Ruijie Reyee RG-EST, AirMetro Series Wireless Bridges

ReyeeOS 1.280 Configuration Guide

Document Version: V1.0
Date: 2024-05-06

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 names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

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

Conventions

1. Signs

The signs used in this document are described as below:

Danger

An alert that calls attention to safety operation instructions that if not understood or followed when operating the device can result in physical injury.

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.

2. Note

This manual provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors. It is intended for the users who have some experience in installing and maintaining network hardware. At the same time, it is assumed that the users are already familiar with the related terms and concepts.

Contents

.

1 Login

1.1 Configuration Environment Requirements

Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/Internet Explorer kernel-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.

1.2 Default Configuration

Table 1-1 Default Web Configuration

Item	Default Value
IP address	10.44.77.254
Username/Password	A username is not required on your first login. You can enter the initial password "admin" to log in, and directly start the configuration after login.

1.3 Logging In to Eweb on a PC

1.3.1 Connecting to the Device

You can open the management page and complete the bridge configuration only after connecting a PC to the bridge. You can connect a PC to the bridge in either of the following ways.

- Wired Connection

  Connect a local area network (LAN) port of the bridge to the network port of the PC, and set the IP address of the PC. See 1.3.2 Configuring the IP Address of the Management PC.

Note

Only RG-AirMetro550G-B, RG-EST100-E and RG-EST350 V2 have two LAN ports.

- Wireless Connection

  On a mobile phone or laptop, search for wireless network **@Ruijie-b***XXXX*. (XXXX is the last four digits of the MAC address of each device, and the MAC address can be found at the rear side of each bridge.) In this mode, you do not need to set the IP address of the management PC, and you can skip the operation in 1.3.2 Configuring the IP Address of the Management PC.

1.3.2 Configuring the IP Address of the Management PC

Configure an IP address for the management PC in the same network segment as the default IP address of the device (The default device IP address is 10.44.77.254, and the subnet mask is 255.255.255.0.) so that the management PC can access the device. For example, set the IP address of the management PC to 10.44.77.10.

Caution

The IP address of the management PC cannot be set to 10.44.77.253, because this IP address is reserved by the device. If the management PC uses this IP address, it cannot access the device.

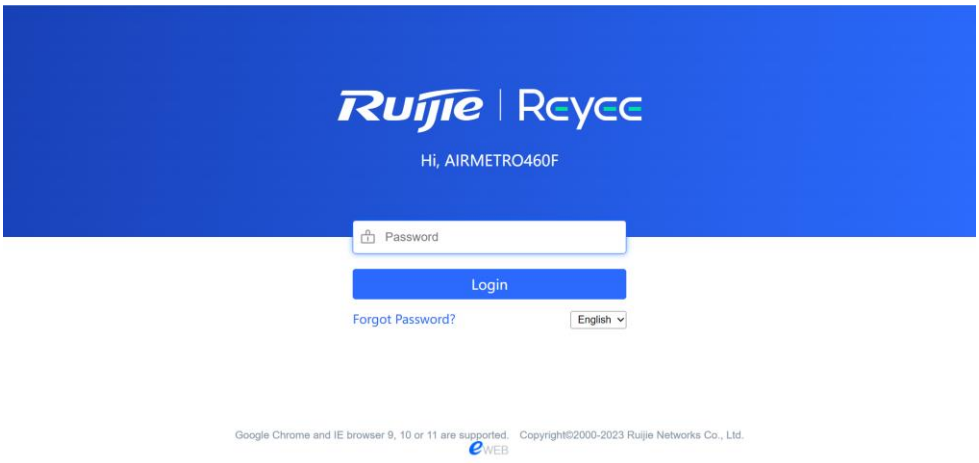
1.3.3 Logging in to the Web Page

(1) Enter the IP address (10.44.77.254 by default) of the bridge in the address bar of the browser to open the login page.

Note

If the static IP address of the device is changed, or the device obtains a new dynamic IP address, the new IP address can be used to access the web management system of the device as long as the management PC and the device are in the same network segment of a LAN.

(2) On the web page, enter the password and click **Login** to enter the web management system.



A username is not required on your first login. You can enter the initial password "admin" to log in, and directly start the configuration after login.

For device security, you are advised to set the management password after your first login to the web management system. After the password is set, you need to enter the password when you log in to the web management system again.

The login page will be locked for 60 seconds if you enter incorrect passwords multiple times. You can press and hold the Reset button on the device for more than 10 seconds when the device is powered on to restore it to factory settings. After the restoration, you can use the default IP address and password for login.

Caution

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

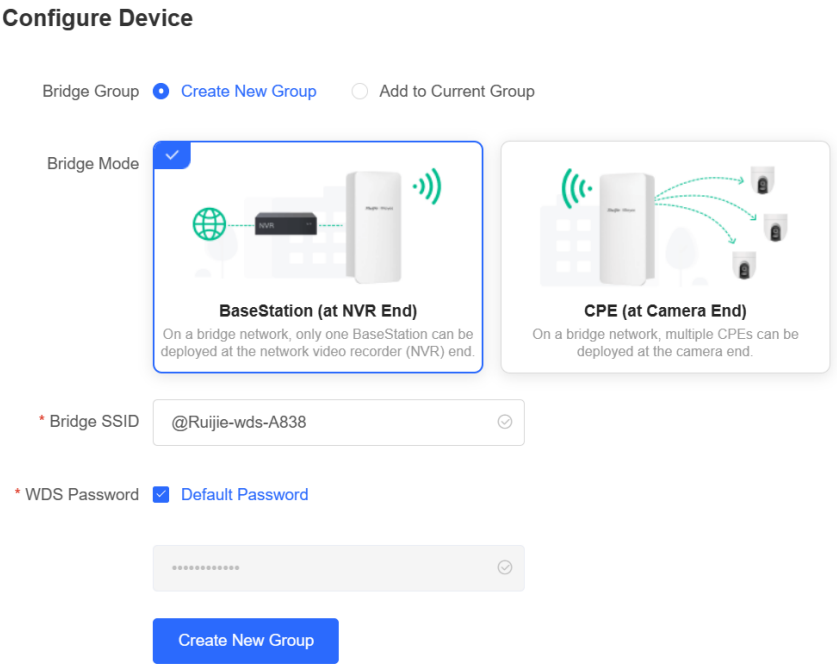
1.3.4 Configuring the Wireless Bridge

Note

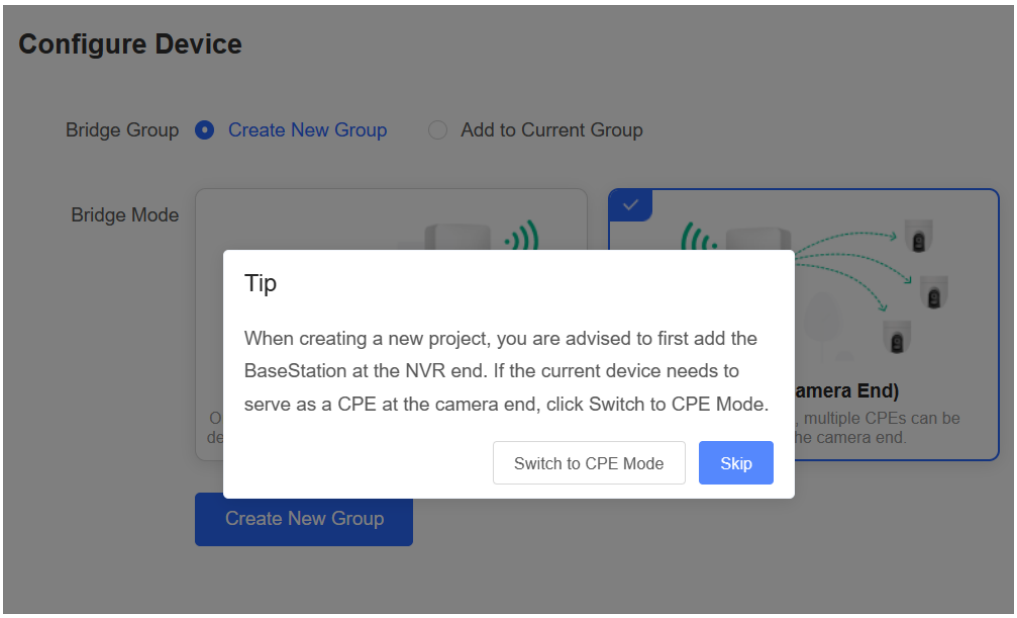
The configuration page is displayed only after the wireless bridge is restored to factory settings.

1. Create a bridge group

If the **Bridge Mode** is set to **BaseStation(at NVR End)**, click **Create New Group** to access the configuration page.

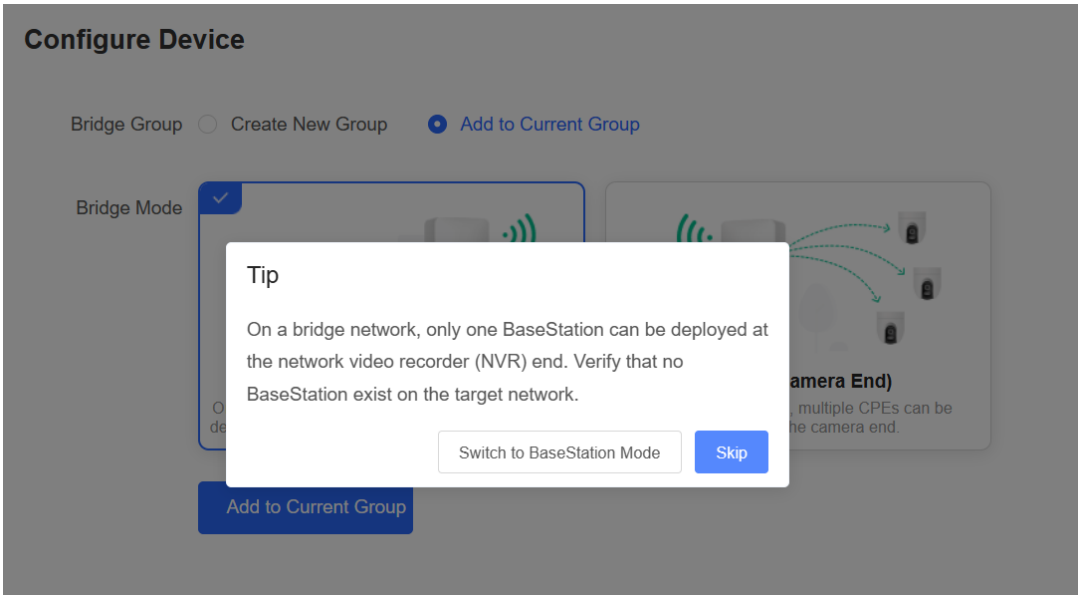


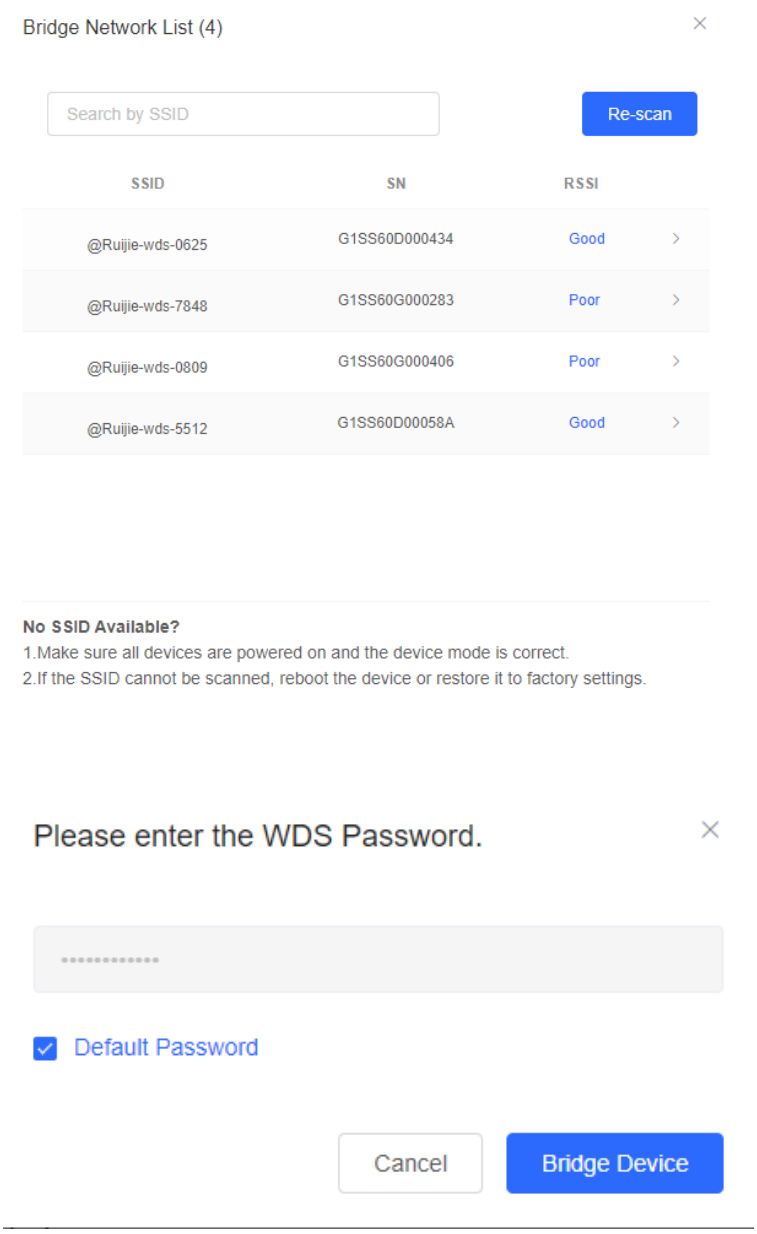
If the **Bridge Mode** is set to **CPE (at Camera End)**, a pop-up window is displayed. Click **Switch to CPE Mode** to proceed.



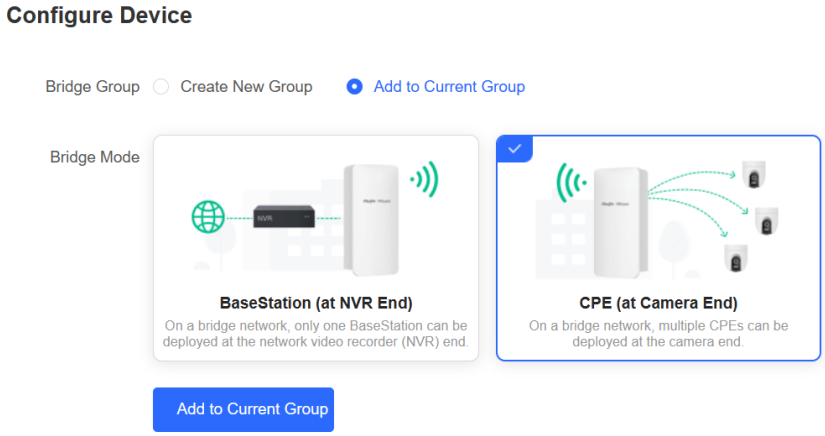
2. Add to the current group

Set the **Bridge Group** to **Add to Current Group**, and select the bridge mode as required. If **BaseStation (at NVR End)** is selected, click **Switch to BaseStation Mode** on the pop-up window, and then click **Add to Current Group** to proceed.





If CPE (at Camera End) is selected, then click Add to Current Group to proceed.


Configure Device
Bridge Group
Create New Group
Add to Current Group
Bridge Mode
NVR
BaseStation (at NVR End)
On a bridge network, only one BaseStation can be deployed at the network video recorder (NVR) end.
CPE (at Camera End)
On a bridge network, multiple CPEs can be deployed at the camera end.
Add to Current Group

2 Wi-Fi Network Settings

2.1 Overview

2.1.1 BaseStation and CPE

Wireless bridges purchased in pairs can be automatically paired after power-on. The wireless bridge also supports manual pairing by connecting to the Wi-Fi signal broadcast by another bridge. For details, see 2.3 Scanning to Pair and Add Devicess. In a paired WDS group, bridges can work in BaseStation or Customer Premises Equipment (CPE) mode.

- **BaseStation**: A bridge sending bridging signals is generally connected to the NVR end in a surveillance room. A WDS group can contain at most one BaseStation.
- **CPE**: A bridge that enables customers to access ISP's communication services is generally connected to the camera end. A WDS group can contain multiple CPE.

2.1.2 WDS Wi-Fi and Management Wi-Fi

- **WDS Wi-Fi**: A BaseStation broadcasts the WDS Wi-Fi signal. A CPE accesses the WDS Wi-Fi and upload videos or other data to the BaseStation.
- **Management Wi-Fi**: Both the BaseStation and the CPE can broadcast a dedicated management Wi-Fi network for device management purposes. You can connect to this network to configure and manage your devices.

2.2 Switching Between BaseStation Mode and CPE Mode

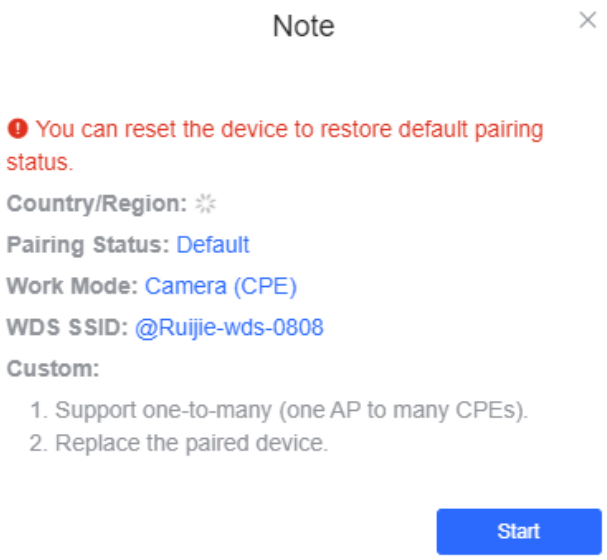
Note

The CPE functions are available only when the wireless bridge switches from the BaseStation mode to the CPE mode.

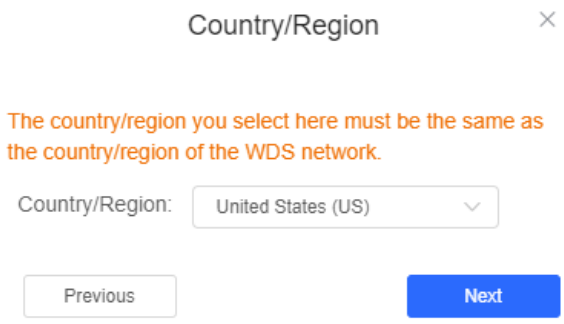
If the original BaseStation fails, you need to set the new device to BaseStation mode to replace the faulty device. If multiple CPE are required, a newly added device joining the WDS group must be switched to CPE mode.

(1) You can check the current mode in the upper right corner of the web page and click **Pair Again** to switch the mode.

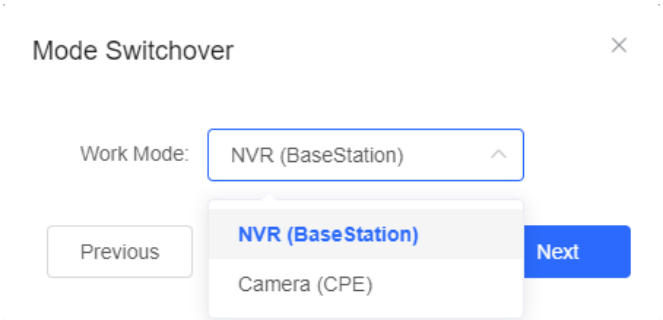
(2) In the displayed dialog box, click **Start**.



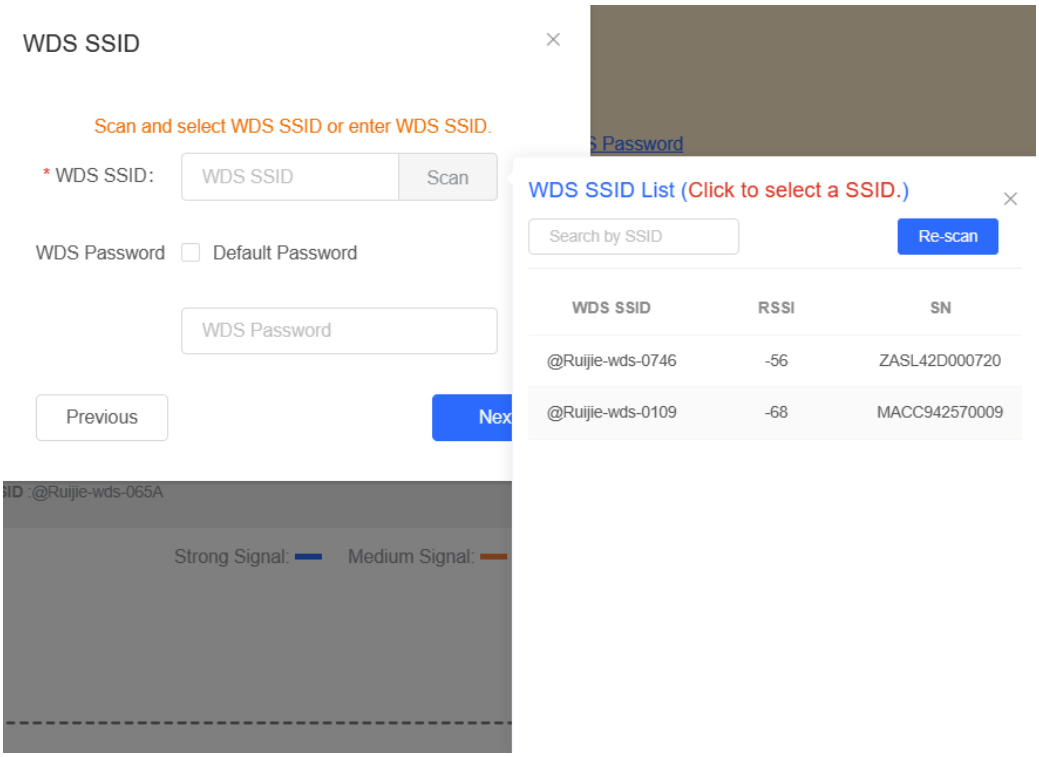
(3) Click **Next**.



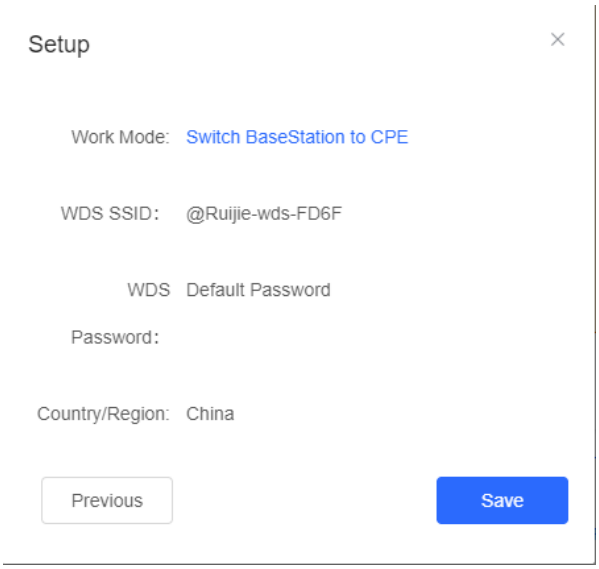
(4) Select a mode from the **Work Mode** drop-down list.



(5) Click **Scan**. A list of camera (CPE) is displayed. Select the target camera (CPE), enter the WDS password, and click **Next**.



(6) Verify the settings on the **Setup** page. Then, click **Save**.



Caution

Switching the mode will reboot the device. Therefore, exercise caution when performing this operation.

2.3 Scanning to Pair and Add Devices

2.3.1 Overview

When a wireless bridge is added to a WDS group or connected to another wireless bridge, you can scan the surrounding wireless bridges, compare their models, serial numbers, and other information, and then select the bridging target.

2.3.2 Configuration Steps

Choose **Home** > **Add Device**.

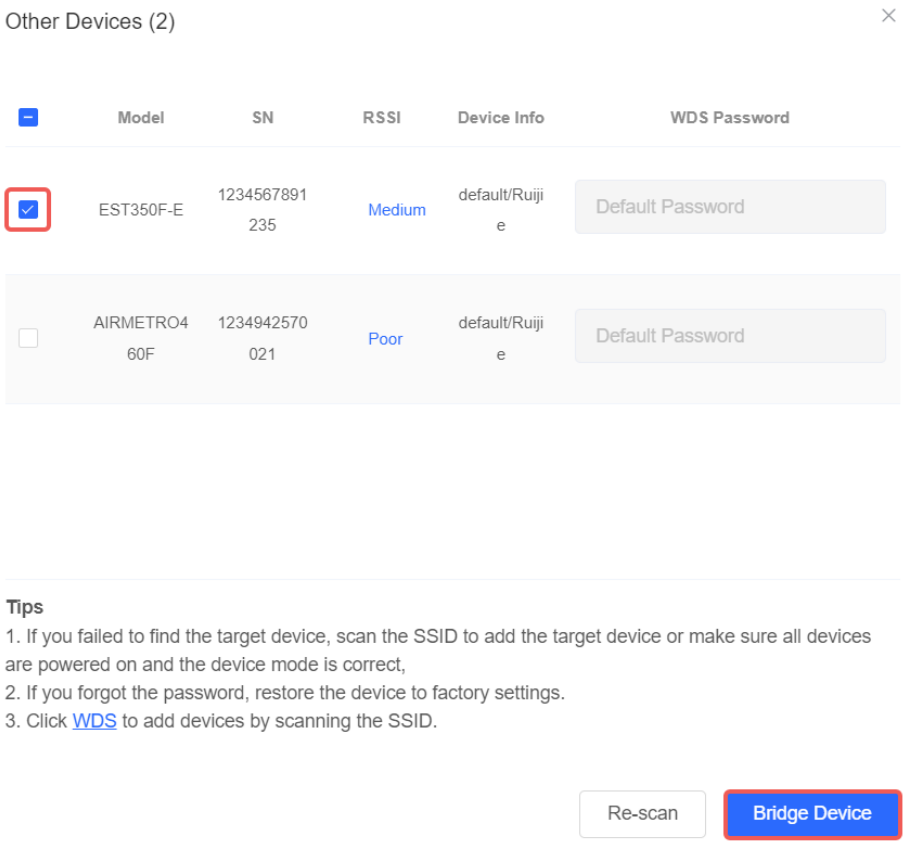
1. Scanning Surrounding Devices

Go to the home page and click **Add Device**.

2. Selecting a Device for Pairing

Select the desired device, enter the bridging password in the **WDS Password** field, and click **Bridge Device**. The selected device will be bridged.

If no device is displayed, click **Re-scan**.

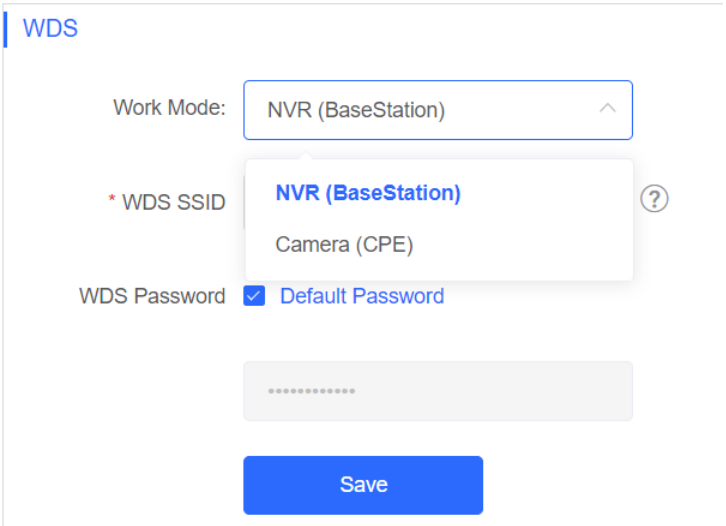


2.4 Configuring the WDS Wi-Fi for a Single BaseStation or CPE

2.4.1 Configuring the Work Mode

Choose **Wireless > WDS**.

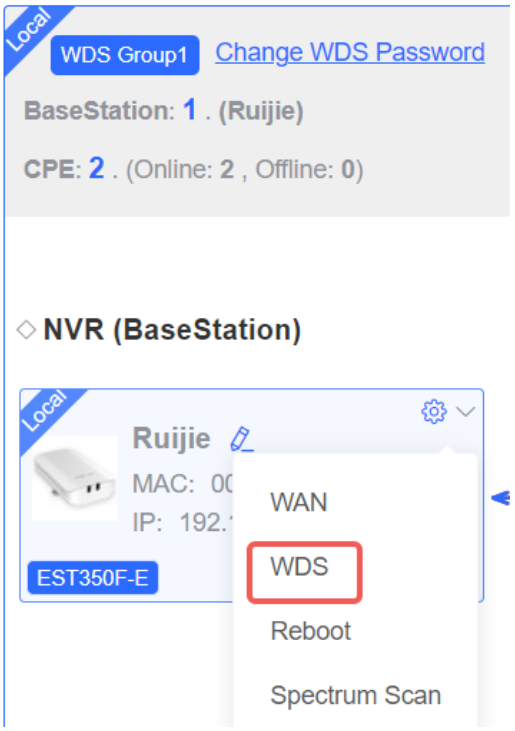
Select the work mode as **NVR (BaseStation)** or **Camera (CPE)**.



2.4.2 Setting the WDS SSID

Go to the configuration page:

- Method 1: Choose **Wireless > WDS**.
- Method 2: Choose **Overview > WDS Group Info > WDS**.



To prevent network exceptions, you are advised to keep the default WDS SSID unless otherwise specified.

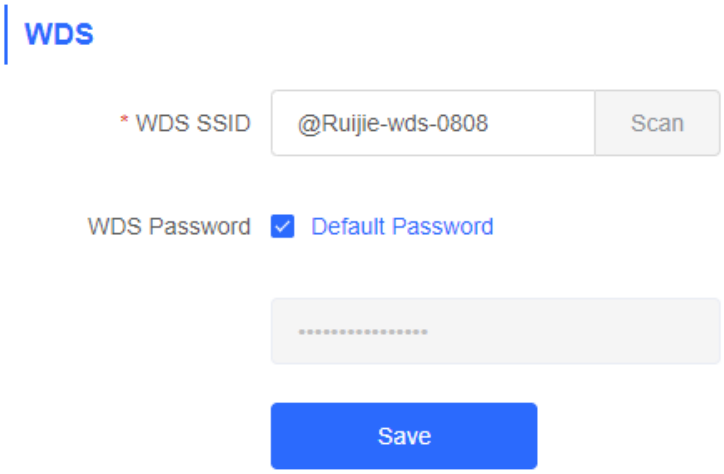
If a new WDS SSID is set for a device in a WDS group, other bridges in the group need to change to the new SSID as well to connect with this device.

When a new device is connected, you can either configure a new WDS SSID or click **Scan** to select a target WDS SSID.

To check the WDS SSIDs of WDS groups, choose **Overview** > **WDS Group Info**. For details, see 2.9 Displaying WDS Group Information.

Caution

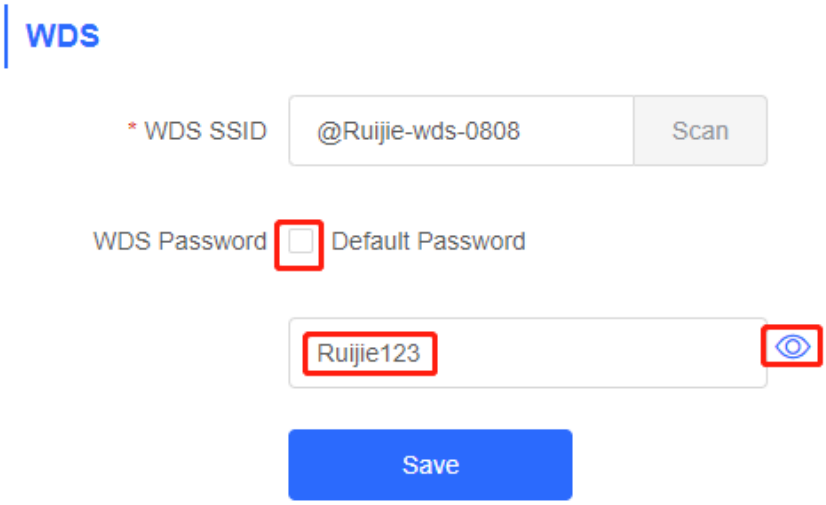
Configuring a WDS SSID will disconnect the WDS link. Incorrect WDS SSID will cause a WDS connection failure. Therefore, exercise caution when performing this operation.



2.4.3 Configuring the WDS Password

Choose **Wireless** > **WDS** > **WDS**.

A correct WDS password is required for a successful WDS link. To prevent unauthorized devices from connecting to the WDS Wi-Fi network, high-security passwords are used for devices by default, and the password for devices of the same model is the same. You are advised to change the password for devices in the entire network or in a WDS group to prevent others from accessing the network using a device of the same model.



Caution

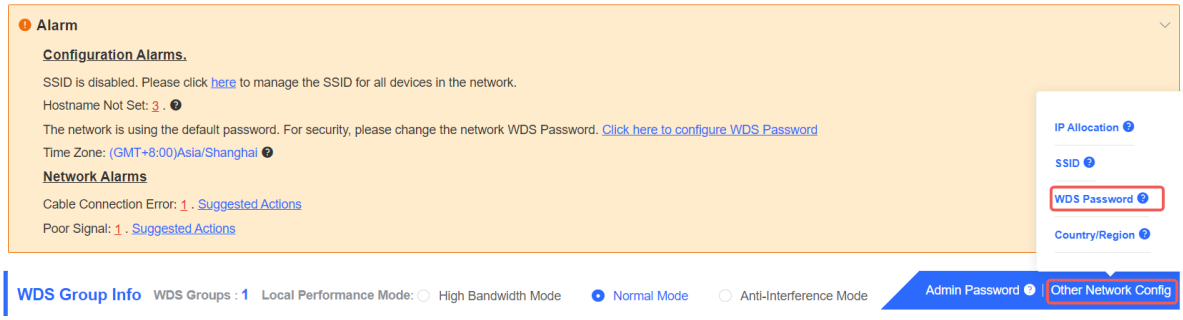
- WDS passwords can be configured only for CPE devices, and not for the BaseStation.
- Configuring a WDS password will disconnect the WDS link. An incorrect WDS password will cause a WDS connection failure. Therefore, exercise caution when performing this operation.

2.4.4 Saving the Settings

After changing the WDS SSID or password, click **Save** to activate settings at once.

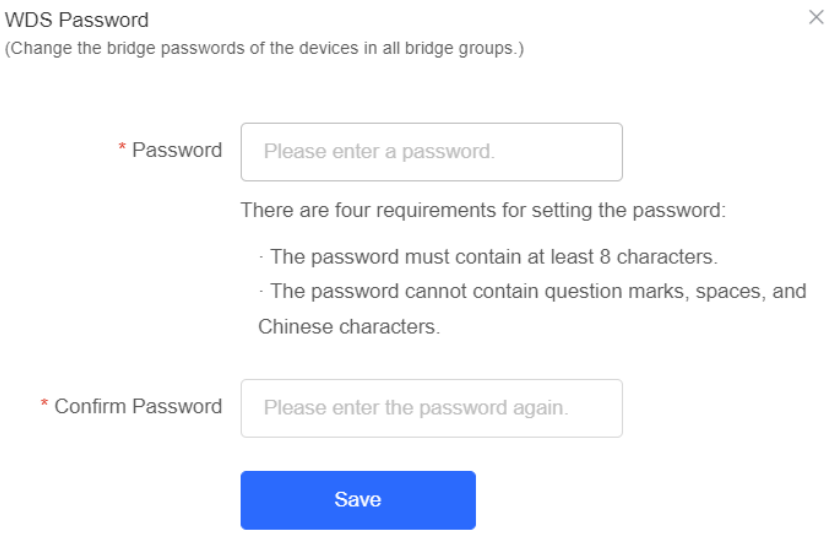
2.5 Configuring the WDS Password for a LAN

Choose **Overview** > **Other Network Config** > **WDS Password**.



Click **WDS Password**, enter the password in the displayed dialog box, and click **Save**.

Hover the cursor over to view the help information.



Caution

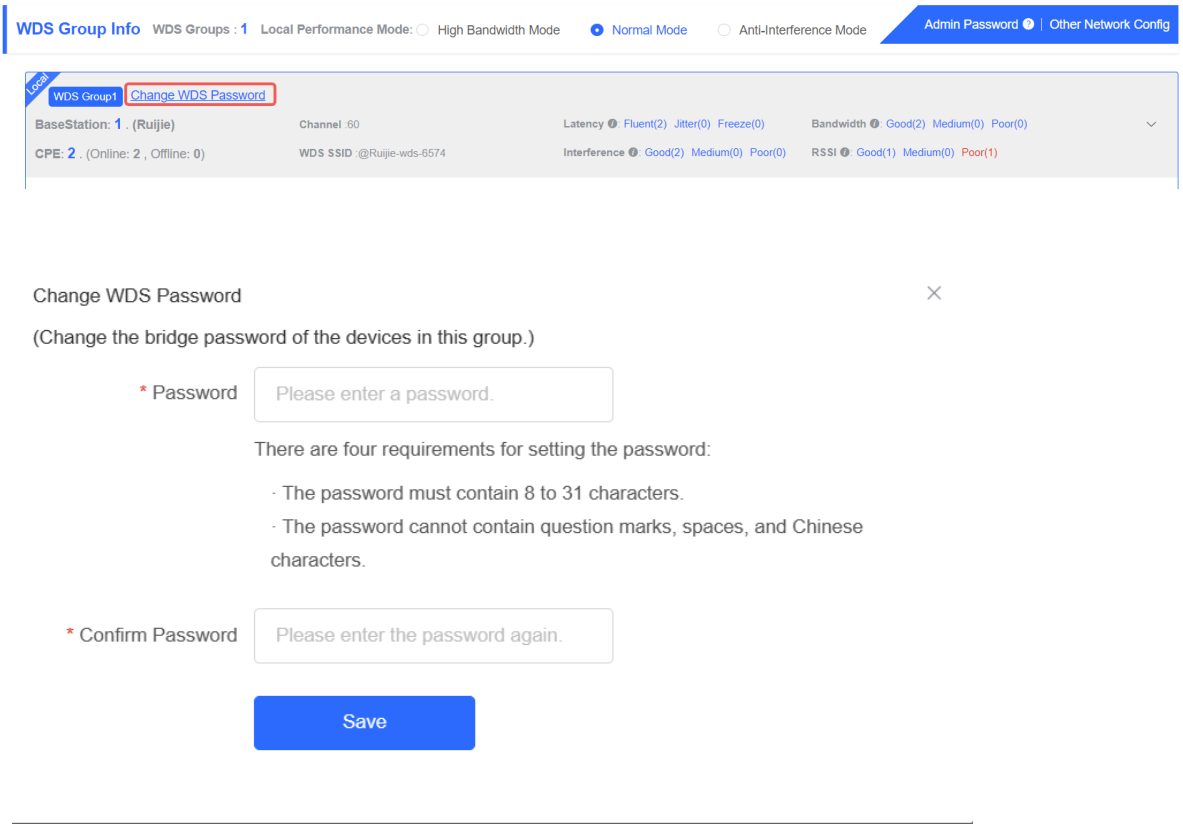
- When configuring the WDS password for the entire network, ensure that all devices in the network are online. Otherwise, the WDS passwords of the devices will be inconsistent.
- Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation.
- If there is an unbridged device in the network, the WDS password cannot be configured.

2.6 Configuring the WDS Password for a WDS Group

Choose **Overview** > **Change WDS Password**.

The default WDS password of devices is the same. Changing the WDS password can prevent others from illegally accessing the user network by using a device of the same model.

When configuring the WDS password for bridges in the entire network is unavailable or unnecessary, you can click **Change WDS Password** to configure the WDS password for bridges in the WDS group. If there is an unbridged device in the group, the **Change WDS Password** function will be unavailable.



Caution

When configuring the WDS password for a WDS group, ensure that all devices in the group are online. Otherwise, WDS passwords of the devices will be inconsistent.

Configuring the WDS password for a WDS group will reconnect devices in the group. Therefore, exercise caution when performing this operation.

If there is an unbridged device in the WDS group, this function will be unavailable.

2.7 Configuring the Management Wi-Fi for a Single BaseStation or CPE

Choose **Wireless > Manage SSID**.

Note

The management SSID is used only for accessing the web interface and managing devices. It cannot be used for Internet access, and is isolated from the service network.

2.7.1 Selecting the Work Mode

1. Default Configuration

When Default Settings is selected, the management SSID of the device will automatically be hidden after 2 hours, making it inaccessible for connection.

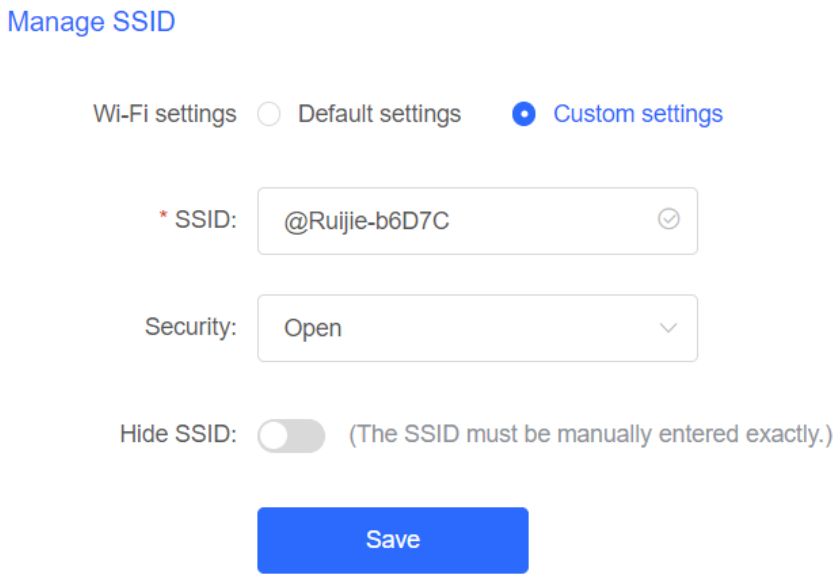
2. Custom Configuration

SSID: Indicates the Wi-Fi name to which the mobile phone or management PC connects for access.

Security: The options include **Open**, **WPA-PSK**, **WPA2-PSK**, and **WPA_WPA2-PSK**. You are advised to choose **WPA_WPA2-PSK** and set a password for security purpose.

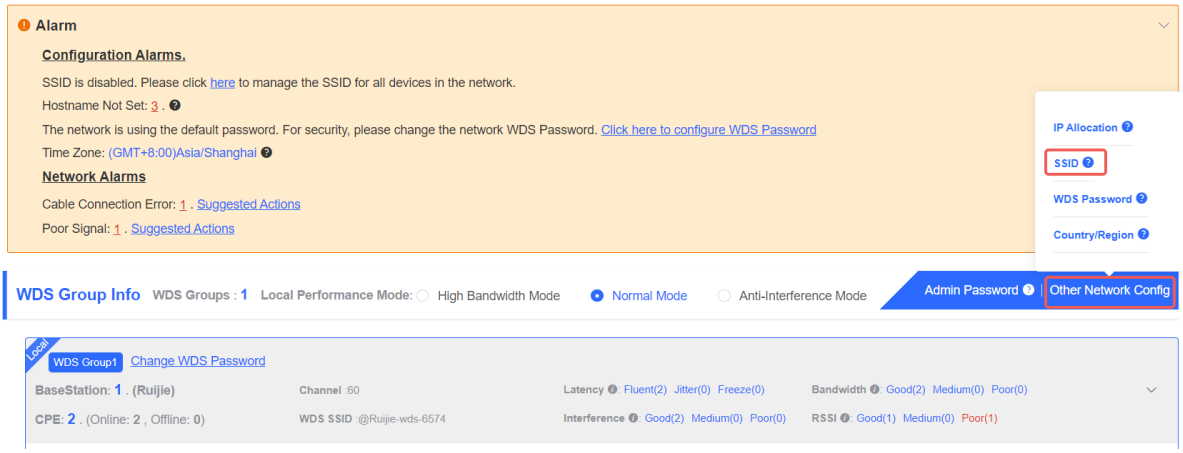
Hide SSID: When the **Hide SSID** switch is toggled on, mobile phones or PCs cannot discover the SSID. You need to manually enter the SSID and password for access. This can prevent the SSID from being accessed by unauthorized users.

You can view the network-wide management SSID for each bridge group at **Overview** > **Other Network Config** > **SSID**. For details, see2.8 Configuring the Management Wi-Fi and Password for a LAN.



2.8 Configuring the Management Wi-Fi and Password for a LAN

Choose **Overview** > **Other Network Config** > **SSID**.



Note

The management SSID is used only for accessing the web interface and managing devices. It cannot be used for Internet access, and is isolated from the service network.

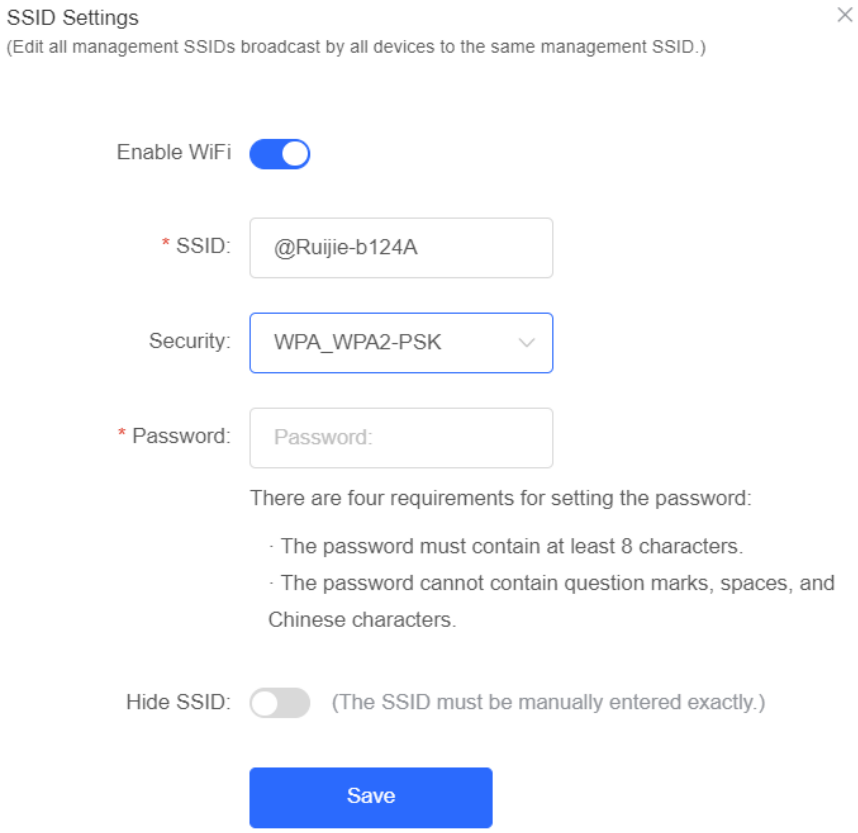
The default SSID for device management is @Ruijie-bXXXX. (XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with each device.) Click **SSID** on the page to set the same management SSID and password for all bridges in the LAN.

Enable Wi-Fi: Choose whether to enable the management Wi-Fi for all devices in the network.

SSID: The SSID is the name of the management Wi-Fi network.

Security: The options include **Open**, **WPA-PSK**, **WPA2-PSK**, and **WPA_WPA2-PSK**. You are advised to choose **WPA_WPA2-PSK** and set a password for security purpose.

Hide SSID: When the **Hide SSID** switch is toggled on, mobile phones or PCs cannot discover the SSID. Users need to manually enter the SSID and password for access. This can prevent the SSID from being accessed by unauthorized users.



Caution

After the configuration is saved, the BaseStation and CPE devices in the network will be reconnected. Therefore, exercise caution when performing this operation.

2.9 Displaying WDS Group Information

Choose **Overview** > **WDS Group Info**.

Displayed WDS group information includes the number of Base Stations and CPE in the group, current working channel, SSID, latency, interference, wireless bandwidth and quality, RSSI and quality, data rate, real-time traffic, and uptime. Hover the cursor over to view the detailed information of every item.

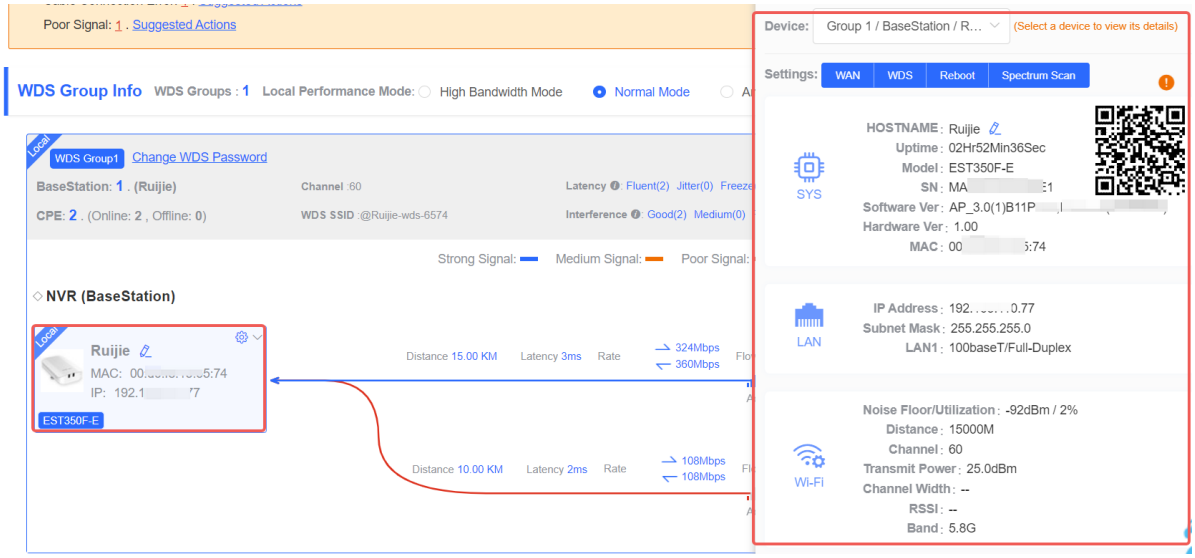
Note

BaseStation is at the NVR end, while CPE is at the camera end.

2.10 Displaying the Information About a Bridge

Choose **Overview** > **WDS Group Info** > **NVR (BaseStation)** or **Camera (CPE)**.

Click the  icon of a device to display the basic information about the device in the right panel of the page, including the hostname, uptime, online status, model, SN, MAC address, software and hardware versions, IP address, subnet mask, LAN port status, noise floor/utilization, distance, channel, transmit power, channel width, RSSI, and band.



Note

The device at the NVR end does not involve channel width and RSSI, and only the device at the camera end does.

2.11 Configuring the Country/Region Code for a Bridge

2.11.1 Getting Started

The country/region code switch will take effect on a single device. Configuring the country/region code for a single device in bridging state will result in bridge disconnection. For network-wide country/region code configuration, please refer to 2.12 Setting the Country/Region Code for a WDS Group for details.

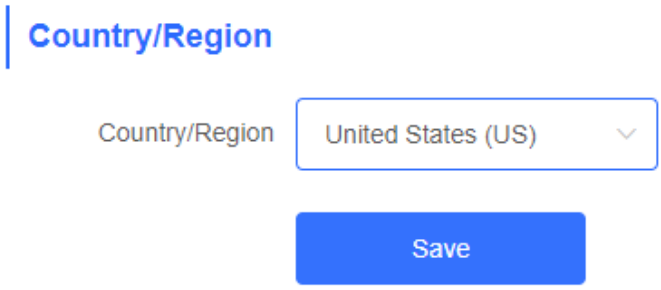
Caution

If you change the country/region code in the case of device disconnection, WDS connection may fail.

2.11.2 Configuration Steps

Choose **Wireless** > **Country/Region** > **Country/Region**.

Choose the target country/region from the drop-down list, and click **Save**.



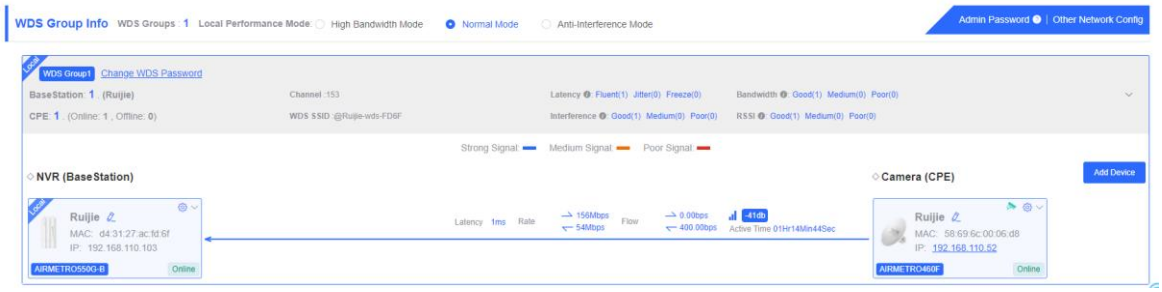
Caution

- After the country/region code is changed, the Wi-Fi network will restart, and the BaseStation and the camera will be reconnected after the Wi-Fi network is restarted.
- The current channel may be switched to **Auto** because it is not supported by the country/region. Therefore, exercise caution when performing this operation.

2.12 Setting the Country/Region Code for a WDS Group

2.12.1 Getting Started

The country/region code switch will take effect on all devices on the network, including those listed on the homepage of the web interface. Therefore, before configuring the country/region code, you are advised to go to the homepage and check whether the target devices are on the current network and their bridging status is normal.

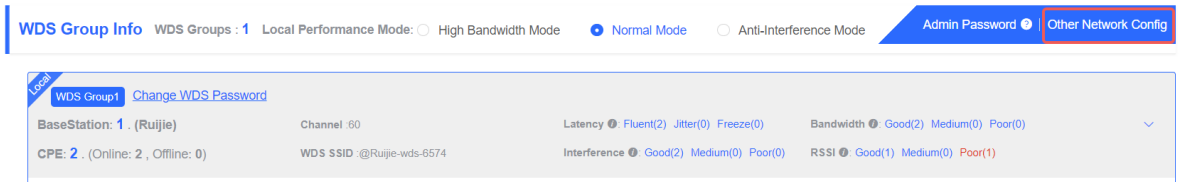


Caution

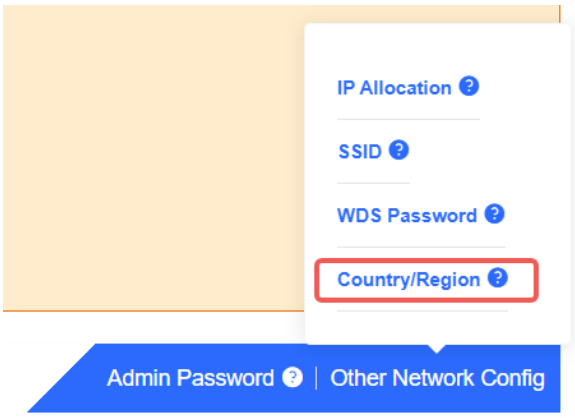
If the target device is not on the network or if the bridge is disconnected during the country/region code switch, it may lead to the device being unable to bridge properly.

2.12.2 Configuration Steps

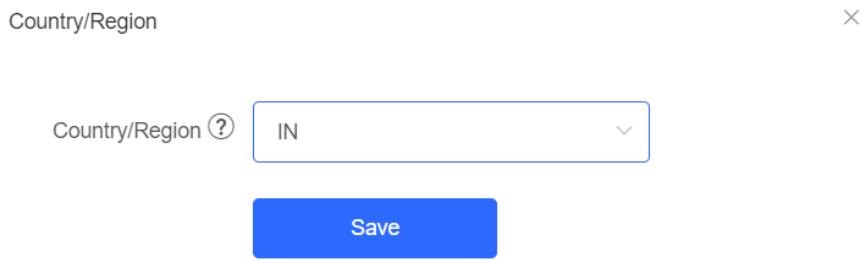
Choose **Overview > WDS Group Info > Other Network Config**.



(1) Click **Country/Region**.



(2) After setting the country/region code, click **Save**.



2.13 Setting the SSID for a Single Bridge

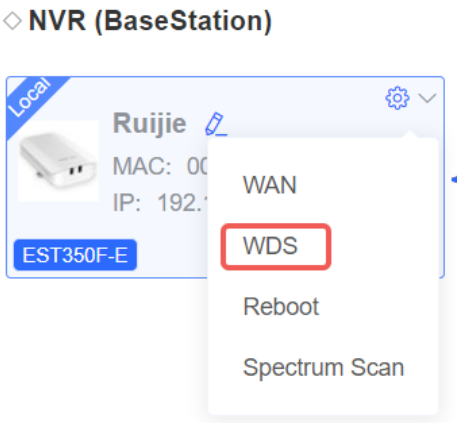
2.13.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network freezing caused by wireless environment changes cannot be prevented. You can also analyze the wireless environment around the bridge and manually select appropriate parameters.

2.13.2 Getting Started

Go to the configuration page:

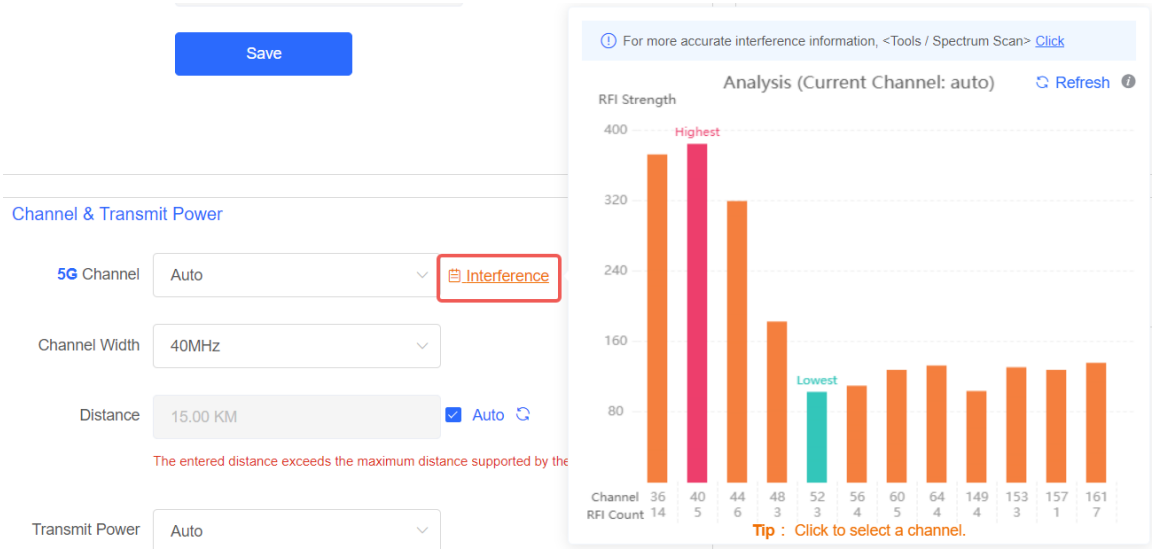
- Method 1: Choose **Wireless > Channel & Transmit Power**.
- Method 2: Choose **Overview > WDS Group Info > WDS > Channel & Transmit Power**.



Before configuration, you can check the interference in the current environment in the following way to find the optimal channel.

Click **Interference** to view the interference of each channel. The channel with the smallest interference is the optimal channel.

To view the interference details of each channel, go to the **Spectrum Scan** page. For details, see 4.2 Configuring Spectrum Scan.



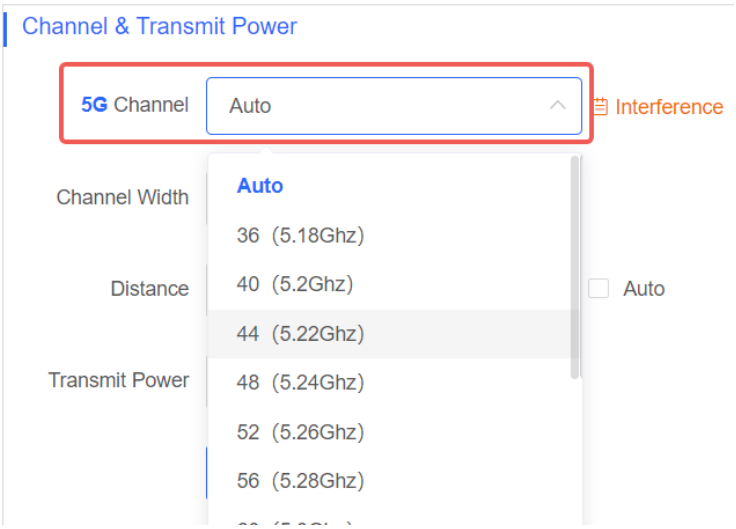
2.13.3 Configuration Steps

1. Configuring the Channel

(1) Channel Settings

Automatic channel selection is enabled by default, that is, the device automatically selects a channel based on the surrounding environment when it is powered on.

Excessive wireless clients connected to a channel can cause strong wireless interference. Choose the optimal channel identified through the proceeding analysis. Click **Save** to make the configuration take effect immediately.



Once the channel is adjusted at the NVR end, the CPE end will follow the channel configuration of the NVR end automatically. Independent channel settings are not supported on the CPE end.

Note

- The available channels are subject to the country/region code. Select the country or region where the device will be used.
- The preceding figure shows the channel configuration for 5 GHz, and that for 2.4 GHz is the same.

- The bridge that supports only the 2.4 GHz frequency band does not support the 5 GHz channel configuration.

Caution

Changing the channel will cause the BaseStation to disconnect and then reconnect to the CPE. Exercise caution when performing this operation.

2. Configuring the Channel Width

If the interference is severe in the wireless environment, choose a narrower channel width to avoid network stalling.

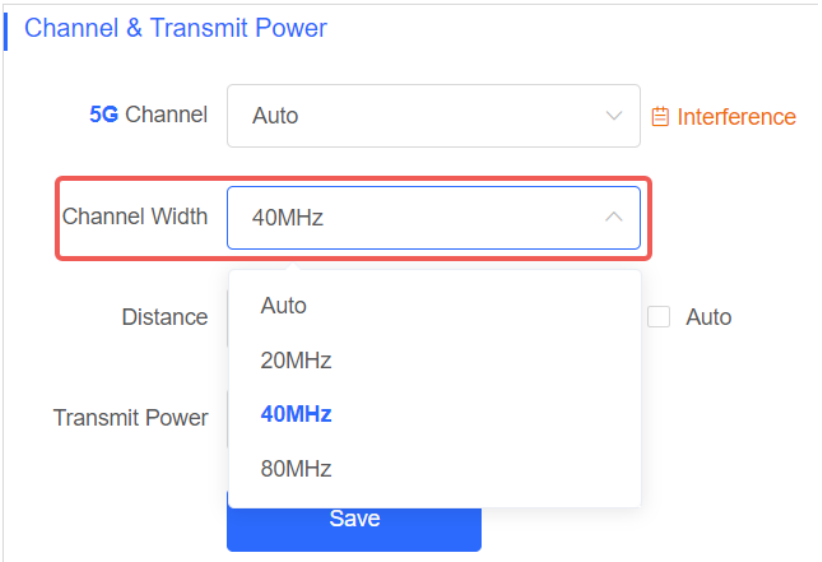
The 5 GHz bridge supports 20 MHz, 40 MHz, and 80 MHz, while the 2.4 GHz bridge supports 20 MHz and 40 MHz.

A narrower channel width indicates a more stable network with a smaller bandwidth. Conversely, a wider channel width indicates a less stable network but with a larger bandwidth. The default value is 20 MHz for 2.4 GHz and 40 MHz for 5 GHz. The default settings are recommended.

After setting the channel width, click **Save** to make the configuration take effect immediately.

Caution

Changing the channel will cause the BaseStation to disconnect and then reconnect to the CPE. Exercise caution when performing this operation.

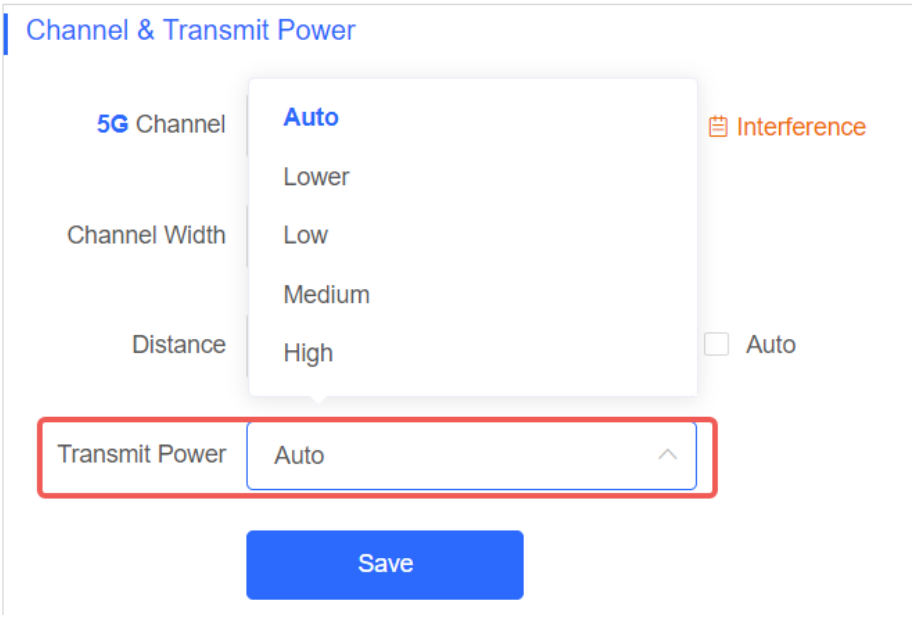


3. Configuring the Transmit Power

Higher transmit power provides greater coverage but may introduce stronger interference to surrounding wireless devices.

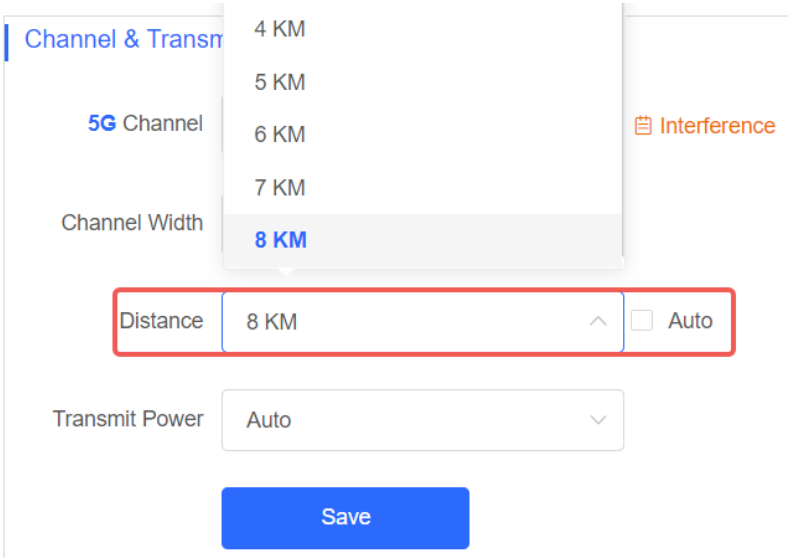
The default value is **Auto**, indicating that the transmit power is automatically adjusted. In scenarios where wireless devices are densely deployed, lower power is recommended.

Lower, **Low**, **Medium**, and **High** correspond to 25%, 50%, 75%, and 100% of the transmit power.



4. Configuring the Distance

The default setting automatically measures the distance between the NVR end and the camera end after they are bridged. In manual mode, you are advised to set the distance slightly greater than the actual distance. Setting a small distance may degrade wireless performance and lead to bridging failure.



Note

Automatic distance setting is only supported on the RG-EST310 V2, RG-EST350 V2, RG-AirMtro460F, RG-AirMetro460G, and RG-AirMetro5500G-B. Manual distance setting is only supported on the RG-AirMtro460F, RG-AirMetro460G, and RG-AirMetro5500G-B. The maximum distance vary with the devices: 1 km for the RG-EST310 V2, 5 km for the RG-EST350 V2, 15 km for the RG-AirMetro460F, RG-AirMetro460G, and RG-AirMetro5500G-B.

2.14 Configuring TDMA Mode

Note

The TDMA mode is only supported on the RG-AirMtro460F, RG-AirMetro460G, and RG-AirMetro5500G-B.

2.14.1 Overview

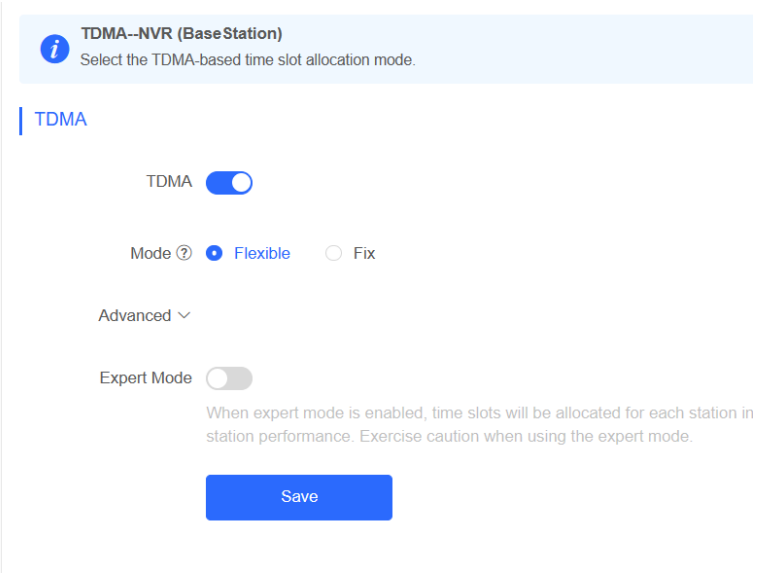
Time Division Multiple Access (TDMA) is specifically designed to address the challenge of CPE nodes being hidden from each other over long distances. In the traditional Wi-Fi mechanism utilizing Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the nodes are unable to listen to each other, leading to significant performance degradation. With the TDMA mode enabled, the traffic of each node remains unaffected by long distances, ensuring high performance.

2.14.2 Selecting the TDMA Mode

Choose **Wireless** > **TDMA**.

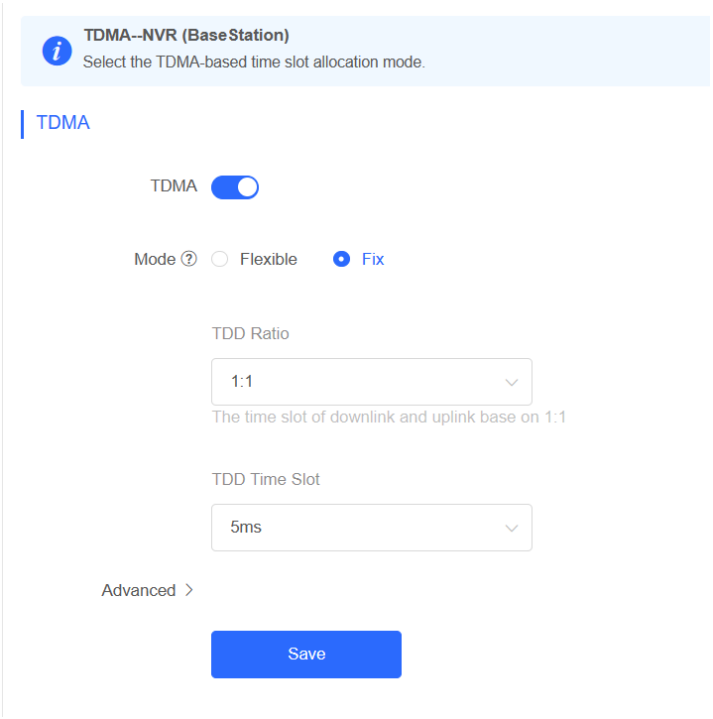
1. Flexible mode

The flexible mode is the default TDMA mode. When enabled, it employs an algorithm to automatically calculate the necessary time slots for each CPE or BaseStation. Additionally, the ratio between BaseStation and CPE is dynamically adjusted to optimize uplink and downlink traffic for maximum efficiency.

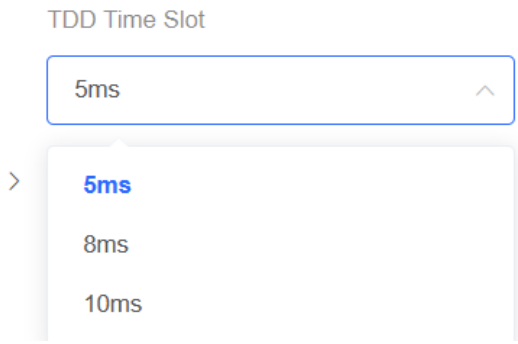


2. Fixed mode

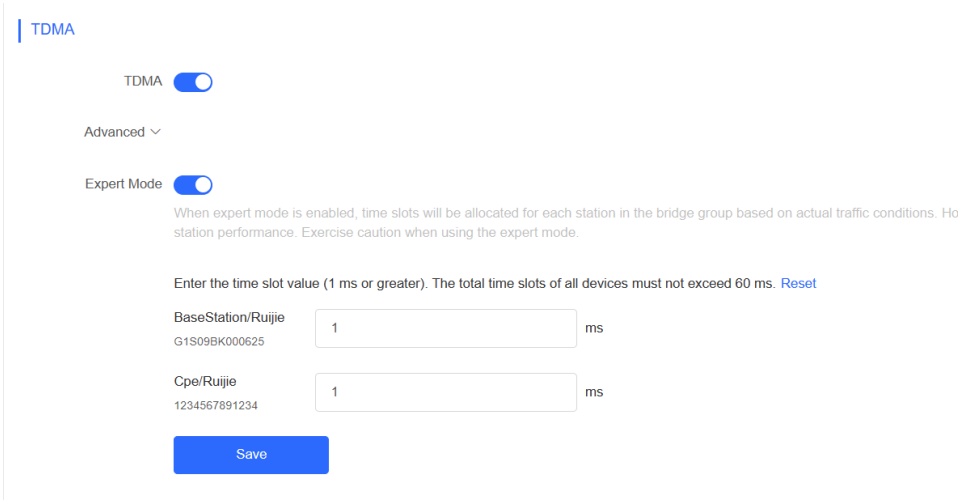
The fixed mode is designed for scenarios that require traffic balance, consistent latency, and consistent uplink and downlink throughput for each node. By utilizing fix intervals (such as 5 ms, 8 ms, and 10 ms), the duration of each frame can be fixed to achieve a consistent latency. In terms of the uplink and downlink throughput, you can set the uplink and downlink ratio accordingly. Currently, there are five ratios available: 1:1, 1:2, 1:3, 2:1, and 3:1, which can be selected from the provided drop-down menu.


TDMA--NVR (BaseStation)
Select the TDMA-based time slot allocation mode.
TDMA
TDMA
Mode
Flexible
Fix
TDD Ratio
1:1
The time slot of downlink and uplink base on 1:1
TDD Time Slot
5ms
Advanced
Save


TDD Ratio
1:1
1:1
1:2
1:3
2:1
3:1


TDD Time Slot
5ms
5ms
8ms
10ms

3. Expert mode



Caution

The expert mode is designed for situations where a specific node requires a dedicated and fixed time slot, unaffected by algorithm adjustments. In this mode, the desired time slot can be set by the customer. However, it is important to note that the expert mode is not recommended for general customers and should only be configured by individuals with relevant professional knowledge. Incorrect configuration in this mode may result in the device failing to go online.

3 Advanced Settings

3.1 Rate Limiting

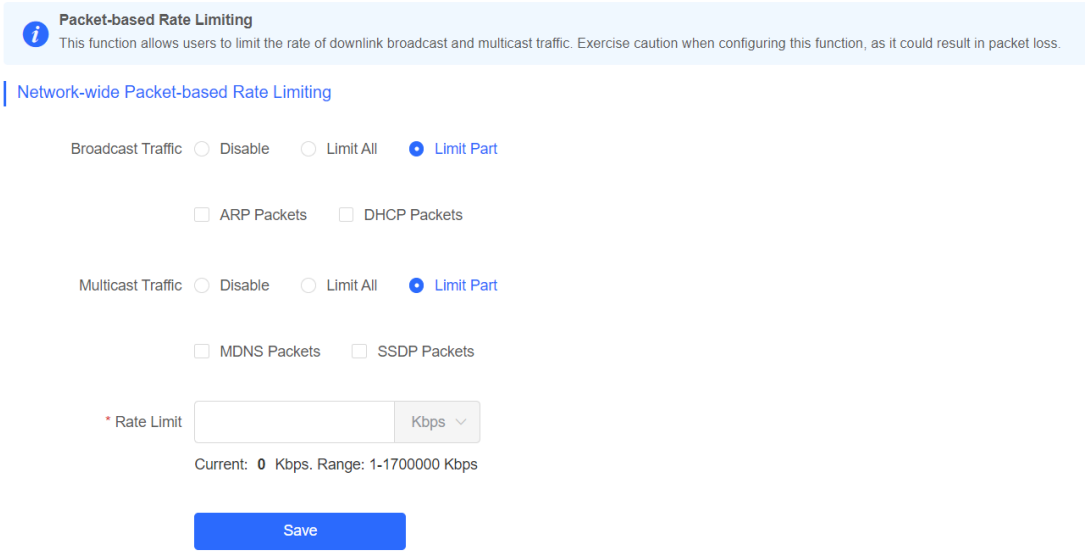
Enable rate limiting on broadcast or multicast packets to avoid congestion on the air interface.

The device supports rate limiting on specified broadcast packets (ARP and DHCP), specified multicast packets (MDNS and SSDP), or all broadcast and multicast packets.

Caution

Rate limiting takes effect on all devices over the network, that is, all bridges capable of rate limiting on the homepage.

Choose **Advanced** > **Rate Limiting**.



3.2 Configuring One-Touch Pairing

3.2.1 Overview

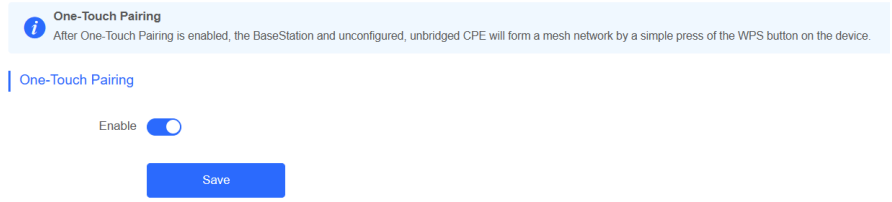
When the One-Touch Pairing feature is enabled, a simple press of the One-Touch Pairing button on the device triggers the mesh operation. During the mesh process, the BaseStation promptly forms a mesh connection with the factory-configured and unbridged CPE, streamlining the networking process.

3.2.2 Configuration Steps

Choose **Wireless** > **One-Touch Pairing**

Toggle on **Enable** and click **Save**.

Check whether the bridge is in BaseStation mode or CPE mode. If the bridge is currently in BaseStation mode, pressing the One-Touch Pairing button on the wireless bridge will bridge it to all nearby devices operating in CPE mode. If the device is currently in CPE mode, pressing the **One-Touch Pairing** button will switch it to BaseStation mode and continue bridging with all nearby devices operating in CPE mode.



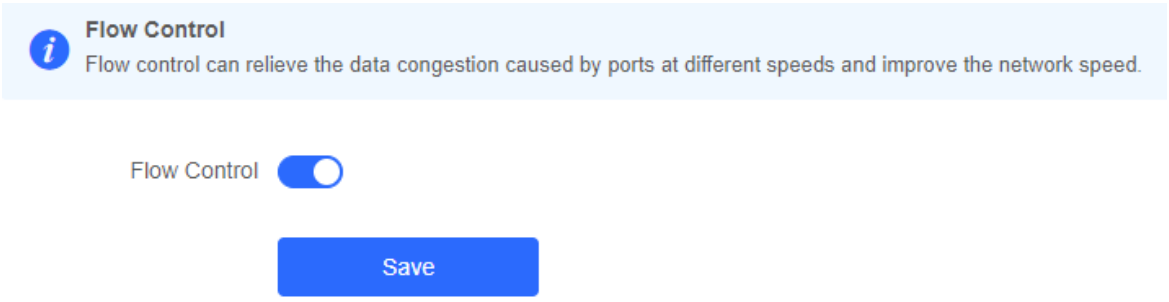
Note

The One-Touch Pairing feature is enabled by default.

3.3 Port-based Flow Control

Choose **Advanced** > **Flow Control**.

Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed. This function is enabled by default and can be manually disabled.



3.4 Wi-Fi Protection

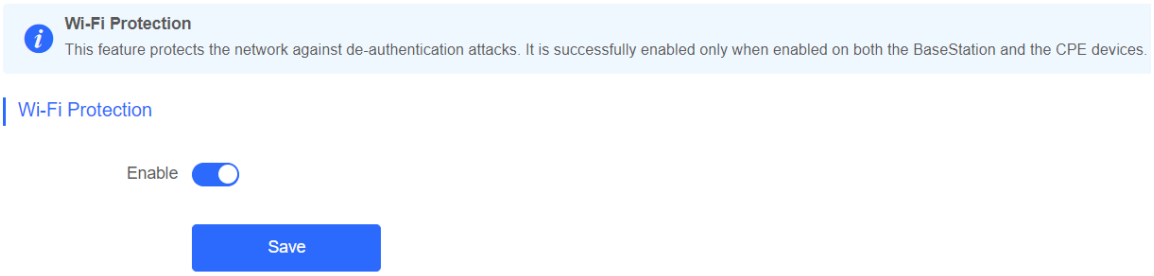
3.4.1 Overview

When there is any attacker in the operational environment of the bridge, the attacker will transmit authentication attack packets to the bridge, resulting in abnormal disconnection of the bridge. Enabling **Wi-Fi Protection** can safeguard the bridge from authentication attacks.

3.4.2 Configuration Steps

Choose **Advanced > Wi-Fi Protection**.

This function is enabled by default. You can manually disable the Wi-Fi protection function. Click **Save**.


Wi-Fi Protection
This feature protects the network against de-authentication attacks. It is successfully enabled only when enabled on both the BaseStation and the CPE devices.
Wi-Fi Protection
Enable
Save

4 Tools

4.1 Antenna Alignment

Caution

If the current device is in the BaseStation mode, you can view information about all devices in the CPE mode. If the current device is in the CPE mode, you can only view information about the current device and the device in the BaseStation mode.

4.1.1 Overview

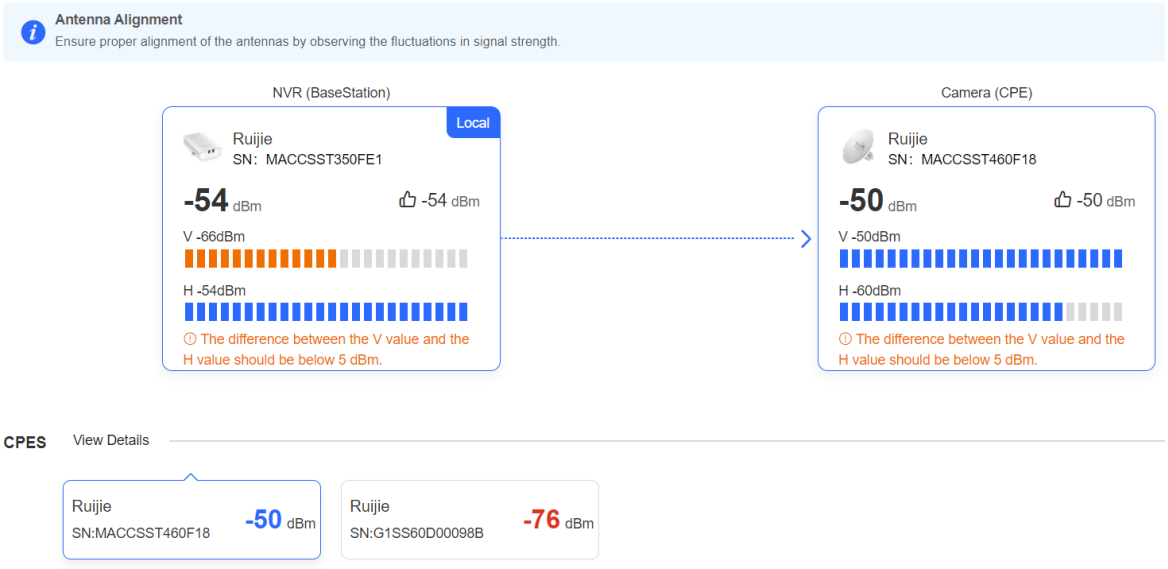
The **Antenna Alignment** tool can be used only when the device is in normal bridging state. Proper alignment can help you achieve the best bridging signal. When the device moves in the horizontal and vertical directions, the RSSI changes in real time.

4.1.2 Configuration Steps

Go to the configuration page:

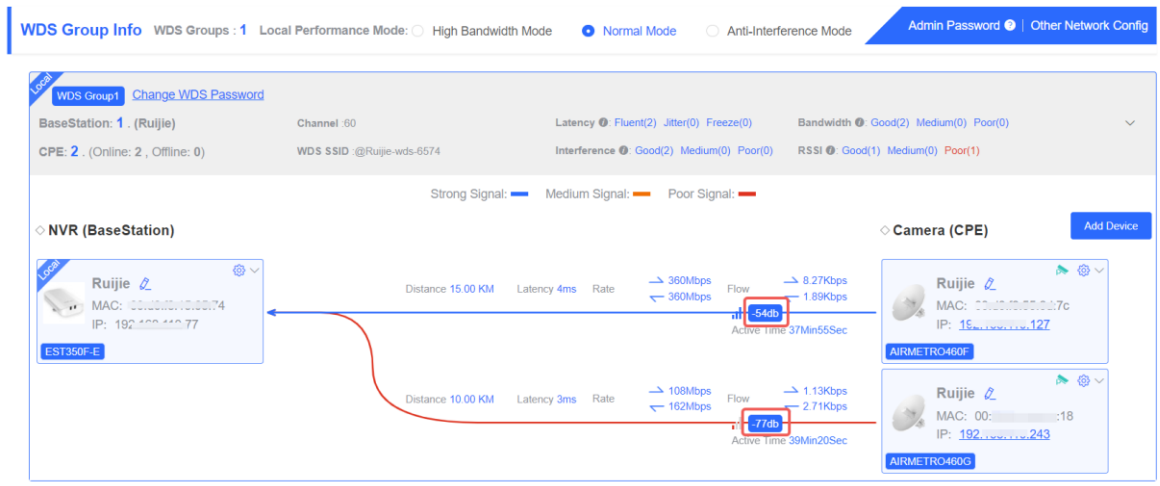
- Method 1: Choose **Tools** > **Antenna Alignment**.

Click **Antenna Alignment**. The RSSI of all CPEs in the bridge group will be displayed. Click any CPE to display the details of the bridging link.

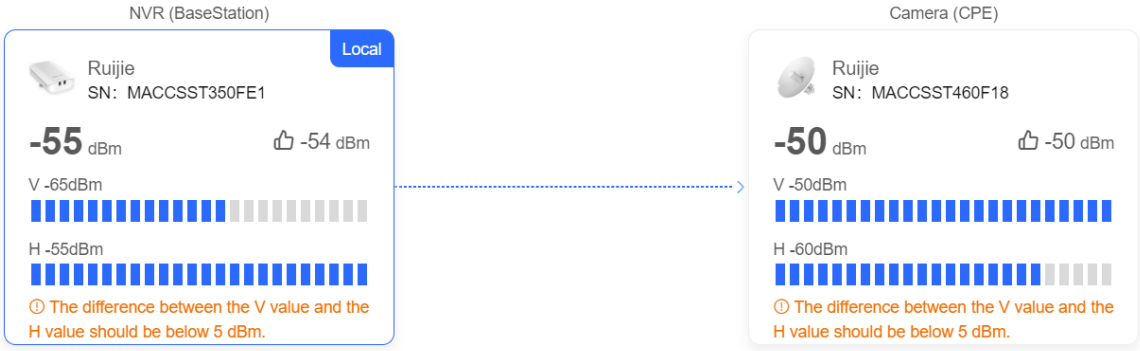


- Method 2: Click an RSSI on the home page.

Click an RSSI value on the **WDS Group Info** page.



The bridge group information that can be viewed includes the maximum vertical and horizontal values of the BaseStation and camera in the bridge group, the optimal historical RSSI, and the real-time vertical and horizontal RSSIs.



Caution

The left pane displays details about the local device, while the right pane shows information about the peer device.

4.2 Configuring Spectrum Scan

Note

- This function is supported only in the BaseStation mode.
- Bridges will be disconnected during spectrum scanning. Exercise caution when performing this operation.

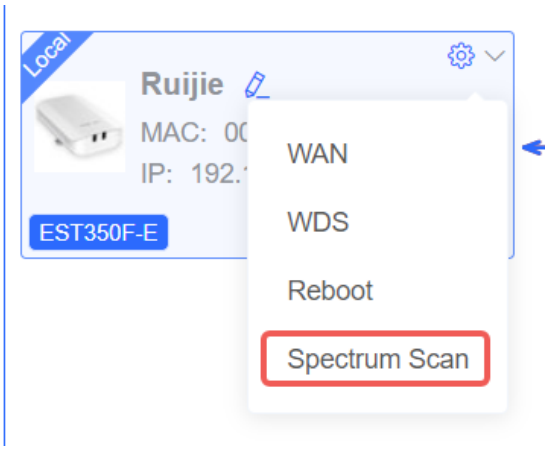
4.2.1 Overview

When a bridge is installed outdoors, outdoor base stations from other networks may cause wireless interference that will impact the bridge's performance. Spectrum scan provides details on interference across all channels. A higher interference score indicates severer interference on that channel.

4.2.2 Configuration Steps

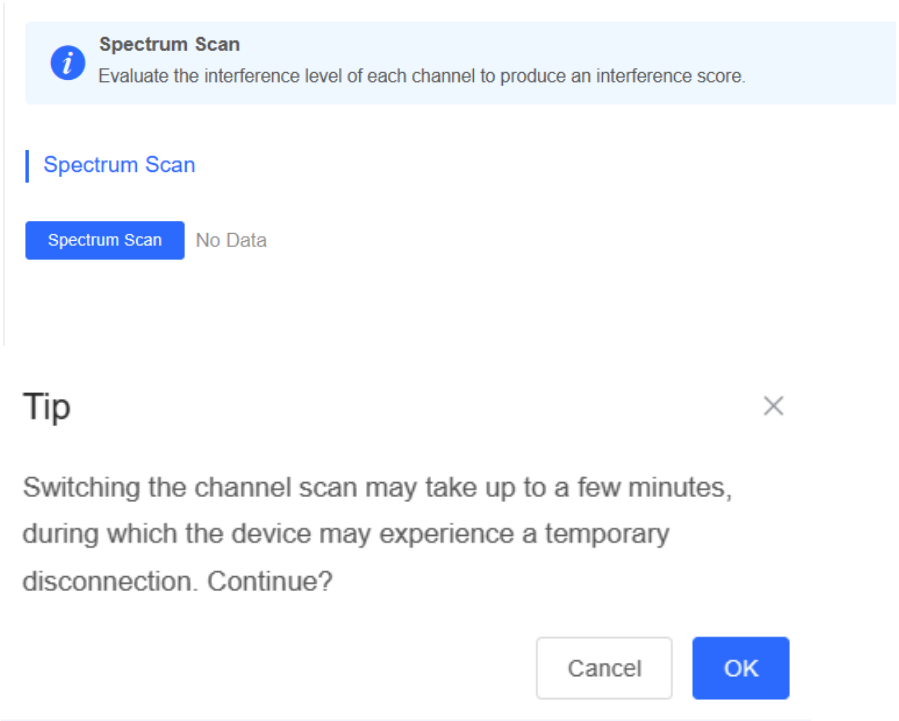
Go to the configuration page:

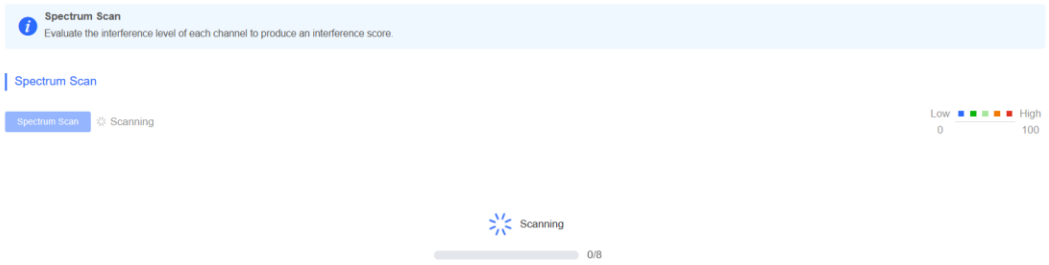
- Method 1: Choose **Tools > Spectrum Scan**.
- Method 2: Choose **Overview** > **WDS Group Info** > **Spectrum Scan**.



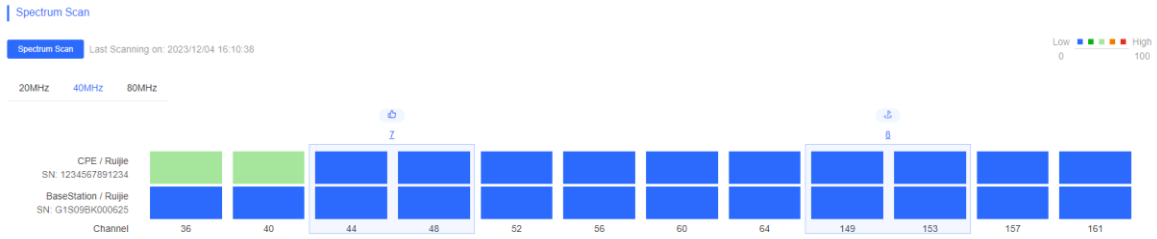
This feature is only supported when the bridge is in BaseStation mode.

Click **Spectrum Scan**, and then click **OK** on the pop-up window. The **Spectrum Scan** page is displayed.

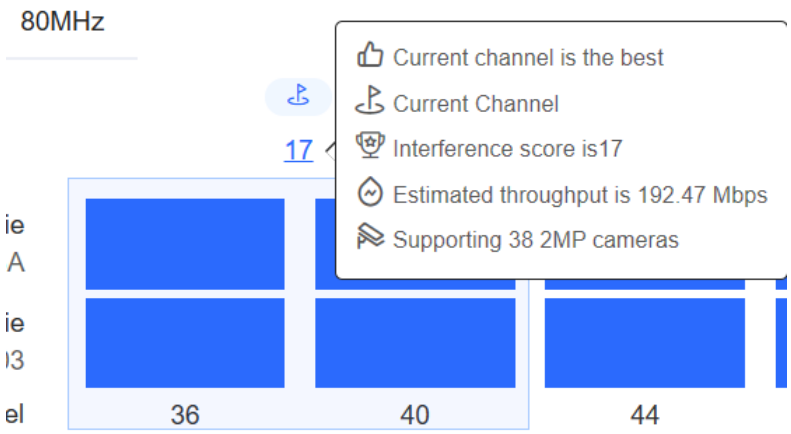




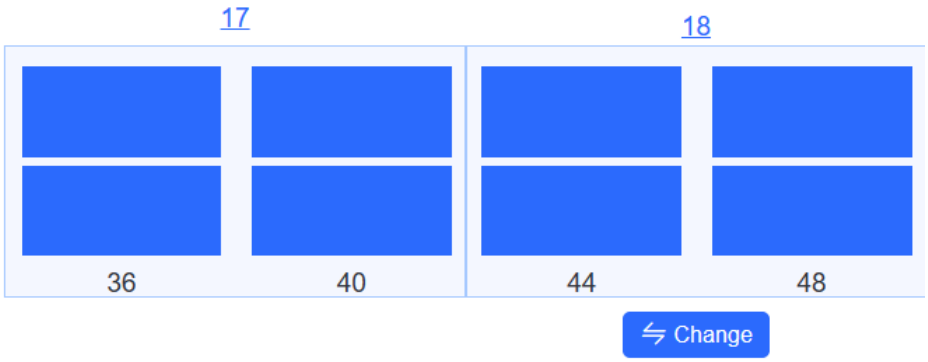
You can click the **20 MHz**, **40 MHz**, or **80 MHz** tabs to view the channel interference. The color gradient from left to right indicates the level of interference, ranging from low to high. Each row represents the channels used by a device.

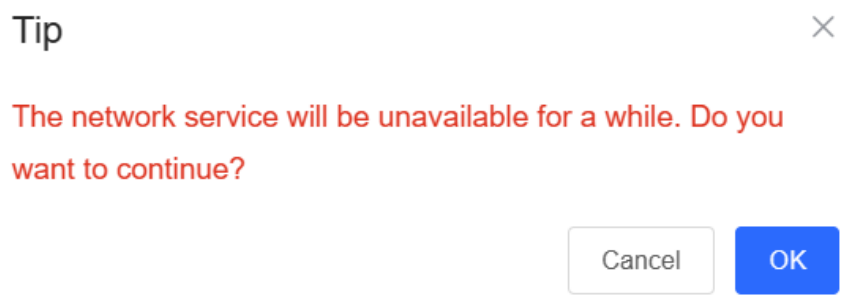


Hovering the mouse over it will display detailed information about the current channel, including throughput and estimated number of cameras that can be supported.



To change channels, click on the target channels, and then click **Change Channel**. A pop-up window is displayed. Click **OK**.





4.3 Network Diagnosis Tools

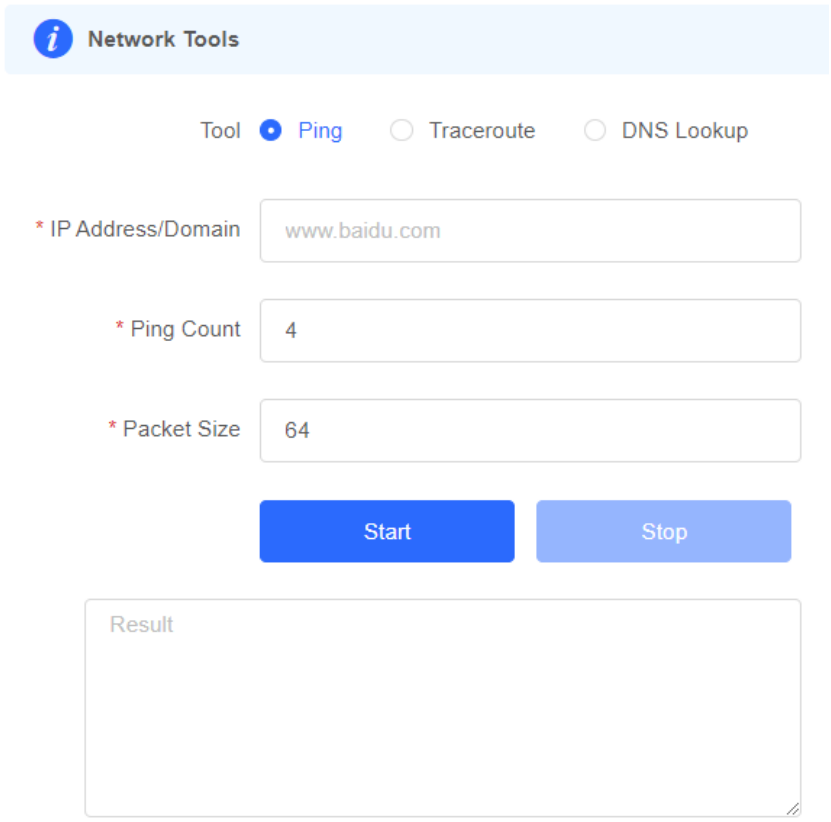
4.3.1 Network Test Tool

Choose Diagnostics > Network Tools.

When you select the ping tool, you can enter the IP address or URL and click **Start** to test the connectivity between the bridge and the IP address or URL. The message "Ping failed" indicates that the bridge cannot reach the IP address or URL.

The Traceroute tool displays the network path to a specific IP address or URL.

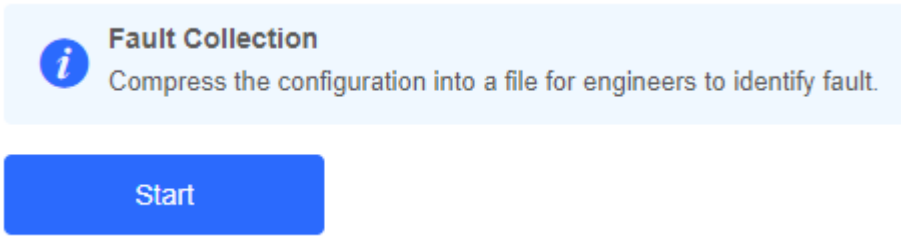
The DNS Lookup tool displays the DNS server address used to resolve a URL.



4.3.2 Collecting Fault Info

Choose Diagnostics> Fault Collection.

Click **Start** to collect fault information and compress it into a file for engineers to identify fault.



Note

If the preceding troubleshooting steps fail to resolve the issue, and remote assistance from technical support is needed, you can contact them to assist in enabling the developer mode. The technical support team can then perform diagnostics to identify and address the issue effectively.

5 Network Settings

5.1 Network Modes

5.1.1 Configuring the Network Mode

The device supports two network modes: bridge mode and router mode. The system menu and functions vary with the network mode. A bridge is in bridge mode by default.

1. Bridge Mode

The device performs Layer 2 forwarding, and does not support the DHCP address pool function. In bridge mode, it is used in combination with a routing device for networking. The downlink devices' IP addresses are uniformly allocated and managed by the uplink device (with a DHCP address pool). The bridge only performs transparent transmission.

If the network is already connected to the Internet, you are advised to select the bridge mode.

2. Router Mode

The device has the routing function, and supports NAT routing and forwarding. The IP address of the downlink device can be allocated by the bridge. Data is forwarded by the bridge and NAT is supported.

In router mode, the device supports DHCP and static IP for Internet connection, and can directly connect to the uplink device.

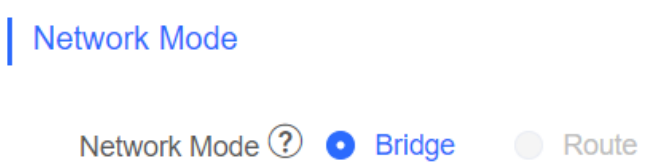
Caution

After the device is switched to the router mode, its network settings will be changed. The IP address of the LAN port will be changed to 192.168.130.1, and the DHCP server will be enabled. You are advised to set the PC to automatically obtain an IP address, and to log in to 10.44.77.254 to configure the device in router mode. Router mode is supported only when the bridge acts as a CPE.

5.1.2 Configuration Steps

Choose **Network** > **Network Mode**.

Select the required network mode. Hover the mouse over the icon to view the help information.



5.2 Configuring the IPv4 Address of the WAN Port

In bridge mode, the IPv4 address of the WAN port is only used for accessing the web interface, and does not affect the service network.

5.2.1 Allocating IPv4 Addresses to Bridges on the Network

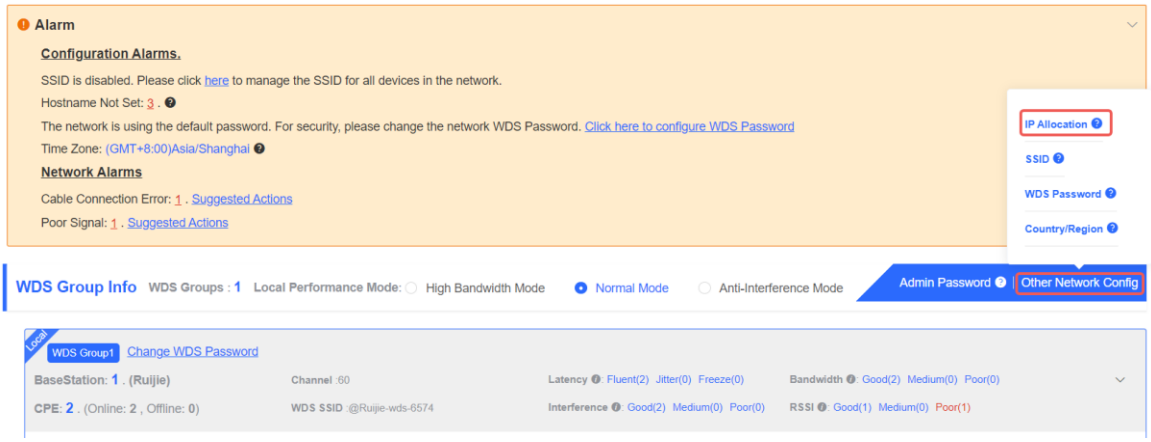
1. Static IP Address

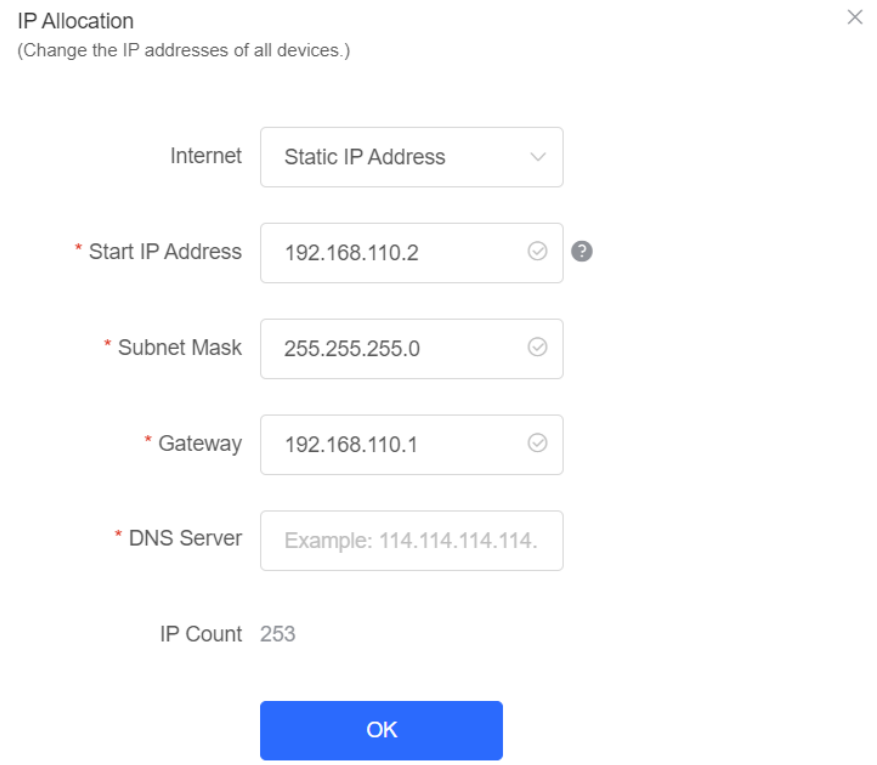
Choose **Overview** > **WDS Group Info** > **Other Network Config**.

When a large number of devices on the network need to be configured with static IP addresses, you can use the IP Allocation feature to automatically allocate a static IP address to each device.

Click **IP Allocation**. In the dialog box that appears, select **Static IP Address** from the **Internet** drop-down list, enter the start IP address, subnet mask, gateway IP address, and DNS server IP address. Then, click **OK**.

Hover the mouse over the icon to view the help information.





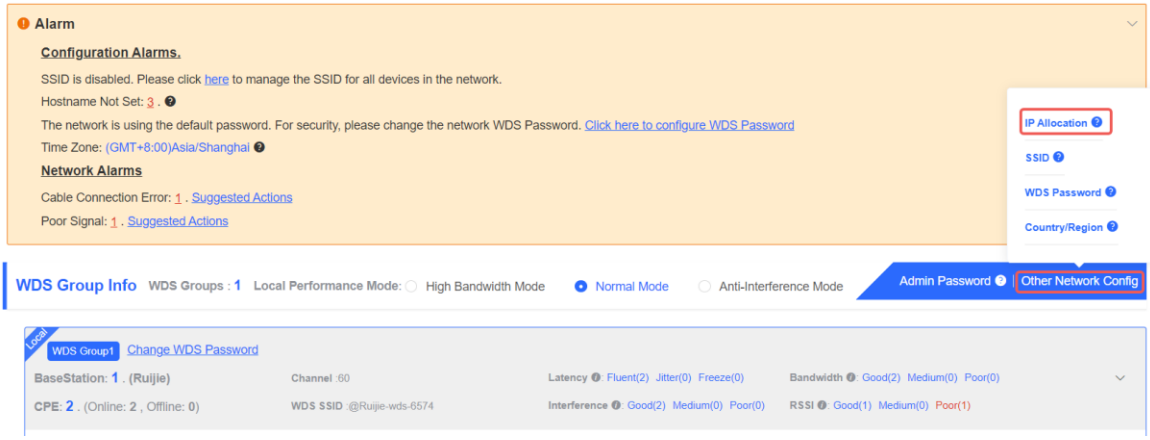
Caution

- The start IP address cannot be on the same network segment as the current IP address. Otherwise, the configuration will fail.
- After the configuration is saved, the device IP address will change, and you may fail to access the device's web interface. In this case, you need to enter the new IP address in the browser's address bar for login. Ensure that the IP addresses of the management PC and the device are on the same network segment. If they are not on the same network segment, change the management PC's IP address. For details, see 1.3.2 Configuring the IP Address of the Management PC. Therefore, exercise caution when performing this operation.

2. DHCP

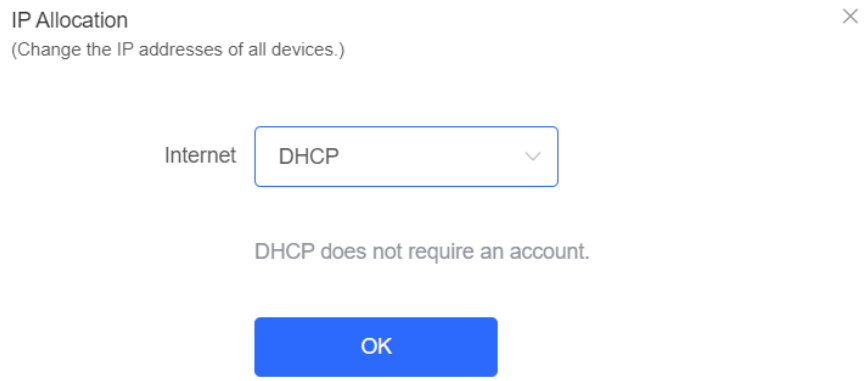
Choose **Overview** > **WDS Group Info** > **Other Network Config**.

Click **IP Allocation**.



When a large number of devices on the network require dynamic IP addresses, you can configure dynamic IP addresses for all devices on the network, so that each device can dynamically obtain an IP address.

Select **DHCP** from the **Internet** drop-down list. Then, click **OK**.

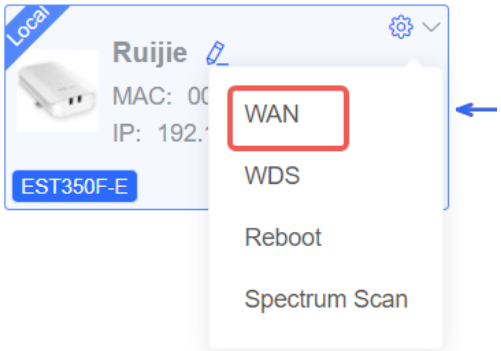


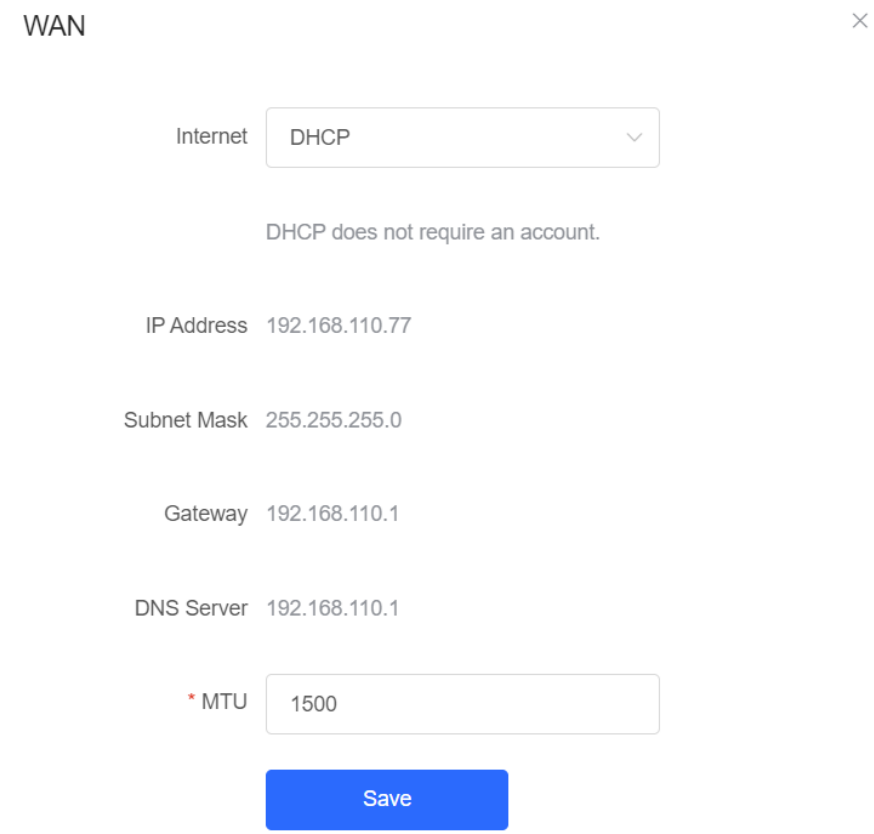
5.2.2 Set the WAN Port IP Address for a Single Online Bridge

Choose **Overview** > **WDS Group Info** > **NVR (BaseStation)** or **Camera (CPE)**.

You can set an IP address for a single device using the **Network-wide Management** menu.

Click . Select **WAN** from the drop-down list. For details, see5.2.1 Allocating IPv4 Addresses to Bridges.





Caution

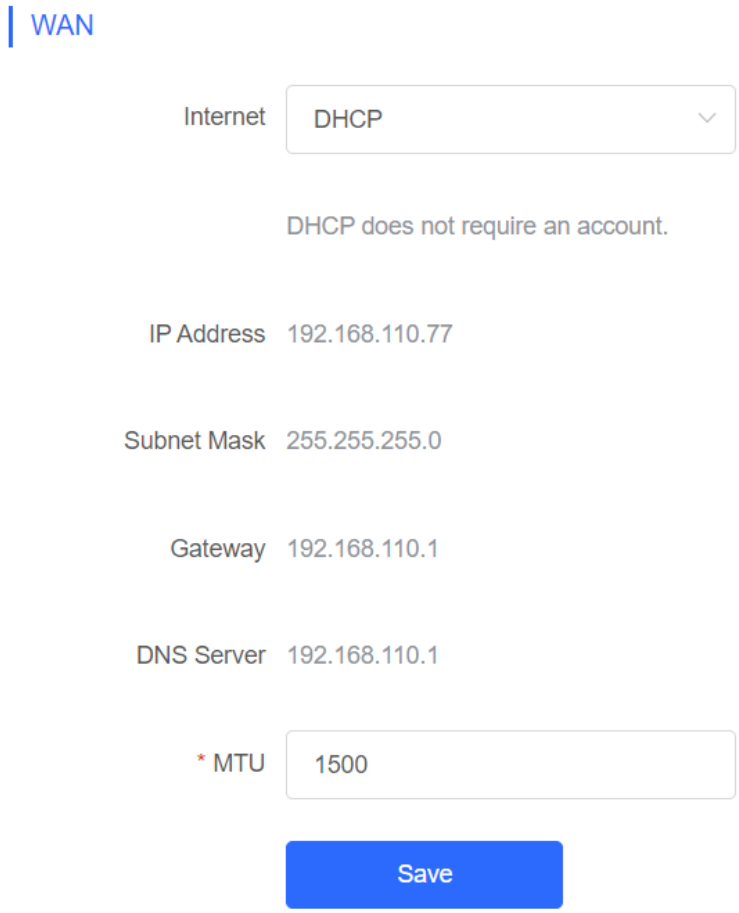
After the IP address and subnet mask are changed, you may fail to access the device's web interface. In this case, you need to enter the new IP address in the browser's address bar for login. Ensure that the IP addresses of the management PC and the device are on the same network segment. If they are not on the same network segment, change the management PC's IP address. For details, see 1.3.2 Configuring the IP Address of the Management PC. Therefore, exercise caution when performing this operation.

5.2.3 Configuring an IP Address for the WAN Port

Choose **Network > Base Configuration > WAN**.

Select the Internet connection type. You are advised to select **DHCP** for networks with a DHCP server, or **Static IP** for networks without a DHCP server.

If **Static IP** is selected, enter the IP address, subnet mask, gateway IP address, and DNS server address. Click **Save**.



Caution

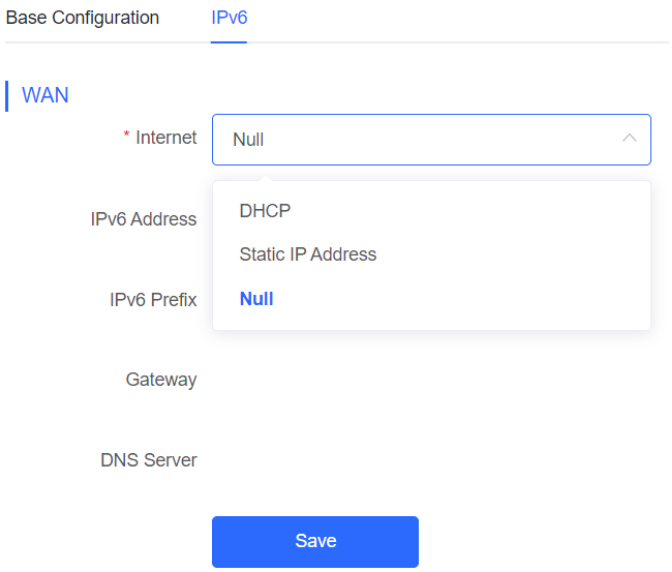
After the IP address and subnet mask are changed, you may fail to access the device's web interface. In this case, you need to enter the new IP address in the browser's address bar for login. Ensure that the IP addresses of the management PC and the device are on the same network segment. If they are not on the same network segment, change the management PC's IP address. For details, see 1.3.2 Configuring the IP Address of the Management PC. Therefore, exercise caution when performing this operation.

5.3 Configuring the IPv6 Address for the WAN Port

Note

This feature is only supported on RG-AirMetro460F, RG-AirMetro460G and RG-AirMetro550G-B when the network mode of these devices are set to bridge mode.

Choose **Network** > **IPv6** > **WAN**.



The following Internet connection types are supported:

- DHCP: The device will act as a DHCPv6 client, and apply for an IPv6 address/prefix from the uplink device.
- Static IP: If this option is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server.
- Null: The IPv6 function is disabled on the WAN port.

5.4 Changing the IP Address of a LAN Port

Caution

This function is supported only when the network mode of the device is set to router mode.

Choose **Network** > **Base Configuration** > **LAN**.

Enter the IP address and subnet mask, and click **Save**. After changing the IP address of the LAN port, enter the new IP address in the browser to access the web interface of the device for configuration and management.

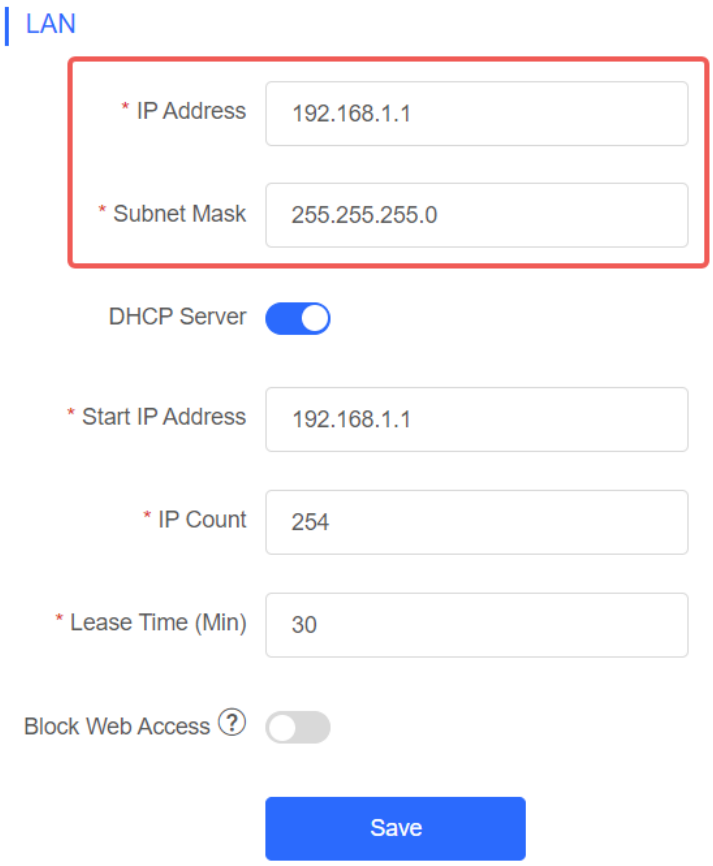


Table 5-1 LAN Configuration Parameters

Parameter	Description
IP Address	This IP address is the default gateway IP address for devices connected to the internet through this LAN.
Subnet Mask	Subnet mask of devices on the LAN.
DHCP Server	After this function is enabled, devices on the LAN can automatically obtain IP addresses. You need to configure the start IP address to be assigned, number of IP addresses to be assigned, and address lease time for the DHCP server, as well as other DHCP server options. For details, see 5.6 Configuring the DHCP Server.
Start IP Address	Start IP address of the IP address range automatically allocated by the DHCP server. The start address should be on the network segment calculated based on the IP address and the subnet mask.
IP Count	The number of assignable IP addresses, which is determined by the LAN segment and the start IP address.
Lease Time (Min)	Lease time of the automatically assigned IP addresses. When the lease time expires, devices on the LAN will obtain IP addresses again.

Parameter	Description
Block Web Access	After this function is enabled, you cannot log in to the web interface of the CPE through the LAN port. You can only log in to the web interface of the CPE by connecting to the SSID or connecting to the NVR (BaseStation) to access the web interface of the CPE.

5.5 Changing the MTU

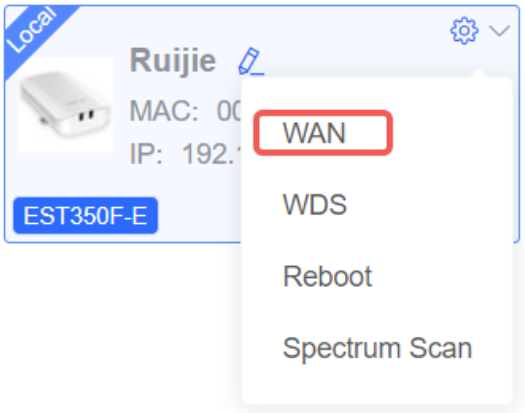
WAN port MTU indicates the maximum transmission unit (MTU) allowed by the WAN port. The default value is 1500 bytes. However, at times, ISP networks may limit the speed of large data packets or block their transmission. This can lead to slow network speeds or even disconnections. In such cases, you are advised to set a smaller MTU value.

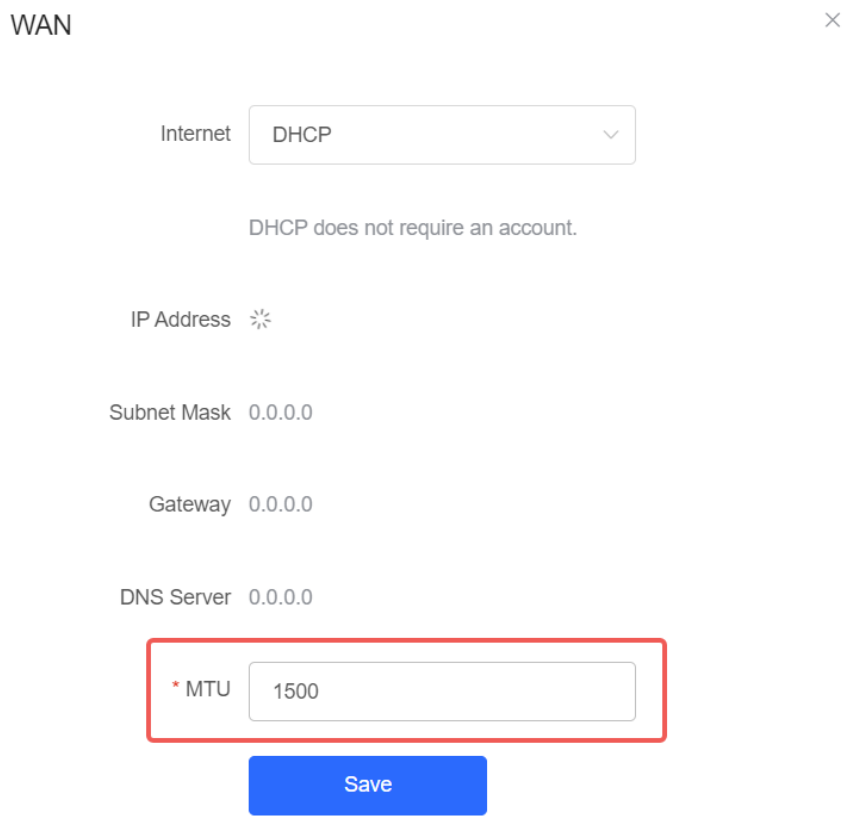
5.5.1 Changing the MTU of a Single Online Bridge

Choose **Network** > **WDS Group Info** > **NVR (BaseStation)** or **Camera (CPE)**.

The MTU of a single device can be configured using the **Network-wide Management** menu.

Click . Select **WAN** from the drop-down menu. On the page that is displayed, enter the MTU value, and click **Save**.

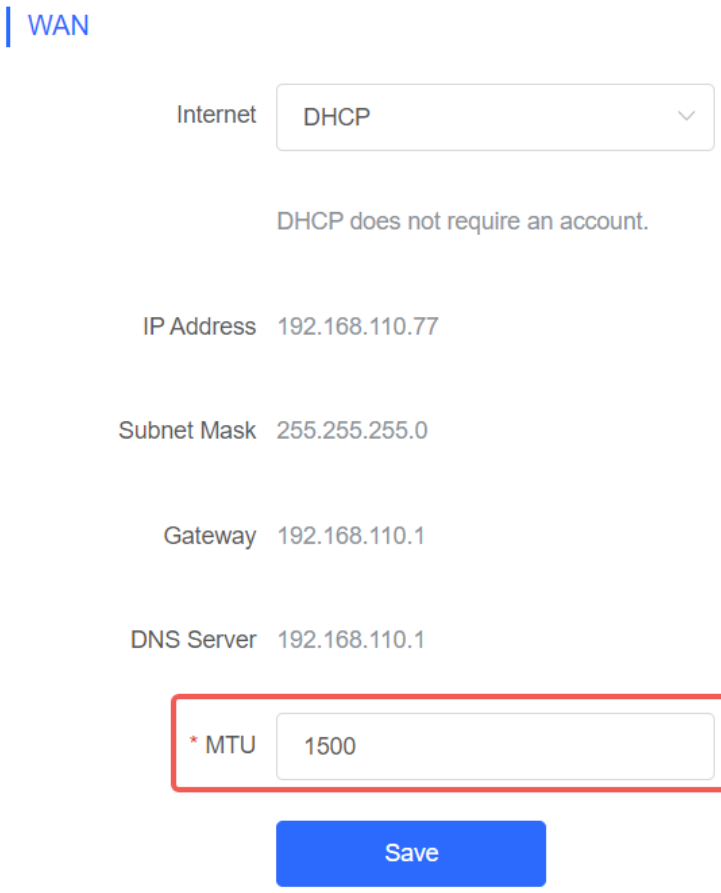




5.5.2 Modifying the MTU of the Current Device

Choose **Network** > **Base Configuration** > **WAN**.

On the **WAN** page, enter the MTU value and click **Save**.



5.6 Configuring the DHCP Server

Caution

This function is supported only when the network mode of the device is set to router mode.

5.6.1 Overview

In router mode, the DHCP server function can be enabled on the device to automatically assign IP addresses to clients, so that clients connected to the LAN ports of the device can obtain IP addresses for Internet access.

5.6.2 Configuring the DHCP Server

Choose **Network** > **Base Configuration** > **LAN**.

DHCP Server: This function is enabled by default when the network mode of the device is set to router mode. When the device is used as the only routing device on the network, you are advised to keep this function enabled. When multiple routing devices are connected to the uplink device through the LAN port, you are advised to disable this function.

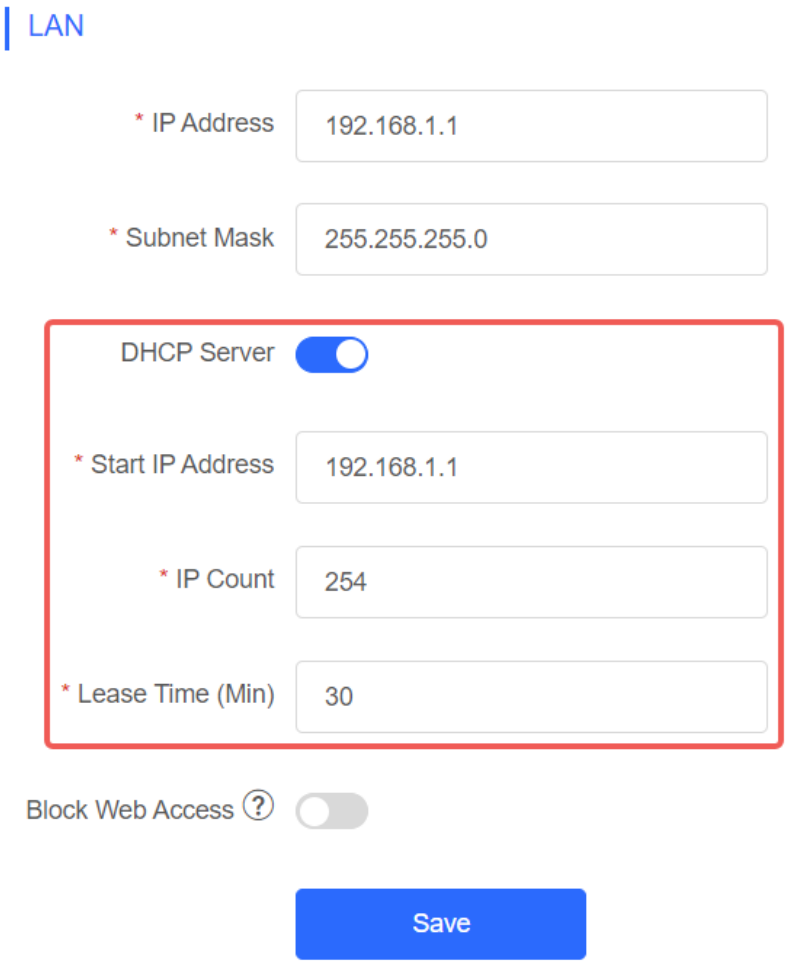
Caution

If the DHCP Server function is disabled on all devices on the network, clients cannot automatically obtain IP addresses. You need to enable the DHCP Server function on one device or manually configure a static IP address for each client for Internet access.

Start IP Address: Start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, no IP address will be assigned to the clients.

IP Count: Number of IP addresses in the address pool.

Lease Time (Min): Lease time of IP addresses. When a client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease time expires. After the client connection is restored, the client can request for an IP address again. The default lease time is 30 minutes.



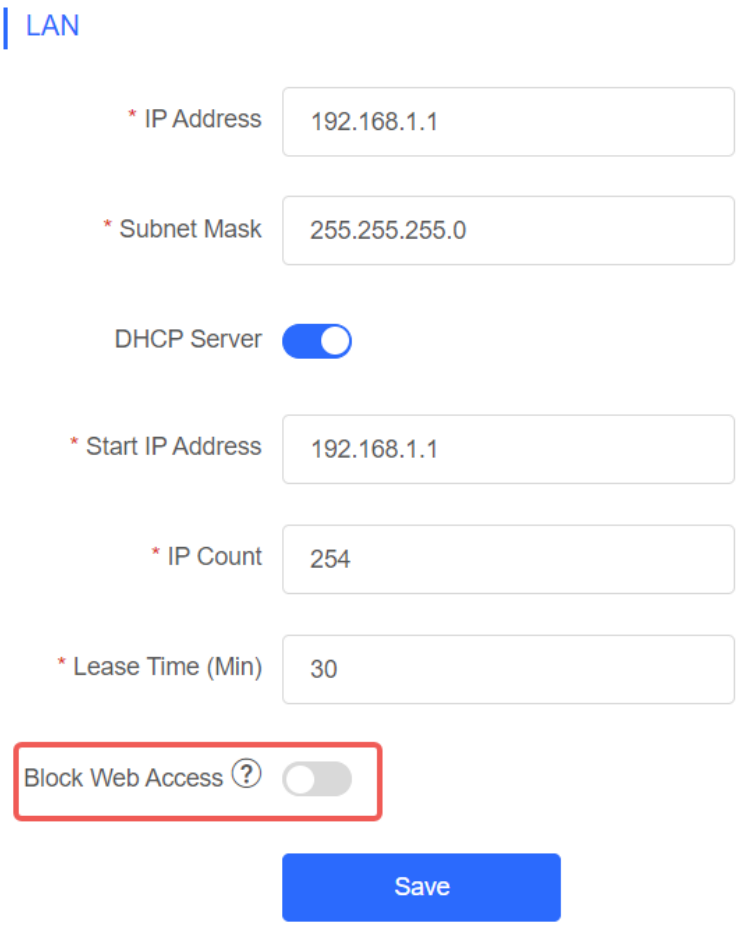
5.7 Blocking Web Access

Caution

This function is supported only when the network mode of the device is set to router mode.

Choose **Network** > **Base Configuration** > **LAN**.

After this function is enabled, you cannot log in to the web interface of the camera through the LAN port of the PC. You can only access the web interface of the camera through the SSID or by connecting to the BaseStation.



5.8 IPv6 Settings

Note

This feature is only supported on the RG-AirMetro460F, RG-AirMetro460G, and RG-AirMetro550G-B when they are in router mode.

5.8.1 Overview

Internet Protocol Version 6 (IPv6) is the next-generation IP protocol designed by the Internet Engineering Task Force (IETF) to replace IPv4 and solve the IPv4 problems such as address depletion.

5.8.2 IPv6 Basics

1. IPv6 Address Format

IPv6 increases the length of the address from 32 bits in IPv4 to 128 bits, and therefore has a larger address space than IPv4.

The basic format of an IPv6 address is X:X:X:X:X:X:X:X. The 128-bit IPv6 address is divided into eight 16-bit sections that are separated by colons (:), and 16 bits in each section are represented by four hexadecimal characters (0–9 and A–F). Each X represents a 4-character hexadecimal number.

For example: 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:0:1, 1080:0:0:0:8:800:200C:417A

The number 0 in the IPv6 address can be abbreviated as follows:

- The starting 0s can be omitted. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be written as 2001:CD:34:78:A:B:1200:2100.
- Some IPv6 addresses may contain a long string of zeroes. "::" can be used to represent this long string of zeroes. For example, 800:0:0:0:0:0:0:1 can be written as 800::1. Consecutive 0s can be replaced by two colons only when the 16-bit section contains all 0s, and the two colons can only appear once in the address.

2. IPv6 Prefix

An IPv6 address consists of two parts:

- Prefix length: Indicates the number of bits in an IPv6 address that identifies the network. This is similar to the network ID part of an IPv4 address, which is used to distinguish different networks.
- Interface identifier: It contains 128-n bits, and is equivalent to the host ID in an IPv4 address.

The length of the network prefix is separated from the IPv6 address by a slash (/). For example, 12AB::CD30:0:0:0:0/60 indicates that the length of the prefix used for routing in the address is 60 bits.

3. Special IPv6 Addresses

There are also some special IPv6 addresses, for example:

fe80::/8 is a link local address, and is equivalent to 169.254.0.0/16 in IPv4.

fc00::/7 is a local address, and is similar to 10.0.0.0/8, 172.16.0.0/16, or 192.168.0.0/16 in IPv4.

ff00::/12 is a multicast address, and is similar to 224.0.0.0/8 in IPv4.

4. NAT66

IPv6-to-IPv6 network address translation (NAT66) can change the IPv6 addresses sent and received by network devices, helping devices communicate smoothly on the Internet. NAT66 prefix translation is an implementation of NAT66. It replaces the IPv6 address prefix in the packet header with another IPv6 address prefix to achieve IPv6 address translation. NAT66 can realize mutual access between an intranet and the Internet.

5.8.3 IPv6 Address Assignment Methods

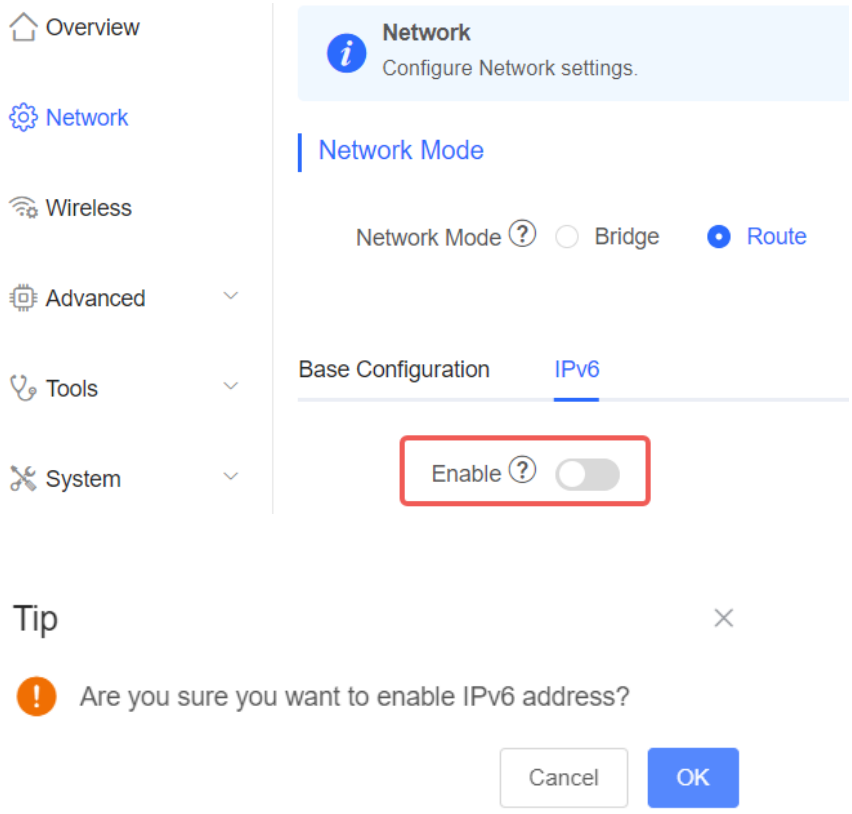
- Manual configuration. The IPv6 address/prefix and other network configuration parameters are manually configured.
- Stateless Address Autoconfiguration (SLAAC): The link local address is generated based on the interface ID, and then the local address is automatically configured based on the prefix information contained in the router advertisement packet

- Stateful Address Autoconfiguration, that is, DHCPv6. DHCPv6 is classified into the following two types:
  - DHCPv6 autoconfiguration: The DHCPv6 server automatically configures the IPv6 address/prefix and other network configuration parameters.
  - DHCPv6 Prefix Delegation (PD): The lower-layer network device sends a prefix allocation application to the upper-layer network device. The upper-layer network device assigns an appropriate address prefix to the lower-layer device. The lower-layer device automatically subdivides the obtained prefix (generally less than 64 bits in length) into subnet segments with 64-bit prefix length, and then advertises the subdivided address prefixes to the user link directly connected to the IPv6 host through the route to realize automatic address configuration of the host.

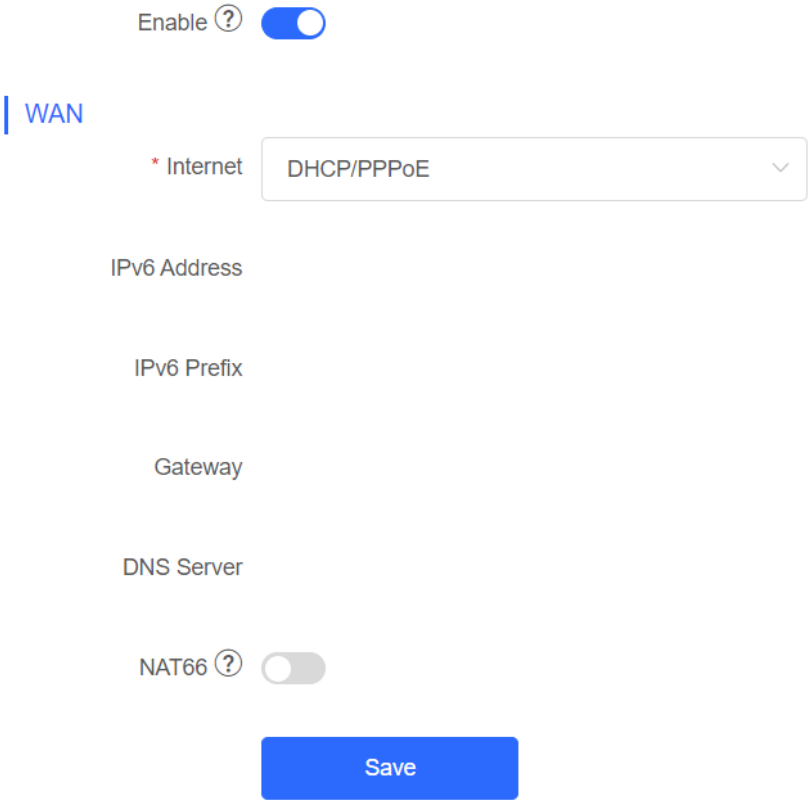
5.8.4 Enabling IPv6

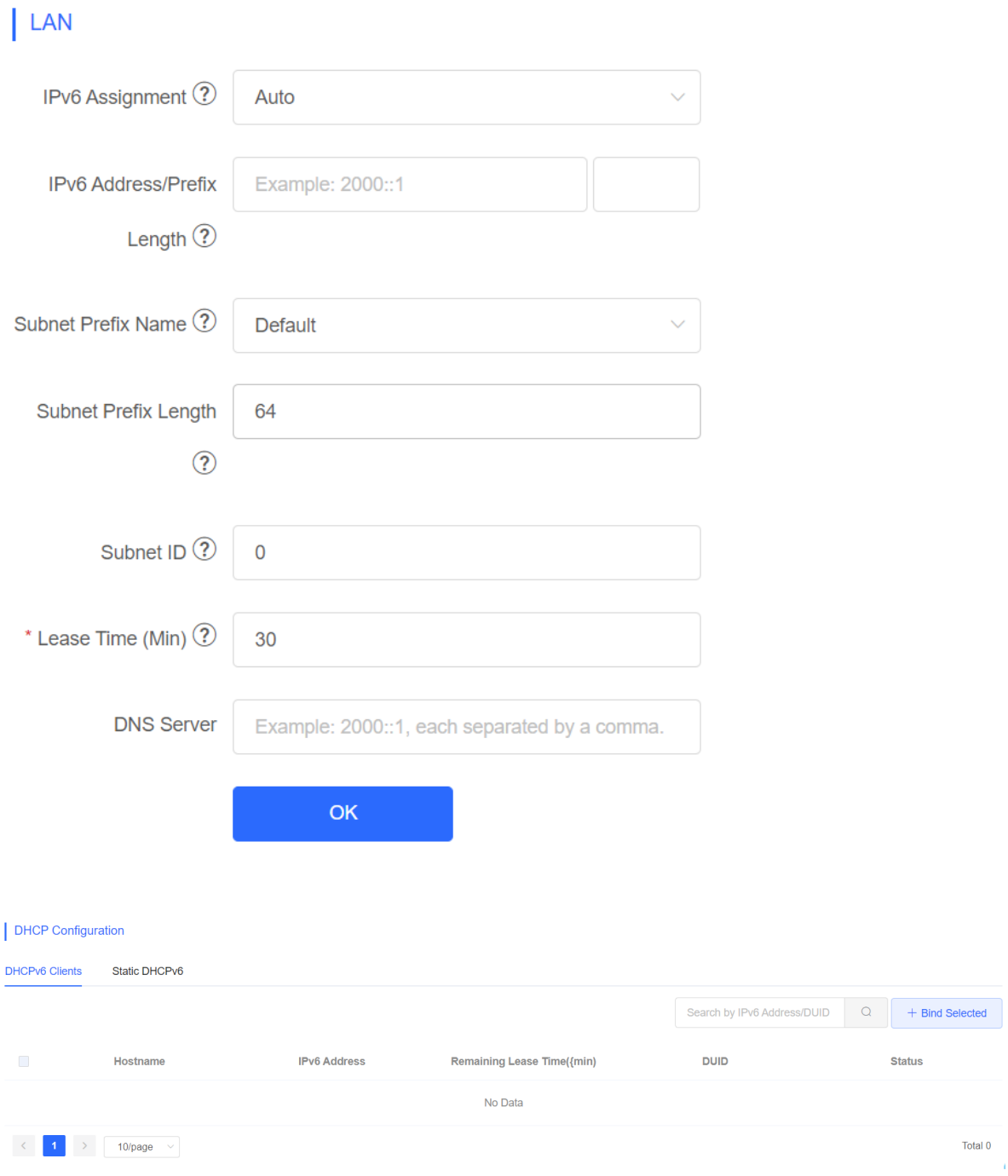
Choose **Network** > **IPv6**.

Toggle on **Enable**, and then click **OK** in the dialog box that appears to enable IPv6.



After IPv6 is enabled, you can configure the IPv6 addresses for WAN and LAN ports, view the DHCPv6 client, and configure a static DHCPv6 address for the client.


Enable
WAN
* Internet
DHCP/PPPoE
IPv6 Address
IPv6 Prefix
Gateway
DNS Server
NAT66
Save



5.8.5 Configuring the IPv6 Address for the WAN Port

Choose **Network** > **IPv6** > **WAN**.

Configure an IPv6 address for the WAN port. Then, click **Save** to make the configuration take effect.

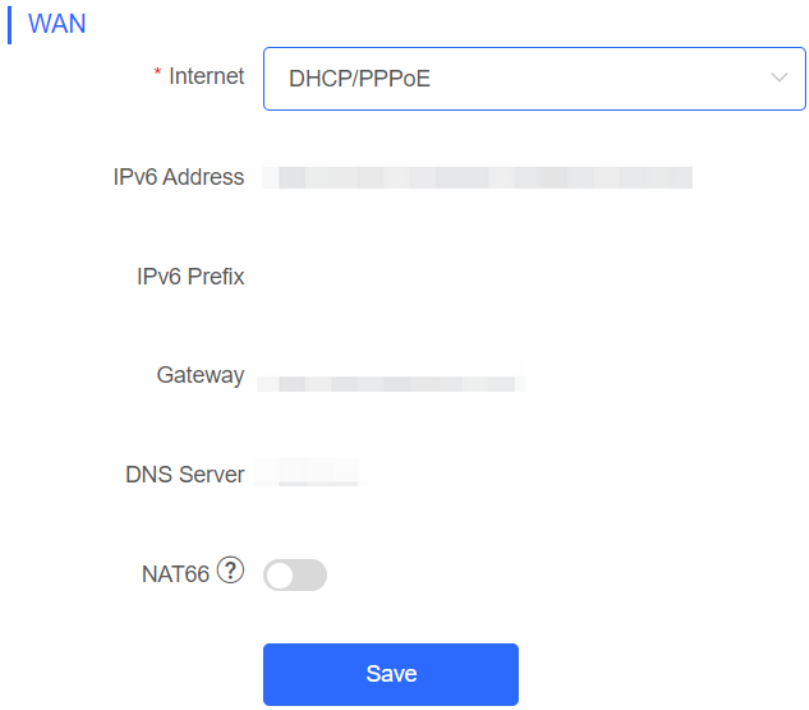


Table 5-2 WAN Port IPv6 Address Configuration Parameters

Parameter	Description
Internet	Specify the method for obtaining an IPv6 address for the WAN port. ● DHCP: The current device acts as a DHCPv6 client and apply for an IPv6 address/prefix from the uplink device. ● Static IP: If this internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server. ● Null: The IPv6 function is disabled on the WAN port.
IPv6 Address	● If **DHCP** is selected, the automatically obtained IPv6 address is displayed. ● If **Static IP** is selected, you need to manually configure this parameter.
IPv6 Prefix	If **DHCP** is selected, and the current device obtains an IPv6 address prefix from the uplink device, then the obtained IPv6 address prefix is displayed.
Gateway	● If **DHCP** is selected, the automatically obtained gateway address is displayed. ● If **Static IP** is selected, you need to manually configure this parameter.
DNS Server	● If **DHCP** is selected, the automatically obtained DNS server address is displayed. ● If **Static IP** is selected, you need to manually configure this parameter.

Parameter	Description
NAT66	If the current device cannot access the internet in DHCP mode or cannot obtain the IPv6 address prefix, you must enable NAT66 to assign the IPv6 address to an intranet client.

5.8.6 Configuring the IPv6 Address for the LAN Port

Choose **Network** > **IPv6** > **LAN**.

When a device accesses the network through DHCP, an uplink device can assign an IPv6 address to a LAN port, and use an IPv6 address prefix to assign IPv6 addresses to clients on the LAN. If the uplink device cannot assign an IPv6 address prefix to the current device, you need to manually configure an IPv6 address prefix for the LAN port, and assign IPv6 addresses to the clients on the LAN by toggling on the **NAT66** switch (see5.8.5 Configuring the IPv6 Address for the WAN Port) to allocate IPv6 addresses to clients on the LAN.

In the **IPv6 Address/Prefix Length** field, enter a local address with a length not greater than 64 bits. This address will also be used as the IPv6 address prefix.

IPv6 Assignment specifies the method for assigning IPv6 addresses for clients. The following options are available:

- **Auto**: Both DHCPv6 and SLAAC are used to assign IPv6 addresses to clients.
- **DHCPv6**: DHCPv6 is used to assign IPv6 addresses to clients.
- **SLAAC**: SLAAC is used to assign IPv6 addresses to clients.
- **Null**: No IPv6 addresses are assigned to clients.

The option selected for IPv6 address assignment is determined by the protocol supported by intranet clients. If you are not sure about the protocol supported by intranet clients, select **Auto**.

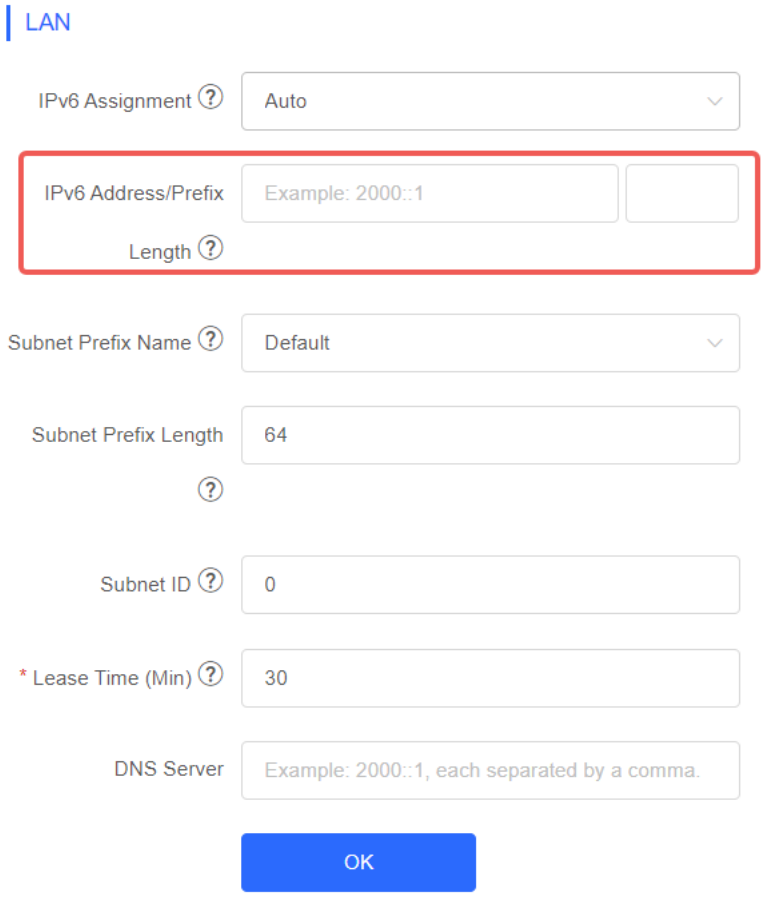


Table 5-3 LAN Port IPv6 Address Configuration Parameters

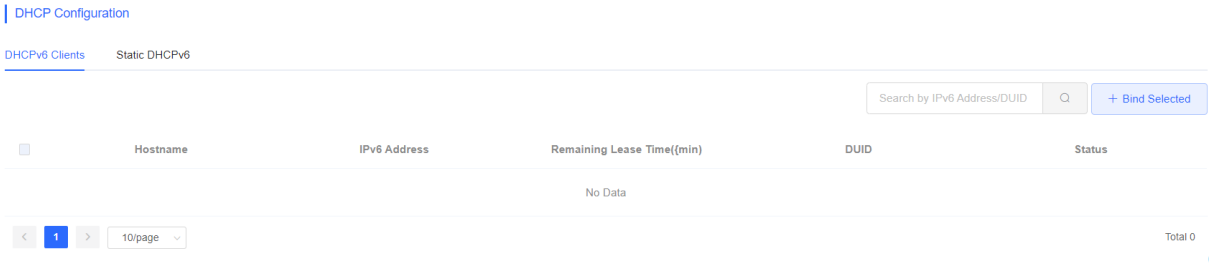
Parameter	Description
Subnet Prefix Name	Set the interface from which the prefix is obtained, for example, WAN_V6. The default value is all interfaces.
Subnet Prefix Length	Set the subnet prefix length. The value ranges from 48 to 64.
Subnet ID	Set the subnet ID in hexadecimal notation. 0 indicates that the subnet ID automatically increments.
Lease Time (Min)	Set the lease of an IPv6 address, in minutes.
DNS Server	Set the address of the IPv6 DNS server.

5.8.7 Viewing DHCPv6 Clients

Choose **Network** > **IPv6** > **DHCP Configuration** > **DHCPv6 Clients**.

When the device acts as a DHCPv6 server to assign IPv6 addresses to clients, you can view information about the clients that obtain IPv6 addresses from the device on the current page. The information includes the host name, IPv6 address, remaining lease time, and DHCPv6 Unique Identifier (DUID) of each client.

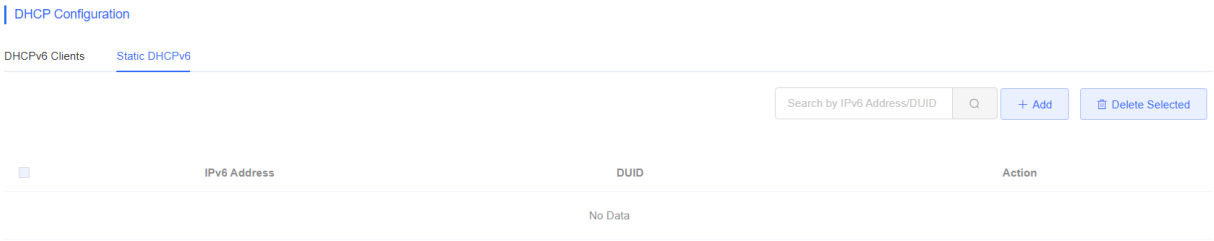
Enter an IPv6 address or DUID in the search box and click to query the target DHCPv6 client.



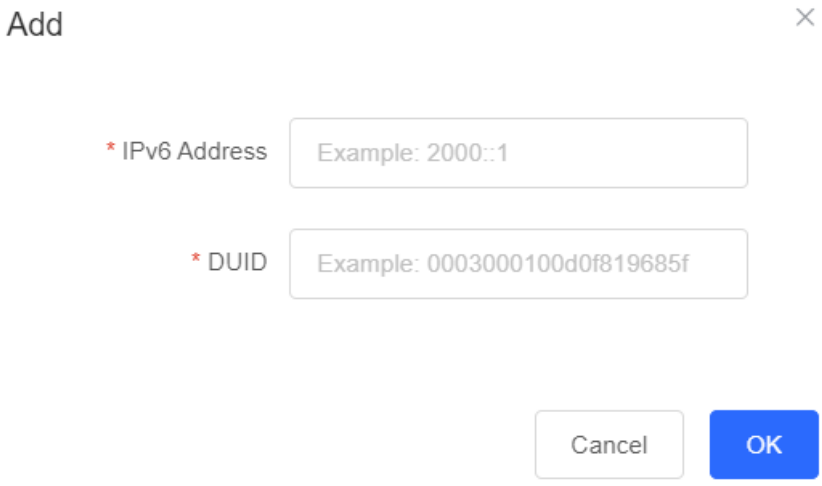
5.8.8 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client, so that the client can obtain the specified address each time.

Choose **Network** > **IPv6** > **DHCP Configuration** > **Static DHCPv6**.



(1) Click **Add**.



(2) Enter the IPv6 address and DUID of the client.

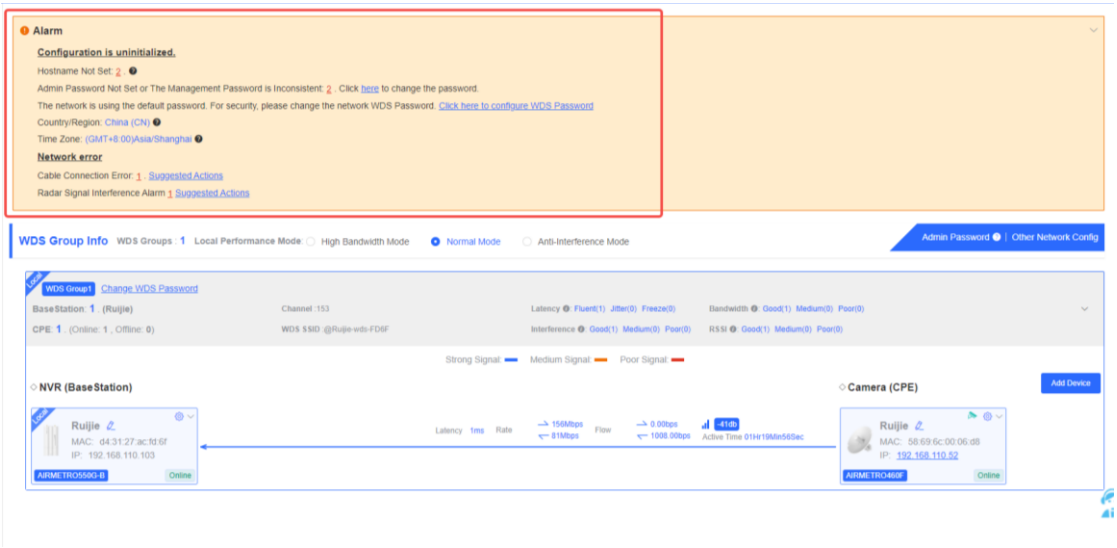
(3) Click **OK**.

6 Alarm and Fault Diagnosis

6.1 Alarm Information and Suggested Action

When bridges fail or lack some necessary security configuration, the system prompts key alarms about the bridges on the homepage, so that users can handle the exceptions promptly.

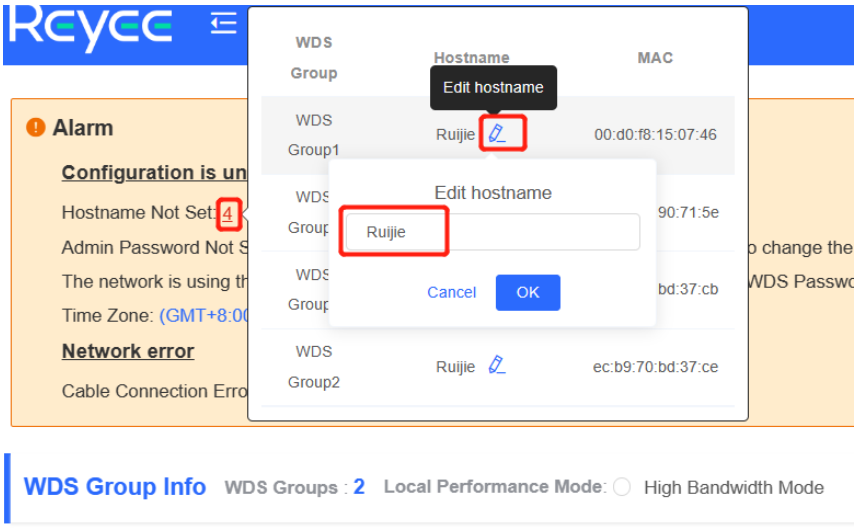
Choose Overview > Alarm.



6.1.1 Default Device Name Is Not Modified

Modifying device names can help you better distinguish each bridge. Unless otherwise specified, you are advised to modify default device names.

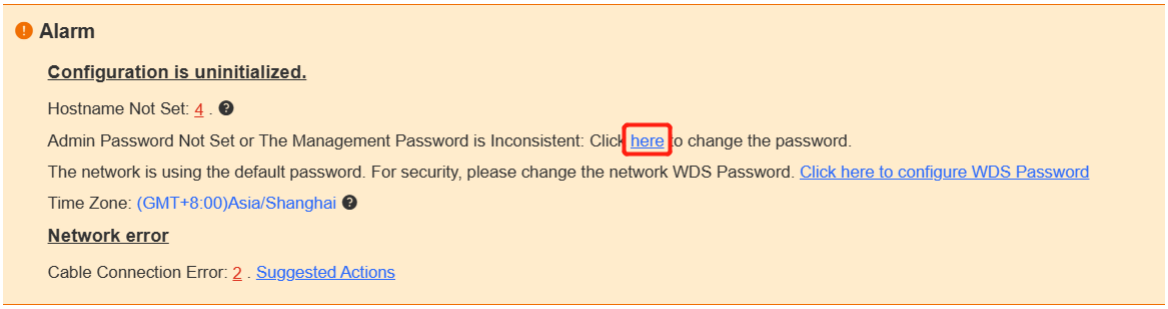
When viewing the alarm, hover the cursor over the orange number of the prompt and click  in the displayed dialog box to modify the name of each device. (The orange number, 2 in the figure, indicates the number of devices that still use the default name in the network.) Enter the new device name and click **OK** to make the change take effect immediately.



6.1.2 Default Admin Password Is Still Used

For device and network security, you are advised to configure the admin password for the network to prevent login of unauthorized users.

Click the prompt to configure the admin password for the network. Hover the cursor over the orange number (1 in the figure) of the prompt to configure the device password. For configuration steps, refer to 6.1.1 Default Device Name Is Not Modified.



Caution

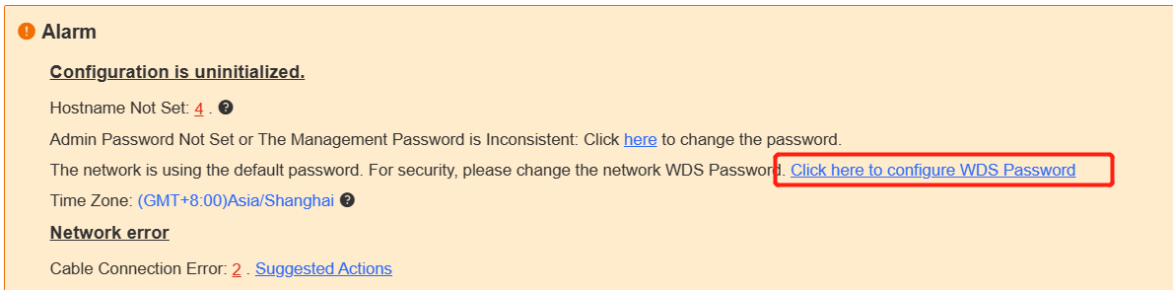
The admin password is used to log in to the web page of any device in the network. Therefore, remember the admin password. If you forget the admin password, restore factory settings. For the method, see 1.3.3 Logging in to the Web Page.

If there is an unbridged device in the network, the function of configuring the admin password will be disabled.

6.1.3 Default WDS Password Is Still Used by All Devices

The default WDS password of devices of the same model is the same. Changing the WDS password can prevent others from illegally accessing the network by using a device of the same model.

Click **Click here to configure WDS Password**, enter the new password, and click **Save** to change the WDS password for the entire network.



Caution

When configuring the WDS password for the entire network, ensure that all devices are online. Otherwise, WDS passwords of the devices will be inconsistent.

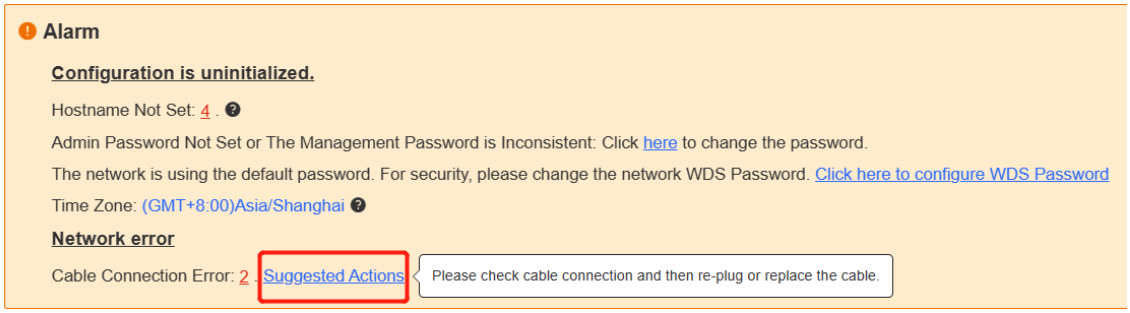
Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation.

If there is an unbridged device in the network, the function of configuring the WDS password for the entire network will be disabled.

6.1.4 Network Cable Is Disconnected or Incorrectly Connected

Hover the cursor over the orange number of the prompt to display the alarm details.

Click the suggested action to check the solution.



6.1.5 Latency Is High or Bandwidth Is Insufficient

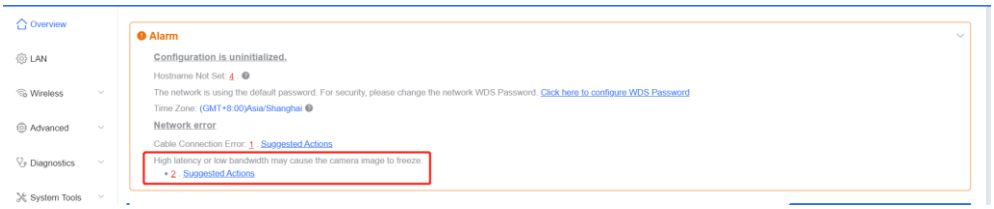
First, check whether the device latency is too high. If yes, the interference in the environment may be severe. Then, you are advised to change to a channel with smaller interference.

If not, increase the channel width. For channel settings, see 2.13.3 2. Configuring the Channel Width.

To check whether the latency is too high, perform as follows:

Hover the cursor over the orange number of the prompt to display all WDS groups, and click a group to display the details.

On the **Overview** page, check whether **Latency** is **Freeze**. If so, the latency is too high. Otherwise, the latency is normal.

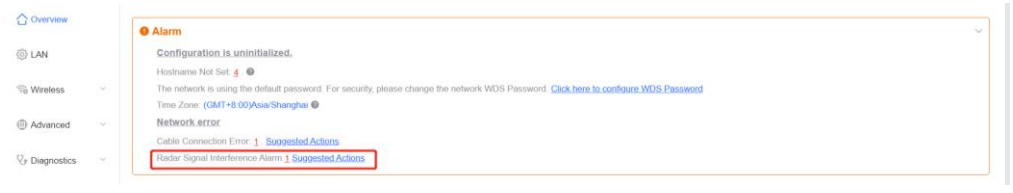


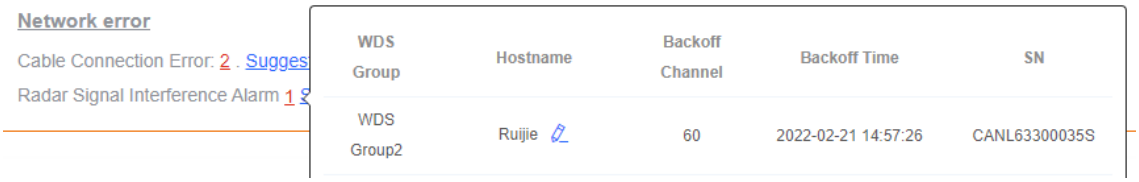
Caution

Channel and channel width settings described in this section are performed on the local device. You can click the IP address of a device to open the management page of the device and set the channel and channel width.

6.1.6 Radar Signal Interference

When the device detects a radar signal in a channel, it generates an alarm and automatically switches the channel. Hover the cursor over the orange number of the prompt to display alarm details.





According to the information about the WDS group and back-off channel in the alarm record, check whether the current working channel in the WDS group (group 2 in the example) is consistent with the back-off channel. (See 2.9 Displaying WDS Group Information.) If so, manually switch the channel to a non-dynamic frequency selection (DFS) channel. For the setting method, see 2.13.3 1. Configuring the Channel.

Note

Non-DFS channels include 36-48 and 149-165.

Detecting radar signal interference is supported on RG-EST310, RG-EST310 V2, RG-EST350 and RG-EST350 V2 only.

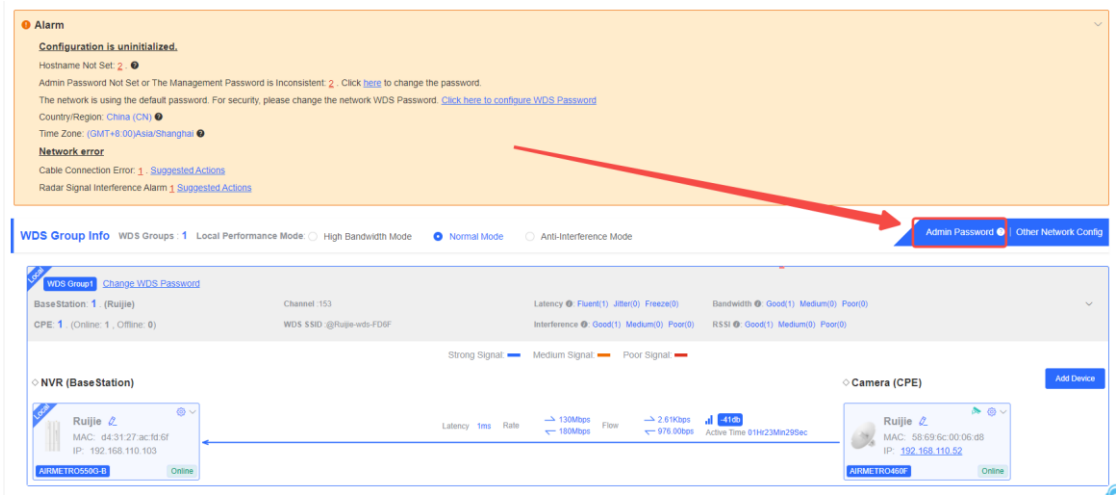
Note

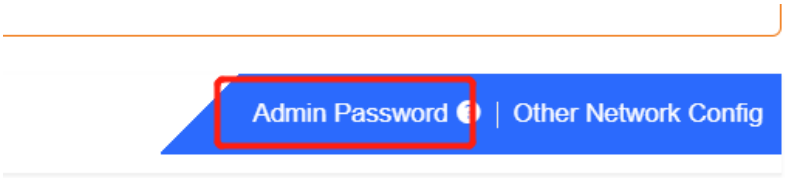
If the preceding troubleshooting steps fail to resolve the issue, and remote assistance from technical support is needed, you can contact them to assist in enabling the developer mode. The technical support team can then perform diagnostics to identify and address the issue effectively.

7 System Settings

7.1 Configuring Management Password

Choose Overview > Admin Password

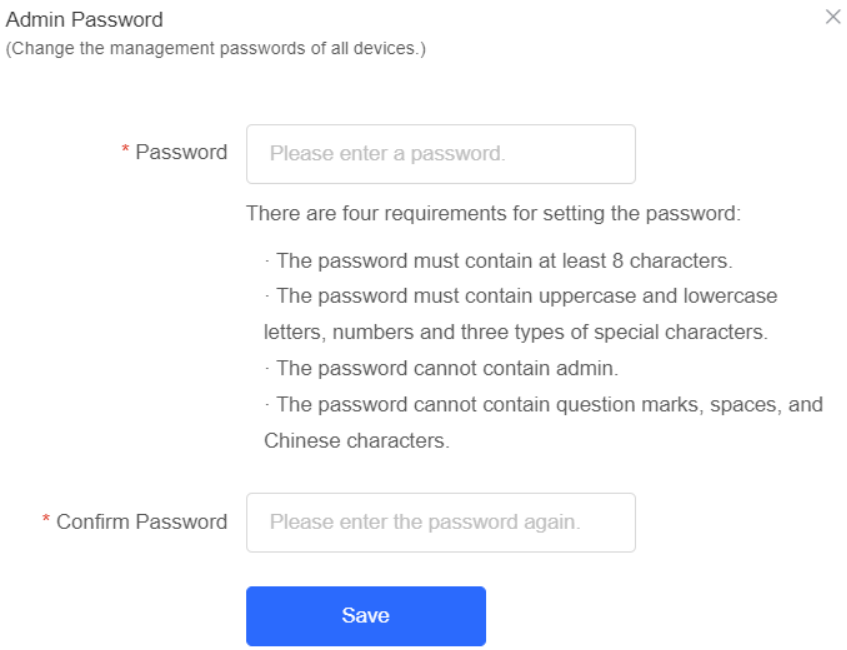




Click **Admin Password** to change the login password for all devices.

If there is an unbridged device in the network, the link will be unavailable.

Hover the cursor over to view the help information.



Caution

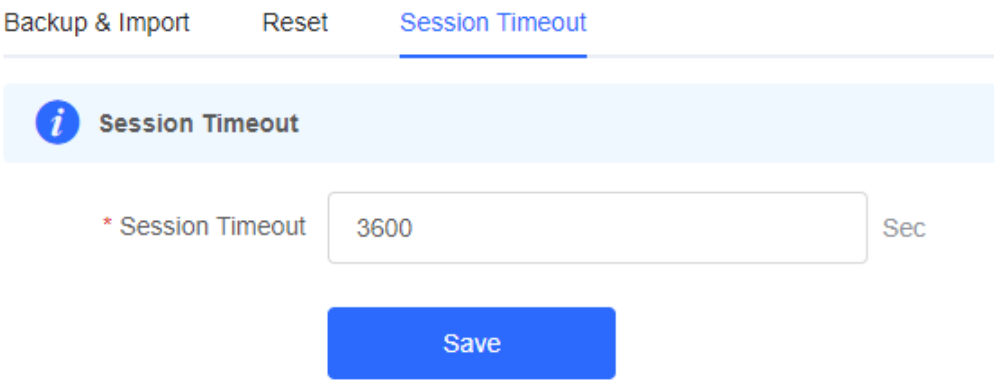
This password is used to log in to Eweb system of any device in the network.

If there is an unbridged network in the network, the function of configuring the admin password will be disabled.

7.2 Configuring Session Timeout Duration

Choose System > Management > Session Timeout.

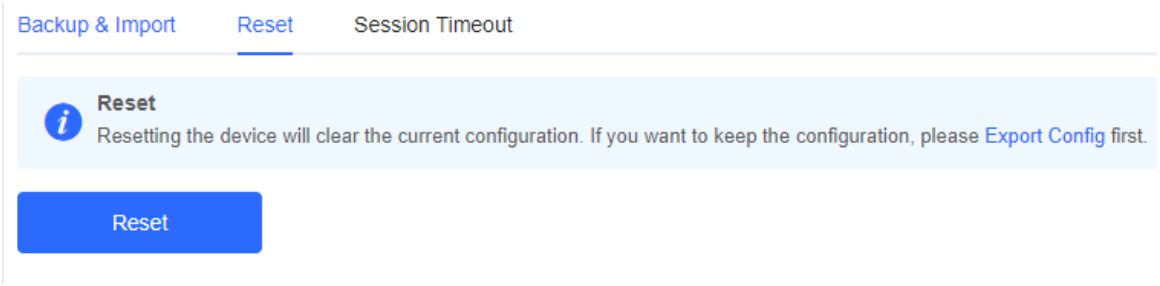
If no operation is performed on the page within a period of time, the session will be down. When you need to perform operations again, enter the password to open the configuration page. The default timeout duration is 3600 seconds, that is, 1 hour.



7.3 Resetting Factory Settings

Choose System > Management > Reset

Click **Reset** to restore factory settings.



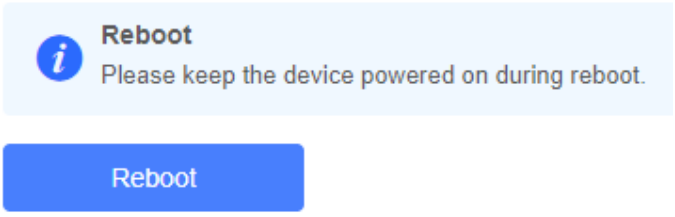
Caution

This operation will clear existing settings and restart the device. Therefore, exercise caution when performing this operation. If there is any configuration in the current system, please export the configuration before resetting the device.

7.4 Rebooting the Device

Choose System > Reboot > Reboot

Click **Reboot** to reboot the device immediately.



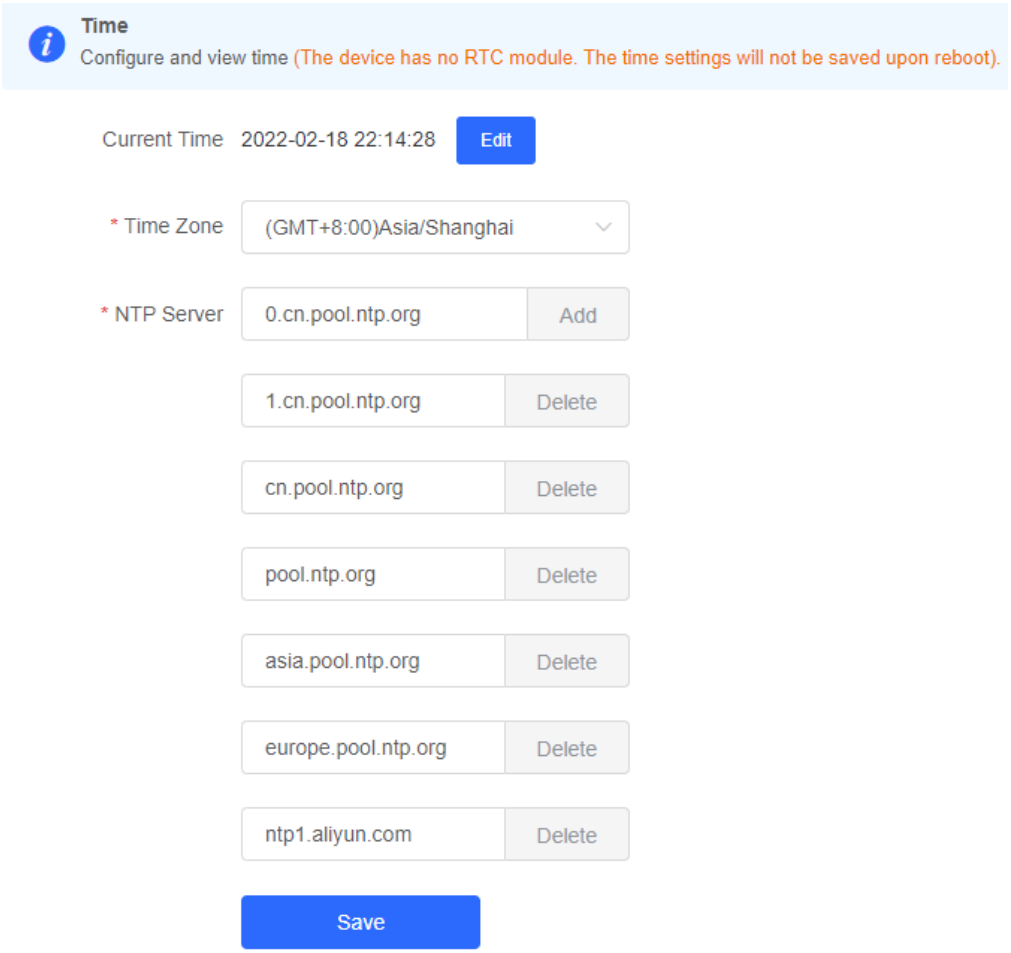
Caution

Please keep the device powered on during reboot. Otherwise, the device may be damaged.

7.5 Configuring System Time

Choose System > Time.

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the bridge supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.

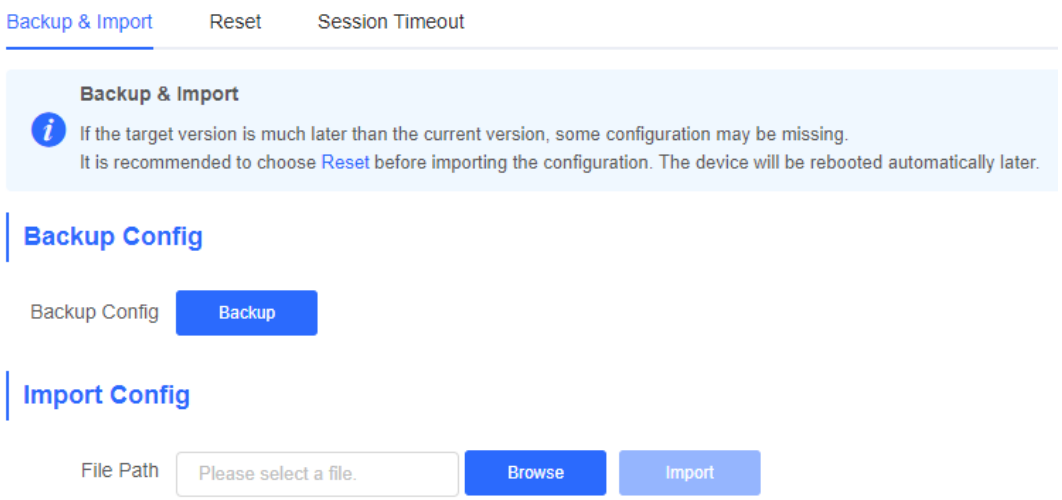


7.6 Configuring Config Backup and Import

Choose System > Management > Backup & Import

Configure backup: Click **Backup** to download a configuration file locally.

Configure import: Click **Browse**, select a configuration file backup on the local PC, and click **Import** to import the configuration file. The device will restart.



7.7 Performing Update and Displaying the System Version

7.7.1 Online Update

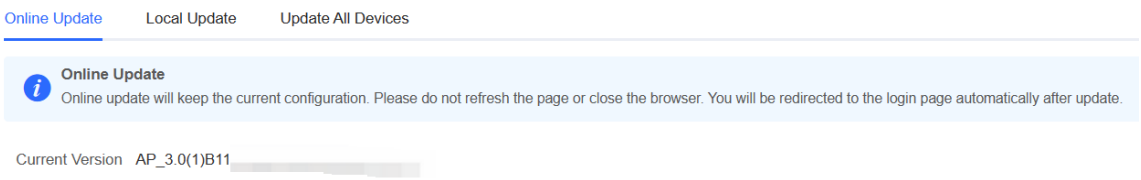
Choose System > Update > Online Update.

If there a new version available, you can click it for an update.

Caution

After being updated, the device will reboot. Therefore, exercise caution when performing this operation.

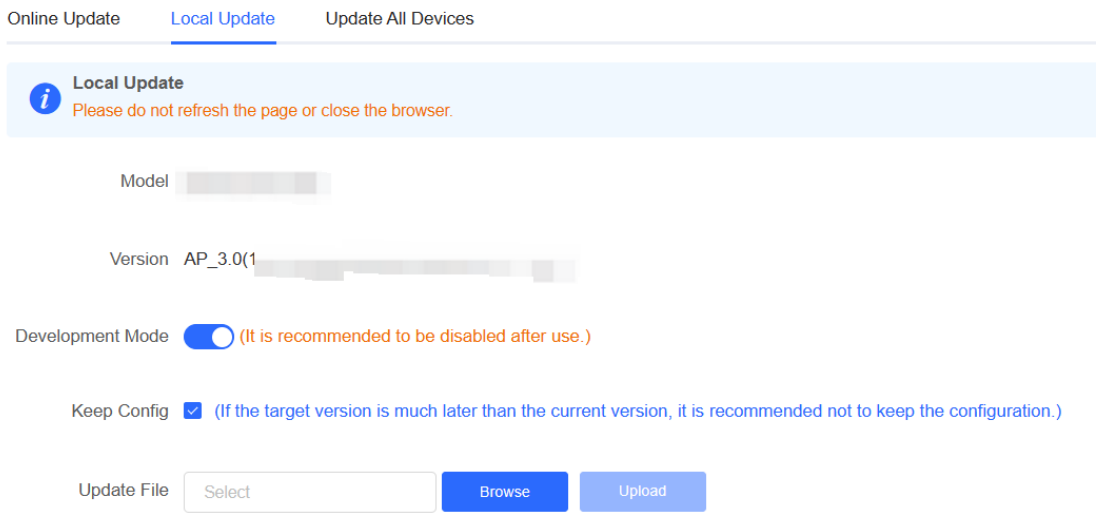
If no version update is detected or online update cannot be performed, check whether the bridge is connected to the Internet.



7.7.2 Local Update

Choose System > Update > Local Update.

You can view the current software version, hardware version and device model. If you want to update the device with the configuration retained, check **Keep Config**. Click **Browse**, select an update package on the local PC, and click **Upload** to upload the file. The device will be updated.



Caution

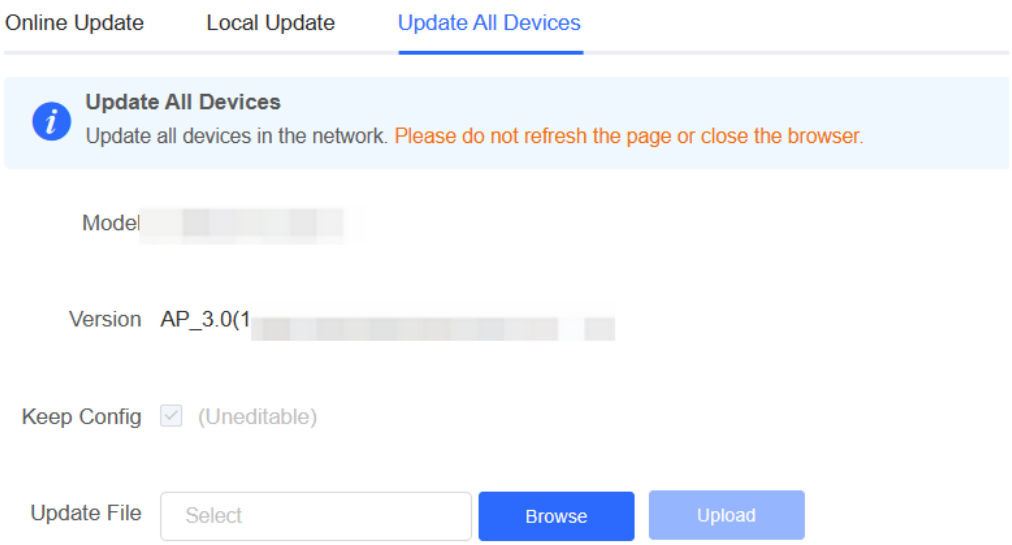
After being updated, the device will reboot. Therefore, exercise caution when performing this operation.

7.7.3 Update All Devices

Choose System > Update > Update All Devices.

You can view the current software version, hardware version and device model. You are advised to update all devices with configuration data retained.

Click **Browse**, select an update package on the local PC, and click **Upload** to upload the file. In the pop-up page, click **Details** to check the target update package and devices. Click **Update** to start updating all devices.

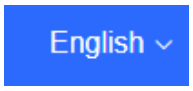


Caution

After being updated, all devices in the network will reboot, which may take a long time. Therefore, exercise caution when performing this operation.

After the update is complete, please log in to Eweb to check the software version number (see 2.10 Displaying the Information About a Single Device). If update fails, please choose **Local Update** or **Update All Devices** to perform update again.

7.8 Switching System Language

Click 

in the upper right corner of the page.

Select the target language from the drop-down list.

Note

Only Chinese and English are available.

7.9 Configuring SNMP

Note

SNMP is supported on RG-AirMetro550G-B, RG-AirMetro460F and RG-AirMetro460G only.

7.9.1 Overview

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

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

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

7.9.2 Global Configuration

1. Overview

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

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

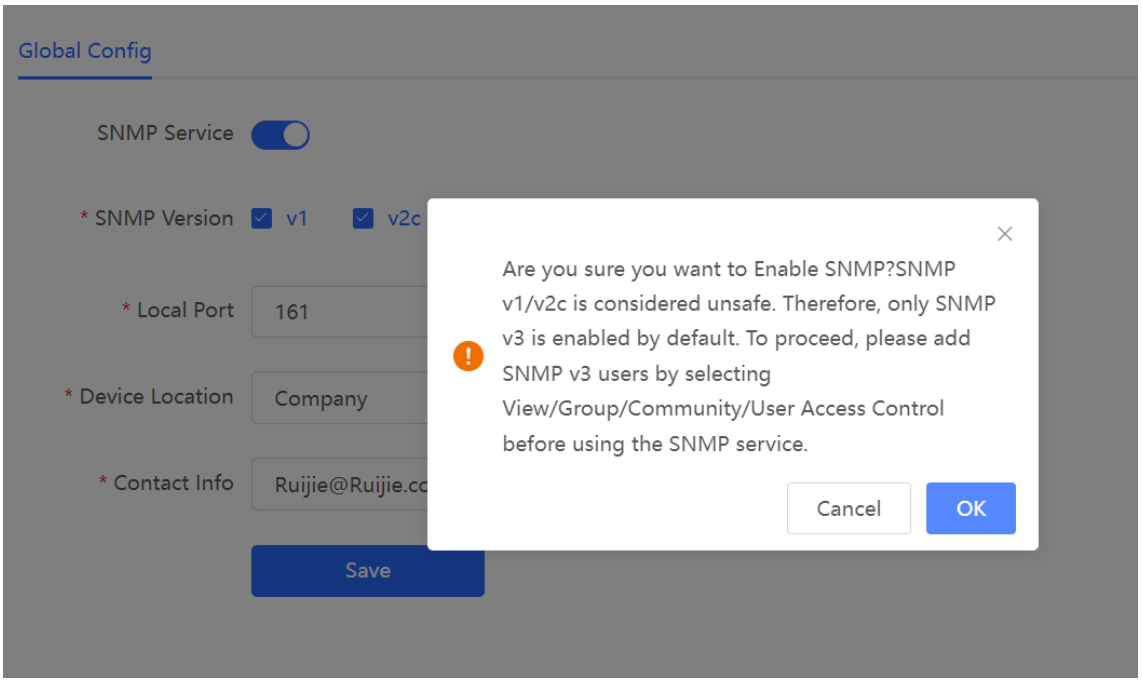
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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

2. Configuration Steps

System > SNMP > Global Config

(1) Enable the SNMP service.



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

(2) Set SNMP service global configuration parameters.

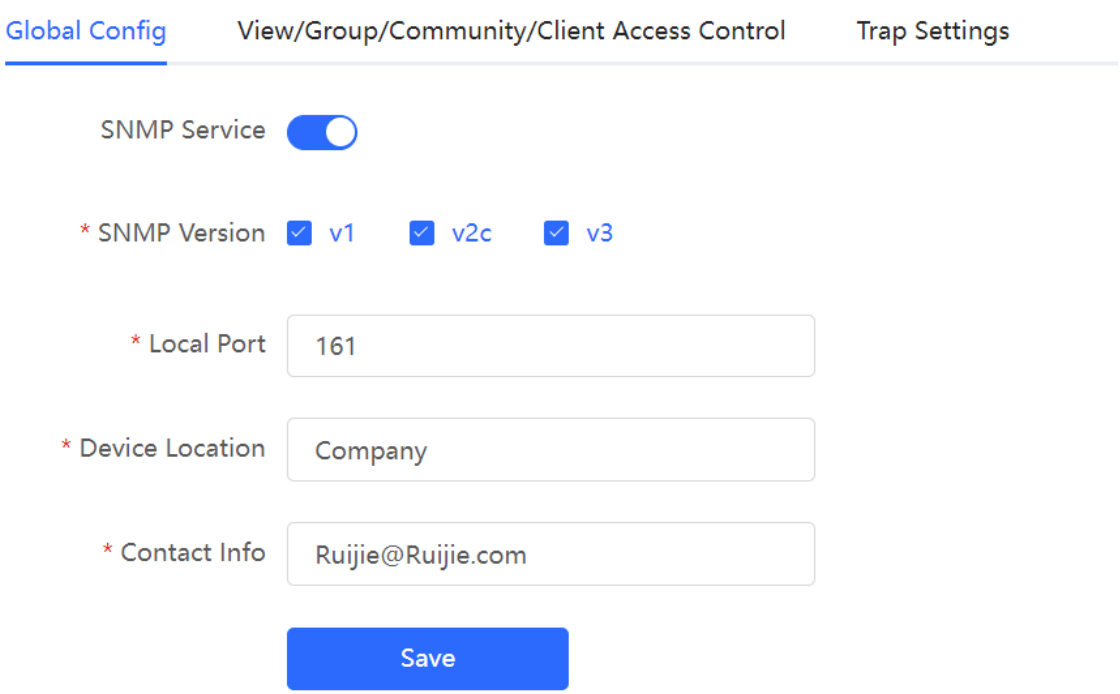


Table 7-1 Global Configuration Parameters

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

(3) Click **Save**.

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

7.9.3 View, Group, Community, User Access Control

1. Configuring Views

- Overview

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

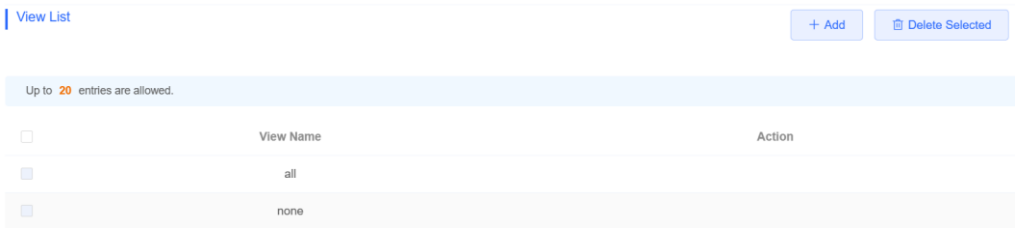
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

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

- Configuration Steps

System > SNMP > View/Group/Community/Client Access Control

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



(2) Configure basic information of a view.

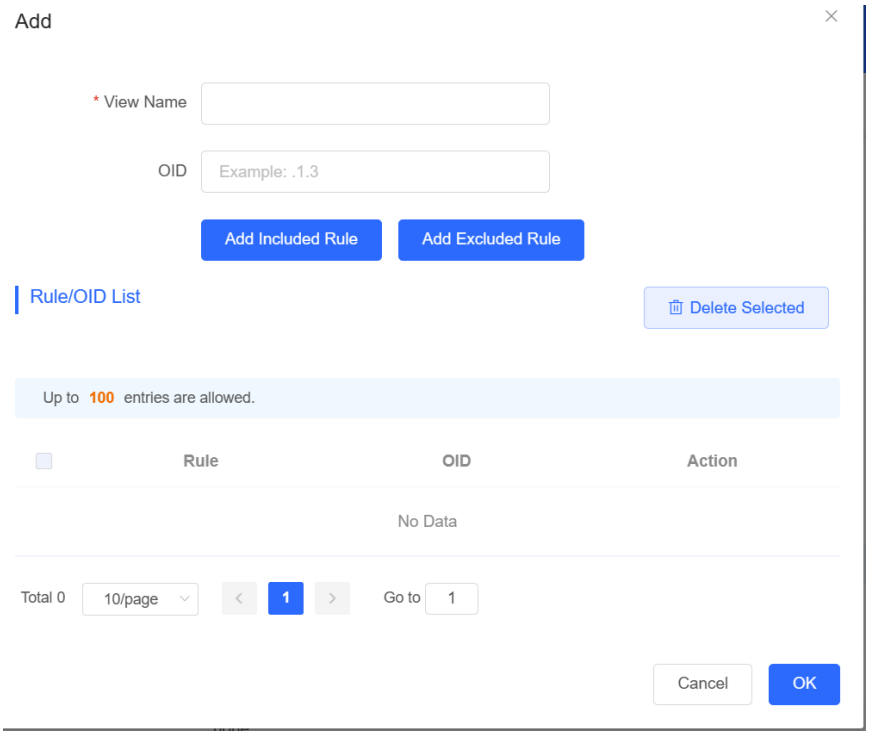


Table 7-2 View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.

Parameter	Description
Type	There are two types of rules: included and excluded rules. The included rule only allows access to OIDs within the OID range. Click Add Included Rule to set this type of view. Excluded rules allow access to all OIDs except those in the OID range. Click Add Excluded Rule to configure this type of view.

Note

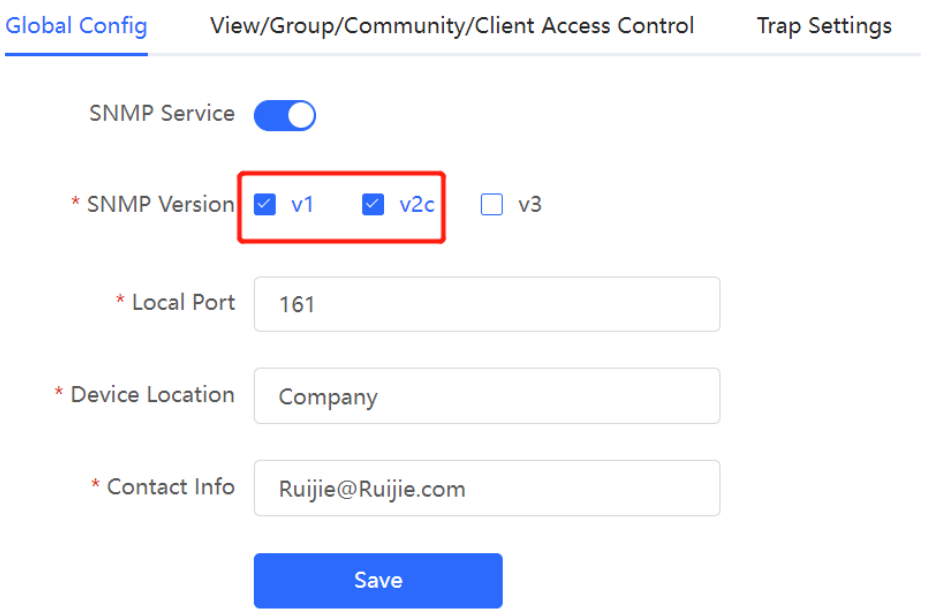
A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1 and v2c Users

- Overview

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



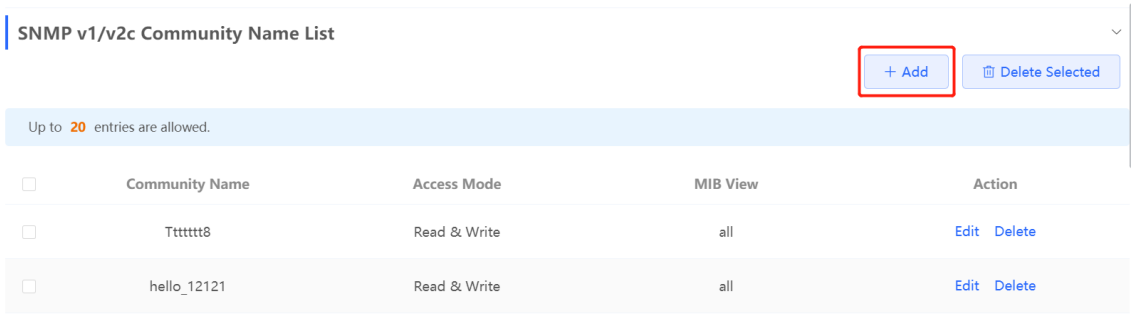
Note

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

- Configuration Steps

System > SNMP > View/Group/Community/Client Access Control

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



(2) Add a v1/v2c user.

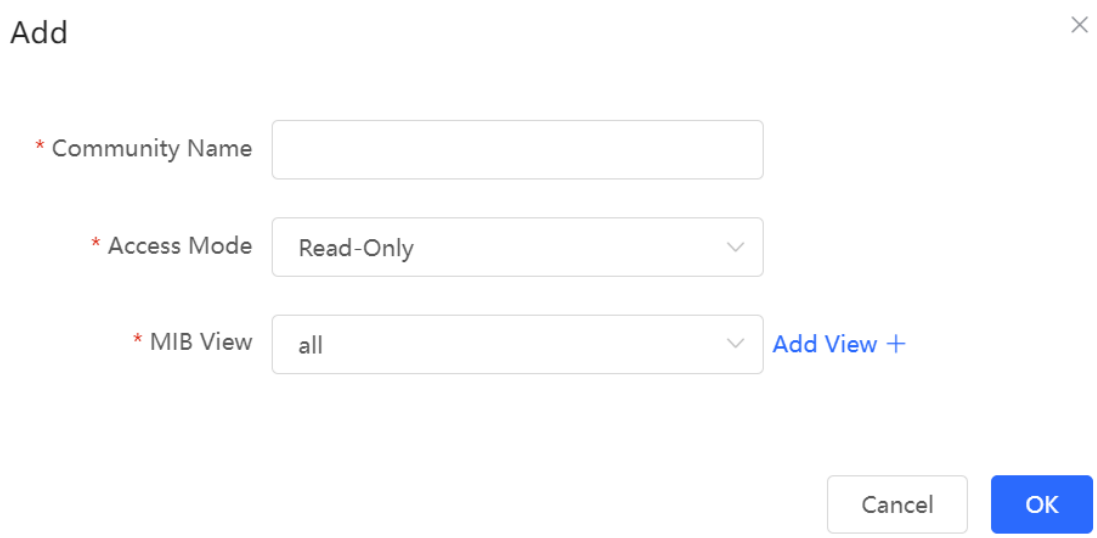


Table 7-3 v1/v2c User Configuration Parameters

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

Note

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

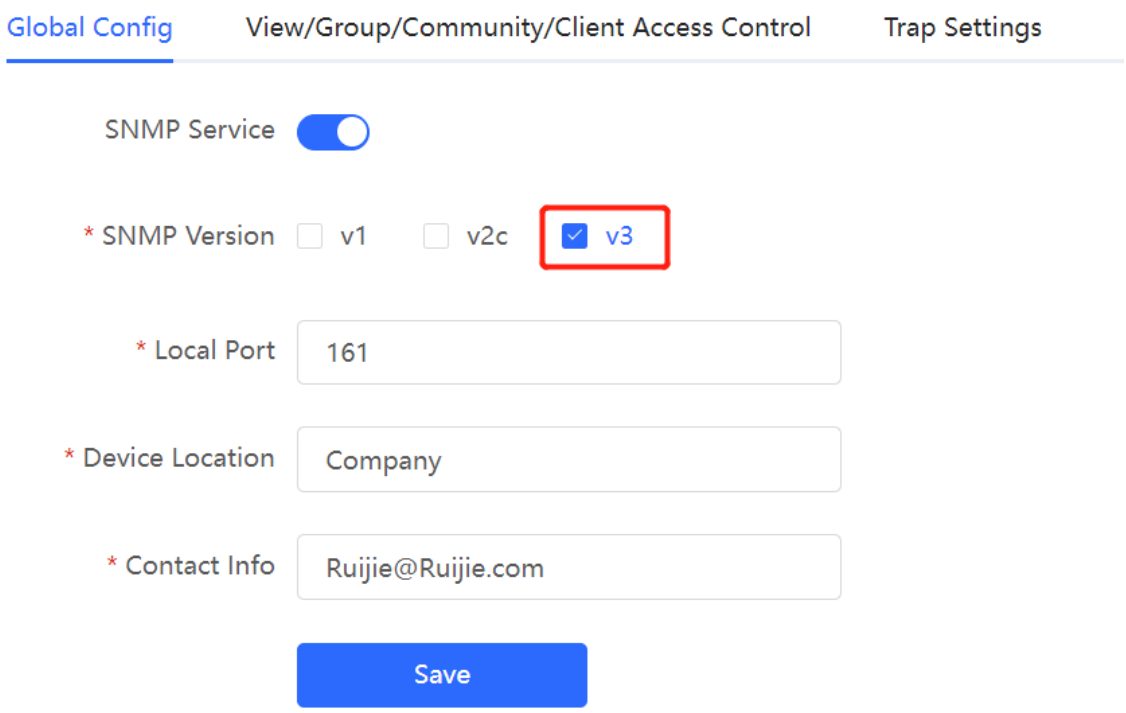
3. Configuring v3 Groups

- Overview

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

- Prerequisites

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



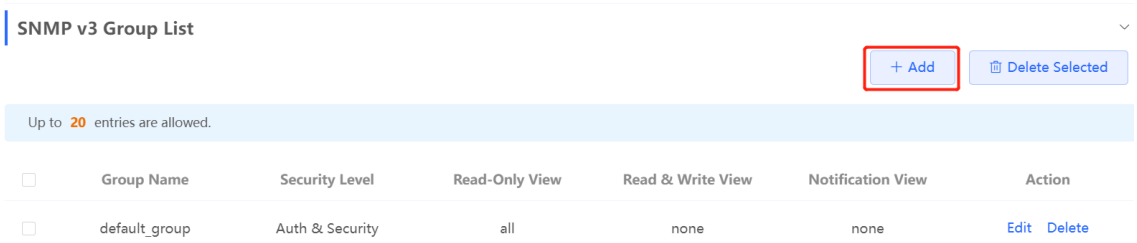
Note

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

- Configuration Steps

System > SNMP > View/Group/Community/Client Access Control

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



(2) Configure v3 group parameters.

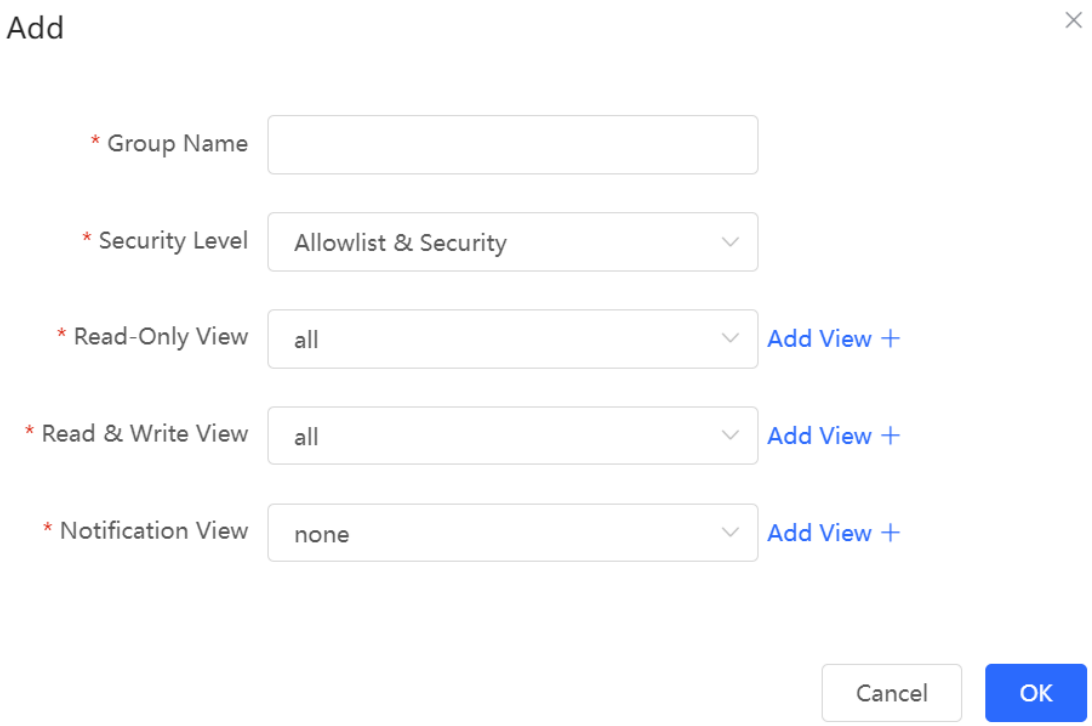


Table 7-4 v3 Group Configuration Parameters

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

Parameter	Description
Read & Write View	The options under the drop-down box are configured views (default: all, none).
Notify View	The options under the drop-down box are configured views (default: all, none).

Note

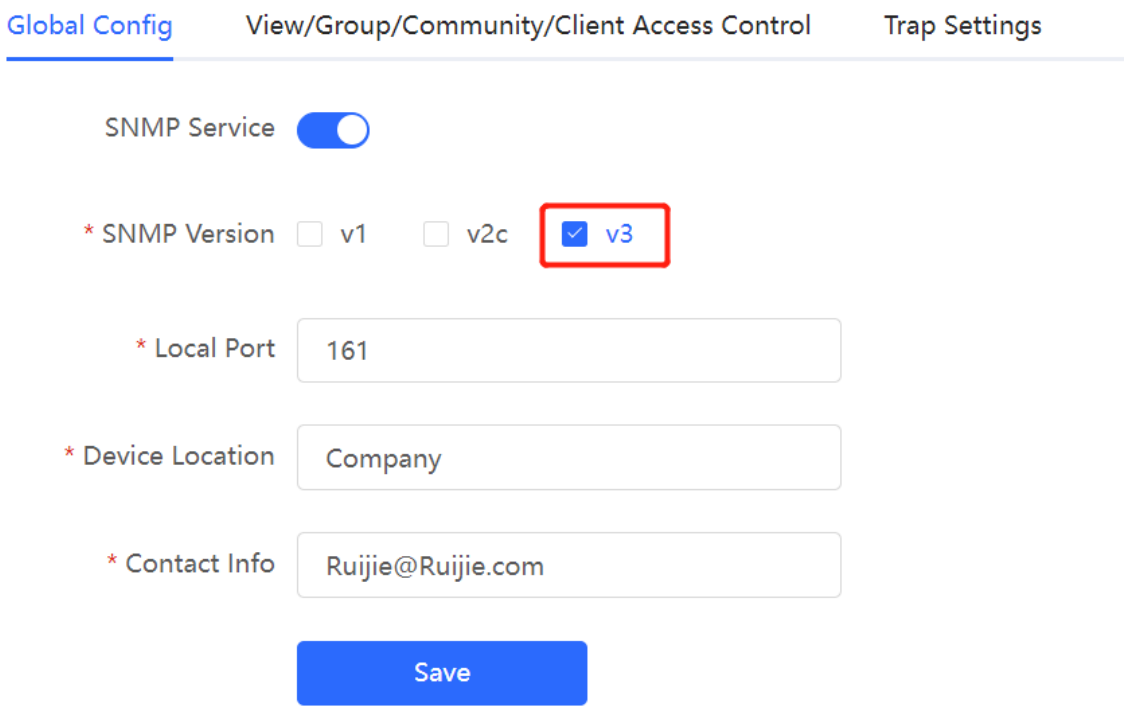
- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

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



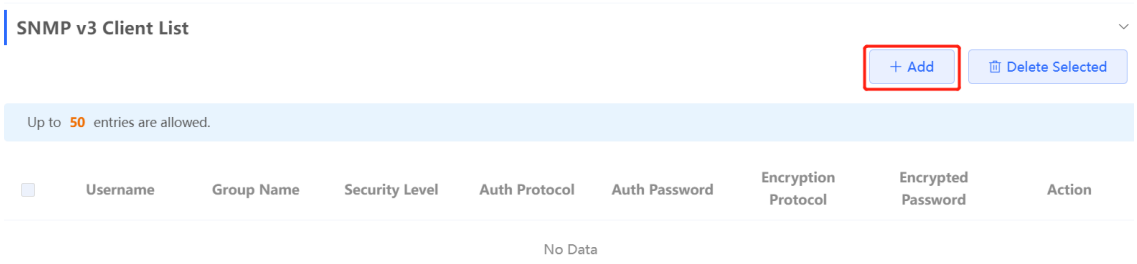
Note

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

- Configuration Steps

System > SNMP > View/Group/Community/Client Access Control

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



(2) Configure v3 user parameters.

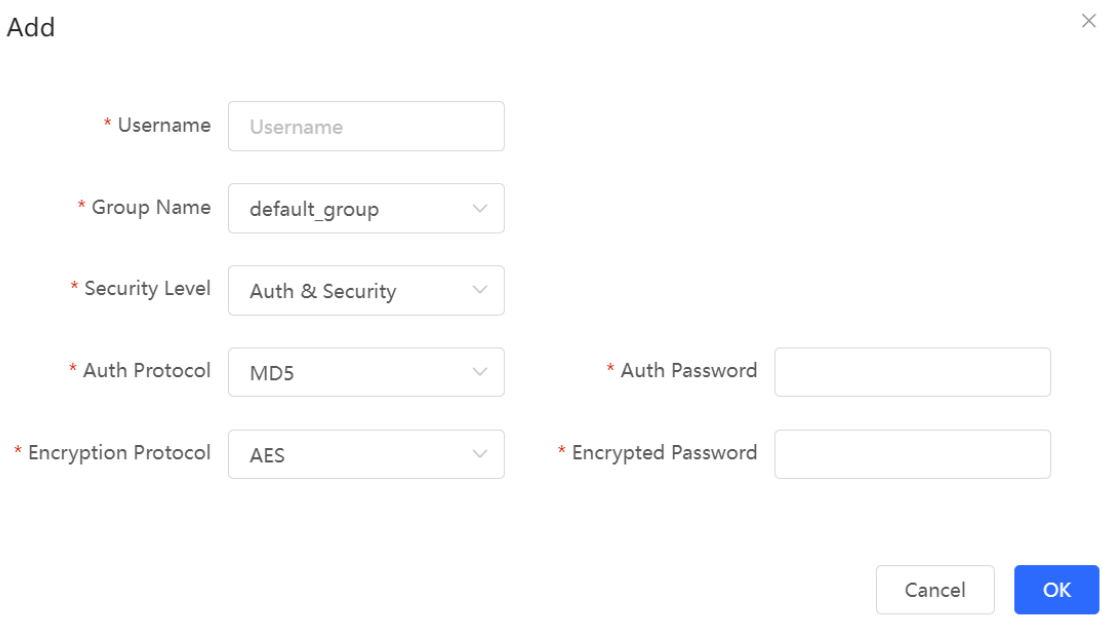


Table 7-5 v3 User Configuration Parameters

Parameter	Description
Username	Username At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Group Name	Indicates the group to which the user belongs.
Security Level	Indicates the security level (authentication and encryption, authentication but no encryption, and no authentication and encryption) of the user.

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

Note

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

7.9.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

- Application Scenario

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

- Configuration Specification

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

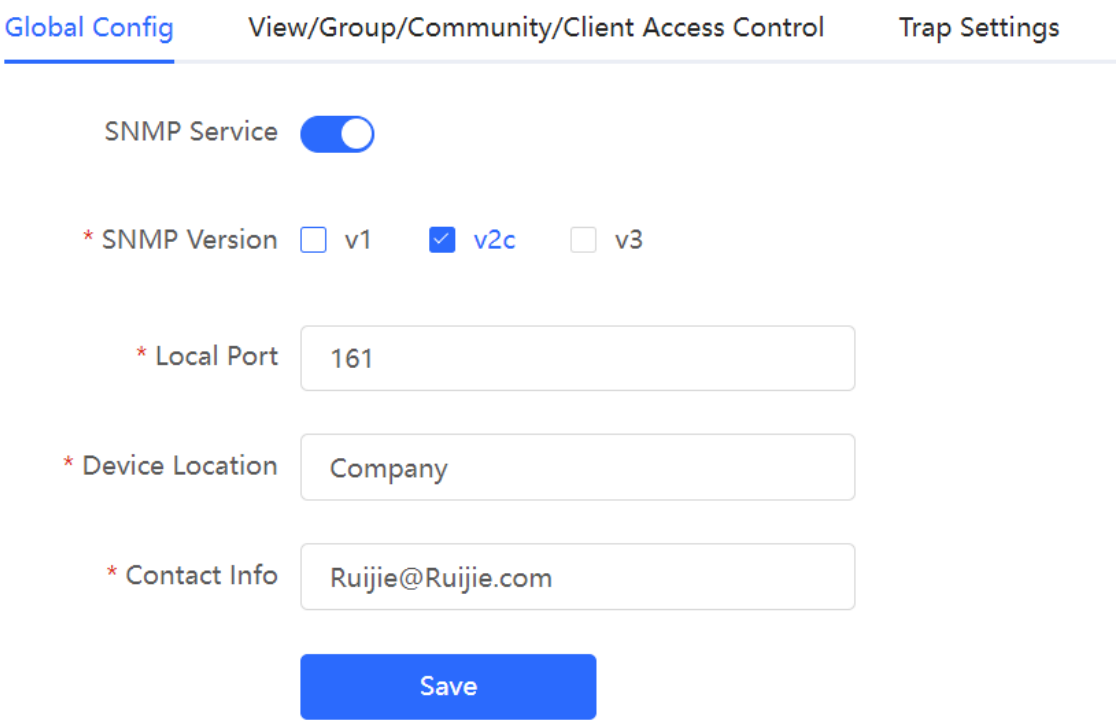
Table 7-6 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "public", and the default port number is 161.

Item	Description
Read & write permission	Read-only permission.

- Configuration Steps

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

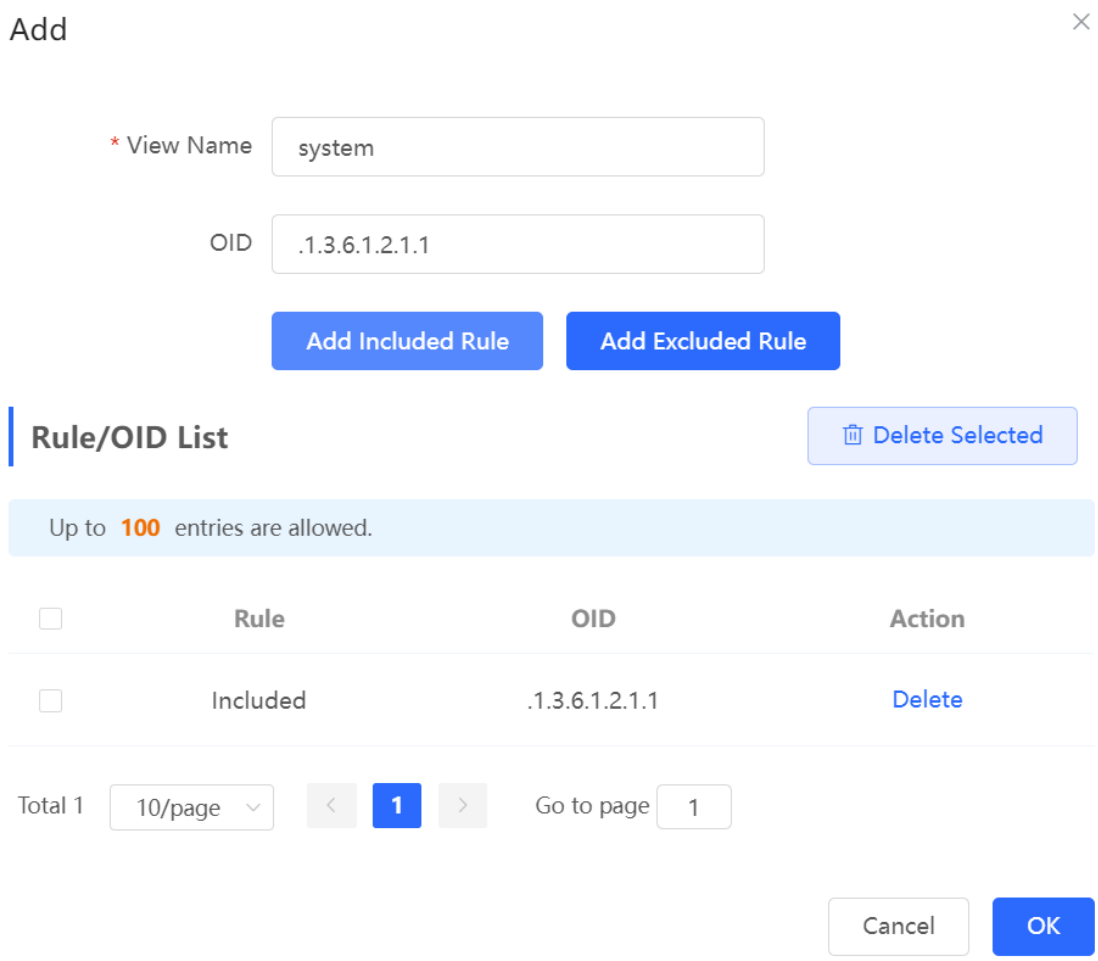


(2) Add a view on the View/Group/Community/Client Access Control interface.

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

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

c Click **OK**.

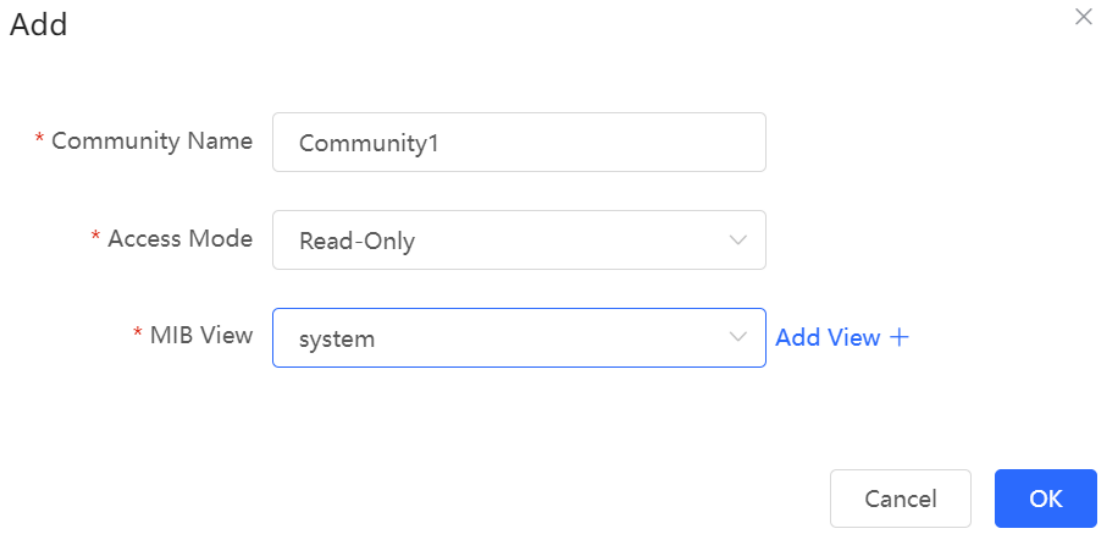


(3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.

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

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

c Click **OK**.



2. Configuring SNMP v3

- Application Scenario

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

- Configuration Specification

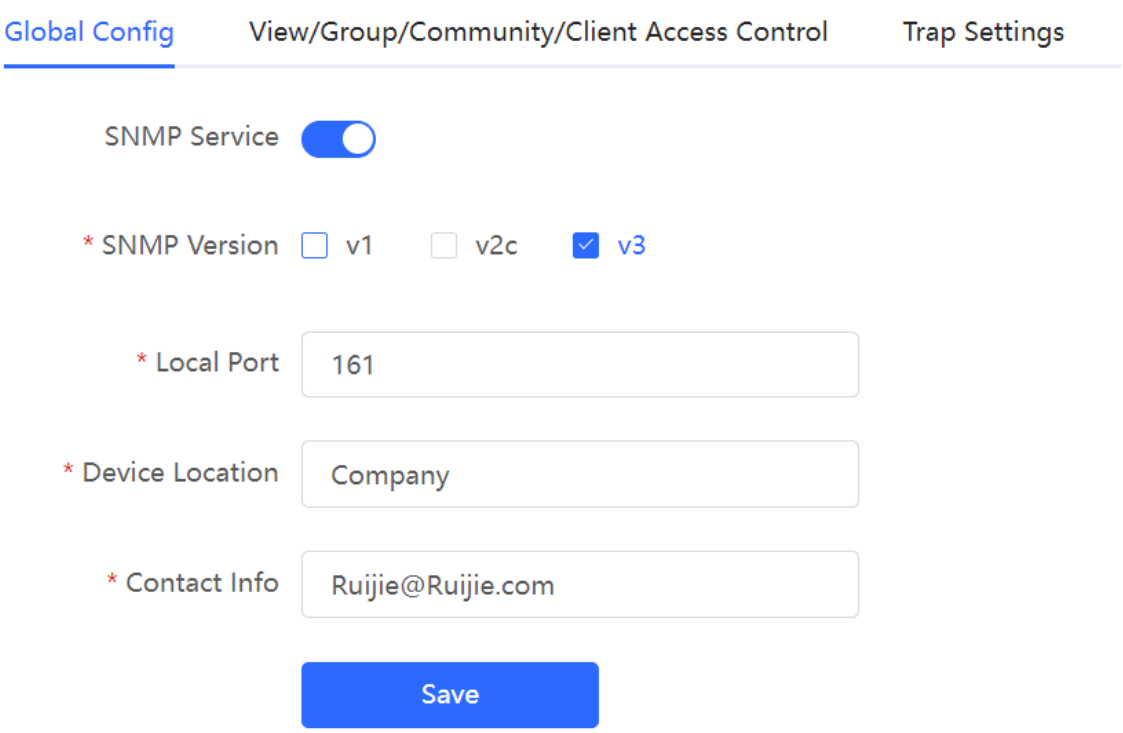
According to the user's application scenario, the requirements are shown in the following table:

Table 7-7 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.
Configuring v3 Users	User name: v3_user Group name: group Security level: authentication and encryption Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123
Version	For SNMP v3, the default port number is 161.

- Configuration Steps

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

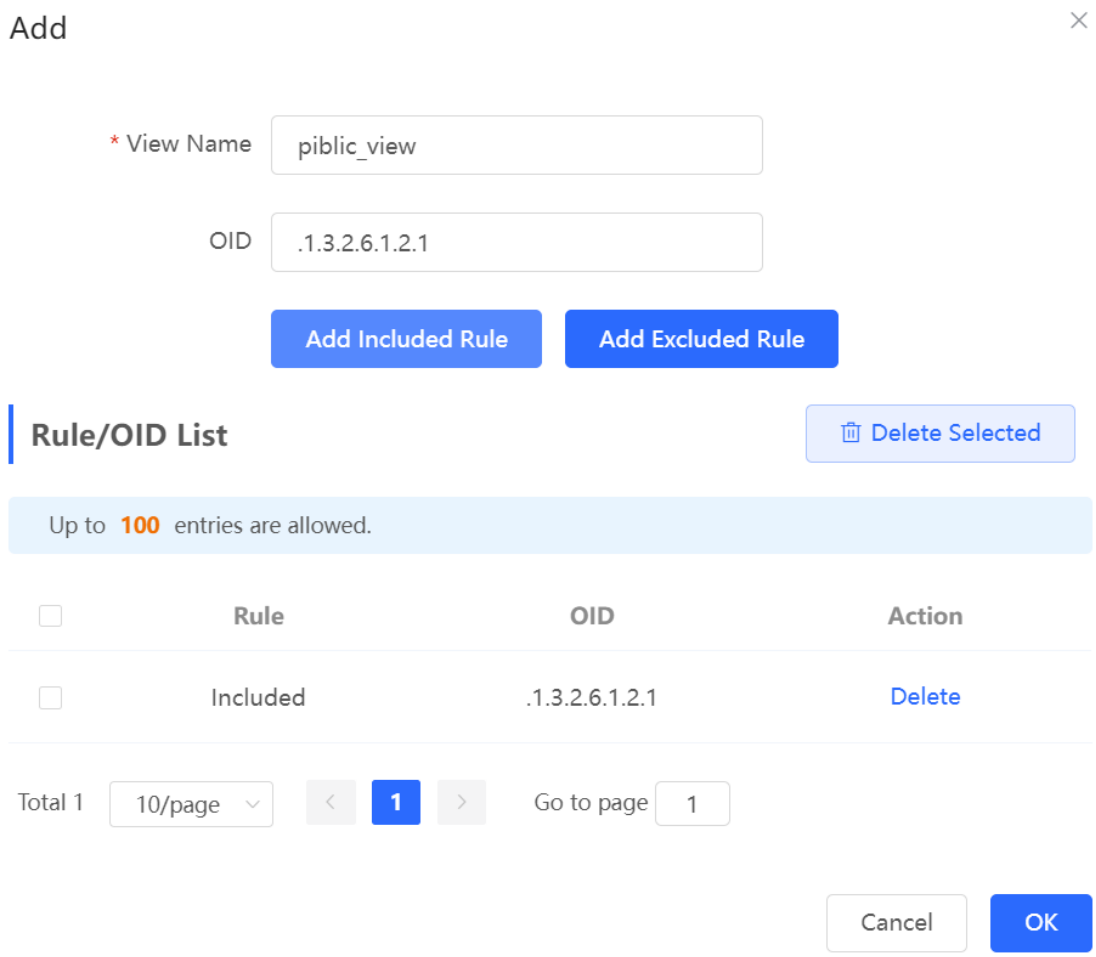


(2) Add a view on the View/Group/Community/Client Access Control interface.

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

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

c Click **OK**.

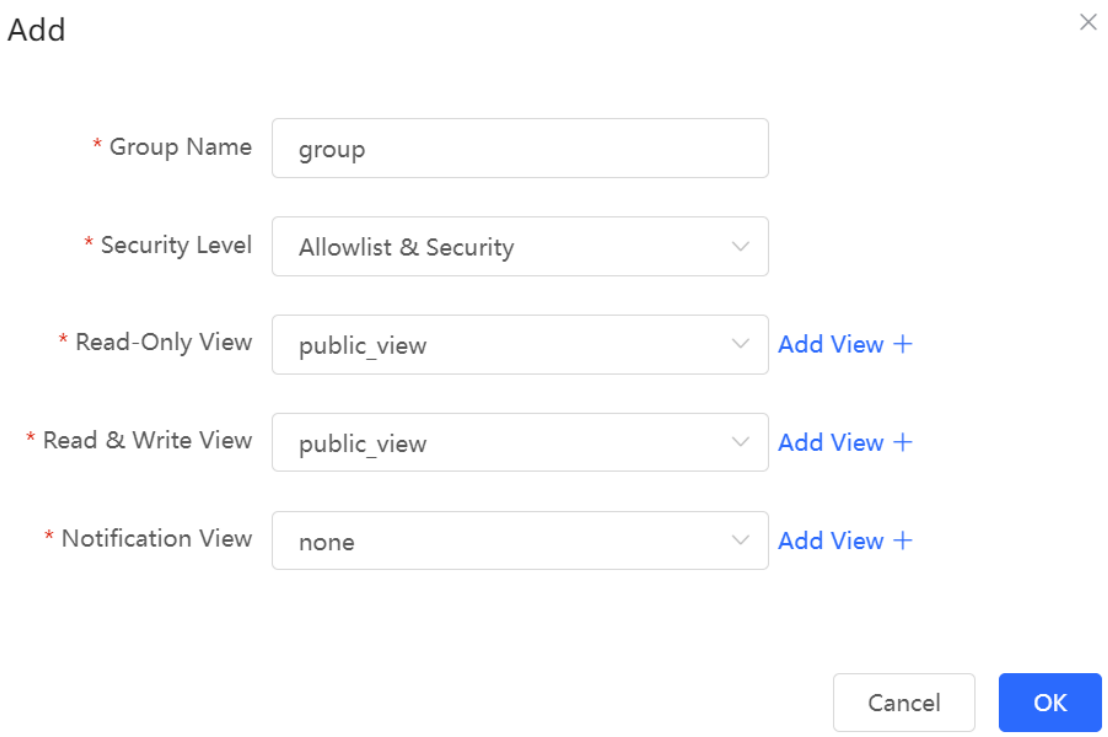


(3) On the View/Group/Community/Client Access Control interface, add an SNMP v3 group.

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

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

c Click **OK**.

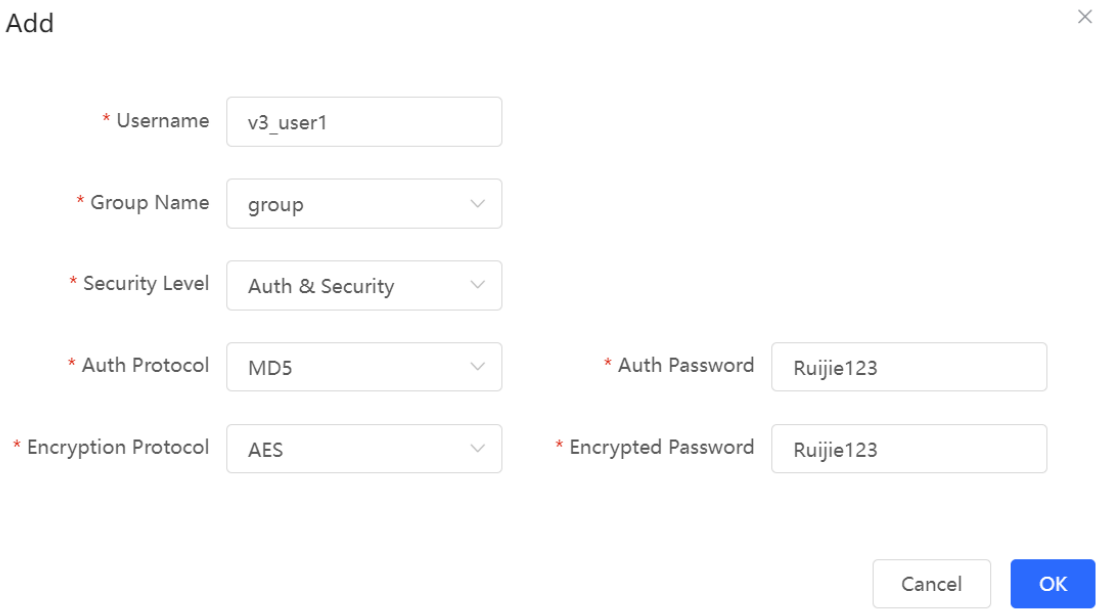


(4) On the View/Group/Community/Client Access Control interface, add an SNMP v3 user.

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

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

c Click **OK**.



7.9.5 Configuring Trap Service

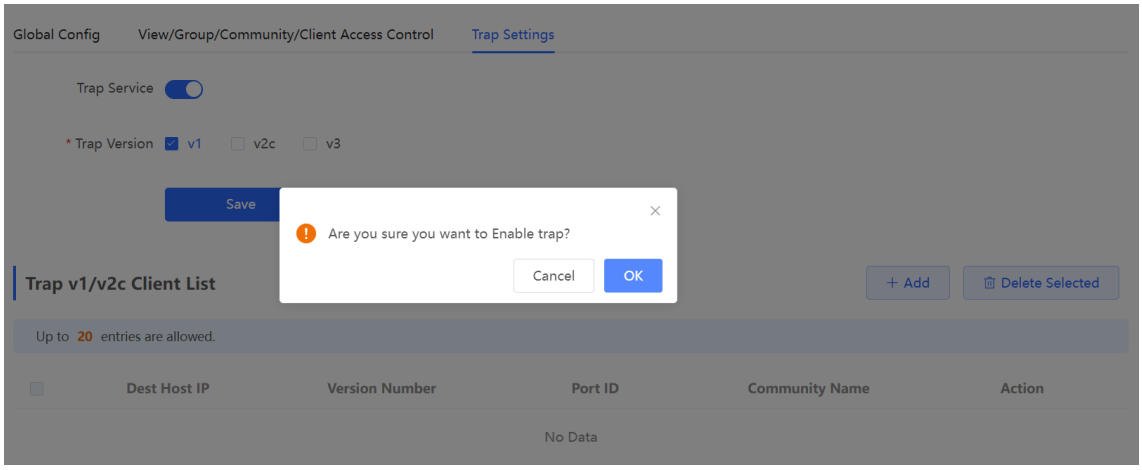
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring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

1. Enabling Trap Service

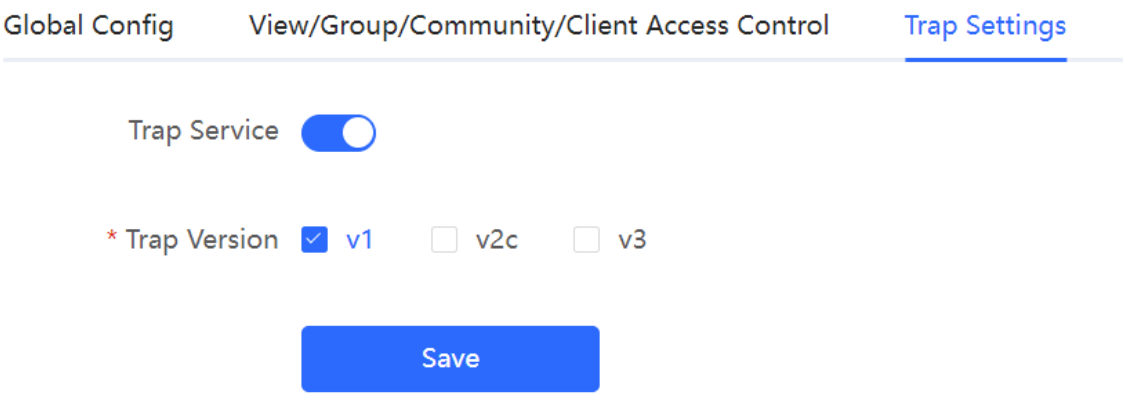
Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

System > SNMP > Trap Setting

(1) Enable the trap service.



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



(2) Set the trap version.

The trap versions include v1, v2c, and v3.

(3) Click **OK**.

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

2. Configuring Trap v1 and v2c Users

- Overview

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

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

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

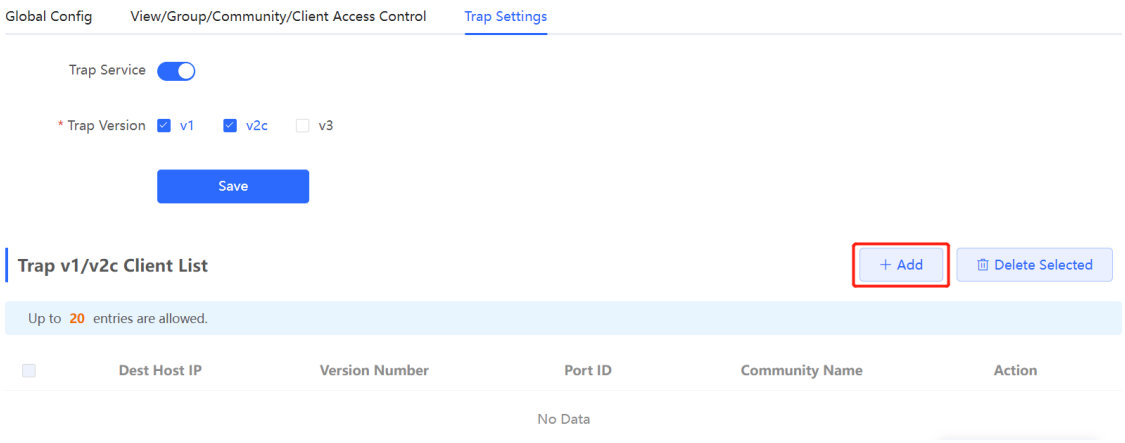
- Prerequisites

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

- Procedure

System > SNMP > Trap Setting

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



(2) Configure trap v1/v2c user parameters.

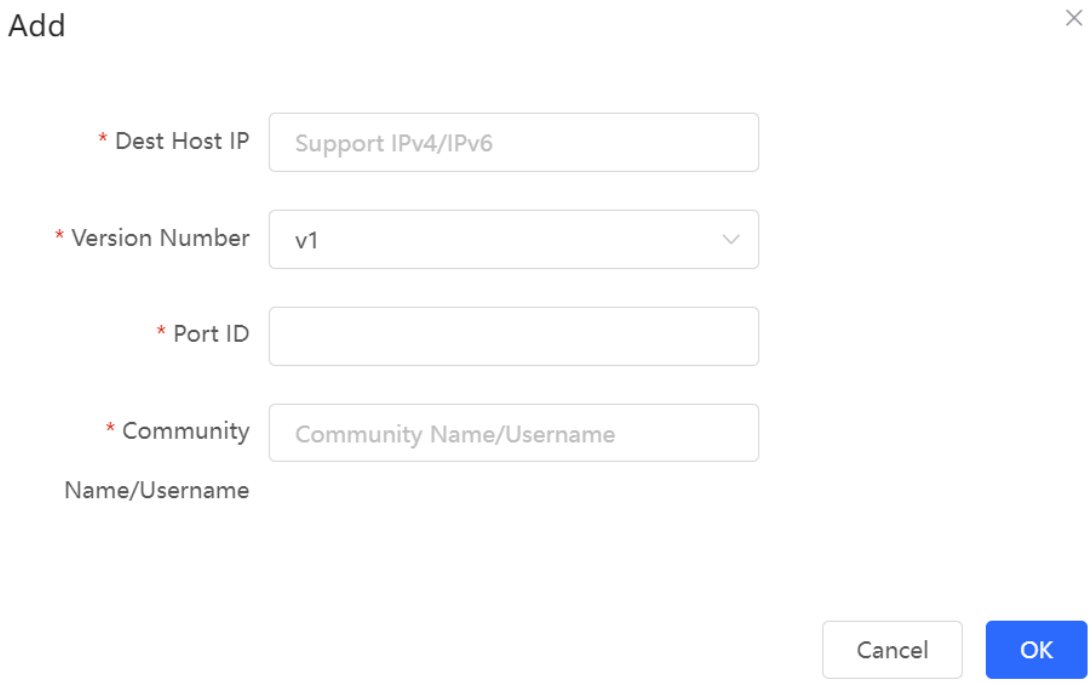


Table 7-8 Trap v1/v2c User Configuration Parameters

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

Note

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

(3) Click **OK**.

3. Configuring Trap v3 Users

- Overview

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

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

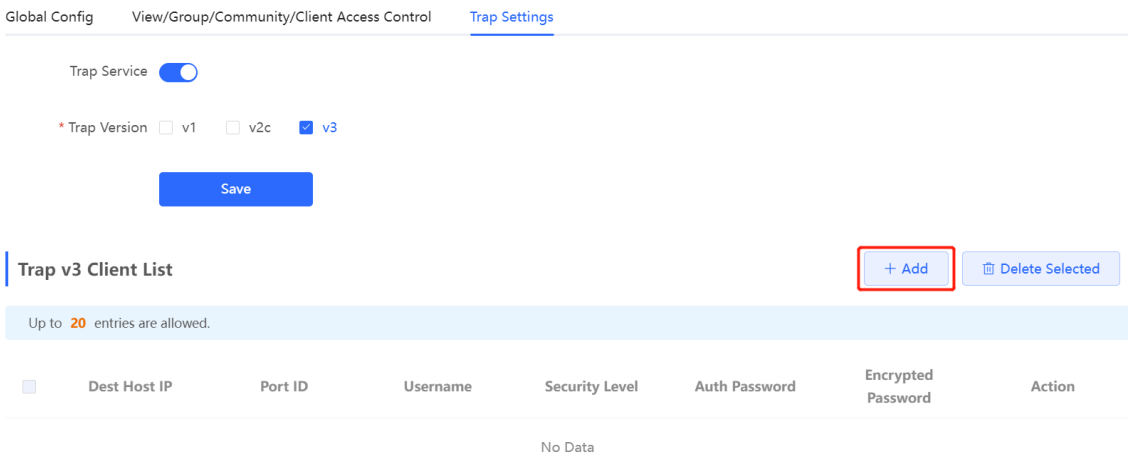
- Prerequisites

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

- Configuration Steps

System > SNMP > Trap Setting

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



(2) Configure trap v3 user parameters.

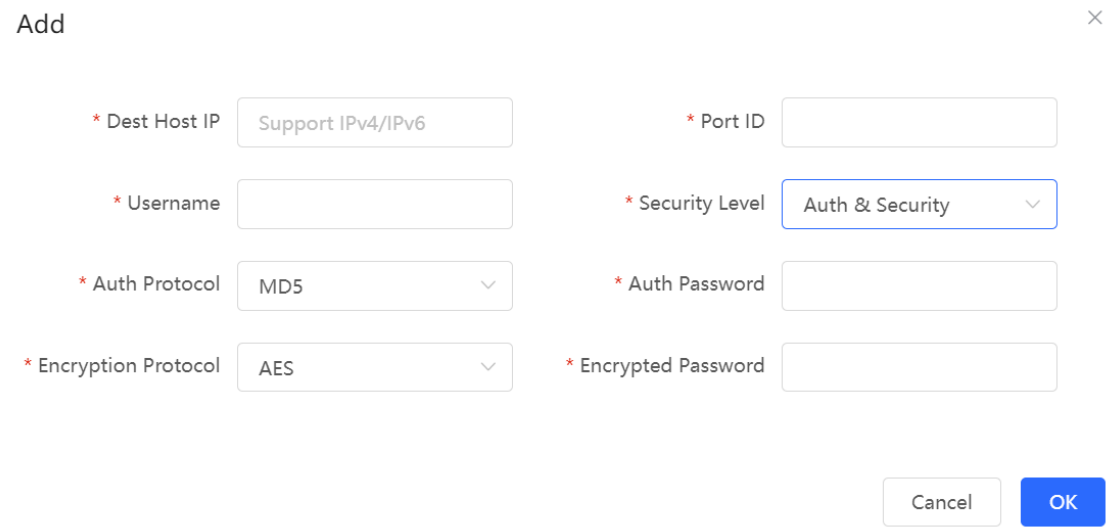


Table 7-9 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.
Username	Name of the trap v3 user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Security Level	Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

Note

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

7.9.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

- Application Scenarios

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

- Configuration Specification

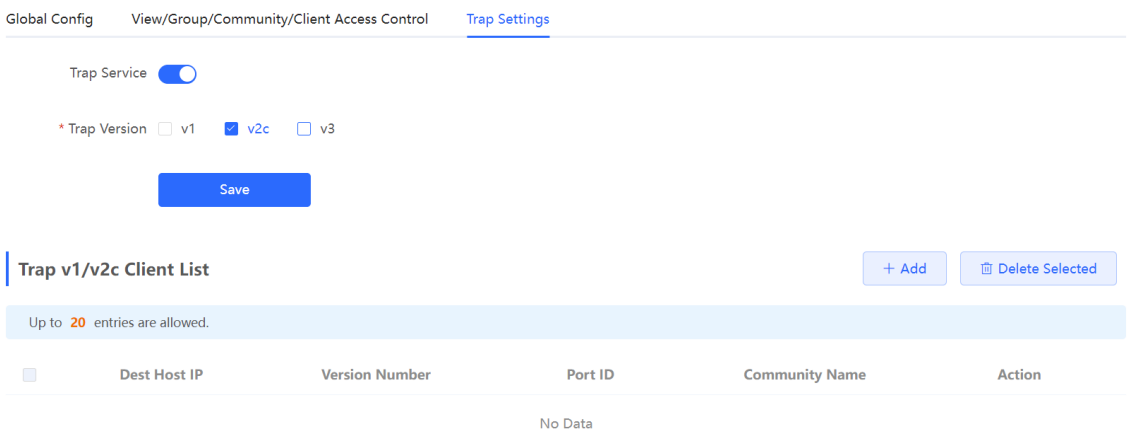
According to the user's application scenario, the requirements are shown in the following table:

Table 7-10 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port number is 166.
Version	Select the v2 version.
Community name/User name	Trap_user

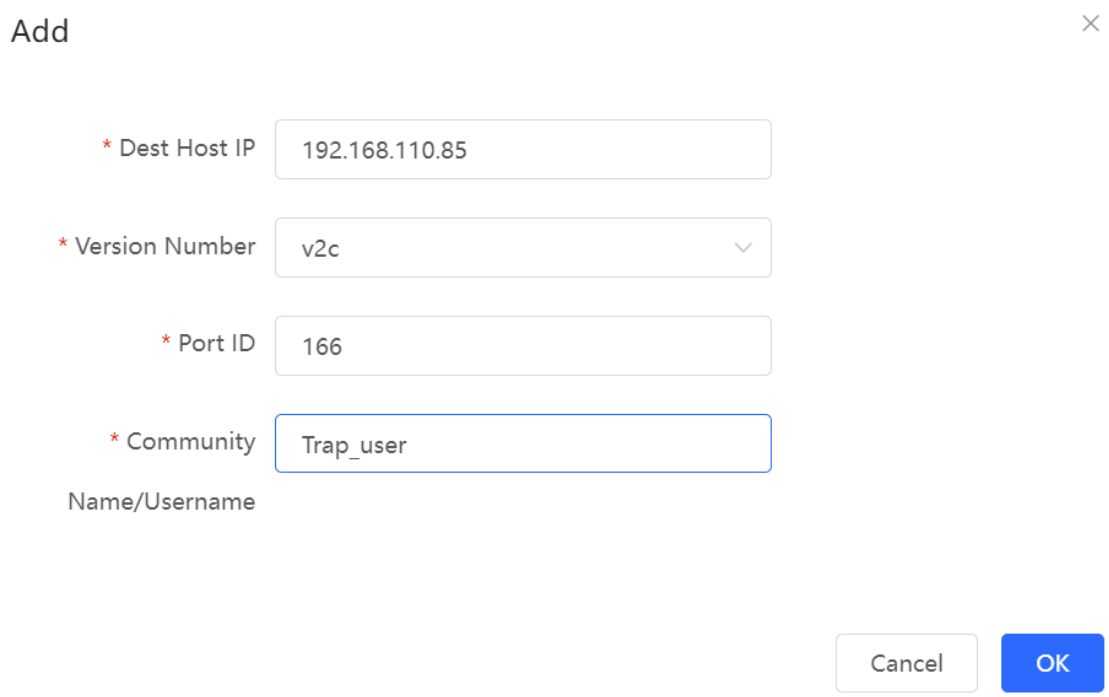
- Configuration Steps

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



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

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



2. Configuring Trap v3

- Application Scenarios

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

- Configuration Specification

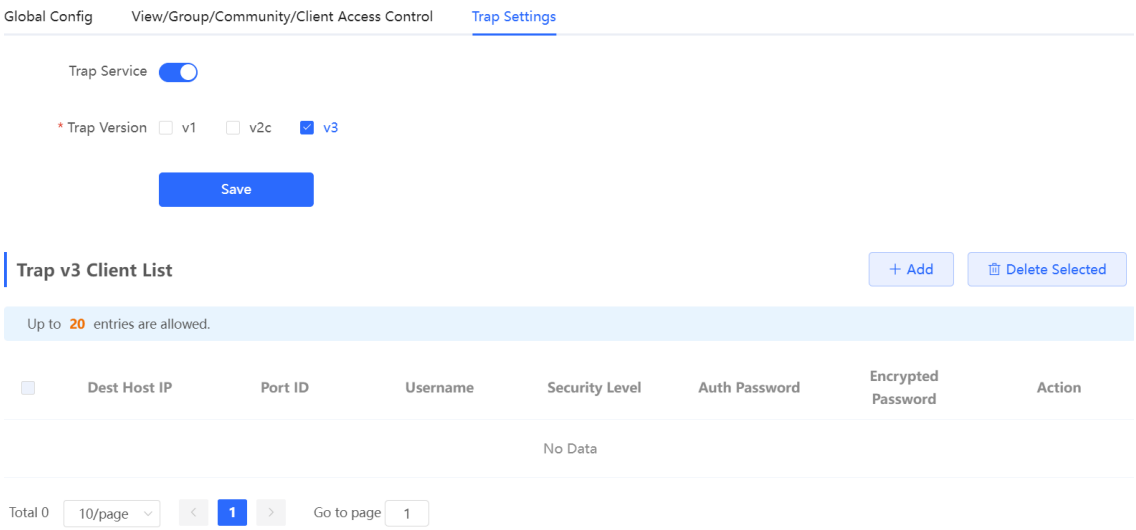
According to the user's application scenario, the requirements are shown in the following table:

Table 7-11 User Requirement Specification

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

- Configuration Steps

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



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

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