



Ruijie RG-WLAN Series Access Point AP_RGOS 11.9(6)W3B3

Web-based Configuration Guide

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

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

Trademarks including  and  are owned by Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Live Chat: <https://www.ruijienetworks.com/rita>

Conventions

1. 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.

Contents

Preface	I
1 Web-based Configuration	1
1.1 Overview	1
1.2 Application	1
1.2.1 Web-based Management	1
1.3 Web Configuration	3
1.3.1 Config Wizard	3
1.3.2 Monitor	6
1.3.3 Configuration	8
1.3.4 Diagnosis	73
1.3.5 Maintenance	78
1.3.6 Others	86
1.4 Fit AP-Eweb	89
1.4.1 SmartAP	89
1.5 Enabling the Web Server	90
1.6 Configuration Examples	92
1.6.1 Constructing a WLAN for the DHCP Server on the AP Device	92

1 Web-based Configuration

1.1 Overview

A user accesses the Web-based management system using a browser such as Internet Explorer (IE) to manage the AP device.

Web-based management involves two parts: Web server and Web client. A Web server is integrated into a device to receive and process requests sent from a client (for example, read a Web file or execute a command request) and returns the processing results to the client. Generally, a Web client refers to a Web browser.

✔ Currently, this file is applicable to only AP devices.

1.2 Application

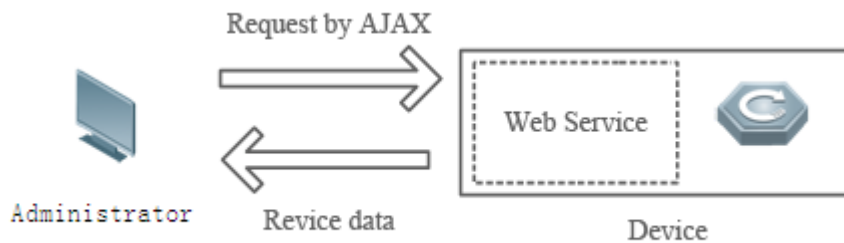
Application	Description
Web-based Management	After configuring, a user can access the Web-based management system through a browser.

1.2.1 Web-based Management

Scenario

As shown in the following figure, an administrator can access a device through a browser on a PC to manage the device.

Figure 1-1



Note	The Web management system integrates configuration commands and sends them to the device through AJAX requests. Web service is enabled on the device to process HTTP requests to return requested data.
-------------	--

Function Deployment

Configuration Environment Requirements

Requirements for Client

- An administrator logs in to the Web-based management system using the Web browser on a client to manage the device. Generally, a client refers to a PC. It may also be other mobile terminal devices, for example, a laptop.
- Google Chrome is recommended, and Internet Explorer 11 and 360 Browser are supported. Exceptions such as messy code and format errors may occur when other browsers are used.
- Resolution: It is recommended that the resolution be set to 1024 x 768, 1280 x 1024, or 1440 x 960. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

Requirements for server


- The Web service must be enabled for the AP device.
- Login authentication information for Web-based management must be configured for the AP device.
- A management IP address must be configured for the AP device.

Default Configuration

The following table lists the Web management system default configuration.

Feature	Default Settings
Web service	Enabled
Management IP	192.168.110.1

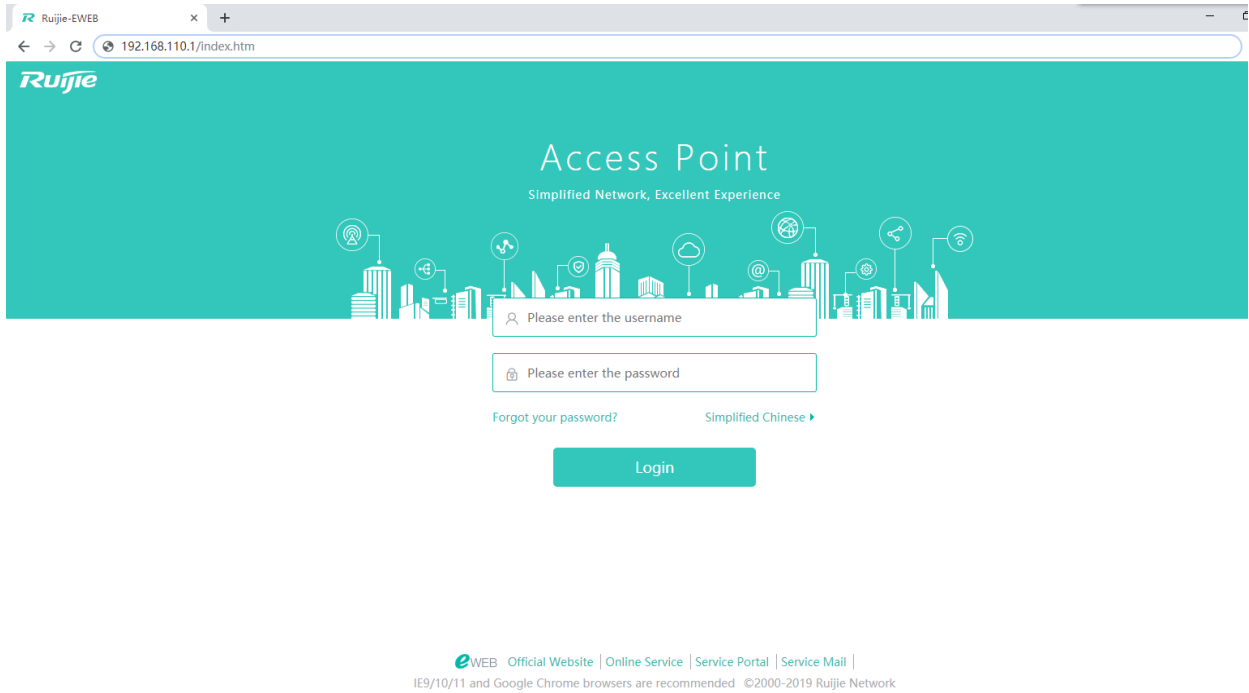
Default Username/Password	Permission Description
admin/admin	Super administrator with all permissions.

 The default password is not saved in **show running-config**.

Login

Type **http://X.X.X.X** (management IP address), default: <http://192.168.110.1>, in the address bar of a browser and press **Enter** to access the login page, as shown in the following figure.

Figure 1-2 Login page



After typing the username and password, click **Login**.

Enter the username and password. Click **Login** to access the Web management system.

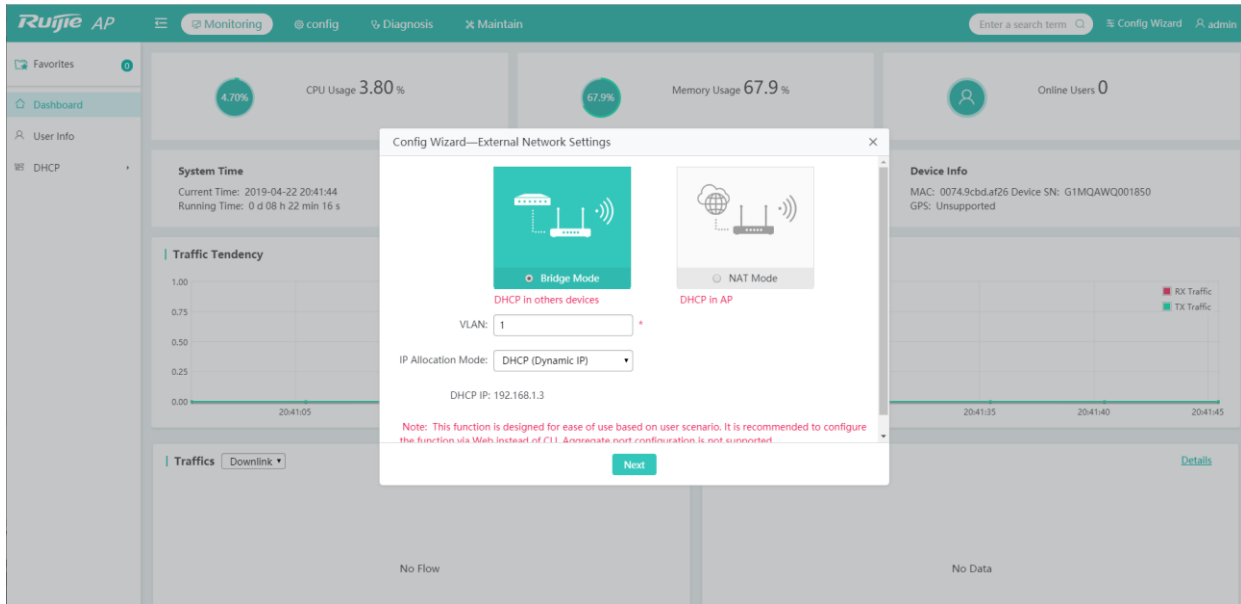
Click **Online Service** for configuration help.

If you enter the wrong username or password for five consecutive times, your account will be locked for 10 minutes.

1.3 Web Configuration

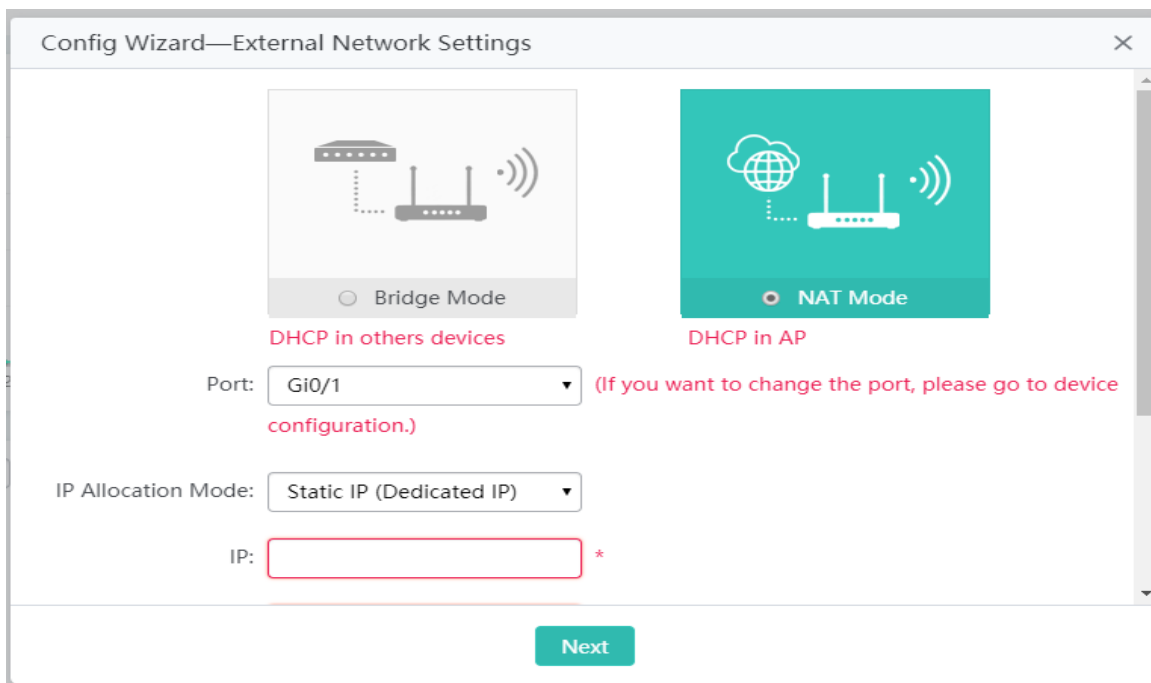
1.3.1 Config Wizard

Build a WiFi network for STAs to access for Internet services.



- 1) The **Config Wizard** page is displayed after successfully logging in to the Web if the device is in the default factory setting state, as shown in the preceding figure.
- 2) The **Config Wizard** page is also displayed when you click the **Config Wizard** link in the upper-right corner on the homepage.

The device supporting NAT can work in Bridge mode or NAT mode.



A device not supporting NAT can work only in Bridge Mode.

Config Wizard—External Network Settings

Bridge Mode
DHCP in others devices

VLAN: *

IP Allocation Mode:

DHCP IP: 192.168.2.47

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI. Aggregate port configuration is not supported.

Config Wizard—WiFi

SSID: *

WiFi Password: Show Password

DHCP: Enable (IP addresses are allocated by AP)

VLAN ID:

IP Range: to

DHCP Gateway:

Preferred DNS Server: Optional

Secondary DNS Server: Optional

Configure the WiFi parameters, and click **Finish** to finish the configuration.

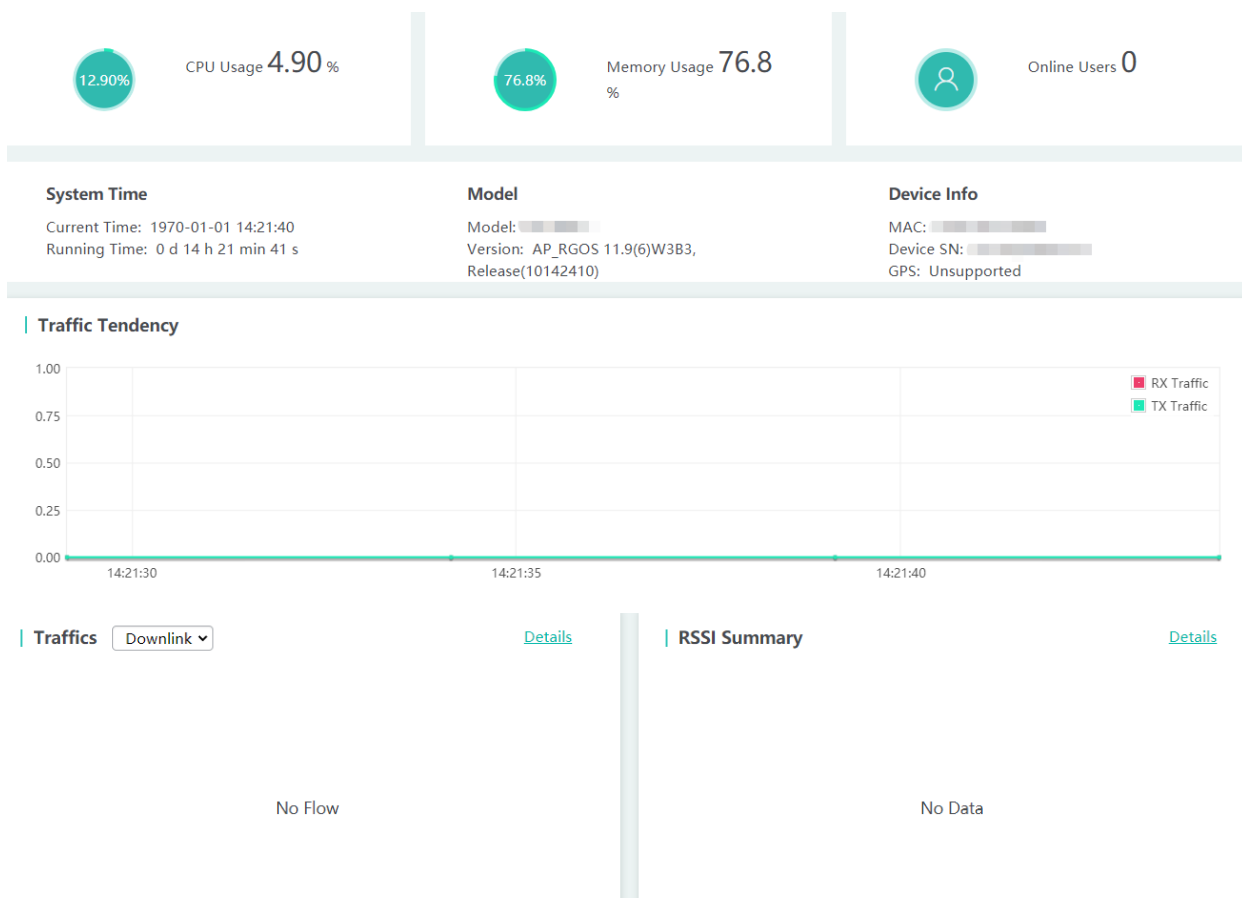
 After the AP device is initialized, please configure the AP device through the **Config Wizard** page.

- ⚠ All quick settings are scenario-based settings. And some of the configuration is delivered by default. If configurations such as NAT, interface, or address pool are changed via CLI or MACC system, it is recommended to not change the configuration again via Quick Settings, otherwise there could be incompatibility.
- ⚠ If the AP device is in access mode, it is recommended to build the gateway and address pool on the other device. If the AP device is in routing mode, it is recommended to build the gateway and address pool on the AP device and configure the NAT for it.

1.3.2 Monitor

1.3.2.1 Dashboard

The dashboard enables viewing basic information for the AP device, including the device MAC address, device model, system alarm information, flow trends of AP device ports, latest trends of all management APs, and STA information corresponding to each management AP. In addition, it enables you to know the distribution condition of STA signal strength in real time.



Click the **Traffics > Details** or **RSSI Summary > Details** link in the lower left corner to view the STA details on the displayed page, for example, the MAC address and RSSI.

1.3.2.2 User Info

User information is displayed here.

Note: If you want to delete STAs from blacklist or whitelist, please go to Blacklist/Whitelist.

Refresh Blacklist Whitelist MAC-based: Search

STA	MAC	IP	Uptime	Speed(Kbps)	RSSI	Channel(Radio)	Network	Action
No Data Found								

Show No.: 10 Total Count:0 K First < Pre Next > Last 1 GO

1.3.2.3 DHCP

DHCP includes DHCP client list and DHCP server status.

1.3.2.3.1 DHCP Client List

DHCP clients are displayed here.

IP-based Search

IP	MAC	Lease Time	Allocation Type	Action
192.168.23.3	14bd.61a9.79c2	0 Day(s) 23 hour(s) 44 minute(s)	Dynamic Allocation	Delete

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

1.3.2.3.2 DHCP Server Status

DHCP server status and address pool usage are displayed here.

DHCP Server Status: ● On ⚙️ Config DHCP

IPv4 DHCP Name: Search

Name	Usage	IP Address Range	Lease Time	DNS	Default Gateway
macc_sta_pool	<div style="width: 40%;"><div style="background-color: #ccc; height: 10px; width: 100%;"></div><div style="background-color: #00a651; height: 10px; width: 40%;"></div></div> 0.40% (1 / 253)	192.168.23.0/255.255.255.0	1 Day(s)	114.114.114.114	192.168.23.1
test_sta	<div style="width: 0%;"><div style="background-color: #ccc; height: 10px; width: 100%;"></div><div style="background-color: #00a651; height: 10px; width: 0%;"></div></div> 0.00% (0 / 253)	192.168.2.0/255.255.255.0	8 hour(s)		192.168.2.1

Show No.: Total Count:2 K First < Pre 1 Next > Last > GO

IPv6 DHCP Name: Search

Name	IP Address Range	Lease Time	DNS
No Data Found			

Show No.: Total Count:0 K First < Pre Next > Last > GO

1.3.3 Configuration

1.3.3.1 WiFi/WLAN

A Wireless Local Area Network (WLAN) refers to a network system that allows different PCs to communicate and share resources with each other by interconnecting different PCs through wireless communication technologies. The essence of a WLAN is that PCs are interconnected with each other in wireless rather than wired mode, thus constructing a network and allowing terminals to move more flexibly.

Wi-Fi or WiFi is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, smart TVs, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.

Service Set Identifier (SSID), also referred to as ESSID: It is used to distinguish different networks, that is, identifying an ESS. An SSID contains a maximum of 32 characters. A WNIC configured with different SSIDs can access different networks. SSIDs are usually broadcasted by an AP or a wireless router. The scanning function delivered with the XP can be used to view SSIDs within the current area. In consideration of security, SSIDs may not be broadcasted. In this case, users need to manually set SSIDs to access corresponding networks. To be simple, an SSID is the name of a WLAN. Only computers with the same SSID can communicate with each other.

The WLAN allows wireless STAs to access the AP through WiFi for Internet services. Multiple WLANs can be added or deleted.

The following figure shows the page for adding a WLAN.

WiFi-1 + ▾

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI.

WLAN ID: 1 * Range: 1-16

SSID: @eweb_chu_840i *

Encryption Type: WPA/WPA2-PSK ▾

WiFi Password: ***** * Show Password

>> Advanced Settings

Save Delete

- Adding WiFi/WLAN

WiFi-1 WiFi-2 X + ▾

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI.

WLAN ID: 2 * Range: 1-16


SSID: Eweb_AF262 *

Encryption Type: WPA/WPA2-PSK ▾

WiFi Password: ewebwifi * Show Password

>> Advanced Settings

Save

- 1) Click , and a new panel for WiFi configuration is displayed.
- 2) Set the WiFi parameters.
- 3) Click **Save** to finish the configuration.

- Editing WiFi/WLAN

- 1) Click the WiFi panel you want to edit.
- 2) Edit the WiFi configuration.
- 3) Click **Save**. The **Edit succeeded** message is displayed.

WLAN ID

WLAN ID is used to identify a WLAN network.

SSID

An SSID is the name of a wireless local area network.

Encryption Type

Open: No password is required.

WPA/WPA2-PSK: This encryption type is secure and simple, often used in homes and small offices.

WPA/WPA2-802.1x: An authentication server is required. This encryption type is complicated and costs much, not recommended for common users.

Advanced Settings

Hide SSID

This function is disabled by default.

SSID Code

UTF-8: Most terminals support UTF-8. The default code is UTF-8.

GBK: Some terminals and PCs support GBK.

WiFi Type

Radio1 is a 2.4GHz network and Radio2 is a 5GHz network.

Rate Limiting

The device only supports rate limiting on each user currently.

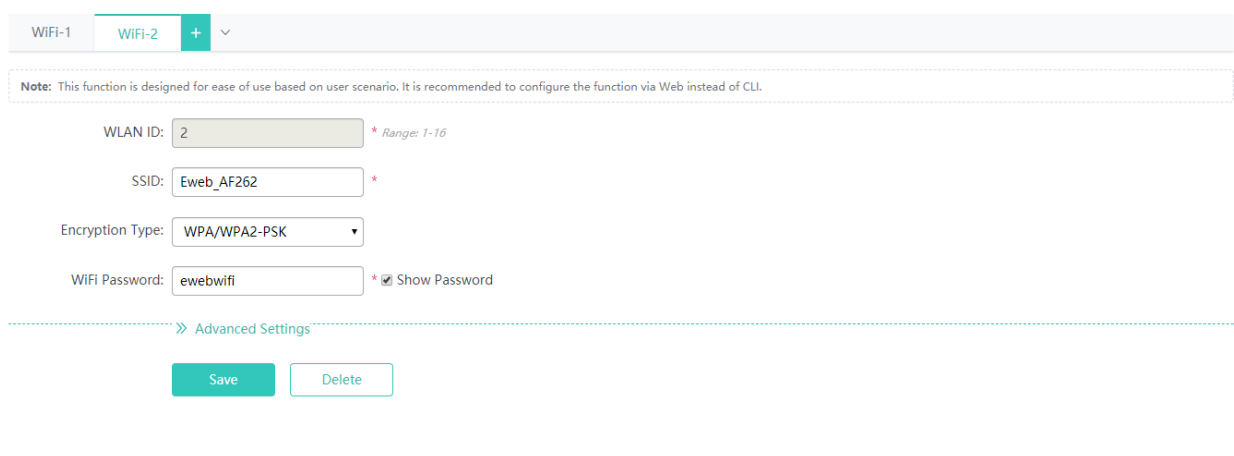
wlan-qos wlan-based * per-user-limit up-streams average-data-rate ** burst-data-rate **

wlan-qos wlan-based * per-user-limit down-streams average-data-rate ** burst-data-rate **

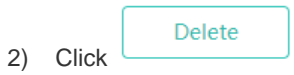
5G-prior Access

This feature will be displayed if supported by the device.

- Deleting WiFi/WLAN



- 1) Click the WiFi panel you want to delete a WiFi.



- 2) Click **Delete**.
- 3) Click **OK** in the dialog box displayed to finish the deletion operation.

1.3.3.2 AP

1.3.3.2.1 Radio Settings

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries and frequency bands. For example, the 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13), and the 5 GHz frequency band can be configured with five channels (channels 149, 153, 157, 161, and 165). The overlapping channels in the 2.4 GHz frequency band generate interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision. The five channels in the 5 GHz frequency band do not overlap or generate interference.

Wireless channel settings are mainly about adjusting the strength of the WiFi signal sent out by the device. Channel parameters can be set for the 2.4G and 5G networks.

- Enabling the 2.4G Network

Note: If the signal is unstable or poor, please modify the following parameters.
Note: Take the following factors into consideration: antenna installation, signal interference, magnetic fields, and walls.

2.4G Network: ON
[\[Force switching from 2.4GHz to 5GHz Network\]](#)

Country or Region:

Radio Protocol:

Radio Channel: Current Channel: 1

RF Bandwidth:

Power: [?](#)

STA Limit: (Range: 1 - 128)

- 1) Click ON to enable or disable the 2.4G network.
- 2) Click **Enforce switching from 2.4GHz to 5GHz Network** to switch the network type.

- Enabling the 5G Network

5G Network: ON

Country or Region:

Radio Protocol:

Radio Channel: Current Channel: 149

RF Bandwidth:

Power: [?](#)

STA Limit: (Range: 1 - 128)

- 1) Click  to enable or disable the 5G network.
- 2) Click **Enforce switching from 5GHz to 2.4GHz Network** to switch the network type.

- **Country & Region**

The country or region of the current radio.

Radio Protocol

2.4G Network: (1) 11bgn indicates the set of 802.11b, 802.11g and 802.11n. (2) 11bgn+11ax indicates the set of 802.11b, 802.11g, 802.11n and 802.11ax.

5G Network: (1) 11an indicates the set of 802.11a and 802.11n. (2) 11an+11ac indicates the set of 802.11a, 802.11n, 802.11ac. (3) 11an+11ac+11ax indicates the set of 802.11a, 802.11n, 802.11ac and 802.11ax.

Radio Channel

The channel of the current radio.

RF Bandwidth

The channel width of the current radio, including 20 Mhz and 40 Mhz.

Power

The power of the current radio. **Power Saving**, **Standard** and **Enhanced** indicate 30, 80 and 100 respectively.

STA Limit

The number of clients associated to the current radio.

1.3.3.2.2 WDS

Multiple APs are connected to each other in a wireless repeater or bridging mode to connect distributed networks and spread wireless signals. An AP device can be regarded as a repeater. It spreads the front-end network and elongates the WiFi transmission distance for association and connection of STAs far away. Wireless bridging supports the 2.4G network and 5G network bridging.

Enable the 2.4G or 5G network bridging function as required, select the **Central Base Station** operating mode, and click **Save** to finish configuration.

Note: Buildings over 100 meters away from each other need to be connected by optical cables. However, Digging roads or installing overhead lines to lay cables consumes great effort and cost. Applying WDS in this case is cost-efficient and effort-saving. The WDS is deployed on outdoor APs generally. [WDS Topology](#)

Radio1 (2.4G) WDS: ON

Operating Mode: Root Bridge Non-root Bridge

Root Bridge Network: (The WIFI does not exist.)

Distance: Meters

Other WiFi Allowed: (If not ticked, the device has a better forwarding performance.)

State: **WDS succeeded.**

Radio2 (5G) WDS: ON

Operating Mode: Root Bridge Non-root Bridge

Root Bridge Network: (The WIFI does not exist.)

Distance: Meters

Other WiFi Allowed: (If not ticked, the device has a better forwarding performance.)

1.3.3.2.3 iBeacon

iBeacon uses Bluetooth low energy proximity sensing to transmit a universally unique identifier picked up by a compatible app or operating system. The identifier and several bytes sent with it can be used to determine the device's physical location, track customers, or trigger a location-based action on the device such as a check-in on social media or a push notification.

iBeacon signals are broadcast over Bluetooth, and mainly applied to WeChat Shake.

i If iBeacon is not displayed in the menu, this function is not supported.

- If the AP does not support Bluetooth radio, the following page will be displayed.

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. The following data is provided by the third party (mall). [?](#)

UUID: ⓘ

Major: Range: 0 - 65535

Minor: Range: 0 - 65535

- If the AP does not support Bluetooth radio, the following page will be displayed. You can configure iBeacon globally or based on radio. Radio-based iBeacon settings prevail over global iBeacon settings.

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

Config iBeacon based on Radio ⌕ Global Setting

Radio 1

UUID: ⓘ

Major: Range: 0 - 65535

Minor: Range: 0 - 65535

Save

1.3.3.2.4 Client Limit

Client limit refers to the maximum number of associated STAs.

Note: Client Limit: Client Limit indicates the number of max associated clients allowed by the device

Client Limit: * (Range 1 - 512)

Save

1.3.3.2.5 Radio Balance

Radio balance refers to the balance of STAs on each radio.

Note: Radio balance refers to the balance of STAs on each radio.

Enable Load Balance: ON

Radio1 : Radio2

RF Access Ratio: : *

Save

1.3.3.3 Network

1.3.3.3.1 External Network Settings

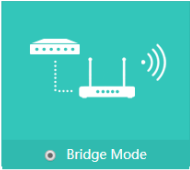
External network settings are mainly about configuration of the communication mode between the AP and external network. Two communication modes are available: Bridge mode and NAT mode.

In **Bridge Mode**, the Ruijie APs act as bridges, allowing wireless clients to obtain their IP addresses from an upstream DHCP server.

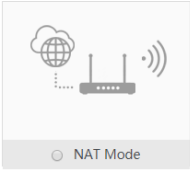
In **NAT Mode**, the Ruijie APs run as DHCP servers to assign IP addresses to wireless clients out of a private 10.x.x.x IP address pool behind a NAT.

 The AP you use might not support this function, which is subject to the actual menu items.

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI. Aggregate port configuration is not supported.



Bridge Mode
DHCP in others devices



NAT Mode
DHCP in AP

VLAN:

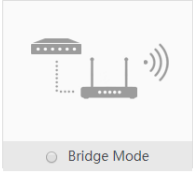
IP Allocation Mode:

IP: (in the same subnet with the uplink device)

Mask: *

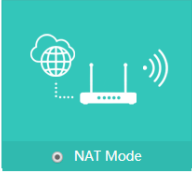
Default Gateway: Optional

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI. Aggregate port configuration is not supported.



Bridge Mode

DHCP in others devices



NAT Mode

DHCP in AP

Port: (If you want to change the port, please go to device configuration.)

IP Allocation Mode:

IP: *

IP Mask: *

Default Gateway: *

NAT: Check this box if you want to convert all internal addresses to external addresses.

You can select the AP working mode to determine the AP role and then configure based on the corresponding working mode.

Set corresponding parameters and save the configuration.

1.3.3.3.2 Interface

A port is a physical entity that is used for connections on the network devices.

Speed

Generally, the speed of an Ethernet physical port is determined through negotiation with the peer device. The negotiated speed can be any speed within the interface capability. You can also configure any speed within the interface capability for the Ethernet physical port on the Web page.

When you configure the speed of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Duplex Mode

Set the duplex mode of the interface to full-duplex so that the interface can receive packets while sending packets.

Set the duplex mode of the interface to half-duplex so that the interface can receive or send packets at a time.

Set the duplex mode of the interface to auto-negotiation so that the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.

Interface Name

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

Administrative Status

You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface, and the interface will loss all its functions. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

Interface Settings

Port	Link Status	Admin Status	Description	Information	Action
Gi0/1	Up	Up			Edit
Gi0/2	Down	Up		IPv4: 192.168.111.1, Mask: 255.255.255.0	Edit
Gi0/3	Down	Up		IPv4: 192.168.112.1, Mask: 255.255.255.0	Edit

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

- Editing port settings

Admin Status: Up

IPv4:

Mask:

Description:

[Advanced Settings](#)

Cancel Save

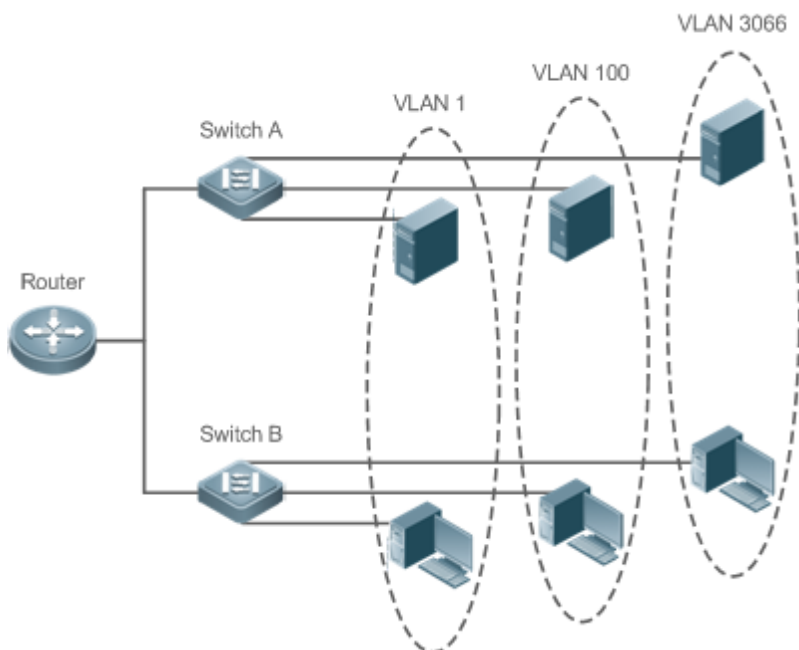
- 1) Click the **Edit** button for a port in the list.
- 2) The configuration for the port is displayed in the dialog box. Next, edit the configuration.
- 3) Click **Save**. The **Save operation succeeded** message is displayed.

1.3.3.3.3 VLAN

A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer-2 networks of the OSI model.

A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

We may define a port as a member of a VLAN, and all terminals connected to this port are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing and modifying users. Communication among VLANs is realized through Layer-3 devices, as shown in the following figure.



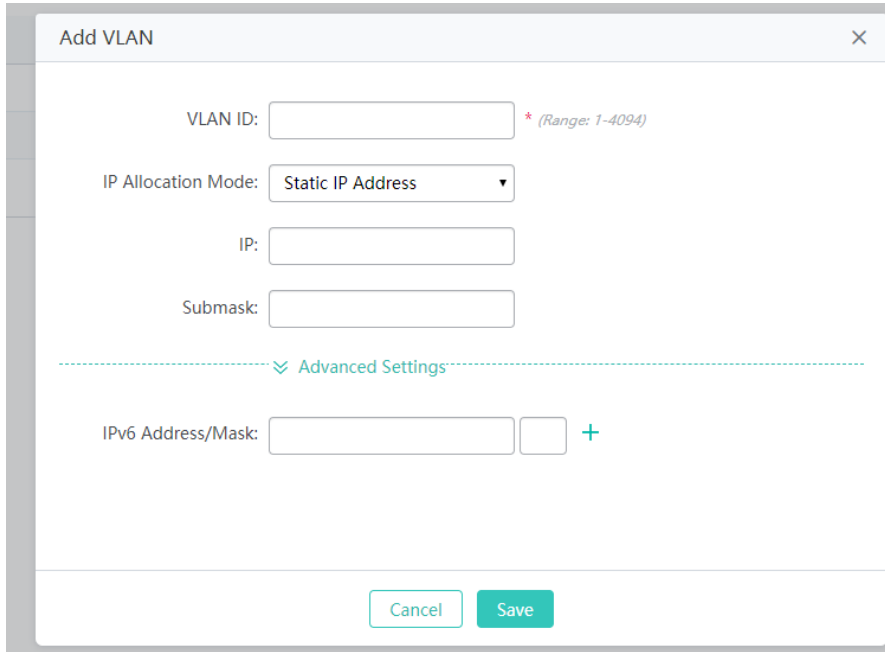
The VLANs supported by Ruijie products comply with the IEEE802.1Q standard. A maximum of 4094 VLANs (VLAN ID 1-4094) are supported, among which VLAN 1 cannot be deleted.

+ Add VLAN × Delete Selected

<input type="checkbox"/> VLAN ID	IPv4	IPv4 Mask	IPv6 Address/Mask	IP Allocation Mode	Action
<input type="checkbox"/> 1	192.168.1.3	255.255.255.0		DHCP	Edit
<input type="checkbox"/> 2	192.168.10.1	255.255.255.0		Static IP Address	Edit Delete

Show No.: Total Count:2 K First < Pre 1 Next > Last > GO

- Adding a VLAN



The 'Add VLAN' dialog box contains the following fields and controls:

- VLAN ID:** A text input field with a red asterisk and the text '(Range: 1-4094)' to its right.
- IP Allocation Mode:** A dropdown menu currently set to 'Static IP Address'.
- IP:** A text input field.
- Submask:** A text input field.
- Advanced Settings:** A section header with a downward arrow icon, separated from the fields above by a dashed line.
- IPv6 Address/Mask:** A text input field followed by a smaller empty input field and a '+' sign.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

Click **Add VLAN**. A dialog box is displayed, as shown in the preceding figure. Set corresponding parameters in the dialog box and click **Save**. The newly added VLAN is displayed in the VLAN list after the **Add operation succeeded** message is displayed.

- Deleting VLANs in batches

+ Add VLAN × Delete Selected

<input type="checkbox"/>	VLAN ID	IPv4	IPv4 Mask	IPv6 Address/Mask	IP Allocation Mode	Action
<input type="checkbox"/>	1	192.168.1.3	255.255.255.0		DHCP	Edit
<input type="checkbox"/>	2	192.168.10.1	255.255.255.0		Static IP Address	Edit Delete

Show No.: Total Count:2 K First < Pre Next > Last X [GO](#)

- 1) Select the VLAN to be deleted from the list.
- 2) Click **Delete Selected** to finish deleting.

- Editing a VLAN

Dialog box titled "Edit VLAN" with a close button (X). Fields include: VLAN ID: 2 (with a note: * (Range: 1-4094)), IP Allocation Mode: Static IP Address (dropdown), IP: 192.168.10.1, and Submask: 255.255.255.0. A link for "Advanced Settings" is visible. Buttons for "Cancel" and "Save" are at the bottom.

Click the **Edit** button. A dialog box is displayed, as shown in the preceding figure. Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a VLAN

Page header: + Add VLAN x Delete Selected

<input type="checkbox"/>	VLAN ID	IPv4	IPv4 Mask	IPv6 Address/Mask	IP Allocation Mode	Action
<input type="checkbox"/>	1	192.168.1.3	255.255.255.0		DHCP	Edit
<input type="checkbox"/>	2	192.168.10.1	255.255.255.0		Static IP Address	Edit Delete

Show No.: 10 Total Count: 2

Navigation: K First < Pre 1 Next > Last X 1 GO

Are you sure you want to delete the VLAN?

Cancel OK

Click the **Delete** button for a VLAN in the list and then click **OK** in the displayed dialog box to finish deleting.

1.3.3.3.4 Route

Routing is the process of selecting a path for traffic in a network, or between or across multiple networks.

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.

Default route is a setting on a computer that defines the packet forwarding rule to use when no specific route can be determined for a given Internet Protocol (IP) destination address. All packets for destinations not established in the routing table are sent via the default 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 X Delete Selected

<input type="checkbox"/>	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Routing	Type	Action
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.1.1	VLAN1	Primary Route	Default Route	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

● Adding a 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 X Delete Selected

IP Type: IPv4 IPv6

Destination Subnet: *

Subnet Mask: *

Egress Port: ▼

Next Hop Address: *

Routing: ▼ ⓘ

Click **Add Static Route**, set the configuration items in the dialog box displayed, and click **Save**. The newly added static route is displayed in the route list after the **Save operation succeeded** message is displayed.

● Adding the default 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 X Delete Selected

IP Type: IPv4 IPv6

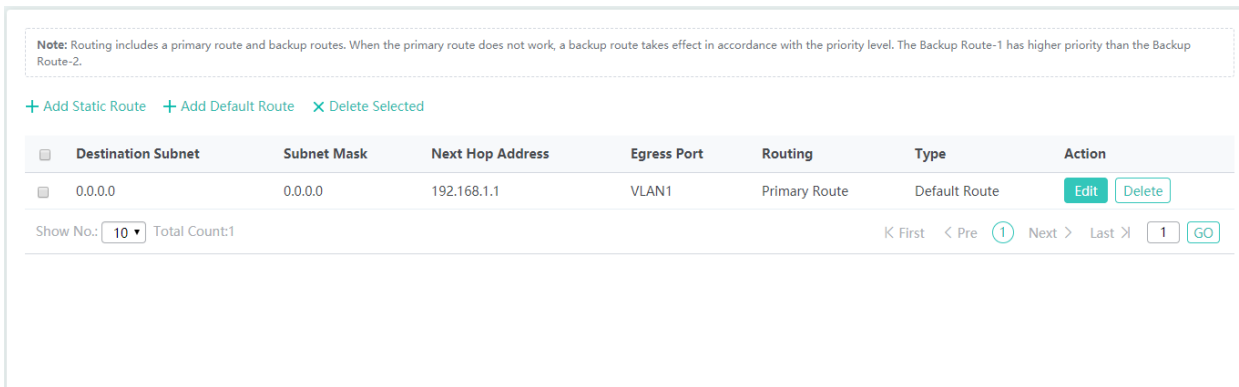
Egress Port: ▼

Next Hop Address: *

Routing: ▼ ⓘ

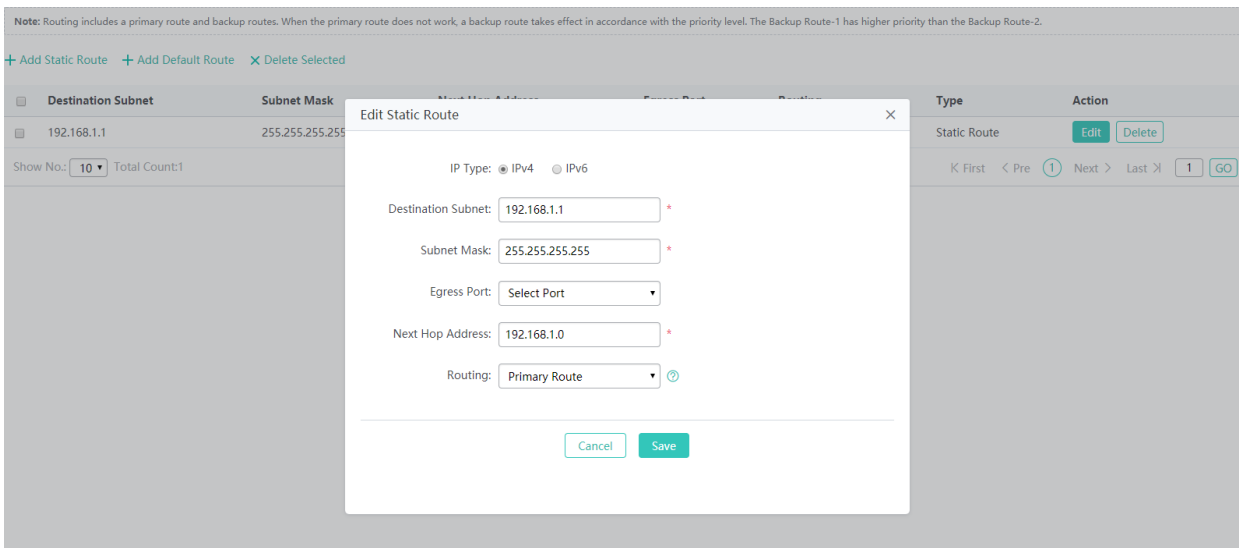
Click **Add Default Route**. Set the configuration items in the displayed dialog box, and click **Save**. The newly added route is displayed in the route list after the **Save operation succeeded** message appears.

- Deleting routes in batches



- 1) Select the route from the list.
- 2) Click **Delete Selected Route** to finish deleting.

- Editing a route



- 1) Click the **Edit** button for a route in the list.
- 2) A dialog box is displayed, as shown in the preceding figure. The configuration for the route is displayed. Next, edit the configuration.
- 3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a 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 X Delete Selected

Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Routing	Type	Action
192.168.1.1	255.255.255.255	192.168.1.0		Primary Route	Static Route	Edit Delete

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

Click the **Delete** button for a route in the list and then click **OK** in the displayed dialog box to finish deleting.

1.3.3.3.5 DHCP

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a permanent IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In "static allocation", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.

DHCP Settings

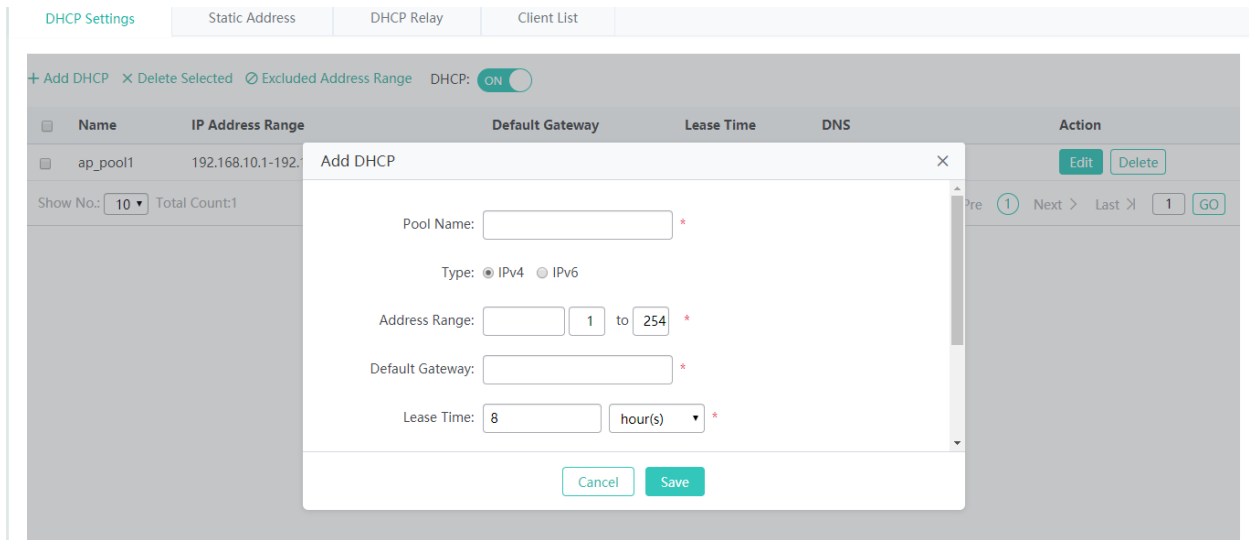
DHCP Settings | Static Address | DHCP Relay | Client List

+ Add DHCP X Delete Selected Excluded Address Range DHCP:

Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
ap_pool1	192.168.10.1-192.168.10.254	192.168.10.1	8 hour(s)	192.168.58.110,8.8.8.8	Edit Delete

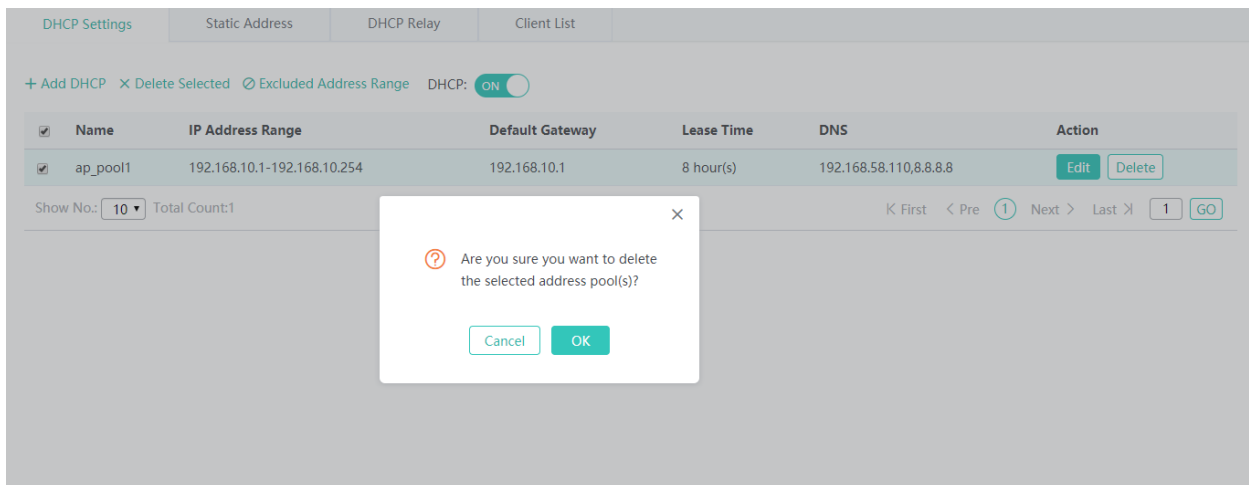
Show No.: 10 Total Count:1 K First < Pre 1 Next > Last X 1 GO

- Adding a DHCP Pool



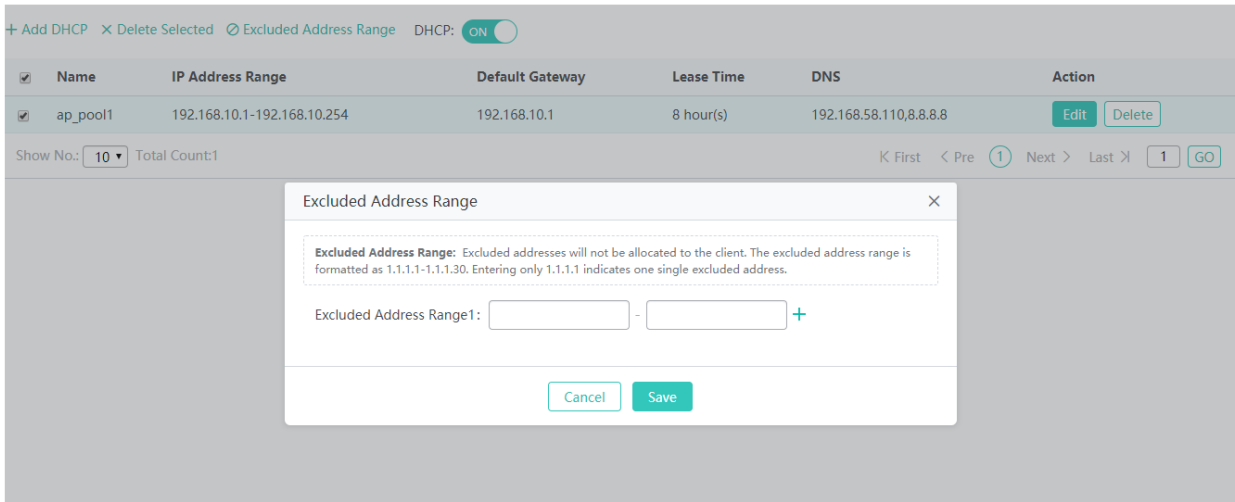
Click **Add DHCP**, set the configuration items in the dialog box displayed, and click **Save**. The newly added DHCP pool is displayed in the DHCP pool list after the **Save operation succeeded** message is displayed.

- Deleting DHCPs in batches

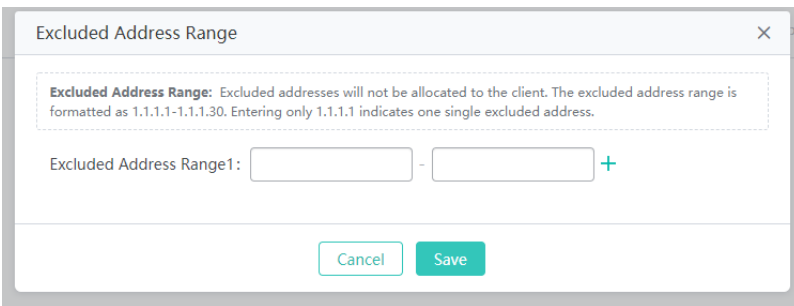


- 1) Select the DHCP pool from the list.
- 2) Click **Delete Selected DHCP** and then click **OK** in the dialog box displayed to finish deleting.

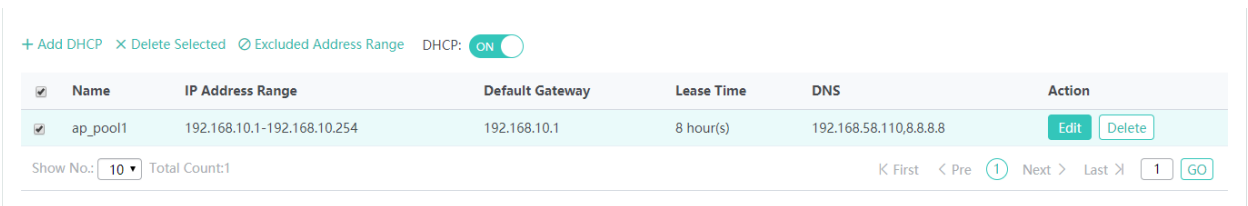
- Configuring excluded address range



Click **Excluded Address Range**. A dialog box is displayed, as shown in the preceding figure. Set the configuration items in the displayed dialog box, and click **Save**. The newly configured address range is displayed in the DHCP pool list after the **Save operation succeeded** message is displayed.

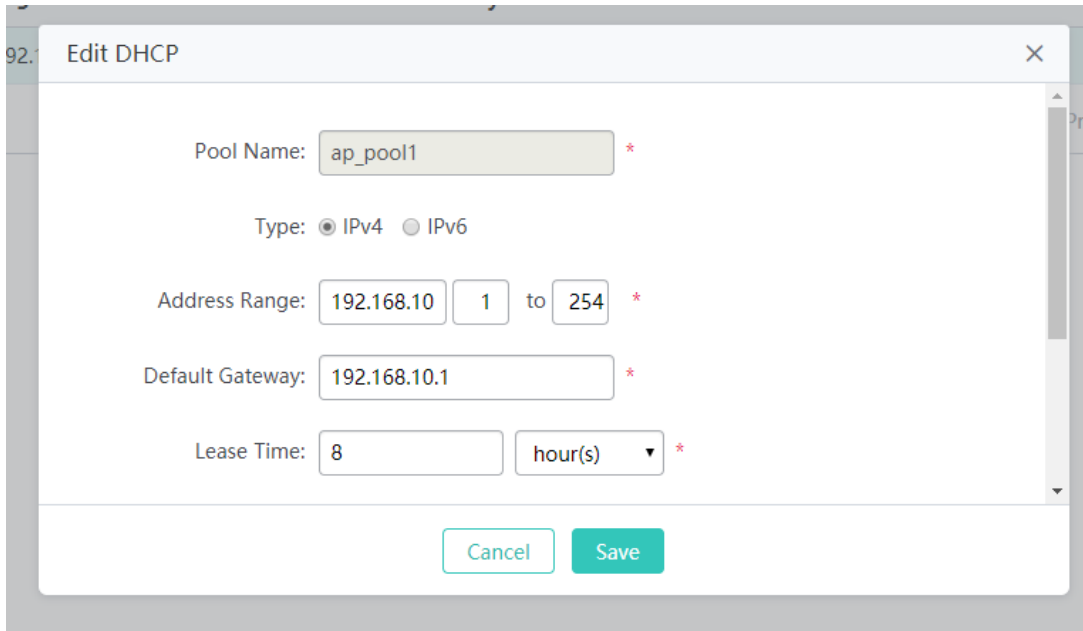


● DHCP service

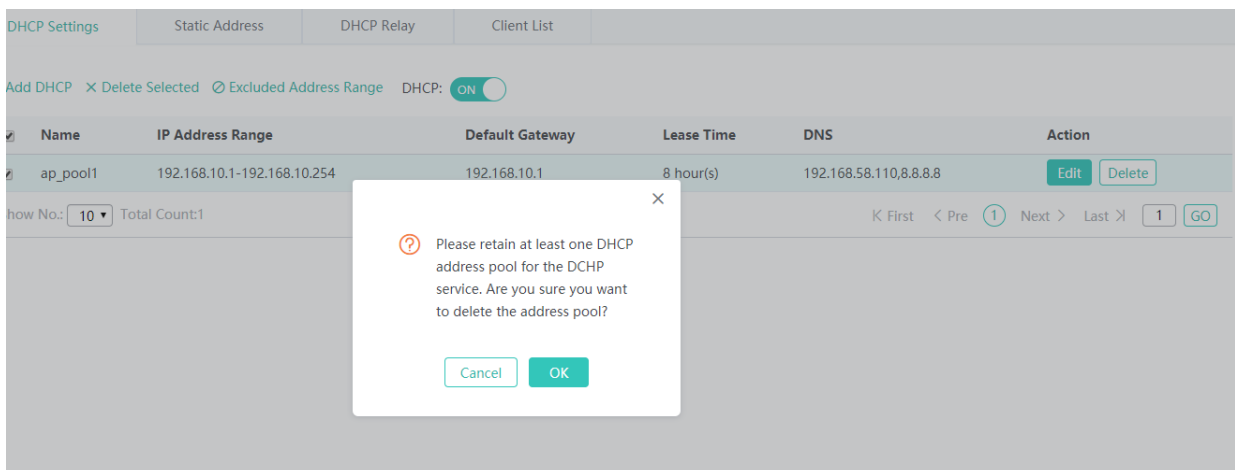


Click **DHCP: ON** to enable or disable the DHCP service.

● Editing a DHCP pool

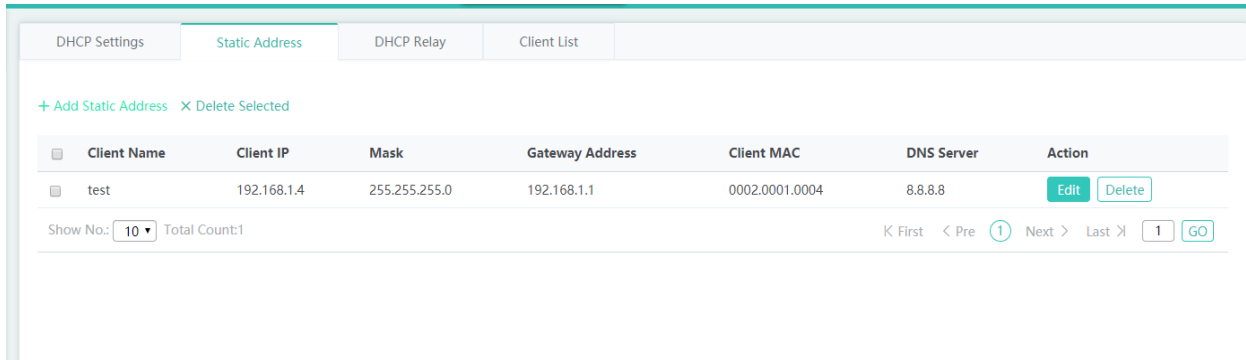


- 1) Click the **Edit** button for a DHCP pool in the list.
 - 2) The configuration for the DHCP pool is displayed in the dialog box. Next, edit the configuration.
 - 3) Click **Save**. The **Save operation succeeded** message is displayed.
- Deleting a DHCP pool

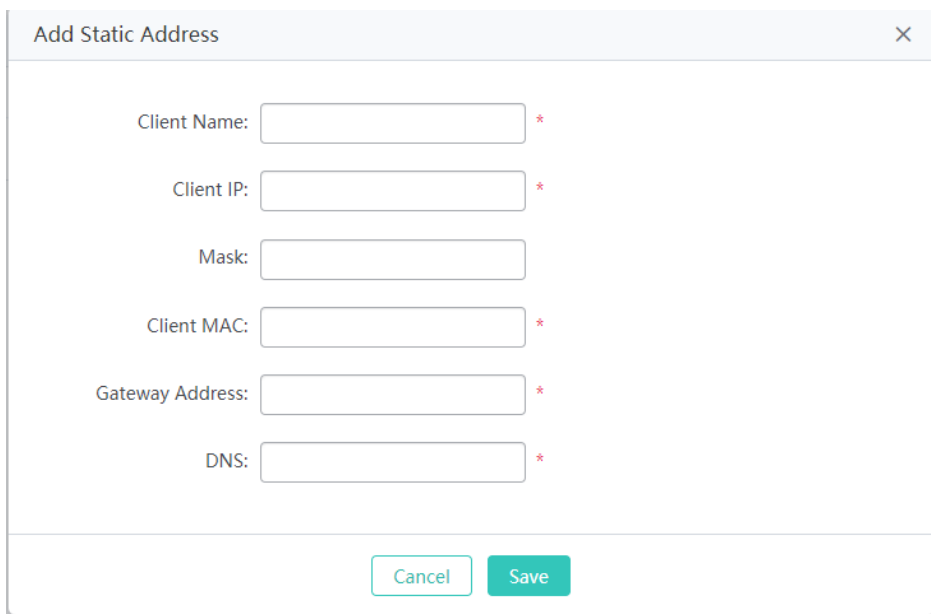


Click **Delete** to finish deleting.

➤ **Static Address**

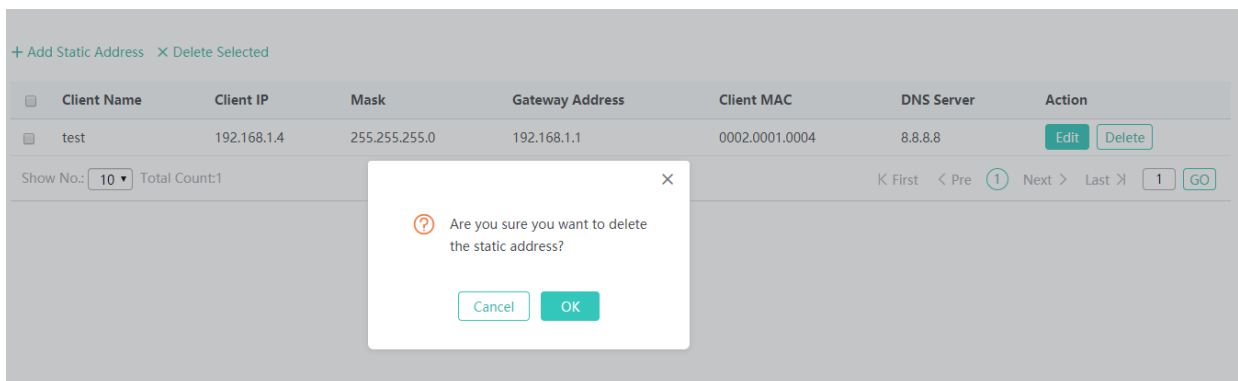


- Adding a static address



Click **Add Static Address**, set the configuration items in the displayed dialog box, and then click **Save**. The newly added static address is displayed in the list after the **Save operation succeeded** message is displayed.

- Deleting static addresses in batches



- 1) Select the static address from the list.
 - 2) Click **Delete Selected Address** and then click **OK** in the dialog box displayed to finish deleting.
- Editing a static address

Edit Static Address ×

Client Name: *

Client IP: *

Mask:

Client MAC: *

Gateway Address: *

DNS: *

- 1) Click the **Edit** button for a static address in the list. A dialog box is displayed.
 - 2) The configuration for the static address is displayed in the dialog box. Next, edit the configuration.
 - 3) Click **Save**. The **Save operation succeeded** message is displayed.
- Deleting a static address

+ Add Static Address
× Delete Selected

	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
<input type="checkbox"/>	test	192.168.1.4	255.255.255.0	192.168.1.1	0002.0001.0004	8.8.8.8	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.: Total Count:1

⏪ First
⏴ Pre
1
Next
⏵ Last
⏩
1
GO

? Are you sure you want to delete the static address?

Click the **Delete** button for a static address in the list to finish deleting.

↙ DHCP Relay

DHCP Settings Static Address **DHCP Relay** Client List

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

DHCP server IP1: +

Save

Enter the relay server address and click **Save**.

Client List

DHCP Settings Static Address DHCP Relay **Client List**

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

Bind MAC to Dynamic IP IP-based **Search**

IP	MAC	Lease Time	Allocation Type	Action
<input type="checkbox"/> 192.168.10.2	b40b.4456.f837	0 Day(s) 7 hour(s) 59 minute(s)	Dynamic Allocation	Delete

Show No.: Total Count:1 K First < Pre 1 Next > Last X 1 **GO**

- Binding a MAC address to a dynamic IP address

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

Bind MAC to Dynamic IP IP-based **Search**

IP	MAC	Lease Time	Allocation Type	Action
----	-----	------------	-----------------	--------

Show No.: Total Count:0 K First < Pre Next > Last X 1 **GO**

! Bind operation succeeded. STA information will be updated after the STA goes online next time.

OK

- 1) Select the static address from the list.
 - 2) Click **Bind MAC to Dynamic IP** and then click **OK** in the displayed dialog box to finish deleting.
- Querying clients based on IP address:

DHCP Settings Static Address DHCP Relay **Client List**

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

[Bind MAC to Dynamic IP](#) IP-based 192. **Search**

<input type="checkbox"/>	IP	MAC	Lease Time	Allocation Type	Action
<input type="checkbox"/>	192.168.10.2	b40b.4456.f837	0 Day(s) 7 hour(s) 59 minute(s)	Dynamic Allocation	Delete

Show No.: Total Count:1 < First < Pre 1 Next > Last > 1 **GO**

Input the IP address in the text box. Click **Search**. The search results meeting the criterion are displayed in the list.

1.3.3.3.6 Port Mapping

Generally, this function is used to map a specified port of a specified host in the internal network to a specified port of an external network address.

 This function may not be supported. The actual menu may vary with the device.

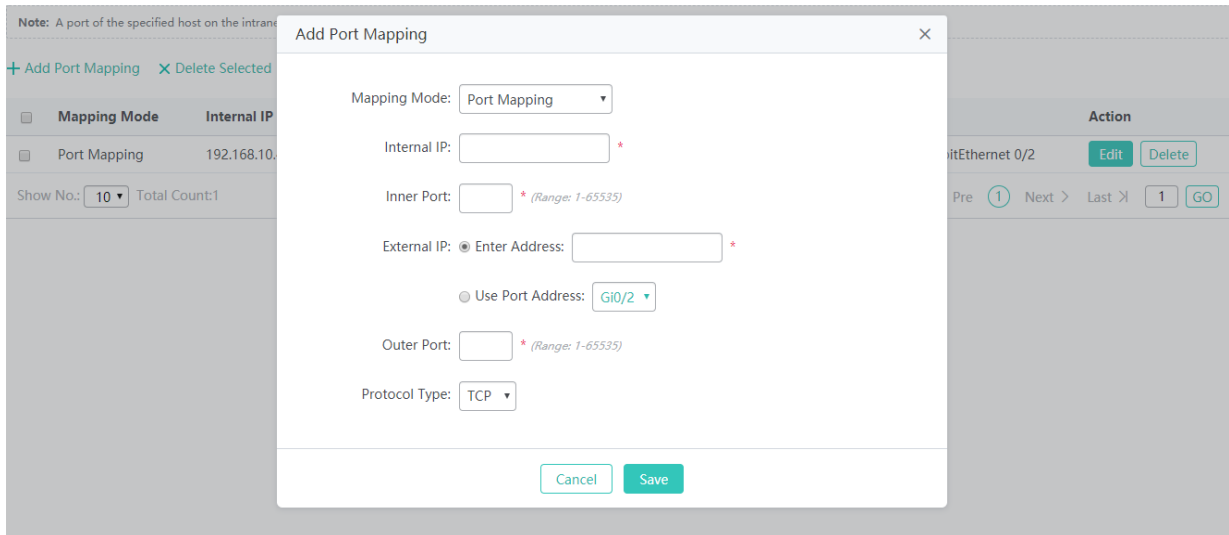
Note: A port of the specified host on the intranet is mapped to the specified port on the internet generally.

[+ Add Port Mapping](#) [X Delete Selected](#)

<input type="checkbox"/>	Mapping Mode	Internal IP Address	Inner Port	External IP Address	Outer Port	Protocol Type	Port	Action
<input type="checkbox"/>	Port Mapping	192.168.10.4	8083	-	8083	TCP	GigabitEthernet 0/2	Edit Delete

Show No.: Total Count:1 < First < Pre 1 Next > Last > 1 **GO**

- Adding port mapping



Click **Add Port Mapping**, set the configuration items in the dialog box displayed, and then click **Save**. The newly added port mapping is displayed in the list after the **Save operation succeeded** message is displayed.

- Batch deleting port mapping entries



- 1) Select the port mapping from the list.
- 2) Click **Delete Selected Port Mapping** and then click **OK** in the displayed dialog box to finish deleting.

- Editing port mapping

Edit Port Mapping
✕

Mapping Mode: Port Mapping ▼

Internal IP: 192.168.10.4 *

Inner Port: 8083 * (Range: 1-65535)

External IP: Enter Address: *

Use Port Address: Gi0/2 ▼

Outer Port: 8083 * (Range: 1-65535)

Protocol Type: TCP ▼

Cancel
Save

- 1) Click the **Edit** button for a port mapping in the list.
- 2) The configuration for port mapping is displayed in the dialog box. Next, edit the configuration.
- 3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting port mapping

Note: A port of the specified host on the intranet is mapped to the specified port on the internet generally.

+ Add Port Mapping ✕ Delete Selected

☐	Mapping Mode	Internal IP Address	Inner Port	External IP Address	Outer Port	Protocol Type	Port	Action
☐	Port Mapping	192.168.10.4	8083	-	8083	TCP	GigabitEthernet 0/2	Edit Delete

Show No.: 10 ▼ Total Count:1

K First < Pre 1 Next > Last > 1 GO

Click the **Delete** button for a port mapping entry in the list to finish deleting.

1.3.3.3.7 VPN

It is only allowed to configure VPN settings on a WAN port.

Note: IPSec settings only take effect on a layer-3 interface.

WAN Port: (If you change the WAN port here, please also change the uplink port on the device.)

Local IP Address: *(Example: 192.168.0.0)

Local Submask: *

HQ IP Address: *(Example: 192.168.0.0)

HQ Submask: *

VPN Address: *

Shared Key: *

The **Advanced Settings** include some algorithm settings. It is recommended to use the default settings.

Advanced Settings

Encryption Algorithm: DES 3DES AES256 AES192 AES128

Auth Algorithm: MD5 SHA

DH Group 5 2 1

ESP Encryption esp-des
Algorithm:

ESP Auth Algorithm: esp-md5-hmac

Keepalive Time(s):

1.3.3.4 Security

1.3.3.4.1 Containment

Rogue APs may exist in a WLAN. Rogue APs may have security vulnerabilities and can be manipulated by attackers to seriously threaten and endanger network security. The containment function can be enabled on the AP to attack rogue devices and prevent other wireless STAs from being associated with rogue devices.

Containment Settings

Containment Settings Trusted Device List 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.
Note: If you want to view rogue APs, please click[Rogue AP]

Rogue AP Containment: ON [\[Scan All Neighboring APs\]](#)

Working Mode: Monitor Hybrid Normal [?](#)

Apply to: AP Radio AI Radio [?](#)

Containment Mode: SSID Mode: Contain APs emitting the same WIFI signal as the current AP [\[Configure Phishing WIFI Keyword\]](#)

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

Rogue Mode: Contain APs according to RSSI

CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [\[+MAC Address\]](#) [\[+SSID Blacklist\]](#)

Enable Fuzzy Containment [?](#)

Containment Range: Scan/Contain APs in the same channel as the current AP

Scan/Contain APs in all channels (consuming more resources)

Click ON to enable or disable rogue AP containment for the device.

- Adding a MAC address

You can add the MAC address to be contained here.

Add MAC Address(BSSID) to be Contained ✕

[+ Add](#)

Current MAC: 8005.8808.17e0

- Adding an SSID blacklist

You can add the MAC address to be contained here.

Add SSID Blacklist ✕

+ Add

Cancel Save

Trusted AP

When the rogue AP containment function is enabled, the APs not authorized will be contained. However, some APs are trusted devices and special processing is required. You can configure the MAC addresses of trusted devices.

Containment Settings **Trusted Device List** Keyword

Note: The following MAC addresses correspond to trusted APs, which will not be contained.

Trusted MAC(BSSID):

+ Add

Trusted Vendor List

OUI: + Add

SSID: + Add

Multi-to-Multi

Save

↳ Phishing WiFi Keyword

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

Containment Settings Trusted Device List **Keyword**

Note: If an SSID matches with the keyword fuzzily, the WiFi is a phishing WiFi.
Note: The keyword takes effect only when fuzzy containment is enabled. Please enable fuzzy containment first. [Containment Settings]

Phishing WiFi Keyword1: +

Save

1.3.3.4.2 Prevent Share

Click this button to enable the sharing prevention function to detect whether one STA provides the proxy service to another and add the STA providing the proxy service to the STA dynamic blacklist.

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]

Prevent Share: OFF

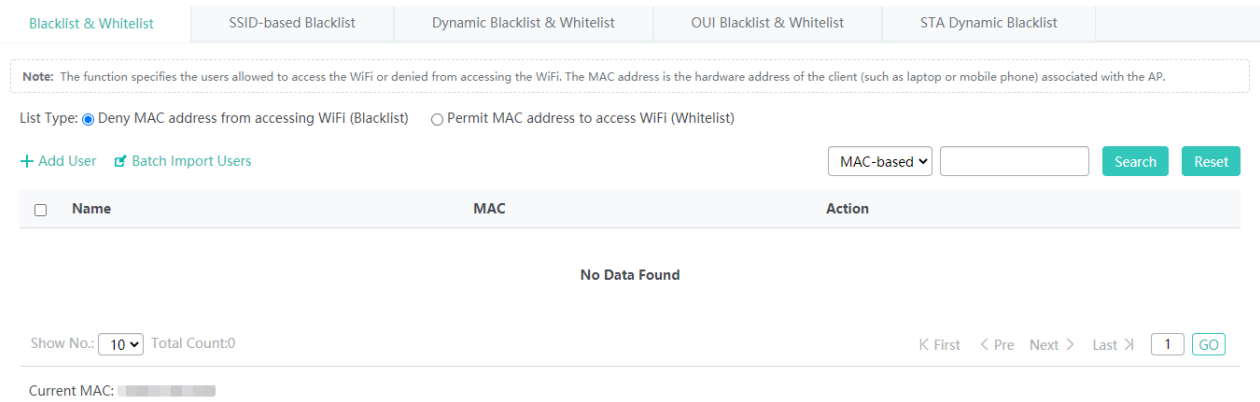
1.3.3.4.3 Blacklist & Whitelist

This function allows or blocks specified users from accessing the WiFi.

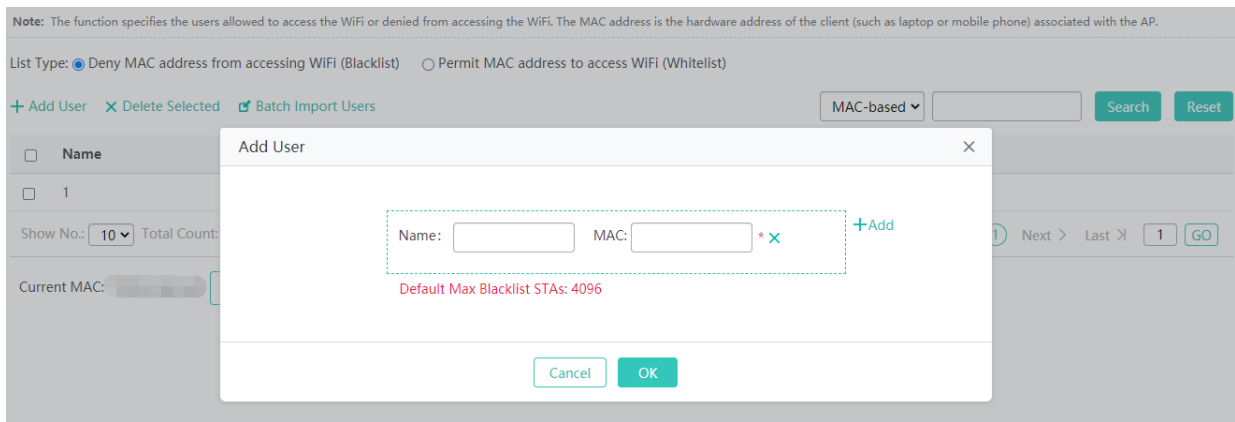
The whitelist/blacklist capacity is 1024 by default.

↳ Blacklist & Whitelist

Add the blacklist or whitelist user by adding the MAC address.

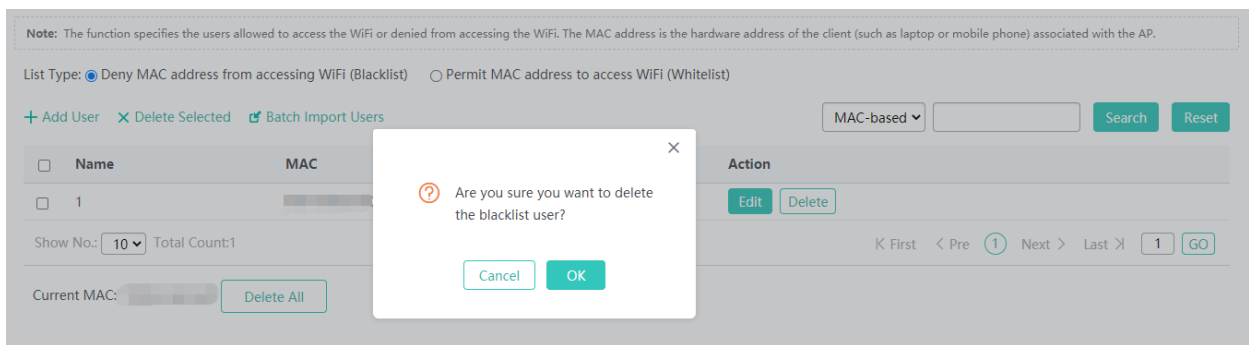


Click **+ Add User** to add a MAC address for a user. You can add multiple MAC addresses.



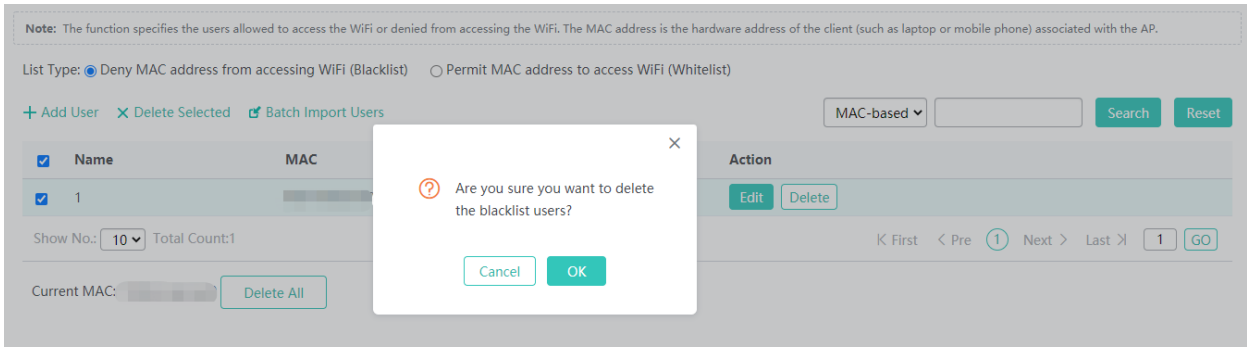
- Deleting a blacklist user

Click **Delete** to delete a MAC address for a user.



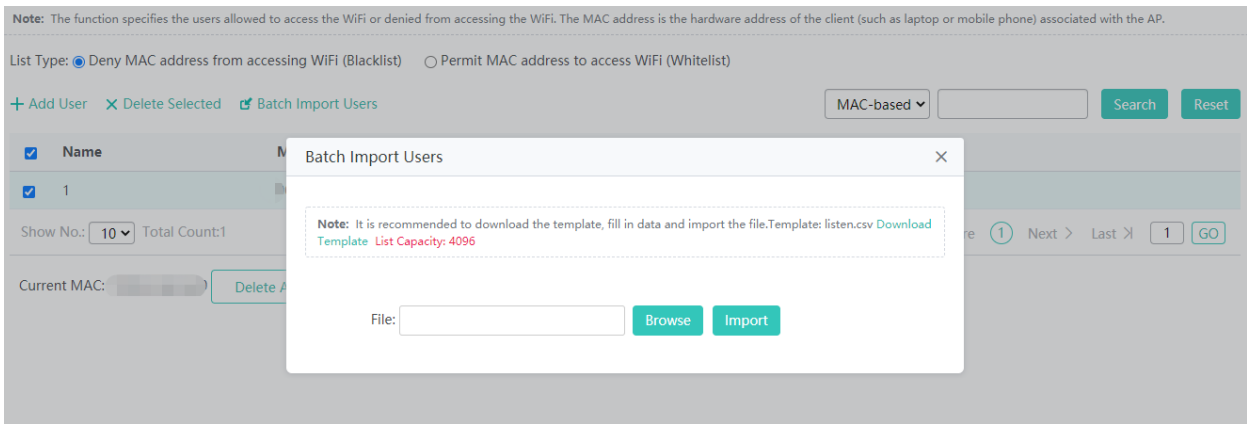
- Deleting blacklist users in batches

1. Select one or more records from the list.
2. Click **Delete Selected**.

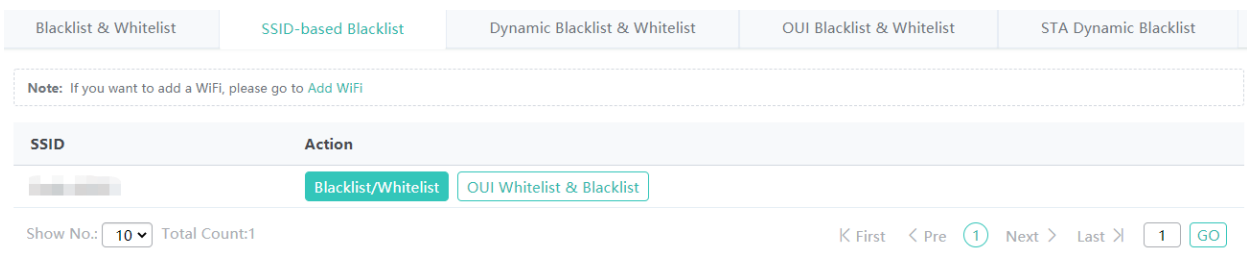


● Importing blacklist users

1. Click **Batch Import Users**.
2. Download the template file and enter the data.
3. Import the file.



📄 **SSID-based Blacklist**



Click **Blacklist/Whitelist** in the list and configure the whitelist/blacklist for the specified SSID.

Blacklist & Whitelist SSID-based Blacklist **Dynamic Blacklist & Whitelist** OUI Blacklist & Whitelist STA Dynamic Blacklist

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)

+ Add User ✚ Batch Import Users
 MAC-based ▾ Search Reset

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

Show No.: Total Count:0 ⏪ First < Pre Next > Last ⏩ GO

Current MAC:

You can select the blacklist/whitelist type, add blacklist/whitelist users, and import blacklist/whitelist users.

Dynamic Blacklist & Whitelist

Add malicious attack sources to the dynamic blacklist to prohibit access.

Blacklist & Whitelist SSID-based Blacklist **Dynamic Blacklist & Whitelist** OUI Blacklist & Whitelist STA Dynamic Blacklist

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: * (Range: 60-86400 seconds)

Save

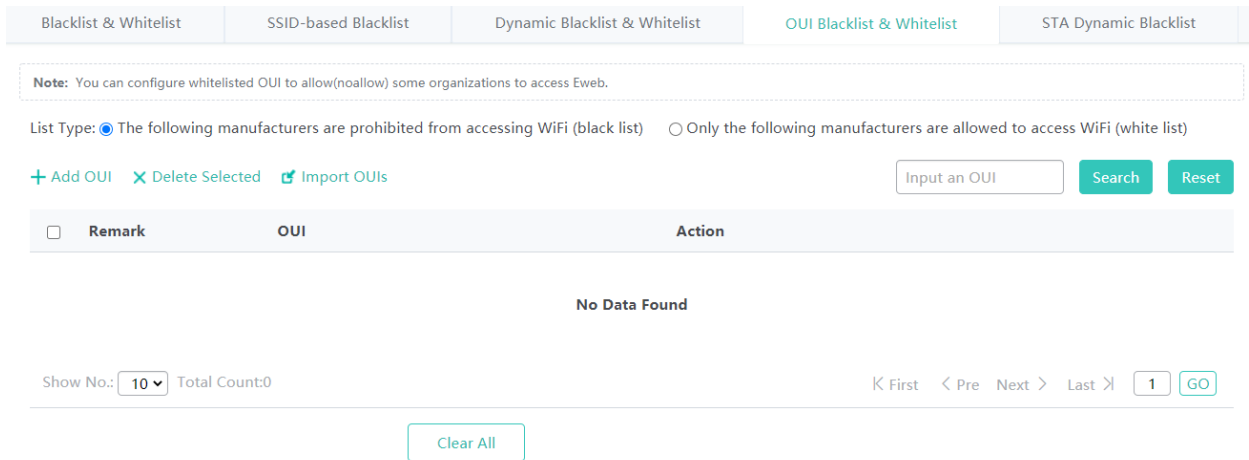
↻ Refresh ✕ Delete Selected

<input type="checkbox"/>	Number	MAC	Effective Time	Type	Action
No Data Found					

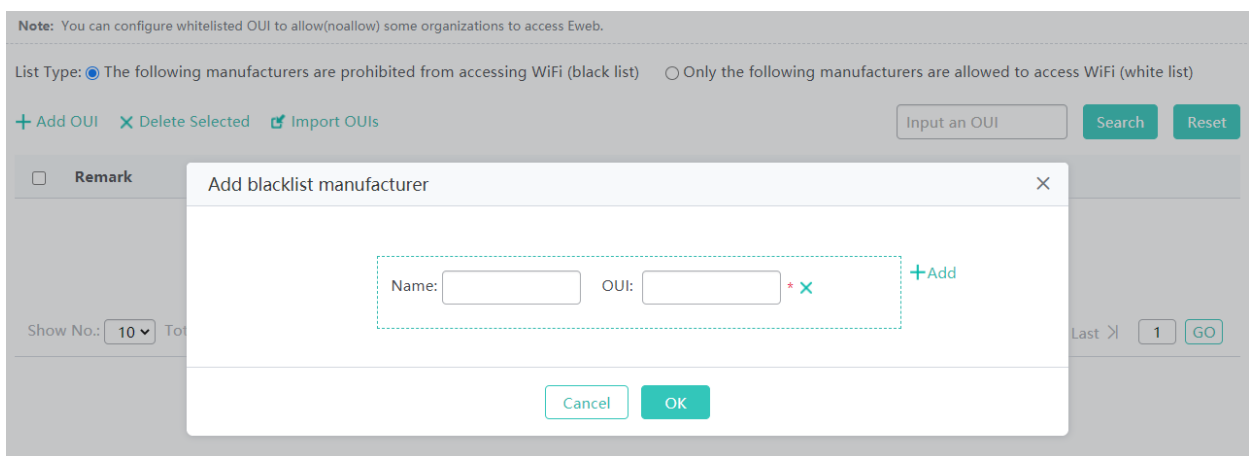
Show No.: Total Count:0 ⏪ First < Pre Next > Last ⏩ GO

- 1) Set the parameters and then save the configuration.
- 2) Select the blacklist from the list.
- 3) Click Delete Selected and then click OK in the displayed dialog box to finish deleting.

OUI Blacklist & Whitelist

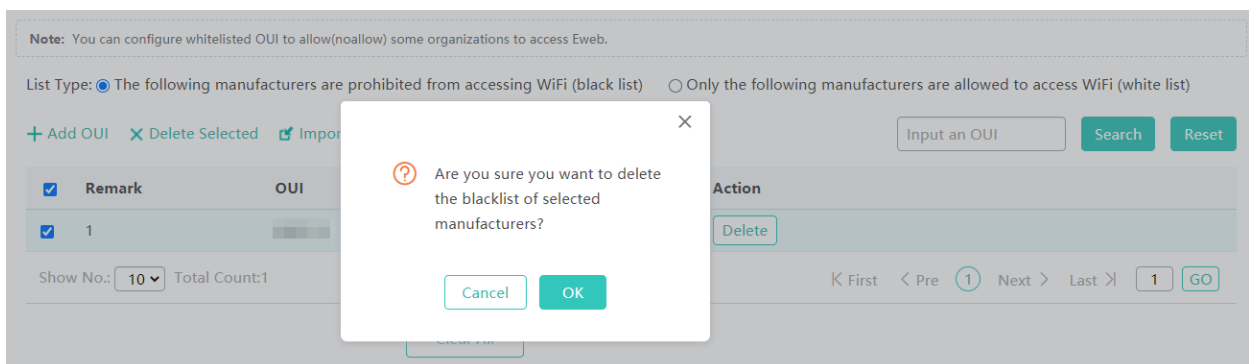


● Add OUI



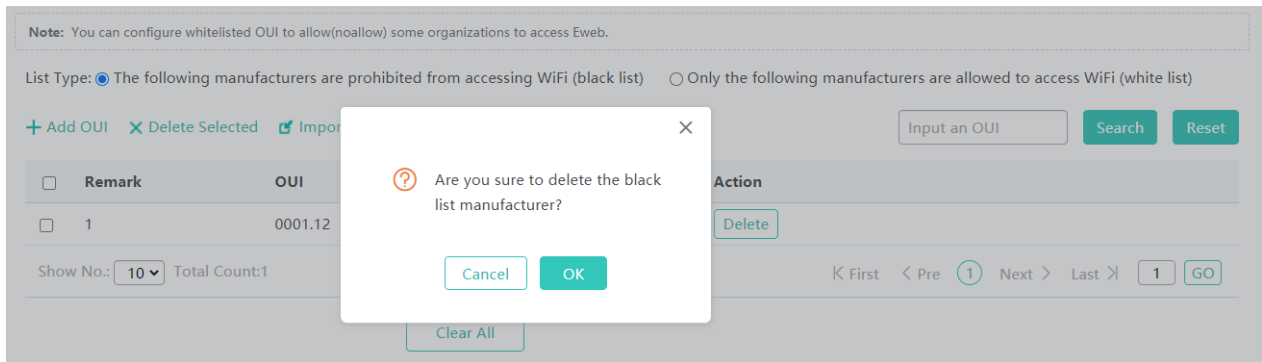
Click **Add OUI**, set the configuration items in the dialog box displayed, and click **Save**. The newly added OUI is displayed in the OUI list after the **Add succeeded** message is displayed.

● Deleting OUIs in batches



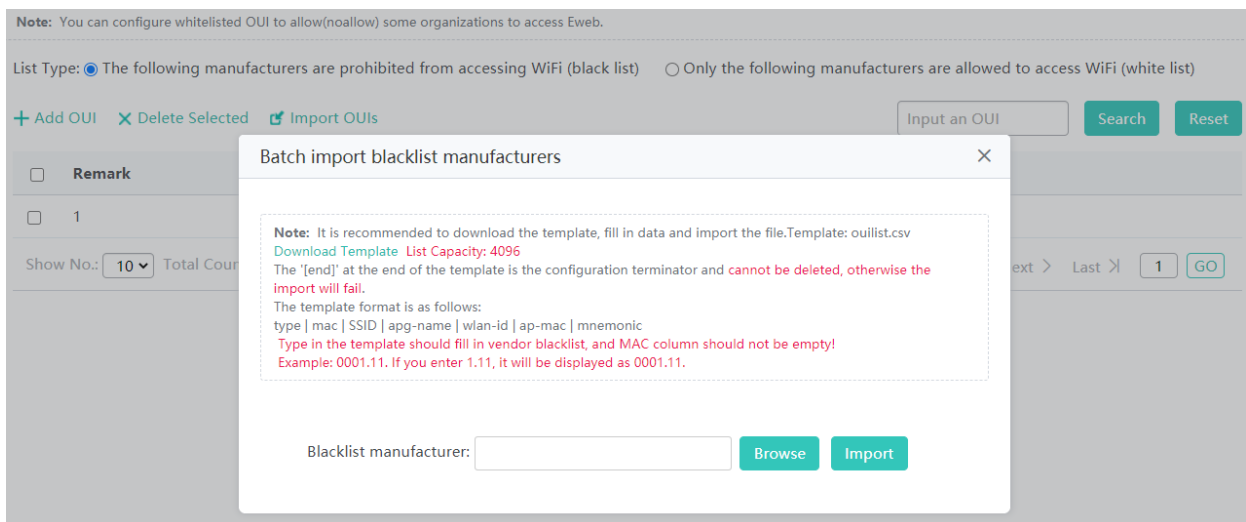
1. Select the OUI from the list.
2. Click **Delete Selected** and then click **OK** in the dialog box displayed to finish deleting.

- Deleting a OUI



Click **Delete** to finish deleting.

- Importing OUIs



1. Click **Import OUIs**.
2. Download the template file and enter the data.
3. Import the file.

📌 STA Dynamic Blacklist

Add malicious attack sources and illegitimate STAs to the STA dynamic blacklist to prevent their access.

Blacklist & Whitelist SSID-based Blacklist Dynamic Blacklist & Whitelist OUI Blacklist & Whitelist **STA Dynamic Blacklist**

Note: When the effective time runs out, the STA that in the dynamic blacklist will be removed from the blacklist automatically.

Dynamic Blacklist: On Refresh

Number	MAC	Add Time
No Data Found		

Show No.: Total Count:0 First < Pre Next > Last > 1 GO

Note: When the effective time runs out, the STA that in the dynamic blacklist will be removed from the blacklist automatically.

Dynamic Blacklist: On Refresh

Number	Add Time
--------	----------

Show No.: Total Count:0 First < Pre Next > Last > 1 GO

Are you sure you want to enable the STA dynamic blacklist function?

Cancel

Enable or disable the dynamic blacklist function.

1.3.3.4.4 User Isolation

To ensure network security and prevent unwitting information transfer, you can prohibit communication between internal network users by means of configuration. Some special users (users who can access each other) can be identified based on the user name and MAC address.


Note: The function prevents users from communicating with each other without affecting their access to the network, ensuring service security.
Note: Only Layer-2 isolation is supported currently.

User Isolation: ON

Whitelisted MAC: Username: MAC:

Current MAC: 0074.9cbd.af26

- 1) Click **User Isolation:** ON to enable or disable mutual access for internal network users.

- 2) Click  to delete the MAC address of the user.
- 3) Click the **Add** icon to add a MAC address for a mutual-access user. You can add multiple MAC addresses.
- 4) Click **Save** to finish the configuration.

1.3.3.4.5 Anti-attack

Some malicious attacks are always found in the network environment. These attacks may bring about an extremely heavy burden for the switch, resulting in the switch using an excessive amount of CPU power and giving rise to a potential operational failure.

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.
[\[DHCP-guard List\]](#)

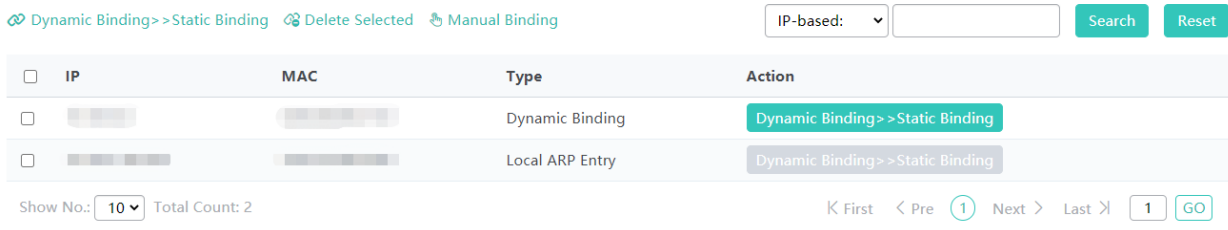
DHCPv6-guard: Enable DHCPv6-guard, so as to prevent malicious requests from exhausting DHCPv6 pools and leaving legitimate users unable to access the Internet.
[\[DHCPv6-guard List\]](#)

ND-guard: Enable ND-guard, so as to prevent Neighbor Discovery packets from consuming bandwidth.

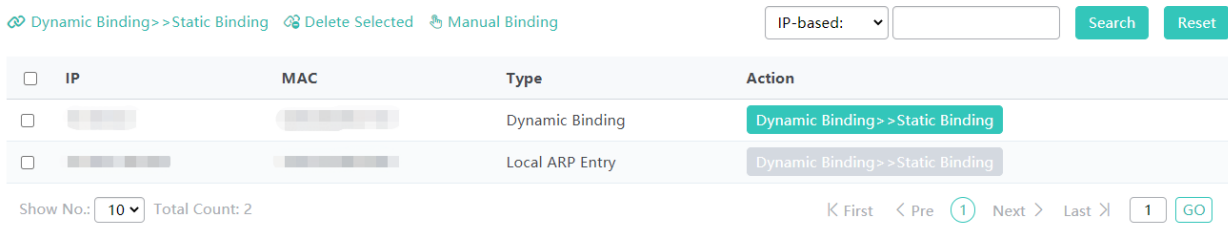
Display NFPP Log: [\[Display NFPP Log\]](#)

- 1) **ARP-guard**: Enables ARP-guard configuration. Click the **ARP-guard List** link to view the host where ARP attack is detected.
- 2) **IP-guard**: Enables IP-guard configuration. Click the **IP-guard List** link to view the host where IP scanning is detected.
- 3) **ICMP-guard**: Enables ICMP-guard configuration. Click the **ICMP-guard List** link to view the host where an ICMP attack is detected.
- 4) **DHCP-guard**: Enables DHCP-guard configuration. Click the **DHCP-guard List** link to view the host where a DHCPv4 attack is detected.
- 5) **DHCPv6-guard**: Enables DHCPv6-guard configuration. Click the **DHCPv6-guard List** link to view the host where a DHCPv6 attack is detected.
- 6) **ND-guard**: Enables ND-guard configuration.

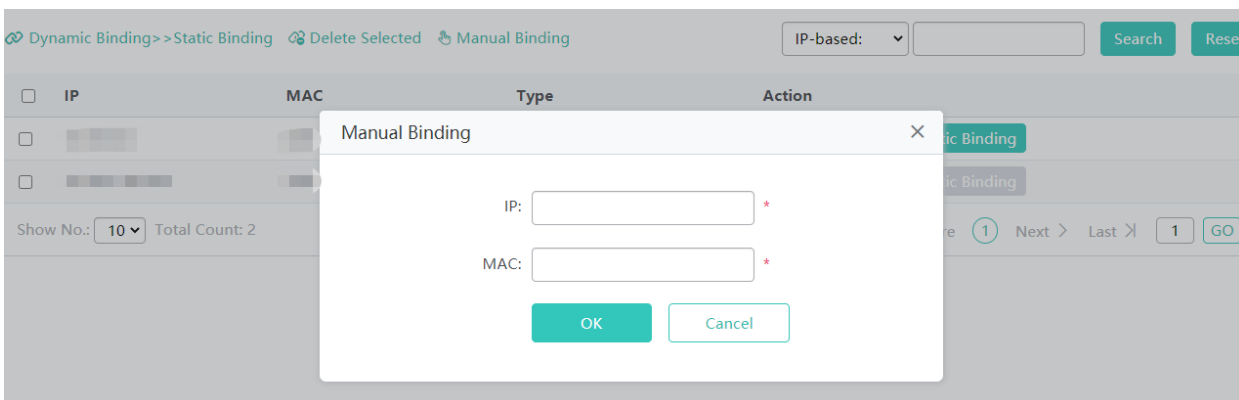
1.3.3.4.6 ARP



- Dynamic Binding>>Static Binding
 - 1) Select one or multiple records from the ARP list.
 - 2) Click the **Dynamic Binding>>Static Binding** icon to switch from dynamic binding to static binding in batches.
- Remove static Binding



- 1) Select one or multiple records from the ARP list.
 - 2) Click the **Delete Selected** icon to remove static binding in batches.
- Manual Binding



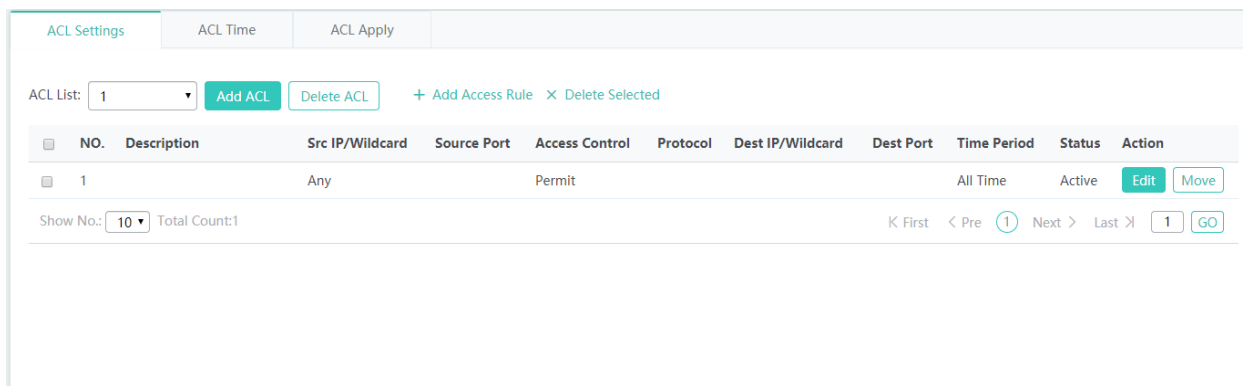
- 1) Click the **Manual Binding** icon.
 - 2) Set the IP address and MAC address.
- Click **OK**. The newly bound ARP is displayed in the ARP list after the **Save operation succeeded** message is displayed.

1.3.3.4.7 ACL

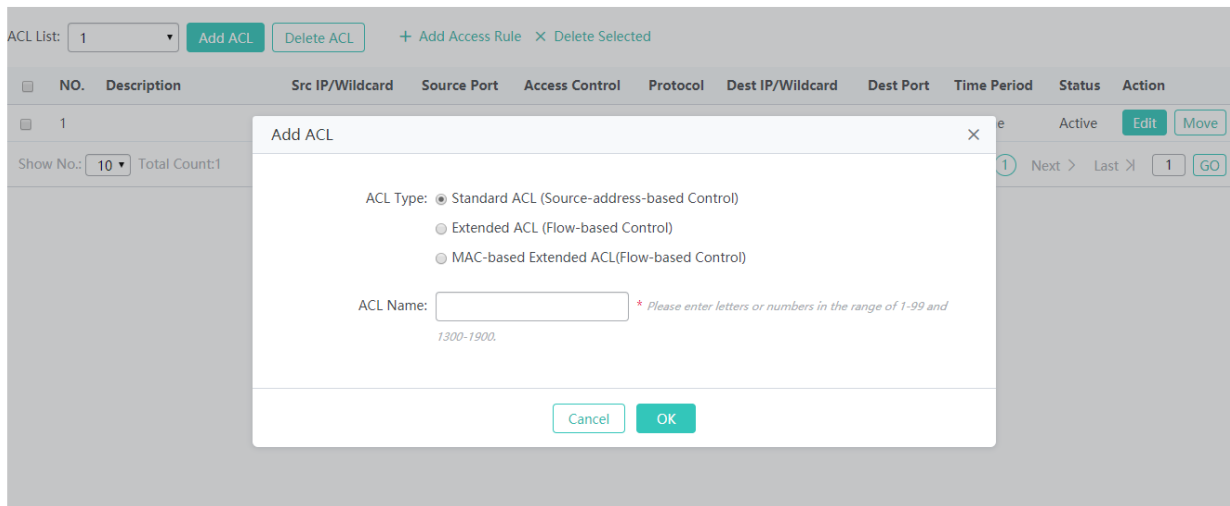
When receiving a packet on a port, the input ACL checks whether the packet matches the ACE entry for this port. When the device intends to output a packet through a port, the output ACL checks whether the packet matches the ACE entry for this port.

When there are different filtration rules, multiple rules may be applied simultaneously and only several of them can be applied. If a packet matches an ACE entry, this packet is processed (permitted or denied) according to the action policy defined by this ACE.

ACL Settings

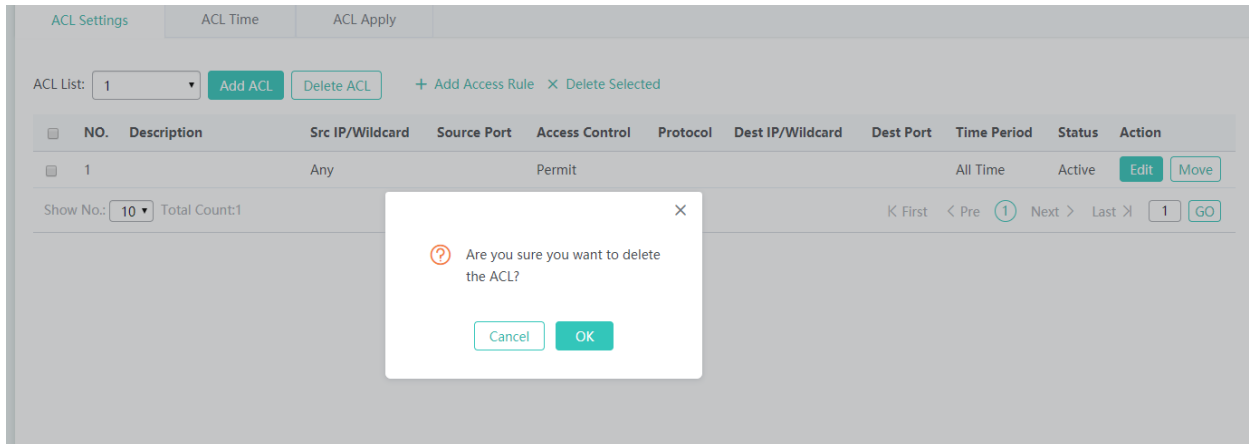


- Adding an ACL

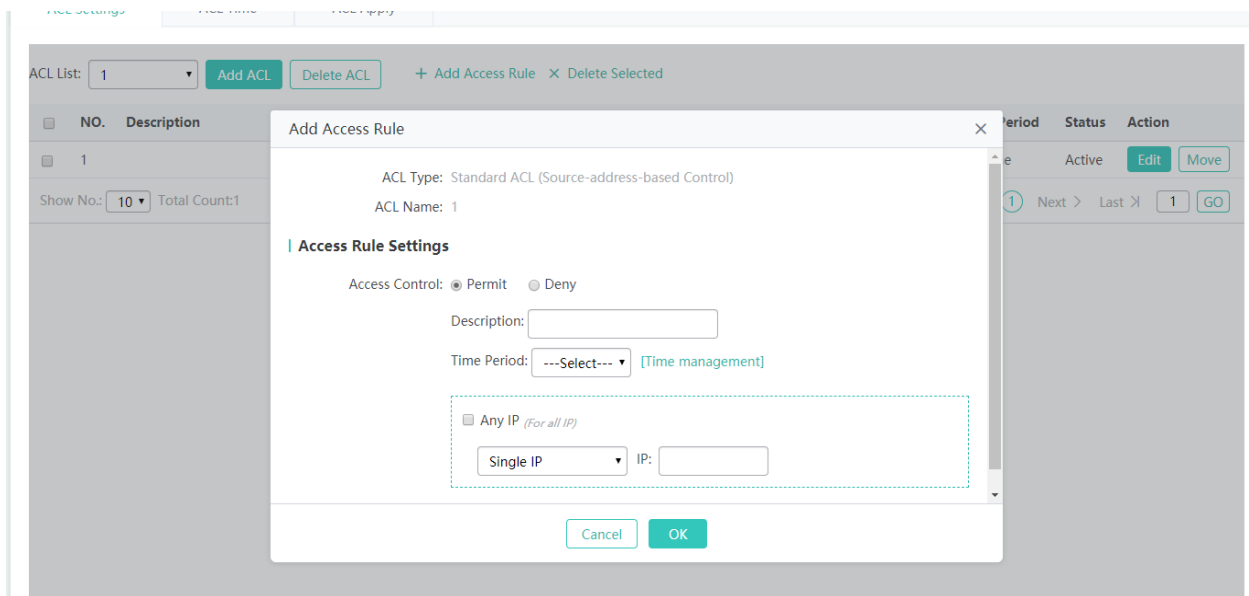


Click **Add ACL** and set the configuration items in the dialog box displayed. Click **OK**. The newly added ACL is displayed in the **ACL List** drop-down list on the left after the **Save operation succeeded** message is displayed.

- Deleting an ACL

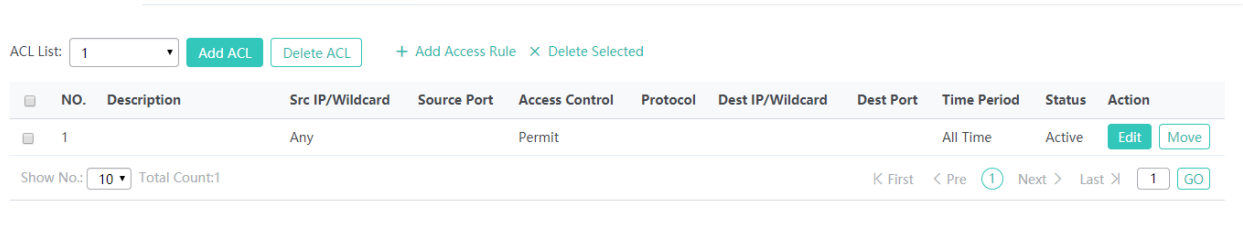


- 1) Select the ACL from the **ACL List** drop-down list.
 - 2) Click **Delete ACL** to finish deleting.
- Adding an access rule



- 1) Click **Add Access Rule**.
 - 2) Set the configuration items in the dialog box displayed.
 - 3) Click **OK**. The newly added access rule is displayed in the access rule list after the Save operation succeeded message is displayed.
- Editing an access rule
- 1) Click the **Edit** button for an access rule in the access rule list.
 - 2) The configuration for the access rule is displayed in the dialog box and the configuration can be edited.
 - 3) Click **OK**. The **Save operation succeeded** message is displayed.

- Deleting an access rule

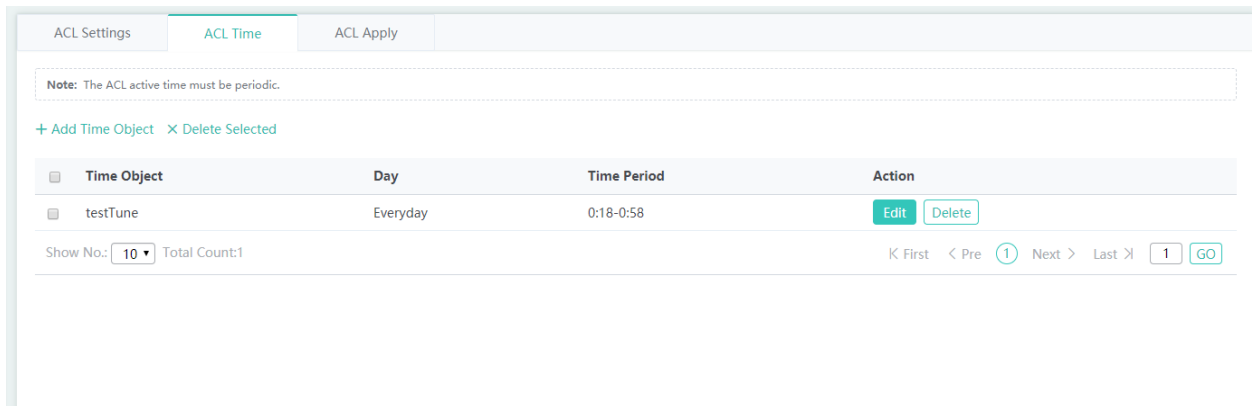


1) Select one or multiple records from the access rule list.

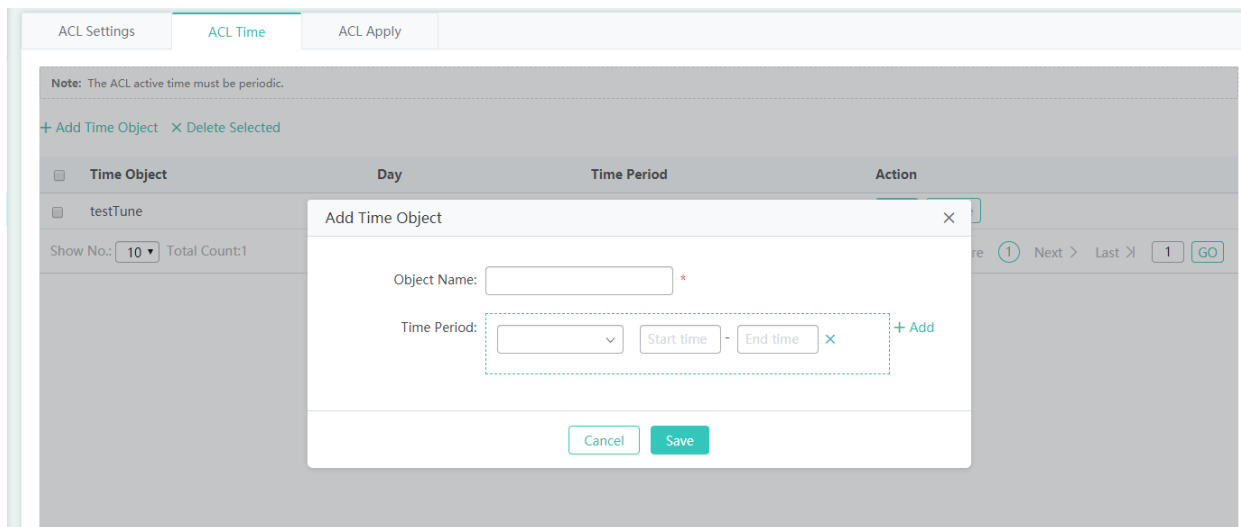
Click **Delete Selected** and then click **OK** in the displayed dialog box to finish deleting ACL Time

ACLs based on time can be enabled. For example, you can set ACLs to take effect in different time segments for a week, but first a time object must be configured.

ACL Time



- Adding a time object



Click **Add Time Object**, then set the configuration items in the dialog box displayed, and click **Save**. The newly added time object is displayed in the time object list after the **Save operation succeeded** message is displayed.

- Deleting time objects in batches

Note: The ACL active time must be periodic.

+ Add Time Object × Delete Selected

<input type="checkbox"/>	Time Object	Day	Time Period	Action
<input type="checkbox"/>	test2	Tuesday	16:00-21:58	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	testTune	Everyday	0:18-0:58	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.: Total Count:2 K First < Pre ① Next > Last X 1

- 1) Select one or multiple records from the time object list.
- 2) Click **Delete Selected** and then click **OK** in the dialog box displayed to finish deleting.

- Editing a time object

Edit Time Period
×

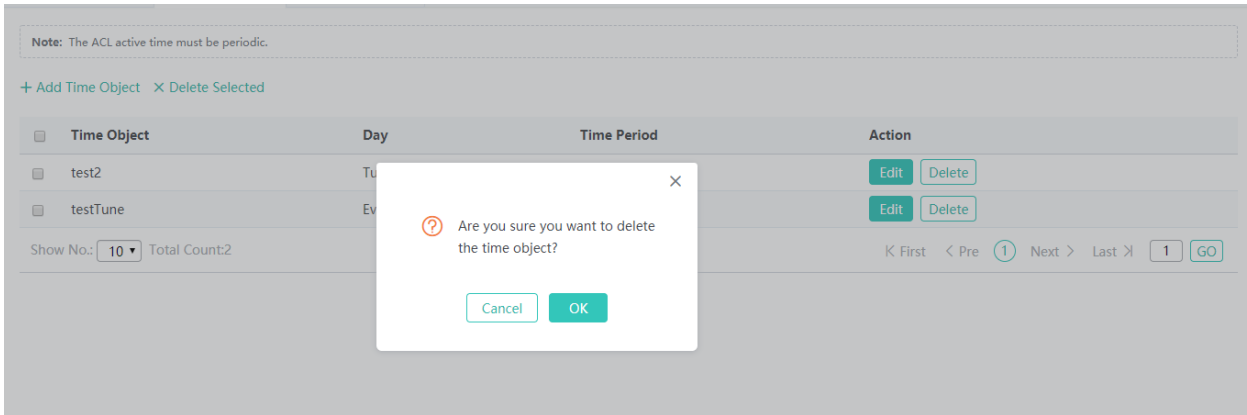
Object Name: *

Time Period:

 -
×
 + Add

- 1) Click the **Edit** button for a time object in the list.
- 2) The configuration about the time object is displayed in the dialog box. Then edit the configuration.
- 3) Click **Save**. The **Save operation succeeded** message is displayed.

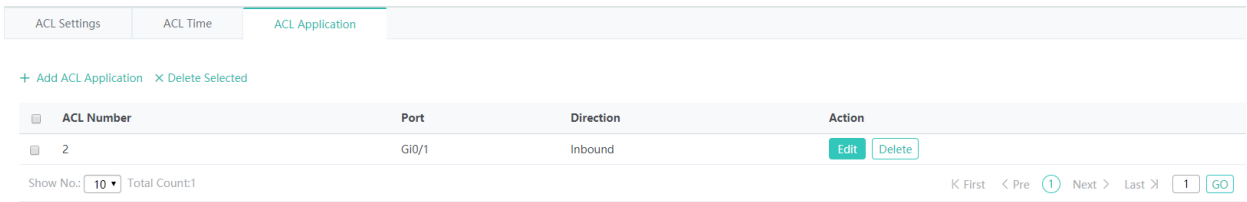
- Deleting a time object



Click the **Delete** button for a time object in the list.

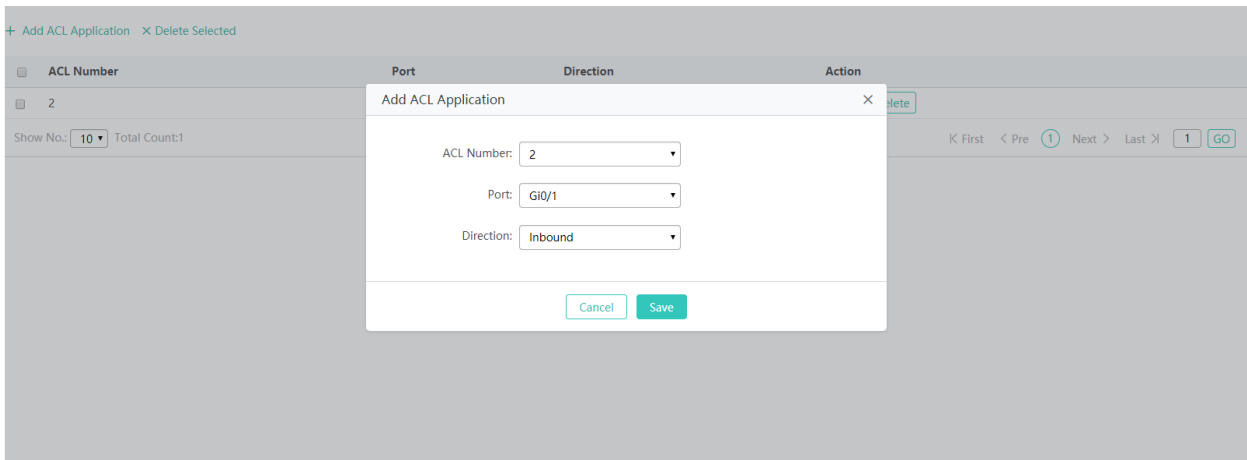
ACL Application

Apply an ACL to a port or a WiFi to limit user access.

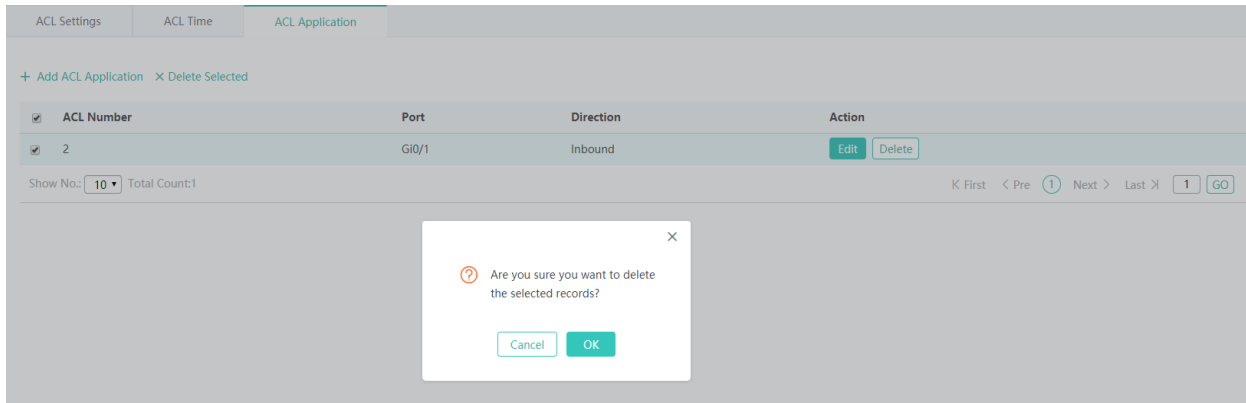


- Adding an ACL application

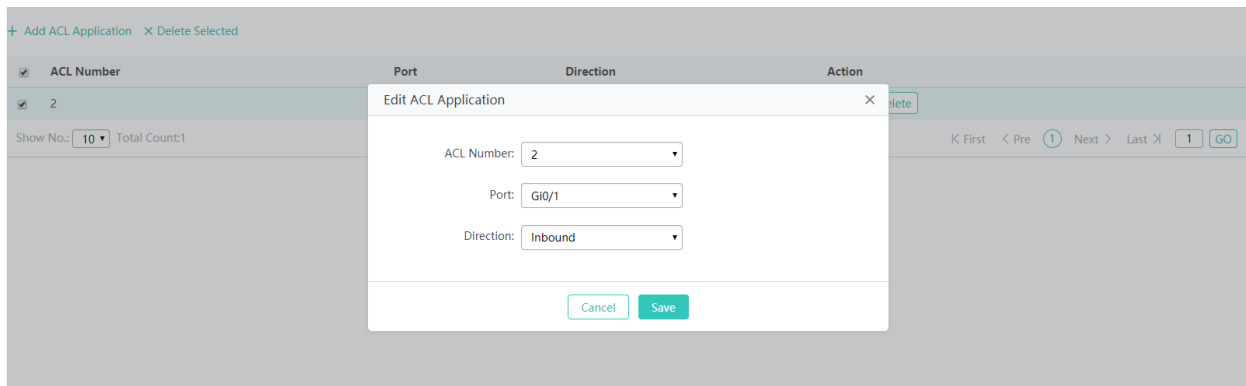
1. Click **+ Add ACL Application**.
2. Select ACL number, port and direction in the popup window.
3. Click **Save**. After the message "Configuration succeeded." is displayed, the ACL will appear in the list.



- Deleting selected ACL applications



- Editing an ACL application



1.3.3.5 Authentication

1.3.3.5.1 Web Authentication

Web authentication allows you to control user access to the Internet. The users can perform authentication on the browser without installing any application, which is easy and convenient. Web authentication can be classified into iPortal authentication and ePortal authentication based on the server location.

↳ ePortal Authentication

Unauthenticated users will be redirected to the specified website for authentication. If the Portal is not built into the AC, please select ePortal authentication.

ePortal Authentication | iPortal 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: [Radius Server Settings]

Accounting Server:

SNMP Server: [SNMP Server] *

SSID: [WiFi/WLAN Settings]

» Advanced Settings

Save Clear

↳ iPortal Authentication

Unauthenticated users will be redirected to the specified website for authentication. If the Portal is built into the AC, please select iPortal authentication.

ePortal Authentication | iPortal Authentication

Download Template: Default

Authentication Package: Default Package Custom Package

Authentication Mode: [Radius Server] [SNMP Server]

iPortal Server Port: (Range: 1025-65535, Default: 8081)

AD Push Mode: No AD

SSID:

» Advanced Settings

Save Clear

1.3.3.5.2 WeChat Authentication

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 authentication modes are available: WiFi Auth 3.x and WiFi+SMS Auth. (The default is the WeChat template)

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: *

NAS IP: *

Target WiFi: [WiFi/WLAN Settings]

DNS: *

[» Advanced Settings](#)

Choose **Advanced Settings > Parameter Settings > Advanced.**

WeChat Auth-Advanced Settings ×

Escape Clients Function: ON [View Escape Clients](#)

Seamless Auth: ON

Choose **Advanced Settings > Parameter Settings > Whitelist Settings.**

WeChat Auth Whitelist Settings✕

Redirection HTTP Port: (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.

Kick Inactive Users Off: Enable

Whitelisted Network Resource: All users(including unauthorized users) can access the server IP address. You can configure up to 50 IP addresses.

IP: Mask: ✕ +Add

Whitelisted User IP: The user can access the network without authentication. You can configure up to 50 IP addresses.

IP: Mask: ✕ +Add

Whitelisted MAC: The user can access the Internet without authentication. You can configure up to 50 MAC addresses.

MAC: ✕ +Add

1.3.3.5.3 WiFiDog Authentication

WiFiDog Authentication enables new users to be redirected to the authentication page.

Note: WiFiDog authentication enables new users to be redirected to the authentication page

Portal Server IP: * [More](#)

Redirection URL: *

NAS IP: *

Gateway ID:

Redirection Mode:

SSID: [\[WiFi/WLAN Settings\]](#)

⌵ [Advanced Settings](#)

Parameter Settings: [\[Advanced Settings\]](#)

Choose **Advanced Settings > Advanced Settings**.

Advanced Settings ×

Redirection HTTP Port: (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.

Kick Inactive Users Off: Enable

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: ×

+Add

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: ×

+Add

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: ×

+Add

Whitelisted URL: Enable

Advanced Settings provide some optional features applicable to both Web authentication V1 and Web authentication V2.

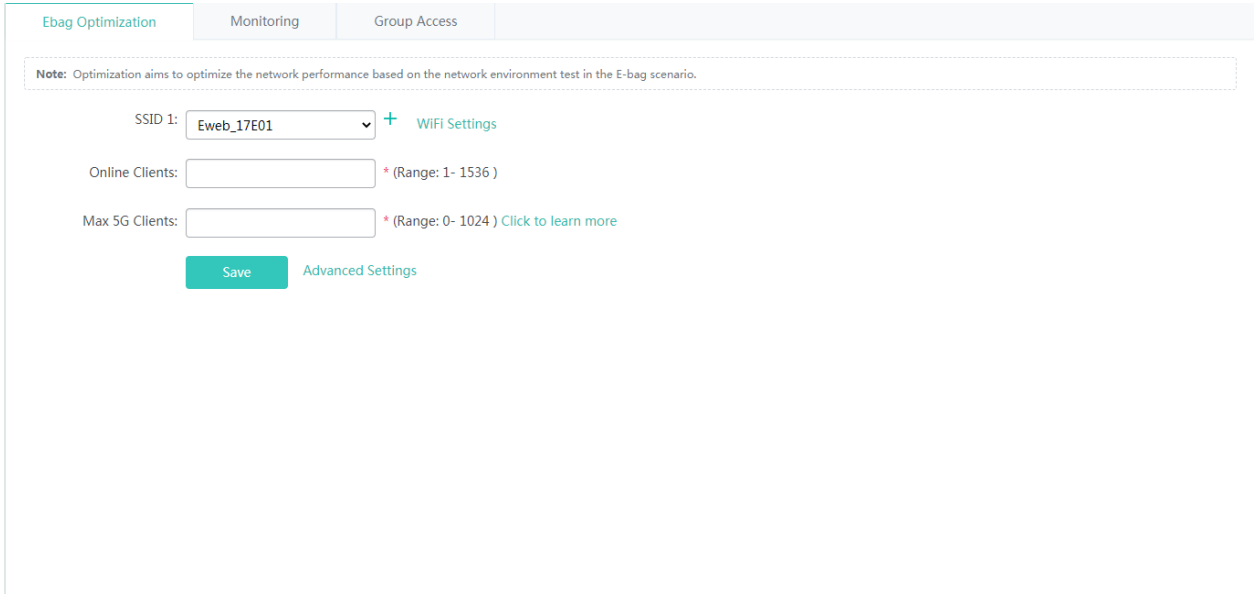
1.3.3.6 Solution

1.3.3.6.1 E-bag Optimization

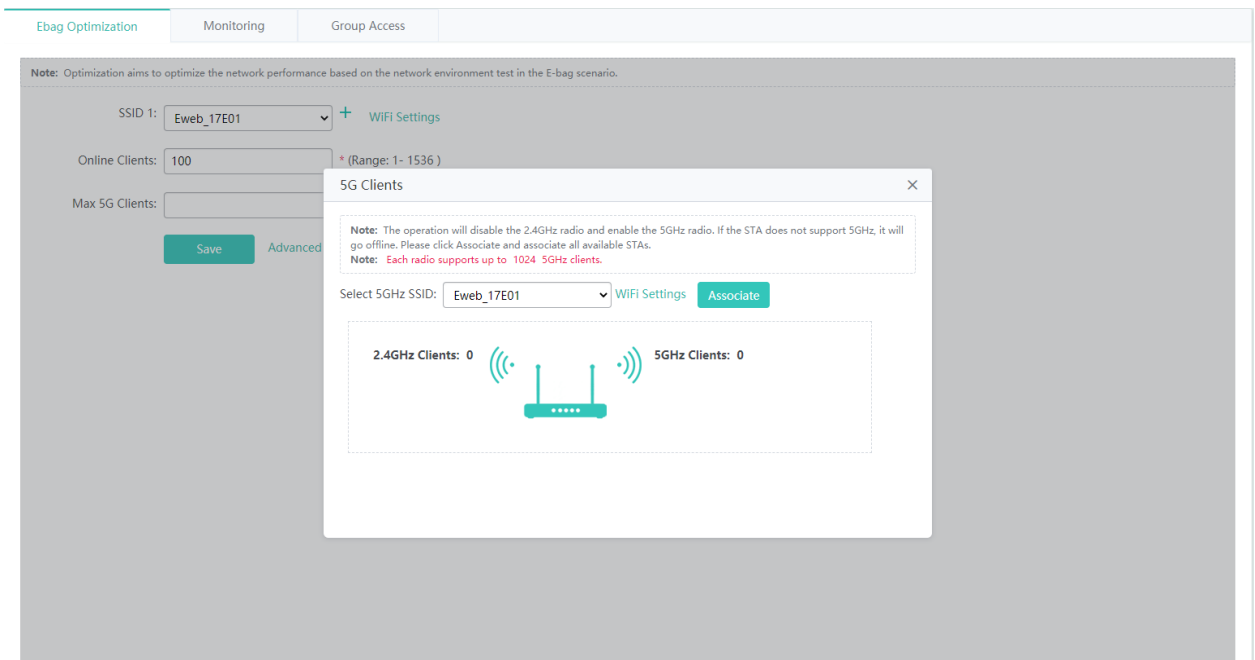
 Your AP might not support this function. The menu may vary with the device.

This function is mainly applicable to the E-bag solution for schools. Balanced optimization ensures a smooth network experience and avoids disconnection when a user uses the E-bag application.

E-bag Optimization



Click **Click to learn more**, and the following page will appear.



Select an SSID, and click **Associate** to enable all 5G clients in the classroom to connect to this SSID. The maximum number of 5G clients will be calculated automatically.

Ebag Optimization Monitoring Group Access

Note: Optimization aims to optimize the network performance based on the network environment test in the E-bag scenario.

SSID 1: + [WiFi Settings](#)

Online Clients: * (Range: 1- 1536)

Max 5G Clients: * (Range: 0- 1024) [Click to learn more](#)

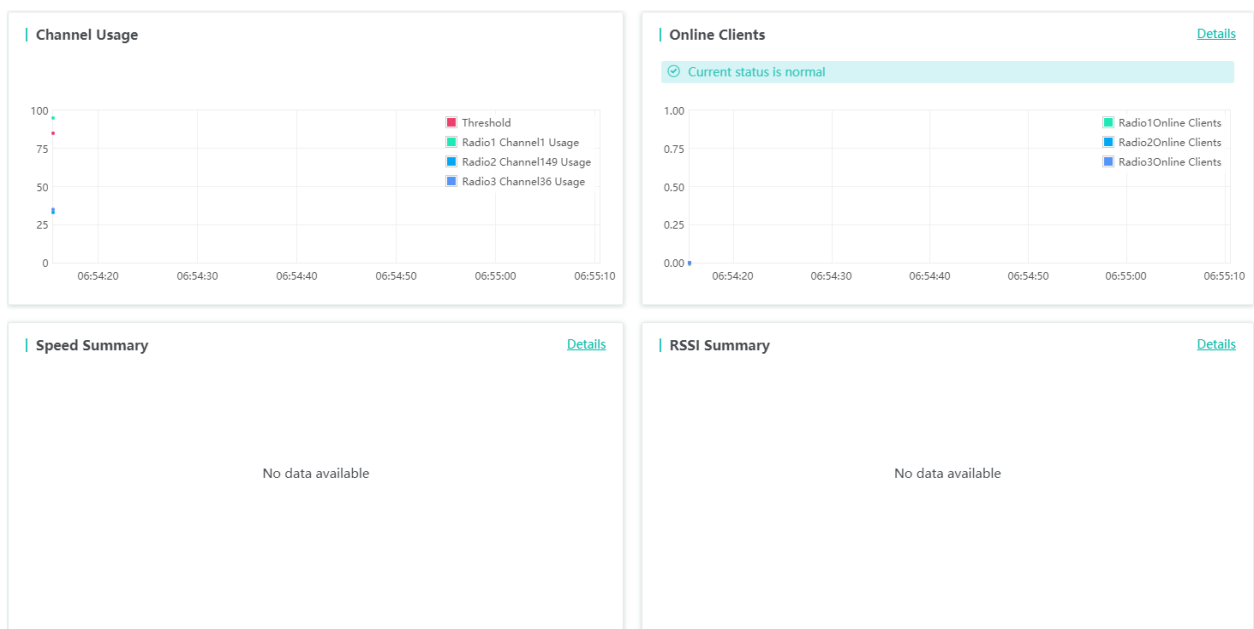
[Advanced Settings](#)

Enter the maximum number of 5G clients here, and click **Save**. E-bag optimization settings will take effect.

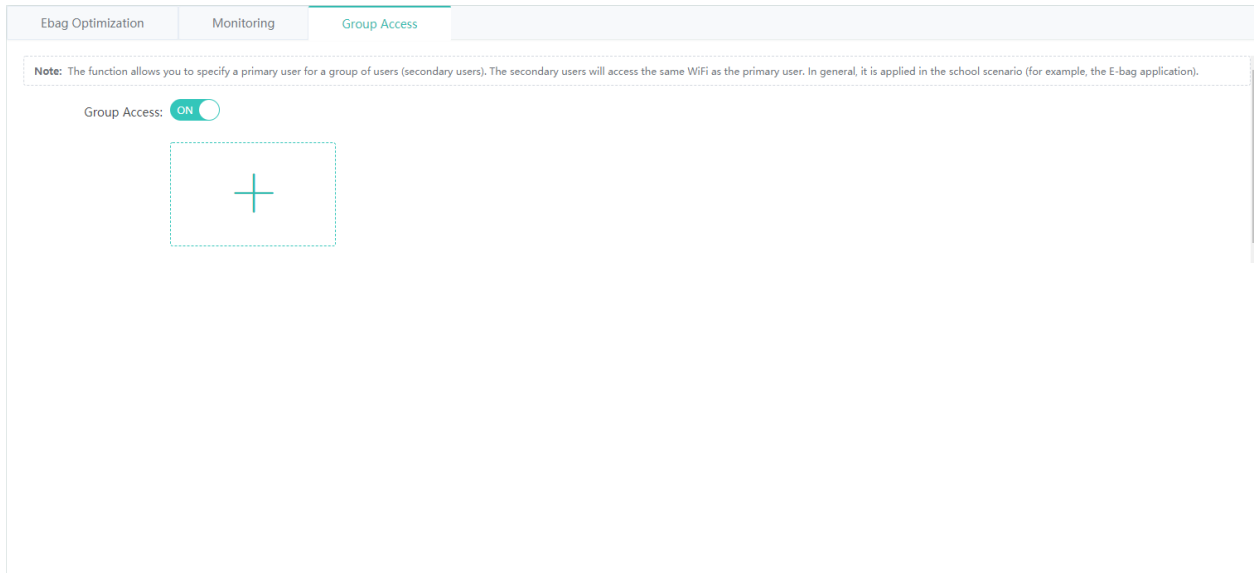
You can click **Advanced Settings** to configure advanced settings. If you perform E-bag optimization again, the advanced settings will be overridden.

Monitoring

This function allows you to monitor the network performance after E-bag settings are applied.

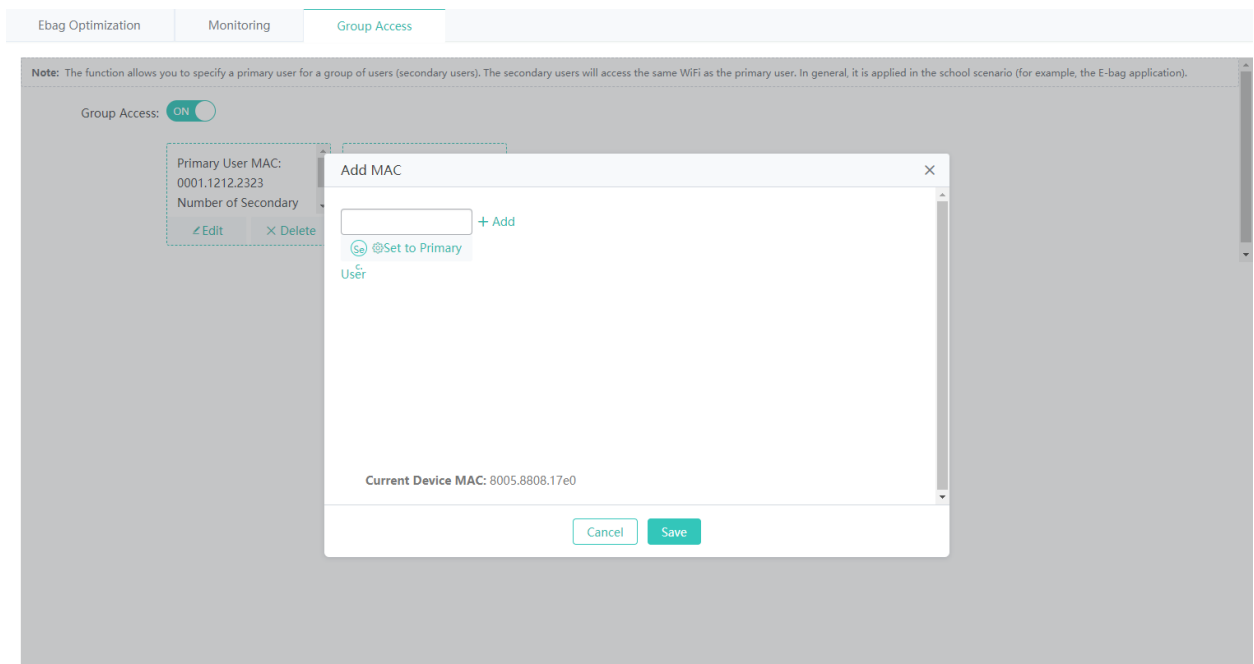


Group Access



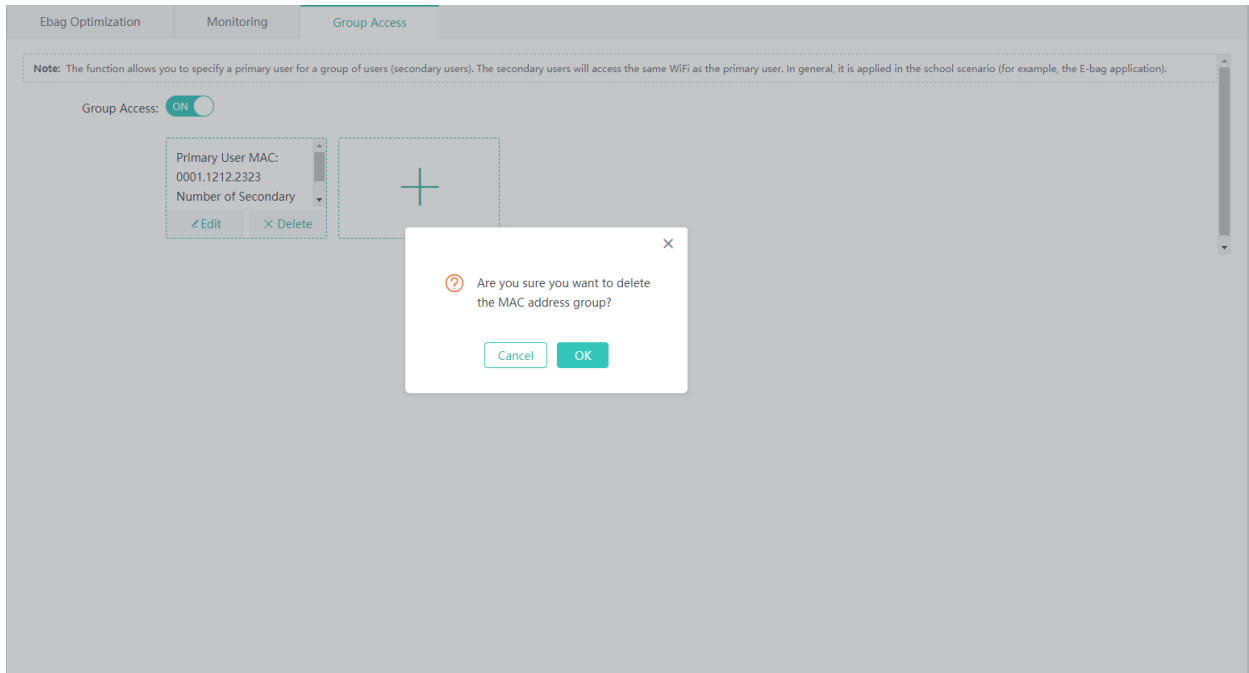
Toggle the **Group Access:** button to enable or disable the Group Access function.

- Adding a user group



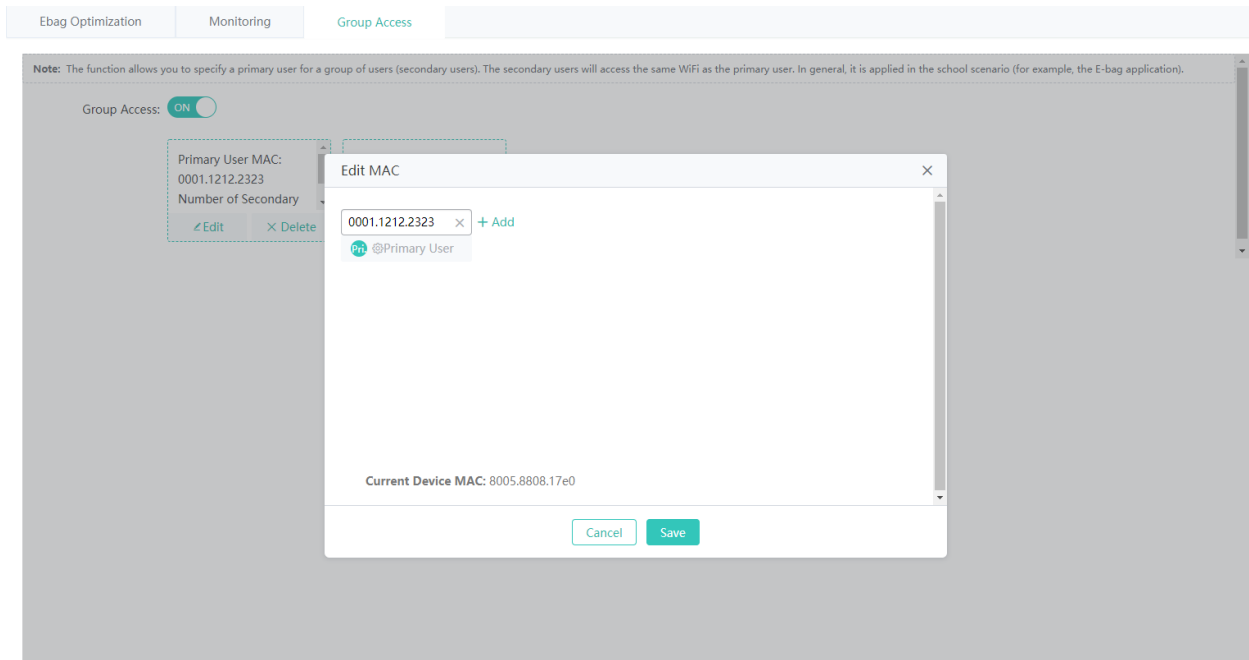
1. Click +.
2. On the **Add MAC** page, enter a MAC address.
3. Click **Save**, and the "Add succeeded." message appears.

- Deleting a user group



1. Click **Delete**.
2. In the deletion confirmation box, click **OK**.
3. The "Delete succeeded." message appears, indicating that the MAC address is deleted.

- **Editing a user group**



1. Click **Edit**.

2. On the **Edit MAC** page, edit the MAC address.
3. Click **Save**, and the "Edit succeeded." message appears.

1.3.3.7 Advanced

1.3.3.7.1 Unicast/Multicast

Unicast refers to a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address.

Multicast is group communication where information is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

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): Range: 1-65535, Default: 260, 65535 indicates no aging.

Ignore Query Timer: Enable

Query Interval(s): Range: 1-18000

Response Time(s): Range: 1-25

Proxy Server: IP:

VLAN-based Multicast: All

Vid=1 Vid=2

Multicast-to-Unicast Conversion: OFF

Set parameters as required, and then click **Save**.

1.3.3.7.2 Hotspot2.0



Your AP might not support this function. The menu may vary with the device.

Hotspot 2.0 is a technical standard developed by Wi-Fi Alliance. It allows wireless STAs to complete automatic identity identification and seamless switching on a WLAN through IEEE 802.11u without using additional identities, providing wireless users with the access and roaming experience similar to that of cellular network users.

Template Management

Template management includes adding, editing, and deleting templates.

- Adding a template

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: *

Apply to SSID: ▾ ⓘ [WiFi/WLAN Settings]

» Advanced Settings

1. Click + to add a template editing page.

2. Enter the template name, select the Wi-Fi network, to which the template is to be applied, complete advanced settings (optional), and click **Save** to add a template.

Configuration items in **Advanced Settings** include **OSU Provider**, **Protocol**, **Carrier**, **Cellular**, and **Other (Venue)**.

OSU Provider

OSU SSID: ▾ ⓘ

OSU Service Provider: ▾ [Manage OSU Service Provider]

Protocol

Protocol: ▾ ⓘ

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:

English Name:

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

Domain Name: ×

Cellular

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

Domain Member: Auth Type: Auth Method: Auth Param: +Add

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

MCC: MNC: +Add

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

Organization Identifier: in-beacon +Add

HESSID:

Other

Venue: The Hotspot2.0 scenario

Type:
 Chinese Name:
 English Name:

● Editing a template

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: *

Apply to SSID: [WiFi/WLAN Settings]

» Advanced Settings

Select an existing template to go to the editing page of the template. Configuration fields are the same as those for adding a template.

 The template name cannot be modified.

- Deleting a template

Template-1
Template-2
+
▼

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:

Apply to SSID: ? [WiFi/WLAN Settings]

»» Advanced Settings

Save
Delete

Click the tab of the template to be deleted and click **Delete** to delete the template.

Choose **Advanced Settings > Parameter Settings**.

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: *

Apply to SSID: ? [WiFi/WLAN Settings]

»» Advanced Settings

OSU Provider

OSU SSID: ?

OSU Service Provider: ? [Manage OSU Service Provider]

Click **Manage OSU Service Provider** to manage OSU service providers.

- Querying an OSU service provider

OSU Service Provider ×

+ Add Provider
 × Delete Provider
 + Manage Provider Icon

Provider Name:
Search
Reset

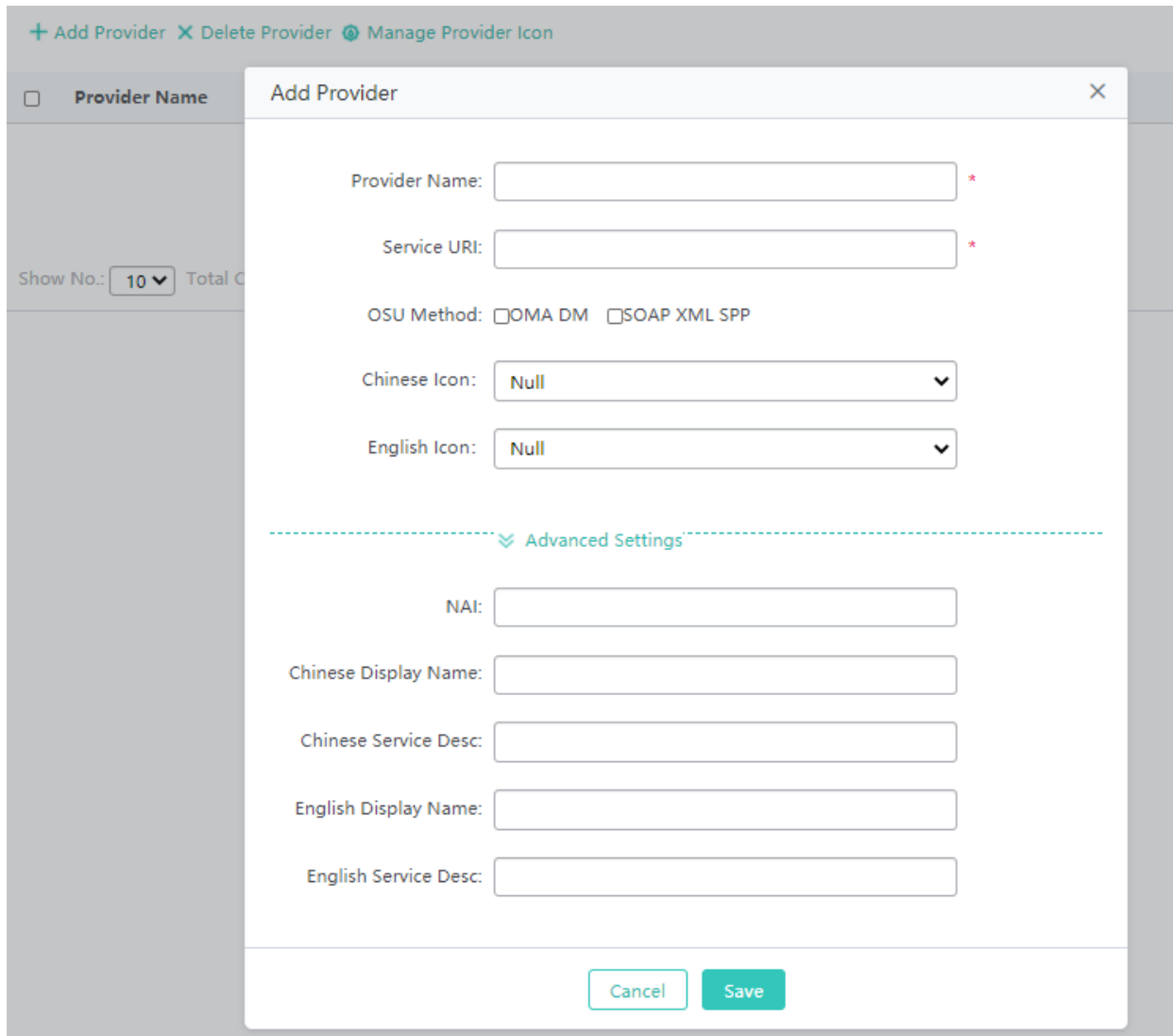
<input type="checkbox"/>	Provider Name	Action
No Data Found		

Show No.: Total Count:0

⏪ First
< Pre
Next >
Last ⏩
1
GO

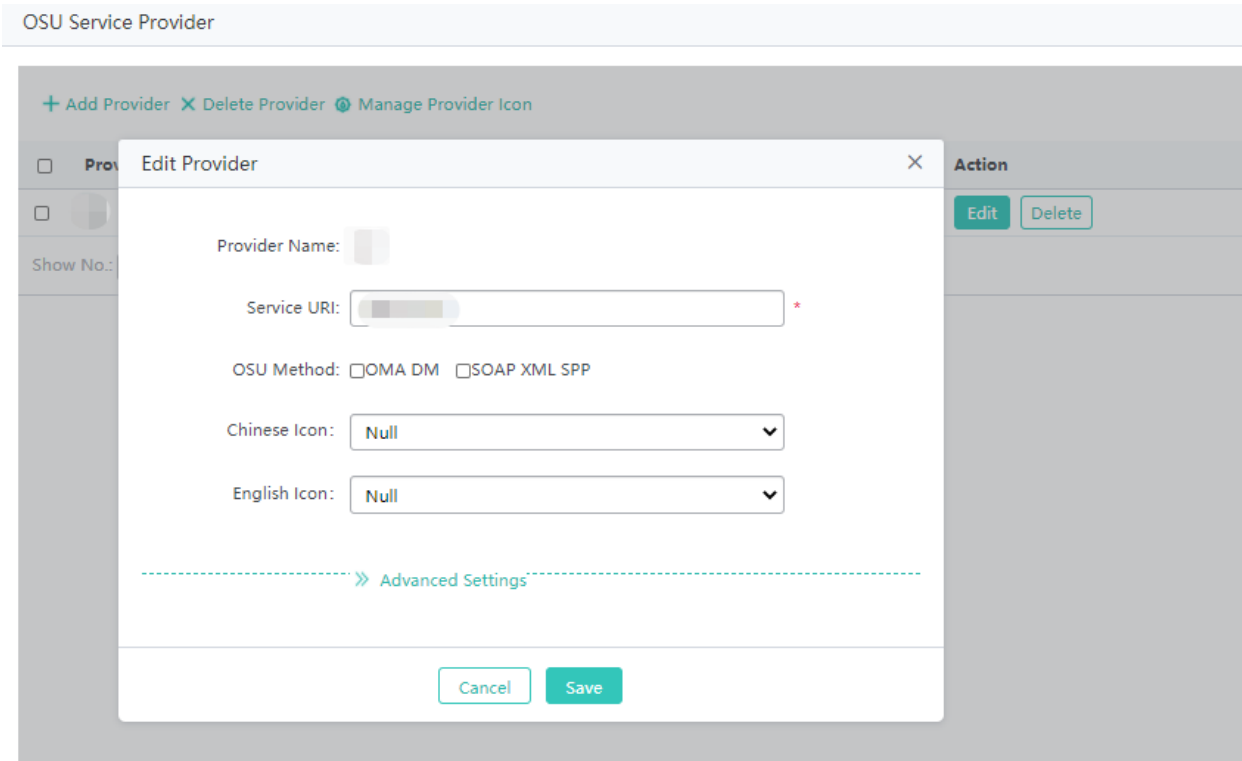
The page displays OSU service providers. You can enter a provider name to search for an OSU service provider. Fuzzy search is supported.

- Adding a provider



1. Click **Add Provider**. The **Add Provider** dialog box is displayed.
2. Enter the provider name, service URL, and other fields, complete advanced settings (optional), and click **Save** to add a provider.

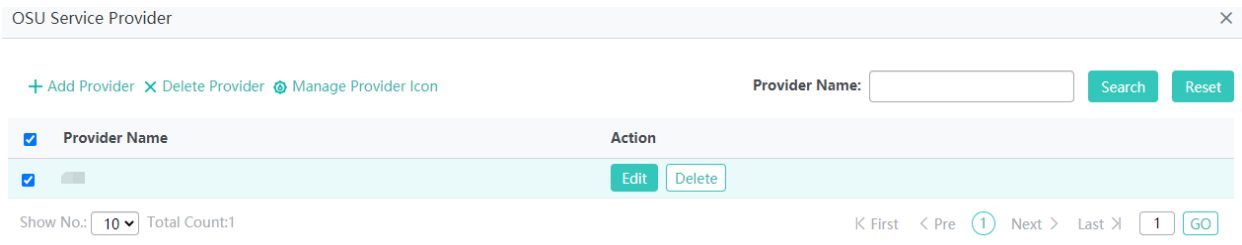
- Editing a provider



1. Click **Edit**. The **Edit Provider** dialog box is displayed.
2. Modify relevant fields and click **Save**.

The provider name cannot be modified. Configuration fields are the same as those for adding a service provider.

- Bulk Deleting Service Providers



Select providers to be deleted in the list and click **Delete Provider** to bulk delete the providers.

- Deleting a Service Provider

OSU Service Provider ✕

[+ Add Provider](#) [✕ Delete Provider](#) [🔗 Manage Provider Icon](#) Provider Name: [Search](#) [Reset](#)

<input type="checkbox"/>	Provider Name	Action
<input type="checkbox"/>	█	Edit Delete

Show No.: Total Count:1 K First < Pre 1 Next > Last X [GO](#)

Click **Delete** to delete a specified service provider.

📄 Provider Icon Management

OSU Service Provider ✕

[+ Add Provider](#) [✕ Delete Provider](#) [🔗 Manage Provider Icon](#) Provider Name: [Search](#) [Reset](#)

<input type="checkbox"/>	Provider Name	Action
<input type="checkbox"/>	█	Edit Delete

Show No.: Total Count:1 K First < Pre 1 Next > Last X [GO](#)

Click **Manage Provider Icon** to manage icons.

- **Uploading an Icon**

Provider Icon ✕

[✕ Batch Delete](#) Please select icon file (<64KB) [Browse](#) [Upload Icon](#)

<input type="checkbox"/>	Icon Name	Icon Size	Provider	Action
No Data Found				

Show No.: Total Count:0 K First < Pre Next > Last X [GO](#)

Click the input box or click **Browse** to show the icon file selection dialog box. Select an icon file and click **Upload Icon** to upload the icon file.

- **Bulk Deleting Icons**

Provider Icon ✕

[✕ Batch Delete](#) Please select icon file (<64KB) [Browse](#) [Upload Icon](#)

<input type="checkbox"/>	Icon Name	Icon Size	Provider	Action
No Data Found				

Show No.: Total Count:0 K First < Pre Next > Last X [GO](#)

Select icons to be deleted in the list and click **Batch Delete** to bulk delete the icons.

1.3.3.7.3 Antenna

The antenna is divided into internal and external, and can generate directional or omnidirectional radiation patterns. Whether antenna type switchover and orientation switchover are supported depends on the radio capacity, which is displayed on the page.

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. [Click to view diagram.](#)

Radio: dot11radio 1/0

Antenna Type: Internal External This radio does not support switching the type.

Orientation: Omni-directional Directional This radio does not support switching the orientation.

1.3.3.7.4 Radius

➤ RADIUS Server

The Remote Authentication Dial-In User Service (RADIUS) server conducts identity authentication and accounting on access users to protect the network security and facilitate management for network administrators.

Choose **Config > Advanced > Radius** to go to the RADIUS server configuration page.

Radius Server Radsec Server

Server Group: All Servers + Add Server X Delete Selected

<input type="checkbox"/>	Server IP	Authentication Port	Accounting Port	Radsec Server	Action
No Data Found					

Show No.: 10 Total Count:0

K First < Pre Next > Last X 1 GO

● Adding a server

Server Group: All Servers + Add Server

<input type="checkbox"/>	Server IP	Authentication	Accounting	Radsec Server	Action
No Data Found					

Show No.: 10 Total Count:0

K First < Pre Next > Last X 1 GO

Server IP: *

Authentication Port: 1812 *

Accounting Port: 1813 *

Shared Password: *

Radsec Server: Null

1. Click **Add Server** to add a RADIUS server.
2. Set fields and click **Save**. The message "Save Succeeded" is displayed.

Server IP

Indicates the IP address of the RADIUS server host.

Authentication Port

Indicates the UDP port ID for RADIUS authentication. The value range is from 0 to 65535 and **0** indicates that the host does not perform identity authentication.

Accounting Port

Indicates the UDP port ID for RADIUS accounting. The value range is from 0 to 65535 and **0** indicates that the host does not perform accounting.

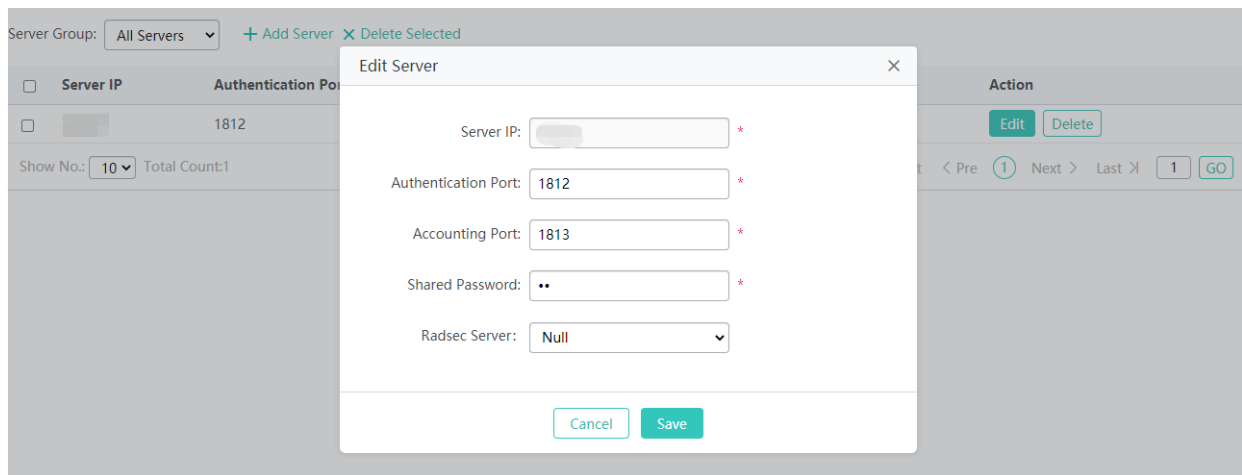
Shared Password

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. This field is not displayed if the device does not support the RadSec function.

- Editing a server



1. Click **Edit** to edit the RADIUS server.
2. After editing fields, click **Save**. The message "Save Succeeded" is displayed.

Fields for editing a RADIUS server are the same as those for adding a RADIUS server.

- Bulk deleting servers

Server Group: All Servers + Add Server ✕ Delete Selected

<input checked="" type="checkbox"/>	Server IP	Authentication Port	Accounting Port	Radsec Server	Action
<input checked="" type="checkbox"/>	[REDACTED]	1812	1813	--	Edit Delete

Show No.: 10 Total Count:1 ⏪ First < Pre 1 Next > Last ⏩ 1 GO

Select servers to be deleted in the list and click **Delete Selected** to bulk delete the servers.

● Deleting a Server

Server Group: All Servers + Add Server ✕ Delete Selected

<input type="checkbox"/>	Server IP	Authentication Port	Accounting Port	Radsec Server	Action
<input type="checkbox"/>	[REDACTED]	1812	1813	--	Edit Delete

Show No.: 10 Total Count:1 ⏪ First < Pre 1 Next > Last ⏩ 1 GO

Click **Delete** to delete a single server.

● Adding a Server Group

Radius Server Radsec Server

Server Group: All Servers + Add Server ✕ Delete Selected

<input type="checkbox"/>	Server IP	Authentication Port	Accounting Port	Radsec Server	Action
<input type="checkbox"/>	2.2.2.2	1812	1813	--	Edit Delete

Show No.: 10 Total Count:1 ⏪ First < Pre 1 Next > Last ⏩ 1 GO

Click the **Server Group** drop-down list and select **Add Server Group**. The **Add Server Group** dialog box is displayed.

Add Server Group✕

Server Group: *

Server Type: New Server Existing Server

Server IP: *

Authentication Port: *

Accounting Port: *

Shared Password: *

Radsec Server: ▼

1. Set server and server group fields.
2. After editing fields, click **Save**. The message "Save Succeeded" is displayed.

Server Group

Indicates the name of a server group.

Server Type

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.

- Deleting a Server Group

Server Group: ▼

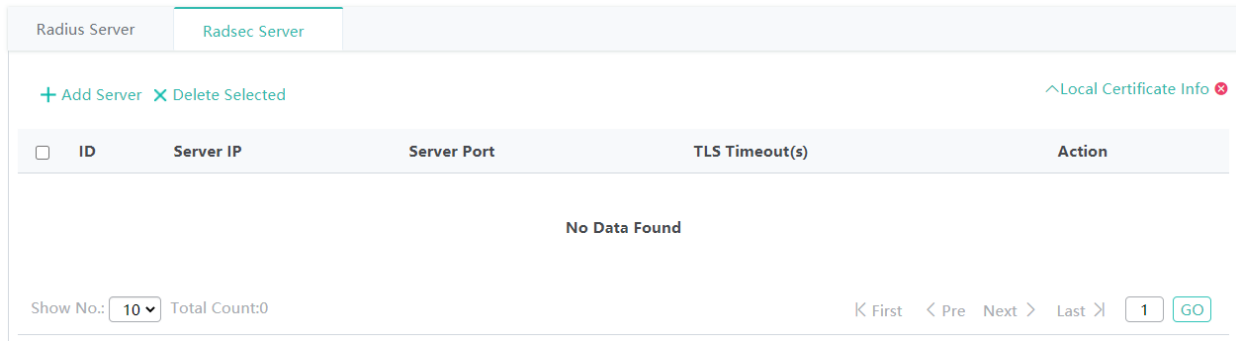
<input type="checkbox"/>	Server IP	Authentication Port	Accounting Port	Radsec Server	Action
<input type="checkbox"/>	---	1812	1813	--	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.: ▼ Total Count:1 < First < Pre (1) Next > Last >

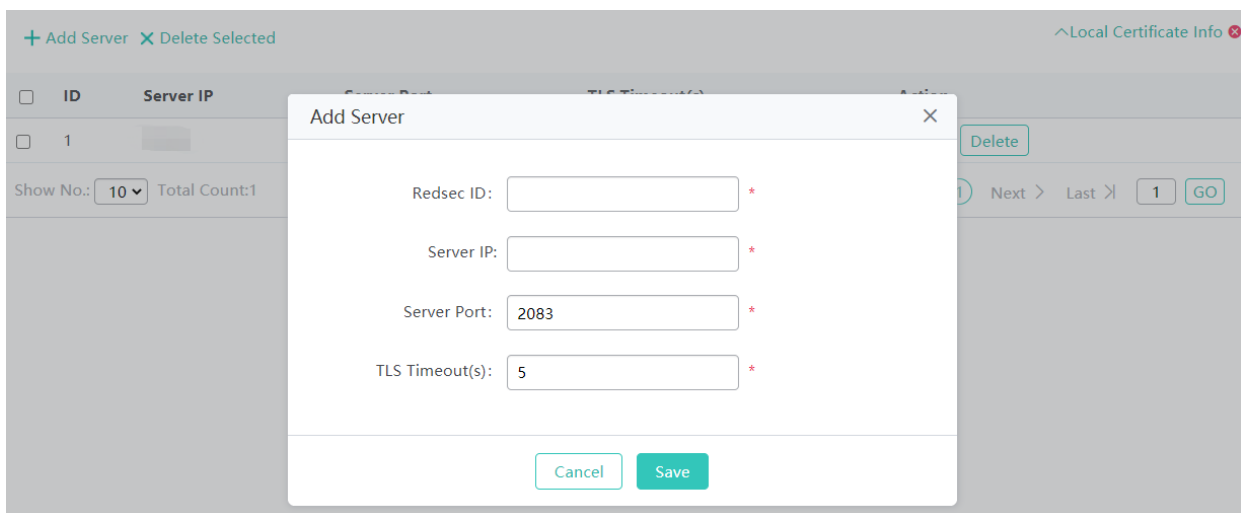
Select a server group and click **Delete Server Group** to delete the server group.

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.



● Adding a server



1. Click **Add Server** to add a RadSec server.
2. After editing fields, click **Save**. The message "Save Succeeded" is displayed.

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

Indicates the port ID of the RadSec server. The value range is from 1 to 65535 and the default value is **2083**.

TLS Timeout(s)

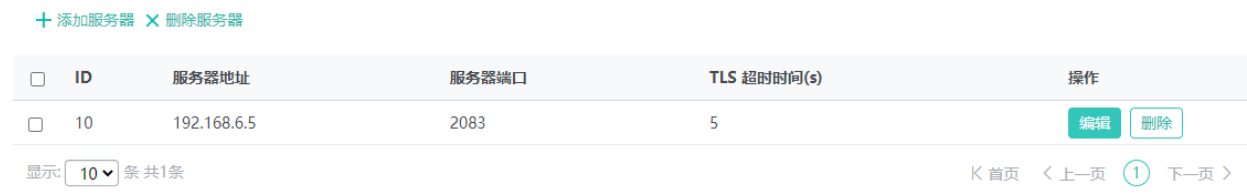
Indicates the TLS connection timeout time. The value range is 1 to 1000 and the default value is 5.

- Editing a server

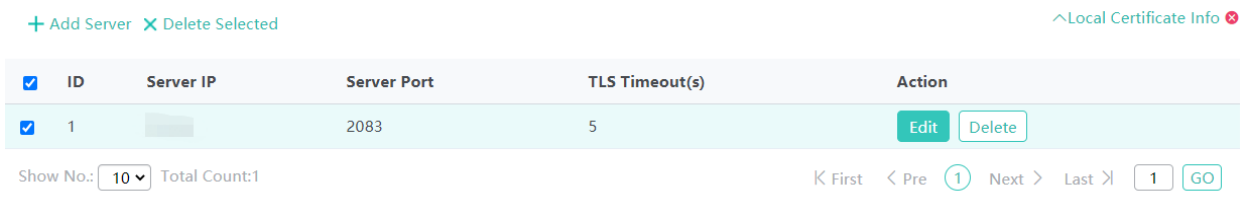


1. Click **Edit** to edit a RadSec server.
2. After editing fields, click **Save**. The message "Save Succeeded" is displayed.

- Bulk deleting servers



Select servers to be deleted in the list and click **Delete Selected** to bulk delete the servers.



Click **Delete** to delete a single server.

+ Add Server X Delete Selected ^Local Certificate Info X

ID	Server IP	Server Port	TLS Timeout(s)	Action
1		2083	5	Edit Delete

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

Local Certificate Management

+ Add Server X Delete Selected vLocal Certificate Info X

ID	Server IP	Server Port	TL
1		2083	5

Show No.: 10 Total Count:1

Certificate: X Private Key: X CA: X X

Format: PEM PFX

Certificate:

Private Key:

Password:

[Upload & Load](#)

CA:

[Upload & Load](#)

1. Click **Local Certificate Info**. The local certificate management window is displayed. The icon on the right of **Certificate** shows the certificate loading status.
2. Select a certificate file and private key file, enter the certificate password (if any), and 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**.

1.3.4 Diagnosis

1.3.4.1 Network Diagnosis

1.3.4.1.1 Network Diagnosis

Connectivity Test

When the network malfunctions, you can test the network connectivity to facilitate troubleshooting.

The screenshot shows a web interface for connectivity testing. At the top, there are three tabs: 'Connectivity Test' (selected), 'Ping', and 'Tracert'. Below the tabs, there are three status indicators, each with a green checkmark: 'Port Status', 'AC-AP Connection Status', and 'Internet Connection Status'. A green button labeled 'Test Again' is positioned below these indicators.

Port Status

The system detects whether an interface of the AC is in the up state.

AC-AP Connection Status

The system detects whether an AP is online on the AC.

Internet Connection Status

The system detects whether the AC is reachable to an external network by pinging 114.114.114.114, or pinging 8.8.8.8 if the AC is deployed abroad.

⏏ **Ping**

The screenshot shows the 'Ping' configuration page. It has three tabs: 'Connectivity Test', 'Ping' (selected), and 'Tracert'. The configuration fields are: 'Ping Type' (dropdown menu set to 'Not via Management Port'), 'Dest IP/Domain Name' (text input field with a red asterisk), 'Timeout Interval(s)' (text input field set to '2', range '1-10'), 'Repeat Times' (text input field set to '5', range '1-100'), 'Packet Size(Bytes)' (text input field set to '100', range '36-18024'), and 'Fragment' (checkbox checked, labeled 'Enable'). A green 'Test' button is at the bottom.

Ping Type

Sets the out-of-band channel. It is supported only on MGMT-supported devices. When a MGMT interface is configured as a source interface, **Ping Type** must be set to **via Management Port**, or otherwise, set to **Not via Management Port**.

Dest IP/Domain Name

Indicates the address or domain name to be pinged.

Timeout Interval(s)

Indicates the timeout interval.

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 DF flag bit is **0** by default.

↘ **Tracert**

Connectivity Test	Ping	Tracert
-------------------	------	---------

Tracert Type:

Dest IP/Domain Name: *

Timeout Interval(s):

Tracert Type

Sets the out-of-band channel. It is supported only on MGMT-supported devices. When a MGMT interface is configured as a source interface, **Tracert Type** must be set to **via Management Port**, or otherwise, set to **Not via Management Port**.

Dest IP/Domain Name

Indicates the Tracert destination address or domain name address.

Timeout Interval(s)

Indicates the timeout interval.

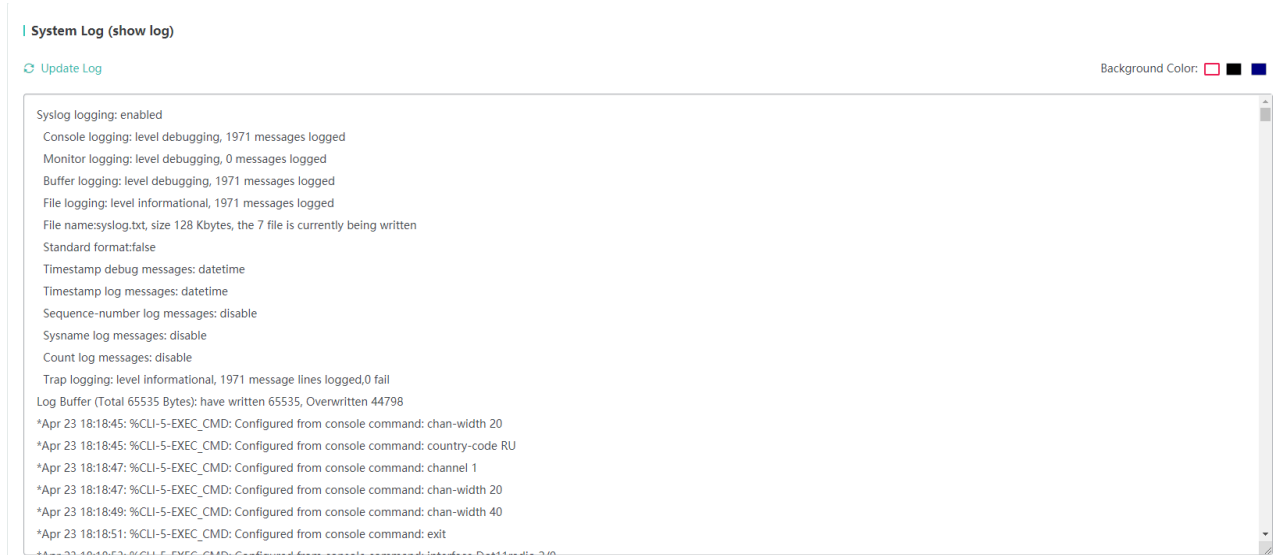
1.3.4.2 One-Click Collection

Note: One-Click Collection is used to collect fault information for troubleshooting.

1.3.4.3 Syslog

1.3.4.3.1 Syslog

Syslog helps technical support to locate problems.



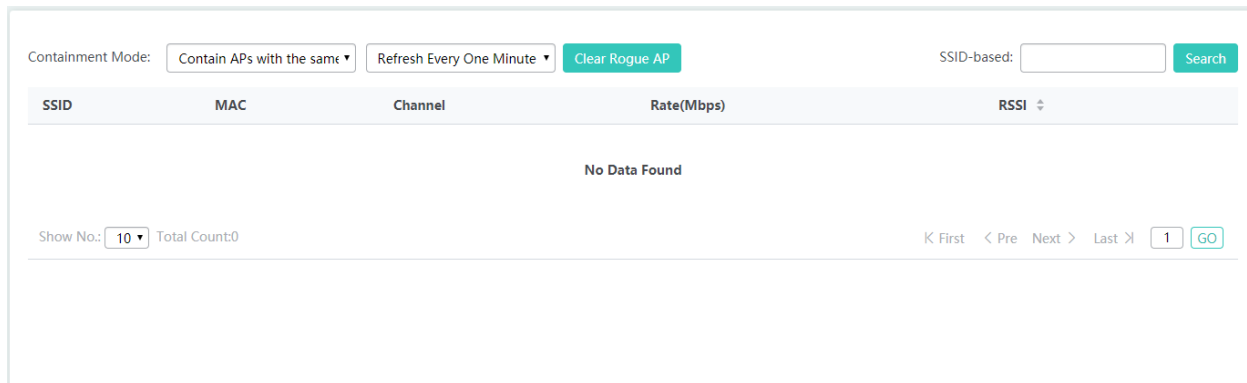
1.3.4.4 WIDS

1.3.4.4.1 Rogue AP

Rogue APs pose threat to the network security.

The following containment modes are available.

SSID mode: Contain APs emitting the same WiFi signals as the local AP.



AdHoc mode: Contain AdHoc devices simulating the same WiFi signals.

Containment Mode: Contain APs with signals s Refresh Every One Minute Clear Rogue AP SSID-based: Search

SSID	MAC	Channel	Rate(Mbps)	RSSI
No Data Found				

Show No.: 10 Total Count:0 First Pre Next Last 1 GO

Rogue mode: Contain APs according to RSSI.

Containment Mode: Contain APs with RSSI high Refresh Every One Minute Clear Rogue AP SSID-based: Search

SSID	MAC	Channel	Rate(Mbps)	RSSI
No Data Found				

Show No.: 10 Total Count:0 First Pre Next Last 1 GO

CONFIG mode: Contain APs by configuring the MAC address and the SSID blacklist manually.

Containment Mode: Contain APs added manually Refresh Every One Minute Clear Rogue AP SSID-based: Search

SSID	MAC	Channel	Rate(Mbps)	RSSI
No Data Found				

Show No.: 10 Total Count:0 First Pre Next Last 1 GO

1.3.5 Maintenance

1.3.5.1 Settings

1.3.5.1.1 Local Upgrade

Download the main program or Web package to the local device and perform local upgrade.

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 Version

Download Firmware: [Check for Later Version & Download](#) ⓘ

File Name:

Browse

Upgrade

Cancel

Click to select the main program or Web package to be upgraded.

You can click **Cancel** to terminate an ongoing upgrade.

Click the **DNS Server** and **Route** links to check network connection.

1.3.5.1.2 Restart

Conveniently restart the system with a click.

Note: Click 'Restart' to restart the device. Please wait a few minutes and the page will be refreshed after restart.

Restart

Click **Restart** to restart the device.

1.3.5.1.3 Backup & Restore

Backup

Back up the configuration file on the device. You can export current settings for batch operation.

Backup Restore

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: [Browse](#) [Import](#) [Export Current Settings](#) [Export black-white-list-config](#)

Restore

After you restore the device to factory settings, please use the default IP address to access Eweb.

Backup Restore

Note: After the device is reset to the factory default settings, all settings will be cleared. Please [Export Current Settings](#) before resetting the device.

[Restore Factory Settings](#)

[Display Current Settings](#)

1.3.5.1.4 System Time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of *year-month-day, hour:minute:second*, day of the week.

When you use a network device for the first time, set its system clock to the current date and time manually.

Set the system time based on the region for the device.

Current Time: **1970-1-1-03:34:18**

Reset Time:

Time Zone:

Time Synchronization: Automatically synchronize with an Internet time server **(Please set DNS Server first, otherwise the system time will not be synchronized.)**

[Save](#)

1.3.5.1.5 System Mode

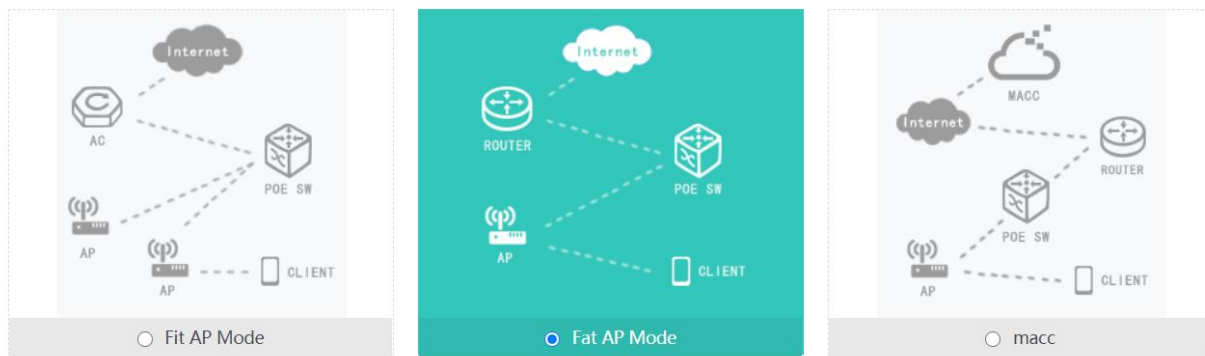
Two types of APs are available: Fat Access Points and Fit Access Points.

A FAT AP is suitable for family and small-scaled networks and provides full features. Generally, one device can implement access, authentication, routing, VPN, address translation, and even the firewall functions.

A FIT AP is suitable for large-scale wireless network deployment. A dedicated wireless controller is needed to provide unified management. A FIT-AP can be used only after the wireless controller delivers configurations and it cannot complete configuration by itself.

Select the AP mode.

Current Mode: Fat AP Mode



Note: The device restarts after mode switch. Please wait for a minute.

1.3.5.1.6 Log Server

The device sends local logs to the server for storage. History logs are stored for ease of query.

Server Logging can be set to ON/OFF to enable/disable the server log function.

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:

1.3.5.1.7 Device DNS

Domain names can be dynamically parsed only after a DNS server is configured.

DNS Server 1: +

DNS Server 2: ×

Save

1.3.5.2 System

1.3.5.2.1 Web Management

Admin Password

To enhance the system security and information interaction security, you need to change the default password of the system.

On the **Admin Password** tab page, enter the old password, new password, and confirm password, and click **Save**.

Admin Password	Basic Settings	Permissions	Web Log	
-----------------------	----------------	-------------	---------	--

Username: admin

Old Password: *

New Password: *

Confirm Password: *

Save

Basic Settings

Configure the device location to better inspect devices and facilitate device management. Set the timeout time. When you do not perform operations on the system for long, the Web-based system automatically exits to ensure your system security.

Web Access Port: Indicates the access port. It needs to be added when you access the Web-based system from a browser.

Login Timeout: Indicates the timeout time.

Device Location: Indicates the device location. Setting this parameter facilitates management.

Admin Password **Basic Settings** Permissions Web Log

Web Access Port: * (Range: 80,1025-65535)

Login Timeout: ▼

Device Location:

Access Redirection: HTTP Redirection to HTTPS *In NAT scenario, redirection may cause HTTP access failure.*

Permissions

A system may have multiple users of different levels that correspond to different permissions. You can set or view permissions through the **Permission Settings** page. The system has two default users: user **admin**

Admin Password Basic Settings **Permissions** Web Log

+ Add Admin

Username	Action
No Data Found	

Show No.: Total Count:0

First < Pre Next > Last >

● Adding an administrator

+ Add Admin

Username	Action
No Data Found	

Show No.: Total Count:0

Next > Last >

Add Admin [X]

Username: *

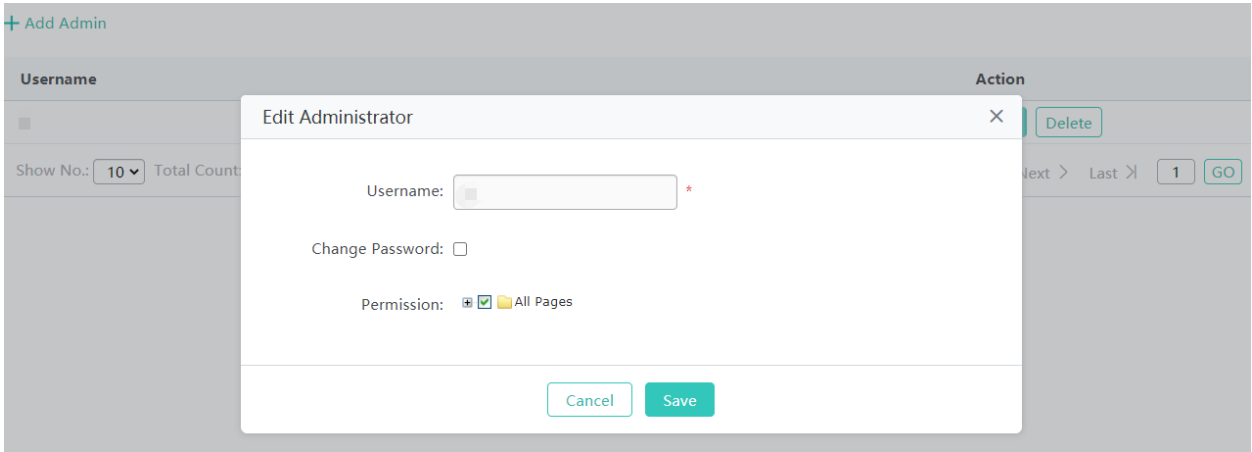
New Password: *

Confirm Password: *

Permission: All Pages

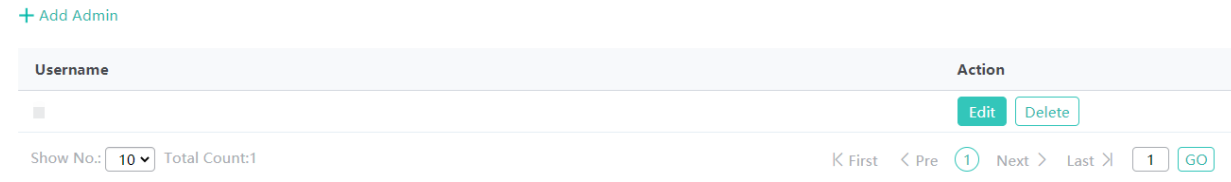
Click **Add Administrator**. A dialog box is displayed, as shown in the preceding figure. Set the configuration items in the dialog box, and click **Save**. The newly added administrator is displayed in the list after the **Save succeeded** message is displayed.

- Editing administrator information



- 1) Click the **Edit** button for an administrator in the list.
- 2) A dialog box is displayed, as shown in the preceding figure. The configuration about the administrator is displayed in the dialog box. Then edit the configuration.
- 3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting an administrator



Click **Delete** to delete an administrator.

Web Log

This function allows you to customize the website icon to be displayed on the browser tab, logo image to be displayed at the top left corner of the menu page, and the background of the Web login page.

Admin Password Basic Settings Permissions Web Log

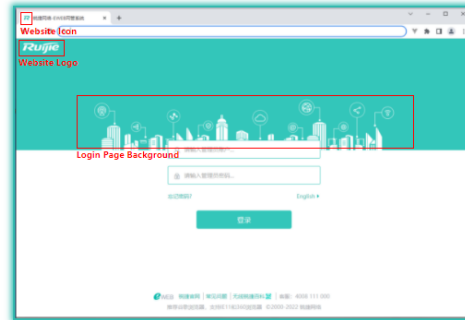
Note: Note: You can customize the background of the web login interface, the logo image at the top left corner of the menu interface, and the website icon in the browser tab.
Note: Caution: Please upload images according to the size requirements and image commands specified in the upload box. The image size should not exceed 150KB. The uploaded image takes effect after the device is restarted.

Upload Website Icon: favicon.ico Size (L x W): 16px*16px

Upload Logo: complyLogo.png Size (L x W): 100px

Upload Login Page Background: lg-pic.gif Size (L x W): 800px*132px

Image Example



1. Import the website icon.
2. Import the logo.
3. Import the background image used for the login page.

1.3.5.2.2 Telnet & SSH

Enable Telnet and SSH access for security purposes.

Note: The password will also be applied to the Console

Telnet Service: ON

SSH Service: OFF

New Password: *

Confirm Password: *

1.3.5.2.3 Web Console

The Web console function is similar to the Telnet function and you can configure any command on the console. However, the Web console function does not support commands in shell mode, telnetting to APs, or batch refresh of commands.

Console Output: Background Color:

Ruijie#

Command Input:

1.3.5.2.4 SNMP

The Simple Network Management Protocol (SNMP) is by far the dominant protocol in network management. This Protocol (SNMP) was designed to be an easily implementable, basic network management tool that could be used to meet network management needs. It is named Simple Network Management Protocol as it is really easy to understand. A key reason for its widespread acceptance, besides being the chief Internet standard for network management, is its relative simplicity. There are different versions of SNMP, such as SNMP V1, SNMP V2c, and SNMP V3.

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.

1.3.5.2.5 CWMP/MACC

The CPE WAN Management Protocol (CWMP) is used by a server to manage, configure, and monitor ACs, APs, routers, or switches.

The CWMP enables a device to interconnect to the cloud platform or other servers for management.

 Your AC may not support this function and the actual menu items shall prevail. When a device is interconnected to a server over CWMP, a correct DNS server needs to be configured so that the device correctly parses the domain name of the server. Therefore, check whether a correct DNS server is configured.

Click **DNS server** behind **Note** to redirect to the related configuration page.
Set parameters and click **Save**.

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:

Server URL: *

Server Username:

Server Password:

Device URL:

Device Username:

Device Password:

CPE Inform Interval(s): Range: 30-3600

CWMP

Indicates whether to enable CWMP.

Server URL

Indicates the server address.

Server Username

Indicates the server username, which can be used for verification.

Server Password

Indicates the server password, which can be used for verification.

Device URL

Indicates the device URL, which can be used for active connection within the server LAN.

Device Username

Indicates the device username, which can be used for verification.

Device Password

Indicates the device password, which can be used for verification.

CPE Inform Interval(s)

Indicates the interval for connecting to the server, that is, heartbeat packet interval. Other Functions

1.3.6 Others

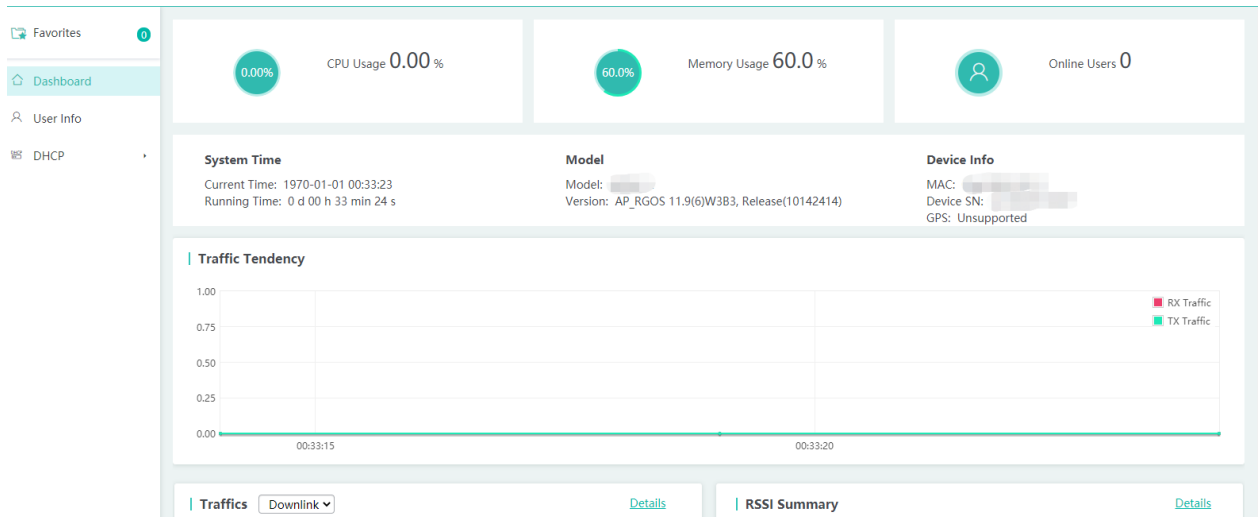
1.3.6.1 Favorites

After you add frequently configured functions to favorites, you can click menu items in the favorites and configure the functions rapidly next time.

 Currently, a maximum of ten menu items can be added to favorites.

- Adding to favorites

Select a required menu and drag it to **Favorites**.



- Canceling favorites

Click **Favorites** to display the favorites list. Select a menu item from the list and click the **X** icon. Confirm the delete operation to delete the menu item from the favorites.



1.3.6.2 Fast Query Menu

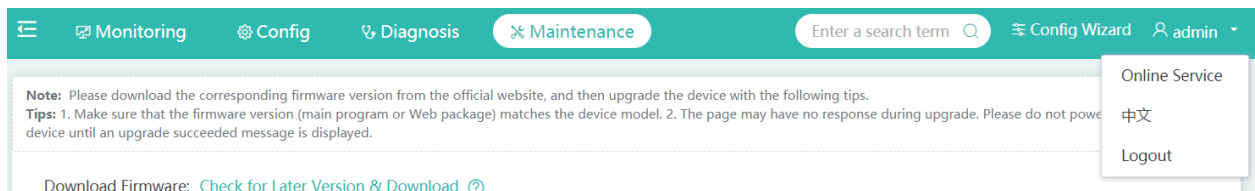
There are increasing functions in the system. The fast query menu helps users rapidly search for required functions. Enter a search condition in the search box on the home page. A list of records meeting the search condition is rapidly displayed. Click a function to redirect to the function page.



1.3.6.3 More Functions

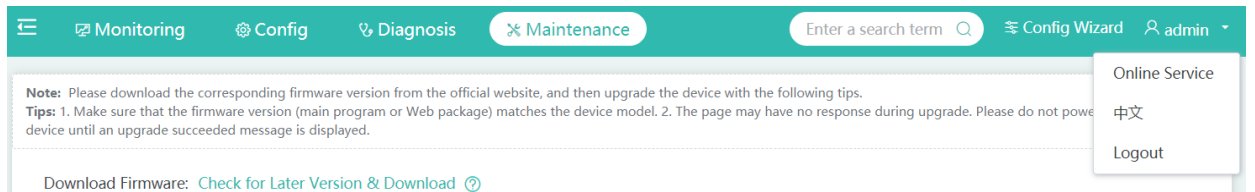
- Displaying the current account

The current account is displayed in the upper right corner of the home page. The current account is **admin**, as shown in the figure below.



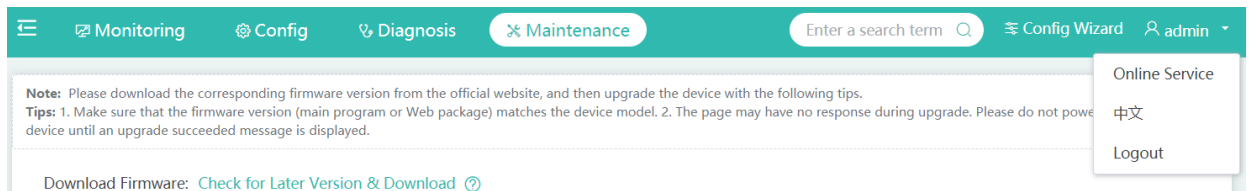
- Online Service

Click the current account icon in the upper right corner. A function drop-down list is displayed. Click **Online Service** when you need to seek help.



- Language switching

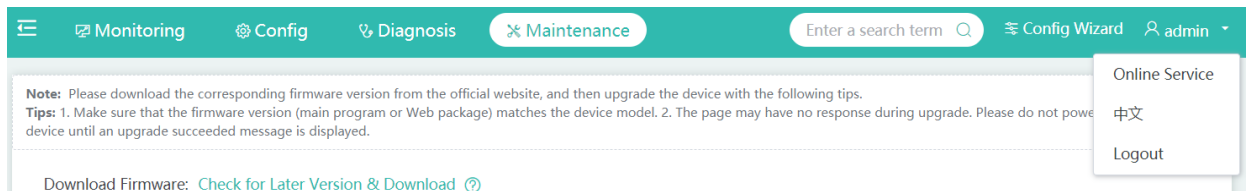
Click the current account icon in the upper right corner. A function drop-down list is displayed. The second item is used for language switching. If the system is in Chinese, click **English** to switch to the English edition; if the system is in English, click **中文** to switch to the Chinese edition.



The language switching item is displayed based on actual requirements. If only Chinese is supported, this item is not displayed. It is displayed only when both Chinese and English are supported.

- Exiting the system

Click the current account icon in the upper right corner. A function drop-down list is displayed. Click **Logout** and click **OK** to exit the system.



1.4 Fit AP-Eweb

1.4.1 SmartAP

SmartAP allows you to deploy APs in mobile office scenario. Click **Config Wizard** to end the SmartAP configuration page, including **System Mode**, **Network Configuration** and **Change Web NMS Password**. If APs are not applied to mobile office scenario, only system mode will be displayed.

1. System Mode

Click **Change** and the **System Mode** window is displayed. You can select a mode among three modes available: Fit AP, Fat AP and MACC.



Note: The device restarts after mode switch. Please wait for a minute.

2. Network Configuration

IP Allocation Type:

SSID:

Hide: Enable

Active AC IP:

Standby AC IP:

L2TP Tunnel: ON

HQ IP: * (Peer ip address for l2tp tunnel)

Access AC Through Yes No

Tunnel:

»» Advanced Settings

3. Change Web NMS Password

Old Password: *

New Password: *

Confirm Password: *

1.5 Enabling the Web Server

The Web service is enabled for an AP device when this AP is delivered. By default, the IP address is 192.168.110.1. The following describes how to enable Web service on the CLI when it is disabled.

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

Configuration Method

▾ Enabling the Web Service

- Mandatory configuration.
- This configuration is performed on the AP device.

▾ Configuring the IP Address

- Optional configuration.

▾ Configuring the Username and Password for Logging in to the Web-Based Management System

- Optional configuration.
- When the Web service is enabled, the administrator username/passwords (admin/admin) and guest user/passwords (guest/guest) are created by default. The passwords of these two accounts can be changed. In addition, you can create other Web-based management accounts.

Verification

Log in to the Web page by using the preset IP address and Web-based management account and password, then check whether the login is successful.

Relevant Commands

▾ Enabling the Web Service

Command	<code>enable service web-server [http https all]</code>
---------	---

Parameter Description	http https all : Enables corresponding services. http enables the HTTP service, https enables the HTTPS service, and all enables both the HTTP and HTTPS services. By default, both the HTTP and HTTPS services are enabled.
Command Mode	Global configuration mode.

▾ **Configuring the IP Address**

Command	ip address <i>ip-address ip-mask</i>
Parameter Description	<i>ip-address</i> : IP address <i>ip-mask</i> : network mask.
Command Mode	Interface configuration mode.

▾ **Configuring the Account and Password for Logging in to the Web-Based Management System**

Command	webmaster level <i>privilege-level</i> username <i>name</i> password { <i>password</i> [0 7] <i>encrypted-password</i>
Parameter Description	<i>privilege-level</i> : indicates the level of the permission bound to the user. Three levels are available, which are 0, 1, and 2. The super administrator account (admin) created by default corresponds to level 0, a guest account (guest) corresponds to level 2, and other accounts correspond to level 1. <i>name</i> : address of the static RP. <i>password</i> : The ACL is used to limit the group address range of the static RP service. The default range is all group services. 0 7 : password encryption type. 0 indicates no encryption, and 7 indicates simple encryption. The default value is 0. <i>encrypted-password</i> : password.
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

▾ **Configuring the Web Server**

Configuration Steps	Enable the Web service. Configure the local username and password. Configure the device management IP address. The default management VLAN is VLAN 1. Configure an IP address for VLAN 1. Ensure that the management IP address can be pinged from the user's PC.
	<pre>Ruijie# configure terminal Ruijie(config)# enable service web-server Ruijie(config)# webmaster level 0 username admin password admin Ruijie(config)#interface vlan 1</pre>

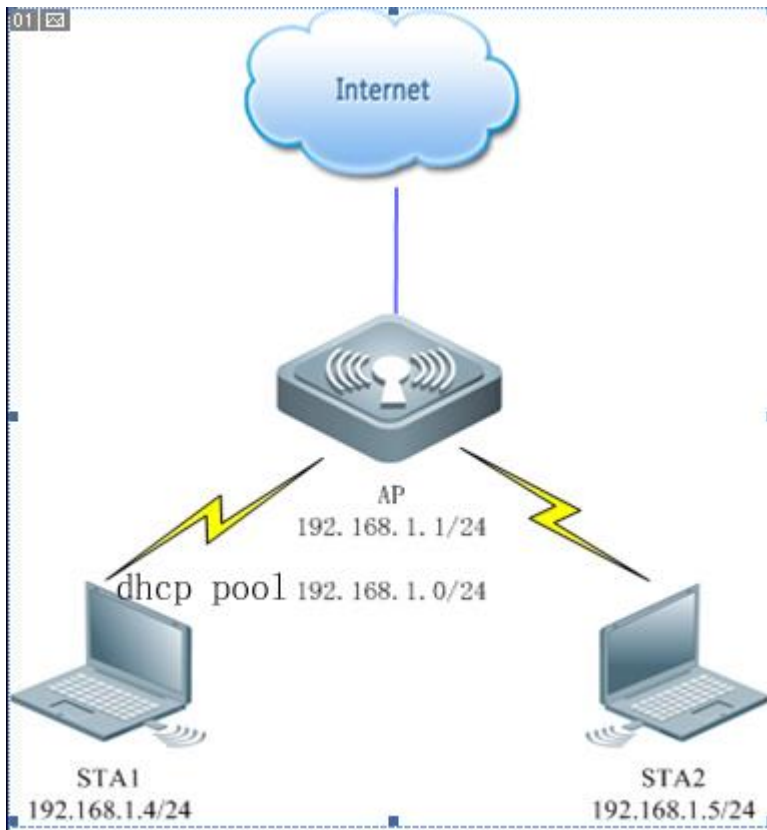
	<pre>Ruijie(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0 Ruijie(config)# end</pre>
Verification	Run the show running-config command to display related configuration commands.
	<pre>Ruijie(config)#show running-config Building configuration... Current configuration: 6312 bytes ! hostname ruijie ! ! webmaster level 0 username admin password 7 08022b181b29 webmaster level 1 username manager password 7 06073f webmaster level 2 username guest password 7 14155f083206 http update mode auto-detect ! ! interface VLAN 1 ip address 192.168.1.200 255.255.255.0 no shutdown ! line con 0 line vty 0 4 login ! ! End</pre>

1.6 Configuration Examples

1.6.1 Constructing a WLAN for the DHCP Server on the AP Device

The AP is regarded as a wireless router and constructs a small-scale network as a fat AP. The DHCP server is configured on the AP device. The following figure shows the topology.

Figure 1-3 Topology 1 (AP is in routing mode)



Configuration	Description and Command	
Construction of a WLAN for the DHCP server on the AP	i Mandatory. It is used to configure a WLAN.	
	WiFi name	Associates internet access wireless signals for an STA
	WiFi password	An STA inputs the password for internet access.
	DHCP configuration	Allocates IP addresses to wireless STAs.

Verification

- ↘ Select AP working mode and set the Internet connection type

Config Wizard—External Network Settings

Bridge Mode

DHCP in others devices

NAT Mode

DHCP in AP

Port: (If you want to change the port, please go to device configuration.)

IP Allocation Mode:

IP: *

IP Mask: *

Default Gateway: *

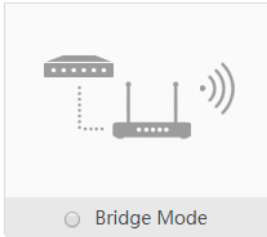
NAT: Check this box if you want to convert all internal addresses to external addresses.

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI. Aggregate port configuration is not supported.

Next

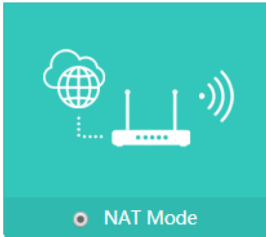
- The AP works in wireless routing mode.
- You can select the following Internet connection types when the AP works in wireless routing mode.
- Static IP (dedicated IP)

Config Wizard—External Network Settings



Bridge Mode

DHCP in others devices



NAT Mode

DHCP in AP

Port: (If you want to change the port, please go to device configuration.)

IP Allocation Mode:

IP: *

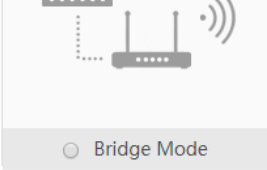
IP Mask: *

Default Gateway: *

NAT: Check this box if you want to convert all internal addresses to external addresses.

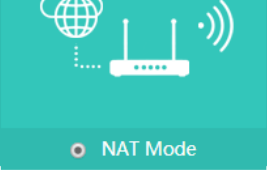
- PPPoE (ADSL line)

Config Wizard—External Network Settings



Bridge Mode

DHCP in others devices



NAT Mode

DHCP in AP

Port: (If you want to change the port, please go to device configuration.)

IP Allocation Mode:

Account: *

Password: *

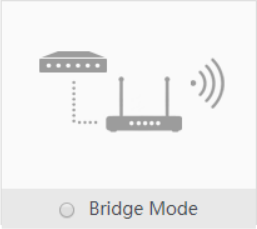
PPPOE IP: Not Obtained

NAT: Check this box if you want to convert all internal addresses to external addresses.

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI. Aggregate port configuration is not supported.


- DHCP (dynamic IP)

Config Wizard—External Network Settings



Bridge Mode

DHCP in others devices



NAT Mode

DHCP in AP

Port: (If you want to change the port, please go to device configuration.)

IP Allocation Mode:

Default Gateway: Optional

DHCP IP: Not Obtained

NAT: Check this box if you want to convert all internal addresses to external addresses.

Note: This function is designed for ease of use based on user scenario. It is recommended to configure the function via Web instead of CLI. Aggregate port configuration is not supported.

- **Configure a WiFi name (use a simple name that is easy to remember). A WiFi name contains up to 32 characters.**

Figure 1-4 AP Quick Settings for SSID

The screenshot shows a web-based configuration window titled "Config Wizard—WiFi". The window contains several configuration fields:

- SSID:** A text input field containing "@test_ssid" with a red asterisk to its right.
- WiFi Password:** A text input field with masked characters (dots) and a "Show Password" checkbox to its right.
- DHCP:** A checkbox labeled "Enable (IP addresses are allocated by AP)" which is checked.
- Vlan ID:** A text input field containing the number "2".
- IP Range:** Three text input fields: the first contains "192.168.1", the second contains "1", and the third contains "254", with the word "to" between the second and third.
- DHCP Gateway:** A text input field containing "192.168.1.1".
- Preferred DNS Server:** A text input field containing "192.168.58.110" with the word "Optional" to its right.
- Secondary DNS Server:** A text input field containing "8.8.8.8" with the word "Optional" to its right.

At the bottom of the window, there are two buttons: a teal "Finish" button and a white "Back" button with a teal border.

- **Security configuration**

By default, the WPA2-PSK mode is selected. A password consists of 8 to 64 characters and can be a combination of letters, digits, and special characters.

Figure 1-5 AP Quick Settings for Security

Config Wizard—WiFi ✕

SSID: *

WiFi Password: Show Password

DHCP: Enable (IP addresses are allocated by AP)

Vlan ID:

IP Range: to

DHCP Gateway:

Preferred DNS Server: Optional

Secondary DNS Server: Optional

DHCP configuration

Figure 1-6 AP Quick Settings for DHCP

The screenshot shows a 'Config Wizard—WiFi' window with the following fields and values:

- SSID: @test_ssid *
- WiFi Password: [masked] Show Password
- DHCP: Enable (IP addresses are allocated by AP)
- Vlan ID: 2
- IP Range: 192.168.1.1 to 254
- DHCP Gateway: 192.168.1.1
- Preferred DNS Server: 192.168.58.110 Optional
- Secondary DNS Server: 8.8.8.8 Optional

Buttons: Finish, Back

- IP address range: 192.168.1.0/24 to 192.168.1.254/24.
- DNS server: 192.168.58.110 (Perform configuration based on actual conditions.)
- Click **Finish**.

Verification

- Associate an STA with WiFi: Eweb_AAAA1 and obtain the IP address 192.168.1.4.
- Verify that the STA can connect to the WiFi and then visit the Web through 192.168.1.1.

i If the management IP address is changed, use the new management IP address to use the Web again.