



Ruijie RG-EW1200 Router Web-Based Configuration Guide

Copyright Statement

Ruijie Networks©2020

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerpt, 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.

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. 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

Thank you for using our products.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: [service_rj@ruijienetworks.com](https://www.ruijienetworks.com)

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

1 Overview

eWeb is a Web-based network management system that manages or configures devices. You can access eWeb via browsers such as Google Chrome.

Web-based management involves a Web server and a Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

1.1 Conventions

In this document, texts in bold are names of buttons (for example, **OK**) or other graphical user interface (GUI) elements (for example, **ARP List**).

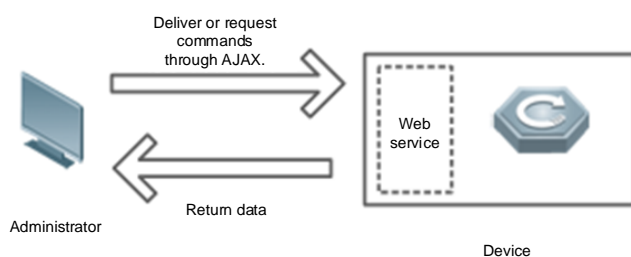
2 Configuration Guide

2.1 Preparation

Scenario

As shown in the figure below, an administrator can access the device from a browser and configure the device through the eWeb management system.

Figure 2-1-1 Data Exchange Principle



Remarks	The eWeb management system combines various device commands and then delivers them to the device through AJAX requests. The device then returns data based on the commands. A Web service is available on the device to process basic HTTP protocol requests.
----------------	---

Deployment

Configuration Environment Requirements

Client requirements:

- An administrator can log into the eWeb management system from a Web browser to manage devices. The client refers to a PC or some other mobile endpoints such as laptops or tablets.
- Google Chrome, Firefox, IE10.0 and later versions, and some Chromium-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned and the GUI is less artistic, or other exceptions may occur.
- The client IP address is set in the same LAN network as the device IP address, such as 192.168.110.X. The subnet mask is 255.255.255.0. The default gateway is device management address 192.168.110.1. Alternatively, you can set the IP assignment mode to **Obtain an IP address automatically** or enter **ruiyi.cn** into the address bar of the browser to access eWeb.

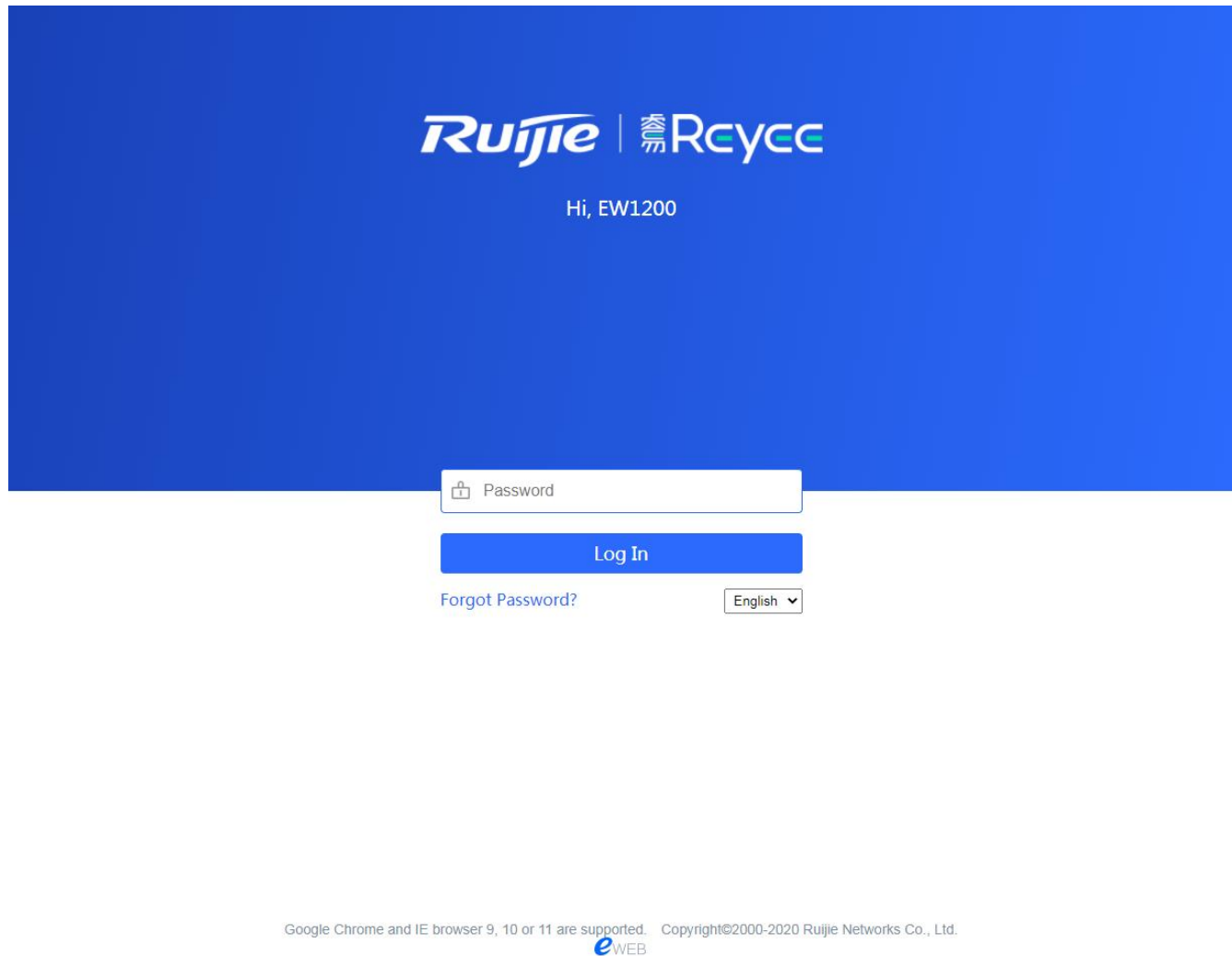
Server requirements:

- The device is enabled with Web service (enabled by default).

- The device is configured with a management IP address (Default: 192.168.110.1).

To log into the eWeb management system, open the Google Chrome browser, and enter `http://ruiyi.cn` into the address bar, and press **Enter**.

Figure 2-1-2 Login Page



Enter the password and click **Login**.

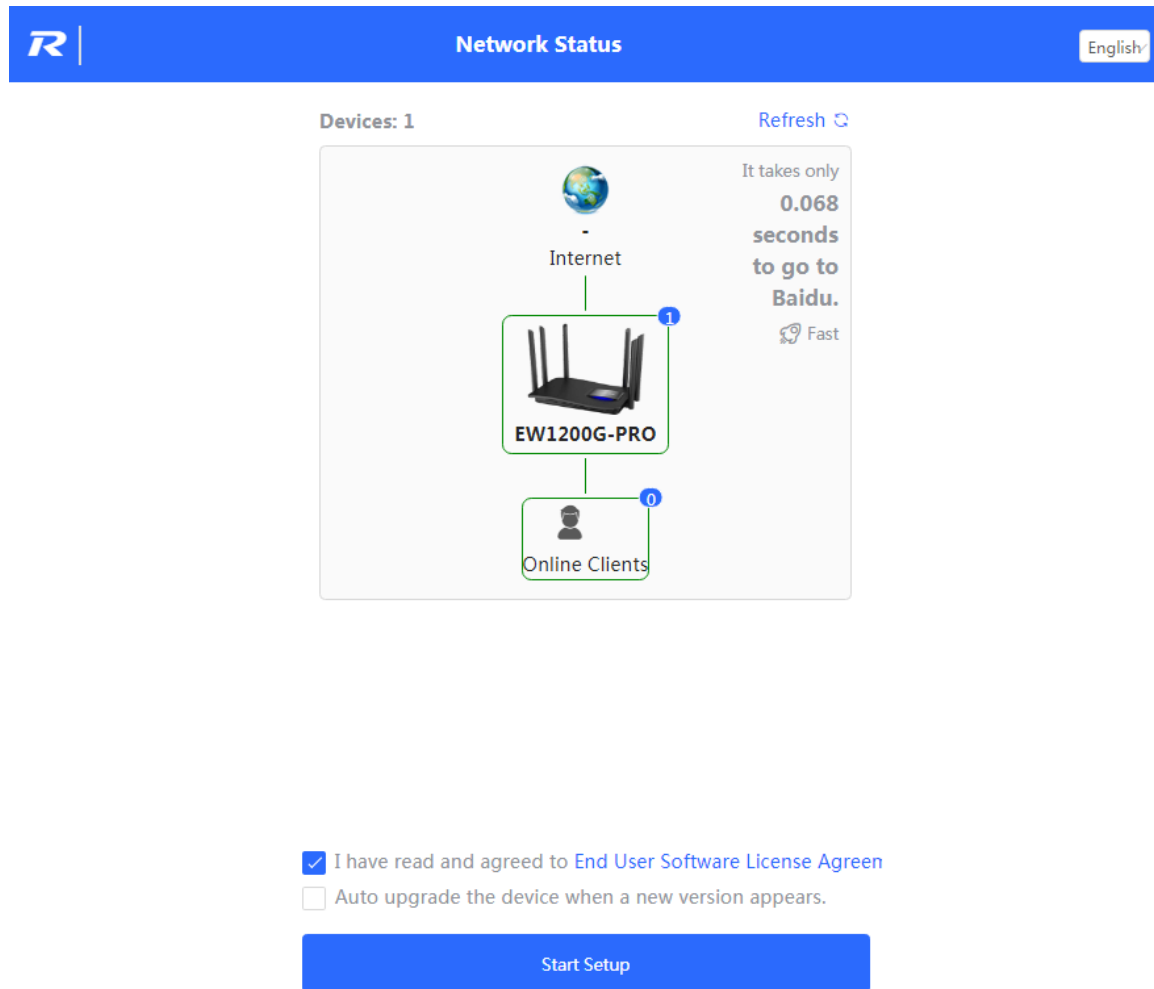
2.2 Wizard

You will enter the **Wizard** page without login at initial setup.

2.2.1 Network Status

The page displays device count, client count, network status and the time it takes to go to Baidu.

Figure 2-2-1 Network Status



Network Status


If the device fails to access the network, click **Start Setup**, and you will go to the [IP Assignment](#) page.

If the device has accessed the network, click **Start Setup**, and you will go to the [WiFi Settings](#) page.

2.2.2 IP Assignment

The system will check IP assignment automatically. It is recommended to select DHCP. If you select PPPoE, please enter the PPPoE account provided by the ISP.

Figure 2-2-2 IP Assignment



IP Assignment

English

IP Assignment:

DHCP Recommended

PPPoE	DHCP	Static IP
Dynamically Assigned IP Address		


Previous

Next

2.2.3 WiFi Settings

Configure the SSID, WiFi password and management password and Click **Deliver Setup**.

Figure 2-2-3 WiFi Settings

 **WiFi Settings** 801px × 900px English


WiFi Settings [Change IP Assignment](#)

Dual-Band Single SSID ☒

* SSID Used by Dual Bands

@lgh_ew1200g_m


* Wi-Fi Password ☒

..... 

Management Password (Please remember the password.)


☐ Same as Wi-Fi Password

* Management Password


The password is 8-31 characters long. 

Country/Region/Time Zone

* Country/Region

China (CN) 

* Time Zone

(GMT+8:00)Asia/Shanghai 

Previous

Deliver Setup

You can change the IP assignment mode by clicking **Change IP Assignment** in the upper right corner.

2.2.4 Finish

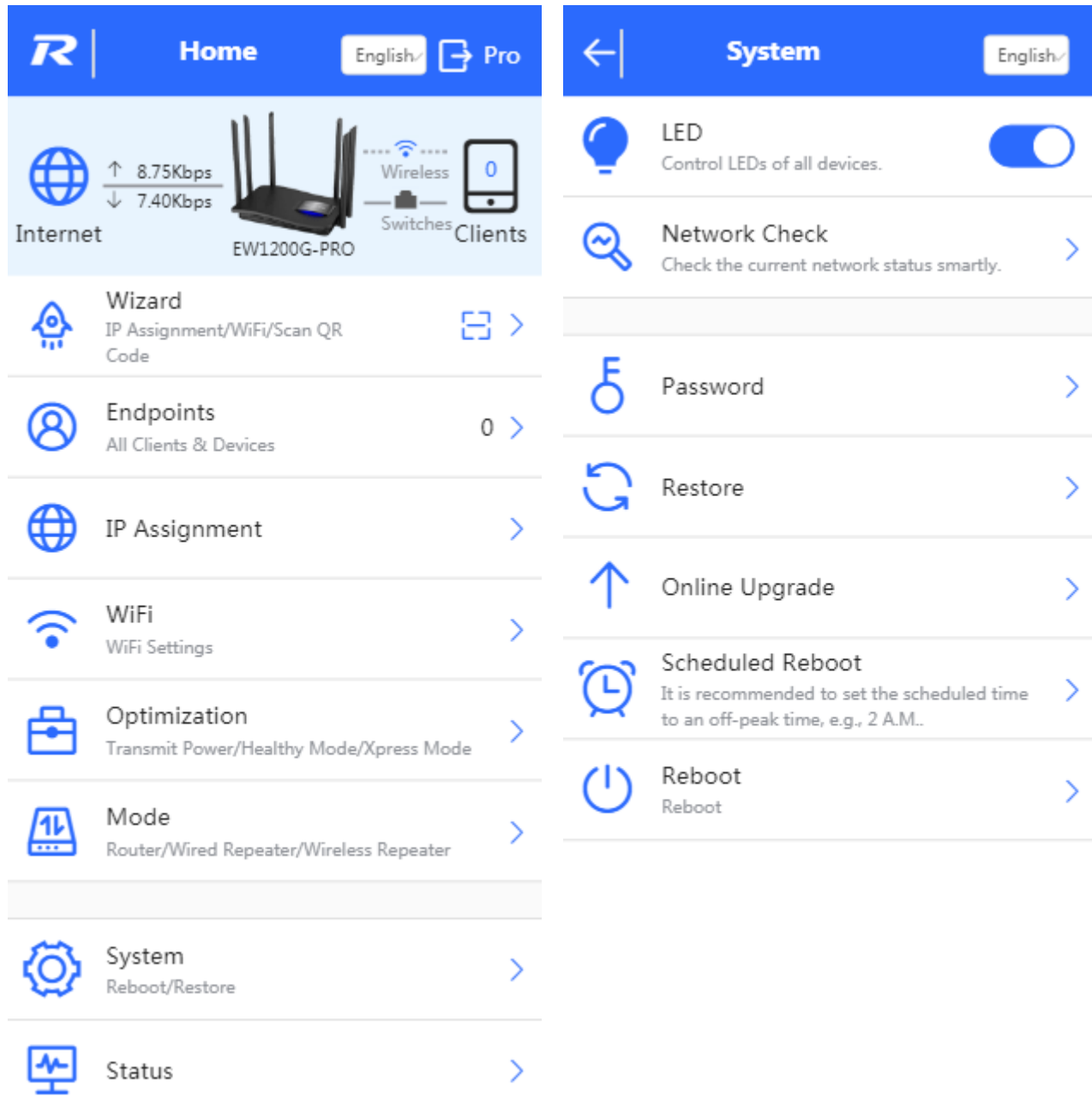
After the configuration is delivered, click **Finish** to enter the homepage.

2.3 GUI

2.3.1 Phone-Based GUI

The system switches between the phone-based GUI and PC-based GUI according to the screen width and browser type. The phone-based GUI is more concise.

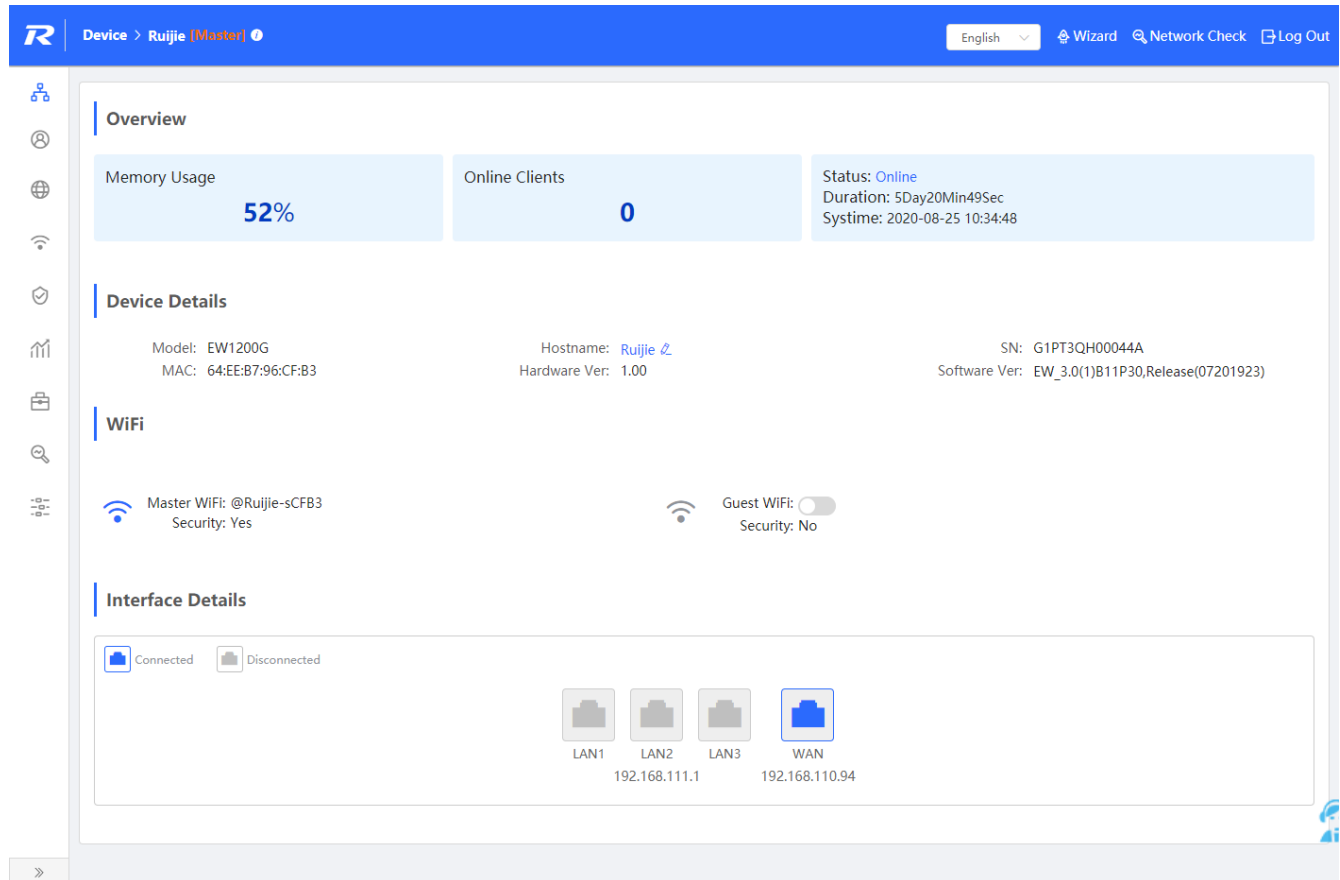
Figure 2-3-1 Phone-Based GUI



2.3.2 PC-Based GUI

Click **Pro** in the upper right corner of phone-based GUI to switch over to the PC-based GUI. The PC-based GUI provides more configuration items. For details, see [eWeb Configuration](#).

Figure 2-3-2 PC-Based GUI



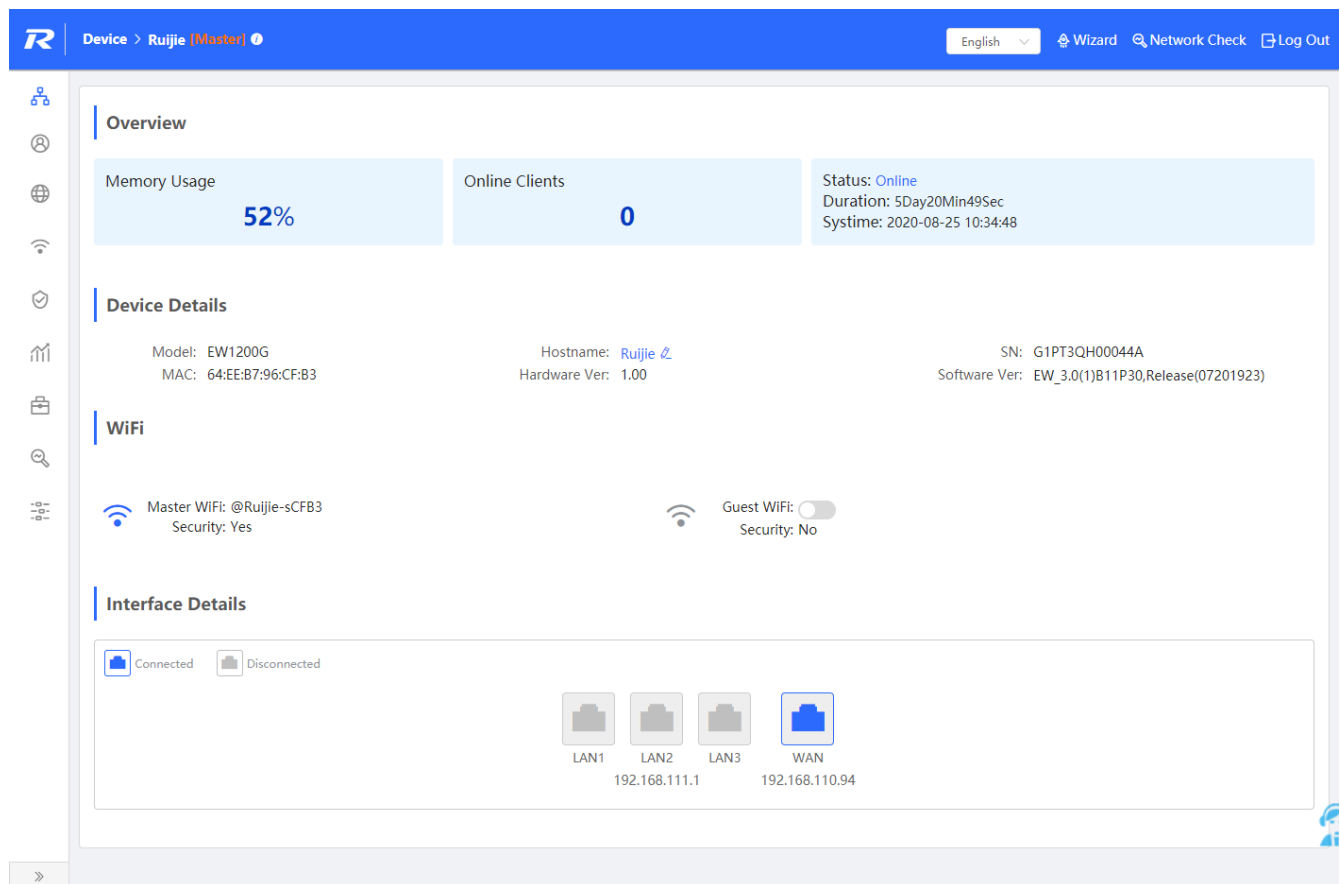
3 eWeb Configuration

This chapter introduces the features on the PC-based GUI.

3.1 Overview

The **Overview** page displays the device details, WiFi and interface details.

Figure 3-1 Overview



3.2 Online Clients

The **Online Clients** module allows you to view online clients.

Figure 3-2-1 Online Clients

Online Clients

There is a delay of 3 minutes. After a client is offline, he will stay in the list for about 3 more minutes.

Online Clients

Refresh

Search

Username	IP Address	MAC	Access Type	Wireless Info	Access Control
X	192.168.111.220	70:3c:69:9f:88:e7	Wireless	Channel:165 RSCP:-56 Duration:07Sec Negotiation Rate:156M	Add Rule

Total 1

10/page

<1>

Go to page

1

Figure 3-2-2 Advanced Search

Refresh

Search

IP Address

MAC

Username

Type

All Types

Search


Cancel

3.3 Basics

3.3.1 WAN

The **WAN** module allows you to configure WAN settings. There are three IP assignment modes available: **Static IP Address**, **DHCP** and **PPPoE**.

Figure 3-3-1 WAN Settings

 **WAN Settings**
Configure WAN settings.

* IP Assignment

DHCP

▼

No username or password is required for DHCP clients.

IP Address

192.168.110.94

Subnet Mask

255.255.255.0

Gateway

192.168.110.1

DNS Server

192.168.110.1

Advanced Settings

Save


3.3.2 LAN


The **LAN** module contains **LAN Settings**, **DHCP Clients**, **Static IP Addresses** and **DNS Proxy**.

3.3.2.1 LAN Settings

The **LAN** module allows you to set the IP address of the LAN port and DHCP status.

Figure 3-3-2 LAN Settings

 **LAN Settings**



LAN Settings

<input type="checkbox"/>	IP Address	Subnet Mask	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
<input type="checkbox"/>	192.168.111.1	255.255.255.0	-	Enabled	192.168.111.1	254	30	Edit

Click **Edit** in the **Action** column to add a VLAN. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-3 Edit

Edit

×

* IP Address

192.168.111.1

* Subnet Mask

255.255.255.0

Remark

Remark

* MAC

00:74:9c:87:6d:ab

DHCP Server

☒

* Start

192.168.111.1

* IP Count

254

* Lease Time(Min)


30

DNS Server

192.168.111.1

Cancel

OK

You can click  in the upper right corner to see description about each configuration item.

3.3.2.2 DHCP Clients

The **DHCP Clients** page displays DHCP clients.

Figure 3-3-4 DHCP Clients

DHCP Clients

View DHCP clients.

Refresh

+ Batch Convert

<input type="checkbox"/>	No.	Hostname	MAC	IP Address	Remaining Lease Time(Min)	Status
No Data						

Total 0

10/page

<1>

Go to page

1

Click **Convert to Static IP** in the **Action** column to convert a DHCP-assigned IP address to a static IP address. Alternatively, select DHCP-assigned IP addresses and click **Batch Convert** to convert more than one IP address.

3.3.2.3 Static IP Addresses

The **Static IP Addresses** module allows you to add, delete and edit static IP addresses.

Figure 3-3-5 Static IP Addresses

Static IP Address List

Static IP Address List

+ Add

Delete Selected

Up to 300 entries can be added.

No.	IP Address	MAC	Action
No Data			

Total 0

10/page

< 1 >

Go to page 1

Click **Add** to add a static IP address manually. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-6 Add Static IP Address

Add

* IP Address

Example: 1.1.1.1

* MAC

Example: 00:11:22:33:44:55

Cancel


OK

3.3.2.4 DNS Proxy


The **DNS Proxy** module allows you to configure DNS proxy settings.

Figure 3-3-7 DNS Proxy

6

 **DNS Proxy**

DNS proxy is not required. The device will obtain the DNS server address from the uplink device by default.



DNS Proxy ☒

* DNS Server

Please enter a DNS server address.

Save

3.3.3 Work Mode

The **Work Mode** module displays the current mode and the other available modes.

Figure 3-3-8 Router Mode

The device is working in **Router** mode. The following three modes are available:

☒ Router

☐ Wired Repeater

☐ Wireless Repeater


Switch the device over to the wired repeater mode.

Figure 3-3-9 Wired Repeater

The device is working in **Router** mode. The following three modes are available:

☐ Router ☒ **Wired Repeater** ☐ Wireless Repeater

Wired Repeater


 This mode allows you to establish a wired connection between a primary router and a secondary router, extending network coverage.
Cable Connection: Please connect the WAN port of the local router to the LAN port of the primary router.

Wired Repeater

Status **Cable Plugged**

IP Address: 192.168.110.94

* Local Router SSID

Password 

Save


Switch the device over to the wireless repeater mode.

Figure 3-3-10 Wireless Repeater

The device is working in **Router** mode. The following three modes are available:

☐ Router ☐ Wired Repeater ☒ **Wireless Repeater**


Wireless Repeater

 This mode allows you to establish a wireless connection between a primary router and a secondary router, extending network coverage.

- The local router will work as a secondary router.
- It is recommended to select a 5G WiFi of the primary router.

Please unplug the cable to avoid loops.

Wireless Repeater

Status **Disabled** 

* Primary Router SSID

Password

Local Router WiFi ☒ **Same as Primary Router WiFi** ☐ New WiFi

Save

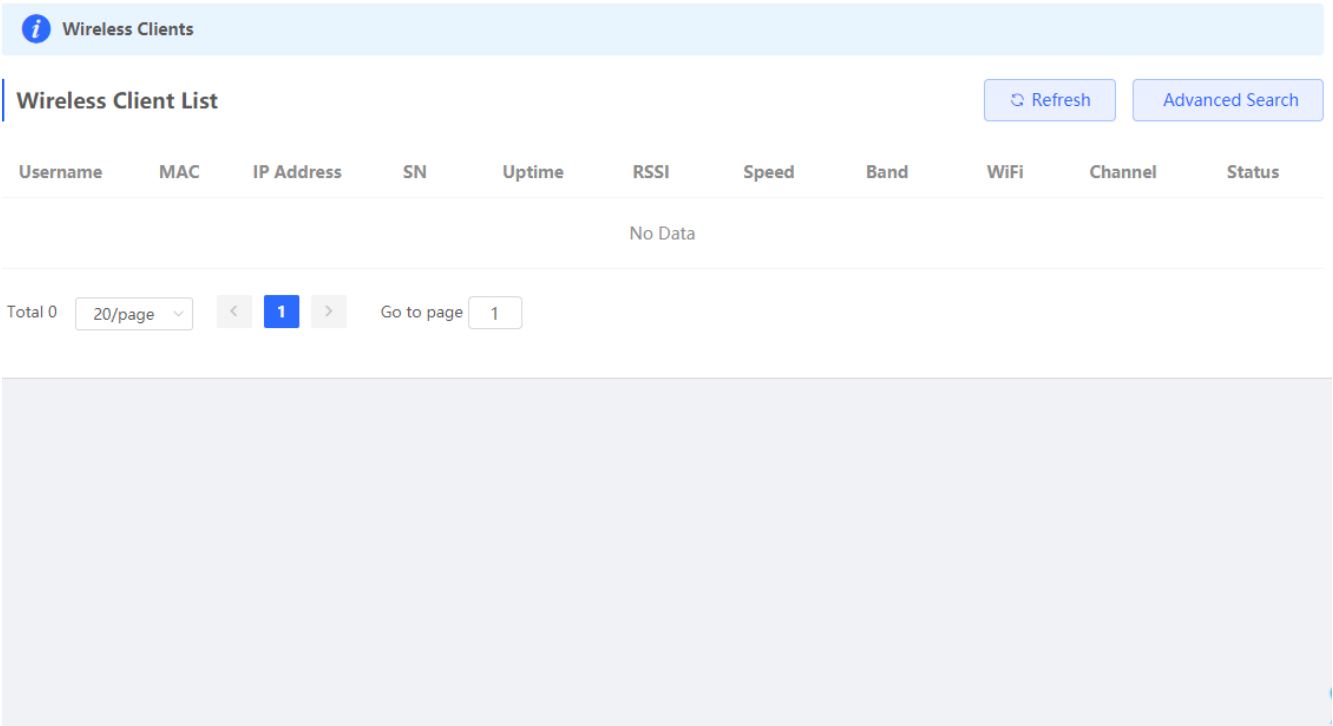
3.4 Wireless

3.4.1 Clients

3.4.1.1 Clients

The **Clients** module displays the wireless clients.

Figure 3-4-1 Wireless Clients



Click **Advanced Search**, and you can search clients by SN and MAC address.

This is a fuzzy search. You can enter an incomplete MAC address or part of an SN.

Figure 3-4-2 Advanced Search

MAC

SN

Search

Cancel

3.4.1.2 Blacklist/Whitelist

Blacklist Mode: All STAs except blacklisted STAs are allowed to access WiFi.

Click **Delete** in the **Action** column to delete a blacklisted STA. Alternatively, select target STAs and click **Delete Selected** to delete more than one blacklisted STAs.

Figure 3-4-3 Blacklist Mode

Blacklist Mode

Whitelist Mode

i

All STAs except blacklisted STAs are allowed to access WiFi.

?

Blacklist

+ Add

Delete Selected

Up to 30 members can be added.

	MAC	Remark	Action
		No Data	

Click **Add** to add a blacklisted STA. In the displayed dialog box, configure settings and click **OK**.

Figure 3-4-4 Add Blacklist STA

Add

×

* MAC

Example: 00:11:22:33:44:55

Remark

Cancel

OK

Whitelist Mode: Only the whitelisted STAs are allowed to access WiFi.

Click **Delete** in the **Action** column to delete a whitelisted STA. Alternatively, select target STAs and click **Delete Selected** to delete more than one whitelisted STAs.

Figure 3-4-5 Blacklist Mode

☐ Blacklist Mode

☒ Whitelist Mode

i

Only the whitelisted STAs are allowed to access WiFi.

?

Whitelist

+ AddDelete Selected

Up to 30 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
		No Data	

Click **Add** to add a whitelisted STA. In the displayed dialog box, configure settings and click **OK**.

Figure 3-4-6 Add Whitelisted STA

Add

×

* MAC

Example: 00:11:22:33:44:55

Remark

Cancel

OK


3.4.2 WiFi

The **WiFi** module allows you to configure WiFi settings for all devices.

3.4.2.1 WiFi Settings

The **WiFi Settings** module allows you to configure the primary WiFi.

Figure 3-4-7 WiFi Settings

 Tip: Changing configuration requires a reboot and clients will be reconnected.


WiFi Settings

Dual-Band Single SSID ☐ (The 2.4G and 5G bands use the same SSID.)

* SSID(2.4G)

* SSID(5G)

Security

* WiFi Password 

[Collapse](#)

Wireless Schedule

Hide SSID ☐ (The SSID is hidden and must be manually entered.)

AP Isolation ☐ (The client joining this WiFi network will be isolated.)

5G Bandsteering ☐ (The 5G-supported client will access 5G radio preferentially.)

XPress ☐ (The client will experience faster speed.)


3.4.2.2 Guest WiFi

The guest WiFi is disabled by default. You can enable guest WiFi on this page or homepage.

AP isolation is enabled by default and cannot be edited.

Set a schedule, and the guest WiFi will be enabled only during this period time. When the time expires, the guest WiFi will be disabled.

Figure 3-4-8 Guest WiFi


 Tip: Changing configuration requires a reboot and will force online clients to go offline.

Guest WiFi Device Group: Default

Enable ☐

Save

Figure 3-4-9 Enable Guest WiFi

 Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest WiFi

Enable ☒

Dual-Band Single SSID ☒ (The 2.4G and 5G bands use the same SSID.)

* SSID @Ruijie-guest-CFB3

Security Open

[Collapse](#)

Wireless Schedule Never Disable

Hide SSID ☐ (The SSID is hidden and must be manually entered.)

AP Isolation ☒ (The client joining this WiFi network will be isolated.)

5G Bandsteering ☐ (The 5G-supported client will access 5G radio preferentially.)



XPress ☐ (The client will experience faster speed.)

Save

3.4.2.3 Healthy Mode

The **Healthy Mode** module allows you to enable health mode and set a schedule.

Figure 3-4-10 Healthy Mode

 Tip: Changing configuration requires a reboot and clients will be reconnected. 

Healthy Mode

Healthy Mode ☒

Wireless Schedule


All Time

Save

3.4.3 Advanced

The **Advanced** module allows you to configure client count limit and channel width.

Figure 3-4-11 Advanced Settings

 Tip: Changing configuration requires a reboot and will force online clients to go offline.

Advanced

Device Group:

Default

Country Code

China (CN)

2.4G Channel Width

Auto

5G Channel Width

Auto

Client Count Limit

32

Client Count Limit

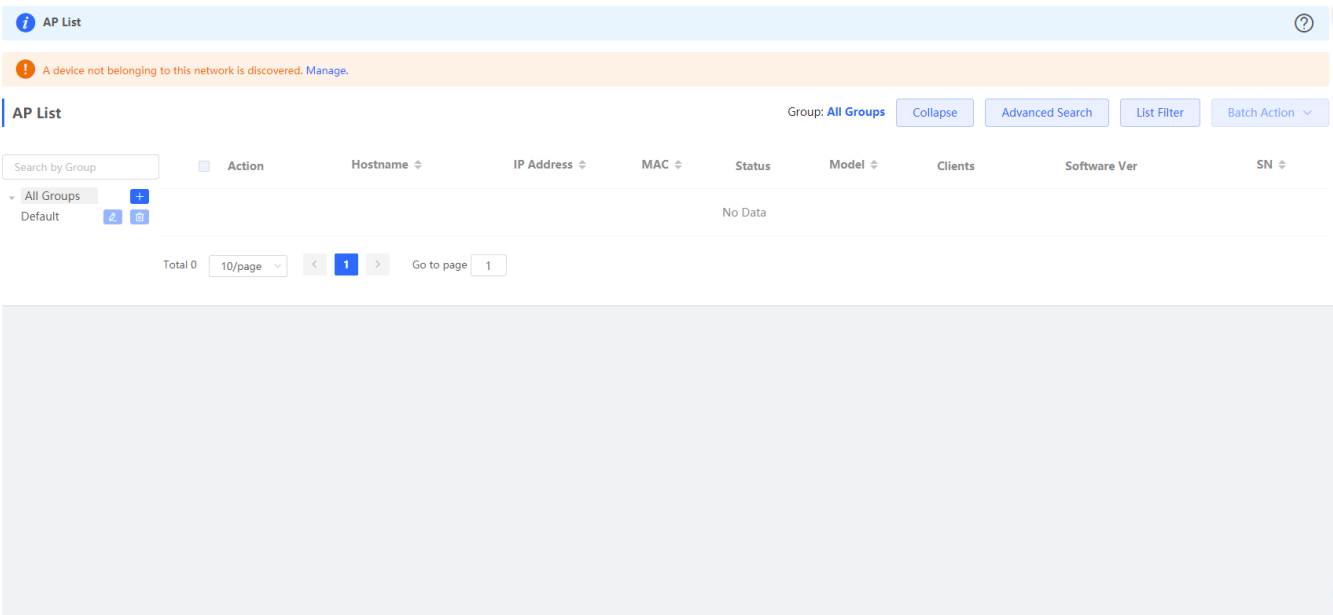
32

Save

3.5 APs

The **APs** module allows you to group, upgrade and delete APs.

Figure 3-5-1 AP List



Click **Advanced Search**, and you can search APs by SN, model, software version, MAC address and status.

Figure 3-5-2 Advanced Search

Advanced Search

SN

Model

Software

Version

MAC

Status

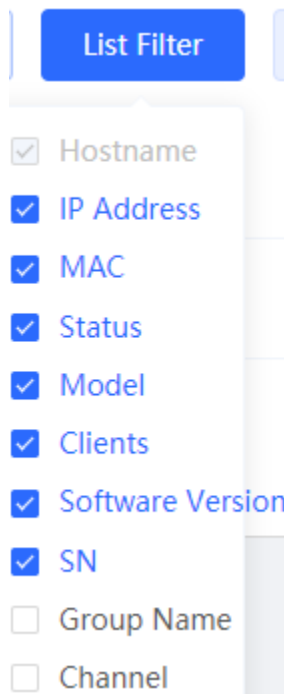
All

Search

Cancel

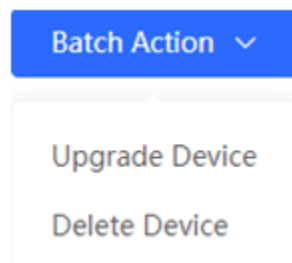
Click **List Filter**, and you can select columns to be displayed in the list.

Figure 3-5-3 List Filter



Select the target devices and click **Batch Action**. The following actions are available:

Figure 3-5-4 Batch Action



Upgrade Device: If there is a new version available, you can upgrade the APs in batches.

Delete Device: You can delete the APs in batches.

3.6 Security

3.6.1 ARP List

The **ARP List** page displays ARP entries.

Figure 3-6-1 ARP List

ARP List

The device learns IP-MAC mapping of all devices connected to its interfaces. You can bind or filter the MAC address.

You can cancel IP-MAC binding in batches on the page.

ARP List

Search by IP/MAC

Refresh

Batch Bind

<input type="checkbox"/>	No.	IP Address	MAC	Status
<input type="checkbox"/>	1	192.168.110.1	00:74:9c:87:6d:85	Bind

Total 1

10/page

<1>

Go to page

1

Click **Bind** in the **Action** column to bind an IP address with a MAC address. Alternatively, select ARP entries and click **Batch Bind** to bind more than one IP address. You can click [MAC Binding](#) to view static ARP entries.

3.6.2 MAC Binding

The **MAC Binding** module allows you to add, delete and edit IP-MAC binding entries.

Figure 3-6-2 IP-MAC Binding

MAC Binding

Enable ARP guard and configure IP-MAC binding to improve network security.

ARP Guard

ARP Guard

Only the devices configured with IP-MAC binding are allowed to access the Internet.

IP-MAC Binding List

+ Add

Delete Selected

Up to 256 IP-MAC bindings can be added.

	No.	MAC	IP Address	Action
No Data				

Total 0

10/page

<1>

Go to page

1

Click **Add** to add an IP-MAC binding. In the displayed dialog box, enter or select an IP address and a MAC address and click **OK**.

Figure 3-6-3 Add IP-MAC Binding

Add

×

* IP Address

Enter or select an IP address.

* MAC

Enter or select a MAC address.

Cancel

OK

Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

3.7 Behavior

3.7.1 Access Control

The **Access Control** module allows you to add, delete and edit access control policies.

Figure 3-7-1 Access Control

ACL

Configure ACL based on IP addresses. **Reverse flow mismatches .**

i

Example: **Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 192.168.2.0/24.** Device configured with IP address 192.168.1.x will fail to access device 192.168.2.x. **But device 192.168.2.x will be allowed to access device 192.168.1.x.**

?

Tip: **Configure one more deny ACL entry containing source IP address 192.168.2.0/24 and destination IP address 192.168.1.0/24.** The two devices will be mutually unreachable.

ACL List

+ Add

🗑️

Delete Selected

Up to 50 entries can be added.

<input type="checkbox"/>	Rule	Control Type	Active Time	Interface	Effective State	Remark	Action
No Data							

Total 0

10/page

<

1

>

Go to page

1

Click **Add** to add a MAC-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-7-2 MAC-Based ACL

Add ACL

×

Based on ☒ MAC ☐ IP Address

* MAC

Enter a MAC address.

Control Type

Allow

▼

Active Time

All Time

▼

Remark

Enter the ACL purpose.

Cancel

OK

Click **Add** to add an IP address-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-7-3 IP Address-Based ACL

Add ACL

×

Based on

☐ MAC

☒ IP Address

Src IP Address: Port

Net:192.168.1.1/24

:

1-65535

Dest IP Address: Port

Net:192.168.1.1/24

:

1-65535

Protocol Type

All Protocols

▼

Control Type

Allow

▼

Active Time

All Time

▼

Interface

WAN

▼

Remark

Enter the ACL purpose.

Cancel

OK

3.7.2 Time Management

The **Time Management** module allows you to add, delete and edit time objects.




Figure 3-7-4 Time List

Time List

+ Add

Delete Selected

Up to 20 entries can be added.

<input type="checkbox"/>	Time Name	Time Span	Action
<input type="checkbox"/>	All Time		Edit Delete
<input type="checkbox"/>	Weekdays		Edit Delete
<input type="checkbox"/>	Weekends		Edit Delete

Click **Add** to add a time object. In the displayed dialog box, configure settings and click **OK**.

Figure 3-7-5 Add Time Object

Add Time

×

* Time Name

Please enter a time name.

* Time

📅

Select Time

Cancel

OK

Click in the time list or in the **Add Time** box, and a time management page will appear.

Figure 3-7-6 Select Time

×

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
23:59							

Cancel

Clear

OK

Select the time and click **OK**.

3.8 Advanced

3.8.1 Flow Control

3.8.1.1 Smart Flow Control

The **Smart Flow Control** module allows you to configure smart flow control.

Figure 3-8-1 Smart Flow Control

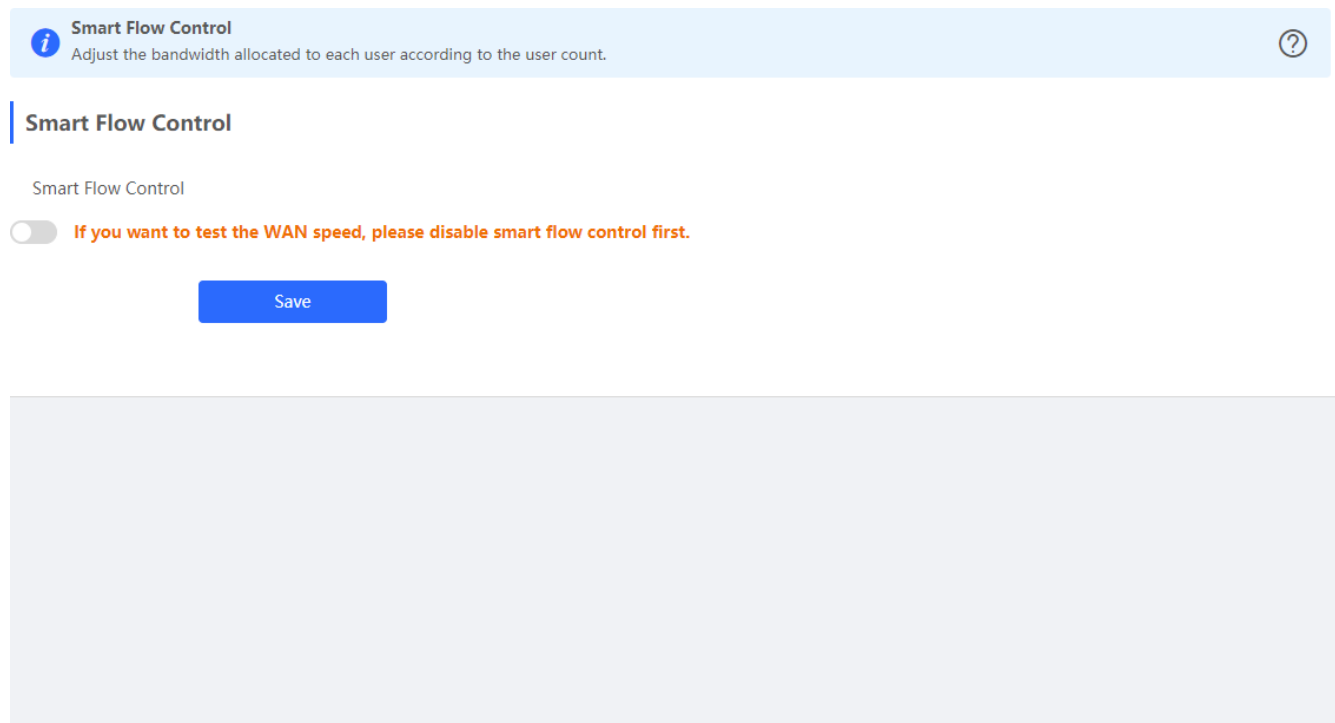


Figure 3-8-2 Enable Smart Flow Control

Smart Flow Control
Adjust the bandwidth

Adjust the bandwidth allocated to each user according to the user count.



Smart Flow Control

Smart Flow Control



If you want to test the WAN speed, please disable smart flow control first.

WAN Bandwidth	* Up	100	Mbps	* Down	100	Mbps
---------------	------	-----	------	--------	-----	------

Save

If there is more than one WAN port, **WAN Bandwidth** settings of each port will be displayed accordingly.

3.8.1.2 Custom Policy

The **Custom Policy** module allows you to add, delete and edit custom flow control policies.

Figure 3-8-3 Custom Flow Control Policy

 Custom Policy

Allocate bandwidth to the specified IP address or range. The custom policy has a higher priority than smart flow control.



Policy List

+ Add

+ Delete Selected

Up to **30** entries can be added.

	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
No Data									

Click **Add** to add a custom flow control policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-8-4 Add Flow Control Policy

Add



* Policy Name

* IP/IP Range

Example: 192.168.1.2-192.168.1.100

Bandwidth Type

Shared



Uplink Rate

* CIR

* PIR

Kbps

Downlink Rate

* CIR

* PIR

Kbps

Status



Cancel

OK

3.8.2 Port Mapping

3.8.2.1 Port Mapping

The **Port Mapping** module allows you to add, delete and edit port mapping policies.

Figure 3-8-5 Port Mapping List

Port Mapping

Port Mapping List

+ Add

Delete Selected

Up to 50 entries can be added.

<div></div>	Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Action
No Data							

Total 0

10/page

<

1

>

Go to page

1

Click **Add** to add a port mapping policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-8-6 Add Port Mapping Policy

Add

✕

* Name

Protocol

UDP



External IP Address

Default: WAN IP address.

* External Port/Range

Example: X or X-X (Range: 1-6553!)

* Internal IP Address

Enter or select an IP address.

* Internal Port/Range

Example: X or X-X (Range: 1-6553!)


Cancel


OK

3.8.2.2 NAT-DMZ

The **NAT-DMZ** module allows you to add, delete and edit NAT-DMZ rules.


Figure 3-8-7 NAT-DMZ Rule List

 **NAT-DMZ**
You can view NAT-DMZ settings and edit or delete the rule.



NAT-DMZ Rule List

+ Add

 Delete Selected


There are 1 outbound interfaces. Up to 1 rules can be added.

<input type="checkbox"/>	Name	Outbound Interface	Dest IP Address	Status	Action
No Data					

Click **Add** to add a NAT-DMZ rule. In the displayed dialog box, configure settings and click **OK**.

Figure 3-8-8 Add NAT-DMZ Rule

Add Rule




* Name

* Dest IP Address


Example: 1.1.1.1

Outbound Interface

WAN



Status



Cancel

OK

3.8.3 UPnP Settings

The **UPnP Settings** module allows you to enable UPnP and view UPnP settings.

Figure 3-8-9 UPnP Settings

UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving communication between devices.

UPnP List

UPnP: ☐

Protocol	App	Client IP Address	Internal Port	External Port
UPnP Disabled				

3.8.4 Local DNS

The **Local DNS** module allows you to configure a local DNS server.

Figure 3-8-10 Local DNS

Local DNS server

The local DNS server is not required to be configured. By default, the device will get the DNS server address from the uplink device.

Local DNS server

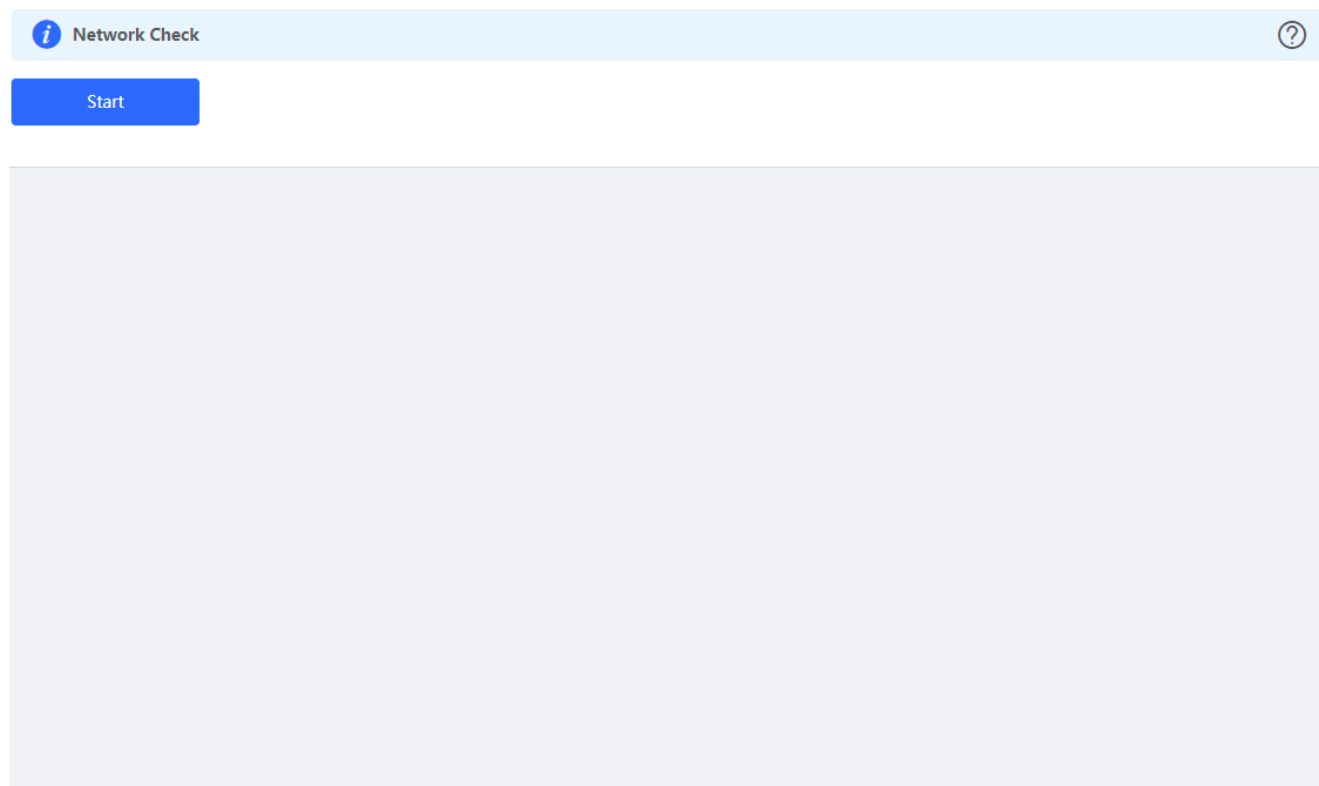
Example: 8.8.8.8, each separated by a comma.

Save

3.9 Diagnostics

3.9.1 Network Check

Figure 3-9-1 Network Check



Click **Start**, and click **OK** in the confirmation box. After the test finishes, the result will be displayed.

Figure 3-9-2 Result



If any problem occurs, the result will be displayed as follows:

Figure 3-9-3 Issue & Advice

Network Check

Recheck

100%

WAN/LAN Cable

Check WAN Cable

Result : OK

Check LAN Cable

Result : The LAN cable is unplugged. Internet access may fail.

Advice : Please verify that the device is plugged into the LAN port properly and check the cable and plug.

Auto-Negotiated Speed	✓
WAN Port	✓
DHCP-Assigned IP Address	✓
LAN & WAN Address Conflict	✓
Loop	✓
DHCP Server Conflict	✓
IP Address Conflict	✓
Route	✓
Next Hop Connectivity	✓
DNS Server	✓
IP Session Count	✓

DHCP Capacity	✓
Flow Control	✓
Ruijie Cloud Server	✓

Please fix the problem by taking the suggested action.

3.9.2 Network Tools

The **Network Tools** module provides the following network tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

Figure 3-9-4 Ping Test and Result

Network Tools

Tool

Ping

Traceroute

DNS Lookup

* IP Address/Domain

www.google.com

* Ping Count

4

* Packet Size

64

Bytes

Start

Stop

Result

Figure 3-9-5 Traceroute Test and Result

Network Tools

Tool

Ping

Traceroute

DNS Lookup

* IP Address/Domain

www.google.com

* Max TTL

20

Start

Stop

Result

Figure 3-9-6 DNS Lookup Test and Result

Network Tools

Tool

☐ Ping

☐ Traceroute

☒ DNS Lookup

* IP Address/Domain

www.google.com

Start

Stop

Result

3.9.3 Packet Capture

The **Packet Capture** module allows you to perform packet capture and download the result for troubleshooting.

Figure 3-9-7 Packet Capture

i Packet Capture ?

Interface

ALL

▼

Protocol

ALL

▼

IP Address

File Size Limit

2

▼

Available Memory **192.82** M

Packet Count Limit

500

▼

Start

Stop

Specify an IP address and click **Start**. After a few seconds, click **Stop**.

Figure 3-9-8 Start Packet Capture

i Packet Capture ?

Interface

ALL

▼

Protocol

ALL

▼

IP Address

File Size Limit

2

▼

Available Memory **192.82** M

Packet Count Limit

500

▼

Download Link

Click to download the PCAP file. *i*

Start

Stop

Click to download the packet capture result in the PCAP format.

3.10 System

3.10.1 System Time

The **System Time** module allows you to set the system time. The system time is synchronized with the NTP server by default.

Select a time zone and set at least one NTP server, and click **Save**.

Figure 3-10-1 Synchronized with NTP Server

The screenshot displays the 'System Time' configuration interface. At the top, a light blue header bar contains an information icon, the title 'System Time', the subtitle 'Configure and view system time', and a help icon. Below the header, the 'Current Time' is shown as '2020-08-24 14:52:34' with an 'Edit' button. The 'Time Zone' is set to '(GMT+8:00)Asia/Shanghai'. Under the 'NTP Server' section, there is an 'Add' button and a list of servers: '0.cn.pool.ntp.org', '1.cn.pool.ntp.org', 'cn.pool.ntp.org', 'pool.ntp.org', 'asia.pool.ntp.org', 'europe.pool.ntp.org', and 'ntp1.aliyun.com'. Each server entry has a 'Delete' button. A large blue 'Save' button is at the bottom.

System Time	
Configure and view system time	
Current Time	2020-08-24 14:52:34 Edit
* Time Zone	(GMT+8:00)Asia/Shanghai
* NTP Server	<div><div>0.cn.pool.ntp.org</div><div>Add</div></div> <div><div>1.cn.pool.ntp.org</div><div>Delete</div></div> <div><div>cn.pool.ntp.org</div><div>Delete</div></div> <div><div>pool.ntp.org</div><div>Delete</div></div> <div><div>asia.pool.ntp.org</div><div>Delete</div></div> <div><div>europe.pool.ntp.org</div><div>Delete</div></div> <div><div>ntp1.aliyun.com</div><div>Delete</div></div>
Save	

Alternatively, Click **Edit**, select a data and a time and click **OK**.

Figure 3-10-2 Manually Set Time

Edit

×

* Time

⌚ Select a time. ×

Current Time

Please select a time.

Cancel

OK

3.10.2 Login

The **Login** module contains **Login Password** and **Session Timeout** settings.

3.10.2.1 Login Password

The **Login Password** module allows you to set the device's login password. You need to log into the system again after changing the password.

Figure 3-10-3 Login Password

i

Login Password

?

Change the login password. Please log in again with the new password later.

* Old Password

* New Password


* Confirm Password


Save

3.10.2.2 Session Timeout

The **Session Timeout** module allows you to set the session timeout period for login to the eWeb management system.

Figure 3-10-3 Session Timeout

 Session Timeout



* Session Timeout

Sec

Save

3.10.3 Management

3.10.3.1 Backup & Import

The **Backup & Import** module allows you to import a configuration file and apply the imported settings. It also allows exporting the configuration file to generate a backup.

Figure 3-10-4 Backup & Import

Backup & Import

i

If the target version is much later than the current version, some configuration may be missing.
It is recommended to choose [Reset](#) before importing the setup. The device will be rebooted automatically later.

?

Backup Setup

Backup Setup

Backup

Import Setup

File Path

Please select a file.

Browse

Import

3.10.3.2 Restore

The **Restore** module allows you to restore the device to factory settings.

Figure 3-10-5 Restore

Restore

i

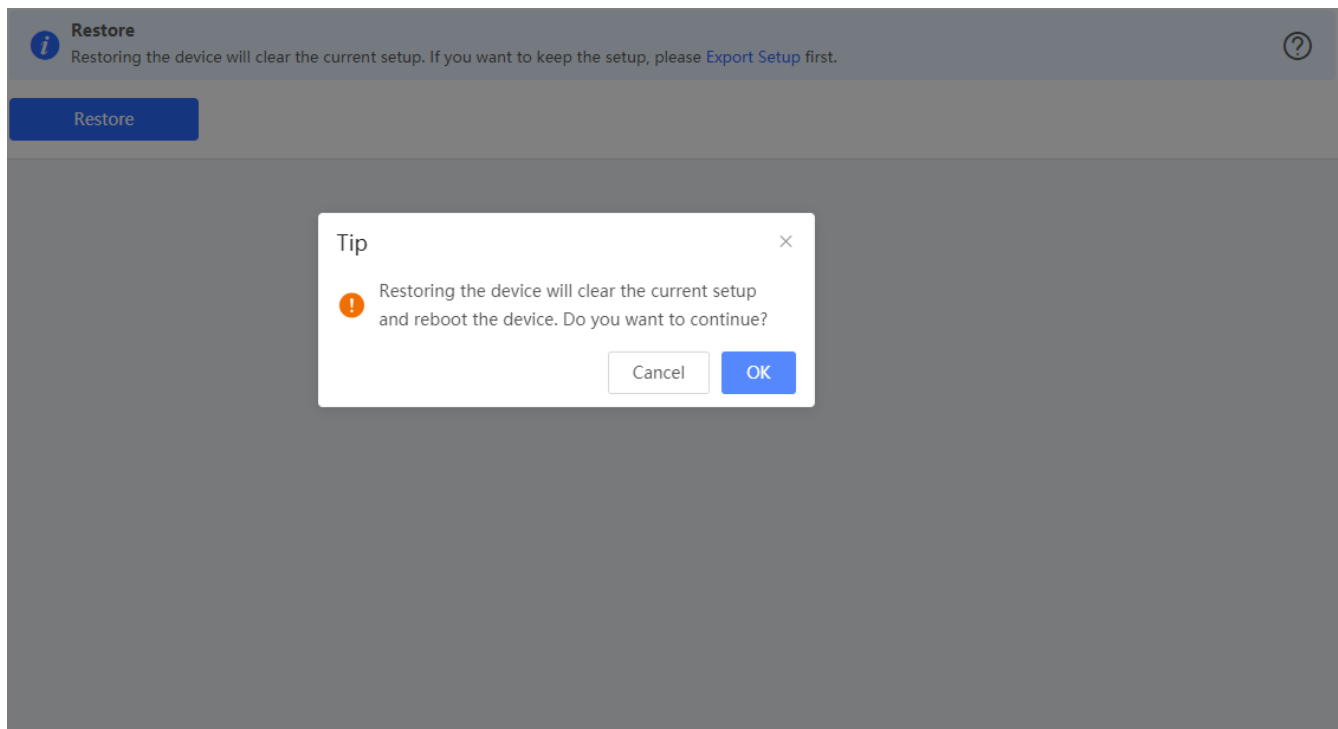
Restoring the device will clear the current setup. If you want to keep the setup, please [Export Setup](#) first.

?

Restore

Please exercise caution if you want to restore the factory settings.

Figure 3-10-6 Confirm Restore

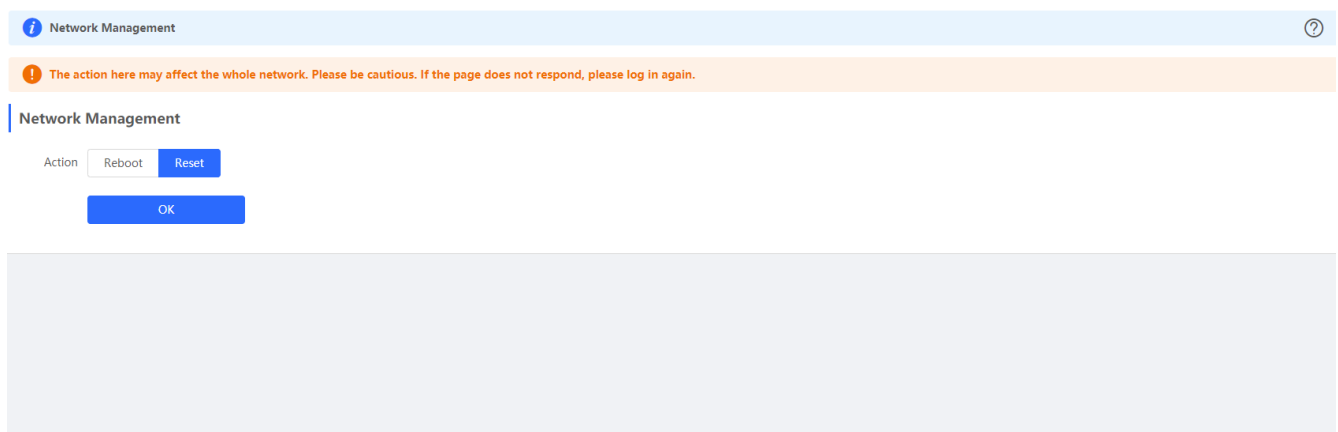


Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed.

3.10.3.3 Reboot & Reset

The **Reboot & Reset** module allows you to reboot or reset all devices in the network.

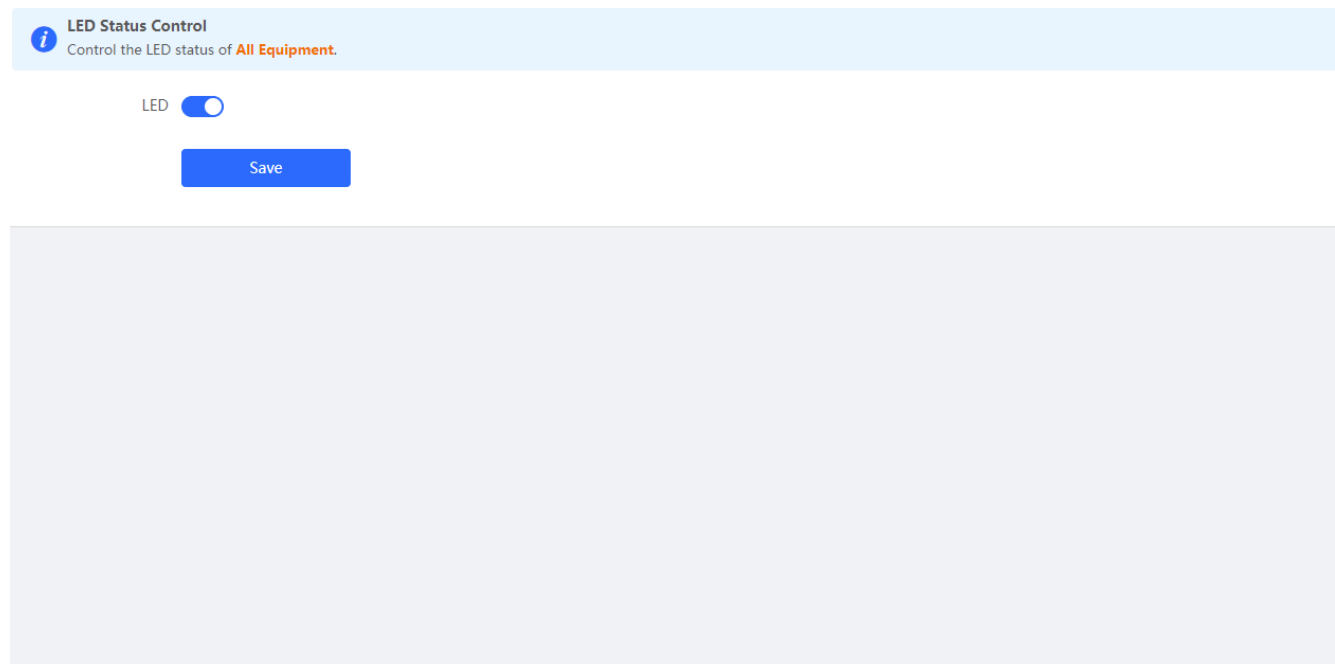
Figure 3-10-7 Reboot & Reset



3.10.3.4 LED

The **LED** module allows you to enable LED.

Figure 3-10-8 LED




3.10.4 Upgrade

Both online upgrade and local upgrade are available

3.10.4.1 Online Upgrade

Click **Upgrade Now**. The device downloads the upgrade package from the network, and upgrades the current version. The upgrade operation retains configuration of the current device. Alternatively, you can select **Download File** to the local device and import the upgrade package on the **Local Upgrade** page.

Figure 3-10-9 Online Upgrade

**Online Upgrade**
Online upgrade will keep the current setup. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrade.

Current Version EW_3.0(1)B11P32,Release(07202120)

New Version EW_3.0(1)B11P25,Release(07172318)

Description Solve the problem that PPPoE cannot learn;
Improve system stability.


- Tip
1. If your device cannot access the Internet, please click [Download File](#).
 2. Choose [Local Upgrade](#) to upload the file for local upgrade.

Upgrade Now

Auto Upgrade ☐ Auto upgrade the device when a new version appears.

If there is no available new version, the device displays a prompt indicating that the current version is the latest.

Figure 3-10-10 Latest Version

**Online Upgrade**
Online upgrade will keep the current setup. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrade.

Current Version EW_3.0(1)B11P30,Release(07201923) (Your version is the latest version.)

Auto Upgrade ☐ Auto upgrade the device when a new version appears.

3.10.4.2 Local Upgrade

Click **Browse** to select an upgrade package, and click **Upload**. After uploading and checking the package, the device displays the upgrade package information and a prompt asking for upgrade confirmation. Click **OK** to start the upgrade.

Figure 3-10-11 Local Upgrade

The screenshot shows the 'Local Upgrade' configuration page. At the top, there is a light blue header bar with an information icon (i) on the left and a help icon (?) on the right. Below the header, the text 'Please do not refresh the page or close the browser.' is displayed. The main content area includes the following elements:

- Model:** EW1200G
- Current Version:** EW_3.0(1)B11P30,Release(07201923) 1.00
- Development:** A toggle switch is currently turned on (blue). To its right, the text '(It is recommended to be disabled after use.)' is displayed in orange.
- Mode:** A label with no associated input.
- Keep Setup:** A checkbox is checked (blue). To its right, the text '(If the target version is much later than the current version, it is recommended not to keep the setup.)' is displayed in blue.
- File Path:** A text input field containing 'Please select a file.', followed by a 'Browse' button and an 'Upload' button.

Below these elements is a large, empty light gray rectangular area.

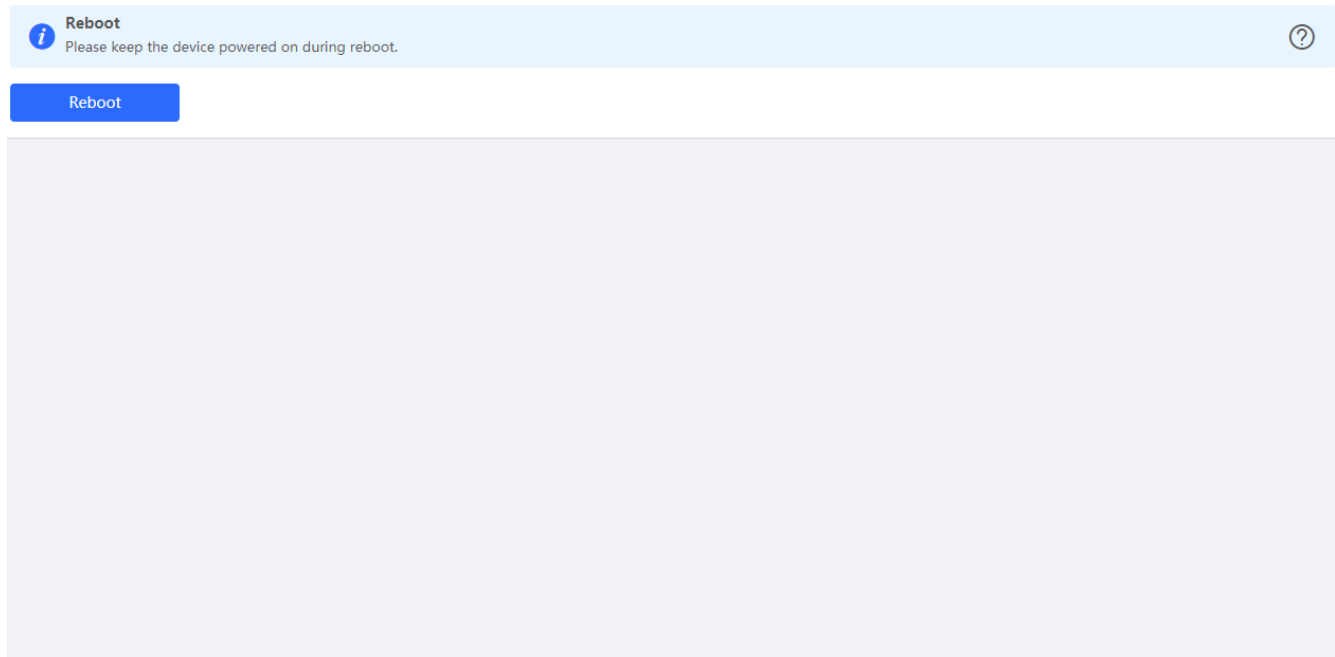
3.10.5 Reboot

Both immediate reboot and scheduled reboot are available.

3.10.5.1 Reboot

The **Reboot** module allows you to reboot the device immediately.

Figure 3-10-12 Reboot



Click **Reboot**, and click **OK** in the confirmation box. The device is rebooted and you need to log into the eWeb management system again after the reboot. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the eWeb service becomes available, you will be redirected to the login page of the eWeb management system.

3.10.5.2 Scheduled Reboot

The **Scheduled Reboot** module allows you to reboot the device at a scheduled time.

Figure 3-10-13 Scheduled Reboot

**Scheduled Reboot**

It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..

Scheduled Reboot ☒

Day ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Time :

Save

Enable scheduled reboot, select the time and click **Save**.

4 FAQs

Q1: I failed to log into the eWeb management system. What can I do?

Perform the following steps:

- (1) Check that the network cable is properly connected to the LAN port of the device and the corresponding LED indicator blinks or is steady on.
- (2) Before accessing the configuration GUI, set the IP assignment mode to **Obtain an IP address automatically** (recommended), so that the server with DHCP enabled can automatically assign an IP address to the PC. To designate a static IP address to the PC, set the IP address of the PC in the same network segment as the IP address of the management interface. For example, if the default IP address of the management interface is 192.168.110.1 and the subnet mask is 255.255.255.0, set the IP address of the PC to 192.168.110.X (X is any integer ranging from 2 to 254), and the subnet mask is 255.255.255.0.
- (3) Run the **ping** command to test the connectivity between the PC and the device.
- (4) If the login failure persists, restore the device to factory settings.

Q2: What can I do if I forget my username and password? How to restore the factory settings?

To restore the factory settings, power on the device, and press and hold the **Reset** button for 5s or more, and release the **Reset** button after the system LED indicator blinks. The device automatically restores the factory settings and restarts. The original configuration will be lost after the factory settings are restored. After the restoration, the default management address is 192.168.110.1 and the default password is admin.

Q3: The subnet mask value needs to be specified to divide the address range for certain functions. What are the common subnet mask values?

A subnet mask is a 32-bit binary address that is used to differentiate between the network address and host address. The subnet and the quantity of hosts in the subnet vary with the subnet mask.

Common subnet mask values include 8 (default subnet mask 255.0.0.0 for class A networks), 16 (default subnet mask 255.255.0.0 for class B networks), 24 (default subnet mask 255.255.255.0 for class C networks), and 32 (default subnet mask 255.255.255.255 for a single IP address).