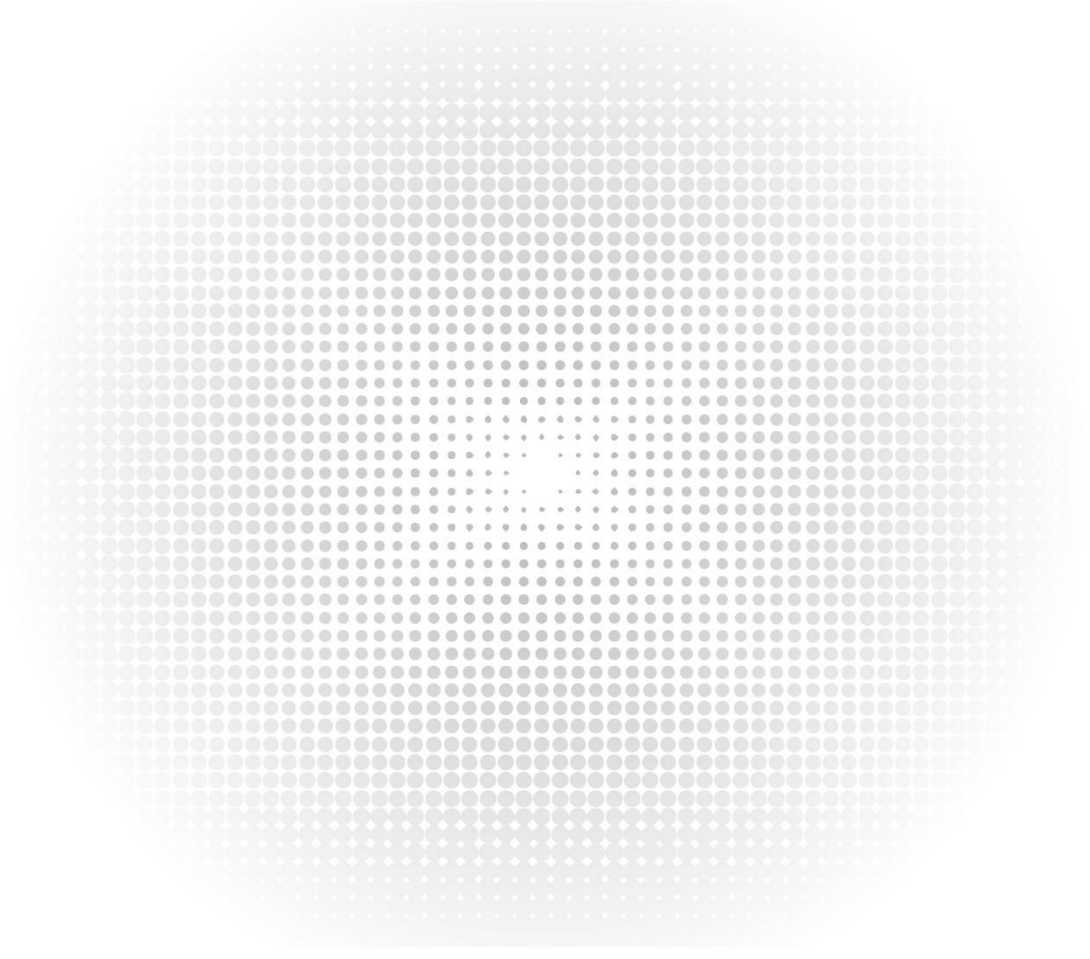
AP Series Web-based Configuration Guide

Models: AP-W6D1775C; AP-W6D2400C; AP-W6T3267C; AP-W6Q4134C; AP-W6T6817C; AP-W6T10000C
AP-N303; AP-N505; AP-T565; AP-T567



CONFIGURATION GUIDE

Contents

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

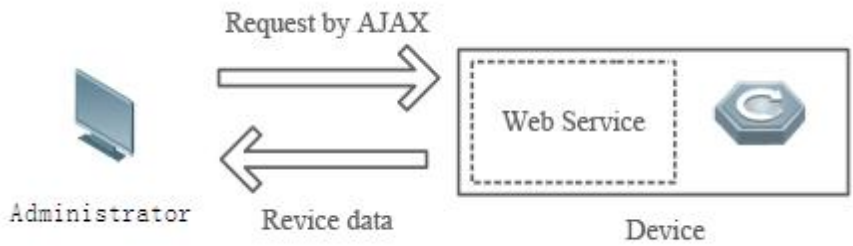
Application	Description
Web-based Management	After configuring, a user can access the Web-based management system through a browser.

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.
- Browsers supported: IE7.0, IE8.0, IE9.0, IE10.0, IE11.0, Google chrome, Firefox, and some IE kernel-based browsers (for example, Maxthon). 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	192.168.1.1

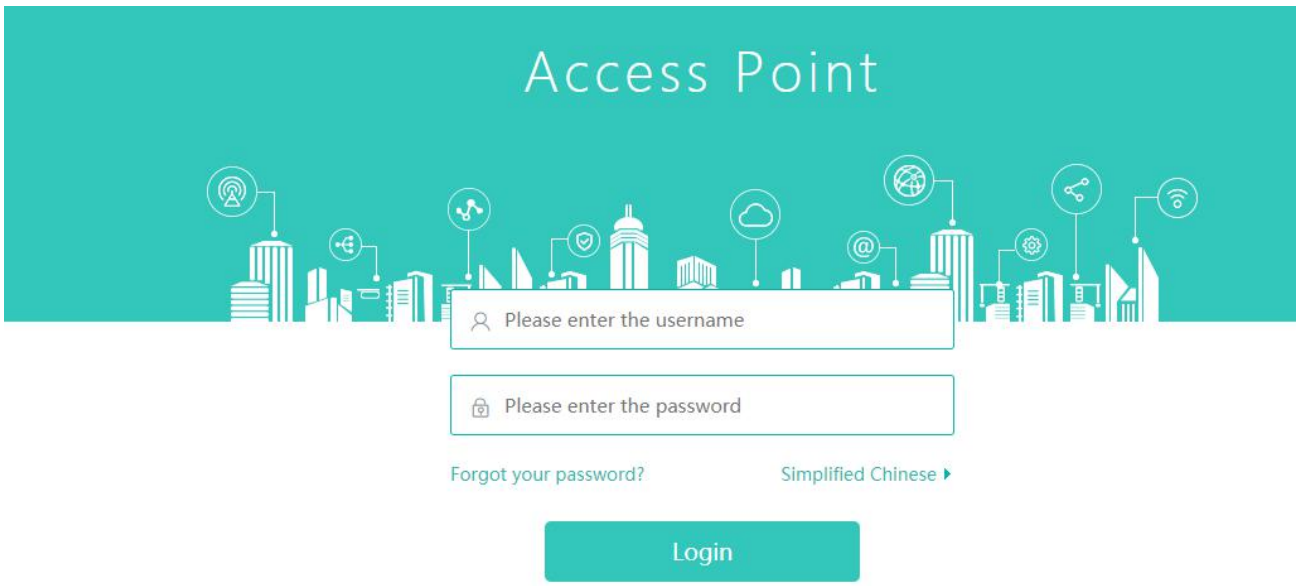
Default Username/Password	Permission Description
admin/admin	Super administrator with all permissions.

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

Login

Type **http://X.X.X.X** (management IP address), default: http://192.168.1.1, in the address bar of a browser and press **Enter** to access the login page, as shown in the following figure.

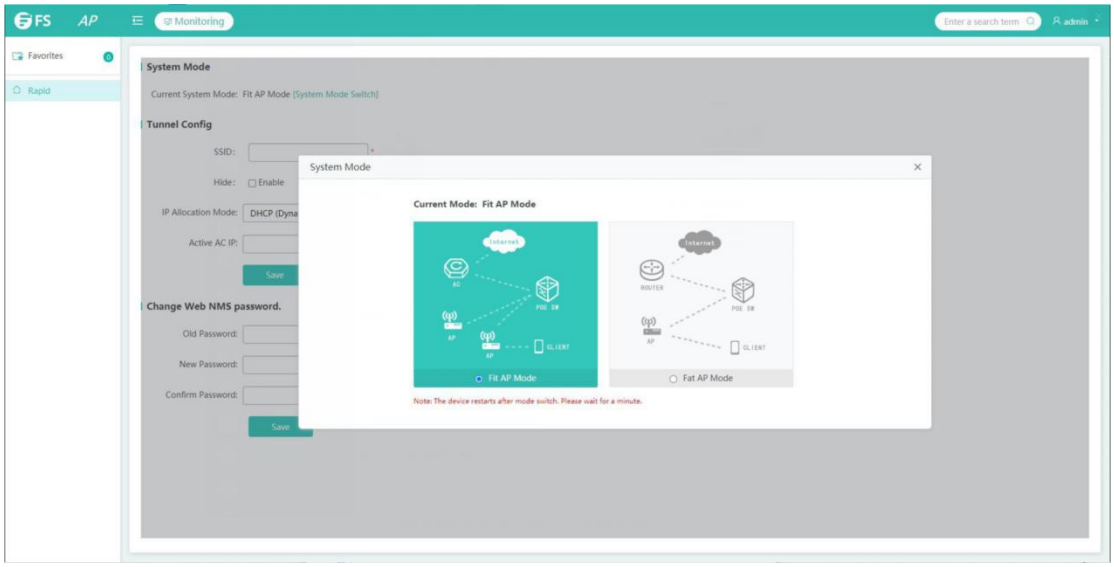
Figure 1-2 Login page



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

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

Click the **System Mode Switch** to switch the FIT/FAP working mode. (Note: The access points working in Fit AP Mode by default.)



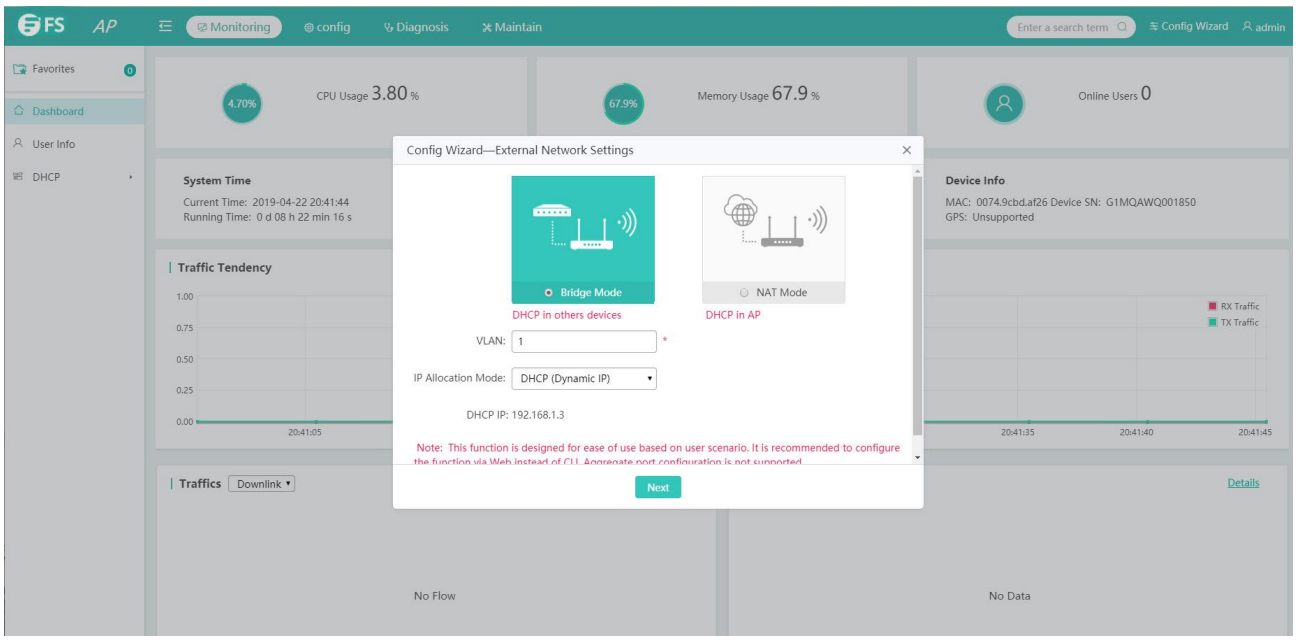
Click **Online Service** for configuration help.

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

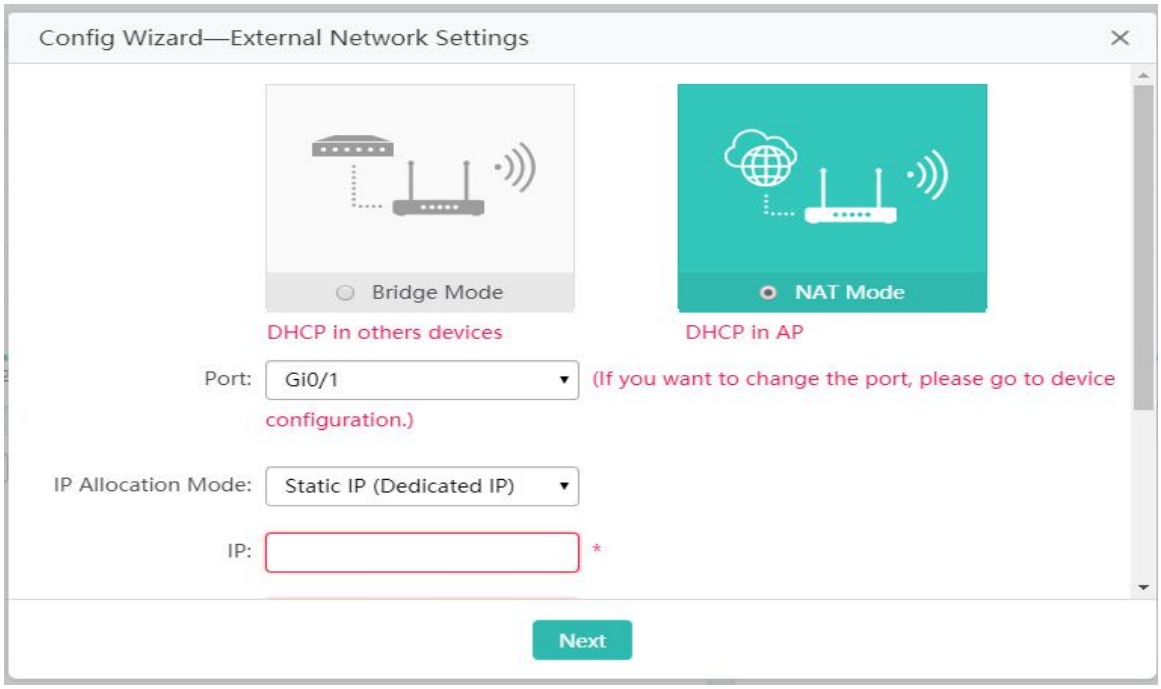
Build a WiFi network for STAs to access for Internet services.



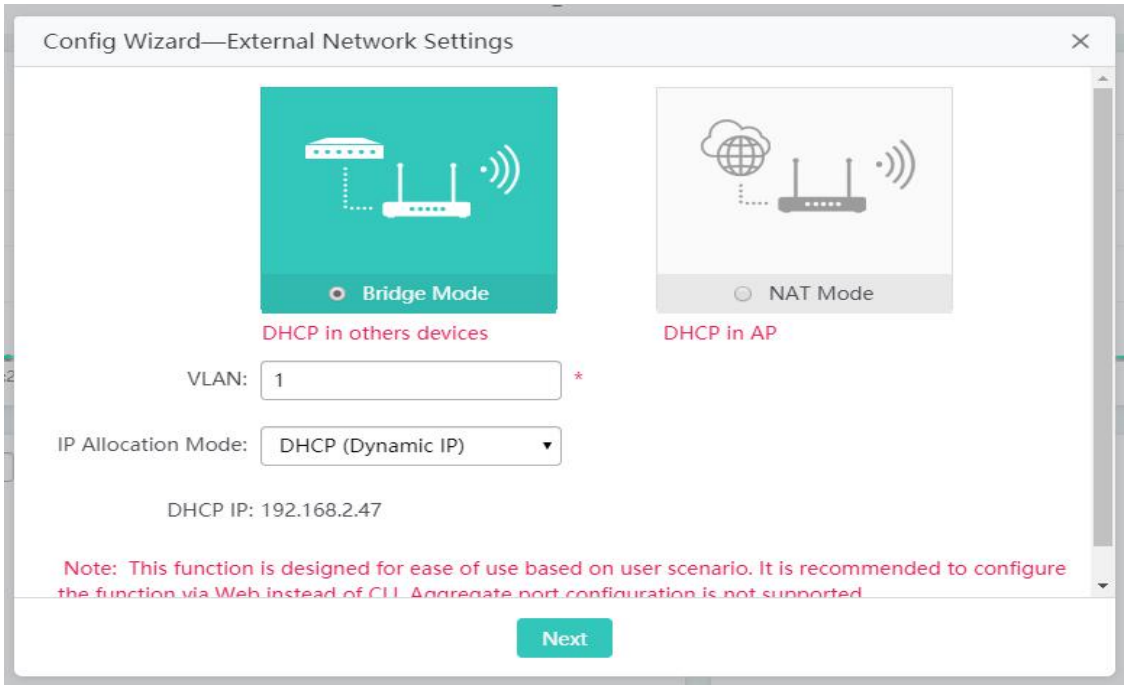
1) The **Config Wizard** page is displayed after successfully logging in to the Web if the device is in the default factory setting state, as shown in the preceding figure.

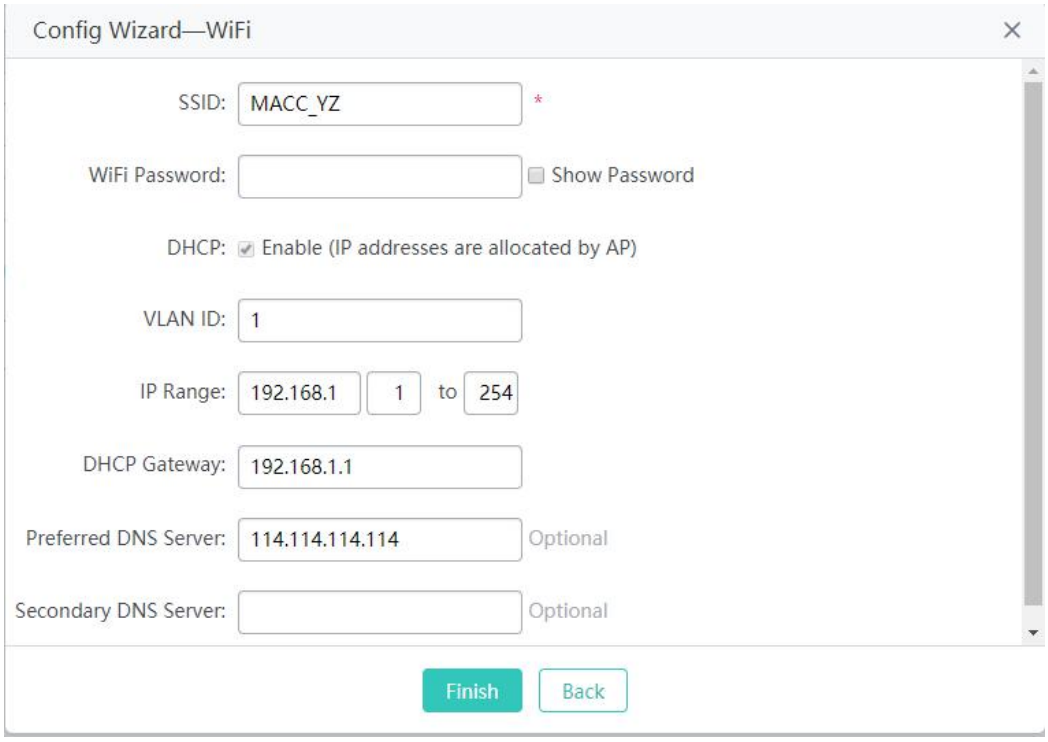
2) The **Config Wizard** page is also displayed when you click the **Config Wizard** link in the upper-right corner on the homepage.

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



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





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.

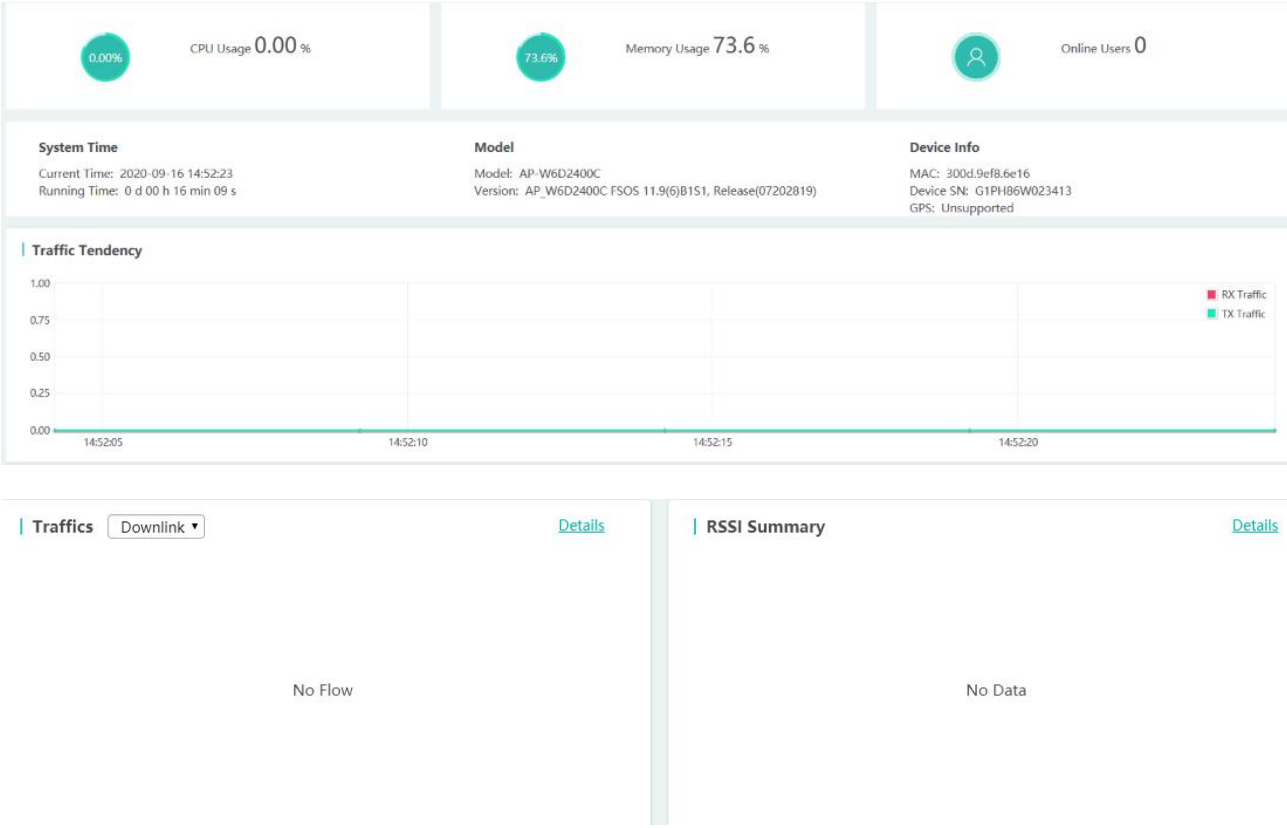
All quick settings are scenario-based settings. And some of the configuration is delivered by default. If configurations such as NAT, interface, or address pool are changed via CLI or MACC system, it is recommended to not change the configuration again via Quick Settings, otherwise there could be incompatibility.

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

Dashboard

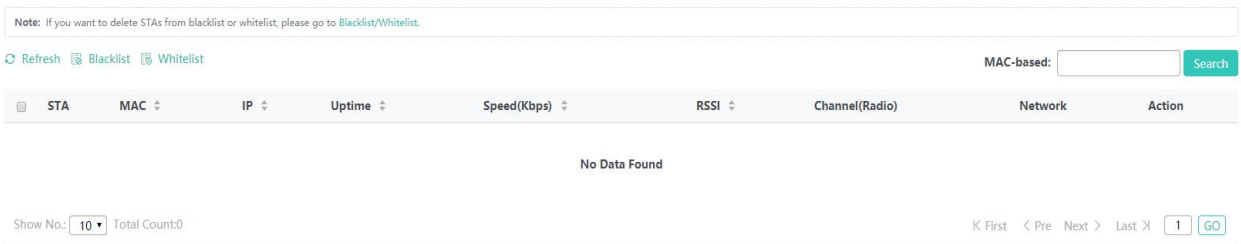
The dashboard enables viewing basic information for the AP device, including the device MAC address, device model, system alarm information, flow trends of AP device ports, latest trends of all management APs, and STA information corresponding to each management AP. In addition, it enables you to know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

User Info

User information is displayed here.

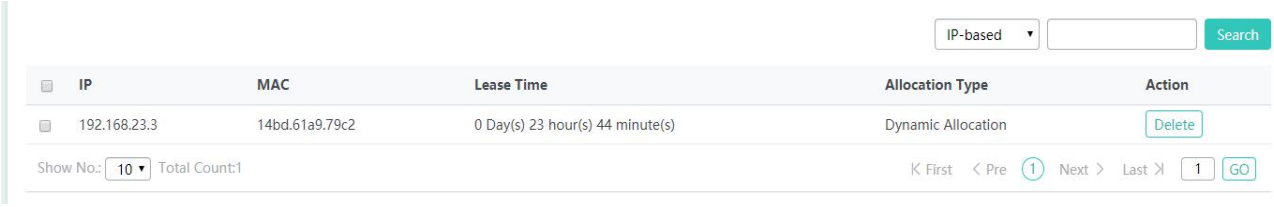


DHCP

DHCP includes DHCP client list and DHCP server status.

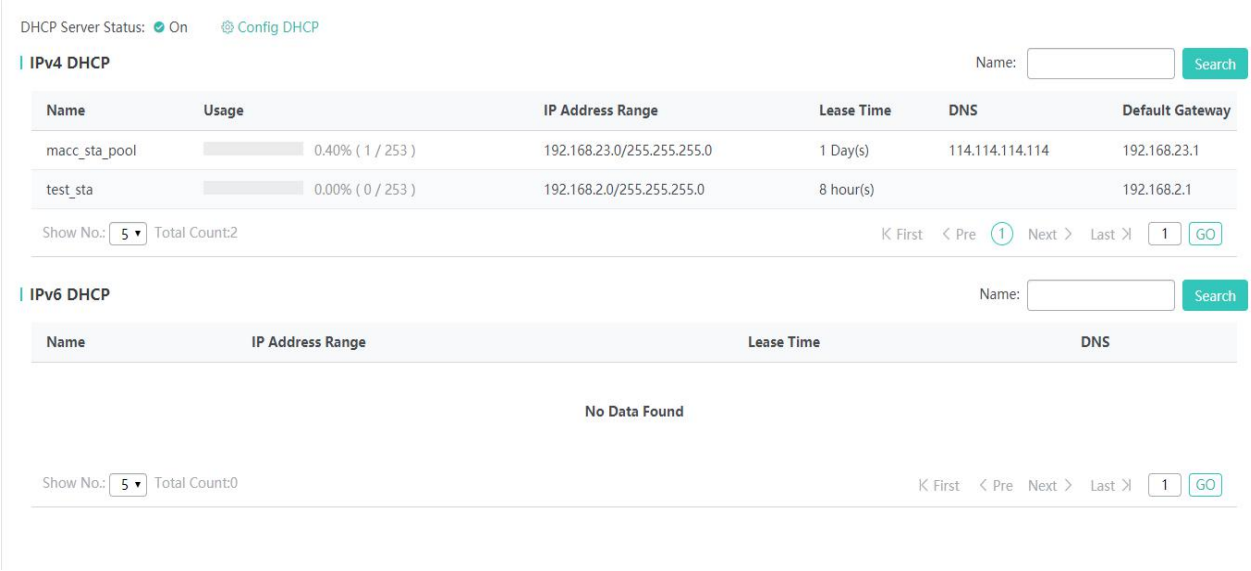
DHCP Client List

DHCP clients are displayed here.



DHCP Server Status

DHCP server status and address pool usage are displayed here.



1.3.3 Configuration

WiFi/WLAN

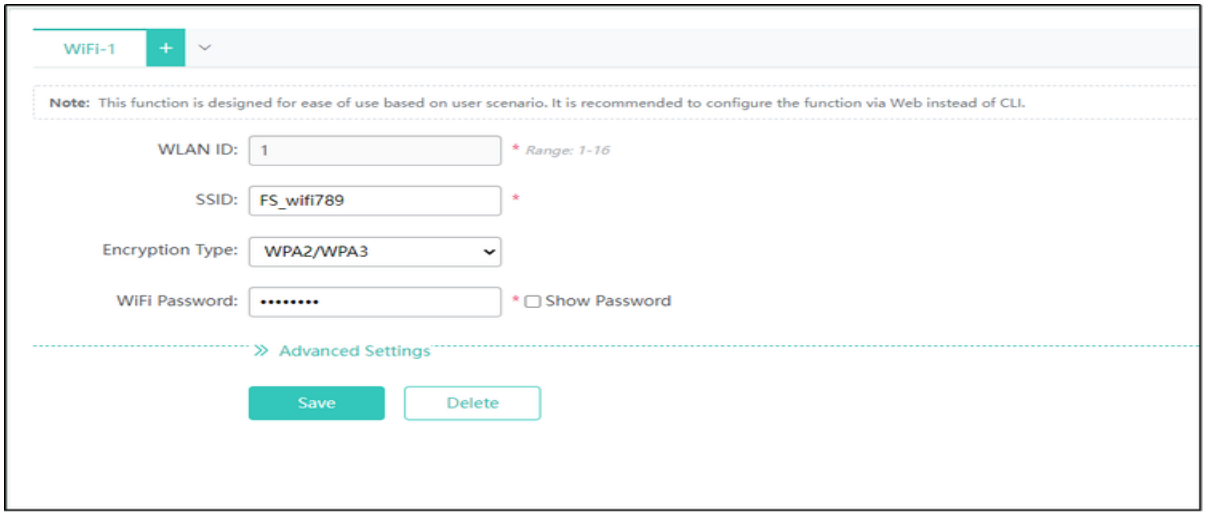
A Wireless Local Area Network (WLAN) refers to a network system that allows different PCs to communicate and share resources with each other by interconnecting different PCs through wireless communication technologies. The essence of a WLAN is that PCs are interconnected with each other in wireless rather 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 802.11standards. 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.

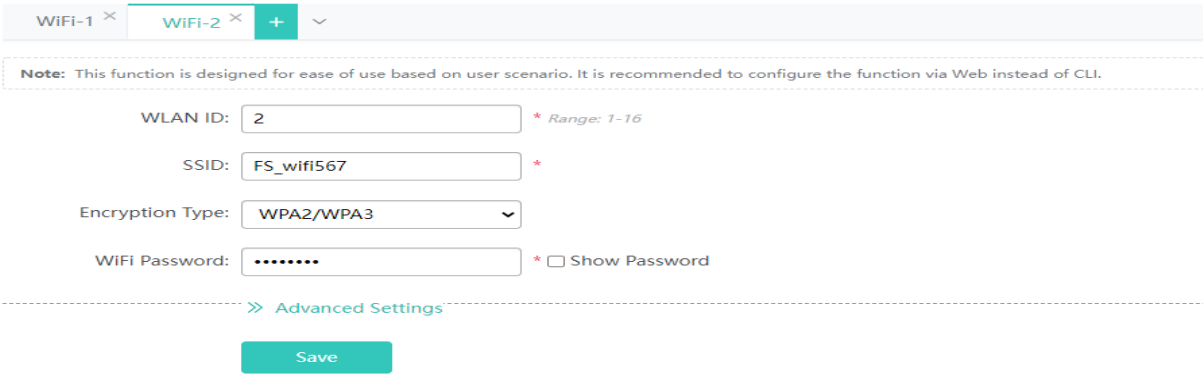
Service Set Identifier (SSID), also referred to as ESSID: It is used to distinguish different networks, that is, identifying an ESS. An SSID contains a maximum of 32 characters. A WNIC configured with different SSIDs can access different networks. SSIDs are usually broadcasted by an AP or a wireless 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.



- Adding WiFi/WLAN

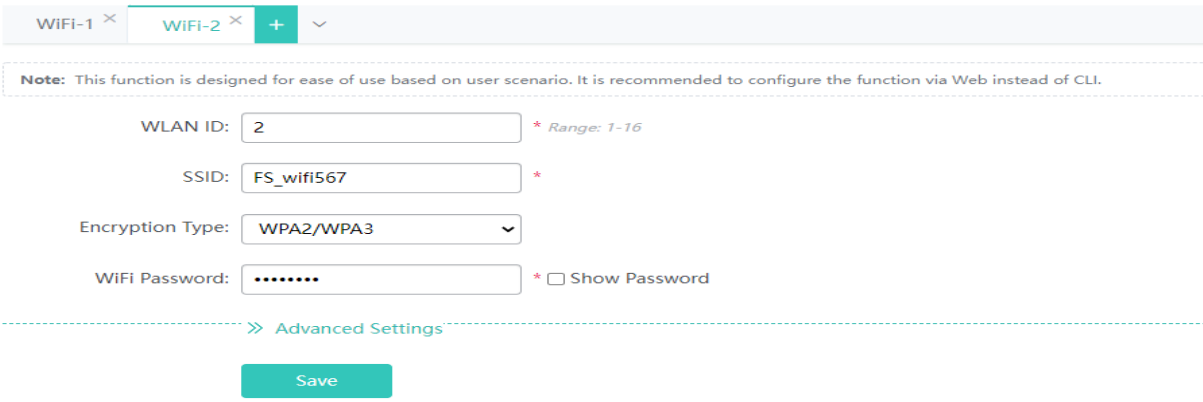


1) Click +, and a new panel for WiFi configuration is displayed.

2) Set the WiFi parameters.

3) Click **Save** to finish the configuration.

- Editing the 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.

WPA3-PERSONAL: WPA mode with higher security, this mode is suitable for ordinary home users and small businesses (currently only supports Only mode).

WPA3-ENTERPRISE-CCMP: The WPA3 security mode that uses the RADIUS server for authentication and key acquisition requires the deployment of a special authentication server (only the Only mode is currently supported).

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.

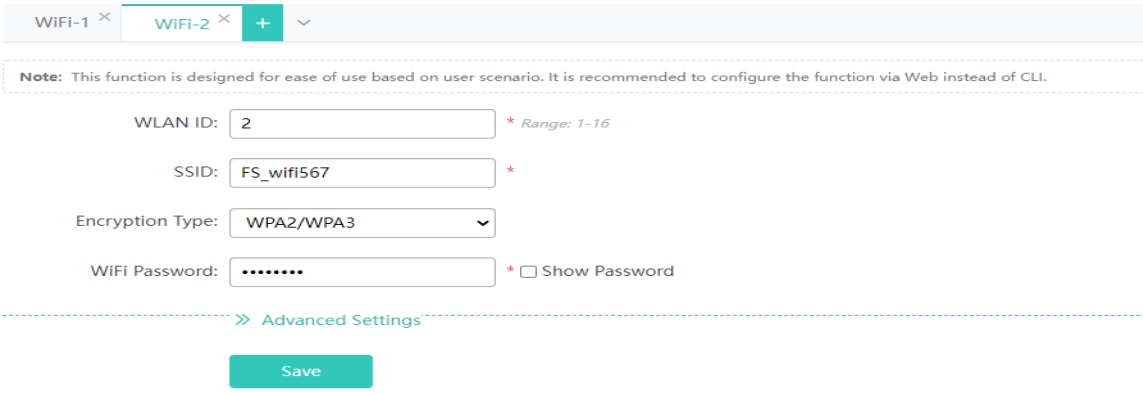
wlan-qos wlan-based * per-user-limit up-streams average-data-rate ** burst-data-rate **

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 WLANs



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

2) Click 

.

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

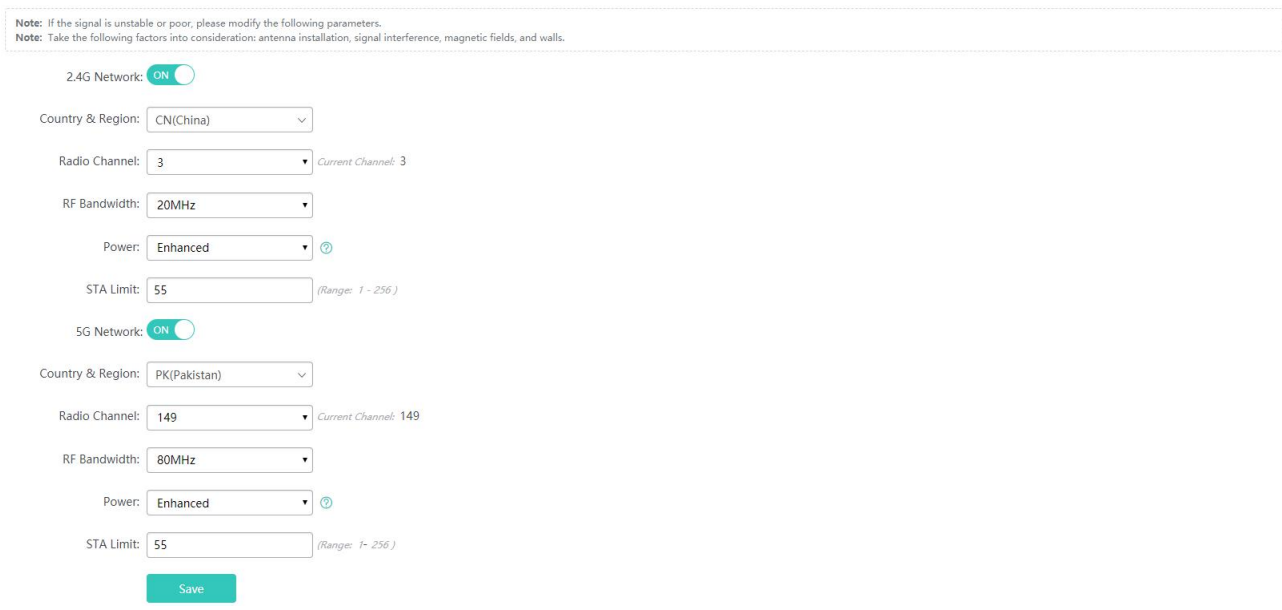
AP

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 a 2.4G network

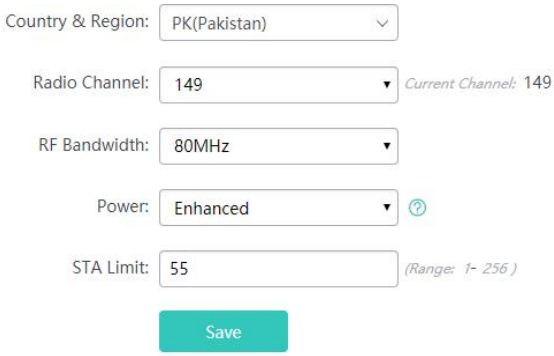


1) Click 

to enable or disable the 2.4G network.

2) Click **Enforce switch from 2.4GHz to 5GHz Network** to forcibly switch the network type.

- Enabling the 5G network



1) Click 

to enable or disable the 5G network.

2) Click **Enforce switch from 5GHz to 2.4GHz Network** to forcibly switch the network type.

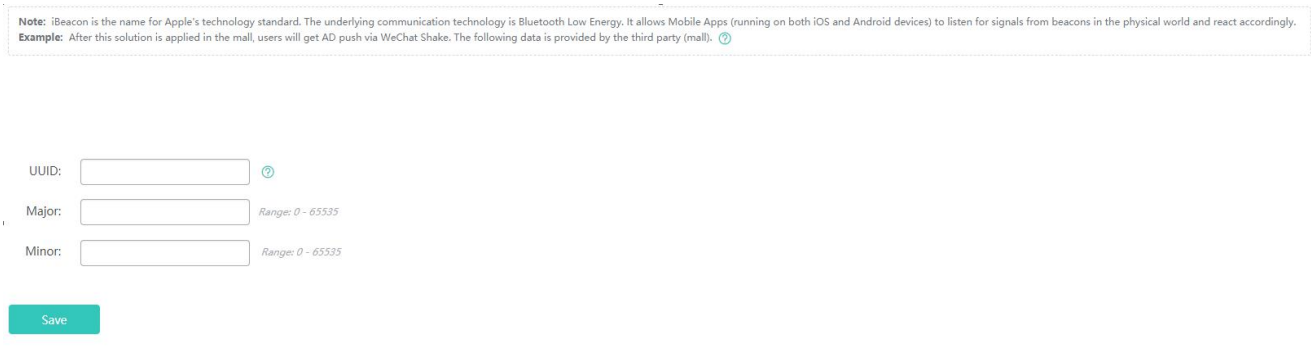
iBeacon

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.

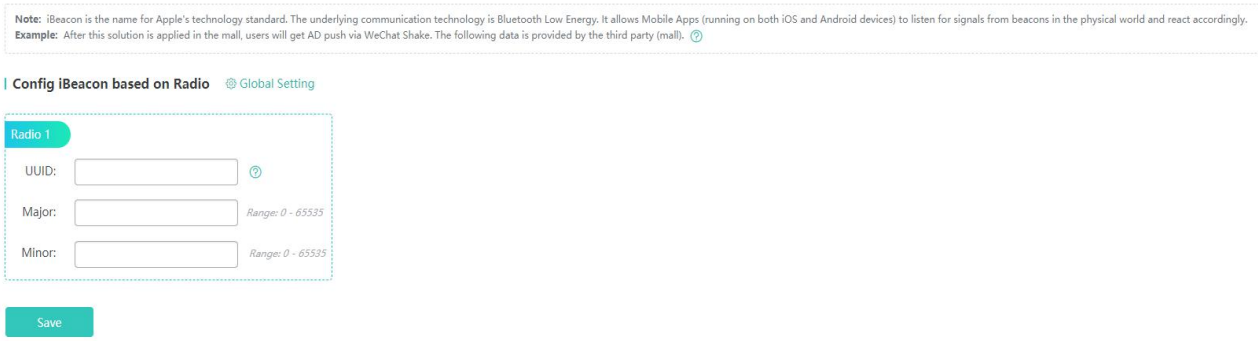
iBeacon signals are broadcast over Bluetooth, and mainly applied to WeChat Shake.

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.



- 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.



Client Limit

Client limit refers to the maximum number of associated STAs.

Radio Balance

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

Network

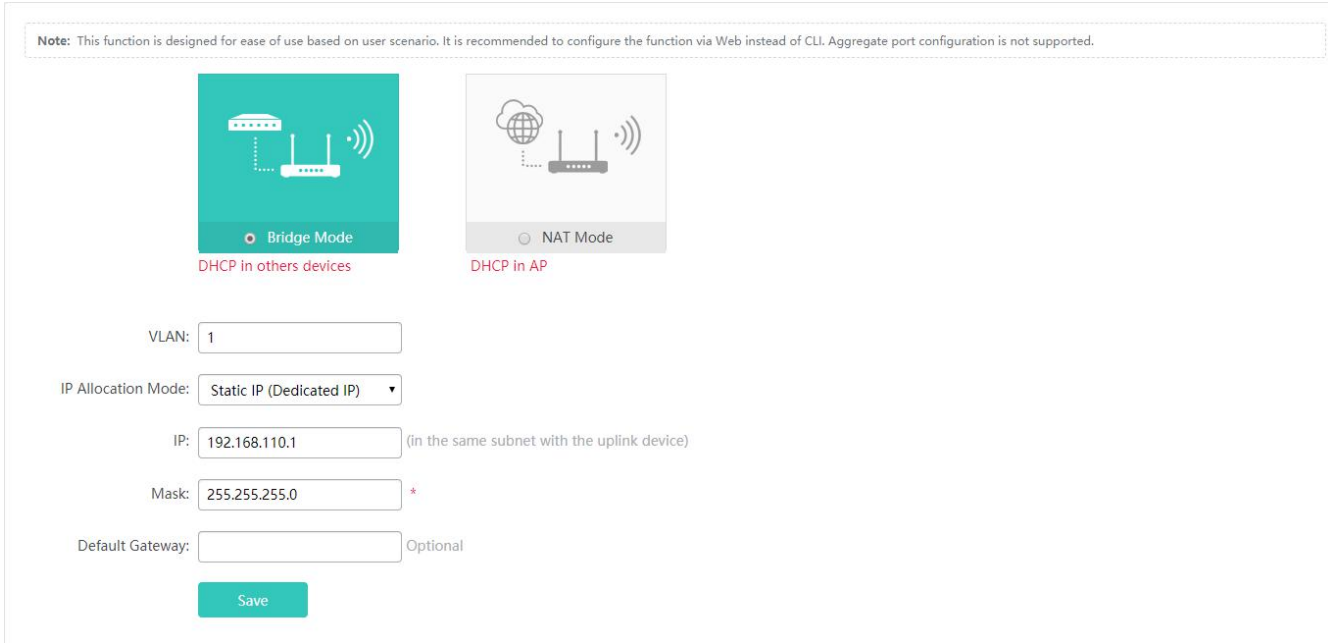
External Network Settings

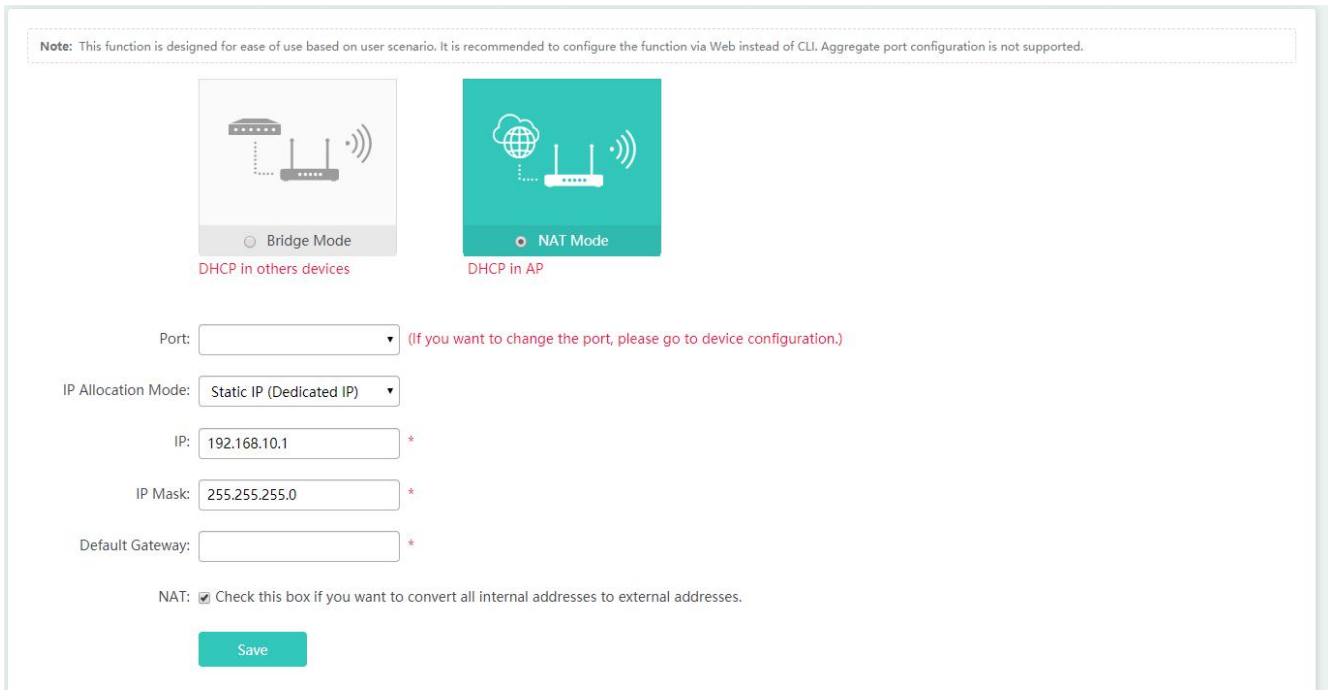
External network settings are mainly about configuration of the communication mode between the AP and external network. Two communication modes are available: Bridge mode and NAT mode.

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

In **NAT Mode**, the FS 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.





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.

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.

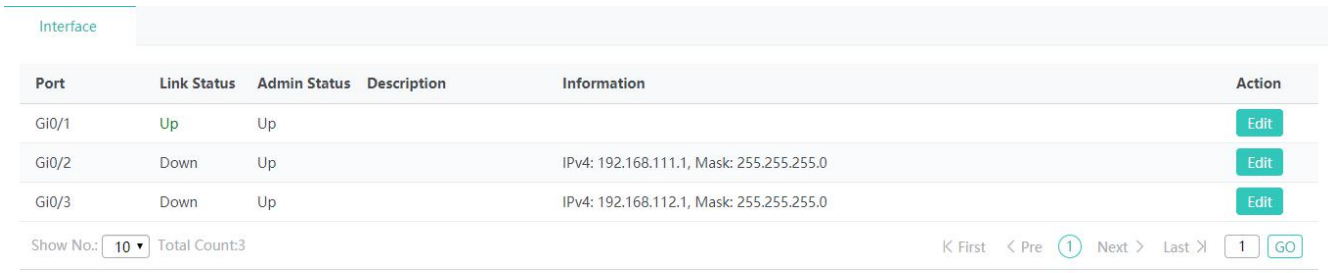
Interface Name

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."

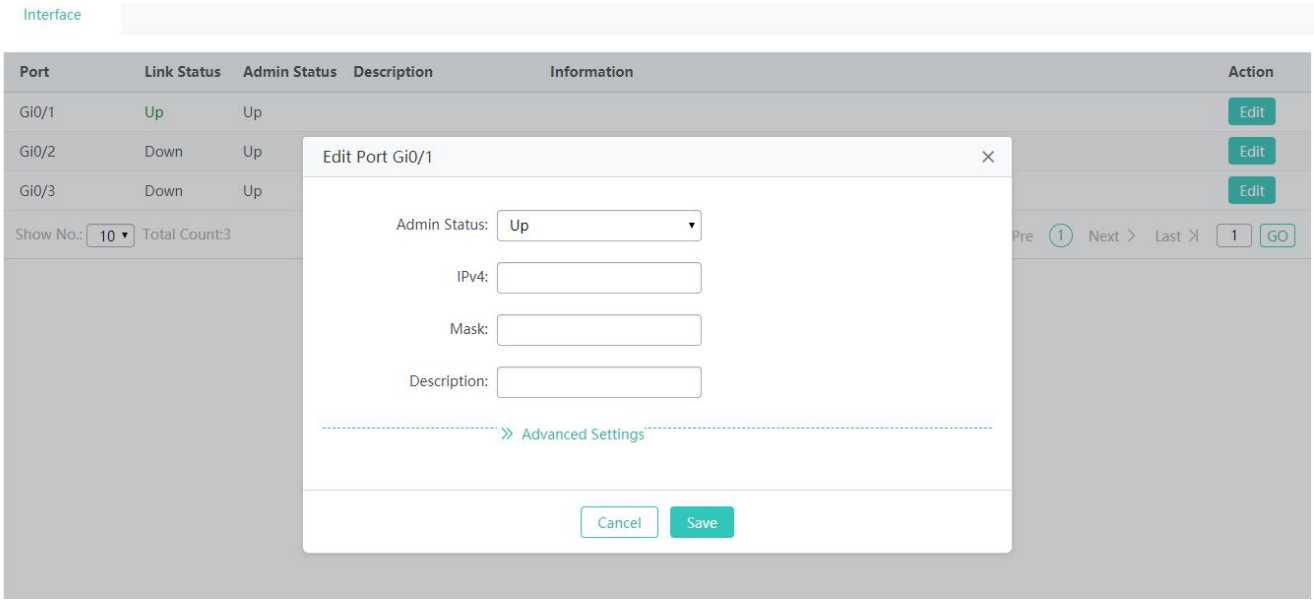
Administrative Status

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



- Editing port settings



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.

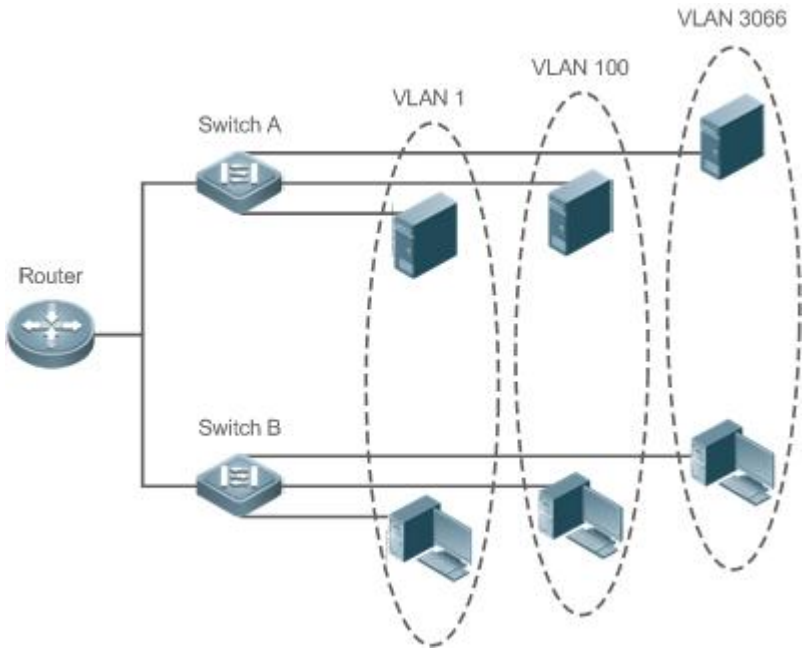
3) Click **Save**. The **Save operation succeeded** message is displayed.

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.

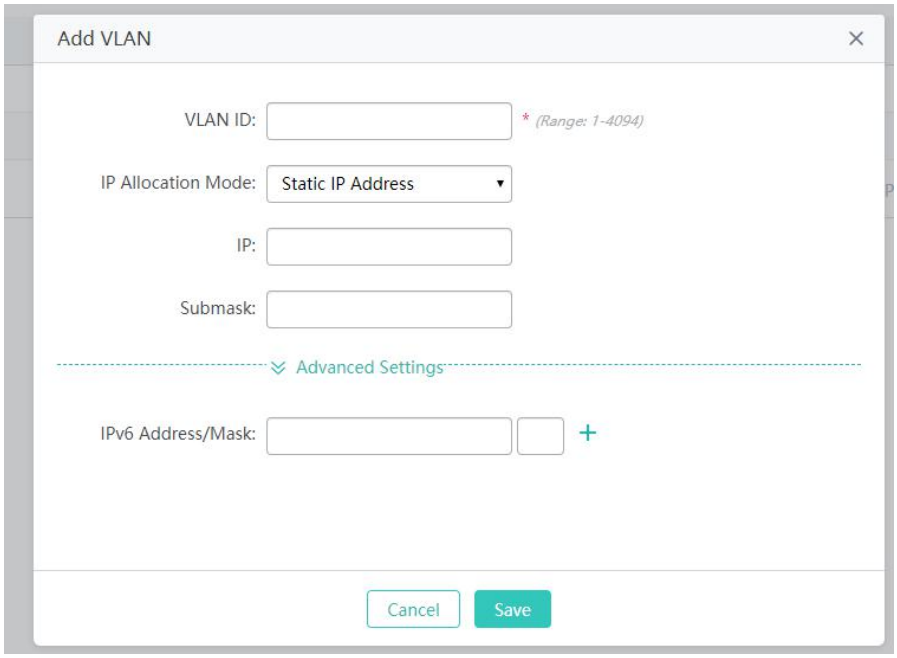
A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

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 FS 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.

- Adding a VLAN



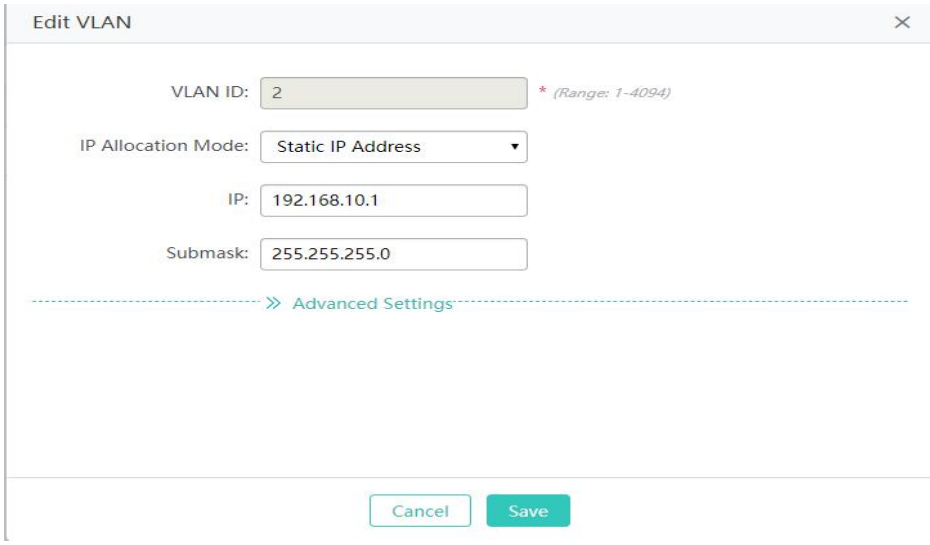
Click **Add VLAN**. A dialog box is displayed, as shown in the preceding figure. Set corresponding parameters in the dialog box and click **Save**. The newly added VLAN is displayed in the VLAN list after the **Add operation succeeded** message is displayed.

- Deleting VLANs in Batches

1) Select the VLAN to be deleted from the list.

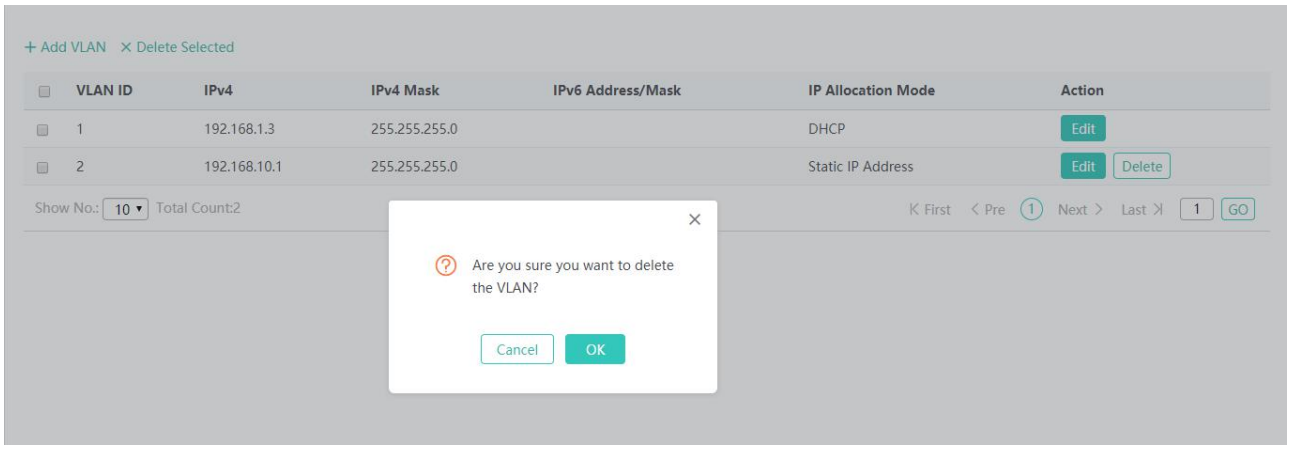
2) Click **Delete Selected** to finish deleting.

- Editing a VLAN



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



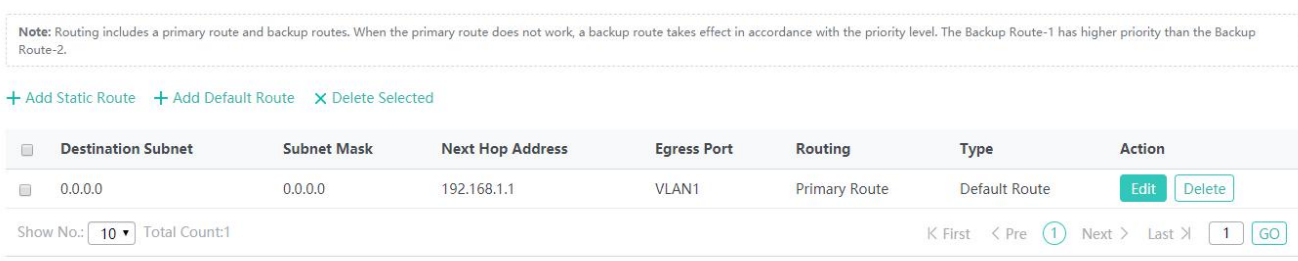
Click the **Delete** button for a VLAN in the list and then click **OK** in the displayed dialog box to finish deleting.

Route

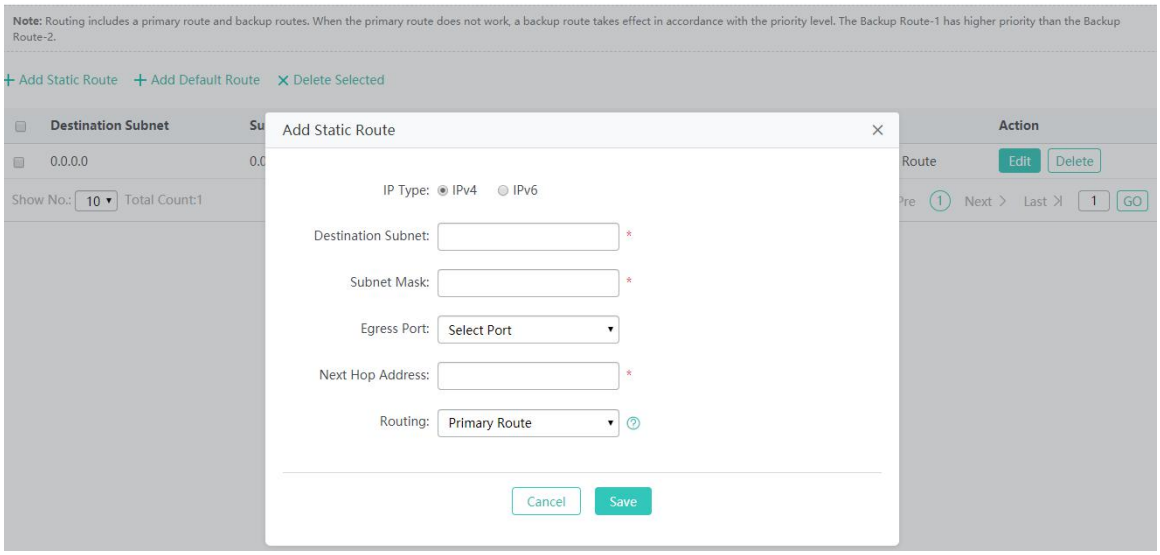
Routing is the process of selecting a path for traffic in a network, or between or across multiple networks.

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.

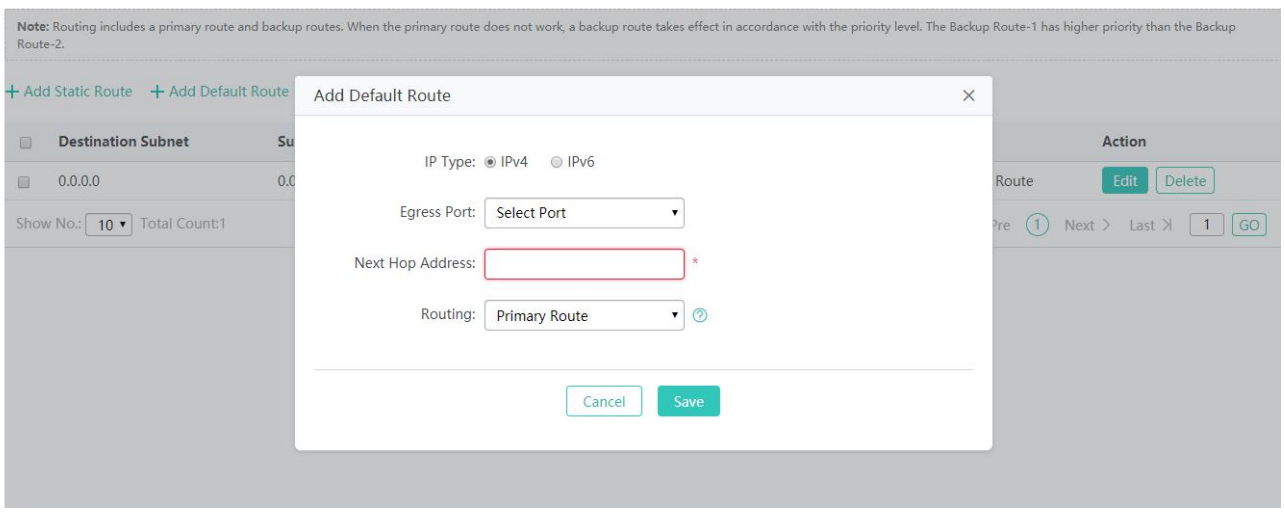


- Adding a static route



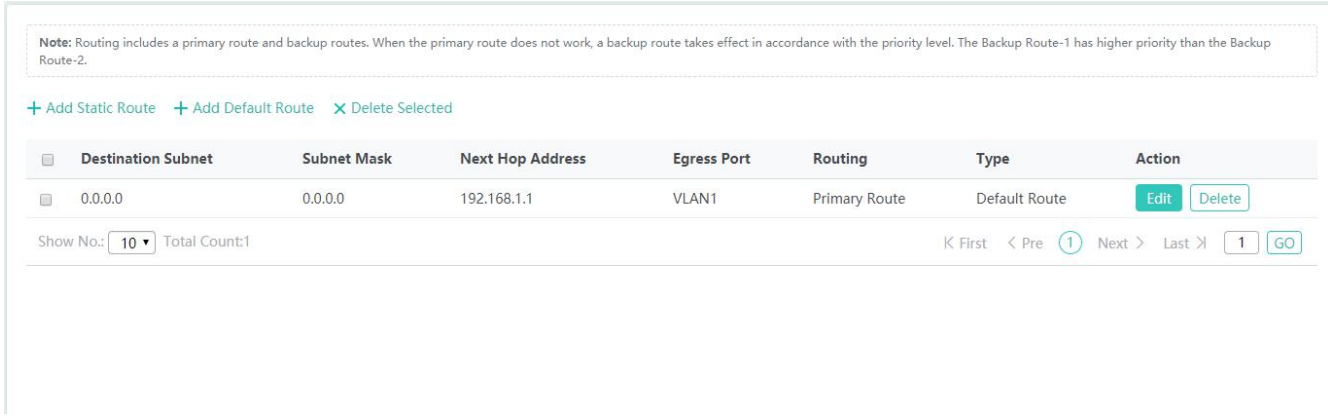
Click **Add Static Route**, set the configuration items in the dialog box displayed, and click **Save**. The newly added static route is displayed in the route list after the **Save operation succeeded** message is displayed.

- Adding the Default Route



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.

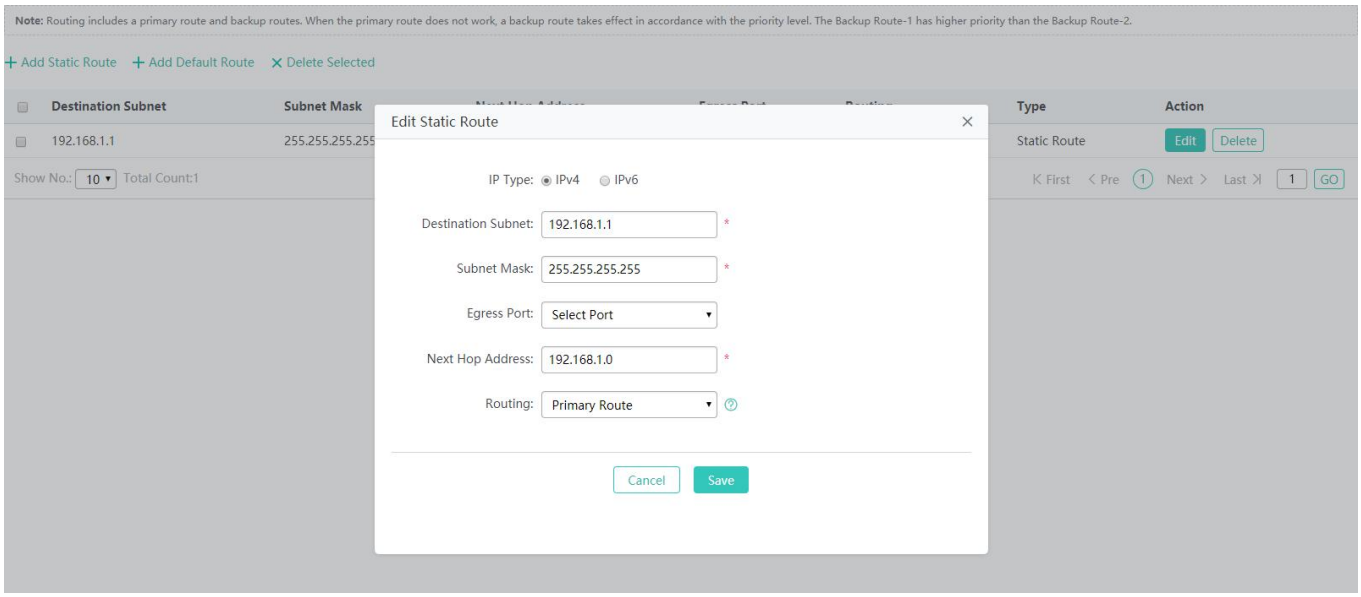
- Deleting Routes in Batches



1) Select the route from the list.

2) Click **Delete Selected Route** to finish deleting.

- Editing a Route

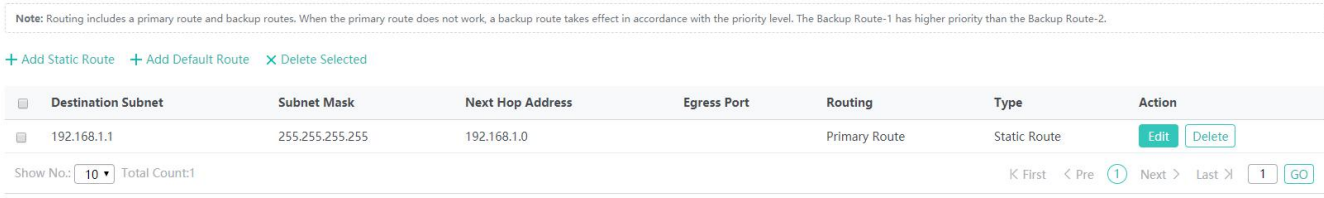


1) Click the **Edit** button for a route in the list.

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



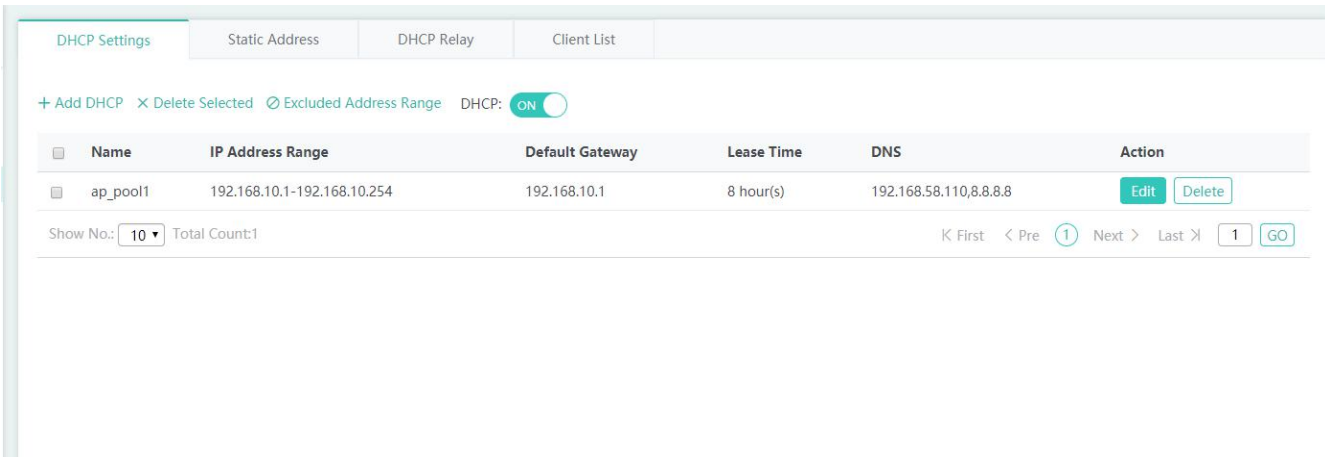
Click the **Delete** button for a route in the list and then click **OK** in the displayed dialog box to finish deleting.

DHCP

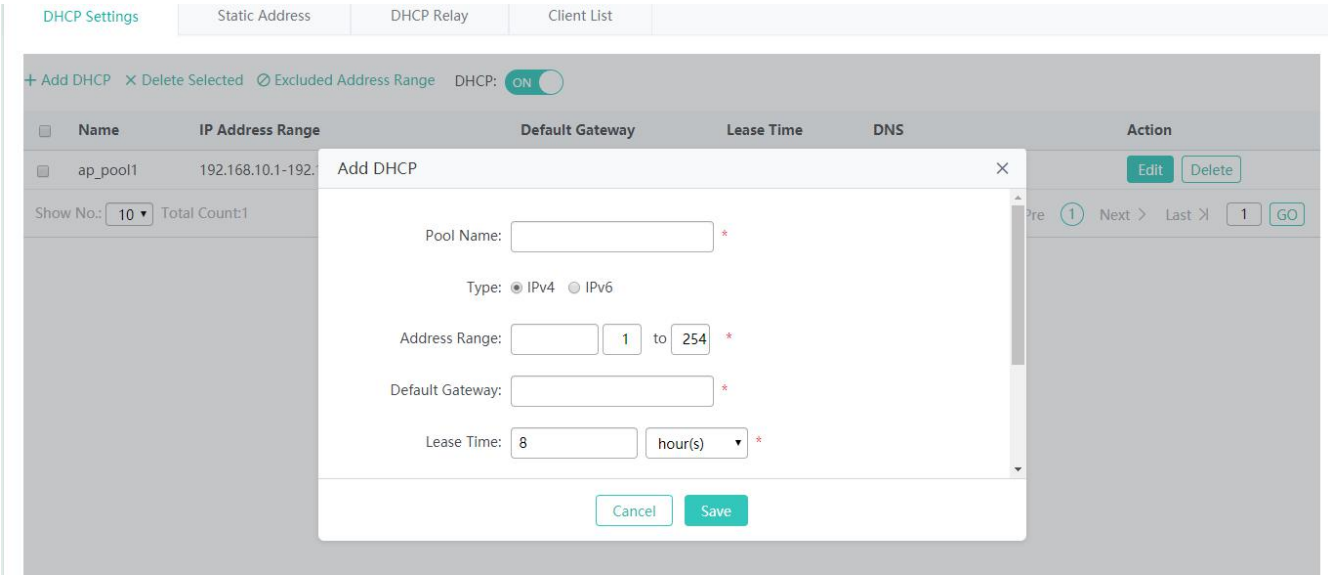
Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task 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

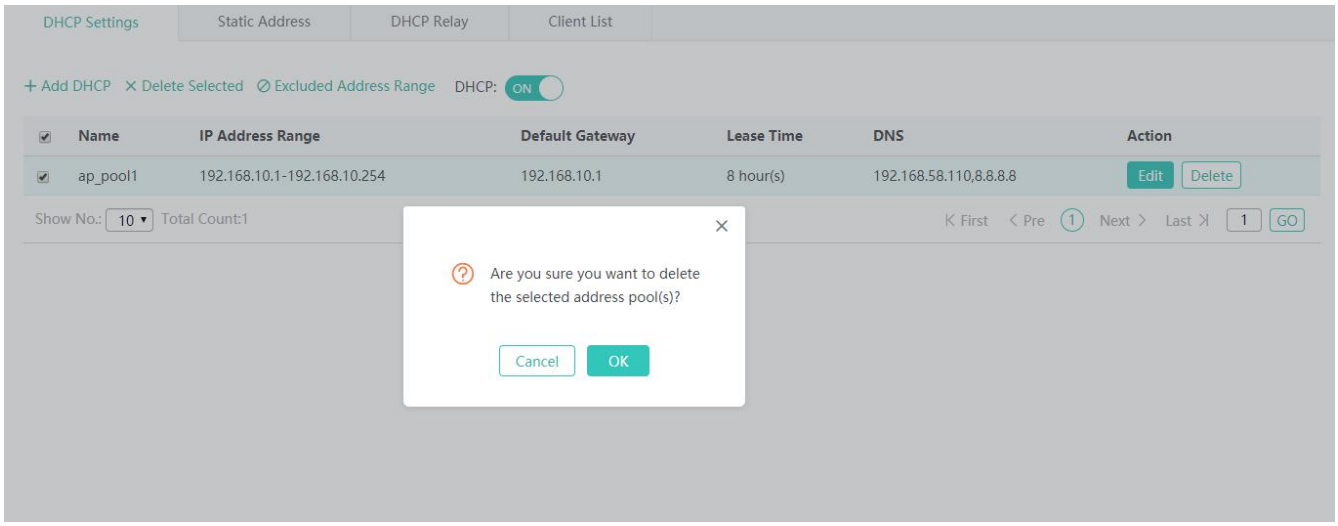


- Adding a DHCP Pool



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.

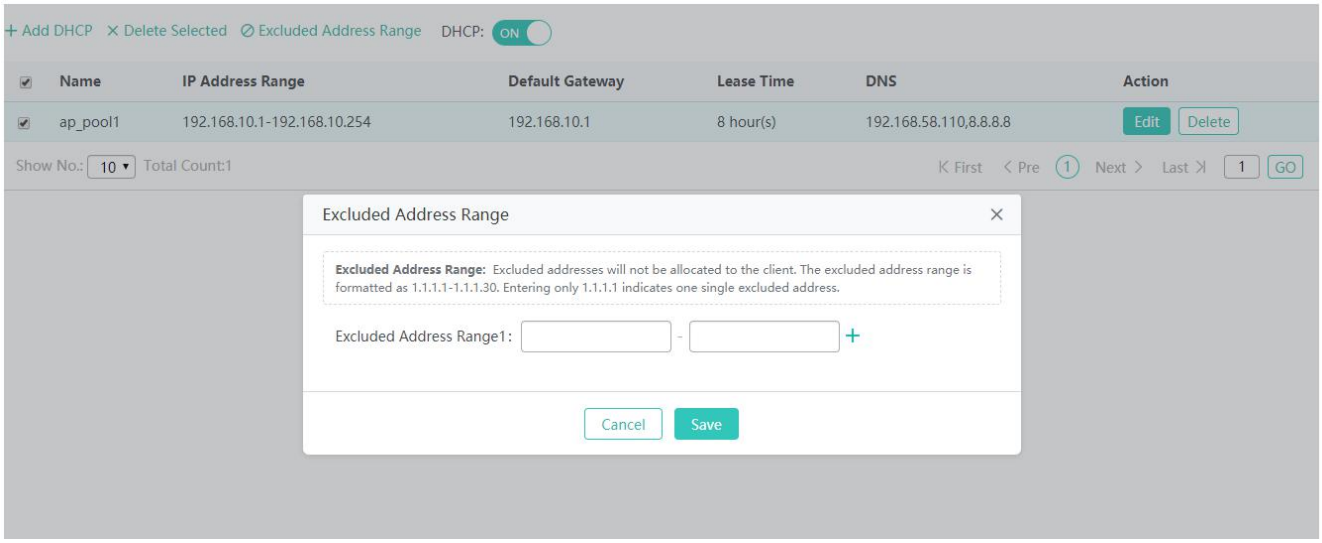
- Deleting DHCPs in Batches



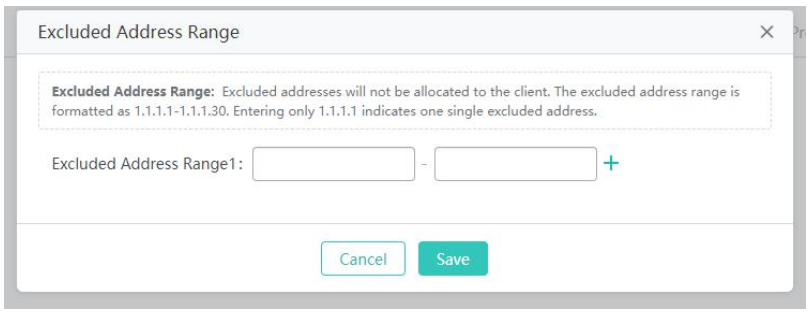
1) Select the DHCP pool from the list.

2) Click **Delete Selected DHCP** and then click **OK** in the dialog box displayed to finish deleting.

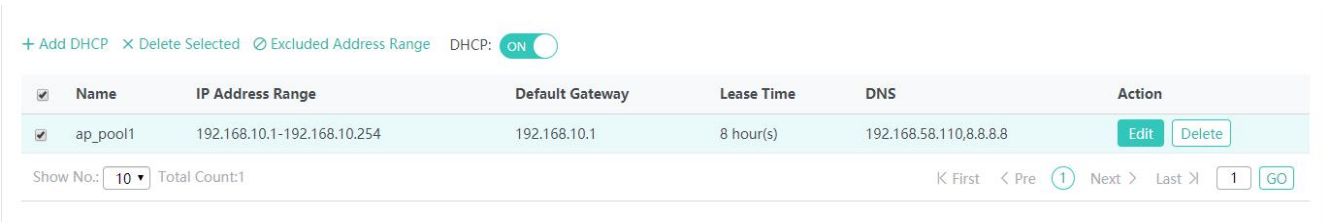
- Configuring Excluded Address Range



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.



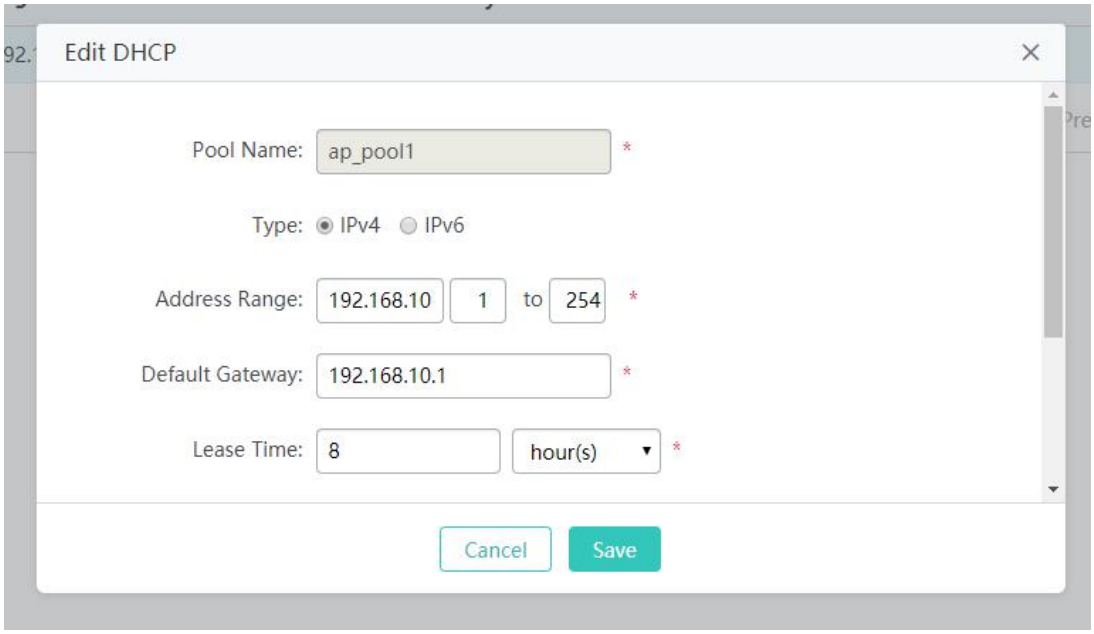
- DHCP Service



Click 

to enable or disable the DHCP service.

- Editing a DHCP Pool

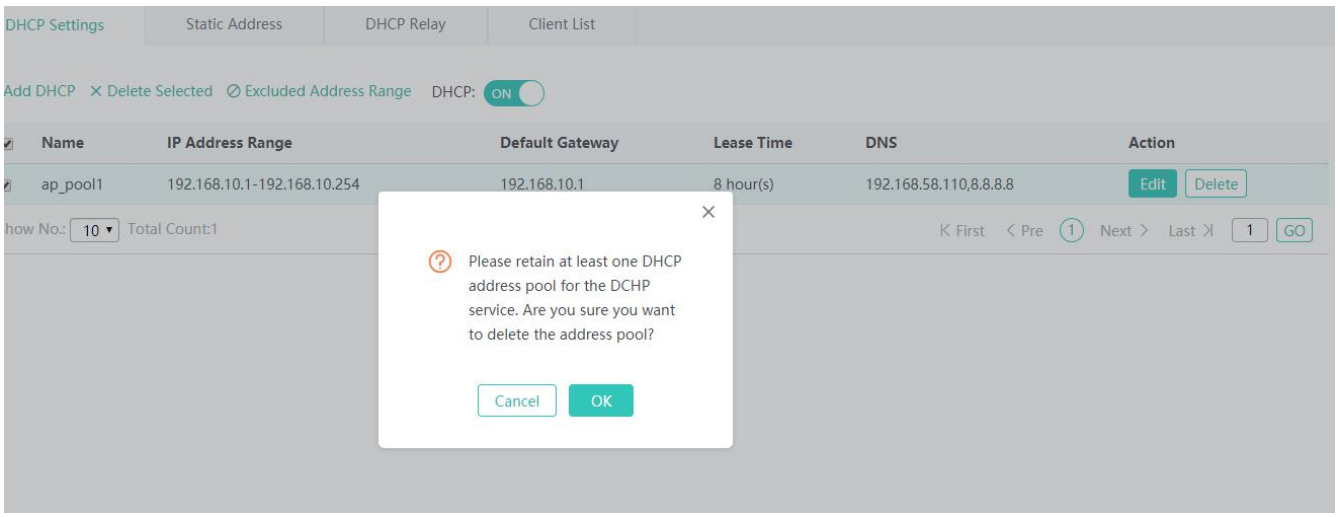


1) Click the **Edit** button for a DHCP pool in the list.

2) The configuration for the DHCP pool is displayed in the dialog box. Next, edit the configuration.

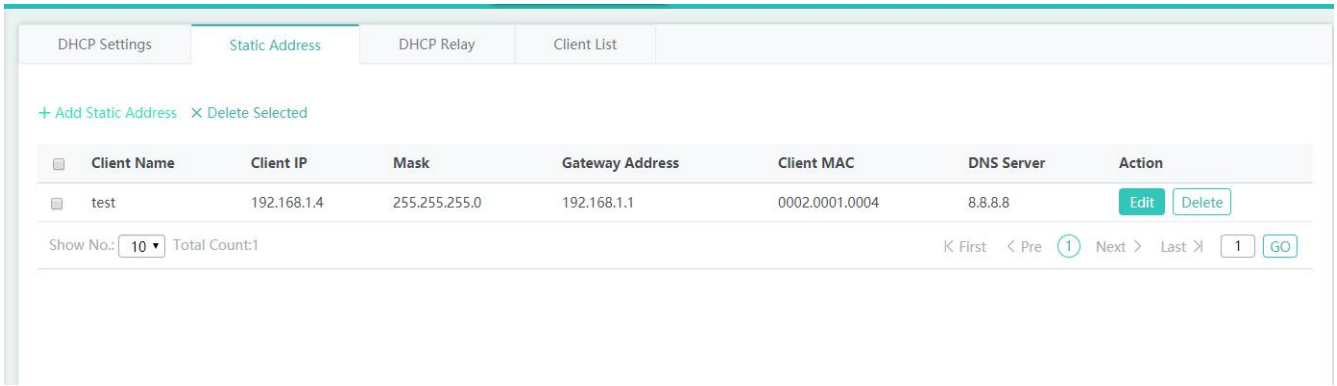
3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a DHCP Pool

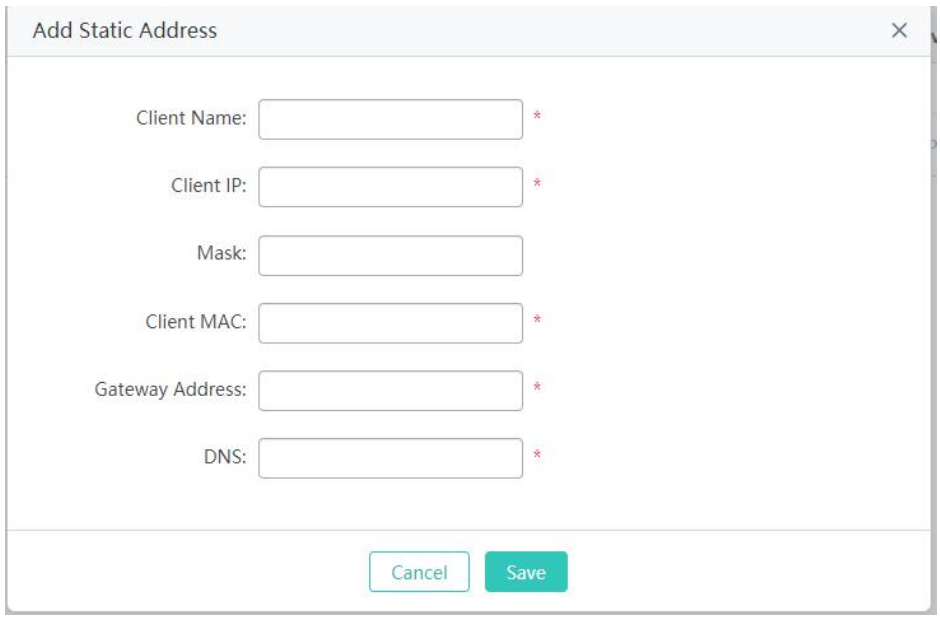


Click **Delete** to finish deleting.

Static Address

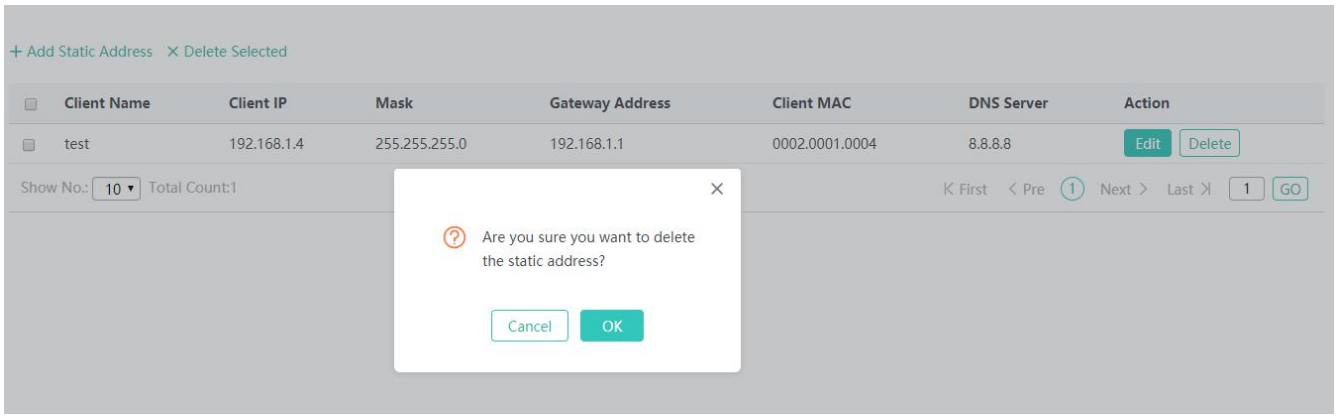


- Adding a Static Address



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.

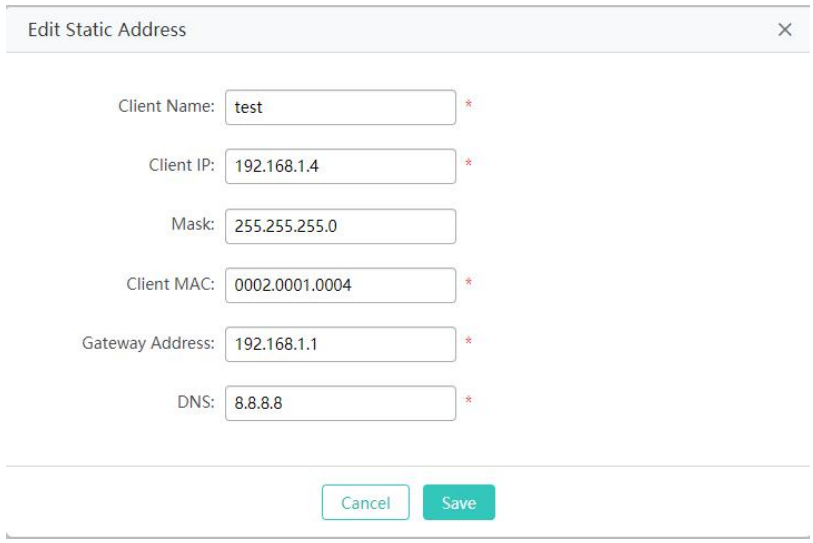
- Deleting Static Addresses in Batches



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

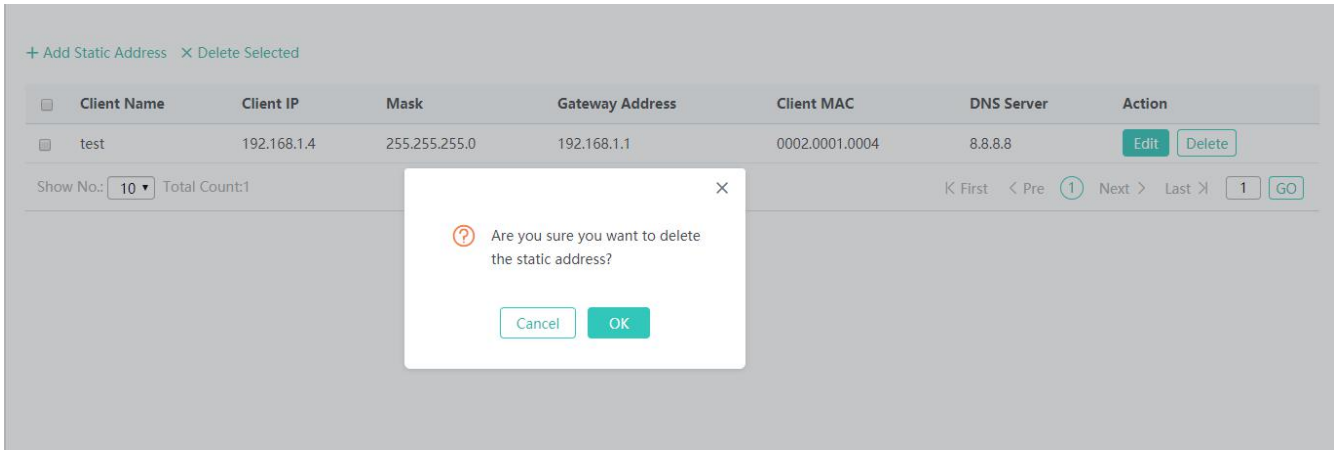


1) Click the **Edit** button for a static address in the list. A dialog box is displayed.

2) The configuration for the static address is displayed in the dialog box. Next, edit the configuration.

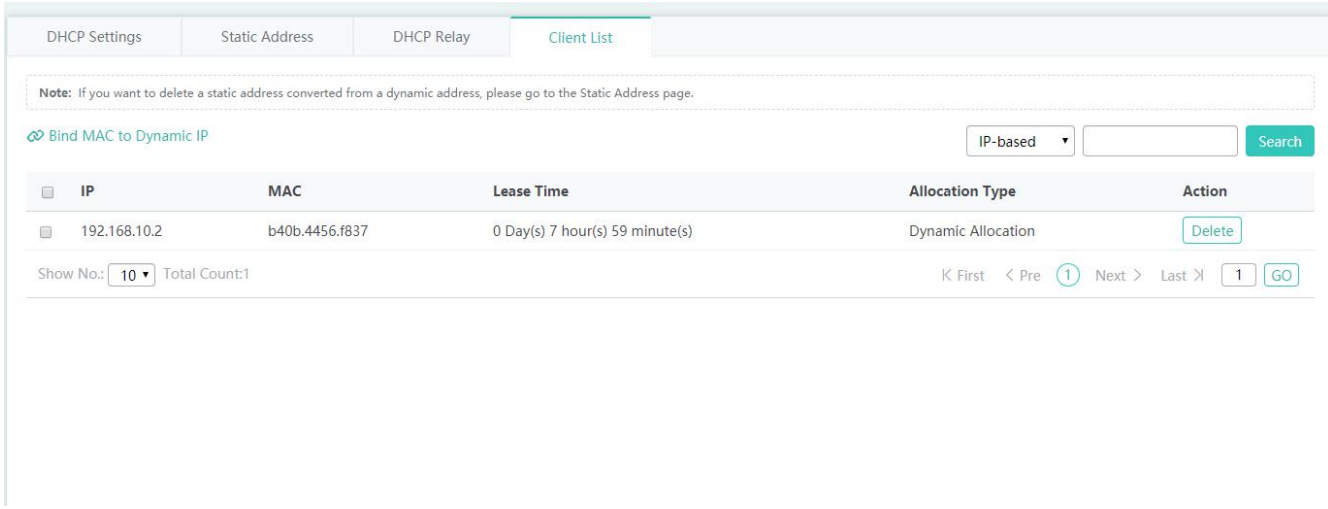
3) Click **Save**. The **Save operation succeeded** message is displayed.

- Deleting a Static Address

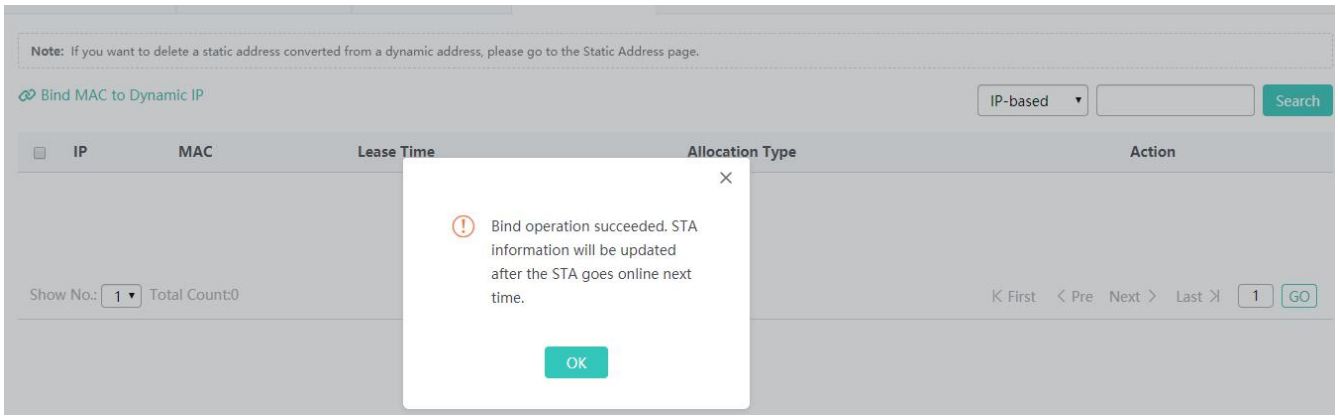


Click the **Delete** button for a static address in the list to finish deleting.

Client List



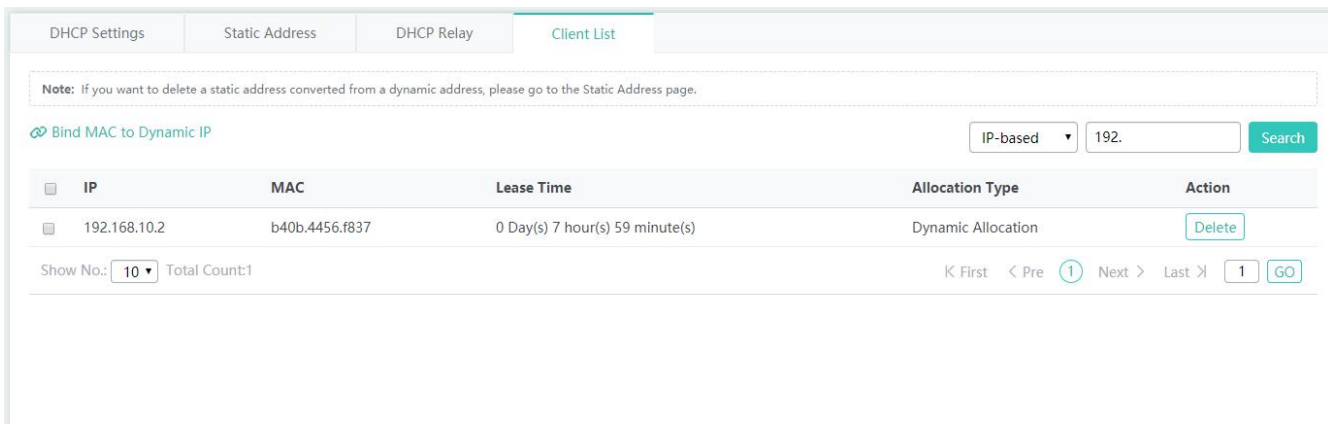
- Binding a MAC Address to a Dynamic IP Address



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:



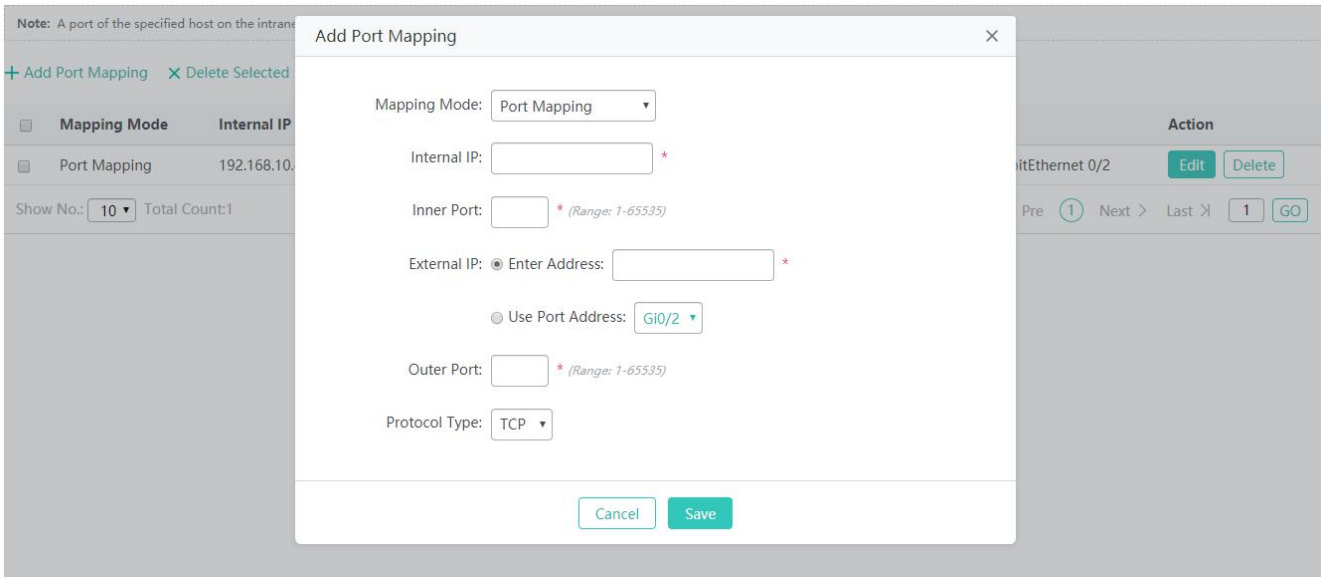
Input the IP address in the text box. Click **Search**. The search results meeting the criterion are displayed in the list.

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.

- Adding Port Mapping



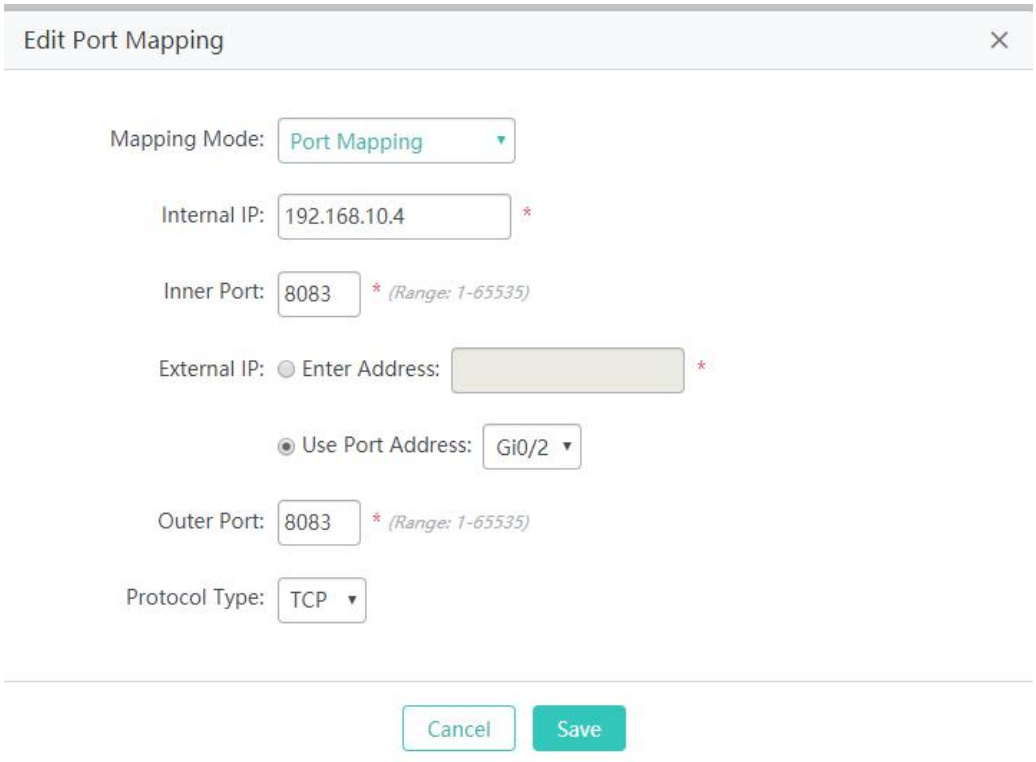
Click **Add Port Mapping**, set the configuration items in the dialog box displayed, and then click **Save**. The newly added port mapping is displayed in the list after the **Save operation succeeded** message is displayed.

- 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

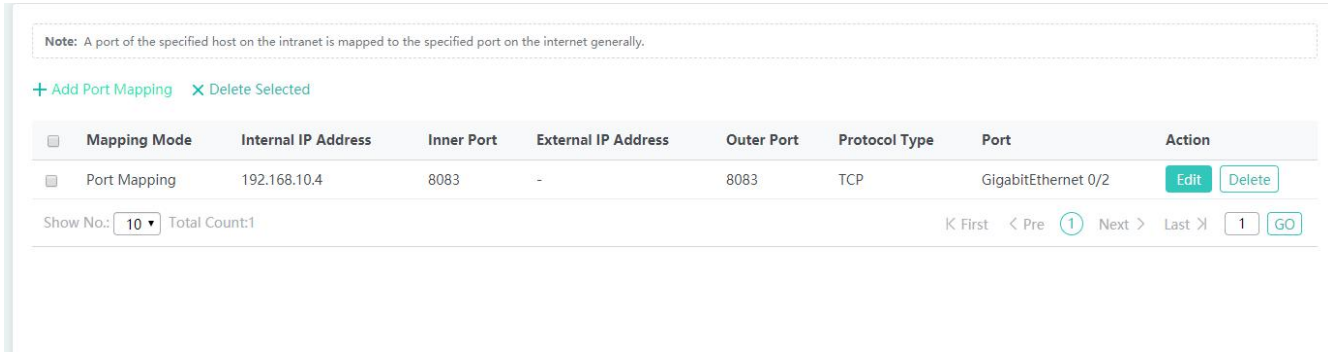


1) Click the **Edit** button for a port mapping in the list.

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



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

VPN

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

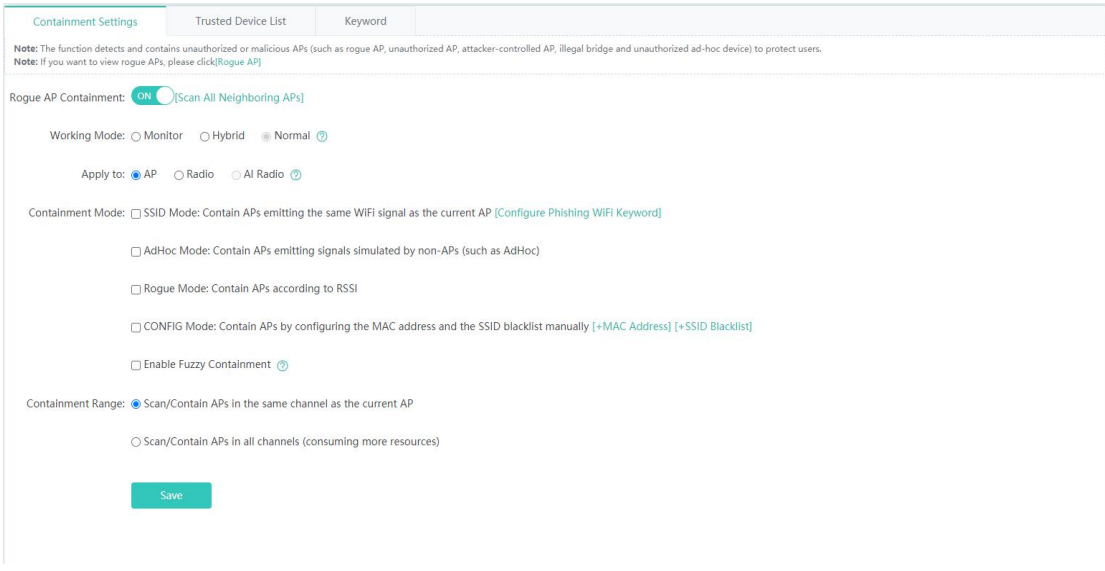
The **Advanced Settings** include some algorithm settings. It is recommended to use the default settings.

Security

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.

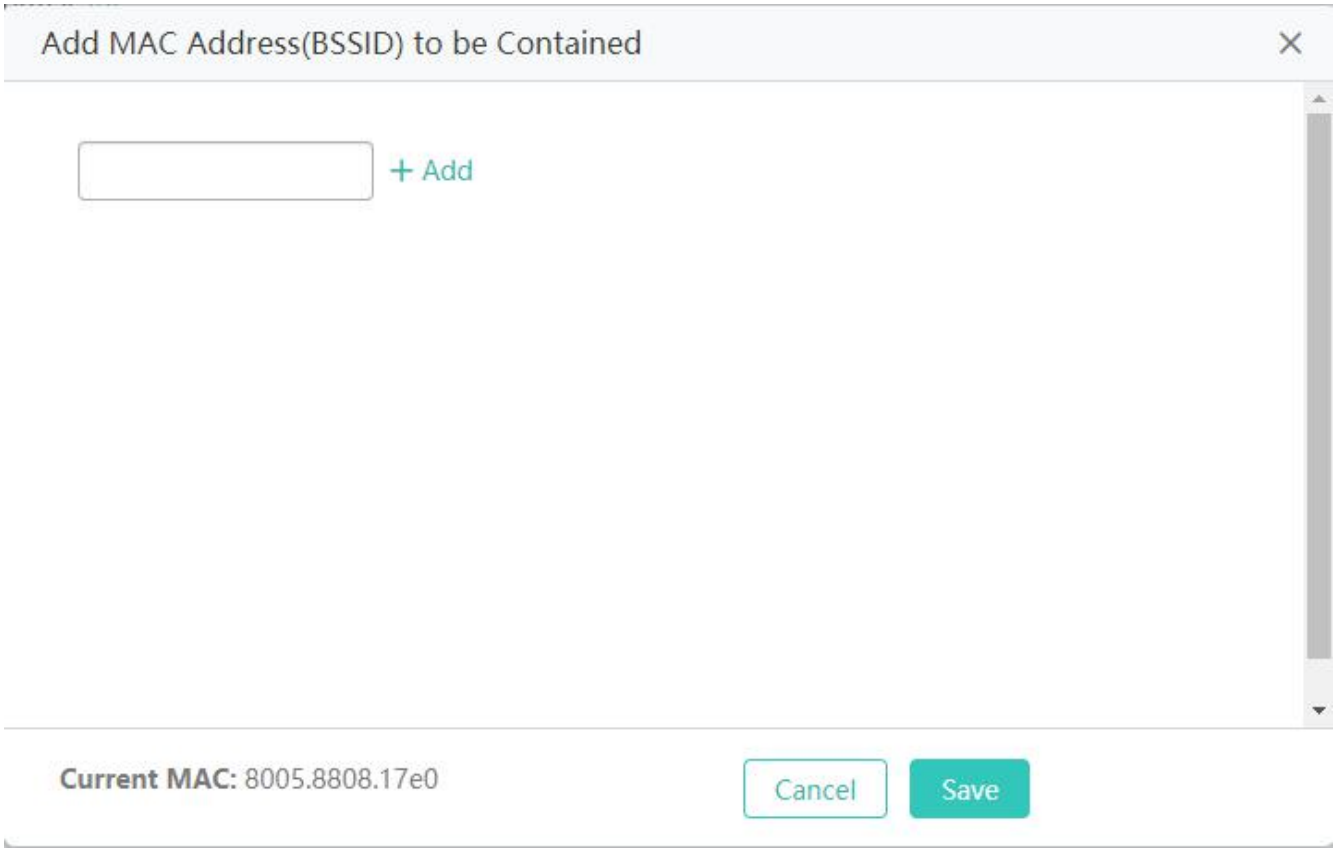
Containment Settings



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

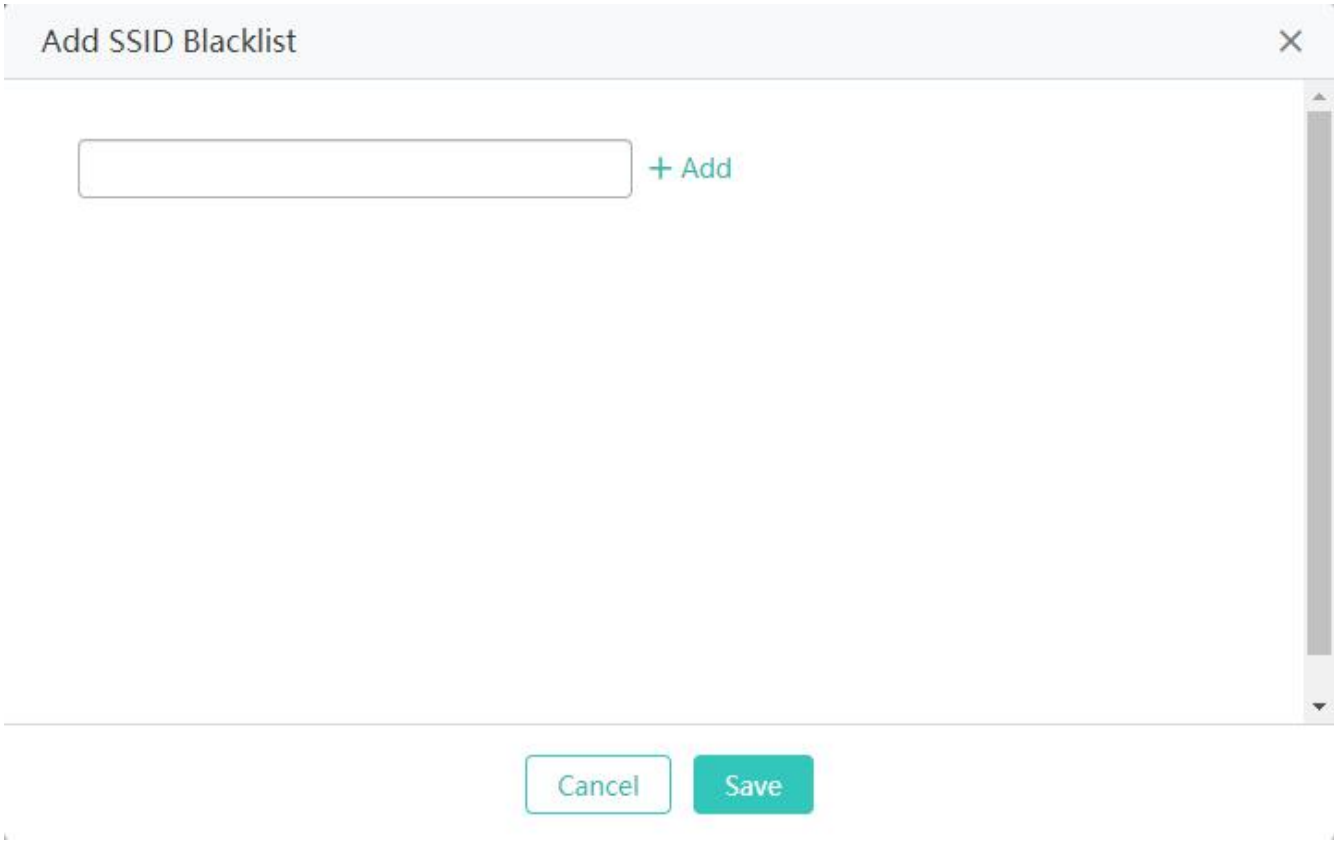
- Adding a MAC address

You can add the MAC address to be contained here.



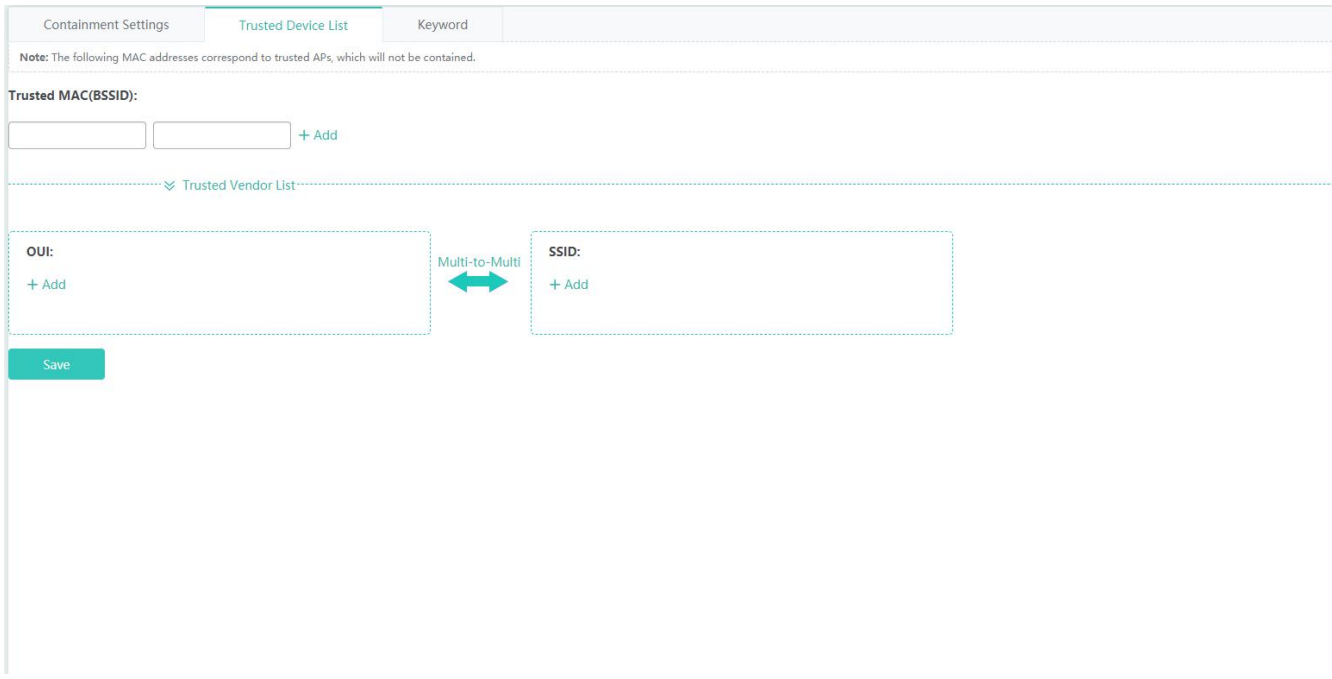
- Adding an SSID blacklist

You can add the MAC address to be contained here.



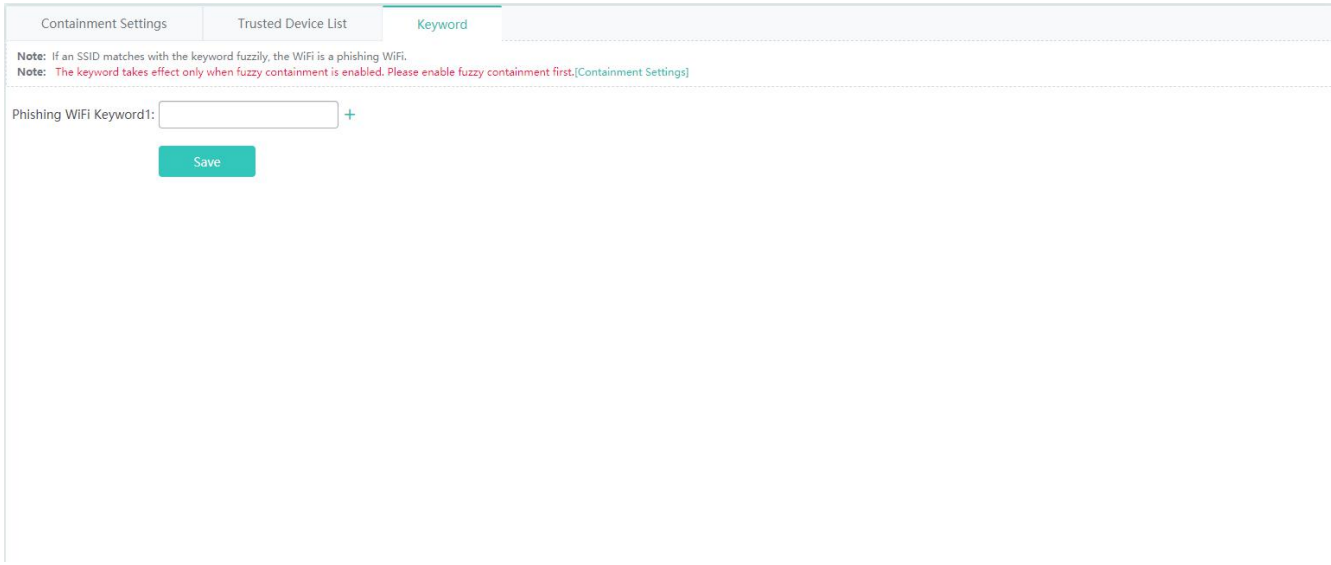
Trusted AP

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.



Phishing WiFi Keyword

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

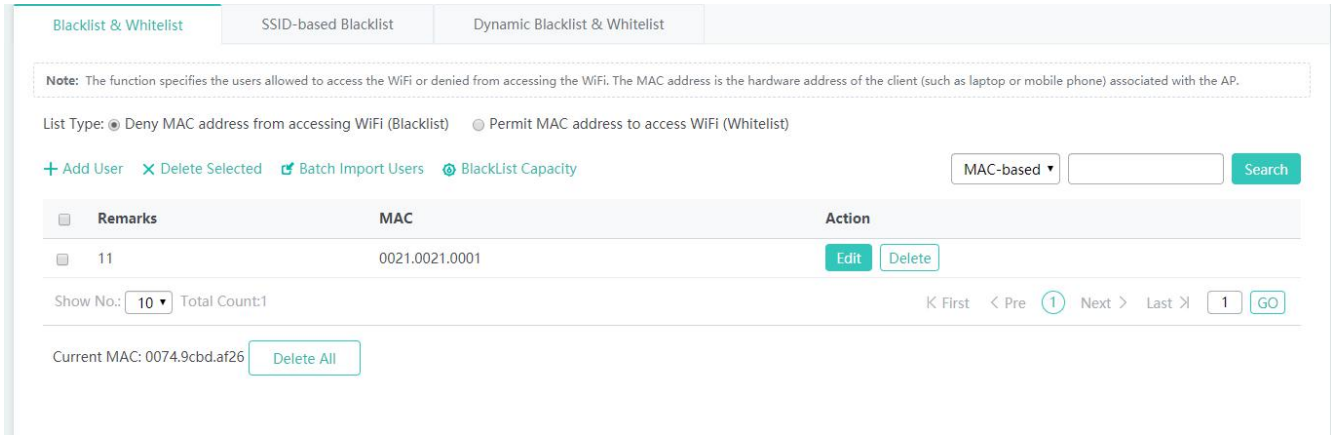


Blacklist & Whitelist

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

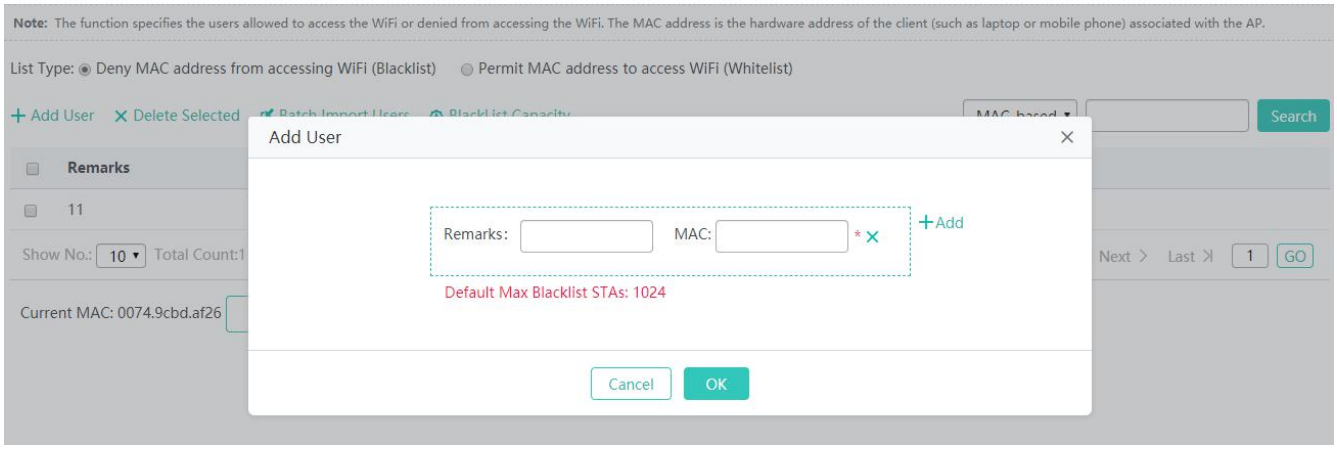
The whitelist/blacklist capacity is 1024 by default.

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

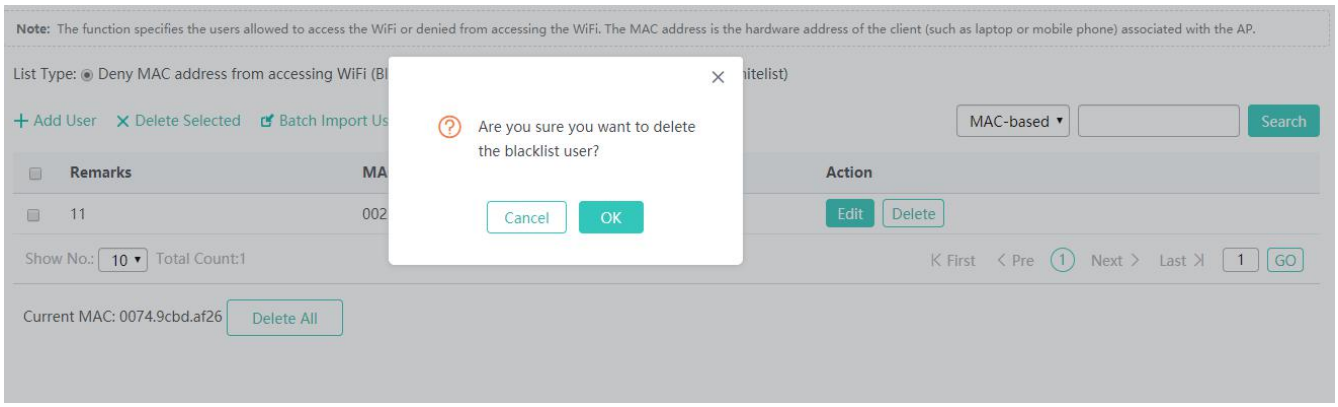


Click + Add User to add a MAC address for a user. You can add multiple MAC addresses.

Click the **SSID-based Access Control** link to configure the blacklist and whitelist for each WiFi.



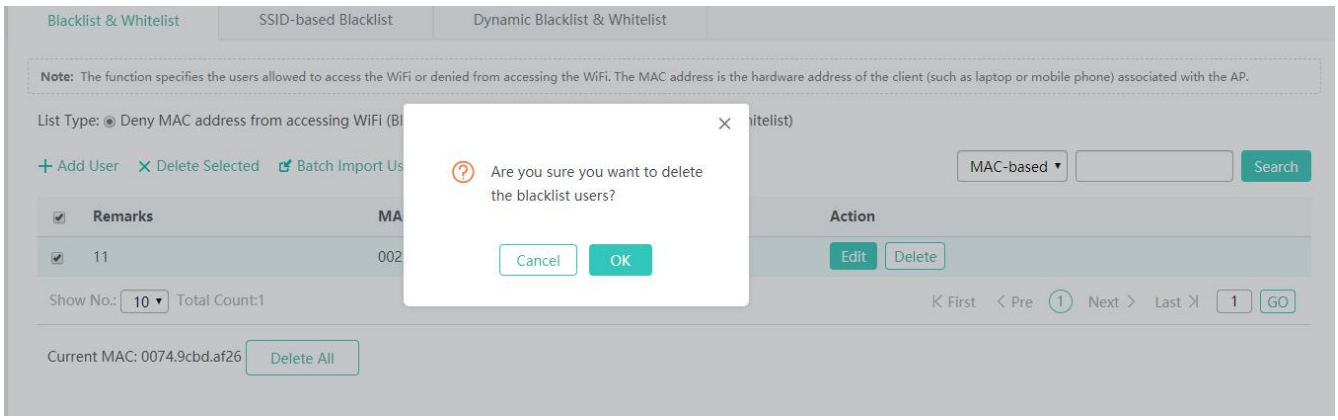
- Deleting a Blacklist User



- Deleting Blacklist Users in Batches

1. Select one or more records from the list.

2. Click **Delete Selected**.

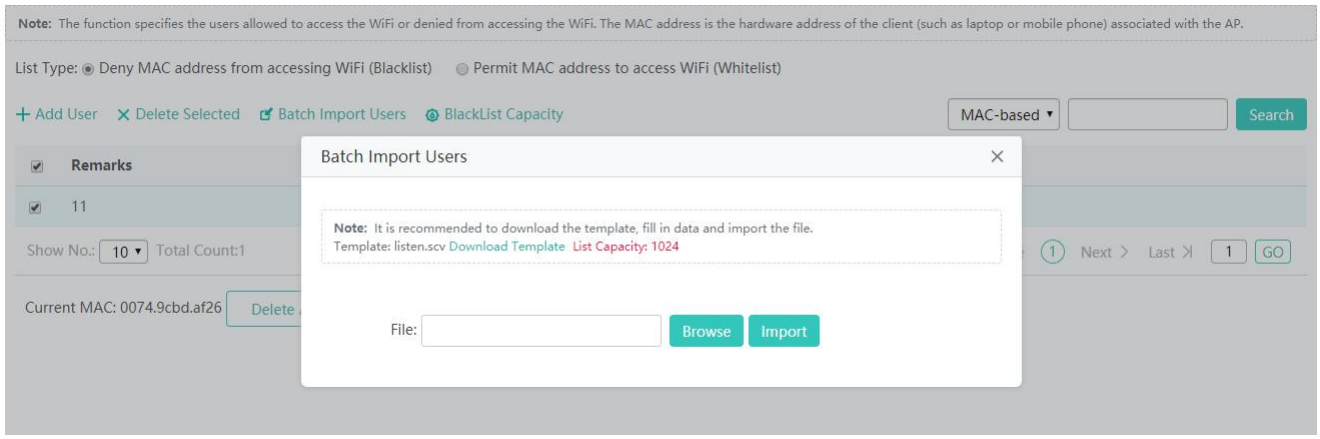


- Importing Blacklist Users

1. Click **Batch Import Users**.

2. Download the template file and enter the data.

3. Import the file.

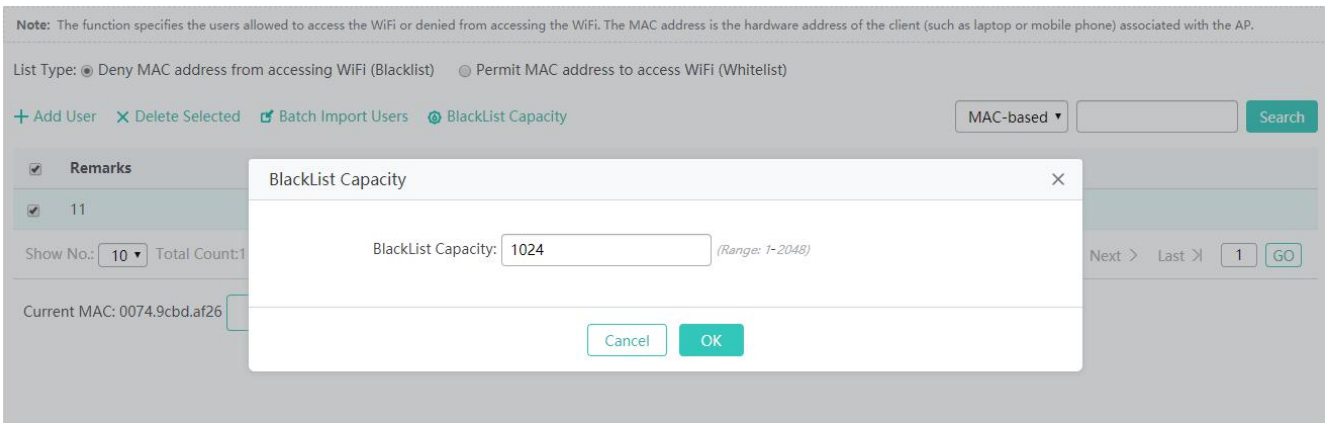


- Setting Blacklist Capacity

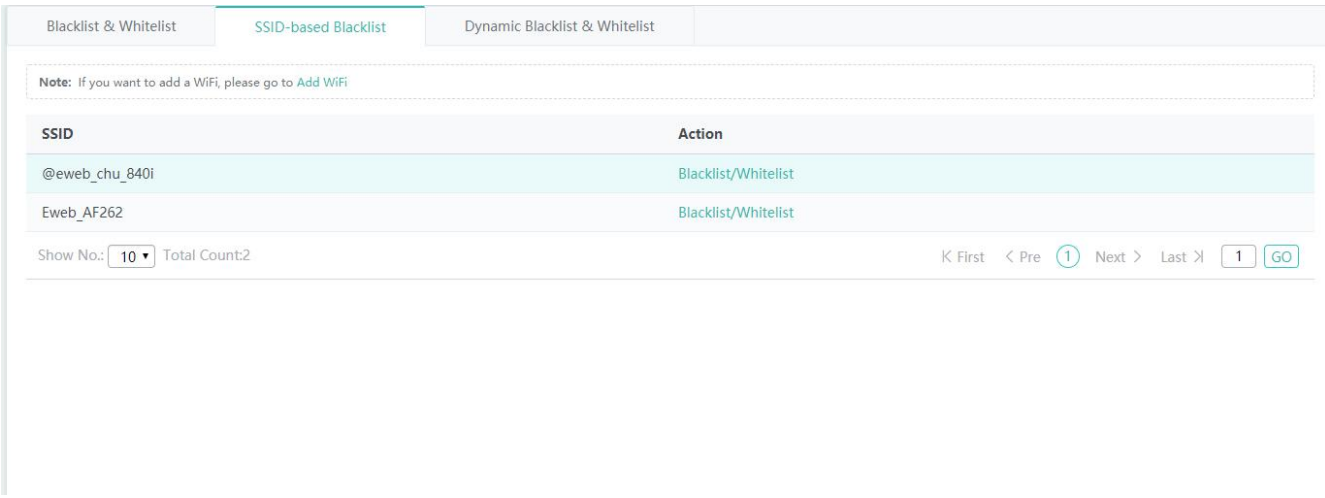
1. Click BlackList Capacity .

2. Enter a value.

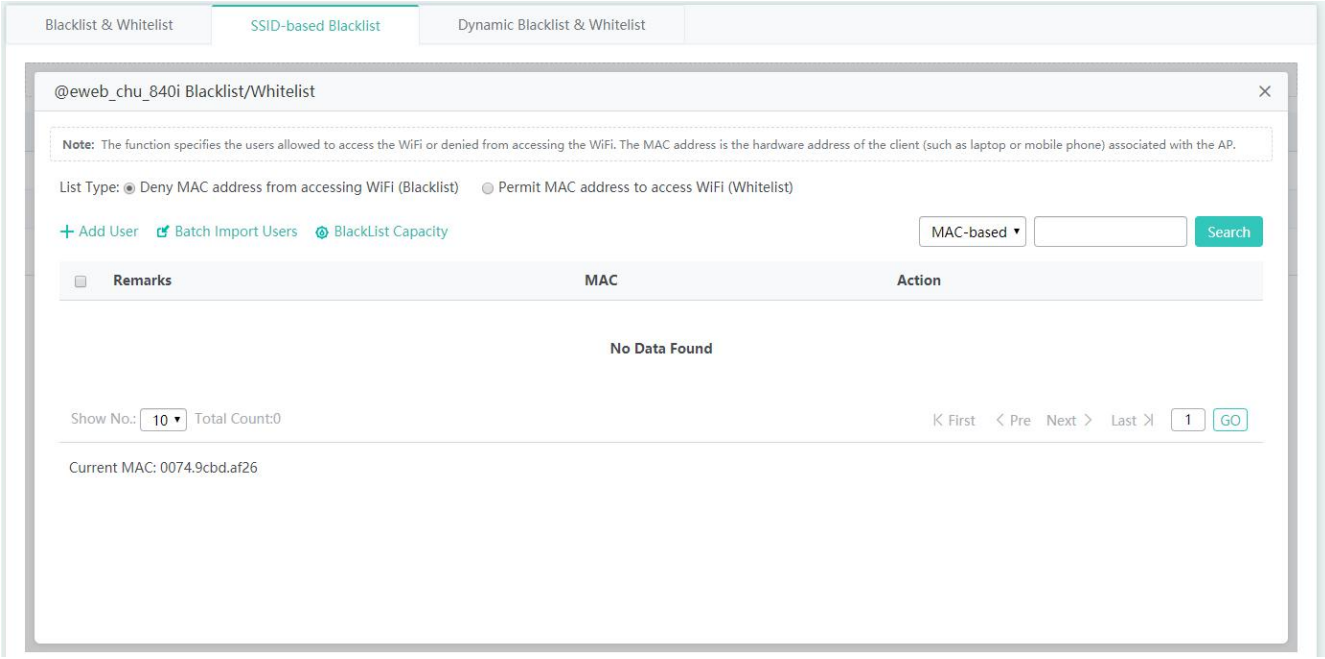
3. Click **OK**. The message "Configuration succeeded." will be displayed.



SSID-based Blacklist



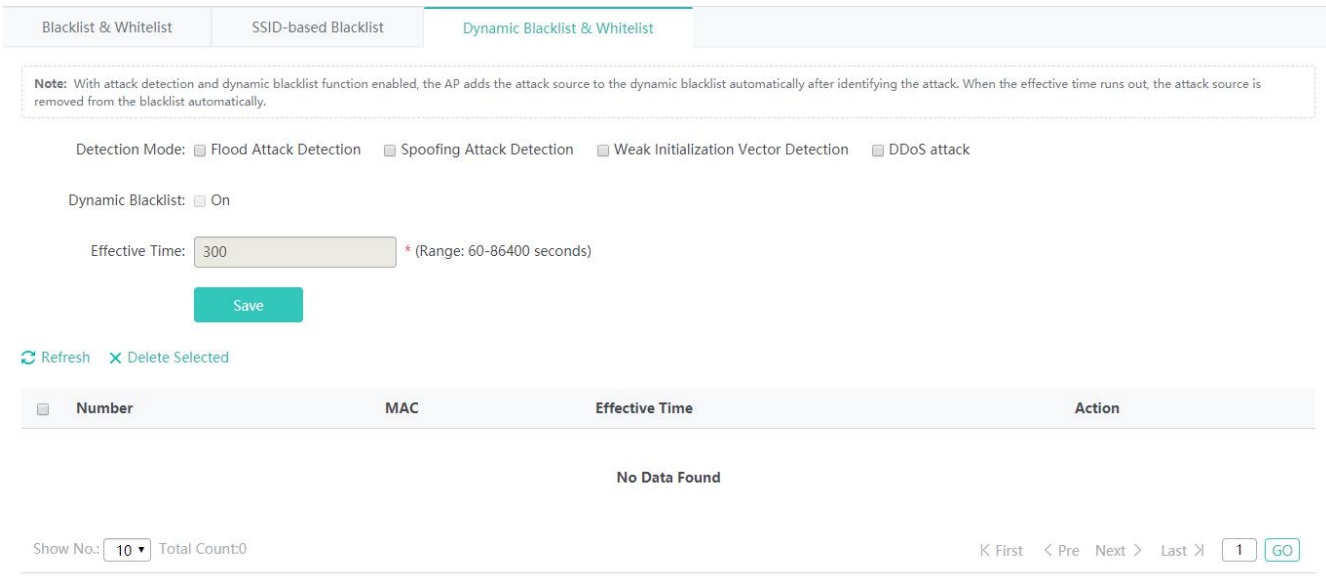
Click Blacklist/Whitelist in the list and configure the whitelist/blacklist for the specified SSID.

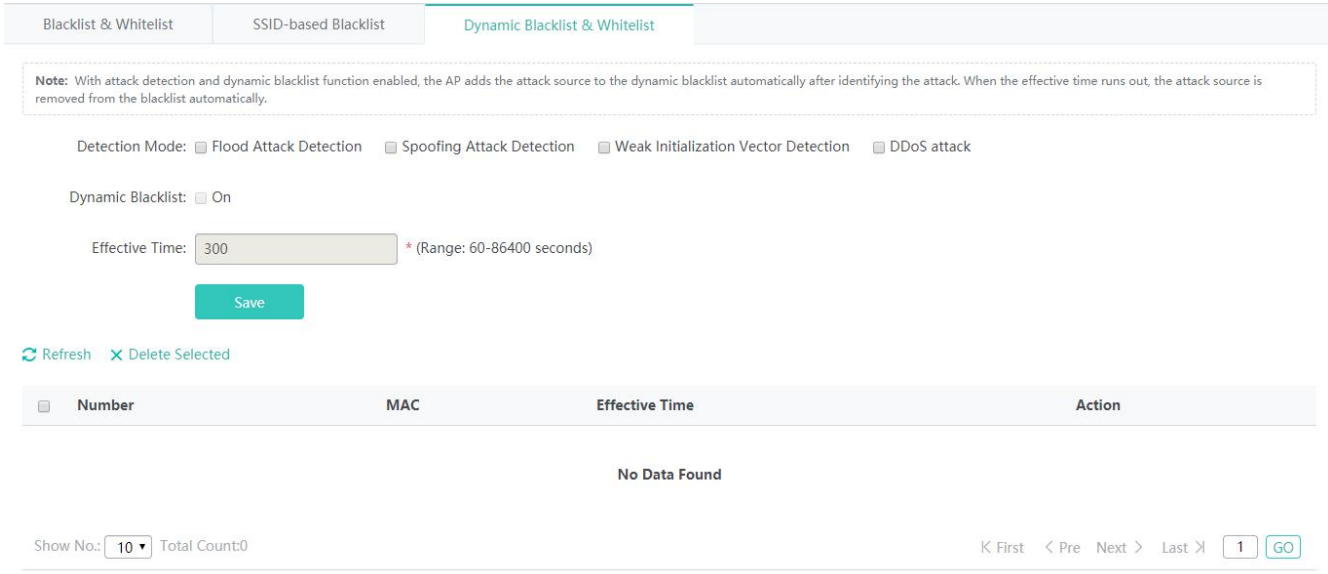


You can select the blacklist/whitelist type, add blacklist/whitelist users, import blacklist/whitelist users and set blacklist/whitelist capacity.

Dynamic Blacklist & Whitelist

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





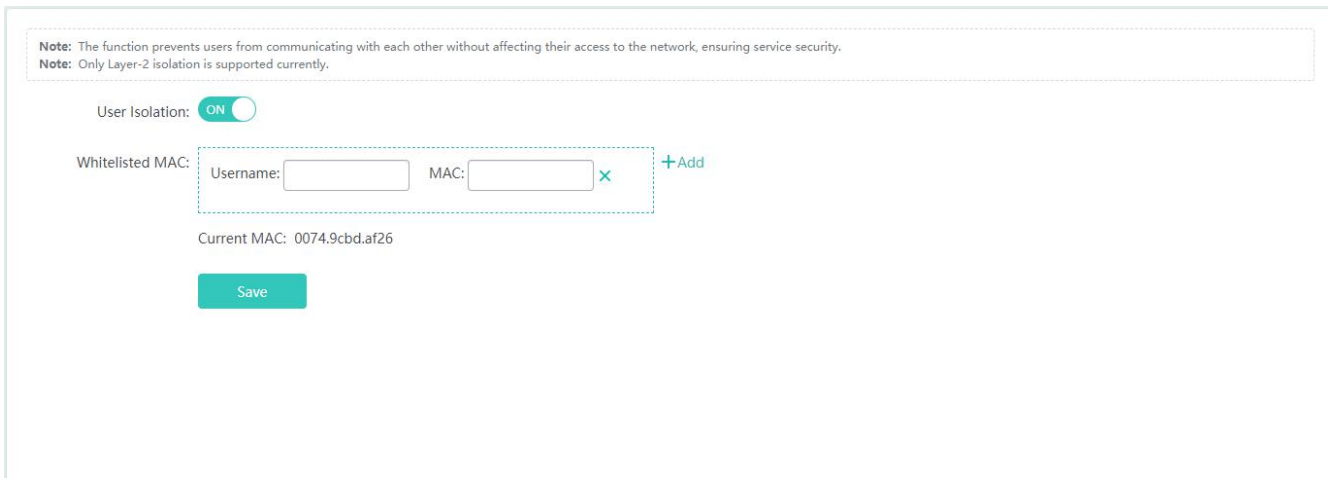
1) Set the parameters and then save the configuration.

2) Select the blacklist from the list.

3) Click **Delete Selected** and then click **OK** in the displayed dialog box to finish deleting.

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.



1) Click 

to enable or disable mutual access for internal network users.

2) Click  to delete the MAC address of the user.

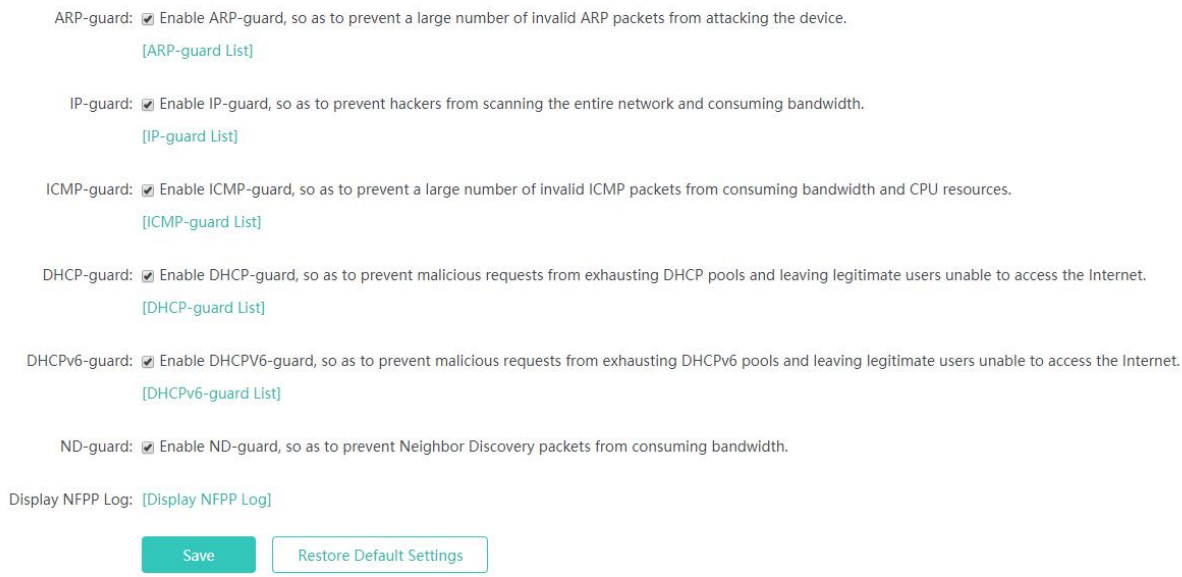
3) Click the **Add** icon to add a MAC address for a mutual-access user. You can add multiple MAC addresses.

4) Click **Save** to finish the configuration.

Anti-attack

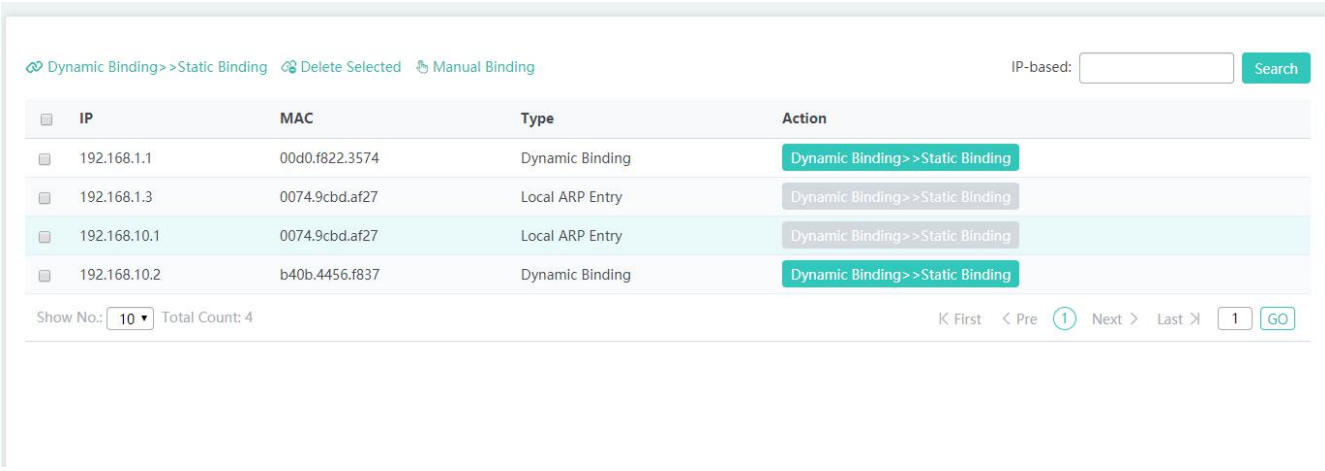
Some malicious attacks are always found in the network environment. These attacks may bring about an extremely heavy burden for the switch, resulting in the switch using an excessive amount of CPU power and giving rise to a potential operational failure.

NFPP

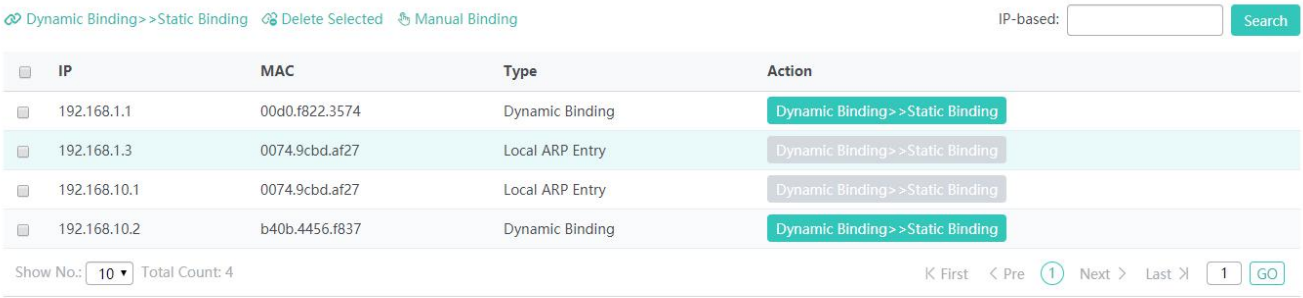


1) **ARP-guard**: Enables ARP-guard configuration. Click the **ARP-guard List** link to view the host where ARP attack is detected.
2) **IP-guard**: Enables IP-guard configuration. Click the **IP-guard List** link to view the host where IP scanning is detected.
3) **ICMP-guard**: Enables ICMP-guard configuration. 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.

ARP



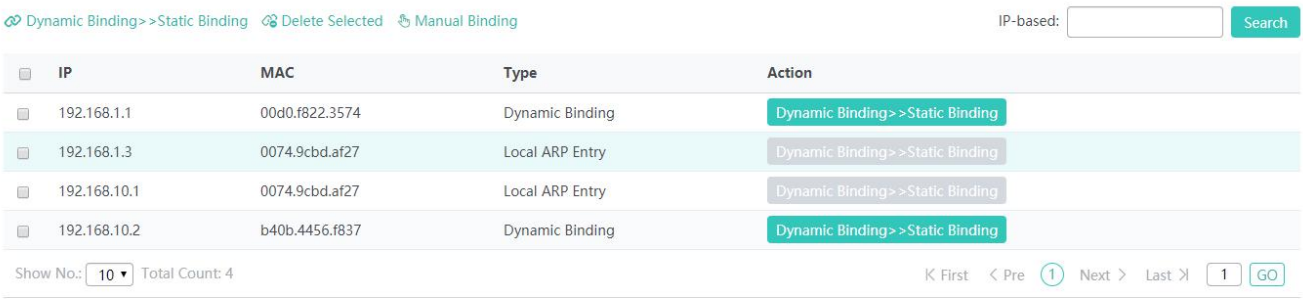
- Dynamic Binding>>Static Binding



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.

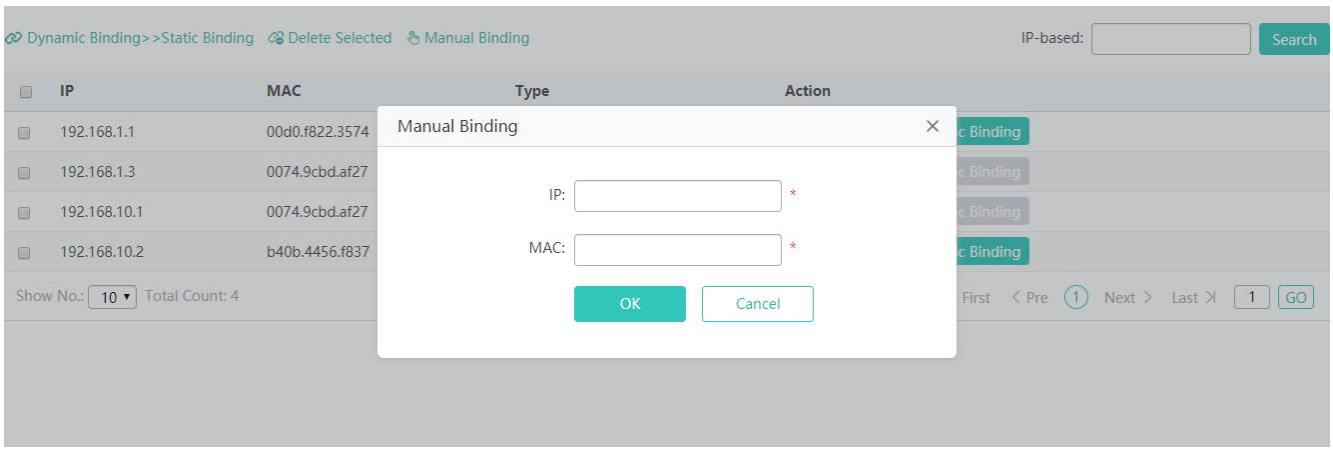
- Remove Static Binding



1) Select one or multiple records from the ARP list.

2) Click the **Remove Static Binding** icon to remove static binding in batches.

- Manual Binding



1) Click the **Manual Binding** icon.

2) Set the IP address and MAC address.

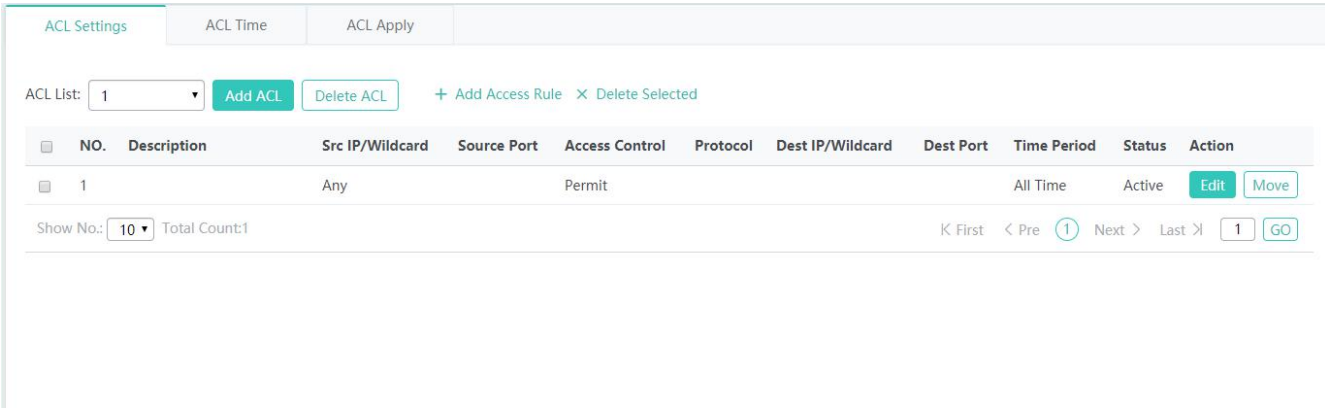
Click **OK**. The newly bound ARP is displayed in the ARP list after the **Save operation succeeded** message is displayed.

ACL

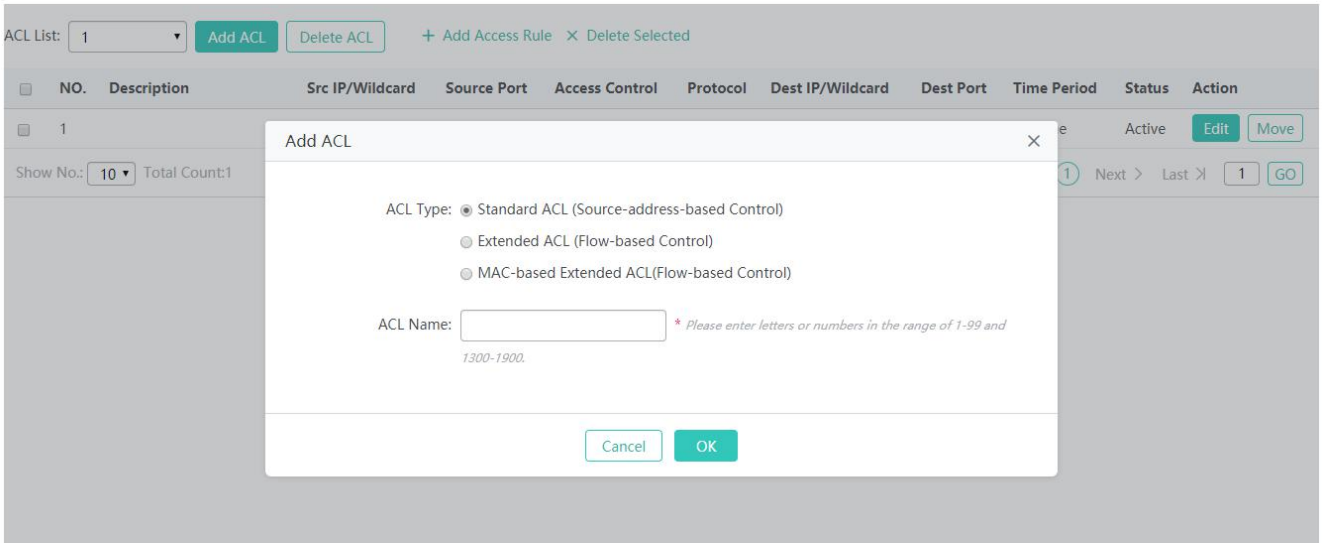
When receiving a packet on a port, the input ACL checks whether the packet matches the ACE entry for this port. When the device intends to output a packet through a port, the output ACL checks whether the packet matches the ACE entry for this port.

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

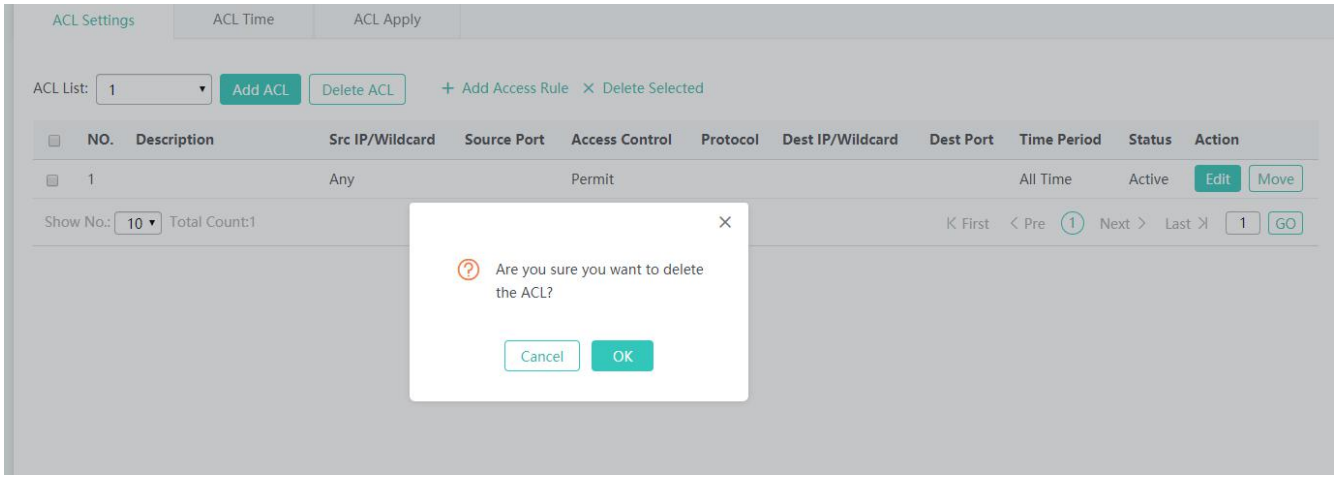


- Adding an ACL



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.

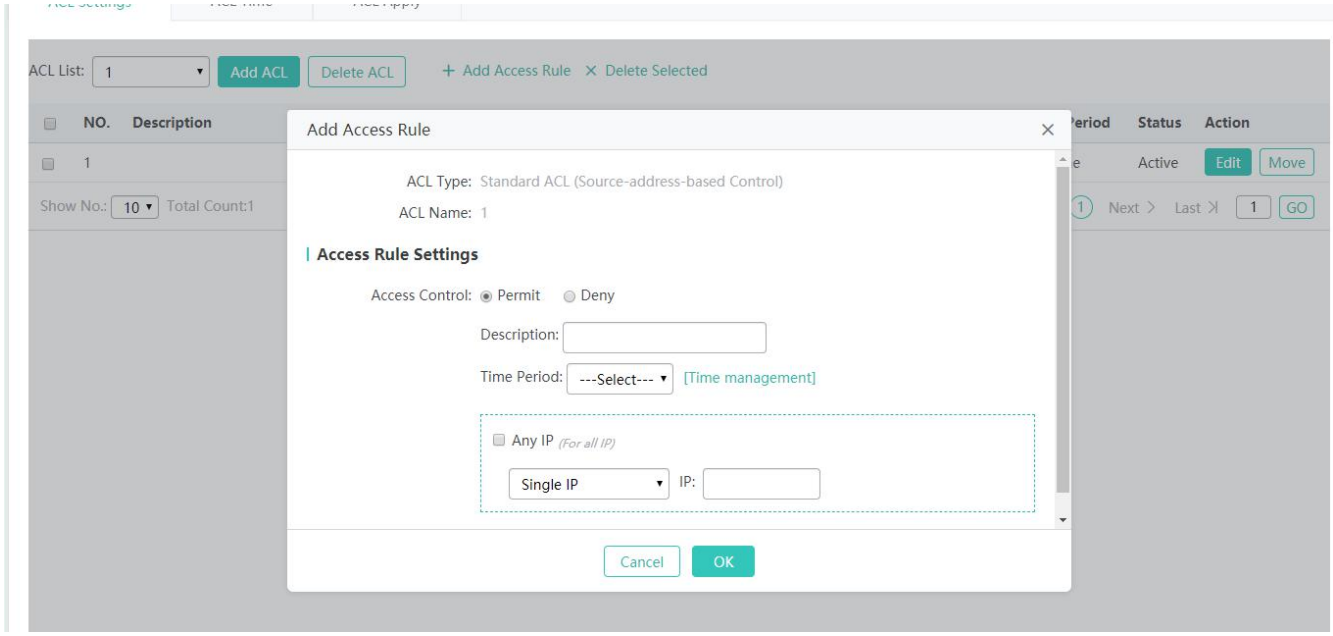
- Deleting an ACL



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.

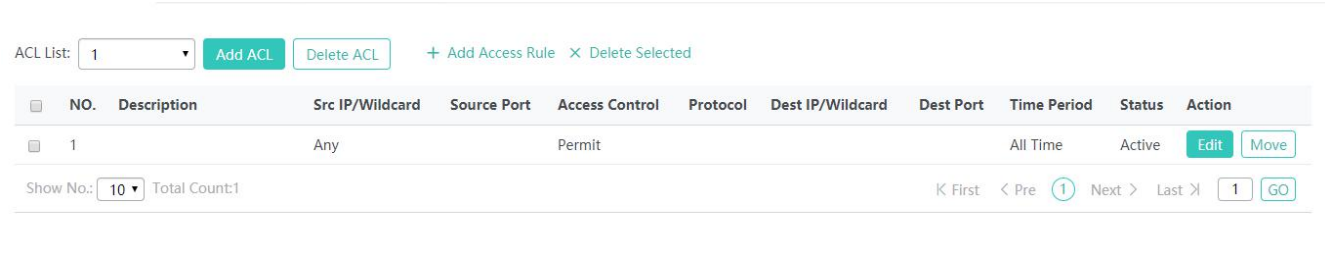
- Editing an Access Rule

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

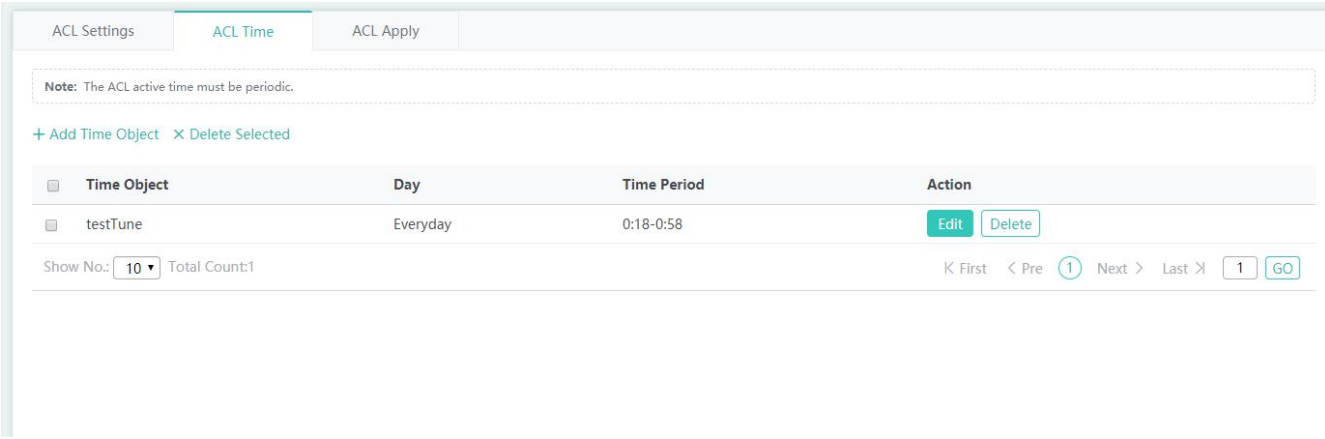


1) Select one or multiple records from the access rule list.

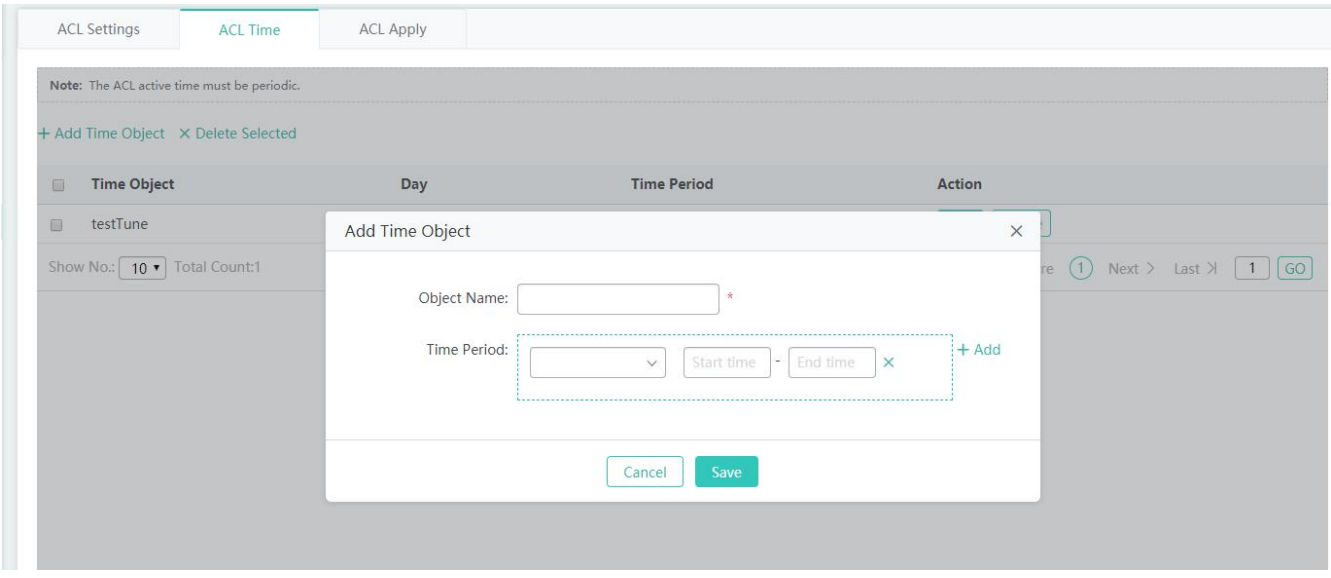
Click **Delete Selected** and then click **OK** in the displayed dialog box to finish deleting ACL Time

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

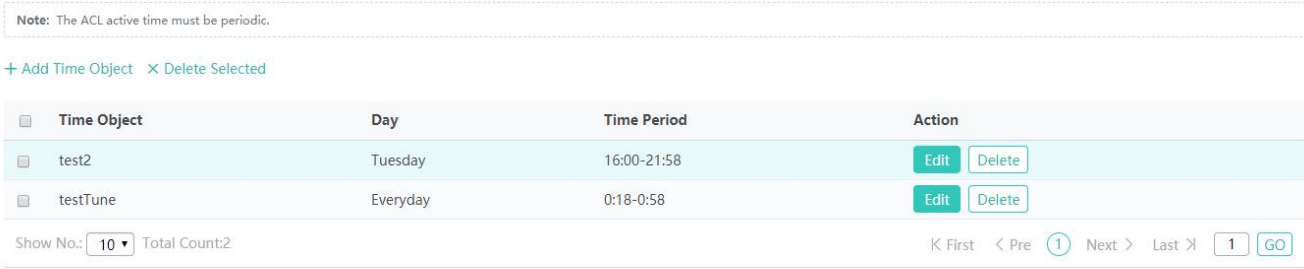


- Adding a Time Object



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.

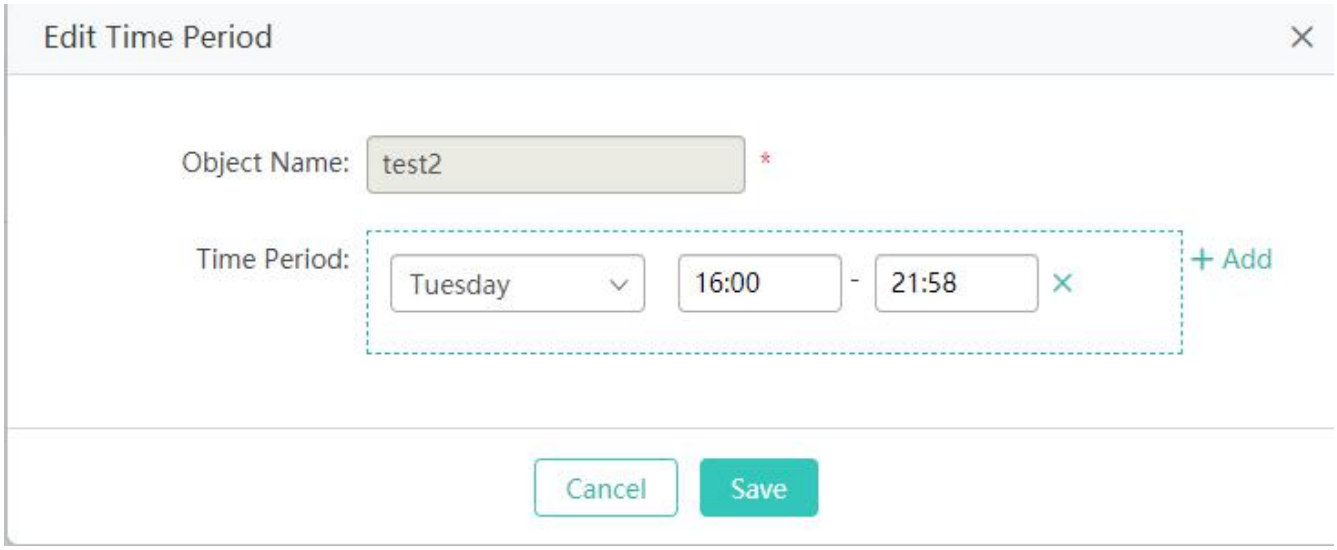
- Deleting Time Objects in Batches



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

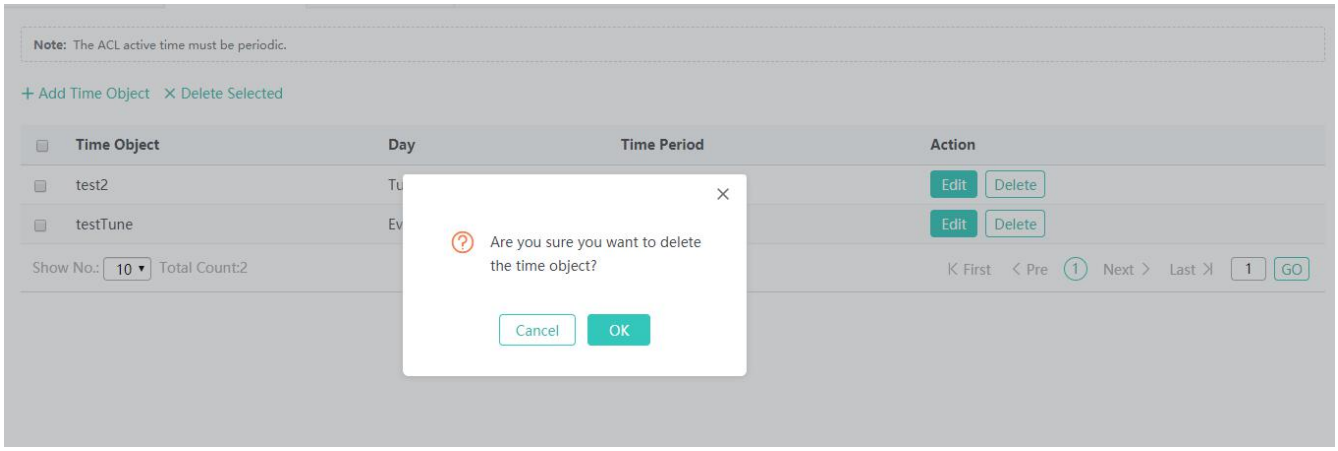


1) Click the **Edit** button for a time object in the list.

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.

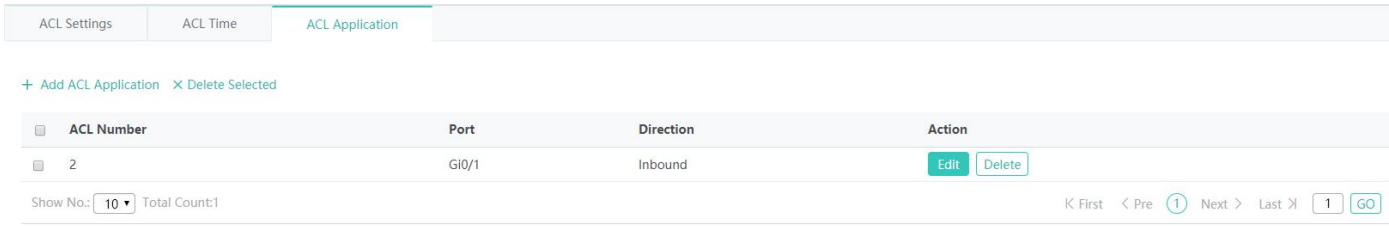
- Deleting a Time Object



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.

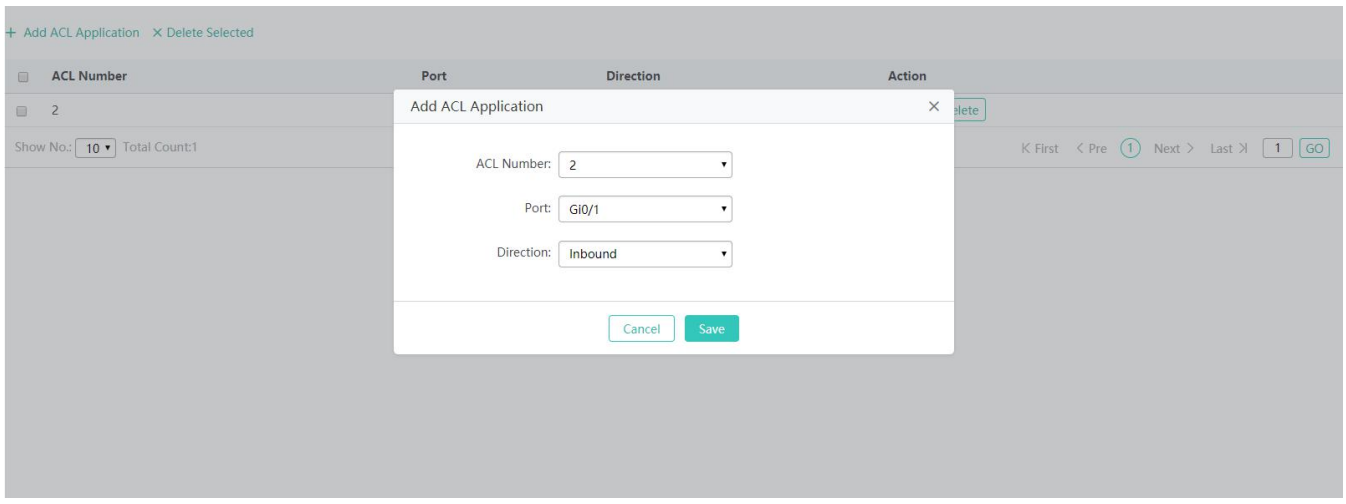


- Adding an ACL Application

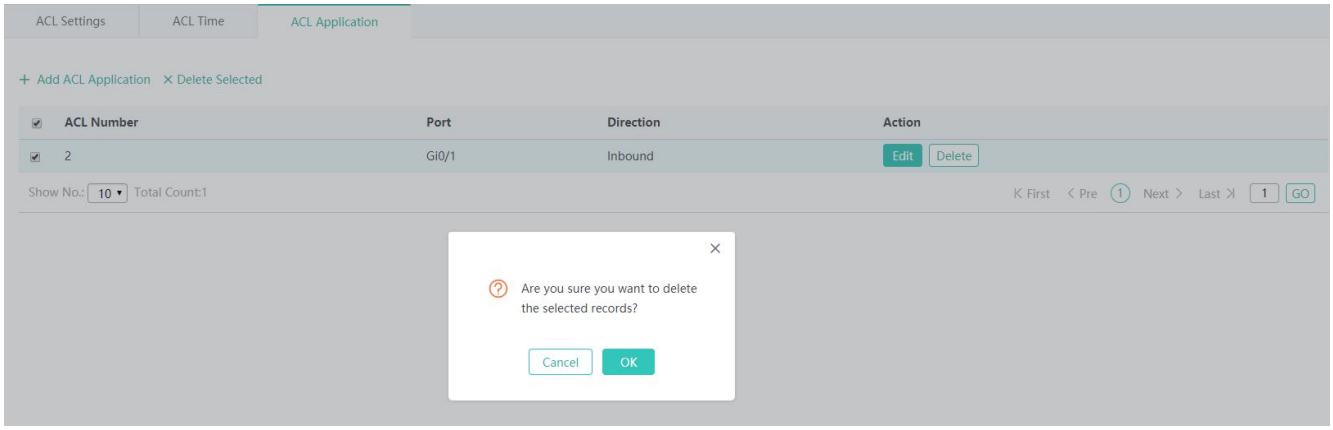
1. Click + Add ACL Application .

2. Select ACL number, port and direction in the popup window.

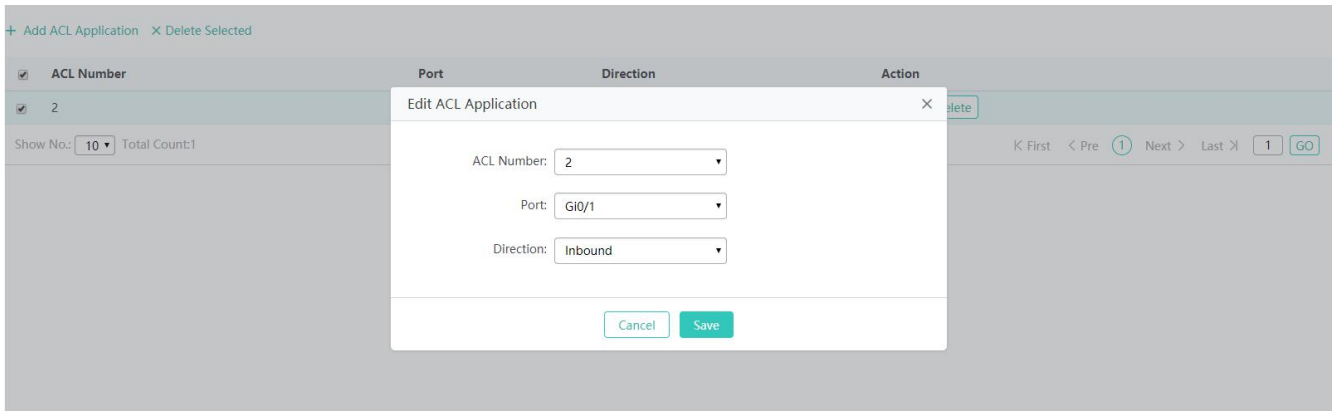
3. Click **Save**. After the message "Configuration succeeded." is displayed, the ACL will appear in the list.



- Deleting Selected ACL Applications



- Editing an ACL Application



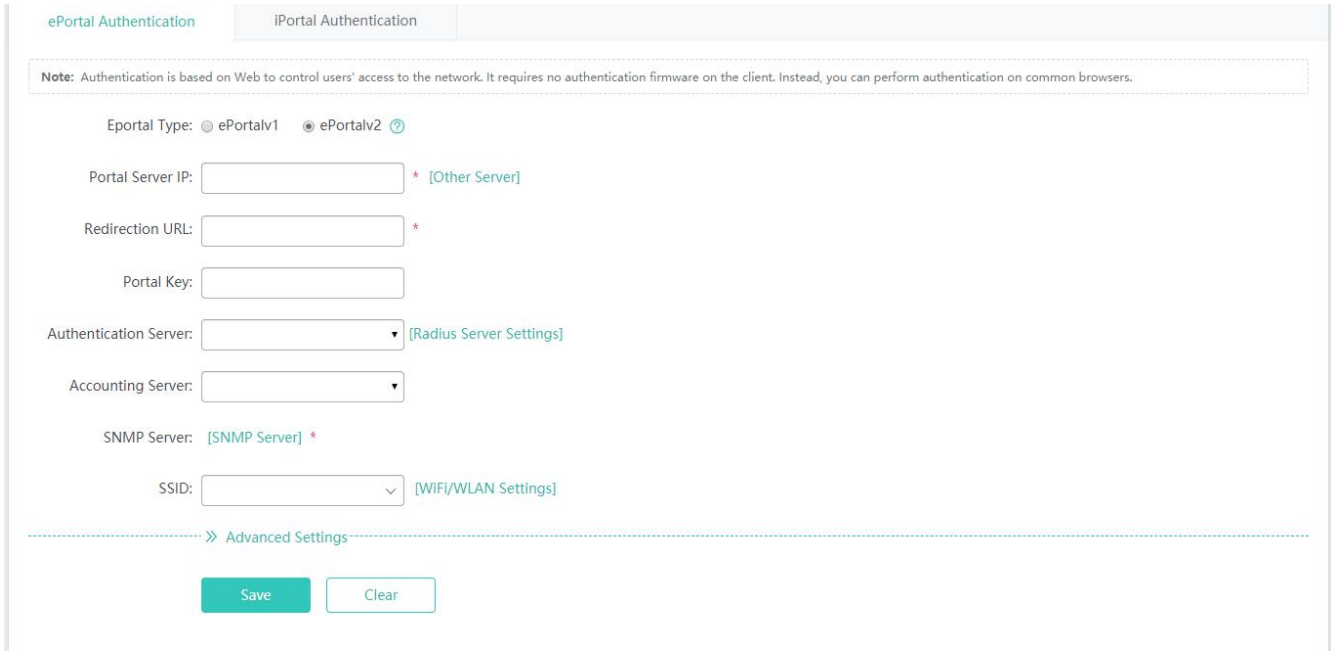
Authentication

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.

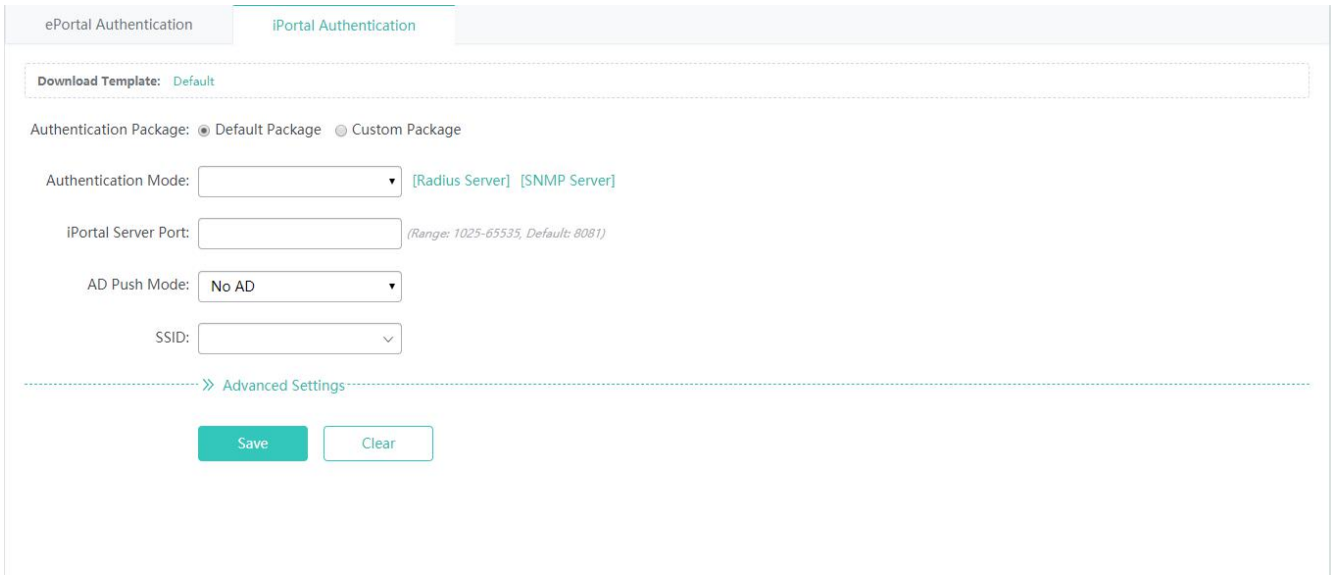
ePortal Authentication

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



iPortal Authentication

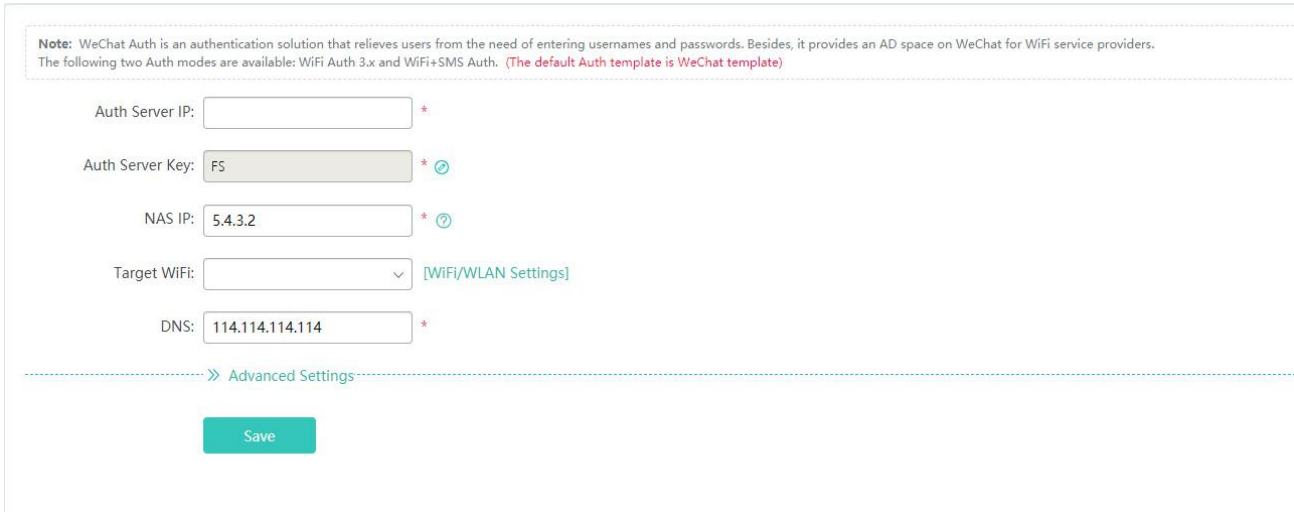
Unauthenticated users will be redirected to the specified website for authentication. If the Portal is built into the AC, please select iPortal authentication.



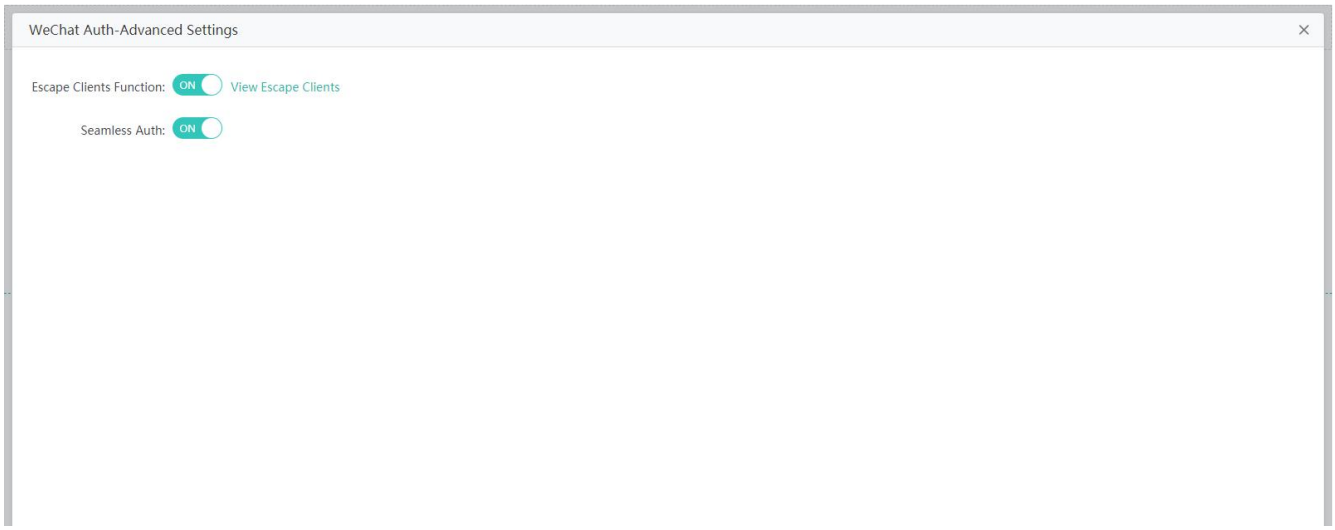
WeChat Authentication

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.

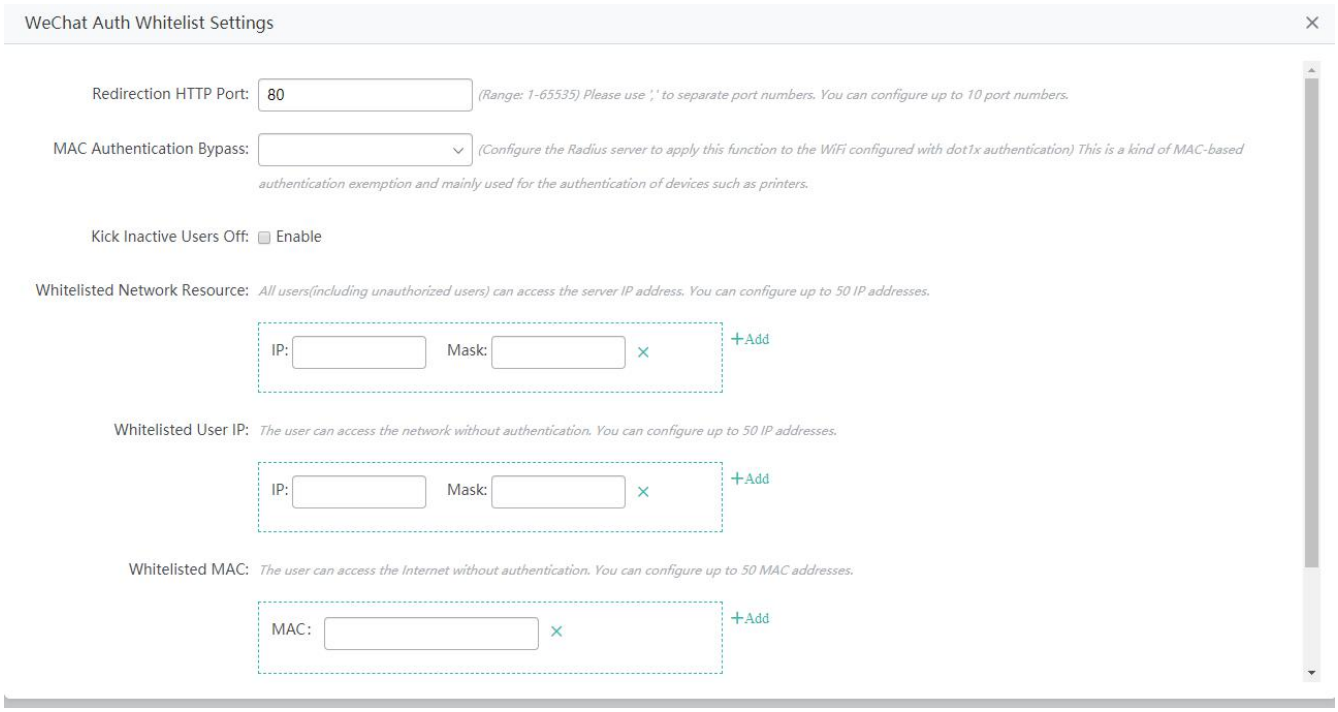
The following two authentication modes are available: WiFi Auth 3.x and WiFi+SMS Auth. (The default is the WeChat template)



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

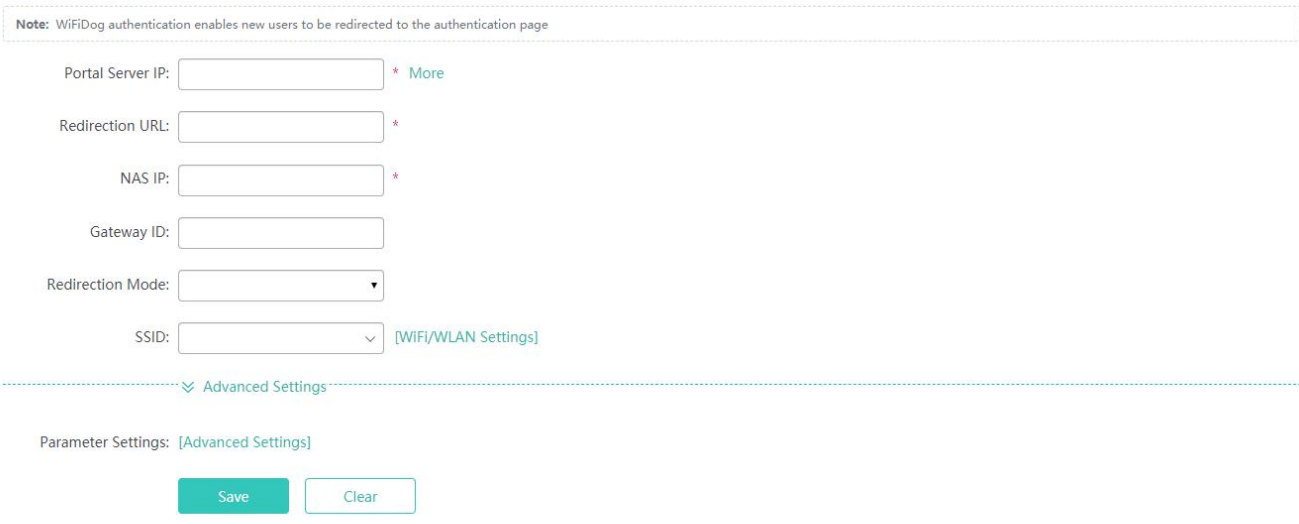


Choose **Advanced Settings** > **Parameter Settings** > **Whitelist Settings**.



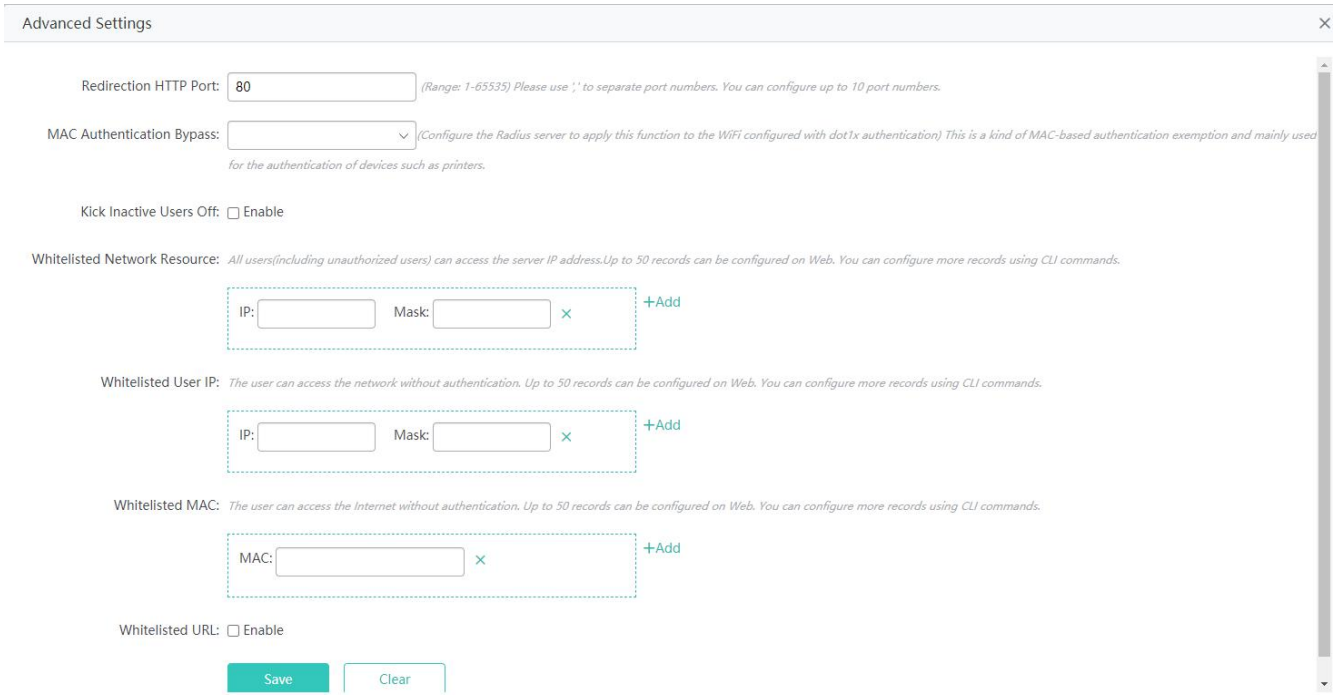
WiFiDog Authentication

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



Advanced Settings

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



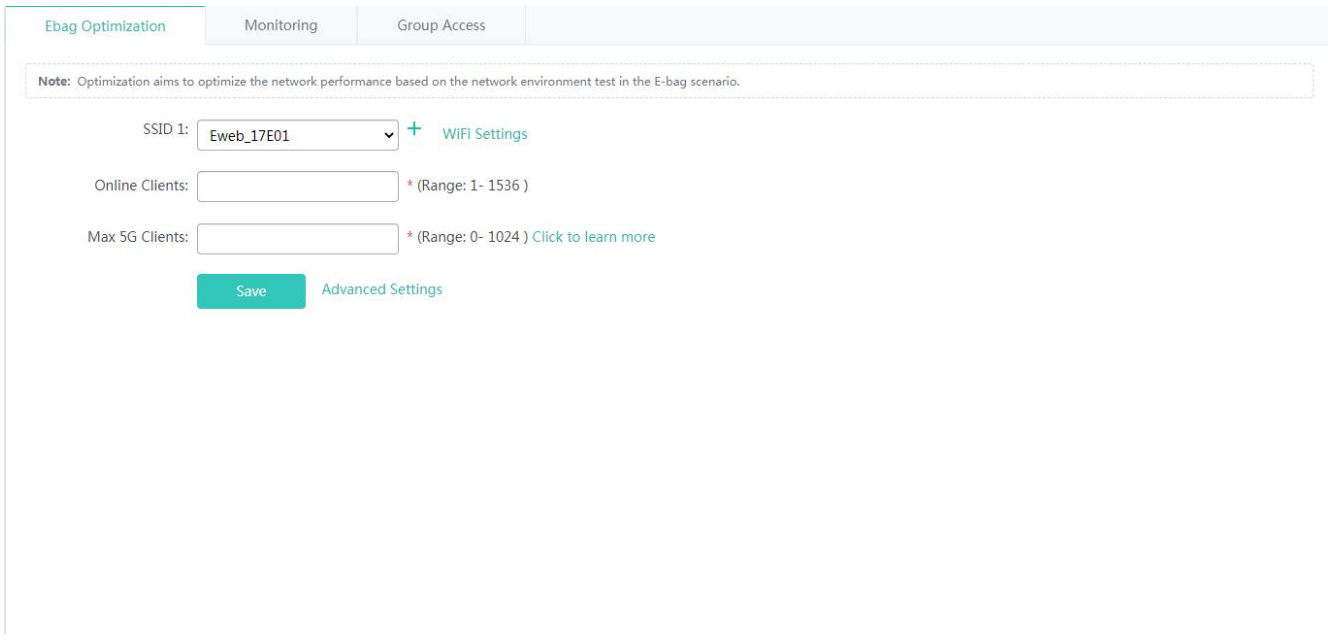
Advanced

E-bag Optimization

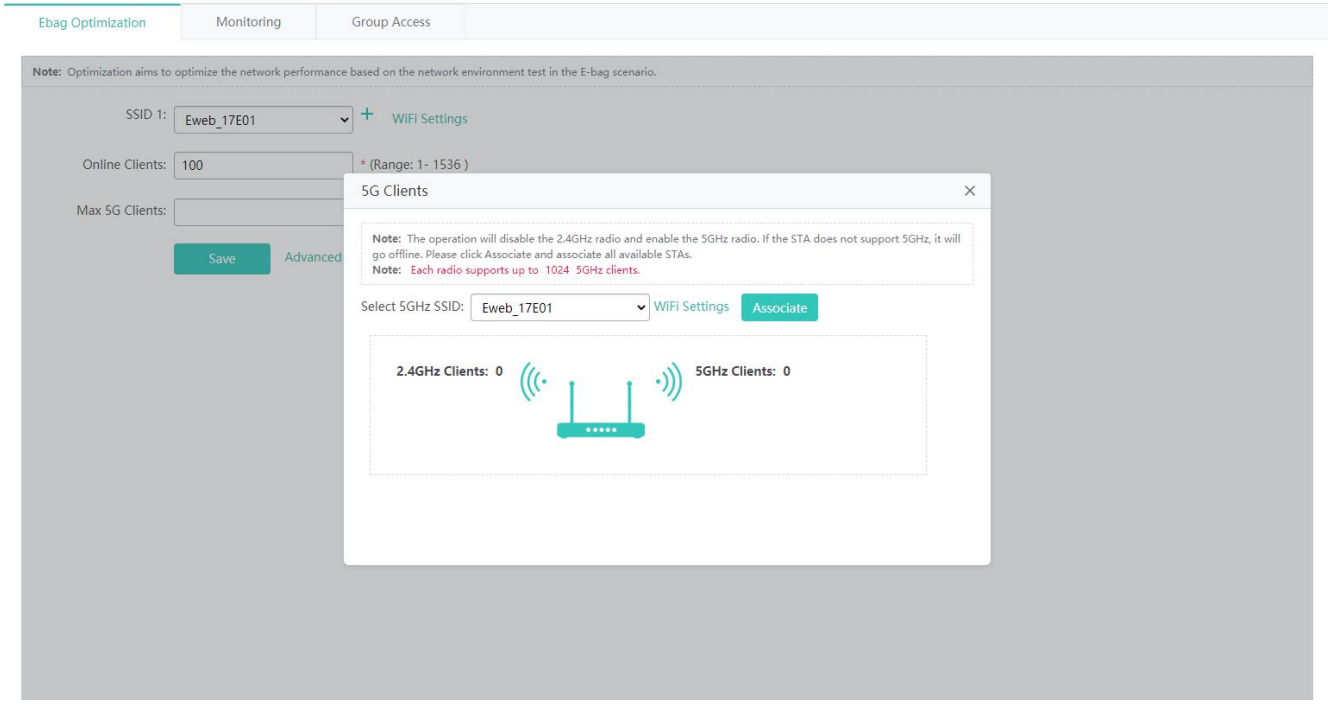
Your AP might not support this function. The menu may vary with the device.

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.

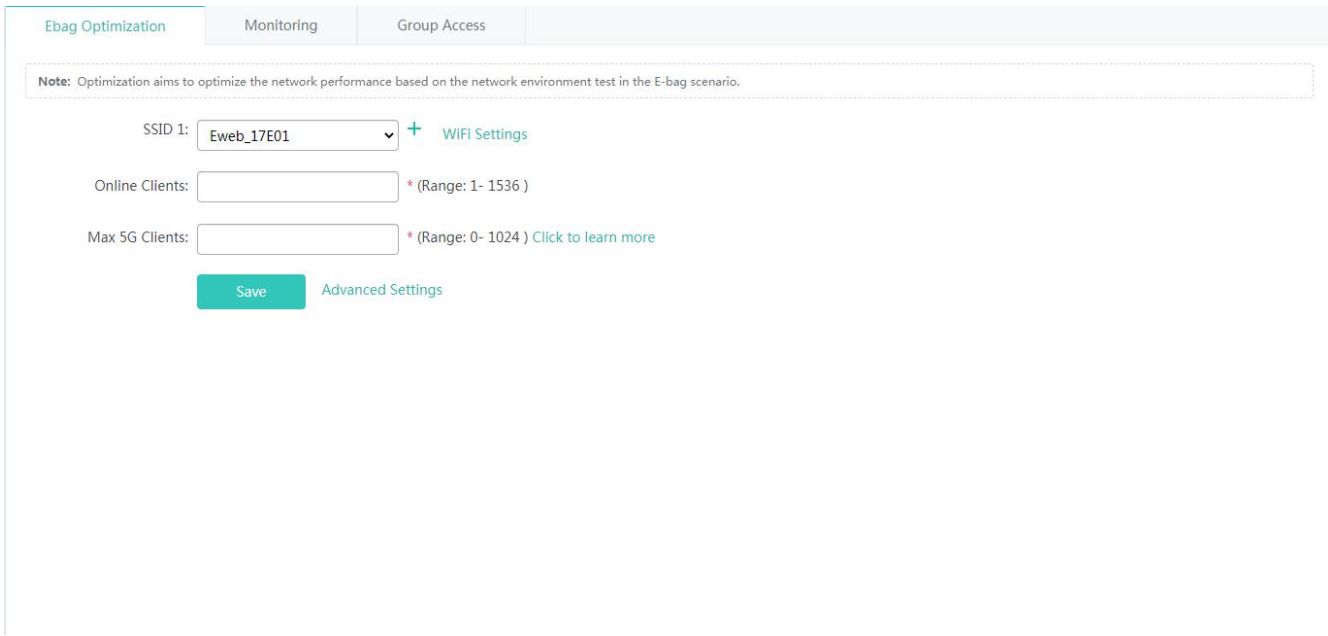
E-bag Optimization



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.

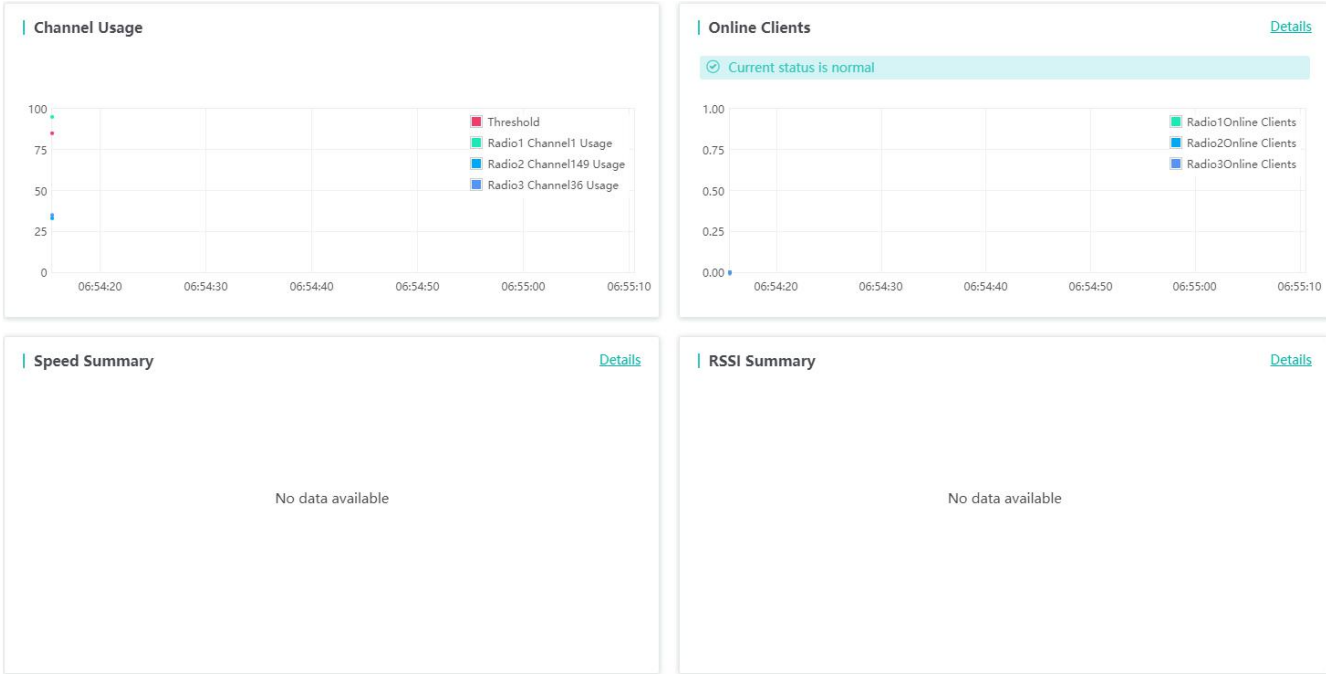


Enter the maximum number of 5G clients here, and click **Save**. E-bag optimization settings will take effect.

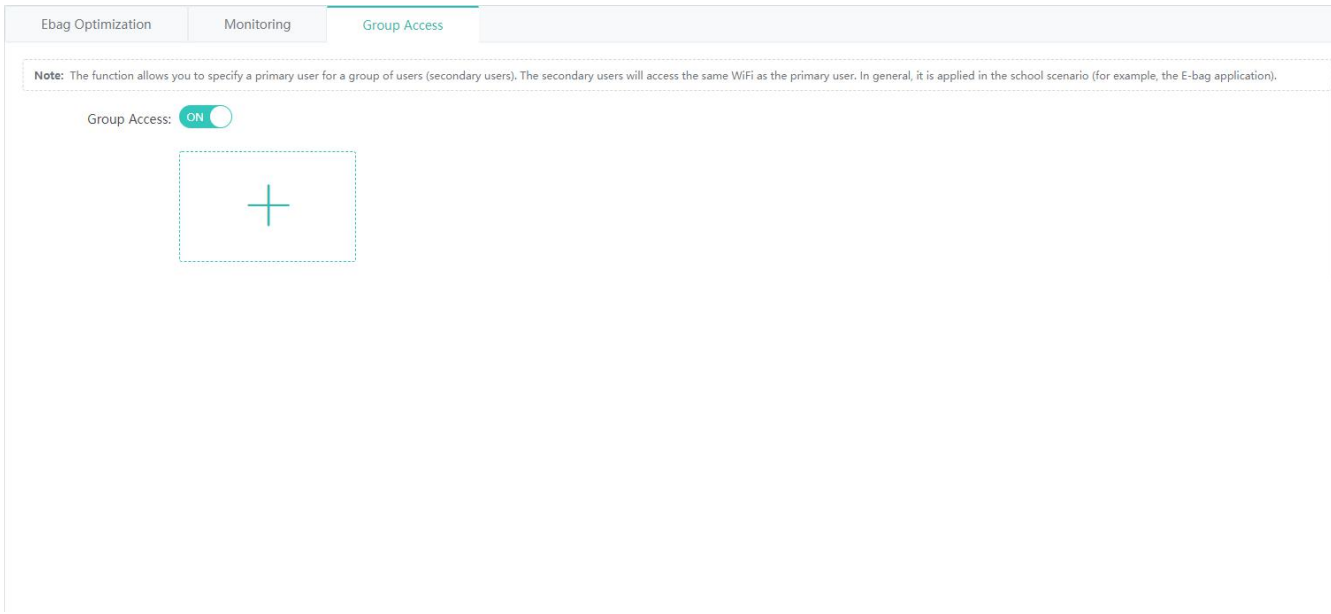
You can click **Advanced Settings** to configure advanced settings. If you perform E-bag optimization again, the advanced settings will be overriden.

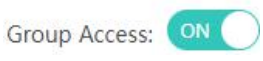
Monitoring

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



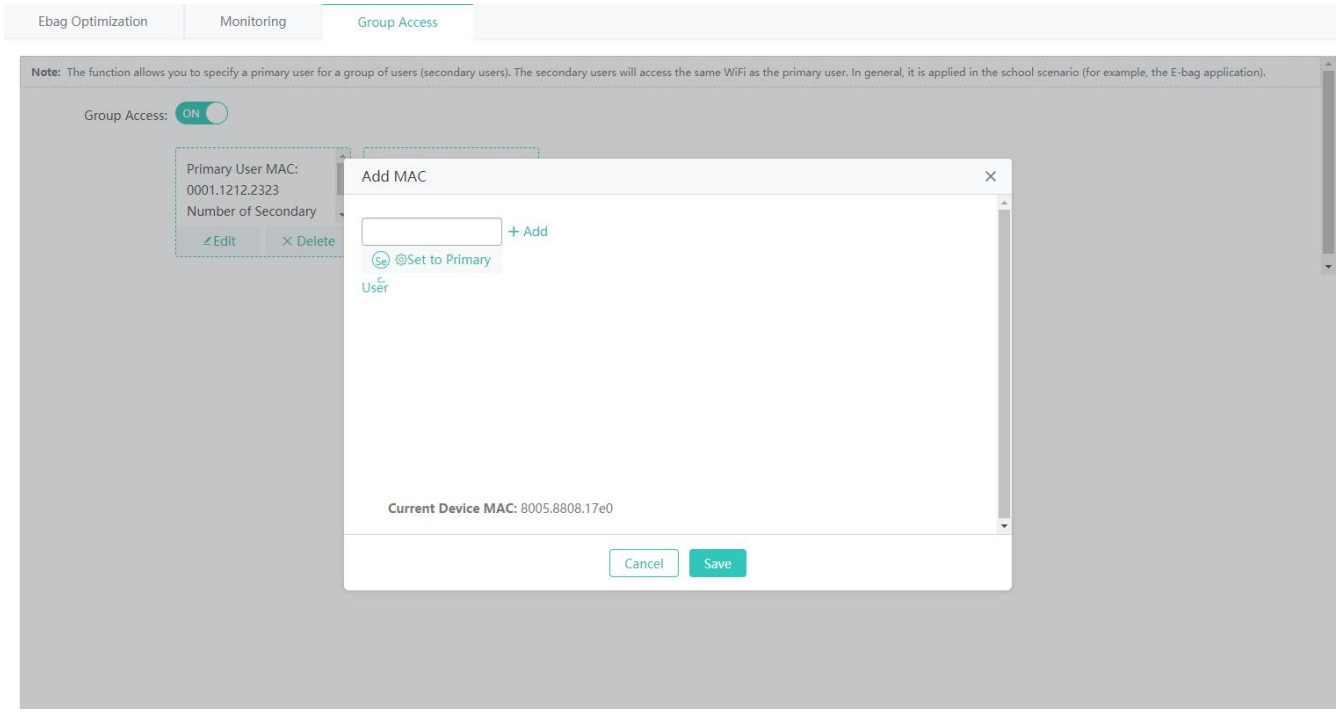
Group Access



Toggle the 

button to enable or disable the Group Access function.

- Adding a User Group

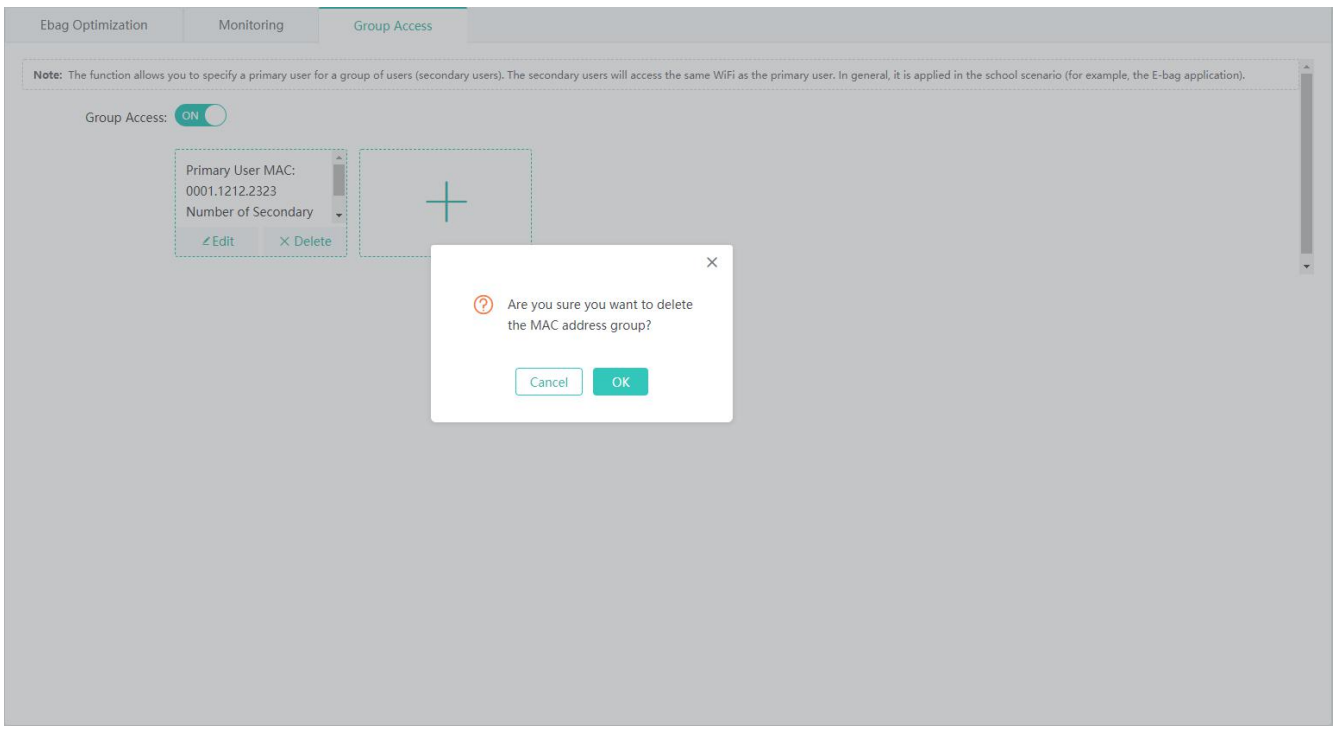


1. Click +.

2. On the **Add MAC** page, enter a MAC address.

3. Click **Save**, and the "Add succeeded." message appears.

- Deleting a User Group

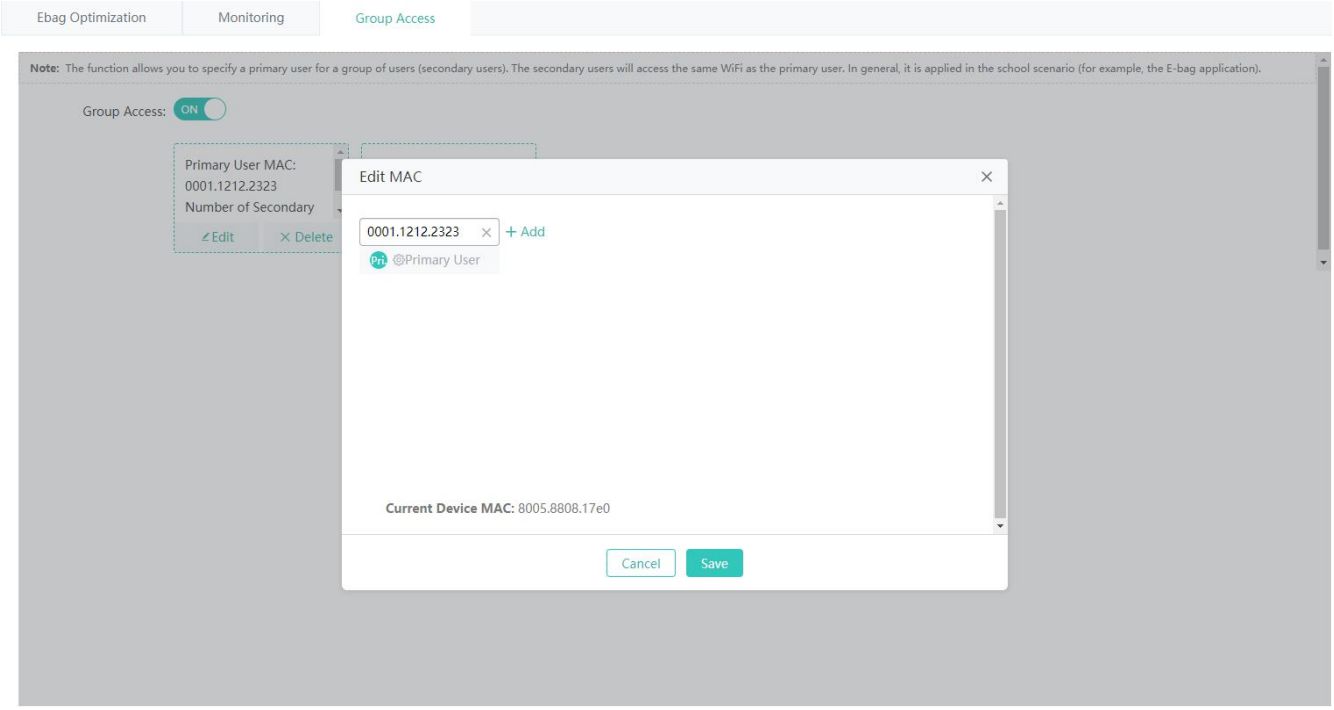


1. Click **Delete**.

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**.

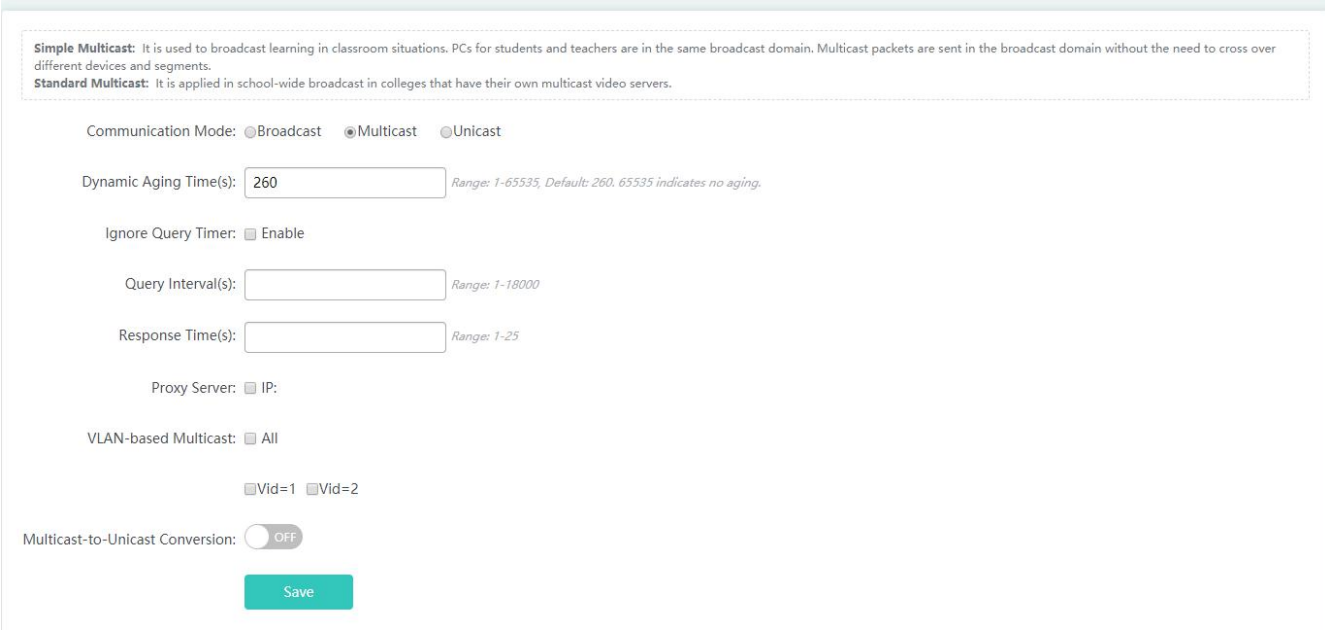
2. On the **Edit MAC** page, edit the MAC address.

3. Click **Save**, and the "Edit succeeded." message appears.

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.

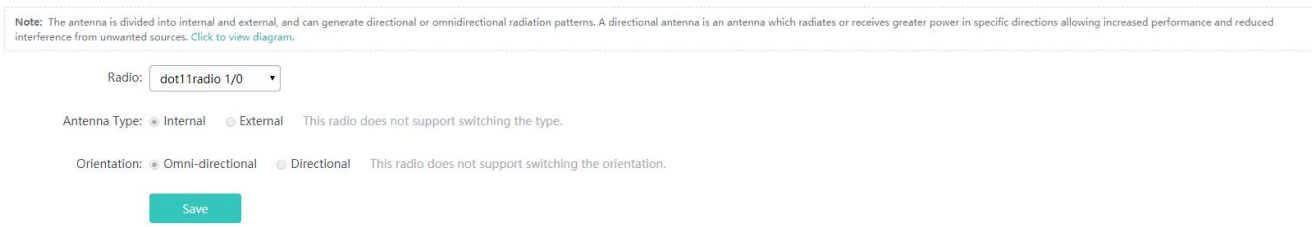
Multicast is group communication where information is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.



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

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.

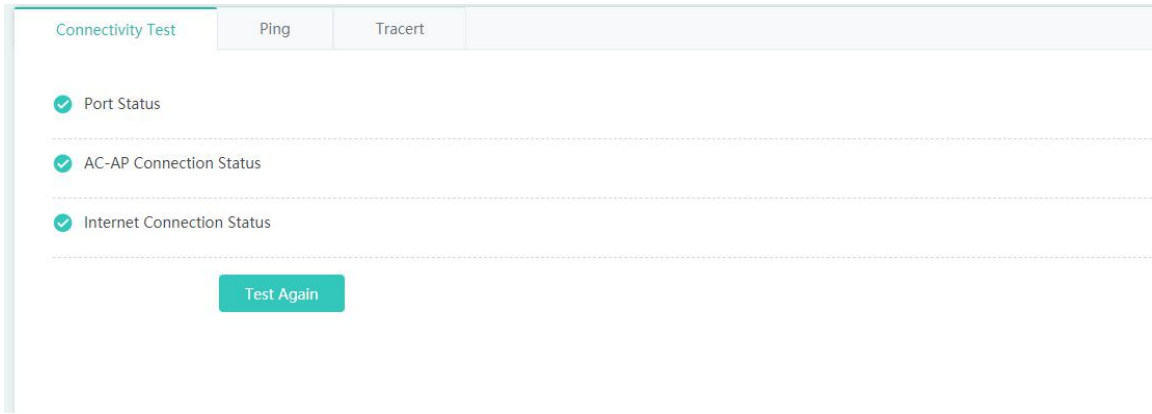


1.3.4 Diagnosis

Network Diagnosis

Connectivity Test

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



Port Status

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

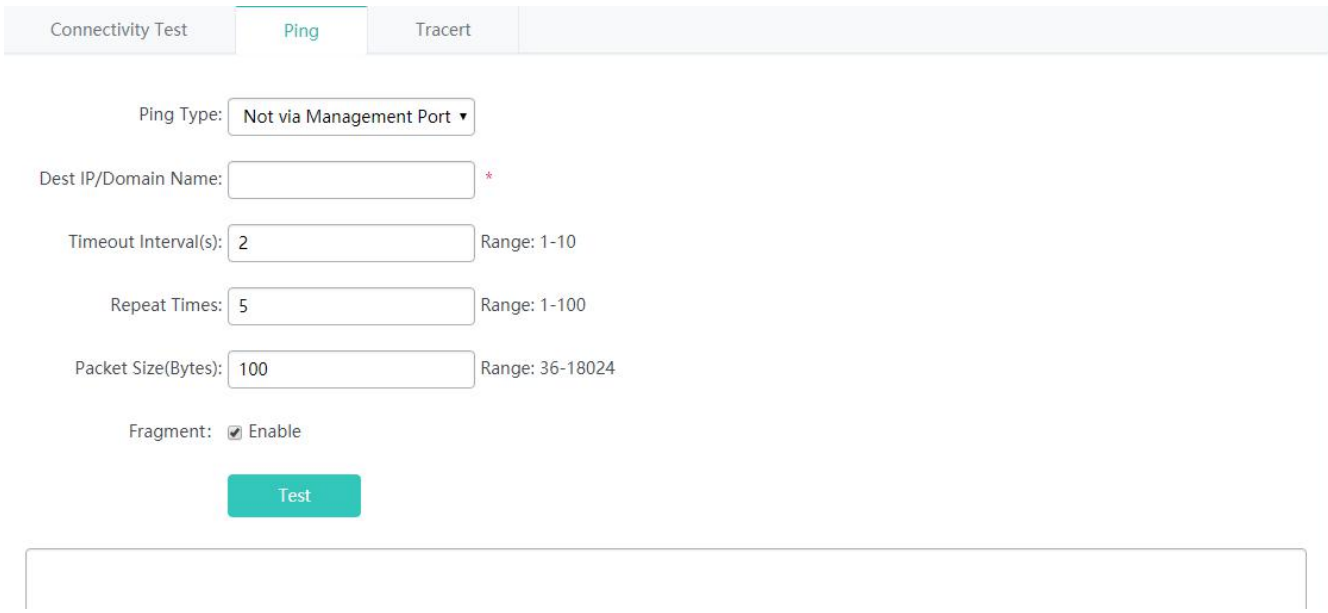
AC-AP Connection Status

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



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.

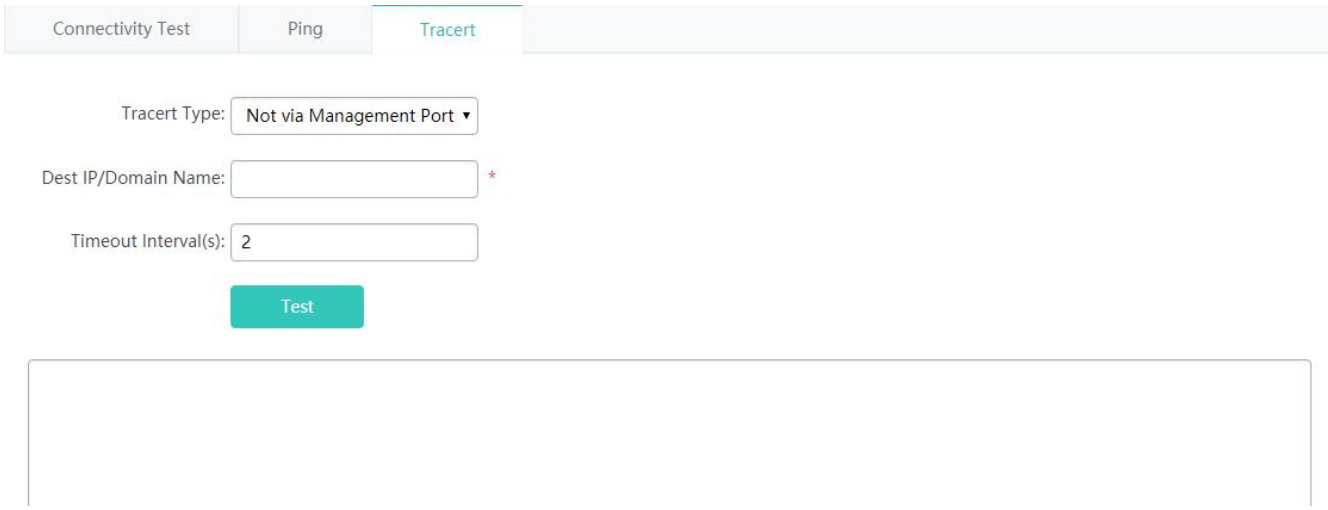
Packet Size (Bytes)

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



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.

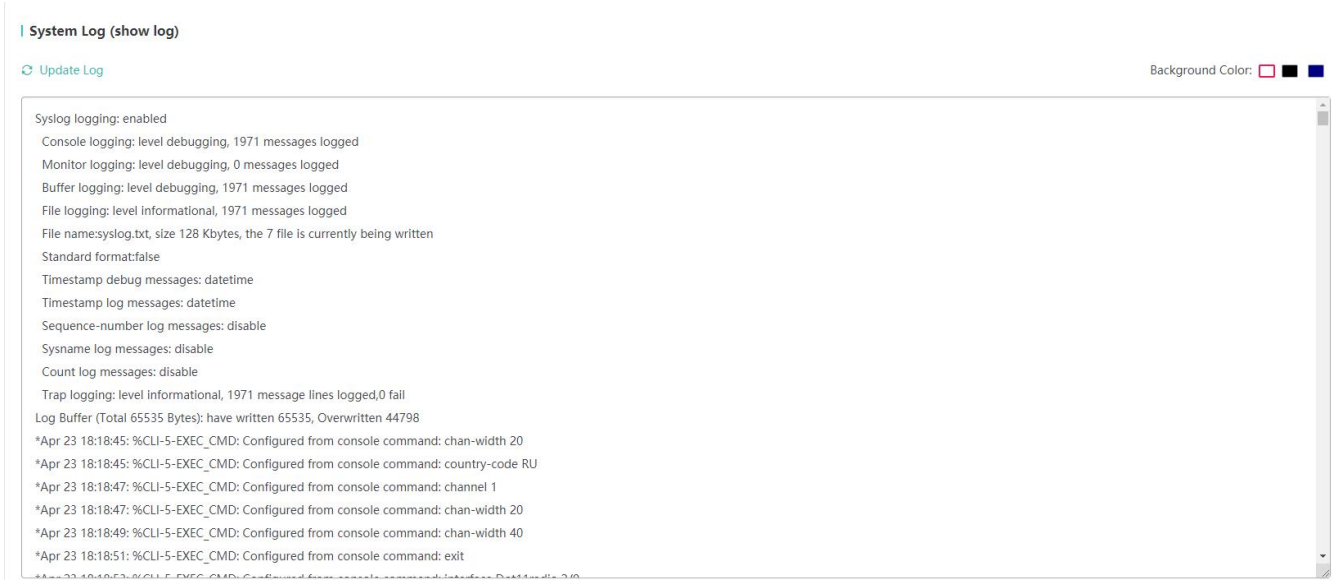
Timeout Interval(s)

Indicates the timeout interval.

One-Click Collection

Syslog

Syslog helps technical support to locate problems.



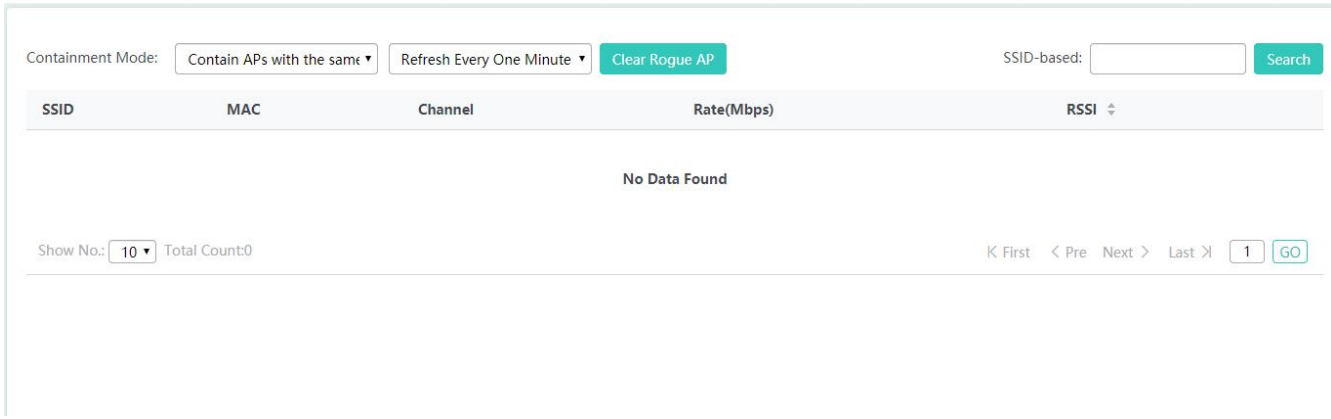
WIDS

Rogue AP

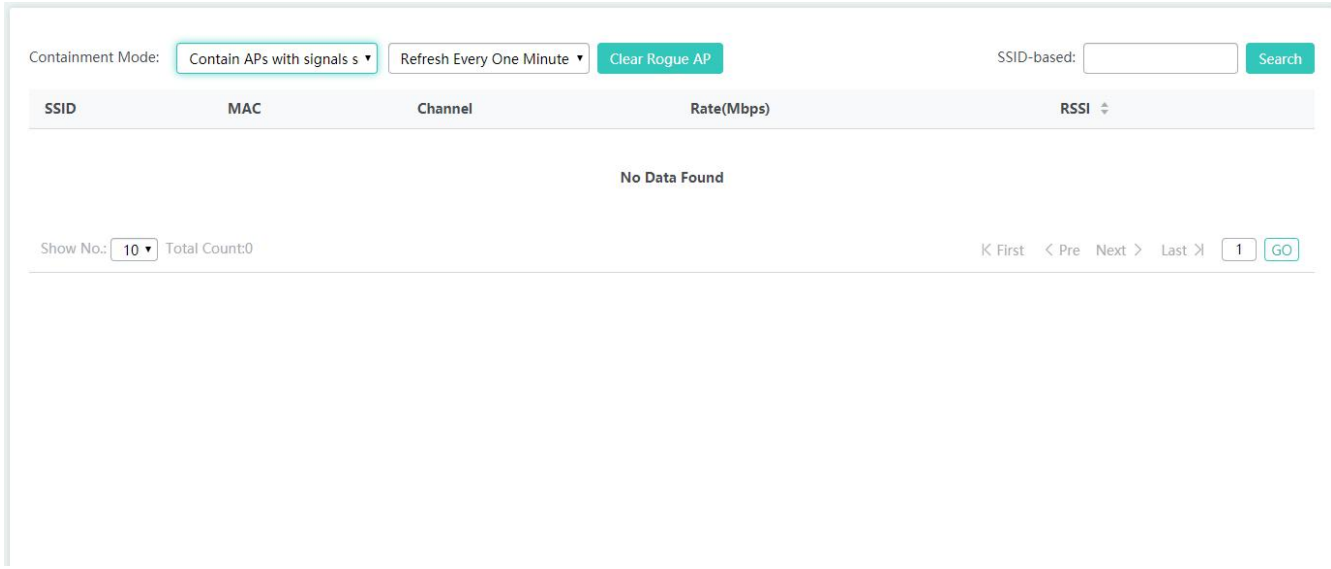
Rogue APs pose threat to the network security.

The following containment modes are available.

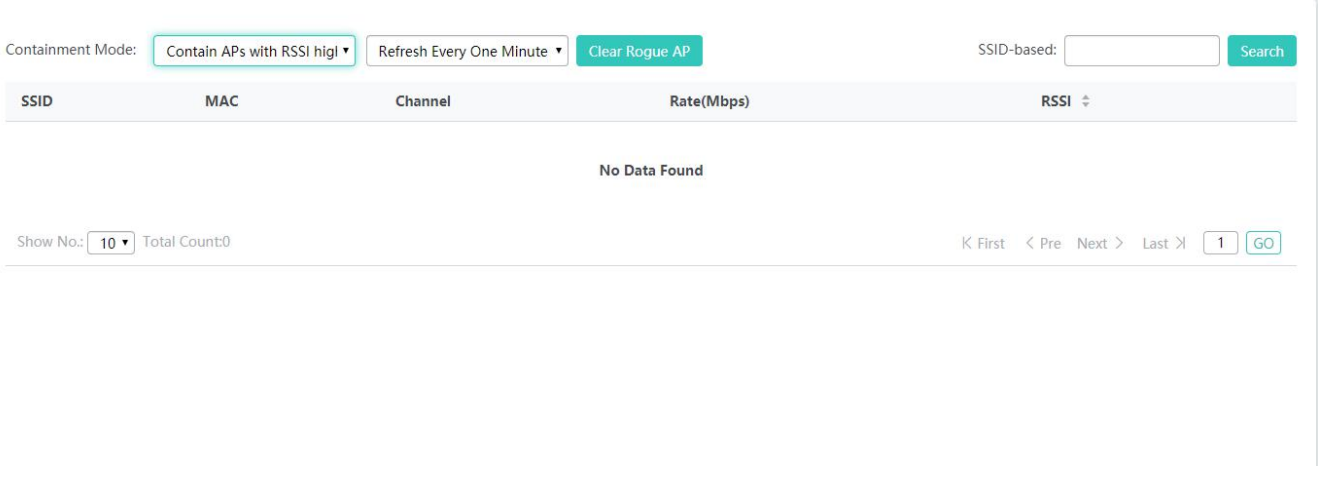
SSID mode: Contain APs emitting the same WiFi signals as the local AP.



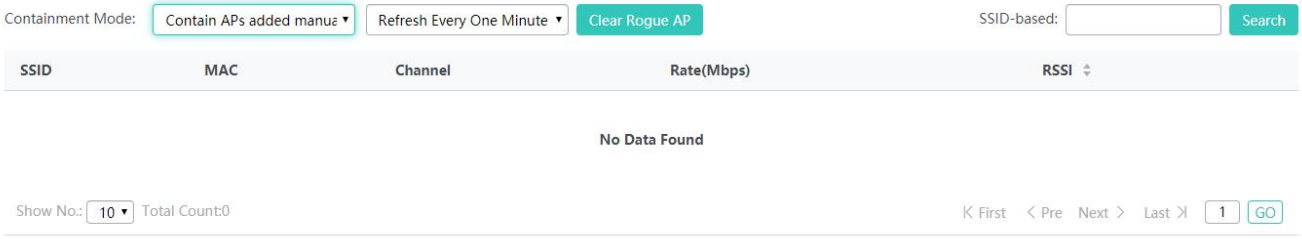
AdHoc mode: Contain AdHoc devices simulating the same WiFi signals.



Rogue mode: Contain APs according to RSSI.



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



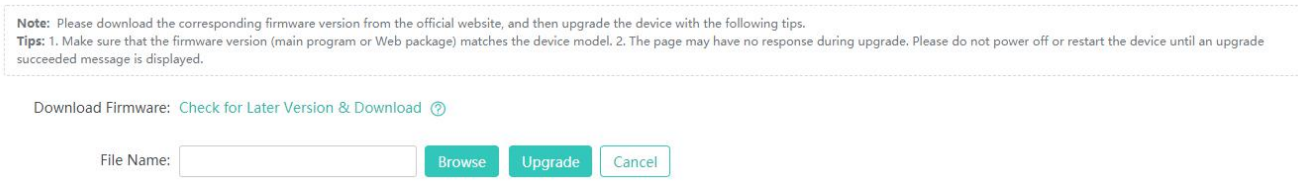
1.3.5 Maintenance

Settings

Upgrade

Local Upgrade

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



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.

Restart

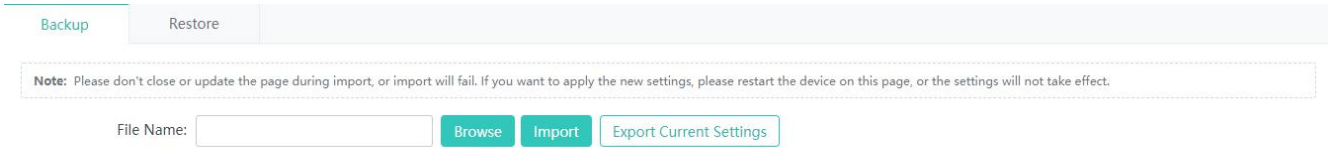
Conveniently restart the system with a click.

Click **Restart** to restart the device.

Backup & Restore

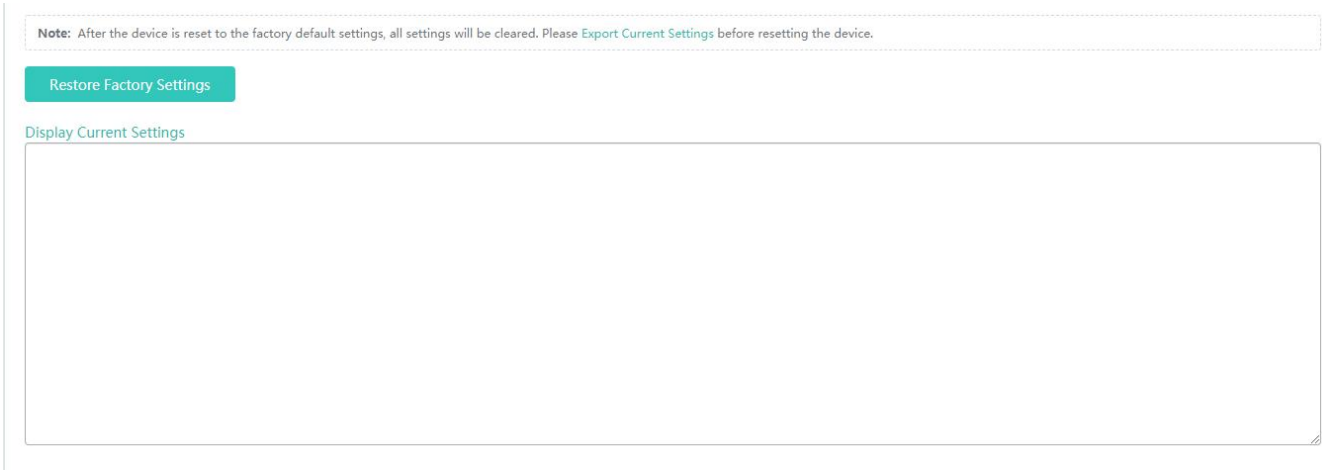
Backup

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



Restore

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

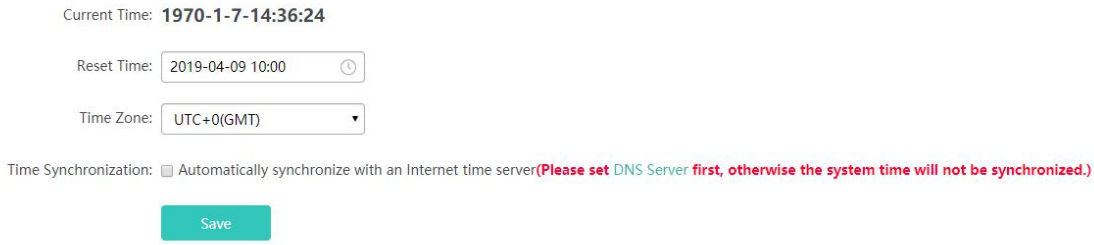


System Time

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.



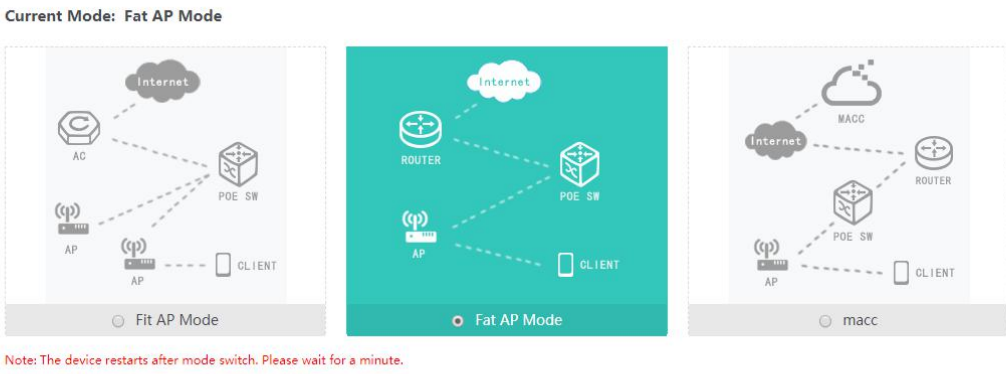
System Mode

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.

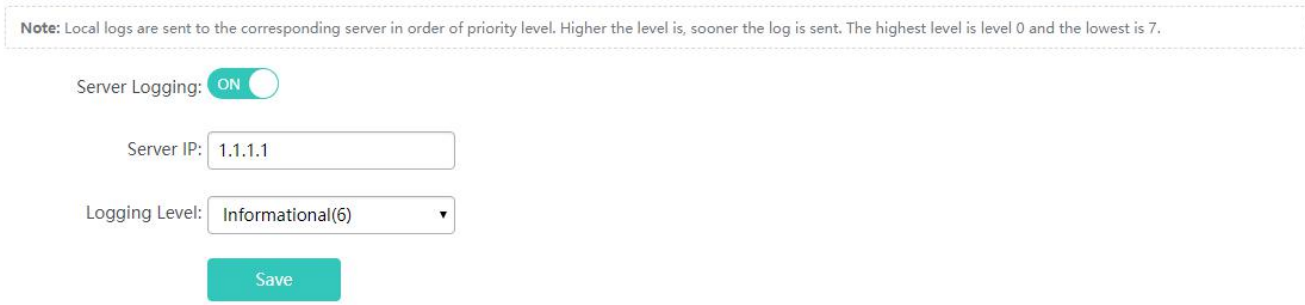
Select the AP mode.



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.



DNS

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

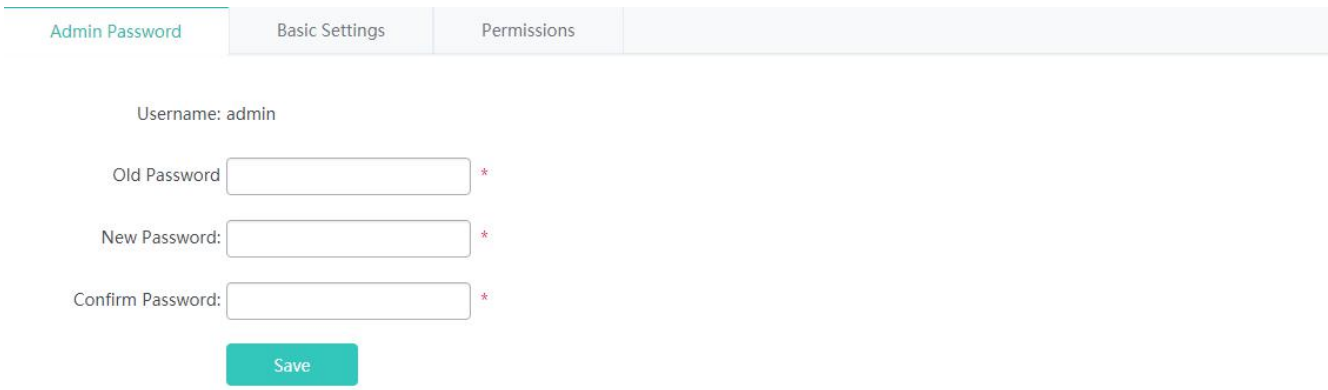
System

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**.



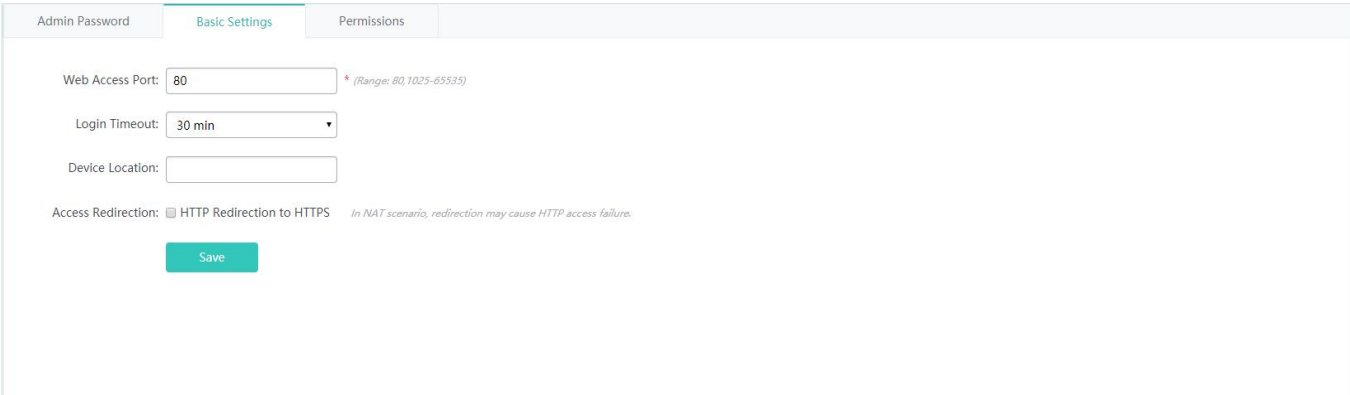
Basic Settings

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.

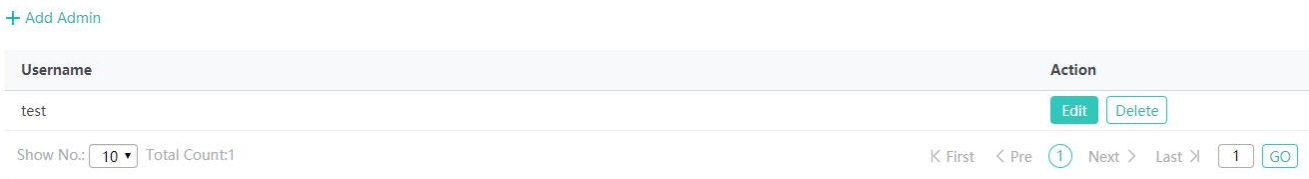
Login Timeout: Indicates the timeout time.

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

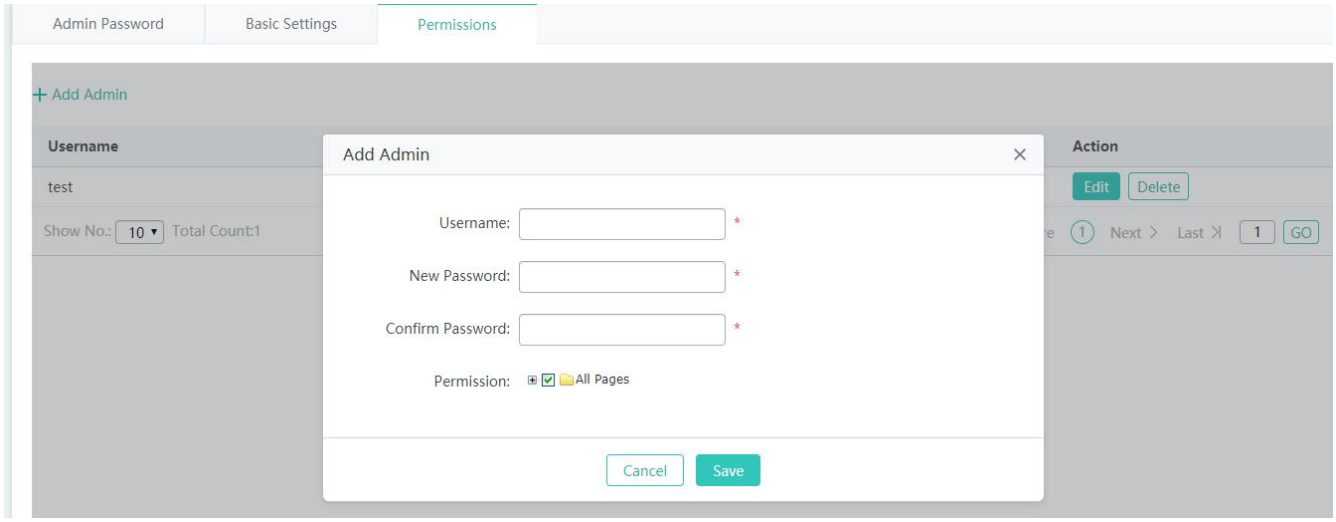


Permissions

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**

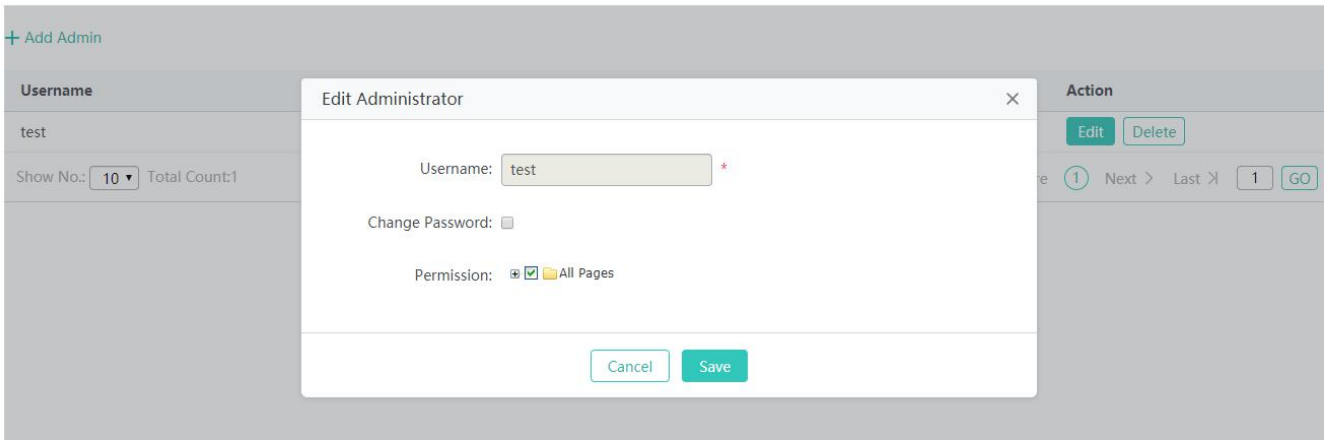


- Adding an Administrator



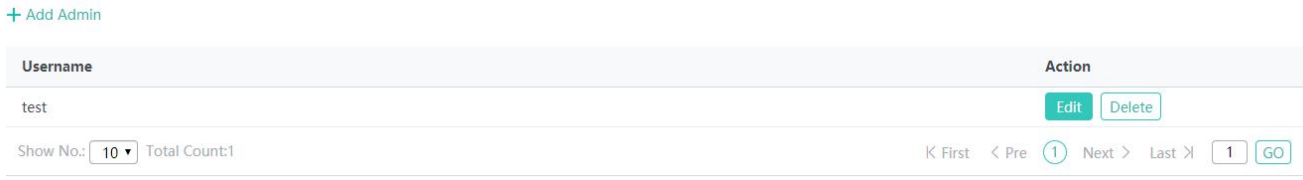
Click **Add Administrator**. A dialog box is displayed, as shown in the preceding figure. Set the configuration items in the dialog box, and click **Save**. The newly added administrator is displayed in the list after the **Save succeeded** message is displayed.

- 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.

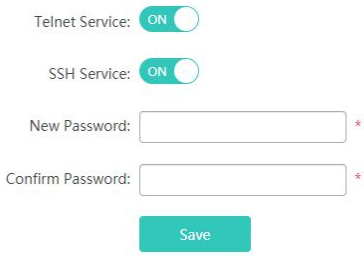
- Deleting an Administrator



Click **Delete** to delete an administrator.

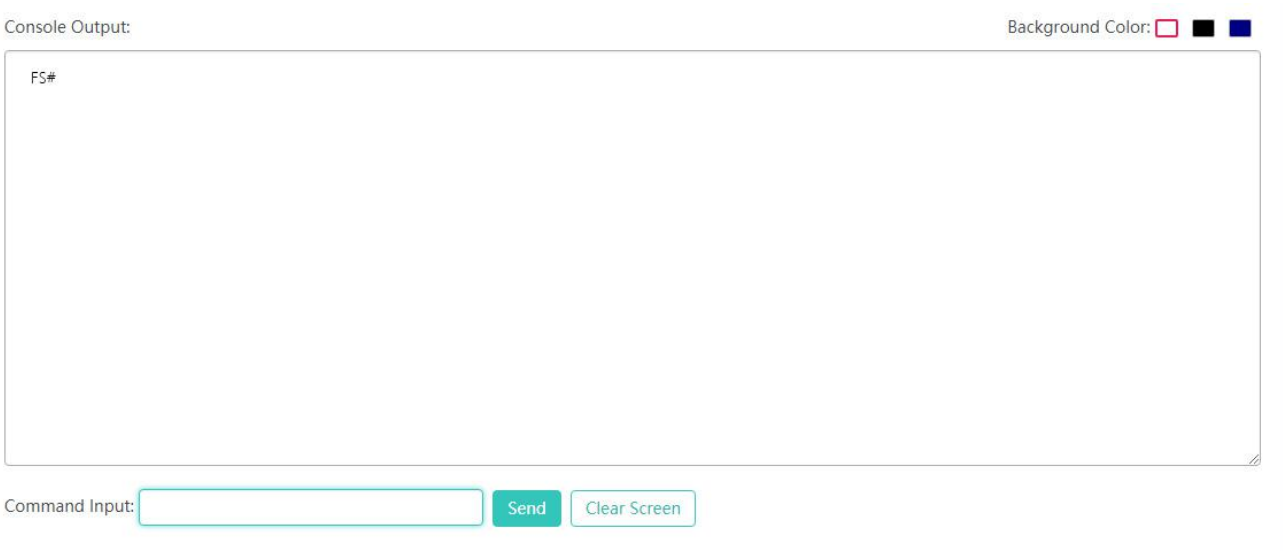
Telnet & SSH

Enable Telnet and SSH access for security purposes.



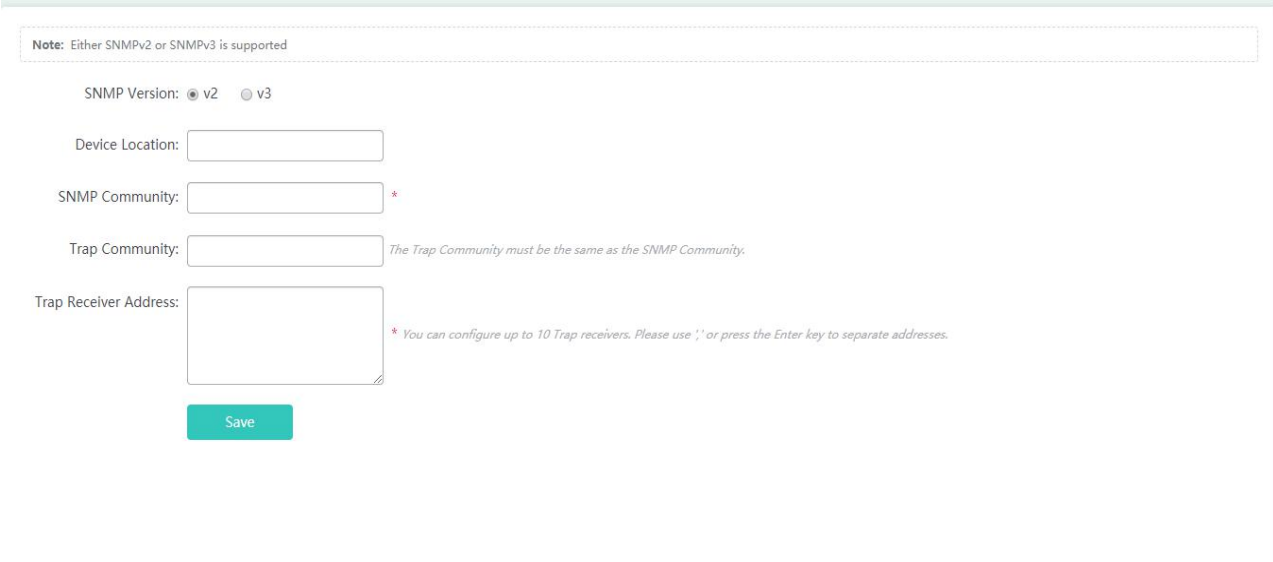
Web Console

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.



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.



CWMP/MACC

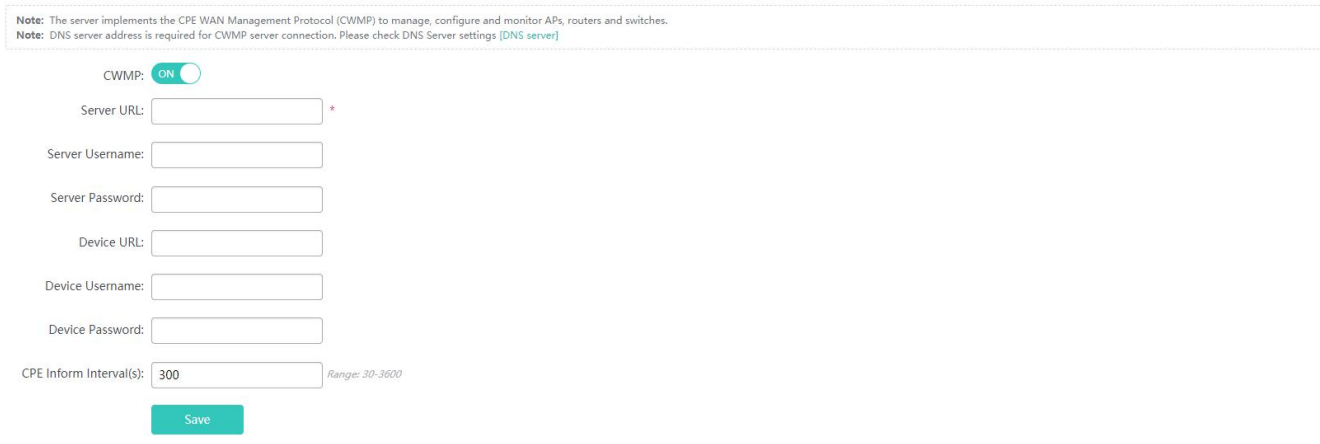
The CPE WAN Management Protocol (CWMP) is used by a server to manage, configure, and monitor ACs, APs, routers, or switches.

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**.



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

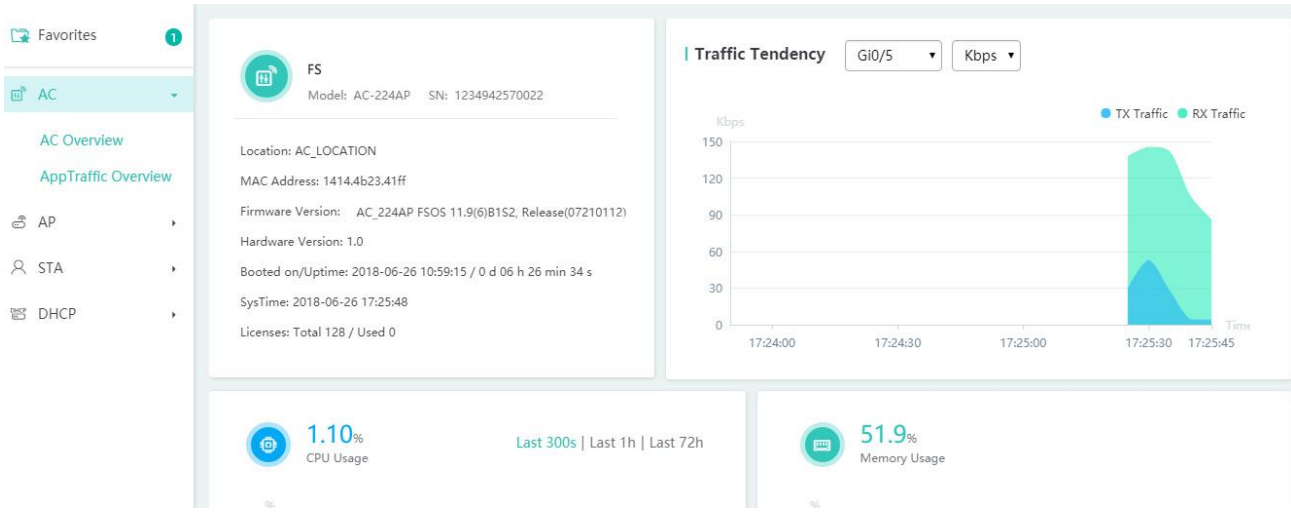
Favorites

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.

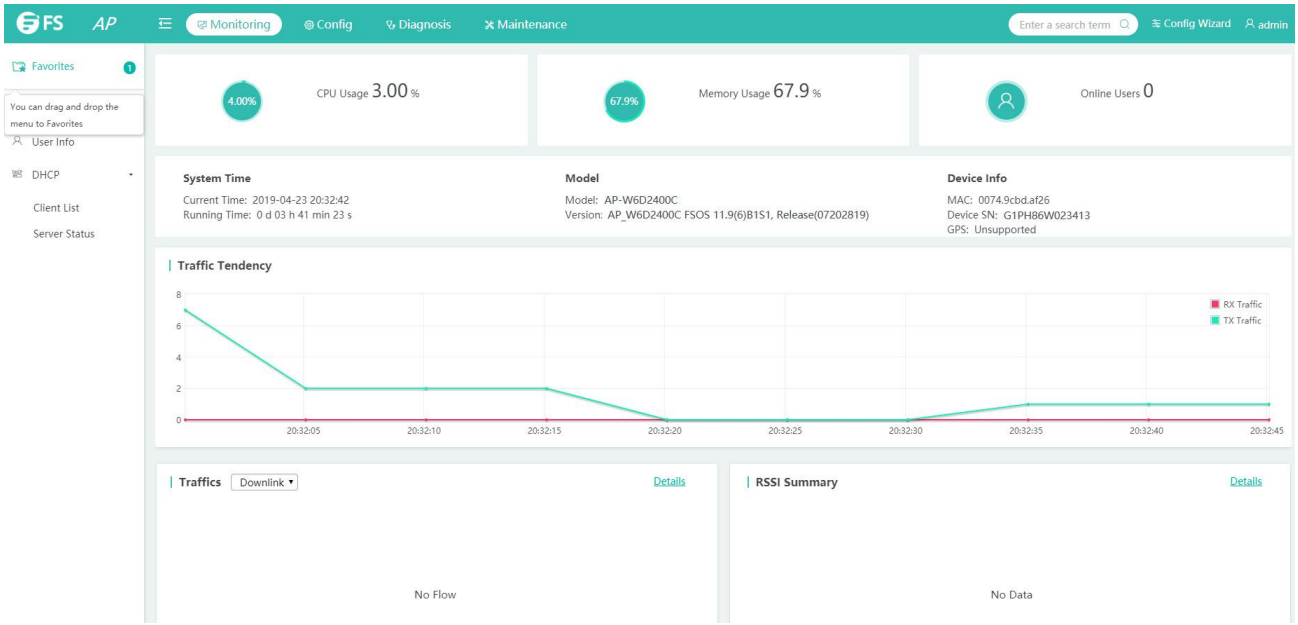
- Adding to Favorites

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 deletion icon. Confirm the delete operation to delete the menu item from the favorites.



Fast Query Menu

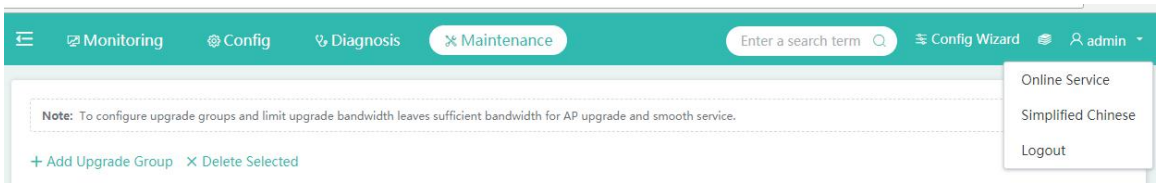
There are increasing functions in the system. The fast query menu helps users rapidly search for required functions.

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.

More Functions of the System

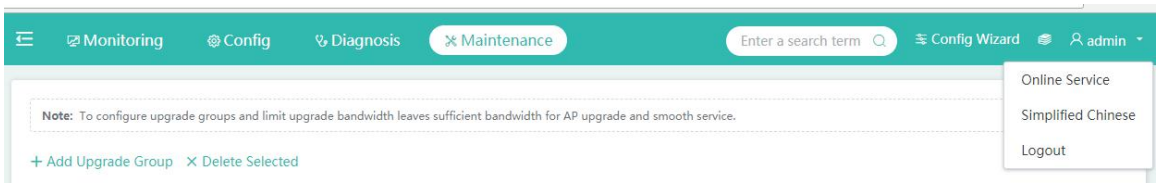
- Displaying the Current Account

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.



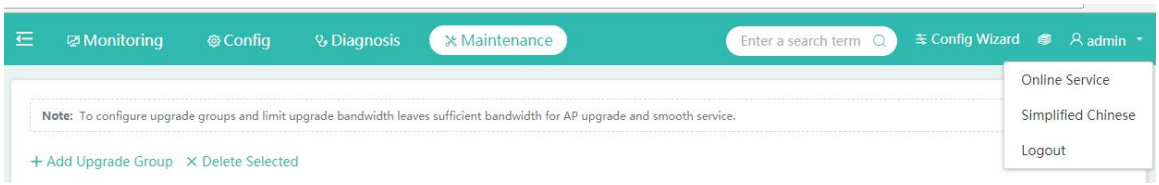
- Online Service

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

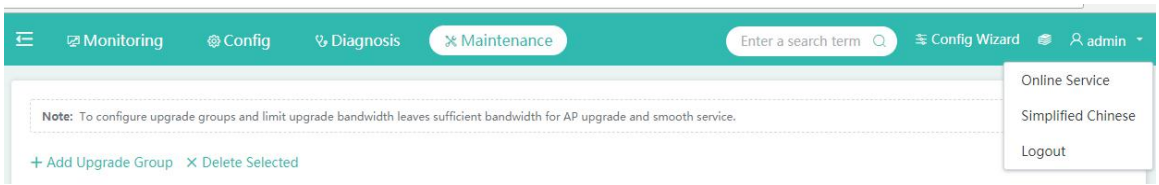
Click the current account icon in the upper right corner. A function drop-down list is displayed. The second item is used for language switching. If the system is in Chinese, click **English** to switch to the English edition; if the system is in English, click **Simplified Chinese** to switch to the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

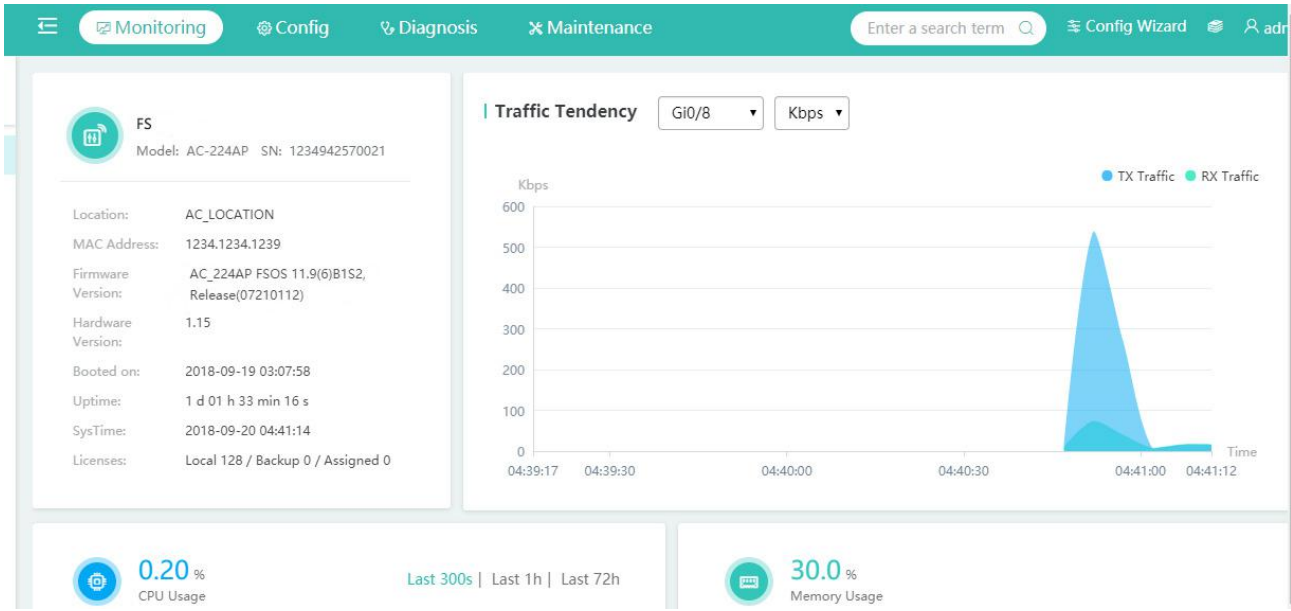
- Exiting the system

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.



Help Information

When users are unfamiliar with system functions and need help information, click  to query required information.



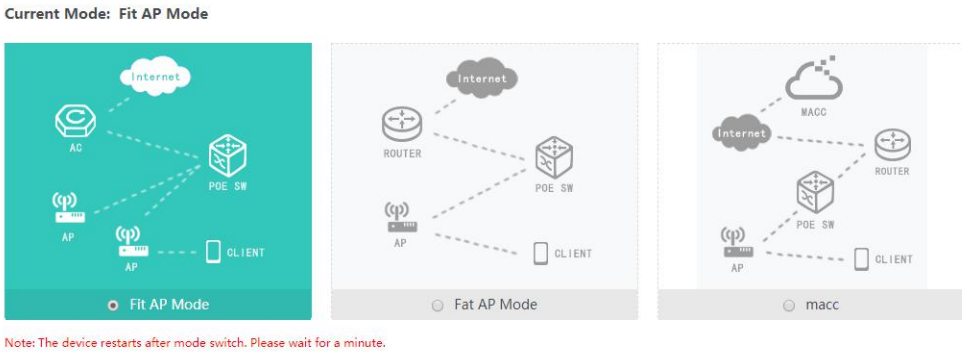
1.4 Fit AP-Eweb

1.4.1 SmartAP

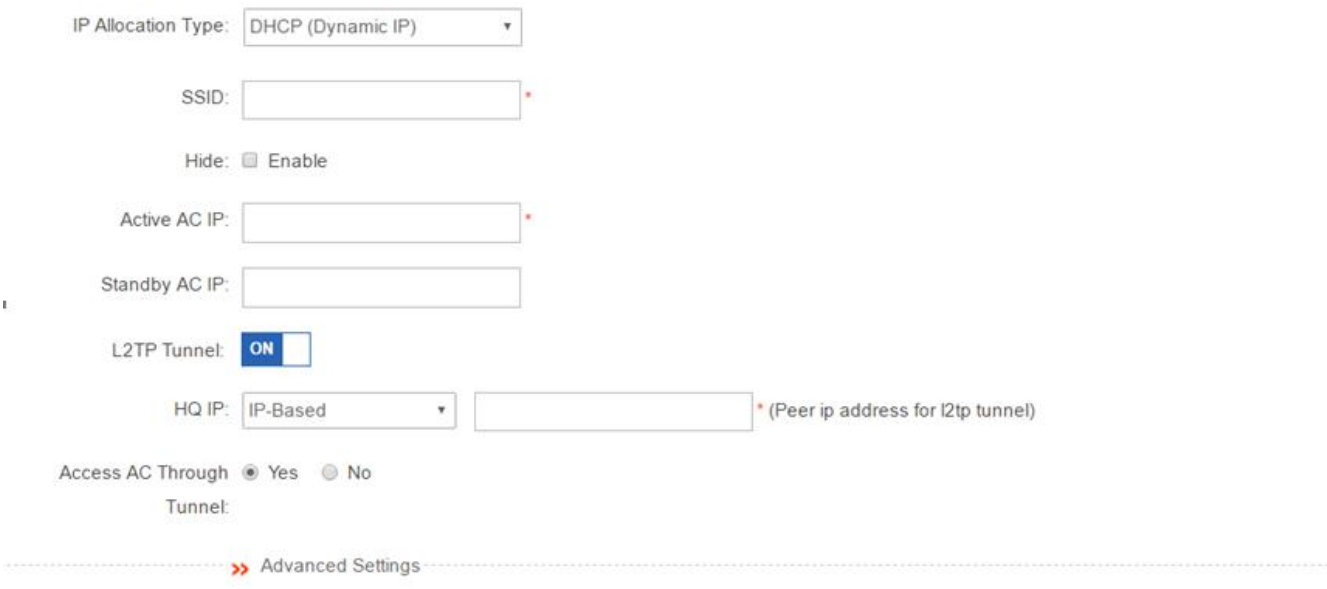
SmartAP allows you to deploy APs in mobile office scenario. Click **Config Wizard** to end the SmartAP configuration page, including **System Mode**, **Network Configuration** and **Change Web NMS Password**. If APs are not applied to mobile office scenario, only system mode will be displayed.

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.



2. Network Configuration



3. Change Web NMS 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	enable service web-server [http | https | all]
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** *ip-address ip-mask*
Parameter Description	*ip-address*: IP address. *ip-mask*: network mask.
Command Mode	Interface configuration mode.

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

Command	**webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password*
Parameter Description	*privilege-level*: 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. *name*: address of the static RP. *password*: 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. *encrypted-password*: 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.
	FS# configure terminal FS(config)# enable service web-server FS(config)# webmaster level 0 username admin password admin FS(config)#interface vlan 1 FS(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0 FS(config)# end
Verification	Run the **show running-config** command to display related configuration commands.
	FS(config)#show running-config Building configuration... Current configuration : 6312 bytes

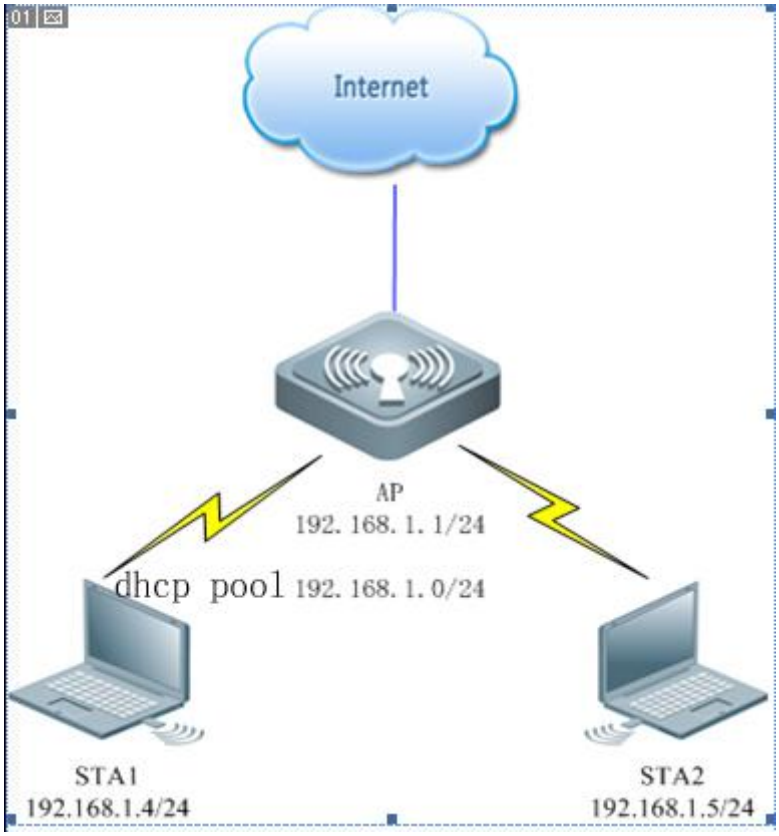
```
!
hostname FS
!
!
webmaster level 0 username admin password 7 08022b181b29
webmaster level 1 username manager password 7 06073f
webmaster level 2 username guest password 7 14155f083206
http update mode auto-detect
!
!
interface VLAN 1
 ip address 192.168.1.200 255.255.255.0
 no shutdown
!
line con 0
line vty 0 4
 login
!
!
End
```

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.

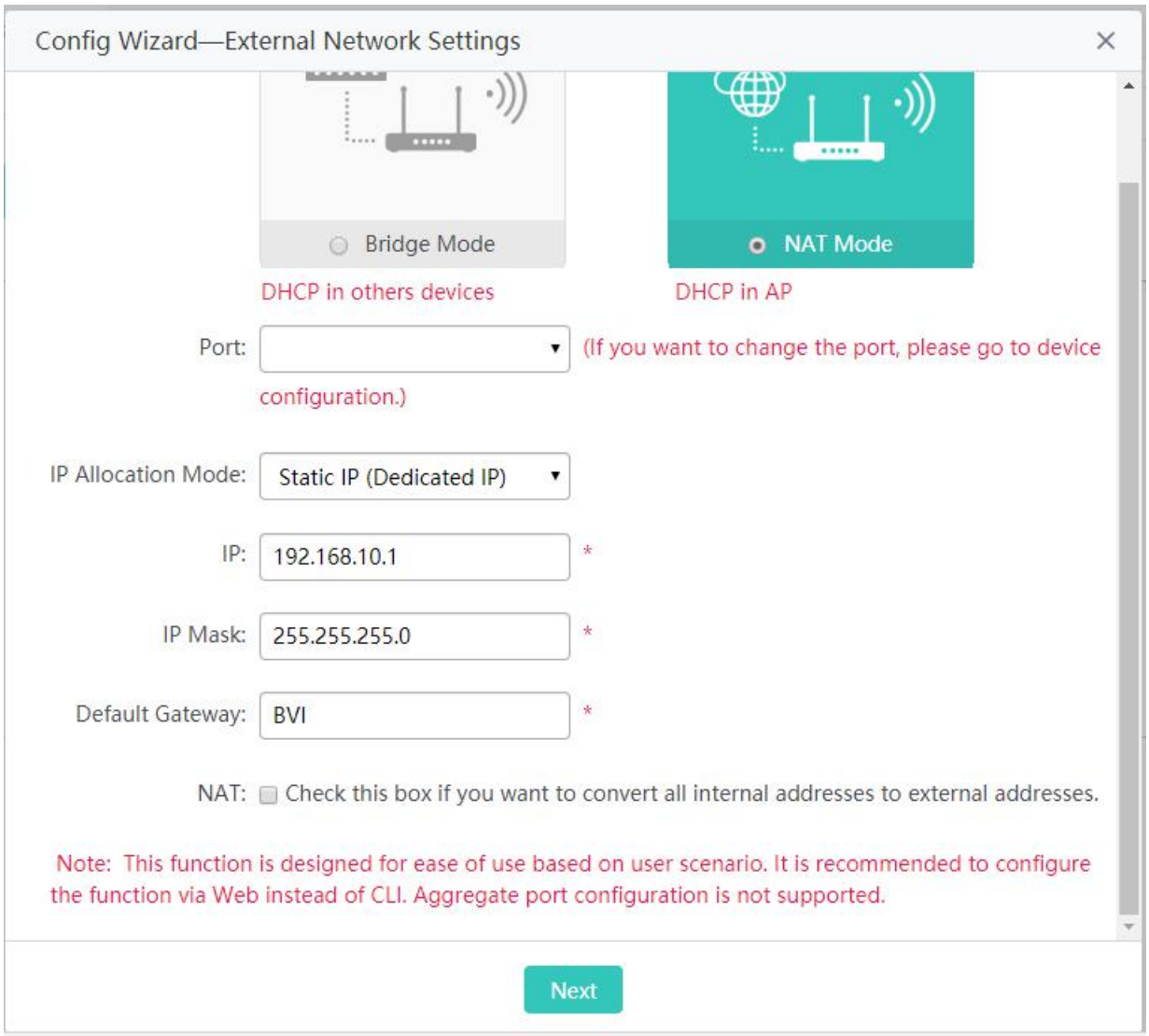
Figure 1-3 Topology 1 (AP is in routing mode)



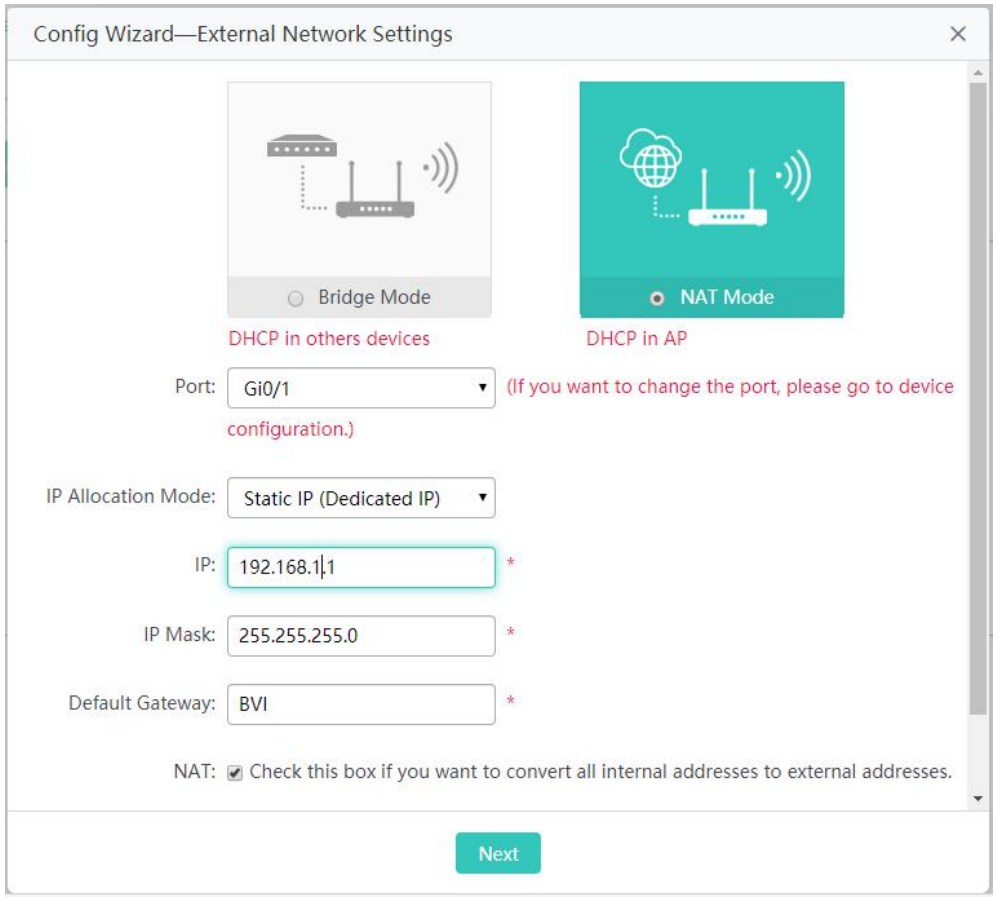
Configuration	Description and Command	
Construction of a WLAN for the DHCP server on the AP	Mandatory. It is used to configure a WLAN.	
	WiFi name	Associates internet access wireless signals for an STA
	WiFi password	An STA inputs the password for internet access.
	DHCP configuration	Allocates IP addresses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

Verification

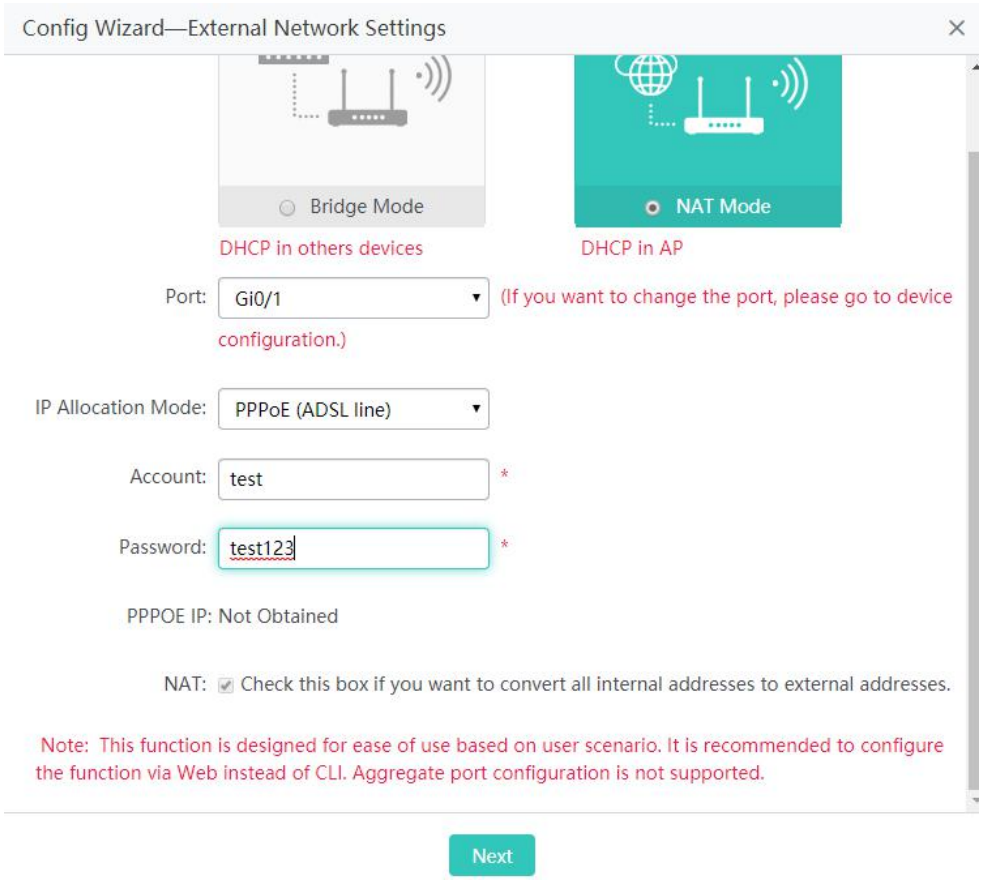
Select AP working mode and set the Internet connection type



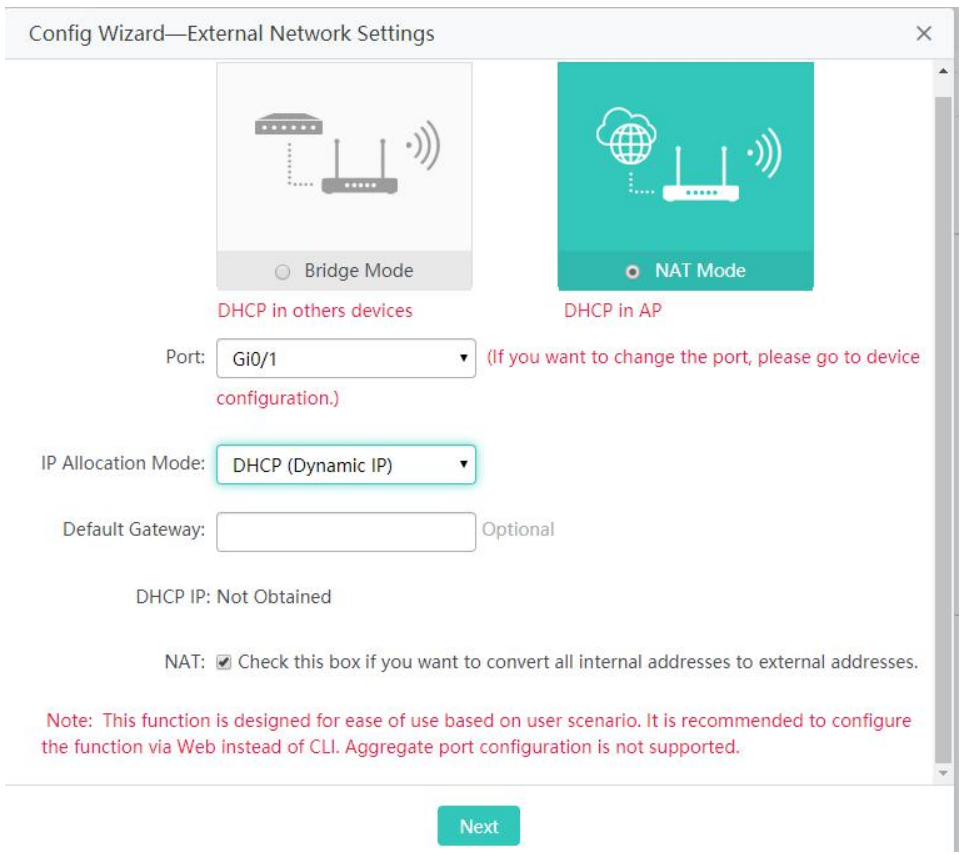
- The AP works in wireless routing mode.
- You can select the following Internet connection types when the AP works in wireless routing mode.
- Static IP (dedicated IP)



- PPPoE (ADSL line)

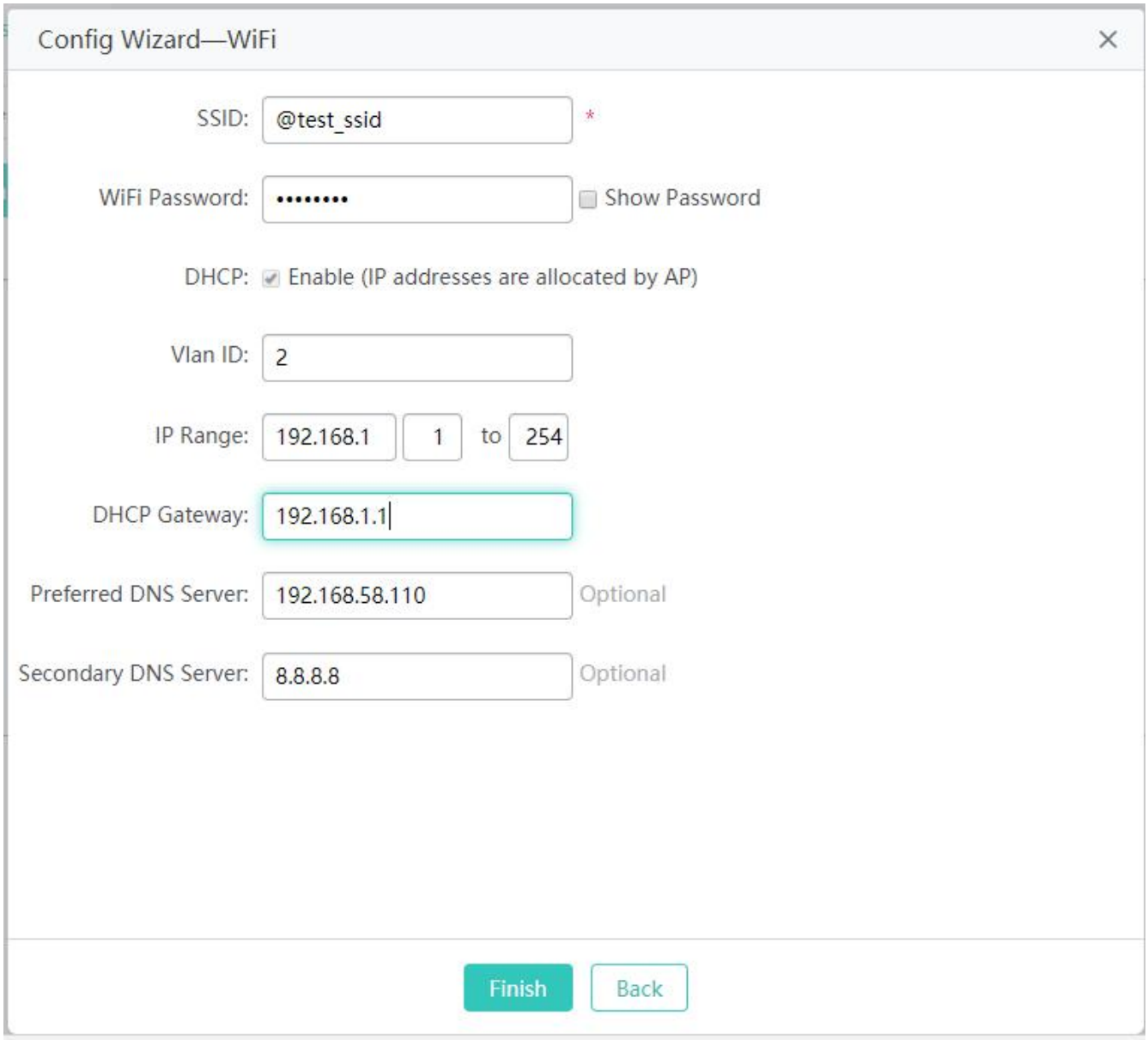


- DHCP (dynamic IP)



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

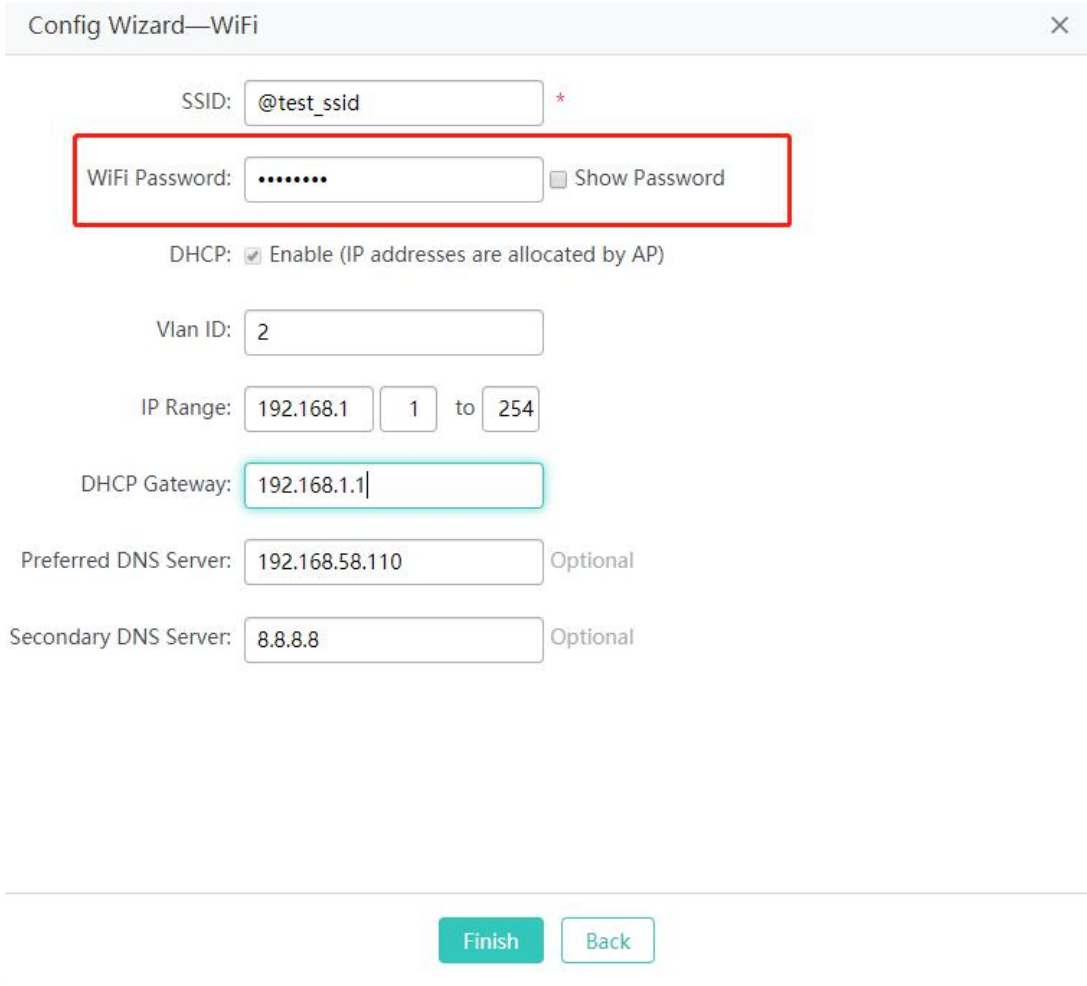
Figure 1-4 AP Quick Settings for SSID



Security configuration

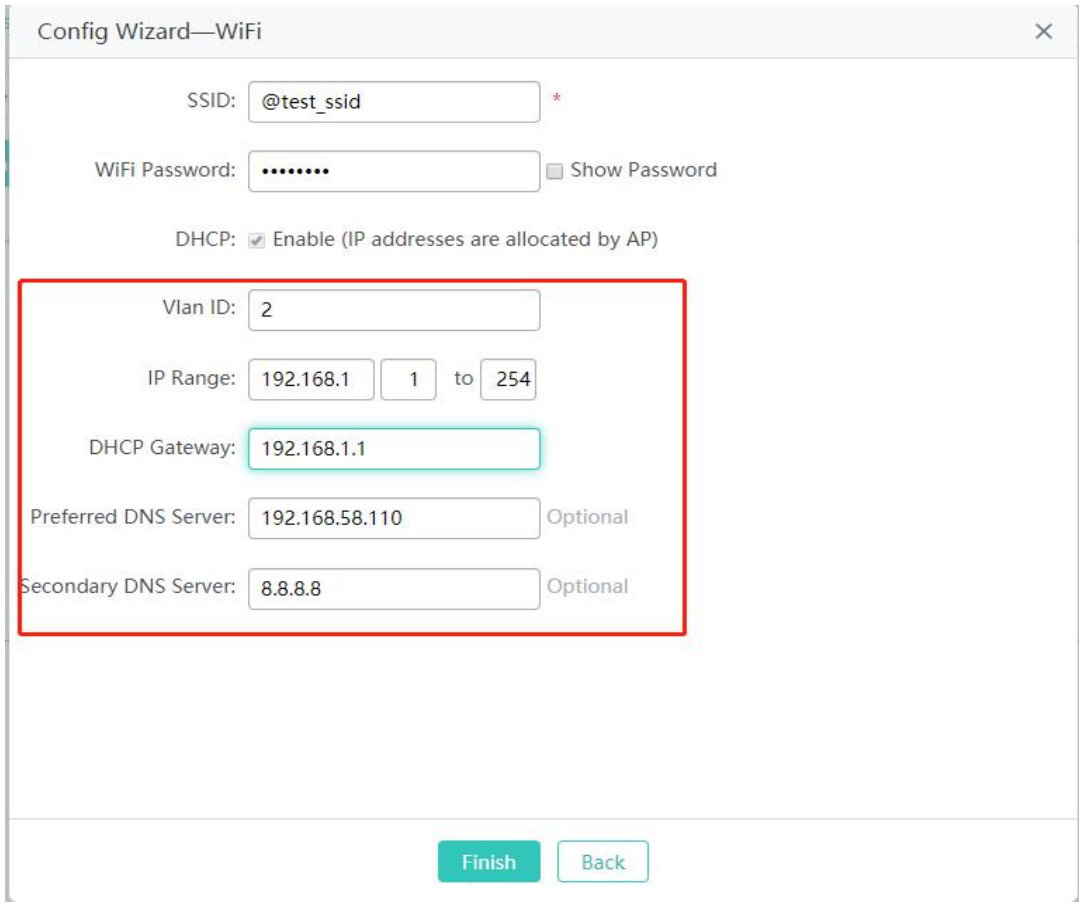
- By default, the WPA2-PSK mode is selected. A password consists of 8 to 64 characters and can be a combination of letters, digits, and special characters.

Figure 1-5 AP Quick Settings for Security



DHCP configuration

Figure 1-6 AP Quick Settings for DHCP



- 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.

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

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.