Ruijie Cloud On-Premises

User Guide

Document Version: V1.0
Date: November 17, 2023

Copyright

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

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

Warning

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

Caution

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

Note

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

Specification

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

3. Note

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

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

Contents

1 Product Introduction

1.1 Ruijie Cloud On-Premises (OP) Service Overview

Ruijie Cloud OP Service is Ruijie's easy and efficient cloud solutions for ISP and MSP to provide cloud 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 cloud 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 Portal service.

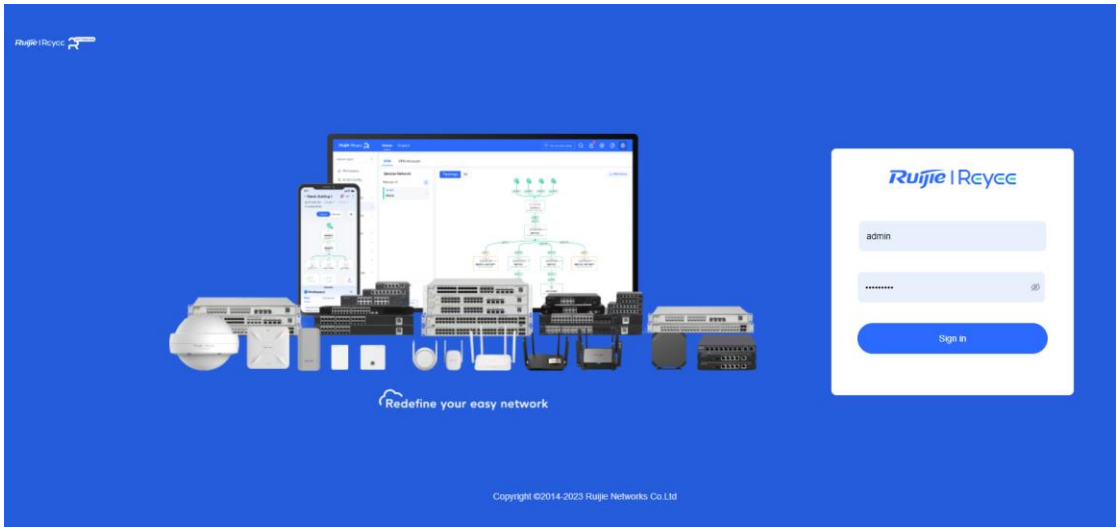
1.2 Key Features

- Unified device management
- Secure PPSK authentication for employees
- Captive portal for guests
- Cloud Monitoring & alert
- Tenant and Subaccount permission assignment

2 Quick Start

2.1 How to Login Ruijie Cloud OP Service

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



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

2.2 Adding a Project

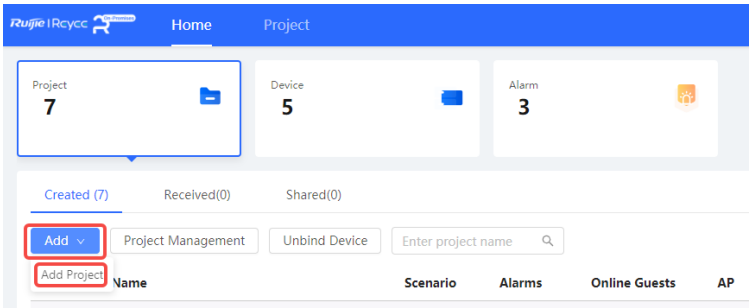
A project group includes many networks, and is usually used to represent the network of a province, a city, or a company.

Note

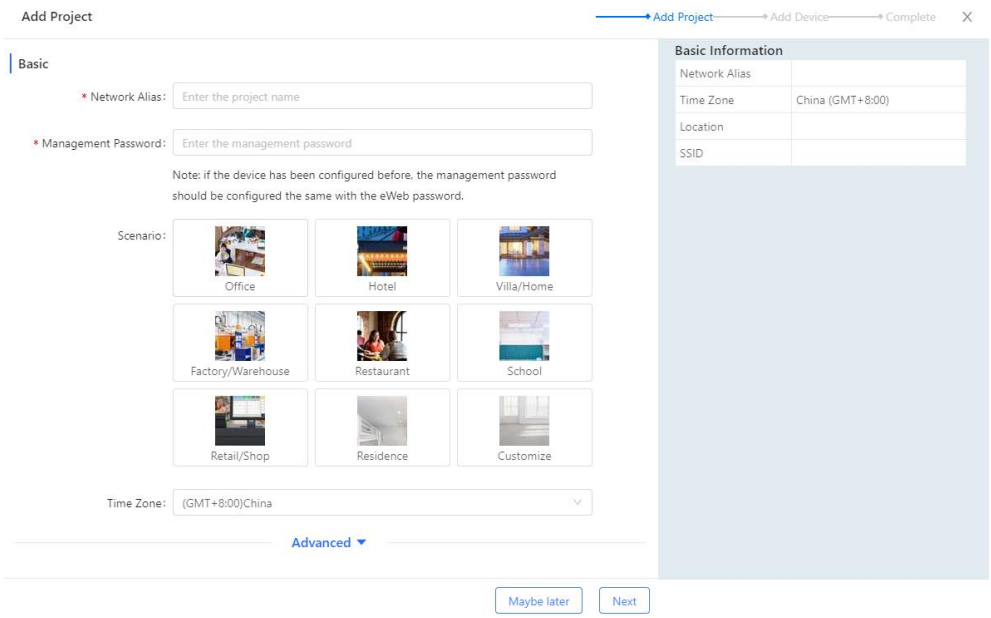
Adding devices to a project group is not supported. The project group is used to manage multiple projects.

Procedure

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



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



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.

Caution

If the device has been configured before, the management password should be configured the same with the Eweb password.

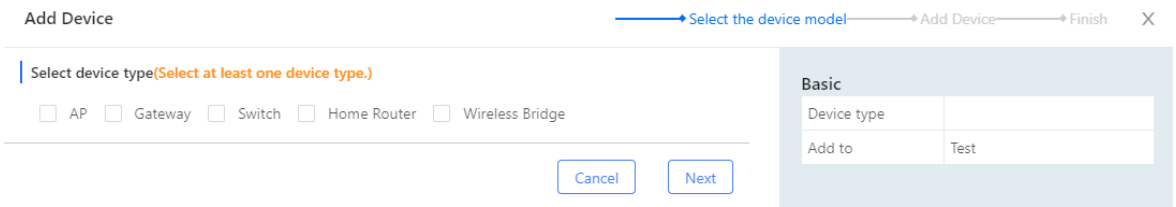
Scenario: indicates the scenario that suits the customer's actual scenario.

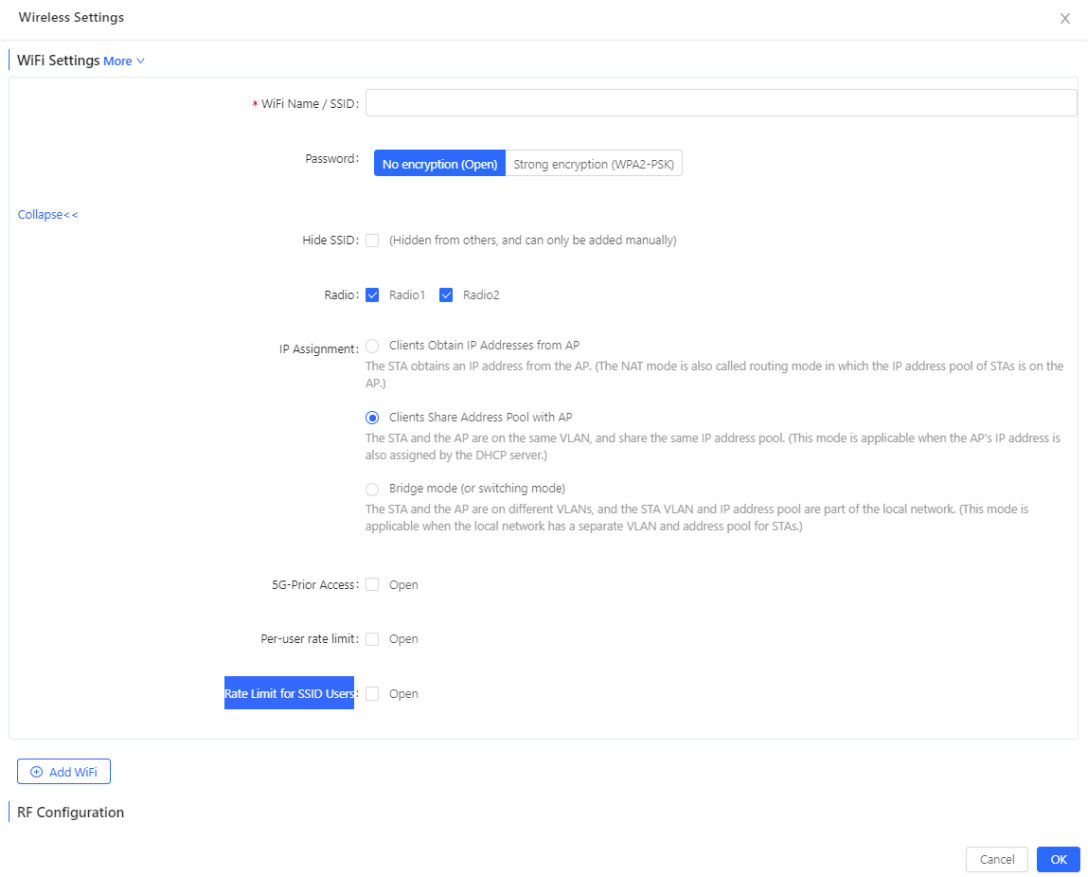
Time Zone: indicates the time zone where the current customer is located.

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) Select device type and set Wi-Fi parameters. Then click **OK**.





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.

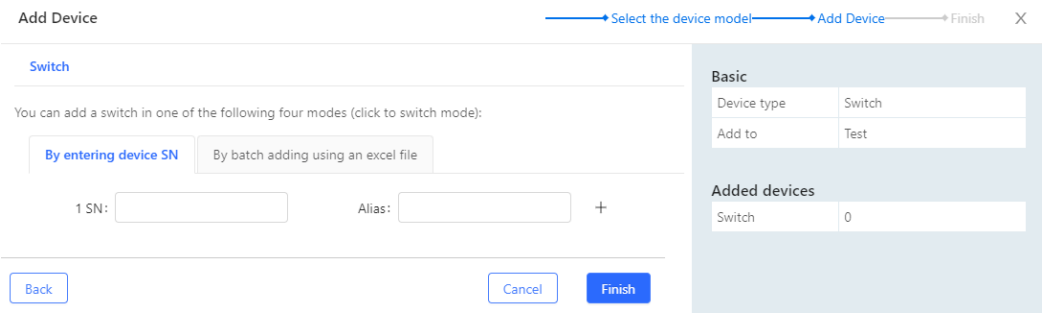
Per-user rate limit: indicates channel width control for each user who connects to this Wi-Fi.

Rate Limit for SSID Users: indicates channel width control for the total traffic on this SSID.

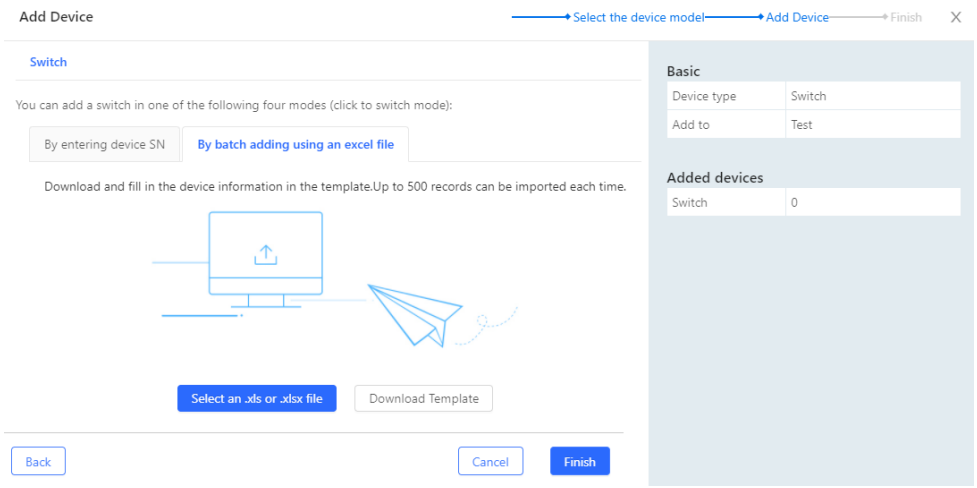
(4) Add devices manually or through batch import.

- Option 1: Add devices manually.

  Enter the device SN and alias.



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



a Click **Batch Import**.

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

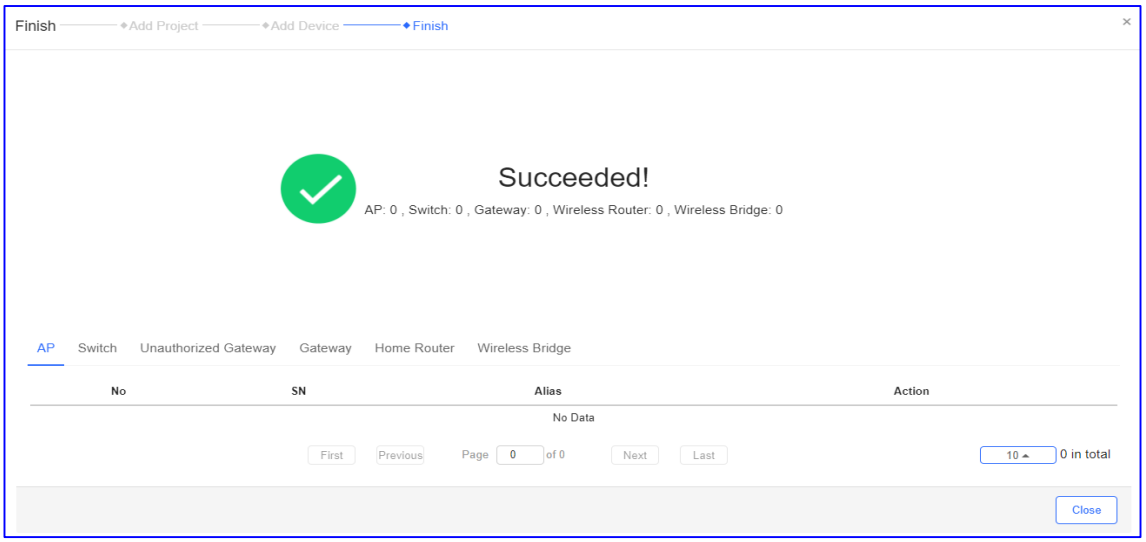
c Fill in the device SN and alias in the template and save it.

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.



3 AI Networking

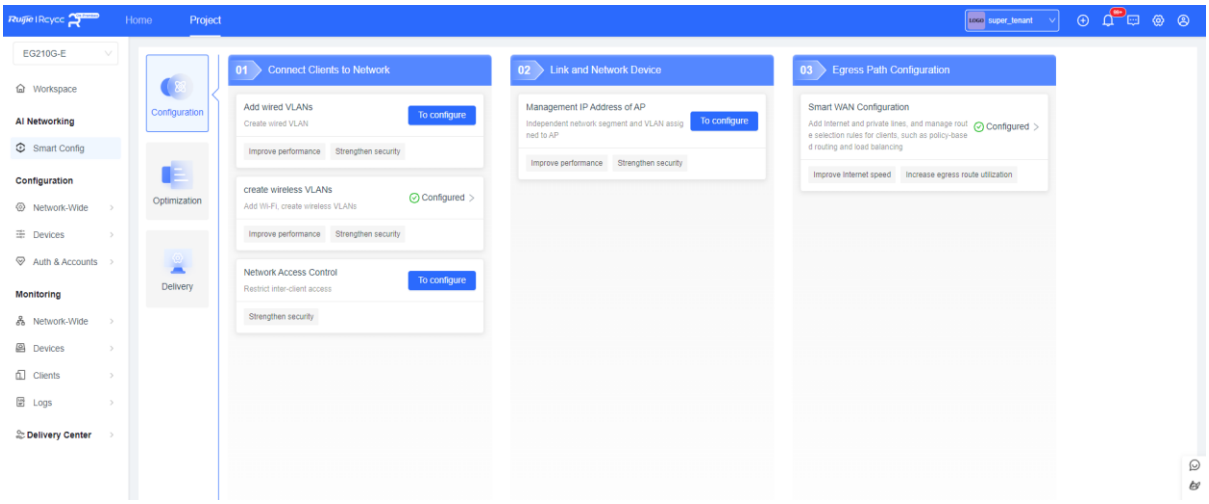
3.1 Smart Config

3.1.1 Configuration

(1) Choose **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.

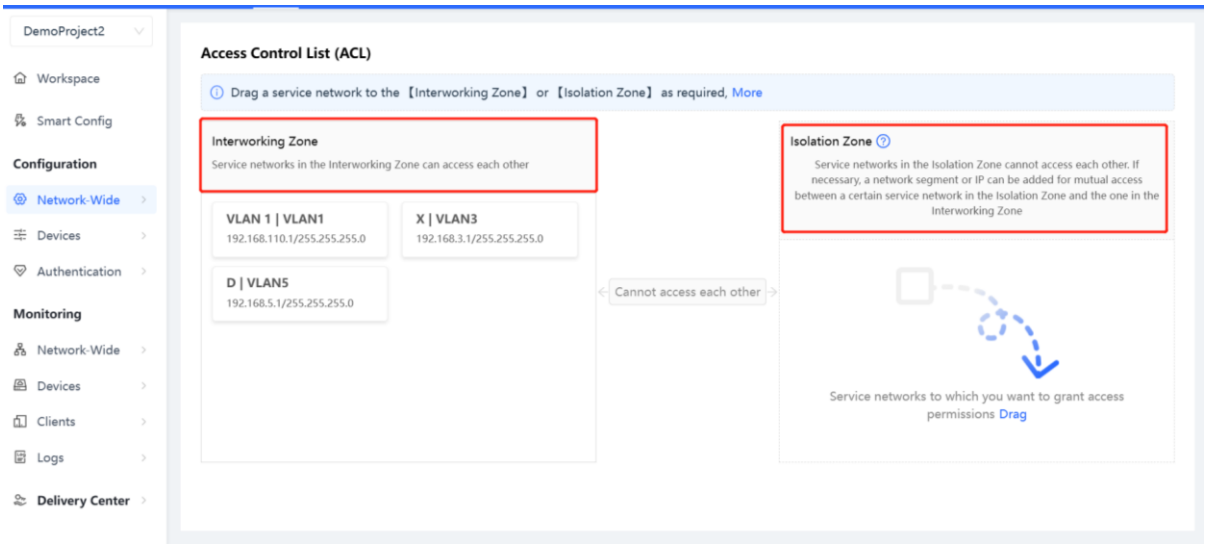
First, click **To configure**. The ACL page is displayed. On the page that is displayed, click **To configure** to start the configuration.

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 **Interworking 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.



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.

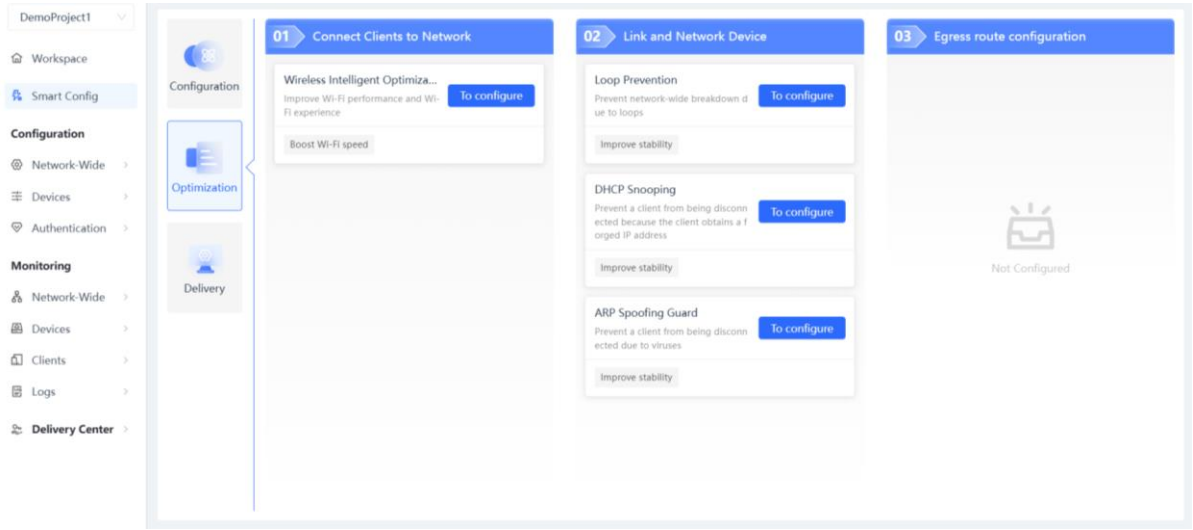
Click **To configure** under the item that you want to configure. You will be redirected to the corresponding configuration page.

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.



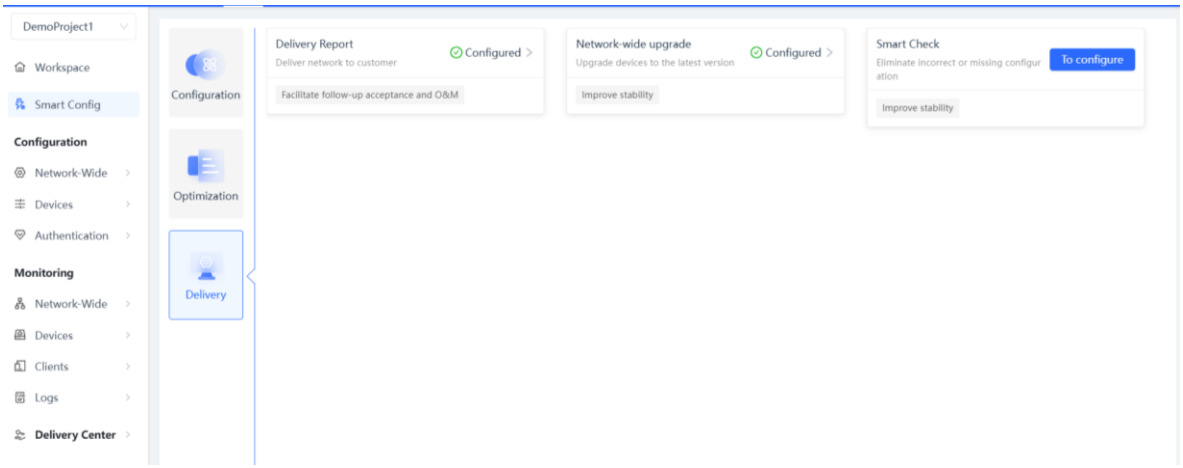
3.1.3 Delivery

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

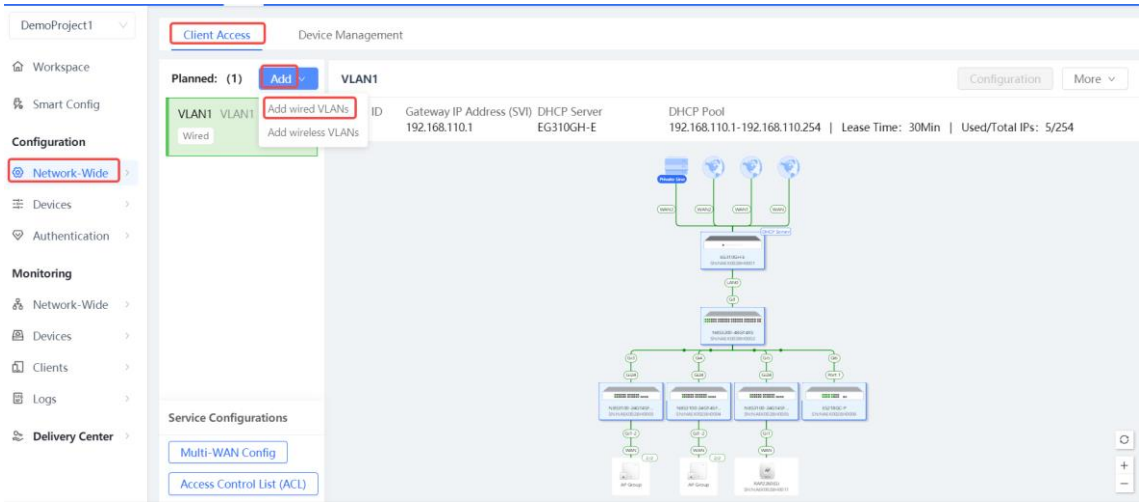
4.1 Creating a Wired VLAN

4.1.1 Overview

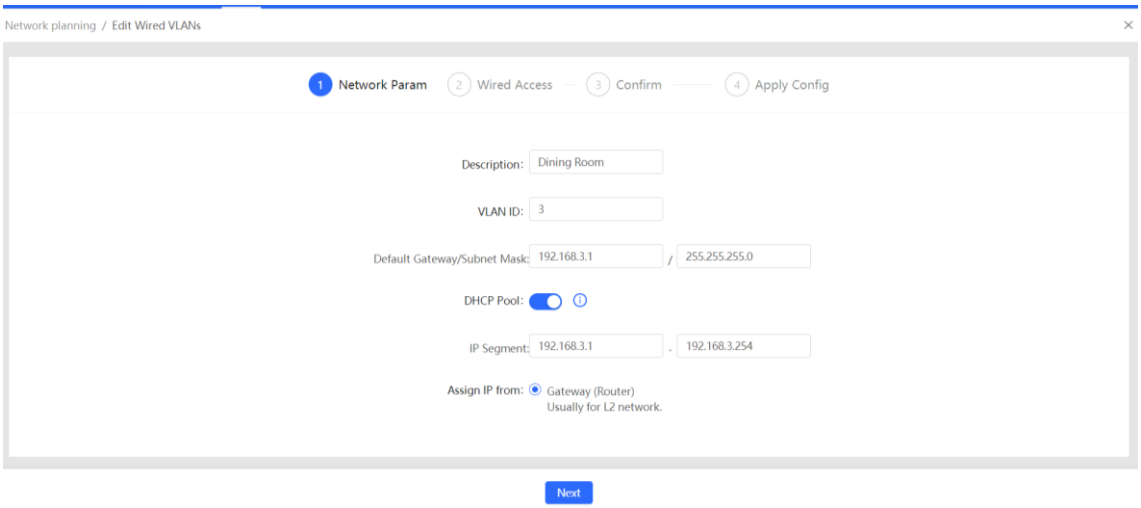
Different clients exist on a network, such as PCs and cameras. When a camera is running, broadcast or abnormal traffic often occurs, imposing negative effects on the service network. The administrator wants to isolate the broadcast and abnormal traffic of the camera from the running service network.

4.1.2 Configuration Steps

(1) Adding a wired VLAN: Choose **Project > Configuration > Network-Wide > Client Access,** 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**.



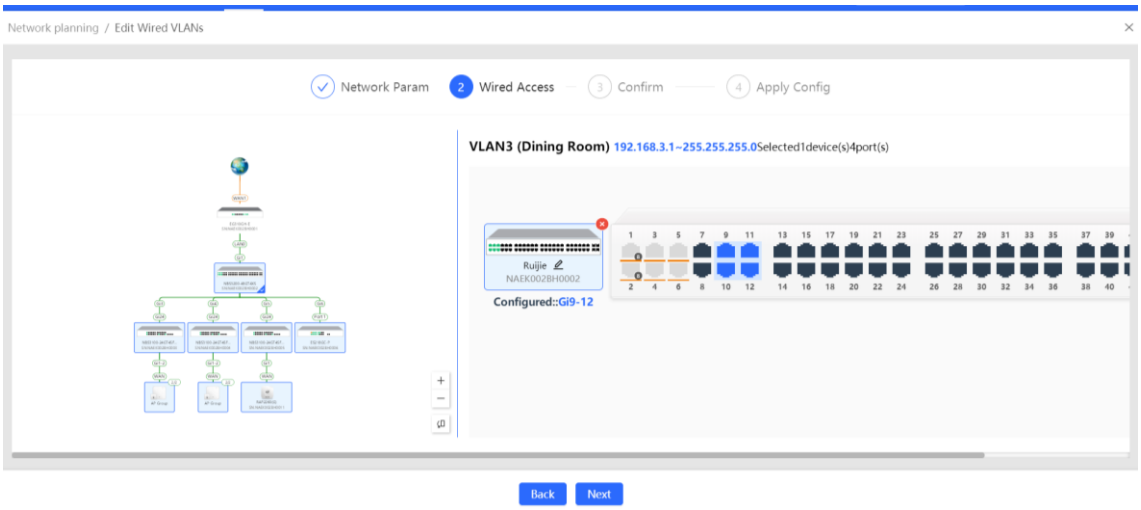
(2) Setting service parameters: Set the VLAN for wired access and create a Dynamic Host Configuration Protocol (DHCP) address pool for devices in the VLAN to automatically obtain IP addresses. The gateway can serve as the address pool server to assign addresses to access clients. If a core switch supporting 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**.



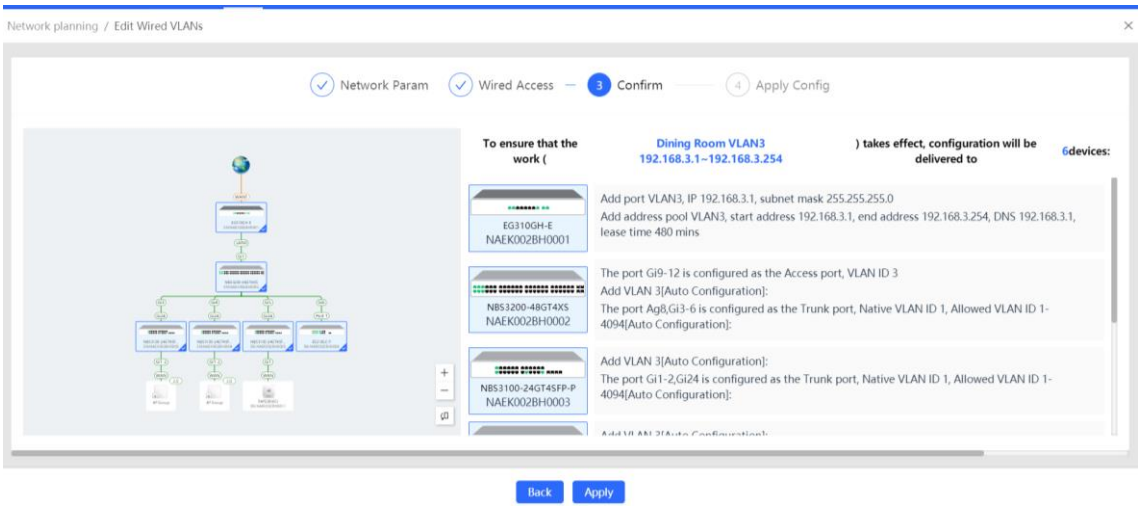
The following table lists the description of parameters.

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.

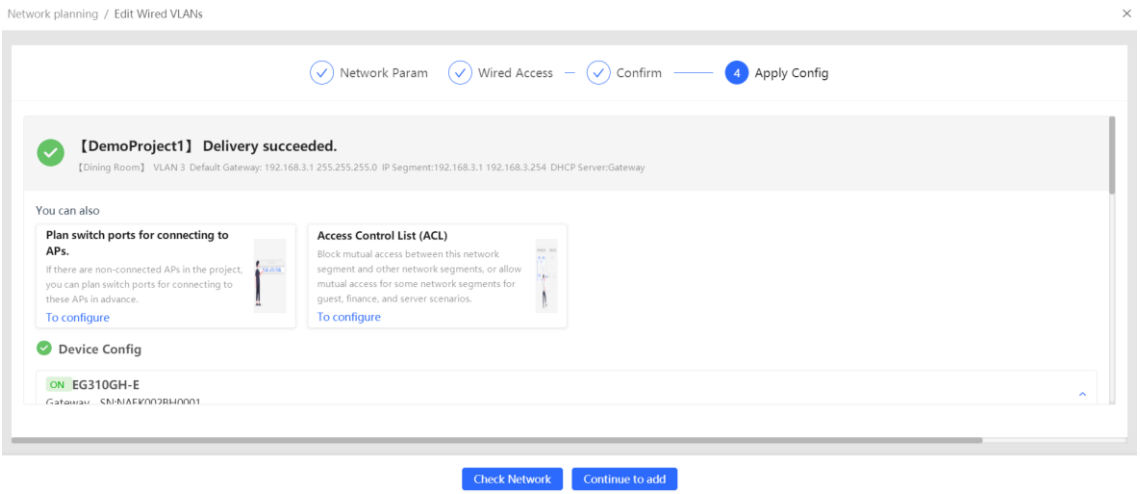
(3) Select the interface for connecting the camera in the topology on the left, and select the port to connect the camera from port icons on the right. The port icon will change from gray-black to blue. Click **Next**.



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



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



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.

- There 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.
- In 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

- In 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.
- Some 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?

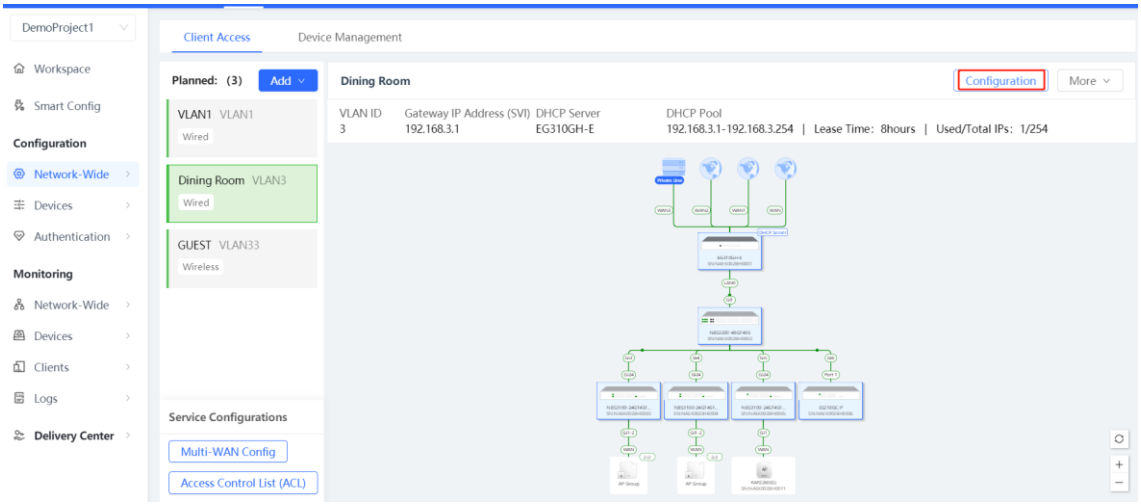
Purpose of Lease Period

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

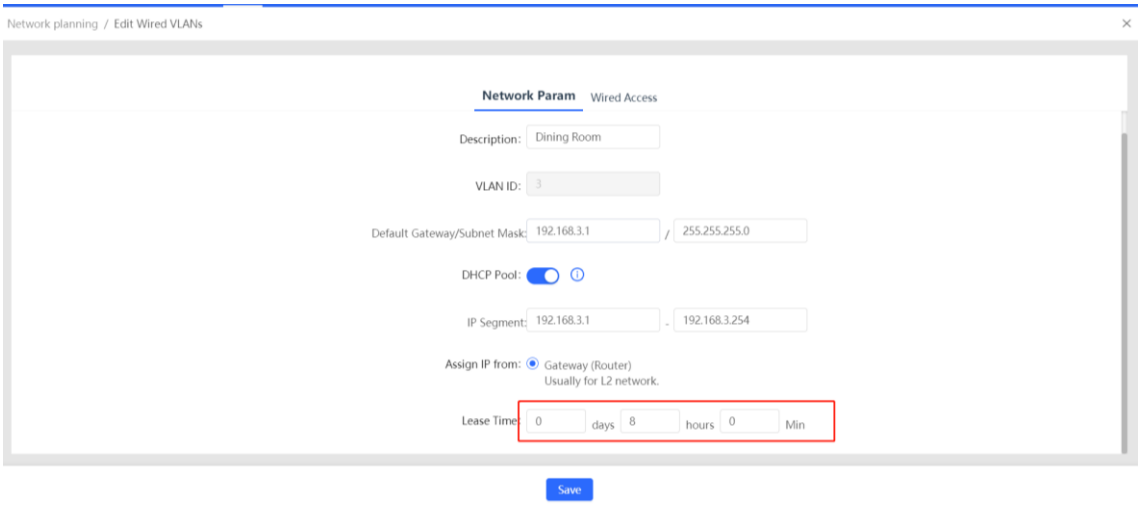
again, it will obtain an address again. In general scenarios, keep the default value for the lease period. If the address pool has sufficient addresses, set the lease period to a smaller value; if the addresses are sufficient, set the lease period to a larger value.

Configuration Steps

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



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



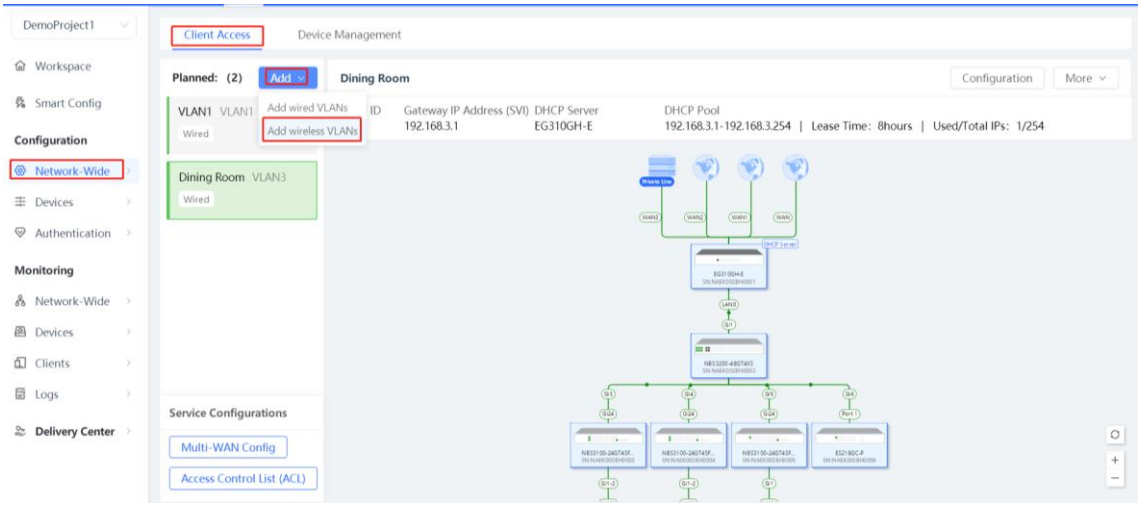
4.2 Creating a Wireless VLAN

4.2.1 Overview

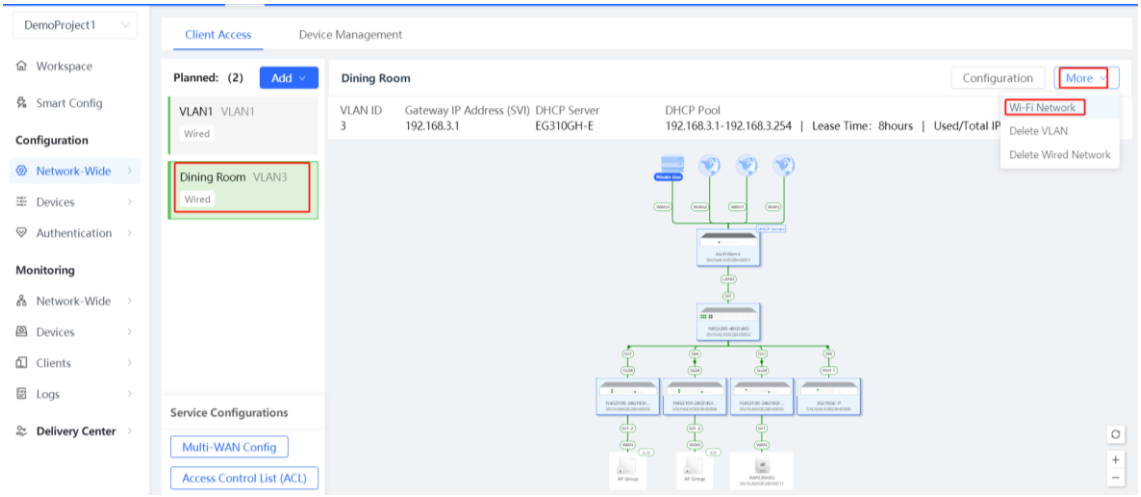
To manage the Wi-Fi usage of different user groups (such as company employees and external guests) separately, the company wants to provide separate Wi-Fi access for guests, and isolate the IP segment used by the guests' terminals and the VLAN to which they belong from company employees.

4.2.2 Configuration Steps

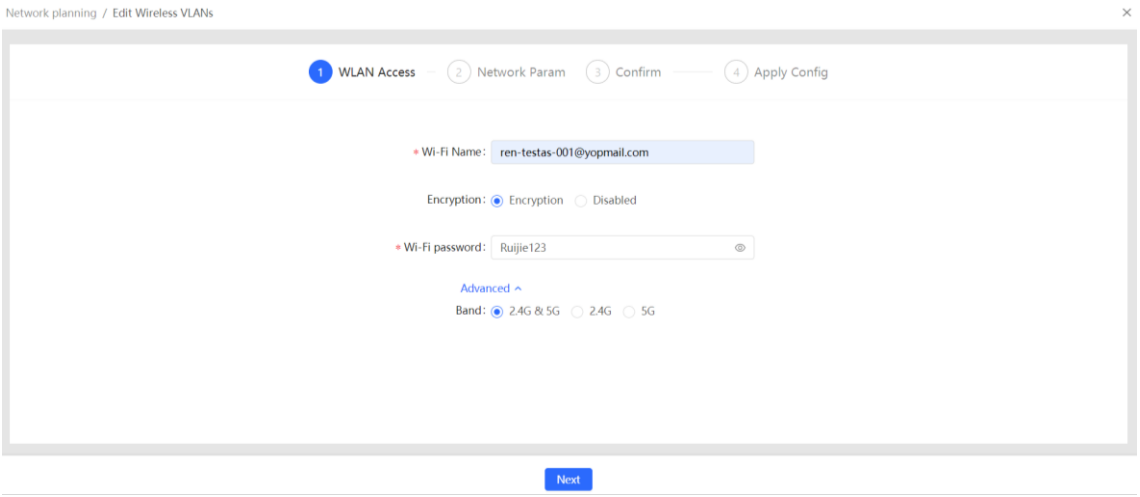
(1) Adding a wireless VLAN: Click **Add** and select **Add wireless VLANs** to add wireless VLAN configuration for the current network.



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.



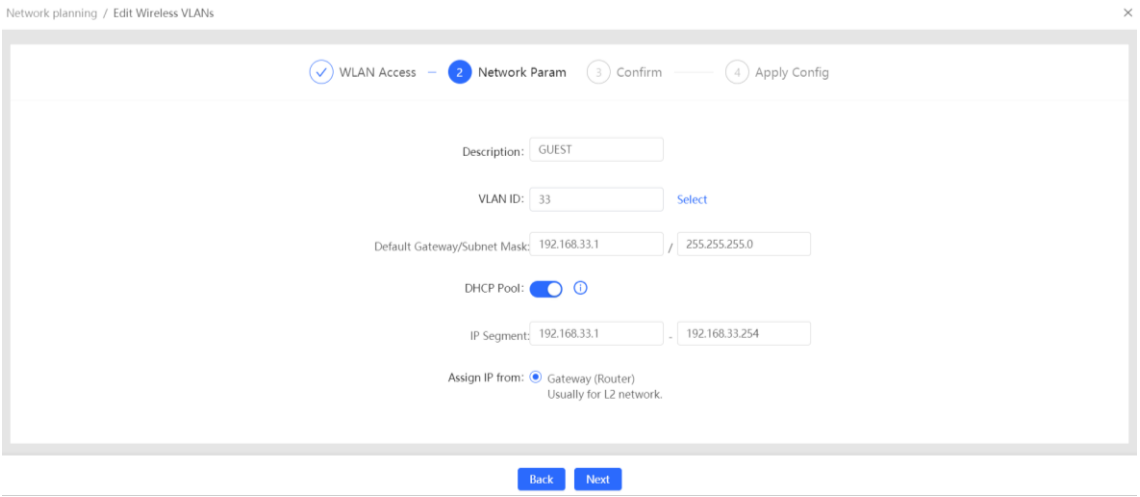
(2) Setting Wi-Fi service parameters: Set Wi-Fi information first, such as the Wi-Fi name and password.



The following table lists the description of parameters.

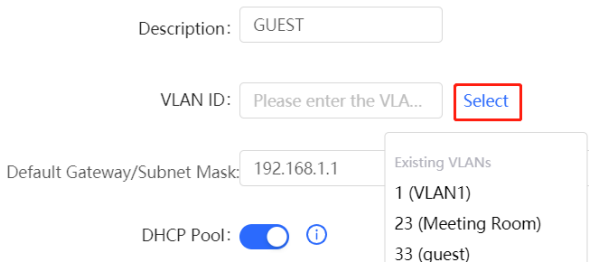
Parameter	Description
SSID	Enter a string of less than 32 charters, including letters, numerals, spaces, and special characters (-_@&.). If spaces are contained, it cannot be longer than characters. For example, set SSID to Guest.
Encryption	You are advised to encrypt the network to prevent other clients 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**.

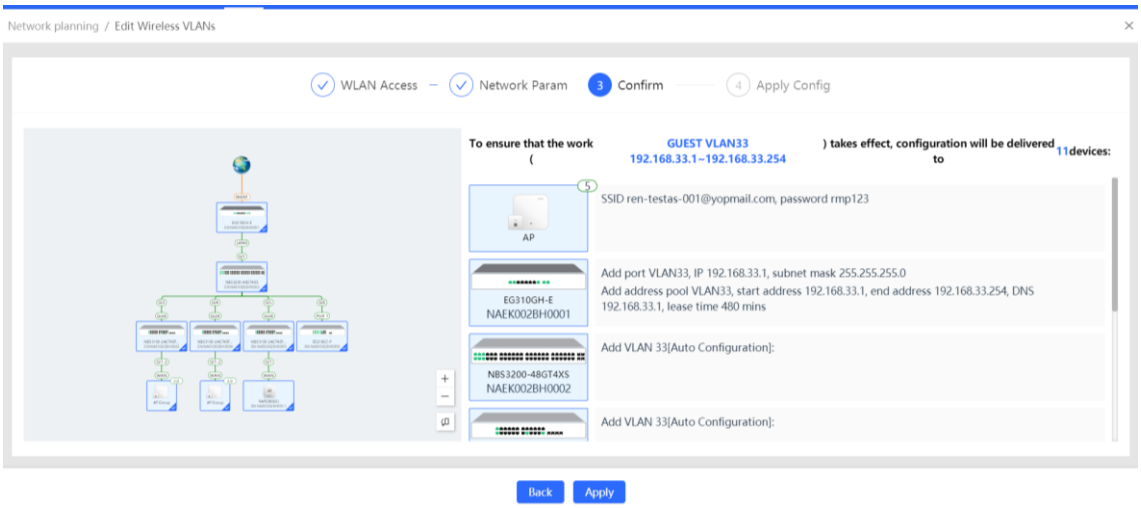


The following table lists the description of parameters.

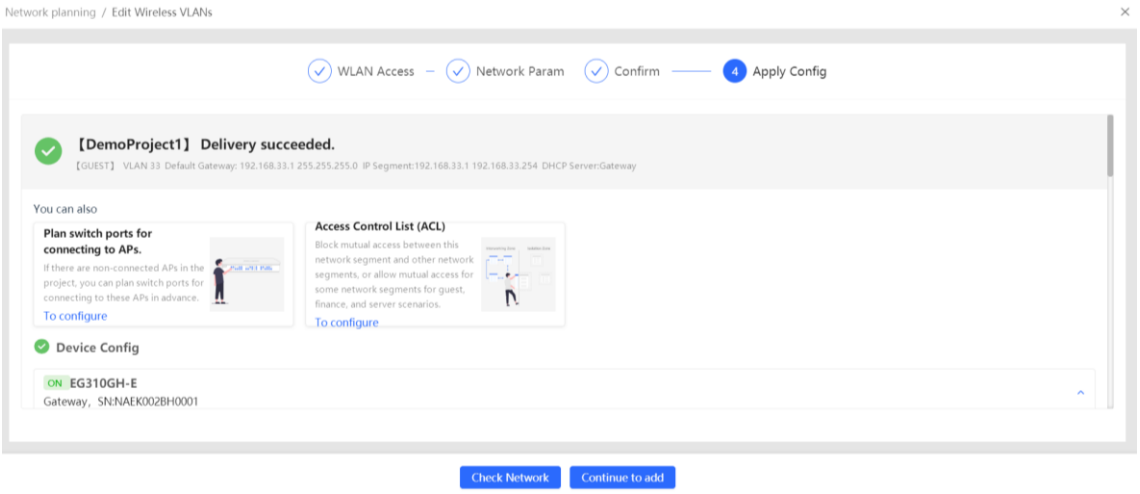
Parameter	Description
Description	Enter the description of the guest VLAN.

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. 
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.



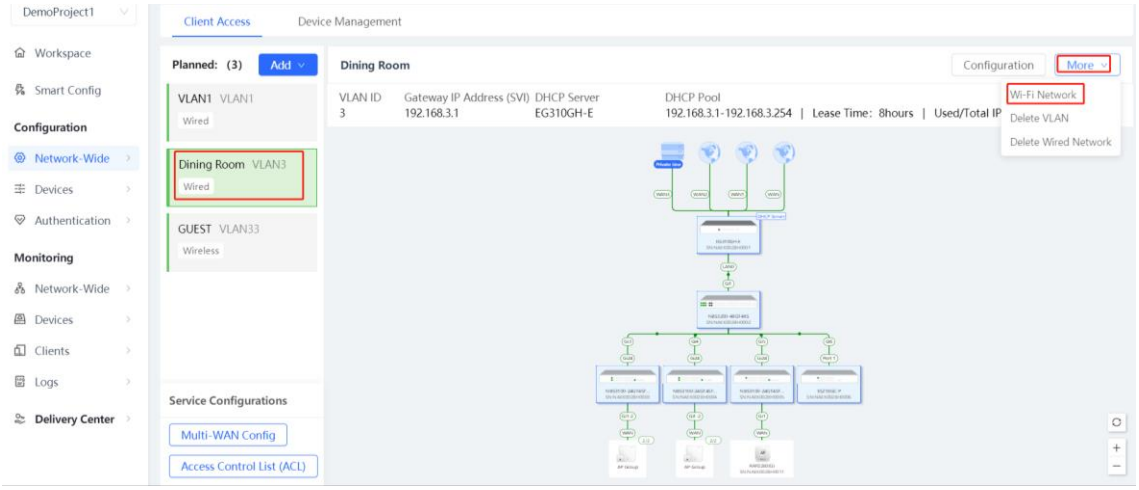
(5) The service network is added successfully when the message indicating delivery success is displayed.



4.2.3 FAQs

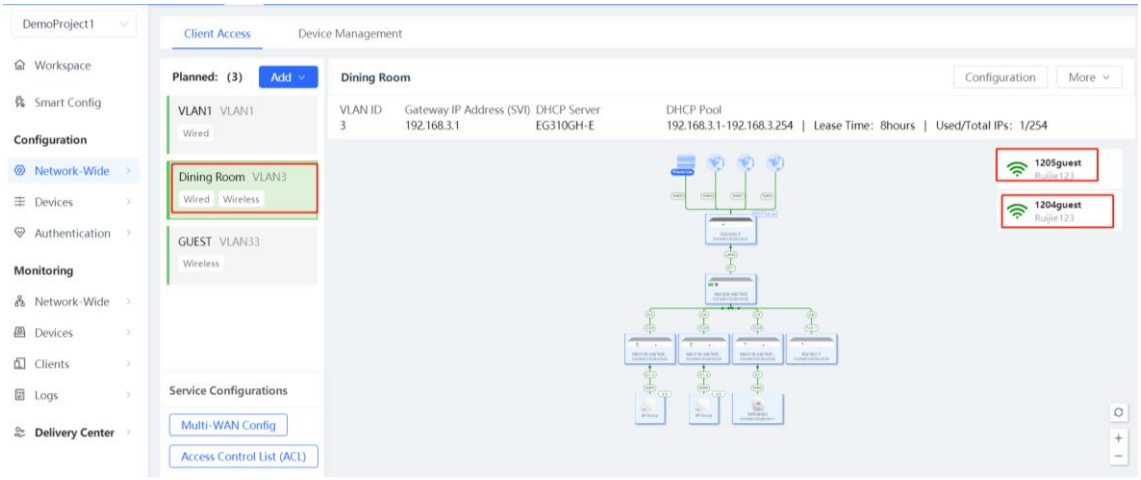
1. How Do I Add the Names of Multiple Wi-Fi Networks to the Same VLAN?

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.



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.



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

4.3.1 Demand

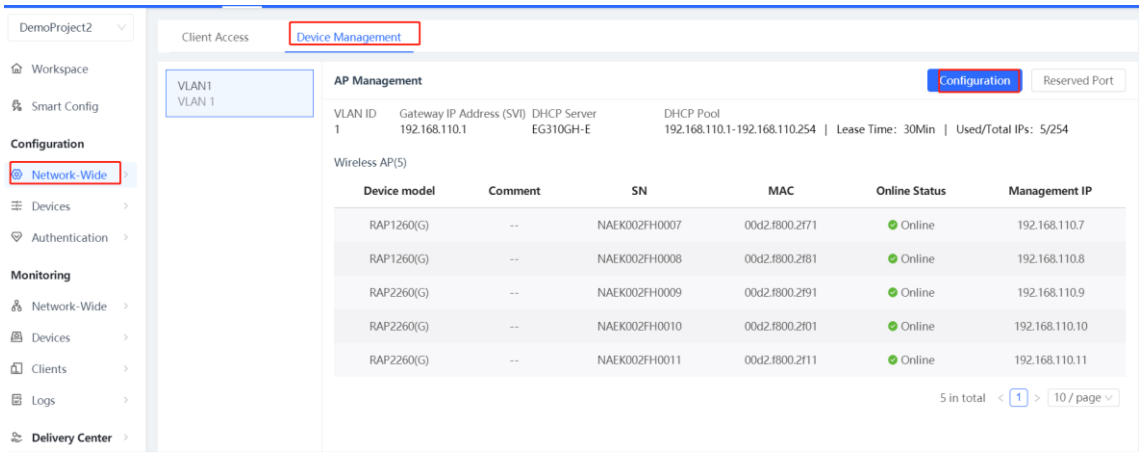
Multiple access points (APs) are deployed on the network to transmit wireless network signals. One separate VLAN needs to be configured for management packets of the APs. Configuring a separate management service network can avoid AP go-offline due to the complex environment on the service network, thereby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

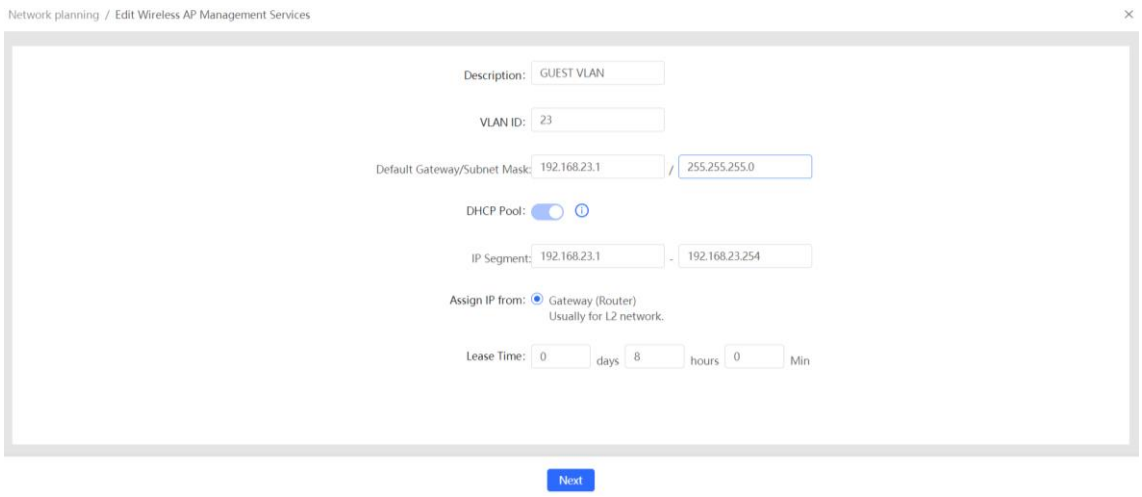
(1) Choose **Network-Wide** > **Network** > **VLAN** > **Device Management**. Information about APs on the network is displayed, including the management VLAN, device models, SNs, management IP addresses, MAC addresses, and online status. Click **Configuration** to configure the AP management service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



(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

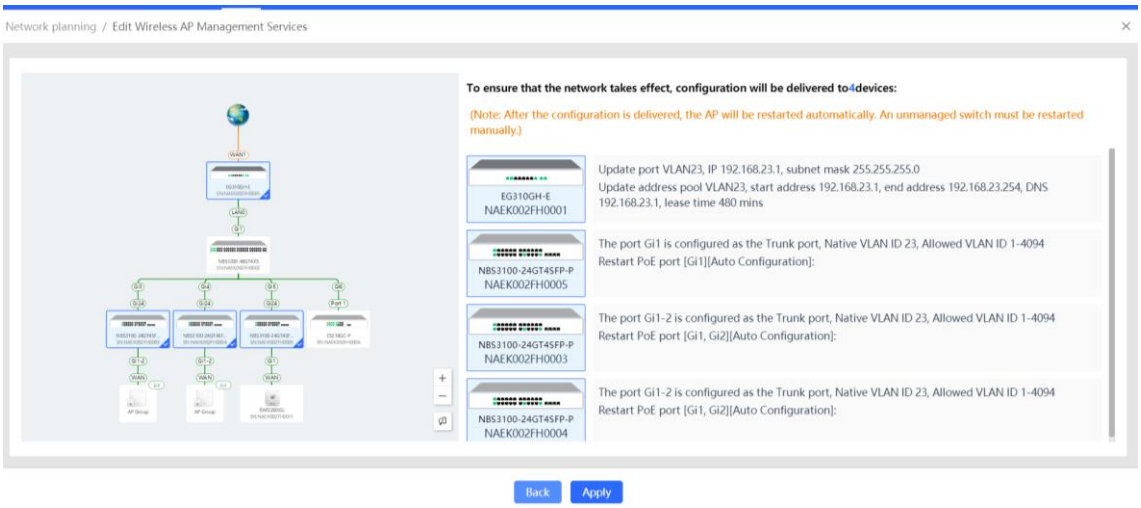
- You are advised to use default configurations for other parameters. Do not disable the DHCP address pool. Otherwise, IP addresses cannot be assigned to APs and you have to configure static IP addresses to the APs manually one by one.
- In **Description**, enter the description of the current service 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.



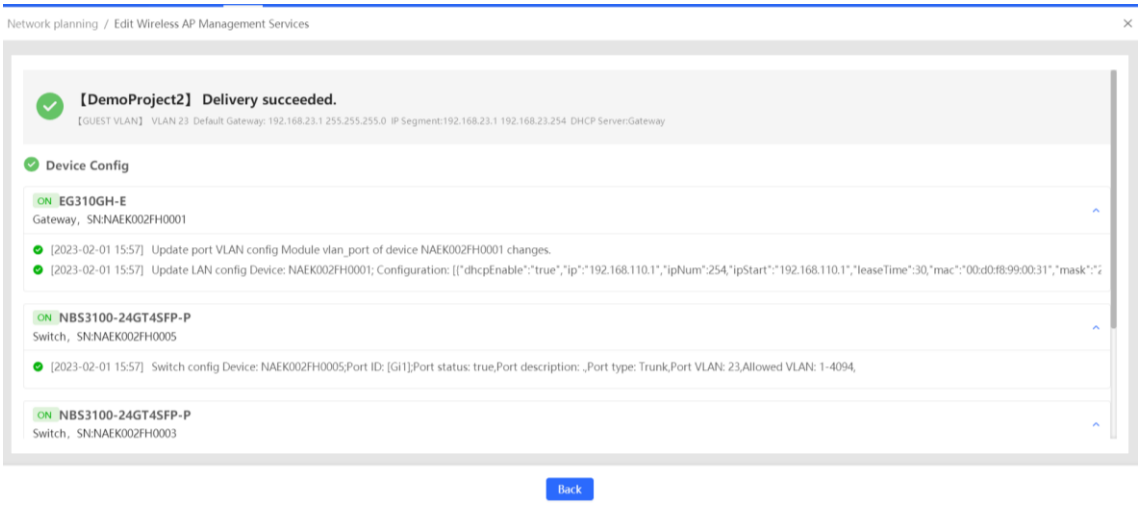
(3) Click **Apply**. The configuration is delivered to the gateways and switches and takes effect. Wait till the prompt "Delivery succeeded" is displayed, indicating that the service network is added.

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.



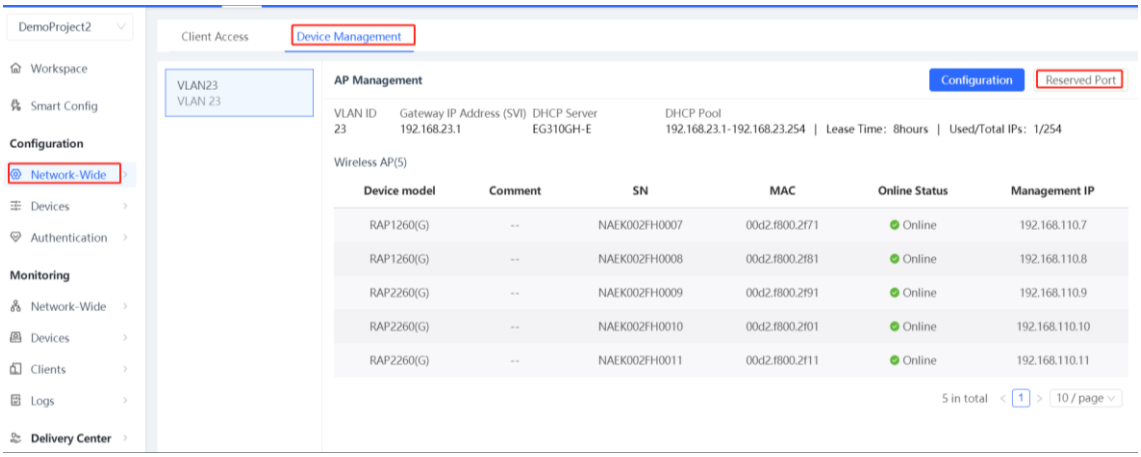
(4) The AP management network configuration is delivered.



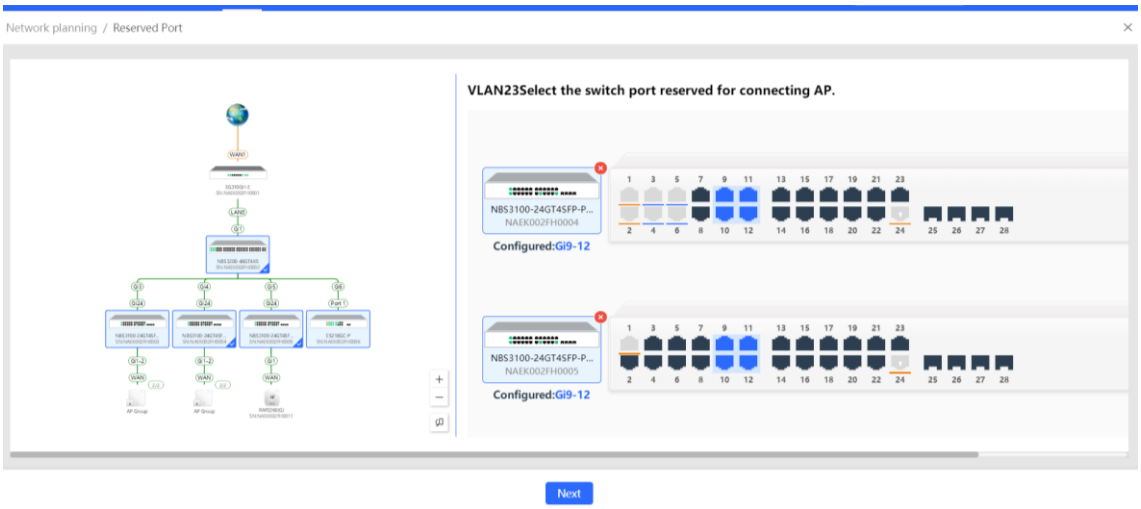
2. Configuring a Reserved Port for an AP (applicable to the scenario in which APs are not connected)

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

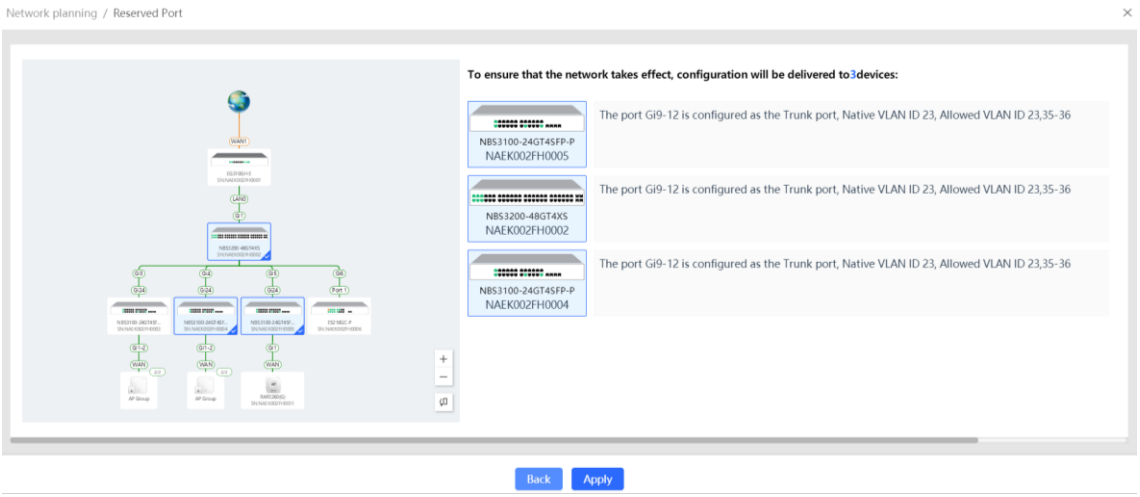
(1) Choose **Network-Wide** > **VLAN** > **Device Management** > **Reserved Port**.



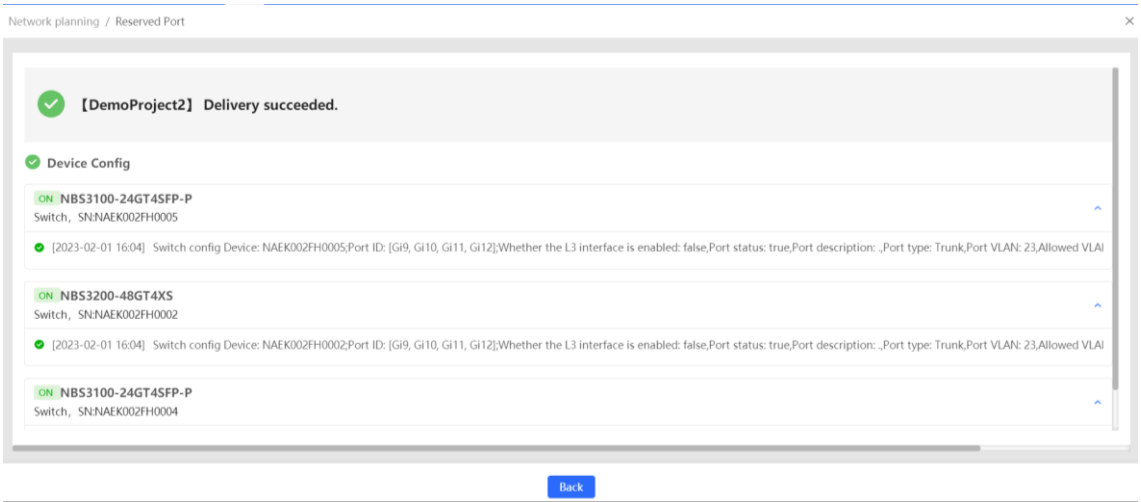
(2) Click the switch for connecting to an AP (you can select multiple switches) in the topology on the left, and select the port reserved for AP wired connection on the switch on the port icon panel on the right. The port icon changes from dark gray to blue. Click **Next**.



(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.

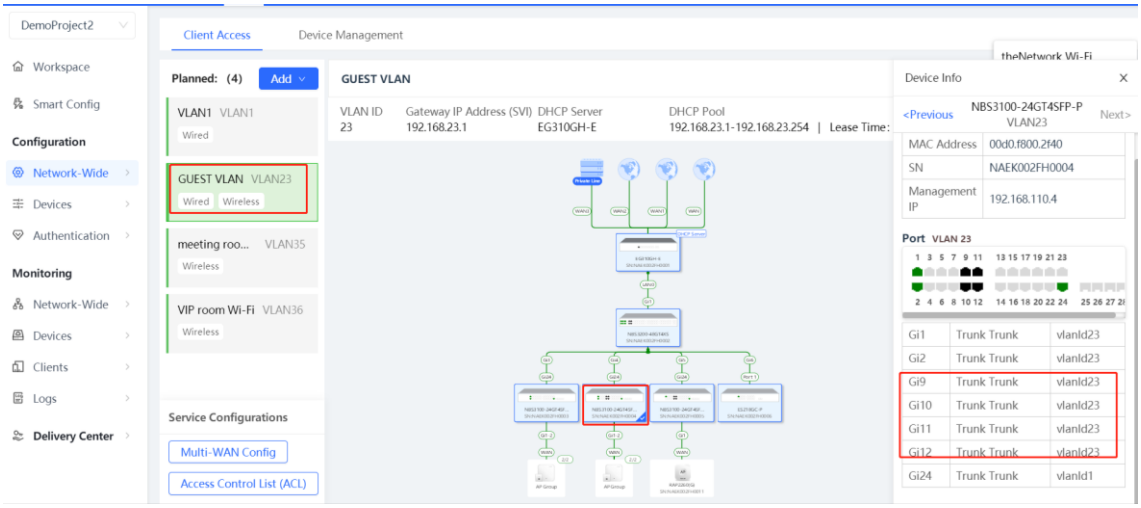


(4) The port configuration is delivered successfully.



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.

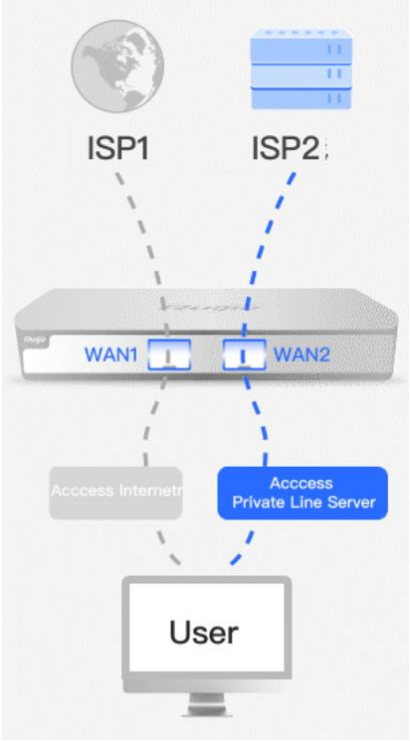


4.4 Multi-WAN

4.4.1 Overview

1. Applicable Scenarios

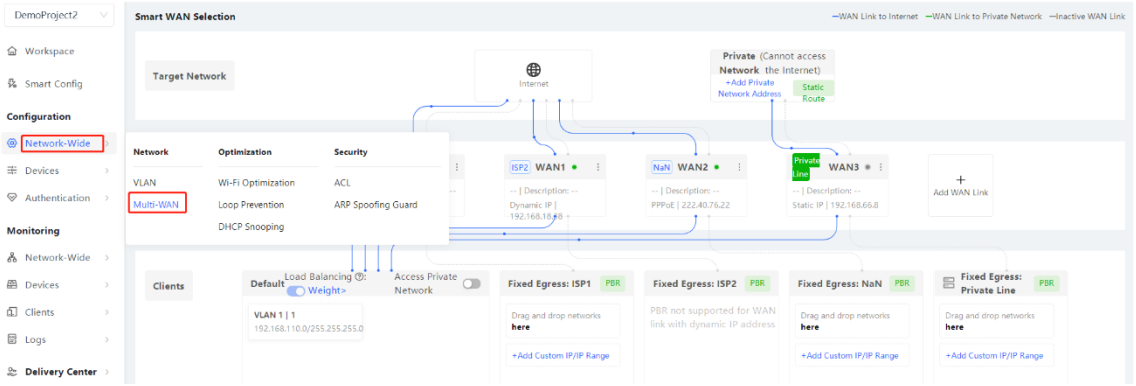
When a gateway is connected to multiple extranet lines, the multi-WAN function can be configured to meet different requirements. This function mainly applies to the following three scenarios:



- 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

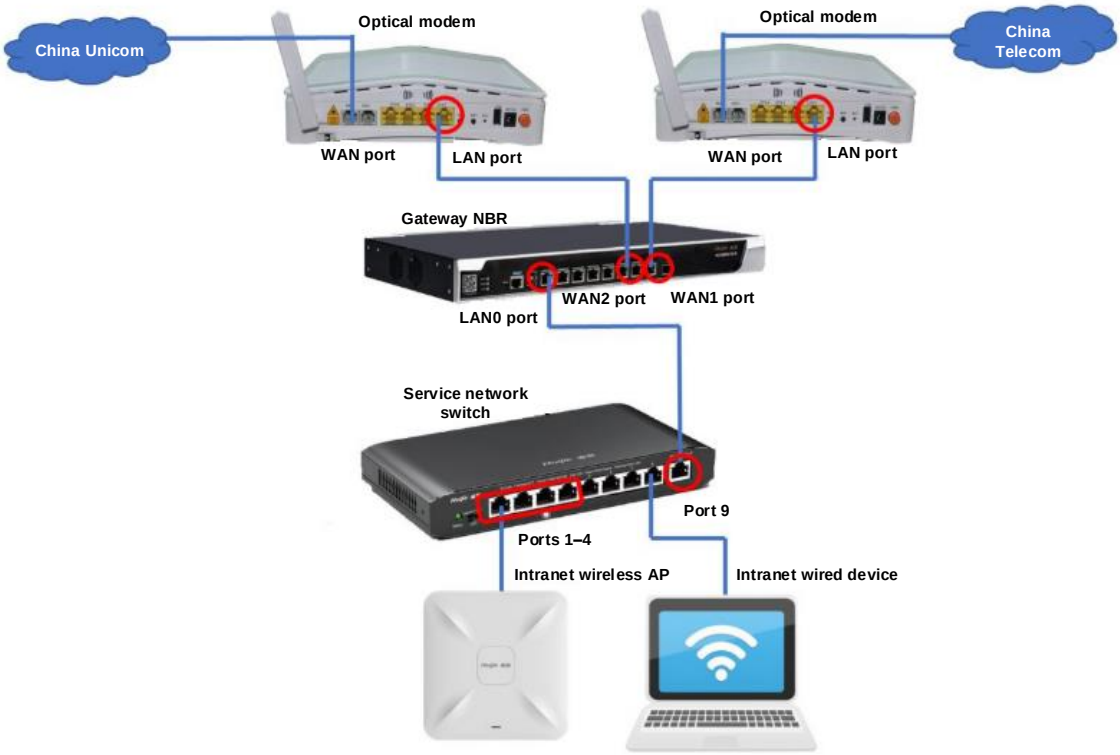
Choose Network-Wide > Multi-WAN to go to the Smart WAN Selection page.



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.

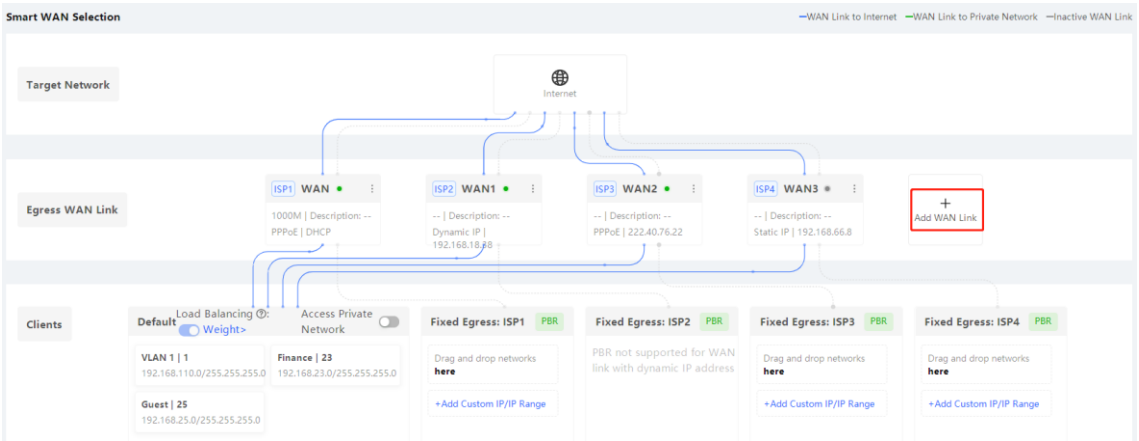
2. Configuration Ideas

(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

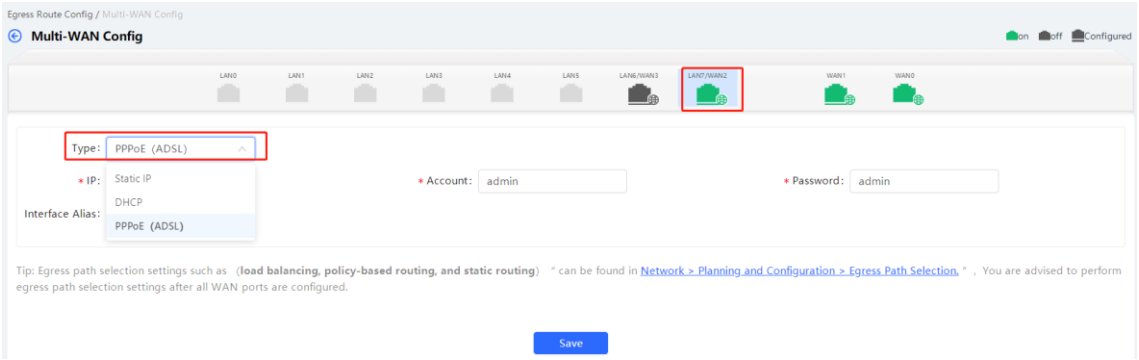
(1) Click **Add WAN Link** to go to the **Multi-WAN Config** page of the gateway.



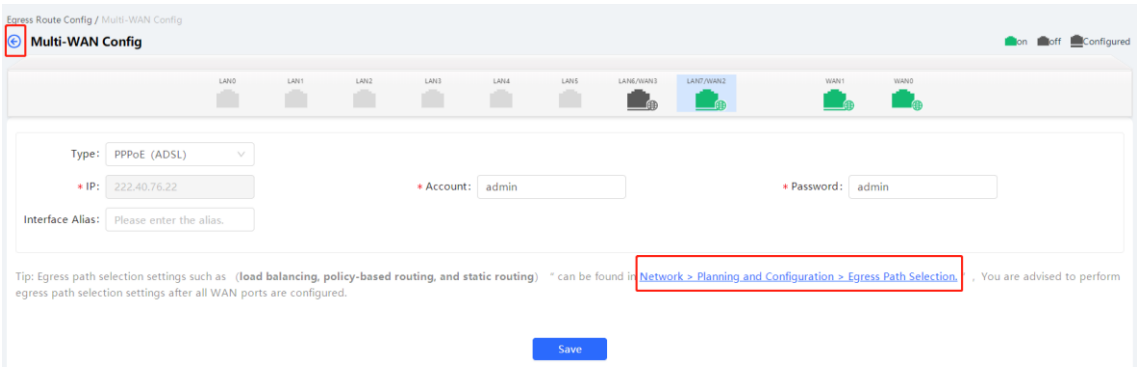
(2) Select a WAN port and configure the Internet access type for the WAN port based on the operator's requirements. It can be set to **Static IP**, **DHCP**, or **PPPoE (ADSL)**.Click **Save**.

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.

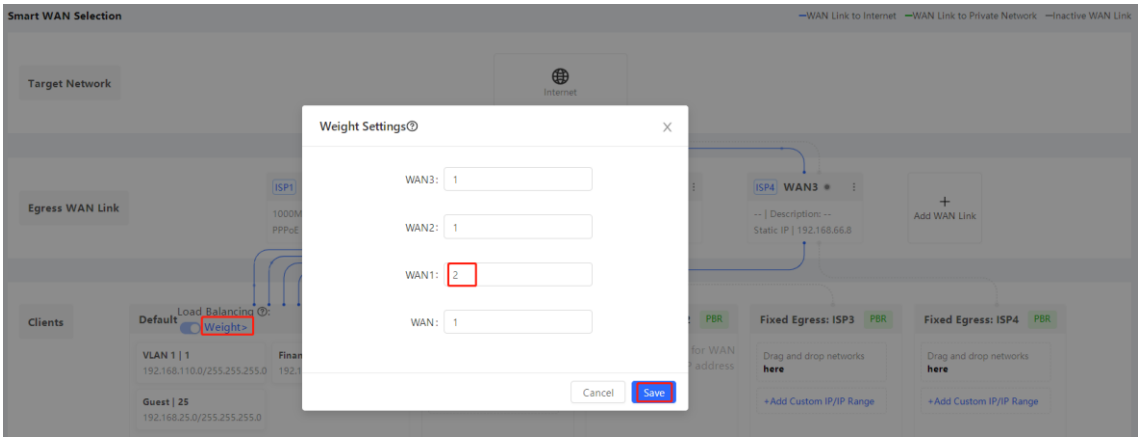


(3) Click the back button on the right of Multi-WAN Config or click Network > Planning and Configuration > Egress Path Selection to return to the Smart WAN Selection page.



(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**.



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

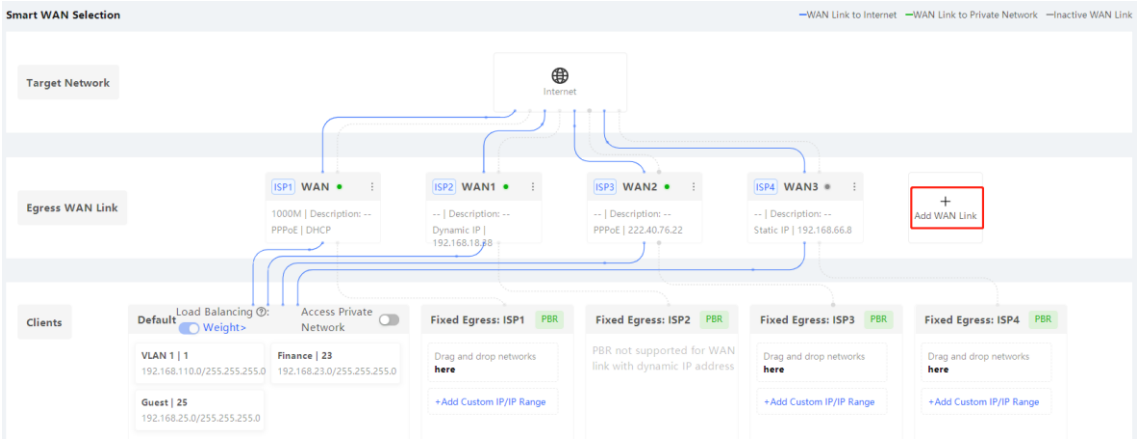
(1) Configure WAN ports to access the Internet through static IP addresses PPPoE.

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

(3) Bandwidth is automatically assigned to other users.

3. Configuration Steps

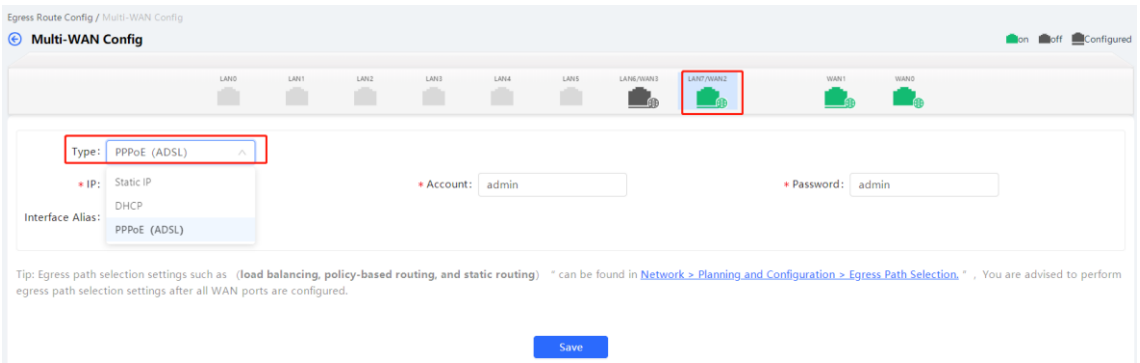
(1) Click **Add WAN Link** to go to the **Multi-WAN Config** page of the gateway.



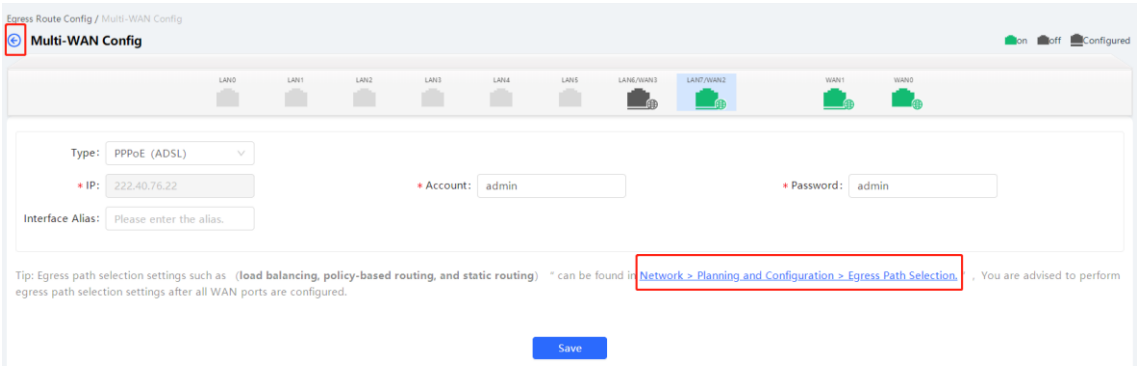
(2) Select a WAN port and configure the Internet access type for the WAN port based on the operator's requirements. It can be set to **Static IP**, **DHCP**, or **PPPoE (ADSL)**.Click **Save**.

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.



(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.

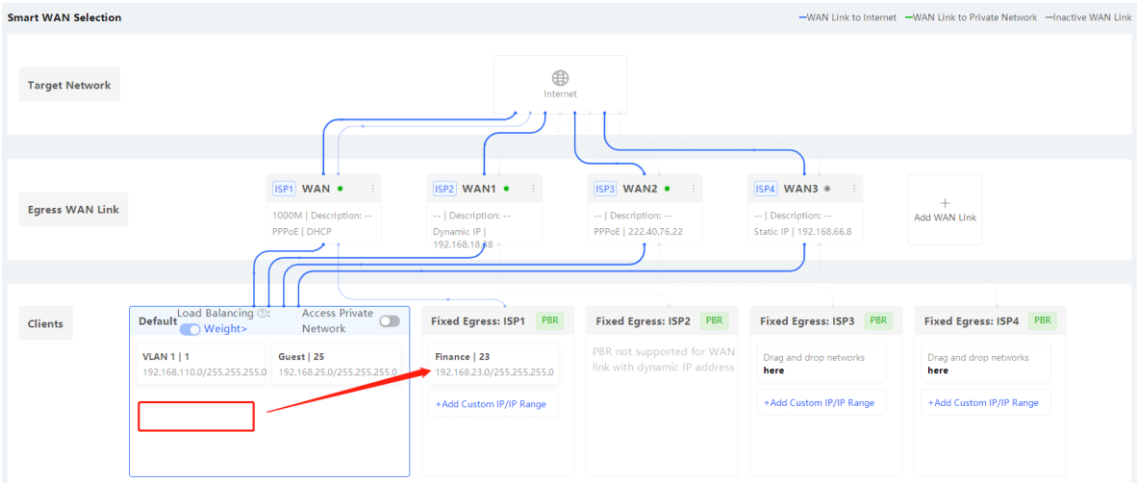


(4) Configure a routing policy.

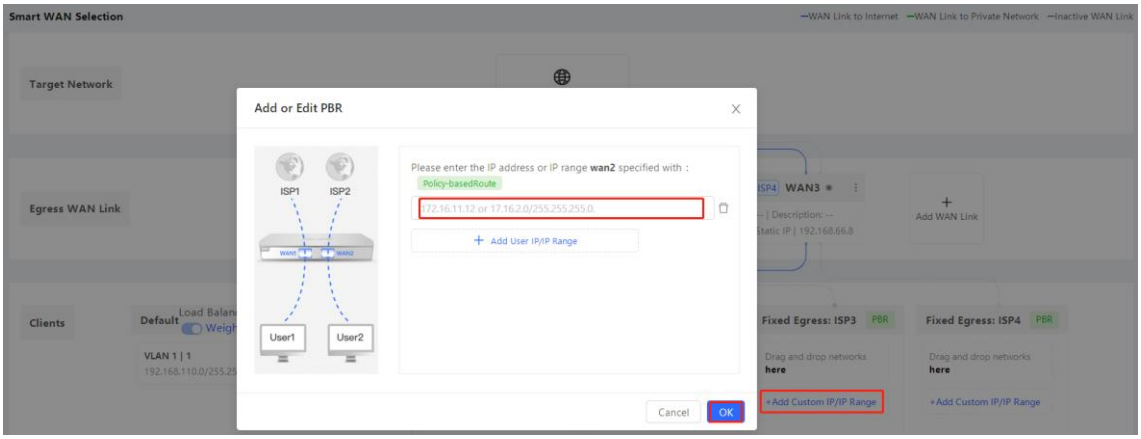
Caution

- 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**.



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



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.

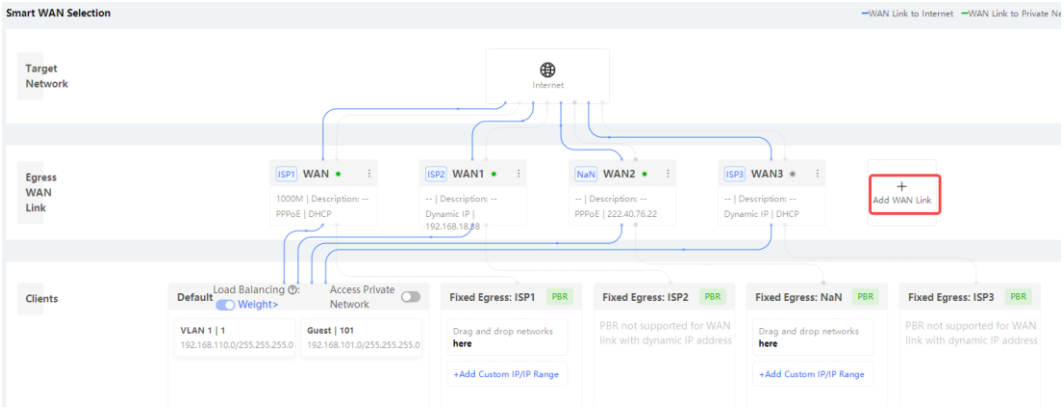
(2) There are two policies available for private networks:

○ 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.

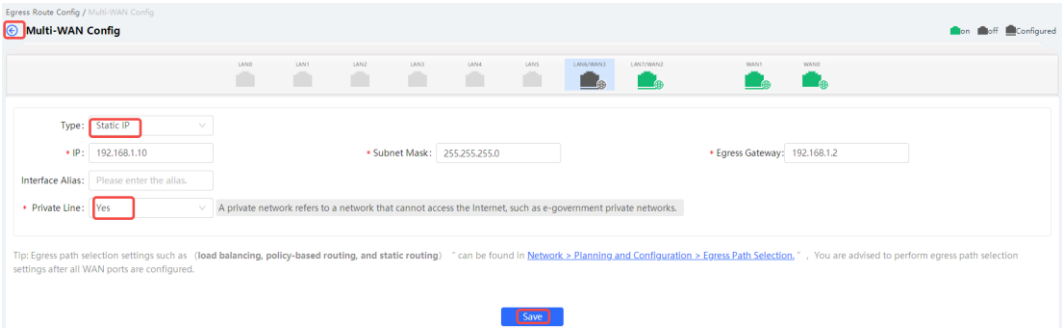
○ Specifying Intranet users: When specified Intranet users access the Internet, the traffic of the users is transmitted through the private line and the traffic of other users is not transmitted through the private line.

3. Configuration Steps

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



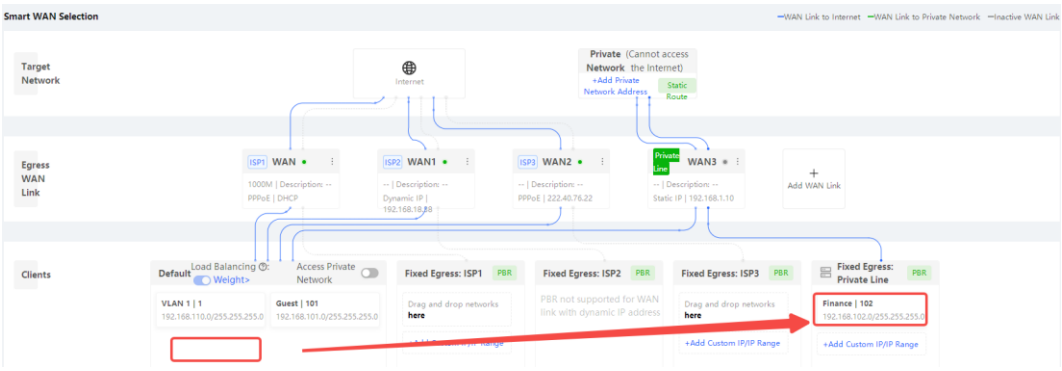
(2) Configure Internet access type for the WAN port based on the operator's requirements. **Type** can be set to **Static IP** for private lines. Set **Private Line** to **Yes**, click **Save**, and then click the back arrow on the right of **Multi-WAN Config** at the upper right corner.



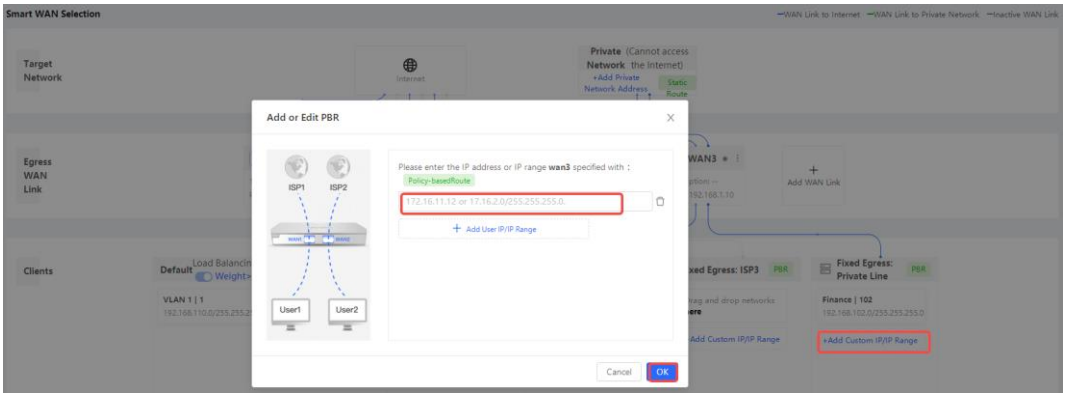
Note

- 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.

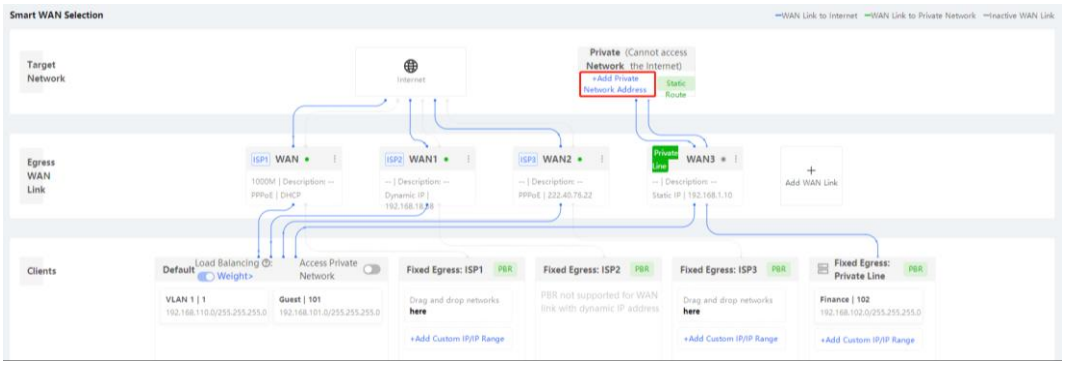


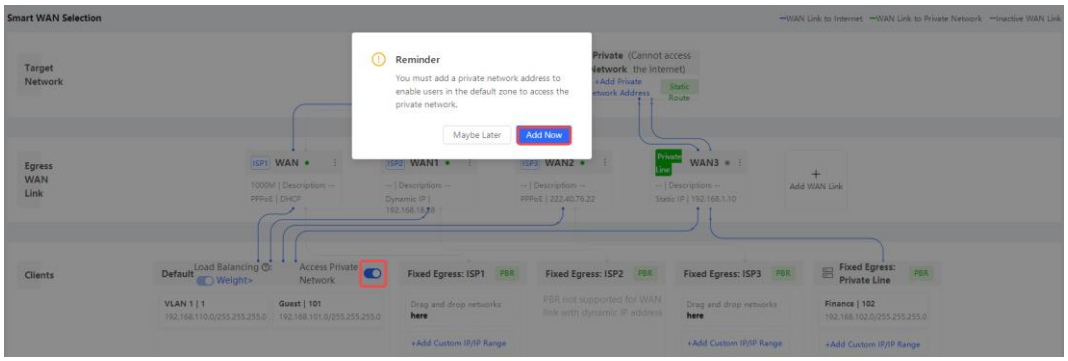
You can also click **Add Custom IP/IP Range** to add an IP address or IP address segment.



(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.

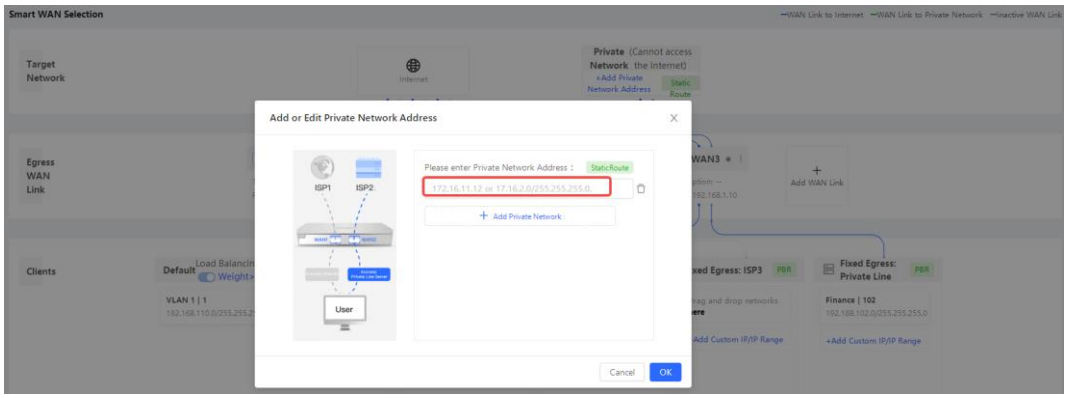




Edit the destination network specified for the private line (you need to specify the address or address segment of the private line you want to access, such as the tax network or medical network; you can set multiple addresses).

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.



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.

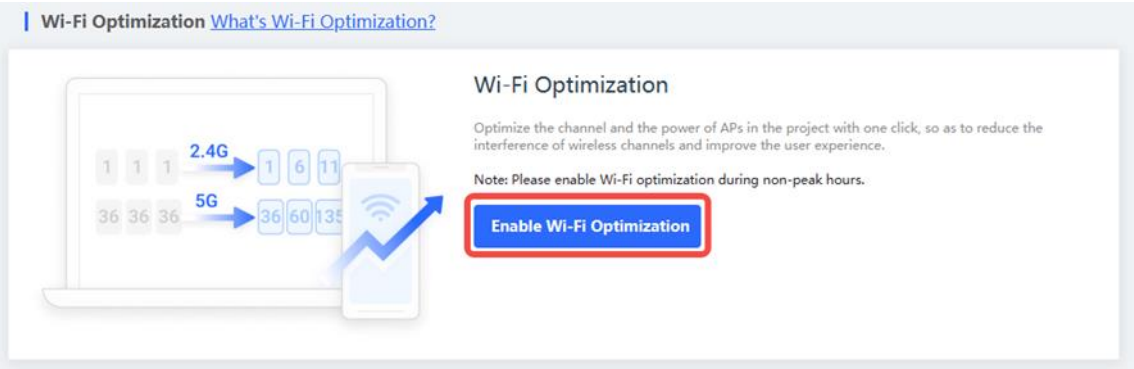
Wi-Fi optimization is applicable to the following scenarios:

- 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.

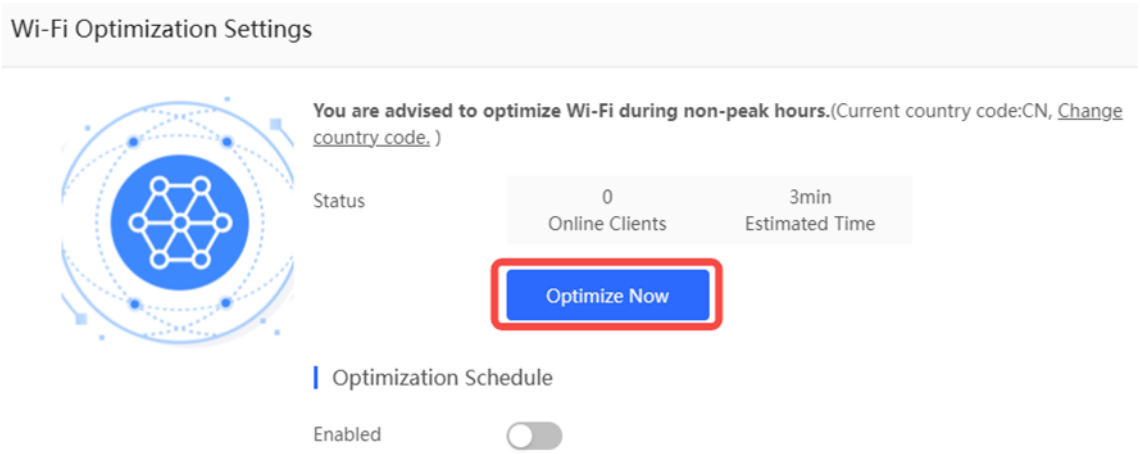
Procedure

(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**.



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

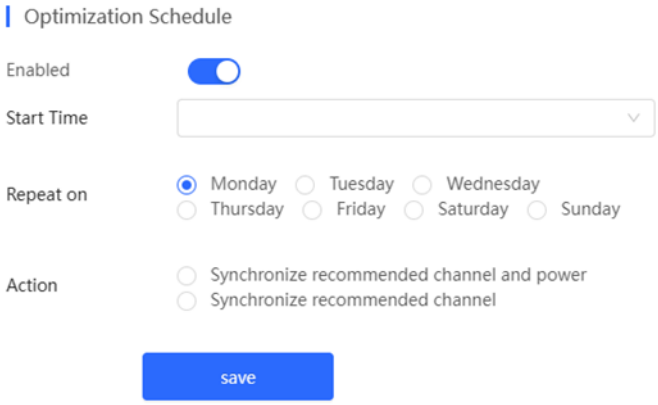


Online Clients: indicates the number of all online wireless clients.

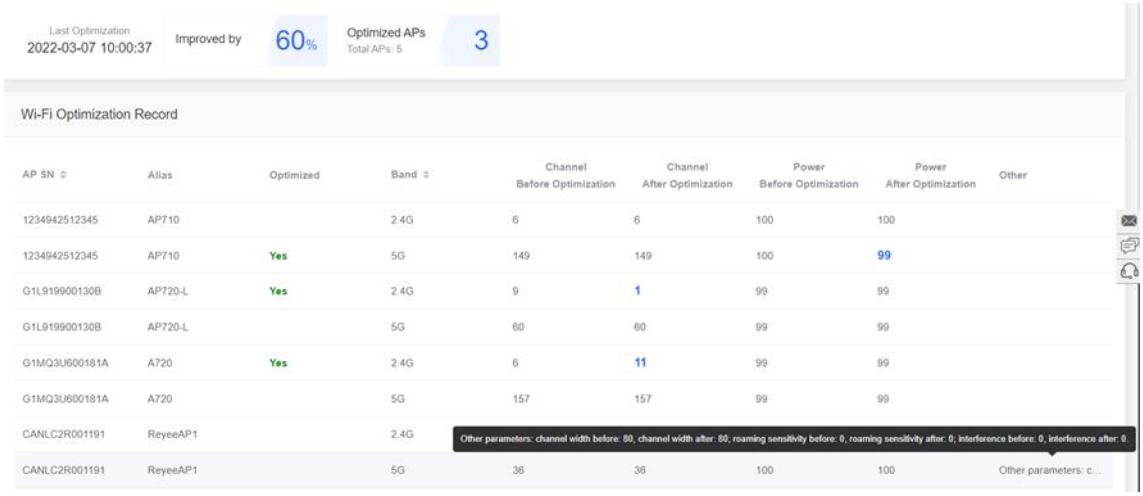
Estimated Time: indicates the estimated time to complete optimization.

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**.



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



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.

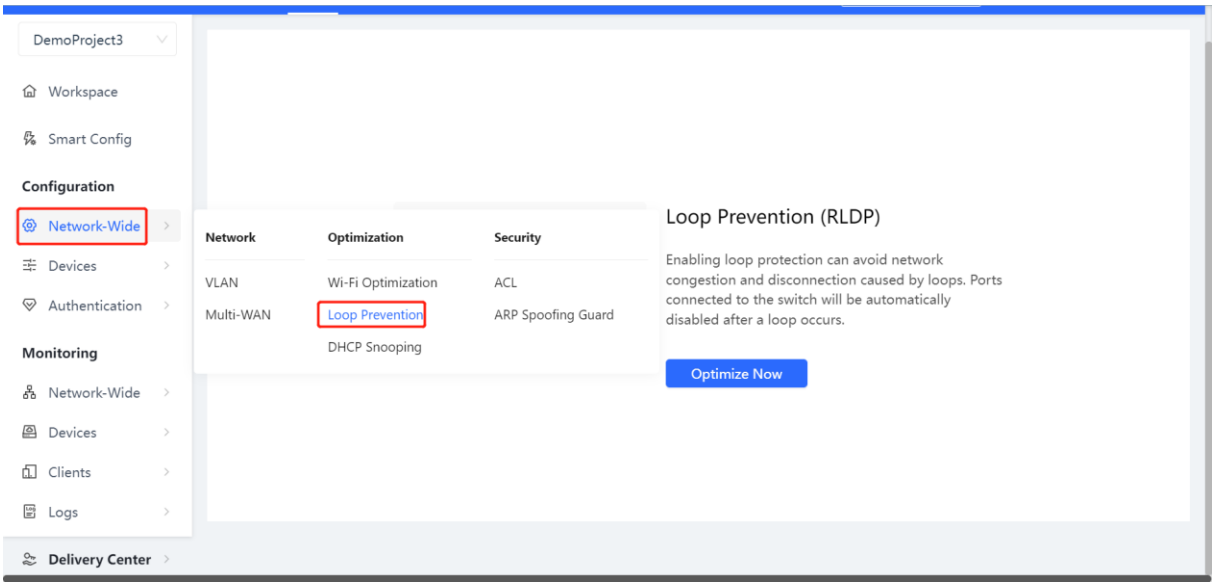
5.2 Loop Prevention

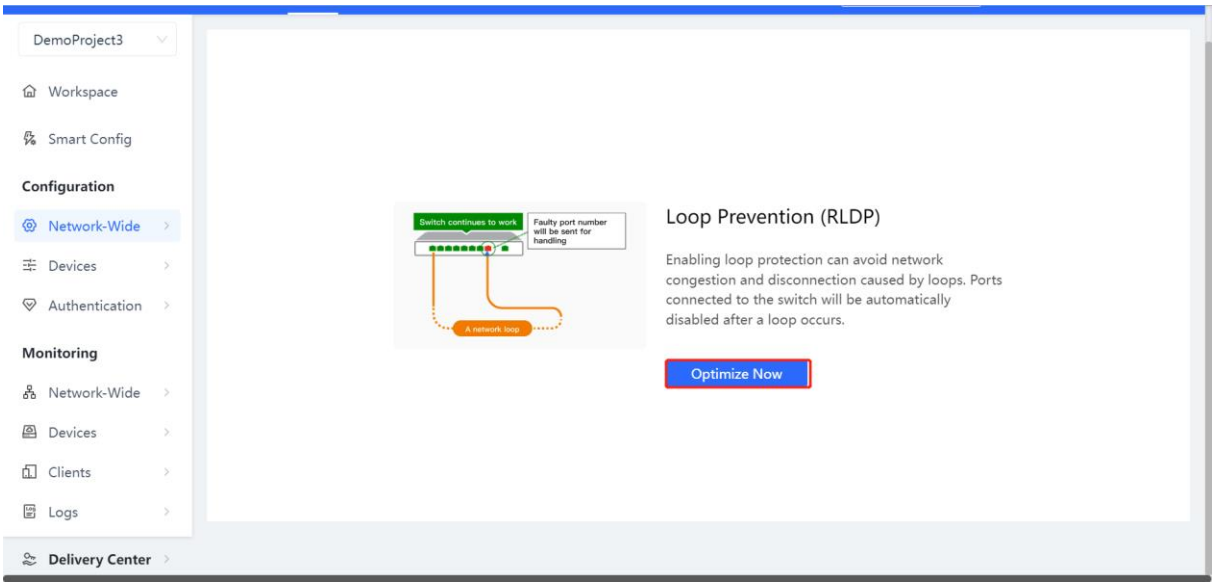
5.2.1 Overview

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.

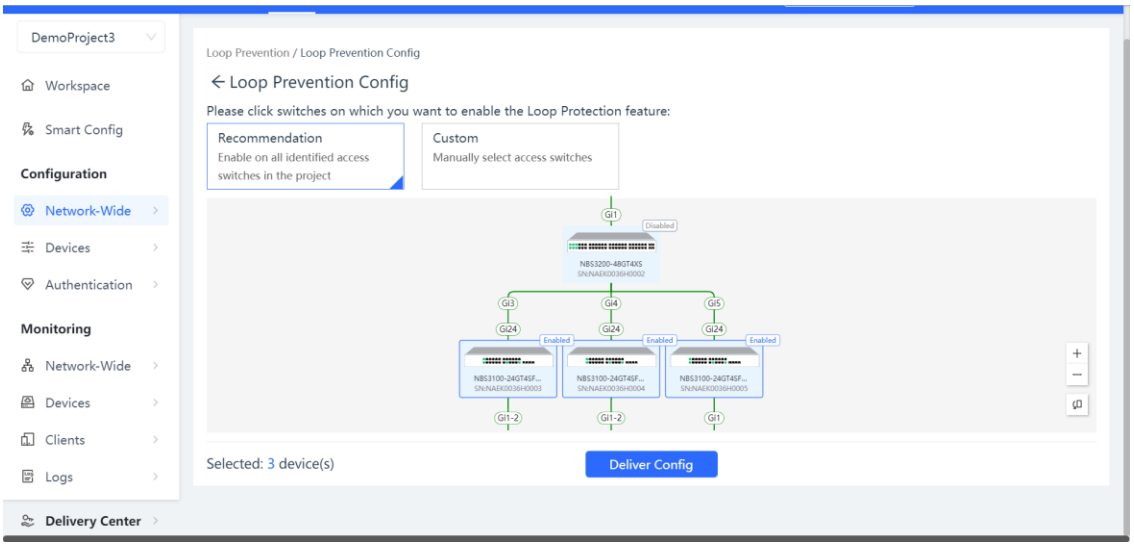
5.2.2 Configuration Steps

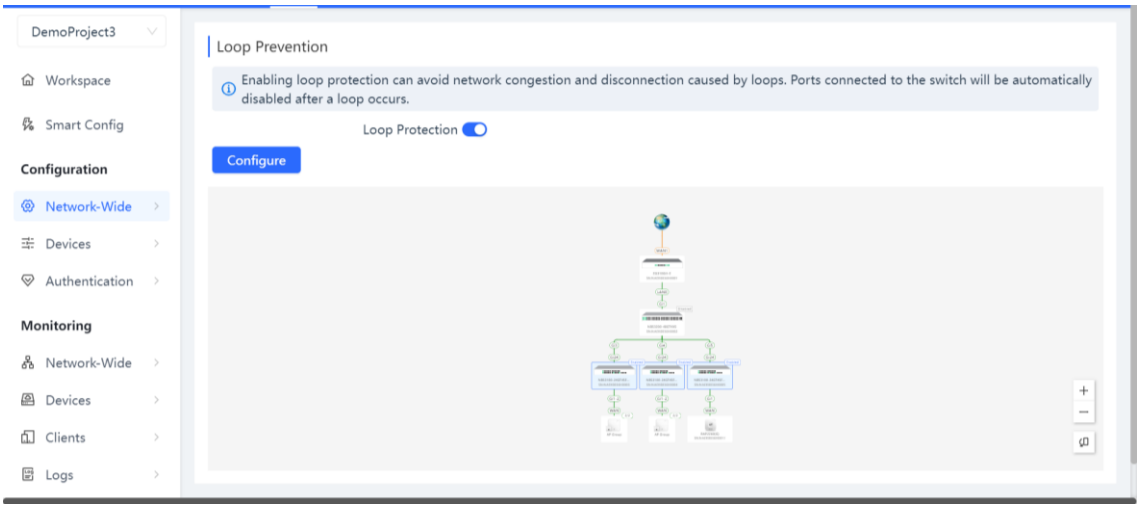
Choose **Configuration** > **Network-Wide** > **Optimization** > **Loop Prevention**.





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



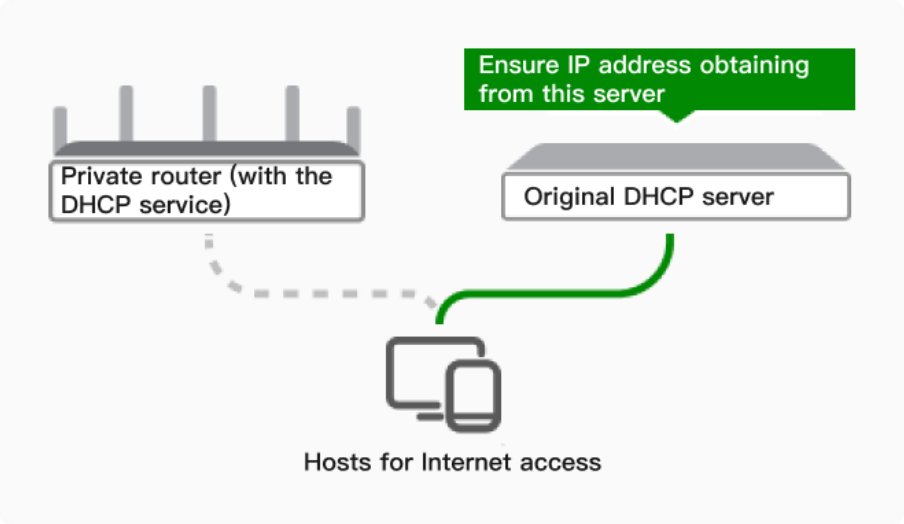


5.3 DHCP Snooping

5.3.1 Overview

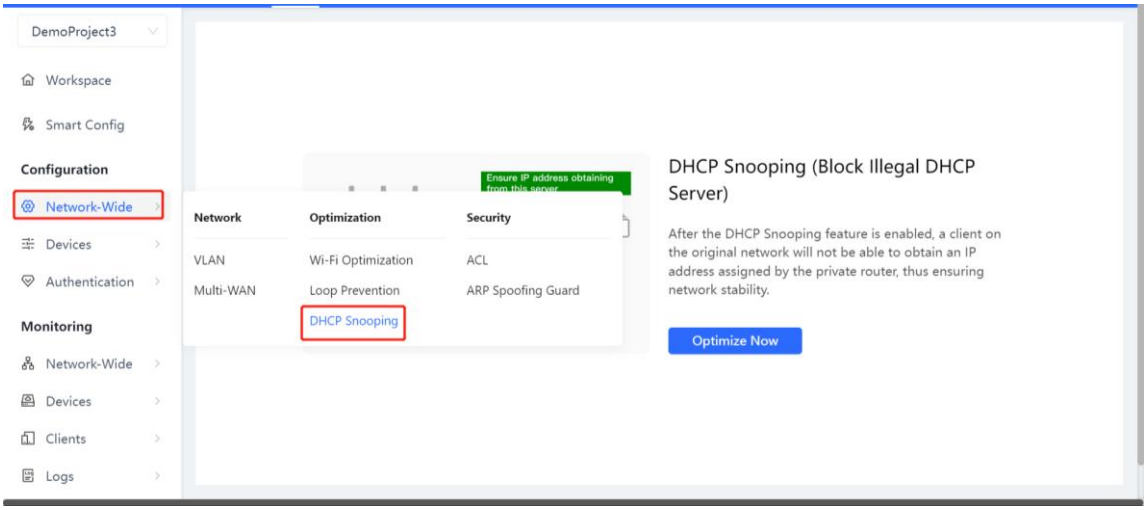
If a private router is connected to the network, some clients may obtain incorrect IP addresses and fail to access the Internet.

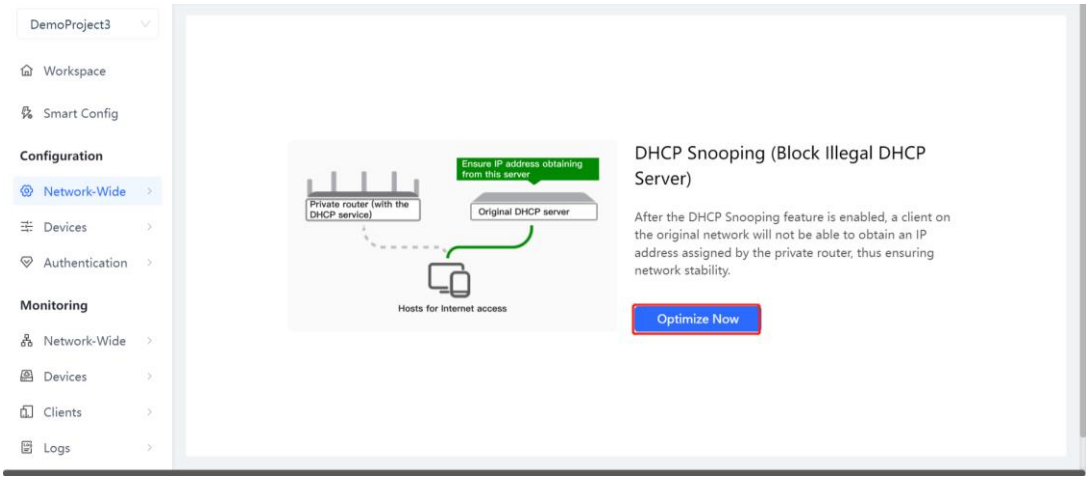
After the DHCP Snooping feature is enabled, a client on the original network will not be able to obtain an IP address assigned by the private router, thus ensuring network stability.



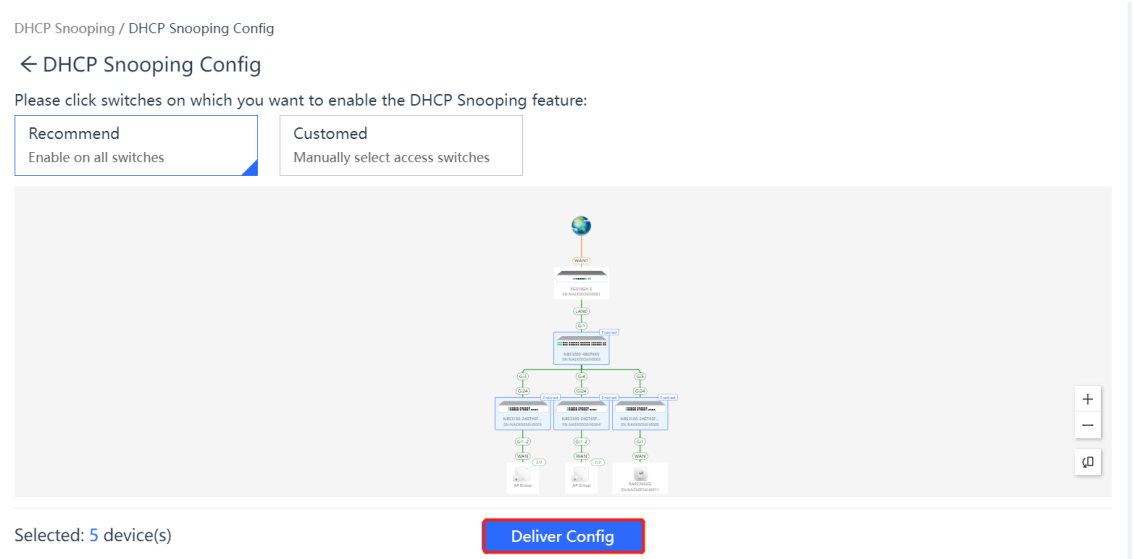
5.3.2 Configuration Steps

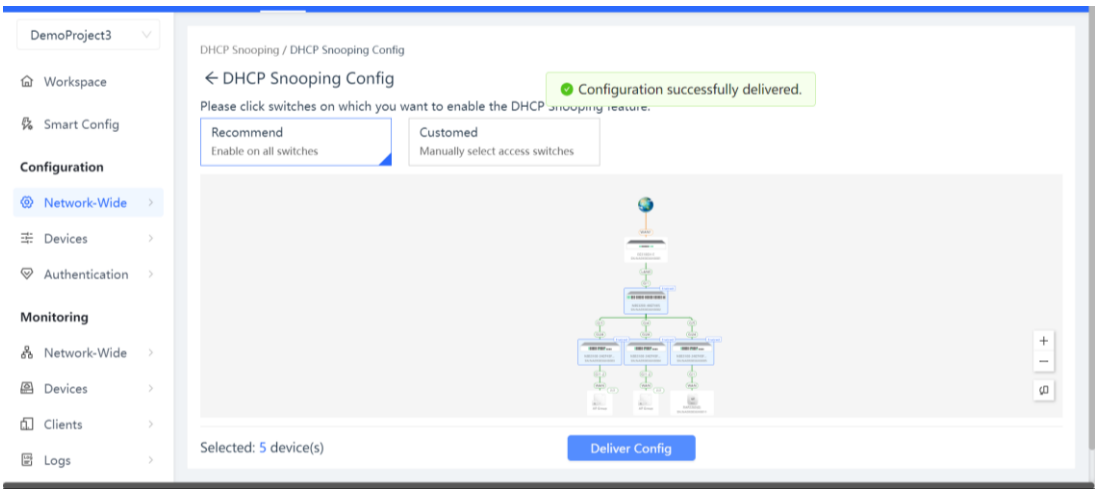
Choose **Configuration** > **Network-Wide** > **Optimization** > **DHCP Snooping**.

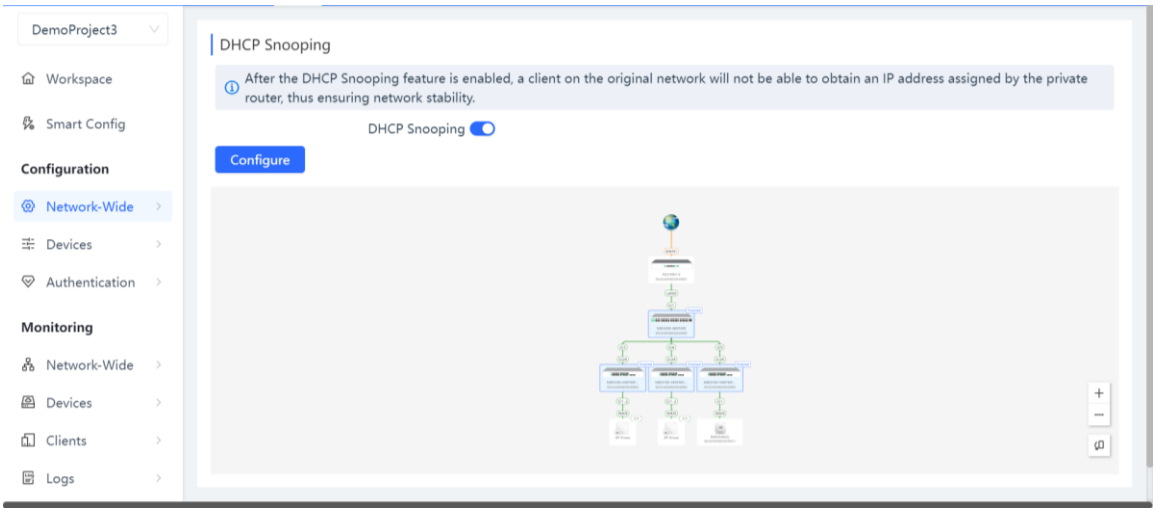




Click **Optimize Now**. You are advised to use the default value. Click **Deliver Config**.







5.4 Traffic Control

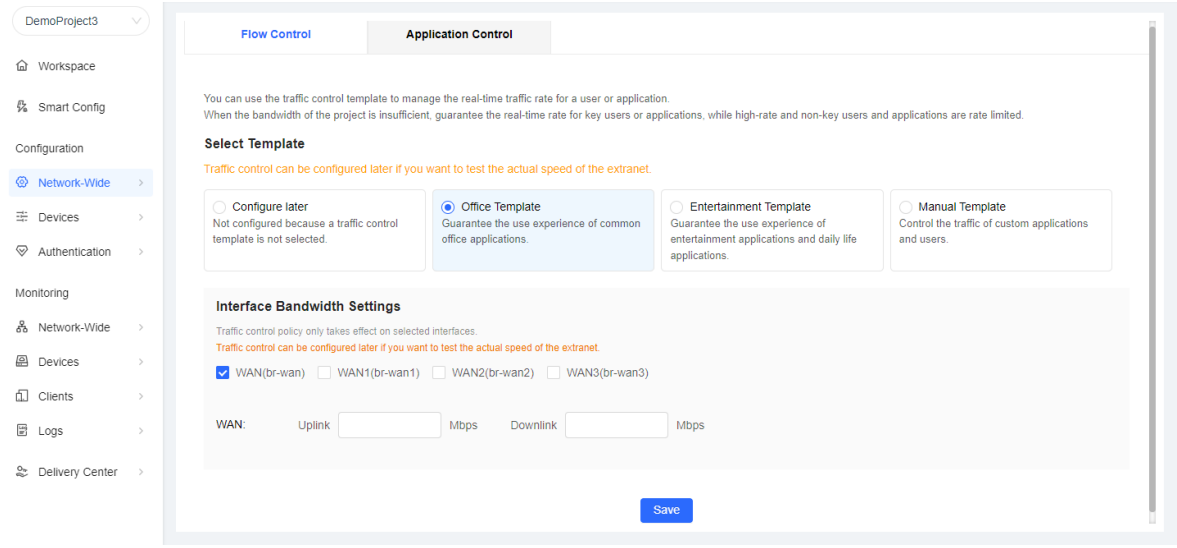
Set real-time traffic rate for a user or an application.

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.



2. Select a template.

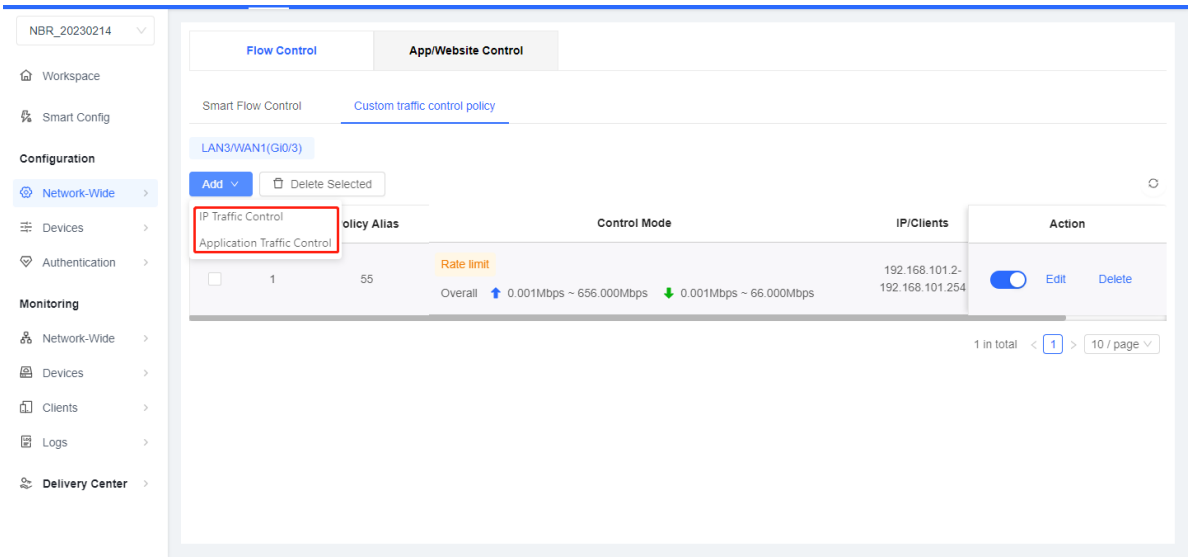
Configure later: indicates that traffic control is disabled.

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.

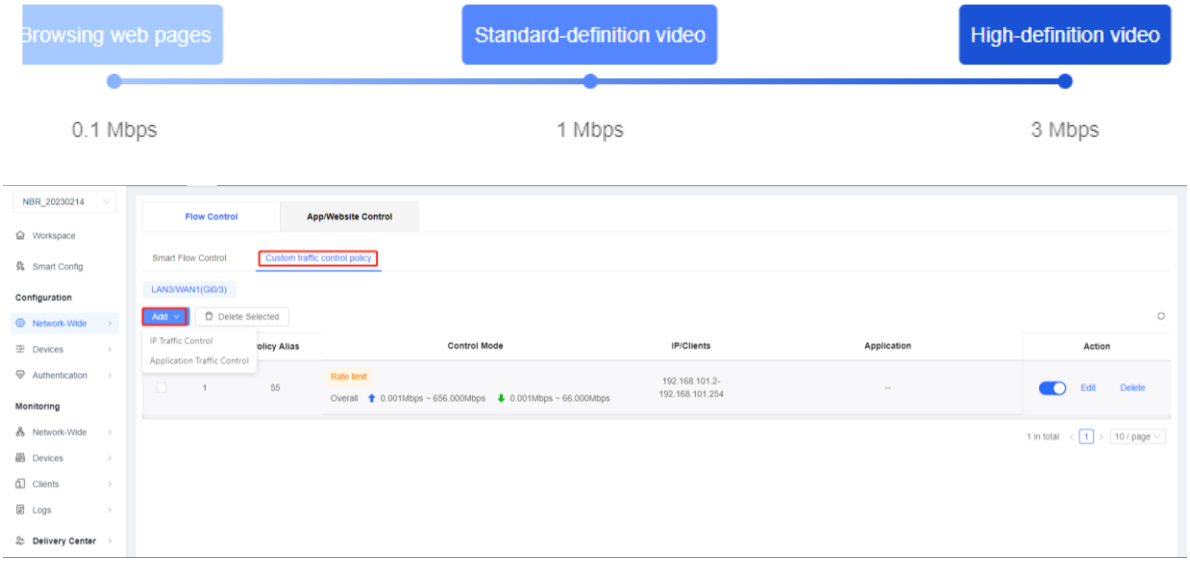
Entertainment Template: indicates that the embedded smart traffic control policy guarantees the traffic of entertainment and common daily life applications, and user-defined policies can be added.

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.

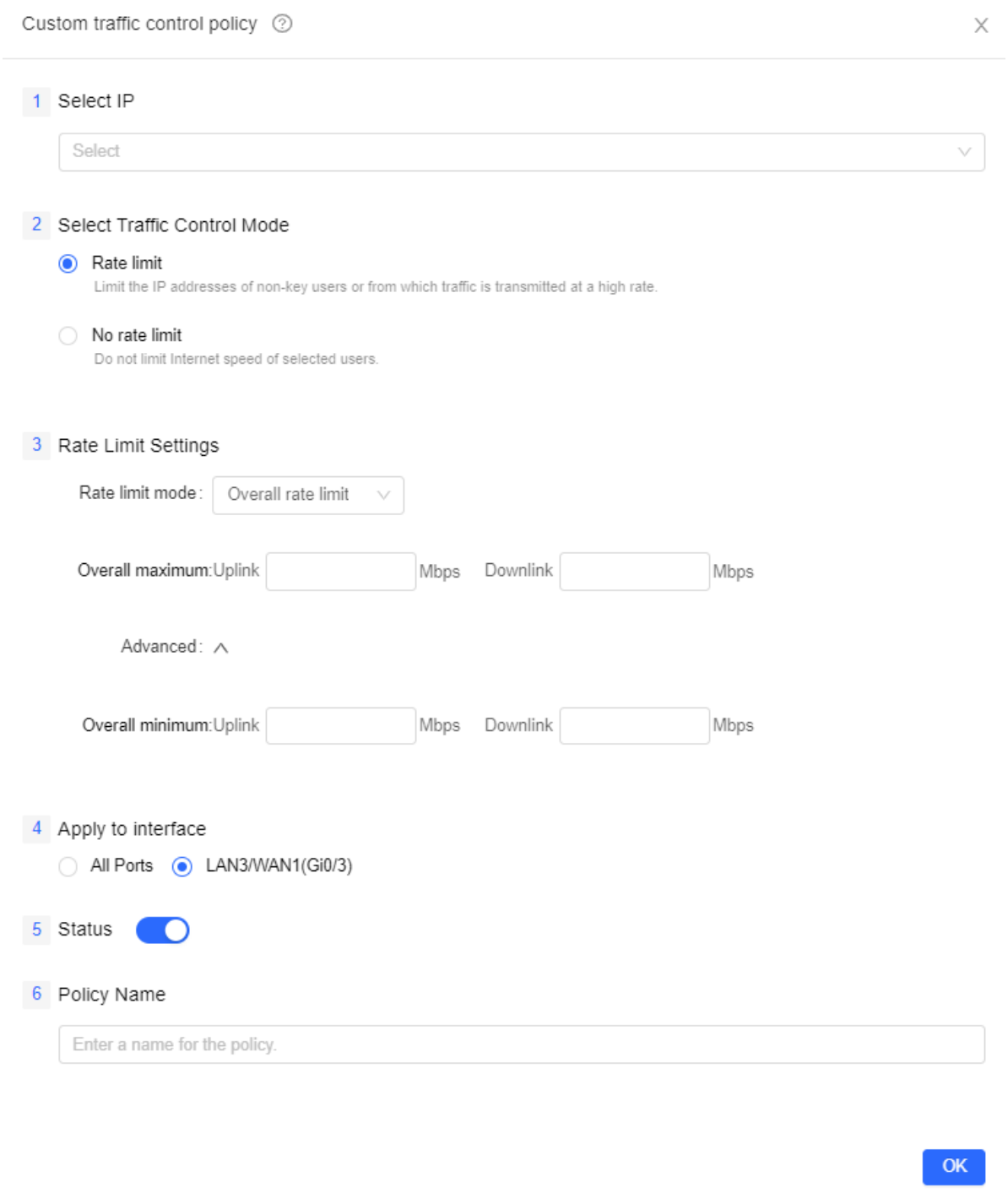
Rate Limit Settings: **Overall rate limit** indicates the overall maximum rate and **Per IP rate limit** indicates the maximum rate for each IP address.

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**.

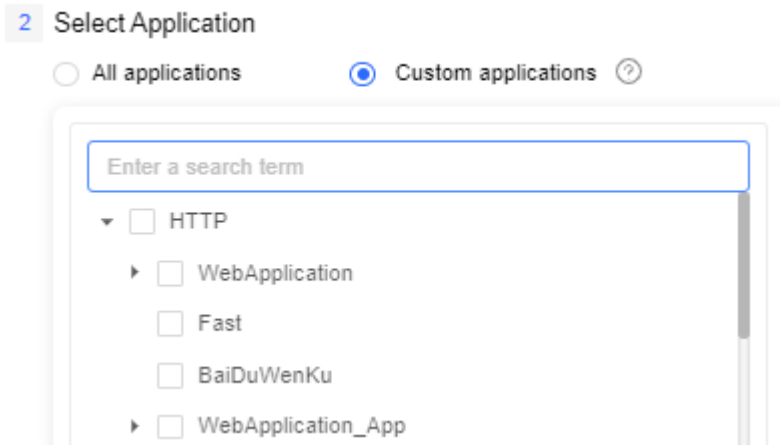
Policy Name: Configure a name for the policy to facilitate maintenance.



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.



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

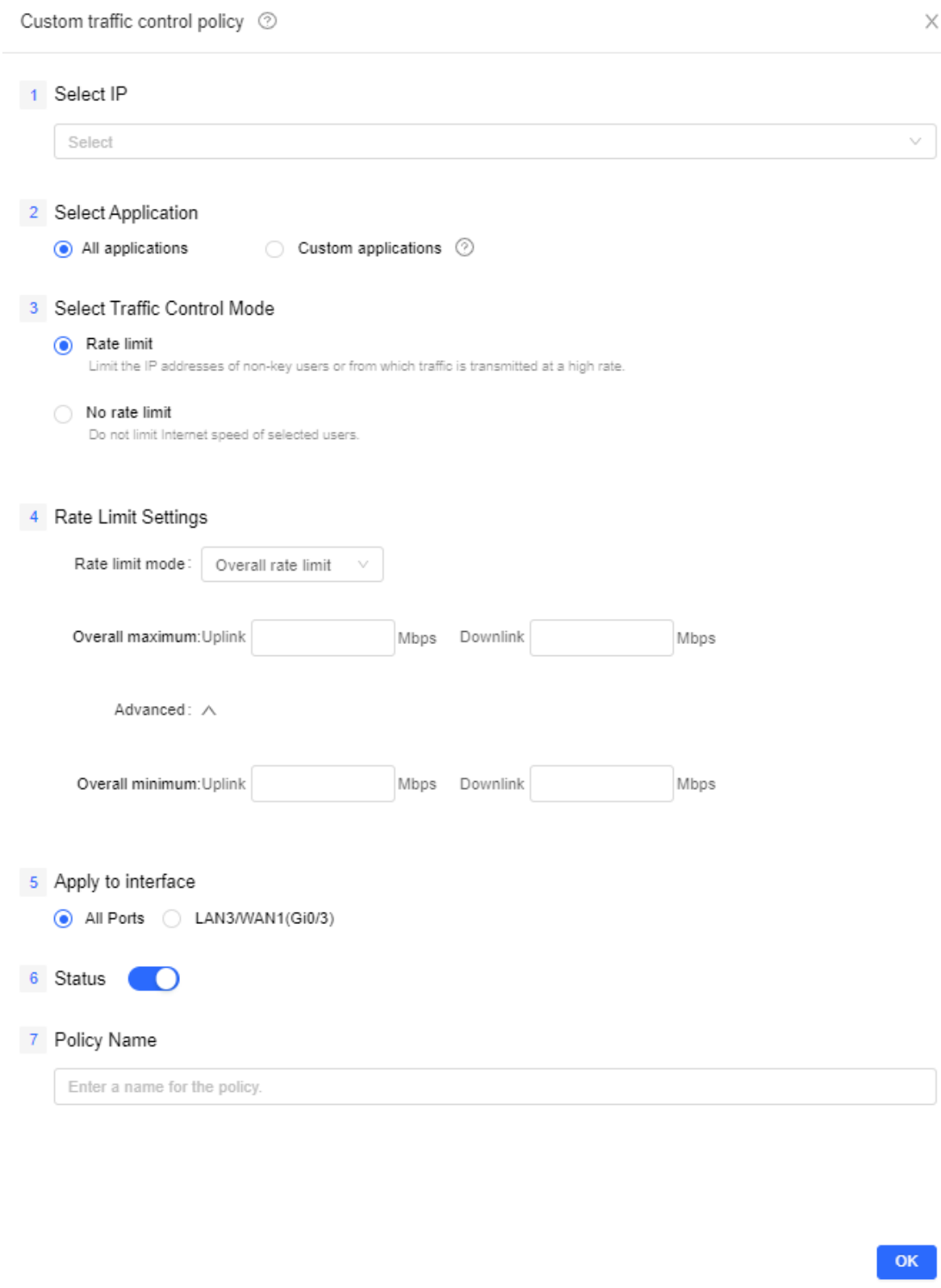
Rate Limit Settings: **Overall rate limit** indicates the overall maximum rate and **Per IP rate limit** indicates the maximum rate for each IP address.

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.

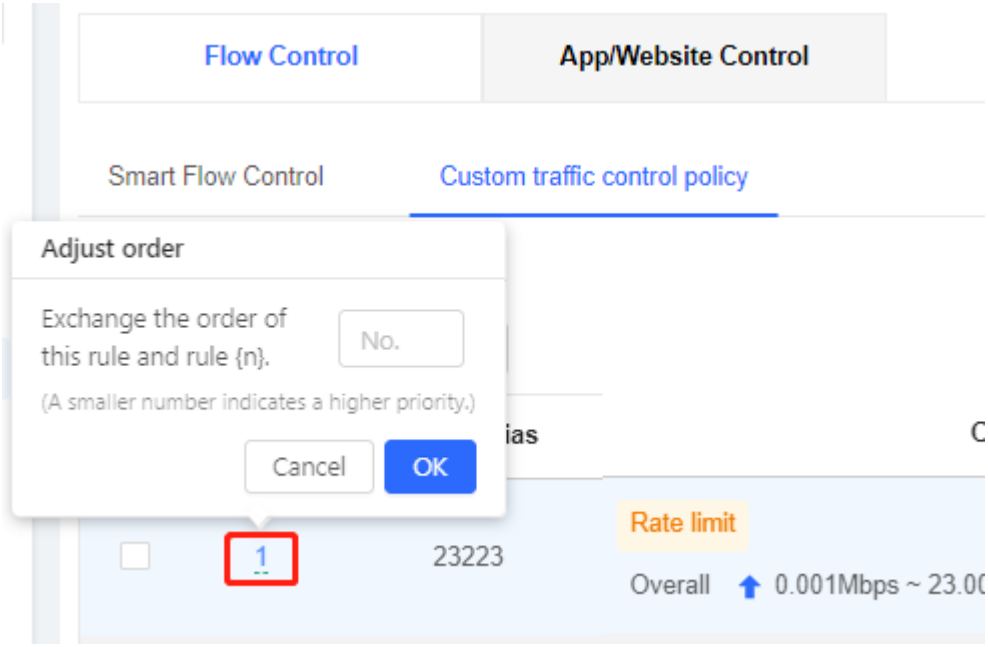
Apply to interface: indicates the port, in which the policy takes effect. You are advised to select **All Ports**.

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



5.4.3 Configuring the Policy Priority

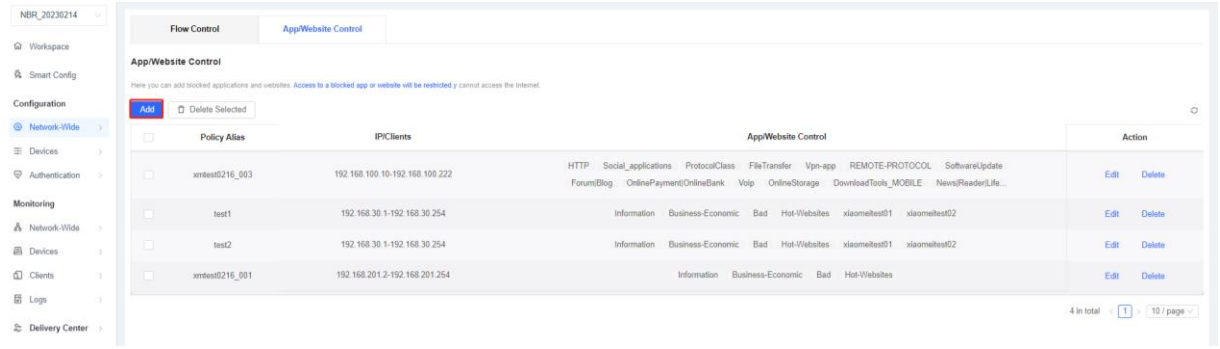
Click the number of a policy to adjust the policy sequence. A smaller number indicates a higher priority.



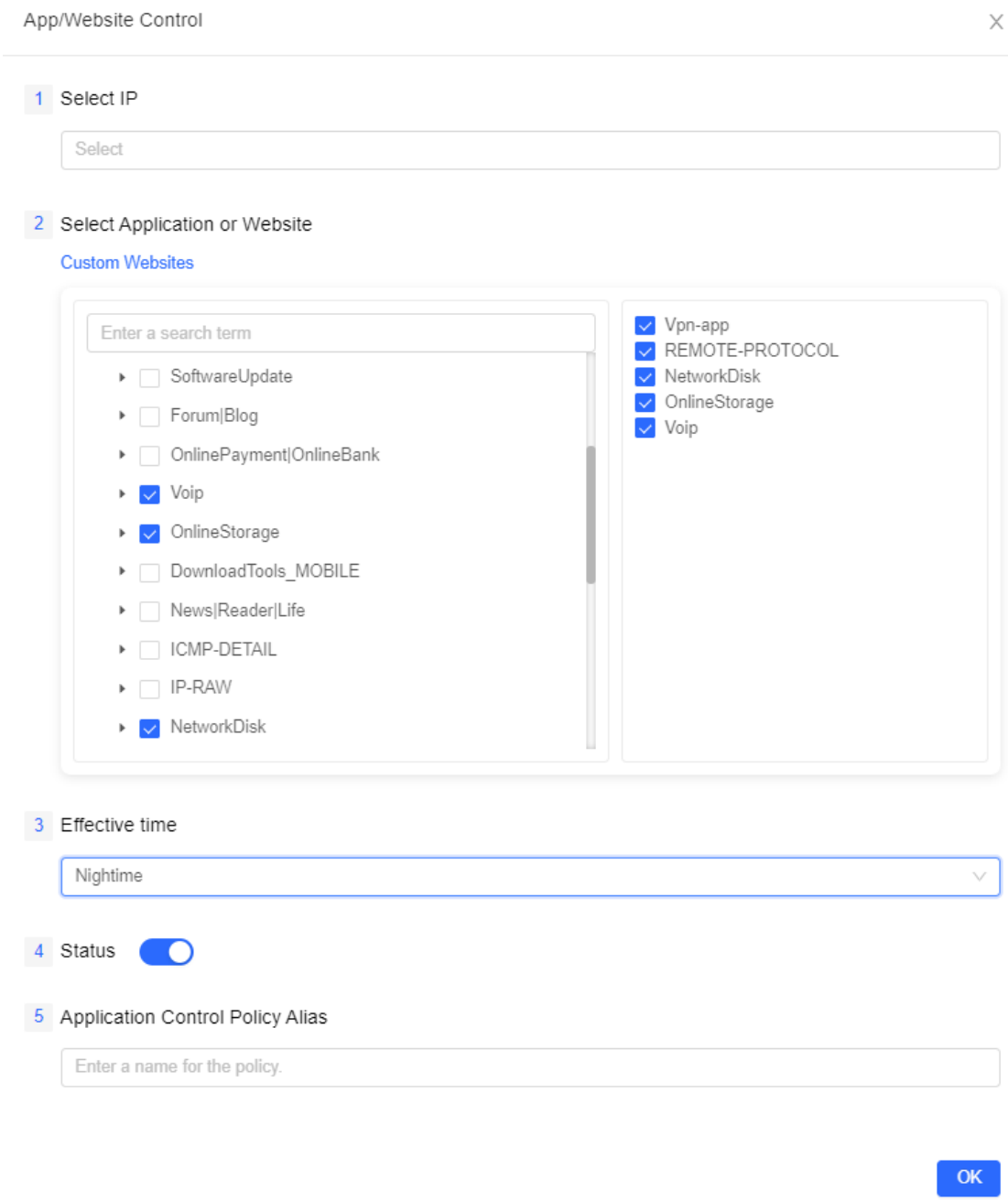
5.4.4 App/Website Control

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**.

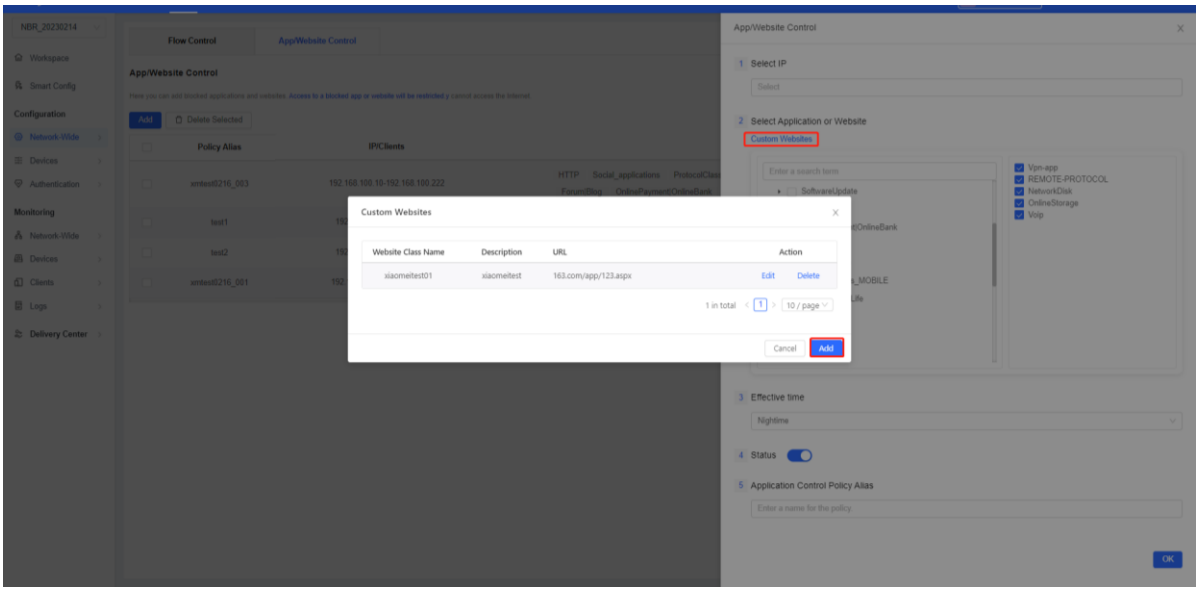


2. Configure a policy.



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.



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

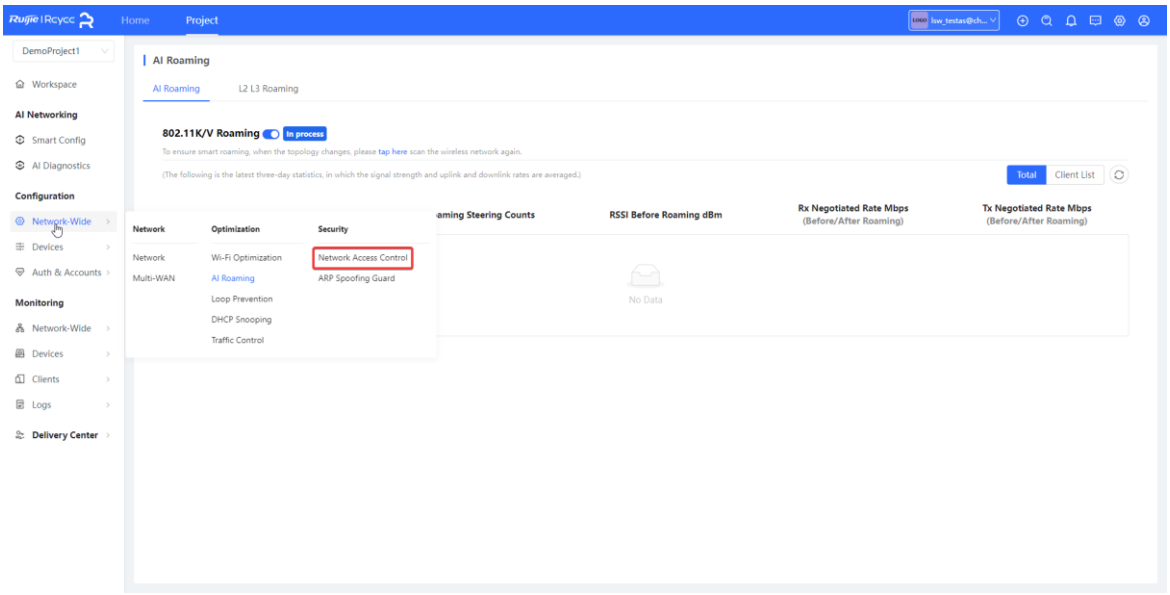
6.1.3 Configuration Steps

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

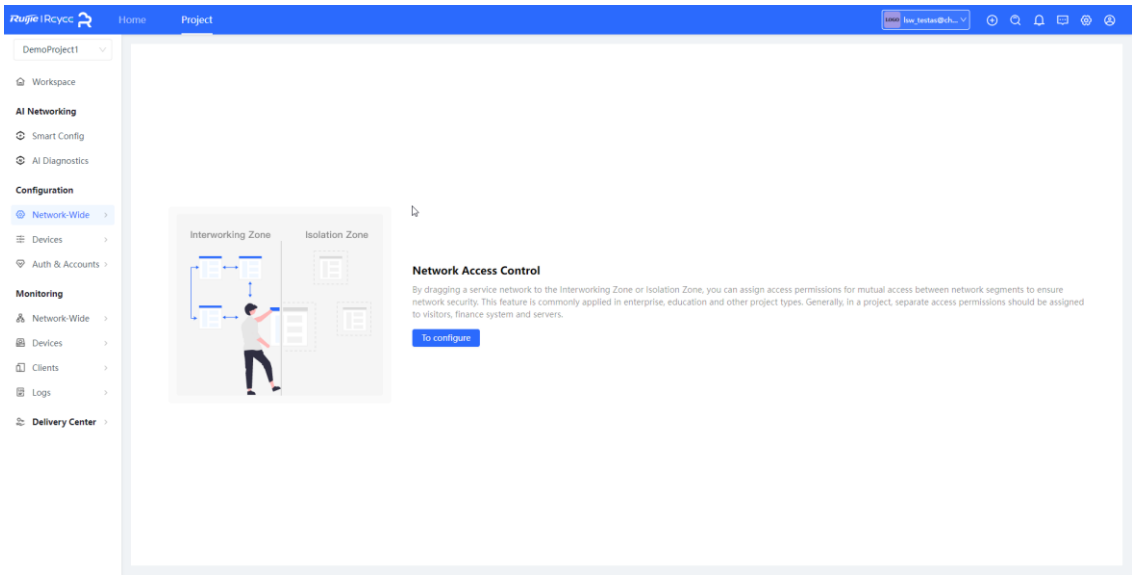
  Service networks in the interworking zone can access each other.

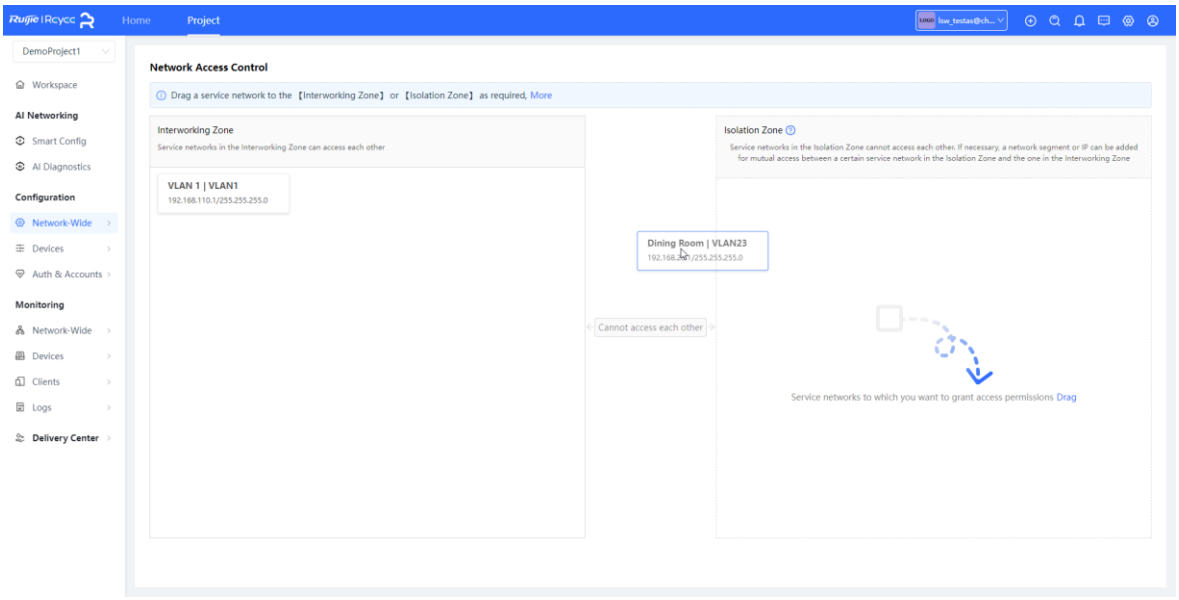
- Isolation Zone

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

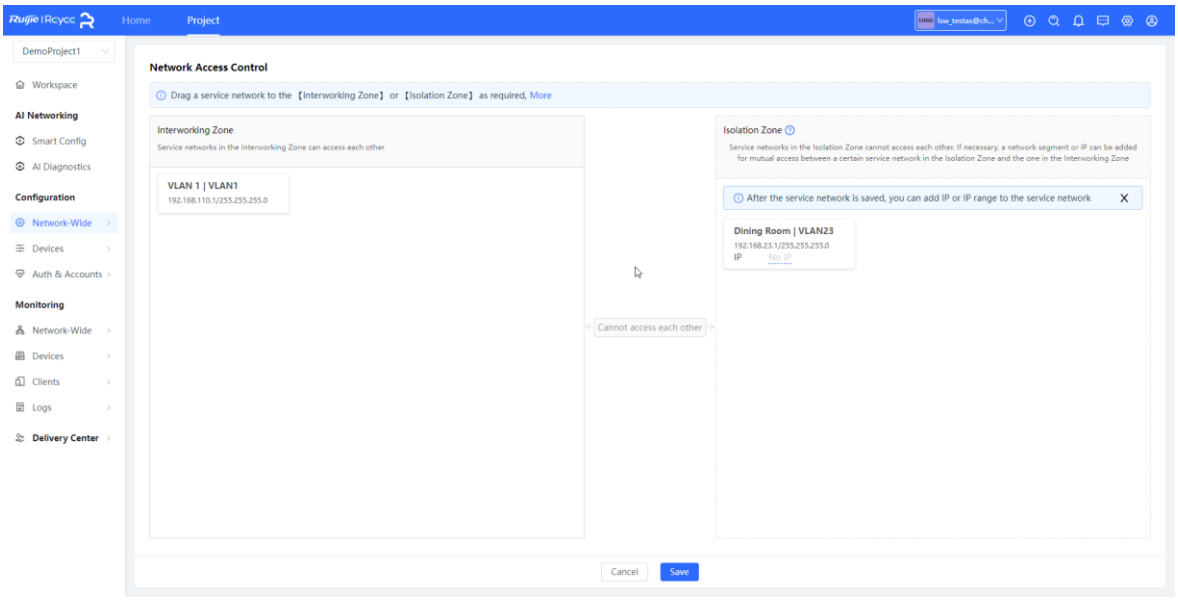
  Service network segments in the isolation zone are isolated from each other.

  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.





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

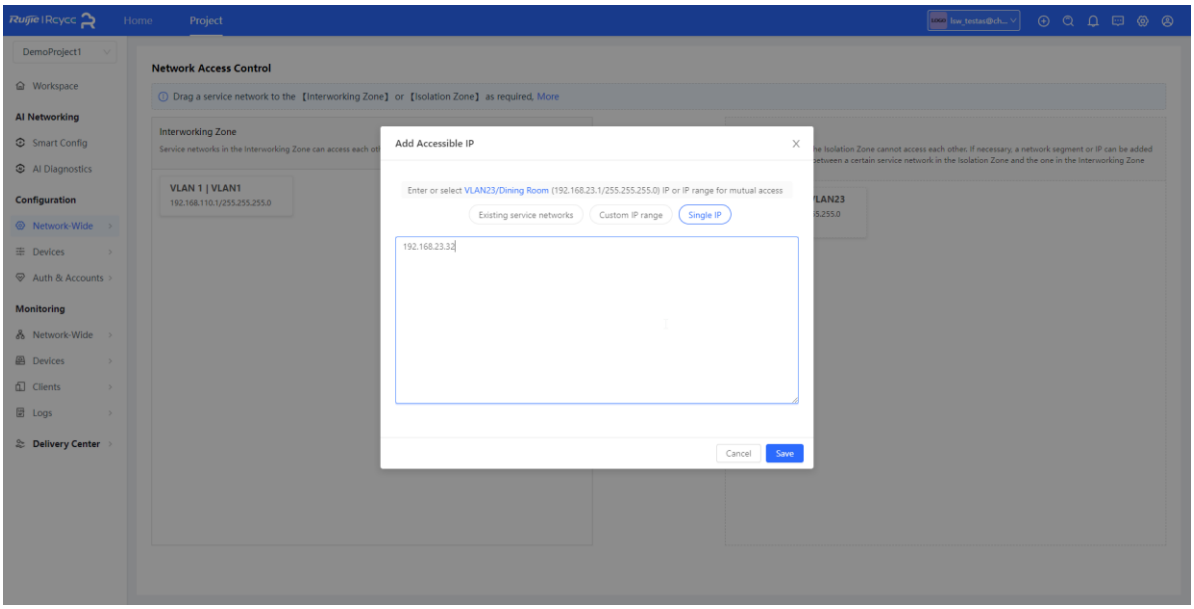


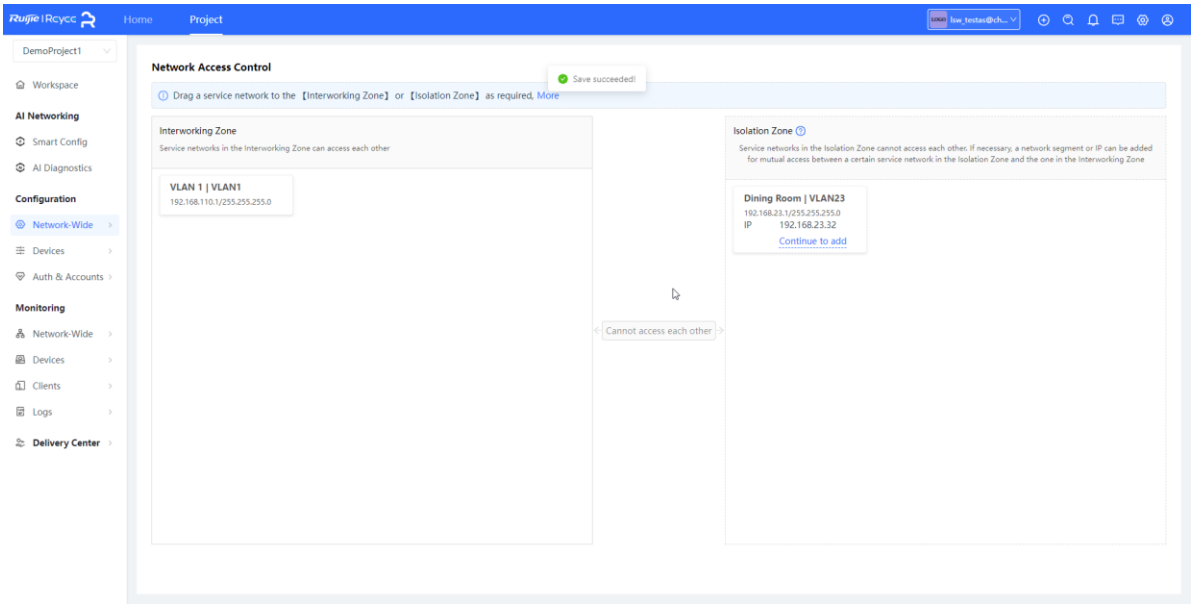
(3) (Optional) In **Isolation Zone**, click **No IP**.

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**.





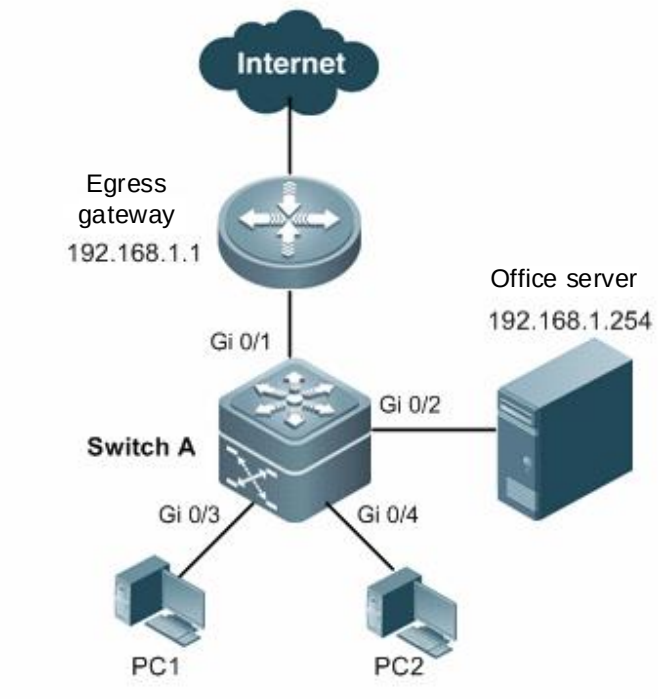
6.2 Gateway Anti-ARP Spoofing Solution

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.

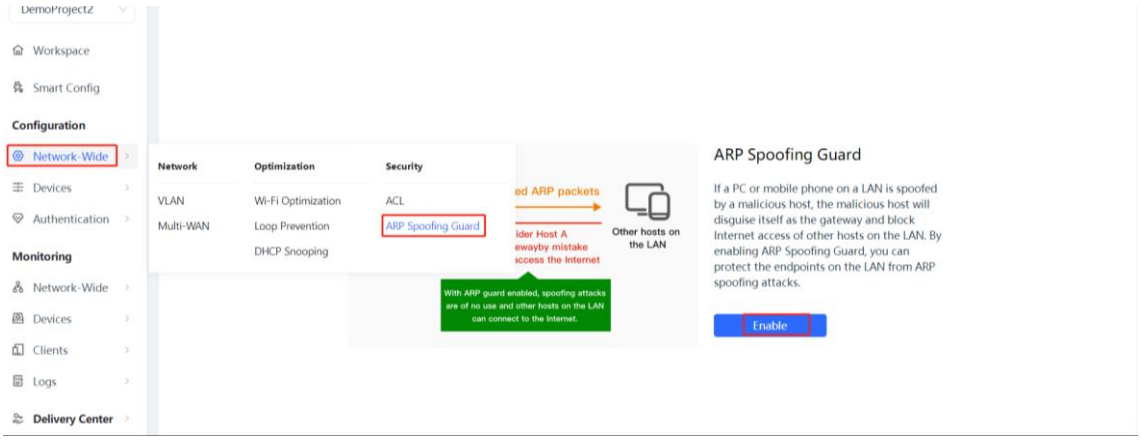
Enable gateway anti-ARP spoofing on the ports (Gi 0/3 and Gi 0/4 in this example) of the access switch (switch A) that are directly connected to PCs. The gateway address is the intranet gateway address and the intranet server address.

6.2.3 Models of Products Supporting the Feature and Topology

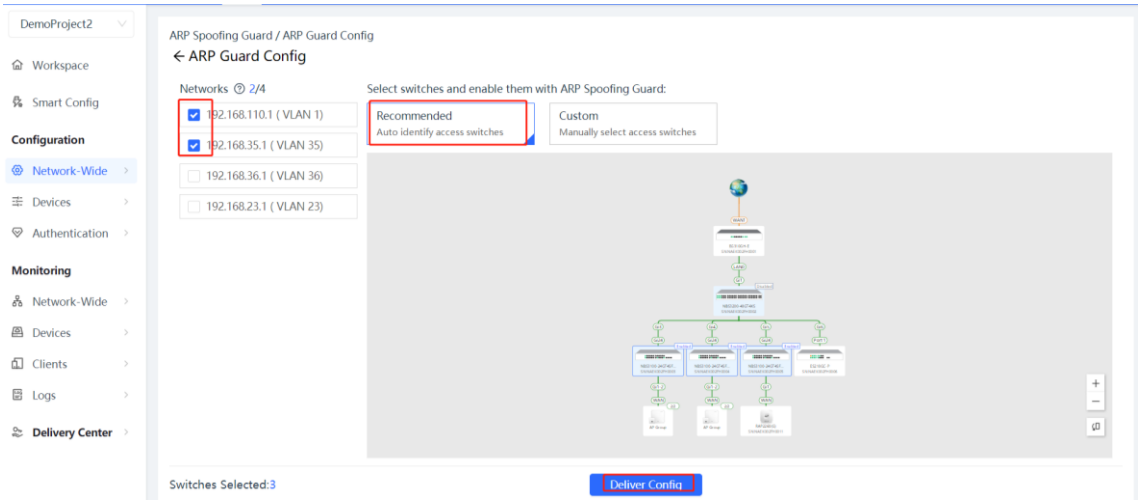
Product Type	Device Name	Version
Switch	NBS series	The version is unlimited. You are advised to upgrade the device to the latest version.

6.2.4 Configuration Steps

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

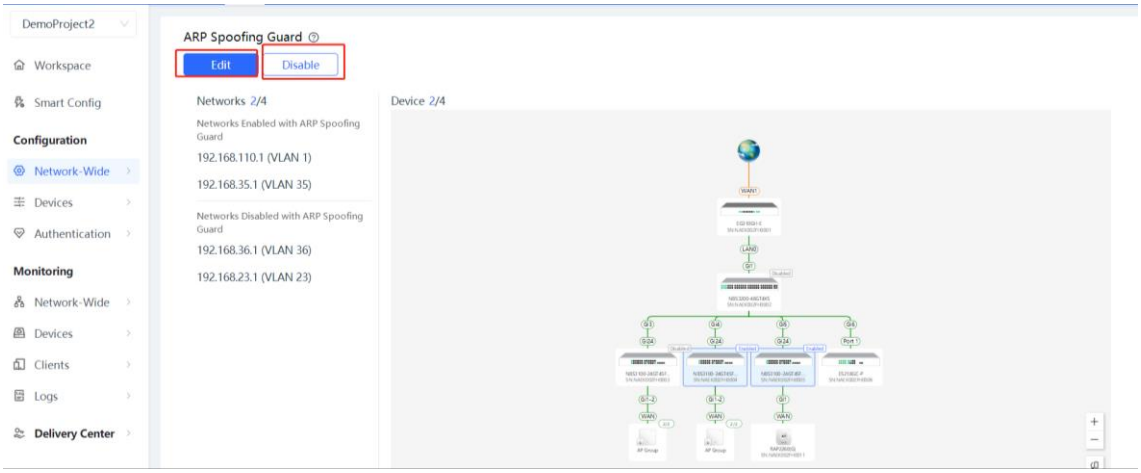


Select the gateway IP address and switch, for which anti-ARP spoofing needs to be configured. The system automatically lists the gateway IP addresses of the service networks. By default (recommended), all access switches of the current network are selected.



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**.

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**.



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

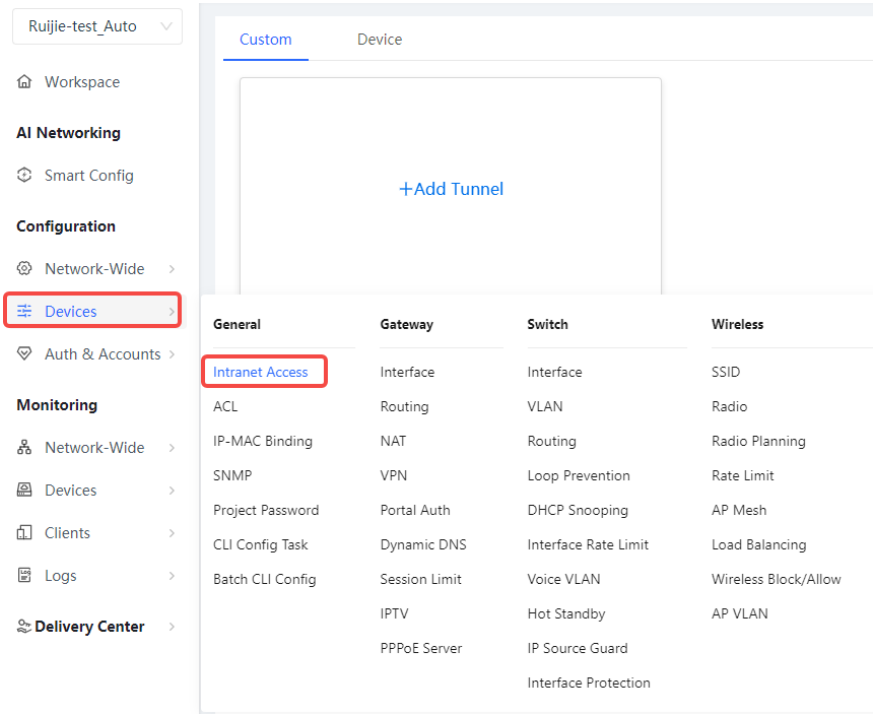
7.1 Intranet Access

7.1.1 Overview

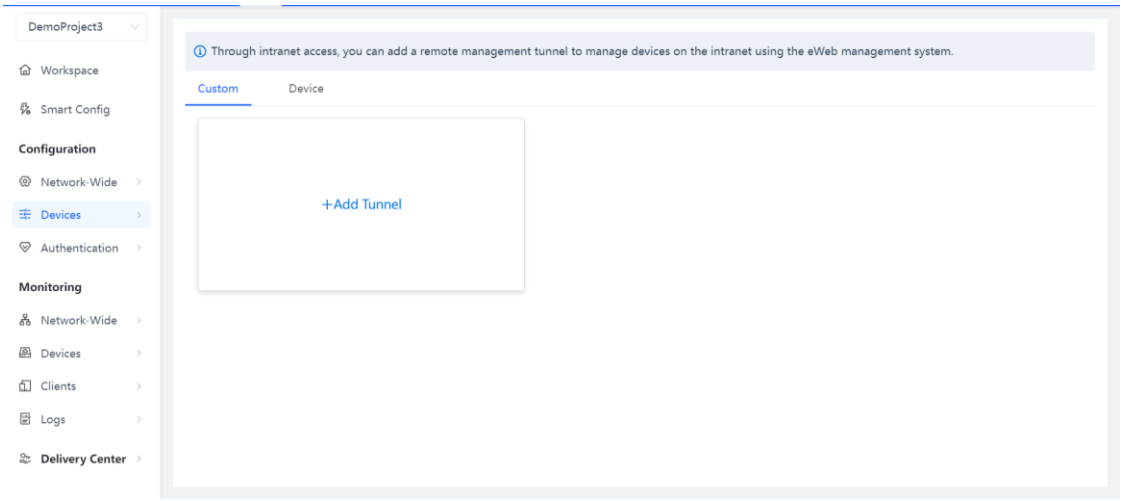
Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.

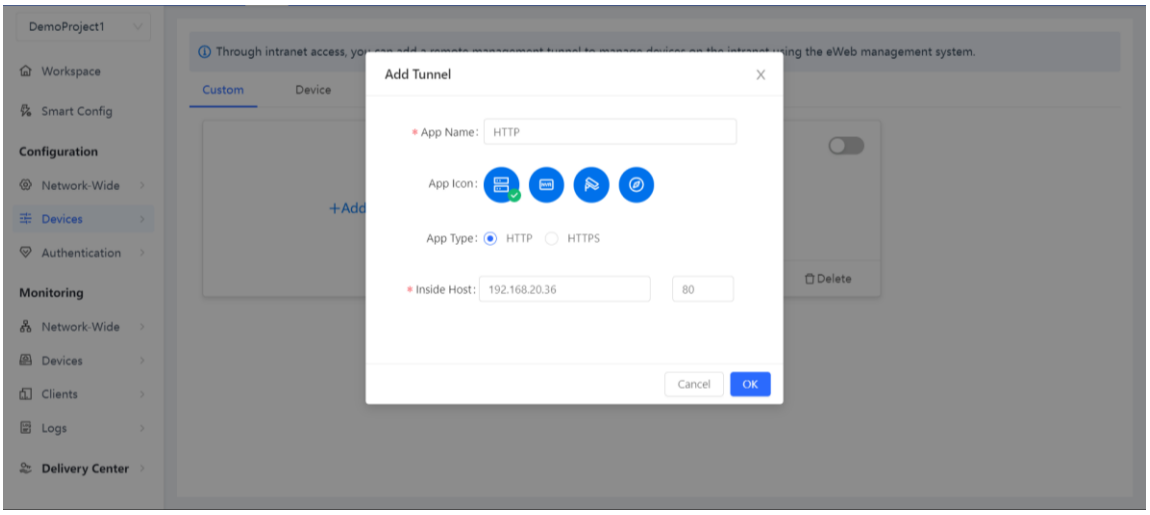
7.1.2 Configuration Steps

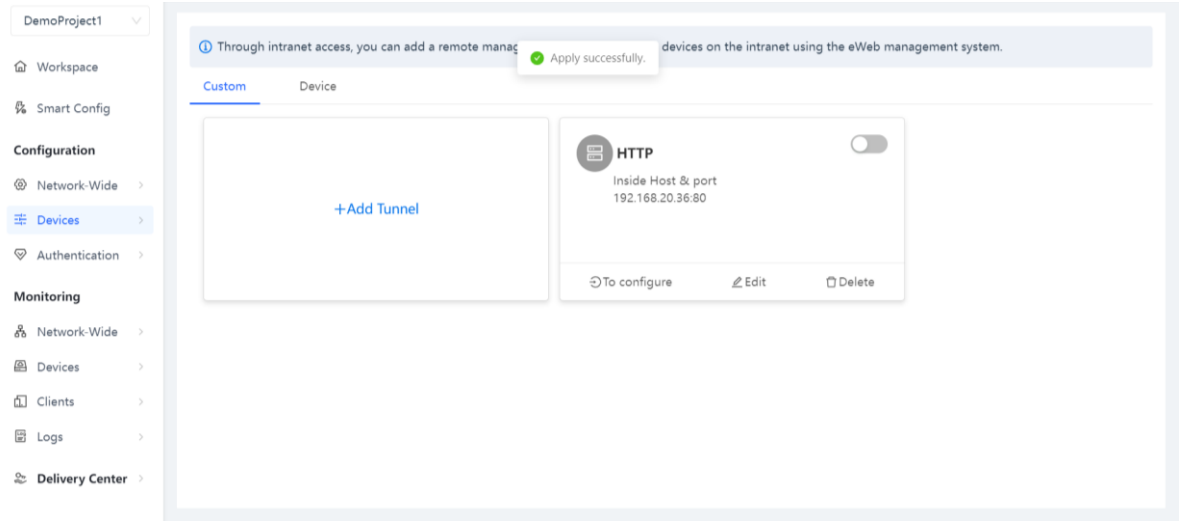
Choose **Configuration** > **Devices** > **General** > **Intranet Access**.

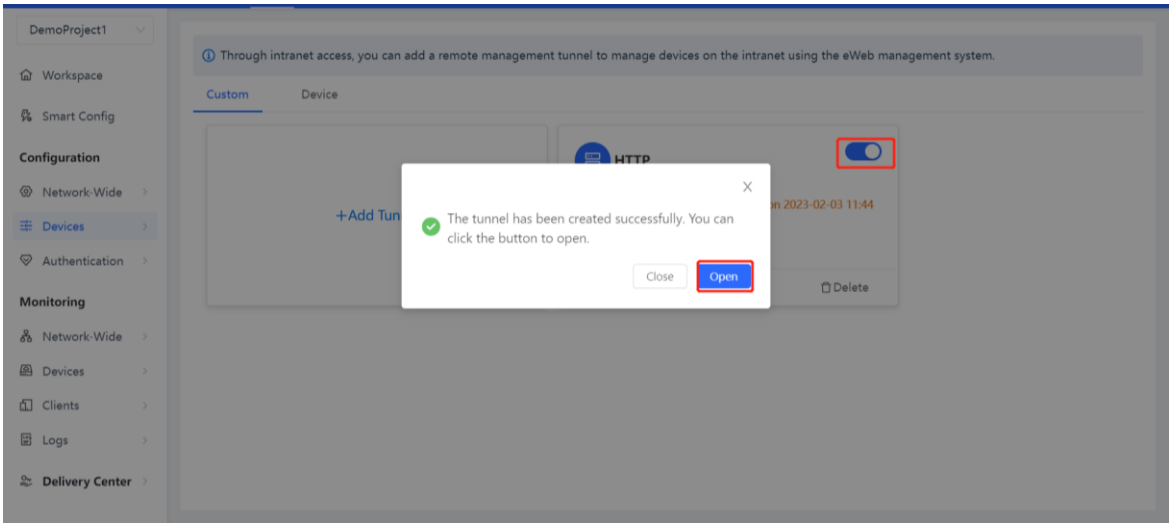


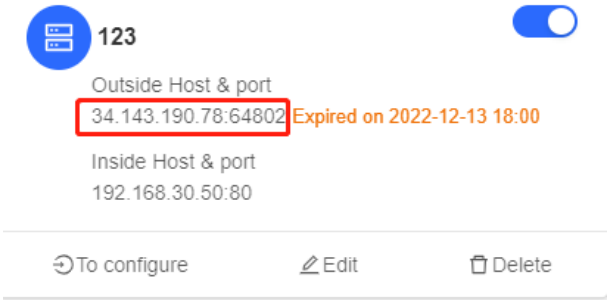
Click **Add Tunnel** on the **Intranet Access** page. You can create a remote tunnel to access the intranet devices.

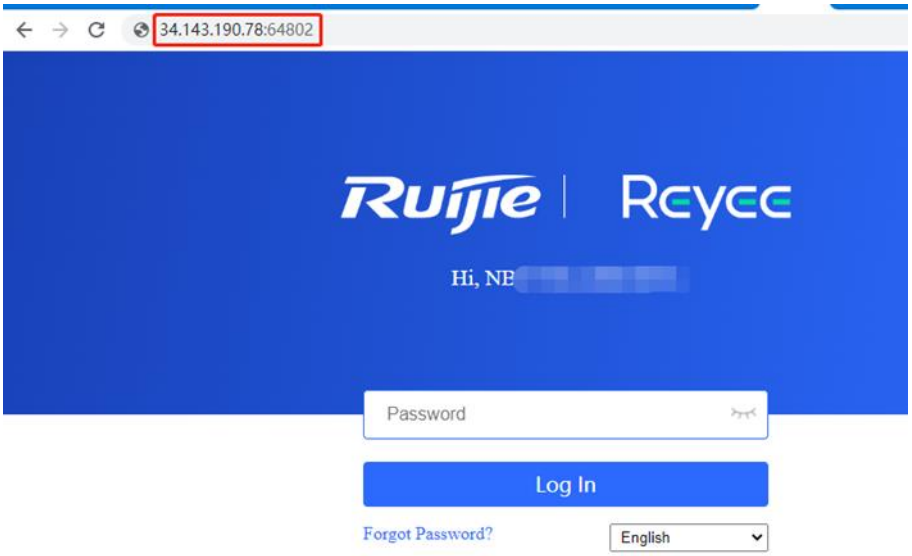



DemoProject1
Workspace
Smart Config
Configuration
Network-Wide
Devices
Authentication
Monitoring
Network-Wide
Devices
Clients
Logs
Delivery Center
Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.
Custom
Device
Add Tunnel
App Name: HTTP
App Icon:
App Type: HTTP HTTPS
Inside Host: 192.168.20.36
80
Cancel
OK
Delete


DemoProject1
Workspace
Smart Config
Configuration
Network-Wide
Devices
Authentication
Monitoring
Network-Wide
Devices
Clients
Logs
Delivery Center
Through intranet access, you can add a remote manag
Apply successfully.
devices on the intranet using the eWeb management system.
Custom
Device
+Add Tunnel
HTTP
Inside Host & port
192.168.20.36:80
To configure
Edit
Delete


DemoProject1
Workspace
Smart Config
Configuration
Network-Wide
Devices
Authentication
Monitoring
Network-Wide
Devices
Clients
Logs
Delivery Center
Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.
Custom
Device
HTTP
The tunnel has been created successfully. You can click the button to open.
Close
Open
Delete

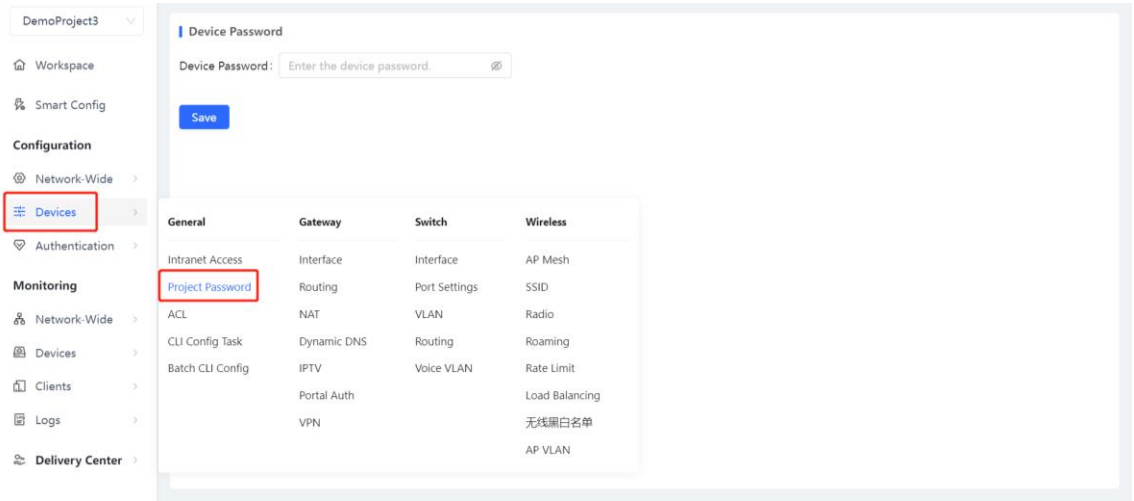


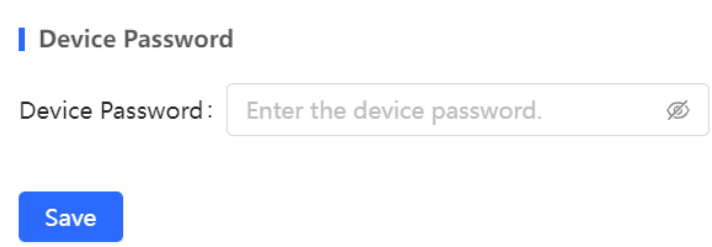


7.2 Project Password

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

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





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.

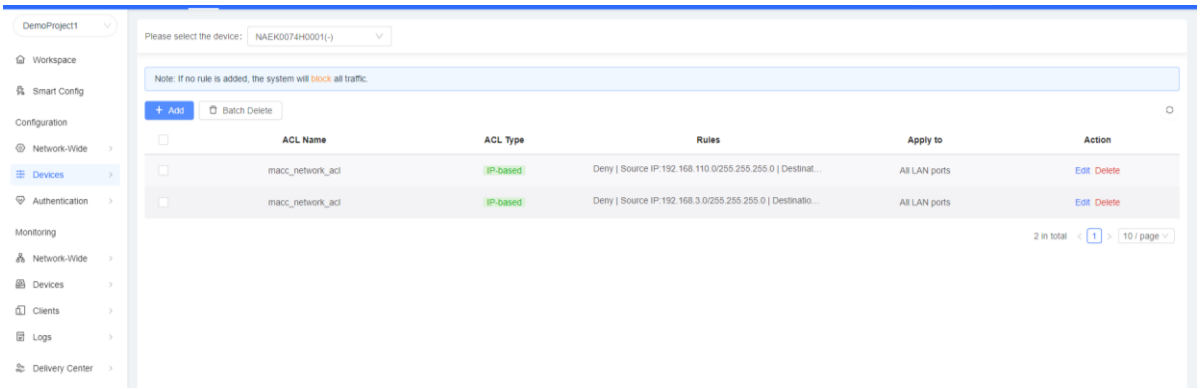
7.3.1 Creating ACL Rules

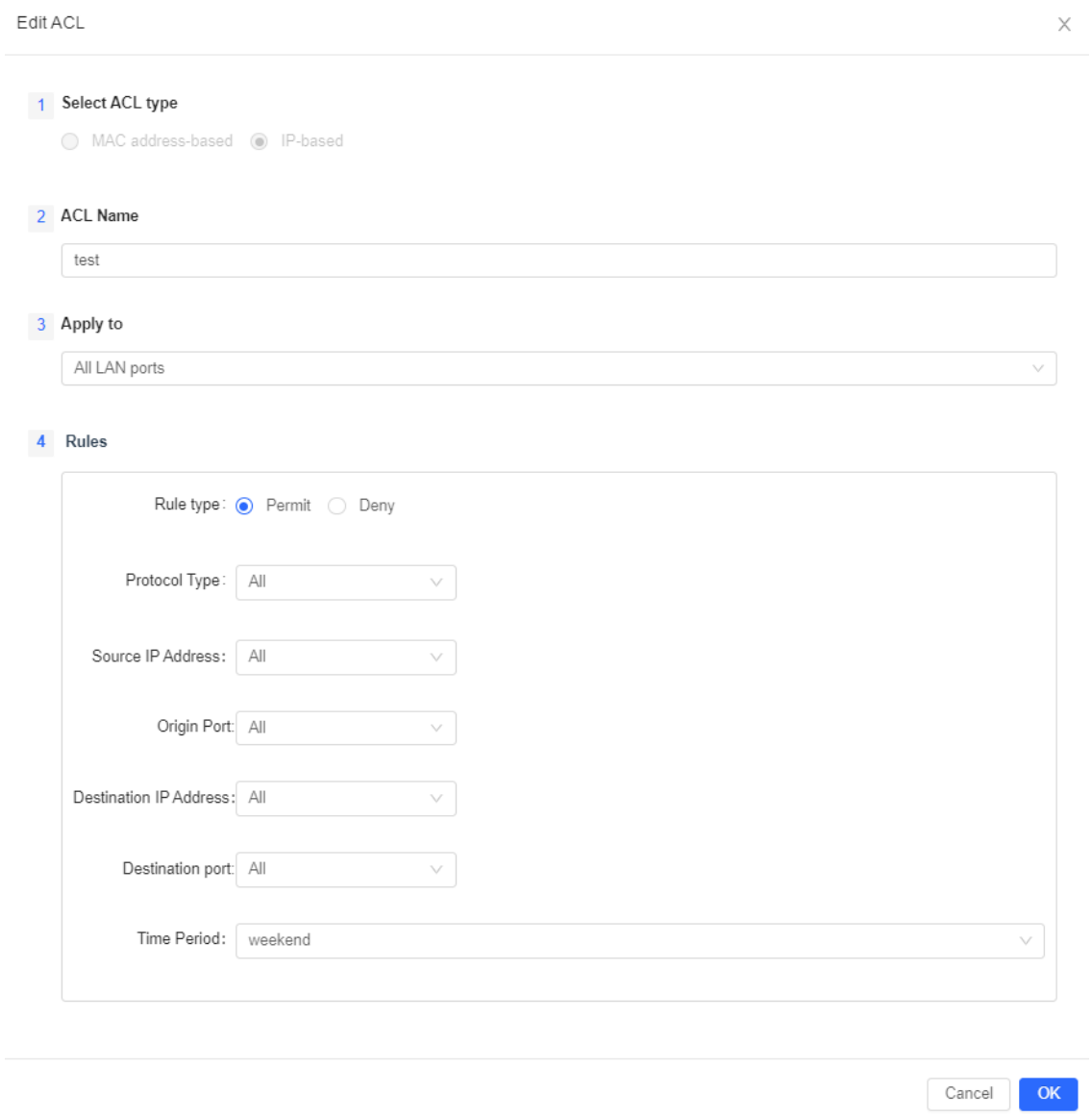
Choose Project > Configuration > Devices > General > ACL.

(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.





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 CLI Config Task

7.4.1 Add a CLI Command Set

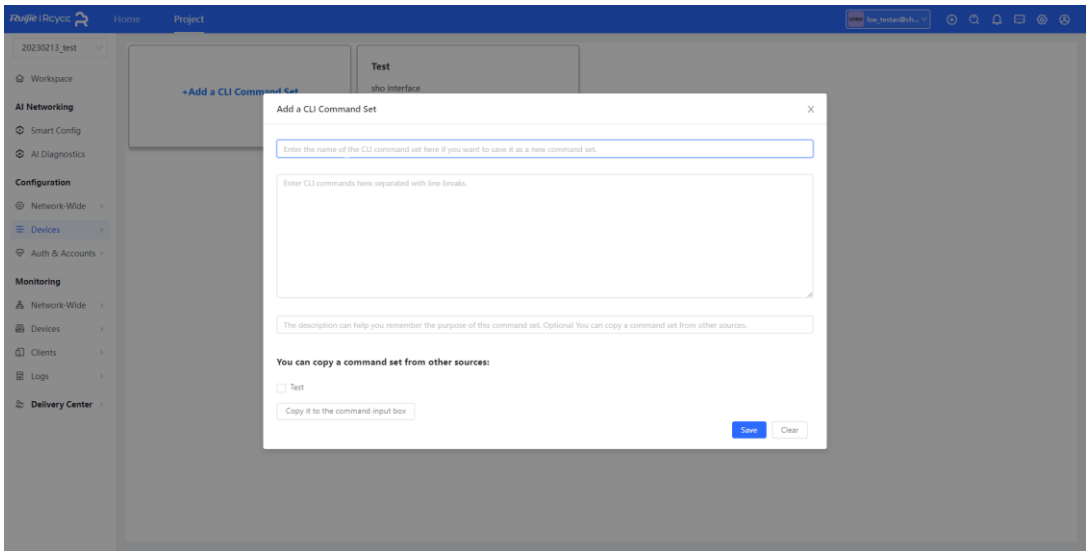
Limitations

The function is only supported on RGOS devices.

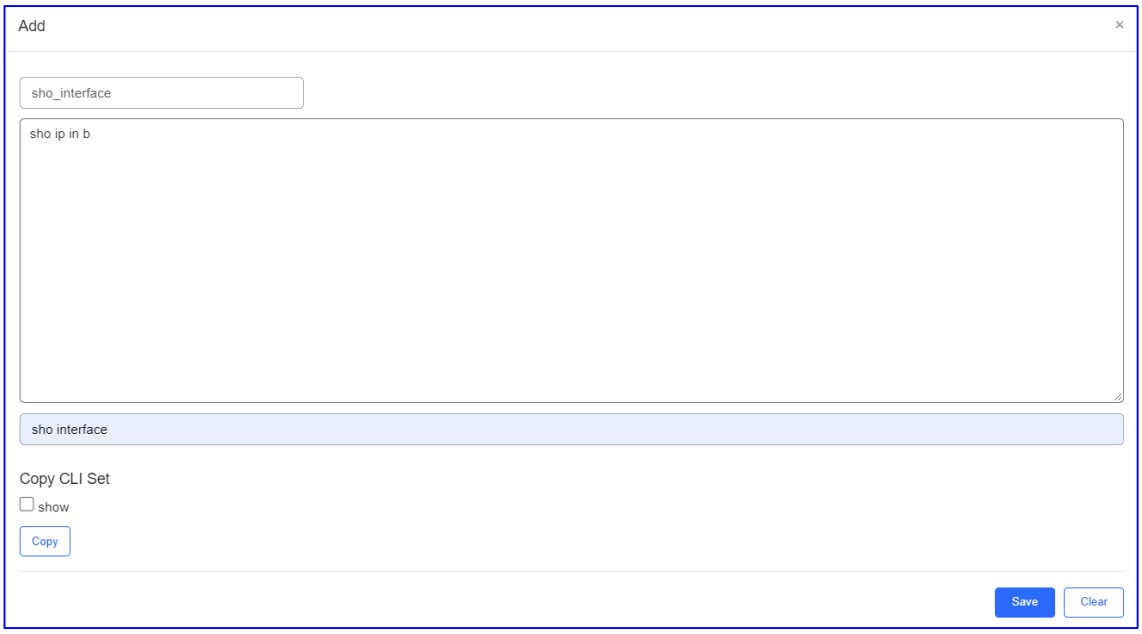
Procedure

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

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



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



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

7.4.2 Batch CLI Configuration

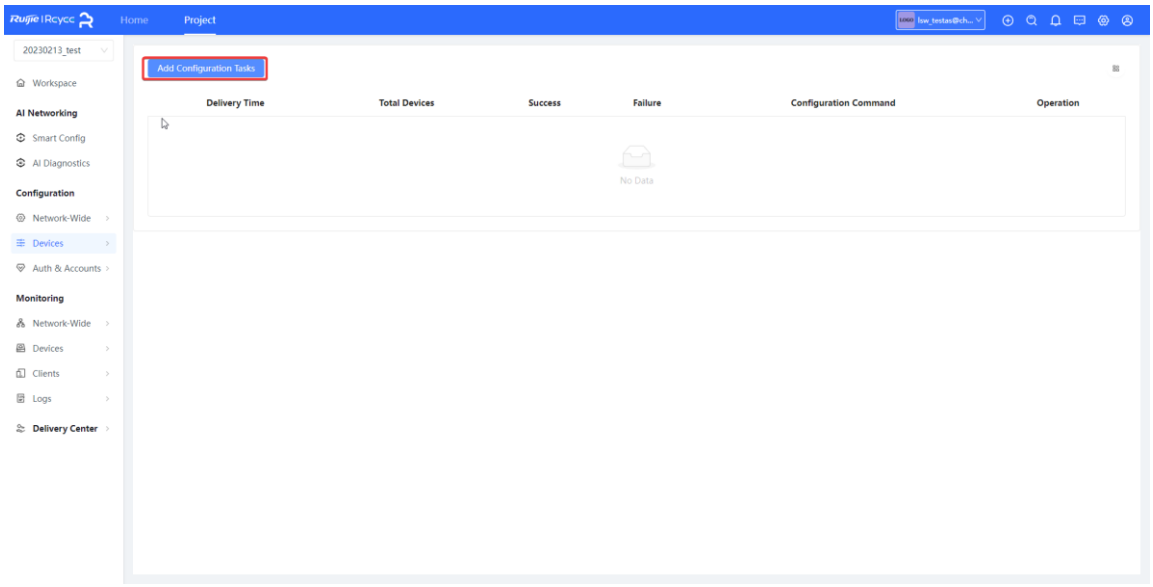
Limitations

The function is only supported on RGOS devices.

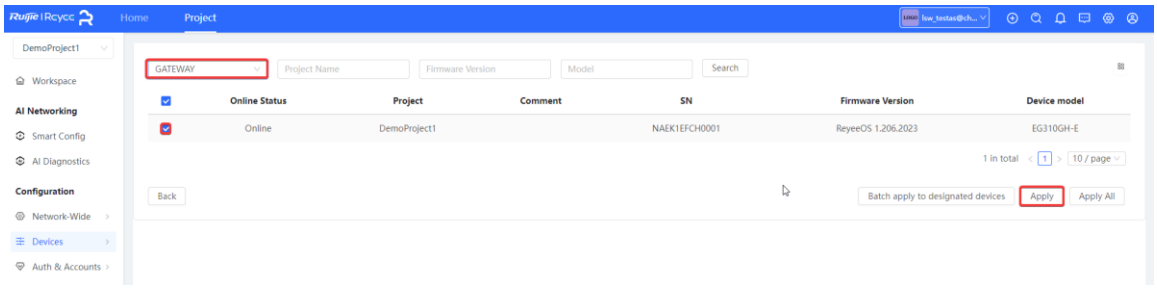
Procedure

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

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

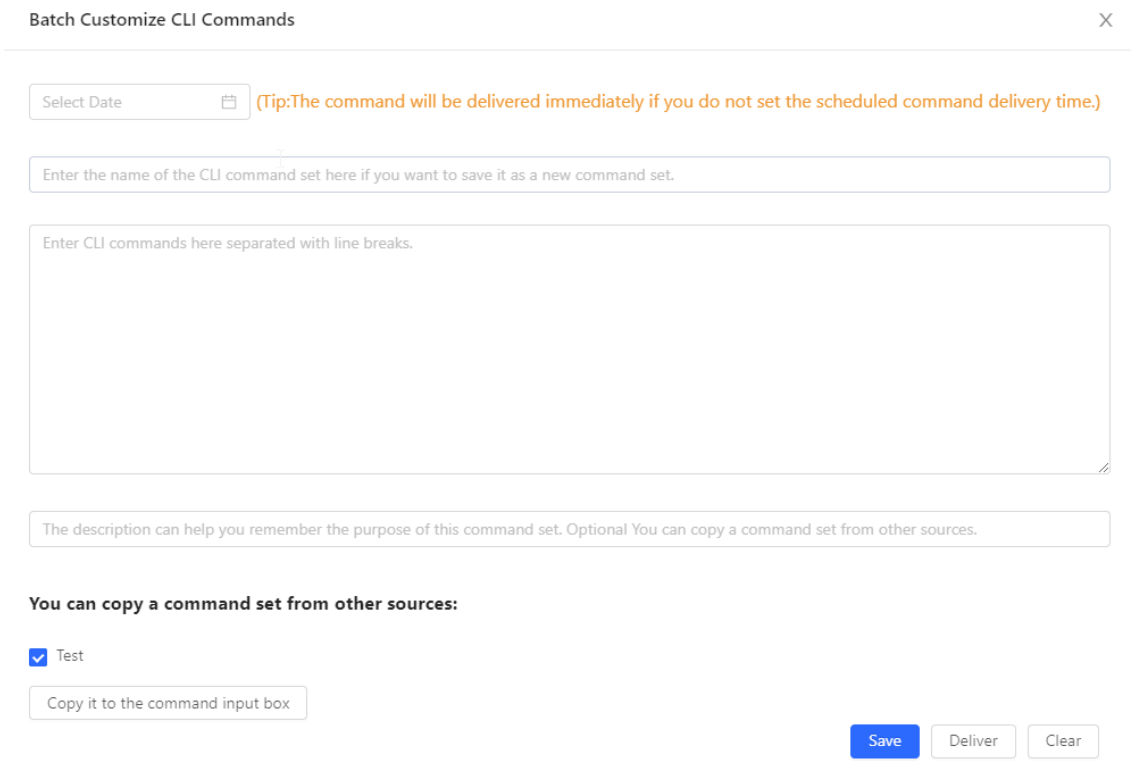


(3) Select one or more devices, and click **Apply**.

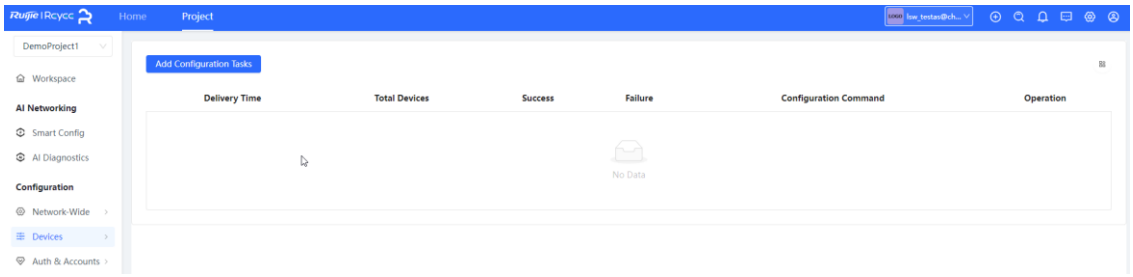


(4) Set parameters and click **Apply**.

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



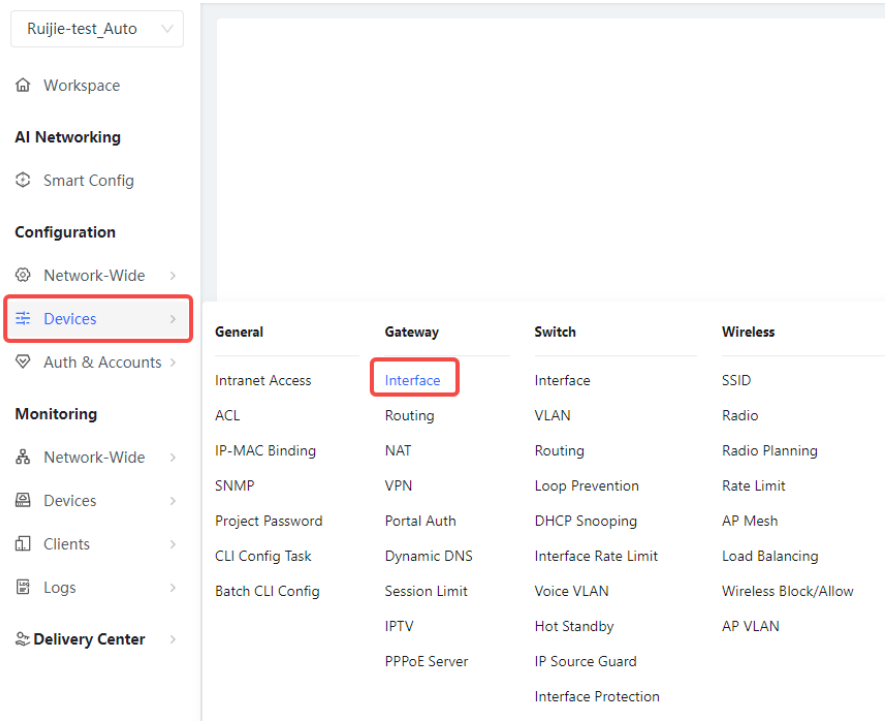
(5) Click **Back** to return to the **Batch CLI Config Status** page.



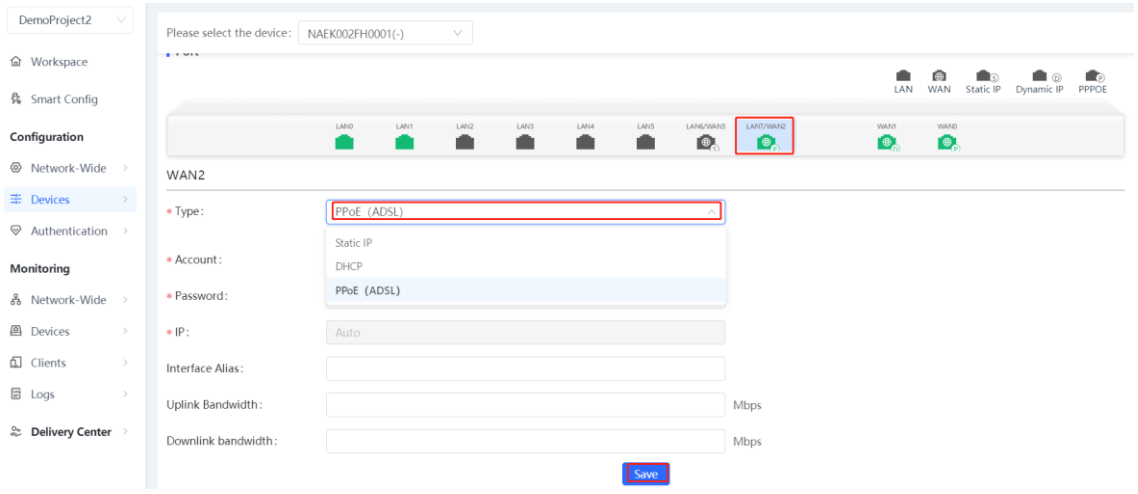
8 Gateway Configuration

8.1 Interface

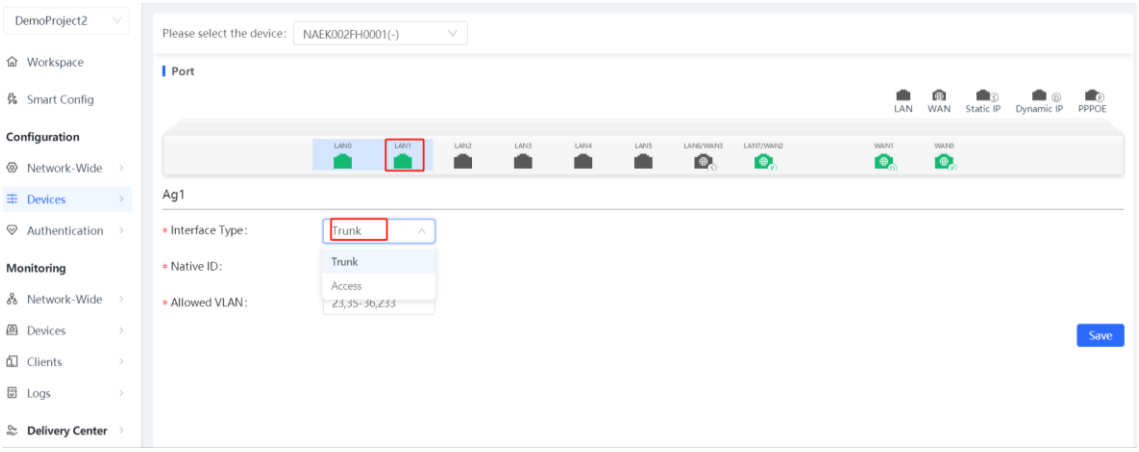
Choose **Project** > **Configuration** > **Devices** > **Gateway** > **Interface**. The gateway port page is displayed.



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**.



8.2 Routing

8.2.1 Adding a Static Route

1. Introduction

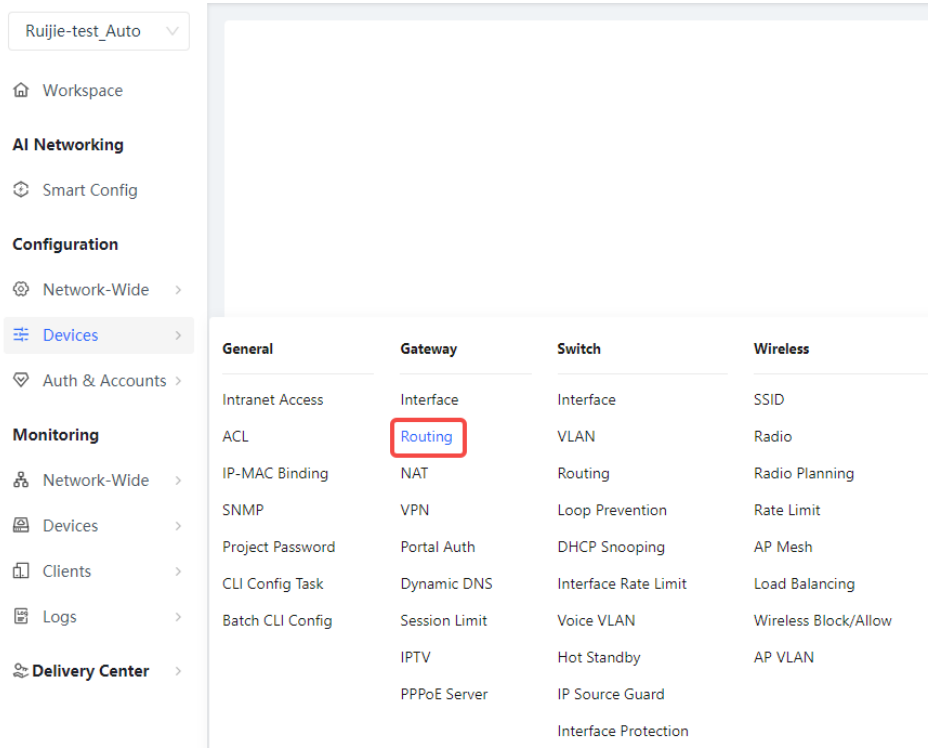
Static routes are manually configured. When a data packet matches a static route, the packet will be forwarded based on the specified forwarding mode.

Caution

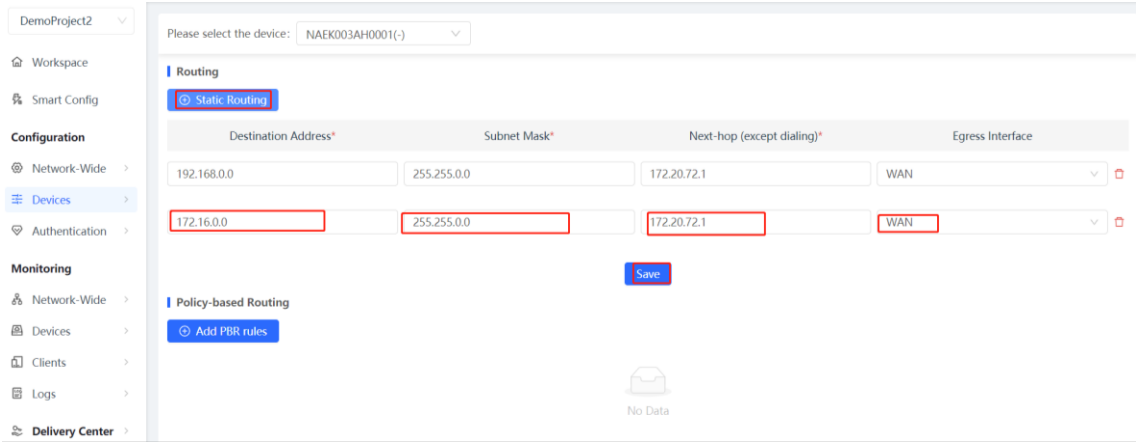
Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

2. Configuration Steps

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



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



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

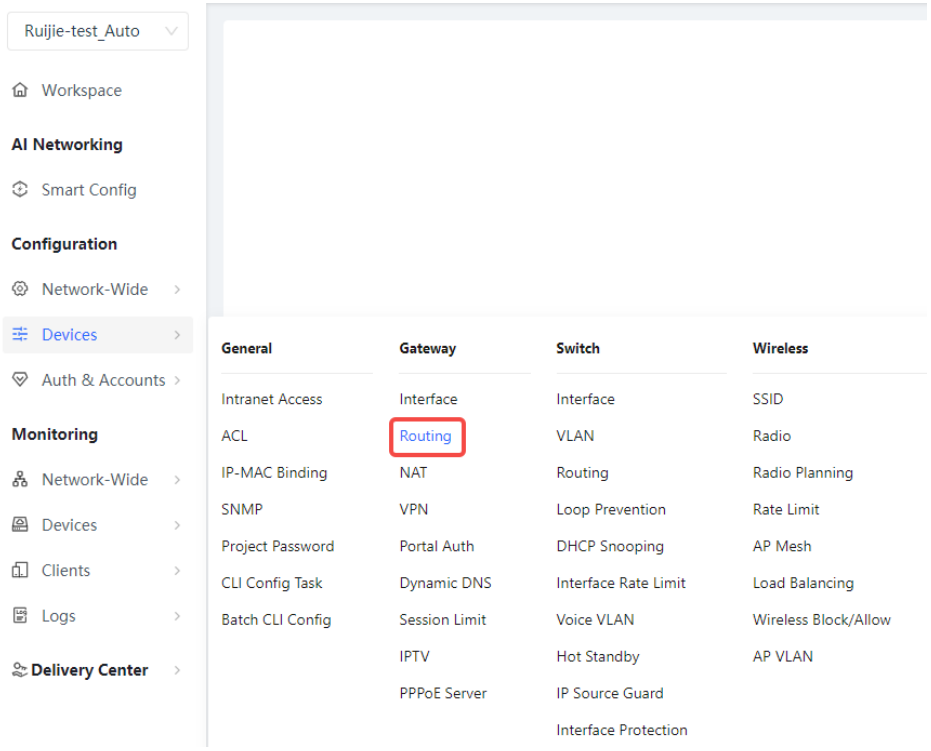
Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets based on configured rules, and then forwards the matched packets according to the specified forwarding policy. PBR enables the device to define 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.

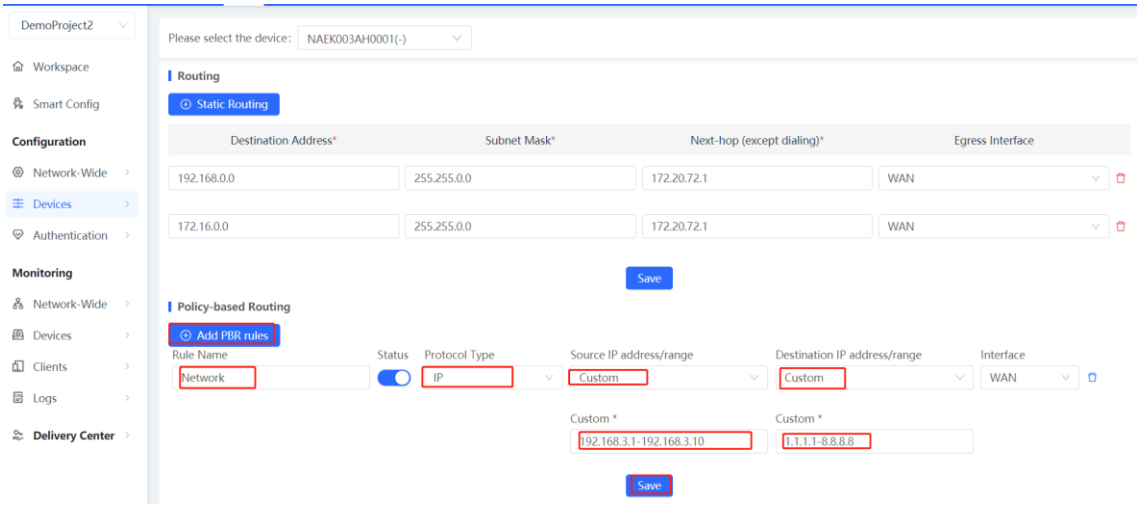
The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing are in descending order of priority.

2. Configuration Steps

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



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



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.

Parameter	Description
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 address/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 Source IP address/range	When **Source IP address/range** is set to **Custom**, you need to enter a single source IP address or a source IP address range.
Destination IP address/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 Destination address/range	When **Destination IP address/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

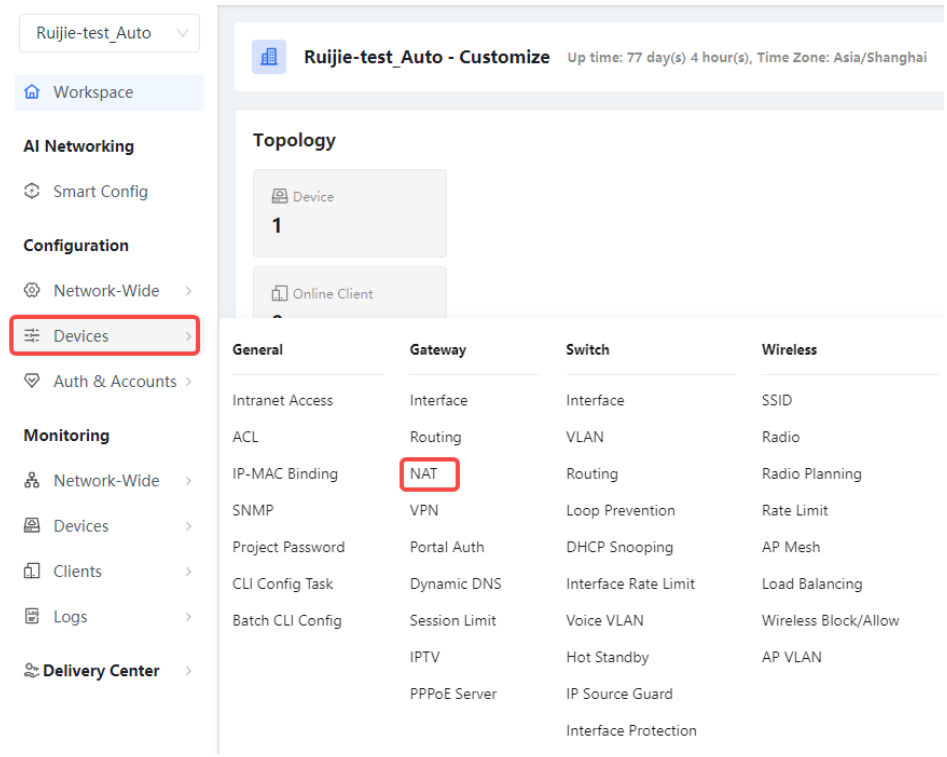
8.3.1 Applicable Scenarios

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.

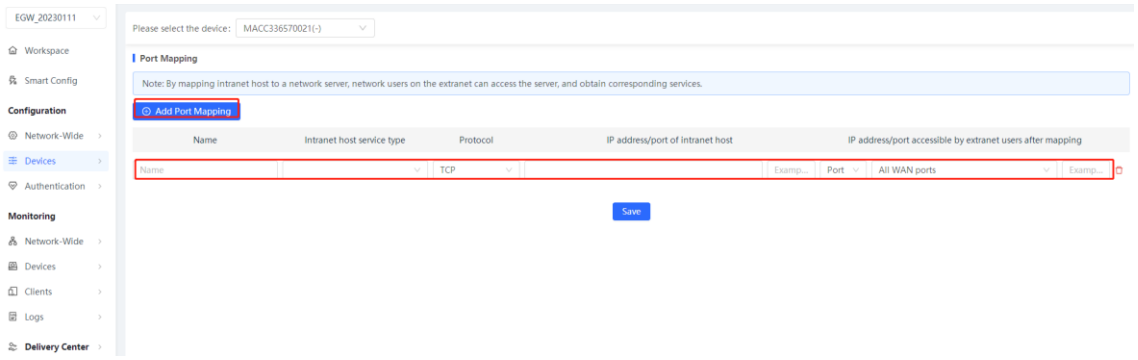
Port mapping enables users to access cameras or computers on their home network when they are in the enterprise or on a business trip.

8.3.2 Configuration Steps

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

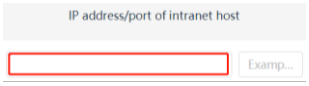
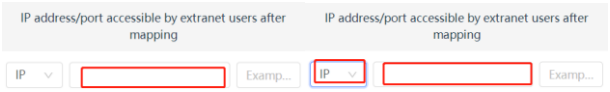


(2) Click ⊕ **Add Port Mapping**, set parameters, and then click **Save**.



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.

Parameter	Description
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. 
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. 

(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

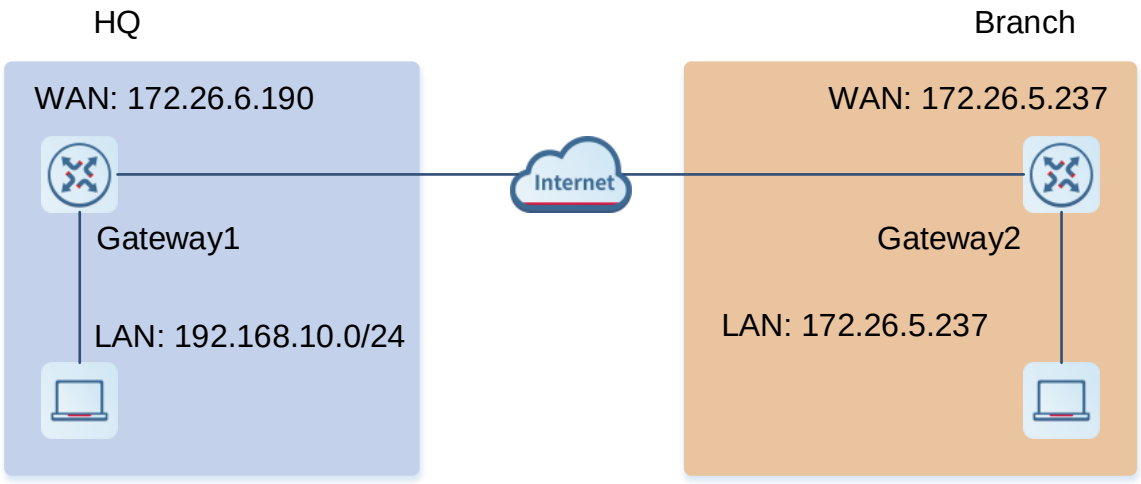
Virtual private network (VPN) is used to build a virtual private network on the public network, and transmit private network traffic on this virtual network.

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.

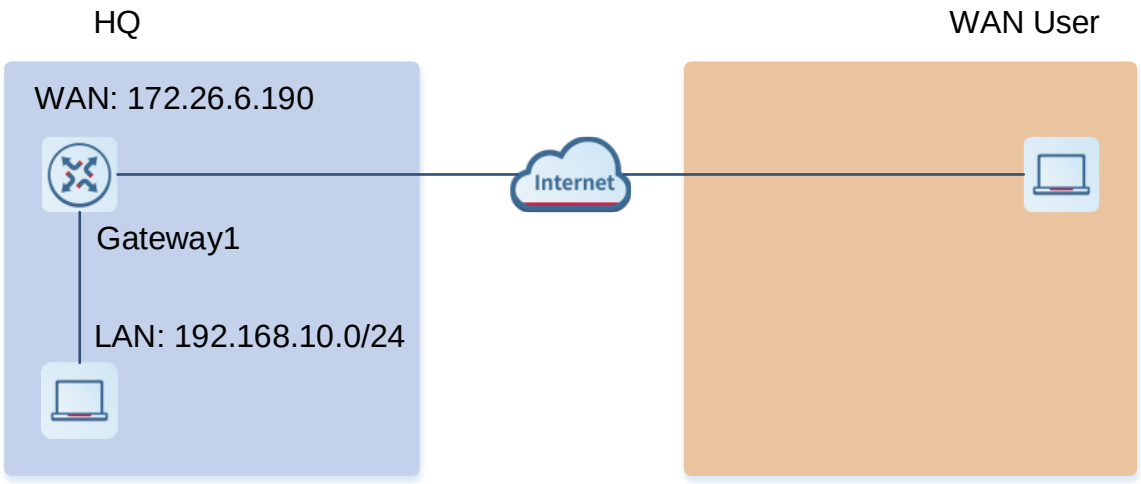
  Site-to-site VPN can be implemented in the following ways: PPTP, L2TP, IPSec, and L2TP over IPsec. Ruijie Cloud supports only the IPsec VPN mode.

- 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



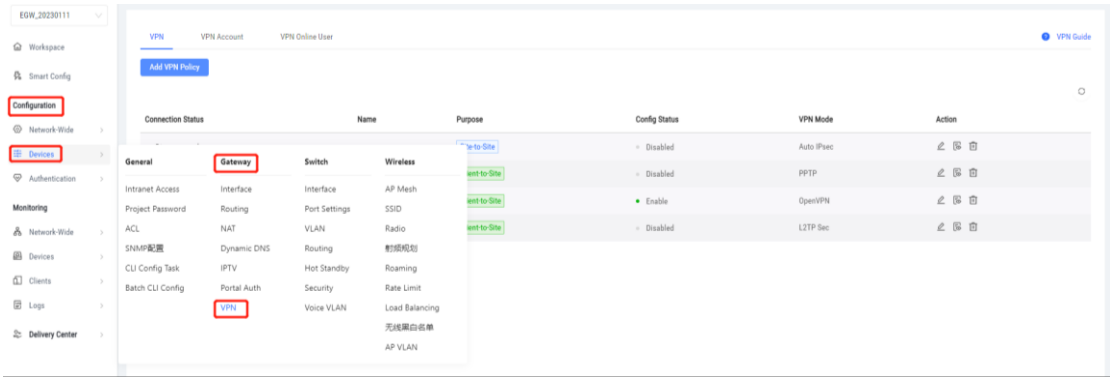
Client-to-site VPN can be implemented in the following ways: PPTP, L2TP, L2TP over VPN, and open VPN.

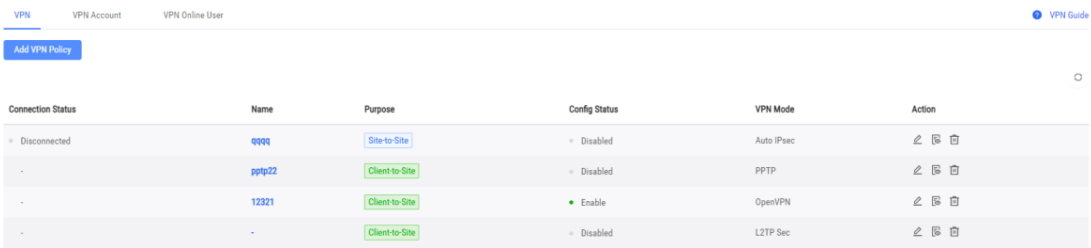
2. Configuring Site-to-Site VPN (Based on IPsec VPN)

(1) Configure VPN for the HQ gateway.

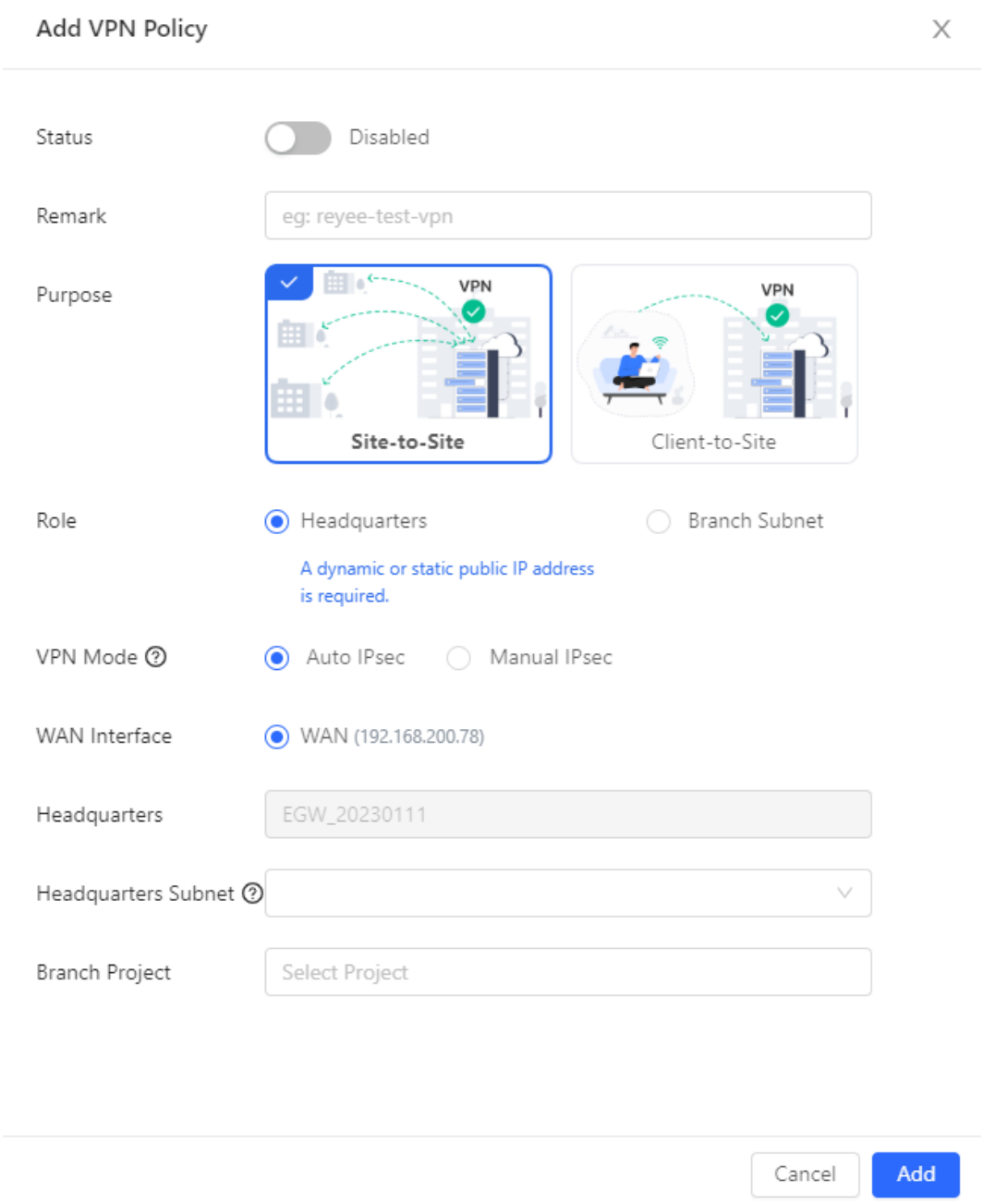
a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.

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





c Click **Add VPN Policy**.



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**.

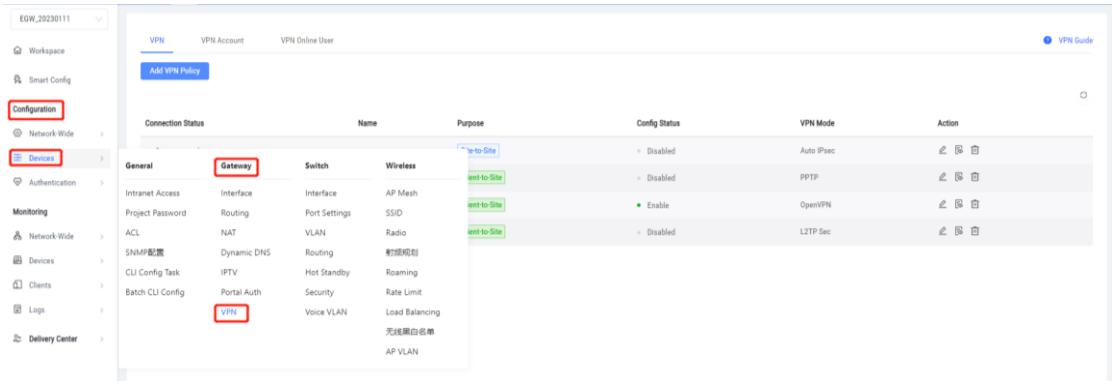
e Click **Add**.

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

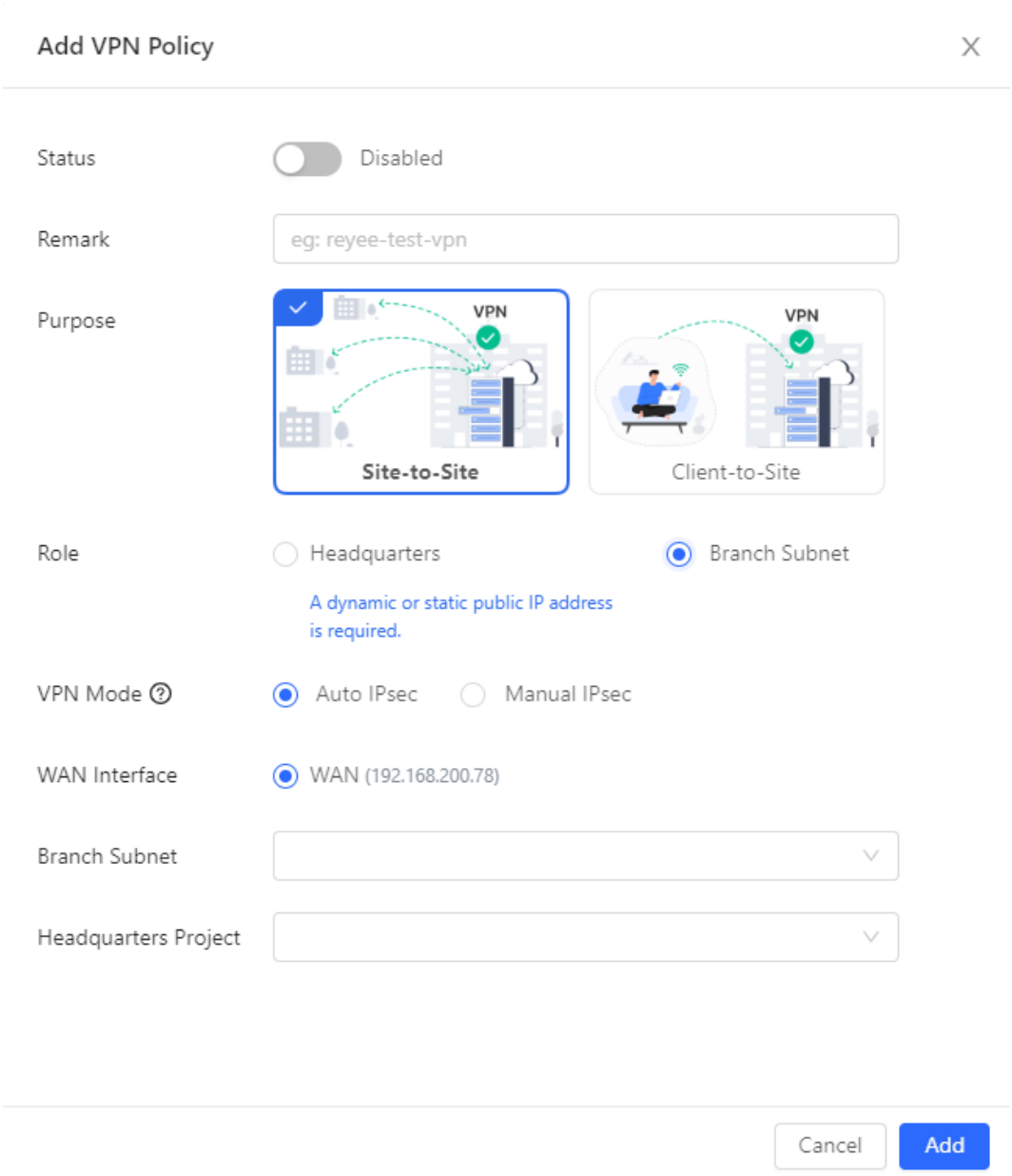
When VPN is configured for the HQ gateway, if **VPN Mode** is set to **Manual IPSec**, perform the following operations. If **VPN Mode** is not set to **Auto IPsec**, the following operations are not required.

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

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



c Click **Add VPN Policy**.



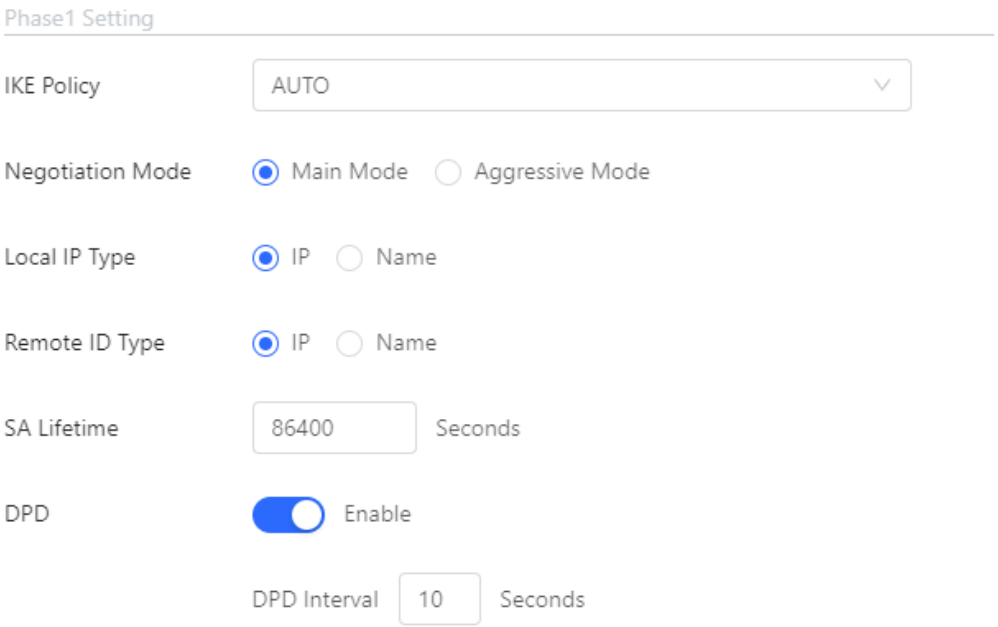
d Set configuration items related to the branch VPN.

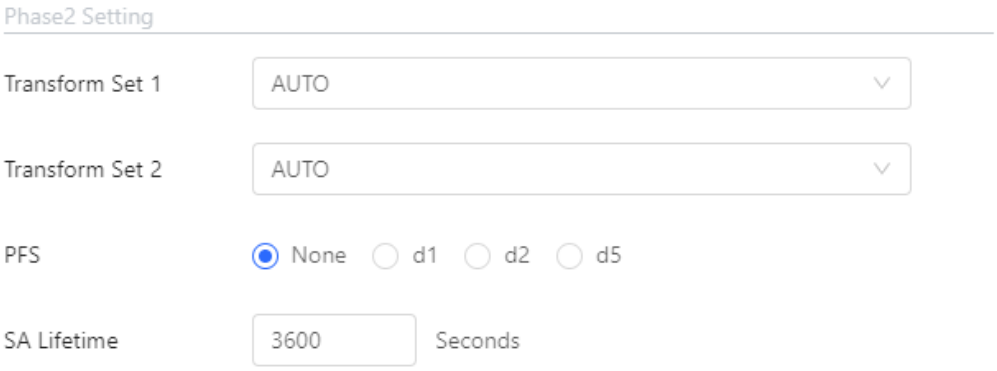
Table 8-2 Configuration Items Related to the Branch VPN

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**.

Parameter	Description
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.





f Click **Add**.

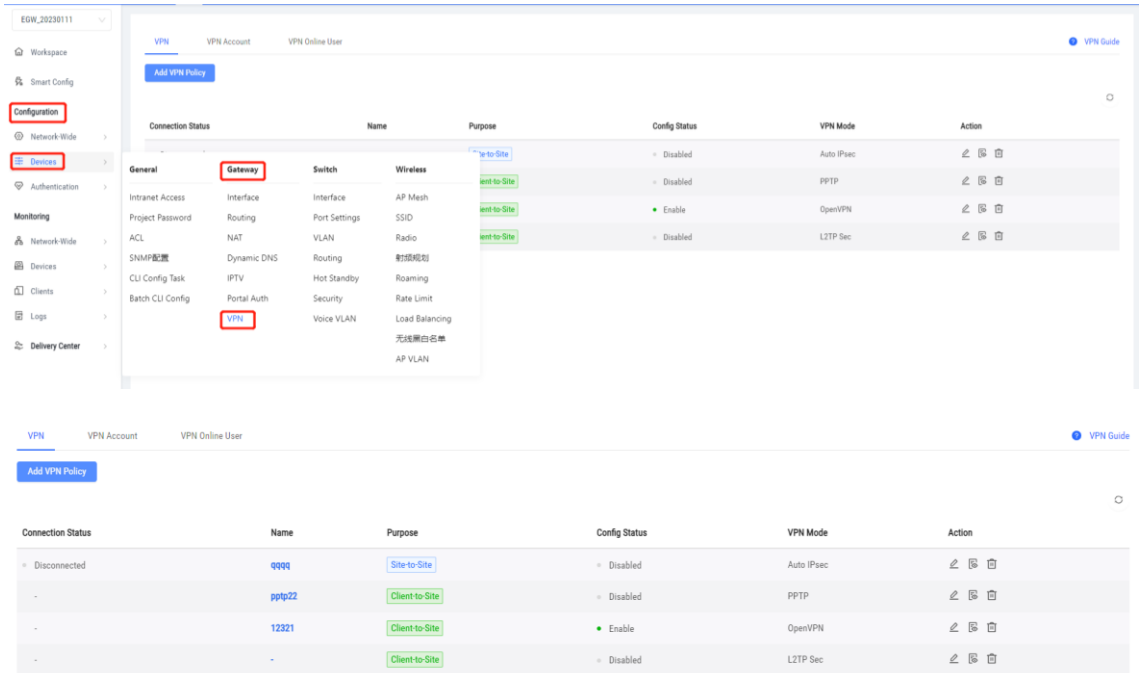
3. Configuring Client-to-Site VPN (Based on PPTP VPN)

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.

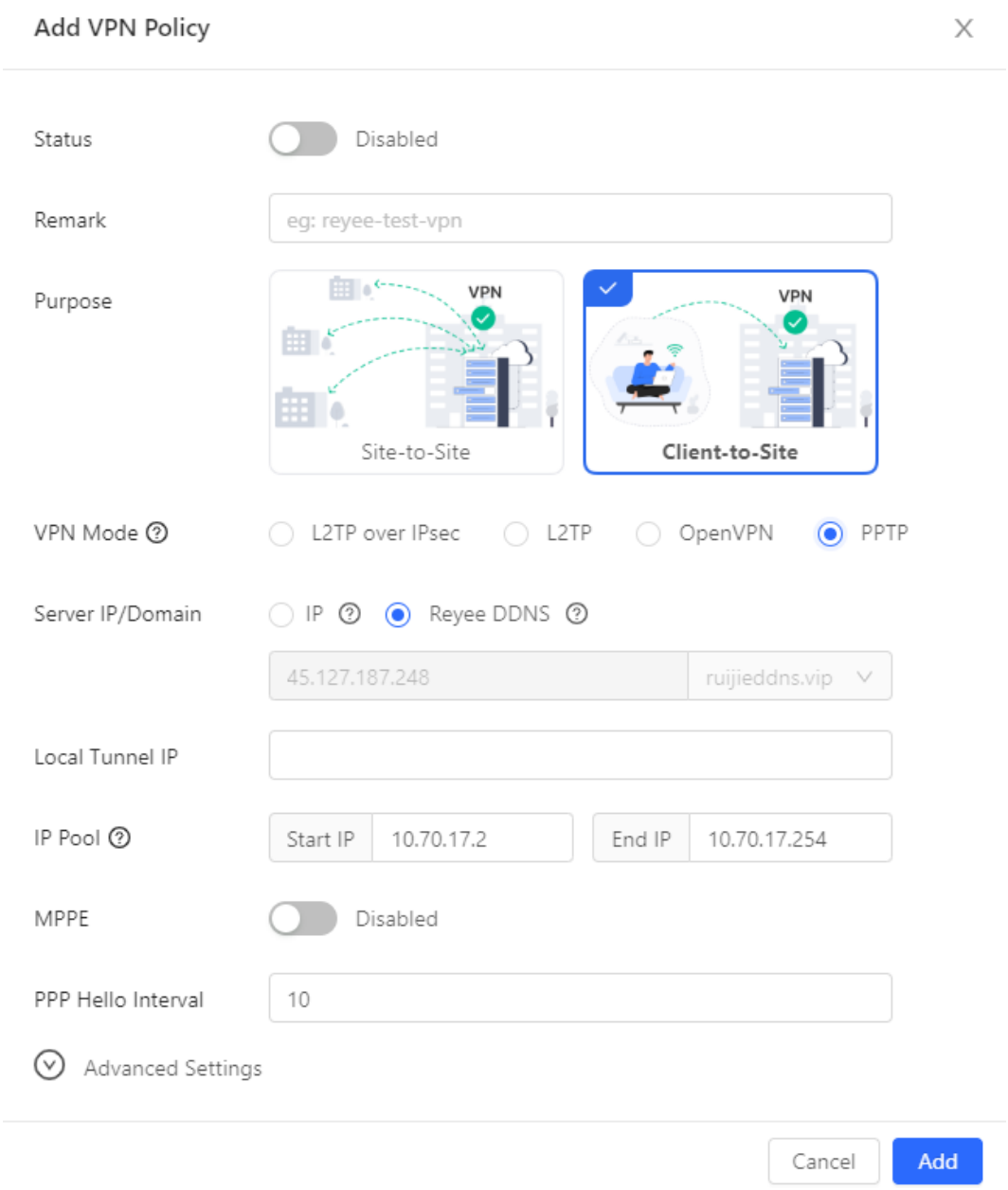
(1) Configure VPN for the HQ gateway.

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**.



c Click **Add VPN Policy**.



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**.

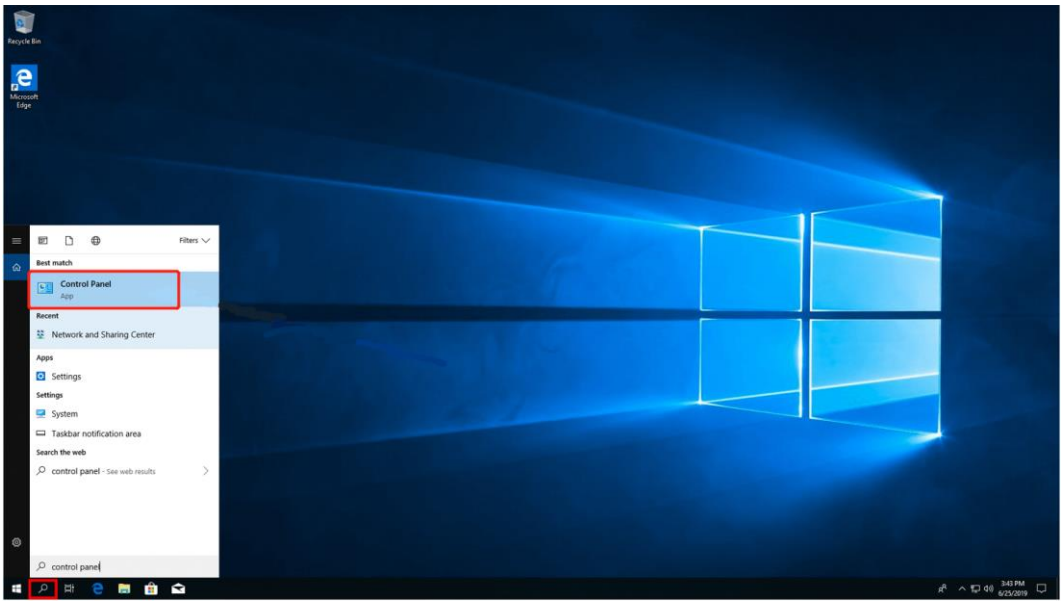
Parameter	Description
Server IP/Domain	Specify the IP address or domain name of the PPTP server.
Local Tunnel IP	Specify the local virtual IP address of the server of the VPN tunnel. After the client dials into the VPN, the client can access the server through this IP address.
IP Pool	Specify the address 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.

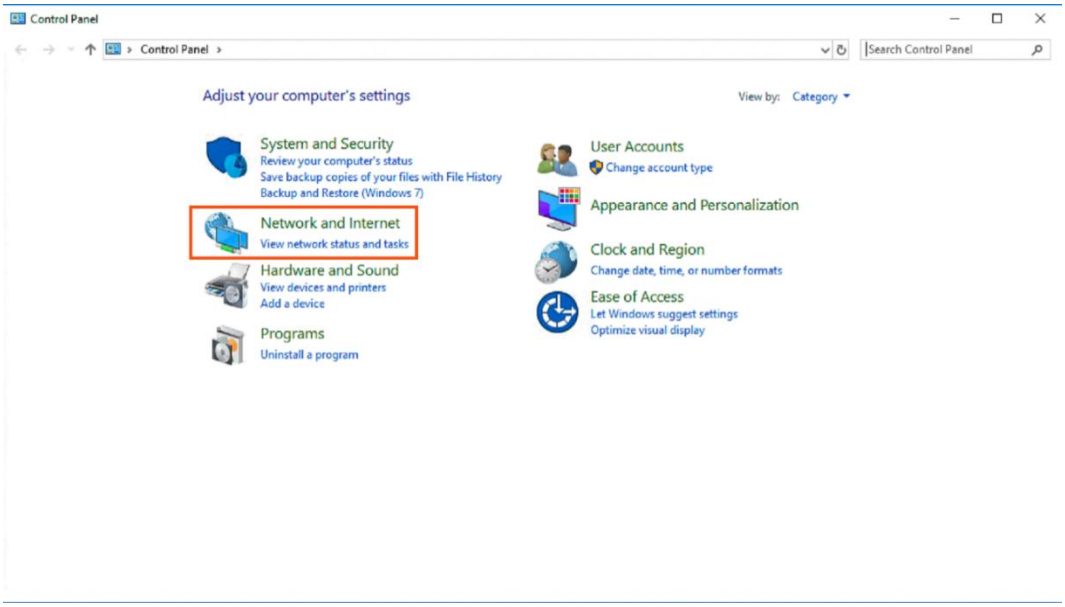
e Click **Add**.

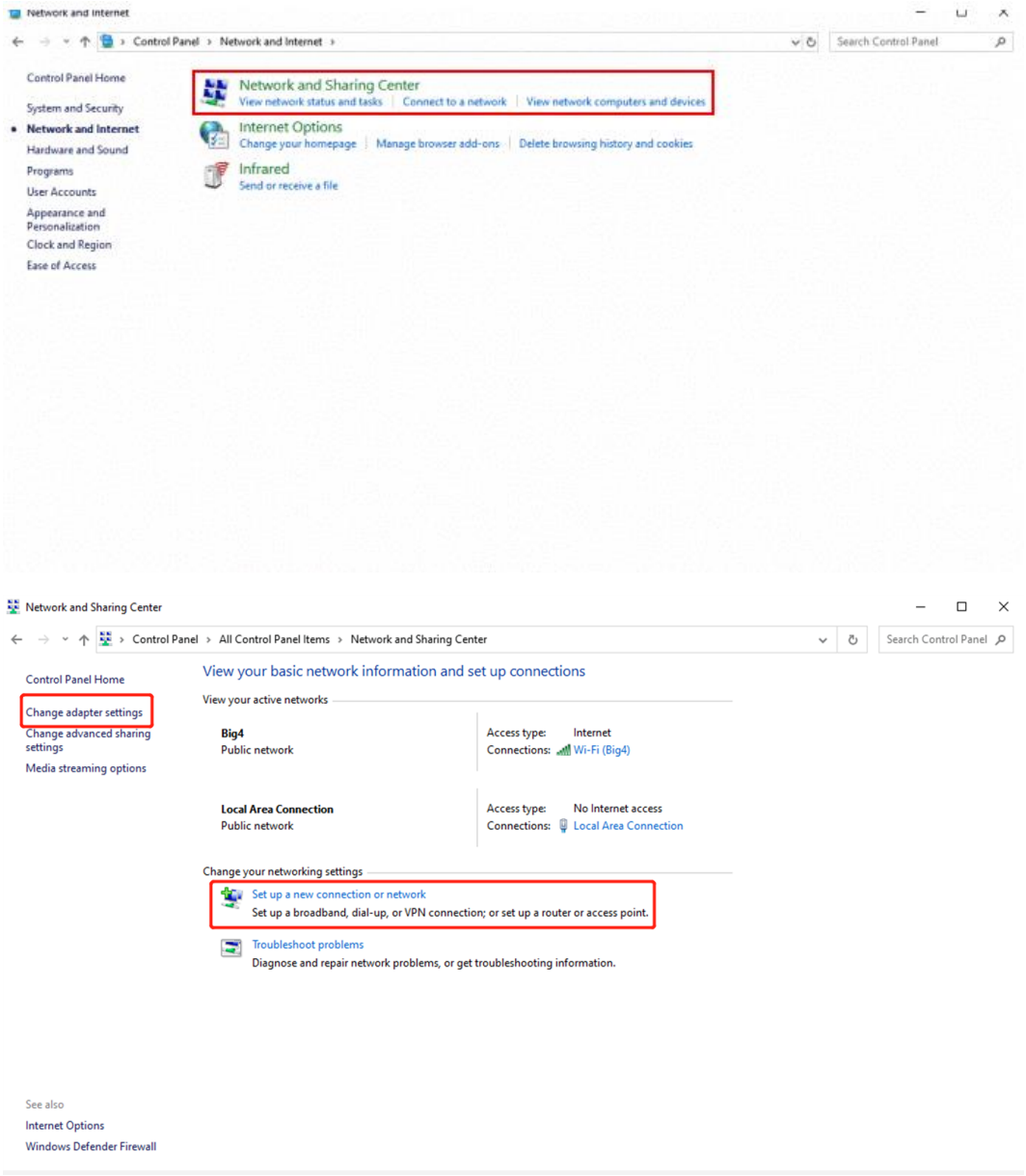
(2) Configure the client.

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.

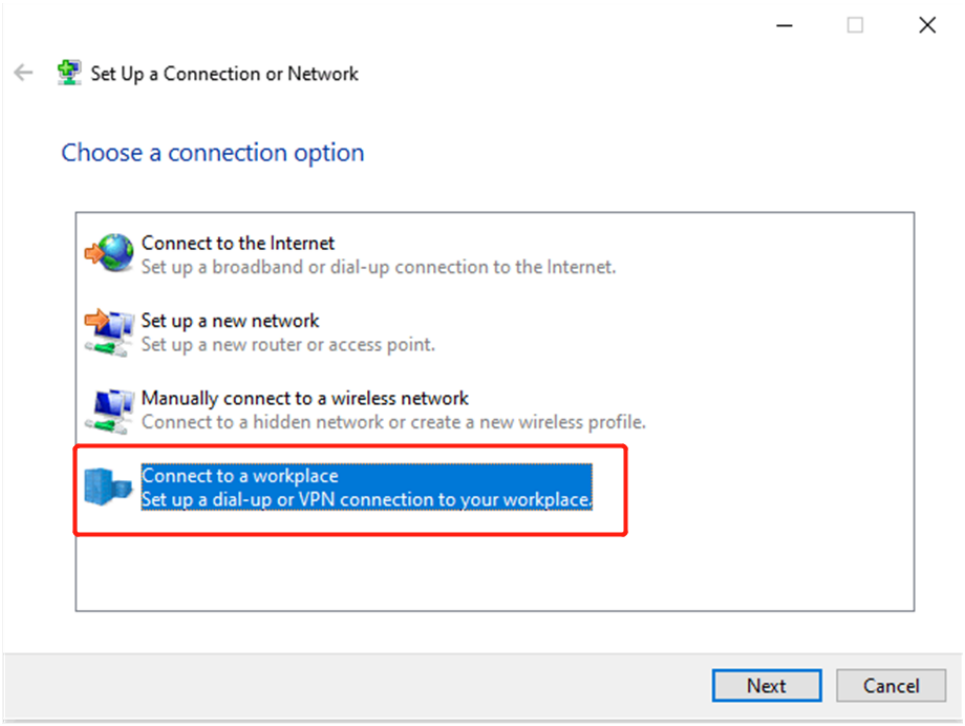
a Log in to the Windows client and choose **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

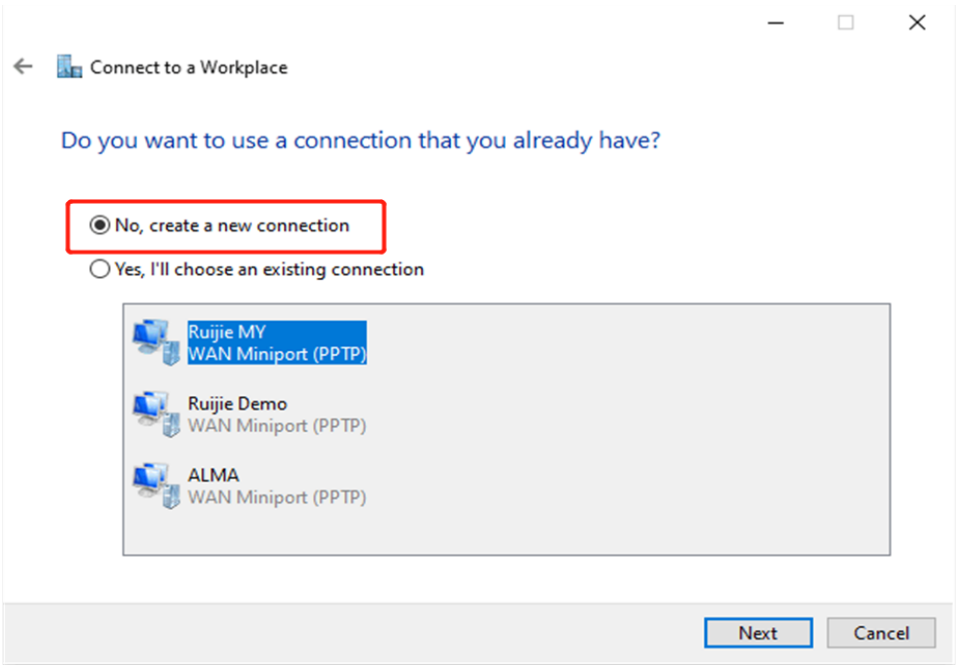

Recycle Bin
Microsoft Edge
Filters
Best match
Control Panel
App
Recent
Network and Sharing Center
Apps
Settings
Settings
System
Taskbar notification area
Search the web
control panel - See web results
control panel

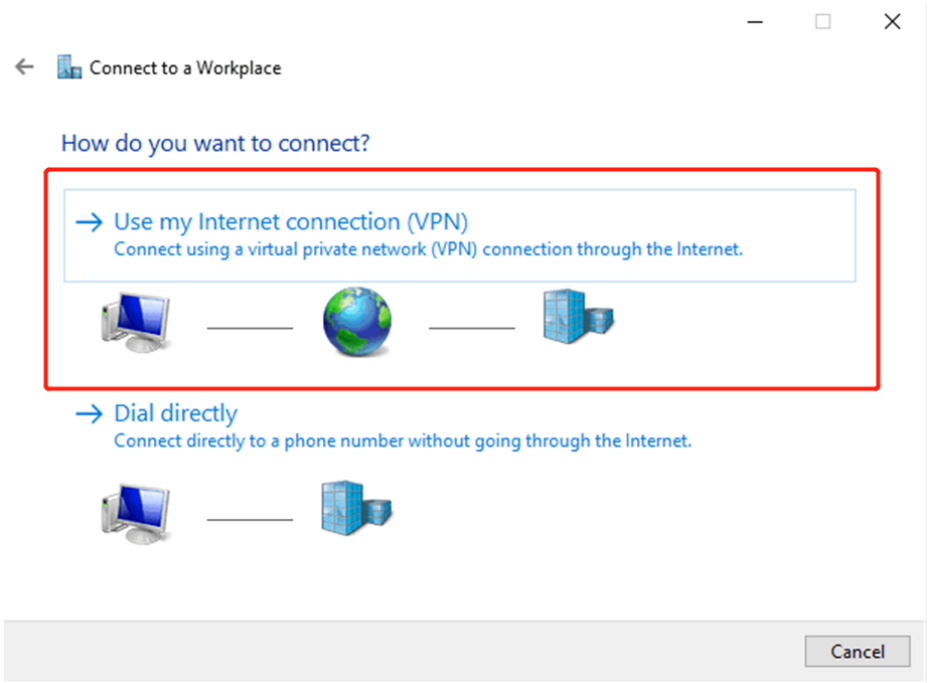

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
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

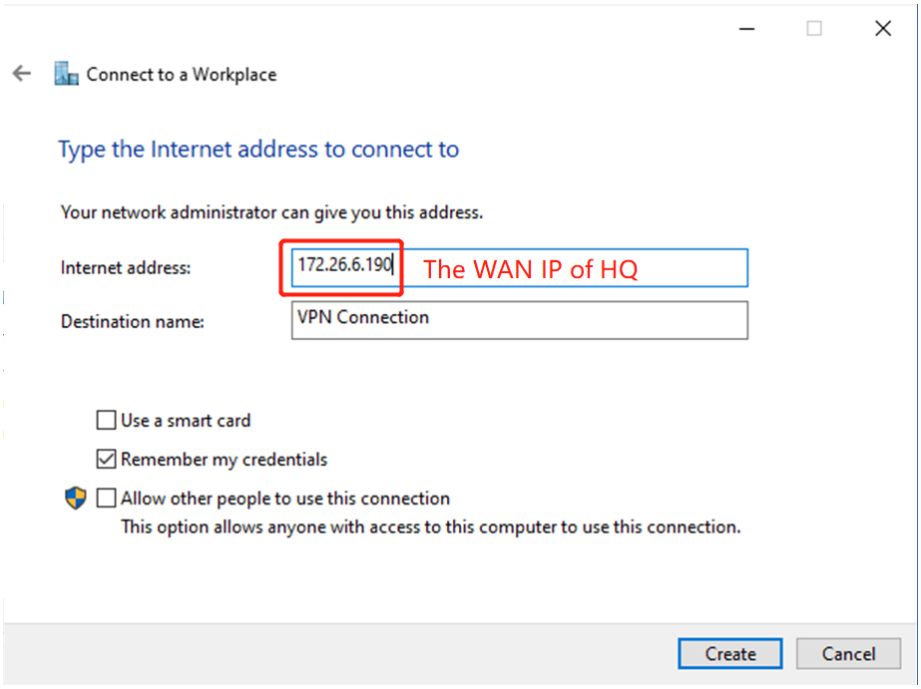


b Configure a VPN connection.

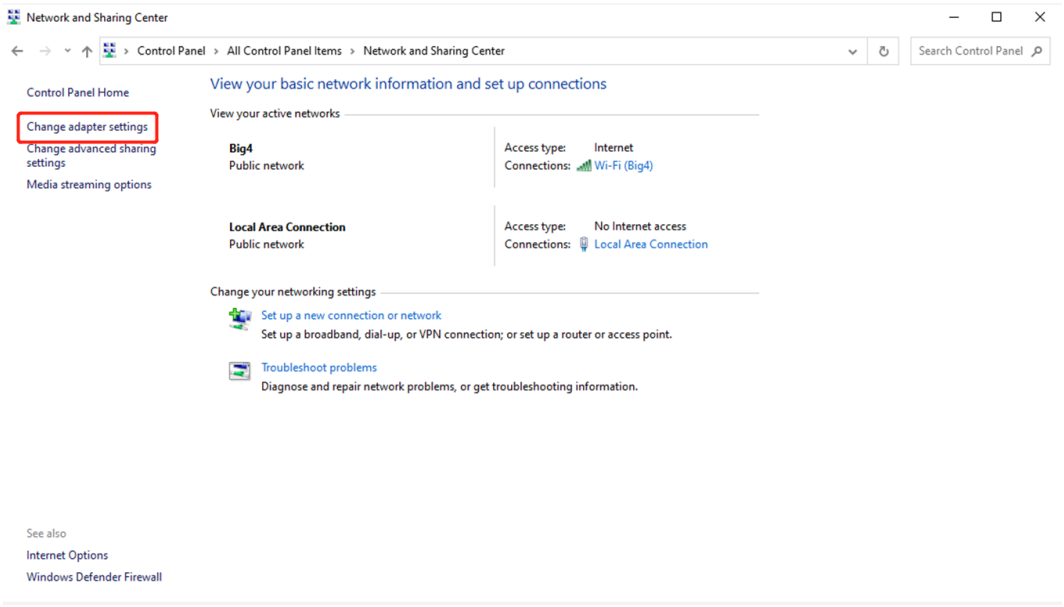

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel

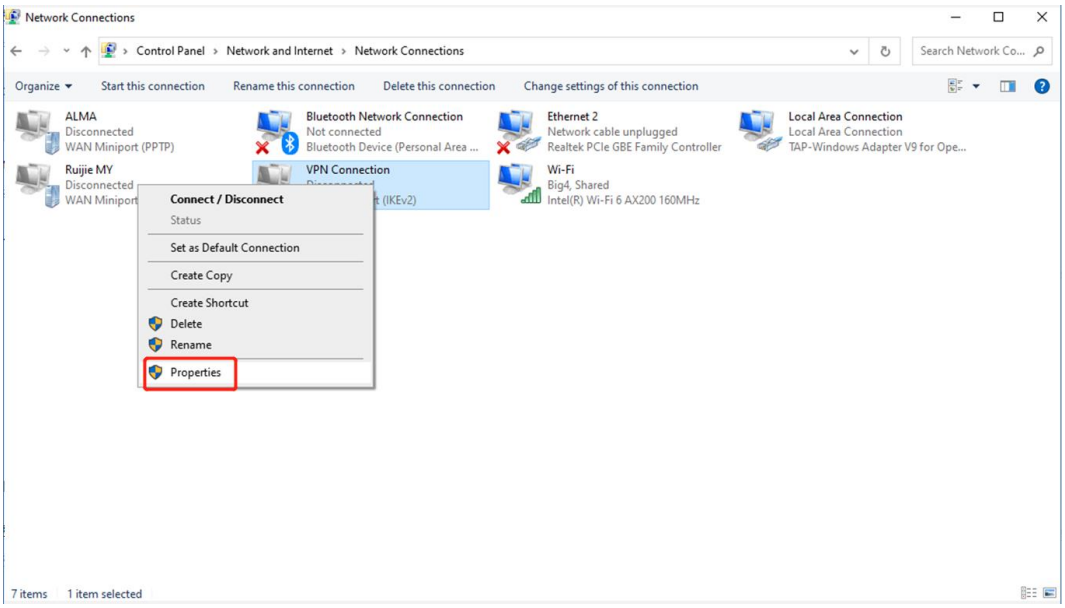

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

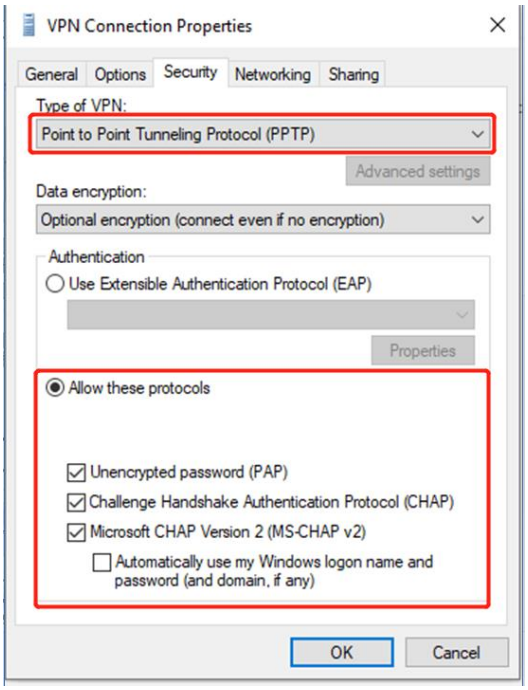




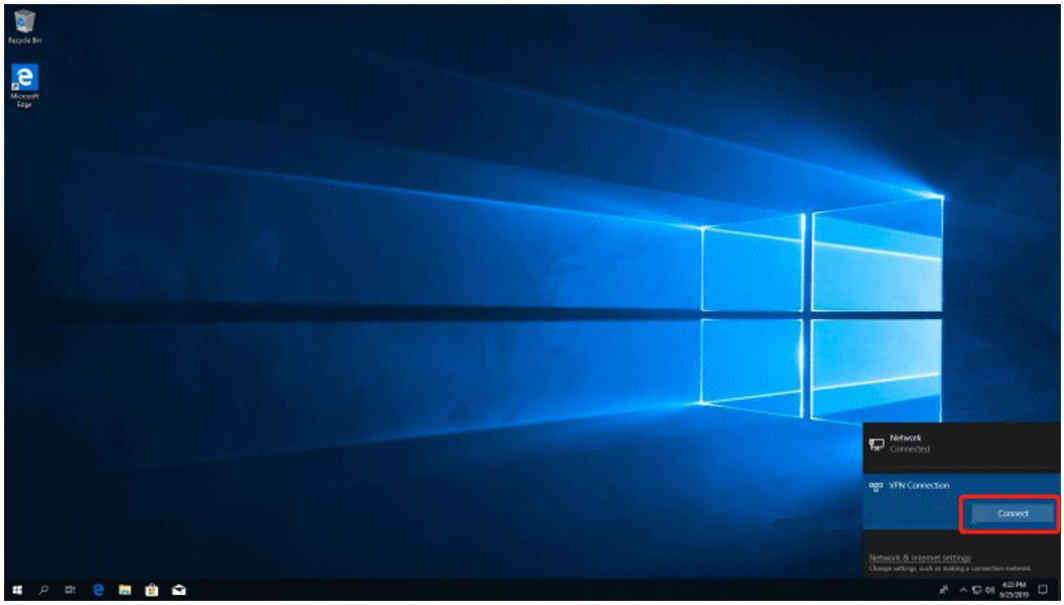
c Change settings of the adapter.

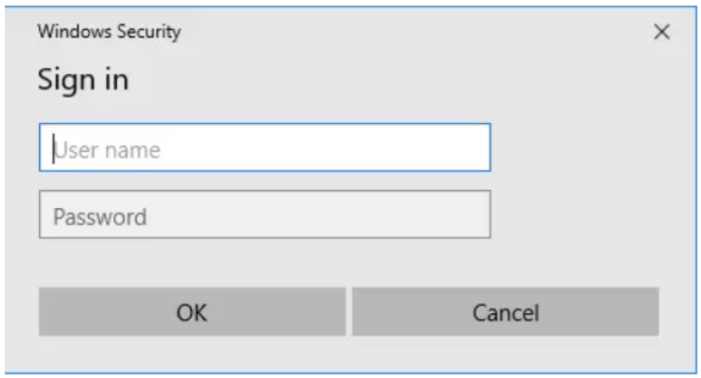

Network and Sharing Center
Control Panel › All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
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

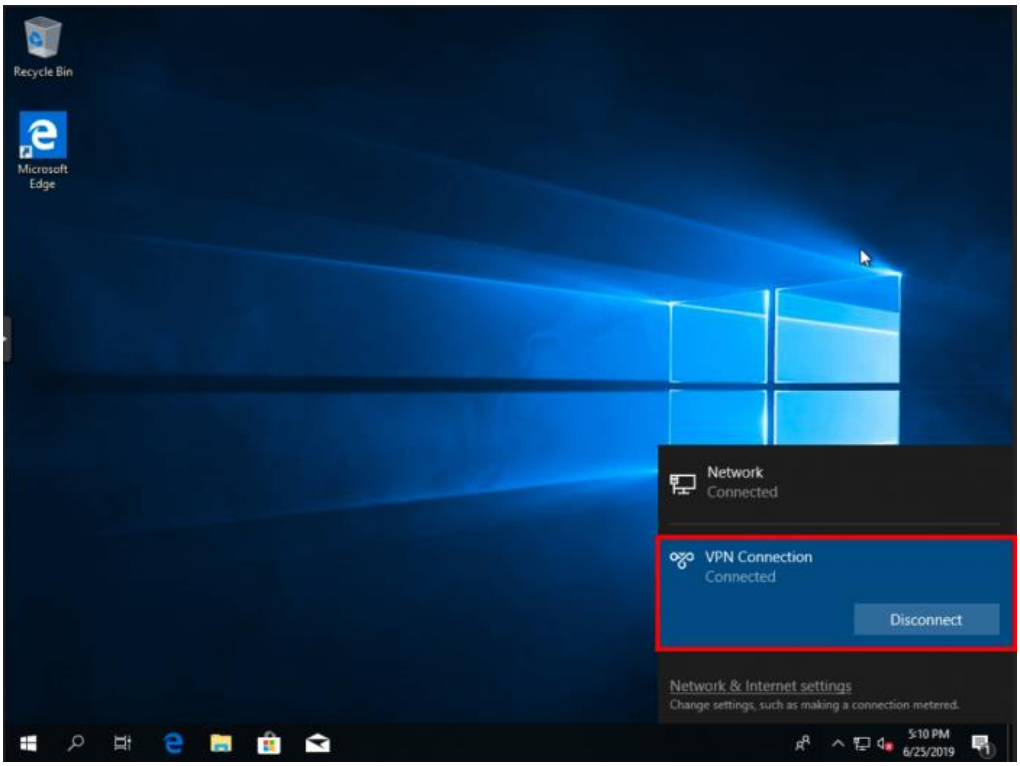

Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Co...
Organize
Start this connection
Rename this connection
Delete this connection
Change settings of this connection
ALMA
Disconnected
WAN Miniport (PPTP)
Bluetooth Network Connection
Not connected
Bluetooth 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
VPN Connection
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



d Check the VPN connection status.







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
```

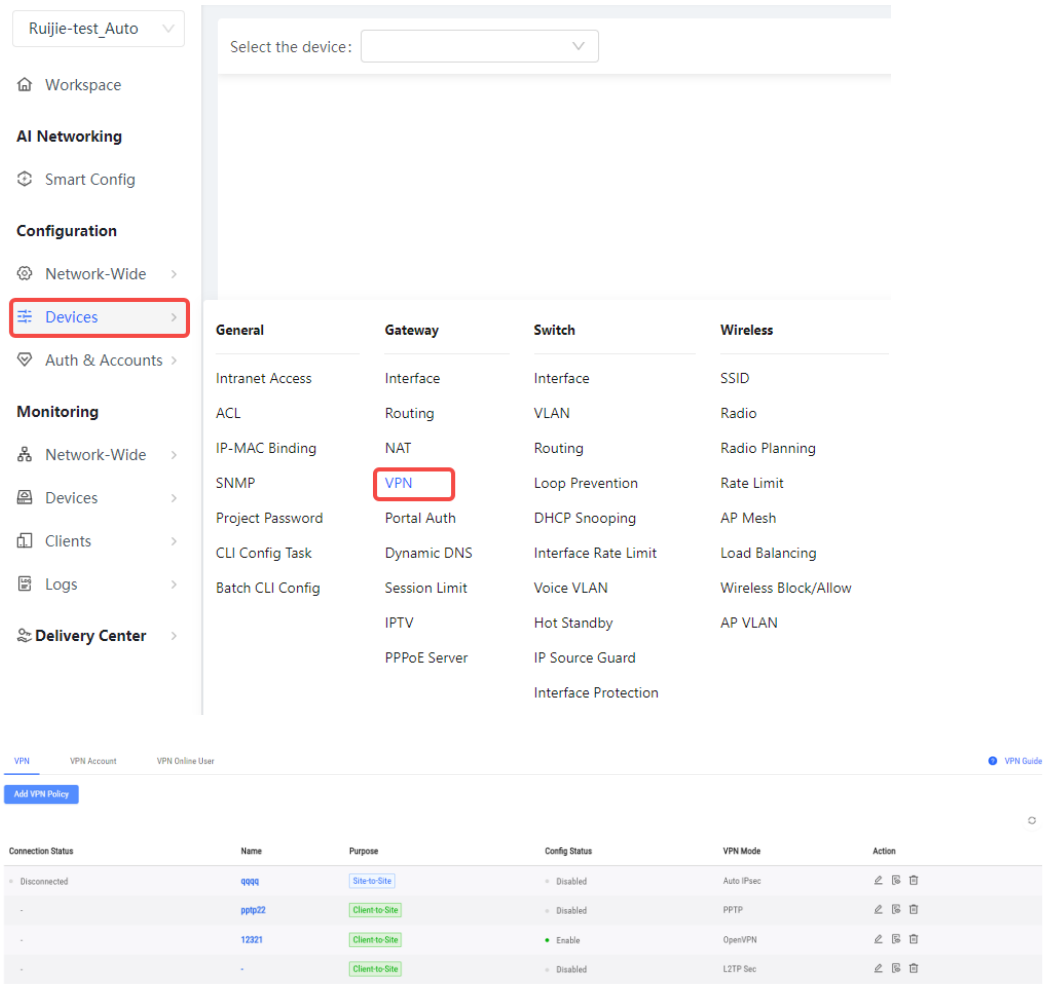
4. Configuring Client-to-Site VPN (Based on L2TP VPN)

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.

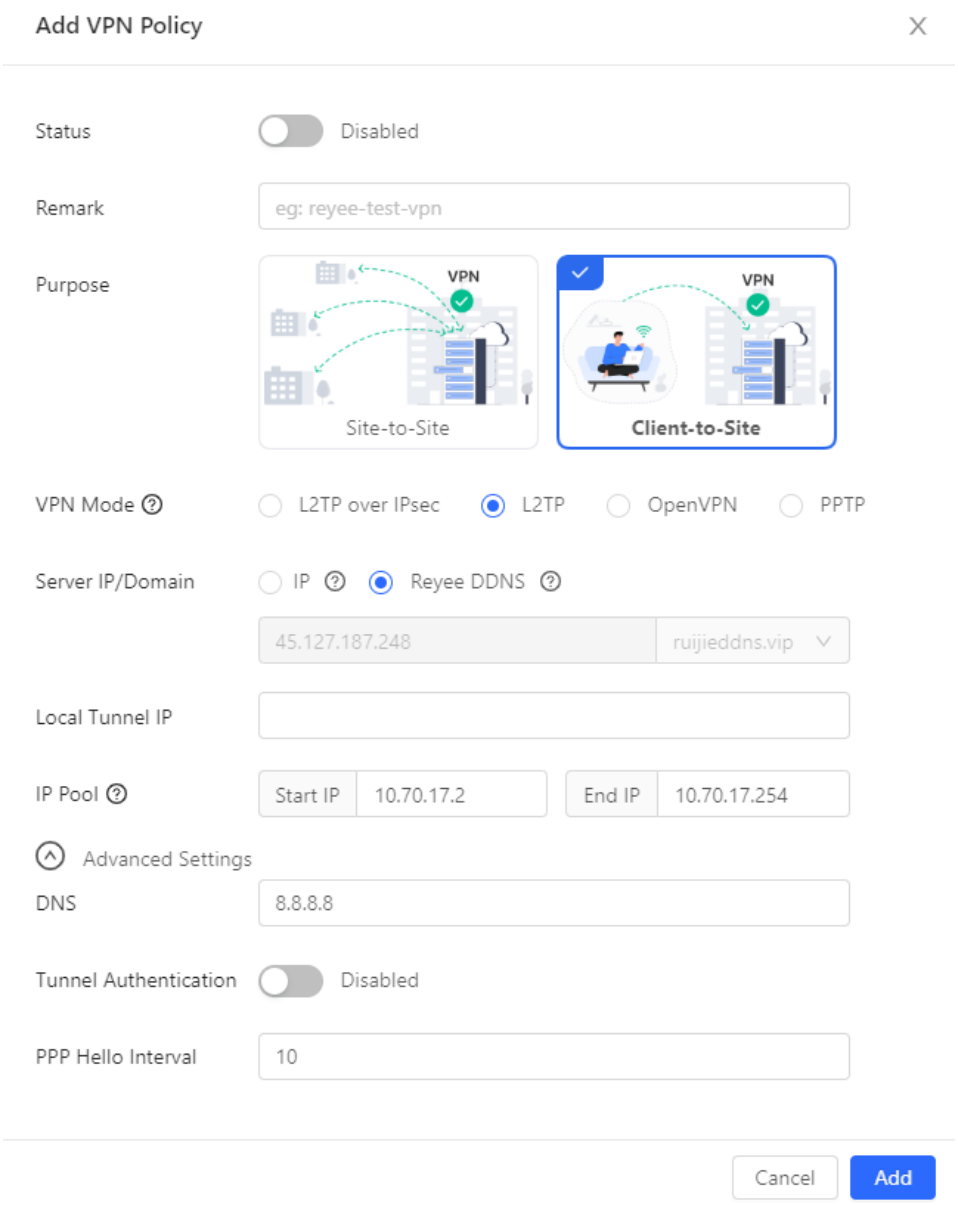
(1) Configure VPN for the HQ gateway.

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 **Project > Configuration** > **Devices** > **Gateway** > **VPN**.



c Click **Add VPN Policy**.



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.

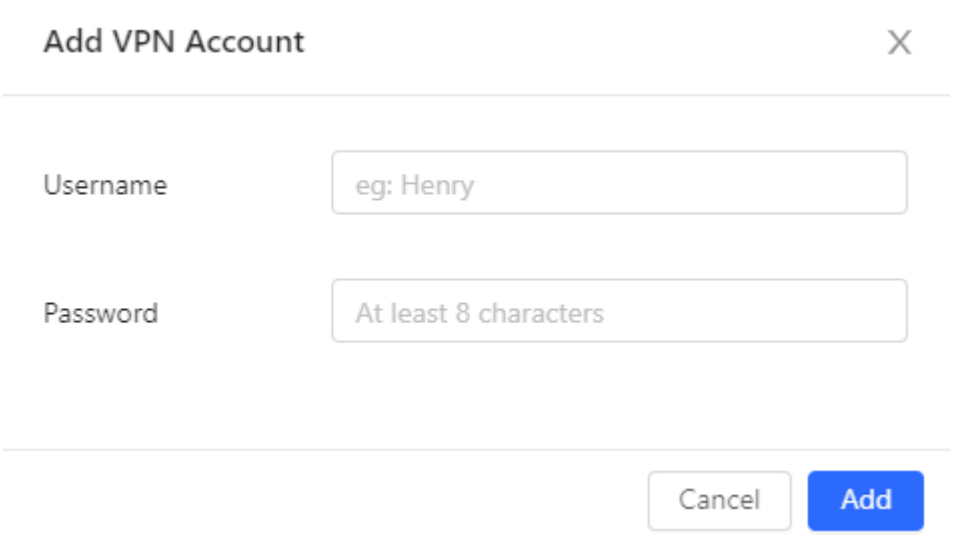
Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the server of the VPN tunnel. After the client dials into the VPN, the client can access the server through this IP address.
IP Pool	Specify the address pool used by the L2TP server to allocate IP addresses to clients.
DNS	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 **Project > Configuration** > **Devices** > **Gateway** > **VPN** > **VPN Account**.

b Click **Add VPN Account**.



c Configure items related to a VPN account.

Table 8-4 VPN Account Configuration Items

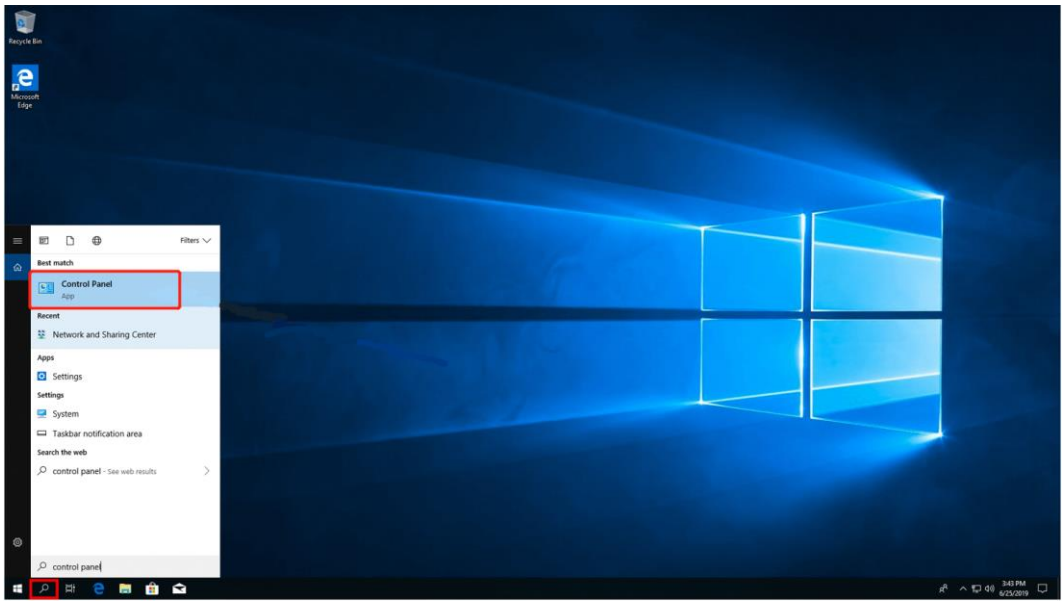
Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

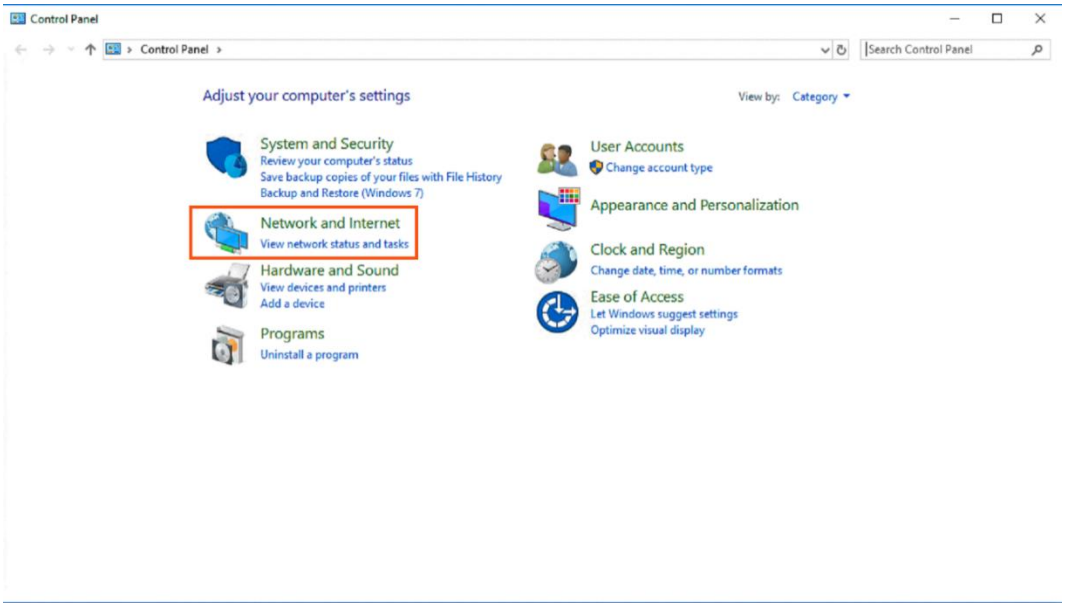
d Click **Add**.

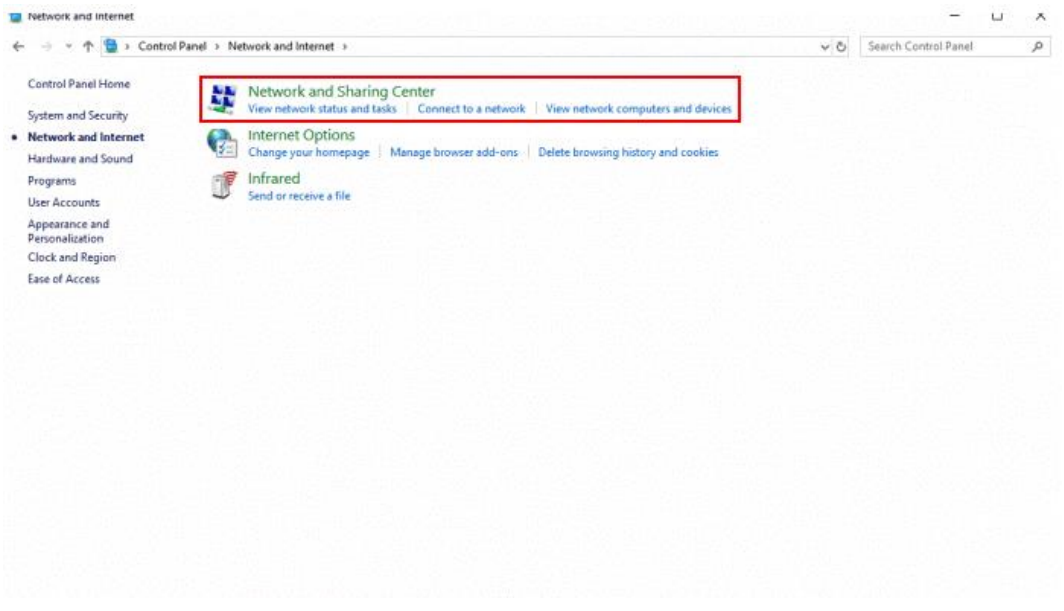
(3) Configure the client.

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.

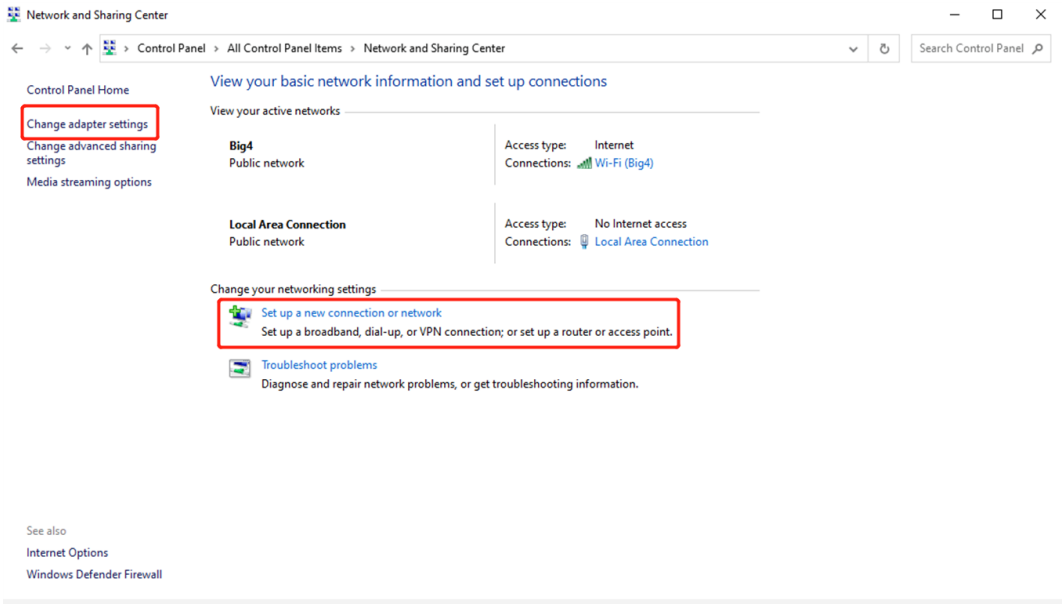
a Choose **Control Pane** > **Network and Internet** > **Network and Sharing Center**.

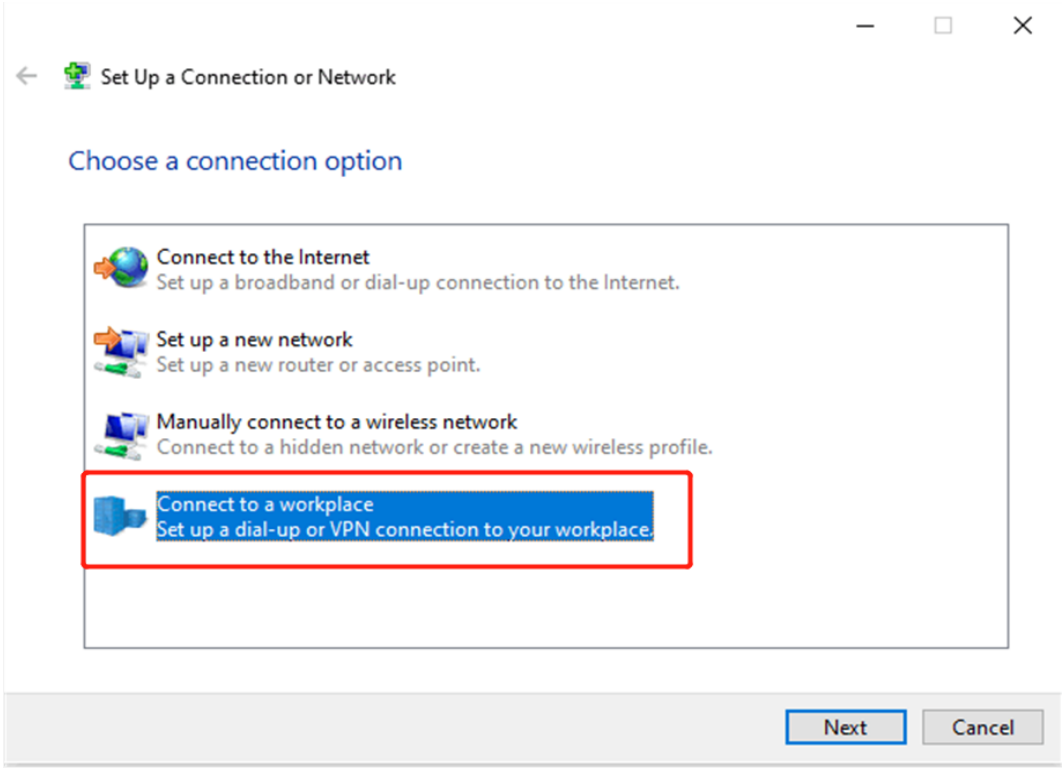

Recycle Bin
Microsoft Edge
Filters
Best match
Control Panel
App
Recent
Network and Sharing Center
Apps
Settings
Settings
System
Taskbar notification area
Search the web
control panel - See web results
control panel

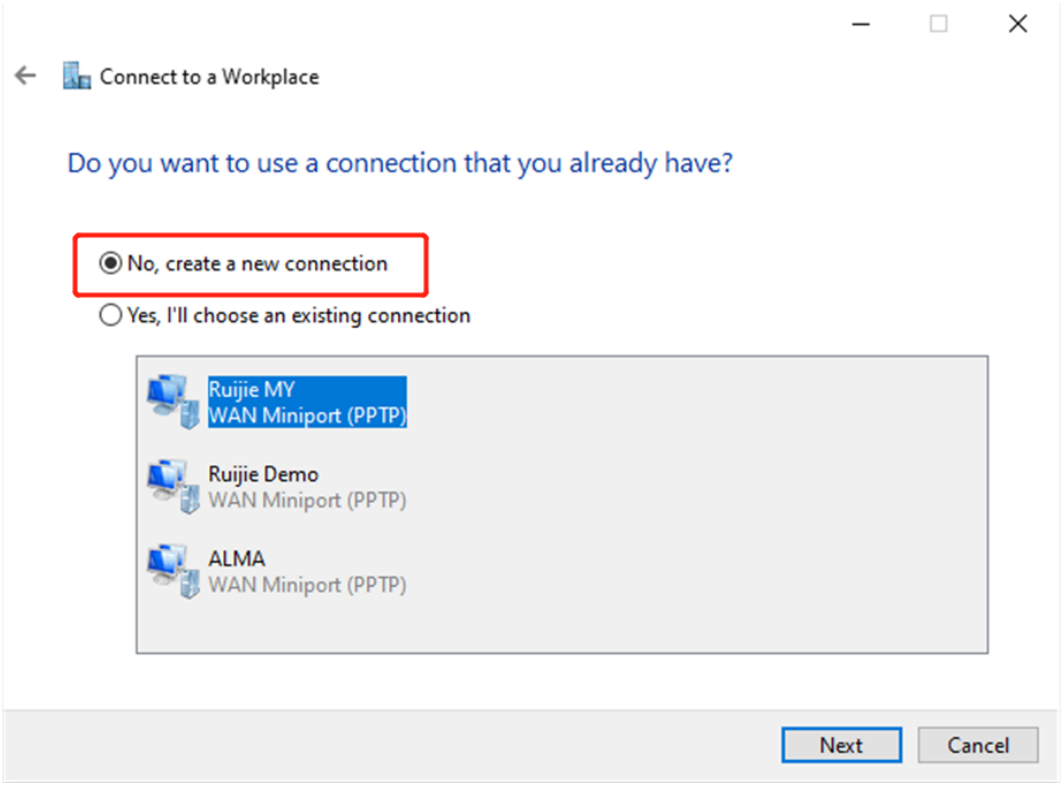

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
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

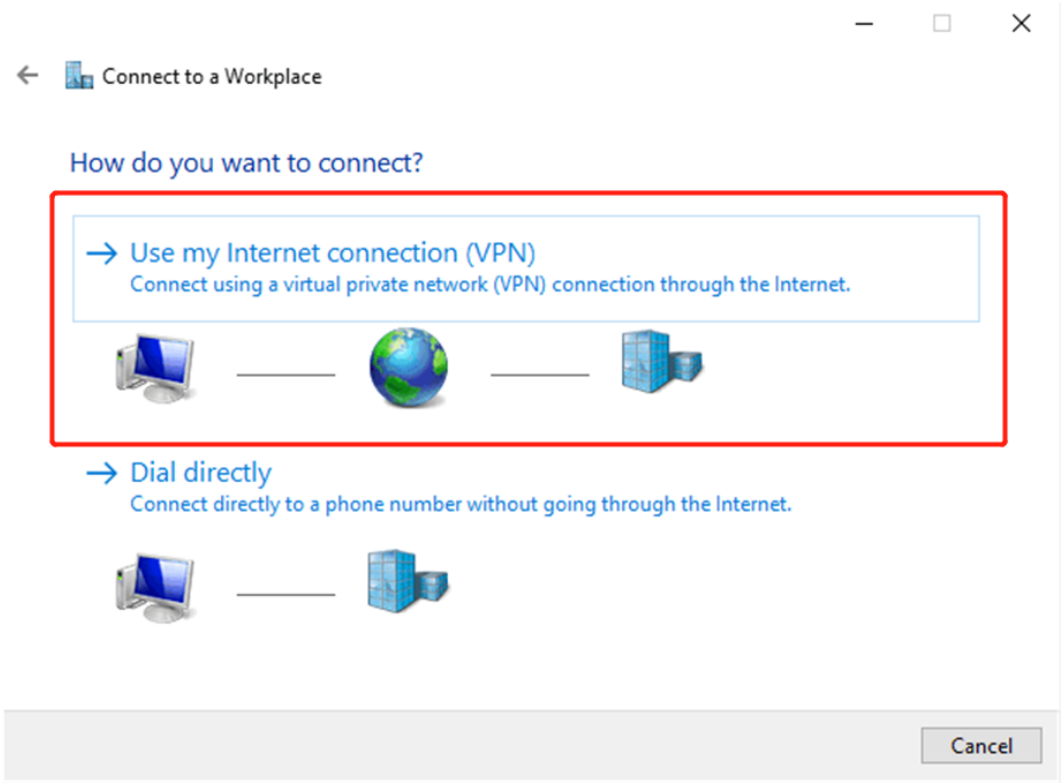

Network and Internet
Control Panel
Network and Internet
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect 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

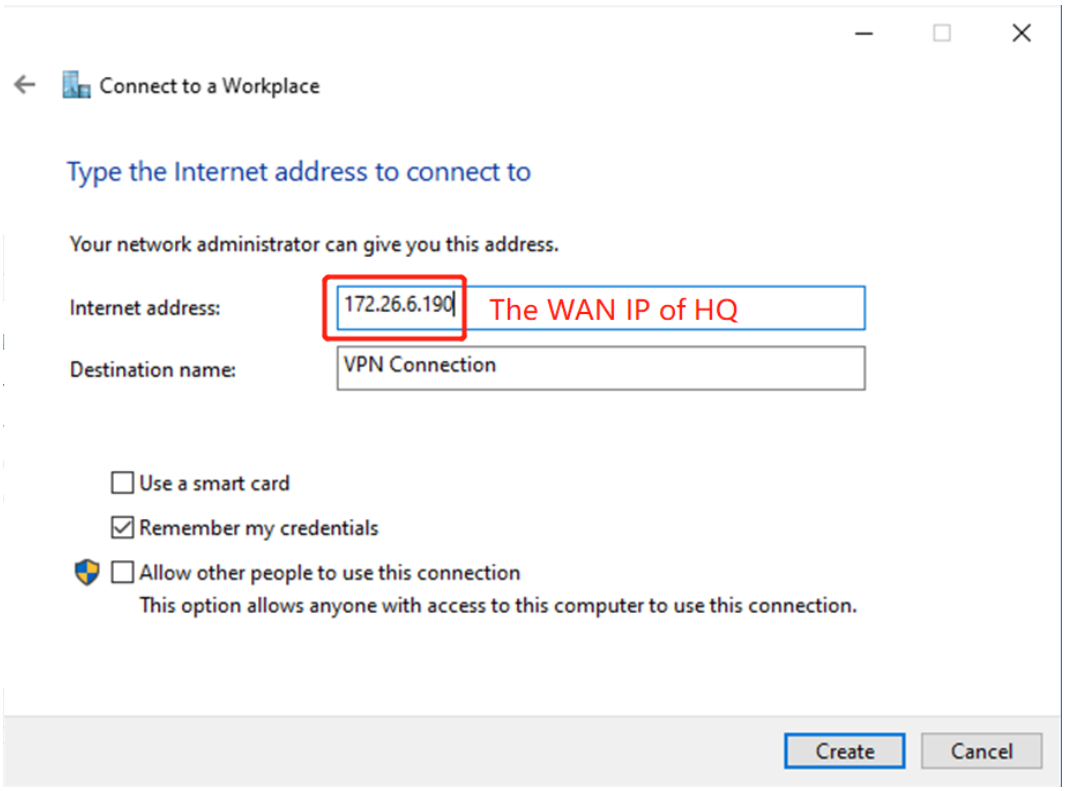
b Configure a VPN connection.



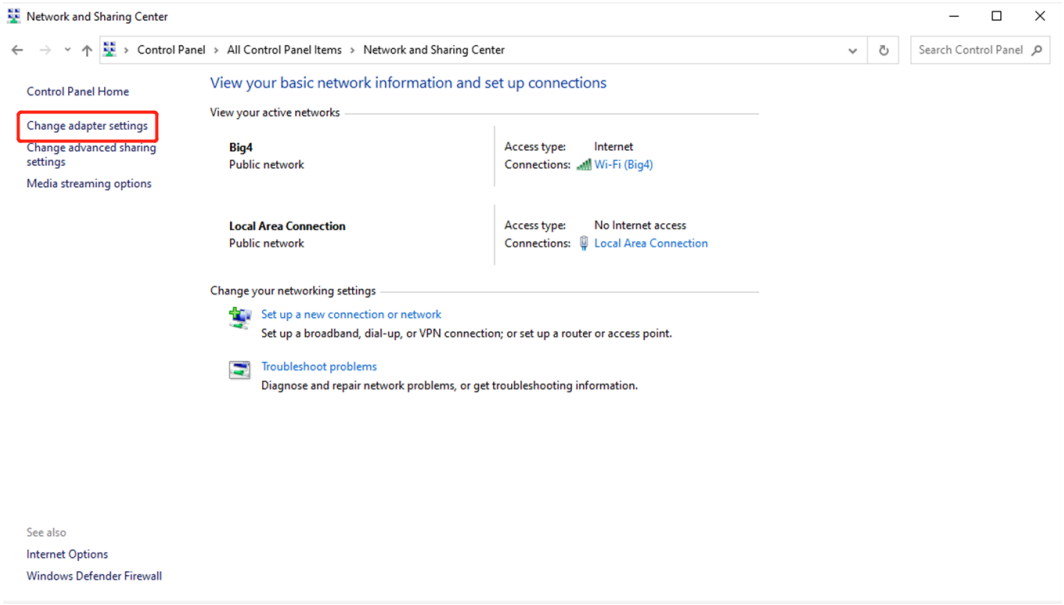


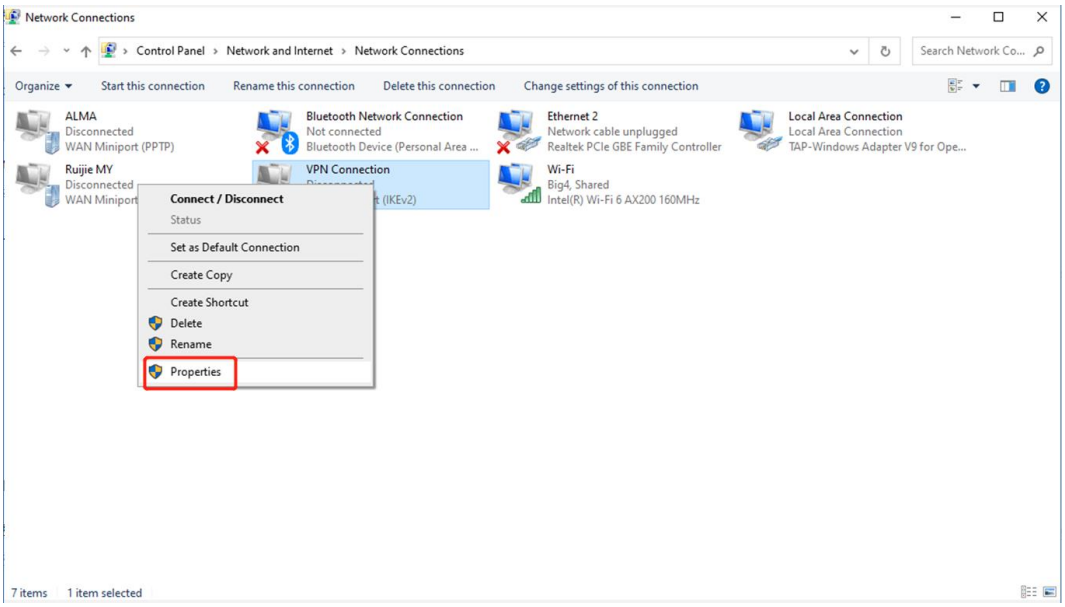

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

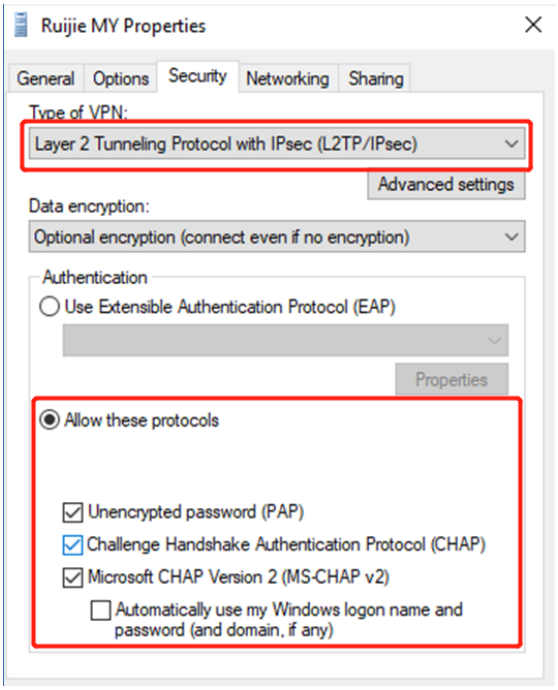

Connect to a Workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
Cancel



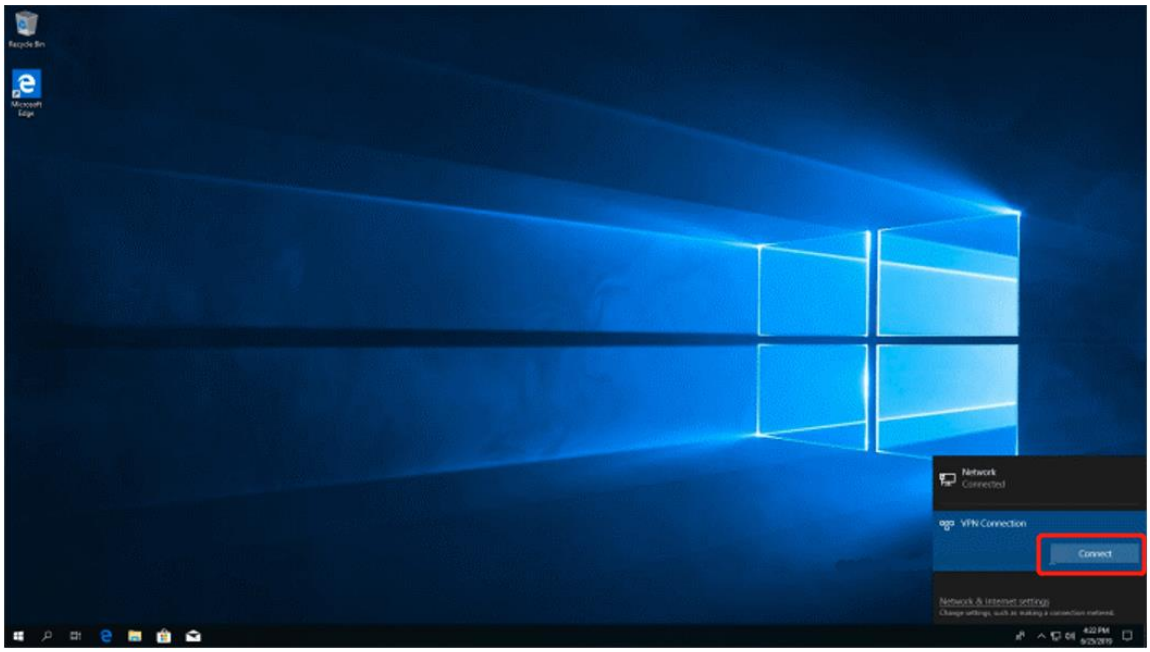
c Change adapter's settings.

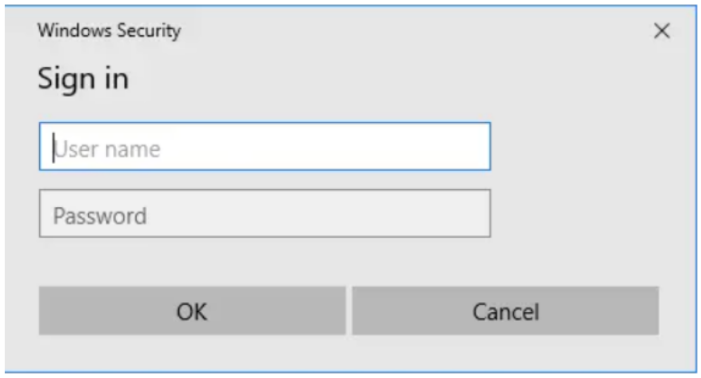


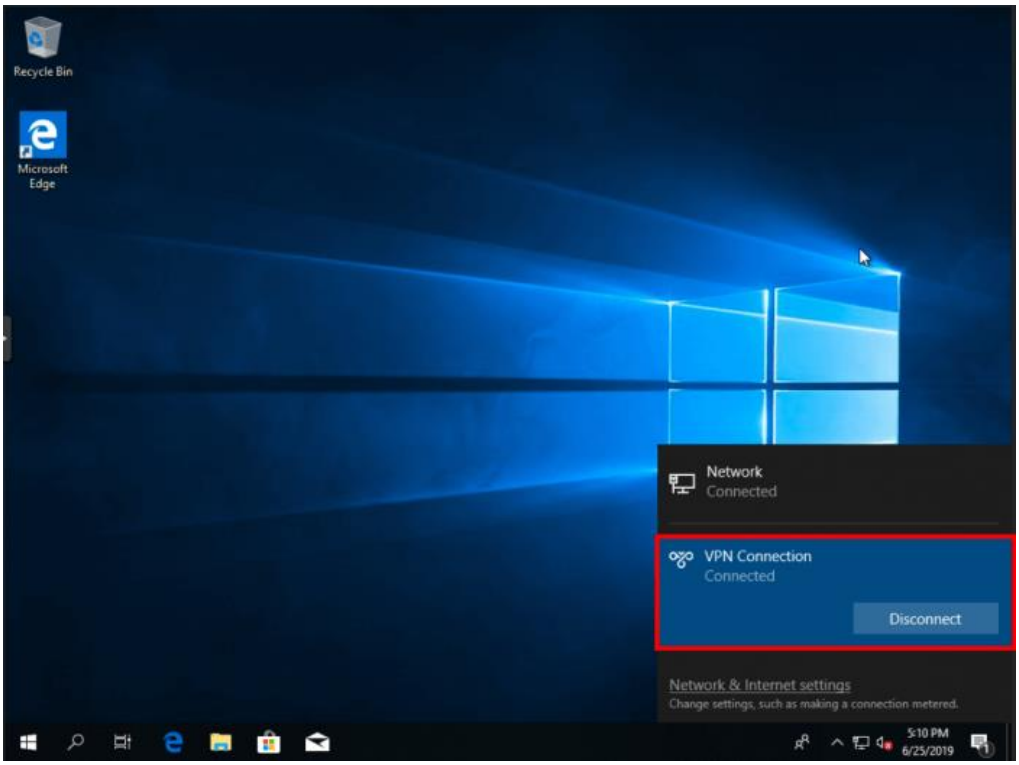




d Check the VPN connection status.


Network
Connected
VPN Connection
Connect
Network & Internet settings


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
```

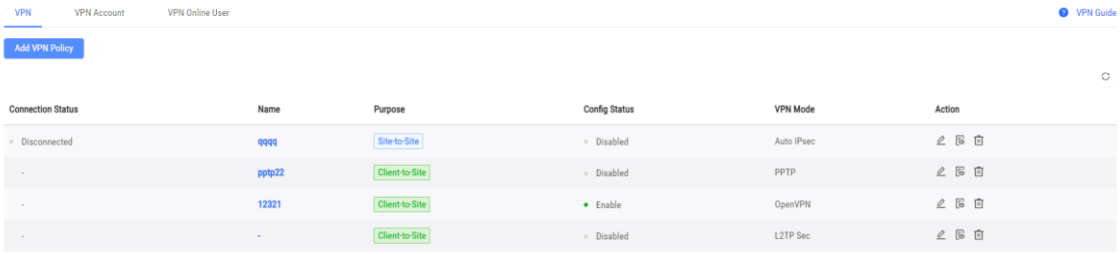
5. Configuring Client-to-Site VPN (Based on L2TP over IPSec VPN)

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.

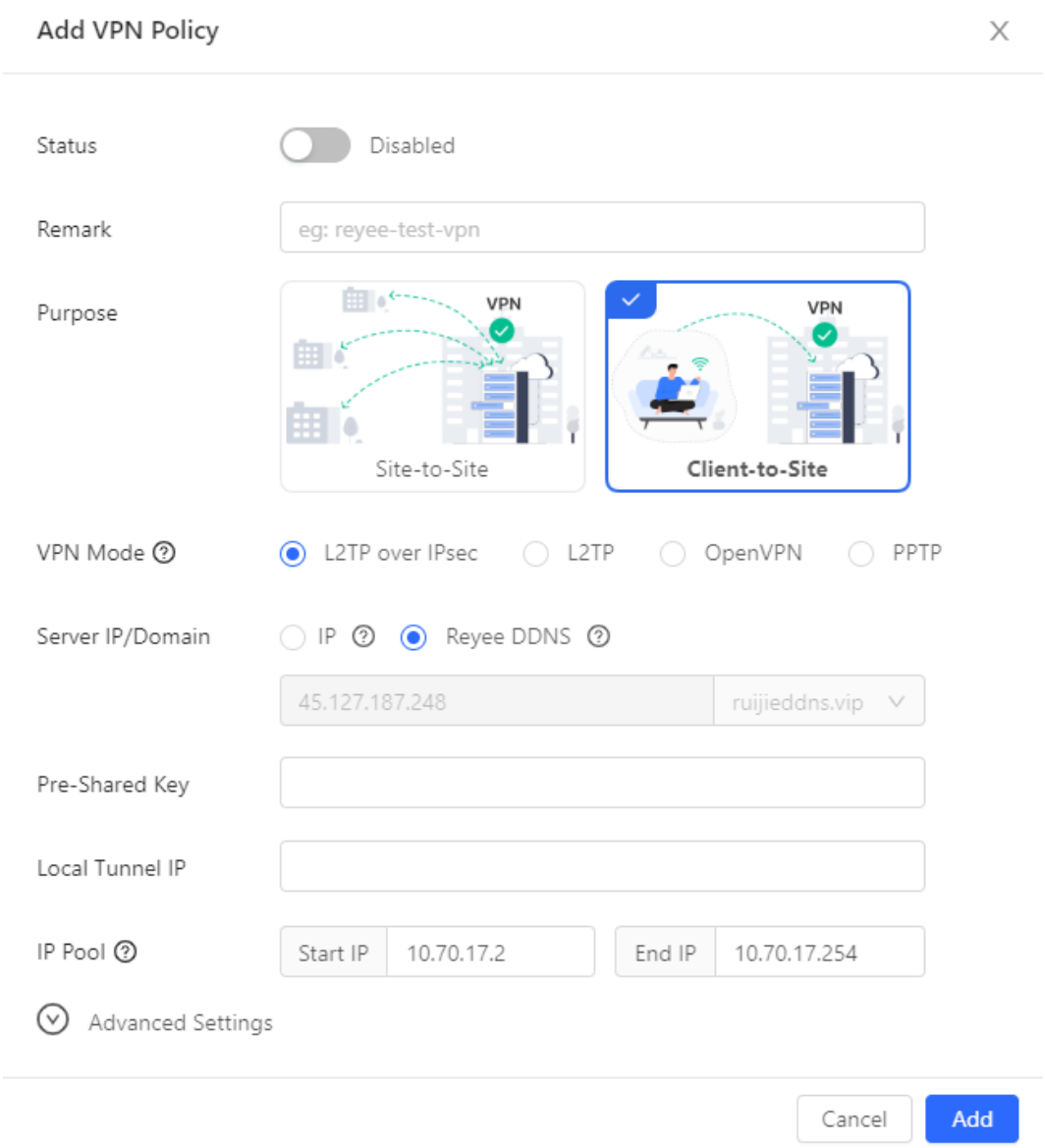
(1) Configure VPN for the HQ gateway.

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 **Project > Configuration** > **Devices** > **Gateway** > **VPN** > **VPN**.



c Click **Add VPN Policy**.



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.

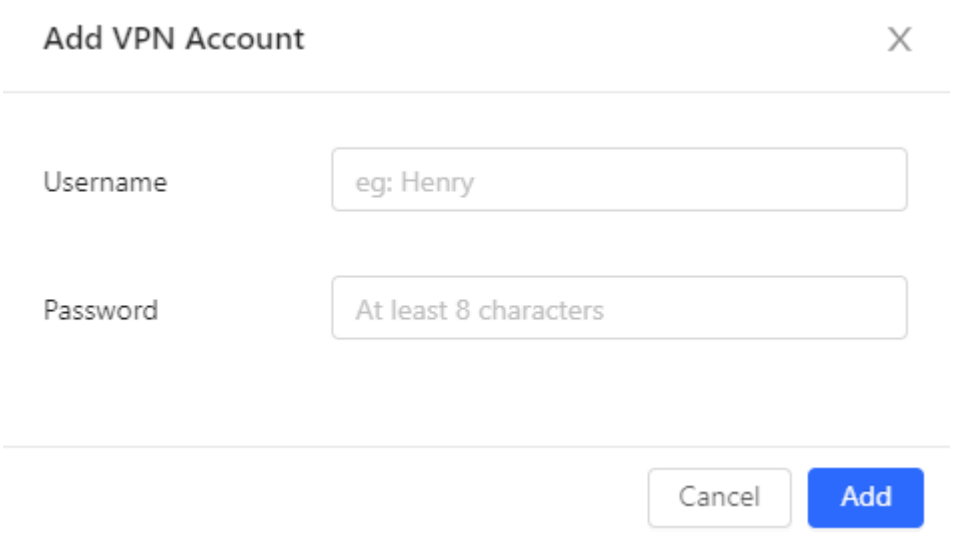
Parameter	Description
Local Tunnel IP	
IP Pool	Specify the address pool used by the server to allocate IP addresses to clients.
DNS	
Tunnel Authentication	
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP over IPsec VPN is deployed.

(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**.

b Click **Add VPN Account**.



c Configure items related to a VPN account.

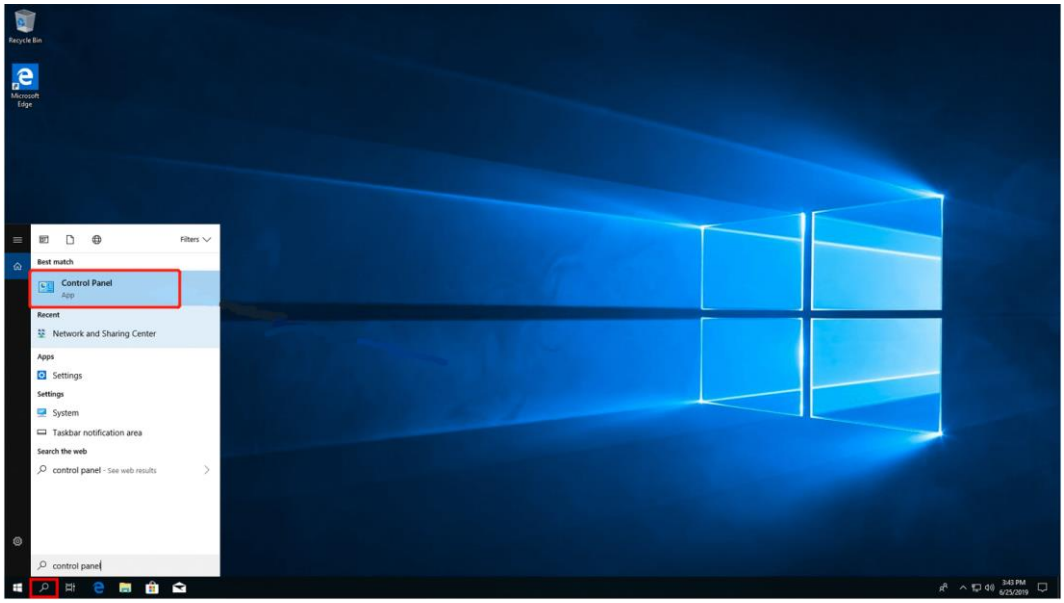
Table 8-5 VPN Account Configuration Items

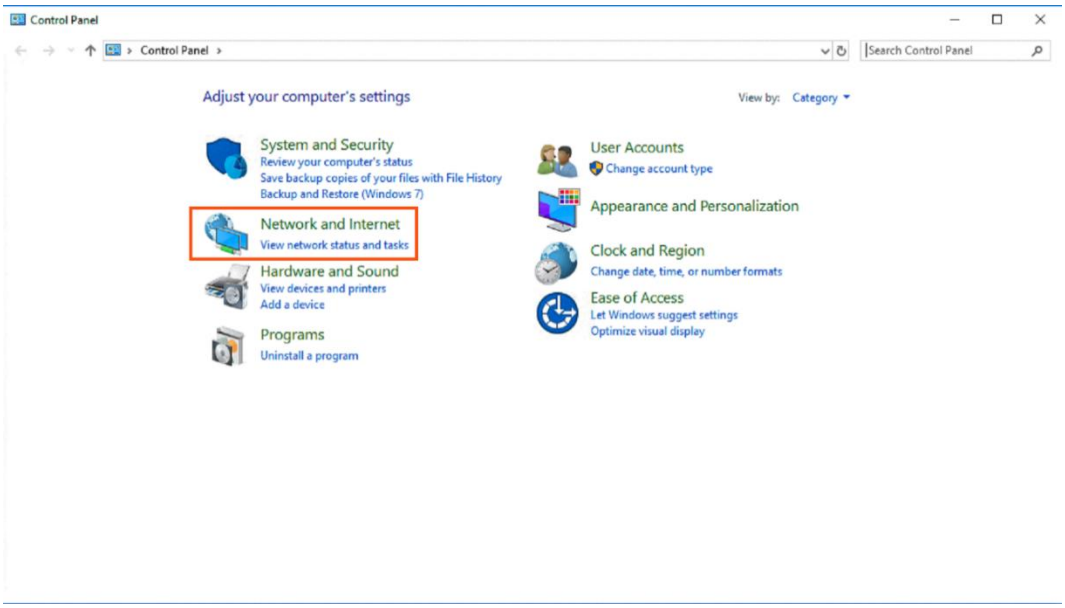
Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

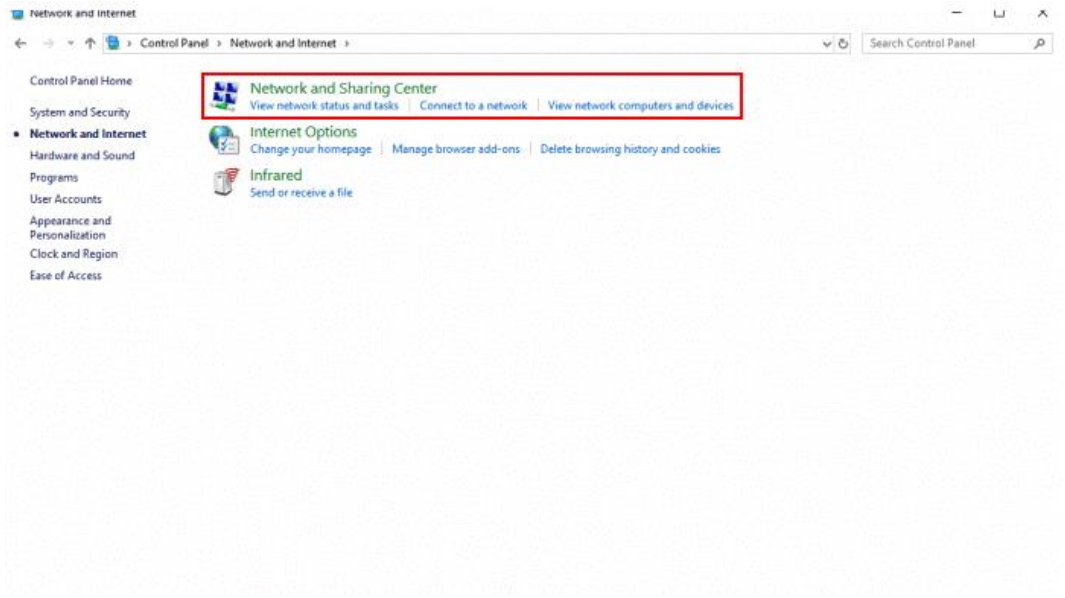
d Click **Add**.

(3) Configure the client.

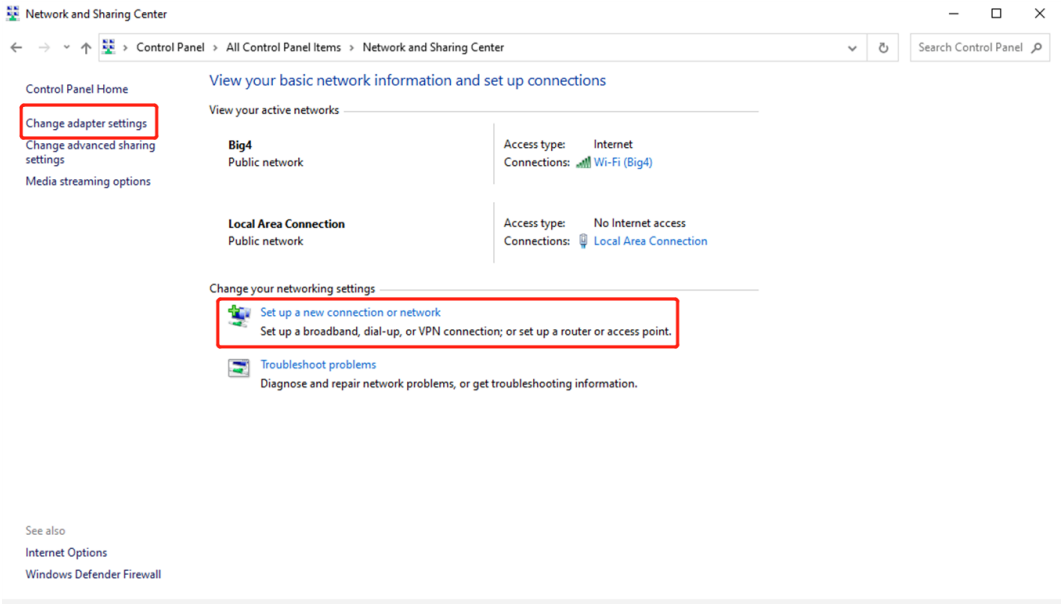
a Choose **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

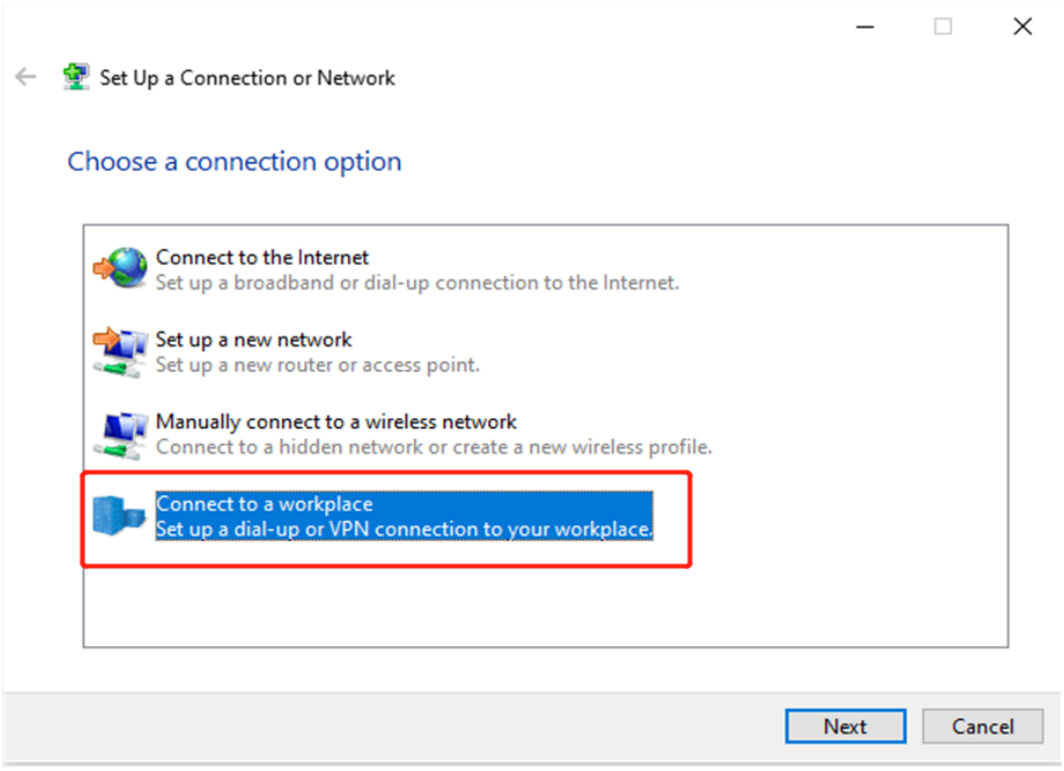


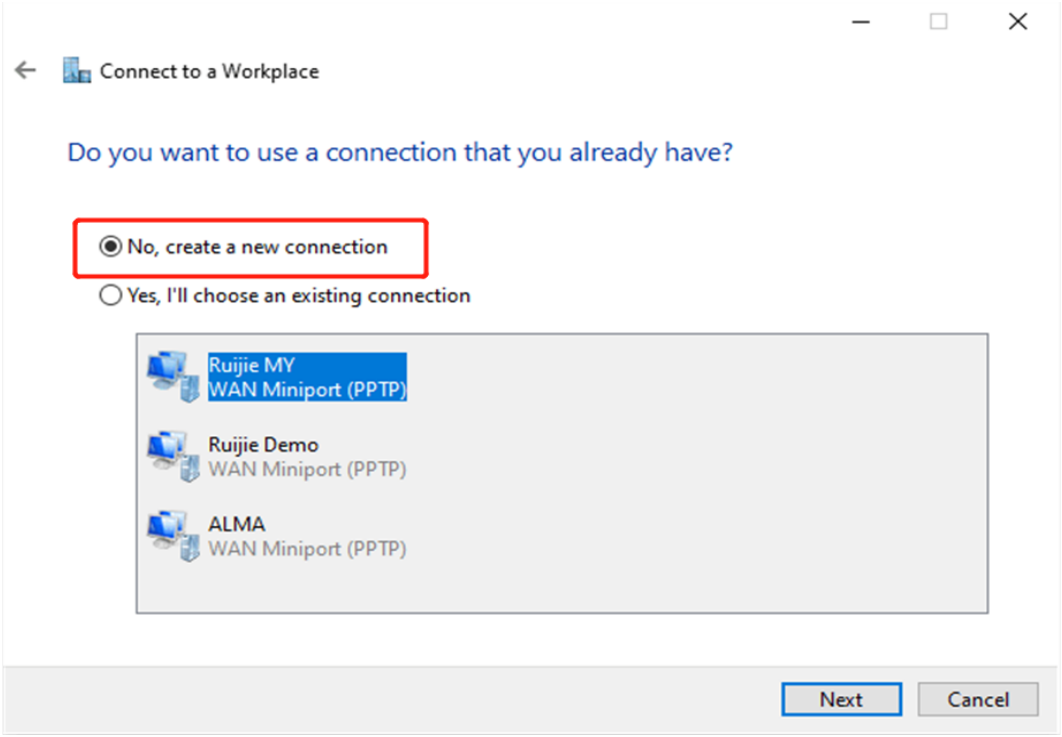


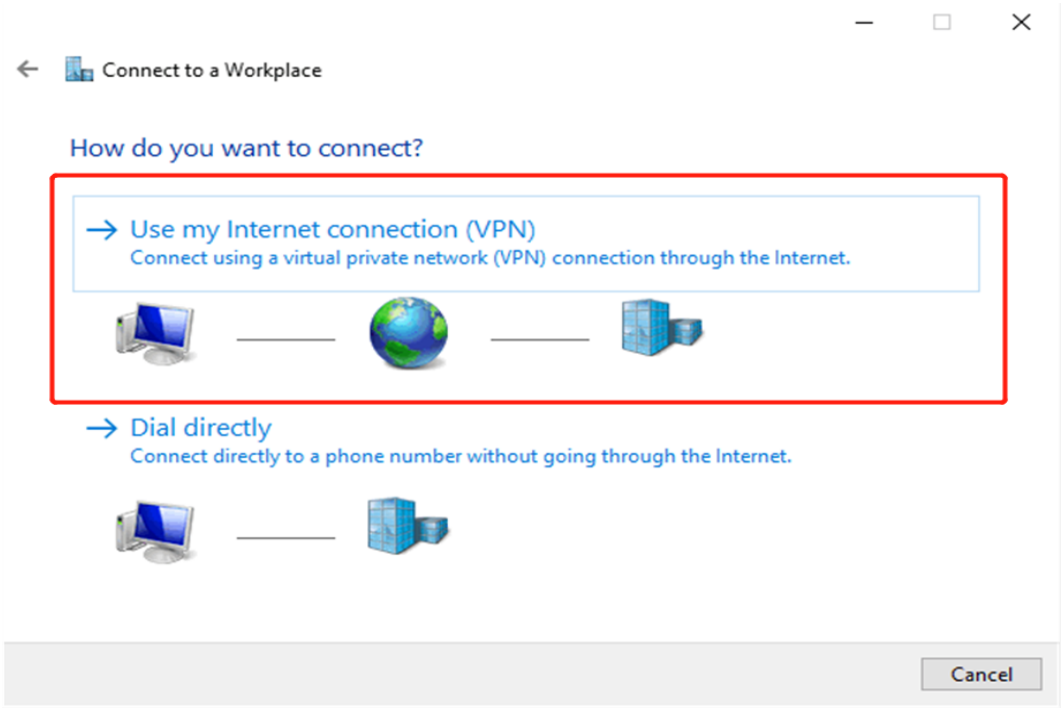


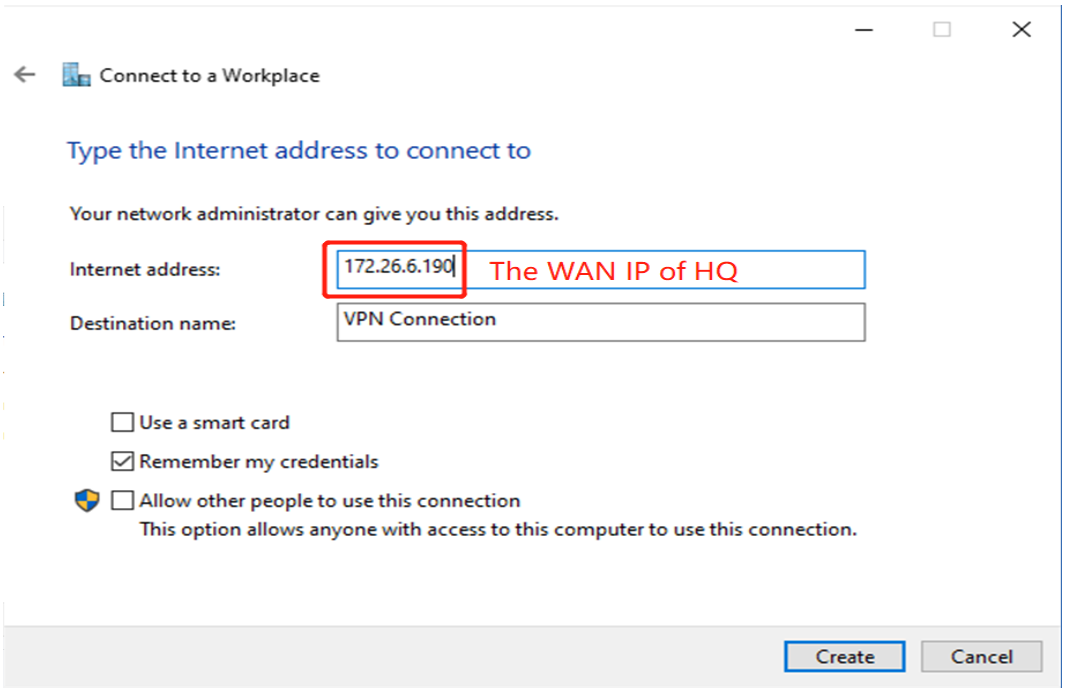
b Configure a VPN connection.



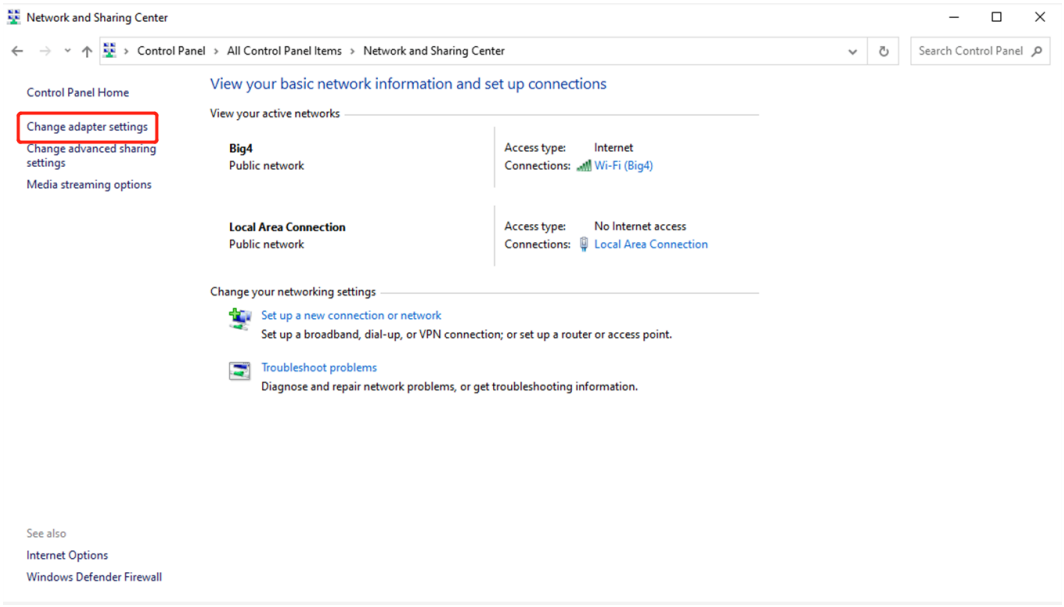

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel

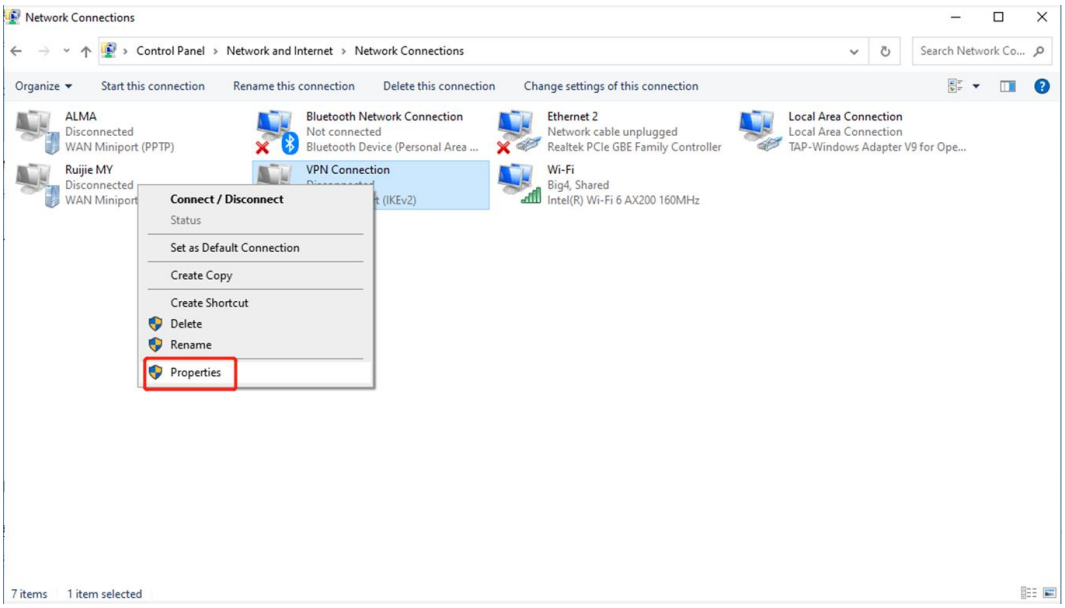

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

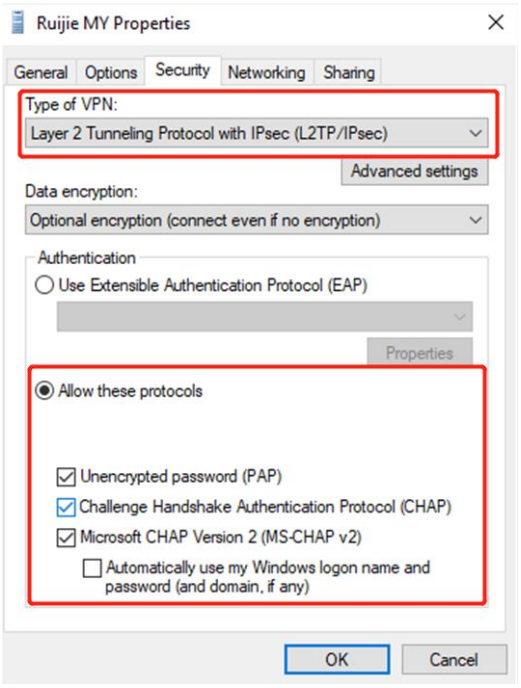




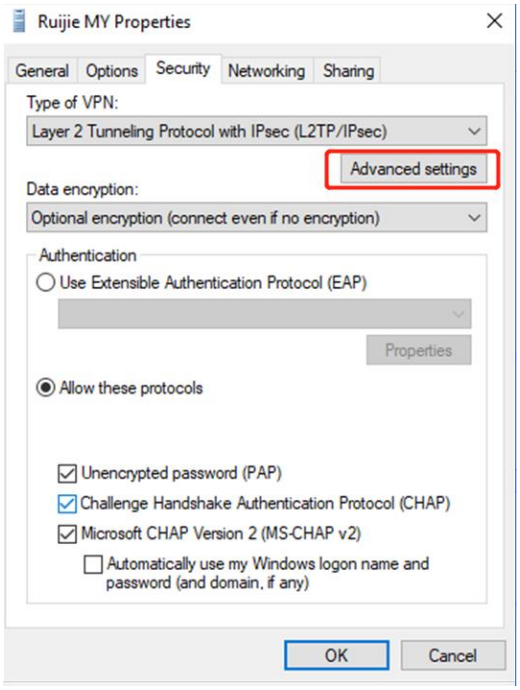
c Change adapter's settings.

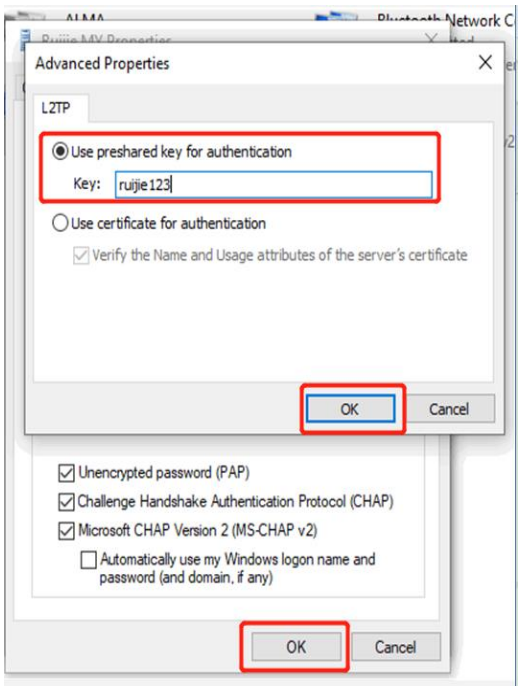

Network and Sharing Center
Control Panel › All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
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
VPN Connection
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

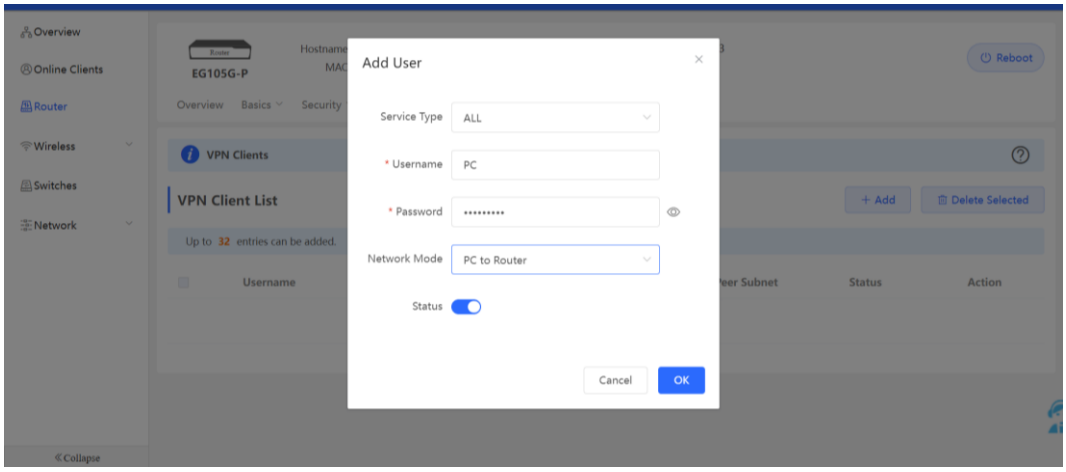


d Click **Advanced Settings** to configure the pre-shared password.





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



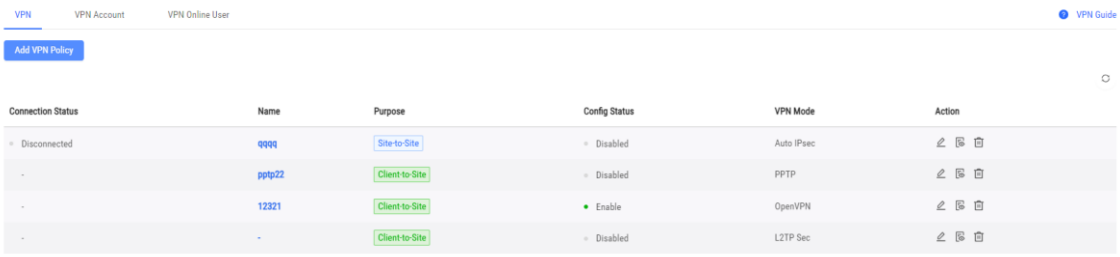
6. Configuring Client-to-Site VPN (Based on Open VPN)

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.

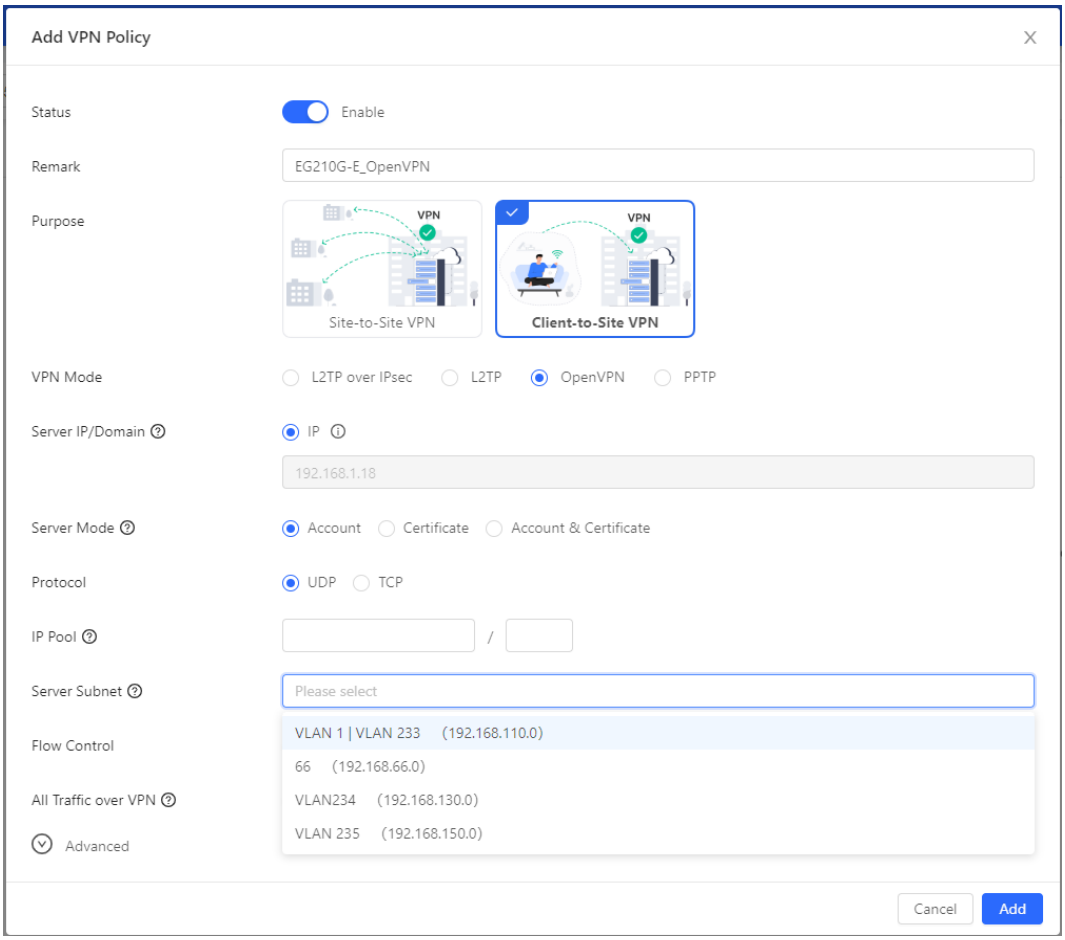
(1) Configure VPN for the HQ gateway.

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**.



c Click **Add VPN Policy**.



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.

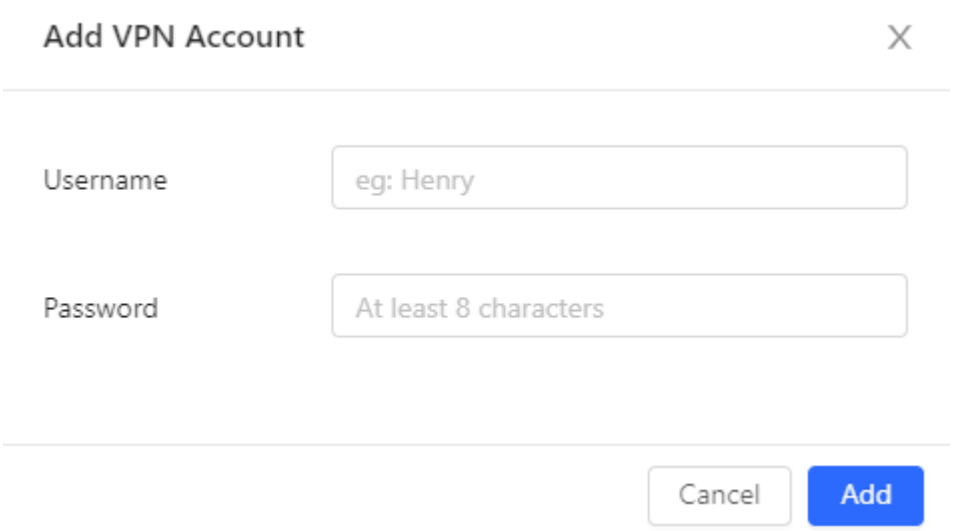
Parameter	Description
Server Mode	Select a server authentication mode. The options are **Account** and **Certificate**, • Account: Enter the correct username and password and upload the CA certificate on the client to connect to the server. The configuration is simple. • Certificate: Upload the CA certificate 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.
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**.

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.

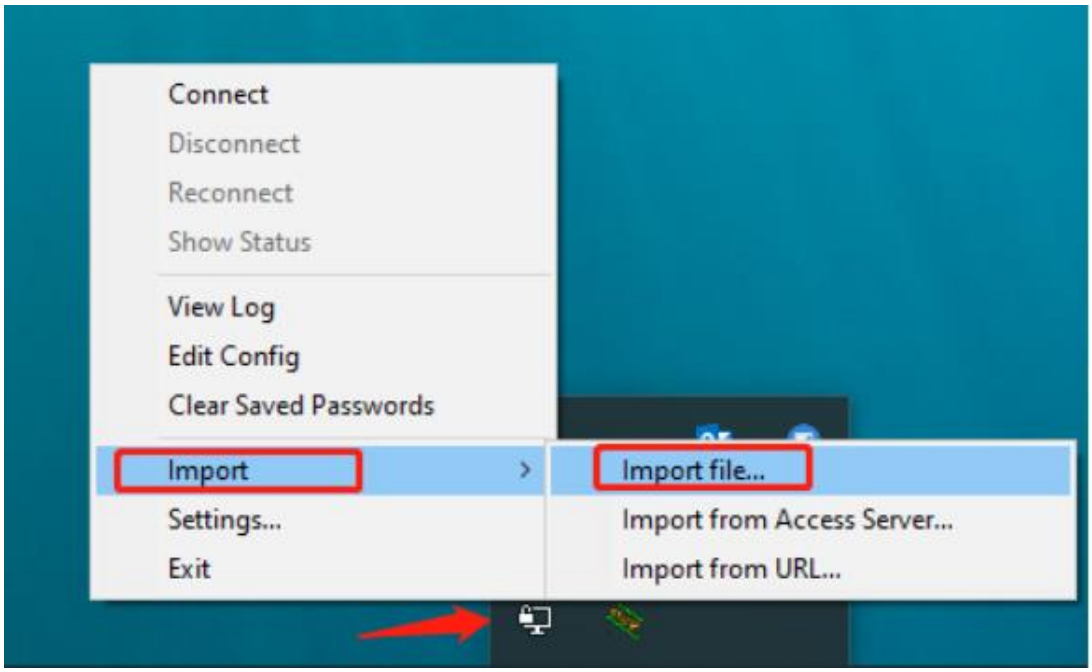
The following uses a Windows 10 client as an example for description. For the configuration of other clients, click **VPN Guide** at the upper right corner of the configuration page.

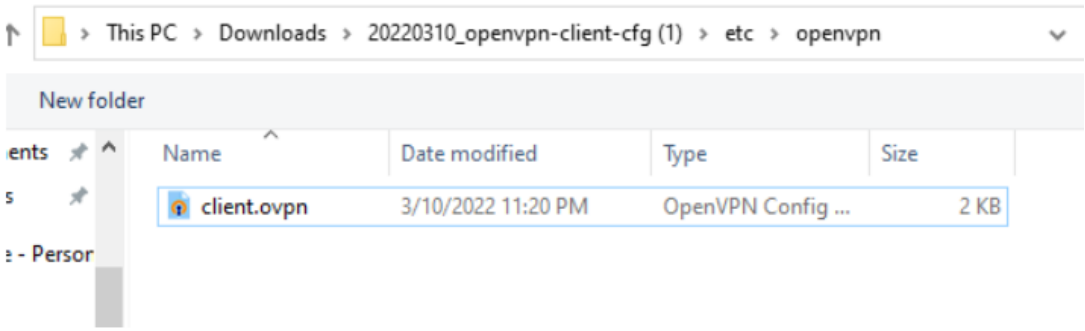
a Download and install OpenVPN application to your PC.

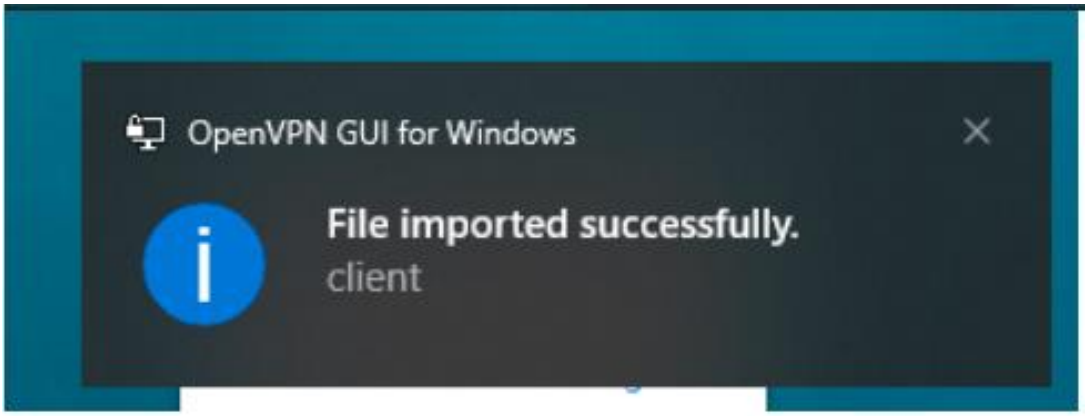
You can download OpenVPN client at https://openvpn.net/community-downloads/. Select a suitable version for your PC.

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.

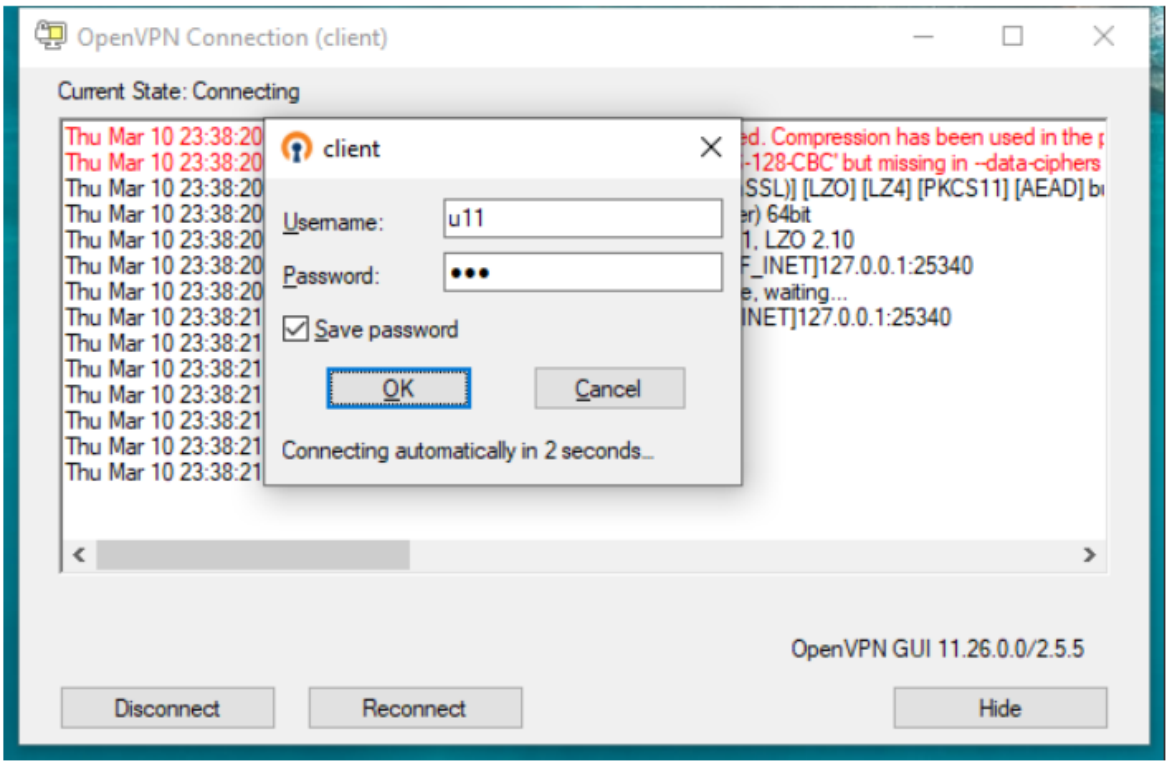


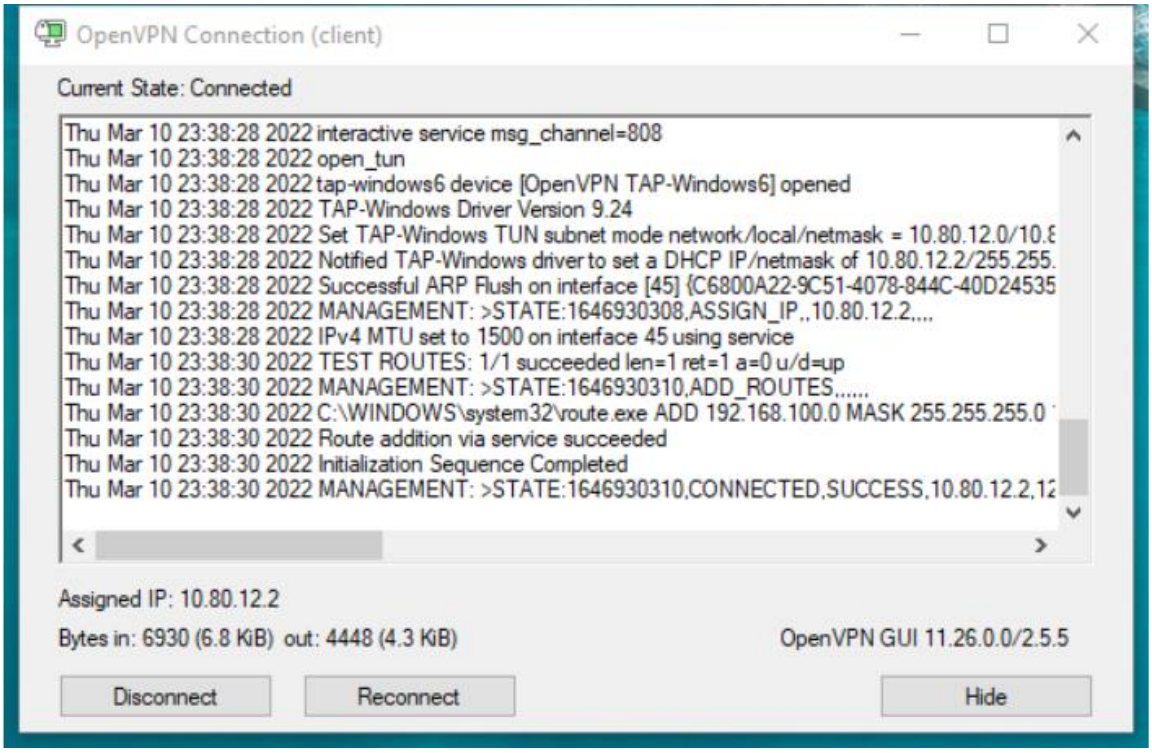




After the message "**File Imported successfully**" appears, you can connect to the VPN.

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


OpenVPN Connection (client)
Current State: Connecting
client
Username:
u11
Password:
Save password
OK
Cancel
Connecting automatically in 2 seconds...
OpenVPN GUI 11.26.0.0/2.5.5
Disconnect
Reconnect
Hide


OpenVPN Connection (client)
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 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
Disconnect
Reconnect
Hide

8.5 Configuring Portal Authentication

1. Overview

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

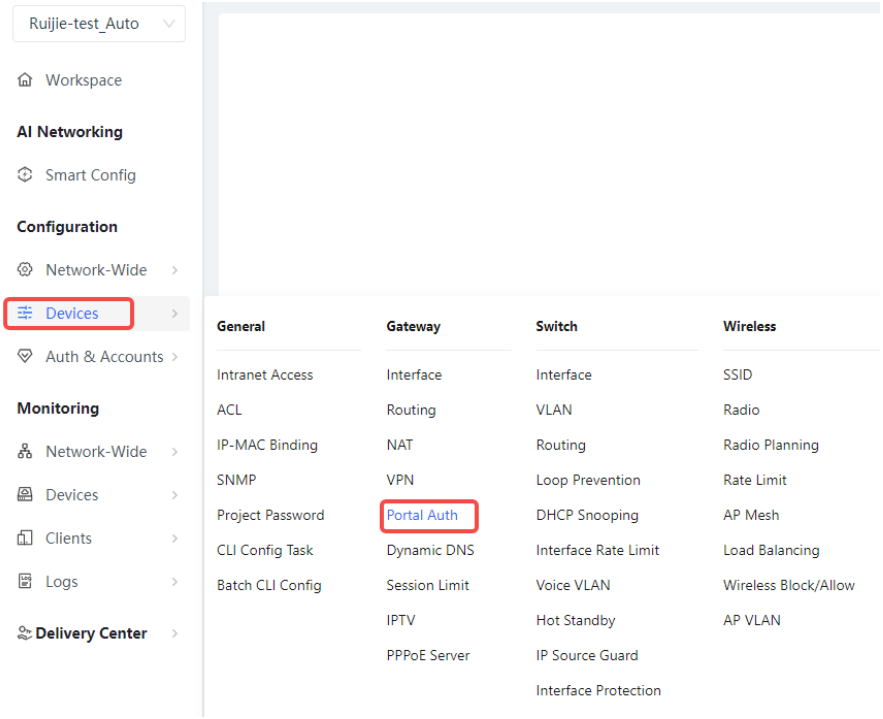
After completing the configuration on Ruijie Cloud, the configuration is synchronized Reyee EG devices.

2. Getting Started

- Before configuring portal authentication, choose **Configuration** > **Network-Wide** > **Network** to configure service networks, that is, configure the VLANs, to which the IP addresses of the authenticated clients belong.
- Choose **Configuration** > **Auth & Accounts** > **Authentication** > **Captive Portal** to configure the portal authentication page.

3. Configuration Steps

Choose Configuration > Devices > Gateway > Portal Auth.



(1) Enable the portal authentication function.

(2) In the **Authenticated IP segment** area, click **Add** and set parameters related to authenticated IP addresses.

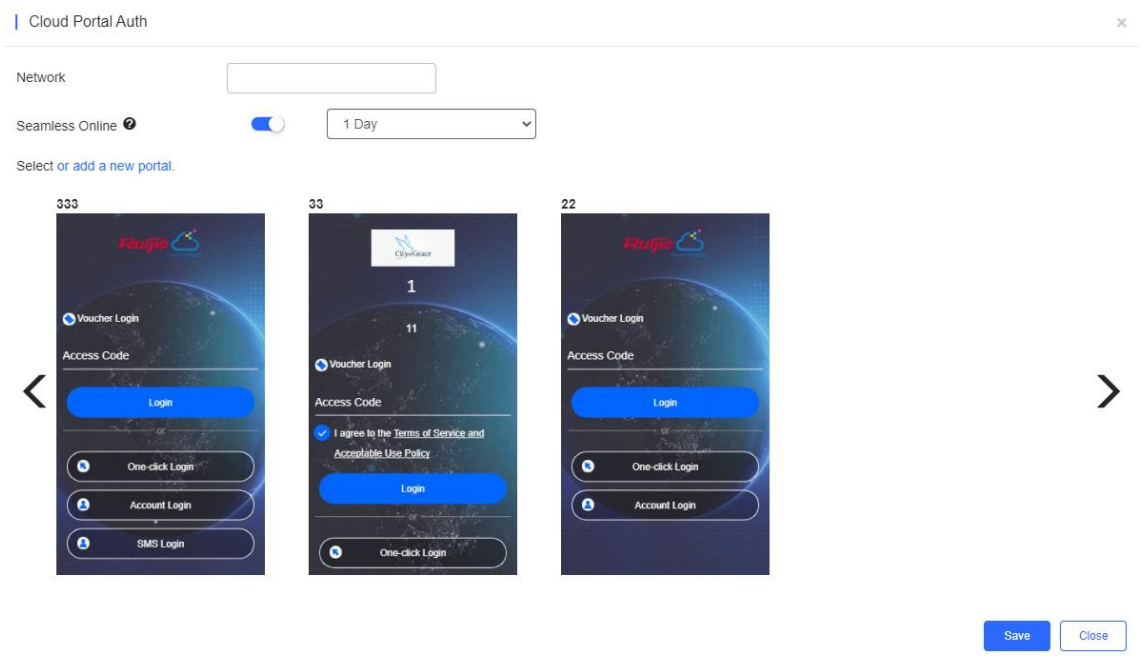


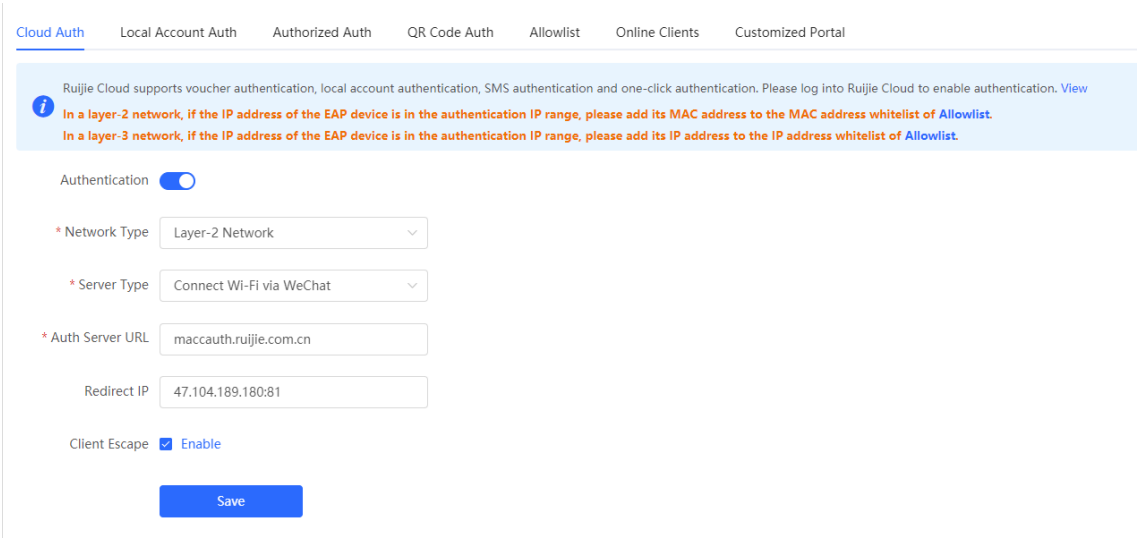
Table 8-7 Configuration Items Related to Authenticated IP Addresses

Parameter	Description
Network	Select the network segment, to which the IP address of an authenticated client belongs.
Seamless Online	After the function is enabled, clients in the authenticated IP address segment need to be authenticated only once if they log in within the specified time. After the function is enabled, you need to set the time range.
Select or add a new portal	Select the portal page to be displayed during authentication. The portal page can be customized as required. For details, see 11.1 Captive Portal.

(3) Click **Save**.

4. Verification

Log in to the Web management page of the gateway. In local device mode, choose **Advanced** > **Authentication** > **Cloud Auth**. The configurations on the cloud have been synchronized to the device.



8.6 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 two DDNS protocols: No-IP DNS and DynDNS.

2. Getting Started

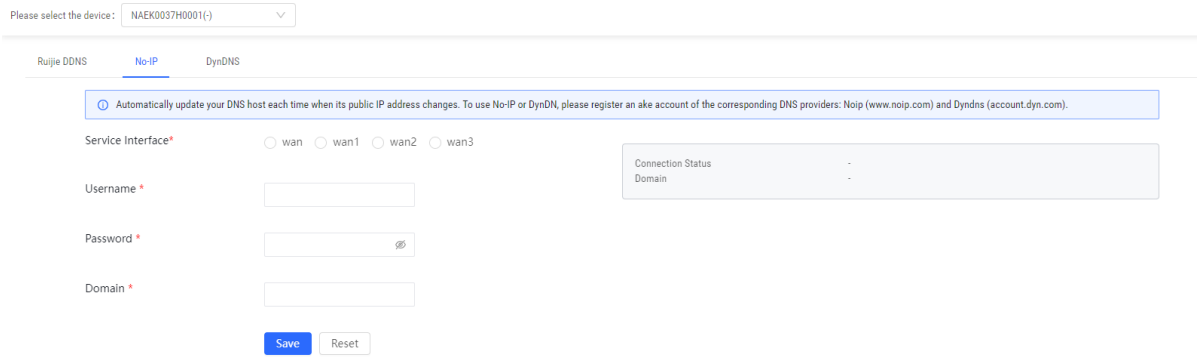
Before you use the DDNS service, you need to register an account and a domain name on the third-party DDNS service provider for this service.

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.



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

Table 8-8 DDNS login information

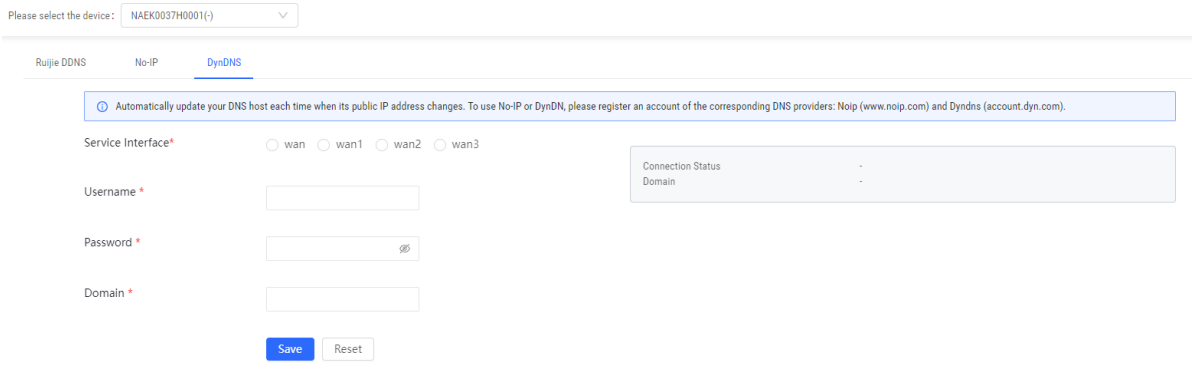
Parameter	Description
Service Interface	One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN port bound to the domain name when multiple WAN ports are available. By default, the service interface is a WAN port.
Username & Password	Enter the username and password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



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

Table 8-9 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.

8.7 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. Limitations

IPTV is only supported on Reyee devices.

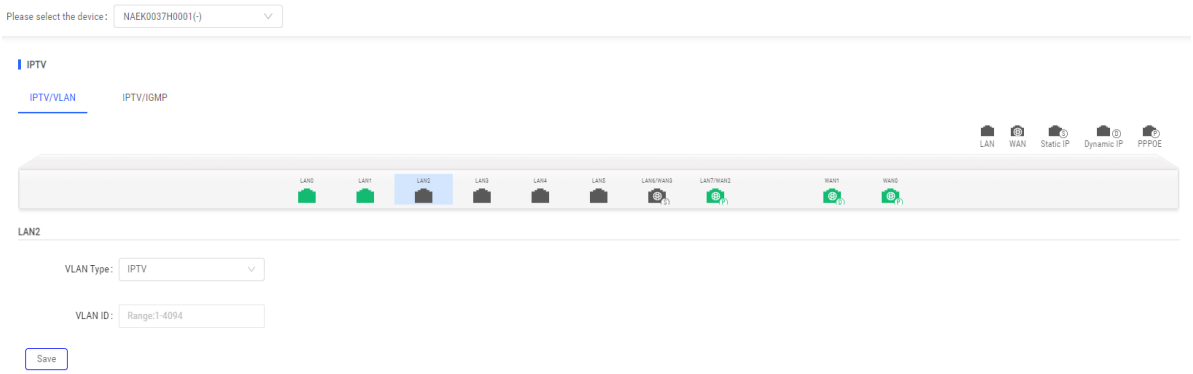
3. Getting Started

- 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.

4. Configuration Steps

- Configuring the IPTV Service of the VLAN Type

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



(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.

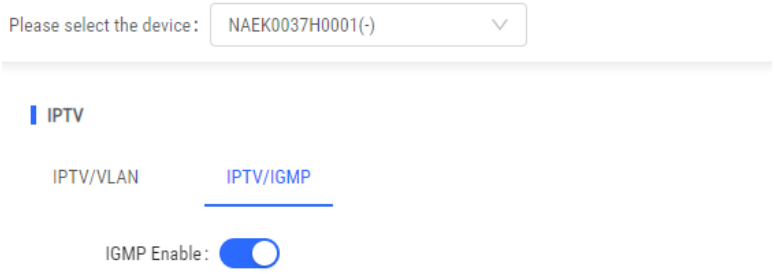
Caution

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.



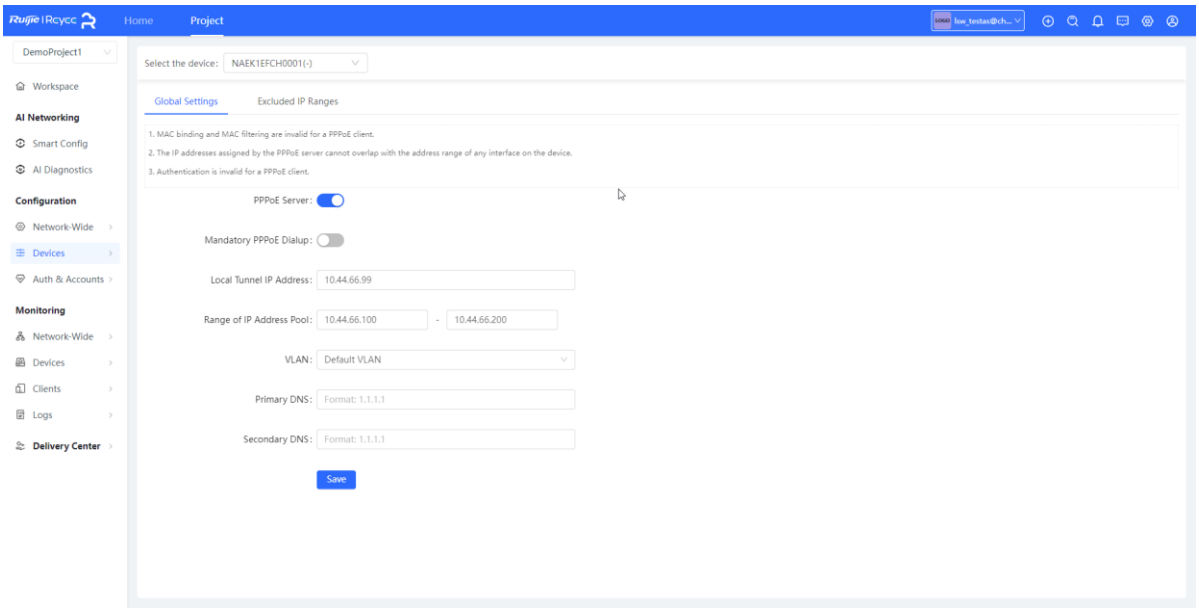
8.8 PPPoE Server

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.

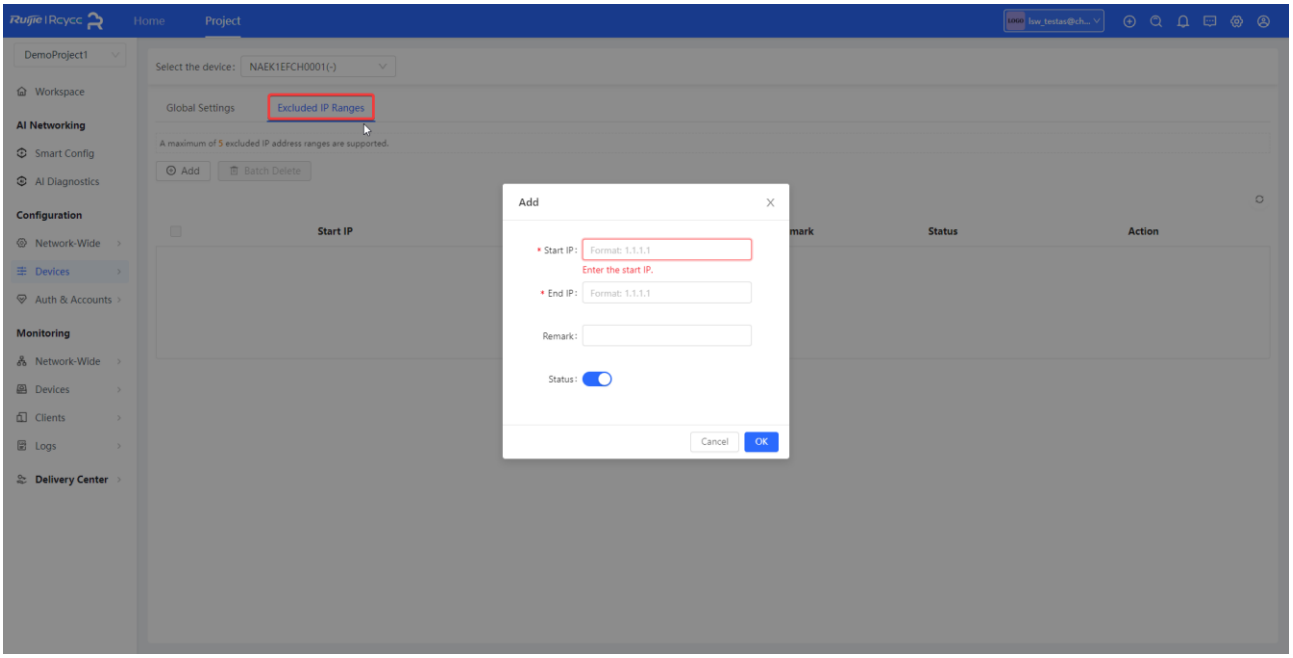
2. The IP addresses assigned by the PPPoE server cannot overlap with the address range of any interface on the device.

3. Authentication is invalid for a PPPoE client.



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

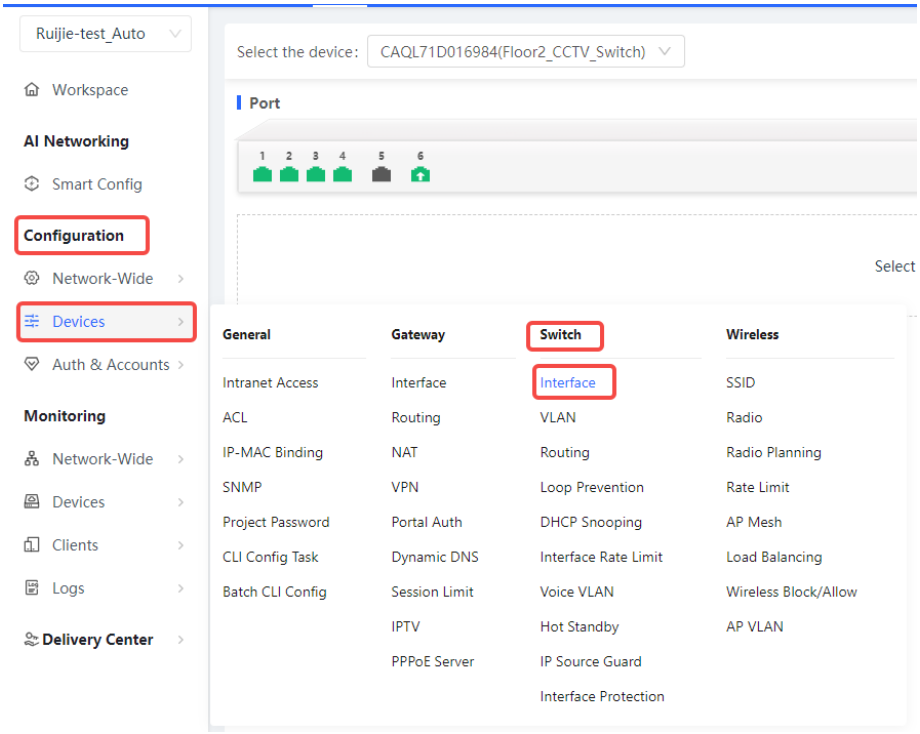
A maximum of 5 excluded IP address ranges are supported.



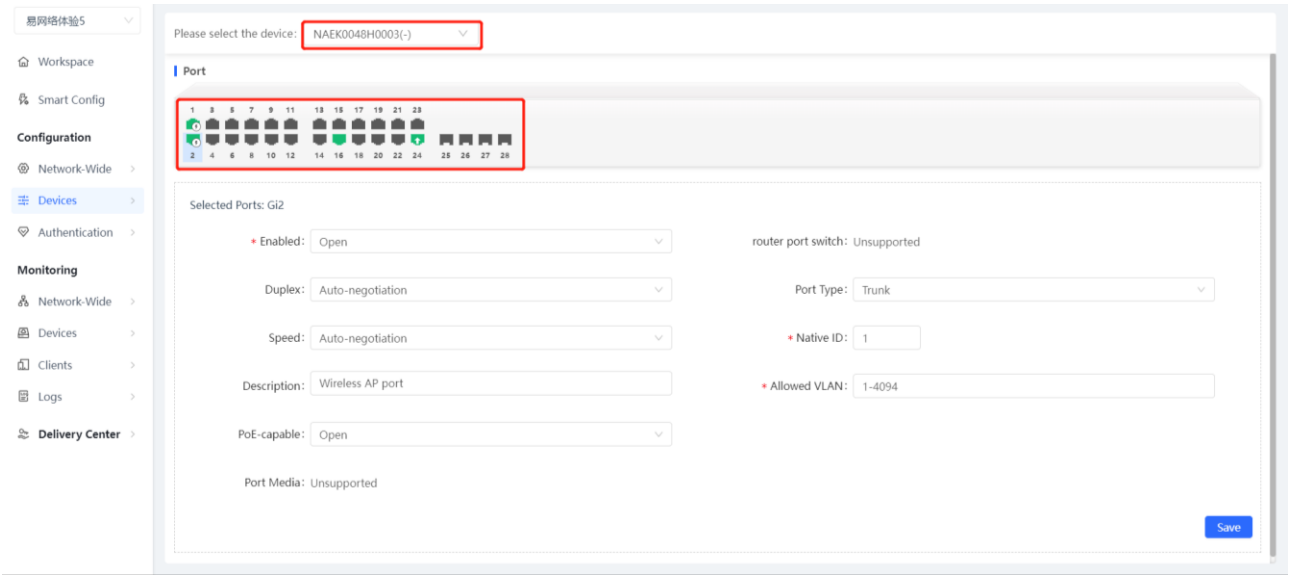
9 Switch Configuration

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**.

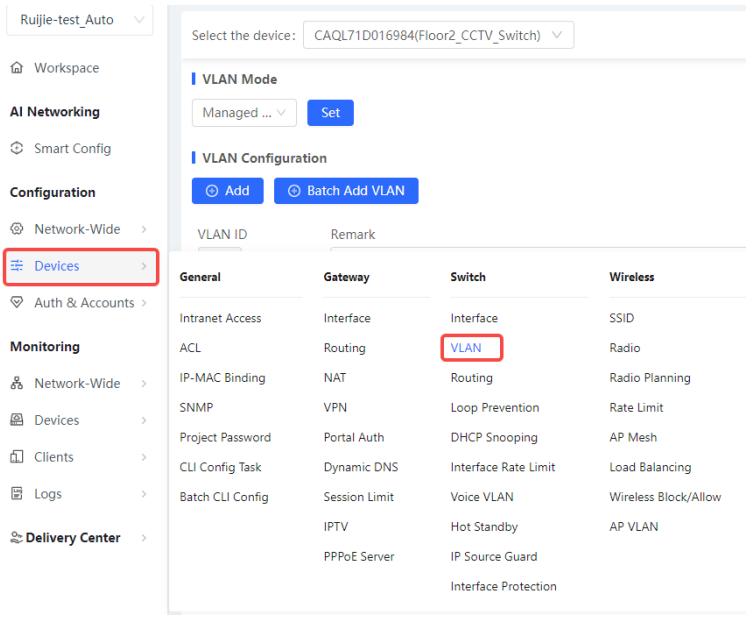


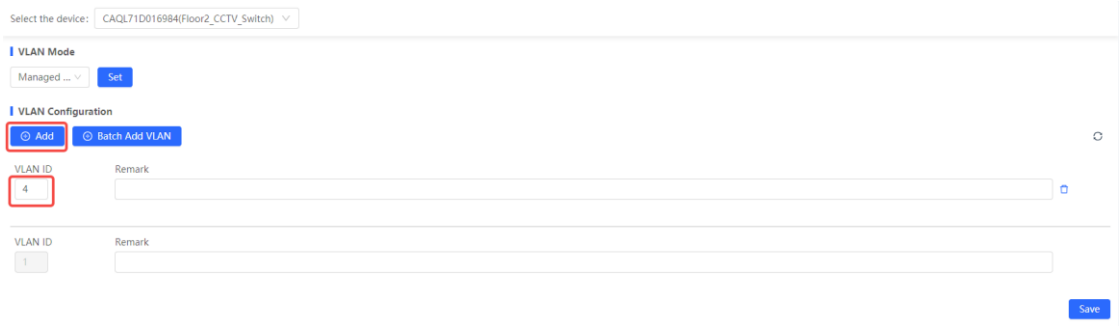
9.2 Configuring a VLAN for an Interface

(1) Creating a VLAN

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

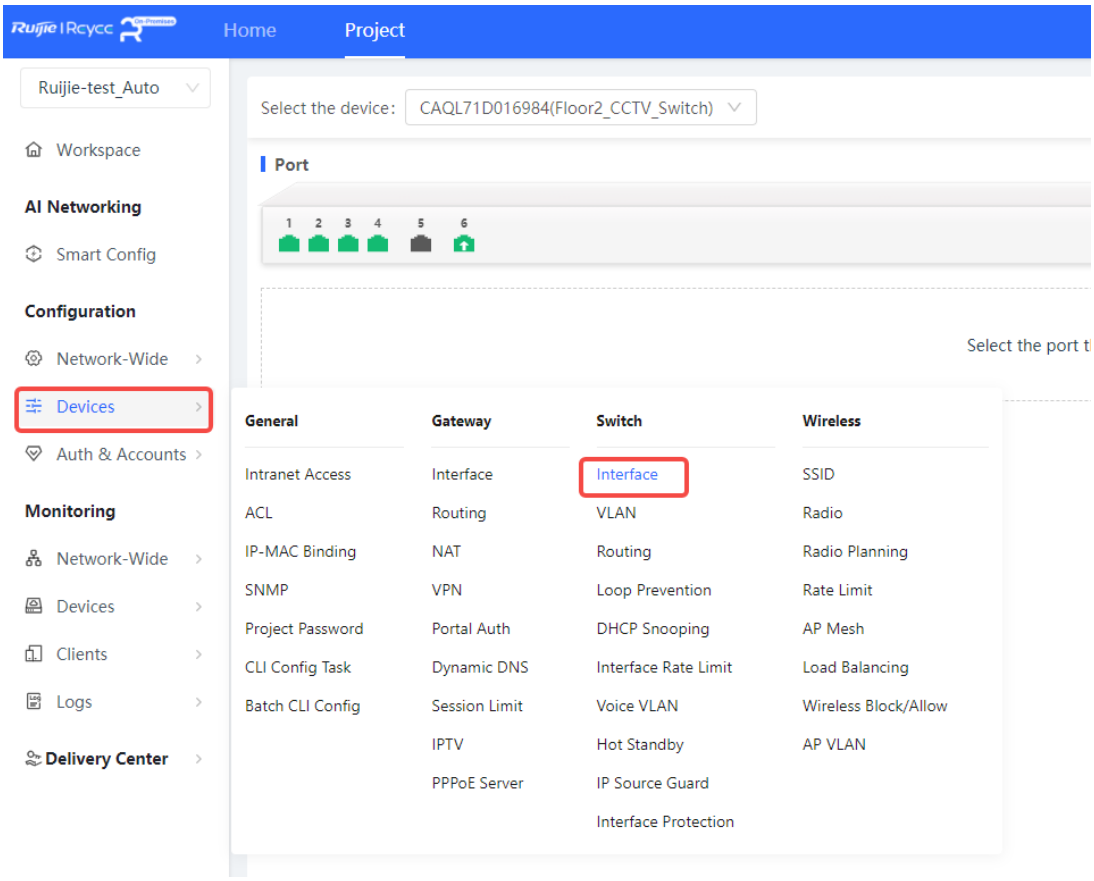
Click **Add**, set **VLAN ID**, and click **Save** to add a VLAN.



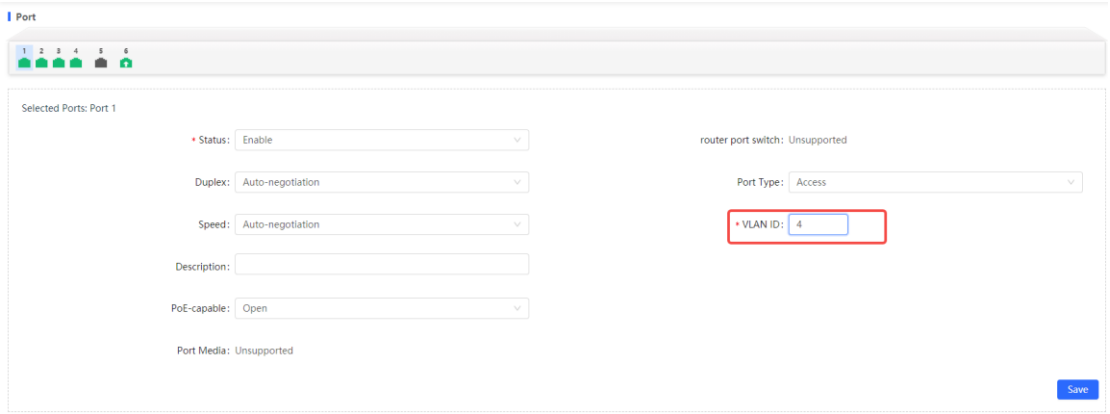


(2) Adding an interface to the VLAN

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



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



9.3 Routing

9.3.1 Adding a Static Route

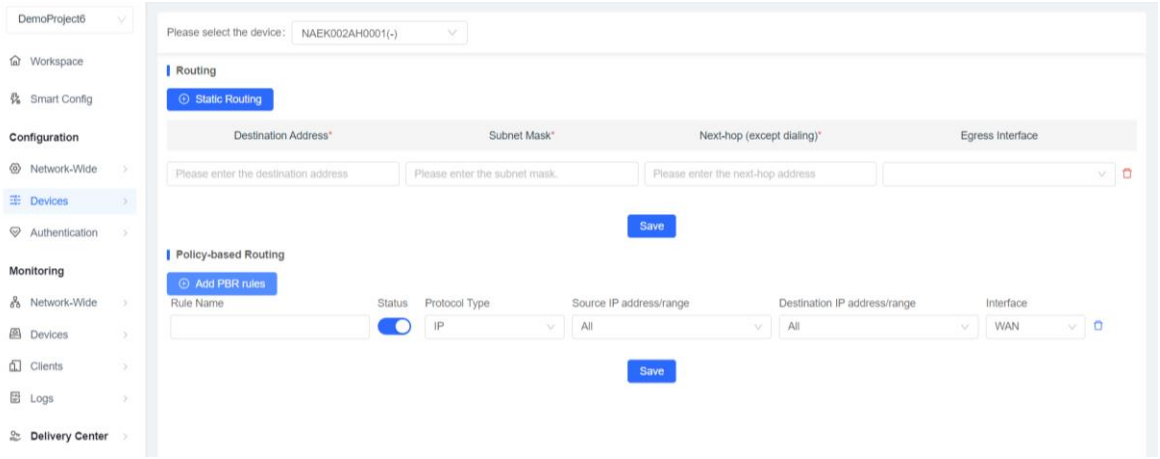
Static routes are manually configured. When a data packet matches a static route, the packet will be forwarded based on the specified forwarding mode.

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 > Switch > Routing, click Static Routing, click Save.



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.

9.3.2 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.

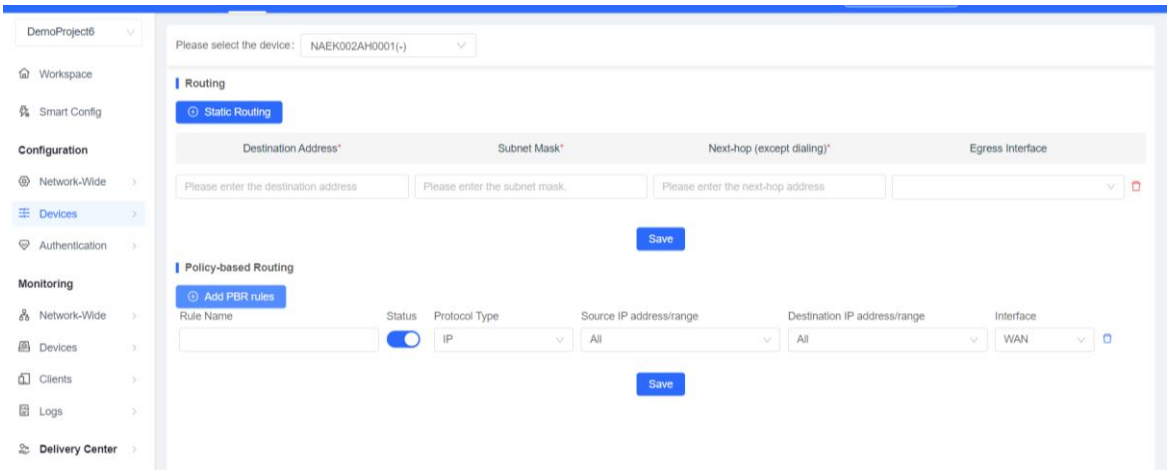
In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data 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 > Switch** > **Routing**, choose **Add PBR rules**, set parameters, and click **Save**.



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.
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.

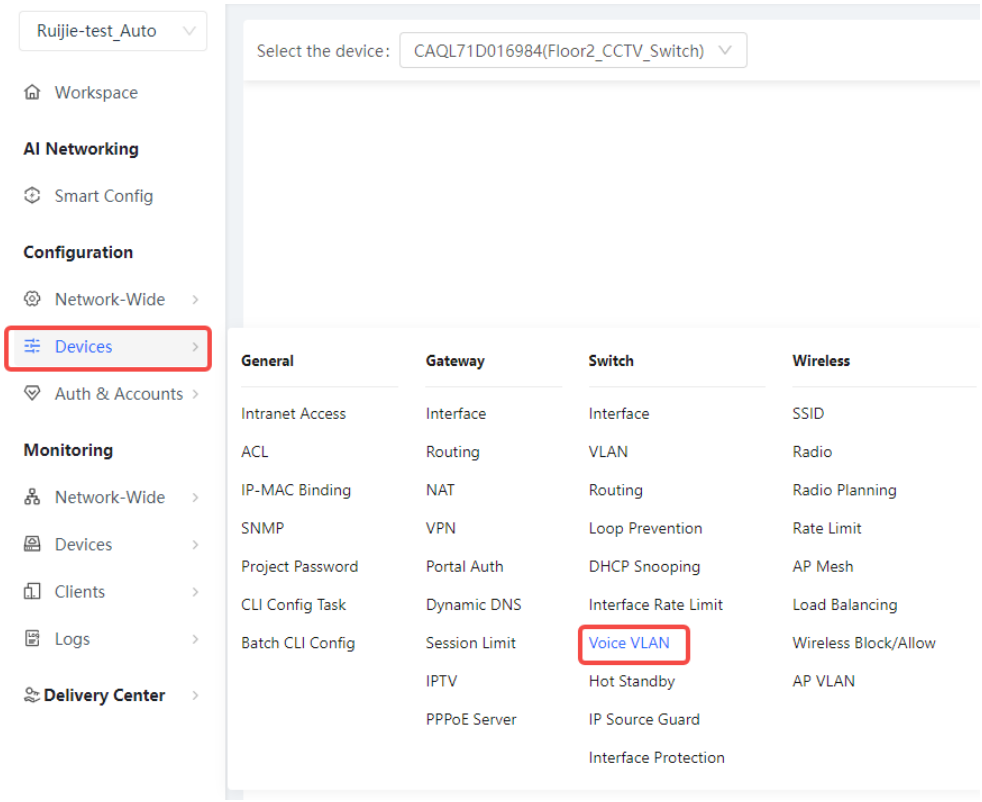
9.4 Voice VLAN

9.4.1 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.

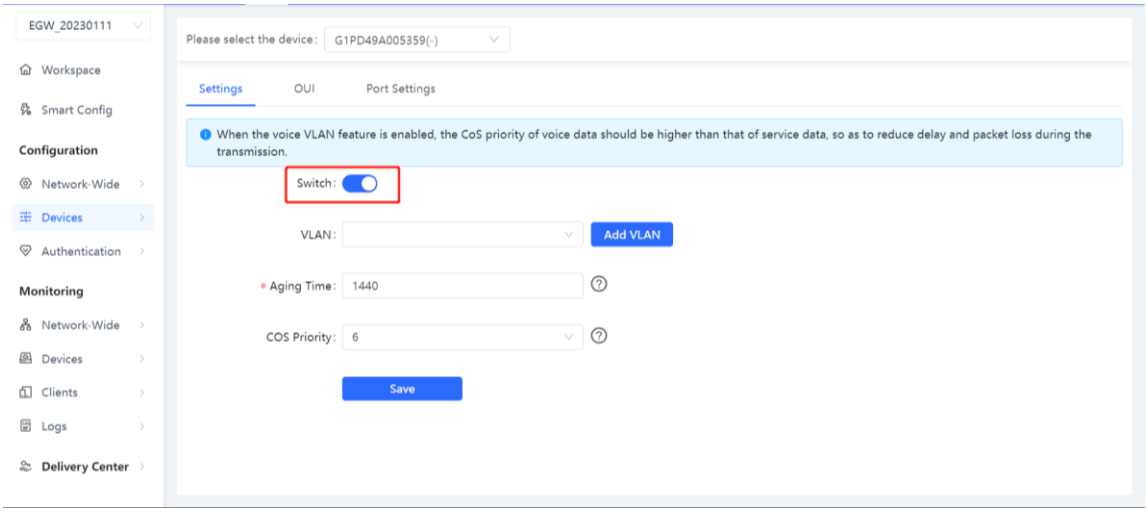
9.4.2 Configuration Steps

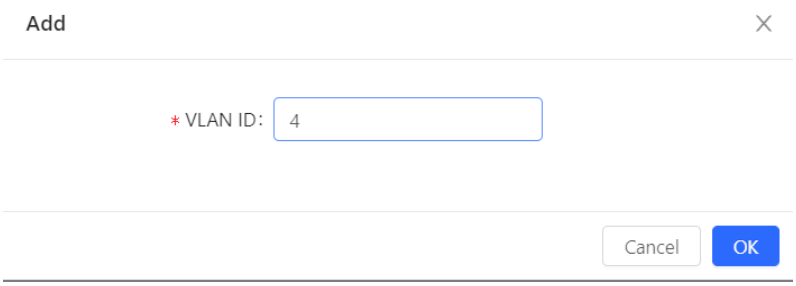
Choose Configuration > Devices > Switch > Voice VLAN.



1. Voice VLAN Settings

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

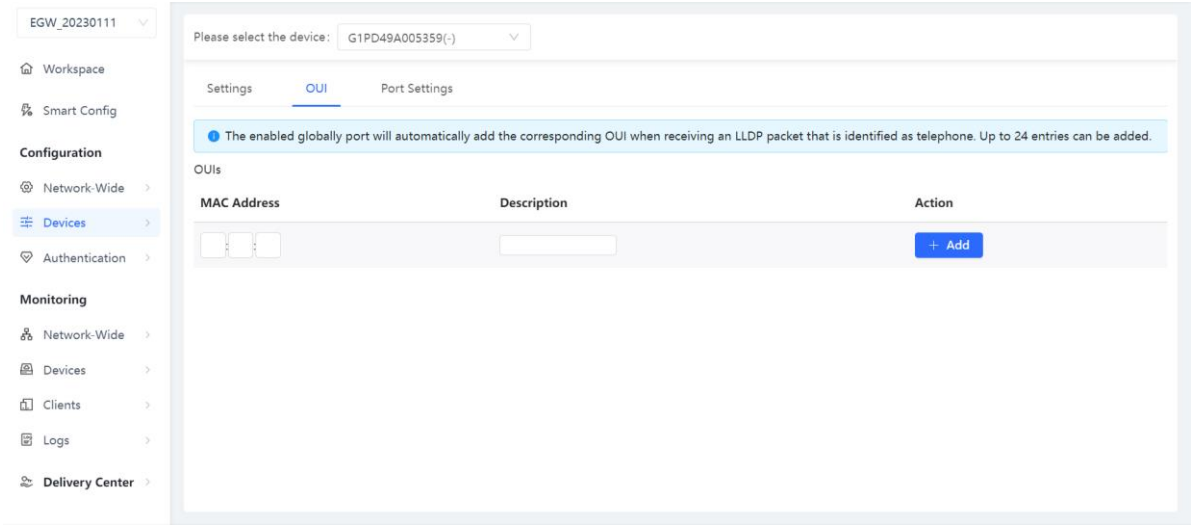


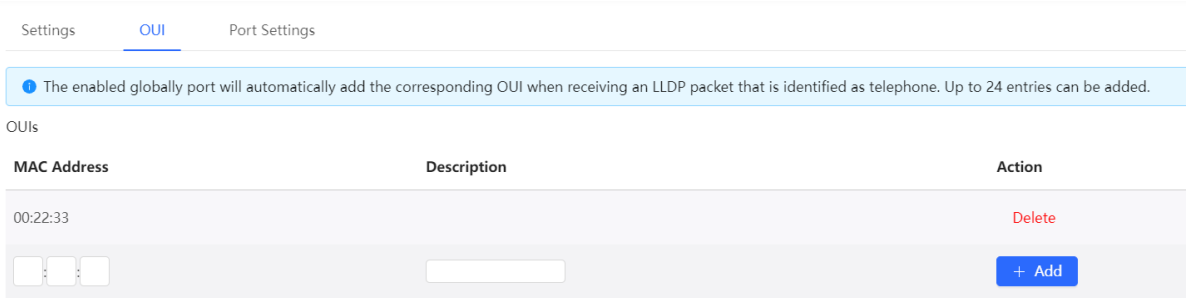


2. OUI Settings

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.





3. Port Settings

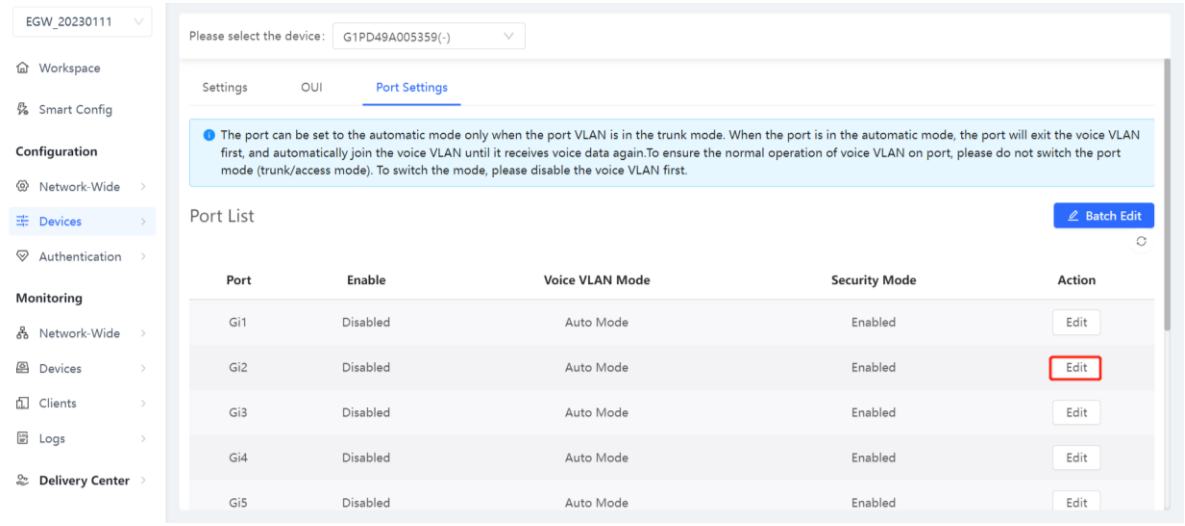
The port can be set to the automatic mode only when the port VLAN is in the trunk mode.

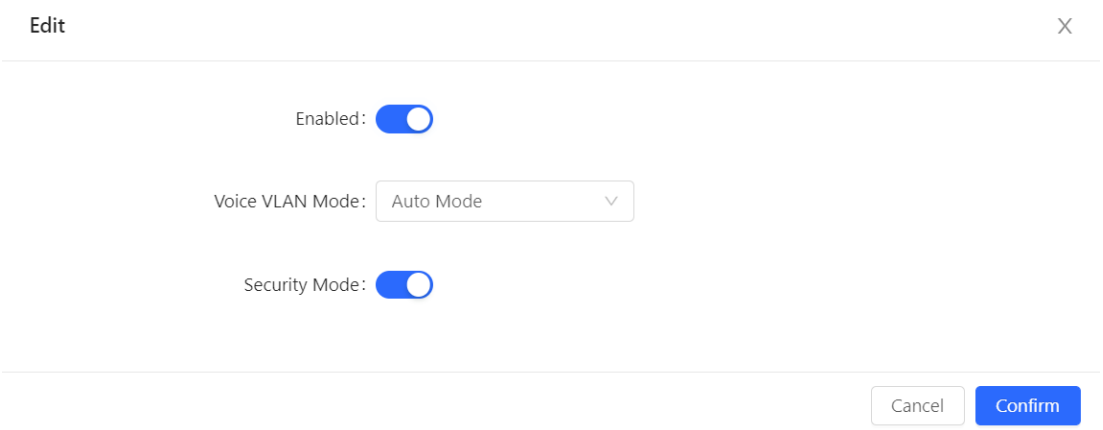
When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

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**.





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.

Limitations

The function is only supported on **Reyee APs**.

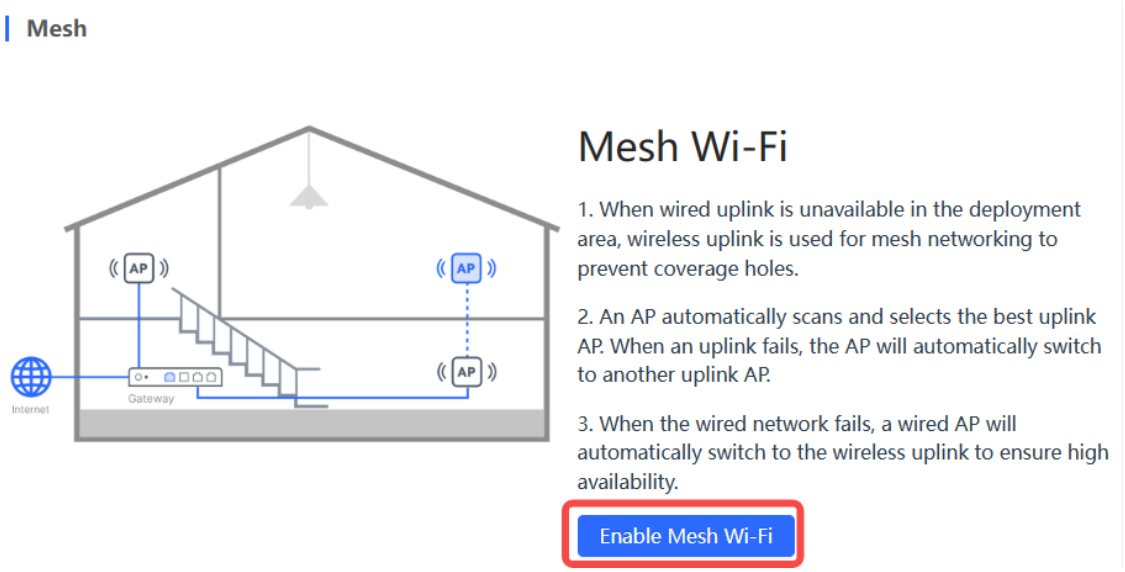
Configuration

(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**.

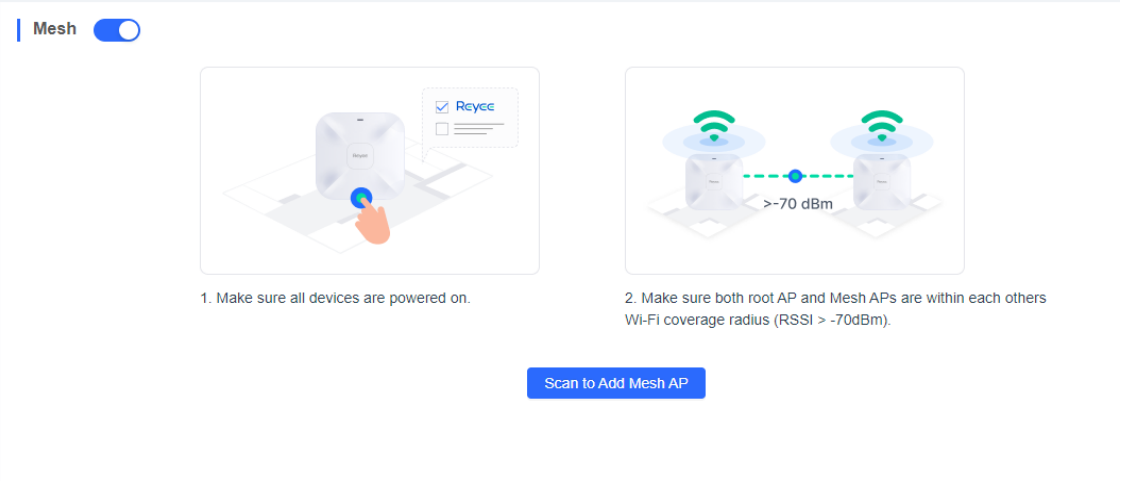


(5) Click **Scan to Add Mesh AP**.

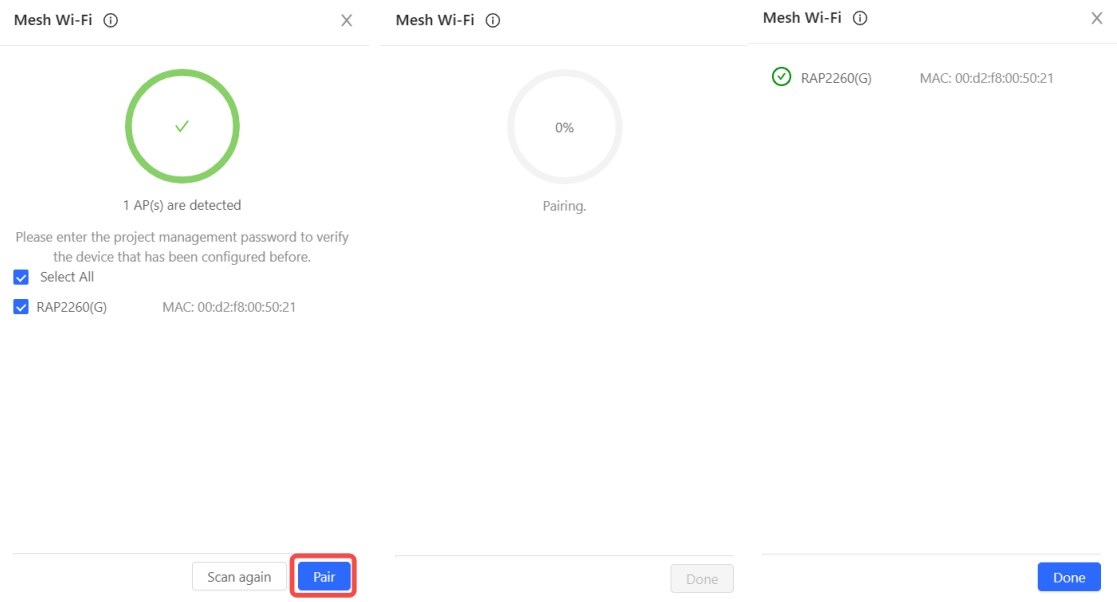
Caution

- 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.

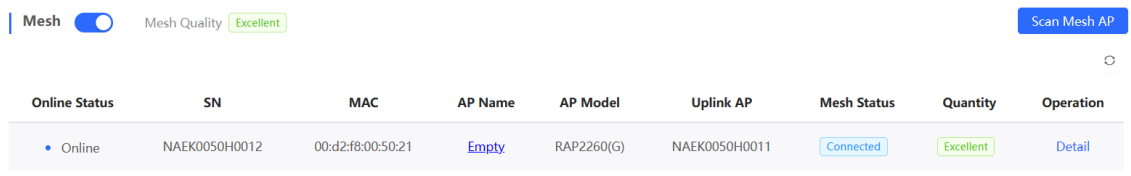
- The Mesh AP must be a Reyee AP.
- The AP is powered on.
- The distance between Root AP and Mesh AP should be less than 2 m.
- A provisioned AP is restored to factory defaults.



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



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

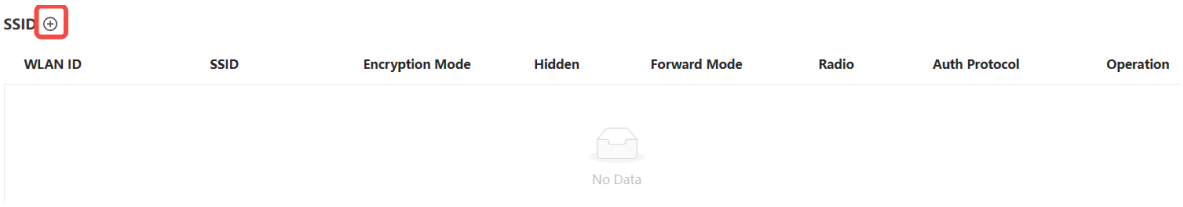


10.2 SSID

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.



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

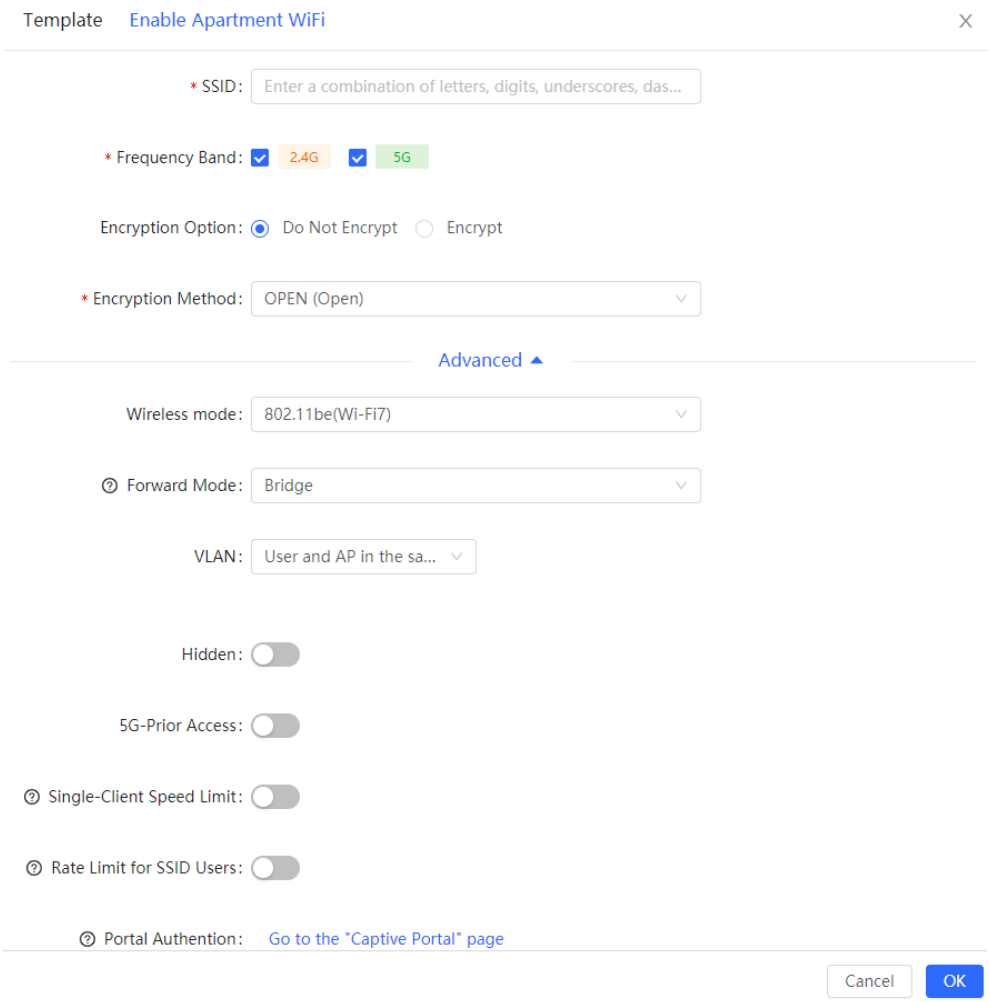
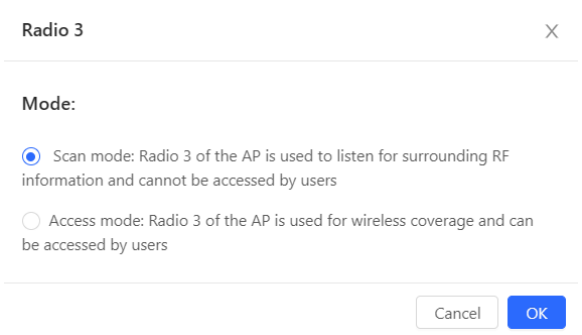
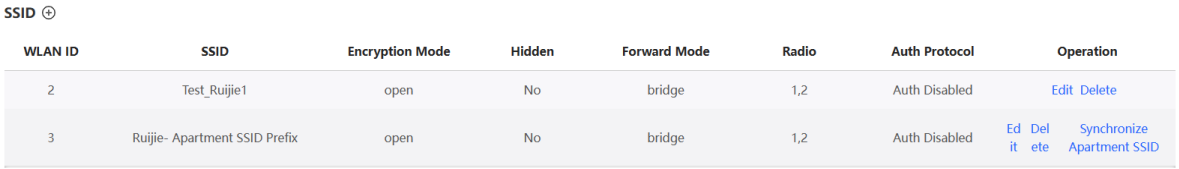


Table 10-1 Description of SSID Configuration Parameters

Parameter	Description
Enable Apartment Wi-Fi	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.
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**. 

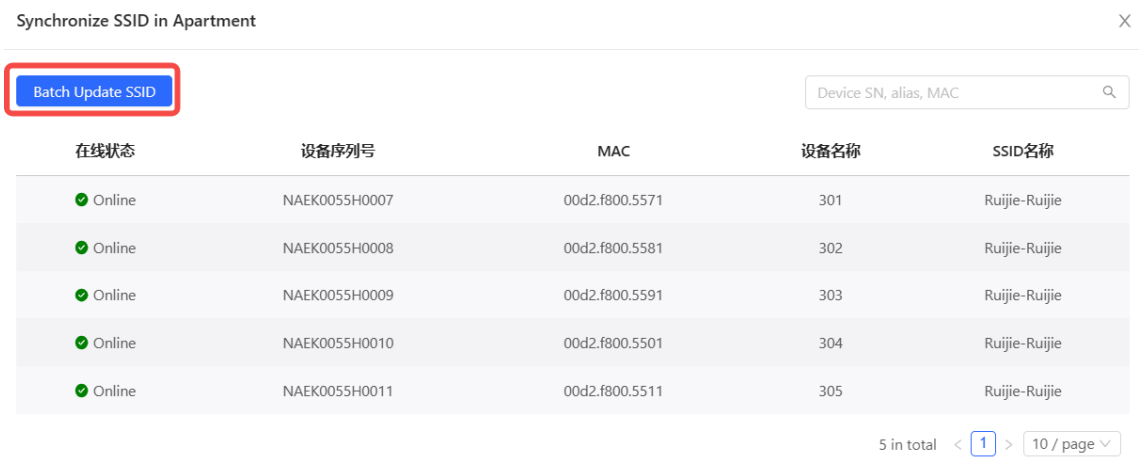
Parameter	Description
Enable Wi-Fi 6	Specify whether to enable **Wi-Fi 6**. On Reyee APs, **Wi-Fi 6** can be enabled based on the SSID. On RGOS APs, **Wi-Fi 6** can only be enabled based on the radio. After **Wi-Fi 6** is enabled, Wi-Fi 6 is applied to the radio corresponding to the SSID.
5G-Prior Access	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.



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.



1. Configuration Description of Forward Mode

Parameter Description

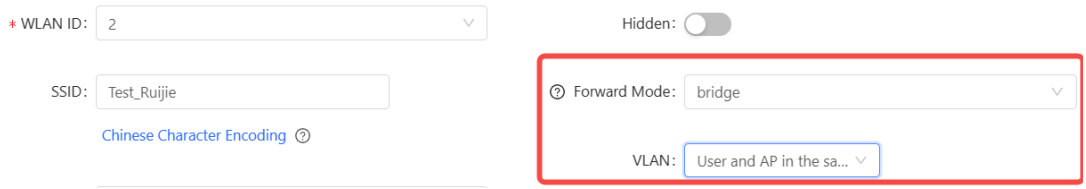
The following forwarding modes are supported: bridge, nat.

- 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.

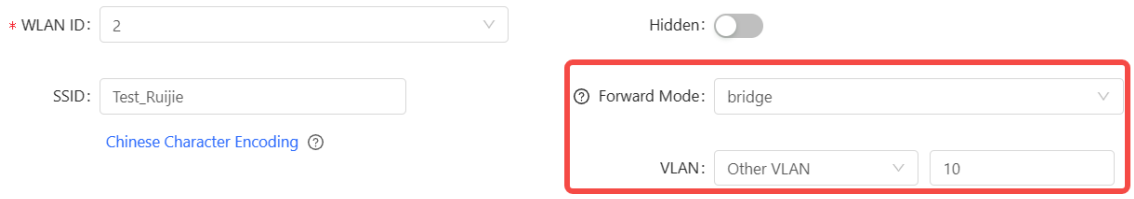
  If SSIDs in both NAT mode and Cloud NAT mode are configured, Ruijie Cloud will only deliver the Cloud NAT pool (that is, assign a pool to each device), but not the NAT pool.
- Bridge mode: An AP will function as a switch and allow all traffic to pass through. You need to specify the VLAN ID for users. 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

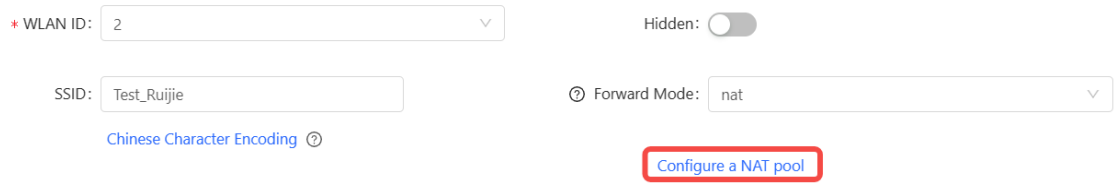
- **Forward Mode** is set to **bridge** and users and the AP are in the same VLAN.



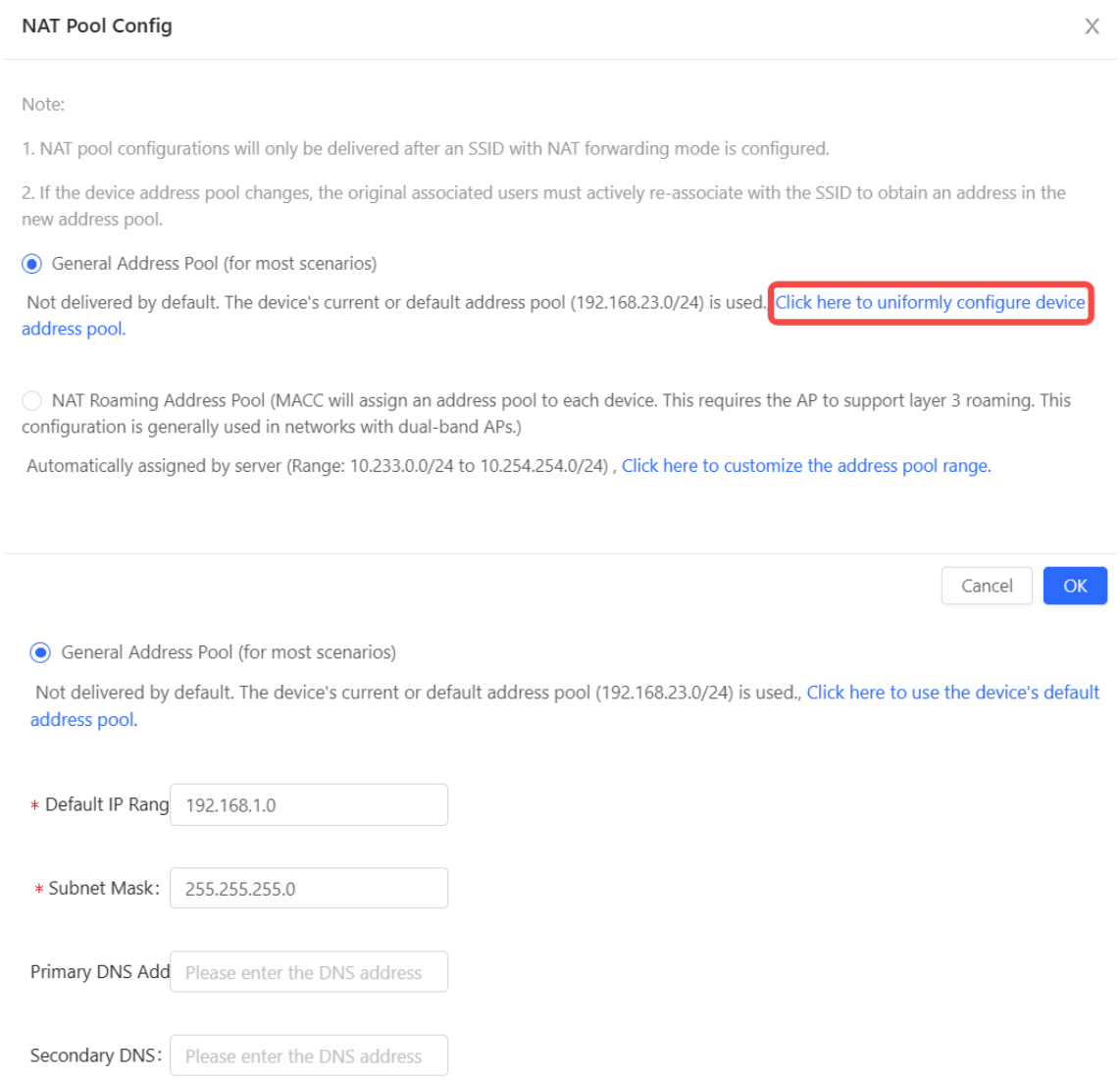
- **Forward Mode** is set to **bridge** and users and the AP are in different VLANs. The client connected to the SSID will seek the DHCP server with VLAN 10 on the network to obtain the address.



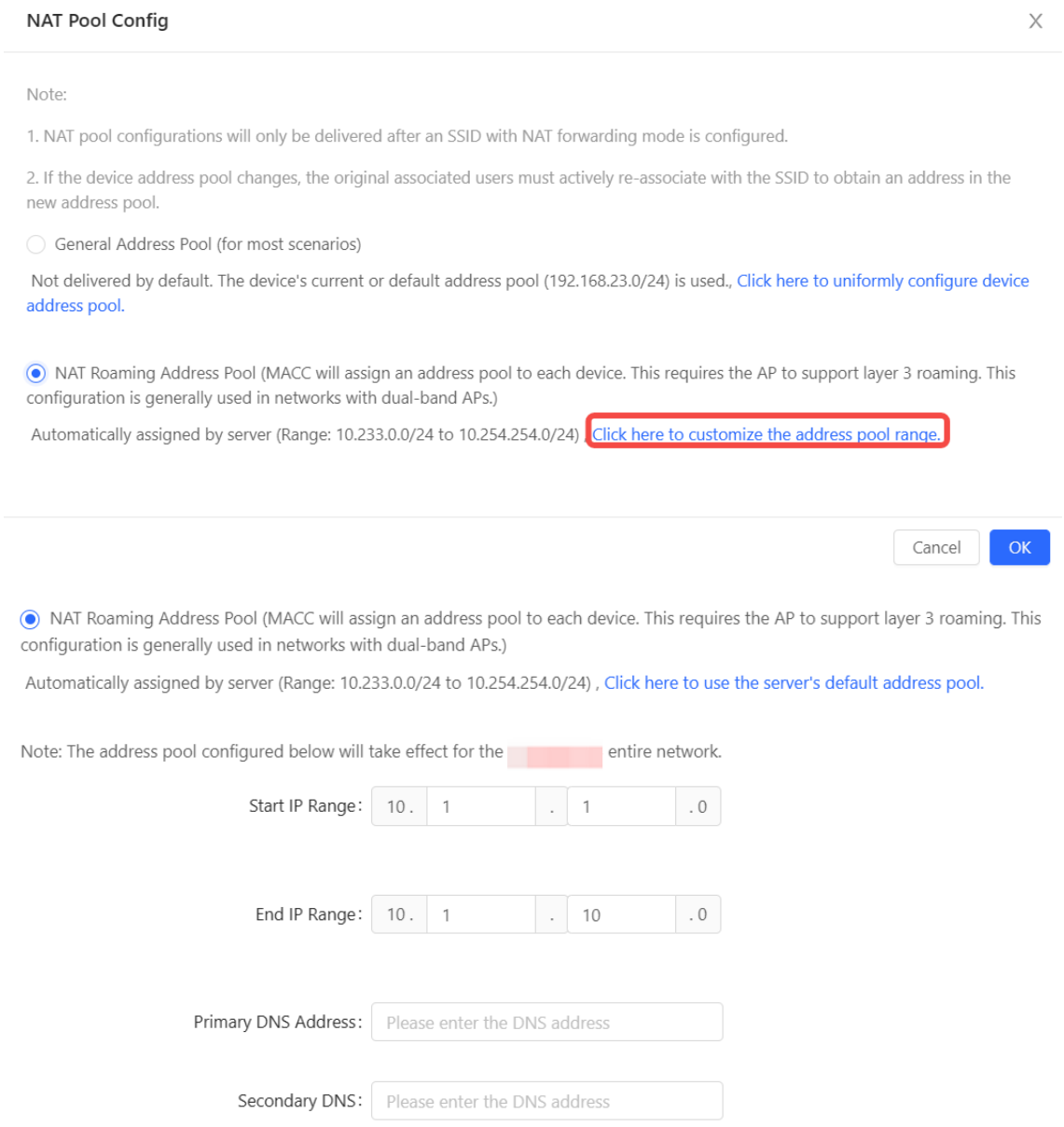
- When the NAT mode is configured, click **Configure a NAT Pool** to access the address pool configuration interface.



- 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**.



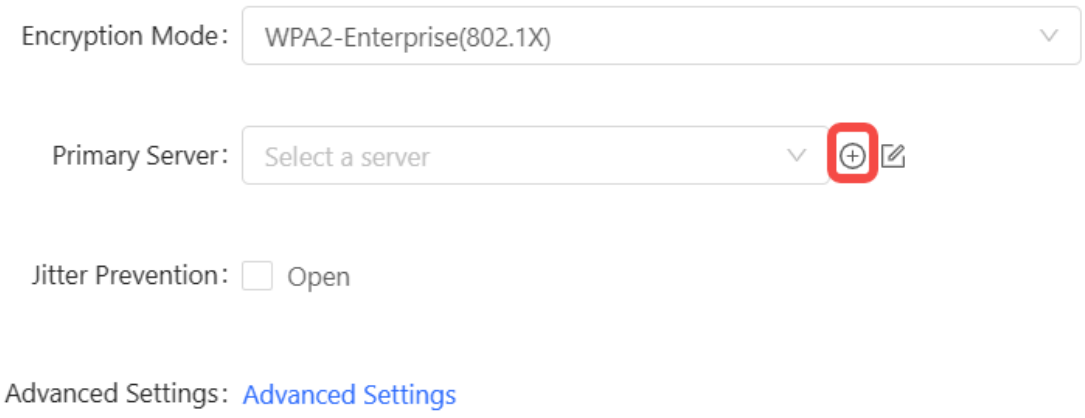
- When there are multiple APs on a network and Layer 3 roaming is enabled, select **NAT Roaming Address Pool** Mode and click **Click here to customize the address pool range.** to configure the address pool range. After configuration, click **OK**.



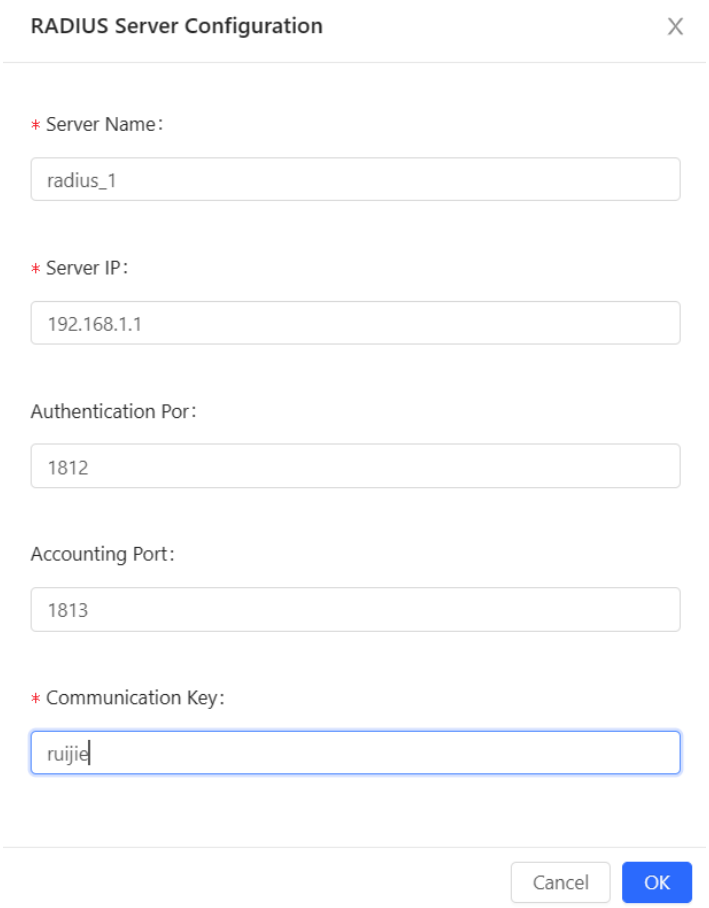
2. Configuration Description of Encryption Mode

- **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.

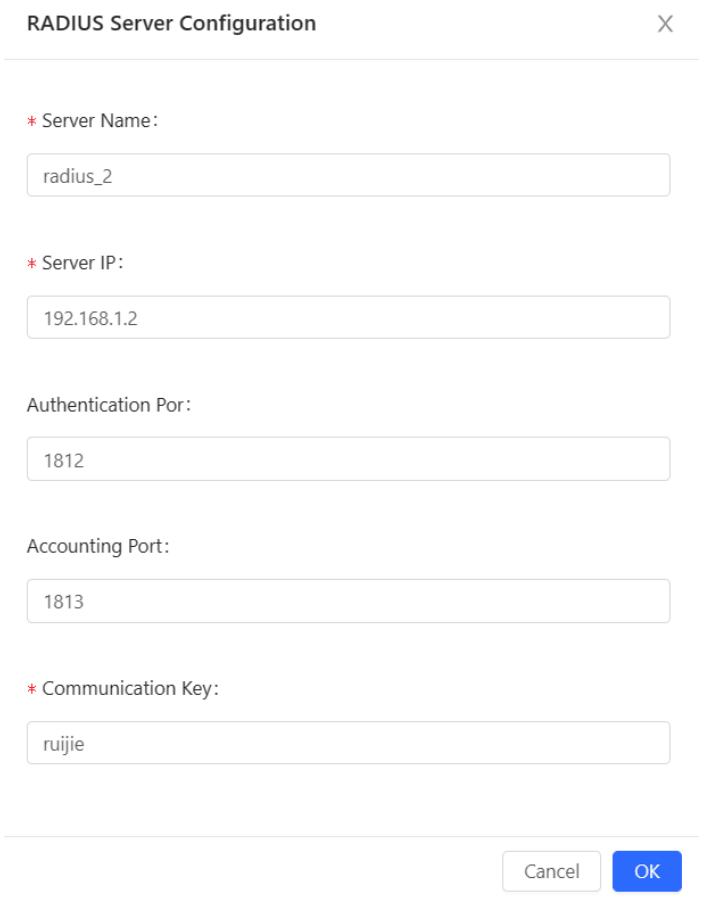
a Set **Encryption Mode** to **WPA2-Enterprise(802.1x)** and click ⊕ in the **Primary Server** line.



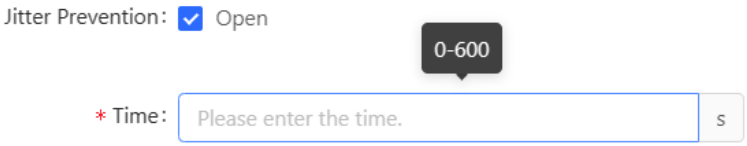
b Set parameters of the standby RADIUS server and click **OK**



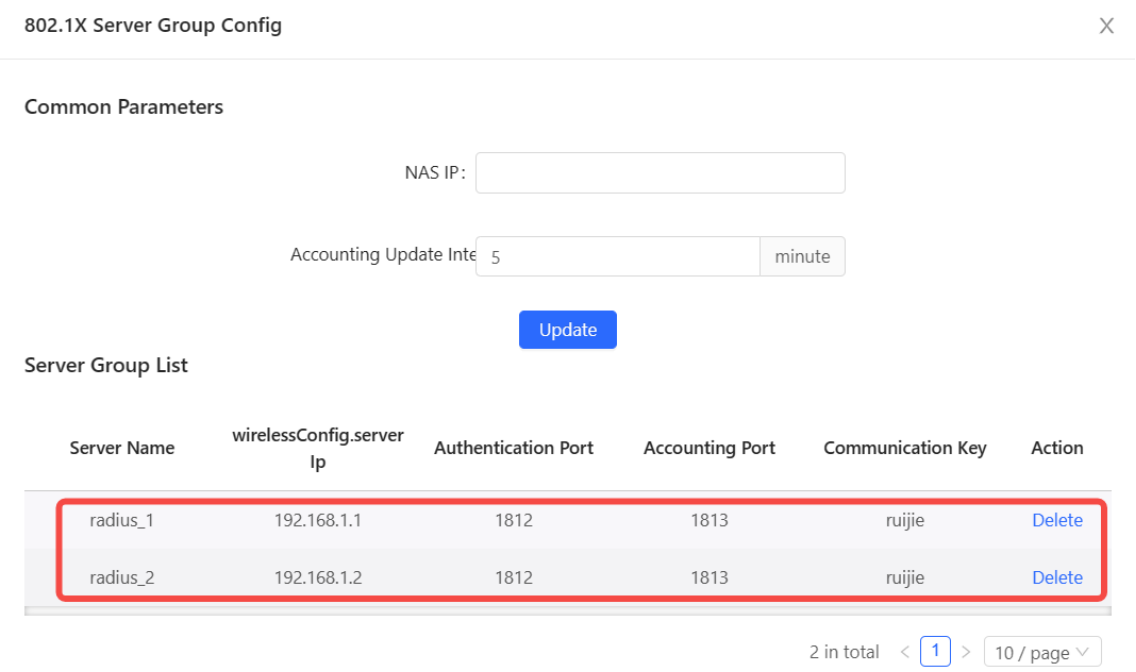
c If the standby RADIUS server exists, click ⊕ in the **Standby Server** line. Set parameters of the standby RADIUS server and click **OK**



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).



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



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.

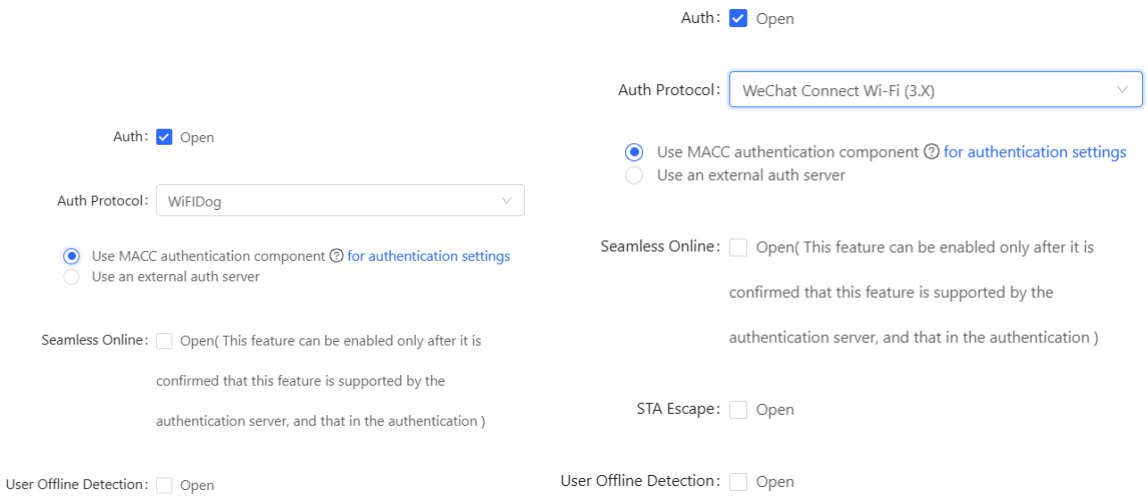


Table 10-2 Description of Authentication Configuration Parameters

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

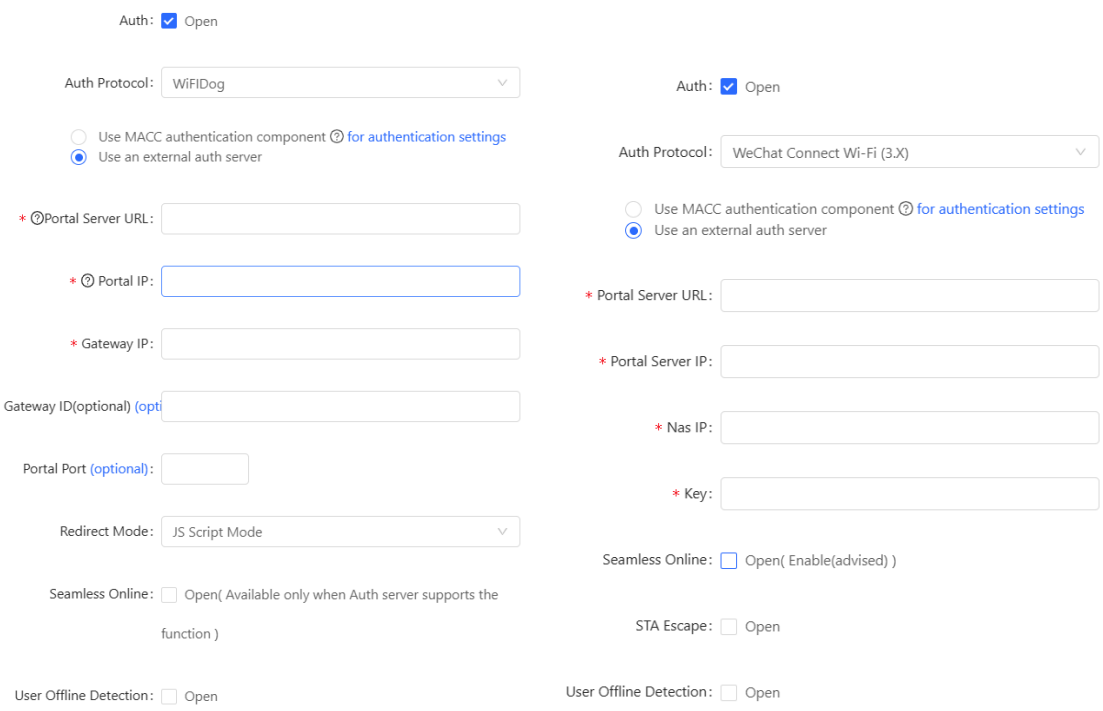


Table 10-3 Description of WiFiDog Authentication Configuration Parameters

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.

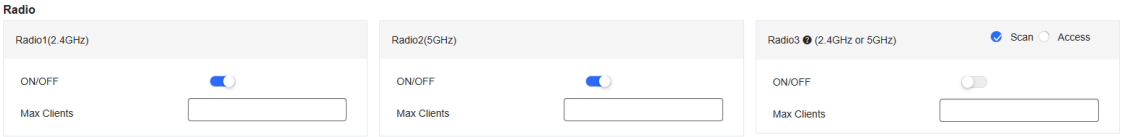
Table 10-4 Description of WeChat Connect Wi-Fi (3.X) Authentication Configuration Parameters

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.



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.

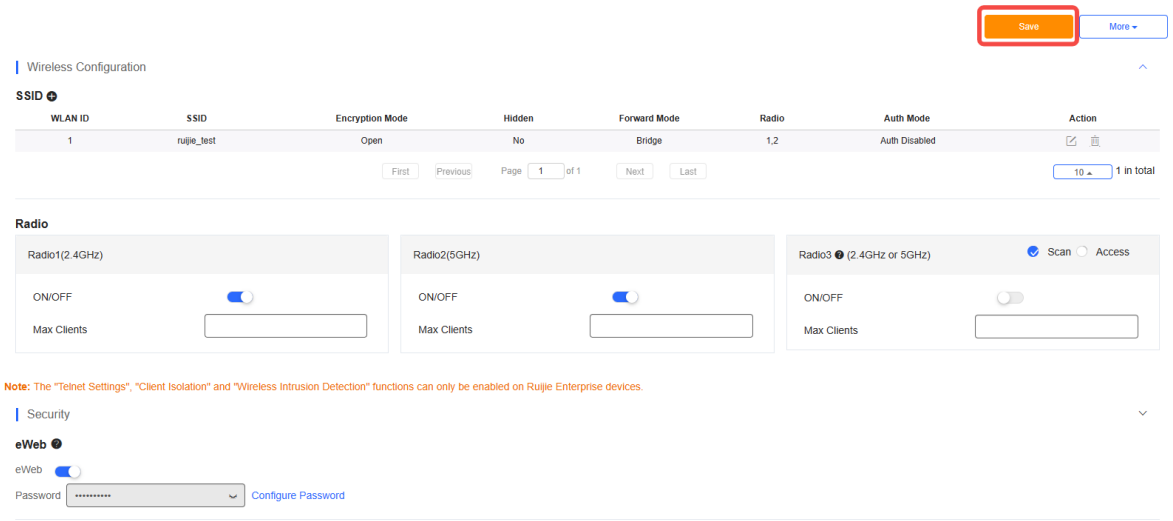
Max Clients: The maximum number of users set will take effect as the maximum number of users if it exceeds the maximum number of users actually supported by the AP; leave it blank to turn off the user limit.

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**.



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.

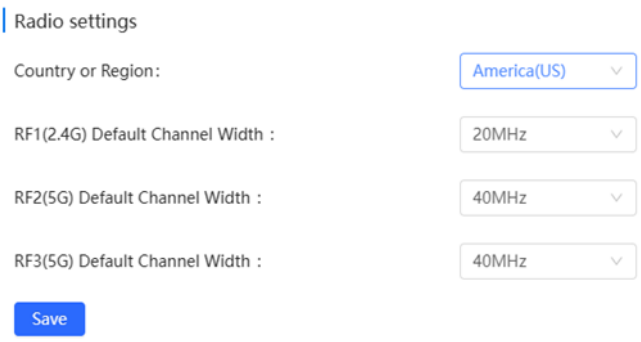
The best practice for user experience is 2.4 GHz in 20 MHz and 5 GHz in 40 MHz.

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**.



  Country or Region: Select a country code.

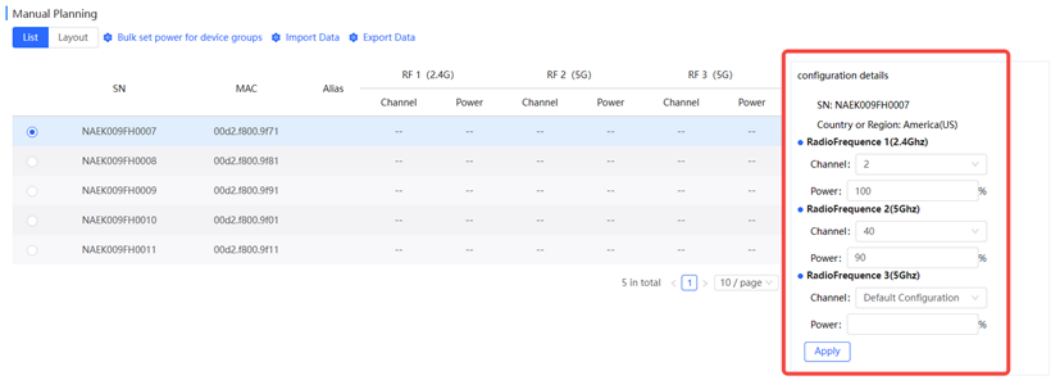
  RF1(2.4G) Default Channel Width: Configure the default channel width of RF1.

  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**.



SN: indicates the SN of an AP.

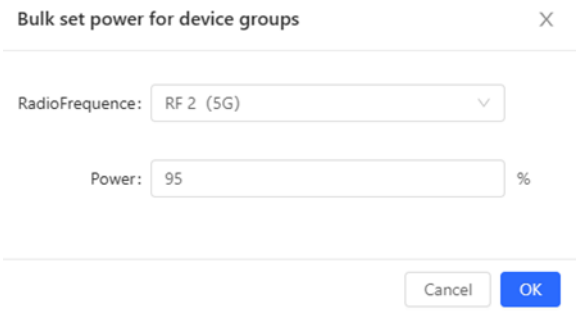
MAC: indicates the MAC address of an AP.

Device Name: indicates the AP name.

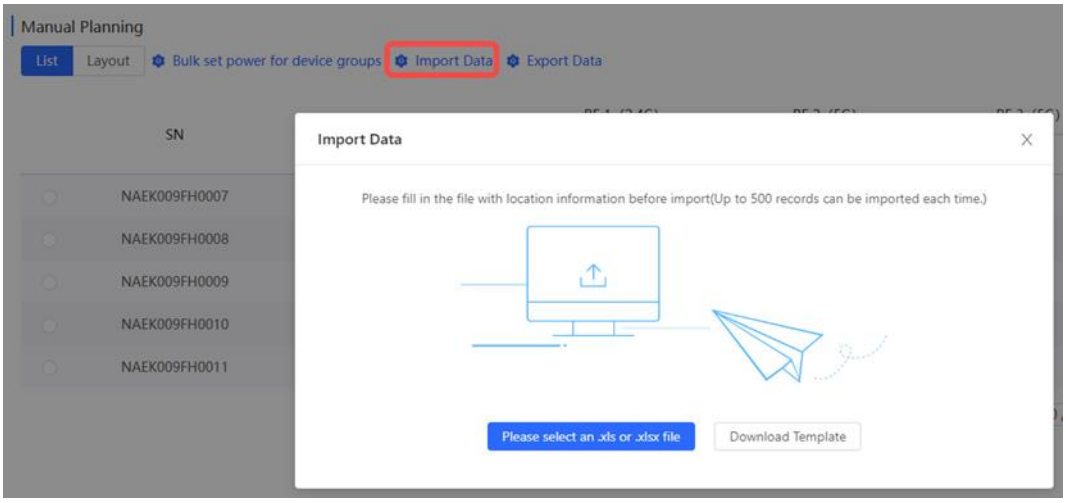
RadioFrequence > **Channel**: Check the current channel of radios.

RadioFrequence > **Power**: Check the local power of radios.

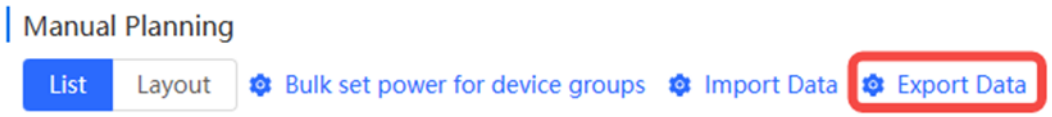
- Bulk configure devices (all devices) in a band: Click **Bulk set power for device groups**, select a band, and configure power. After configuration, click **OK**.



- Bulk 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.



- Export current configuration: Click **Export Data** to export configuration data to an .xlsx file.



10.4 Rate Limit

10.4.1 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**.

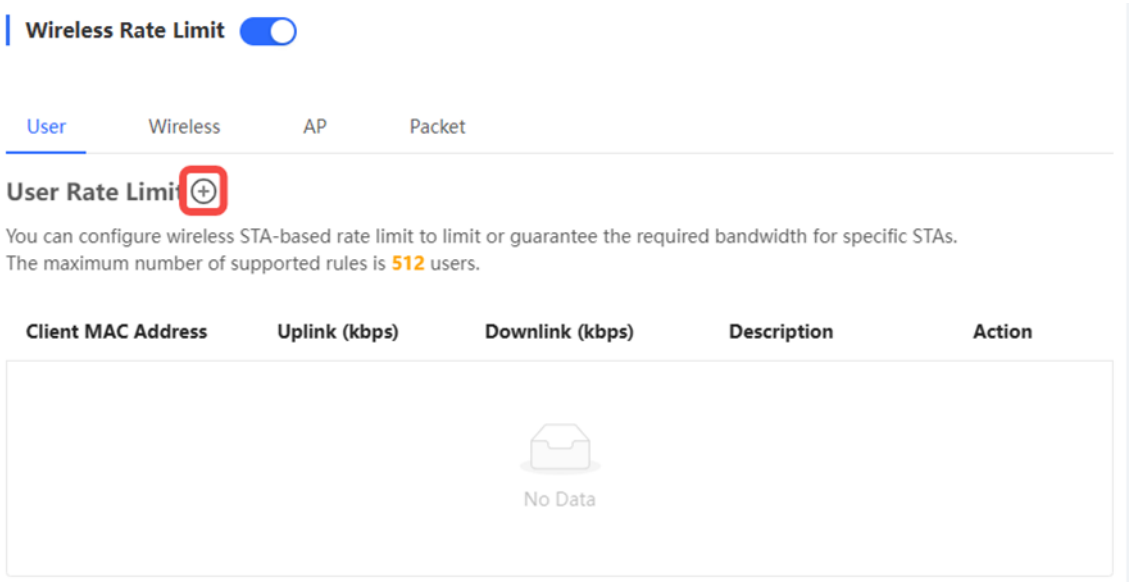
- User Rate Limit: You can configure wireless STA-based rate limit to limit or guarantee the required bandwidth for specific STAs. The maximum number of supported rules is 512 users.
- Wireless Rate Limit: You can configure per-user rate limit, dynamic rate limit, and other functions for designated SSIDs.
  - 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.

10.4.2 User Rate Limit

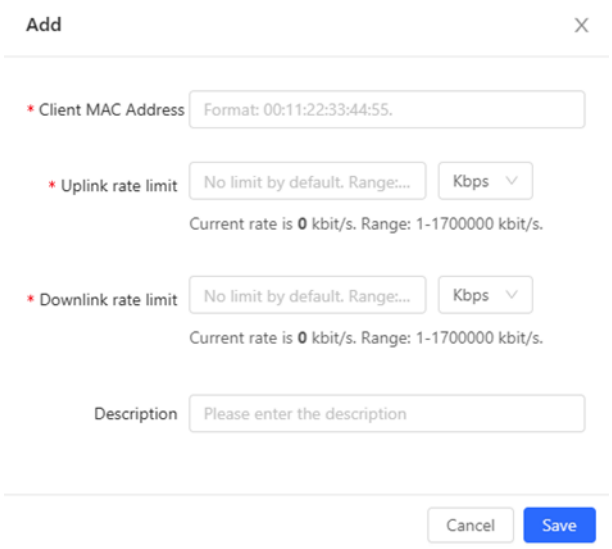
(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Rate Limit**, and select a network in this account.

(2) Confirm that **Wireless Rate Limit** (enabled by default) is enabled.

(3) On the **User** tab, click ⊕ to go to the configuration page.



(4) Configure the MAC address of the client whose rate needs to be limited and the rate limit value. After configuration, click **Save**.

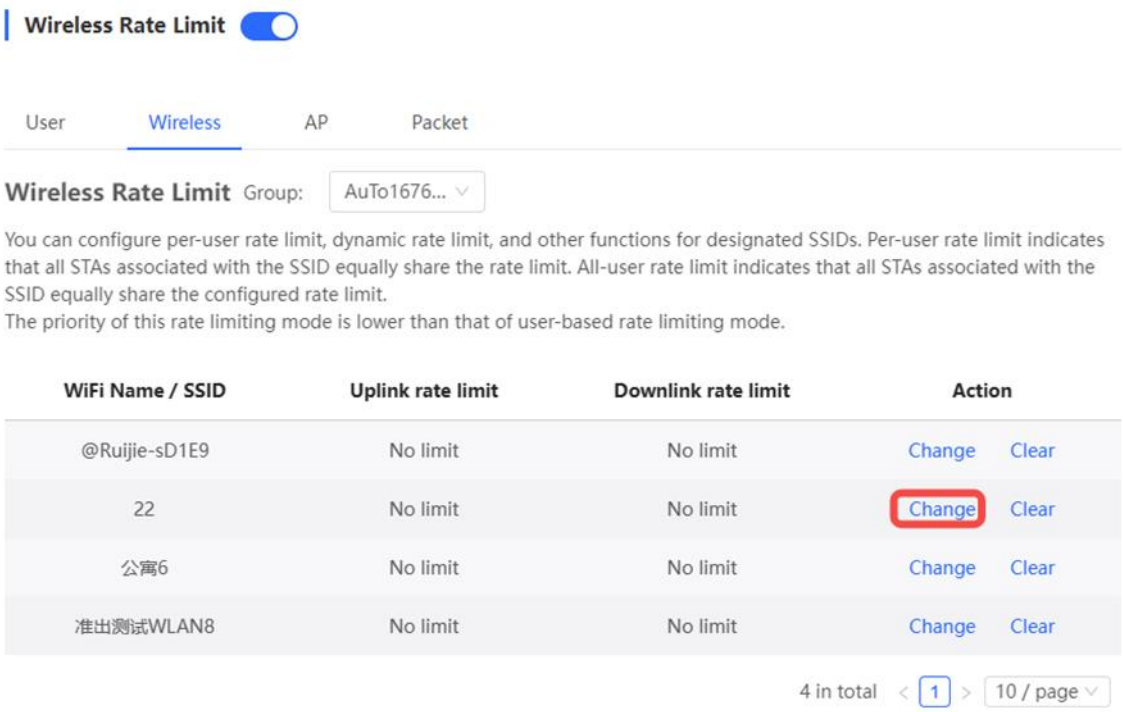


10.4.3 Wireless Rate Limit

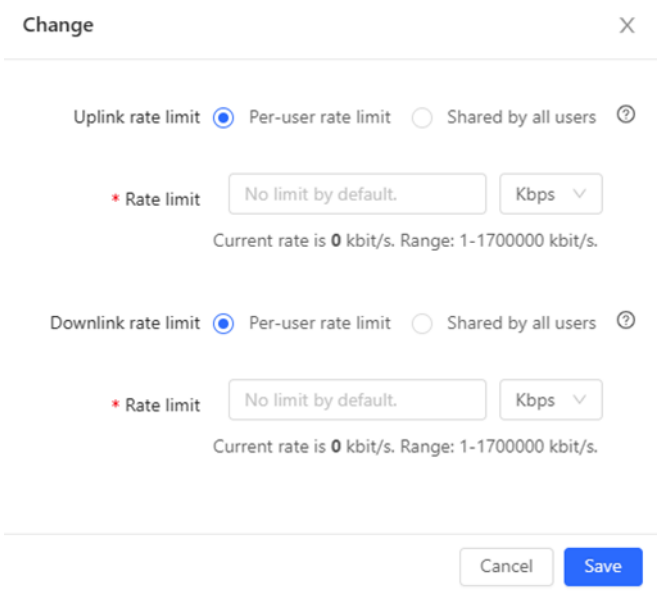
(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Rate Limit**, and select a network in this account.

(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.



(4) Configure the rate limit modes for the uplink and downlink directions and rate limit values. After configuration, click **Save**.

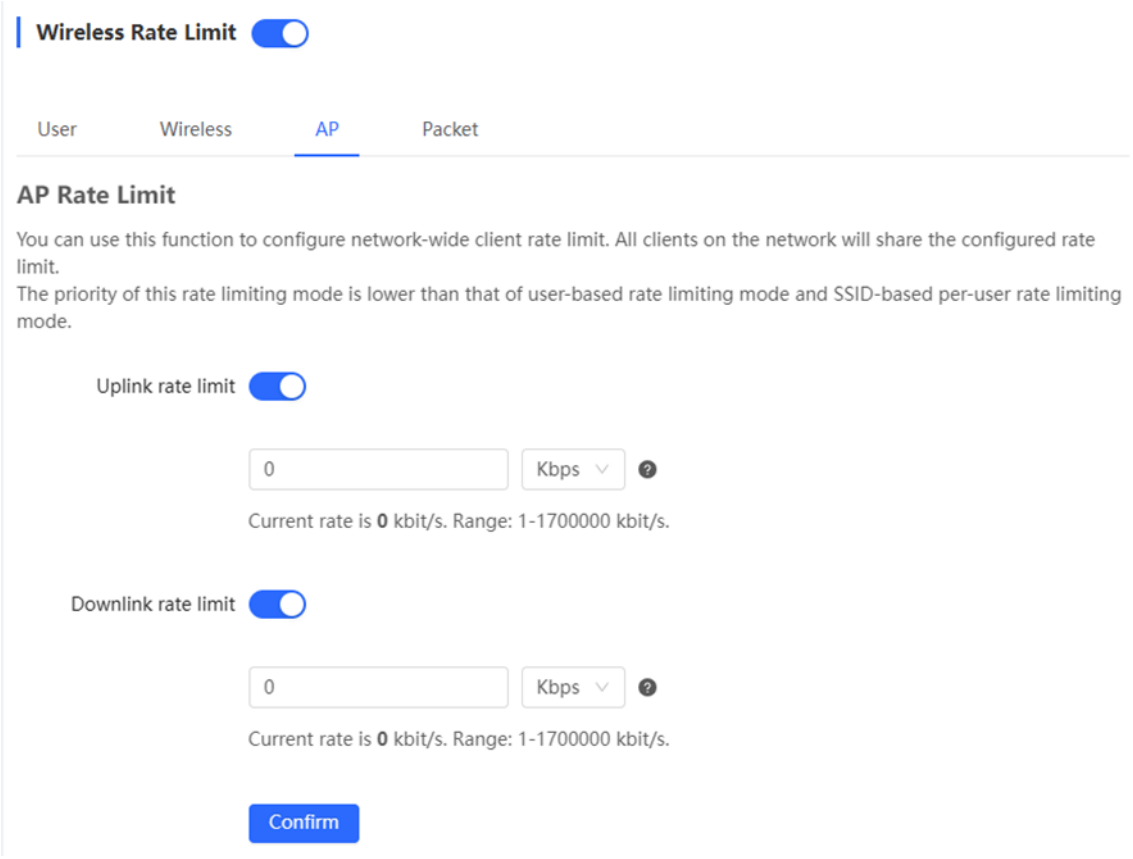


10.4.4 AP Rate Limit

(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**.

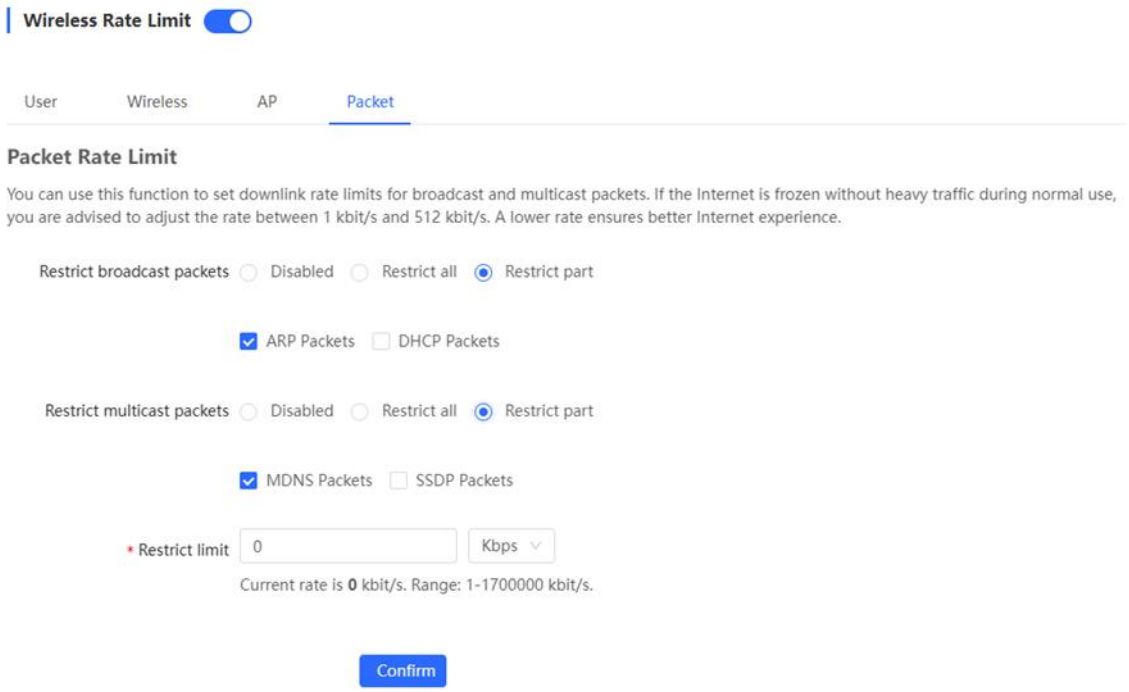


10.4.5 Packet Rate Limit

(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**.



10.5 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.

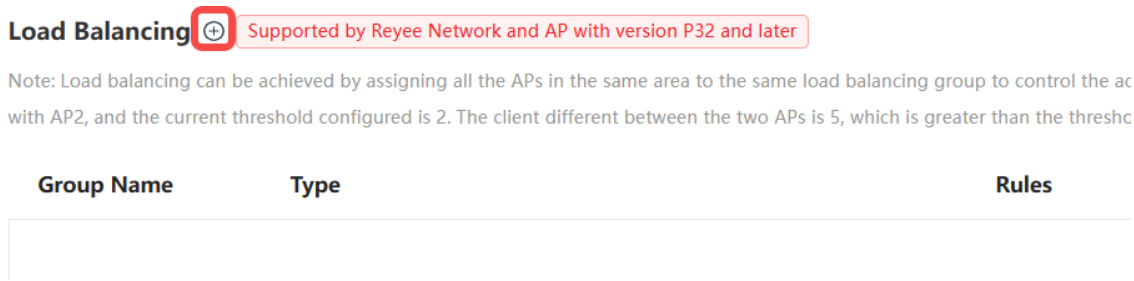
Limitations

Load balancing is only supported by Reyee Network and AP with P32 or a higher version, and there must be a Reyee EG on the network.

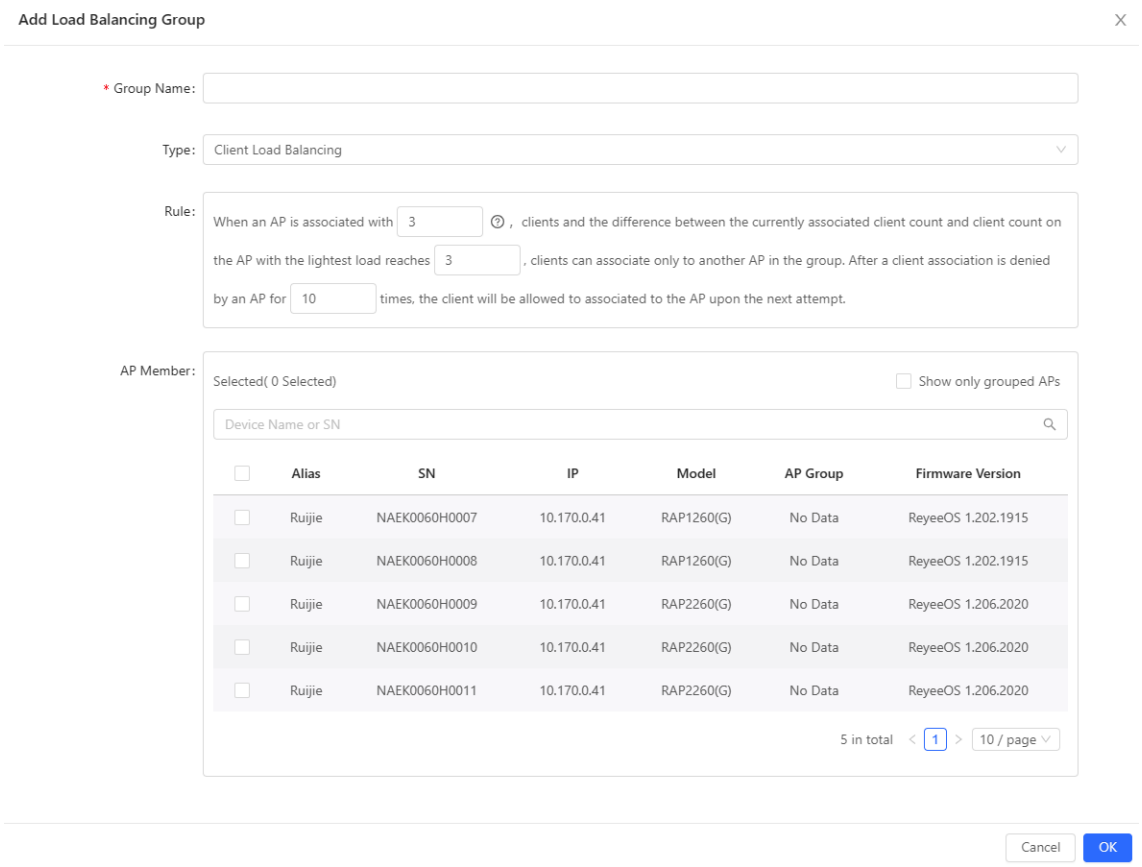
Procedure

(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.



(3) Configure parameters for the load balancing group, including **Group Name**, **Type**, **Rule**, and **AP Member**. After configuration, click **OK**.



Group Name: indicates the load balance group name.

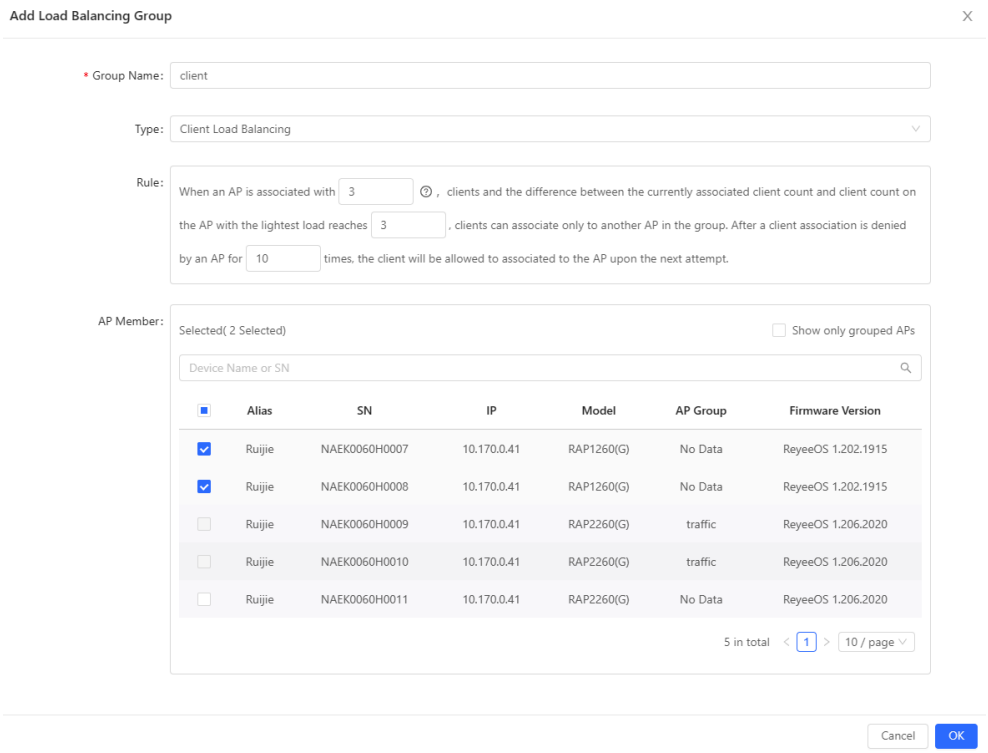
Type: indicates the type of load balancing (client or traffic).

Rule: indicates the rule of load balancing group.

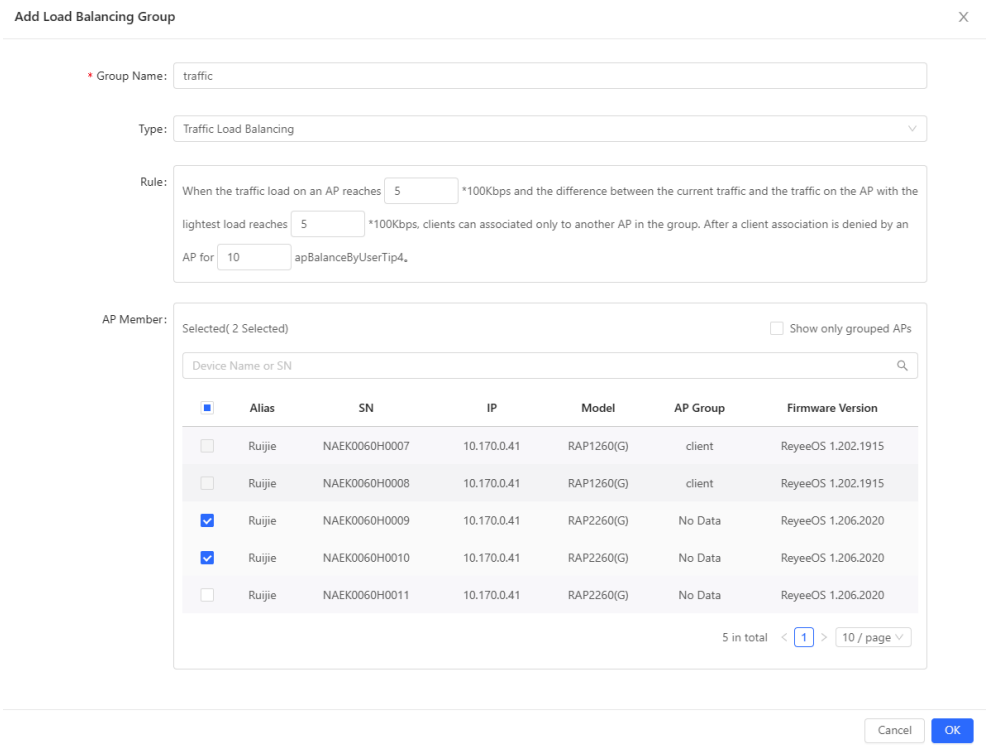
AP Member: indicates the AP added to the group.

Implementation of client and traffic load balancing are as follows:

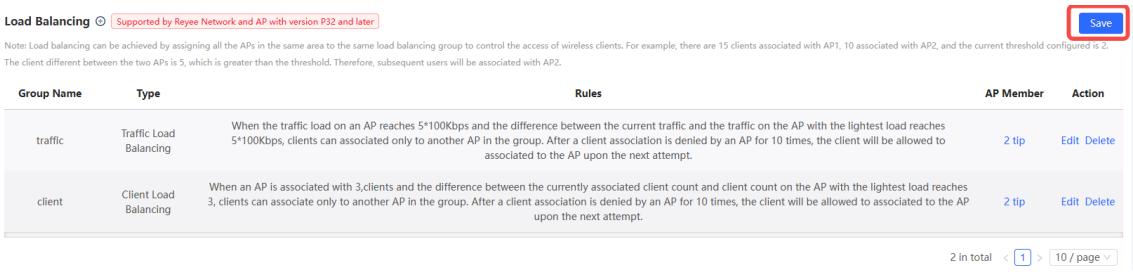
- **Client Load Balancing:** When an AP is associated with *n* clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches *n*, clients can be associated only with another AP in the group. After a client association is denied by an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



- **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.



(4) After configuring the load balancing group, click **Save** at the upper right corner of the **Load Balancing** 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.

10.6 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.

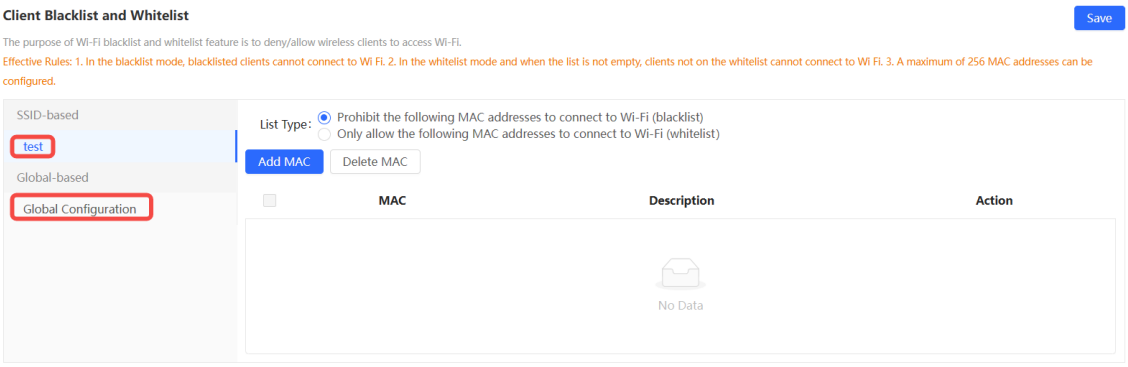
Caution

- The function is only supported on **Reyee APs**.
- 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.

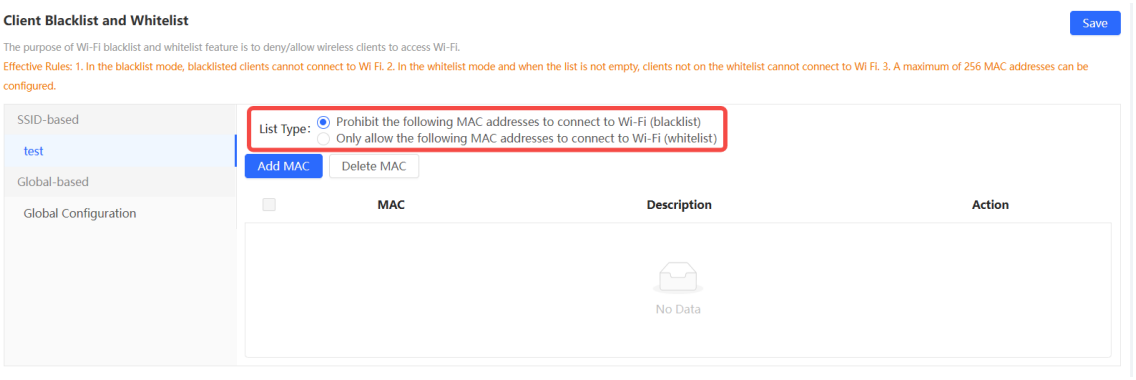
Configuration Steps

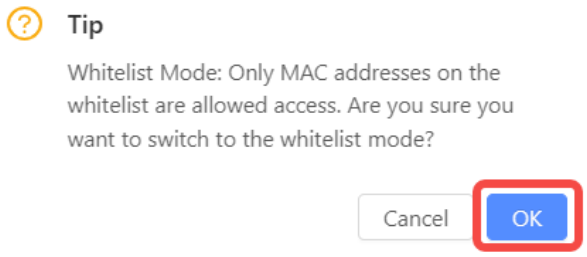
(1) Log in to Ruijie Cloud, choose **Project** > **Configuration** > **Devices** > **Wireless** > **Wireless Block/Allow**, and select a network in this account.

(2) Select the scope (**SSID-based** or **Global-based**), in which the blocklist or allowlist takes effect, in the list on the left.

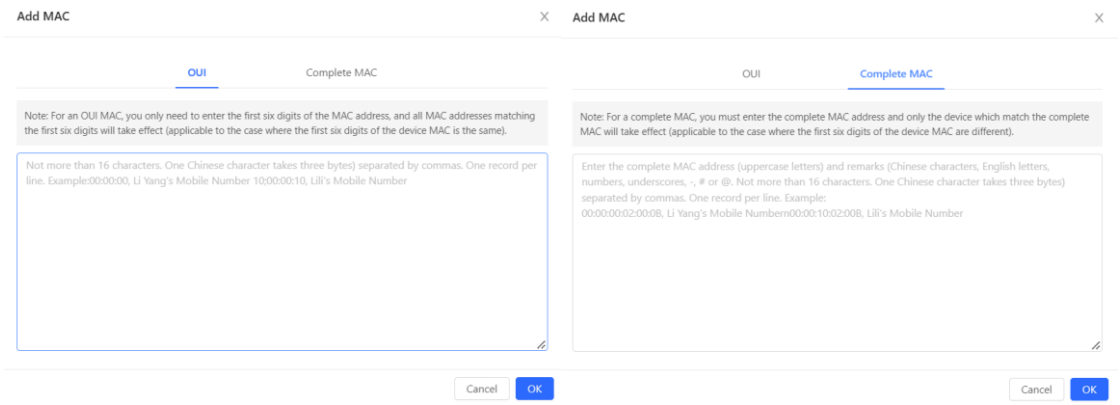


(3) Select the blocklist/allowlist mode. The default mode is blocklist mode. When you switch the mode, click **OK** in the pop-up prompt box to make the mode take effect.



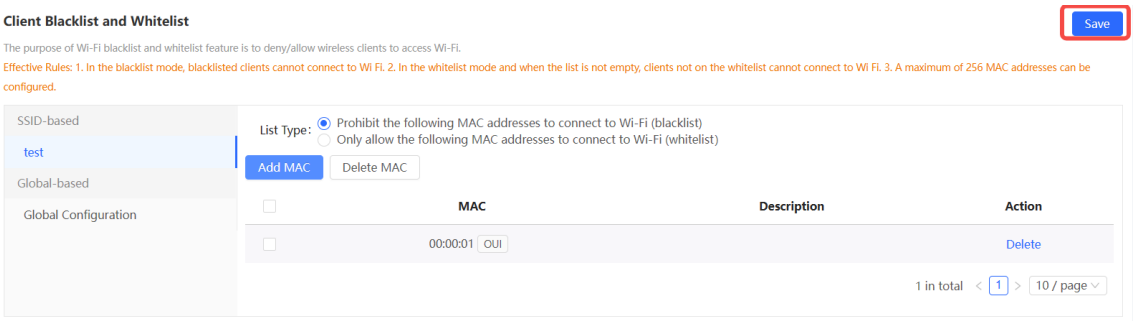


(4) Click **Add MAC**. On the **Add MAC** page, add MAC address prefixes or MAC addresses. After adding, click **OK**.

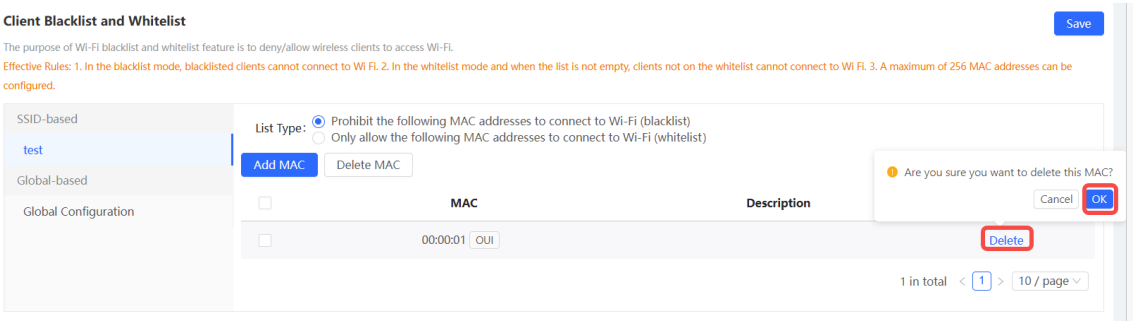


- OUI: For an OUI MAC, you only need to enter the first six digits of the MAC address, and all MAC addresses matching the first six digits will take effect (applicable to the case where the first six digits of the device MAC is the same).
- Complete MAC: For a complete MAC, you must enter the complete 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.



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.



10.7 AP VLAN

Overview

This feature can be used to deliver the port VLAN configuration to multiple designated devices.

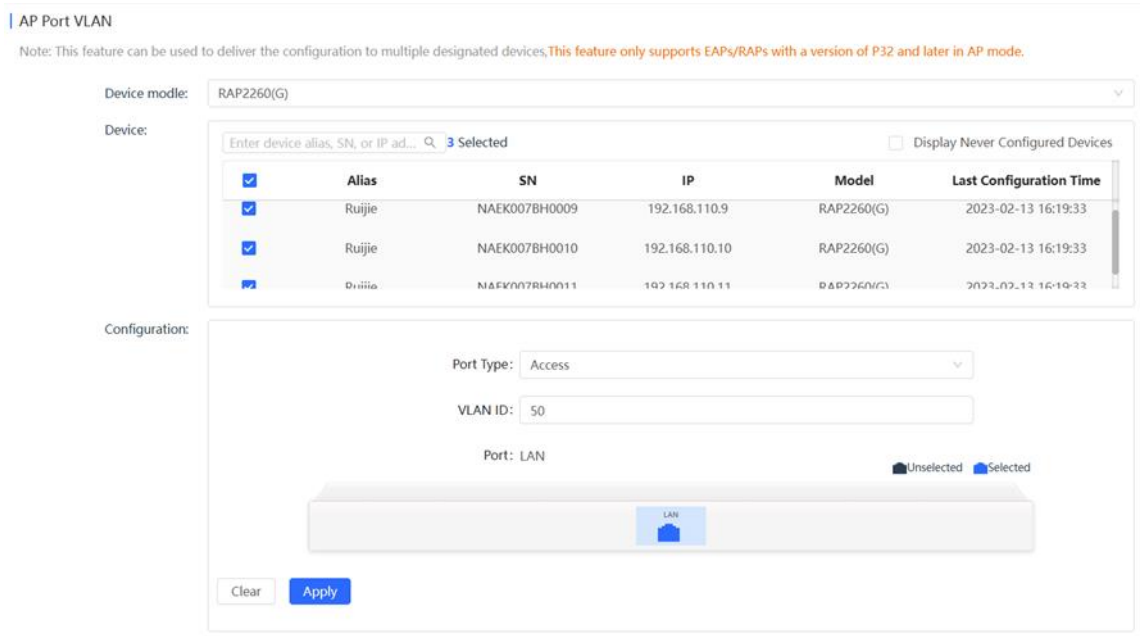
Limitations

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.



Device Model: indicates the AP model.

Device: indicates the device to which the configuration needs to be delivered.

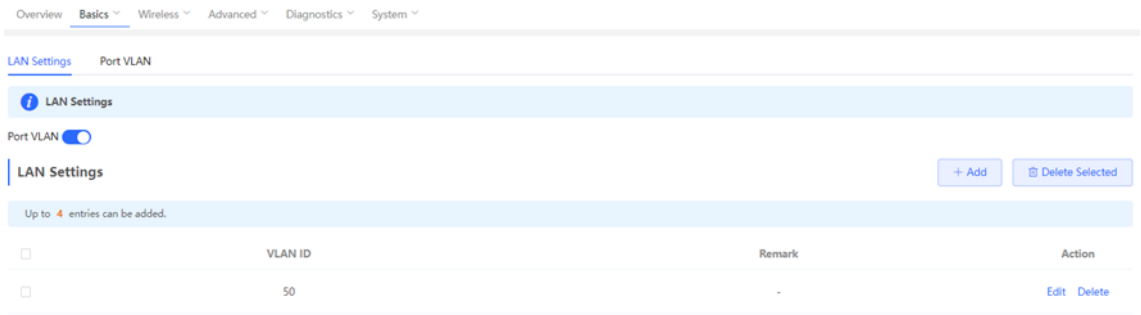
Port Type: indicates the port type, which is access or trunk.

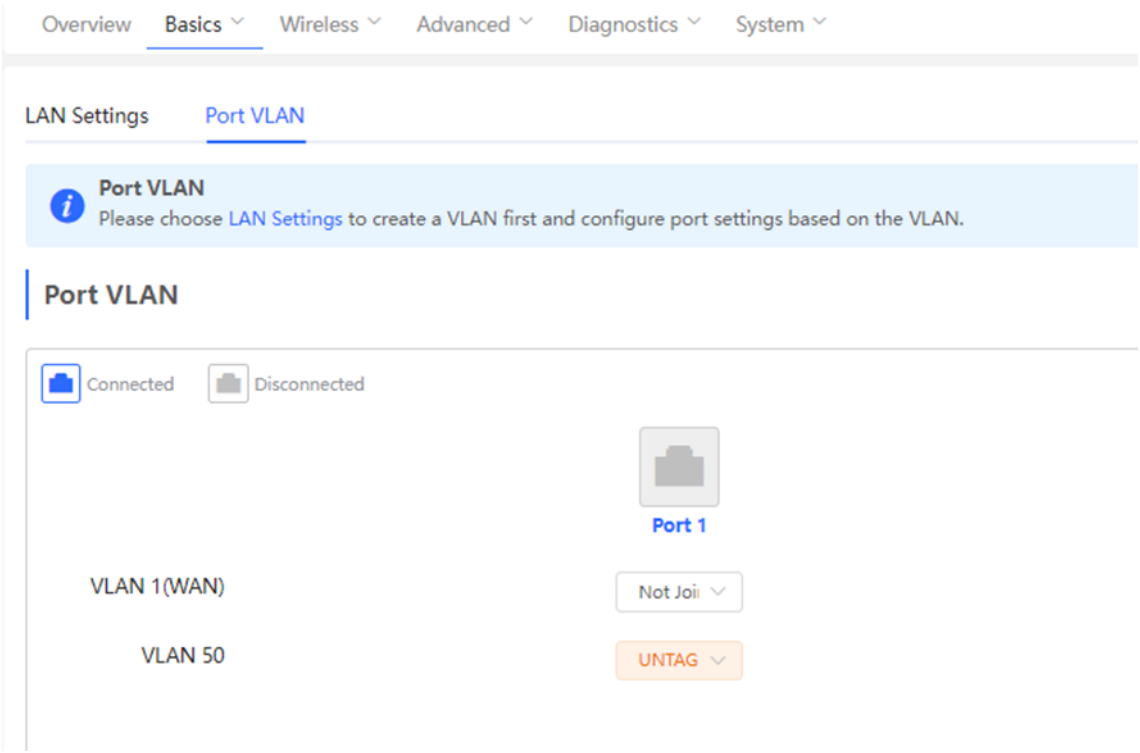
VLAN ID: indicates the VLAN ID of a port.

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.




Overview
Basics
Wireless
Advanced
Diagnostics
System
LAN Settings
Port VLAN
Port VLAN
Please choose LAN Settings to create a VLAN first and configure port settings based on the VLAN.
Port VLAN
Connected
Disconnected
Port 1
VLAN 1(WAN)
Not Joi
VLAN 50
UNTAG

11 Authentication Configuration

11.1 Captive Portal

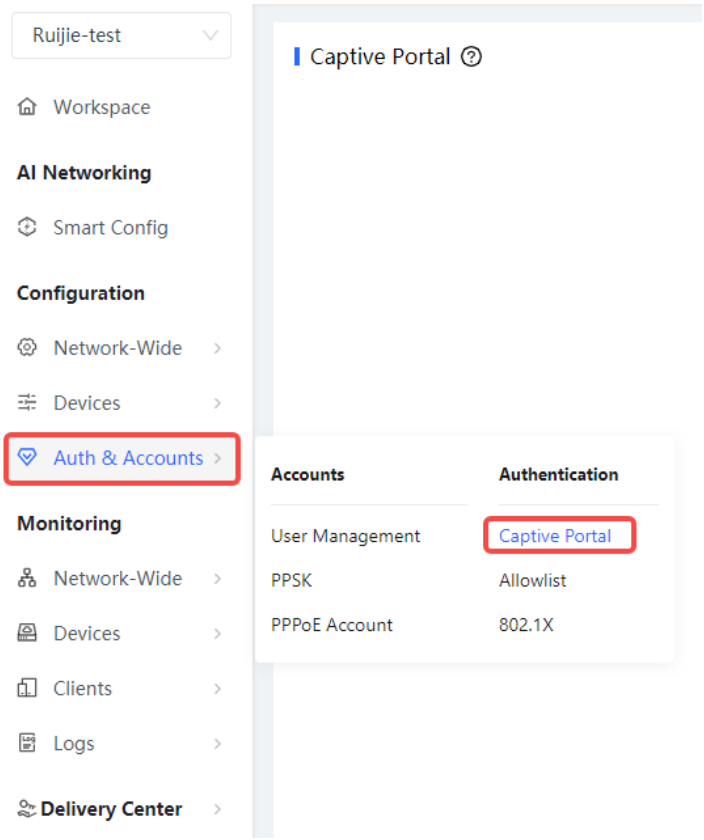
You can use the **Captive Portal** feature to set authentication policies, including customizing authentication pages, setting authentication network segments, SSID, and other information.

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.

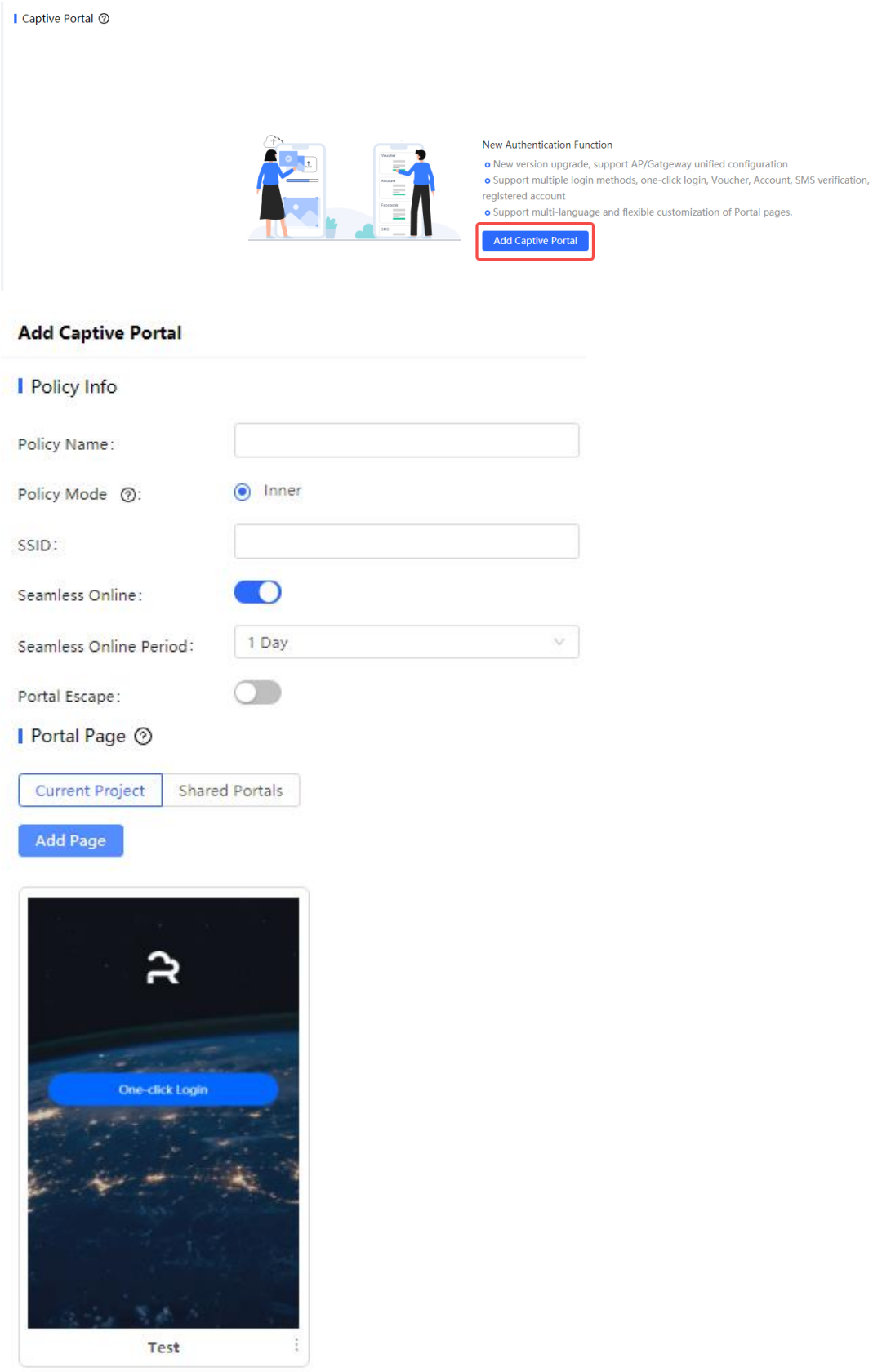
The network security can be enhanced by configuring the **Captive Portal**.

Procedure

(1) Choose **Configuration**> **Auth & Accounts** > **Authentication** > **Captive Portal**.



(2) Click **Add Captive Portal** to add a captive portal.



a Configure basic information about the captive portal.

Table 11-1 Basic Information About the Captive Portal

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

Parameter	Description
Portal Page	Indicates the portal page that is displayed after portal authentication. Click **Current Project** to select the portal page for an existing project. Click **Shared Portals** to select an existing portal page. Click **Add Page** to customize a portal page.

b To customize a portal page, the portal basic settings and portal visual settings of the device is required.

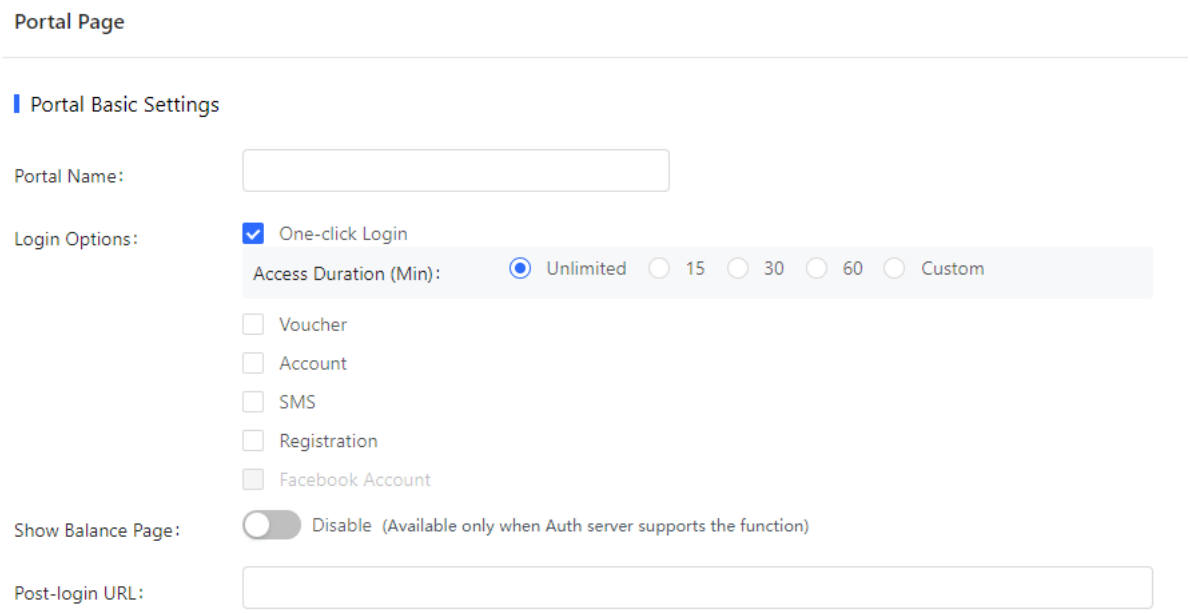


Table 11-2 Basic Information of the Portal Page

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Indicates the option to perform the desired action. **One-click Login**: indicates login without the username and password. You can set **Access Duration** and **Access Times Per Day**. **Voucher**: indicates login with a random eight-digit password. **Account**: indicates login with the account and password. **SMS**: indicates login with the phone number and code. Registration:
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

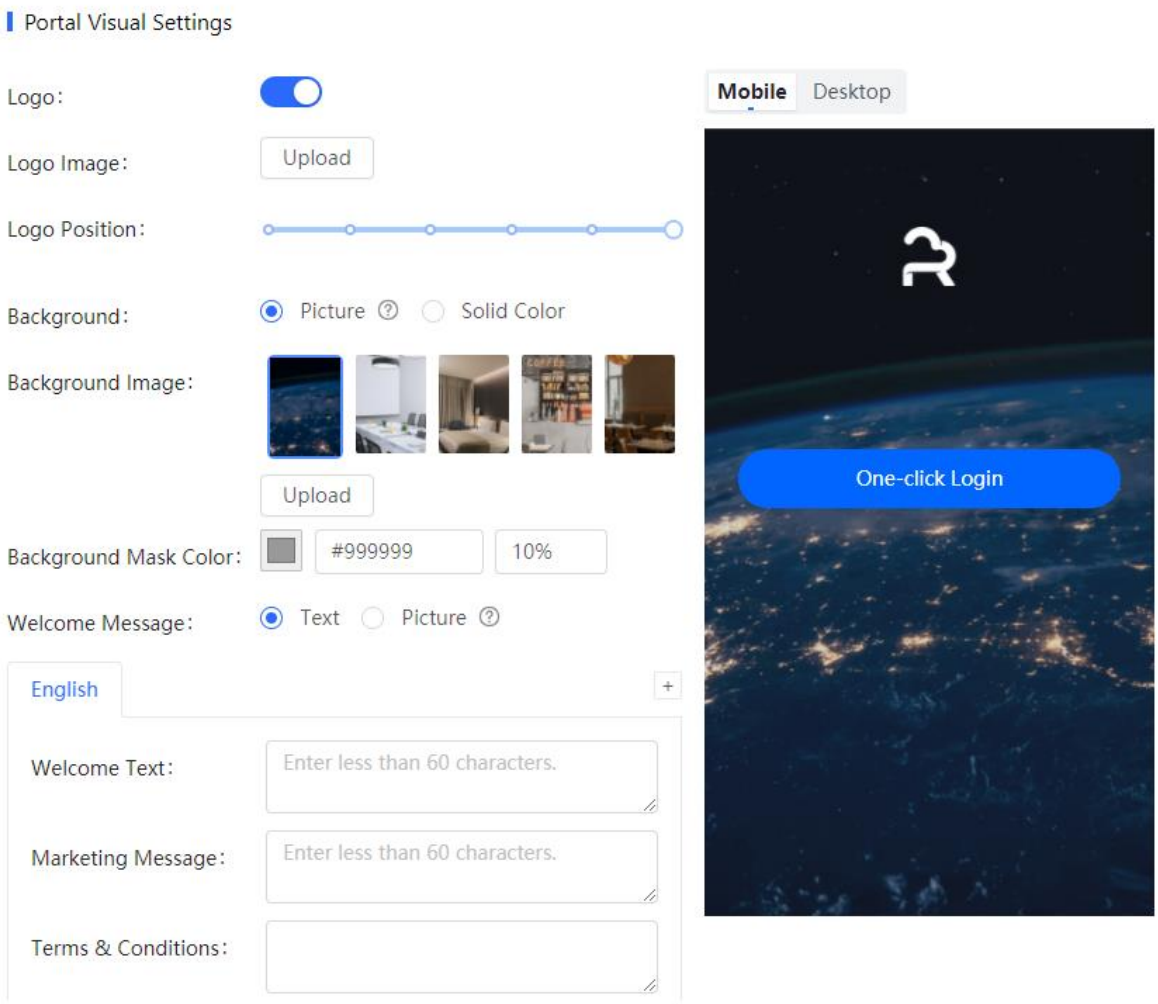


Table 11-3 Visual Information of the Portal Page

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

Parameter	Description
Language	Select the language of the portal page.
Welcome Message	Select the welcome message with the image or text.
Marketing message	Enter the marketing message.
Terms & Conditions	Enter terms and conditions.
Copyright	Enter the copyright.
Login Button	Select the login button on the authentication page.
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

c Click **OK**.

Note

- Considering the performance and good design of the page, one network supports up to 50 portal templates.
- The portal template supports multiple languages including Chinese (Simplified), Chinese (Traditional), English, German, Indonesian, Japanese, Korean, Malay, Portuguese, Russian, Spanish, Thai, Turkish, and Vietnamese.
- The preview image including mobile and desktop format. The actual effects vary with devices at different resolutions.

After the captive portal is successful configured on the cloud, relevant configurations will be automatically delivered to the device end.

11.2 User Management

11.2.1 Account

Account authentication allows the valid account to access the specified Wi-Fi.

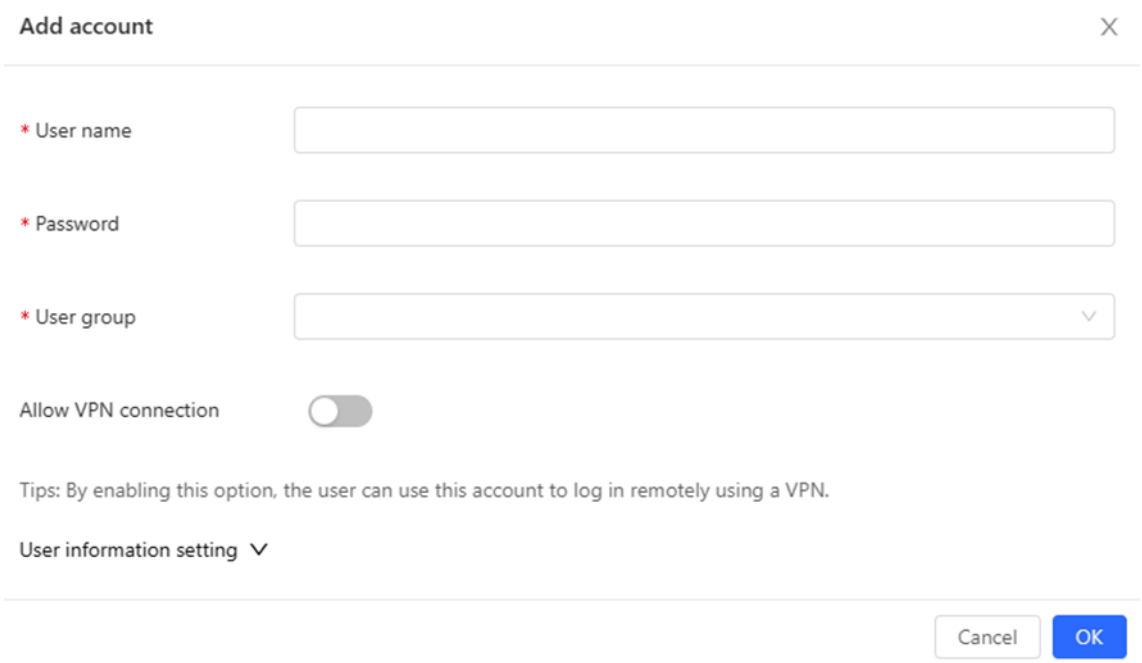
Procedure

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

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

- Adding an account manually

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



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

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

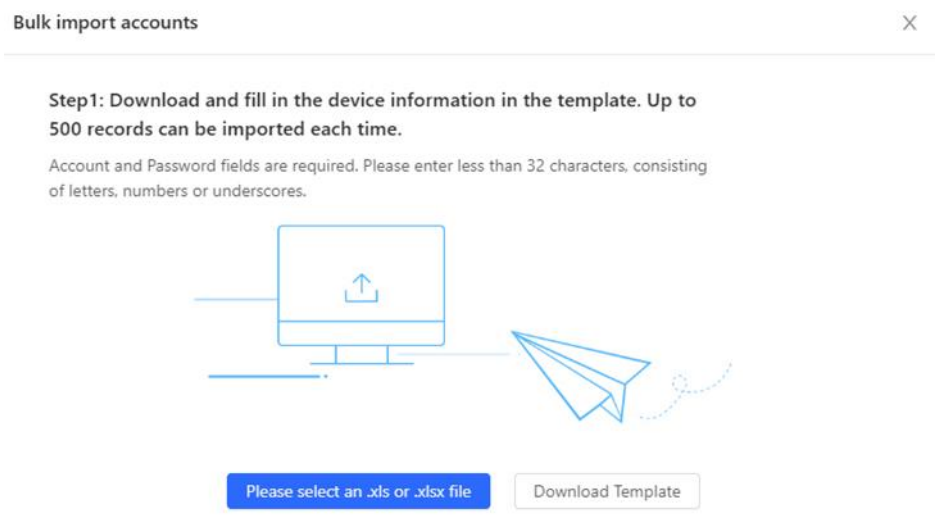
  User group: It indicates a user group. Select a user group from the drop-down list or click **Custom** to create a user group.

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

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

- Adding accounts through batch import

  a Click **Bulk import**.



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

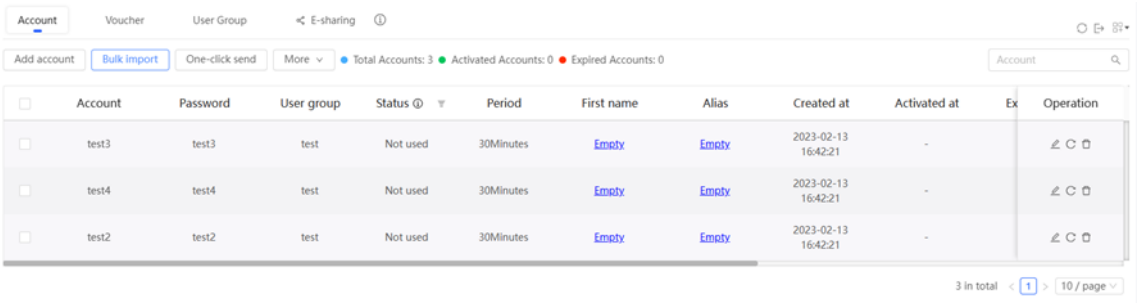
c Edit the template and save it.

Note

- **Account**, **Password**, and **User Group** are mandatory.
- Check that the user group already exists and the added accounts are not duplicate with existing accounts. For details about how to create a user group, see 11.2.3 User Group.

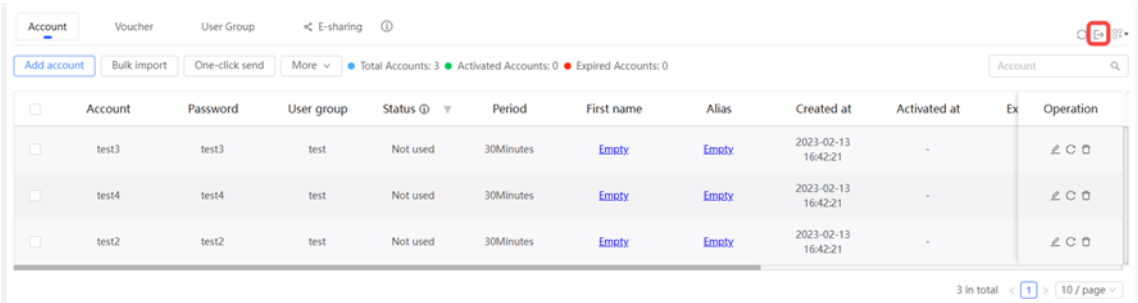
Account	Password	First name	Last name	Alias	User group	Email
test2	test2				test	
test3	test3				test	
test4	test4				test	

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

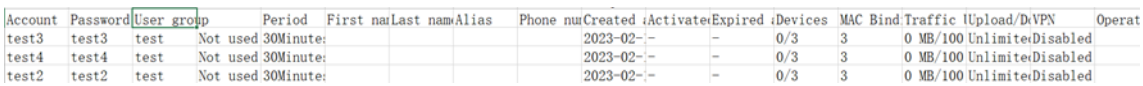


Follow-up Operations

- In the account list, click to export the accounts in .xlsx format.

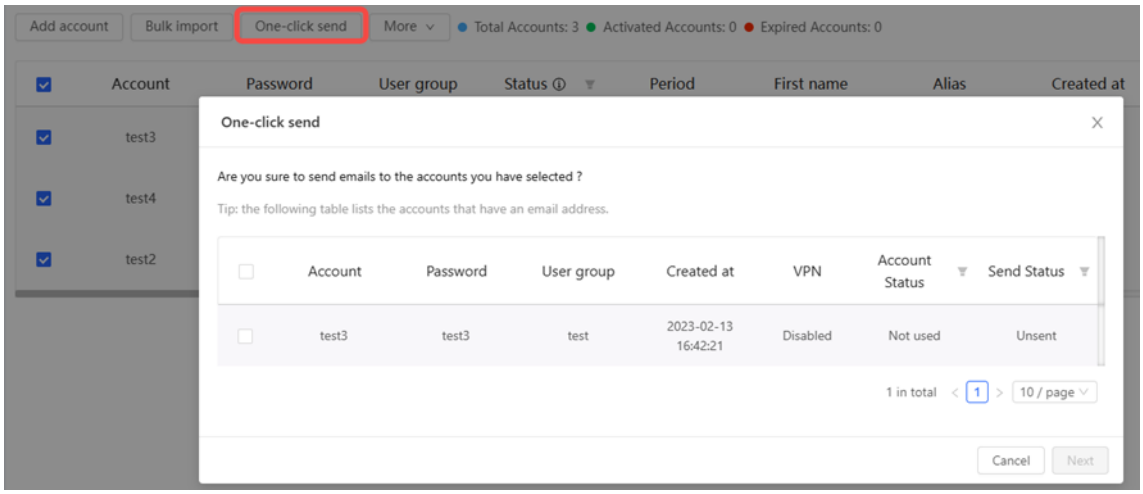


The following figure shows the export result.



Account	Password	User group	Period	First na	Last nam	Alias	Phone nu	Created	Activate	Expired	Devices	MAC Bind	Traffic l	Upload/D	VPN	Operat
test3	test3	test	Not used	30Minute				2023-02-	-	-	0/3	3	0 MB/100	Unlimite	Disabled	
test4	test4	test	Not used	30Minute				2023-02-	-	-	0/3	3	0 MB/100	Unlimite	Disabled	
test2	test2	test	Not used	30Minute				2023-02-	-	-	0/3	3	0 MB/100	Unlimite	Disabled	

- Click **One-click send** to email the accounts to employees.



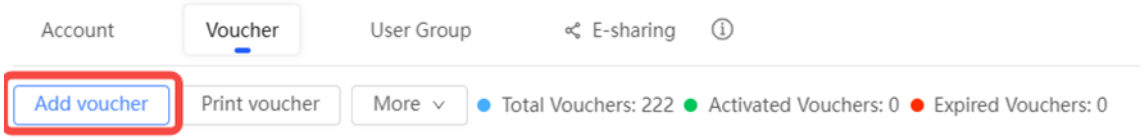
11.2.2 Voucher

Voucher authentication on Ruijie Cloud allows you to charge users for wireless network access using access codes. The number of concurrent users, time, and data quota limit can be customized and offer to your guests.

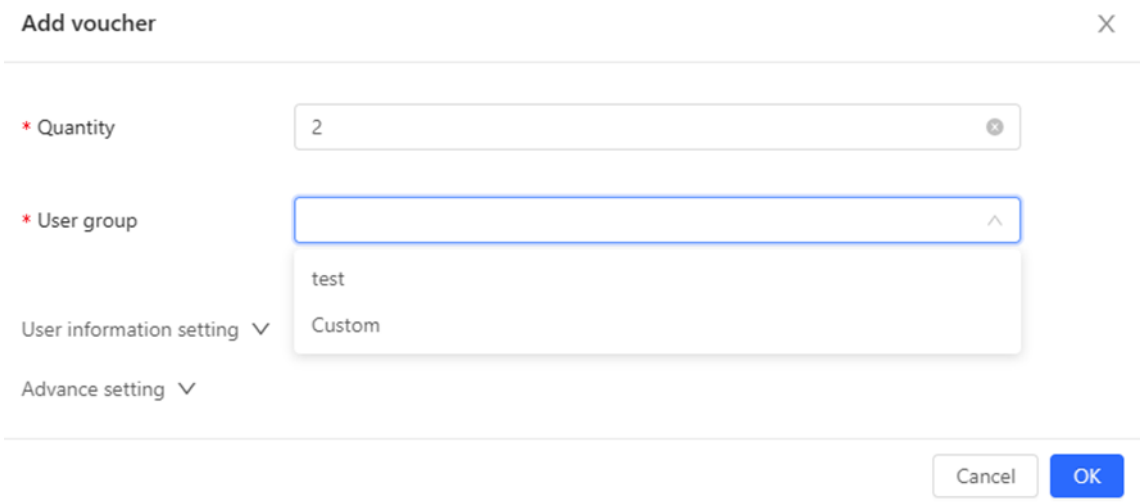
Procedure

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

(2) On the **Voucher** tab, click **Add voucher**.



(3) Configuring voucher parameters. After configuration, click **OK**.



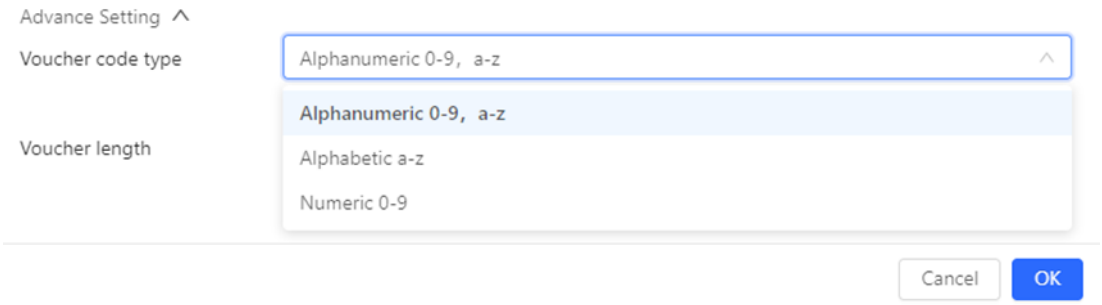
Quantity: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the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

User group: Select a user group or click **Custom** to customize a new user group.

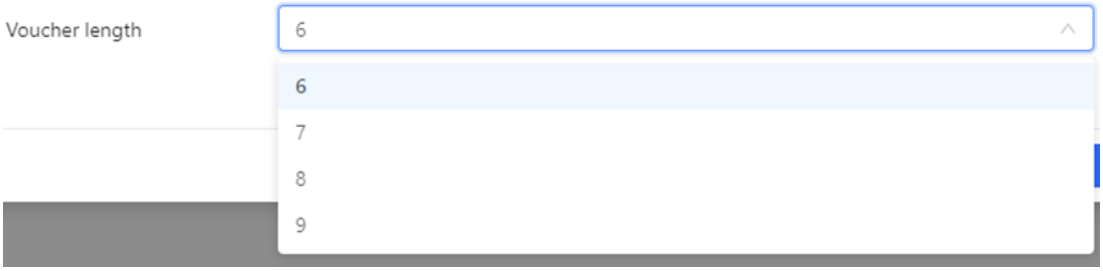
User information setting: Configure user information, which is optional.

Advance setting:

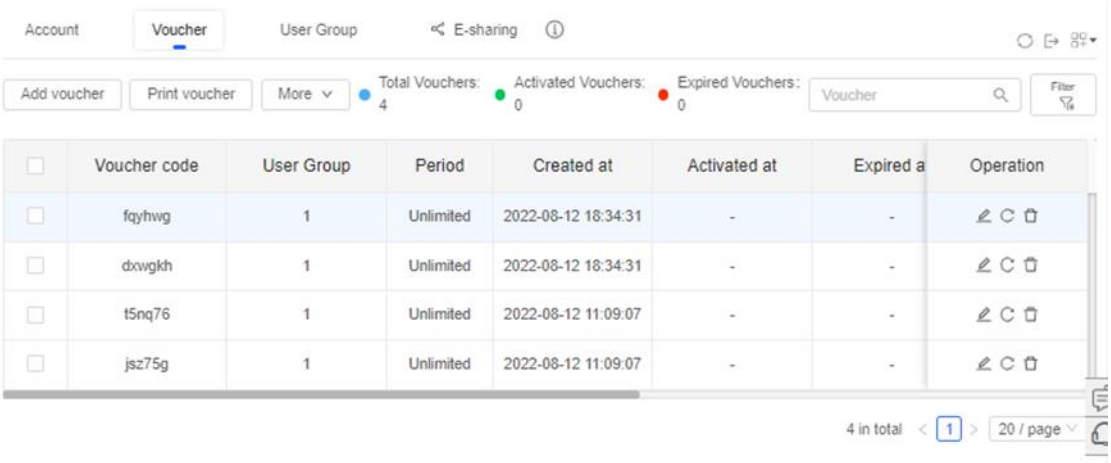
- **Voucher code type**: Set the value to Alphanumeric 0-9, a-z, Alphabetic a-z, or Numeric 0-9.



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

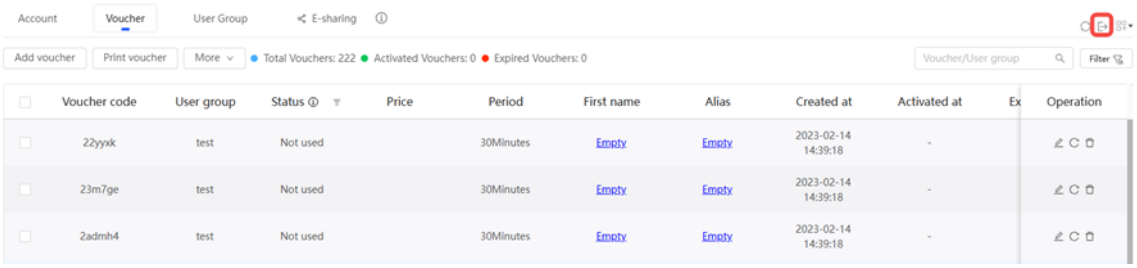


(4) View the voucher list.



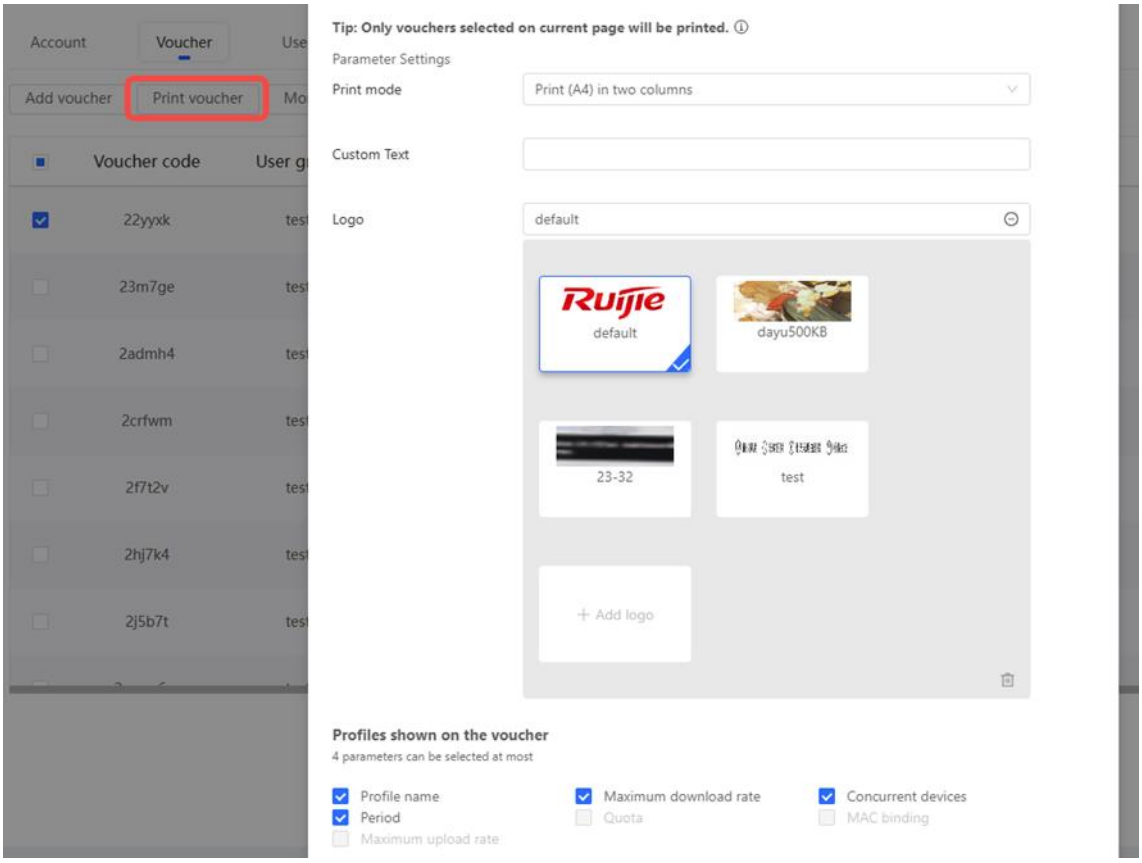
Follow-up Operations

- Exporting the voucher



- Printing the voucher

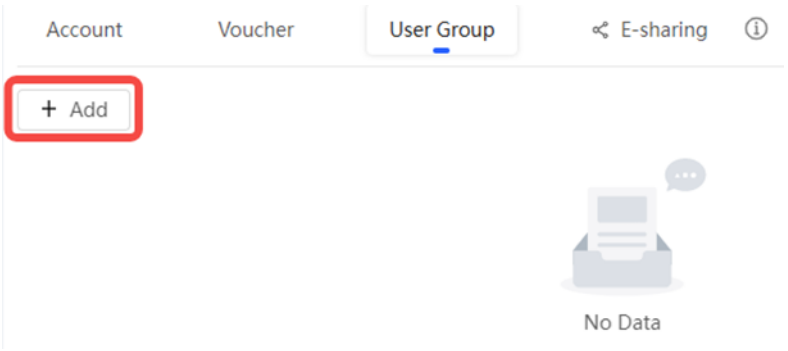
  Click **Printing Voucher** and complete print configurations.



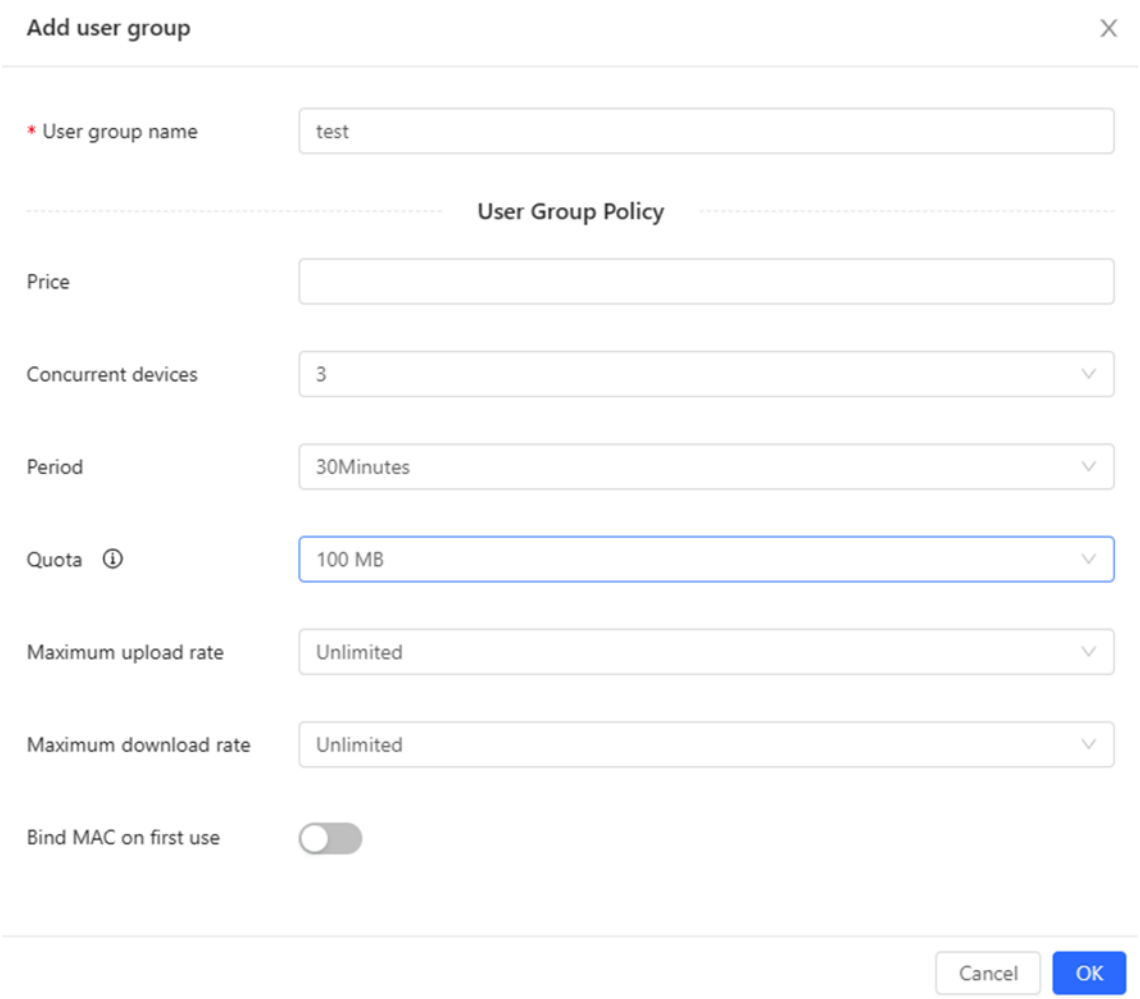
11.2.3 User Group

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

(2) On the **User Group** tab, click **Add**.



(3) Configure user group parameters. After configuration, click **OK**.



User Group Name: indicates the user group name.

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

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

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

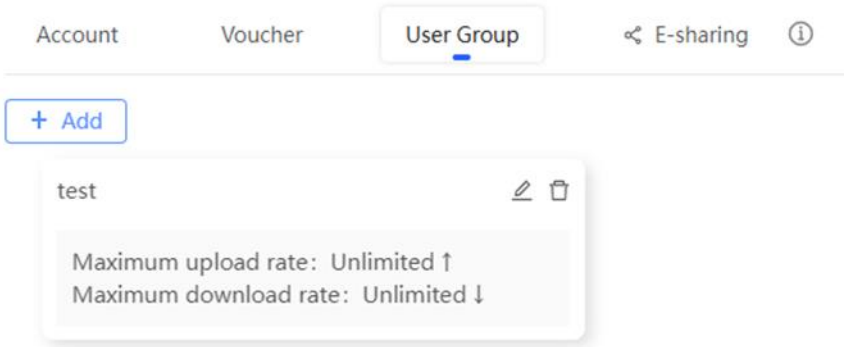
Quota: indicates the maximum amount of data transfer.

Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

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

(4) View the user group list. Click or for a specified user group to modify or delete the user group.



11.3 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

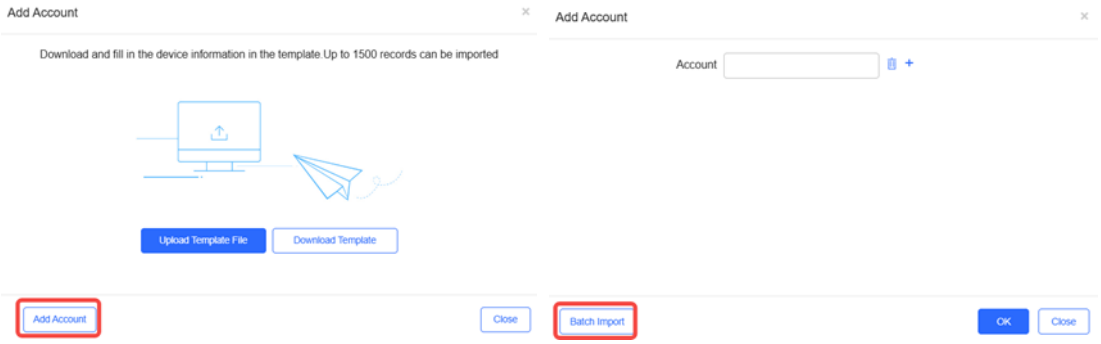
- PPSK only supports import of 1500 passwords.
- PPSK is based on MAC address binding of terminals, and multiple devices of the same user also need to log in with different passwords.
- Each AP can only be configured with a PPSK authentication SSID.
- The PPSK password is generated randomly and does 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.
- Only Ruijie AP support PPSK expect the AP130(L).
- 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.

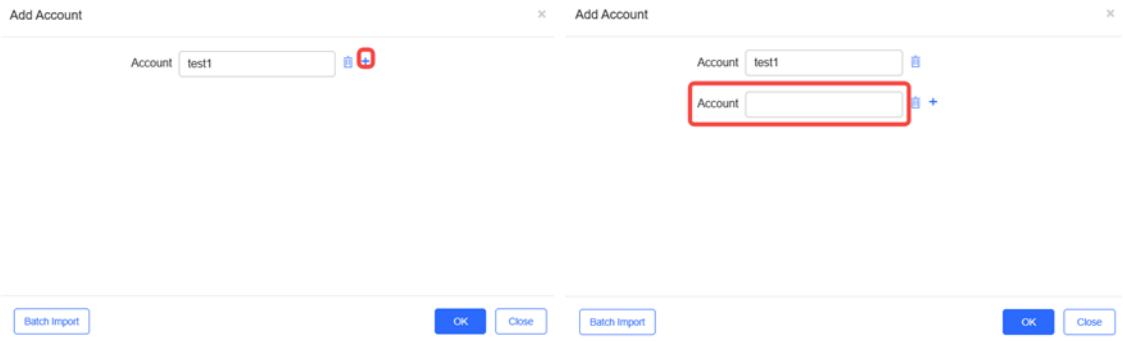
(2) Click **Add** to go to the PPSK account configuration page.

(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.



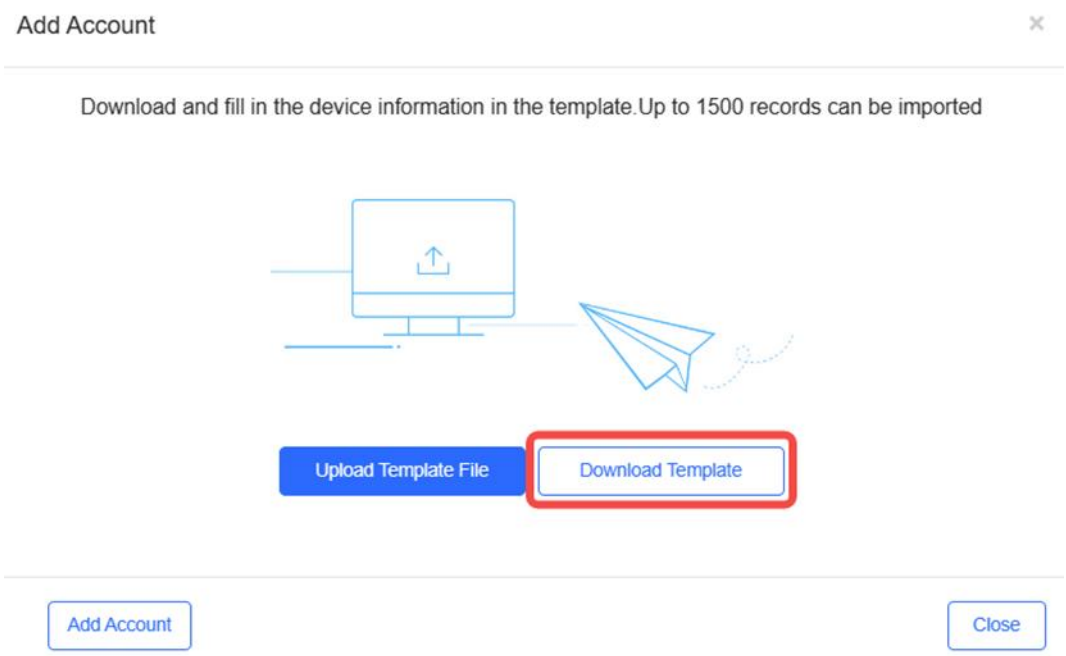
- Adding PPSK accounts manually

  On the **Add Account** page, enter an account name. Click + to add one row. After configuration, click **OK**.

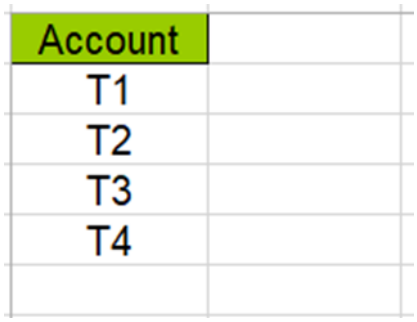


- Adding PPSK accounts through batch import

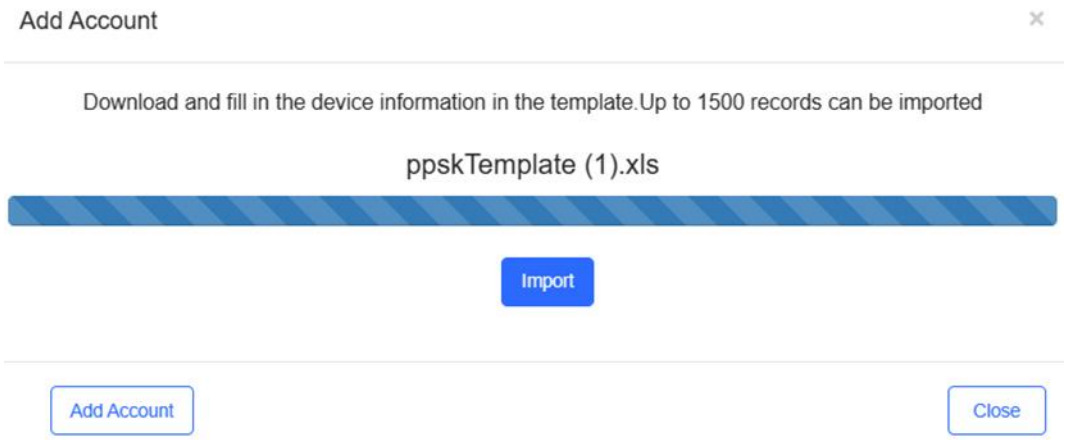
  a Click **Download Template** to download the template.



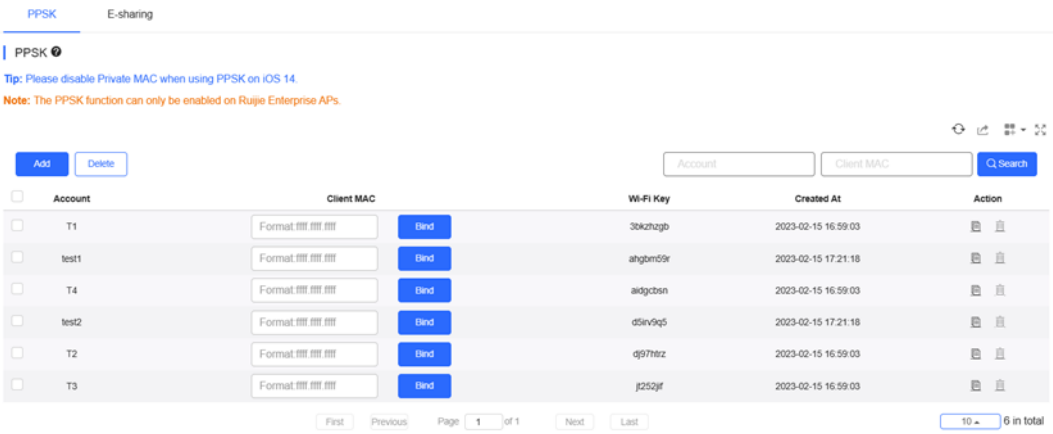
b Edit the template and save it.



c Click **Upload Template File** to upload the file. After uploading, users are automatically created.



(4) View the account list.



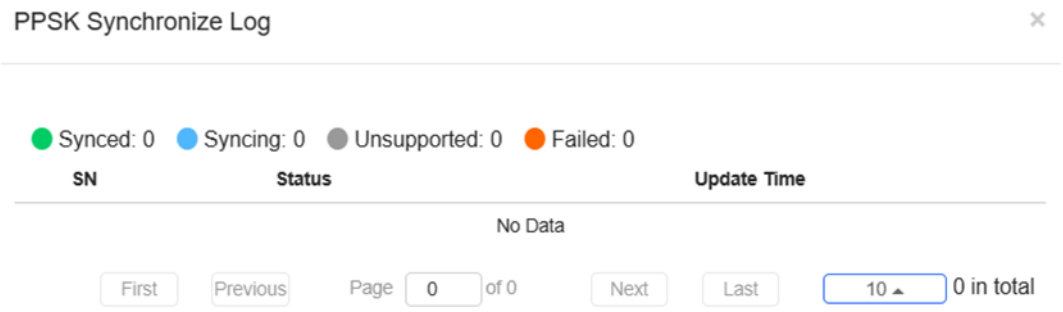
Account: indicates the name of PPSK account.

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.

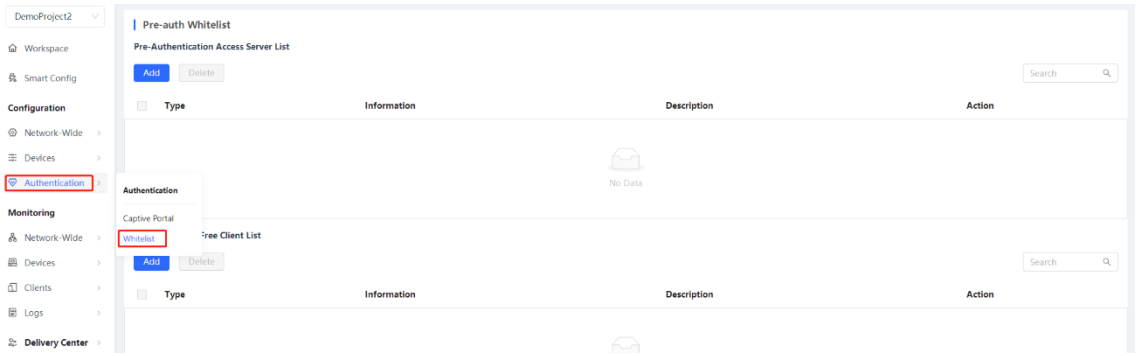
Action: indicates the **View** or **Delete** action. You can view the account to check the PPSK synchronization log.



(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.

11.4 Allowlist

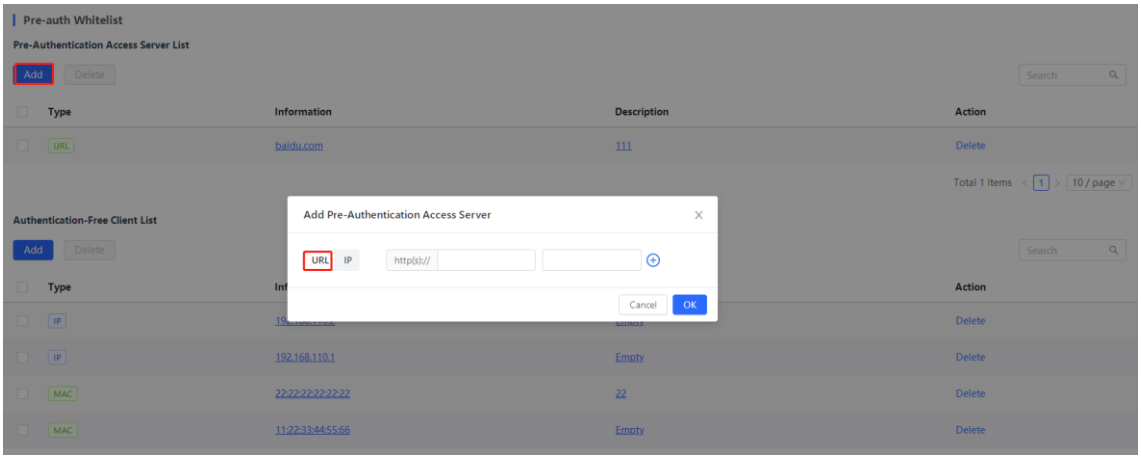
Choose **Authentication** > **Allowlist** to go to the allowlist configuration page.



11.4.1 Pre-Authentication Access Server List

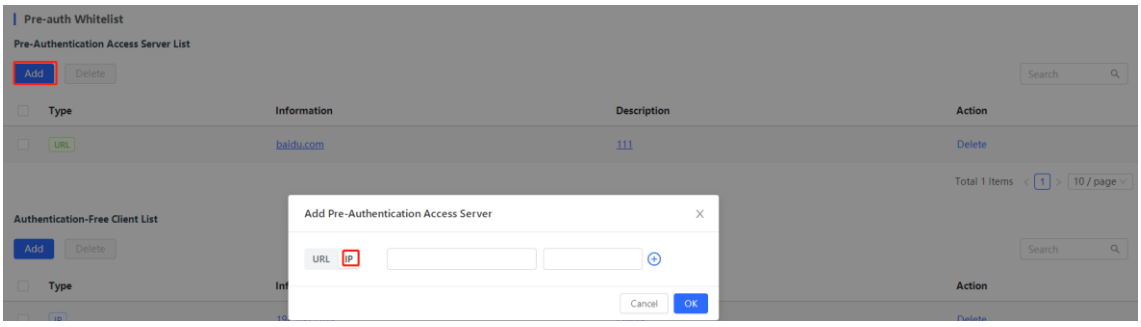
(1) Pre-authentication URL list: It lists websites that can be accessed by users even if the users are not authenticated.

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.



(2) Pre-authentication IP list: It lists external network IP addresses that can be accessed by all users including unauthenticated users.

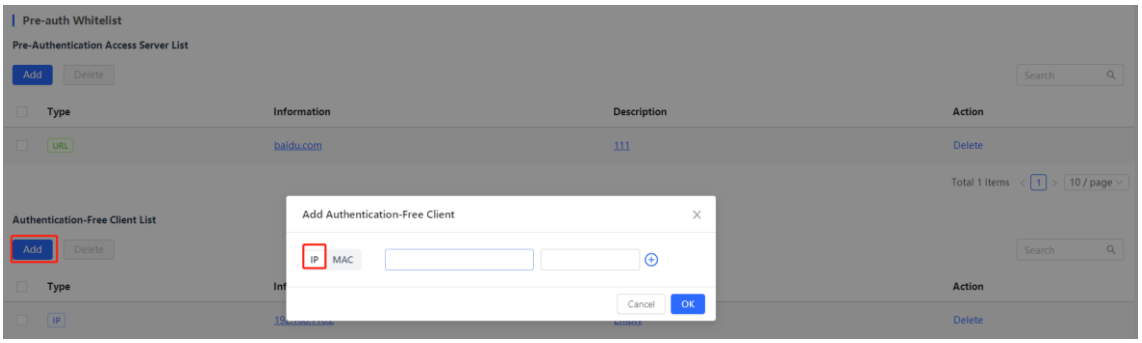
Click **Add** below **Pre-Authentication Access Server List**, select **IP**, and add an IP address. You can add a description for the IP address behind the IP address.



11.4.2 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.



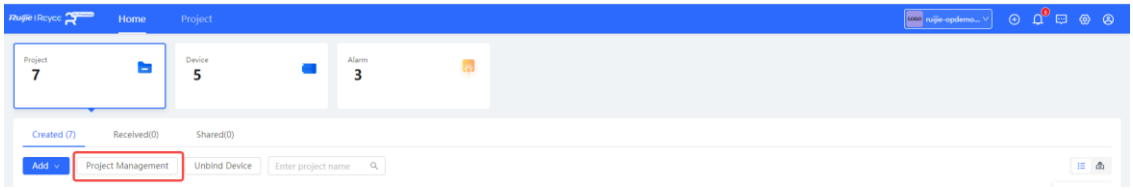
(2) Authentication-free MAC list: MAC addresses in the list can access the Internet without authentication.

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.

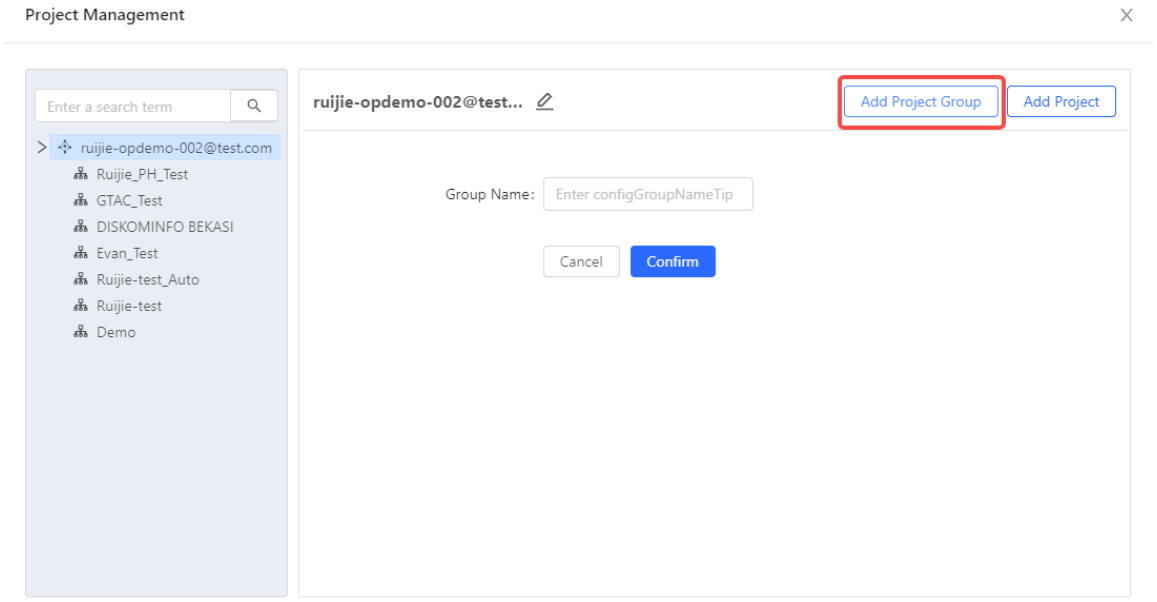
12 Cloud Account and Project Management

12.1 Adding a Sub Project

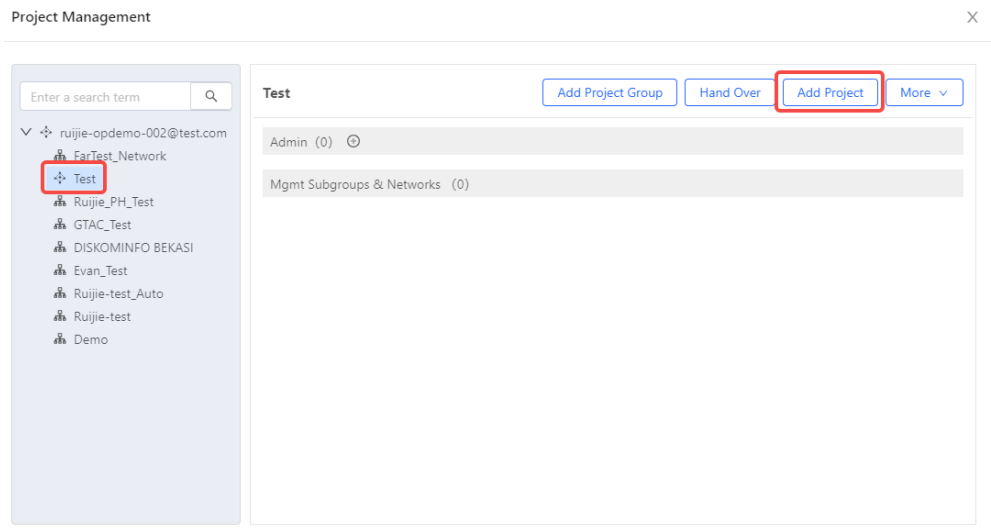
(1) Choose **Home** > **Project** and click **Project Management**.

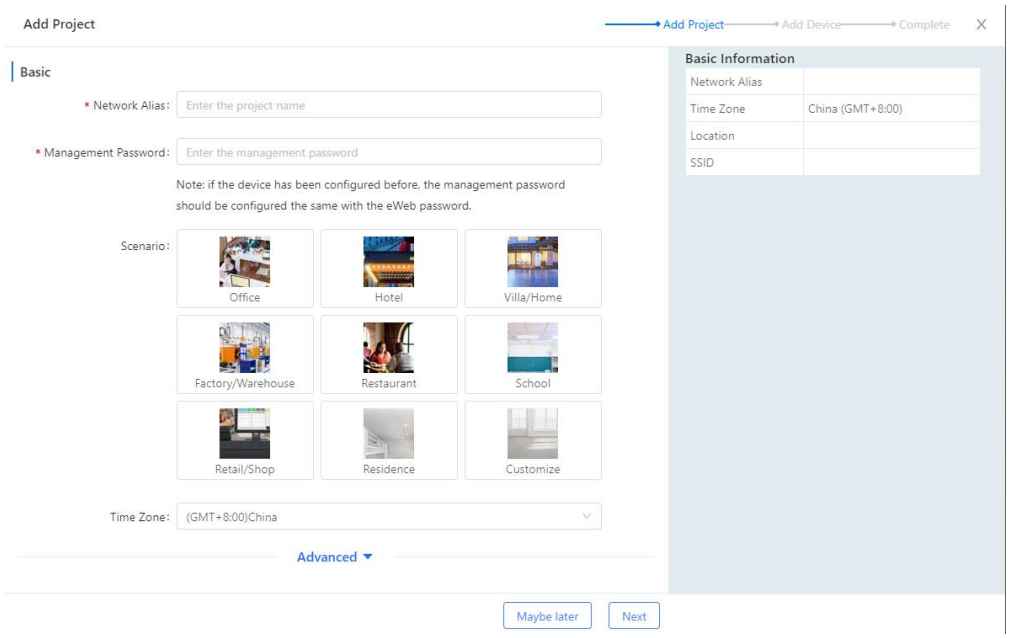


(2) Click **Add Project Group** and enter the **Group Name** to create a group.



(3) Select a project group and click **Add Project**. Set basic parameters of the sub project. Then click **Next**.

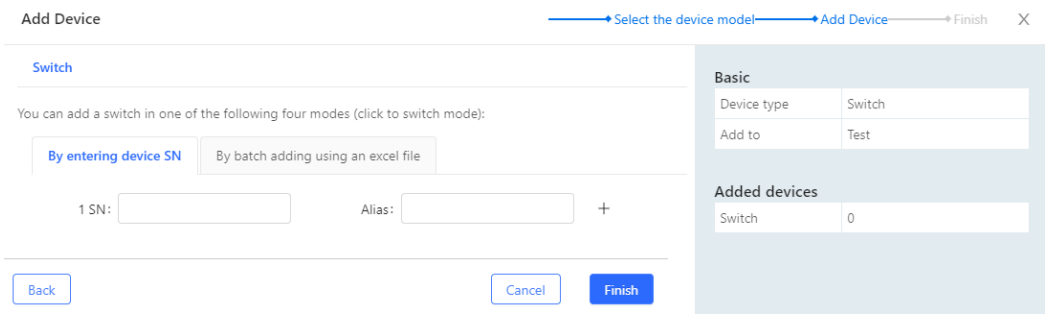




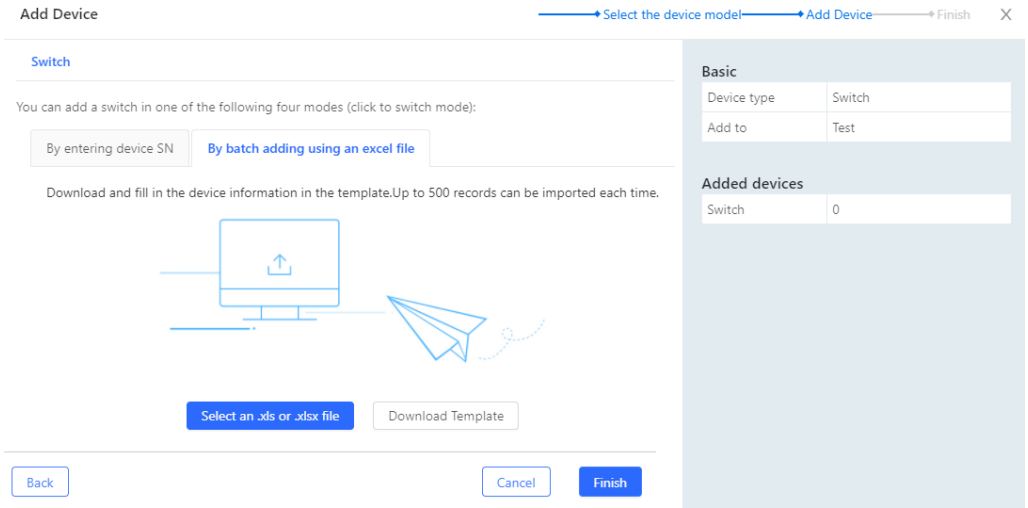
(4) Add devices manually or through batch import.

- Option 1: Add devices manually.

  Enter the device SN and alias.



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



a Click **Batch Import**.

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

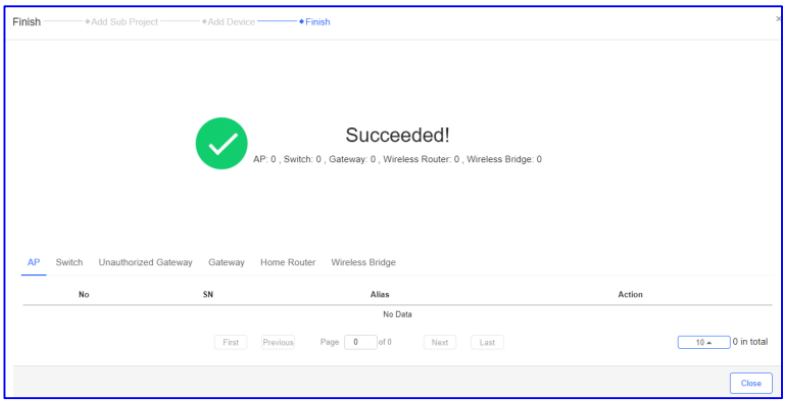
c Fill in the device SN and alias in the template and save it.

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

e Click the **Import** button.

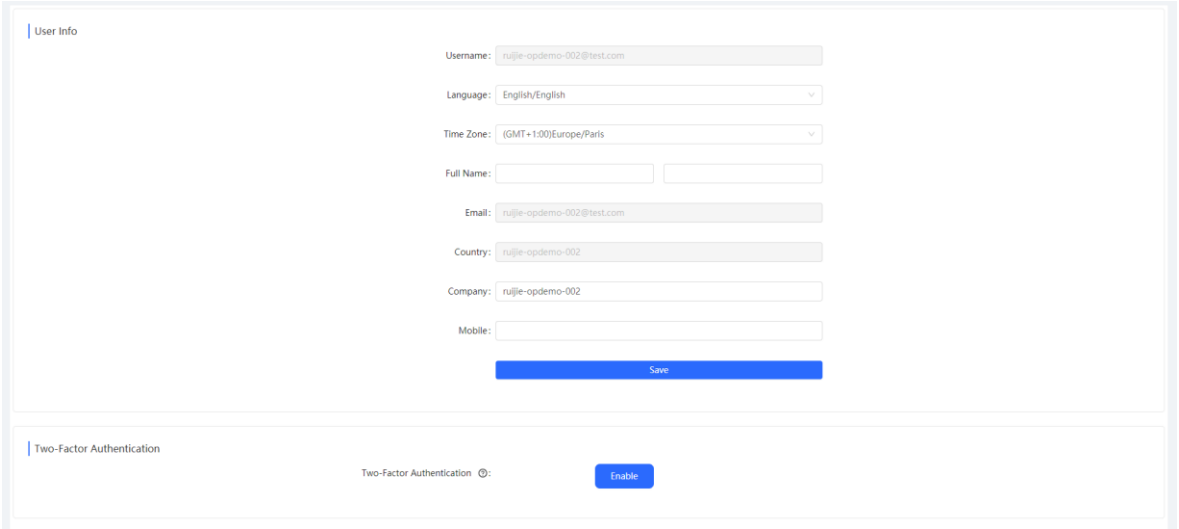
(5) After the devices are added, click **Save & Next**.

The sub project is added successfully.



12.2 Managing Cloud Login Accounts

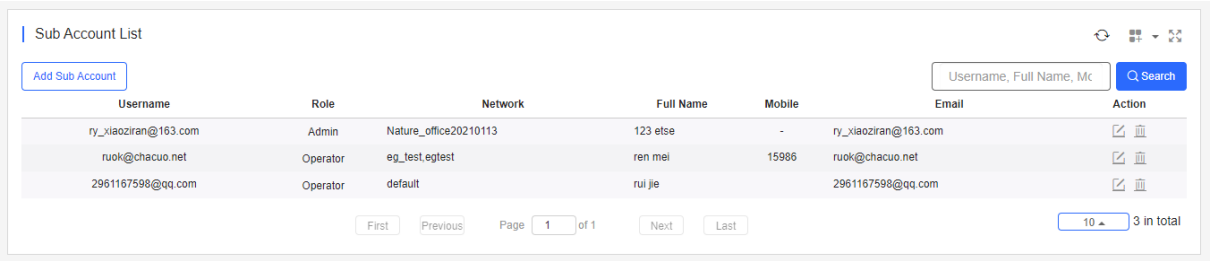
Click  at the upper right corner and click **Account**.



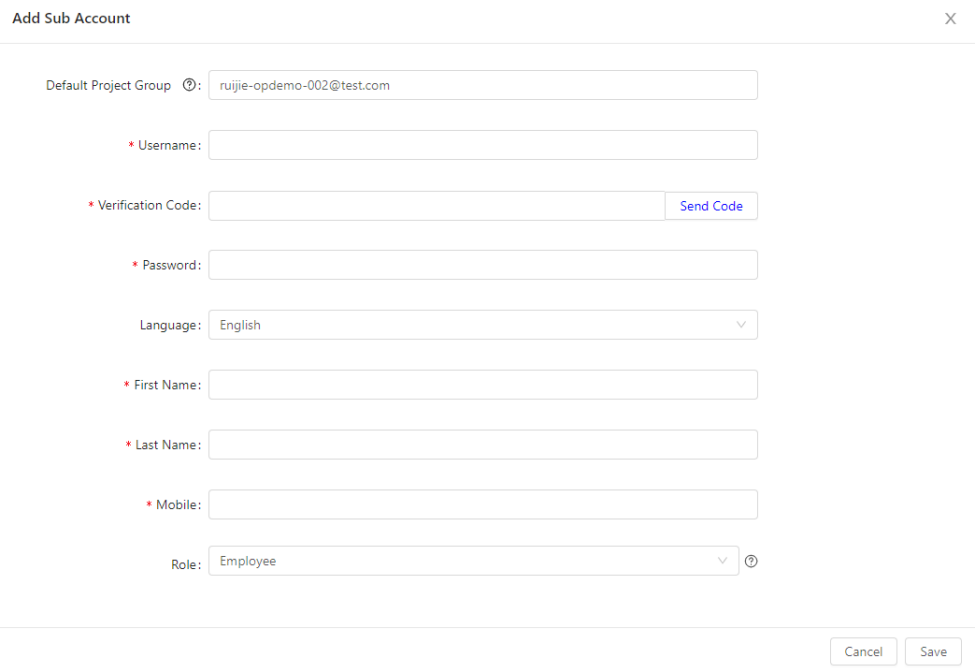
12.3 Managing Cloud Sub Accounts

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.



Click **Add Sub Account** to add a new sub account. Select the network, enter the Email in the **Username** box and click **Send Code**. Enter the security code contained in the Email, set the password, language, full name, expiration date, mobile and role, and click **Save**.



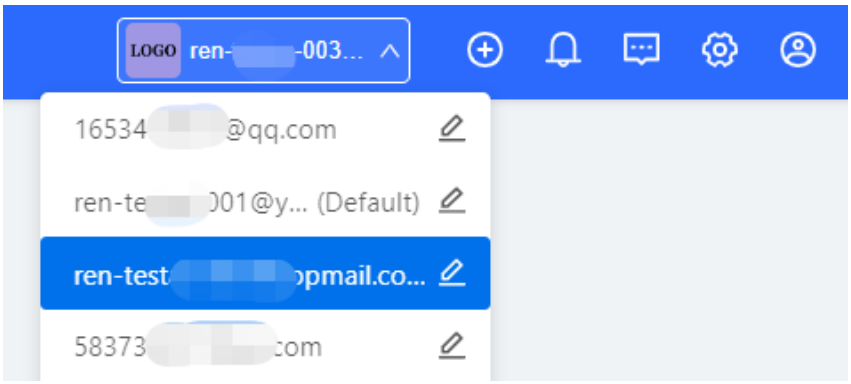
Role:

- **Admin** owns the permissions to create an account.
- **Employee** owns the permissions to edit data.
- **Operator** owns the permissions to print voucher and view account data.
- **Guest** owns the permissions to view data.

12.4 Switching Accounts

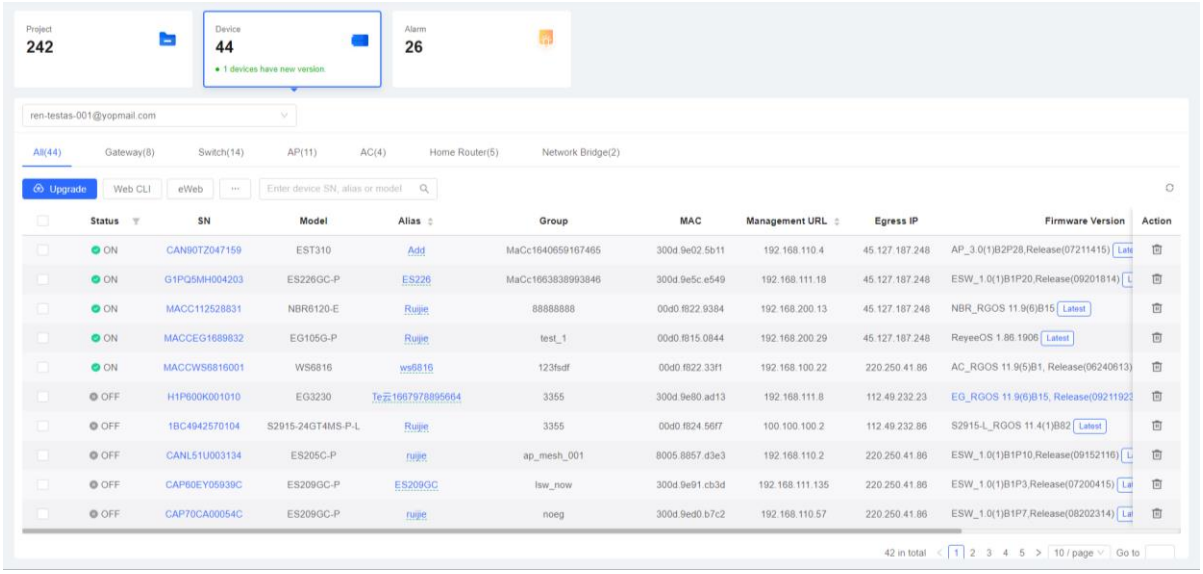
Click 

at the upper right corner.

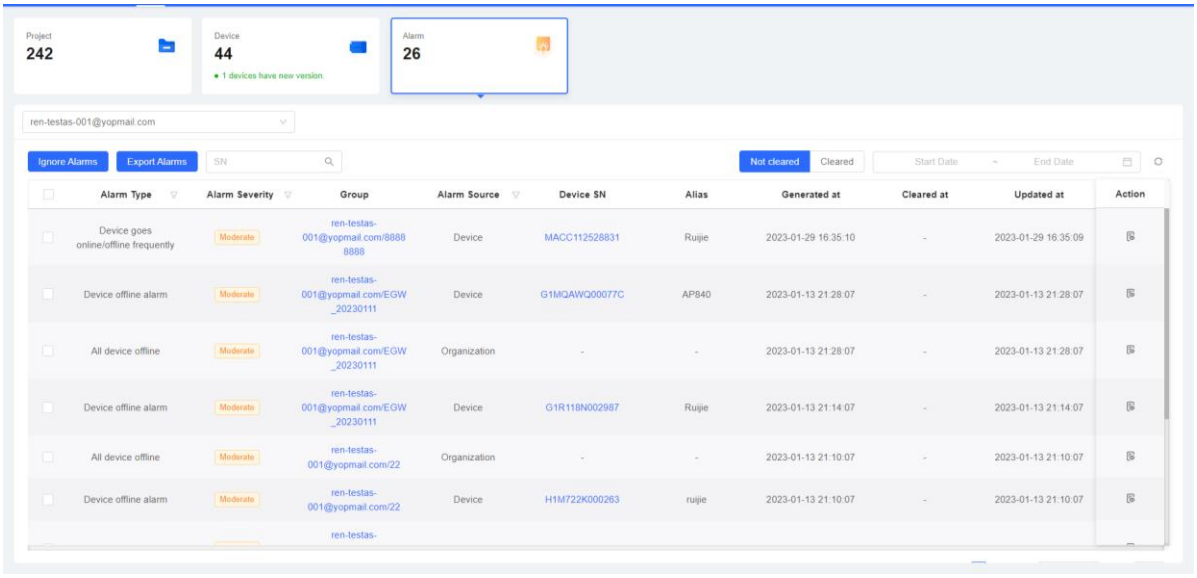

LOGO
ren-
-003...
16534
@qq.com
ren-te
001@y... (Default)
ren-test
opmail.co...
58373
com

13 Monitoring

13.1 Viewing all the Device



13.2 Viewing all the Alarm



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.

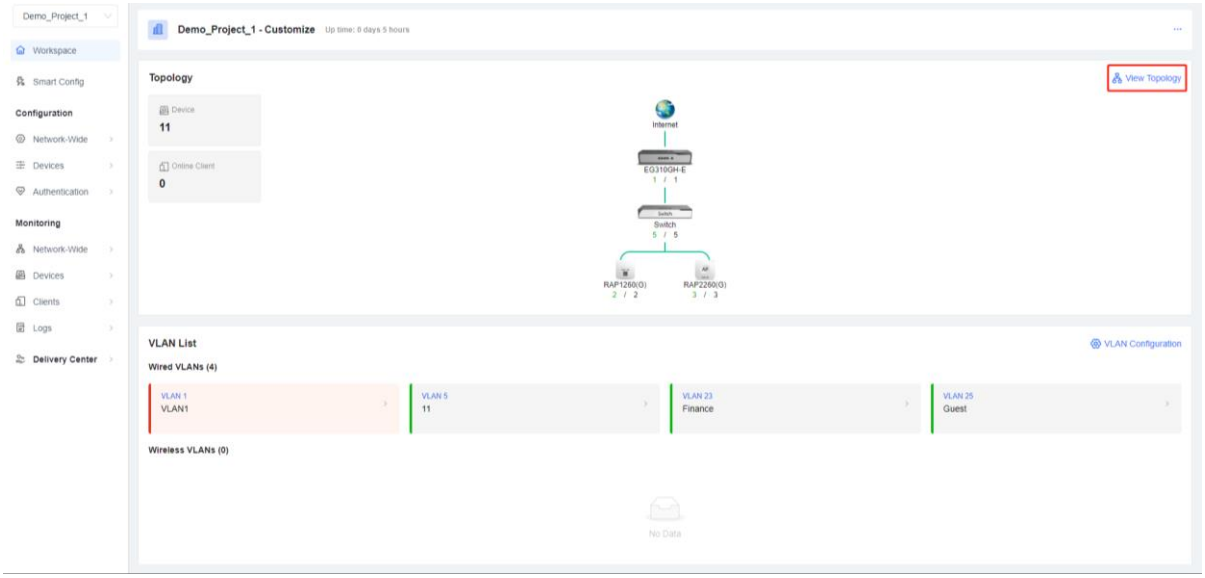
(3) The number of connected devices is calculated based on the root node and the topology is refreshed. Data such as MAC addresses, ARP entries, and routing entries is required.

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

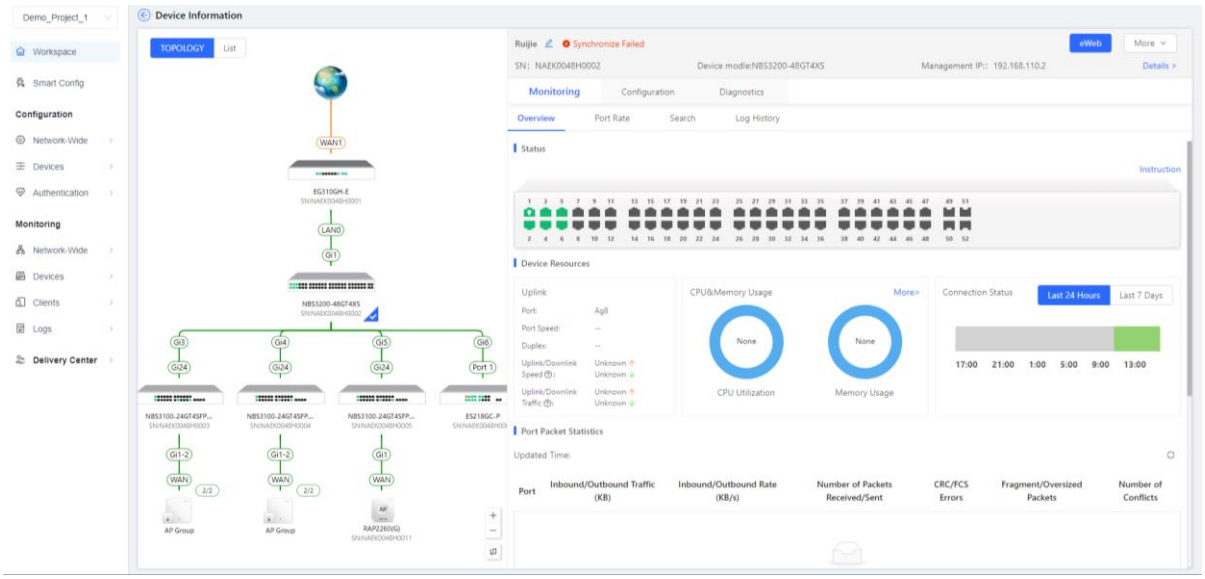
Click Project > Workspace > View Topology



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.

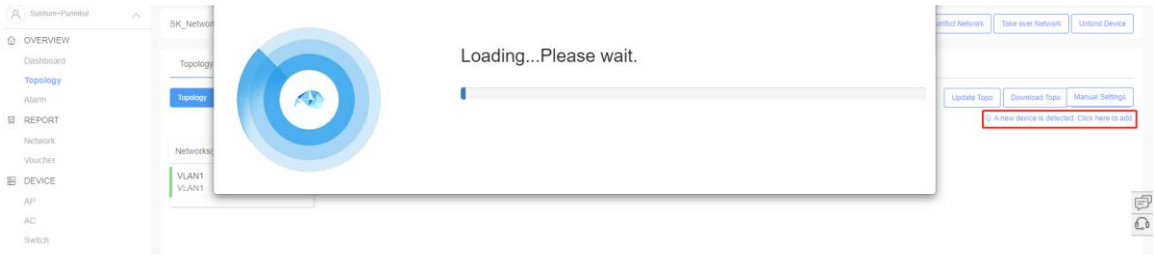


13.4 Detecting Device

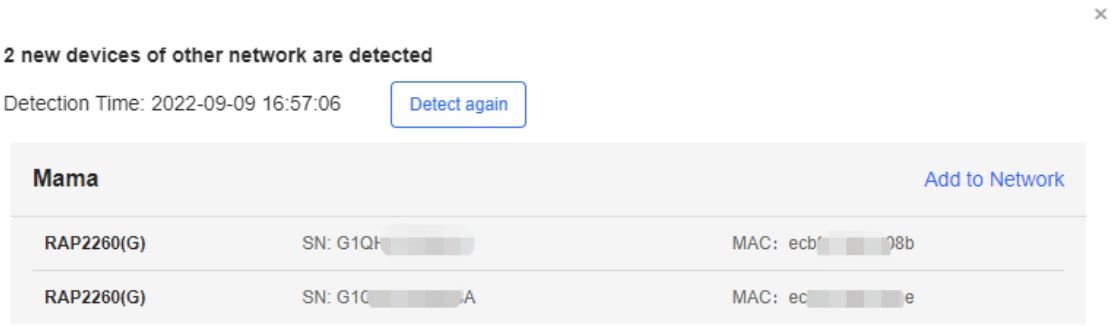
Detect Device: After the detection is completed, the detection result will be displayed.

Procedure

Click **Project** > **Workspace** > **View Topology**, Click Detect Device.



After the detection is completed, the detection result will be displayed.



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.

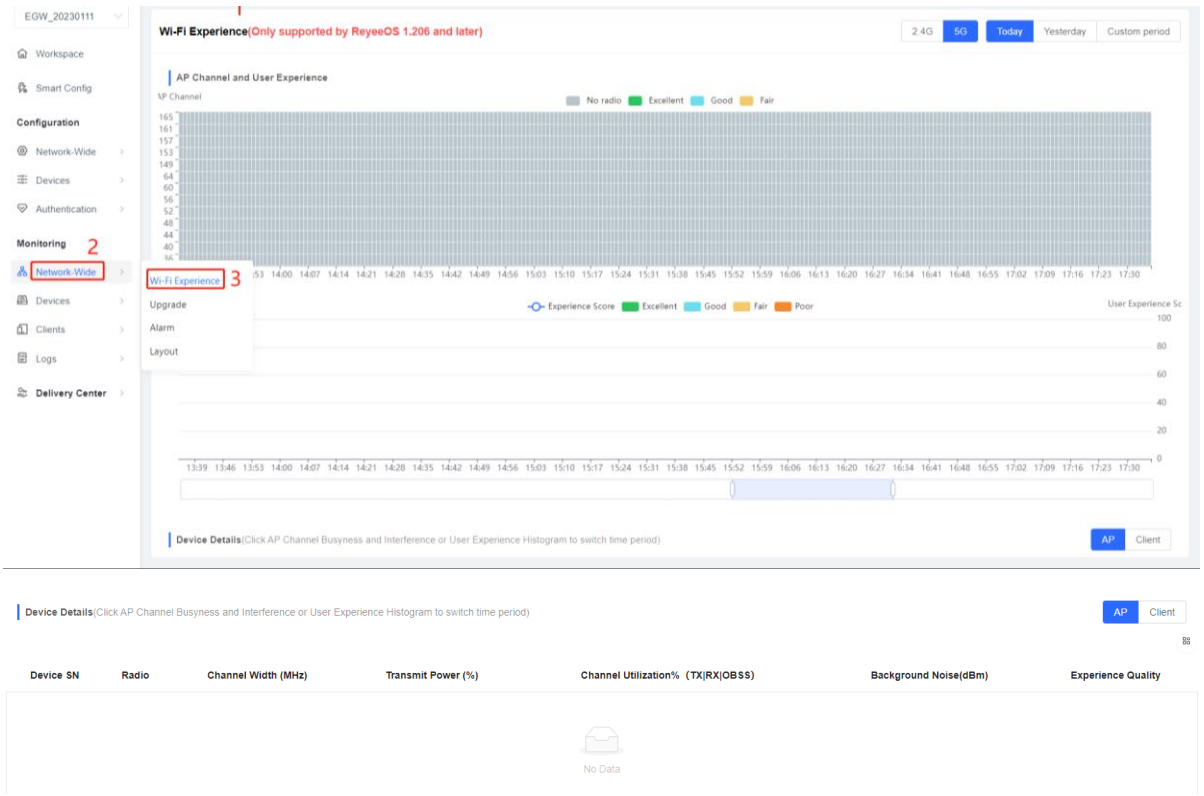
Ruijie Cloud refreshes the topology by default when a device is added to the network. When Ruijie Cloud fails to detect the added devices, click **Detect again** to update the topology.

13.5 Wi-Fi Experience

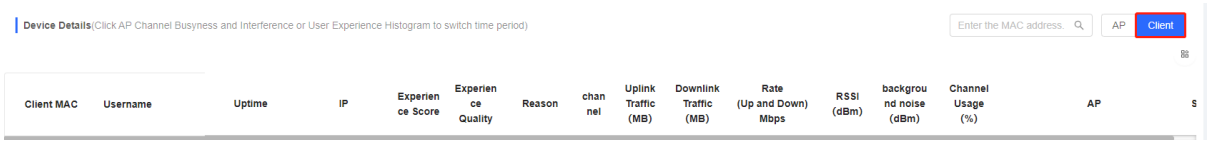
The bar chart displays the experience status in a given period of time and collects data approximately every 5 minutes.

Experience: Parameters include the client delay, packet loss, and signal strength, and the SVM algorithm is used to calculate the score.

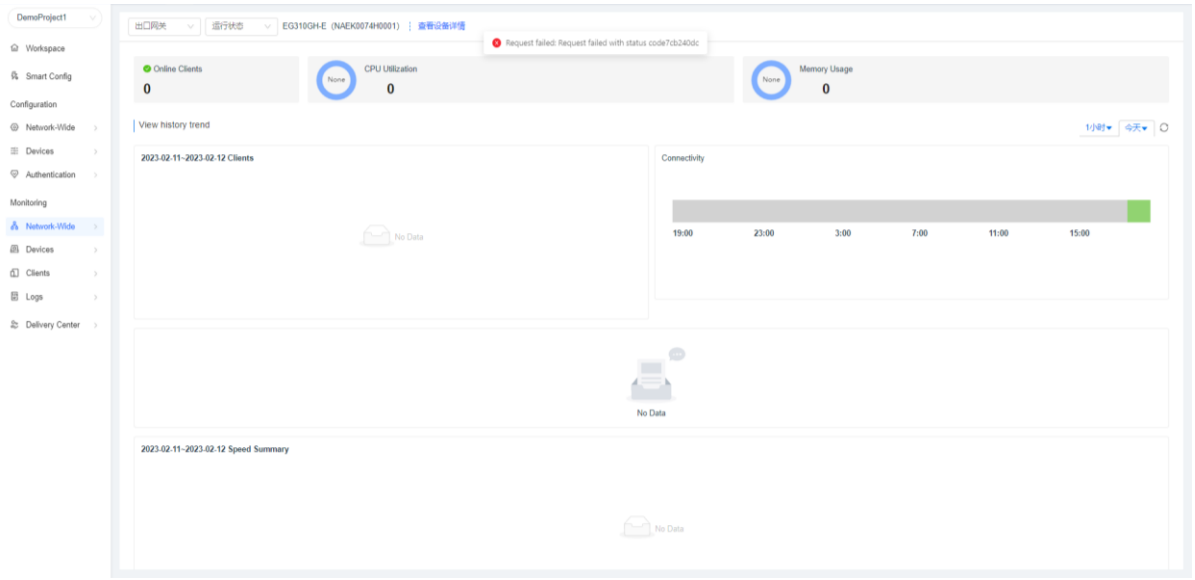
Color	Experience Type	Experience
	Excellent	The HDV and internet game are available
	Good	The communication application, web page, and VoIP are available
	Fair	The client goes offline frequently
	Poor	The client is difficult for the client to go online
	No radio	Check whether a client is inactive according to the traffic and power usage



Client



13.6 Data insights



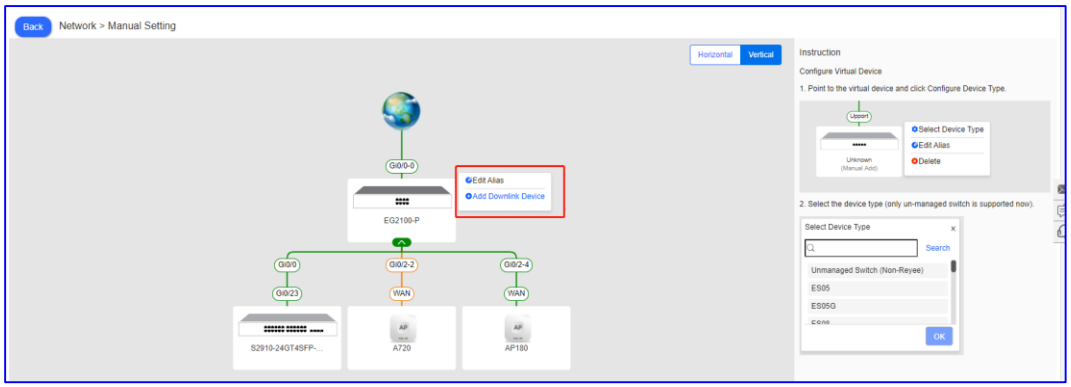
13.7 Edit Topology

Procedure

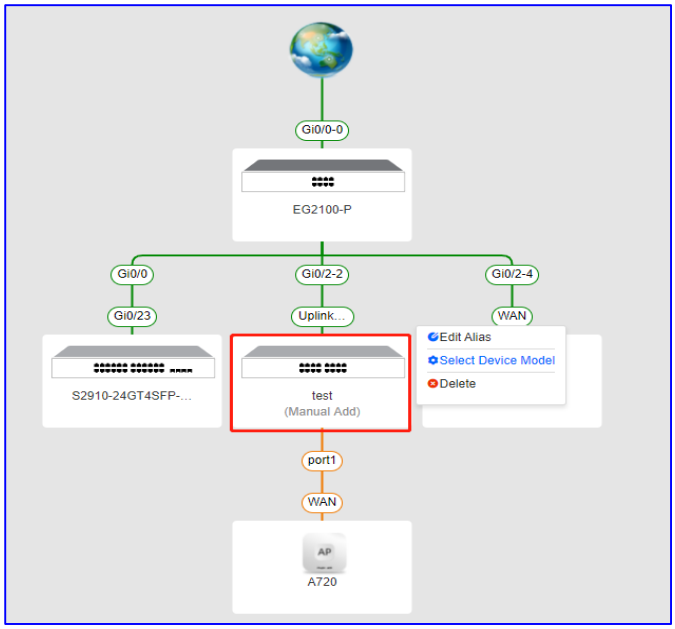
Click Project > Workspace > View Topology and click Edit

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.



- 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).



13.7.1 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?

(1) If the version is not the latest one, you need upgrade it to the latest version.

(2) 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?

(3) **show mac/show arp/show ip route**: If the output of any of the preceding commands contains the configuration with S*, static bindings exist.

(4) Dynamic routing protocols such as OSPF are configured for the topology.

(5) The switches in the topology are configured with VSU.

4. What can I do if virtual devices are displayed in the topology?

(6) The network device is not on the Ruijie Cloud or is offline.

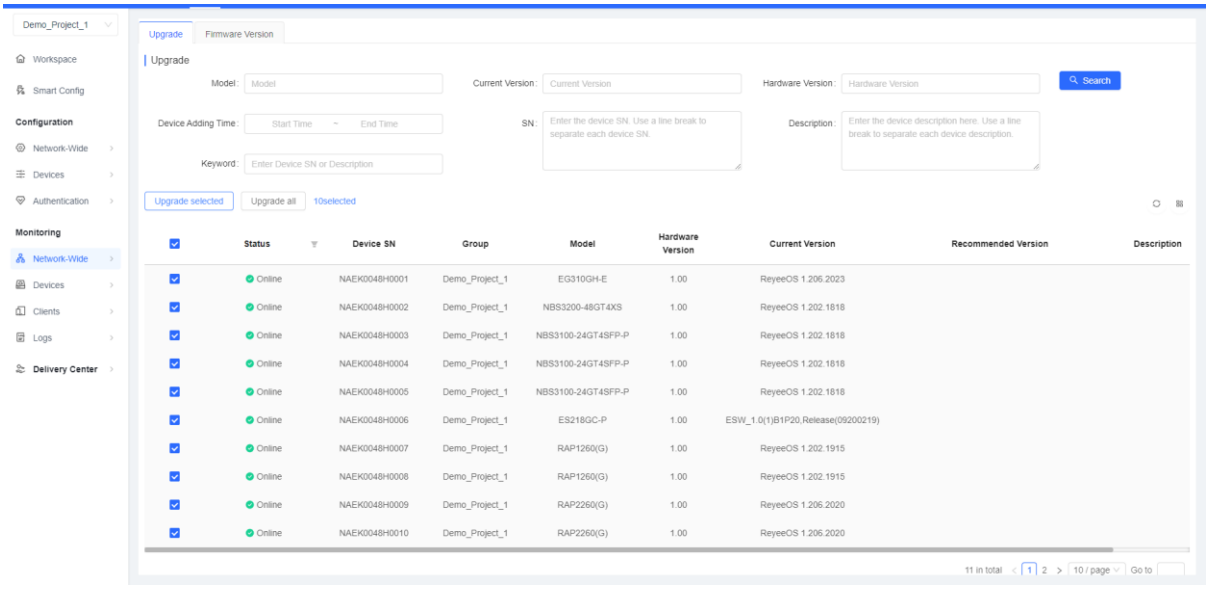
(7) The network device is not the Ruijie device.

(8) If the network device is an unmanaged switch, you are advised to edit the name and the port manually.

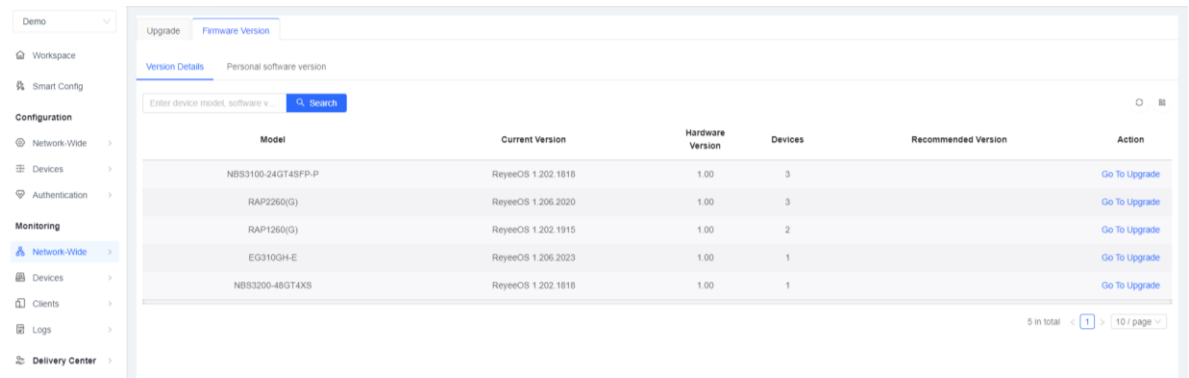
13.8 Upgrade

13.8.1 Upgrade

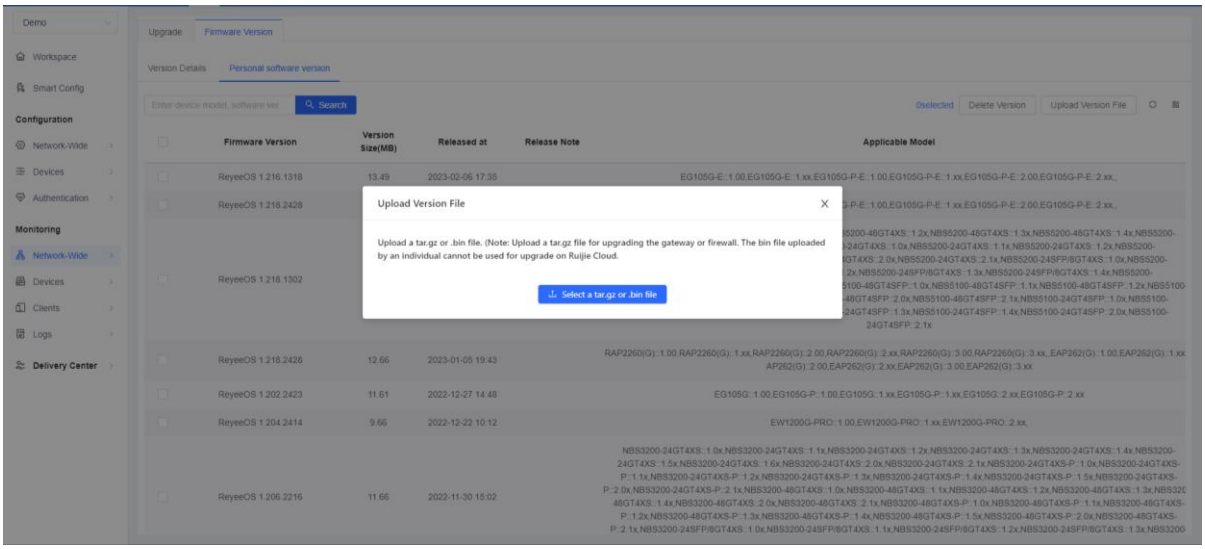
Select products to upgrade the software versions of the products in batches.

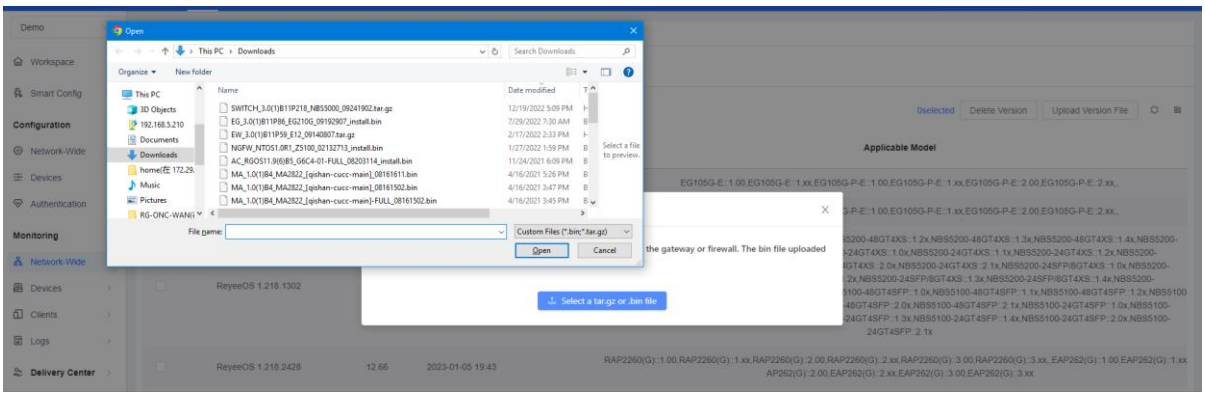


13.8.2 Firmware Version



This page lists device version files that are manually uploaded by users.



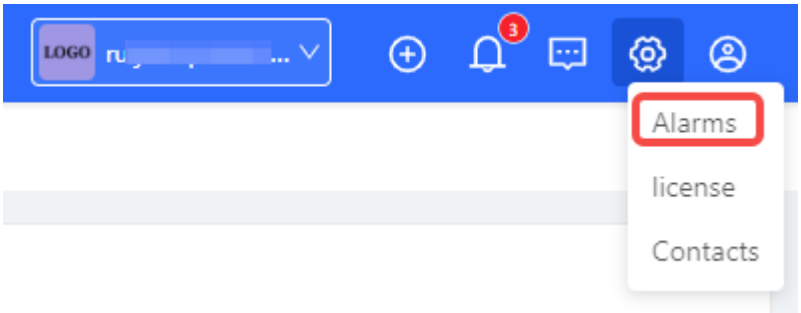


13.9 Configuring Alarms

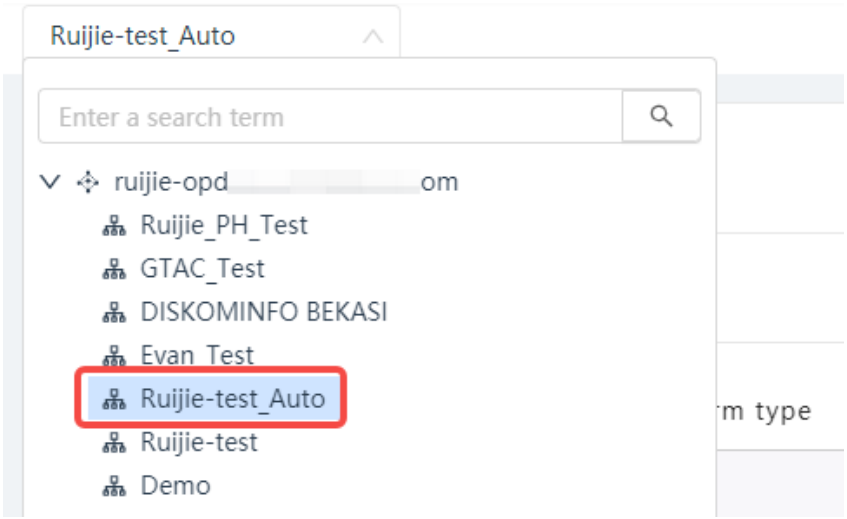
Click  at the upper right corner, and click **Alarm**. When no alarm is configured, global settings are used. On the **Alarm Settings** page, you can specify whether to enable or disable alarms and how the alarms should be received.

Procedure

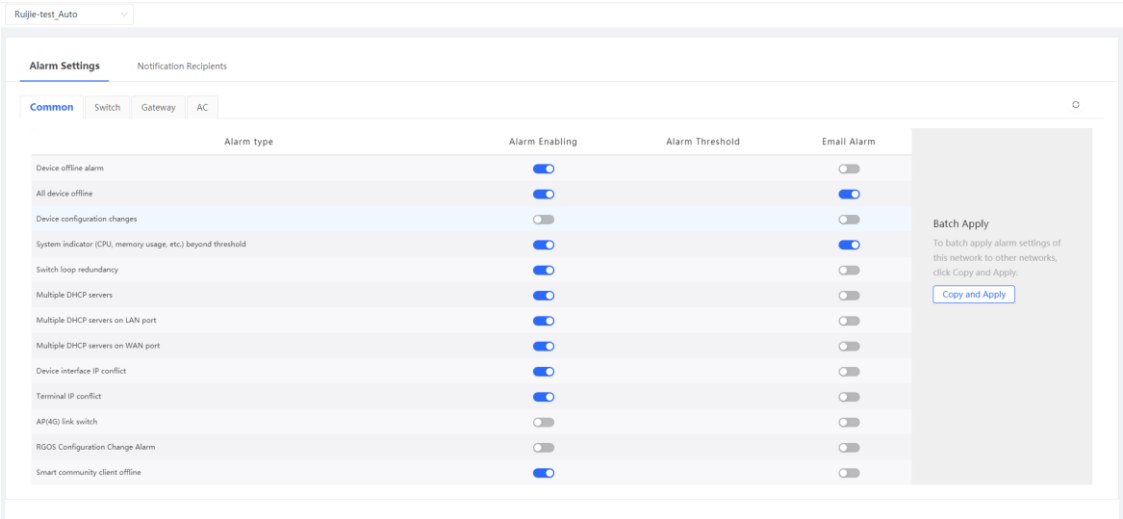
(1) Click  at the upper right corner and click **Alarm Settings**.



(2) Select one project in this account.



(3) Set alarm parameters.

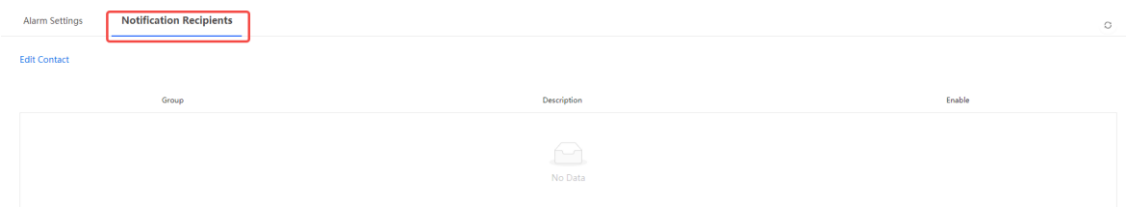


Type: indicates the type of alarms.

Alarm Enabling: 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.

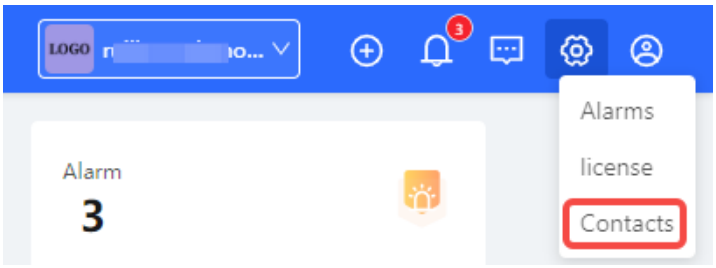
Email Alarm: indicates that alarms will be pushed to the contacts in **Contact Group List** of the network through the email when **Email Alarm** and **Status** are enabled.



13.10 Managing Contacts

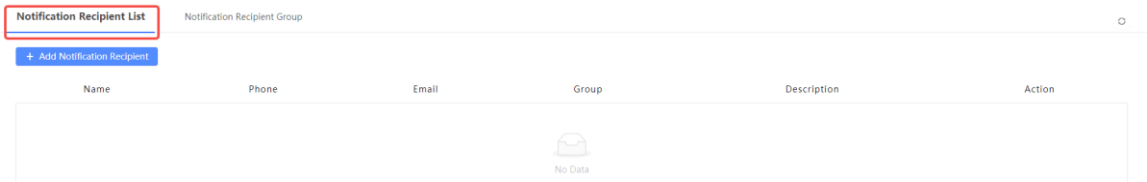
Procedure

Click ⚙ at the upper right corner, and click **Contact** to access **Notification Recipient List** and **Notification Recipient Group**.



- **Notification Recipient List**

  In the **Notification Recipient List** area, you can add contacts and contact groups that will receive the alarm emails.



  Name: displays the customized name of a recipient.

  Phone: displays the mobile number of a recipient.

  Email: displays the email address of a recipient.

  Group: indicates the group of a recipient.

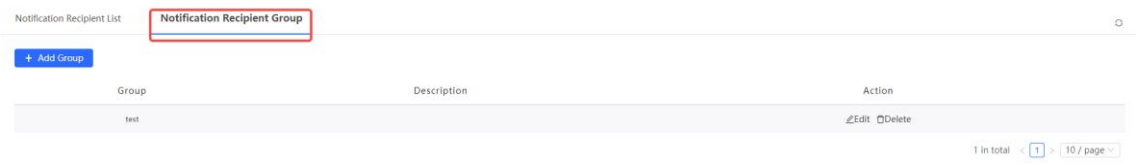
  Description: describes the recipient.

  Action: indicates the operation for the recipient. The value is **Edit** or **Delete**. After clicking **Edit**, you can edit recipient information in the displayed window.

  Add Notification Recipient: adds a recipient to the notification recipient list.

- **Notification Recipient Group**

  In the **Notification Recipient Group** area, you can add a group and move the recipients to the group.



  Group: displays the customized name of the group.

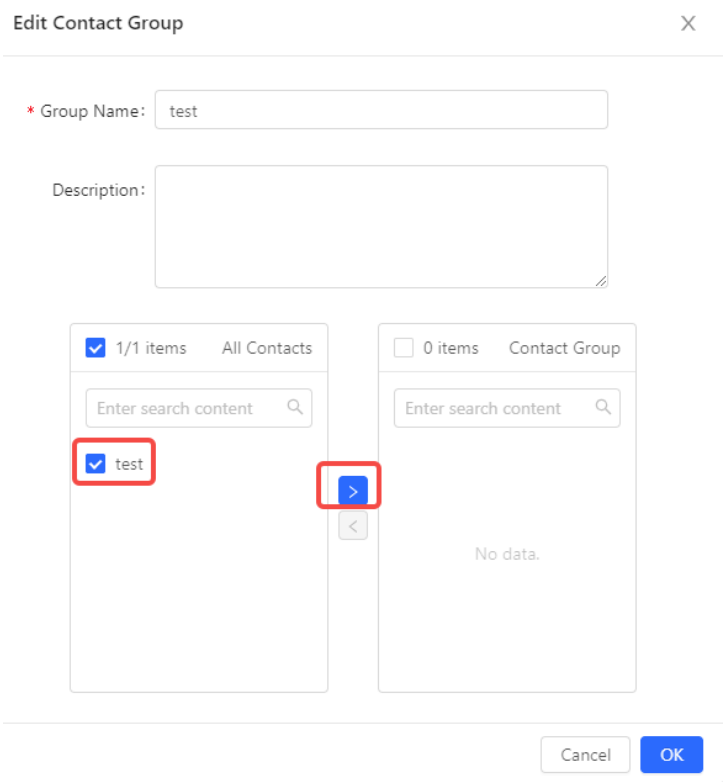
  Description: displays some words to describe the recipient group.

  Action: indicates the operation for the recipient group. The value is **Edit** or **Delete**.

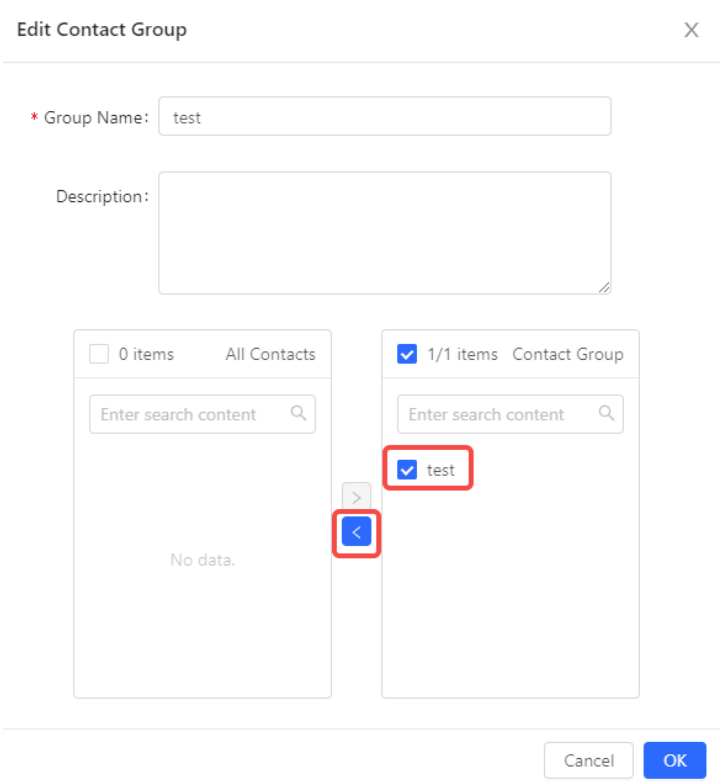
  Add Group: adds a recipient group to the notification recipient list.

  After clicking **Edit**, you can edit recipient group information in the displayed window. The value is **Add to Group** or **Delete from Group**.

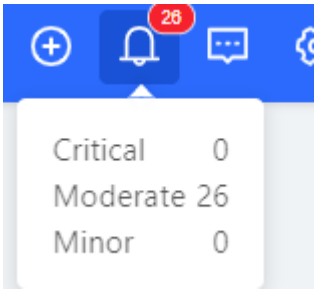
- **Add to Group**: adds the selected recipients to current group.



- **Delete from Group**: deletes the selected recipients from the current group.

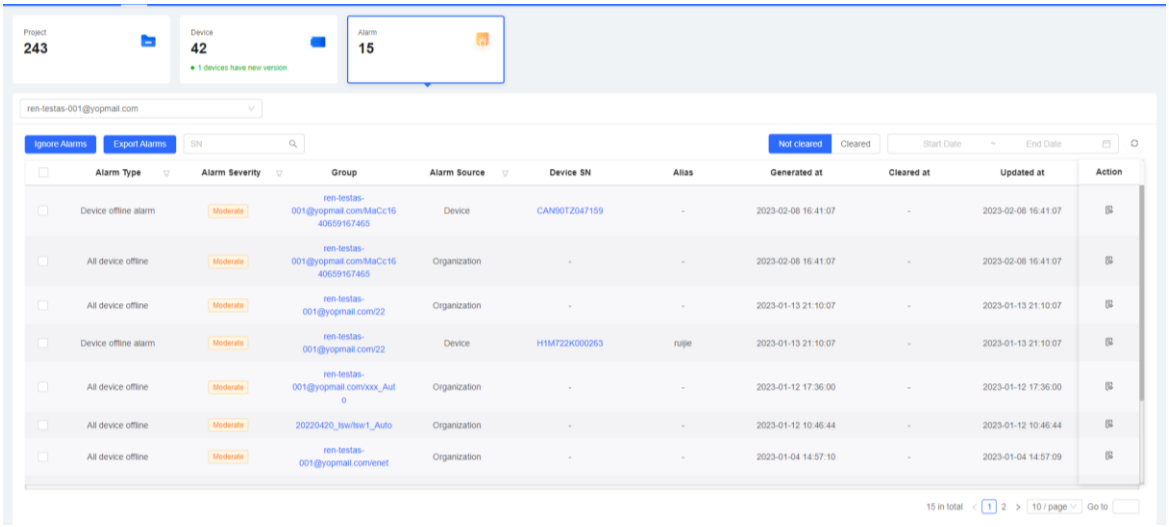


13.11 Viewing the Number of Global Alarms Quickly



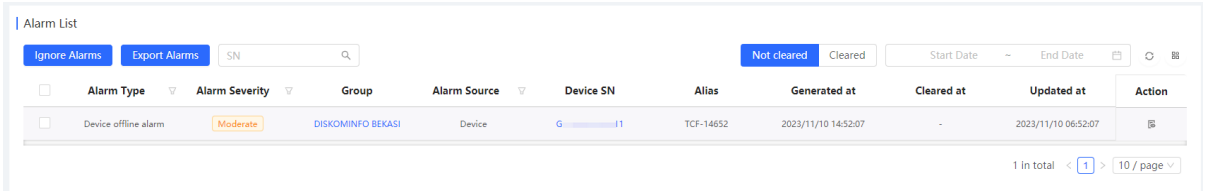
13.12 Viewing Details About Global Alarms

Click **Home** > **Alarm**



13.13 Viewing Alarms of a Project

Choose Project > Monitoring > Network-Wide > Alarm.



13.14 Layout

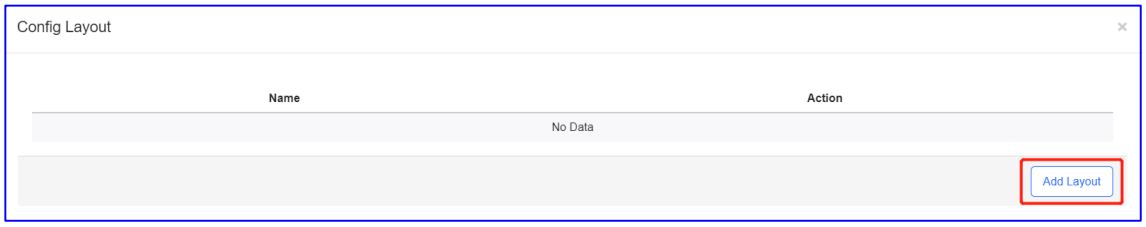
Layout is used to identify the AP location.

Procedure

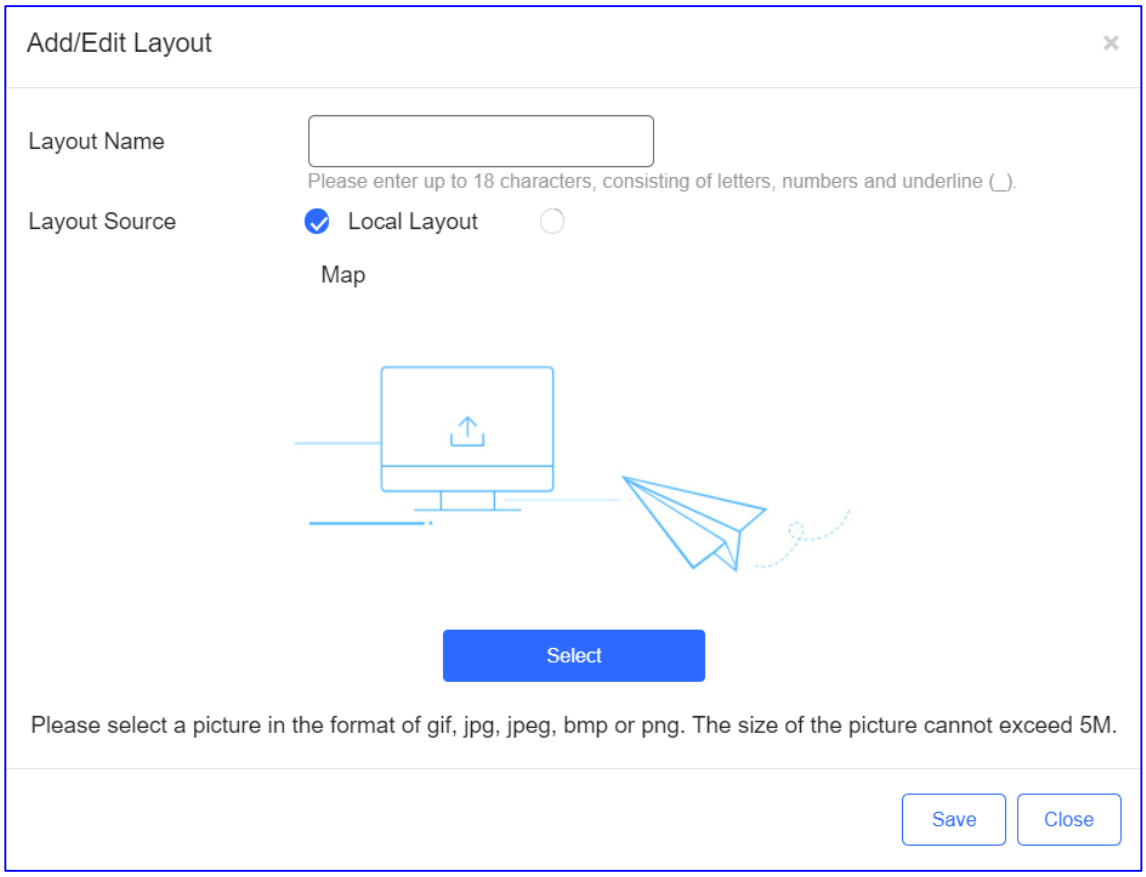
(1) Choose **CONFIGURATION** > **WIRELESS** > **Layout** and select a network in this account.

(2) Click **Config Layout** in the **Layout** area.

(3) Click **ADD Layout** on the **Config Layout** page.



(4) Set parameters of the layout and click **Save**.



Layout Name: Enter up to 18 characters, consisting of letters, numerals, and underlines (_).

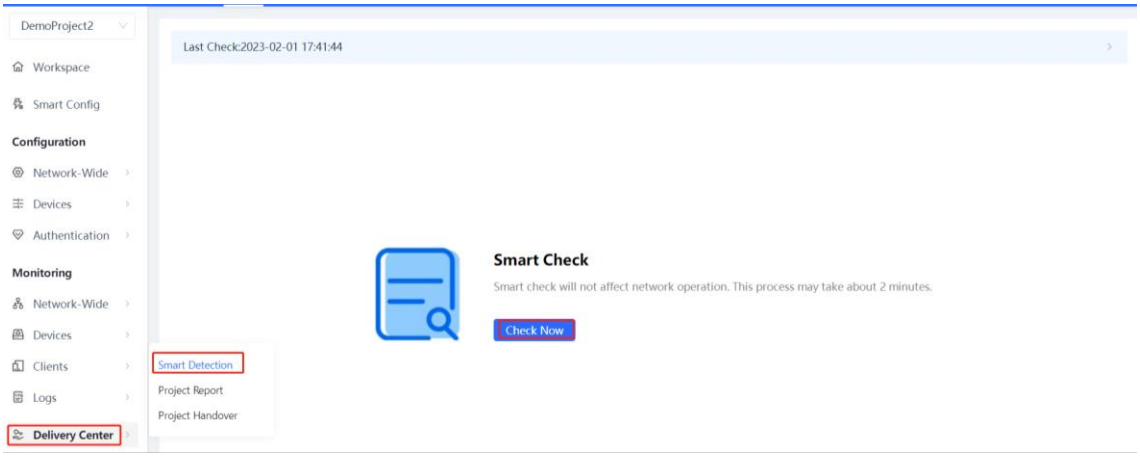
Layout Source: Select a local layout or map.

- **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**.

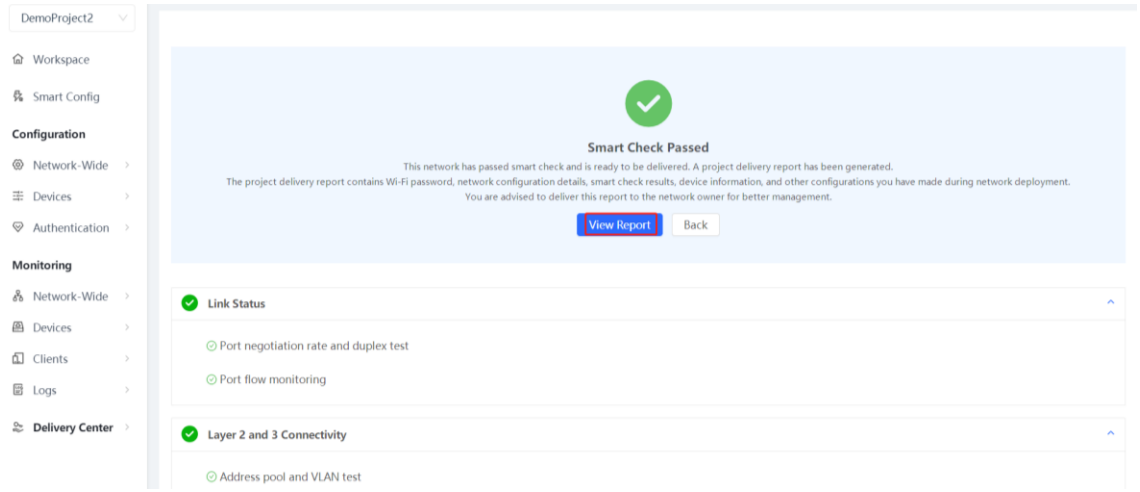
14 Delivery Center

14.1 Smart Detection

Choose **Delivery Center** > **Smart Detection** > **Check Now** to generate a project delivery report.



After a project delivery report is generated, click **View Report** to view the report.



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.

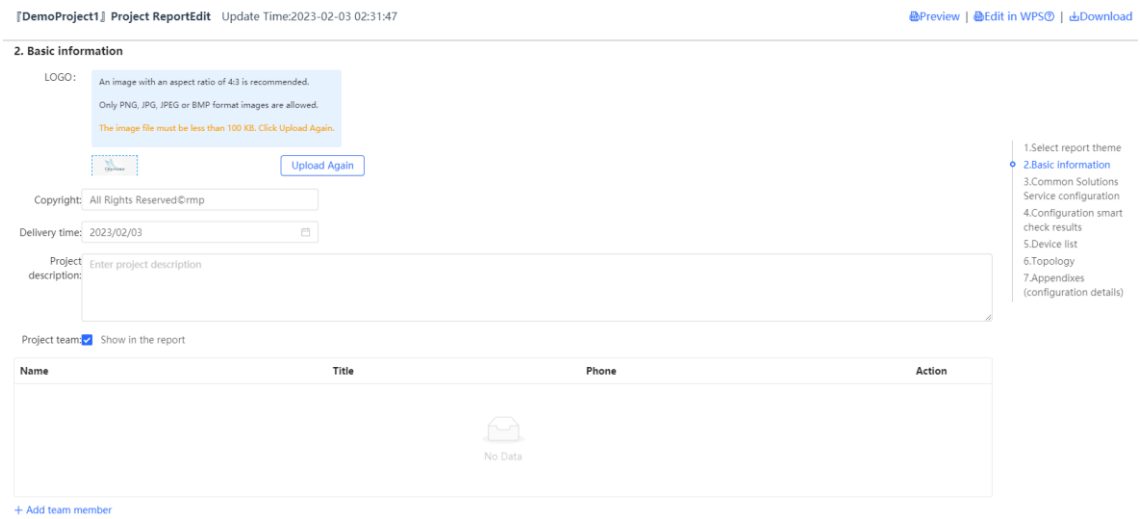
After the project deployment is completed, a report can be offered to the owner. The report can provide the revised project network device overview and delivery time, customized company logo, company name, and

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.

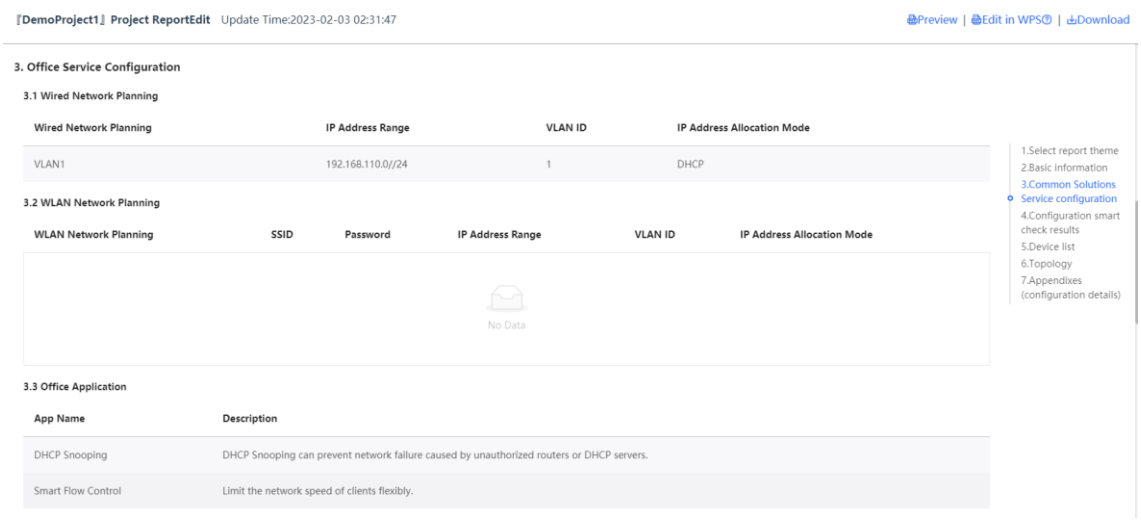
14.2.2 Configuration Steps

1. Choose **Project** > **Delivery Center** > **Project Report** to view the latest delivery report of the current project.

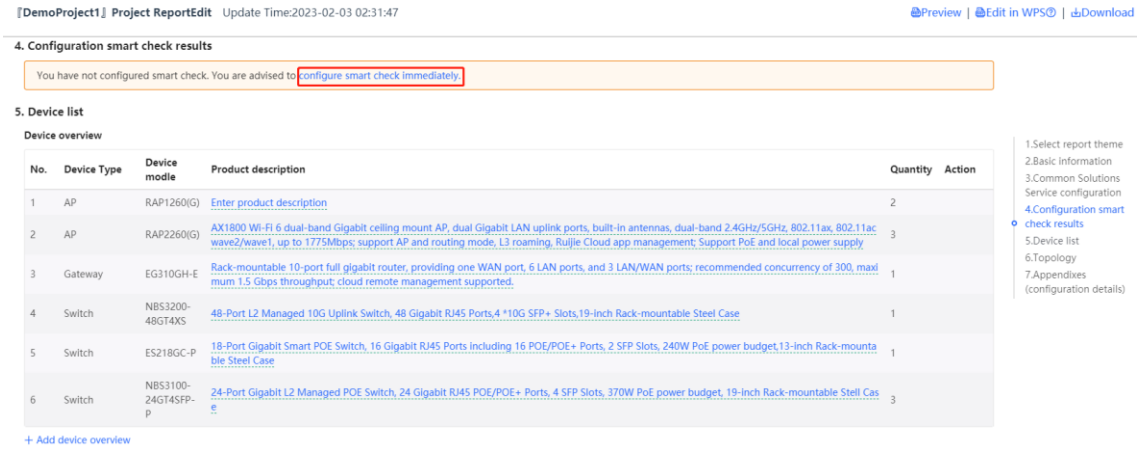
2. Click **Edit** at the upper right corner to edit basic information in the project report.



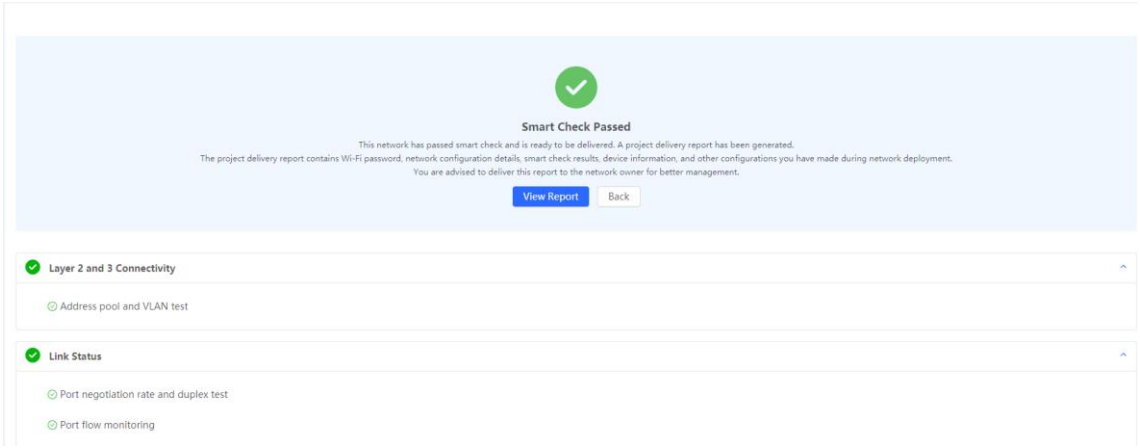
3. You can view service configuration of the general solution in the delivery report.



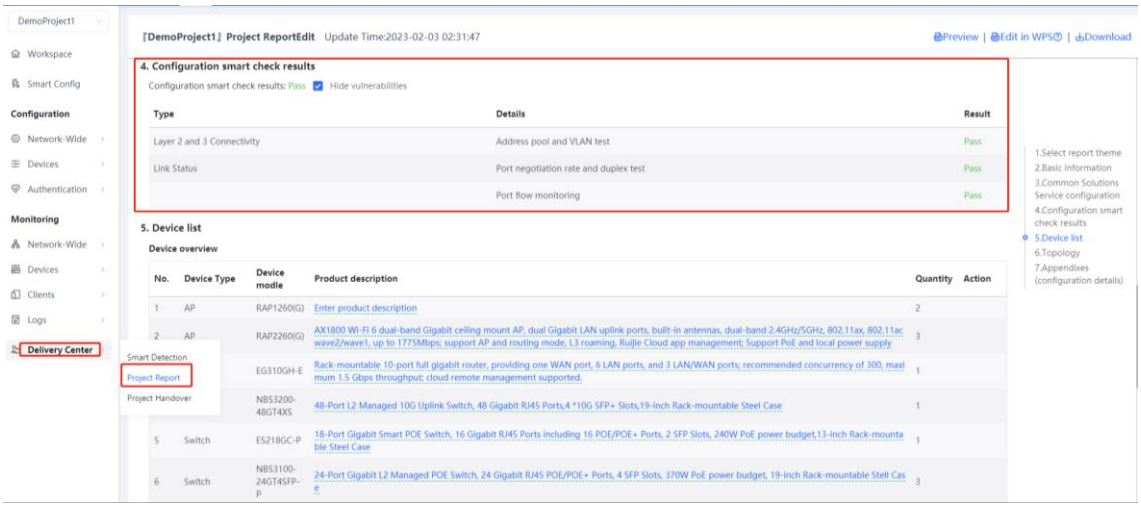
4. Checking the network intelligently: Click **Configure smart check immediately**. The page automatically redirects to **Smart Detection**.



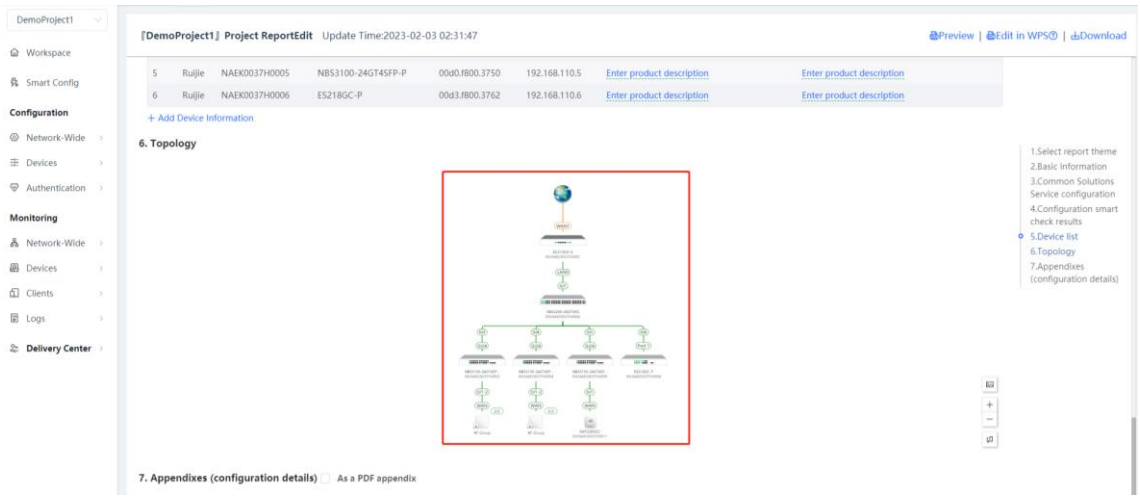
5. Click Check Now.



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.



7. Check the network topology.



8. Click **Download** at the upper right corner to download the delivery report in PDF and Word formats.

14.3 Project Handover

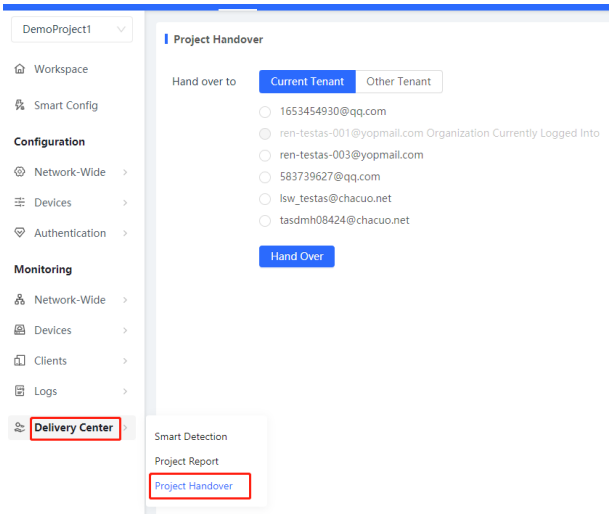
14.3.1 Applicable Scenarios

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.

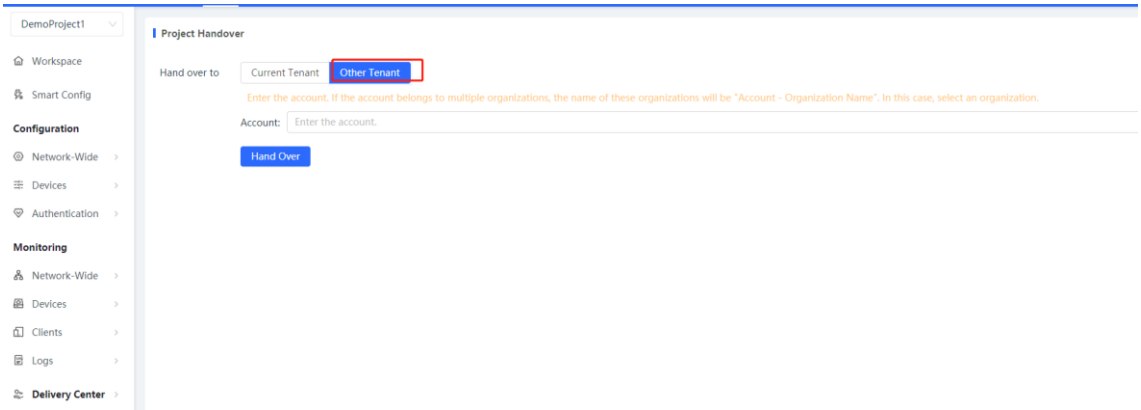
You can transfer your network (including devices on the network and device-related configuration) to other accounts. You can also share a network with other accounts. Read/write permission and read-only permission can be configured for sharing. The read-only permission is used for monitoring requirements 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**.



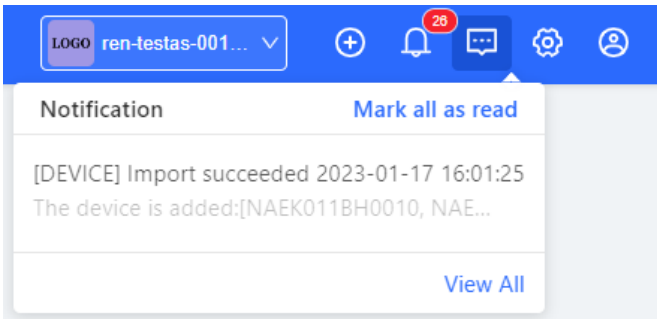
You can also click **Other Tenant**. Enter a complete account for search, select the target account, and hand the project over to the account.



15 Appendix: Frequently-Used Controls

15.1 Notification

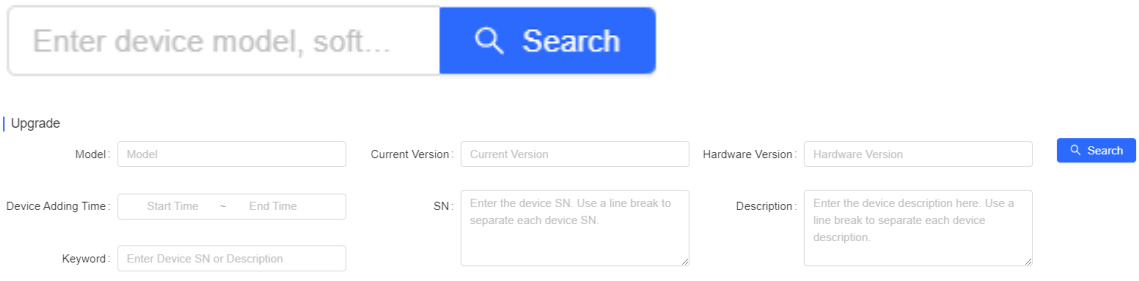
You can view device go-online and go-offline reminders.



15.2 Add

15.3 Delete

15.4 Quickly locate the table entry you want to find by entering keywords



15.5 Status

Disabled:  ; enabled:  . You can click it to switch the status.

15.6 Change Project Name or Password