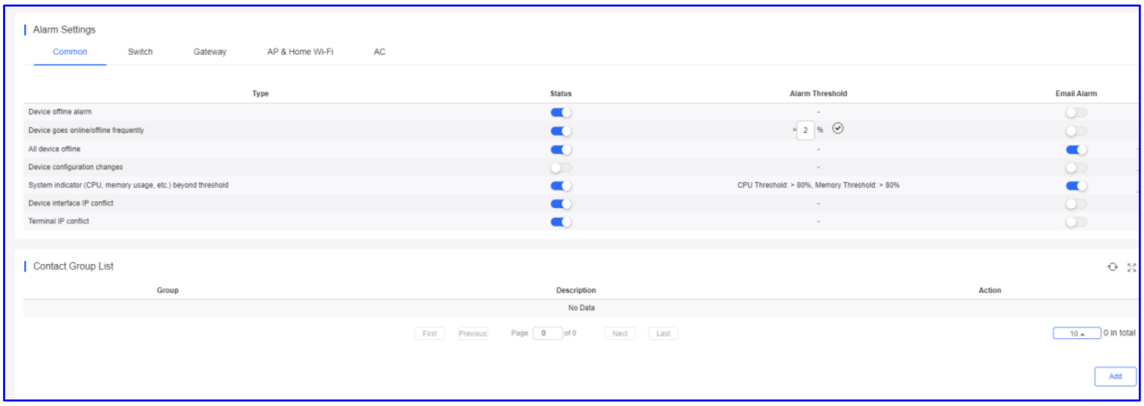
(1) Select one project in this account.



(2) Click ⚙ at the upper right corner and click **Alarm Settings**.



(3) Set alarm parameters.



Alarm Settings

Common | Switch | Gateway | AP & Home Wi-Fi | AC

Type	Status	Alarm Threshold	Email Alarm
Device offline alarm	●	-	○
Device goes online/offline frequently	●	> 2 %	○
All device offline	●	-	●
Device configuration changes	○	-	○
System indicator (CPU, memory usage, etc.) beyond threshold	●	CPU Threshold: > 80%, Memory Threshold: > 80%	●
Device interface IP conflict	●	-	○
Terminal IP conflict	●	-	○

Contact Group List

Group	Description	Action
No Data		

First Previous Page 0 of 0 Next Last 10 0 in total

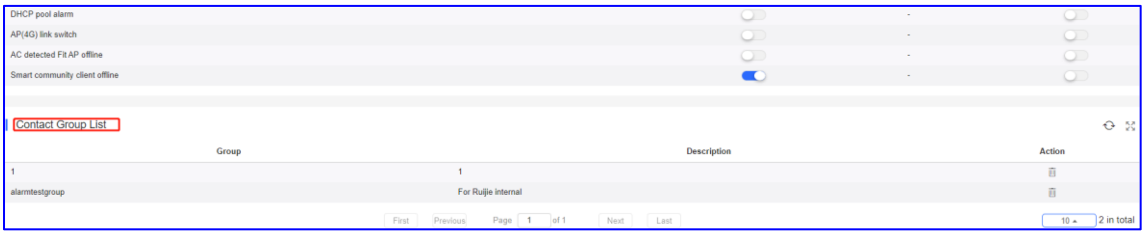
Add

Type: indicates the type of alarms.

Status: indicates whether to enable the function. If the function is enabled, alarm information is displayed on the alarm page.

Alarm Threshold: indicates the alarm threshold.

Email Alarm: indicates that alarms will be pushed to the contacts in **Contact Group List** of the network through the email when **Email Alarm** and **Status** are enabled.



DHCP pool alarm	○	-	○
AP(4G) link switch	○	-	○
AC detected Fit AP offline	○	-	○
Smart community client offline	●	-	○

Contact Group List

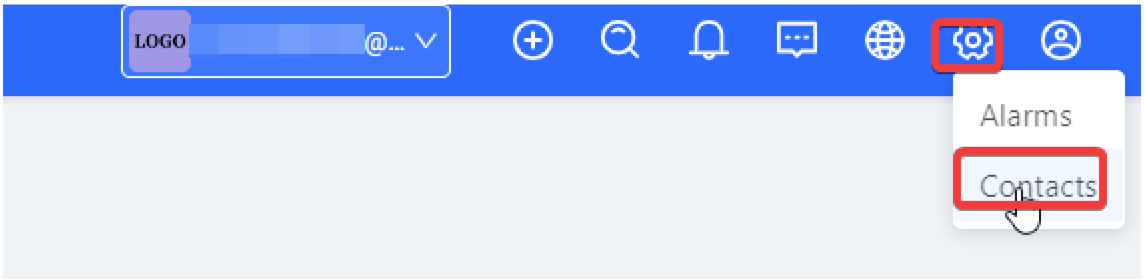
Group	Description	Action
1	1	🗑
alarmtestgroup	For Ruijie internal	🗑

First Previous Page 1 of 1 Next Last 10 2 in total

13.9 Managing Contacts

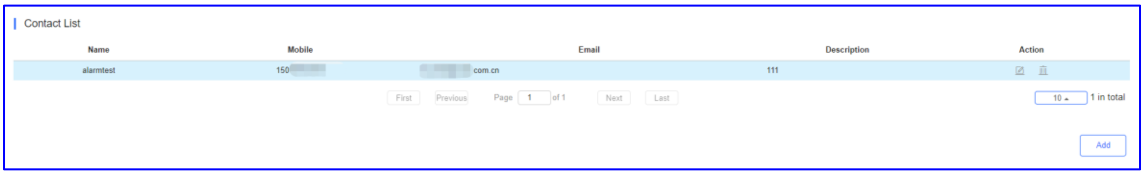
Procedure

Click ⚙ at the upper right corner, and click **Contact** to access **Contact List** and **Contact Group**.



- **Contact List**

  In the **Contact List** area, you can add contacts and contact groups that will receive the alarm emails.



Contact List

Name	Mobile	Email	Description	Action
alarmtest	150[redacted]	[redacted]com.cn	111	✎ 🗑

Name: displays the customized name of a contact.

Mobile: displays the mobile number of a contact.

Email: displays the email address of a contact.

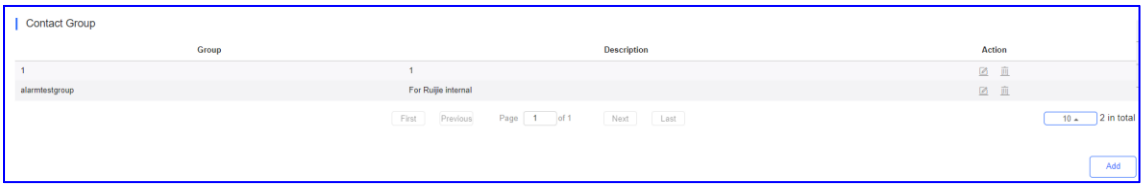
Description: describes the contact.

Action: indicates the operation for the contact. The value is **Edit** or **Delete**. After clicking **Edit**, you can edit contact information in the displayed window.

Add: adds a contact to the contact list.

- **Contact Group**

  In the **Contact Group** area, you can add a group and move the contacts to the group.



Contact Group

Group	Description	Action
1	1	✎ 🗑
alarmtestgroup	For Ruijie internal	✎ 🗑

Group: displays the customized name of the group.

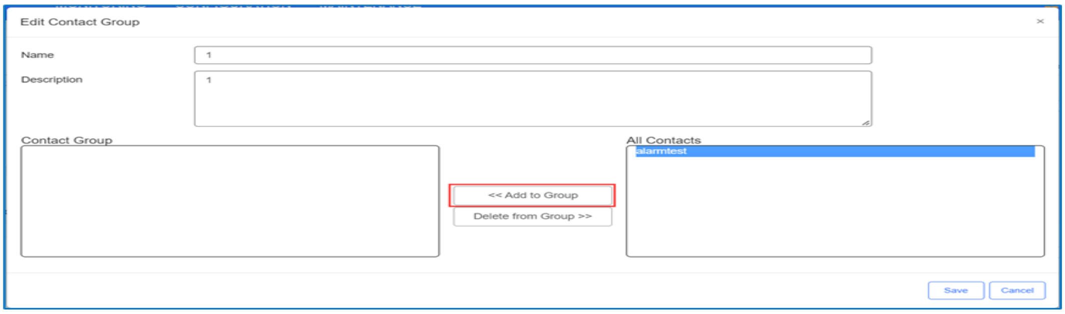
Description: displays some words to describe the contact group.

Action: indicates the operation for the contact group. The value is **Edit** or **Delete**.

Add: adds a contact group to the contact group list.

After clicking **Edit**, you can edit contact group information in the displayed window. The value is **Add to Group** or **Delete from Group**.

- **Add to Group**: adds the selected contacts in **All Contacts** to the contact group.



Edit Contact Group

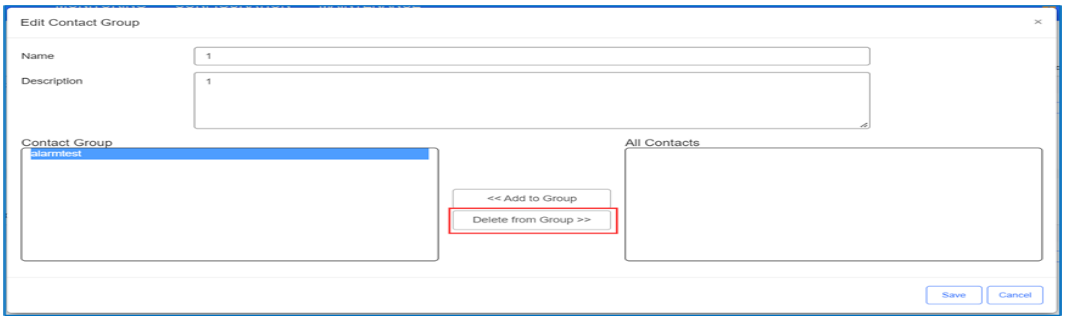
Name: 1

Description: 1

Contact Group

All Contacts: alarmtest

- **Delete from Group**: deletes the selected contacts from **Contact Group**.



Edit Contact Group ×

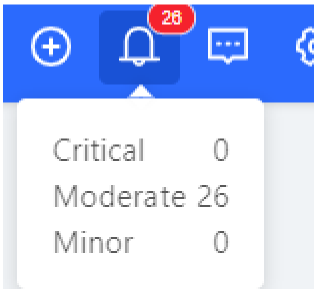
Name: 1

Description: 1

Contact Group: alarmtest

All Contacts

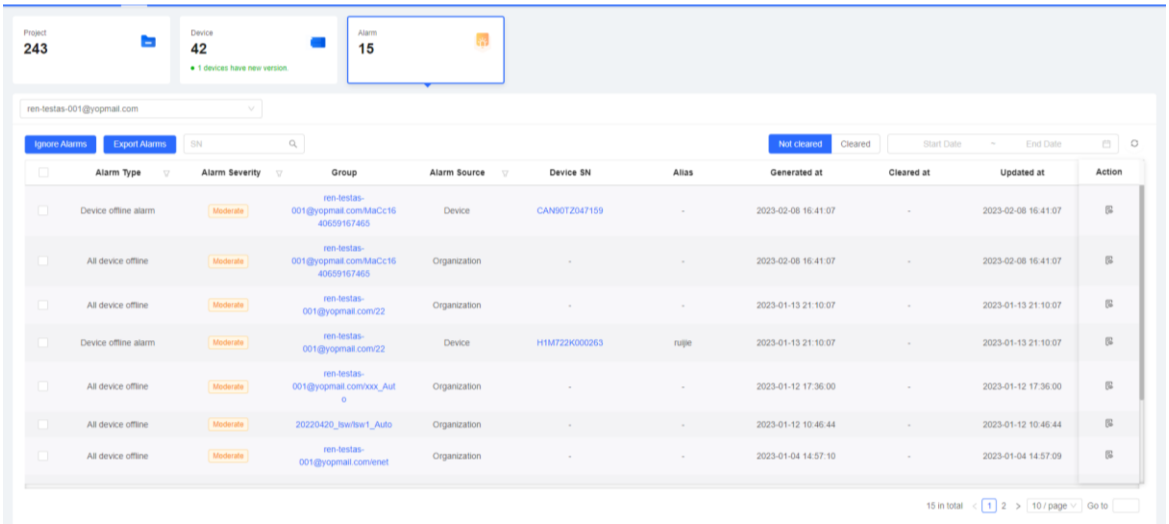
13.10 Viewing the Number of Global Alarms Quickly



Critical	0
Moderate	26
Minor	0

13.11 Viewing Details About Global Alarms

Click **Home** > **Alarm**



Project 243

Device 42
- 1 devices have new version.

Alarm 15

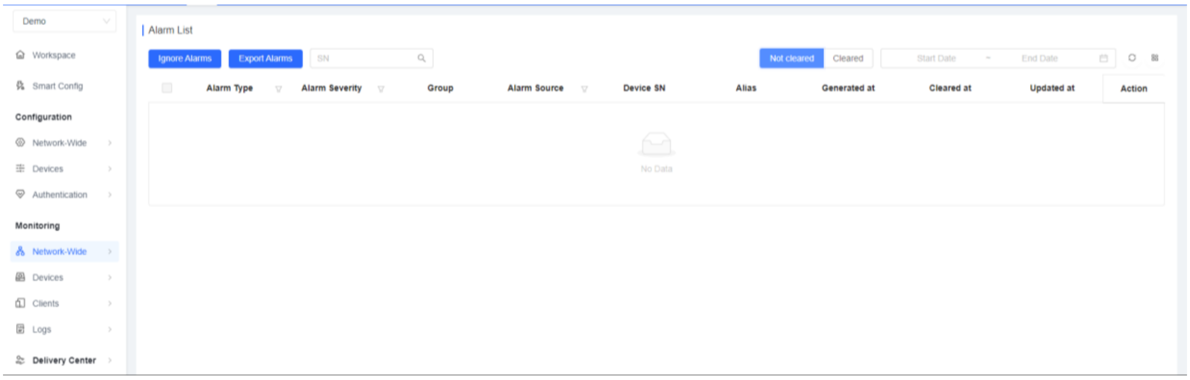
ren-testas-001@yopmail.com

□	Alarm Type	Alarm Severity	Group	Alarm Source	Device SN	Alias	Generated at	Cleared at	Updated at	Action
□	Device offline alarm	Moderate	ren-testas-001@yopmail.com/MaCc1640659167465	Device	CAN90TZ047159	-	2023-02-08 16:41:07	-	2023-02-08 16:41:07	
□	All device offline	Moderate	ren-testas-001@yopmail.com/MaCc1640659167465	Organization	-	-	2023-02-08 16:41:07	-	2023-02-08 16:41:07	
□	All device offline	Moderate	ren-testas-001@yopmail.com/22	Organization	-	-	2023-01-13 21:10:07	-	2023-01-13 21:10:07	
□	Device offline alarm	Moderate	ren-testas-001@yopmail.com/22	Device	H1M722K000263	ruijie	2023-01-13 21:10:07	-	2023-01-13 21:10:07	
□	All device offline	Moderate	ren-testas-001@yopmail.com/xxx_Auto	Organization	-	-	2023-01-12 17:36:00	-	2023-01-12 17:36:00	
□	All device offline	Moderate	20220420_lsw/lsw1_Auto	Organization	-	-	2023-01-12 10:46:44	-	2023-01-12 10:46:44	
□	All device offline	Moderate	ren-testas-001@yopmail.com/enet	Organization	-	-	2023-01-04 14:57:10	-	2023-01-04 14:57:09	

15 in total < 1 2 > 10 / page Go to

13.12 Viewing Alarms of a Project

Choose **Project** > **Monitoring** > **Network-Wide** > **Alarm**.



□	Alarm Type	Alarm Severity	Group	Alarm Source	Device SN	Alias	Generated at	Cleared at	Updated at	Action
No Data										

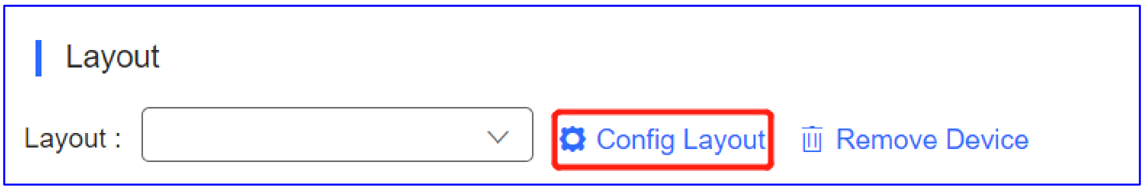
13.13 Layout

Layout is used to identify the AP location.

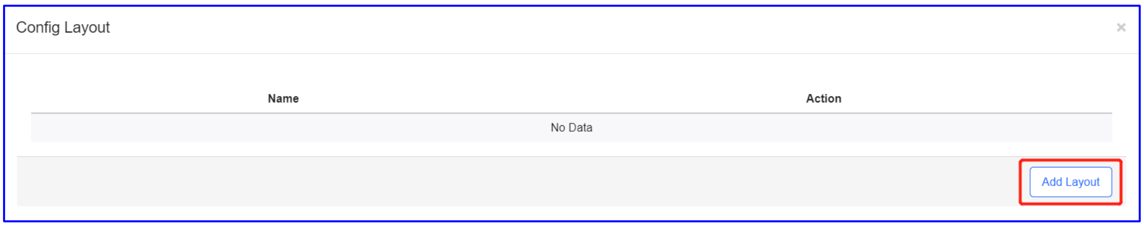
Procedure

(1) Choose **CONFIGURATION** > **WIRELESS** > **Layout** and select a network in this account.

(2) Click **Config Layout** in the **Layout** area.

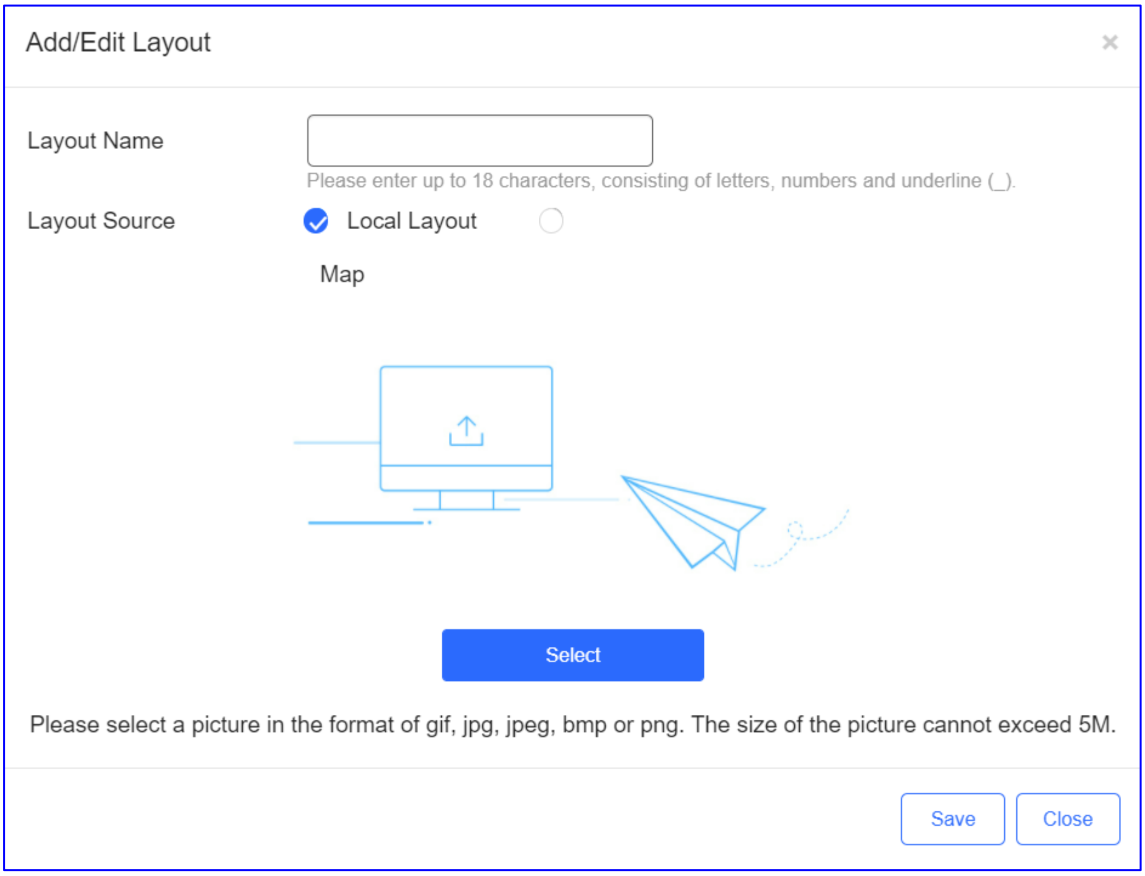


(3) Click **ADD Layout** on the **Config Layout** page.



Name	Action
No Data	

(4) Set parameters of the layout and click **Save**.



Add/Edit Layout

Layout Name

Please enter up to 18 characters, consisting of letters, numbers and underline (_).

Layout Source ● Local Layout ○ Map

Please select a picture in the format of gif, jpg, jpeg, bmp or png. The size of the picture cannot exceed 5M.

Layout Name: Enter up to 18 characters, consisting of letters, numerals, and underlines (_).

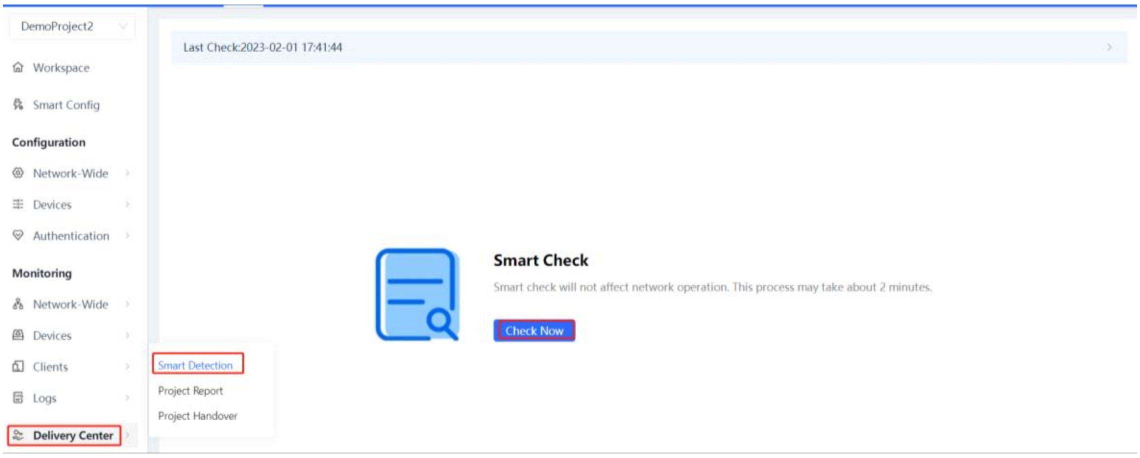
Layout Source: Select a local layout or map.

- **Local Layout**: Select a picture in the format of gif, jpg, jpeg, bmp, or png on the local PC. The size of the picture cannot exceed 5 MB.
- **Map**: Enter a location name for **Bind Location**.

14 Project Delivery

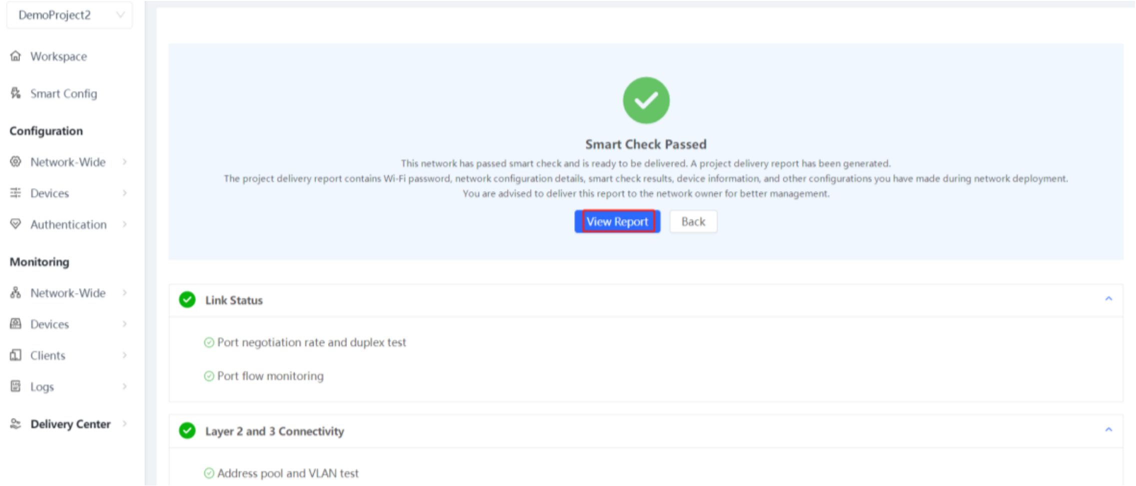
14.1 Smart Detection

Choose **Delivery Center** > **Smart Detection** > **Check Now** to generate a project delivery report.



Smart check will not affect network operation. This process may take about 2 minutes.

After a project delivery report is generated, click **View Report** to view the report.



This network has passed smart check and is ready to be delivered. A project delivery report has been generated.
The project delivery report contains Wi-Fi password, network configuration details, smart check results, device information, and other configurations you have made during network deployment.
You are advised to deliver this report to the network owner for better management.

14.2 Project Report

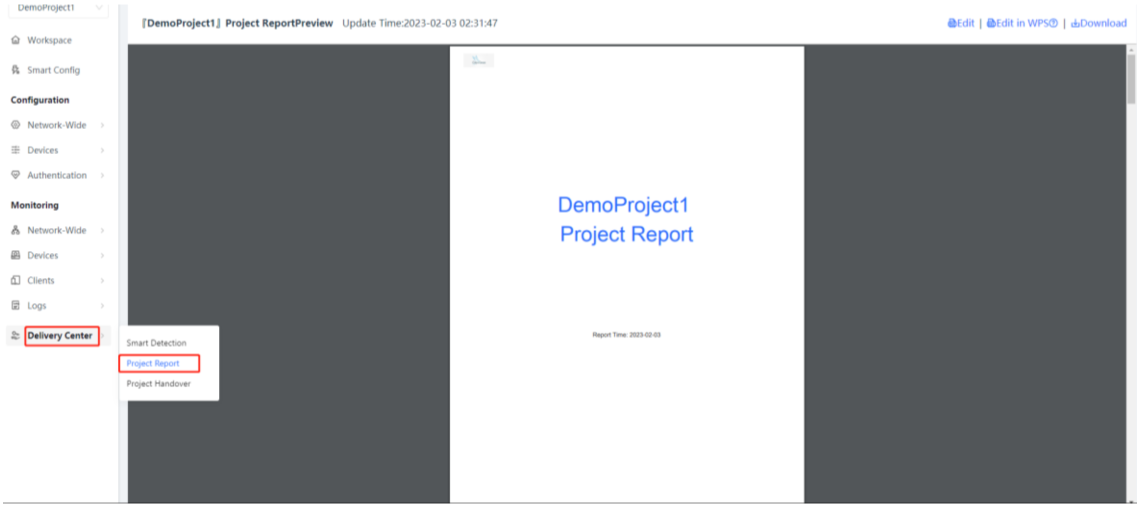
14.2.1 Applicable Scenarios

After project deployment is completed, a delivery report needs to be submitted to the owner, which often requires considerable testing and writing time. This function can conduct intelligent check, summarize all types of information and check results, and automatically generate a project delivery report in both PDF and Word formats. The report covers basic information, general solution, intelligent configuration check results, device list, and topology.

After the project deployment is completed, a report can be offered to the owner. The report can provide the revised project network device overview and delivery time, customized company logo, company name, and project introduction, show the topology of the whole project, and supplement other vendors' devices to the device list. The report can be in PDF and Word formats.

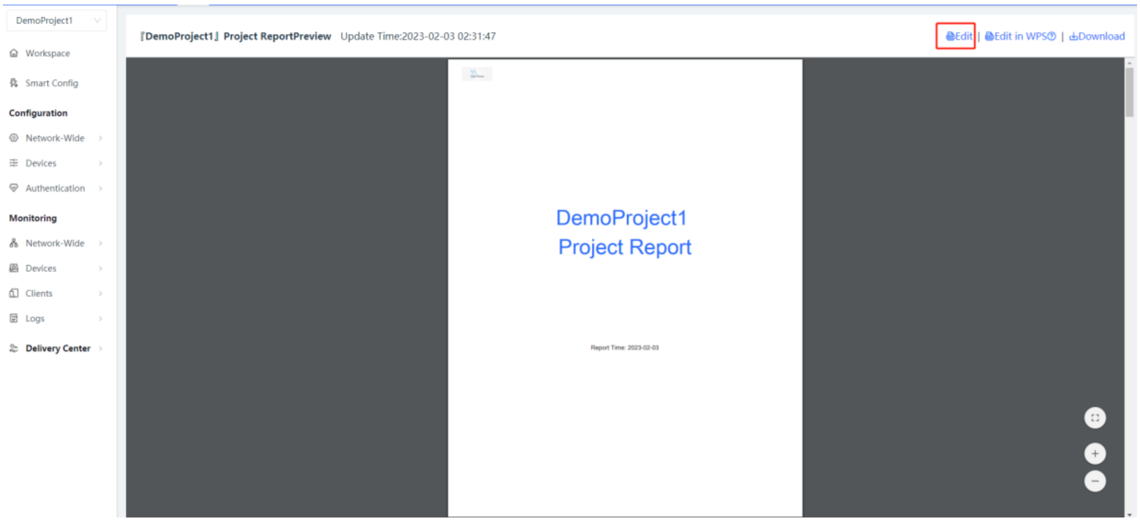
14.2.2 Configuration Steps

1. Choose **Project** > **Delivery Center** > **Project Report** to view the latest delivery report of the current project.

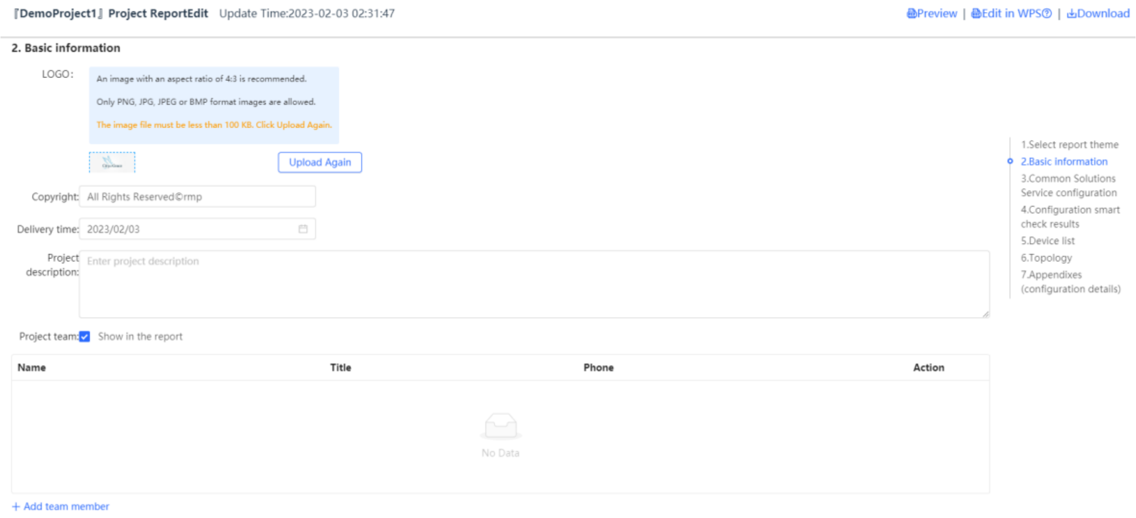


『DemoProject1』 Project ReportPreview Update Time:2023-02-03 02:31:47

2. Click **Edit** at the upper right corner to edit basic information in the project report.



『DemoProject1』 Project ReportPreview Update Time:2023-02-03 02:31:47



『DemoProject1』 Project ReportEdit Update Time:2023-02-03 02:31:47

2. Basic information

LOGO:

An image with an aspect ratio of 4:3 is recommended.

Only PNG, JPG, JPEG or BMP format images are allowed.

The image file must be less than 100 KB. Click Upload Again.

Copyright: All Rights Reserved©rmp

Delivery time: 2023/02/03

Project description: Enter project description

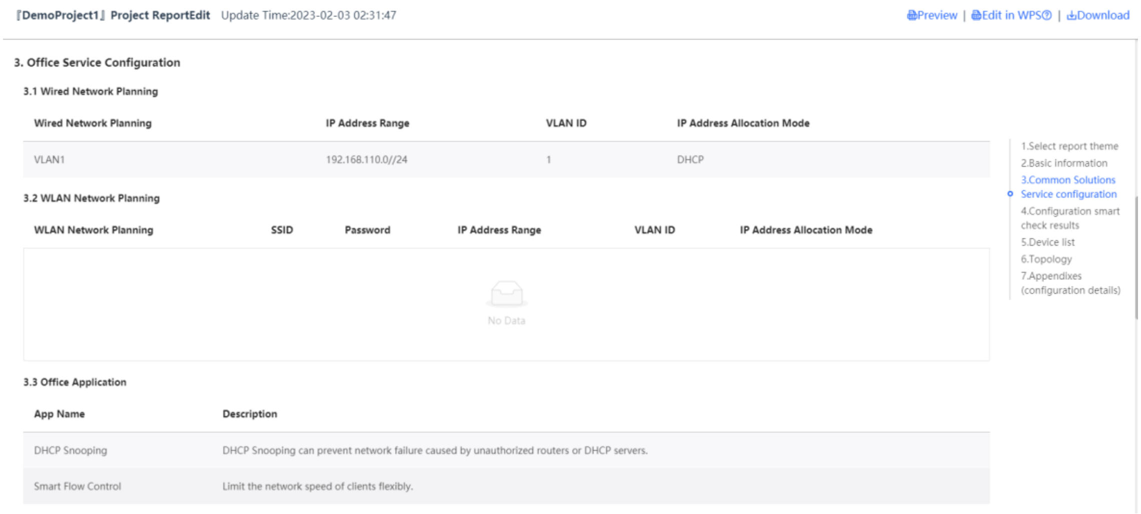
Project team: ☑ Show in the report

Name	Title	Phone	Action

No Data

Preview | Edit in WPS | Download
Upload Again
+ Add team member
1.Select report theme
2.Basic information
3.Common Solutions Service configuration
4.Configuration smart check results
5.Device list
6.Topology
7.Appendixes (configuration details)

3. You can view service configuration of the general solution in the delivery report.


Preview | Edit in WPS | Download
1.Select report theme
2.Basic information
3.Common Solutions Service configuration
4.Configuration smart check results
5.Device list
6.Topology
7.Appendixes (configuration details)
No Data

『DemoProject1』 Project ReportEdit Update Time:2023-02-03 02:31:47

3. Office Service Configuration

3.1 Wired Network Planning

Wired Network Planning	IP Address Range	VLAN ID	IP Address Allocation Mode
VLAN1	192.168.110.0//24	1	DHCP

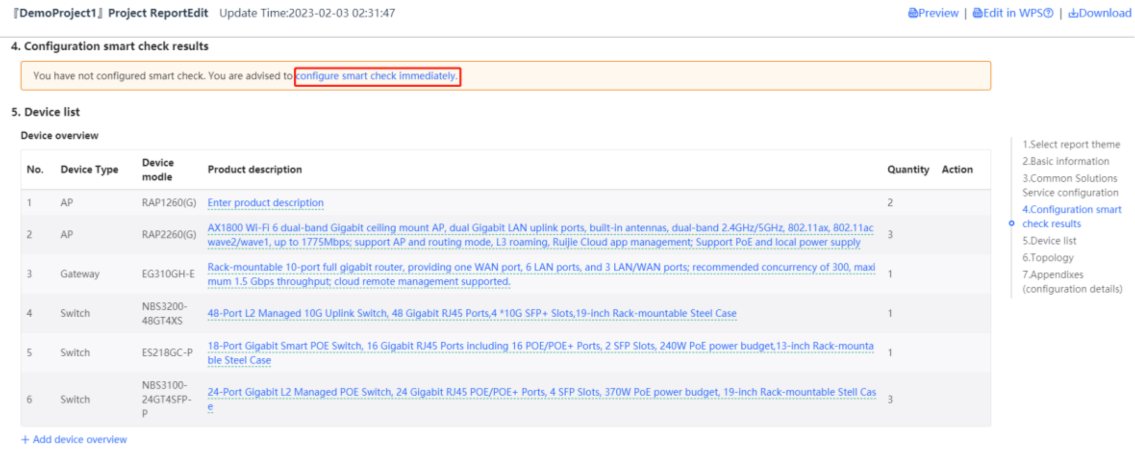
3.2 WLAN Network Planning

WLAN Network Planning	SSID	Password	IP Address Range	VLAN ID	IP Address Allocation Mode

3.3 Office Application

App Name	Description
DHCP Snooping	DHCP Snooping can prevent network failure caused by unauthorized routers or DHCP servers.
Smart Flow Control	Limit the network speed of clients flexibly.

4. Checking the network intelligently: Click **Configure smart check immediately**. The page automatically redirects to **Smart Detection**.


Preview | Edit in WPS | Download
1.Select report theme
2.Basic information
3.Common Solutions Service configuration
4.Configuration smart check results
5.Device list
6.Topology
7.Appendixes (configuration details)
+ Add device overview

『DemoProject1』 Project ReportEdit Update Time:2023-02-03 02:31:47

4. Configuration smart check results

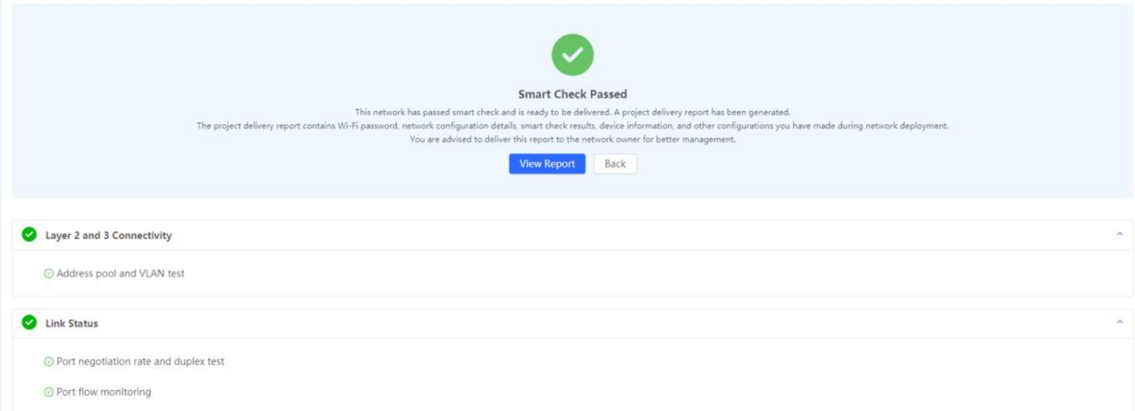
You have not configured smart check. You are advised to configure smart check immediately.

5. Device list

Device overview

No.	Device Type	Device modle	Product description	Quantity	Action
1	AP	RAP1260(G)	Enter product description	2	
2	AP	RAP2260(G)	AX1800 Wi-Fi 6 dual-band Gigabit ceiling mount AP, dual Gigabit LAN uplink ports, built-in antennas, dual-band 2.4GHz/5GHz, 802.11ax, 802.11ac wave2/wave1, up to 1775Mbps; support AP and routing mode, L3 roaming, Ruijie Cloud app management; Support PoE and local power supply	3	
3	Gateway	EG310GH-E	Rack-mountable 10-port full gigabit router, providing one WAN port, 6 LAN ports, and 3 LAN/WAN ports; recommended concurrency of 300, maximum 1.5 Gbps throughput; cloud remote management supported.	1	
4	Switch	NBS3200-48GT4XS	48-Port L2 Managed 10G Uplink Switch, 48 Gigabit RJ45 Ports,4 *10G SFP+ Slots,19-inch Rack-mountable Steel Case	1	
5	Switch	ES218GC-P	18-Port Gigabit Smart POE Switch, 16 Gigabit RJ45 Ports including 16 POE/POE+ Ports, 2 SFP Slots, 240W PoE power budget,13-inch Rack-mountable Steel Case	1	
6	Switch	NBS3100-24GT4SFP-P	24-Port Gigabit L2 Managed POE Switch, 24 Gigabit RJ45 POE/POE+ Ports, 4 SFP Slots, 370W PoE power budget, 19-inch Rack-mountable Stell Case	3	

5. Click **Check Now**.



Smart Check Passed

This network has passed smart check and is ready to be delivered. A project delivery report has been generated.
The project delivery report contains Wi-Fi password, network configuration details, smart check results, device information, and other configurations you have made during network deployment.
You are advised to deliver this report to the network owner for better management.

✓ Layer 2 and 3 Connectivity

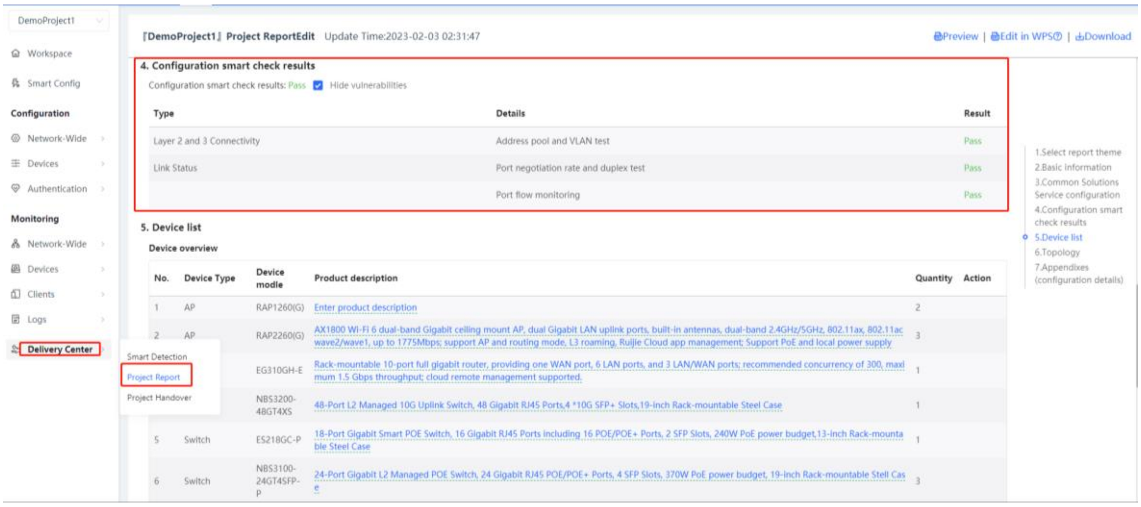
✓ Address pool and VLAN test

✓ Link Status

✓ Port negotiation rate and duplex test

✓ Port flow monitoring

6. After check, go to **Project** > **Delivery Center** > **Project Report** > **Edit**. The check results of functions supported by the network will be automatically incorporated into the delivery report.



『DemoProject1』 Project ReportEdit Update Time:2023-02-03 02:31:47

4. Configuration smart check results

Configuration smart check results: Pass ☑ Hide vulnerabilities

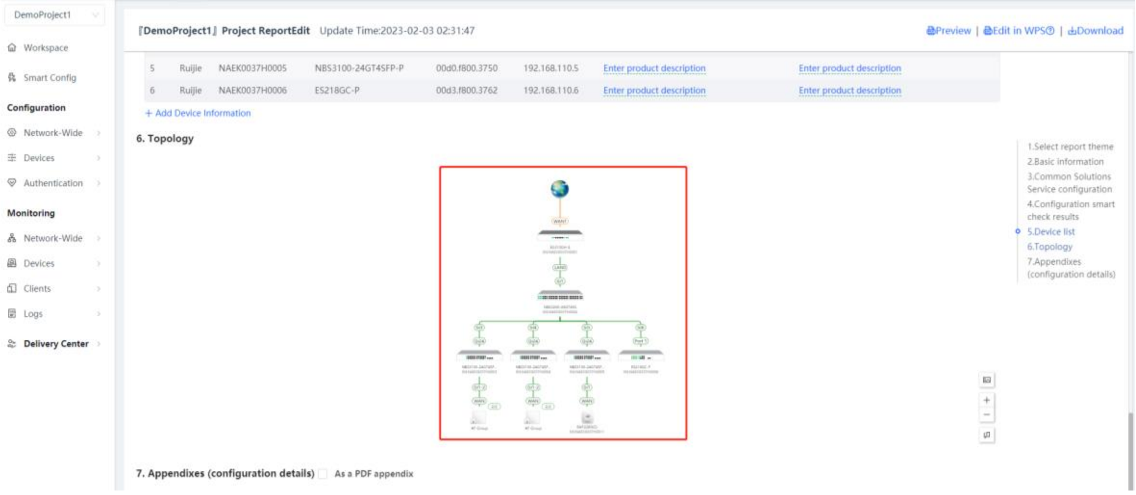
Type	Details	Result
Layer 2 and 3 Connectivity	Address pool and VLAN test	Pass
Link Status	Port negotiation rate and duplex test	Pass
	Port flow monitoring	Pass

5. Device list

Device overview

No.	Device Type	Device modle	Product description	Quantity	Action
1	AP	RAP1260(G)	Enter product description	2	
2	AP	RAP2260(G)	AX1800 Wi-Fi 6 dual-band Gigabit ceiling mount AP, dual Gigabit LAN uplink ports, built-in antennas, dual-band 2.4GHz/5GHz, 802.11ax, 802.11ac wave2/wave1, up to 1775Mbps; support AP and routing mode, L3 roaming, Ruijie Cloud app management; Support PoE and local power supply	3	
		EG310GH-E	Rack-mountable 10-port full gigabit router, providing one WAN port, 6 LAN ports, and 3 LAN/WAN ports; recommended concurrency of 300, maximum 1.5 Gbps throughput; cloud remote management supported.	1	
		NBS3200-48GT4XS	48-Port L2 Managed 10G Uplink Switch, 48 Gigabit RJ45 Ports,4 *10G SFP+ Slots,19-inch Rack-mountable Steel Case	1	
5	Switch	ES218GC-P	18-Port Gigabit Smart POE Switch, 16 Gigabit RJ45 Ports including 16 POE/POE+ Ports, 2 SFP Slots, 240W PoE power budget,13-inch Rack-mountable Steel Case	1	
6	Switch	NBS3100-24GT4SFP-P	24-Port Gigabit L2 Managed POE Switch, 24 Gigabit RJ45 POE/POE+ Ports, 4 SFP Slots, 370W PoE power budget, 19-inch Rack-mountable Stell Case	3	

7. Check the network topology.



『DemoProject1』 Project ReportEdit Update Time:2023-02-03 02:31:47

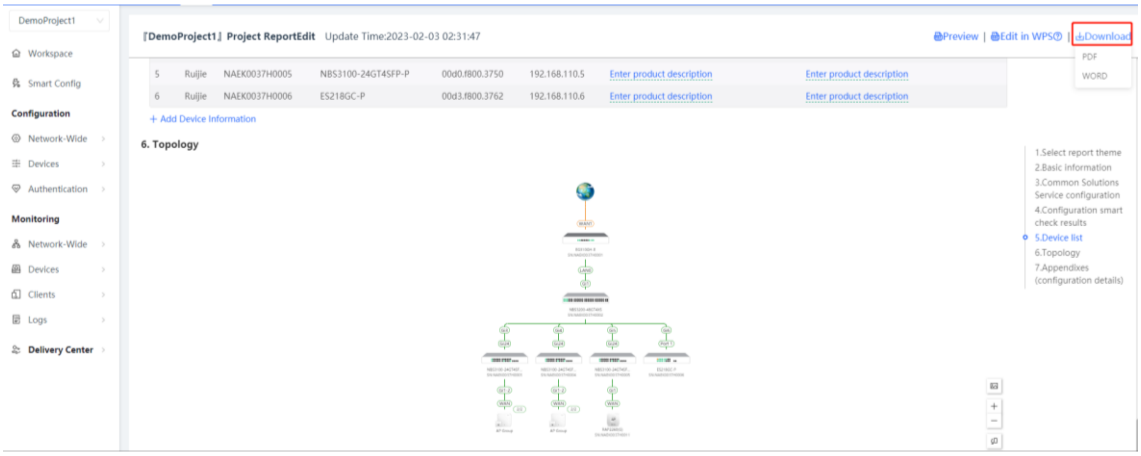
5	Ruijie	NAEK0037H0005	NBS3100-24GT4SFP-P	00d0.f800.3750	192.168.110.5	Enter product description	Enter product description
6	Ruijie	NAEK0037H0006	ES218GC-P	00d3.f800.3762	192.168.110.6	Enter product description	Enter product description

+ Add Device Information

6. Topology

7. Appendixes (configuration details) □ As a PDF appendix

8. Click **Download** at the upper right corner to download the delivery report in PDF and Word formats.



『DemoProject1』 Project ReportEdit Update Time:2023-02-03 02:31:47

5	Ruijie	NAEK0037H0005	NBS3100-24GT4SFP-P	00d0.f800.3750	192.168.110.5	Enter product description	Enter product description
6	Ruijie	NAEK0037H0006	ES218GC-P	00d3.f800.3762	192.168.110.6	Enter product description	Enter product description

+ Add Device Information

6. Topology

14.3 Project Handover

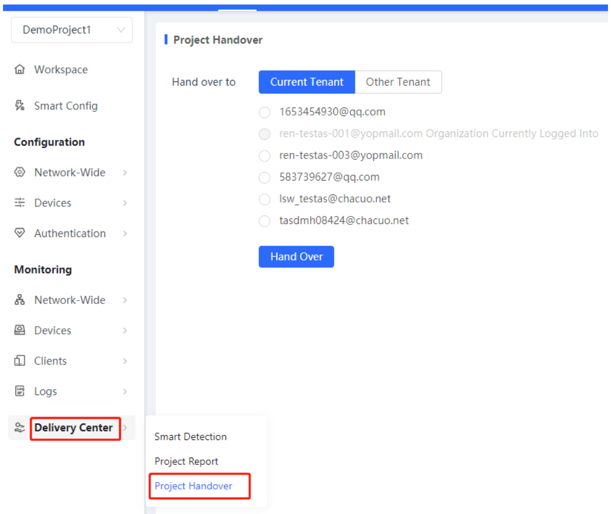
14.3.1 Applicable Scenarios

After-sales technical personnel of channels may be unable to solve some problems during maintenance. In this case, channel technicians generally seek support from Ruijie technical support engineers, who will temporarily need network management permissions for troubleshooting.

You can transfer your network (including devices on the network and device-related configuration) to other accounts. You can also share a network with other accounts. Read/write permission and read-only permission can be configured for sharing. The read-only permission is used for monitoring requirements while the read/write permission is used for troubleshooting requirements.

14.3.2 Configuration Steps

Choose **Delivery Center** > **Project Handover** to hand a project over to a contact in **Current Tenant**.



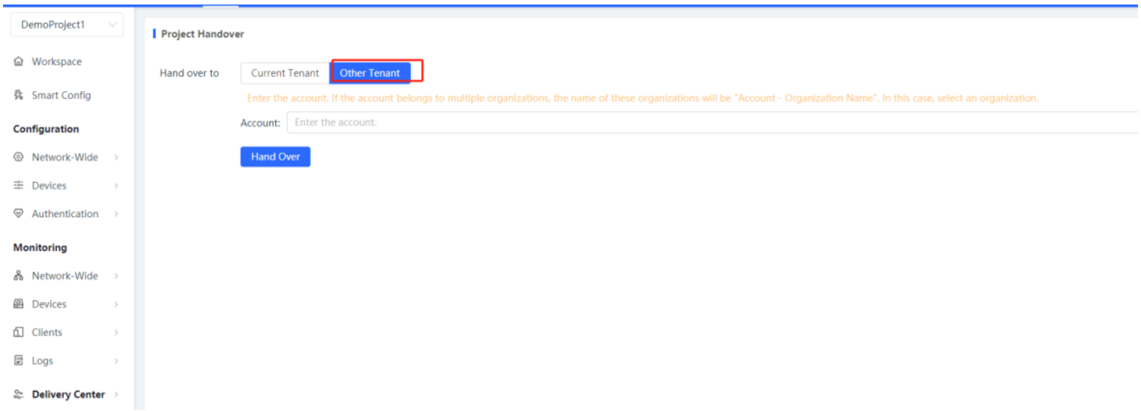
Project Handover

Hand over to: Current Tenant | Other Tenant

○ 1653454930@qq.com
○ ren-testas-001@yopmail.com Organization Currently Logged Into
○ ren-testas-003@yopmail.com
○ 583739627@qq.com
○ lsw_testas@chacuo.net
○ tasdmh08424@chacuo.net

Hand Over

You can also click **Other Tenant**. Enter a complete account for search, select the target account, and hand the project over to the account.



Project Handover

Hand over to: Current Tenant | Other Tenant

Enter the account. If the account belongs to multiple organizations, the name of these organizations will be "Account - Organization Name". In this case, select an organization.

Account: Enter the account.

Hand Over

15 Linking Between RG-OCE NM and IM Platforms

15.1 Background

Linking the RG-OCE Network Manager (NM) platform with the RG-OCE Identity Manager (IM) platform allows users to access both platforms through single sign-on (SSO).

15.2 Procedure

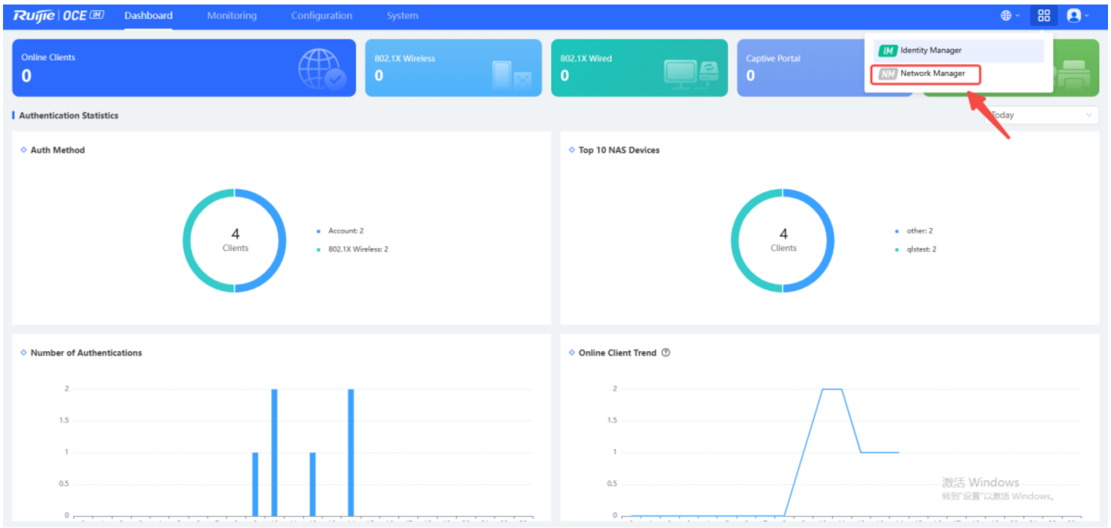
(1) Log in to the IM platform to obtain the account linking code as instructed.

(2) Then, log in to the NM platform and paste the code to complete the linking process.

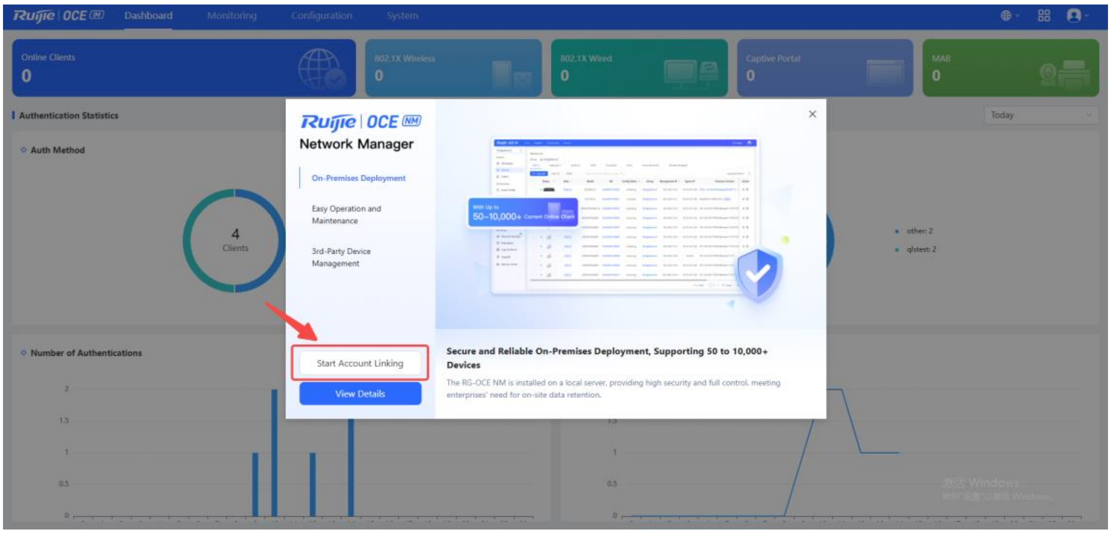
15.3 Configuration Steps

15.3.1 Operations on the IM Platform

1. **Click the Switch Platform icon in the upper right corner of the IM platform and select Network Manager from the drop-down list.**



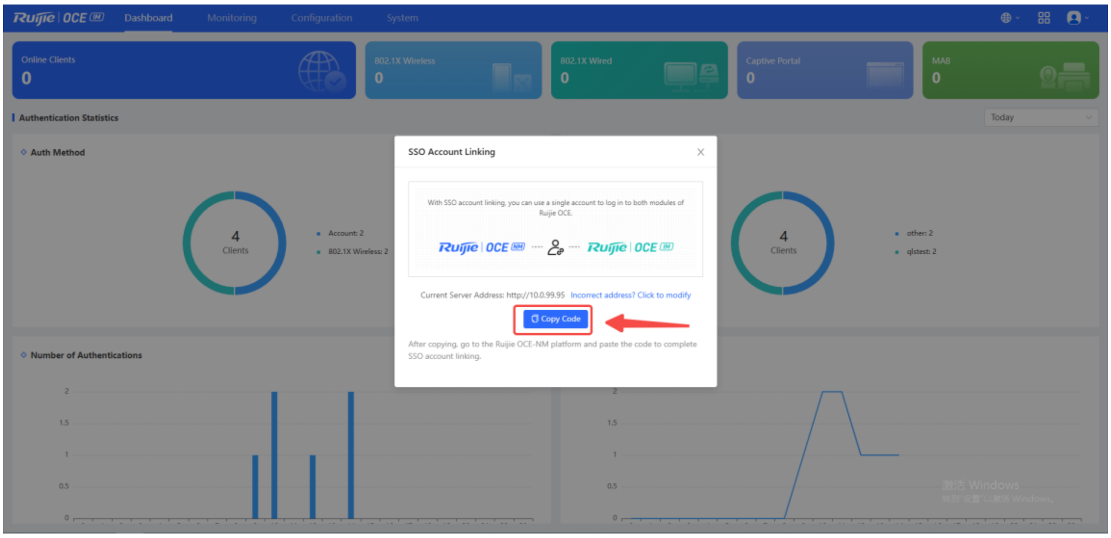
2. **On the displayed window, click Start Account Linking to start the linking process.**



Secure and Reliable On-Premises Deployment, Supporting 50 to 10,000+ Devices

The RG-OCE NM is installed on a local server, providing high security and full control, meeting enterprises' need for on-site data retention.

3. **On the displayed SSO Account Linking window, click Copy Code to obtain the code. The system automatically copies the code to the clipboard.**



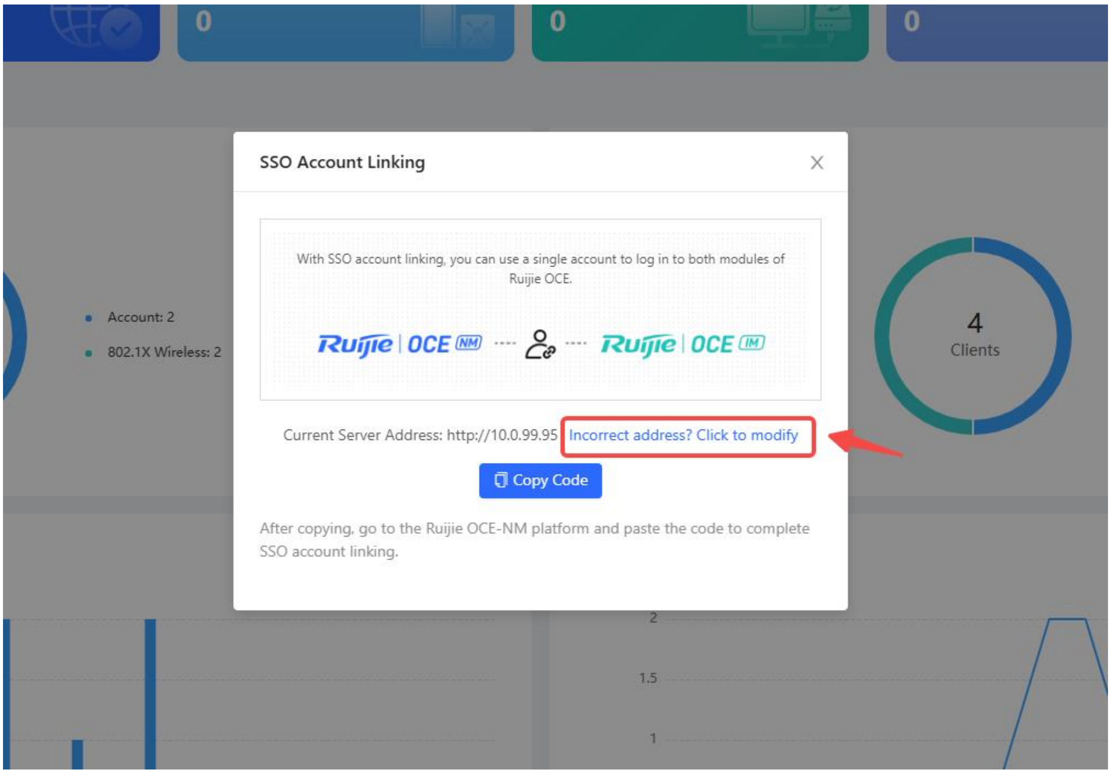
SSO Account Linking

With SSO account linking, you can use a single account to log in to both modules of Ruijie OCE.

Current Server Address: http://10.0.99.95 Incorrect address? Click to modify

After copying, go to the Ruijie OCE-NM platform and paste the code to complete SSO account linking.

4. **If the value of Current Server Address is incorrect, click Incorrect address? Click to modify to modify the server address, as shown in the following figure. After changing the server address, click Copy Code again to obtain the latest code.**



SSO Account Linking

With SSO account linking, you can use a single account to log in to both modules of Ruijie OCE.

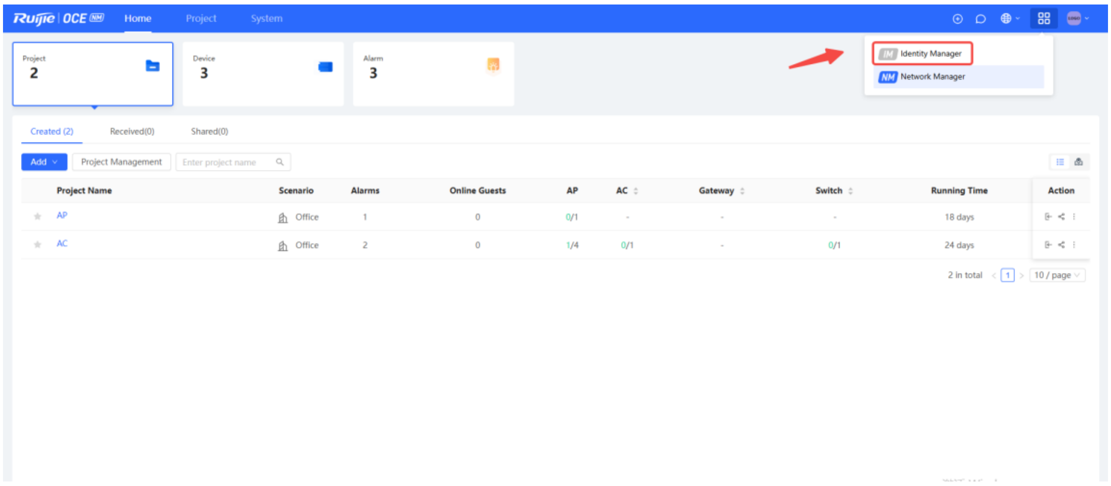
Current Server Address: http://10.0.99.95 Incorrect address? Click to modify

Copy Code

After copying, go to the Ruijie OCE-NM platform and paste the code to complete SSO account linking.

15.3.2 Operations on the NM Platform

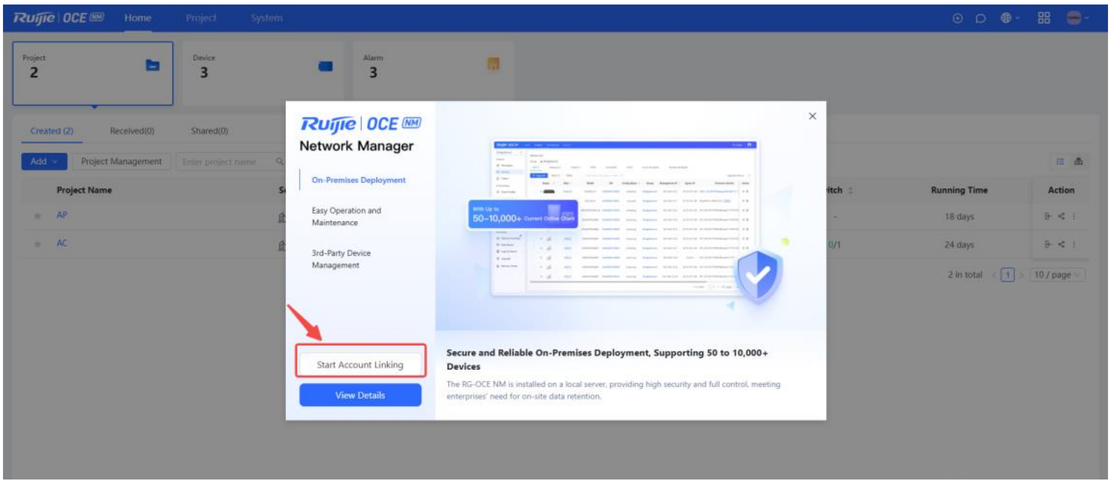
1. **Click the Switch Platform icon in the upper right corner of the NM platform and select Identity Manager from the drop-down list.**



	Project Name	Scenario	Alarms	Online Guests	AP	AC	Gateway	Switch	Running Time	Action
★	AP	Office	1	0	0/1	-	-	-	18 days	
★	AC	Office	2	0	1/4	0/1	-	0/1	24 days	

2 in total 1 10 / page

2. **On the displayed window, click Start Account Linking to start the linking process.**



Ruijie | OCE NM

Network Manager

On-Premises Deployment

Easy Operation and Maintenance

3rd-Party Device Management

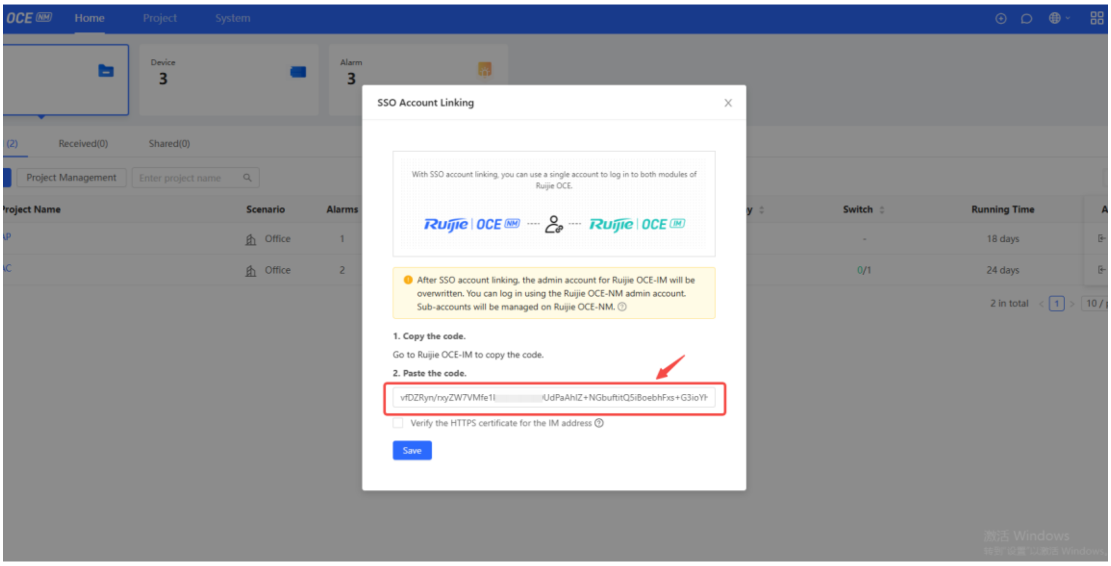
Start Account Linking

View Details

Secure and Reliable On-Premises Deployment, Supporting 50 to 10,000+ Devices

The RG-OCE NM is installed on a local server, providing high security and full control, meeting enterprises' need for on-site data retention.

3. **On the displayed SSO Account Linking window, paste the code obtained from the IM platform to the specified input box, and click Save.**



SSO Account Linking

With SSO account linking, you can use a single account to log in to both modules of Ruijie OCE.

After SSO account linking, the admin account for Ruijie OCE-IM will be overwritten. You can log in using the Ruijie OCE-NM admin account. Sub-accounts will be managed on Ruijie OCE-NM.

1. Copy the code.

Go to Ruijie OCE-IM to copy the code.

2. Paste the code.

vfDZRyn/rxyZW7VMfe1I[redacted]UdPaAhlZ+NGbuftitQ5iBoebhFxs+G3ioYł

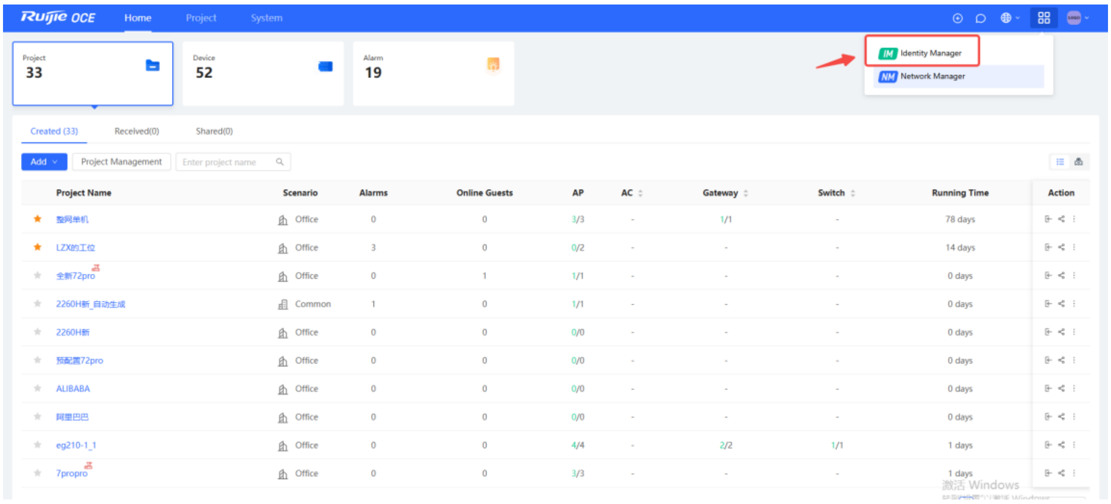
□ Verify the HTTPS certificate for the IM address

Save

If the IM address is a domain name bound to a formal CA certificate, you can check the "Verify the HTTPS certificate for the IM address" option.

4. **Once the binding is successful, log in to the NM platform again.**

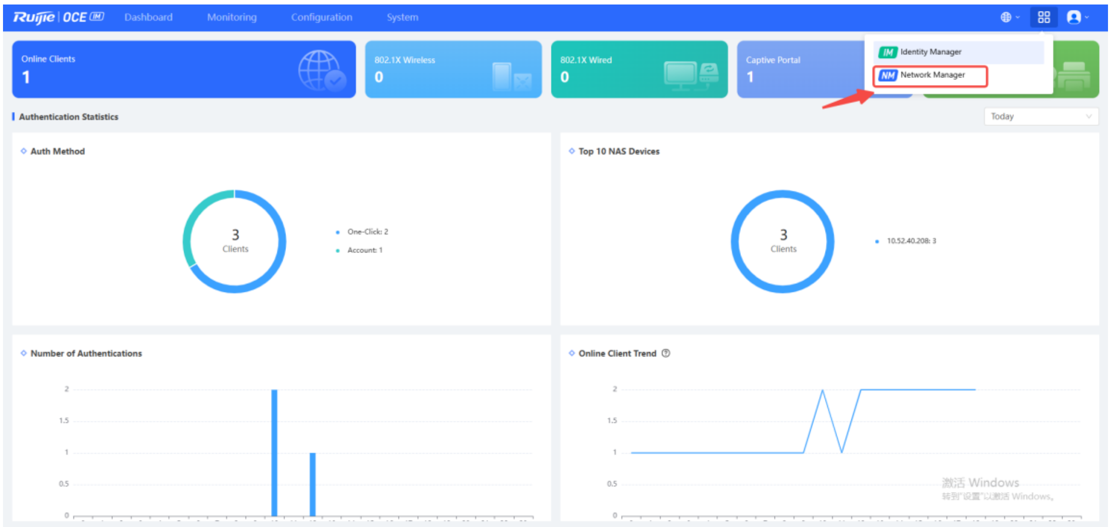
After successful login, you can click the **Switch Platform** icon in the upper right corner and select **Identity Manager** from the drop-down list to switch to the **Identity Manager** platform.



	Project Name	Scenario	Alarms	Online Guests	AP	AC	Gateway	Switch	Running Time	Action
★	整网单机	Office	0	0	3/3	-	1/1	-	78 days	
★	LZX的工位	Office	3	0	0/2	-	-	-	14 days	
☆	全新72pro	Office	0	1	1/1	-	-	-	0 days	
☆	2260H新_自动生成	Common	1	0	1/1	-	-	-	0 days	
☆	2260H新	Office	0	0	0/0	-	-	-	0 days	
☆	预配置72pro	Office	0	0	0/0	-	-	-	0 days	
☆	ALIBABA	Office	0	0	0/0	-	-	-	0 days	
☆	阿里巴巴	Office	0	0	0/0	-	-	-	0 days	
☆	eg210-1_1	Office	0	0	4/4	-	2/2	1/1	1 days	
☆	7propro	Office	0	0	3/3	-	-	-	1 days	

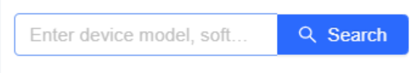
15.3.3 Switch Platform

On the IM platform, you can click the **Switch Platform** icon in the upper right corner and select **Network Manager** from the drop-down list to switch to the **Network Manager** platform.



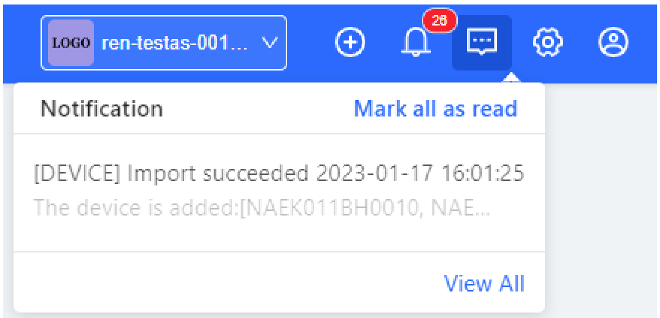
16 Appendix: Frequently-Used Controls

16.1 Quickly locate the table entry you want to find through the drop-down list or by entering a keyword



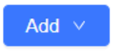
16.1.1 Notification

You can view device go-online and go-offline reminders.



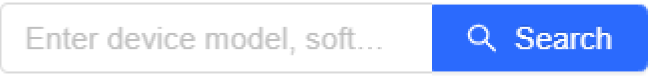
[DEVICE] Import succeeded 2023-01-17 16:01:25
The device is added:[NAEK011BH0010, NAE...

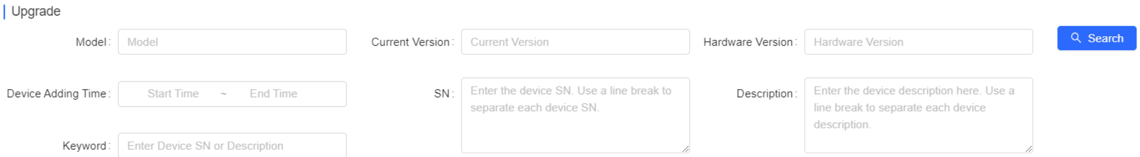
16.1.2 Add



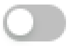
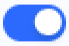
16.1.3 Delete

16.1.4 Quickly locate the table entry you want to find by entering keywords

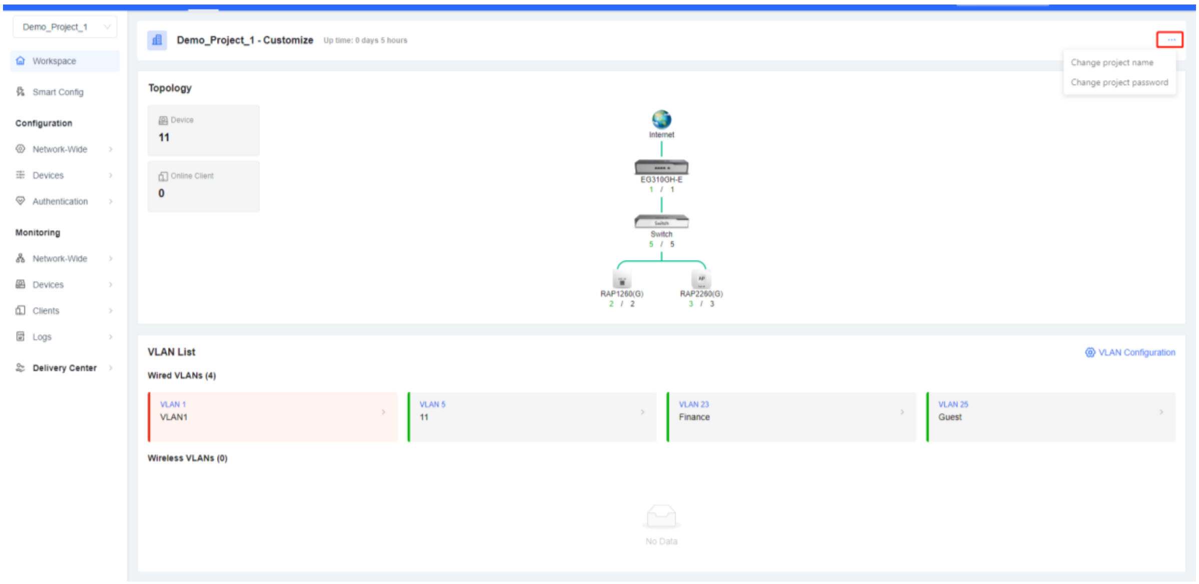



Upgrade
Model:
Model
Current Version:
Current Version
Hardware Version:
Hardware Version
Search
Device Adding Time:
Start Time ~ End Time
SN:
Enter the device SN. Use a line break to separate each device SN.
Description:
Enter the device description here. Use a line break to separate each device description.
Keyword:
Enter Device SN or Description

16.1.5 Status

Disabled:  ; enabled:  . You can click it to switch the status.

16.2 Change Project Name or Password


Demo_Project_1
Workspace
Smart Config
Configuration
Network-Wide
Devices
Authentication
Monitoring
Network-Wide
Devices
Clients
Logs
Delivery Center
Demo_Project_1 - Customize
Up time: 0 days 5 hours
···
Change project name
Change project password
Topology
Device
11
Online Client
0
Internet
EG310GH-E
1 / 1
Switch
5 / 5
RAP1260(G)
2 / 2
RAP2260(G)
3 / 3
VLAN List
VLAN Configuration
Wired VLANs (4)
VLAN 1
VLAN1
VLAN 5
11
VLAN 23
Finance
VLAN 25
Guest
Wireless VLANs (0)
No Data