Lysora LB Series Wireless Bridge

Lysora 2.400 Configuration Guide

Document version: V1.0
Date: 2025.9.26

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Availability may vary by jurisdiction or contract, 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 as expressly provided in a written agreement between you and Lysora Technology Inc.**, **all representations and warranties**, **regarding the content of this document**, **to the maximum extent permitted by applicable law — including implied warranties of merchantability**, **fitness for a particular purpose**, **and non-infringement—are hereby disclaimed**.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for informational purposes only. **Lysora Technology Inc. does not endorse**, **recommend, guarantee**, **or assume liability for such third-party software's functionality**, **security**, **legality**, **accuracy**, **or fitness**. You are solely responsible for: (a) evaluating and selecting any third-party software based on your specific business requirements; (b) ensuring you have obtained all necessary licenses and authorizations for its use; and (c) assuming all risks associated with its use. **Lysora Technology Inc. shall have no liability for any claims or damages arising from your use of or reliance upon any third-party software**.

Lysora Technology Inc. reserves the right, at its sole discretion and without prior notice, to modify the content of this document at any time. These modifications may occur due to product updates, corrections, regulatory changes, or other reasons. **Lysora Technology Inc. undertakes no obligation to update or notify users of changes to this document**.

This document is provided “AS IS” and for general informational and guidance purposes only. While Lysora Technology Inc. strives to ensure the accuracy and reliability of the content at the time of publication, **it makes no warranty**, **express or implied**, **that the content is error-free**, **complete**, **or current**. All information contained herein is provided without any warranty of merchantability, fitness for a particular purpose, or non-infringement. **You assume all risk for the use or application of this information**. For regulatory compliance queries (e.g., FCC/CPSC standards), please contact our support channel.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Official website: https://help.lysoratech.com/
- Technical support email: support@lysoratech.com

Conventions

1. UI Conventions

UI Convention	Description	Example
Boldface	The interactive UI elements are in **boldface**, including buttons, tabs, menus, and so on.	Click **OK**. Select Config Wizard. Click the **Clients** tab.
>	The ">" symbol indicates a hierarchical relationship or a path to a specific item.	Select **System** > **Time**.

2. Symbols

The symbols that may be found in this document are described as follows:

Warning

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

⚠ Caution

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

ℹ Note

An alert that contains additional or supplementary information.

✓ Specification

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

3. Notes

This document provides configuration details (including model, description, port type, and software interface) of the expected version for reference purposes only. In the event of any discrepancy or inconsistency between the expected version and the actual version, the actual version shall take precedence.

Contents

.

1 Change Description

This chapter describes the major changes in software and hardware of different versions and related documentation. For details about hardware changes, see the release notes published with software versions.

1.1 Lysora 2.400

1.1.1 Hardware Change

The following table lists the applicable hardware models of this version.

Model	Hardware Version
CPE3-P	1.xx
CPE5	1.xx

1.1.2 Software Feature Change

This is the baseline version, with no changes to software features.

2 Login

2.1 Configuration Environment Requirements

- Browser: 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.
- Resolution: 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

2.2 Default Configuration

Table 2-1 Default Web Configuration

Item	Default Value
IP address	10.100.111.254
Password	You can enter the initial password "admin" to log in, and directly start the configuration after login.

2.3 Logging In to Web Management Interface on a PC

2.3.1 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 2.3.2 Configuring the IP Address of the Management PC.

- **Wireless Connection**

On a mobile phone or laptop, search for wireless network ***Lysora-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 2.3.2Configuring the IP Address of the Management PC.

2.3.2 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 10.100.111.254, 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 10.100.111.10.

⚠ Caution

The IP address of the management PC cannot be set to 10.100.111.253, because this IP address is reserved by the device. If the management PC uses this IP address, it cannot access the device.

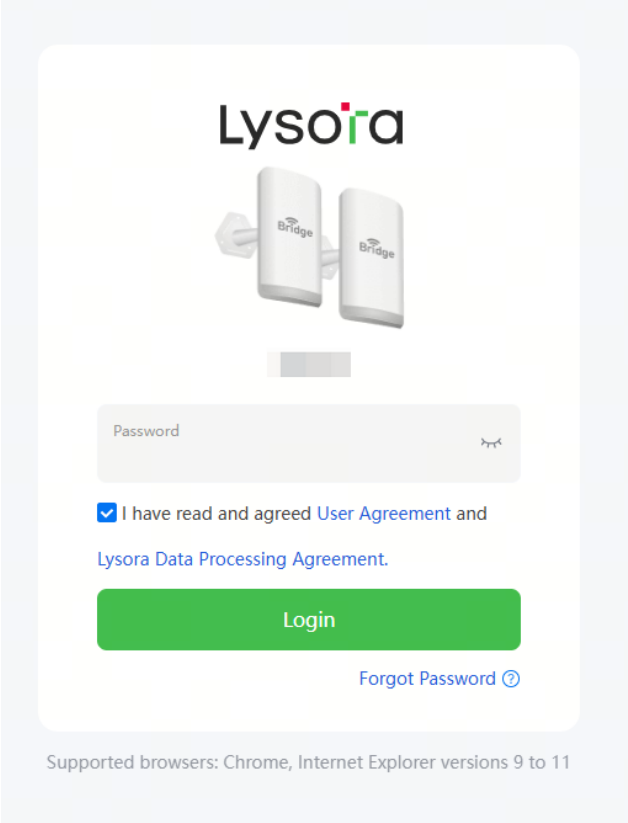
2.3.3 Logging in to the Web Management Interface

(1) Enter the IP address (10.100.111.254 by default) of the bridge in the address bar of the browser to open the login page.

Note

- By logging in to the IP address 10.100.111.253, you will be redirected to the home page of the primary device on the self-organizing network.
- 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 interface 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 interface.



⚠ Caution

- The default password for the device upon first login is admin. To ensure device security, you need to reset the device password after the first login. For details, see 2.4.2Configuring Project Settings
- 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.
- 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.

2.4 Initial Setup

✅ Specification

The initial setup page will be displayed only when the device is first configured or restored to factory settings.

2.4.1 Configuration Steps

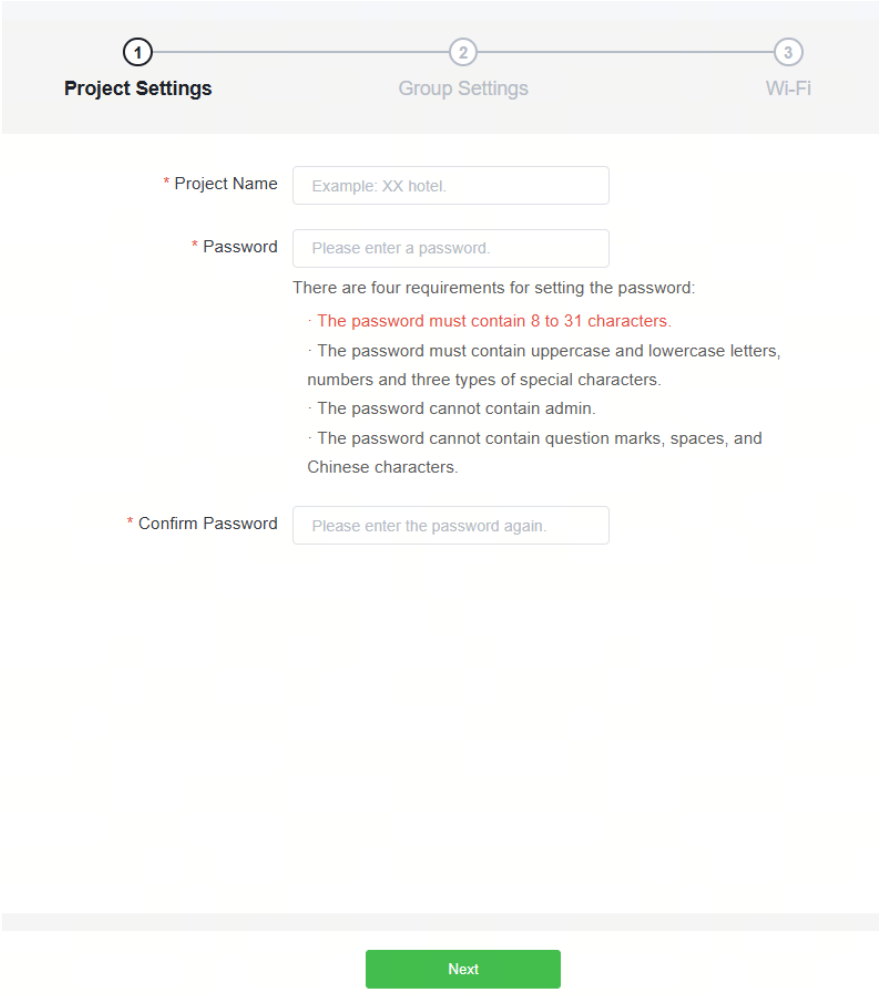
(1) Configure project settings. For details, see 2.4.2Configuring Project Settings.

(2) Configure the WDS group settings. Based on your usage scenario, choose whether to create a new WDS group or to add devices to an existing one. For creating a new WDS group, see 2.4.31Creating a New WDS Group. For adding devices to an existing WDS group, see 2.4.32Adding Devices to an Existing WDS Group.

(3) Wi-Fi Settings: Configure the bridges' management Wi-Fi network for connecting to and managing the bridges. For details, see 2.4.4Wi-Fi Settings.

2.4.2 Configuring Project Settings

Enter the project name and password. Click **Next**.



Note

- The password is used to log in to web management interface of the devices. Please remember it. If you forget the password, press and hold the Reset button on a device for more than 5s to restore factory settings.
- After configuration, all bridges in the bridge group use the same management password.

2.4.3 Configuring WDS Group Settings

Caution

If devices are delivered in pairs, retain the default configuration in **Group Settings**. Otherwise, modifying the bridge mode, bridge SSID, or WDS password may cause bridge pairing failure.

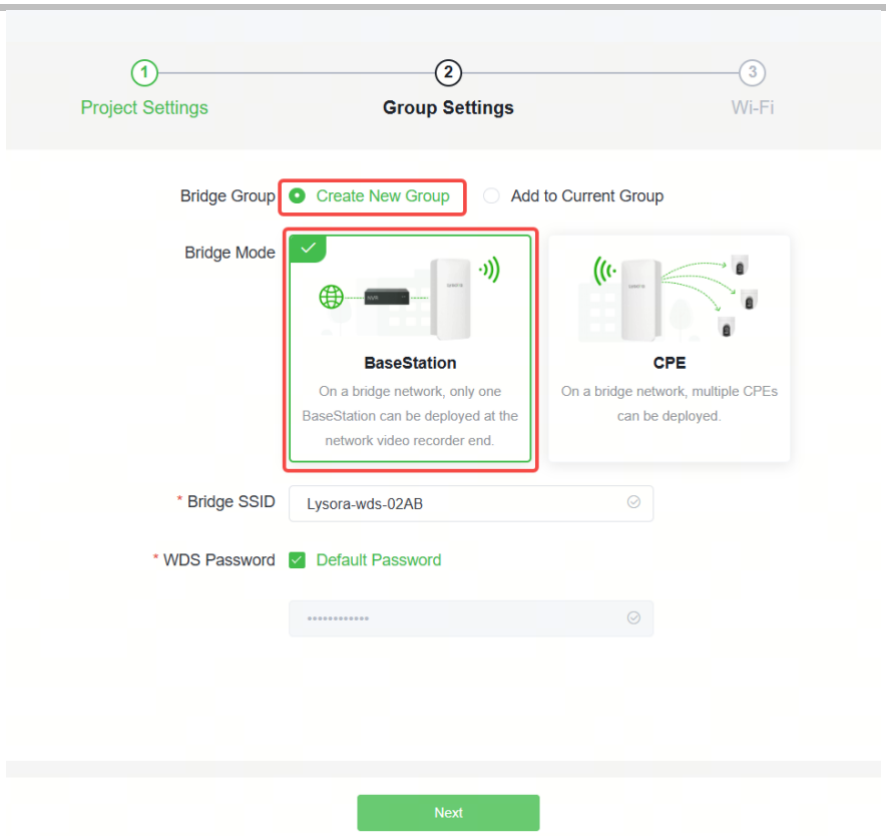
1. Creating a New WDS Group

- **Configuration in BaseStation Mode**

(1) Set **Bridge Group** to **Create New Group**.

(2) Set **Bridge Mode** to **BaseStation**.

(3) Enter the WDS SSID and WDS password, and click **Next**.

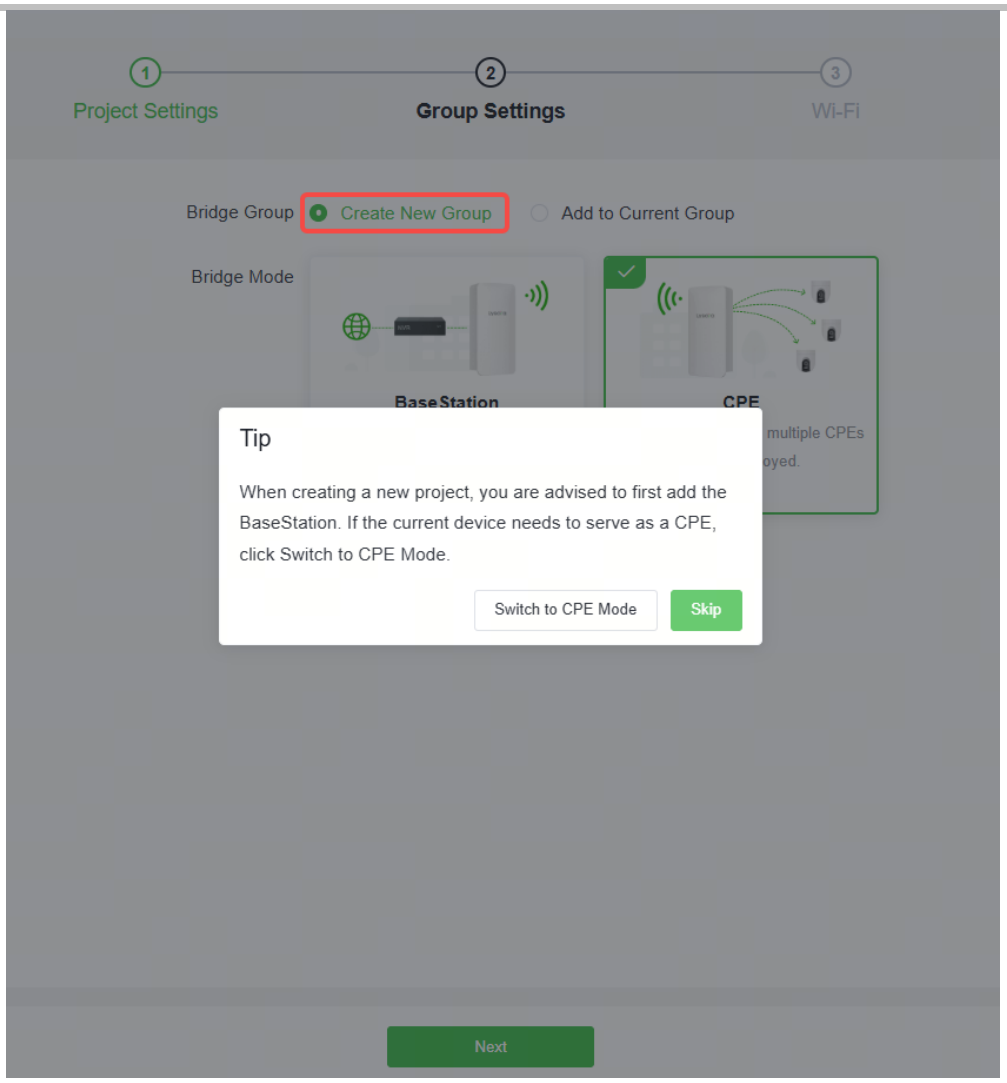


- **Configuration in CPE Mode**

(1) Set Bridge Group to Create New Group.

(2) Set **Bridge Mode** to **CPE**. A pop-up window is displayed. Click **Switch to CPE Mode**.

(3) Click **Next**.



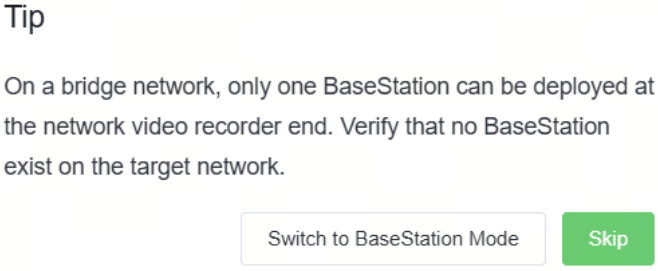
2. Adding Devices to an Existing WDS Group

(1) Set Bridge Group to Add to Current Group.

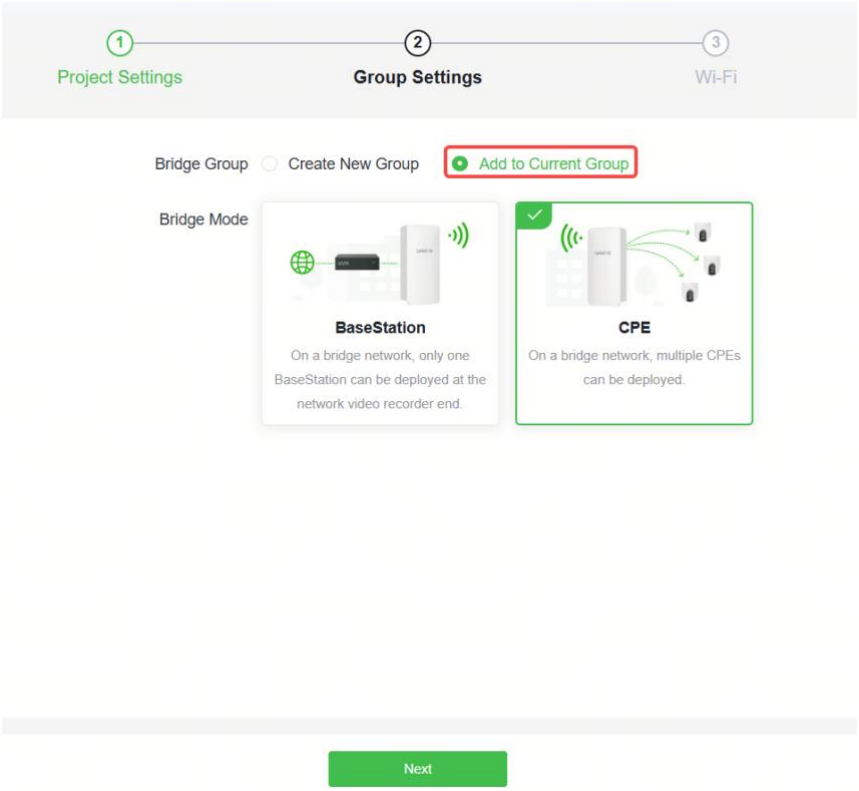
(2) Select the bridge mode.

Note

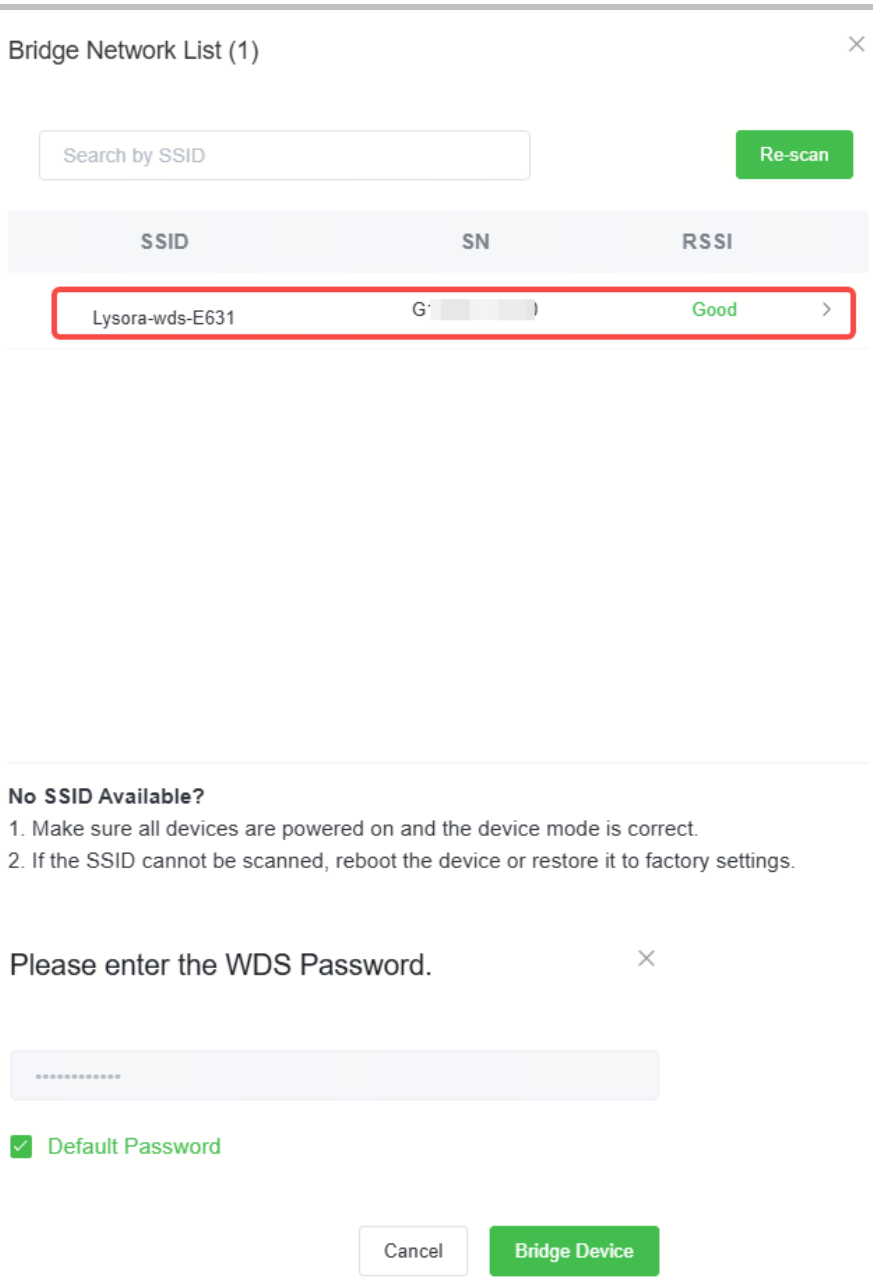
When you set **Bridge Group** to **Add to Current Group**, **Bridge Mode** is set to **CPE** by default. To set the bridge mode to **BaseStation**, check the reminder and click **Switch to BaseStation Mode** in the pop-up dialog box.



(3) Click **Next**.

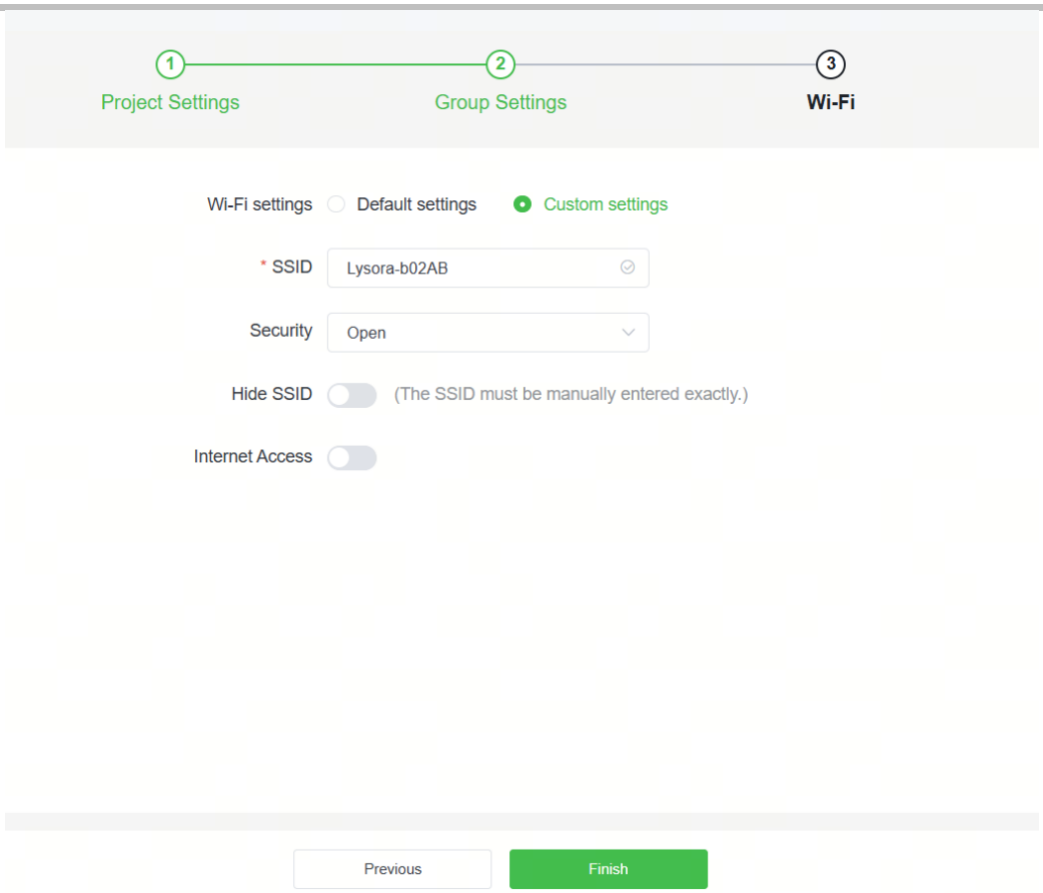


(4) The device automatically detects available WDS groups. Select the WDS SSID from the **Bridge Network List**, enter the WDS password, and click **Bridge Device**.



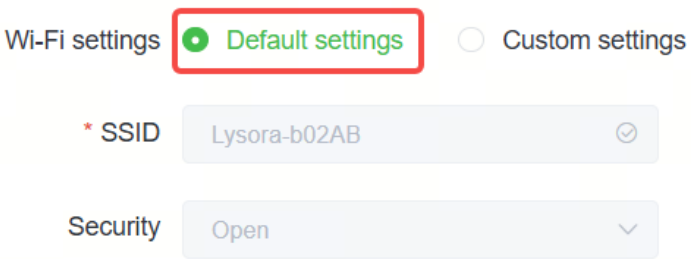
2.4.4 Wi-Fi Settings

Configure the Wi-Fi network of the bridges. After connecting a PC or mobile phone to the Wi-Fi network, enter the IP address (10.100.111.254 by default) of the bridges in the browser to log in to the bridges' web management interface for configuration and management.



(1) Set **Wi-Fi settings** to **Default settings** or **Custom settings**.

- **Default settings**: The SSID is ***Lysora-bxxxx*** (*xxxx* is the last four digits of the device's MAC address), and the Wi-Fi network is not encrypted by default.

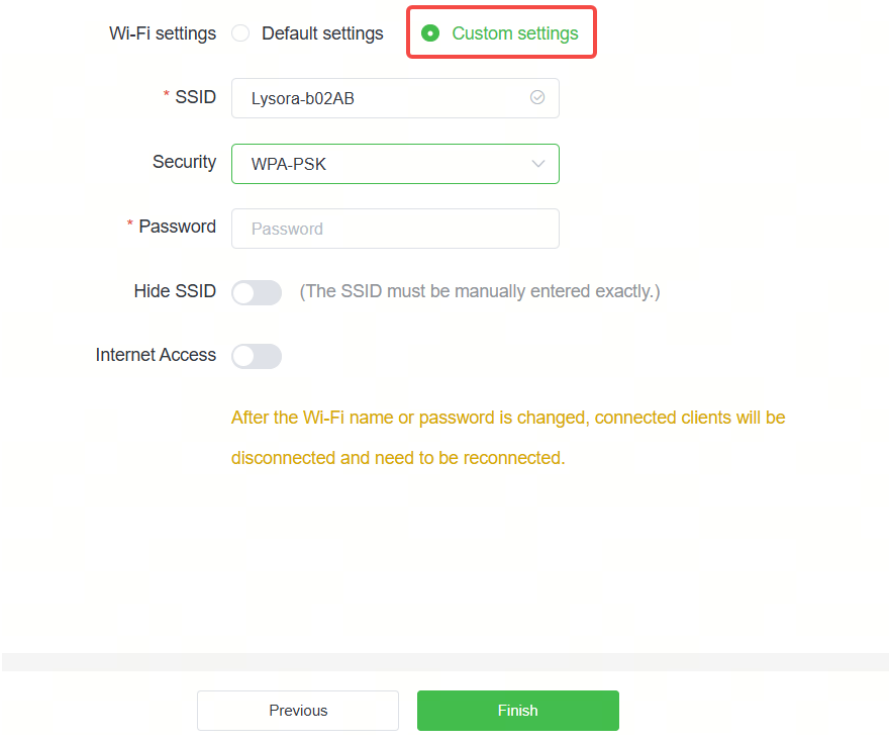


- **Custom settings**: Enter the Wi-Fi name, select the Wi-Fi encryption type, and set the Wi-Fi password. You can hide the Wi-Fi network as required.

Note

- After the Wi-Fi name or password is changed, the Wi-Fi network is reset. Clients need to reconnect to the Wi-Fi network to access the web management interface.

- When the **Hide SSID** feature is enabled, mobile phones or computers cannot detect the Wi-Fi name, and users need to manually enter the correct name and password. This can prevent unauthorized access and enhance network security.

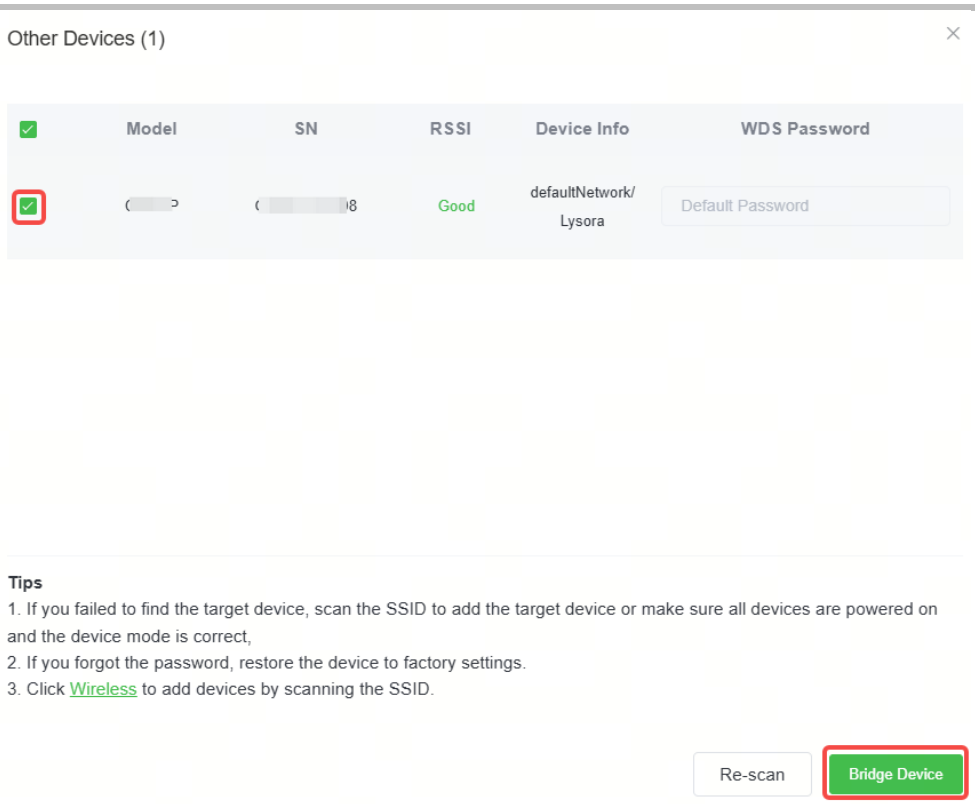


(2) Click **Finish**.

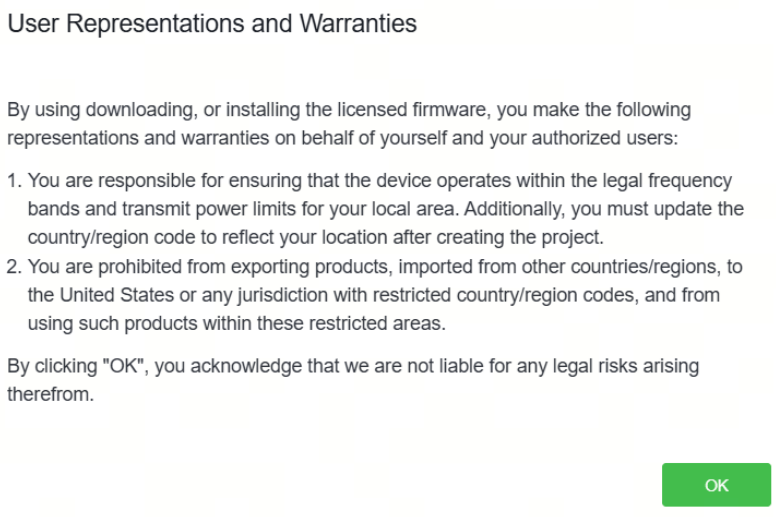
2.4.5 Completing the Configuration

After the project setup is complete, you will be automatically redirected to the web management interface of the device.

To prevent accidental modification of bridge group settings for already paired bridges during the initial setup in 2.4.3Configuring WDS Group Settings, the system will automatically discover nearby bridges available for pairing when you access the web management interface. You can directly select the devices to be bridged and click **Bridge Device** to add the selected devices to the bridge group.



Upon first login, the **User Representations and Warranties** pop-up window is displayed. Please read it carefully and click **OK**.



2.5 Introduction to the Web Management Interface

2.5.1 Frequently-Used Controls on the Web Management Interface

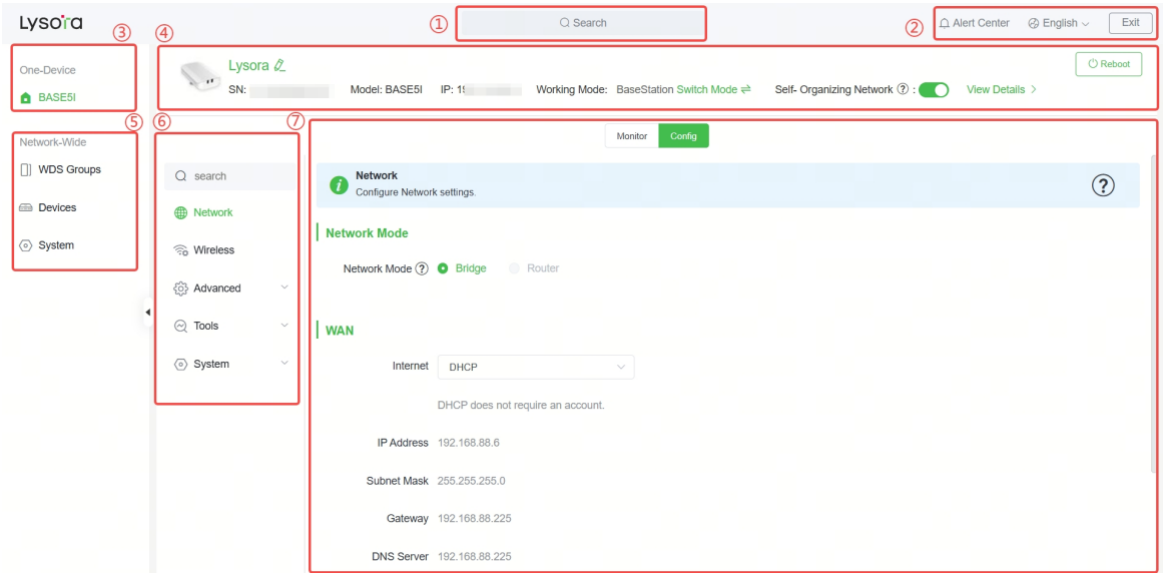
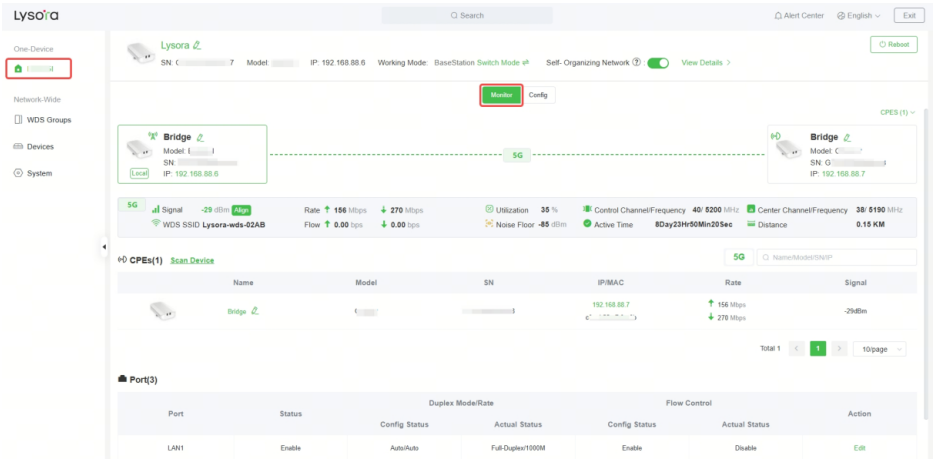
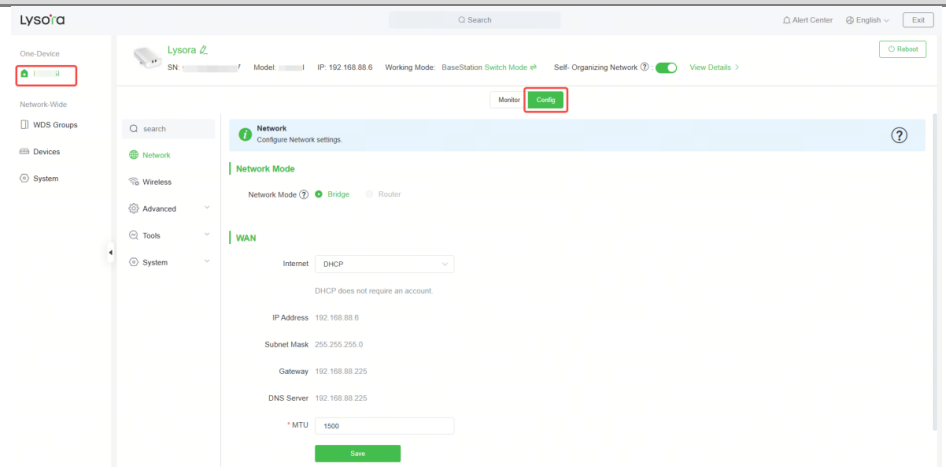


Table 2-2 Frequently-Used Controls on the Web Management Interface

No.	Description
1	Navigate to common functions of the device, including network-wide management, device, and system functions.
2	Switch the language of the web management interface and exit the web management interface.
3	Click the device under the **One-Device** menu to access the device monitoring or configuration page. ● When Self-Organizing Network is enabled: The **One-Device** menu displays the current login device and the primary device on the self-organizing network. If the current login device is the primary device on the self-organizing network, it is indicated by the icon. o The icon indicates the primary device on the self-organizing network. o The icon indicates the current login device. ● When Self-Organizing Network is disabled: The **One-Device** menu

No.	Description
	displays the current login device, indicated by the icon.
4	Current device information, work mode, Self-Organizing Network status, and the reboot button.
5	The navigation bar for network-wide management, which includes common functions applicable to all devices on the self-organizing network.
6	● Configuration options under the **Network** menu: The network configuration navigation bar is displayed for unified management and configuration of all devices on the network. ● Select **One-Device** and click **Configure**: The device configuration navigation bar is displayed for configuring common features of the standalone device. Note: When you select **One-Device** and click **Monitor**, the navigation bar will not be displayed in this pane.
7	Device monitoring and configuration pane: ● In Pane 3, select a device and click **Monitor**: This will display the WDS group information and port status of the device.  ● In Pane 3, select a device and click **Configure**: You can click the configuration options in Pane 6 to configure the corresponding features for the device.

No.	Description
	

2.5.2 Network-wide Management Interface

Click a configuration item under the **Network-Wide** menu on the left navigation bar to manage and configure devices on the self-organizing network. The configuration functions and displayed content on the network-wide management interface vary depending on whether the primary device on the self-organizing network is a Lysora LB series bridge.

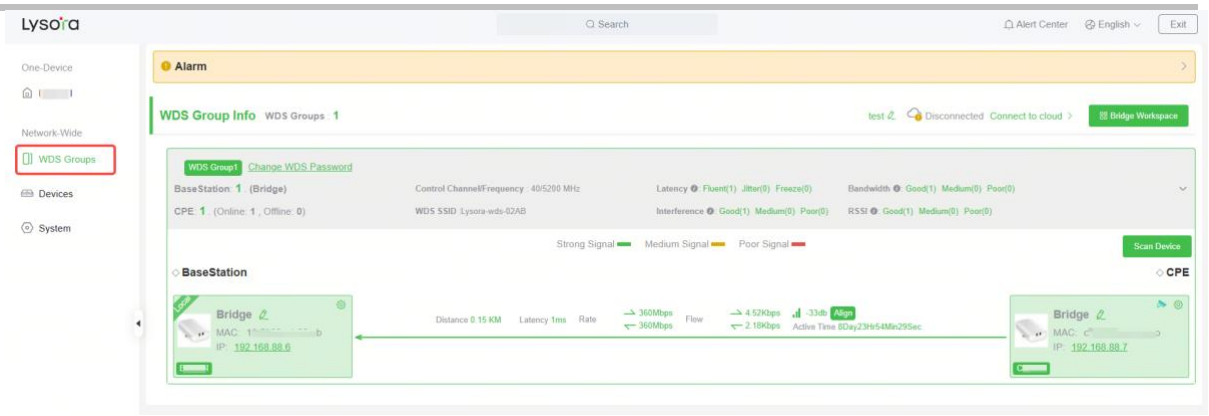
1. The Primary Device on the Self-Organizing Network Is a Bridge

When the primary device in the self-organizing network is a Lysora LB series bridge, the **Network** menu includes only the **WDS Group**, **Devices**, and **System** options.

- **Managing Bridge Groups**

Choose **Network-Wide** > **WDS Groups**.

The interface displays information about the WDS groups on the network, including project details, alarms, and bridging link status. Click **Bridge Workspace** to configure common functions for the WDS group.



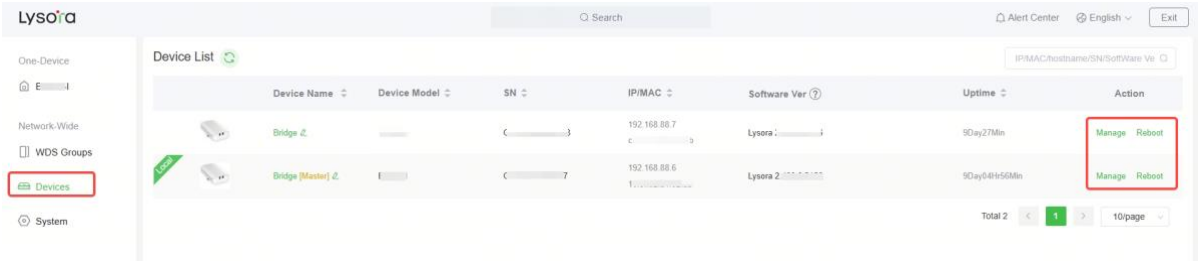
- **Managing Network-wide Devices**

Choose **Network-Wide** > **Devices**.

The **Device List** displays all devices on the self-organizing network. Click **Manage** or **Reboot** in the **Action** column to configure functions for the device or restart the device.

Note

Configuration and reboot operations are only supported on devices that have Self-Organizing Network enabled. For details, see 2.6Self-Organizing Network.



- **Network-wide system settings**

Choose **Network-Wide** > **System**.

Click **System** under the **Network-Wide** menu. Select a tab from the navigation bar on the right to configure and manage devices on the network.

(1) **Time**: For details, see 8.6Configuring System Time.

(2) **SNMP**: For details, see 8.9Configuring SNMP.

(3) **Compatibility Mode**: For details, see 8.10Configuring Compatibility Mode.

(4) **Password**: For details, see 8.1Configuring Management Password.

2. The Primary Device on the Self-Organizing Network Is Not a Bridge

When the primary device on the self-organizing network is not a Lysora LB series bridge, the **Network-Wide** menu includes **Workspace, Devices**, **Clients** and **System**. In addition, the physical topology of the whole network is displayed on the web management interface.

- **Network-wide workspace**

Choose **Network-Wide** > **Workspace**.

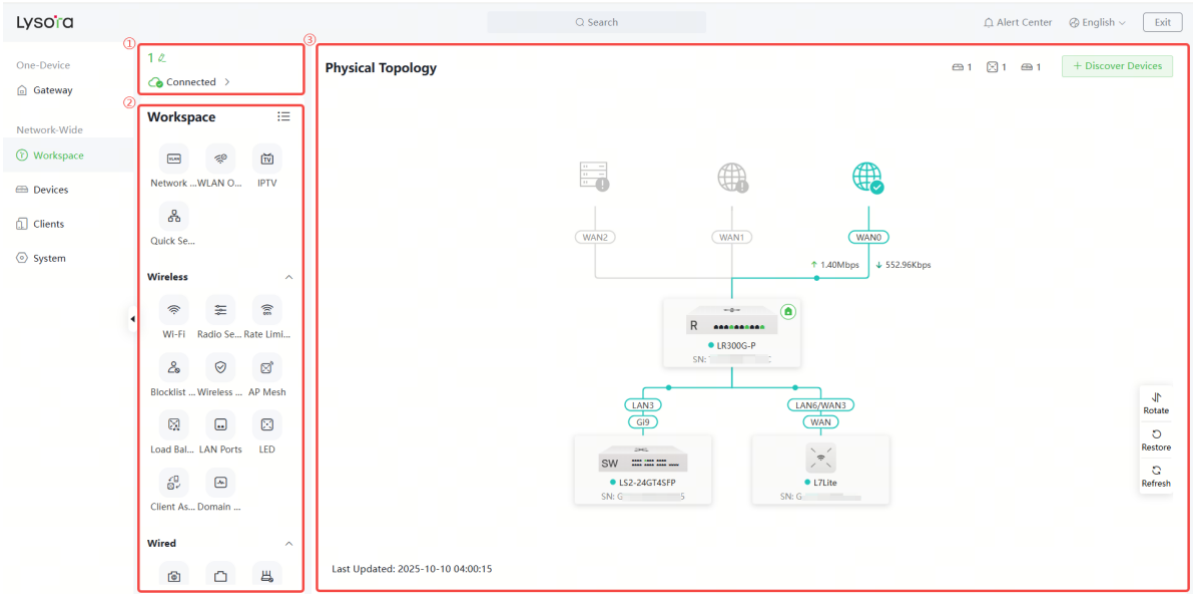


Table 2-3 Description of the Workspace

No.	Description
1	Displays the project name and whether the project is managed in Lysora Cloud.

No.	Description
2	Displays the network-wide configuration items, including network-wide service network planning, wireless functions, wired functions, and network-wide system functions.
3	Displays the physical topology of the network. Click any device in the topology to access the device configuration interface. Click **+ Discover Devices** on the top right corner to add devices.

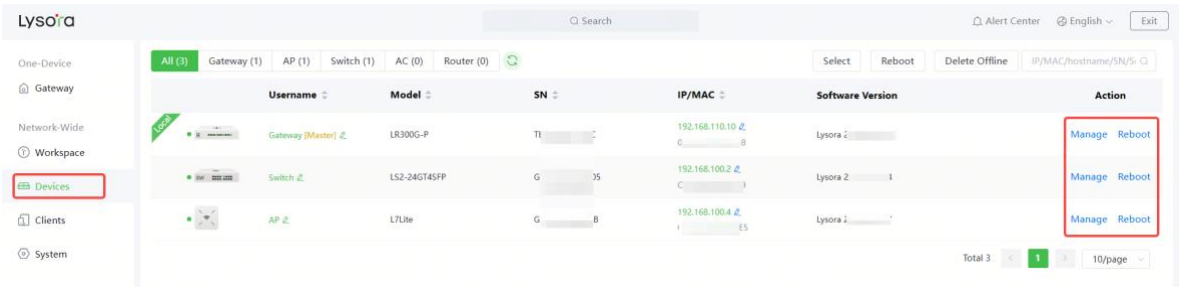
- **Network-wide device management**

Choose **Network-Wide** > **Devices**.

The device list displays all devices on the self-organizing network. Click **Manage** or **Reboot** to configure or reboot the selected device.

Specification

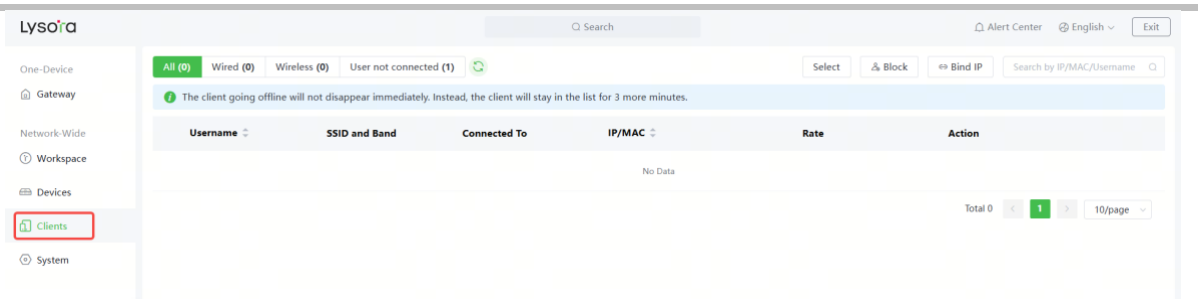
- When the primary device on the self-organizing network is not a bridge, restarting a bridge is not supported on the **Devices** page. You need to go to the device configuration page to perform the operation. For details, see 8.5Rebooting the Device.
- When the primary device on the self-organizing network is a bridge, the Device page only displays bridges on the network.



- **Network-wide client management**

Choose **Network-Wide** > **Clients**.

You can view wired clients, wireless clients, and clients not connected on the network. The list displays the client name, connection mode, associated device, IP/MAC addresses, IP binding status, rate, and related operations.



(1) Click **Not Bound** in the **IP/MAC** column to bind the client to a static IP address.

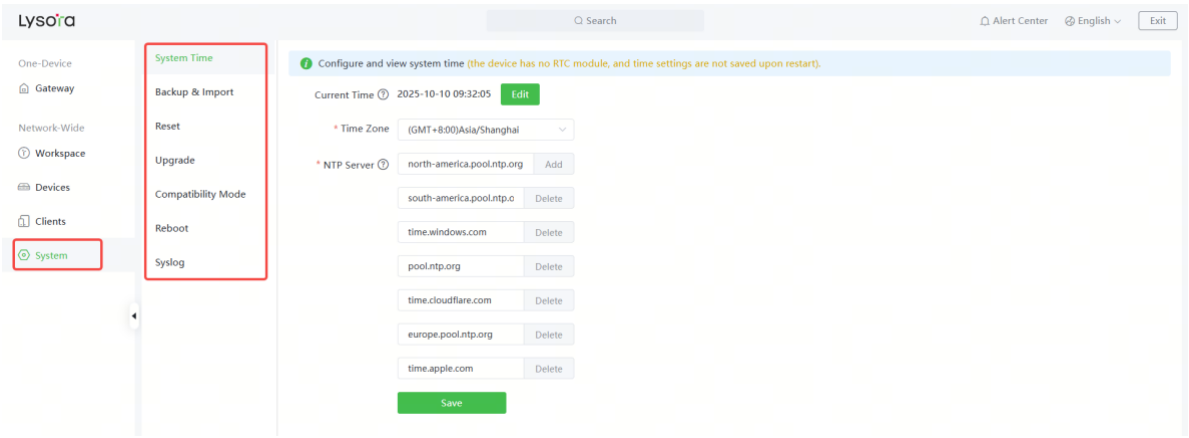
(2) Click a button in the **Action** column to perform the corresponding operations on the client:

- Wired clients: Only access control can be configured.
- Wireless clients: Access control, client association, and blacklisting can be configured.

- **Network-wide system settings**

Choose **Network-Wide** > **System**.

Click **System** under the **Network-Wide** menu and select a tab from the navigation bar on the right to configure and manage devices on the network. The specific functions and function support are subject to the primary device. For details, see the configuration guide of the primary device.



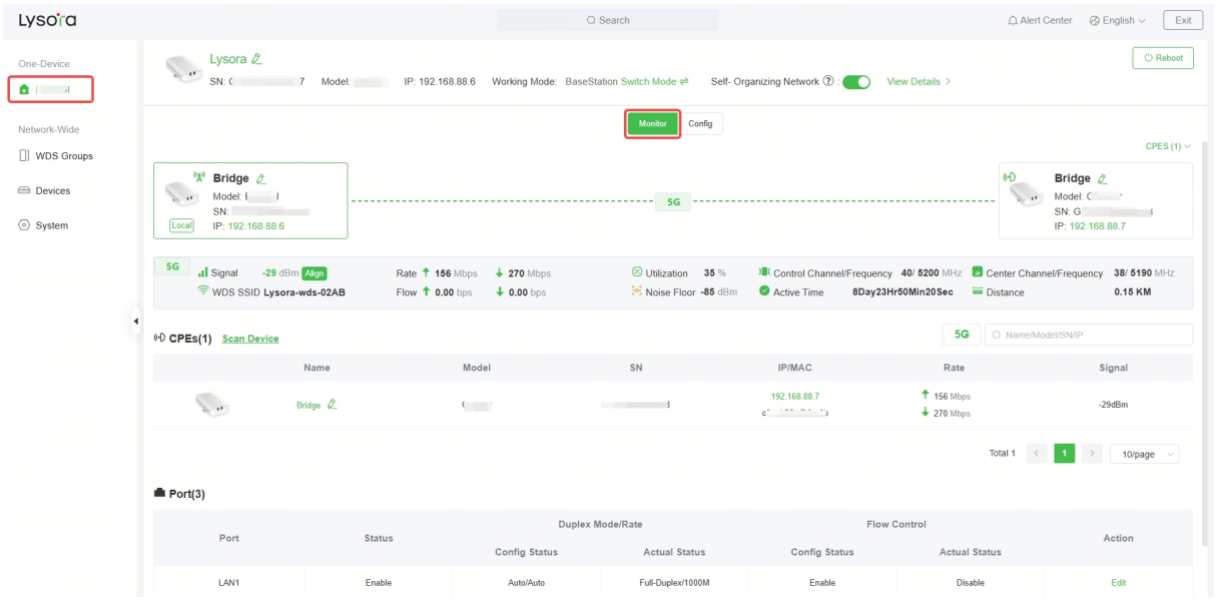
2.5.3 One-Device Monitor/Configuration Page

Go to the configuration page:

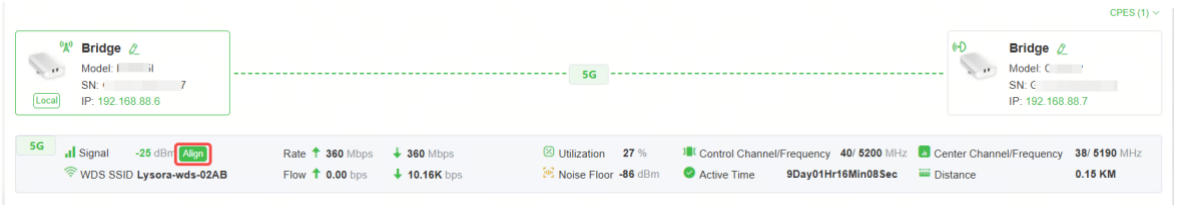
- Method 1: Click the device under the **One-Device** menu on the left. After selecting **One-Device**, you can monitor and configure the device.
- Method 2: Choose **Network-Wide** > **Devices** on the left, and click **Manage** to manage the device.

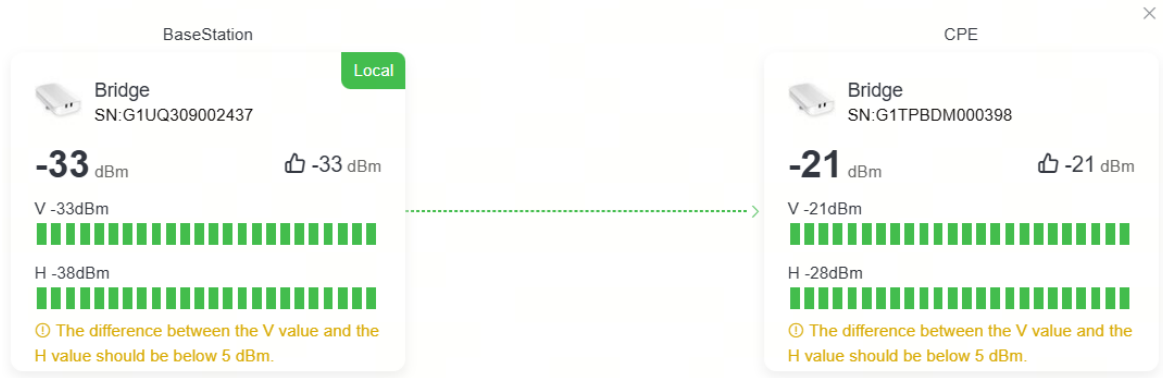
1. One-Device Monitor Page

Click **Monitor**. The page displays relevant information about the device, including the peer device in the WDS group, bridging link status, CPE details, and port status. On the **Monitor** page, you can perform antenna alignment, scan for CPE, and modify the port status.

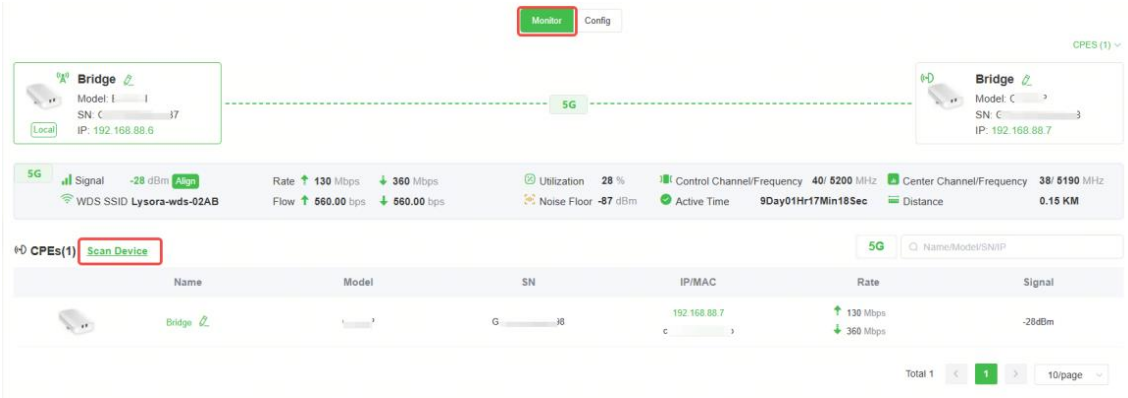


- Antenna alignment: Click **Align** to view the real-time RSSI in the pop-up window. For details, see 5.1Antenna Alignment.

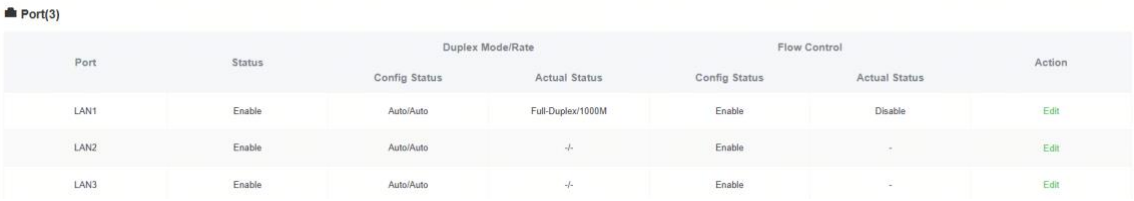




- Scan for CPE: Click **Scan Device** to discover other bridges. For details, see 3.3Scanning to Pair and Add Devices.

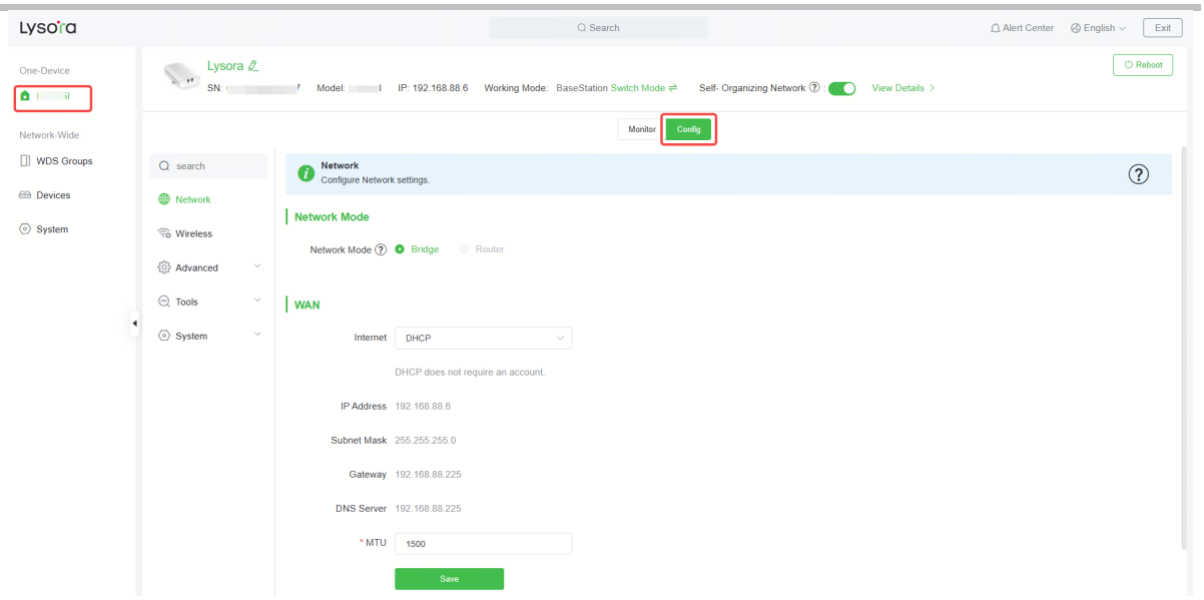


- Modify port settings: In the **Port** pane, click **Edit** to modify the port settings. For details, see 4.5Port Settings.



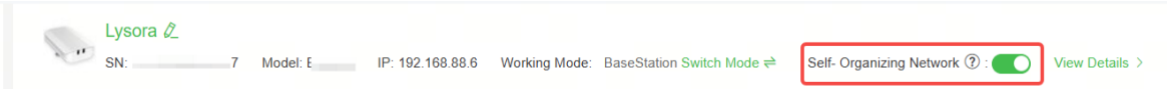
2. One-Device Configuration Page

Configuration page: Click **Config** to manage and configure the selected device.



2.6 Self-Organizing Network

The **Self-Organizing Network** function is enabled by default.



Standalone mode: When the **Self-Organizing Network** function is disabled, the device will not be discovered on the network, and will operate in standalone mode. After logging into the web management interface, you can only configure and manage the current login device. If you only need to configure one device or do not wish to apply global configurations to the device, you can disable the **Self-Organizing Network** function.

Self-Organizing Network mode: When the **Self-Organizing Network** function is enabled, the device can be discovered on the network, and can discover other devices on the network. These devices connect with each other based on their status to form a network, and synchronize global configurations. You can log in to any device on the network to configure and manage all devices on the network. Enabling this function enhances network management efficiency. You are advised to keep this function enabled.

When the device works in Self-Organizing Network mode, the web management interface provides two configuration modes: Network-Wide mode and One-Device mode. For details, see 2.5.2Network-wide Management Interface and 2.5.3One-Device Monitor/Configuration Page.

2.7 Adding Devices to the Self-Organizing Network

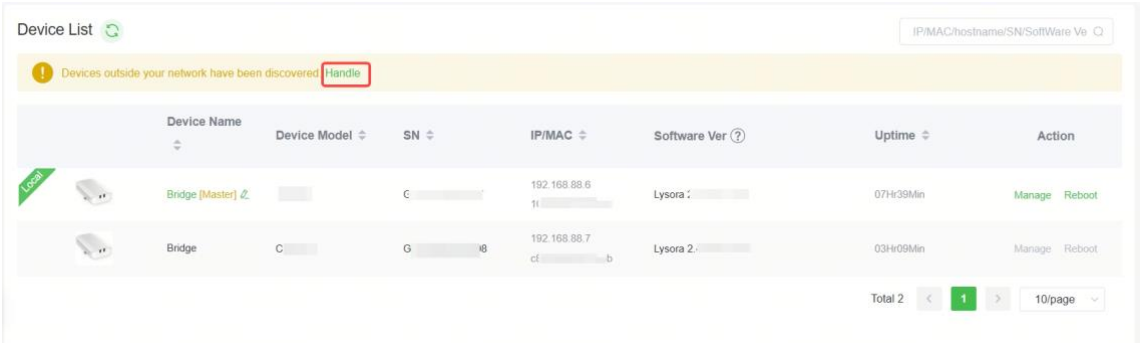
Specification

When the **Self-Organizing Network** function is enabled, the ability to discover and add devices is subject to the primary device. If the primary device is a Lysora LB series bridge, only other bridges on the network can be discovered and added. If the primary device is not a Lysora LB series bridge, all types of Lysora devices can be discovered and added.

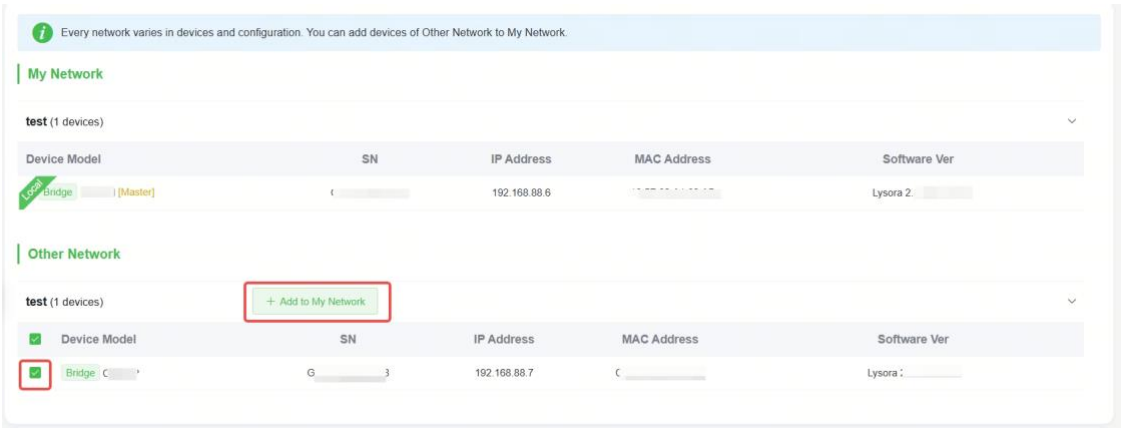
2.7.1 The Primary Device on the Self-Organizing Network Is a Bridge

Choose **Network-Wide** > **Devices**.

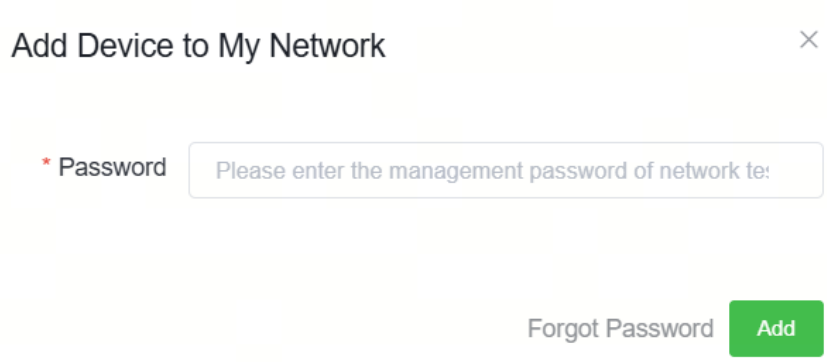
(1) A prompt is displayed under **Device List**. Click **Handle** to add the unconnected devices or other networks to the current network.



(2) After you are redirected to the network list page, expand **Other Network** to select the target devices and click **Add to My Network**.



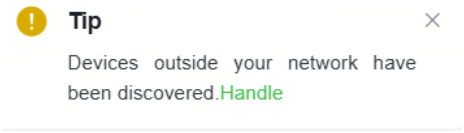
(3) You do not need to enter a password if the device hasn't been configured previously. If the device already has a password, you must enter the device's management password. Adding the device will fail if the password entered is incorrect.



2.7.2 The Primary Device on the Self-Organizing Network Is Not a Bridge

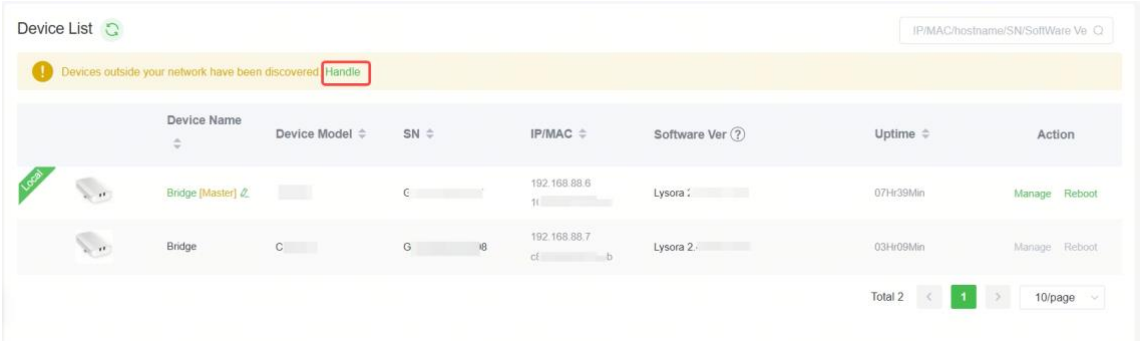
(1) Add devices to a network:

- Method 1: When a new device joins the network via a wired connection, the system prompts that there are other devices not yet connected. Click **Handle** to add the unconnected devices or other networks to the current network.

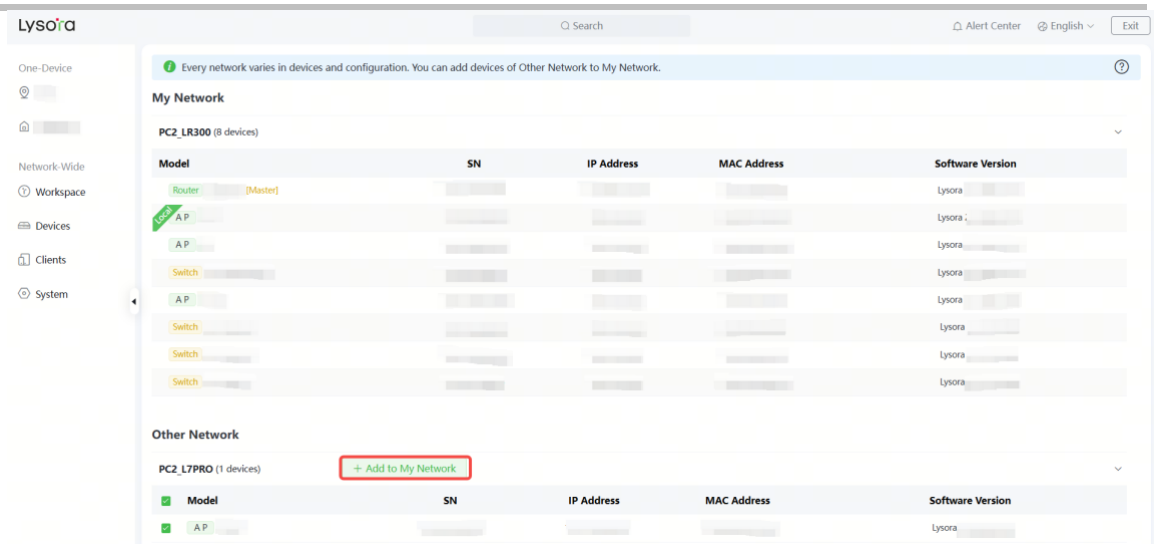


- Method 2: Choose **Network-Wide** > **Workspace** > **Physical Topology**, and click **+ Discover Devices**.

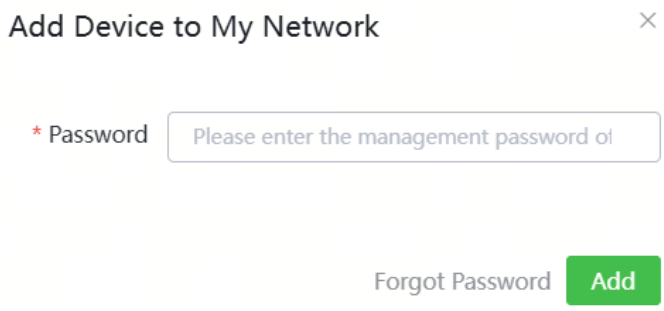
- Method 3: Choose **Network-Wide** > **Devices**. A prompt is displayed under **Device List**. Click **Handle** to add unconnected devices or other networks to the current network.



(2) After you are redirected to the network list page, expand **Other Network** to select the devices to be added and click **Add to My Network**.



(3) You do not need to enter a password if the device hasn't been configured previously. If the device already has a password, you must enter the device's management password. Adding the device will fail if the password entered is incorrect.



3 Wi-Fi Network Settings

3.1 Overview

3.1.1 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 3.3Scanning 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.

3.1.2 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.

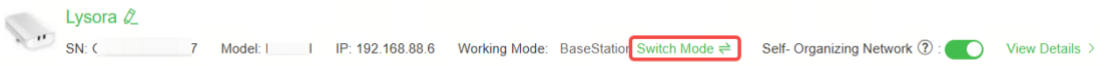
3.2 Switching Between BaseStation Mode and CPE Mode

⚠ Caution

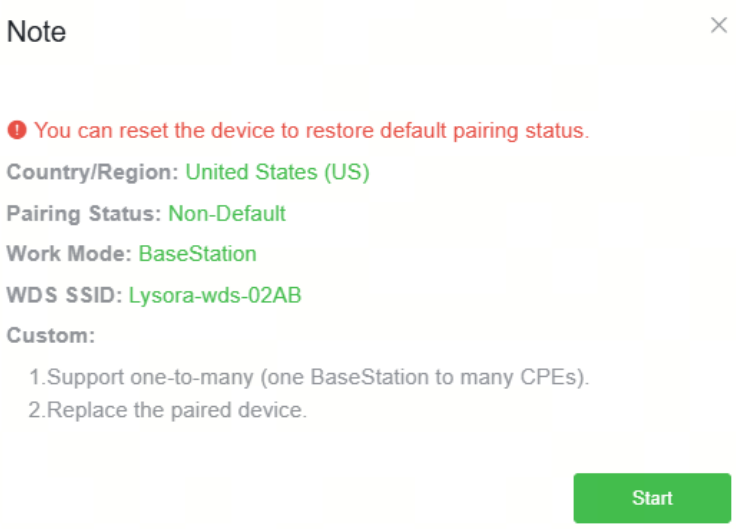
Switching the mode will reboot the device. Therefore, exercise caution when performing this operation.

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.

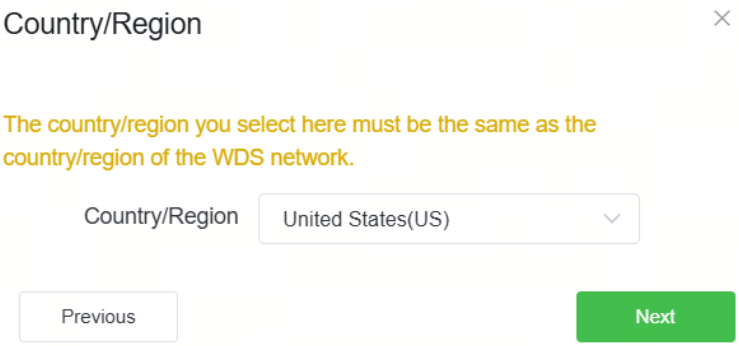
(1) You can check the current mode in the upper right corner of the web management interface and click **Switch Mode** to switch the mode.



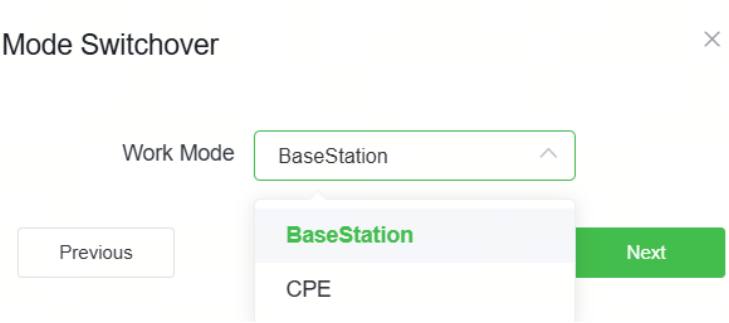
(2) In the displayed dialog box, click **Start**.



(3) Select a country or region, and click **Next**.



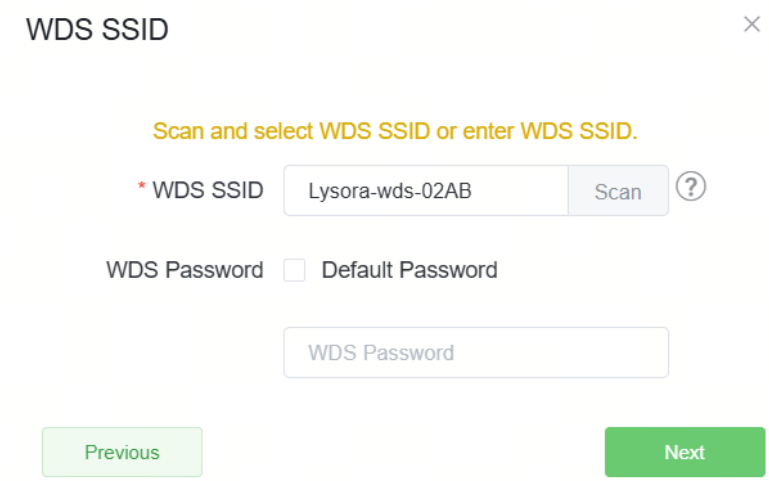
(4) Select the work mode, and click **Next**.



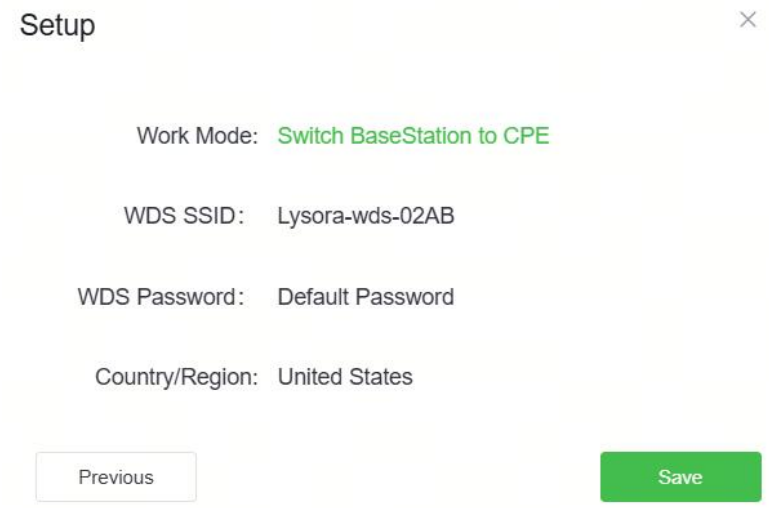
(5) Enter the bridging SSID and password, and click **Next**.

Specification

This feature is supported only when the BaseStation mode is switched to CPE mode.



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



3.3 Scanning to Pair and Add Devices

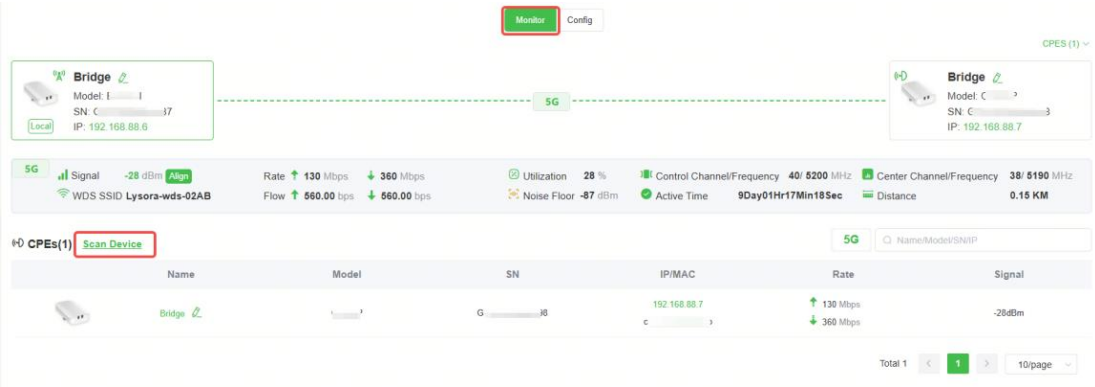
3.3.1 Overview

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.

3.3.2 Configuration Steps

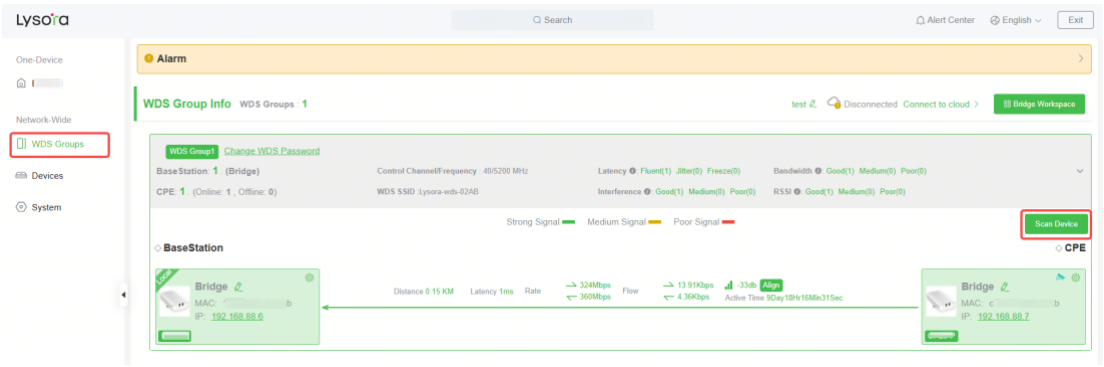
Go to the configuration page:

- Method 1: Choose **One-Device** > **Monitor**.
  - For bridged devices, click **Scan Device** next to **CPEs**.



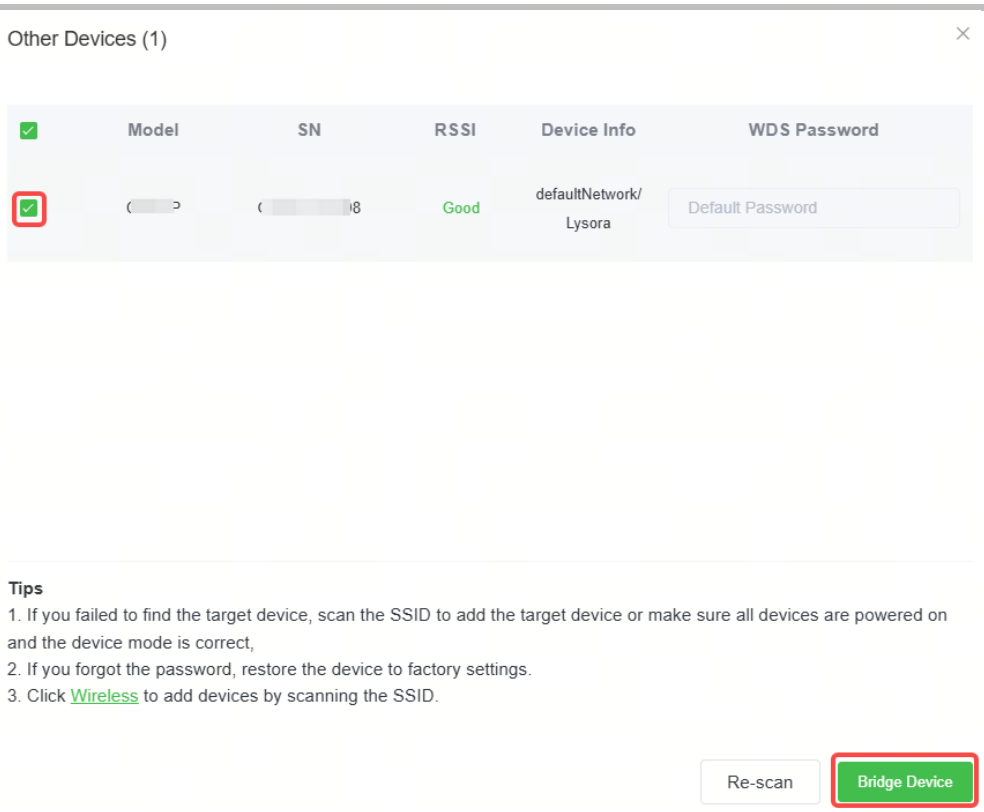
  - For unbridged devices, click the add icon .

- Method 2: Choose **Network-Wide** > **WDS Groups.** Select a WDS group, and click **Scan Device.**



After the device scan is complete, select the desired device, enter the bridging password in the **WDS Password** field, and click **Bridge Device**. The selected device will be bridged.

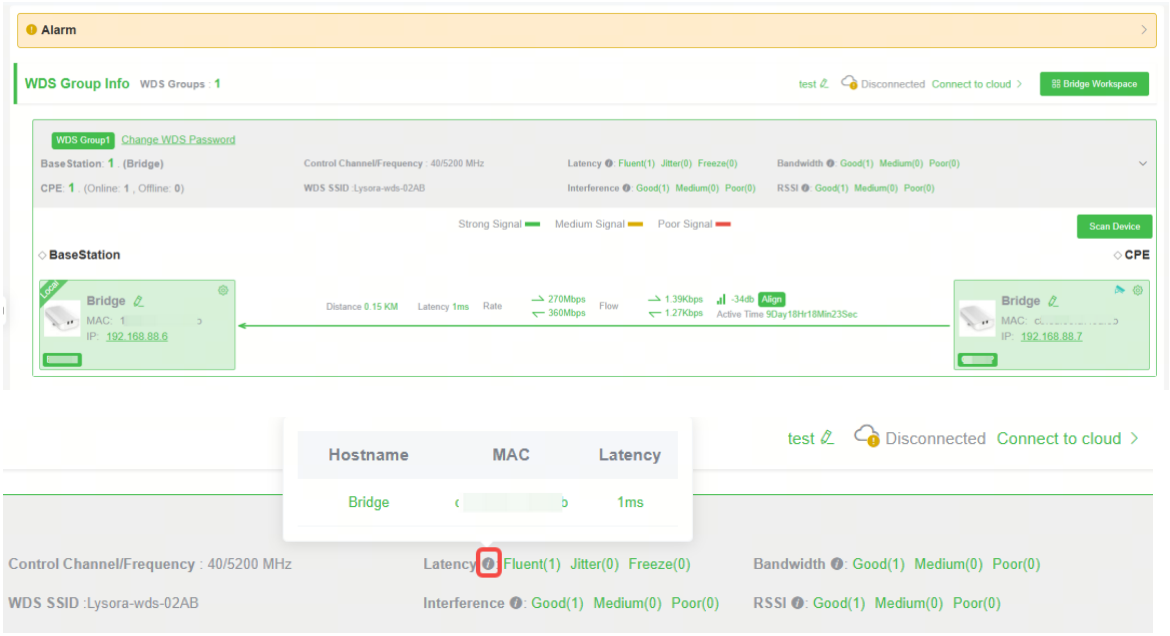
If no device is displayed, click **Re-scan**.



3.4 Displaying WDS Group Information

Choose **Network-Wide** > **WDS Groups**.

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.



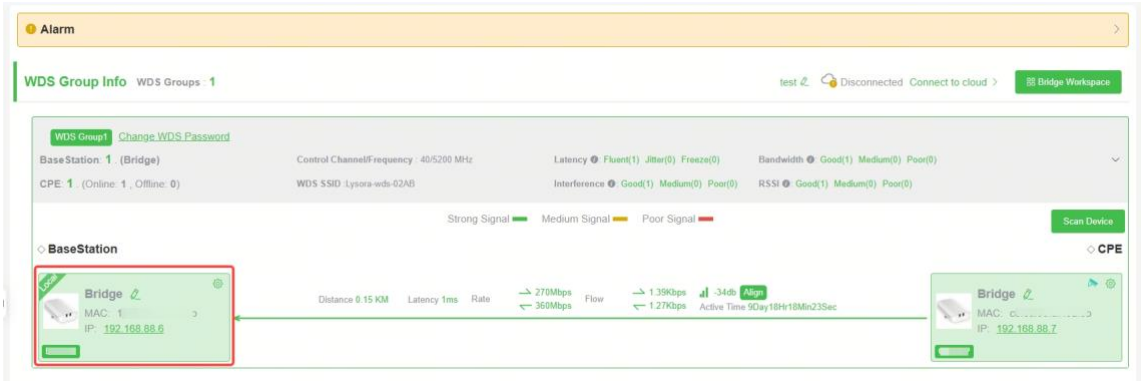
Note

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

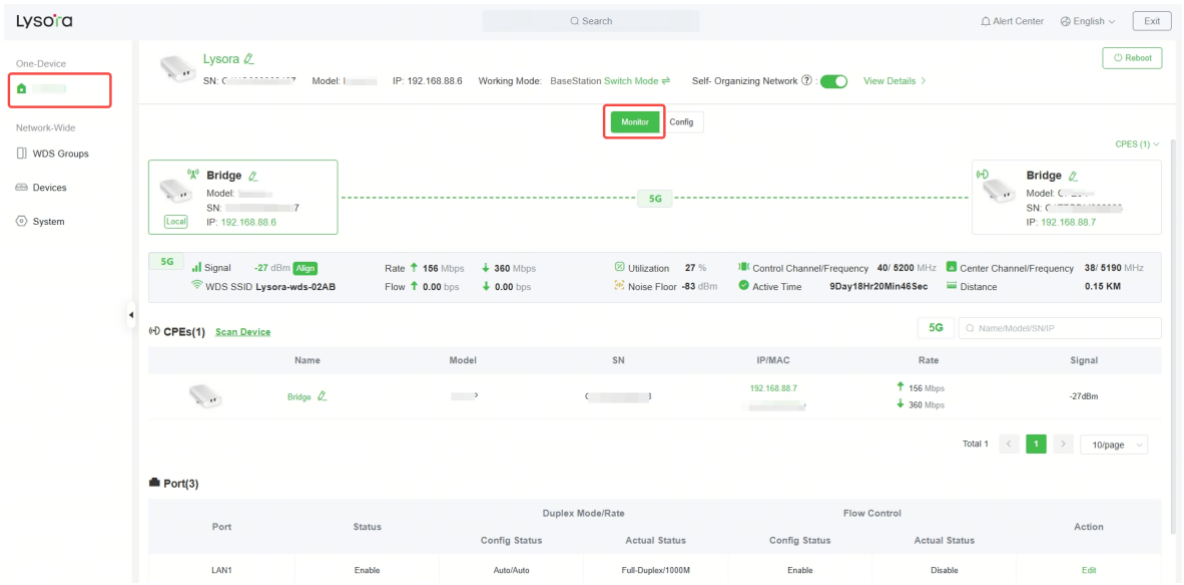
3.5 Displaying the Information About a Bridge

Go to the configuration page:

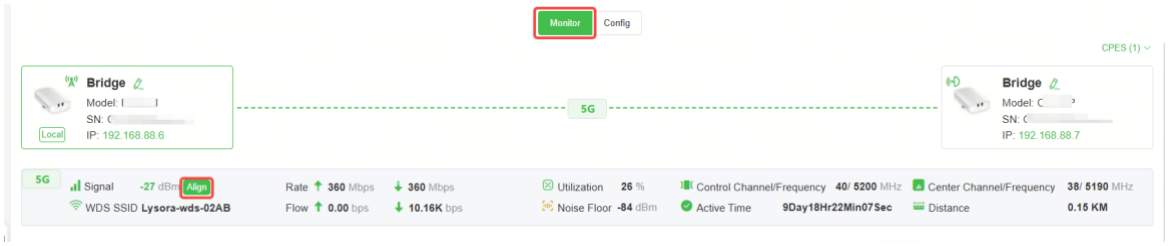
- Method 1: Choose **One-Device** > **Monitor**.
- Method 2: Choose **Network-Wide** > **WDS Groups**. Click the device icon to view the basic information of the selected device in the pop-up window that appears on the right side of the page.

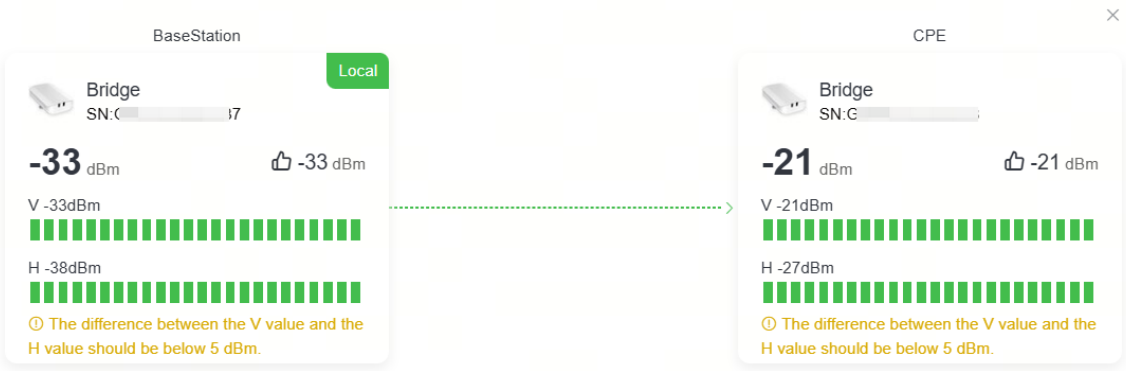


The page displays relevant information about the device, including the peer device in the WDS group, bridging link status, CPE details, and port status. On the **Monitor** page, you can perform antenna alignment, scan for CPE, and modify the port status.

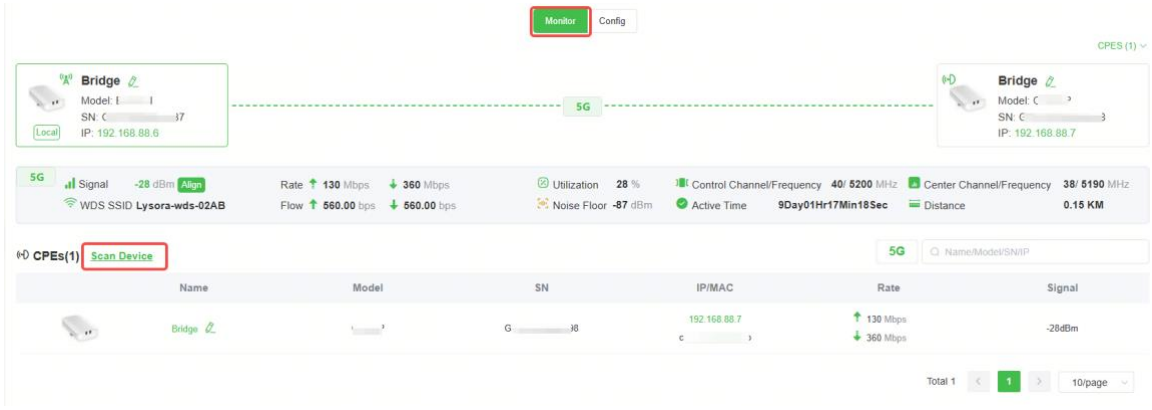


- Antenna alignment: Click **Align** to view the real-time RSSI in the pop-up window. For details, see 5.1Antenna Alignment.





- Scan for CPE: Click **Scan Device** to discover other bridges. For details, see 3.3Scanning to Pair and Add Devices.



- Modify port settings: In the **Port** pane, click **Edit** to modify the port settings. For details, see 4.5Port Settings.

Specification

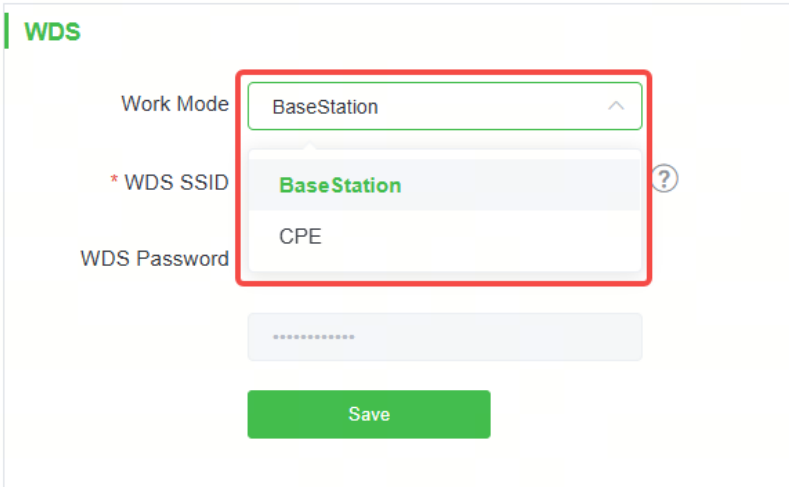
The device at the NVR end does not involve channel width and RSSI, and only the device at the camera end does.

3.6 Configuring a Bridging Wi-Fi Network for a Standalone Device

3.6.1 Configuring the Work Mode

Choose **One-Device** > Config > **Wireless** > **WDS**.

Select the work mode as **BaseStation** or **CPE**.



3.6.2 Setting the WDS SSID

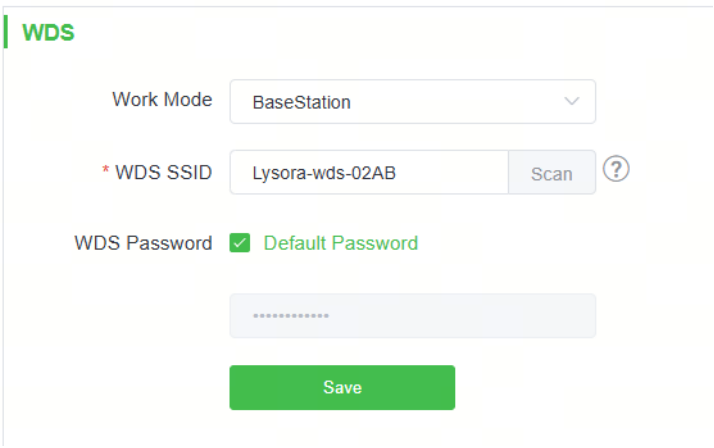
Caution

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.

Choose **One-Device** > **Config** > **Wireless** > **WDS**.

Specification

This feature is only supported by bridges in CPE mode.



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 **Network-Wide** > **WDS Groups** > **WDS Group Info**. For details, see 3.4Displaying WDS Group Information.

3.6.3 Configuring the WDS Password

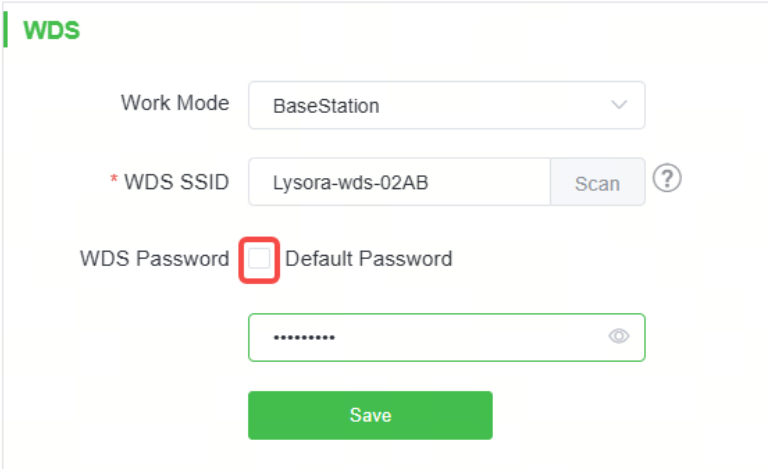
⚠ Caution

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.

Choose **One-Device** > **Config** > **Wireless** > **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.



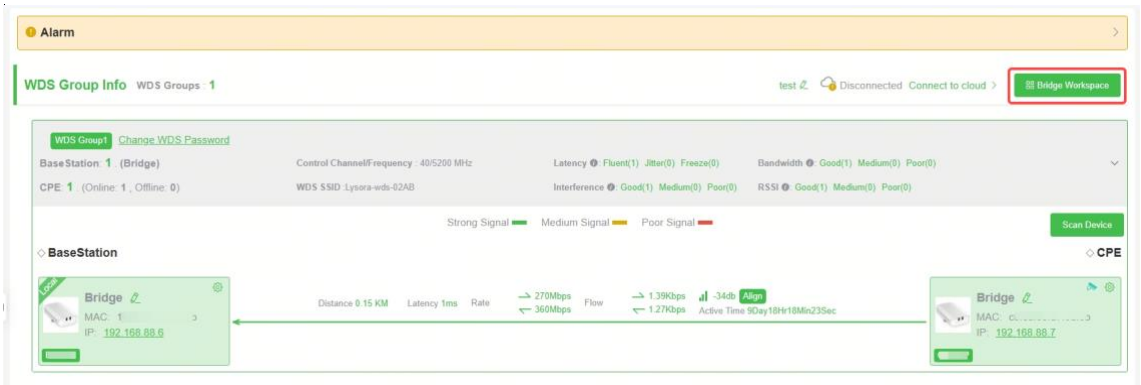
3.6.4 Saving the Settings

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

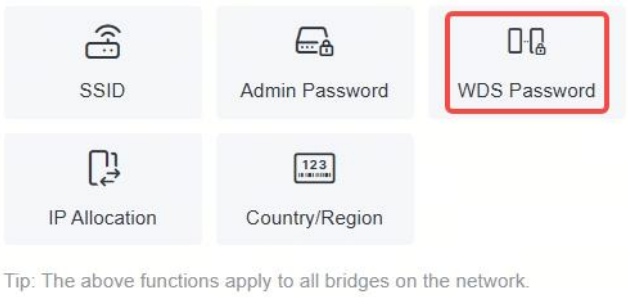
3.7 Configuring the WDS Password for a LAN

Choose **Network-Wide** > **WDS Groups**.

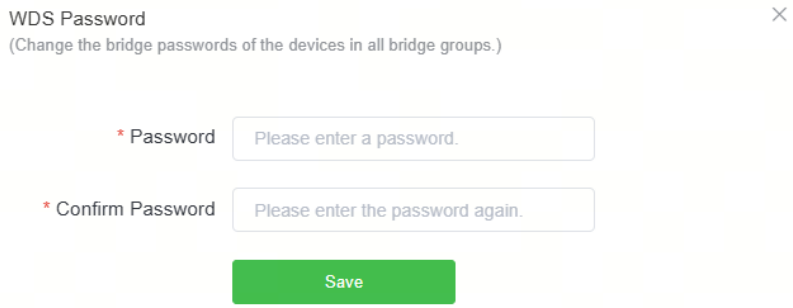
(1) Click **Bridge Workspace**.



(2) Click **WDS Password**.



(3) Enter the password in the displayed dialog box, and click **Save**.



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.

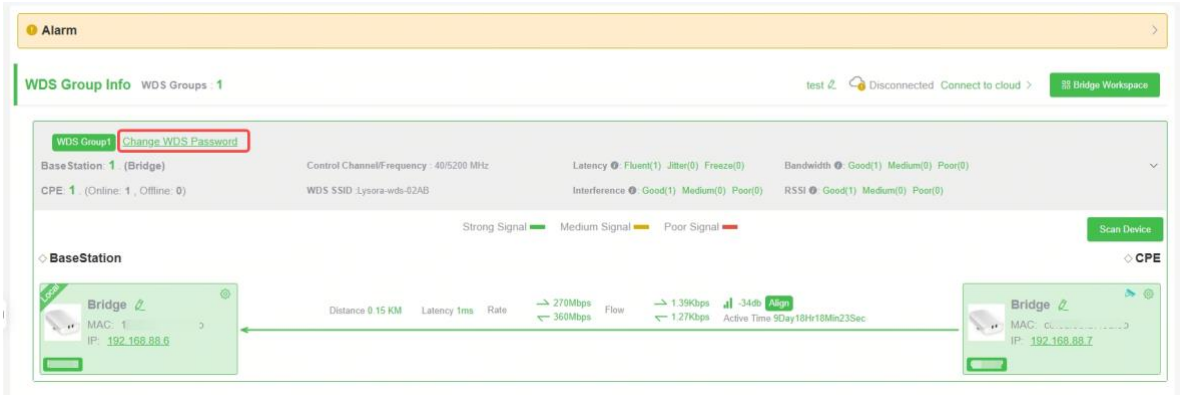
3.8 Configuring the WDS Password for a WDS Group

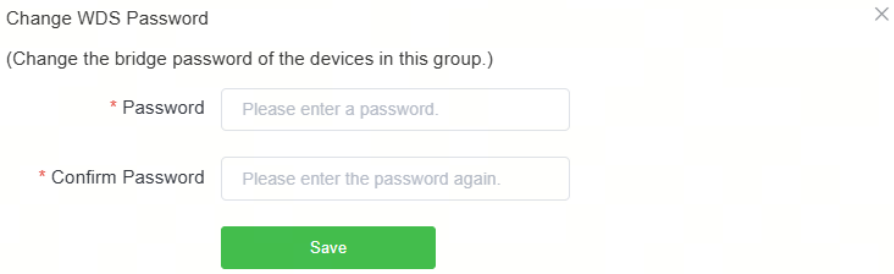
Choose **Network-Wide** > **WDS Groups**.

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.

3.9 Configuring the Management SSID for a Standalone Device

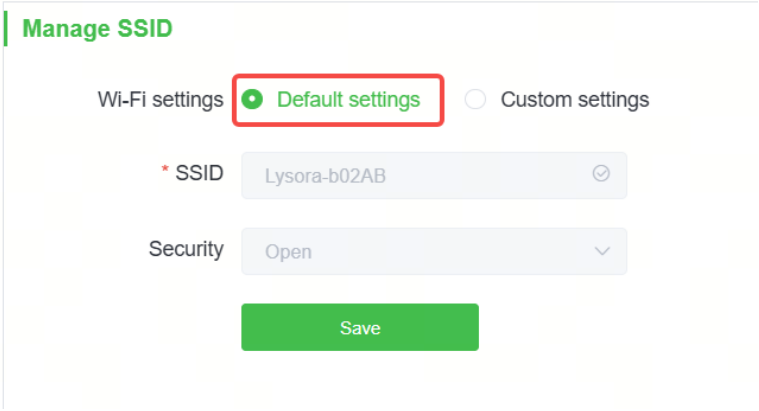
Choose **One-Device** > **Config** > **Wireless** > **Manage SSID**.

ⓘ Note

The management SSID is used for accessing the web management interface and managing devices, and is isolated from the service network.

3.9.1 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.



3.9.2 Custom Configuration

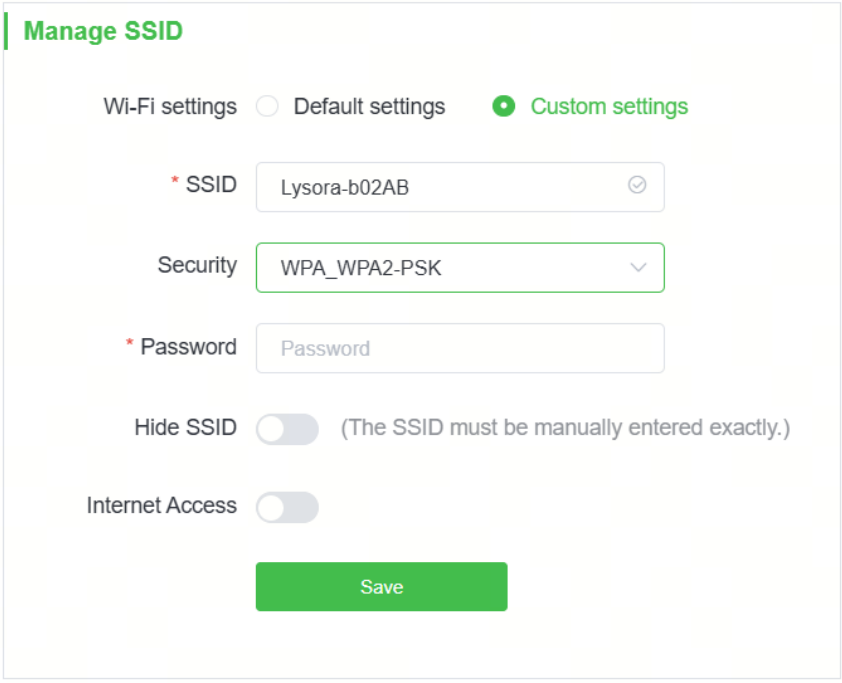
SSID: Indicates the Wi-Fi name to which the mobile phone or management PC connects for accessing the web management interface and managing devices.

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 **Network-Wide** > **WDS Groups** > **Bridge Workspace** > **SSID**. For details, see 3.10Configuring the Management Wi-Fi and Password for a LAN.

Internet Access: After it is toggled on, you can access the Internet through the management SSID.



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

Caution

- Once the configuration is saved, all bridges on the network will share the same SSID and password.
- After the configuration is saved, the BaseStation and CPE devices in the network will be reconnected. Therefore, exercise caution when performing this operation.

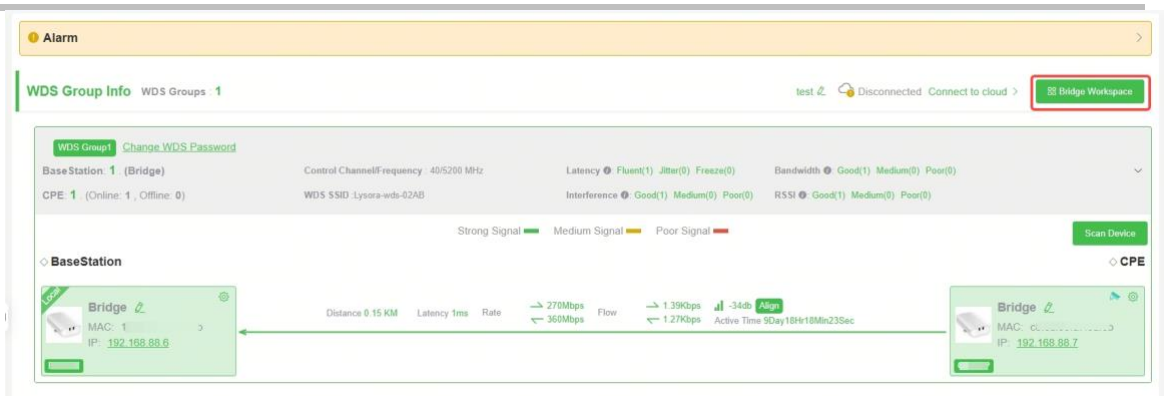
Note

The management SSID is used for accessing the web management interface and managing devices, and is isolated from the service network.

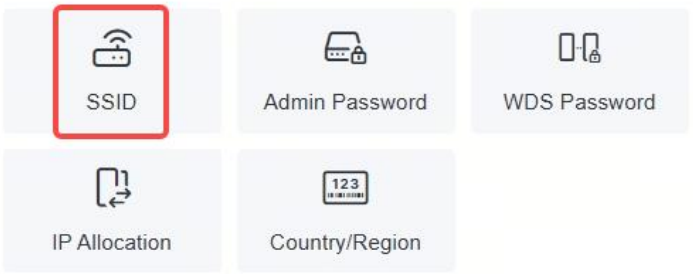
Choose **Network-Wide** > **WDS Groups**.

The default SSID for device management is ***Lysora-bXXXX***. (XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with each device.) You can set the same management SSID and password for all bridges in the LAN.

(1) Click **Bridge Workspace**.

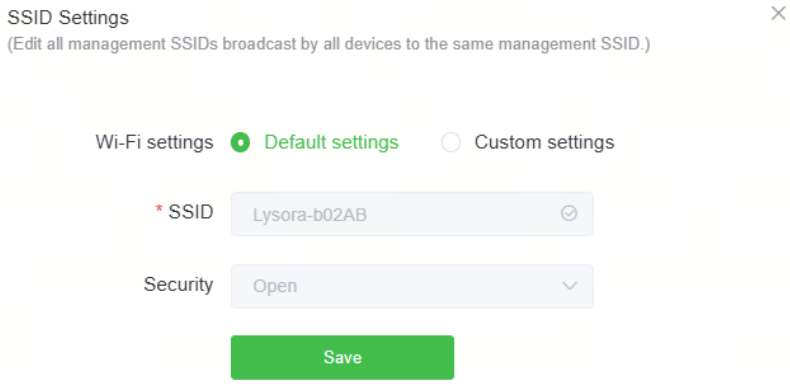


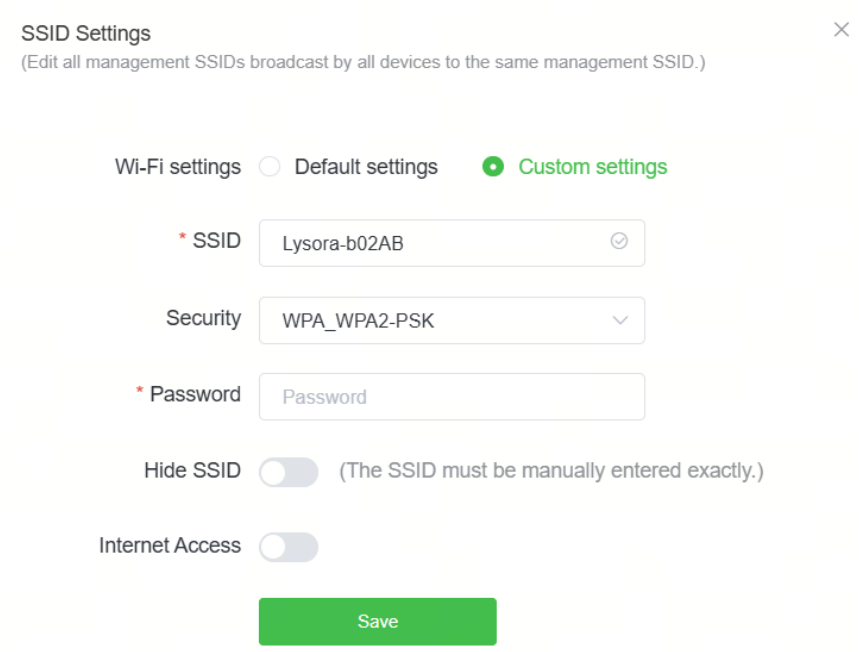
(2) Click **SSID**.



Tip: The above functions apply to all bridges on the network.

(3) Set related parameters.





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.

Internet Access: After it is toggled on, you can access the Internet through the management SSID.

(4) Click **Save**.

3.11 Configuring the Country/Region Code for a Bridge

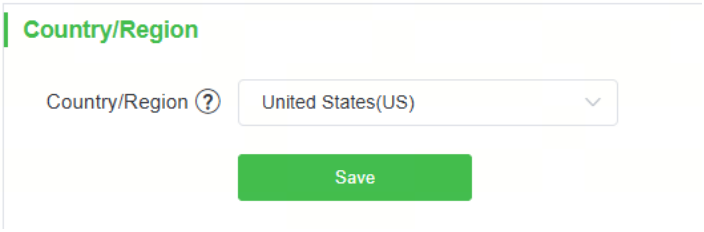
⚠ Caution

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

Choose **One-Device** > **Config** > **Wireless** > **Country/Region**.

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 3.12Setting the Country/Region Code for a WDS Group for details.

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.

3.12 Setting the Country/Region Code for a WDS Group

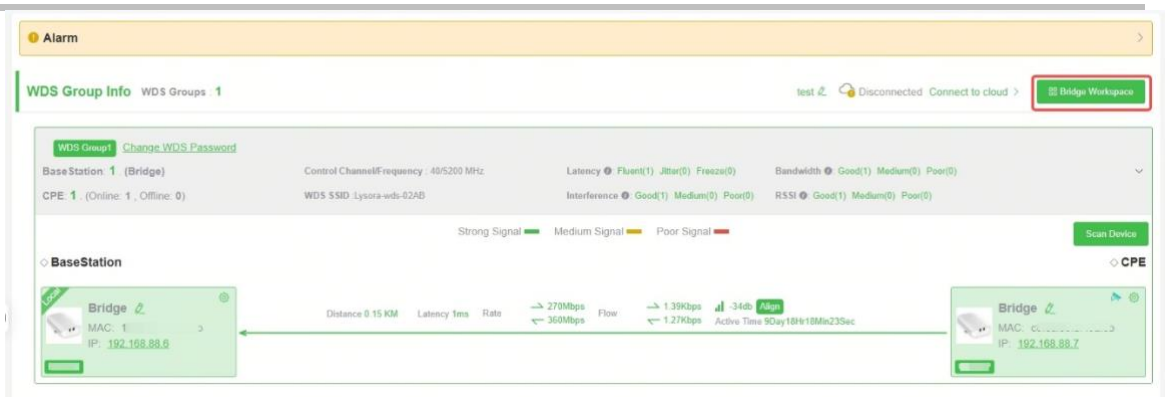
⚠ Caution

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.

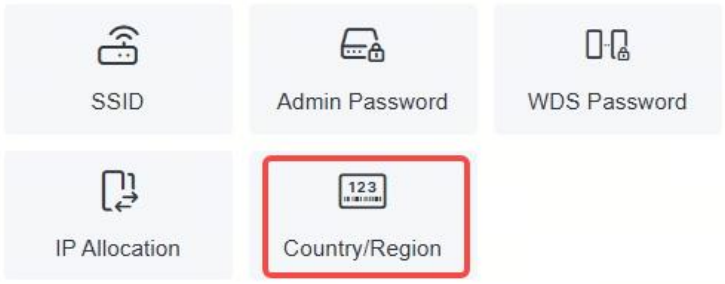
The country/region code switch will take effect on all devices on the network, including those listed on the homepage of the web management interface. Therefore, before configuring the country/region code, you are advised to go to the homepage and check whether the target devices are on the current network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

Choose **Network-Wide** > **WDS Groups**.

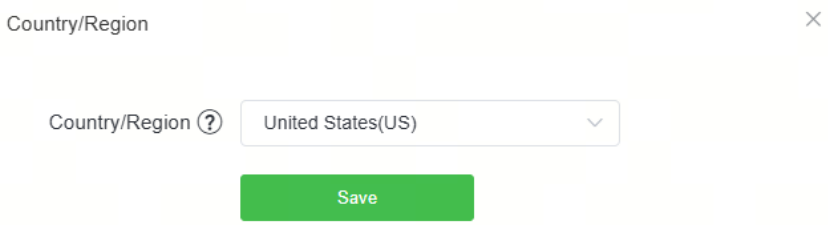
(1) Click **Bridge Workspace**.



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



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



3.13 Setting the SSID for a Single Bridge

3.13.1 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.

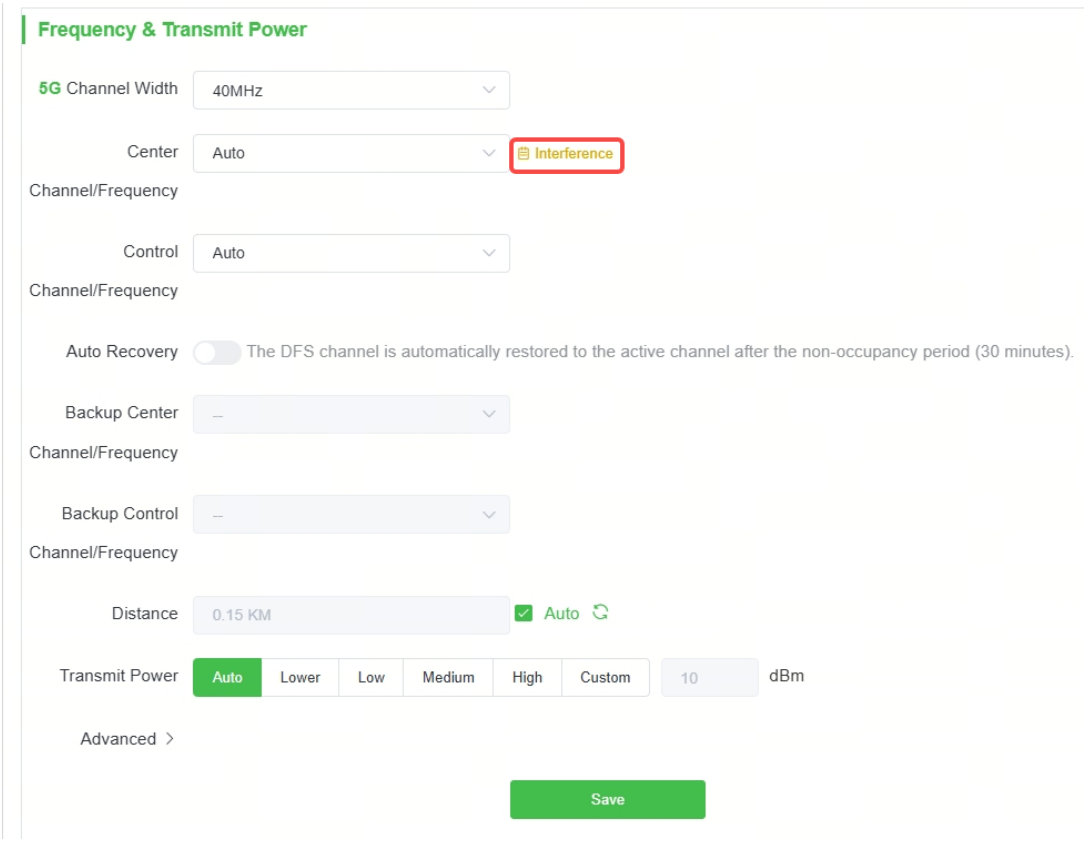
3.13.2 Getting Started

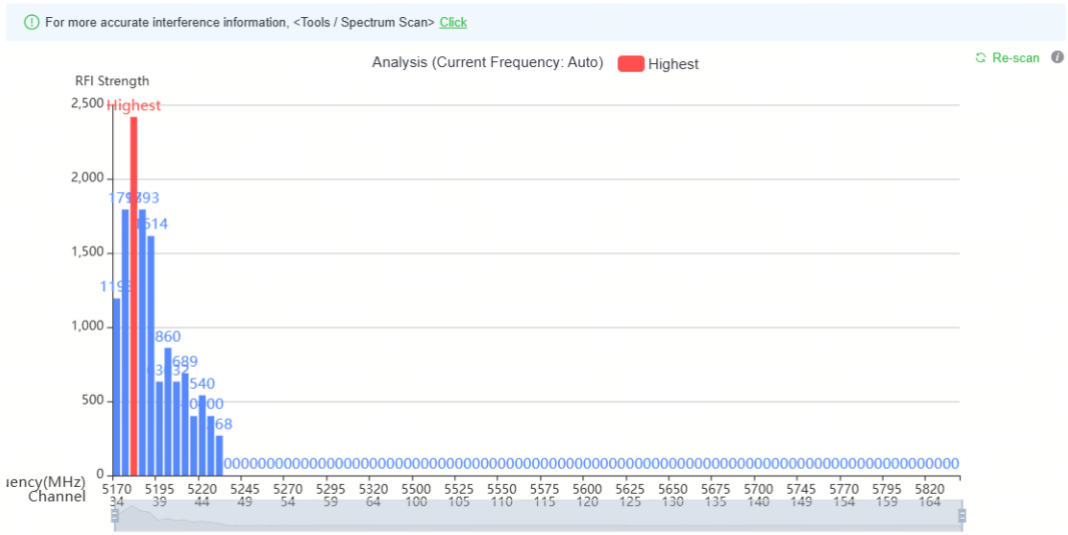
Before configuration, you can check the interference in the current environment in the following way to find the optimal frequency.

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

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

To view the interference details of each frequency, go to the **Spectrum Scan** page. For details, see 5.2Spectrum Scan.





3.13.3 Configuring the Channel Width

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

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

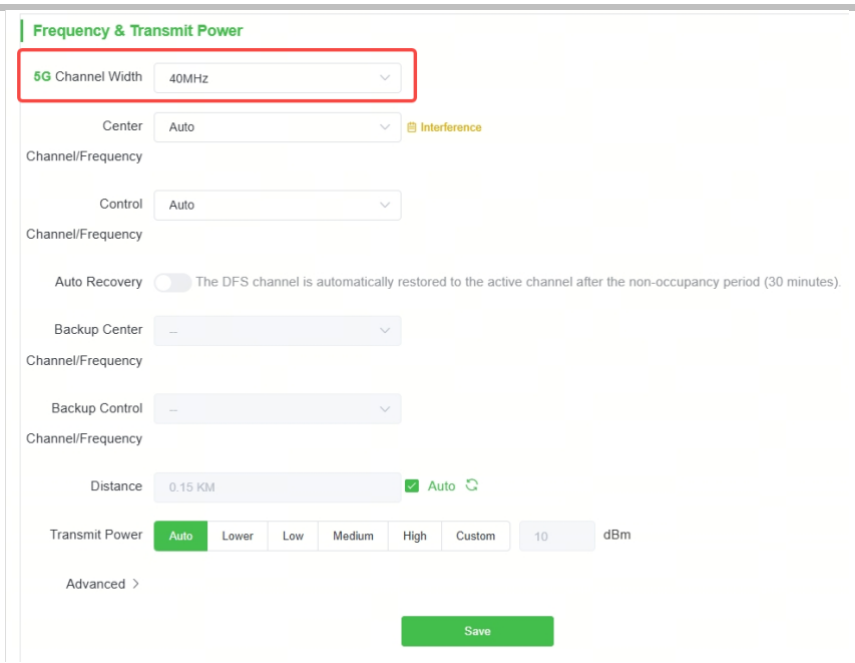
The 5 GHz bridge supports 20 MHz, 40 MHz, and 80 MHz, while the 2.4 GHz bridge supports 20 MHz and 40 MHz.

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.



3.13.4 Configuring Channels and Frequencies

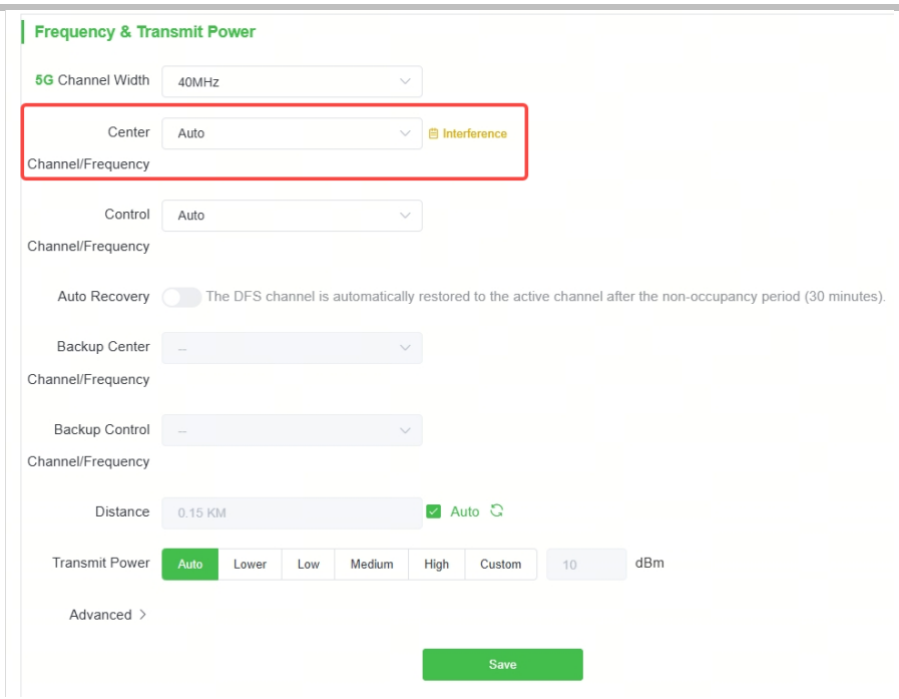
Note

The channel and channel width of bridges in CPE mode automatically match those of bridges in BaseStation mode and cannot be modified.

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

1. Configuring Center Channel/Frequency

The center channel/frequency is used for data transmission. The default value is **Auto**, indicating that the device will automatically adapt to the surrounding environment when powered on. In cases of severe wireless interference or slow data speeds, you can select an optimal channel and frequency based on the interference analysis results. Then, click **Save** to save your changes.



Once the channel/frequency is changed on the bridge in BaseStation mode, the bridge in CPE mode will automatically synchronize with the new settings.

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

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

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

Note

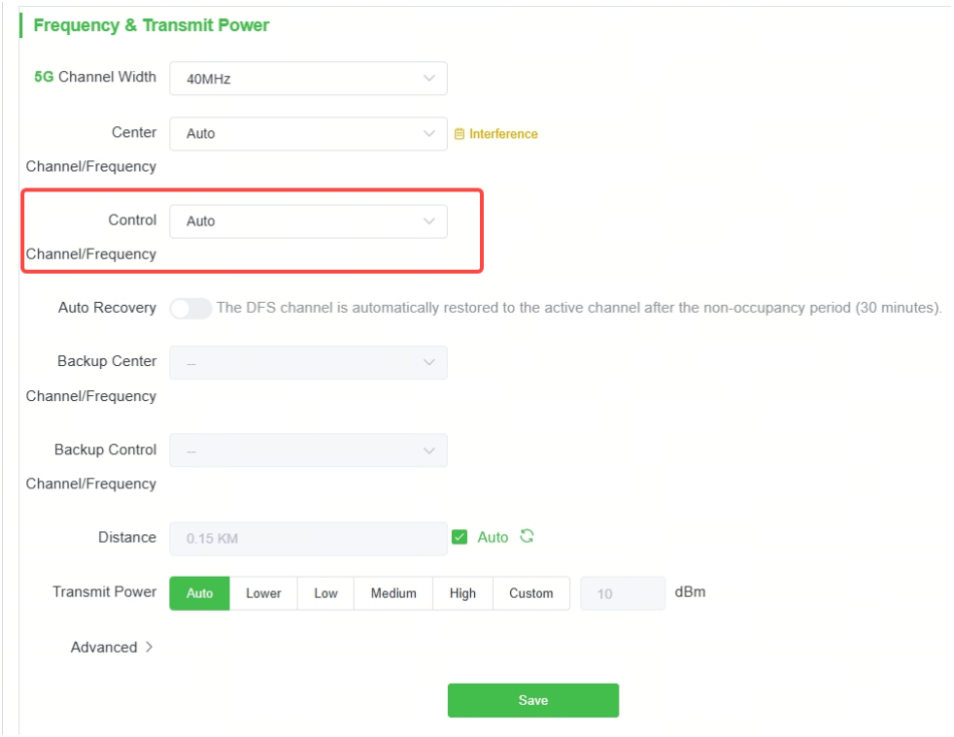
- The available frequencies are subject to the country/region code. Select the country or region where the device will be used.
- The preceding figure shows the frequency configuration for 5 GHz, and that for 2.4 GHz is the same.
- The bridge that supports only the 2.4 GHz frequency band does not support the 5 GHz frequency configuration.

⚠ Caution

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

2. Configuring Control Channel/Frequency

The control channel/frequency is used to transmit network control information, reducing channel conflicts and interference. The default value is **Auto**, indicating that the device will automatically adapt to the surrounding environment when powered on. To modify the value, see 5.2Spectrum Scan.



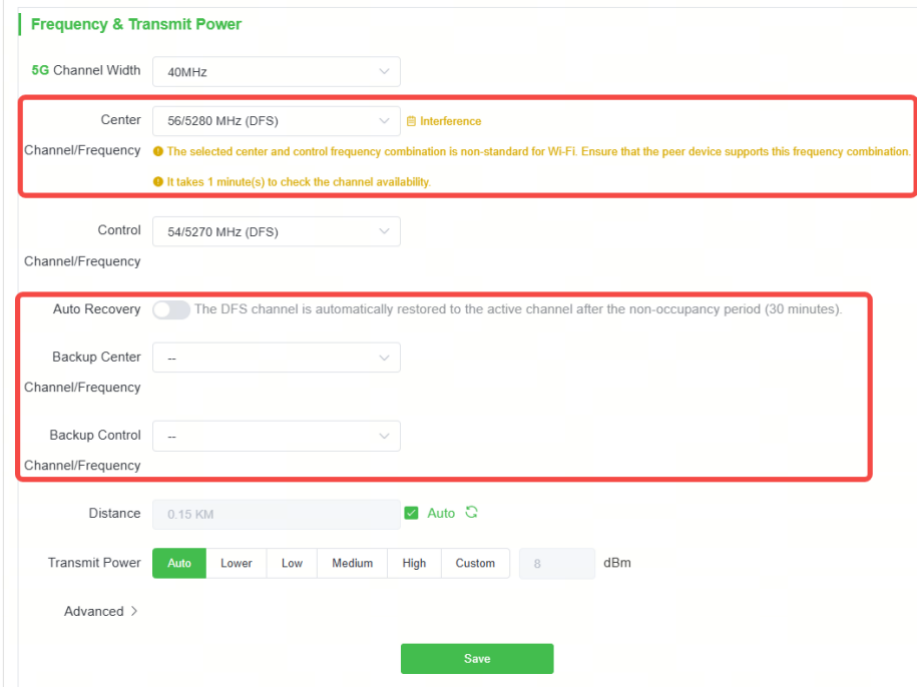
3.13.5 Configuring a Backup DFS Channel

✓ Specification

- Only bridges supporting the 5 GHz band support this feature.
- This feature is only supported on devices operating in recorder (BaseStation) mode. For a device in camera (CPE) mode, its channel and channel width are automatically synchronized with those of the recorder (BaseStation) and cannot be modified.

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

When **Center Channel/Frequency** is set to a DFS channel, you can configure **Auto Recovery**, **Backup Center Channel/Frequency**, and **Backup Control Channel/Frequency** to ensure normal operation of the device in the event of DFS signal detection.



- **Auto Recovery**: After it is toggled on, the device can automatically revert to the original center channel/frequency after the 30-minute DFS non-occupancy period.
- **Backup Center Channel/Frequency**: When a DFS signal is detected on the center channel, the device automatically switches to the backup channel to maintain normal operation.
- **Backup Control Channel/Frequency**: It is used for transmitting network control information in most cases, helping reduce channel conflicts and interference.

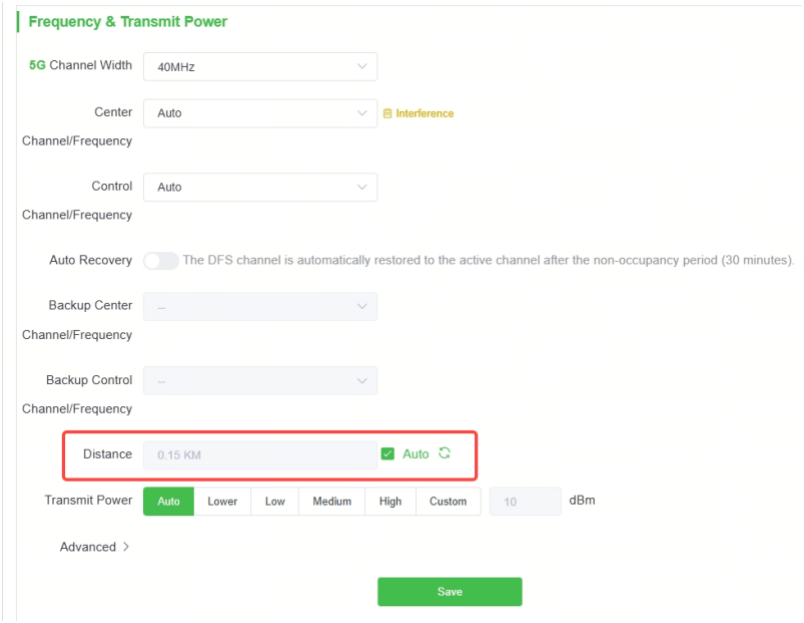
Note

When **Auto Recovery** is toggled on without a backup channel configured, a device backs off to another channel at random if the active channel is a DFS channel and the device detects a radar signal on the channel. After the non-occupancy period ends, the device switches back to the original active channel.

3.13.6 Configuring the Distance

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

The deployment distance between the bridge in BaseStation mode and the bridge in CPE mode must be set manually, except for bridges that support automatic distance measurement. In manual mode, you are advised to set a distance greater than the actual distance. If the configured distance is too small, wireless performance is degraded, and bridging may fail.



The maximum distance vary with the devices: 3 km for the CPE3-P, and 5 km for the CPE5.

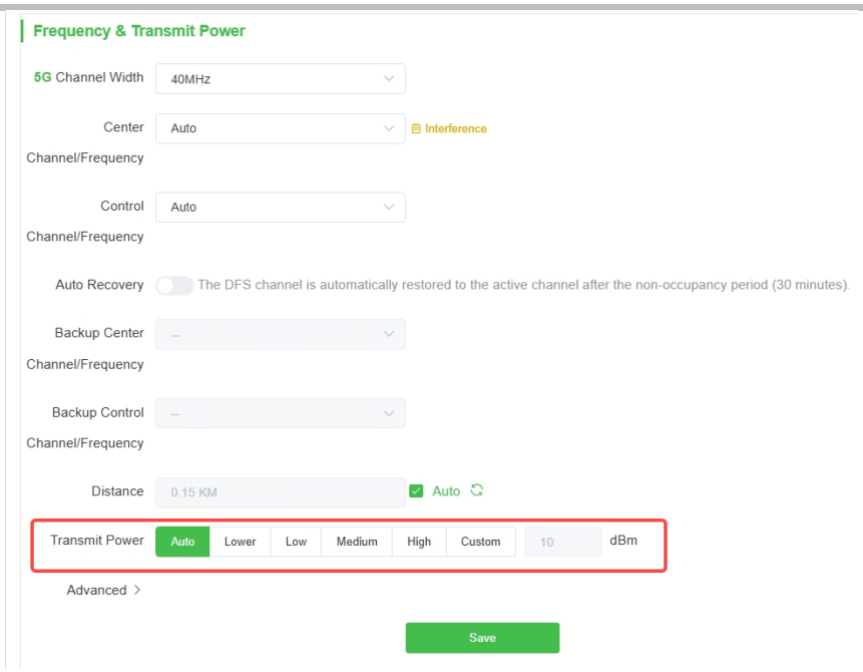
3.13.7 Configuring the Transmit Power

Choose **One-Device** > **Config** > **Wireless** > **Frequency & 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.

When you select **Lower**, **Low**, **Medium**, or **High**, the transmit power is displayed in the input box. If the default options do not meet your needs, you can select **Custom** and enter the desired transmit power for wireless transmission.



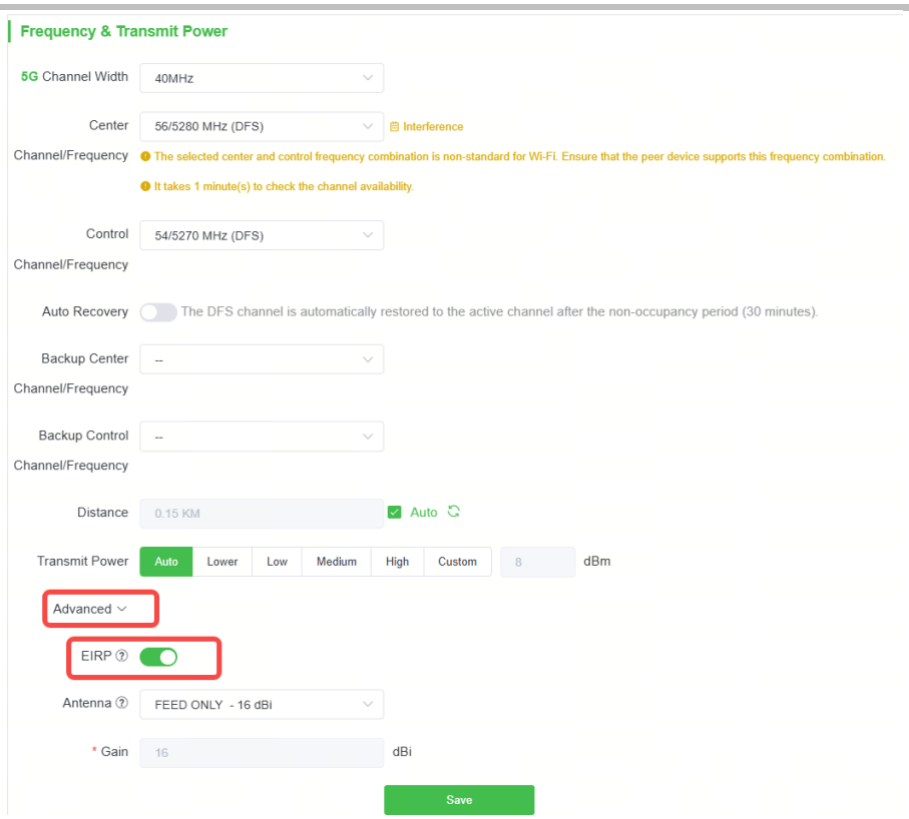
3.13.8 Configuring the EIRP

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

EIRP can be used to limit the transmit power of the device, ensuring compliance with wireless signal transmission regulations.

Note

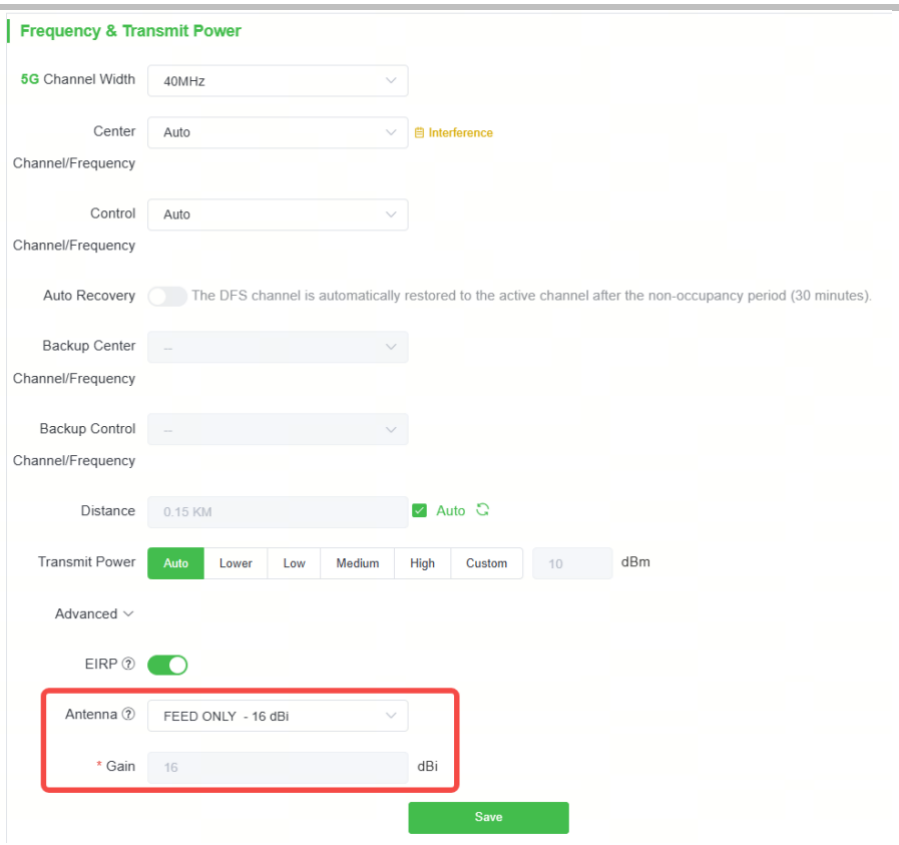
The EIRP feature is enabled by default for bridges intended for the U.S. and Canadian markets, but it is disabled by default for all other countries/regions.



3.13.9 Configuring the Antenna Gain

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

Select the type of antenna for the device. If **Custom** is selected, enter the antenna gain.



3.14 Configuring TDMA Mode

Specification

This function is supported only in the BaseStation mode.

3.14.1 Overview

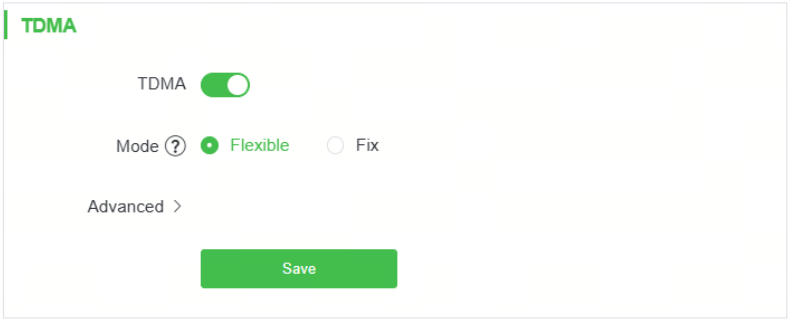
Time Division Multiple Access (TDMA) is specifically designed to address the challenge of CPE nodes being hidden from each other over long distances. In the traditional Wi-Fi mechanism utilizing Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the nodes are unable to listen to each other,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

3.14.2 Selecting the TDMA Mode

Choose **One-Device** > **Config** > **Wireless** > **TDMA**.

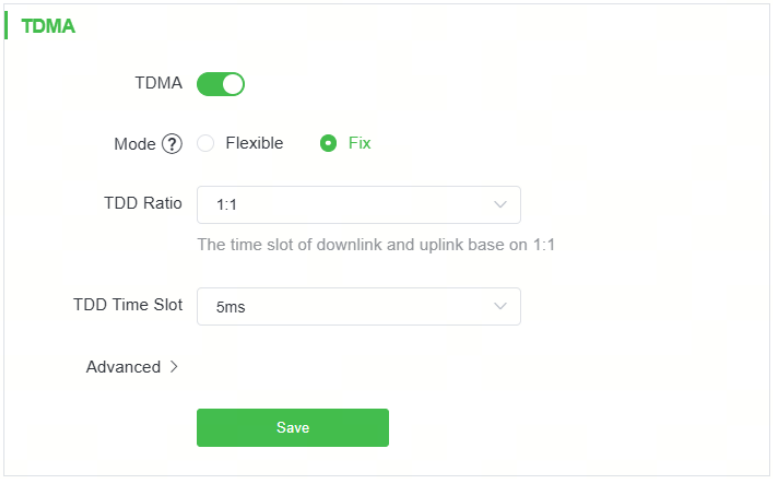
1. Flexible mode

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.



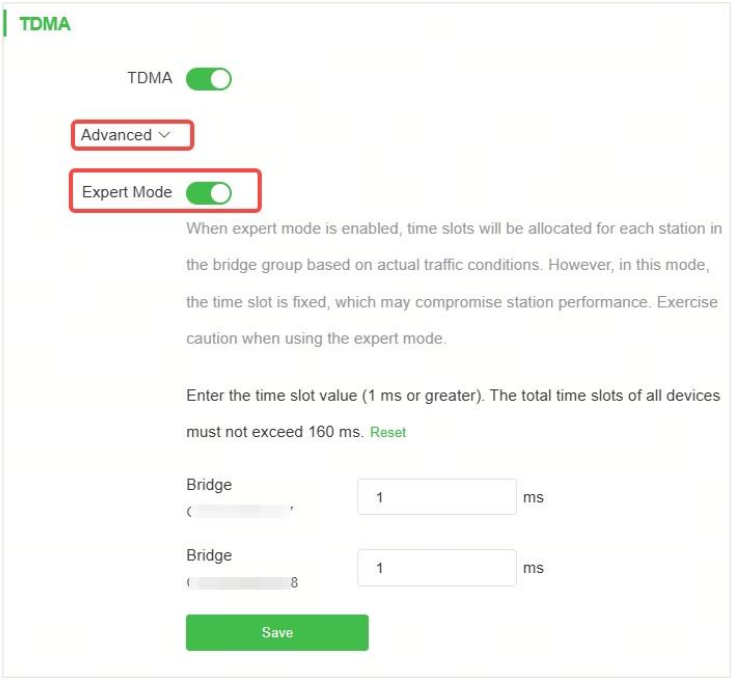
2. Fixed mode

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.



3. Expert mode

Expand **Advanced** and toggle on **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.

4 Advanced Settings

4.1 Storm Control

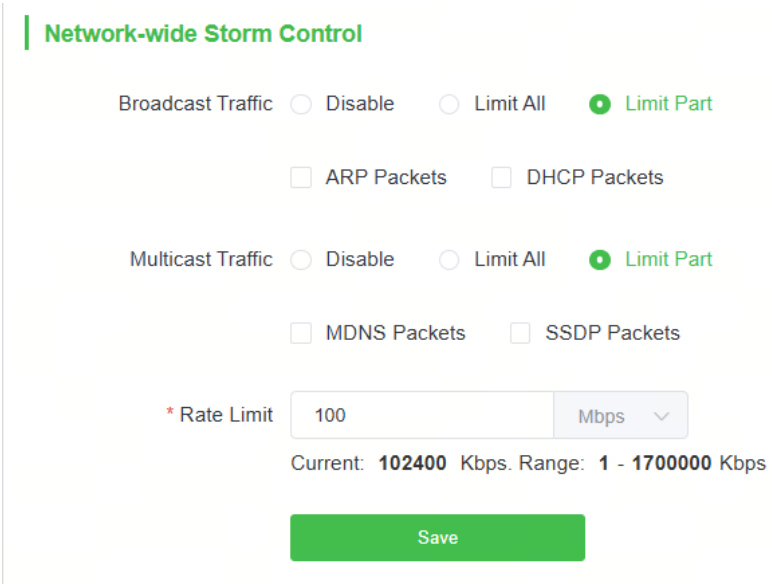
Enable rate limiting on broadcast or multicast packets to avoid congestion on the air interface.

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 **One-Device** > **Config** > **Advanced** > **Storm Control**.



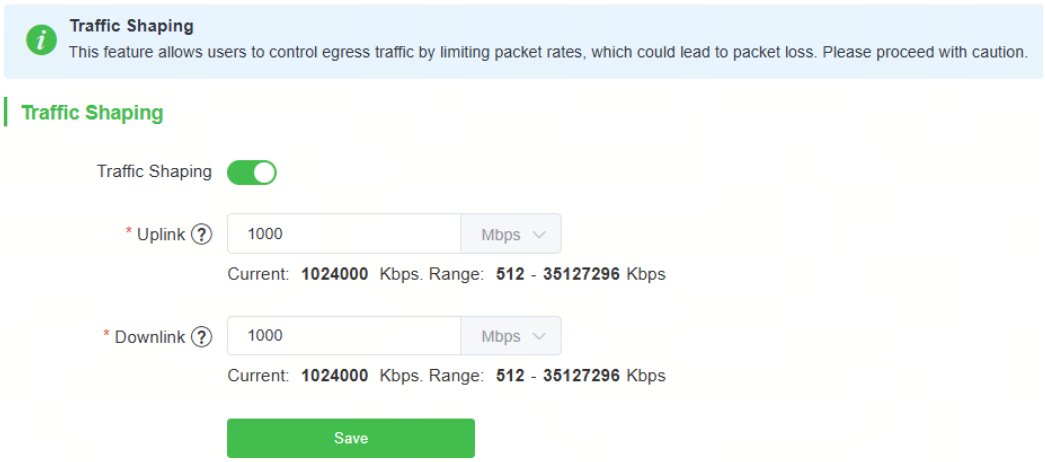
4.2 Configuring Traffic Shaping

Choose **One-Device** > **Config** > **Advanced** > **Traffic Shaping**.

Toggle on **Traffic Shaping**. Set the uplink and downlink rate limits, and click **Save** to limit the packet transmission rates. Improper rate limits may lead to packet loss. Please proceed with caution.

Note

- The **Traffic Shaping** feature allows users to control egress traffic by limiting packet rates.
- The Flow Control feature introduced in 4.5Port Settings can relieve the data congestion caused by ports at different speeds and improve the network speed



- Uplink rate limit: This limits the packet transmission rate from the bridge in CPE mode to the bridge in BaseStation mode, or from the bridge in BaseStation mode to the uplink device.
- Downlink rate limit: This limits the packet transmission rate from the bridge in BaseStation mode to the bridge in CPE mode, or from the bridge in CPE mode to downlink devices.

4.3 Configuring One-Touch Pairing

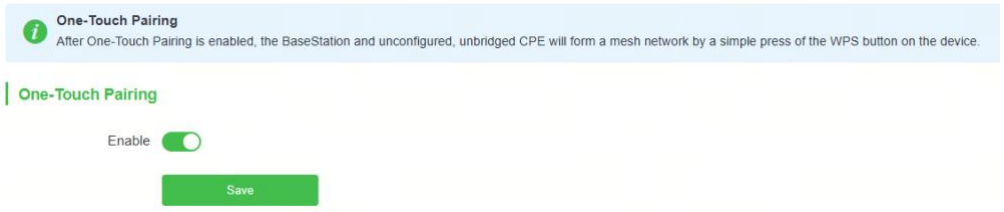
When the One-Touch Pairing feature is enabled, a simple press of the One-Touch Pairing button on the device triggers the mesh operation. During the mesh process, the BaseStation promptly forms a mesh connection with the factory-configured and unbridged CPE, streamlining the networking process.

Choose **One-Device** > **Config** > **Advanced** > **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.



Specification

The **One-Touch Pairing** feature is enabled by default.

4.4 Wi-Fi Protection

Specification

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

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.

Choose **One-Device** > **Config** > **Advanced** > **Wi-Fi Protection**.

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

4.5 Port Settings

Choose **One-Device** > **Monitor.**

In the **Port** pane, click **Edit** to modify the port settings.

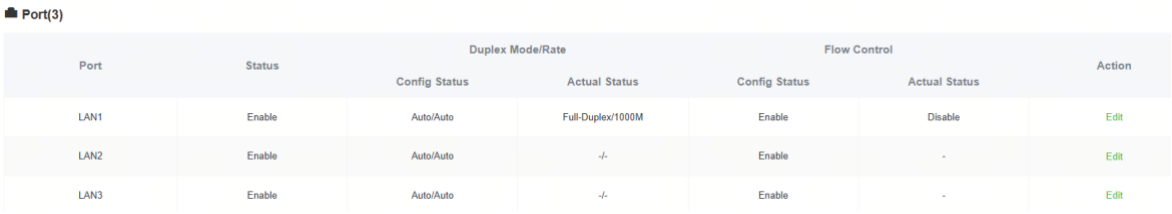


Table 4-1 Port Configuration Parameters

Parameter	Description
Status	Enable or disable the port.
Rate	Set the data transmission rate of the port. The options are **Auto**, **10M**, **100M**, and **1000M**. When selecting the port rate, ensure that the connected device can communicate at the same rate. If a device only supports a rate of 100 Mbps, but the port rate is set to 1000 Mbps, communication may fail due to rate mismatch.
Working Mode	Set the working mode of the port: ● **Auto**: The port automatically detects the working mode of the connected device and automatically selects the full-duplex or half-duplex mode based on the connected device. ● **Full-duplex**: In full-duplex mode, a port can send and receive data simultaneously, achieving bidirectional communication. ● **Half-duplex**: In half-duplex mode, a port can only send or receive data, but not both.
Flow Control	Port Flow Control function is enabled by default. When wired ports of the device work in different rates, data blocking may occur, leading to slow network speed. Enabling port flow control helps relieve the data congestion. **Note** The **Traffic Shaping** feature introduced in 4.2Configuring Traffic Shaping allows users to control egress traffic by limiting packet rates.

(2) Set the port parameters and click **OK**.

5 Tools

5.1 Antenna Alignment

⚠ Caution

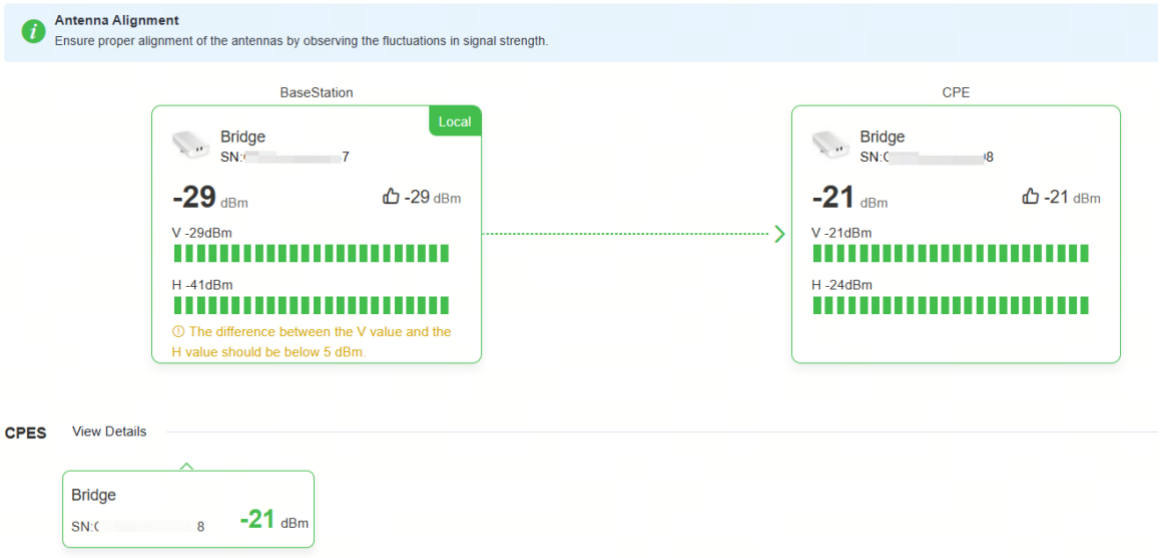
- If the device is in BaseStation mode, you can view the information for all devices in CPE mode.
- If the device is in CPE mode, you can view only information about the local device and the device in BaseStation mode.

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.

Go to the configuration page:

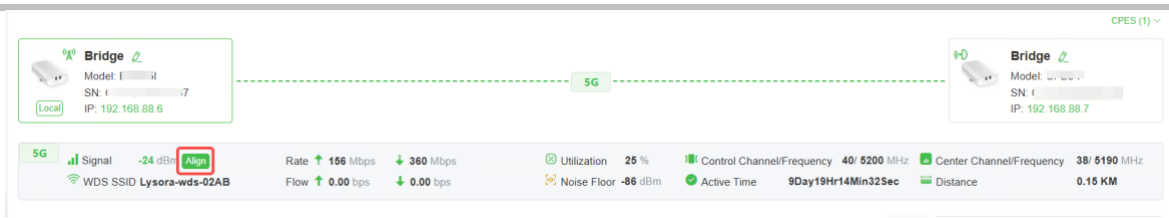
- Method 1: Choose **One-Device** > **Config** > **Tools** > **Antenna Alignment**.

The page displays the RSSI of the device's bridging link. If the device is in BaseStation mode and is bridged with multiple bridges in CPE mode, you can select any bridge in CPE mode to view details of the bridging link.



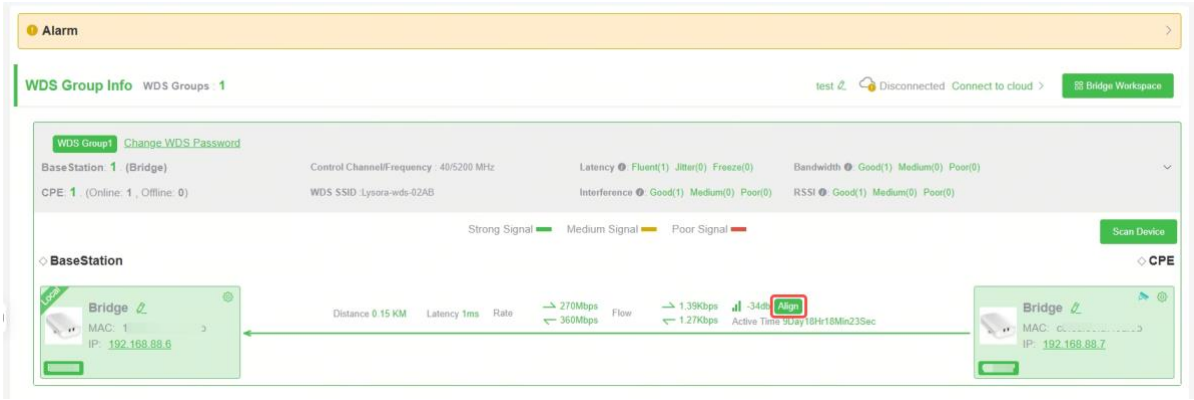
- Method 2: Choose **One-Device** > **Monitor**.

The page displays the RSSI of the device’s bridging link. Select a link and click **Align** to view details of the bridging link.

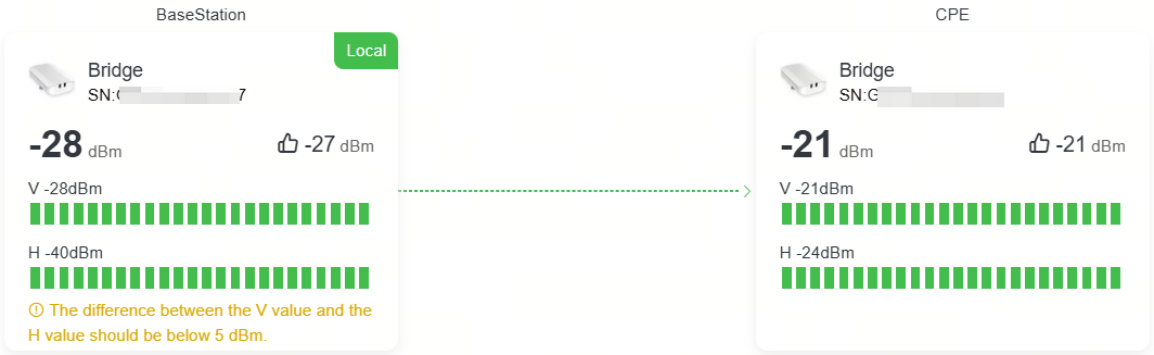


- Method 3: Choose **Network-Wide** > **WDS Groups**.

Select a link and click **Align** next to the RSSI, as shown in the following figure.



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.



5.2 Spectrum Scan

⚠ Caution

Bridges will be disconnected during spectrum scanning. Exercise caution when performing this operation.

Specification

This function is supported only in the BaseStation mode.

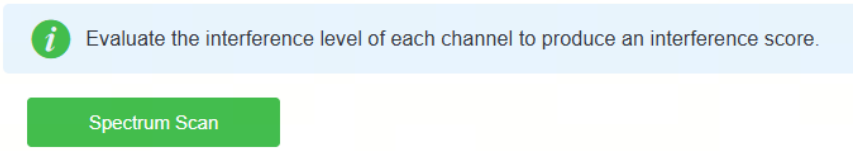
5.2.1 Overview

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 frequencies, and recommends a center channel/frequency for data transmission and a control channel/frequency for transmission of network control information based on the scan results.

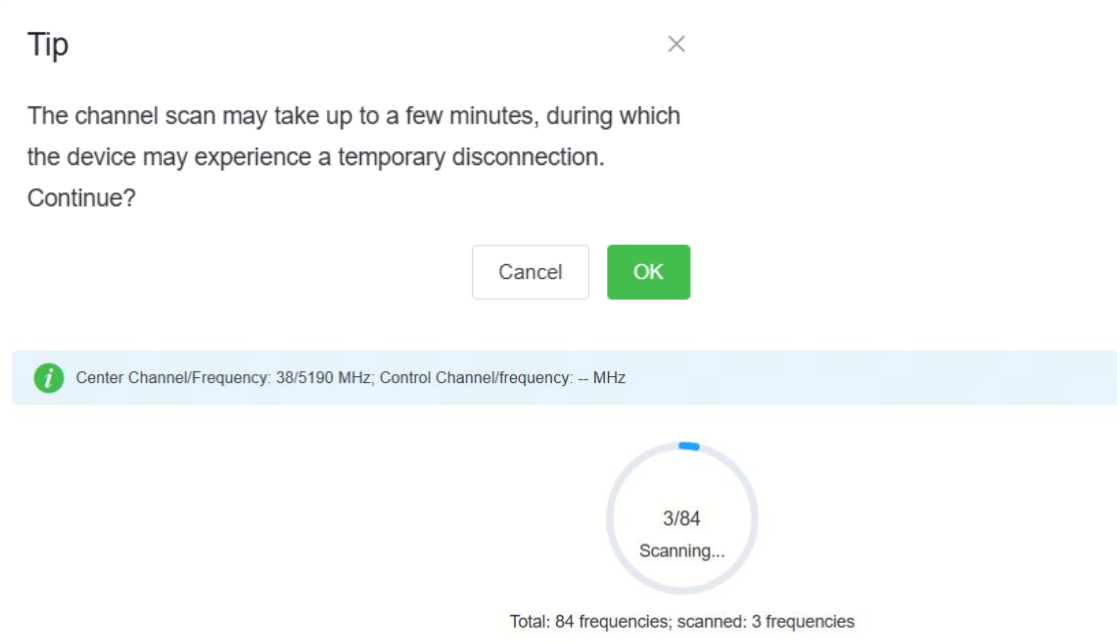
5.2.2 Configuration Steps

Choose **One-Device** > **Config** > **Tools** > **Spectrum Scan**.

(1) Click **Spectrum Scan**.



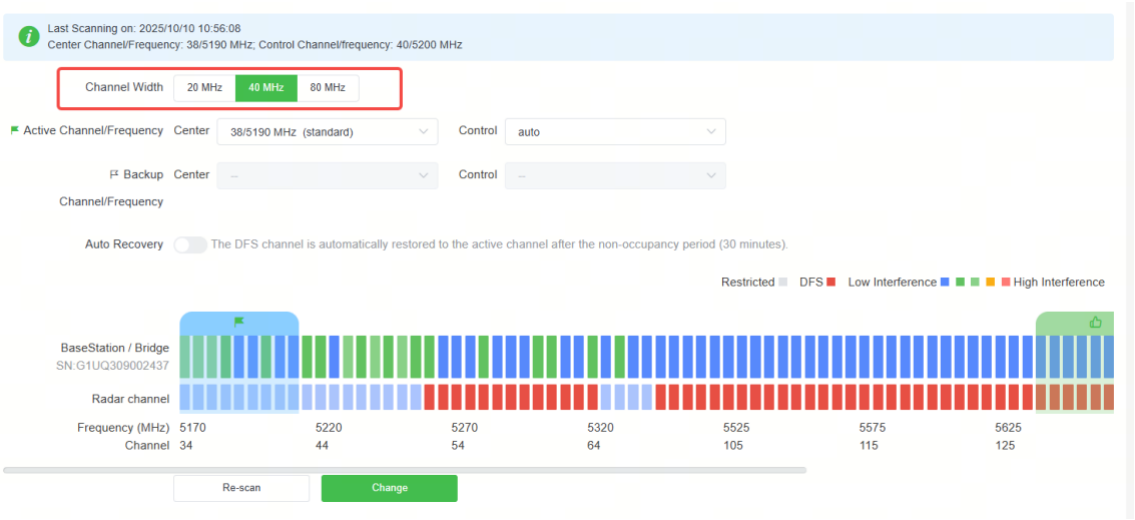
(2) Click **OK** on the pop-up window, and the device will begin scanning the surrounding channels.



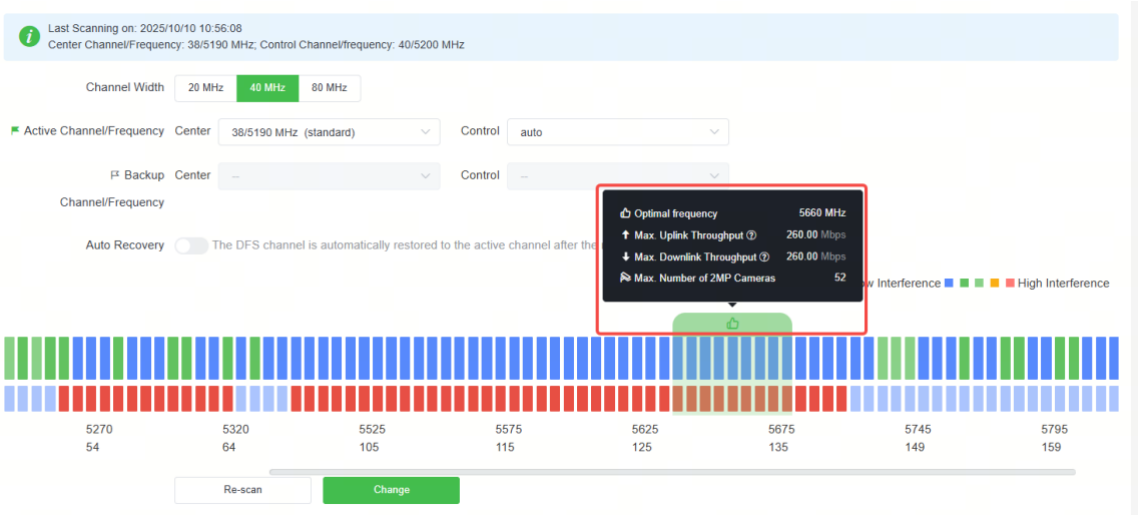
(3) After the scan is complete, you can click the **20 MHz**, **40 MHz**, or **80 MHz** tabs to view the frequency interference. The color gradient from left to right indicates the level of interference, ranging from low to high.

Specification

Only bridges supporting the 5 GHz band support the configuration of **Backup Channel/Frequency** and **Auto Recovery**.



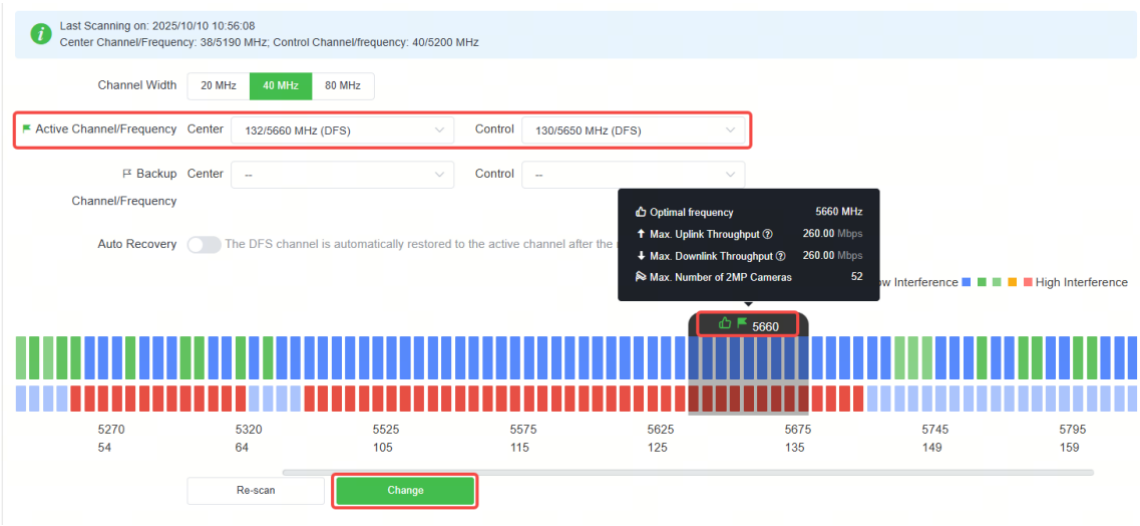
(4) Hovering the mouse over it will display detailed information about the current frequency, including throughput and estimated number of cameras that can be supported.



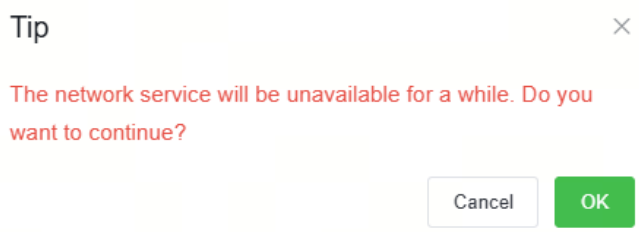
(5) Click the recommended optimal channels, select a control channel/frequency based on the recommendation, and then click **Change**.

Note

When the device's active channel is a DFS channel, **Backup Channel/Frequency** and **Auto Recovery** can be configured. For details, see 3.13.5Configuring a Backup DFS Channel.



(6) Click **OK** on the pop-up window to change the frequency.



5.3 Bridge Speed Test

Specification

- The speed test is only supported on paired bridges.
- Before the speed test, ensure that the peer device is online. Otherwise, speed test cannot be performed.

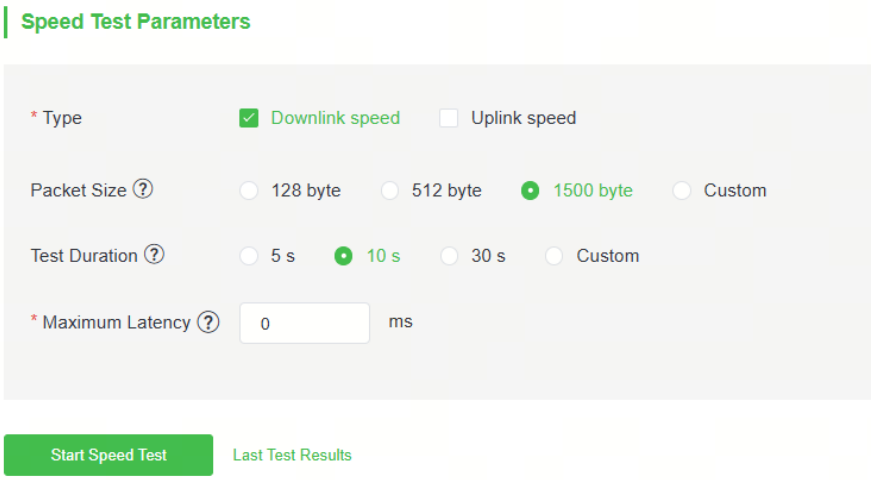
Note

The actual test rate may be affected by various factors and fall below the device's maximum rate. This is a normal phenomenon as long as it does not affect service performance.

Choose **One-Device** > **Config** > **Tools** > **Bridge Speed Test**.

(1) Select a test device and click **Change Device**. You can select the peer device that has been bridged.

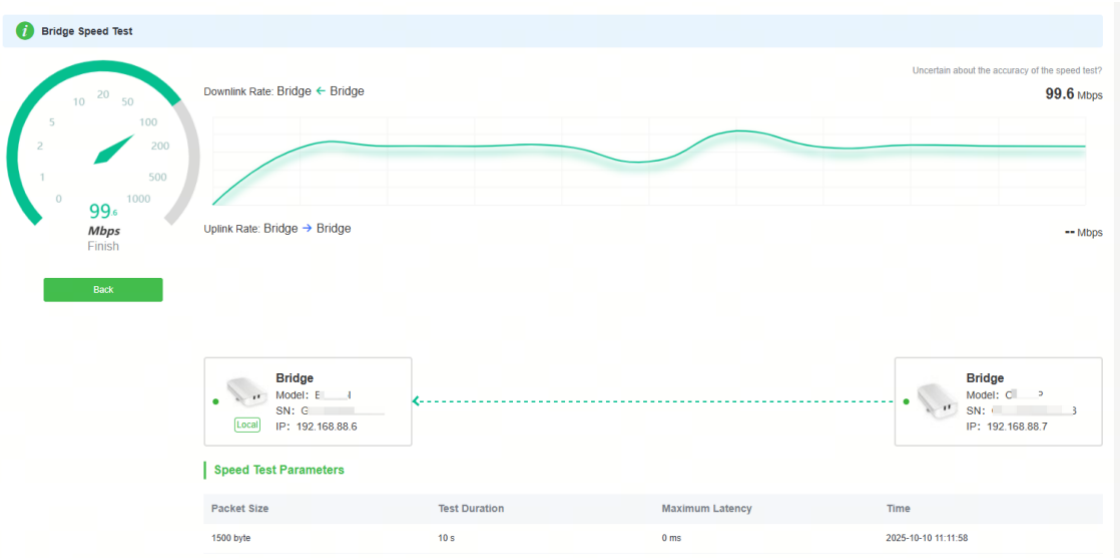
(2) Set speed test parameters.



- **Type**: Select the downlink or uplink rates for the test (multiple selections are supported):
  - **Downlink speed**: Data transmission rate from the peer device to the local device (indicated by the green arrow).
  - **Uplink speed**: Data transmission rate from the local device to the peer device (indicated by the blue arrow).
- **Packet Size**: Using smaller packets is more suited for evaluating network latency and connectivity, whereas larger packets help test bandwidth utilization and the capacity of network devices.
- **Test Duration**: A short duration reflects the peak rate, while a long duration reflects the stable rate.
- **Maximum Latency**: The maximum acceptable network latency during the speed test. A lower acceptable latency indicates a higher requirement for the network environment. The default value is 0 ms.

(3) Click **Start Speed Test**.

(4) After the speed test is complete, the test results will be displayed on the page. Click **Back** to return to the speed test page.



6 Fault Diagnosis

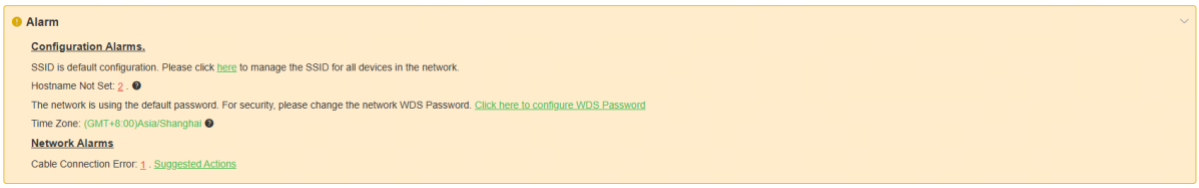
⚠ Caution

If the issue persists despite following the troubleshooting methods provided in this section, you may require remote support from a technician who will enable developer mode to resolve the issue. We will ensure your data is protected during this process.

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.

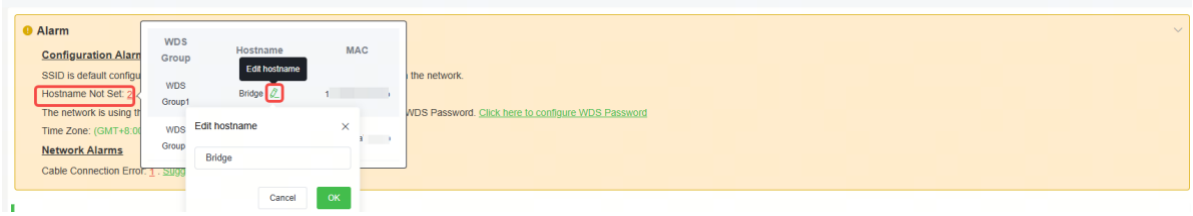
Choose **Network-Wide** > **WDS Groups** > **Alarm**.



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.

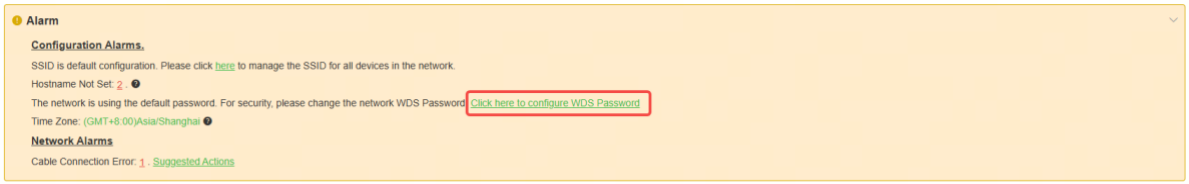
When viewing the alarm, hover the cursor over the orange number of the prompt and click  in the displayed dialog box to modify the name of each device. (The orange number, 2 in the figure, indicates the number of devices that still use the default name in the network.) Enter the new device name and click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



6.1.2 Default 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.



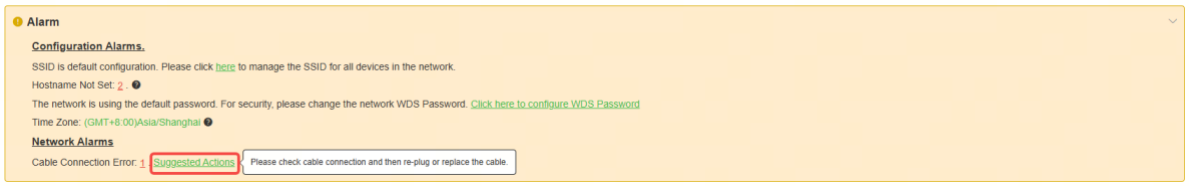
⚠ Caution

- 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.

6.1.3 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.



6.1.4 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 frequency with smaller interference.

If not, increase the channel width. For frequency settings, see 3.13.3Configuring the Channel Width

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

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

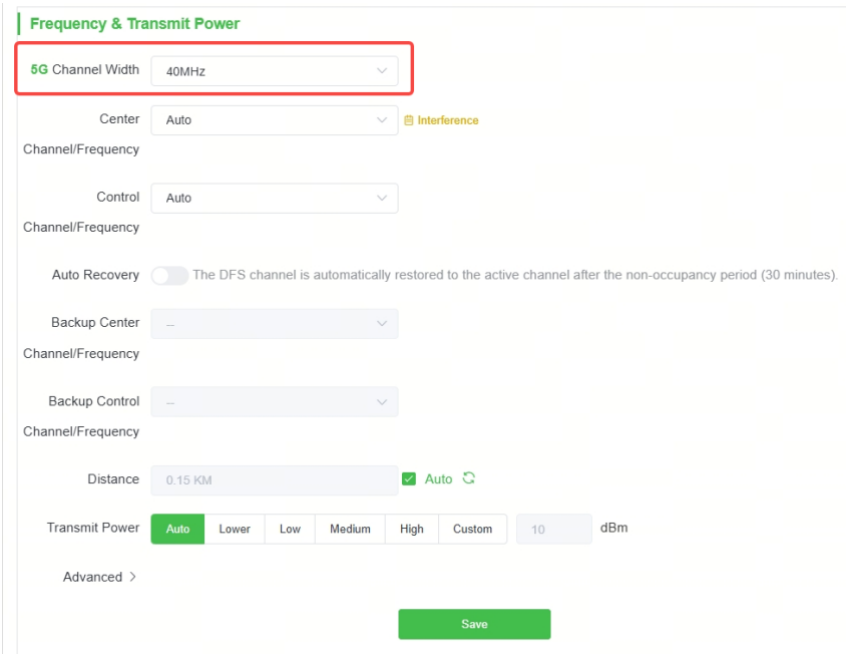
The 5 GHz bridge supports 20 MHz, 40 MHz, and 80 MHz, while the 2.4 GHz bridge supports 20 MHz and 40 MHz.

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.

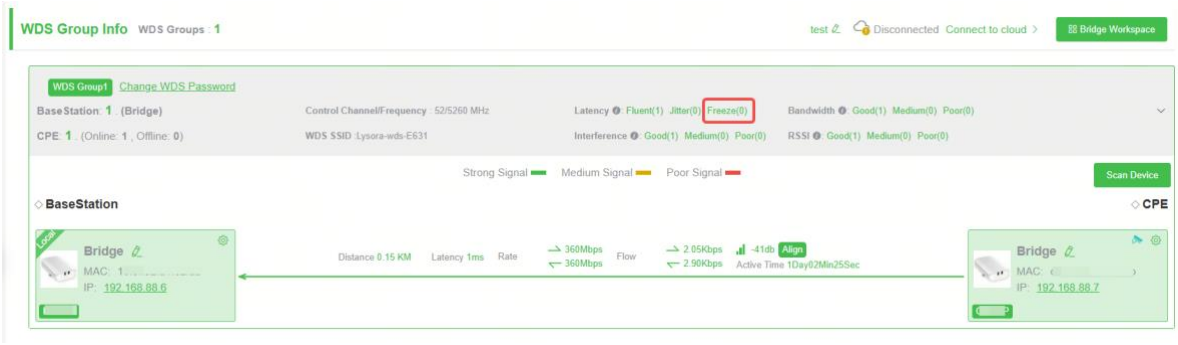


Configuring Channels and Frequencies. For channel width settings, see 3.13.3Configuring the Channel Width.

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 **WDS Group Info** page, check whether **Latency** is **Freeze**. If so, the latency is too high. Otherwise, the latency is normal.

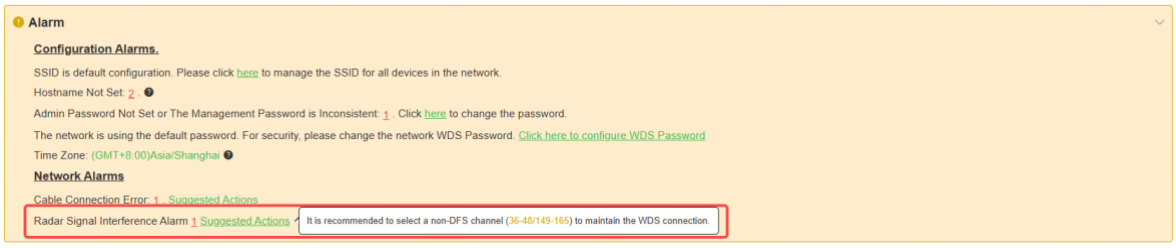


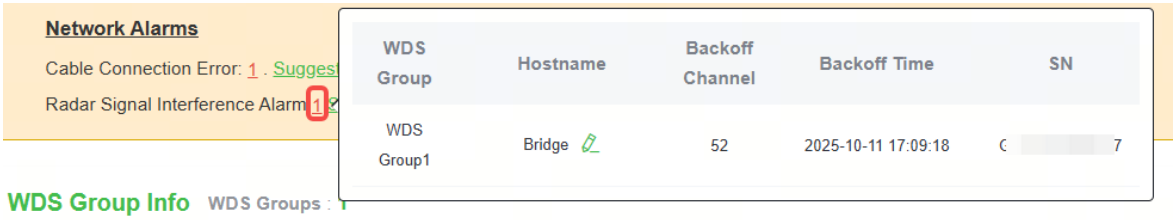
⚠ Caution

Frequency 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 frequency and channel width.

6.1.5 Radar Signal Interference

When the device detects a radar signal in a channel, it generates an alarm. 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 frequency in the WDS group (group 2 in the example) is consistent with that of back-off channels. (See 3.4Displaying WDS Group Information.) If so, manually switch the frequency to a non-dynamic frequency selection (DFS) channel. For details, see 3.13.3Configuring the Channel Width

Choose **One-Device** > **Config** > **Wireless** > **Frequency & Transmit Power**.

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

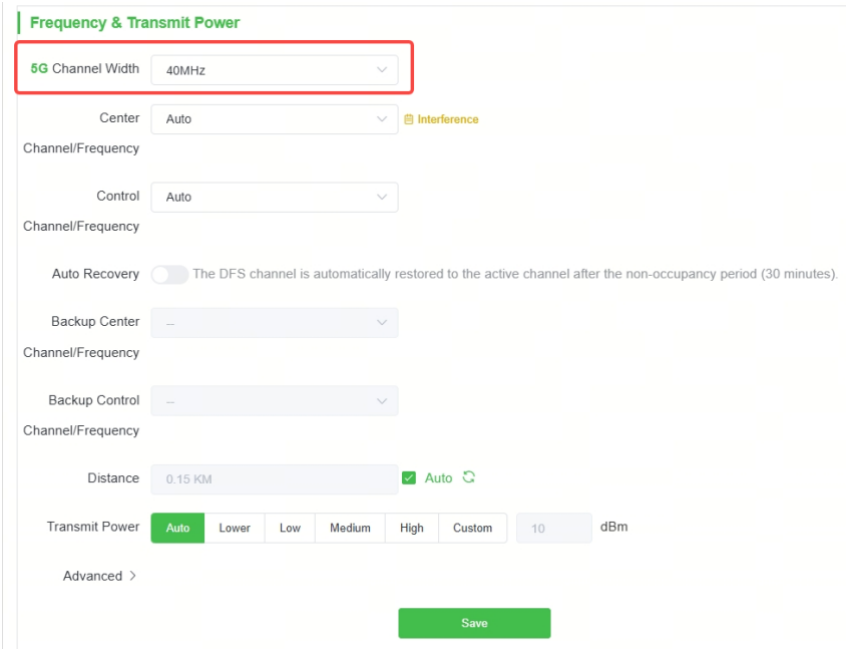
The 5 GHz bridge supports 20 MHz, 40 MHz, and 80 MHz, while the 2.4 GHz bridge supports 20 MHz and 40 MHz.

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.

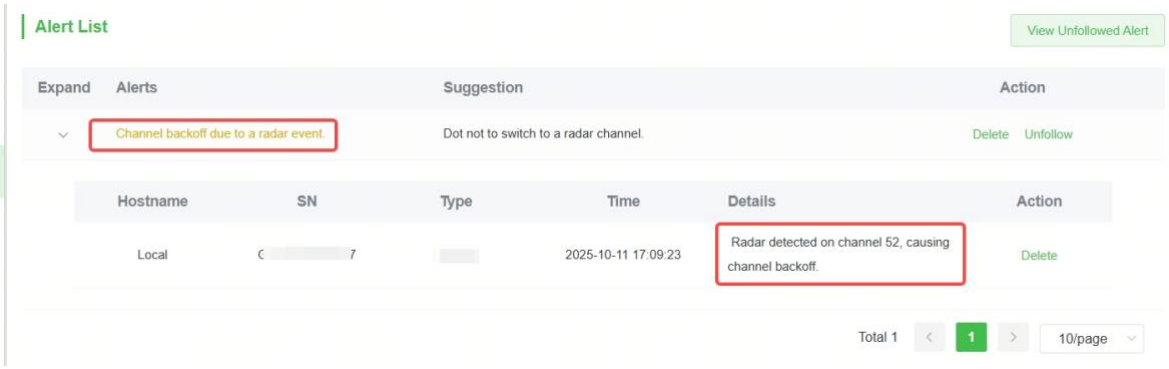


Configuring Channels and Frequencies.

Note

- Non-DFS channels include channels 36–48 and 149–165, corresponding to 5180 MHz to 5260 MHz and 5745 MHz to 5825 MHz.
- This feature is supported only on bridges operating in the 5 GHz band. When a radar signal is detected, an alarm is triggered and the operating frequency is automatically switched.

Alarms are displayed in **Alert Center** when radar signals are detected. If the devices are managed by Lysora Cloud and connected to the network, the alarm information will be synchronized to Lysora Cloud.



6.1.6 CPE Disconnection Alarm

Specification

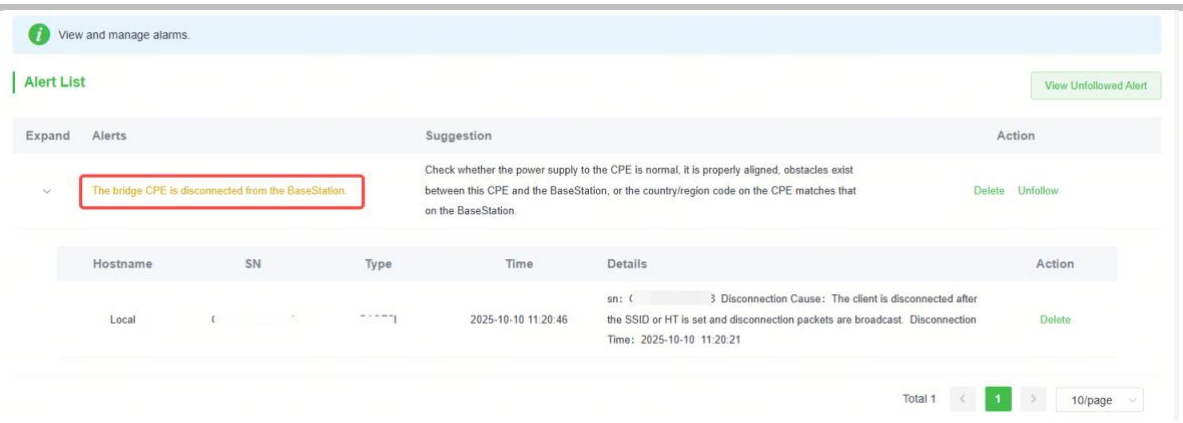
CPE disconnection alarms are available only on specified BaseStations, including the CPE5.

Go to the configuration page:

- Method 1: Click **Alert Center** in the top navigation bar.

- Method 2: Choose **One-Device** > **Config** > **Tools** > **Alarms**.

When a CPE in a bridge group is disconnected, you can view the CPE disconnection alarm on the BaseStation, including the disconnection time and reason.



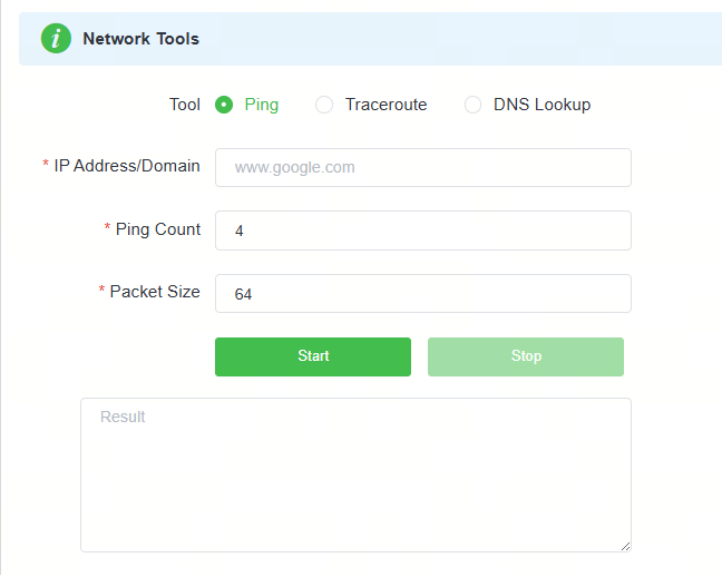
6.2 Network Test Tool

Choose **One-Device** > **Config** > **Tools** > **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.

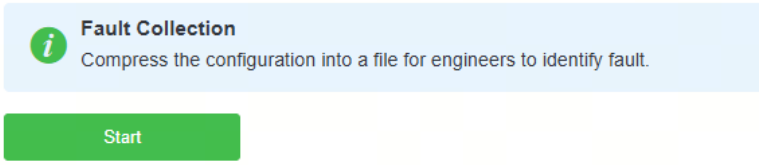
The DNS Lookup tool displays the DNS server address used to resolve a URL.



6.3 Collecting Fault Info

Choose **One-Device** > **Config** > **Tools** > **Fault Collection**.

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


Fault Collection
Compress the configuration into a file for engineers to identify fault.

Start

7 Network Settings

7.1 Network Modes

7.1.1 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.

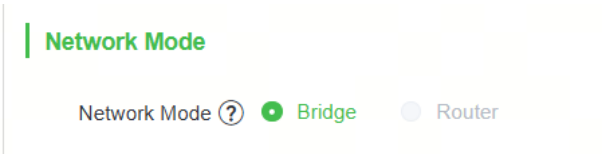
⚠ Caution

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 10.100.111.254 to configure the device in router mode. Router mode is supported only when the bridge acts as a CPE.

7.1.2 Configuration Steps

Choose **One-Device** > **Config** > **Network** > **Network Mode**.

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



7.2 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 management interface, and does not affect the service network.

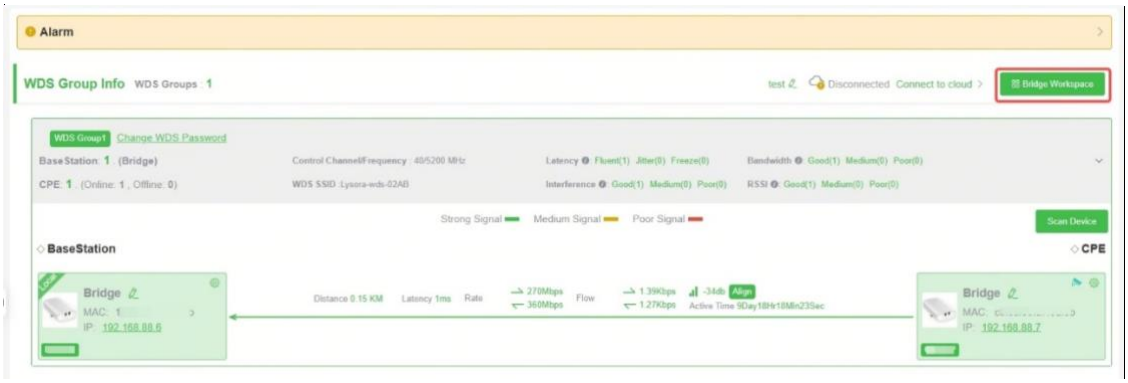
7.2.1 Allocating IPv4 Addresses to Bridges on the Network

1. Static IP Address

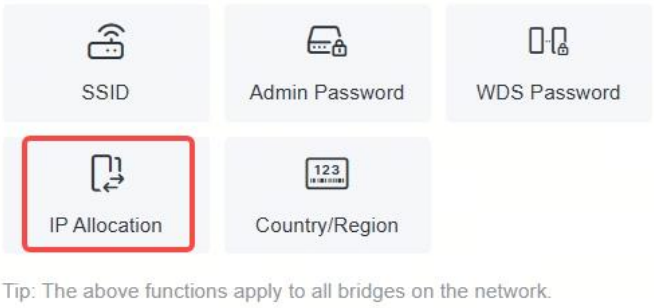
Choose **Network-Wide** > **WDS Groups**.

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.

(1) Click **Bridge Workspace**.

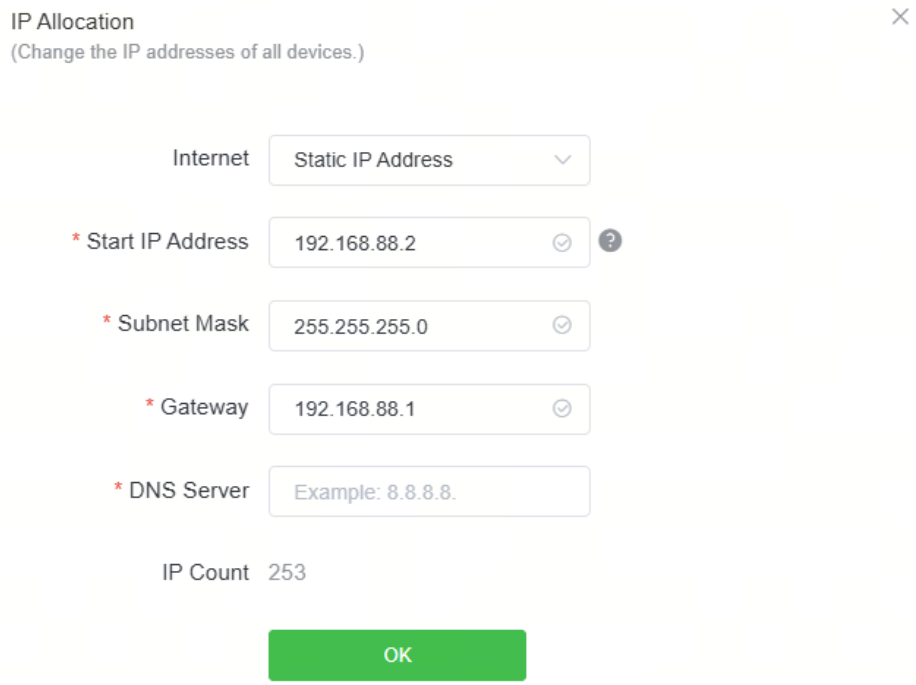


(2) Click **IP Allocation**.



(3) 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 management interface. In this case, you need to enter the new IP address in the browser's address bar for login. Ensure that the IP

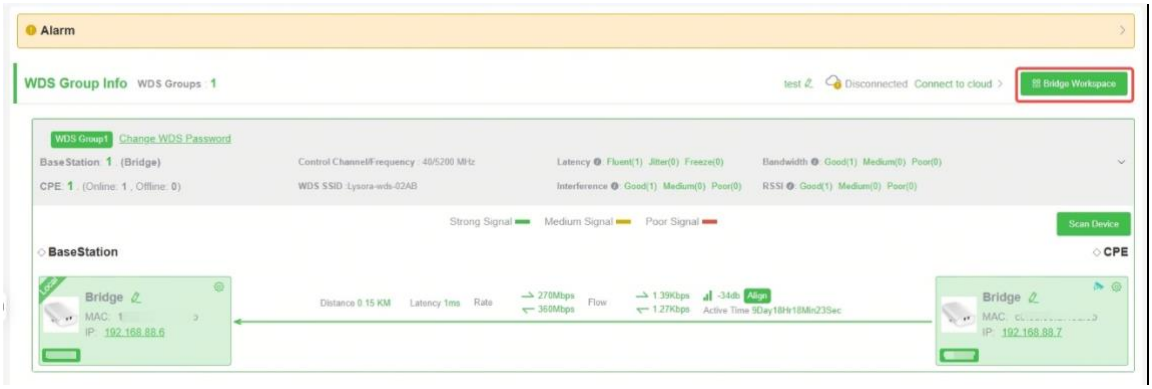
addresses of the management PC and the device are on the same network segment. If they are not on the same network segment, change the management PC's IP address. For details, see 2.3.2Configuring the IP Address of the Management PC. Therefore, exercise caution when performing this operation.

2. DHCP

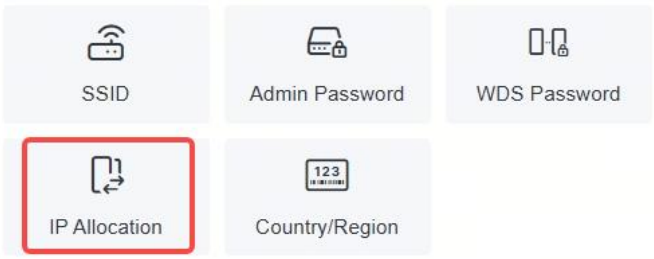
Choose **Network-Wide** > **WDS Groups**.

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.

(1) Click **Bridge Workspace**.

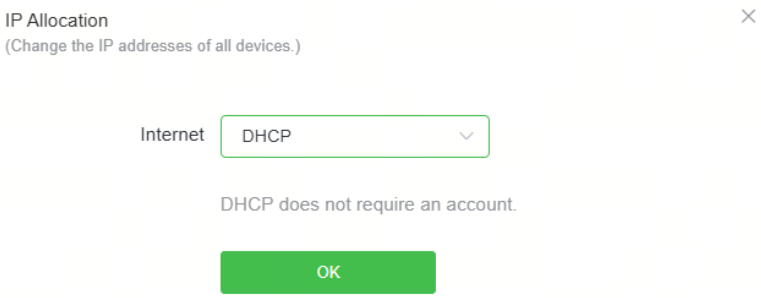


(2) Click **IP Allocation**.



Tip: The above functions apply to all bridges on the network.

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

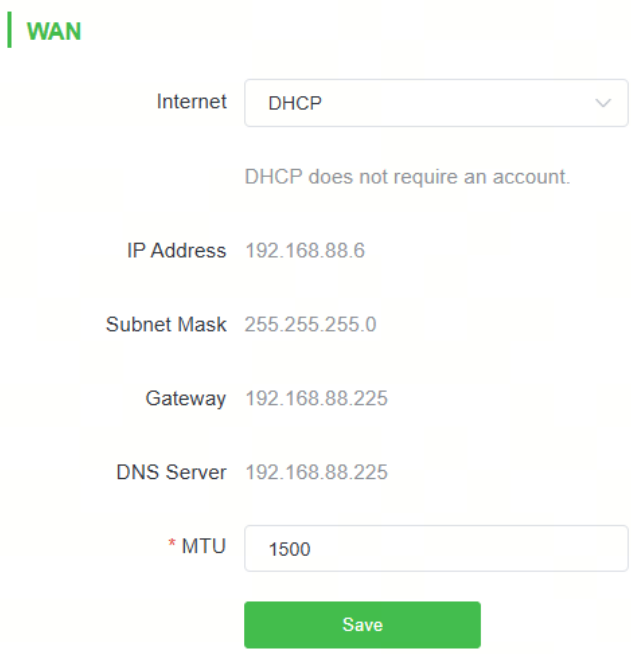


7.2.2 Configuring an IP Address for the WAN Port

Choose **One-Device** > **Config** > **Network** > **WAN**.

(1) 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.

(2) Click **Save**.



⚠ Caution

After the IP address and subnet mask are changed, you may fail to access the device's web management 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

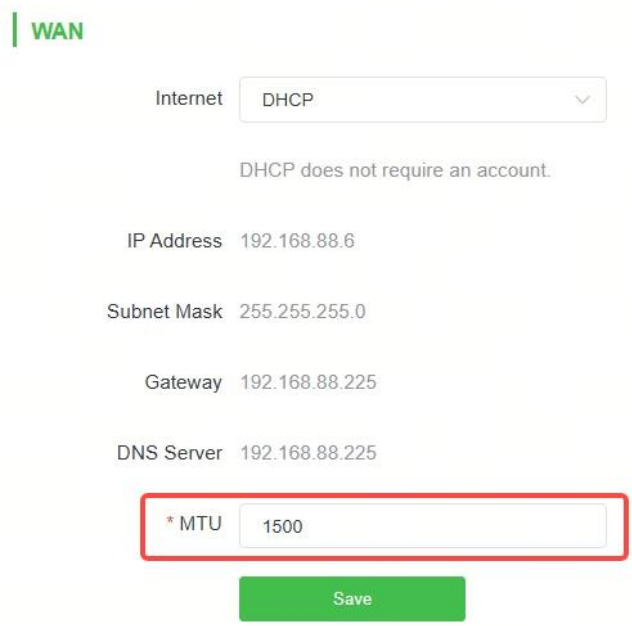
and the device are on the same network segment. If they are not on the same network segment, change the management PC's IP address. For details, see 2.3.2Configuring the IP Address of the Management PC. Therefore, exercise caution when performing this operation.

7.3 Modifying 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.

Choose **One-Device** > **Config** > **Network** > **WAN**.

Enter the MTU value, and click **Save**.



7.4 Changing the IP Address of a LAN Port

Specification

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

Choose **One-Device** > **Config** > **Network** > **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 management interface of the device for configuration and management.

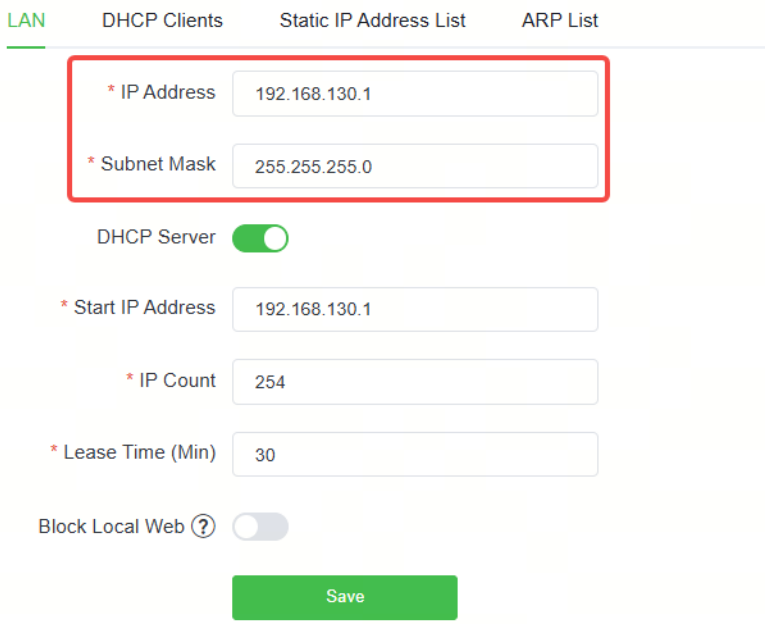


Table 7-1 LAN Configuration Parameters

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 7.5Configuring 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

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

7.5 Configuring the DHCP Server

Specification

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

7.5.1 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.

7.5.2 Configuring the DHCP Server

Choose **One-Device** > **Config** > **Network** > **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.

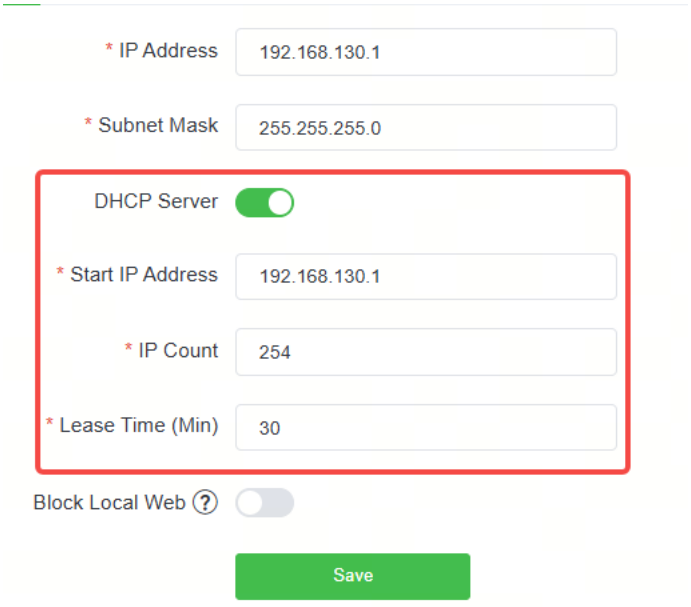
⚠ Caution

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.

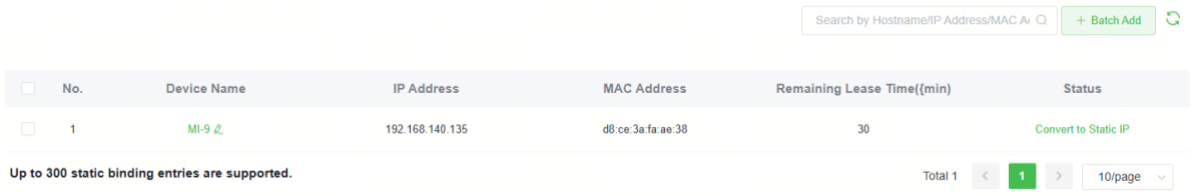
Lease Time (Min): Lease time of IP addresses. When a client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease time expires. After the client connection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



7.5.3 Viewing the DHCP Client

Choose **One-Device** > **Config** > **Network** > **LAN** > **DHCP Clients**.

View the client addresses automatically allocated by thorough DHCP. Find the target client and click **Convert to Static IP** in the **Status** column, or select desired clients and click **Batch Add**. The dynamic address allocation relationship is added to the static address allocation list, so that the host can obtain the bound IP address for each connection. For details on how to view the static address allocation list, see Section 7.5.4Configuring Static IP Addresses.

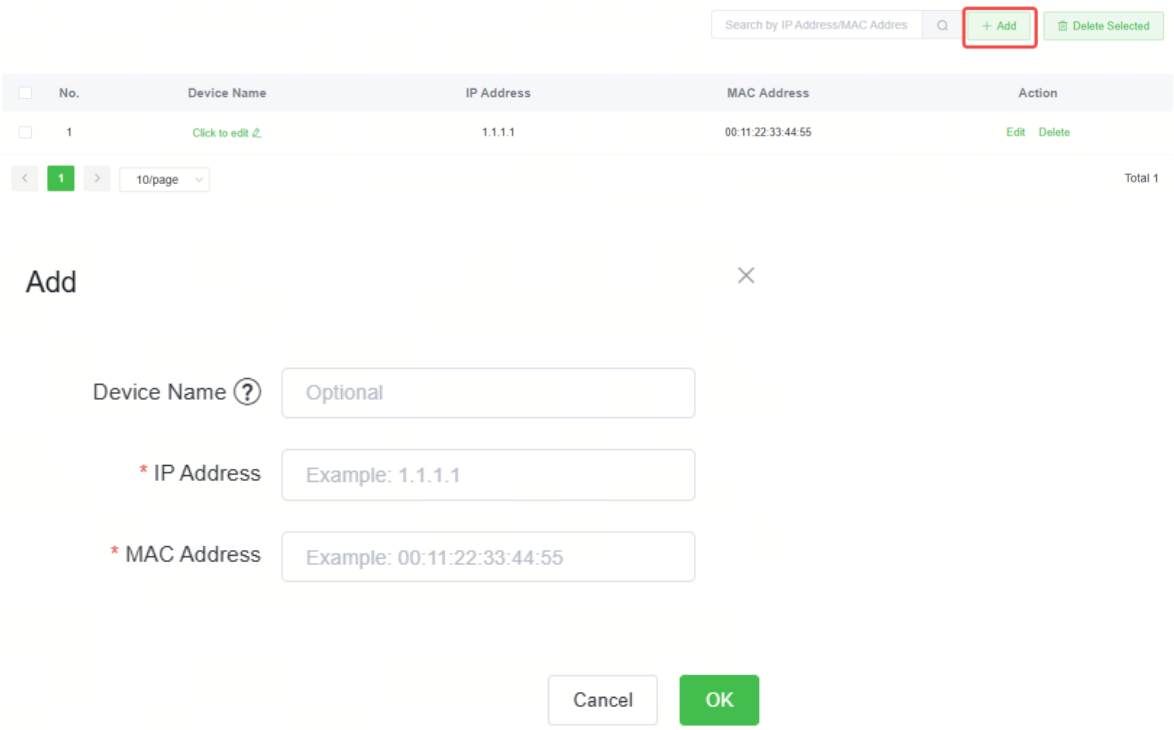


7.5.4 Configuring Static IP Addresses

Choose **One-Device** > **Config** > **Network** > **LAN** > **Static IP Addresses**.

The page displays all configured static IP addresses.

Click **Add**. In the pop-up window, enter the device name, MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the client connects to the network.



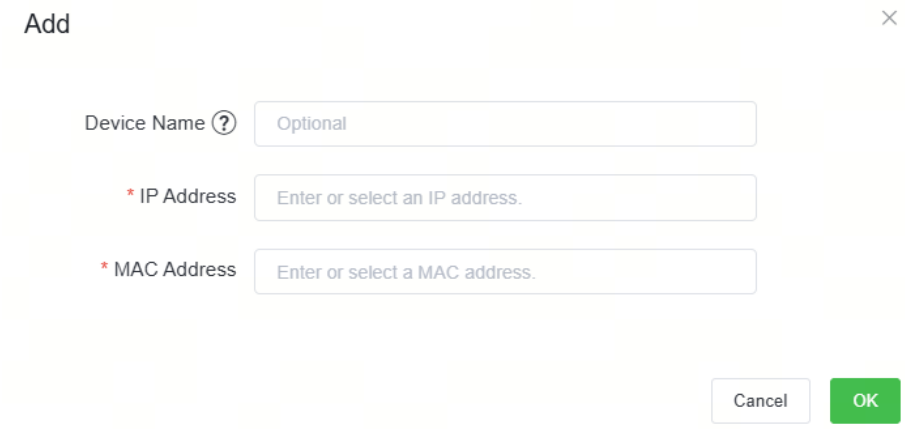
7.5.5 Configuring ARP Binding

Choose **One-Device** > **Config** > **Network** > **LAN** > **ARP List**.

The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. You can enable ARP guard and configure IP-MAC binding to restrict Internet access of LAN hosts and improve network security.

(1) Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them.

(2) Click **Add**, enter the device name, IP address and MAC address to be bound, and click **OK**. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the address mapping.



To remove the binding between a static IP address and a MAC address, click **Delete** in the **Action** column.

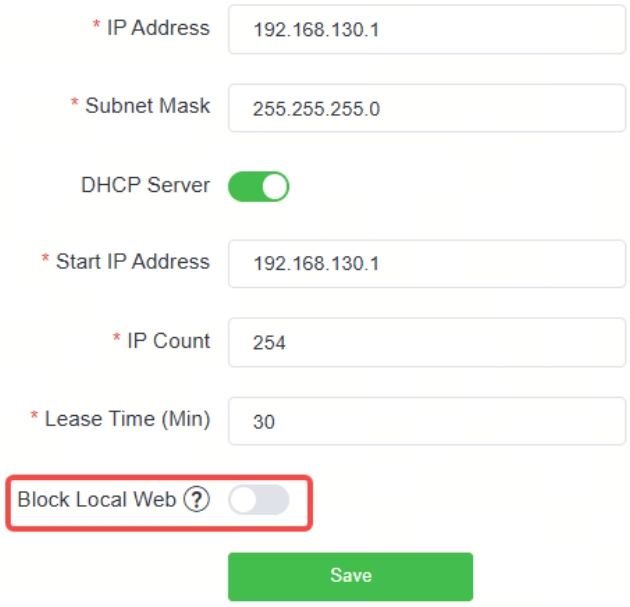
7.6 Blocking Web Access

Specification

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

Choose **One-Device** > **Config** > **Network** > **LAN**.

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

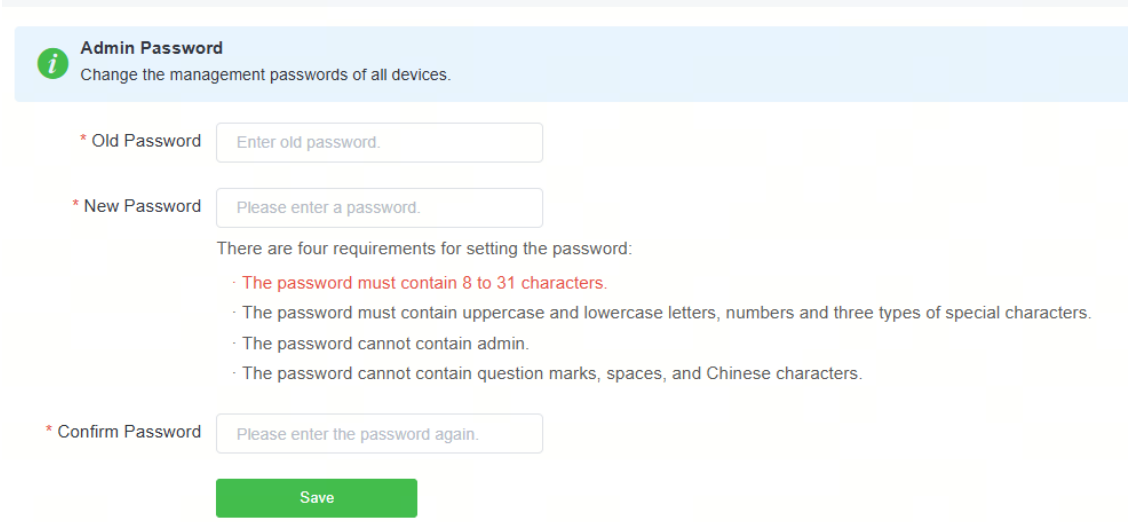


8 System Settings

8.1 Configuring Management Password

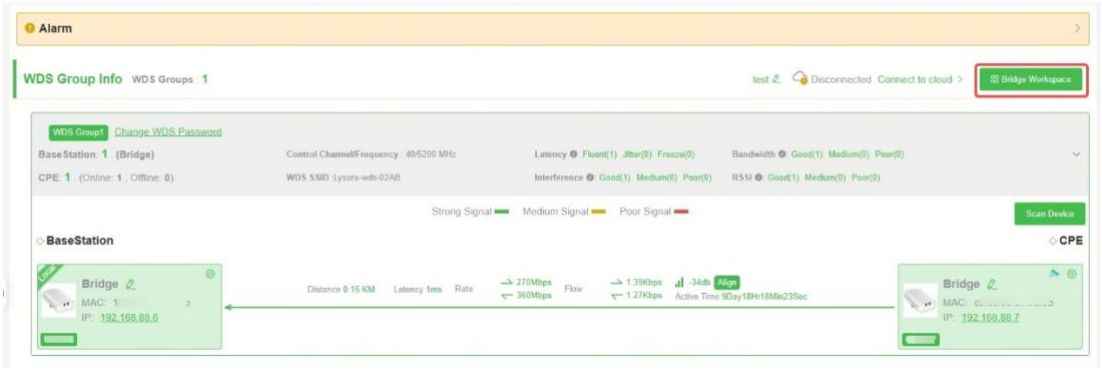
Go to the configuration page:

- Method 1: Choose **Network-Wide** > **System** > **Password**.

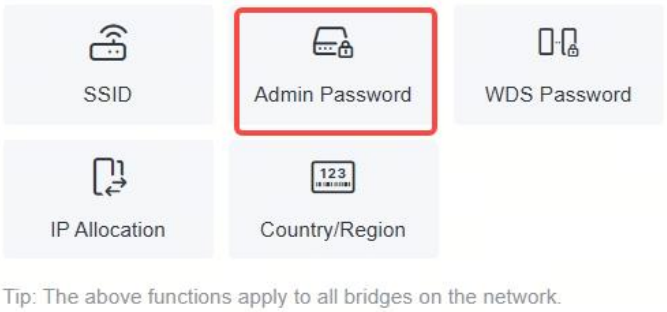


- Method 2: Choose **Network-Wide** > **WDS Groups**.

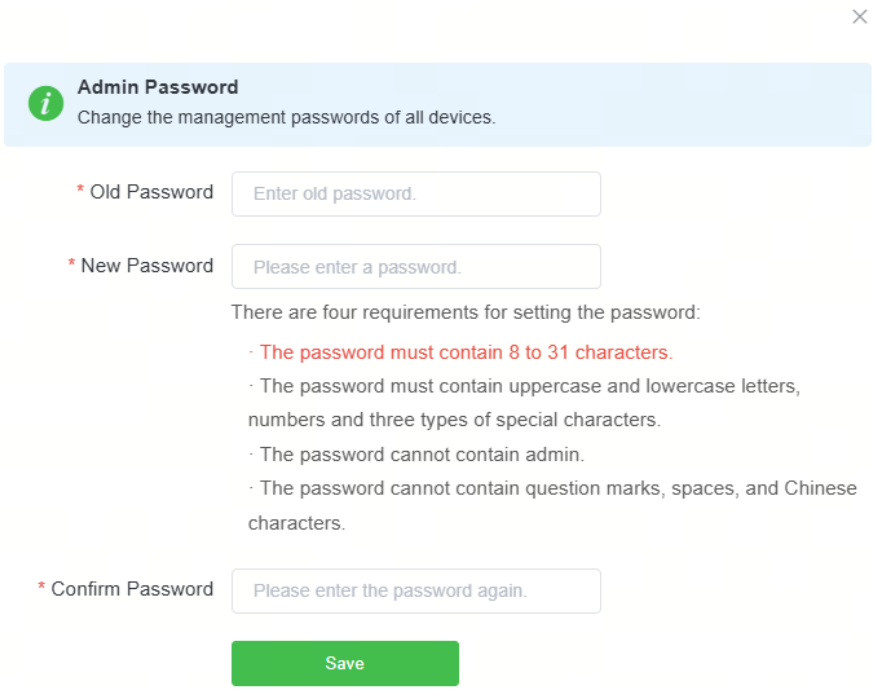
(1) Click **Bridge Workspace**.



(2) 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.



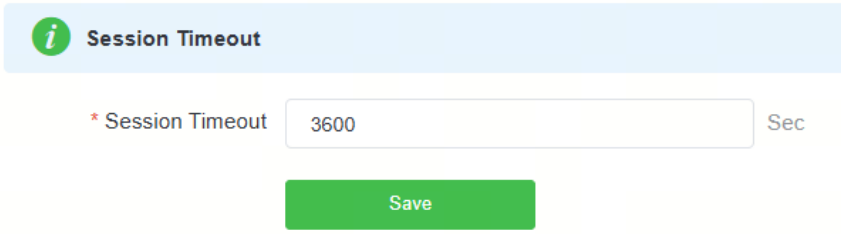
⚠ Caution

- This password is used to log in to web management interface 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.

8.2 Configuring Session Timeout Duration

Choose **One-Device** > **Config** > **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.

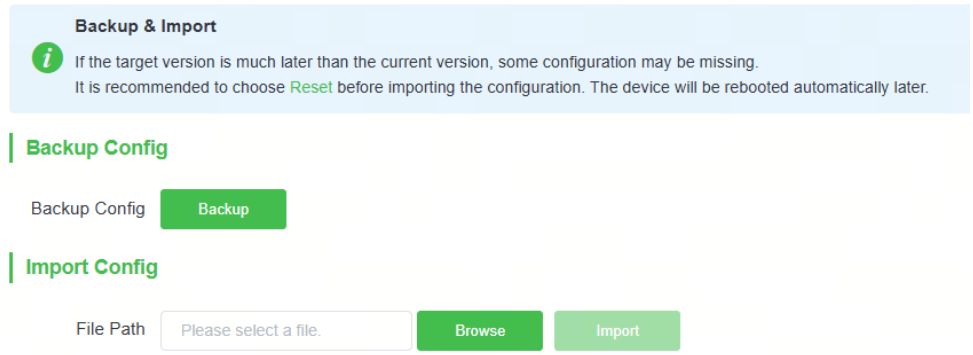


8.3 Configuring Config Backup and Import

Choose **One-Device** > **Config** > **System** > **Management** > **Backup & Import**.

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

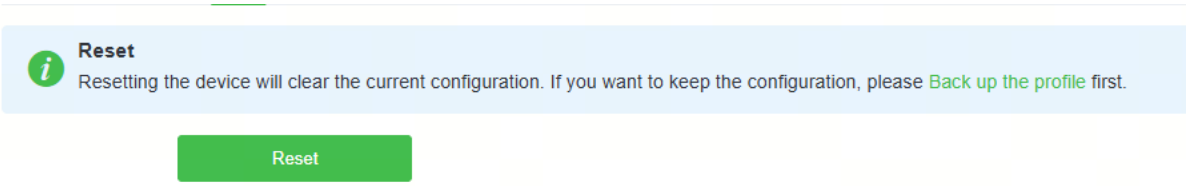
Configure import: Click **Browse**, select a configuration file backup on the local PC, and click **Import** to import the configuration file. The device will restart.



8.4 Resetting Factory Settings

Choose **One-Device** > **Config** > **System** > **Management** > **Reset**

Click **Reset** to restore factory settings.



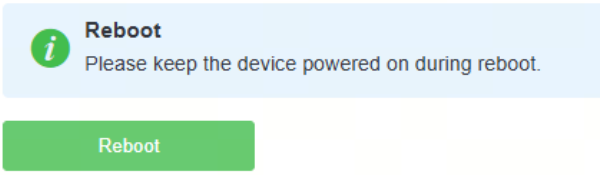
⚠ Caution

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.

8.5 Rebooting the Device

Choose **One-Device** > **Config** > **System** > **Reboot**.

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



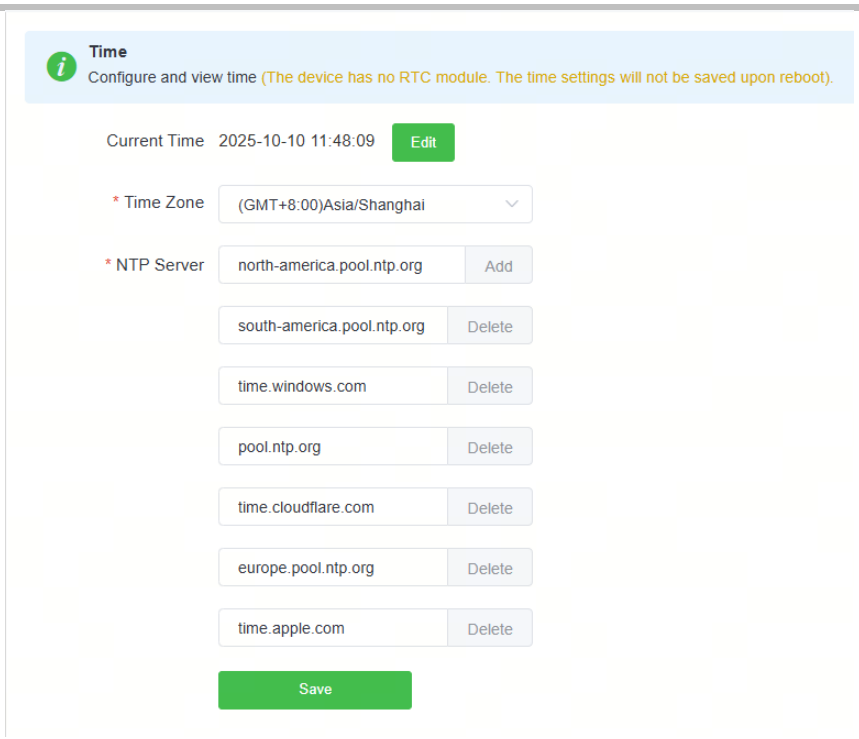
⚠ Caution

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

8.6 Configuring System Time

Choose **Network-Wide > 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.



8.7 Performing Update and Displaying the System Version

8.7.1 Online Update

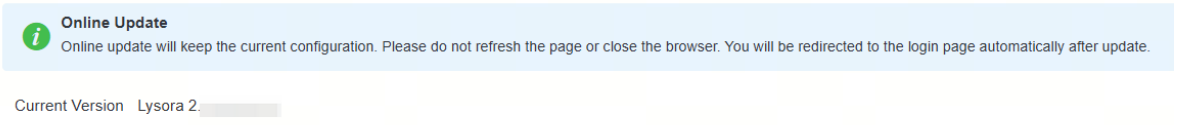
Choose **One-Device** > **Config** > **System** > **Update** > **Online Update**.

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.

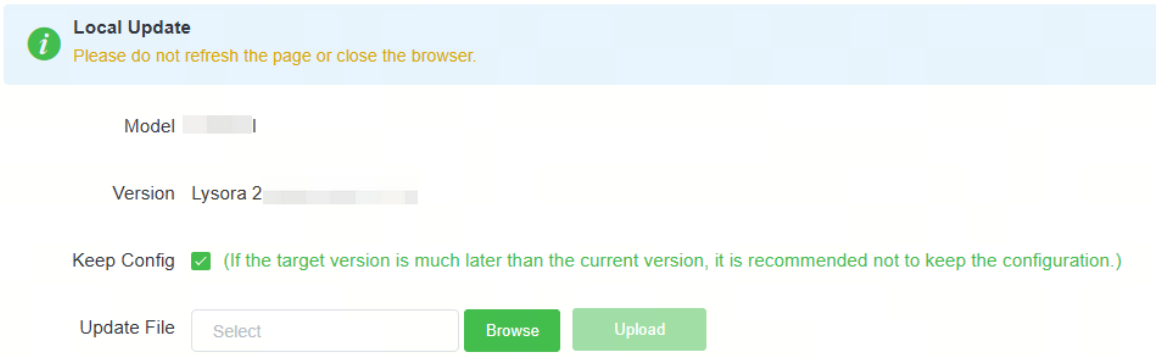
If no version update is detected or online update cannot be performed, check whether the bridge is connected to the Internet.



8.7.2 Local Update

Choose **One-Device** > **Config** > **System** > **Update** > **Local Update**.

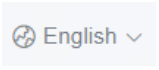
You can view the current software version, hardware version and device model. If you want to update the device with the configuration retained, check **Keep Config**. Click **Browse**, select an update package on the local PC, and click **Upload** to upload the file. The device will be updated.



Caution

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

8.8 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.

8.9 Configuring SNMP

Specification

SNMP is supported on CPE5 only.

8.9.1 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 device management through the SNMP configuration interface and monitor and control devices through the third-party software.

8.9.2 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.

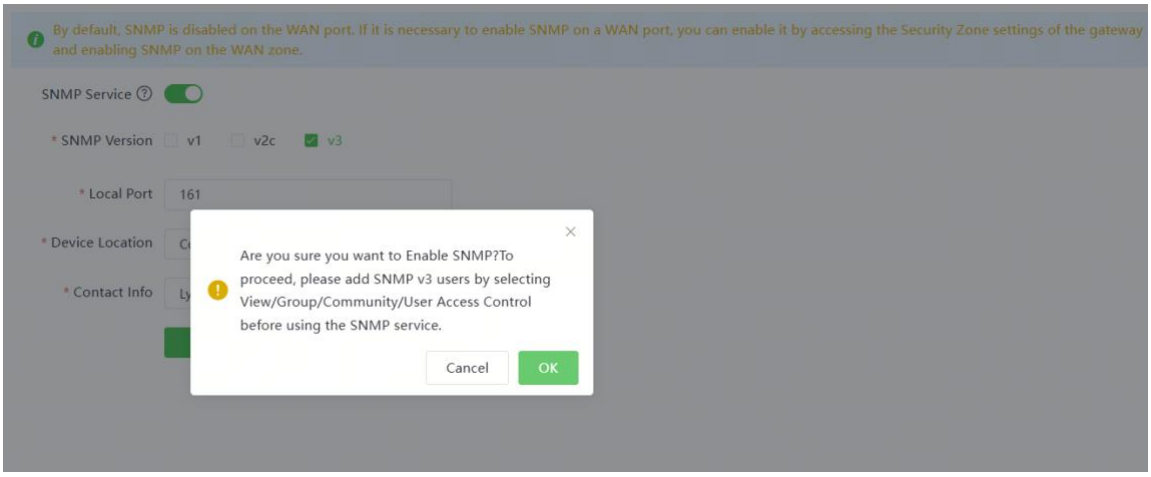
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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

Choose **Network-Wide** > **System** > **SNMP** > **Global Config**

(1) Enable the **SNMP service**.



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

(2) Click **OK** in the pop-up window.

(3) Set SNMP service global configuration parameters.

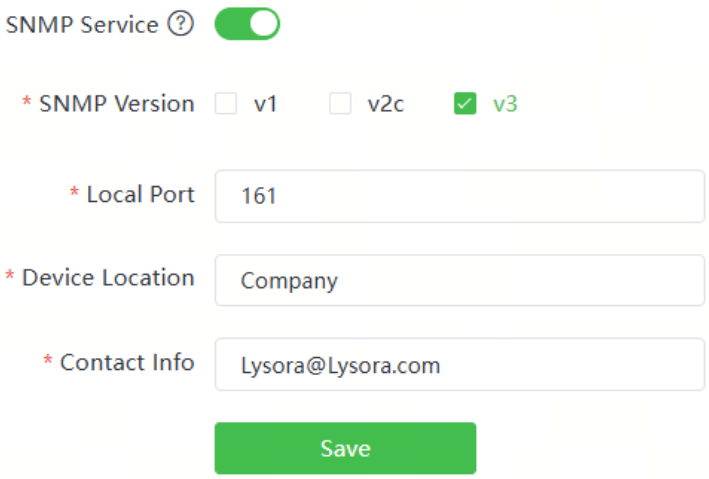


Table 8-1 Global Configuration Parameters

Parameter	Description
SNMP Server	Indicates whether SNMP service is enabled.
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.

Parameter	Description
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.

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

8.9.3 View, Group, Community, Client 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**

Choose **Network-Wide** > **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.

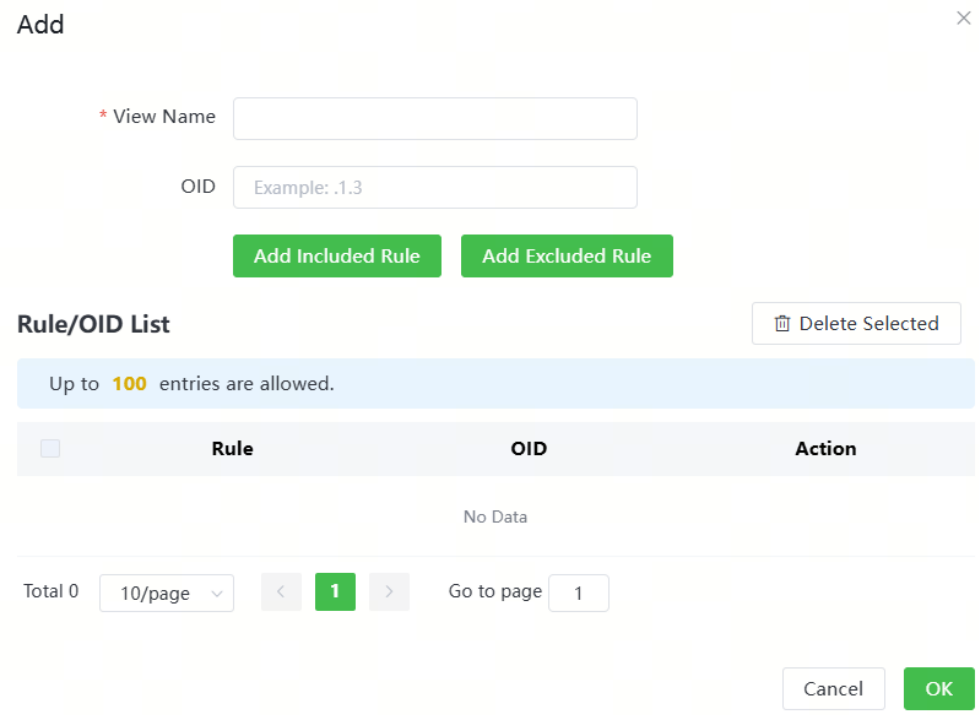


Table 8-2 View Configuration Parameters

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.
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

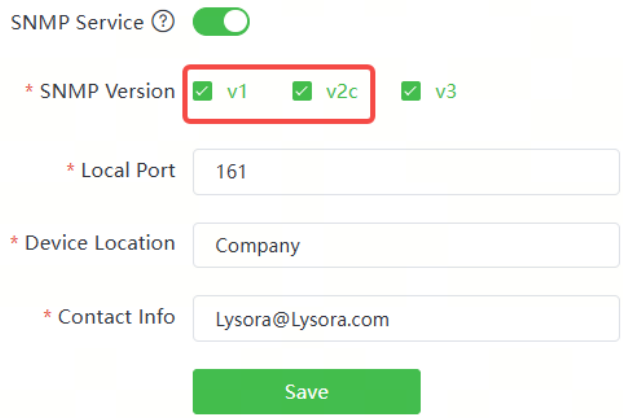
A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1 and v2c Users

- Overview

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



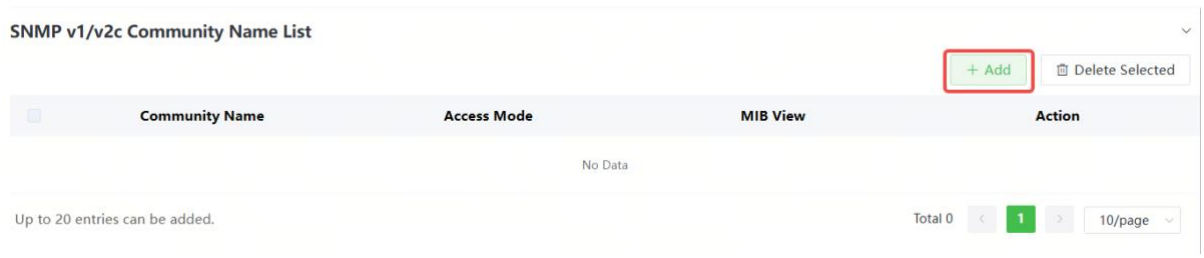
Note

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

Choose **Network-Wide** > **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.

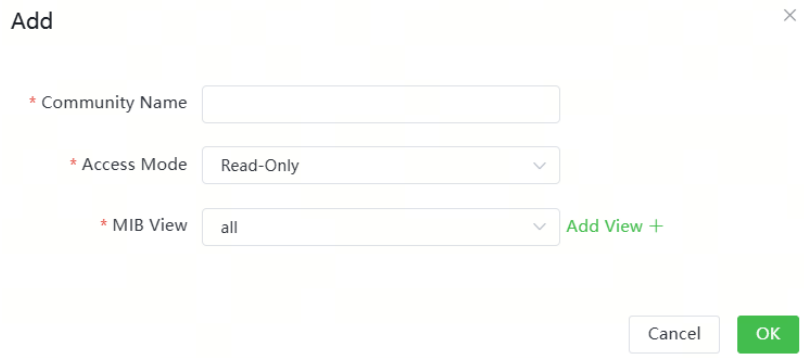


Table 8-3 v1/v2c User Configuration Parameters

Parameter	Description
Community Name	● 8-32 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.

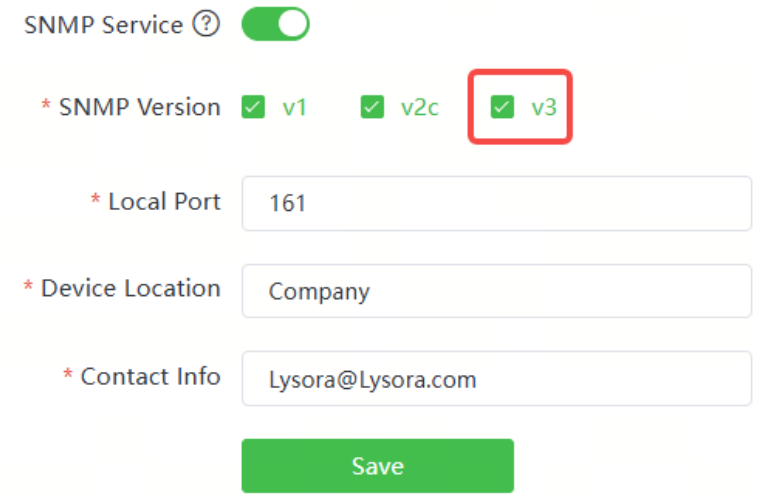
3. Configuring v3 Groups

- 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

Choose **Network-Wide** > **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.

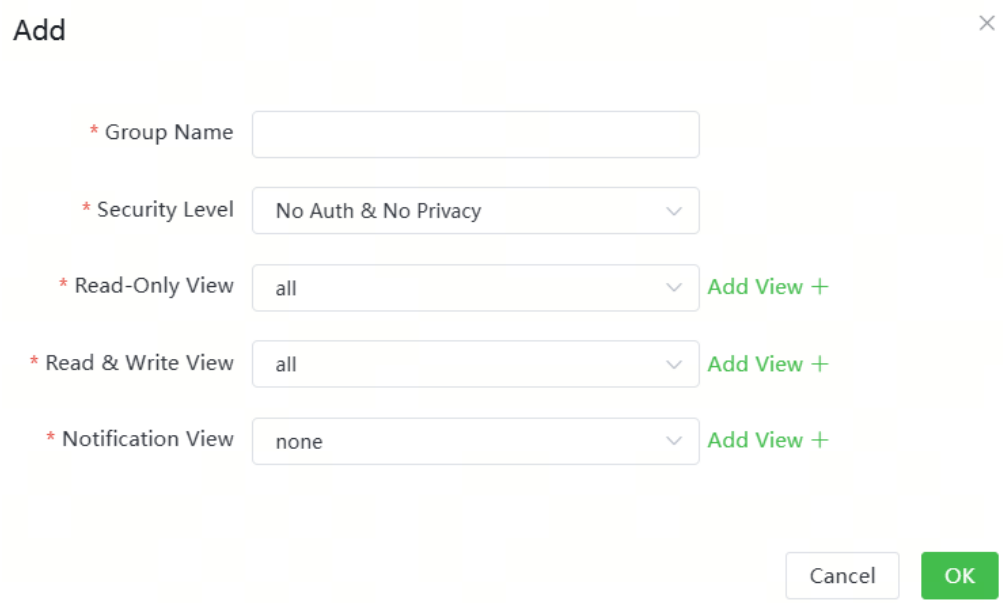


Table 8-4 v3 Group Configuration Parameters

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

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

Note

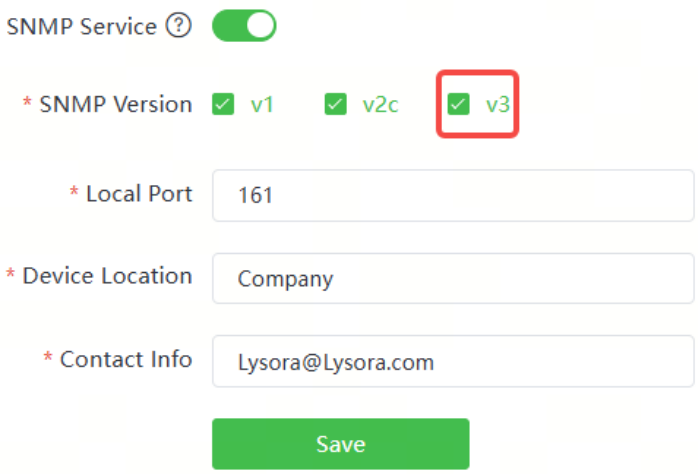
- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

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



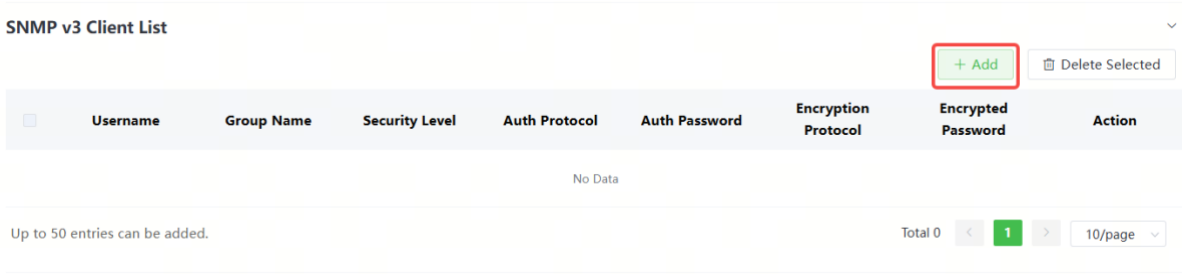
Note

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

Choose **Network-Wide** > **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.

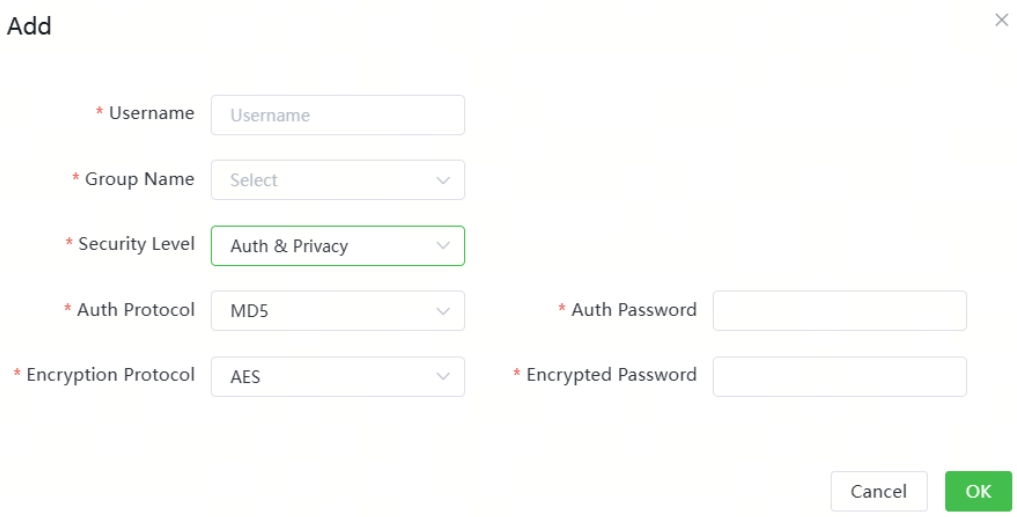


Table 8-5 v3 User Configuration Parameters

Parameter	Description
Username	Username ● 8-32 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.

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

8.9.4 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

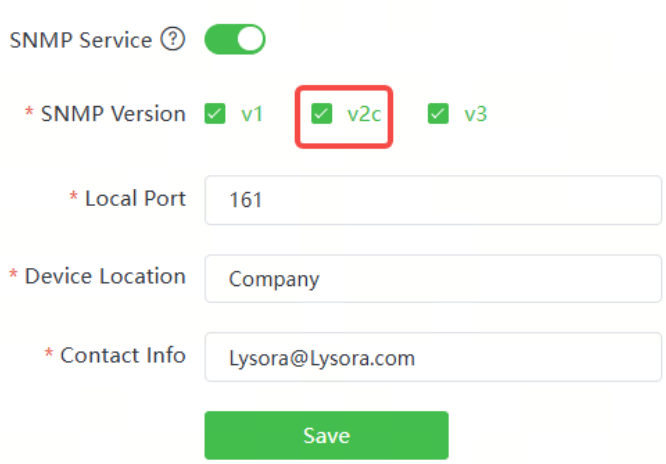
According to the user's application scenario, the requirements are shown in the following table:

Table 8-6 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.
Read & write permission	Read-only permission.

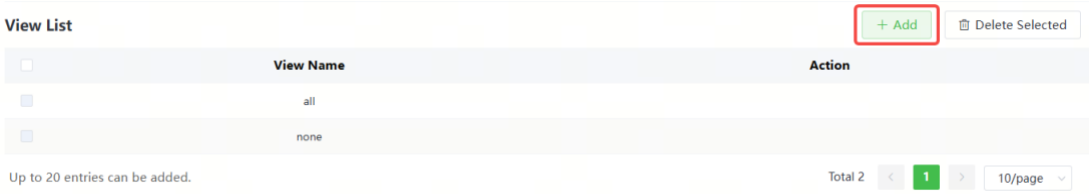
- Configuration Steps

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

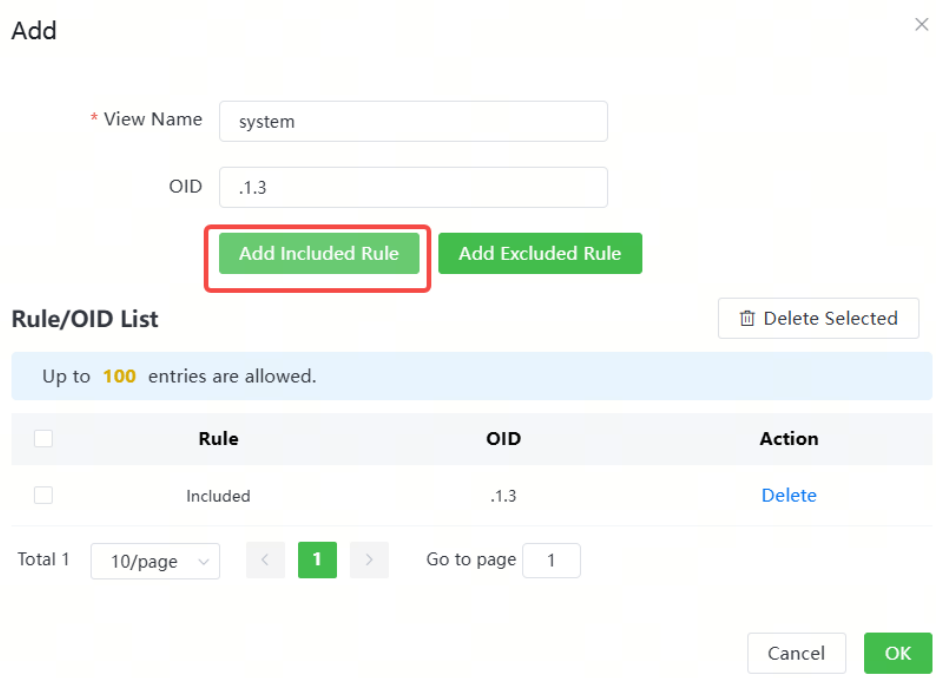


(2) Add a view on the View/Group/Community/Client Access Control interface.

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



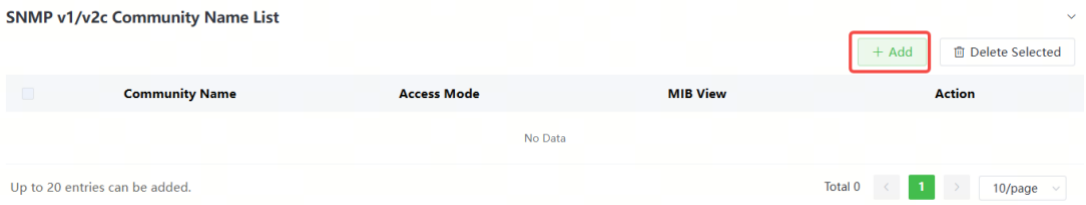
b. Enter the view name and OID in the pop-up window, and click **Add Included Rule**.



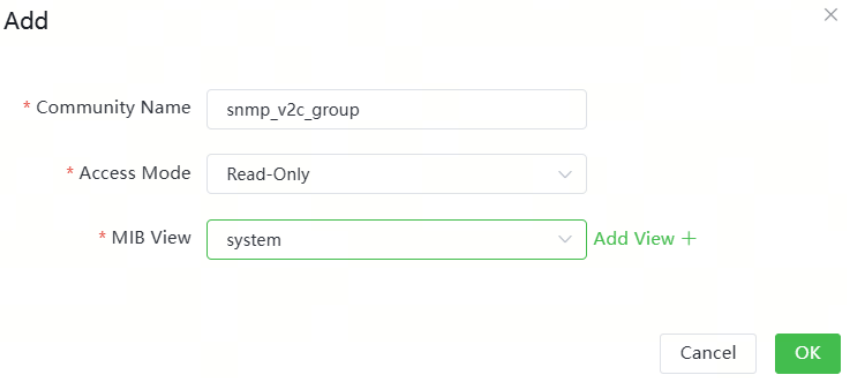
c. Click **OK**.

(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:

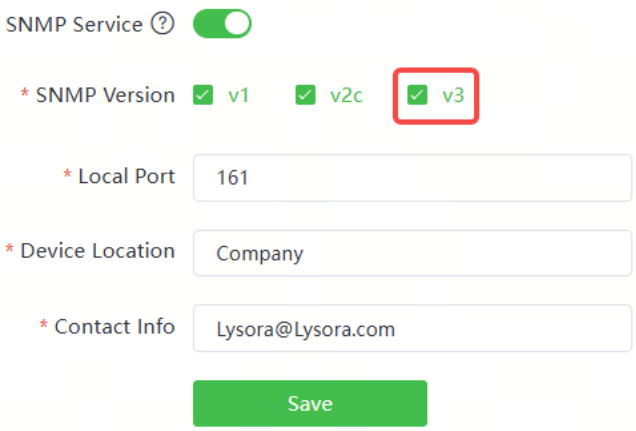
Table 8-7 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".

Item	Description
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: MD5 Encryption protocol: AES
Version	For SNMP v3, the default port number is 161.

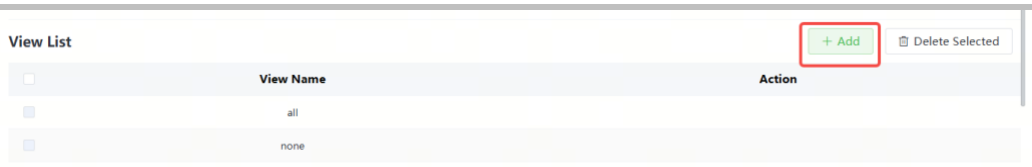
- Configuration Steps

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

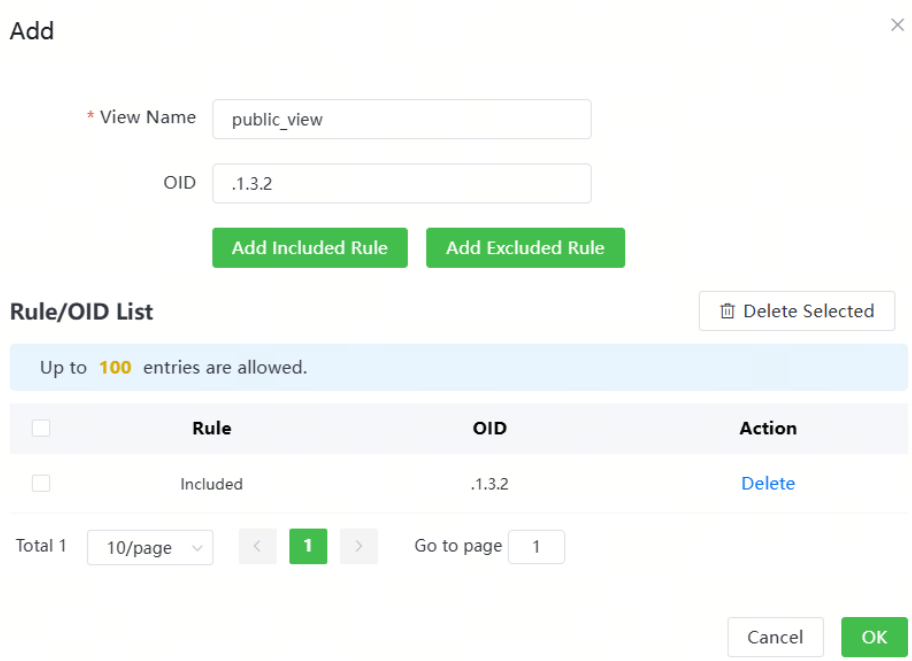


(2) Add a view on the View/Group/Community/Client Access Control interface.

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



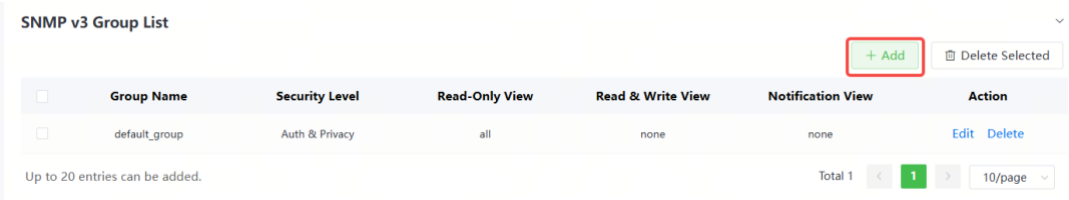
b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.



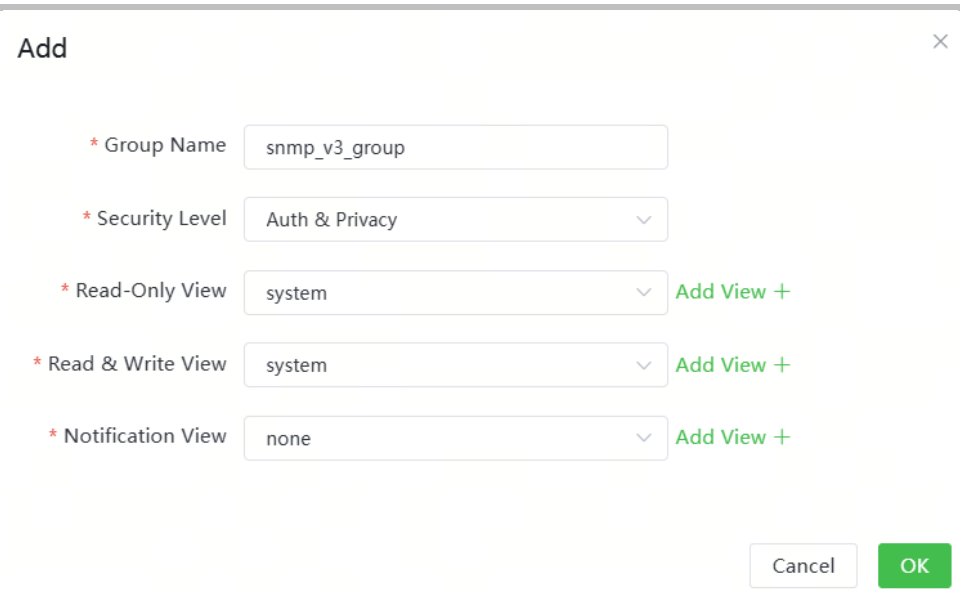
c Click **OK**.

(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.



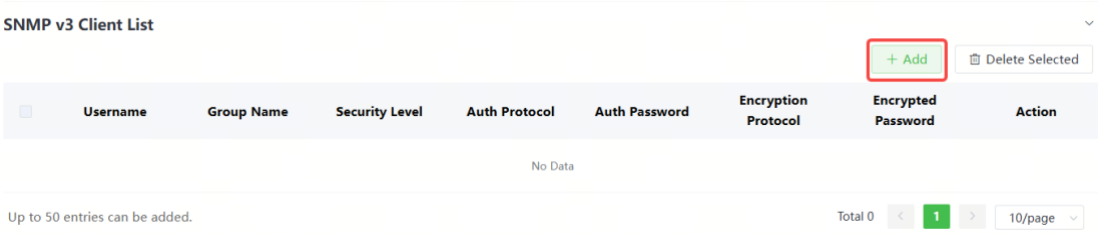
b Enter the group name and security level on the pop-up window. As this user has read and write permissions, select public_view for read-only and read & write views, and select none for notify views.



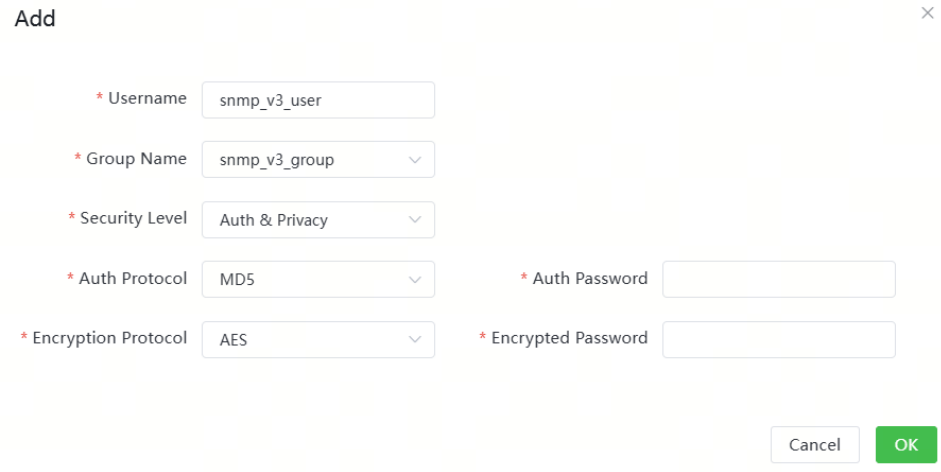
c Click **OK**.

(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**.

8.9.5 Configuring Trap Service

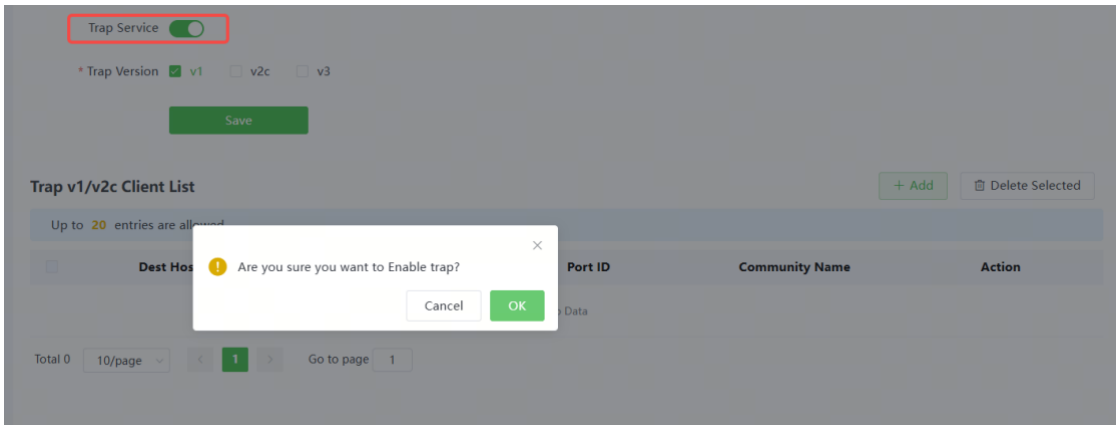
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring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

1. Enabling Trap Service

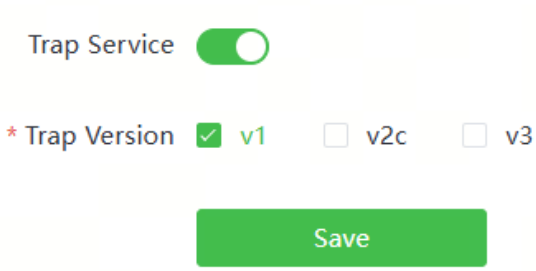
Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

Choose **Network-Wide** > **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) 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.

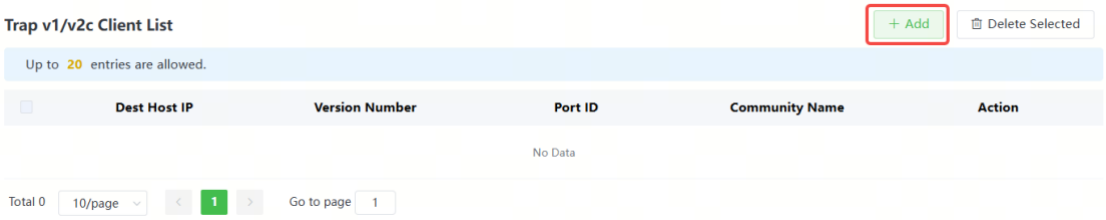
- Prerequisites

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

- Procedure

Choose **Network-Wide** > **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.

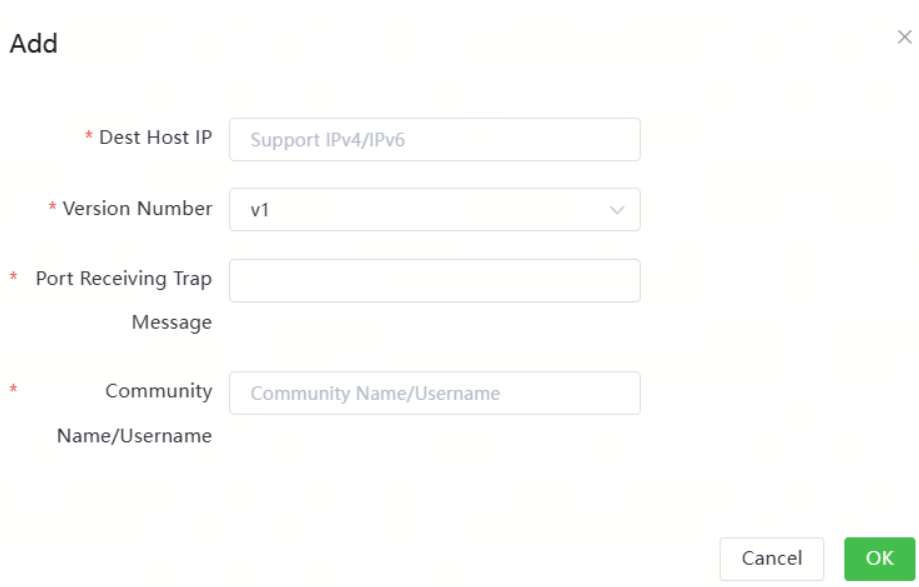


Table 8-8 Trap v1/v2c User Configuration Parameters

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. ● 8-32 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.

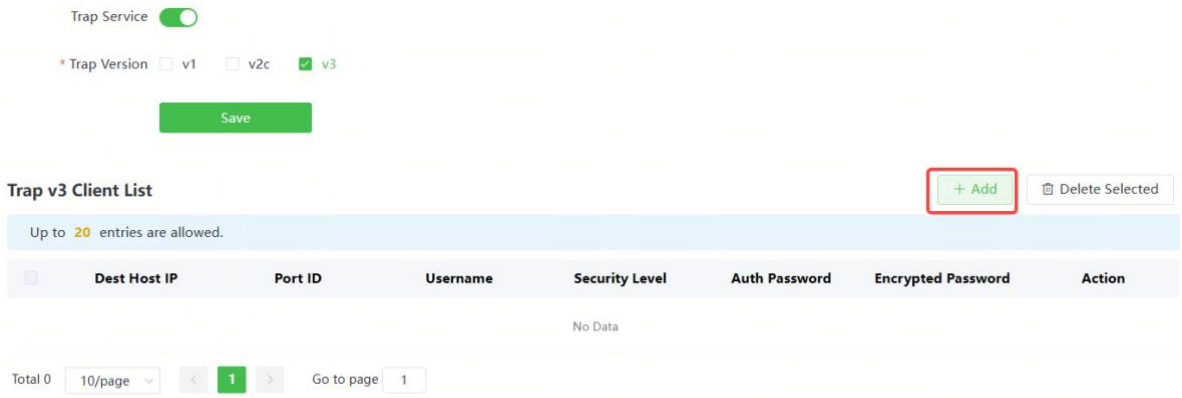
- Prerequisites

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

- Configuration Steps

Choose **Network-Wide** > **System** > **SNMP** > **Trap Setting**.

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



(2) Configure trap v3 user parameters.

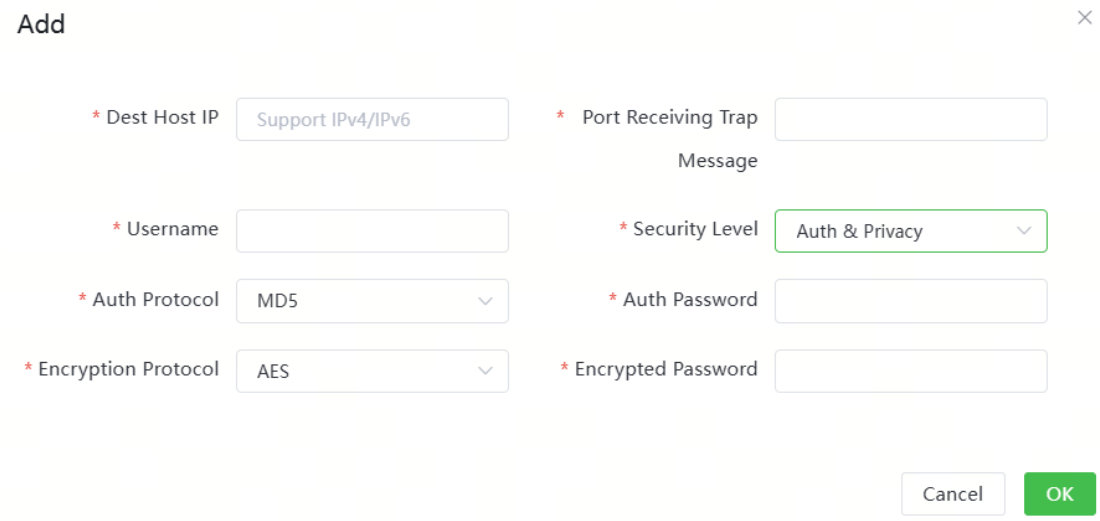


Table 8-9 Trap v3 User Configuration Parameters

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. ● 8-32 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-

Parameter	Description
	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.

8.9.6 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:

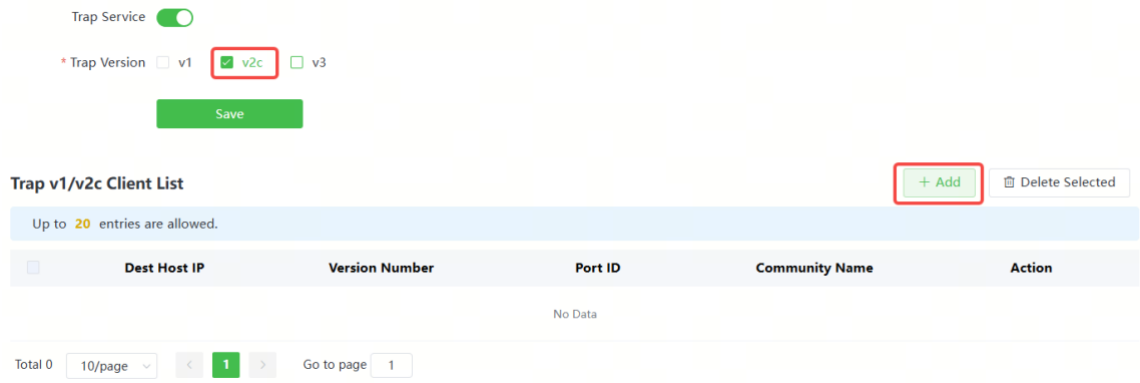
Table 8-10 User Requirement Specification

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	Trap_user

Item	Description
name	

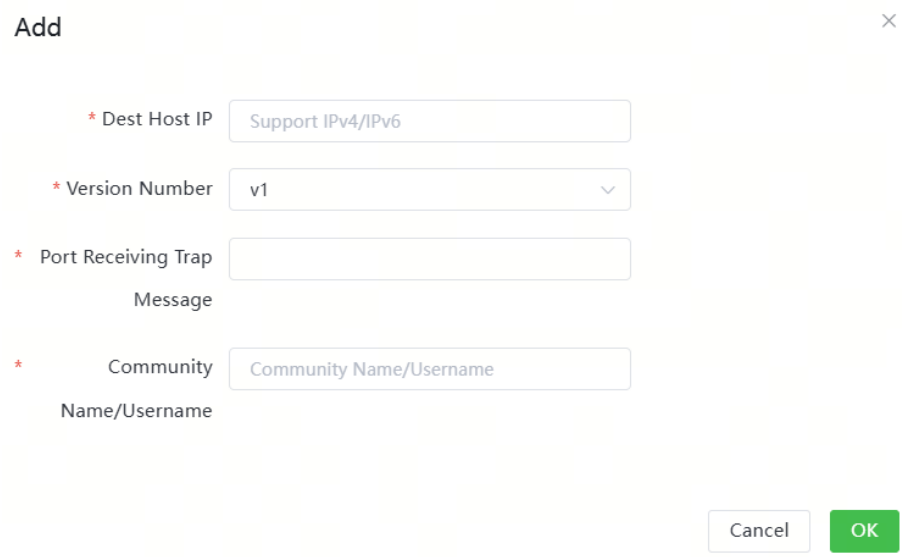
- Configuration Steps

(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

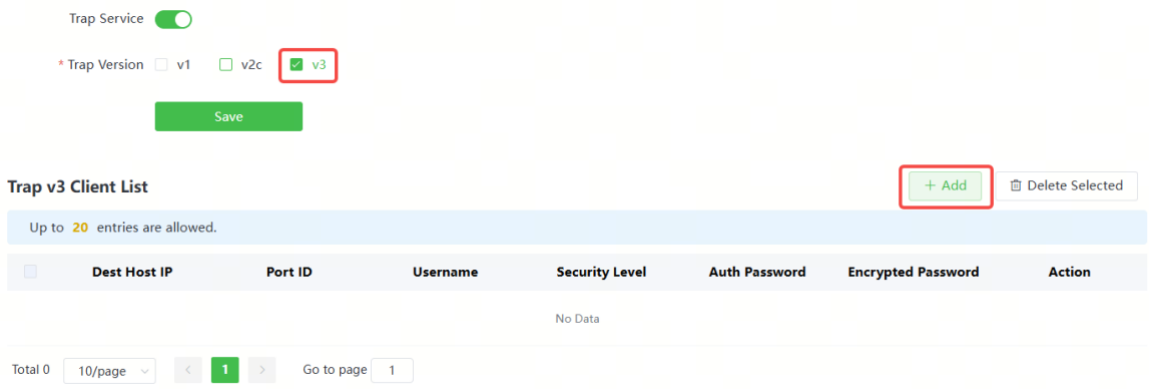
According to the user's application scenario, the requirements are shown in the following table:

Table 8-11 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: MD5 Encryption protocol: AES

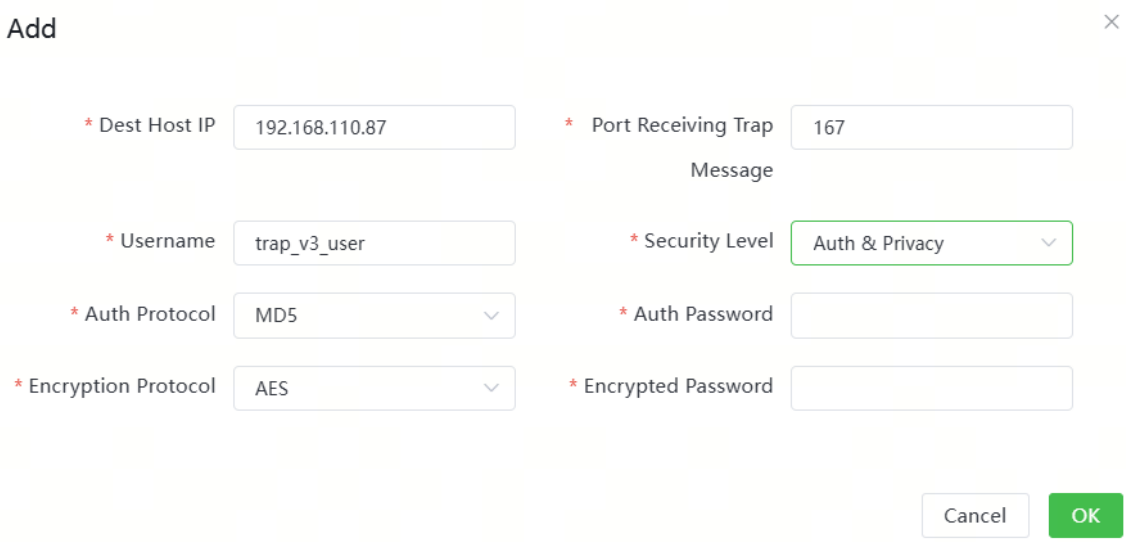
- Configuration Steps

(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.

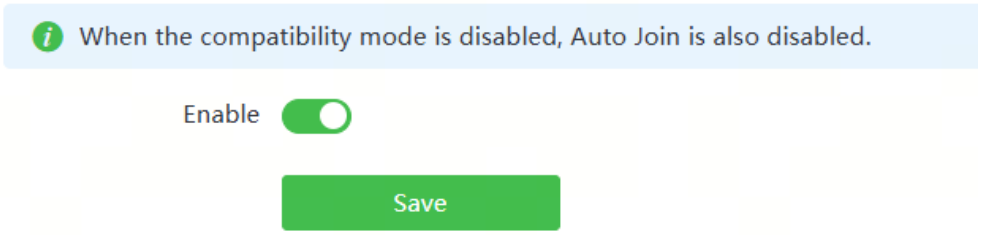
(3) Enter the destination host IP address, port number, user name, and other information. Then, click **OK**.



8.10 Configuring Compatibility Mode

Choose **Network-Wide** > **System** > **Compatibility Mode**.

The compatibility mode is enabled by default, which can improve compatibility between devices running the earlier and latest versions during networking. If the compatibility mode is disabled, devices running earlier software versions cannot join the network, and the uplink gateway cannot automatically incorporate undeployed devices.



8.11 Configuring Cloud Service

8.11.1 Overview

The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-

name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

By configuring Cloud Service, you can conveniently mange networks through Lysora Cloud or the Lysora app.

8.11.2 Configuration Steps

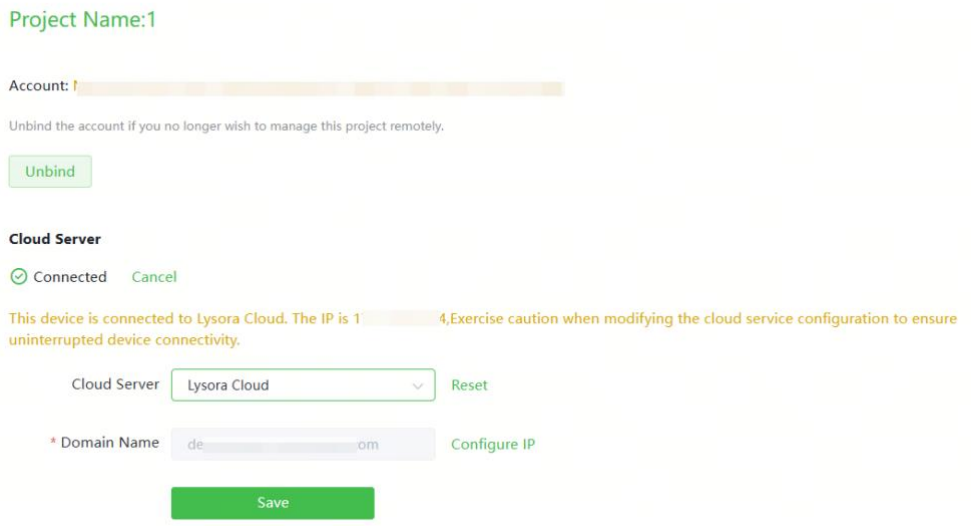
Choose **One-Device** > **Config** > **System** > **Cloud Service**.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Lysora app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.

Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

⚠ Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.



To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, enter the domain name and IP address, and click **Save**.

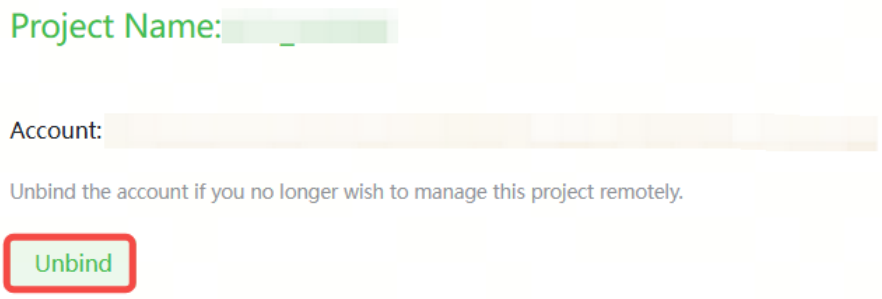
Note

If the server selected is not **Other Cloud**, the system automatically fills in the domain name and IP address of the cloud server. When **Other Cloud** is selected, you need to manually configure the domain name and IP address and upload the cloud server certificate. .

8.11.3 Unbinding Cloud Service

Choose **One-Device** > **Config** > **System** > **Cloud Service**.

You can click **Unbind** to unbind the account if you no longer wish to manage this project remotely.



9 Appendix

9.1 User Ports

Table 9-1 Default Open Port Information

Port Number	Protocol	Service
9883	TCP	Lysora Self-Organizing Network service
23561/23562	TCP	Lysora Self-Organizing Network service
53	TCP/UDP	DNS domain name service
67	UDP	DHCP service
69	UDP	TFTP service
80/443/2062	TCP	Web service
6380	TCP	Database service
63245	TCP	SSH service