HA3515-DG Access Point

MA_1.3(1)B9P1

Web-based Configuration Guide

Document Version: V1.0

Date: 2023.12.11

Copyright

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

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: http://caseportal.ruijienetworks.com
- Community: http://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

Conventions

1. Signs

The symbols used in this document are described as follows:

Caution

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

Note

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

Contents

Preface I
1 Overview of Web-GUI 1
1.1 Web-GUI 1
1.2 Configurable Functions on Web-GUI 1
1.3 Preparations before Web-GUI Connection 2
1.4 Preparation for Web-GUI Connection 2
1.4.1 Connection between the AP and the PC 2
1.4.2 Configuring the IP Address of PC 3
1.5 Web-GUI Login 4
1.5.1 Open WWW Browser 4
1.5.2 Measures for Certificate Error 5
1.5.3 Entering Username and Password 6
2 Quick Settings 7
2.1 Web-GUI Login 7
2.2 Dashboard 7
2.3 Configuring Wireless SSIDs 8
2.4 Configuring RF Parameters 12
2.4.1 Configuring RF Parameters on 2.4 GHz 13
2.4.2 Configuring RF Parameters on 5 GHz 14
2.4.3 Other Settings 15
2.5 Additional Instructions for Enterprises 16
2.5.1 Device Management 16
2.5.2 Access Point Mode 16
2.5.3 Routing Mode 17
3 Device Overview 19
3.1 Equipment Overview 20
3.2 Device Details 21
3.3 Wi-Fi Status 22
3.4 Interface Information 22
4 Basic Configurations 23
4.1 Basic Management 24
4.1.1 WAN Settings (Routing Mode) 24
4.1.2 LAN Settings (Routing Mode) 25
4.1.3 IPv6 Settings 27
4.1.4 Clients 28
4.1.5 Mode Switching 32
4.2 Wireless Management 33
4.2.1 Wireless Settings 33
4.2.2 Configuring RF Parameters 33
4.2.3 WPS 34
4.3 Network Management 35
4.3.1 VLAN 35
4.4 Behavior Management 36

4.4.1 Access Control 36
4.4.2 Security 38
4.5 Diagnostics 40
4.5.1 Network Tools 40
5 Advanced Management 42
5.1 User Isolation 42
5.2 IGMP Snooping 43
5.3 Acceleration Settings 45
5.4 DMZ (Routing Mode) 45
5.5 Port Mapping (Routing Mode) 46
5.6 UPnP (Routing Mode) 47
5.7 DNS Server 48
5.8 DHCP (Routing Mode) 49
5.9 Firewall (Routing Mode) 50
6 System Management 53
6.1 NTP Settings 53
6.2 Port Management 53
6.3 Login Management 54
6.3.1 Administrator Password 54
6.3.2 Session Timeout 55
6.3.3 Account Name 56
6.4 Configuration Management 56
6.4.1 Restore 56
6.4.2 Backup and Import 57
6.5 Reset Settings 60
6.6 LED Settings 60
6.7 Web CLI 62
6.8 System Log 62
6.9 System Upgrade 63
6.9.1 Manual Upgrade 63
6.9.2 G.hn Firmware Upgrade 65
6.10 Reboot 65
6.10.1 Reboot 65
6.10.2 Scheduled Reboot 66
6.11 Developer Mode 67
7 Troubleshooting 68
7.1 Failing to Connect to Web-GUI 68
7.2 Failing to Log into Web-GUI 68
7.3 Communication Failure 69
7.4 About Device Setup and Usage Support 69

1 Overview of Web-GUI

📖 This document is applicable only to HA3515-DG.

This chapter will provide an overview of Web-GUI from the following aspects:

- Web-GUI: The Web management system can be accessed through a WWW server (such as Google Chrome) to manage APs;
- Available Functions: This section briefly introduces the features that can be set via the Web-GUI, including SSID parameters, network configurations, security configuration, etc.;
- Preparation before Web-GUI Connection: This section introduces the materials required before connection and provides precautions;
- Preparation for Web-GUI Connection: This section introduces the connection between this device and the PC, the IP address setting and the Internet settings of the browser;
- Web-GUI Login: This section introduces the specific steps of Web login.

📖 Web-based management involves two parts: Web server and Web client. A web server is integrated into a device to receive and process requests sent from a client and returns the processing results. Generally, a Web client refers to a web browser like Firefox, Google Chrome, Safari.

📖 If the kernel version of the Microsoft Internet Explorer browser you are using is too low, the Web-GUI may experience slow response. Please roll back the interface or use other browsers. Google Chrome and Safari are recommended.

1.1 Web-GUI

This device can be configured through a WWW browser.

When logging into the Web-GUI, you can easily configure the AP without running commands in CLI (Command Line Interface). Almost all main functions can be set via Web-GUI.

1.2 Configurable Functions on Web-GUI

The main features that can be set via the Web-GUI are as follows:

- SSID Parameters: passwords, encryption modes, etc.
- 2. 4G/5G Parameter: channel, bandwidth, transmit power, etc.
- Network Configuration: WAN port, LAN, DHCP, etc.
- Security Configuration: black lists, white lists, user isolation, etc.
- AP Management: device upgrade, restart, etc.
- G.hn firmware upgrade.

1.3 Preparations before Web-GUI Connection

Please prepare the following materials before connecting to Web-GUI:

Materials	Description
Management Terminal	WWW Browser: Google Chrome, Firefox, Safari. Others: a PC with LAN port, or some other mobile terminal devices, such as laptops, iPads, mobile phones, etc. 🕮 It is recommended that the resolution settings are 1280*1024, 1920*1080 and 1440*960. At other resolutions, the page fonts and formats may be misaligned and not beautiful enough. For example, due to the smaller screen of mobile phone terminals, the interface layout and format may be misaligned, unsightly, and other abnormalities. 🕮 Due to the influence of WWW browsers, file uploads (updating program file versions, setting files) may fail. If it fails repeatedly, please try changing the WWW browser. We recommend Google Chrome, Firefox, and Safari. Internet Explorer or Microsoft Edge can also be used, but some functions may not be available, such as displaying English when the browser starts. 🕮 If you perform "Save Settings", "Save File" or "Return" while updating the screen, it may not function properly. Please perform the above operations after the screen update is completed.
Ethernet Cable	UTP/STP Category 5e or higher is recommended.

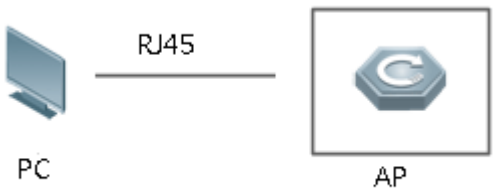
1.4 Preparation for Web-GUI Connection

This section describes how to connect to the Web-GUI via the PC. The operations are:

- Form the connection between the AP and a PC
- Set the IP address of the PC
- Set the Internet settings of a WWW browser

1.4.1 Connection between the AP and the PC

As shown in the figure below, the administrator can access the device through a browser and uses the WEB management system to configure the device.
The topology is shown as follows:



Use an Ethernet cable (RJ45) to connect this AP to the PC. Plug one end of the Ethernet cable connected to the PC into the LAN port of the AP until it clicks to the place.

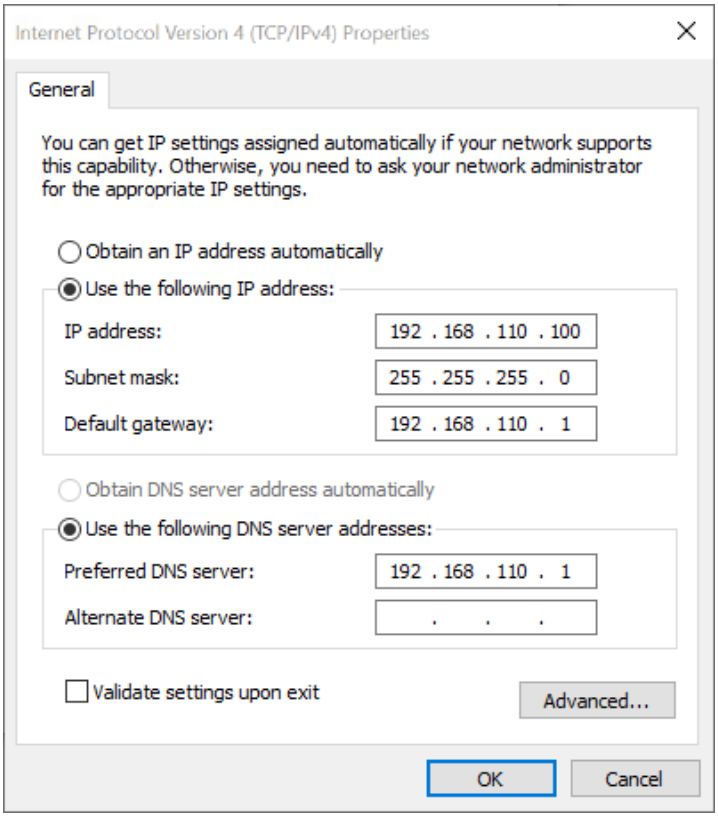
- For unplugging the Ethernet cable, hold the plug, press down on the plastic clip at the top of the plug, and pull the plug from port.
- Do not use a cable other than an Ethernet cable to connect the AP and the PC, otherwise it may cause the device to work abnormally or burned out.

1.4.2 Configuring the IP Address of PC

Set the IP address of the PC to an IP address that can connect to the HA3515-DG. The IP address configured varies from the working modes of AP.

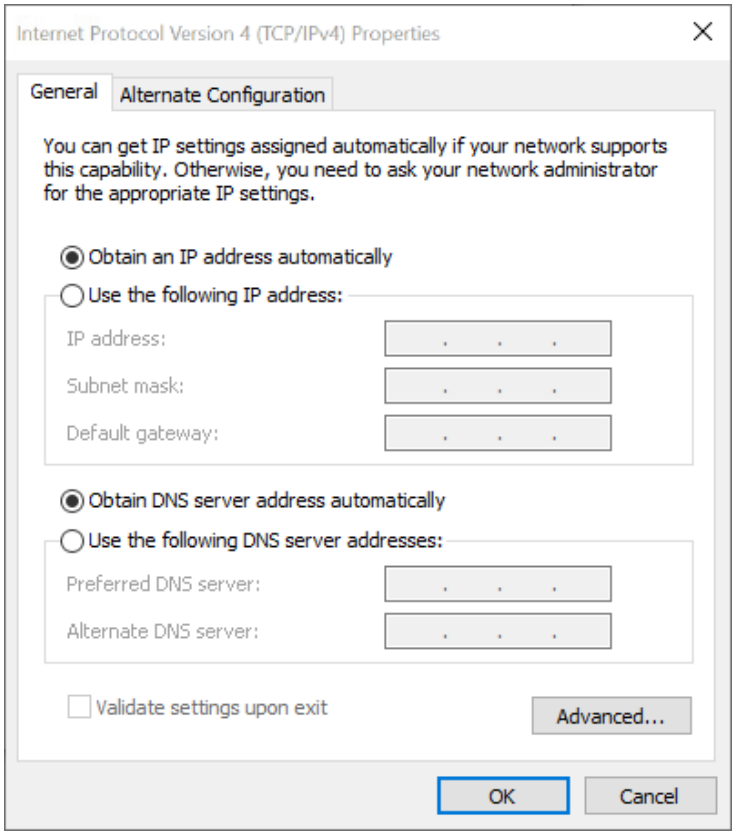
- AP Mode:

Select "Use the following IP address" in the page, set the IP address to 192.168.110.X (the value of X ranges from 100 to 200) and set the DNS server to 192.168.110.1. For example, set the fixed IP to 192.168.110.100 and the DNS server to 192.168.110.1.



- Routing Mode:

Select "Obtain an IP address automatically" in the settings.



1.5 Web-GUI Login

This section introduces the operation method of logging into the Web-GUI. The specific steps are:

- Open a WWW browser
- What to do when a certificate error appears
- Enter username and password

1.5.1 Open WWW Browser

Open a WWW browser of your PC and enter the following IP address or website. The default URLs are http://192.168.110.1 or https://rjap.jp.

🕮 It is recommended to use the default URL https://rjap.jp to access the Web.

🕮 Both http:// and https:// are supported to be connected to the Web-GUI.

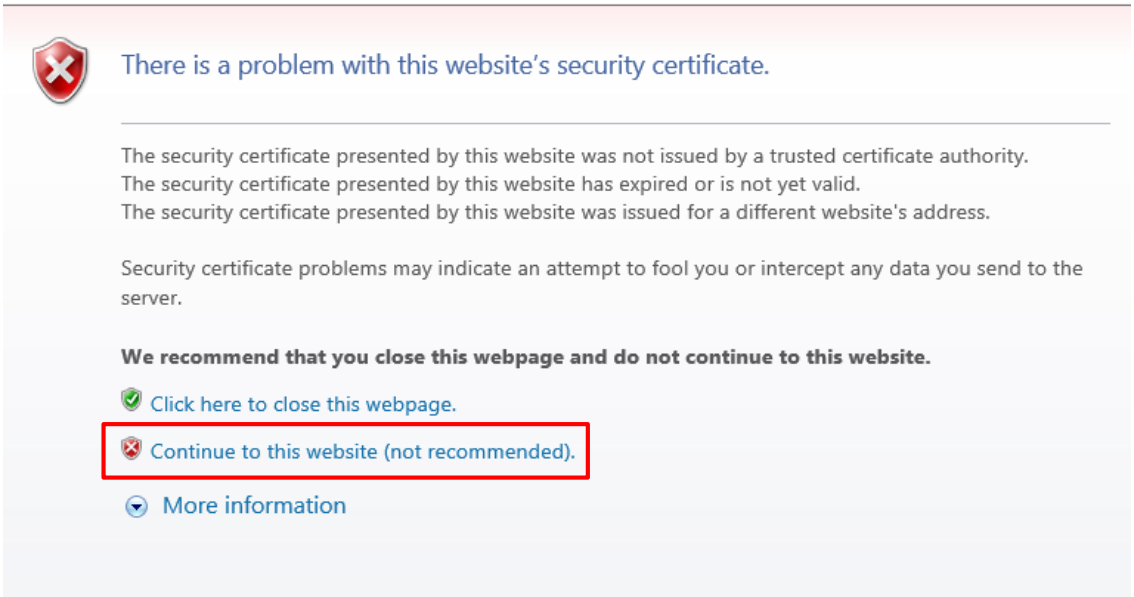
🕮 If users access the Web from the WAN port of the AP, the default URL cannot be used. Please use the IP address of the AP to access the Web via the LAN port.

🕮 If you want to check the IP of the WAN port IP, you can click “Basics”-> “WAN” in routing mode. In bridge mode, you can click “Basics” -> “External Network” to check.

- It is recommended to use Google Chrome, Firefox and Safari. When using other browsers to log into Web management, exceptions such as garbled characters or format errors may occur.
- In routing mode, if the "No WAN-Side Access" function is enabled and the whitelist IP is not configured, the AP's Web cannot be accessed through the WAN port. To address this issue, you can access the Web by connecting the SSID or via the LAN port, and then set the whitelist IP address.

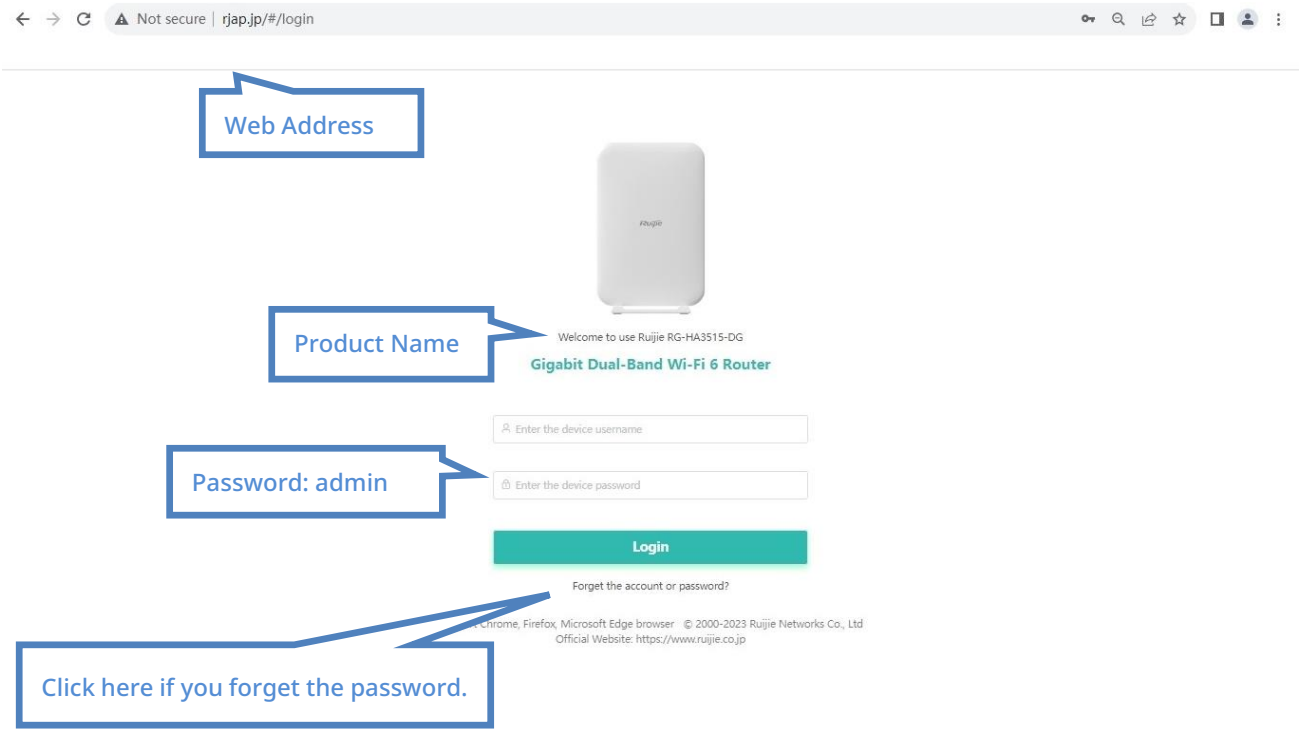
1.5.2 Measures for Certificate Error

A WWW browser may display the following warning message indicating that there is a problem with this website's security certificate. In this case, please click "Continue to this website (not recommended)" to continue browsing.



1.5.3 Entering Username and Password

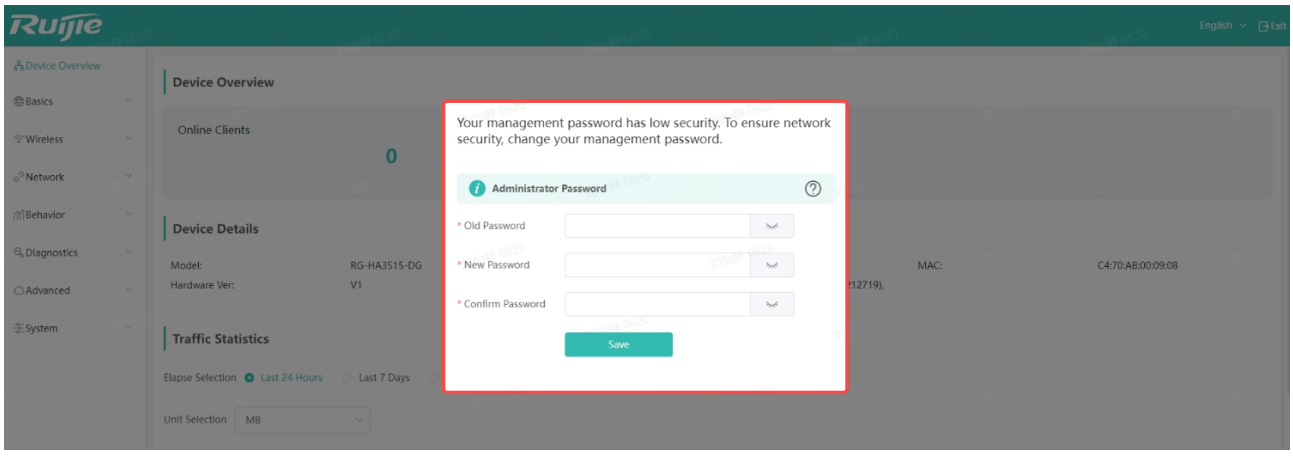
Enter your username and password and click “Login”.



Default username and password

Default Username / Password	Permission
admin/admin	Super administrator owning all permissions.

The initial password admin is only set for initial use. Since the security is very low, please set a new password after the following page pops up.



It is recommended to set a strong password. The length of a strong password should be more than 6 characters and formed by uppercase, lowercase and numbers.

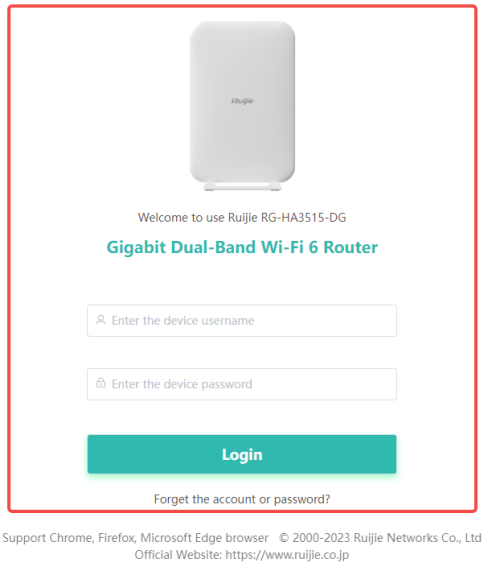
2 Quick Settings

This chapter will introduce how to quickly configure the device, which includes:

- Web-GUI Login: Users can use the default password admin to log into the Web;
- Dashboard: The dashboard displays multiple system information to users;
- Configure wireless SSID: When the dual band is configured, up to 6 SSIDs can be set;
- Wireless RF Parameters: Users can not only set the parameters of 2. 4 GHz and 5 GHz, but also configure some items, such as the number of online terminals, signal switching and the interval for automatic signal switching;
- Additional Instructions for Enterprises: An introduction to device management, AP mode configuration and routing mode configurations are provided;

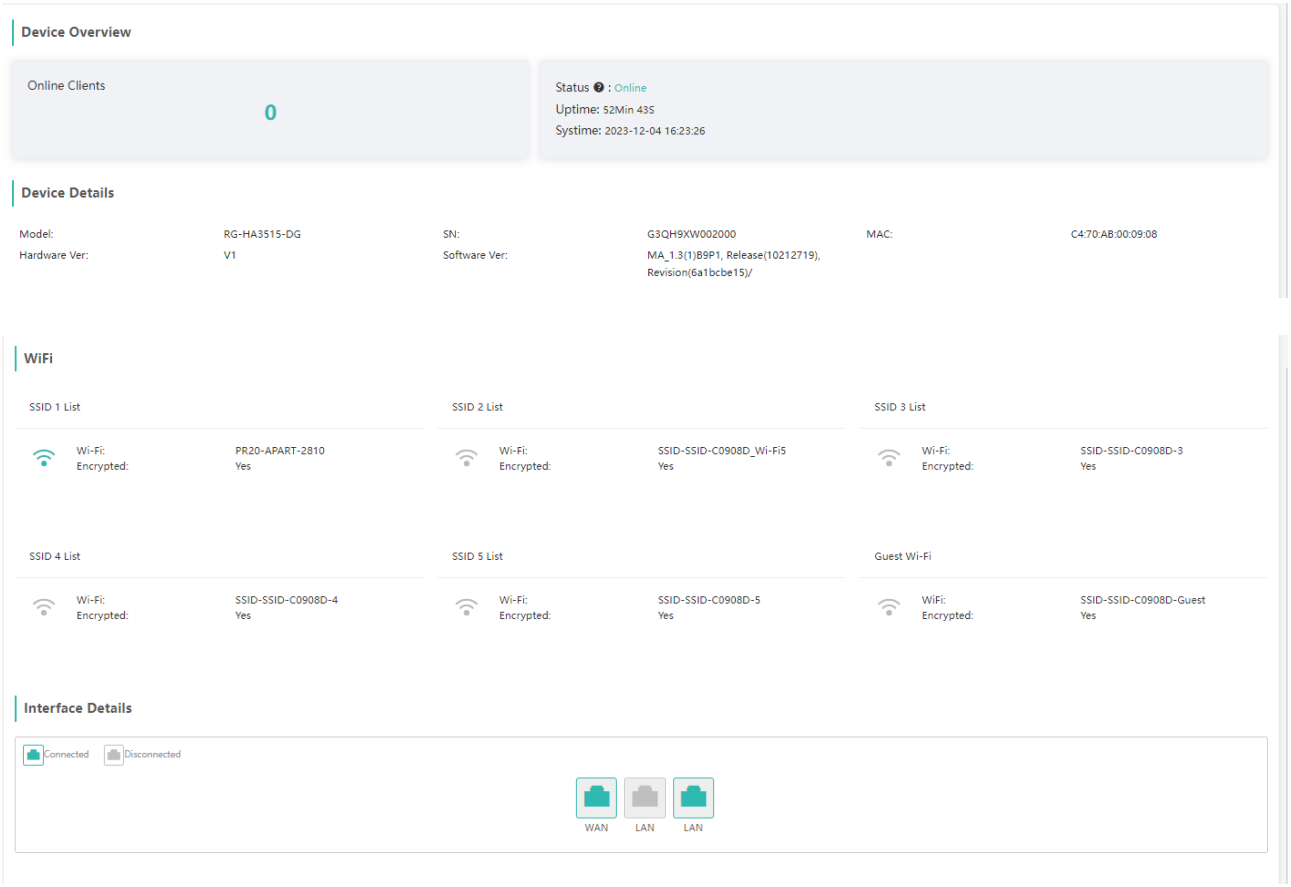
2.1 Web-GUI Login

Use the default password admin to log into the Web page



2.2 Dashboard

When you log into the Web management system, the dashboard will be displayed. On the dashboard, you can see several system information.



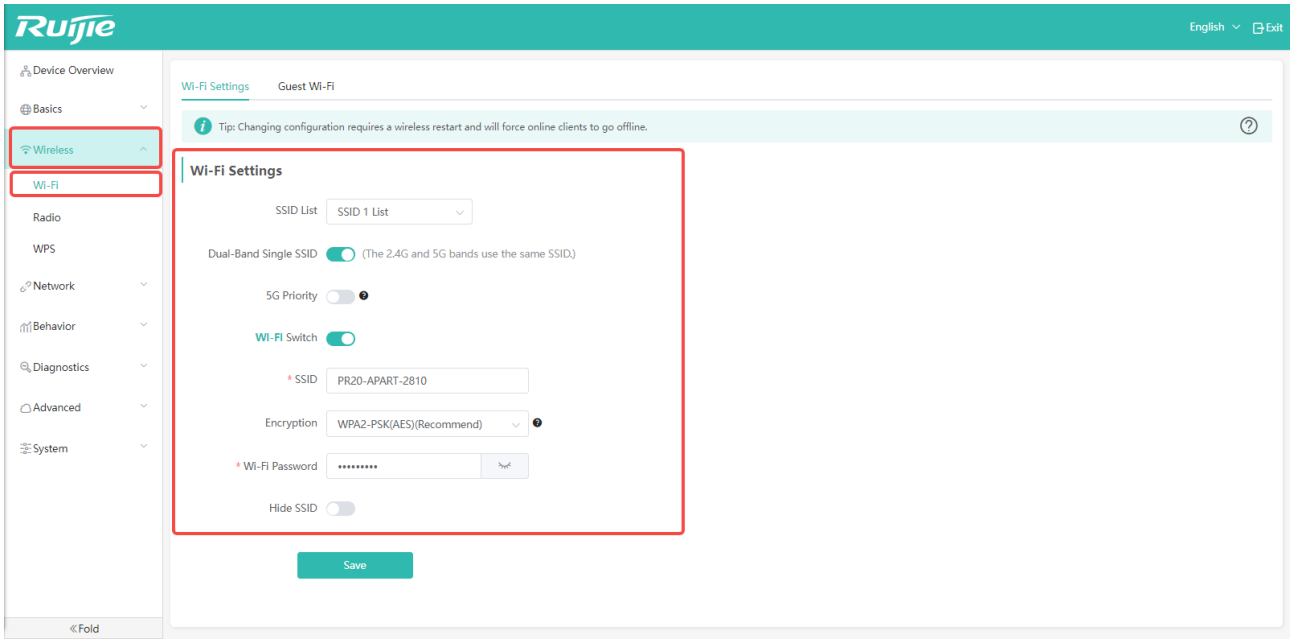
2.3 Configuring Wireless SSIDs

On the Web management system, you can configure wireless SSIDs. For a dual band integration, up to 6 SSIDs can be configured, of which one is specifically used for a guest network and the other five are universal.

Follow the following steps to configure wireless SSIDs:

Step 1: Click the “Wireless” in the left navigation bar (marked "1" in the figure);

Step 2: Click "Wi-Fi" (marked "2" in the figure), and then click "Wi-Fi Settings".

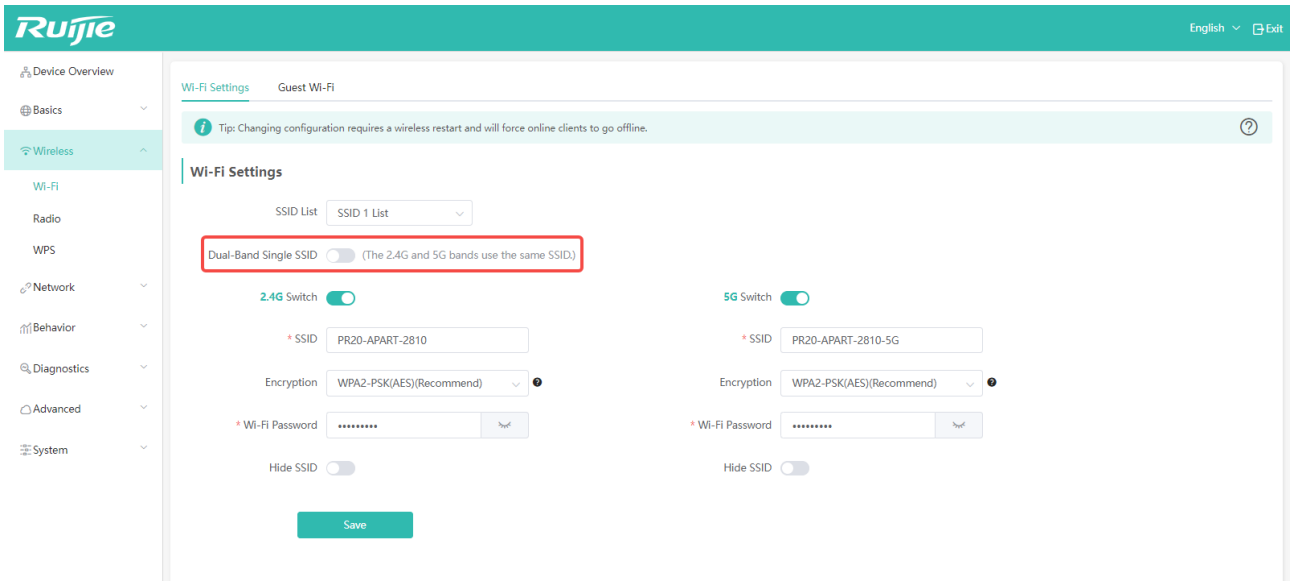


The configuration items are shown as follows:

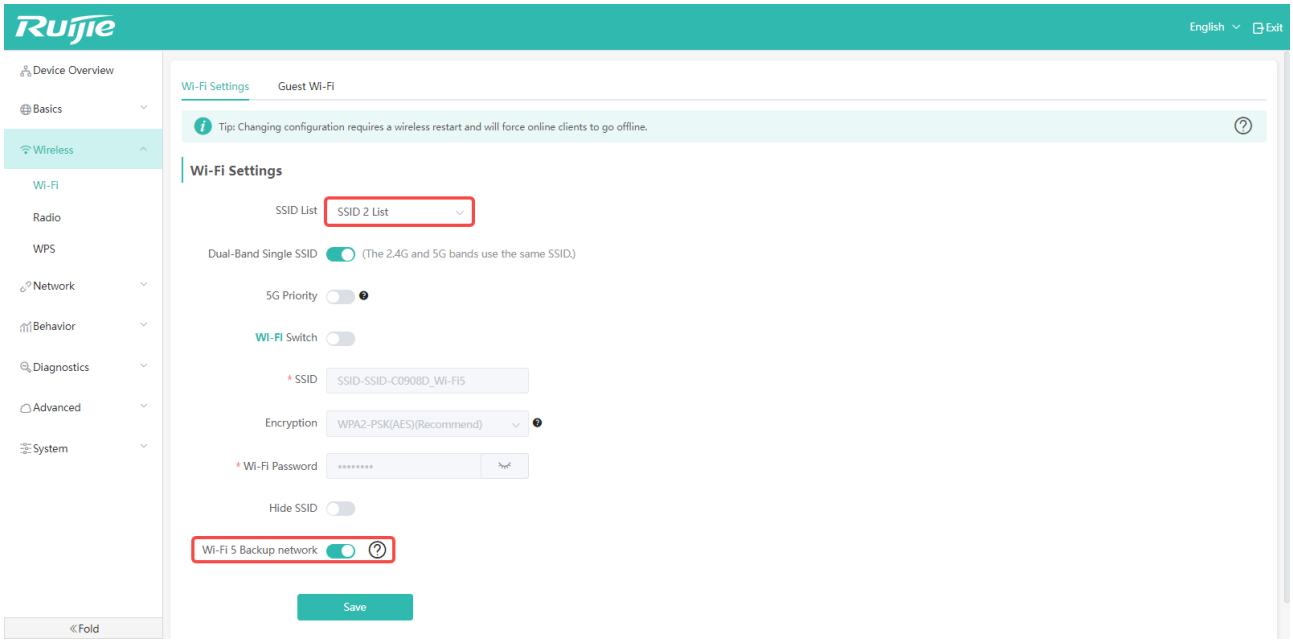
Items	Description	Default/Options
SSID List	Select the SSID list to be configured. Up to 5 SSID lists can be configured with different SSID names at the same time.	Default: SSID 1 List Option: SSID 1 List to SSID 5 List.
Dual-Band Single SSID	Choose whether to use the same SSID on 2.4GHz and 5Ghz. If it is disabled, you can configure different SSIDs on 2. 4GHz and 5GHz.	Default: Enabled (the same SSID is used for 2.4 GHz and 5 GHz) Option: Enabled/Disabled
5G Priority	When 5G priority is enabled, it will give priority to guiding terminals to access the 5G channel. ※It is important to note that the 5G priority function will take effect throughout the entire machine. That is to say, after 5G priority is enabled on a SSID, it takes effect globally, even if it is not enabled on the rest of SSIDs.	Default: Disabled Option: Enabled/Disabled
Wi-Fi Switch	If this switch is off, the SSID is turned off.	Default: SSID 1 list is enabled by default, and SSID 1 list to SSID 5 list is disabled by default.
SSID	Set a SSID name.	Default: A random value on the device's sticker ※ The name cannot exceed 32 characters.
Encryption	Specify an authentication method. OPEN: It requires no password which means anyone can connect to the SSID. WPA-PSK (TKIP): It is an earlier security protocol that evolves from the WEP (Wired Equivalent Privacy). Due to its low security, it is only suggested to be used on some early	Default: WPA2-PSK(AES) Options: WPA2 -PSK(AES) WPA3-SAE(AES) WPA2-PSK & WPA3-SAE (AES) Open (None) WAP-PSK & WPA2-PSK(AESTKIP)

	terminal devices that supports WPA. WPA2-PSK: It is a higher security protocol based on the WPA-PSK. It is designed for home users and small offices to protect their networks. WPA/WPA2-PSK: It is a mixed mode of WPA-PSK and WPA2-PSK, and is backward-compatible, which means it can be operated on terminals that do not support WPA2. WPA3-SAE: It is an overall improvement over its iteration, WPA2. It provided more personalized settings to deliver a higher security. But it only can be used on the devices that support WPA3. WPA2-PSK & WPA3-SAE : It is a mixed mode of WPA2-PSK and WPA3- SAE, and is backward-compatible, which means it can be operated on terminals that do not support WPA3.	WPA-PSK(TKIP)
Wi-Fi Password	The length of a SSID password must be formed by at least 8 characters. For security reasons, we recommend that you change the initial password.	Default: A random value printed on the device's sticker.
Hide SSID	Sometimes for security reasons, you can hide the SSID so that others cannot search for the SSID name. However, when you search the SSID via your mobile phone, it can be found and connected. When the SSID is hidden, the terminals that have connected to it will not be affected.	Default: Disabled. Option: Enabled/Disabled

When you disable "Dual-Band Single SSID", the following page is displayed. In this page, you can configure 2.4GHz and 5GHz bands separately.



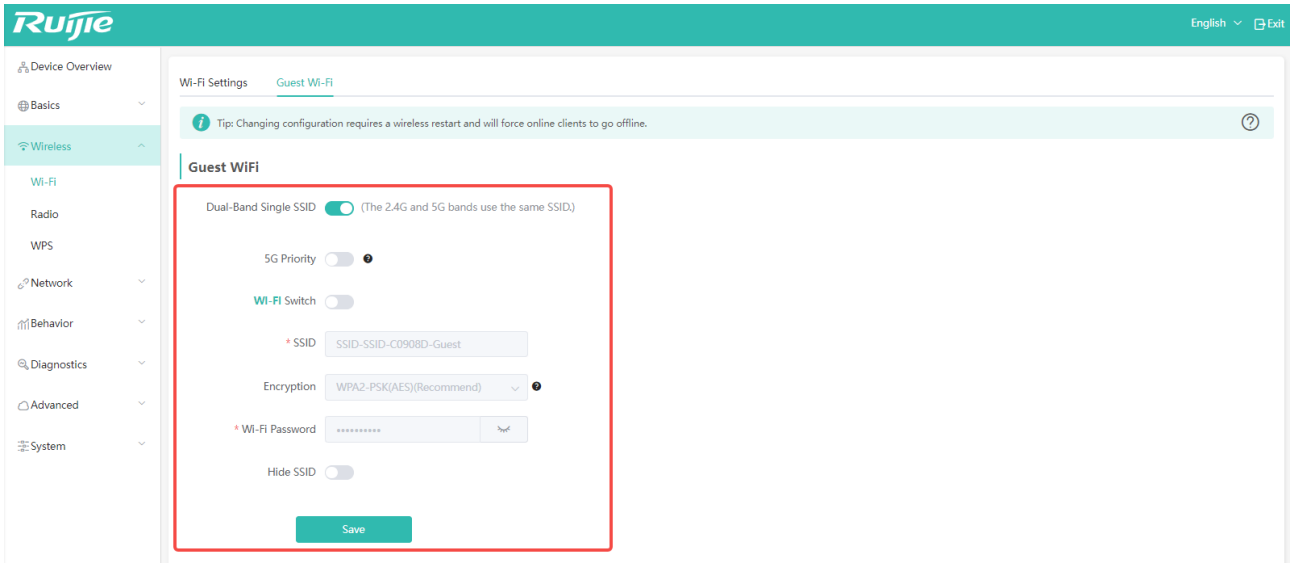
When the SSID 2 list is configured, an additional item will be provided as shown in the red box in the figure below (Wi-Fi 5 Backup network):



This item is only applicable to the SSID 2 list.

Items	Description	Defaults/Options
Wi-Fi 5 Backup network	This AP is an 802.11ax (Wi-Fi 6) device. Although the 802.11ax standard supports being compatible with the 802.11ac (Wi-Fi 5), there are still a small number of laptops and other terminals that cannot be connected to the Wi-Fi 6 signal released by this device due to their old drives. When this feature is enabled, these terminal devices can be connected to the Wi-Fi 5 signal. But they will not be able to take advantage of the new features brought by Wi-Fi 6 devices.	Default: Enabled Option: Enabled/Disabled

Under the "Wi-Fi" menu, in addition to the "Wi-Fi Settings" tab page, there is also a "Guest Wi-Fi" tab page.



All the configurable items on this tab page are the same as the configurable items on the SSID 1 List~ SSID 5 List in "Wi-Fi Settings". The difference is that the signal emitted by this SSID is exclusively for guests. After they are associated with this SSID, they cannot access the local network in routing mode, but only the Internet.

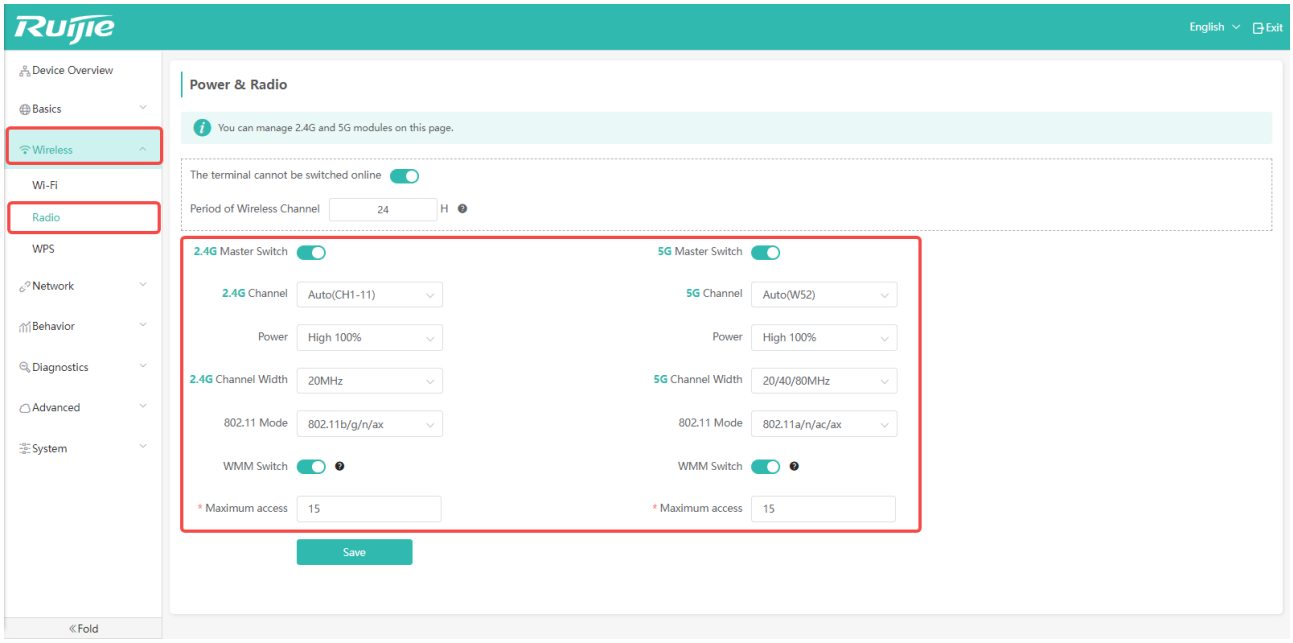
2.4 Configuring RF Parameters

This feature can be configured for 2. 4 GHz and 5 GHz.

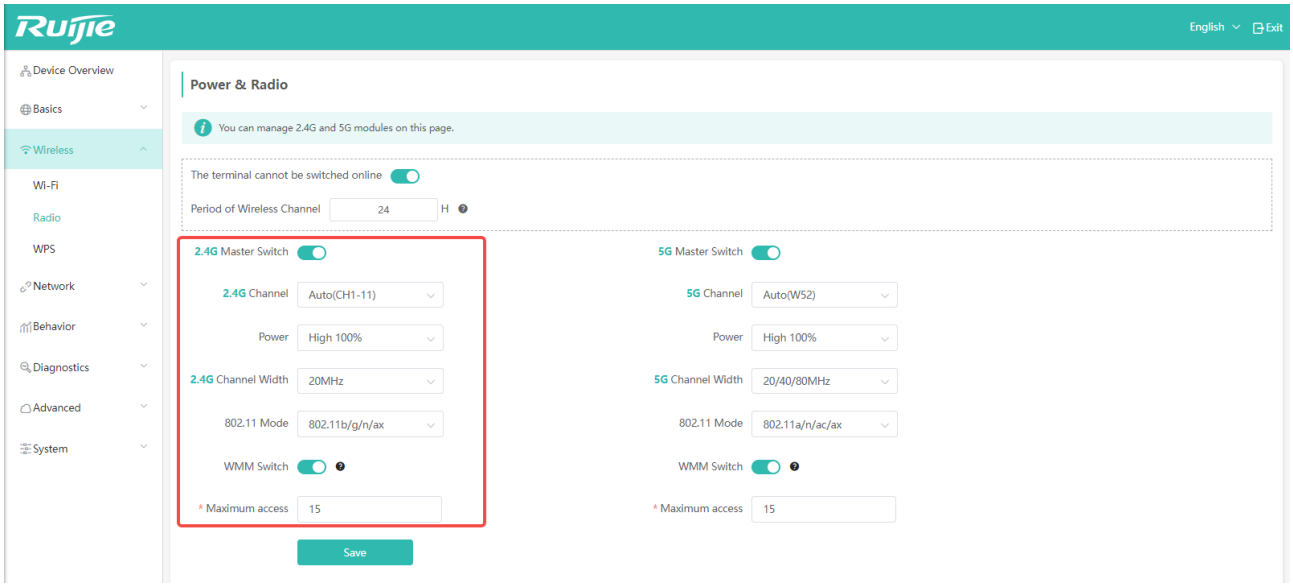
- The specific steps are:

Step 1: Click "Wireless" on the Web (marked "1" in the picture);

Step 2: Click "Radio" (marked "2" in the picture) to go to the setting page.

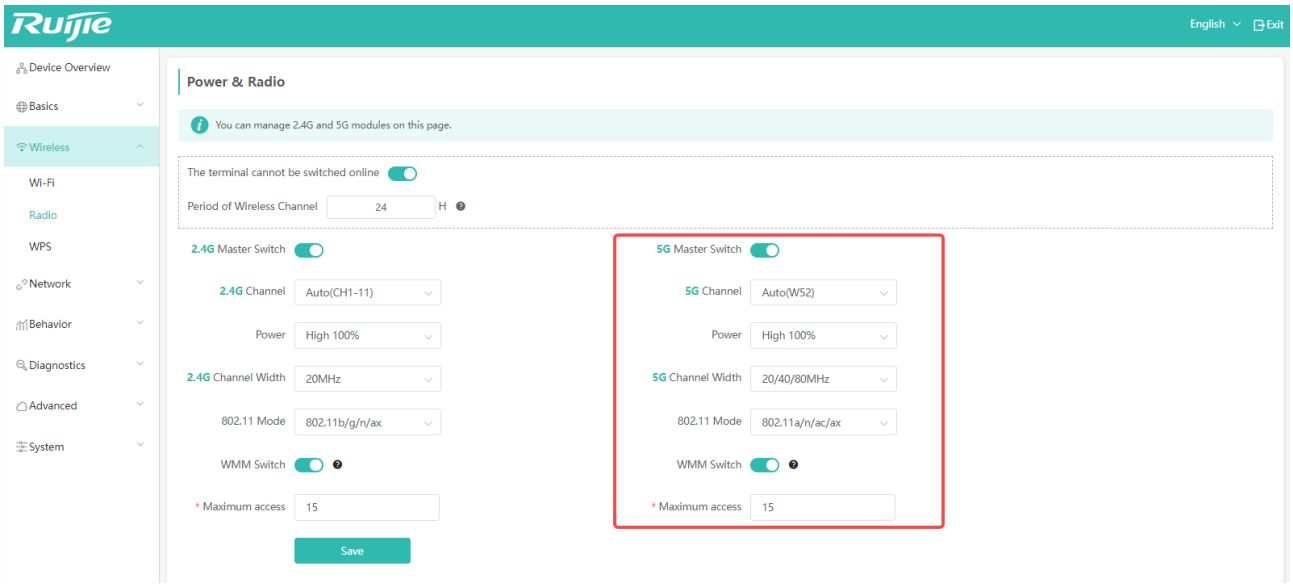


2.4.1 Configuring RF Parameters on 2.4 GHz



Items	Description	Defaults/Options
2.4G Master Switch	Used to determine whether to release the 2.4 GHz signal. If is disabled, the 2. 4 GHz signal is not released.	Default: Enabled Options: Enabled/Disabled.
2.4G Channel	Set the channel on 2. 4 GHz. You can choose a fixed channel, or choose to automatically select within the channel range 1-11 or the channel range 1-13 .	Default: Auto (CH1-11). Options: Automatic(CH1-11),Auto(CH1-13), 1,2,3,4,5,6,7,8,9,10,11,12,13
Power	Set the transmit power of 2. 4 GHz signal.	Default: High 100% Options: High 100%, Medium 60%, Low 40%
2.4G Channel Width	Configure 2.4GHz bandwidth. You can choose a fixed bandwidth or an automatic bandwidth of 20/40MHz.	Default: 20 MHz Options: 20 MHz, 40 MHz, 20/40 MHz
802.11 Mode	Set the wireless working mode of 2. 4 GHz.	Default: 802.11b/g/n/ax Options: 802.11b/g/n/ax, 802.11b/g/n, 802.11b/g
WMM Switch	When it is enabled, the better quality of multimedia is provided. We recommend turning it on.	Default: Enabled Options: Enabled/Disabled.
Maximum Access	Maximum number of terminals supported on 2.4GHz.	Default: 15 Options: 1-15

2.4.2 Configuring RF Parameters on 5 GHz

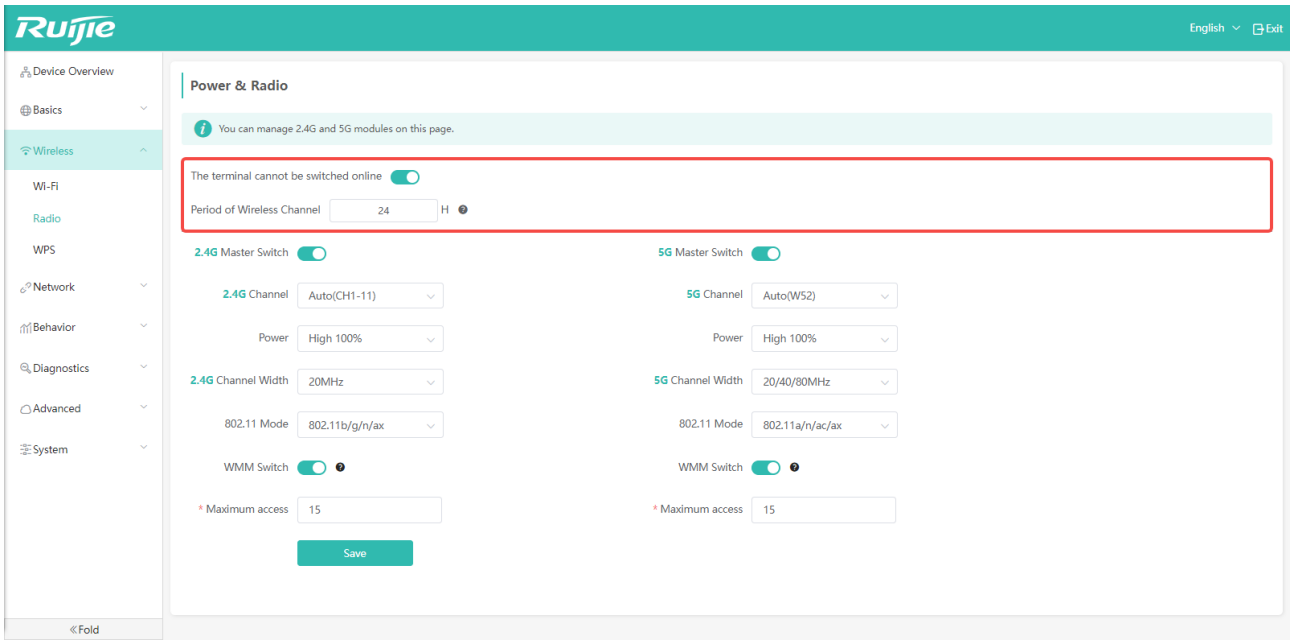


Items	Description	Defaults/Options
5G Master Switch	Used to determine whether to release the 5GHz signal. If is disabled, the 5GHz signal is not released.	Default: Enabled. Options: Enabled/Disabled.
5G Channel	Set the channel on 5GHz. You can choose a fixed channel, or choose to automatically select within the channel range 1-11 or the channel range 1-13 .	Default: Auto (W52). Options: Auto (W52), Auto (W52+ W53), Auto (W52+W53+W56), 36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140
Power	Set the transmit power of 5GHz signal.	Default: High 100% Options: High 100%, Medium 60%, Low 40%
5G Channel Width	Configure 5GHz bandwidth. You can choose a fixed bandwidth or an automatic bandwidth.	Default: 20/40/80MHz Options: 20MHz, 20/40MHz , 20/40/80MHz
802.11 Mode	Set the wireless working mode of 5 GHz signal.	Default: 802.11a/n/ac/ax Options: 802.11a/n/ac/ax, 802.11a/n/ac, 802.11a/n, 802.11a
WMM Switch	When it is enabled, the better quality of multimedia is provided. We recommend turning it on.	Default: Enabled. Options: Enabled/Disabled.
Maximum Access	Maximum number of terminals supported by 5GHz.	Default: 15 Options: 1-15

It should be noted that if the 5G channel is set to a fixed channel, automatic bandwidth switching will be used by default, but in fact the underlying algorithm of the AP does not currently support automatic switching between 20/40/80MHz.

2.4.3 Other Settings

After the automatic channel and automatic bandwidth settings take effect, the device will scan the channel and bandwidth according to the set period and reselect the optimal channel and bandwidth.

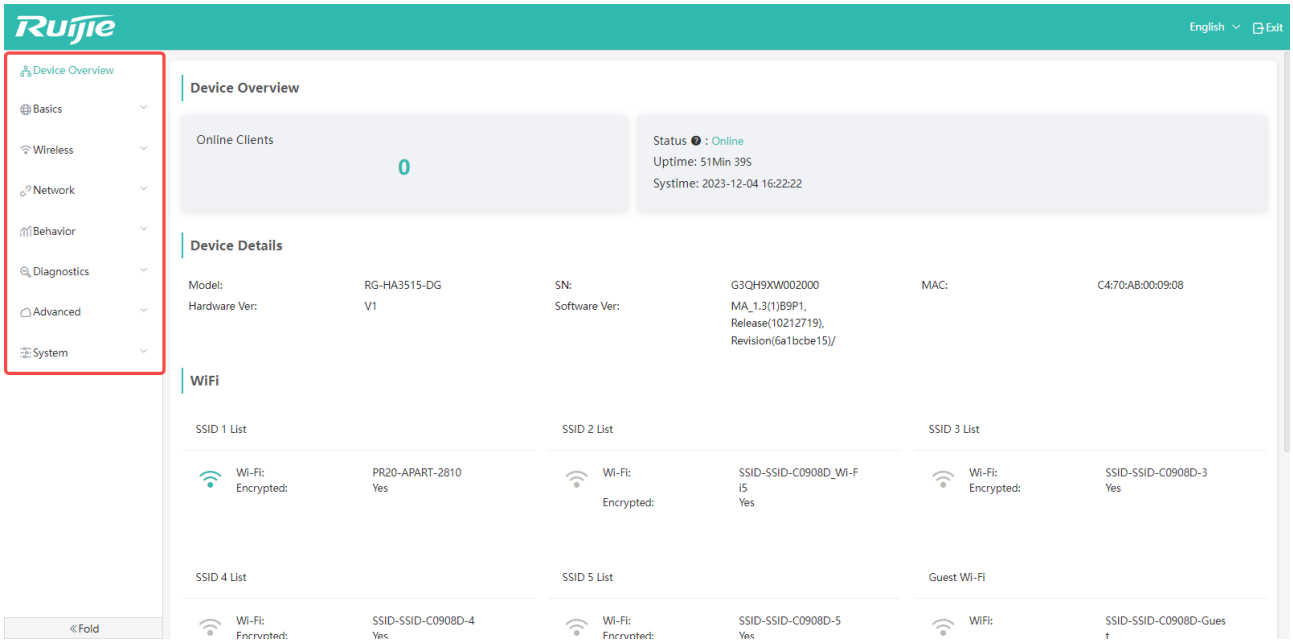


Items	Description	Defaults/Options
The terminal cannot be switched online	When a terminal is online, do not switch the channel and the bandwidth.	Default: On. Options: On/Off.
Period of Wireless Channel	Set the time interval for automatic channel switching. The default setting is to automatically select channels after each 24 hours.	Default: 24 hours. Options: 1-48 hours

2.5 Additional Instructions for Enterprises

2.5.1 Device Management

In the left panel of the Web, eight menus are offered to you to manage the AP.



2.5.2 Access Point Mode

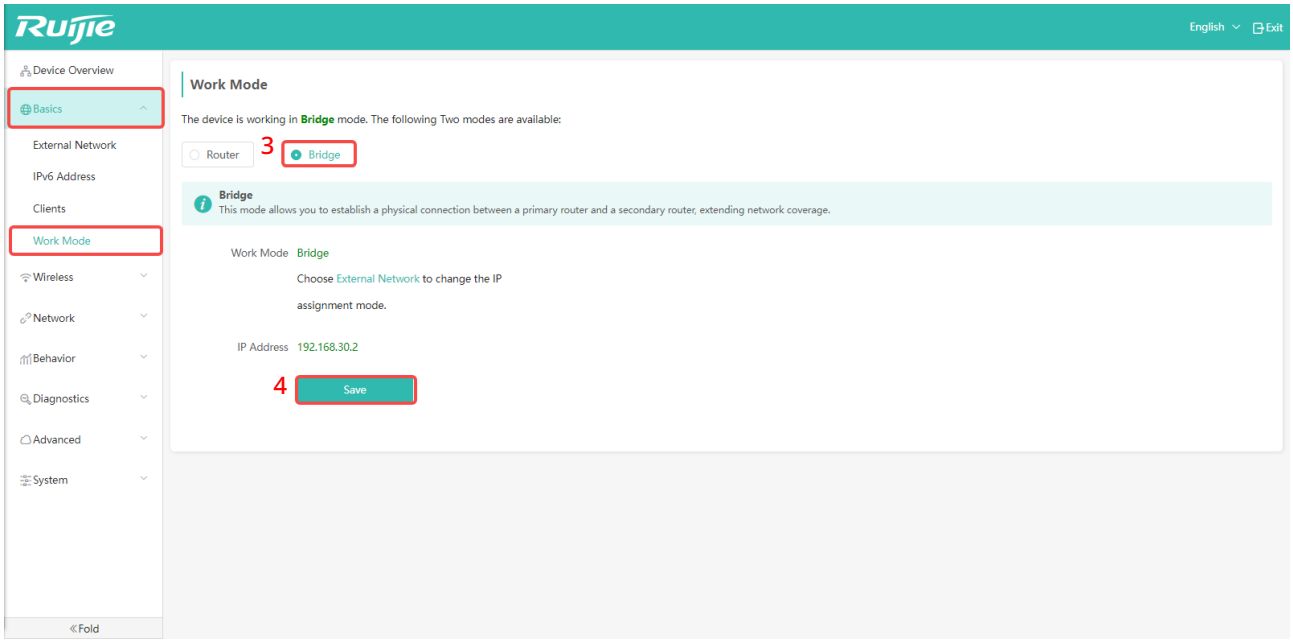
The following page allows you to set the device to the bridge mode.

- The specific steps are as follows:

Step 1: Click "Basic " in the left panel (marked "1" in the picture);

Step 2: Click on “Work Mode " (marked "2" in the picture);

Step 3: Select "AP Mode" (bridge mode) (marked "3" in the picture).

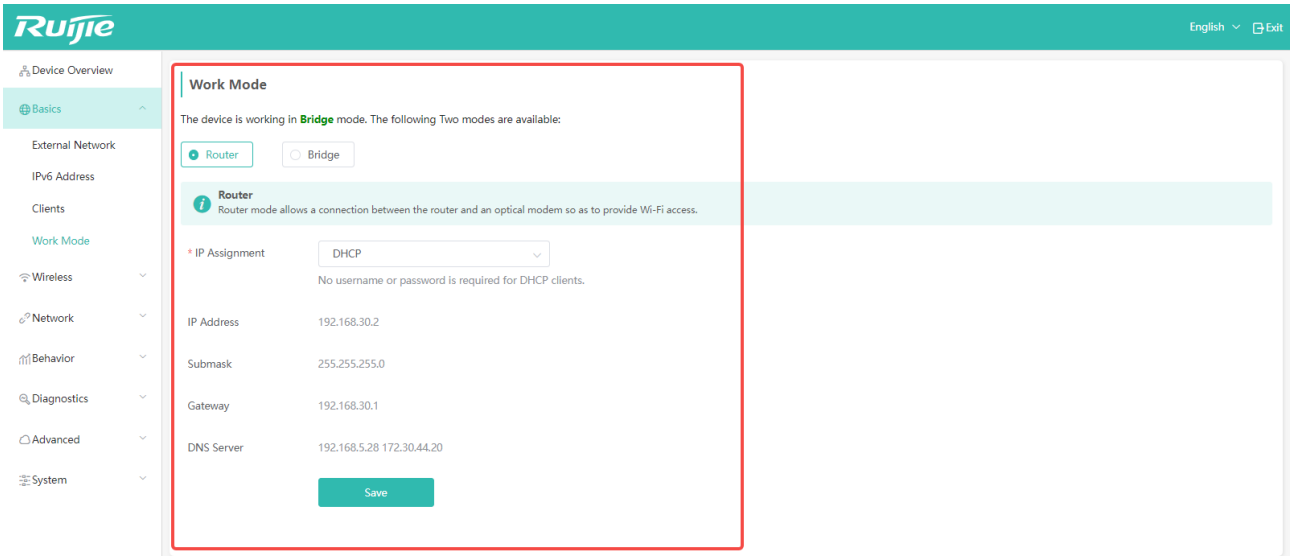


In bridge mode, the management address of 192.168.110.1 has been set for the device. In bridge mode, if the AP is not connected to the upper-level network, the downstream client will not be able to obtain DHCP. In this case, the client can configure an IP in the same network segment as the management address to access the Web homepage through this management address.

2.5.3 Routing Mode

- In bridge mode, a terminal such as a mobile phone can obtain IP addresses from the uplink network of the AP. If there is no uplink network or the uplink network does not assign an IP address, the terminal may not be able to access to the network. To address this issue, you can set the IP address to 1 92.168.110.x on your mobile phone or wired terminal, and then access the Web management system via 192.168.110.1.

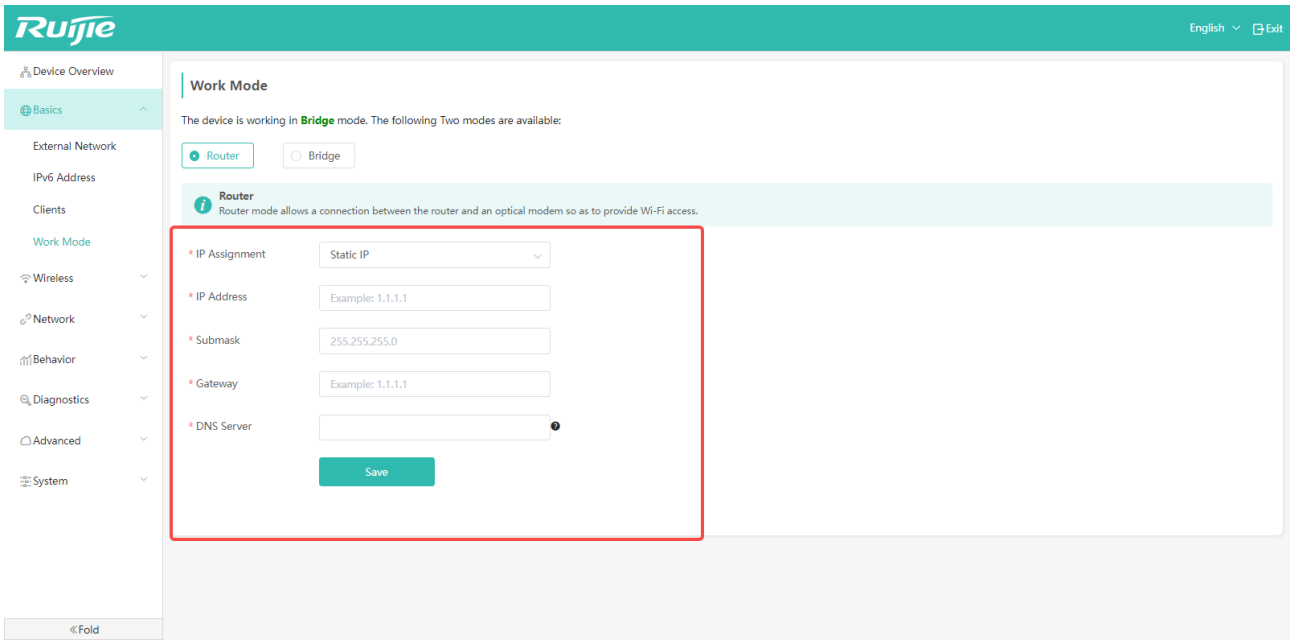
- In routing mode, a terminal such as a mobile phone can obtain an IP address in the network segment of 1 92.168.110.x by default. The terminal device can access the Web management system via 192.168.110.1 or http s:// rjap.jp. The configuration page of routing mode is shown as the following figure:



Items	Description	Defaults/Options
IP Assignment	Set the address assignment method of the AP to the terminal. DHCP and static IP are supported.	Default: DHCP Options: DHCP/Static IP

If DHCP is set, the address ranging from 192.168.110.100 to 192.168.110.200 will be assigned to the terminal, the default gateway is 1 92.168.110.1, and the default network mask is 255.255.255.0.

■ If you select the static IP, the setting page is shown as below:

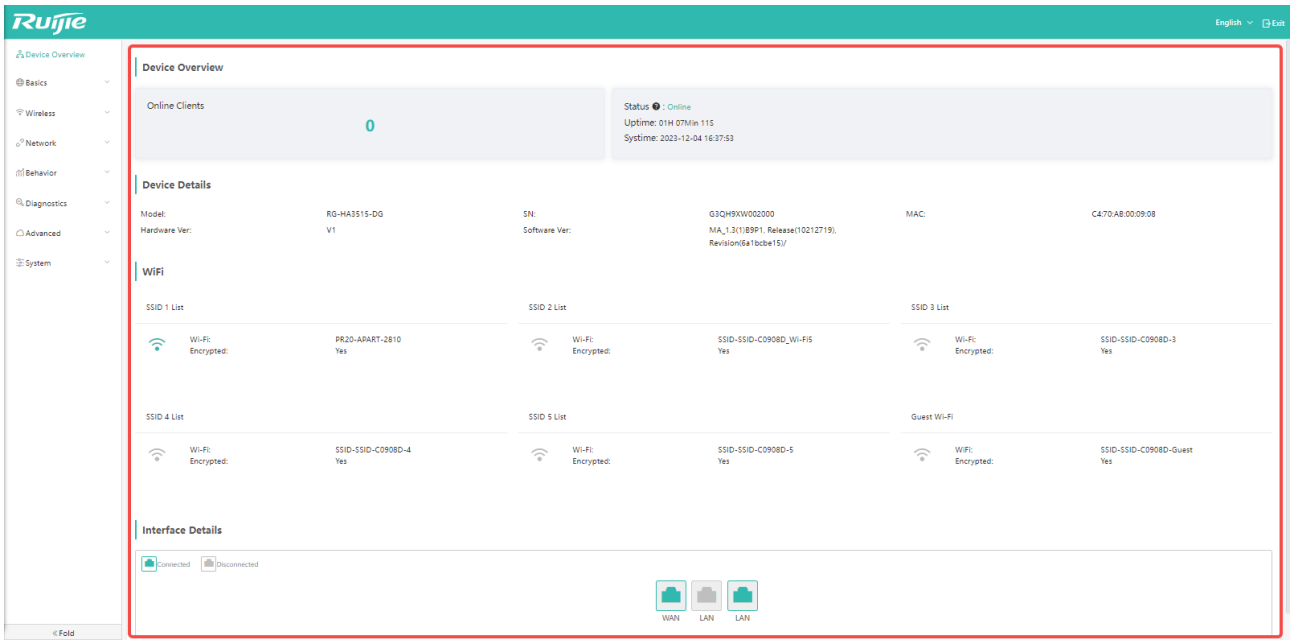


Items	Description	Defaults/Options
IP Assignment	Set an address allocation method of the AP to the terminal. DHCP and Static IP can be selected.	Default: DHCP Options: DHCP/Static IP ※ If you select the static IP, the AP will use the IP address configured by the user. In this case, users may need to configure their IP address to be in the same network segment as the AP to ensure they can log into the Web of AP again for configuration.
IP Address	Set an IP address for the AP.	Default : N/A
Submask	Set the subnet mask for the AP	Default : N/A
Gateway	Set the gateway address for the AP.	Default : N/A
DNS Server	Set the DNS server address for the AP.	Default: N/A

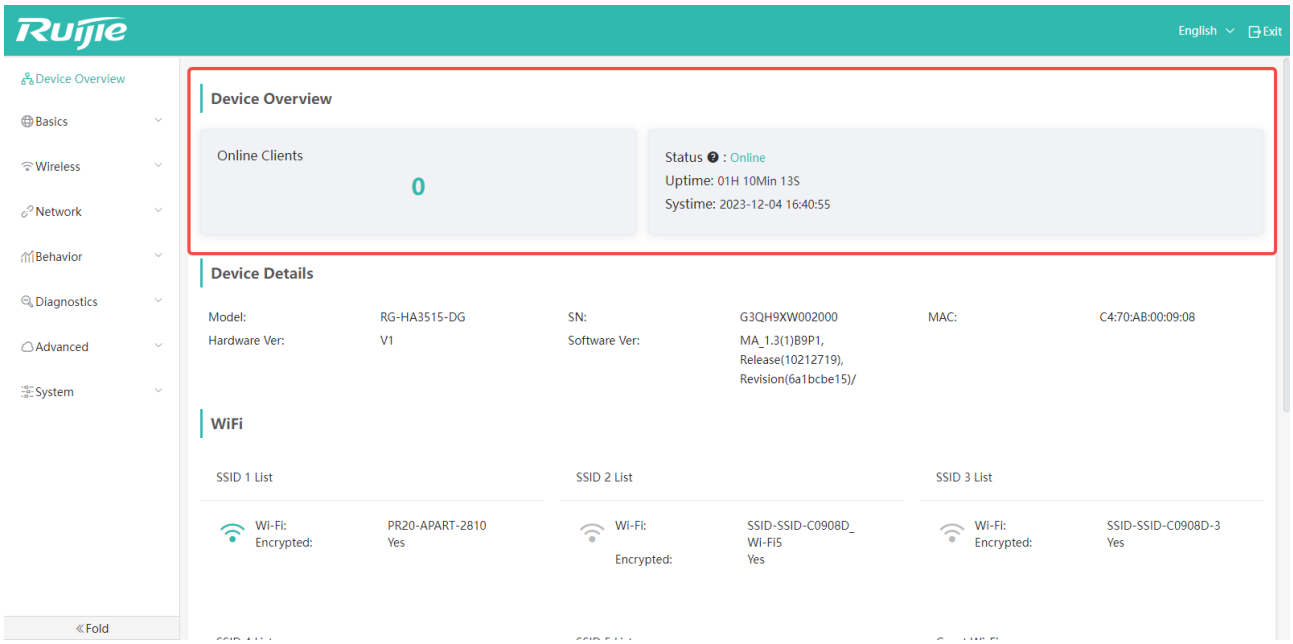
3 Device Overview

When users log into the Web management system, the device overview page is displayed. The overview page includes:

- Device Overview: Display the number of online users, network status and uptime.
- Device Details: Display the detailed information of the AP, such as its model, serial number, MAC address, hardware version, and software version information.
- WiFi: Display the detailed information of SSIDs, including SSID names, connection status, and encryption modes.
- Interface Details: You can check the connection status of a port by its color. When you move your mouse to the corresponding port, you can know the current rate of the port.



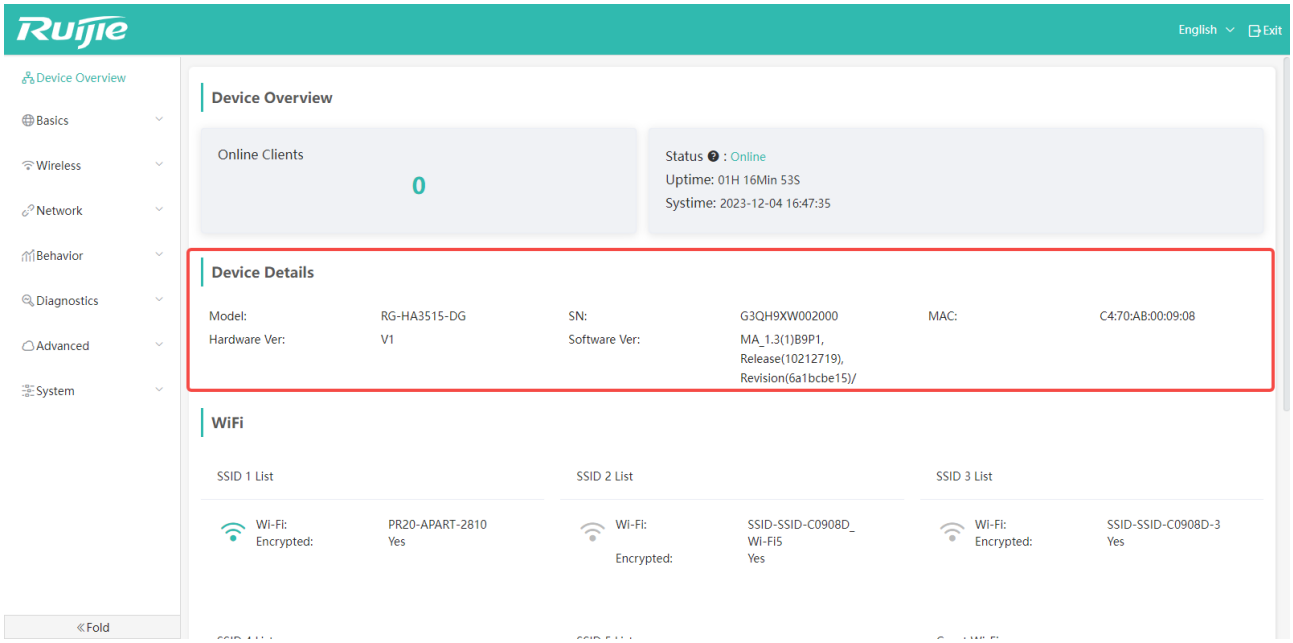
3.1 Equipment Overview



Items	Description
Online Clients	Display the number of current online wireless terminals.
Status	Display the status of Internet connection. Offline indicates that the Internet is not connected, and online means that the Internet is connected.
Uptime	Display the uptime of the device.
Systime	Displays the current time of the system.

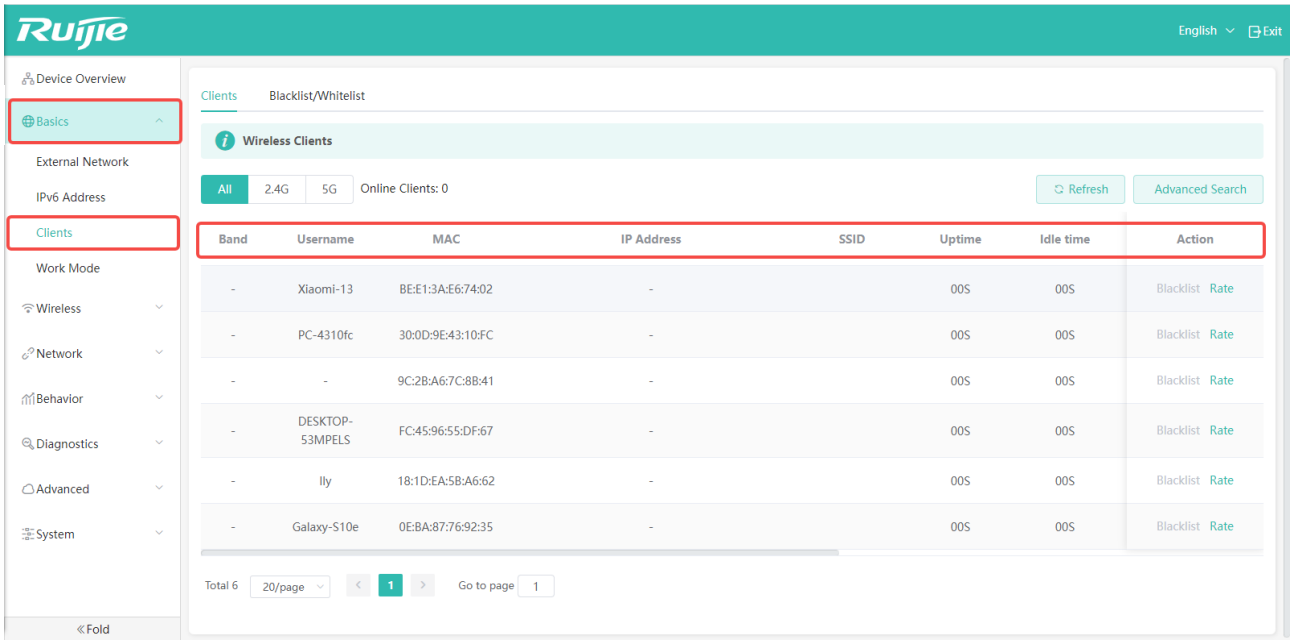
The offline status may be caused by network disconnection, DNS or other firewalls. You can re-obtain the status by refreshing the interface. If it is still displayed as offline, check whether the network connection is normal.

3.2 Device Details



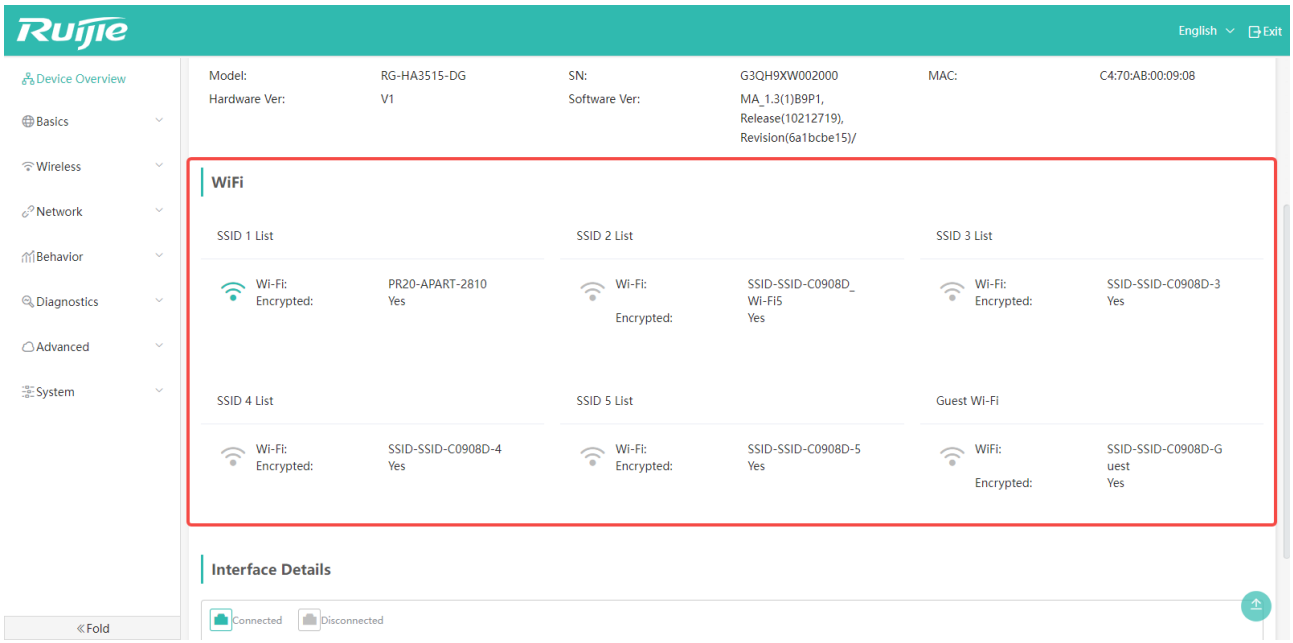
Items	Description
Model	Display the device model.
Hardware Version	Display the hardware version. The initial version starts from V1.
SN	Displays the SN of the device. A SN is an unique identifier for the equipment manufacturer to trace the product.
Software Version	Display the currently software version.
MAC	Display the MAC address of the device.

Click the "Basics" > "Clients" to view the terminal information connected to the AP. In this page, you also can view the IP addresses of clients.



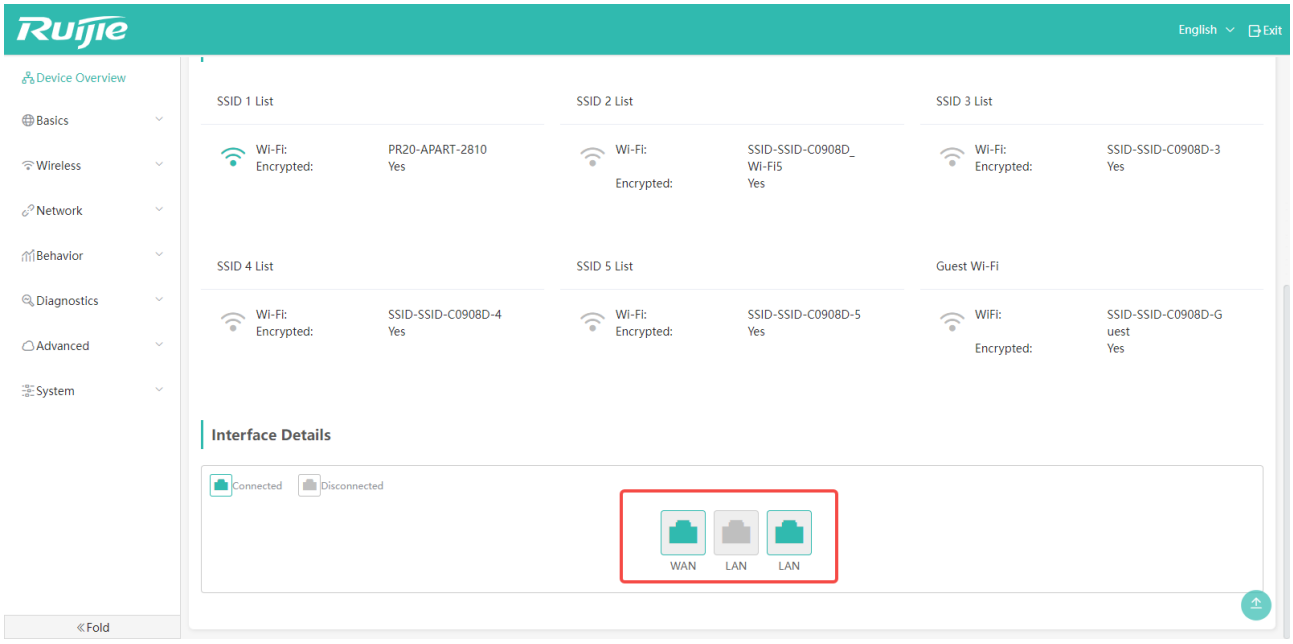
3.3 Wi-Fi Status

This area displays the detailed information about currently available SSIDs, including the SSID status and encryption modes. The system can be configured with up to 5 general SSID lists and a guest SSID. When clients access the guest SSID in routing mode, they only can access the external Internet. The example below shows that only the SSID 1 list is enabled. The SSID 1 list name is PR20-APART-2810, and it is encrypted.



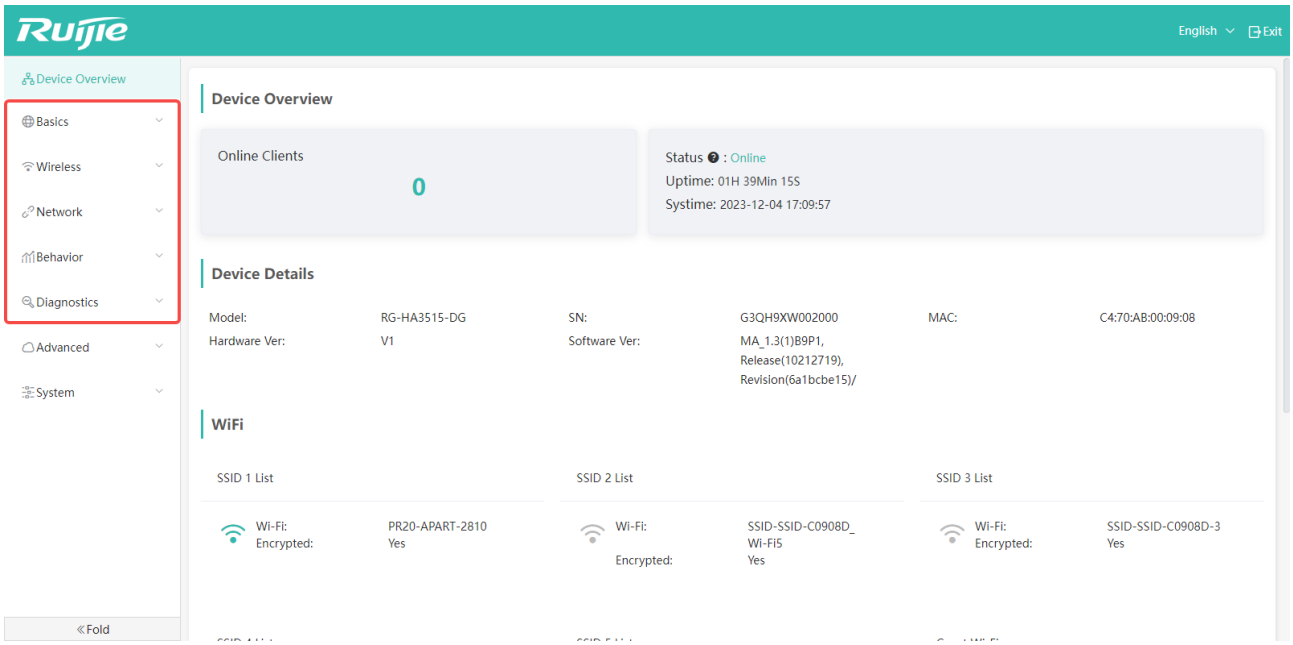
3.4 Interface Information

This area displays the current wired port status. As shown in the following figure, the system has three wired ports. The ports in green indicate that they are enabled, and the ports in gray indicate that they are disabled. Based on port color, we can know that the first and third ports are enabled.



4 Basic Configurations

The content introduced in this chapter is suitable for users who are familiar with AP configurations. Users can optimize their networks via configuring the following features.



The main menus of basic configuration are shown as follows:

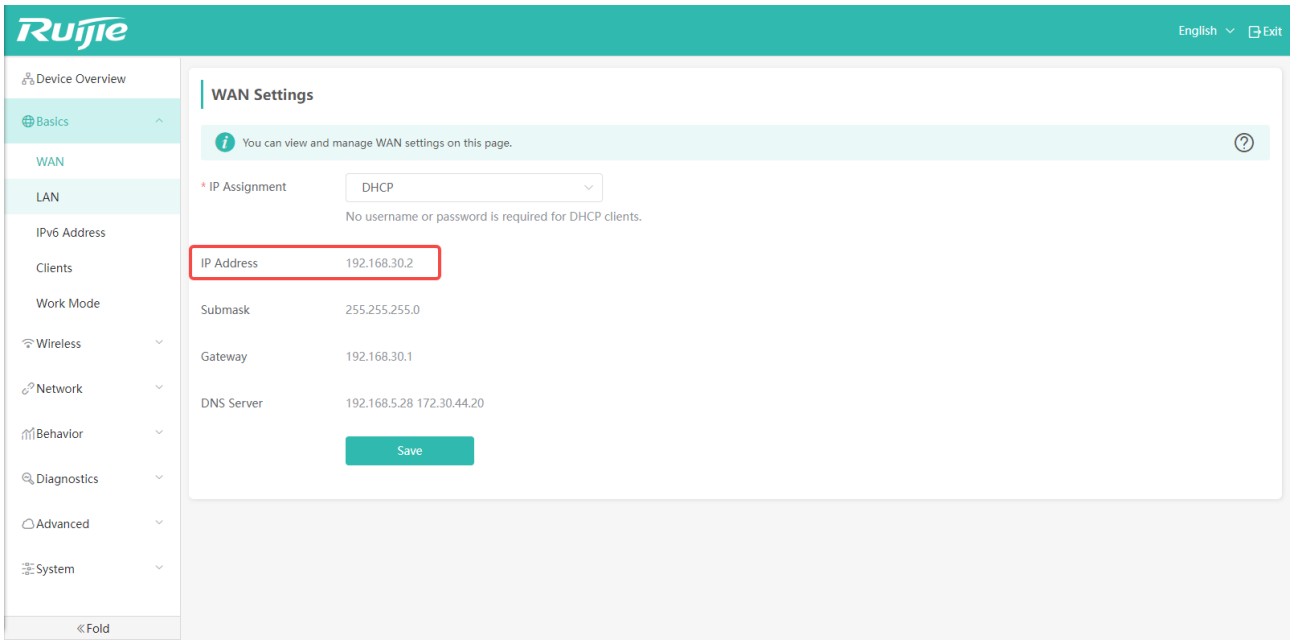
Menus	Description
Basics	Configure working modes, port features and blacklists and whitelists, and display terminal information.
Wireless	Configure the parameters of SSIDs and radios, and WPS function.
Network	Configure and display the parameters of VLANs.
Behavior	Configure the blacklists or whitelists of DNS/URL, port security and other security features.
Diagnostics	Use network tools such as ping, traceroute and DNS lookup to diagnose networks.

4.1 Basic Management

4.1.1 WAN Settings (Routing Mode)

In routing mode, you can connect to the Internet by modifying the IP assignment method of the WAN port.

- Click "Basics" -> "WAN" to enter the page to check the IP address of the WAN port.

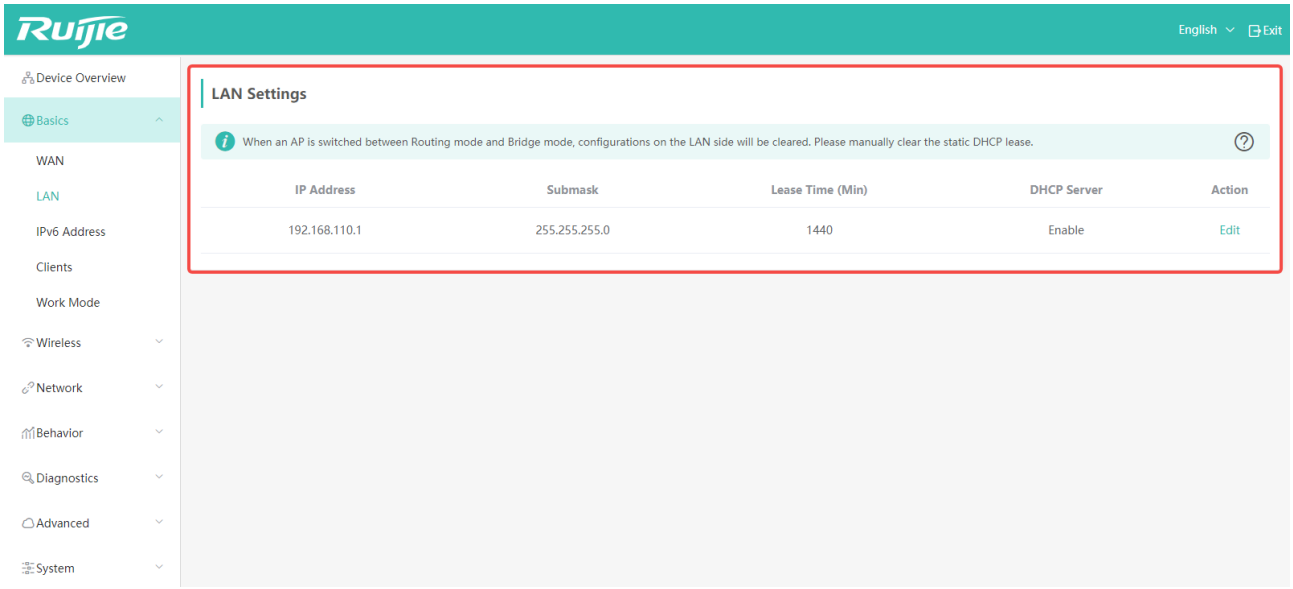


If you want to select another IP assignment method, you can click “IP Assignment" to change the assignment method. DHCP and static IP are available. For specific configuration steps, please refer to the section 2.5.3 “Routing Mode".

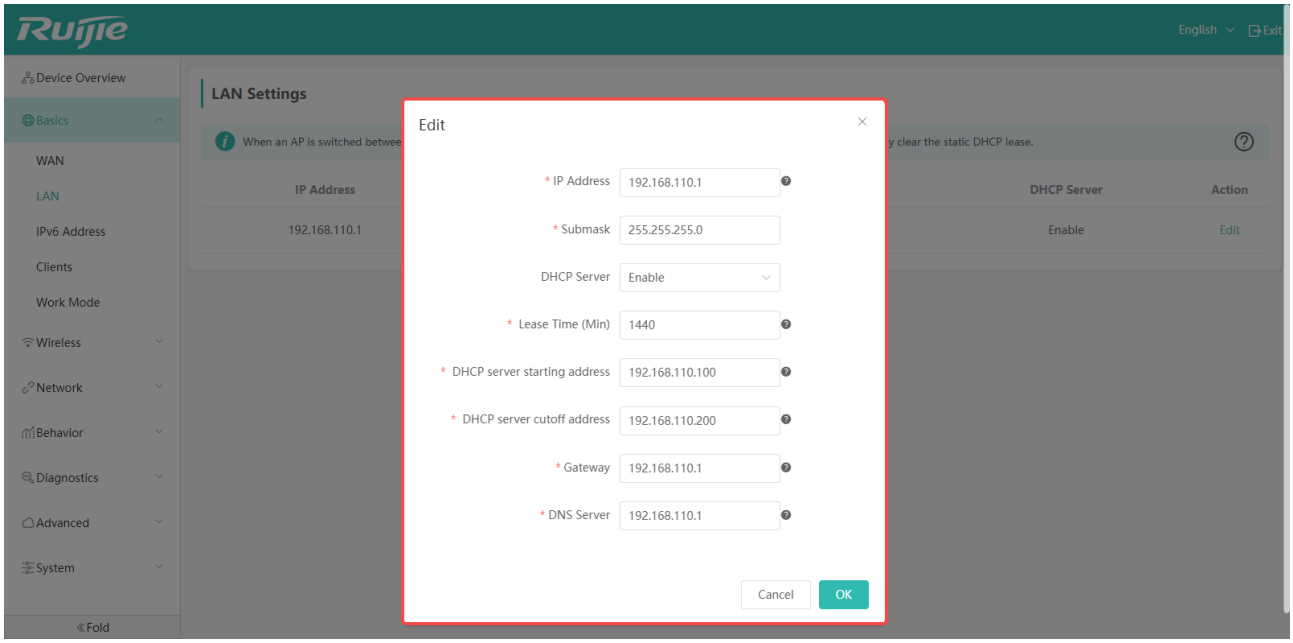
4.1.2 LAN Settings (Routing Mode)

In routing mode, you can change the default DHCP address pool settings in the LAN page.".

- Click "Basics" -> "LAN" to enter the setting page.



- Click "Edit" to enter the modification page.



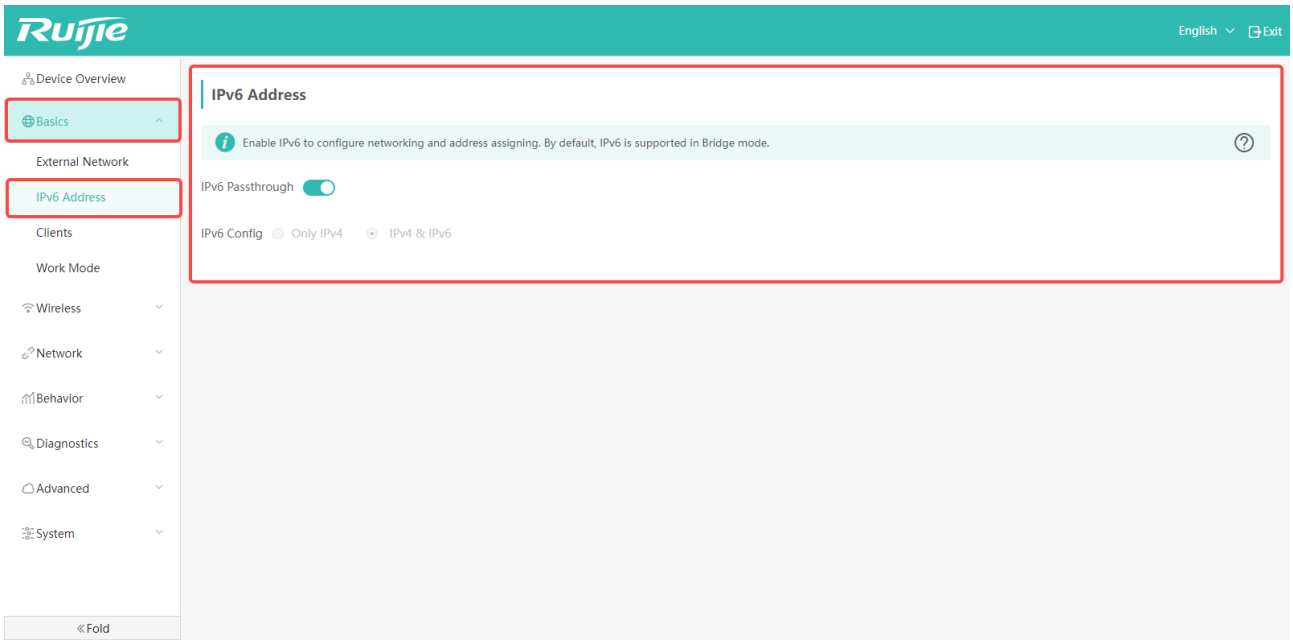
Items	Description	Defaults/Options
IP Address	The gateway IP of DHCP server.	Default: 192.168.110.1
Submask	The subnet mask of gateway IP of the DHCP server.	Default: 255.255.255.0
DHCP Server	The switch of DHCP address pool. It is not recommended to disable it because when it is disabled, the terminal will not be assigned an IP address.	Default: Enabled Option: Enabled/Disabled/DHCP Relay

Lease Time (Min)	The lease time of the assigned IP. When the lease expires, the IP will be reclaimed, and the terminal needs to reapply for an new IP address.	Default: 1440 minutes (24 hours) Option: 2-2880 minutes
DHCP server starting address	Specify the start address of the IP address pool.	Default: 192.168.110.100
DHCP server cutoff address	Specify the end address of the IP address pool.	Default: 192.168.110.200
Gateway	Specify the gateway address assigned to the terminal.	Default: 192.168.110.1
DNS Server	Specify the DNS address assigned to the terminal.	Default: 192.168.110.1

📖 In routing mode, if the WAN port is assigned an IP address in the range of 192.168.110.XX, the IP address of the DHCP address pool on the LAN side will be changed to an IP address in the range of 192.168.111.XX, and the gateway address is changed to 192.168.111.1, the start address to 192.168.111.100, and the end address to 192.168.111.200. The rest of configurations remain unchanged.

4.1.3 IPv6 Settings

Click "Basics" -> "IPv6 Address" to enter the IPv6 configuration page.



The configuration items provided on the IPv6 configuration page are described in the following table:

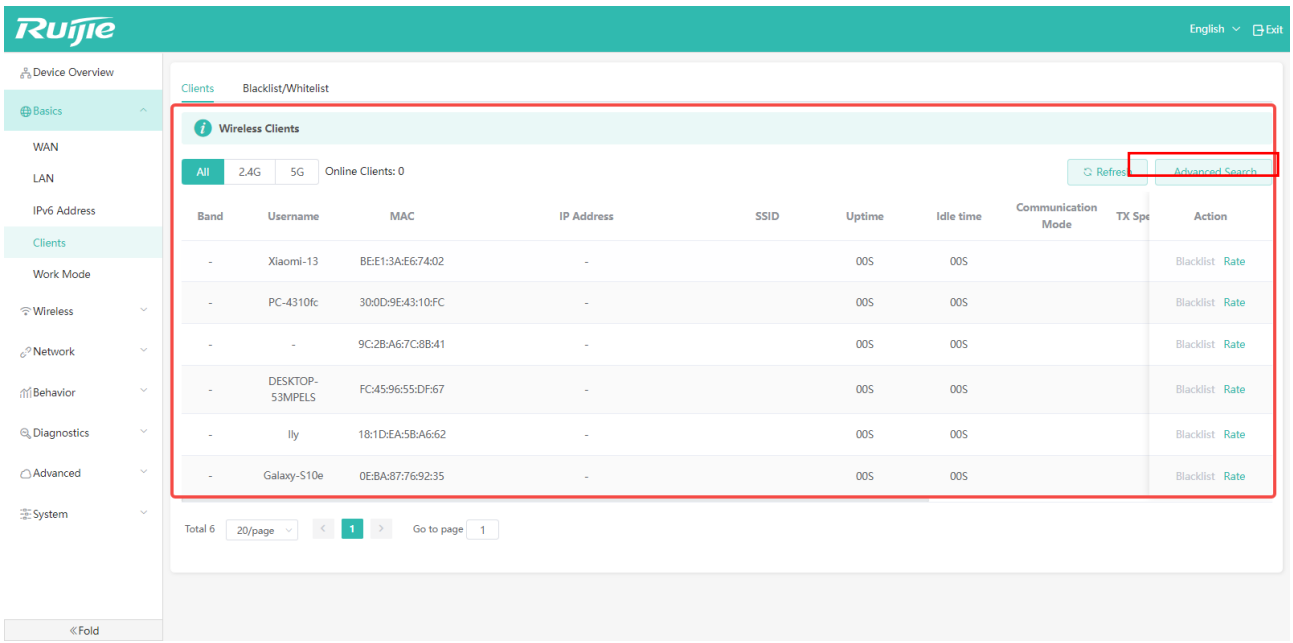
Items	Description	Defaults/Options
IPv6 Passthrough	Configure whether to block IPv6 packets. When this feature is enabled, IPv6 packets can be sent to wireless clients. ※ If the devices on both sides have learned the other party's local link address, this function will not take effect.	Default: Enabled. Options: Enabled/Disabled.
IPv6 Configuration	Configure whether the AP provides IPv6 services in routing mode. When “Only IPv4” option is selected, the AP only provides IPv4 addresses to clients. If the “IPv4&IPv6” option is selected, the AP will assign IPv4 and IPv6 addresses to clients.	Default: IPv4 &IP v6 Options: Only IPv4, IPv4&IPv6

📖 In AP mode, IPv6 packets are transparently transmitted by default and will not be blocked.

📖 Please note that if you select the IPv4&IPv6 option, faults may occur on a small number of APPs that do not support IPv6.

4.1.4 Clients

■ Click "Basics" -> "Clients" to display the current client list:

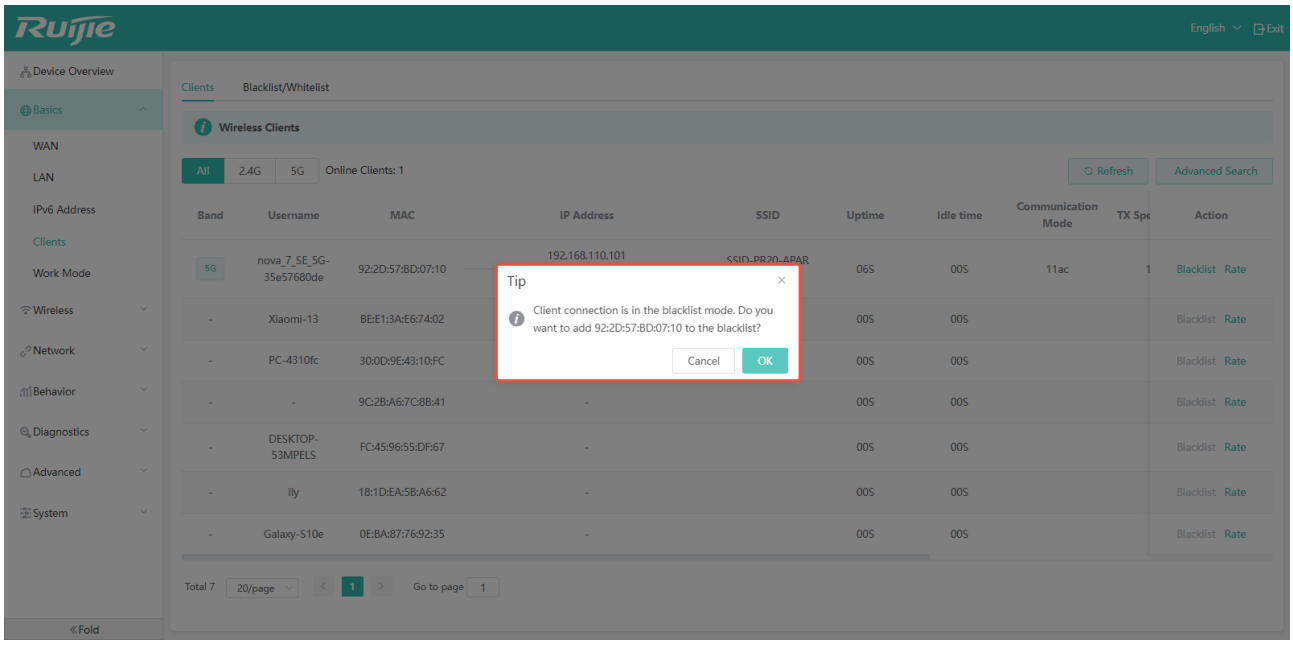


Items	Description
Band	If the client is a wireless client, it will be displayed here whether the client is currently accessing the 2.4G signal or the 5G signal.
Username	The host names of some clients, such as PC are displayed here.
MAC	The MAC addresses of clients.
IP Address	The IP address of clients.
SSID	The SSID name associated with the terminal.
Uptime	The online duration of the client.
Idle Time	The duration of no activity or data transfer.
Communication Mode	Wi-Fi standards, such as 802.11a/b/g/n/ac/ax.
TX Speed (kbps)	If the client is a wireless client, its sending rate with the unit of Mbps will be displayed here. This value will be updated only by refreshing the page manually.
RX (PKTS)	If the client is a wireless client, the number of packets it received will be displayed here.
TX (PKTS)	If the client is a wireless client, the number of packets it sent will be displayed here.
Signal Intensity (dbm)	If the client is a wireless client, the signal intensity received by the AP from the client will be displayed here.
RSSI (dbm)	If the client is a wireless client, its wireless signal strength will be displayed here. RSSI is expressed as a negative number. The larger the number, the stronger the signal strength.
Status	Whether the client is currently online.
Access	This displays the client's connection type. The possible value displayed here is “wireless”.
Action	Here you can choose to conduct some simple operations on the client. There are two management actions that can be performed: blacklisting and rate limiting.
Refresh	The information on the page will not be updated dynamically. You can press this button to refresh the page to get the latest information.
Advanced	If there are too many terminals displayed on the page, you can click the button to search a

Search	device by using its MAC address.

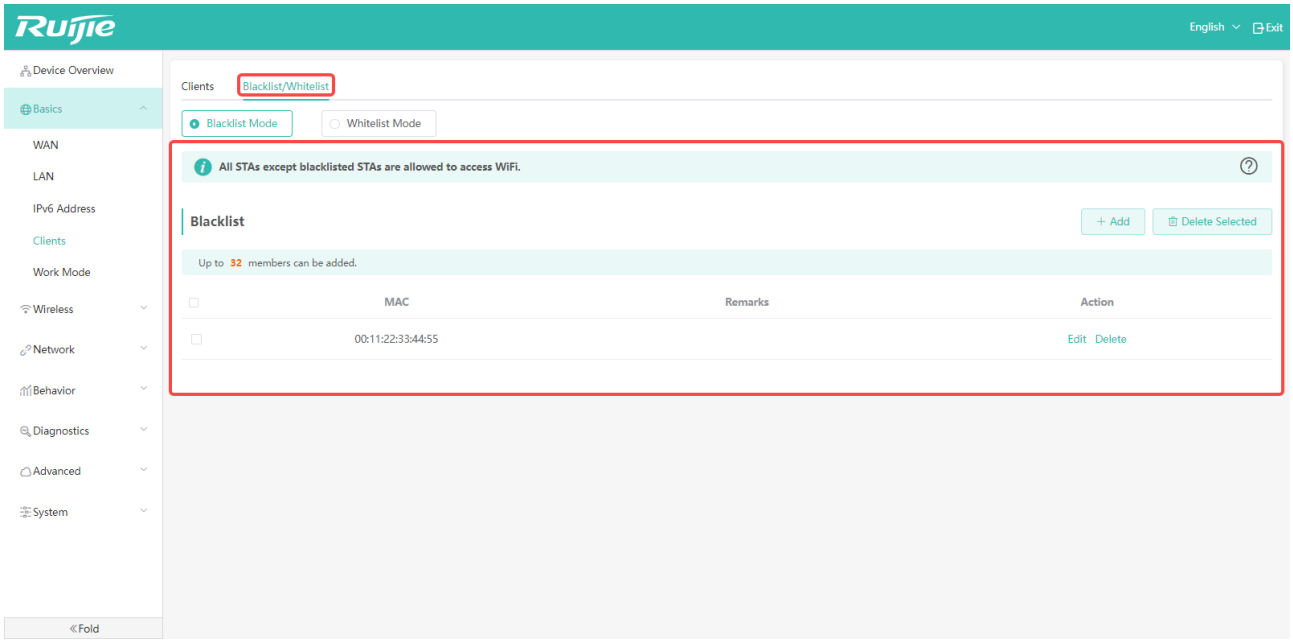
The descriptions of "Blacklist" and "Rate" in Action column are as follows:

- Click "Blacklist" and the following message will appear:

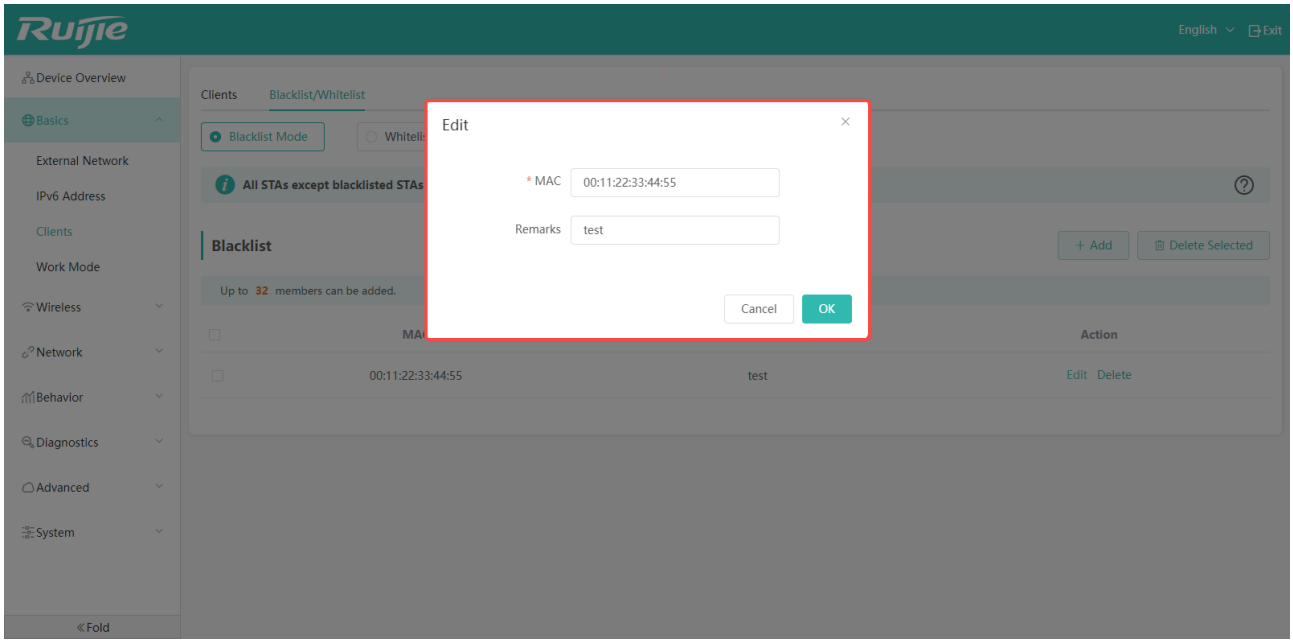


Clients added to the blacklist will not be able to access the AP. For the clients that are whitelisted or blacklisted, you can go to the "Blacklist/Whitelist " page to check the information.

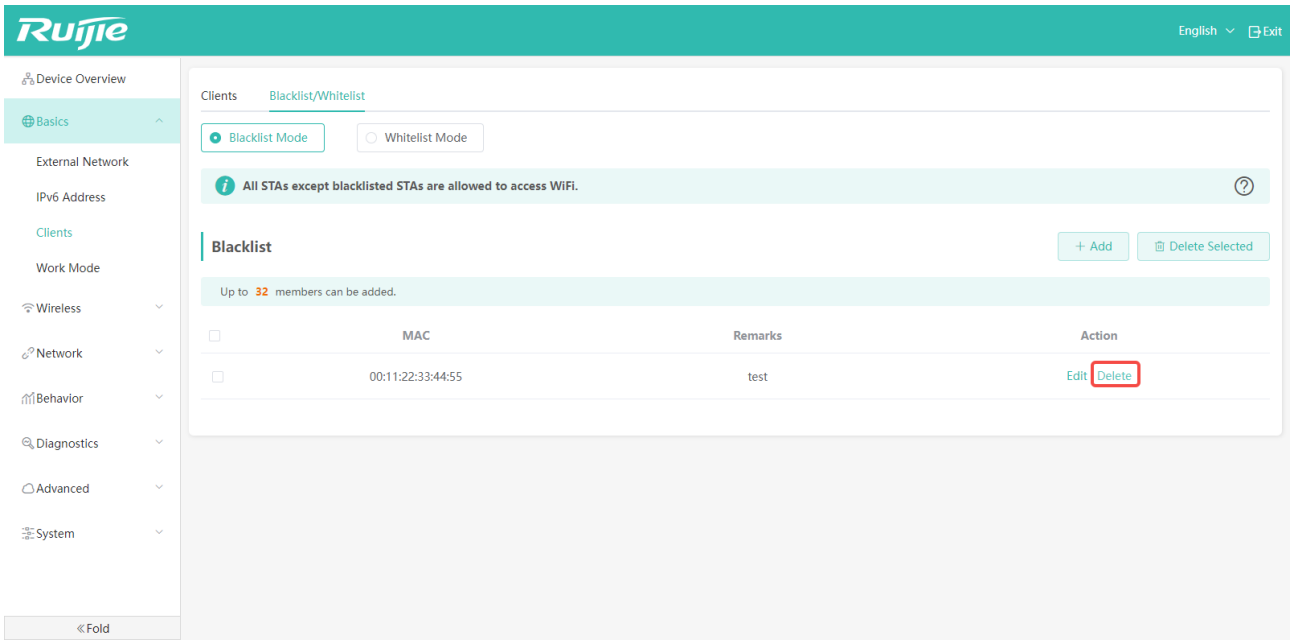
- Click the "Blacklist/Whitelist", you can view the MAC of a client that is blacklisted.



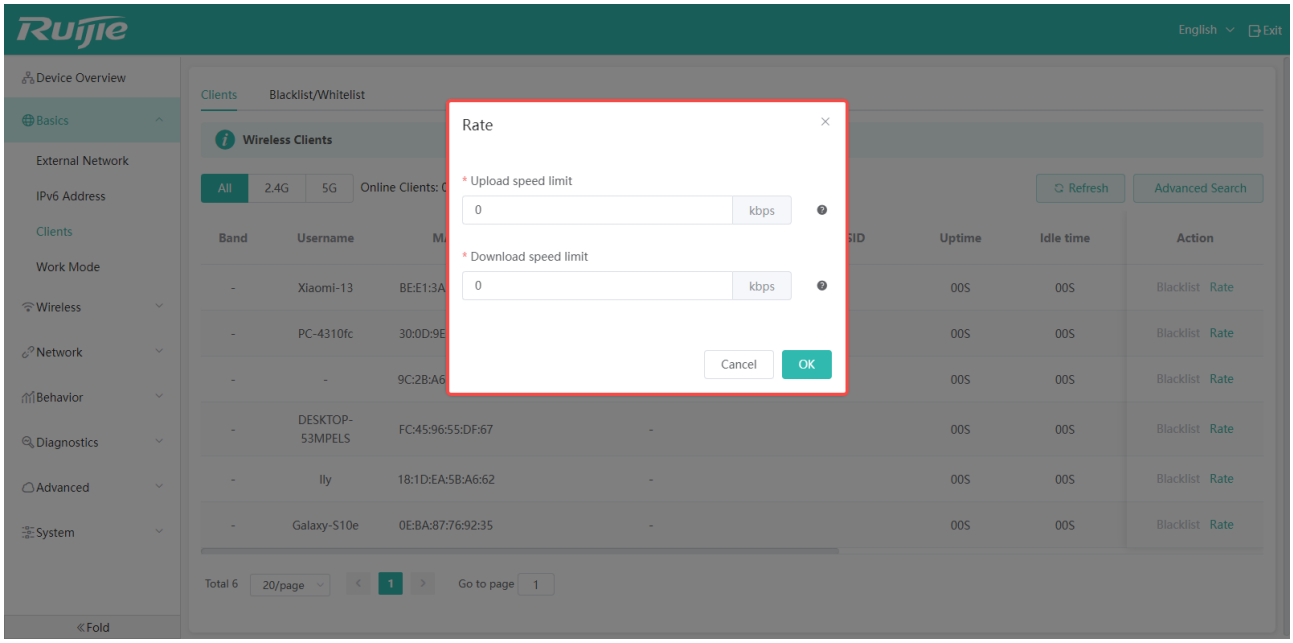
- Click the “Edit” button on the Action column of a client to change the MAC address and the remarks.



- Click “Delete” button in the “Action” column of client to remove the client from the blacklist so that it can connect to the AP normally.



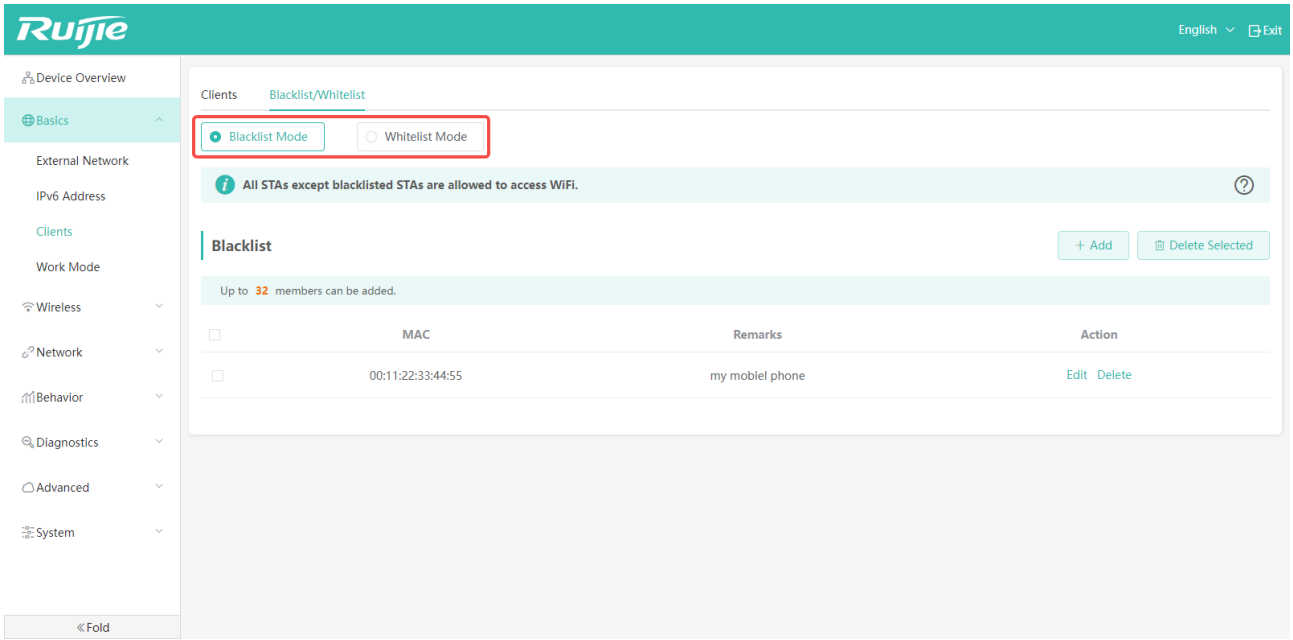
- Click "Rate", and then the following configuration window will appear. In this configuration window, you can configure the uplink and downlink speeds of the clients.

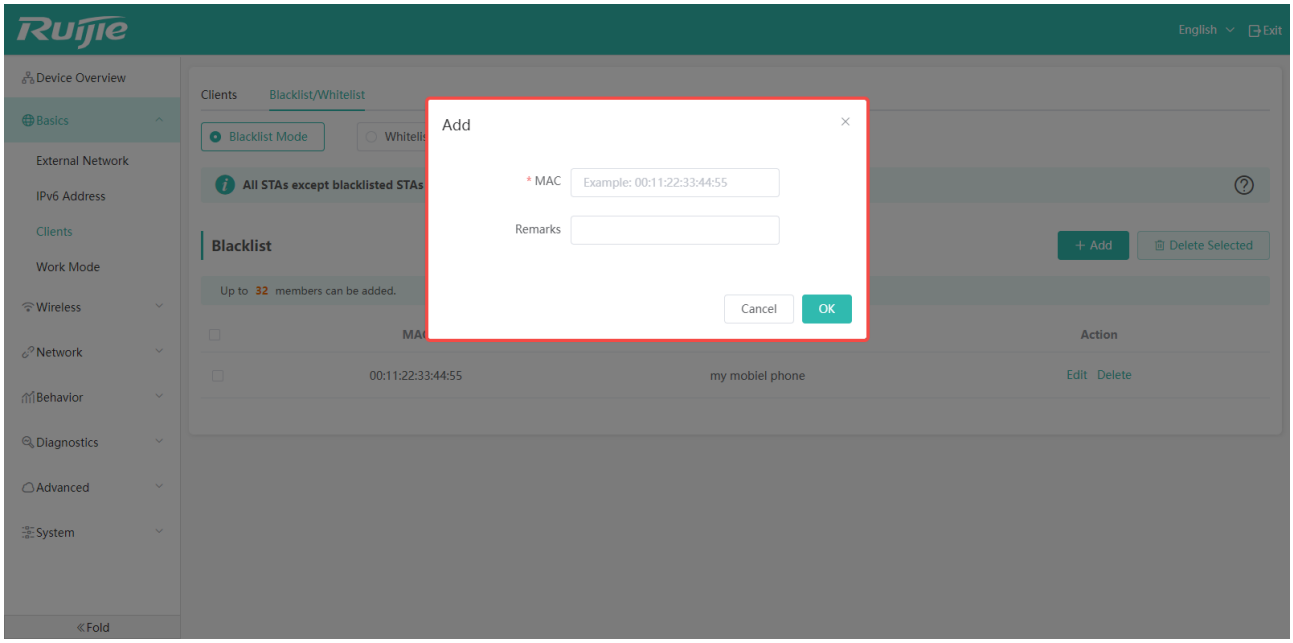


Items	Description	Defaults / options
Upload speed limit	Limit the uplink speed of the client. If it is set to 100 kbps, the uplink speed of the client's network will not exceed 100 kbps.	Default: 0, indicating no limit on the uplink rate.
Download speed limit	Limit the downlink speed of the client. If it is set to 100 kbps, the downlink speed of the client's network will not exceed 100 kbps.	Default: 0, indicating no limit on the downlink rate.

■ Blacklist/Whitelist

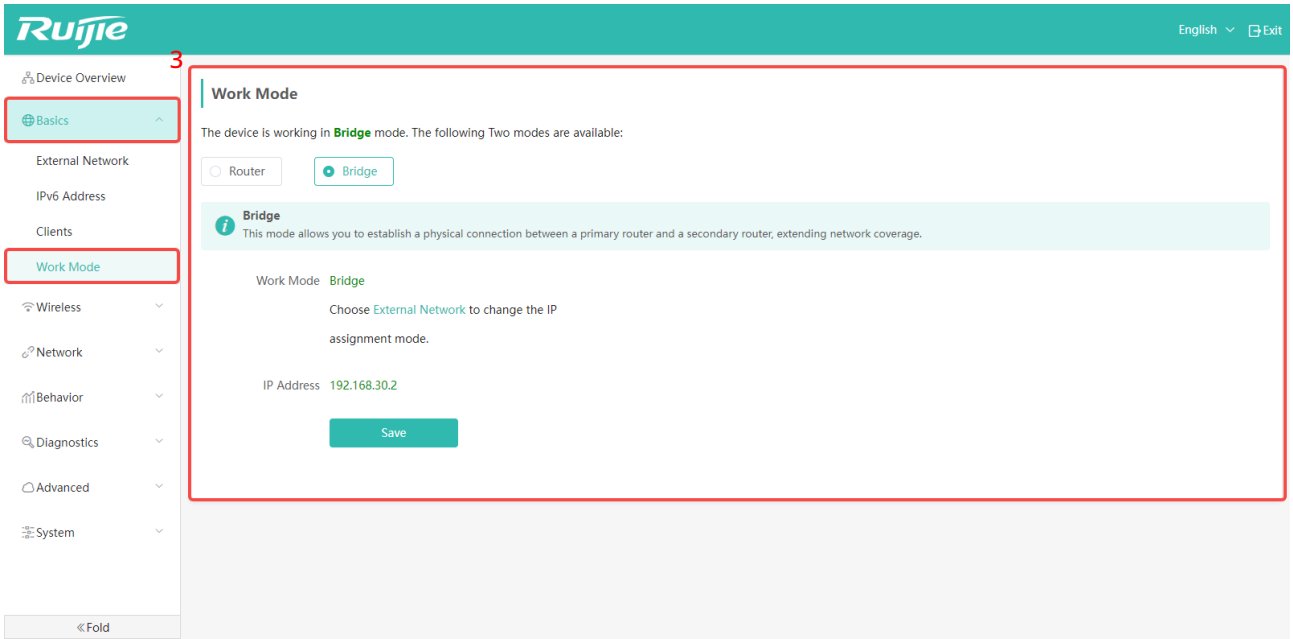
The blacklist and whitelist take effect only on wireless clients. Click the "Add" to add the specified a MAC address to the blacklist or whitelist. Wireless clients whose MAC address is added to the blacklist will not be able to access the AP. You can enter any characters such as "my mobile phone" in the Remark to help you identify the client. The operation of adding a MAC address to the whitelist is the same as that added to the blacklist. When a whitelist is configured, only the terminals with the listed MAC addresses can access the AP.





4.1.5 Mode Switching

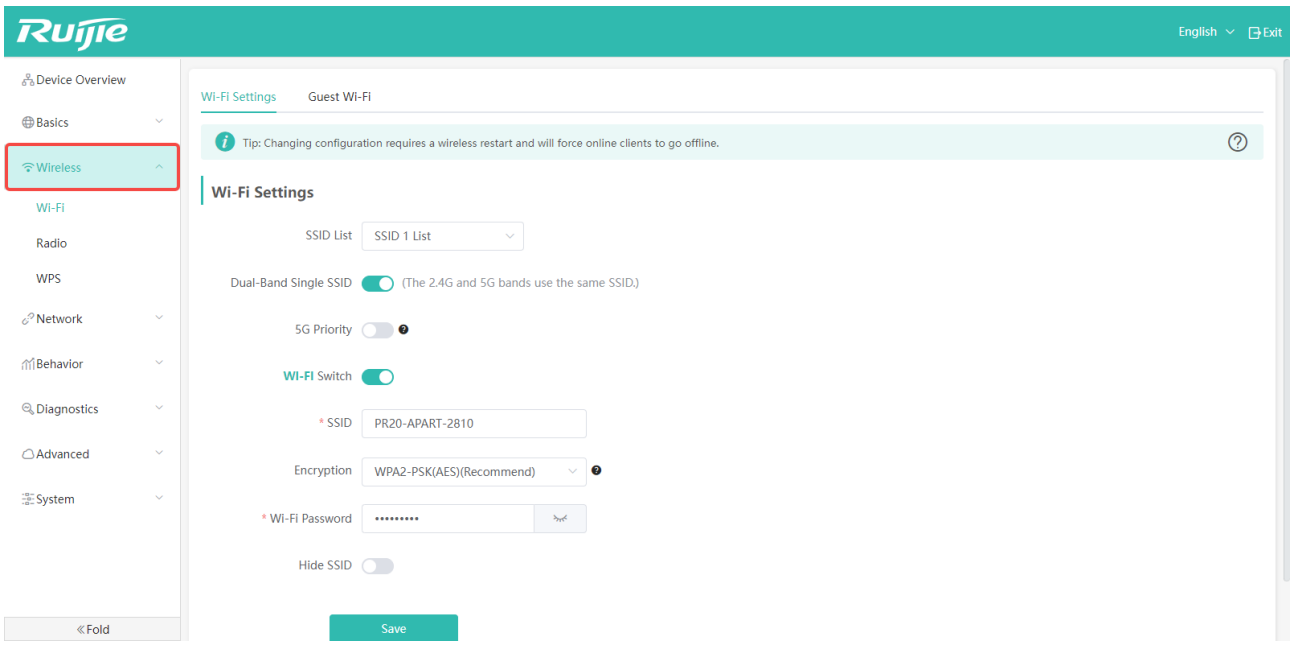
Click "Basics" -> "Work Mode" to switch the working mode.



For details, please refer to Section 2.5.2 AP Mode, and Section 2.5.3 Routing Mode.

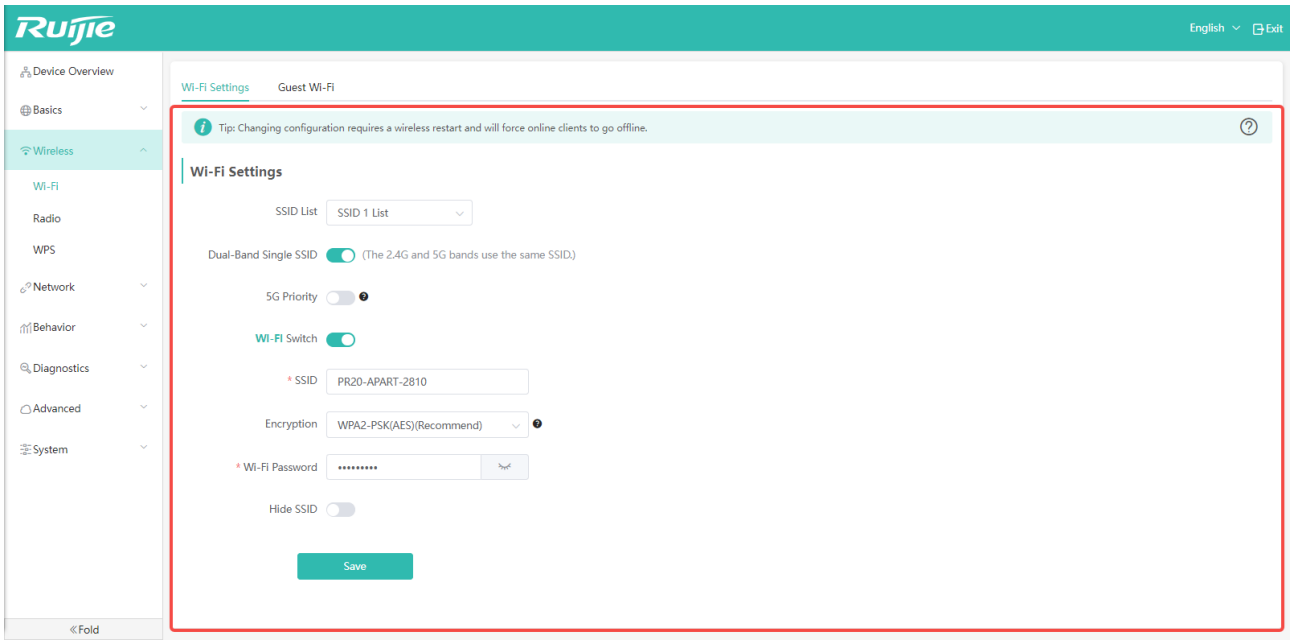
4.2 Wireless Management

Click the "Wireless" -> ”Wi-Fi” on the left panel to configure wireless parameters.



4.2.1 Wireless Settings

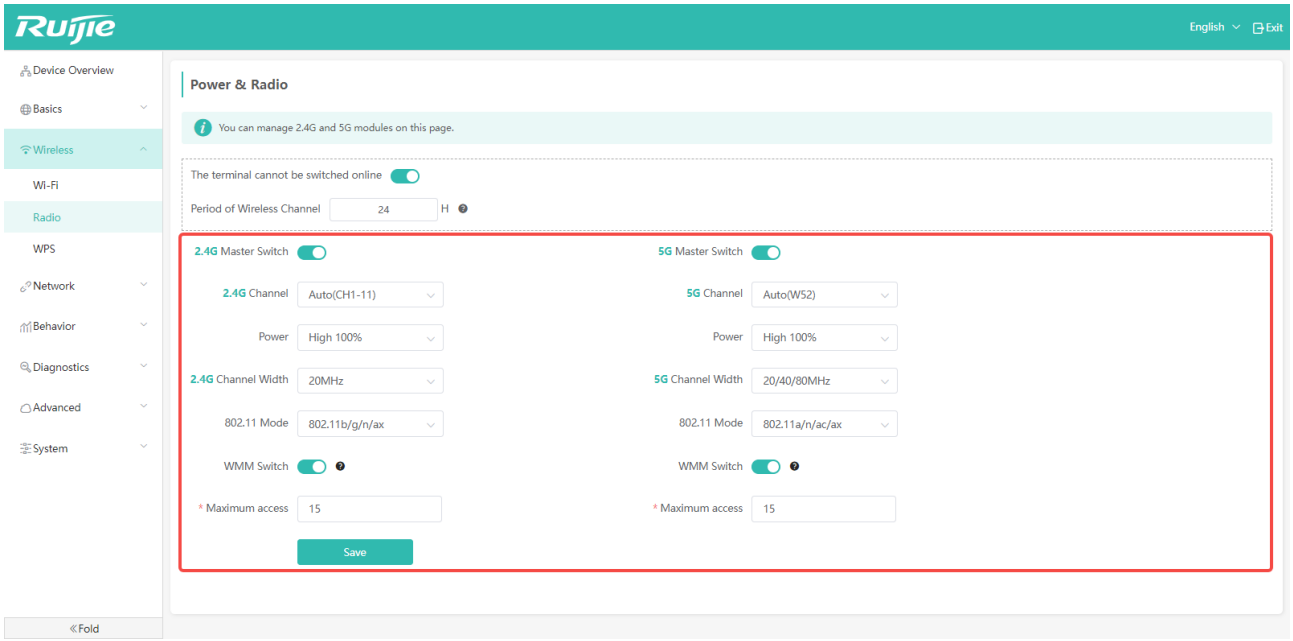
The wireless management page is as shown as follows:



The operations about wireless settings are detailed in Section 2.3 Configuring Wireless SSIDs.

4.2.2 Configuring RF Parameters

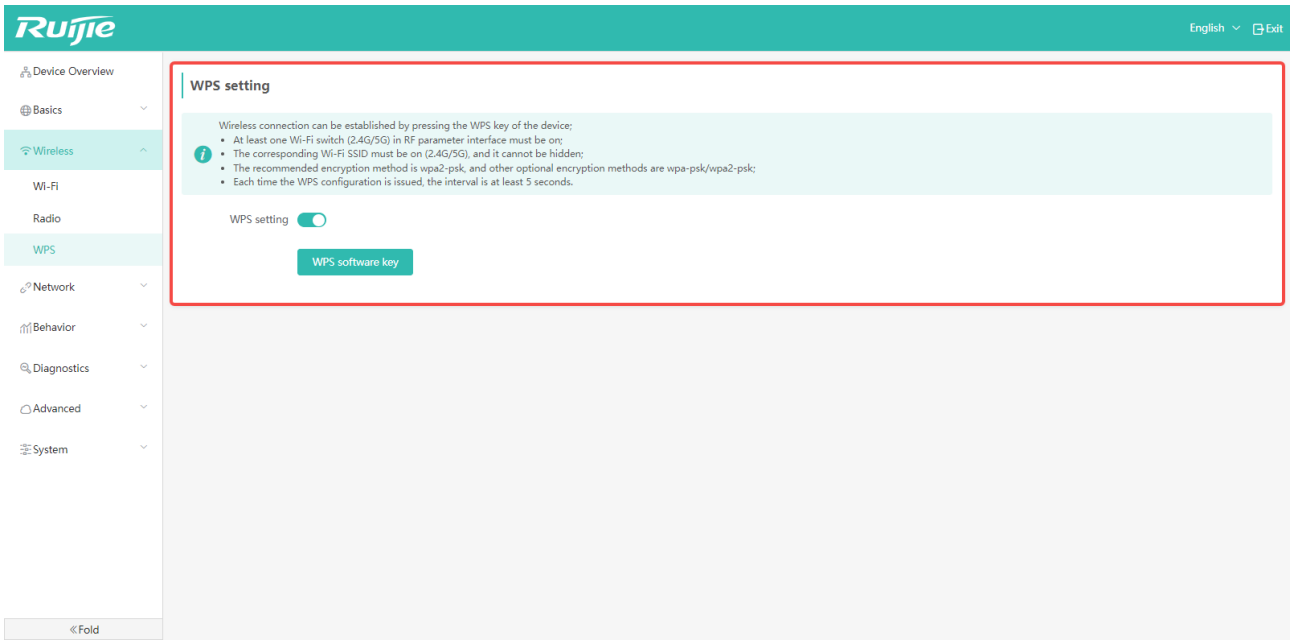
The configuration page of RF is shown as follows:



The operations about RF settings are detailed in Section 2.4 Configuring RF Parameters.

4.2.3 WPS

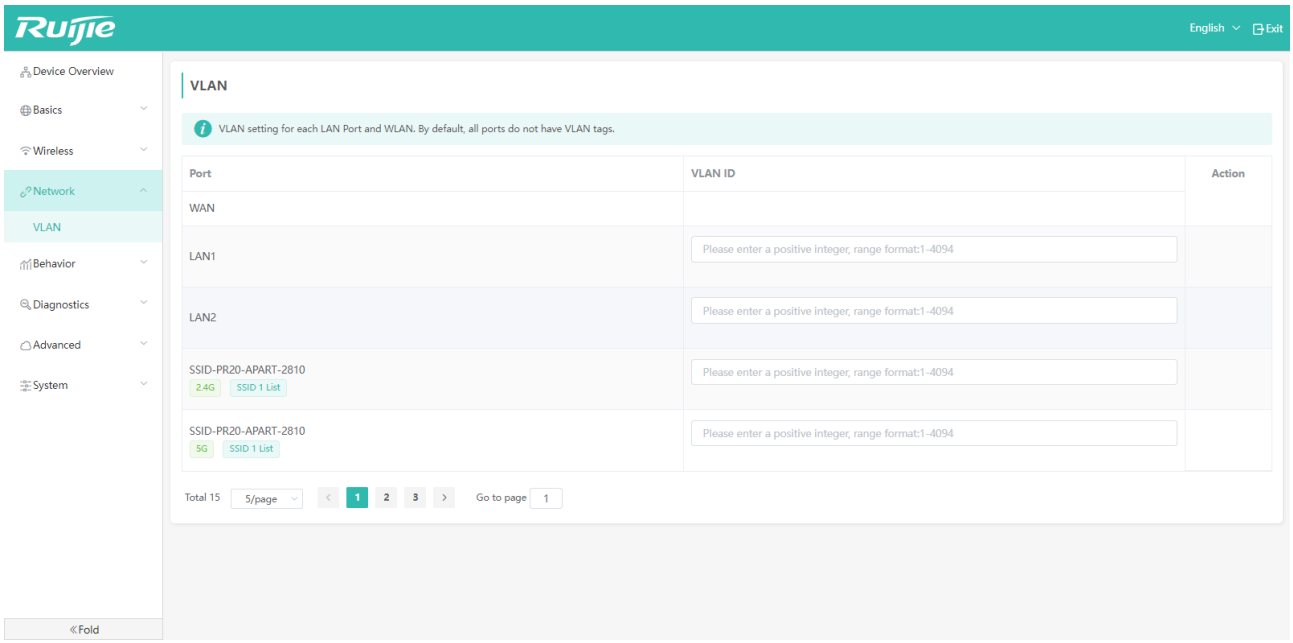
Currently, WPS (Wi-Fi Protected Setup) can be configured only via the PBC (Push Button Configuration). Press and hold the WPS button for 2 seconds or click "WPS software key" to allow terminals that support WPS to access the AP without entering a password.



4.3 Network Management

4.3.1 VLAN

After configuring the VLAN ID for wired ports and SSIDs, only packets with this VLAN tag can be forwarded.



Items	Description	Defaults / options
WAN	Configure a VLAN tag for the WAN port.	Default: Untagged Range : 1-4094
LAN1	Configure a VLAN tag for the first LAN port.	Default: Untagged Range : 1-4094
LAN 2	Configure a VLAN tag for the second LAN port.	Default: Untagged Range : 1-4094
SSIDxxxxxx	Configure a VLAN tag for a specified SSID.	Default: Untagged Range : 1-4094

4.4 Behavior Management

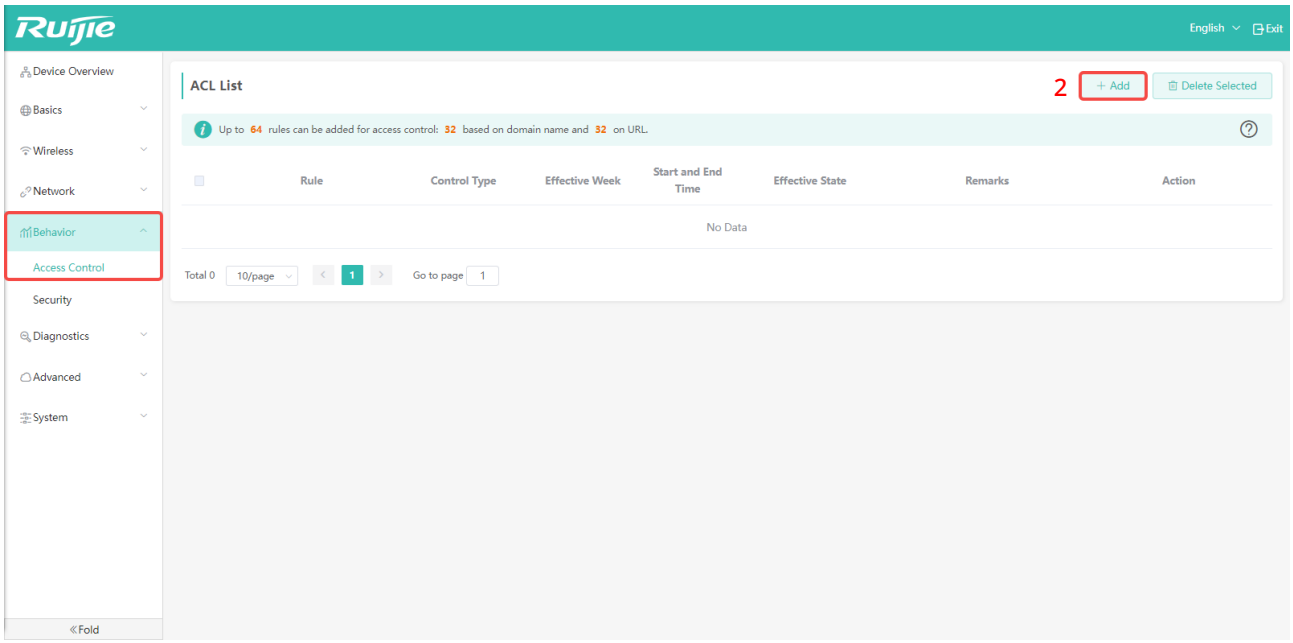
4.4.1 Access Control

You can restrict specific devices to access specific websites according to your needs. If you want to prevent a device from accessing a website, you can set the control type to blacklist. If you want a device to be able to access only specified websites, you can set the control type to whitelist.

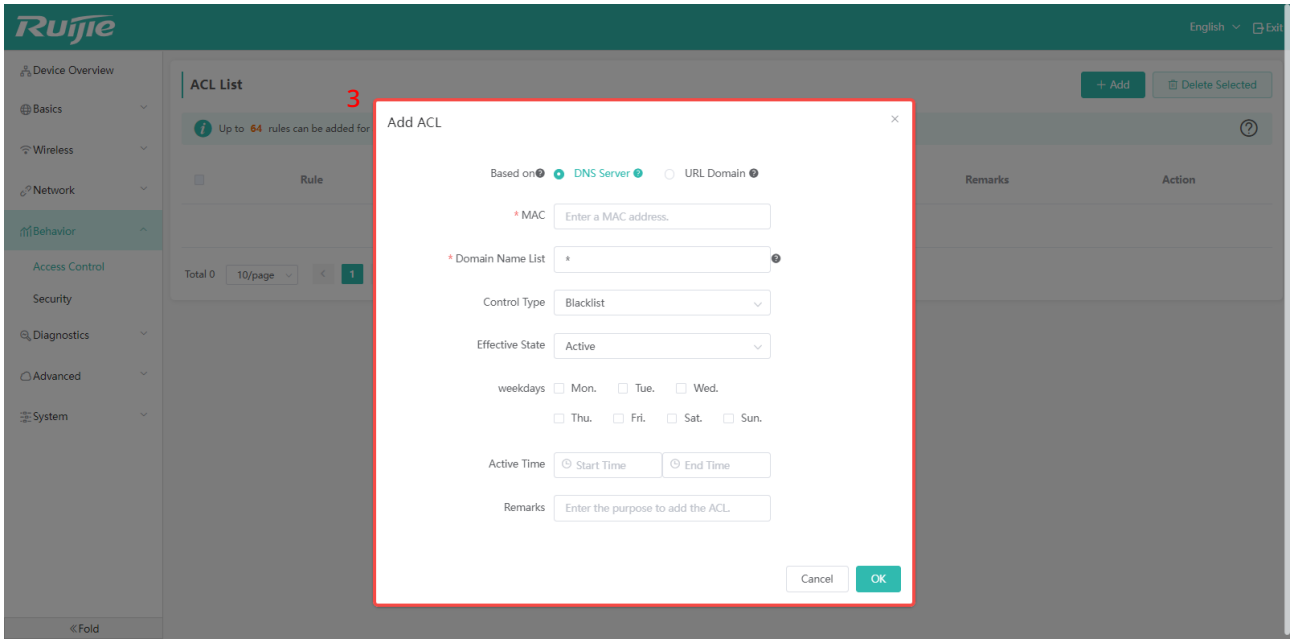
- The specific operations are as follows:

Step 1: Click "Behavior" -> "Access Control"

Step 2: Click the "Add" to add a ACL.



Step 3: Then, enter the configuration page.



Items	Description	Defaults/Options
Based on	Specify the rule to be based on DNS server or URL domain. The implementation principles of these two methods are different. Based on DNS server: When the rule is set to be filtered based on DNS, the system will resolve the DNS request of a client. If the request asks for the configured address, the rule will take effect. Based on URL domain: When the rule is set to be filtered based on URL domain, the system will resolve the URL visited by the client. If the URL accessed by the client is the configured URL, the rules will take effect.	Default: Based on DNS Server Options: Based on DNS Server or URL Domain
MAC	Specify the MAC address of the device to be controlled.	Default: N/A
Domain Name List	If the rule is based on the DNS address, you can enter a domain name list string to clarify the domain name to which the rule applies. A device in the blacklist cannot access the domain name even though its DNS addresses is matched. A device in the whitelist that matches this rule can only access the domain name configured. If you want the rule to match all URLs/addresses, enter * .	Default: * * means matching all URLs and addresses.
	If the rule is based on the domain names of URLs, you can enter the URL string to clarify the URL to which the rule applies. In this way,	

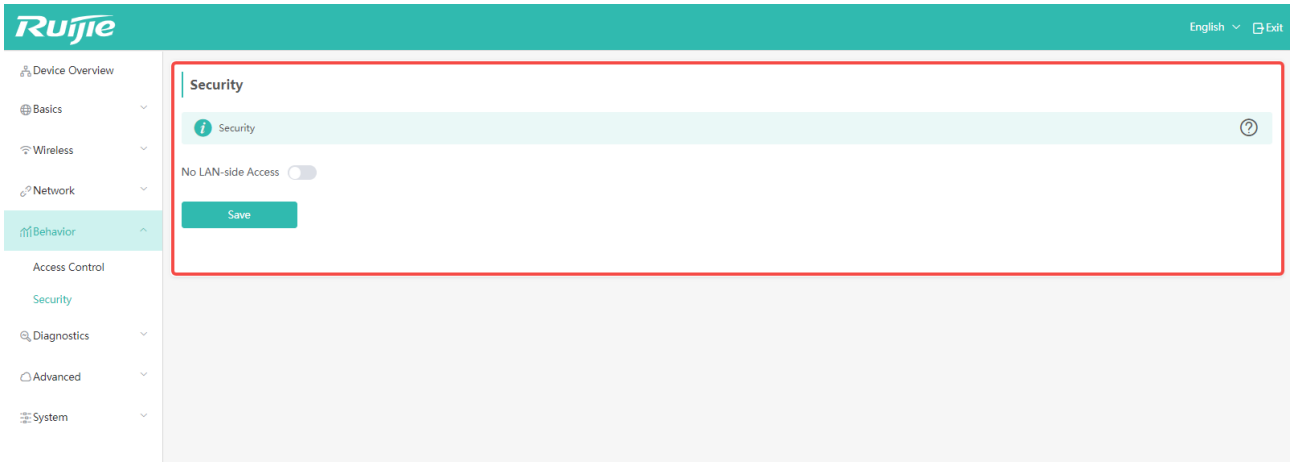
	the devices in the blacklist that match this rule cannot access the URL, and the devices in the whitelist that match this rule can only access the URL. If you want the rule to match all URLs/ addresses , enter *.	
Control Type	Select whether to add the domain name of the rule to the blacklist or whitelist. Blacklist: Devices are not allowed to access domain names in the blacklist. Whitelist: Devices are only allowed to access domain names in the whitelist.	Default: Blacklist Options: Blacklist/Whitelist
Effective State	Make the rule active or inactive.	Default: Active Options: Active/Inactive
Weekdays	Select the day(s) of the week on which the rule will be enabled.	Default: N/A Option: Support to select any day in a week.
Active Time	Select the time period for this rule to take effect.	Default : N/A
Remarks	Notes can be added to identify the purpose of the rule.	Default : N/A

Up to 64 rules can be configured, including 32 DNS-based rules and 32 URL-based rules.

4.4.2 Security

- Bridge Mode

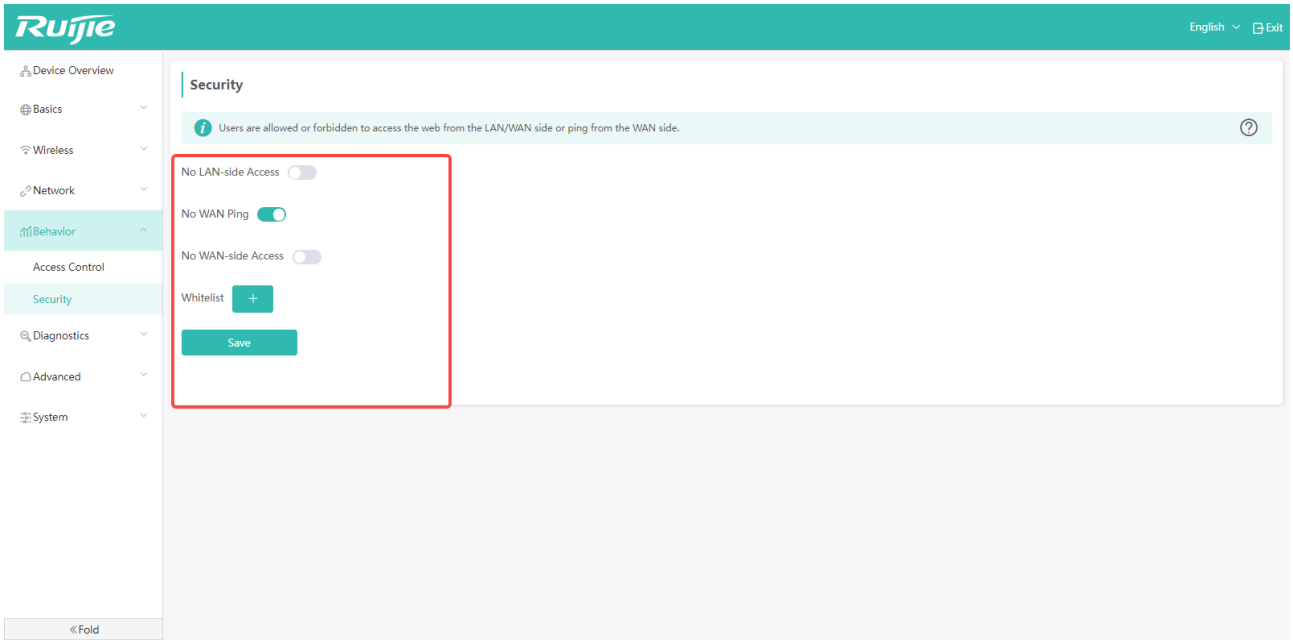
If you do not want the terminals on LAN side to access the Web of the AP, you can click “Behavior” -> “Security” to enable "No LAN-side Access”.



Items	Description	Defaults /Options
No LAN-side Access	When it is enabled, the client cannot access the device's Web from the LAN side.	Default: Disabled Option: Enabled/Disabled

- Routing Mode

In routing mode, apart from the security settings for accessing the WEB from the LAN side, you can also set the switch for accessing the WEB from the WAN side to prevent external access and attacks on the AP.



Items	Description	Defaults /Options
No LAN-side Access	When it is enabled, the client cannot access the device's Web from the LAN side.	Default: Disabled Options: Enabled/Disabled
No WAN Ping	When it is enabled, the client cannot ping the device successfully from the WAN side.	Default: Enabled Options: Enabled/Disabled
No WAN-side Access	When it is enabled, the client cannot access the Web from the WAN side.	Default: Disabled Options: Enabled/Disabled
Whitelist	In routing mode, if the “No WAN-side Access” is enabled, addresses in the whitelist can still access the device Web through the WAN port. The first address in the whitelist is still valid after reset.	Default: N/A Up to four IP addresses or IP address ranges can be configured.

In routing mode, because the "No WAN-side Access" function is enabled by default, and no default IP address is configured on the "Whitelist", any IP address will not be able to access the AP from the WAN side.

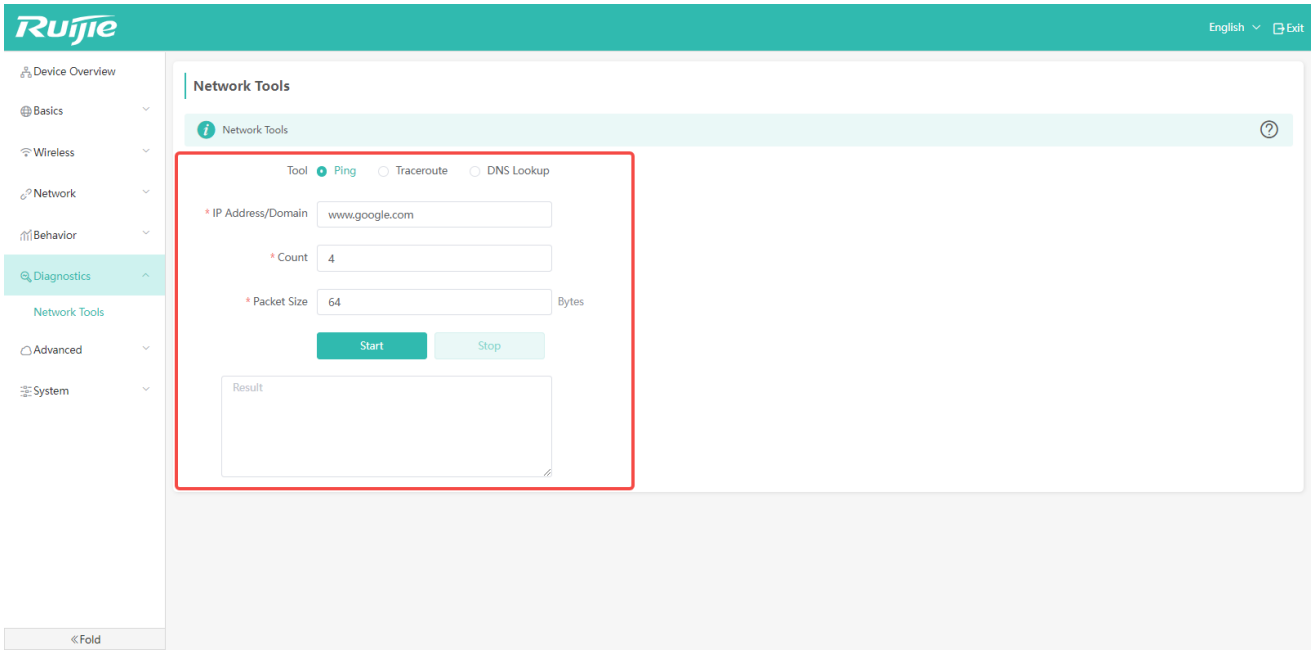
"After the device is reset, the default IP address range stays unchanged, and WAN ping and WAN-side access are allowed." means that after setting the IP address or range, the AP can still retain it after restoring the factory settings.

4.5 Diagnostics

4.5.1 Network Tools

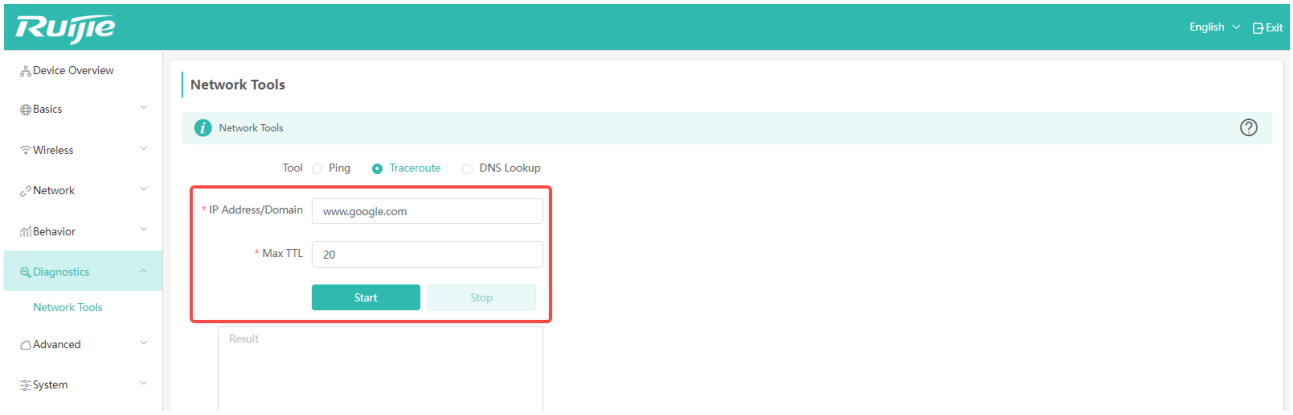
When the network disconnection occurs, you can use three diagnostic tools to check the network status: Ping, Traceroute, and DNS Lookup. Ping is generally used.

■ Ping



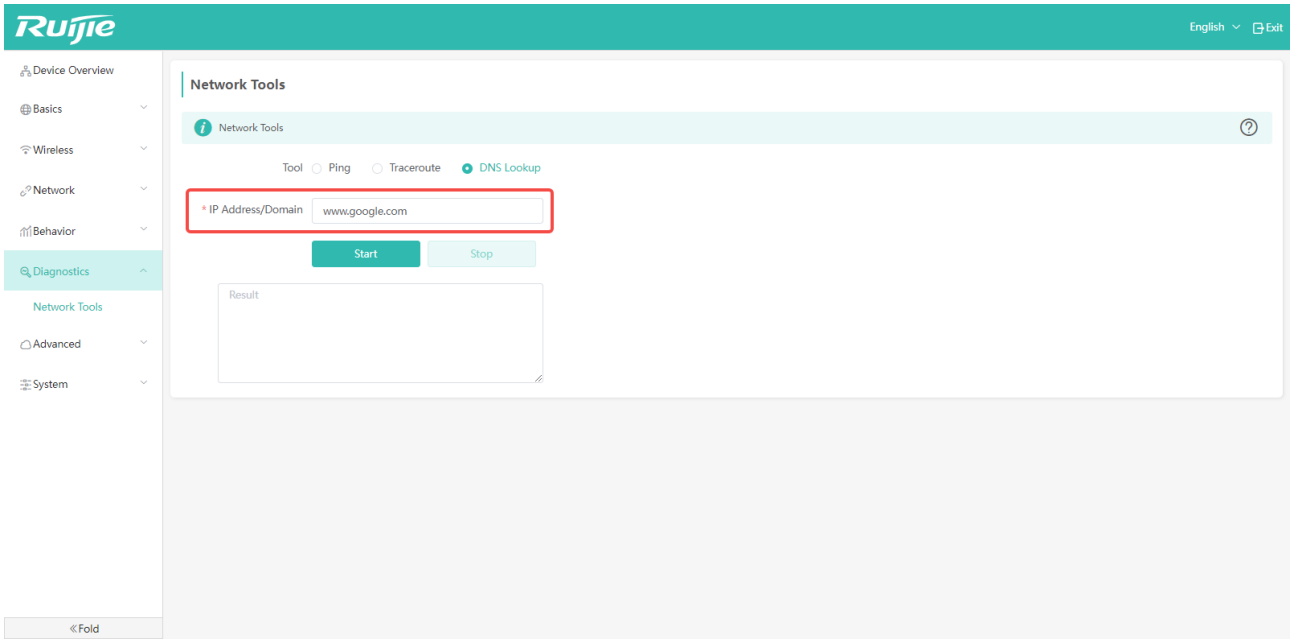
Items	Description	Defaults /Options
IP Address/Domain	Specify an IPv4 address or a domain name used to be tested.	Default: www.google.com Support modifying the IP address or the domain name.
Count	Set the number of times to send packets.	Default: 4 times Options: 1-50 times
Packet Size	Set the size of the packet to be sent.	Default: 64 bytes Options: 4-1472 bytes

■ Trace Route:



Items	Description	Defaults/Options
IP Address/Domain	Specify an IPv4 address or a domain name used to be tested.	Default: www.google.com Support modifying the IP address or the domain name.
Max TTL	Specify the maximum value of TTLs for ICMP messages.	Default: 20 hops Options: 1~30 hops

■ DNS Lookup:



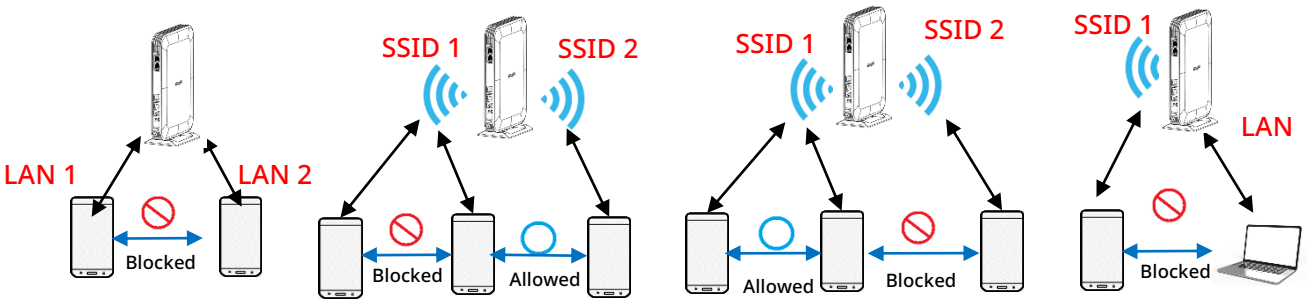
Items	Description	Defaults/Options
IP Address/Domain	Specify an IPv4 address or a domain name to be tested.	Default : www.google.com Support modifying the IP address or the domain name.

5 Advanced Management

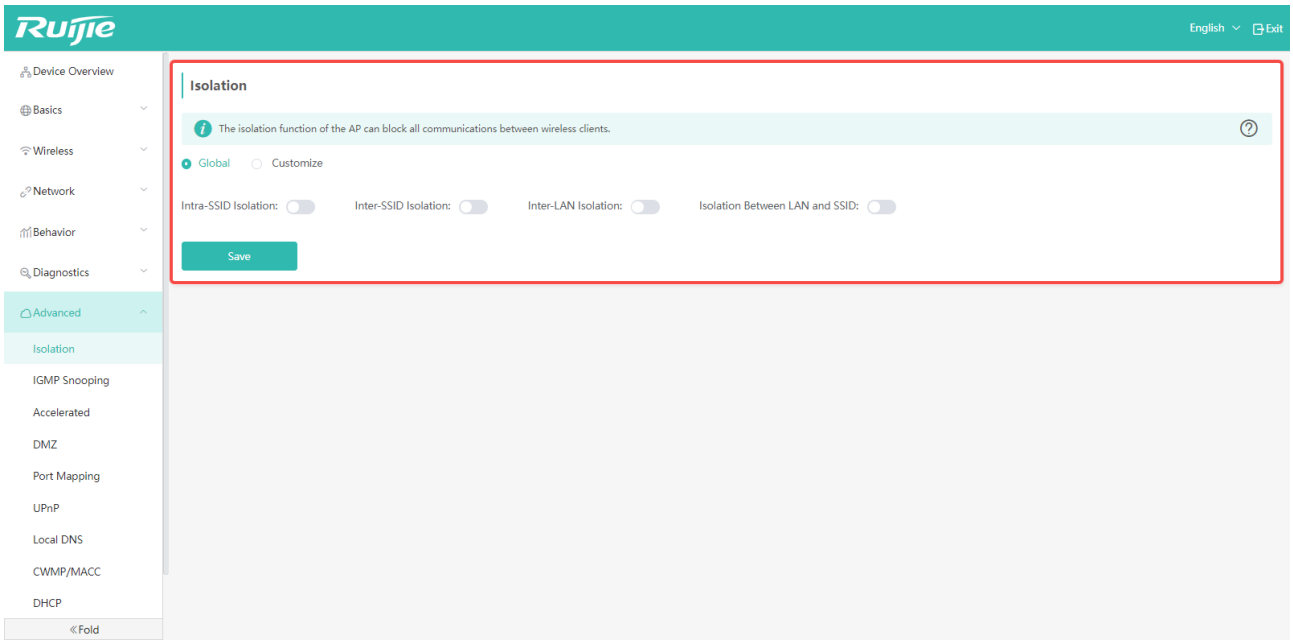
5.1 User Isolation

User isolation feature can prevent users on a local Wi-Fi network from communicating with each other to ensure network security and block inadvertent data transmission. It can identify some special users that are allowed to communicate with each other via their usernames and MAC addresses. This feature is disabled by default. If you want to use it, please enable it manually.

Four working modes of user isolation:



Inter-LAN Intra-SSID Inter-SSID LAN-SSID

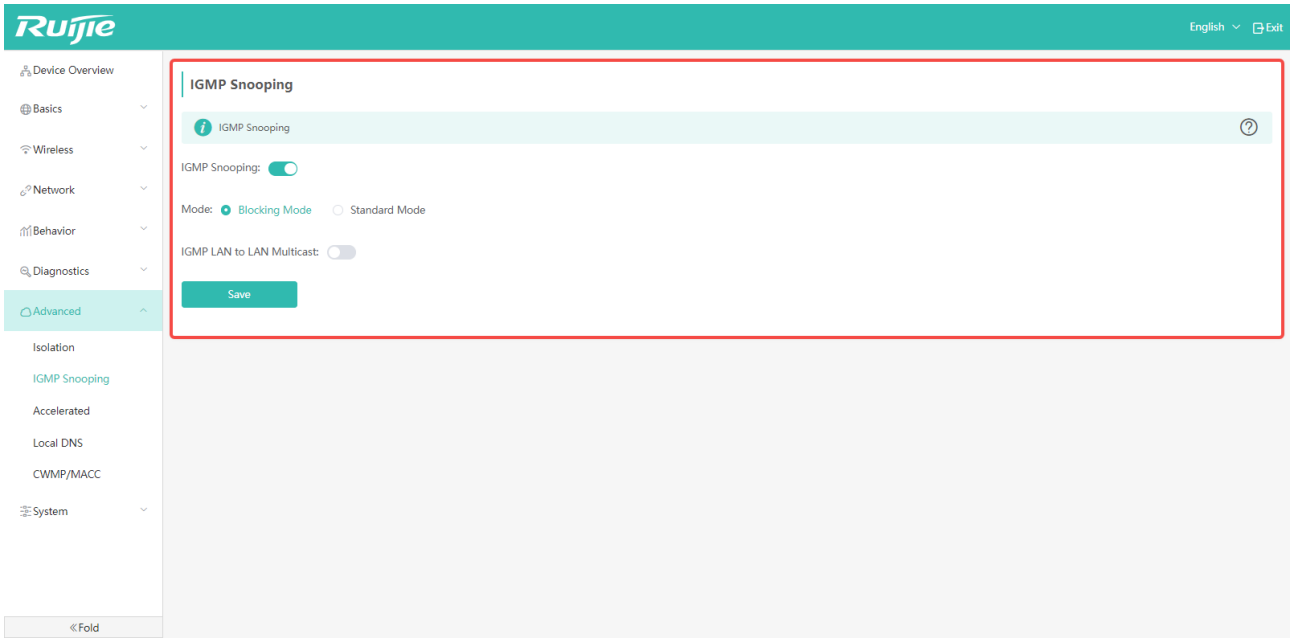


Items	Description	Defaults/Options
Intra-SSID Isolation	Indicate the Intra-SSID isolation mode. When it is enabled, users connected to the same SSID cannot communicate with each other.	Default: Disabled Options: Enabled/Disabled
Inter-SSID Isolation	Indicate the Inter-SSID isolation mode. When it is enabled, users connected to the different SSIDs cannot communicate with each other.	Default: Disabled Options: Enabled/Disabled
Inter-LAN Isolation	Indicate the Inter-LAN isolation mode. When it	Default: Disabled

	is enabled, users connected to the different LAN ports cannot communicate with each other.	Options: Enabled/Disabled
Isolation Between LAN and SSID	Indicate the LAN-SSID isolation mode. When it is enabled, the traffic of the AP's LAN port will be separated from the that of the Wi-Fi network (SSID), so that users connected to the LAN port and users connected to the SSID cannot communicate with each other.	Default: Disabled Options: Enabled/Disabled

5.2 IGMP Snooping

If Internet Group Management Protocol (IGMP) snooping is enabled in your network environment, it can help to control the broadcast of IGMP messages to avoid affecting other terminals. By default, the IGMP snooping is enabled on the device.

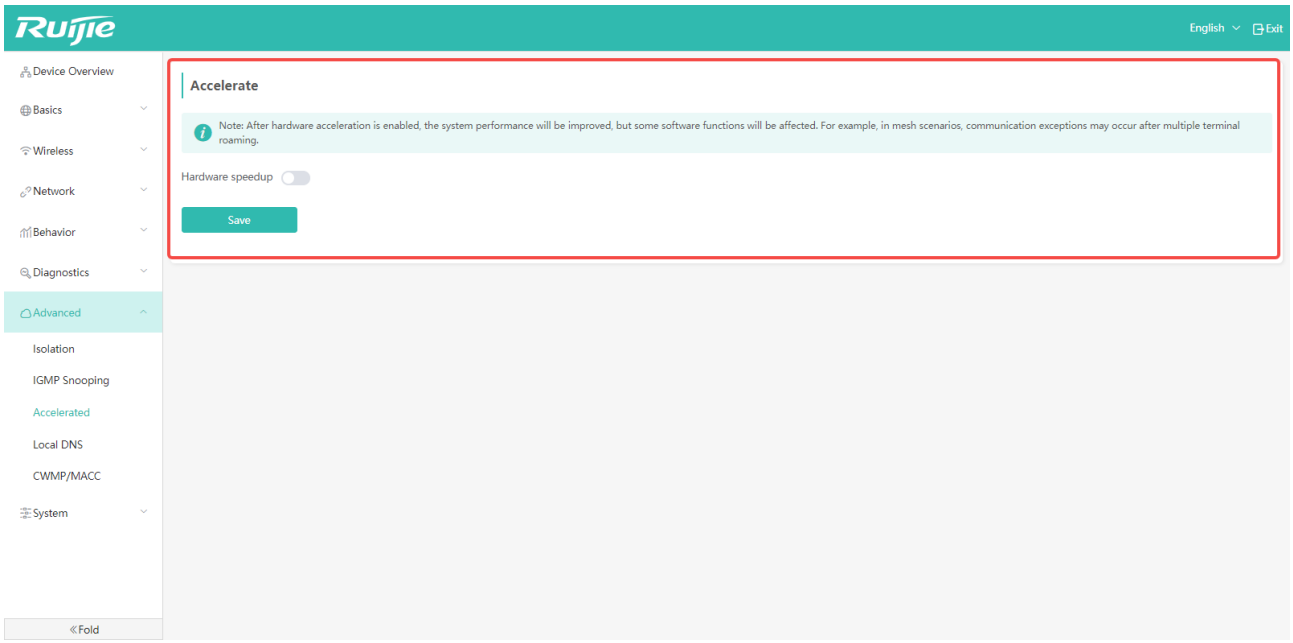


Items	Description	Defaults/Options
IGMP Snooping	Indicate the switch of enabling or disabling the IGMP Snooping. When it is disabled, IGMP messages can be broadcasted in the LAN. When it is enabled, IGMP messages cannot be broadcasted in the LAN network.	Default: Enabled. Options: Enabled/Disabled
Mode	When IGMP Snooping is enabled, specify its mode. There are two modes available: Blocking Mode: In this mode, IGMP messages are blocked in the LAN by default. Only when a client joins a broadcast group can the corresponding IGMP message be sent to the LAN port where the client is located.	Default: Blocking Mode Options: Blocking Mode/Standard mode

	Standard Mode: In this mode, IGMP messages are broadcasted to all LAN ports by default. Only when a client joins a certain broadcast group can the corresponding IGMP message be sent to the LAN port where the client is located, instead of broadcasting to all LAN ports.	
IGMP LAN to LAN Multicast	Generally speaking, the IGMP source messages come from the WAN port. By default, IGMP source messages on the LAN port will not be affected by IGMP Snooping function. But with its feature enabled, IGMP Snooping also takes effect on the IGMP source messages from the LAN ports.	Default: Disabled. Options: Enabled/Disabled

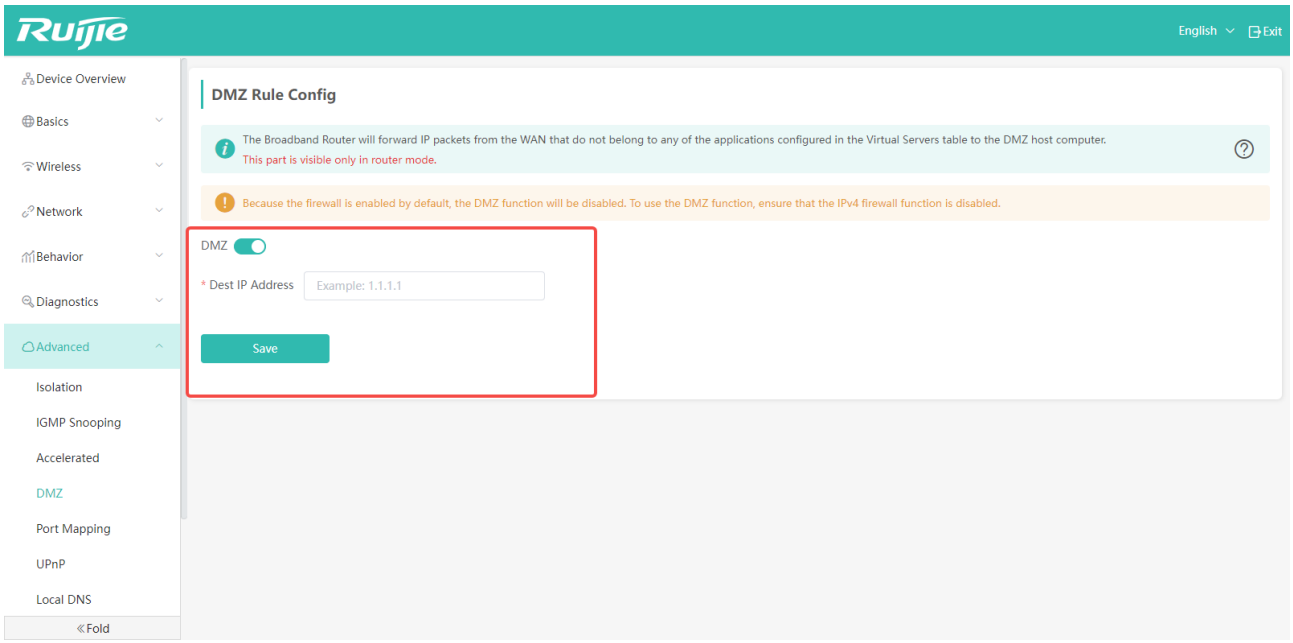
5.3 Acceleration Settings

When the hardware acceleration is enabled, the overall performance of the device will be improved, but some software functions will be affected.



5.4 DMZ (Routing Mode)

If you set up a server on an internal network, such as an FTP server, and want to access the server from an external network, you can use the DMZ function to specify the host on the internal network to enable all ports to be accessed from the external network.



Items	Description	Defaults/Options
DMZ	Enable or disable DMZ function. Only when it is	Default: Disabled.

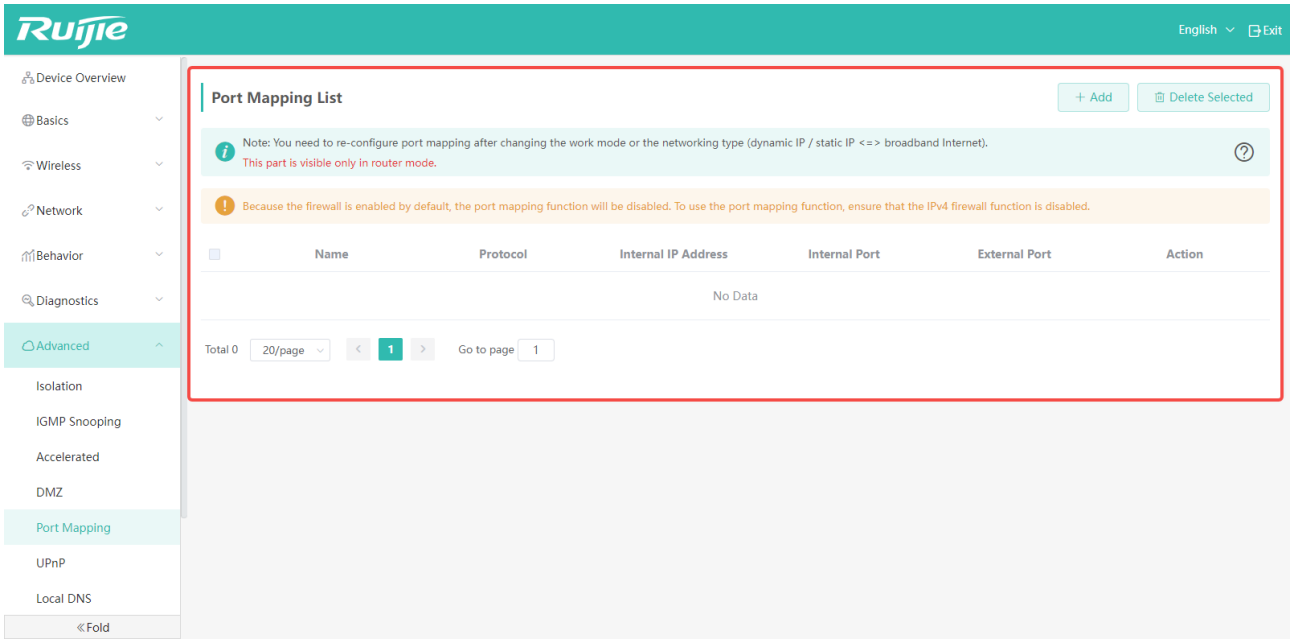
	enabled can the IP address of the host be configured.	Options: Enabled/Disabled
Destination IP Address	After the DMZ function is enabled, specify the IP address of the DMZ host in the internal network. After configuration, AP will use the IP address of WAN port as the external IP address by default .	Default: N/A Specify the IPv4 address of the DMZ host.

5.5 Port Mapping (Routing Mode)

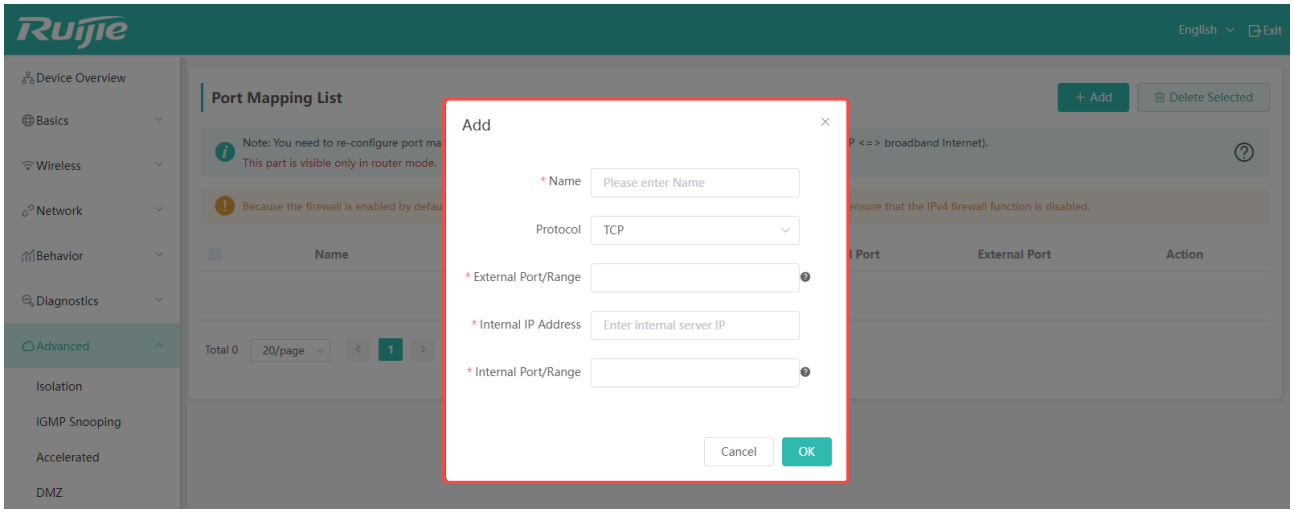
Normally, the host of an internal network cannot be accessed from an external network. However, if the port mapping is enabled, users can access the host from the external network.

Port mapping maps the host IP address n port of an external network to a device in the local area network to provide corresponding services. When a user accesses the port of this IP, the server automatically maps the request to the device in the local area network.

Click "Advanced" - > "Port Mapping" to go to setting page.



Click "Add" to add a port mapping entry.

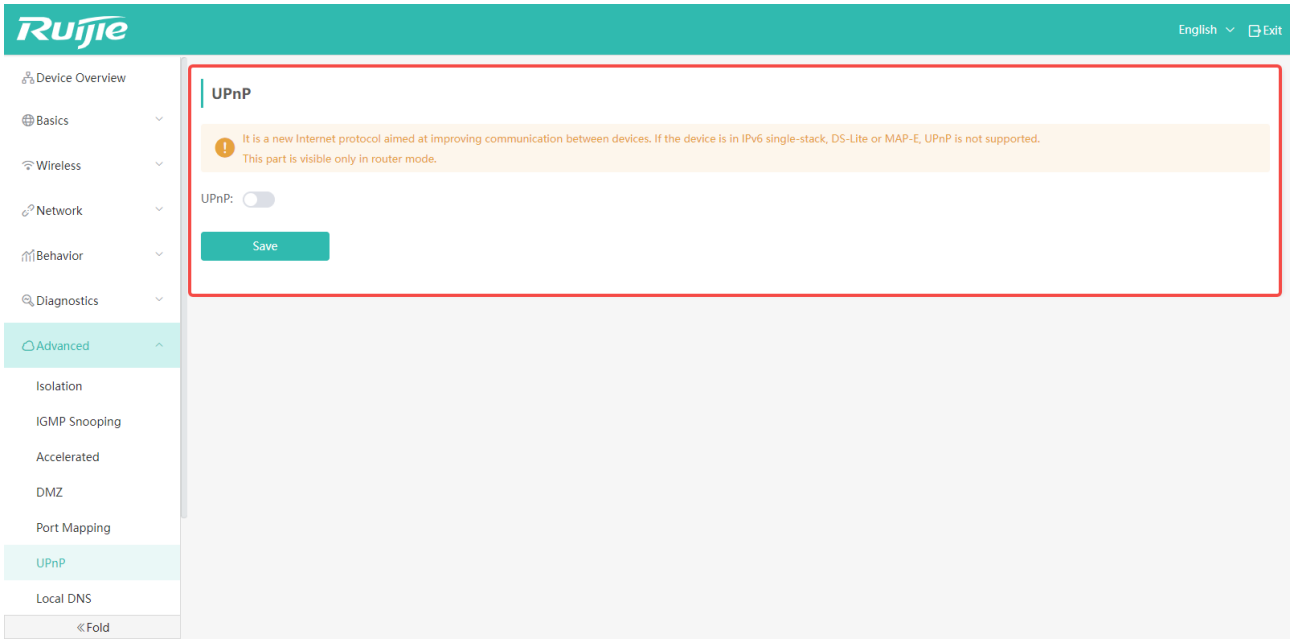


Items	Description	Defaults/Options
Name	Set a rule name.	Default: N/A
Protocol	Specify a protocol.	Default: TCP Options: TCP and UDP
External Port/Range	Specify the port number to be mapped to the external network. By default, the IPv4 address of the external network is the IP address the WAN port.	Default: N/A Port Number Range: 1-65535
Internal IP Address	Specify the IPv4 address to be mapped to the external network.	Default : N/A
Internal Port/Range	Specify the port number to be mapped to the internal network.	Default: N/A Port Number Range: 1-65535

It should be noted that after changing the working mode or network type (such as changing the dynamic IP to the static IP), you need to reconfigure the port mapping.

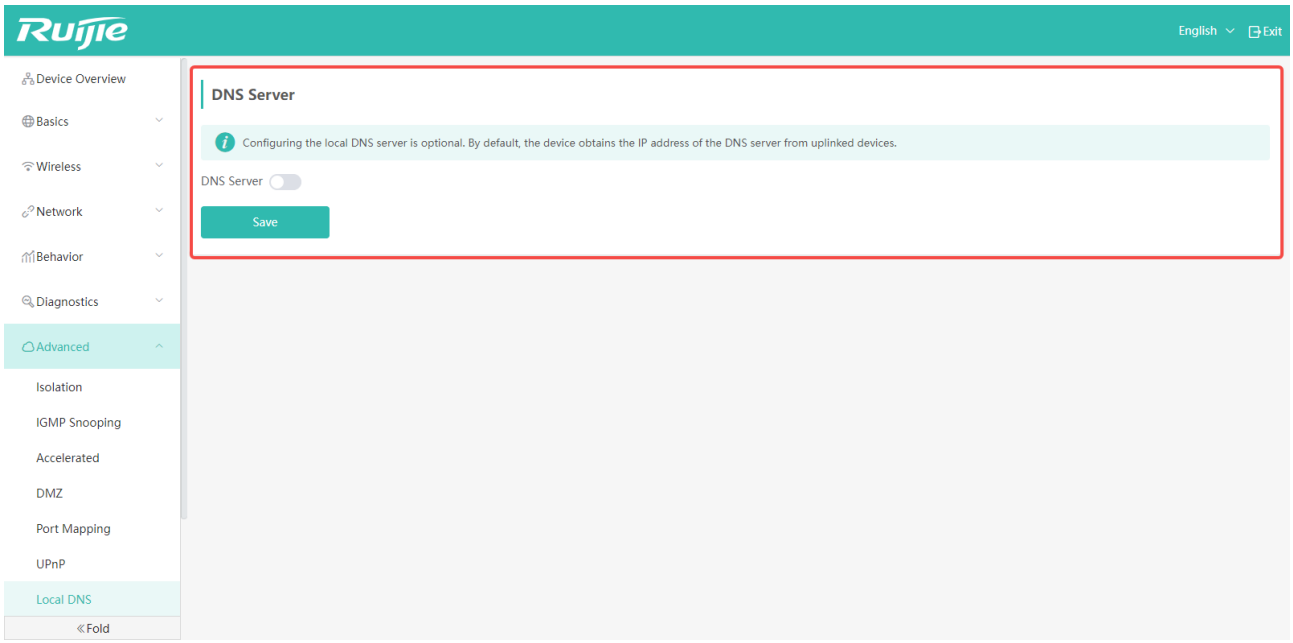
5.6 UPnP (Routing Mode)

The main function of UPnP (Universal Plug and Play) is to automatically install and configure a network device. With the UPnP, devices can share resources within the LAN.

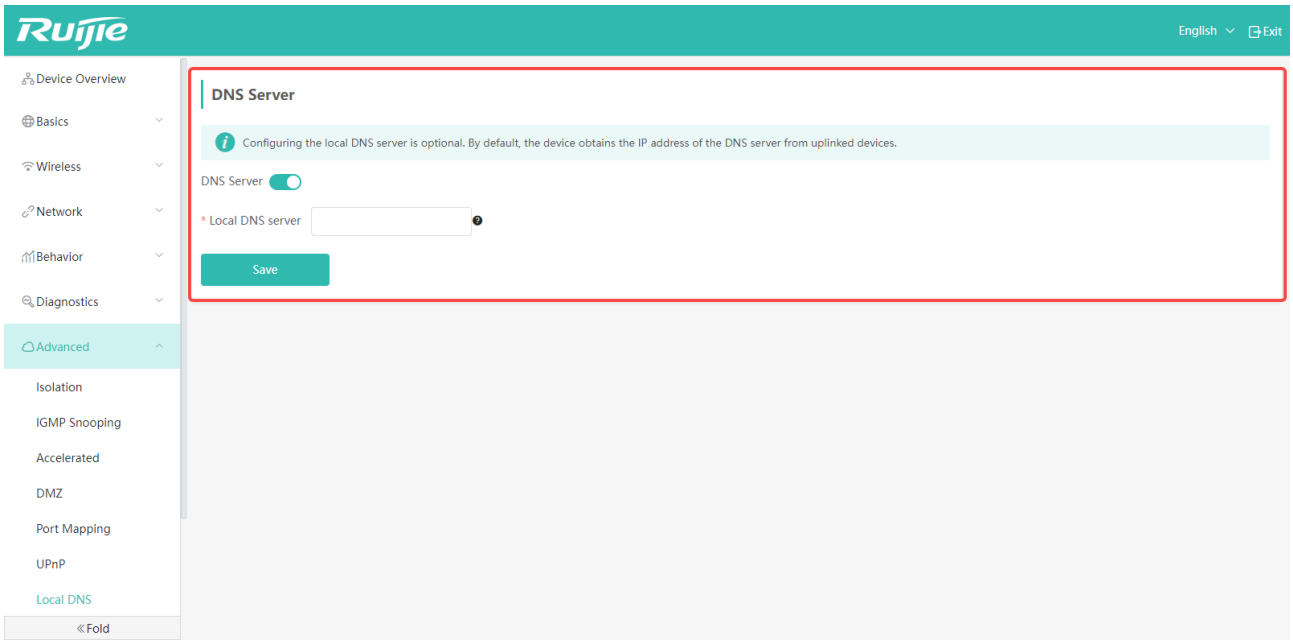


5.7 DNS Server

If you want to use a specific DNS server, you can set it on this page. Usually the DNS server address used by the AP is automatically obtained from its uplink network.



Items	Description	Defaults/Options
DNS Sever	When it is enabled, you can specify the local DNS server address for the AP, so that the AP will not use the address automatically obtained from its uplink network.	Default: Disabled. By default, the DNS address is not specified, but automatically obtained from its uplink network. Options: Enabled/Disabled



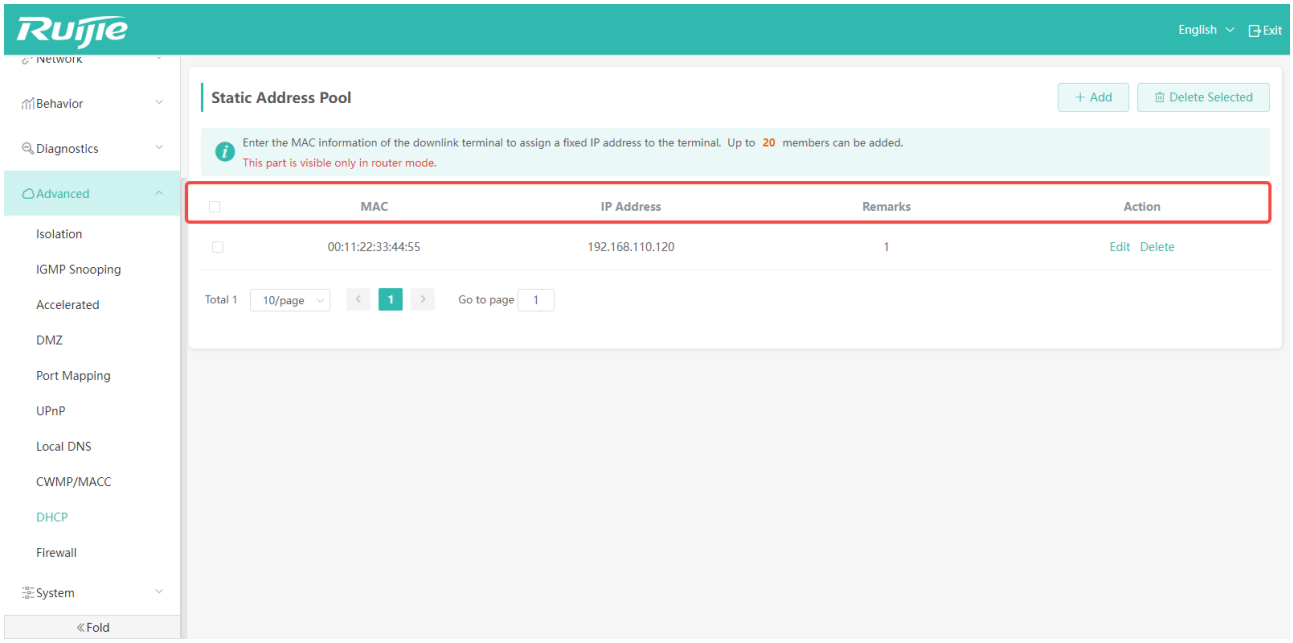
After it is enabled, you can enter the DNS server address.

Items	Description	Defaults/Options
Local DNS Server	Manually specify the address of DNS Server.	Default: N/A. The DNS server address is automatically assigned by the uplink network .

It should be noted that before configuration, please ensure that the DNS Server to be configured is working normally, otherwise it may fail to access the Internet.

5.8 DHCP (Routing Mode)

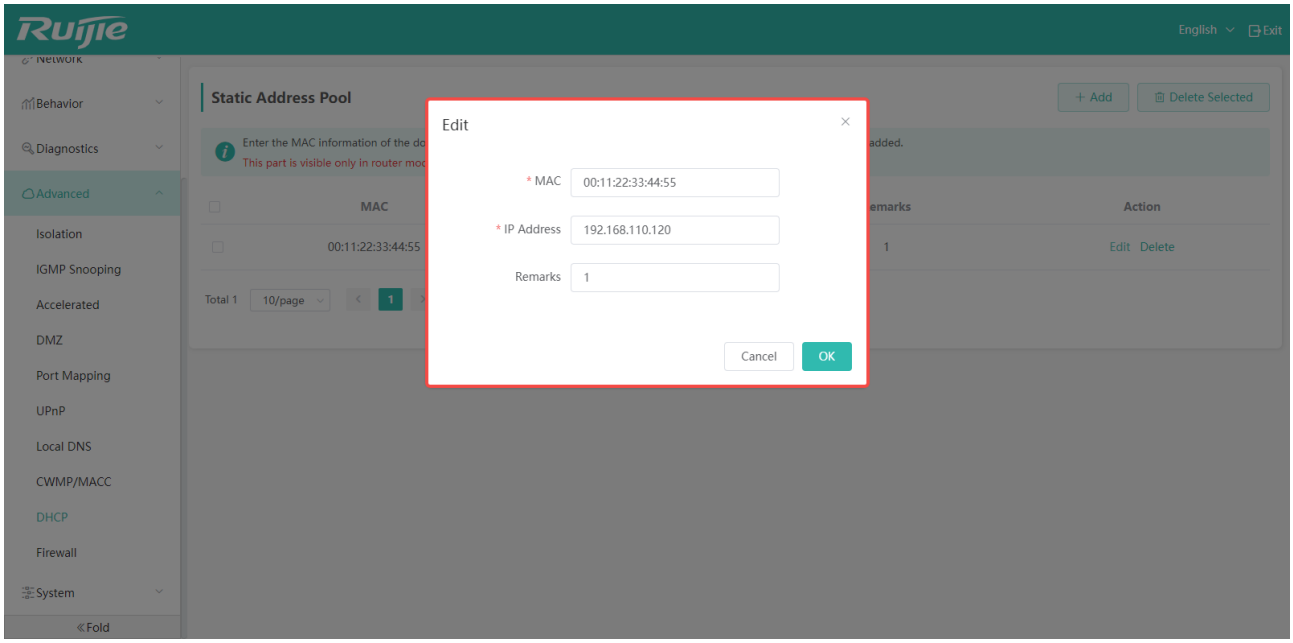
Assign a fixed IP address to the downstream client by adding its MAC address. (Up to 20 clients can be added.)



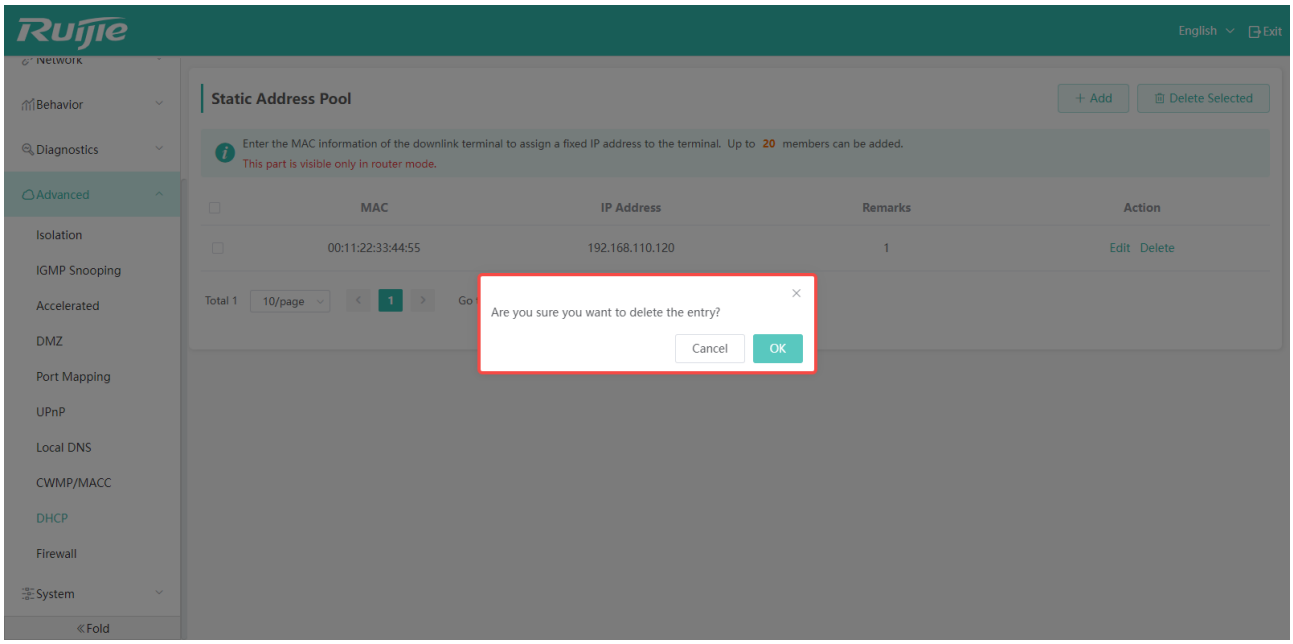
Items	Description
MAC	Display the client's MAC address.
IP Address	Display the assigned IP address.
Remarks	Display the note for the MAC address. You can enter any description such as "my mobile phone".
Action	Two management actions can be performed, including modification and deletion.

The description of "Edit" and "Delete" in the Action column:

- Click "Edit" to modify the client's MAC address, assigned IP and the remark.



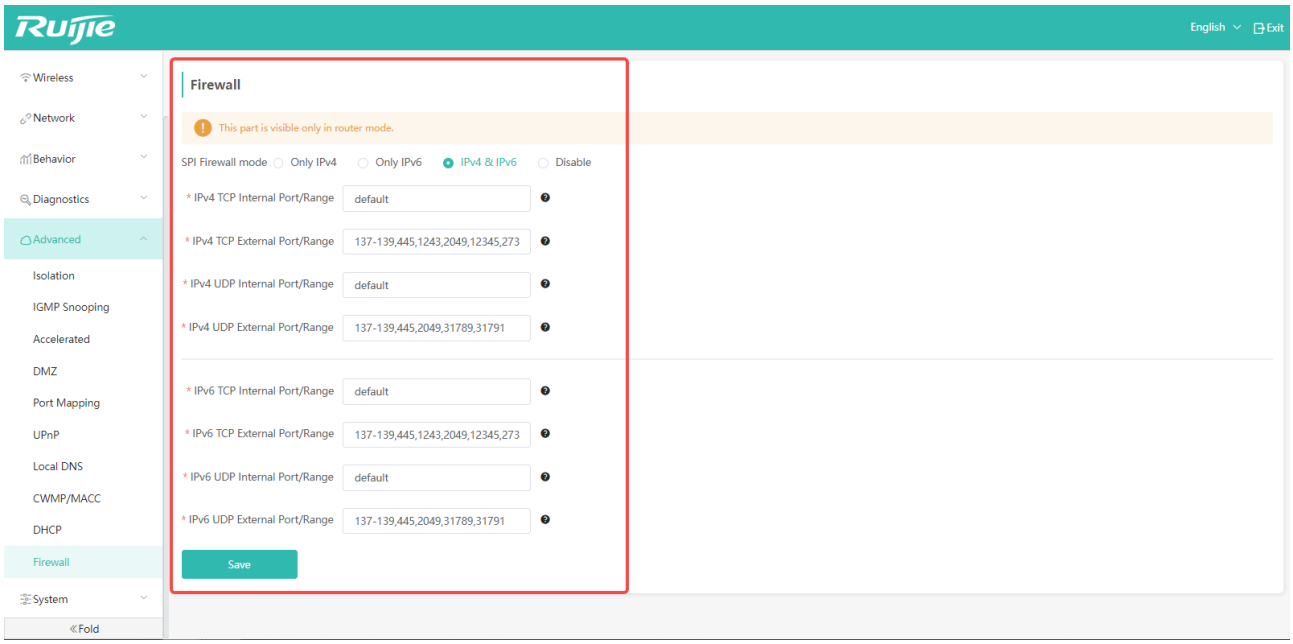
- Click "Delete" to delete the assigned IP. After the AP is connected again, a random IP address is obtained.



5.9 Firewall (Routing Mode)

A firewall is a network security device or software used to monitor and control network traffic to protect the network from suffering unauthorized access, malicious attacks, and data leaks. Firewalls filter network traffic by restricting access to specific IP addresses, ports or protocols through rules or implementing access control policies to block potential threats.

With the firewall feature, the AP restricts access to the ports based on its IPv4 or IPv6 TCP and UDP protocols.



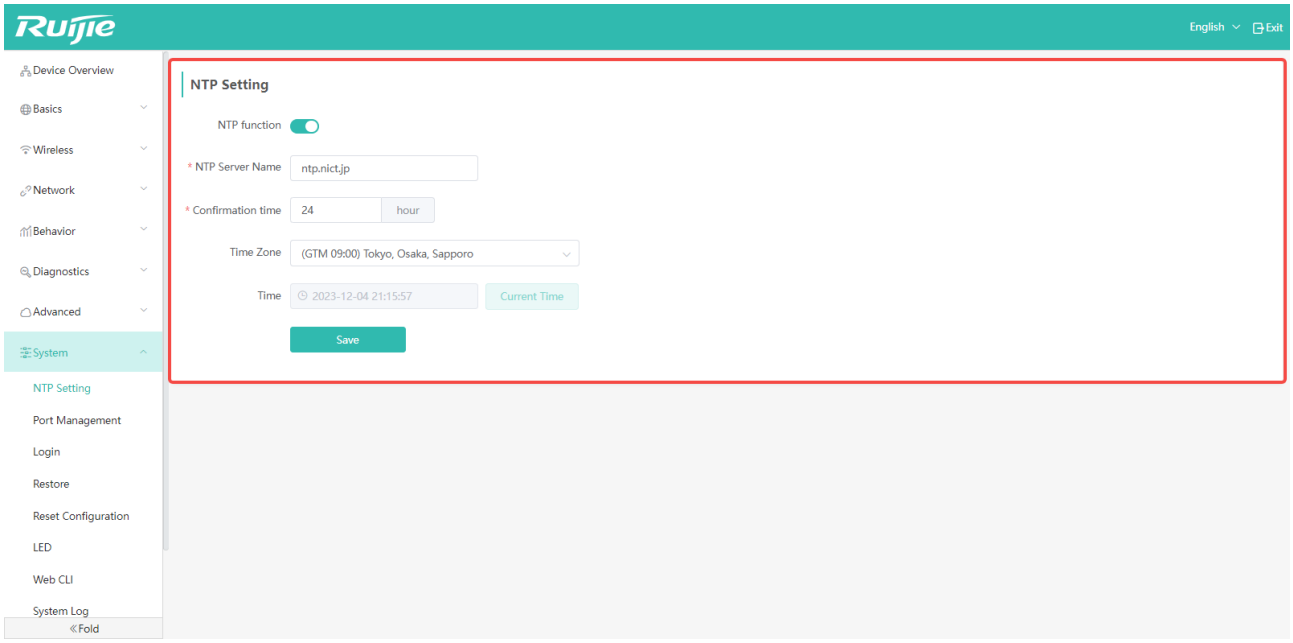
Items	Description	Defaults/Options
SPI Firewall Mode	Four options are available: Only IPv4, IPv4 & IPv6, Only IPv6, Disabled.	Default: IPv4 & IPv6
IPv4 TCP Internal Port/Range	The internal port range of IPv4 TCP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to specify the default configuration, which is to select all ports.
IPv4 TCP External Port/Range	The external port range of IPv4 TCP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated the by commas (,).	It is recommended to specify the following ports that are frequently attacked: 137-139, 445, 1243, 2049, 12345, 27374, 31785
IPv4 UDP Internal Port/Range	The internal port range of IPv4 UDP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to select the default configuration, which is to select all ports.
IPv4 UDP External Port/Range	The external port range of IPv4 UDP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to specify the following ports that are frequently attacked: 137-139, 445, 2049, 31789, 31791
IPv6 TCP Internal Port/Range	The internal port range of IPv6 TCP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to select the default configuration, which is to select all ports.
IPv6 TCP External Port/Range	The external port range of IPv6 TCP is from 1 to 65535. You can specify a single port (X)	It is recommended to specify the following ports that are

	or a port range (X-Y). If multiple items are configured, separated them by commas (,).	frequently attacked: 137-139, 445, 1243, 2049, 12345, 27374, 31785
IPv6 UDP Internal Port/Range	The internal port range of IPv6 UDP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to select the default configuration, which is to select all ports.
IPv6 UDP External Port/Range	The external port range of IPv6 UDP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to select the following ports that are frequently attacked: 137-139,445,2049,31789,31791

6 System Management

6.1 NTP Settings

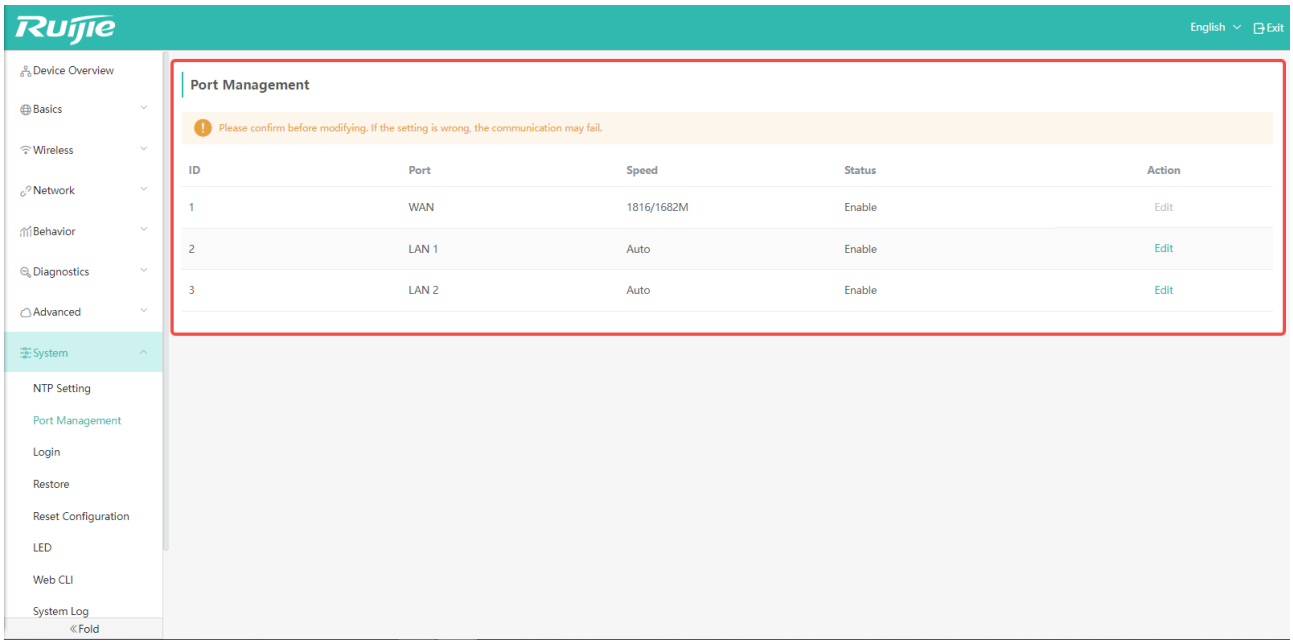
Network Time Protocol (NTP) is a protocol used to synchronize the clocks of devices on a network. NTP is designed to ensure that the consistency and accuracy of clicks of devices on the network.



Items	Description	Defaults
NTP function	Enable or disable NTP function.	Default: Enabled.
NTP Server Name	Specify the domain name of the NTP server.	Default: ntp.nict.jp
Confirmation Time	Specify the synchronization period.	Default: 24 hours
Time Zone	Specify the time zone.	Default: (GTM 09:00) Tokyo, Osaka, Sapporo
Time	Display the current time.	Default: Current time.

6.2 Port Management

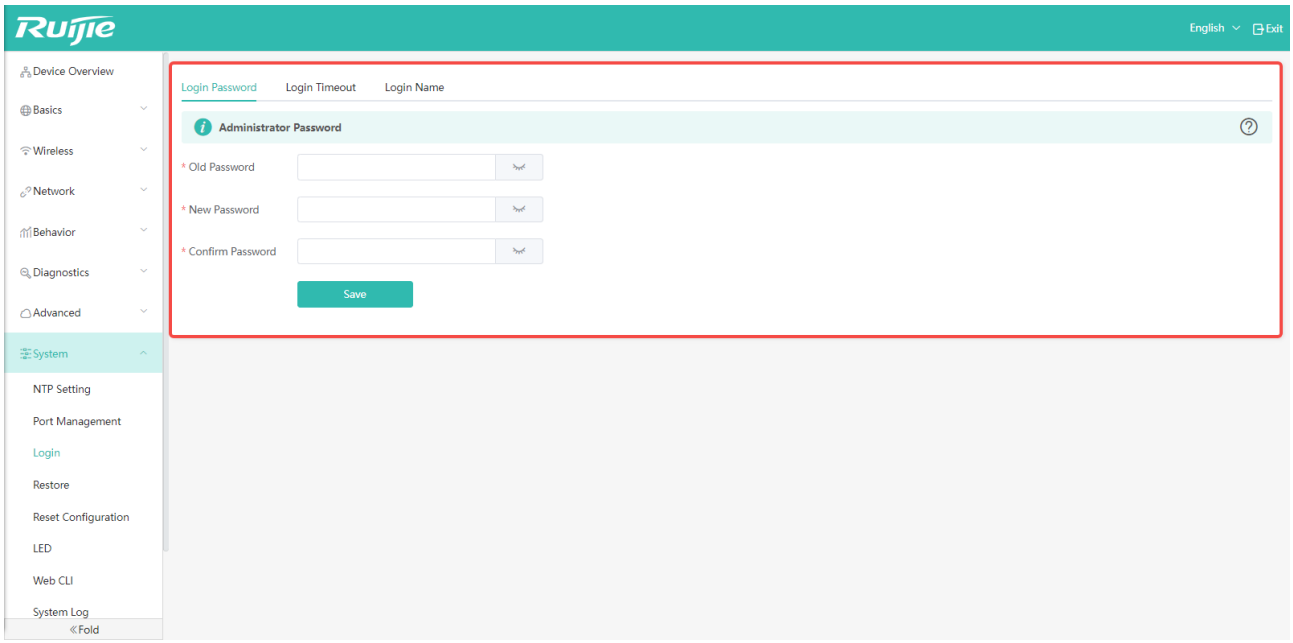
This function is designed to manage the physical attributes of the WAN port and two LAN ports. Currently, a WAN port cannot be set to a G.hn port. The LAN port supports shutdown and rate negotiation (Auto/100Mbps/1000Mbps).



6.3 Login Management

6.3.1 Administrator Password

In order to improve system security and make information interaction more secure, please click "System" -> "Login"-> "Login Password" to change the default password.

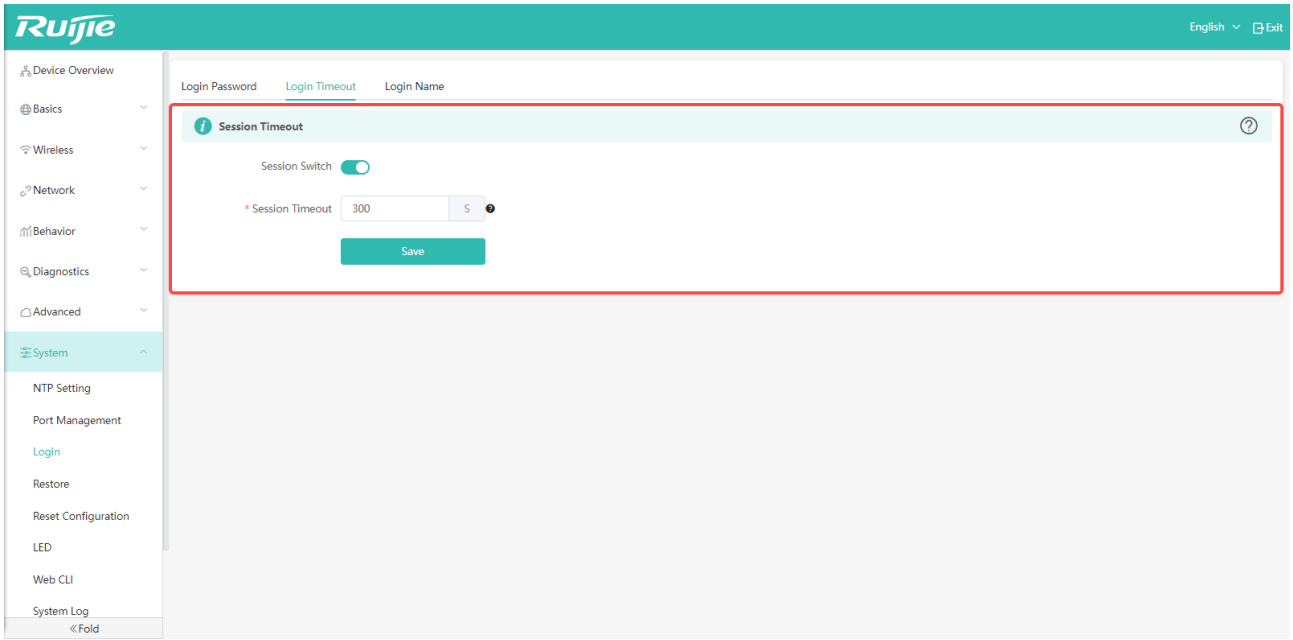


Items	Description	Defaults/Options
Old Password	Enter the original password: admin	Default: admin

New Password	Enter a new password.	Default: N/A
Confirm Password	Enter the password you set for confirmation.	Default: N/A

6.3.2 Session Timeout

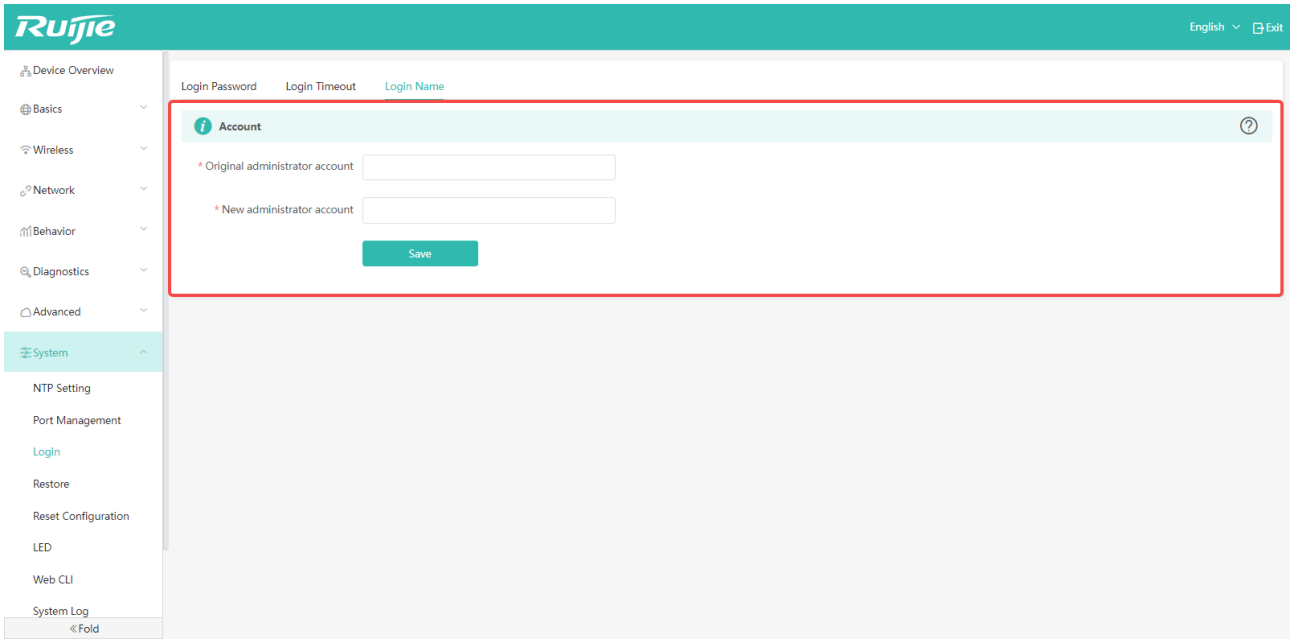
In this page, you can set the Web session timeout. After the timeout is configured, Web will automatically log out when it is in standby state for a long time.



Items	Description	Defaults/Options
Session Switch	Enable or disable the login timeout function.	Default: Enabled. Options: Enabled/Disabled
Session Timeout	When the session timeout is enabled, specify the time value. If no operation is performed on the Web management system for the time that exceeds the configured time, the system will be logged out.	Default: 300 seconds Options: 300-7200 seconds

6.3.3 Account Name

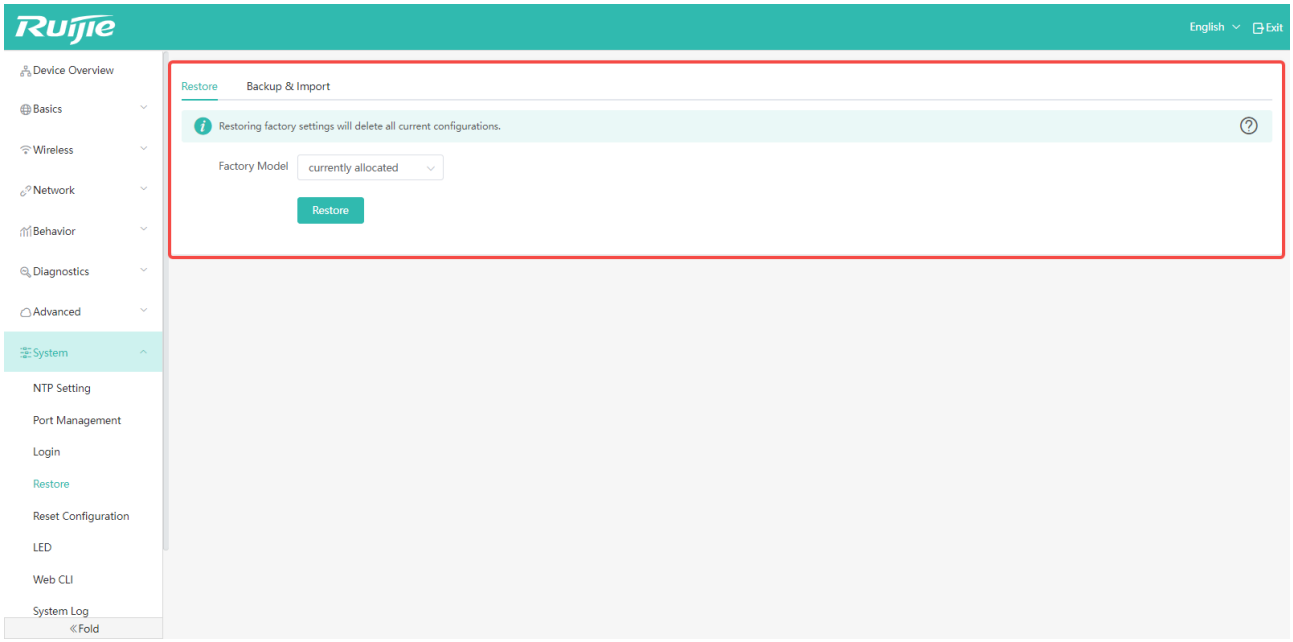
By default, the account name is admin. You can change the account name in the following page.



6.4 Configuration Management

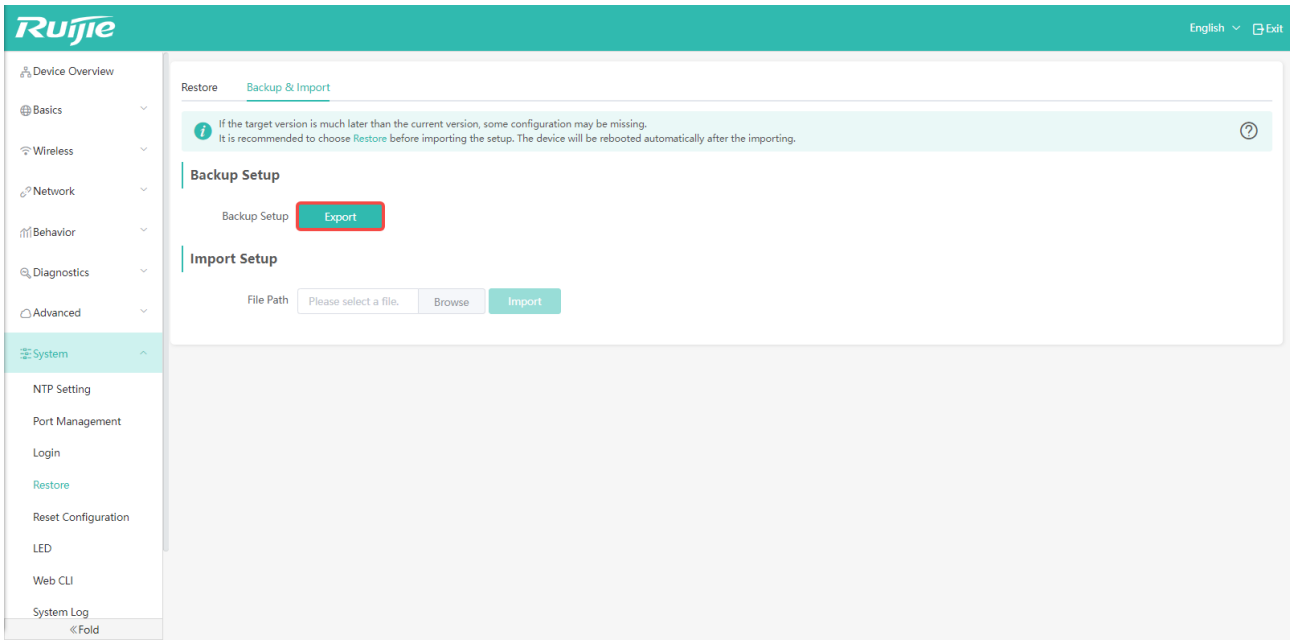
6.4.1 Restore

If you need to restore the system, please click "System" -> "Restore" to restore the device.

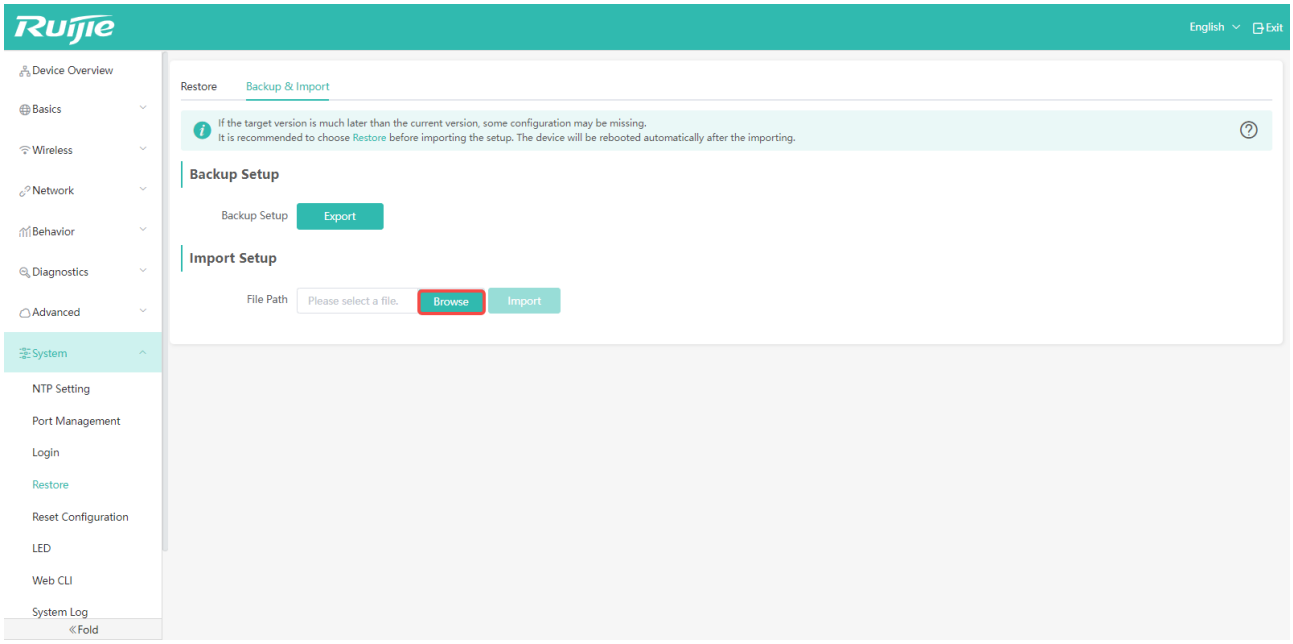


6.4.2 Backup and Import

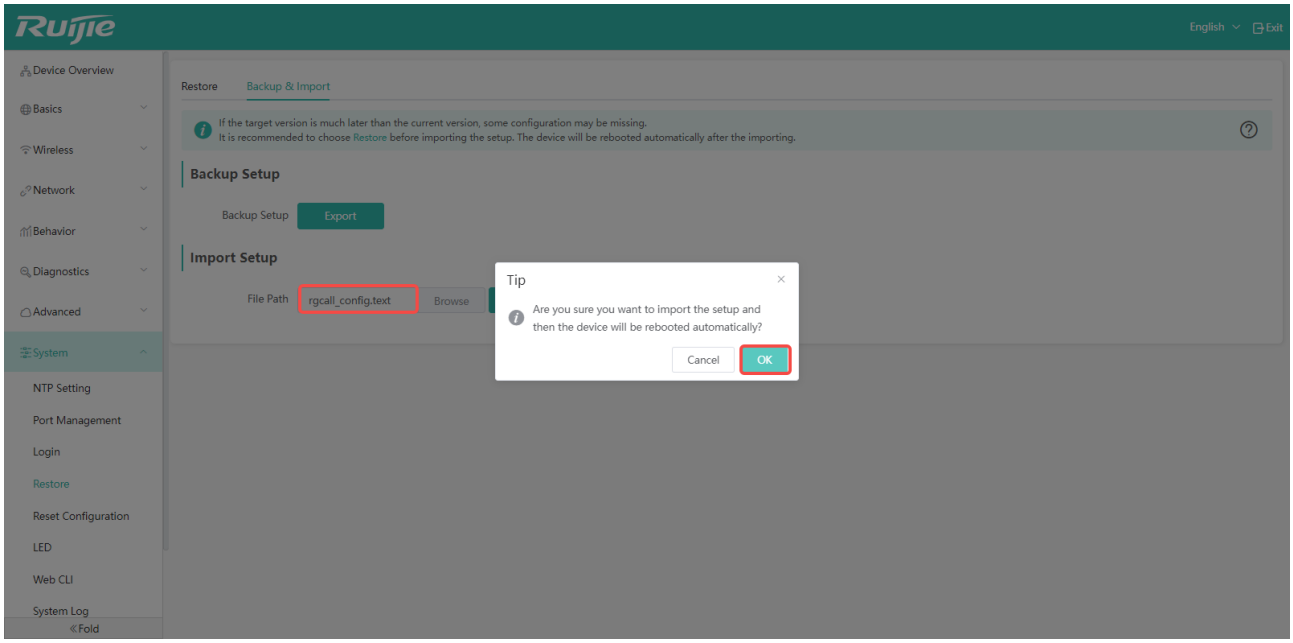
- If you want to keep the current configuration settings after restore the system, please click "Restore" -> "Backup & Import" -> "Export" to export the current configuration file of the device.



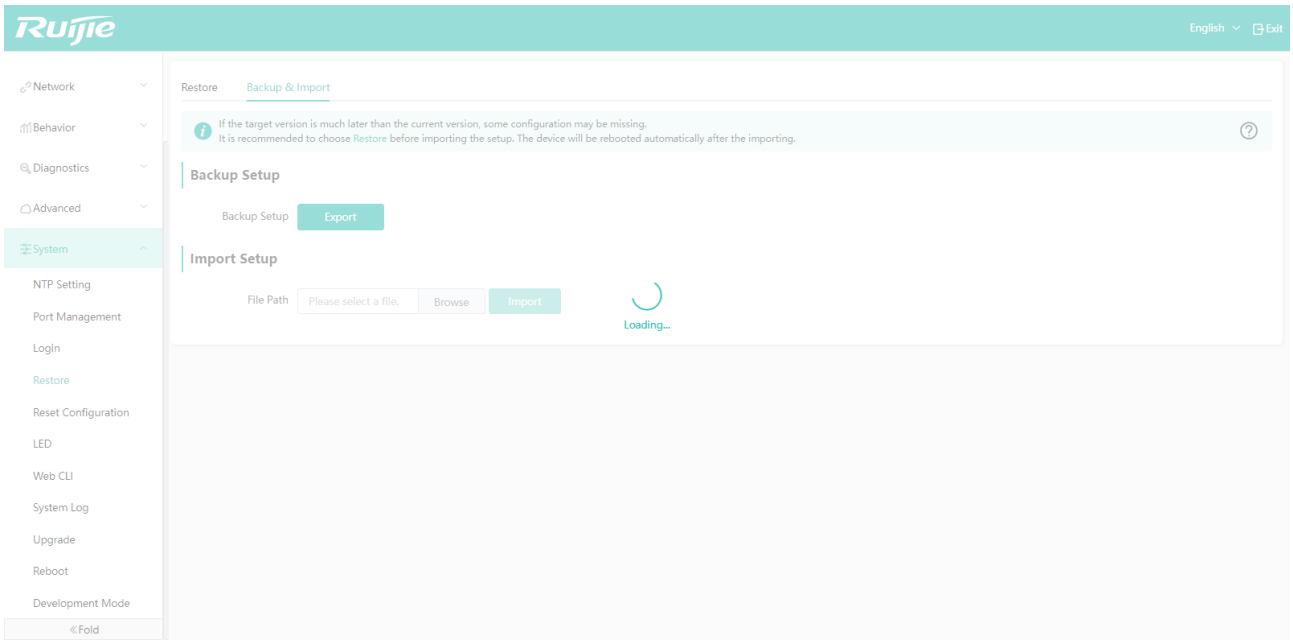
- After the device is restored, if you want to reuse the previous configurations, please click "Browse" in the Import Setup page to select the previous configuration file.



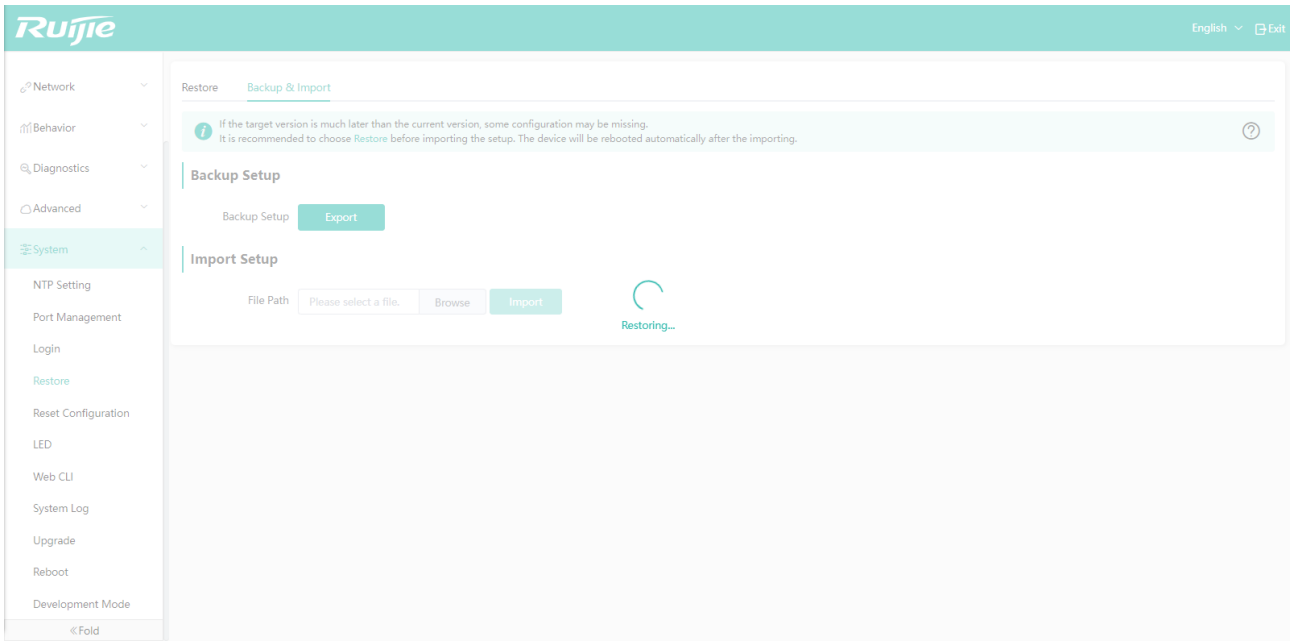
- Click “Import” to import the previous configurations. Then, click “OK” to confirm the operation.



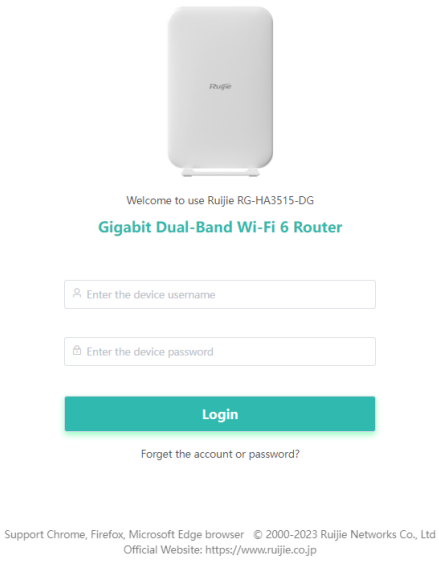
- Load the configurations. Please wait.



- After the configuration is completed, the device will restart. Please wait.



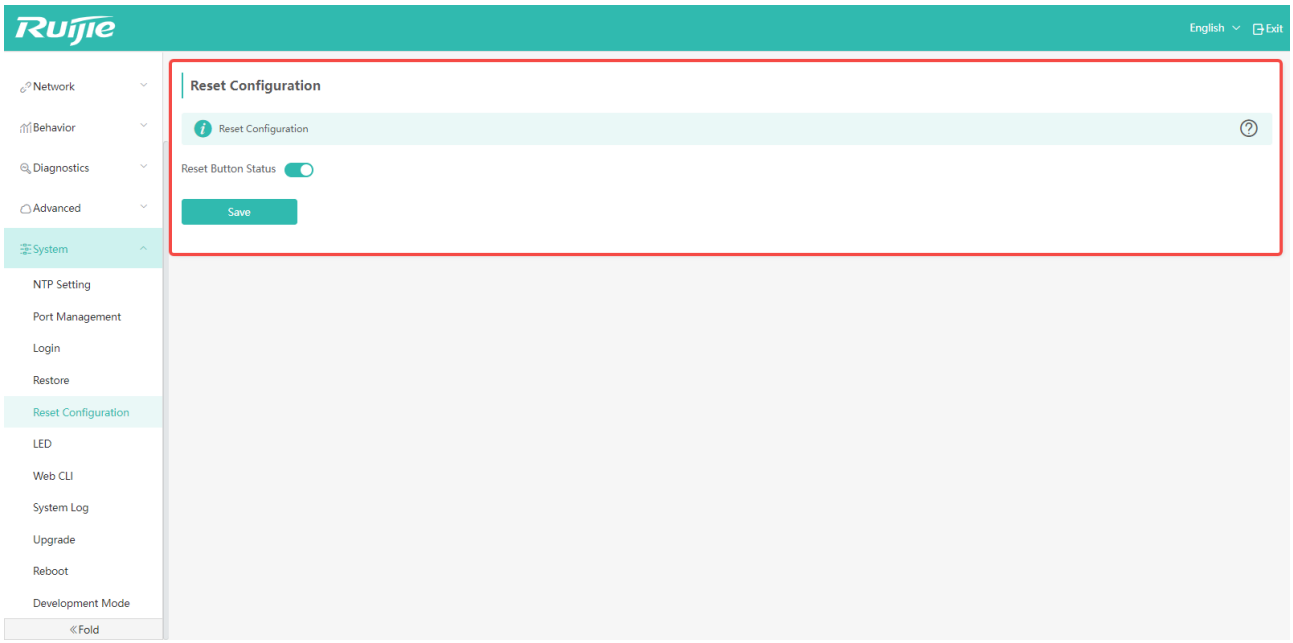
- After the restart is complete, log in to the Web system again.



The related operations of device login have been described in detail in Section 2.1.

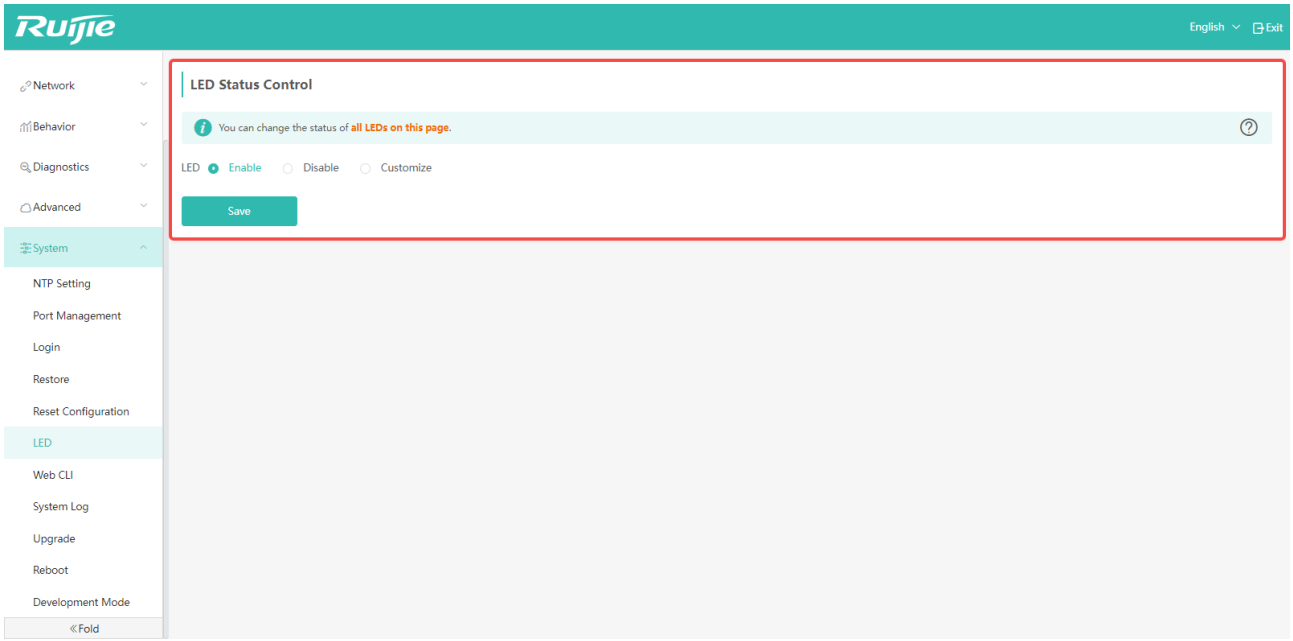
6.5 Reset Settings

In this page, you can determine whether the reset button can be used or not. It is enabled by default.



6.6 LED Settings

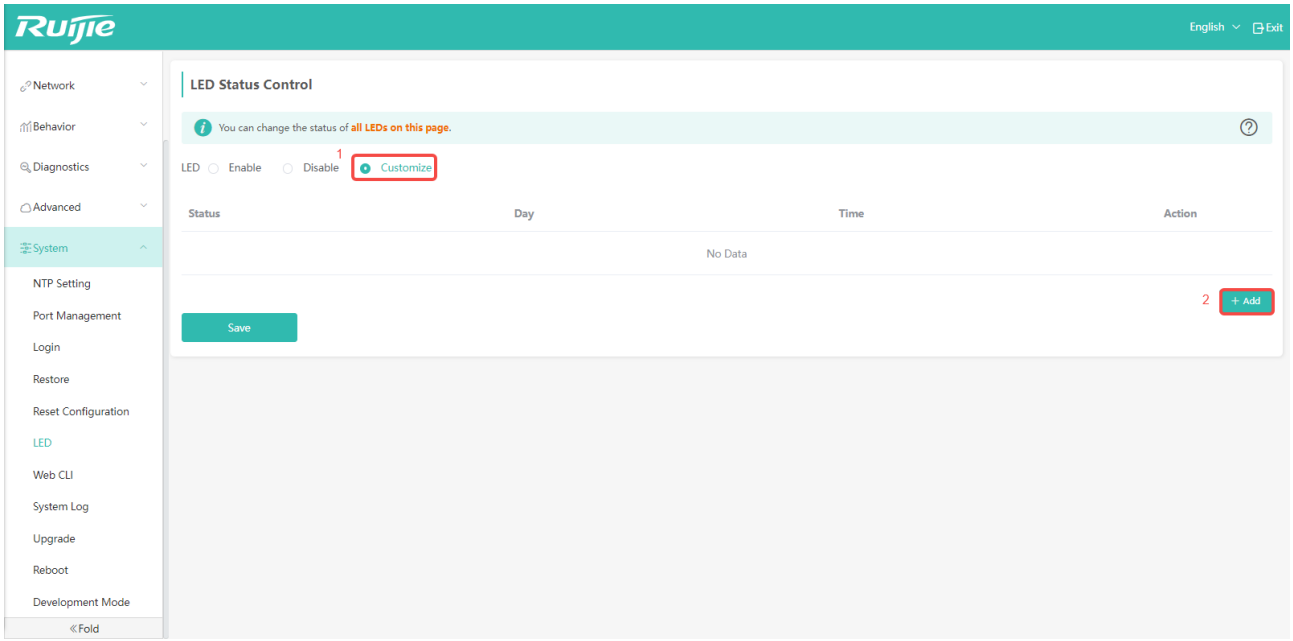
In this page, you can enable or disable LEDs. Also, you can schedule the LED to be enabled or disabled at a specific time period.

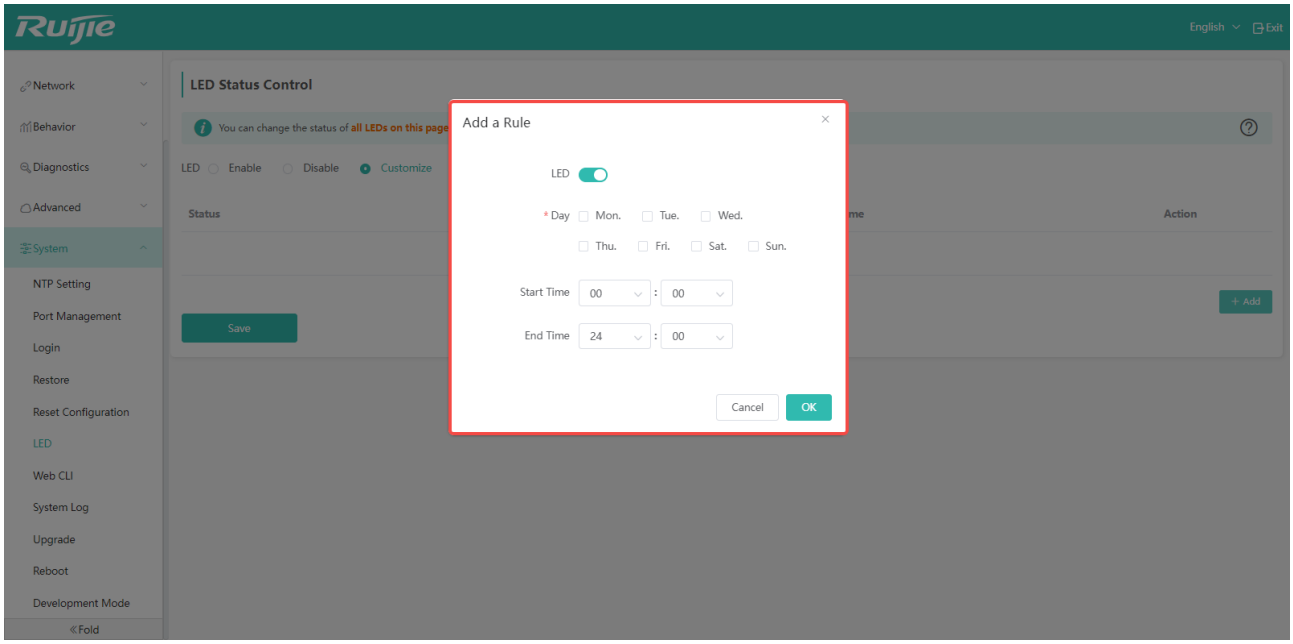


- If you want to LEDs to light at a scheduled time, follow the following steps:

Step 1: Click "Customize".

Step 2: Click the "Add" button to go to the setting page.



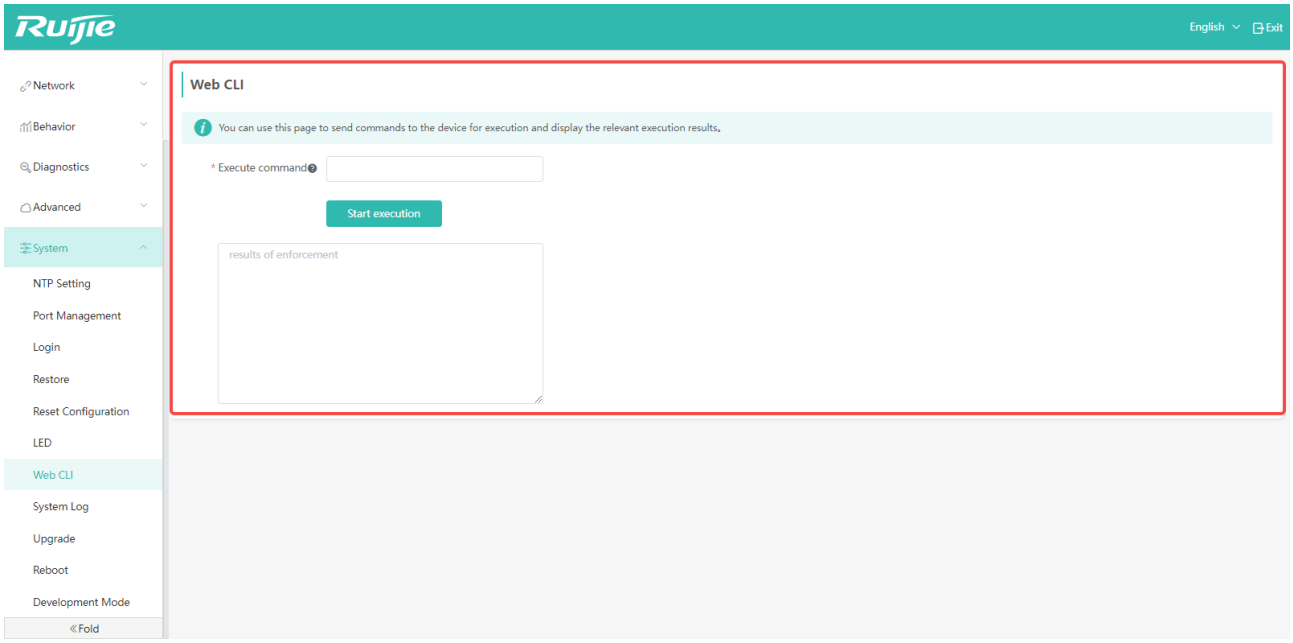


Items	Description	Defaults/Options
LED	If the switch is in on state, it means that the LEDs will turn on in the specified time period. If the switch is in off state, the LEDs will turn off in the specified time period.	Default: Enabled Option: Enabled/Disabled
Day	Specify the day(s) of a week.	Default: N/A Options: Any day of the week.
Start Time	Specify the start time on the day of a week.	Default: 00:00 Drop down the selection box to select a start time.
End Time	Specify the end time on the day of a week.	Default: 24:00 Drop down the selection box to

		select an end time.

6.7 Web CLI

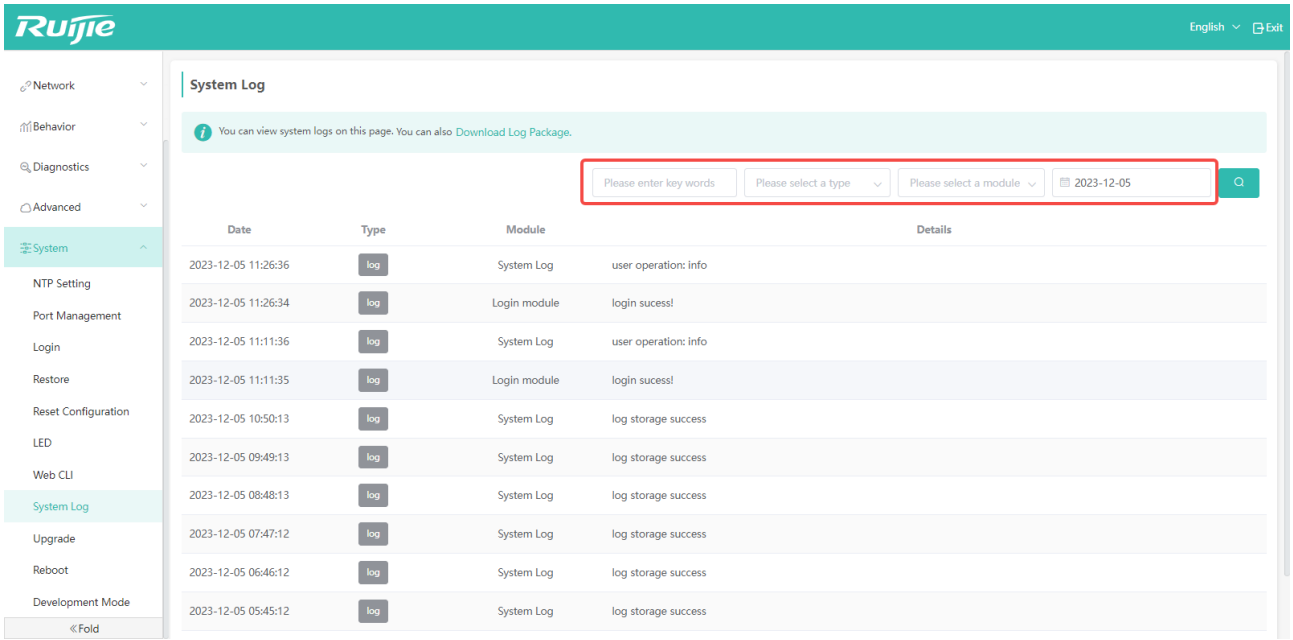
You can run rgcall commands in the page to deliver configurations.



6.8 System Log

Checking system logs is a way for locating fault causes.

When a large number of logs are available, you can enter key words, log types, modules or dates to figure out the logs you need for locating fault causes.

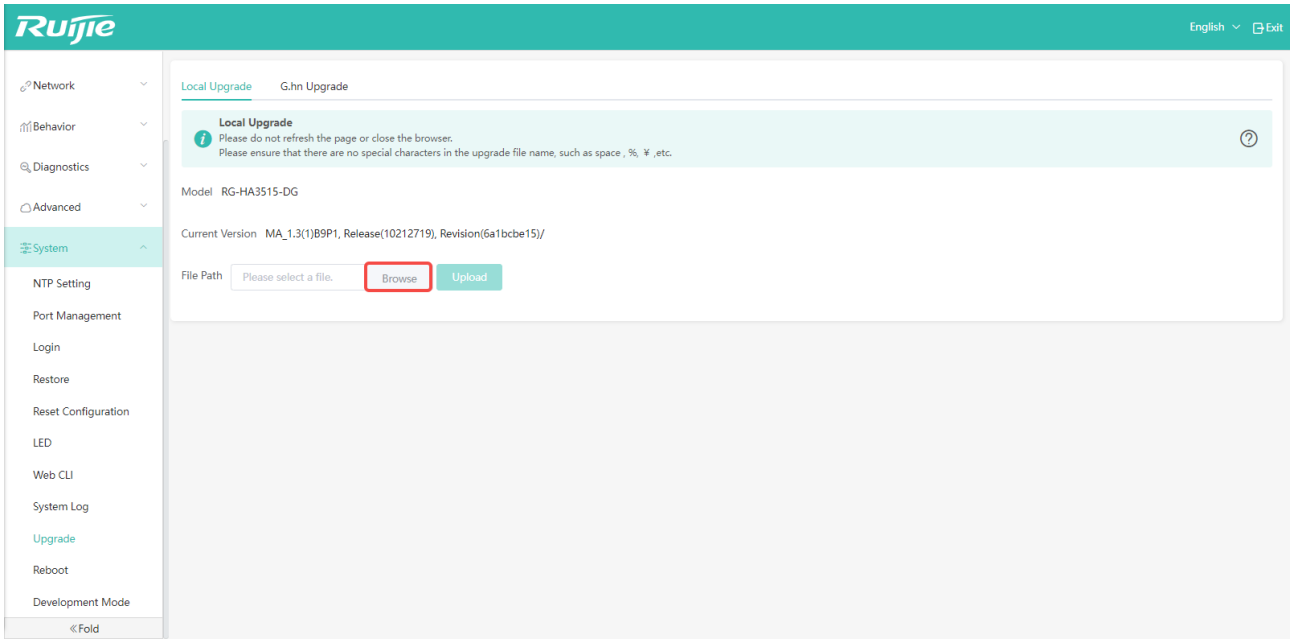


6.9 System Upgrade

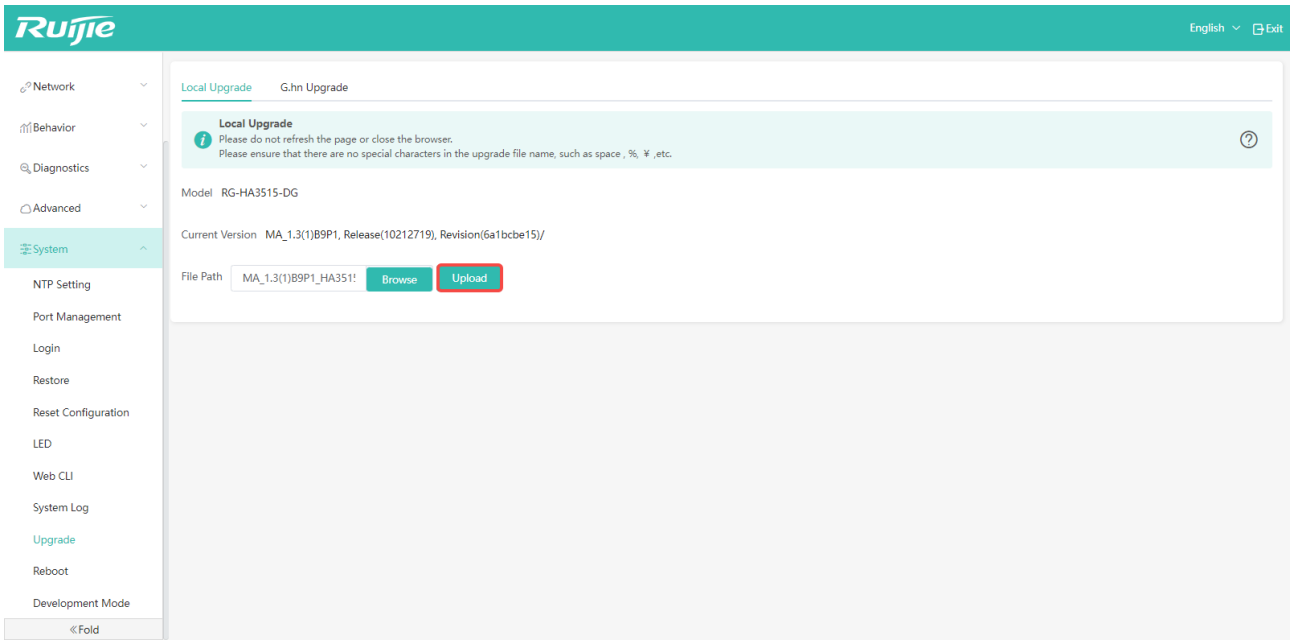
6.9.1 Manual Upgrade

Click "System" -> "Upgrade" to manually upgrade the software version of the device

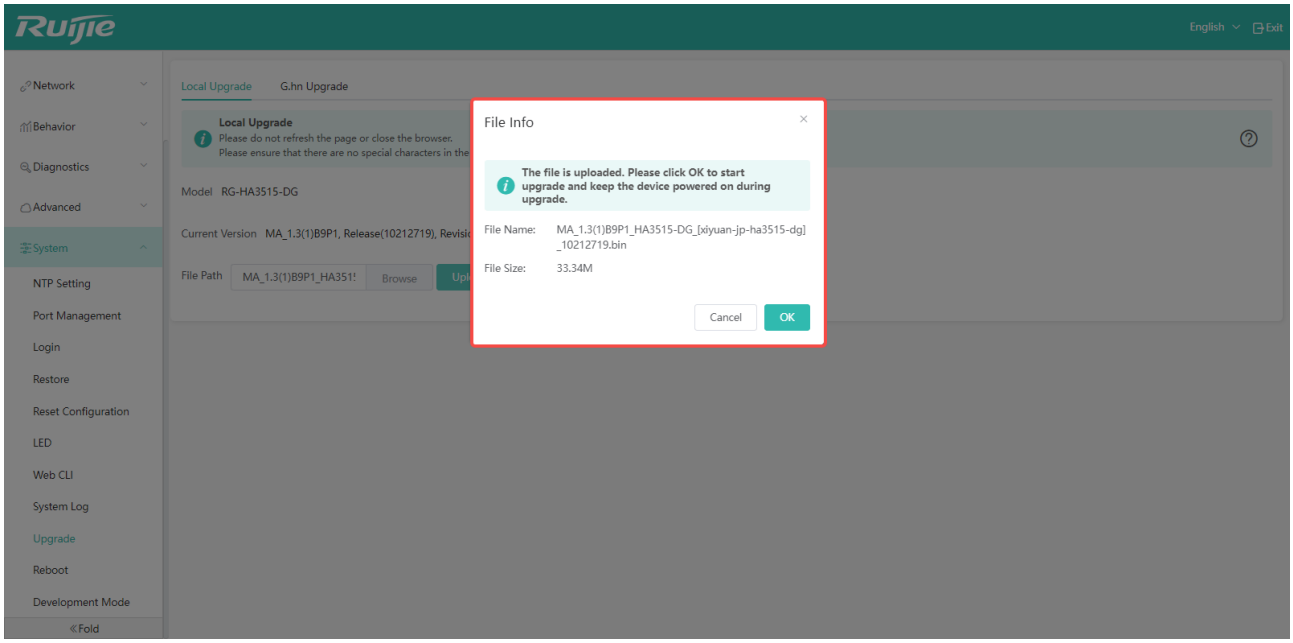
Step 1: Click the "File" button to select an upgrade file.



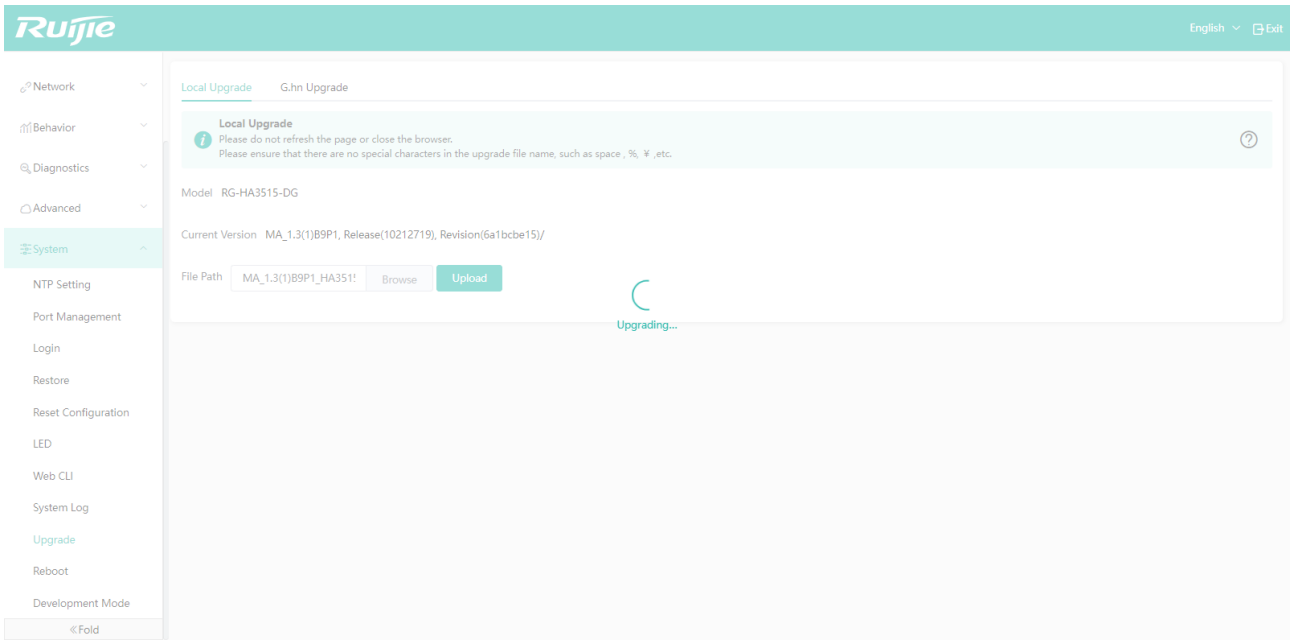
Step 2: After selecting the upgrade file, click the "Upload" button to start downloading the software to the device.



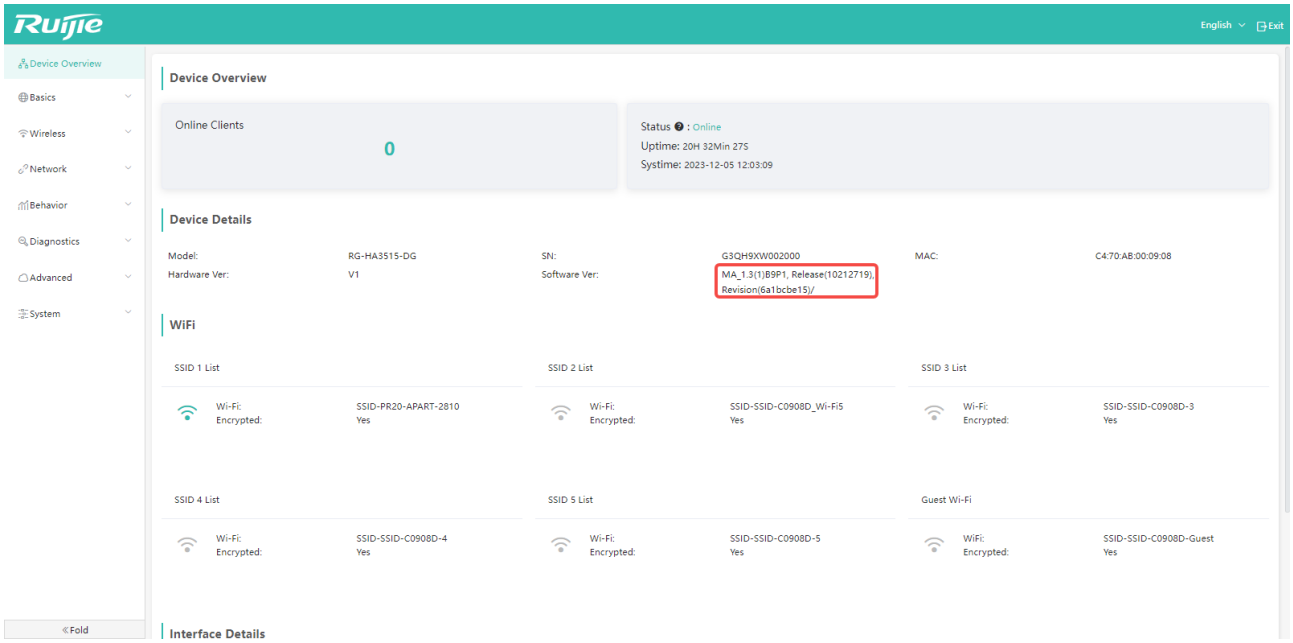
Step 3: Click " OK " to start the upgrade process.



Please wait patiently during the upgrade process.

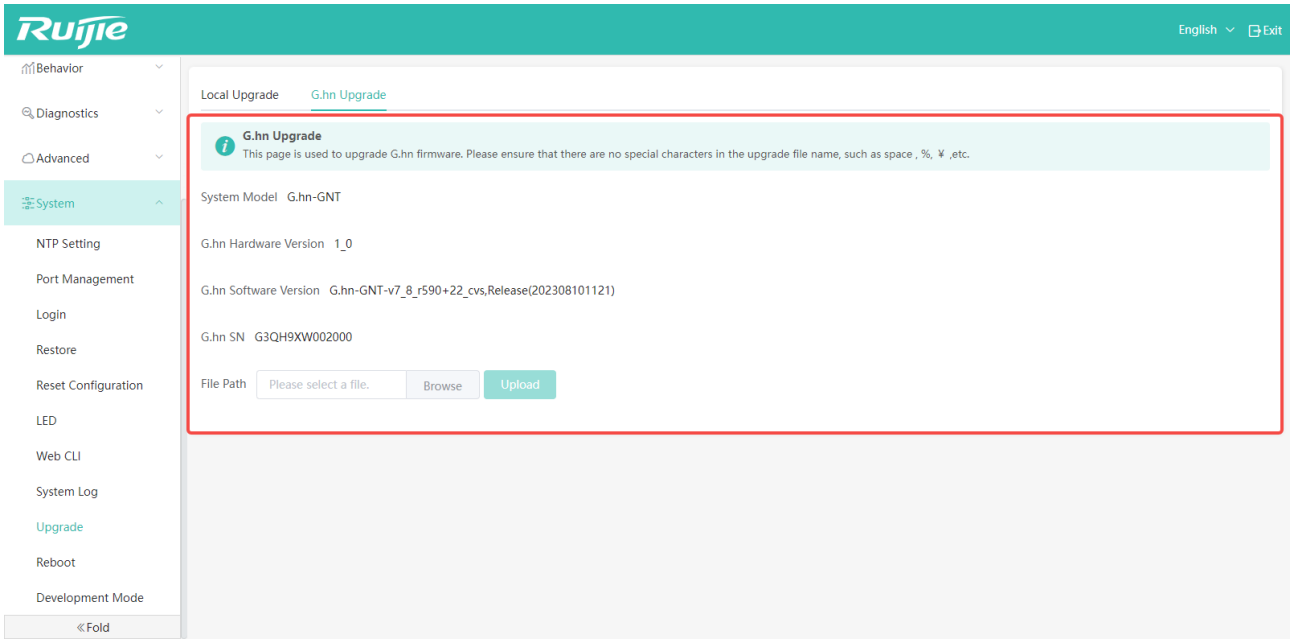


Step 4: After the upgrade is successful, you will return to the login interface. Please use the password to log into the Web management system again, and check the software version in "Device Details" to confirm whether the upgrade is successful.



6.9.2 G.hn Firmware Upgrade

G.hn firmware can be upgraded separately. The upgrade of G.hn firmware is perfumed by the main program.

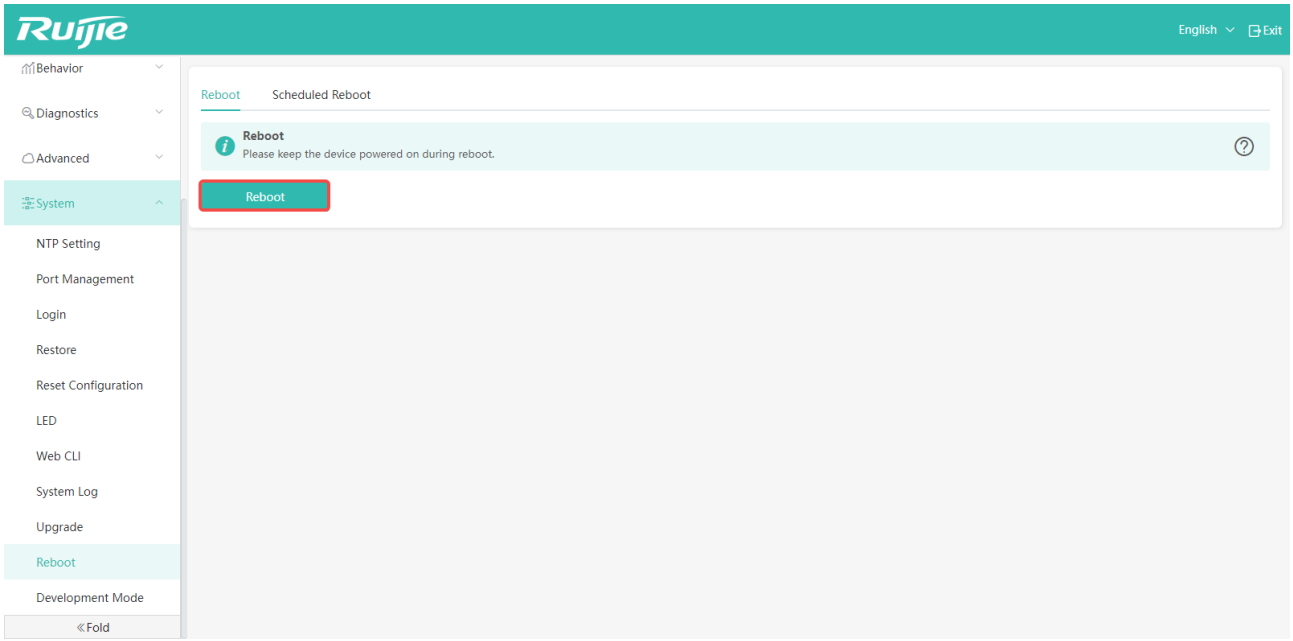


6.10 Reboot

6.10.1 Reboot

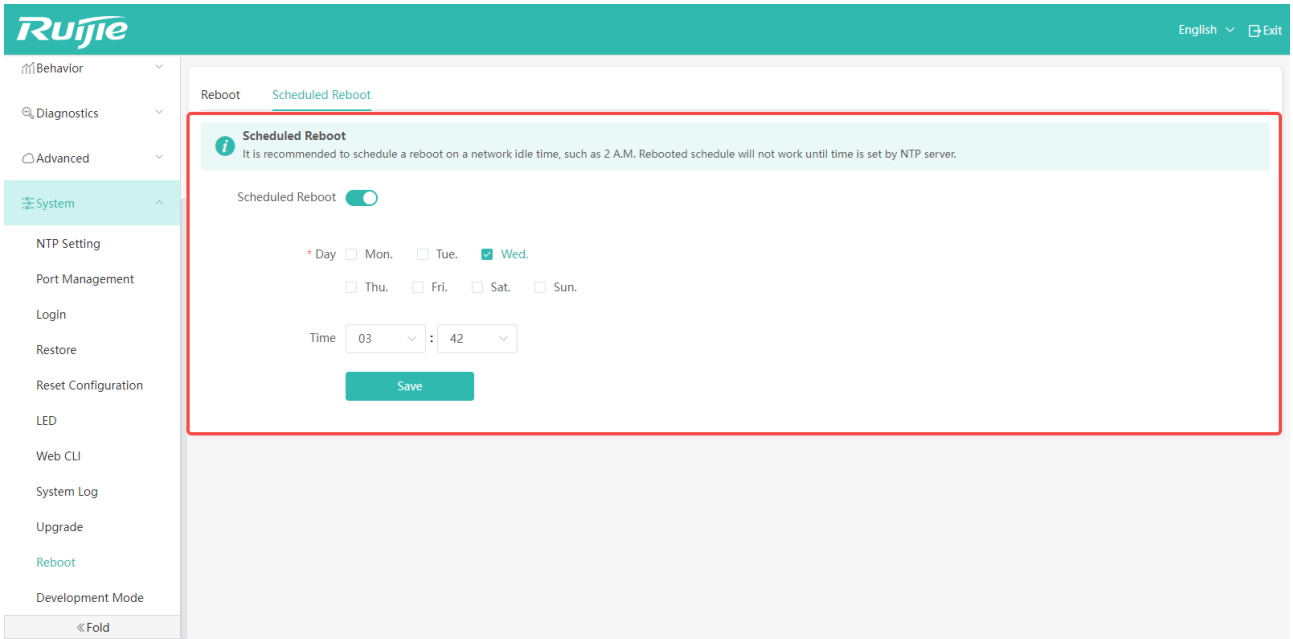
You can click "System" -> “Reboot” to reboot the AP remotely.

If you want to reboot the device directly, click “Reboot” on the page.



6.10.2 Scheduled Reboot

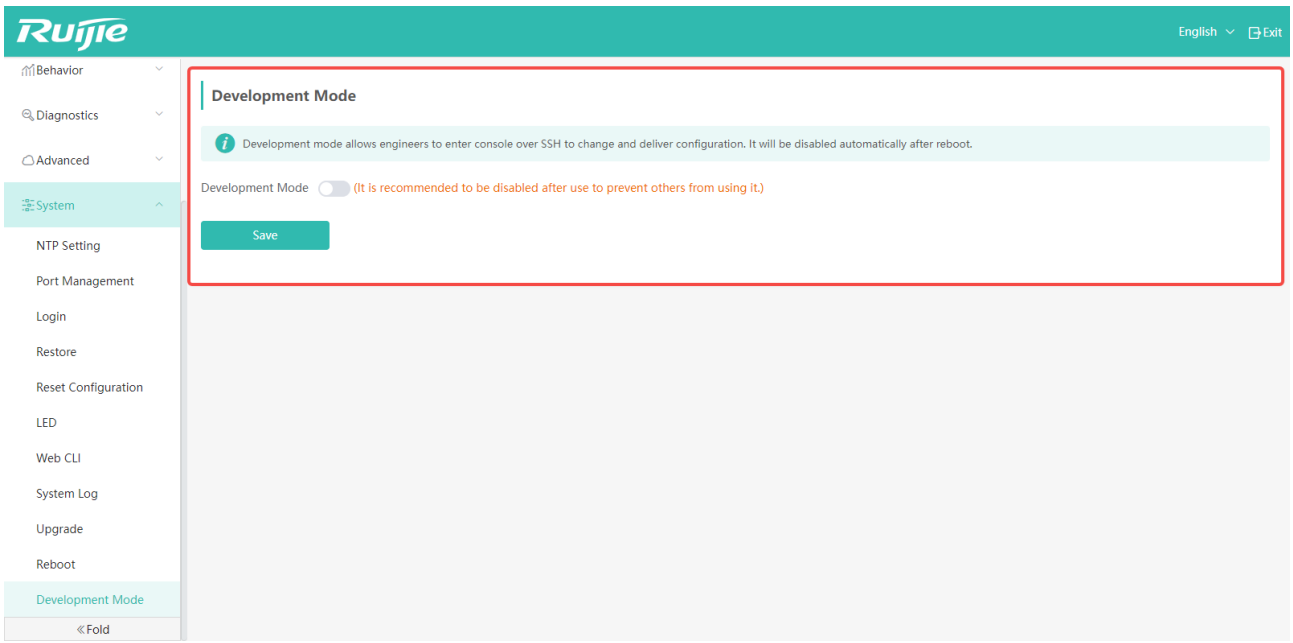
In this page, you can schedule the reboot of the AP to take effect at a specific time in a day of a week.



Items	Description	Defaults/Options
Scheduled Reboot	Enable or disable the scheduled reboot function.	Default: Disabled. Option: Enabled/Disabled
Day	Specify the day of a week to restart the device.	Default: Any day of the week.
Time	Set the specific time to restart the device.	Default: A specific time between 3 a.m and 4 a.m.

6.11 Developer Mode

With the developer mode enabled, you can log in to the device console through SSH to configure the device.



7 Troubleshooting

This chapter mainly introduces countermeasures when you encounter problems that you cannot solve.

7.1 Failing to Connect to Web-GUI

When you cannot connect to the Web-GUI, please confirm the following points:

(1) Check the connection between the AP and your PC.

Please refer to section 1.4 "Preparation for Web-GUI Connection" to confirm whether the connection is correct.

(2) Check whether the AP works in routing mode and the PC accesses the AP through the LAN port.

When the AP works in routing mode, the PC cannot access the AP via a WAN port, because the WAN port is a G.hn port. By default, the PC accesses the AP via the LAN port.

(3) Check whether the PC can ping the AP.

(4) Check whether your browser can display the Web-GUI interface correctly.

The Web-GUI of HA3515-DG supports Google Chrome, Firefox, Safari and some browsers based on IE kernel. It is strongly recommended that you use Google Chrome to access the Web-GUI again.

7.2 Failing to Log into Web-GUI

If you cannot log in to the Web-GUI, please check the following points:

(1) Check whether the username and password are correct.

Please log in again with the correct username and password. Default username/password: admin/admin.

(2) Forget the password.

If you forget the login password, you can use a slender needle to press the Reset button on the AP panel to restore the device to factory settings.

(3) Check whether the browser you use can display the Web-GUI interface normally.

The Web-GUI of HA3515-DG supports Google Chrome, Firefox, Safari and some browsers based on IE kernel. It is strongly recommended that you use Google Chrome to access the Web-GUI again.

7.3 Communication Failure

When the device connects normally but cannot communicate normally, please check the following things:

(1) Check device status:

When the IP address of WAN port is set to be obtained automatically via DHCP, you can check the interface status by checking whether the AP automatically obtains an IP address or DNS address.
If the address cannot be obtained, the WAN cannot be connected (no Internet service is provided). Please check whether the DHCP server is reachable or whether the IP+ MAC binding have been configured.

(2) Blacklist and Whitelist

Only clients in the whitelist are allowed to access the Web-GUI. If the device cannot communicate normally, check whether the device has been listed in the whitelist. If not, please add the device to the whitelist. Also, check whether the device has been added to the blacklist by mistake.

For details, please refer to section 4.4.1 "Access Control".

7.4 About Device Setup and Usage Support

If you need to analyze the cause of a fault or collect usage status, please refer to section 6.8 "System Log". And provide the saved logs to your service provider for support.