Ruijie RG-WLAN Series Access Controllers AC_RGOS 11.9(6)W6B1

Web-based Configuration Guide

Document Version: V1.0
Date: May 23, 2025

Copyright

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding the content of this document.

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

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained in this manual does not constitute any explicit or implicit warranties.

Personal Data Statement

During the operation or troubleshooting of the products, services, or features you have purchased, certain personal data of users may be collected or used. Therefore, it is essential for you to establish and implement appropriate privacy policies, in compliance with the relevant laws and regulations of the applicable countries or regions, to ensure the complete protection of users' personal data.

If Ruijie Networks is involved in this process, we will strictly adhere to the relevant laws and regulations of the applicable countries or regions and take all necessary actions to safeguard users' personal data.

When discarding, reclaiming, or reusing a device, please ensure to back up or clear any stored data to avoid data leakage. For assistance, please contact our after-sales technical support.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Networks website: https://www.ruijie.com/
- Online support center: https://www.ruijie.com/support
- Case portal: https://caseportal.ruijie.com
- Community: https://community.ruijienetworks.com
- Email support: service_rj@ruijie.com
- Live chat: https://www.ruijie.com/rita
- Documentation feedback: doc@ruijie.com.cn

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

3. Notes

The manual provides configuration information, including models, port types, and command line interfaces, for reference purposes only. In the event of any discrepancy or inconsistency between the manual and the actual version, the actual version shall take precedence.

Contents

1 Operating Environment

1.1 Overview

You can access the Web management system through a web browser such as Google Chrome or Microsoft Edge to manage APs.

Web management system involves Web server and Web client. The Web server is integrated into the device to receive and process requests from a client. It then returns the processing results to the client. Web clients typically refer to web browsers, such as Internet Explorer and Google Chrome.

1.2 Connecting to the Device

The web management system involves two parts: web server and web client. A web server is integrated into the device to receive and process requests from a client, and return the processing result to the client.

As shown in the following figure, an administrator can access and configure the device on the web management system through the web browser. The web management system integrates configuration commands and sends them to the device through Asynchronous JavaScript and XML (AJAX) requests. The web service is enabled on the device to process basic HTTP requests and return requested data based on the commands.

Figure 1-1 Application Topology

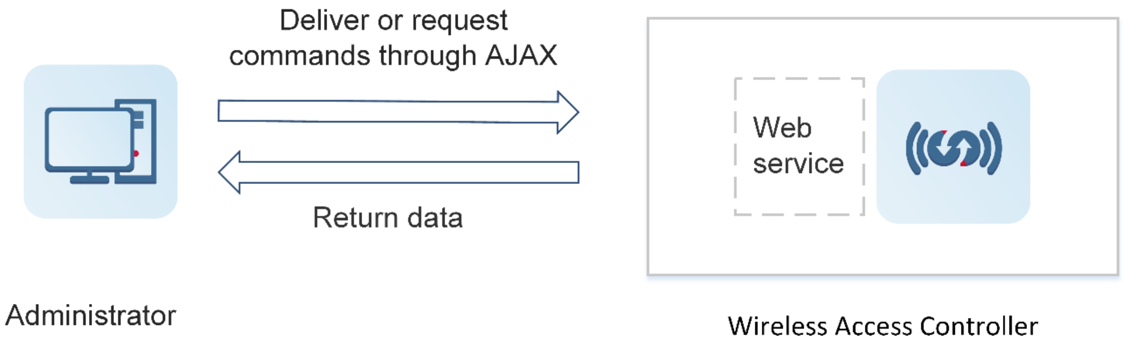
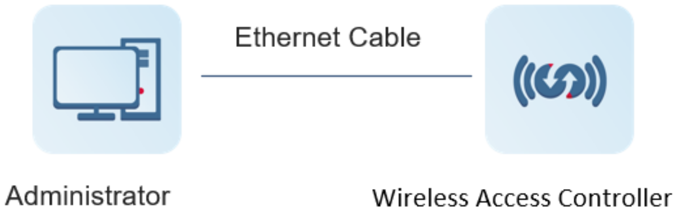

Deliver or request commands through AJAX
Return data
Web service
Administrator
Wireless Access Controller

Figure 1-2 Simplified Topology



1.3 Configuration Environment for PC Clients

- An administrator logs in to the web management system to manage the device through the web browser on a client. Typically, a client refers to a PC. It may also be other mobile terminal such as a laptop or iPad. Mobile phones are not supported.

- Web browser: Google Chrome is recommended, and Microsoft Edge is supported. Exceptions such as garbled characters or format errors may occur when other browsers are used.
- Resolution: You are advised to set the resolution to 1280 pixels x 1024 pixels, 1920 pixels x 1080 pixels, or 1440 pixels x 960 pixels. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

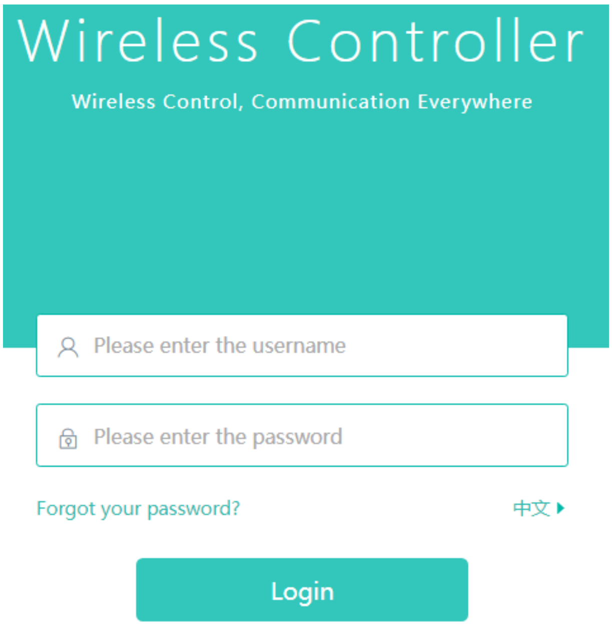
1.4 Web Service Environment for ACs

- The AC is enabled with Web service.
- The AC is configured with the username and password for logging authentication.
- The AC is configured with a management IP address.

Default Web Configuration

Feature	Default Value
Web service	Enabled
Device IP address	192.168.110.1

After the Web service is enabled and the IP address is correctly configured, enter the IP address in the address bar of your browser, such as https://192.168.110.1. Press **Enter** and the following page is displayed:


Wireless Controller
Wireless Control, Communication Everywhere
Please enter the username
Please enter the password
Forgot your password?
中文
Login

Enter the username and password and click **Login**. The following table provides the default username and password.

Default Username/Password	Description
admin/admin	Super administrator with full permissions.

1.5 Enabling the Web Service

The AC is enabled with the Web service and configured with IP address 192.168.110.1 by default. The following describes how to enable the Web service using the command line interface (CLI).

Configuration Item	Command	
Configures the Web server.	**enable service web-server**	Enables the Web service.
	ip address	(Optional) Configures an IP address.
	webmaster level username password	(Optional) Configures the username and password for logging in to the Web management system.

1.5.1 Configuration Steps

↘ **Enabling the Web Service**

- Mandatory.
- Enable the Web service on the AC.

↘ **Configuring the IP Address**

- Optional.

↘ **Configuring the Username and Password for Logging Into the Web Management System**

- Optional.
- When the Web service is enabled, the administrator username and password are **admin** and **admin** respectively, and the guest username and password are **guest** and **guest** respectively by default. Users can change and create accounts.

1.5.2 Verification

Log in to the Web management system using the configured IP address and Web management account to check whether you can log in successfully.

1.5.3 Related Commands

↘ **Enabling the Web Service**

Command	**enable service web-server** [**all** | **http** | **https**]
Parameter Description	**all** | **http** | **https: Indicates enabling different services. all** indicates enabling both HTTP and HTTPS services. **http** indicates enabling the HTTP service. **https** indicates enabling the HTTPS service. Both HTTP and HTTPS services are enabled by default.
Command Mode	Global configuration mode

Configuring the IP Address

Command **ip address** *ip-address ip-mask*

Parameter Description *ip-address*: Indicates the IP address.

mask: Indicates the network mask.

Command Mode Interface configuration mode

Configuring the Username and Password for Logging Into the Web Management System

Command **webmaster level** *privilege-level* **username** *name* password { *password* | [**0 |** 7] *encrypted-password* }

Parameter Description *privilege-level*: Indicates the privilege level of users., including privilege levels 0, 1, and 2. Default administrator account **admin** and **guest** account guest have permissions of privilege levels 0 and 2 respectively. Other manually created accounts have permissions of privilege level 1.

name: Indicates the username.

password: Indicates the password.

0 | **7:** Indicates the password encryption types, **0** for no encryption, and **7** for simple encryption. The default value is **0**.

encrypted-password: Indicates the password text.

Command Mode Global configuration mode

Usage Guide N/A

1.5.4 Configuration Example

Configuration Steps

(1) Enable the Web service.

(2) Configure a management IP address for the device. The default management VLAN is VLAN 1. Configure an IP address for VLAN 1 and ensure that users can ping the management IP address successfully from their PCs.

```
Hostname# configure terminal
Hostname(config)# enable service web-server
Hostname(config)# webmaster level 0 username test password test
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ip address 192.168.1.200
255.255.255.0
Hostname(config)# end
```

Verification

Run the **show running-config** command to check configuration result.

```
Hostname(config)# show running-config
Building configuration...
Current configuration : 6312 bytes

!
hostname Hostname
!
!
webmaster level 0 username test password test   //Indicates
the username and password for Web management authentication.
The password is encrypted.
http update mode auto-detect
!
!
interface VLAN 1
 ip address 192.168.1.200 255.255.255.0
//Indicates the management IP address of the device.
 no shutdown
!
line con 0
line vty 0 4
 login
!
!
End
```

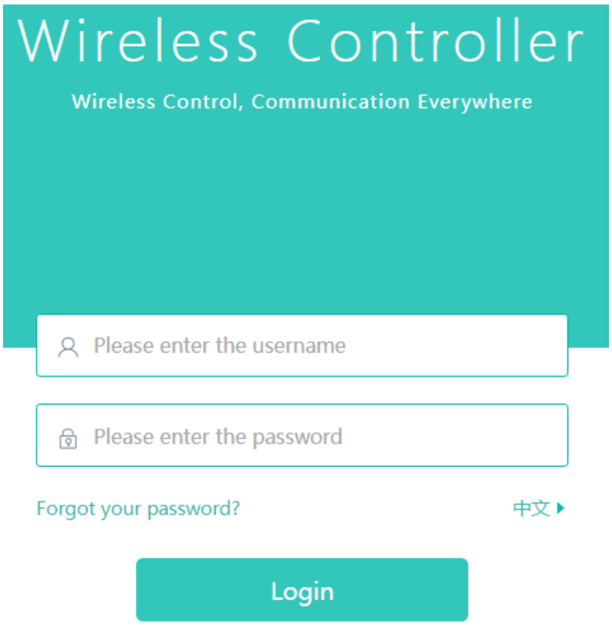
2 Quick Setup

2.1 Logging in to the Web Management System

You will be prompted to change the password upon your first login to the web management system. You are advised to set a complex password. Use the new password upon next login.

Caution

- If there are five consecutive failed login attempts within 10 minutes, your account will be locked for 10 minutes.
- For some ACs, the maximum number of concurrent users of an account can be configured. If the number of concurrent users exceeds the upper limit, login fails.


Wireless Controller
Wireless Control, Communication Everywhere
Please enter the username
Please enter the password
Forgot your password?
中文
Login

2.2 Config Wizard

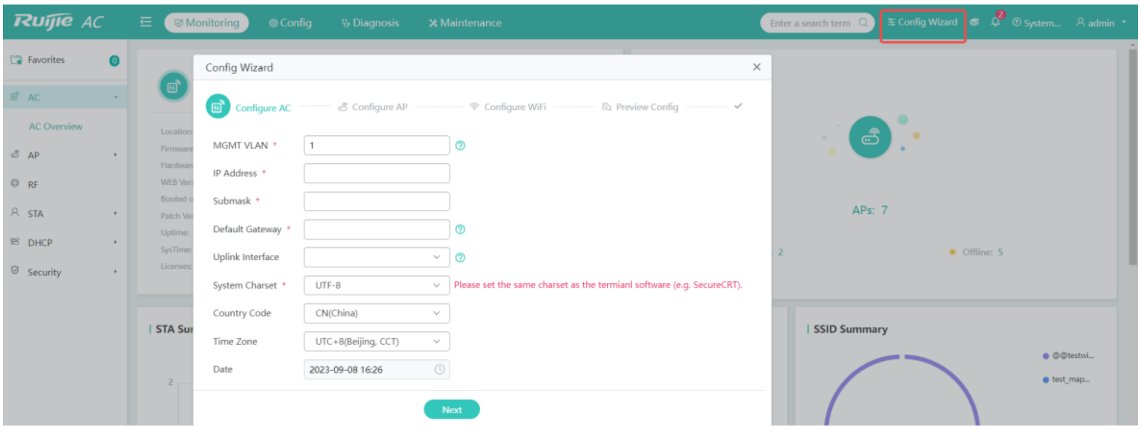
Quick wizard is typically used for first setup. Click **Config Wizard** on the navigation bar. It provides some common scenario-based configurations.

(1) If no config.text file is found, that is, the current device is not configured yet, the **Config Wizard** window will pop up to guide you through configuration.

(2) The **Config Wizard** allows the configuration of only one or two WLANs for setting up a Wi-Fi network.

(3) Once the **Config Wizard** is completed, the existing configurations of the device will be overwritten.

The **Config Wizard** includes four steps: Configure AC, Configure AP, Configure Wi-Fi, and Preview Config.



Config Wizard

MGMT VLAN * 1

IP Address *

Submask *

Default Gateway *

Uplink Interface

System Charset * UTF-8 Please set the same charset as the termianl software (e.g. SecureCRT).

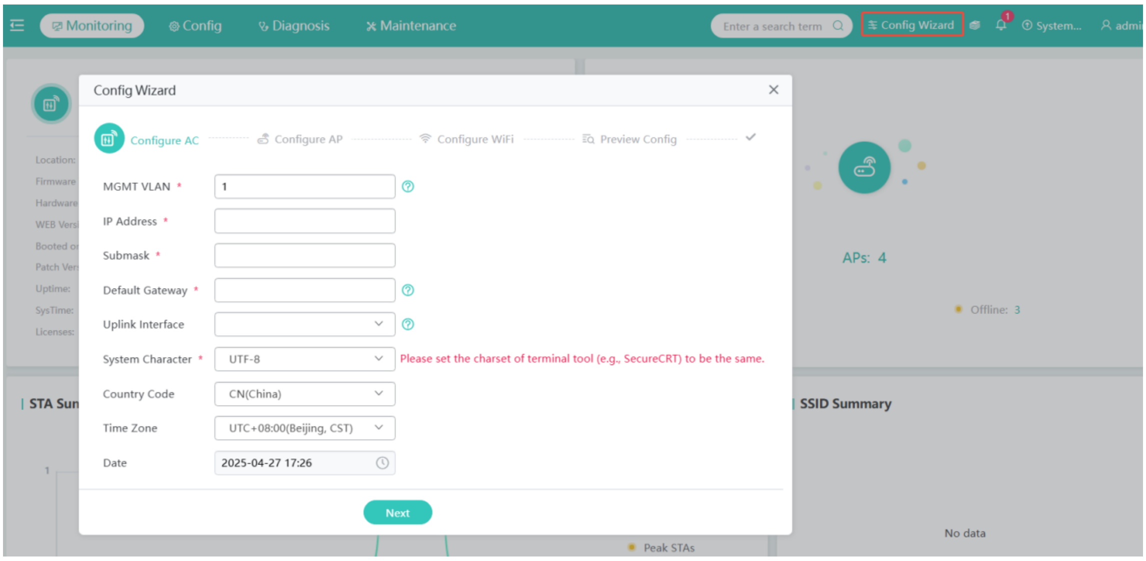
Country Code CN(China)

Time Zone UTC+8(Beijing, CCT)

Date 2023-09-08 16:26

Next

2.2.1 Configuring an AC



Config Wizard

MGMT VLAN * 1

IP Address *

Submask *

Default Gateway *

Uplink Interface

System Character * UTF-8 Please set the charset of terminal tool (e.g., SecureCRT) to be the same.

Country Code CN(China)

Time Zone UTC+08:00(Beijing, CST)

Date 2025-04-27 17:26

Next

Parameter	Description
MGMT VLAN	Enter the VLAN for the AC to communicate with an external network and for users to visit the Web management system.
IP Address	Enter the IP address for the AC to communicate with an external network and for users to visit the Web management system. It is also the default IP address of the tunnel between the AC and AP.
Submask	Enter the IP submask for the AC to communicate with an external network.
Default Gateway	Enter the egress gateway.
Uplink Interface	Enter the interface connecting the AC and its uplink device.
System Charset	Enter the system charset and the default is UTF-8 encoding. If you intend to use other client tools, you are advised to use UTF-8 encoding as well. Otherwise, code mixing may occur, resulting in configuration problems or garbled text on the page.
Country Code	Enter the country or region where the device is located. Regulations for radio frequency (RF) bands, channels, and power vary in different countries or regions.
Time Zone	Enter the time zone where the device is located.

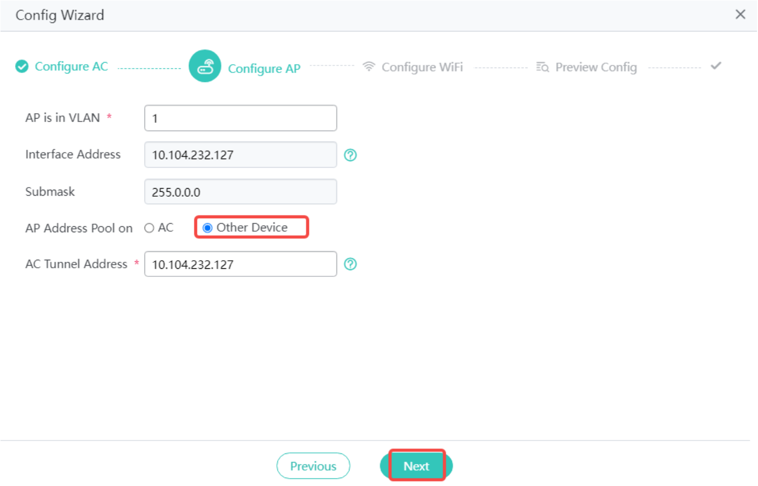
Date	Enter the time of the device.

2.2.2 Configuring an AP

(1) **AP is in VLAN**: Configure the VLAN for the AP. By default, it is the same as the management VLAN.

(2) AP Address Pool on:

If you select **Other Device**, configure the AP address pool on other devices after finishing this process.



AP is in VLAN * 1

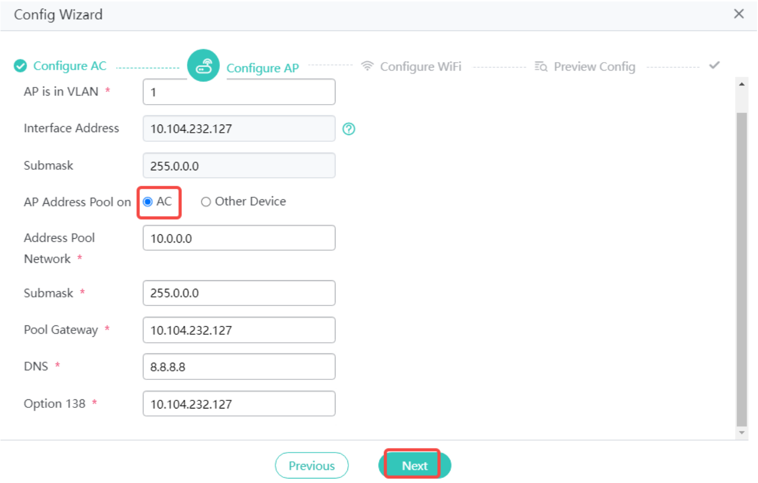
Interface Address 10.104.232.127

Submask 255.0.0.0

AP Address Pool on ○ AC ● Other Device

AC Tunnel Address * 10.104.232.127

If you select **AC**, configure the address pool network, submask, pool gateway, and other parameters. The default DNS server address is 8.8.8.8.



AP is in VLAN * 1

Interface Address 10.104.232.127

Submask 255.0.0.0

AP Address Pool on ● AC ○ Other Device

Address Pool Network * 10.0.0.0

Submask * 255.0.0.0

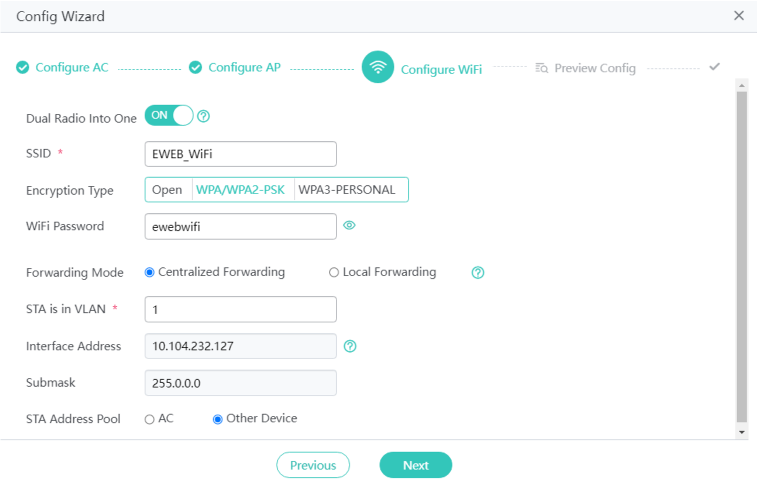
Pool Gateway * 10.104.232.127

DNS * 8.8.8.8

Option 138 * 10.104.232.127

2.2.3 Configuring a Wi-Fi Network

The Wi-Fi networks are associated with default AP groups in **Config Wizard**.



Config Wizard

✓ Configure AC ✓ Configure AP Configure WiFi Preview Config

Dual Radio Into One: ON

SSID *: EWEB_WiFi

Encryption Type: Open | WPA/WPA2-PSK | WPA3-PERSONAL

WiFi Password: ewebwifi

Forwarding Mode: ● Centralized Forwarding ○ Local Forwarding

STA is in VLAN *: 1

Interface Address: 10.104.232.127

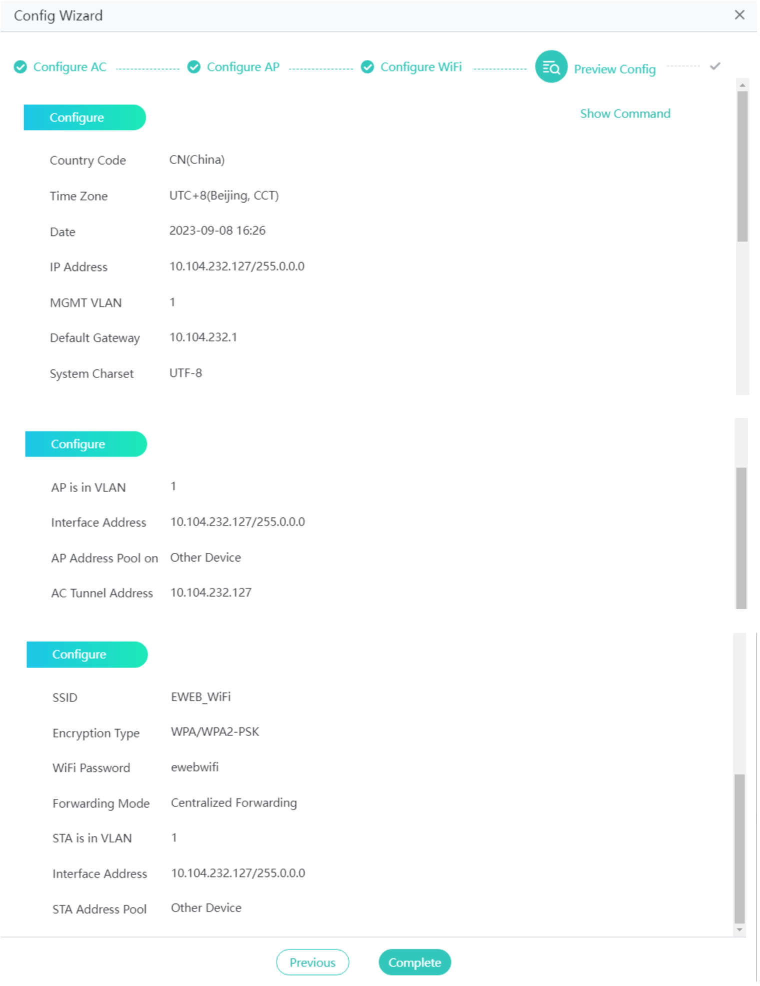
Submask: 255.0.0.0

STA Address Pool: ○ AC ● Other Device

Parameter	Description
Dual Radio Into One	It is enabled by default, indicating that one Wi-Fi network broadcasts both 2.4 GHz and 5 GHz signals. If it is disabled, two Wi-Fi networks are configured, one for 2.4 GHz signals and the other for 5 GHz signals.
SSID	Set the SSID.
Encryption Type	Open: No encryption method is configured. No password is required when the STA connects to the Wi-Fi network. WPA/WPA2-PSK: The WPA mode with a pre-shared key features high security and easy setup, applicable to homes and small-sized enterprises. WPA3-Personal: Compared with WPA2, it is more secure and capable of preventing dictionary attacks.
Forwarding Mode	Centralized Forwarding: All data is routed through the AC before being forwarded to other devices. This mode is configured by default. Local Forwarding: The data is forwarded to other devices directly from the switch, reducing the load on the AC.
STA is in VLAN	Configure the VLAN for the STA.
STA Address Pool	STA address pool can be configured either on the AC or on other devices. If you choose to configure it on other devices, configure and verify the address pool settings on those devices after completing this process.

2.2.4 Verifying Configurations

This process allows users to verify the configurations. Check the CLI commands for the current configurations by clicking **Show Command**.

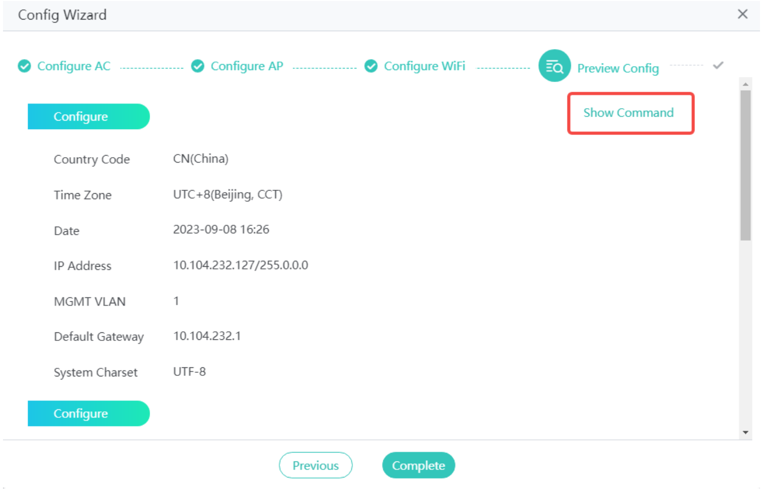


Country Code	CN(China)
Time Zone	UTC+8(Beijing, CCT)
Date	2023-09-08 16:26
IP Address	10.104.232.127/255.0.0.0
MGMT VLAN	1
Default Gateway	10.104.232.1
System Charset	UTF-8

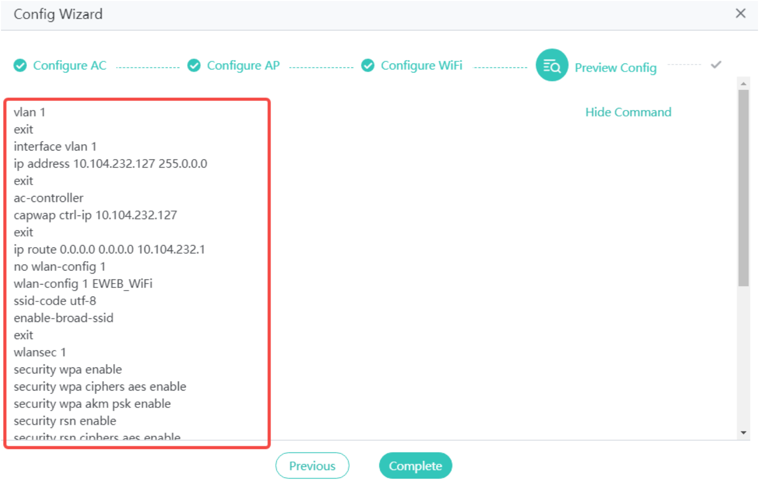
AP is in VLAN	1
Interface Address	10.104.232.127/255.0.0.0
AP Address Pool on	Other Device
AC Tunnel Address	10.104.232.127

SSID	EWEB_WiFi
Encryption Type	WPA/WPA2-PSK
WiFi Password	ewebwifi
Forwarding Mode	Centralized Forwarding
STA is in VLAN	1
Interface Address	10.104.232.127/255.0.0.0
STA Address Pool	Other Device

Click **Show Command** to display the CLI commands for the current configurations.

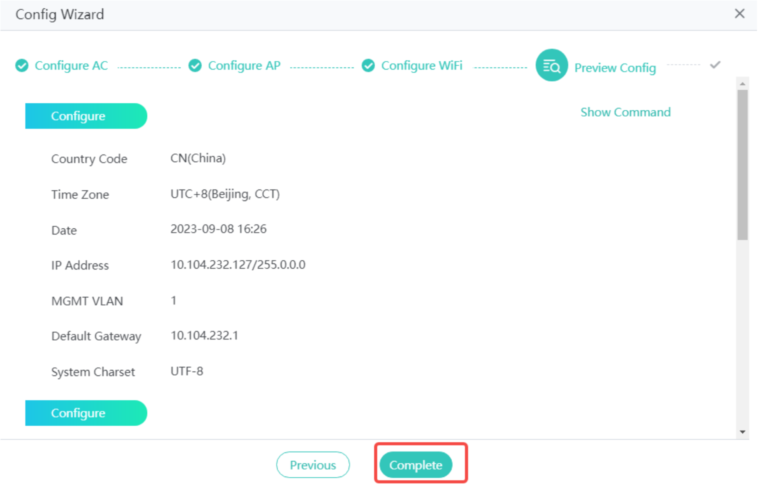


Country Code	CN(China)
Time Zone	UTC+8(Beijing, CCT)
Date	2023-09-08 16:26
IP Address	10.104.232.127/255.0.0.0
MGMT VLAN	1
Default Gateway	10.104.232.1
System Charset	UTF-8



```
vlan 1
exit
interface vlan 1
ip address 10.104.232.127 255.0.0.0
exit
ac-controller
capwap ctrl-ip 10.104.232.127
exit
ip route 0.0.0.0 0.0.0.0 10.104.232.1
no wlan-config 1
wlan-config 1 EWEB_WiFi
ssid-code utf-8
enable-broad-ssid
exit
wlansec 1
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
```

Once you confirm the configuration, click **Complete** and a window pops up, displaying the network deployment. You can test the network connectivity with the external network through network detection.

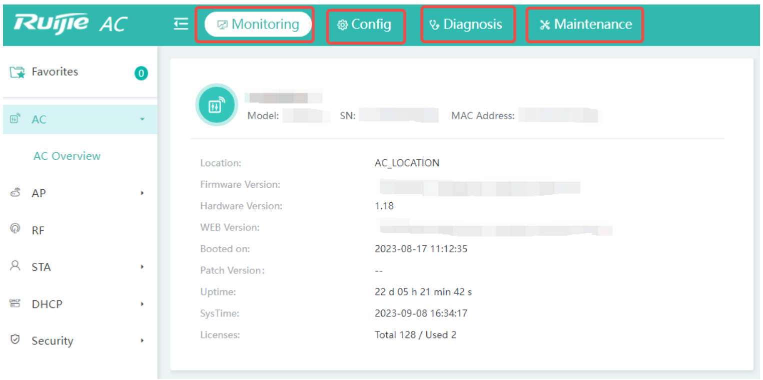


Country Code	CN(China)
Time Zone	UTC+8(Beijing, CCT)
Date	2023-09-08 16:26
IP Address	10.104.232.127/255.0.0.0
MGMT VLAN	1
Default Gateway	10.104.232.1
System Charset	UTF-8

3 Web Management System

3.1 Home Page

The Web GUI includes four main modules: **Monitoring**, **Config**, **Diagnosis**, and **Maintenance**. Click these modules in the navigation bar to view configurations within each module.



[redacted]
Model: [redacted] SN: [redacted] MAC Address: [redacted]

Location: AC_LOCATION
Firmware Version: [redacted]
Hardware Version: 1.18
WEB Version: [redacted]
Booted on: 2023-08-17 11:12:35
Patch Version: --
Uptime: 22 d 05 h 21 min 42 s
SysTime: 2023-09-08 16:34:17
Licenses: Total 128 / Used 2

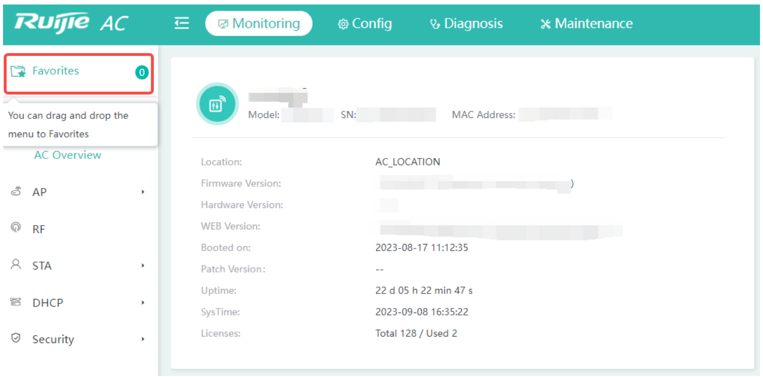
3.2 Favorites

The feature allows you to bookmark frequently used functions. Click **Favorites** to expand the list of bookmarked items and quickly enter the configuration page.

Note

Up to 10 configuration items can be added to **Favorites**.

(1) Adding to Favorites: Drag and drop the menu items to Favorites.

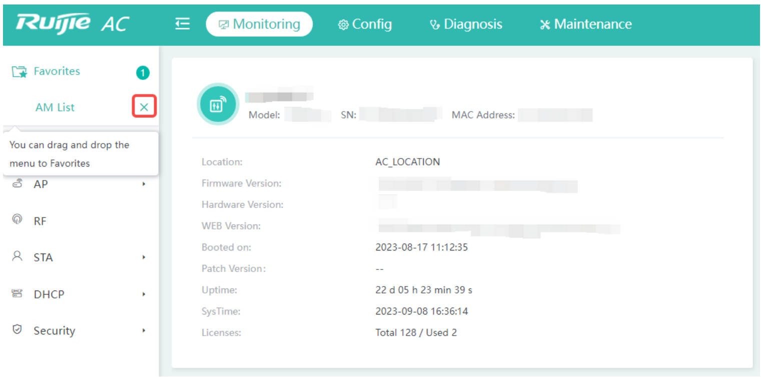


You can drag and drop the menu to Favorites

[redacted]
Model: [redacted] SN: [redacted] MAC Address: [redacted]

Location: AC_LOCATION
Firmware Version: [redacted])
Hardware Version: [redacted]
WEB Version: [redacted]
Booted on: 2023-08-17 11:12:35
Patch Version: --
Uptime: 22 d 05 h 22 min 47 s
SysTime: 2023-09-08 16:35:22
Licenses: Total 128 / Used 2

(2) Removing from Favorites: Select the menu items and click the × icon. Click OK to remove the item from Favorites.

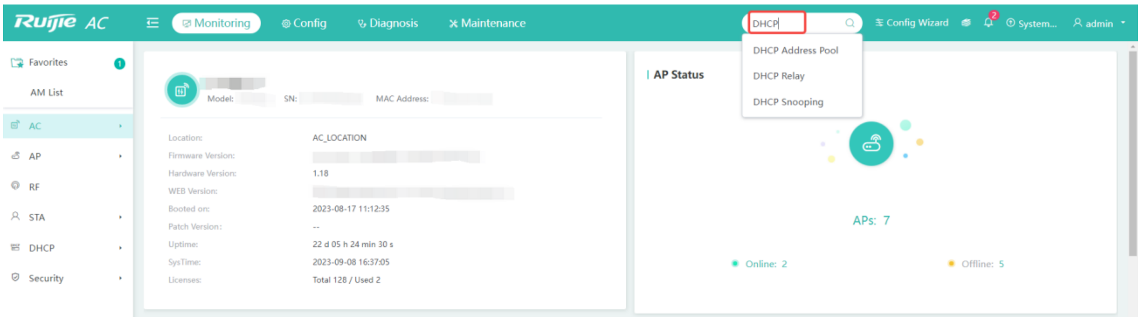


[redacted]
Model: [redacted] SN: [redacted] MAC Address: [redacted]

Location: AC_LOCATION
Firmware Version: [redacted]
Hardware Version: [redacted]
WEB Version: [redacted]
Booted on: 2023-08-17 11:12:35
Patch Version: --
Uptime: 22 d 05 h 23 min 39 s
SysTime: 2023-09-08 16:36:14
Licenses: Total 128 / Used 2

3.3 Menu Search Bar

Given the extensive features in the system, you may find it hard to locate a specific configuration item. Enter keywords in the search bar in the navigation bar to search the configuration items and enter the configuration page quickly.

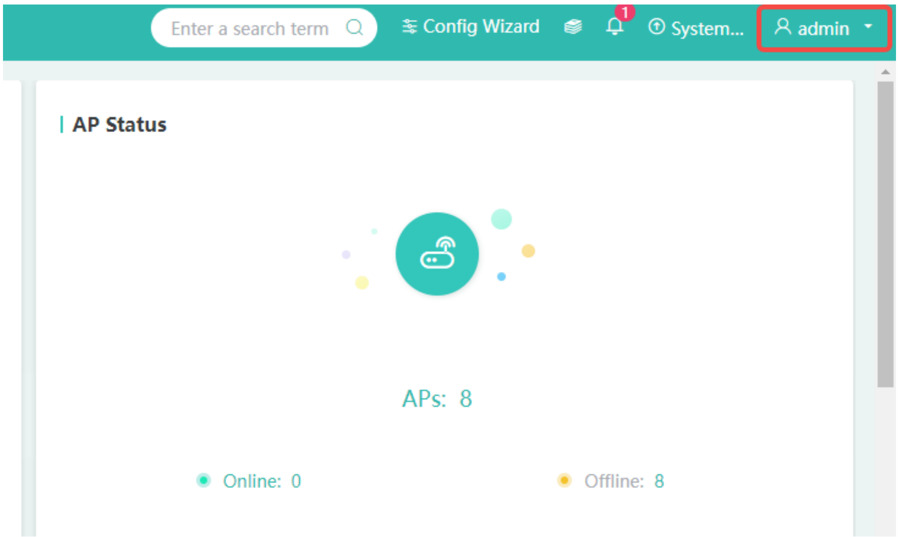


[redacted]
Model: [redacted] SN: [redacted] MAC Address: [redacted]

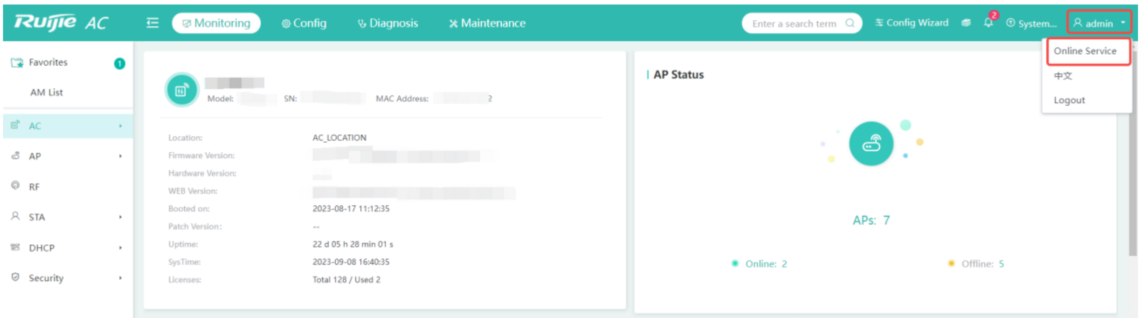
Location: AC_LOCATION
Firmware Version: [redacted]
Hardware Version: 1.18
WEB Version: [redacted]
Booted on: 2023-08-17 11:12:35
Patch Version: --
Uptime: 22 d 05 h 24 min 30 s
SysTime: 2023-09-08 16:37:05
Licenses: Total 128 / Used 2

3.4 Other Functions

(1) Displaying the Current Account



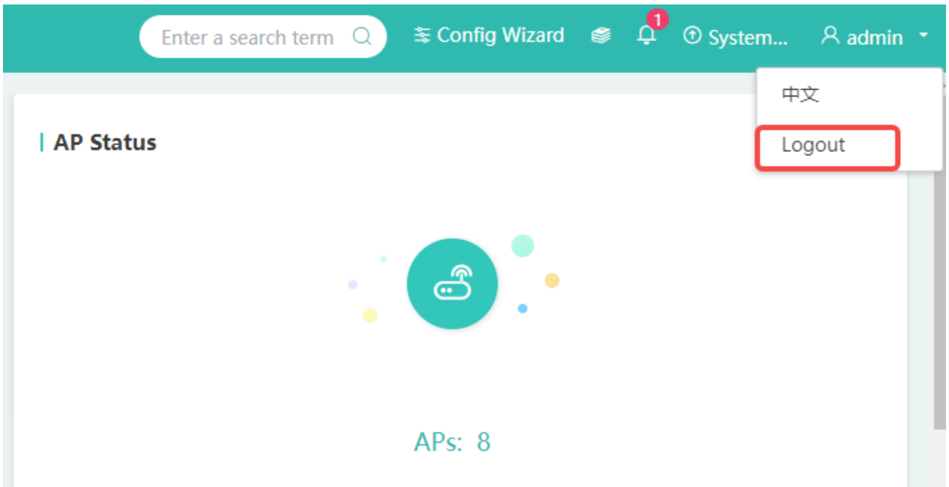
(2) Online service: If you need assistance during the configuration process, click **Online Service** after expanding the account menu in the navigation bar.



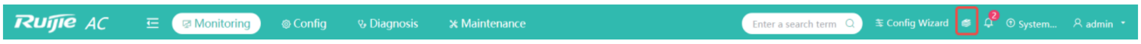
Model: [redacted] SN: [redacted] MAC Address: [redacted]

Location: AC_LOCATION
Firmware Version: [redacted]
Hardware Version: [redacted]
WEB Version: [redacted]
Booted on: 2023-08-17 11:12:35
Patch Version: --
Uptime: 22 d 05 h 28 min 01 s
SysTime: 2023-09-08 16:40:35
Licenses: Total 128 / Used 2

(3) Logout: Click **Logout** after expanding the account menu to log out of the Web management system.



(4) Searching files: If you are unfamiliar with the features of this system and in need of help files, click the icon in the navigation bar to redirect to the documentation center of Ruijie's official website and search for documents.



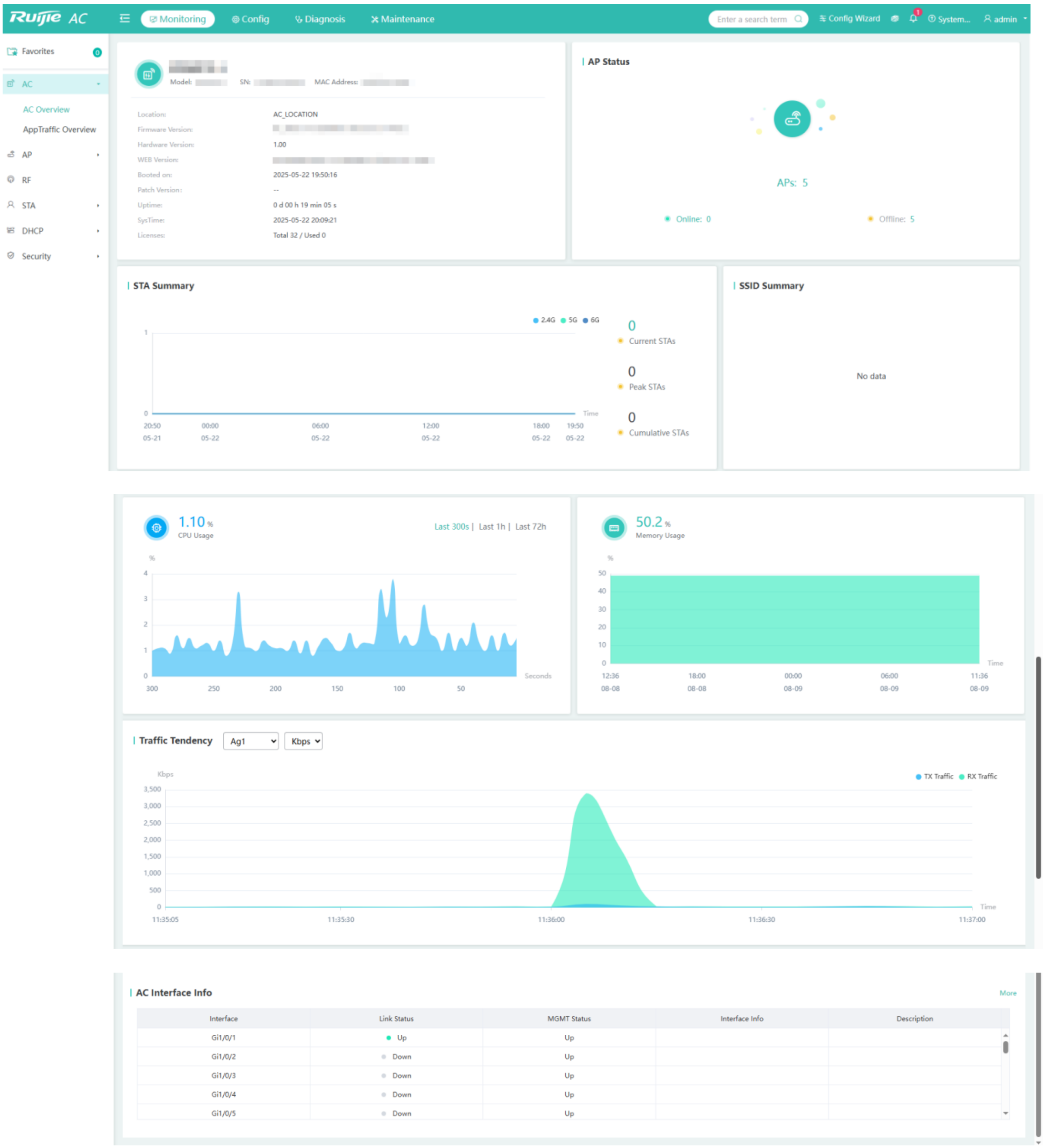
4 Monitoring

4.1 AC

4.1.1 Overview

Choose **Monitoring** > **AC** > **AC Overview**.

The **AC Overview** page displays the basic information about the AC such as MAC address, model, and version details. It also allows you to check the AP status, STA summary, SSID summary, CPU usage, memory usage, traffic tendency, and AC interface information.



[redacted]

Model: [redacted] SN: [redacted] MAC Address: [redacted]

Location: AC_LOCATION
Firmware Version: [redacted]
Hardware Version: 1.00
WEB Version: [redacted]
Booted on: 2025-05-22 19:50:16
Patch Version: --
Uptime: 0 d 00 h 19 min 05 s
SysTime: 2025-05-22 20:09:21
Licenses: Total 32 / Used 0

AP Status

APs: 5

Online: 0

Offline: 5

STA Summary

0 Current STAs

0 Peak STAs

0 Cumulative STAs

SSID Summary

No data

1.10 % CPU Usage

50.2 % Memory Usage

Traffic Tendency

AC Interface Info

Interface	Link Status	MGMT Status	Interface Info	Description
Gi1/0/1	● Up	Up		
Gi1/0/2	● Down	Up		
Gi1/0/3	● Down	Up		
Gi1/0/4	● Down	Up		
Gi1/0/5	● Down	Up		

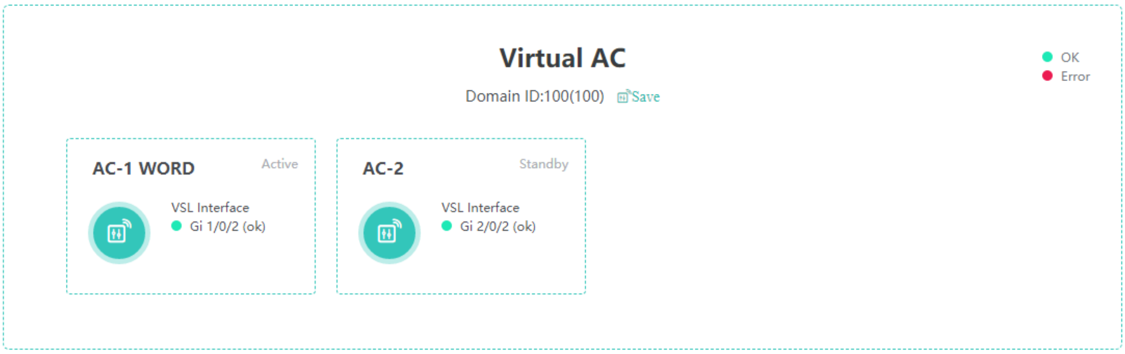
4.1.2 Virtual AC

Choose **Monitoring** > **AC** > **Virtual AC**.

Note

The virtual AC menu is displayed based on the configuration of the device. This menu is only available when the device is configured with the **device convert mode virtual** command.

The virtual AC page displays the current virtual AC members and their basic information.



Virtual AC

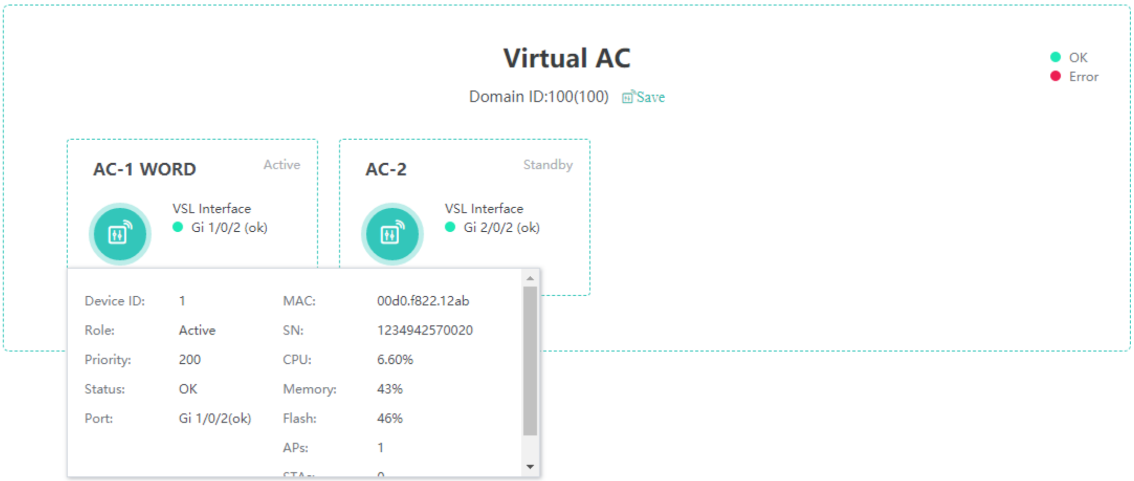
Domain ID:100(100) Save

● OK
● Error

AC-1 WORD Active
VSL Interface
● Gi 1/0/2 (ok)

AC-2 Standby
VSL Interface
● Gi 2/0/2 (ok)

Click a specific virtual AC to view the detailed information about its AC members.



Virtual AC

Domain ID:100(100) Save

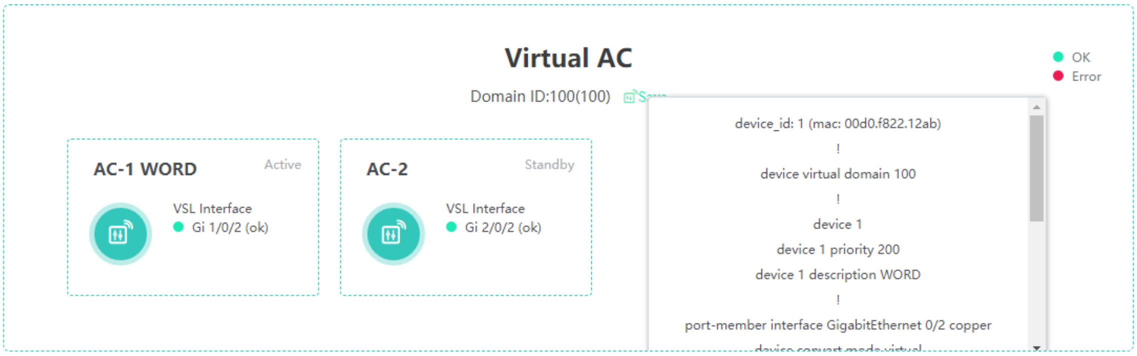
● OK
● Error

AC-1 WORD Active
VSL Interface
● Gi 1/0/2 (ok)

AC-2 Standby
VSL Interface
● Gi 2/0/2 (ok)

Device ID:	1	MAC:	00d0.f822.12ab
Role:	Active	SN:	1234942570020
Priority:	200	CPU:	6.60%
Status:	OK	Memory:	43%
Port:	Gi 1/0/2(ok)	Flash:	46%
		APs:	1
		STAs:	0

Click **Save** to view the configurations of the virtual AC.

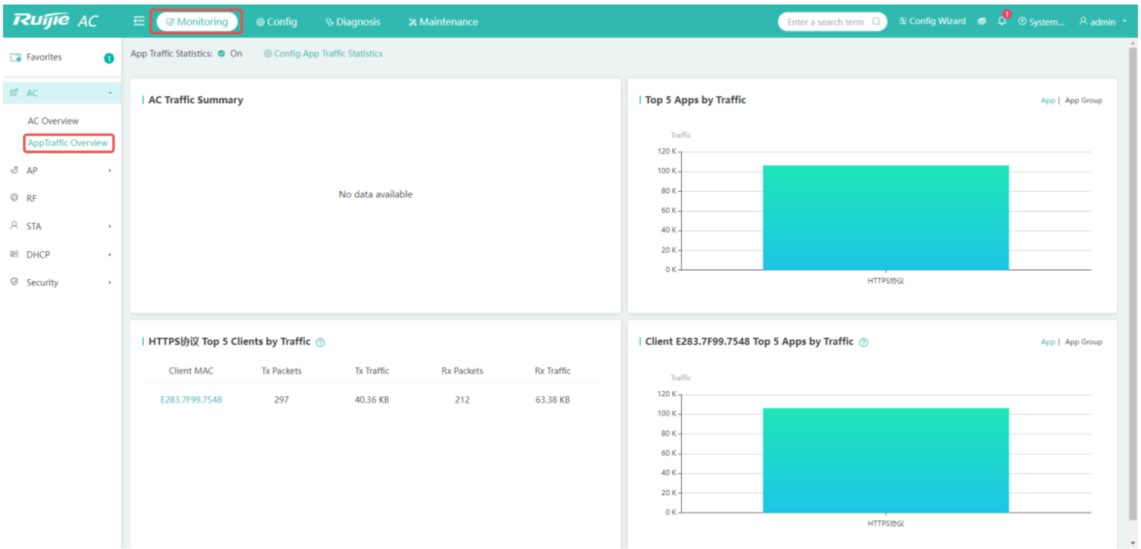


```
device_id: 1 (mac: 00d0.f822.12ab)
!
device virtual domain 100
!
device 1
device 1 priority 200
device 1 description WORD
!
port-member interface GigabitEthernet 0/2 copper
```

4.1.3 App Traffic Statistics

Choose **Monitoring** > **AC** > **AppTraffic Overview**.

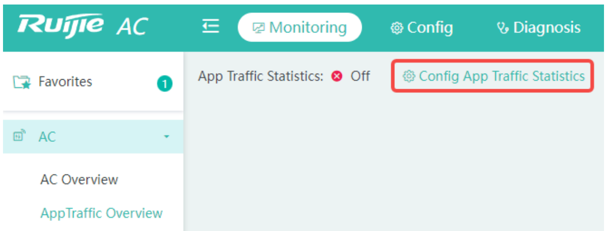
If application identification is enabled, you can view the traffic of applications used by clients connected to the ACs on the **App Traffic Statistics** page.



Client MAC	Tx Packets	Tx Traffic	Rx Packets	Rx Traffic
E283.7F99.7548	297	40.36 KB	212	63.38 KB

Note

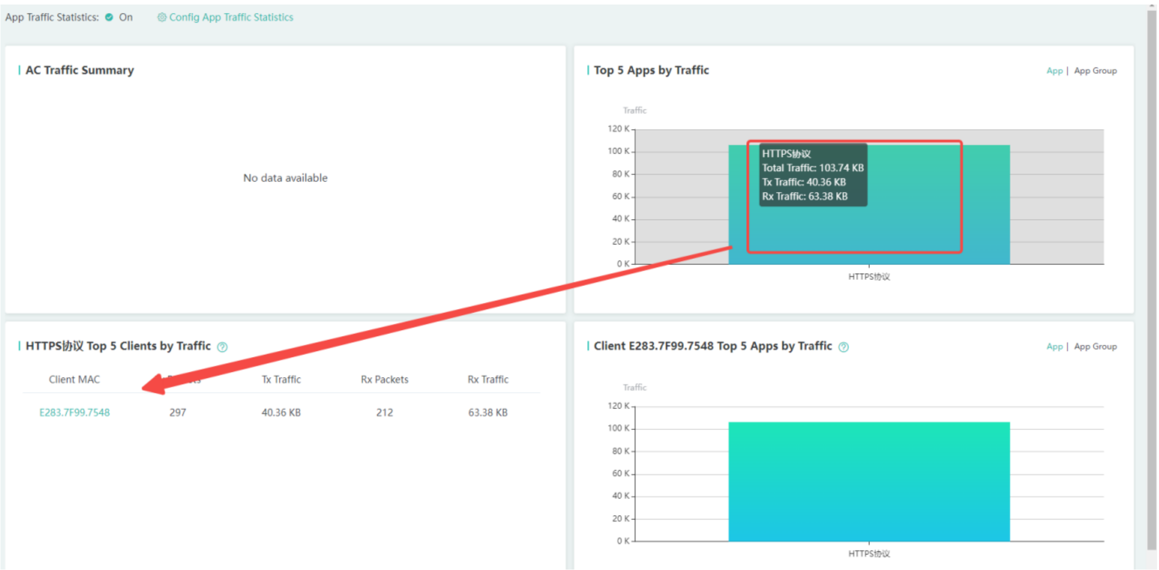
- Application traffic statistics can be displayed only after application identification is enabled. To enable application identification, click **Config App Traffic Statistics** and toggle on **App Identification** on the application identification configuration page. For details, see section 5.9.1 App Identification.



-
- The application traffic statistics are updated every 10 minutes.

(1) AC application traffic statistics: Hover the cursor over the graph to view the uplink and downlink traffic usage and proportions of applications.

(2) View top applications: In the **Top 5 Apps by Traffic** area, click an application (or application group) to view the client ranking of the application in the lower left area of the page. For example, click the block of the HTTPS protocol in the **Top 5 Apps by Traffic** area to view statistics about top 5 clients ranked by traffic of HTTPS in the lower left area.



App Traffic Statistics: ● On ⚙ Config App Traffic Statistics

AC Traffic Summary

No data available

Top 5 Apps by Traffic

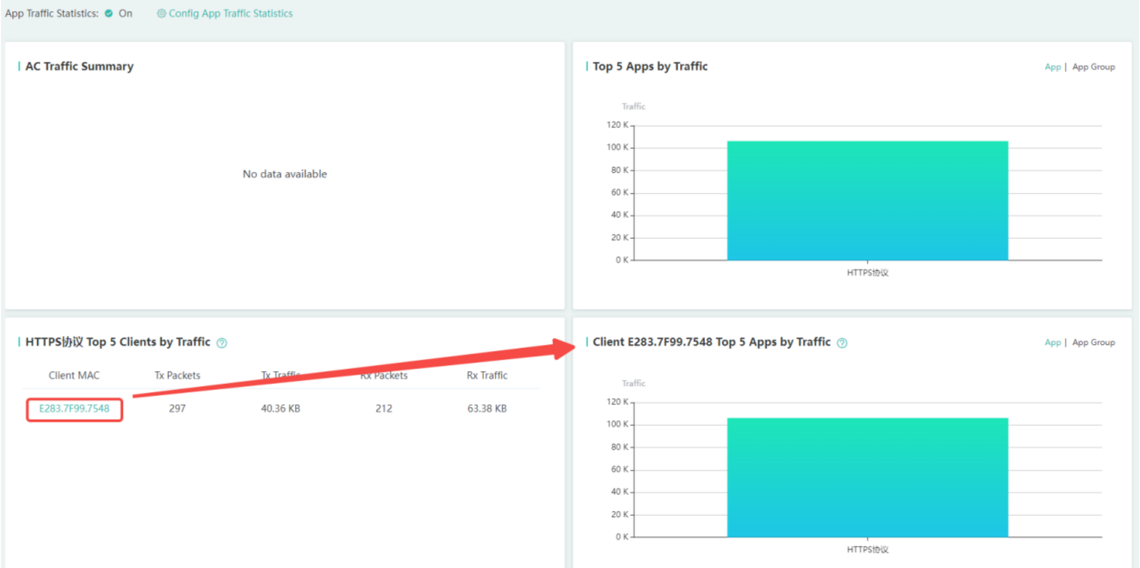
HTTPS协议
Total Traffic: 103.74 KB
Tx Traffic: 40.36 KB
Rx Traffic: 63.38 KB

HTTPS协议 Top 5 Clients by Traffic

Client MAC	Tx Packets	Tx Traffic	Rx Packets	Rx Traffic
E283.7F99.7548	297	40.36 KB	212	63.38 KB

Client E283.7F99.7548 Top 5 Apps by Traffic

(3) View top clients: In the **Top 5 Clients by Traffic** area, view MAC addresses, numbers of uplink and downlink packets, and traffic information of top clients ranked by traffic of the selected application. Click a client MAC address to view the application traffic usage of the client in the lower right area.



App Traffic Statistics: ● On ⚙ Config App Traffic Statistics

AC Traffic Summary

No data available

Top 5 Apps by Traffic

HTTPS协议 Top 5 Clients by Traffic

Client MAC	Tx Packets	Tx Traffic	Rx Packets	Rx Traffic
E283.7F99.7548	297	40.36 KB	212	63.38 KB

Client E283.7F99.7548 Top 5 Apps by Traffic

4.2 AP

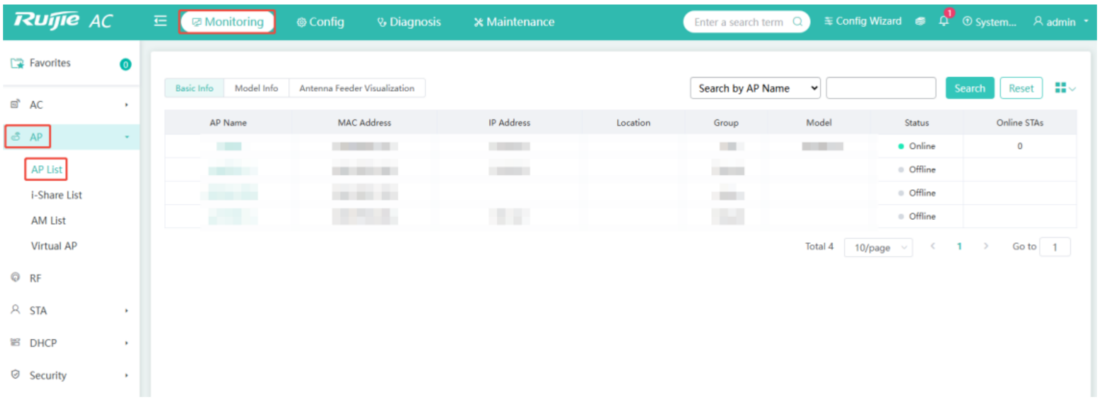
4.2.1 AP List

Choose **Monitoring** > **AP** > **AP List**.

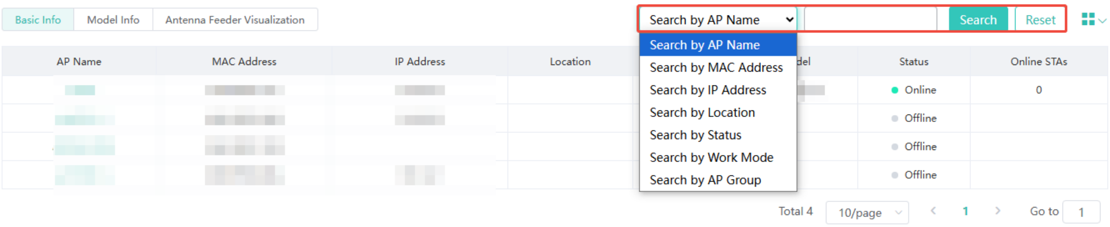
The **AP List** page displays the basic information, model information, and antenna feeder information of APs connected with the AC.

Note

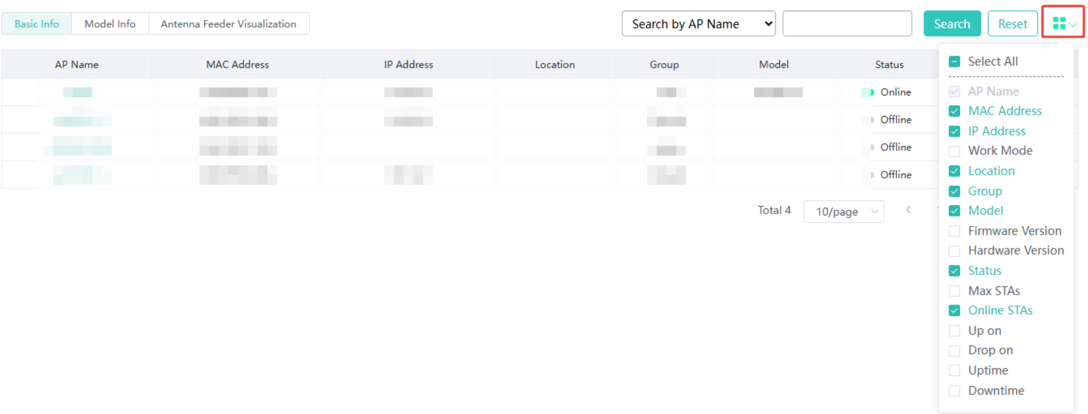
Some APs support antenna feeder visualization, depending on whether the **Antenna Feeder Visualization** menu is available on the GUI.



(1) Querying the basic AP information and models: Enter keywords in the search bar and click **Search**. Click **Reset** to clear the search criteria and display the list of all APs.



(2) To display additional information about the APs, click ▦ and select the information you wish to view.



Basic Info | Model Info | Antenna Feeder Visualization

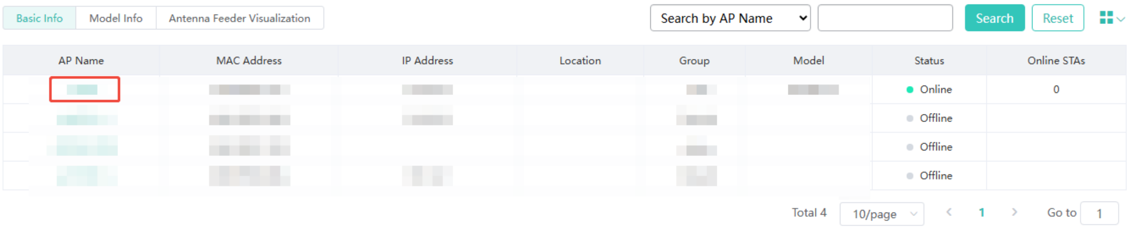
Search by AP Name | Search | Reset

AP Name	MAC Address	IP Address	Location	Group	Model	Status
[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]		[redacted]		Offline
[redacted]	[redacted]			[redacted]		Offline
[redacted]	[redacted]	[redacted]		[redacted]		Offline

Total 4 10/page

- ☑ Select All
- ☑ AP Name
- ☑ MAC Address
- ☑ IP Address
- □ Work Mode
- ☑ Location
- ☑ Group
- ☑ Model
- □ Firmware Version
- □ Hardware Version
- ☑ Status
- □ Max STAs
- ☑ Online STAs
- □ Up on
- □ Drop on
- □ Uptime
- □ Downtime

(3) Viewing AP details: Click the AP name to redirect to the AP page.



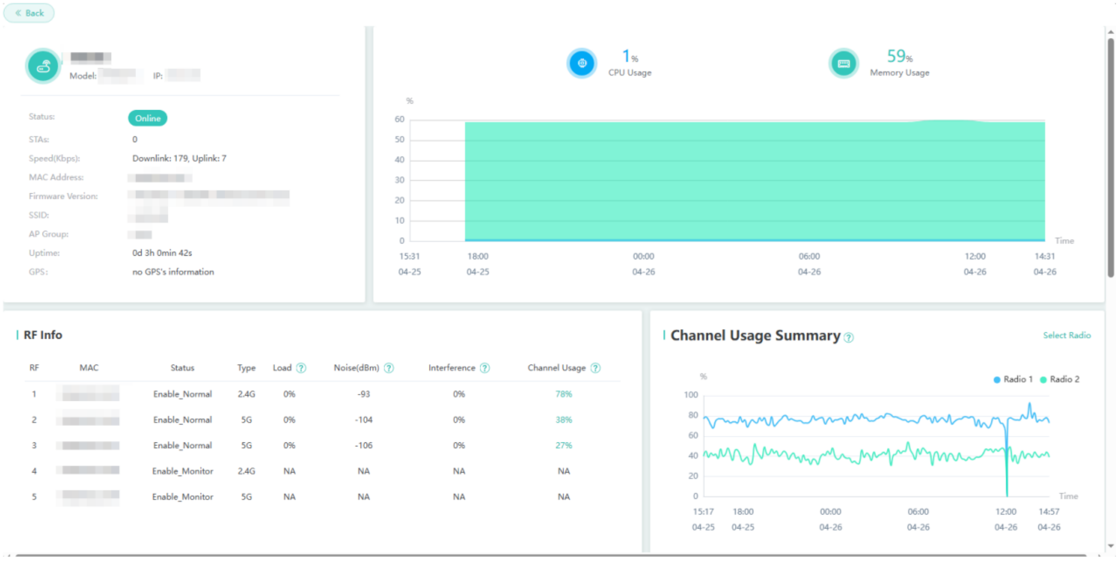
Basic Info | Model Info | Antenna Feeder Visualization

Search by AP Name | Search | Reset

AP Name	MAC Address	IP Address	Location	Group	Model	Status	Online STAs
[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	● Online	0
[redacted]	[redacted]	[redacted]		[redacted]		● Offline	
[redacted]	[redacted]			[redacted]		● Offline	
[redacted]	[redacted]	[redacted]		[redacted]		● Offline	

Total 4 10/page < 1 > Go to 1

On the AP details page, you can view the RF information, channel usage summary, and traffic summary of the current AP.



« Back

[redacted]

Model: [redacted] IP: [redacted]

Status: Online

STAs: 0

Speed(Kbps): Downlink: 179, Uplink: 7

MAC Address: [redacted]

Firmware Version: [redacted]

SSID: [redacted]

AP Group: [redacted]

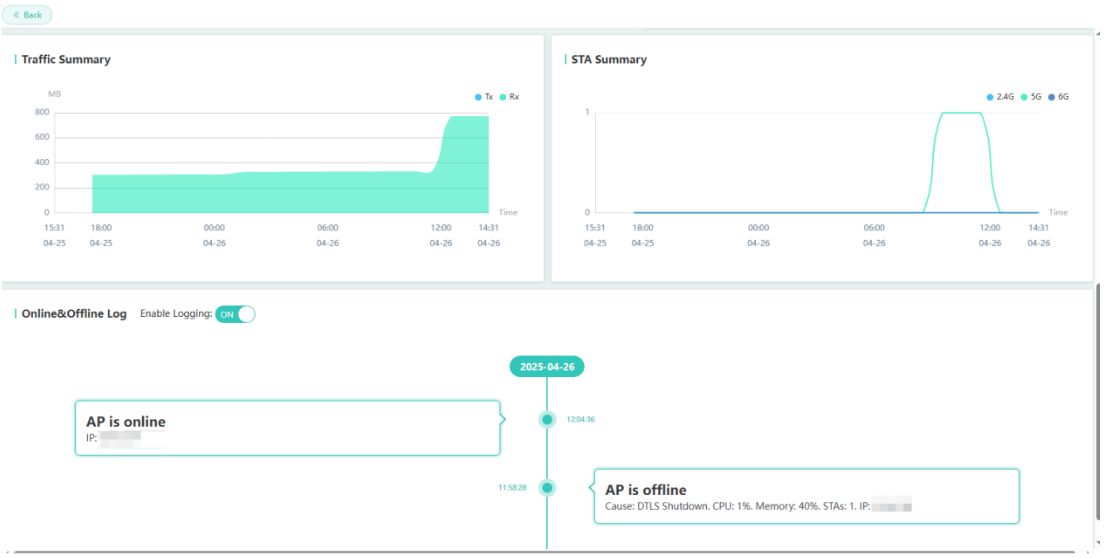
Uptime: 0d 3h 0min 42s

GPS: no GPS's information

RF Info

RF	MAC	Status	Type	Load	Noise(dBm)	Interference	Channel Usage
1	[redacted]	Enable_Normal	2.4G	0%	-93	0%	78%
2	[redacted]	Enable_Normal	5G	0%	-104	0%	38%
3	[redacted]	Enable_Normal	5G	0%	-106	0%	27%
4	[redacted]	Enable_Monitor	2.4G	NA	NA	NA	NA
5	[redacted]	Enable_Monitor	5G	NA	NA	NA	NA

Channel Usage Summary



Online&Offline Log Enable Logging: ON

2025-04-26

12:04:36 AP is online
IP: [redacted]

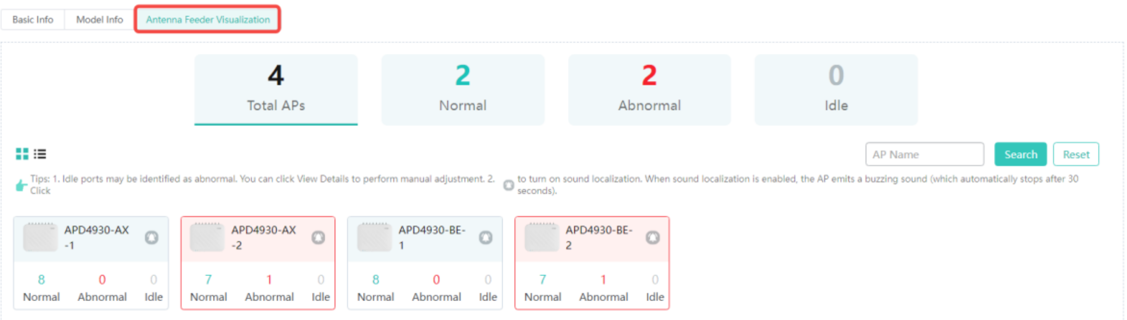
11:58:28 AP is offline
Cause: DTLS Shutdown. CPU: 1%. Memory: 40%. STAs: 1. IP: [redacted]

Page Name	Description
RF Info	Displays the radio ID, MAC address, status, type, noise, load, interference, and channel usage, and the proportions of outbound packets, inbound packets, interference, and idle channels concerning the channel usage.
Channel Usage Summary	Displays the summary of channel usage.
Traffic Summary	Displays the traffic summary of wired interfaces on the AP.
STA Summary	Displays the summary of STAs associated with the AP.
Online & Offline Log	Displays the logout reason, memory usage, CPU usage, and number of STAs associated with this AP.

(4) Viewing the antenna feeder information of APs: Click the **Antenna Feeder Visualization** tab to view the antenna feeder information. The information includes the number of APs with antenna feeder and the status of the antenna feeders.

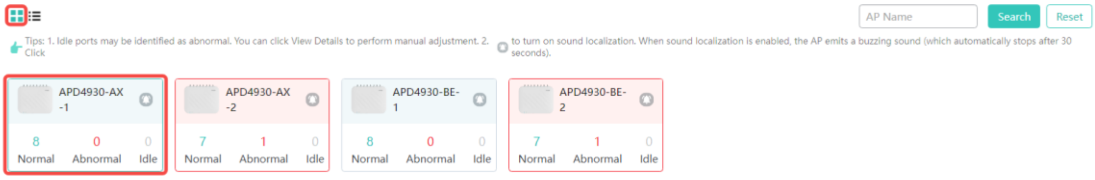
⚠ **Caution**

- Idle ports may be identified as exceptions. In this case, you can click the device card in the ▦ view or click **View Details** in the **Antenna Feeder Status** column in the ☰ view. In the **Antenna Feeder Status** dialog box that is displayed, you can modify the port status.
- Click 🔔 to enable sound localization. After this feature is enabled, the AP emits a buzzing sound that automatically stops after 30s.

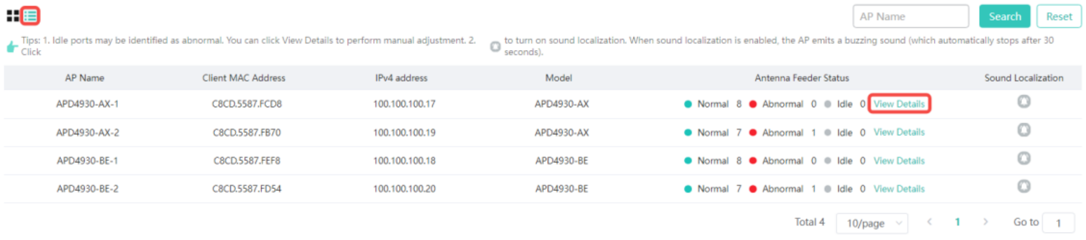

Basic Info
Model Info
Antenna Feeder Visualization
4
Total APs
2
Normal
2
Abnormal
0
Idle
AP Name
Search
Reset
APD4930-AX-1
8 Normal 0 Abnormal 0 Idle
APD4930-AX-2
7 Normal 1 Abnormal 0 Idle
APD4930-BE-1
8 Normal 0 Abnormal 0 Idle
APD4930-BE-2
7 Normal 1 Abnormal 0 Idle

Tips: 1. Idle ports may be identified as abnormal. You can click View Details to perform manual adjustment. 2. Click ○ to turn on sound localization. When sound localization is enabled, the AP emits a buzzing sound (which automatically stops after 30 seconds).

- Viewing the number of APs with antenna feeder: The total number of APs, number of APs with normal antenna feeder, number of APs with abnormal antenna feeder, and number of APs with idle antenna feeder are displayed in the upper part of the page.
- Viewing the antenna feeder status: Click the device card in the ▦ view or click **View Details** in the **Antenna Feeder Status** column in the ☰ view. In the **Antenna Feeder Status** dialog box that is displayed, you can view and modify the port status.


AP Name
Search
Reset
APD4930-AX-1
8 Normal 0 Abnormal 0 Idle
APD4930-AX-2
7 Normal 1 Abnormal 0 Idle
APD4930-BE-1
8 Normal 0 Abnormal 0 Idle
APD4930-BE-2
7 Normal 1 Abnormal 0 Idle

Tips: 1. Idle ports may be identified as abnormal. You can click View Details to perform manual adjustment. 2. Click ○ to turn on sound localization. When sound localization is enabled, the AP emits a buzzing sound (which automatically stops after 30 seconds).

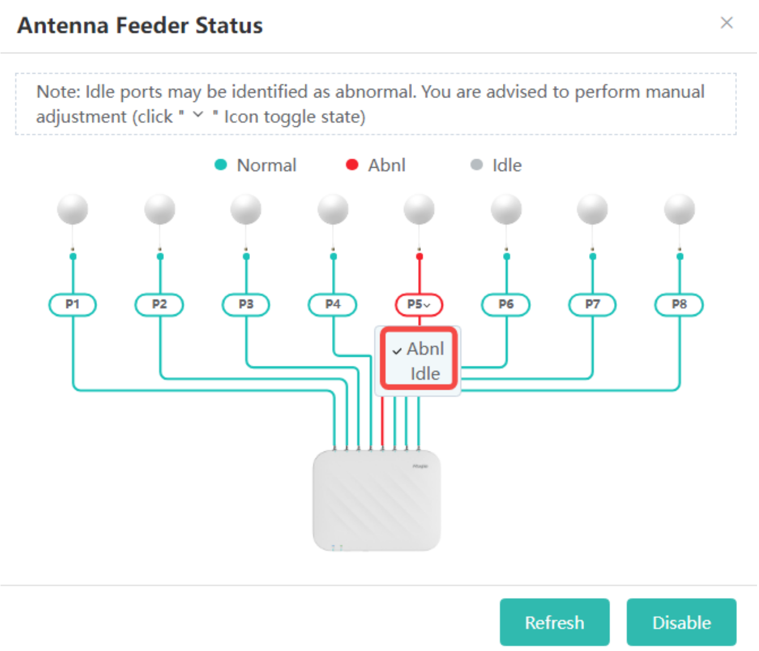


Tips: 1. Idle ports may be identified as abnormal. You can click View Details to perform manual adjustment. 2. Click ○ to turn on sound localization. When sound localization is enabled, the AP emits a buzzing sound (which automatically stops after 30 seconds).

AP Name	Client MAC Address	IPv4 address	Model	Antenna Feeder Status	Sound Localization
APD4930-AX-1	C8CD.5587.FCD8	100.100.100.17	APD4930-AX	● Normal 8 ● Abnormal 0 ● Idle 0 View Details	○
APD4930-AX-2	C8CD.5587.FB70	100.100.100.19	APD4930-AX	● Normal 7 ● Abnormal 1 ● Idle 0 View Details	○
APD4930-BE-1	C8CD.5587.FEF8	100.100.100.18	APD4930-BE	● Normal 8 ● Abnormal 0 ● Idle 0 View Details	○
APD4930-BE-2	C8CD.5587.FD54	100.100.100.20	APD4930-BE	● Normal 7 ● Abnormal 1 ● Idle 0 View Details	○

Total 4 10/page ‹ 1 › Go to 1

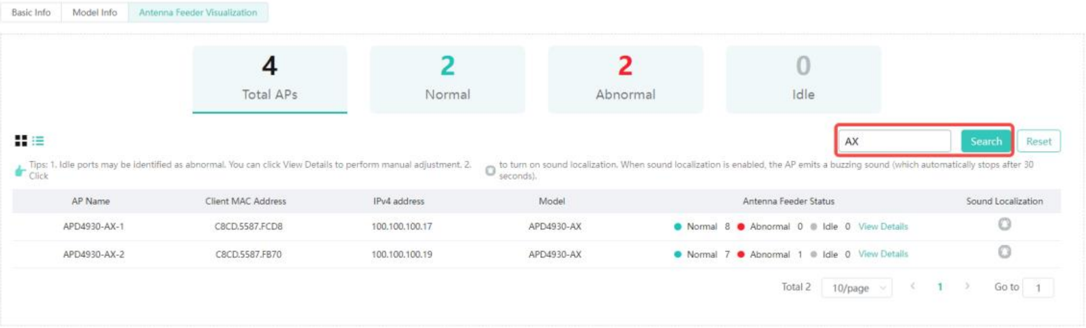
In the **Antenna Feeder Status** dialog box, as shown in the following figure, set the status of an abnormal port to **Idle** or the status of an idle port to **Abnl**.



Antenna Feeder Status

Note: Idle ports may be identified as abnormal. You are advised to perform manual adjustment (click " ⌄ " Icon toggle state)

- ○ Querying APs meeting the search condition: Enter the AP name keyword in the search box and click **Search**. APs are found in fuzzy match mode. Click **Reset** to clear the search criteria and display the list of all APs.



Tips: 1. Idle ports may be identified as abnormal. You can click View Details to perform manual adjustment. 2. Click ○ to turn on sound localization. When sound localization is enabled, the AP emits a buzzing sound (which automatically stops after 30 seconds).

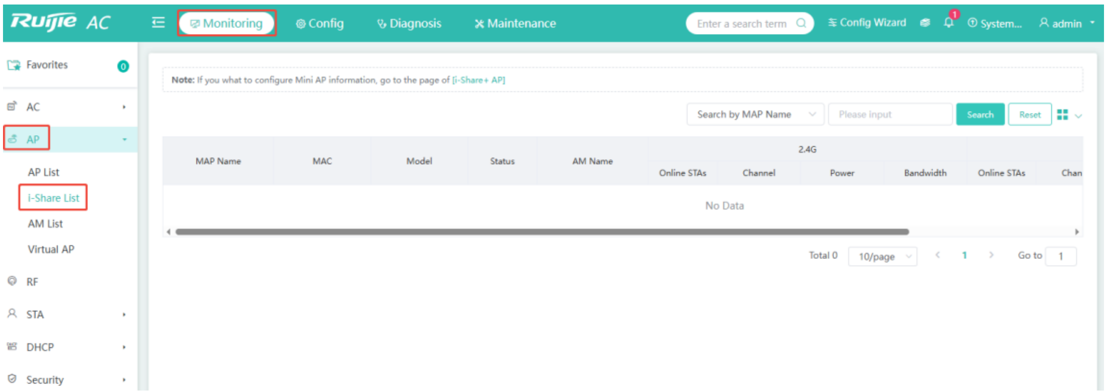
AP Name	Client MAC Address	IPv4 address	Model	Antenna Feeder Status	Sound Localization
APD4930-AX-1	C8CD.5587.FCD8	100.100.100.17	APD4930-AX	● Normal 8 ● Abnormal 0 ● Idle 0 View Details	○
APD4930-AX-2	C8CD.5587.FB70	100.100.100.19	APD4930-AX	● Normal 7 ● Abnormal 1 ● Idle 0 View Details	○

Total 2 10/page ‹ 1 › Go to 1

4.2.2 i-Share List

Choose **Monitoring** > **AP** > **i-Share List**.

The **i-Share List** page displays i-Share Mini APs (MAPs). If an MAP is offline, the device name, MAC address, and model are not displayed.

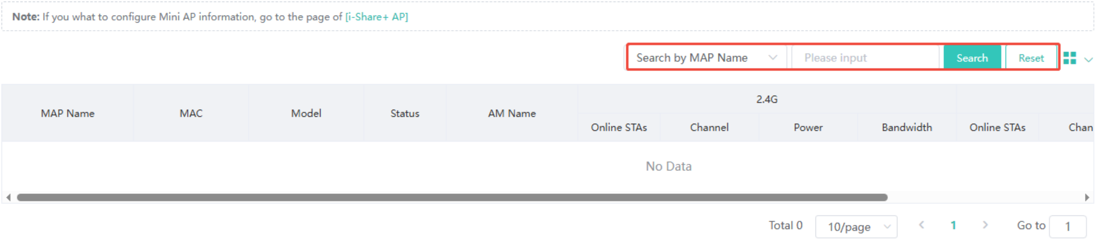


Note: If you what to configure Mini AP information, go to the page of [i-Share+ AP]

MAP Name	MAC	Model	Status	AM Name	2.4G					
					Online STAs	Channel	Power	Bandwidth	Online STAs	Chan
No Data										

Total 0 10/page < 1 > Go to 1

Querying MAPs: Narrow down the search scope by category, enter the search criteria in the search box, and click **Search** to search for MAPs. Click **Reset** to clear the search criteria and display the list of all APs.

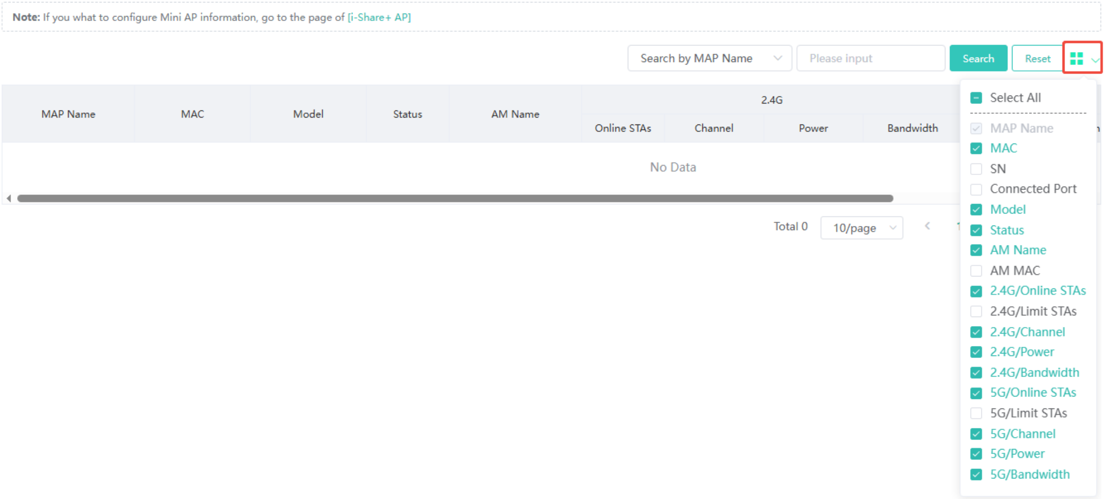


Note: If you what to configure Mini AP information, go to the page of [i-Share+ AP]

MAP Name	MAC	Model	Status	AM Name	2.4G					
					Online STAs	Channel	Power	Bandwidth	Online STAs	Chan
No Data										

Total 0 10/page < 1 > Go to 1

If you want to display other information of MAPs on the **i-Share List** page, click ▦ and select the information to display.



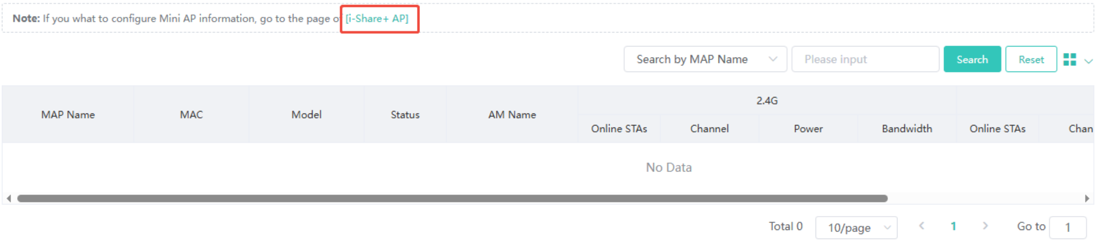
Note: If you what to configure Mini AP information, go to the page of [i-Share+ AP]

MAP Name	MAC	Model	Status	AM Name	2.4G			
					Online STAs	Channel	Power	Bandwidth
No Data								

Total 0 10/page

- ☑ Select All
- ☑ MAP Name
- ☑ MAC
- □ SN
- □ Connected Port
- ☑ Model
- ☑ Status
- ☑ AM Name
- □ AM MAC
- ☑ 2.4G/Online STAs
- □ 2.4G/Limit STAs
- ☑ 2.4G/Channel
- ☑ 2.4G/Power
- ☑ 2.4G/Bandwidth
- ☑ 5G/Online STAs
- □ 5G/Limit STAs
- ☑ 5G/Channel
- ☑ 5G/Power
- ☑ 5G/Bandwidth

If you want to configure MAPs, click [i-Share+ AP] to configure MAPs on the **i-Share+ AP** page.



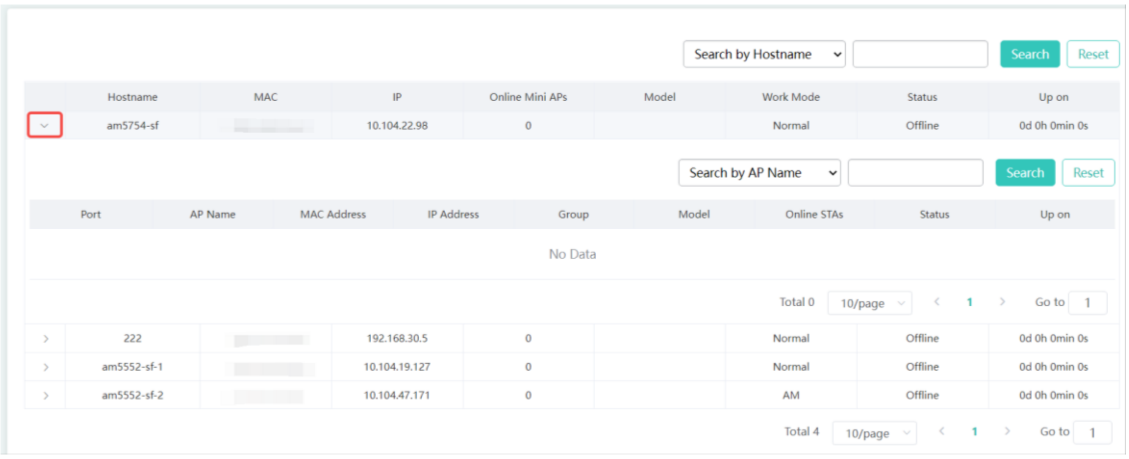
Note: If you what to configure Mini AP information, go to the page o [i-Share+ AP]

MAP Name	MAC	Model	Status	AM Name	2.4G					
					Online STAs	Channel	Power	Bandwidth	Online STAs	Chan
No Data										

4.2.3 AM List

Choose **Monitoring** > **AP** > **AM List**.

This page displays the all-optical i-Share+ master APs and their associated micro APs. If a device is offline, its name will not be displayed. Click the › on the left side of the hostname to view the information about the micro APs associated with the master AP. You can search for the master AP or micro AP.



	Hostname	MAC	IP	Online Mini APs	Model	Work Mode	Status	Up on
⌄	am5754-sf	[redacted]	10.104.22.98	0		Normal	Offline	0d 0h 0min 0s

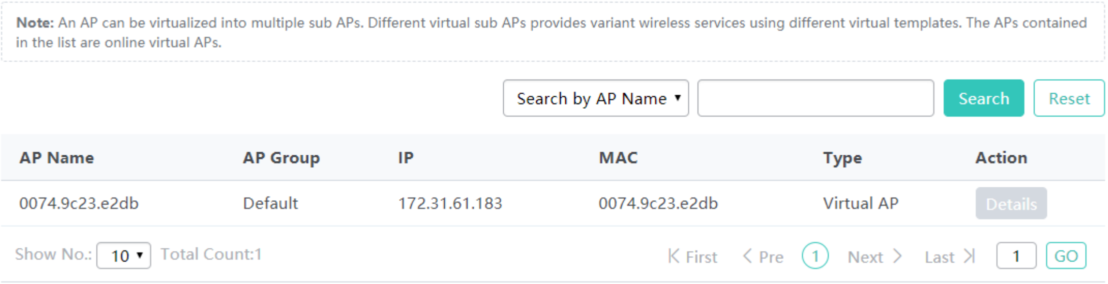
Port	AP Name	MAC Address	IP Address	Group	Model	Online STAs	Status	Up on
No Data								

	Hostname	MAC	IP	Online Mini APs	Model	Work Mode	Status	Up on
›	222	[redacted]	192.168.30.5	0		Normal	Offline	0d 0h 0min 0s
›	am5552-sf-1	[redacted]	10.104.19.127	0		Normal	Offline	0d 0h 0min 0s
›	am5552-sf-2	[redacted]	10.104.47.171	0		AM	Offline	0d 0h 0min 0s

4.2.4 Virtual AP

Choose **Monitoring** > **AP** > **Virtual AP**.

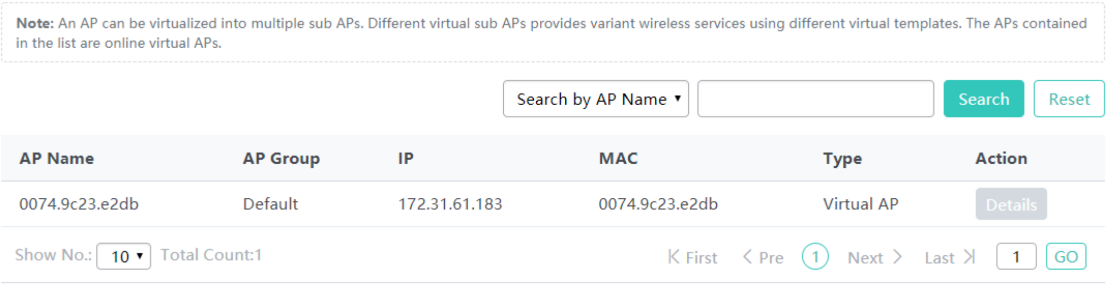
This page displays details of virtual APs.



Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates. The APs contained in the list are online virtual APs.

AP Name	AP Group	IP	MAC	Type	Action
0074.9c23.e2db	Default	172.31.61.183	0074.9c23.e2db	Virtual AP	Details

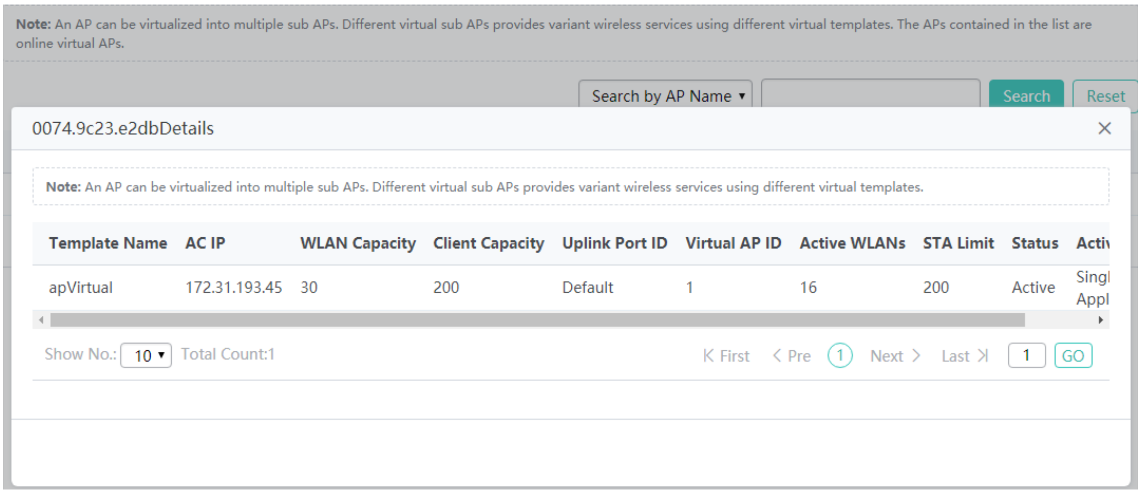
Searching for APs: Enter keywords in the search bar and click **Search**. Click **Reset** to clear the search criteria and display the list of all APs.



Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates. The APs contained in the list are online virtual APs.

AP Name	AP Group	IP	MAC	Type	Action
0074.9c23.e2db	Default	172.31.61.183	0074.9c23.e2db	Virtual AP	Details

Details: Click **Details** in the Action column and a window displaying the details of the virtual AP pops up.



Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates. The APs contained in the list are online virtual APs.

0074.9c23.e2dbDetails

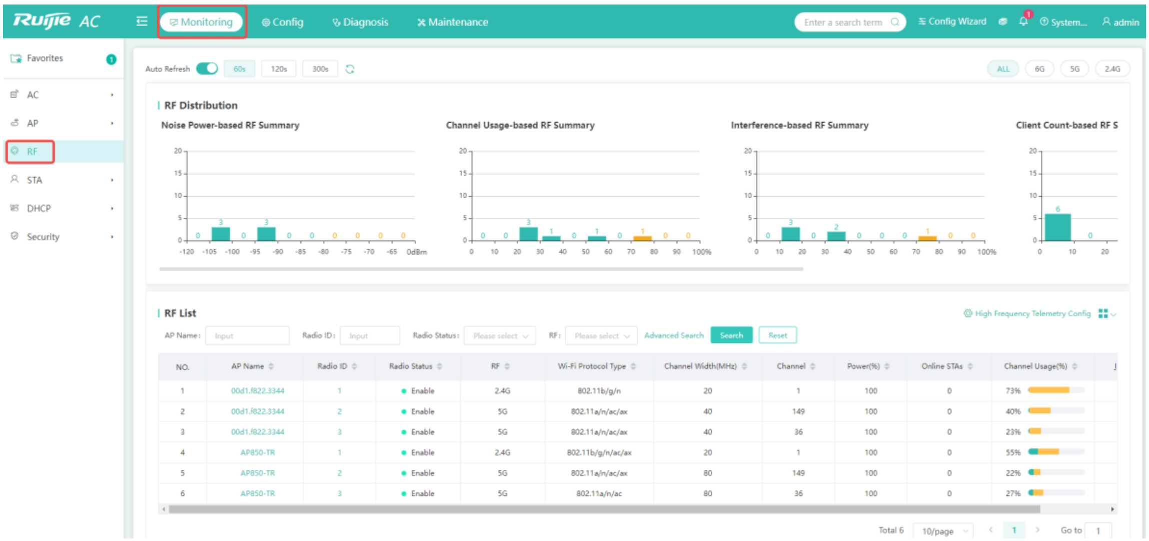
Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates.

Template Name	AC IP	WLAN Capacity	Client Capacity	Uplink Port ID	Virtual AP ID	Active WLANs	STA Limit	Status	Acti
apVirtual	172.31.193.45	30	200	Default	1	16	200	Active	Singl Appl

4.3 RF

Choose **Monitoring** > **RF**.

The RF page displays noise power-based, channel usage-based, and interference-based RF summary. The RF details about all APs are available in the RF list.

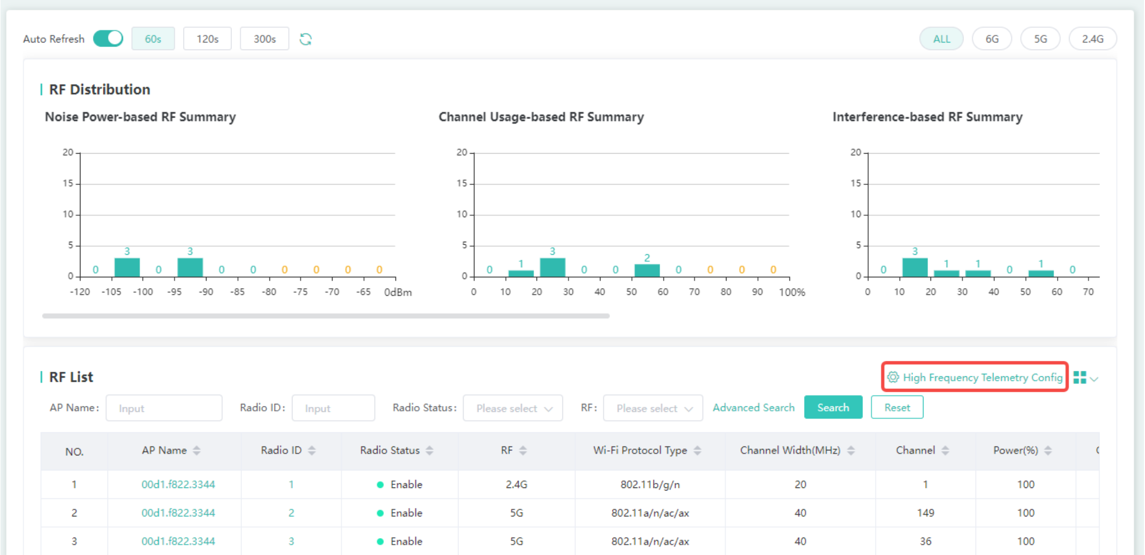


NO.	AP Name	Radio ID	Radio Status	RF	Wi-Fi Protocol Type	Channel Width(MHz)	Channel	Power(%)	Online STAs	Channel Usage(%)
1	00d1.f822.3344	1	● Enable	2.4G	802.11b/g/n	20	1	100	0	73%
2	00d1.f822.3344	2	● Enable	5G	802.11a/n/ac/ax	40	149	100	0	40%
3	00d1.f822.3344	3	● Enable	5G	802.11a/n/ac/ax	40	36	100	0	23%
4	AP850-TR	1	● Enable	2.4G	802.11b/g/n/ac/ax	20	1	100	0	55%
5	AP850-TR	2	● Enable	5G	802.11a/n/ac/ax	80	149	100	0	22%
6	AP850-TR	3	● Enable	5G	802.11a/n/ac	80	36	100	0	27%

4.3.1 Configuring RF Data for High-Frequency Telemetry

High-frequency telemetry enables high-frequency monitoring and data recording for specified clients or radios, visualizing client details and some key indicators on the web UI. This feature allows administrators to view the historical trend and details of key indicators of specified clients or radios based on data provided by ACs, so as to locate faults and issues in a timely manner.

Click **High Frequency Telemetry Config**. The **High Frequency Telemetry Config for RF Data Collection** dialog box is displayed.



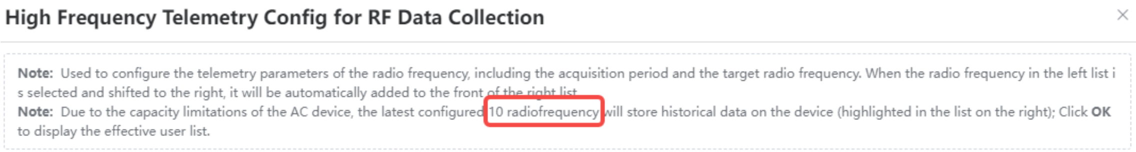
AP Name: Input Radio ID: Input Radio Status: Please select RF: Please select

NO.	AP Name	Radio ID	Radio Status	RF	Wi-Fi Protocol Type	Channel Width(MHz)	Channel	Power(%)
1	00d1.f822.3344	1	● Enable	2.4G	802.11b/g/n	20	1	100
2	00d1.f822.3344	2	● Enable	5G	802.11a/n/ac/ax	40	149	100
3	00d1.f822.3344	3	● Enable	5G	802.11a/n/ac/ax	40	36	100

In the **High Frequency Telemetry Config for RF Data Collection** dialog box, configure the RF data collection cycle and objects. Select objects in the left pane, and click > to add them to the **Selected** pane on the right.

Note

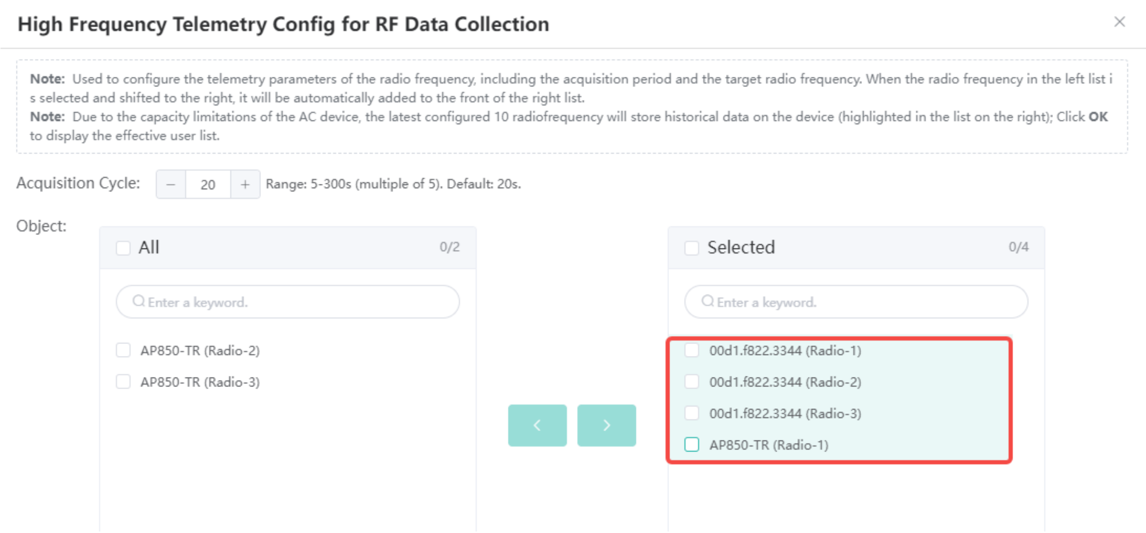
- Due to the AC capacity limitation, historical data of only radios newly added for high-frequency telemetry (highlighted in the **Selected** pane on the right) will be stored on the AC. For radios that are not highlighted, only data collection is enabled, but the collected data is not stored on the AC.
- The capacity limit of an AC varies with the AC model. Therefore, the number of radios for which historical data can be stored on an AC varies. For details about the number of radios that can be stored, check the prompt on the web UI.



High Frequency Telemetry Config for RF Data Collection

Note: Used to configure the telemetry parameters of the radio frequency, including the acquisition period and the target radio frequency. When the radio frequency in the left list is selected and shifted to the right, it will be automatically added to the front of the right list.
Note: Due to the capacity limitations of the AC device, the latest configured 10 radiofrequency will store historical data on the device (highlighted in the list on the right); Click **OK** to display the effective user list.

The radios highlighted in the **Selected** pane on the right are newly added ones.



High Frequency Telemetry Config for RF Data Collection

Note: Used to configure the telemetry parameters of the radio frequency, including the acquisition period and the target radio frequency. When the radio frequency in the left list i s selected and shifted to the right, it will be automatically added to the front of the right list.
Note: Due to the capacity limitations of the AC device, the latest configured 10 radiofrequency will store historical data on the device (highlighted in the list on the right); Click **OK** to display the effective user list.

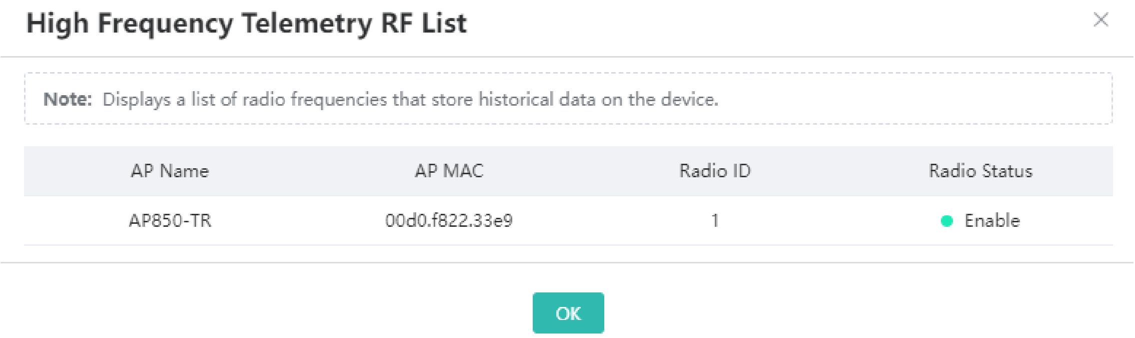
Acquisition Cycle: 20 Range: 5-300s (multiple of 5). Default: 20s.

Object:

□ All 0/2
- □ AP850-TR (Radio-2)
- □ AP850-TR (Radio-3)

□ Selected 0/4
- □ 00d1.f822.3344 (Radio-1)
- □ 00d1.f822.3344 (Radio-2)
- □ 00d1.f822.3344 (Radio-3)
- □ AP850-TR (Radio-1)

Click **OK**. After successful configuration, the **High Frequency Telemetry RF List** is displayed. In the list, check RF information about high-frequency telemetry, including the AP name, AP MAC address, radio ID, and radio status.

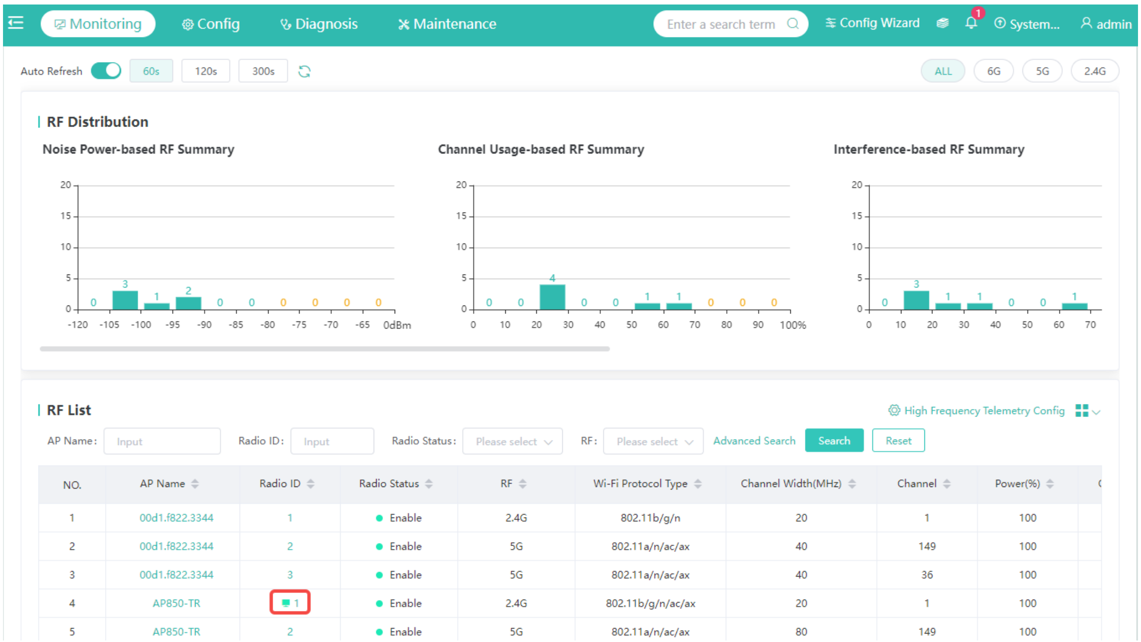


High Frequency Telemetry RF List

Note: Displays a list of radio frequencies that store historical data on the device.

AP Name	AP MAC	Radio ID	Radio Status
AP850-TR	00d0.f822.33e9	1	● Enable

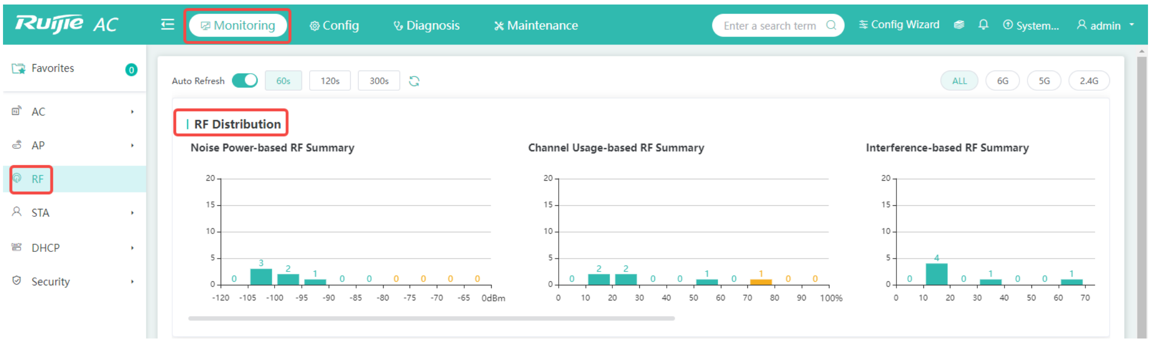
Click **OK** to return to the **RF List**. In the list, radios with the 🖥 icon in the **Radio ID** column are enabled with high-frequency telemetry.

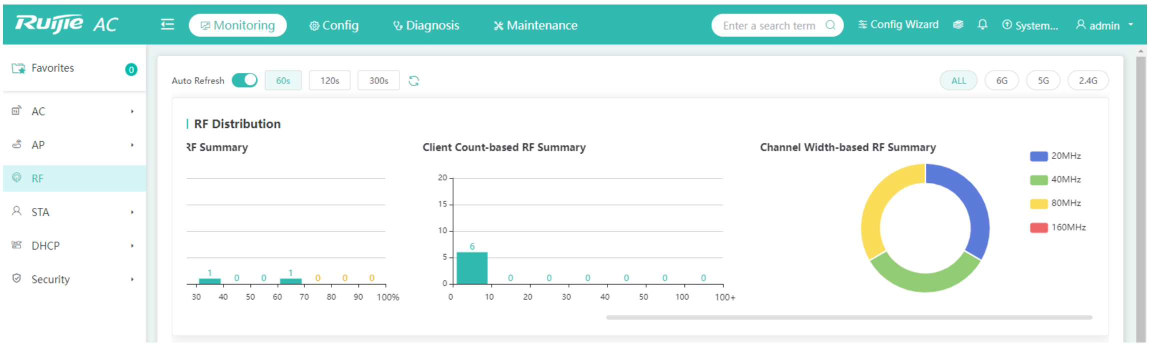


NO.	AP Name	Radio ID	Radio Status	RF	Wi-Fi Protocol Type	Channel Width(MHz)	Channel	Power(%)
1	00d1.f822.3344	1	● Enable	2.4G	802.11b/g/n	20	1	100
2	00d1.f822.3344	2	● Enable	5G	802.11a/n/ac/ax	40	149	100
3	00d1.f822.3344	3	● Enable	5G	802.11a/n/ac/ax	40	36	100
4	AP850-TR	1	● Enable	2.4G	802.11b/g/n/ac/ax	20	1	100
5	AP850-TR	2	● Enable	5G	802.11a/n/ac/ax	80	149	100

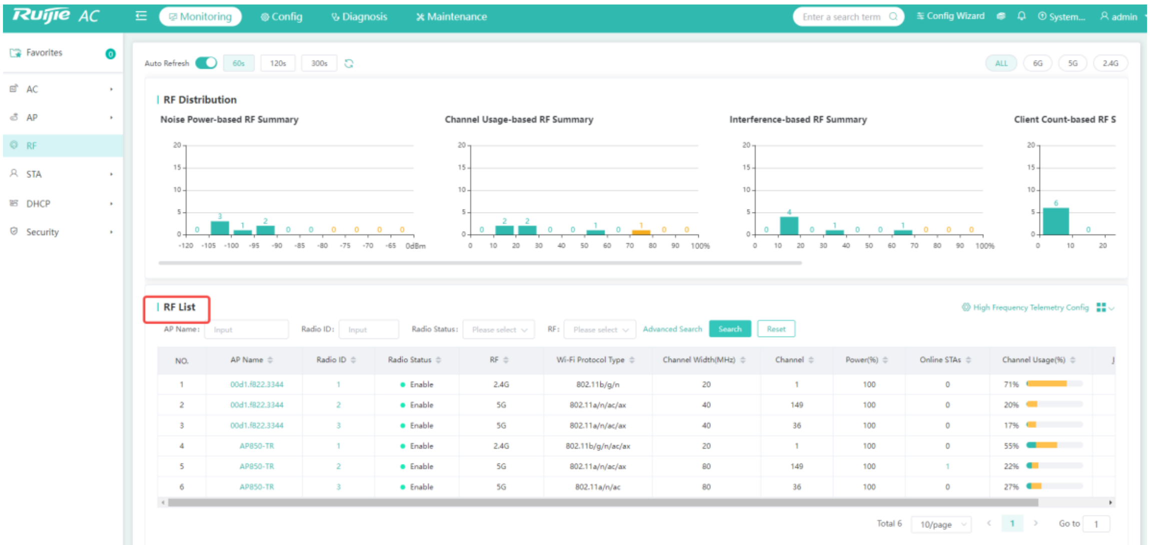
4.3.2 RF Distribution and RF List

On the **RF** page, check the RF distribution based on the noise power, channel usage, interference, client count, and channel width of the AC.





In the **RF List**, check detailed RF information about all APs.



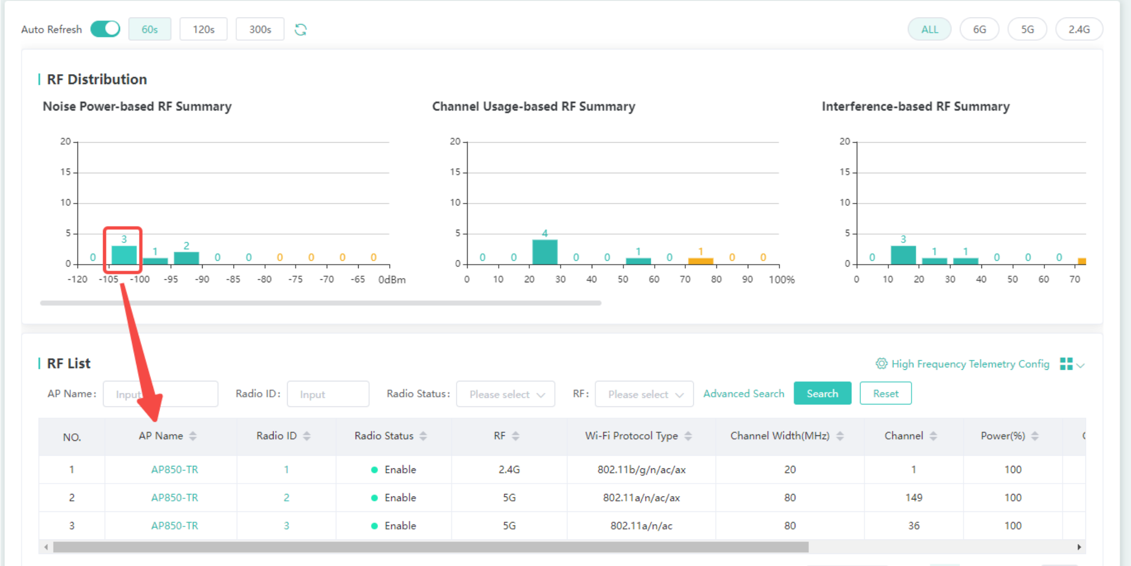
RF List

AP Name: Input Radio ID: Input Radio Status: Please select RF: Please select Advanced Search Search Reset

NO.	AP Name	Radio ID	Radio Status	RF	Wi-Fi Protocol Type	Channel Width(MHz)	Channel	Power(%)	Online STAs	Channel Usage(%)
1	00d1.f822.3344	1	Enable	2.4G	802.11b/g/n	20	1	100	0	71%
2	00d1.f822.3344	2	Enable	5G	802.11a/n/ac/ax	40	149	100	0	20%
3	00d1.f822.3344	3	Enable	5G	802.11a/n/ac/ax	40	36	100	0	17%
4	AP850-TR	1	Enable	2.4G	802.11b/g/n/ac/ax	20	1	100	0	55%
5	AP850-TR	2	Enable	5G	802.11a/n/ac/ax	80	149	100	1	22%
6	AP850-TR	3	Enable	5G	802.11a/n/ac	80	36	100	0	27%

Total 6 10/page 1 Go to 1

(1) The RF summary bars are linked to the items in the RF list. Click a bar, and its related items in the RF list are displayed.

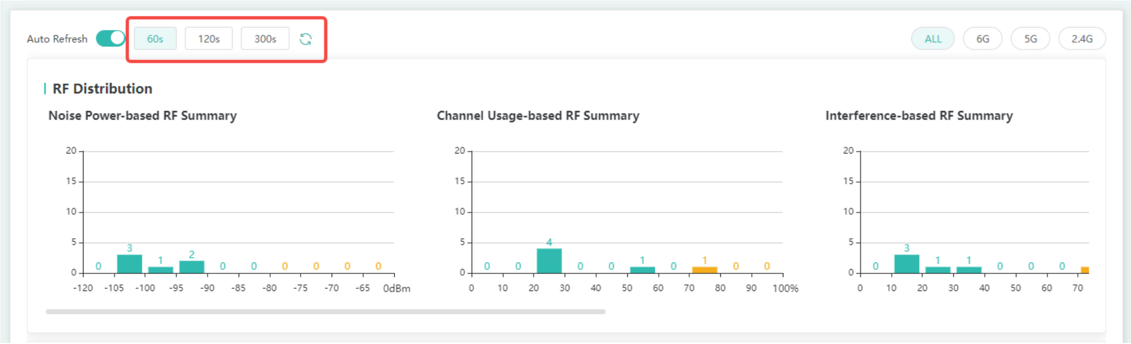

Auto Refresh
60s
120s
300s
ALL
6G
5G
2.4G
RF Distribution
Noise Power-based RF Summary
Channel Usage-based RF Summary
Interference-based RF Summary
High Frequency Telemetry Config

RF List

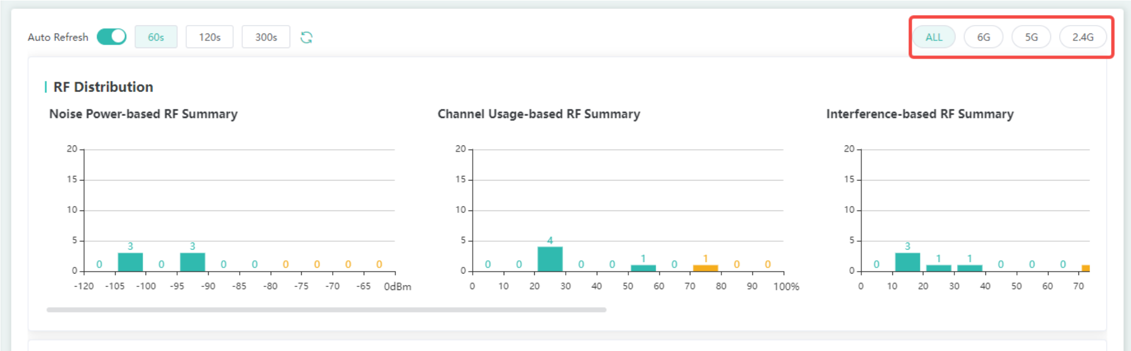
AP Name: Input Radio ID: Input Radio Status: Please select RF: Please select Advanced Search Search Reset

NO.	AP Name	Radio ID	Radio Status	RF	Wi-Fi Protocol Type	Channel Width(MHz)	Channel	Power(%)
1	AP850-TR	1	Enable	2.4G	802.11b/g/n/ac/ax	20	1	100
2	AP850-TR	2	Enable	5G	802.11a/n/ac/ax	80	149	100
3	AP850-TR	3	Enable	5G	802.11a/n/ac	80	36	100

(2) Enable **Auto Refresh** and set an auto-refresh interval. The RF summaries will be refreshed automatically at regular intervals.


Auto Refresh
60s
120s
300s
ALL
6G
5G
2.4G
RF Distribution
Noise Power-based RF Summary
Channel Usage-based RF Summary
Interference-based RF Summary

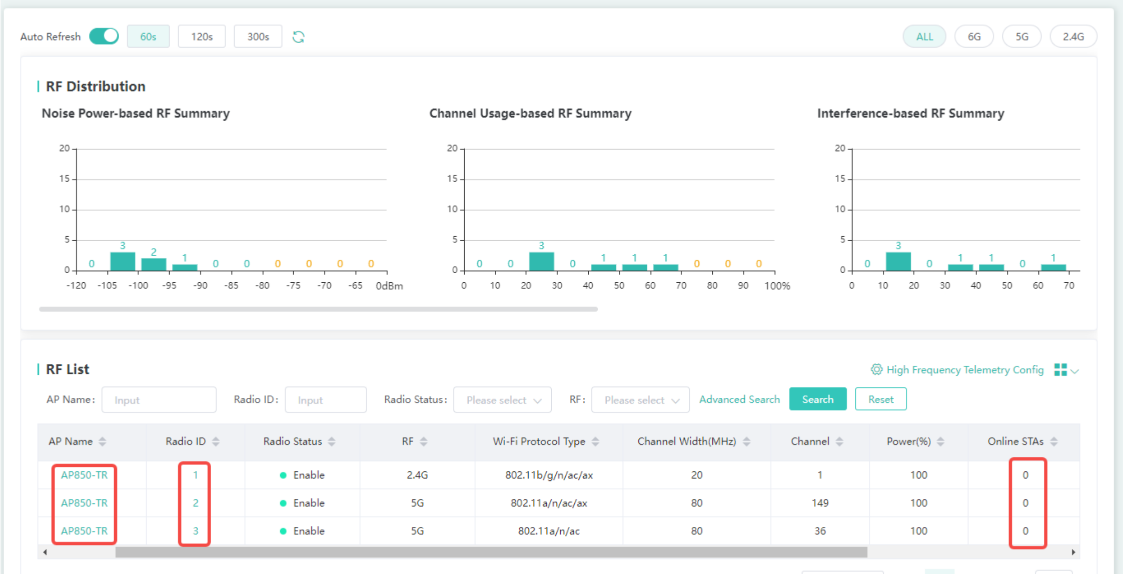
(3) Click a radio in the upper right corner to filter data on the page by radio.


Auto Refresh
60s
120s
300s
ALL
6G
5G
2.4G
RF Distribution
Noise Power-based RF Summary
Channel Usage-based RF Summary
Interference-based RF Summary
-120 -105 -100 -95 -90 -85 -80 -75 -70 -65 0dBm
0 10 20 30 40 50 60 70 80 90 100%
0 10 20 30 40 50 60 70

(4) Click the values in the **AP Name**, **Radio ID**, or **Online STAs** column in the **RF List** to redirect to the details page of the specified radio.

Note

You can only redirect to the details page of the specified radio when there is at least one online STA.


Auto Refresh
60s
120s
300s
ALL
6G
5G
2.4G
RF Distribution
Noise Power-based RF Summary
Channel Usage-based RF Summary
Interference-based RF Summary
-120 -105 -100 -95 -90 -85 -80 -75 -70 -65 0dBm
0 10 20 30 40 50 60 70 80 90 100%
0 10 20 30 40 50 60 70
RF List
High Frequency Telemetry Config
AP Name: Input
Radio ID: Input
Radio Status: Please select
RF: Please select
Advanced Search
Search
Reset

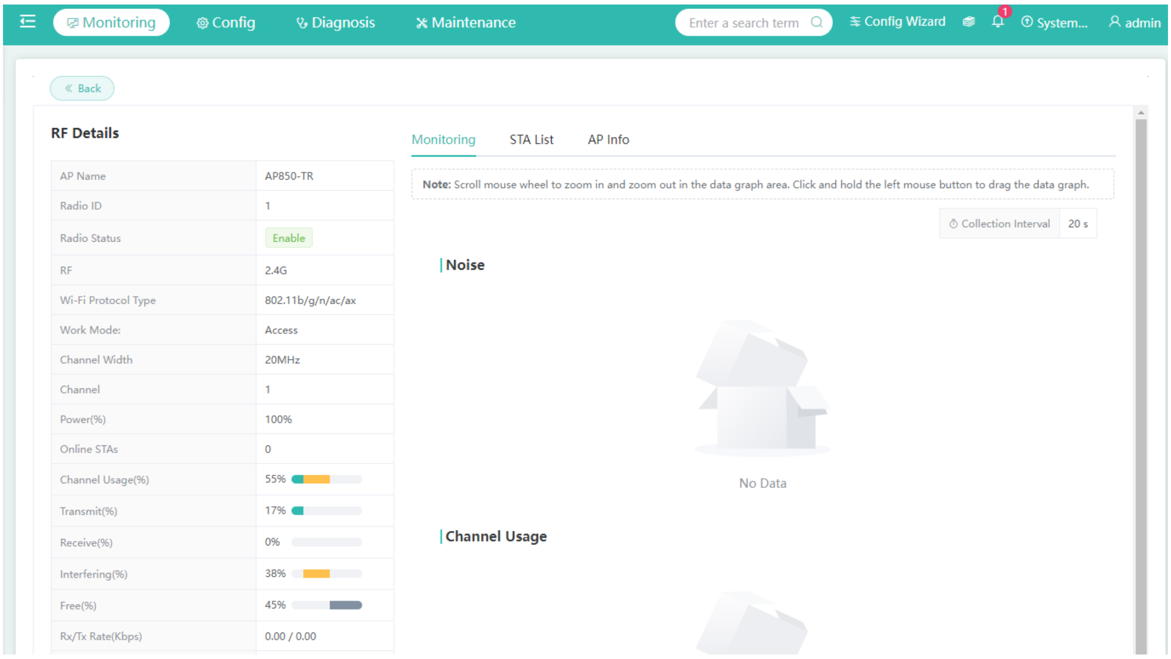
AP Name	Radio ID	Radio Status	RF	Wi-Fi Protocol Type	Channel Width(MHz)	Channel	Power(%)	Online STAs
AP850-TR	1	● Enable	2.4G	802.11b/g/n/ac/ax	20	1	100	0
AP850-TR	2	● Enable	5G	802.11a/n/ac/ax	80	149	100	0
AP850-TR	3	● Enable	5G	802.11a/n/ac	80	36	100	0

4.3.3 Viewing RF Details

On the **RF Details** page, check the details, monitoring data, and STA list of the radio, and basic information about the AP to which the radio belongs.

1. RF Details

Check RF details in the RF details table.



RF Details

AP Name	AP850-TR
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n/ac/ax
Work Mode:	Access
Channel Width	20MHz
Channel	1
Power(%)	100%
Online STAs	0
Channel Usage(%)	55%
Transmit(%)	17%
Receive(%)	0%
Interfering(%)	38%
Free(%)	45%
Rx/Tx Rate(Kbps)	0.00 / 0.00

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

Noise

Channel Usage

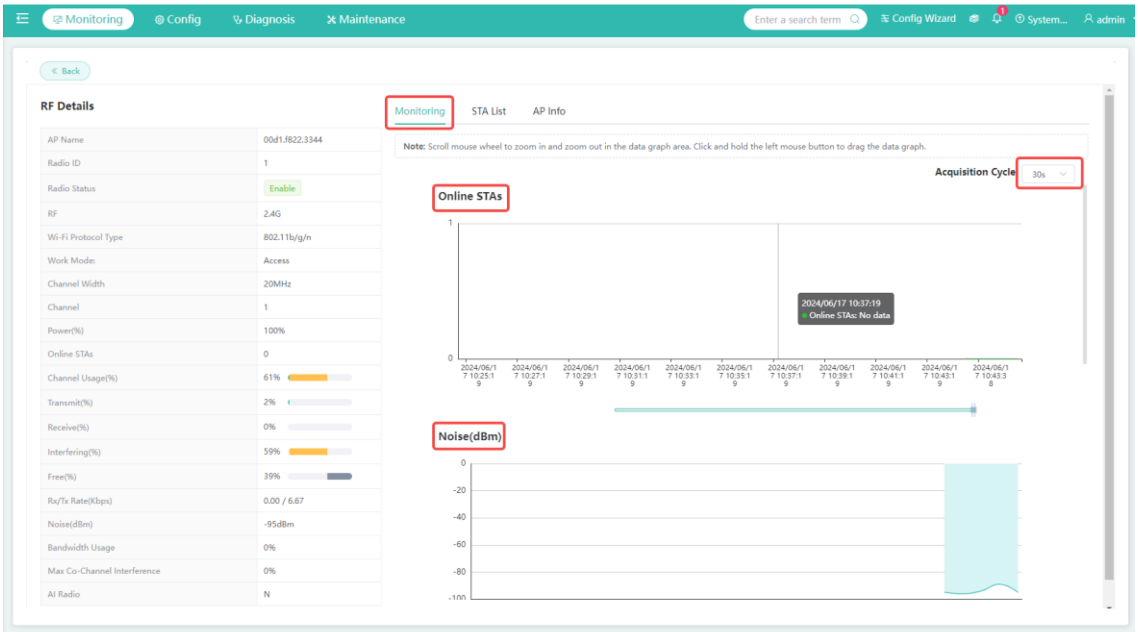
2. Monitoring

Note

If the radio is an AI Radio or the radio is disabled, no data is displayed on the **Monitoring** tab page.

- If the radio is not enabled with high-frequency telemetry, when the **Monitoring** tab page is accessed, the system collects **Online STAs**, **Noise**, **Channel Usage**, and **Speed** data based on the collection cycle of the radio and displays the collected data in real time.

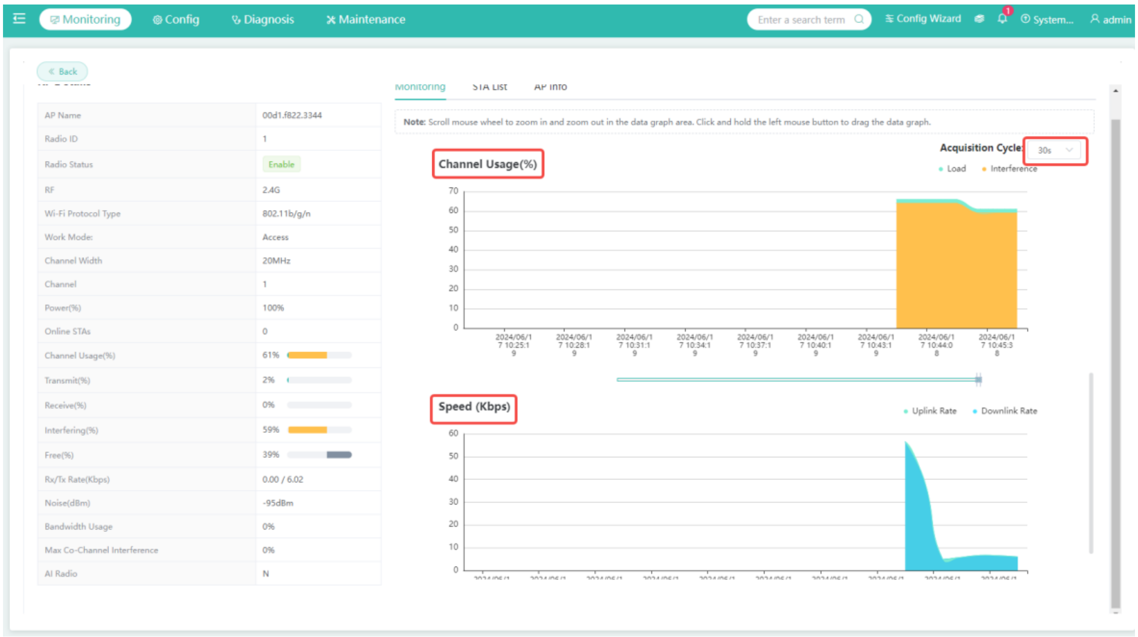
  If you exit the **RF Details** page, the data collection function on the **Monitoring** tab page will be disabled for this radio. When you access the **RF Details** page and click the **Monitoring** tab next time, data on the radio is collected based on the configured collection cycle and displayed in real time again.



RF Details

AP Name	00d1.f822.3344
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n
Work Mode:	Access
Channel Width	20MHz
Channel	1
Power(%)	100%
Online STAs	0
Channel Usage(%)	61%
Transmit(%)	2%
Receive(%)	0%
Interfering(%)	59%
Free(%)	39%
Rx/Tx Rate(Kbps)	0.00 / 6.67
Noise(dBm)	-95dBm
Bandwidth Usage	0%
Max Co-Channel Interference	0%
AI Radio	N

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.



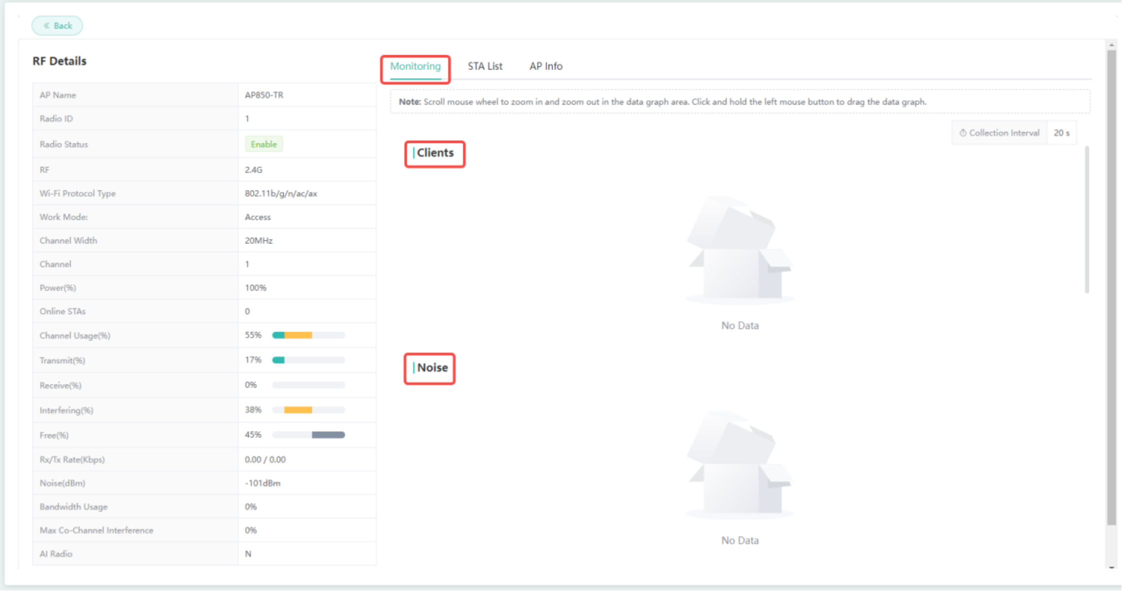
Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

AP Name	00d1.f822.3344
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n
Work Mode:	Access
Channel Width	20MHz
Channel	1
Power(%)	100%
Online STAs	0
Channel Usage(%)	61%
Transmit(%)	2%
Receive(%)	0%
Interfering(%)	59%
Free(%)	39%
Rx/Tx Rate(Kbps)	0.00 / 6.02
Noise(dBm)	-95dBm
Bandwidth Usage	0%
Max Co-Channel Interference	0%
AI Radio	N

Note

If the device supports the configuration of the sampling interval, select a value from the **Sampling Interval** drop-down list in the upper right corner of this page to set a sampling interval. If it is not supported, the sampling interval is 300s by default.

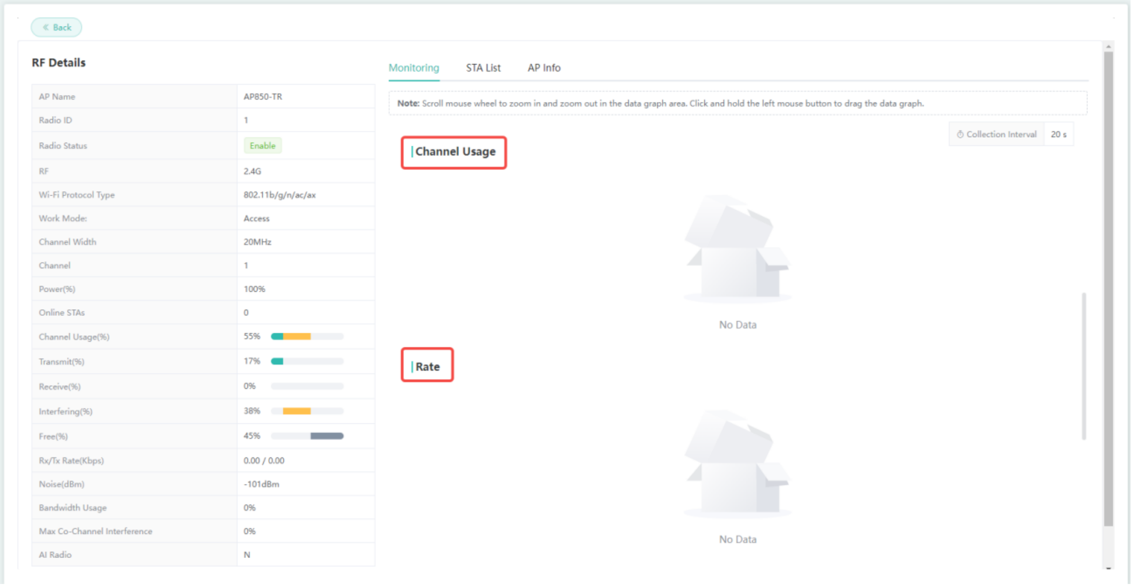
- If high-frequency telemetry is enabled for a radio, historical data about **Clients**, **Noise**, **Channel Usage**, **Rate**, and **Packet Loss/Retry Rate** of the radio is displayed on the **Monitoring** tab page.



RF Details

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

AP Name	AP850-TR
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n/ac/ax
Work Mode:	Access
Channel Width	20MHz
Channel	1
Power(%)	100%
Online STAs	0
Channel Usage(%)	55%
Transmit(%)	17%
Receive(%)	0%
Interfering(%)	38%
Free(%)	45%
Rx/Tx Rate(Kbps)	0.00 / 0.00
Noise(dBm)	-101dBm
Bandwidth Usage	0%
Max Co-Channel Interference	0%
AI Radio	N

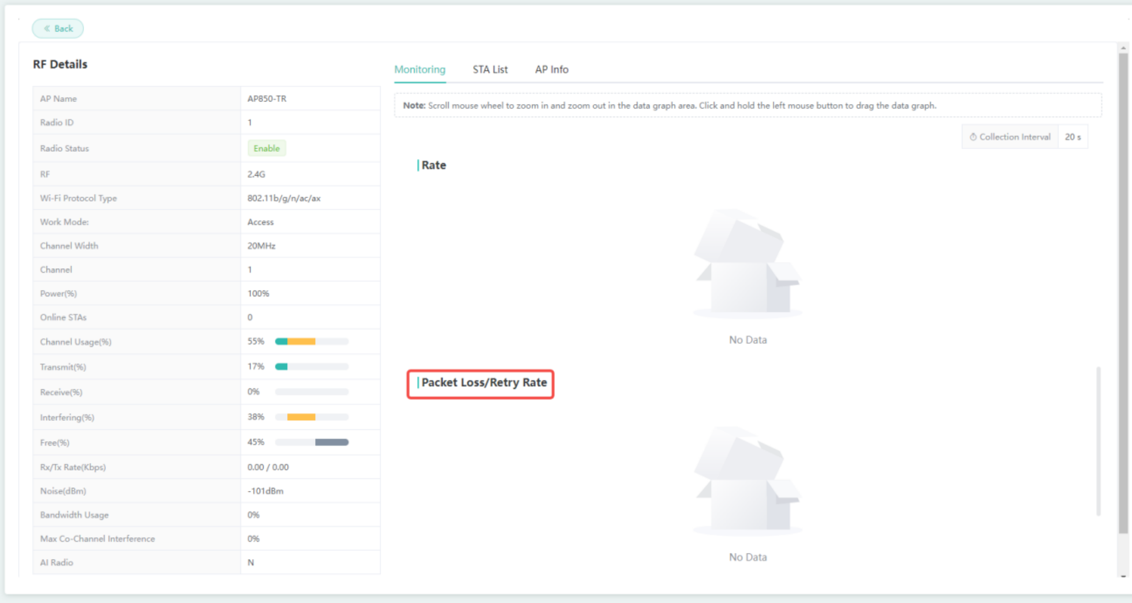


RF Details

AP Name	AP850-TR
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n/ac/ax
Work Mode:	Access
Channel Width	20MHz
Channel	1
Power(%)	100%
Online STAs	0
Channel Usage(%)	55%
Transmit(%)	17%
Receive(%)	0%
Interfering(%)	38%
Free(%)	45%
Rx/Tx Rate(Kbps)	0.00 / 0.00
Noise(dBm)	-101dBm
Bandwidth Usage	0%
Max Co-Channel Interference	0%
AI Radio	N

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

Collection Interval 20 s



RF Details

AP Name	AP850-TR
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n/ac/ax
Work Mode:	Access
Channel Width	20MHz
Channel	1
Power(%)	100%
Online STAs	0
Channel Usage(%)	55%
Transmit(%)	17%
Receive(%)	0%
Interfering(%)	38%
Free(%)	45%
Rx/Tx Rate(Kbps)	0.00 / 0.00
Noise(dBm)	-101dBm
Bandwidth Usage	0%
Max Co-Channel Interference	0%
AI Radio	N

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

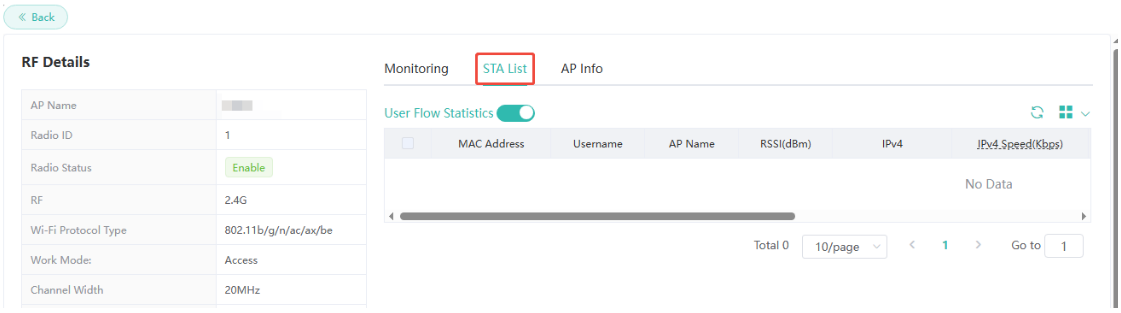
Collection Interval 20 s

Note

When high-frequency telemetry is enabled for a radio, data is collected based on the **Acquisition Cycle** configured on the **RF** > **High Frequency Telemetry Config for RF Data Collection** page.

3. STA List

On the **STA List** tab page, check online STAs on the current radio.



RF Details

AP Name	
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n/ac/ax/be
Work Mode:	Access
Channel Width	20MHz

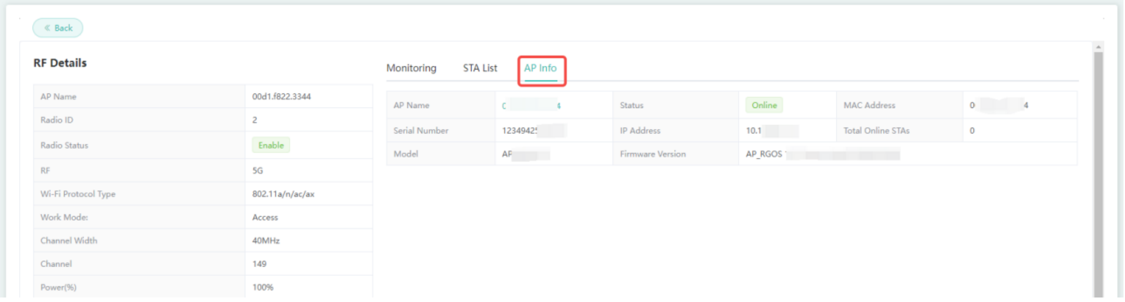
□	MAC Address	Username	AP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)

No Data

Total 0 10/page ‹ 1 › Go to 1

4. AP Info

On the **AP Info** tab page, check the name, status, MAC address, SN, and other information about the AP to which the current radio belongs.



RF Details

AP Name	00d1.f822.3344
Radio ID	2
Radio Status	Enable
RF	5G
Wi-Fi Protocol Type	802.11a/n/ac/ax
Work Mode:	Access
Channel Width	40MHz
Channel	149
Power(%)	100%

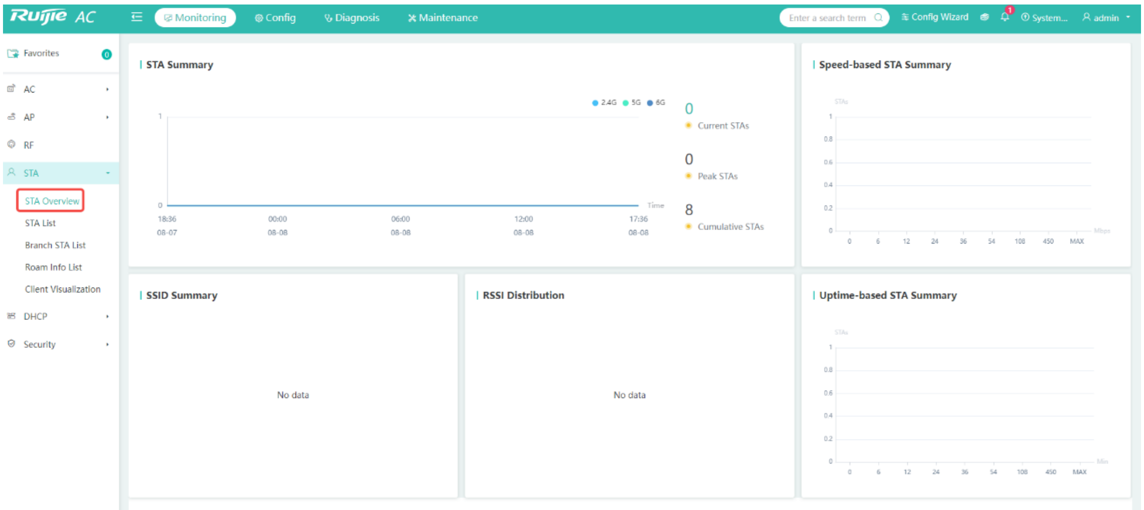
AP Name	C 4	Status	Online	MAC Address	0 4
Serial Number	12349425	IP Address	10.1	Total Online STAs	0
Model	AF	Firmware Version	AP_RGOS		

4.4 STA

4.4.1 Overview

Choose **Monitoring** > **STA** > **STA Overview**.

This page presents STA statistics from various perspectives, updated at an interval of 30s.



0 Current STAs

0 Peak STAs

8 Cumulative STAs

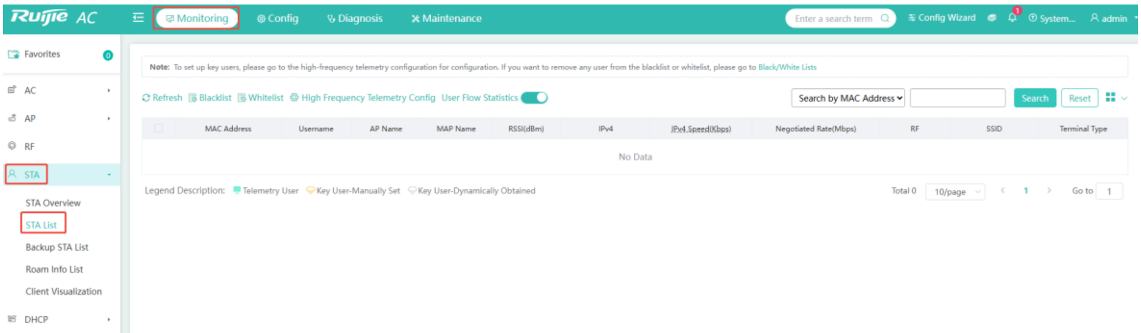
No data

No data

Page Name	Description
STA Summary	Displays the summaries of STAs associated with 2.5 GHz, 5 GHz and 6 GHz Wi-Fi respectively. Current STAs: Displays the number of current online STAs. Peak STAs: Displays the maximum number of online STAs within 24 hours. Cumulative STAs: Displays the cumulative number of online STAs within 24 hours. (The STAs that log in multiple times are counted only once.)
Speed-based STA Summary	Displays the speed-based STA summary in a bar chart. Click the bar to redirect to the STA list.
SSID Summary	Displays the proportion of STAs associated with different Wi-Fi networks. Click the pie chart to redirect to the STA list.
RSSI Distribution	Displays the proportions of STAs' RSSIs.
Uptime-based STA Summary	Displays the uptime-based STA summary in a bar chart. Click the bar to redirect to the STA list.

4.4.2 STA List

Choose **Monitoring** > **STA** > **STA List**.



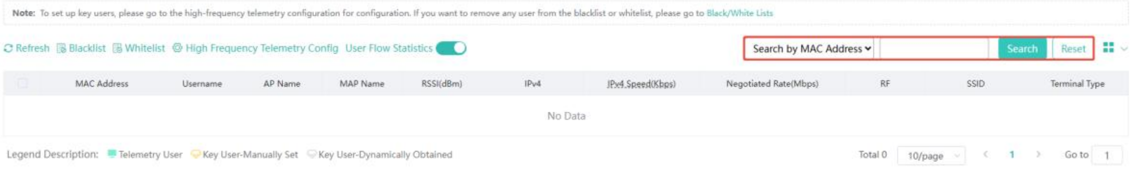
Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

□	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
					No Data						

Legend Description: Telemetry User Key User-Manually Set Key User-Dynamically Obtained

1. Searching for STAs

Enter keywords in the search bar and click **Search**. Click **Reset** to clear the search criteria and display the list of all STAs.

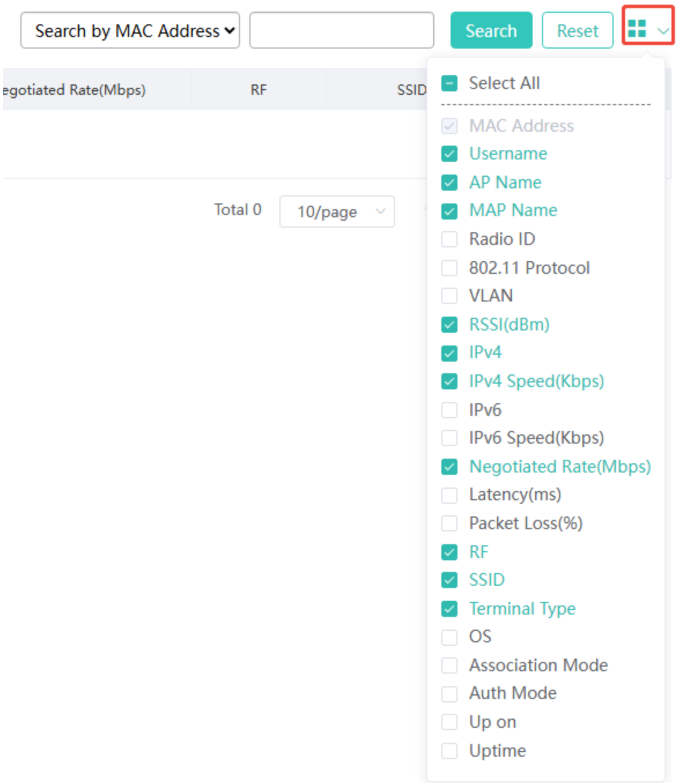


Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

□	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
					No Data						

Legend Description: Telemetry User Key User-Manually Set Key User-Dynamically Obtained

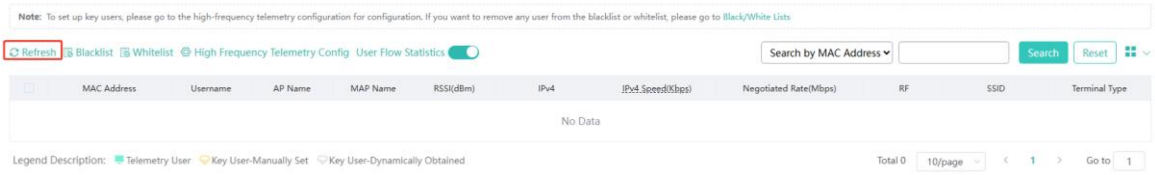
To display additional information about the STAs listed, click ▦ and select the information you wish to view.



- ▣ Select All
- ☑ MAC Address
- ☑ Username
- ☑ AP Name
- ☑ MAP Name
- □ Radio ID
- □ 802.11 Protocol
- □ VLAN
- ☑ RSSI(dBm)
- ☑ IPv4
- ☑ IPv4 Speed(Kbps)
- □ IPv6
- □ IPv6 Speed(Kbps)
- ☑ Negotiated Rate(Mbps)
- □ Latency(ms)
- □ Packet Loss(%)
- ☑ RF
- ☑ SSID
- ☑ Terminal Type
- □ OS
- □ Association Mode
- □ Auth Mode
- □ Up on
- □ Uptime

2. Refreshing STAs

Click **Refresh** to reload the list of STAs and ensure that the latest information is displayed.

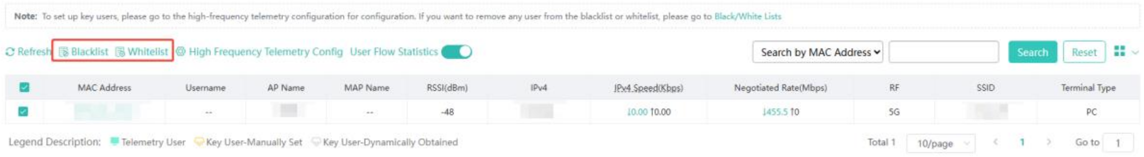

Refresh
Blacklist
Whitelist
High Frequency Telemetry Config
User Flow Statistics
Search by MAC Address
Search
Reset
Legend Description: Telemetry User Key User-Manually Set Key User-Dynamically Obtained
Total 0
10/page
1
Go to 1

Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

□	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
No Data											

3. Adding to the Blacklist or Whitelist

Select the STAs you want to add to the blacklist or whitelist and click **Blacklist** or **Whitelist**.


Refresh
Blacklist
Whitelist
High Frequency Telemetry Config
User Flow Statistics
Search by MAC Address
Search
Reset
Legend Description: Telemetry User Key User-Manually Set Key User-Dynamically Obtained
Total 1
10/page
1
Go to 1

Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

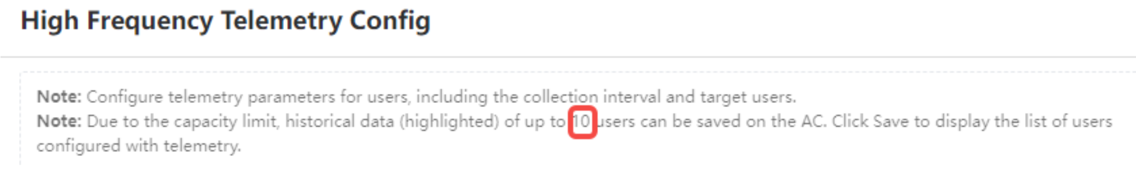
☑	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
☑	[redacted]	--	[redacted]	--	-48	[redacted]	↓0.00 ↑0.00	↓455.5 ↑0	5G	[redacted]	PC

4. High-Frequency Telemetry Config

Click **High Frequency Telemetry Config** to access the **High Frequency Telemetry Config** dialog box where you can set **Acquisition Cycle** and **Collection Object**.

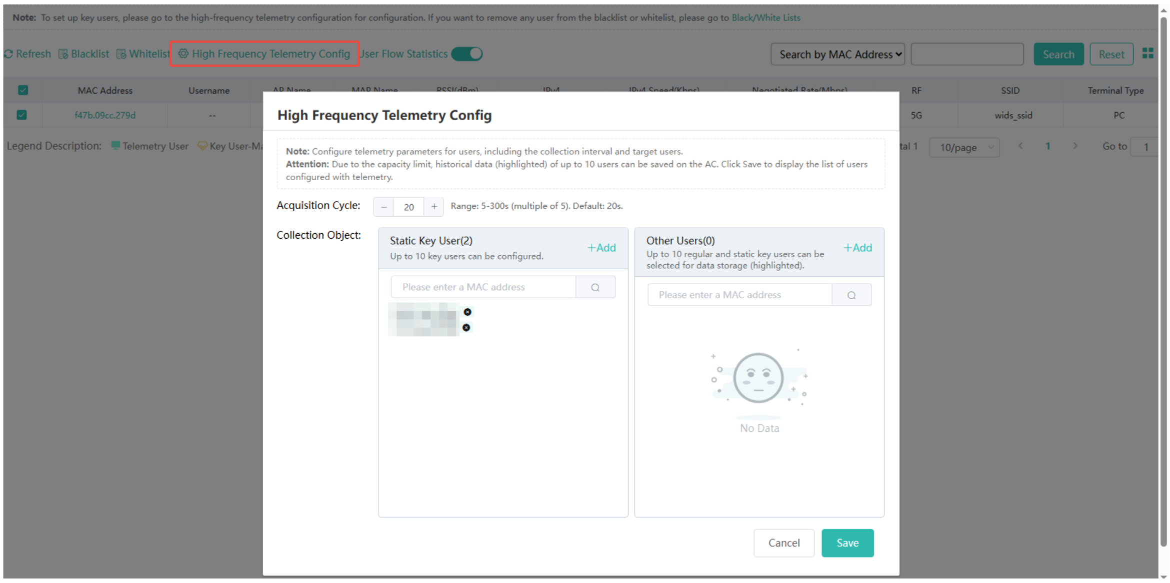
Note

- Due to the AC capacity limitation, historical data of only STAs newly added for high-frequency telemetry (highlighted in the **Selected** pane on the right) will be stored on the AC. For STAs that are not highlighted, only data collection is enabled, but the collected data is not stored on the AC.
- The capacity limit of an AC varies with the AC model. Therefore, the number of STAs for which historical data can be stored on an AC varies. For details about the number of STAs that can be stored, check the prompt on the web UI.



High Frequency Telemetry Config

Note: Configure telemetry parameters for users, including the collection interval and target users.
Note: Due to the capacity limit, historical data (highlighted) of up to 10 users can be saved on the AC. Click Save to display the list of users configured with telemetry.



Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

☑	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
☑	f47b.09cc.279d	--							5G	wids_ssid	PC

Legend Description: Telemetry User Key User-M...

High Frequency Telemetry Config

Note: Configure telemetry parameters for users, including the collection interval and target users.
Attention: Due to the capacity limit, historical data (highlighted) of up to 10 users can be saved on the AC. Click Save to display the list of users configured with telemetry.

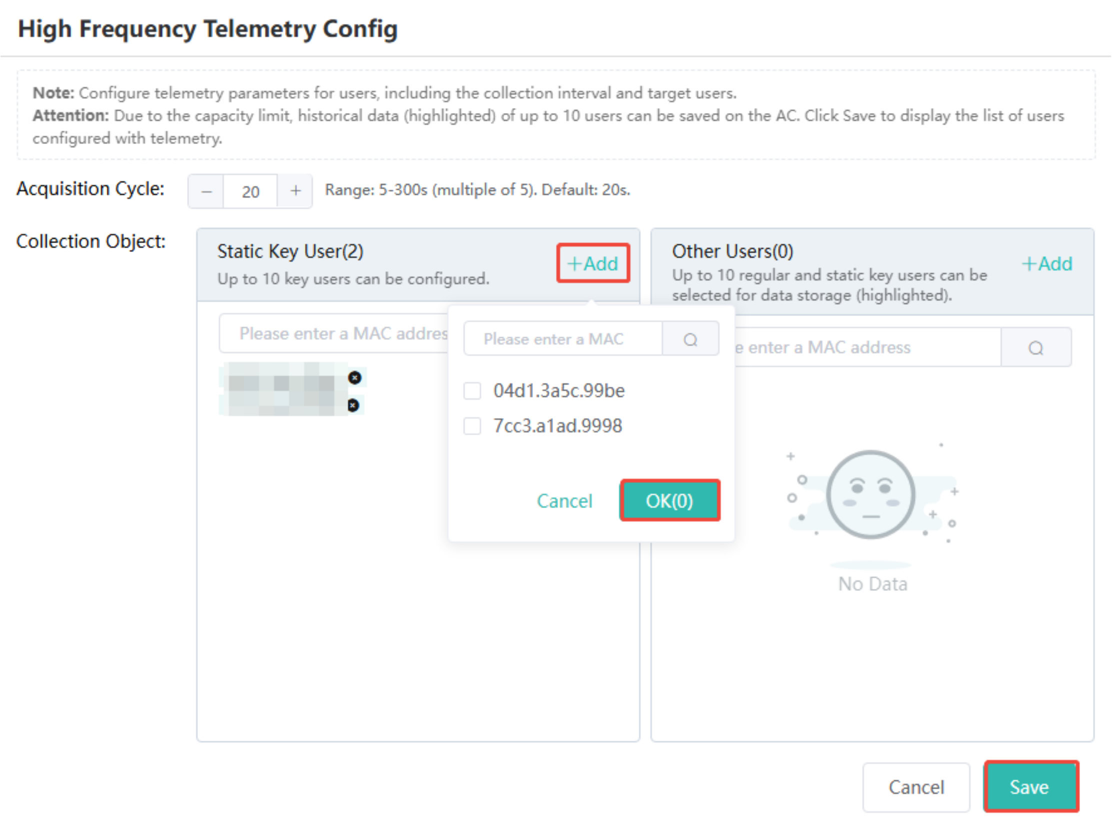
Acquisition Cycle: – 20 + Range: 5-300s (multiple of 5). Default: 20s.

Collection Object:

Static Key User(2) +Add
Up to 10 key users can be configured.
Please enter a MAC address
[redacted]

Other Users(0) +Add
Up to 10 regular and static key users can be selected for data storage (highlighted).
Please enter a MAC address
No Data

Click **Add**, select the STAs that you want to add, and then click **OK(*number*)**, *number* indicating the number of added STAs. After all the collection objects are added, click **Save**. After successful setting, you can view the list of STAs configured with high frequency telemetry and the user status.



High Frequency Telemetry Config

Note: Configure telemetry parameters for users, including the collection interval and target users.
Attention: Due to the capacity limit, historical data (highlighted) of up to 10 users can be saved on the AC. Click Save to display the list of users configured with telemetry.

Acquisition Cycle: – 20 + Range: 5-300s (multiple of 5). Default: 20s.

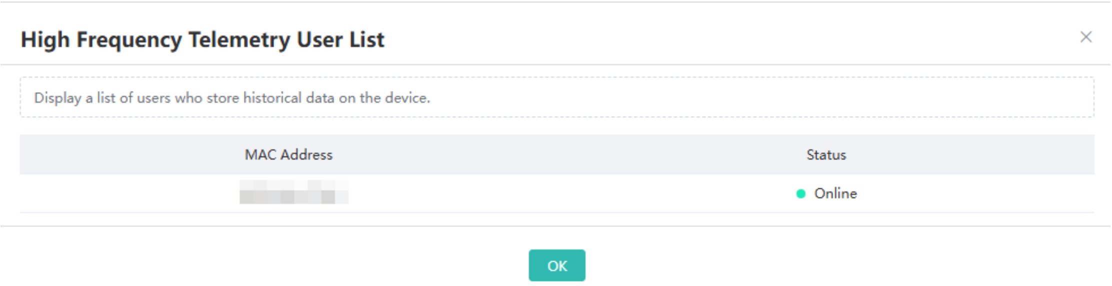
Collection Object:

Static Key User(2) +Add
Up to 10 key users can be configured.
Please enter a MAC address
[redacted]

Please enter a MAC
□ 04d1.3a5c.99be
□ 7cc3.a1ad.9998
Cancel OK(0)

Other Users(0) +Add
Up to 10 regular and static key users can be selected for data storage (highlighted).
Please enter a MAC address
No Data

Cancel Save



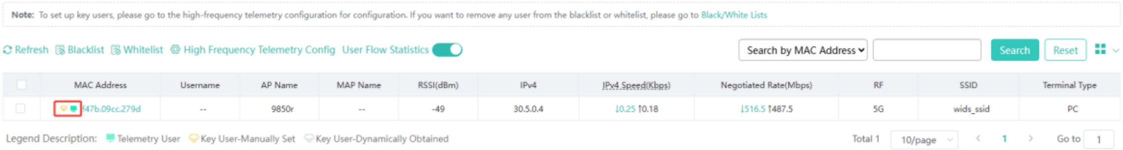
High Frequency Telemetry User List

Display a list of users who store historical data on the device.

MAC Address	Status
[redacted]	● Online

OK

Click **OK** to return to the **STA List** page. In the list, STAs with the 🟩 icon in the **MAC Address** column are configured with high frequency telemetry, with the ♡ icon are static key STAs, and with the ♡ icon are dynamic key STAs.



Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

Refresh Blacklist Whitelist High Frequency Telemetry Config User Flow Statistics Search by MAC Address Search Reset

□	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
□	♡ 🟩 f47b.09cc.279d	--	9850r	--	-49	30.5.0.4	↓0.25 ↑0.18	↓516.5 ↑487.5	5G	wids_ssid	PC

Legend Description: 🟩 Telemetry User ♡ Key User-Manually Set ♡ Key User-Dynamically Obtained

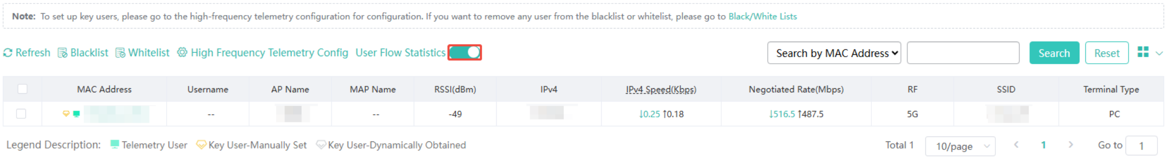
Total 1 10/page < 1 > Go to 1

5. User Flow Statistics

Enable or disable user flow statistics collection on STAs connecting to the device by toggling the switch. Data is available in the **IPv4** column only after the user flow statistics feature is enabled. Otherwise, data in the IPv4 column is always 0.

Caution

Enabling user flow statistics will reduce the AP forwarding performance.



Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

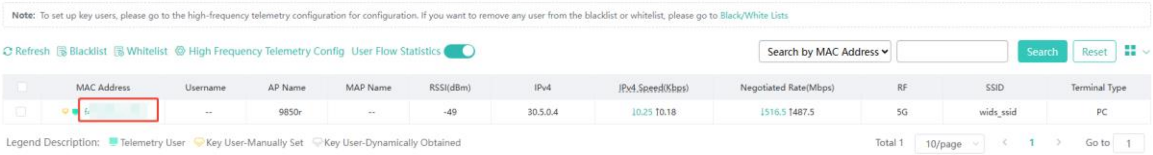
□	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
□	[redacted]	--	[redacted]	--	-49	[redacted]	↓0.25 ↑0.18	↓516.5 ↑487.5	5G	[redacted]	PC

Legend Description: 🟩 Telemetry User ♡ Key User-Manually Set ♡ Key User-Dynamically Obtained

Total 1 10/page < 1 > Go to 1

6. Viewing STA Details

Click the MAC address of the STA to redirect to the STA page. The **Client Details** page displays the client network information, STA topology, **Client Info**, **Speed Tendency**, **RSSI**, **Packet Loss Rate(%)**, **Client History**, **Link Detection**, and **App Experience Metrics**.



Note: To set up key users, please go to the high-frequency telemetry configuration for configuration. If you want to remove any user from the blacklist or whitelist, please go to Black/White Lists

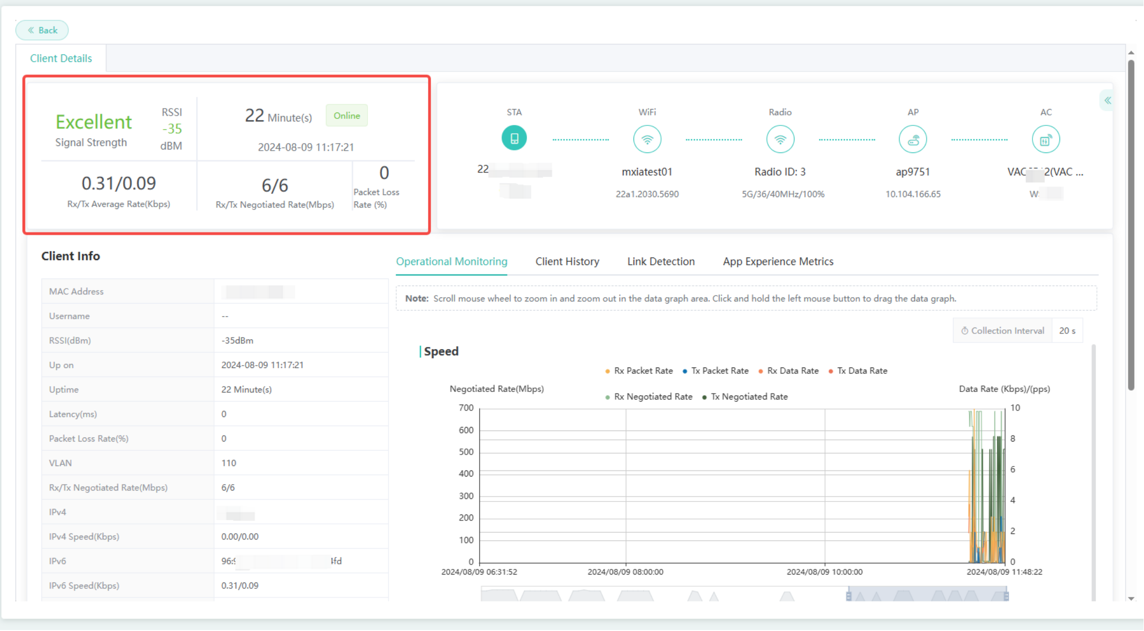
□	MAC Address	Username	AP Name	MAP Name	RSSI(dBm)	IPv4	IPv4 Speed(Kbps)	Negotiated Rate(Mbps)	RF	SSID	Terminal Type
□	f[redacted]	--	9850r	--	-49	30.5.0.4	↓0.25 ↑0.18	↓516.5 ↑487.5	5G	wids_ssid	PC

Legend Description: 🟩 Telemetry User ♡ Key User-Manually Set ♡ Key User-Dynamically Obtained

Total 1 10/page < 1 > Go to 1

(1) Client Network Information

In the upper left corner of the **Client Details** page, you can view the signal quality, online duration, **Rx/Tx Average Rate(Kbps)**, **Rx/Tx Negotiated Rate(Mbps)**, and **Packet Loss Rate (%)**.



Excellent Signal Strength

RSSI -35 dBM

22 Minute(s) Online

2024-08-09 11:17:21

0.31/0.09 Rx/Tx Average Rate(Kbps)

6/6 Rx/Tx Negotiated Rate(Mbps)

0 Packet Loss Rate (%)

22[redacted]

mxiatest01 22a1.2030.5690

Radio ID: 3 5G/36/40MHz/100%

ap9751 10.104.166.65

VAC[redacted]2(VAC ... W[redacted]

Client Info

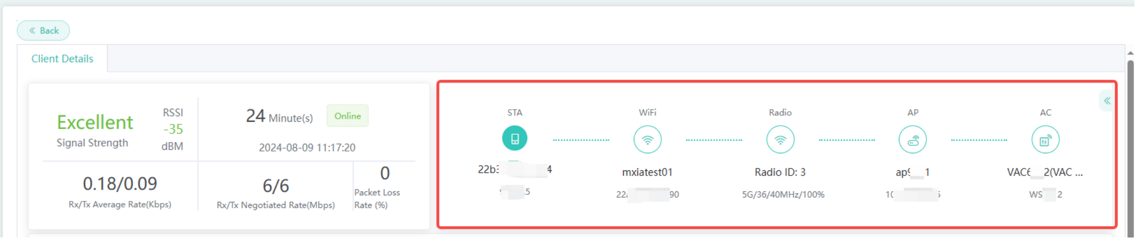
MAC Address	[redacted]
Username	--
RSSI(dBm)	-35dBm
Up on	2024-08-09 11:17:21
Uptime	22 Minute(s)
Latency(ms)	0
Packet Loss Rate(%)	0
VLAN	110
Rx/Tx Negotiated Rate(Mbps)	6/6
IPv4	[redacted]
IPv4 Speed(Kbps)	0.00/0.00
IPv6	96:[redacted]4fd
IPv6 Speed(Kbps)	0.31/0.09

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

Collection Interval 20 s

(2) STA Topology

In the upper right corner of the **Client Details** page, you can view the topology, including the SSID, radio ID, and the AP and AC associated with the client.



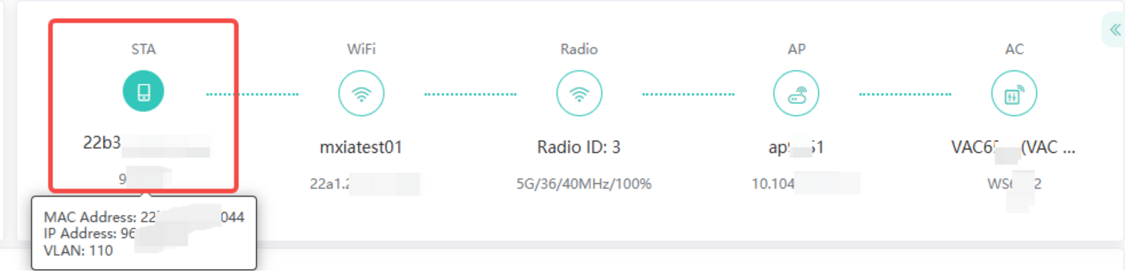
« Back

Client Details

Excellent Signal Strength	RSSI -35 dBM
24 Minute(s) Online	2024-08-09 11:17:20
0.18/0.09	Rx/Tx Average Rate(Kbps)
6/6	Rx/Tx Negotiated Rate(Mbps)
0	Packet Loss Rate (%)

STA	WiFi	Radio	AP	AC
22b[redacted]4	mxiatest01	Radio ID: 3	ap[redacted]1	VAC6[redacted]2(VAC ...
[redacted]5	22[redacted]90	5G/36/40MHz/100%	1[redacted]	WS[redacted]2

Move the cursor to a client in the topology to view detailed information about the client.

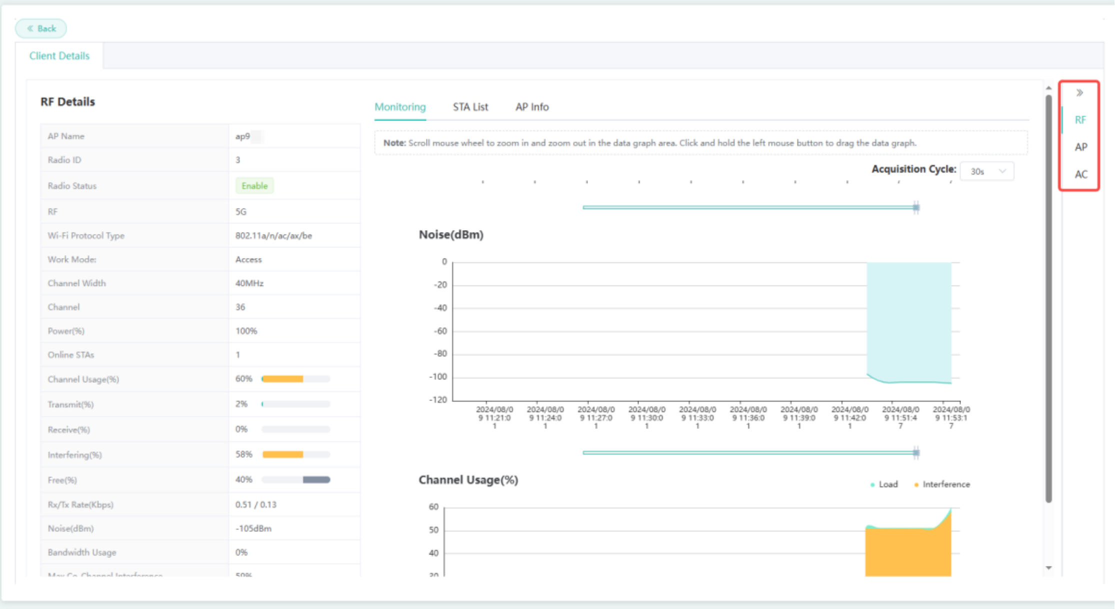


STA	WiFi	Radio	AP	AC
22b3[redacted]	mxiatest01	Radio ID: 3	ap[redacted]1	VAC6[redacted](VAC ...
9[redacted]	22a1.[redacted]	5G/36/40MHz/100%	10.104[redacted]	WS[redacted]2

MAC Address: 22[redacted]044
IP Address: 9[redacted]
VLAN: 110

Click « in the upper right corner of the topology to view the details about the radio, AP, and AC associated with the STA.

- Details about the radio associated with the client:



« Back

Client Details

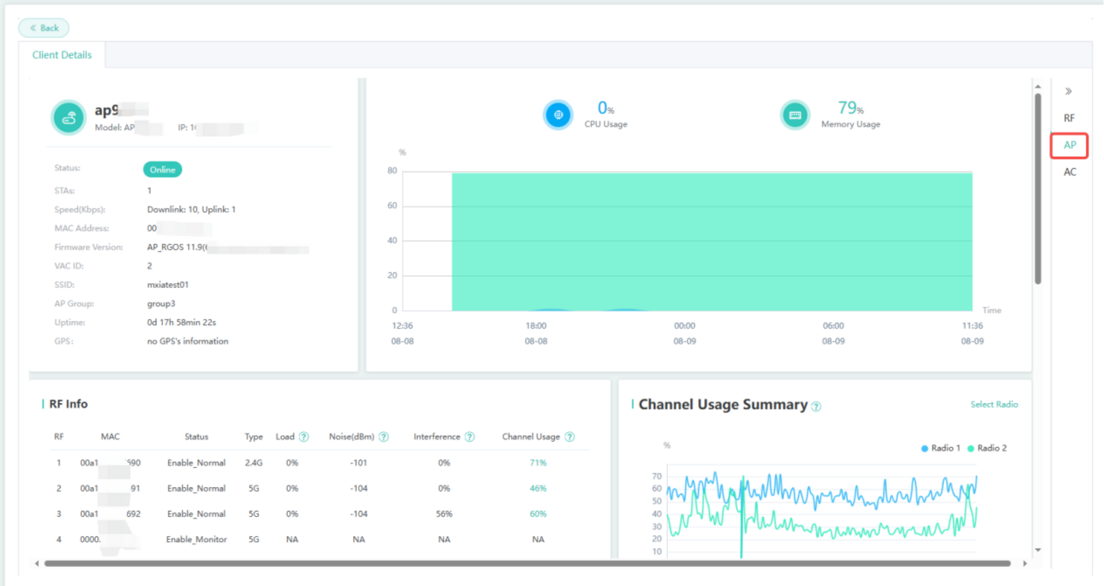
RF Details

AP Name	ap9[redacted]
Radio ID	3
Radio Status	Enable
RF	5G
Wi-Fi Protocol Type	802.11a/n/ac/ax/be
Work Mode:	Access
Channel Width	40MHz
Channel	36
Power(%)	100%
Online STAs	1
Channel Usage(%)	60%
Transmit(%)	2%
Receive(%)	0%
Interfering(%)	58%
Free(%)	40%
Rx/Tx Rate(Kbps)	0.51 / 0.13
Noise(dBm)	-105dBm
Bandwidth Usage	0%
Max Co-Channel Interference	50%

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

Acquisition Cycle: 30s

- Details about the AP associated with the client:



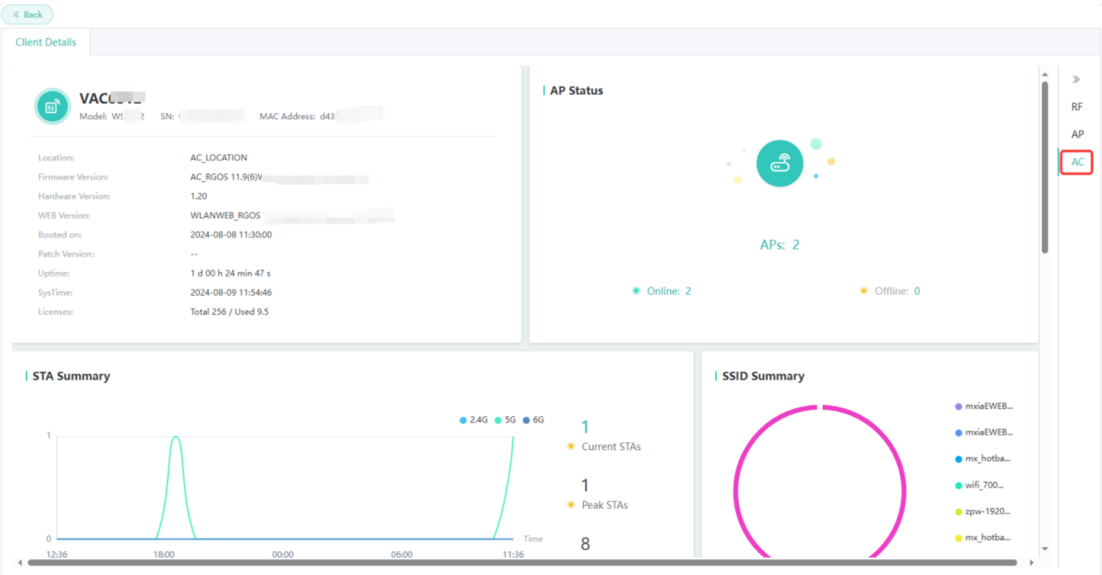
ap9[redacted]
Model: AP[redacted] IP: 1[redacted]

Status:	Online
STAs:	1
Speed(Kbps):	Downlink: 10, Uplink: 1
MAC Address:	00[redacted]
Firmware Version:	AP_RGOS 11.9([redacted]
VAC ID:	2
SSID:	mxiatest01
AP Group:	group3
Uptime:	0d 17h 58min 22s
GPS:	no GPS's information

RF Info

RF	MAC	Status	Type	Load	Noise(dBm)	Interference	Channel Usage
1	00a1[redacted]590	Enable_Normal	2.4G	0%	-101	0%	71%
2	00a1[redacted]91	Enable_Normal	5G	0%	-104	0%	46%
3	00a1[redacted]692	Enable_Normal	5G	0%	-104	56%	60%
4	0000.[redacted]	Enable_Monitor	5G	NA	NA	NA	NA

- Details about the AC associated with the client:

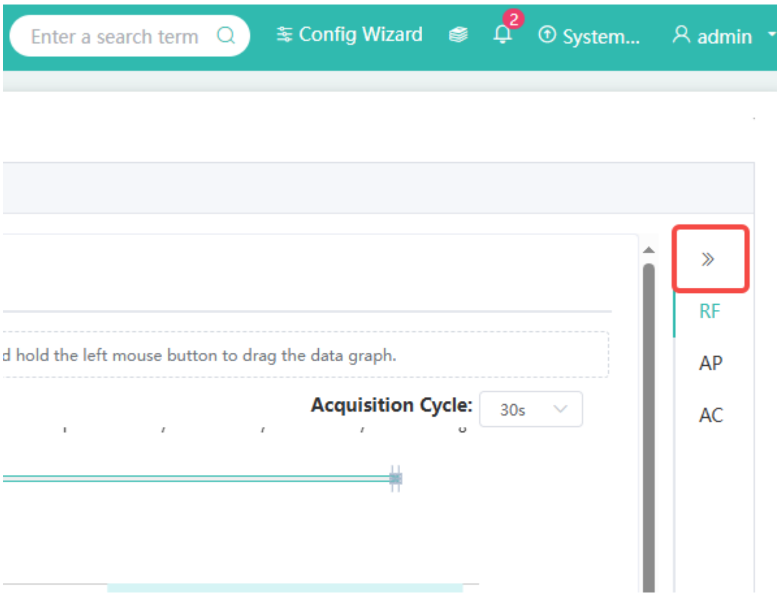


VAC[redacted]
Model: WS[redacted]2 SN: [redacted] MAC Address: d43[redacted]

Location:	AC_LOCATION
Firmware Version:	AC_RGOS 11.9(6)W[redacted]
Hardware Version:	1.20
WEB Version:	WLANWEB_RGOS [redacted]
Booted on:	2024-08-08 11:30:00
Patch Version:	--
Uptime:	1 d 00 h 24 min 47 s
SysTime:	2024-08-09 11:54:46
Licenses:	Total 256 / Used 9.5

1
Current STAs
1
Peak STAs
8

Click » to exit the details page and return to the **Client Details** page.

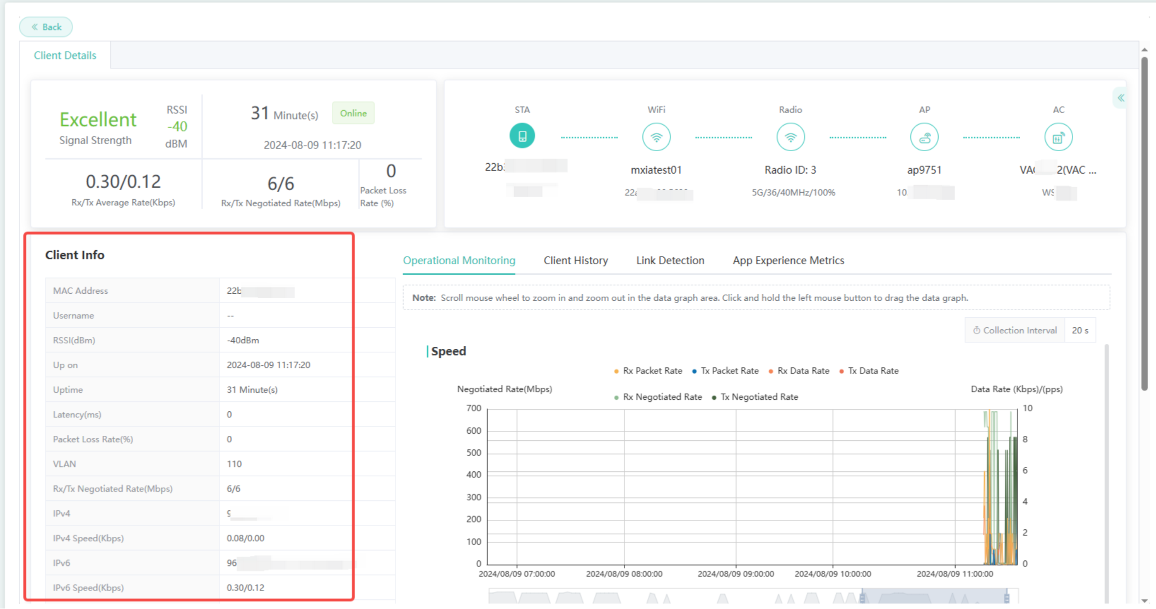


d hold the left mouse button to drag the data graph.

Acquisition Cycle: 30s

(3) Client Info

In the lower left corner of the **Client Details** page, you can view details of the client.



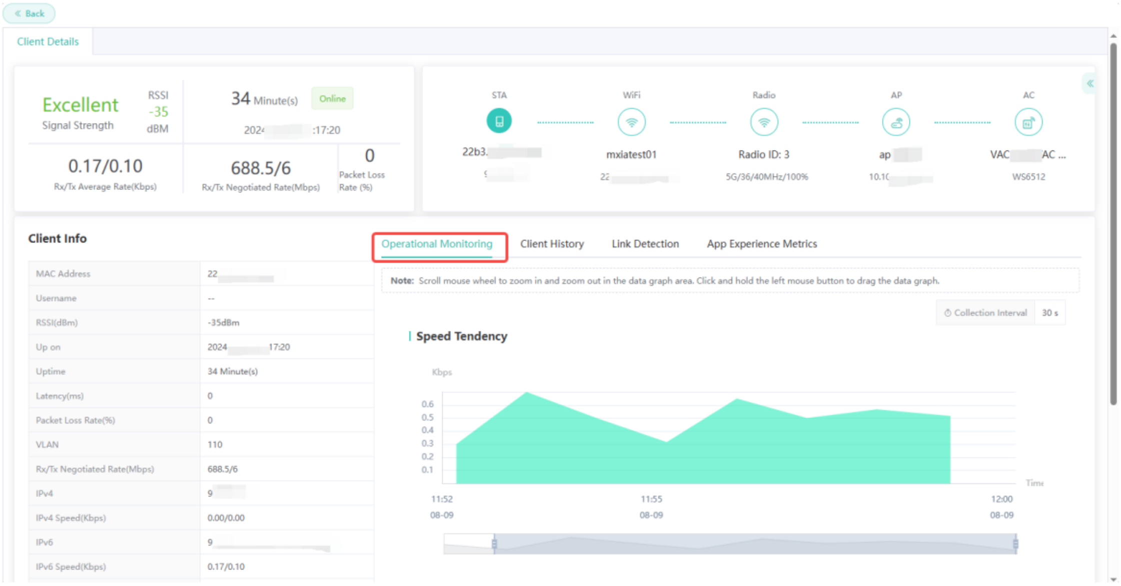
Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

Client Info

MAC Address	22b
Username	--
RSSI(dBm)	-40dBm
Up on	2024-08-09 11:17:20
Uptime	31 Minute(s)
Latency(ms)	0
Packet Loss Rate(%)	0
VLAN	110
Rx/Tx Negotiated Rate(Mbps)	6/6
IPv4	9
IPv4 Speed(Kbps)	0.08/0.00
IPv6	96
IPv6 Speed(Kbps)	0.30/0.12

(4) Operational Monitoring

- If the client is not enabled with high-frequency telemetry, the **Operational Monitoring** tab page displays the **Speed Tendency** graph of the client.



Excellent Signal Strength

RSSI -35 dBM

34 Minute(s) Online

2024 [redacted] :17:20

0.17/0.10 Rx/Tx Average Rate(Kbps)

688.5/6 Rx/Tx Negotiated Rate(Mbps)

0 Packet Loss Rate (%)

22b3. [redacted]

mxiatest01

22 [redacted]

Radio ID: 3

5G/36/40MHz/100%

ap [redacted]

10.10 [redacted]

VAC [redacted] AC ...

WS6512

Client Info

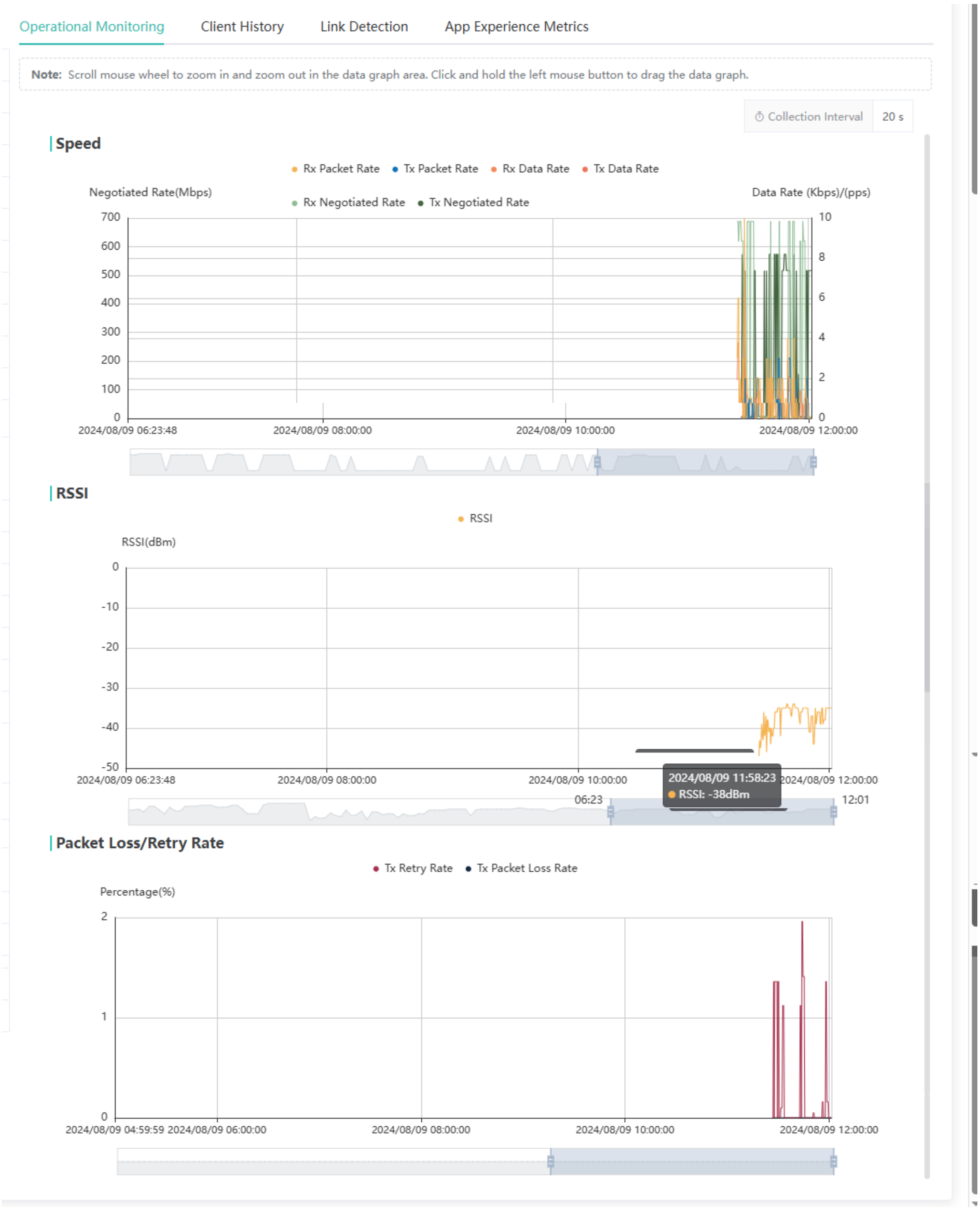
MAC Address	22 [redacted]
Username	--
RSSI(dBm)	-35dBm
Up on	2024 [redacted] 17:20
Uptime	34 Minute(s)
Latency(ms)	0
Packet Loss Rate(%)	0
VLAN	110
Rx/Tx Negotiated Rate(Mbps)	688.5/6
IPv4	9 [redacted]
IPv4 Speed(Kbps)	0.00/0.00
IPv6	9 [redacted]
IPv6 Speed(Kbps)	0.17/0.10

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

Collection Interval 30 s

Speed Tendency

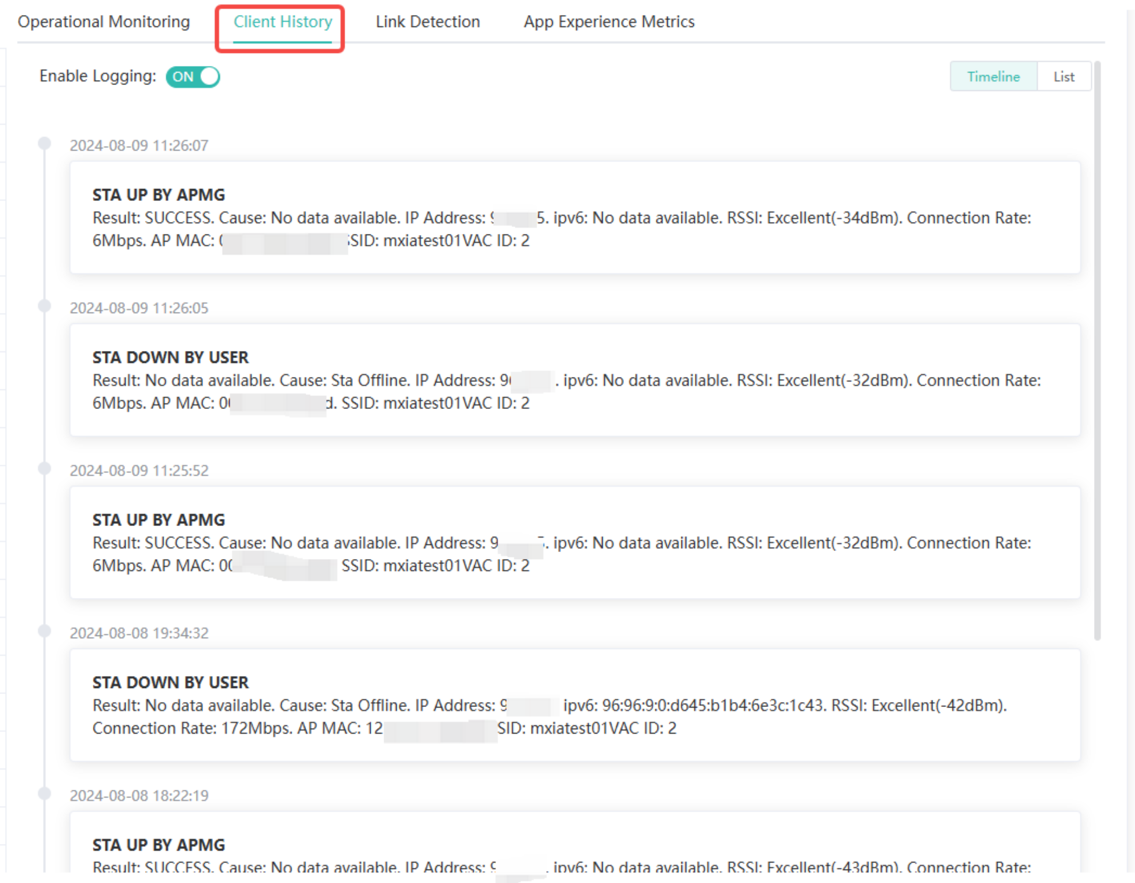
- If the client is enabled with high-frequency telemetry and is in telemetry state, the **Operational Monitoring** tab page displays the **Speed**, **RSSI**, and **Packet Loss/Retry Rate** trend graphs of the client.



Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

(5) Client History

View the login and logout records of clients.



Enable Logging: ON

2024-08-09 11:26:07

STA UP BY APMG
Result: SUCCESS. Cause: No data available. IP Address: [redacted]5. ipv6: No data available. RSSI: Excellent(-34dBm). Connection Rate: 6Mbps. AP MAC: [redacted]SID: mxiatest01VAC ID: 2

2024-08-09 11:26:05

STA DOWN BY USER
Result: No data available. Cause: Sta Offline. IP Address: 9[redacted]. ipv6: No data available. RSSI: Excellent(-32dBm). Connection Rate: 6Mbps. AP MAC: 0[redacted]d. SSID: mxiatest01VAC ID: 2

2024-08-09 11:25:52

STA UP BY APMG
Result: SUCCESS. Cause: No data available. IP Address: 9[redacted]. ipv6: No data available. RSSI: Excellent(-32dBm). Connection Rate: 6Mbps. AP MAC: 0[redacted] SSID: mxiatest01VAC ID: 2

2024-08-08 19:34:32

STA DOWN BY USER
Result: No data available. Cause: Sta Offline. IP Address: [redacted] ipv6: 96:96:9:0:d645:b1b4:6e3c:1c43. RSSI: Excellent(-42dBm). Connection Rate: 172Mbps. AP MAC: 12[redacted]SID: mxiatest01VAC ID: 2

2024-08-08 18:22:19

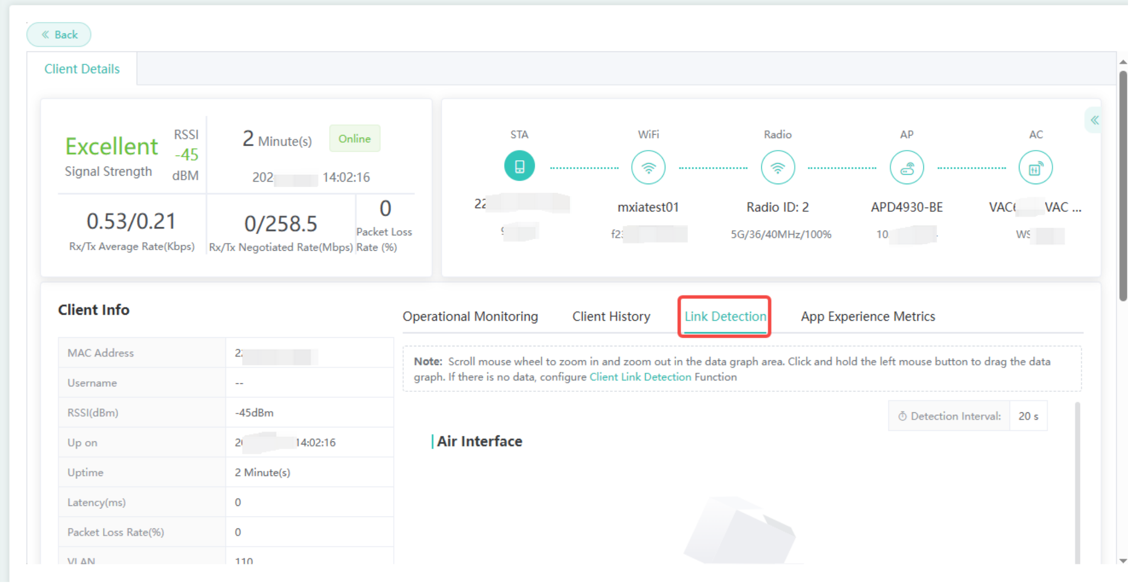
STA UP BY APMG
Result: SUCCESS. Cause: No data available. IP Address: [redacted]. ipv6: No data available. RSSI: Excellent(-43dBm). Connection Rate:

(6) Link Detection

If the client is configured for link detection, the **Link Detection** tab page displays the **Air Interface**, **Gateway**, **DHCP**, DNS packet loss rate, minimum latency, average latency, and maximum latency trend graphs. If the client is not configured for link detection, no client information is displayed on the **Link Detection** tab page.

Note

The display of the air interface, gateway, DHCP, and DNS information depends on whether a detection item is configured. To configure a detection item, choose **Diagnosis** > **STA Teach** > **WLAN-Sta-Link Check** > **Parameter Config**. Click **Client Link Detection** to view or configure link detection data of a client. For details, see STA Link Detection.



MAC Address	2[redacted]
Username	--
RSSI(dBm)	-45dBm
Up on	2[redacted] 14:02:16
Uptime	2 Minute(s)
Latency(ms)	0
Packet Loss Rate(%)	0
VLAN	110

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph. If there is no data, configure Client Link Detection Function

Detection Interval: 20 s

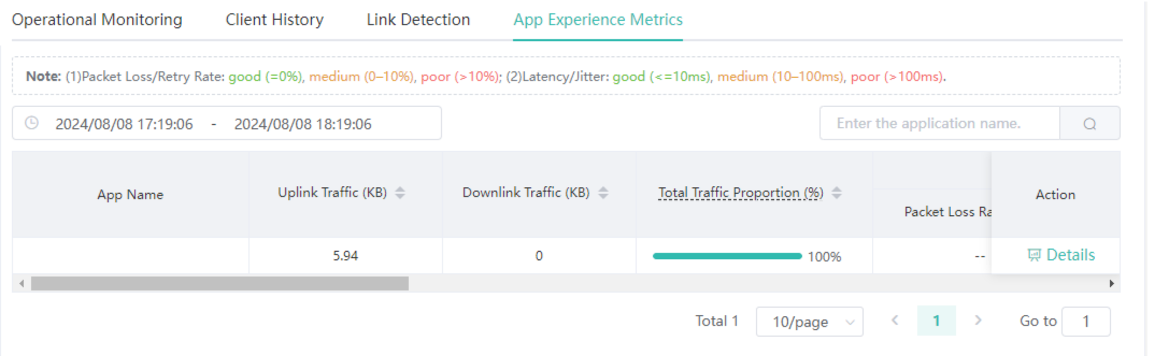
Air Interface

(7) App Experience Metrics

The **App Experience Metrics** tab page displays traffic usage by application. The list of applications used by a client within the last one hour is displayed by default (the time range can be customized).

Note

The **App Experience Metrics** tab page displays only the data of clients with the high-frequency telemetry icon 🖥 on the left of the MAC addresses on the **STA List** page.



Note: (1)Packet Loss/Retry Rate: good (=0%), medium (0–10%), poor (>10%); (2)Latency/Jitter: good (<=10ms), medium (10–100ms), poor (>100ms).

2024/08/08 17:19:06 - 2024/08/08 18:19:06

Enter the application name.

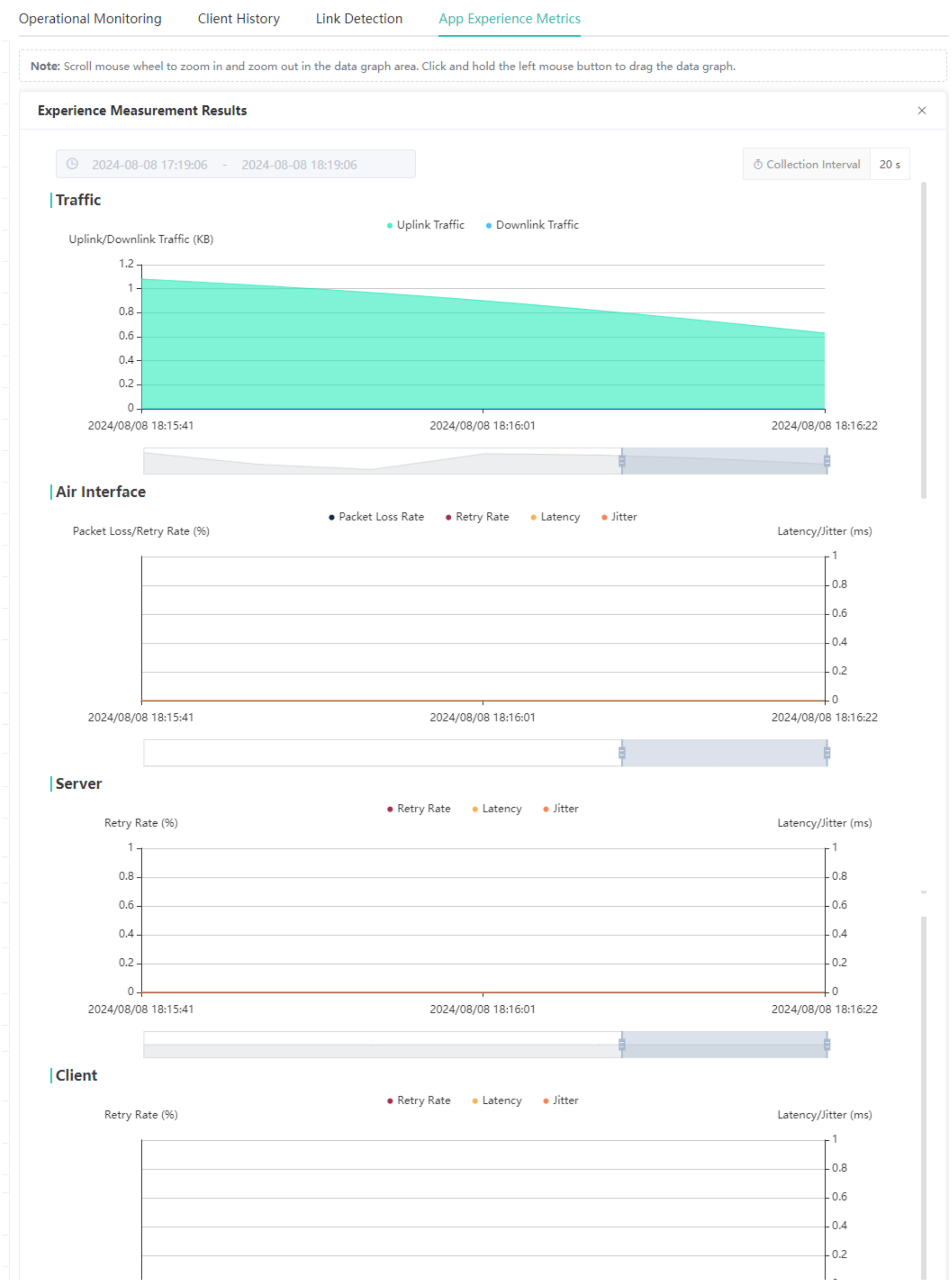
App Name	Uplink Traffic (KB)	Downlink Traffic (KB)	Total Traffic Proportion (%)	Packet Loss Ra	Action
	5.94	0	100%	--	Details

Total 1 10/page < 1 > Go to 1

Parameter	Description
Total Traffic Proportion	Displays the proportion of the total uplink and downlink traffic used by an application to the total traffic within the selected time period.
Server	Displays the latency, packet loss rate, and retransmission rate of Transmission Control Protocol (TCP) packets sent from the AP to the server, calculated based on TCP.

Parameter	Description
STA	Displays the latency, packet loss rate, and retransmission rate of TCP packets sent from the AP to the STA, calculated based on TCP. The calculation model is different from that on air interfaces.
Air Interface	Displays the latency, packet loss rate, and retransmission rate of wireless packets sent from the AP to the STA, calculated based on the traffic sending and receiving on the wireless protocol layer.

Click **Details** of an application to view the traffic trend graph of the application.



Operational Monitoring Client History Link Detection App Experience Metrics

Note: Scroll mouse wheel to zoom in and zoom out in the data graph area. Click and hold the left mouse button to drag the data graph.

Experience Measurement Results

2024-08-08 17:19:06 - 2024-08-08 18:19:06

Collection Interval: 20 s

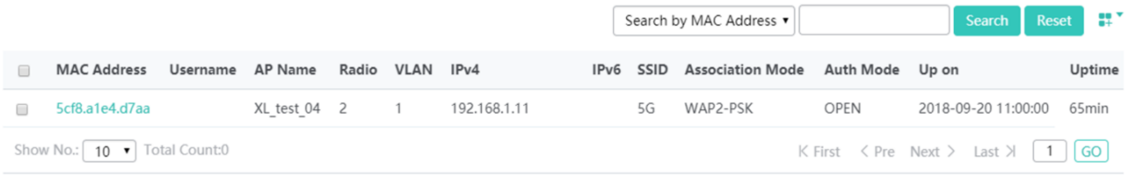
4.4.3 STA List of a Branch AC

Note

This feature is only supported on headquarters ACs.

Choose **Monitoring** > **STA** > **STA List of a Branch AC**.

The **STA List of a Branch AC** displays the basic information of online branch STAs.

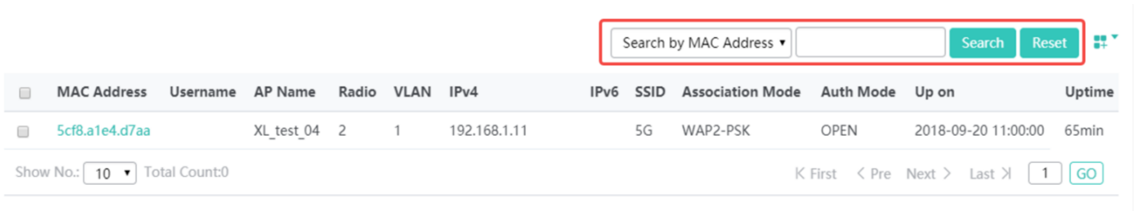


Search by MAC Address ▾ | Search | Reset

□	MAC Address	Username	AP Name	Radio	VLAN	IPv4	IPv6	SSID	Association Mode	Auth Mode	Up on	Uptime
□	5cf8.a1e4.d7aa		XL_test_04	2	1	192.168.1.11		5G	WAP2-PSK	OPEN	2018-09-20 11:00:00	65min

Show No.: 10 ▾ Total Count:0 | K First ‹ Pre Next › Last ›I | 1 | GO

(1) Searching for STAs: If there are a large number of STAs, search for STAs by the MAC address, IP address, authentication mode, and AP name. Enter keywords in the search bar and click **search**. Click **Reset** to clear search criteria.

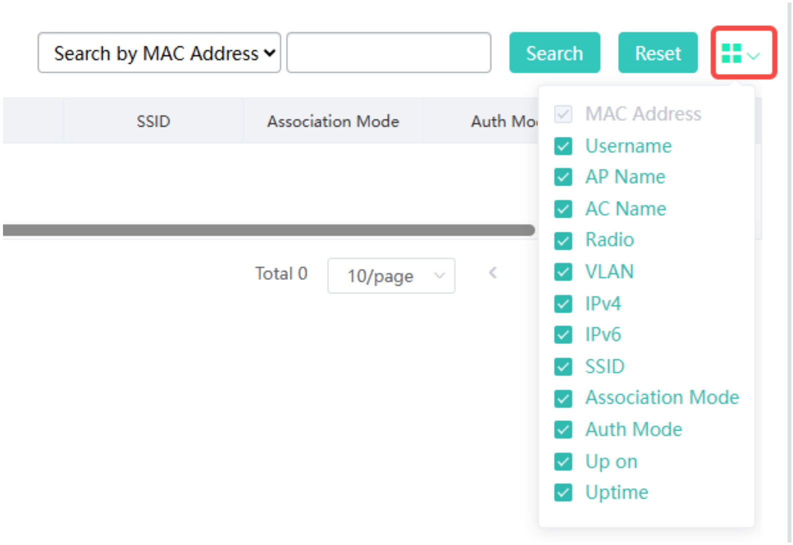


Search by MAC Address ▾ | Search | Reset

□	MAC Address	Username	AP Name	Radio	VLAN	IPv4	IPv6	SSID	Association Mode	Auth Mode	Up on	Uptime
□	5cf8.a1e4.d7aa		XL_test_04	2	1	192.168.1.11		5G	WAP2-PSK	OPEN	2018-09-20 11:00:00	65min

Show No.: 10 ▾ Total Count:0 | K First ‹ Pre Next › Last ›I | 1 | GO

(2) Displaying Information: Click ▦ to select the parameters you want to display. Deselect the parameters if you want to hide them.



4.4.4 Backup STA List

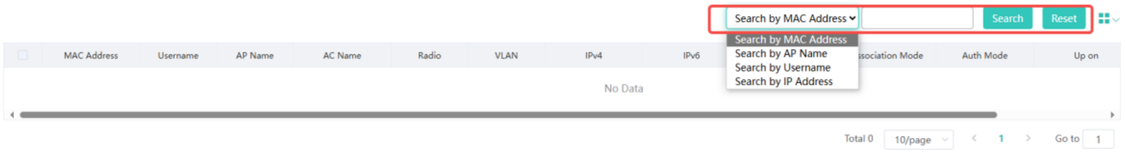
Note

This feature is supported only in AC hot backup scenarios.

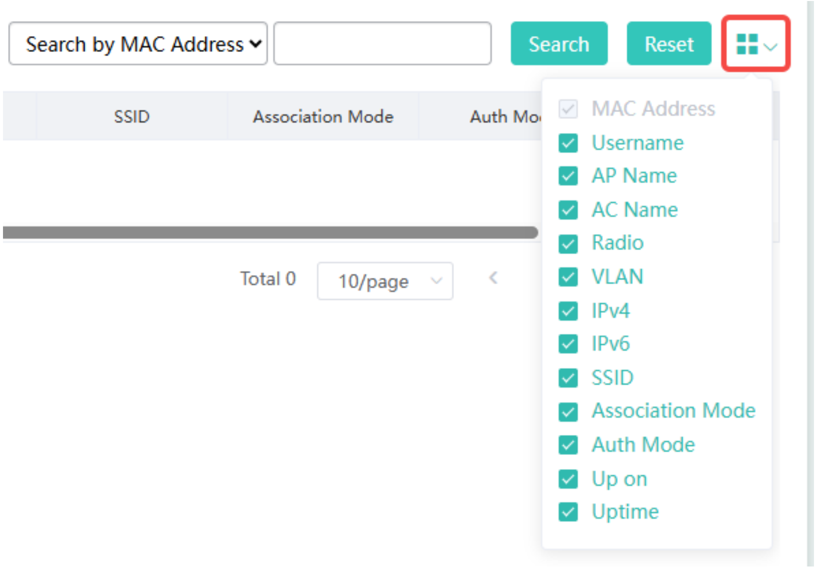
Choose **Monitoring** > **STA** > **Backup STA List**.

The backup STA list displays the basic information of online STAs backed up from the active AC in AC hot standby scenarios.

(1) Searching for APs: If there are a large number of STAs, search for STAs by the MAC address, IP address, authentication mode, and AP name. Enter keywords in the search bar and click **search**. Click **Reset** to clear the search criteria.



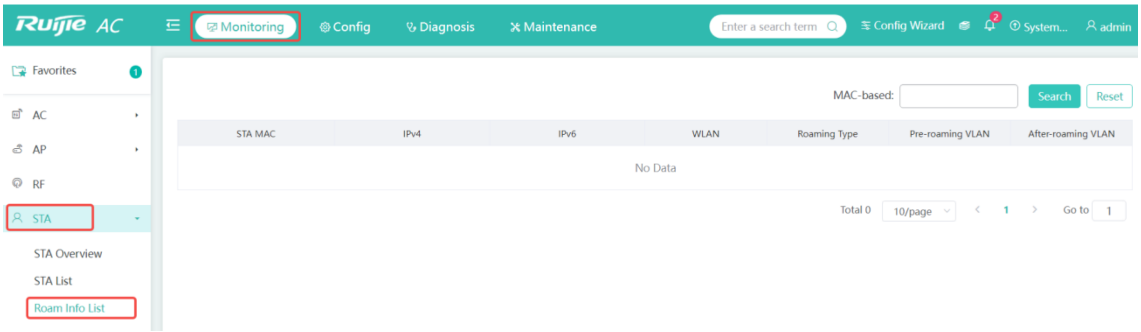
(2) Displaying Information: Click ▦∨ to select the parameters you want to display. Deselect the parameters if you want to hide them.



4.4.5 Roam Info List

Choose **Monitoring** > **STA** > **Roam Info List**.

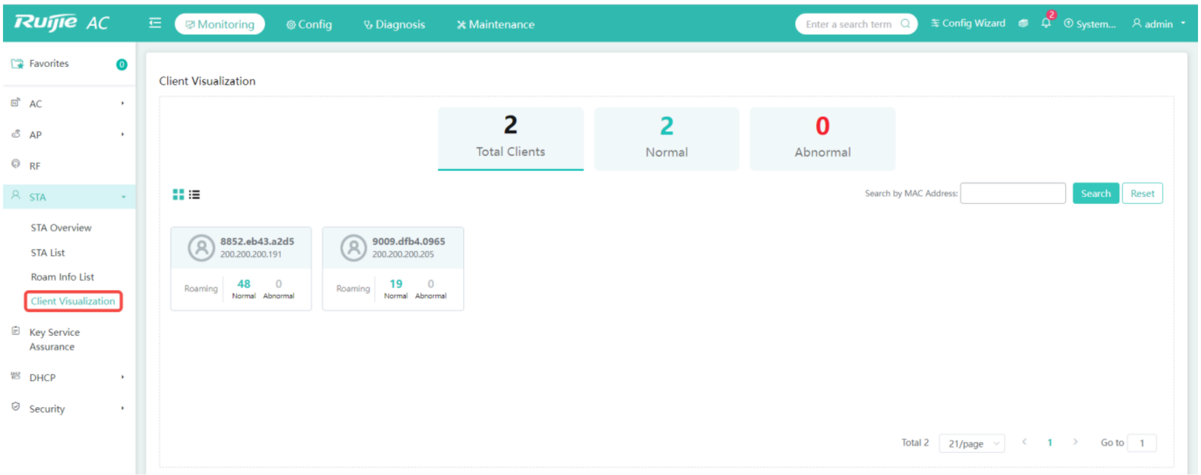
The roaming information list displays the list of roaming devices. Enter the MAC address in the search box and click **Search**. Click **Reset** to clear contents in the search bar and display all STAs.



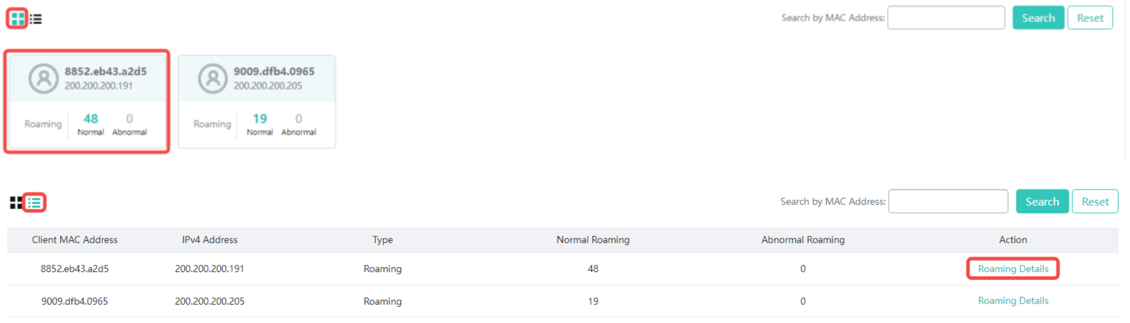
4.4.6 Client Visualization

Choose **Monitoring** > **STA** > **Client Visualization**.

The **Client Visualization** page displays the roaming information of clients, including the number of roaming clients and roaming details.

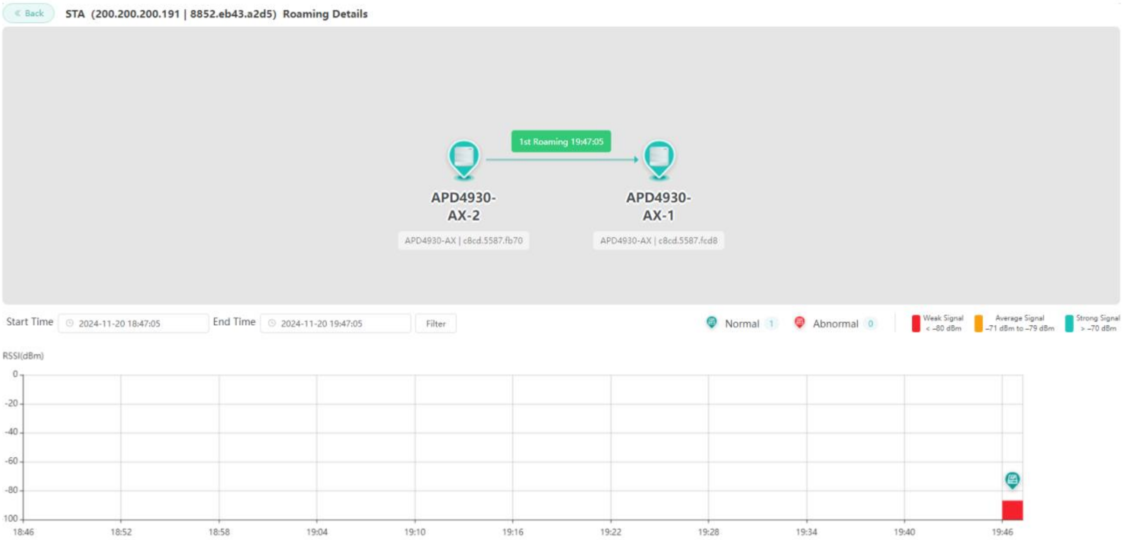


- Querying the number of roaming clients: The total number of roaming clients, number of normal roaming clients, and number of abnormal roaming clients are displayed in the upper part of the page.
- Querying the roaming details: Click the device card in the ▦ view or click **Roaming Details** in the **Action** column in the ☰ view to access the **Roaming Details** page of the corresponding client.

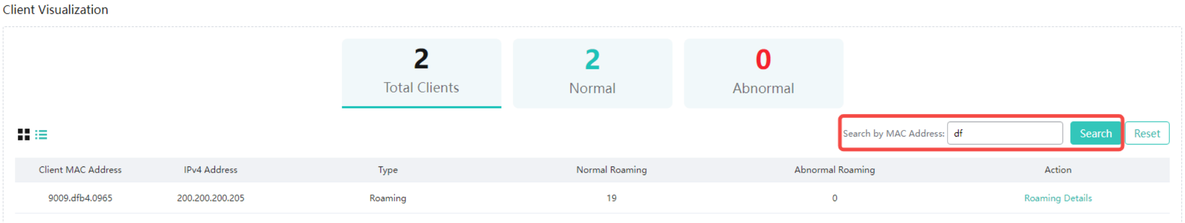


Client MAC Address	IPv4 Address	Type	Normal Roaming	Abnormal Roaming	Action
8852.eb43.a2d5	200.200.200.191	Roaming	48	0	Roaming Details
9009.dfb4.0965	200.200.200.205	Roaming	19	0	Roaming Details

On the **Roaming Details** page, as shown in the following figure, set the start time and end time and click **Filter** to view the roaming details within the specified time range.



- Querying roaming clients meeting the search criteria: Enter the MAC address keyword in the search box and click **Search**. Roaming clients are found in fuzzy match mode. Click **Reset** to clear the search criteria and display the list of all roaming clients.



Client Visualization

2 Total Clients | 2 Normal | 0 Abnormal

Search by MAC Address: df

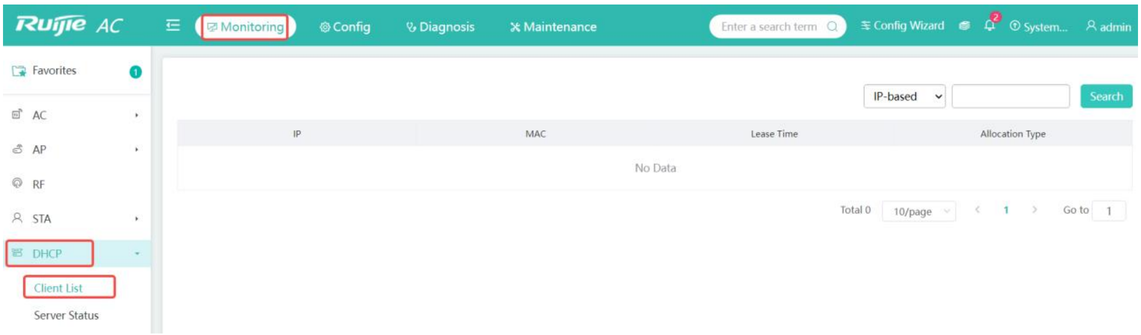
Client MAC Address	IPv4 Address	Type	Normal Roaming	Abnormal Roaming	Action
9009.dfb4.0965	200.200.200.205	Roaming	19	0	Roaming Details

4.5 DHCP

4.5.1 DHCP Client List

Choose **Monitoring** > **DHCP** > **Client List**.

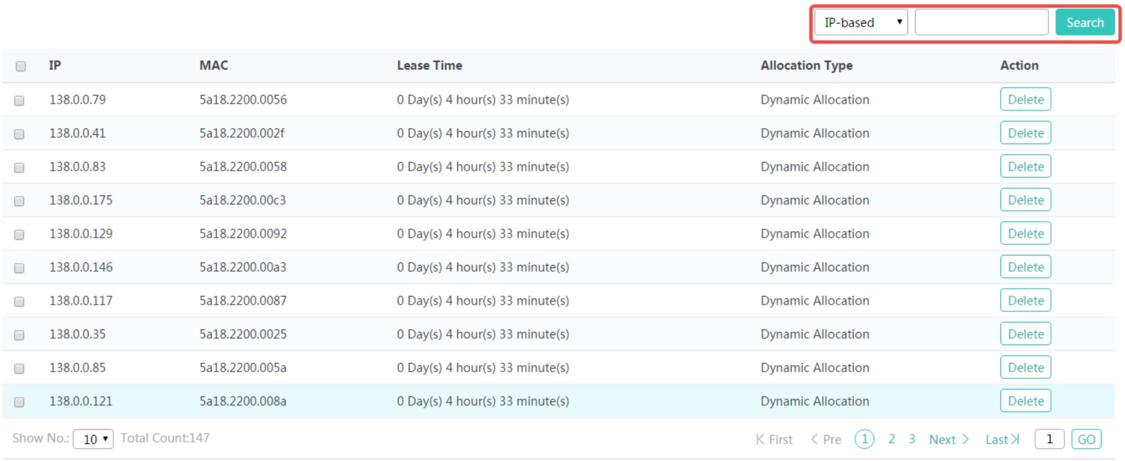
The DHCP client list displays the clients allocated with addresses from the address pool.



IP	MAC	Lease Time	Allocation Type
No Data			

Total 0 10/page 1 Go to 1

Searching for STAs: If there are a large number of STAs, search for STAs by the MAC address or IP address. Enter keywords in the input box and click **search**.



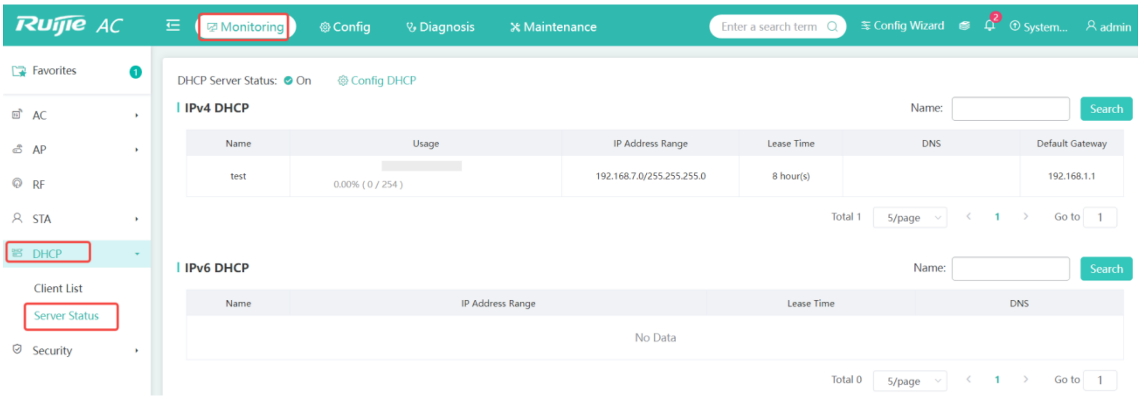
□	IP	MAC	Lease Time	Allocation Type	Action
□	138.0.0.79	5a18.2200.0056	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.41	5a18.2200.002f	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.83	5a18.2200.0058	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.175	5a18.2200.00c3	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.129	5a18.2200.0092	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.146	5a18.2200.00a3	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.117	5a18.2200.0087	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.35	5a18.2200.0025	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.85	5a18.2200.005a	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete
□	138.0.0.121	5a18.2200.008a	0 Day(s) 4 hour(s) 33 minute(s)	Dynamic Allocation	Delete

Show No.: 10 Total Count:147 First Pre 1 2 3 Next Last 1 GO

4.5.2 DHCP Server Status

Choose **Monitoring** > **DHCP** > **Server Status**.

The DHCP server status page displays the DHCP server status and the usage of the address pool.



DHCP Server Status: On Config DHCP

IPv4 DHCP Name: Search

Name	Usage	IP Address Range	Lease Time	DNS	Default Gateway
test	0.00% (0 / 254)	192.168.7.0/255.255.255.0	8 hour(s)		192.168.1.1

Total 1 5/page < 1 > Go to 1

IPv6 DHCP Name: Search

Name	IP Address Range	Lease Time	DNS
No Data			

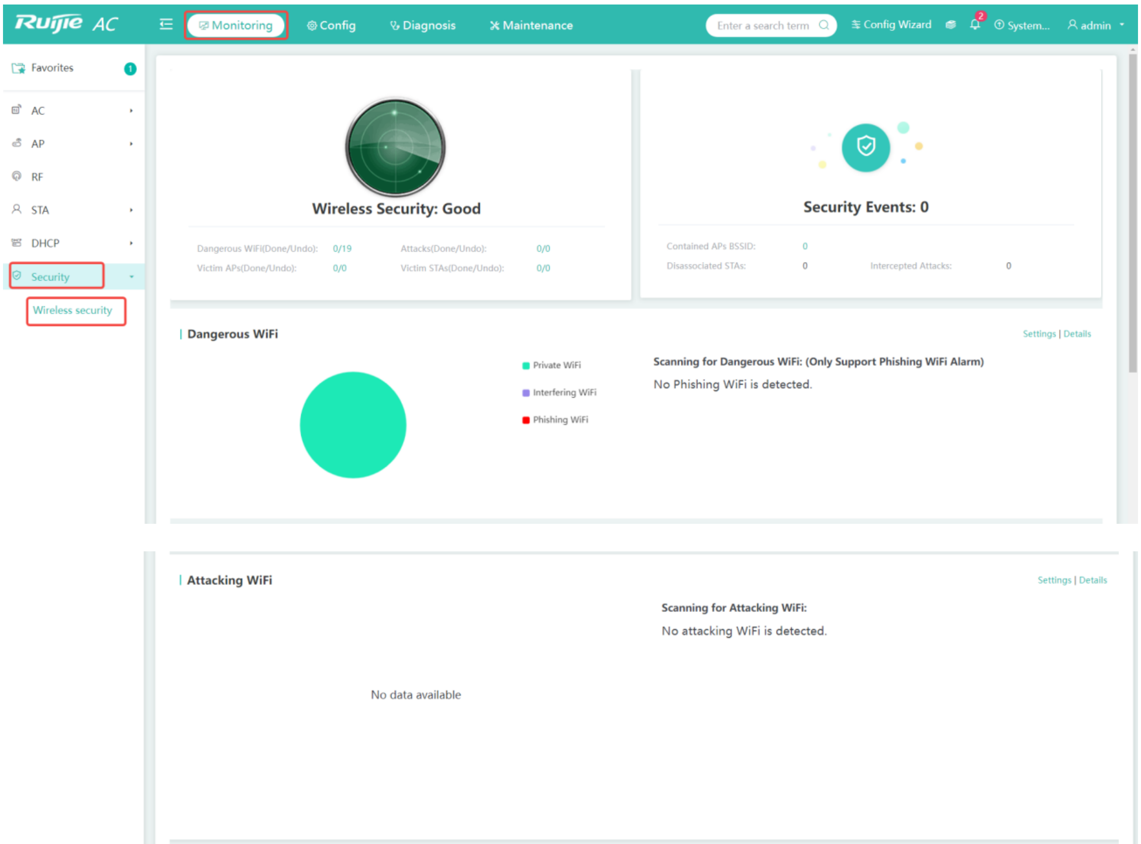
Total 0 5/page < 1 > Go to 1

4.6 Security

4.6.1 Wireless Security

Choose **Monitoring** > **Security** > **Wireless security**.

The **Wireless security** page displays the security situation and the number of security events handled by the device. The **Dangerous WiFi** page displays categories of dangerous Wi-Fi signals and dangerous Wi-Fi alarms. The **Attacking WiFi** page displays Wi-Fi attacks and attack alarms.



Wireless Security: Good

Dangerous WiFi(Done/Undo): 0/19 Attacks(Done/Undo): 0/0

Victim APs(Done/Undo): 0/0 Victim STAs(Done/Undo): 0/0

Security Events: 0

Contained APs BSSID: 0

Disassociated STAs: 0 Intercepted Attacks: 0

Dangerous WiFi

Scanning for Dangerous WiFi: (Only Support Phishing WiFi Alarm)

No Phishing WiFi is detected.

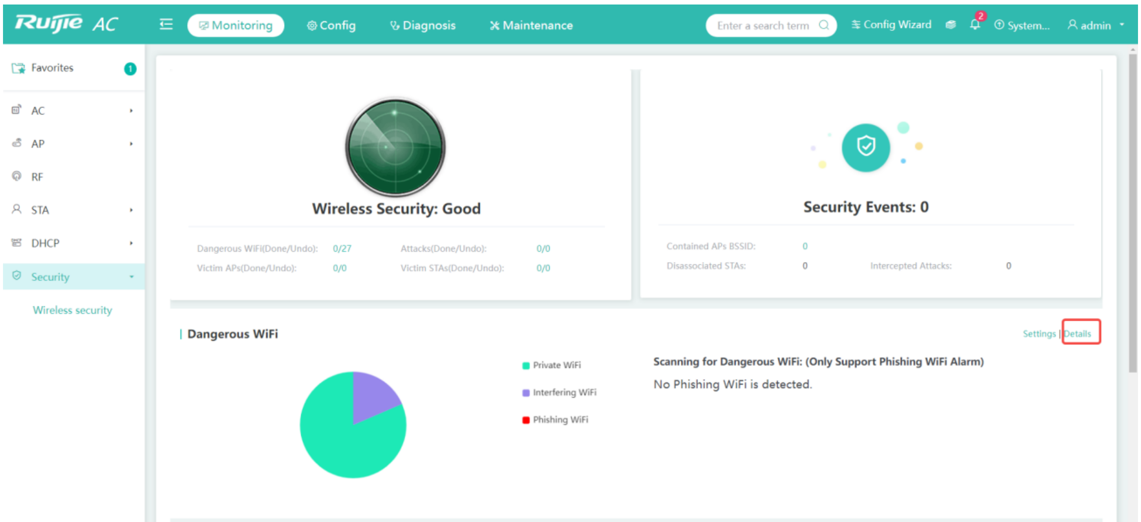
Attacking WiFi

Scanning for Attacking WiFi:

No attacking WiFi is detected.

No data available

(1) Dangerous Wi-Fi List: Click **Details** on the **Dangerous WiFi** page to redirect to the **Dangerous WiFi List** page.



Wireless Security: Good

Dangerous WiFi(Done/Undo): 0/27 Attacks(Done/Undo): 0/0
Victim APs(Done/Undo): 0/0 Victim STAs(Done/Undo): 0/0

Security Events: 0

Contained APs BSSID: 0
Disassociated STAs: 0 Intercepted Attacks: 0

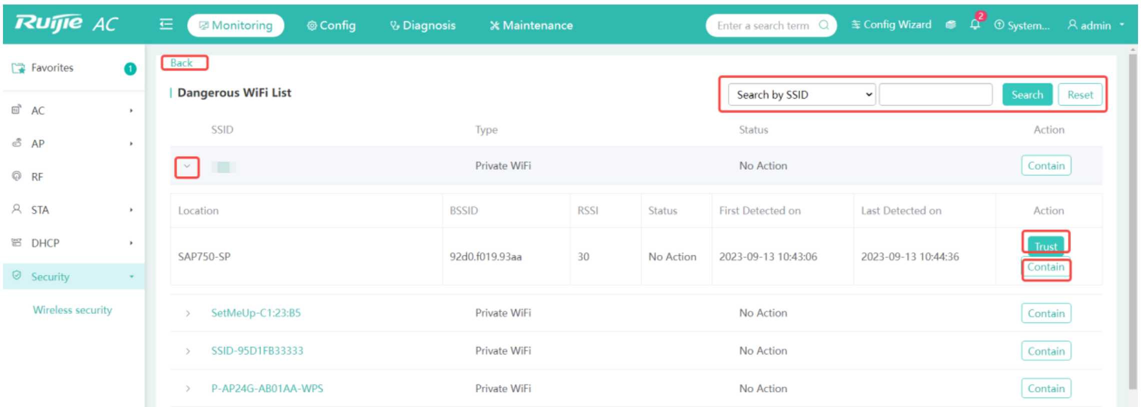
Dangerous WiFi

Scanning for Dangerous WiFi: (Only Support Phishing WiFi Alarm)

No Phishing WiFi is detected.

This function allows you to:

- Display the information about the dangerous Wi-Fi signals.
- Search for Wi-Fi signals by SSID, security type, and status.
- Contain or trust the devices with a certain BSSID.
- Contain an SSID or disable the containment.



Dangerous WiFi List

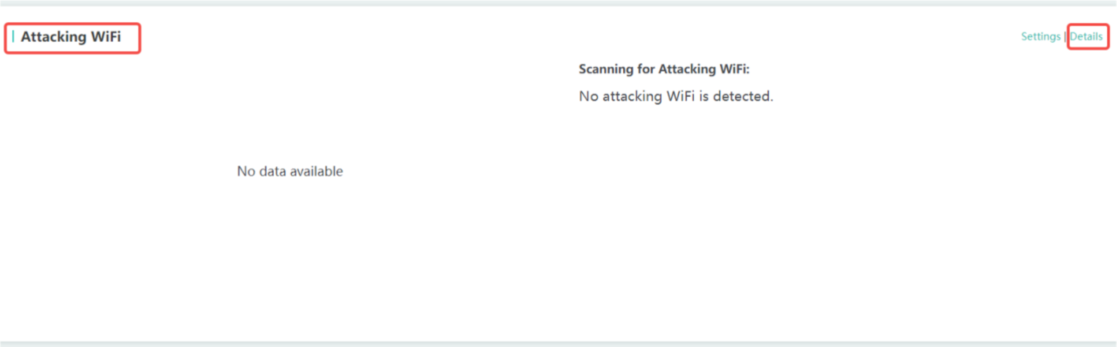
SSID	Type	Status	Action
	Private WiFi	No Action	Contain

Location	BSSID	RSSI	Status	First Detected on	Last Detected on	Action
SAP750-SP	92d0.f019.93aa	30	No Action	2023-09-13 10:43:06	2023-09-13 10:44:36	Trust Contain

SSID	Type	Status	Action
SetMeUp-C1:23:B5	Private WiFi	No Action	Contain
SSID-95D1FB33333	Private WiFi	No Action	Contain
P-AP24G-AB01AA-WPS	Private WiFi	No Action	Contain

Click **Back** to return to the **Wireless security** page.

(2) Attacking WiFi: Click Details on the Attacking WiFi page to redirect to the Attacking WiFi List page.



Attacking WiFi

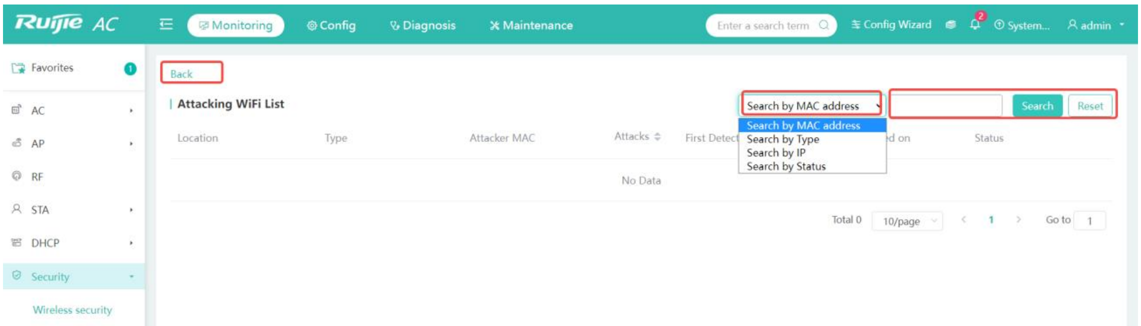
Scanning for Attacking WiFi:

No attacking WiFi is detected.

No data available

This function allows you to:

- Display the information about the Wi-Fi networks.
- Sort the Wi-Fi networks by the number of attacks.
- Search by MAC address, type, location, and status.



Click **Back** to return to the **Wireless security** page.

5 Configuration

5.1 WLAN

5.1.1 Add WiFi

Choose **Config** > **WLAN** > **Add WiFi**.

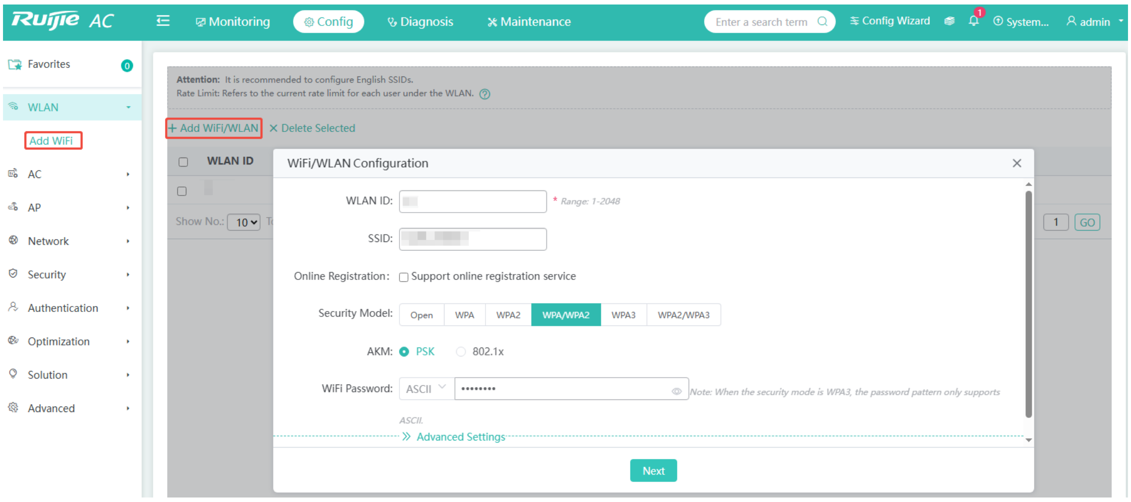
The Wi-Fi allows wireless STAs to be associated with the AP for network access. Multiple Wi-Fi networks can be added or deleted.

Note

- The maximum number of Wi-Fi networks is subject to device models.
- Click ⓘ to view the typical data rates in common scenarios.

1. Adding Wi-Fi

Click Add WiFi/WLAN and the WiFi/WLAN Configuration window pops up.



Attention: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.

WiFi/WLAN Configuration

WLAN ID: * Range: 1-2048

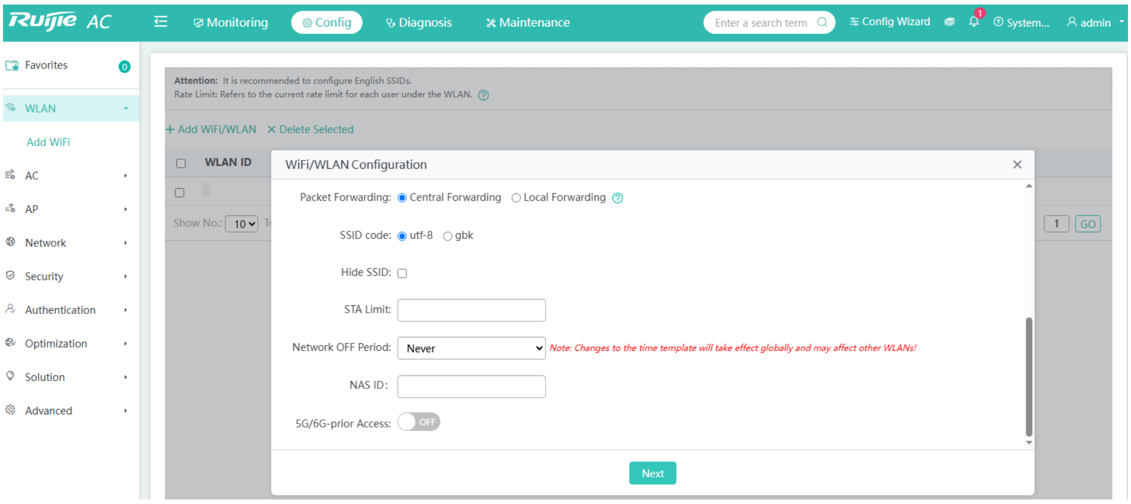
SSID:

Online Registration: □ Support online registration service

Security Model: Open | WPA | WPA2 | WPA/WPA2 | WPA3 | WPA2/WPA3 (WPA/WPA2 selected)

AKM: ● PSK ○ 802.1x

WiFi Password: ASCII •••••••• Note: When the security mode is WPA3, the password pattern only supports ASCII.



Attention: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.

WiFi/WLAN Configuration

Packet Forwarding: ● Central Forwarding ○ Local Forwarding

SSID code: ● utf-8 ○ gbk

Hide SSID: □

STA Limit:

Network OFF Period: Never Note: Changes to the time template will take effect globally and may affect other WLANs!

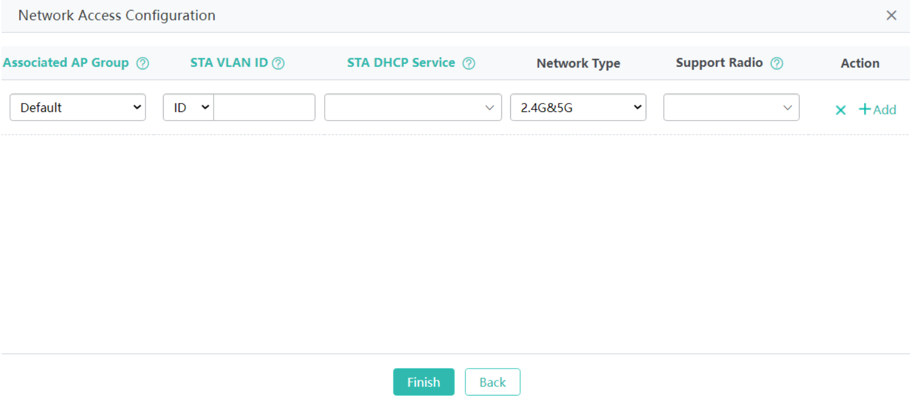
NAS ID:

5G/6G-prior Access: OFF

Parameter	Description
WLAN ID	Enter the WLAN ID.
SSID	Enter the Wi-Fi name.
Online Registration	Enable or disable online registration.
Security Model	● **Open**: Indicates no encryption. No password is required when the STA connects to the Wi-Fi network ● **WPA1, WPA2, and WPA/WPA2**: Indicate WPA1, WPA2, and WPA/WPA2 modes, respectively. PSK authentication and 802.1X authentication can be applied. ● **WPA3**: The WPA3 mode can work with four security policies, namely Simultaneous Authentication of Equals (SAE), Opportunistic Wireless Encryption (OWE), Enterprise-GCMP-256, and Enterprise-CCMP-128. ● **WPA2/WPA3**: The WPA2/WPA3 transition mode is supported. The STA determines the access mode. In this case, only PSK authentication and SAE security policies are supported.
AKM	● **PSK**: PSK authentication features high security and simple configuration, and is applicable to common home users and small enterprises. ● **802.1X**: 802.1X authentication requires authentication and accounting servers. The dedicated RADIUS server needs to be set up for authentication. Therefore, this authentication mode is not recommended for common users. **Note** If **Authentication Server** is set to **All Servers**, click **Radius Server Settings** next to **All Servers** to access the **Radius Server Settings** page. Alternatively, choose **Config** > **Advanced** > **Radius**. For details, see section 5.9.5 RADIUS. If **Authentication Server** is set to **Local Authentication**, click **Local STA Settings** next to **Local Authentication** to access the **STA Settings** page. Alternatively, choose **Config** > **Advanced** > **Local User Management**. For details, see section 5.9.6 1. Local User Management.
Encryption Type	● **SAE**: Compared with the WPA2 mode, SAE is more secure and can prevent dictionary attacks effectively. ● **OWE**: No authentication information is required. ● **Enterprise-GCMP-256**: Configures WPA3-Enterprise mode with GCMP-256 encryption, providing additional protection for networks transmitting sensitive data. It is applicable to data-sensitive networks like government or financial systems. ● **Enterprise-CCMP-128**: Configures WPA3-Enterprise mode with CCMP-128 encryption, providing additional protection for networks transmitting sensitive data. It is applicable to data-sensitive networks like government or financial systems.
PPSK	You can select **Enable** to enable the system to automatically generate an independent Wi-Fi password when a PPSK account is added.
WiFi Password	Enter the Wi-Fi password.

Packet Forwarding	**Central Forwarding**: All data is routed through the AC before being forwarded to other devices. This mode is configured by default. **Local Forwarding**: The data is forwarded to other devices directly from the switch, reducing the load on the AC.
SSID Code	**UTF-8**: You are advised to select **utf-8**, as most STAs support UTF-8 encoding by default. **GBK**: Some STAs, PCs, and Network Interface Cards (NICs) support GBK encoding. You can select encoding modes as required.
Hide SSID	If you enable **Hide SSID**, the SSID is not displayed on the STA. You can only find the SSID through searching.
STA Limit	Configure the maximum number of STAs that can be associated with this Wi-Fi. It is not configured by default, implying that there is no limit.
Network OFF Period	Configure a period when the Wi-Fi is turned off. The default value is **Never**. Configure a period to turn off the Wi-Fi when it is necessary in specific scenarios.
NAS ID	Configure the NAS ID for the WLAN by entering a string of up to 32 bytes without spaces.
5G/6G-prior Access	If this feature is enabled, the STA logs in to 5G/6G networks preferentially. It is disabled by default.

After the configuration is completed, click **Next** to enter the **Network Access Configuration** page.



Network Access Configuration

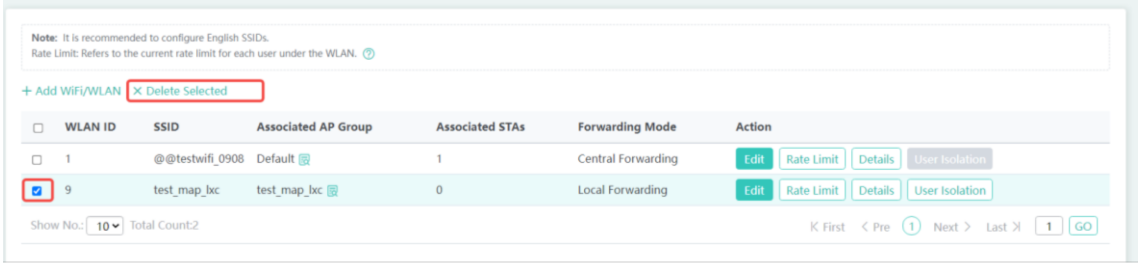
Associated AP Group	STA VLAN ID	STA DHCP Service	Network Type	Support Radio	Action
Default	ID		2.4G&5G		× +Add

Parameter	Description
Associated AP Group	Specify which APs transmit the signals for this Wi-Fi. Typically, a single Wi-Fi hotspot's signal is broadcast by multiple APs. These APs are organized into one group for easy management. If no AP group is configured, all APs transmit the Wi-Fi signal by default.
STA VLAN ID	Enter the VLAN to which the STAs of this Wi-Fi belong.

STA DHCP Service	The STAs connecting to this WLAN network can be allocated with IP addresses from an address pool that is configured on the local device or other devices. It is configured on other devices by default. If you choose to configure the address pool on the local device, click **STA DHCP Service** to redirect to the **Configure DHCP on AC** page. **Note** The IP addresses assigned by DHCP to STAs should be on the same network segment as the STA VLAN.
Network Type	Specify the network types supported by this Wi-Fi. 2.4 GHz, 5 GHz, and 6 GHz are supported by default.
Support Radio	Specify the radios supported by the AP for transmitting the Wi-Fi signal. All radios are supported by default.

2. Deleting WLAN

Select the WLAN you want to delete and click **Delete Selected**. Click **OK** in the pop-up window.

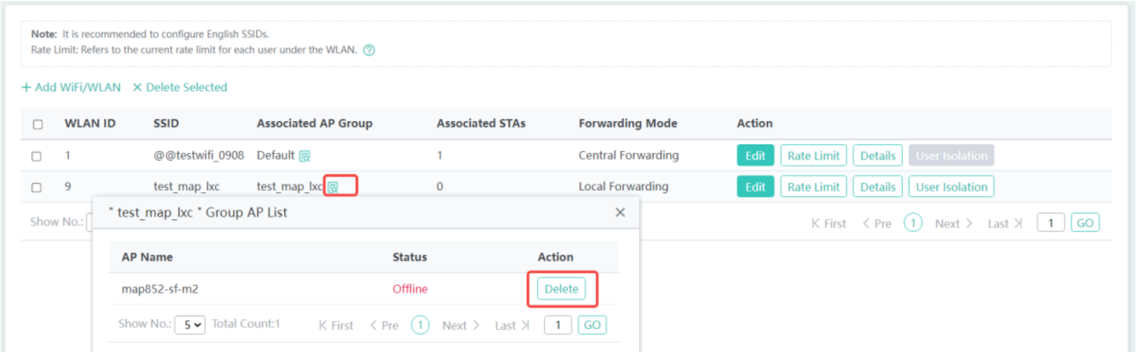


Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.

□	WLAN ID	SSID	Associated AP Group	Associated STAs	Forwarding Mode	Action
□	1	@@testwifi_0908	Default	1	Central Forwarding	Edit Rate Limit Details User Isolation
☑	9	test_map_lxc	test_map_lxc	0	Local Forwarding	Edit Rate Limit Details User Isolation

3. Viewing the Associated AP Group

Click in the **Associated AP Group** column to display or delete APs in the AP group.



Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.

□	WLAN ID	SSID	Associated AP Group	Associated STAs	Forwarding Mode	Action
□	1	@@testwifi_0908	Default	1	Central Forwarding	Edit Rate Limit Details User Isolation
□	9	test_map_lxc	test_map_lxc	0	Local Forwarding	Edit Rate Limit Details User Isolation

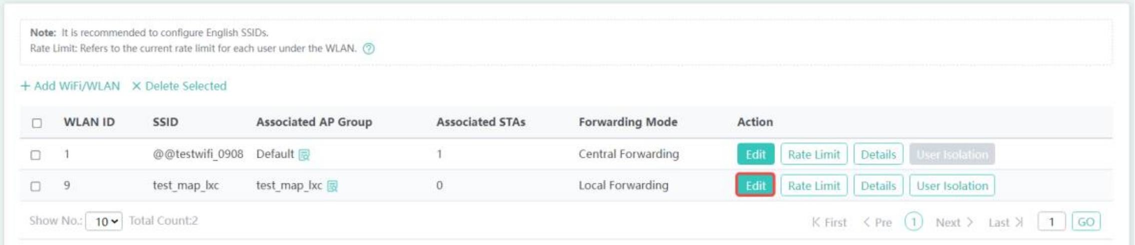
" test_map_lxc " Group AP List

AP Name	Status	Action
map852-sf-m2	Offline	Delete

4. Editing WLAN

(1) Edit the configuration of a created WLAN.

Click **Edit** in the **Action** column to edit the existing WLAN. A pop-up window will display the information about this WLAN. After editing, click **Finish**. A message indicating operation success is displayed.



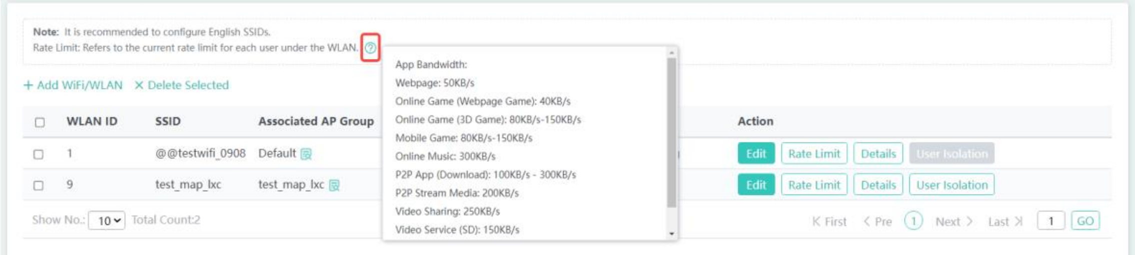
Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN. ⓘ

□	WLAN ID	SSID	Associated AP Group	Associated STAs	Forwarding Mode	Action
□	1	@@testwifi_0908	Default	1	Central Forwarding	Edit Rate Limit Details User Isolation
□	9	test_map_lxc	test_map_lxc	0	Local Forwarding	Edit Rate Limit Details User Isolation

Show No.: 10 Total Count:2

(2) Rate limiting

To set uplink and downlink rate limits for a Wi-Fi network, click ⓘ to view the typical bandwidth for common application download scenarios. Click **Rate Limit** to configure the maximum uplink and downlink rate in the pop-up window, and click **Save**.

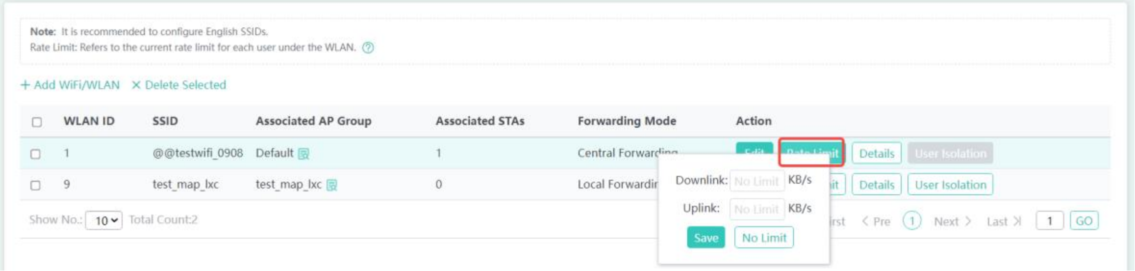


Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN. ⓘ

App Bandwidth:
Webpage: 50KB/s
Online Game (Webpage Game): 40KB/s
Online Game (3D Game): 80KB/s-150KB/s
Mobile Game: 80KB/s-150KB/s
Online Music: 300KB/s
P2P App (Download): 100KB/s - 300KB/s
P2P Stream Media: 200KB/s
Video Sharing: 250KB/s
Video Service (SD): 150KB/s

□	WLAN ID	SSID	Associated AP Group	Action
□	1	@@testwifi_0908	Default	Edit Rate Limit Details User Isolation
□	9	test_map_lxc	test_map_lxc	Edit Rate Limit Details User Isolation

Show No.: 10 Total Count:2



Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN. ⓘ

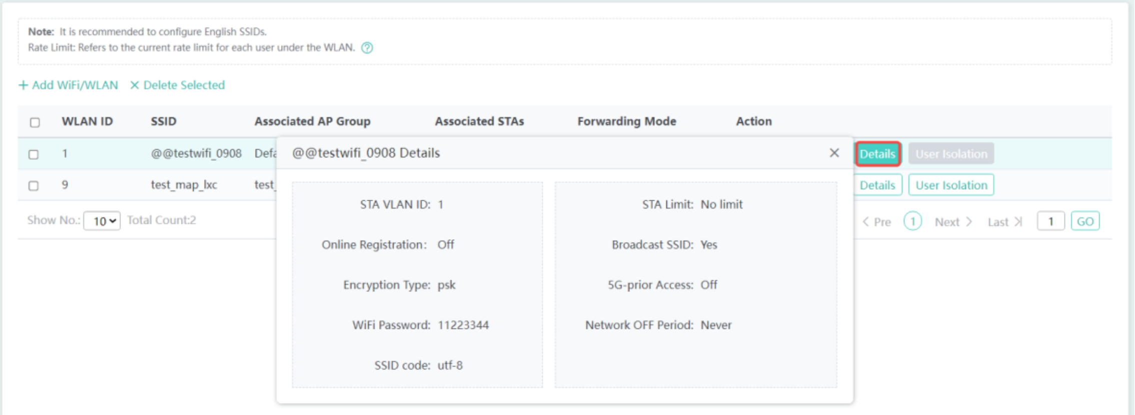
□	WLAN ID	SSID	Associated AP Group	Associated STAs	Forwarding Mode	Action
□	1	@@testwifi_0908	Default	1	Central Forwarding	Edit Rate Limit Details User Isolation
□	9	test_map_lxc	test_map_lxc	0	Local Forwardir	Details User Isolation

Show No.: 10 Total Count:2

Downlink: No Limit KB/s
Uplink: No Limit KB/s

(3) Viewing WLAN details

Click **Details** in the Action column and a window pops up, displaying details of the WLAN.



Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN. ⓘ

□	WLAN ID	SSID	Associated AP Group	Associated STAs	Forwarding Mode	Action
□	1	@@testwifi_0908	Defa			Details User Isolation
□	9	test_map_lxc	test_			Details User Isolation

Show No.: 10 Total Count:2

@@testwifi_0908 Details ×

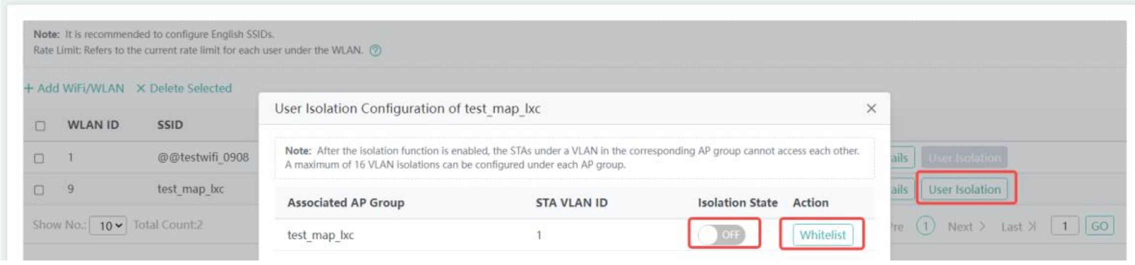
STA VLAN ID: 1
Online Registration: Off
Encryption Type: psk
WiFi Password: 11223344
SSID code: utf-8

STA Limit: No limit
Broadcast SSID: Yes
5G-prior Access: Off
Network OFF Period: Never

(4) Configuring user isolation

SSID-based isolation is equivalent to AP group-based VLAN isolation. Click **User Isolation** in the **Action** column and a window pops up, displaying the **User Isolation Configuration** page.

Toggle on or off the **Isolation State** switch. Click **Whitelist** and the **Whitelist Configuration** window pops up.



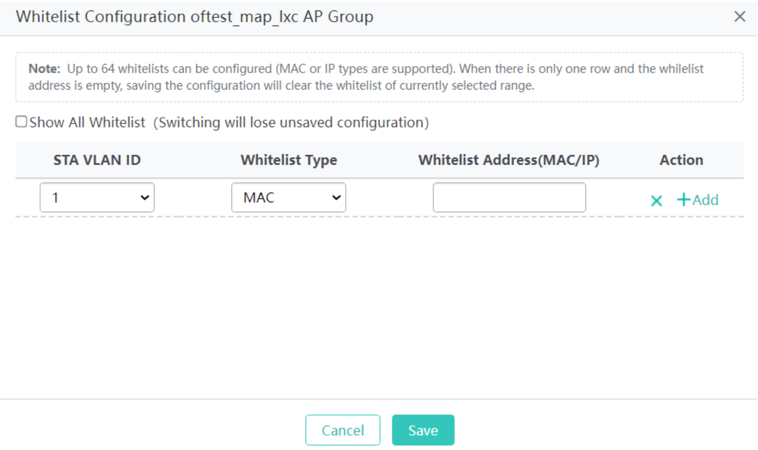
Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.

User Isolation Configuration of test_map_lxc

Note: After the isolation function is enabled, the STAs under a VLAN in the corresponding AP group cannot access each other. A maximum of 16 VLAN isolations can be configured under each AP group.

Associated AP Group	STA VLAN ID	Isolation State	Action
test_map_lxc	1	OFF	Whitelist

Configure the whitelist and it takes effect based on the associated AP group.



Whitelist Configuration oftest_map_lxc AP Group

Note: Up to 64 whitelists can be configured (MAC or IP types are supported). When there is only one row and the whitelist address is empty, saving the configuration will clear the whitelist of currently selected range.

☐ Show All Whitelist (Switching will lose unsaved configuration)

STA VLAN ID	Whitelist Type	Whitelist Address(MAC/IP)	Action
1	MAC		× +Add

Parameter	Description
STA VLAN ID	Select the VLAN that the whitelist applies to. Select only VLANs already mapped under this AP group.
Whitelist Type	Both MAC address- and IP address-based whitelists are supported.
Whitelist Address (MAC/IP)	When you set **Whitelist Type** to **MAC**, broadcast and multicast addresses are not supported. When you set **Whitelist Type** to **IP**, IP addresses **0.0.0.0** and **255.255.255.255** are not supported.

5.2 AC

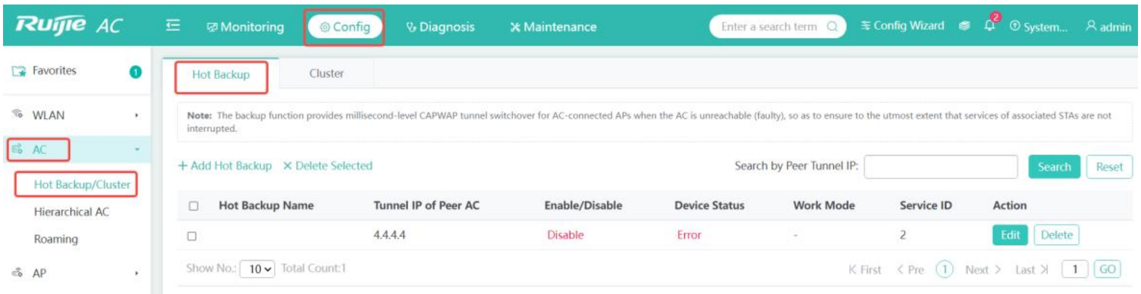
5.2.1 Hot Backup/Cluster

The **Hot Backup/Cluster page** includes **Hot Backup** and **Cluster** tabs.

1. **Hot Backup**

Choose **Config** > **AC** > **Hot Backup/Cluster** > **Hot Backup**.

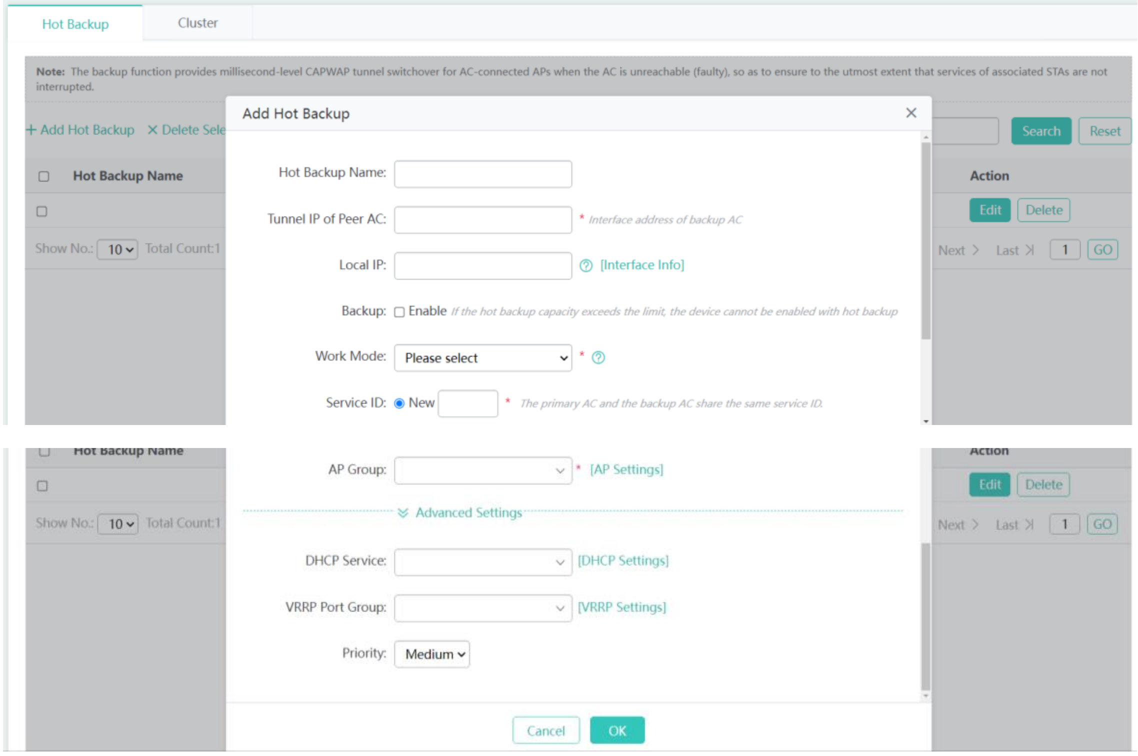
In Fit AP mode, the AP has to establish a CAPWAP Tunnel with the AC to operate normally. Hot backup enables the AP interconnected with the AC to switch the CAPWAP tunnel in milliseconds when the AC fails. This allows the STA to quickly switch over to the backup AC and guarantees non-stop services, ensuring the availability and stability of STAs.



Note: The backup function provides millisecond-level CAPWAP tunnel switchover for AC-connected APs when the AC is unreachable (faulty), so as to ensure to the utmost extent that services of associated STAs are not interrupted.

□	Hot Backup Name	Tunnel IP of Peer AC	Enable/Disable	Device Status	Work Mode	Service ID	Action
□		4.4.4.4	Disable	Error	-	2	Edit Delete

(1) Adding the hot backup: Click **Add Hot Backup**. The configuration page is displayed.



Note: The backup function provides millisecond-level CAPWAP tunnel switchover for AC-connected APs when the AC is unreachable (faulty), so as to ensure to the utmost extent that services of associated STAs are not interrupted.

Hot Backup Name:

Tunnel IP of Peer AC: * *Interface address of backup AC*

Local IP: [Interface Info]

Backup: □ Enable *If the hot backup capacity exceeds the limit, the device cannot be enabled with hot backup*

Work Mode: Please select *

Service ID: ● New * *The primary AC and the backup AC share the same service ID.*

AP Group: * [AP Settings]

DHCP Service: [DHCP Settings]

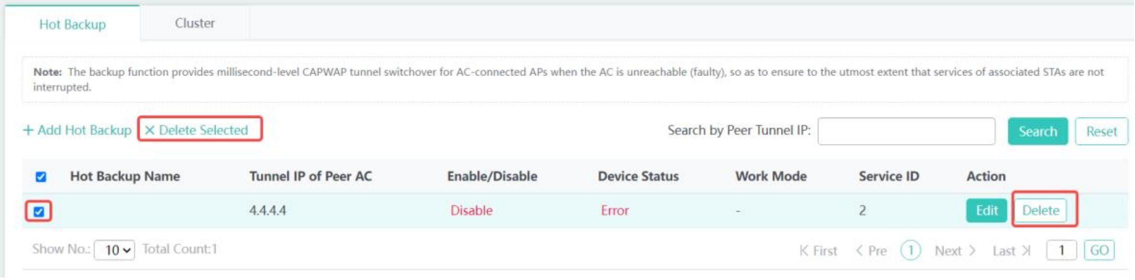
VRRP Port Group: [VRRP Settings]

Priority: Medium

Parameter	Description
Hot Backup Name	Configure the hot backup name.
Tunnel IP of Peer AC	Enter the IP address on the peer side of the tunnel for communications between the AP and AC. The IP address of interface Loopback0 is configured as the tunnel IP address by default.
Local IP	If the communication is not established through interface Loopback0, configure the local IP address. Typically, the interface IP address is configured as the local IP address. Configure this parameter by clicking **Interface Info** to view interface details.

Backup	Enable or disable hot backup. This feature cannot be enabled if the number of hot backups reaches the limit.
Work Mode	The **Hot Backup Mode** and **Fast Switchover Mode** are supported by a regular AC. The **Hot Backup Mode** and **Cold Backup Mode** are supported by a headquarters or branch AC. The work modes are described as follows: **Hot Backup Mode**: Applies to scenarios with requirements for stable performance. To avoid hot standby flapping, you are advised to adopt this mode. **Fast Switchover Mode**: Applies to scenarios with high requirements for switching performance. This mode may lead to frequent hot backup switching. **Cold Backup Mode**: Applies to hierarchical AC scenarios.
Service ID	Enter the service ID, that is, context ID. This field is optional.
AP Group	The AP groups for active and backup devices must be configured consistently. Click **AP Settings** to add AP groups for the current device.
Advanced Settings	Advanced settings are not supported in virtual AC (VAC) and hierarchical AC (headquarters AC and branch AC) scenarios. They are supported by only normal ACs.
VRRP Port Group	The VRRP groups for active and backup devices must be configured consistently. Click **VRRP Settings** to add VRRP for the current device.
DHCP Service	The DHCP for active and backup devices must be configured consistently. Click **DHCP Settings** to add DHCP for the current device.
Priority	Select the priorities of the hot backup devices, including three options: low, medium, and high.

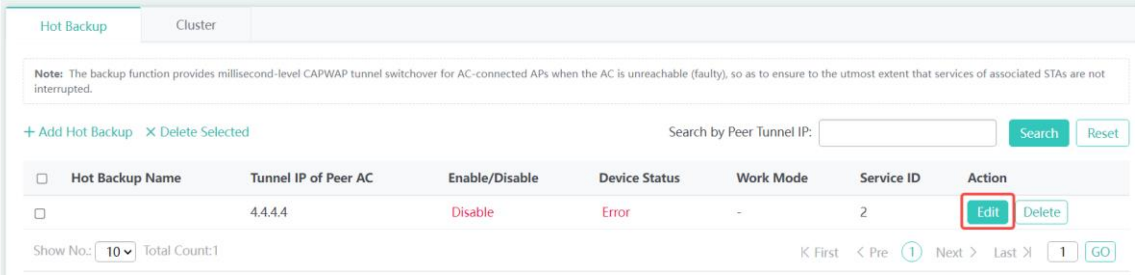
(2) Deleting hot backup devices: Click **Delete** in the **Action** column to delete an item. Select multiple items and click **Delete Selected** to batch delete items.



Note: The backup function provides millisecond-level CAPWAP tunnel switchover for AC-connected APs when the AC is unreachable (faulty), so as to ensure to the utmost extent that services of associated STAs are not interrupted.

☑	Hot Backup Name	Tunnel IP of Peer AC	Enable/Disable	Device Status	Work Mode	Service ID	Action
☑		4.4.4.4	Disable	Error	-	2	Edit Delete

(3) Editing hot backup devices: Click **Edit** in the **Action** column. Edit the fields in the pop-up window and click **Save**.



Note: The backup function provides millisecond-level CAPWAP tunnel switchover for AC-connected APs when the AC is unreachable (faulty), so as to ensure to the utmost extent that services of associated STAs are not interrupted.

Search by Peer Tunnel IP:

□	Hot Backup Name	Tunnel IP of Peer AC	Enable/Disable	Device Status	Work Mode	Service ID	Action
□		4.4.4.4	Disable	Error	-	2	Edit Delete

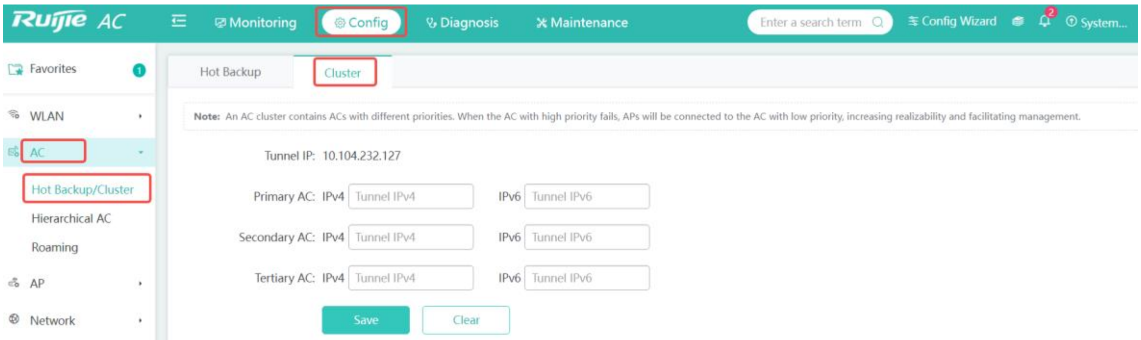
Show No.: 10 Total Count:1

2. Cluster

Choose **Config** > **AC** > **Hot Backup/Cluster** > **Cluster**.

An AC cluster includes multiple ACs for an AP. When the AP fails to interconnect with an AC, the AP can use a backup AC. It prevents the unavailability of APs due to AC failure, enhancing the reliability of wireless networks.

Configure up to three backup ACs based on IPv4 or IPv6 addresses.



Note: An AC cluster contains ACs with different priorities. When the AC with high priority fails, APs will be connected to the AC with low priority, increasing realizability and facilitating management.

Tunnel IP: 10.104.232.127

Primary AC: IPv4 Tunnel IPv4 IPv6 Tunnel IPv6

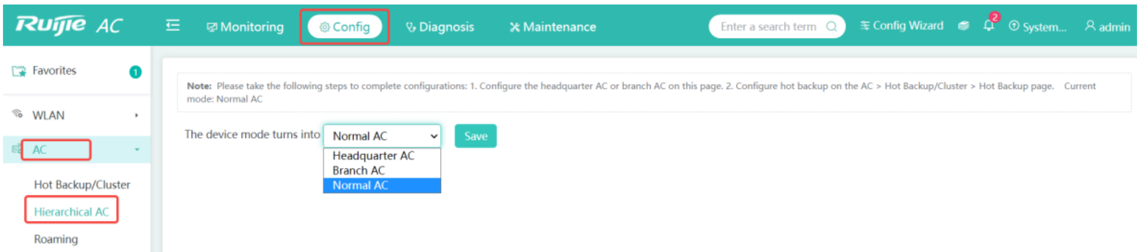
Secondary AC: IPv4 Tunnel IPv4 IPv6 Tunnel IPv6

Tertiary AC: IPv4 Tunnel IPv4 IPv6 Tunnel IPv6

5.2.2 Hierarchical AC

Choose **Config** > **AC** > **Hierarchical AC**.

Details of hierarchical ACs are displayed on this page. This AC can be configured as a branch or normal AC but not a central AC.



Note: Please take the following steps to complete configurations: 1. Configure the headquarter AC or branch AC on this page. 2. Configure hot backup on the AC > Hot Backup/Cluster > Hot Backup page. Current mode: Normal AC

The device mode turns into Normal AC

5.2.3 Roaming

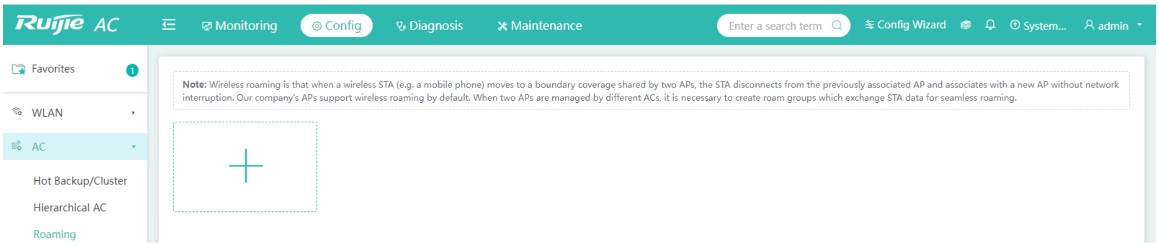
Choose **Config** > **AC** > **Roaming**.

Wireless roaming is that when a wireless STA (e.g. a mobile phone) moves to a boundary coverage shared by two APs, the STA disconnects from the previously associated AP and associates with a new AP without network interruption. Our company's APs support wireless roaming by default. When two APs are managed by different ACs, it is necessary to create roam groups which exchange STA data for seamless roaming.

The roaming range for STAs cannot extend infinitely. To enable STAs to roam across APs associated with different ACs and manage the roaming range of STAs, the ACs in the area where the STA moves are moved into a roam group.

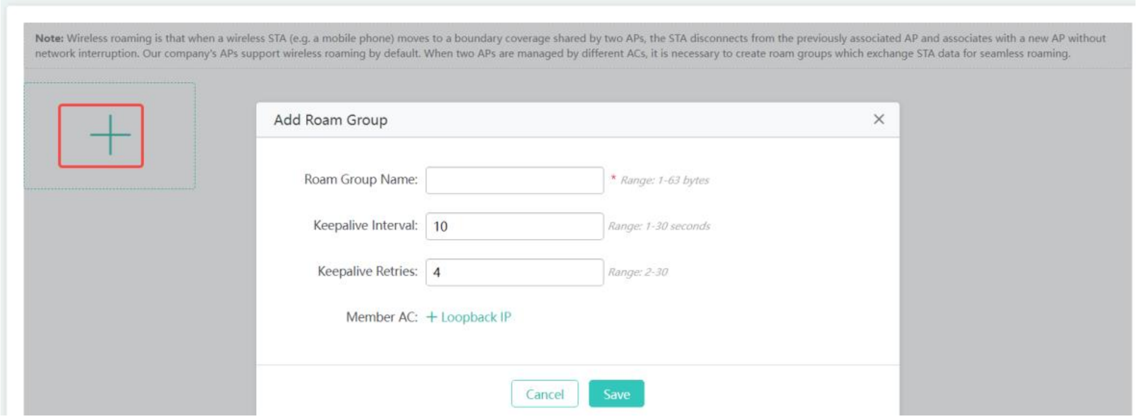
Note

The number of member devices in the roam group is limited to ensure the efficiency and reliability of communications between ACs in a roam group. Each roam group contains a maximum of 24 AC members.



Note: Wireless roaming is that when a wireless STA (e.g. a mobile phone) moves to a boundary coverage shared by two APs, the STA disconnects from the previously associated AP and associates with a new AP without network interruption. Our company's APs support wireless roaming by default. When two APs are managed by different ACs, it is necessary to create roam groups which exchange STA data for seamless roaming.

(1) Adding roam groups: Click the **+** button on the **Roaming** page to add a roam group. The **Roam Group Name** field is mandatory, while other fields are optional. Multiple member ACs can be selected. Clicking **Save** and the roam group will be displayed on the **Roaming** page after a message indicating operation success appears.



Note: Wireless roaming is that when a wireless STA (e.g. a mobile phone) moves to a boundary coverage shared by two APs, the STA disconnects from the previously associated AP and associates with a new AP without network interruption. Our company's APs support wireless roaming by default. When two APs are managed by different ACs, it is necessary to create roam groups which exchange STA data for seamless roaming.

Add Roam Group

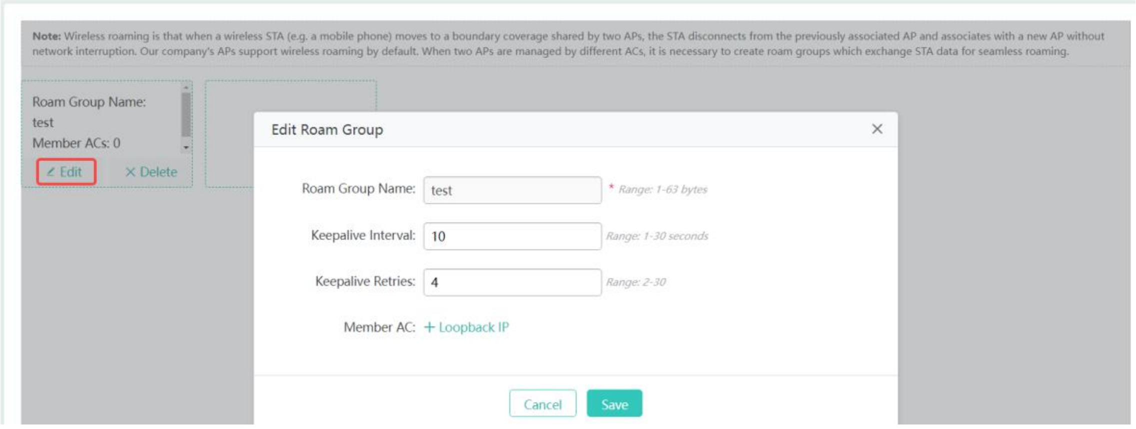
Roam Group Name: * Range: 1-63 bytes

Keepalive Interval: 10 Range: 1-30 seconds

Keepalive Retries: 4 Range: 2-30

Member AC: + Loopback IP

(2) Editing roam groups: Click **Edit** in the box of a roam group. Edit the fields in the **Edit Roam Group** window and click **Save**.



Note: Wireless roaming is that when a wireless STA (e.g. a mobile phone) moves to a boundary coverage shared by two APs, the STA disconnects from the previously associated AP and associates with a new AP without network interruption. Our company's APs support wireless roaming by default. When two APs are managed by different ACs, it is necessary to create roam groups which exchange STA data for seamless roaming.

Roam Group Name: test

Member ACs: 0

Edit Roam Group

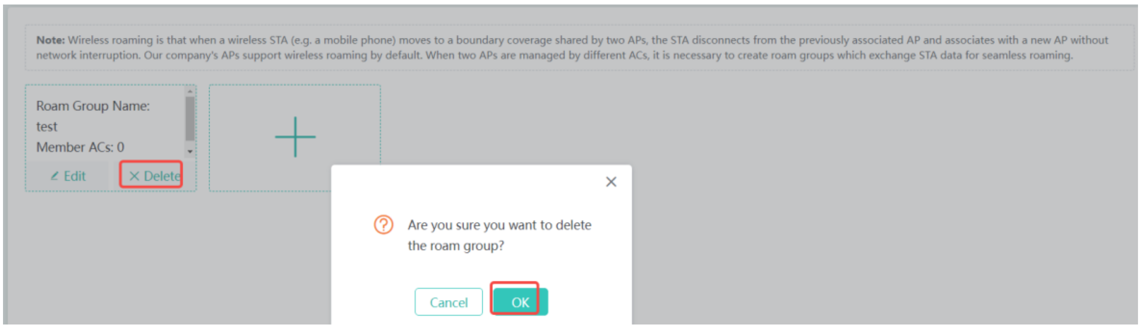
Roam Group Name: test * Range: 1-63 bytes

Keepalive Interval: 10 Range: 1-30 seconds

Keepalive Retries: 4 Range: 2-30

Member AC: + Loopback IP

(3) Deleting roam groups: Click **Delete** in the box of the roam group you want to delete and click **OK** in the pop-up window.



Note: Wireless roaming is that when a wireless STA (e.g. a mobile phone) moves to a boundary coverage shared by two APs, the STA disconnects from the previously associated AP and associates with a new AP without network interruption. Our company's APs support wireless roaming by default. When two APs are managed by different ACs, it is necessary to create roam groups which exchange STA data for seamless roaming.

Roam Group Name: test
Member ACs: 0

Are you sure you want to delete the roam group?

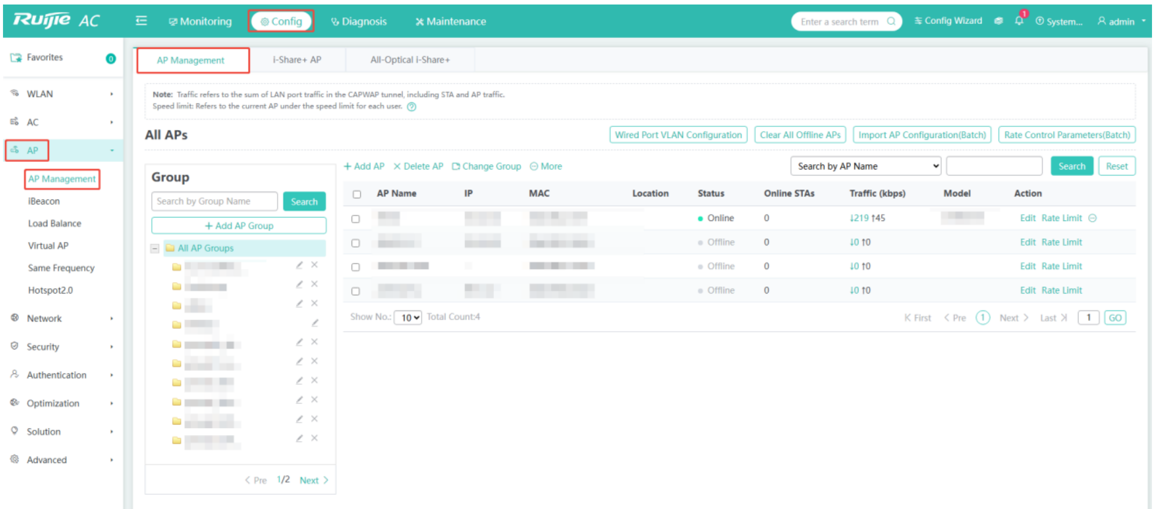
5.3 AP

5.3.1 AP Management

1. AP Management

Choose **Config** > **AP** > **AP Management**.

APs must be associated with an AC and added to an AP group before providing services wireless STAs. All newly added APs are assigned to the default AP group.



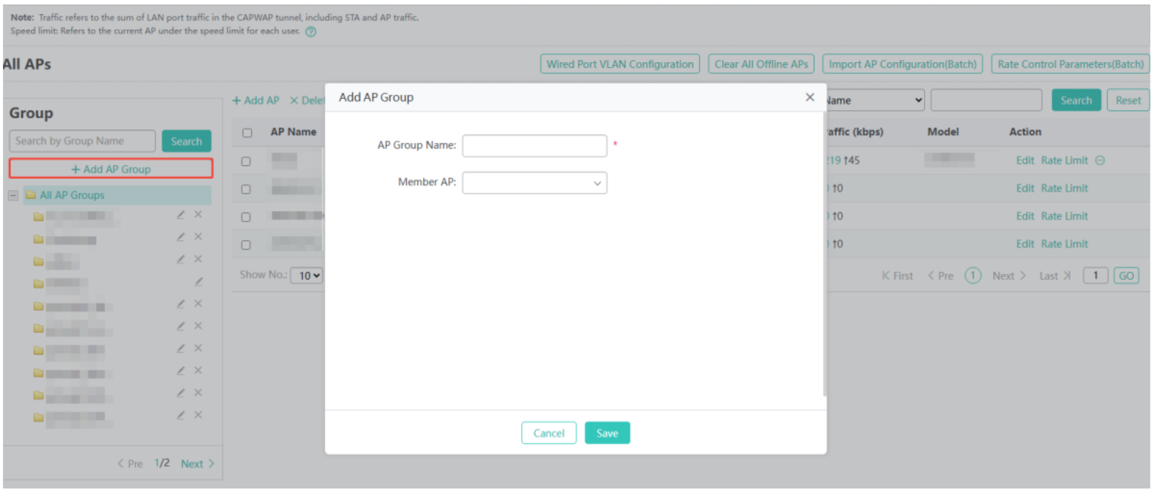
Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

All APs

Group

☐	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
☐	[redacted]	[redacted]	[redacted]		● Online	0	↓219 ↑45	[redacted]	Edit Rate Limit
☐	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]		[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit

(1) Adding AP groups: Click **+ Add AP Group** and the **Add AP Group** window pops up. Enter the AP group name, select member APs to be added to this AP group, and Click **Save**.



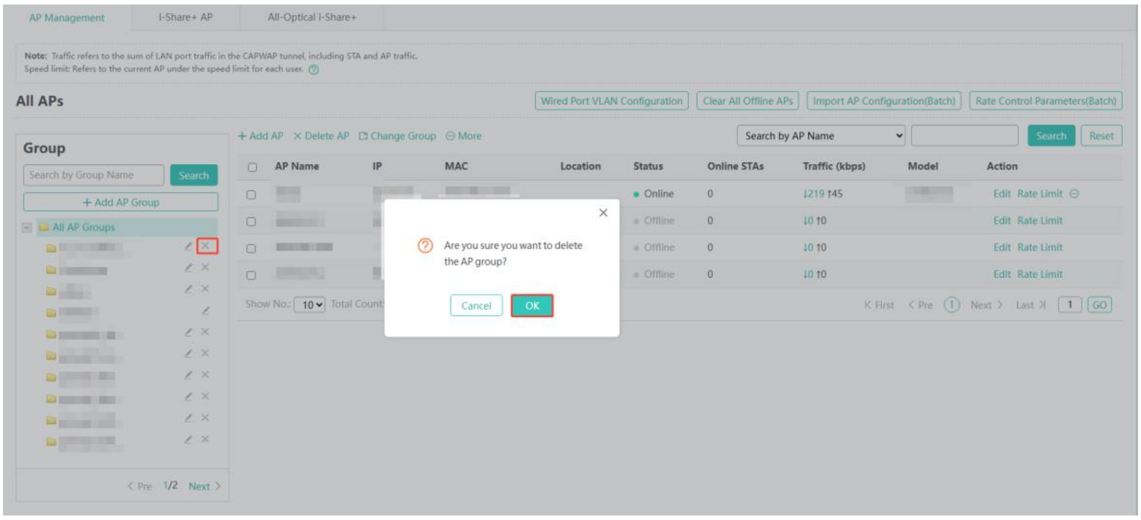
Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

Parameter	Description
AP Group Name	This field is mandatory.
Member AP	Select member APs to be added to this AP group. An AP can be added to only one group. If APs are not added to any group, they are assigned to the default AP group.

(2) Deleting AP groups: Select the AP group you want to delete and click **x**. Click **OK** in the pop-up window to delete the AP group.

Note

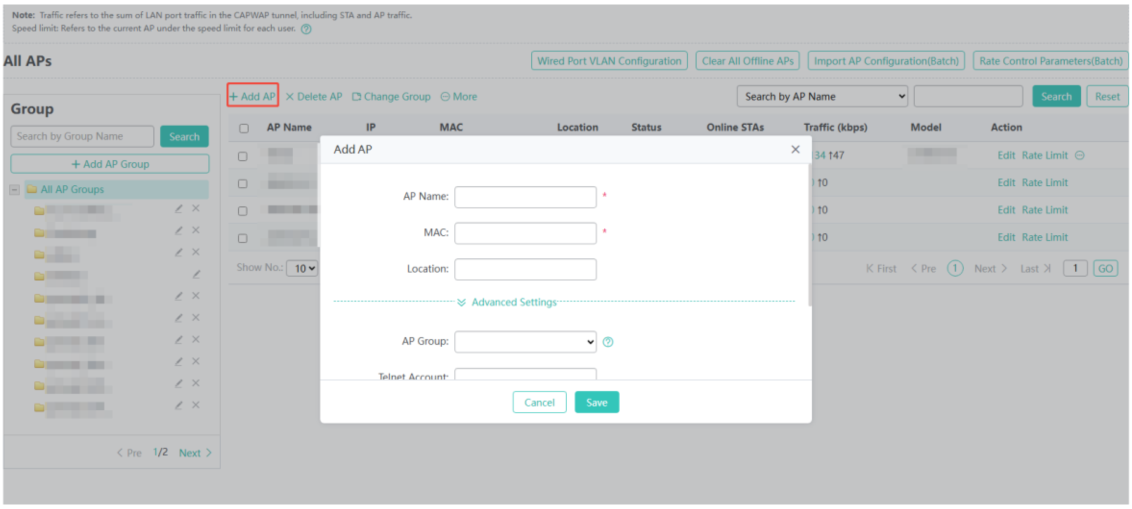
- The default group cannot be deleted.
- After an AP group is deleted, the APs in this group are automatically assigned to the default group.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

Are you sure you want to delete the AP group?

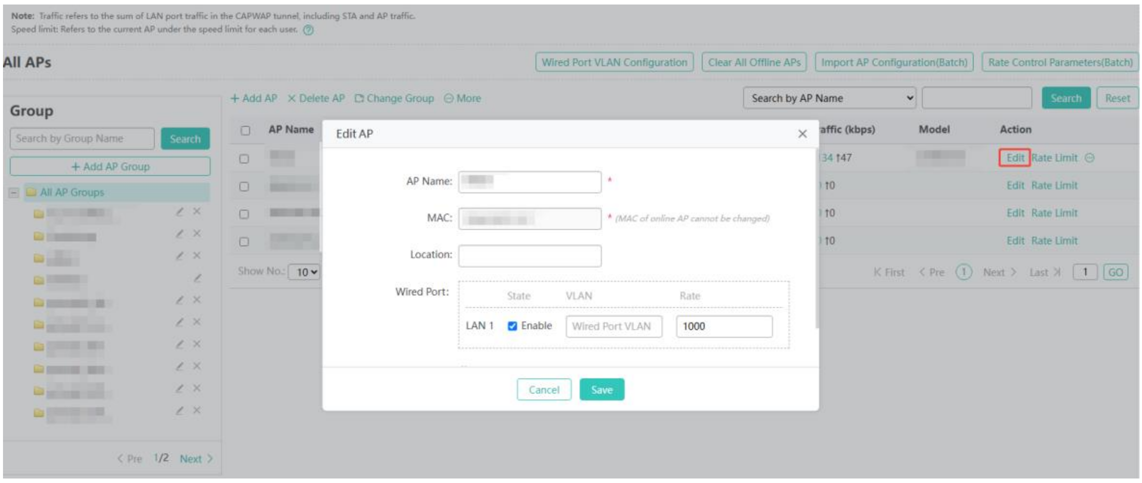
(3) Adding APs: Click **+ Add AP** to add APs to a specific AP group. The **AP Name** and **MAC** fields are mandatory while other fields are optional. Click **OK** and the AP will be displayed in the AP list after a message indicating operation success appears.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

Parameter	Description
AP Name	Enter the name of the AP. If the AP is offline, the AP name cannot be edited.
MAC	Enter the MAC address of the AP. The MAC address cannot be edited if the AP is online.
Location	Enter the location of the AP. For instance, if the AP is deployed in Room 201 on the 19th floor, enter **19#201** in this field.
AP Group	AP group to which an AP belongs. An AP belongs to the default group by default and can belong to only one AP group.
Telnet Account	Enter the account for logging into the AP. Both Telnet account and password are mandatory.
Telnet Password	Enter the password for logging into the AP. Both Telnet account and password are mandatory.
Tunnel IP	The tunnel IP address is the loopback port IP address. It is configured on the AP to quickly locate the AC for connection. The tunnel IP address must be the same as the one configured on the WiFi/WLAN Settings page.

(4) Editing APs: Click **Edit** in the **Action** column of an AP and edit the AP information in the pop-up window. Click **Save** and a message indicating operation success is displayed.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

(MAC of online AP cannot be changed)

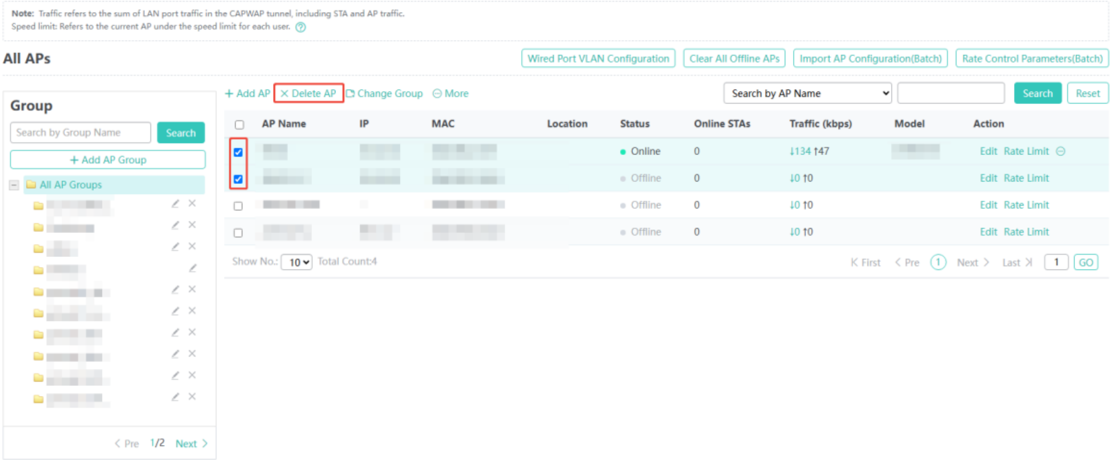
State	VLAN	Rate
LAN 1 ☑ Enable	Wired Port VLAN	1000

Parameter	Description
Wired Port	The wired port is enabled by default.
AP over IPv4	The AP can be assigned with an IP address through DHCP. You can also configure a static IP address, which requires the configuration of the gateway address, tunnel IP address, IPv4 address, and IPv4 subnet mask. You can configure the IPv4 address, IPv4 subnet mask, and IPv4 gateway by running the **ip address 2.2.2.2 255.255.255.0 2.2.2.1** command. **Caution** This configuration may cause an AP disconnection.
AP IPv4 Mask	
AP IPv4 Gateway	
Offline SSID	Enter the SSID broadcast by the AP when it is disconnected.
Hide Offline SSID	Display or hide the SSID broadcast by the AP when it is disconnected.

Note

- The **Edit AP** window displays the configurations instead of the AP status. Run the **show ap-config running +name** command to display the configurations.
- The AP list displays the AP status through the **getAPList**.

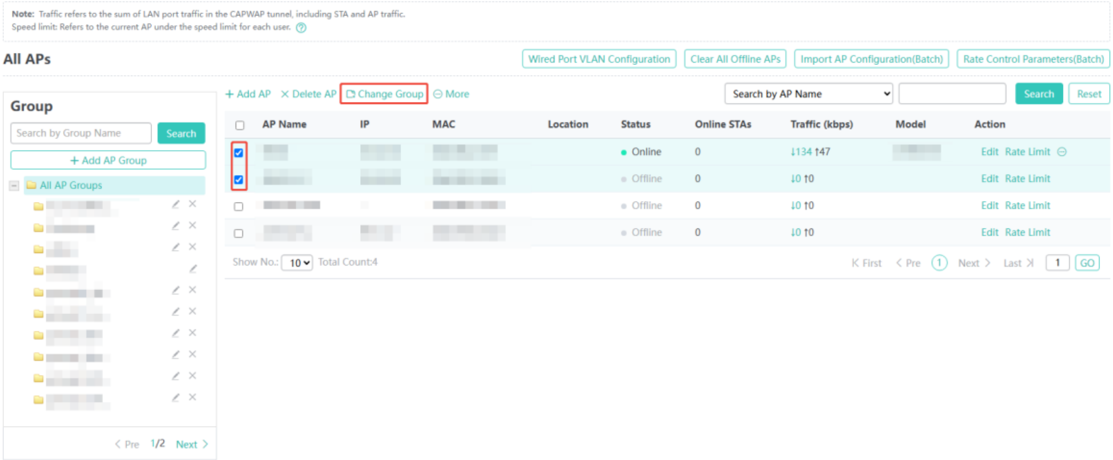
(5) Deleting APs: Select one or multiple items in the AP list and click **X Delete AP**. Click **OK** in the pop-up window to batch delete the APs.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

□	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
☑	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit
☑	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]		[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit

(6) Modifying AP groups: Select one or more entries in the AP list and click **Change Group**. In the displayed dialog box, modify the AP group to which the APs belong and click **Save**.



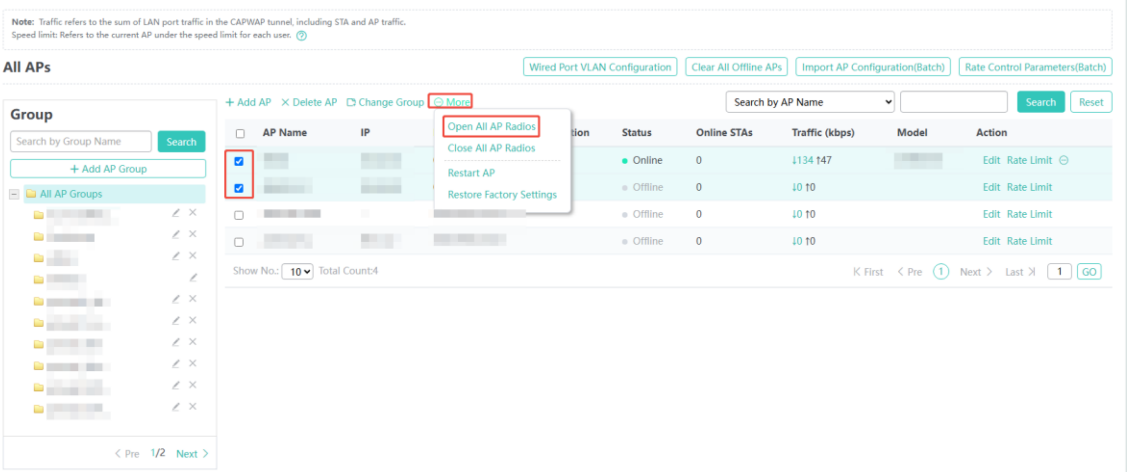
Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user. ⓘ

All APs

☐	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
☑	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit ⊖
☑	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]		[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit

Show No.: 10 Total Count:4 K First 〈 Pre 1 Next 〉 Last >| 1 GO

(7) Enabling all AP radios: Select one or more entries in the AP list, click ⊖ More, and select **Open All AP Radios** to batch enable all the AP radios.



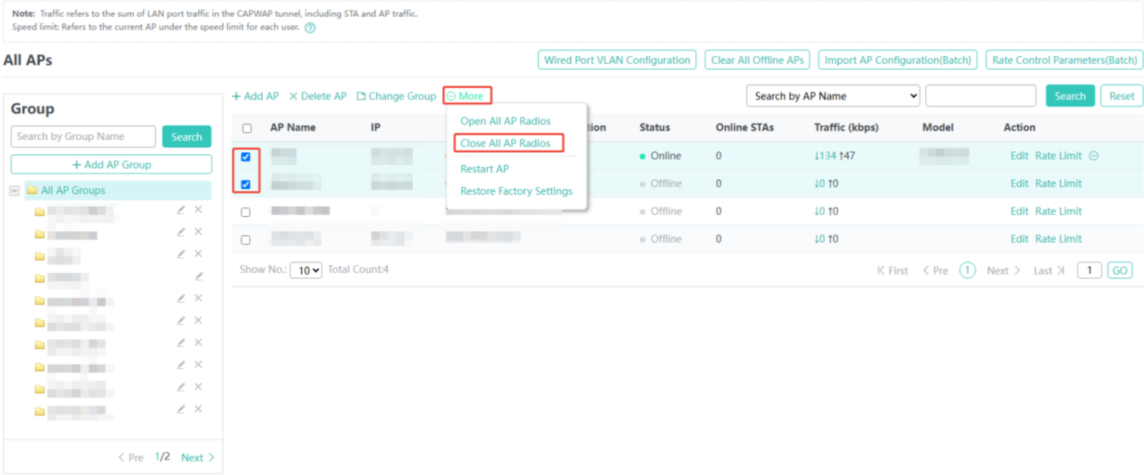
Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user. ⓘ

All APs

☐	AP Name	IP	tion	Status	Online STAs	Traffic (kbps)	Model	Action
☑	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit ⊖
☑	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]			● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit

Show No.: 10 Total Count:4 K First 〈 Pre 1 Next 〉 Last >| 1 GO

(8) Disabling all AP radios: Select one or more entries in the AP list, click ⊖ More, and select **Close All AP Radios** to batch disable all the AP radios.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user. ⓘ

All APs

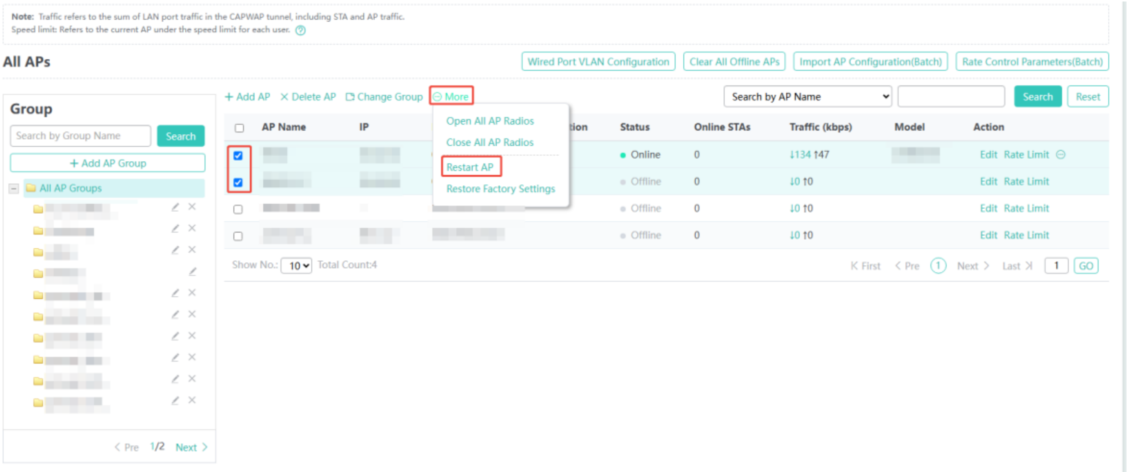
☐	AP Name	IP	tion	Status	Online STAs	Traffic (kbps)	Model	Action
☑	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit ⊖
☑	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]			● Offline	0	↓0 ↑0		Edit Rate Limit
☐	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit

Show No.: 10 Total Count:4 K First 〈 Pre 1 Next 〉 Last >| 1 GO

(9) Restarting APs: Select one or more entries in the AP list, click ⊖ More, and select **Restart AP** to batch restart the selected APs. In the dialog box that is displayed, click **OK**.

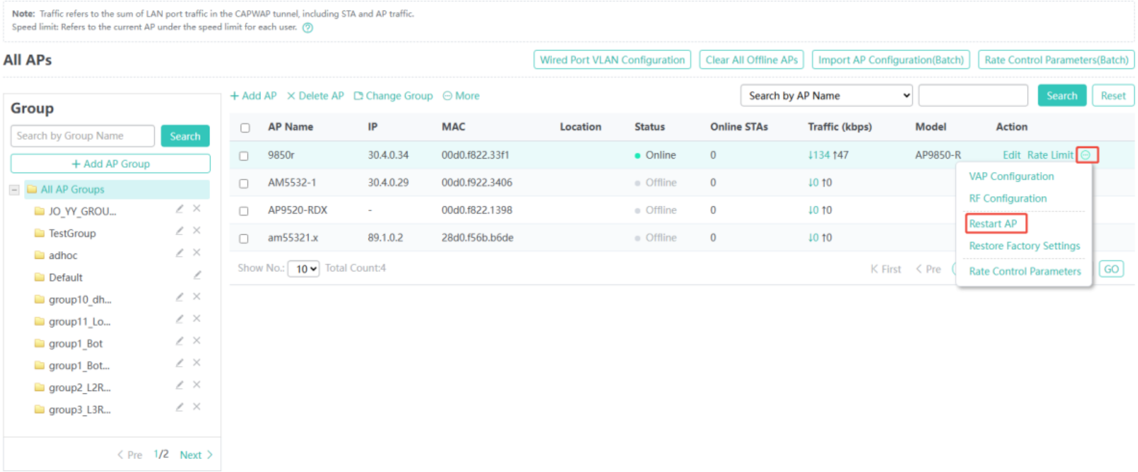
Caution

AP restart may disconnect STAs connecting to the AP. Exercise caution when you perform this operation.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

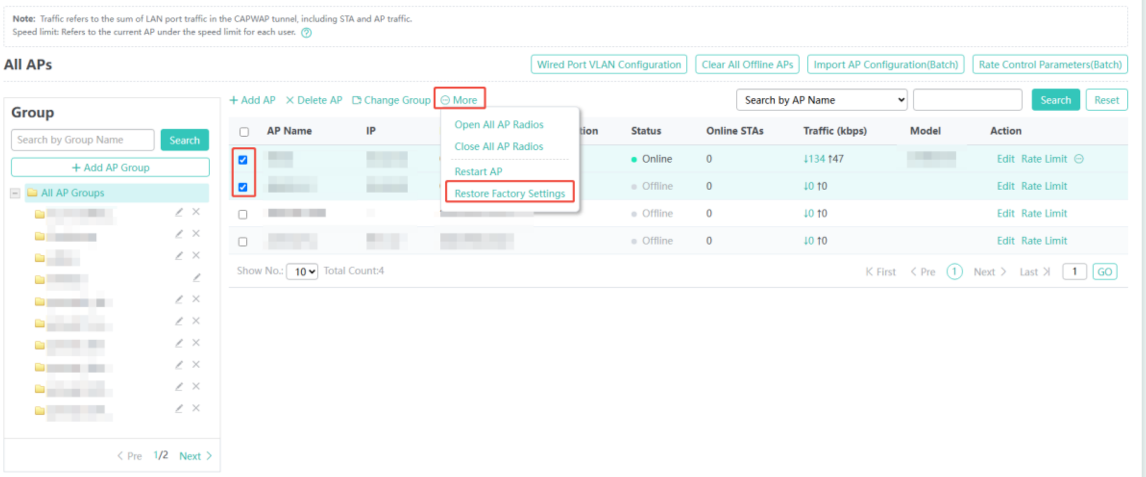
You can also click ⊖ in the **Action** column of an AP and click **Restart AP**. In the dialog box that is displayed, click **OK** to restart a single AP.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

☐	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
☐	9850r	30.4.0.34	00d0.f822.33f1		● Online	0	↓134 ↑47	AP9850-R	Edit Rate Limit ⊖
☐	AM5532-1	30.4.0.29	00d0.f922.3406		● Offline	0	↓0 ↑0		
☐	AP9520-RDX	-	00d0.f822.1398		● Offline	0	↓0 ↑0		
☐	am55321.x	89.1.0.2	28d0.f56b.b6de		● Offline	0	↓0 ↑0		

(10) Restoring factory settings: Select one or more entries in the AP list, click ⊖ More, and select **Restore Factory Settings** to batch restore the selected APs to factory settings. In the dialog box that is displayed, click **OK**.

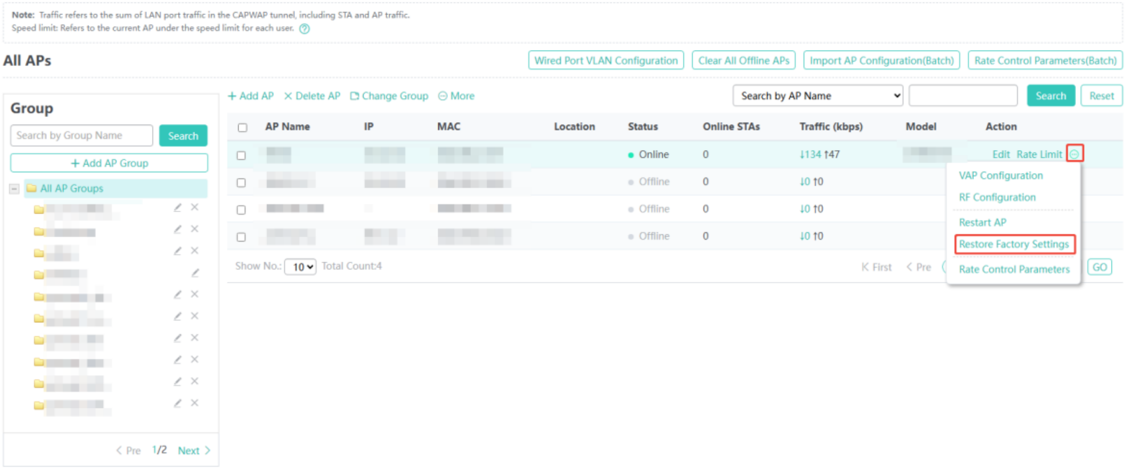


Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

	AP Name	IP	Status	Online STAs	Traffic (kbps)	Model	Action
☑	[redacted]	[redacted]	● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit
☑	[redacted]	[redacted]	● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]	[redacted]	● Offline	0	↓0 ↑0		Edit Rate Limit

Show No.: 10 Total Count:4

You can also click ⊖ in the **Action** column of an AP and click **Restore Factory Settings**. In the dialog box that is displayed, click **OK** to restore a single AP to factory settings.

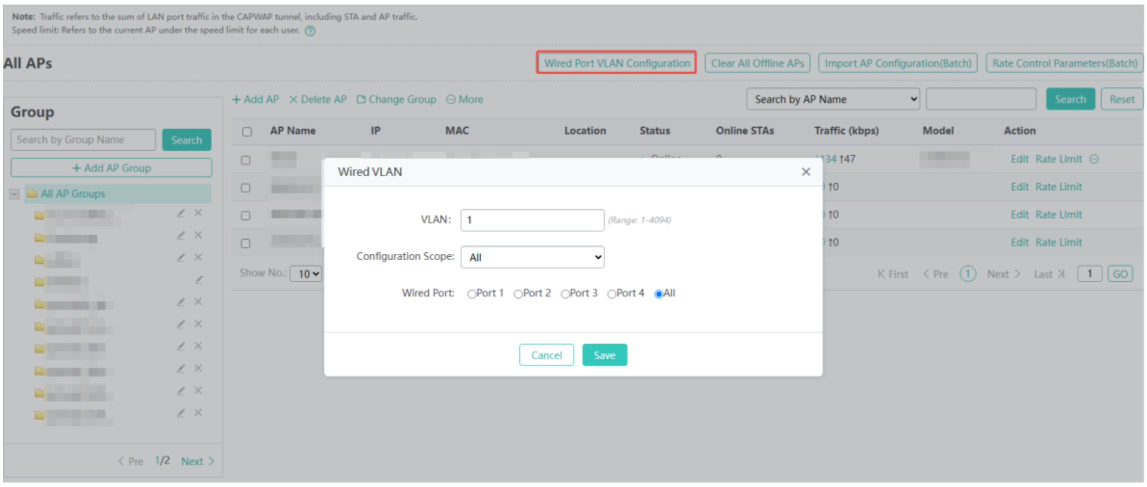


Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
□	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		
□	[redacted]		[redacted]		● Offline	0	↓0 ↑0		
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		

Show No.: 10 Total Count:4

(11) Configuring wired VLAN: Click **Wired Port VLAN Configuration** and the **Wired VLAN** window pops up. Enter the VLAN ID, select the wired port, and click **Save**.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

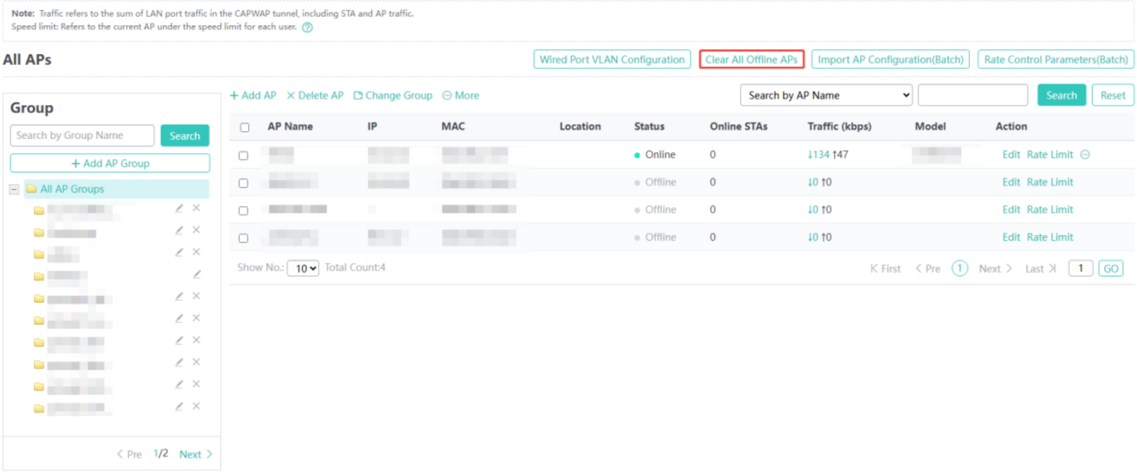
Wired VLAN

VLAN: 1 (Range: 1-4094)

Configuration Scope: All

Wired Port: ○Port 1 ○Port 2 ○Port 3 ○Port 4 ●All

(12) Deleting offline APs: Click **Clear All Offline APs** to delete all offline APs.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

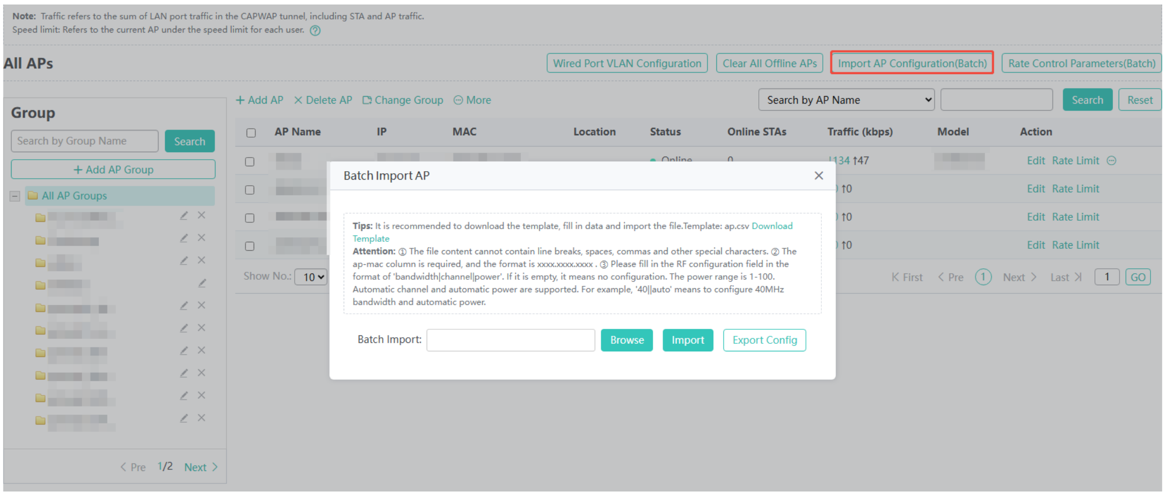
□	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
□	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]		[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit

Show No.: 10 Total Count:4

(13) Batch importing APs: Click **Import AP Configuration(Batch)**. In the **Batch Import AP** window that is displayed, batch modify or add AP configurations.

- If you want to batch modify the AP configurations, click **Export Config** to export the current AP configuration data. Modify the configurations in the exported file and then click **Import** to import the modified file. AP configurations are modified in batches.

If you want to add multiple AP configuration records, click **Download Template** to obtain the standard template file. Enter the AP configurations in the template file and then upload the template file. AP configuration records are added in batches.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

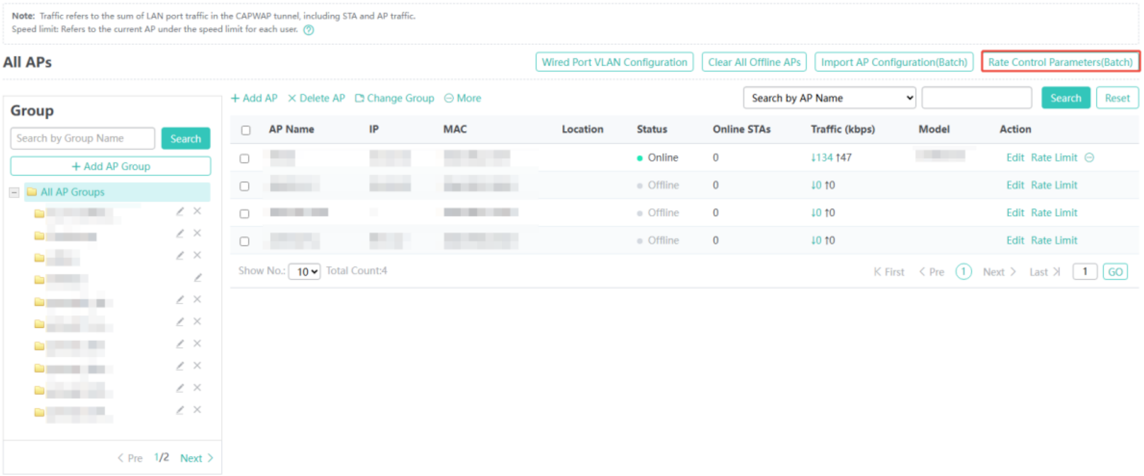
Batch Import AP

Tips: It is recommended to download the template, fill in data and import the file.Template: ap.csv Download Template

Attention: ① The file content cannot contain line breaks, spaces, commas and other special characters. ② The ap-mac column is required, and the format is xxxx.xxxx.xxxx . ③ Please fill in the RF configuration field in the format of 'bandwidth|channel|power'. If it is empty, it means no configuration. The power range is 1-100. Automatic channel and automatic power are supported. For example, '40||auto' means to configure 40MHz bandwidth and automatic power.

Batch Import:

(14) Batch configuring rate control parameters: Click **Rate Control Parameters(Batch)**. On the **Rate Control Parameter Configuration** page that is displayed, configure the rate control parameters for different frequency bands in each configuration mode.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

All APs

Wired Port VLAN Configuration | Clear All Offline APs | Import AP Configuration(Batch) | Rate Control Parameters(Batch)

Group

Search by Group Name | Search

+ Add AP Group

All AP Groups

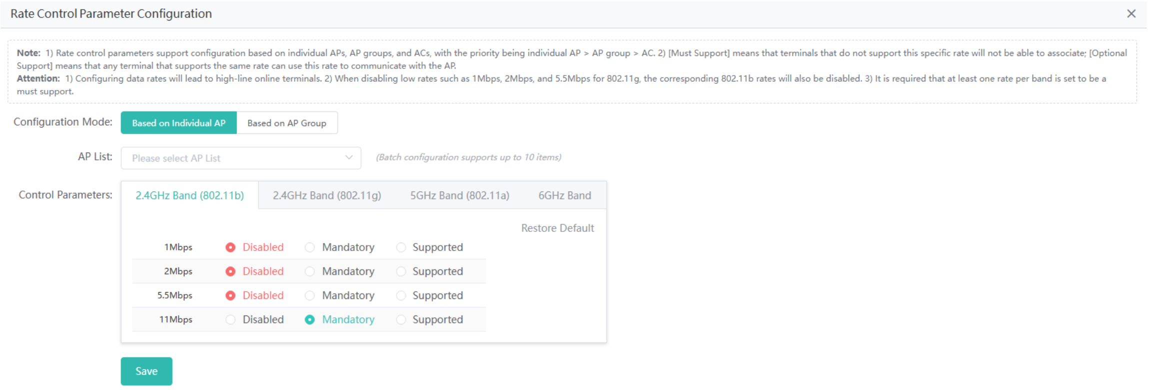
[redacted]

< Pre 1/2 Next >

+ Add AP | × Delete AP | Change Group | More | Search by AP Name | Search | Reset

□	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
□	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]		[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		Edit Rate Limit

Show No.: 10 Total Count:4 | First | Pre | 1 | Next | Last | 1 | GO



Rate Control Parameter Configuration

Note: 1) Rate control parameters support configuration based on individual APs, AP groups, and ACs, with the priority being individual AP > AP group > AC. 2) [Must Support] means that terminals that do not support this specific rate will not be able to associate; [Optional Support] means that any terminal that supports the same rate can use this rate to communicate with the AP.
Attention: 1) Configuring data rates will lead to high-line online terminals. 2) When disabling low rates such as 1Mbps, 2Mbps, and 5.5Mbps for 802.11g, the corresponding 802.11b rates will also be disabled. 3) It is required that at least one rate per band is set to be a must support.

Configuration Mode: Based on Individual AP | Based on AP Group

AP List: Please select AP List *(Batch configuration supports up to 10 items)*

Control Parameters: 2.4GHz Band (802.11b) | 2.4GHz Band (802.11g) | 5GHz Band (802.11a) | 6GHz Band

Restore Default

1Mbps	● Disabled	○ Mandatory	○ Supported
2Mbps	● Disabled	○ Mandatory	○ Supported
5.5Mbps	● Disabled	○ Mandatory	○ Supported
11Mbps	○ Disabled	● Mandatory	○ Supported

Save

Parameter	Description
Configuration Mode	Select a configuration mode, which can be **Based on Individual AP** or **Based on AP Group**. Individual AP has a higher priority than AP group.
AP List/AP Group List	Select an individual AP or an AP group that you want to configure. Batch configuration supports up to 10 APs.
Control Parameters	Configure the rate for STAs in different bands to communicate with the AP. ● Mandatory: The STA must support the specified rate. Otherwise, the STA cannot associate with the AP. ● Supported: Any STA supporting the specified rate can communicate with the AP at the rate. ● Disabled: STAs cannot establish connections to the AP or transmit data to the AP at the specified rate.

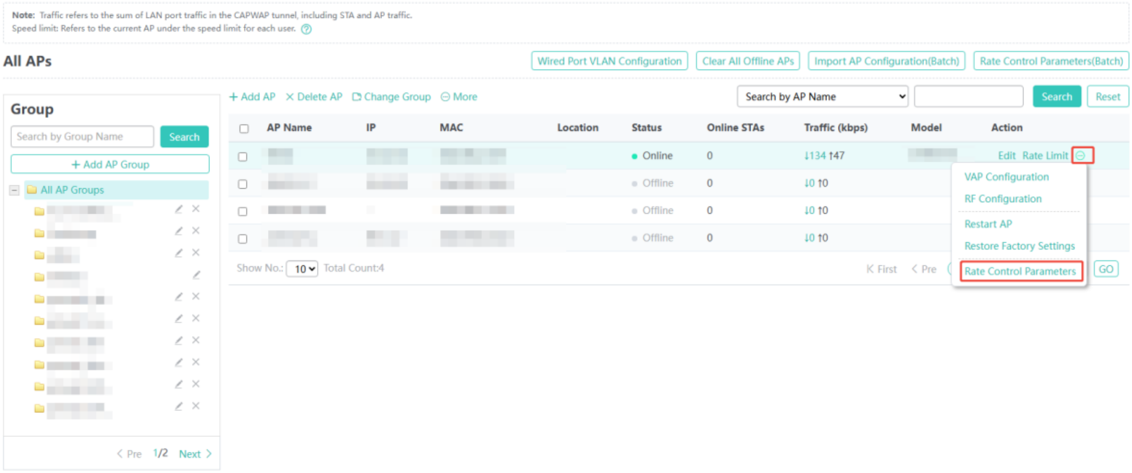
Caution

- Rate control settings will cause online STAs to go offline.
- If you disable the low rate sets, such as 1 Mbps, 2 Mbps, and 5.5 Mbps for the 2.4 GHz band (802.11g), these low rate sets are also disabled for the 2.4 GHz band (802.11b).
- At least one rate must be set as **Mandatory** for each band.

To configure rate control parameters for a single AP, click ⊖ in the **Action** column of the AP and select **Rate Control Parameters**. On the **Rate Control Parameter Configuration** page that is displayed, configure rate control parameters for the AP.

Note

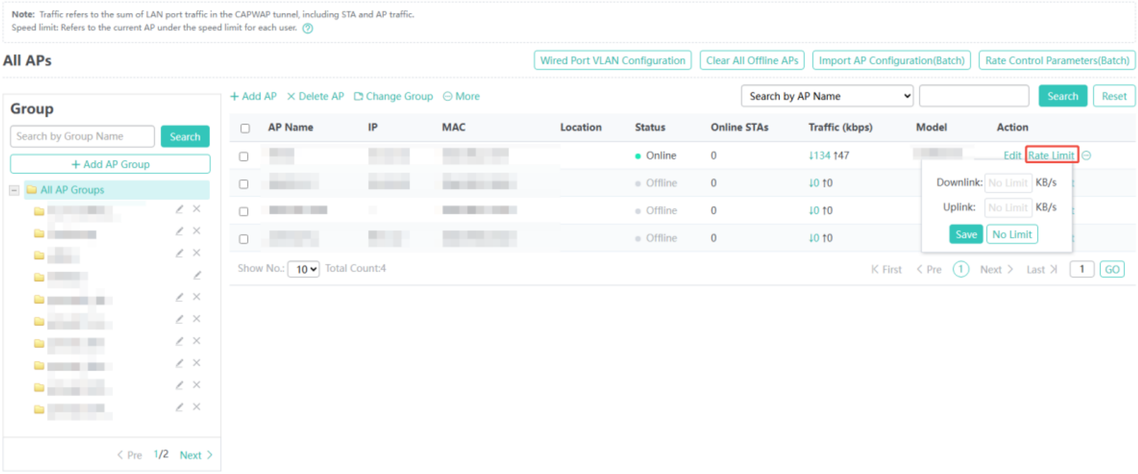
You can configure rate control parameters for APs one by one only when they are online.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

□	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
□	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit ⊖
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		
□	[redacted]		[redacted]		● Offline	0	↓0 ↑0		
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		

(15) Rate limiting: Click **Rate Limit** in the **Action** column to configure the uplink and downlink rate limits.



Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

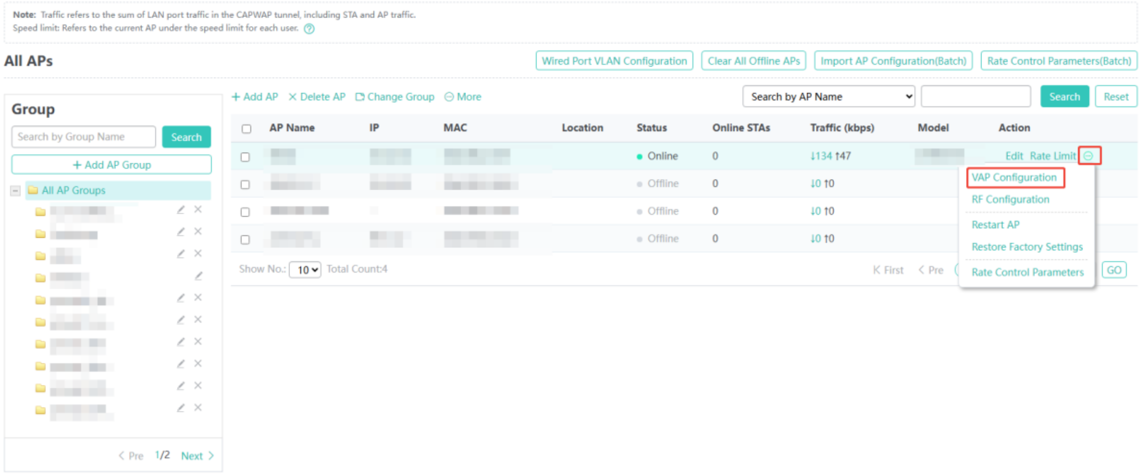
□	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
□	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit ⊖
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		
□	[redacted]		[redacted]		● Offline	0	↓0 ↑0		
□	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		

Downlink: No Limit KB/s
Uplink: No Limit KB/s

(16) Configuring VAP: To configure the VAP, click ⊖ in the **Action** column of the AP and select **VAP Configuration**. On the **Configure AP** page that is displayed, click **Apply Template**, select a template name, set the virtual AP ID, and then click **OK**.

Note

Only online APs support VAP configuration. Some APs do not support this feature, depending on whether the **VAP Configuration** menu is available on the GUI.

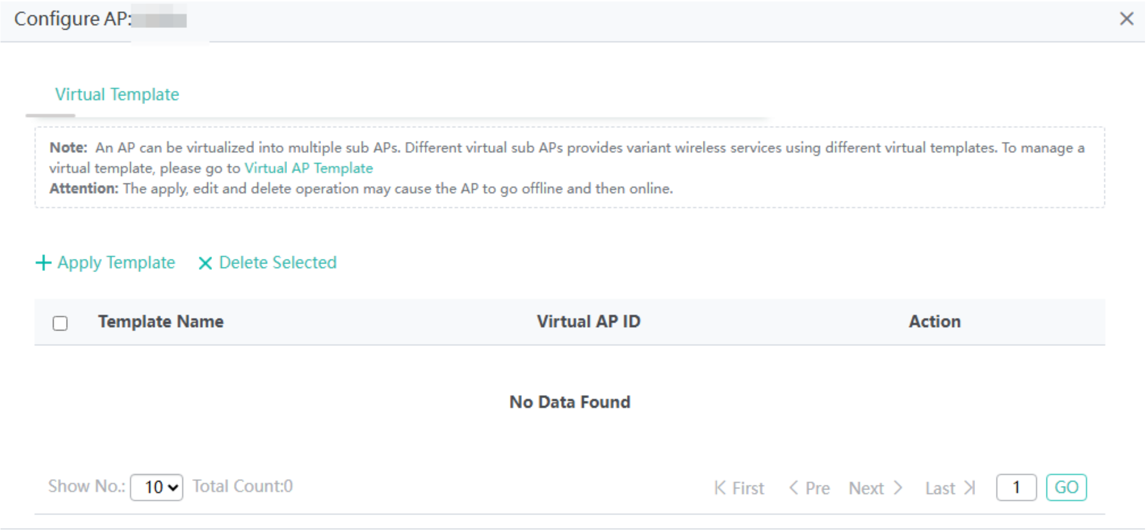


Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

All APs

☐	AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
☐	[redacted]	[redacted]	[redacted]		● Online	0	↓134 ↑47	[redacted]	Edit Rate Limit ⊝
☐	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		
☐	[redacted]		[redacted]		● Offline	0	↓0 ↑0		
☐	[redacted]	[redacted]	[redacted]		● Offline	0	↓0 ↑0		

Show No.: 10 Total Count:4



Configure AP: [redacted]

Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates. To manage a virtual template, please go to Virtual AP Template
Attention: The apply, edit and delete operation may cause the AP to go offline and then online.

☐	Template Name	Virtual AP ID	Action

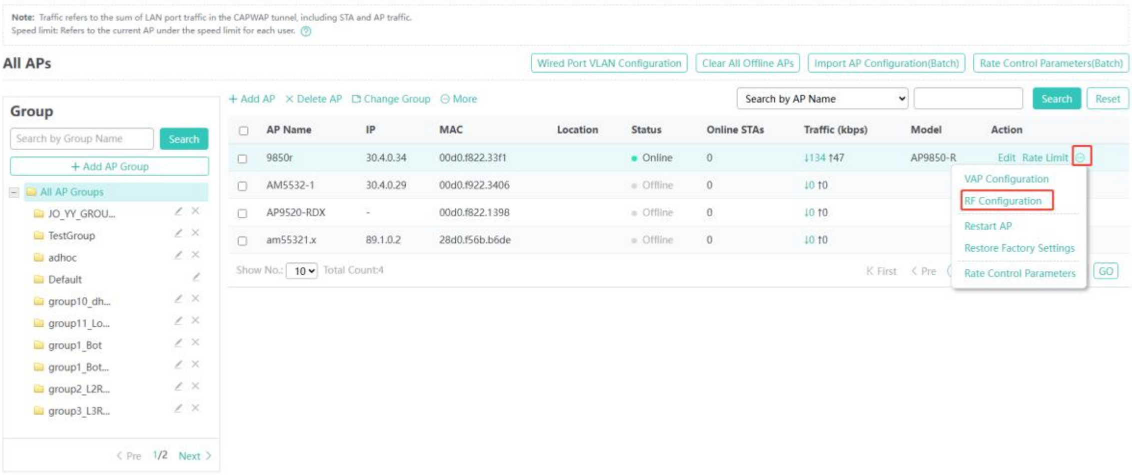
No Data Found

Show No.: 10 Total Count:0

(17) Click ⊝ in the **Action** column of the AP and select **RF Configuration**. On the **WiFi Radio Settings** page that is displayed, click the radio tabs to configure parameters for the radios.

Note

Only online APs support radio configuration.

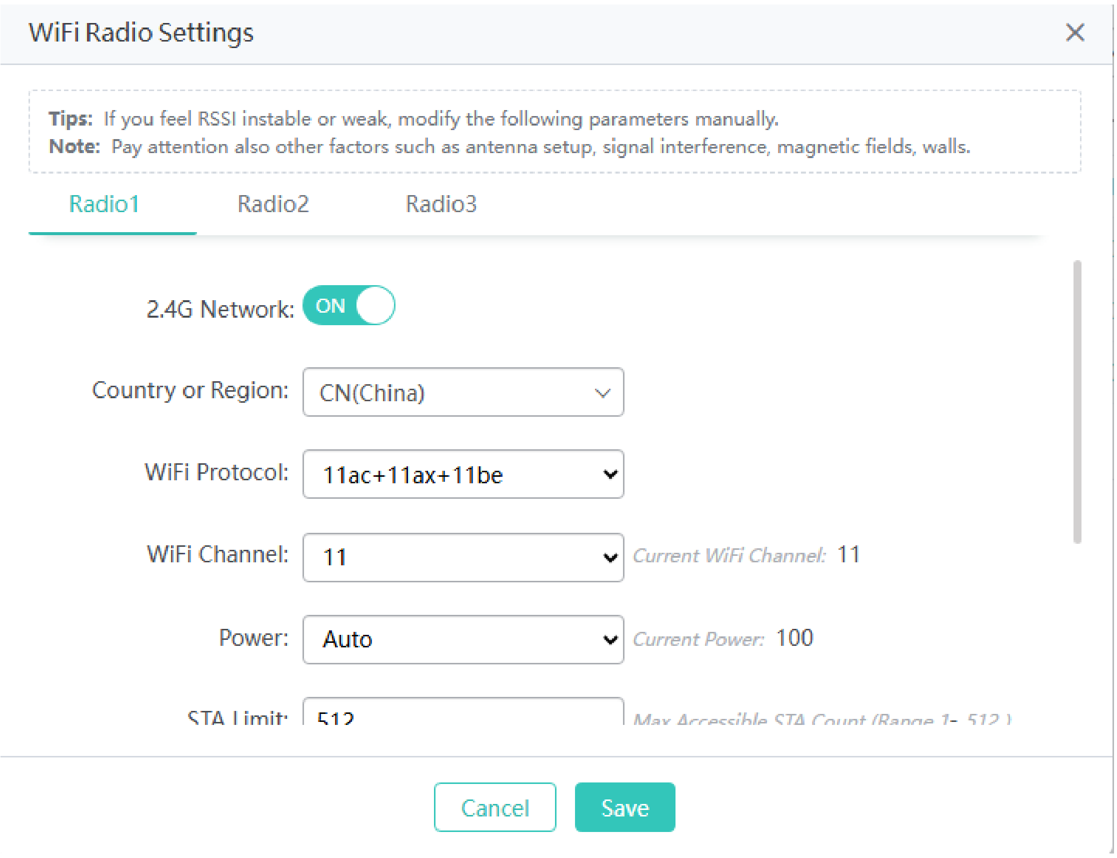


Note: Traffic refers to the sum of LAN port traffic in the CAPWAP tunnel, including STA and AP traffic.
Speed limit: Refers to the current AP under the speed limit for each user.

All APs

AP Name	IP	MAC	Location	Status	Online STAs	Traffic (kbps)	Model	Action
9850r	30.4.0.34	00d0.f822.33f1		Online	0	↓134 ↑47	AP9850-R	Edit Rate Limit
AM5532-1	30.4.0.29	00d0.f922.3406		Offline	0	↓0 ↑0		
AP9520-RDX	-	00d0.f822.1398		Offline	0	↓0 ↑0		
am55321.x	89.1.0.2	28d0.f56b.b6de		Offline	0	↓0 ↑0		

Show No.: 10 Total Count:4



WiFi Radio Settings

Tips: If you feel RSSI instable or weak, modify the following parameters manually.
Note: Pay attention also other factors such as antenna setup, signal interference, magnetic fields, walls.

2.4G Network: ON

Country or Region: CN(China)

WiFi Protocol: 11ac+11ax+11be

WiFi Channel: 11 *Current WiFi Channel:* 11

Power: Auto *Current Power:* 100

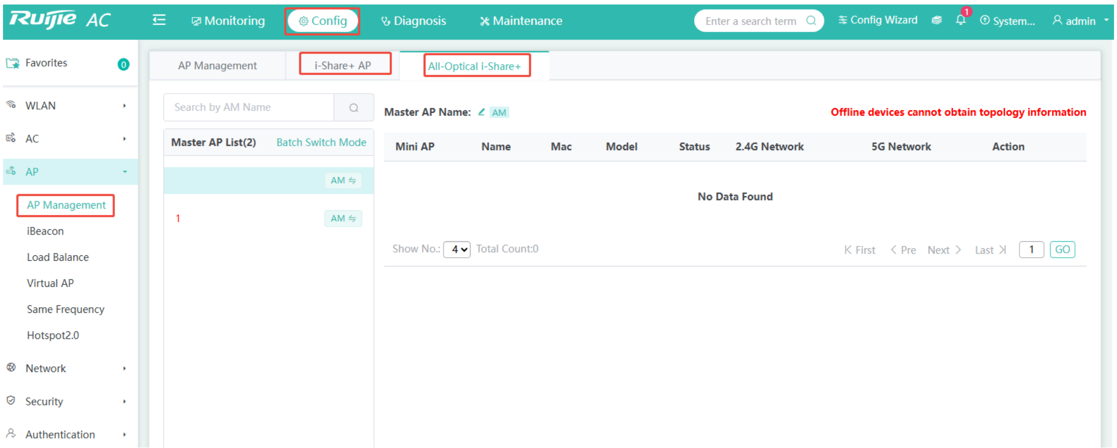
STA Limit: 512 *Max Accessible STA Count (Range 1- 512)*

Parameter	Description
RF Port	This field is displayed only when the AP has at least three radios.
2.4G Network	Enable or disable the radio.
5G Network	
6G Network	
Country or Region	Configure the country or region code for the AP.

WiFi Protocol	Select the IEEE 802.11 standard that the RF card complies with. The protocol options vary with networks. The actual web UI prevails. 11bgn, indicating IEEE 802.11b/g/n. 11bgn+11ax, indicating IEEE 802.11b/g/n/ax 11an, indicating IEEE 802.11a/n. 11an+11ac, indicating IEEE 802.11a/n/ac. 11an+11ac+11ax, indicating IEEE 802.11a/n/ac/ax.
WiFi Channel	Select the Wi-Fi channel based on the country or region and network type.
Power	Options: Auto: Auto Power Saving: The power value is 30. Standard: The power value is 80. Enhanced: The power value is 100. Custom: The power value is customized.
STA Limit	Configure the maximum number of STAs on the Wi-Fi radio.
Channel Bandwidth	Specify the channel bandwidth supported by the radio.
Receiving/Sending	Enable or disable the receive or transmit antenna.

2. i-Share+ AP/All-Optical i-Share+

The **i-Share+ AP** and **All-Optical i-Share+** tab pages display the list of all i-Share+ APs and all-optical i-Share+ master APs on the network and the information of each AP. A red icon indicates that a radio card is offline, and a black icon indicates that a radio card is online. Click the hostname of an online i-Share+ AP or all-optical i-Share+ master AP to display its details.

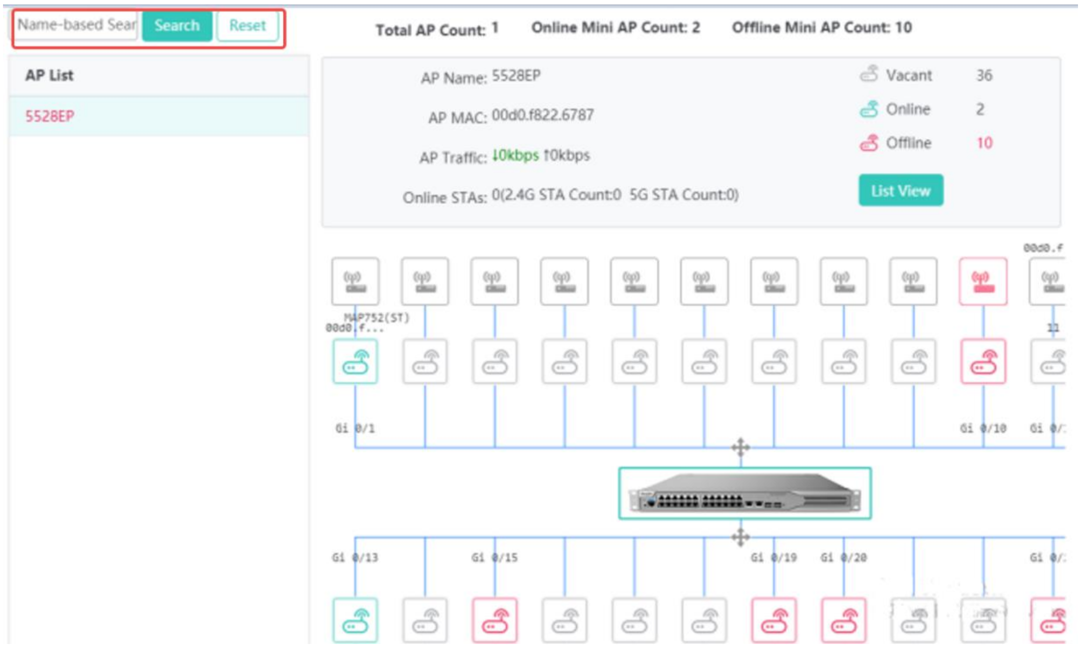


Offline devices cannot obtain topology information

No Data Found

The left pane displays the list of i-Share+ APs and all-optical i-Share+ master APs. The details on the selected AP are displayed on the right, which can be switched between the topology view and the list view.

(1) Searching for APs: Enter keywords and click **Search** to search for the specified APs.



Total AP Count: 1 Online Mini AP Count: 2 Offline Mini AP Count: 10

AP List

5528EP

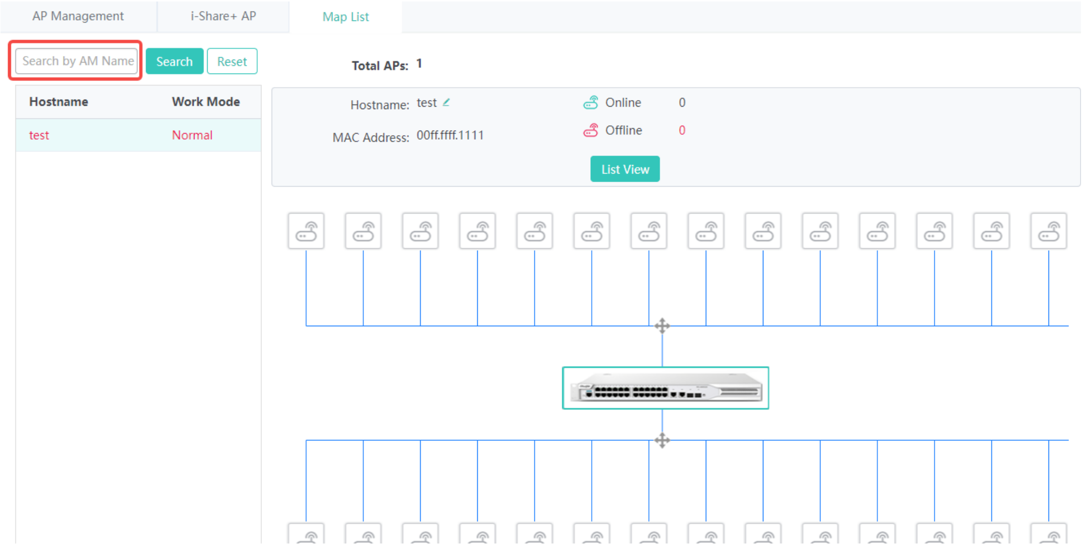
AP Name: 5528EP

AP MAC: 00d0.f822.6787

AP Traffic: ↓0kbps ↑0kbps

Online STAs: 0(2.4G STA Count:0 5G STA Count:0)

Vacant	36
Online	2
Offline	10



Total APs: 1

Hostname	Work Mode
test	Normal

Hostname: test

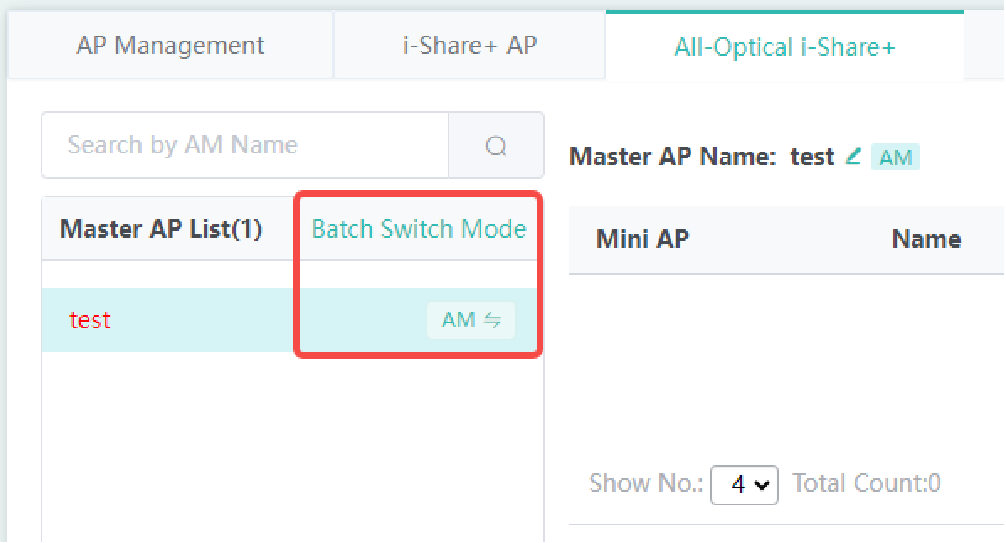
MAC Address: 00ff.ffff.1111

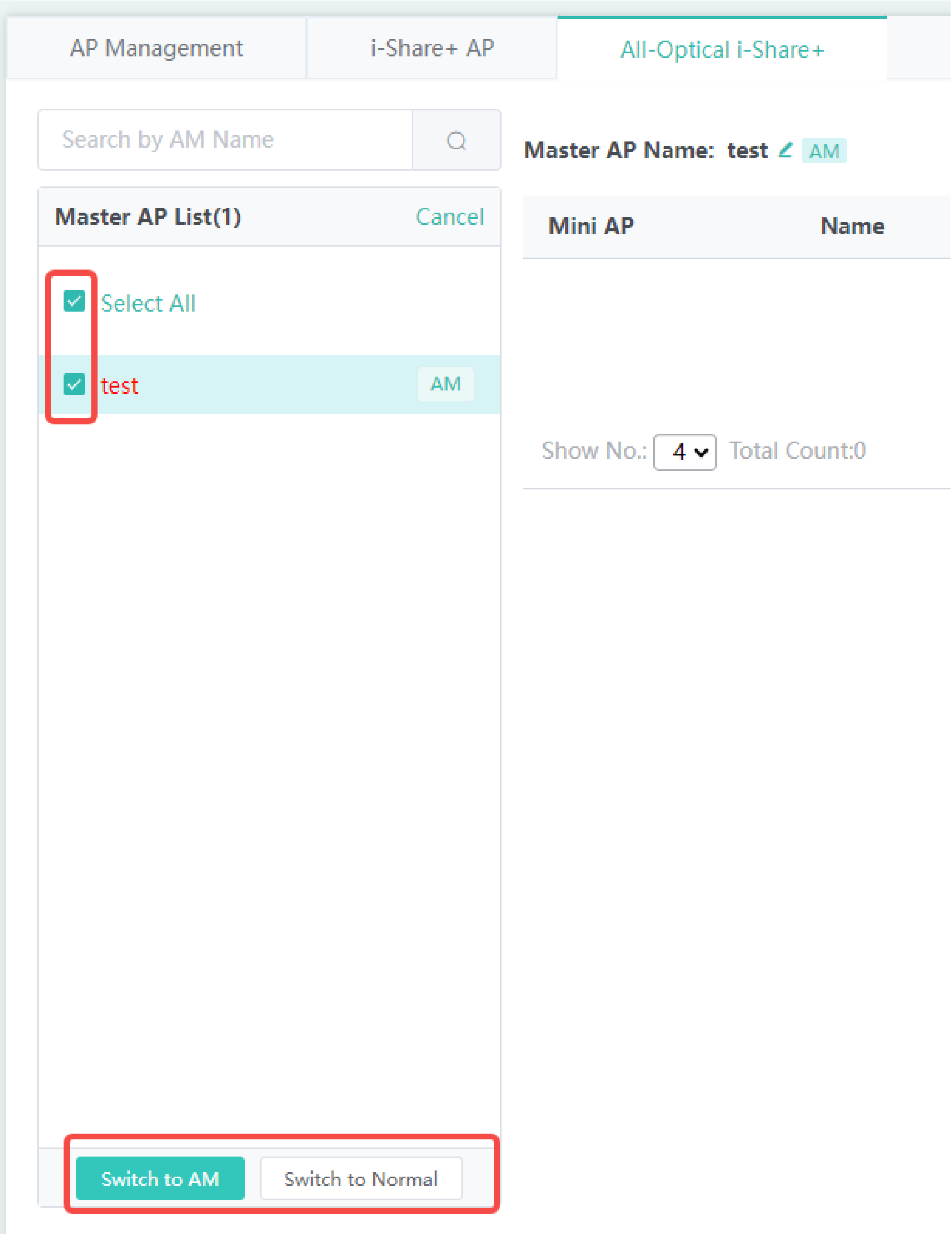
Online	0
Offline	0

(2) Switching modes. Click **AM** or **Normal** to switch the mode of a single AP. Alternatively, click **Batch Switch Mode** and select APs, and click **Switch to AM** or **Switch to Normal** to switch the mode of APs in batches.

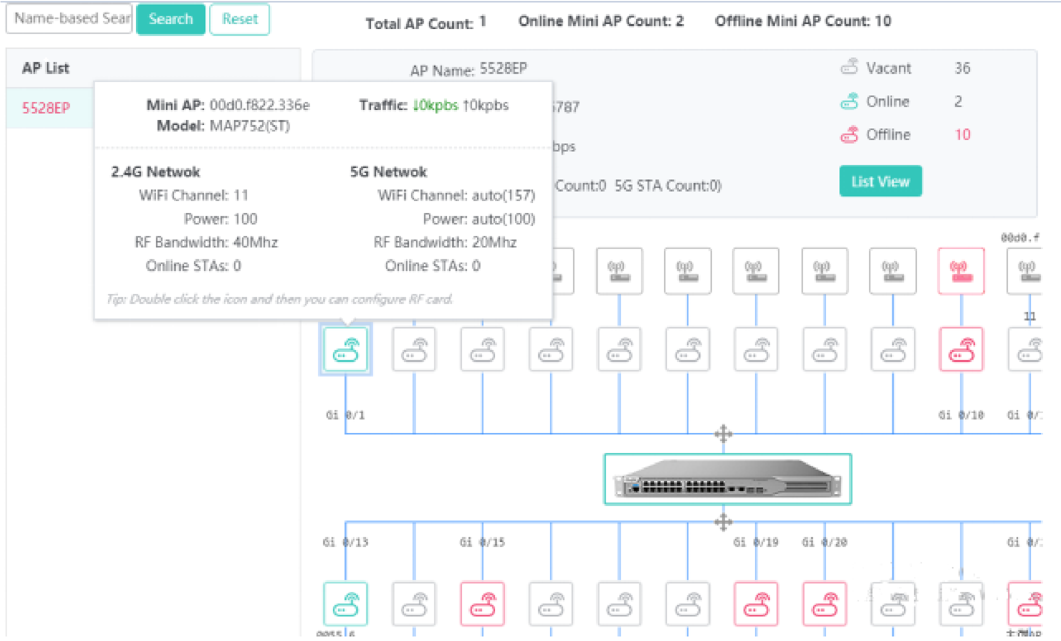
Note

- Mode switching is supported by only all-optical i-Share+ APs.
- The AM mode typically applies to scenarios of high density and with numerous barriers. iShare+ APs can work with and centrally manage micro APs to streamline network configurations and maintenance.
- The normal mode typically applies to traditional network architecture where APs are centrally managed on AC.


AP Management
i-Share+ AP
All-Optical i-Share+
Search by AM Name
Master AP Name: test
AM
Master AP List(1)
Batch Switch Mode
test
AM ⇋
Mini AP
Name
Show No.: 4
Total Count:0


AP Management
i-Share+ AP
All-Optical i-Share+
Search by AM Name
Master AP Name: test
AM
Master AP List(1)
Cancel
☑ Select All
☑ test
AM
Mini AP
Name
Show No.: 4
Total Count:0
Switch to AM
Switch to Normal

(3) Viewing RF details: Hover the cursor over the icon of the RF card to view the RF details. Double-click the RF card to configure it.



Name-based Sear Search Reset

Total AP Count: 1 Online Mini AP Count: 2 Offline Mini AP Count: 10

AP List

5528EP

AP Name: 5528EP

Vacant 36

Online 2

Offline 10

List View

Mini AP: 00d0.f822.336e Model: MAP752(ST)

Traffic: ↓0kpbs ↑0kpbs

2.4G Netwok

WiFi Channel: 11

Power: 100

RF Bandwidth: 40Mhz

Online STAs: 0

5G Netwok

WiFi Channel: auto(157)

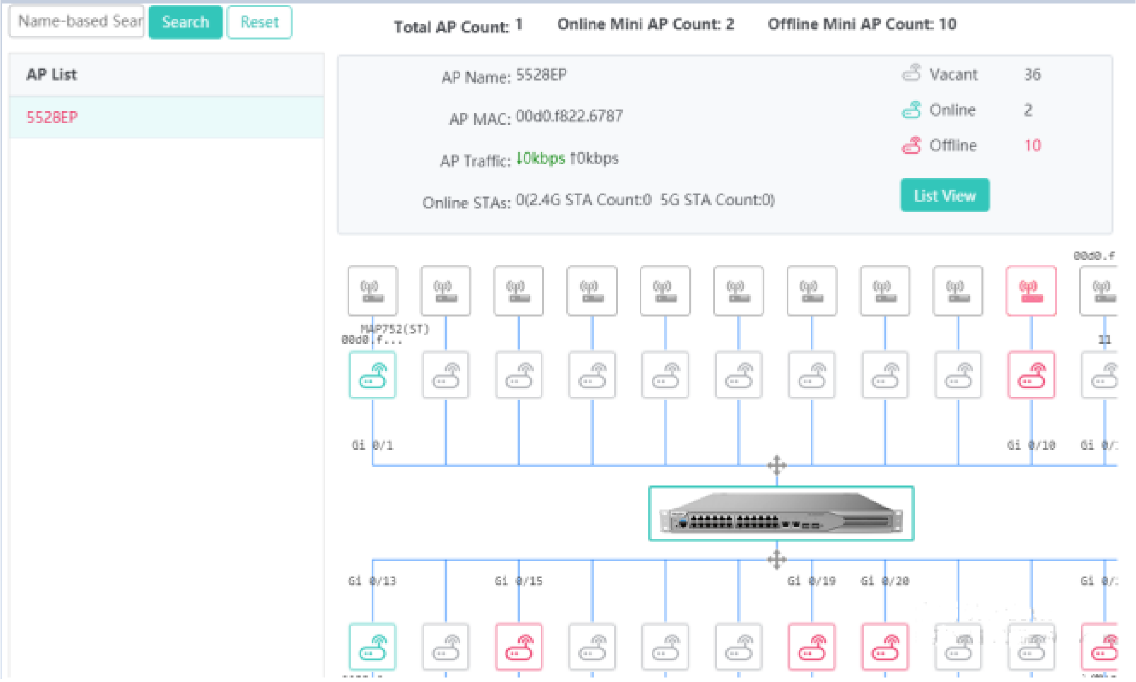
Power: auto(100)

RF Bandwidth: 20Mhz

Online STAs: 0

Tip: Double click the icon and then you can configure RF card.

(4) Switching views: Click **List View** to switch over to the list view.



Name-based Sear Search Reset

Total AP Count: 1 Online Mini AP Count: 2 Offline Mini AP Count: 10

AP List

5528EP

AP Name: 5528EP

AP MAC: 00d0.f822.6787

AP Traffic: ↓0kbps ↑0kbps

Online STAs: 0(2.4G STA Count:0 5G STA Count:0)

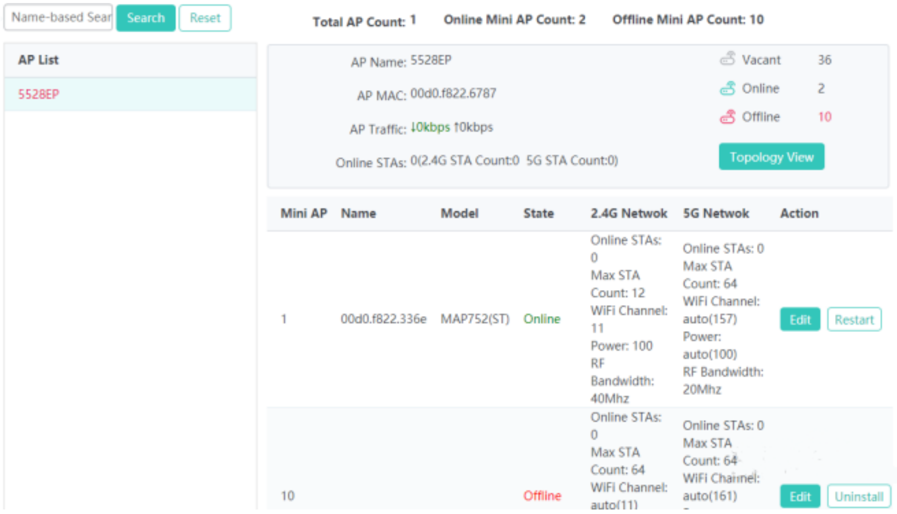
Vacant 36

Online 2

Offline 10

List View

(5) Configuring RF cards: Click **Edit** to configure the RF card. Click **Uninstall** to uninstall the offline RF card. Click **Restart** to restart the RF card.



Total AP Count: 1 Online Mini AP Count: 2 Offline Mini AP Count: 10

AP List

5528EP

AP Name: 5528EP

AP MAC: 00d0.f822.6787

AP Traffic: ↓0kbps ↑0kbps

Online STAs: 0(2.4G STA Count:0 5G STA Count:0)

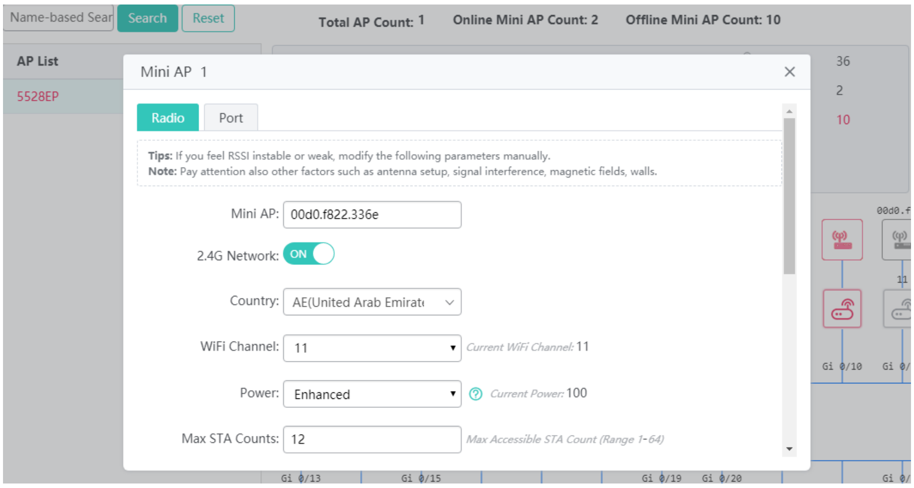
Vacant 36

Online 2

Offline 10

Mini AP	Name	Model	State	2.4G Netwok	5G Netwok	Action
1	00d0.f822.336e	MAP752(ST)	Online	Online STAs: 0 Max STA Count: 12 WiFi Channel: 11 Power: 100 RF Bandwidth: 40Mhz	Online STAs: 0 Max STA Count: 64 WiFi Channel: auto(157) Power: auto(100) RF Bandwidth: 20Mhz	Edit Restart
10			Offline	Online STAs: 0 Max STA Count: 64 WiFi Channel: auto(11)	Online STAs: 0 Max STA Count: 64 WiFi Channel: auto(161)	Edit Uninstall

Configuring RF cards:



Total AP Count: 1 Online Mini AP Count: 2 Offline Mini AP Count: 10

AP List

5528EP

Mini AP 1

Tips: If you feel RSSI instable or weak, modify the following parameters manually.
Note: Pay attention also other factors such as antenna setup, signal interference, magnetic fields, walls.

Mini AP: 00d0.f822.336e

2.4G Network: ON

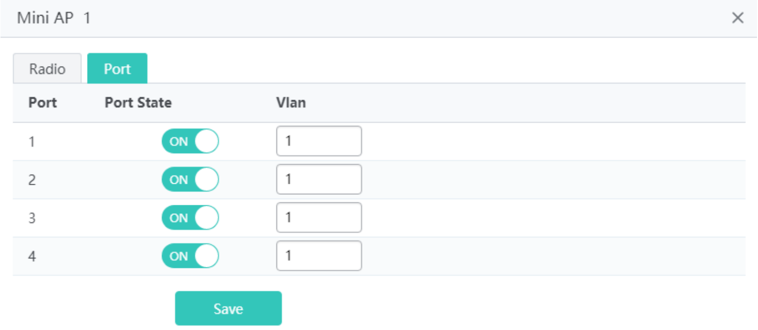
Country: AE(United Arab Emirate

WiFi Channel: 11 *Current WiFi Channel:* 11

Power: Enhanced *Current Power:* 100

Max STA Counts: 12 *Max Accessible STA Count (Range 1-64)*

(6) Configure the wired port of the RF card: The wired ports displayed here are subject to the device model.



Mini AP 1

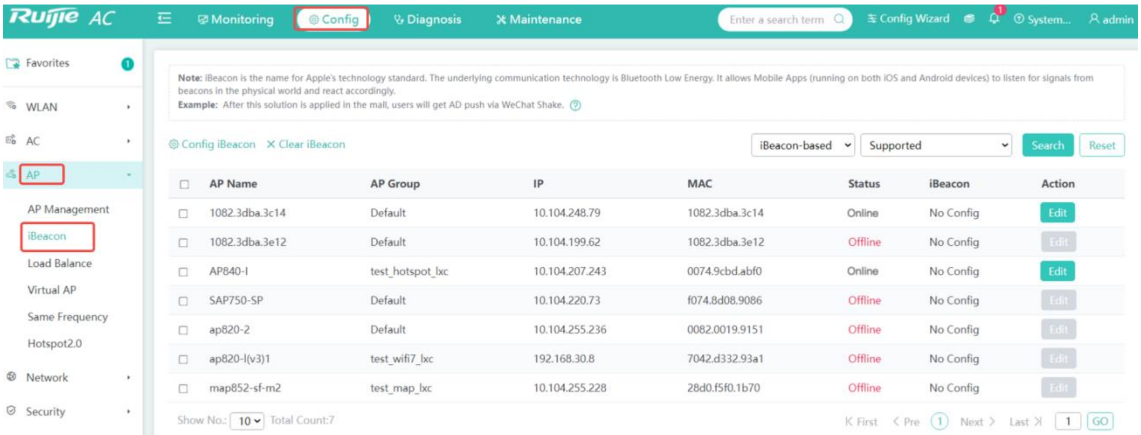
Port	Port State	Vlan
1	ON	1
2	ON	1
3	ON	1
4	ON	1

5.3.2 iBeacon

Choose **Config** > **AP** > **iBeacon**.

iBeacon is a protocol based on the Bluetooth Low Energy (BLE) technology. The APs enabled with iBeacon can broadcast a specified ID generated by a third party and the software on clients respond accordingly after receiving the ID.

Example: The shopping mall can apply iBeacon to push ads to customers when they use the Shake function on WeChat.



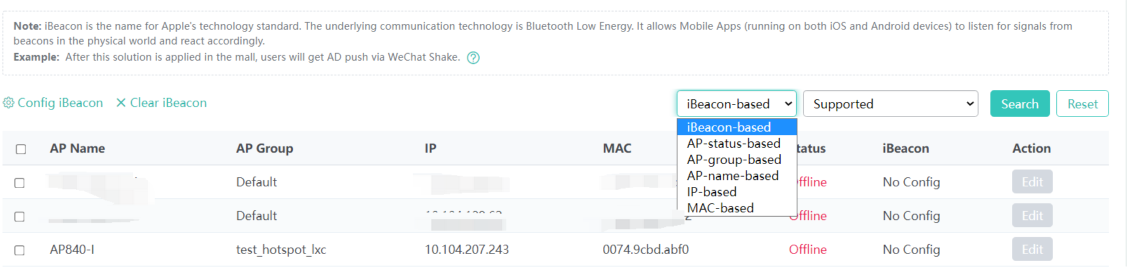
Note: iBeacon is the name for Apple's technology standard. The underlying communication technology is Bluetooth Low Energy. It allows Mobile Apps (running on both iOS and Android devices) to listen for signals from beacons in the physical world and react accordingly.
Example: After this solution is applied in the mall, users will get AD push via WeChat Shake.

Config iBeacon ✕ Clear iBeacon   iBeacon-based   Supported   Search   Reset

□	AP Name	AP Group	IP	MAC	Status	iBeacon	Action
□	1082.3dba.3c14	Default	10.104.248.79	1082.3dba.3c14	Online	No Config	Edit
□	1082.3dba.3e12	Default	10.104.199.62	1082.3dba.3e12	Offline	No Config	Edit
□	AP840-I	test_hotspot_lxc	10.104.207.243	0074.9cbd.abf0	Online	No Config	Edit
□	SAP750-SP	Default	10.104.220.73	f074.8d08.9086	Offline	No Config	Edit
□	ap820-2	Default	10.104.255.236	0082.0019.9151	Offline	No Config	Edit
□	ap820-I(v3)1	test_wifi7_lxc	192.168.30.8	7042.d332.93a1	Offline	No Config	Edit
□	map852-sf-m2	test_map_lxc	10.104.255.228	28d0.f5f0.1b70	Offline	No Config	Edit

Show No.: 10 Total Count:7   K First < Pre 1 Next > Last >| 1 GO

(1) Searching for APs: Search for APs using the filter or entering keywords. Click **Reset** to clear the search criteria.

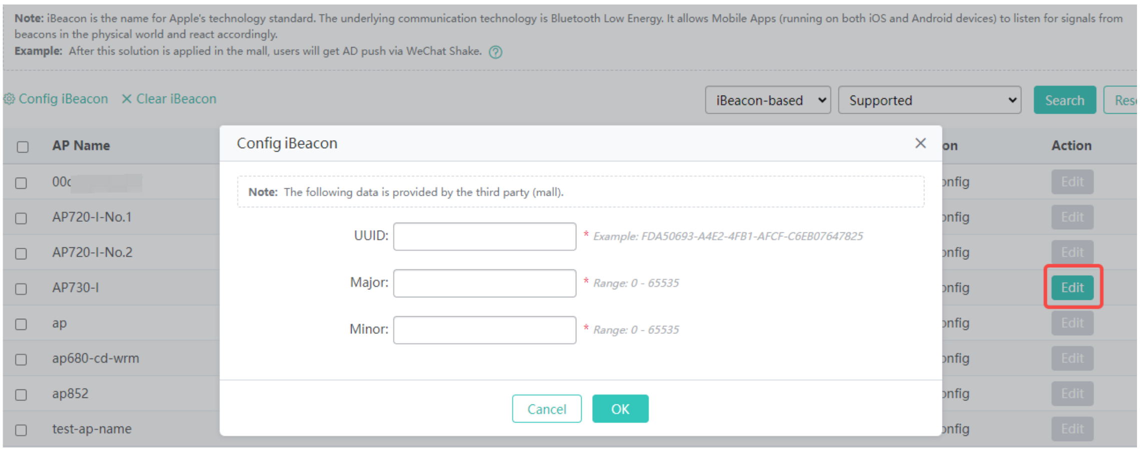


Note: iBeacon is the name for Apple's technology standard. The underlying communication technology is Bluetooth Low Energy. It allows Mobile Apps (running on both iOS and Android devices) to listen for signals from beacons in the physical world and react accordingly.
Example: After this solution is applied in the mall, users will get AD push via WeChat Shake.

Config iBeacon ✕ Clear iBeacon   iBeacon-based   Supported   Search   Reset

□	AP Name	AP Group	IP	MAC	tatus	iBeacon	Action
□	[redacted]	Default	[redacted]	[redacted]	ffline	No Config	Edit
□	[redacted]	Default	[redacted]	[redacted]	ffline	No Config	Edit
□	AP840-I	test_hotspot_lxc	10.104.207.243	0074.9cbd.abf0	Offline	No Config	Edit

(2) Configuring iBeacon: Click Edit in the **Action** column to enter the iBeacon configuration page. Fill in the parameters and click **Save**.



Note: iBeacon is the name for Apple's technology standard. The underlying communication technology is Bluetooth Low Energy. It allows Mobile Apps (running on both iOS and Android devices) to listen for signals from beacons in the physical world and react accordingly.
Example: After this solution is applied in the mall, users will get AD push via WeChat Shake.

Config iBeacon ✕ Clear iBeacon   iBeacon-based   Supported   Search   Res

□	AP Name	on	Action
□	00c [redacted]	nfig	Edit
□	AP720-I-No.1	nfig	Edit
□	AP720-I-No.2	nfig	Edit
□	AP730-I	nfig	Edit
□	ap	nfig	Edit
□	ap680-cd-wrm	nfig	Edit
□	ap852	nfig	Edit
□	test-ap-name	nfig	Edit

Config iBeacon ✕

Note: The following data is provided by the third party (mall).

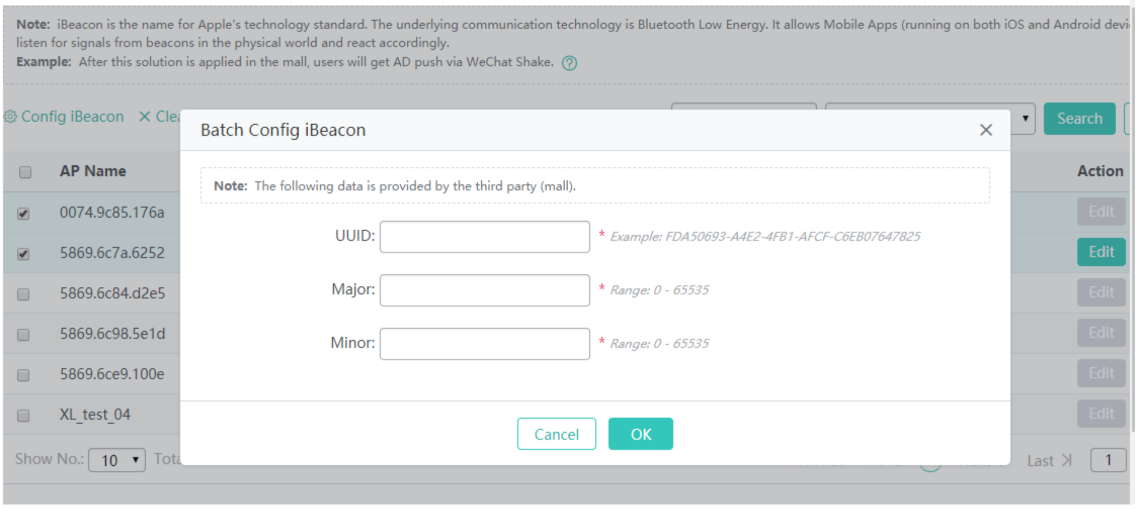
UUID: * *Example: FDA50693-A4E2-4FB1-AFCF-C6EB07647825*

Major: * *Range: 0 - 65535*

Minor: * *Range: 0 - 65535*

Cancel   OK

(3) Batch configuring iBeacon: Select the items in the list and edit the fields in the **Batch Config iBeacon** pop-up window.



Note: iBeacon is the name for Apple's technology standard. The underlying communication technology is Bluetooth Low Energy. It allows Mobile Apps (running on both iOS and Android devi
listen for signals from beacons in the physical world and react accordingly.
Example: After this solution is applied in the mall, users will get AD push via WeChat Shake.

Note: The following data is provided by the third party (mall).

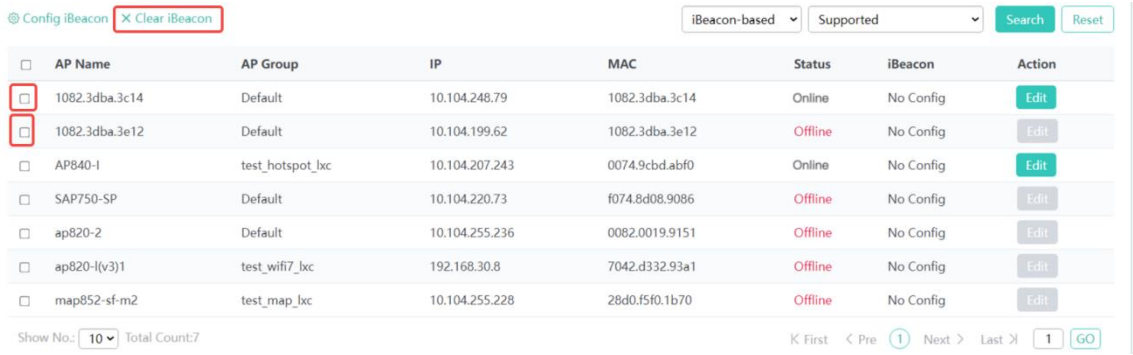
UUID: * Example: FDA50693-A4E2-4FB1-AFCF-C6EB07647825

Major: * Range: 0 - 65535

Minor: * Range: 0 - 65535

	AP Name	Action
☑	0074.9c85.176a	Edit
☑	5869.6c7a.6252	Edit
□	5869.6c84.d2e5	Edit
□	5869.6c98.5e1d	Edit
□	5869.6ce9.100e	Edit
□	XL_test_04	Edit

(4) Batching deleting iBeacon: Select the items in the list and click **Clear iBeacon**.

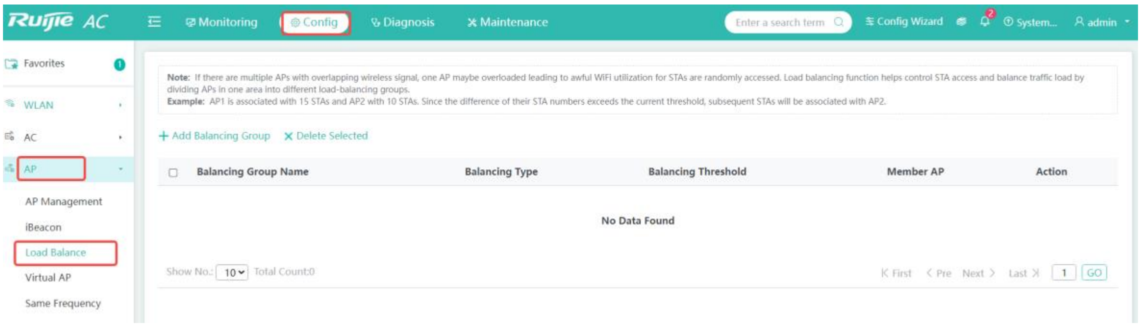


□	AP Name	AP Group	IP	MAC	Status	iBeacon	Action
□	1082.3dba.3c14	Default	10.104.248.79	1082.3dba.3c14	Online	No Config	Edit
□	1082.3dba.3e12	Default	10.104.199.62	1082.3dba.3e12	Offline	No Config	Edit
□	AP840-I	test_hotspot_lxc	10.104.207.243	0074.9cbd.abf0	Online	No Config	Edit
□	SAP750-SP	Default	10.104.220.73	f074.8d08.9086	Offline	No Config	Edit
□	ap820-2	Default	10.104.255.236	0082.0019.9151	Offline	No Config	Edit
□	ap820-I(v3)1	test_wifi7_lxc	192.168.30.8	7042.d332.93a1	Offline	No Config	Edit
□	map852-sf-m2	test_map_lxc	10.104.255.228	28d0.f5f0.1b70	Offline	No Config	Edit

5.3.3 Load Balance

Choose **Config** > **AP** > **Load Balance**.

If there are multiple APs on the WLAN, signal overlapping occurs. STAs are associated with APs randomly, leading to heavier load on some APs and poorer network utilization. To realize load balancing, assign the APs within an area into one group to coordinate STA access.

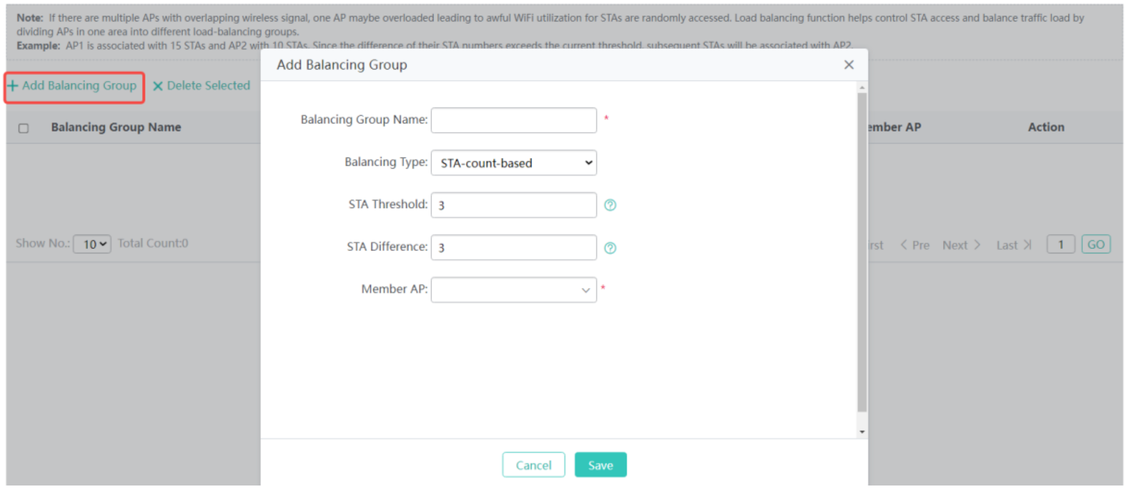


Note: If there are multiple APs with overlapping wireless signal, one AP maybe overloaded leading to awful WiFi utilization for STAs are randomly accessed. Load balancing function helps control STA access and balance traffic load by dividing APs in one area into different load-balancing groups.
Example: AP1 is associated with 15 STAs and AP2 with 10 STAs. Since the difference of their STA numbers exceeds the current threshold, subsequent STAs will be associated with AP2.

□	Balancing Group Name	Balancing Type	Balancing Threshold	Member AP	Action

No Data Found

(1) Adding balancing groups: Click **Add Balancing Group** and edit the fields in the pop-up window. Click **Save** and the balancing group will be displayed in the list after a message indicating operation success appears.



Note: If there are multiple APs with overlapping wireless signal, one AP maybe overloaded leading to awful WiFi utilization for STAs are randomly accessed. Load balancing function helps control STA access and balance traffic load by dividing APs in one area into different load-balancing groups.
Example: AP1 is associated with 15 STAs and AP2 with 10 STAs. Since the difference of their STA numbers exceeds the current threshold, subsequent STAs will be associated with AP2.

Add Balancing Group

Balancing Group Name: *

Balancing Type: STA-count-based

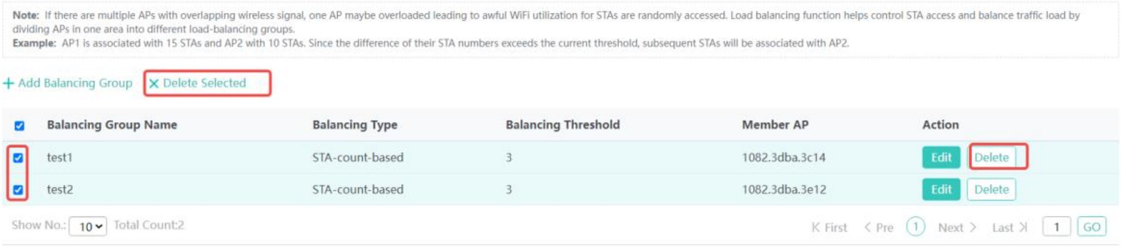
STA Threshold: 3

STA Difference: 3

Member AP: *

Parameter	Description
Balancing Group Name	This field is mandatory. This parameter cannot be modified in edit mode.
Balancing Type	Select **STA-count-based** or **AP-traffic-based**. This parameter cannot be modified in edit mode.
STA Threshold	To realize load balancing, the number of STAs associated with each AP should exceed the STA threshold.
STA Difference	To realize load balancing, the difference in the number of STAs associated with APs should exceed the STA difference value.
Traffic Threshold	To realize load balancing, the data traffic on each AP should exceed the traffic threshold. The traffic load is balanced when the difference of traffic on APs is reduced to a certain value.
Member AP	Select the AP members in this load balancing group. Each AP can be assigned to only one group.

(2) Deleting load balancing groups: Click **Delete** in the **Action** column to delete a load balancing group. Select load balancing groups in the list and click **Delete Selected**. Click **OK** in the pop-up window to batch delete load balancing groups.

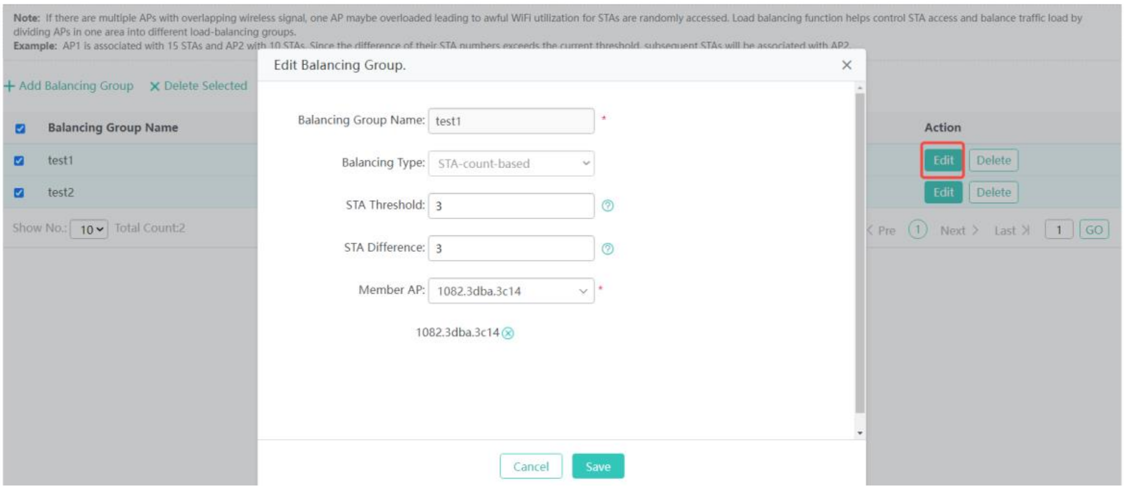


Note: If there are multiple APs with overlapping wireless signal, one AP maybe overloaded leading to awful WiFi utilization for STAs are randomly accessed. Load balancing function helps control STA access and balance traffic load by dividing APs in one area into different load-balancing groups.
Example: AP1 is associated with 15 STAs and AP2 with 10 STAs. Since the difference of their STA numbers exceeds the current threshold, subsequent STAs will be associated with AP2.

☑	Balancing Group Name	Balancing Type	Balancing Threshold	Member AP	Action
☑	test1	STA-count-based	3	1082.3dba.3c14	Edit Delete
☑	test2	STA-count-based	3	1082.3dba.3e12	Edit Delete

+ Add Balancing Group
× Delete Selected
Show No.: 10 Total Count:2
K First < Pre 1 Next > Last >| 1 GO

(3) Editing load balancing groups: Click **Edit** in the **Action** column and edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.



Note: If there are multiple APs with overlapping wireless signal, one AP maybe overloaded leading to awful WiFi utilization for STAs are randomly accessed. Load balancing function helps control STA access and balance traffic load by dividing APs in one area into different load-balancing groups.
Example: AP1 is associated with 15 STAs and AP2 with 10 STAs. Since the difference of their STA numbers exceeds the current threshold, subsequent STAs will be associated with AP2.

Edit Balancing Group.

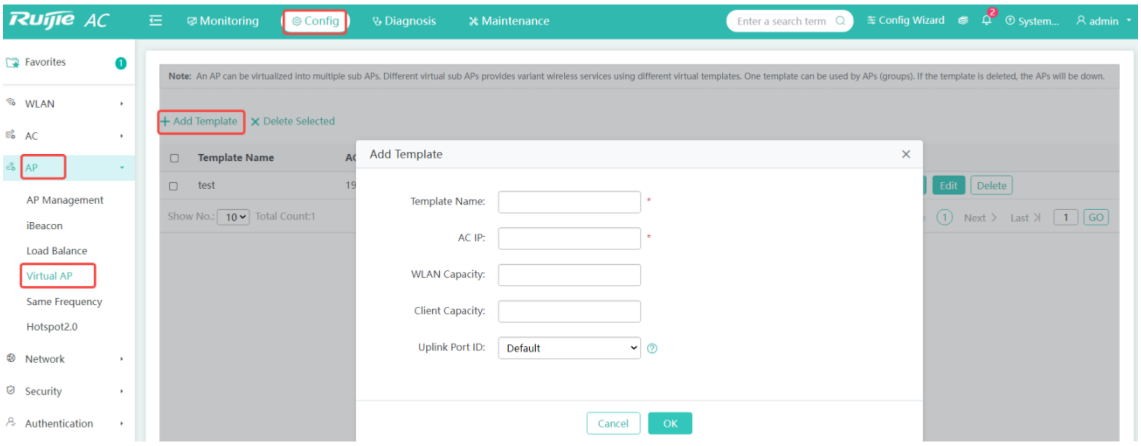
Balancing Group Name: test1 *
Balancing Type: STA-count-based
STA Threshold: 3
STA Difference: 3
Member AP: 1082.3dba.3c14 *
1082.3dba.3c14

5.3.4 Virtual AP

Choose **Config** > **AP** > **Virtual AP**.

Add and configure a template and apply the template to an AP group or an AP to realize AP virtualization.

(1) Adding templates: Click **Add Template** and configure the parameters on the **Add Template** page. Click **OK** to create the template. After the template is added, click **OK** to redirect to the **AP Management** page to apply the template. Click **Cancel** to return to the **Virtual AP** page.



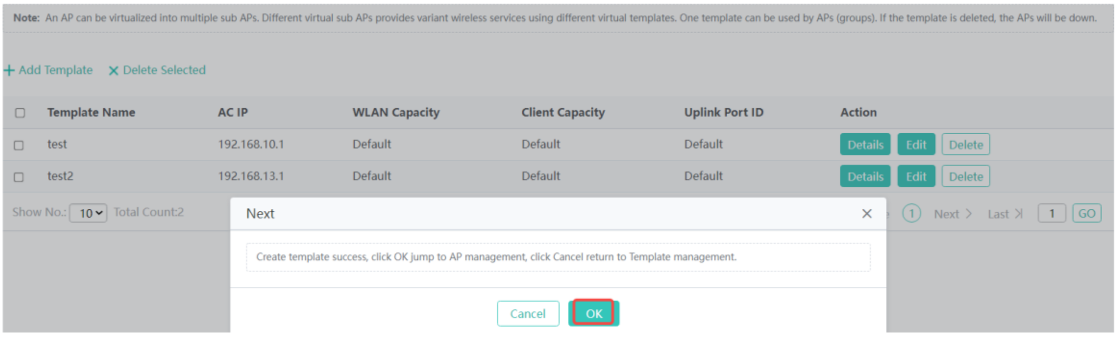
Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates. One template can be used by APs (groups). If the template is deleted, the APs will be down.

Add Template

Template Name: *
AC IP: *
WLAN Capacity:
Client Capacity:
Uplink Port ID: Default

Parameter	Description
Template Name	Enter the template name for virtual AP management. This field is mandatory.
AC IP	Enter the tunnel IP address of the AC for AP management.
WLAN Capacity	Enter the maximum number of WLANs supported by this template.
Client capacity	Enter the maximum number of clients supported by this template.

Uplink port ID	Virtual APs use the uplink port ID used by the active AP by default.

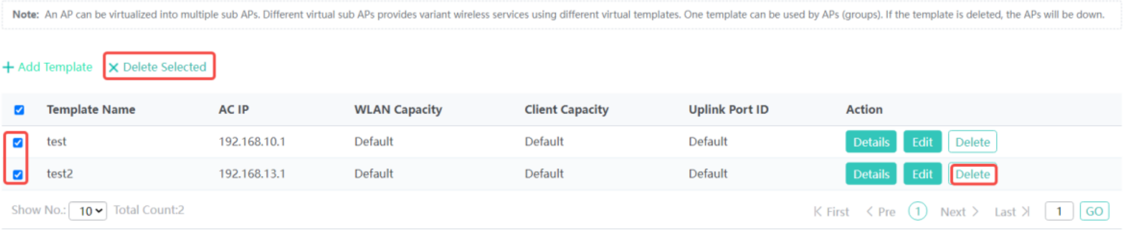


Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates. One template can be used by APs (groups). If the template is deleted, the APs will be down.

□	Template Name	AC IP	WLAN Capacity	Client Capacity	Uplink Port ID	Action
□	test	192.168.10.1	Default	Default	Default	Details Edit Delete
□	test2	192.168.13.1	Default	Default	Default	Details Edit Delete

Create template success, click OK jump to AP management, click Cancel return to Template management.

(2) Deleting templates: Click **Delete** in the **Action** column to delete a template. Select multiple items and click **Delete Selected** to batch delete templates.



Note: An AP can be virtualized into multiple sub APs. Different virtual sub APs provides variant wireless services using different virtual templates. One template can be used by APs (groups). If the template is deleted, the APs will be down.

☑	Template Name	AC IP	WLAN Capacity	Client Capacity	Uplink Port ID	Action
☑	test	192.168.10.1	Default	Default	Default	Details Edit Delete
☑	test2	192.168.13.1	Default	Default	Default	Details Edit Delete

5.3.5 Same Frequency

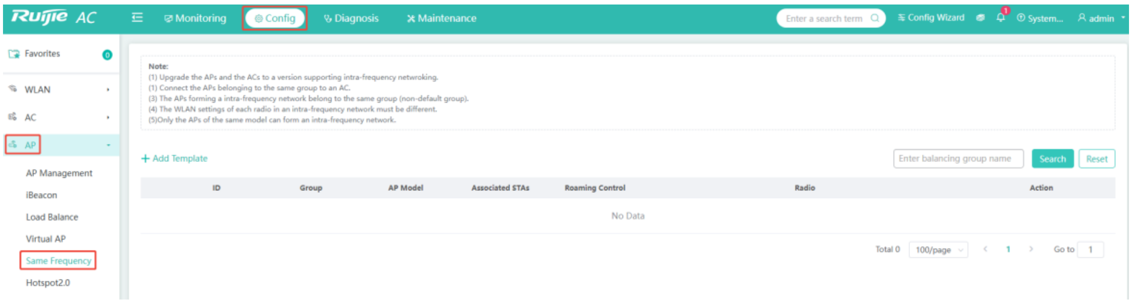
Choose **Config** > **AP** > **Same Frequency**.

Intra-frequency networking virtualizes multiple APs into one virtual AP on a WLAN. It is deployed based on a single channel, which can achieve seamless roaming. Multiple layers of independent intra-frequency networks implement high-density deployment with simplified maintenance. It applies to high-density scenarios with high roaming requirements but without specific demands for throughput, or low-density scenarios involving fast-moving STAs.

Different radios cannot be bound with the same WLAN and one AP group can be bound with only one intra-frequency networking solution.

Note

In the virtual AC mode, make sure that the SSID for intra-frequency networking adopts the local forwarding mode.

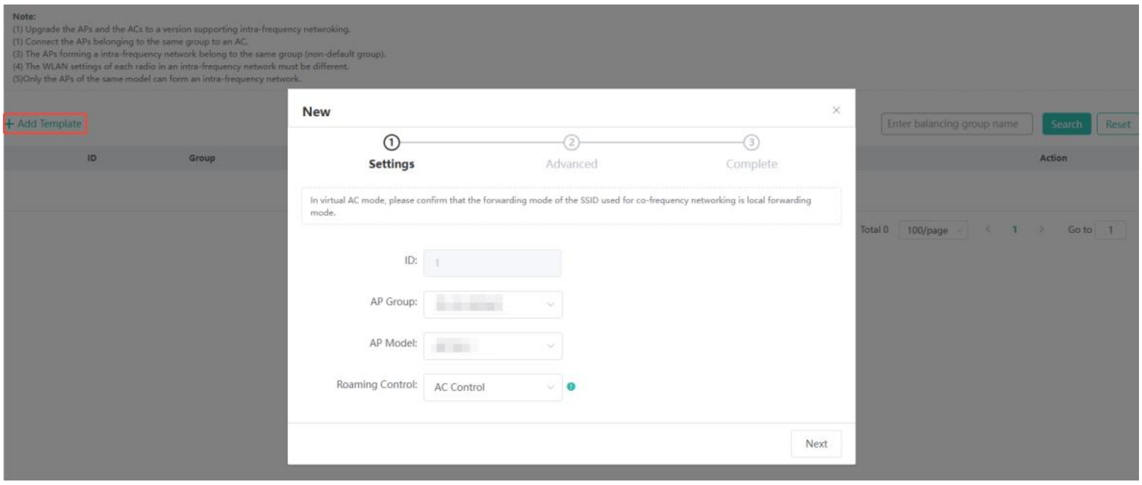


Note:
(1) Upgrade the APs and the ACs to a version supporting intra-frequency networking.
(1) Connect the APs belonging to the same group to an AC.
(3) The APs forming a intra-frequency network belong to the same group (non-default group).
(4) The WLAN settings of each radio in an intra-frequency network must be different.
(5)Only the APs of the same model can form an intra-frequency network.

ID	Group	AP Model	Associated STAs	Roaming Control	Radio	Action
No Data						

Total 0 100/page < 1 > Go to 1

Click **Add Template** and select an AP group, an AP model, and a roaming control mode.


Note:
(1) Upgrade the APs and the ACs to a version supporting intra-frequency netwroking.
(1) Connect the APs belonging to the same group to an AC.
(3) The APs forming a intra-frequency network belong to the same group (non-default group).
(4) The WLAN settings of each radio in an intra-frequency network must be different.
(5)Only the APs of the same model can form an intra-frequency network.

In virtual AC mode, please confirm that the forwarding mode of the SSID used for co-frequency networking is local forwarding mode.

ID: 1

AP Group:

AP Model:

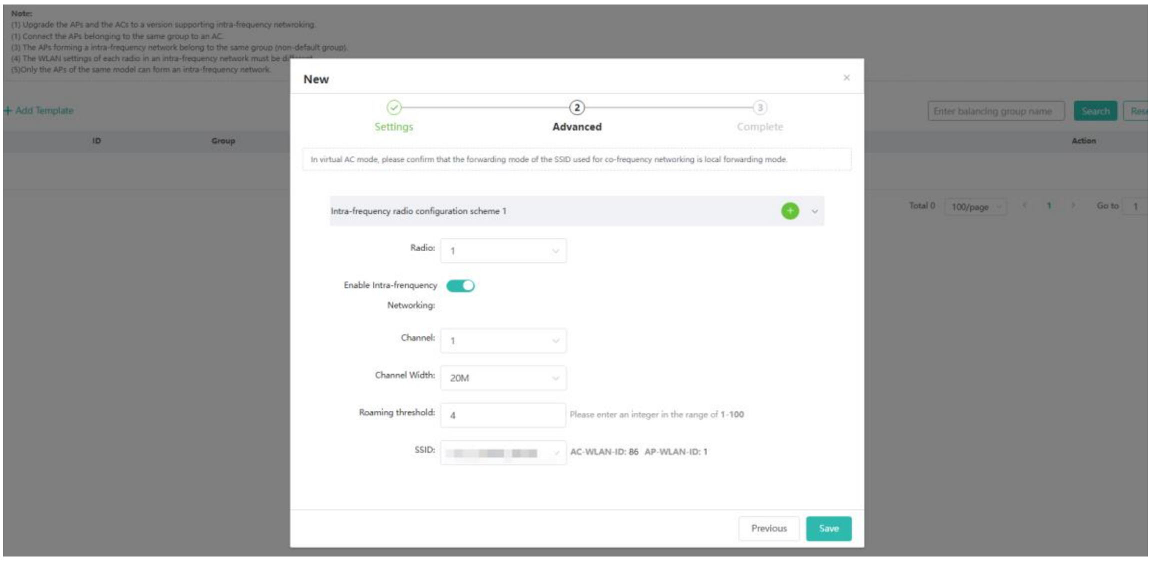
Roaming Control: AC Control

Parameter	Description
AP Group	Select an AP group that the template is applied to.
AP Model	Select an AP model that the template is applied to.
Roaming Control	Select a roaming control mode and observe the following precautions: The AC control mode (excluding the virtual AC) is configured by default. The virtual AC only supports the AP control mode. In the case of hierarchical ACs, if the headquarter AC or branch AC is a virtual AC, you can only select the AP control mode here.

Click **Next** to enter advanced settings.

Note

If a radio of the AP group is not bound with the SSID associated with the AC, switch over to the radio that is bound with the SSID. Or bind the radio with the SSID in the **Add WiFi** page.



Note:
(1) Upgrade the APs and the ACs to a version supporting intra-frequency netwroking.
(1) Connect the APs belonging to the same group to an AC.
(3) The APs forming a intra-frequency network belong to the same group (non-default group).
(4) The WLAN settings of each radio in an intra-frequency network must be di
(5)Only the APs of the same model can form an intra-frequency network.

New

In virtual AC mode, please confirm that the forwarding mode of the SSID used for co-frequency networking is local forwarding mode.

Intra-frequency radio configuration scheme 1

Radio: 1

Enable Intra-frenquency Networking:

Channel: 1

Channel Width: 20M

Roaming threshold: 4 Please enter an integer in the range of 1-100

SSID: [redacted] AC-WLAN-ID: 86 AP-WLAN-ID: 1

Parameter	Description
Radio	Specify the radio on which the intra-frequency networking feature is enabled.
Enable Intra-frenquency Networking	Enable the intra-frequency networking feature.
Channel	Specify working channel of the current radio.
Channel Width	Specify the working frequency bandwidth of the current radio.
Roaming threshold	Specify the RSSI threshold below which roaming is triggered.
SSID	Specify the WLAN ID of the radio for intra-frequency networking.

Click **Save** to add the template.

5.3.6 Hotspot 2.0

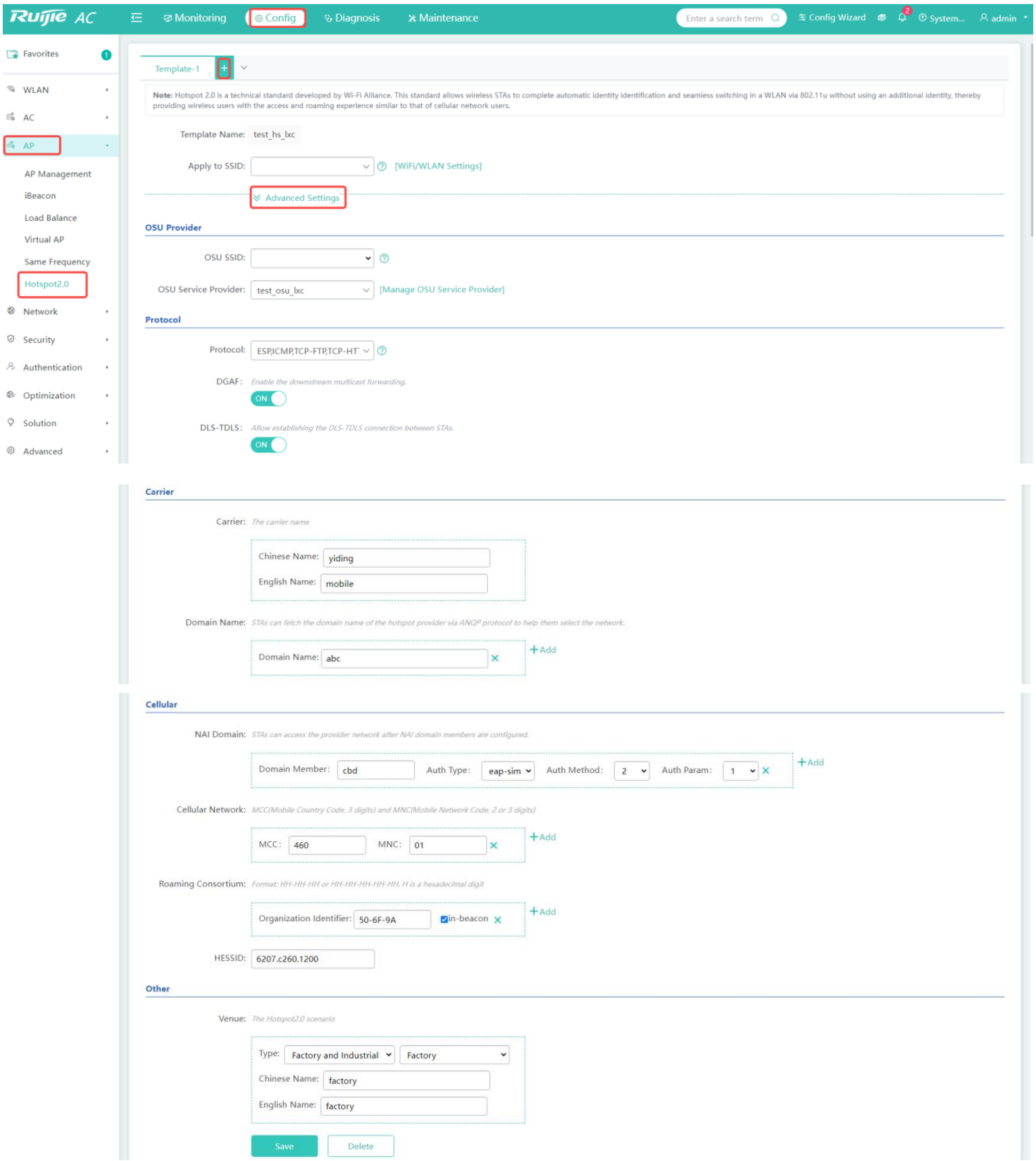
Choose **Config** > **AP** > **Hotspot2.0**.

Hotspot 2.0 is a technical standard developed by Wi-Fi Alliance. It allows STAs to complete automatic identification and seamless switching in compliance with IEEE 802.11u on a WLAN without using an additional identity identifier. This standard provides STAs with access and roaming experience comparable to that of cellular networks.

1. Template

(1) Adding templates: Click **+** to add a template page. Enter the template name and select the SSID that the template is applied to. Complete the optional advanced settings and click **Save** to add the template.

The advanced settings include the Online Sign Up (OSU) provider, protocol, carrier, cellular network, and other.



Note: Hotspot 2.0 is a technical standard developed by Wi-Fi Alliance. This standard allows wireless STAs to complete automatic identity identification and seamless switching in a WLAN via 802.11u without using an additional identity, thereby providing wireless users with the access and roaming experience similar to that of cellular network users.

Template Name: test_hs_lxc

Apply to SSID: [WiFi/WLAN Settings]

Advanced Settings

OSU Provider

OSU SSID:

OSU Service Provider: test_osu_lxc [Manage OSU Service Provider]

Protocol

Protocol: ESP,ICMP,TCP-FTP,TCP-HT

DGAF: *Enable the downstream multicast forwarding.* ON

DLS-TDLS: *Allow establishing the DLS-TDLS connection between STAs.* ON

Carrier

Carrier: *The carrier name*

Chinese Name: yiding

English Name: mobile

Domain Name: *STAs can fetch the domain name of the hotspot provider via ANQP protocol to help them select the network.*

Domain Name: abc ✕ +Add

Cellular

NAI Domain: *STAs can access the provider network after NAI domain members are configured.*

Domain Member: cbd Auth Type: eap-sim Auth Method: 2 Auth Param: 1 ✕ +Add

Cellular Network: *MCC(Mobile Country Code, 3 digits) and MNC(Mobile Network Code, 2 or 3 digits)*

MCC: 460 MNC: 01 ✕ +Add

Roaming Consortium: *Format: HH-HH-HH or HH-HH-HH-HH-HH. H is a hexadecimal digit*

Organization Identifier: 50-6F-9A ☑in-beacon ✕ +Add

HESSID: 6207.c260.1200

Other

Venue: *The Hotspot2.0 scenario*

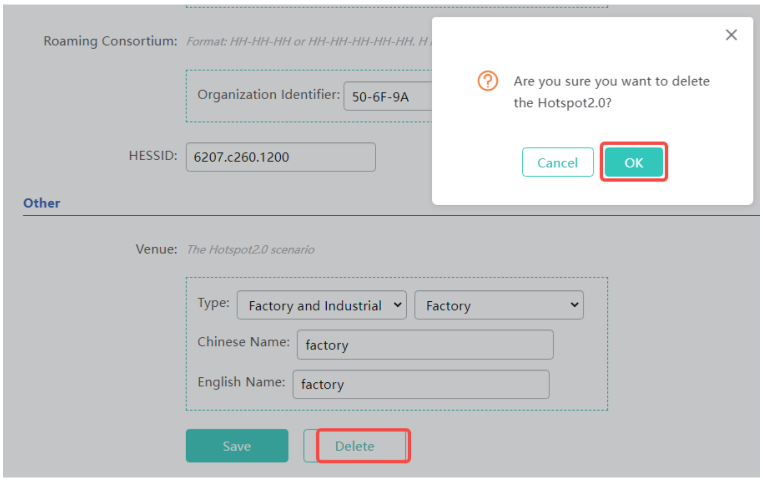
Type: Factory and Industrial Factory

Chinese Name: factory

English Name: factory

Save Delete

(2) Deleting templates: Click the template to enter the template page, and click **Delete** to delete the template.



Roaming Consortium: *Format: HH-HH-HH or HH-HH-HH-HH-HH. H*

Organization Identifier: 50-6F-9A

HESSID: 6207.c260.1200

Other

Venue: *The Hotspot2.0 scenario*

Type: Factory and Industrial Factory

Chinese Name: factory

English Name: factory

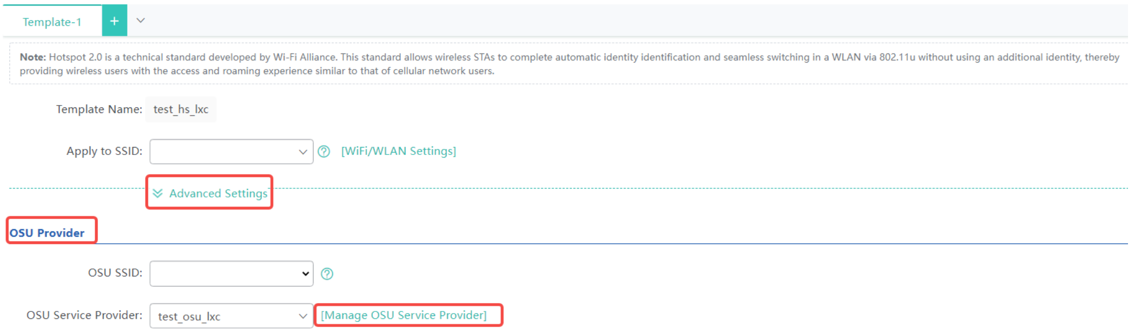
Save Delete

Are you sure you want to delete the Hotspot2.0?

Cancel OK

2. OSU Provider

Click **Manage OSU Service Provider** in the **OSU Provider** section to enter the **OSU Service Provider** page.



Template-1 +

Note: Hotspot 2.0 is a technical standard developed by Wi-Fi Alliance. This standard allows wireless STAs to complete automatic identity identification and seamless switching in a WLAN via 802.11u without using an additional identity, thereby providing wireless users with the access and roaming experience similar to that of cellular network users.

Template Name: test_hs_lxc

Apply to SSID: [WiFi/WLAN Settings]

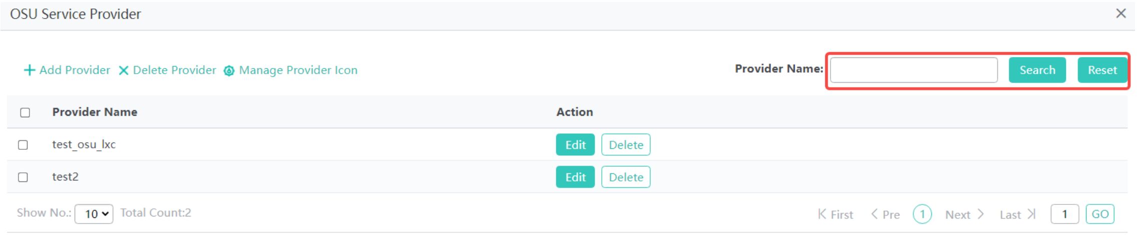
Advanced Settings

OSU Provider

OSU SSID:

OSU Service Provider: test_osu_lxc [Manage OSU Service Provider]

(1) Searching for providers: This page displays the list of OSU providers and supports the fuzzy query by the provider name.



OSU Service Provider

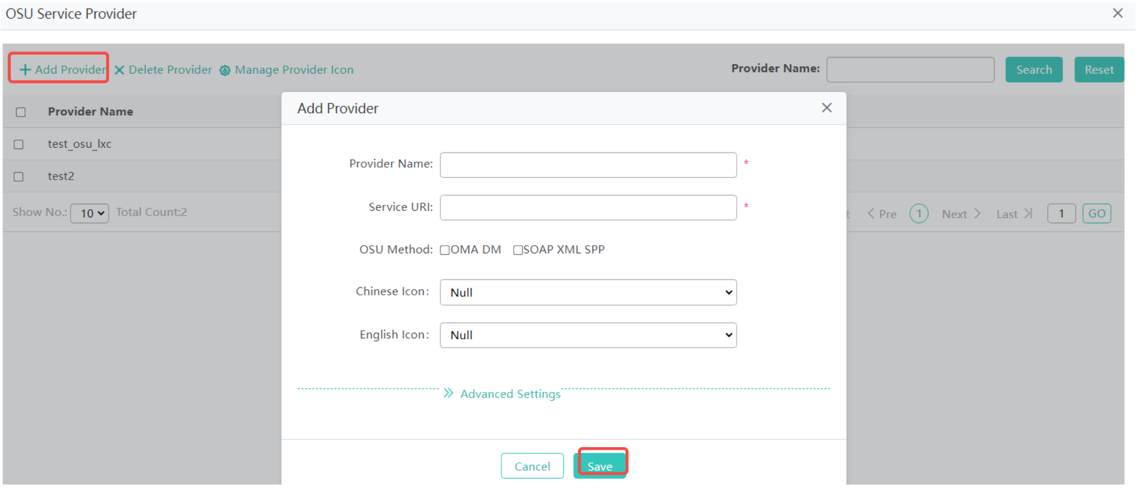
+ Add Provider ✕ Delete Provider Manage Provider Icon

Provider Name: Search Reset

□	Provider Name	Action
□	test_osu_lxc	Edit Delete
□	test2	Edit Delete

Show No.: 10 Total Count:2 First Pre 1 Next Last 1 GO

(2) Adding providers: Click **Add Provider** and the **Add Provider** window pops up. Enter the provider name and the service URL, and complete the optional advanced settings. Click **Save** to add the provider.



OSU Service Provider

+ Add Provider ✕ Delete Provider Manage Provider Icon

Provider Name: Search Reset

Add Provider

Provider Name: *

Service URI: *

OSU Method: □OMA DM □SOAP XML SPP

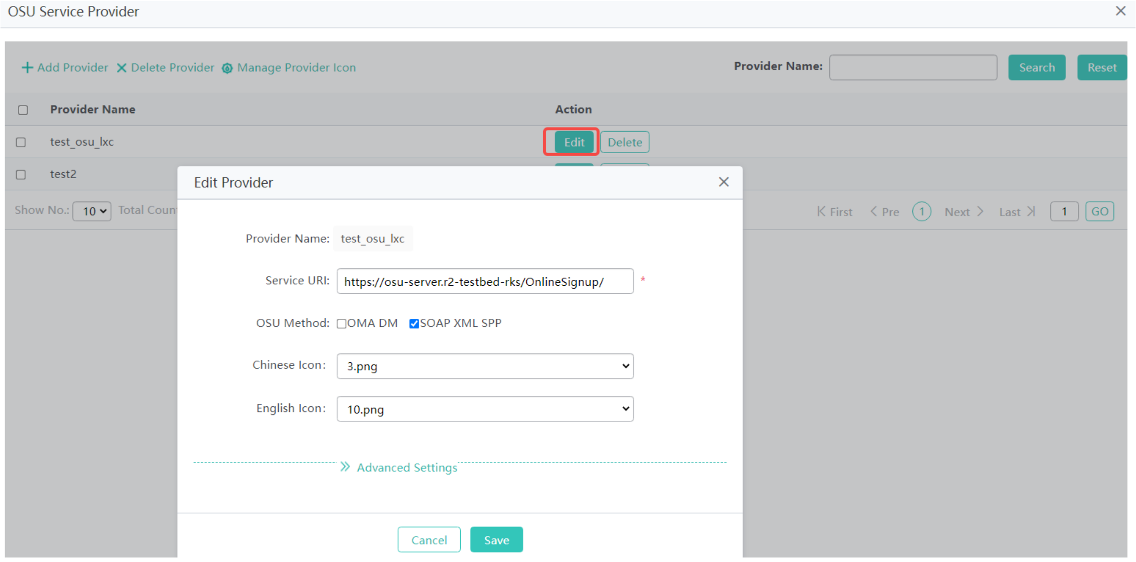
Chinese Icon: Null

English Icon: Null

Advanced Settings

Cancel Save

(3) Editing providers: Click **Edit** in the **Action** column to enter the **Edit Provider** page. Edit the fields and click **Save**. The provider name cannot be changed on this page.



OSU Service Provider ×

+ Add Provider × Delete Provider Manage Provider Icon Provider Name: Search Reset

□	Provider Name	Action
□	test_osu_lxc	Edit Delete
□	test2	

Show No.: 10 Total Coun

First Pre 1 Next Last 1 GO

Edit Provider ×

Provider Name: test_osu_lxc

Service URI: https://osu-server.r2-testbed-rks/OnlineSignup/ *

OSU Method: □OMA DM ☑SOAP XML SPP

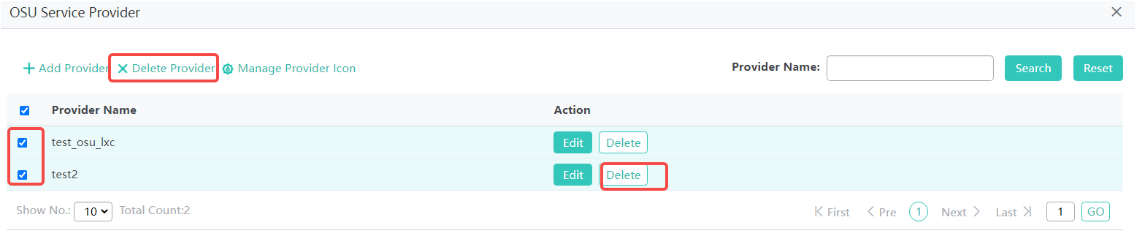
Chinese Icon: 3.png

English Icon: 10.png

» Advanced Settings

Cancel Save

(4) Deleting providers: Click **Delete** in the **Action** column to delete a provider. Select multiple providers and click **Delete Provider** to batch delete providers.



OSU Service Provider ×

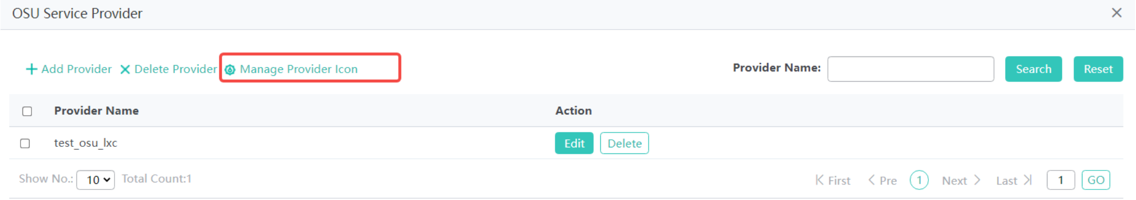
+ Add Provider × Delete Provider Manage Provider Icon Provider Name: Search Reset

☑	Provider Name	Action
☑	test_osu_lxc	Edit Delete
☑	test2	Edit Delete

Show No.: 10 Total Count:2

First Pre 1 Next Last 1 GO

(5) Managing provider icons: Click **Manage Provider Icon**.



OSU Service Provider ×

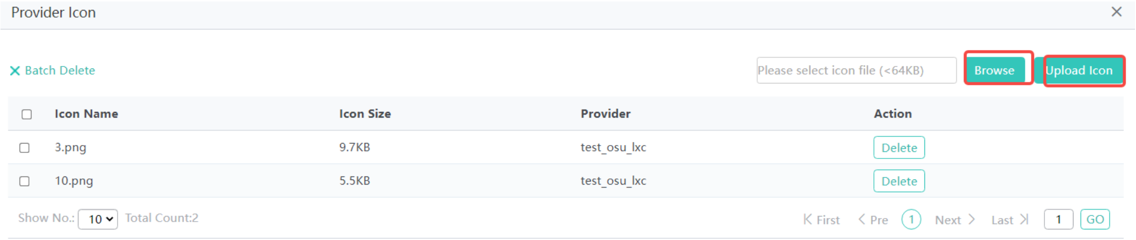
+ Add Provider × Delete Provider Manage Provider Icon Provider Name: Search Reset

□	Provider Name	Action
□	test_osu_lxc	Edit Delete

Show No.: 10 Total Count:1

First Pre 1 Next Last 1 GO

Click the search bar or **Browse** and a window pops up. Select files and click **Upload Icon**.



Provider Icon ×

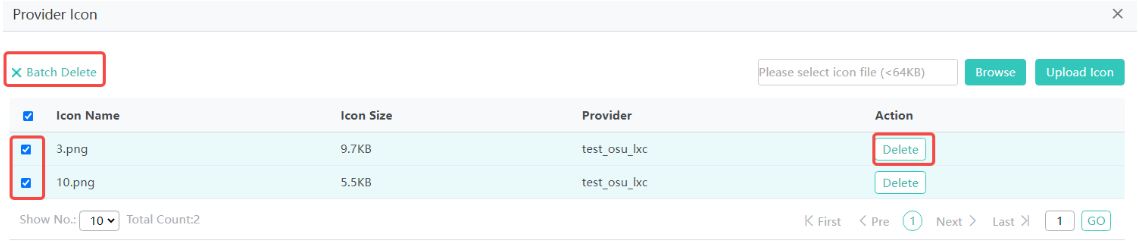
× Batch Delete Please select icon file (<64KB) Browse Upload Icon

□	Icon Name	Icon Size	Provider	Action
□	3.png	9.7KB	test_osu_lxc	Delete
□	10.png	5.5KB	test_osu_lxc	Delete

Show No.: 10 Total Count:2

First Pre 1 Next Last 1 GO

Select at least one icon and click **Batch Delete** to batch delete icons.



Provider Icon ✕

✕ Batch Delete

Please select icon file (<64KB) Browse Upload Icon

☑	Icon Name	Icon Size	Provider	Action
☑	3.png	9.7KB	test_osu_lxc	Delete
☑	10.png	5.5KB	test_osu_lxc	Delete

Show No.: 10 Total Count:2

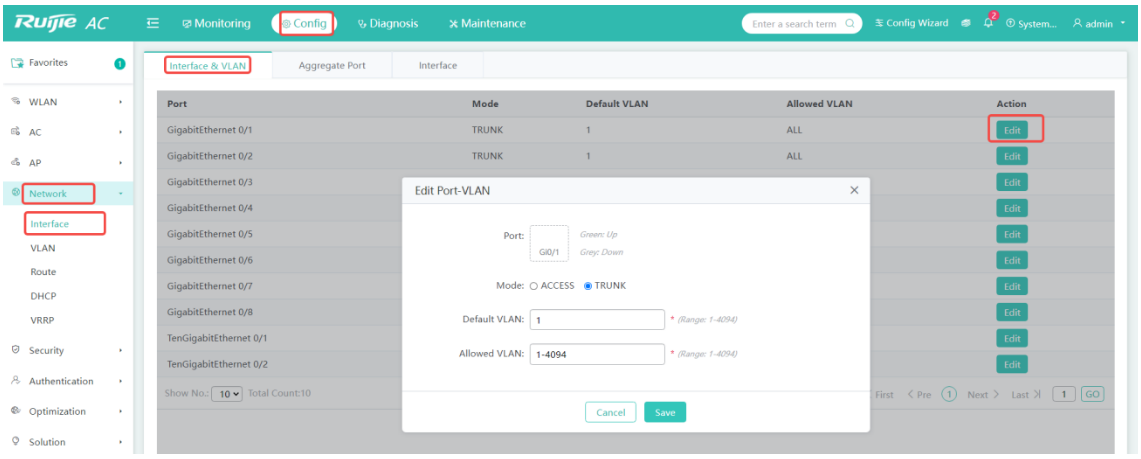
5.4 Network

5.4.1 Interface

Choose **Config** > **Network** > **Interface**.

1. Interface & VLAN

Click **Edit** in the **Action** column. A window pops up displaying the information about the VLAN to which the port belongs. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



Port	Mode	Default VLAN	Allowed VLAN	Action
GigabitEthernet 0/1	TRUNK	1	ALL	Edit
GigabitEthernet 0/2	TRUNK	1	ALL	Edit
GigabitEthernet 0/3				Edit
GigabitEthernet 0/4				Edit
GigabitEthernet 0/5				Edit
GigabitEthernet 0/6				Edit
GigabitEthernet 0/7				Edit
GigabitEthernet 0/8				Edit
TenGigabitEthernet 0/1				Edit
TenGigabitEthernet 0/2				Edit

Show No.: 10 Total Count:10

Edit Port-VLAN ✕

Port: Gi0/1 Green: Up Grey: Down

Mode: ○ ACCESS ● TRUNK

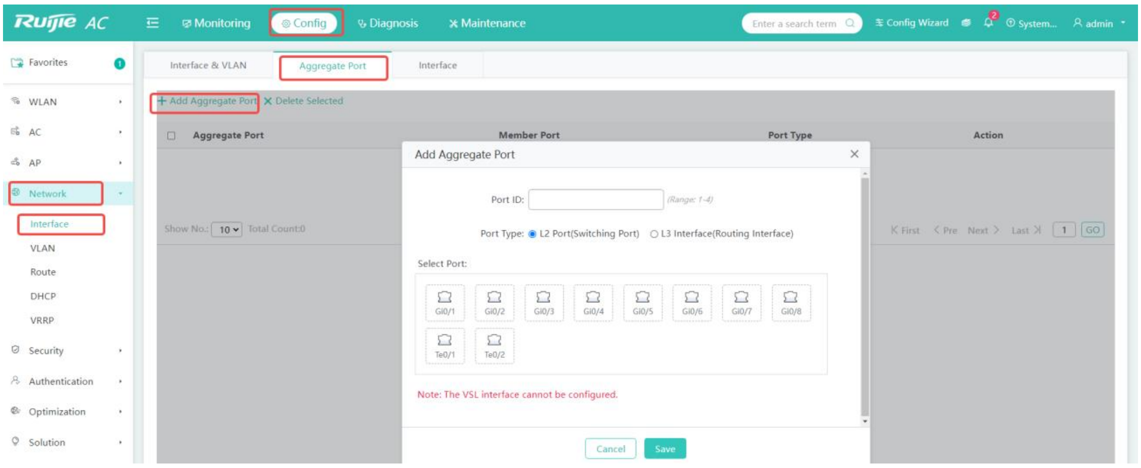
Default VLAN: 1 * (Range: 1-4094)

Allowed VLAN: 1-4094 * (Range: 1-4094)

Cancel Save

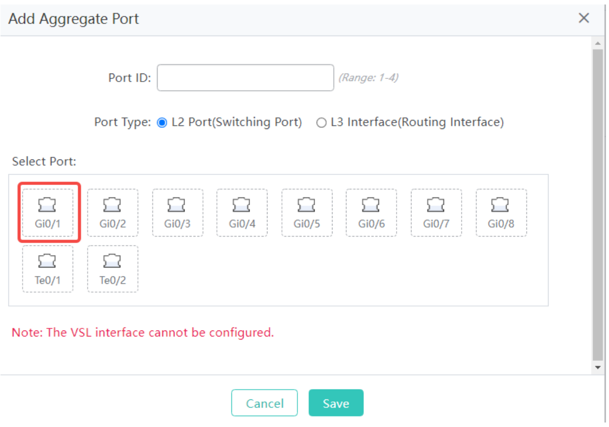
2. Aggregate Port

(1) Adding aggregate ports: Click **Add Aggregate Port**. Edit the fields in the pop-up window. Click **Save** and the aggregate port will be displayed in the list of aggregate ports after a message indicating operation success is displayed.



Note: The VSL interface cannot be configured.

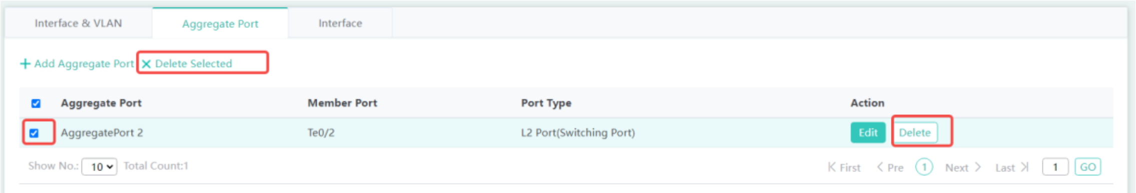
The following figure shows the panel where you can select member ports. The ports in gray have been configured as member ports of an aggregate port. The number under the port icon indicates that this port is a member port of the specified aggregate port.



Port Type: ● L2 Port(Switching Port) ○ L3 Interface(Routing Interface)

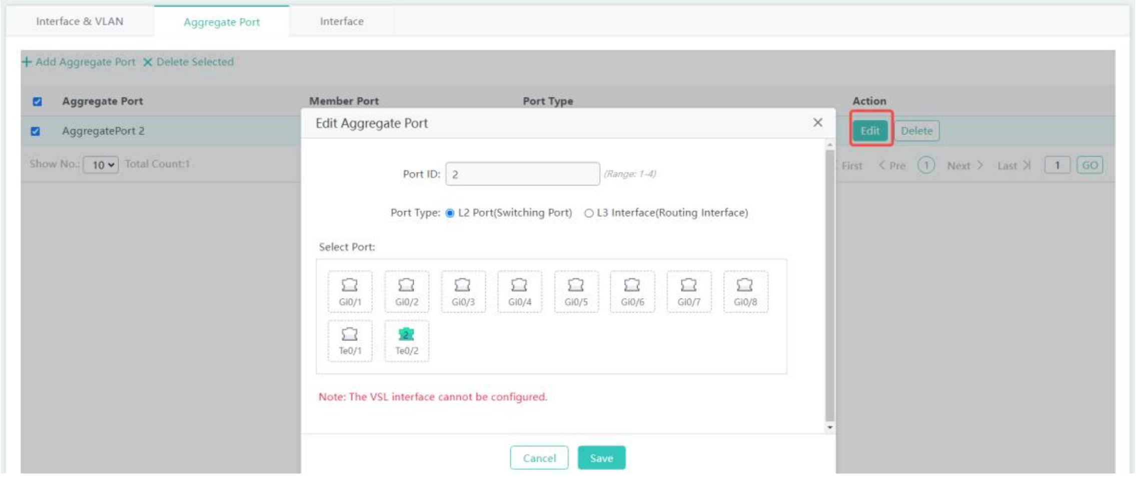
Note: The VSL interface cannot be configured.

(2) Deleting aggregate ports: Select the aggregate ports in the list. Click **Delete Selected** and click **OK** in the pop-up window to delete the aggregate ports.



☑	Aggregate Port	Member Port	Port Type	Action
☑	AggregatePort 2	Te0/2	L2 Port(Switching Port)	Edit Delete

(3) Editing aggregate ports: Click **Edit** in the **Action** column. A window pops up displaying the information about the aggregate port and edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



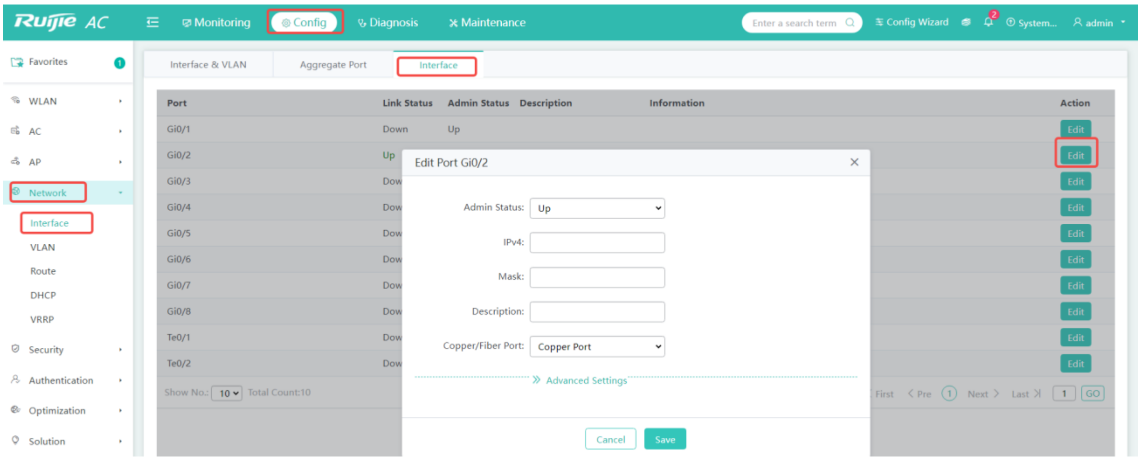
Port ID: 2 (Range: 1-4)

Port Type: ● L2 Port(Switching Port) ○ L3 Interface(Routing Interface)

Note: The VSL interface cannot be configured.

3. Interface

Click **Delete** in the **Action** column. A window pops up displaying the information about the interface. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



Port	Link Status	Admin Status
Gi0/1	Down	Up
Gi0/2	Up	
Gi0/3	Dow	
Gi0/4	Dow	
Gi0/5	Dow	
Gi0/6	Dow	
Gi0/7	Dow	
Gi0/8	Dow	
Te0/1	Dow	
Te0/2	Dow	

Admin Status: Up

IPv4:

Mask:

Description:

Copper/Fiber Port: Copper Port

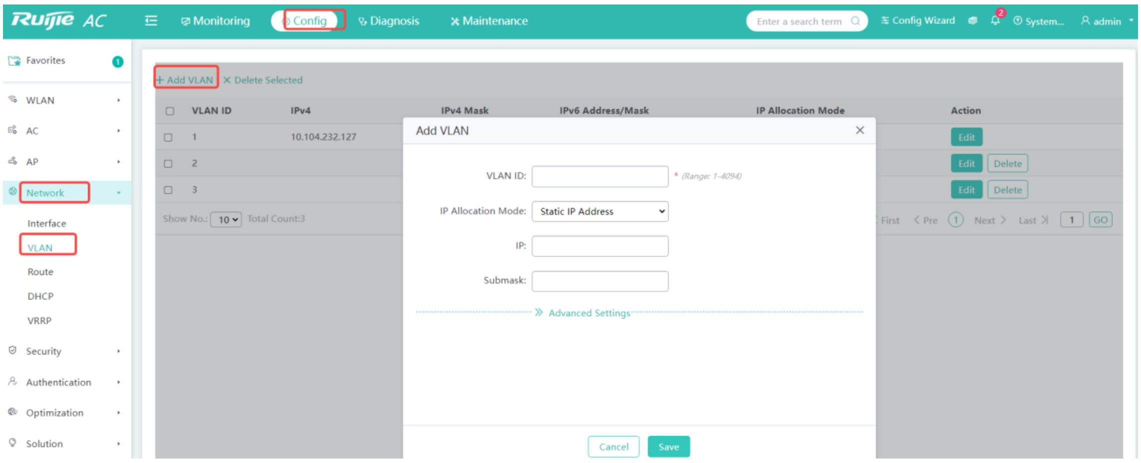
Parameter	Description
Admin Status	Select the status of the interface.
IPv4	Enter the IPv4 address of the interface.
Mask	Enter the IPv4 subnet mask of the interface.
Description	Enter the description or alias of the interface.
Copper/Fiber Port	The options including Copper Port and Fiber Port are displayed based on the hardware capability.
IPv6	Enter the IPv6 address of the interface.
Speed	Configure the rate of the interface.

Working Mode	The work modes of the interface include negotiation, duplex, and half-duplex modes.

5.4.2 VLAN

Choose **Config** > **Network** > **VLAN**.

(1) Adding VLANs: Click **Add VLAN** and edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed. The added VLAN is displayed in the VLAN list.



□	VLAN ID	IPv4	IPv4 Mask	IPv6 Address/Mask	IP Allocation Mode	Action
□	1	10.104.232.127				Edit
□	2					Edit Delete
□	3					Edit Delete

Show No.: 10 Total Count:3 First Pre 1 Next Last 1 GO

Add VLAN

VLAN ID: * (Range: 1-4094)

IP Allocation Mode: Static IP Address

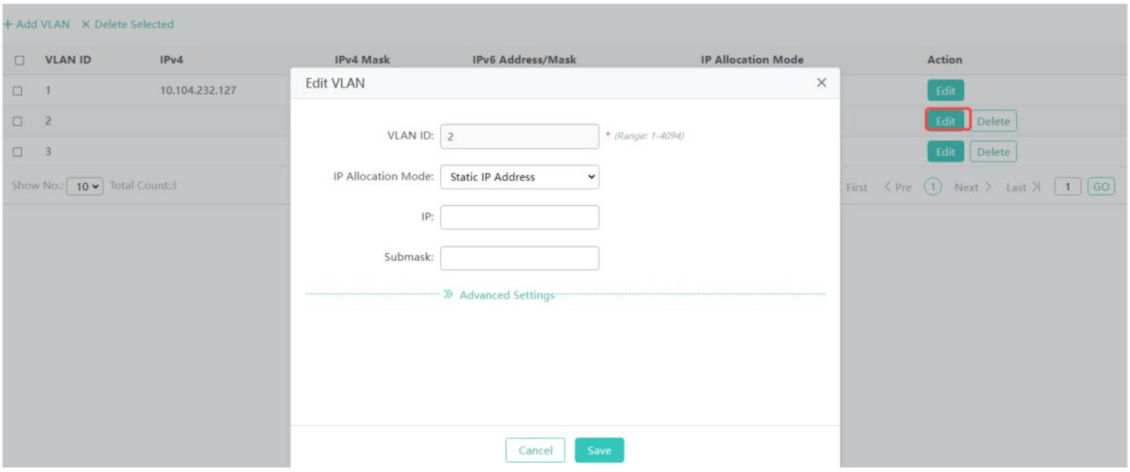
IP:

Submask:

Advanced Settings

Cancel Save

(2) Editing VLANs: Click **Edit** in the **Action** column and a window pops up displaying the information about the VLAN. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



□	VLAN ID	IPv4	IPv4 Mask	IPv6 Address/Mask	IP Allocation Mode	Action
□	1	10.104.232.127				Edit
□	2					Edit Delete
□	3					Edit Delete

Show No.: 10 Total Count:3 First Pre 1 Next Last 1 GO

Edit VLAN

VLAN ID: 2 * (Range: 1-4094)

IP Allocation Mode: Static IP Address

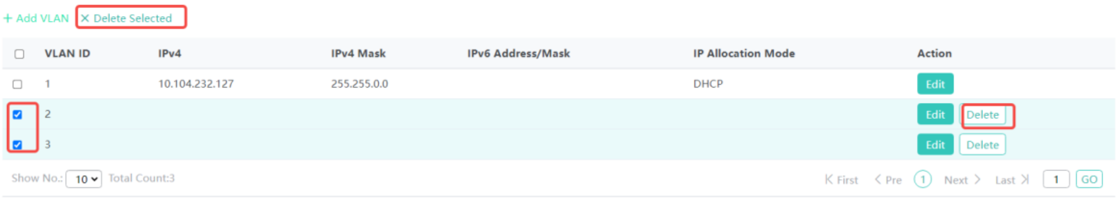
IP:

Submask:

Advanced Settings

Cancel Save

(3) Deleting VLANs: Click **Delete** in the **Action** column and click OK in the pop-up window to delete a VLAN. Select multiple items in the list. Click **Delete Selected** and a window pops up. Click **OK** to batch delete VLANs.



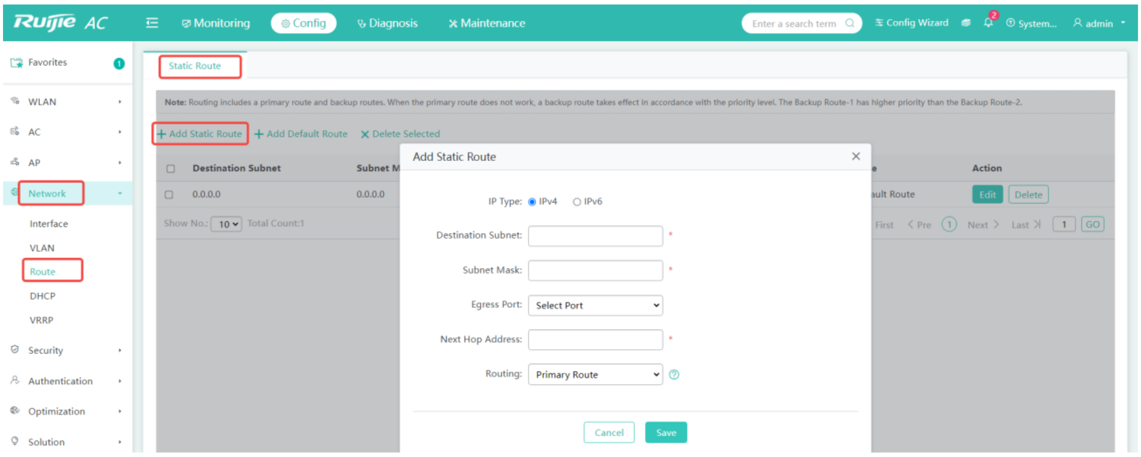
□	VLAN ID	IPv4	IPv4 Mask	IPv6 Address/Mask	IP Allocation Mode	Action
□	1	10.104.232.127	255.255.0.0		DHCP	Edit
☑	2					Edit Delete
☑	3					Edit Delete

Show No.: 10 Total Count:3 First Pre 1 Next Last 1 GO

5.4.3 Route

Choose **Config** > **Network** > **Route**.

(1) Adding static routes: Click **Add Static Route**. Edit the fields in the pop-up window. Click **Save** and the static route will be displayed in the route list after a message indicating operation success appears.



Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.

Add Static Route

IP Type: ● IPv4 ○ IPv6

Destination Subnet: *

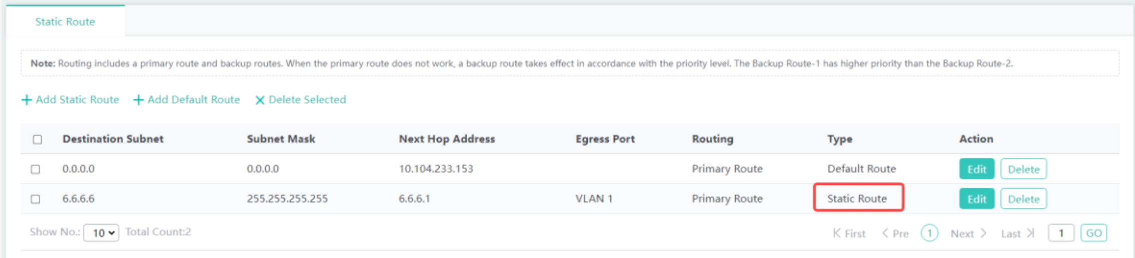
Subnet Mask: *

Egress Port: Select Port

Next Hop Address: *

Routing: Primary Route

Cancel Save



Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.

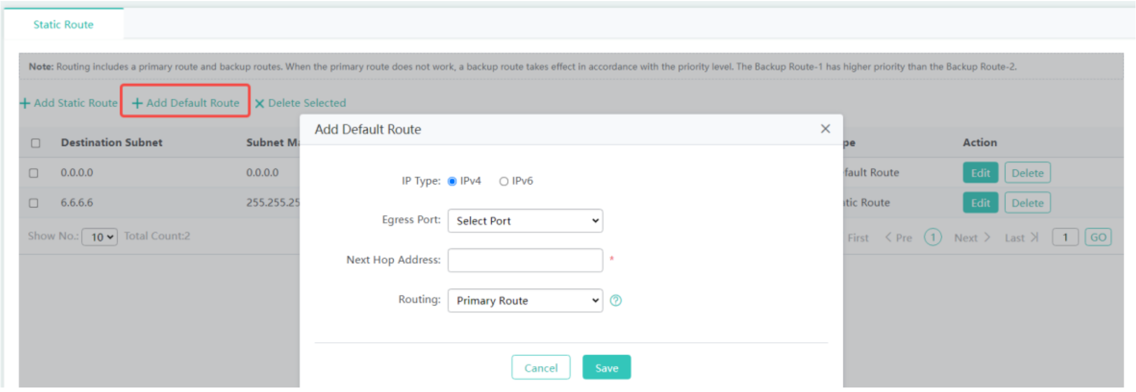
□	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Routing	Type	Action
□	0.0.0.0	0.0.0.0	10.104.233.153		Primary Route	Default Route	Edit Delete
□	6.6.6.6	255.255.255.255	6.6.6.1	VLAN 1	Primary Route	Static Route	Edit Delete

Show No.: 10 Total Count:2

(2) Adding default routes: Click **Add Default R**oute. Edit the fields in the pop-up window. Click Save and the default route will be displayed in the route list after a message indicating operation success appears.

Note

Route selection involves a primary route and backup routes. When the primary route is unavailable, the backup route will be adopted. The selection of the backup route is also determined by the priority levels. For instance, backup route 1 has a higher priority than backup route 2.



Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.

Add Default Route

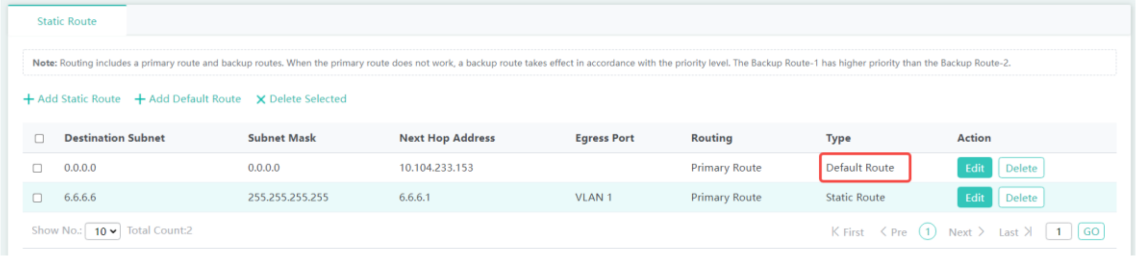
IP Type: ● IPv4 ○ IPv6

Egress Port: Select Port

Next Hop Address: *

Routing: Primary Route

Cancel Save



Static Route

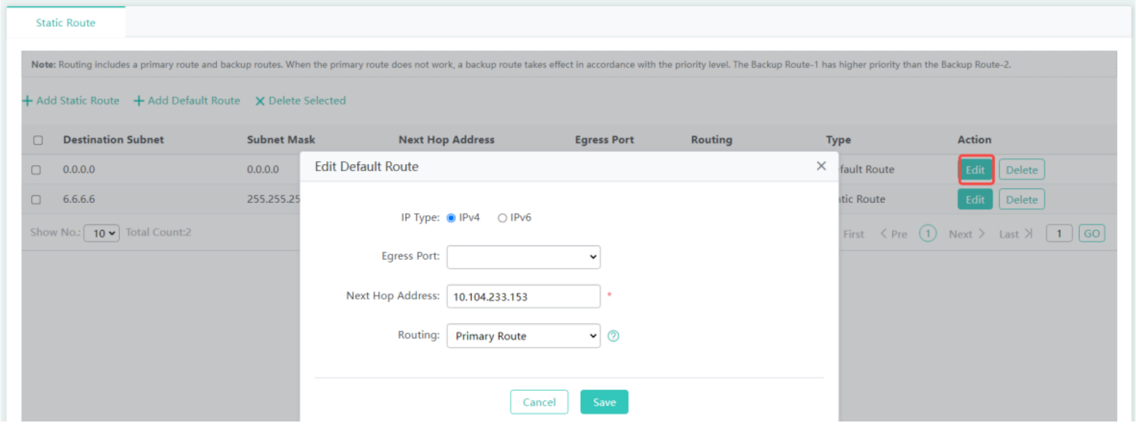
Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.

+ Add Static Route + Add Default Route ✕ Delete Selected

□	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Routing	Type	Action
□	0.0.0.0	0.0.0.0	10.104.233.153		Primary Route	Default Route	Edit Delete
□	6.6.6.6	255.255.255.255	6.6.6.1	VLAN 1	Primary Route	Static Route	Edit Delete

Show No.: 10 Total Count:2

(3) Editing routes: Click **Edit** in the **Action** column, and a window pops up displaying the information about the route. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



Edit Default Route

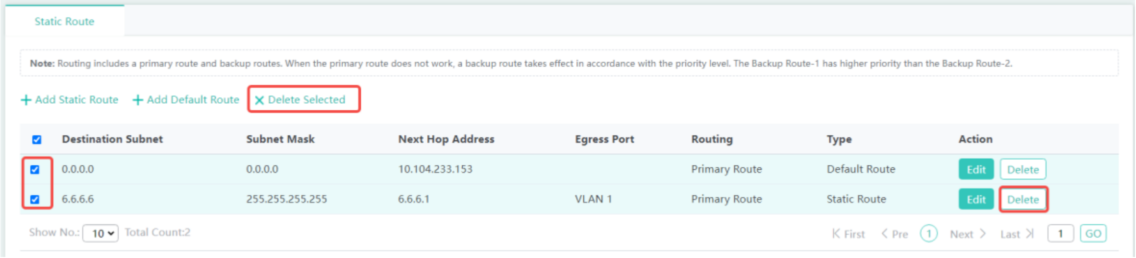
IP Type: ● IPv4 ○ IPv6

Egress Port:

Next Hop Address: 10.104.233.153 *

Routing: Primary Route

(4) Deleting routes: Click **Delete** in the **Action** column to delete a route. Select multiple items and click **Delete Selected**. Click **OK** in the pop-up window to batch delete routes.



Static Route

Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.

+ Add Static Route + Add Default Route ✕ Delete Selected

☑	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Routing	Type	Action
☑	0.0.0.0	0.0.0.0	10.104.233.153		Primary Route	Default Route	Edit Delete
☑	6.6.6.6	255.255.255.255	6.6.6.1	VLAN 1	Primary Route	Static Route	Edit Delete

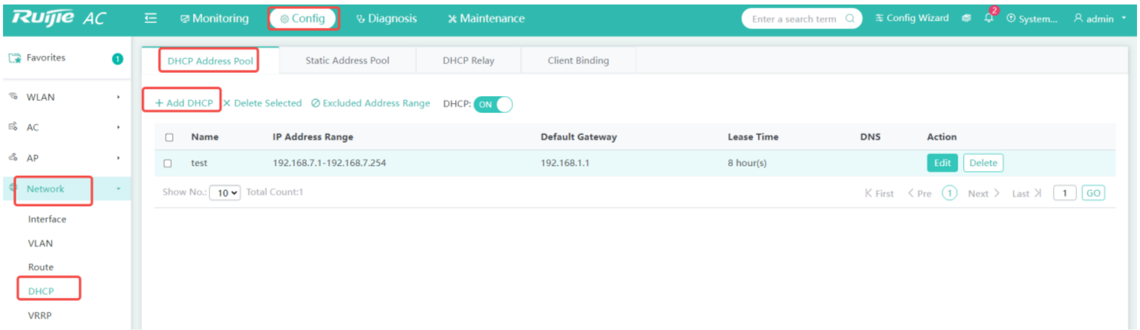
Show No.: 10 Total Count:2

5.4.4 DHCP

1. DHCP Address Pool

Choose **Config** > **Network** > **DHCP** > **DHCP Address Pool**.

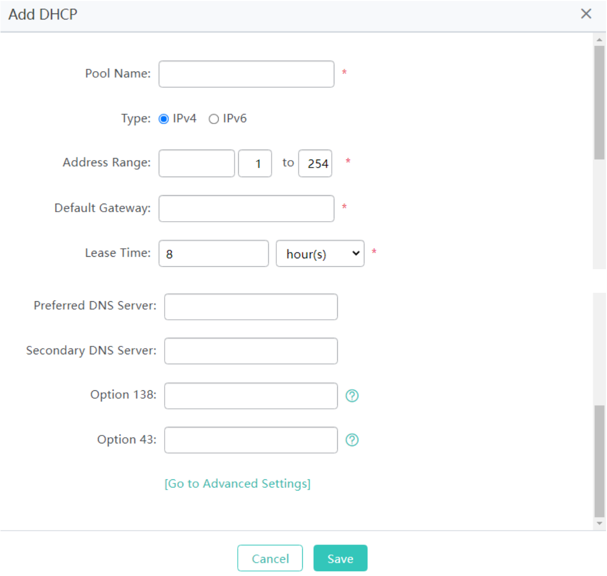
(1) Adding DHCP address pools: Click **Add DHCP** and edit the fields in the pop-up window. Click **Save** and the DHCP address pool will be displayed in the list after a message indicating operation success appears.



DHCP: ON

□	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
□	test	192.168.7.1-192.168.7.254	192.168.1.1	8 hour(s)		Edit Delete

Show No.: 10 Total Count:1



Pool Name: *

Type: ● IPv4 ○ IPv6

Address Range: 1 to 254 *

Default Gateway: *

Lease Time: 8 hour(s) *

Preferred DNS Server:

Secondary DNS Server:

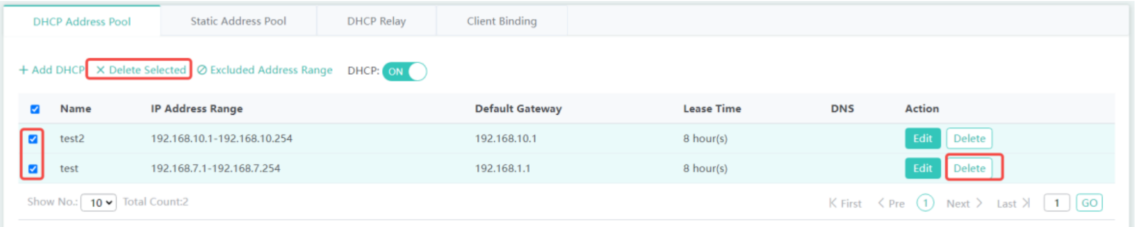
Option 138:

Option 43:

Parameter	Description
Pool Name	Enter the name of the DHCP address pool.
Type	The options include **IPv4** and **IPv6**.
Address Range	Configure the range of the DHCP address pool.
Default Gateway	Configure the default gateway for the DHCP address pool.
Lease Time	Configure the lease time for the DHCP address pool, either a limited time span or no time limit.
Preferred DNS Server	Configure the preferred DNS server for the clients using the DHCP address pool.
Secondary DNS Server	Configure the secondary DNS server for the clients using the DHCP address pool.
Option 138	The DHCP Option 138 is used to inform the AP of the IP address of the AC to associate the AP with the AC. Typically, this field is filled in with the IP address of the loopback interface of the AC. It is specific to Ruijie products.

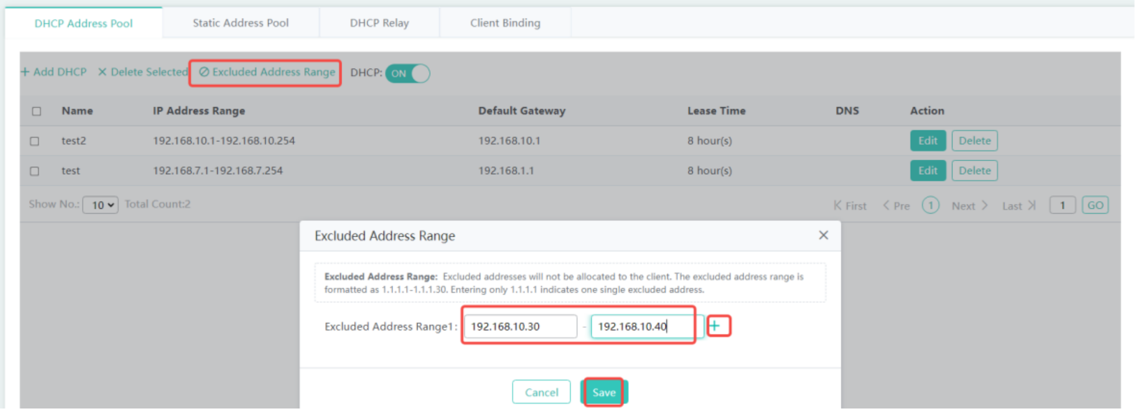
Option 43	The DHCP Option 43 is used to inform the AP of the IP address of the AC to associate the AP with the AC. Typically, this field is filled with the IP address of the loopback interface of the AC. It is commonly used.

(2) Deleting DHCP pools: Click **Delete** in the **Action** column to delete a DHCP address pool. Select multiple items and click **Delete Selected**. Click **OK** in the pop-up window to batch delete DHCP address pools.



☑	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
☑	test2	192.168.10.1-192.168.10.254	192.168.10.1	8 hour(s)		Edit Delete
☑	test	192.168.7.1-192.168.7.254	192.168.1.1	8 hour(s)		Edit Delete

(3) Configuring excluded address ranges: Click **Excluded Address Range**. Configure the range of IP addresses that will not be allocated to clients in the pop-up window. You can configure multiple excluded address ranges. Click **OK** and the excluded address ranges will be displayed in the list after a message indicating operation success appears.

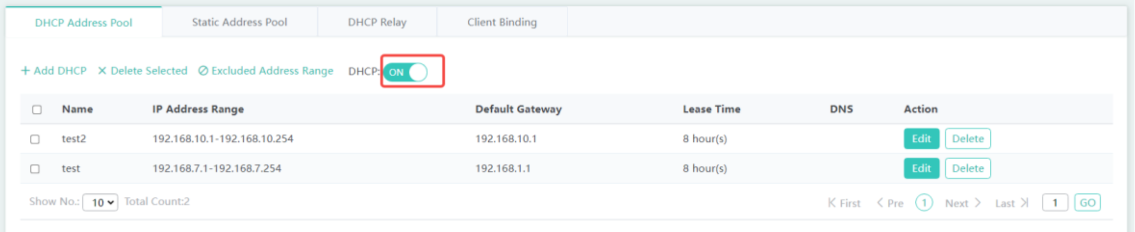


□	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
□	test2	192.168.10.1-192.168.10.254	192.168.10.1	8 hour(s)		Edit Delete
□	test	192.168.7.1-192.168.7.254	192.168.1.1	8 hour(s)		Edit Delete

Excluded Address Range: Excluded addresses will not be allocated to the client. The excluded address range is formatted as 1.1.1.1-1.1.1.30. Entering only 1.1.1.1 indicates one single excluded address.

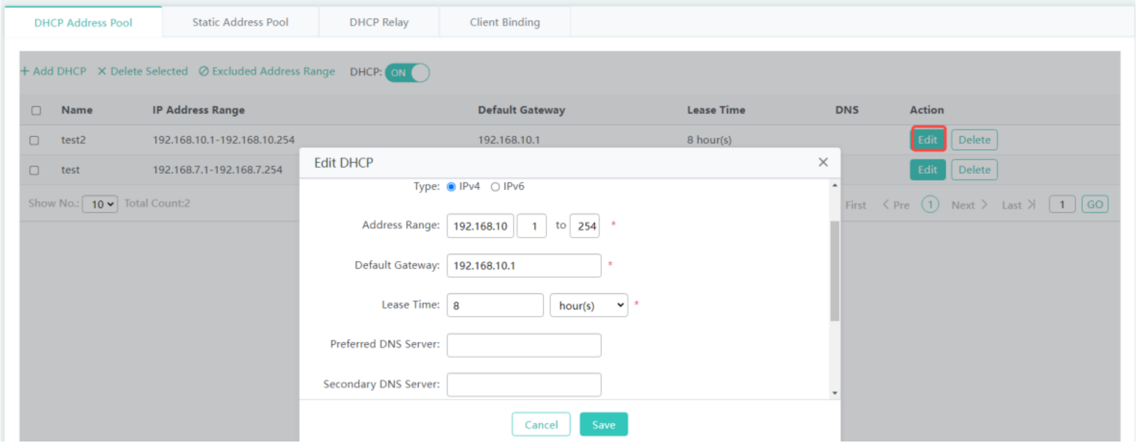
Excluded Address Range1: 192.168.10.30 - 192.168.10.40 +

(4) Enabling or disabling DHCP service: Toggle on or off the **DHCP** button to enable or disable the DHCP service. Choose **Monitoring** > **DHCP** > **Server Status** to view the DHCP service status.



□	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
□	test2	192.168.10.1-192.168.10.254	192.168.10.1	8 hour(s)		Edit Delete
□	test	192.168.7.1-192.168.7.254	192.168.1.1	8 hour(s)		Edit Delete

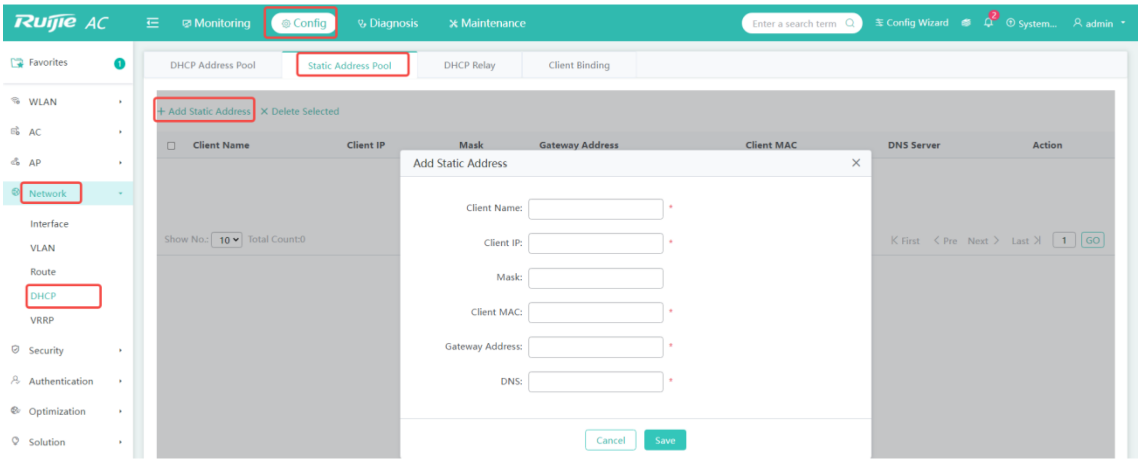
(5) Editing DHCP address pools: Click **Edit** in the **Action** column and a window pops up displaying the information about the DHCP address pool. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



2. Static Address Pool

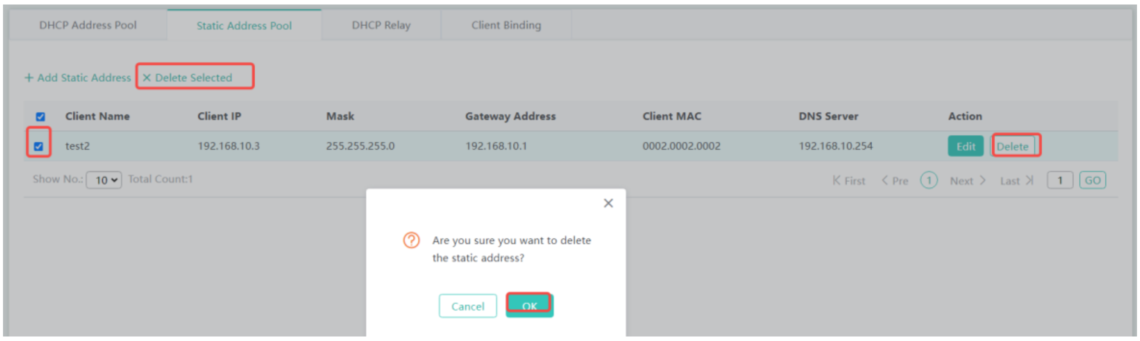
Choose **Config** > **Network** > **DHCP** > **Static Address Pool**.

(1) Adding static address pools: Click **Add Static Address** and edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.



Parameter	Description
Client Name	Enter the name of the static address.
Client IP	Configure the IP address.
Mask	Configure the subnet mask.
Client MAC	Enter the MAC address of the client.
Gateway Address	Configure the IP address of the egress gateway. This field is mandatory.
DNS	Configure the DNS server address. This field is mandatory.

(2) Deleting static IP address: Click **Delete** in the **Action** column to delete a static IP address. Select multiple items and click **Delete Selected**. Click **OK** in the pop-up window to batch delete static IP addresses.



DHCP Address Pool | Static Address Pool | DHCP Relay | Client Binding

+ Add Static Address ✕ Delete Selected

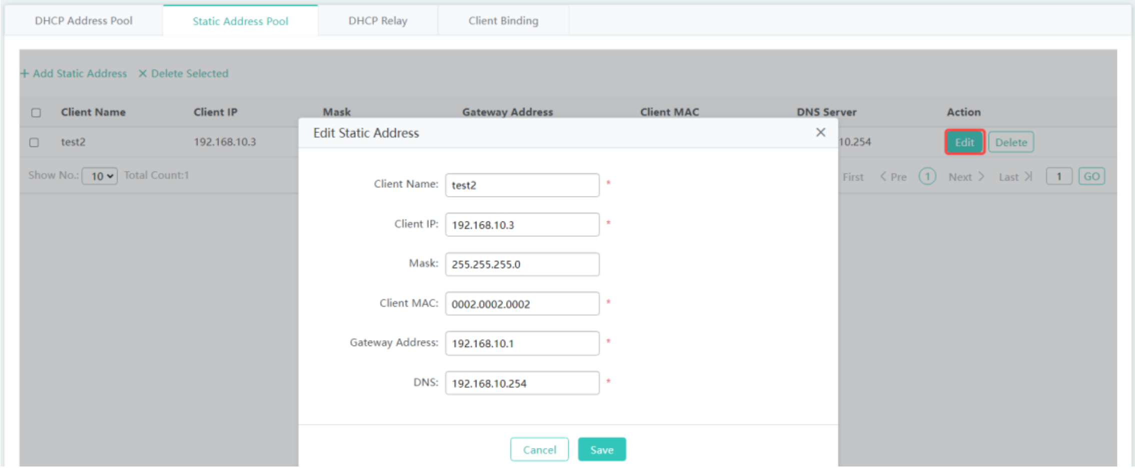
☑	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
☑	test2	192.168.10.3	255.255.255.0	192.168.10.1	0002.0002.0002	192.168.10.254	Edit Delete

Show No.: 10 Total Count:1 First Pre 1 Next Last 1 GO

Are you sure you want to delete the static address?

Cancel OK

(3) Editing static IP address: Click **Edit** in the **Action** column and a window pops up displaying the information about the static IP address. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



DHCP Address Pool | Static Address Pool | DHCP Relay | Client Binding

+ Add Static Address ✕ Delete Selected

□	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
□	test2	192.168.10.3				10.254	Edit Delete

Show No.: 10 Total Count:1 First Pre 1 Next Last 1 GO

Edit Static Address

Client Name: test2 *

Client IP: 192.168.10.3 *

Mask: 255.255.255.0

Client MAC: 0002.0002.0002 *

Gateway Address: 192.168.10.1 *

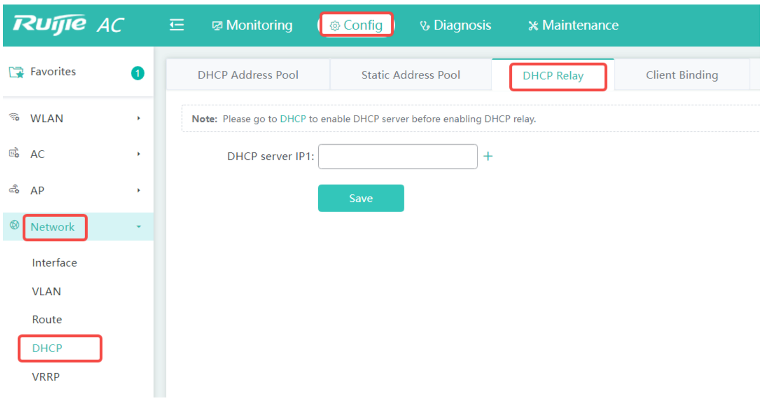
DNS: 192.168.10.254 *

Cancel Save

3. DHCP relay

Choose **Config** > **Network** > **DHCP** > **DHCP Relay**.

Enter the IP address of the DHCP relay and click **Save**.



Ruijie AC Monitoring Config Diagnosis Maintenance

Favorites 1

WLAN

AC

AP

Network

Interface

VLAN

Route

DHCP

VRRP

DHCP Address Pool | Static Address Pool | DHCP Relay | Client Binding

Note: Please go to DHCP to enable DHCP server before enabling DHCP relay.

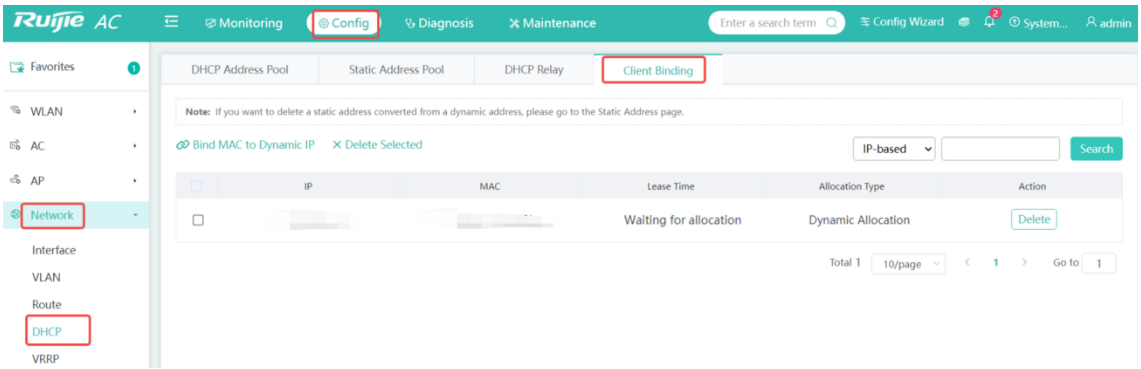
DHCP server IP1: +

Save

4. Client Binding

Choose **Config** > **Network** > **DHCP** > **Client Binding**.

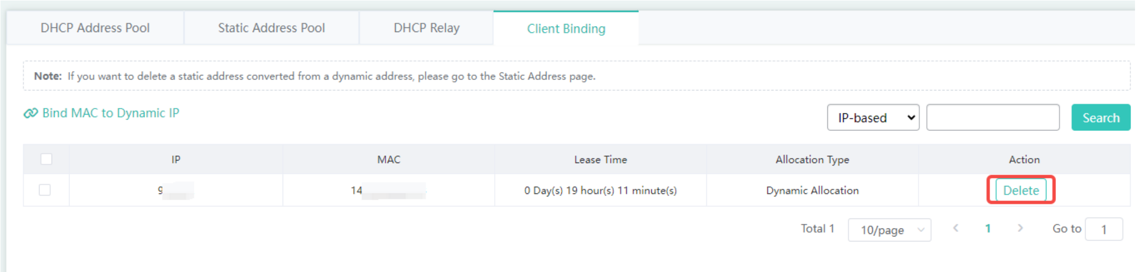
(1) Binding MAC address with dynamic IP address: Select the MAC addresses in the list and click **Bind MAC to Dynamic IP**. Click **OK** in the pop-up window to bind the MAC addresses with dynamic IP addresses.



Note: If you want to delete a static address converted from a dynamic address, please go to the Static Address page.

□	IP	MAC	Lease Time	Allocation Type	Action
□	[redacted]	[redacted]	Waiting for allocation	Dynamic Allocation	Delete

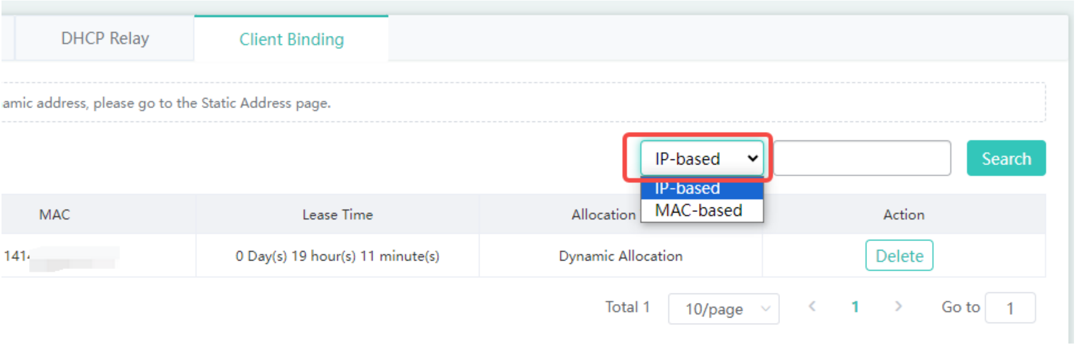
(2) Unbinding MAC address with dynamic IP address: Click **Delete** in the **Action** column and a window pops up. Click **OK** to unbind the MAC address.



Note: If you want to delete a static address converted from a dynamic address, please go to the Static Address page.

□	IP	MAC	Lease Time	Allocation Type	Action
□	9[redacted]	14[redacted]	0 Day(s) 19 hour(s) 11 minute(s)	Dynamic Allocation	Delete

(3) Searching for clients by IP address or MAC: Enter the IP address or MAC in the search bar. Click **Search** and the results are displayed in the list.



amic address, please go to the Static Address page.

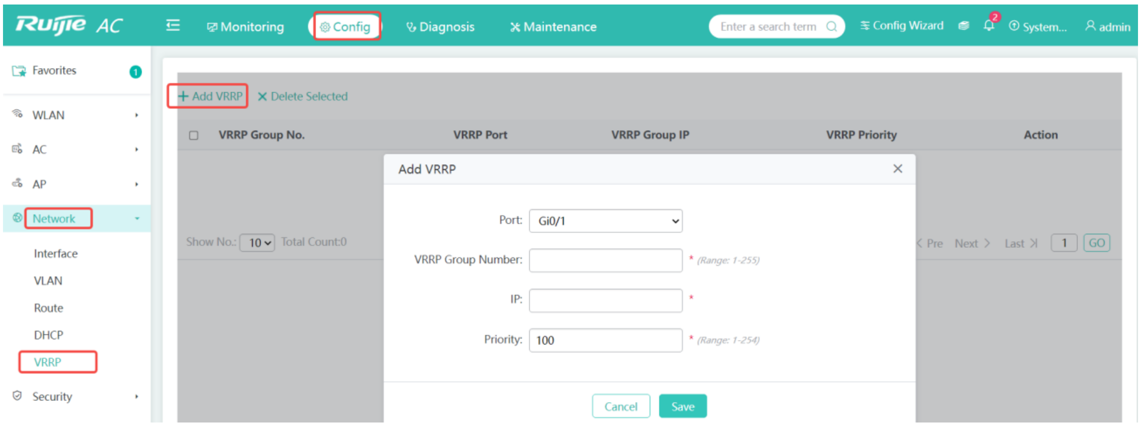
MAC	Lease Time	Allocation	Action
141[redacted]	0 Day(s) 19 hour(s) 11 minute(s)	Dynamic Allocation	Delete

5.4.5 VRRP

Choose **Config** > **Network** > **VRRP**.

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol. VRRP adopts the master-backup design to ensure migration of functions from a Master router to a Backup one when the Master failed, without influencing internal and external data communication or modifying Local Area Network (LAN) configuration.

(1) Adding VRRP groups: Click **Add VRRP**. Edit the fields in the pop-up window. Click **Save** and the VRRP group will be displayed in the list after a message indicating operation success appears.



☐	VRRP Group No.	VRRP Port	VRRP Group IP	VRRP Priority	Action

Add VRRP

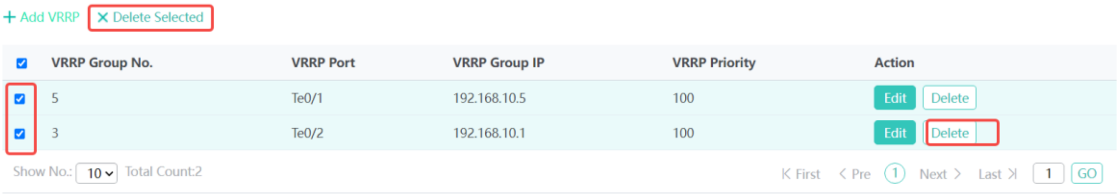
Port: Gi0/1

VRRP Group Number: * (Range: 1-255)

IP: *

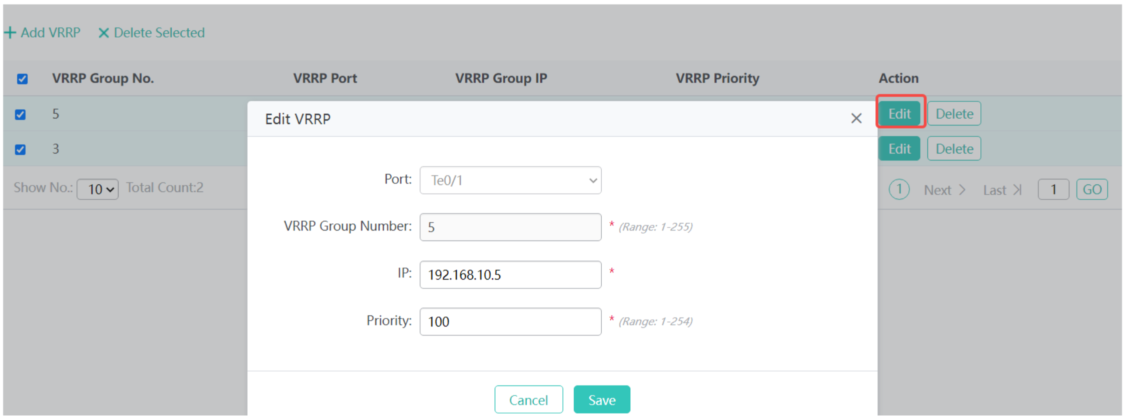
Priority: 100 * (Range: 1-254)

(2) Deleting VRRP groups: Select the VRRP groups in the list and click **Delete Selected**. Click **OK** in the pop-up window to delete VRRP groups.



☑	VRRP Group No.	VRRP Port	VRRP Group IP	VRRP Priority	Action
☑	5	Te0/1	192.168.10.5	100	Edit Delete
☑	3	Te0/2	192.168.10.1	100	Edit Delete

(3) Editing VRRP groups: Click **Edit** in the **Action** column and a window pops up displaying the information about the VRRP group. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



☑	VRRP Group No.	VRRP Port	VRRP Group IP	VRRP Priority	Action
☑	5				Edit Delete
☑	3				Edit Delete

Edit VRRP

Port: Te0/1

VRRP Group Number: 5 * (Range: 1-255)

IP: 192.168.10.5 *

Priority: 100 * (Range: 1-254)

5.5 Security

5.5.1 Containment

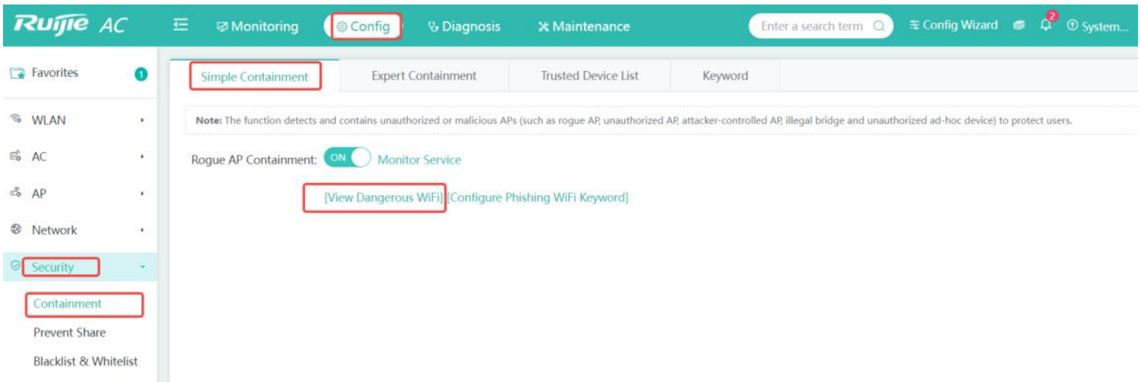
Choose **Config** > **Security** > **Containment**.

Rogue APs may exist on a wireless network. They may have security vulnerabilities or be controlled by attackers, seriously threatening the security of user networks. Enable the containment feature on the AC to attack the rogue APs so that other wireless clients cannot associate with the rogue APs.

1. Basic Configuration for Containment

When containment is currently disabled, and no AP in monitoring or hybrid mode is detected, a pop-up window is displayed to ask users to enable the AP monitoring feature. Click **OK** to jump to the **Monitor Service** page.

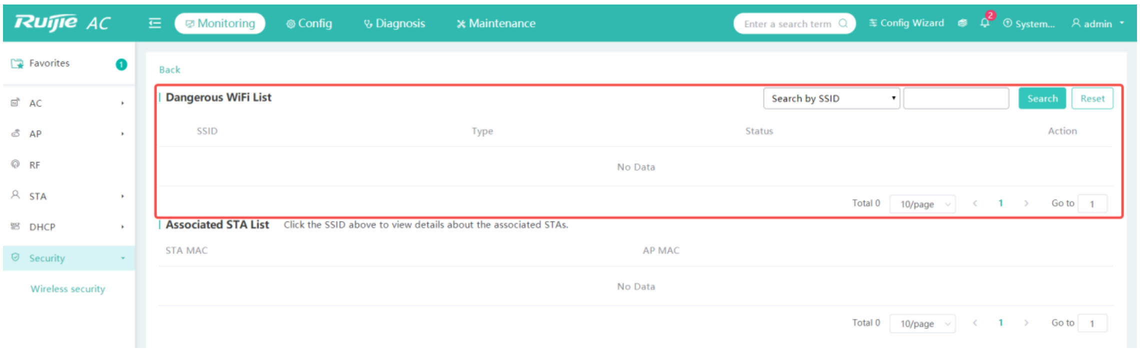
After enabling containment, click **View Dangerous WiFi** to access the **Dangerous WiFi List** page and trust or contain Wi-Fi networks.



Note: The function detects and contains unauthorized or malicious APs (such as rogue AP, unauthorized AP, attacker-controlled AP, illegal bridge and unauthorized ad-hoc device) to protect users.

Rogue AP Containment: ON Monitor Service

[View Dangerous WiFi] [Configure Phishing WiFi Keyword]



Dangerous WiFi List

SSID	Type	Status	Action
No Data			

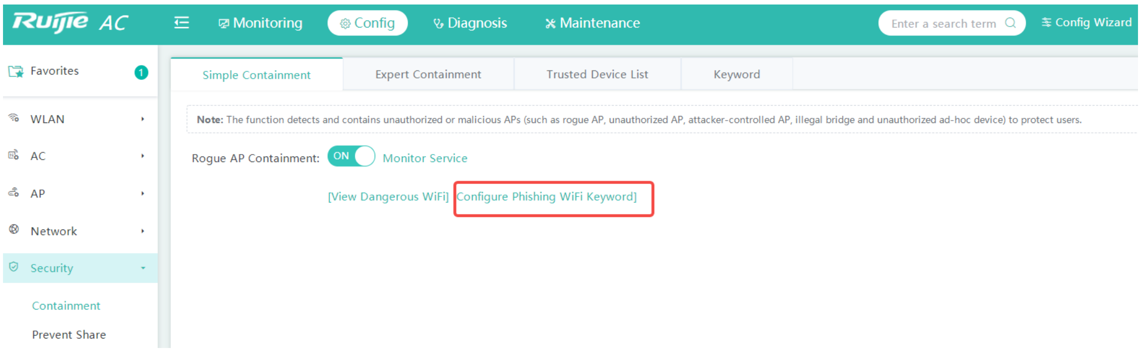
Total 0 10/page 1 Go to 1

Associated STA List Click the SSID above to view details about the associated STAs.

STA MAC	AP MAC
No Data	

Total 0 10/page 1 Go to 1

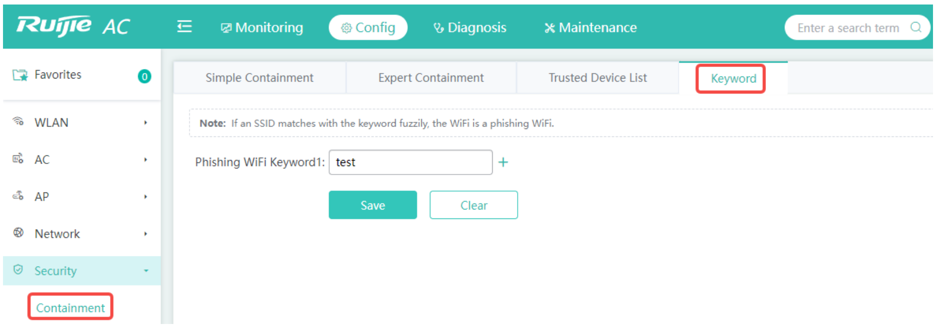
Click **Configure Phishing WiFi Keyword** to access the **Keyword** page and configure the keyword.



Note: The function detects and contains unauthorized or malicious APs (such as rogue AP, unauthorized AP, attacker-controlled AP, illegal bridge and unauthorized ad-hoc device) to protect users.

Rogue AP Containment: ON Monitor Service

[View Dangerous WiFi] [Configure Phishing WiFi Keyword]

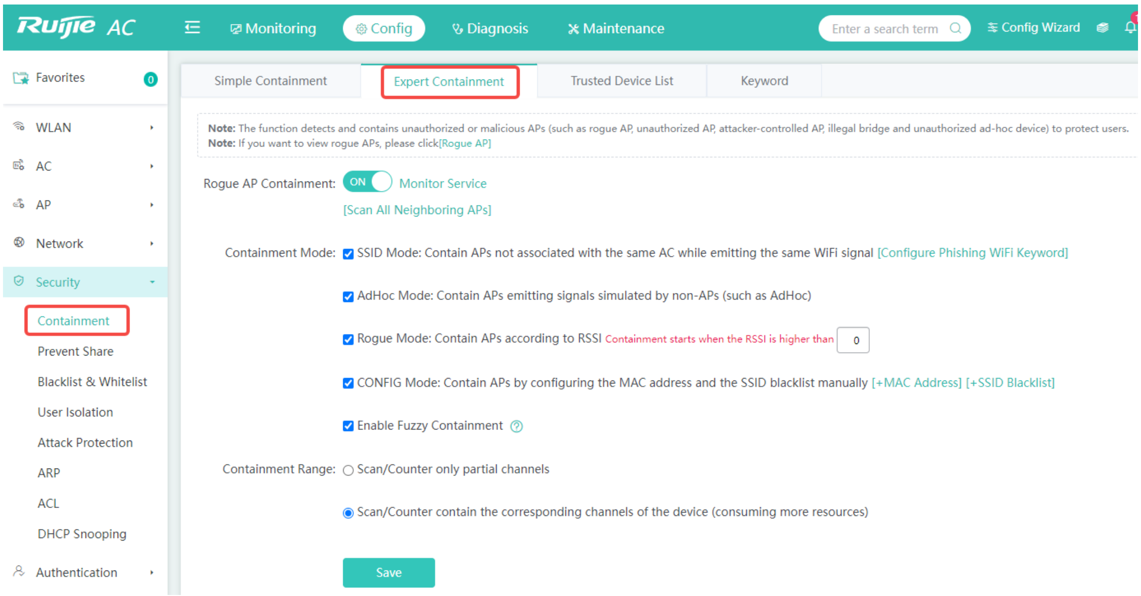


Note: If an SSID matches with the keyword fuzzily, the WiFi is a phishing WiFi.

Phishing WiFi Keyword1: test +

2. Specialized Configuration for Containment

Enable or disable the rogue AP containment feature on the AC.



Note: The function detects and contains unauthorized or malicious APs (such as rogue AP, unauthorized AP, attacker-controlled AP, illegal bridge and unauthorized ad-hoc device) to protect users.
Note: If you want to view rogue APs, please click[Rogue AP]

Rogue AP Containment: ON Monitor Service
[Scan All Neighboring APs]

Containment Mode: ☑ SSID Mode: Contain APs not associated with the same AC while emitting the same WiFi signal [Configure Phishing WiFi Keyword]

☑ AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)

☑ Rogue Mode: Contain APs according to RSSI Containment starts when the RSSI is higher than 0

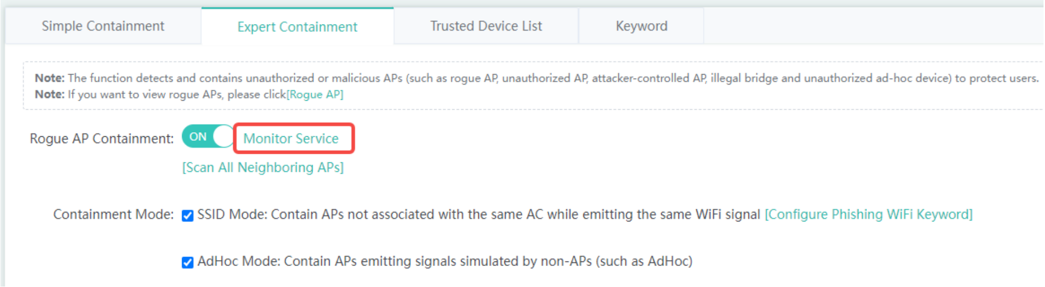
☑ CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [+MAC Address] [+SSID Blacklist]

☑ Enable Fuzzy Containment

Containment Range: ○ Scan/Counter only partial channels

● Scan/Counter contain the corresponding channels of the device (consuming more resources)

(1) Enable the monitoring mode for a specified AP: The AP must be configured with the hybrid or monitoring mode before the containment feature takes effect. Click **Monitor Service** to access the **Monitor Service** page. Click **Monitor** or **Hybrid** to configure the AP mode.

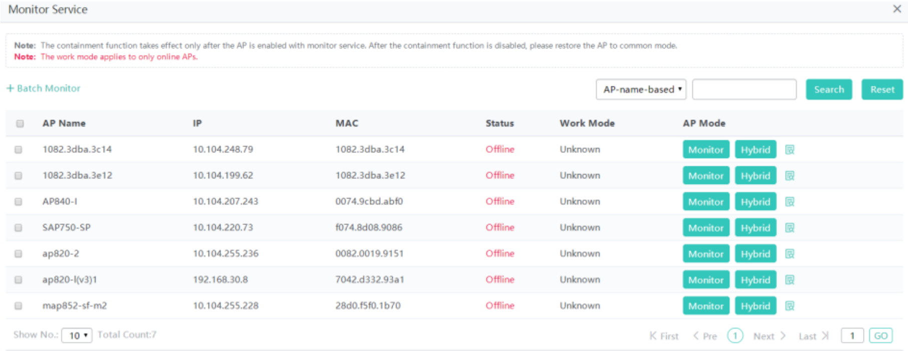


Note: The function detects and contains unauthorized or malicious APs (such as rogue AP, unauthorized AP, attacker-controlled AP, illegal bridge and unauthorized ad-hoc device) to protect users.
Note: If you want to view rogue APs, please click[Rogue AP]

Rogue AP Containment: ON Monitor Service
[Scan All Neighboring APs]

Containment Mode: ☑ SSID Mode: Contain APs not associated with the same AC while emitting the same WiFi signal [Configure Phishing WiFi Keyword]

☑ AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)

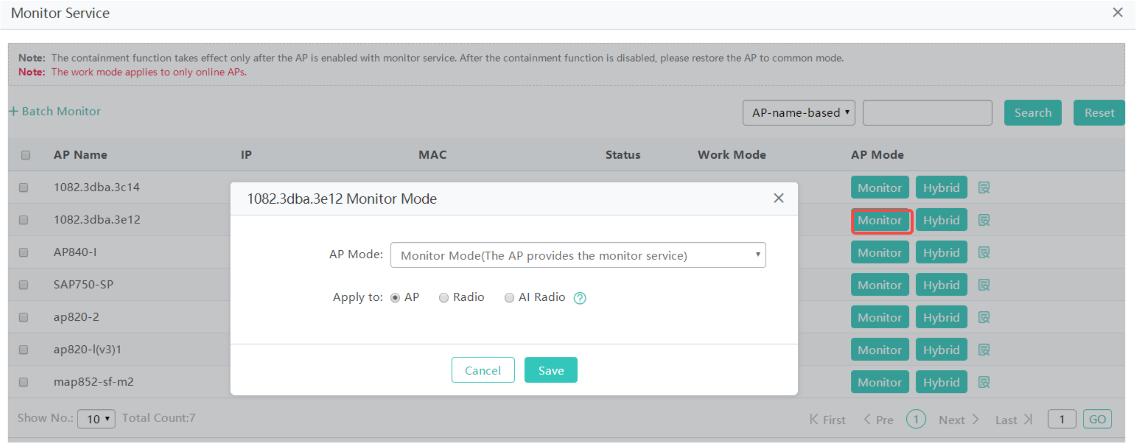


Note: The containment function takes effect only after the AP is enabled with monitor service. After the containment function is disabled, please restore the AP to common mode.
Note: The work mode applies to only online APs.

□	AP Name	IP	MAC	Status	Work Mode	AP Mode
□	1082.3dba.3c14	10.104.248.79	1082.3dba.3c14	Offline	Unknown	Monitor Hybrid
□	1082.3dba.3e12	10.104.199.62	1082.3dba.3e12	Offline	Unknown	Monitor Hybrid
□	AP840-I	10.104.207.243	0074.9cbd.abf0	Offline	Unknown	Monitor Hybrid
□	SAP750-SP	10.104.220.73	f074.8d08.9086	Offline	Unknown	Monitor Hybrid
□	ap820-2	10.104.255.236	0082.0019.9151	Offline	Unknown	Monitor Hybrid
□	ap820-I(v3)1	192.168.30.8	7042.d332.93a1	Offline	Unknown	Monitor Hybrid
□	map852-sf-m2	10.104.255.228	28d0.f5f0.1b70	Offline	Unknown	Monitor Hybrid

Show No.: 10 Total Count:7 First Pre 1 Next Last 1 GO

The AP information is displayed on the pop-up dialog box. Edit the information. When the AP that provides the AI radio feature is configured with the monitoring mode, the AI radio should be monitored and contained first. Click **Save**. The **Save succeeded.** message is displayed.



Monitor Service

Note: The containment function takes effect only after the AP is enabled with monitor service. After the containment function is disabled, please restore the AP to common mode.
Note: The work mode applies to only online APs.

AP Name	IP	MAC	Status	Work Mode	AP Mode
1082.3dba.3c14					Monitor Hybrid
1082.3dba.3e12					Monitor Hybrid
AP840-I					Monitor Hybrid
SAP750-SP					Monitor Hybrid
ap820-2					Monitor Hybrid
ap820-I(v3)1					Monitor Hybrid
map852-sf-m2					Monitor Hybrid

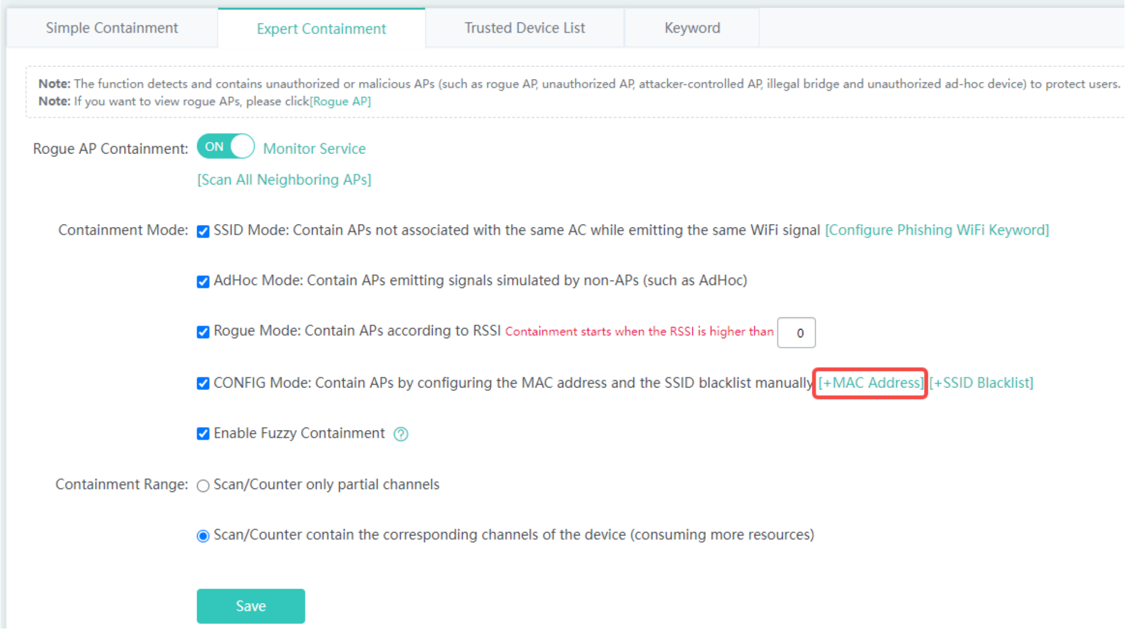
Show No.: 10 Total Count:7

1082.3dba.3e12 Monitor Mode

AP Mode: Monitor Mode(The AP provides the monitor service)

Apply to: ● AP ○ Radio ○ AI Radio

(2) Add the MAC address of a wireless device: The following configured MAC addresses will be contained.



Note: The function detects and contains unauthorized or malicious APs (such as rogue AP, unauthorized AP, attacker-controlled AP, illegal bridge and unauthorized ad-hoc device) to protect users.
Note: If you want to view rogue APs, please click[Rogue AP]

Rogue AP Containment: ON Monitor Service

[Scan All Neighboring APs]

Containment Mode: ☑ SSID Mode: Contain APs not associated with the same AC while emitting the same WiFi signal [Configure Phishing WiFi Keyword]

☑ AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)

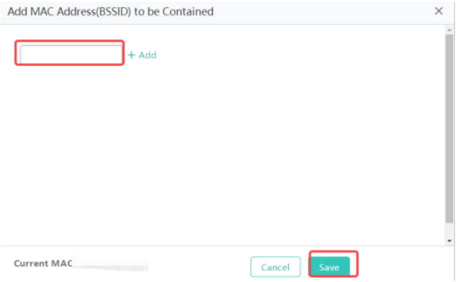
☑ Rogue Mode: Contain APs according to RSSI Containment starts when the RSSI is higher than 0

☑ CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [+MAC Address] [+SSID Blacklist]

☑ Enable Fuzzy Containment

Containment Range: ○ Scan/Counter only partial channels

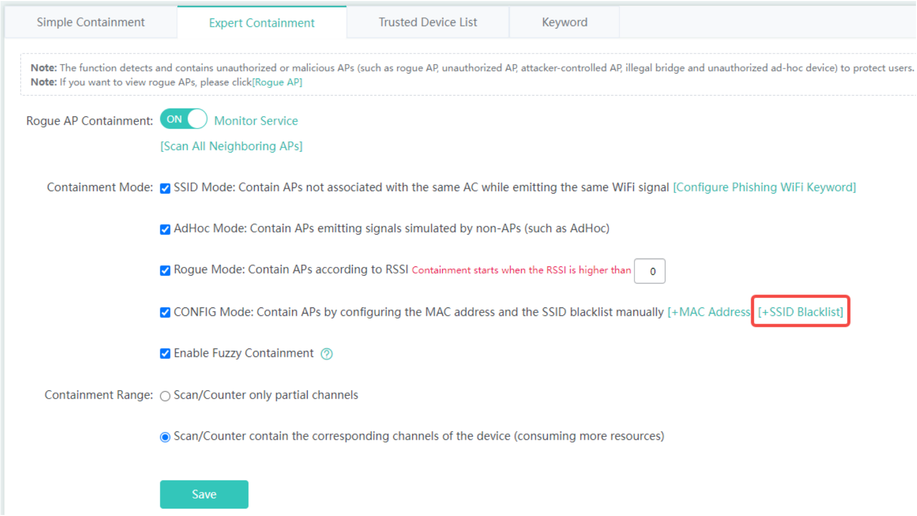
● Scan/Counter contain the corresponding channels of the device (consuming more resources)



Add MAC Address(BSSID) to be Contained

Current MAC

(3) Add an SSID blocklist:



Note: The function detects and contains unauthorized or malicious APs (such as rogue AP, unauthorized AP, attacker-controlled AP, illegal bridge and unauthorized ad-hoc device) to protect users.
Note: If you want to view rogue APs, please click[Rogue AP]

Rogue AP Containment: ON Monitor Service
[Scan All Neighboring APs]

Containment Mode: ☑ SSID Mode: Contain APs not associated with the same AC while emitting the same WiFi signal [Configure Phishing WiFi Keyword]

☑ AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)

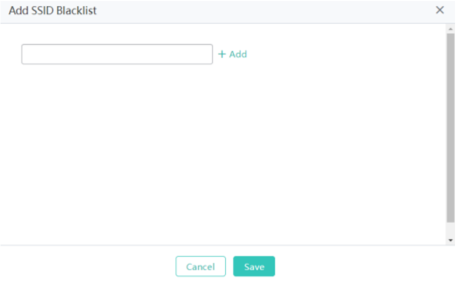
☑ Rogue Mode: Contain APs according to RSSI Containment starts when the RSSI is higher than 0

☑ CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [+MAC Address [+SSID Blacklist]

☑ Enable Fuzzy Containment

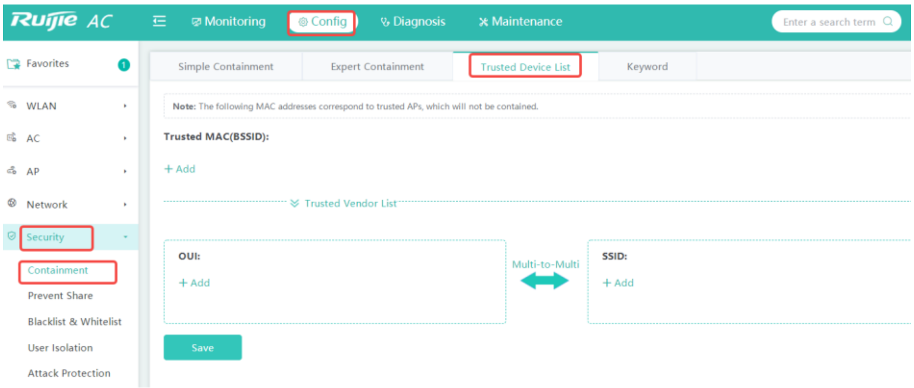
Containment Range: ○ Scan/Counter only partial channels

● Scan/Counter contain the corresponding channels of the device (consuming more resources)



3. Trusted Device List

When the rogue AP containment feature is enabled on the AC, unauthorized APs will be contained, while some APs are trusted devices and should be treated differently. The MAC address of a trusted device can be configured.

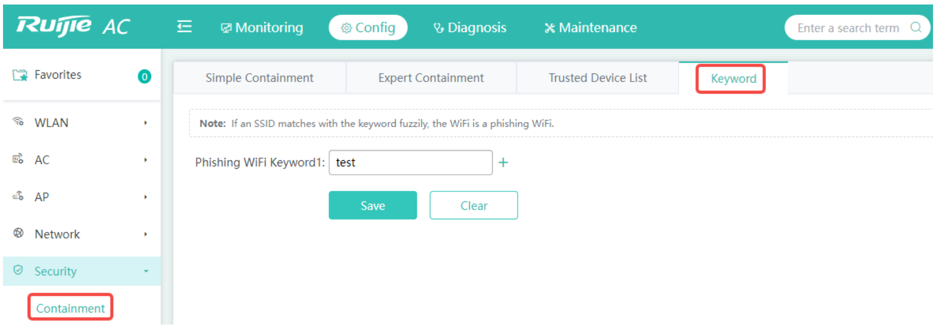


Note: The following MAC addresses correspond to trusted APs, which will not be contained.

Trusted MAC(BSSID):

4. Phishing Wi-Fi Keyword

Fuzzy matching of a phishing Wi-Fi keyword helps scan Wi-Fi signals on a network. If an SSID of a Wi-Fi network matches the keyword fuzzily, the Wi-Fi network is regarded as a phishing network.



Note: If an SSID matches with the keyword fuzzily, the WiFi is a phishing WiFi.

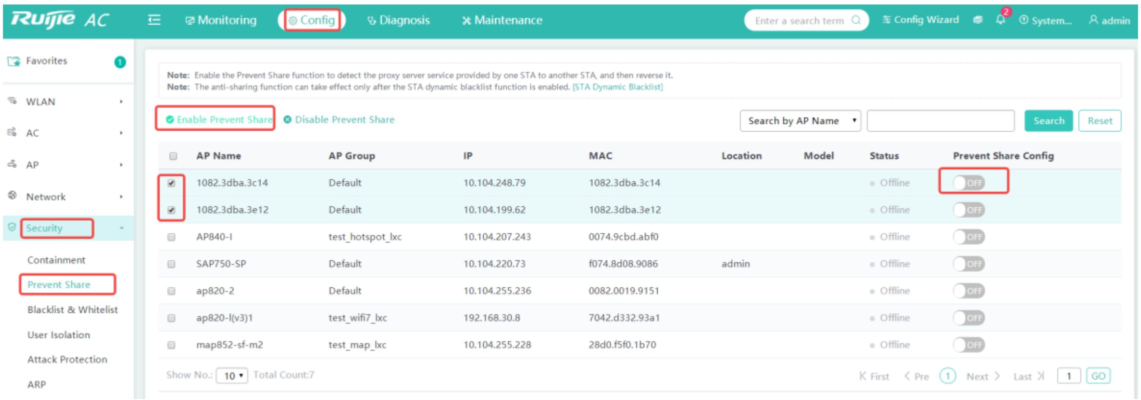
Phishing WiFi Keyword1: test

5.5.2 Sharing Prevention

Choose **Config** > **Security** > **Prevent Share**.

After sharing prevention is enabled, the system detects whether one STA provides the proxy service to another and adds the STA providing the proxy service into the containment list.

(1) Enable sharing prevention: Select APs to be enabled with sharing prevention in the list. Click **Enable Prevent Share**. In the pop-up confirmation dialog box, click **OK** to enable sharing prevention.

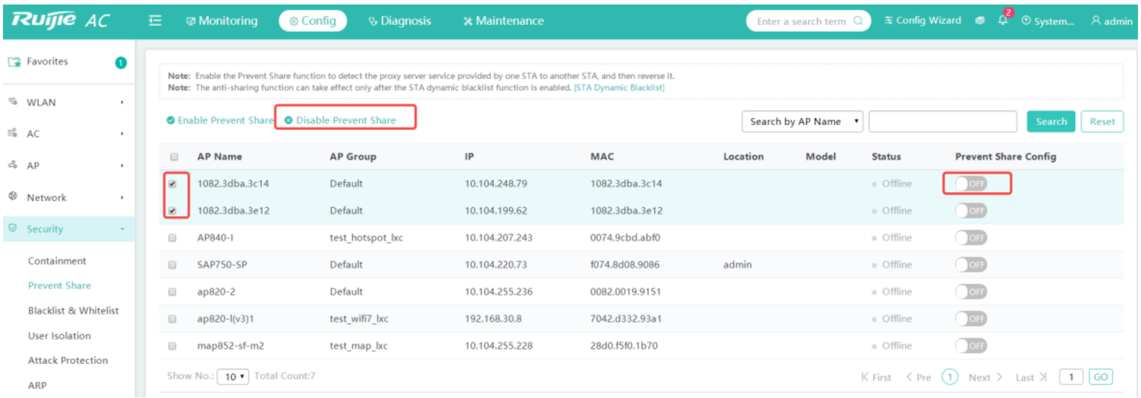


Note: Enable the Prevent Share function to detect the proxy server service provided by one STA to another STA, and then reverse it.
Note: The anti-sharing function can take effect only after the STA dynamic blacklist function is enabled. [STA Dynamic Blacklist]

□	AP Name	AP Group	IP	MAC	Location	Model	Status	Prevent Share Config
☑	1082.3dba.3c14	Default	10.104.248.79	1082.3dba.3c14			Offline	OFF
☑	1082.3dba.3e12	Default	10.104.199.62	1082.3dba.3e12			Offline	OFF
□	AP840-I	test_hotspot_lxc	10.104.207.243	0074.9cbd.abf0			Offline	OFF
□	SAP750-SP	Default	10.104.220.73	f074.8d08.9086	admin		Offline	OFF
□	ap820-2	Default	10.104.255.236	0082.0019.9151			Offline	OFF
□	ap820-l(v3)1	test_wifi7_lxc	192.168.30.8	7042.d332.93a1			Offline	OFF
□	map852-sf-m2	test_map_lxc	10.104.255.228	28d0.f5f0.1b70			Offline	OFF

Show No.: 10 Total Count:7

(2) Disable sharing prevention: Select APs for which sharing prevention needs to be disabled in the list. Click **Disable Prevent Share**. In the pop-up confirmation dialog box, click **OK** to disable sharing prevention.



Note: Enable the Prevent Share function to detect the proxy server service provided by one STA to another STA, and then reverse it.
Note: The anti-sharing function can take effect only after the STA dynamic blacklist function is enabled. [STA Dynamic Blacklist]

□	AP Name	AP Group	IP	MAC	Location	Model	Status	Prevent Share Config
☑	1082.3dba.3c14	Default	10.104.248.79	1082.3dba.3c14			Offline	OFF
☑	1082.3dba.3e12	Default	10.104.199.62	1082.3dba.3e12			Offline	OFF
□	AP840-I	test_hotspot_lxc	10.104.207.243	0074.9cbd.abf0			Offline	OFF
□	SAP750-SP	Default	10.104.220.73	f074.8d08.9086	admin		Offline	OFF
□	ap820-2	Default	10.104.255.236	0082.0019.9151			Offline	OFF
□	ap820-l(v3)1	test_wifi7_lxc	192.168.30.8	7042.d332.93a1			Offline	OFF
□	map852-sf-m2	test_map_lxc	10.104.255.228	28d0.f5f0.1b70			Offline	OFF

Show No.: 10 Total Count:7

5.5.3 Configuring the Blocklist/Allowlist

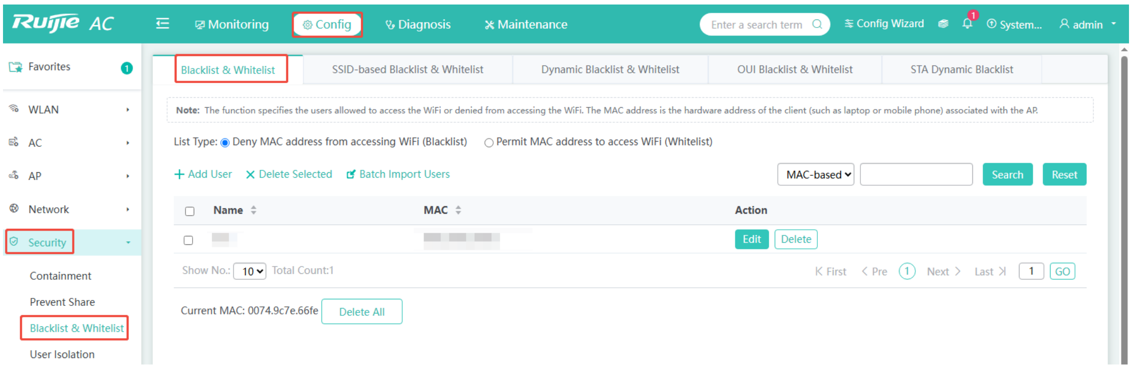
Choose **Config** > **Security** > **Blacklist & Whitelist**.

Note

- The number of users denied or permitted to access the Internet through Wi-Fi varies with the device. The value displayed on the page shall prevail.
- The procedure for configuring blacklists and allowlists is similar. The following uses blacklists as an example.

1. Configuring the Blocklist or Allowlist for the AC

To enhance wireless security, control the access of wireless users by assigning wireless access to certain users or prohibiting certain users from accessing the wireless network.



Note: The function specifies the users allowed to access the WiFi or denied from accessing the WiFi. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

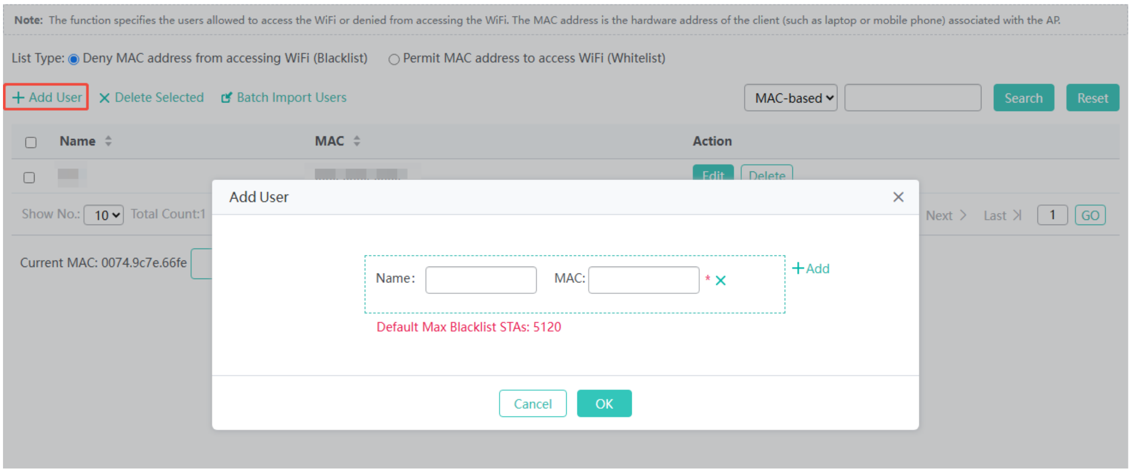
List Type: ● Deny MAC address from accessing WiFi (Blacklist) ○ Permit MAC address to access WiFi (Whitelist)

Show No.: 10 Total Count:1

Current MAC: 0074.9c7e.66fe

Add a MAC address to the blocklist or allowlist.

(1) Add a list: Click **Add User** to add the MAC address of a user. Multiple addresses can be added.



Note: The function specifies the users allowed to access the WiFi or denied from accessing the WiFi. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

List Type: ● Deny MAC address from accessing WiFi (Blacklist) ○ Permit MAC address to access WiFi (Whitelist)

Show No.: 10 Total Count:1

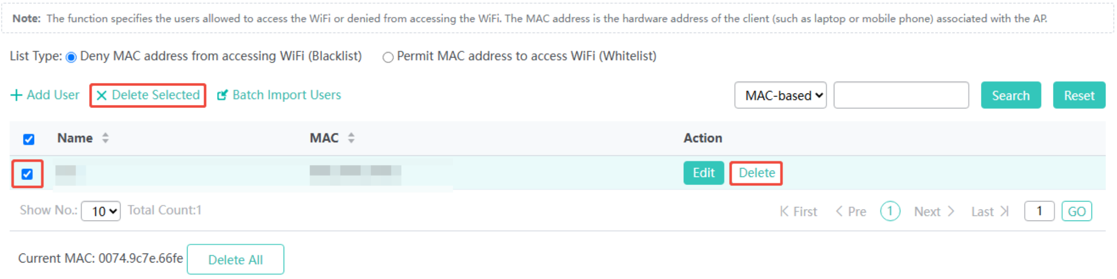
Current MAC: 0074.9c7e.66fe

Name:

MAC: *

Default Max Blacklist STAs: 5120

(2) Delete a list: Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a user. To delete multiple users, select the target users in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the users.



Note: The function specifies the users allowed to access the WiFi or denied from accessing the WiFi. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

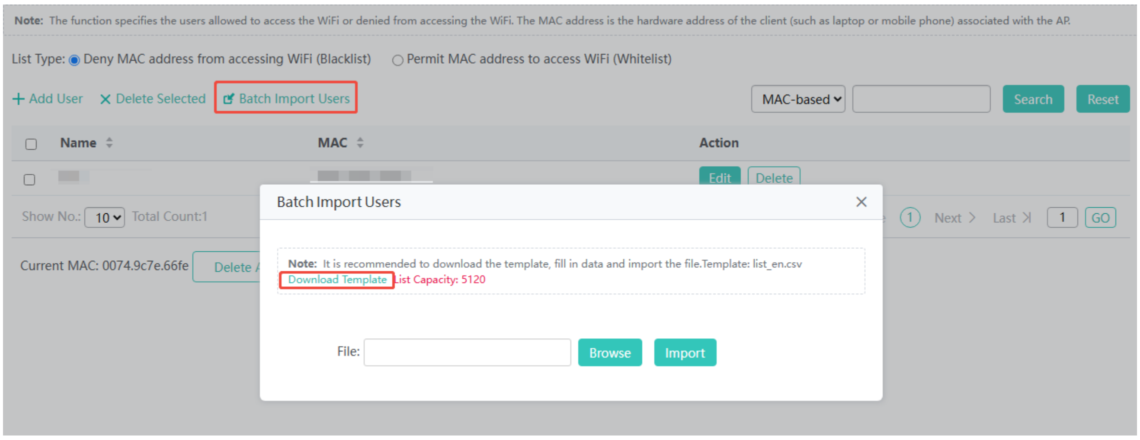
List Type: ● Deny MAC address from accessing WiFi (Blacklist) ○ Permit MAC address to access WiFi (Whitelist)

☑	Name	MAC	Action
☑	[redacted]	[redacted]	Edit Delete

Show No.: 10 Total Count:1

Current MAC: 0074.9c7e.66fe

(3) Batch import lists: Click **Batch Import Users**. Download and fill in the template. Import the file.



Note: The function specifies the users allowed to access the WiFi or denied from accessing the WiFi. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

List Type: ● Deny MAC address from accessing WiFi (Blacklist) ○ Permit MAC address to access WiFi (Whitelist)

Batch Import Users

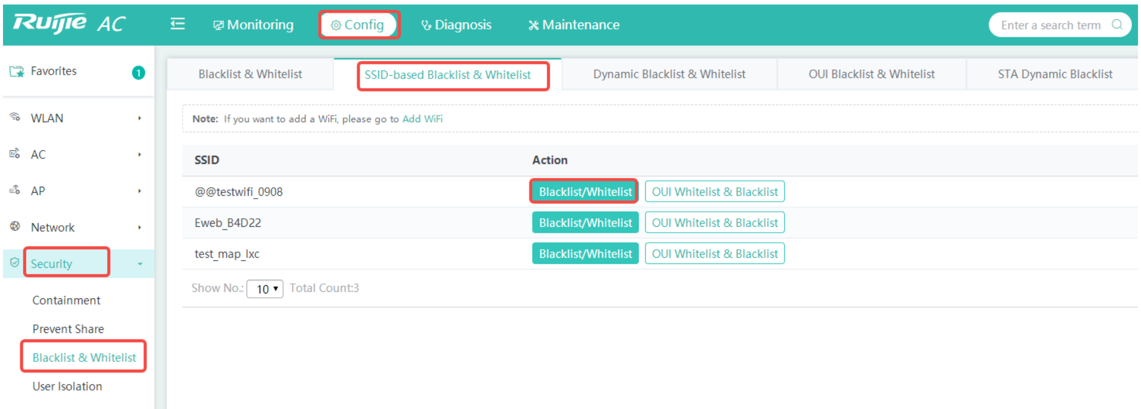
Note: It is recommended to download the template, fill in data and import the file.Template: list_en.csv

Download Template List Capacity: 5120

File:

2. Configuring the SSID-based Blocklist or Allowlist

Click **Blacklist/Whitelist** for a specified Wi-Fi to access the configuration page. Select one list type.

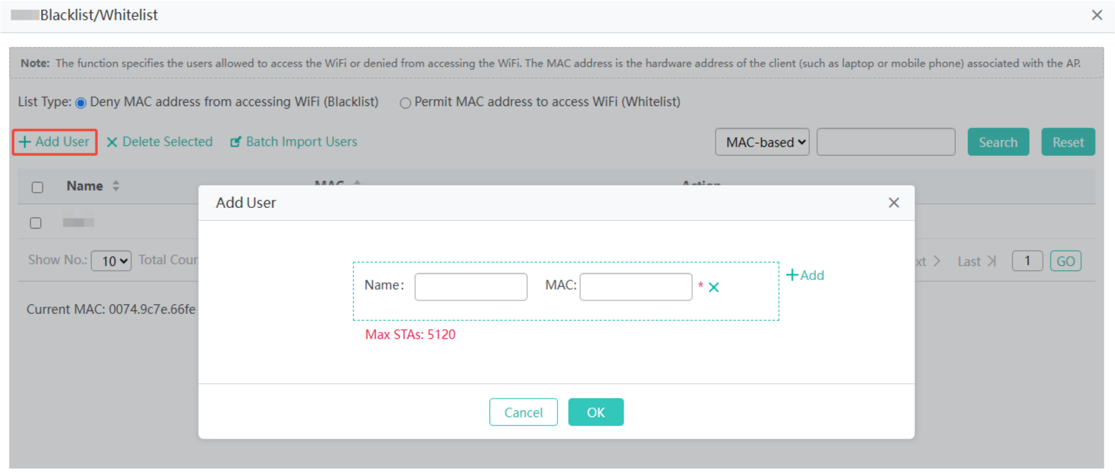


Note: If you want to add a WiFi, please go to Add WiFi

SSID	Action
@@testwifi_0908	Blacklist/Whitelist OUI Whitelist & Blacklist
Eweb_B4D22	Blacklist/Whitelist OUI Whitelist & Blacklist
test_map_lxc	Blacklist/Whitelist OUI Whitelist & Blacklist

Show No.: 10 Total Count:3

(1) Add a list: Click **Add User**. Add the MAC address of a device. Click **OK**.



[redacted]Blacklist/Whitelist

Note: The function specifies the users allowed to access the WiFi or denied from accessing the WiFi. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

List Type: ● Deny MAC address from accessing WiFi (Blacklist) ○ Permit MAC address to access WiFi (Whitelist)

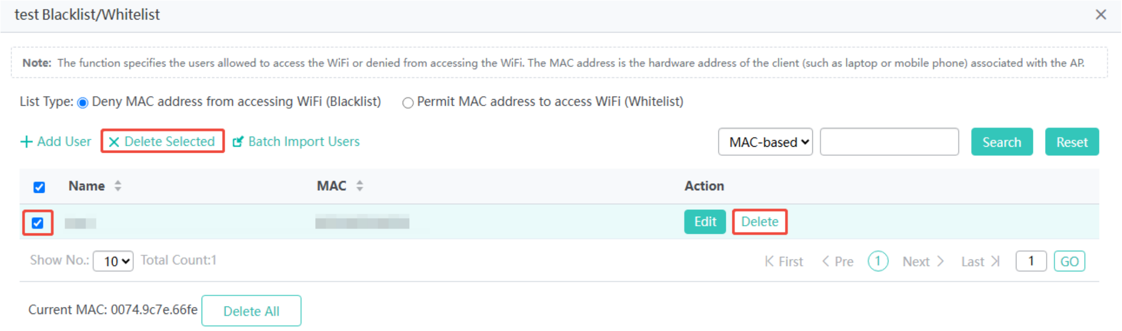
Current MAC: 0074.9c7e.66fe

Add User

Name: MAC: *

Max STAs: 5120

(2) Delete a list: Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a user. To delete multiple users, select the target users in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the users.



test Blacklist/Whitelist

Note: The function specifies the users allowed to access the WiFi or denied from accessing the WiFi. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

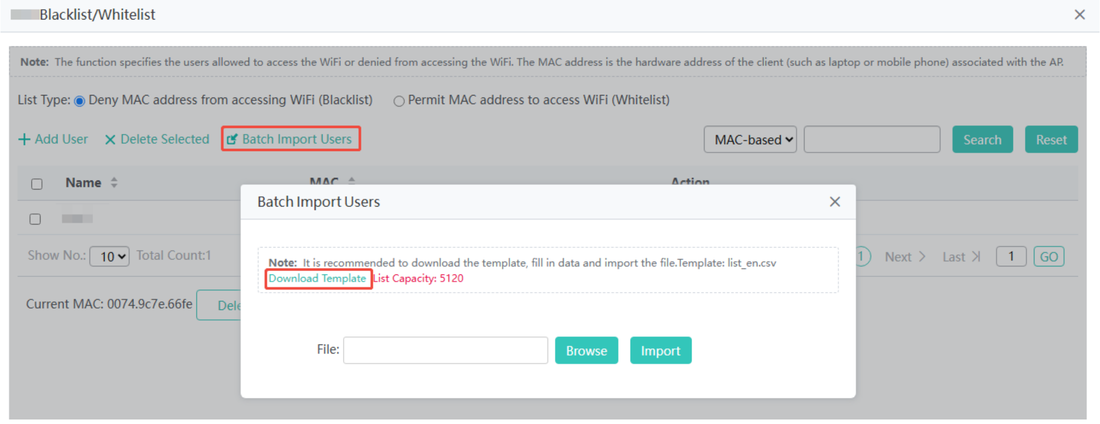
List Type: ● Deny MAC address from accessing WiFi (Blacklist) ○ Permit MAC address to access WiFi (Whitelist)

☑	Name	MAC	Action
☑	[redacted]	[redacted]	Edit Delete

Show No.: 10 Total Count:1

Current MAC: 0074.9c7e.66fe

(3) Batch import blacklists: Click **Batch Import Users**. Download the template. Fill in the template and save it. Click **Browse**. Select the preceding saved template. Click **Import**.



[redacted]Blacklist/Whitelist

Note: The function specifies the users allowed to access the WiFi or denied from accessing the WiFi. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

List Type: ● Deny MAC address from accessing WiFi (Blacklist) ○ Permit MAC address to access WiFi (Whitelist)

Show No.: 10 Total Count:1

Current MAC: 0074.9c7e.66fe

Batch Import Users

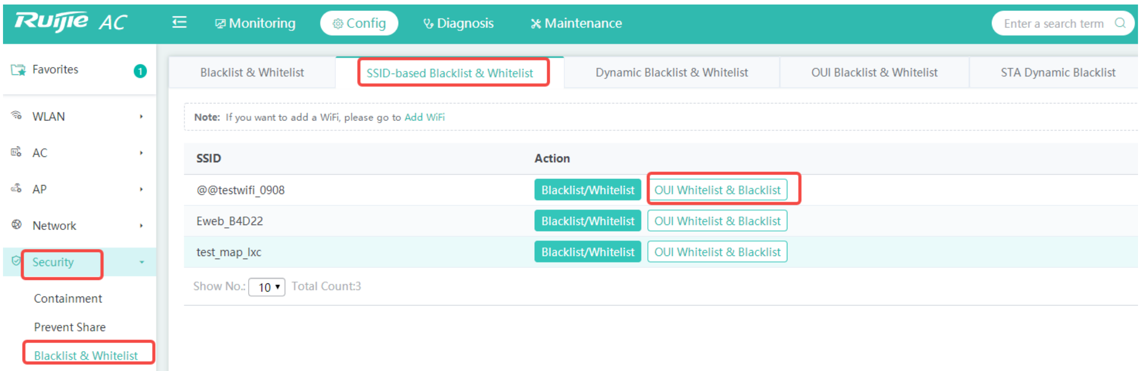
Note: It is recommended to download the template, fill in data and import the file.Template: list_en.csv

Download Template List Capacity: 5120

File:

(4) Configure Organizationally Unique Identifiers (OUIs): An OUI is the first 8 bits of the MAC address of a device. If devices to be added to the blocklist or allowlist belong to the same manufacturer, add their OUI into the list directly, without the need to add the MAC address of each device one by one.

Click **OUI Whitelist&Blacklist**. Access the **Add blacklist OUI** page.

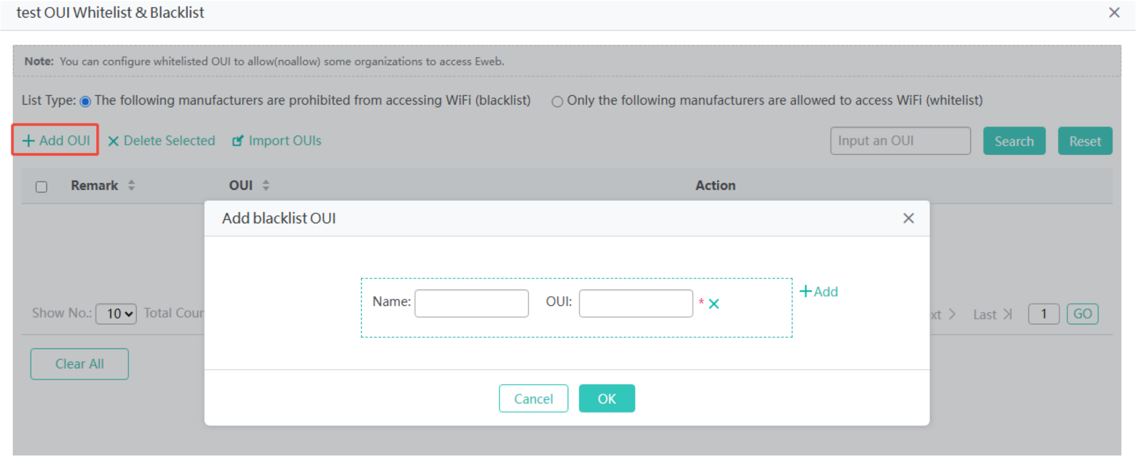


Note: If you want to add a WiFi, please go to Add WiFi

SSID	Action
@@testwifi_0908	Blacklist/Whitelist OUI Whitelist & Blacklist
Eweb_B4D22	Blacklist/Whitelist OUI Whitelist & Blacklist
test_map_lxc	Blacklist/Whitelist OUI Whitelist & Blacklist

Show No.: 10 Total Count:3

Click **Add OUI**. Enter the name and OUI of a manufacturer. Click **OK**.


test OUI Whitelist & Blacklist

Note: You can configure whitelisted OUI to allow(noallow) some organizations to access Eweb.

List Type: ● The following manufacturers are prohibited from accessing WiFi (blacklist) ○ Only the following manufacturers are allowed to access WiFi (whitelist)

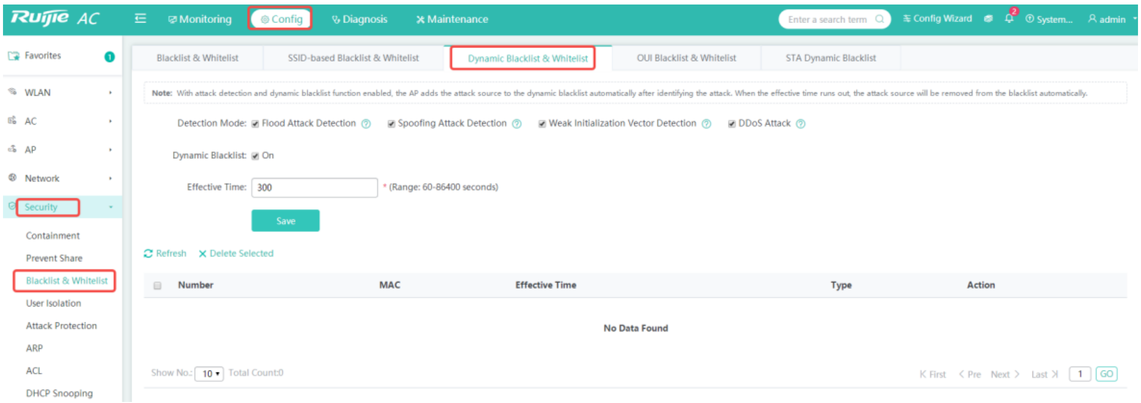
Add blacklist OUI

Name: OUI: *

3. Dynamic Blocklist

Dynamic blocklist: Add malicious attack sources to the dynamic blocklist to prevent their access. After a detection mode is configured and dynamic blocklist is enabled, the device will automatically add the attack source to the dynamic blocklist when an attack is detected. After the effective time expires, the attack source will be automatically deleted from the blocklist.

Configure dynamic blocklist: Select a detection mode, enable dynamic blocklist, configure the effective time, and click **Save**.



Note: With attack detection and dynamic blacklist function enabled, the AP adds the attack source to the dynamic blacklist automatically after identifying the attack. When the effective time runs out, the attack source will be removed from the blacklist automatically.

Detection Mode: ☑ Flood Attack Detection ☑ Spoofing Attack Detection ☑ Weak Initialization Vector Detection ☑ DDoS Attack

Dynamic Blacklist: ☑ On

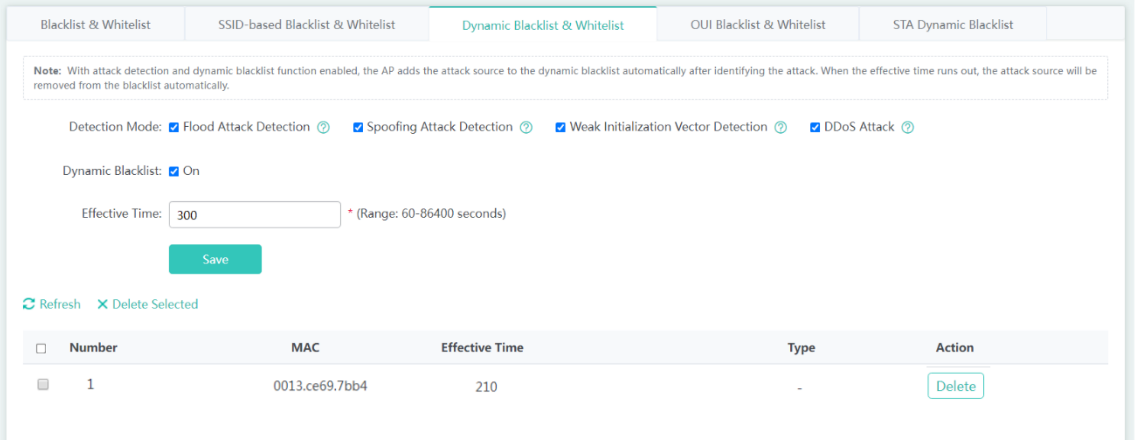
Effective Time: 300 * (Range: 60-86400 seconds)

□	Number	MAC	Effective Time	Type	Action

No Data Found

Show No.: 10 Total Count:0

Delete a blocklist: Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a dynamic blacklist. To delete multiple dynamic blacklists, select the target dynamic blacklists. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the dynamic blacklists.


Blacklist & Whitelist
SSID-based Blacklist & Whitelist
Dynamic Blacklist & Whitelist
OUI Blacklist & Whitelist
STA Dynamic Blacklist
Save
Refresh
Delete Selected
Delete

Note: With attack detection and dynamic blacklist function enabled, the AP adds the attack source to the dynamic blacklist automatically after identifying the attack. When the effective time runs out, the attack source will be removed from the blacklist automatically.

Detection Mode: ☑ Flood Attack Detection ☑ Spoofing Attack Detection ☑ Weak Initialization Vector Detection ☑ DDoS Attack

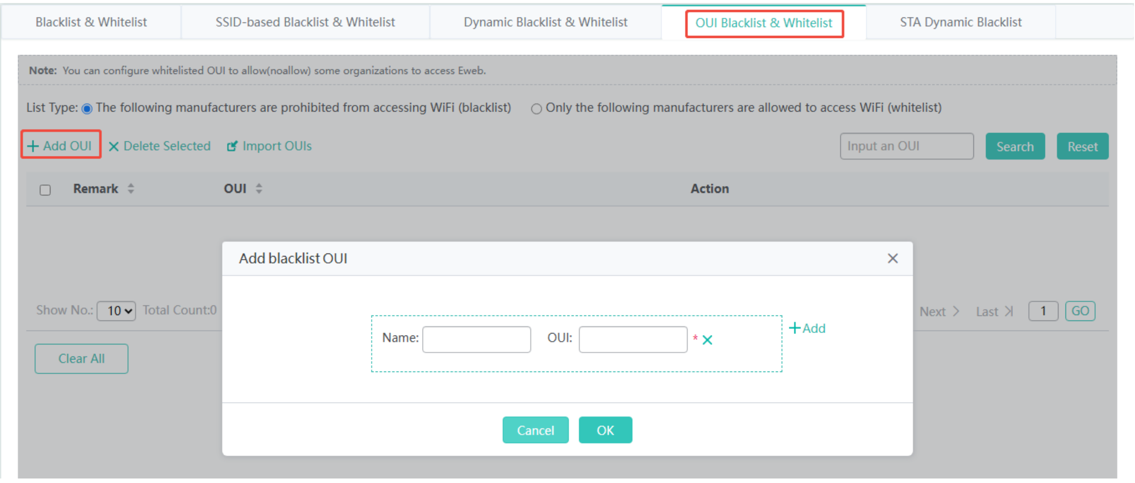
Dynamic Blacklist: ☑ On

Effective Time: 300 * (Range: 60-86400 seconds)

□ Number	MAC	Effective Time	Type	Action
□ 1	0013.ce69.7bb4	210	-	Delete

4. Configuring the OUI Blocklist or Allowlist for the AC

Configure manufacturer information: Click **Add OUI**. Enter the name and OUI of a manufacturer. Click **OK**.



Note: You can configure whitelisted OUI to allow(noallow) some organizations to access Eweb.

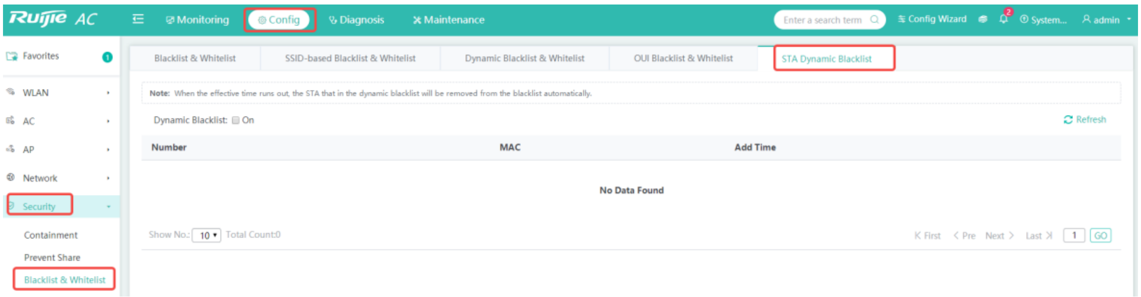
List Type: ● The following manufacturers are prohibited from accessing WiFi (blacklist) ○ Only the following manufacturers are allowed to access WiFi (whitelist)

□ Remark	OUI	Action

Name: OUI: *

5. STA Dynamic Blocklist

Add STAs from malicious attack sources to the STA dynamic blocklist to prevent them from accessing the network.



Note: When the effective time runs out, the STA that in the dynamic blacklist will be removed from the blacklist automatically.

Dynamic Blacklist: □ On

Number	MAC	Add Time

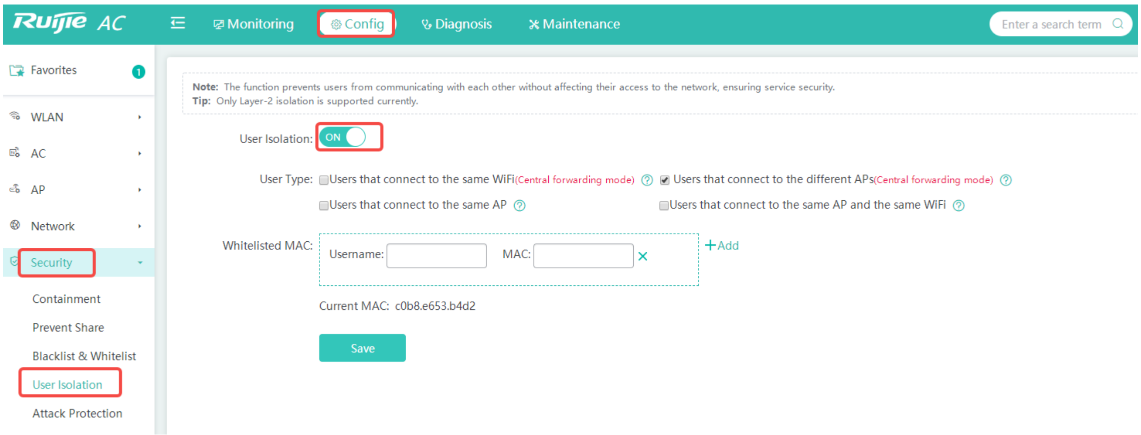
No Data Found

5.5.4 User isolation

Choose **Config** > **Security** > **User Isolation**.

To ensure network security and information confidentiality, intranet users can be configured not to communicate with each other. Some special users (users who can access each other) can be identified by user name and MAC address.

Toggle on or off the user isolation switch to enable or disable mutual access between intranet users. Select the types of users to be isolated. Click **Add** to add MAC addresses of users for mutual access. Click **x** to delete a specified user MAC address.



Note: The function prevents users from communicating with each other without affecting their access to the network, ensuring service security.
Tip: Only Layer-2 isolation is supported currently.

User Isolation: ON

User Type: □ Users that connect to the same WiFi(Central forwarding mode) ☑ Users that connect to the different APs(Central forwarding mode)
□ Users that connect to the same AP □ Users that connect to the same AP and the same WiFi

Whitelisted MAC: Username: MAC:

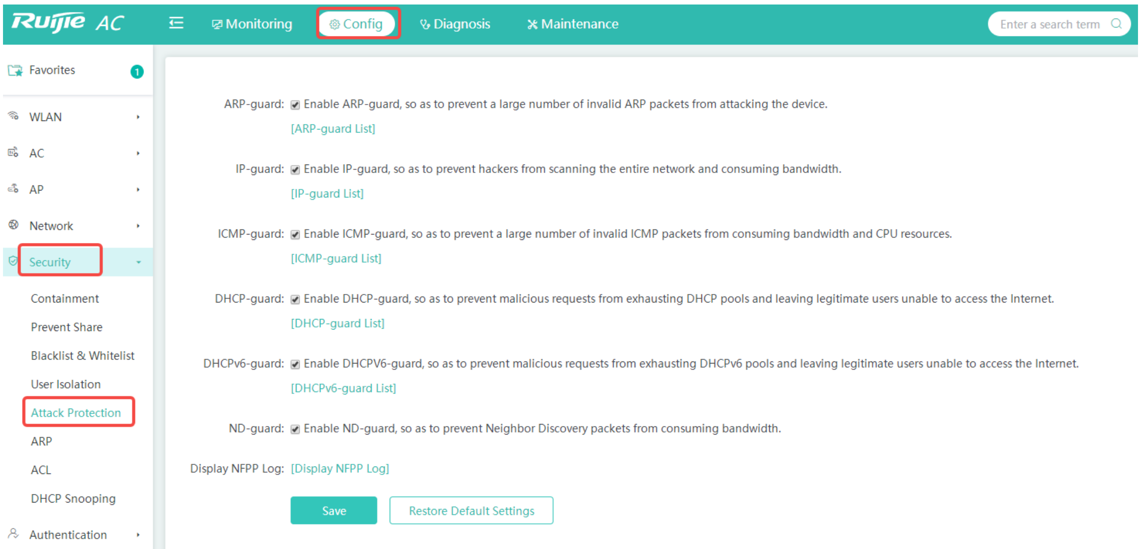
Current MAC: c0b8.e653.b4d2

5.5.5 Attack Prevention

Choose **Config** > **Security** > **Attack Protection**.

Malicious attacks often occur in a network environment. These attacks overload the device, resulting in high CPU usage and an operation failure of the device.

Select attack prevention types and click **Save**. Click the text within square brackets ([]) to display the list.



ARP-guard: ☑ Enable ARP-guard, so as to prevent a large number of invalid ARP packets from attacking the device.
[ARP-guard List]

IP-guard: ☑ Enable IP-guard, so as to prevent hackers from scanning the entire network and consuming bandwidth.
[IP-guard List]

ICMP-guard: ☑ Enable ICMP-guard, so as to prevent a large number of invalid ICMP packets from consuming bandwidth and CPU resources.
[ICMP-guard List]

DHCP-guard: ☑ Enable DHCP-guard, so as to prevent malicious requests from exhausting DHCP pools and leaving legitimate users unable to access the Internet.
[DHCP-guard List]

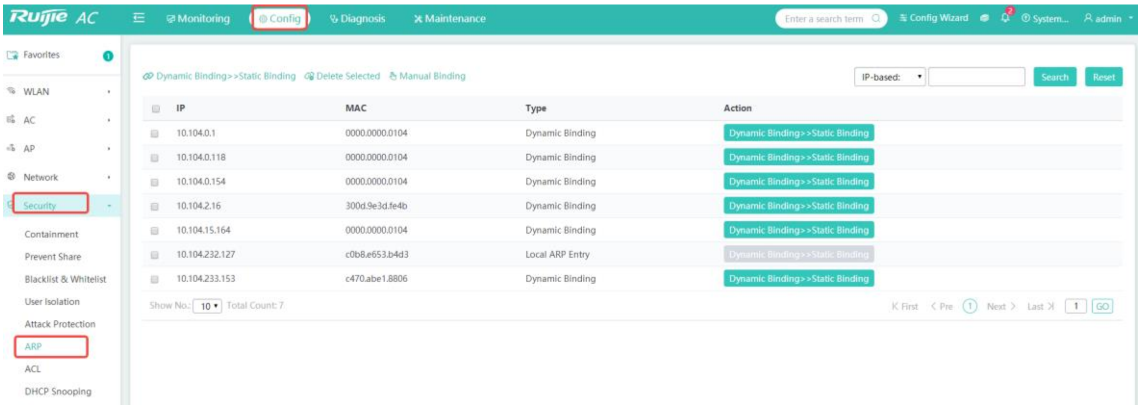
DHCPv6-guard: ☑ Enable DHCPV6-guard, so as to prevent malicious requests from exhausting DHCPv6 pools and leaving legitimate users unable to access the Internet.
[DHCPv6-guard List]

ND-guard: ☑ Enable ND-guard, so as to prevent Neighbor Discovery packets from consuming bandwidth.

Display NFPP Log: [Display NFPP Log]

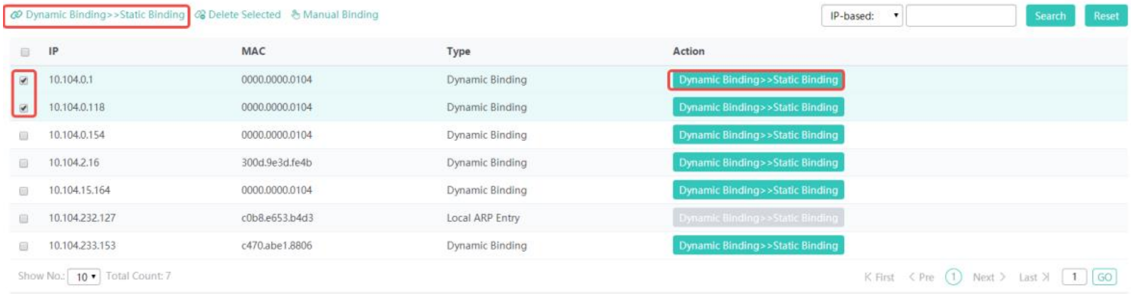
5.5.6 ARP Entry Binding

Choose **Config** > **Security** > **ARP**.



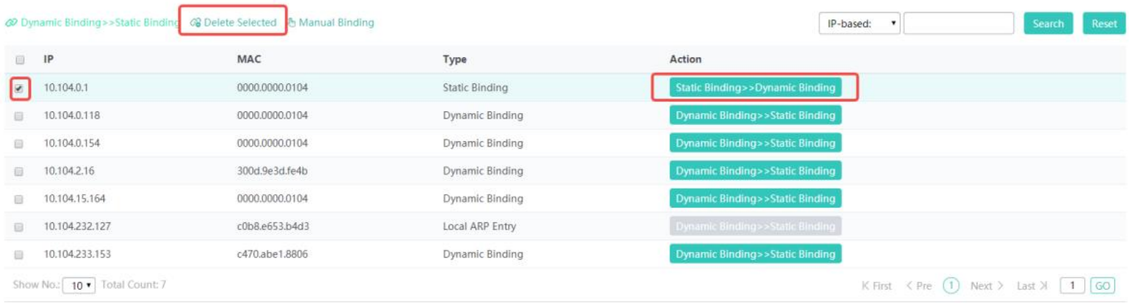
□	IP	MAC	Type	Action
□	10.104.0.1	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.0.118	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.0.154	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.2.16	300d.9e3d.fe4b	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.15.164	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.232.127	c0b8.e653.b4d3	Local ARP Entry	Dynamic Binding>>Static Binding
□	10.104.233.153	c470.abe1.8806	Dynamic Binding	Dynamic Binding>>Static Binding

(1) Convert dynamic bindings to static bindings: Select one or more records in the ARP list. Click **Dynamic Binding>>Static Binding** to batch convert dynamic bindings to static bindings.



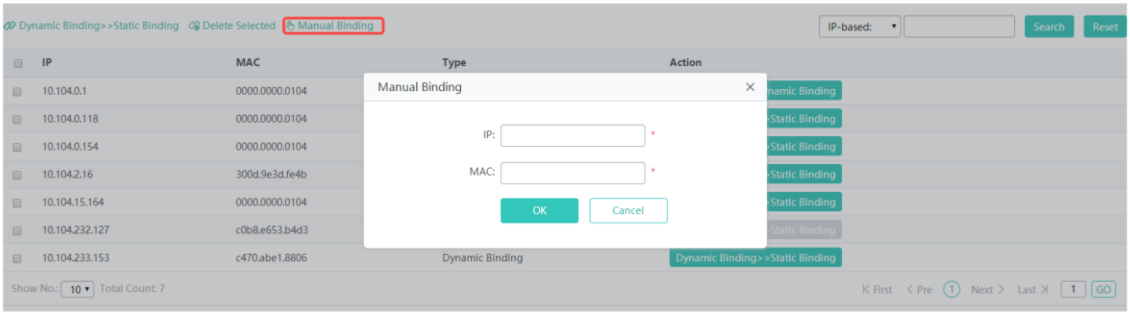
□	IP	MAC	Type	Action
☑	10.104.0.1	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
☑	10.104.0.118	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.0.154	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.2.16	300d.9e3d.fe4b	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.15.164	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.232.127	c0b8.e653.b4d3	Local ARP Entry	Dynamic Binding>>Static Binding
□	10.104.233.153	c470.abe1.8806	Dynamic Binding	Dynamic Binding>>Static Binding

(2) Delete static bindings: Select one entry in the ARP list. Click **Static Binding >> Dynamic Binding** in the **Action** column to switch the static binding to the dynamic binding. To delete multiple static bindings, select the target IP addresses in the ARP list. Click **Delete Selected** to batch delete the static bindings.



□	IP	MAC	Type	Action
☑	10.104.0.1	0000.0000.0104	Static Binding	Static Binding>>Dynamic Binding
□	10.104.0.118	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.0.154	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.2.16	300d.9e3d.fe4b	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.15.164	0000.0000.0104	Dynamic Binding	Dynamic Binding>>Static Binding
□	10.104.232.127	c0b8.e653.b4d3	Local ARP Entry	Dynamic Binding>>Static Binding
□	10.104.233.153	c470.abe1.8806	Dynamic Binding	Dynamic Binding>>Static Binding

(3) Manual binding: Click **Manual Binding**. Enter the IP and MAC addresses. Click **OK**. The **Configuration succeeded.** message is displayed. The new entry is displayed in the ARP list.



IP	MAC	Type	Action
10.104.0.1	0000.0000.0104		namic Binding
10.104.0.118	0000.0000.0104		Static Binding
10.104.0.154	0000.0000.0104		Static Binding
10.104.2.16	300d.9e3d.fe4b		Static Binding
10.104.15.164	0000.0000.0104		Static Binding
10.104.232.127	c0b8.e653.b4d3		Static Binding
10.104.233.153	c470.abe1.8806	Dynamic Binding	Dynamic Binding>>Static Binding

Manual Binding

IP: *

MAC: *

OK Cancel

5.5.7 Number of ACL Entries

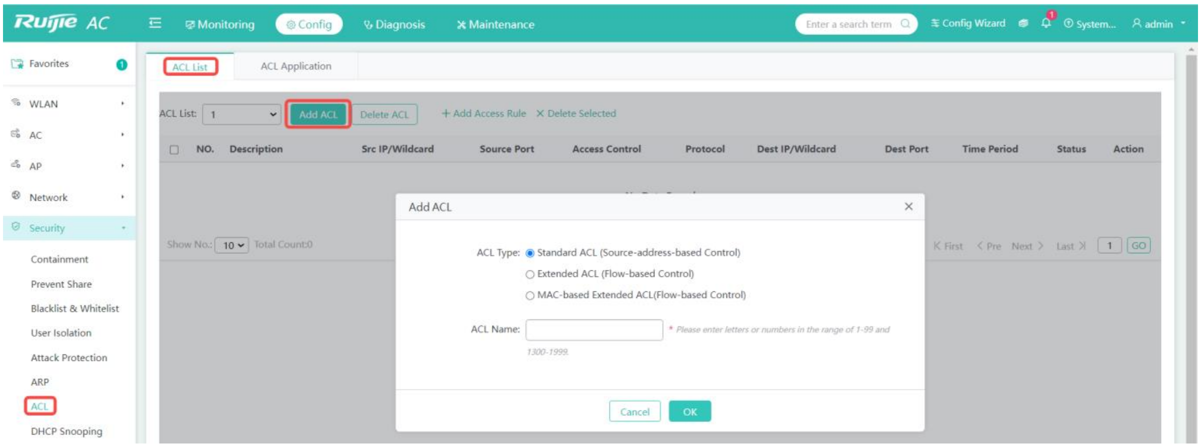
Choose **Config** > **Security** > **ACL**.

When receiving a packet, a device interface on which an ingress ACL is configured checks whether the packet matches an access control entry (ACE) in the ingress ACL. When sending out a packet, a device interface on which an egress ACL is configured checks whether the packet matches an ACE in the egress ACL.

When different ACEs are configured, multiple ACEs may be applied at the same time, or only some ACEs are applied. Packets are processed according to the first matched ACE (permit or deny).

1. ACL List

(1) Add an ACL: Click **Add ACL**. Configure ACL information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added ACL is displayed in the drop-down ACL list in the upper left corner.



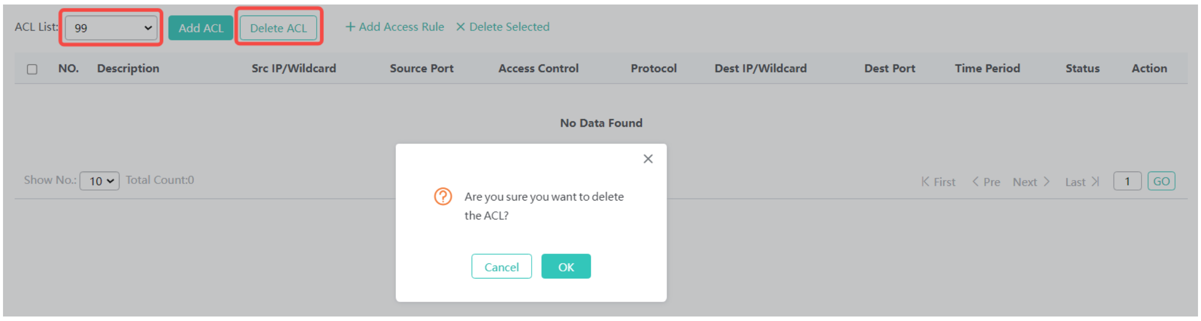
Add ACL

ACL Type: ● Standard ACL (Source-address-based Control)
○ Extended ACL (Flow-based Control)
○ MAC-based Extended ACL(Flow-based Control)

ACL Name: * Please enter letters or numbers in the range of 1-99 and 1300-1999.

Cancel OK

(2) Delete an ACL: Select the ACL to be deleted from the drop-down ACL list. Click **Delete ACL**. The confirmation dialog box pops up. Click **OK** to finish the operation.

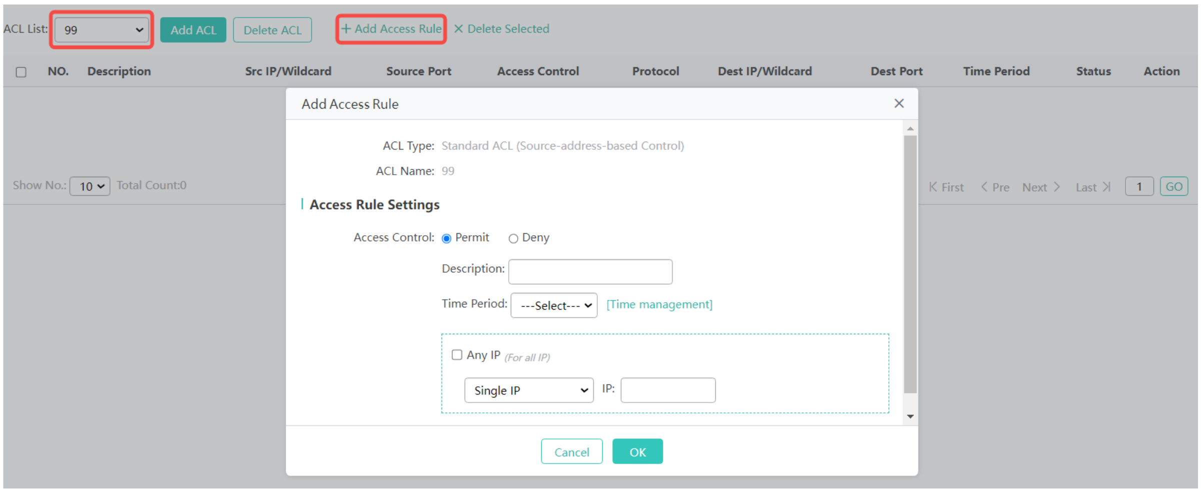


No Data Found

Are you sure you want to delete the ACL?

Cancel OK

(3) Add an ACE: Select an ACL to which an ACE needs to be added from the drop-down ACL list. Click **Add Access Rule**. Configure ACE information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added ACE is displayed in the ACL list.



ACL List: 99

□	NO.	Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action

Show No.: 10 Total Count:0

ACL Type: Standard ACL (Source-address-based Control)

ACL Name: 99

Access Rule Settings

Access Control: ● Permit ○ Deny

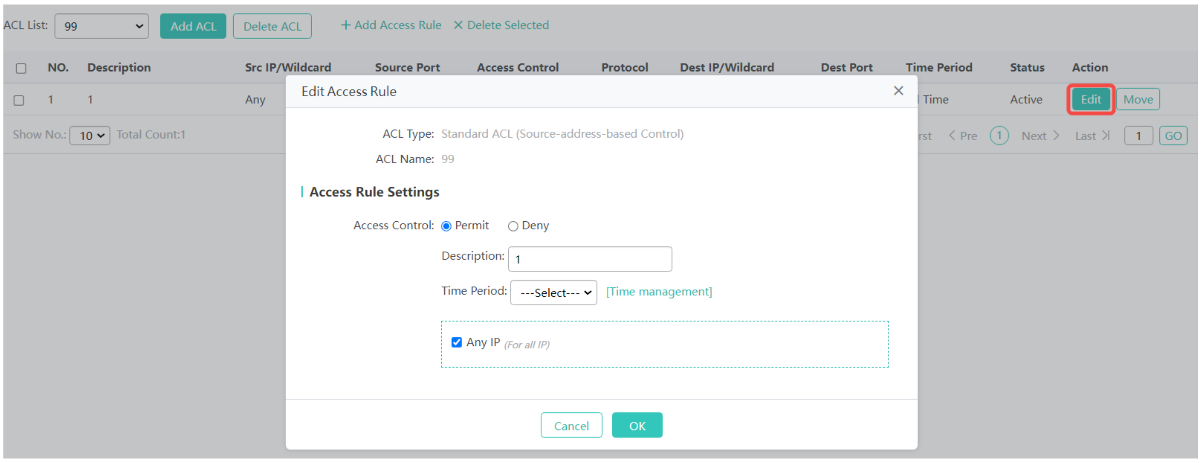
Description:

Time Period: ---Select--- [Time management]

□ Any IP (For all IP)

Single IP IP:

(4) Edit an ACE: Click **Edit** behind a specified ACE in the ACL list. The pop-up dialog box displays the information about the ACE. Edit the information. Click **OK**. A message indicating the configuration has been saved is displayed.



ACL List: 99

□	NO.	Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
□	1	1	Any						Time	Active	Edit Move

Show No.: 10 Total Count:1

ACL Type: Standard ACL (Source-address-based Control)

ACL Name: 99

Access Rule Settings

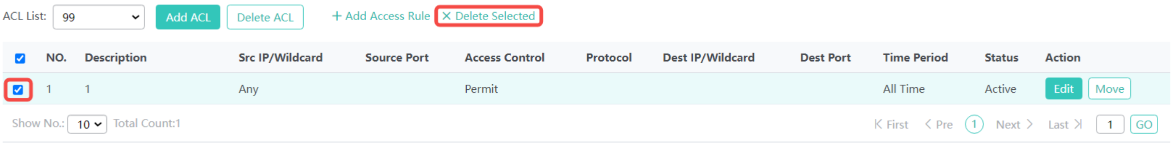
Access Control: ● Permit ○ Deny

Description: 1

Time Period: ---Select--- [Time management]

☑ Any IP (For all IP)

(5) Delete an ACE: Select one or more records in the ACL list. Click **Delete Selected**. The confirmation dialog box pops up. Click **OK** to finish the operation.



ACL List: 99

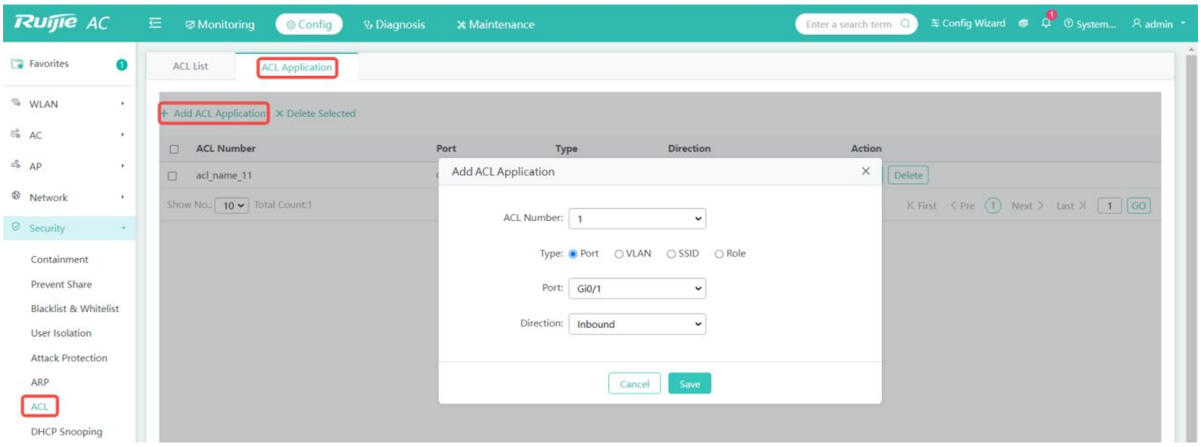
☑	NO.	Description	Src IP/Wildcard	Source Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
☑	1	1	Any		Permit				All Time	Active	Edit Move

Show No.: 10 Total Count:1

2. ACL Application

You can configure ACEs and apply them to interfaces or Wi-Fis to restrict the access of specified users or allow users to access specified networks.

(1) Add ACL application: Click **Add ACL Application**. The **Add ACL Application** dialog box pops up. Configure the information. Click **Save**. A message indicating the configuration has been saved is displayed. The newly added ACL application entry is displayed in the list.



☐	ACL Number	Port	Type	Direction	Action
☐	acl_name_11				

Show No.: 10 Total Count:1

Add ACL Application

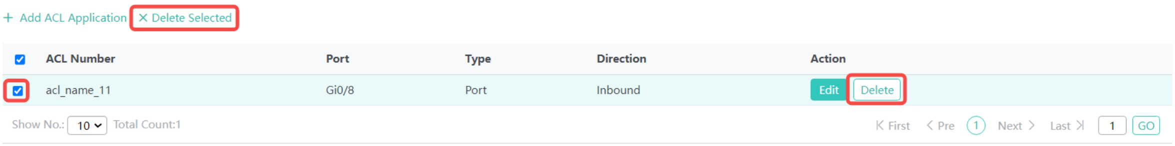
ACL Number: 1

Type: ● Port ○ VLAN ○ SSID ○ Role

Port: Gi0/1

Direction: Inbound

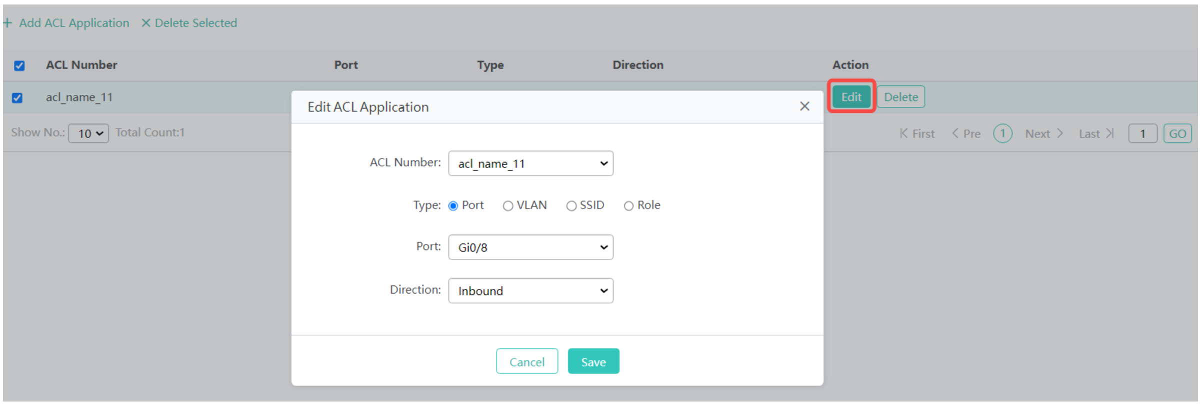
(2) Delete ACL application: Click **Delete** behind a specified ACL application entry in the list. The confirmation dialog box pops up. Click **OK** to finish the operation. To delete multiple ACL application entries, select one or more records in the ACL application list. Click **Delete Selected** to batch delete the records. The confirmation dialog box pops up. Click **OK** to finish the operation.



☑	ACL Number	Port	Type	Direction	Action
☑	acl_name_11	Gi0/8	Port	Inbound	Edit Delete

Show No.: 10 Total Count:1

(3) Edit ACL application: Click **Edit** behind a specified ACL application entry in the list. The pop-up dialog box displays the information about the ACL application. Edit the information. Click **Save**. A message indicating the configuration has been saved is displayed.



☑	ACL Number	Port	Type	Direction	Action
☑	acl_name_11				Edit Delete

Show No.: 10 Total Count:1

Edit ACL Application

ACL Number: acl_name_11

Type: ● Port ○ VLAN ○ SSID ○ Role

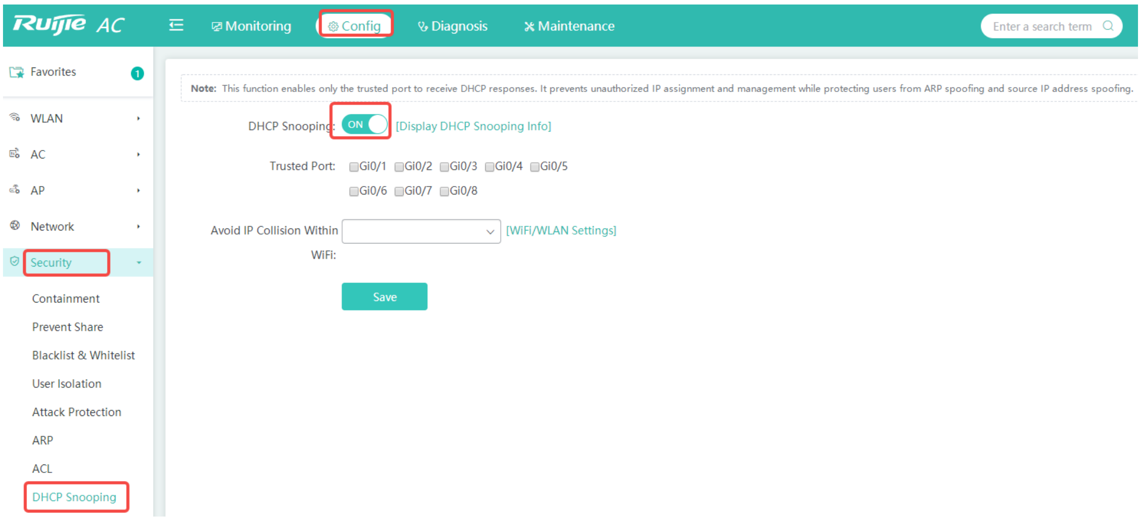
Port: Gi0/8

Direction: Inbound

5.5.8 DHCP Security

This function enables only the trusted port to receive DHCP responses. It prevents unauthorized IP assignment and management while protecting users from ARP spoofing and source IP address spoofing.

Click **Config** > **Security** > **DHCP Snooping**.



Note: This function enables only the trusted port to receive DHCP responses. It prevents unauthorized IP assignment and management while protecting users from ARP spoofing and source IP address spoofing.

DHCP Snooping: ON [Display DHCP Snooping Info]

Trusted Port: □Gi0/1 □Gi0/2 □Gi0/3 □Gi0/4 □Gi0/5 □Gi0/6 □Gi0/7 □Gi0/8

Avoid IP Collision Within WiFi: [WiFi/WLAN Settings]

Parameter	Description
DHCP Snooping	Enables or disables the DHCP snooping feature.
Display DHCP Snooping Info	Displays the information about users and bounded IP addresses saved on the AC.
Trusted Port	Enables the AC to only forward DHCP packets received on trusted ports.
Avoid IP Collision Within WiFi	Specifies the Wi-Fi network to be enabled with the IP address conflict prevention feature. After this feature is enabled, the AC will filter users connecting to the Wi-Fi based on the information about users and bounded IP addresses.

5.6 Authentication

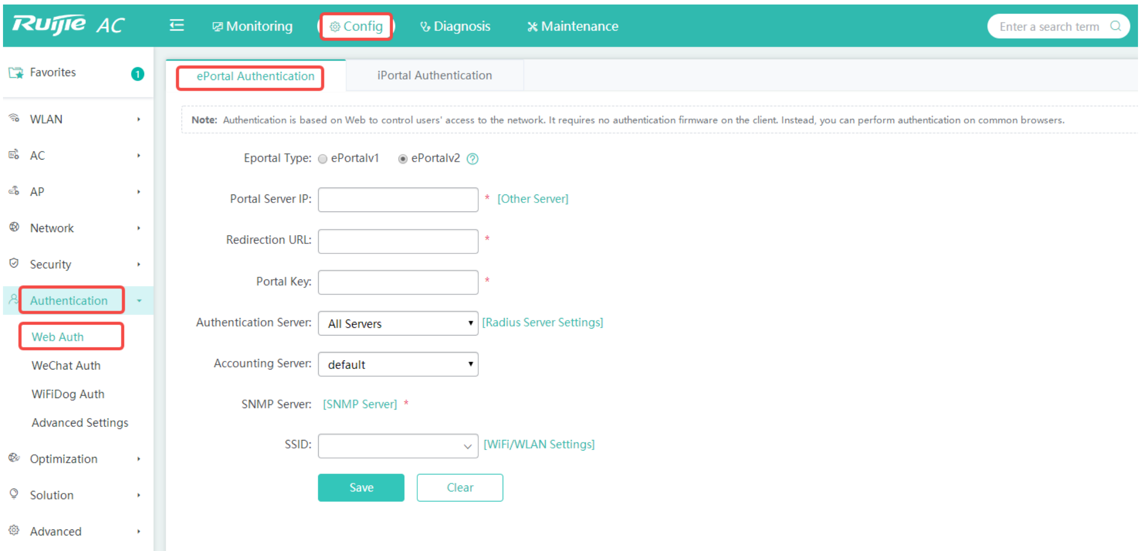
5.6.1 Web-based Authentication

Choose **Config** > **Authentication** > **Web Auth**.

Web-based authentication is an identity authentication method for controlling user permissions for network access. This authentication method does not require dedicated client authentication software. Identity authentication can be implemented using a common browser. Real-name authentication facilitates user management. Based on the location of the authentication server, web-based authentication is classified into **ePortal Authentication** and **iPortal Authentication**.

1. ePortal Authentication

When unauthenticated users access the Internet through a browser, the access device forcibly redirects the browser to a specified URL to perform authentication. When the portal (the authentication web page) is located in a separate device outside the AC, the authentication is external web-based authentication.



Note: Authentication is based on Web to control users' access to the network. It requires no authentication firmware on the client. Instead, you can perform authentication on common browsers.

Eportal Type: ○ ePortalv1 ● ePortalv2

Portal Server IP: * [Other Server]

Redirection URL: *

Portal Key: *

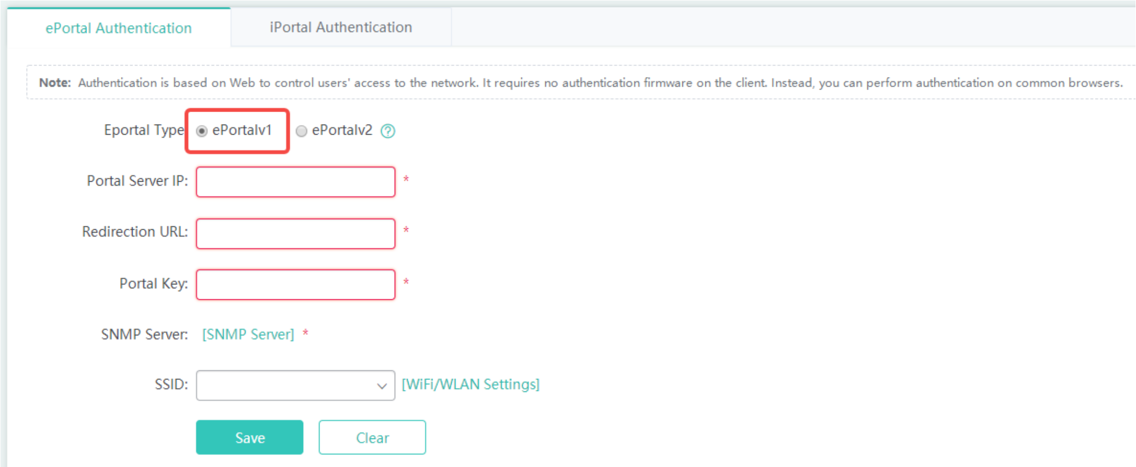
Authentication Server: All Servers [Radius Server Settings]

Accounting Server: default

SNMP Server: [SNMP Server] *

SSID: [WiFi/WLAN Settings]

(1) **ePortalv1**:



Note: Authentication is based on Web to control users' access to the network. It requires no authentication firmware on the client. Instead, you can perform authentication on common browsers.

Eportal Type ● ePortalv1 ○ ePortalv2

Portal Server IP: *

Redirection URL: *

Portal Key: *

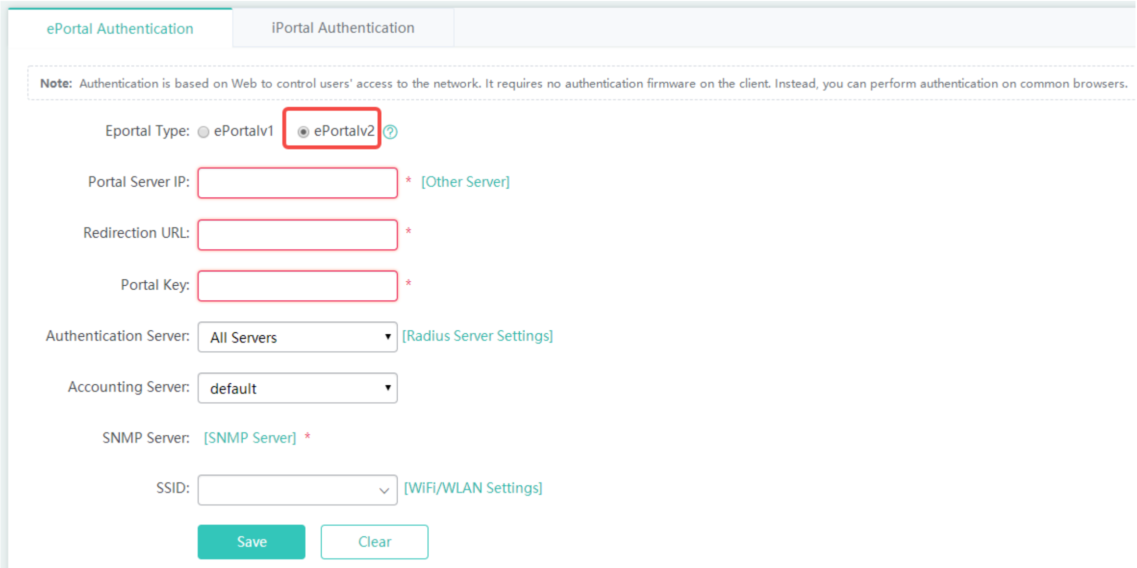
SNMP Server: [SNMP Server] *

SSID: [WiFi/WLAN Settings]

Parameter	Description
Portal Server IP	Enter the IP address of the ePortal server. Typically, the authentication page is provided by the ePortal server.
Redirection URL	Enter the URL of the authentication page. When an unauthenticated user accesses network resources, the user is automatically redirected to this page for authentication.
Portal Key	Configures a key for the communication between the device and the authentication server.
SNMP Server	When the device detects that a user goes offline, it sends a notification to the portal server through SNMP. Upon receiving the notification, the portal server processes it based on the preset rules, such as deleting the saved user information and returning an offline page to the user.

SSID	Specifies the Wi-Fi network to be configured with the **ePortalv1**. Note: Only global authentication mode is supported currently. WLAN-based authentication mode is not available.

(2) **ePortalv2**:



Note: Authentication is based on Web to control users' access to the network. It requires no authentication firmware on the client. Instead, you can perform authentication on common browsers.

Eportal Type: ○ ePortalv1 ● ePortalv2

Portal Server IP: * [Other Server]

Redirection URL: *

Portal Key: *

Authentication Server: All Servers [Radius Server Settings]

Accounting Server: default

SNMP Server: [SNMP Server] *

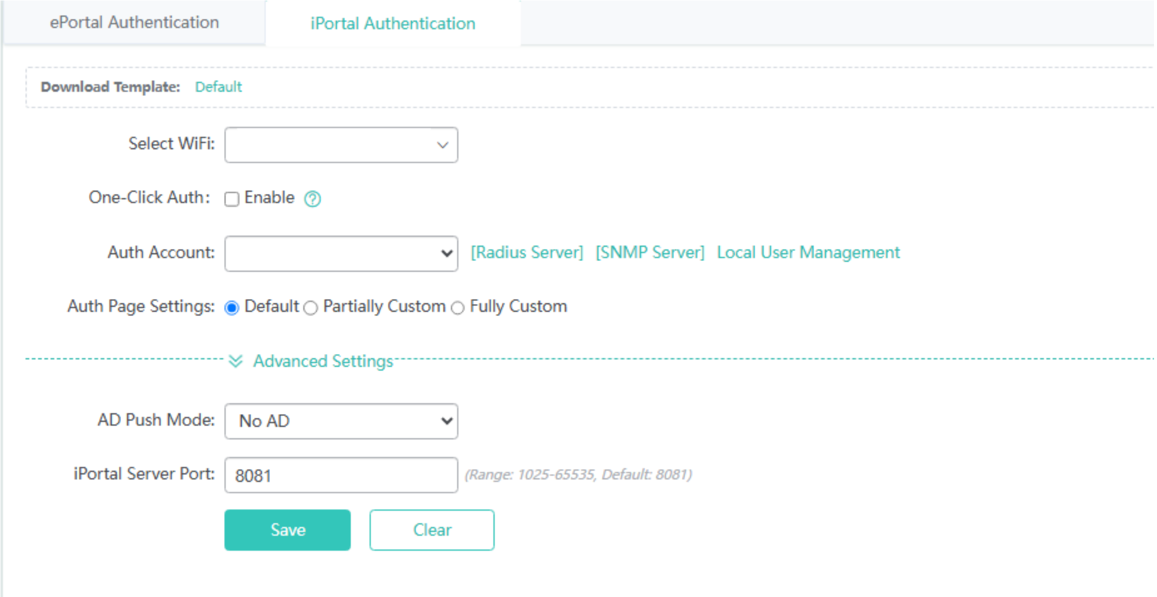
SSID: [WiFi/WLAN Settings]

Parameter	Description
Portal Server IP	Enter the IP address of the ePortal server. Typically, the authentication page is provided by the ePortal server.
Redirection URL	Enter the URL of the authentication page. When an unauthenticated user accesses network resources, the user is automatically redirected to this page for authentication.
Portal Key	Configures a key for the communication between the device and the authentication server.
Authentication Server	To successfully apply second-generation web authentication, Authentication, Authorization, and Accounting (AAA) authentication must be configured. The authentication method list associates web-based authentication requests with the RADIUS server. The NAS selects the authentication method and server based on the web authentication method list.
Accounting Server	Mandatory. To successfully apply second-generation web-based authentication, AAA accounting must be configured. Accounting is used to associate an accounting method with the server. In web authentication, accounting is implemented to record user information or fees.

SNMP Server	When the device detects that a user goes offline, it sends a notification to the portal server through SNMP. Upon receiving the notification, the portal server processes it based on the preset rules, such as deleting the saved user information and returning an offline page to the user.
SSID	Second-generation authentication is applied to Wi-Fi networks.

2. iPortal Authentication

When an unauthenticated user attempts to access the network using a browser, the access device forcibly redirects the browser to a specified web page for user authentication. iPortal authentication is used when the portal (authentication web page) is built in the AC. The authentication page can be set to the **Default**, **Partially Custom**, or **Fully Custom** mode.



ePortal Authentication | iPortal Authentication

Download Template: Default

Select WiFi:

One-Click Auth: □ Enable

Auth Account: [Radius Server] [SNMP Server] Local User Management

Auth Page Settings: ● Default ○ Partially Custom ○ Fully Custom

Advanced Settings

AD Push Mode: No AD

iPortal Server Port: 8081 (Range: 1025-65535, Default: 8081)

Save Clear

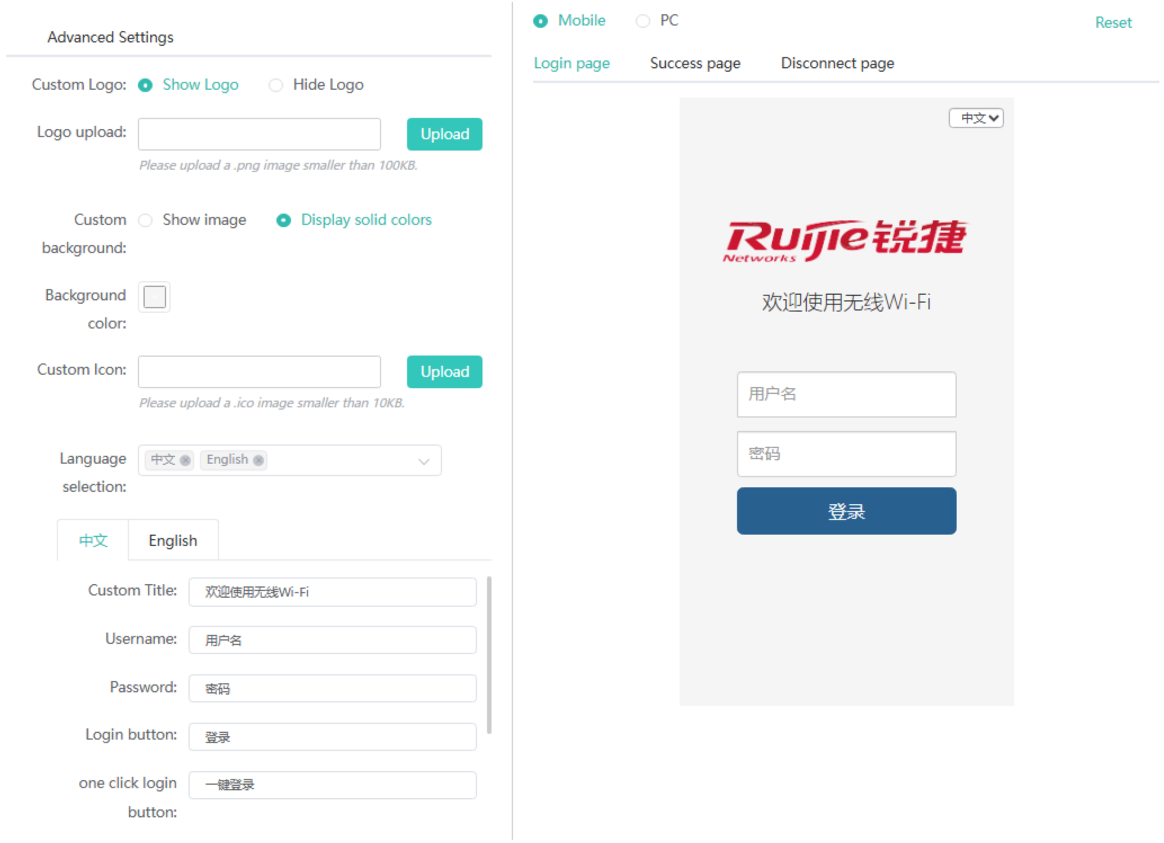
Parameter	Description
Select WiFi	Select Wi-Fi for authentication.
One-Click Auth	When One-Click Auth is enabled, users do not need to enter the username and password. They can click **Log In** on the authentication page to pass the authentication. Only Default and Partially Custom are supported.
Auth Account	The following authentication account sources are supported: Use user information on the server preferentially Use local user information preferentially Use user information on the server only User local user information only

Auth Page Settings	**Default**: Use the system default package for authentication. **Partially Custom**: Customize the logo, icon, title, and disclaimer based on the system default package. **Fully Custom**: Design a package based on the system default package, compress it into a package named custom.zip, and upload the compressed package.
AD Push Mode	The advertisement push mode includes advertisement push before or after authentication. No advertisement is configured by default.
iPortal Server Port	Configures the port number of the authentication page for internal portal authentication. The port number range is from 1025 to 65535. The default port number is 8081.

If you select **Partially Custom** for **Auth Page Settings**, the system provides the GUI-based page customization feature for you to design and modify the appearance and details of authentication pages through convenient GUI operations. You can adjust elements such as the logo, background, icon, and button to flexibly meet diversified customization requirements. You can preview the effects after modification in real time over the entire design process. You can also switch between mobile and PC to preview the effects for different terminals and ensure that the effects meet expectations. The login page, authentication success page, and disconnect page support customization. You can complete the design with a few clicks in an easy and efficient way, without the need for code editing. This implements more user-friendly interaction experience and efficient customization service.

Caution

When you customize an authentication page by means of **Partially Custom**, the disclaimer is available only after you enable **One-Click Auth**.



Advanced Settings

Custom Logo: ● Show Logo ○ Hide Logo

Logo upload: Upload

Please upload a .png image smaller than 100KB.

Custom background: ○ Show image ● Display solid colors

Background color:

Custom Icon: Upload

Please upload a .ico image smaller than 10KB.

Language selection: 中文 English

中文 English

Custom Title: 欢迎使用无线Wi-Fi

Username: 用户名

Password: 密码

Login button: 登录

one click login button: 一键登录

● Mobile ○ PC Reset

Login page Success page Disconnect page

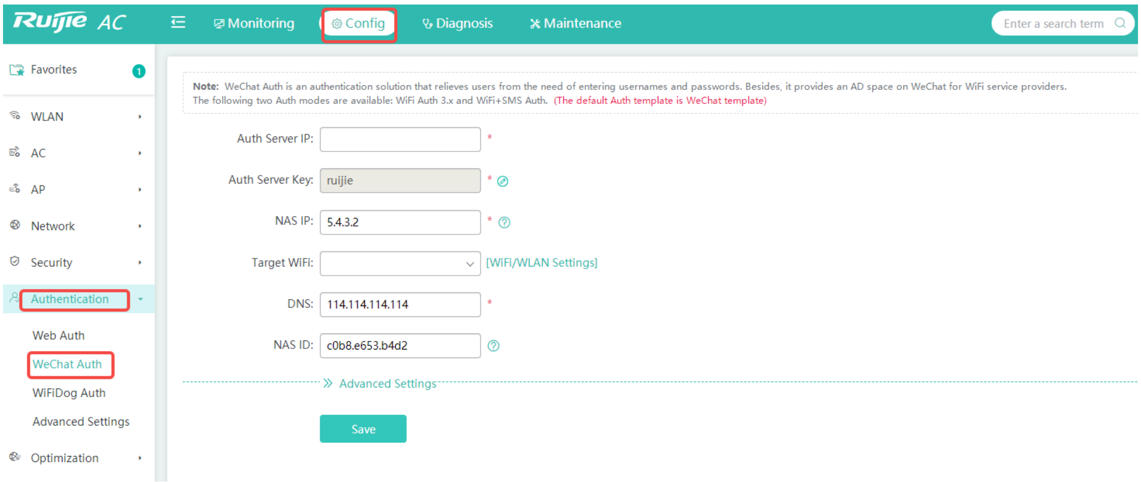
5.6.2 WeChat Authentication

Choose **Config** > **Authentication** > **WeChat Auth**.

Connect to Wi-Fi via WeChat is a solution designed to replace web-based authentication on traditional commercial Wi-Fi networks. It eliminates the need to input the username and password in web-based authentication. Besides, it provides an entrance for Wi-Fi service providers with security certification to display their advertisements, which enhances its commercial value.

Currently, the supported authentication modes include: WeChat-based authentication 3.x, and WeChat-based and SMS-based authentication.

The primary configuration is based on scenarios, allowing for one-click authentication of Wi-Fi connection through WeChat and configuration through the CWMP protocol. You are advised not to configure this feature together with CLI commands (whether this feature is supported varies with devices).



Note: WeChat Auth is an authentication solution that relieves users from the need of entering usernames and passwords. Besides, it provides an AD space on WeChat for WiFi service providers. The following two Auth modes are available: WiFi Auth 3.x and WiFi+SMS Auth. (The default Auth template is WeChat template)

Auth Server IP: *

Auth Server Key: ruijie *

NAS IP: 5.4.3.2 *

Target WiFi: [WiFi/WLAN Settings]

DNS: 114.114.114.114 *

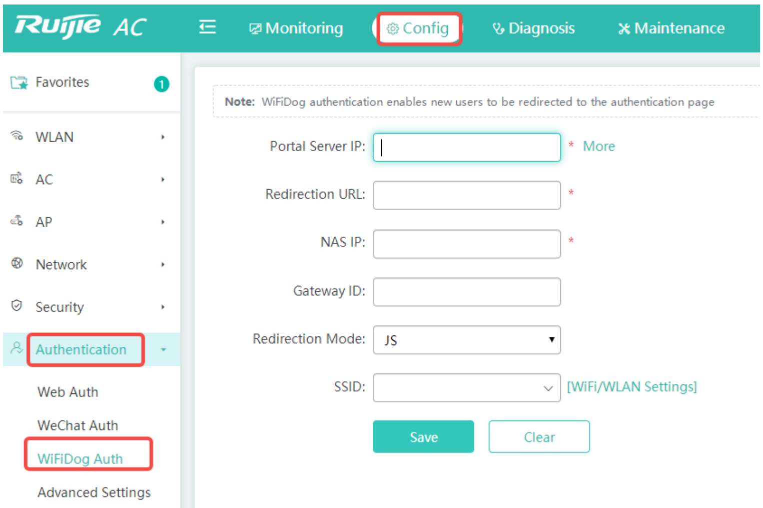
NAS ID: c0b8.e653.b4d2

Parameter	Description
Auth Server IP	Indicates the IP address of a server used for WeChat-based authentication. The default address is 112.124.31.88. Users can modify it by themselves.
Auth Server Key	Indicates a key used for the communication between the device and the authentication server.
NAS IP	Indicates the IP address of a device used for communication with the WMC server.
Target WiFi	Indicates a Wi-Fi network to be configured with WeChat-based authentication.
DNS	Indicates a DNS server which is ensured with connectivity to external networks.
NAS ID	The NAS ID is used in conjunction with the MCP server. In HSB and VAC scenarios, the configurations of each device should be consistent. To activate the function, please use non-default settings.

5.6.3 WiFiDog Authentication

Choose **Config** > **Authentication** > **WiFiDog Auth**.

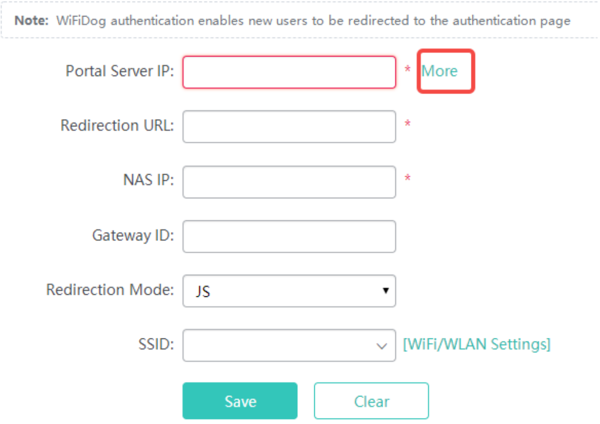
Unauthenticated users can be redirected to the authentication page for authentication. Click **More** to access the **WiFiDog Auth Server List** page.



Note: WiFiDog authentication enables new users to be redirected to the authentication page

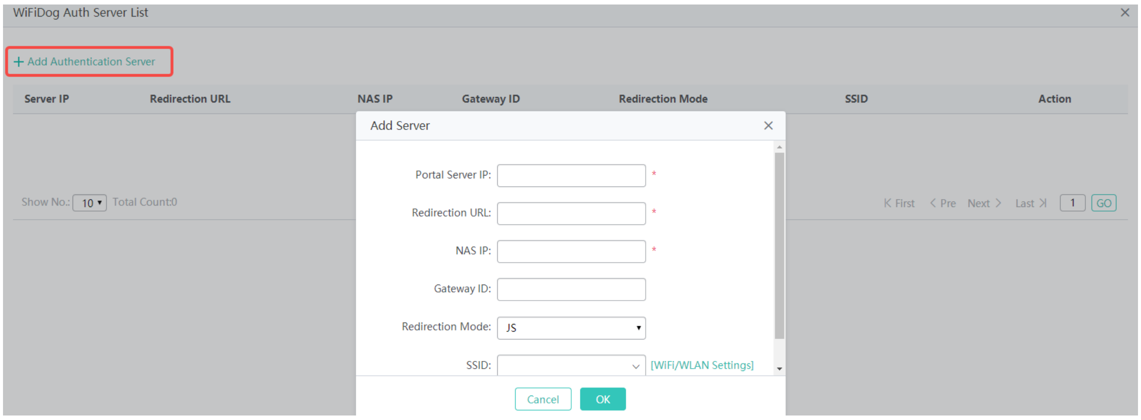
Portal Server IP: *
Redirection URL: *
NAS IP: *
Gateway ID:
Redirection Mode: JS
SSID:

(1) Add a WiFiDog authentication server: Click **Add Authentication Server**. Configure the ACL information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added server is displayed in the server list.



Note: WiFiDog authentication enables new users to be redirected to the authentication page

Portal Server IP: *
Redirection URL: *
NAS IP: *
Gateway ID:
Redirection Mode: JS
SSID:



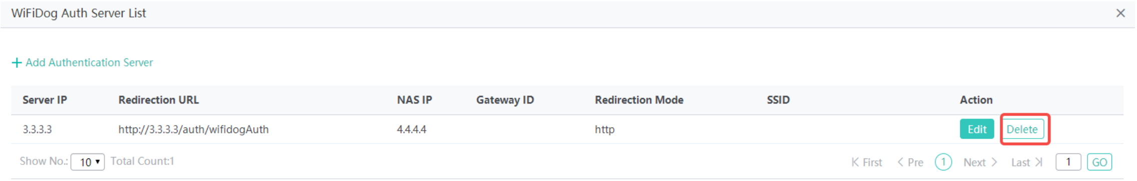
Server IP	Redirection URL	NAS IP	Gateway ID	Redirection Mode	SSID	Action

Add Server

Portal Server IP: *
Redirection URL: *
NAS IP: *
Gateway ID:
Redirection Mode: JS
SSID:

Parameter	Description
Portal Server IP	Indicates the IP address of a portal server.
Redirection URL	Indicates the portal server URL for authentication.
NAS IP	Specifies the IP address of a device to be managed by WiFiDog, which is used for communication from the server.
Redirection Mode	Specifies HTTP redirection or JavaScript redirection. JavaScript redirection is employed by default.
Gateway ID	Specifies the ID of a gateway used by WiFiDog, which is the gateway SN by default.
SSID	Specifies a Wi-Fi network to be configured with WiFiDog authentication.

(2) Delete a WiFiDog authentication server: Click **Delete** behind a specified authentication server. The confirmation dialog box pops up. Click **OK** to finish the operation.



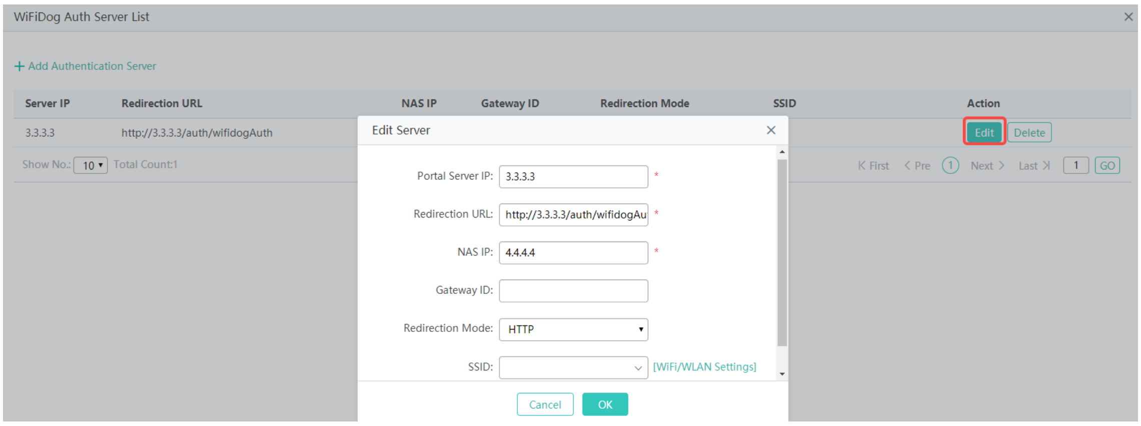
WiFiDog Auth Server List

+ Add Authentication Server

Server IP	Redirection URL	NAS IP	Gateway ID	Redirection Mode	SSID	Action
3.3.3.3	http://3.3.3.3/auth/wifidogAuth	4.4.4.4		http		Edit Delete

Show No.: 10 Total Count:1

(3) Edit a WiFiDog authentication server: Click **Edit**. Configure the information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The modified server is displayed in the server list.



WiFiDog Auth Server List

+ Add Authentication Server

Server IP	Redirection URL	NAS IP	Gateway ID	Redirection Mode	SSID	Action
3.3.3.3	http://3.3.3.3/auth/wifidogAuth					Edit Delete

Show No.: 10 Total Count:1

Edit Server

Portal Server IP: 3.3.3.3 *

Redirection URL: http://3.3.3.3/auth/wifidogAu *

NAS IP: 4.4.4.4 *

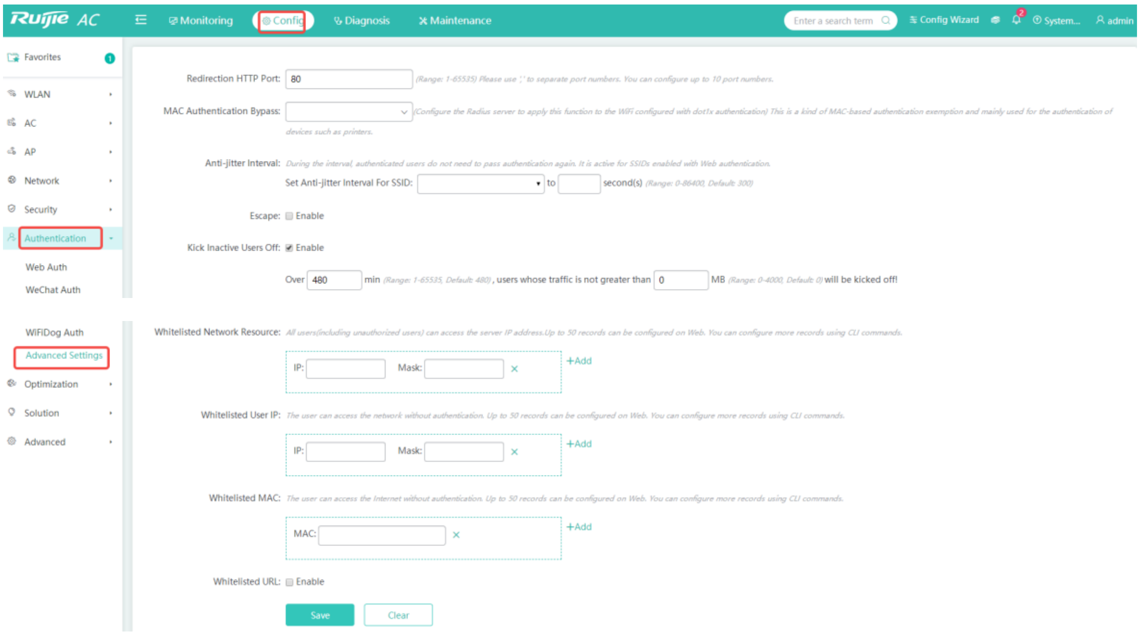
Gateway ID:

Redirection Mode: HTTP

SSID: [WiFi/WLAN Settings]

5.6.4 Advanced Settings

Choose **Config** > **Authentication** > **Advanced Settings**.



Redirection HTTP Port: 80 (Range: 1-65535) Please use ',' to separate port numbers. You can configure up to 10 port numbers.

MAC Authentication Bypass: (Configure the Radius server to apply this function to the WiFi configured with dot1x authentication) This is a kind of MAC-based authentication exemption and mainly used for the authentication of devices such as printers.

Anti-jitter Interval: During the interval, authenticated users do not need to pass authentication again. It is active for SSIDs enabled with Web authentication.

Set Anti-jitter Interval For SSID: to second(s) (Range: 0-86400, Default: 300)

Escape: □ Enable

Kick Inactive Users Off: ☑ Enable

Over 480 min (Range: 1-65535, Default: 480) , users whose traffic is not greater than 0 MB (Range: 0-4000, Default: 0) will be kicked off!

Whitelisted Network Resource: All users(including unauthorized users) can access the server IP address.Up to 50 records can be configured on Web. You can configure more records using CLI commands.

IP: Mask:

Whitelisted User IP: The user can access the network without authentication. Up to 50 records can be configured on Web. You can configure more records using CLI commands.

IP: Mask:

Whitelisted MAC: The user can access the Internet without authentication. Up to 50 records can be configured on Web. You can configure more records using CLI commands.

MAC:

Whitelisted URL: □ Enable

Parameter	Description
Redirection HTTP Port	When accessing network resources, such as accessing the Internet through a browser, users send HTTP packets. Access or aggregation devices intercept HTTP packets from users to determine whether users are accessing network resources. When detecting an unauthenticated user attempting to access network resources, devices block the user's access and redirect the user to the authentication page. By default, network devices intercept HTTP packets with port number 80 from users to determine whether users are accessing network resources. After the redirection HTTP port is configured, devices can redirect HTTP requests with a specified destination port number from users.
MAC Authentication Bypass	MAC-based client-free authentication method is typically applied to devices like printers. This parameter is used to specify the Wi-Fi to be configured with MAC authentication bypass.
Anti-jitter Interval	Within the anti-jitter interval, authenticated users do not need to be reauthenticated, enhancing the user experience. This parameter is used to specify the Wi-Fi network and anti-jitter interval.
Escape	When all of the configured portal servers are unavailable, new users can access the Internet without authentication.
Kick Inactive Users Off	When the online detection function is configured, if the traffic falls below a certain threshold within a specified period, the device will automatically disconnect the user to avoid continuous accounting and consequent financial losses caused to the user.
Whitelisted Network Resource	Enter the IP address of the network resource server. All users (including unauthenticated users) can access the IP address. Up to 50 rules can be configured.

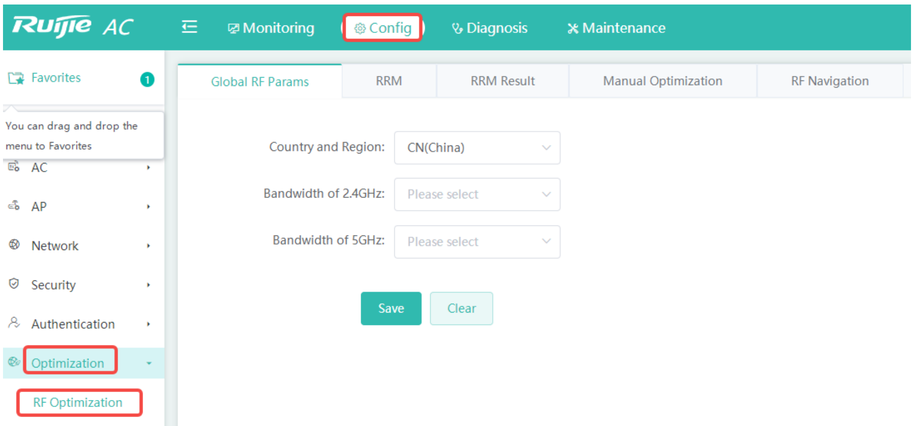
Whitelisted User IP	Users with whitelisted IP addresses can directly access the network without authentication. Up to 50 rules can be configured.
Whitelisted MAC	Users with whitelisted MAC addresses can directly access the network without authentication. Up to 50 rules can be configured.
Whitelisted URL	Users can access these URL addresses without authentication. Up to 50 URLs can be configured.

5.7 Network Optimization

5.7.1 RF Optimization

Choose **Config** > **Optimization** > **RF Optimization**.

1. Global RF Parameters



Country and Region: CN(China)

Bandwidth of 2.4GHz: Please select

Bandwidth of 5GHz: Please select

2. One-click optimization

The one-click network optimization function can optimize the network (including the channel, bandwidth, and power) of the AP to maximize the wireless performance. One-click RRM includes scheduled RRM and immediate RRM. Select either of them as required.

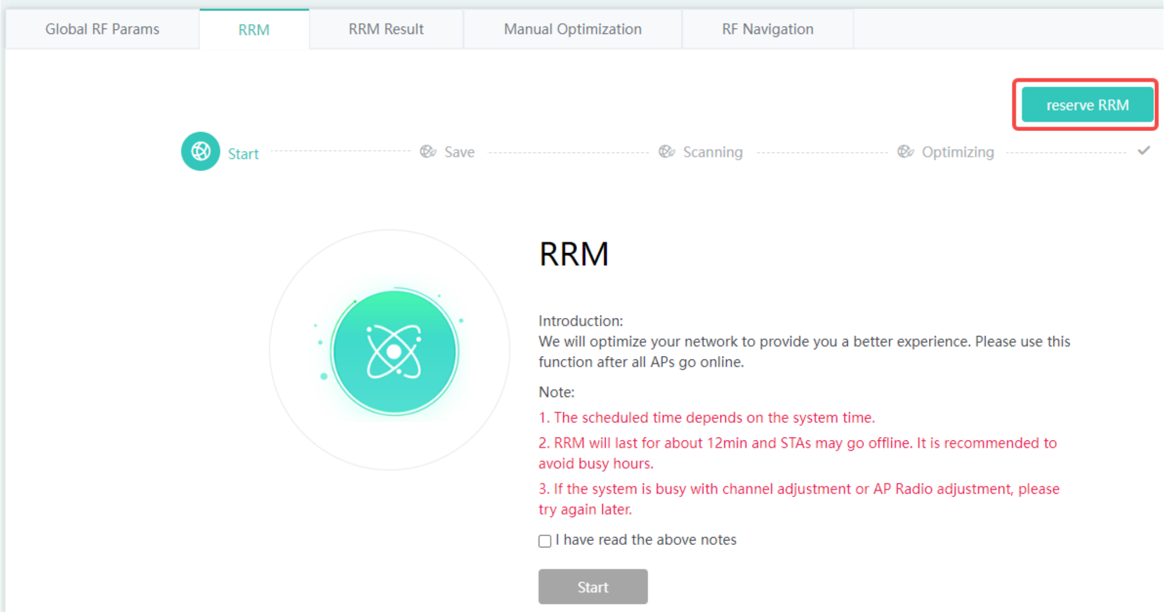
Caution

To use the network optimization function, make sure that the APs to be optimized are online.

- Scheduled Optimization

Procedure

(5) Click Optimization Appointment to go to the Optimization Appointment page.



RRM

Introduction:
We will optimize your network to provide you a better experience. Please use this function after all APs go online.

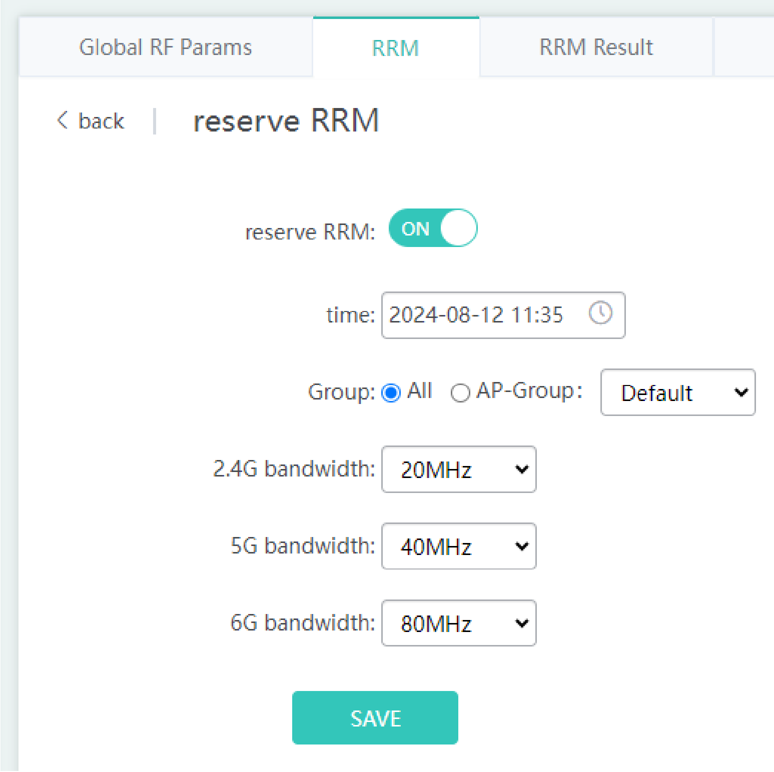
Note:

1. The scheduled time depends on the system time.
2. RRM will last for about 12min and STAs may go offline. It is recommended to avoid busy hours.
3. If the system is busy with channel adjustment or AP Radio adjustment, please try again later.

□ I have read the above notes

Start

(6) Enable and configure network optimization information as required.



reserve RRM

reserve RRM: ON

time: 2024-08-12 11:35

Group: ● All ○ AP-Group: Default

2.4G bandwidth: 20MHz

5G bandwidth: 40MHz

6G bandwidth: 80MHz

SAVE

Config Parameter	Parameter Description
Network Optimization Appointment	Are you sure you want to enable network optimization appointment?

Config Parameter	Parameter Description
Select Time	● Select the optimization time. The reservation time must be based on the device time. During optimization, APs will switch channels, which causes clients to go offline and affects user experience. You are advised to avoid peak hours. ● Network optimization takes about 12 minutes in total.
Select Project	Select to optimize all APs or a specified AP group.
2.4 GHz, 5 GHz, and 6 GHz bandwidths	Configures the bandwidth for the 2.4 GHz, 5 GHz, and 6 GHz frequency bands.

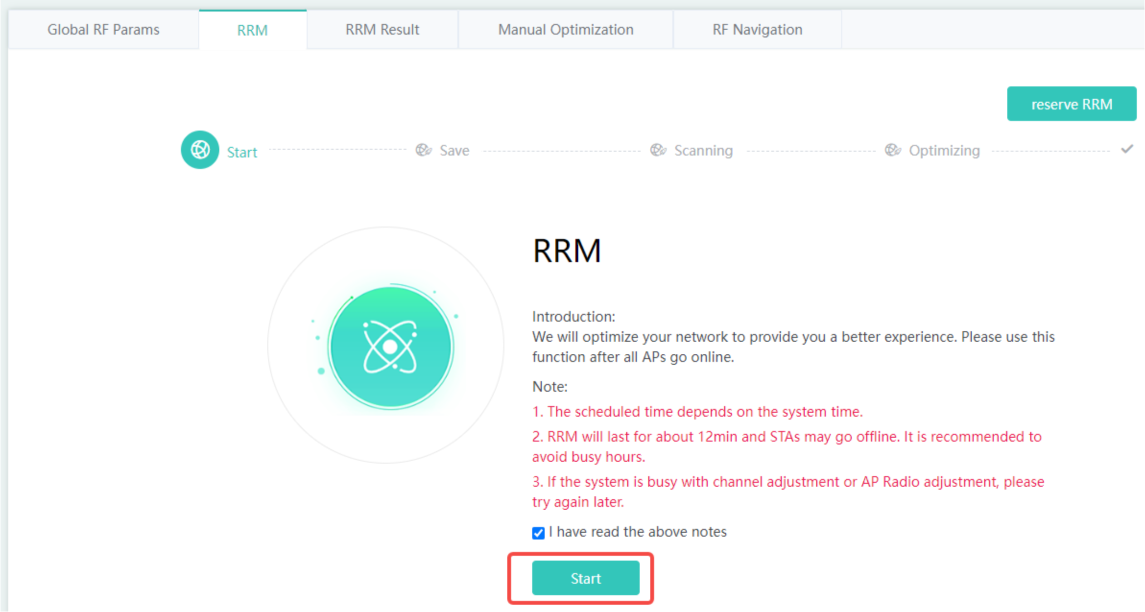
(7) Click Save. When the scheduled AP optimization time is reached, one-click network optimization can be performed based on the preset configuration.

Caution

WIO will be unavailable if the system is undergoing channel dynamic adjustment or auto adjustment of radios of newly connected APs. Please try again later.

- Optimize

(1) Read and check "I have read and agreed to the above precautions", and click Start to go to the Configuration page.



RRM

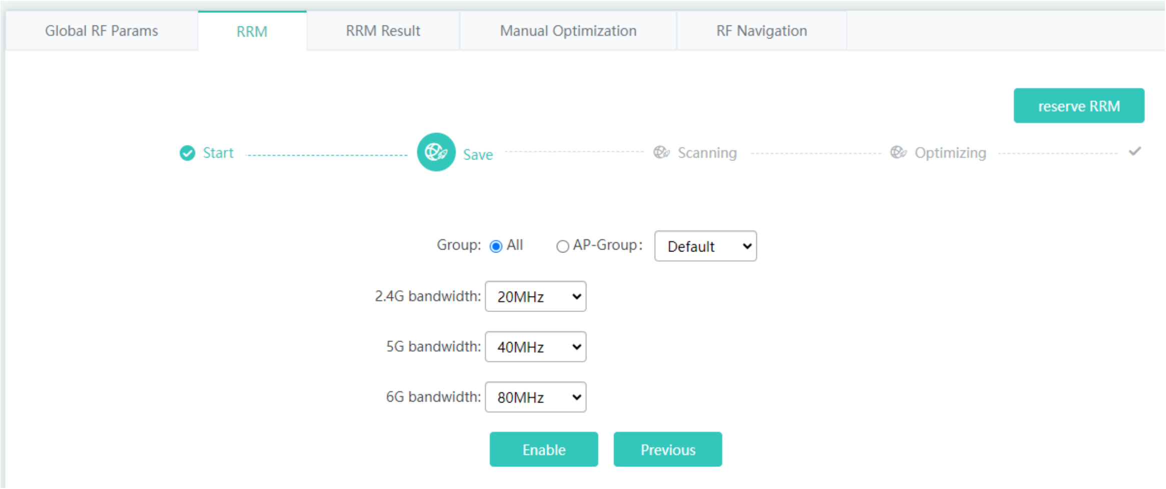
Introduction:
We will optimize your network to provide you a better experience. Please use this function after all APs go online.

Note:

1. The scheduled time depends on the system time.
2. RRM will last for about 12min and STAs may go offline. It is recommended to avoid busy hours.
3. If the system is busy with channel adjustment or AP Radio adjustment, please try again later.

☑ I have read the above notes

(8) Configure network optimization information as required.



Group: ● All ○ AP-Group: Default

2.4G bandwidth: 20MHz

5G bandwidth: 40MHz

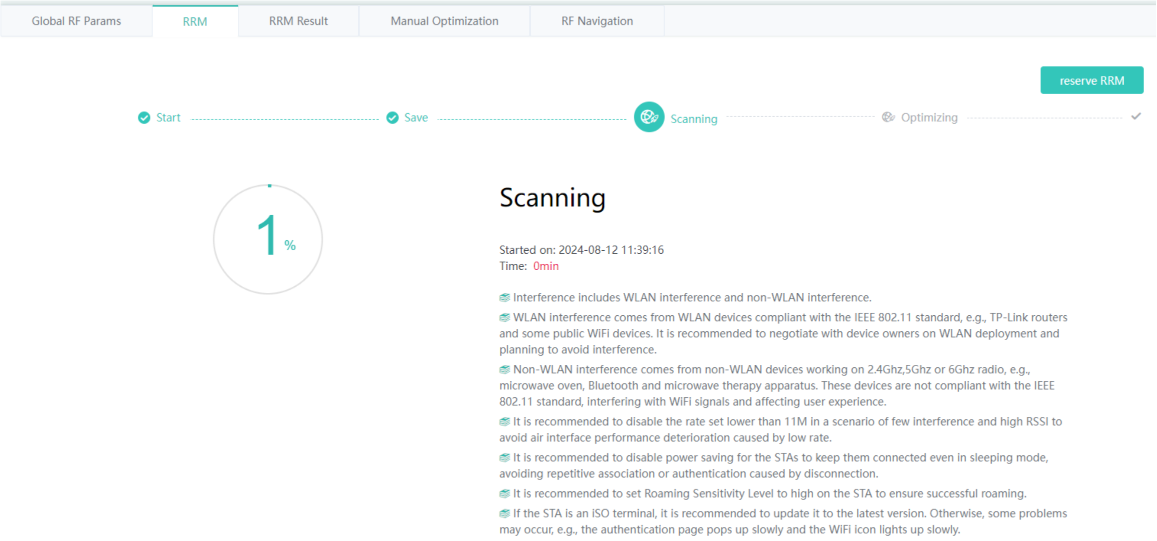
6G bandwidth: 80MHz

Config Parameter	Parameter Description
Select Project	Select to optimize all APs or a specified AP group.
2.4 GHz, 5 GHz, and 6 GHz bandwidths	Configures the bandwidth for the 2.4 GHz, 5 GHz, and 6 GHz frequency bands.

(9) Click Enable. In the displayed dialog box, click OK to enter the automatic scanning and optimization phase of one-click network optimization.

Caution

- Once the RRM is started, the configuration cannot be rolled back. During optimization, APs on the network will switch channels, which may result in temporary disconnection and affect user experience. You are advised to perform RRM in off-peak hours.
- The scan and optimization will take about 12 minutes. Please wait patiently.

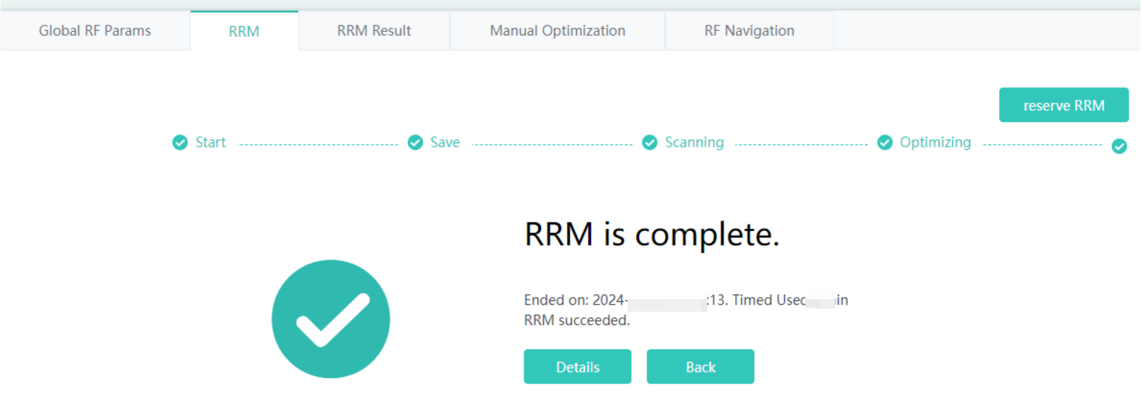


Scanning

Started on: 2024-08-12 11:39:16
Time: 0min

- Interference includes WLAN interference and non-WLAN interference.
- WLAN interference comes from WLAN devices compliant with the IEEE 802.11 standard, e.g., TP-Link routers and some public WiFi devices. It is recommended to negotiate with device owners on WLAN deployment and planning to avoid interference.
- Non-WLAN interference comes from non-WLAN devices working on 2.4Ghz,5Ghz or 6Ghz radio, e.g., microwave oven, Bluetooth and microwave therapy apparatus. These devices are not compliant with the IEEE 802.11 standard, interfering with WiFi signals and affecting user experience.
- It is recommended to disable the rate set lower than 11M in a scenario of few interference and high RSSI to avoid air interface performance deterioration caused by low rate.
- It is recommended to disable power saving for the STAs to keep them connected even in sleeping mode, avoiding repetitive association or authentication caused by disconnection.
- It is recommended to set Roaming Sensitivity Level to high on the STA to ensure successful roaming.
- If the STA is an iSO terminal, it is recommended to update it to the latest version. Otherwise, some problems may occur, e.g., the authentication page pops up slowly and the WiFi icon lights up slowly.

(10) After the RRM is complete, click Back to return to the RRM page. Click Details to be redirected to the RRM Result page and check the optimization.

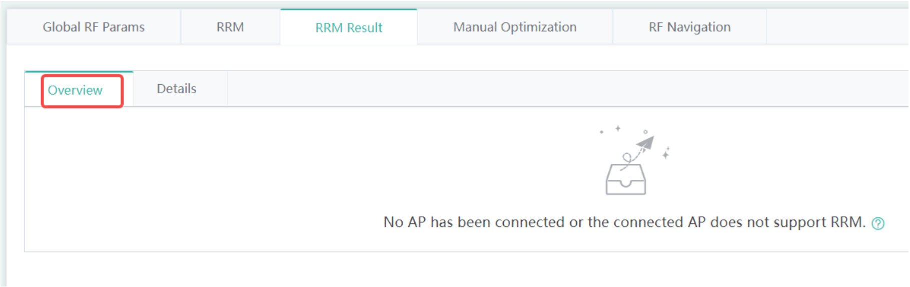


RRM is complete.

Ended on: 2024-[redacted]:13. Timed Usec[redacted]in
RRM succeeded.

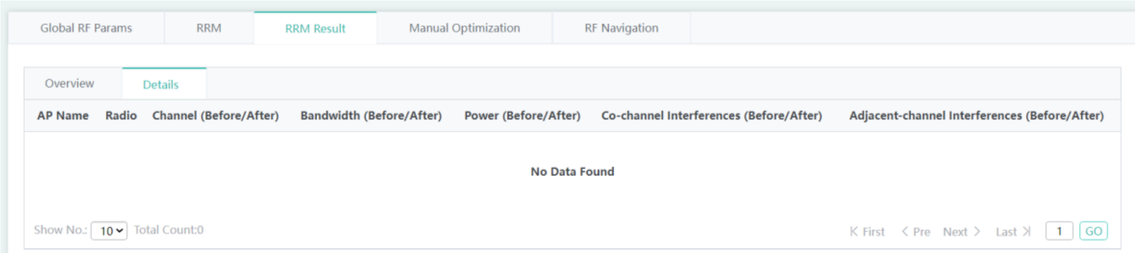
3. RRM Result

Overview: Display the number of signal interferences before and after the RRM in the form of a bar chart (the top 20 most significant changes).



No AP has been connected or the connected AP does not support RRM.

Details: Display all RRM results in a list format, with changes in data before and after the RRM highlighted in red font.



AP Name	Radio	Channel (Before/After)	Bandwidth (Before/After)	Power (Before/After)	Co-channel Interferences (Before/After)	Adjacent-channel Interferences (Before/After)

No Data Found

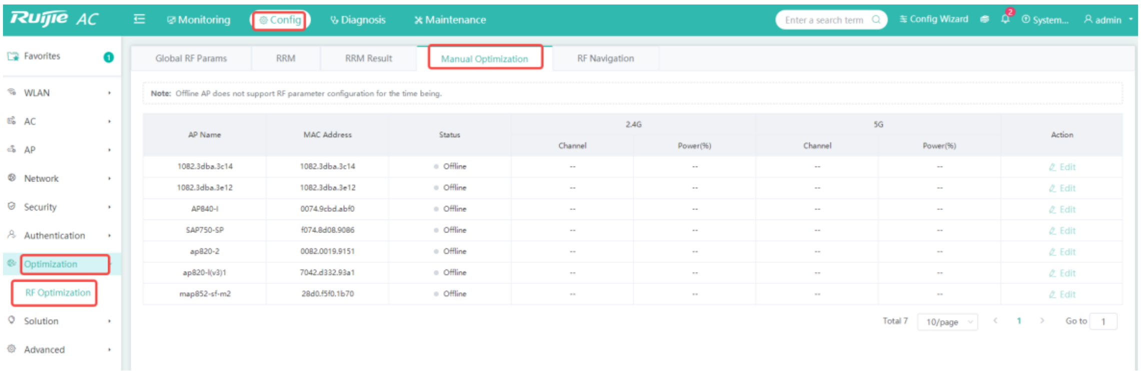
4. Manual Optimization

You can manually plan AP parameters such as the channel and power as required to optimize the network.

Note

Offline AP does not support RF parameter configuration for the time being. Double 5G devices currently only support configuration up to radio 2.

Click **Edit** and manually set parameters such as the channel and power. Click ⊗ to cancel the settings and click ✓ to save the settings.



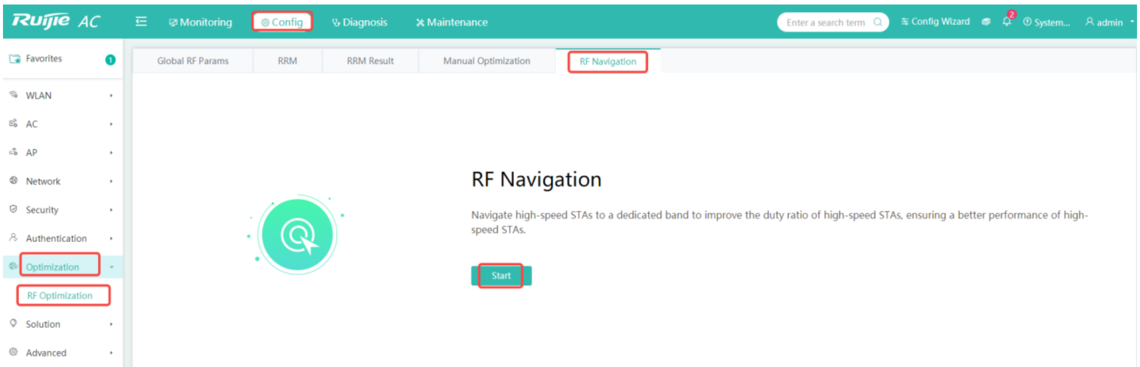
Note: Offline AP does not support RF parameter configuration for the time being.

AP Name	MAC Address	Status	2.4G		5G		Action
			Channel	Power(%)	Channel	Power(%)	
1082.3dba.3c14	1082.3dba.3c14	Offline	--	--	--	--	Edit
1082.3dba.3e12	1082.3dba.3e12	Offline	--	--	--	--	Edit
AP840-I	0074.9cbd.abf0	Offline	--	--	--	--	Edit
SAP750-SP	f074.8d08.9086	Offline	--	--	--	--	Edit
ap820-2	0082.0019.9151	Offline	--	--	--	--	Edit
ap820-l(v3)1	7042.d332.93a1	Offline	--	--	--	--	Edit
map852-sf-m2	28d0.f5f0.1b70	Offline	--	--	--	--	Edit

Total 7 10/page 1 Go to 1

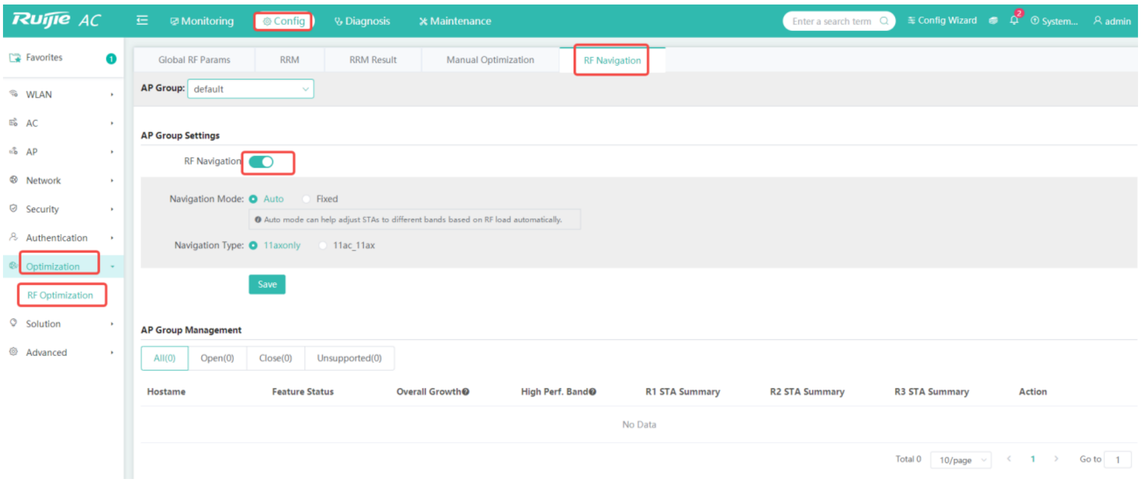
5. RF Navigation

When multiple types of clients coexist, high-performance clients are navigated to a dedicated high-efficiency frequency band. This prevents low-speed clients from occupying the air interface for a long time and improves the duty ratio of high-performance clients. RF navigation ensures that high-performance clients have a better experience in the Wi-Fi 6 frequency band.



RF Navigation

Navigate high-speed STAs to a dedicated band to improve the duty ratio of high-speed STAs, ensuring a better performance of high-speed STAs.



AP Group: default

AP Group Settings

RF Navigation: ●

Navigation Mode: ● Auto ○ Fixed

Auto mode can help adjust STAs to different bands based on RF load automatically.

Navigation Type: ● 11axonly ○ 11ac_11ax

AP Group Management

All(0) Open(0) Close(0) Unsupported(0)

Hostame	Feature Status	Overall Growth	High Perf. Band	R1 STA Summary	R2 STA Summary	R3 STA Summary	Action
No Data							

Total 0 10/page 1 Go to 1

5.7.2 Network Optimization

Choose **Config** > **Optimization** > **Network Optimization** > **Extreme Test Scenario**.

The **Extreme Test Scenario** function helps you deliver the optimal configuration of a specified client with one click.

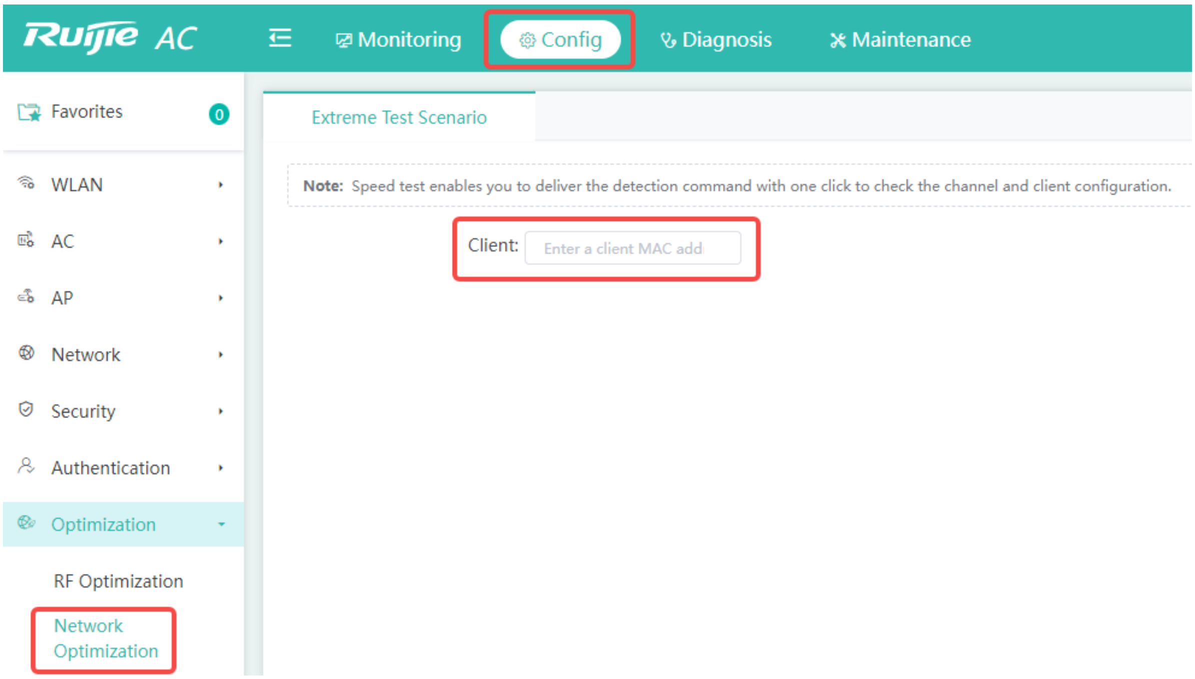
Note

Before detecting a specified client, ensure that the client is online.

Caution

This function may cause network disconnection during configuration delivery, which affects services. Before configuring this function, ensure that normal services are not affected or configure the function in off-peak hours.

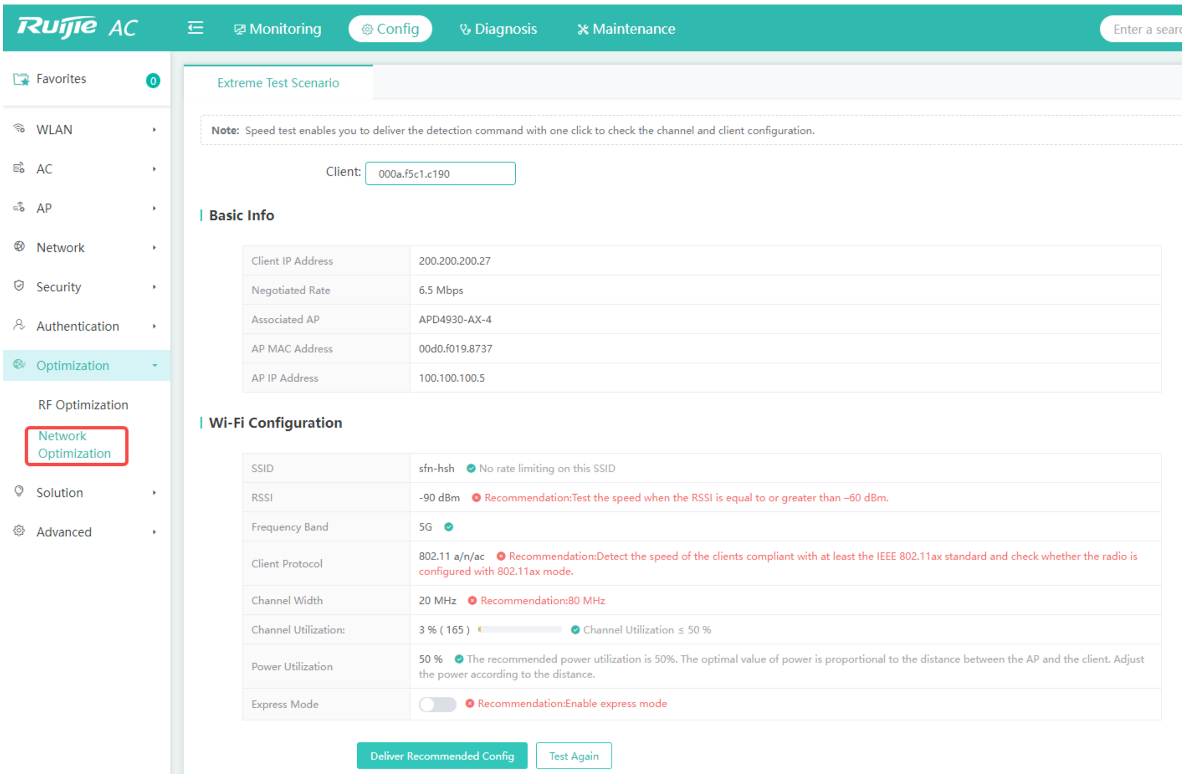
(1) Enter the MAC address of a client to view its basic information and configuration.



Note: Speed test enables you to deliver the detection command with one click to check the channel and client configuration.

Client: Enter a client MAC add

(2) Based on the identified optimal channel, client RSSI, channel utilization, and other information, the AC can recommend the channel, channel width, power, and whether to enable the express mode for the client.



Note: Speed test enables you to deliver the detection command with one click to check the channel and client configuration.

Client: 000a.f5c1.c190

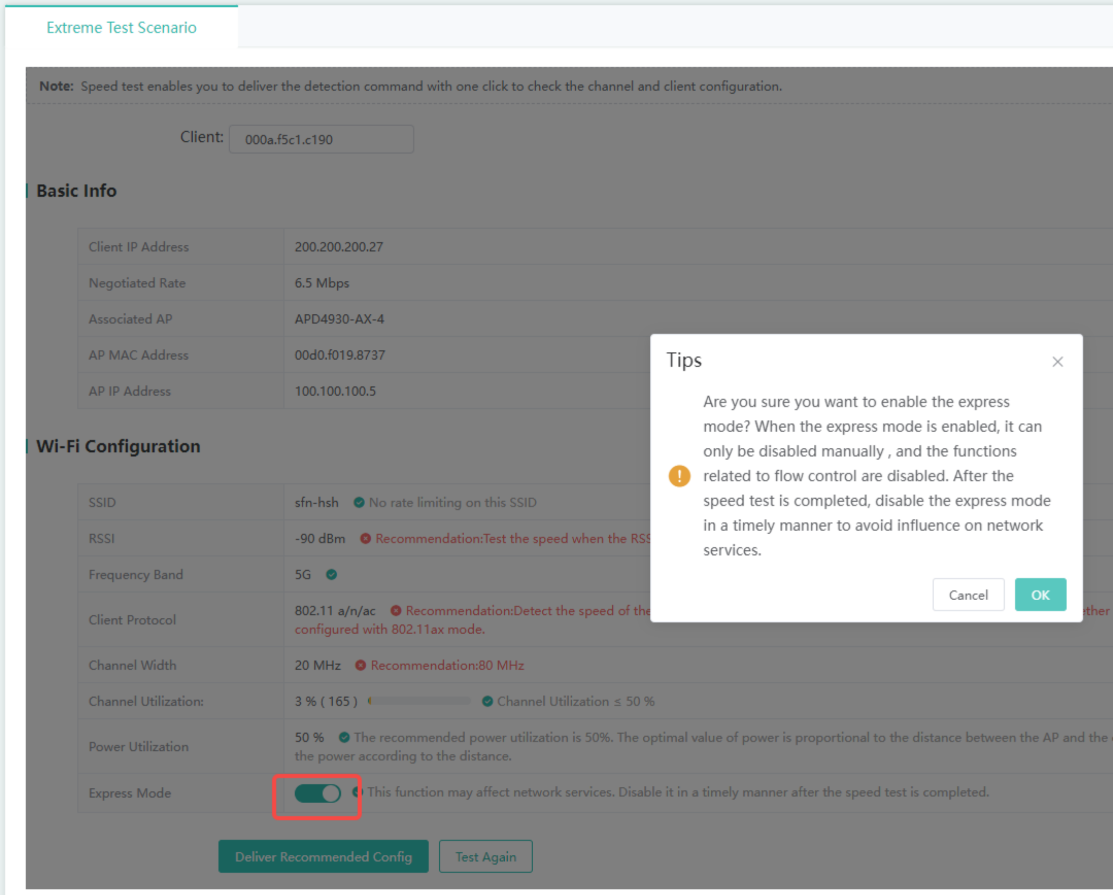
Basic Info

Client IP Address	200.200.200.27
Negotiated Rate	6.5 Mbps
Associated AP	APD4930-AX-4
AP MAC Address	00d0.f019.8737
AP IP Address	100.100.100.5

Wi-Fi Configuration

SSID	sfn-hsh ✓ No rate limiting on this SSID
RSSI	-90 dBm ● Recommendation:Test the speed when the RSSI is equal to or greater than –60 dBm.
Frequency Band	5G ✓
Client Protocol	802.11 a/n/ac ● Recommendation:Detect the speed of the clients compliant with at least the IEEE 802.11ax standard and check whether the radio is configured with 802.11ax mode.
Channel Width	20 MHz ● Recommendation:80 MHz
Channel Utilization:	3 % (165) ✓ Channel Utilization ≤ 50 %
Power Utilization	50 % ✓ The recommended power utilization is 50%. The optimal value of power is proportional to the distance between the AP and the client. Adjust the power according to the distance.
Express Mode	○ ● Recommendation:Enable express mode

(3) If the express mode needs to be enabled according to the recommendation, toggle on **Express Mode**. In the dialog box that is displayed, click **OK** after confirming the message.



Note: Speed test enables you to deliver the detection command with one click to check the channel and client configuration.

Client: 000a.f5c1.c190

Basic Info

Client IP Address	200.200.200.27
Negotiated Rate	6.5 Mbps
Associated AP	APD4930-AX-4
AP MAC Address	00d0.f019.8737
AP IP Address	100.100.100.5

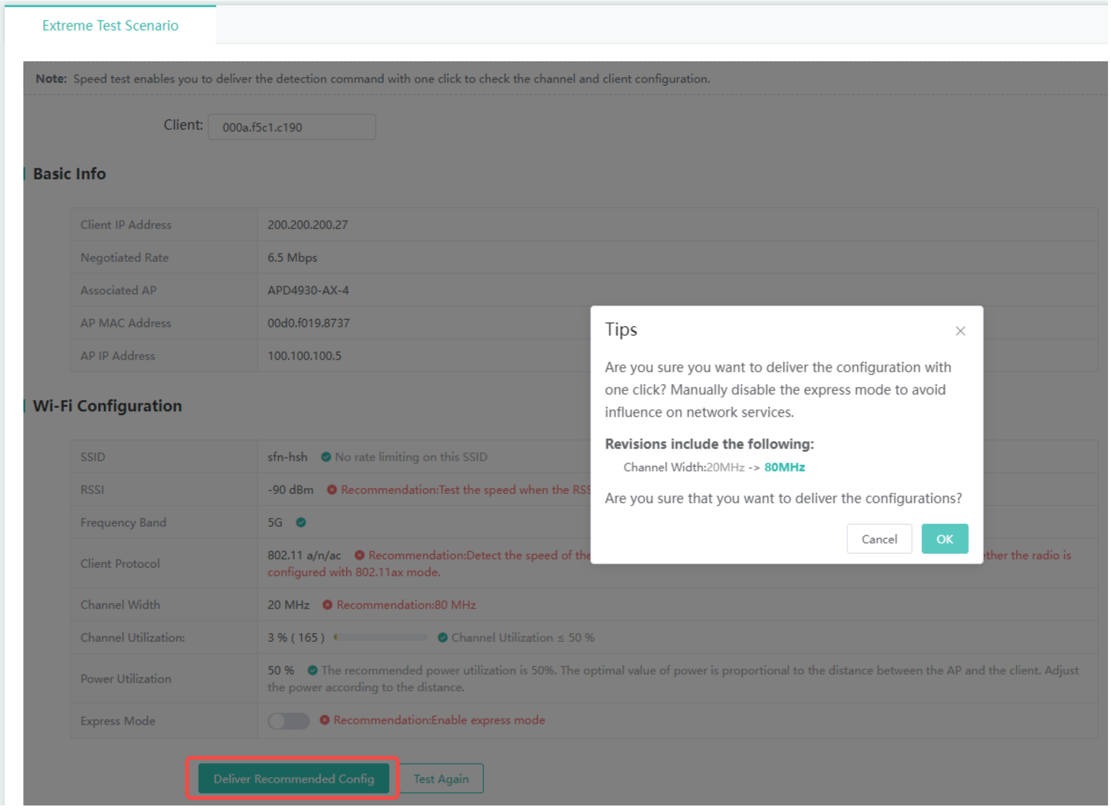
Wi-Fi Configuration

SSID	sfn-hsh ✓ No rate limiting on this SSID
RSSI	-90 dBm ● Recommendation:Test the speed when the RSS
Frequency Band	5G ✓
Client Protocol	802.11 a/n/ac ● Recommendation:Detect the speed of the ... ther configured with 802.11ax mode.
Channel Width	20 MHz ● Recommendation:80 MHz
Channel Utilization:	3 % (165) ✓ Channel Utilization ≤ 50 %
Power Utilization	50 % ✓ The recommended power utilization is 50%. The optimal value of power is proportional to the distance between the AP and the the power according to the distance.
Express Mode	● This function may affect network services. Disable it in a timely manner after the speed test is completed.

Tips

Are you sure you want to enable the express mode? When the express mode is enabled, it can only be disabled manually , and the functions related to flow control are disabled. After the speed test is completed, disable the express mode in a timely manner to avoid influence on network services.

(4) Click **Deliver Recommended Config**. Verify the configuration to be delivered with one click and click **OK**.



Note: Speed test enables you to deliver the detection command with one click to check the channel and client configuration.

Client: 000a.f5c1.c190

Basic Info

Client IP Address	200.200.200.27
Negotiated Rate	6.5 Mbps
Associated AP	APD4930-AX-4
AP MAC Address	00d0.f019.8737
AP IP Address	100.100.100.5

Wi-Fi Configuration

SSID	sfn-hsh ✓ No rate limiting on this SSID
RSSI	-90 dBm ✕ Recommendation:Test the speed when the RSS
Frequency Band	5G ✓
Client Protocol	802.11 a/n/ac ✕ Recommendation:Detect the speed of the ther the radio is configured with 802.11ax mode.
Channel Width	20 MHz ✕ Recommendation:80 MHz
Channel Utilization:	3 % (165) ✓ Channel Utilization ≤ 50 %
Power Utilization	50 % ✓ The recommended power utilization is 50%. The optimal value of power is proportional to the distance between the AP and the client. Adjust the power according to the distance.
Express Mode	✕ Recommendation:Enable express mode

Tips

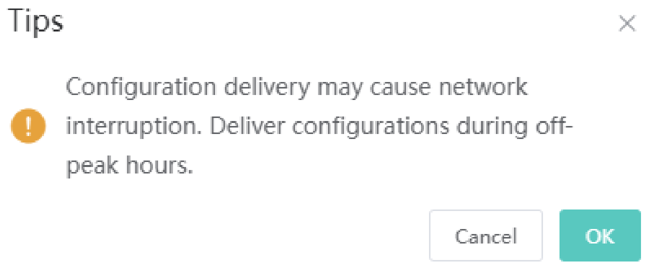
Are you sure you want to deliver the configuration with one click? Manually disable the express mode to avoid influence on network services.

Revisions include the following:

Channel Width:20MHz -> **80MHz**

Are you sure that you want to deliver the configurations?

(5) Check the prompt and click **OK**. You are advised to perform this configuration during off-peak hours.



Tips

Configuration delivery may cause network interruption. Deliver configurations during off-peak hours.

(6) After the configuration, click **Test Again** and view the delivered configuration.

5.8 Solution

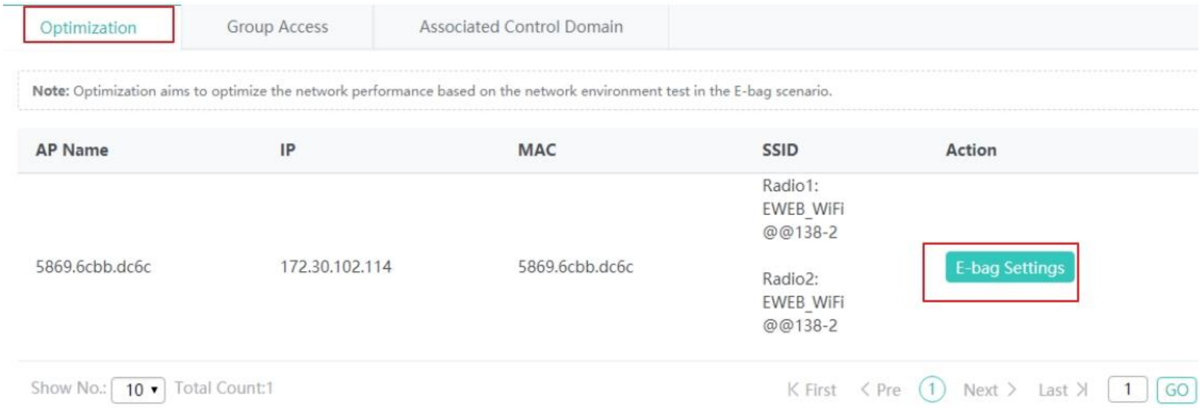
5.8.1 E-bag Solution

Choose **Config** > **Solution** > **Ebag**.

The E-bag solution is mainly applicable to schools. To perform network optimization, evaluate the actual network environment of the E-bag first. Based on the evaluation results, perform a series of network optimization to balance network performance and ensure fast Internet speed for users.

1. E-bag Network Optimization

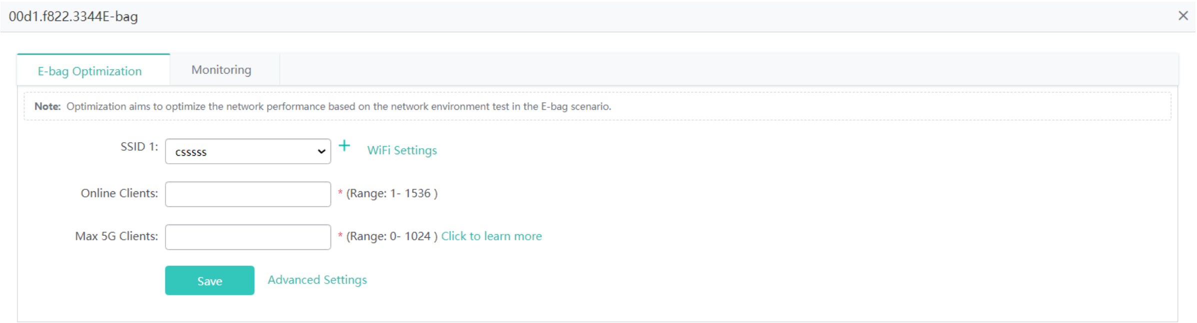
Click **E-bag Settings** to access the E-bag optimization page.



Note: Optimization aims to optimize the network performance based on the network environment test in the E-bag scenario.

AP Name	IP	MAC	SSID	Action
5869.6cbb.dc6c	172.30.102.114	5869.6cbb.dc6c	Radio1: EWEB_WiFi @@138-2 Radio2: EWEB_WiFi @@138-2	E-bag Settings

Show No.: 10 Total Count:1



00d1.f822.3344E-bag

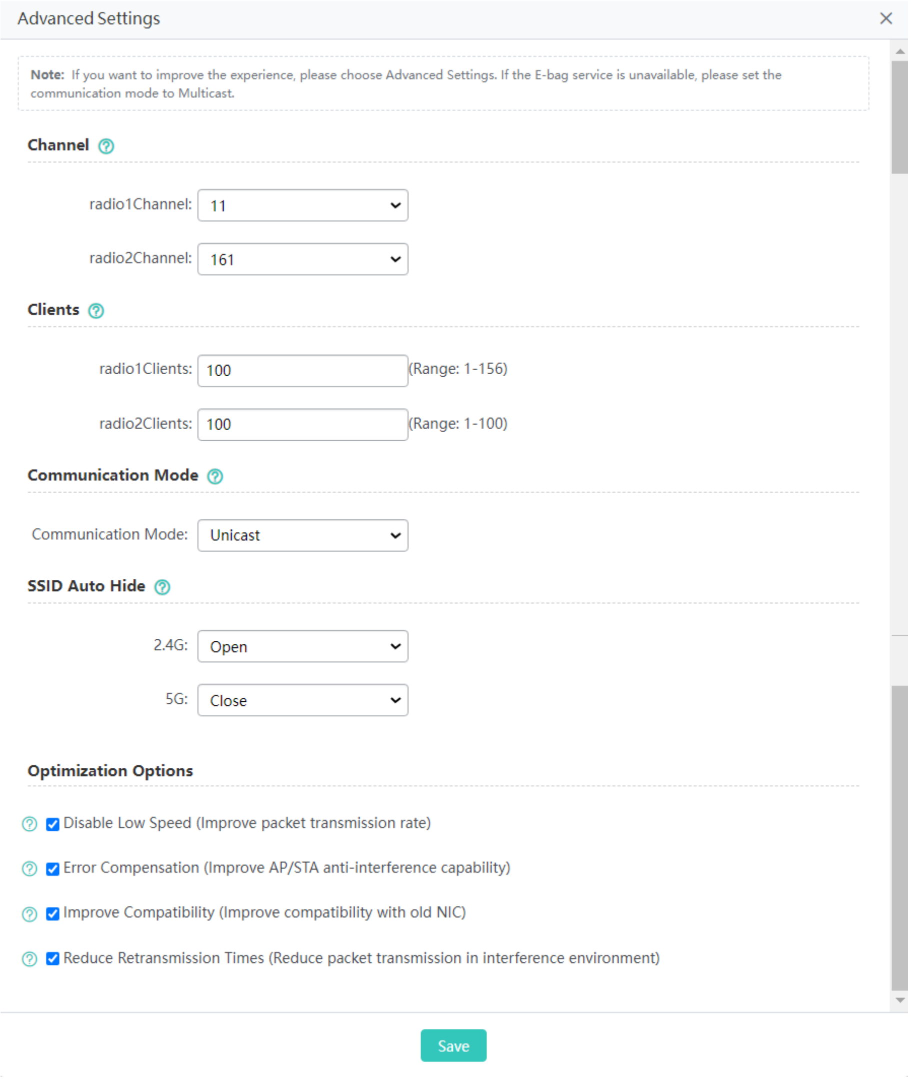
Note: Optimization aims to optimize the network performance based on the network environment test in the E-bag scenario.

SSID 1: csssss + WiFi Settings

Online Clients: * (Range: 1- 1536)

Max 5G Clients: * (Range: 0- 1024) Click to learn more

Advanced Configuration



Advanced Settings ✕

Note: If you want to improve the experience, please choose Advanced Settings. If the E-bag service is unavailable, please set the communication mode to Multicast.

Channel ?

radio1Channel: 11

radio2Channel: 161

Clients ?

radio1Clients: 100 (Range: 1-156)

radio2Clients: 100 (Range: 1-100)

Communication Mode ?

Communication Mode: Unicast

SSID Auto Hide ?

2.4G: Open

5G: Close

Optimization Options

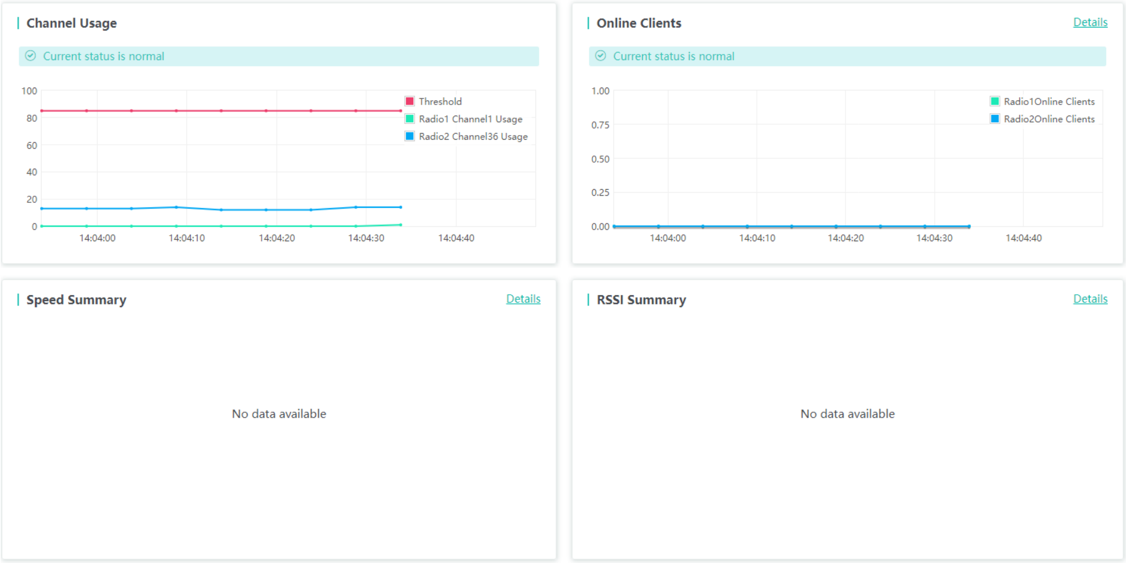
? ☑ Disable Low Speed (Improve packet transmission rate)

? ☑ Error Compensation (Improve AP/STA anti-interference capability)

? ☑ Improve Compatibility (Improve compatibility with old NIC)

? ☑ Reduce Retransmission Times (Reduce packet transmission in interference environment)

Operation Monitoring



Channel Usage

Current status is normal

Online Clients Details

Current status is normal

Speed Summary Details

No data available

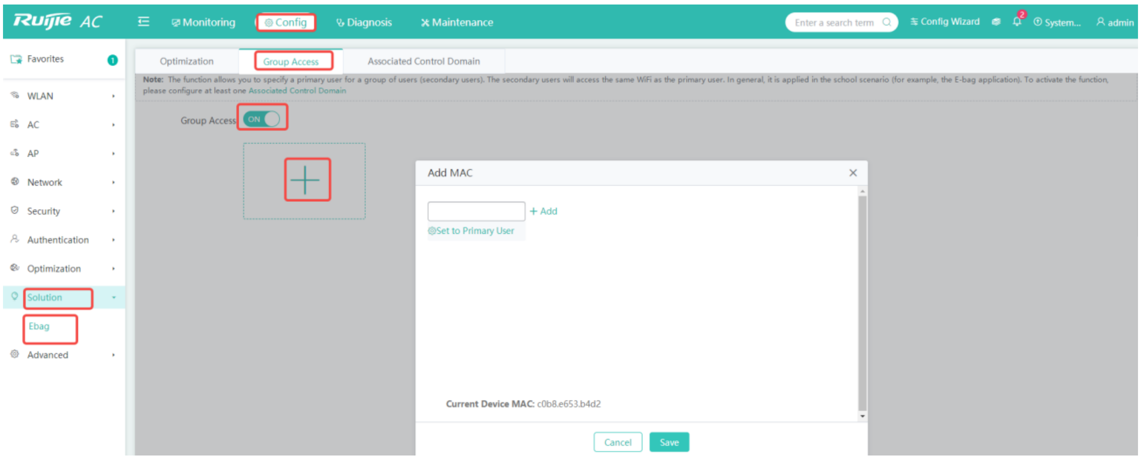
RSSI Summary Details

No data available

2. Group Access

Group Access: Toggle on or off the switch to enable or disable the **Group Access** feature.

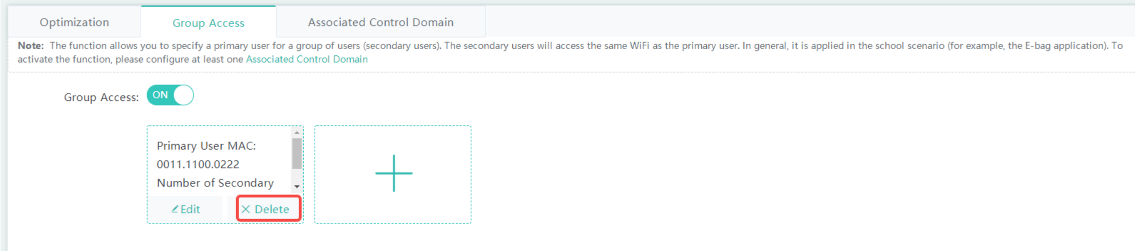
(1) Add a client group: Click **+**. Configure the information in the pop-up dialog box. Click **Save**. A message indicating the configuration has been saved is displayed. The newly added client packet is displayed in the **Associated Control Domain** list.



Note: The function allows you to specify a primary user for a group of users (secondary users). The secondary users will access the same WiFi as the primary user. In general, it is applied in the school scenario (for example, the E-bag application). To activate the function, please configure at least one Associated Control Domain

Current Device MAC: c0b8.e653.b4d2

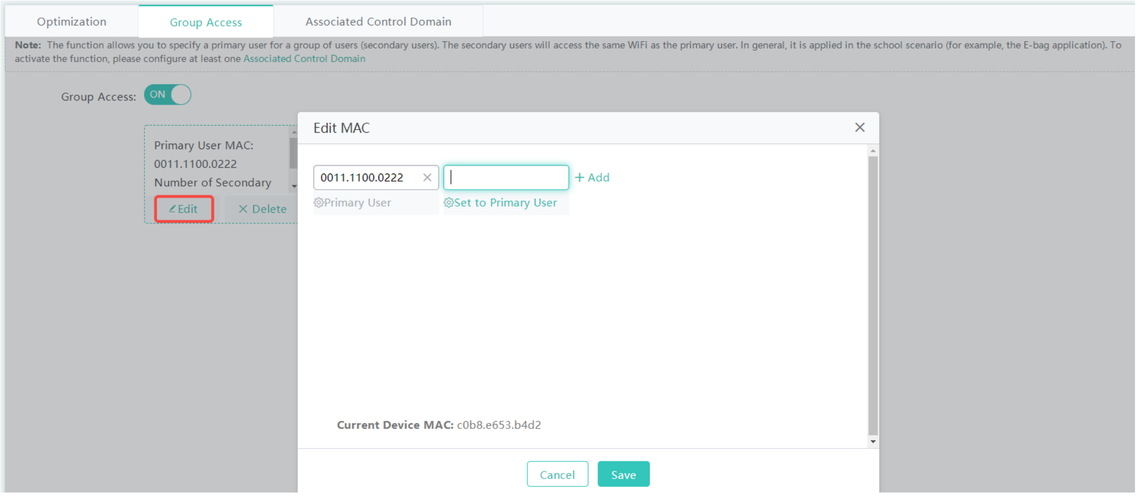
(2) Delete a client group: Click **Delete**. The confirmation dialog box pops up. Click **OK** to finish the operation.



Note: The function allows you to specify a primary user for a group of users (secondary users). The secondary users will access the same WiFi as the primary user. In general, it is applied in the school scenario (for example, the E-bag application). To activate the function, please configure at least one Associated Control Domain

Primary User MAC:
0011.1100.0222
Number of Secondary

(3) Edit a client group: Click **Edit**. Configure the information in the pop-up dialog box. Click **Save**. A message indicating the configuration has been saved is displayed. The edited client packet is displayed in the **Associated Control Domain** list.



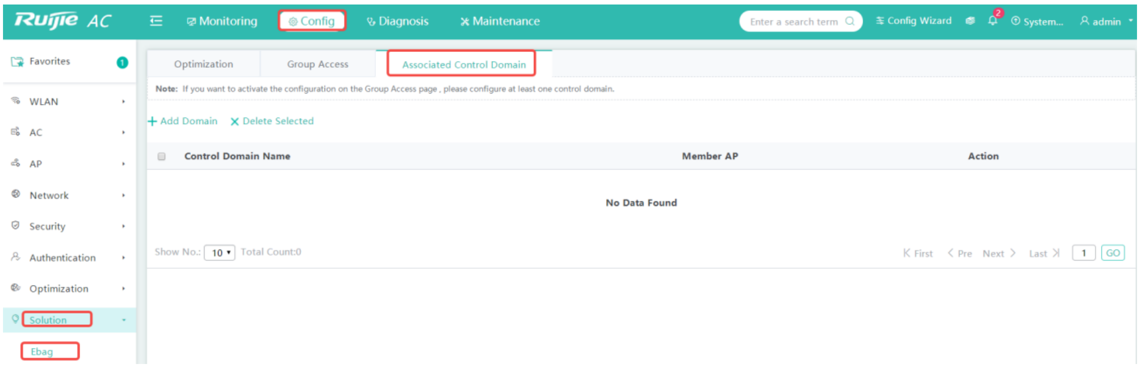
Note: The function allows you to specify a primary user for a group of users (secondary users). The secondary users will access the same WiFi as the primary user. In general, it is applied in the school scenario (for example, the E-bag application). To activate the function, please configure at least one Associated Control Domain

Primary User MAC:
0011.1100.0222
Number of Secondary

0011.1100.0222

Current Device MAC: c0b8.e653.b4d2

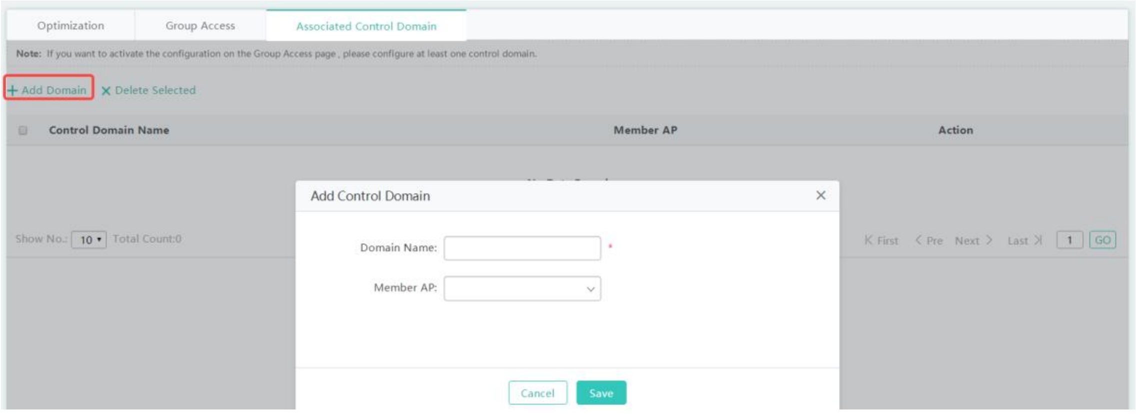
3. Associated Control Domain



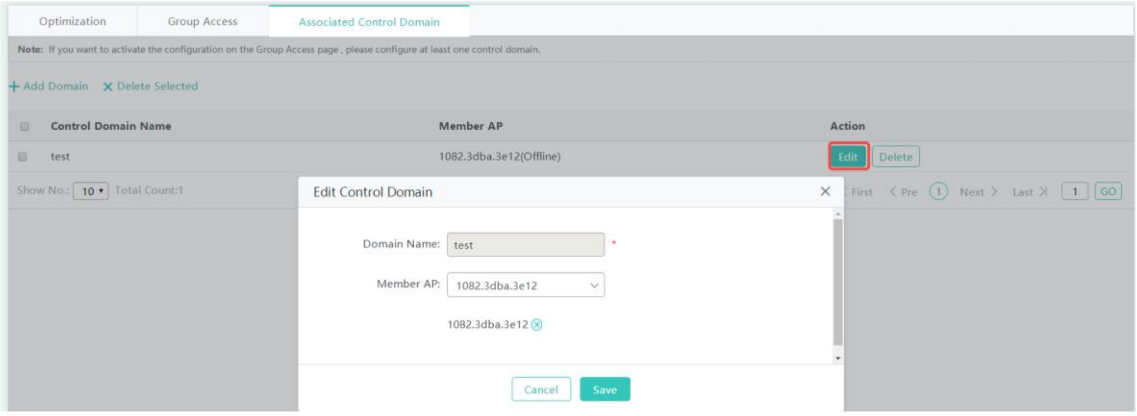
Note: If you want to activate the configuration on the Group Access page , please configure at least one control domain.

Control Domain Name	Member AP	Action
No Data Found		

(1) Add an associated control domain: Click **Add Domain**. Configure the information in the pop-up dialog box. Click **Save**. A message indicating the configuration has been saved is displayed. The newly added associated control domain is displayed in the **Associated Control Domain** list.



(2) Edit an associated control domain: Click **Edit** behind a specified associated control domain in the list. The information about the associated control domain is displayed in the pop-up dialog box. Edit the information. Click **Save**. A message indicating the configuration has been saved is displayed.



Note: If you want to activate the configuration on the Group Access page , please configure at least one control domain.

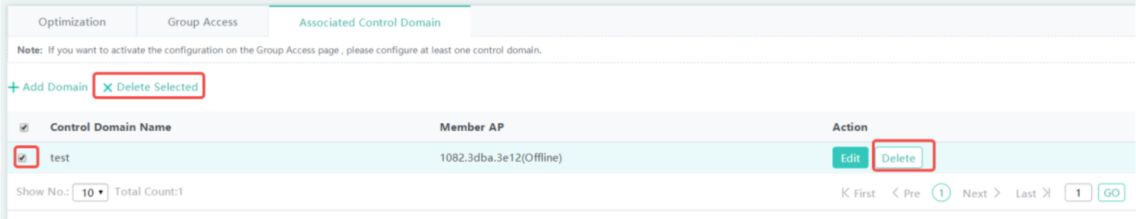
Control Domain Name	Member AP	Action
test	1082.3dba.3e12(Offline)	Edit Delete

Domain Name: test

Member AP: 1082.3dba.3e12

1082.3dba.3e12

(3) Delete an associated control domain: Click **Delete** behind a specified associated control domain in the list. The confirmation dialog box pops up. Click **OK** to finish the operation.


Optimization
Group Access
Associated Control Domain

Note: If you want to activate the configuration on the Group Access page , please configure at least one control domain.

+ Add Domain
✕ Delete Selected

☑	Control Domain Name	Member AP	Action
☑	test	1082.3dba.3e12(Offline)	Edit Delete

Show No.: 10 Total Count:1
First Pre 1 Next Last 1 GO

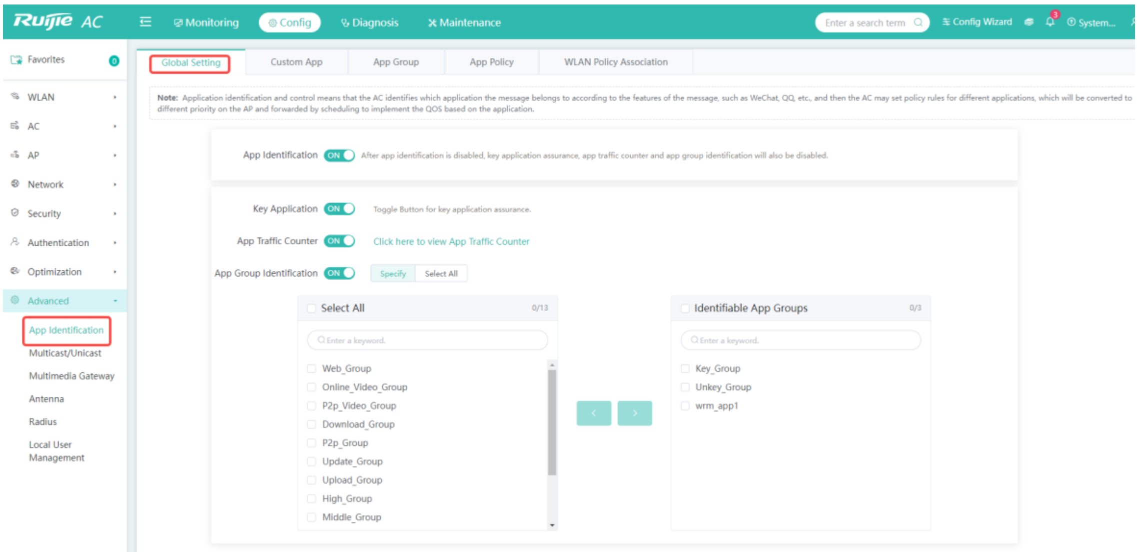
5.9 Advanced

5.9.1 App Identification

Choose **Config** > **Advanced** > **App Identification**.

1. Global Settings

Application identification and control means that the AC identifies which application packets belong to according to the features of the packets, such as WeChat and QQ. Different policies can be set for different applications on the AC to convert them to different priorities on the AP. Then, the AP schedules the packets by implementing QoS based on the application.



Note: Application identification and control means that the AC identifies which application the message belongs to according to the features of the message, such as WeChat, QQ, etc., and then the AC may set policy rules for different applications, which will be converted to different priority on the AP and forwarded by scheduling to implement the QOS based on the application.

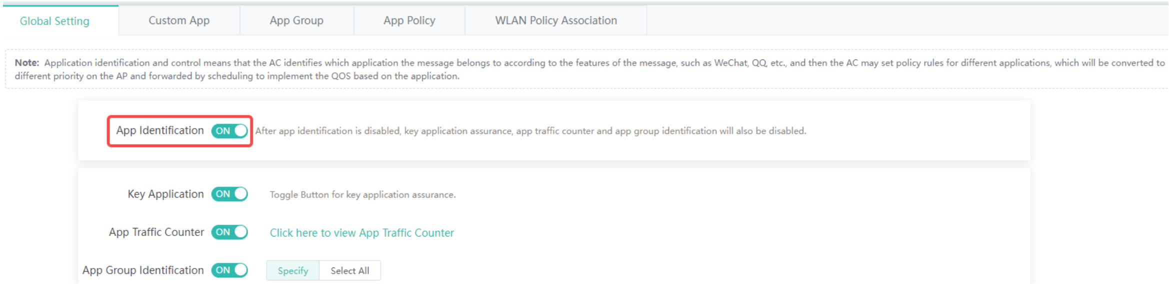
App Identification ON — After app identification is disabled, key application assurance, app traffic counter and app group identification will also be disabled.

Key Application ON — Toggle Button for key application assurance.

App Traffic Counter ON — Click here to view App Traffic Counter

App Group Identification ON — Specify | Select All

After **App Identification** is disabled, **Key Application Guarantee, App Traffic Counter**, and **App Group Identification** are also disabled.



Note: Application identification and control means that the AC identifies which application the message belongs to according to the features of the message, such as WeChat, QQ, etc., and then the AC may set policy rules for different applications, which will be converted to different priority on the AP and forwarded by scheduling to implement the QOS based on the application.

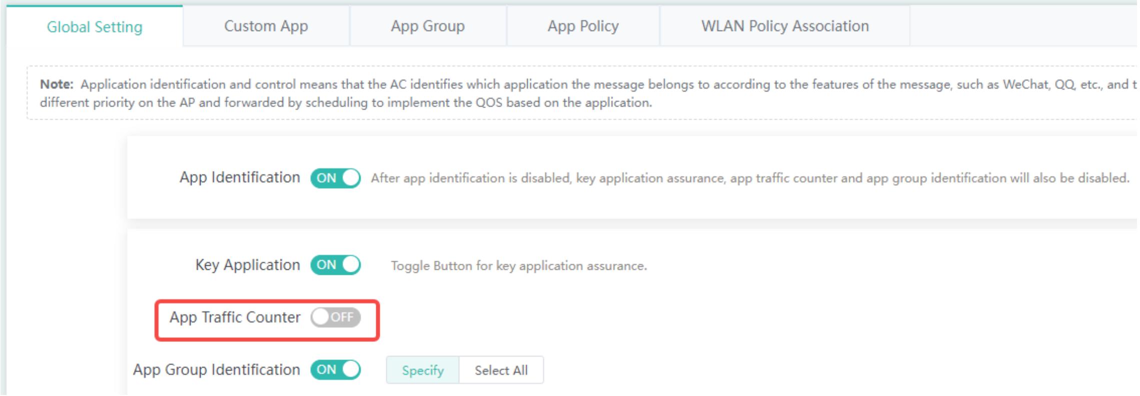
App Identification ON — After app identification is disabled, key application assurance, app traffic counter and app group identification will also be disabled.

Key Application ON — Toggle Button for key application assurance.

App Traffic Counter ON — Click here to view App Traffic Counter

App Group Identification ON — Specify | Select All

If **App Traffic Counter** is disabled, application traffic statistics of clients connected to the AC cannot be displayed on the **AppTraffic Overview** page.



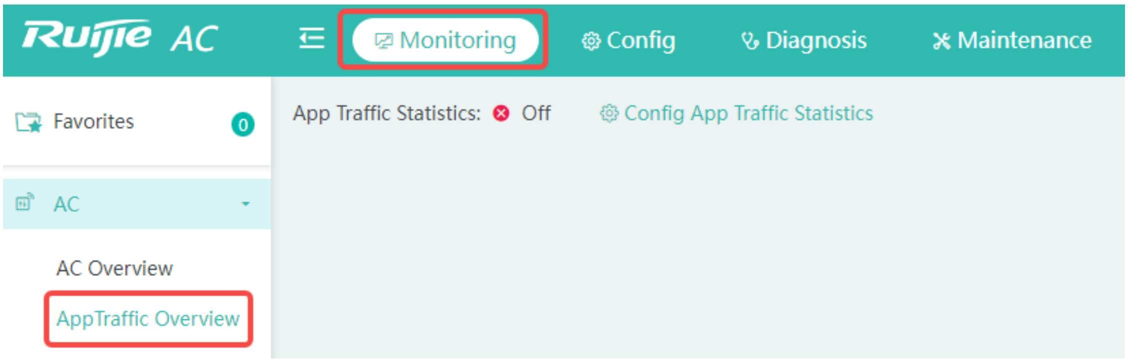
Note: Application identification and control means that the AC identifies which application the message belongs to according to the features of the message, such as WeChat, QQ, etc., and t different priority on the AP and forwarded by scheduling to implement the QOS based on the application.

App Identification ON After app identification is disabled, key application assurance, app traffic counter and app group identification will also be disabled.

Key Application ON Toggle Button for key application assurance.

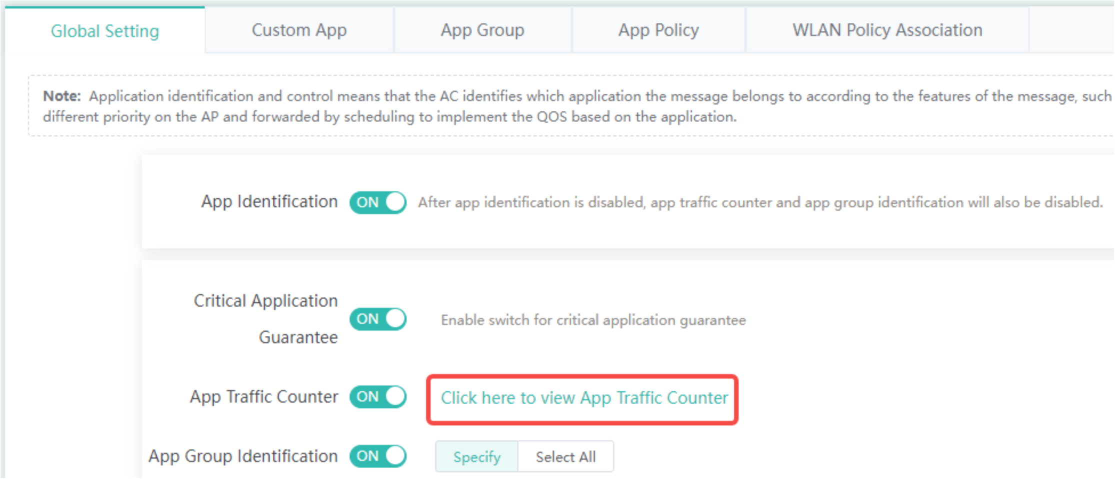
App Traffic Counter OFF

App Group Identification ON



App Traffic Statistics: Off

If **App Traffic Counter** is enabled, application traffic statistics of clients connected to the AC are displayed on the **AppTraffic Overview** page. Click **Click here to view App Traffic Counter** to redirect to the **AppTraffic Overview** page.



Note: Application identification and control means that the AC identifies which application the message belongs to according to the features of the message, such different priority on the AP and forwarded by scheduling to implement the QOS based on the application.

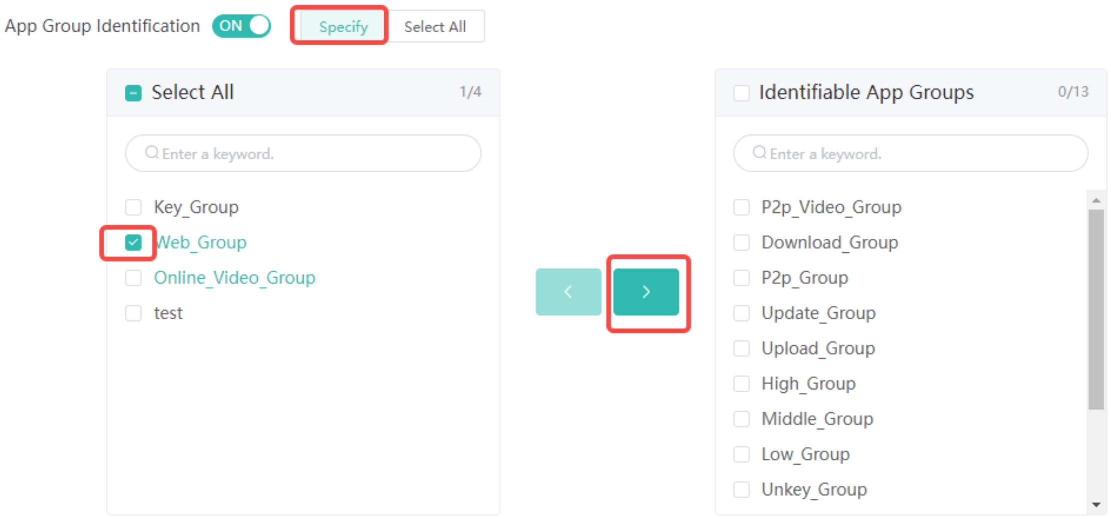
App Identification ON After app identification is disabled, app traffic counter and app group identification will also be disabled.

Critical Application Guarantee ON Enable switch for critical application guarantee

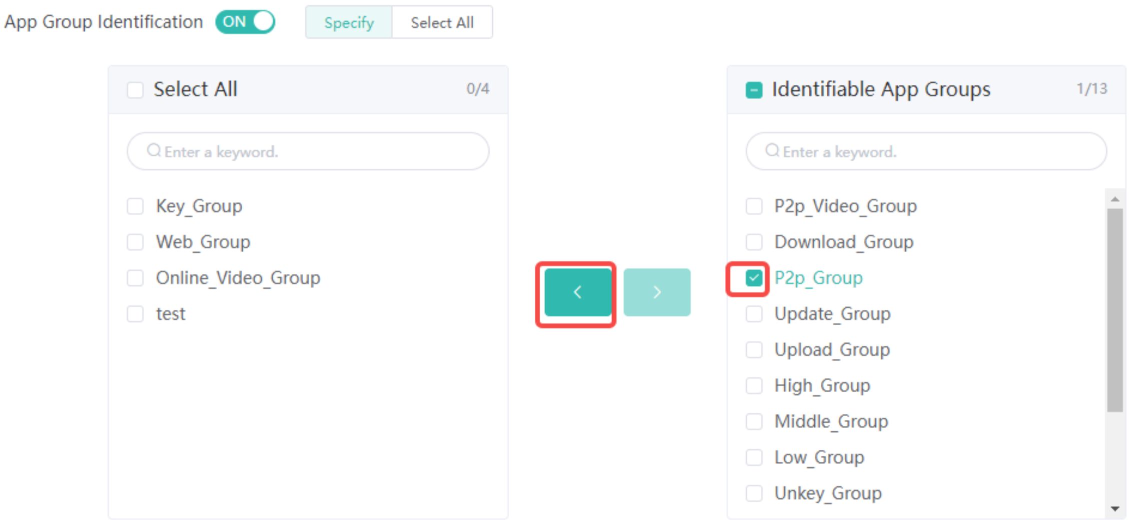
App Traffic Counter ON

App Group Identification ON

Toggle on **App Group Identification**. Click **Specify** or **Select All**. To specify an application group for identification, select the application group in the **Select All** pane on the left and add it to the **Identifiable App Groups** pane on the right.



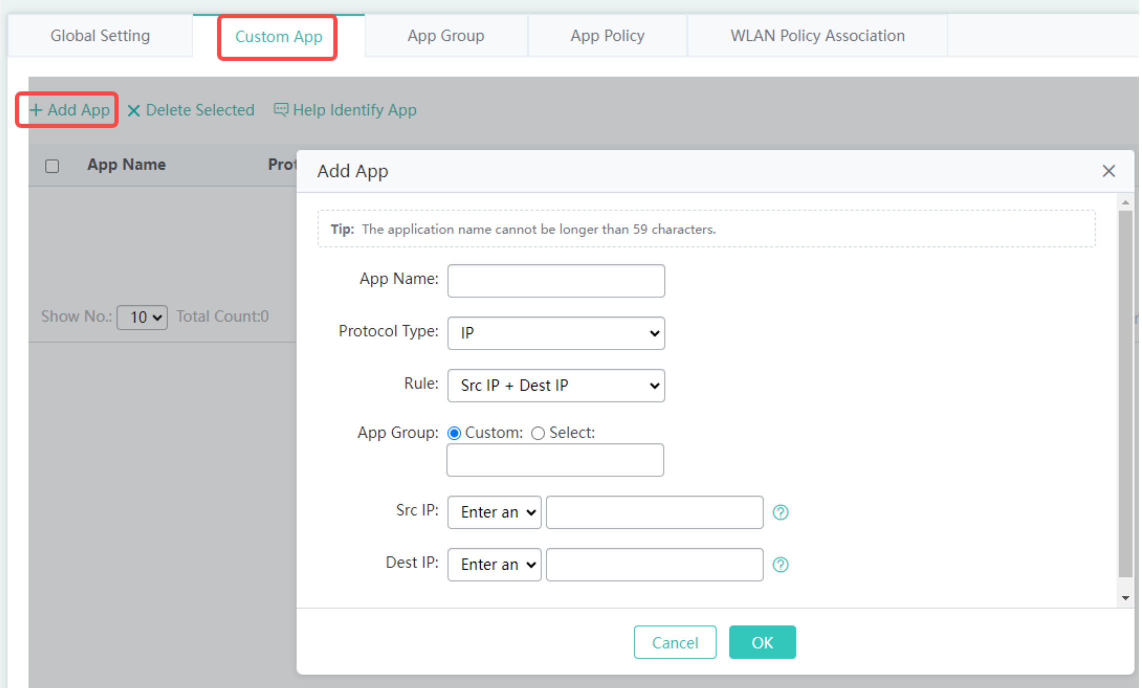
You can also select an application group in the **Identifiable App Groups** pane on the right and add it to the **Select All** pane on the left to cancel the identification of this application group by the AP.



2. Custom App

Configure a custom application to identify application traffic based on the quintuple information (source IP address, source port, destination IP address, destination port, and network protocol). If the device does not have a valid feature database, custom applications cannot be identified.

(1) Add a custom application: On the **Custom App** tab page, click **Add App**. In the dialog box that is displayed, edit information. Click **OK**. A message indicating successful configuration is displayed.



Tip: The application name cannot be longer than 59 characters.

App Name:

Protocol Type: IP

Rule: Src IP + Dest IP

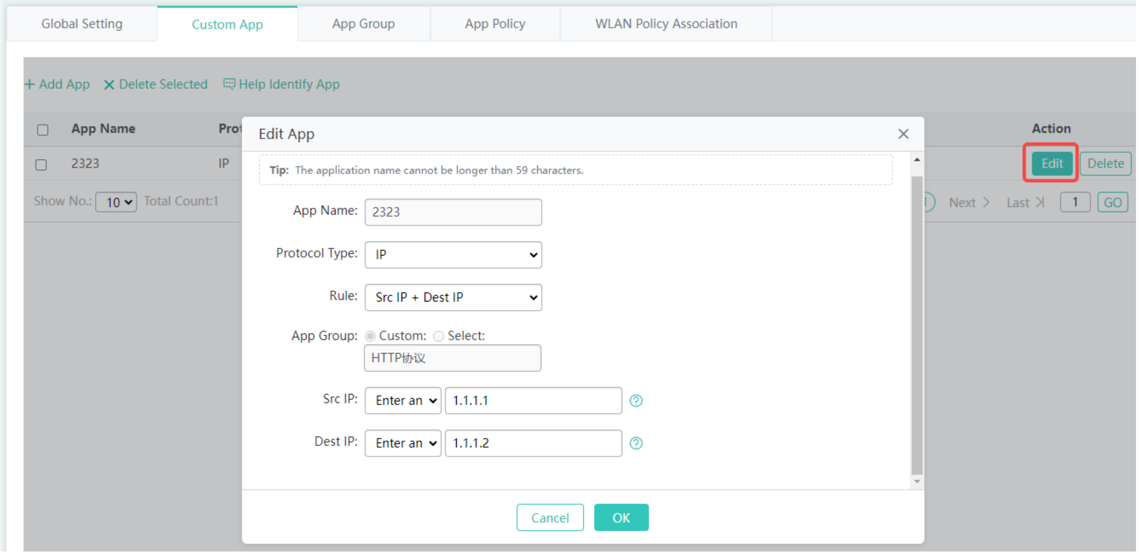
App Group: ● Custom: ○ Select:

Src IP: Enter an

Dest IP: Enter an

Parameter	Description
App Name	Application software name.
Protocol Type	IP, TCP, or UDP is supported.
Rule	Available rules vary with the protocol type.
App Group	Application category name.
Src IP	Start and end source IP addresses.
Dest IP	Start and end destination IP addresses.
Src Port	Start source port. The value range is from 0 to 65535 or the value **any**. End source port. The value range is from 0 to 65535 or the value **any**.
Dest Port	Start destination port. The value range is from 0 to 65535 or the value **any**. End destination port. The value range is from 0 to 65535 or the value **any**.

(2) Edit a custom application: Click **Edit** in the **Action** column. In the dialog box that is displayed, edit information. Click **OK**. A message indicating successful configuration is displayed.



☐	App Name	Pro
☐	2323	IP

Show No.: 10 Total Count:1

Edit App

Tip: The application name cannot be longer than 59 characters.

App Name: 2323

Protocol Type: IP

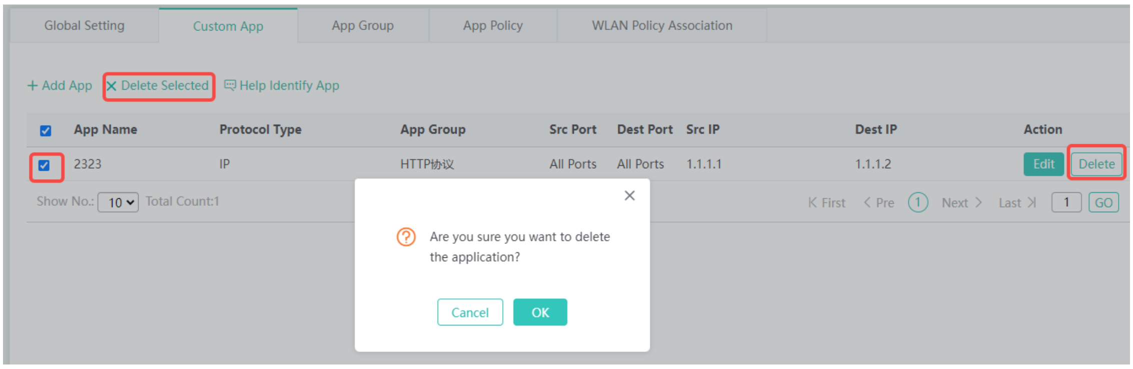
Rule: Src IP + Dest IP

App Group: ● Custom: ○ Select: HTTP协议

Src IP: Enter an 1.1.1.1

Dest IP: Enter an 1.1.1.2

(3) Delete a custom application: Click **Delete** in the **Action** column of an application. In the dialog box that is displayed, click **OK**. To delete multiple applications, select the applications to be deleted in the list, and click **Delete Selected**. In the dialog box that is displayed, click **OK**.

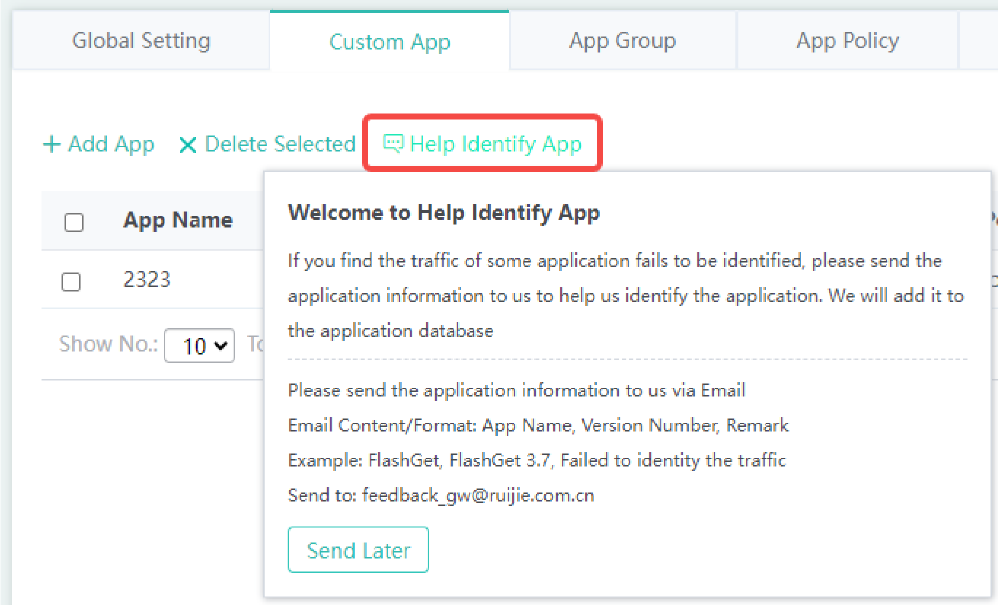


☑	App Name	Protocol Type	App Group	Src Port	Dest Port	Src IP	Dest IP	Action
☑	2323	IP	HTTP协议	All Ports	All Ports	1.1.1.1	1.1.1.2	Edit Delete

Show No.: 10 Total Count:1

Are you sure you want to delete the application?

(4) Report an unidentified application: If an application cannot be identified, click **Help Identify App** to provide feedback.



Welcome to Help Identify App

If you find the traffic of some application fails to be identified, please send the application information to us to help us identify the application. We will add it to the application database

Please send the application information to us via Email

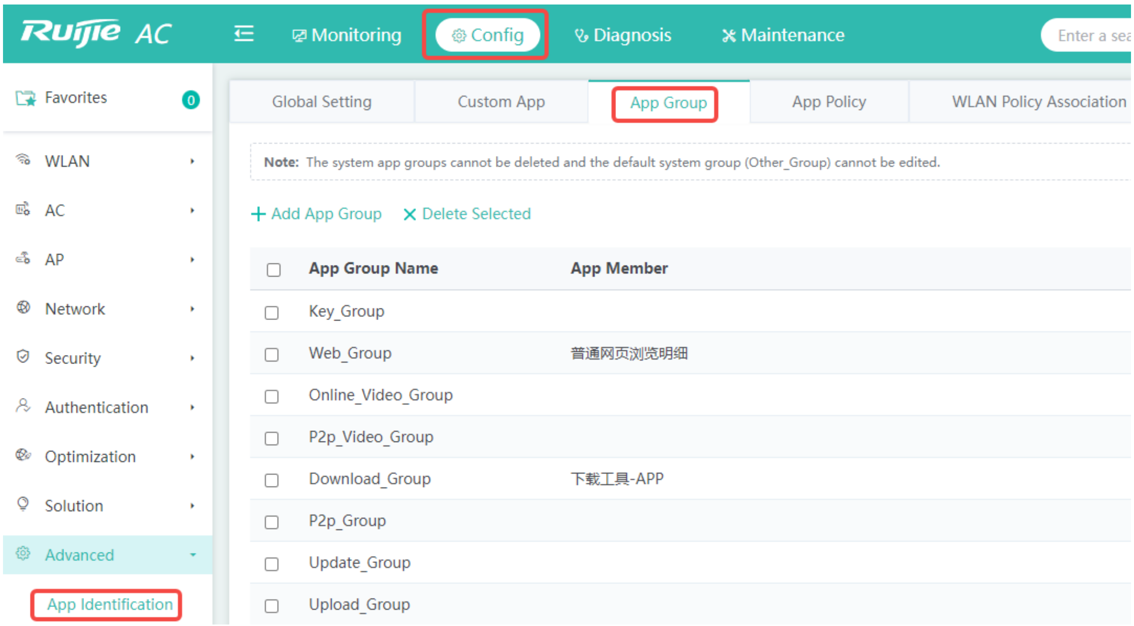
Email Content/Format: App Name, Version Number, Remark

Example: FlashGet, FlashGet 3.7, Failed to identity the traffic

Send to: feedback_gw@ruijie.com.cn

3. App Group

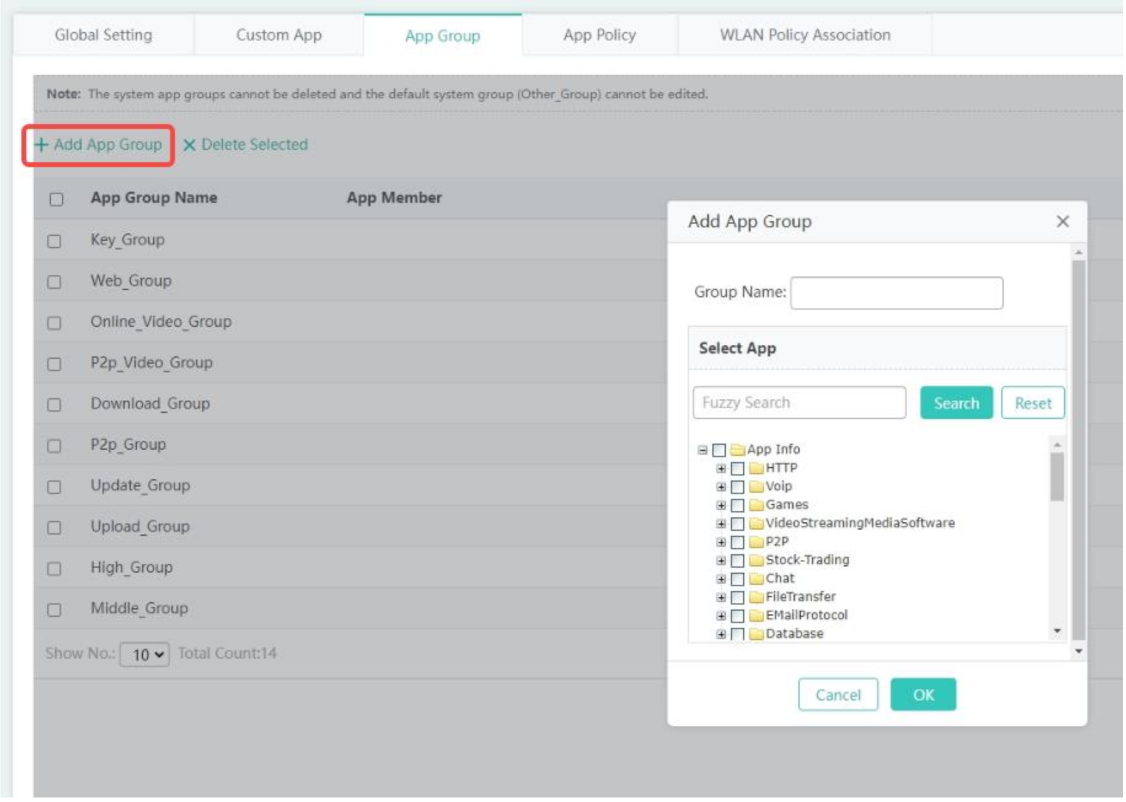
You can configure different application groups and associate configured application groups with different application policies to better control application traffic.



Note: The system app groups cannot be deleted and the default system group (Other_Group) cannot be edited.

□	App Group Name	App Member
□	Key_Group	
□	Web_Group	普通网页浏览明细
□	Online_Video_Group	
□	P2p_Video_Group	
□	Download_Group	下载工具-APP
□	P2p_Group	
□	Update_Group	
□	Upload_Group	

(1) Add an application group: Click **Add App Group**. In the dialog box that is displayed, edit information. Click **OK**. A message indicating a successful operation is displayed.



Global Setting | Custom App | App Group | App Policy | WLAN Policy Association

Note: The system app groups cannot be deleted and the default system group (Other_Group) cannot be edited.

+ Add App Group ✕ Delete Selected

□	App Group Name	App Member
□	Key_Group	
□	Web_Group	
□	Online_Video_Group	
□	P2p_Video_Group	
□	Download_Group	
□	P2p_Group	
□	Update_Group	
□	Upload_Group	
□	High_Group	
□	Middle_Group	

Show No.: 10 Total Count:14

Add App Group

Group Name:

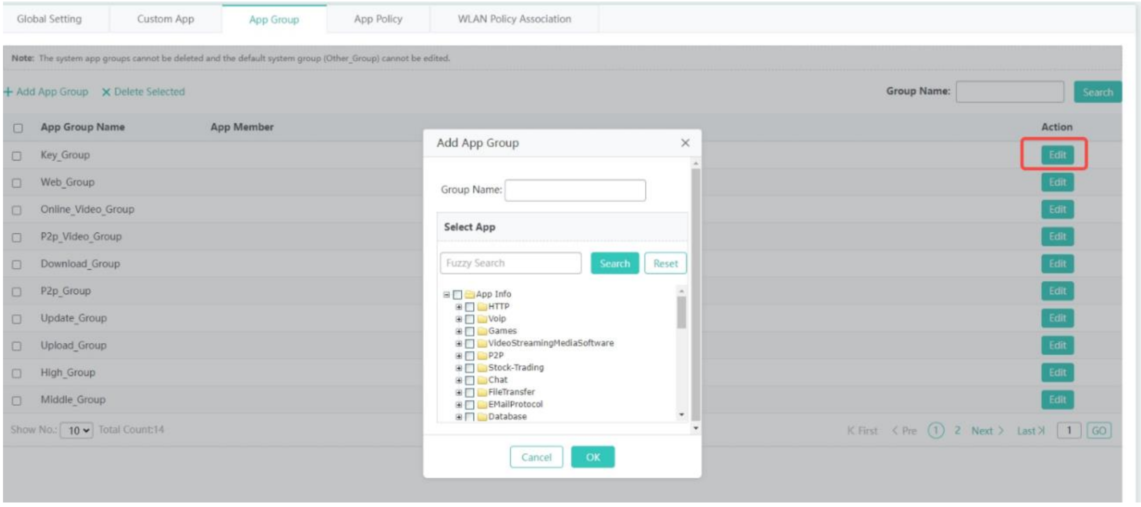
Select App

Fuzzy Search Search Reset

□ App Info
- □ HTTP
- □ Voip
- □ Games
- □ VideoStreamingMediaSoftware
- □ P2P
- □ Stock-Trading
- □ Chat
- □ FileTransfer
- □ EMailProtocol
- □ Database

Cancel OK

(2) Edit an application group: Click **Edit** in the **Action** column. In the dialog box that is displayed, edit information. Click **OK**. A message indicating a successful operation is displayed.



Global Setting | Custom App | App Group | App Policy | WLAN Policy Association

Note: The system app groups cannot be deleted and the default system group (Other_Group) cannot be edited.

+ Add App Group ✕ Delete Selected Group Name: Search

□	App Group Name	App Member	Action
□	Key_Group		Edit
□	Web_Group		Edit
□	Online_Video_Group		Edit
□	P2p_Video_Group		Edit
□	Download_Group		Edit
□	P2p_Group		Edit
□	Update_Group		Edit
□	Upload_Group		Edit
□	High_Group		Edit
□	Middle_Group		Edit

Show No.: 10 Total Count:14 K First < Pre 1 2 Next > Last >| 1 GO

Add App Group

Group Name:

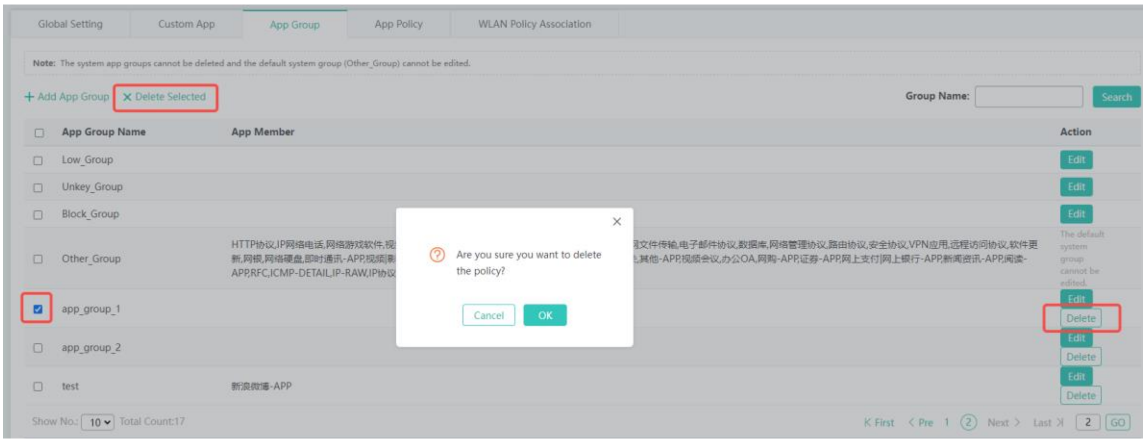
Select App

Fuzzy Search Search Reset

□ App Info
- □ HTTP
- □ Voip
- □ Games
- □ VideoStreamingMediaSoftware
- □ P2P
- □ Stock-Trading
- □ Chat
- □ FileTransfer
- □ EMailProtocol
- □ Database

Cancel OK

(3) Delete an application group: Click **Delete** in the **Action** column of an application group. In the dialog box that is displayed, click **OK**. To delete multiple application groups, select the application groups to be deleted in the list, and click **Delete Selected**. In the dialog box that is displayed, click **OK**.



Global Setting | Custom App | App Group | App Policy | WLAN Policy Association

Note: The system app groups cannot be deleted and the default system group (Other_Group) cannot be edited.

+ Add App Group ✕ Delete Selected Group Name: Search

□	App Group Name	App Member	Action
□	Low_Group		Edit
□	Unkey_Group		Edit
□	Block_Group		Edit
□	Other_Group	HTTP协议,IP网络电话,网络游戏软件,视 网文件传输,电子邮件协议,数据库,网络管理协议,路由协议,安全协议,VPN应用,远程访问协议,软件更 新,网银,网络硬盘,即时通讯-APP,视频影 其他-APP,视频会议,办公OA,网购-APP,证券-APP,网上支付|网上银行-APP,新闻资讯-APP,阅读- APP,RFC,ICMP-DETAIL,IP-RAW,IP协议	The default system group cannot be edited.
☑	app_group_1		Edit Delete
□	app_group_2		Edit Delete
□	test	新浪微博-APP	Edit Delete

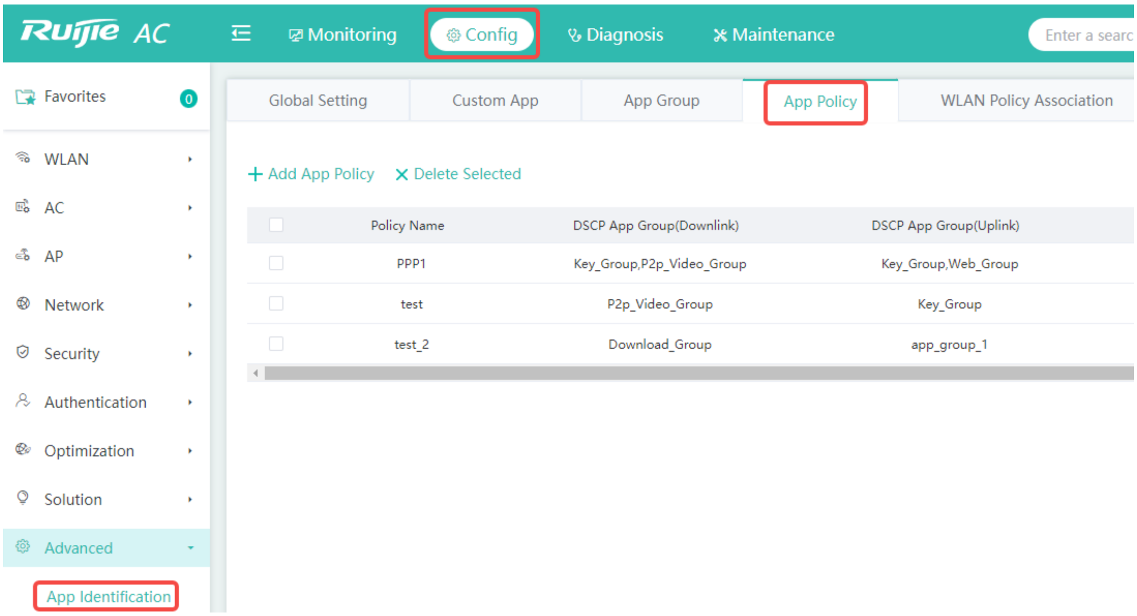
Show No.: 10 Total Count:17 K First < Pre 1 2 Next > Last >| 2 GO

Are you sure you want to delete the policy?

Cancel OK

4. App Policy

Based on the traffic features, the application identification component on the AC can identify applications and configure different Differentiated Services Code Point (DSCP) values for different applications. When a packet is sent to an AP, the Wi-Fi Multimedia (WMM) function on the AP converts the DSCP value of the packet to an 802.11e priority. Then, the AP schedules the packet based on the priority, ensuring priority-based control of different applications.



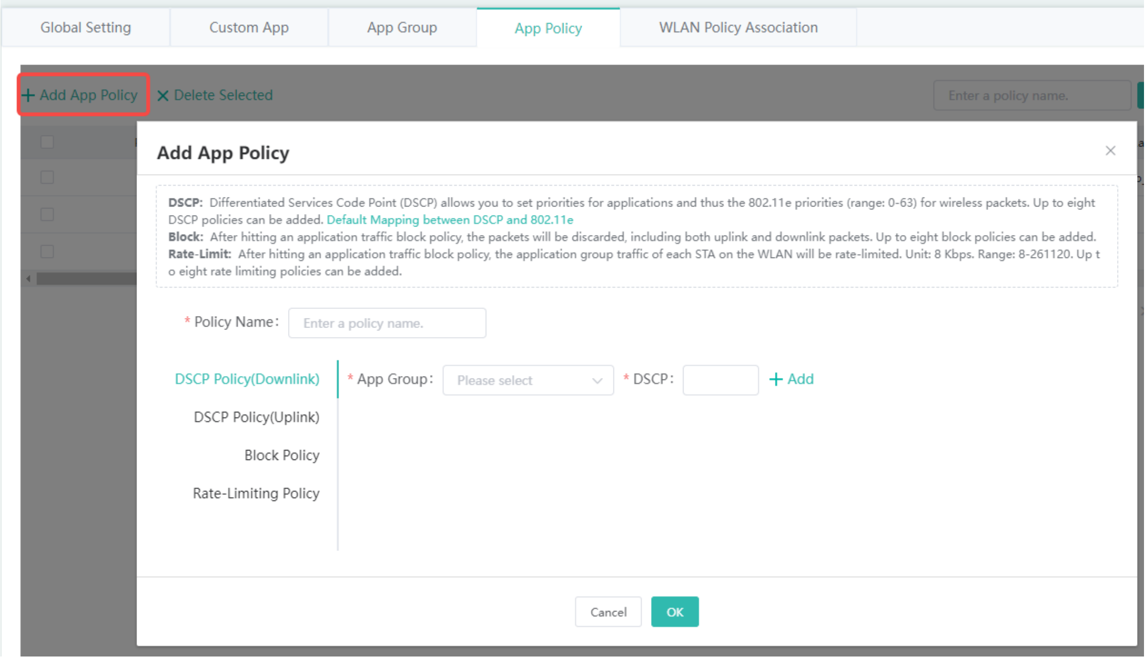
Global Setting | Custom App | App Group | App Policy | WLAN Policy Association

+ Add App Policy ✕ Delete Selected

□	Policy Name	DSCP App Group(Downlink)	DSCP App Group(Uplink)
□	PPP1	Key_Group,P2p_Video_Group	Key_Group,Web_Group
□	test	P2p_Video_Group	Key_Group
□	test_2	Download_Group	app_group_1

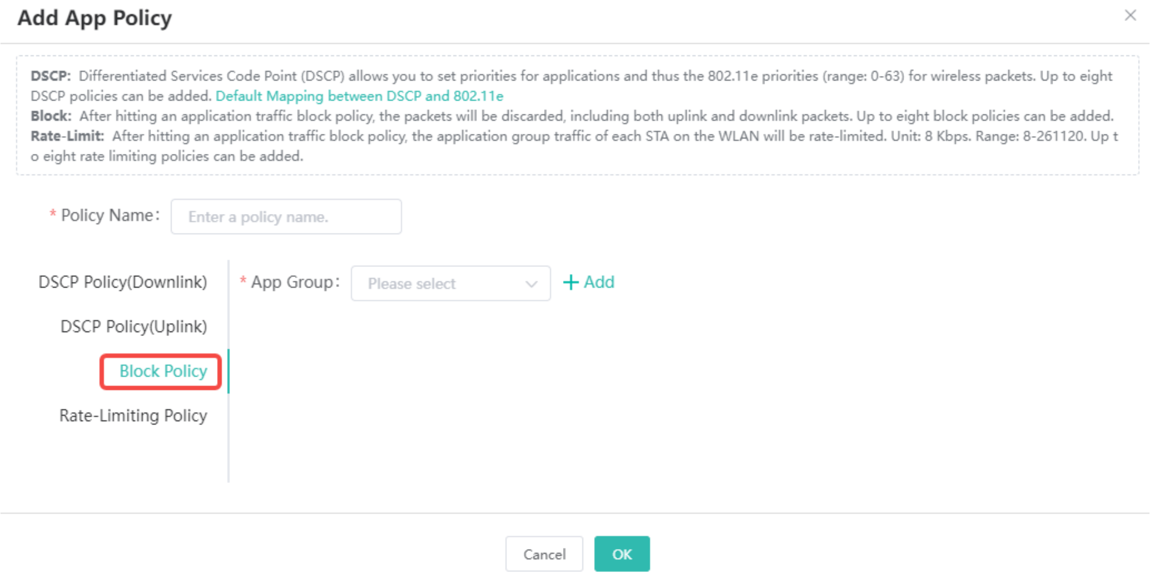
(1) Add an application policy: Click **Add App Policy**. In the dialog box that is displayed, edit policy information. Click **OK**. A message indicating a successful operation is displayed.

- **DSCP Policy**: Set priorities for applications, thereby determining 802.11e priorities for wireless packets. The DSCP value range is from 0 to 63. After configuring an application group a DSCP value, click **Add** to configure multiple DSCP policies. Up to eight DSCP policies can be configured and the application group configured for each DSCP policy must be unique.



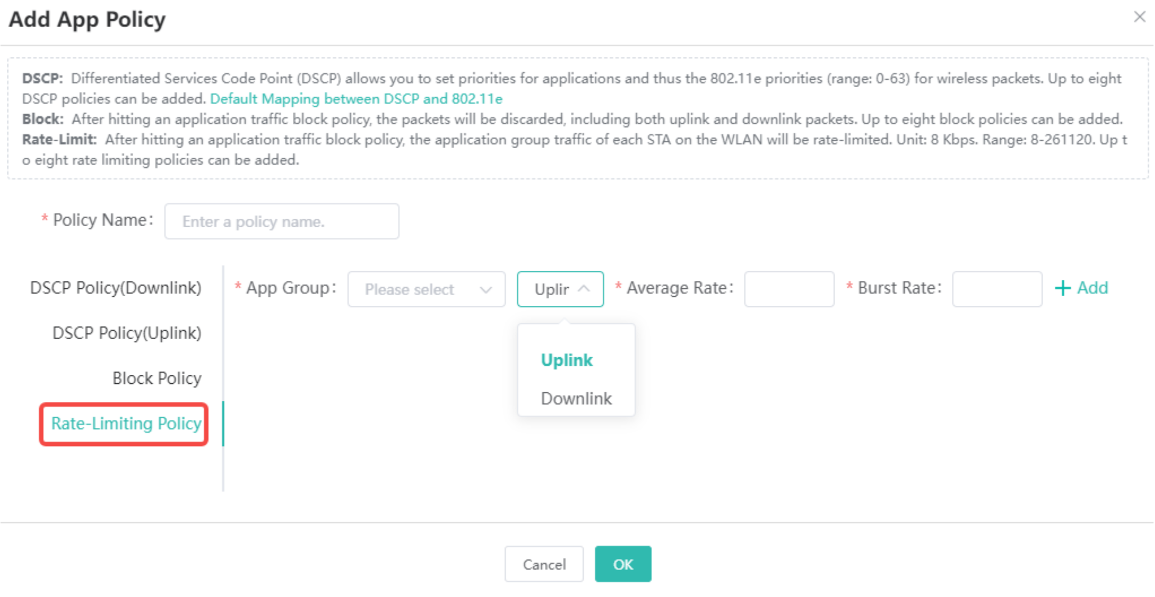
DSCP: Differentiated Services Code Point (DSCP) allows you to set priorities for applications and thus the 802.11e priorities (range: 0-63) for wireless packets. Up to eight DSCP policies can be added. Default Mapping between DSCP and 802.11e
Block: After hitting an application traffic block policy, the packets will be discarded, including both uplink and downlink packets. Up to eight block policies can be added.
Rate-Limit: After hitting an application traffic block policy, the application group traffic of each STA on the WLAN will be rate-limited. Unit: 8 Kbps. Range: 8-261120. Up t o eight rate limiting policies can be added.

- **Block Policy**: When packets hit a blocking policy, they will be discarded (including both uplink and downlink packets). After configuring an application group, click **Add** to configure more blocking policies. Up to eight blocking policies can be configured and the application group configured for each blocking policy must be unique.



DSCP: Differentiated Services Code Point (DSCP) allows you to set priorities for applications and thus the 802.11e priorities (range: 0-63) for wireless packets. Up to eight DSCP policies can be added. Default Mapping between DSCP and 802.11e
Block: After hitting an application traffic block policy, the packets will be discarded, including both uplink and downlink packets. Up to eight block policies can be added.
Rate-Limit: After hitting an application traffic block policy, the application group traffic of each STA on the WLAN will be rate-limited. Unit: 8 Kbps. Range: 8-261120. Up t o eight rate limiting policies can be added.

- **Rate-Limiting Policy**: When packets hit a rate limiting policy, the rate of application group traffic of each STA on the WLAN will be limited. The value range is from 8 to 261120, in Kbps. Specify an application group and configure the uplink or downlink rate limit, average rate limit, and burst rate limit. Then, click **Add** to configure multiple rate limiting policies. Up to eight rate limiting policies can be configured, and an uplink or downlink rate limit can be configured for each application group.

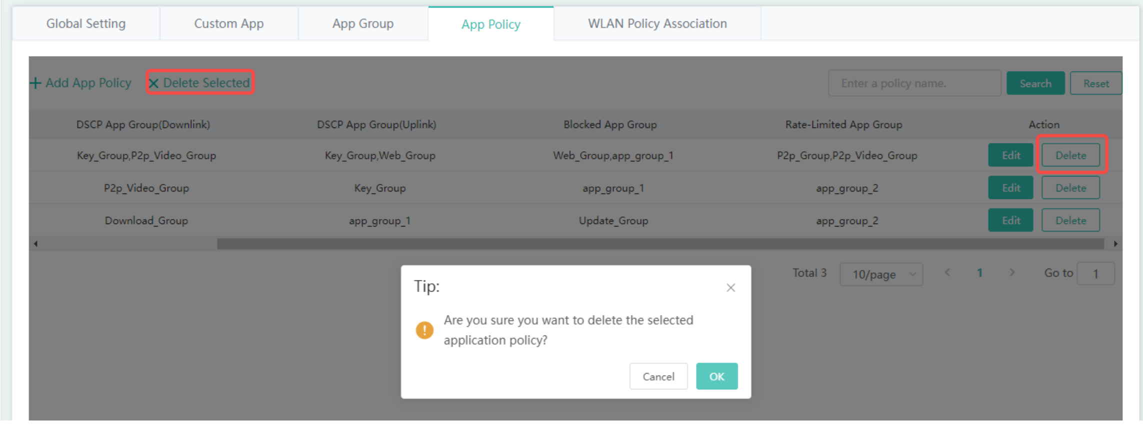


Add App Policy

DSCP: Differentiated Services Code Point (DSCP) allows you to set priorities for applications and thus the 802.11e priorities (range: 0-63) for wireless packets. Up to eight DSCP policies can be added. Default Mapping between DSCP and 802.11e
Block: After hitting an application traffic block policy, the packets will be discarded, including both uplink and downlink packets. Up to eight block policies can be added.
Rate-Limit: After hitting an application traffic block policy, the application group traffic of each STA on the WLAN will be rate-limited. Unit: 8 Kbps. Range: 8-261120. Up t o eight rate limiting policies can be added.

* Policy Name: Enter a policy name.

(2) Delete an application policy: Click **Delete** in the **Action** column of an application policy. In the dialog box that is displayed, click **OK**. To delete multiple application policies, select the application policies to be deleted in the list, and click **Delete Selected**. In the dialog box that is displayed, click **OK**.

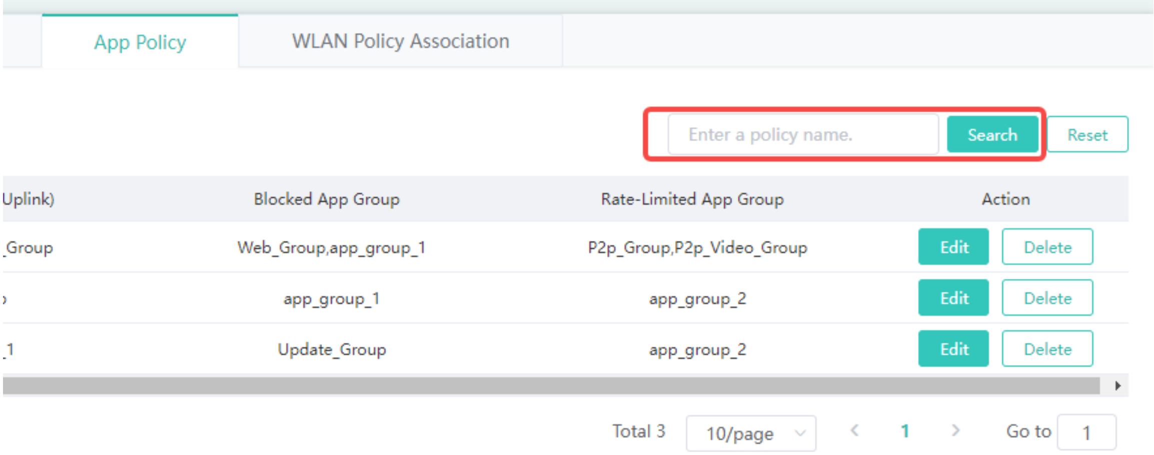


DSCP App Group(Downlink)	DSCP App Group(Uplink)	Blocked App Group	Rate-Limited App Group	Action
Key_Group,P2p_Video_Group	Key_Group,Web_Group	Web_Group,app_group_1	P2p_Group,P2p_Video_Group	Edit Delete
P2p_Video_Group	Key_Group	app_group_1	app_group_2	Edit Delete
Download_Group	app_group_1	Update_Group	app_group_2	Edit Delete

Tip:

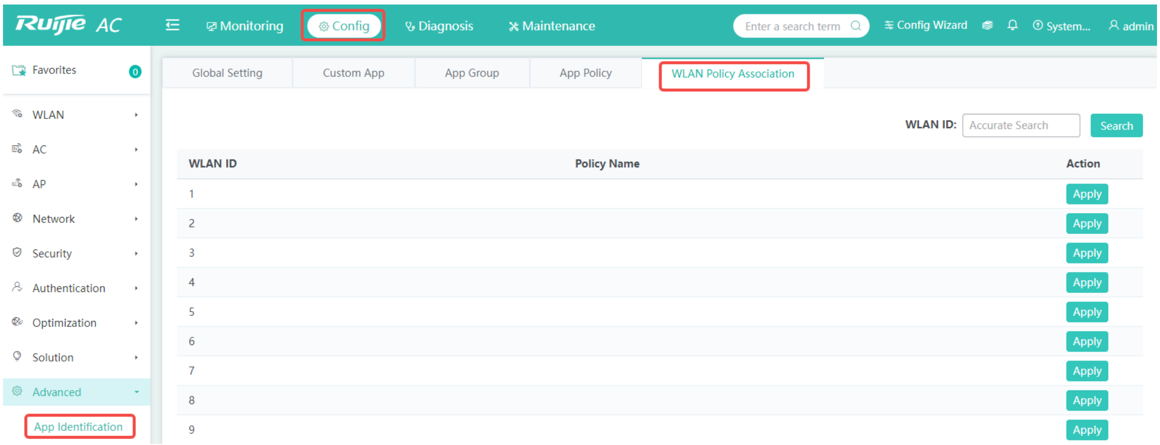
Are you sure you want to delete the selected application policy?

(3) Query an application policy based on query criteria.



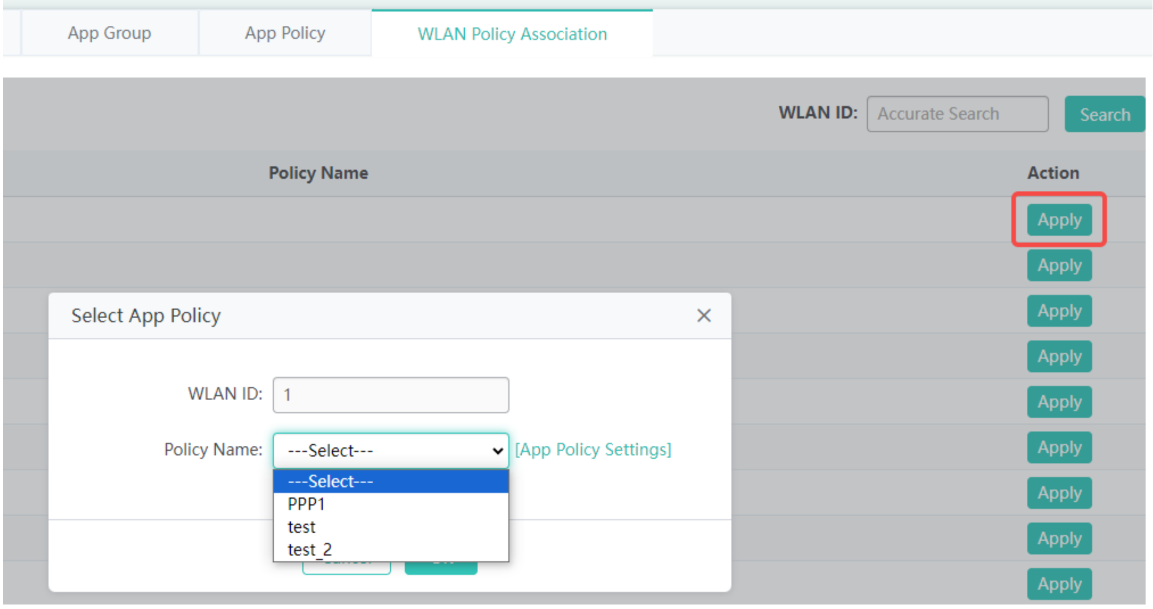
Uplink)	Blocked App Group	Rate-Limited App Group	Action
_Group	Web_Group,app_group_1	P2p_Group,P2p_Video_Group	Edit Delete
›	app_group_1	app_group_2	Edit Delete
_1	Update_Group	app_group_2	Edit Delete

5. WLAN Policy Association



WLAN ID	Policy Name	Action
1		Apply
2		Apply
3		Apply
4		Apply
5		Apply
6		Apply
7		Apply
8		Apply
9		Apply

(1) On the **WLAN Policy Association** tab page, click **Apply** in the **Action** column. In the dialog box that is displayed, select a policy name and click **OK**. A message indicating a successful operation is displayed.



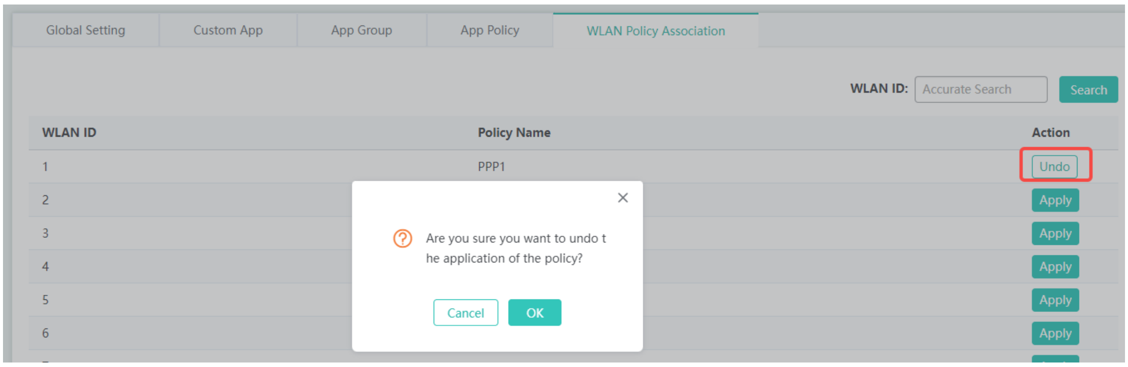
WLAN ID: 1

Policy Name: ---Select---

Note

If an application policy is associated with a WLAN, it cannot be deleted on the **App Policy** tab page.

(2) Disassociate a policy from a WLAN: Click **Undo** in the **Action** column of a WLAN. In the dialog box that is displayed, click **OK**. A message indicating a successful operation is displayed.

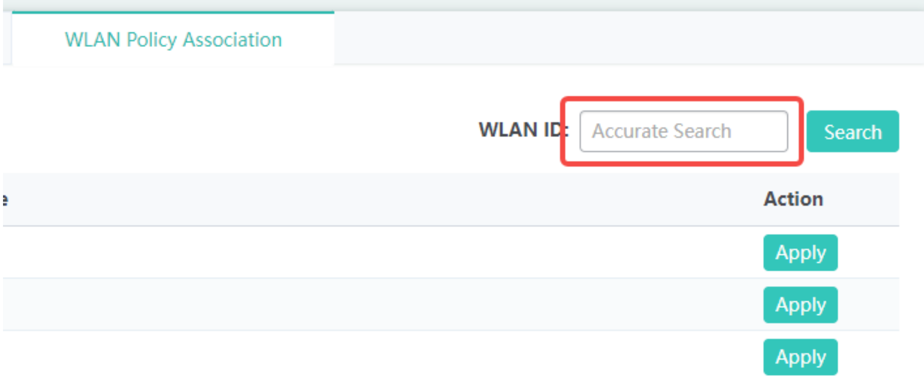


WLAN ID	Policy Name	Action
1	PPP1	Undo
2		Apply
3		Apply
4		Apply
5		Apply
6		Apply

Are you sure you want to undo t he application of the policy?

Cancel OK

(3) Query WLAN policy association: Query policies associated with WLANs based on query criteria.

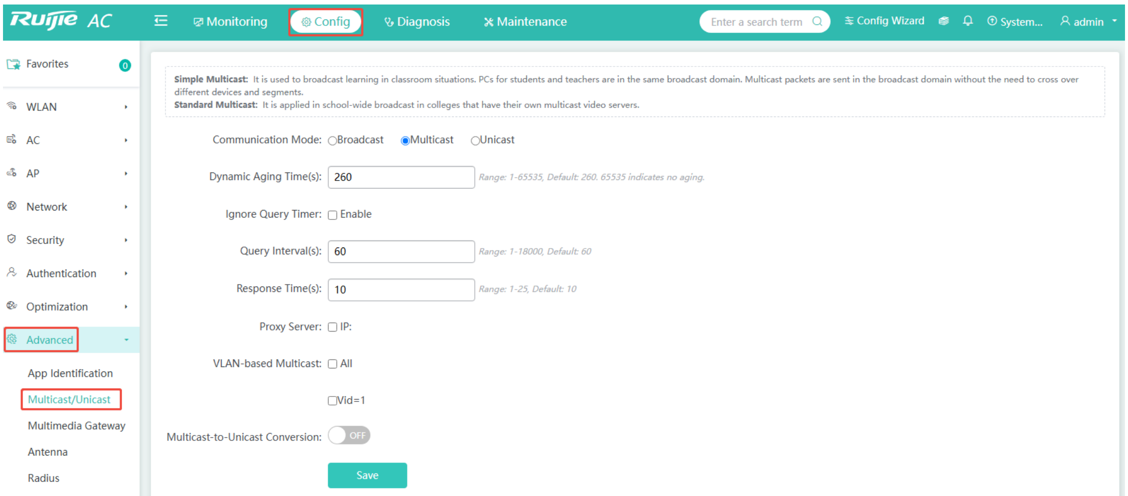


e	Action
	Apply
	Apply
	Apply

5.9.2 Multicast/Unicast

Choose **Config** > **Advanced** > **Multicast/Unicast**.

This feature is used to configure the communication mode of a device as broadcast, multicast, or unicast.



Simple Multicast: It is used to broadcast learning in classroom situations. PCs for students and teachers are in the same broadcast domain. Multicast packets are sent in the broadcast domain without the need to cross over different devices and segments.
Standard Multicast: It is applied in school-wide broadcast in colleges that have their own multicast video servers.

Communication Mode: ○Broadcast ●Multicast ○Unicast

Dynamic Aging Time(s): 260 *Range: 1-65535, Default: 260. 65535 indicates no aging.*

Ignore Query Timer: □ Enable

Query Interval(s): 60 *Range: 1-18000, Default: 60*

Response Time(s): 10 *Range: 1-25, Default: 10*

Proxy Server: □ IP:

VLAN-based Multicast: □ All

□Vid=1

Multicast-to-Unicast Conversion: OFF

Save

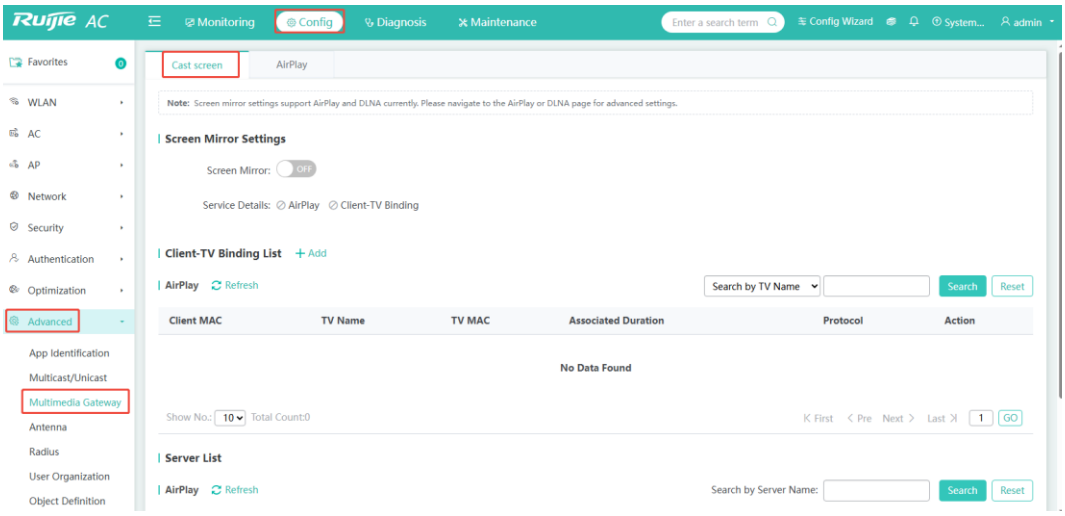
5.9.3 Multimedia Gateway

Choose **Config** > **Advanced** > **Multimedia Gateway**.

Multimedia gateway is mainly used by iOS and Android clients for screen mirroring to device servers that support AirPlay protocol, such as TV boxes.

1. Cast Screen

Accurate screen mirroring solutions can be configured conveniently. Currently, AirPlay protocols is supported. If you need more advanced and professional configuration, go to the corresponding page to configure protocols and standards.



Note: Screen mirror settings support AirPlay and DLNA currently. Please navigate to the AirPlay or DLNA page for advanced settings.

Screen Mirror Settings

Screen Mirror: OFF

Service Details: AirPlay Client-TV Binding

Client-TV Binding List + Add

AirPlay Refresh — Search by TV Name [Search] [Reset]

Client MAC	TV Name	TV MAC	Associated Duration	Protocol	Action

No Data Found

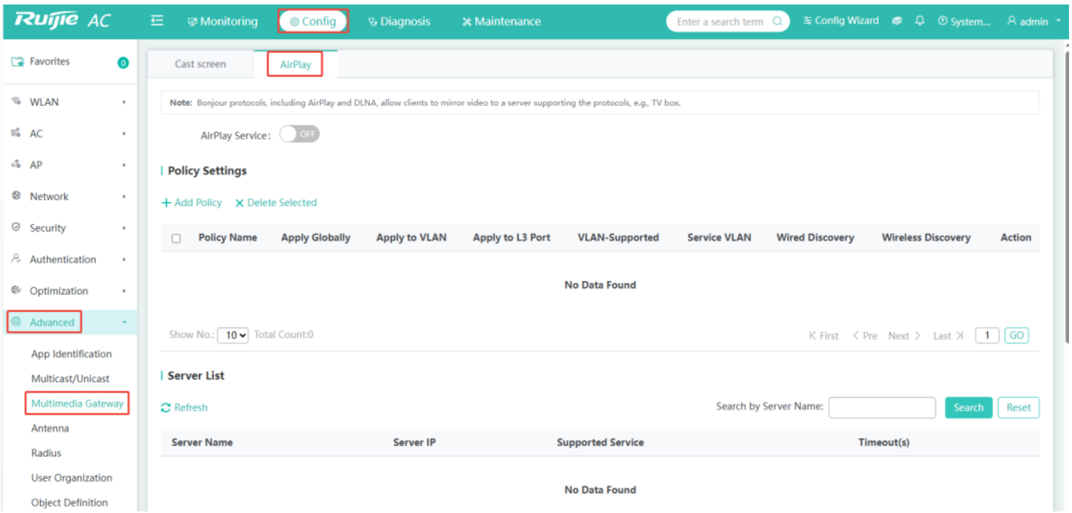
Show No.: 10 Total Count:0 — First Pre Next Last 1 GO

Server List

AirPlay Refresh — Search by Server Name: [Search] [Reset]

2. Airplay

AirPlay is a multimedia gateway protocol used for screen mirroring from mobile clients to servers that support AirPlay, such as TV boxes.



Note: Bonjour protocols, including AirPlay and DLNA, allow clients to mirror video to a server supporting the protocols, e.g., TV box.

AirPlay Service: OFF

Policy Settings

+ Add Policy × Delete Selected

□	Policy Name	Apply Globally	Apply to VLAN	Apply to L3 Port	VLAN-Supported	Service VLAN	Wired Discovery	Wireless Discovery	Action

No Data Found

Show No.: 10 Total Count:0 — First Pre Next Last 1 GO

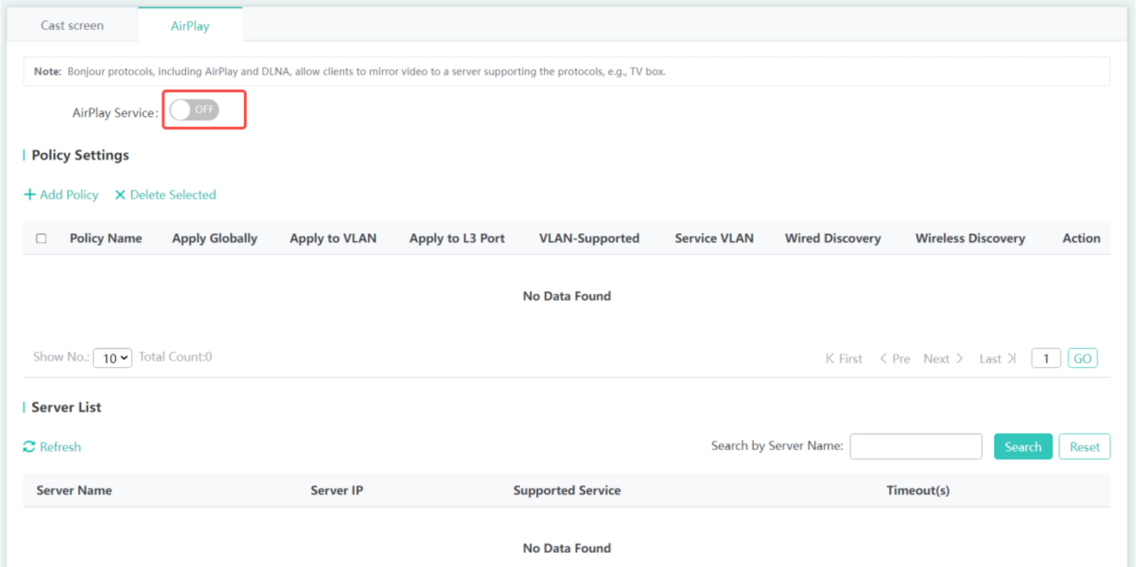
Server List

Refresh — Search by Server Name: [Search] [Reset]

Server Name	Server IP	Supported Service	Timeout(s)

No Data Found

(1) Enable **AirPlay Service**: Enable the AirPlay protocol for the multimedia gateway as required. When the protocol is disabled, the corresponding policy will not take effect. The policy corresponding to the enabled protocol is displayed.



Cast screen AirPlay

Note: Bonjour protocols, including AirPlay and DLNA, allow clients to mirror video to a server supporting the protocols, e.g., TV box.

AirPlay Service: OFF

Policy Settings

+ Add Policy ✕ Delete Selected

□	Policy Name	Apply Globally	Apply to VLAN	Apply to L3 Port	VLAN-Supported	Service VLAN	Wired Discovery	Wireless Discovery	Action

No Data Found

Show No.: 10 Total Count:0 K First < Pre Next > Last >| 1 GO

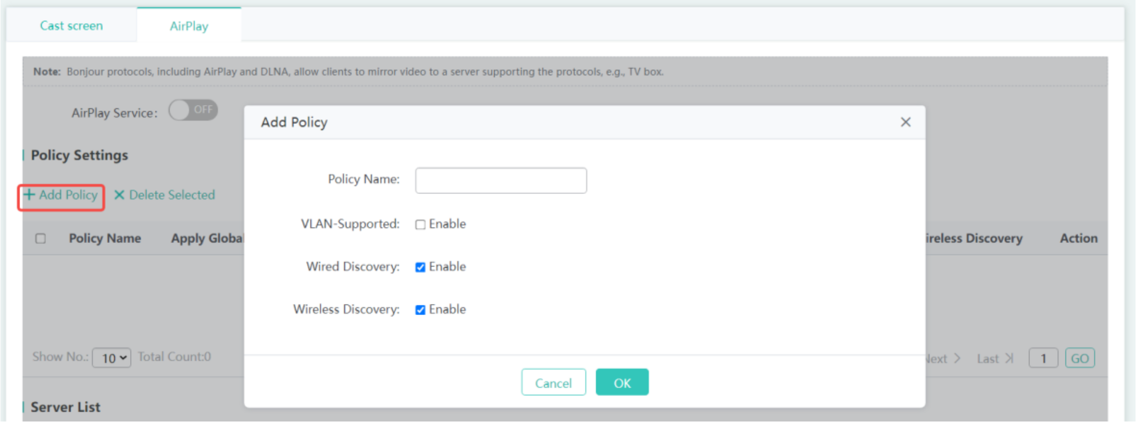
Server List

Refresh Search by Server Name: Search Reset

Server Name	Server IP	Supported Service	Timeout(s)

No Data Found

(2) Add a policy: Choose **Policy Settings** > **Add Policy**. Configure the information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added policy is displayed in the policy list.



Add Policy

Policy Name:

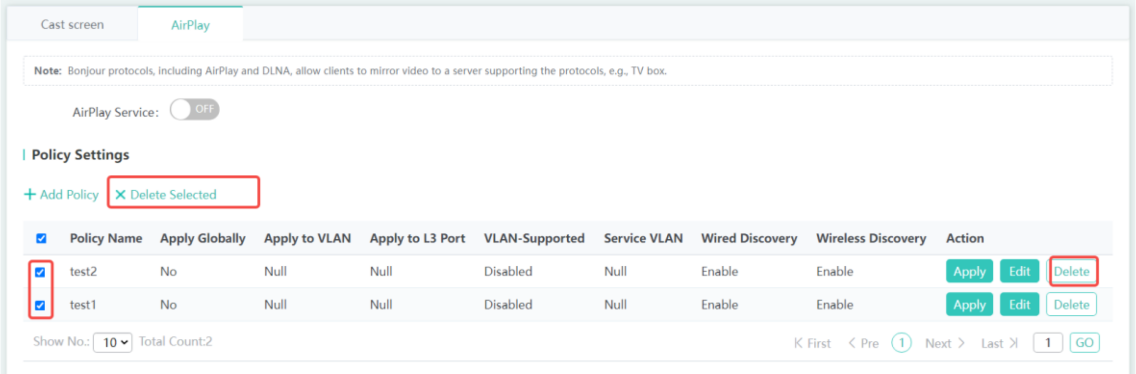
VLAN-Supported: □ Enable

Wired Discovery: ☑ Enable

Wireless Discovery: ☑ Enable

Cancel OK

(3) Delete a policy: Click **Delete** of a specified policy in the list. The confirmation dialog box pops up. Click **OK** to finish the operation. To delete multiple policies, select policies to be deleted from the list. Click **Delete Selected**. The confirmation dialog box pops up. Click **OK** to finish the operation.



Cast screen AirPlay

Note: Bonjour protocols, including AirPlay and DLNA, allow clients to mirror video to a server supporting the protocols, e.g., TV box.

AirPlay Service: OFF

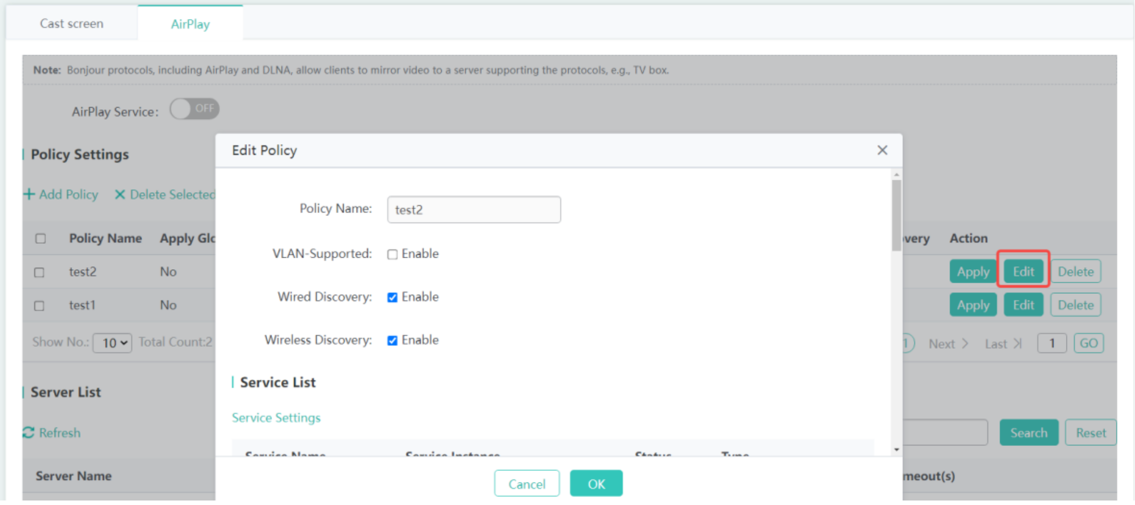
Policy Settings

+ Add Policy ✕ Delete Selected

☑	Policy Name	Apply Globally	Apply to VLAN	Apply to L3 Port	VLAN-Supported	Service VLAN	Wired Discovery	Wireless Discovery	Action
☑	test2	No	Null	Null	Disabled	Null	Enable	Enable	Apply Edit Delete
☑	test1	No	Null	Null	Disabled	Null	Enable	Enable	Apply Edit Delete

Show No.: 10 Total Count:2 K First < Pre 1 Next > Last >| 1 GO

(4) Edit a policy: Click **Edit** of a specified policy in the list. The pop-up dialog box displays the information about the policy. Edit the information. Click **OK**. A message indicating the configuration has been saved is displayed.



Note: Bonjour protocols, including AirPlay and DLNA, allow clients to mirror video to a server supporting the protocols, e.g., TV box.

AirPlay Service: OFF

□	Policy Name	Apply Glo
□	test2	No
□	test1	No

Show No.: 10 Total Count:2

Edit Policy

Policy Name: test2

VLAN-Supported: □ Enable

Wired Discovery: ☑ Enable

Wireless Discovery: ☑ Enable

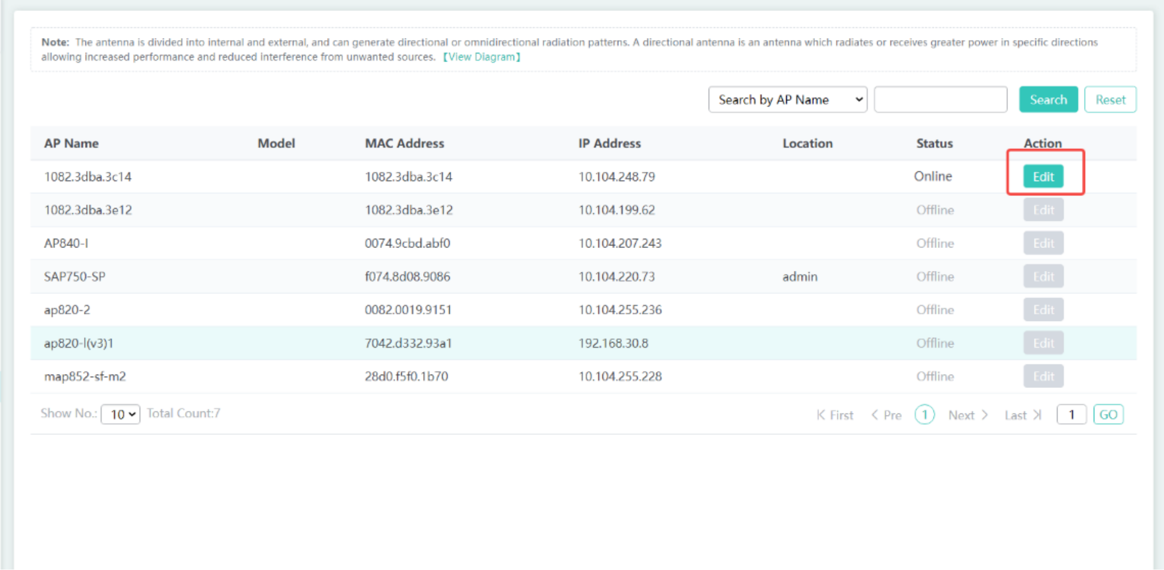
Service List

5.9.4 Antenna type and gain

Choose **Config** > **Advanced** > **Antenna**.

RF antenna types fall into built-in and external antennas, and the radiation patterns fall into directional and omnidirectional. Directional antennas radiate the signal within a certain angle range. The radiation range is like a cone.

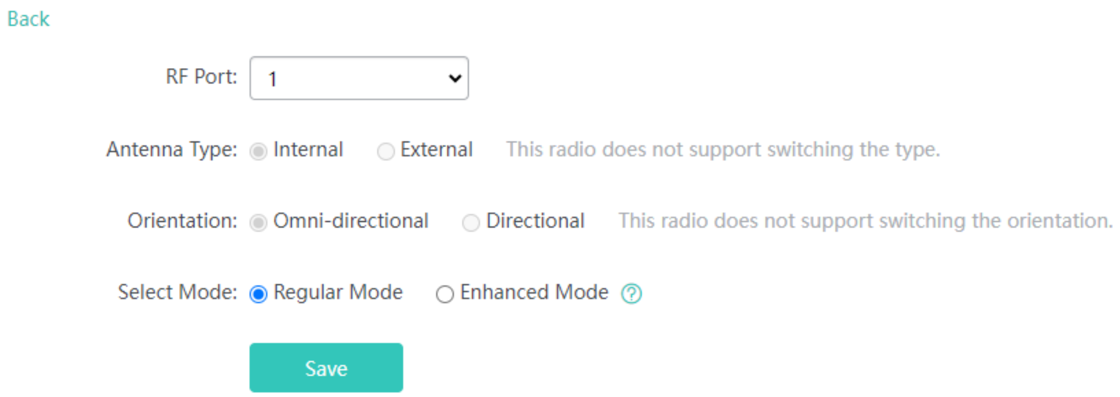
Click **Edit** in the AP list to access the antenna setting page. Whether an RF connector supports type, radiation pattern, or mode switchover is determined by the AP capability. If an RF connector does not support type, radiation pattern, or mode switchover, the corresponding message is displayed on the web UI.



Note: The antenna is divided into internal and external, and can generate directional or omnidirectional radiation patterns. A directional antenna is an antenna which radiates or receives greater power in specific directions allowing increased performance and reduced interference from unwanted sources. 【View Diagram】

AP Name	Model	MAC Address	IP Address	Location	Status	Action
1082.3dba.3c14		1082.3dba.3c14	10.104.248.79		Online	Edit
1082.3dba.3e12		1082.3dba.3e12	10.104.199.62		Offline	Edit
AP840-I		0074.9cbd.abf0	10.104.207.243		Offline	Edit
SAP750-SP		f074.8d08.9086	10.104.220.73	admin	Offline	Edit
ap820-2		0082.0019.9151	10.104.255.236		Offline	Edit
ap820-I(v3)1		7042.d332.93a1	192.168.30.8		Offline	Edit
map852-sf-m2		28d0.f5f0.1b70	10.104.255.228		Offline	Edit

Show No.: 10 Total Count:7



Back

RF Port: 1

Antenna Type: ◉ Internal ○ External This radio does not support switching the type.

Orientation: ◉ Omni-directional ○ Directional This radio does not support switching the orientation.

Select Mode: ◉ Regular Mode ○ Enhanced Mode

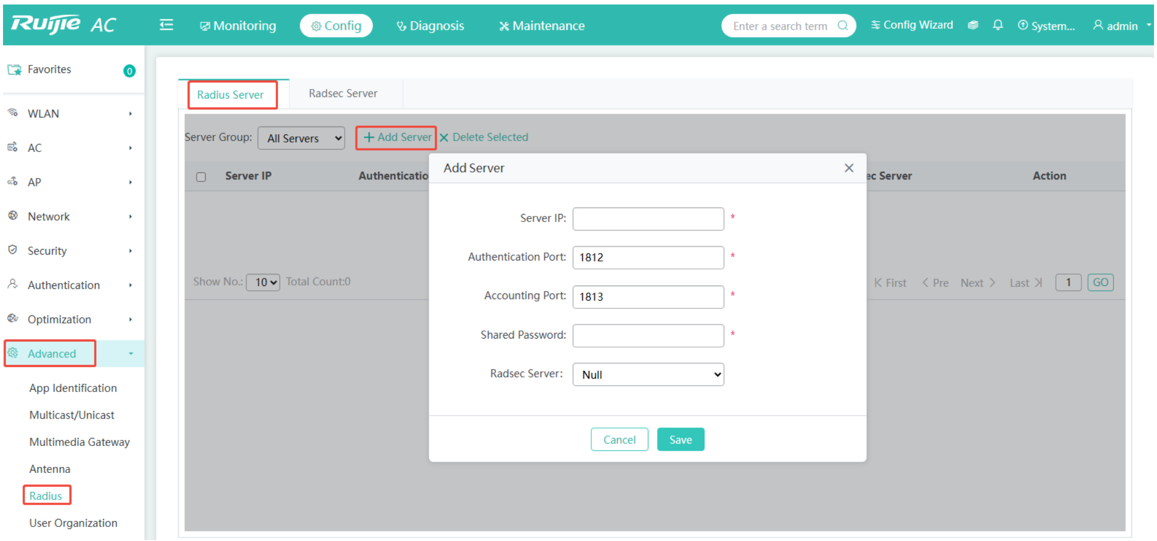
5.9.5 RADIUS

Choose **Config** > **Advanced** > **Radius**.

1. Radius Server

The Remote Authentication Dial-In User Service (RADIUS) server conducts identity authentication and accounting on access users to protect network security and facilitate management for network administrators.

(1) Add a server: Click **Add Server**. Set fields and click **Save**. A message indicating the configuration has been saved is displayed.



Server Group: All Servers

Show No.: 10 Total Count:0

Add Server

Server IP: *

Authentication Port: 1812 *

Accounting Port: 1813 *

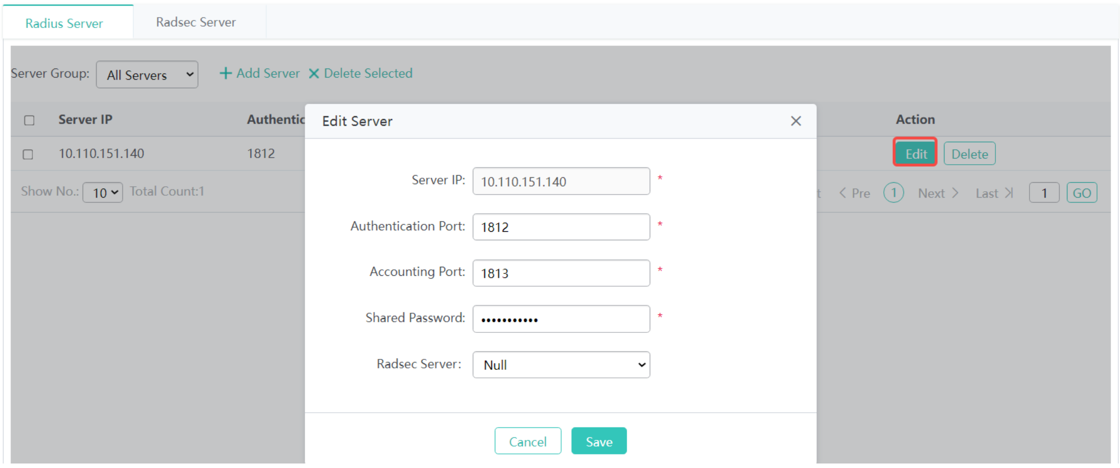
Shared Password: *

Radsec Server: Null

Parameter	Description
Server IP	Indicates the IP address of a RADIUS server.
Authentication Port	Indicates the UDP port ID for RADIUS authentication. The value range is from 0 to 65,535. **0** indicates that the server does not perform identity authentication.
Accounting Port	Indicates the UDP port ID for RADIUS accounting. The value range is from 0 to 65,535. **0** indicates that the server does not perform accounting.

Shared Password	Indicates the shared key for the communication between the network access server (router) and the RADIUS server.
Radsec Server	(Optional) Indicates the ID of the RadSec server, to which traffic is redirected from the RADIUS server. **Note** This field is not displayed if the device does not support the RadSec function.

(2) Edit a server: Click **Edit** for an existing server. Edit the parameter values. Click **Save**.



Server Group: All Servers

□	Server IP	Authentic
□	10.110.151.140	1812

Show No.: 10 Total Count:1

Edit Server

Server IP: 10.110.151.140 *

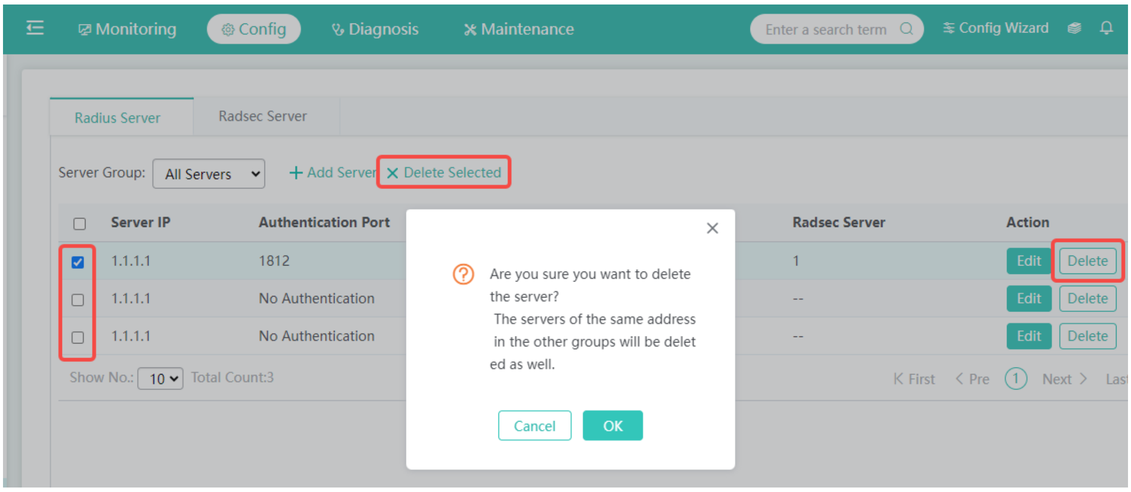
Authentication Port: 1812 *

Accounting Port: 1813 *

Shared Password: ••••••••••• *

Radsec Server: Null

(3) Delete a server: Click **Delete** in the **Action** column of a server. In the dialog box that is displayed, click **OK**. To delete multiple servers, select the servers to be deleted in the list, and click **Delete Selected**. In the dialog box that is displayed, click **OK**.



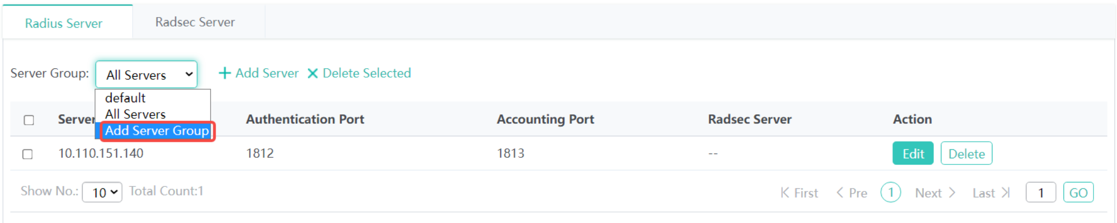
Server Group: All Servers

□	Server IP	Authentication Port	Radsec Server	Action
☑	1.1.1.1	1812	1	Edit Delete
□	1.1.1.1	No Authentication	--	Edit Delete
□	1.1.1.1	No Authentication	--	Edit Delete

Show No.: 10 Total Count:3

Are you sure you want to delete the server?
The servers of the same address in the other groups will be deleted as well.

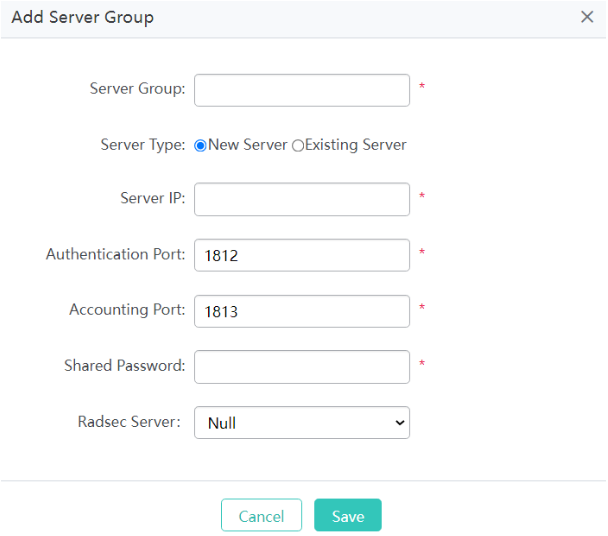
(4) Add a server group: Click the **Server Group** drop-down list and select **Add Server Group**. The **Add Server Group** dialog box pops up. If you select **New Server**, one server group and one server will be added and the server belongs to the server group. If you select **Existing Server**, an existing server will be added to the server group.



Server Group: All Servers

□	Server IP	Authentication Port	Accounting Port	Radsec Server	Action
□	10.110.151.140	1812	1813	--	Edit Delete

Show No.: 10 Total Count:1



Server Group: *

Server Type: ● New Server ○ Existing Server

Server IP: *

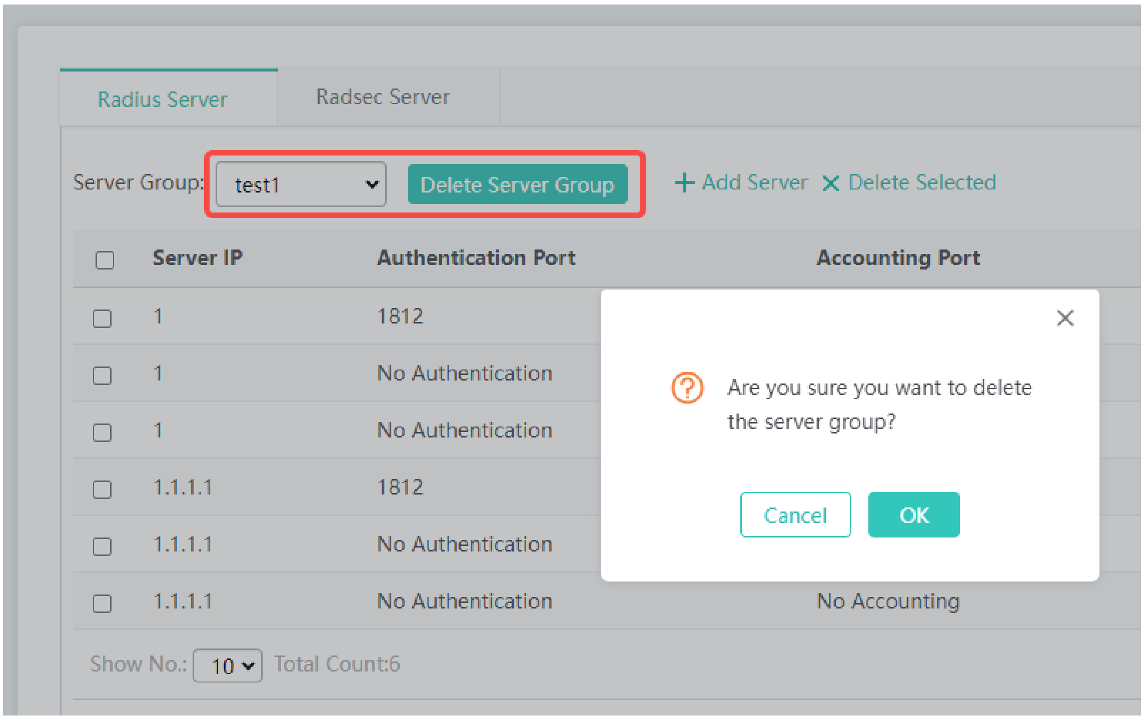
Authentication Port: 1812 *

Accounting Port: 1813 *

Shared Password: *

Radsec Server: Null

(5) Delete a server group: Select a server group to be deleted and click **Delete Server Group**. In the dialog box that is displayed, click **OK**.



Server Group: test1

□	Server IP	Authentication Port	Accounting Port
□	1	1812	
□	1	No Authentication	
□	1	No Authentication	
□	1.1.1.1	1812	
□	1.1.1.1	No Authentication	
□	1.1.1.1	No Authentication	No Accounting

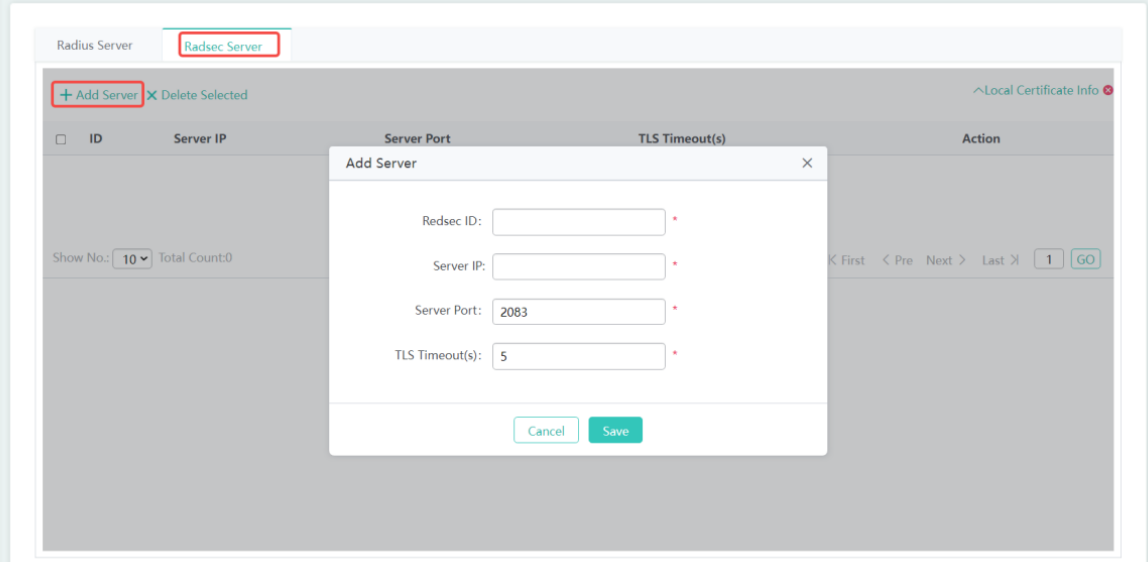
Show No.: 10 Total Count:6

Are you sure you want to delete the server group?

2. RadSec Server

RadSec provides secure communication for RADIUS requests by using the Transport Layer Security (TLS) protocol and allows RADIUS authentication, authorization, and accounting data to be securely transmitted over untrusted networks.

(1) Add a server: Click **Add Server**. Set fields and click **Save**. A message indicating the configuration has been saved is displayed.



Redsec ID: *

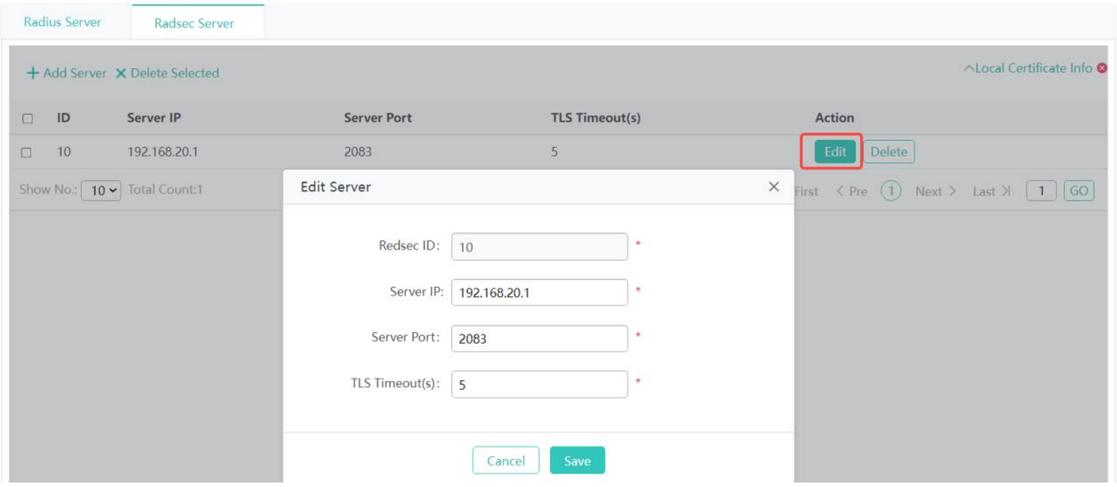
Server IP: *

Server Port: 2083 *

TLS Timeout(s): 5 *

Parameter	Description
Radsec ID	Indicates the unique ID of a RadSec server. The value is an integer in the range from 1 to 255.
Server IP	Indicates the IP address of the RadSec server.
Server Port	Specifies the port ID of the RadSec server. The value range is from 1 to 65,535. The default value is **2,083**.
TLS Timeout(s)	Specifies the TLS connection timeout. The value range is from 1 to 1,000. The default value is **5**.

(2) Edit a server: Click **Edit** behind a specified server. Modify the parameter values and click **Save**.



□	ID	Server IP	Server Port	TLS Timeout(s)	Action
□	10	192.168.20.1	2083	5	Edit Delete

Show No.: 10 Total Count:1

First < Pre 1 Next > Last 1 GO

Edit Server

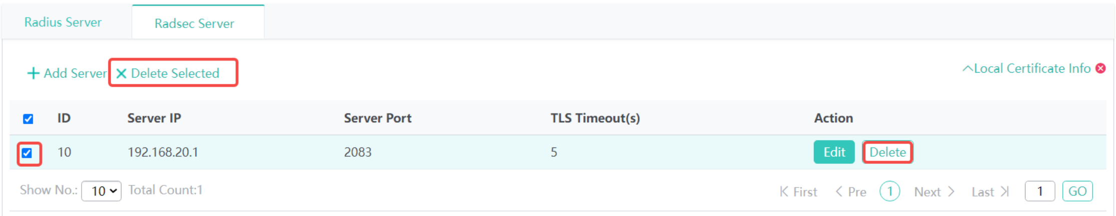
Redsec ID: 10 *

Server IP: 192.168.20.1 *

Server Port: 2083 *

TLS Timeout(s): 5 *

(3) Delete a server: Click **Delete** behind a specified server. If you need to delete multiple servers, select the servers to be deleted and click **Deleted Selected** to batch delete them.

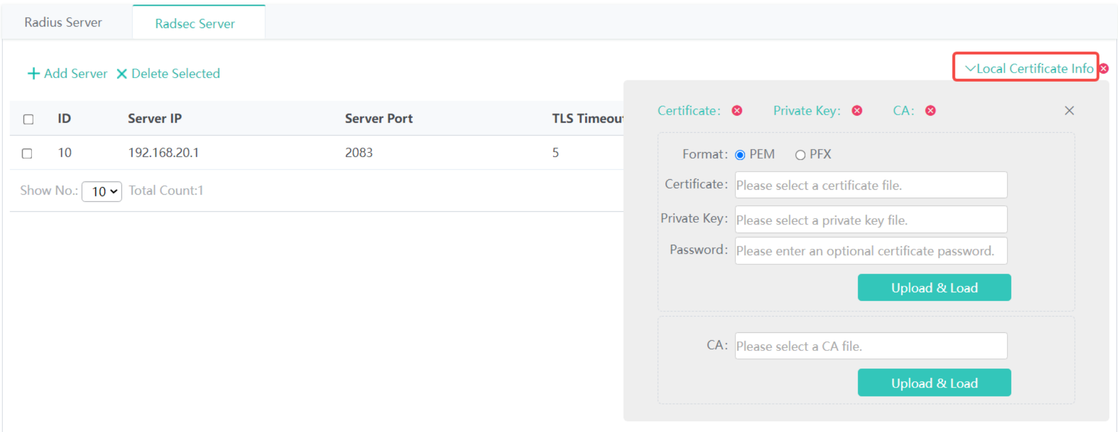


☑	ID	Server IP	Server Port	TLS Timeout(s)	Action
☑	10	192.168.20.1	2083	5	Edit Delete

Show No.: 10 Total Count:1

First < Pre 1 Next > Last 1 GO

(4) Local certificate management: Click **Local Certificate Info**. The local certificate management dialog box pops up. The icon on the right of **Local Certificate Info** shows the certificate loading status. Select a certificate file and private key file. Enter the certificate password (if any). Click **Upload & Load**. A message is displayed, indicating that the certificate is loaded successfully. The PEM and PFX formats are supported. If the certificate file does not contain CA information, select a CA file and click **Upload & Load**.



□	ID	Server IP	Server Port	TLS Timeou
□	10	192.168.20.1	2083	5

Show No.: 10 Total Count:1

Certificate: ⊗ Private Key: ⊗ CA: ⊗

Format: ● PEM ○ PFX

Certificate: Please select a certificate file.

Private Key: Please select a private key file.

Password: Please enter an optional certificate password.

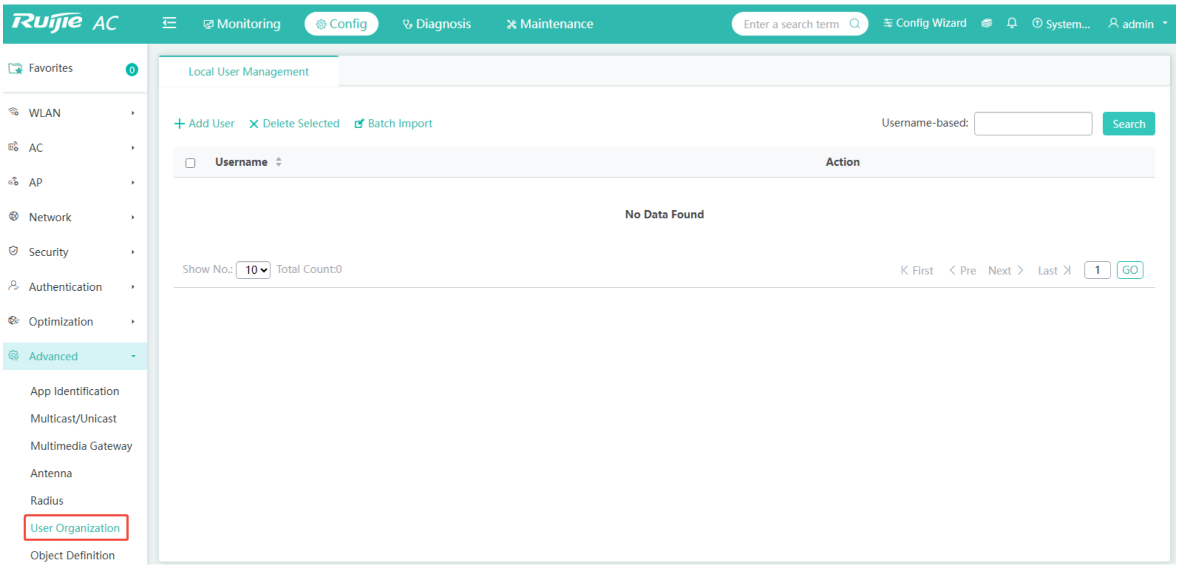
CA: Please select a CA file.

5.9.6 User Organization

Choose **Config** > **Advanced** > **User Organization**.

1. Local User Management

If the authentication server is set to local authentication on the **Configure** > **WLAN** > **Add WiFi** page, or **iPortal Authentication** is configured on the **Config** > **Authentication** > **Web Auth** page, you can view and manage local accounts on the **Local User Management** page.

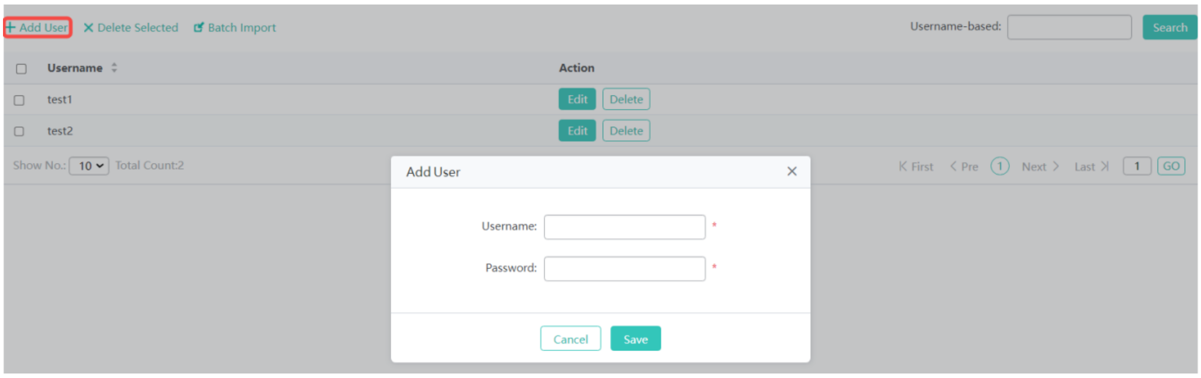


□ Username	Action
No Data Found	

Show No.: 10 Total Count:0

Adding a User

Click **Add User** to add the username and password of a local user. You can also click **Batch Import** to import users in a batch. In the dialog box that is displayed, click **Download Template**. Enter usernames and passwords in the template, and then import it.



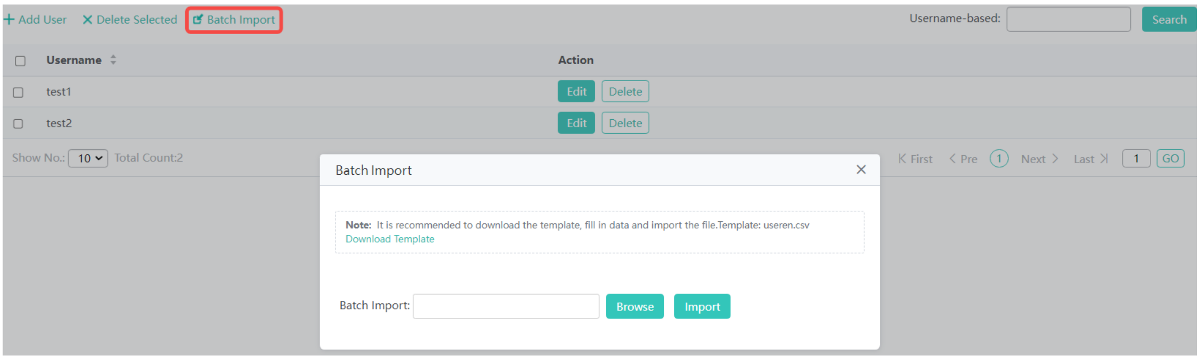
□ Username	Action
□ test1	Edit Delete
□ test2	Edit Delete

Show No.: 10 Total Count:2

Add User

Username: *

Password: *



□ Username	Action
□ test1	Edit Delete
□ test2	Edit Delete

Show No.: 10 Total Count:2

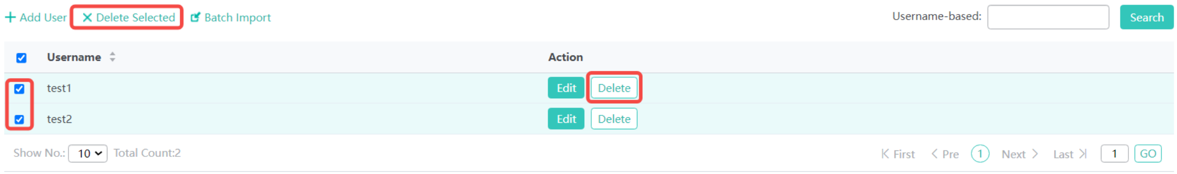
Batch Import

Note: It is recommended to download the template, fill in data and import the file.Template: useren.csv
Download Template

Batch Import:

Deleting a User

- Deleting a user: Select the user to be deleted and click **Delete** in the **Action** column. In the displayed dialog box, click **OK**.
- Batch deleting users: Select users to be deleted in the list and click **Delete Selected**. In the displayed dialog box, click **OK**.



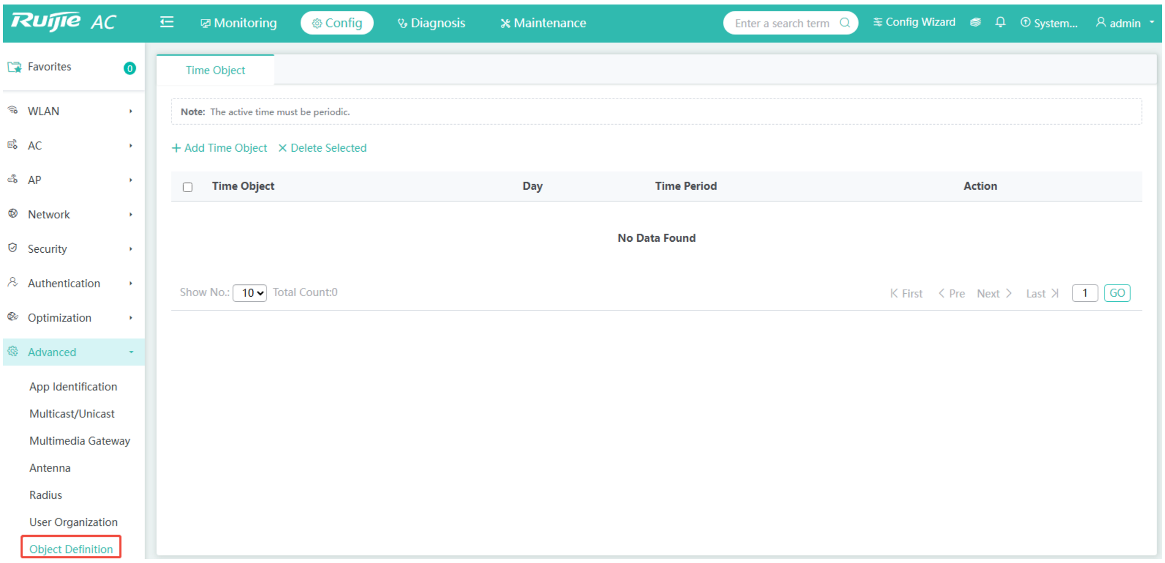
☑	Username	Action
☑	test1	Edit Delete
☑	test2	Edit Delete

5.9.7 Object Definition

Choose **Config** > **Advanced** > **Time Object**.

1. Time Object

Some functions can run based on time. For example, after an effective time range is set for an ACL, the ACL takes effect in the specified time range.

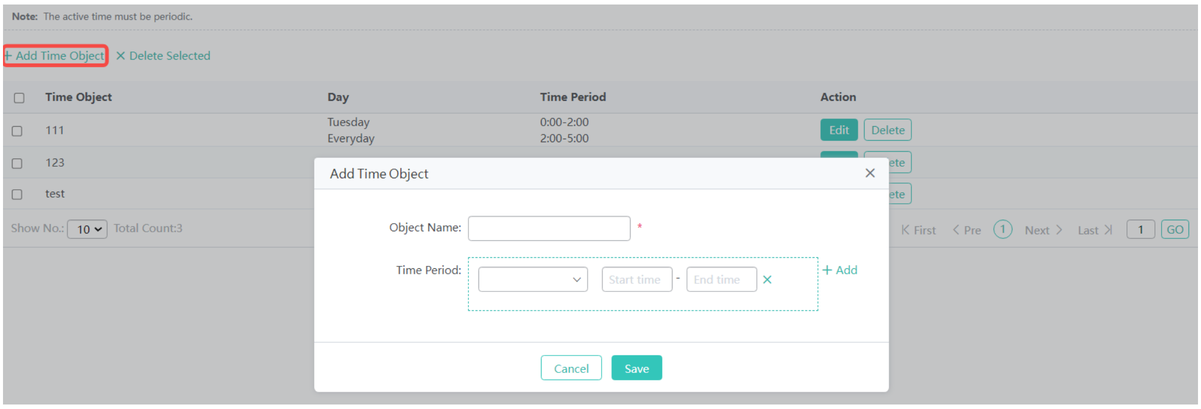


Note: The active time must be periodic.

□	Time Object	Day	Time Period	Action

No Data Found

(1) Add a time object: Click **Add Time Object**. Configure the time object information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed.



Note: The active time must be periodic.

□	Time Object	Day	Time Period	Action
□	111	Tuesday Everyday	0:00-2:00 2:00-5:00	Edit Delete
□	123			
□	test			

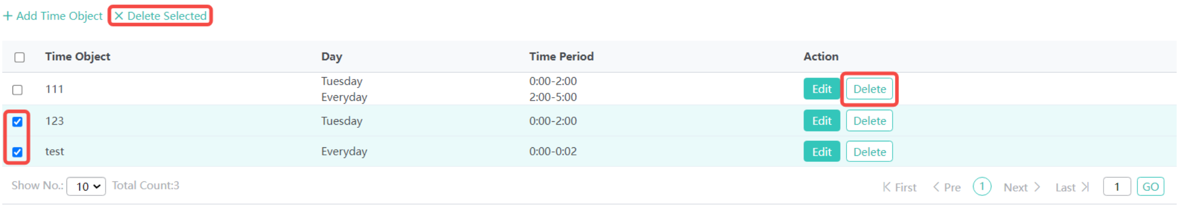
Show No.: 10 Total Count:3

Add Time Object

Object Name: *

Time Period: Start time - End time ×

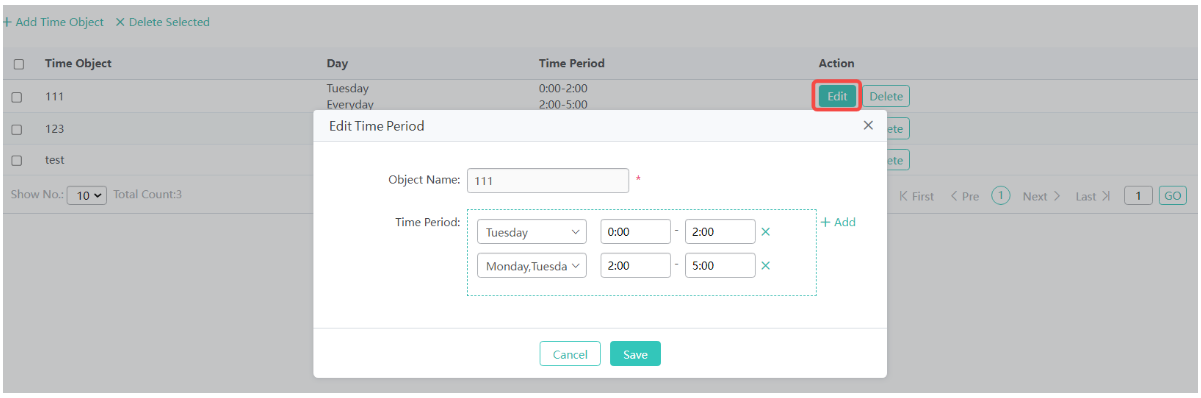
(2) Delete a time object: Click **Delete** behind a specified time object in the list. The confirmation dialog box pops up. Click **OK** to finish the operation. To delete multiple time objects, select time objects to be deleted in the list. Click **Delete Selected**. The confirmation dialog box pops up. Click **OK** to finish the operation.



□	Time Object	Day	Time Period	Action
□	111	Tuesday Everyday	0:00-2:00 2:00-5:00	Edit Delete
☑	123	Tuesday	0:00-2:00	Edit Delete
☑	test	Everyday	0:00-0:02	Edit Delete

Show No.: 10 Total Count:3

(3) Edit a time object: Click **Edit** behind a specified time object in the list. The pop-up dialog box displays the information about the time object. Edit the information. Click **OK**. A message indicating the configuration has been saved is displayed.



□	Time Object	Day	Time Period	Action
□	111	Tuesday Everyday	0:00-2:00 2:00-5:00	Edit Delete
□	123			
□	test			

Show No.: 10 Total Count:3

Edit Time Period

Object Name: 111 *

Time Period: Tuesday 0:00 - 2:00 ×
Monday,Tuesda 2:00 - 5:00 ×

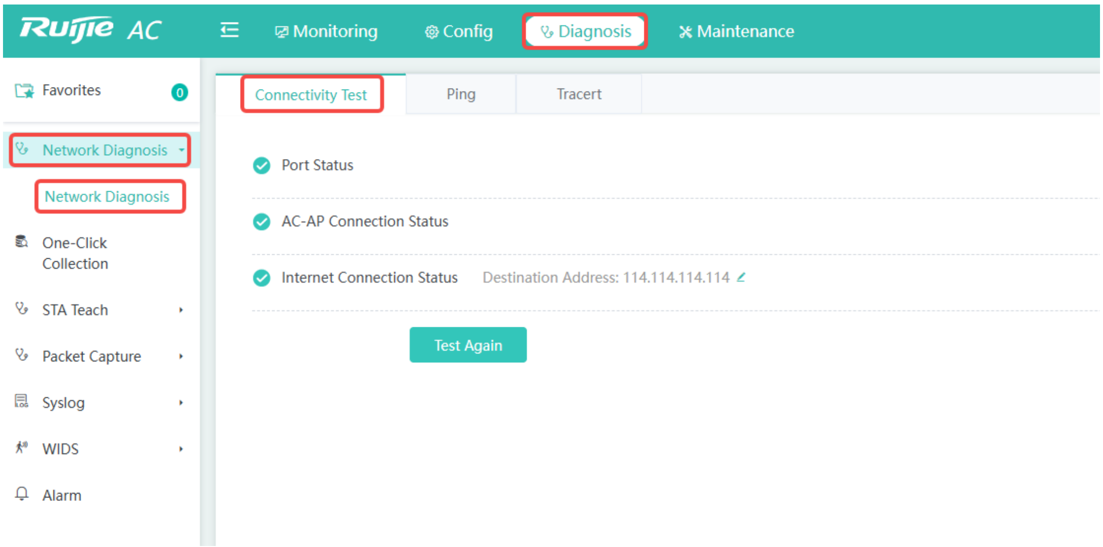
6 Diagnosis

6.1 Network Diagnosis

6.1.1 Network Diagnosis

Choose **Diagnosis** > **Network Diagnosis** > **Network Diagnosis**.

1. Connectivity Test



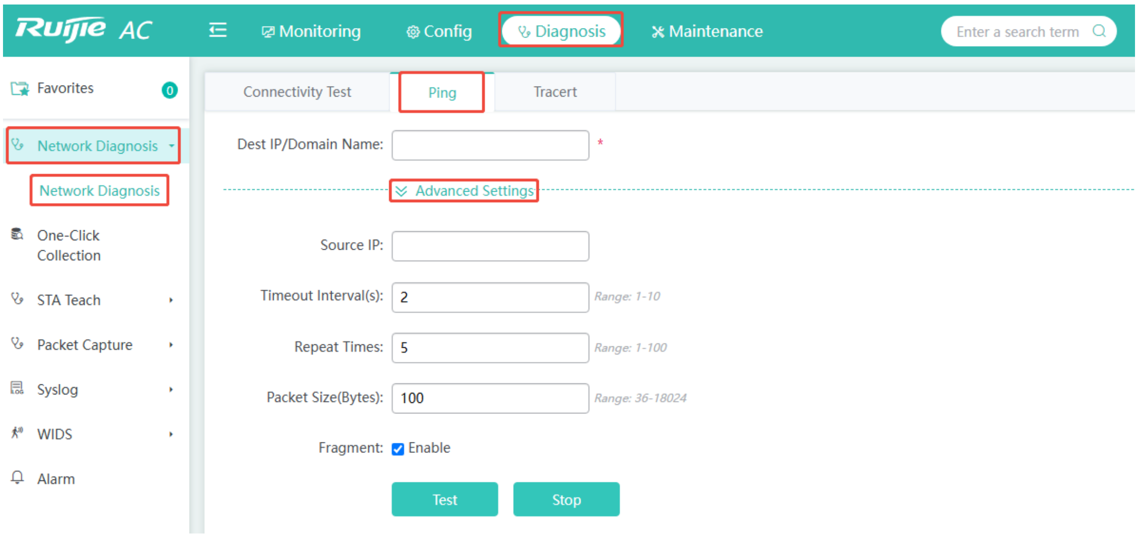
Port Status

AC-AP Connection Status

Internet Connection Status Destination Address: 114.114.114.114

Detection Item	Description
Port Status	Checks whether any interface on the AC is in Up status.
AC-AP Connection Status	Checks whether any AP connected to the AC goes online.
Internet Connection Status	Check whether the AC is connected to the external network. Custom address detection is supported. The IP address of 114.114.114.114 can be pinged in China, and the IP address of 8.8.8.8 can be pinged outside China.

2. Ping



Dest IP/Domain Name: *

Source IP:

Timeout Interval(s): 2 Range: 1-10

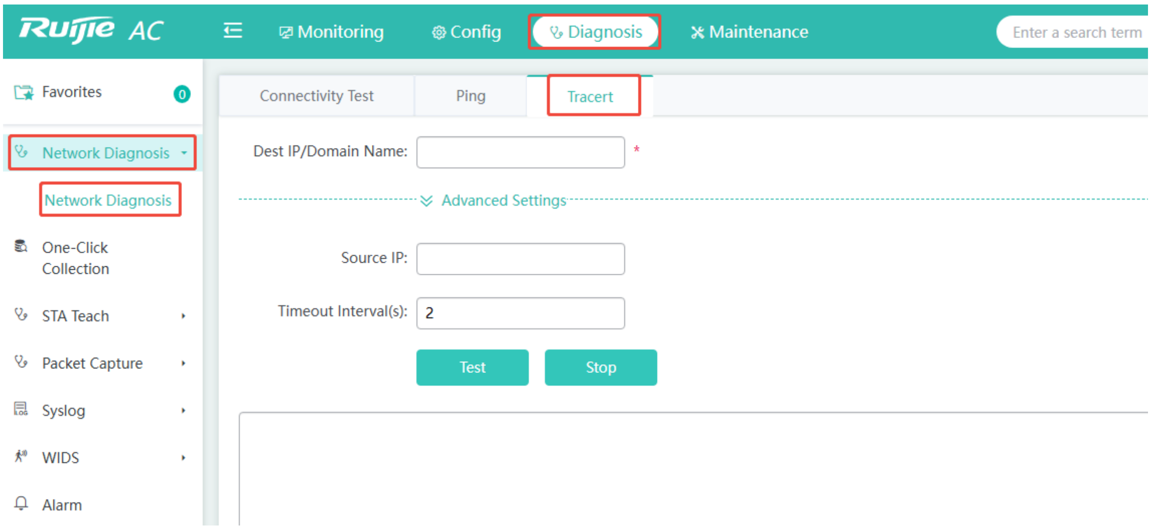
Repeat Times: 5 Range: 1-100

Packet Size(Bytes): 100 Range: 36-18024

Fragment: ☑ Enable

Parameter	Description
Dest IP/Domain Name	Indicates the address or domain name to be pinged.
Source IP	Indicates the source address of ping packets, namely, the local interface address of a device.
Timeout Interval(s)	Indicates the timeout duration.
Repeat Times	Indicates the number of data packets to be transmitted.
Packet Size(Bytes)	Indicates the length of the data padding section in a data packet to be transmitted.
Fragment	Indicates the DF flag bit of an IP address. When the DF flag bit is set to 1, data packets are not fragmented. The default DF flag bit is **0**.

3. Tracert

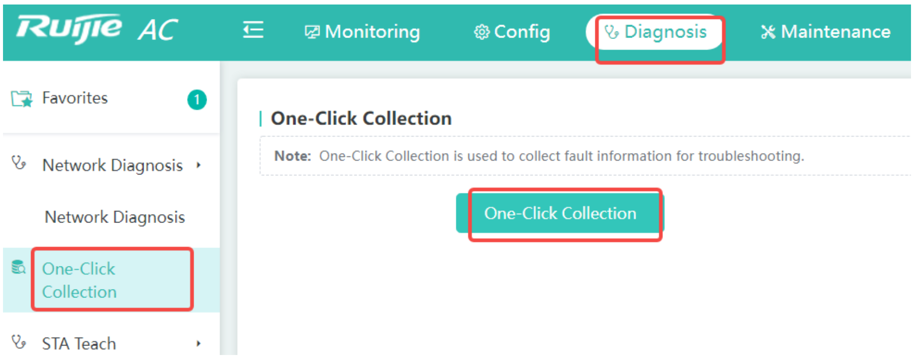


Parameter	Description
Dest IP/Domain Name	Indicates the tracert destination or domain name address.
Source IP	Indicates the tracert source address, namely, the local interface address of a device.
Timeout Interval(s)	Indicates the timeout duration.

6.2 One-Click Collection

Choose **Diagnosis** > **One-Click Collection**.

You can use the one-click collection feature to collect device fault information for troubleshooting.



Note: One-Click Collection is used to collect fault information for troubleshooting.

6.3 Client Diagnosis

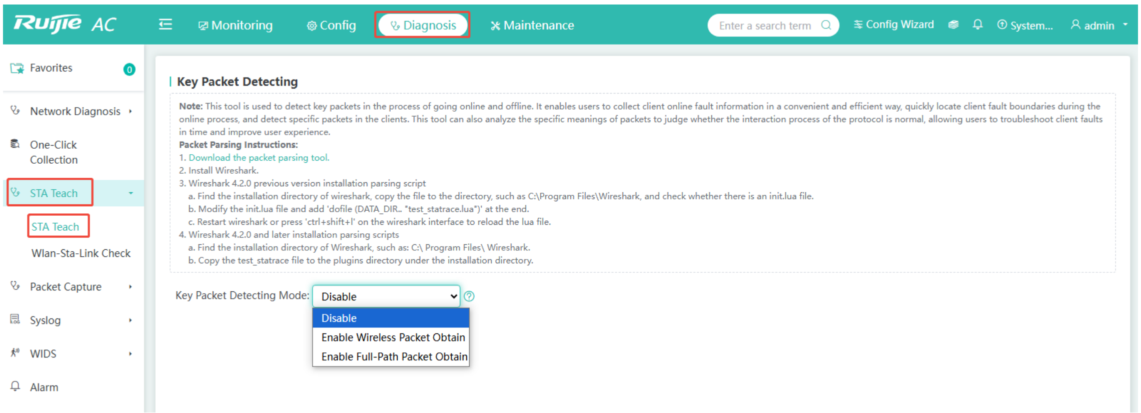
6.3.1 Key Packet Tracking

Choose **Diagnosis** > **STA Teach** > **STA Teach**.

This feature enables users to easily and quickly collect fault information, locate fault scope during the go-online process of clients, and track key packets of the clients. Key packet tracking identifies key packets and analyzes the key fields and meanings of the packets to determine whether the interaction process of the protocol is normal. It enables users to collect fault information conveniently and quickly and troubleshoot client faults in time, thus improving user experience.

Enable Wireless Packet Obtain: obtains packets on the wireless driver side.

Enable Full-Path Packet Obtain: obtains packets on the entire path that the packets pass through.



Key Packet Detecting

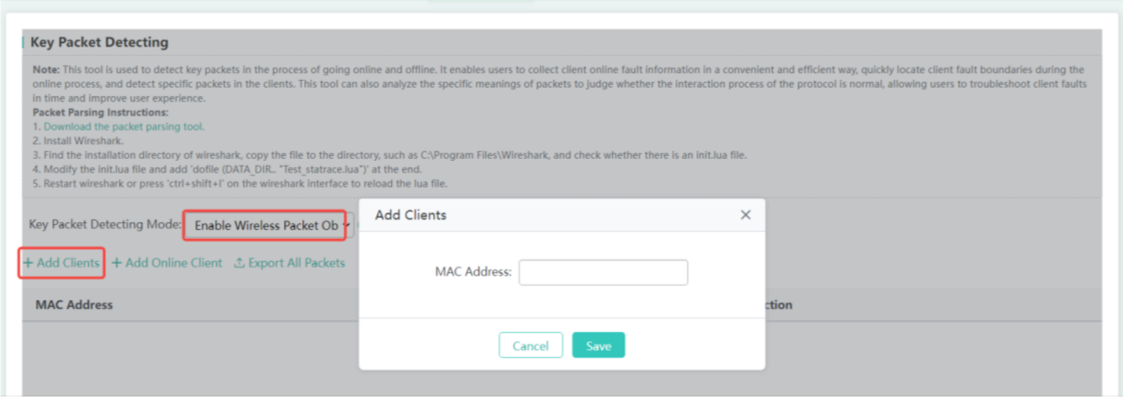
Note: This tool is used to detect key packets in the process of going online and offline. It enables users to collect client online fault information in a convenient and efficient way, quickly locate client fault boundaries during the online process, and detect specific packets in the clients. This tool can also analyze the specific meanings of packets to judge whether the interaction process of the protocol is normal, allowing users to troubleshoot client faults in time and improve user experience.

Packet Parsing Instructions:

1. Download the packet parsing tool.
2. Install Wireshark.
3. Wireshark 4.2.0 previous version installation parsing script
   a. Find the installation directory of wireshark, copy the file to the directory, such as C:\Program Files\Wireshark, and check whether there is an init.lua file.
   b. Modify the init.lua file and add 'dofile (DATA_DIR.. "test_statrace.lua")' at the end.
   c. Restart wireshark or press 'ctrl+shift+l' on the wireshark interface to reload the lua file.
4. Wireshark 4.2.0 and later installation parsing scripts
   a. Find the installation directory of Wireshark, such as: C:\ Program Files\ Wireshark.
   b. Copy the test_statrace file to the plugins directory under the installation directory.

Key Packet Detecting Mode: Disable

(1) Add a client manually: Click **Add Clients**. Enter the MAC address of a client. Click **Save**. The system verifies the validity of the MAC address. If the MAC address is valid, the client will be added.



Key Packet Detecting

Note: This tool is used to detect key packets in the process of going online and offline. It enables users to collect client online fault information in a convenient and efficient way, quickly locate client fault boundaries during the online process, and detect specific packets in the clients. This tool can also analyze the specific meanings of packets to judge whether the interaction process of the protocol is normal, allowing users to troubleshoot client faults in time and improve user experience.

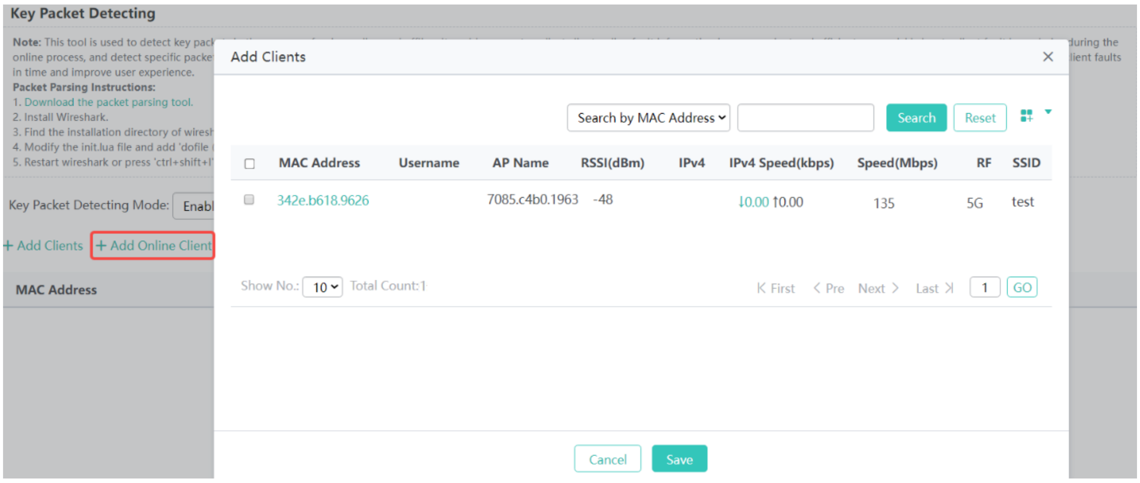
Packet Parsing Instructions:

1. Download the packet parsing tool.
2. Install Wireshark.
3. Find the installation directory of wireshark, copy the file to the directory, such as C:\Program Files\Wireshark, and check whether there is an init.lua file.
4. Modify the init.lua file and add 'dofile (DATA_DIR.. "Test_statrace.lua")' at the end.
5. Restart wireshark or press 'ctrl+shift+l' on the wireshark interface to reload the lua file.

Key Packet Detecting Mode: Enable Wireless Packet Ob

MAC Address:

(2) Select and add an online client: Click **Add Online Client**. Select an online client for packet tracking.



Key Packet Detecting

Note: This tool is used to detect key pack… during the online process, and detect specific packe… lient faults in time and improve user experience.

Packet Parsing Instructions:

1. Download the packet parsing tool.
2. Install Wireshark.
3. Find the installation directory of wiresh…
4. Modify the init.lua file and add 'dofile (…
5. Restart wireshark or press 'ctrl+shift+l'…

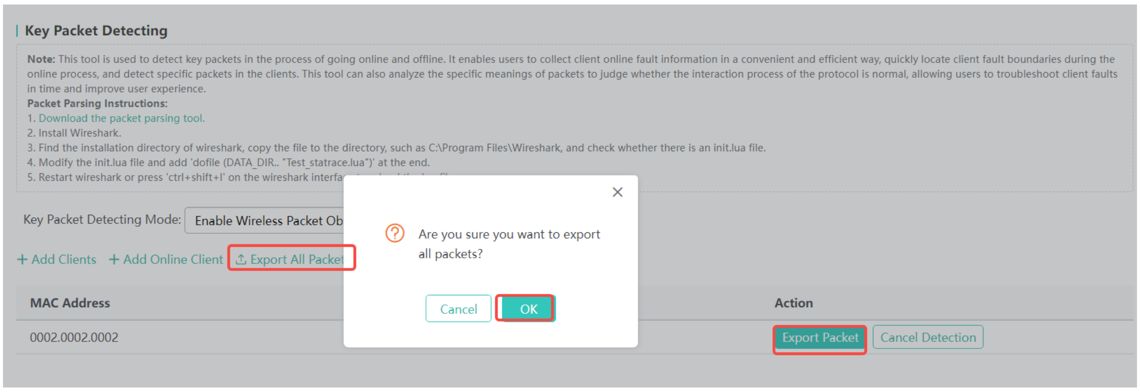
Key Packet Detecting Mode: Enabl…

Add Clients

□	MAC Address	Username	AP Name	RSSI(dBm)	IPv4	IPv4 Speed(kbps)	Speed(Mbps)	RF	SSID
□	342e.b618.9626		7085.c4b0.1963	-48		↓0.00 ↑0.00	135	5G	test

Show No.: 10 Total Count:1

(3) Export packets: Click **Export Packet** behind a specified client. If all client packets need to be exported, click **Export All Packets** to compress all the received packets into a **.tar** file and export the file to users.



Key Packet Detecting

Note: This tool is used to detect key packets in the process of going online and offline. It enables users to collect client online fault information in a convenient and efficient way, quickly locate client fault boundaries during the online process, and detect specific packets in the clients. This tool can also analyze the specific meanings of packets to judge whether the interaction process of the protocol is normal, allowing users to troubleshoot client faults in time and improve user experience.

Packet Parsing Instructions:

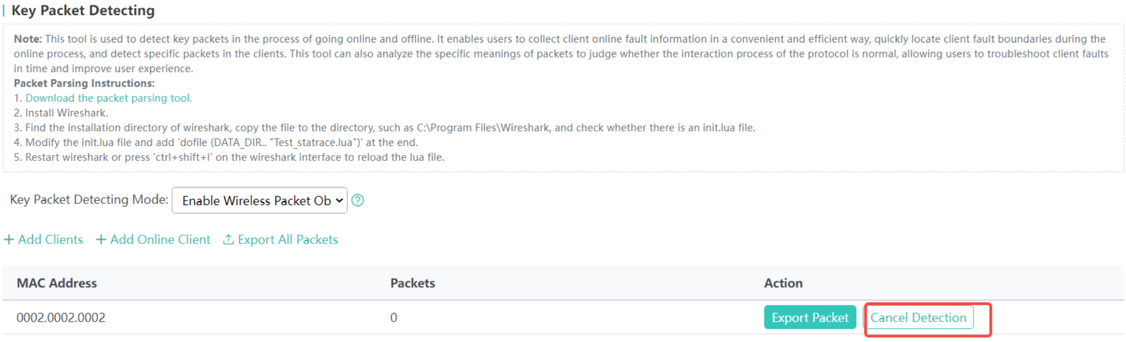
1. Download the packet parsing tool.
2. Install Wireshark.
3. Find the installation directory of wireshark, copy the file to the directory, such as C:\Program Files\Wireshark, and check whether there is an init.lua file.
4. Modify the init.lua file and add 'dofile (DATA_DIR.. "Test_statrace.lua")' at the end.
5. Restart wireshark or press 'ctrl+shift+l' on the wireshark interfa…

Key Packet Detecting Mode: Enable Wireless Packet Ob

Are you sure you want to export all packets?

MAC Address	Action
0002.0002.0002	Export Packet Cancel Detection

(4) Cancel packet tracking: Click **Cancel Detection** behind a specified client.



Key Packet Detecting

Note: This tool is used to detect key packets in the process of going online and offline. It enables users to collect client online fault information in a convenient and efficient way, quickly locate client fault boundaries during the online process, and detect specific packets in the clients. This tool can also analyze the specific meanings of packets to judge whether the interaction process of the protocol is normal, allowing users to troubleshoot client faults in time and improve user experience.

Packet Parsing Instructions:

1. Download the packet parsing tool.
2. Install Wireshark.
3. Find the installation directory of wireshark, copy the file to the directory, such as C:\Program Files\Wireshark, and check whether there is an init.lua file.
4. Modify the init.lua file and add 'dofile (DATA_DIR.. "Test_statrace.lua")' at the end.
5. Restart wireshark or press 'ctrl+shift+l' on the wireshark interface to reload the lua file.

Key Packet Detecting Mode: Enable Wireless Packet Ob

MAC Address	Packets	Action
0002.0002.0002	0	Export Packet Cancel Detection

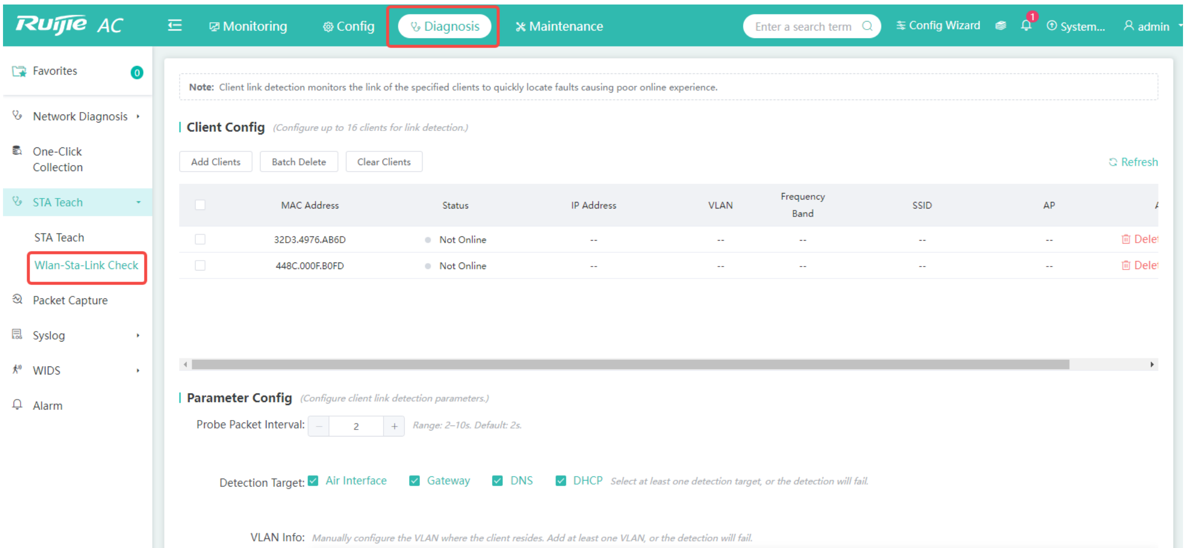
6.3.2 STA Link Detection

Choose **Diagnosis** > **STA Teach** > **Wlan-Sta-Link Check**.

The STA link detection function monitors all the links of a specified STA to quickly locate faults causing poor network experience.

Note

Up to 16 STAs can be configured for link detection.



Note: Client link detection monitors the link of the specified clients to quickly locate faults causing poor online experience.

Client Config *(Configure up to 16 clients for link detection.)*

□	MAC Address	Status	IP Address	VLAN	Frequency Band	SSID	AP	A
□	32D3.4976.AB6D	Not Online	--	--	--	--	--	Dele
□	448C.000F.B0FD	Not Online	--	--	--	--	--	Dele

Parameter Config *(Configure client link detection parameters.)*

Probe Packet Interval: – 2 + *Range: 2–10s. Default: 2s.*

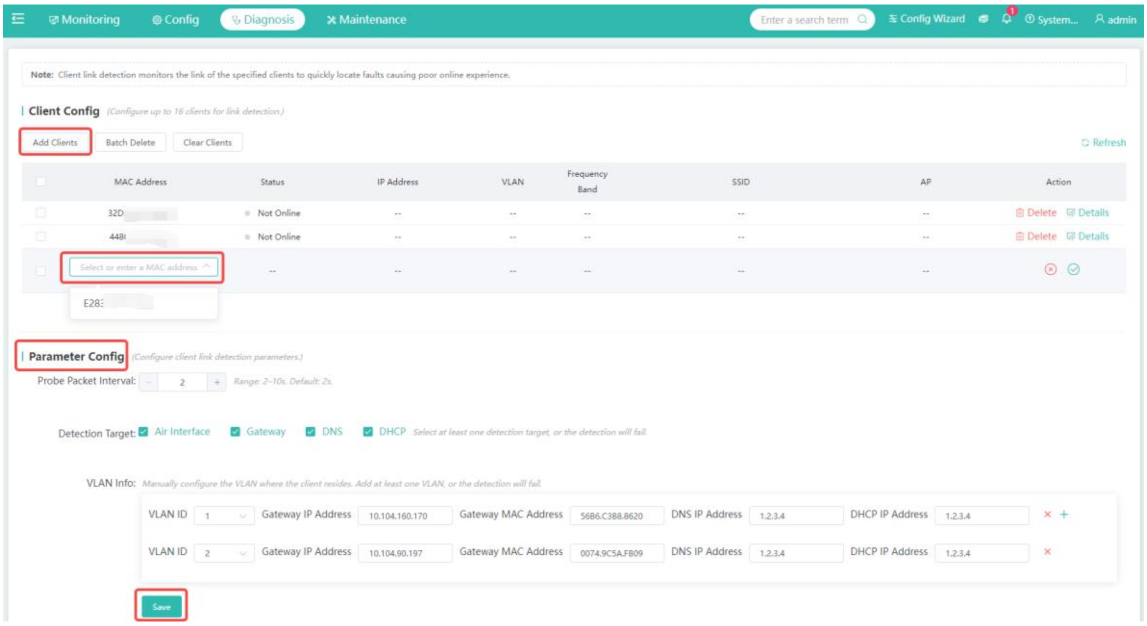
Detection Target: ☑ Air Interface ☑ Gateway ☑ DNS ☑ DHCP *Select at least one detection target, or the detection will fail.*

VLAN Info: *Manually configure the VLAN where the client resides. Add at least one VLAN, or the detection will fail.*

1. STA Configuration

(1) Adding a STA

To add a STA to the STA link detection list, click **Add Clients**, select the MAC address of the STA at the bottom of the STA list, and click ✓. After a STA is added successfully, you need to configure the VLAN to which the STA belongs in the **Parameter Config** area. Otherwise, the detection result may be incorrect.



Note: Client link detection monitors the link of the specified clients to quickly locate faults causing poor online experience.

Client Config *(Configure up to 16 clients for link detection.)*

□	MAC Address	Status	IP Address	VLAN	Frequency Band	SSID	AP	Action
□	32D	Not Online	--	--	--	--	--	Delete Details
□	448(	Not Online	--	--	--	--	--	Delete Details
□	Select or enter a MAC address E28:	--	--	--	--	--	--	⊗ ✓

Parameter Config *(Configure client link detection parameters.)*

Probe Packet Interval: – 2 + *Range: 2–10s. Default: 2s.*

Detection Target: ☑ Air Interface ☑ Gateway ☑ DNS ☑ DHCP *Select at least one detection target, or the detection will fail.*

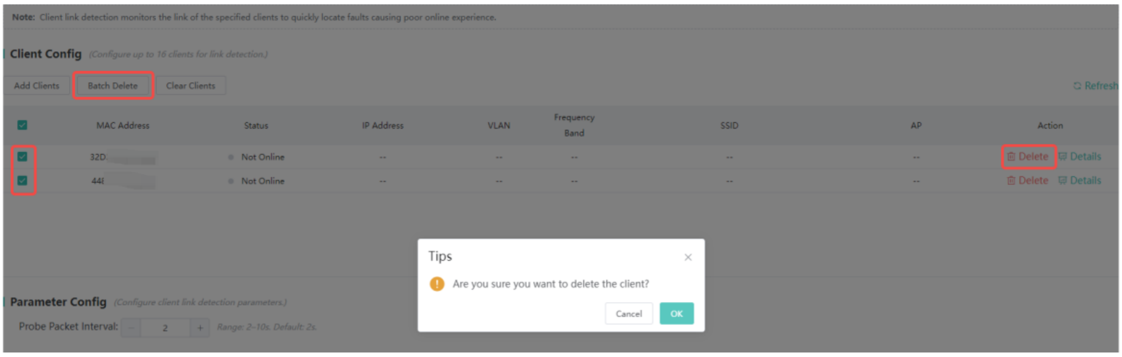
VLAN Info: *Manually configure the VLAN where the client resides. Add at least one VLAN, or the detection will fail.*

VLAN ID 1 Gateway IP Address 10.104.160.170 Gateway MAC Address 5686.C388.8620 DNS IP Address 1.2.3.4 DHCP IP Address 1.2.3.4 × +

VLAN ID 2 Gateway IP Address 10.104.90.197 Gateway MAC Address 0074.9C5A.FB09 DNS IP Address 1.2.3.4 DHCP IP Address 1.2.3.4 ×

(2) Deleting a STA

To delete a STA from the STA link detection list, click **Delete** in the **Action** column of the STA. To delete multiple STAs, select the STAs and click **Batch Delete**.



Note: Client link detection monitors the link of the specified clients to quickly locate faults causing poor online experience.

Client Config *(Configure up to 16 clients for link detection.)*

☑	MAC Address	Status	IP Address	VLAN	Frequency Band	SSID	AP	Action
☑	32D[redacted]	● Not Online	--	--	--	--	--	Delete Details
☑	44[redacted]	● Not Online	--	--	--	--	--	Delete Details

Parameter Config *(Configure client link detection parameters.)*

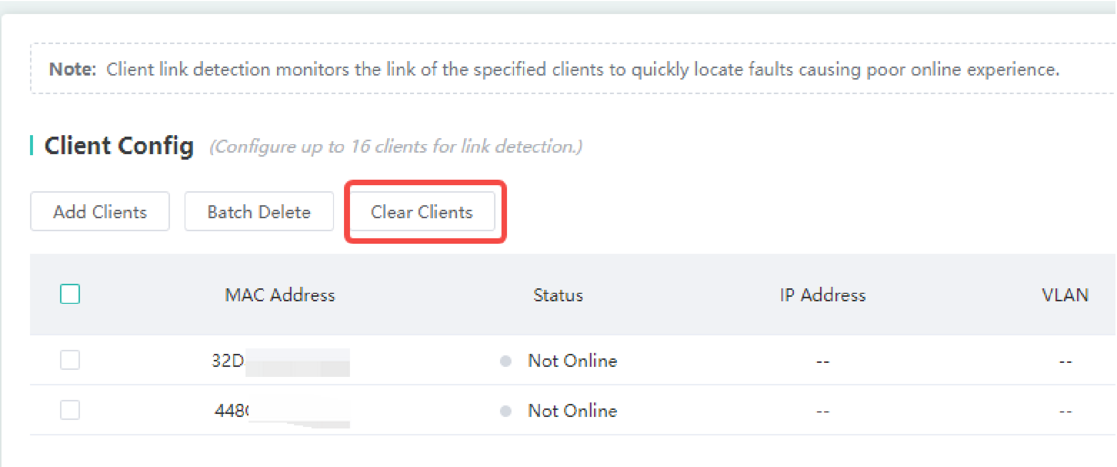
Probe Packet Interval: 2 *Range: 2–10s. Default: 2s.*

Tips

Are you sure you want to delete the client?

(3) Deleting all STAs

To delete all STAs from the STA link detection list, click **Clear Clients**.



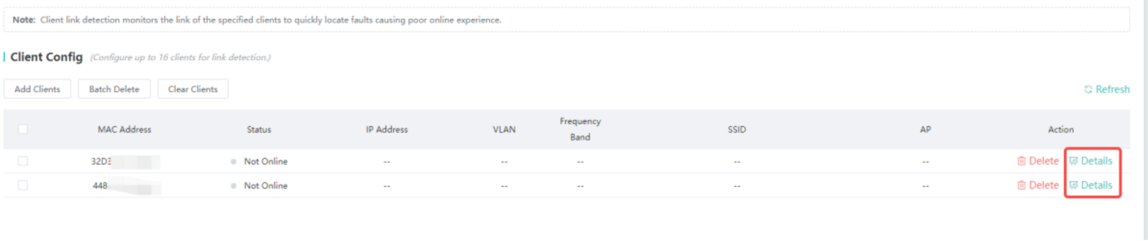
Note: Client link detection monitors the link of the specified clients to quickly locate faults causing poor online experience.

Client Config *(Configure up to 16 clients for link detection.)*

□	MAC Address	Status	IP Address	VLAN
□	32D[redacted]	● Not Online	--	--
□	448[redacted]	● Not Online	--	--

(4) Viewing STA link detection details

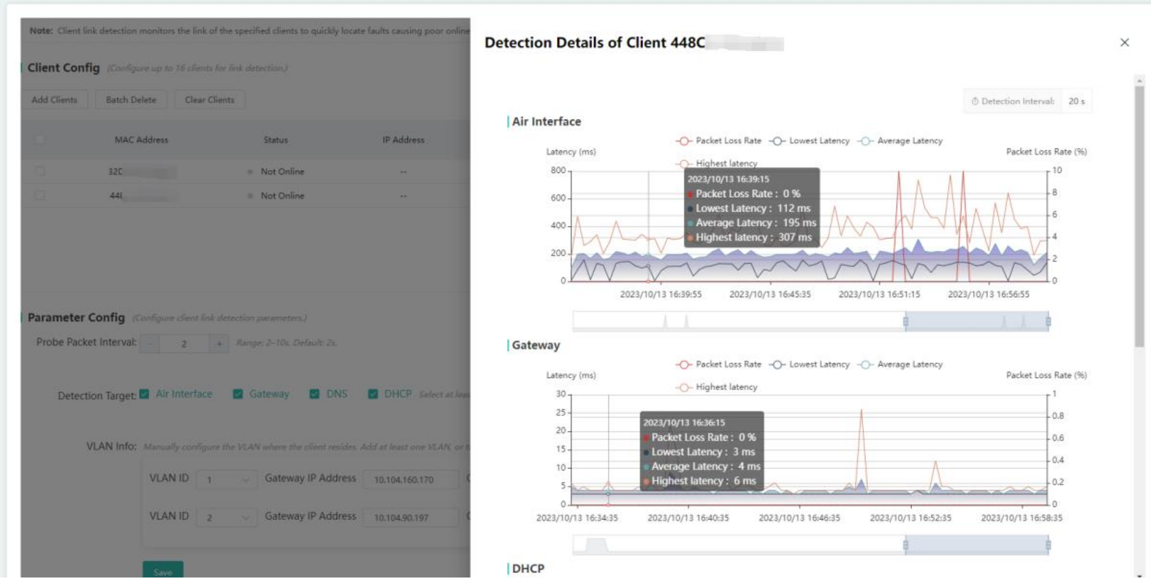
Click **Details** in the **Action** column of a STA to view the line charts of the packet loss rate, lowest latency, average latency, and highest latency of the STA's air interfaces, gateway, DHCP, and DNS. Whether information about air interfaces, gateway, DHCP, and DNS is displayed depends on whether the detection targets are configured in the **Parameter Config** area.



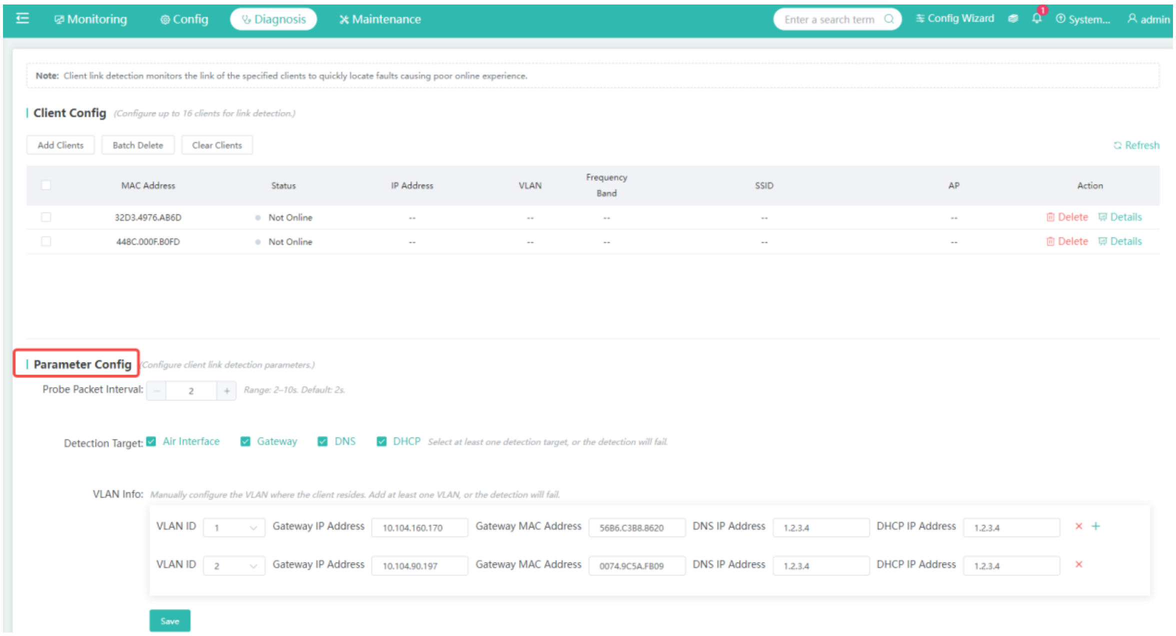
Note: Client link detection monitors the link of the specified clients to quickly locate faults causing poor online experience.

Client Config *(Configure up to 16 clients for link detection.)*

□	MAC Address	Status	IP Address	VLAN	Frequency Band	SSID	AP	Action
□	32D[redacted]	● Not Online	--	--	--	--	--	Delete Details
□	448[redacted]	● Not Online	--	--	--	--	--	Delete Details



2. Parameter Configuration



Note: Client link detection monitors the link of the specified clients to quickly locate faults causing poor online experience.

Client Config (Configure up to 16 clients for link detection.)

Add Clients | Batch Delete | Clear Clients | Refresh

	MAC Address	Status	IP Address	VLAN	Frequency Band	SSID	AP	Action
□	32D3.4976.AB6D	Not Online	--	--	--	--	--	Delete Details
□	448C.000F.B0FD	Not Online	--	--	--	--	--	Delete Details

Parameter Config (Configure client link detection parameters.)

Probe Packet Interval: 2 Range: 2–10s. Default: 2s.

Detection Target: ☑ Air Interface ☑ Gateway ☑ DNS ☑ DHCP Select at least one detection target, or the detection will fail.

VLAN Info: Manually configure the VLAN where the client resides. Add at least one VLAN, or the detection will fail.

VLAN ID	Gateway IP Address	Gateway MAC Address	DNS IP Address	DHCP IP Address
1	10.104.160.170	5686.C3B8.8620	1.2.3.4	1.2.3.4
2	10.104.90.197	0074.9C5A.FB09	1.2.3.4	1.2.3.4

Save

Parameter	Description
Probe Packet Interval	The value range is from 2 to 10, in seconds. The default value is 2 seconds.
Detection Target	Select one or more from **Air Interface**, **Gateway**, **DNS**, and **DHCP** as the detection targets. If an option is not selected, it will not be displayed on the STA link detection details page.

Parameter	Description
VLAN Info	This parameter is mandatory. Configure the VLANs to which the STA to be detected belongs. Add at least one VLAN entry, including the VLAN ID, gateway IP address, gateway MAC address, DNS IP address, and DHCP IP address.

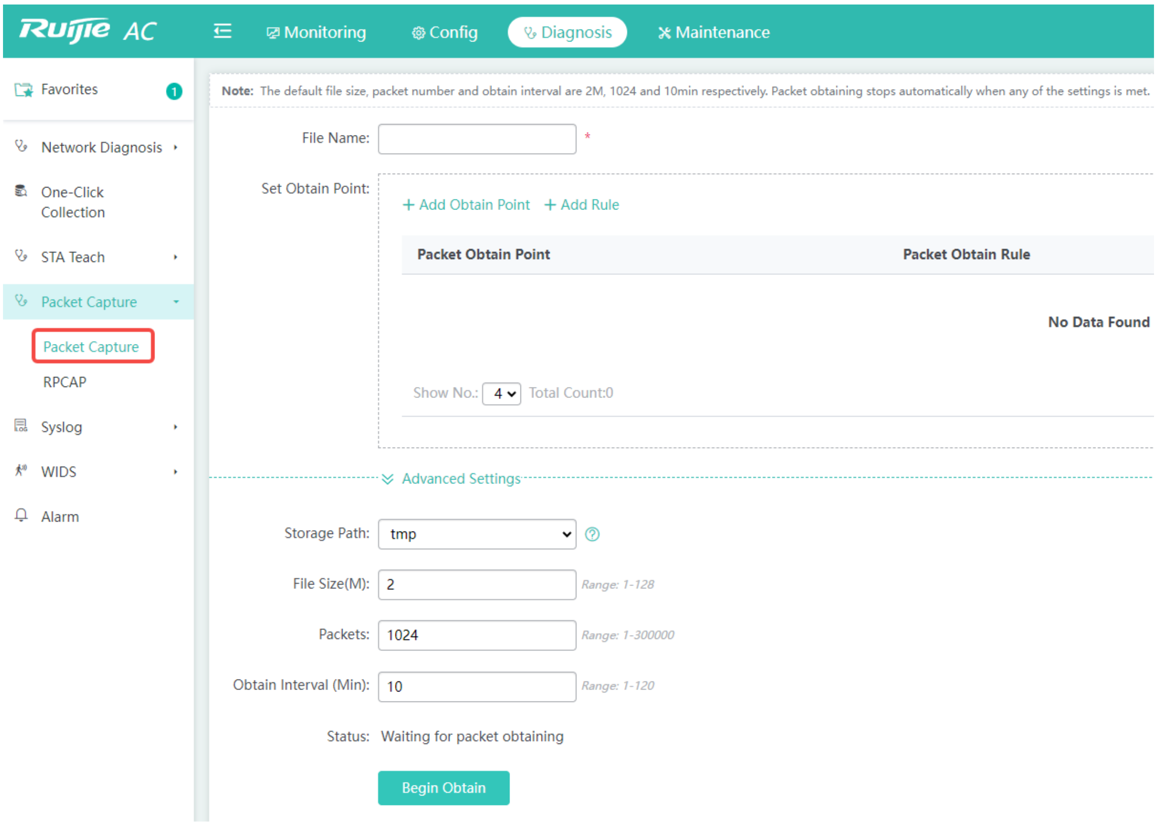
6.4 Packet Obtaining

6.4.1 Packet Obtaining

Choose **Diagnosis** > **Packet Capture** > **Packet Capture**.

This feature is generally used to obtain packets to collect diagnostic data when problems occur with after-sales devices.

(1) Start packet obtaining: Edit the fields on the configuration page. Click **Begin Obtain**.



Note: The default file size, packet number and obtain interval are 2M, 1024 and 10min respectively. Packet obtaining stops automatically when any of the settings is met.

File Name: *

Set Obtain Point:

Packet Obtain Point	Packet Obtain Rule
No Data Found	

Show No.: 4 Total Count:0

Storage Path: tmp

File Size(M): 2 Range: 1-128

Packets: 1024 Range: 1-300000

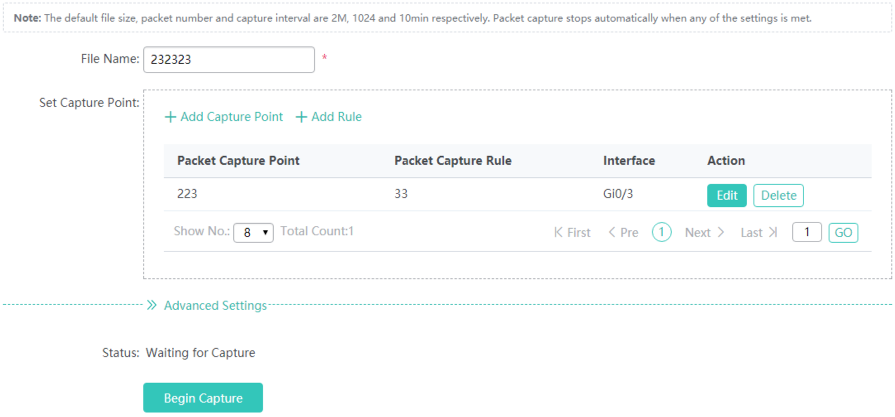
Obtain Interval (Min): 10 Range: 1-120

Status: Waiting for packet obtaining

Parameter	Description
File Name	Specifies the name of the file to be saved.
Set Obtain Point	Specifies the packet obtaining location.
Storage Path	Specifies the storage path of the obtained packet file.
File Size(M)	Specifies the buffer size.

Packets	Specifies the number of packets to be obtained.
Obtain Interval (Min)	Specifies the timeout duration. The packet obtaining is automatically stopped when the timeout duration expires.
Status	Current packet obtaining status.

(2) Stop packet obtaining: During packet obtaining, click **End Capture** to stop packet obtaining.



Note: The default file size, packet number and capture interval are 2M, 1024 and 10min respectively. Packet capture stops automatically when any of the settings is met.

File Name: 232323 *

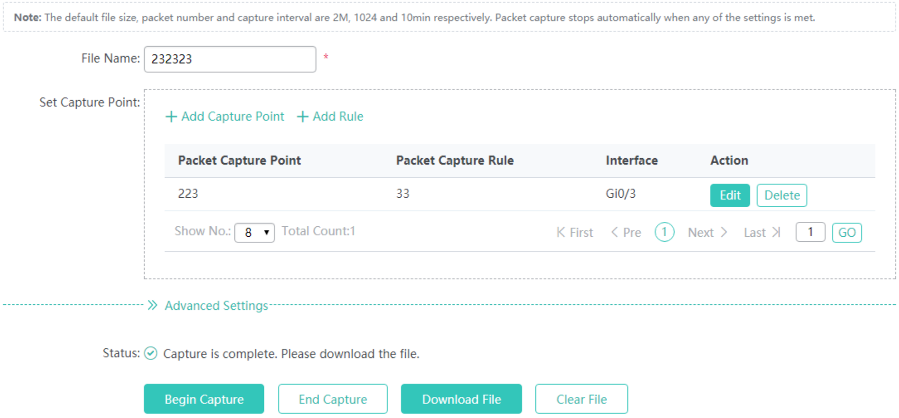
Set Capture Point:

Packet Capture Point	Packet Capture Rule	Interface	Action
223	33	Gi0/3	Edit Delete

Show No.: 8 Total Count:1

Status: Waiting for Capture

(3) Download the file: Click **Download File** to download the obtained file to the computer.



Note: The default file size, packet number and capture interval are 2M, 1024 and 10min respectively. Packet capture stops automatically when any of the settings is met.

File Name: 232323 *

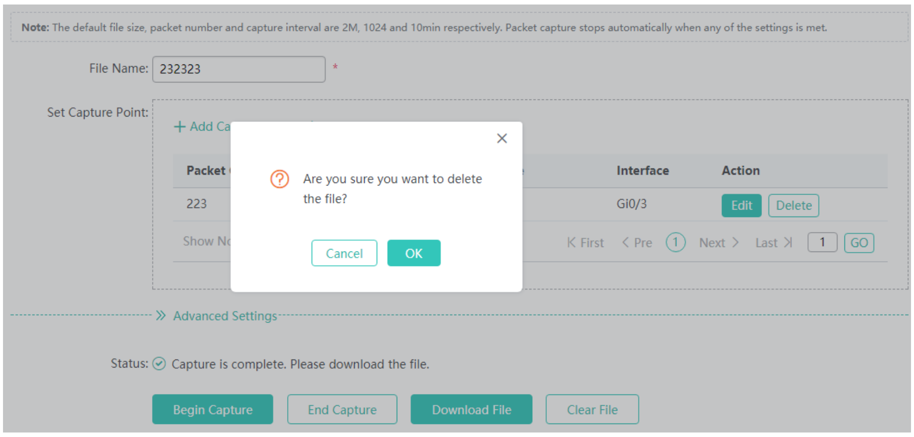
Set Capture Point:

Packet Capture Point	Packet Capture Rule	Interface	Action
223	33	Gi0/3	Edit Delete

Show No.: 8 Total Count:1

Status: Capture is complete. Please download the file.

(4) Clear the file: Click **Clear File** to remove the obtained file from the device.



Note: The default file size, packet number and capture interval are 2M, 1024 and 10min respectively. Packet capture stops automatically when any of the settings is met.

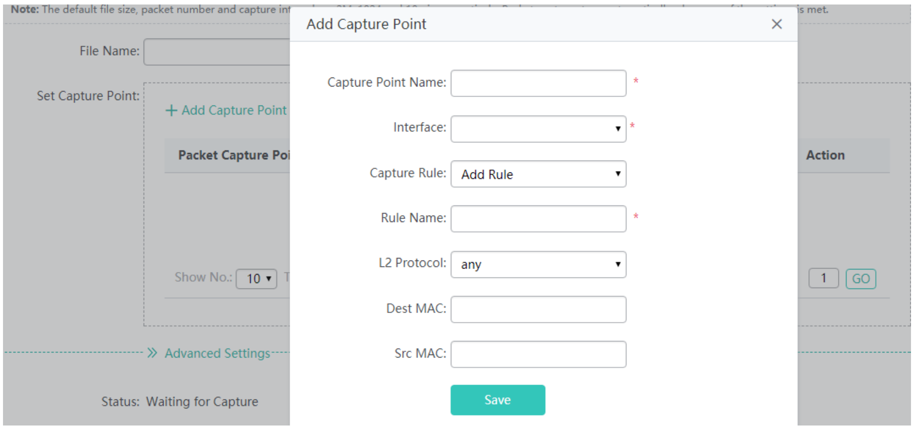
File Name: 232323 *

Are you sure you want to delete the file?

Packet	Interface	Action
223	Gi0/3	Edit Delete

Status: Capture is complete. Please download the file.

(5) Add a capture point: Click **Add Capture Point**. The configuration dialog box pops up. Configure the parameters and click **Save**. A message indicating the point has been successfully added is displayed.



Add Capture Point

Capture Point Name: *

Interface: *

Capture Rule: Add Rule

Rule Name: *

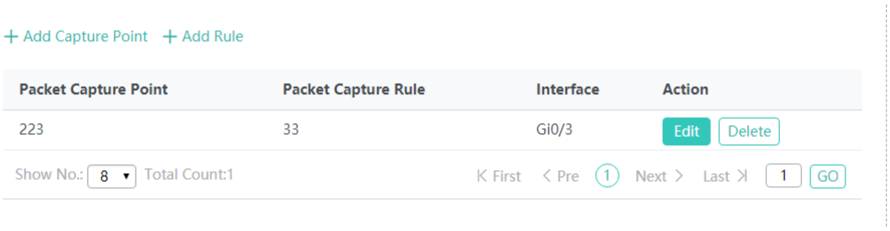
L2 Protocol: any

Dest MAC:

Src MAC:

Status: Waiting for Capture

(6) Delete a capture point: Click **Delete** behind a specified capture point.

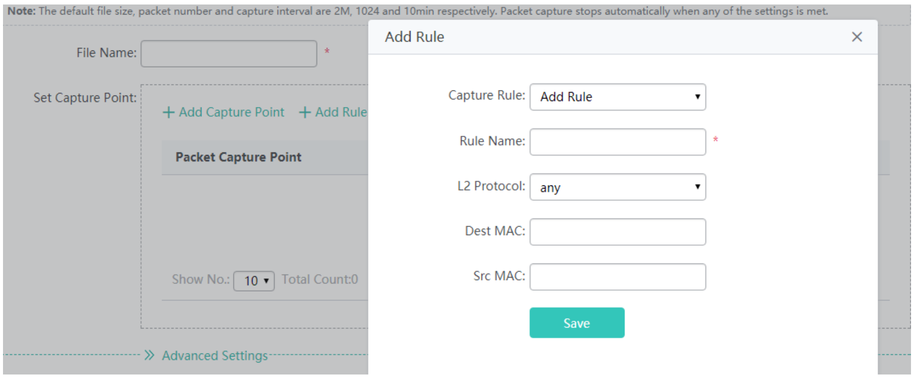


+ Add Capture Point + Add Rule

Packet Capture Point	Packet Capture Rule	Interface	Action
223	33	Gi0/3	Edit Delete

Show No.: 8 Total Count:1

(7) Set rules for packet obtaining: Click **Add Rule**. The configuration dialog box pops up. Configure the parameters and click **Save**. A message indicating the rule has been successfully added is displayed.



Note: The default file size, packet number and capture interval are 2M, 1024 and 10min respectively. Packet capture stops automatically when any of the settings is met.

File Name: *

Set Capture Point:

Packet Capture Point

Show No.: 10 Total Count:0

Add Rule

Capture Rule: Add Rule

Rule Name: *

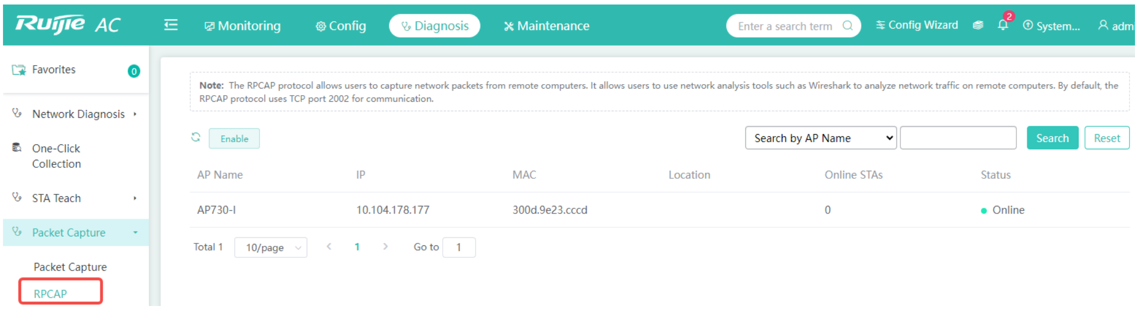
L2 Protocol: any

Dest MAC:

Src MAC:

6.4.2 RPCAP

The Remote Packet Capture Protocol (RPCAP) enables users to obtain network packets from remote computers. It also allows users to analyze network traffic on remote computers through Wireshark and other network analysis tools.



Note: The RPCAP protocol allows users to capture network packets from remote computers. It allows users to use network analysis tools such as Wireshark to analyze network traffic on remote computers. By default, the RPCAP protocol uses TCP port 2002 for communication.

Search by AP Name

AP Name	IP	MAC	Location	Online STAs	Status
AP730-I	10.104.178.177	300d.9e23.cccd		0	● Online

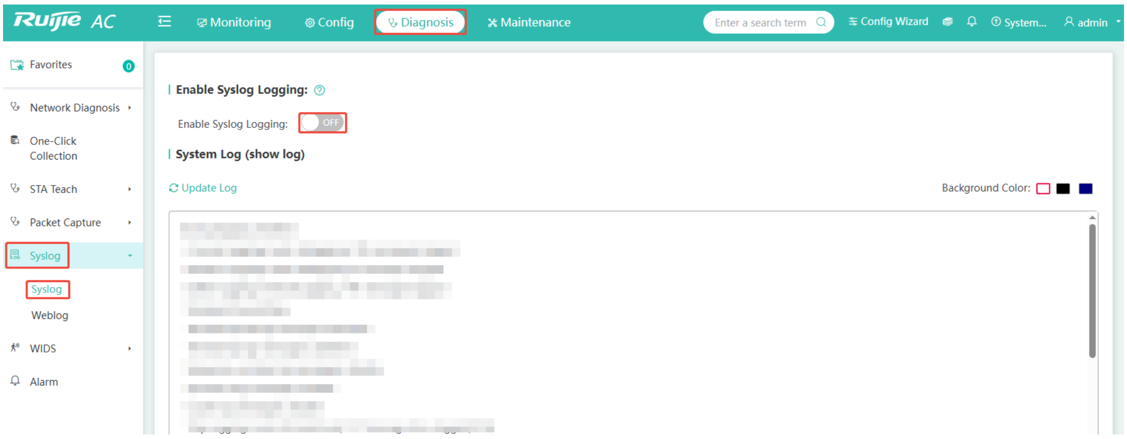
Total 1 10/page 1 Go to 1

6.5 Log Table

6.5.1 Syslog

Choose **Diagnosis** > **Syslog** > **Syslog**.

You can configure the syslog feature to help after-sales and R&D personnel locate problems. Click **Export Syslog** to download the syslog to the computer.



Enable Syslog Logging:

Enable Syslog Logging: OFF

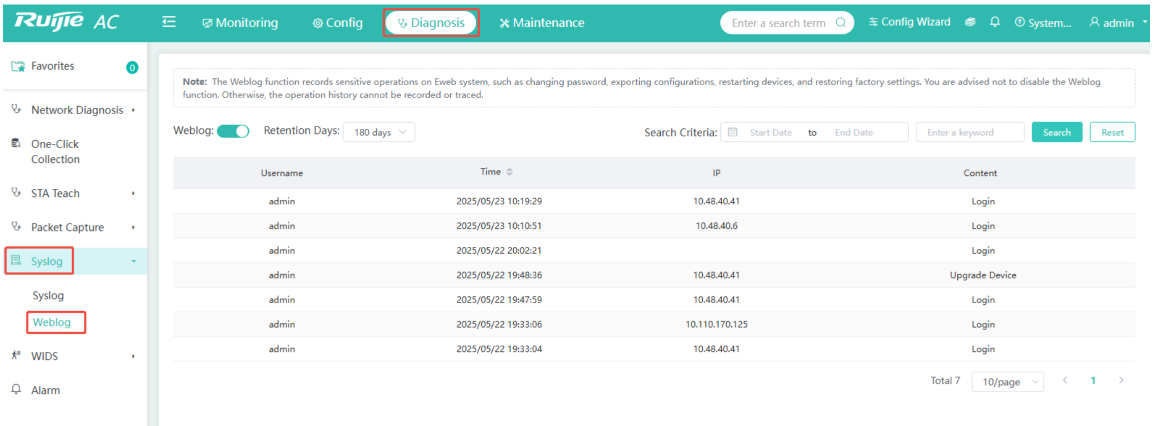
System Log (show log)

Background Color: □ ■ ■

6.5.2 Weblog

Choose **Diagnosis** > **Syslog** > **Weblog**.

The Web operation log is used to record sensitive operations of the network management system, including password modification, configuration export, device restart, and factory reset. You are not advised to disable the Web operation log feature, otherwise the operation history cannot be recorded or traced. Web logs can be retained for up to 360 days.



Note: The Weblog function records sensitive operations on Eweb system, such as changing password, exporting configurations, restarting devices, and restoring factory settings. You are advised not to disable the Weblog function. Otherwise, the operation history cannot be recorded or traced.

Weblog: on   Retention Days: 180 days   Search Criteria: Start Date to End Date   Enter a keyword   Search   Reset

Username	Time	IP	Content
admin	2025/05/23 10:19:29	10.48.40.41	Login
admin	2025/05/23 10:10:51	10.48.40.6	Login
admin	2025/05/22 20:02:21		Login
admin	2025/05/22 19:48:36	10.48.40.41	Upgrade Device
admin	2025/05/22 19:47:59	10.48.40.41	Login
admin	2025/05/22 19:33:06	10.110.170.125	Login
admin	2025/05/22 19:33:04	10.48.40.41	Login

Total 7   10/page   1

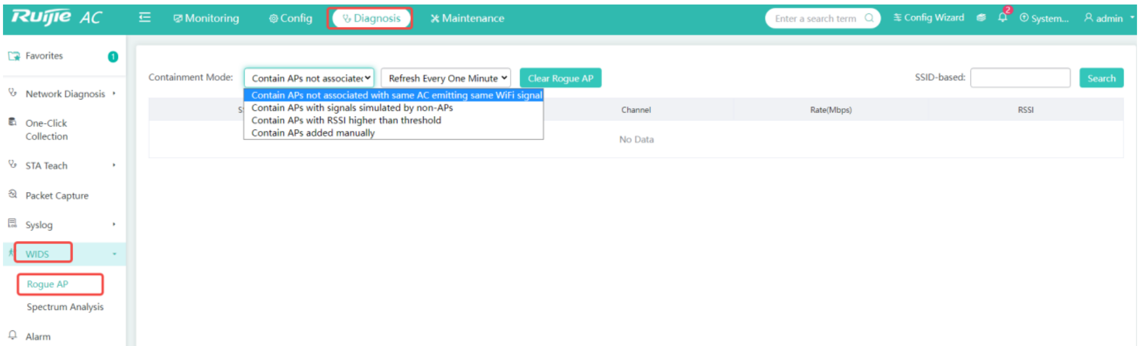
6.6 Air Interface Detection

6.6.1 Rogue AP

Choose **Diagnosis** > **WIDS** > **Rogue AP**.

Rogue APs may exist on a wireless network. They may have security vulnerabilities or may be controlled by attackers, seriously threatening the security of user networks.

The following page displays possible rogue APs that are identified after the containment feature is enabled.



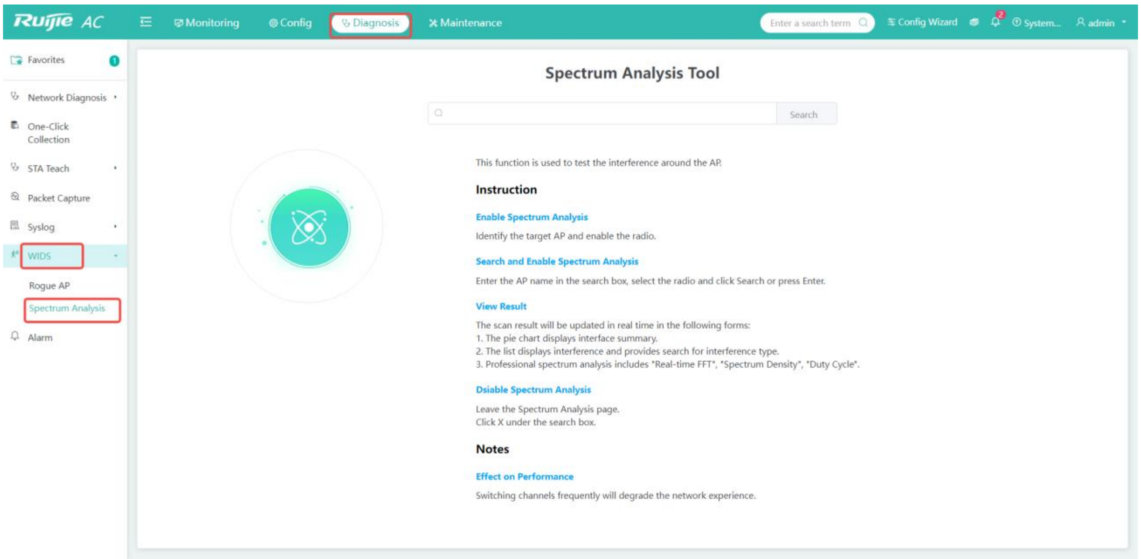
Containment Mode: Contain APs not associatec   Refresh Every One Minute   SSID-based:

S	Channel	Rate(Mbps)	RSSI
	No Data		

6.6.2 Spectrum Analysis

Choose **Diagnosis** > **WIDS** > **Spectrum Analysis**.

When the network quality is poor, the system can detect network interference and determine whether interference exists on the network based on **Real-time FFT**, **Spectrum Density**, and other spectrum diagrams. The interference information is recorded.



Spectrum Analysis Tool

This function is used to test the interference around the AP.

Instruction

Enable Spectrum Analysis

Identify the target AP and enable the radio.

Search and Enable Spectrum Analysis

Enter the AP name in the search box, select the radio and click Search or press Enter.

View Result

The scan result will be updated in real time in the following forms:
1. The pie chart displays interface summary.
2. The list displays interference and provides search for interference type.
3. Professional spectrum analysis includes "Real-time FFT", "Spectrum Density", "Duty Cycle".

Dsiable Spectrum Analysis

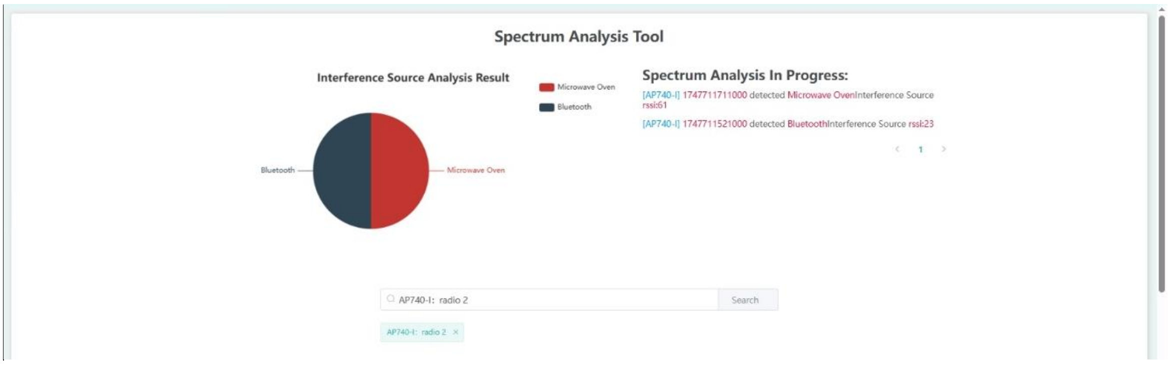
Leave the Spectrum Analysis page.
Click X under the search box.

Notes

Effect on Performance

Switching channels frequently will degrade the network experience.

Count AP interference sources through spectrum analysis and list them.



Spectrum Analysis Tool

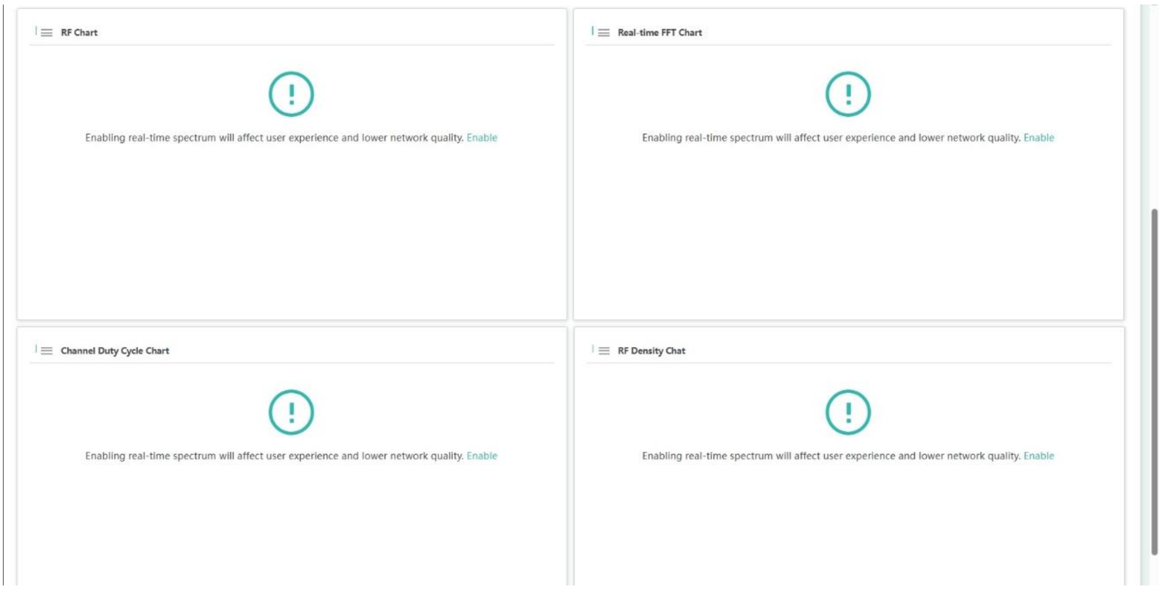
Spectrum Analysis In Progress:

[AP740-I] 1747711711000 detected Microwave OvenInterference Source rssi:61

[AP740-I] 1747711521000 detected BluetoothInterference Source rssi:23

AP740-I: radio 2

The following figure displays the initial state (when real-time spectrum is disabled):



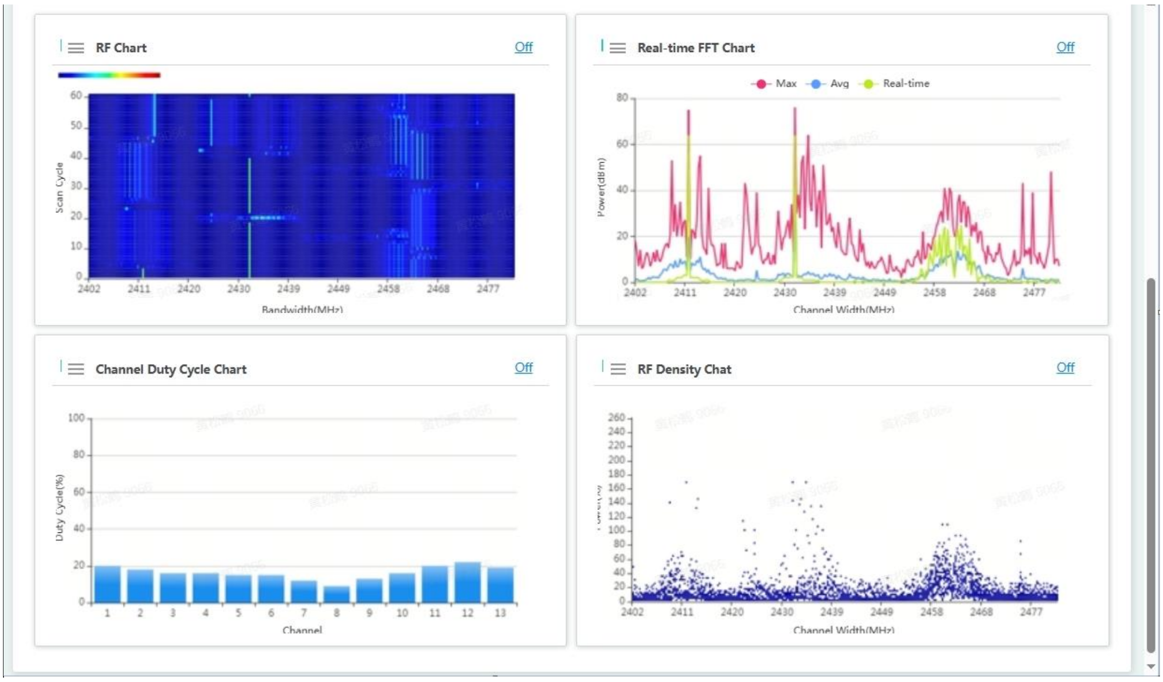
Enabling real-time spectrum will affect user experience and lower network quality.

Enabling real-time spectrum will affect user experience and lower network quality.

Enabling real-time spectrum will affect user experience and lower network quality.

Enabling real-time spectrum will affect user experience and lower network quality.

The following figure displays the spectrum analysis result (when real-time spectrum is enabled):



Note

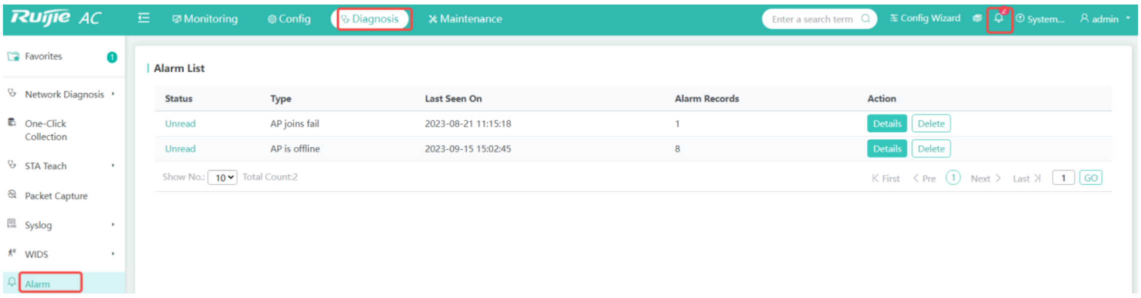
To perform spectrum analysis, the AP must go online.

When you switch to view the spectrum analysis result of another AP, the real-time spectrum analysis feature is automatically disabled and needs to be manually enabled.

6.7 Alarm

Choose **Diagnosis** > **Alarm**.

When alarm records exist on the system, the alarm clock icon in the upper right corner of the page will be marked with a red number indicating the number of alarm types. Click the alarm clock icon to jump to the **Alarm List** page and check detailed alarm information.



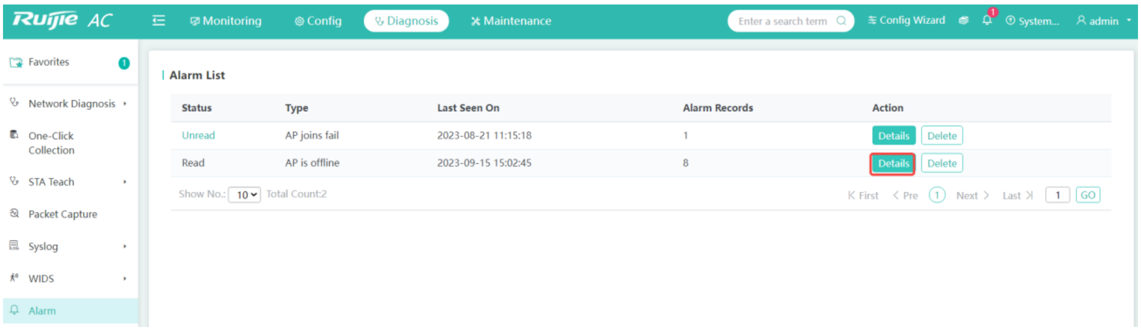
Alarm List

Status	Type	Last Seen On	Alarm Records	Action
Unread	AP joins fail	2023-08-21 11:15:18	1	Details Delete
Unread	AP is offline	2023-09-15 15:02:45	8	Details Delete

Show No.: 10 Total Count:2 First Pre 1 Next Last 1 GO

The list displays an overview of various alarms, mainly including AP offline alarms, AP access failure alarms, alarms about the number of AP/RF user access exceeding the threshold (90%), and AP power saving alarms. The number of alarms of each type and the latest occurrence time of each alarm type are also displayed. For example, if two APs go offline, the displayed number of this type of alarm is 2.

Click **Unread**. A confirmation dialog box is displayed, requesting you to confirm whether to mark the record as a read one. If you confirm the operation, the number of alarms displayed in the upper right corner decreases by 1. Click **Details** to display the alarm details. Click **Delete** to delete this type of alarm.



Alarm List

Status	Type	Last Seen On	Alarm Records	Action
Unread	AP joins fail	2023-08-21 11:15:18	1	Details Delete
Read	AP is offline	2023-09-15 15:02:45	8	Details Delete

Show No.: 10 Total Count:2

First Pre 1 Next Last 1 GO

7 Maintenance

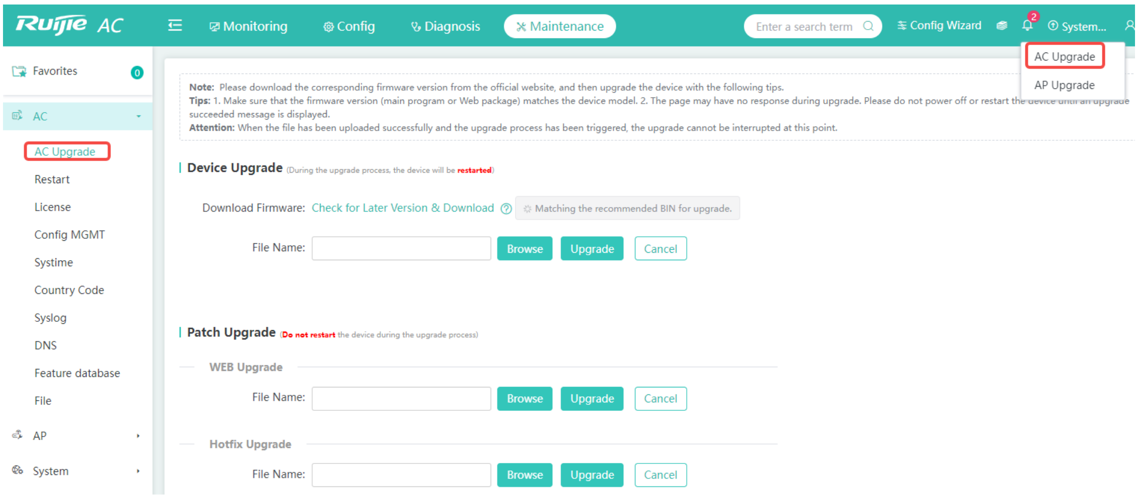
7.1 AC management

7.1.1 Upgrade

Choose **Maintenance** > **AC** > **AC Upgrade**.

Or choose **System Upgrade** > **AC Upgrade** in the navigation bar to access the **AC Upgrade** page quickly.

If the current AC version is the latest one, the following message is displayed: **The current version is the latest.**



Note: Please download the corresponding firmware version from the official website, and then upgrade the device with the following tips.
Tips: 1. Make sure that the firmware version (main program or Web package) matches the device model. 2. The page may have no response during upgrade. Please do not power off or restart the device until an upgrade succeeded message is displayed.
Attention: When the file has been uploaded successfully and the upgrade process has been triggered, the upgrade cannot be interrupted at this point.

Device Upgrade (During the upgrade process, the device will be **restarted**)

Download Firmware: Check for Later Version & Download ⓘ Matching the recommended BIN for upgrade.

File Name:

Patch Upgrade (**Do not restart** the device during the upgrade process)

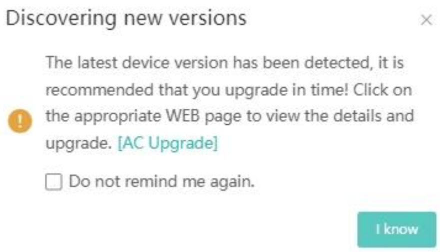
WEB Upgrade

File Name:

Hotfix Upgrade

File Name:

If the current AC or AP can be upgraded to a later version, a dialog box prompting version upgrade will pop up when you access the AC page. Click **AC Upgrade** to access the **AC Upgrade** page.

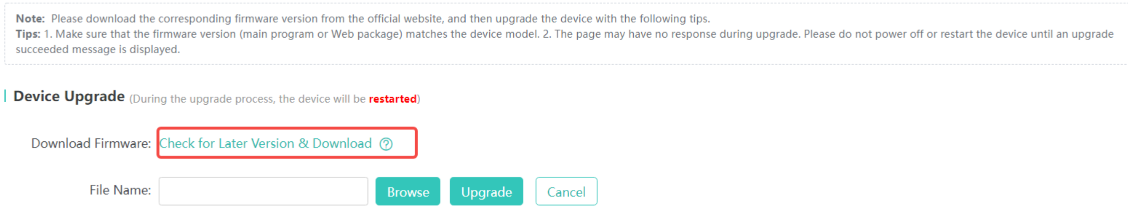


Discovering new versions

The latest device version has been detected, it is recommended that you upgrade in time! Click on the appropriate WEB page to view the details and upgrade. [AC Upgrade]

□ Do not remind me again.

Click **Check for Later Version & Download** to check whether a later version is available.



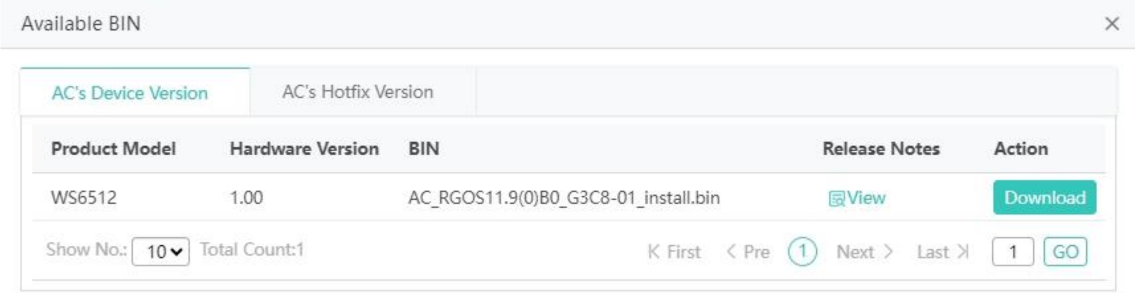
Note: Please download the corresponding firmware version from the official website, and then upgrade the device with the following tips.
Tips: 1. Make sure that the firmware version (main program or Web package) matches the device model. 2. The page may have no response during upgrade. Please do not power off or restart the device until an upgrade succeeded message is displayed.

Device Upgrade (During the upgrade process, the device will be **restarted**)

Download Firmware: Check for Later Version & Download ⓘ

File Name:

If a later version is available, click **Download** for **AC's Device Version** or **AC's Hotfix Version** to download the bin file.



Available BIN

AC's Device Version | AC's Hotfix Version

Product Model	Hardware Version	BIN	Release Notes	Action
WS6512	1.00	AC_RGOS11.9(0)B0_G3C8-01_install.bin	View	Download

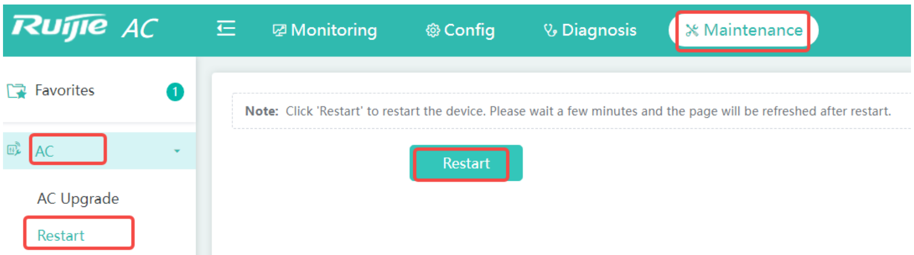
Show No.: 10 Total Count:1

Click **OK** to download the file to the local computer. You will be automatically redirected to the **AC Upgrade** page.

7.1.2 Restart

Choose **Maintenance** > **AC** > **Restart**.

Click **Restart** to restart the current AC.



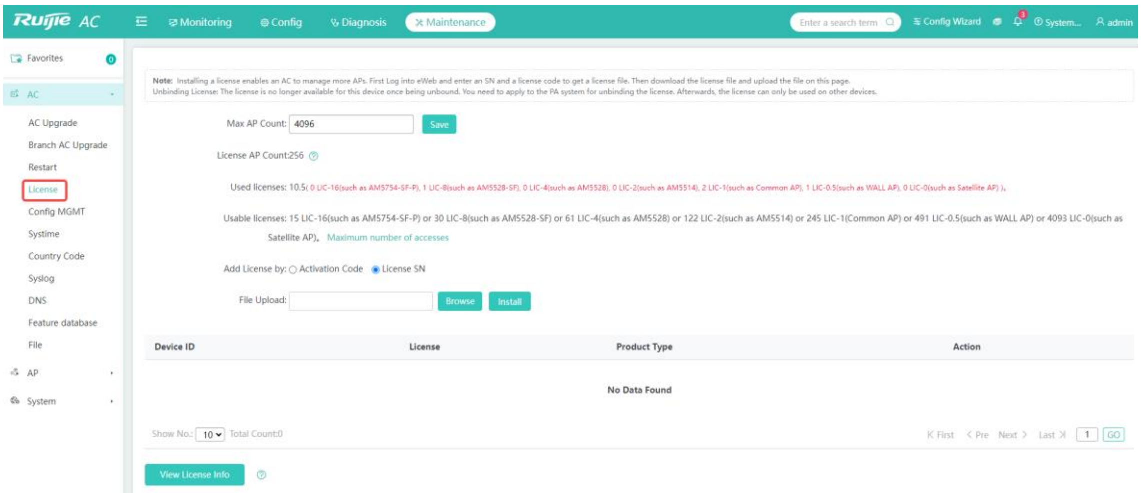
Note: Click 'Restart' to restart the device. Please wait a few minutes and the page will be refreshed after restart.

7.1.3 License Management

Choose **Maintenance** > **AC** > **License**.

The **License** feature protects the legitimate rights and interests of authorized users. It is used to control the maximum number of APs supported on the AC. The supported maximum number of APs and license type vary with devices. The specifications of a license also vary with the license types. The actual license shall prevail.

Licenses can be managed through the activation code and the authorization file.



Note: Installing a license enables an AC to manage more APs. First Log into eWeb and enter an SN and a license code to get a license file. Then download the license file and upload the file on this page.
Unbinding License: The license is no longer available for this device once being unbound. You need to apply to the PA system for unbinding the license. Afterwards, the license can only be used on other devices.

Max AP Count: 4096

License AP Count:256

Used licenses: 10.5(0 LIC-16(such as AM5754-SF-P), 1 LIC-8(such as AM5528-SF), 0 LIC-4(such as AM5528), 0 LIC-2(such as AM5514), 2 LIC-1(such as Common AP), 1 LIC-0.5(such as WALL AP), 0 LIC-0(such as Satellite AP)),

Usable licenses: 15 LIC-16(such as AM5754-SF-P) or 30 LIC-8(such as AM5528-SF) or 61 LIC-4(such as AM5528) or 122 LIC-2(such as AM5514) or 245 LIC-1(Common AP) or 491 LIC-0.5(such as WALL AP) or 4093 LIC-0(such as Satellite AP)。 Maximum number of accesses

Add License by: ○ Activation Code ● License SN

File Upload:

Device ID	License	Product Type	Action
No Data Found			

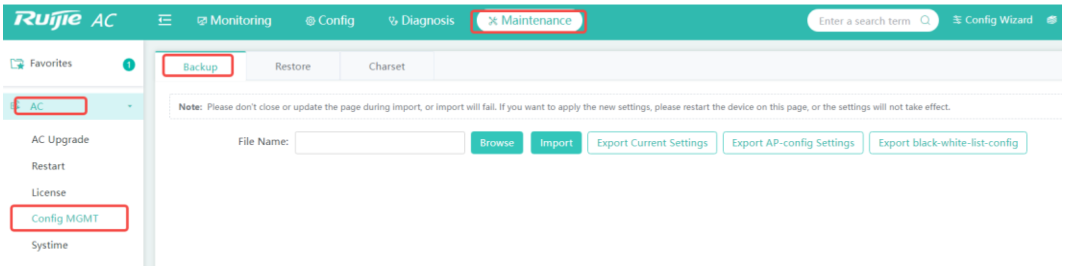
Show No.: 10 Total Count:0 First Pre Next Last 1 GO

7.1.4 Configuration Management

Choose **Maintenance** > **AC** > **Config MGMT**.

1. Backup

You can back up the configuration file on the device and import or export configurations to perform batch operations on the configurations, thereby facilitating user operations.

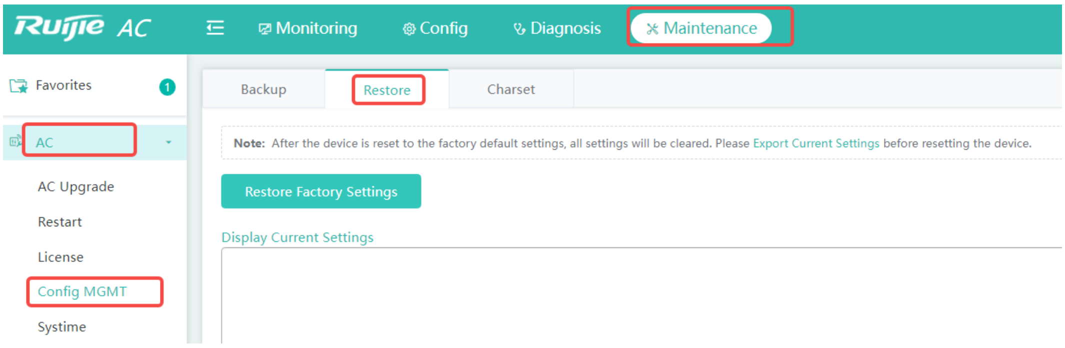


Note: Please don't close or update the page during import, or import will fail. If you want to apply the new settings, please restart the device on this page, or the settings will not take effect.

File Name:

2. Restore

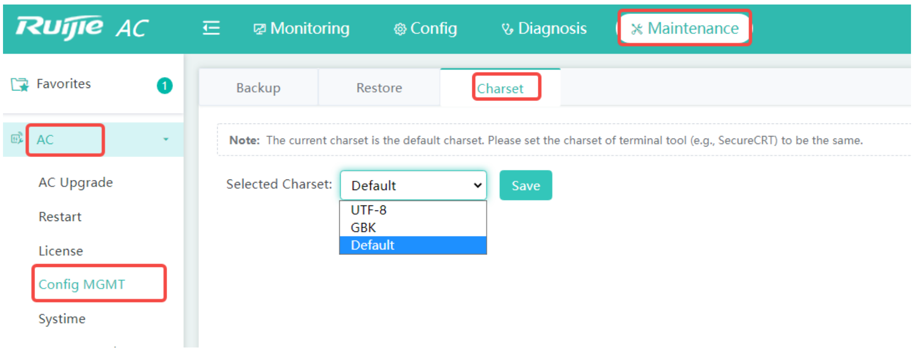
You can clear the configurations to restore the system to the initial state. You need to use the IP address in the factory settings to access the web system. Restoring factory settings will delete all configurations. Therefore, exercise caution when performing this operation.



Note: After the device is reset to the factory default settings, all settings will be cleared. Please Export Current Settings before resetting the device.

3. Charset

The system charset can be set to GBK or UTF-8. The UTF-8 is used for the web system by default. You are advised to keep the system charset on the SecureCRT or other client tools consistent with the charset on the system. Otherwise, garbled and hybrid characters may occur.



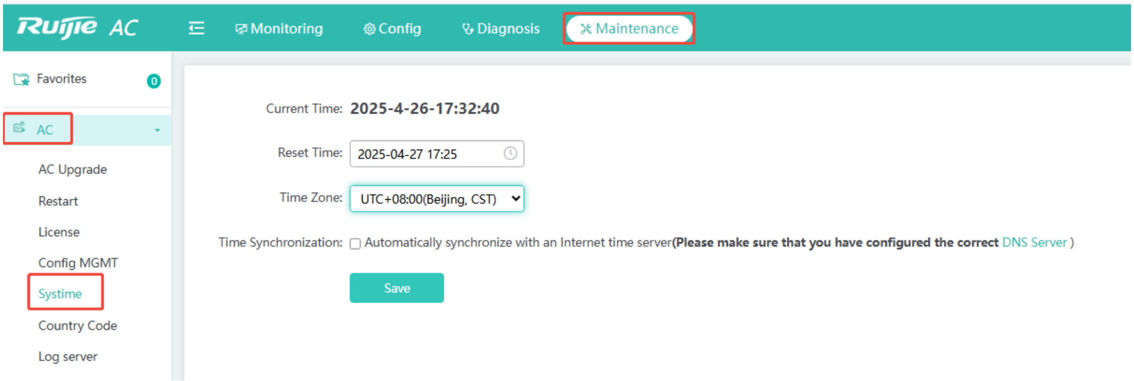
Note: The current charset is the default charset. Please set the charset of terminal tool (e.g., SecureCRT) to be the same.

Selected Charset: Default

7.1.5 System Time

Choose **Maintenance** > **AC** > **Systime**.

You can set the system time of the time zone where the device is located so that the device information is accurate.



Current Time: 2025-4-26-17:32:40

Reset Time: 2025-04-27 17:25

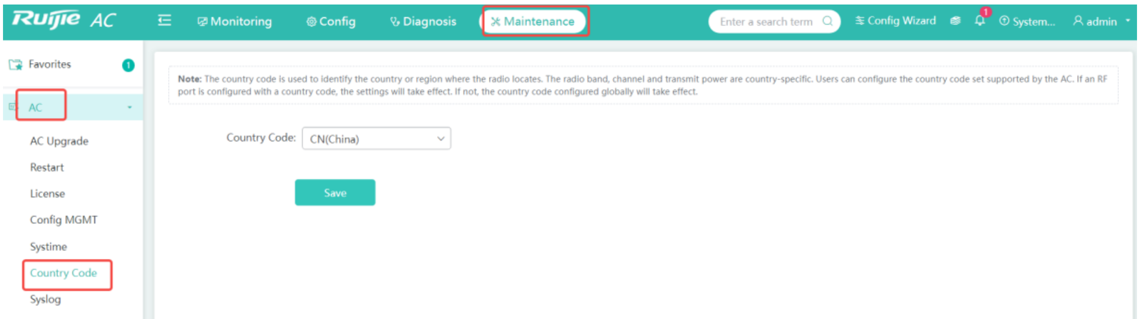
Time Zone: UTC+08:00(Beijing, CST)

Time Synchronization: □ Automatically synchronize with an Internet time server**(Please make sure that you have configured the correct** DNS Server)

7.1.6 Country Code

Choose **Maintenance** > **AC** > **Country Code**.

You can set the country or region where the device is located. The required radio, channel, and power are subject to different countries or regions.



Note: The country code is used to identify the country or region where the radio locates. The radio band, channel and transmit power are country-specific. Users can configure the country code set supported by the AC. If an RF port is configured with a country code, the settings will take effect. If not, the country code configured globally will take effect.

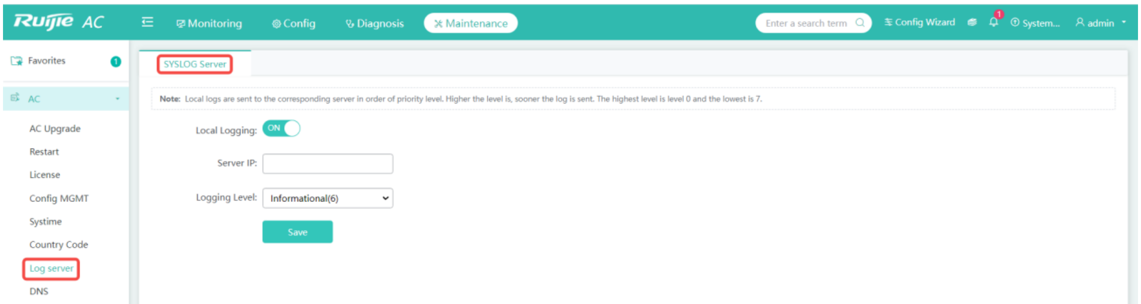
Country Code: CN(China)

7.1.7 Log Server

Choose **Maintenance** > **AC** > **Log server**.

1. Syslog Server

After the syslog server is configured, the device can be configured to send local logs to the server for storage and easy query.



Note: Local logs are sent to the corresponding server in order of priority level. Higher the level is, sooner the log is sent. The highest level is level 0 and the lowest is 7.

Local Logging: ON

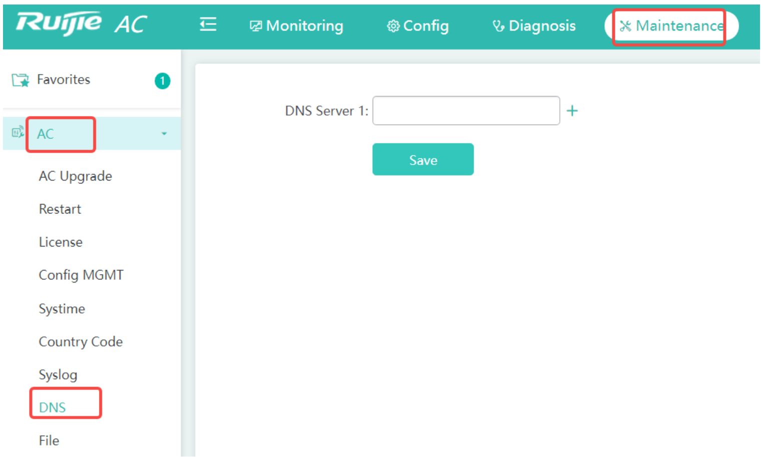
Server IP:

Logging Level: Informational(6)

7.1.8 DNS

Choose **Maintenance** > **AC** > **DNS**.

To implement dynamic domain name resolution, a DNS server must be configured.

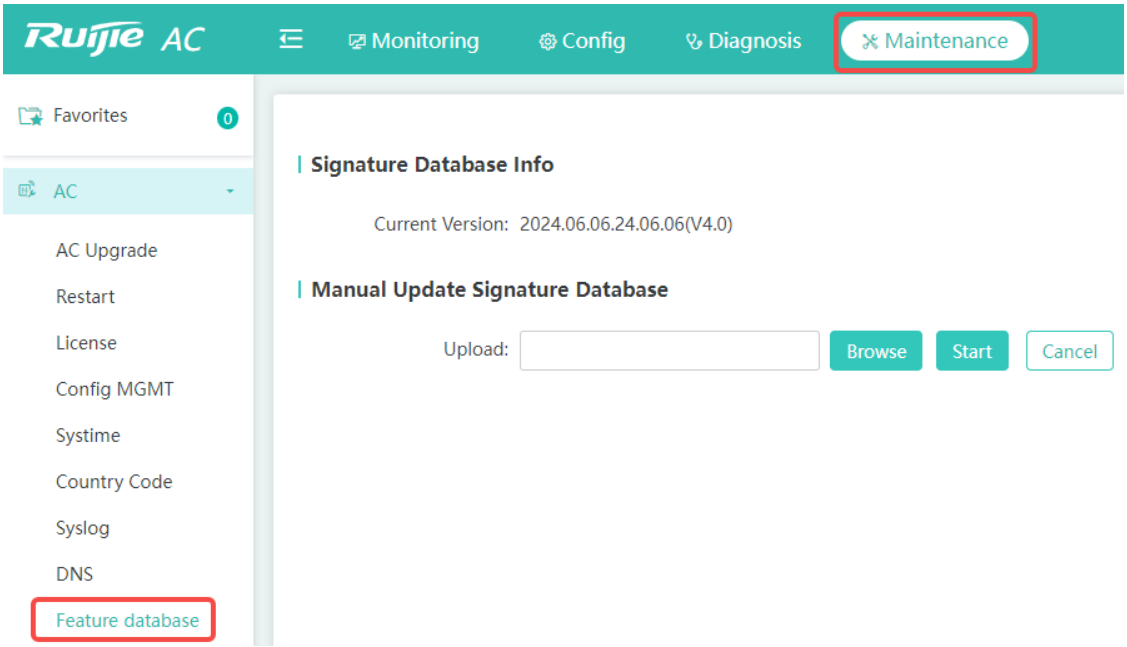


DNS Server 1:

7.1.9 Feature Database

Choose **Maintenance** > **AC** > **Feature database**.

The application identification feature database is updated constantly. You can update the feature database on this page. Click **Browse**, upload the feature database, and click **Start** to update the feature database.



Signature Database Info

Current Version: 2024.06.06.24.06.06(V4.0)

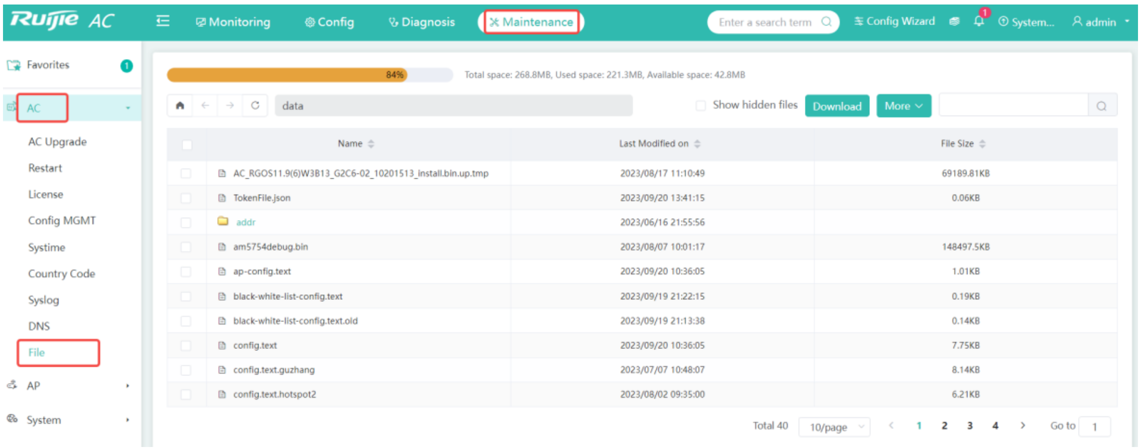
Manual Update Signature Database

Upload:

7.1.10 File Management

Choose **Maintenance** > **AC** > **File**.

The **File** feature is used to manage files in the **data** directory, including software installation packages, debugging log files, and configuration files. The overall storage space, used storage space, and remaining storage space of a device are displayed to facilitate proper management of the device memory. The file management list includes file name, modification date, and file size. Files can be ranked based on the file name, modification date, and file size. The number of file records displayed on each page can be configured.



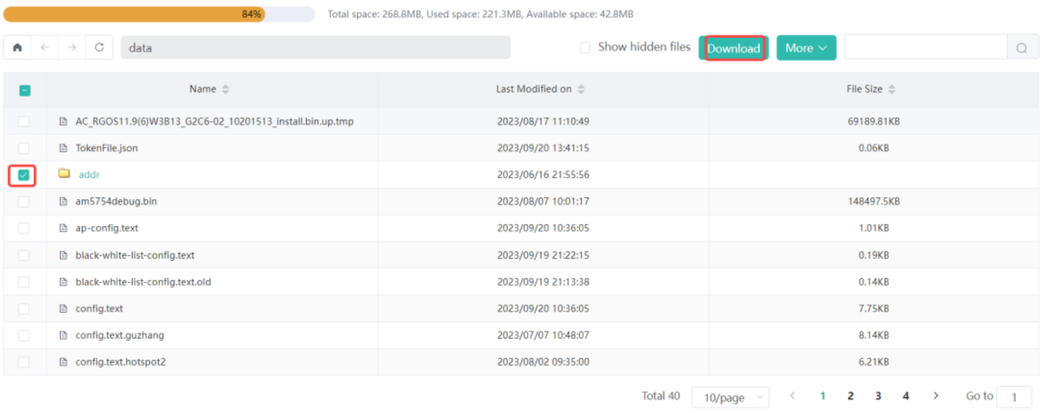
Total space: 268.8MB, Used space: 221.3MB, Available space: 42.8MB

data

	Name	Last Modified on	File Size
□	AC_RGOS11.9(6)W3B13_G2C6-02_10201513_install.bin.up.tmp	2023/08/17 11:10:49	69189.81KB
□	TokenFile.json	2023/09/20 13:41:15	0.06KB
□	addr	2023/06/16 21:55:56	
□	am5754debug.bin	2023/08/07 10:01:17	148497.5KB
□	ap-config.text	2023/09/20 10:36:05	1.01KB
□	black-white-list-config.text	2023/09/19 21:22:15	0.19KB
□	black-white-list-config.text.old	2023/09/19 21:13:38	0.14KB
□	config.text	2023/09/20 10:36:05	7.75KB
□	config.text.guzhang	2023/07/07 10:48:07	8.14KB
□	config.text.hotspot2	2023/08/02 09:35:00	6.21KB

Total 40 10/page < 1 2 3 4 > Go to 1

(1) Download a file: Tick the folder. Click **Download** to download the file on the AC to the local computer.



Total space: 268.8MB, Used space: 221.3MB, Available space: 42.8MB

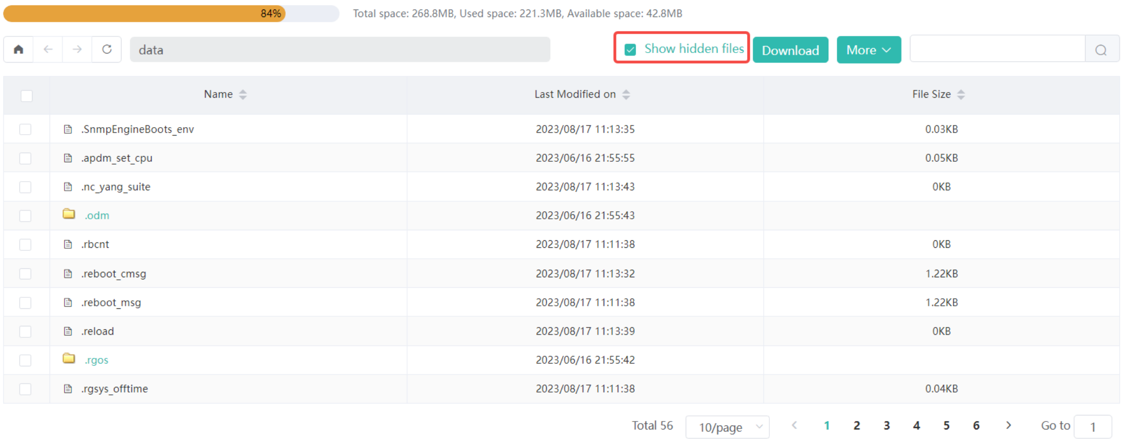
data

□ Show hidden files

	Name	Last Modified on	File Size
□	AC_RGOS11.9(6)W3B13_G2C6-02_10201513_install.bin.up.tmp	2023/08/17 11:10:49	69189.81KB
□	TokenFile.json	2023/09/20 13:41:15	0.06KB
☑	addr	2023/06/16 21:55:56	
□	am5754debug.bin	2023/08/07 10:01:17	148497.5KB
□	ap-config.text	2023/09/20 10:36:05	1.01KB
□	black-white-list-config.text	2023/09/19 21:22:15	0.19KB
□	black-white-list-config.text.old	2023/09/19 21:13:38	0.14KB
□	config.text	2023/09/20 10:36:05	7.75KB
□	config.text.guzhang	2023/07/07 10:48:07	8.14KB
□	config.text.hotspot2	2023/08/02 09:35:00	6.21KB

Total 40 10/page < 1 2 3 4 > Go to 1

(2) Show hidden files: Tick **Show hidden files** to display the hidden files on the file system.



Total space: 268.8MB, Used space: 221.3MB, Available space: 42.8MB

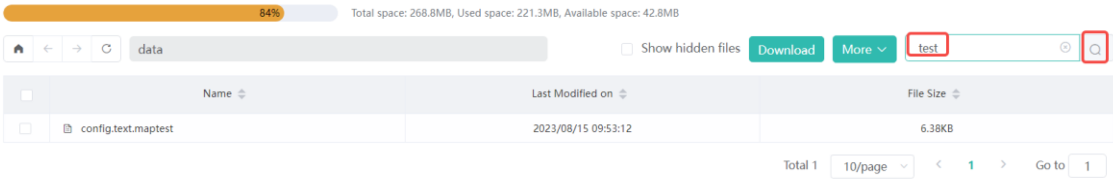
data

☑ Show hidden files

	Name	Last Modified on	File Size
□	.SnmpEngineBoots_env	2023/08/17 11:13:35	0.03KB
□	.apdm_set_cpu	2023/06/16 21:55:55	0.05KB
□	.nc_yang_suite	2023/08/17 11:13:43	0KB
□	.odm	2023/06/16 21:55:43	
□	.rbcnt	2023/08/17 11:11:38	0KB
□	.reboot_cmsg	2023/08/17 11:13:32	1.22KB
□	.reboot_msg	2023/08/17 11:11:38	1.22KB
□	.reload	2023/08/17 11:13:39	0KB
□	.rgos	2023/06/16 21:55:42	
□	.rgsys_offtime	2023/08/17 11:11:38	0.04KB

Total 56 10/page < 1 2 3 4 5 6 > Go to 1

(3) Search for a file: Enter the keyword of a file/file name in the search box. Click the search icon.



Total space: 268.8MB, Used space: 221.3MB, Available space: 42.8MB

data

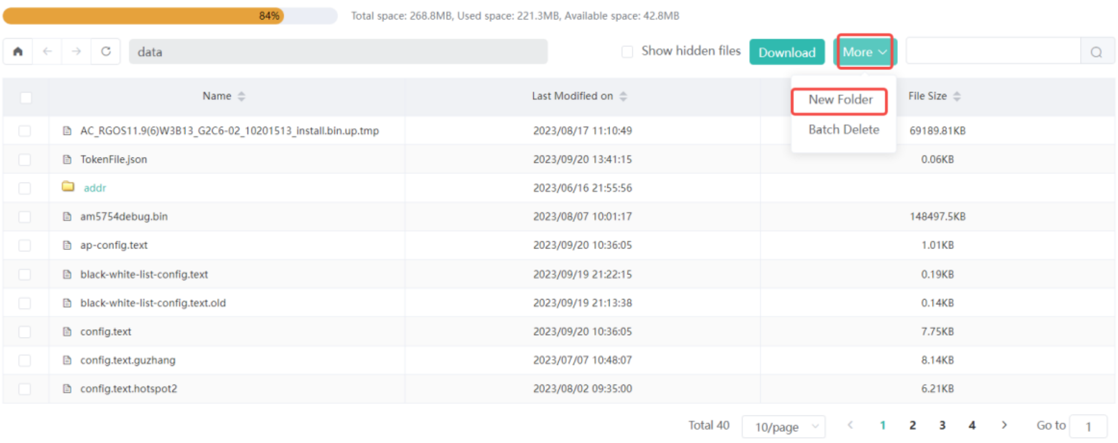
□ Show hidden files

test

	Name	Last Modified on	File Size
□	config.text.maptest	2023/08/15 09:53:12	6.38KB

Total 1 10/page < 1 > Go to 1

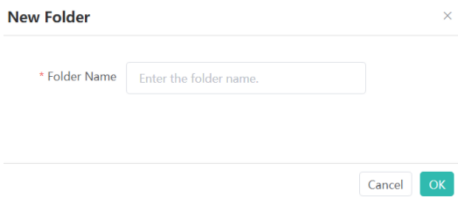
(4) Create a folder: Click the **More** drop-down list and select **New Folder**. Enter the folder name and click **OK**.



Total space: 268.8MB, Used space: 221.3MB, Available space: 42.8MB

Name	Last Modified on	File Size
AC_RGOS11.9(6)W3B13_G2C6-02_10201513_install.bin.up.tmp	2023/08/17 11:10:49	69189.81KB
TokenFile.json	2023/09/20 13:41:15	0.06KB
addr	2023/06/16 21:55:56	
am5754debug.bin	2023/08/07 10:01:17	148497.5KB
ap-config.text	2023/09/20 10:36:05	1.01KB
black-white-list-config.text	2023/09/19 21:22:15	0.19KB
black-white-list-config.text.old	2023/09/19 21:13:38	0.14KB
config.text	2023/09/20 10:36:05	7.75KB
config.text.guzhang	2023/07/07 10:48:07	8.14KB
config.text.hotspot2	2023/08/02 09:35:00	6.21KB

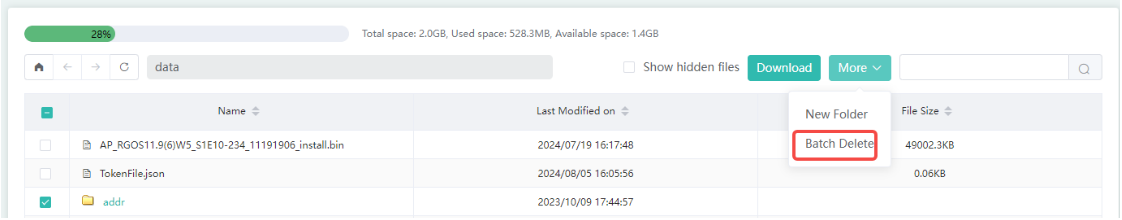
Total 40



New Folder

* Folder Name: Enter the folder name.

(5) Delete files and folders: Select the files and folders to be deleted, click **More**, and select **Batch Delete**. In the dialog box that is displayed, click **OK** to delete the files and folders.



Total space: 2.0GB, Used space: 528.3MB, Available space: 1.4GB

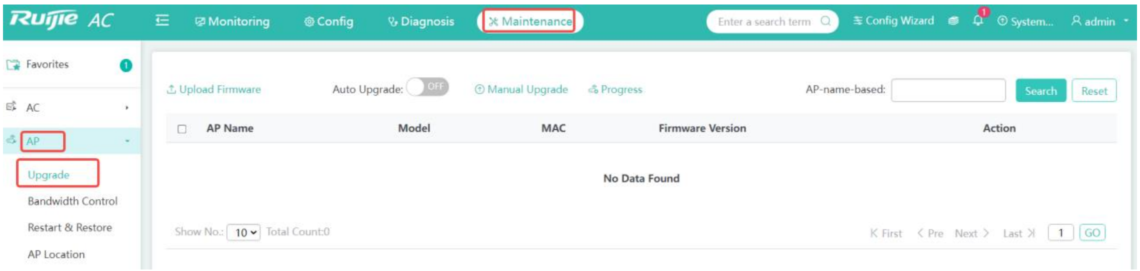
	Name	Last Modified on	File Size
□	AP_RGOS11.9(6)W5_S1E10-234_11191906_install.bin	2024/07/19 16:17:48	49002.3KB
□	TokenFile.json	2024/08/05 16:05:56	0.06KB
☑	addr	2023/10/09 17:44:57	

7.2 AP management

7.2.1 Upgrade

Choose **Maintenance** > **AP** > **Upgrade**.

Multiple APs can be managed on the AC through the web system, which is quick and convenient.



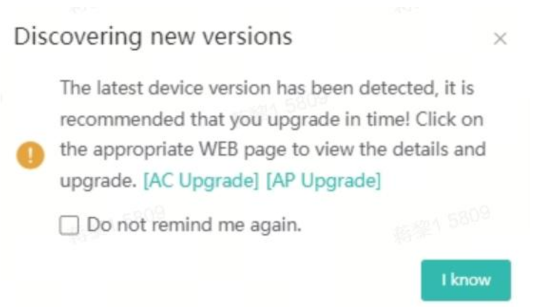
Auto Upgrade: OFF

□	AP Name	Model	MAC	Firmware Version	Action

No Data Found

Show No.: 10 Total Count:0

If the current AC or AP can be upgraded to a later version, a dialog box prompting version upgrade will pop up when you access the AC page. Click **AP Upgrade** to access the **AP Upgrade** page.

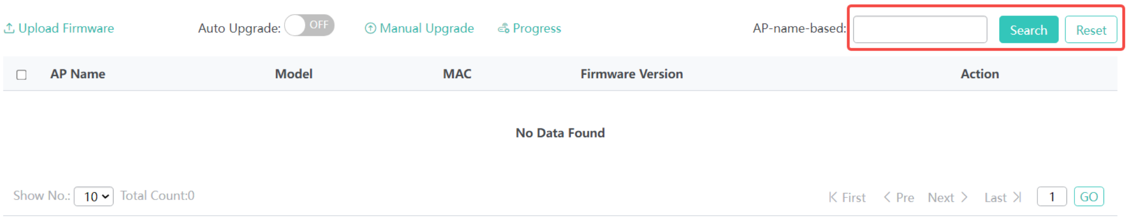


Discovering new versions

The latest device version has been detected, it is recommended that you upgrade in time! Click on the appropriate WEB page to view the details and upgrade. [AC Upgrade] [AP Upgrade]

□ Do not remind me again.

(1) Search for an AP: If there are a large number of APs on the page, you can search for a specified AP by the AP name in the upper right corner of the page. Click **Reset** to clear the content in the search box.



□	AP Name	Model	MAC	Firmware Version	Action

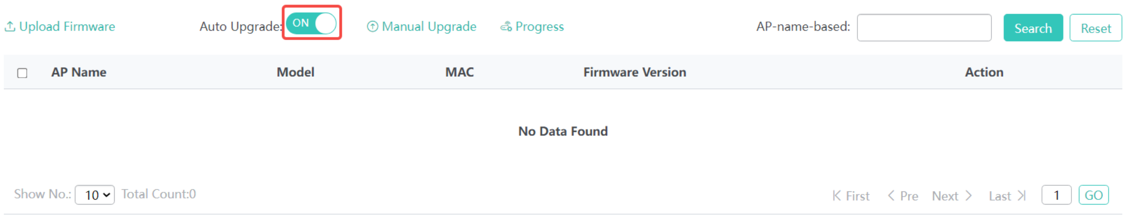
No Data Found

Show No.: 10 Total Count:0

(2) Automatic upgrade: You can toggle on **Auto Upgrade**. The AP will be automatically upgraded to the latest version when a later version is available.

Note

Before upgrading APs on the AC, ensure that the APs can ping each other. Otherwise, the distributed upgrade may fail, which may prolong the upgrade process.

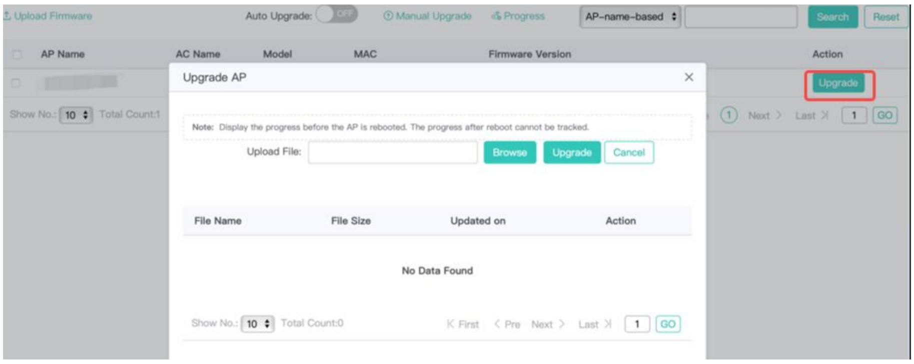


□	AP Name	Model	MAC	Firmware Version	Action

No Data Found

Show No.: 10 Total Count:0

(3) Single AP upgrade: Click **Upgrade** next to an AP. Upload the AP upgrade file and click **Upgrade**.



Upgrade AP

Note: Display the progress before the AP is rebooted. The progress after reboot cannot be tracked.

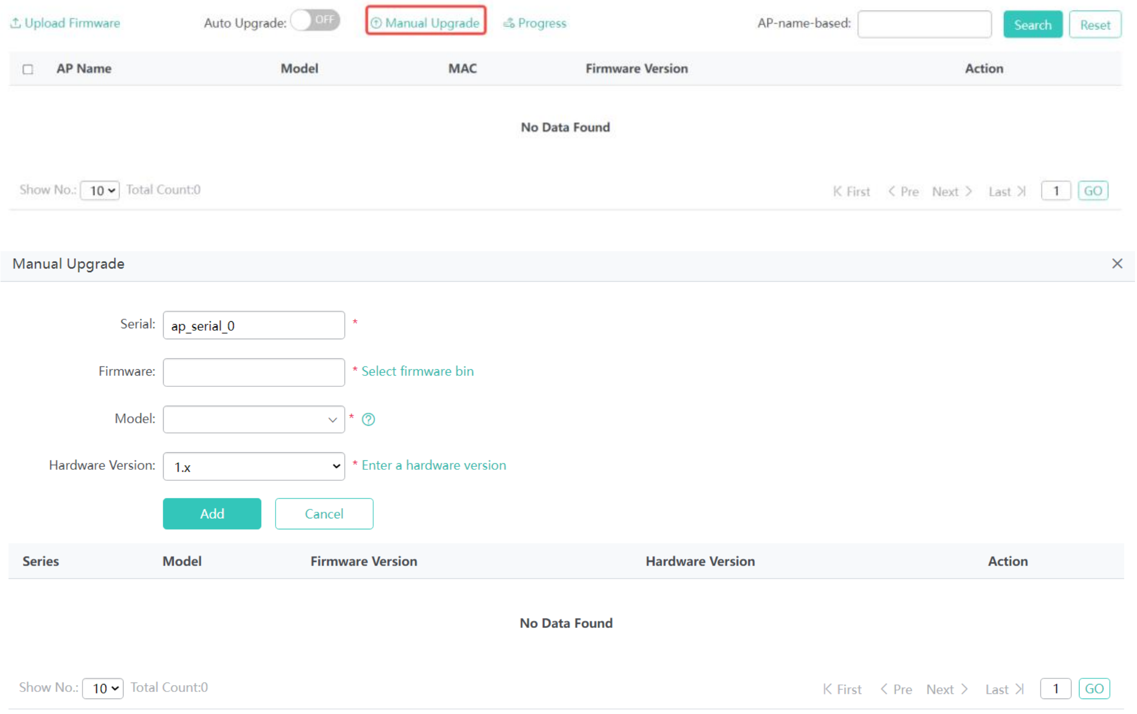
Upload File:

File Name	File Size	Updated on	Action

No Data Found

Show No.: 10 Total Count:0

(4) Manual upgrade: Click **Manual Upgrade** to access the **Manual Upgrade** page. Add APs as prompted. After the APs go online, the system automatically detects the AP versions and completes the upgrade.



□ AP Name	Model	MAC	Firmware Version	Action
No Data Found				

Manual Upgrade

Serial: ap_serial_0 *

Firmware: * Select firmware bin

Model: *

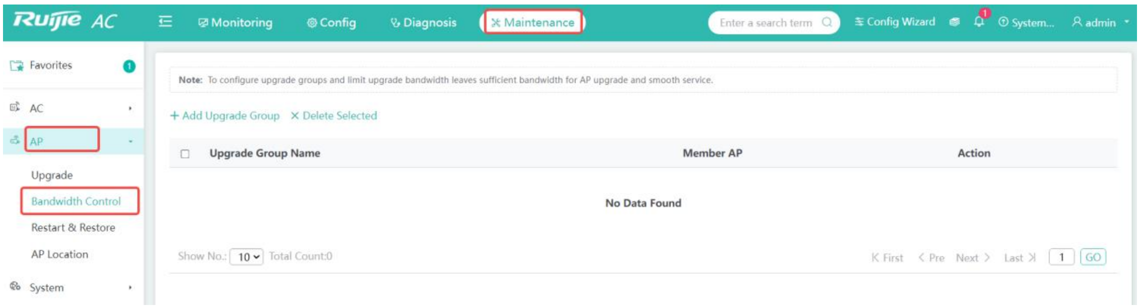
Hardware Version: 1.x * Enter a hardware version

Series	Model	Firmware Version	Hardware Version	Action
No Data Found				

7.2.2 Bandwidth Control

Choose **Maintenance** > **AP** > **Bandwidth Control**.

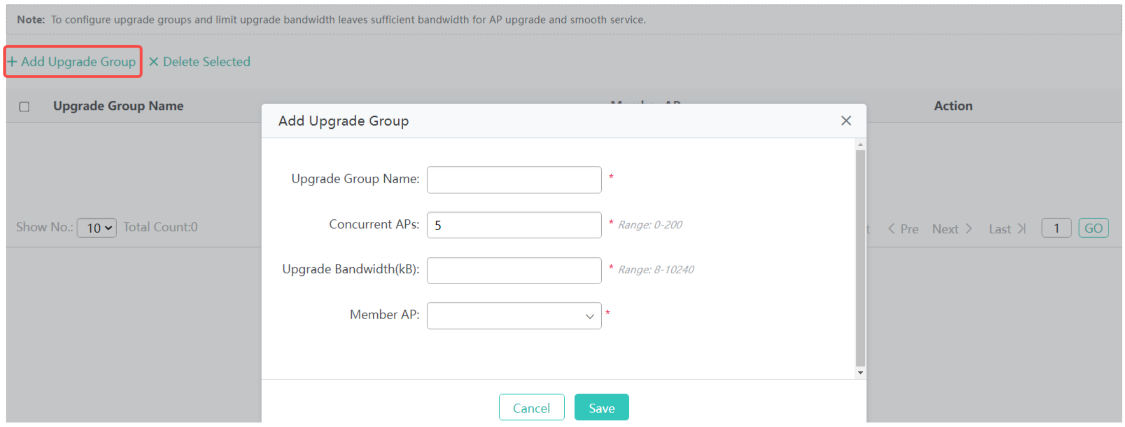
By configuring the upgrade group and limiting the upgrade bandwidth, sufficient bandwidth is reserved when the AP is being upgraded, so that network performance will not be greatly affected by the AP upgrade.



Note: To configure upgrade groups and limit upgrade bandwidth leaves sufficient bandwidth for AP upgrade and smooth service.

□ Upgrade Group Name	Member AP	Action
No Data Found		

(1) Add an upgrade group: Click **Add Upgrade Group**. Edit the fields in the pop-up dialog box. Click **Save**. A message indicating the configuration has been saved is displayed. The newly added upgrade group is displayed in the upgrade group list.



Note: To configure upgrade groups and limit upgrade bandwidth leaves sufficient bandwidth for AP upgrade and smooth service.

Add Upgrade Group

Upgrade Group Name: *

Concurrent APs: 5 * Range: 0-200

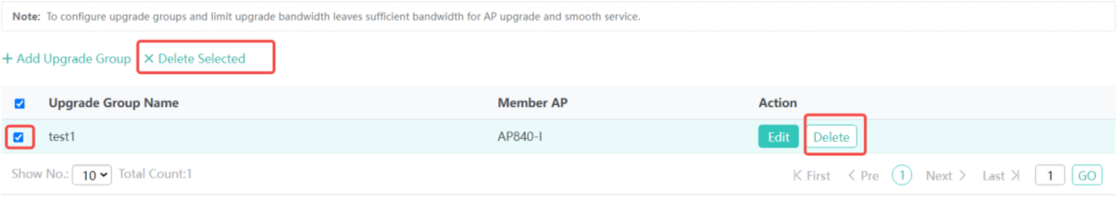
Upgrade Bandwidth(kB): * Range: 8-10240

Member AP: *

Show No.: 10 Total Count:0

Parameter	Description
Upgrade Group Name	Specifies the name of an upgrade group name.
Concurrent APs	Specifies the number of APs being upgraded concurrently.
Upgrade Bandwidth(kB)	Specifies the bandwidth for AP upgrade.
Member AP	Specifies the member APs in the upgrade group.

(2) Delete an upgrade group: Click **Delete** in the **Action** column of an upgrade group. In the dialog box that is displayed, click **OK**. To delete multiple upgrade groups, select the upgrade groups to be deleted in the list, and click **Delete Selected**. In the dialog box that is displayed, click **OK**.

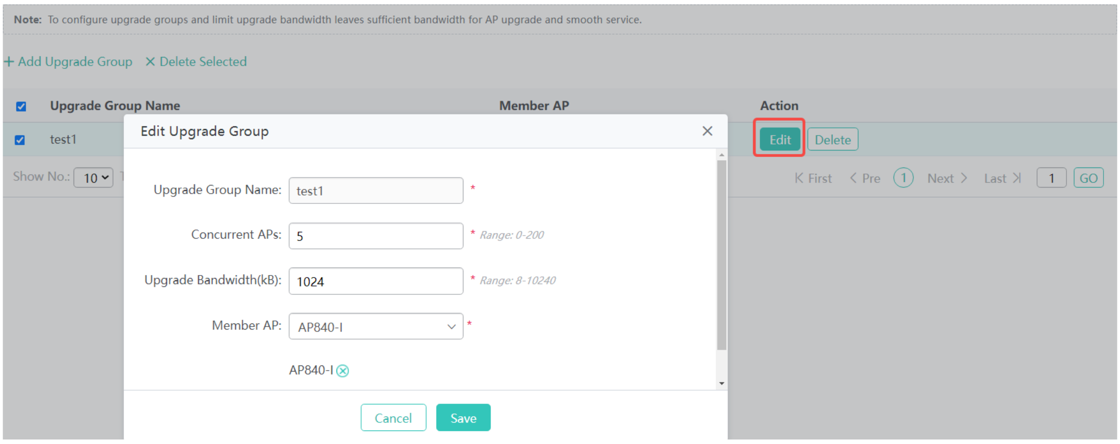


Note: To configure upgrade groups and limit upgrade bandwidth leaves sufficient bandwidth for AP upgrade and smooth service.

	Upgrade Group Name	Member AP	Action
☑	test1	AP840-I	Edit Delete

Show No.: 10 Total Count:1

(3) Edit an upgrade group: Click **Edit** next to an upgrade group. The pop-up dialog box displays the information about the upgrade group. You can edit the information. Click **Save**. A message indicating the configuration has been saved is displayed.



Note: To configure upgrade groups and limit upgrade bandwidth leaves sufficient bandwidth for AP upgrade and smooth service.

☑	Upgrade Group Name	Member AP	Action
☑	test1		Edit Delete

Edit Upgrade Group

Upgrade Group Name: test1 *

Concurrent APs: 5 * *Range: 0-200*

Upgrade Bandwidth(kB): 1024 * *Range: 8-10240*

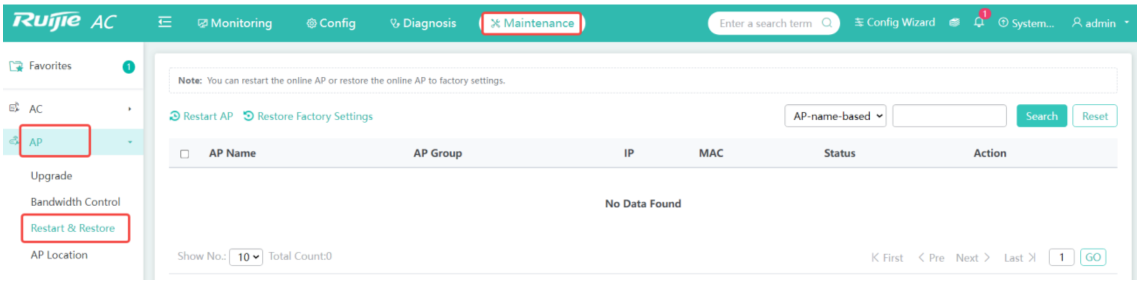
Member AP: AP840-I *

AP840-I ⊗

7.2.3 AP Restart/Restoration

Choose **Maintenance** > **AP** > **Restart & Restore**.

Restart online APs or restore them to factory settings.

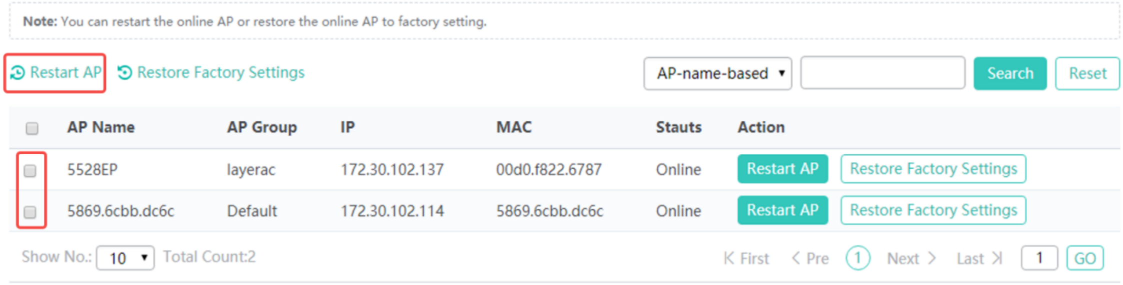


Note: You can restart the online AP or restore the online AP to factory settings.

☐	AP Name	AP Group	IP	MAC	Status	Action
			No Data Found			

Show No.: 10 Total Count:0

(1) Restart the AP: Click **Restart AP** next to an AP. If multiple APs need to be restarted, select the APs and click **Restart AP**.

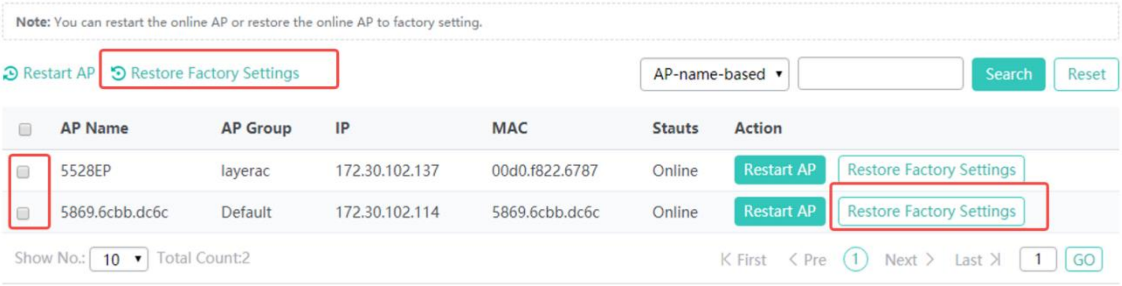


Note: You can restart the online AP or restore the online AP to factory setting.

☐	AP Name	AP Group	IP	MAC	Stauts	Action
☐	5528EP	layerac	172.30.102.137	00d0.f822.6787	Online	Restart AP Restore Factory Settings
☐	5869.6cbb.dc6c	Default	172.30.102.114	5869.6cbb.dc6c	Online	Restart AP Restore Factory Settings

Show No.: 10 Total Count:2

(2) Restore factory settings: Click **Restore Factory Settings** next to an AP. If multiple APs need to be restored to factory settings, select the APs and click **Restore Factory Settings**.



Note: You can restart the online AP or restore the online AP to factory setting.

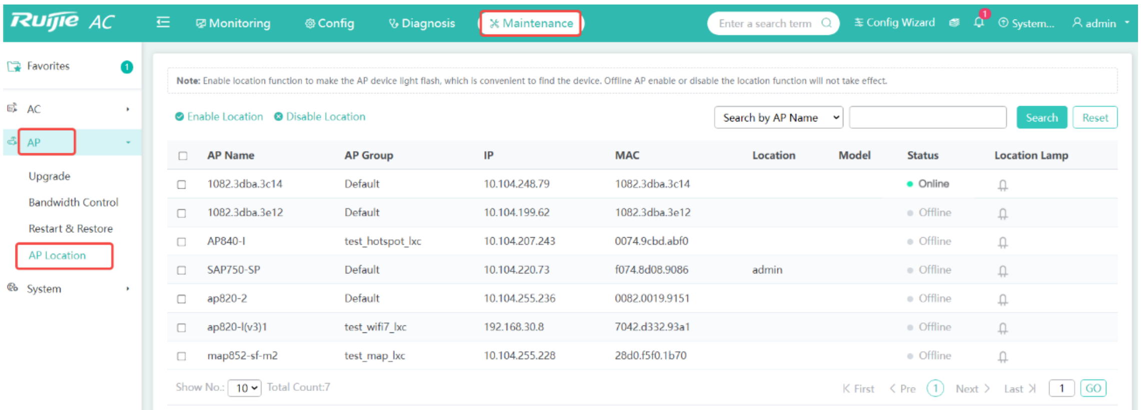
□	AP Name	AP Group	IP	MAC	Stauts	Action
□	5528EP	layerac	172.30.102.137	00d0.f822.6787	Online	Restart AP Restore Factory Settings
□	5869.6cbb.dc6c	Default	172.30.102.114	5869.6cbb.dc6c	Online	Restart AP Restore Factory Settings

Show No.: 10 Total Count:2

7.2.4 Location

Choose **Maintenance** > **AP** > **AP Location**.

When the AP Location feature is enabled, the system LED on the AP flashes to help locate the AP. If an AP goes offline, an attempt to enable or disable AP location will fail.

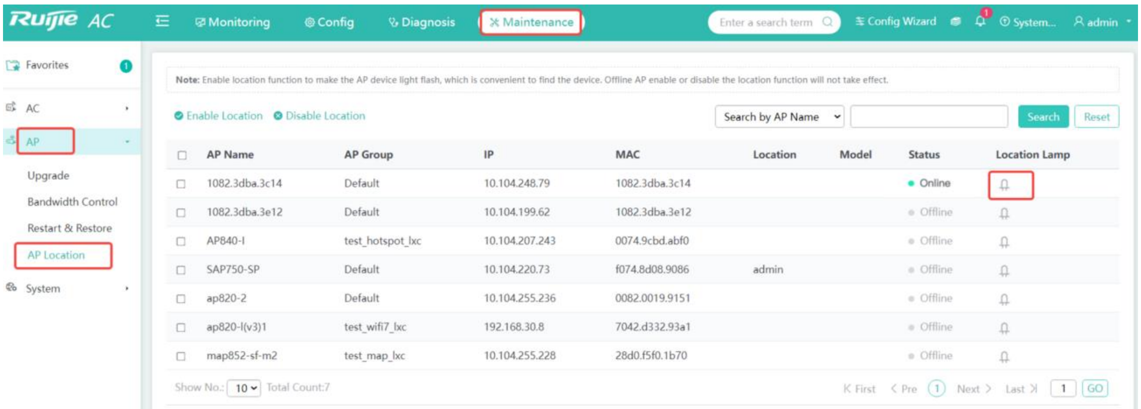


Note: Enable location function to make the AP device light flash, which is convenient to find the device. Offline AP enable or disable the location function will not take effect.

□	AP Name	AP Group	IP	MAC	Location	Model	Status	Location Lamp
□	1082.3dba.3c14	Default	10.104.248.79	1082.3dba.3c14			● Online	🔔
□	1082.3dba.3e12	Default	10.104.199.62	1082.3dba.3e12			● Offline	🔔
□	AP840-I	test_hotspot_lxc	10.104.207.243	0074.9cbd.abf0			● Offline	🔔
□	SAP750-SP	Default	10.104.220.73	f074.8d08.9086	admin		● Offline	🔔
□	ap820-2	Default	10.104.255.236	0082.0019.9151			● Offline	🔔
□	ap820-I(v3)1	test_wifi7_lxc	192.168.30.8	7042.d332.93a1			● Offline	🔔
□	map852-sf-m2	test_map_lxc	10.104.255.228	28d0.f5f0.1b70			● Offline	🔔

Show No.: 10 Total Count:7

Enable/Disable AP location: Click the location icon next to an AP to enable/disable the AP Location feature. If the AP Location feature needs to be enabled/disabled for multiple APs, select the APs and click **Enable Location** or **Disable Location**.



Note: Enable location function to make the AP device light flash, which is convenient to find the device. Offline AP enable or disable the location function will not take effect.

□	AP Name	AP Group	IP	MAC	Location	Model	Status	Location Lamp
□	1082.3dba.3c14	Default	10.104.248.79	1082.3dba.3c14			● Online	🔔
□	1082.3dba.3e12	Default	10.104.199.62	1082.3dba.3e12			● Offline	🔔
□	AP840-I	test_hotspot_lxc	10.104.207.243	0074.9cbd.abf0			● Offline	🔔
□	SAP750-SP	Default	10.104.220.73	f074.8d08.9086	admin		● Offline	🔔
□	ap820-2	Default	10.104.255.236	0082.0019.9151			● Offline	🔔
□	ap820-I(v3)1	test_wifi7_lxc	192.168.30.8	7042.d332.93a1			● Offline	🔔
□	map852-sf-m2	test_map_lxc	10.104.255.228	28d0.f5f0.1b70			● Offline	🔔

Show No.: 10 Total Count:7

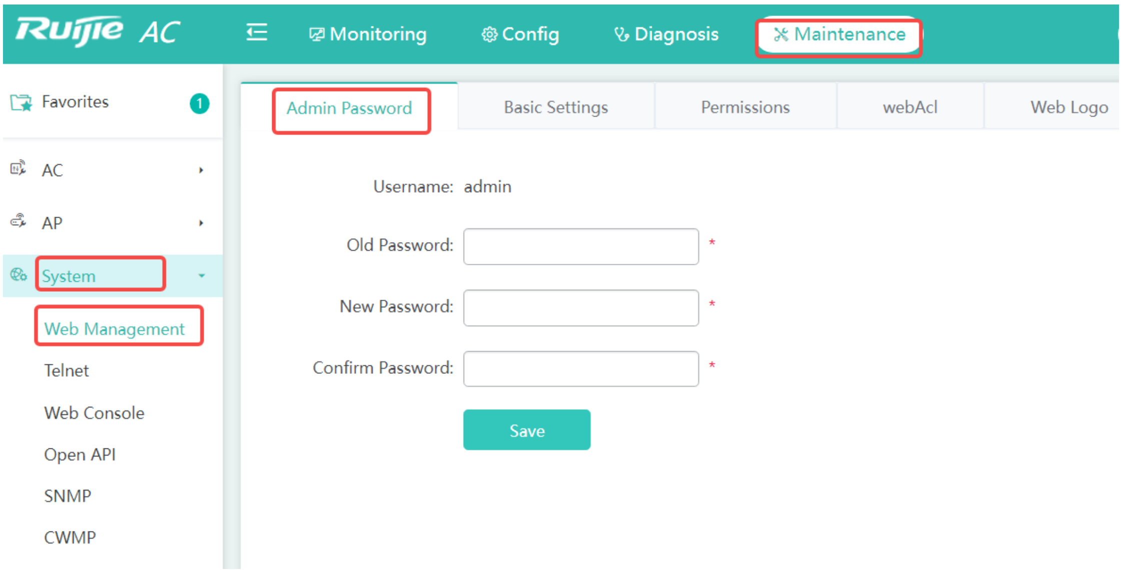
7.3 System

7.3.1 Web-based Management

Choose **Maintenance** > **System** > **Web Management**.

1. Admin Password

To enhance the system security and information interaction security, you are advised to change the default password of the system.



Username: admin

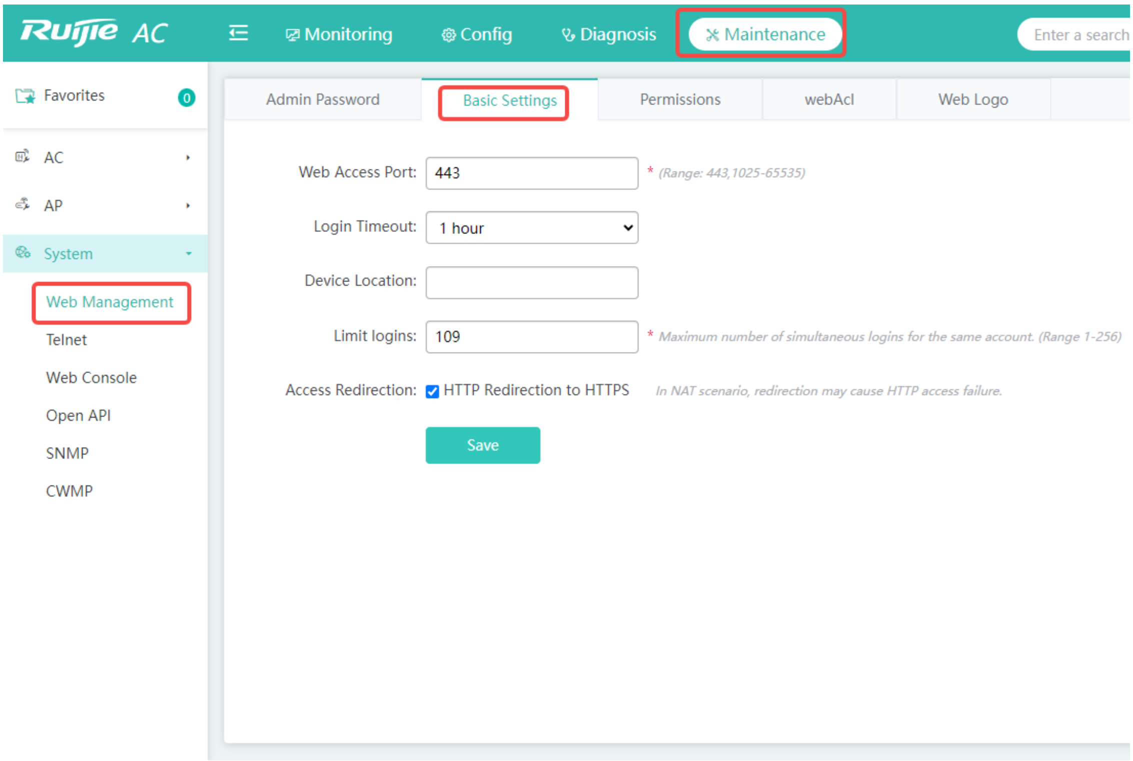
Old Password: *

New Password: *

Confirm Password: *

2. Basic Settings

To facilitate device management, you can enter the device location on the **Basic Settings** tab page. Set the web access port and login timeout period. When the login timeout period expires, you will automatically exit the web UI to ensure system security. If the device supports login limit configuration, you can set the maximum number of users who can log in to the system simultaneously using the same account (the default value is 10).



Web Access Port: 443 * (Range: 443,1025-65535)

Login Timeout: 1 hour

Device Location:

Limit logins: 109 * Maximum number of simultaneous logins for the same account. (Range 1-256)

Access Redirection: ☑ HTTP Redirection to HTTPS In NAT scenario, redirection may cause HTTP access failure.

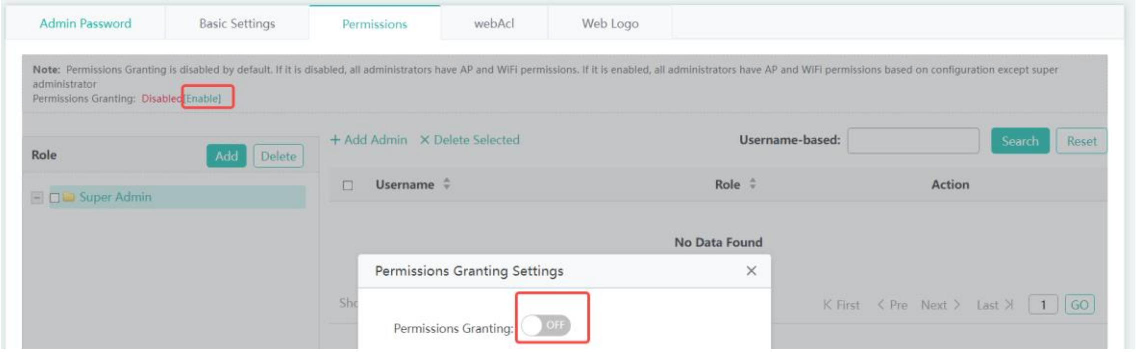
3. Permissions

To enhance system security, you can configure multiple roles for the system. Different roles can have different permissions on APs and Wi-Fi networks.

(2) Enable or disable hierarchical and decentralized management: Click **Enable** or **Disable** to enable or disable **Permissions Granting**.

Note

- **Permissions Granting** is disabled by default. When this function is disabled, all common administrators have permissions on all APs and Wi-Fi networks. When this function is enabled, all common administrators have the corresponding permissions of designated roles.
- The super administrator **admin** has all permissions by default.



Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi permissions based on configuration except super administrator

Permissions Granting: Disabled[Enable]

No Data Found

Permissions Granting Settings ×

Permissions Granting: OFF

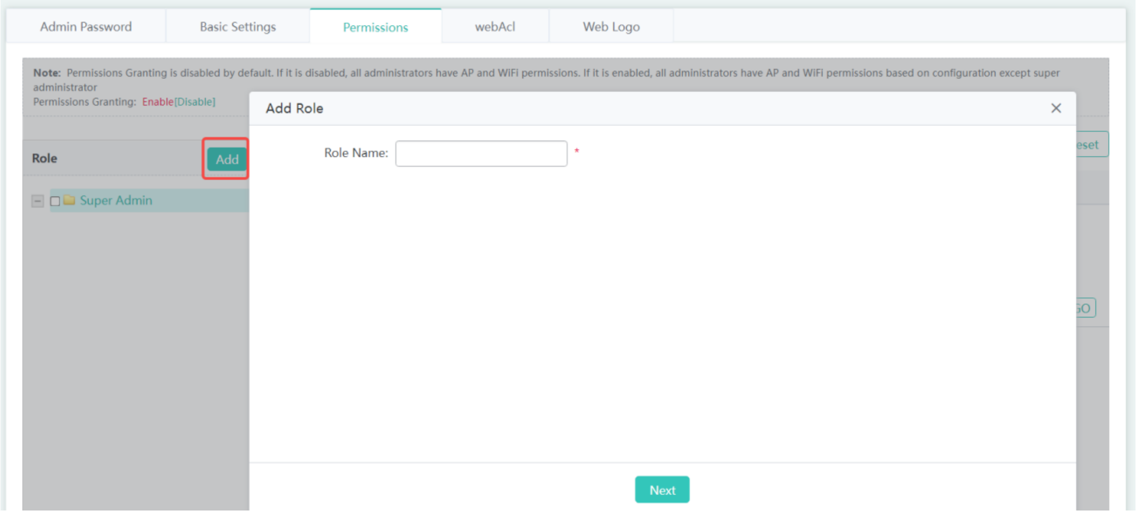
(3) Add a role: Adding a role includes three steps: adding a role, granting permissions on APs, and granting permissions on Wi-Fi networks. After **Permissions Granting** is enabled, administrators with designated roles

will have corresponding permissions on APs and Wi-Fi networks upon logging in to the web UI. The other permissions are not granted.

a Click **Add**. Enter the role name, select administrators for the role (optional), and click **Next**.

Note

When a role is created successfully, no permissions on any APs or Wi-Fi networks are granted by default.

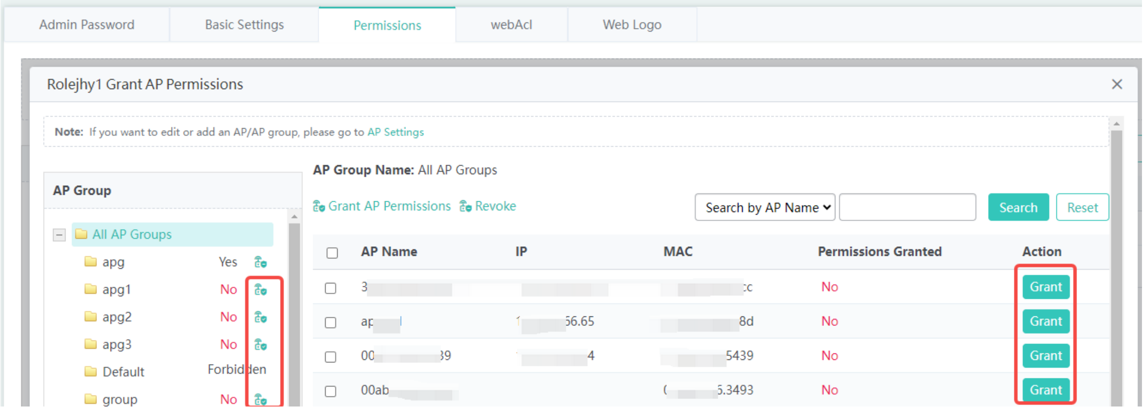


Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi permissions based on configuration except super administrator

Permissions Granting: Enable[Disable]

Role Name: ____ *

b In the **Grant AP Permissions** dialog box, grant permissions on AP groups or APs to the role, and click **Next**.



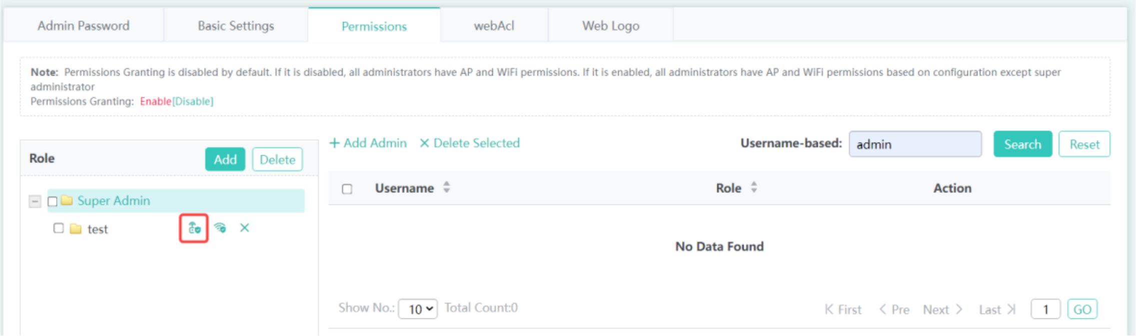
Note: If you want to edit or add an AP/AP group, please go to AP Settings

AP Group Name: All AP Groups

AP Group	
apg	Yes
apg1	No
apg2	No
apg3	No
Default	Forbidden
group	No

□	AP Name	IP	MAC	Permissions Granted	Action
□	3[redacted]	[redacted]	[redacted]c	No	Grant
□	ap[redacted]	[redacted]56.65	[redacted]8d	No	Grant
□	00[redacted]39	[redacted]4	[redacted]5439	No	Grant
□	00ab[redacted]		[redacted]5.3493	No	Grant

Alternatively, click the AP icon in the role list to grant permissions on APs.



Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi permissions based on configuration except super administrator

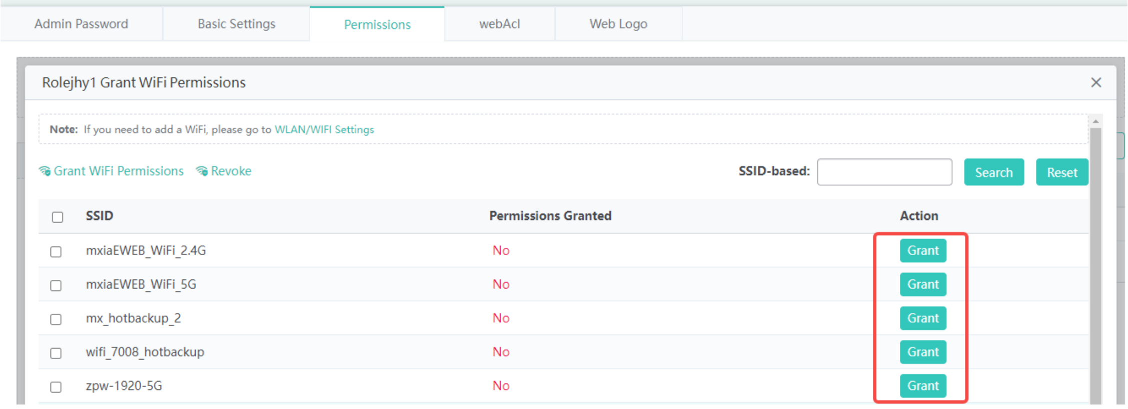
Permissions Granting: Enable[Disable]

Username-based: admin

□	Username	Role	Action
		No Data Found	

Show No.: 10 Total Count:0 1

c In the **Grant WiFi Permissions** dialog box, grant permissions on Wi-Fi networks to the role, and click **Finish**.



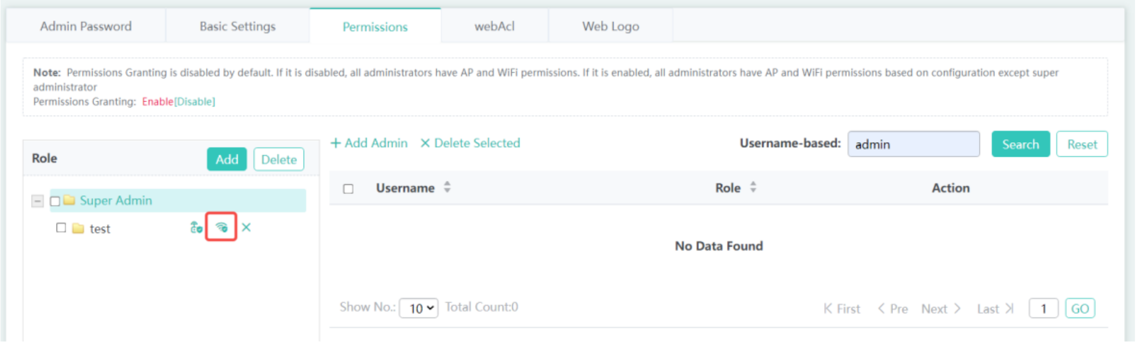
Rolejhy1 Grant WiFi Permissions

Note: If you need to add a WiFi, please go to WLAN/WIFI Settings

Grant WiFi Permissions Revoke SSID-based: Search Reset

□	SSID	Permissions Granted	Action
□	mxiaEWEB_WiFi_2.4G	No	Grant
□	mxiaEWEB_WiFi_5G	No	Grant
□	mx_hotbackup_2	No	Grant
□	wifi_7008_hotbackup	No	Grant
□	zpw-1920-5G	No	Grant

Alternatively, click the Wi-Fi icon in the role list to grant permissions on Wi-Fi networks.



Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi permissions based on configuration except super administrator

Permissions Granting: Enable[Disable]

Username-based: admin Search Reset

□	Username	Role	Action

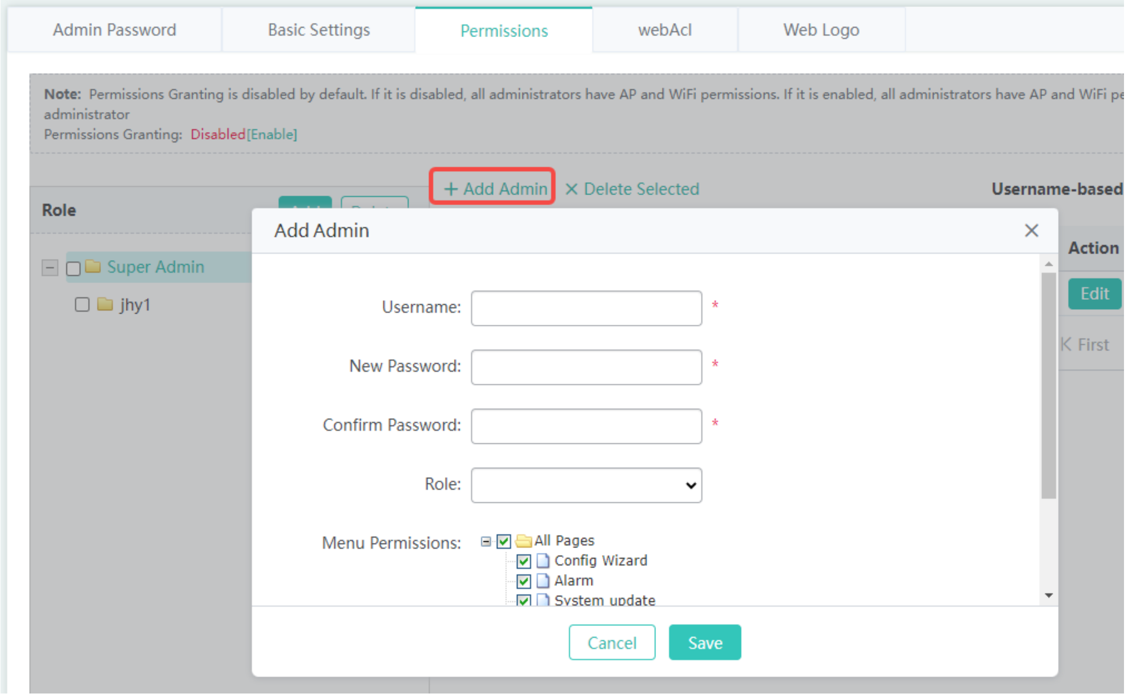
No Data Found

Show No.: 10 Total Count:0 First Pre Next Last 1 GO

(2) Add an administrator: Click **Add Admin**. Enter the username, password, and role of the administrator, select the menu permissions to be granted, and click **Save**.

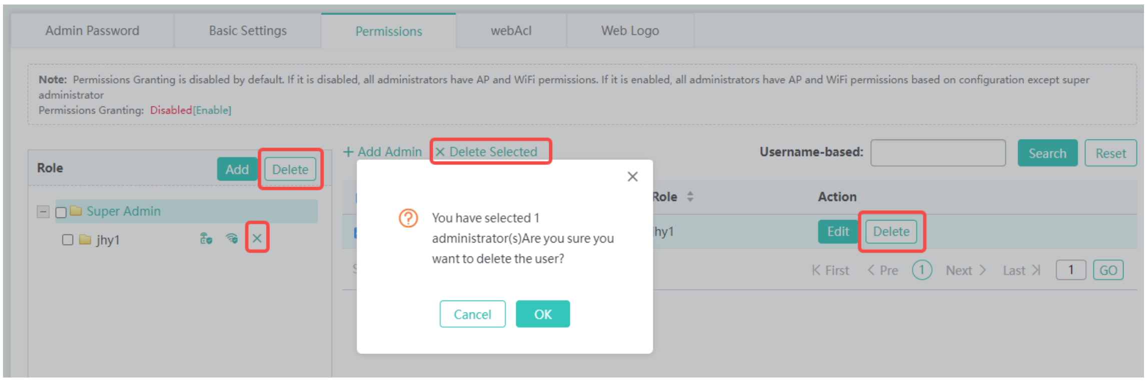
Note

When **Permissions Granting** is enabled, all common administrators have the corresponding permissions of designated roles.



Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi pe
administrator
Permissions Granting: Disabled[Enable]

(3) Delete a role or administrator: Click **Delete** in the **Action** column of a role or administrator. Alternatively, select roles and administrators and click **Delete Selected**. In the dialog box that is displayed, click **OK**.

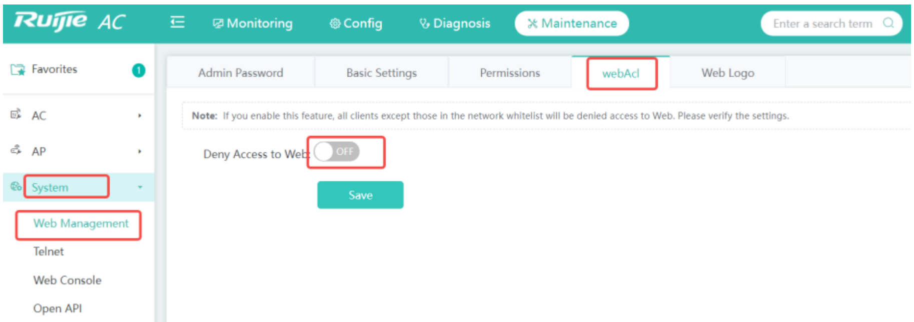


Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi permissions based on configuration except super administrator
Permissions Granting: Disabled[Enable]

You have selected 1 administrator(s)Are you sure you want to delete the user?

4. Web Access Permission Management

This feature is used to manage login permissions for the web system. When **Deny Access to Web** is enabled, addresses that are not on the authorized network segments cannot be used to log in to the web UI.

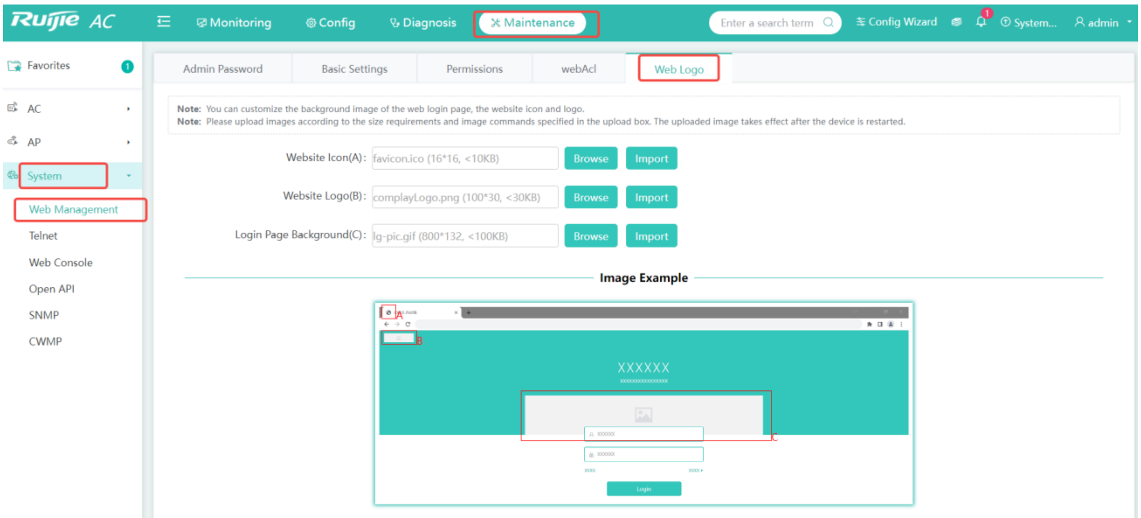


Note: If you enable this feature, all clients except those in the network whitelist will be denied access to Web. Please verify the settings.

Deny Access to Web OFF

5. Web Logo

With this feature, you can customize the login page of the web system and the logo in the upper left corner of the menu.



Note: You can customize the background image of the web login page, the website icon and logo.
Note: Please upload images according to the size requirements and image commands specified in the upload box. The uploaded image takes effect after the device is restarted.

Website Icon(A): favicon.ico (16*16, <10KB) Browse Import

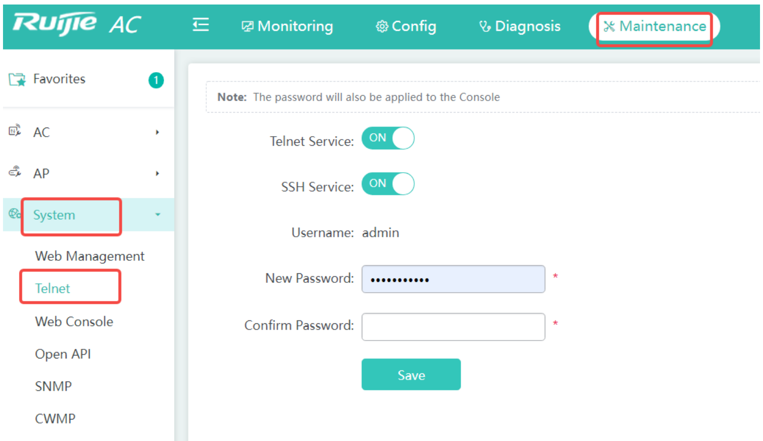
Website Logo(B): complayLogo.png (100*30, <30KB) Browse Import

Login Page Background(C): lg-pic.gif (800*132, <100KB) Browse Import

7.3.2 Telnet

Choose **Maintenance** > **System** > **Telnet**.

The Telnet feature enhances the system security and information interaction security. The Telnet and SSH services can be enabled/disabled and the password can be configured on the Telnet configuration page.



Note: The password will also be applied to the Console

Telnet Service: ON

SSH Service: ON

Username: admin

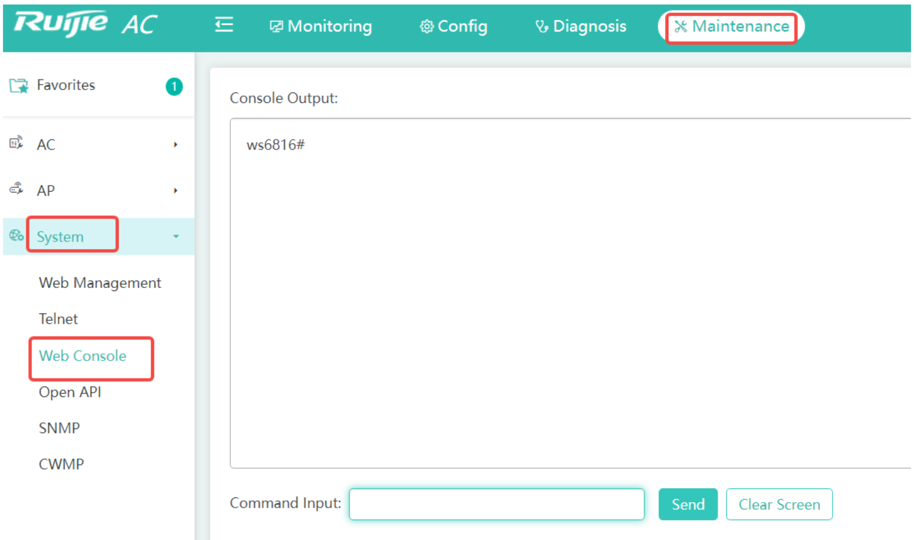
New Password: ••••••••••• *

Confirm Password: *

7.3.3 Web Console

Choose **Maintenance** > **System** > **Web Console**.

You can send CLI commands through the web console.



```
ws6816#
```

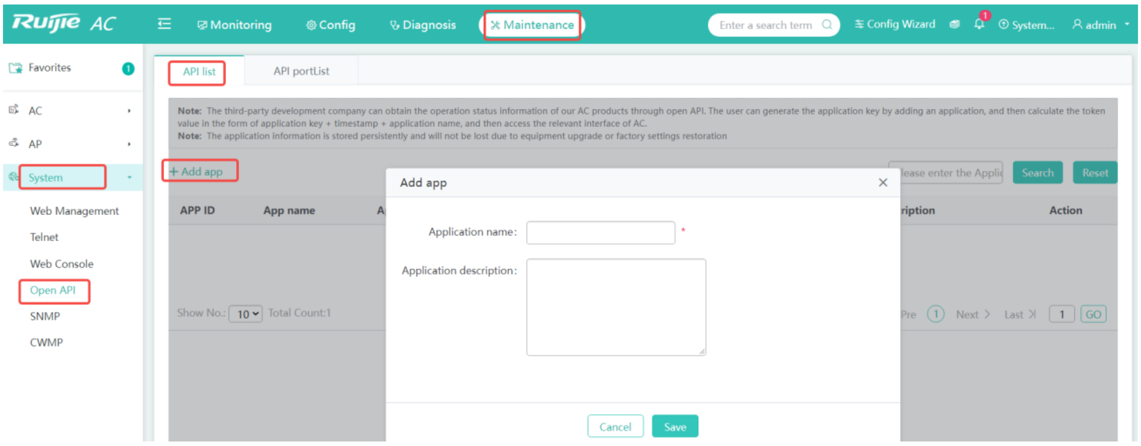
7.3.4 Open API

Choose **Maintenance** > **System** > **Open API**.

Third-party development companies can obtain the running status of Ruijie AC products through open APIs. Users can access interfaces on the AC based on the token value. The token value is calculated based on the application key generated after adding the application, timestamp, and the application name.

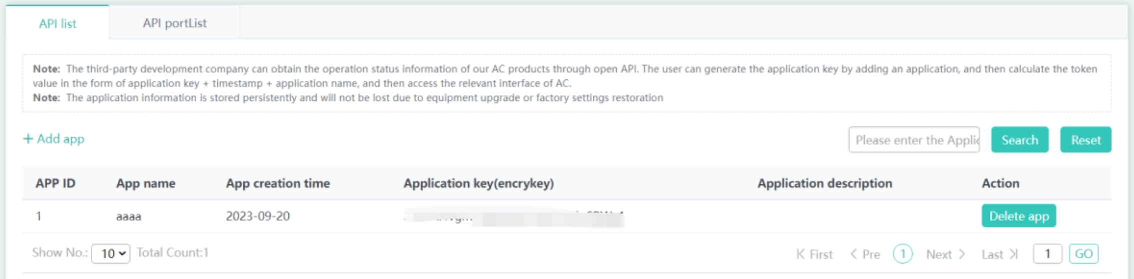
Operations Performed by Network Administrators (Common Users):

(1) Choose **Maintenance** > **System** > **Open API** to perform application authentication.



Note: The third-party development company can obtain the operation status information of our AC products through open API. The user can generate the application key by adding an application, and then calculate the token value in the form of application key + timestamp + application name, and then access the relevant interface of AC.
Note: The application information is stored persistently and will not be lost due to equipment upgrade or factory settings restoration

(2) After successful authentication, check **App name** and **Application key(encrykey)** on this page.



Note: The third-party development company can obtain the operation status information of our AC products through open API. The user can generate the application key by adding an application, and then calculate the token value in the form of application key + timestamp + application name, and then access the relevant interface of AC.
Note: The application information is stored persistently and will not be lost due to equipment upgrade or factory settings restoration

APP ID	App name	App creation time	Application key(encrykey)	Application description	Action
1	aaaa	2023-09-20	[redacted]		Delete app

Open API Examples (for Developers):

(1) Obtain the token based on the authentication information. (The token is effective for a given period of time.)

Description	Obtaining the token		
URL	/Web/init.lua/common.system.register/getAppToken		
Request Method	POST request		
Form Data Request Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
params			
appName	String	Y	Application name
timestamp	String	Y	Indicates the timestamp. (Note: Convert the timestamp into a string during the transfer of the timestamp.)
secrecyKey	String	Y	Value of md5 (encrykey+timestamp+appName)
Returned Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
code	String	Y	If the execution succeeds, **0** is returned. If the execution fails, **–1** is returned.
msg	String	Y	Indicates a message explaining the **code** value. If the execution succeeds, the parameter value is **""**. If the execution fails, this parameter contains the failure cause.
data			
token	String	Y	16-bit random string (success), or empty string (failure)

Request Message Example

```
{
url :http://192.168.1.1/Web/init.lua/common.system.register/getAppToken
-d '{
  "params":{
       "appName":"abc",
       "timestamp":"1592544045848",
       "secrecyKey":"e94395f0cfe7bc1a2aa58a92d0d9d021"
   }
}'
}
```

Response Message Example

```
{
  "code":0,
"msg":"",
"data":{
"token":"0Ywx4MUvRidmWf74",
}
}
```

(3) The token can be carried in any of the following positions: QueryParam, RequestBody, and Cookie. An example of API carrying the token information (for delivering the CLI command) is as follows:

Description	Executing a CLI command as an agent		
URL	/Web/init.lua/common.agent.Webdo/agentToWebConfig		
Request Method	POST request		
Form Data Request Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
command	String	Y	Command to be sent to the device for execution
mode_url	String	Y	config or exec supported
Returned Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
N/A	N/A	N/A	The device execution result is directly returned, and the data may be in non-standard JSON format.

Request Message Example

```
{
url :http://192.168.1.1/Web/init.lua/common.agent.Webdo/agentToWebConfig?Token=0Y
wx4MUvRidmWf74
-H 'Cookie: Token=0Ywx4MUvRidmWf74;
-d '{
  "command":"show Web-api Web-auth WiFiDog support",
  "mode_url":"exec",
"Token":0Ywx4MUvRidmWf74
}
}
```

Response Message Example

```
"{ "code": 0,  "msg": "",  "data": { "status": 1 } }"
```

(4) API carrying the token information (Lua interface):

Description	Configuring the OUI blocklist and allowlist		
URL	/Web/init.lua/wlan_common.macctr.ouidao/configOui		
Request Method	POST request		
Form Data Request Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
returnType	String	Y	Array supported

postData			
isBlack	Boolean		Indicates whether to put xx in the blocklist. The value **true** indicates a blocklist, and **false** indicates an allowlist.
oui_arr	Array	Y	Added blocklist/allowlist array
oui	String	Y	OUI in **xxxx.xx** format, where **x** is any hexadecimal number, for example, **aa11.01**
mnemonic	String	Y	Remarks, which can be null.
Returned Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
N/A	String	N/A	If the OUI is successfully added, a null string is returned. If the OUI fails to be added, an error message is returned.

Request Message Example

```
{
url :http://192.168.1.1/Web/init.lua/wlan_common.macctr.ouidao/configOui?Token=0Ywx4MUvRidmWf74
-H 'Cookie: Token=0Ywx4MUvRidmWf74;
-d '{
    "returnType": "Array",
"postData": {
"oui_arr":[{"oui":"1657.15", "mnemonic":"a"}],
"isBlack":true
}
"Token":0Ywx4MUvRidmWf74
}
}
```

(5) Obtaining all AP information on the AC:

Description	Obtaining all AP information on the AC		
URL	/Web/init.cgi/ac.ap.ap/getApPermit		
Request Method	POST request		
Underlying Implementation	Based on the **getApList** method of the device module **custom.apmg.apmg_ap_config**		
Form Data Request Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
startNum	String	Y	Start subscript number
endNum	String	Y	End subscript number
name:	String	N	AP name
IP address	String	N	IP address of the AP
mac	String	N	MAC address of the AP
location	String	N	Location of the AP

vapSupport	String	N	Indicates whether AP virtualization configuration is supported. The value **1** indicates "supported", and **0** indicates "not supported".
masterGroup	String	N	If there is any pass-in role, it is considered that hierarchical and decentralized management is not supported, that is, permission control is not required.
softwareVersion	String	N	Software Version
workMode	Number	N	Indicates the working mode. The value options include **normal** (search the access part) and **others** (search the non-access part).
acDescription	String	N	Branch AC name
state	String	N	Query by AP state, which can be **Quit** or **Run**.
model	String	N	
apGroup	String	N	
Returned Parameters:			
Parameter	**Type**	**Mandatory**	**Description**
code	String	Y	If the execution succeeds, **0** is returned. If the execution fails, **–1** is returned.
msg	String	Y	Indicates a message explaining the **code** value. If the execution succeeds, the parameter value is **""**. If the execution fails, this parameter contains the failure cause.
data			
totalCount	String	Y	The data count value is returned.
list			
acdes	String		It is modified and inherited from the old command, and not supported if the device goes offline. It is provided by WLAN_HB and currently not supported.
apgroup	String		
apname	String		AP name
cpu_percent	Number		It is modified and inherited from the old command, and not supported if the device goes offline.
ctxid	Number		It is modified and inherited from the old command, and not supported if the device goes offline.
downflow_kbps	Number		It is modified and inherited from the old command, and not supported if the device goes offline.
flow_kbps	Number		It is modified and inherited from the old command, and not supported if the device goes offline.
freememory_percent	Number		It is modified and inherited from the old command, and not supported if the device goes offline.
hardwareVersion	String		Not supported if the device goes offline

IP address	String		IP address of the AP
location	String		Location of the AP
mac	String		MAC address of the AP
masterApName	String		
mastergroup	String		If there is any pass-in role, it is considered that hierarchical and decentralized management is not supported, that is, permission control is not required.
model	String		
offlineCount	Number		Not supported if the device goes online
onlineTime	Number		Not supported if the device goes offline
softwareVersion	String		Not supported if the device goes offline
staLimit	Number		It is modified and inherited from the old command, and is not supported if the device goes offline. **staLimit** is provided based on the AP, and the radio will be considered in the future.
stanum	Number		It is modified and inherited from the old command, and not supported if the device goes offline.
state	String		AP state, which can be **Quit** or **Run**.
subApMac	String		It is modified and inherited from the old command, and is not supported if the device goes offline.
subApName	String		It is modified and inherited from the old command, and is not supported if the device goes offline.
upflow_kbps	Number		It is modified and inherited from the old command, and is not supported if the device goes offline.
vacId	Number		
vapsupport	String		Indicates whether AP virtualization configuration is supported. Value options include **yes** and **no**.
vtapState	Number		This parameter may be set to one of the following four values: **0**: Indicates that this AP is a virtual AP. The current AC is the master AC, and you can add a virtual template for the AP. **1**: Indicates that this AP is a virtual AP. The current AC is not a master AC, and you cannot add a virtual template for the AP. **2**: Indicates that this AP is a physical AP. This AP supports a virtual AP, and you can add any virtual template for the AP. **3**: Indicates that this AP is a physical AP. This AP does not support a virtual AP, and you cannot add a virtual template for the AP.
workMode	Number		Working mode of the device **0**: normal **1**: hybrid **2**: monitor **3**: radio-based monitor

Request Message Example

```
{
url :http://192.168.1.1/Web/init.cgi/ac.ap.ap/getApPermit
-d '{
   "startNum": 1,
"endNum": 1
}
}
```

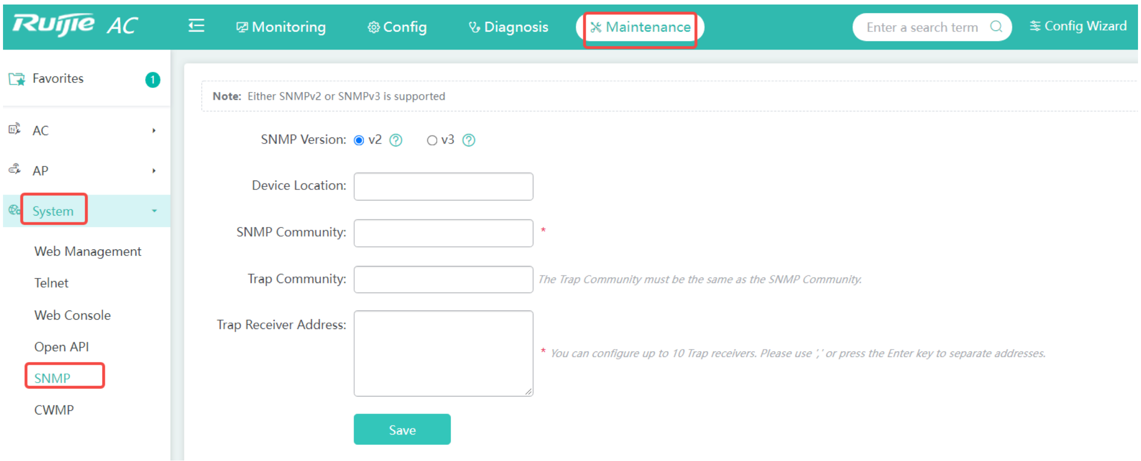
Response Message Example

```
{
  "code": 0,
  "data": {
      "list": [{
          "subApMac": "",
          "downflow_kbps": 0,
          "apgroup": "fenji123",
          "acdes": "",
          "ctxid": 1684301335,
          "cpu_percent": 0,
          "mac": "8005.8806.a367",
          "ip": "3.3.3.4",
          "subApName": "",
          "state": "Run",
          "upflow_kbps": 0,
          "mastergroup": "",
          "location": "",
          "vtapState": 2,
          "flow_kbps": 0,
          "masterApName": "",
          "freememory_percent": 0,
          "onlineTime": 242501,
          "stanum": 0,
          "vacId": 5,
          "offlineCount": 0,
          "apname": "JO-AP720-I",
          "vapsupport": "yes",
          "softwareVersion": "AP_RGOS 11.1(5)B0,  Release(07141708)",
          "hardwareVersion": "1.13",
          "model": "AP720-I",
          "workMode": 0,
          "staLimit": 64
      }],
      "totalCount": 1
  },
  "msg": ""
}
```

7.3.5 SNMP

Choose **Maintenance** > **System** > **SNMP**.

Simple Network Management Protocol (SNMP) provides a method for collecting network management information from devices on the network. It can be used to manage a large number of network devices.



Note: Either SNMPv2 or SNMPv3 is supported

SNMP Version: ● v2 ○ v3

Device Location:

SNMP Community: *

Trap Community: The Trap Community must be the same as the SNMP Community.

Trap Receiver Address: * You can configure up to 10 Trap receivers. Please use ';' or press the Enter key to separate addresses.

7.3.6 CWMP

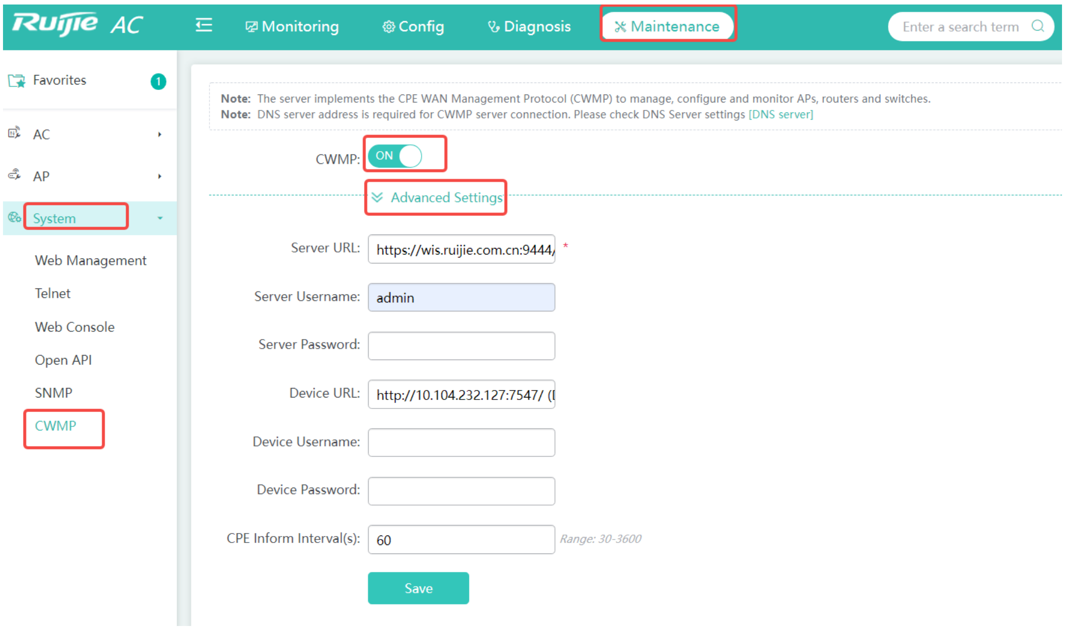
Choose **Maintenance** > **System** > **CWMP**.

The CWMP protocol is the CPE WAN Management Protocol. The server can manage, configure, and monitor devices such as ACs, APs, routers, or switches through this protocol.

Through configuration, the device can be connected to and managed by a cloud platform or other servers.

Note

When connecting to a server through the CWMP protocol, you need to configure the correct DNS server so that the device can correctly resolve the server's domain name. Therefore, check whether the DNS server is correctly configured.



Note: The server implements the CPE WAN Management Protocol (CWMP) to manage, configure and monitor APs, routers and switches.
Note: DNS server address is required for CWMP server connection. Please check DNS Server settings [DNS server]

CWMP: ON

Server URL: https://wis.ruijie.com.cn:9444/ *

Server Username: admin

Server Password:

Device URL: http://10.104.232.127:7547/ (I

Device Username:

Device Password:

CPE Inform Interval(s): 60 Range: 30-3600

Parameter	Description
CWMP	The CWMP switch is used to enable/disable the CWMP feature.
Server URL	Specifies the IP address of the server.
Server Username	Specifies the server username, which can be used for verification.
Server Password	Specifies the server password, which can be used for verification.
Device URL	Specifies the device URL, which can be used to actively connect to the server on the same LAN.
Device Username	Specifies the device username, which can be used for verification.
Device Password	Specifies the device password, which can be used for verification.
CPE Inform Interval(s)	Specifies the interval for connecting to the server, namely, the interval of heartbeat packets.

8 Web Management Configuration Examples

Deploy a simple wireless network: The device is deployed for the first time after being unpacked. Perform basic configuration for the AC to ensure that wireless users can receive signals and obtain IP addresses.

8.1 Scenario Where Both the AP Address Pool and User Address are Deployed on the Local Device

8.1.1 Configuration Requirements

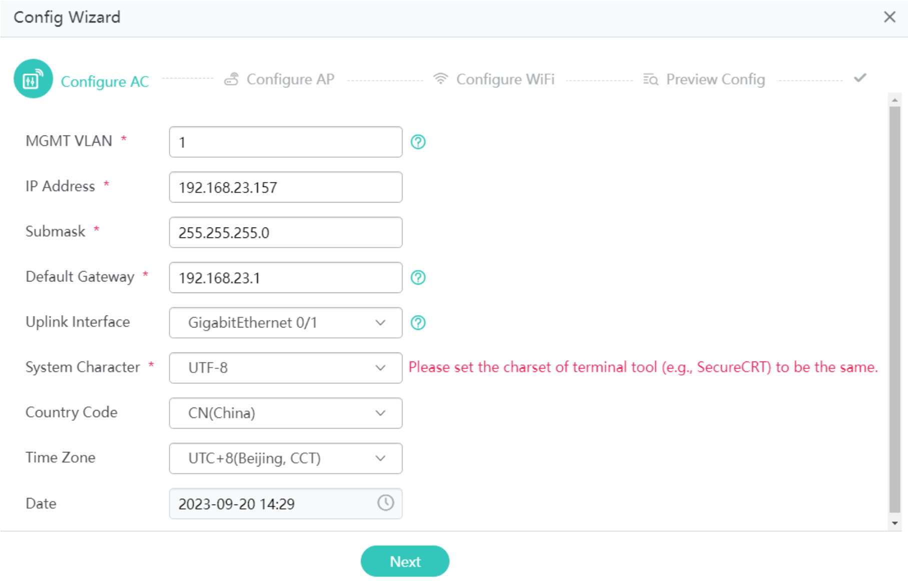
- Configure the **g0/1** interface on the AC as the uplink interface, with the device management VLAN set to **1**. The management address is 192.168.23.157 and the gateway address is 192.168.23.1.
- Configure the **Test_WiFi** wireless network with the WPA/WPA2-PSK encryption. Set the password to **12345678**.
- Configure **Test_WiFi** with dual-band operation and centralized forwarding.
- The IP address of the AP is assigned to VLAN 2, with an address pool in the 192.68.2.0 subnet and a gateway at 192.168.2.1.
- The IP address of the STA is assigned to VLAN 3, with an address pool in the 192.168.3.0 subnet and a gateway at 192.168.3.1.

8.1.2 Configuration Steps

1. **Basic Configuration for the AC**

Configure the basic settings for the AC based on the scenario.

Set the **g0/1** interface as the uplink interface for the AC. Set the device management VLAN to **1**, the management address to **192.168.23.157**, and the default gateway address to **192.168.23.1**.



MGMT VLAN * 1

IP Address * 192.168.23.157

Submask * 255.255.255.0

Default Gateway * 192.168.23.1

Uplink Interface GigabitEthernet 0/1

System Character * UTF-8 Please set the charset of terminal tool (e.g., SecureCRT) to be the same.

Country Code CN(China)

Time Zone UTC+8(Beijing, CCT)

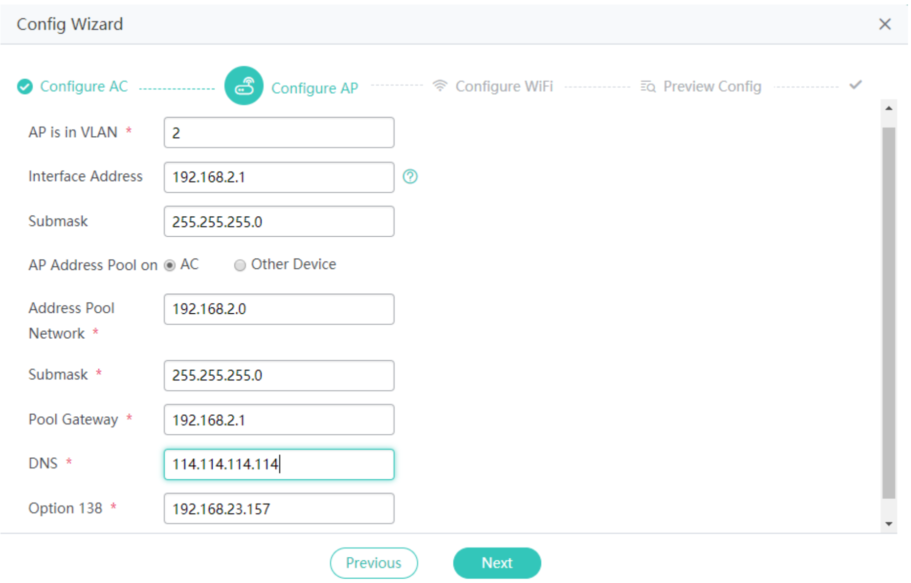
Date 2023-09-20 14:29

Note

- The tunnel address is the same as the management address by default in quick configuration. Therefore, you are not required to set the tunnel address.
- The system charset is UTF-8 encoding by default. To view or change the configuration through other client tools, users are also advised to use UTF-8 in case they are not allowed to change the configuration or the page displays garbled characters.

2. Access Configuration for the AP

The IP address of the AP is assigned to VLAN 2, with an address pool in the 192.168.2.0 subnet and a gateway at 192.168.2.1.



Config Wizard

AP is in VLAN * 2

Interface Address 192.168.2.1

Submask 255.255.255.0

AP Address Pool on ● AC ○ Other Device

Address Pool Network * 192.168.2.0

Submask * 255.255.255.0

Pool Gateway * 192.168.2.1

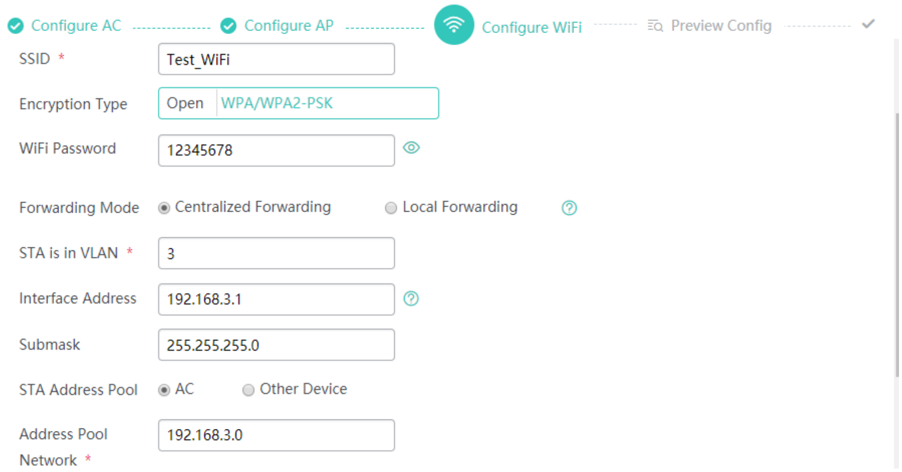
DNS * 114.114.114.114

Option 138 * 192.168.23.157

3. Wi-Fi Configuration

Set the SSID to **Test_WiFi** and configure it with the WPA/WPA2-PSK encryption.
Set the password to **12345678**.

The IP address of the STA is assigned to VLAN 3, with an address pool in the 192.168.3.0 subnet and a gateway at 192.168.3.1.



SSID * Test_WiFi

Encryption Type Open WPA/WPA2-PSK

WiFi Password 12345678

Forwarding Mode ● Centralized Forwarding ○ Local Forwarding

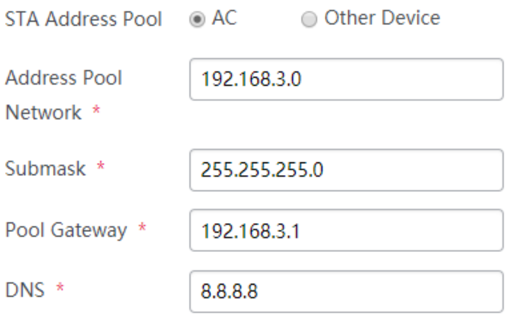
STA is in VLAN * 3

Interface Address 192.168.3.1

Submask 255.255.255.0

STA Address Pool ● AC ○ Other Device

Address Pool Network * 192.168.3.0

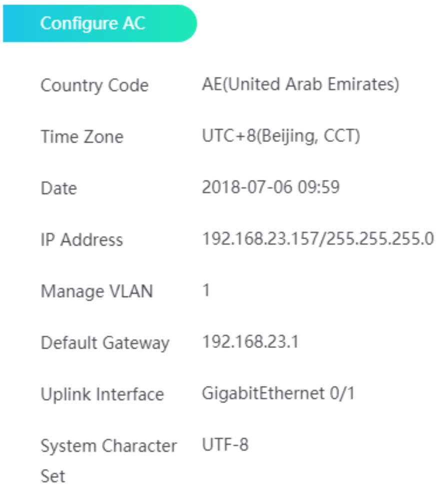


STA Address Pool	● AC ○ Other Device
Address Pool Network *	192.168.3.0
Submask *	255.255.255.0
Pool Gateway *	192.168.3.1
DNS *	8.8.8.8

4. Configuration Preview

Check whether the preceding three steps are configured correctly.

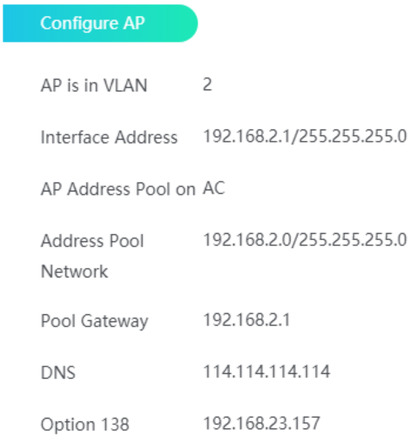
(1) Basic Configuration for the AC



Configure AC

Country Code	AE(United Arab Emirates)
Time Zone	UTC+8(Beijing, CCT)
Date	2018-07-06 09:59
IP Address	192.168.23.157/255.255.255.0
Manage VLAN	1
Default Gateway	192.168.23.1
Uplink Interface	GigabitEthernet 0/1
System Character Set	UTF-8

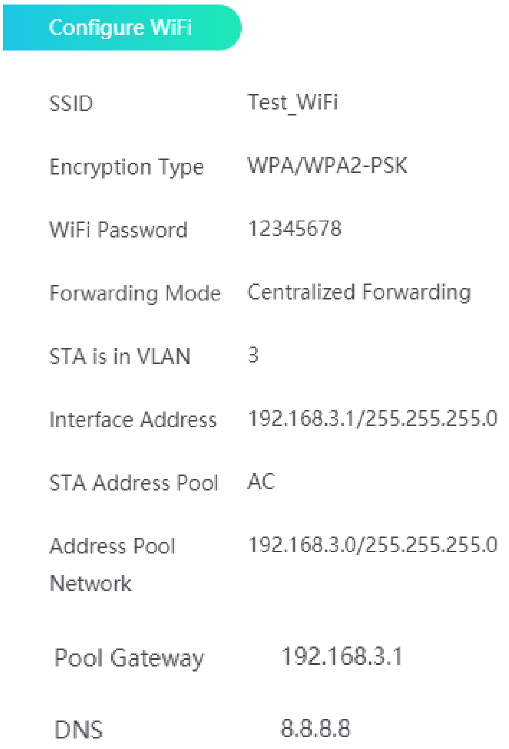
(2) Access Configuration for the AP



Configure AP

AP is in VLAN	2
Interface Address	192.168.2.1/255.255.255.0
AP Address Pool on	AC
Address Pool Network	192.168.2.0/255.255.255.0
Pool Gateway	192.168.2.1
DNS	114.114.114.114
Option 138	192.168.23.157

(3) Wi-Fi Configuration



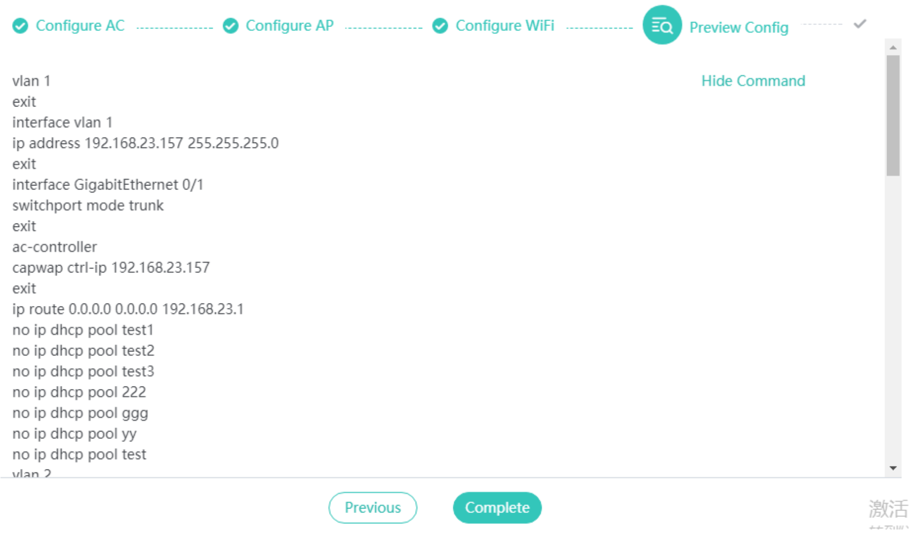
Configure WiFi

SSID	Test_WiFi
Encryption Type	WPA/WPA2-PSK
WiFi Password	12345678
Forwarding Mode	Centralized Forwarding
STA is in VLAN	3
Interface Address	192.168.3.1/255.255.255.0
STA Address Pool	AC
Address Pool Network	192.168.3.0/255.255.255.0
Pool Gateway	192.168.3.1
DNS	8.8.8.8

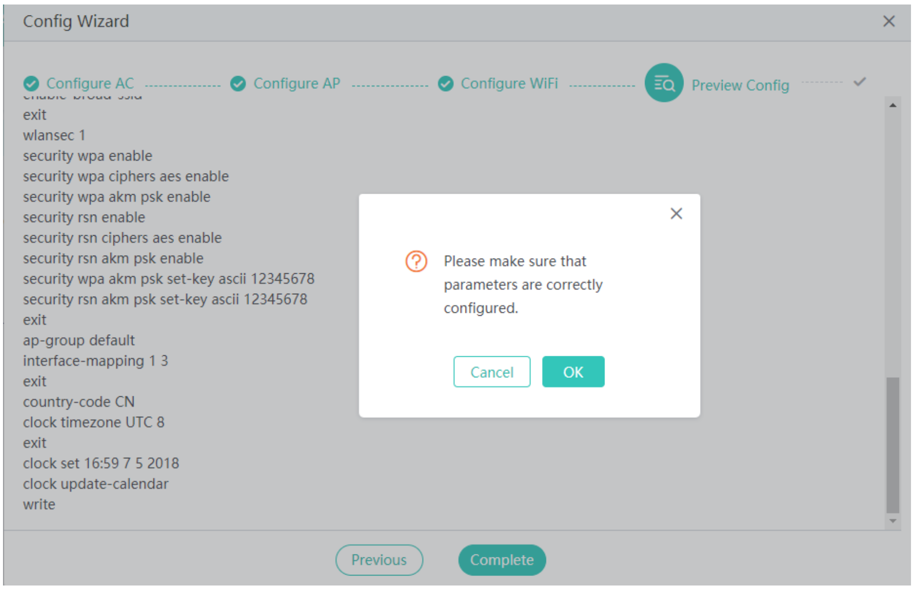
Click **Show Command** to check whether the configuration is correct.

```
VLAN 1
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/1
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.23.157
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
no ip dhcp pool EWeb-WIZARD-AP-POOL
no ip dhcp pool wewe
VLAN 2
exit
interface vlan 2
ip address 192.168.2.1 255.255.255.0
exit
service dhcp
ip dhcp pool EWeb-WIZARD-AP-POOL
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 114.114.114.114
```

```
option 138 ip 192.168.23.157
exit
VLAN 3
exit
interface vlan 3
ip address 192.168.3.1 255.255.255.0
exit
service dhcp
ip dhcp pool EWeb-WIZARD-STA-POOL
network 192.168.3.1 255.255.255.0
default-router 192.168.3.1
dns-server 114.114.114.114
exit
no wlan-config 1
wlan-config 1 Test_WiFi
ssid-code utf-8
enable-broad-ssid
exit
wlansec 1
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
security rsn akm psk enable
security wpa akm psk set-key ascii 12345678
security rsn akm psk set-key ascii 12345678
exit
ap-group default
interface-mapping 1 3
exit
language character-set UTF-8
clock timezone UTC +8
exit
clock set 15:31 3 1 2018
clock update-calendar
write
```



```
vlan 1
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/1
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.23.157
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
no ip dhcp pool test1
no ip dhcp pool test2
no ip dhcp pool test3
no ip dhcp pool 222
no ip dhcp pool ggg
no ip dhcp pool yy
no ip dhcp pool test
vlan 2
```



```
enable broad-ssid
exit
wlansec 1
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
security rsn akm psk enable
security wpa akm psk set-key ascii 12345678
security rsn akm psk set-key ascii 12345678
exit
ap-group default
interface-mapping 1 3
exit
country-code CN
clock timezone UTC 8
exit
clock set 16:59 7 5 2018
clock update-calendar
write
```

Please make sure that parameters are correctly configured.

Click **OK.** The configuration has succeeded.

8.1.3 Verification

A wireless STA connects to the **Test_WiFi** wireless network, the STA is dynamically assigned the **192.168.3.3** IP address.

8.2 Scenario Where Both the AP Address Pool and User Address are Deployed on other Devices

8.2.1 Configuration Requirements

- Set the **g0/1** interface as the uplink interface for the AC. Set the device management VLAN to **1**, the management address to **192.168.23.157**, the gateway address to **192.168.23.1**, and the tunnel address to **192.168.23.157**.

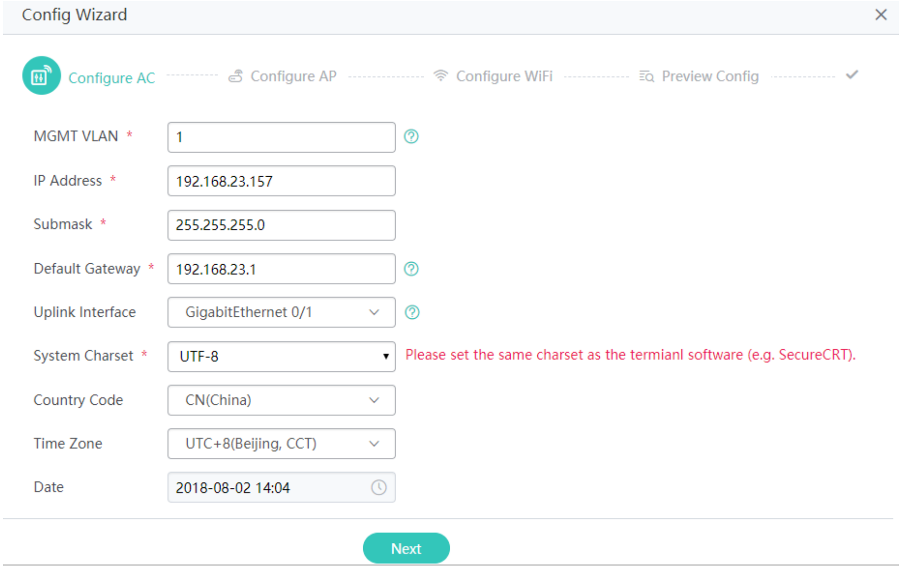
- Configure the **EWEB_WiFi_2.4G** 2.4 GHz Wi-Fi network with the WPA/WPA2-PSK encryption. Set the password to **12345678**.
- Configure the **EWEB_WiFi_5G** 5 GHz Wi-Fi network with the WPA/WPA2-PSK encryption. Set the password to **12345678**.
- The IP address of the AP is assigned to VLAN 2, with an address pool in the 192.68.2.0 subnet and a gateway at 192.168.2.1.
- **EWEB_WiFi_2.4G**: The IP address of the STA is assigned to VLAN 3. The gateway at 192.168.3.1 exists on the local device and the address pool in the 192.168.3.0 subnet exists on the switch.
- **EWEB_WiFi_5G**: The IP address of the STA is assigned to VLAN 4. The gateway at 192.168.3.1 exists on the local device and the address pool in the 192.168.4.0 subnet exists on the switch.

8.2.2 Configuration Steps

1. Basic Configuration for the AC

First, configure the basic settings for the AC based on the scenario.

Set the **g0/1** interface as the uplink interface for the AC. Set the device management VLAN to **1**, the management address to **192.168.23.157**, the gateway address to **192.168.23.1**, and the tunnel address to **192.168.23.157**.



MGMT VLAN *: 1

IP Address *: 192.168.23.157

Submask *: 255.255.255.0

Default Gateway *: 192.168.23.1

Uplink Interface: GigabitEthernet 0/1

System Charset *: UTF-8 Please set the same charset as the termianl software (e.g. SecureCRT).

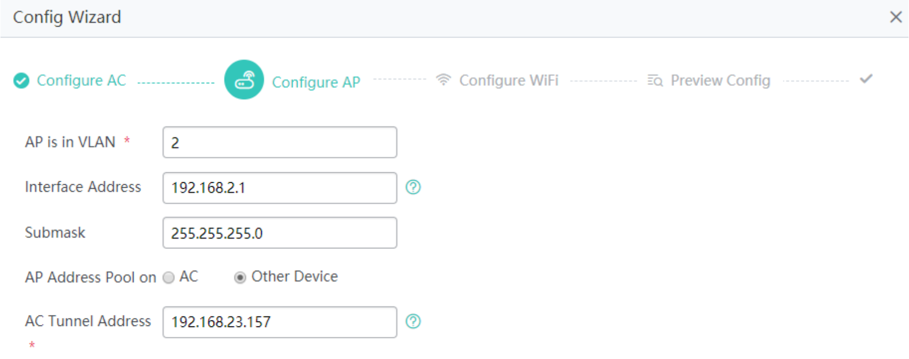
Country Code: CN(China)

Time Zone: UTC+8(Beijing, CCT)

Date: 2018-08-02 14:04

2. Access Configuration for the AP

The IP address of the AP is assigned to VLAN 2. The gateway at 192.168.2.1 exists on the local device and the address pool in the 192.168.2.0 subnet exists on the switch.



Config Wizard

AP is in VLAN *: 2

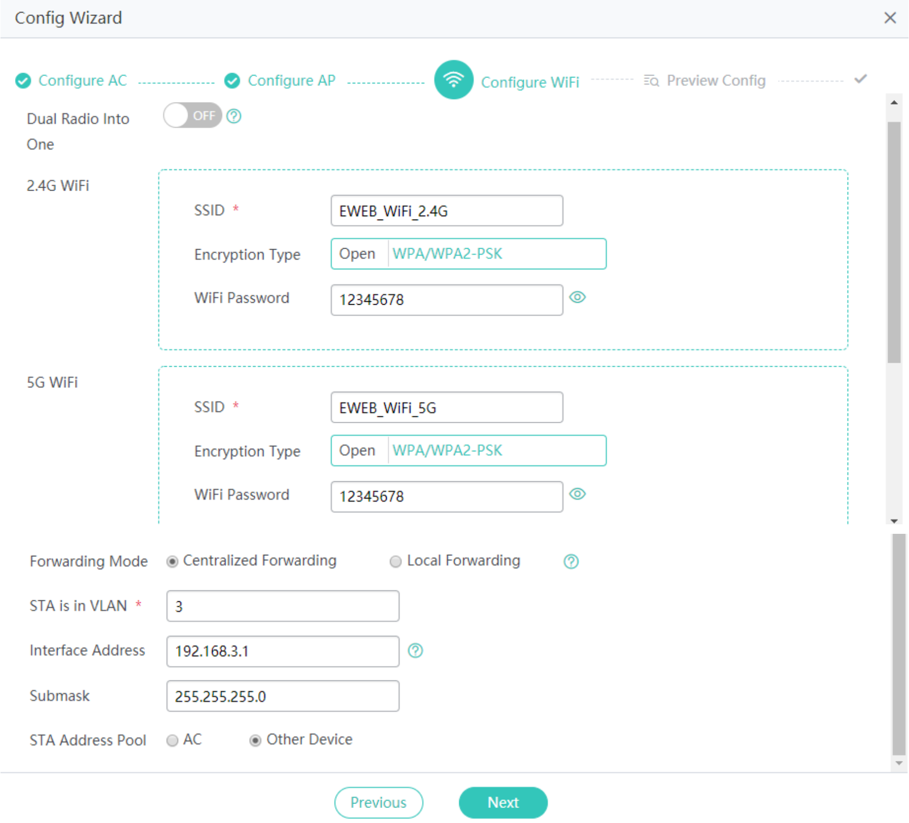
Interface Address: 192.168.2.1

Submask: 255.255.255.0

AP Address Pool on: ○ AC ● Other Device

AC Tunnel Address *: 192.168.23.157

3. Wi-Fi/WLAN Configuration



Config Wizard

Dual Radio Into One: OFF

2.4G WiFi

SSID *: EWEB_WiFi_2.4G

Encryption Type: Open [✓ WPA/WPA2-PSK]

WiFi Password: 12345678

5G WiFi

SSID *: EWEB_WiFi_5G

Encryption Type: Open [✓ WPA/WPA2-PSK]

WiFi Password: 12345678

Forwarding Mode: ● Centralized Forwarding ○ Local Forwarding

STA is in VLAN *: 3

Interface Address: 192.168.3.1

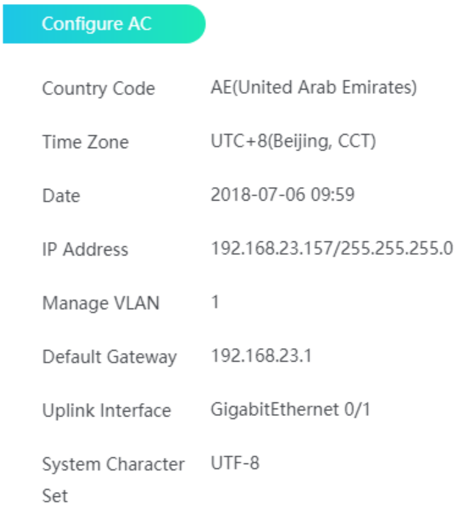
Submask: 255.255.255.0

STA Address Pool: ○ AC ● Other Device

4. Configuration Preview

Check whether the preceding three steps are configured correctly.

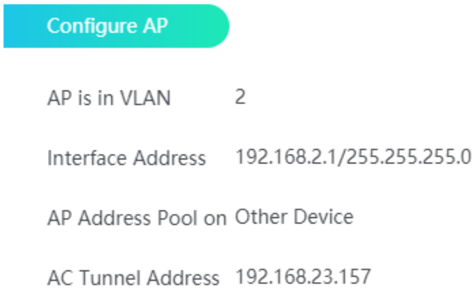
(1) Basic Configuration for the AC



Configure AC

Country Code	AE(United Arab Emirates)
Time Zone	UTC+8(Beijing, CCT)
Date	2018-07-06 09:59
IP Address	192.168.23.157/255.255.255.0
Manage VLAN	1
Default Gateway	192.168.23.1
Uplink Interface	GigabitEthernet 0/1
System Character Set	UTF-8

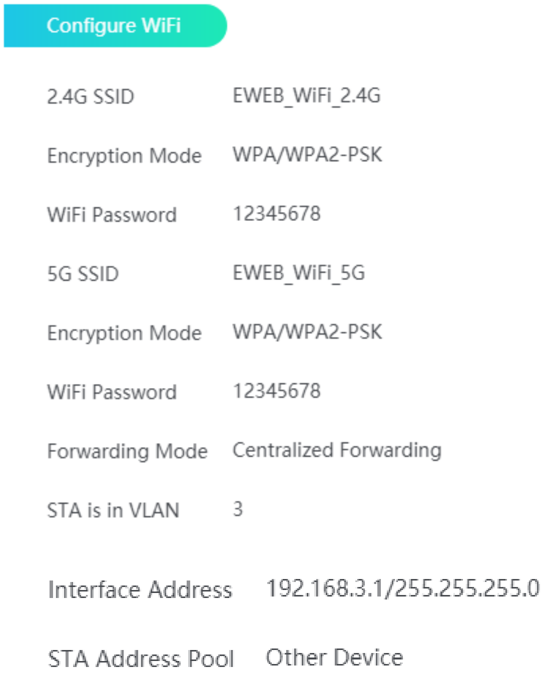
(2) Access Configuration for the AP



Configure AP

AP is in VLAN	2
Interface Address	192.168.2.1/255.255.255.0
AP Address Pool on	Other Device
AC Tunnel Address	192.168.23.157

(3) Wi-Fi Configuration



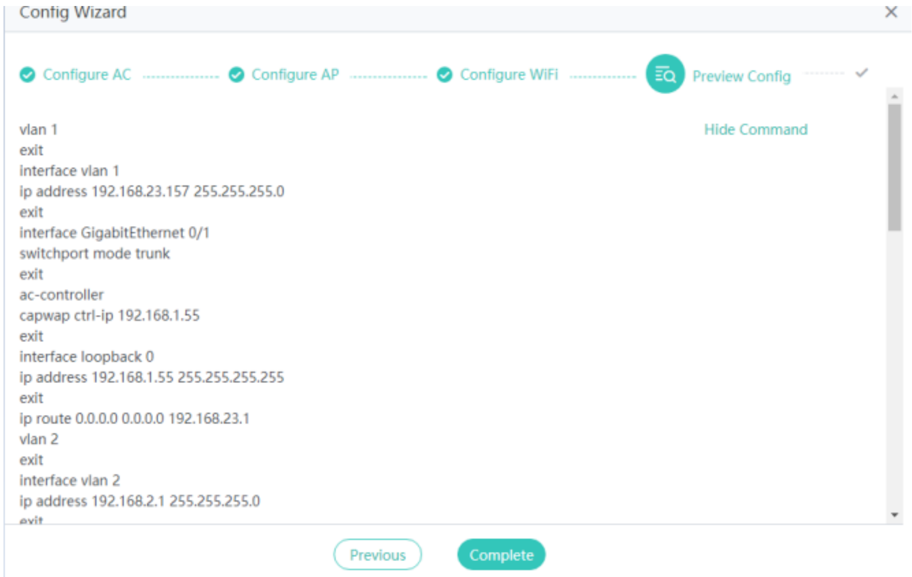
Configure WiFi

2.4G SSID	EWEB_WiFi_2.4G
Encryption Mode	WPA/WPA2-PSK
WiFi Password	12345678
5G SSID	EWEB_WiFi_5G
Encryption Mode	WPA/WPA2-PSK
WiFi Password	12345678
Forwarding Mode	Centralized Forwarding
STA is in VLAN	3
Interface Address	192.168.3.1/255.255.255.0
STA Address Pool	Other Device

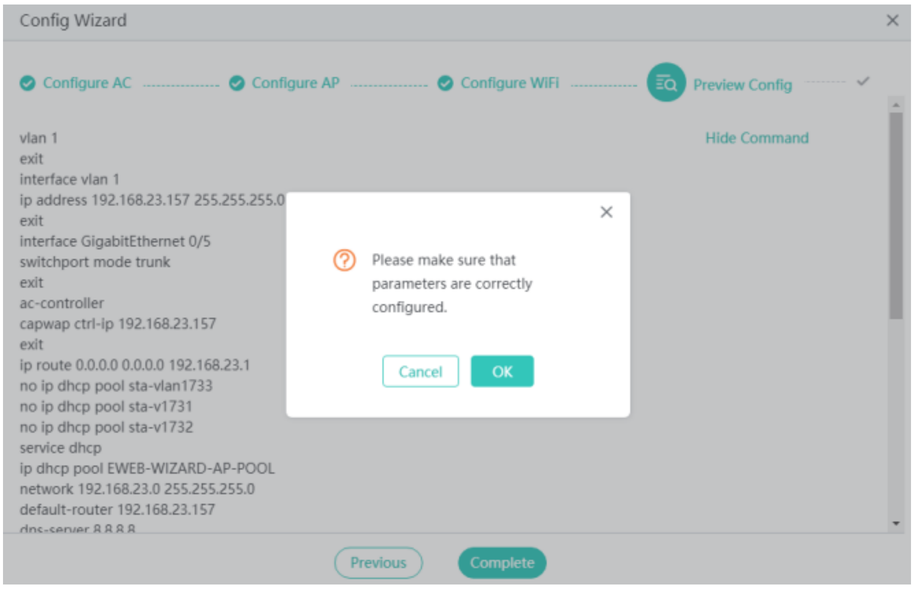
Click **Display Command** to check whether the configuration is correct.

```
VLAN 1
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/1
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.23.157
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
VLAN 2
exit
interface vlan 2
ip address 192.168.2.1 255.255.255.0
exit
VLAN 3
exit
interface vlan 3
ip address 192.168.3.1 255.255.255.0
exit
no wlan-config 1
wlan-config 1 EWEB_WiFi_2.4G
ssid-code utf-8
enable-broad-ssid
exit
wlansec 1
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
security rsn akm psk enable
security wpa akm psk set-key ascii 12345678
security rsn akm psk set-key ascii 12345678
exit
ap-group default
interface-mapping 1 3 radio 802.11b
exit
no wlan-config 2
wlan-config 2 EWEB_WiFi_2.4G
ssid-code utf-8
enable-broad-ssid
```

```
exit
wlansec 2
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
security rsn akm psk enable
security wpa akm psk set-key ascii 12345678
security rsn akm psk set-key ascii 12345678
exit
ap-group default
interface-mapping 2 3 radio 802.11a
exit
language character-set UTF-8
clock timezone UTC +8
exit
clock set 16:53 3 1 2018
clock update-calendar
write
```



```
vlan 1
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/1
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.1.55
exit
interface loopback 0
ip address 192.168.1.55 255.255.255.255
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
vlan 2
exit
interface vlan 2
ip address 192.168.2.1 255.255.255.0
exit
```



```
vlan 1
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/5
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.23.157
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
no ip dhcp pool sta-vlan1733
no ip dhcp pool sta-v1731
no ip dhcp pool sta-v1732
service dhcp
ip dhcp pool EWEB-WIZARD-AP-POOL
network 192.168.23.0 255.255.255.0
default-router 192.168.23.157
dns-server 8.8.8.8
```

Please make sure that parameters are correctly configured.

Click **OK**. The configuration has succeeded.

5. Switch Configuration

Configure the upstream switch after the configuration on the AC is completed. The configuration is as follows:

```
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.2.2 255.255.255.0
!
interface VLAN 3
 no ip proxy-arp
 ip address 192.168.3.3 255.255.255.0
!
no service password-encryption
service dhcp
!
ip dhcp pool ap_pool
 option 138 ip 192.168.23.157
 network 192.168.2.0 255.255.255.0
 dns-server 114.114.114.114
 default-router 192.168.2.1
!
ip dhcp pool sta_pool
 network 192.168.3.0 255.255.255.0
 dns-server 114.114.114.114
 default-router 192.168.3.1
!
!
```

8.2.3 Verification

- When a wireless STA connects to the **EWEB_WiFi_2.4G** 2.4 GHz Wi-Fi, the STA is dynamically assigned the **192.168.3.6** IP address.

- When a wireless STA connects to the **EWEB_WiFi_5G** 5 GHz Wi-Fi, the STA is dynamically assigned the **192.168.3.45** IP address.