# Ruijie Reyee RG-EST Series Wireless Bridges

## Web-Based Configuration Guide
## ReyeeOS 1.80.1305



Document Version: V1.1
Date: 2022.10.25
Copyright © 2022 Ruijie Networks

## Copyright

Copyright © 2022 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademarks including

,

,

are owned by Ruijie Networks.

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

## Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

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

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

# Preface

## Intended Audience

This document is intended for:

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

## Technical Support

- The official website of Ruijie Reyee: https://www.ruijienetworks.com/

## Conventions

### 1. GUI Symbols

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

### 2. Signs

The signs used in this document are described as follows:

**Warning**

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

**Caution**

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

**Note**

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

**Specification**

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

## 3. Note

This manual introduces the features of the product and offers guidance on configuration and testing.

# 1 Login

## 1.1 Configuration Environment Requirements

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

## 1.2 Default Configuration

**Table 1-1 Default Web Configuration**

| Item | Default Value |
| --- | --- |
| IP address | 10.44.77.254 |
| Username/Password | Username and password are not required at your first login and you can configure the bridge directly. |

## 1.3 Login to Eweb on a PC

### 1.3.1 Connecting to the Device

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

- Wired Connection

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

**Note**

Only RG-EST350 and RG-EST350 V2 have two LAN ports.

- Wireless Connection

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

### 1.3.2 Configuring the IP Address of the Management Computer

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

**Caution**

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

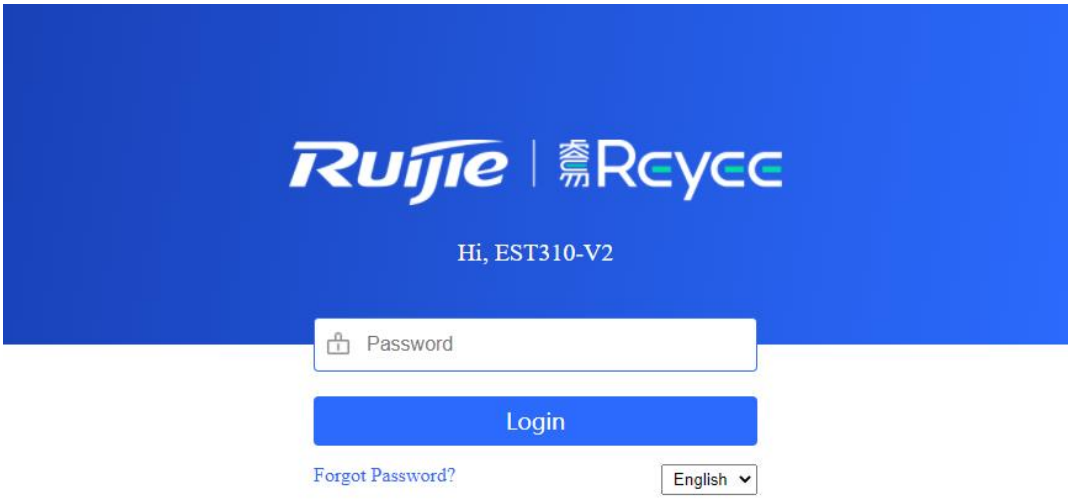
### 1.3.3 Logging in to the Web Page

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

**Instruction Note**

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

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



Username and password are not required at your first login and you can configure the bridge directly.

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

If you forget the IP address or password, hold down the **Reset** button on the device panel for more than 5 seconds when the device is connected to the power supply to restore factory settings. After restoration, you can use the default IP address to log in without entering a password.

**Caution**

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

# 2 Wi-Fi Network Settings

## 2.1 Overview

### 2.1.1 NVR and Camera

Bridges purchased in pairs in the same package can be paired automatically with each other after power-on. You can also manually pair the devices by setting up a WDS network. See Setting WDS Wi-Fi for a Single NVR or Camera. In a paired WDS group, bridges can work in access point (AP) or Customer Premises Equipment (CPE) mode.

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

### 2.1.2 WDS Wi-Fi and Management Wi-Fi

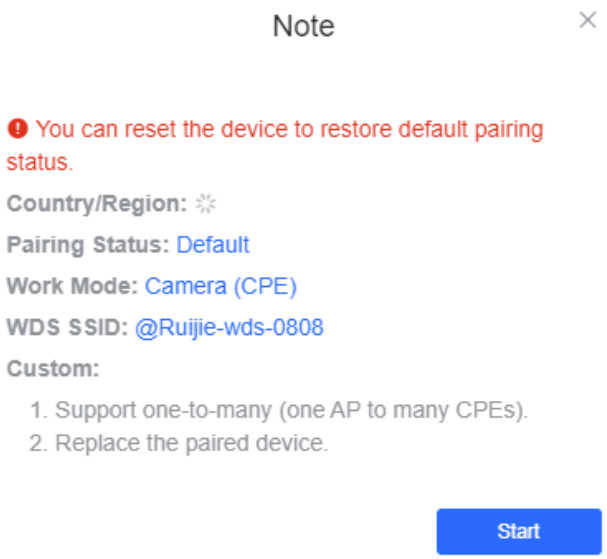
- **WDS Wi-Fi**: An AP broadcasts the WDS Wi-Fi signal. A CPE accesses the WDS Wi-Fi and upload videos or other data to the AP.
- **Management Wi-Fi**: Both an AP and a CPE can broadcast management Wi-Fi signal. You can use a mobile phone or laptop to access the management Wi-Fi and log in to the web page to configure bridges.

## 2.2 Switching NVR and Camera Mode

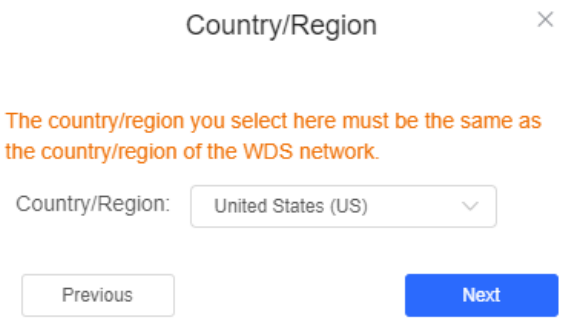
If an NVR fails, replace it and switch the new device to NVR (AP). If multiple cameras (CPE) are required, a device newly joining the WDS group needs to be switched to Camera (CPE).

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

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



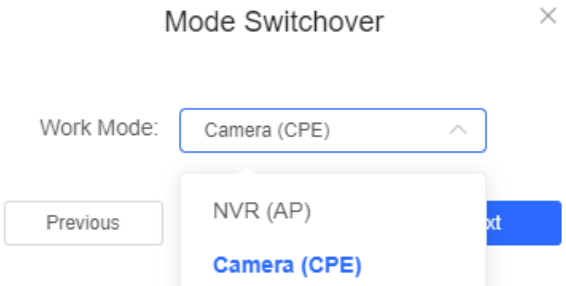

(3) Click **Next**.




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

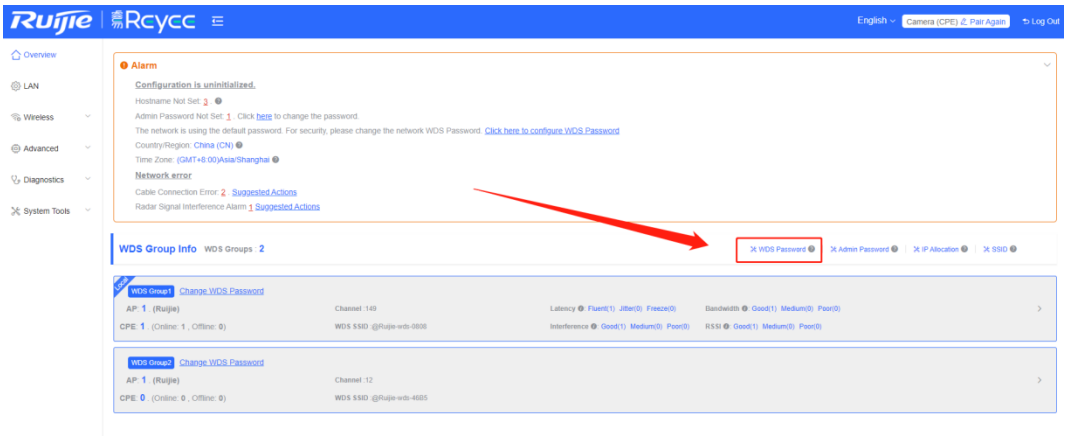
**Caution**

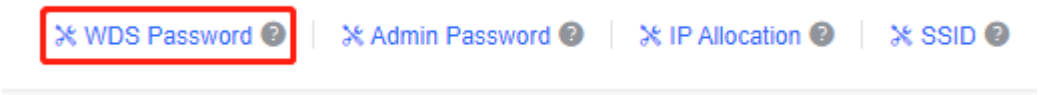
Switching the mode will reboot the device. Therefore, exercise caution when performing this operation.




## 2.3 Configuring the WDS Password for All Bridges in the LAN

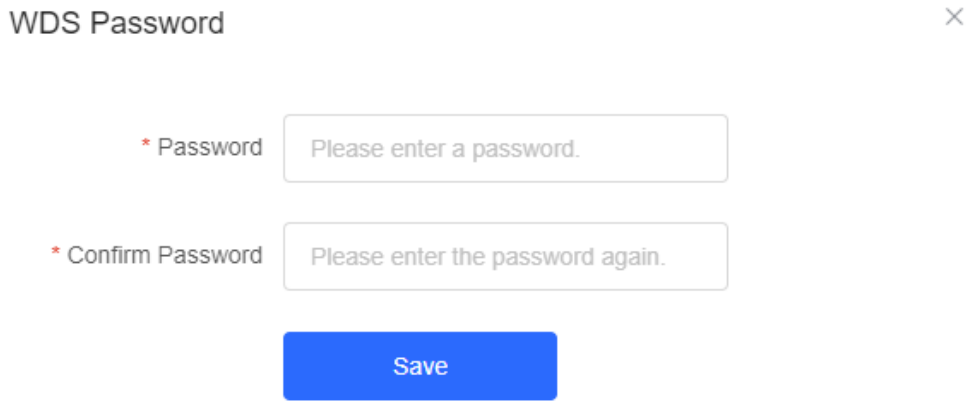
Choose **Overview** > **WDS Password**.






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

Hover the cursor over to view the help information.




**Caution**

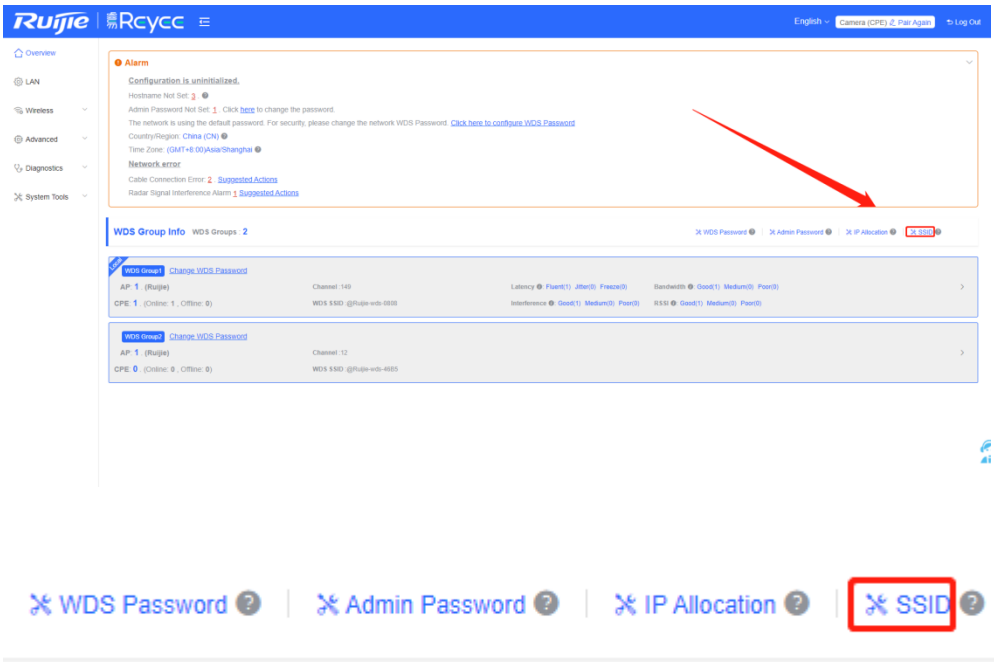
When configuring the WDS password for the entire network, ensure that all devices in the network are online. Otherwise, the WDS passwords of the devices will be inconsistent.

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

If there is an unbridged device in the network, the WDS password cannot be configured.

## 2.4 Configuring the Management SSID and Password for All Bridges in the LAN

Choose **Overview** > **SSID**.







**Note**

The management Wi-Fi network is used only for login to the web page and device management, and cannot be used for Internet access. It is isolated from the service network.

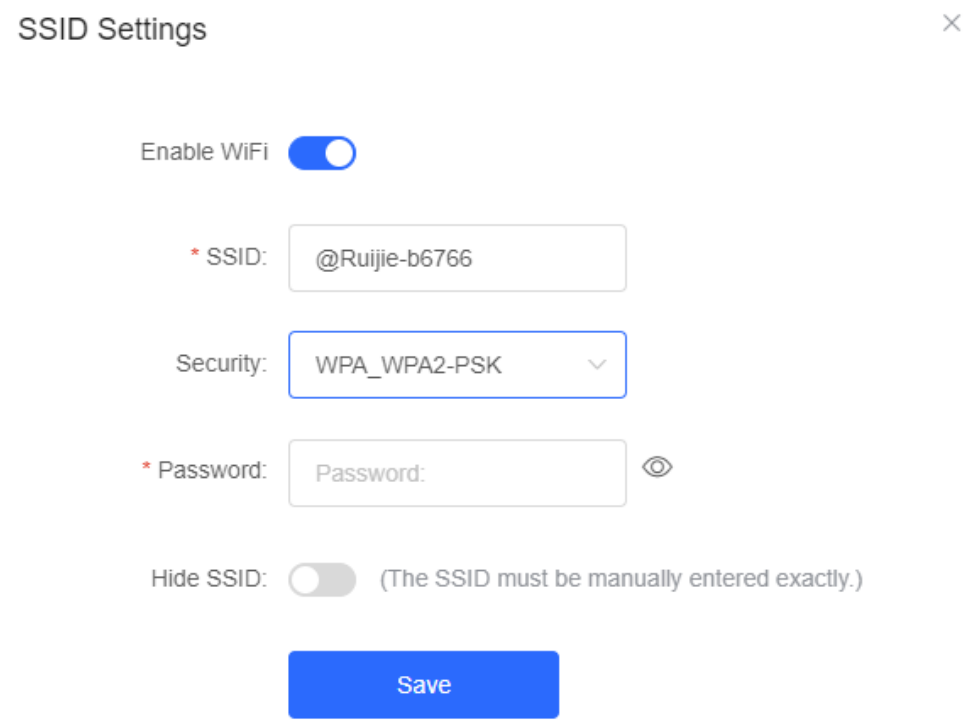
The default device management service set identifier (SSID) is @**Ruijie-b***XXXX*. (XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with device.) Click **SSID** on the page to set the same management SSID and password for all bridges in the LAN.

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

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

**Security**: The following encryption types are available: Open, WPA-PSK, WPA2-PSK, and WPA_WPA2-PSK. You are advised to choose WPA_WPA2-PSK and set the password to improve the security.

**Hide SSID**: When this function is enabled, mobile phones or computers cannot find the Wi-Fi name, and users need to manually enter the correct name and password. This can prevent Wi-Fi from being accessed by unauthorized users and can enhance security.




**Caution**

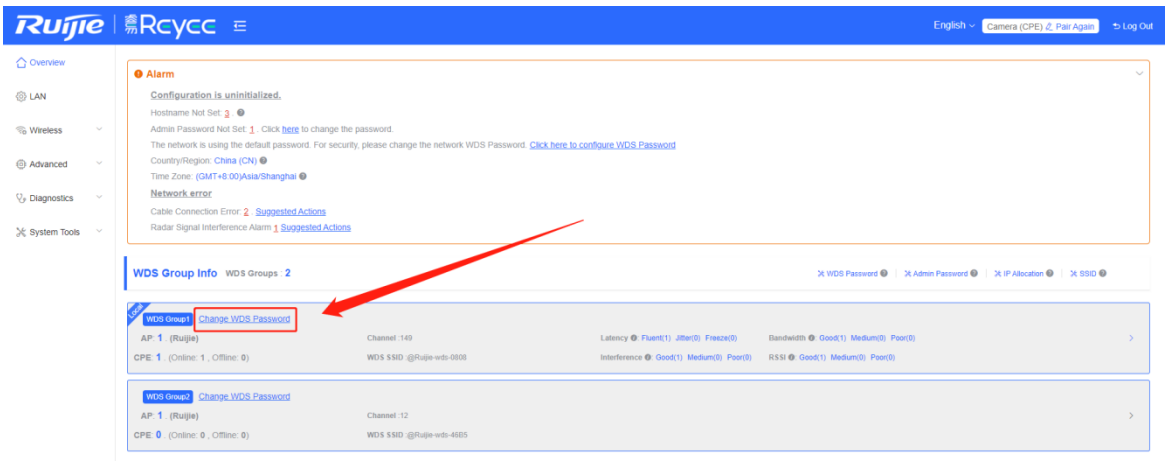
After the configuration is saved, NVRs and cameras in the network will be reconnected. Therefore, exercise caution when performing this operation.

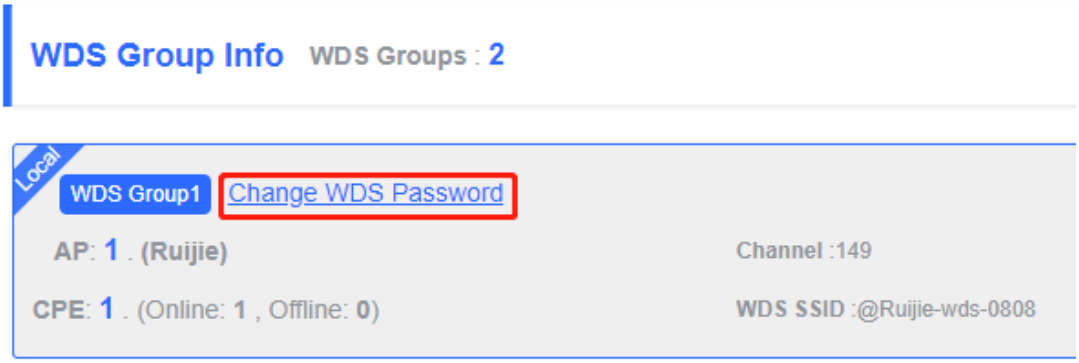
## 2.5 Configuring the WDS Password for All Bridges in the WDS Group

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

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

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






**Caution**

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

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

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

## 2.6 Setting WDS Wi-Fi for a Single NVR or Camera

### 2.6.1 Setting the WDS SSID

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

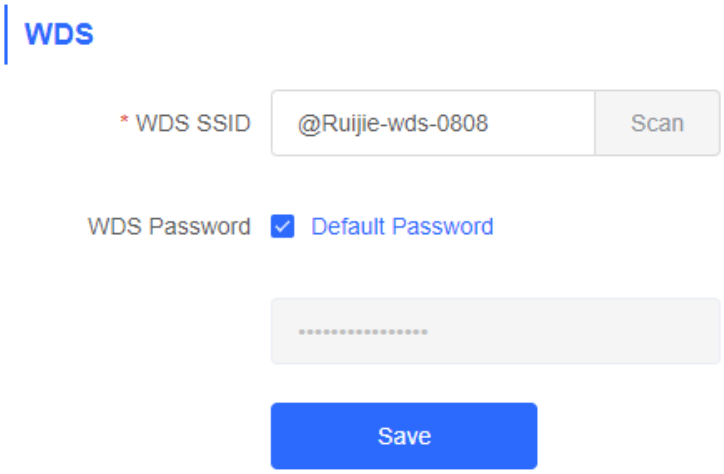
If a new WDS SSID is set for a device in a WDS group, other bridges in the group need to change to the new SSID as well to connect with this device.

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

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

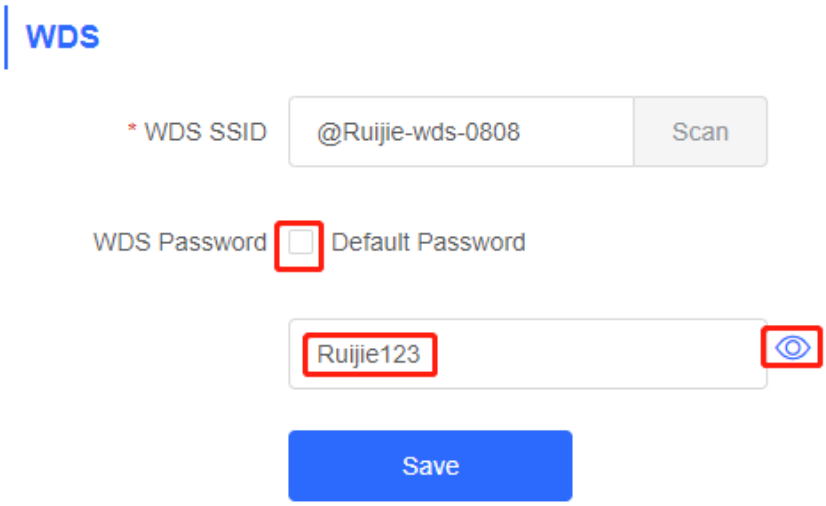
**Caution**

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




### 2.6.2 Configuring the WDS Password

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




**Caution**

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

### 2.6.3 Saving the Settings

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

# 2.7 Optimizing Wireless Network

## 2.7.1 Overview

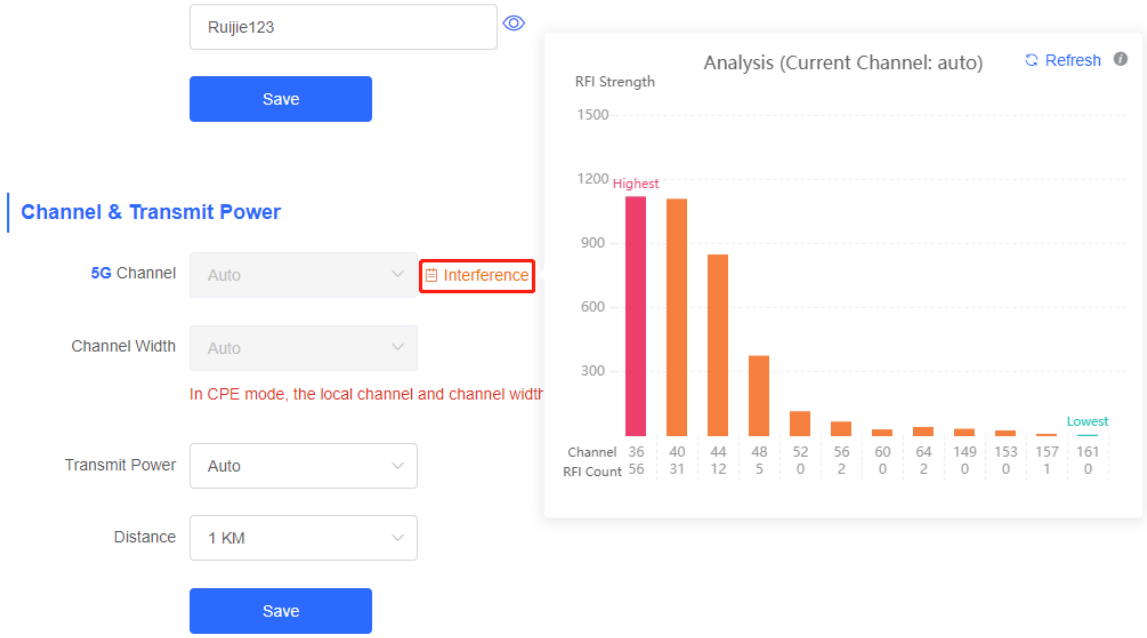
The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can also analyze the wireless environment around the bridge and manually select appropriate parameters.

## 2.7.2 Getting Started

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

Choose **Wireless** > **WDS** > **Channel & Transmit Power**.

Click **Interference** to check the interference of current channels. The channel with the smallest interference is the optimum.



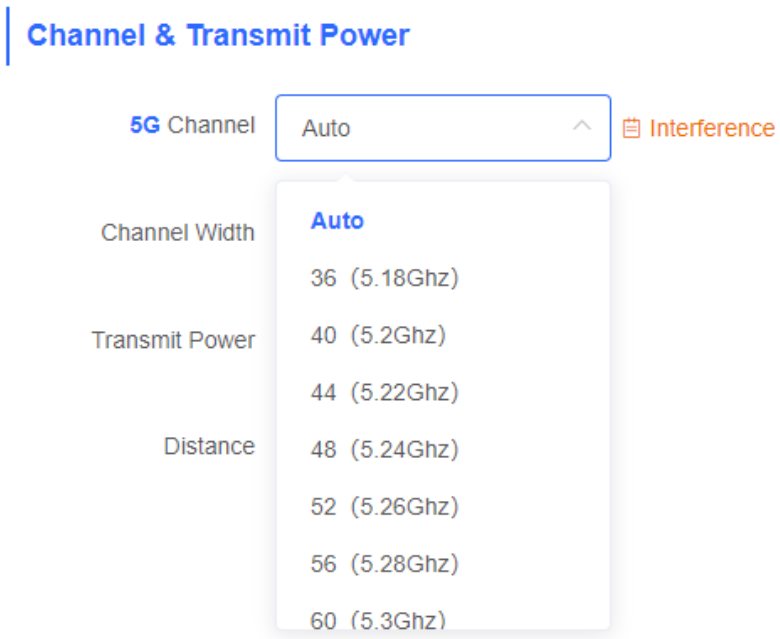

## 2.7.3 Configuration Steps

### 1. Optimizing the Radio Channel

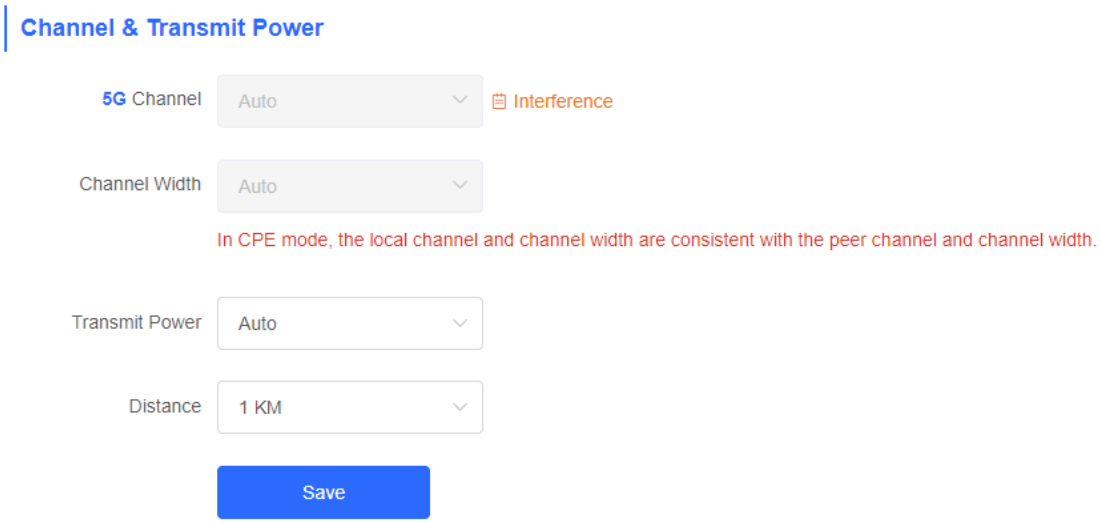
(1) Channel settings

Choose **Wireless** > **WDS** > **Channel & Transmit Power** > **5G Channel**.

The default channel is **Auto**, indicating automatic channel adaption based on the surrounding environment upon power-on. Choose the optimal channel identified through the above analysis. Click **Save** to activate settings immediately. Excess STAs connected to a channel can bring stronger wireless interference.




The camera mode does not support independent channel settings. After the channel at the NVR end is adjusted, the camera end automatically changes its channel to be the same as the NVR end.




**Note**

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

The above figure provides guidance on 5 GHz channel configuration. Take the same steps for 2.4 GHz channel configuration. The single-radio (2.4 GHz) device does not support 5 GHz configuration.

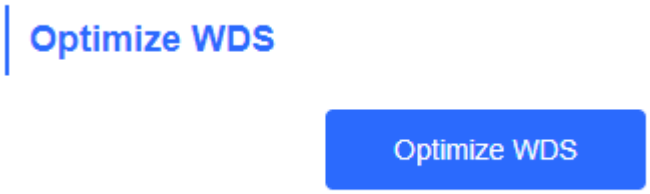
**Caution**

After the channel is changed, the NVR will be reconnected to the camera. Therefore, exercise caution when performing this operation.

(2) One-click optimization

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

Click **Optimize WDS** so that the device automatically selects the channel again based on the interference in the current environment, ensuring that the device works in the optimal channel. You are advised to optimize WDS when the original channel is not the optimum.




**Caution**

After you click **Optimize WDS**, the NVR will be reconnected to the camera. Therefore, exercise caution when performing this operation.

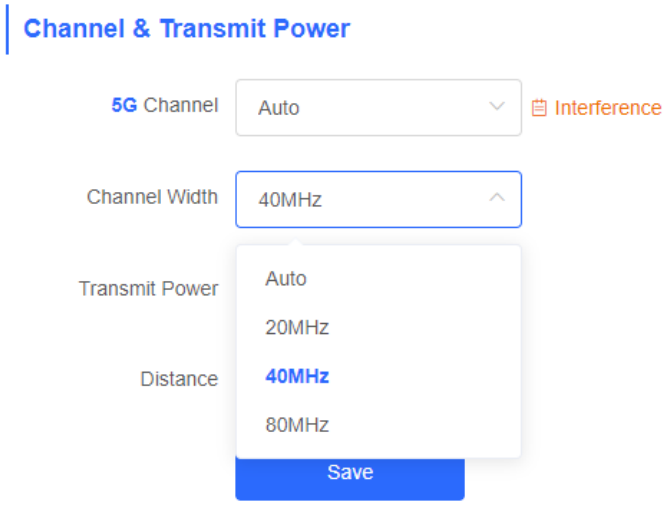
### 2. Optimizing the Channel Width

Choose **Wireless** > **WDS** > **Channel & Transmit Power** > **Channel Width**.

If the interference is severe, choose a lower channel width to avoid network stalling. A 5 GHz bridge supports channel widths of 20 MHz, 40 MHz, and 80 MHz, while a 2.4 GHz bridge supports channel widths of 20 MHz and 40 MHz. The network is stable when the channel width is smaller. A larger channel width is more susceptible to interference. The default channel width of a 2.4 GHz bridge is 20 MHz (recommended configuration). The default channel width of a 5 GHz bridge is 40 MHz (recommended configuration). After changing the channel width, click **Save** to activate settings immediately.

**Caution**

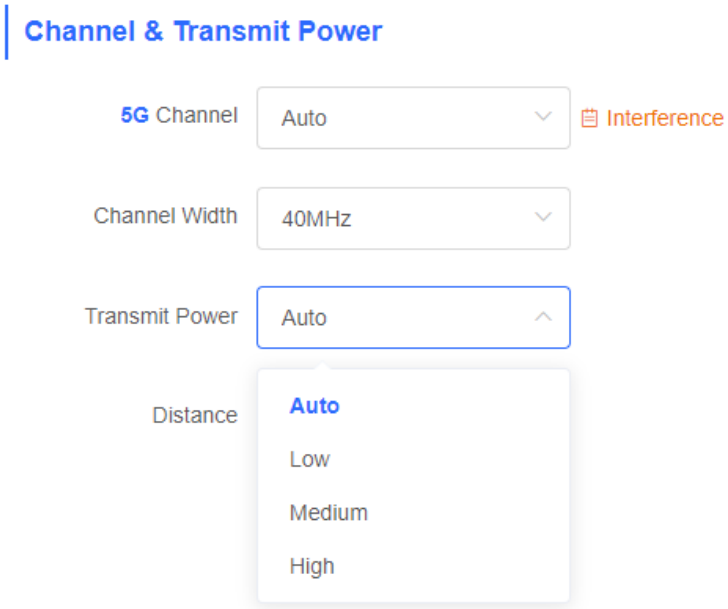
After the channel width is changed, the NVR will be reconnected to the camera. Therefore, exercise caution when performing this operation.




### 3. Optimizing the Transmit Power

Choose **Wireless** > **WDS** > **Channel & Transmit Power** > **Transmit Power**.

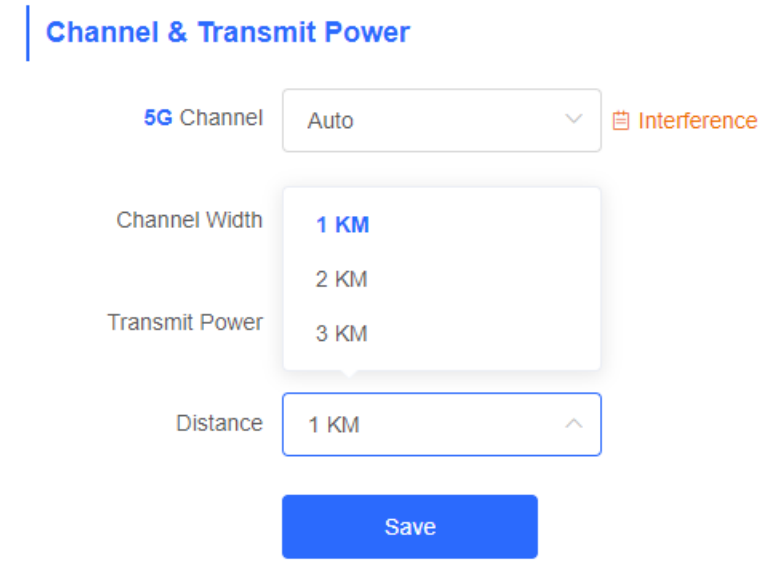
Greater transmit power indicates larger coverage and brings stronger interference to surrounding wireless devices. The default value is **Auto**, indicating automatic adjustment of the transmit power. In a scenario in which wireless devices are installed densely, a lower power is recommended. **Low**, **Medium**, and **High** indicate 50%, 75%, and 100% power, respectively.




### 4. Configuring the Distance

Choose **Wireless** > **WDS** > **Channel & Transmit Power** > **Distance**.

It is recommended that the configured distance between the NVR and camera be greater than their actual distance. If the configured distance is much smaller than the actual distance, the wireless performance will deteriorate, and WDS connection may fail.



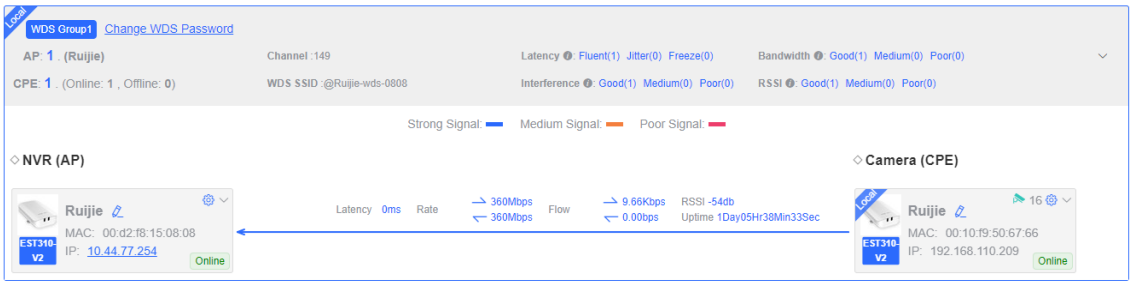

**Note**

Distance configuration is supported on RG-EST310, RG-EST310 V2, RG-EST350 and RG-EST350 V2 only. RG-EST310 and RG-EST310 V2 support a maximum actual distance of 1 km, while RG-EST350 and RG-EST350 V2 support a maximum actual distance of 5 km.

## 2.8 Changing the Country/Region Code

### 2.8.1 Getting Started

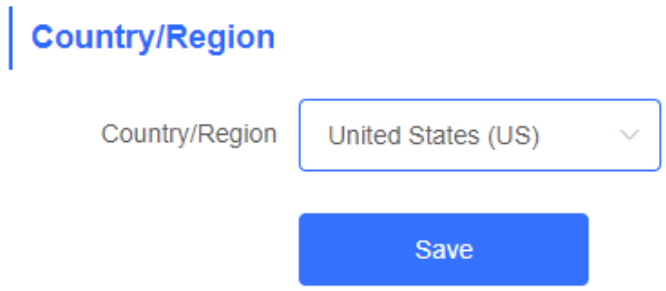
Country/region code change takes effect on all devices in the entire network, that is, all bridges on the **Overview** page. Therefore, before changing the country/region code, confirm that the target device is in the current network and the WDS link works well.




### 2.8.2 Configuration Steps

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

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




**Caution**

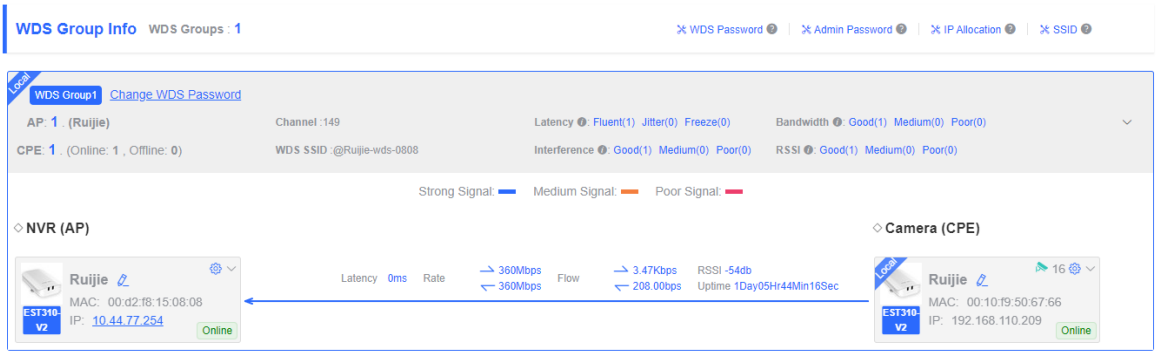
After the country/region code is changed, the Wi-Fi network will restart, and the NVR and the camera will be reconnected after the Wi-Fi network is restarted.

The current channel may be switched to **Auto** because it is not supported by the country/region. Therefore, exercise caution when performing this operation.

## 2.9 Displaying WDS Group Information

Choose Overview > WDS Group Info.

Displayed WDS group information includes the number of APs and CPEs 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.



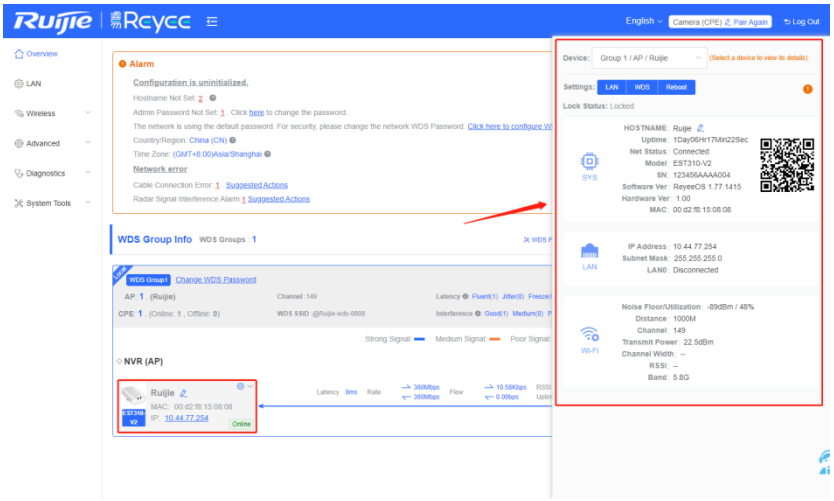
**Note**

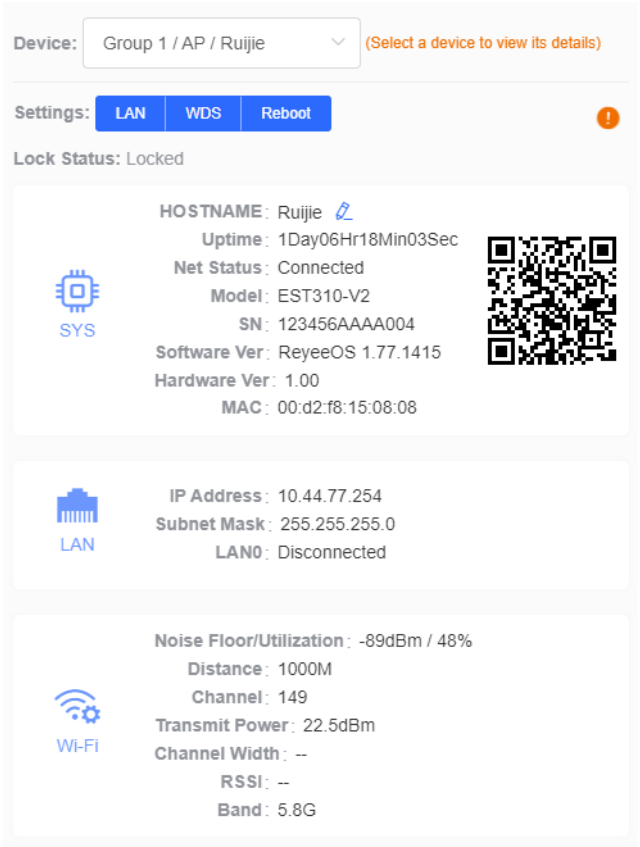
AP is at the NVR end, while CPE is at the camera end.

## 2.10 Displaying the Information About a Single Device

- Choose **Overview** > **WDS Group Info** > **NVR (AP)/Camera (CPE)**.

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



**Note**

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

# 3 Network Settings

## 3.1 Setting the Address of a LAN Port

The address of a LAN port is used only for login to the web page and does not affect the service network.

### 3.1.1 Allocating IP Addresses to All Bridges in the Network

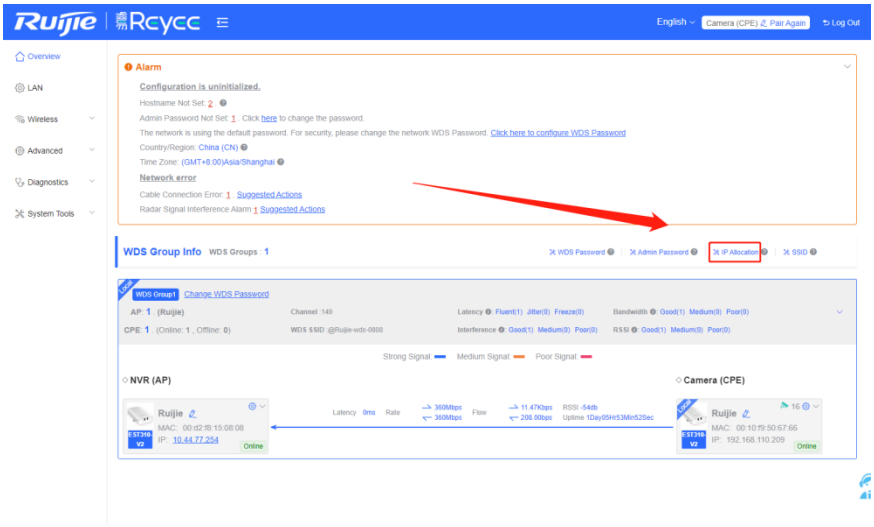
- Static IP address

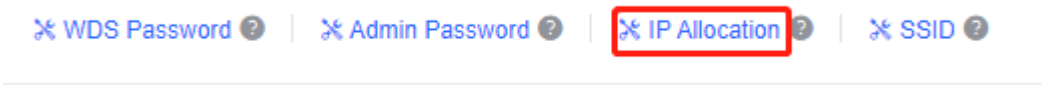
On the **Overview** page, click **IP Allocation**.

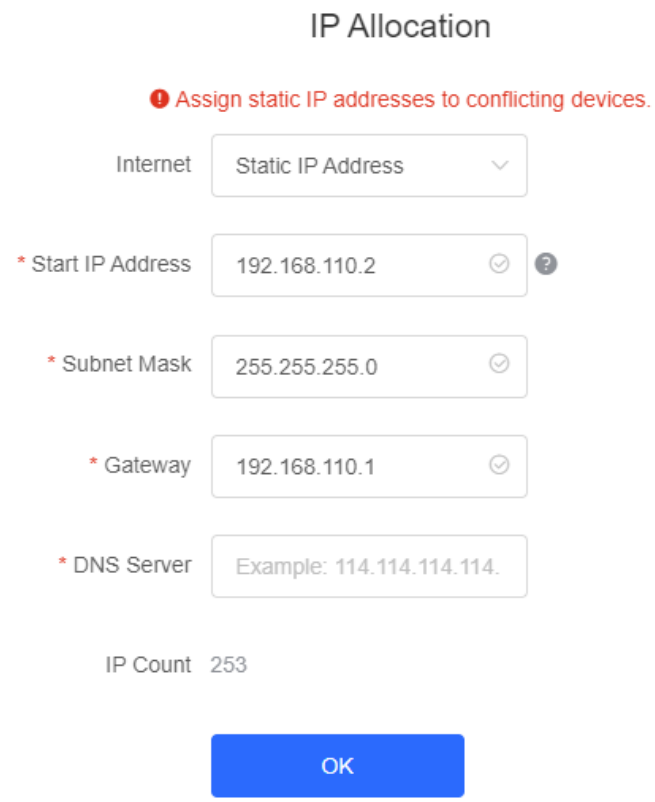
Configuring static IP addresses for the entire network:

When a large number of devices in the network require static IP addresses, you can use **IP Allocation** to automatically allocate a static IP address for each device. Click **IP Allocation**, set **Internet** to **Static IP Address**, set **Start IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server**, and click **OK**.

Hover the cursor over to view the help information.






**Caution**

The start IP address cannot be in the same network segment as the current IP address. Otherwise, the configuration will fail.

After the configuration, the device IP address changes, and the device web page cannot be accessed. You need to enter the new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer. (See Configuring the IP Address of the Management Computer) Therefore, exercise caution when performing this operation.

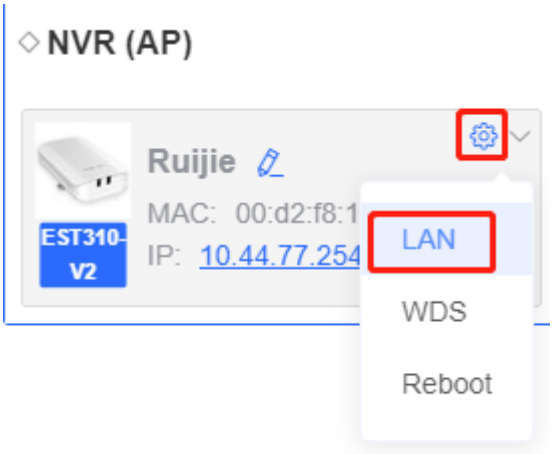
- Dynamic IP address (DHCP)

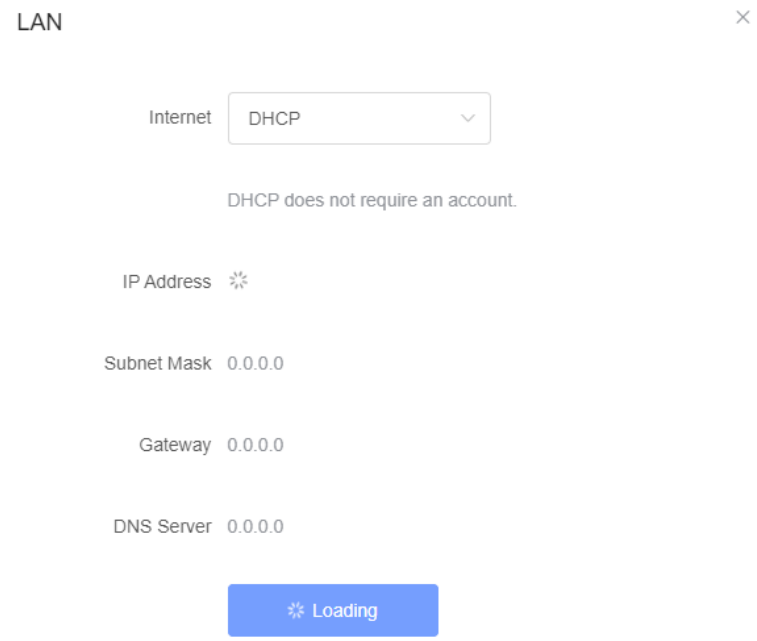
When a large number of devices in the network require dynamic IP addresses, you can configure dynamic IP addresses (DHCP) for the entire network so that each device can dynamically obtain an IP address. Set **Internet** to **DHCP**, and click **OK**.

### 3.1.2 Setting the Address of a LAN Port for a Single Online Bridge

Choose Overview > WDS Group Info > NVR (AP)/Camera (CPE).

To set the IP address for a single device, click , and select LAN from the drop-down list. For the configuration method, see Allocating IP Addresses to All Bridges in the Network.



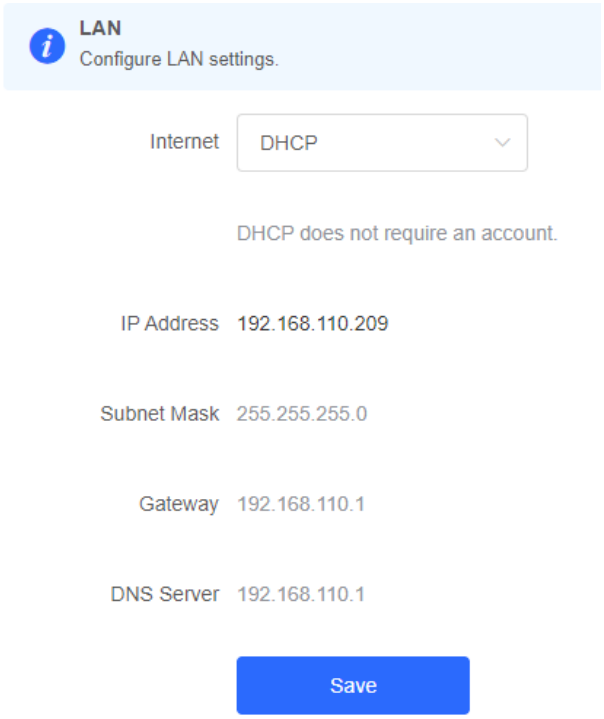

**Caution**

After the IP address and subnet mask are changed, the device web page may not be accessed. You need to enter the new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer. (See Configuring the IP Address of the Management Computer) Therefore, exercise caution when performing this operation.

### 3.1.3 Setting the Address of a LAN Port on the Local Device

Open the **LAN** page.

If a DHCP server is deployed in the network, you are advised to set **Internet** to **DHCP**. If no DHCP server is deployed, set **Internet** to **Static IP Address**, set **IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server**, and click **Save**.



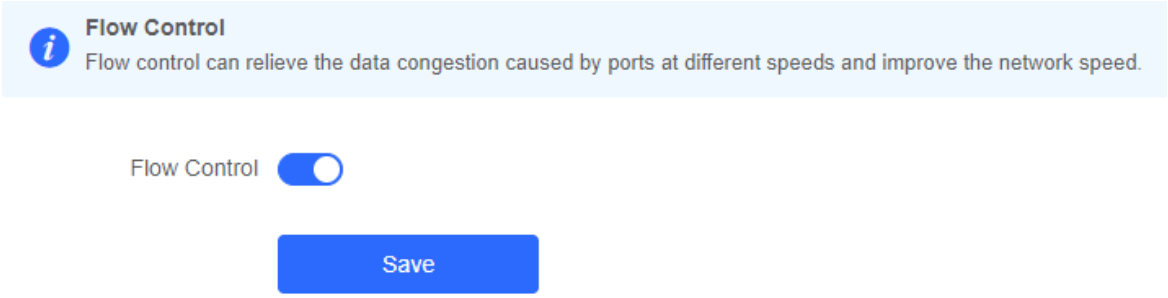

**Caution**

After the IP address and subnet mask are changed, the device web page may not be accessed. You need to enter the new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer. (See Configuring the IP Address of the Management Computer) Therefore, exercise caution when performing this operation.

## 3.2 Port-Based Flow Control

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

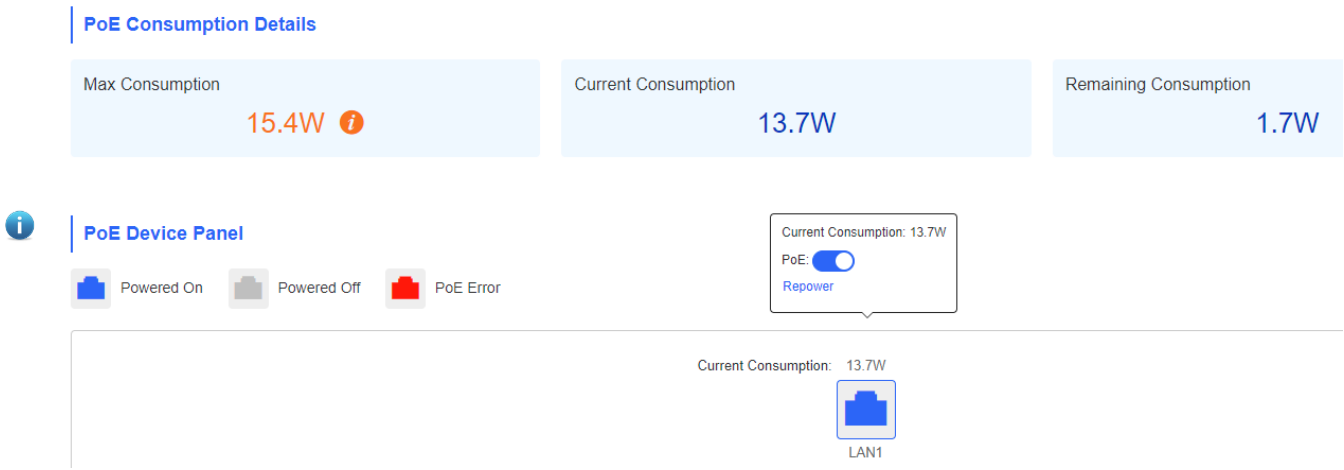
Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed. This function is enabled by default and can be manually disabled.


Flow Control
Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.
Flow Control
Save

# 4 PoE Settings

Choose **Advanced** > **PoE**.

The device supports PoE power supply to cameras (Maximum: 15.4W). You can view the maximum power consumption, current power consumption, remaining power consumption and PoE status. Hover the cursor over to display the PoE switch .




**Note**

PoE is supported on RG-EST100-P only.

# 5 Alarm and Fault Diagnosis

## 5.1 Alarm Information and Suggested Action

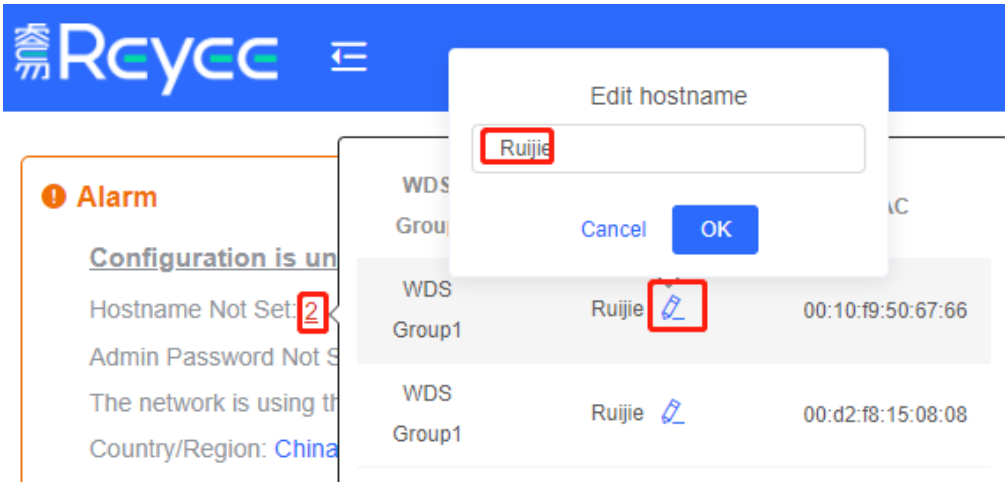
When bridges fail or lack some necessary security configuration, the system prompts key alarms about the bridges on the homepage, so that users can handle the exceptions promptly.

Choose **Overview** > **Alarm**.

### 5.1.1 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.

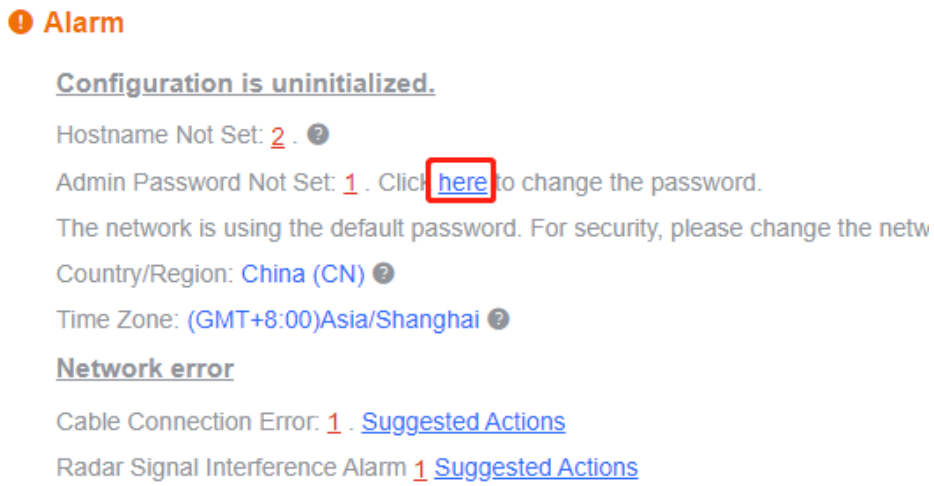
When viewing the alarm, hover the cursor over the orange number of the prompt and click in the displayed dialog box to modify the name of each device. (The orange number, 2 in the figure, indicates the number of devices that still use the default name in the network.) Enter the new device name and click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




### 5.1.2 Default Admin Password Is Still Used

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

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




**Notice** **Caution**

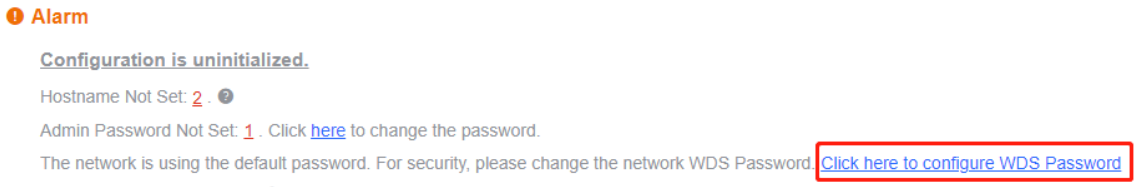
The admin password is used to log in to the web page of any device in the network. Therefore, remember the admin password. If you forget the admin password, restore factory settings. For the method, see Logging in to the Web Page.

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

### 5.1.3 Default WDS Password Is Still Used by All Devices

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

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




**Notice** **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.

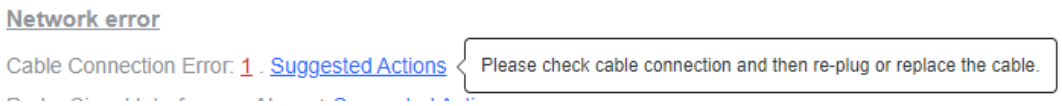
Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation.

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

### 5.1.4 Network Cable Is Disconnected or Incorrectly Connected

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

Click the suggested action to check the solution.




### 5.1.5 Latency Is High or Bandwidth Is Insufficient

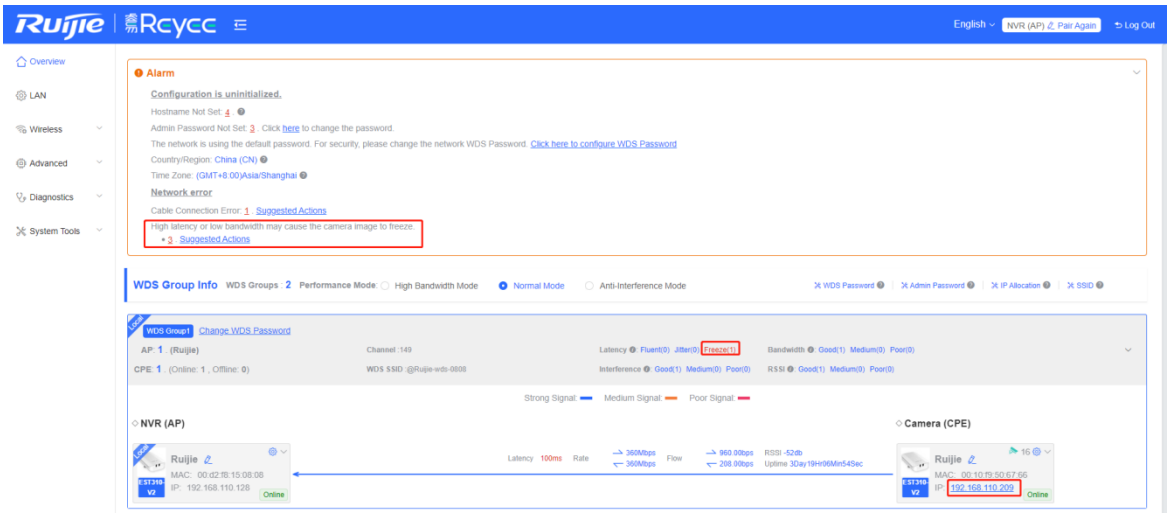
First, check whether the device latency is too high. If yes, the interference in the environment may be severe. Then, you are advised to change to a channel with smaller interference.

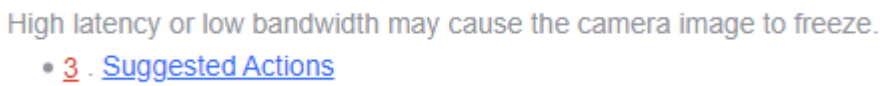
If not, increase the channel width. For channel settings, see Channel settings. For channel width settings, see Optimizing the Channel Width.

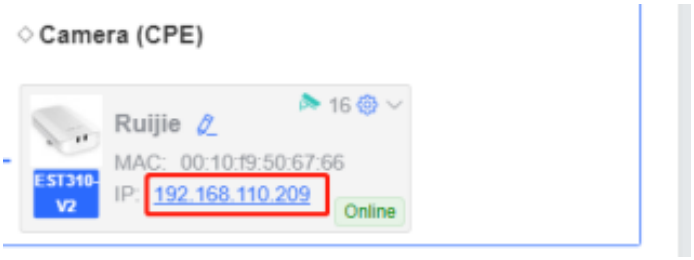
To check whether the latency is too high, perform as follows:

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

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



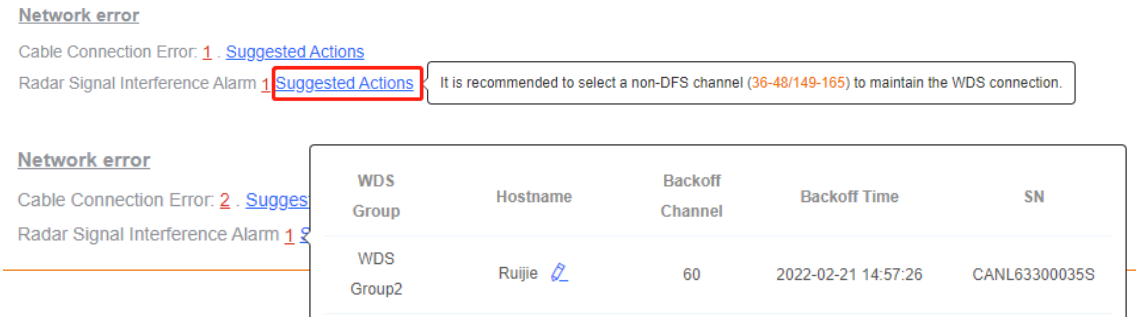



**Caution**

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

### 5.1.6 Radar Signal Interference

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




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

**Note**

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

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

## 5.2 Network Diagnosis Tools

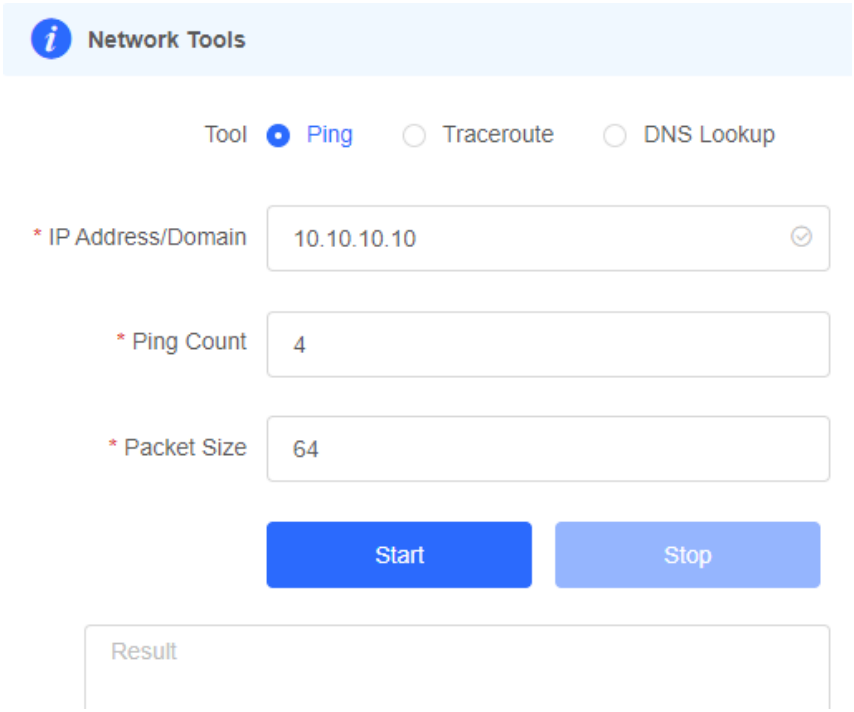
### 5.2.1 Network Test Tool

Choose **Diagnostics** > **Network Tools**.

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

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

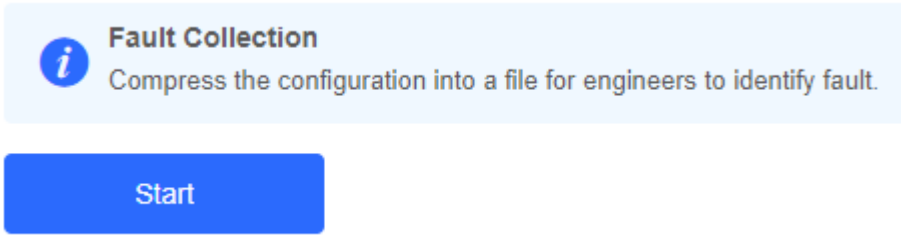
The DNS Lookup tool displays the DNS server address used to resolve a URL.




### 5.2.2 Collecting Fault Info

Choose **Diagnostics**> **Fault Collection**.

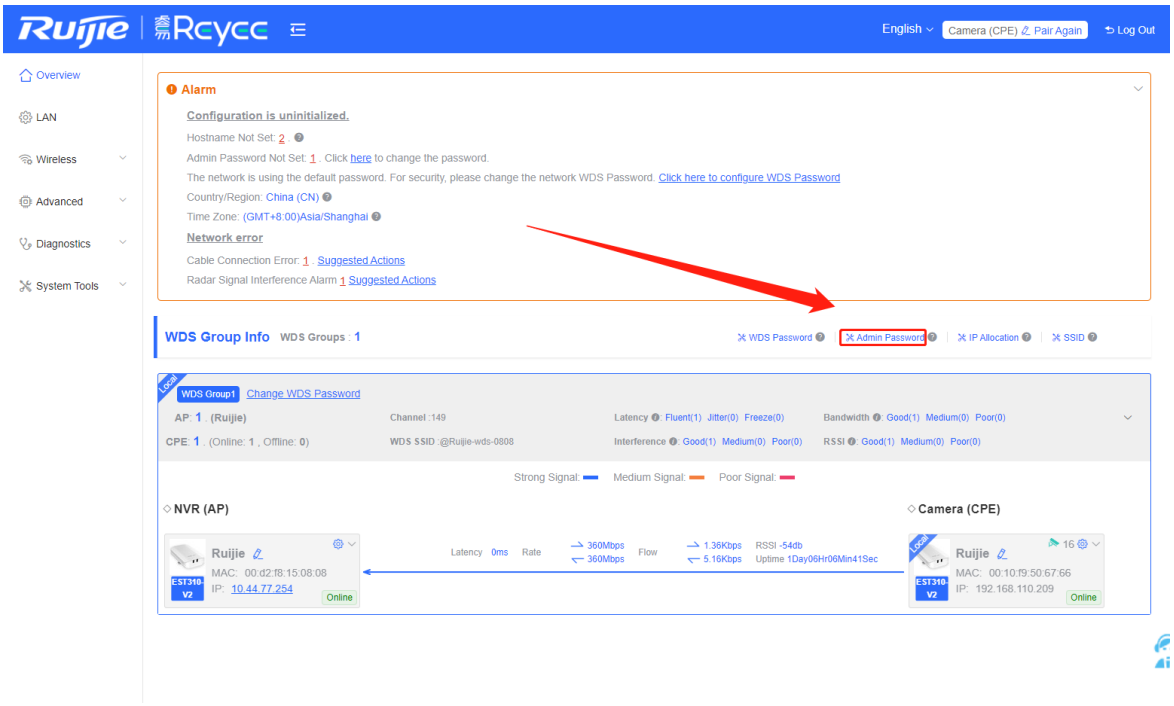
Click **Start** to collect fault information and compress it into a file for engineers to identify fault.

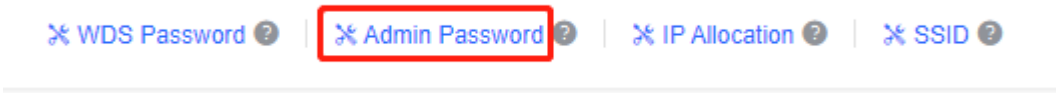


# 6 System Settings

## 6.1 Configuring Management Password

Choose **Admin Password**.

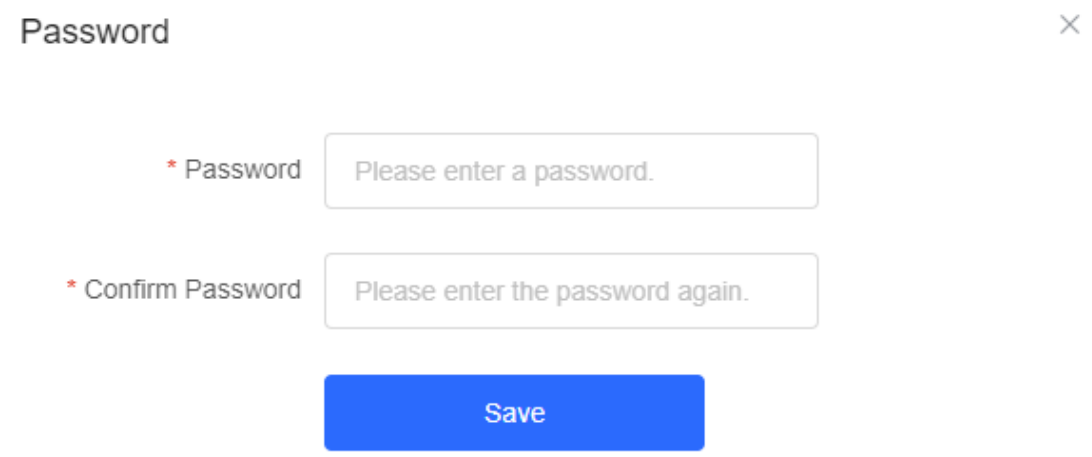



Click **Admin Password** to change the login password for all devices.

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

Hover the cursor over to view the help information.




**Caution**

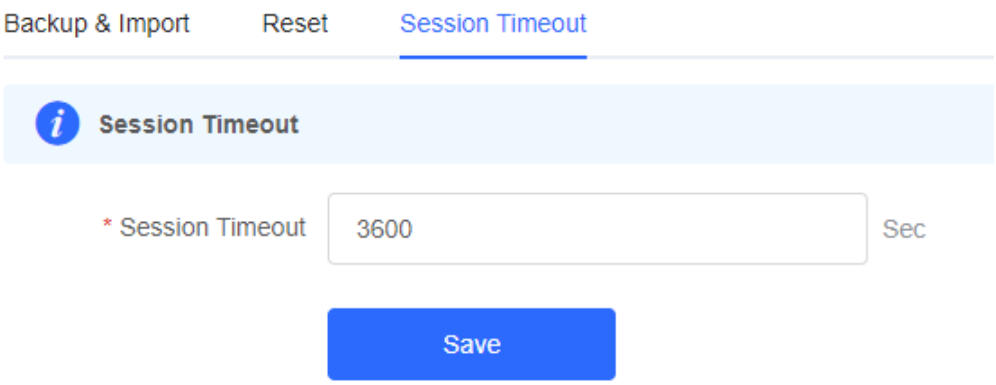
This password is used to log in to Eweb system of any device in the network.

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

## 6.2 Configuring Session Timeout Duration

Choose **System Tools** > **Management** > **Session Timeout**.

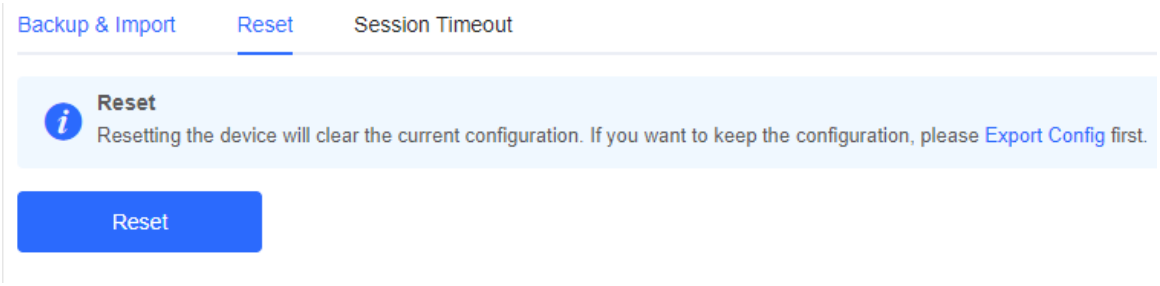
If no operation is performed on the page within a period of time, the session will be down. When you need to perform operations again, enter the password to open the configuration page. The default timeout duration is 3600 seconds, that is, 1 hour.




## 6.3 Resetting Factory Settings

Choose **System Tools** > **Management** > **Reset**

Click **Reset** to restore factory settings.



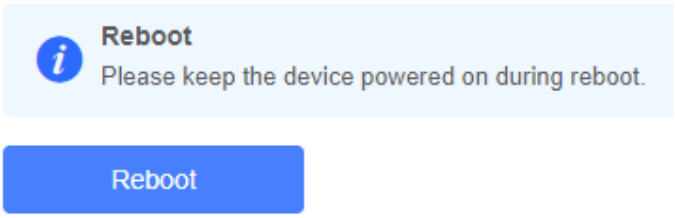

**Caution**

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.

## 6.4 Rebooting the Device

Choose **System Tools** > **Reboot** > **Reboot**

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




**Caution**

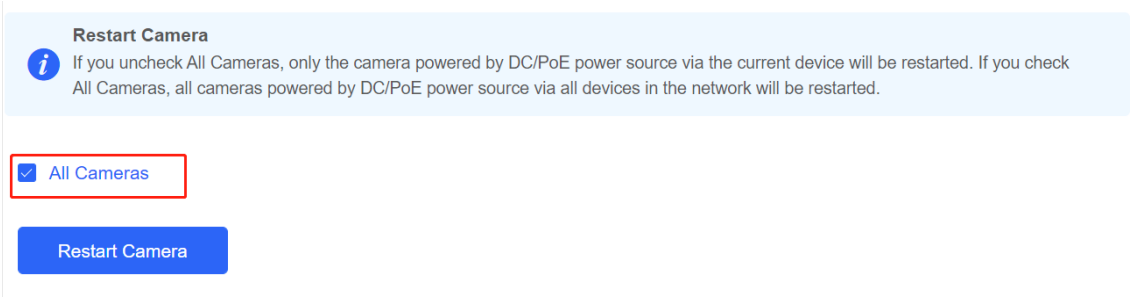
Please keep the device powered on during reboot. Otherwise, the device may be damaged.

## 6.5 Rebooting the Camera

### 6.5.1 Rebooting All Cameras

Choose **Advanced** > **Restart Camera**.

You can reboot all cameras by check **All Cameras** and then clicking **Restart Camera**.




**Caution**

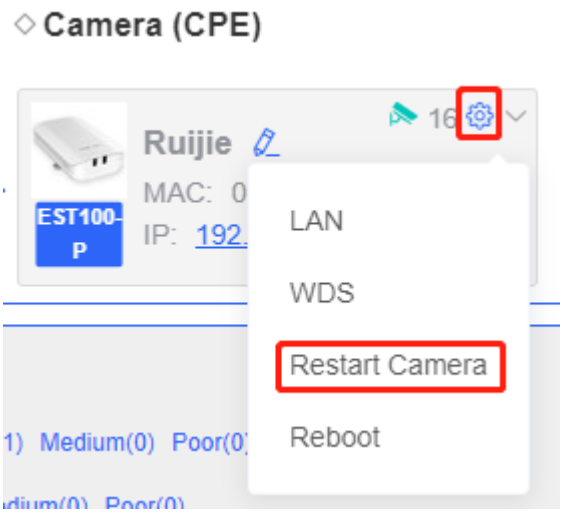
Only the cameras connected to the online devices supporting this function will be restarted.

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

### 6.5.2 Rebooting a Specific Camera

Choose **Overview** > **WDS Group Info** > **NVR (AP)/Camera (CPE)**.

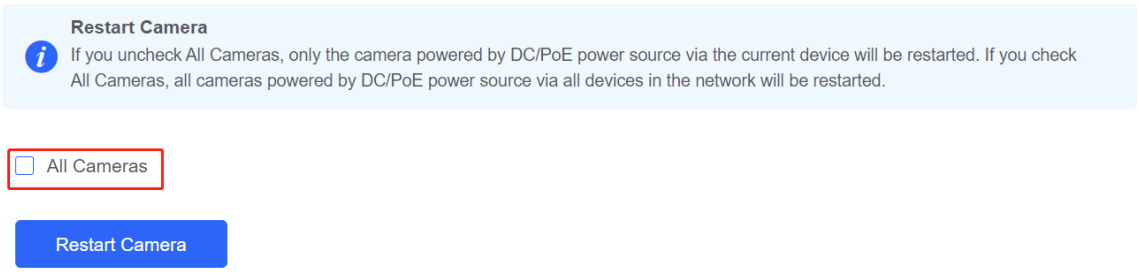
You can restart a specific camera by clicking and selecting **Restart Camera**.




### 6.5.3 Rebooting the Camera Connected to the Current Device

Choose **Advanced** > **Restart Camera**.

Uncheck **All Cameras** and click **Restart Camera**.

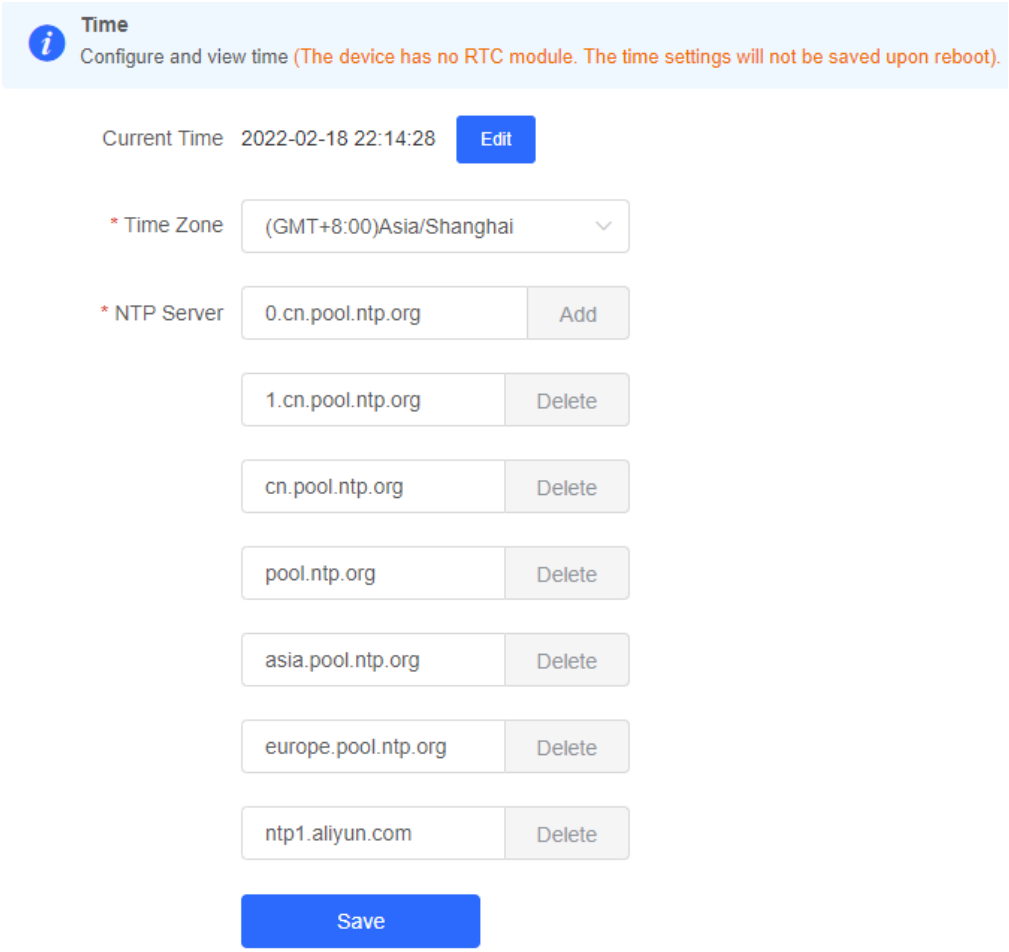



**Note**

## 6.6 Only EST100-P and EST100-D support camera restart. Configuring System Time

Choose **System Tools** > **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.

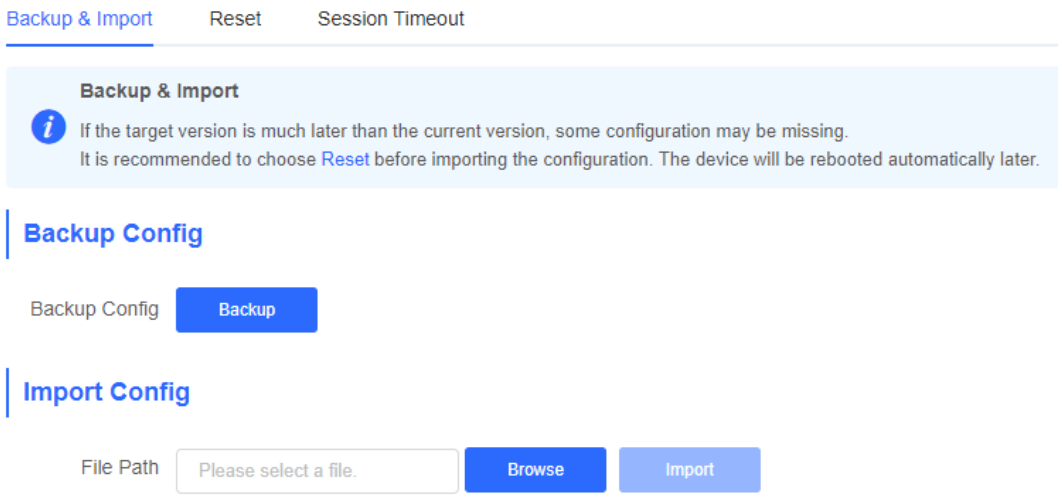


# 6.7 Configuring Config Backup and Import

Choose **System Tools** > **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.




# 6.8 Performing Update and Displaying the System Version

## 6.8.1 Online Update

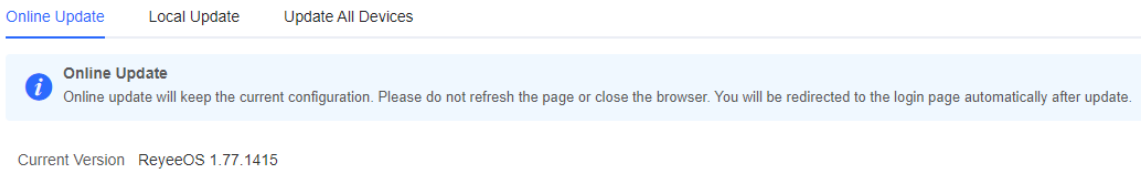
Choose **System Tools** > **Update** > **Online Update**.

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.

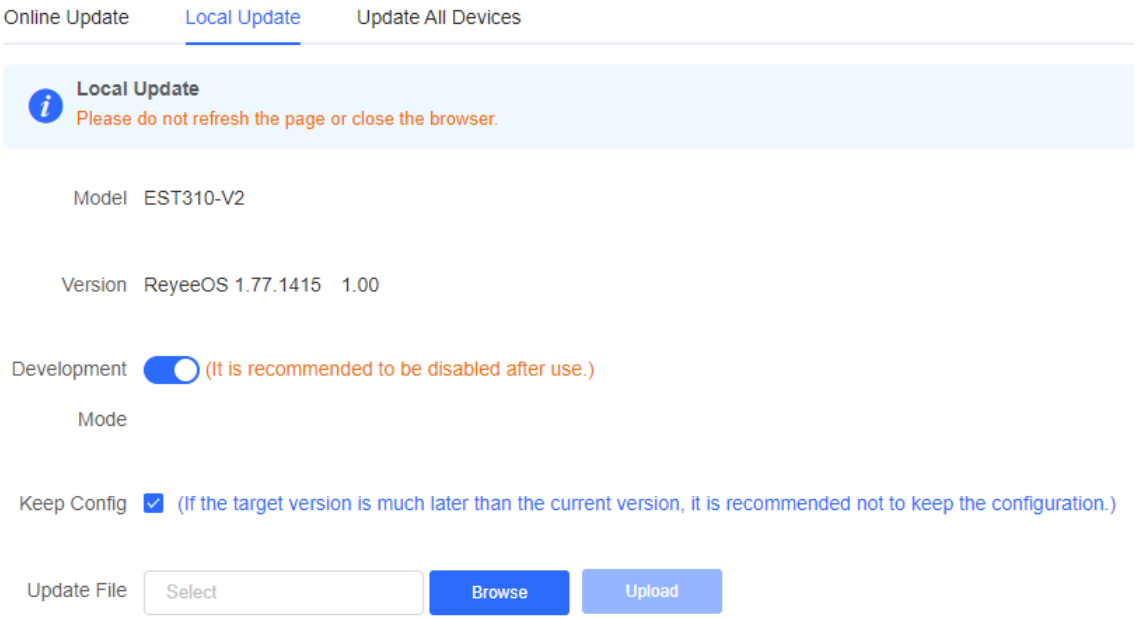
If no version update is detected or online update cannot be performed, check whether the bridge is connected to the Internet.




## 6.8.2 Local Update

Choose System Tools > **Update** > **Online 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**

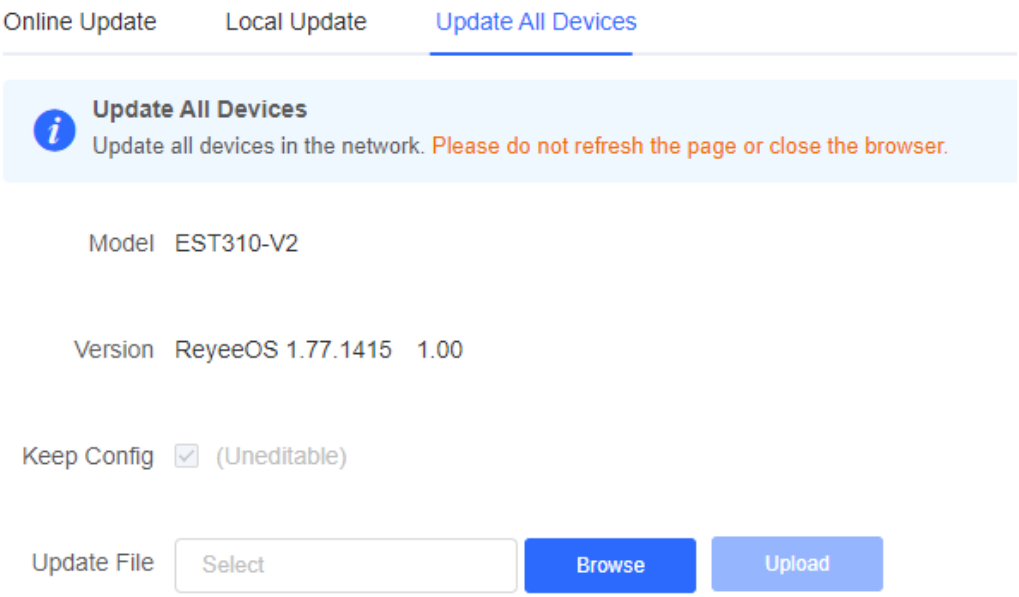
After being updated, the device will reboot. Therefore, exercise caution when performing this operation.

### 6.8.3 Update All Devices

Choose **System Tools** > **Update** > **Update All Devices**.

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

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

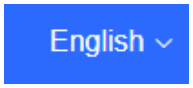



**Caution**

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

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

## 6.9 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.