Ruijie RG-WLAN Series Wireless Controllers

Web-Based Configuration Guide, Release 11.9(0)B7

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Obtaining Technical Assistance

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

1 Web-Based Configuration

1.1 Overview

Web-based management allows administrators to access the Web-based management system by using a browser (such as IE and Google Chrome) to manage Access Points (APs).

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

Currently, this document is applicable only to ACs and WLAN-AC cards.

1.2 Applications

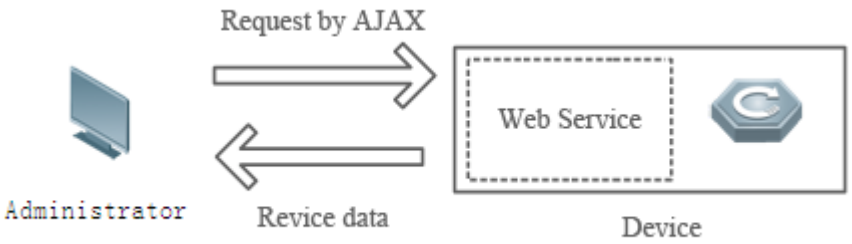
Application	Description
Managing Devices by Using the Web-based Management System	Administrators can access devices from browsers to configure and manage the devices by using the Web-based management system.

1.2.1 Managing Devices by Using the Web-based Management System

Scenario

As shown in Figure 1-1, administrators can access devices from browsers to configure the devices by using the Web-based management system.

Figure 1-2 Application Topology



Remarks	The Web-based management system integrates various device commands. It sends a request command to a device via Asynchronous JavaScript And XML (AJAX) and the device returns relevant data according to the command. The Web service on the device can process basic Hypertext Transfer Protocol (HTTP) requests.

Deployment

- **Configuration Environment Requirements**

Client requirements:

- An administrator can log in to the Web-based management page of a device by using the Web browser on the Web client, to manage the device. The client usually refers to a PC or some other mobile STAs such as laptops or iPads. Mobile phone clients are not supported.
- IE9.0, IE10.0, IE11.0, Google Chrome, and some IE kernel-based browsers (such as 360 browser) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- It is recommended to set the resolution to 1280 x 1024, 1920 x 1080, or 1440 x 960. If other resolutions are used, the page font and format may not be aligned, the UI is unaesthetic, or other exceptions may occur.

Server requirements:

- The Web service needs to be enabled on an AC.
- Login authentication information for Web-based management needs to be configured on the AC.
- A management IP address needs to be configured on the AC.

Default Configurations

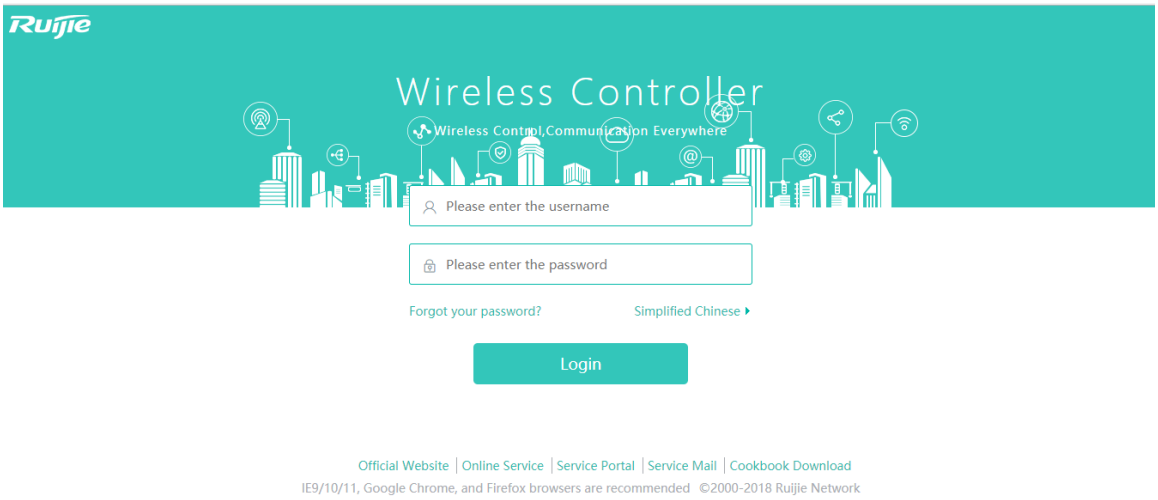
The following tables list the default configurations of the Web-based management system.

Feature	Default Value
Web service	The Web service is enabled by default.
Device IP address	192.168.110.1

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

The default username is displayed in output of the **show running-config** command only after its default password is changed.

After the Web service is enabled and the IP address is configured correctly (the IP address is reachable), you can enter the IP address in the http://ip format in the browser such as http://192.168.110.1 and press **Enter**. A page shown in the figure below is displayed.



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

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

The name of the wireless product is displayed on the login page. Click **Forgot your password?** to display the prompt for retrieving the password. Click the language switching button to switch the language of the current network management system. Only Chinese and English are supported currently.

1.3 Configuration

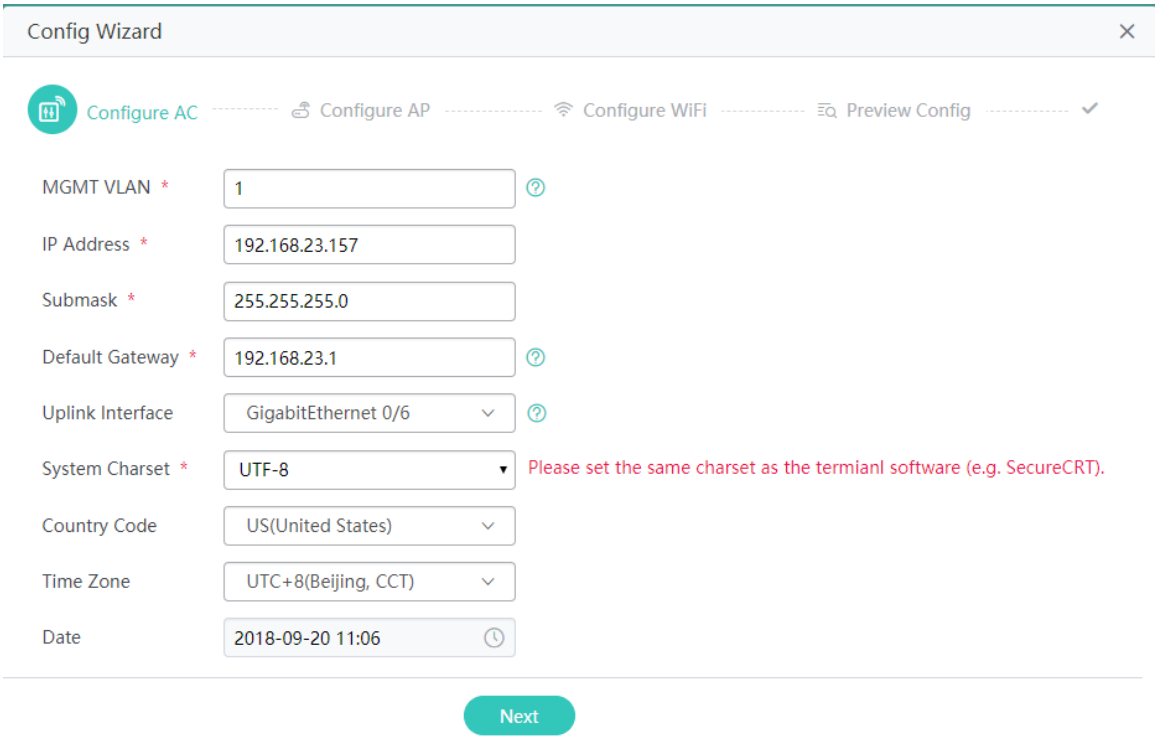
1.3.1 Configuration Wizard

The configuration wizard is generally used in the initial deployment of devices and enables fast configuration for common scenarios. Not all scenarios are supported by the configuration wizard.

1. When detecting no **config.txt** file on the current device, the Web-based management system displays the configuration wizard to guide device configuration by default. Click the **Config Wizard** link in the upper right corner of the home page. The Config Wizard page pops up.
2. Only one or two WLANs can be configured via the current configuration wizard, to build a WLAN or WLANs to transmit WiFi signals.
3. Configurations made via the configuration wizard will overwrite the configurations of the current device.

The configuration wizard involves four steps: basic AC configuration, AP access configuration, WiFi configuration, and configuration preview.

Step 1: Configure AC



Country Code, **Time Zone**, and **Date** are supported only in the English edition.

Manage VLAN

Indicates the VLAN used by the AC to communicate with the external network, that is, VLAN used for Web access.

IP Address

Indicates the IP address used by the AC to communicate with the external network, that is, IP address used for Web access. It is the tunnel address by default and the communication address used for establishing a tunnel between the AC and an AP.

Submask

Indicates the IP address mask used by the AC to communicate with the external network.

Default Gateway

Indicates the egress gateway and is used to deliver the following default route: ip route 0.0.0.0 0.0.0.0 + gateway.

Uplink Interface

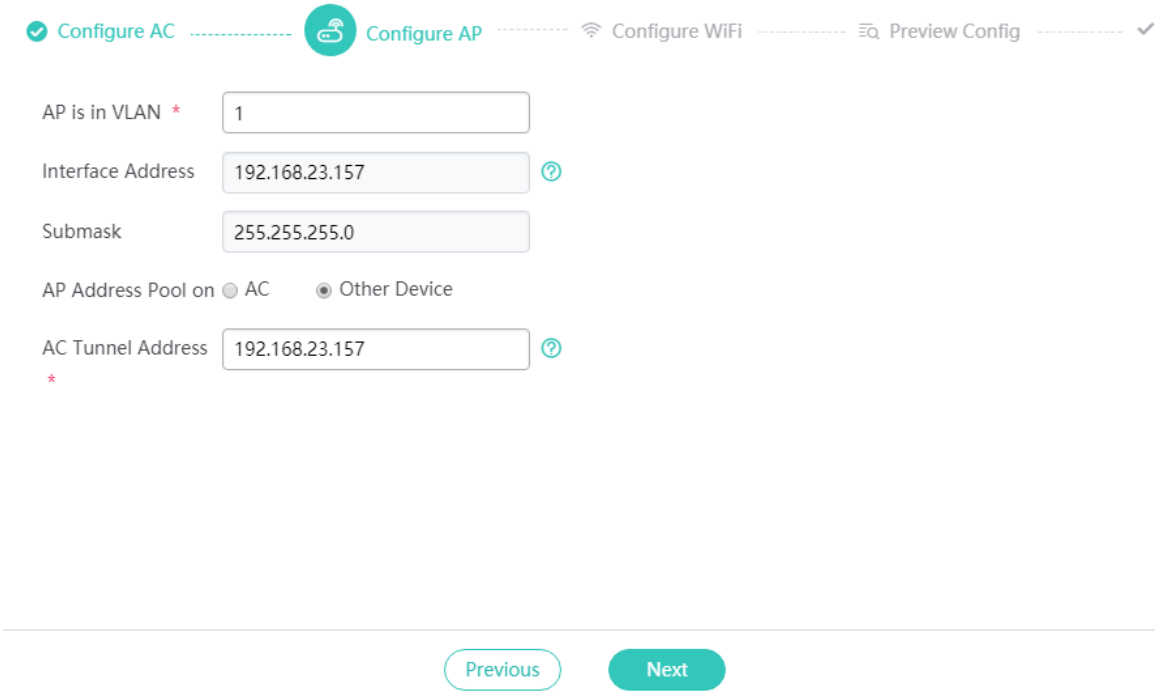
An uplink interface is used by the AC to communicate with an external device. A selected uplink interface can be configured to work in trunk mode.

System Charset

System Charser is set to **UTF-8** by default. If a user needs to view or configure the system by using other terminal tools, it is recommended to set **System Charaset** to **UTF-8**. Otherwise, code mixing may be incurred, resulting in the page configuration failure or garble.

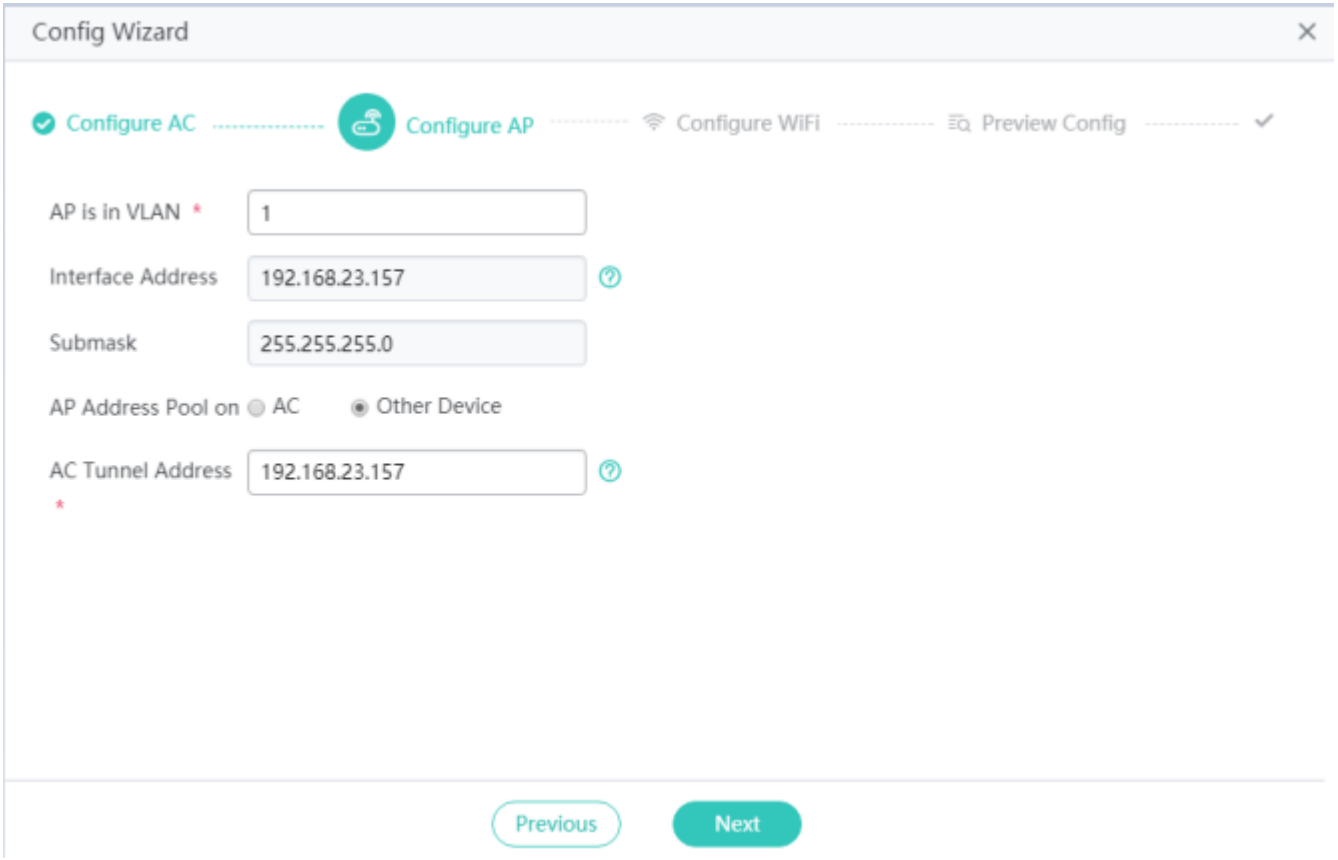
Step 2: Configure AP

- Determine the VLAN to which an AP belongs. The VLAN of the AP is consistent with the management VLAN by default.

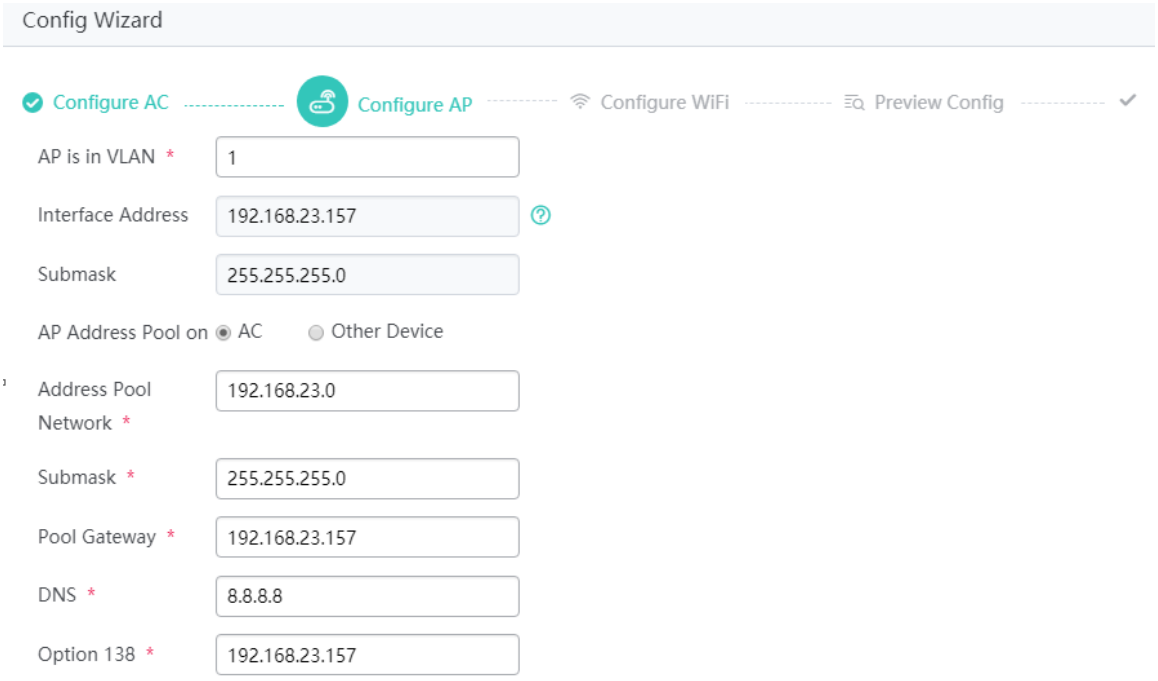


- Determine the location of the AP address pool.

If **AP Address Pool on** is set to **Other Device**, perform related DHCP configuration on the corresponding device after completing the fast configuration.

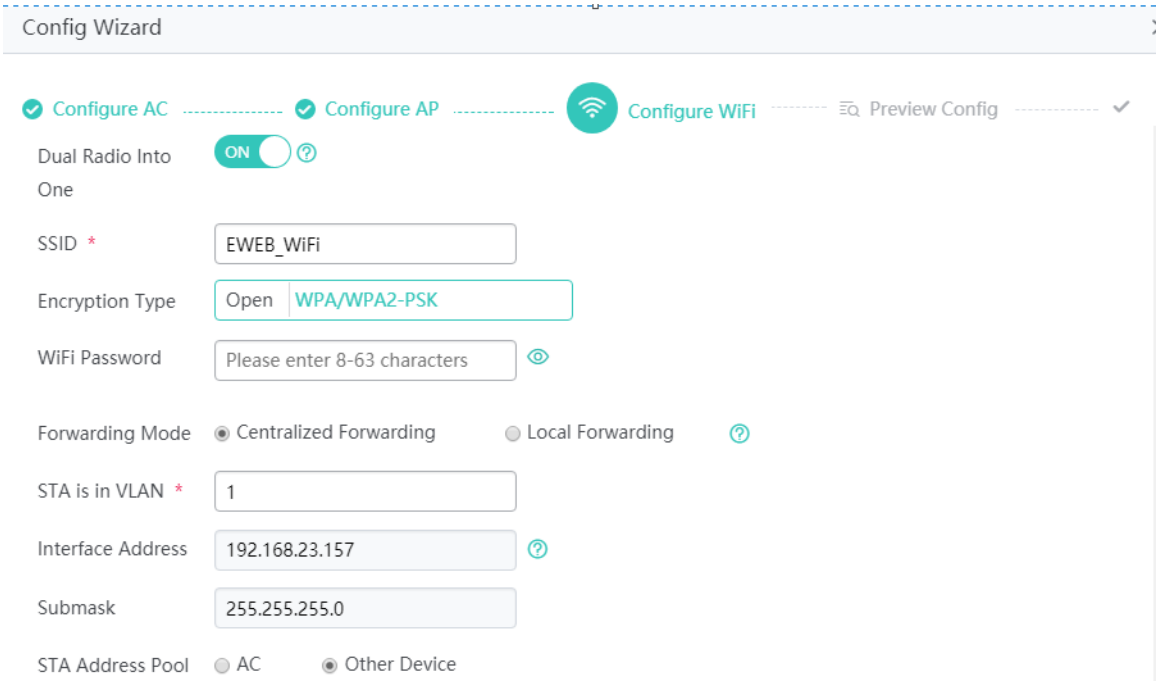


If **AP Address Pool on** is set to **AC**, set **Address Pool Network** and **Submask**. **DNS** is set to **114.114.114.114** in the Chinese edition and **8.8.8.8** in the English edition by default.



Step 3: Configure WiFi

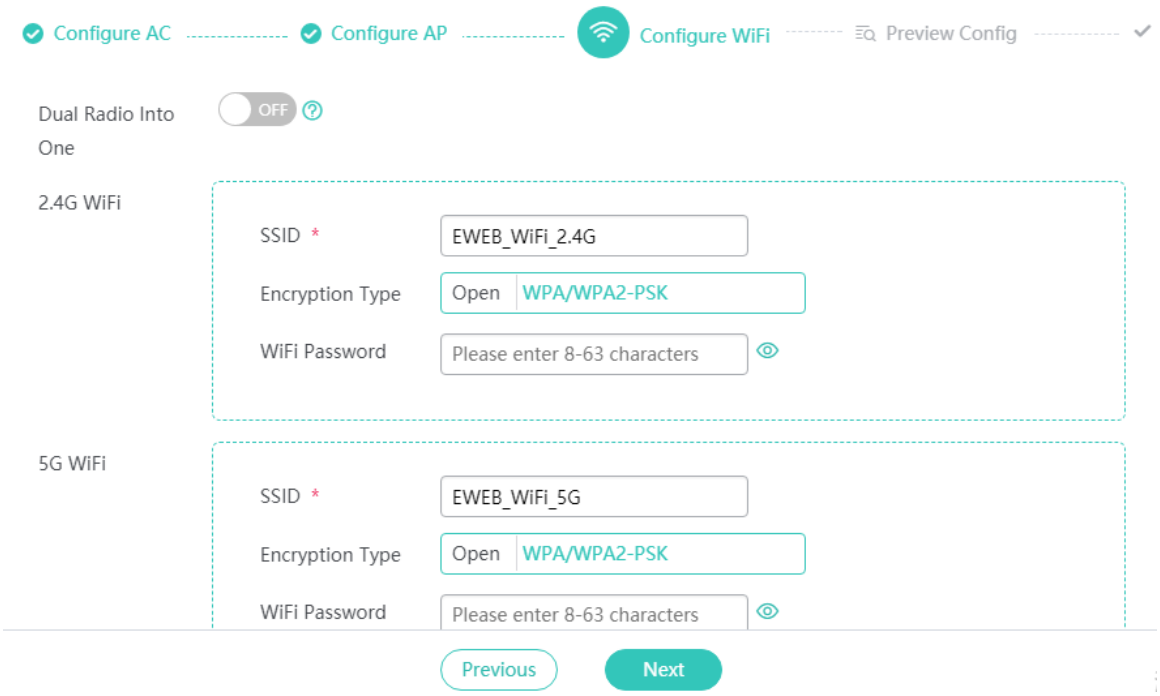
- WiFi configuration



Dual Radio Into One

Dual Radio Into One is set to **ON** by default and indicates that one WiFi network is configured, which transmits both 2.4 GHz and 5 GHz signals.

If **Dual Radio Into One** is set to **OFF**, it indicates that two WiFi networks are configured, with one transmitting 2.4 GHz signals and the other transmitting 5 GHz signals.



Encryption Type

Open: No password is needed for associating a STA with a WiFi network. No encryption mode is configured.

WPA/WPA2-PSK (universal edition): shared key-based WPA mode, enabling high security and easy configuration. This mode is applicable to common home users and small-sized enterprises.

STA Address Pool

Users can select the location for deploying the STA address pool. **STA Address Pool** can be set to **AC** or **Other Device**. If it is set to **Other Device**, confirm related configuration of the address pool on the corresponding device after completing the fast configuration.

- More settings

Forwarding Mode

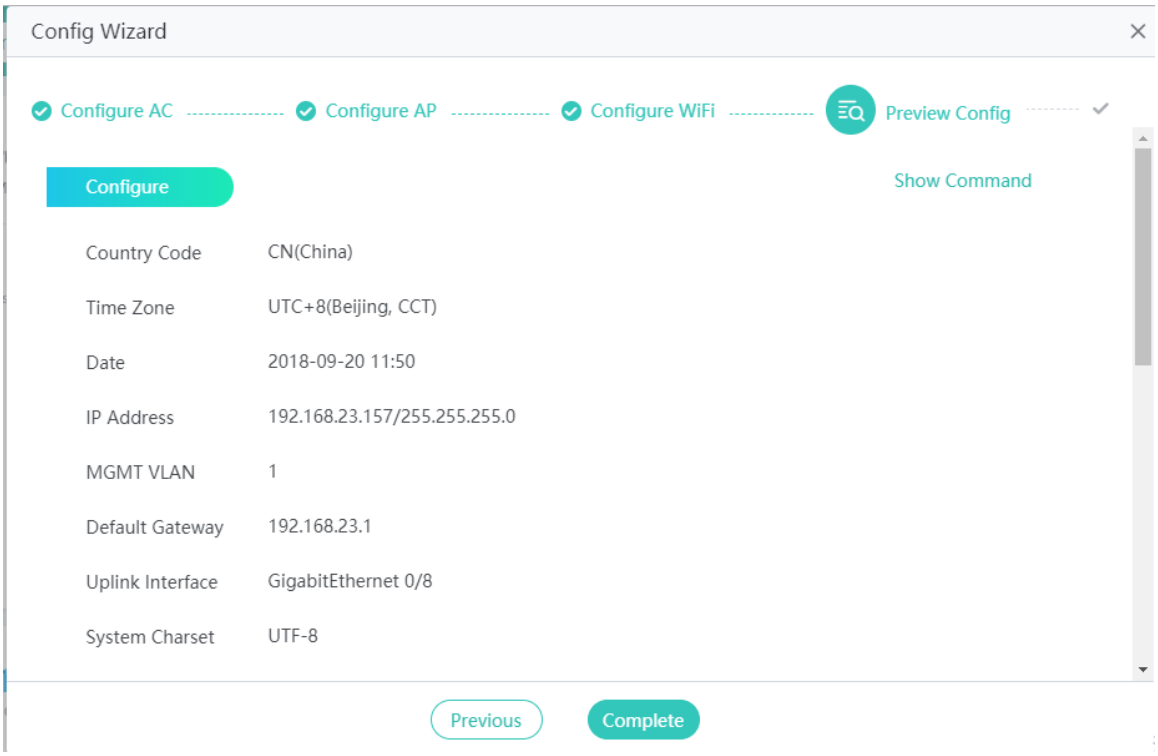
Centralized Forwarding: All data is transmitted to the AC for forwarding. **Forwarding Mode** is set to **Centralized Forwarding** by default.

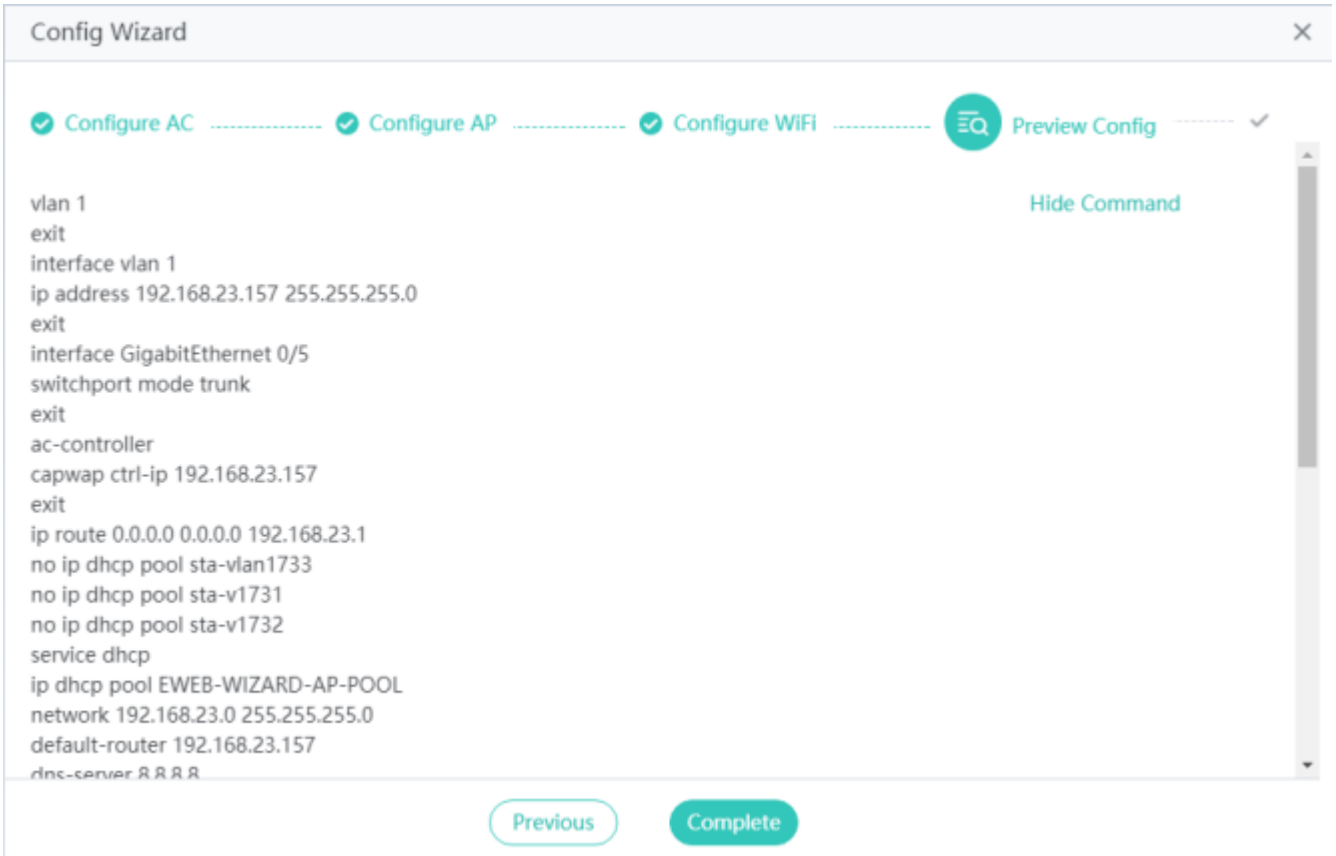
Local Forwarding: Data is directly sent out by the switch, which alleviates the load of the AC.

WiFi configuration in the configuration wizard is performed for the **default** AP group by default.

Step 4: Preview Config

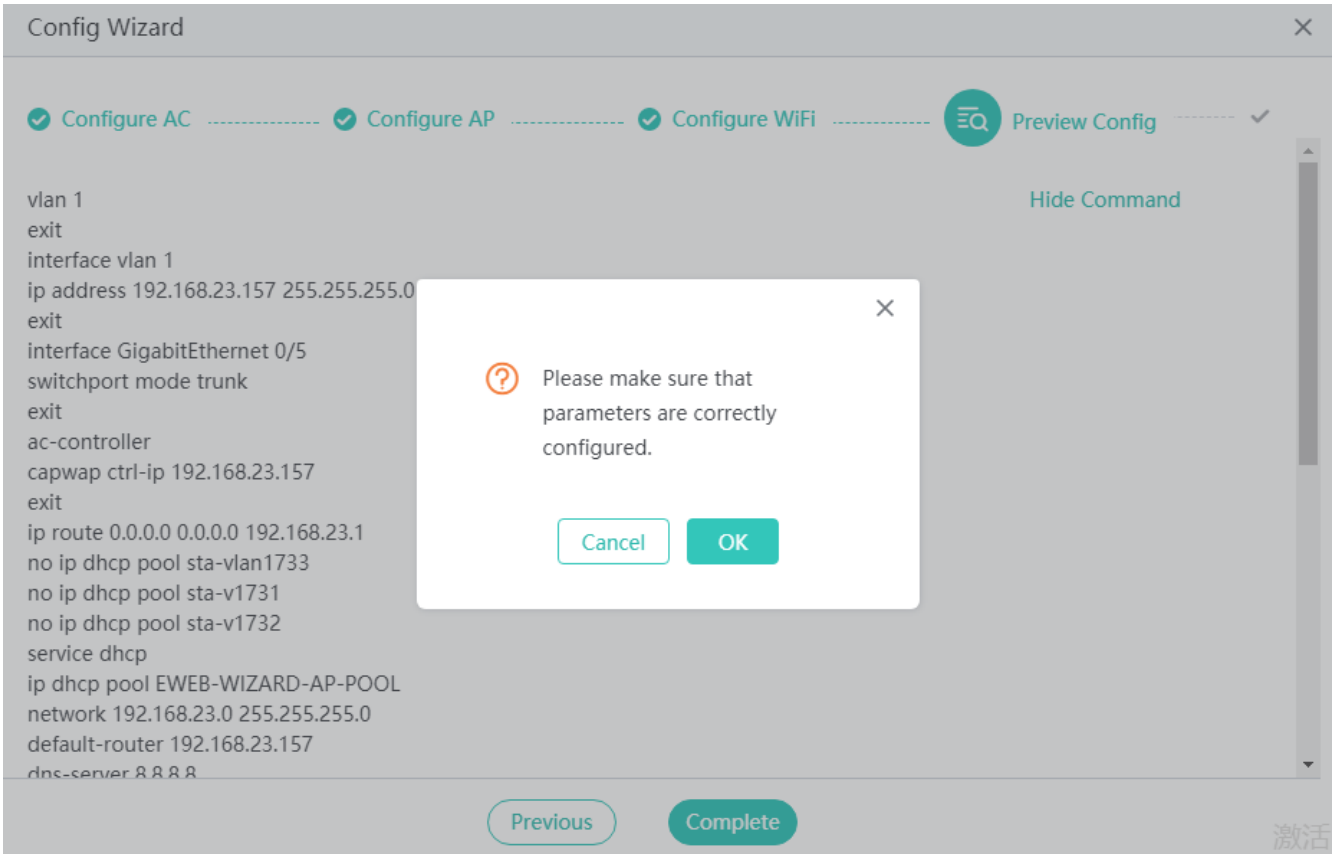
Click **Show Command** to display CLI commands to be delivered, to ensure that the current configurations are correct.



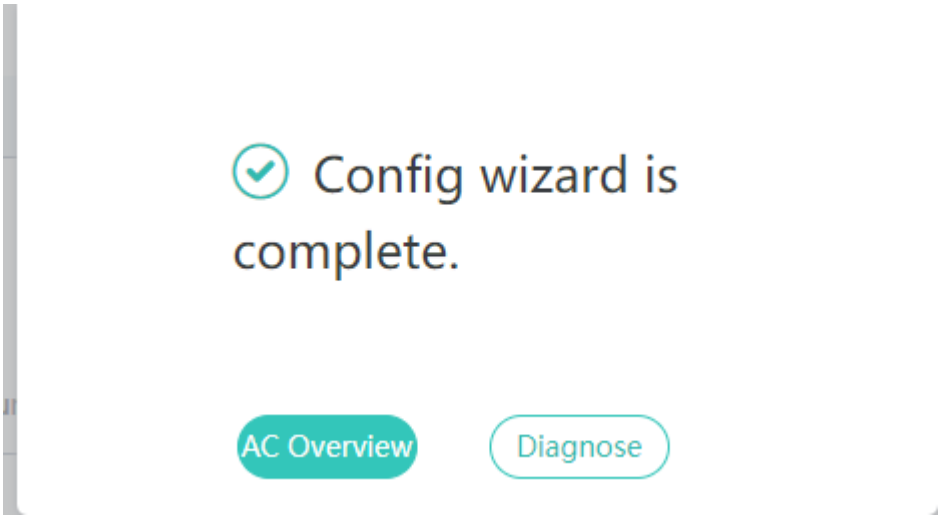


After confirming that the configurations are correct, click **Complete** to complete the configuration.

After completing the configuration, confirm whether the current configurations need to be overwritten.



Click **OK**. A page shown in the figure below is displayed. Click **Diagnose** to check whether the AC is reachable to the external network or click **AC Overview** to access the home page of system monitoring.

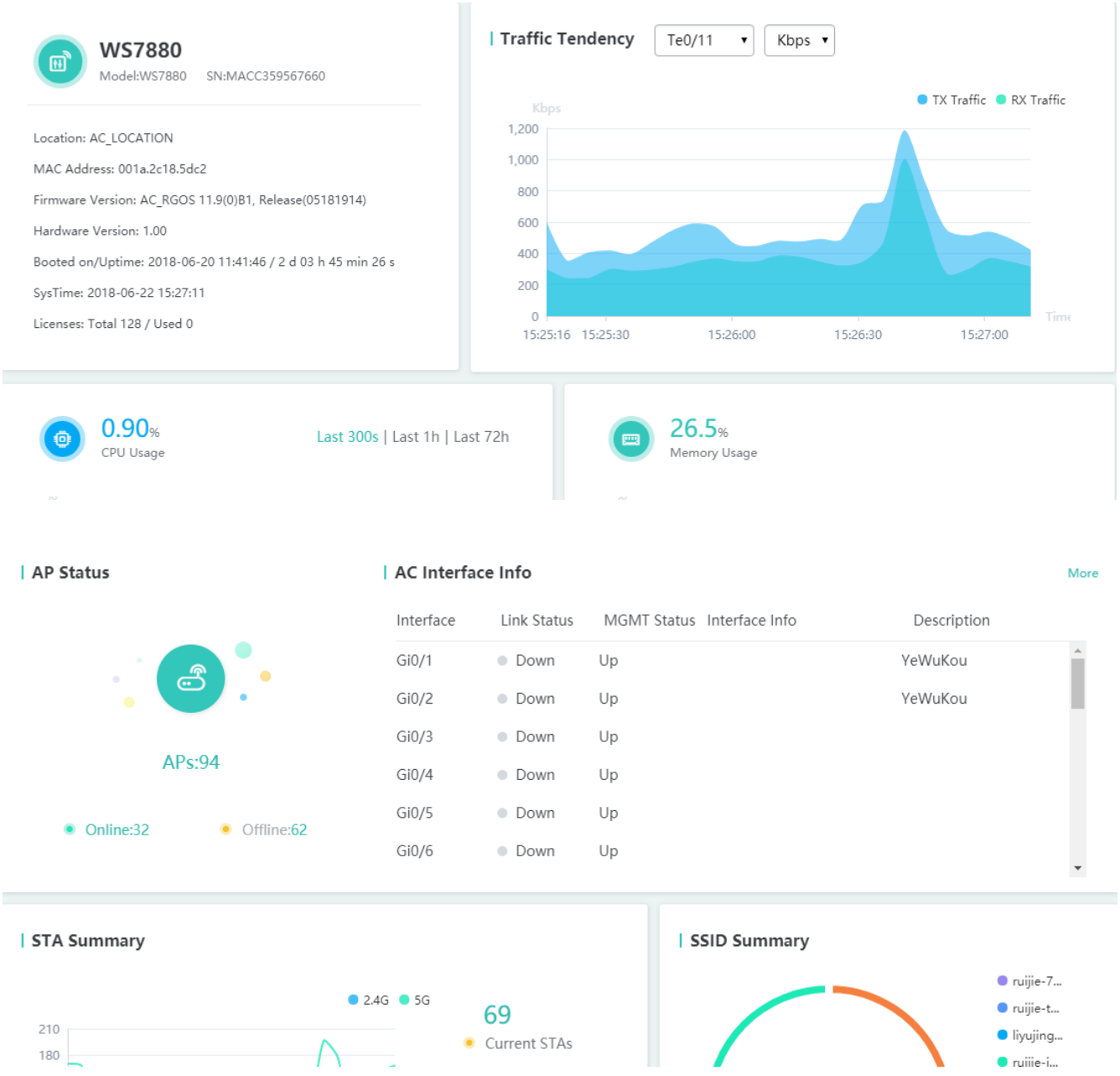


1.3.2 Monitoring

1.3.2.1 AC

1.3.2.1.1 AC Overview

The AC Overview page displays basic information about the AC, such as the MAC address, device model, system running time, version, and traffic tendency of AC interfaces. The AC interface information shows the latest information about all managed APs, STA tendency chart, percentage of WiFi STAs, CPU usage tendency chart, and memory usage tendency chart of the AC.



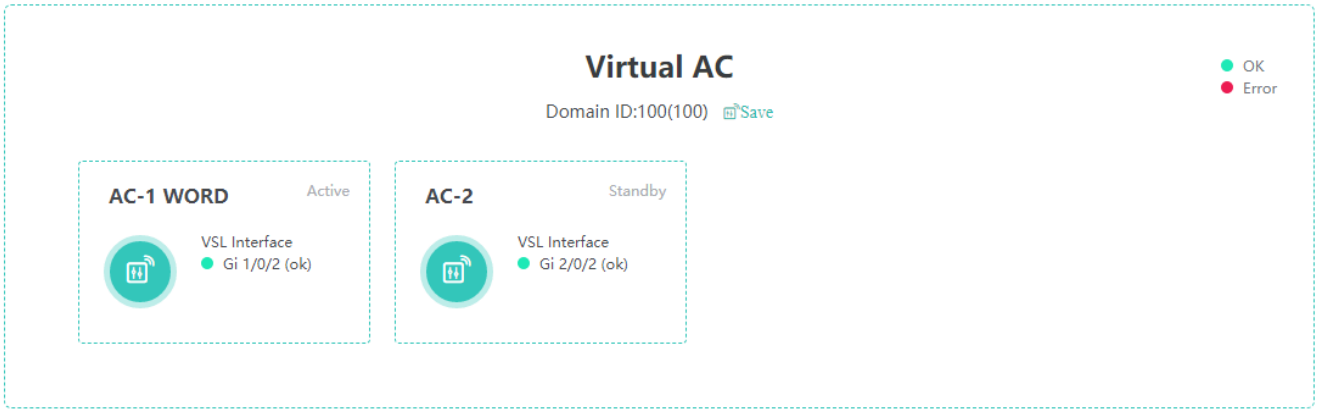
The CPU usage tendency chart, memory usage tendency chart, STA tendency chart, and wireless STA percentage are updated every 30 seconds.

The interface traffic tendency chart is updated every 5 seconds.

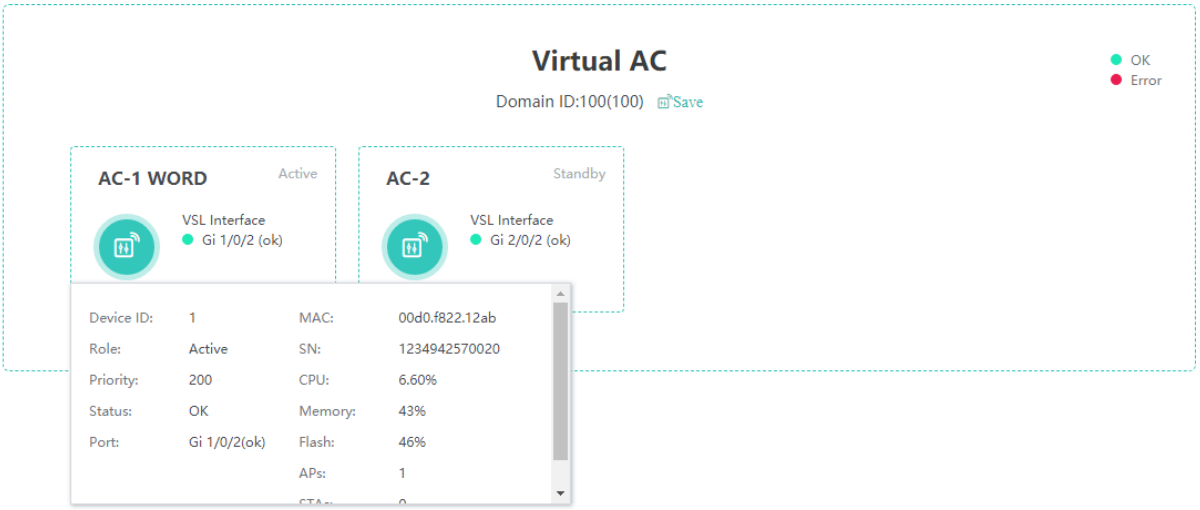
1.3.2.1.2 Virtual AC

The virtual AC function is implemented based on actual configuration. The virtual AC menu is displayed only when a device is configured to work in virtual AC mode and the **device convert mode virtual** command is configured.

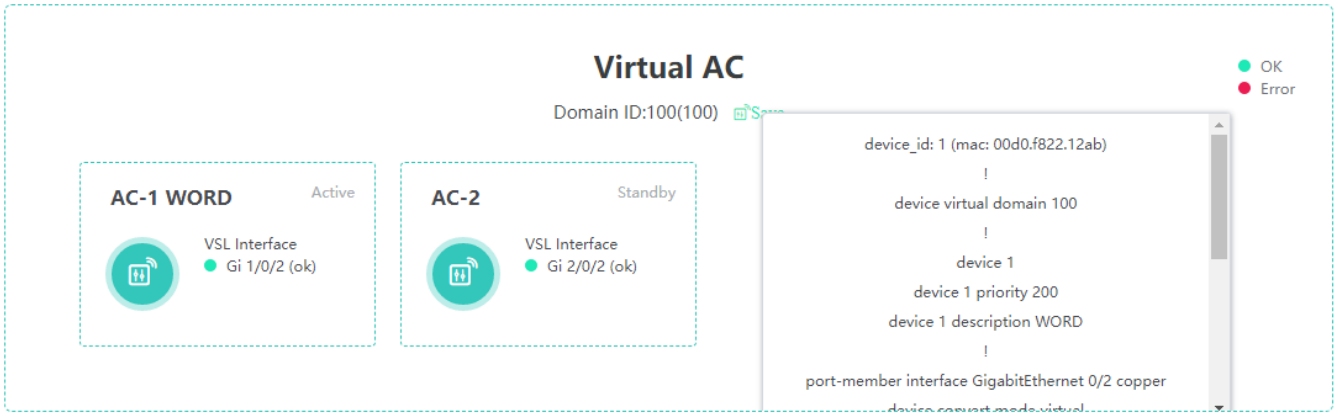
The **Virtual AC** page displays basic information about each current AC member in the virtual AC.



- Displaying information about members of the virtual AC



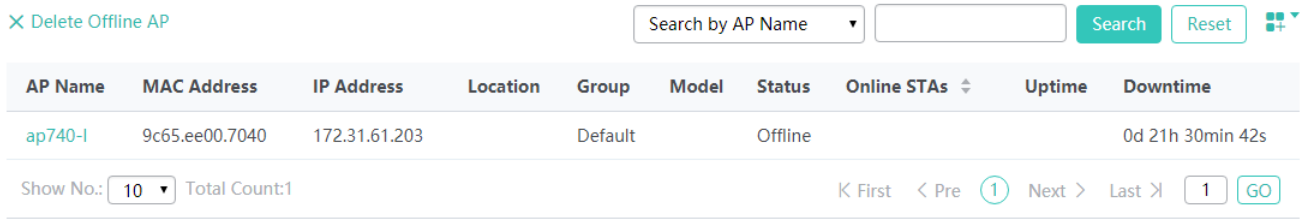
- Displaying device configuration



1.3.2.2 AP

1.3.2.2.1 AP List

The AP list displays basic information about APs associated with the current AC.



- Delete Offline AP

Click **Delete Offline AP**. In the displayed window, click **OK**. A deletion success prompt is displayed.

- Search

You can search for APs by the AP name, MAC address, IP address, location, status, work mode, or AP group.

- Reset

Click **Reset** to reset the search condition.

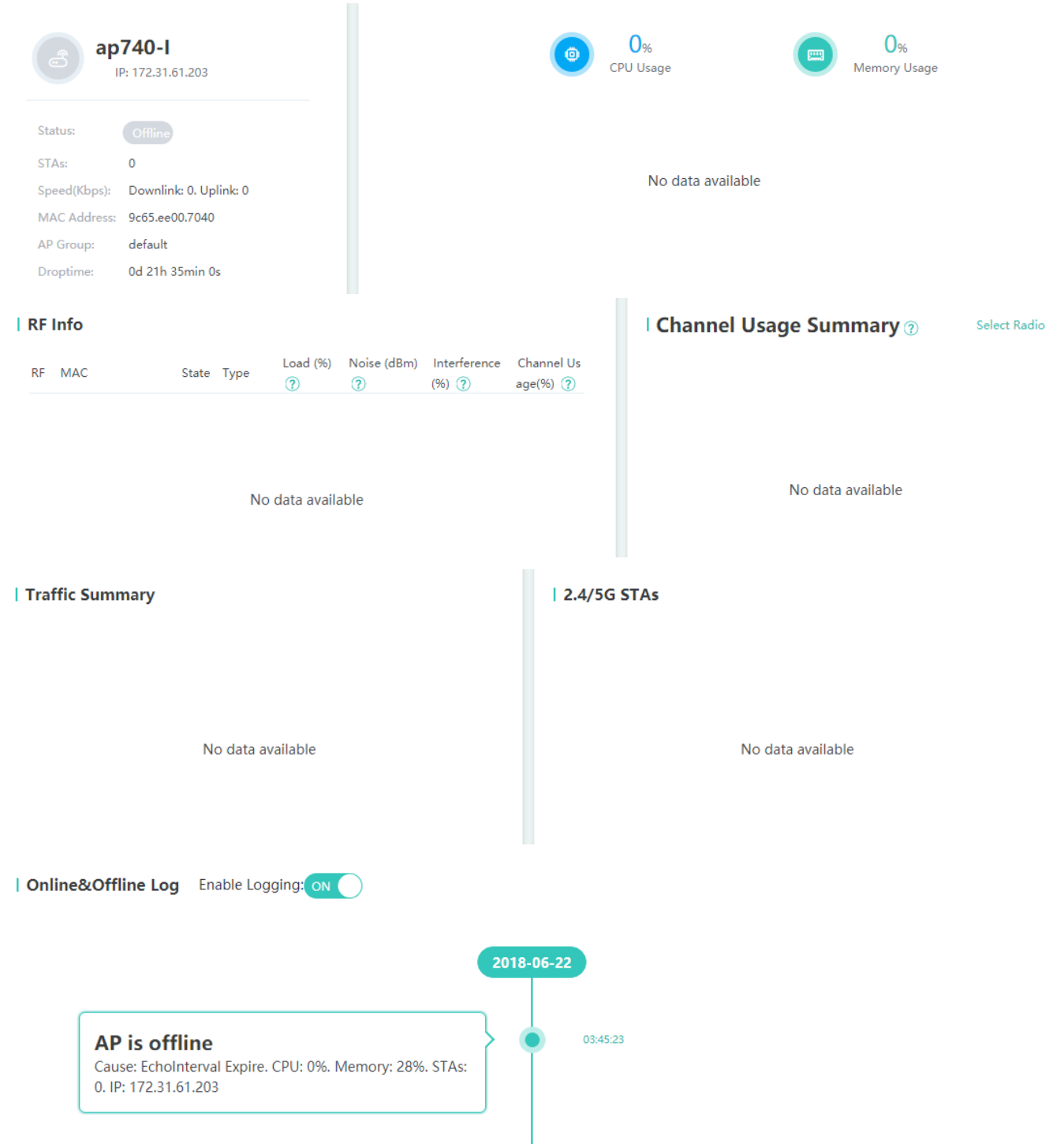
- Displaying more columns

Click . In the displayed window, select columns to be displayed in the AP list.

- Details

Click an AP name in the **AP Name** column. The system redirects to a new page, which displays AP details, as shown in the figure below. Only details about online APs can be viewed.

The details page displays basic AP information, CPU usage tendency, memory usage tendency, uplink and downlink traffic tendency, and online STA tendency. If the log function is enabled, AP go-online/offline history records are displayed, as shown in the figure below.



RF Info

RF Info displays the radio ID, MAC address, status, radio type, load, interference, channel usage, and noise of the AP.

Channel Usage Summary

Channel Usage Summary displays the channel usage tendency.

Traffic Summary

Traffic Summary displays traffic tendency of AP wired interfaces.

2.4G/5G STAs

2.4G/5G STAs displays the tendency of STAs associated with the AP.

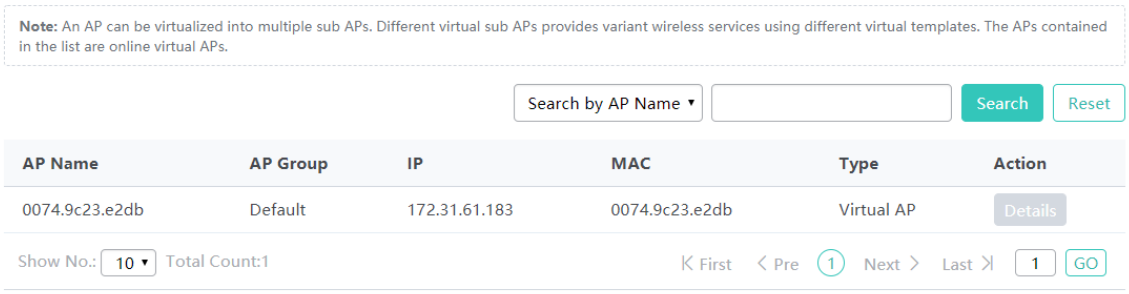
Online&Offline Log

Online&Offline Log displays the history records of the AP, AP go-online/offline causes, memory usage and CPU usage of the AP, and the number of STAs associated with the AP.

1.3.2.2.2 Virtual AP

- Virtual AP

The virtual AP list displays basic information about virtual APs.



- Search

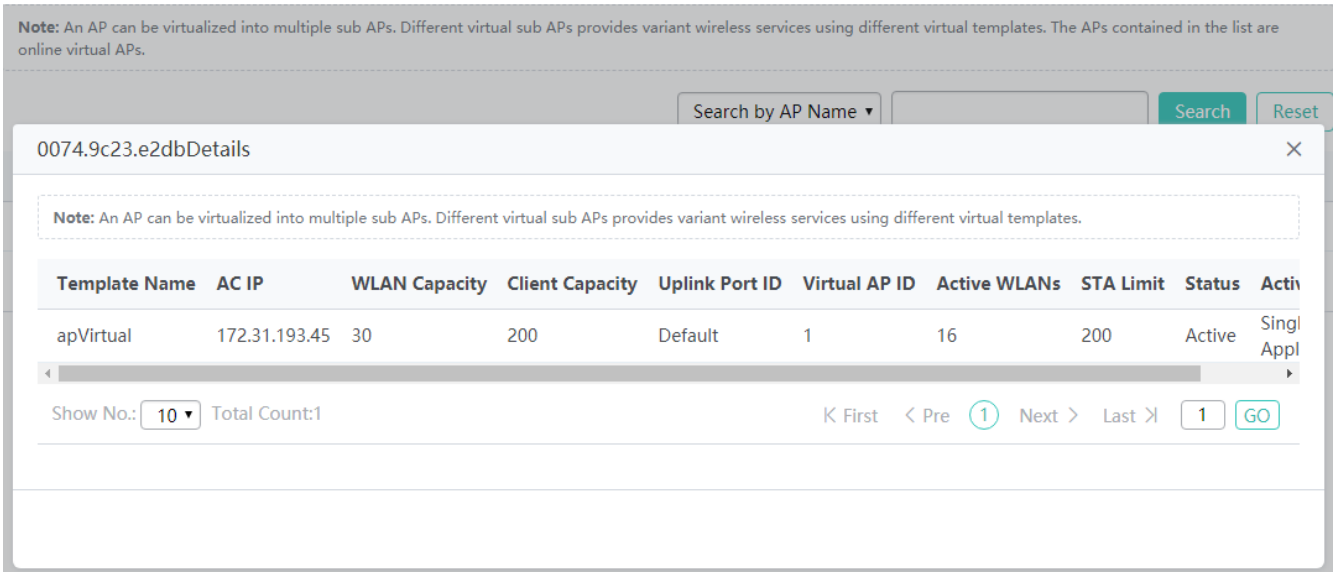
You can display information about the virtual AP by the AP name, IP address, MAC address, or AP type.

- Reset

Click **Reset** to reset the search condition.

- Details

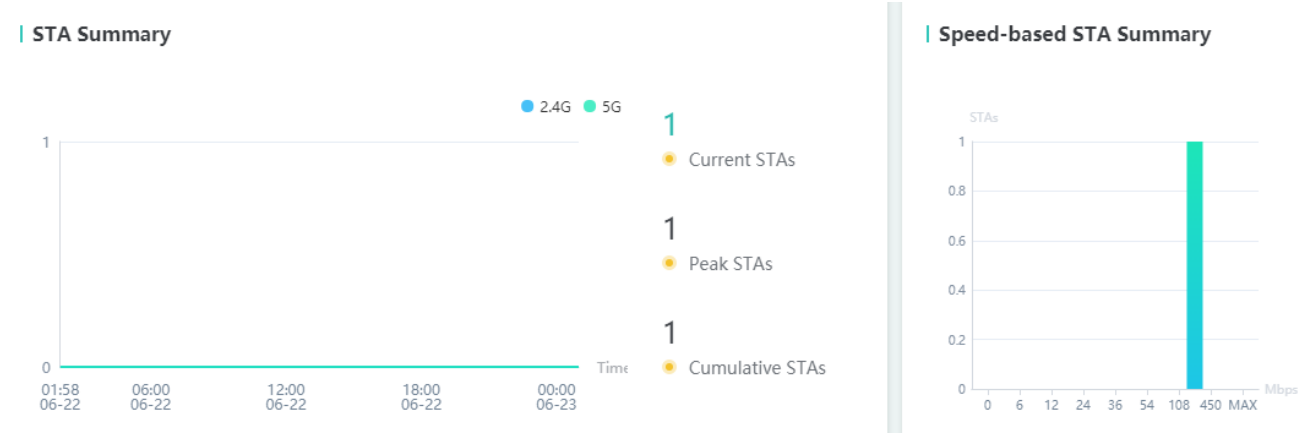
Click **Details** in the list to display details about the virtual AP.



1.3.2.3 STA

1.3.2.3.1 STA Overview

STA Overview displays STA statistics from various dimensions.



STA Summary

The **STA Summary** tendency chart displays the tendencies of 2.4 GHz and 5 GHz WiFi STAs.

Current STAs: Displays the number of current online STAs.

Peak STAs: Displays the maximum number of online STAs within 24 hours.

Cumulative STAs: Displays the cumulative number of online STAs within 24 hours (counted once for a user that logs in repeatedly).

Speed-based STA Summary

Speed-based STA Summary collects statistics of STAs in a bar chart based on the speeds negotiated for STAs in a bar chart. After you click the bar chart, the system redirects to user information.

SSID Summary

SSID Summary displays the percentage of STAs associated with WiFi networks. After you click the pie chart, the system redirects to the STA list.

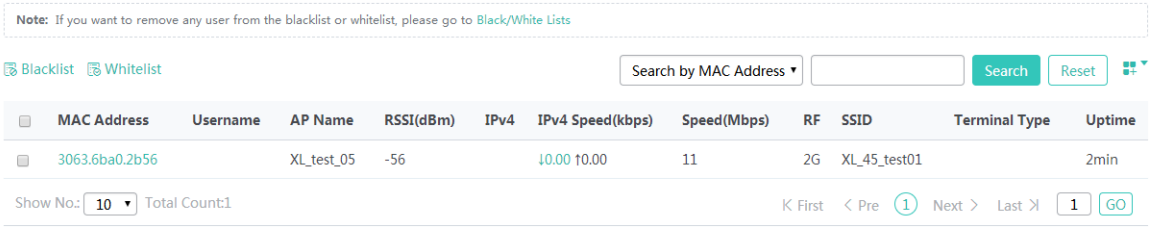
Uptime-based STA Summary

Uptime-based STA Summary collects statistics of STAs based on online duration. After you click the bar chart, the system redirects to the STA list.

The charts above are updated once every 30 seconds.

1.3.2.3.2 STA List

The STA list displays basic information about online STAs.



- Search

You can search for required STAs by the AP name, MAC address, username, IP address, speed, uptime, RSSI, or SSID.

- Reset

Click **Reset** to reset the search condition.

- Displaying more columns

Click  . In the displayed window, select columns to be displayed in the STA list.

- Blacklist

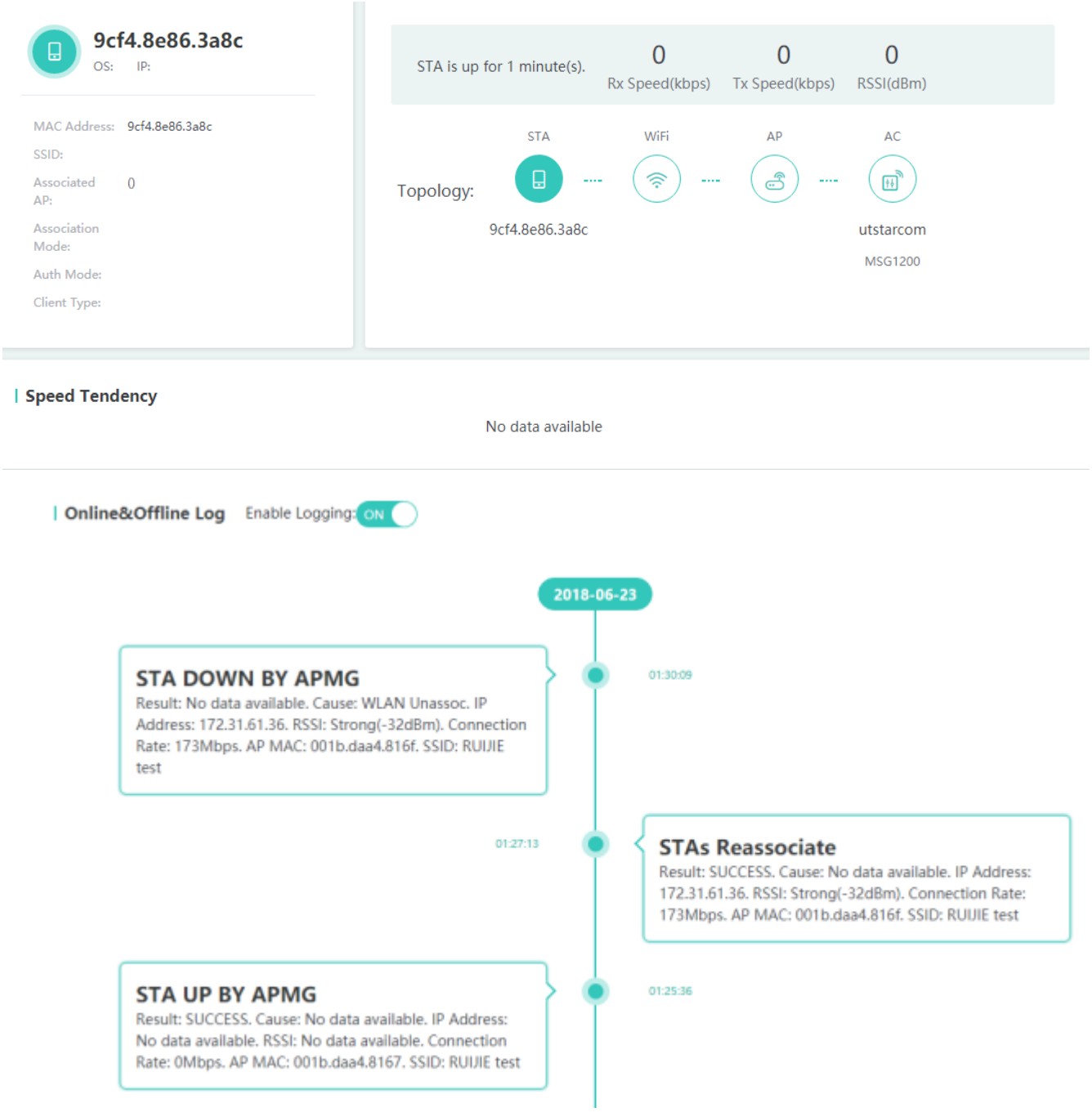
Select an entry in the STA list, and click **Blacklist** to blacklist a STA.

- Whitelist

Select an entry in the STA list, and click **Whitelist** to whitelist a STA.

- Details

Click an entry in the **MAC Address** column in the STA list to display the STA details, as shown in the figure below.



Basic information

Basic information about a STA includes the MAC address, associated WiFi SSID, associated AP, authentication mode, and client type of the STA.

Topology

The topology displays the associated WiFi network, AP, and AC of the STA.

Speed Tendency

Speed Tendency displays the tendency of the STA speed.

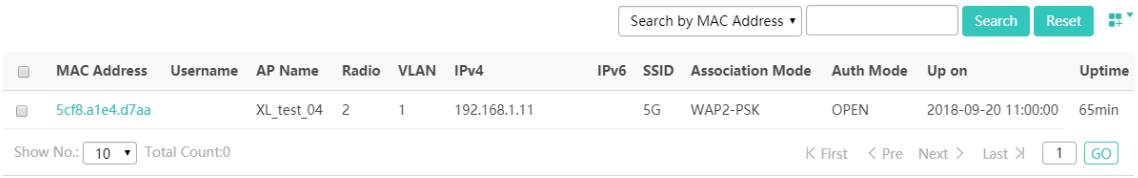
Online&Offline Log

Online&Offline Log displays the STA go-online/offline history records.

1.3.2.3.3 STA List of a Branch AC

The STA list displays basic information about online STAs associated with APs connected to a branch AC.

Note: This function is available only in the central AC.



- Search

You can display information about STAs associated with APs connected to a branch AC by the MAC address, AP name, user name, or IP address.

- Reset

Click **Reset** to reset the search condition.

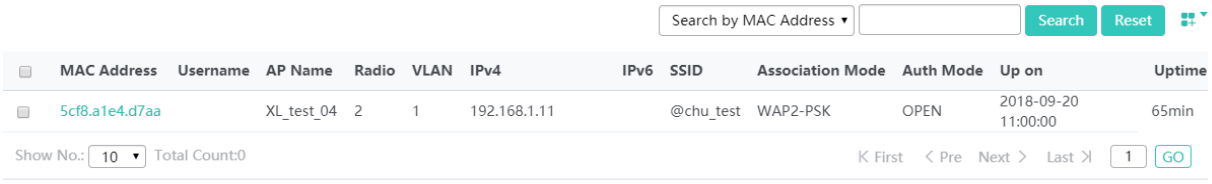
- Displaying more columns

Click . In the displayed window, select columns to be displayed in the STA list.

1.3.2.3.4 Backup STA List

The backup STA list displays basic information about online STAs backed up from the master AC in AC hot backup scenarios.

This function is available only in AC hot backup scenarios.



- Search

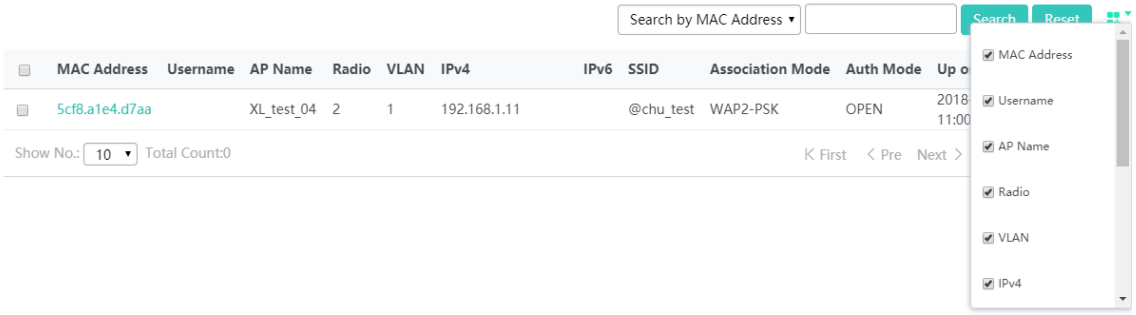
You can query the backup STA list by the MAC address, IP address, authentication mode, or AP name.

- Reset

Click **Reset** to reset the search condition.

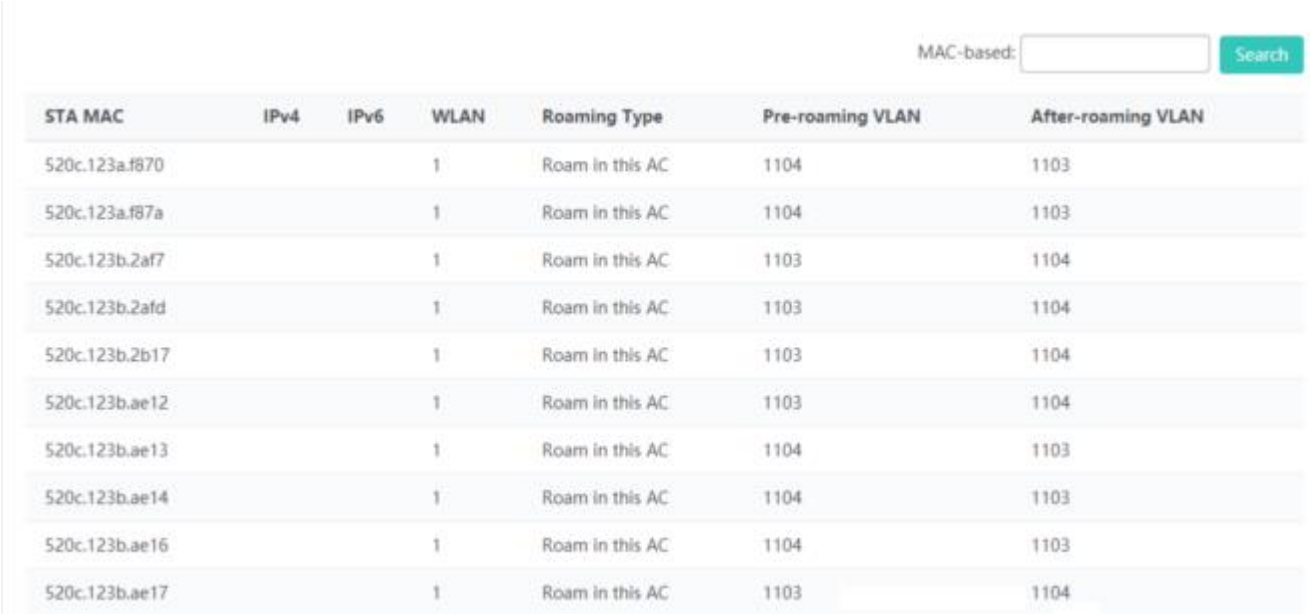
- Displaying more columns

Click  . In the displayed window, select columns to be displayed in the backup STA list, as shown in the figure below.



1.3.2.3.5 Roaming Information List

The roaming information list displays the statuses of STAs roaming in an AC, as shown in the figure below.

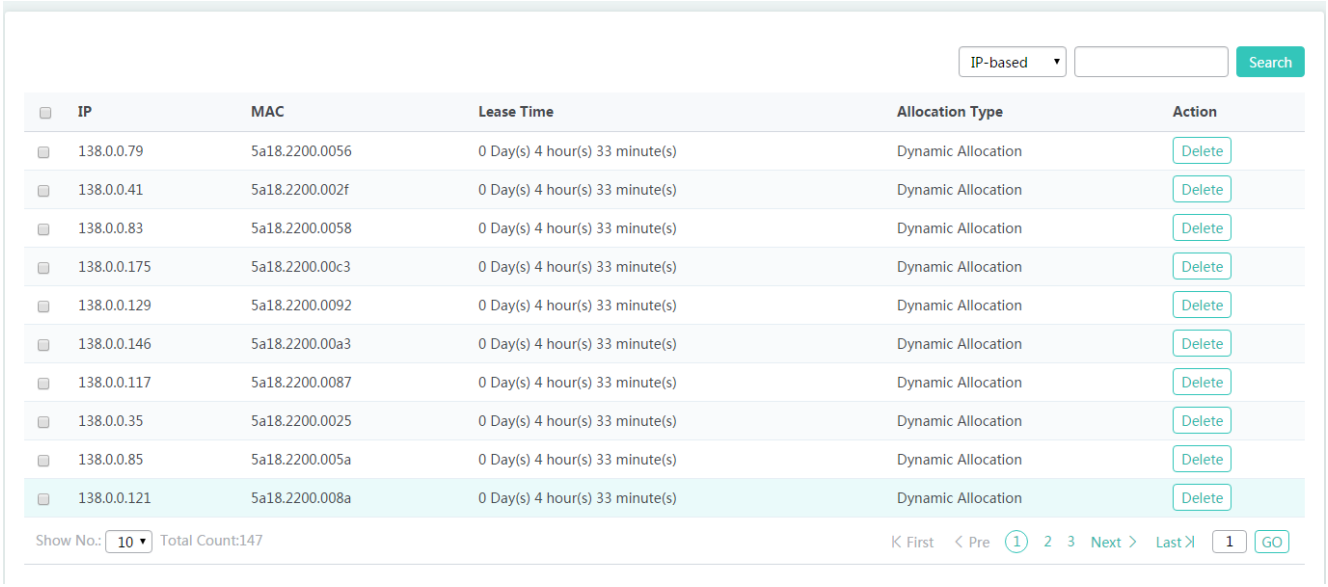


1.3.2.4 DHCP

DHCP monitoring is performed from two dimensions: DHCP server status and DHCP client list.

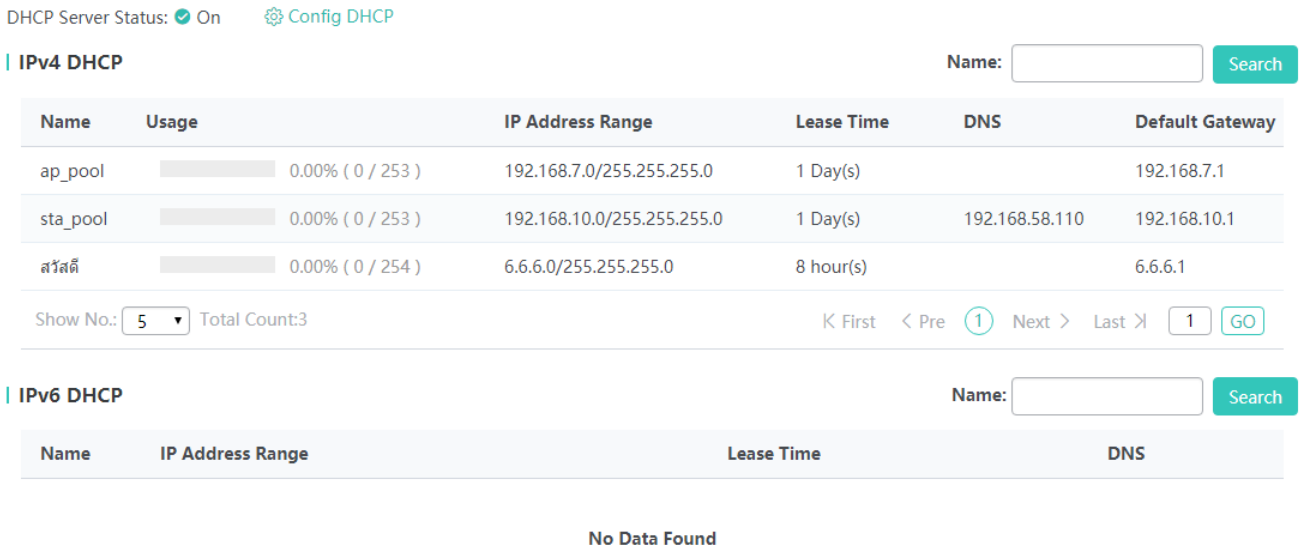
1.3.2.4.1 DHCP Client List

The DHCP client list displays addresses allocated by the DHCP server on an AC to STAs.



1.3.2.4.2 DHCP Server Status

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



1.3.3 Configuration

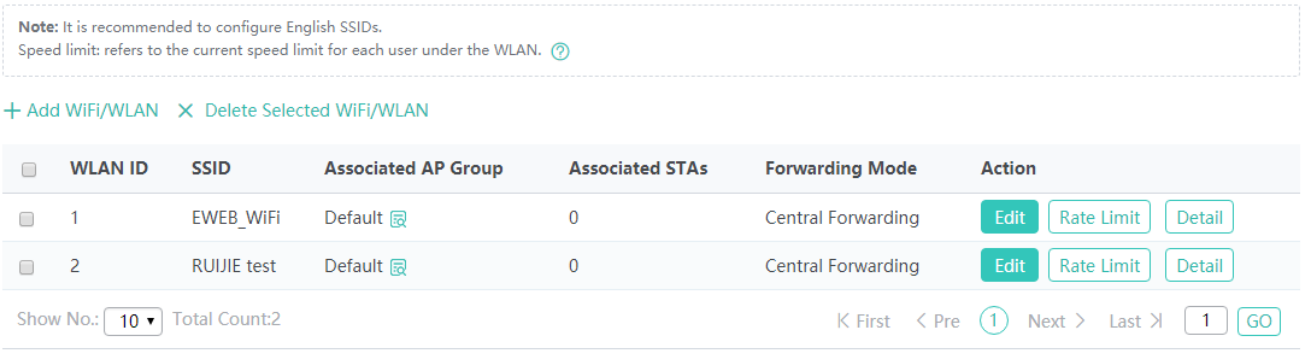
You can choose the level-1 menu **Configuration** to access the following level-2 menus: **WLAN**, **AC**, **AP**, **Network**, **Security**, **Auth**, **Optimization**, **Solution**, and **Advanced**.

1.3.3.1 WLAN

1.3.3.1.1 WiFi/WLAN Adding

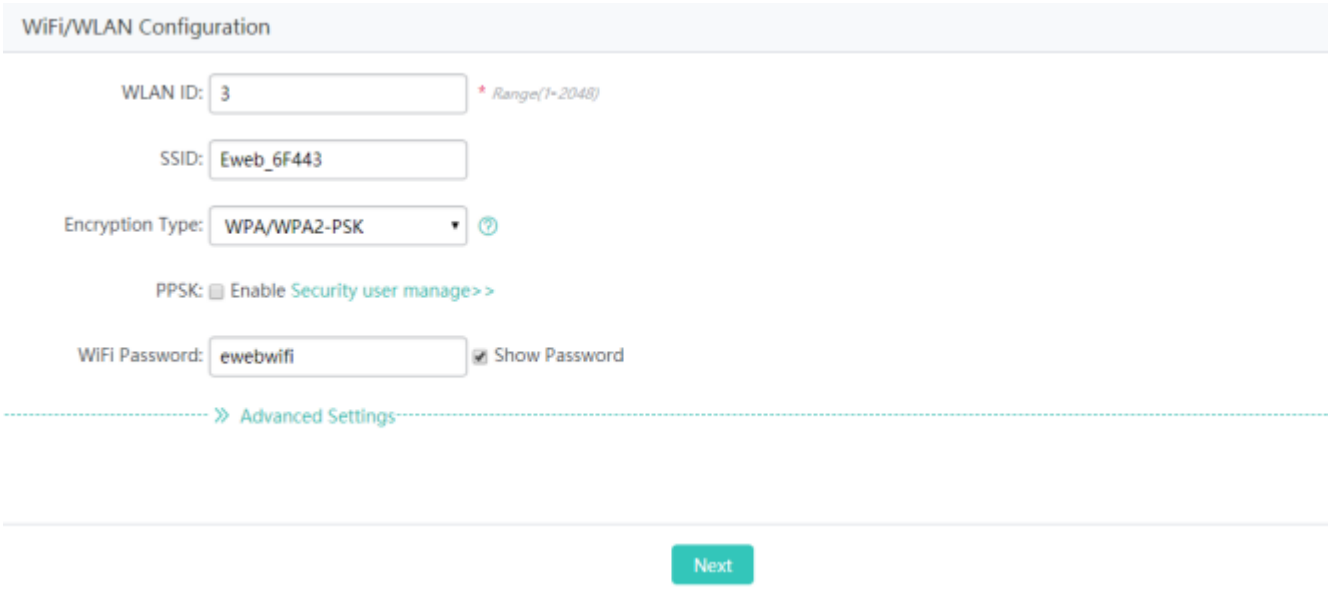
WLANs aim to enable wireless STAs to access an AP via WiFi for Internet access. A maximum of 4094 WLANs can be configured (the quantity depends on the actual capacity of the device) and WLANs can be deleted.

The figure below shows the page for adding a WLAN.



- Adding a WLAN

Click **Add WiFi/WLAN** to add a WLAN, as shown in the figure below.



Encryption Type

Open: No password is needed for associating with a STA with a WiFi network. No encryption mode is configured.

WPA/WPA2-PSK (universal edition): shared key-based WPA mode, enabling high security and easy configuration. This mode is applicable to common home users and small-sized enterprises. **WPA/WPA2-802.1x** (professional edition): WPA or WPA2 security mode in which a RADIUS server is used for identity authentication and key acquisition. This mode is not

recommended for common users because a dedicated authentication server needs to be deployed, which is costly and incurs complex maintenance.

Advanced Settings

Packet Forwarding

Centralized Forwarding: All data is transmitted to the AC for forwarding. **Packet Forwarding** is set to **Centralized Forwarding** by default.

Local Forwarding: Data is directly sent out by the switch, which alleviates the load of the AC.

SSID code

utf-8: Most clients support UTF-8 by default. Therefore, UTF-8 is recommended for the Web-based management system by default and the SSID name of transmitted signals is encoded using UTF-8.

gbk: The network adapters of some clients and PCs support the GBK encoding mode.

The encoding mode is specified by users.

Hide SSID

Hide SSID is used to specify whether the WiFi SSID is visible. The WiFi SSID is visible by default.

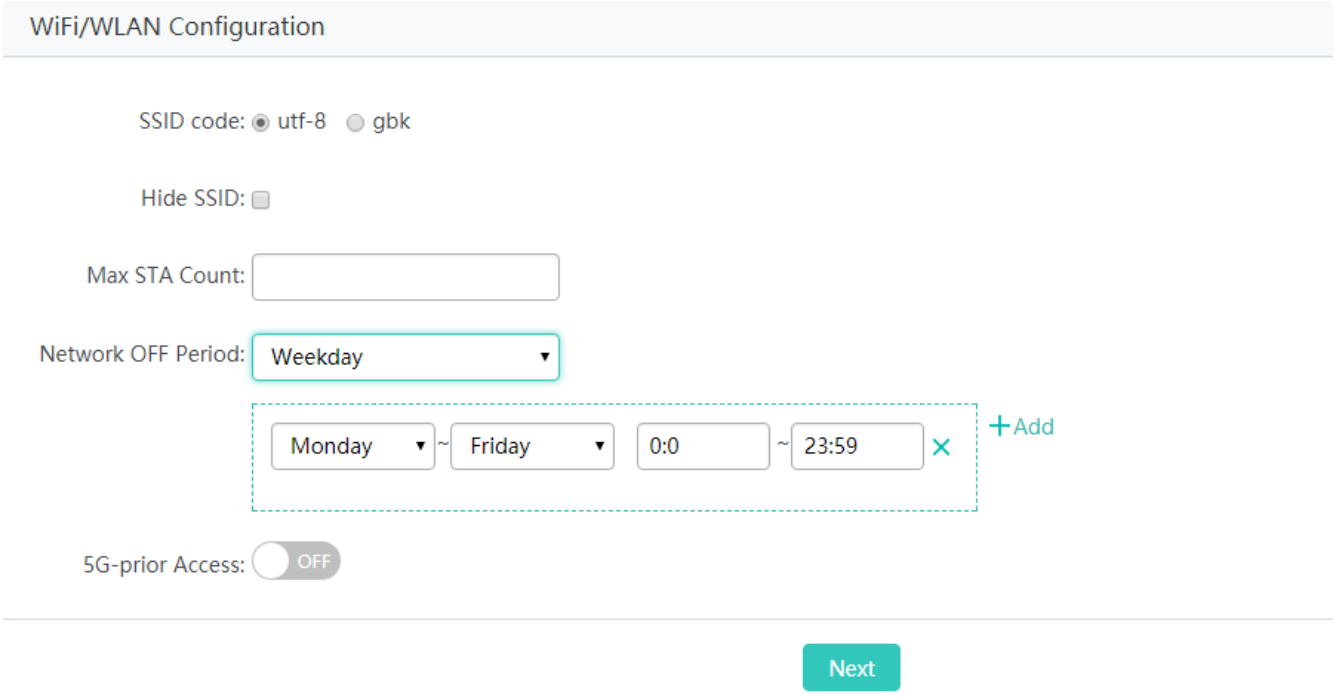
Max STA Count

Max STA Count indicates the maximum number of associated STAs supported by the current WiFi network. It is not configured by default, indicating that the number of associated STA connections is unlimited.

Network OFF Period

Network OFF Period is used to disable the WiFi network within the specified time period. **Network OFF Period** is disabled by default.

It can be set as required in a specified scenario. For example, if the WiFi service does not need to be provided during classes, perform configuration as shown in the figure below.

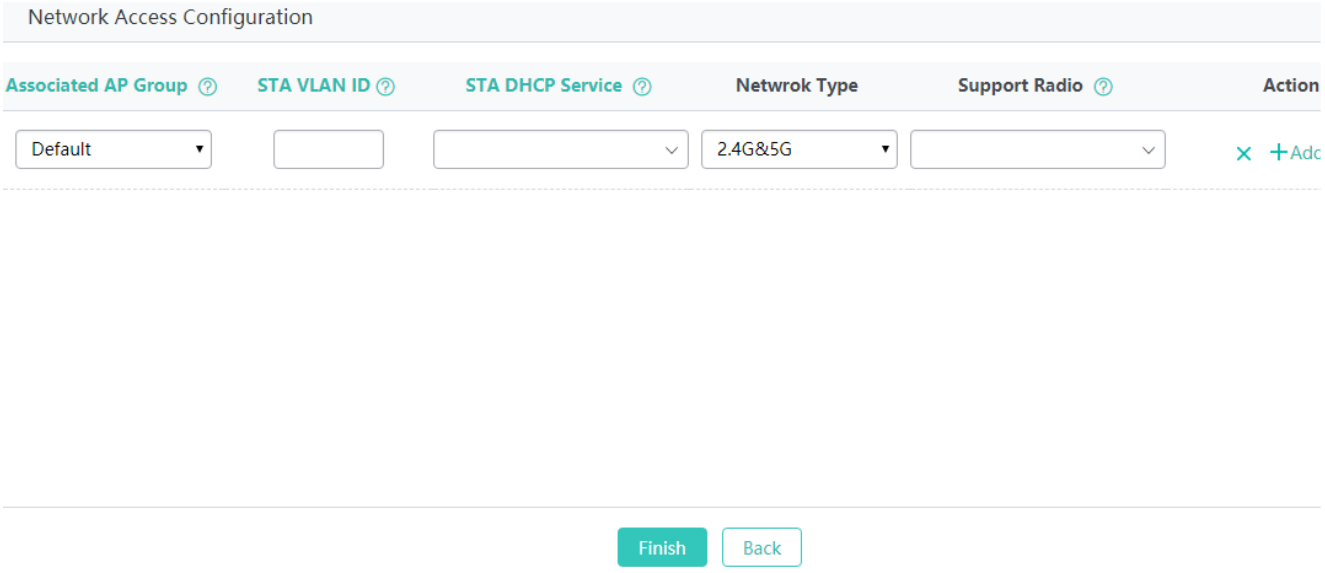


5G-prior Access

If the 5G-prior access function is enabled, STAs preferentially access a 5G network. The function is disabled by default.

The network access configuration of wireless STAs includes the following:

- Allocation of STA IP addresses from the address pool
- Mapping from a WiFi network to an AP group



Associated AP Group

Indicates the AP group whose APs can transmit signals only after the AP group is associated with the WiFi network. The **default** AP group transmits signals by default. Click **Associated AP Group** to add a new AP group.

STA VLAN ID

Indicates the VLAN to which a STA associated with this WiFi network belongs. Click **STA VLAN ID** to configure VLAN information.

STA DHCP Service

Indicates the address pool used for allocating IP addresses to STAs associated with the WiFi network. The address pool can be configured on the local device or other devices, and is configured on other devices by default. If the address pool is configured on the local device, you need to click **Add DHCP** to add the DHCP service. Click **STA DHCP Service** to add an address pool for STAs.

Network Type

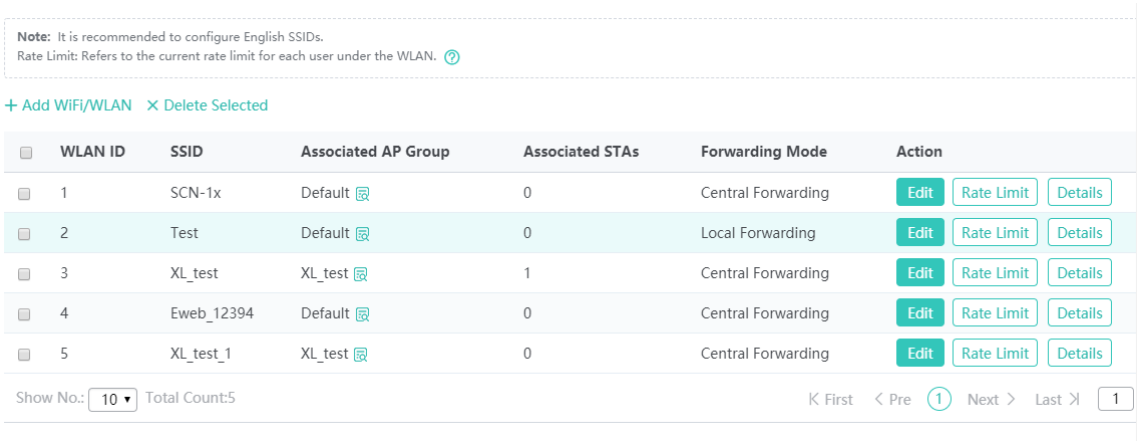
Specifies the network type supported by this WiFi network. Both 2.4 GHz and 5 GHz networks are supported by default.

Support Radio

Specifies the radios supported by APs in the WiFi network. All radios are supported by default.

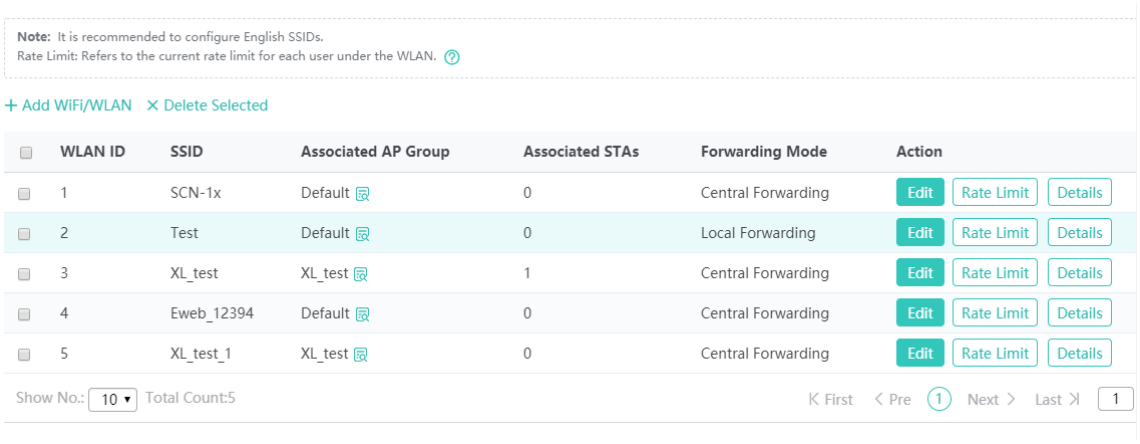
- Batch deleting WLANs

Select WLANs to be deleted from the list, and click **Delete Selected** to delete information about the selected WLANs.



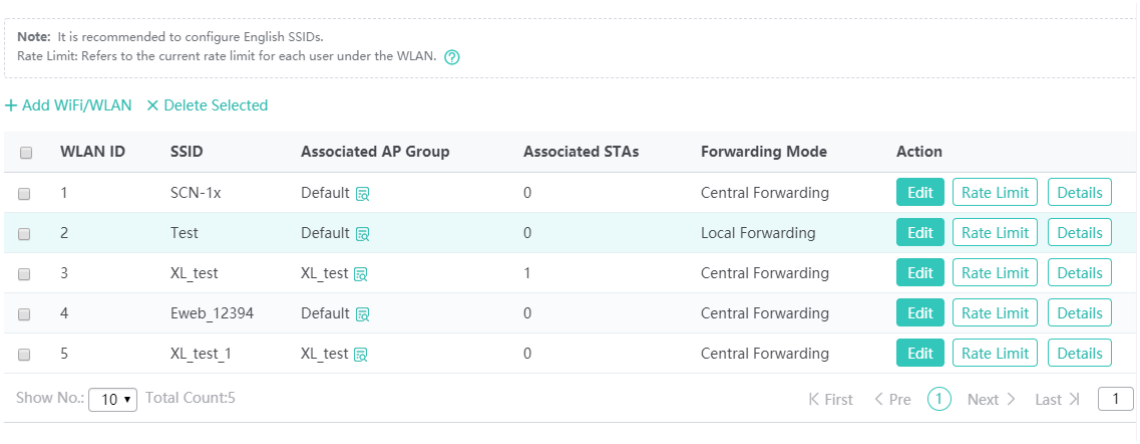
- Displaying an associated AP group

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



- Editing a WLAN

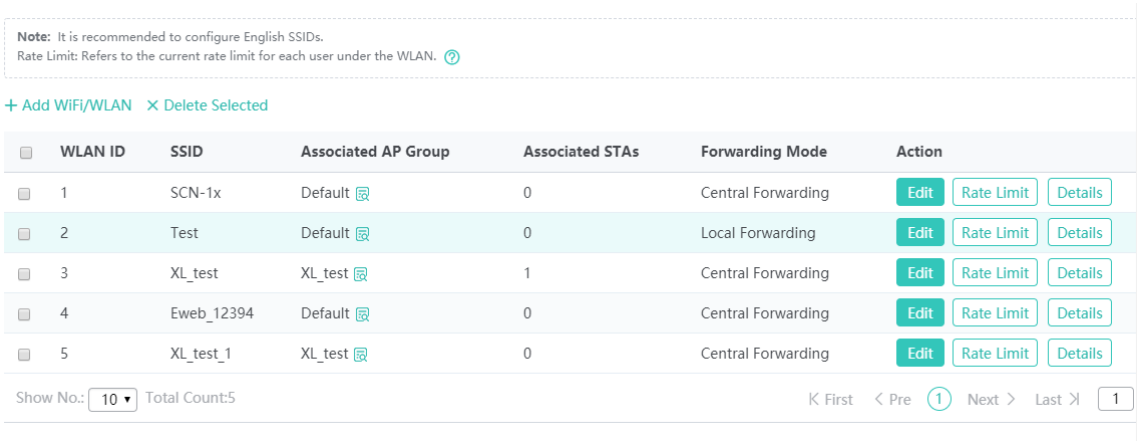
Click **Edit** in the **Action** column. The displayed window shows information about the WLAN. Edit information such as adding a description about the WiFi network, and click **Finish**. A setting success prompt is displayed.



The parameters for editing a WLAN are the same as those for adding a WLAN and are not described again.

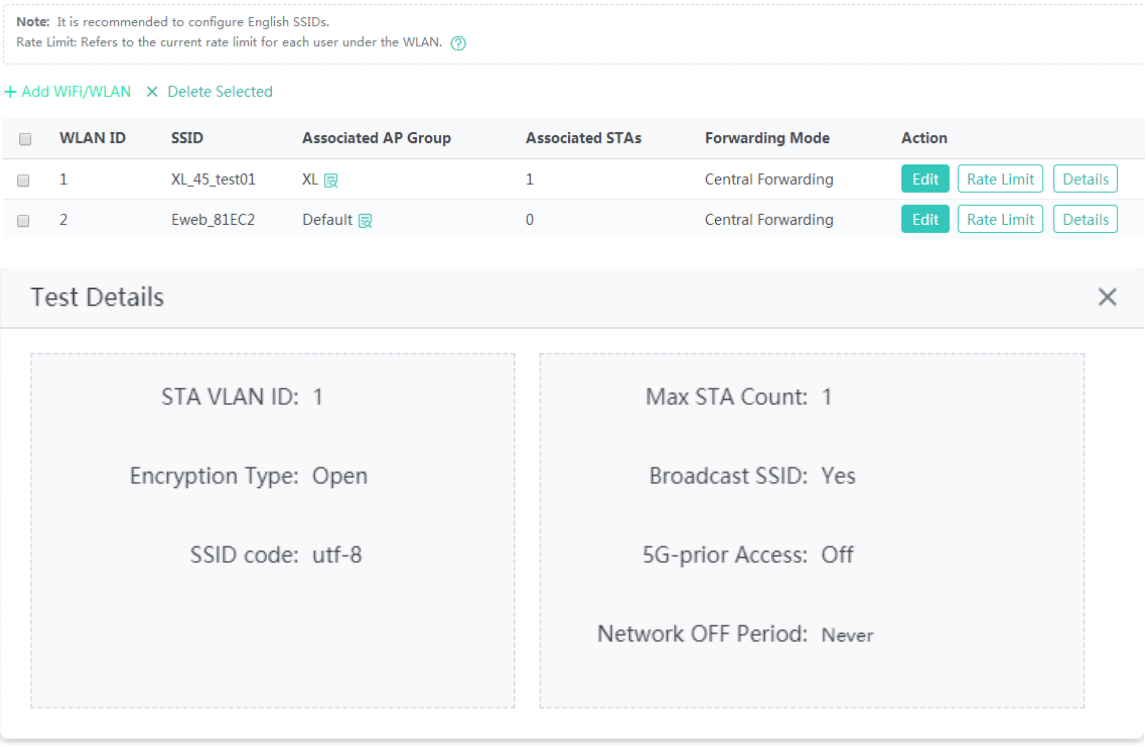
- Rate Limit

Click **Rate Limit** in the **Action** column. A window for configuring the WLAN rate limit is displayed. Modify the related value and click **Save**. A setting success prompt is displayed.



- Detail

Click **Details** in the **Action** column. Details about the WLAN are displayed.

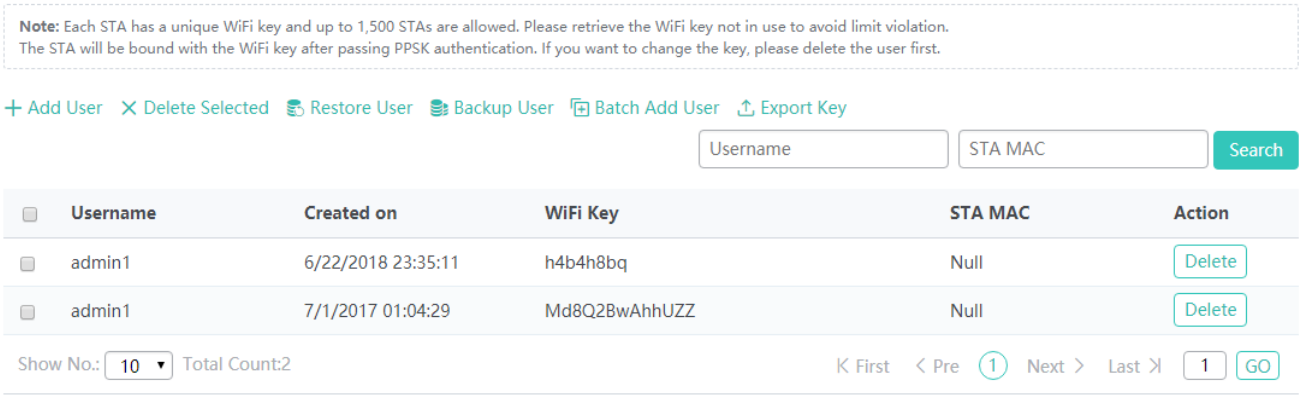


1.3.3.1.2 PPSK Management

Administrators can set Internet access accounts on the PPSK page. PPSK supports a maximum of 1500 keys. Multiple keys can be generated for one username. One unique key is automatically allocated to only one username. The number of keys of one user is unlimited.

To enable the PPSK management function, set **Encryption Type** to **WPA/WPA2-PSK** for one WLAN and enable PPSK on the page of adding a WLAN. PPSK can be enabled for only one WLAN ID.

The figure below shows the PPSK account management page.

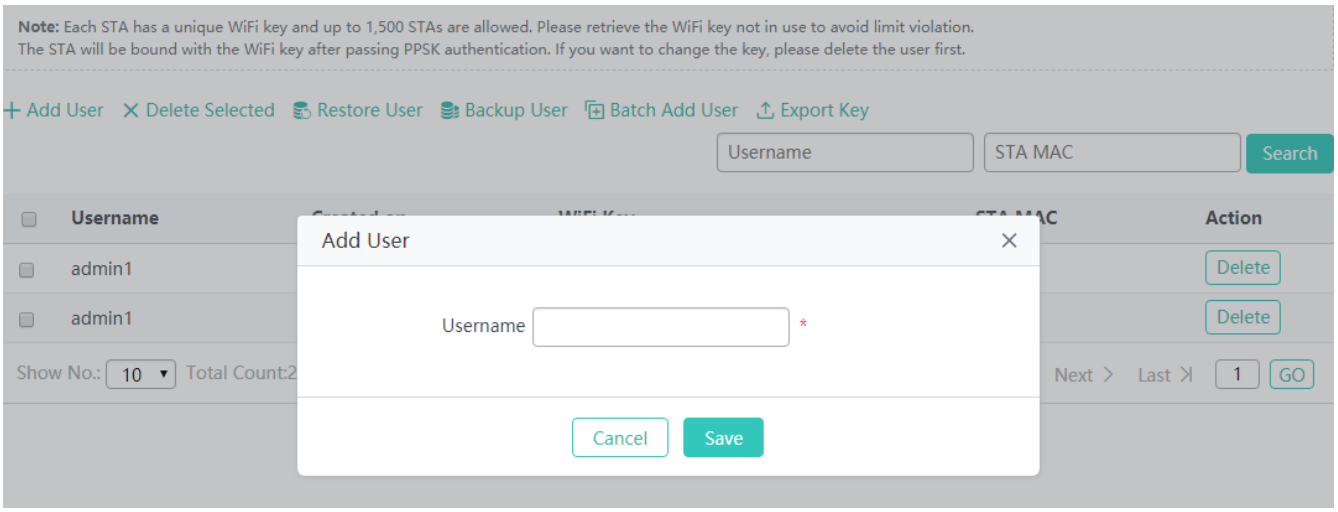


WiFi Key: Indicates the password generated by the device when a user is added. WiFi keys are not duplicated. Ensure that each device has a key.

STA MAC: Indicates the MAC address of a STA that logs in with this account.

- Adding a user

Enter a username to add a user. One username can be added multiple times. One unique key is generated each time a username is added.

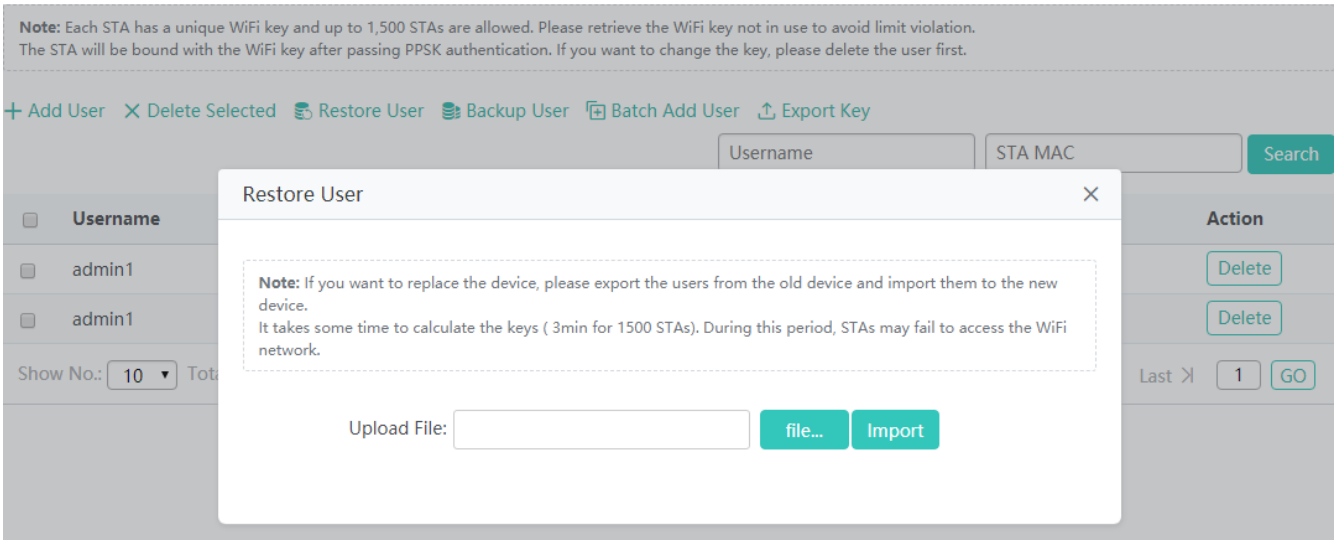


- Deleting a user

Select users to be deleted and click **Delete Selected** to batch delete users. Click **Delete** in the **Action** column to delete a single user.

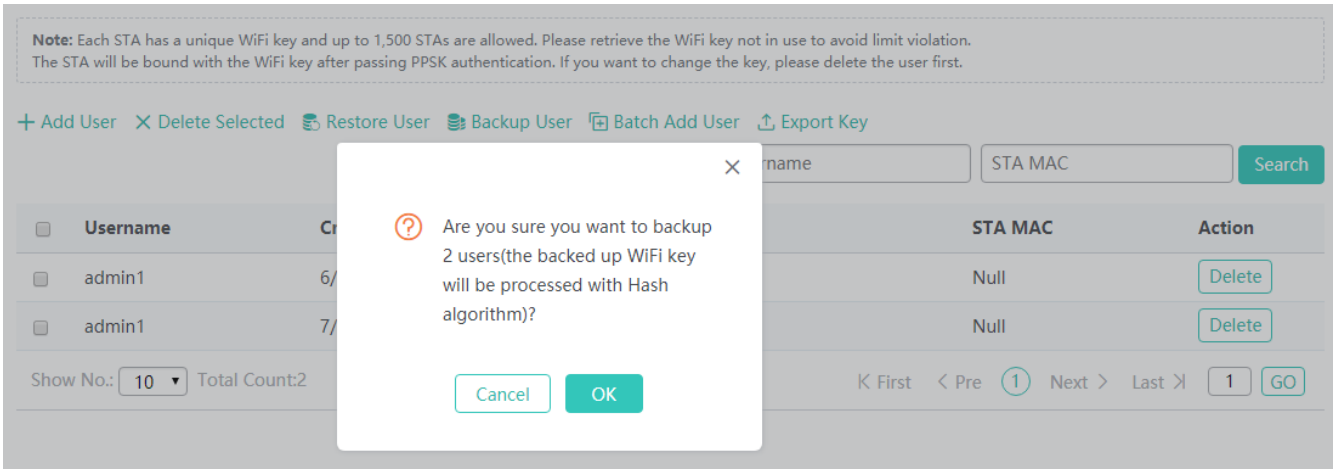
- Restoring data

Click **Restore User**. In the displayed window, import a backup file to restore data.



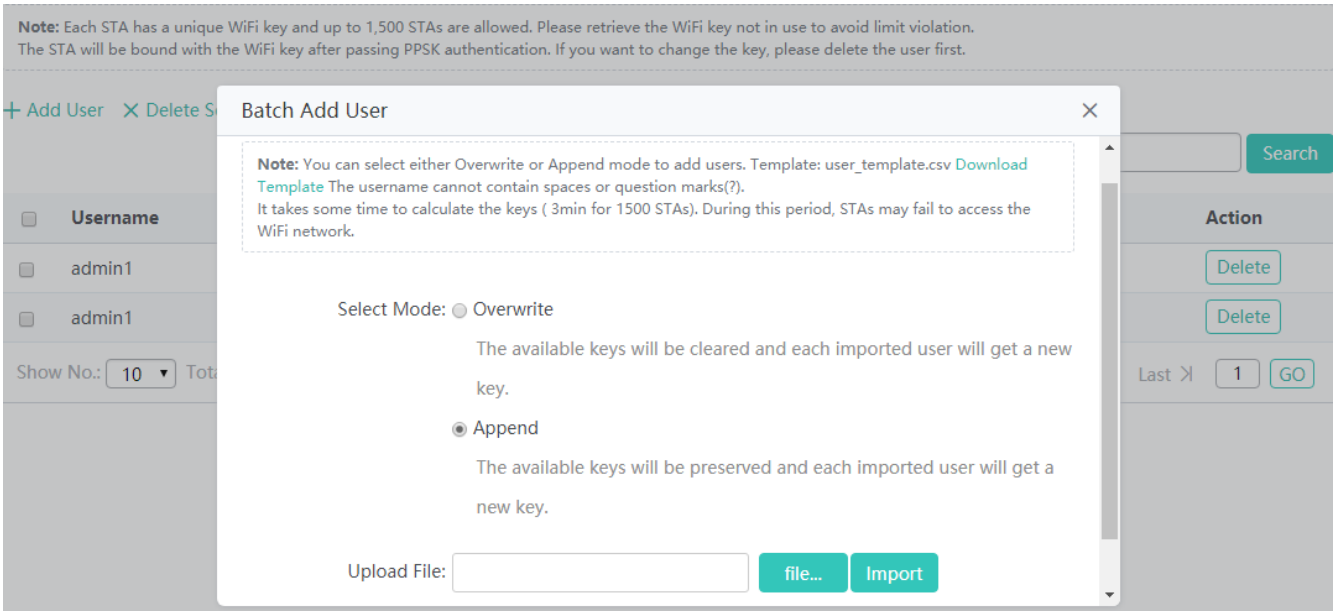
- Backing up data

Click **Backup User**. In the displayed window, click **OK** to download data to the local PC. Exported data can be imported into other devices.



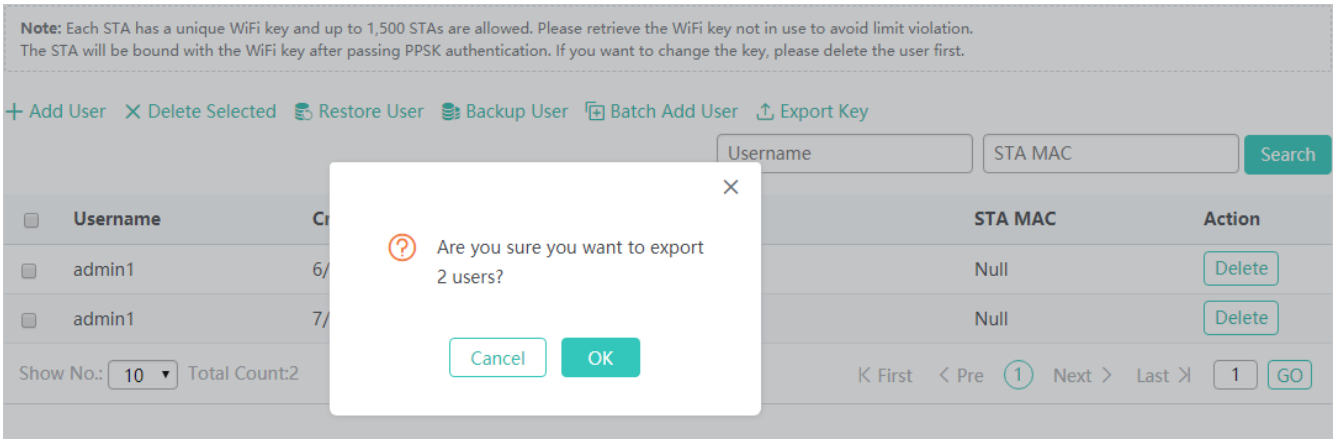
- Batch importing data

Click **Batch Add User**. In the displayed **Batch Add User** window, click **Download Template** to download a template, edit and modify the template and add users. Then, select the batch adding mode to import user data to the device.



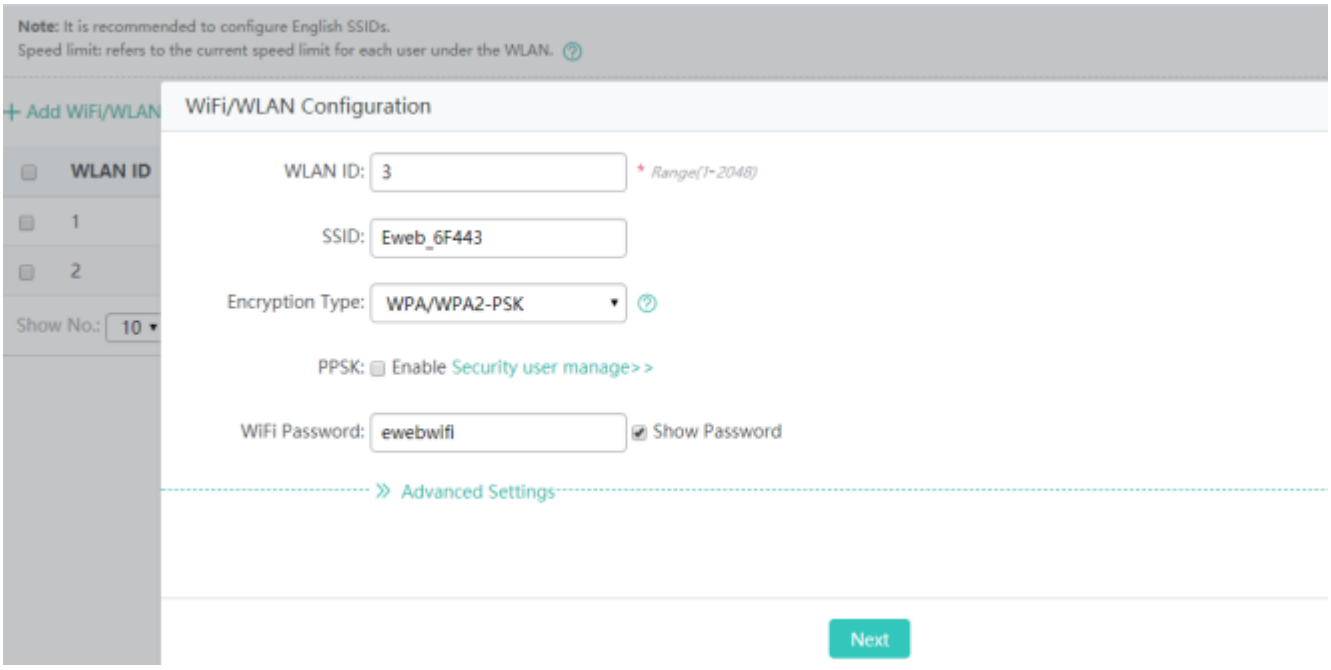
- Exporting a key

Click **Export Key**. In the displayed prompt box, click **OK** to export data.

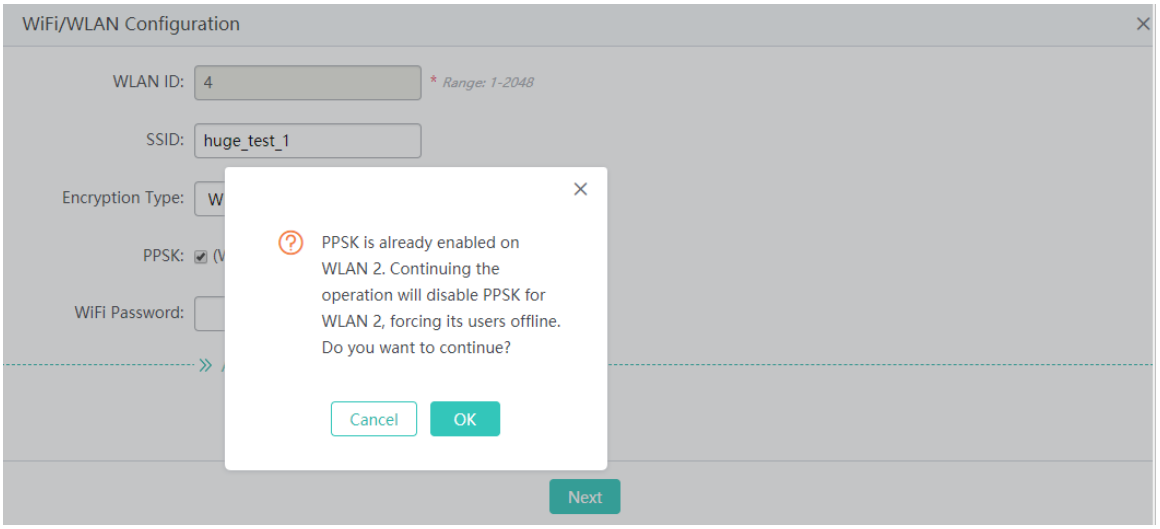


Note: The PPSK configuration function is available only on PPSK-supported devices. PPSK can be enabled for a WLAN ID only when a WiFi/WLAN is added/edited. Choose **WLAN** > **Add WiFi/WLAN**, click **Add WiFi/WLAN**, and set **Encryption Type** to **WPA/WPA2-PSK**. The **PPSK** check box is displayed. Select **Enable**, and click **Next** to save the configuration to enable PPSK for the WLAN ID. PPSK can be enabled for only one WLAN ID, as shown in the figure below.

- Applying PPSK



Note: PPSK can be applied to only one WLAN ID. Therefore, when a WLAN ID is added/edited, if PPSK is already enabled for an existing WLAN ID and needs to be applied to the newly added WLAN ID, a prompt shown in the figure below is displayed.



1.3.3.2 AC

1.3.3.2.1 AC Hot Backup/Cluster

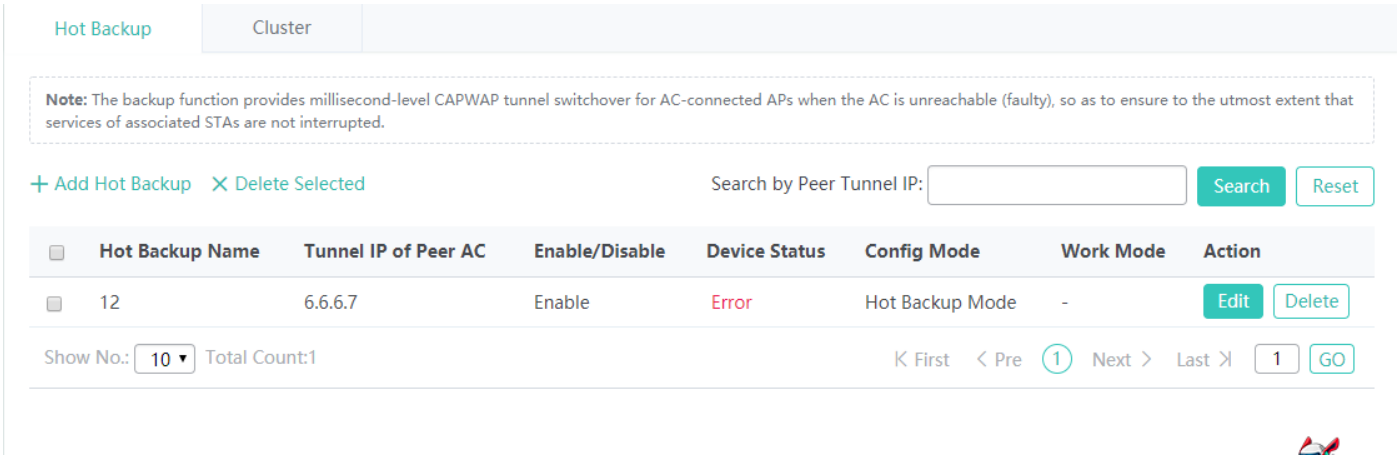
The AC hot backup/cluster function is provided on the AC hot backup/cluster page. The AC hot backup/cluster page contains the **Hot Backup** and **Cluster** tab pages.

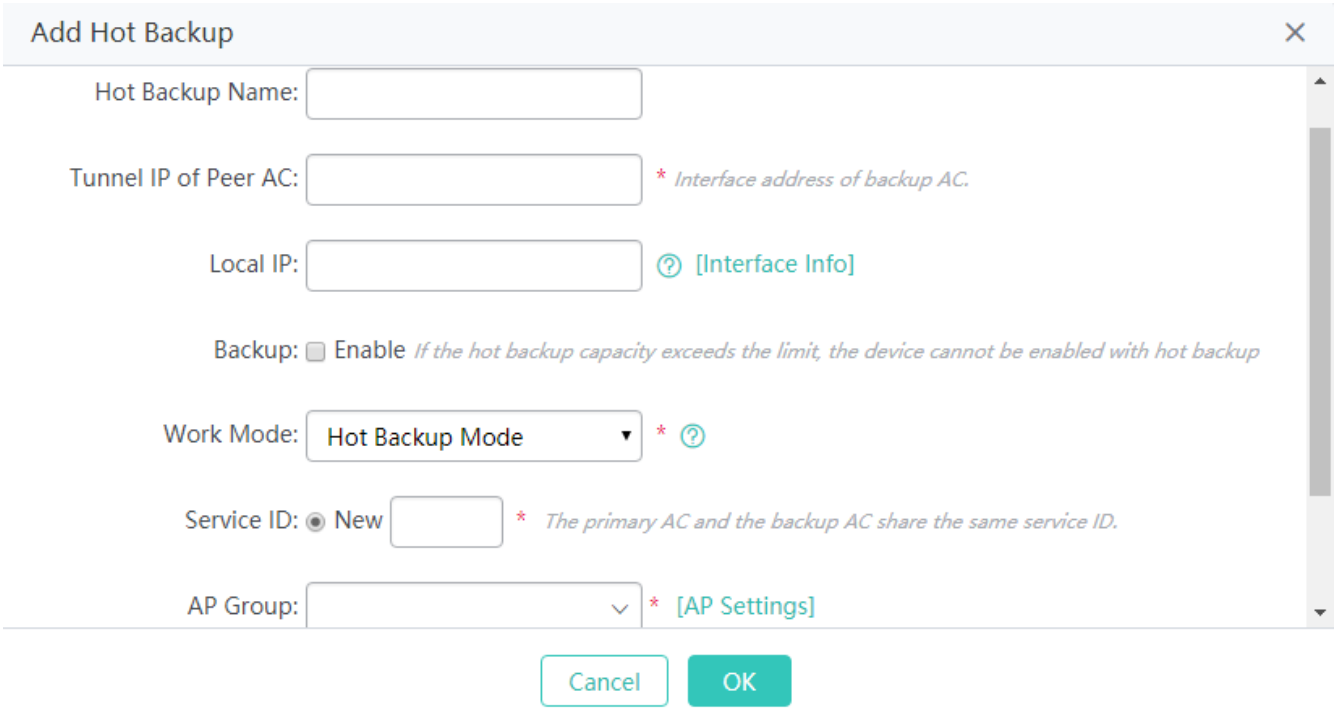
Hot Backup

In the fit AP architecture, the AP needs to establish a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel with an AC for normal operation. The hot backup function implements CAPWAP tunnel switching within milliseconds when the AC is unreachable (faulty). STAs can rapidly switch to the standby AC to ensure that services of associated STAs are not interrupted, thereby ensuring the availability and stability of STAs.

- Adding a hot backup

On the **Hot Backup** tab page, click **Add Hot Backup**. The **Add Hot Backup** dialog box is displayed, and you can configure **Hot Backup Name**, **Tunnel IP of Peer AC**, **Work Mode**, **Service ID**, and other information, as shown in the figures below.





Hot Backup Name

Indicates the identifier, description, or alias of the hot backup.

Tunnel IP of Peer AC

Indicates the CAPWAP IP address of the peer hot backup AC. It is used by the AC to establish a tunnel with the AP. Normally, the IP address of the loopback 0 interface is used as the tunnel IP address.

Local IP

When the peer device or local device does not use the loopback 0 interface to perform communication, Local IP needs to be configured.

Local IP is generally set to the interface IP address on the device. You can click **Interface Info** to display the interface IP address.

Backup

Indicates whether to enable hot backup. When the number of hot backups exceeds the limit, hot backup cannot be enabled on the device.

Work Mode

When a normal common AC is used, the work mode can be set to the normal mode or fast switching mode.

When a central AC and branch ACs are configured, the work mode can be set to the normal mode or cold mode.

Description of the work modes:

Normal mode: This mode is applied in actual application scenarios, in which stable running is required to prevent hot backup oscillation. This mode is recommended in normal cases.

Fast switching mode: This mode is mainly applied in scenarios with very high switching performance requirements. Frequent hot backup switching may be incurred in this mode.

Cold mode: This mode is applied in hierarchical AC scenarios.

Service ID

A service ID is the context ID and is mandatory.

AP Group

The AP groups on the master and slave hot backup devices must be consistent. Click **AP Settings** to redirect to a page for adding an AP group for the current device.

Advanced Settings

Advanced settings are not supported in the VAC scenario and hierarchical AC scenario (with the central AC and branch ACs).

Only common ACs support advanced settings.

VRRP

The VRRP group on the master and slave hot backup devices must be consistent. Click **VRRP** to redirect to a page for adding VRRP to the current device.

DHCP

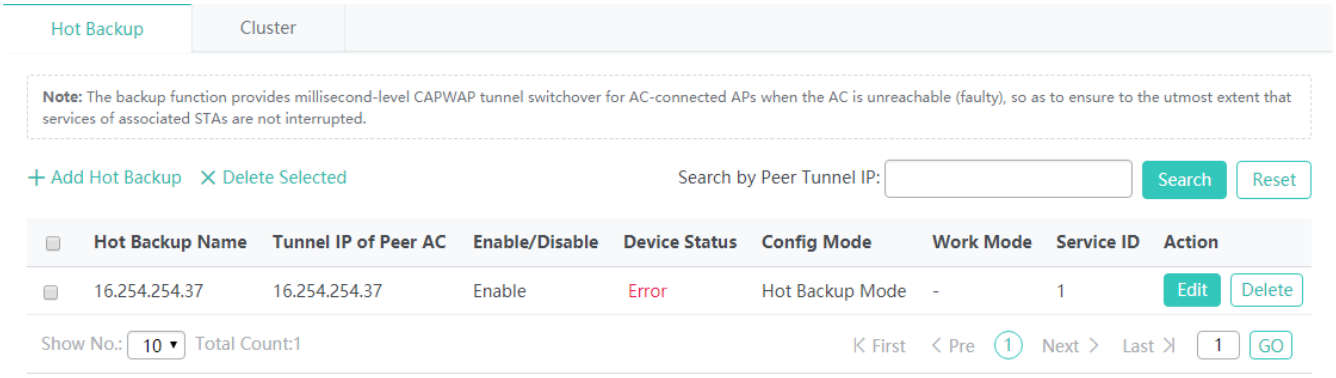
The DHCP configurations on the master and slave hot backup devices must be consistent. Click **DHCP** to redirect to a page for adding DHCP to the current device.

Priority

Indicates the hot backup priority, which can be set to high, medium, or low.

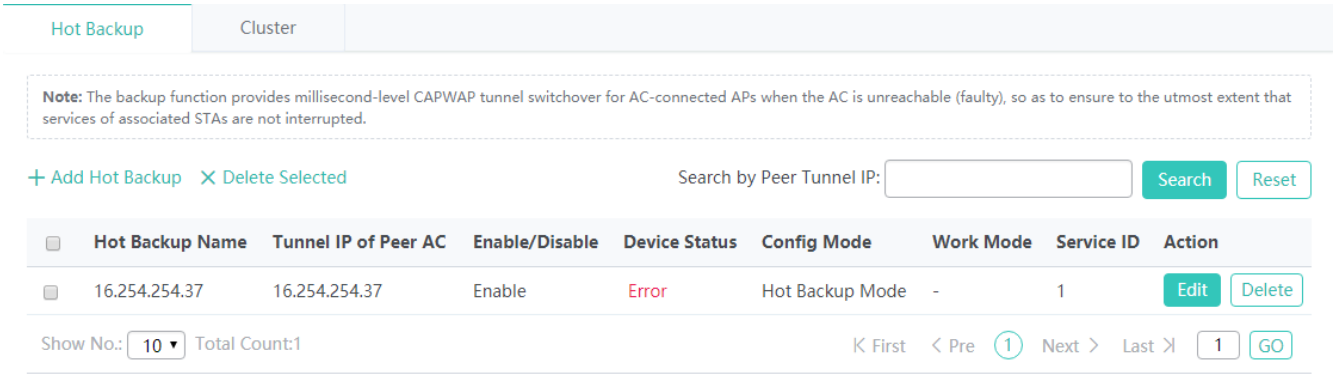
- Batch deleting hot backups

Select entries to be deleted from the list, and click **Delete Selected** to batch delete hot backup information.



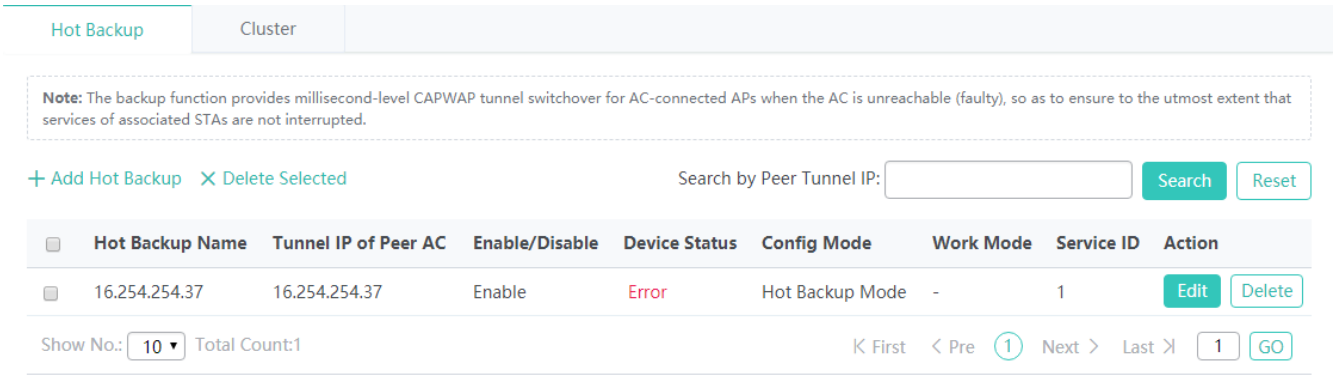
- Deleting a hot backup

Click **Delete** in the **Action** column to delete information about a single hot backup.



- Editing a hot backup

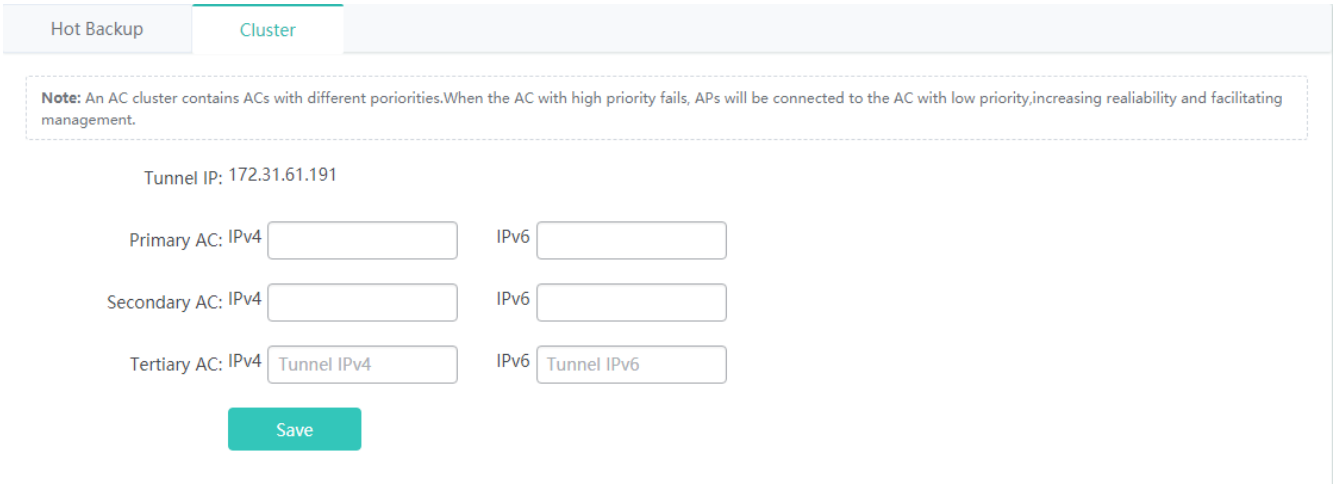
Click **Edit** in the **Action** column in the list. In the displayed window, edit hot backup information.



The parameters for editing a hot backup are the same as those for adding a hot backup and are not described again.

Cluster

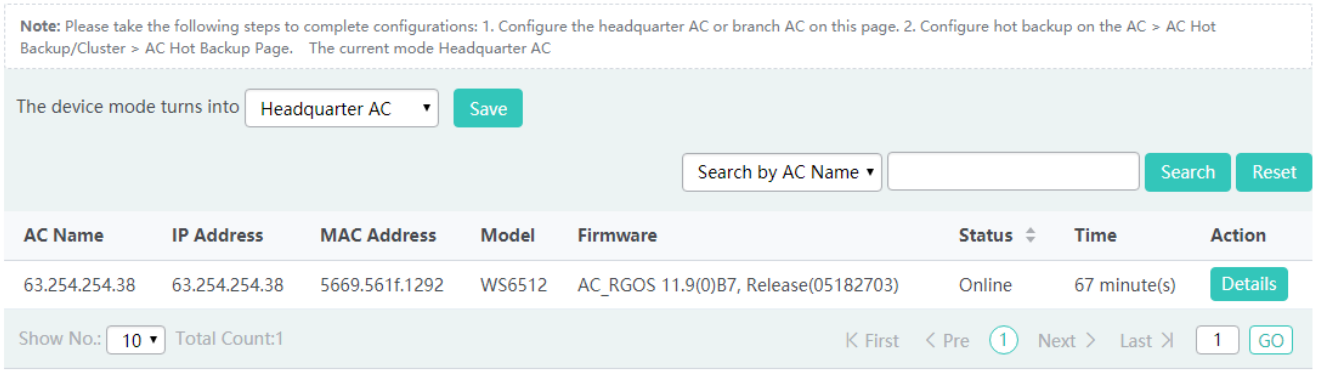
AC cluster is used to specify multiple ACs for an AP. When the connection between an AP and an AC is unreachable, the AP can associate with the backup AC. The AC cluster enhances WLAN reliability so that an AP associated with an AC can still provide services even if the AC is faulty. See the figure below.



Configure an IPv4 or IPv6 address of an AC that serves as the backup AC. A maximum of three ACs can be configured.

1.3.3.2.2 Hierarchical AC

The hierarchical AC function mainly displays details about the hierarchical ACs.



Based on device indicators, only some devices can serve as master ACs, some ACs can serve only as branch ACs, and some ACs that do not support the hierarchical AC function serve only as common ACs.

- Search

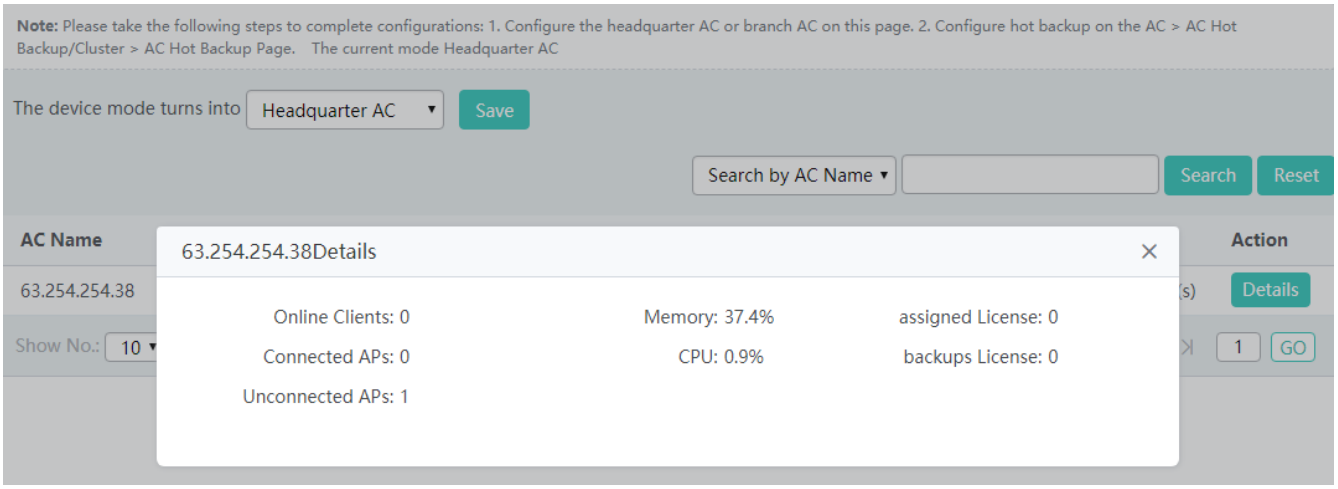
You can search for required hierarchical ACs by the AC name, IP address, MAC address, model, or online status.

- Reset

Click **Reset** to reset the search condition.

- Details

In the **Action** column in the list, click **Details** to display details about the AC, as shown in the figure below.



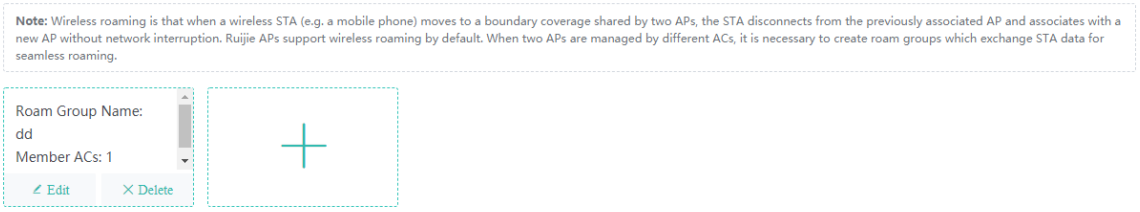
1.3.3.2.3 Inter-AC Roaming Management

Roaming Group Management

The roaming scope of wireless STAs cannot be infinitely large in a WLAN. ACs in the moving scope of a STA can be added to one roaming group, to allow the STA to roam between APs served by the ACs and control and manage the roaming scope of the STA.

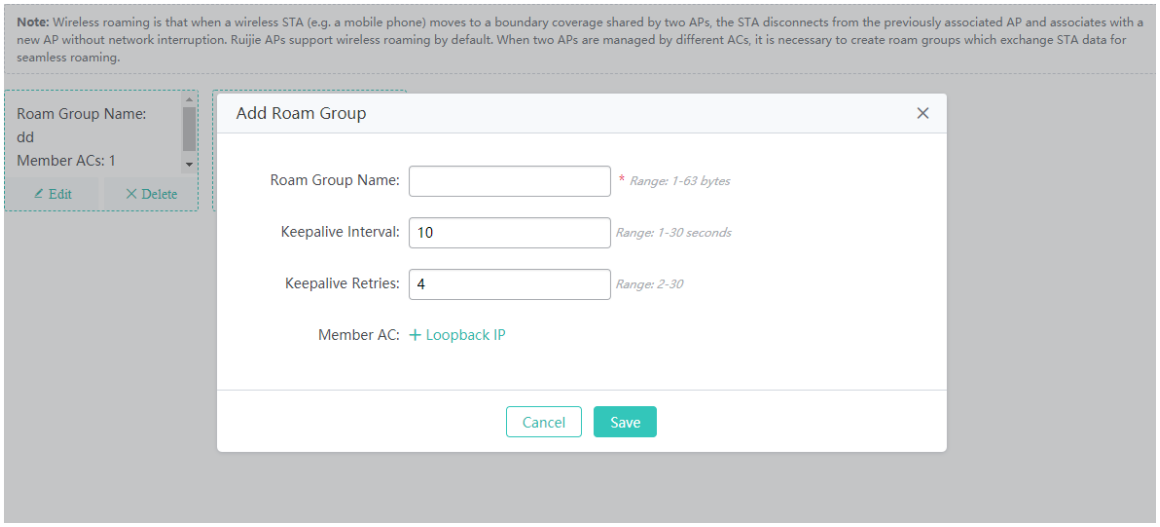
Roaming: When STAs are within the coverage of different APs, ACs in the same roaming group provide the perception-free go-online/offline function for the STAs.

The figure below shows the roaming group management page.



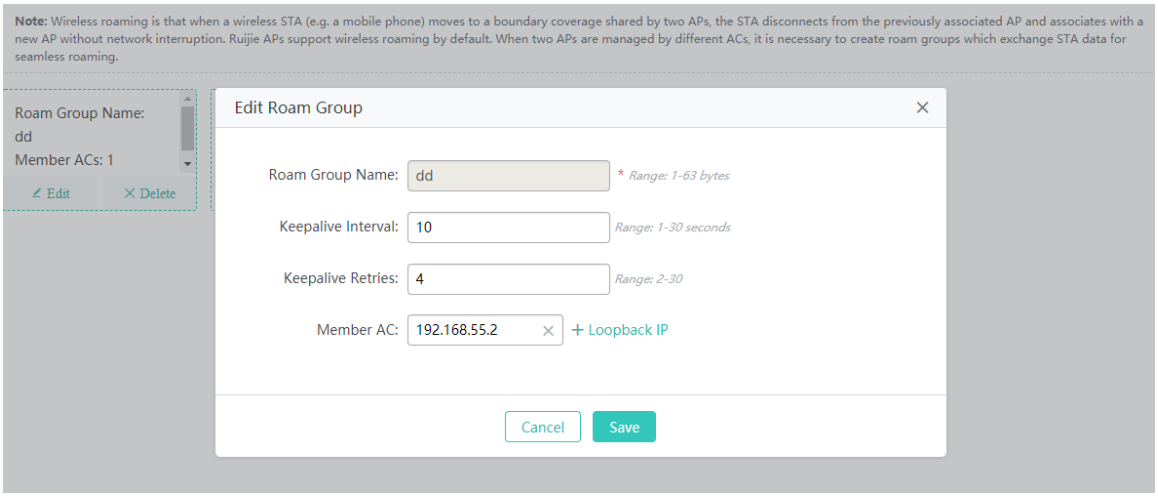
- Adding a roaming group

In roaming group configuration, click  to add a roaming group. **Roam Group Name** is mandatory and other parameters are optional. Multiple member ACs can be selected. Click **Save**. A setting success prompt is displayed and the roaming group is displayed in the roaming group list.



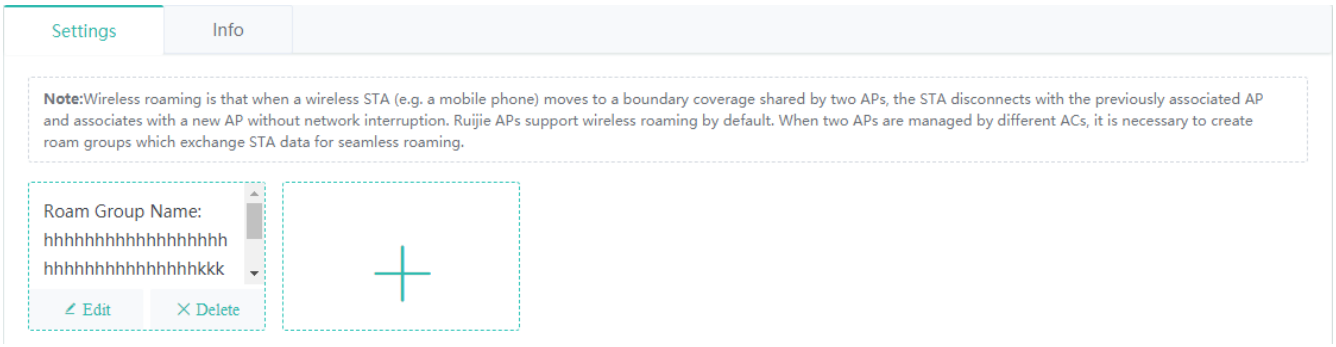
- Editing a roaming group

In a roaming group, click **Edit**. In the displayed **Edit Roam Group** dialog box, edit the roaming group, as shown in the figure below.



- Deleting a roaming group

In a roaming group, click **Delete** to delete the roaming group, as shown in the figure below.



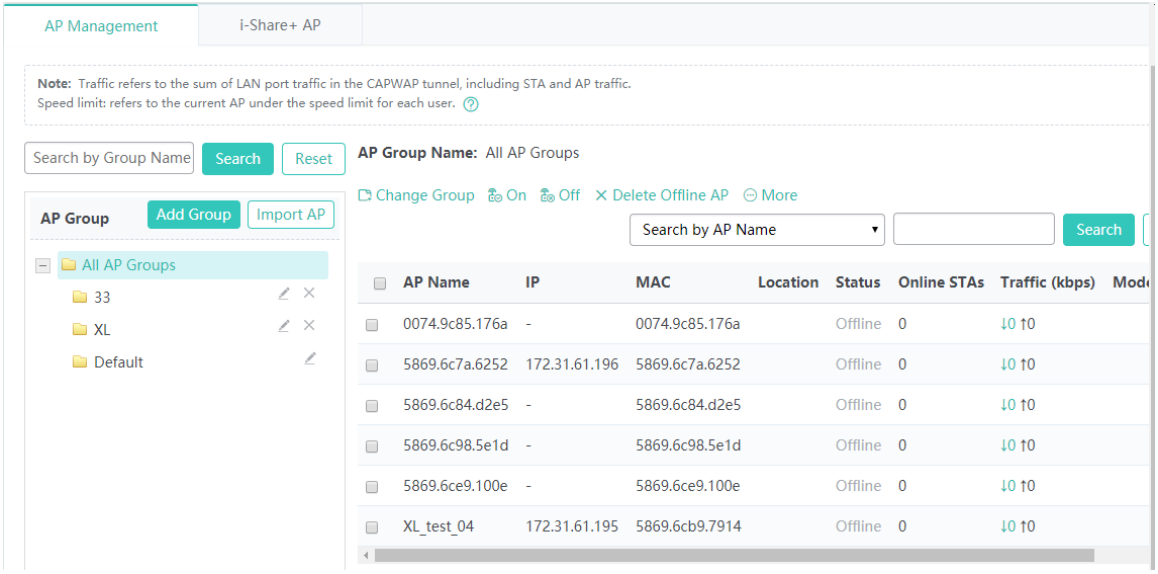
To ensure the efficiency and reliability of inter-AC information synchronization in a roaming group, the number of members in a roaming group is limited. Each roaming group supports a maximum of 24 member ACs.

1.3.3.3 AP

1.3.3.3.1 AP Management

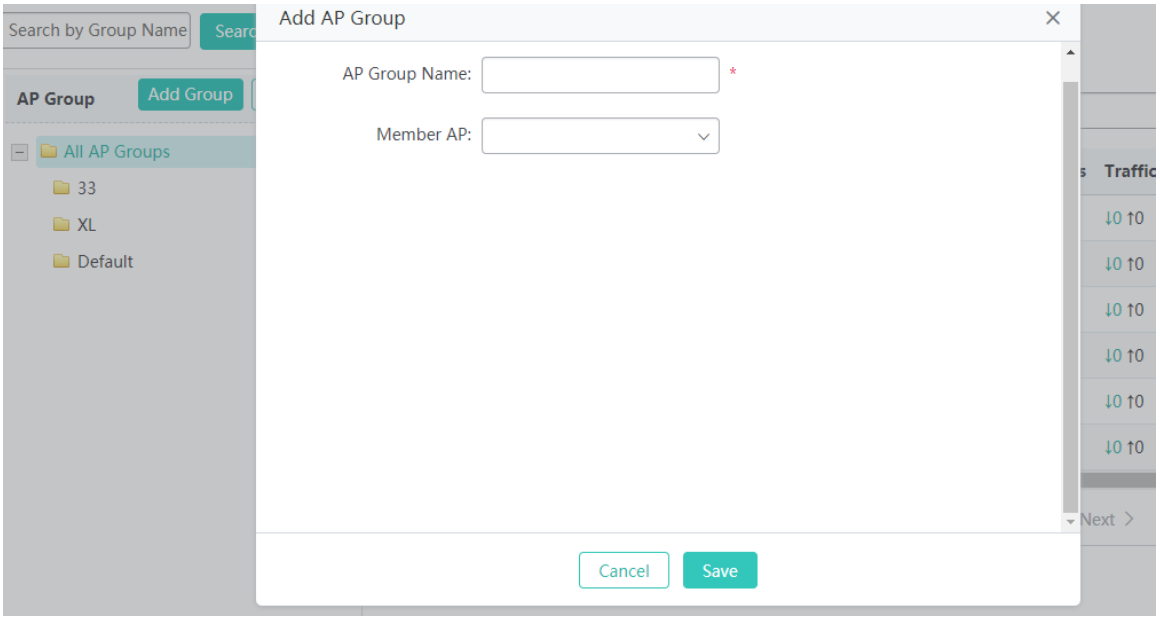
To provide services for STAs in a WLAN, an AP needs to establish a connection with an AC and be added to an AP group. All new APs belong to the **default** AP group.

The figure below shows the **AP Management** page.



- Adding an AP group

Click **Add Group**. In the displayed **Add AP Group** dialog box, enter the AP group name and other information to add an AP group, as shown in the figure below.



AP Group Name

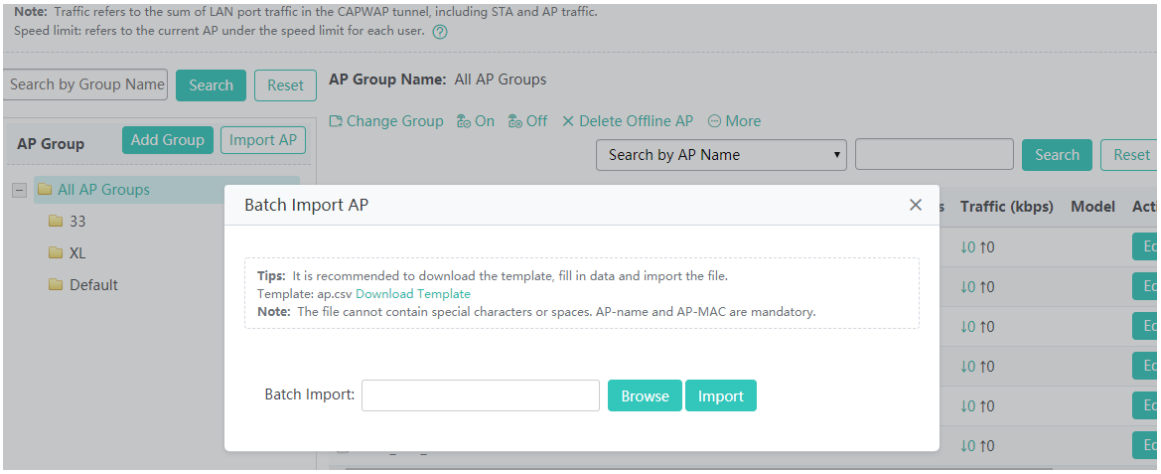
AP Group Name is mandatory.

Member AP

Indicates a member of the AP group. One AP can join only one group and belongs to the **default** group by default.

- Importing an AP

Click **Import AP**. In the displayed **Batch Import AP** window, select the AP data file to be imported and click **Import** to batch import AP information. For a specific AP data file, click **Download Template** to download a template file for reference.

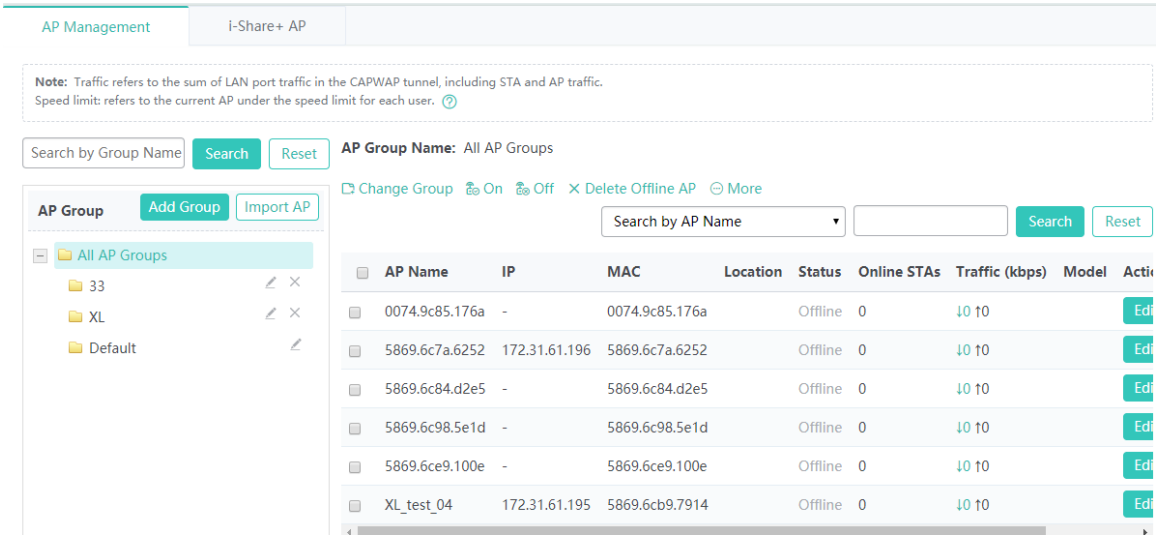


The AP data file cannot contain special characters such as Chinese characters or spaces. The AP name and AP MAC address are mandatory. An AP is imported to the **default** AP group by default.

- Deleting an AP group

In the AP group list, select an AP group and click ✕. In the displayed confirmation window, click **OK** to complete the delete

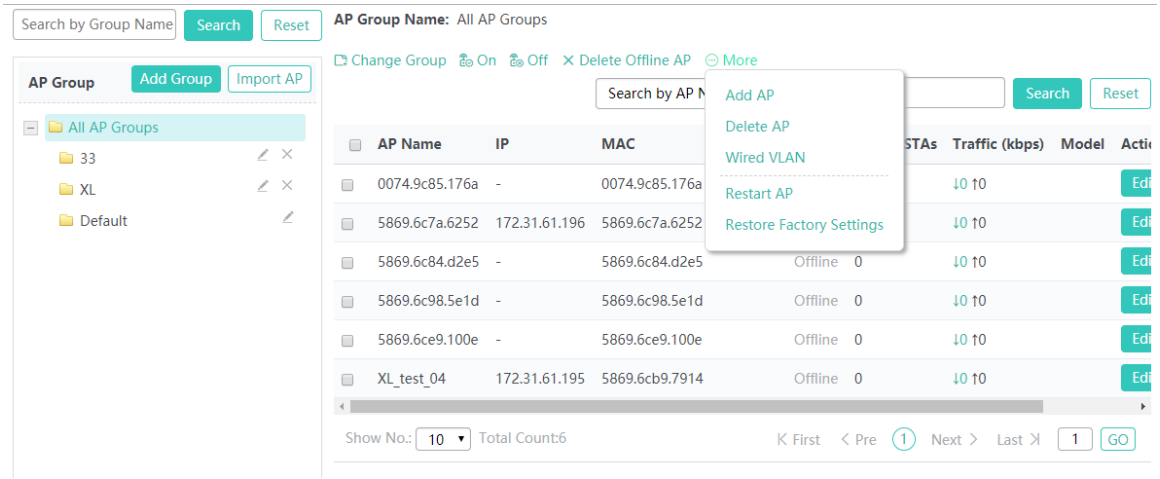
operation.

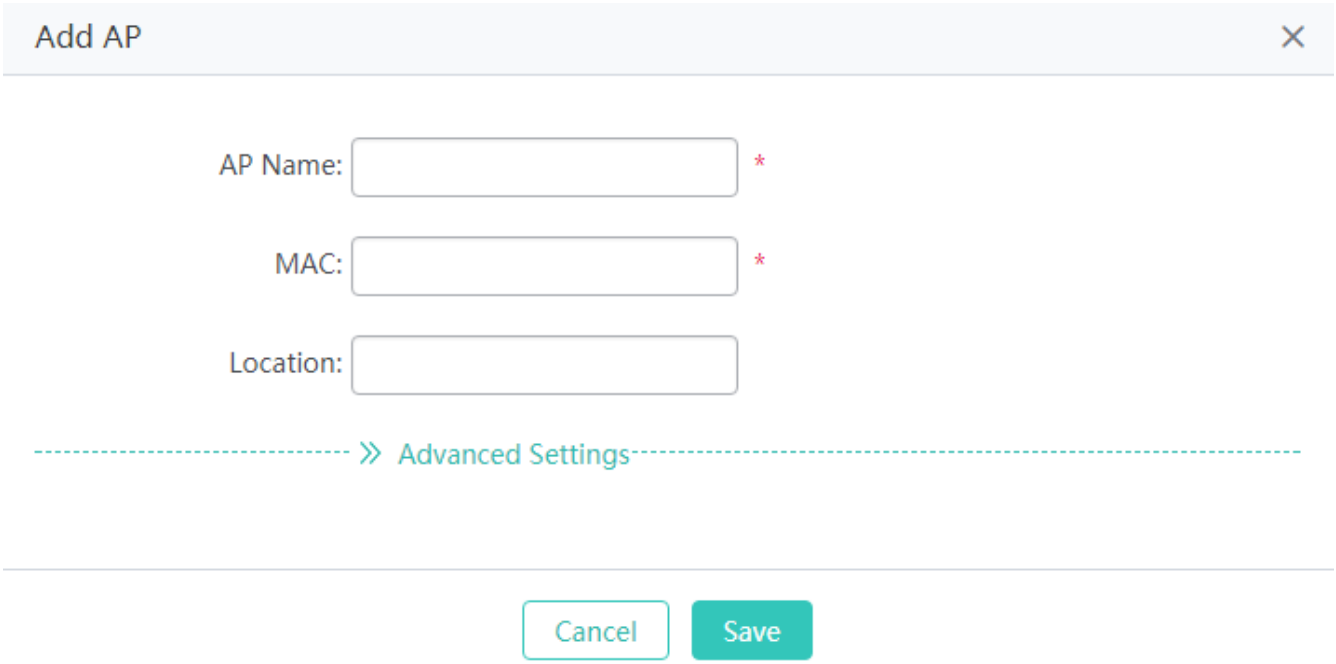


Note: The default group cannot be deleted.

- Adding an AP

In the AP group list, select an AP group, and click **More** and choose **Add AP**. In the displayed **Add AP** window, enter the AP name and MAC address and other optional parameters, and click **Save**. A setting success prompt is displayed and the AP is displayed in the AP list.





AP Name

Indicates the alias of the AP. The name of an AP cannot be modified if the AP is offline.

MAC

Indicates the unique identifier of the AP. The MAC address of an online AP cannot be modified.

Location

Indicates the location of the AP. For example, if an AP is located in 19#201, **Location** can be set to **19#201** to facilitate fast maintenance and locating.

AP Group

Indicates the AP group to which the AP belongs. One AP can belong to only one AP group. An AP belongs to the **default** group by default.

Telnet Account

Indicates the account for connecting to an AP. The account is mandatory.

Telnet Password

Indicates the password for connecting to an AP. The password is mandatory.

Tunnel IP

An AP can obtain an address via DHCP or a static address can be configured for an AP. The tunnel IP address, AP IPv4 address, AP IPv4 mask, and AP IPv4 gateway are required for configuring a static address. To configure the tunnel IP address for the communication between an AP and an AC, run the **acip ipv4 3.3.3.3** command.

The configuration may cause the AP to go offline. Exercise caution when performing the configuration.

AP IPv4

An AP can obtain an address via DHCP or a static address can be configured for an AP. The tunnel IP address, AP IPv4 address, AP IPv4 mask, and AP IPv4 gateway are required for configuring a static address. To configure the AP IPv4 address, AP IPv4 mask, and AP IPv4 gateway, run the **ip address 2.2.2.2 255.255.255.0 2.2.2.1** command.

The configuration may cause the AP to go offline. Exercise caution when performing the configuration.

AP IPv4 Mask

An AP can obtain an address via DHCP or a static address can be configured for an AP. The tunnel IP address, AP IPv4 address, AP IPv4 mask, and AP IPv4 gateway are required for configuring a static address. To configure the AP IPv4 address, AP IPv4 mask, and AP IPv4 gateway, run the **ip address 2.2.2.2 255.255.255.0 2.2.2.1** command.

The configuration may cause the AP to go offline. Exercise caution when performing the configuration.

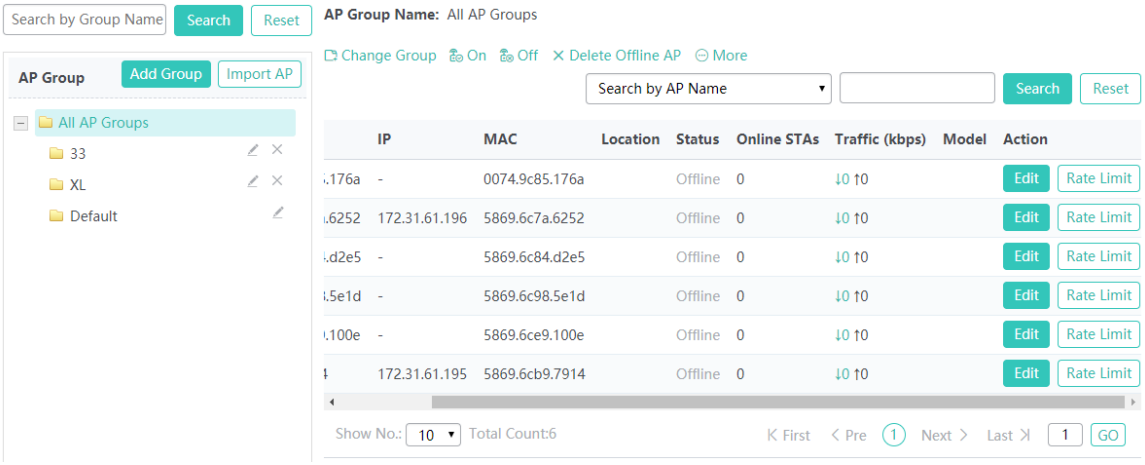
AP IPv4 Gateway

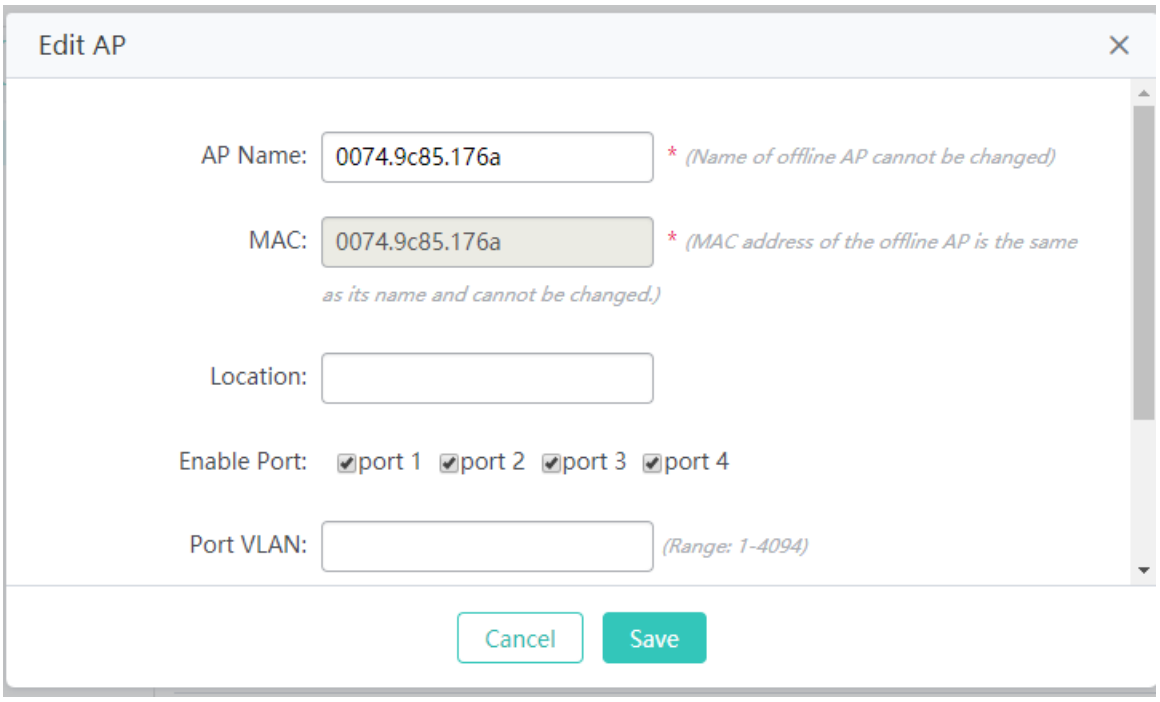
An AP can obtain an address via DHCP or a static address can be configured for an AP. The tunnel IP address, AP IPv4 address, AP IPv4 mask, and AP IPv4 gateway are required for configuring a static address. To configure the AP IPv4 address, AP IPv4 mask, and AP IPv4 gateway, run the **ip address 2.2.2.2 255.255.255.0 2.2.2.1** command.

The configuration may cause the AP to go offline. Exercise caution when performing the configuration.

- Editing an AP

In the AP list, click **Edit** in the **Action** column. The displayed window shows information about the AP. Edit information and click **Save**. A setting success prompt is displayed.





Parameters for editing an AP are the same as those for adding an AP and are not described again.

Enable Port

A wired port of an AP is enabled by default. You can disable the wired port by running the **no wired-interface port 2 enable** command.

Port VLAN

Indicates the VLAN to which a wired port belongs. To configure the port VLAN, run the **wired-vlan 1** command

Port Rate

Indicates the rate of a wired port. To configure the port rate, run the **wired-rate 22** command

SSID Release upon AP Offline

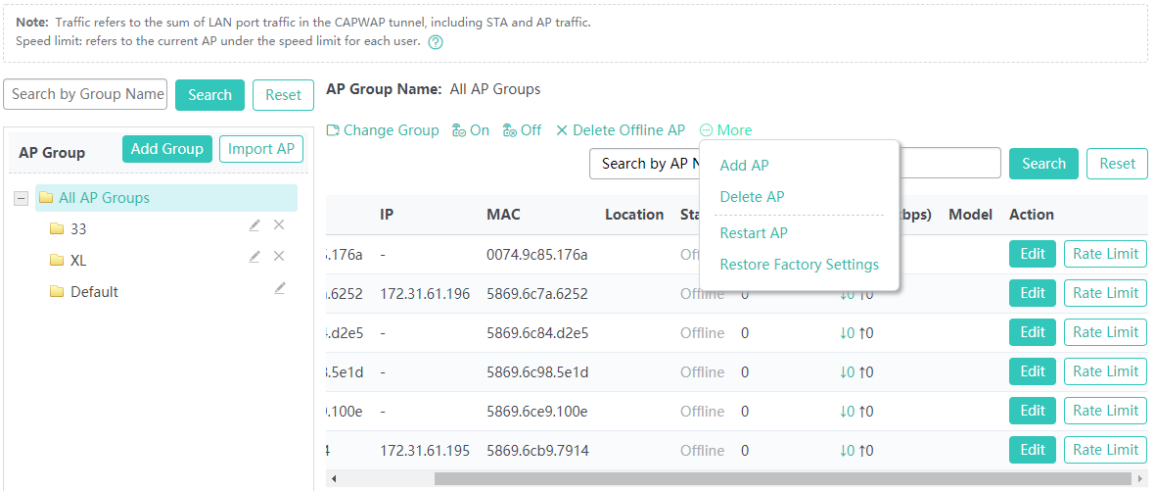
Indicates the WiFi network SSID released when an AP goes offline. To configure the WiFi network SSID released upon AP go-offline, run the **offline-ssid 1212** command

Hide SSID

Indicates whether the WiFi network SSID released when an AP goes offline is hidden. To hide the SSID, run the **offline-ssid 1212 hide** command. Otherwise, run the **offline-ssid 1212** command

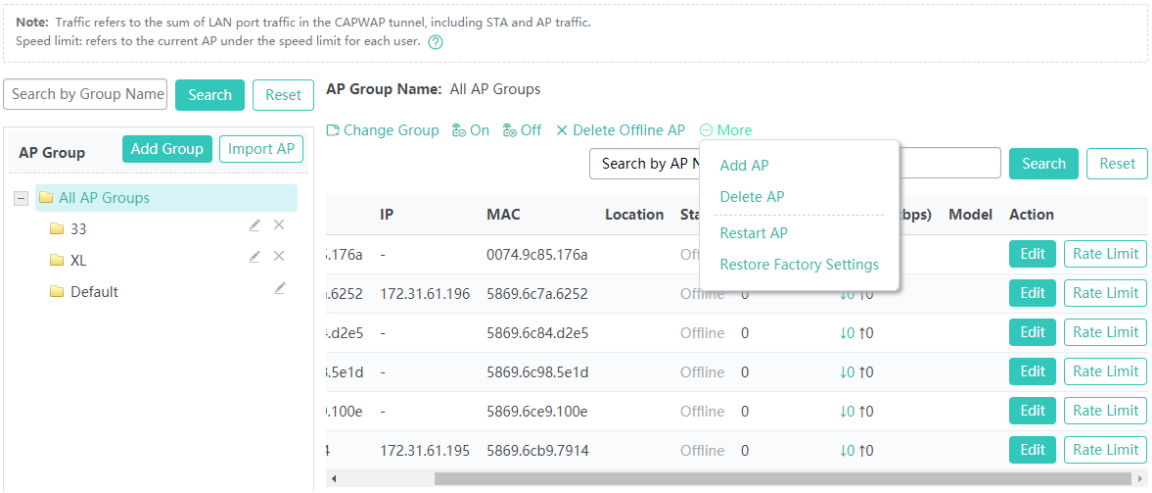
- Deleting an AP

In the AP list, select one or more records, click **More** and choose **Delete AP** to delete data, as shown in the figure below. In the displayed confirmation window, click **OK** to complete the delete operation.



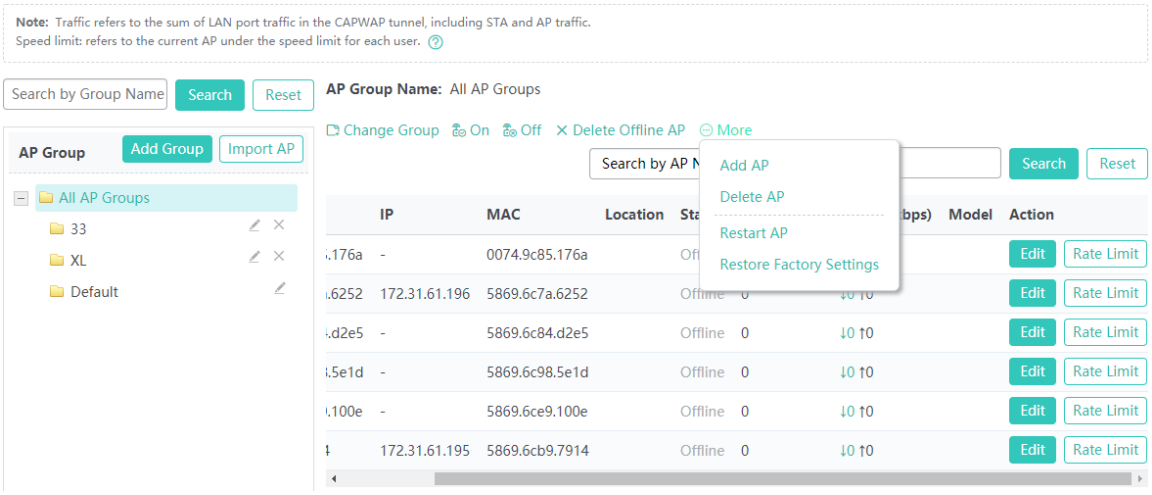
- Restarting an AP

In the AP list, select one or more records, click **More** and choose **Restart AP** to restart APs, as shown in the figure below. In the displayed confirmation window, click **OK** to complete the restart operation.



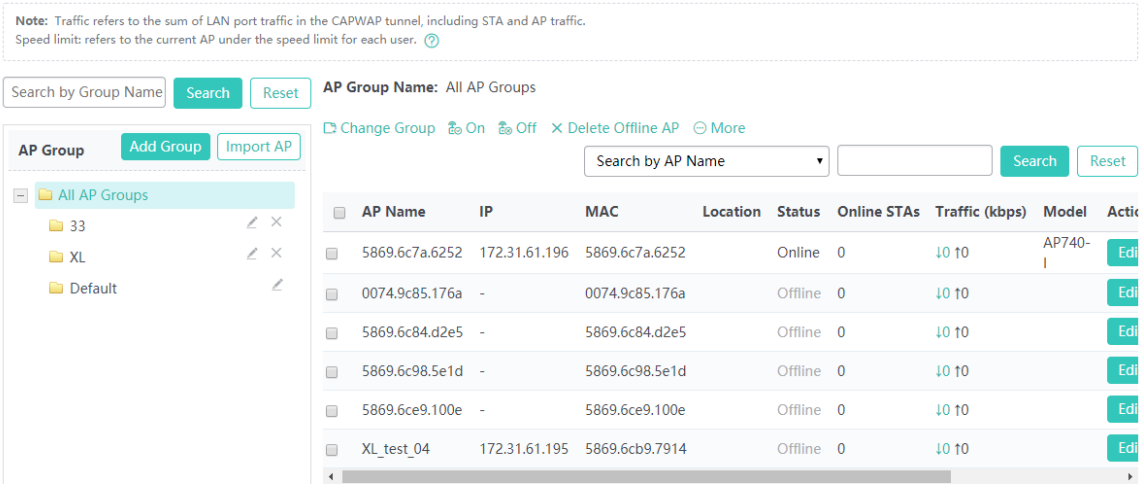
- Restoring factory settings

In the AP list, select one or more records, click **More** and choose **Restore Factory Settings** to restore AP settings, as shown in the figure below. In the displayed confirmation window, click **OK** to complete the factory settings restoration operation.



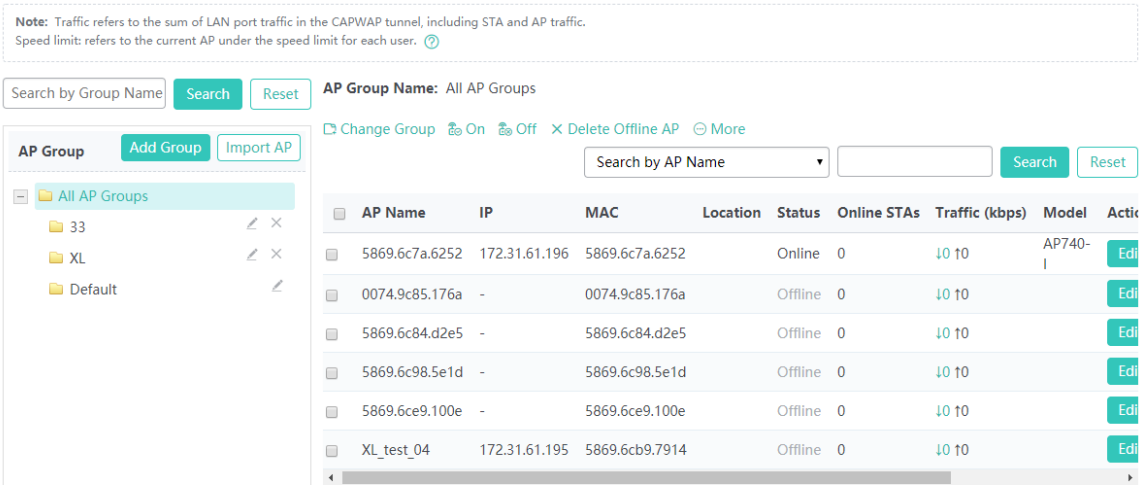
- Enabling an AP

In the AP list, select one or more records and click **On** to enable the radio function of APs, as shown in the figure below.



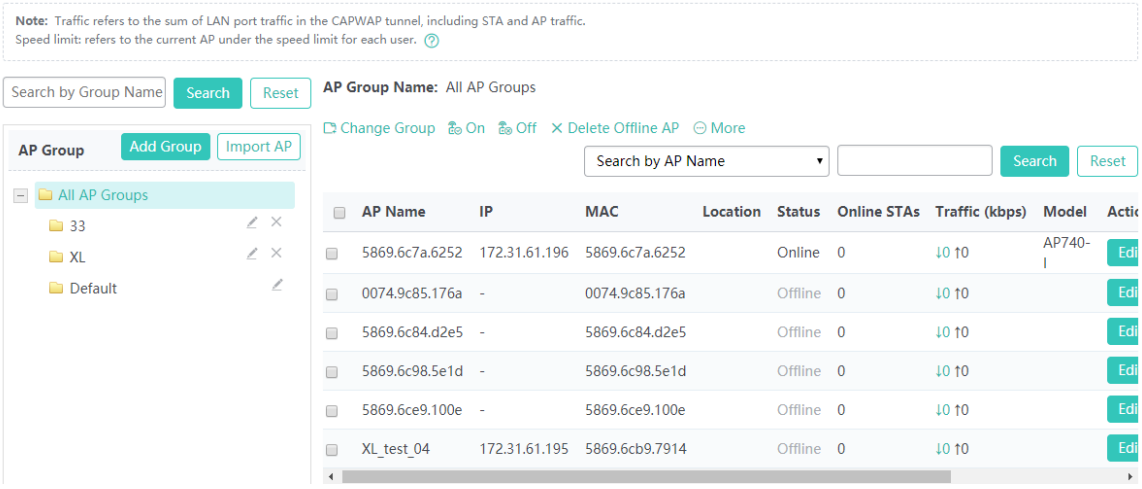
- Disabling an AP

In the AP list, select one or more records and click **Off** to disable the radio function of APs.



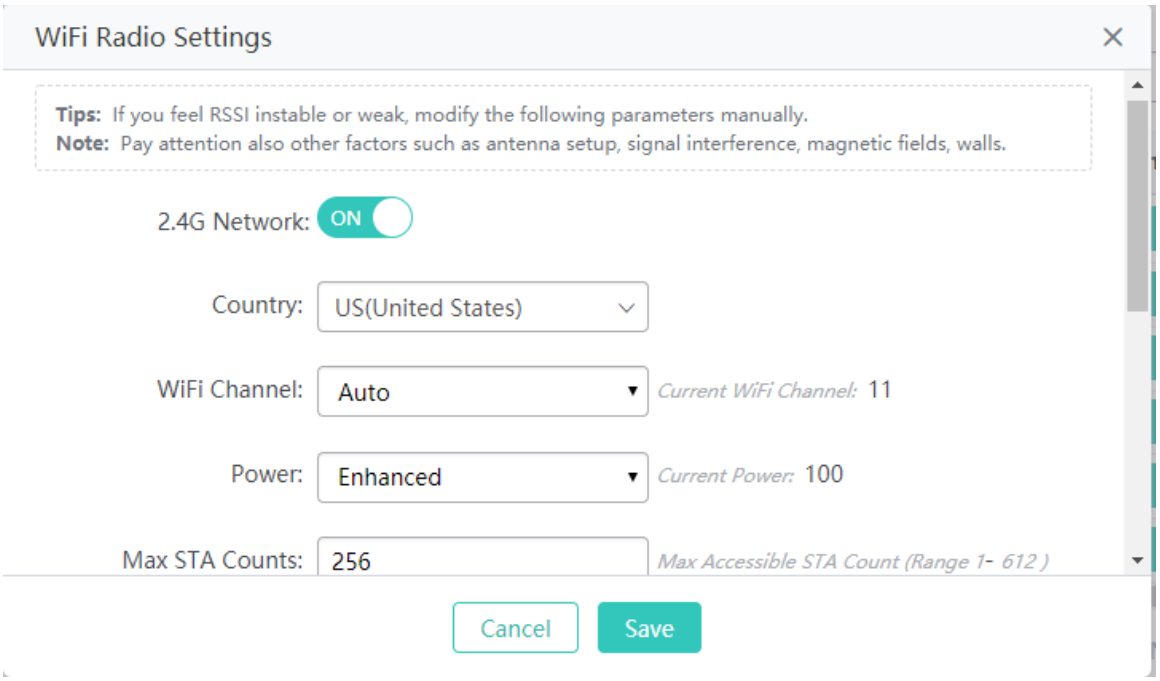
- Deleting all offline APs

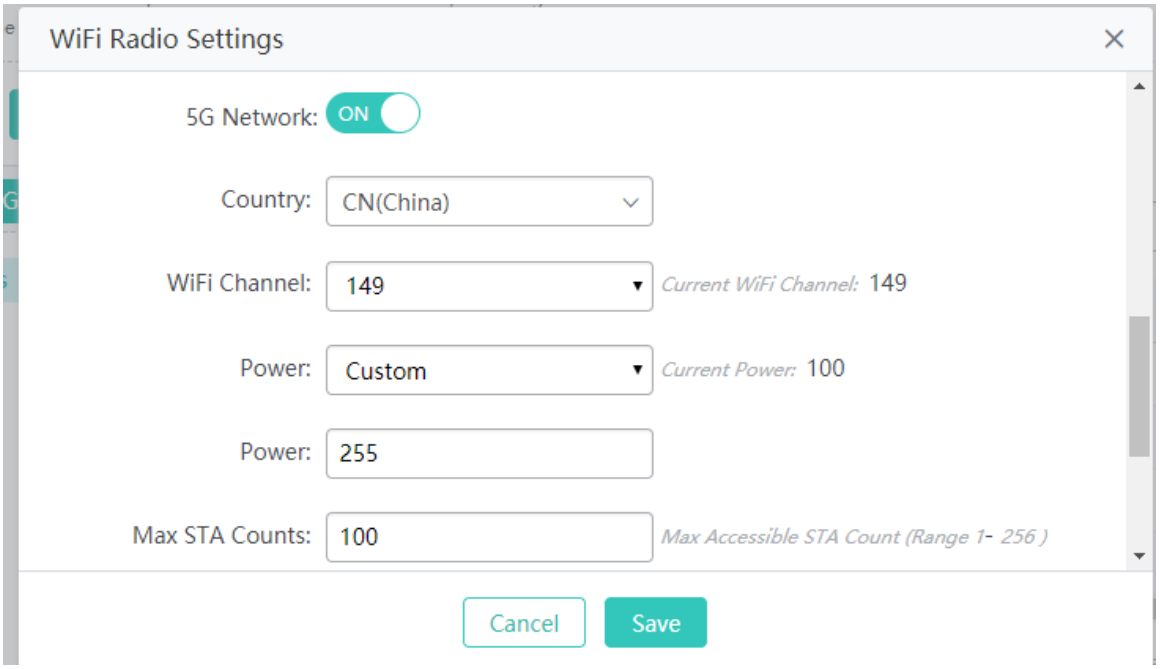
Click **Delete Offline AP** to delete information about all offline APs.



- Radio

The radio configuration button is available only for online APs. In the AP list, click **Radio** to configure radio information for the AP, as shown in the figure below.





RF Port

This parameter is displayed only when an AP supports a radio other than 2.4 GHz and 5 GHz. You can select the required radio.

Network switch

Indicates whether to enable a radio. To enable or disable a radio, run the **radio 1 enable|disabled** command.

Country

Specifies the country code for the current AP. The default country code is displayed by default.

WiFi Channel

The channel is displayed based on the current country code and network type.

Power

Indicates the power, which can be set to the following values:

- **Auto**: Indicates the auto mode.
- **Power Saving**: The power is 30.
- **Standard**: The power is 80.
- **Enhanced**: The power is 100.
- **Custom**: You can customize the power.

Max STA Counts

Indicates the maximum number of STAs supported by a radio. This parameter is configured for a radio.

The range of **Max STA Counts** refers to the range of the maximum number of STAs on the entire AP.

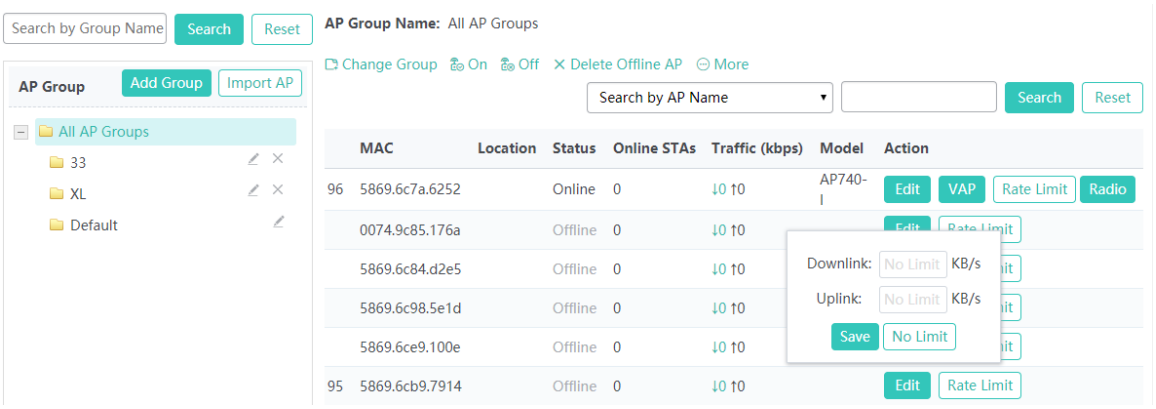
Frequency Bandwidth

Indicates the frequency bandwidth supported by a radio.

Enabling a transmit/receive antenna

Indicates the configuration of the transmit and receive antennas of a radio.

- Rate Limit



Downlink

Indicates the maximum download speed of each STA supported by an AP.

Uplink

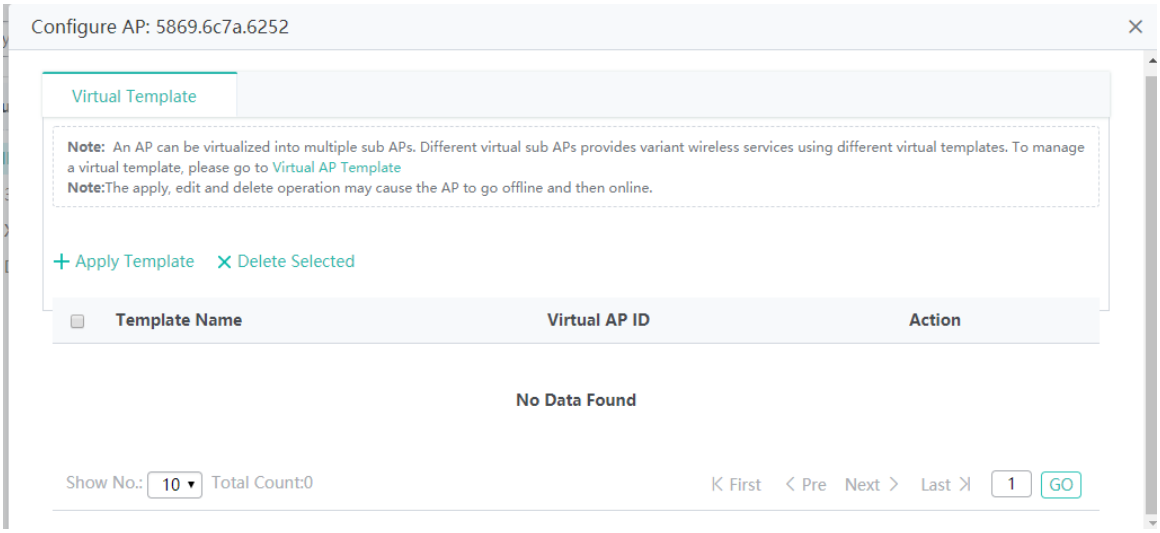
Indicates the maximum upload speed of each STA supported by an AP.

No Limit

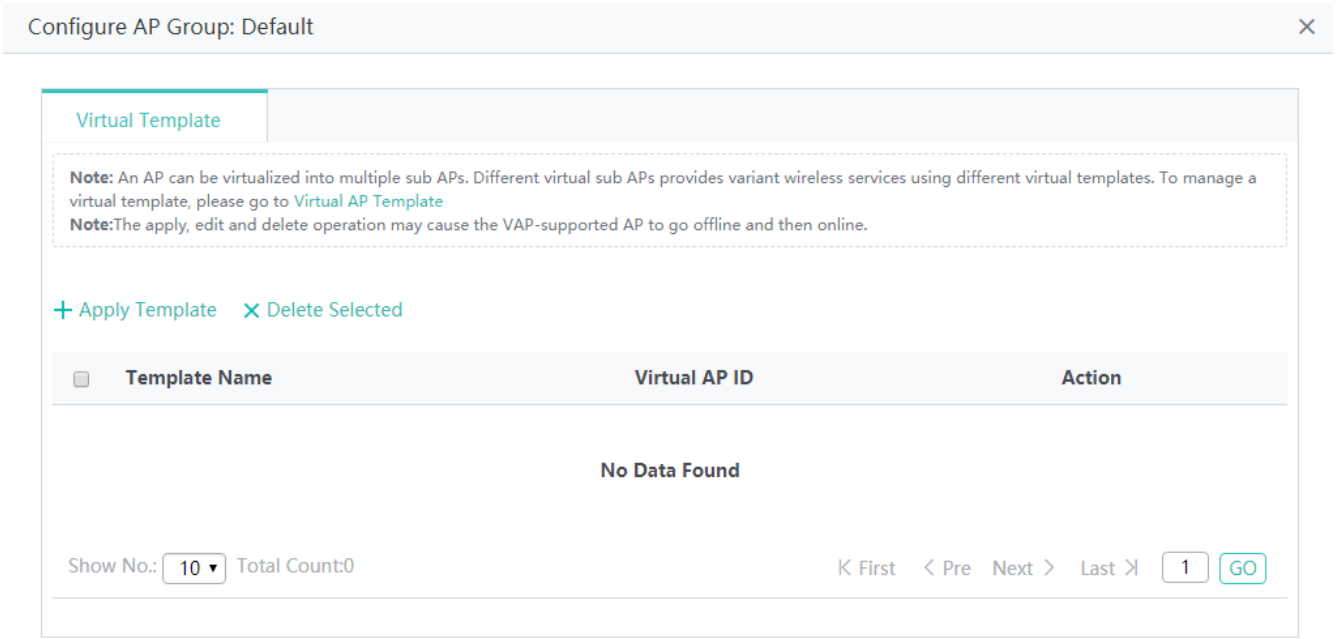
Indicates that no rate limit is configured for each STA supported by an AP.

AP Virtualization

If an AP supports virtualization, the **VAP** button is displayed in the list for configuring the AP as a virtual AP. A virtual template needs to be added for an AP and then applied to the AP during AP virtualization, as shown in the figure below.

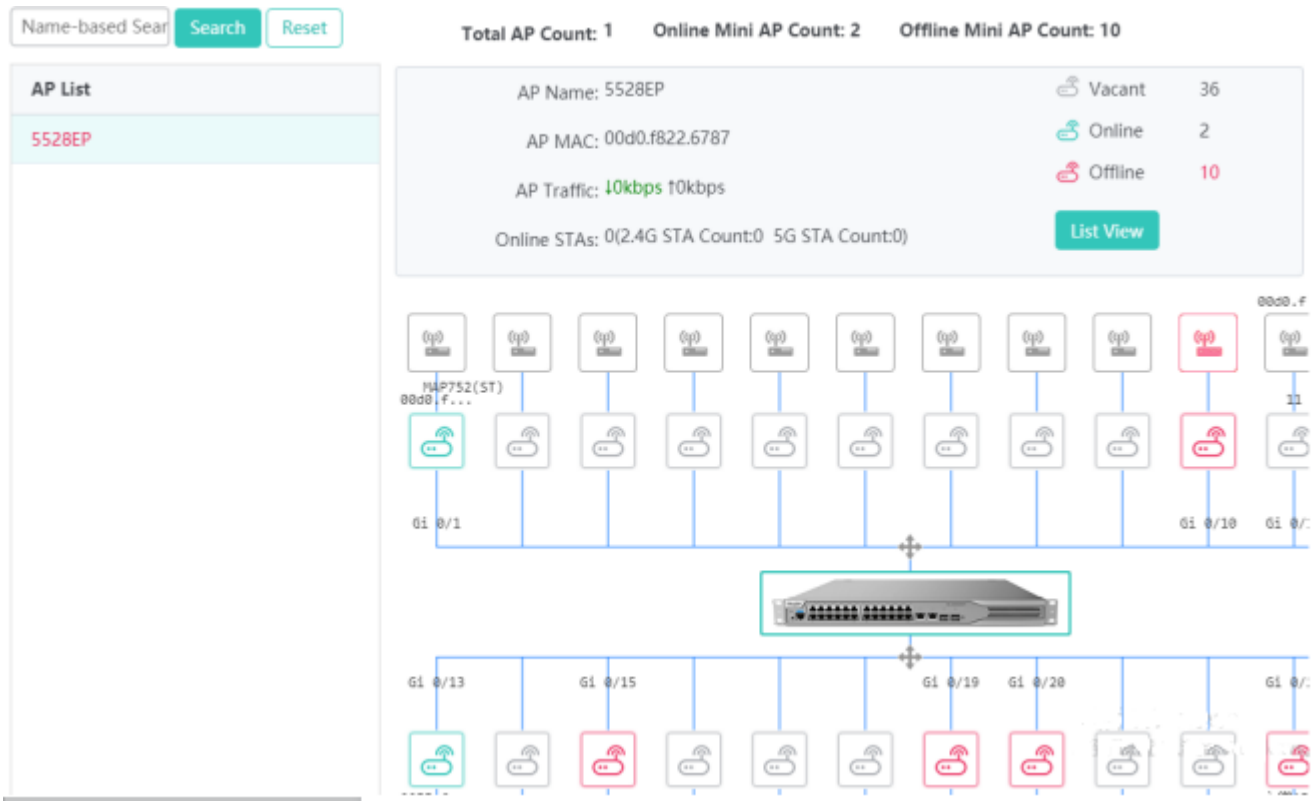


Application and management of a virtual AP template



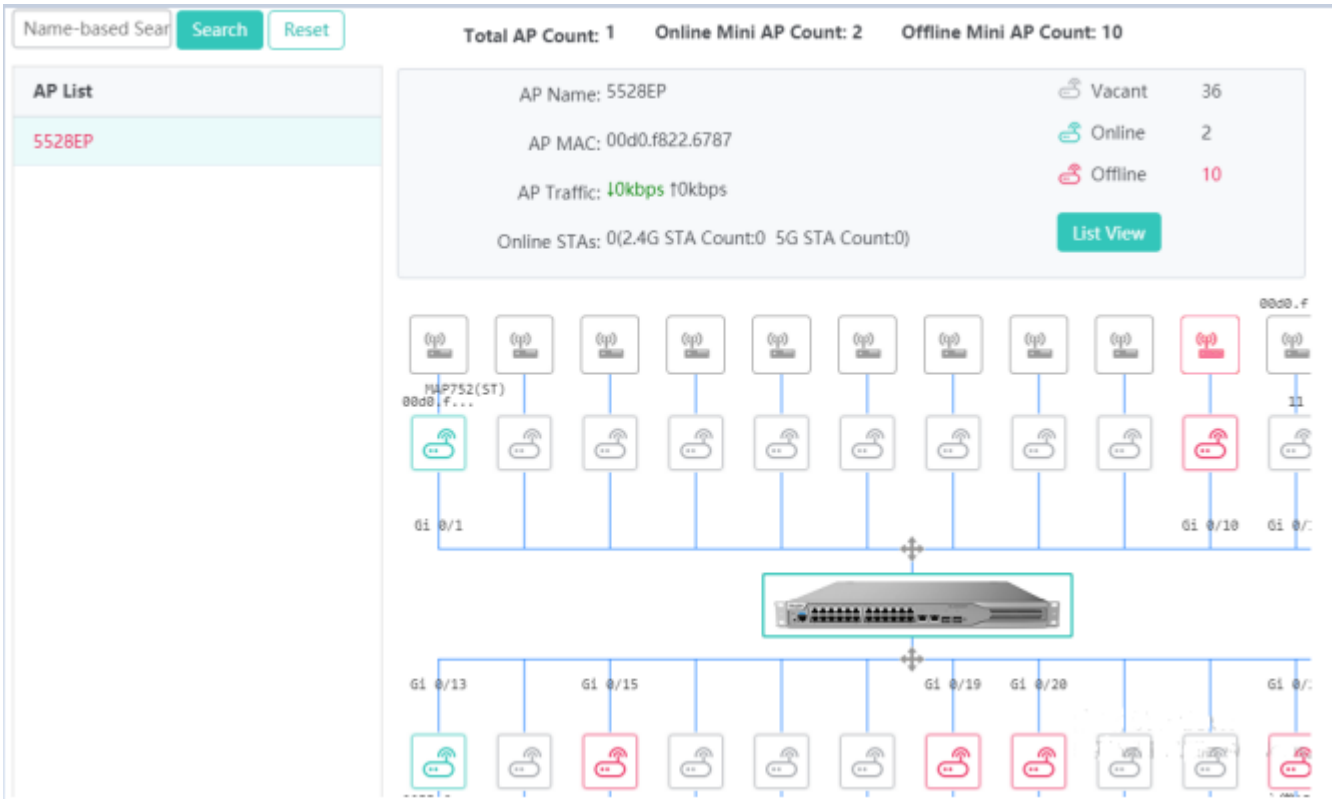
i-Share+ AP

The i-Share+ AP page displays information about all i-Share+ APs on a network and information about each AP. The i-Share+ AP page displays a list of all i-Share+ APs on the left side and details of a selected AP on the right side. The topology view and list view can be switched on the right side. In the view on the right side, an icon in red indicates that the AP has an offline radio card while an icon in black indicates that all radio cards of the AP are online.



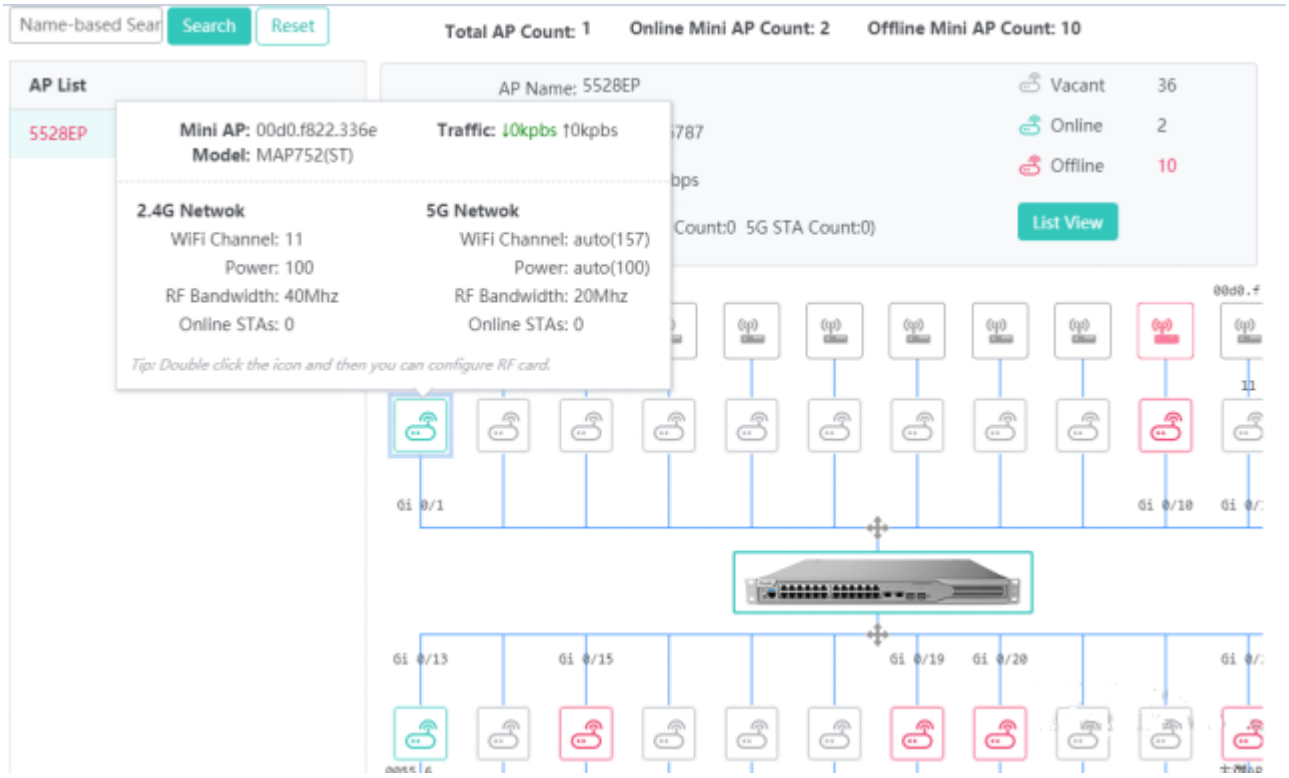
- Displaying i-Share+ APs that meet a condition

In the search box in the AP list, enter a search condition and click **Search** to find out required APs via fuzzy search, as shown in the figure below.

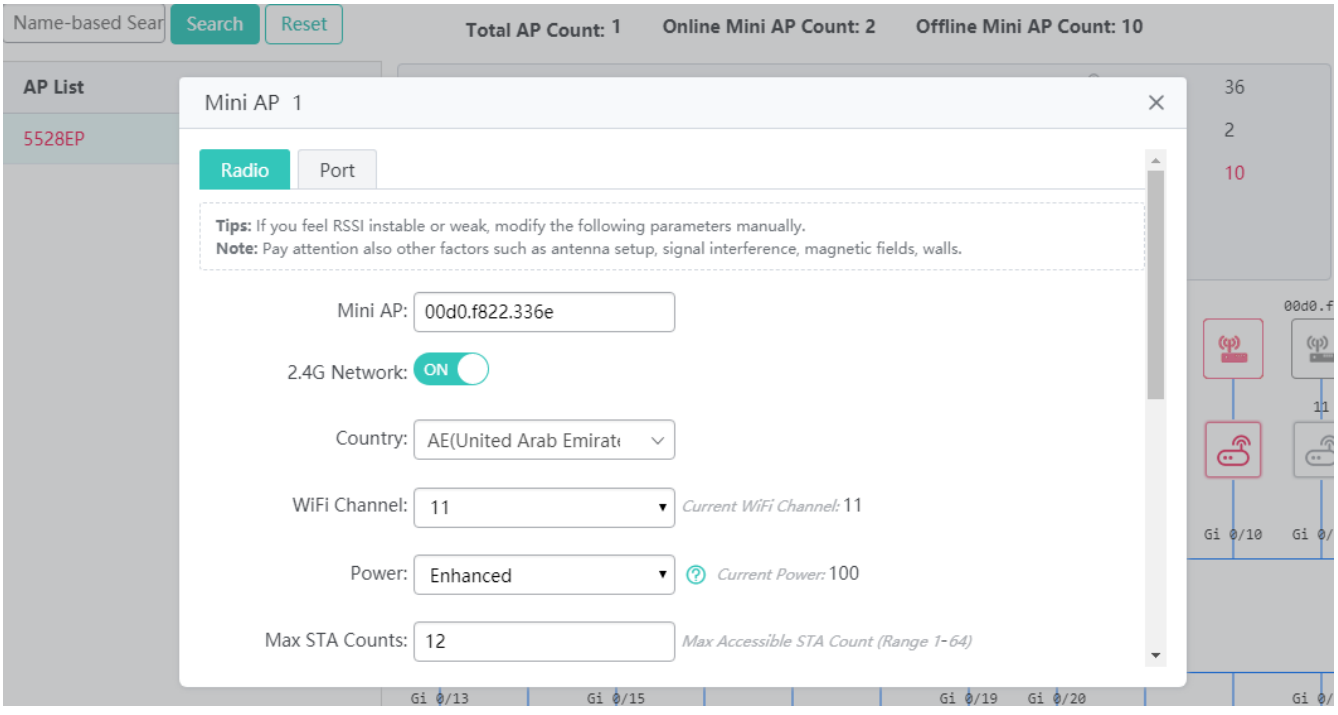


- Displaying radio information

In the radio card topology on the right side, move the cursor over a radio card icon to display details about the radio card. Double-click a radio card to configure the radio card. See the figure below.

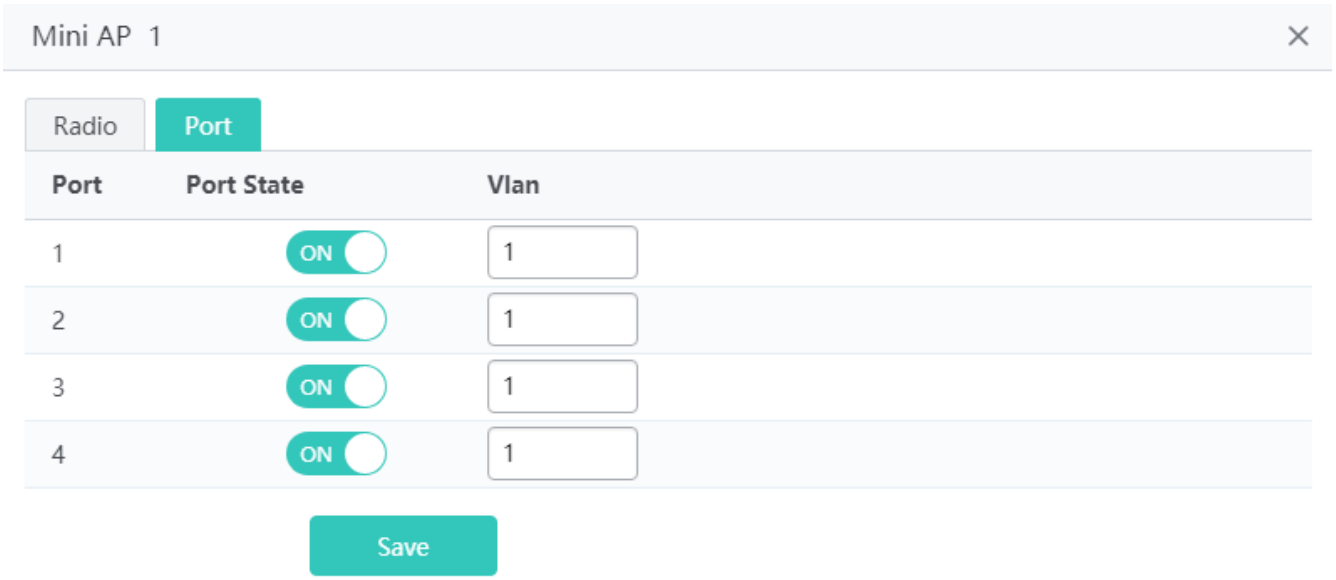


- Configuring radio card information



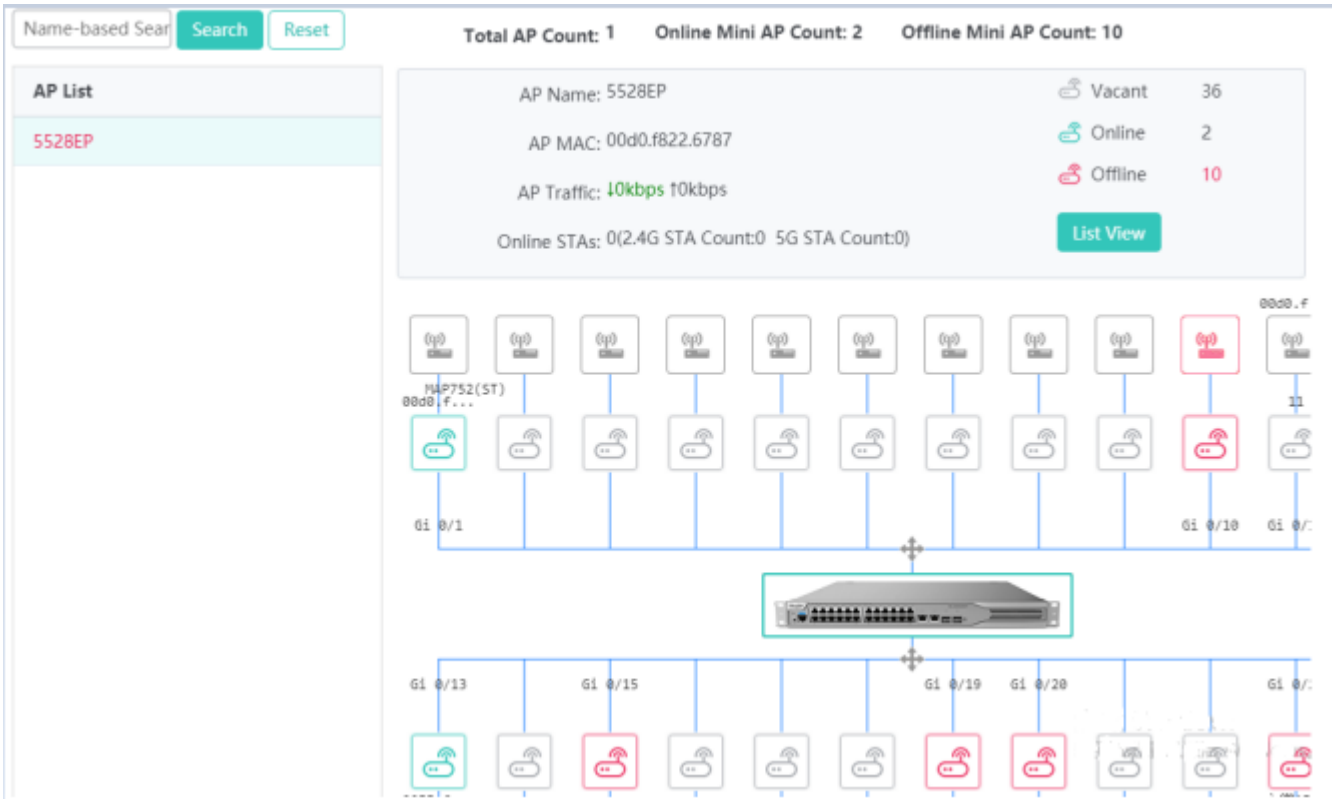
- Configuring wired ports of a radio card

Wired ports are displayed based on actual interfaces of the device.



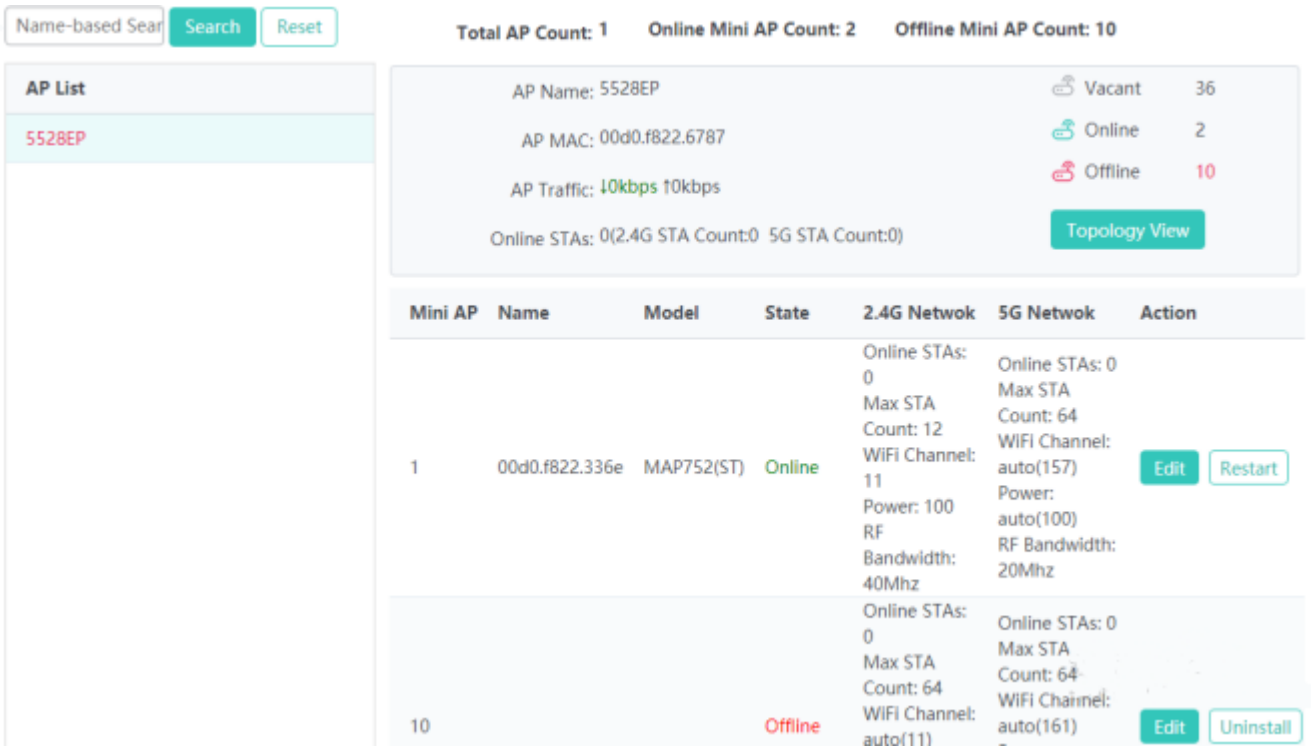
- Switching the list mode.

Click **List View** to switch to the list view.



- Configuring radio cards

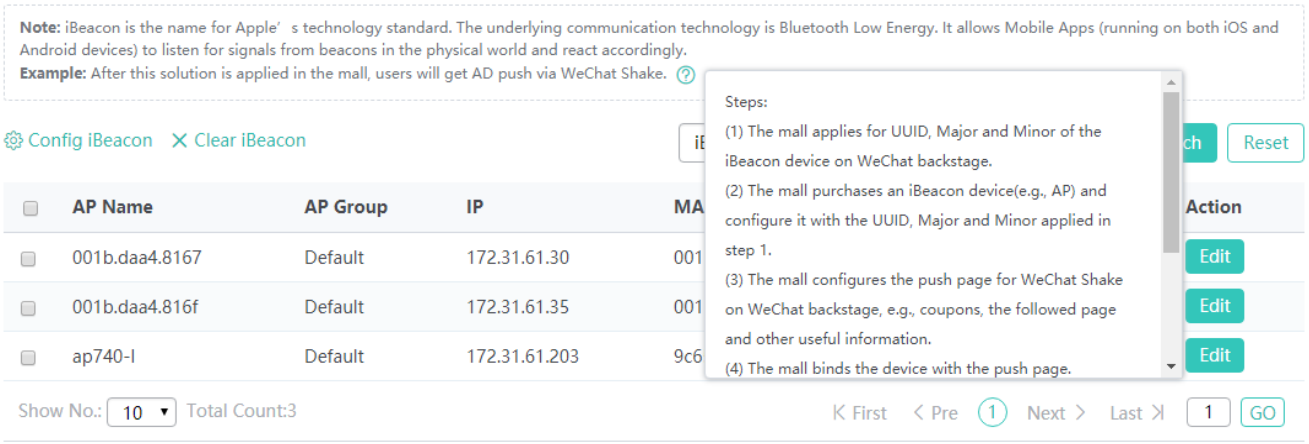
In the list view, click **Edit** to configure a radio card. Click **Restart** to restart a radio card. If the **Uninstall** button is displayed, it indicates that the RF card is in the offline state and you can click this button to uninstall the RF card.



1.3.3.3.2 iBeacon

iBeacon is a communication protocol based on low power consumption Bluetooth. iBeacon-compliant APs can send specific IDs (generated by a third party) to surrounding STAs. After receiving the IDs, the STAs can return feedback by using application installed on the STAs.

For example, after the iBeacon solution is deployed on a mall, users can use the WeChat Shake function and then receive pushed advertisements. Steps are provided on the page below.



- Searching for APs

You can search for APs by iBeacon, AP status, AP group, AP name, IP address, or MAC address.

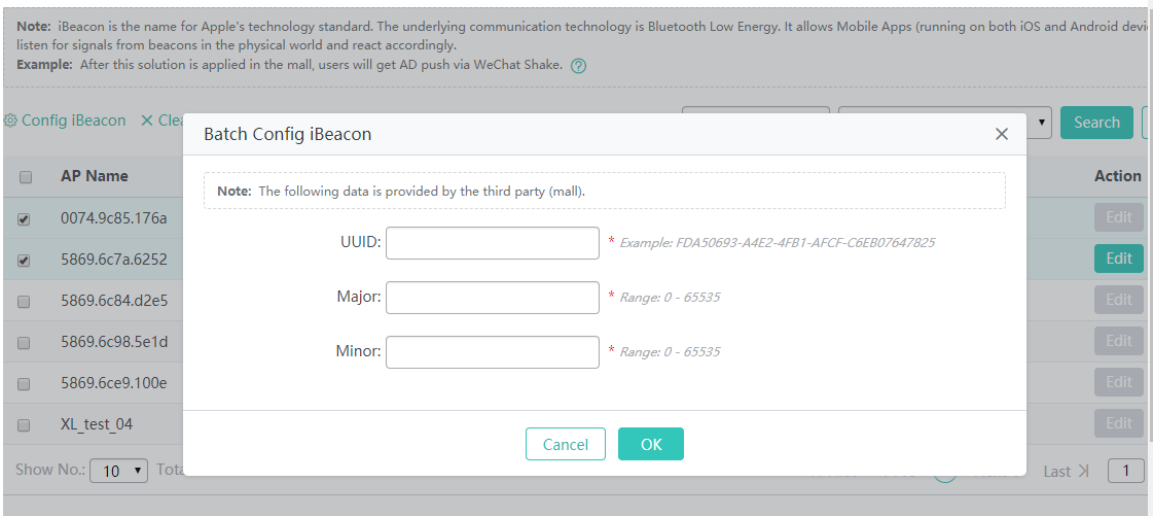
- Resetting search conditions

Click **Reset** to reset the search condition.

- Batch configuring iBeacon

1. Select APs for which iBeacon needs to be configured.

2. Click **iBeacon Config**. In the displayed window, configure iBeacon-related information.



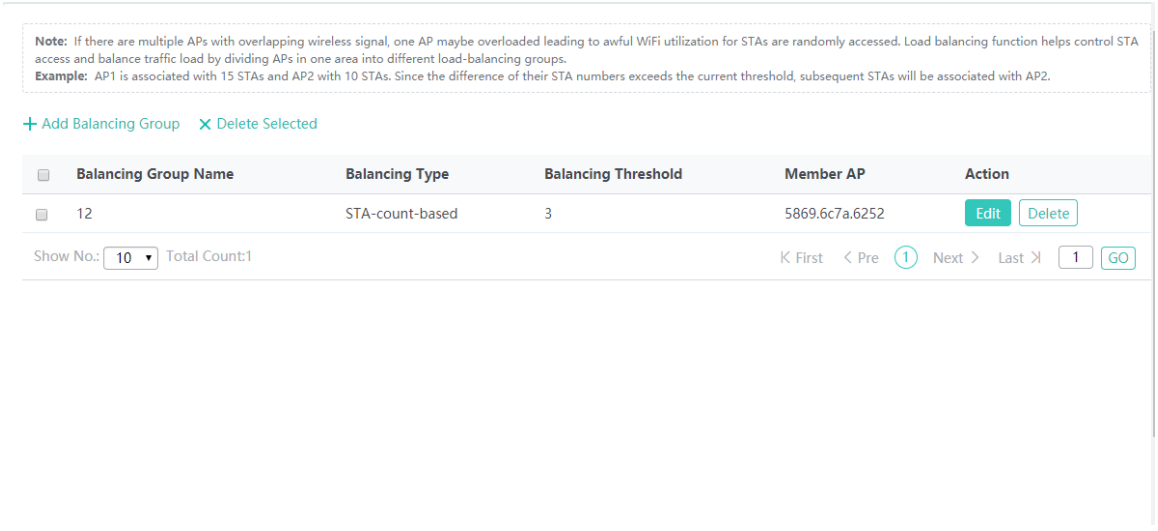
- Batch clearing iBeacon configurations

Select APs to be deleted from the list and click **Clear iBeacon** to delete the iBeacon configurations.

- Configuring iBeacon

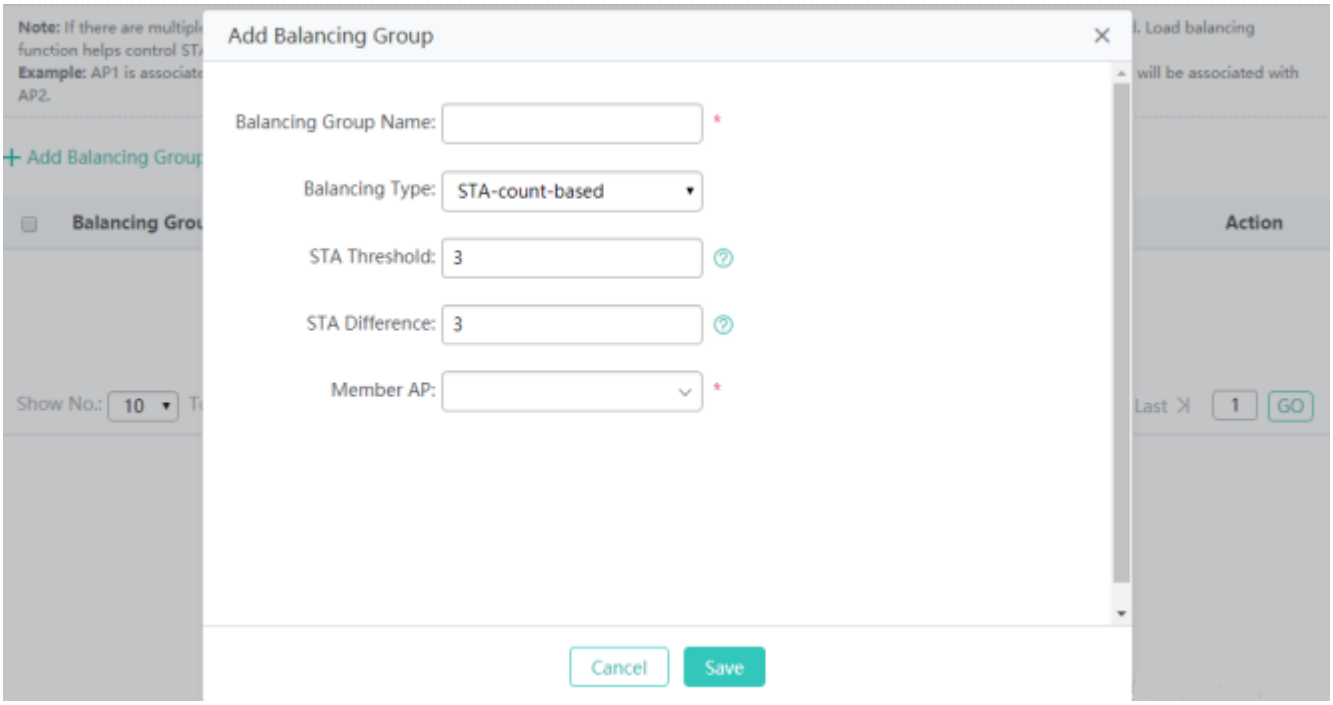
In the list, click **Edit** to edit the iBeacon configuration of a single AP.

1.3.3.3.3 Load Balancing



- Adding a balancing group

Click **Add Balancing Group**. In the displayed **Add Balancing Group** window, enter related information and click **Save** to add the balancing group, as shown in the figure below.



Balancing Group Name

Identifies a balancing group. It is mandatory and cannot be modified when a balancing group is edited.

Balancing Type

Balancing Type can be set to **STA-count-based** or **AP-traffic-based**. It cannot be modified when a balancing group is edited.

STA Threshold

Indicates a prerequisite for load balancing, that is, the number of STAs associated with each AP exceeds this threshold.

STA Difference

Load balancing needs to be implemented when the STA difference reaches a specified value.

Traffic Threshold

Indicates a prerequisite for load balancing, that is, the traffic of each AP exceeds this threshold.

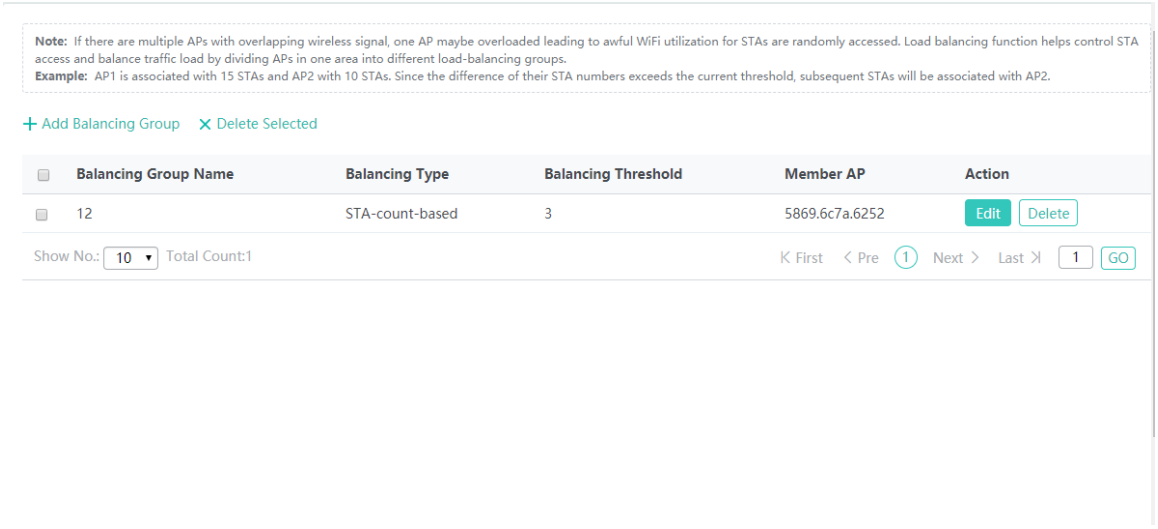
Load balancing needs to be implemented when traffic difference reaches a specified value.

Member AP

Indicates member APs in a balancing group. One AP can be configured in only one balancing group.

- Batch deleting balancing groups

Select balancing groups to be deleted from the list and click **Delete Selected** to batch delete the balancing groups.



- Editing a balancing group

Click **Edit** for a balancing group in the list. In the displayed edit window, edit the balancing group.

- Deleting a balancing group

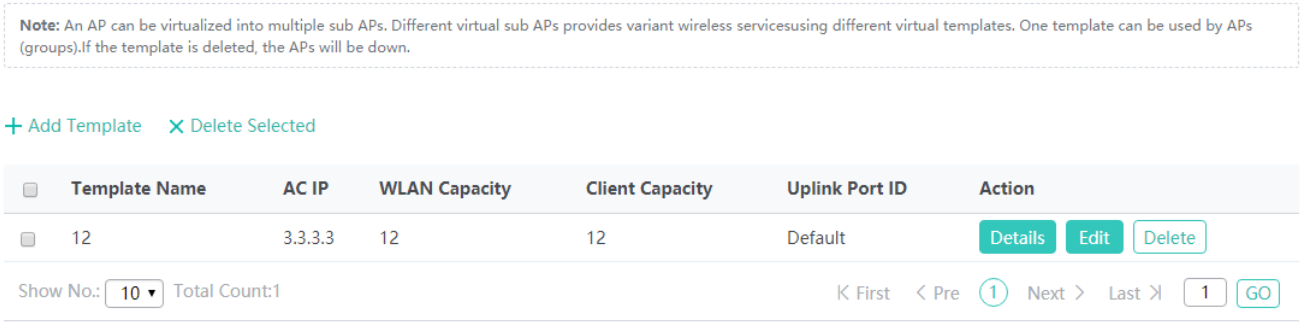
Click **Delete** for a balancing group in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

1.3.3.3.4 AP Virtualization

A template is configured and then applied to an AP group or an AP, so that AP virtualization takes effect.

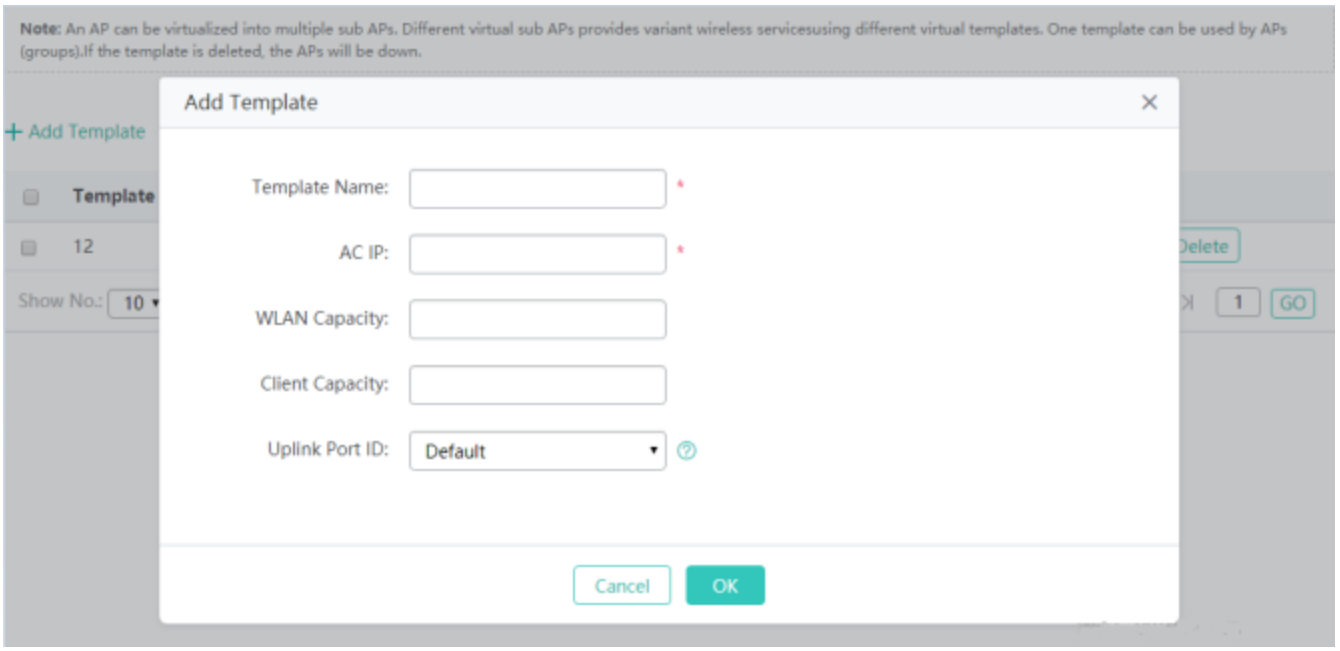
Template Management

You can add, edit, and delete a template and view the template application information, as shown in the figure below.



- Adding a template

Click **Add Template**. In the displayed **Add Template** window, enter information about a virtualization template and click **Save** to add the template to the template list, as shown in the figure below.



Template Name

Indicates the name of a virtual AP management template. It is mandatory.

AC IP

Indicates the IP address of an AC, that is, tunnel address used by an AC to manage an AP.

WLAN Capacity

Indicates the WLAN capacity supported by the template.

Client Capacity

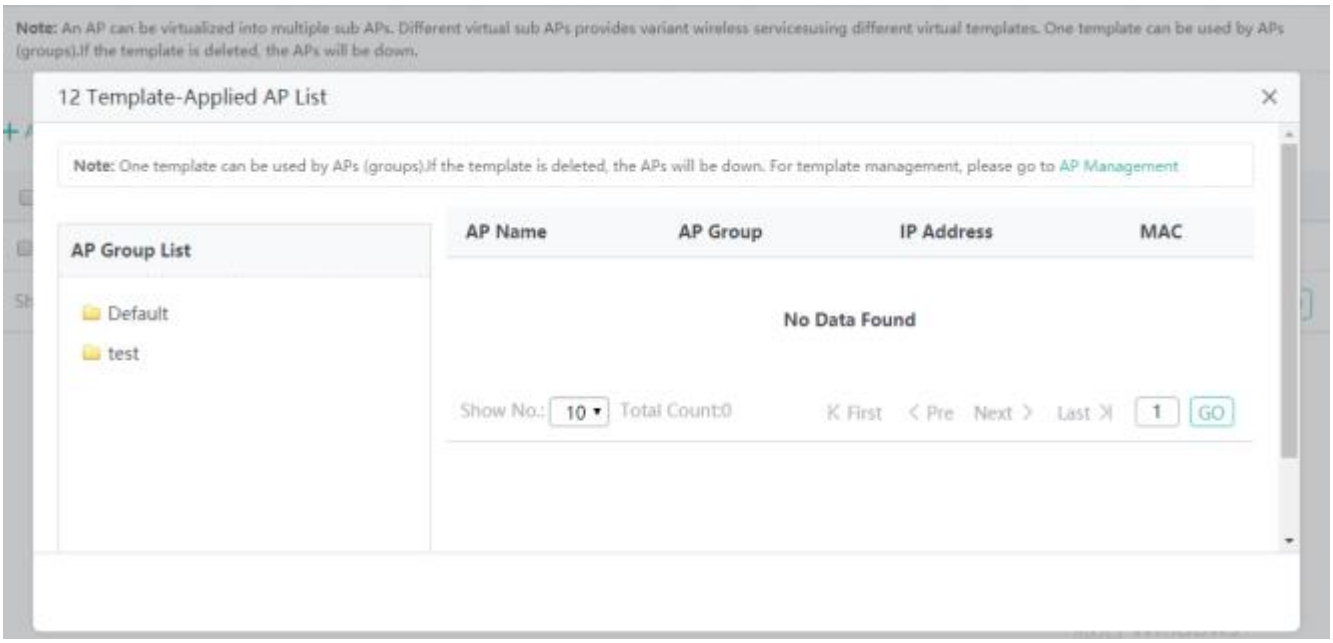
Indicates the client capacity supported by the template.

Uplink Port ID

By default, a virtual AP uses the uplink port ID used by the master AP.

- Details

Click **Details** for a template to list APs to which the template is applied.



Details show the AP groups and APs to which the template is applied.

- Edit

In the template list, click **Edit**. In the displayed window, modify relevant parameters of the template and click **Save**. Parameters for editing a template are the same as those for adding a template and are not described again.

1.3.3.4 Network

1.3.3.4.1 Interface Management

Interface & VLAN

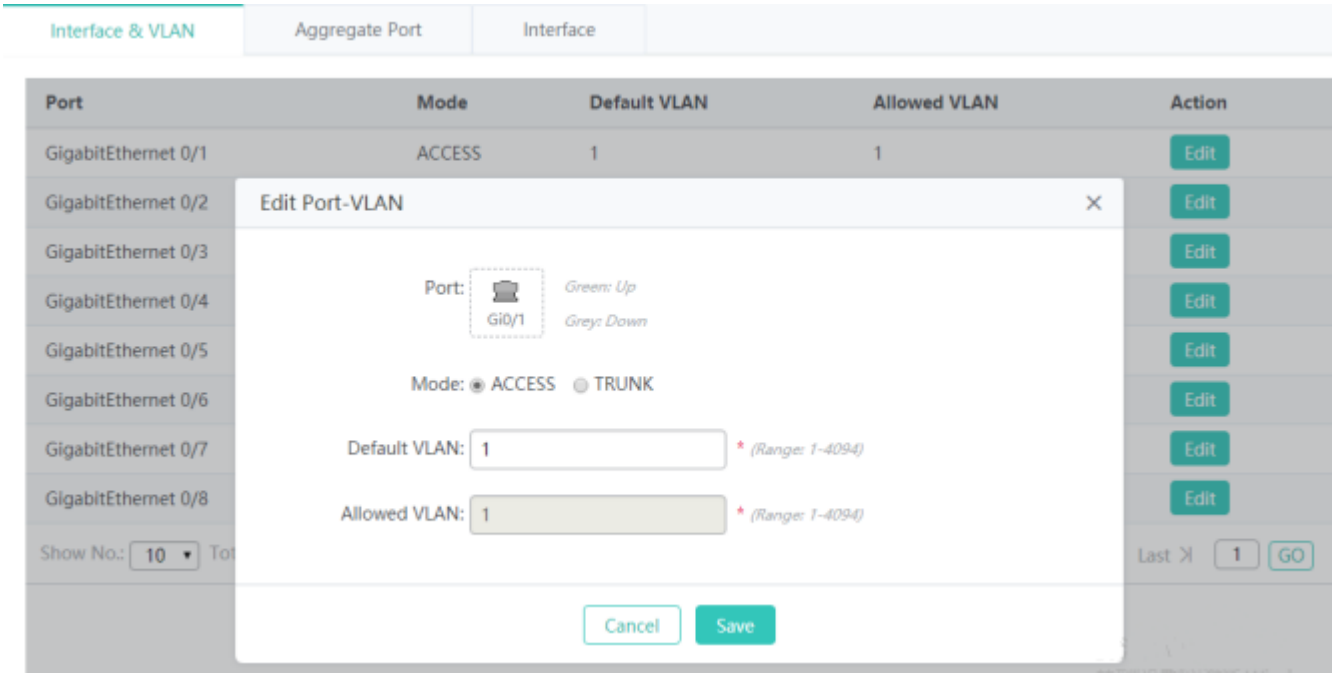
Interface & VLAN | Aggregate Port | Interface

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

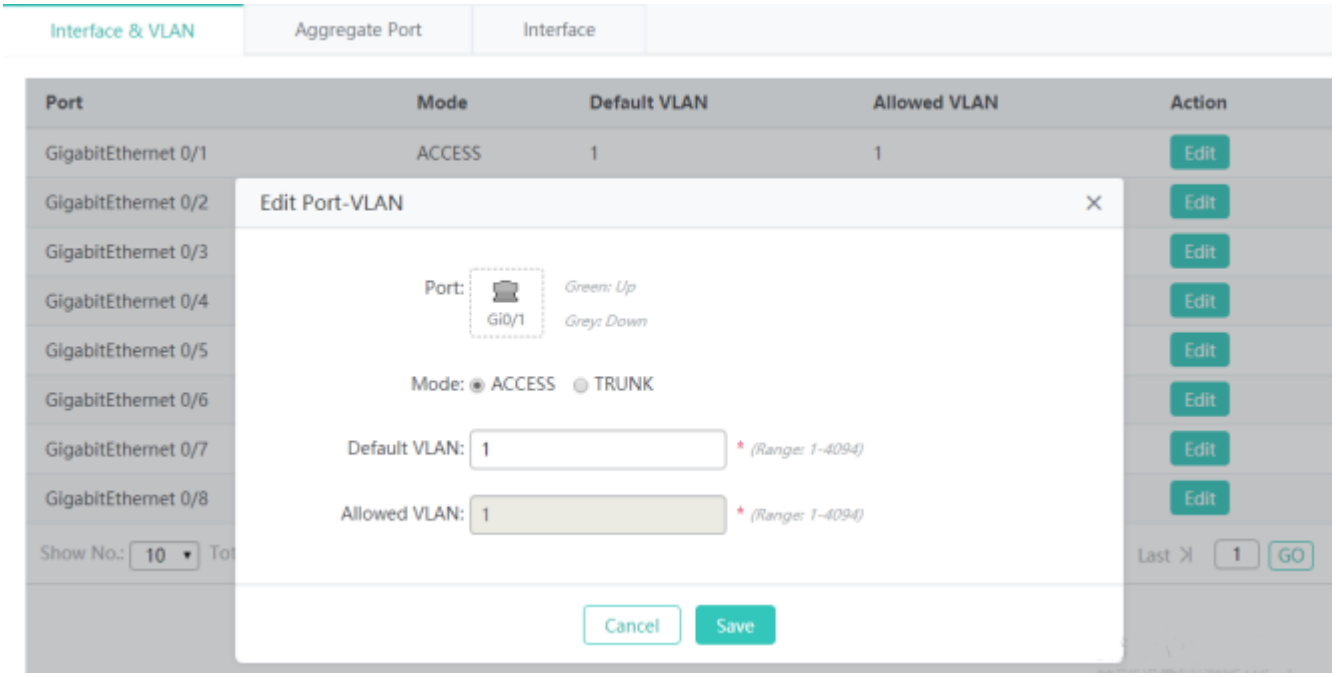
Show No.: 10 Total Count:8 First Pre 1 Next Last 1 GO

- Editing port-VLAN information

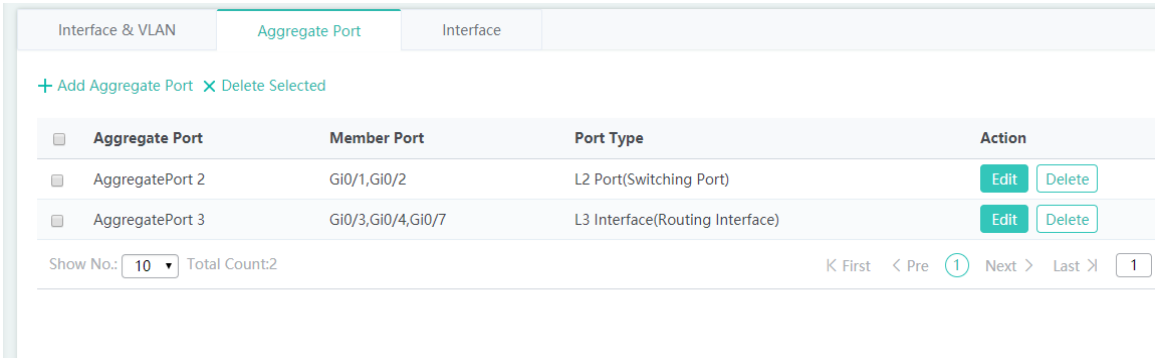
Click **Edit** for an interface in the list. The displayed window shows information about the VLAN of the interface. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.



The port-VLAN information includes the current interface status, interface mode, default VLAN, and allowed VLAN.

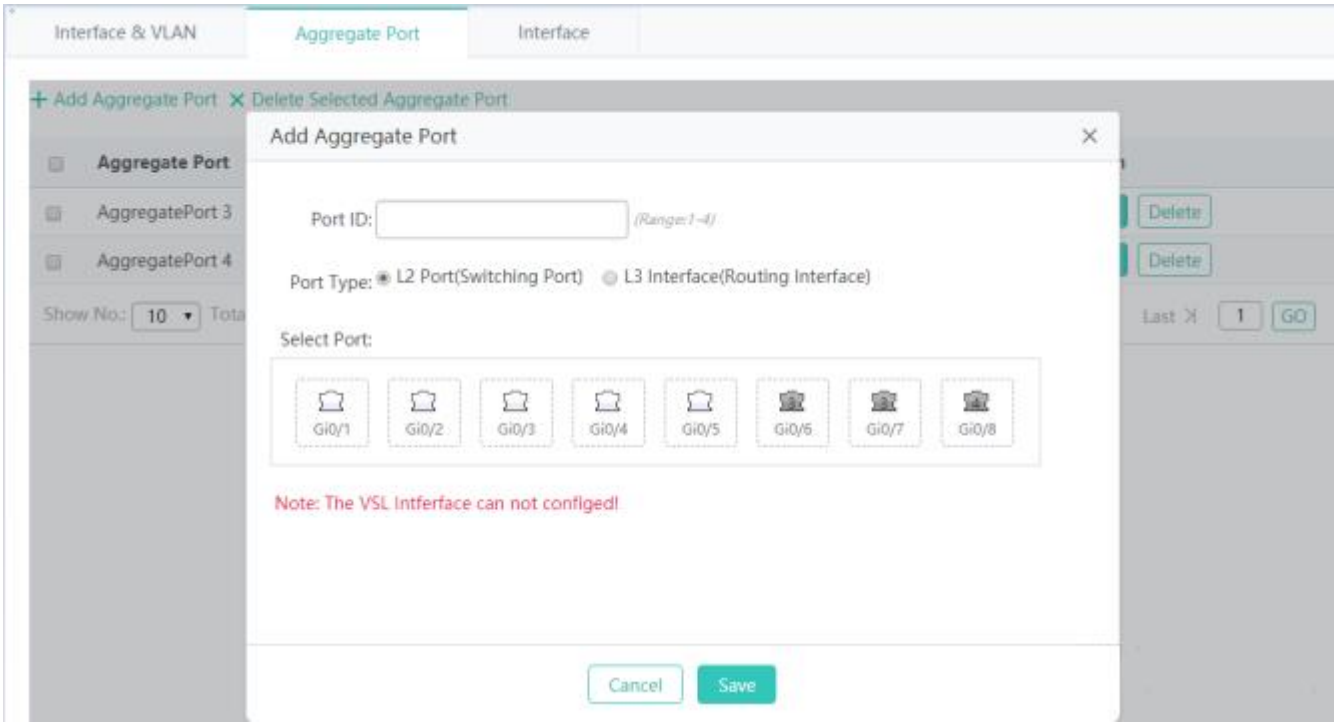


Aggregate Port



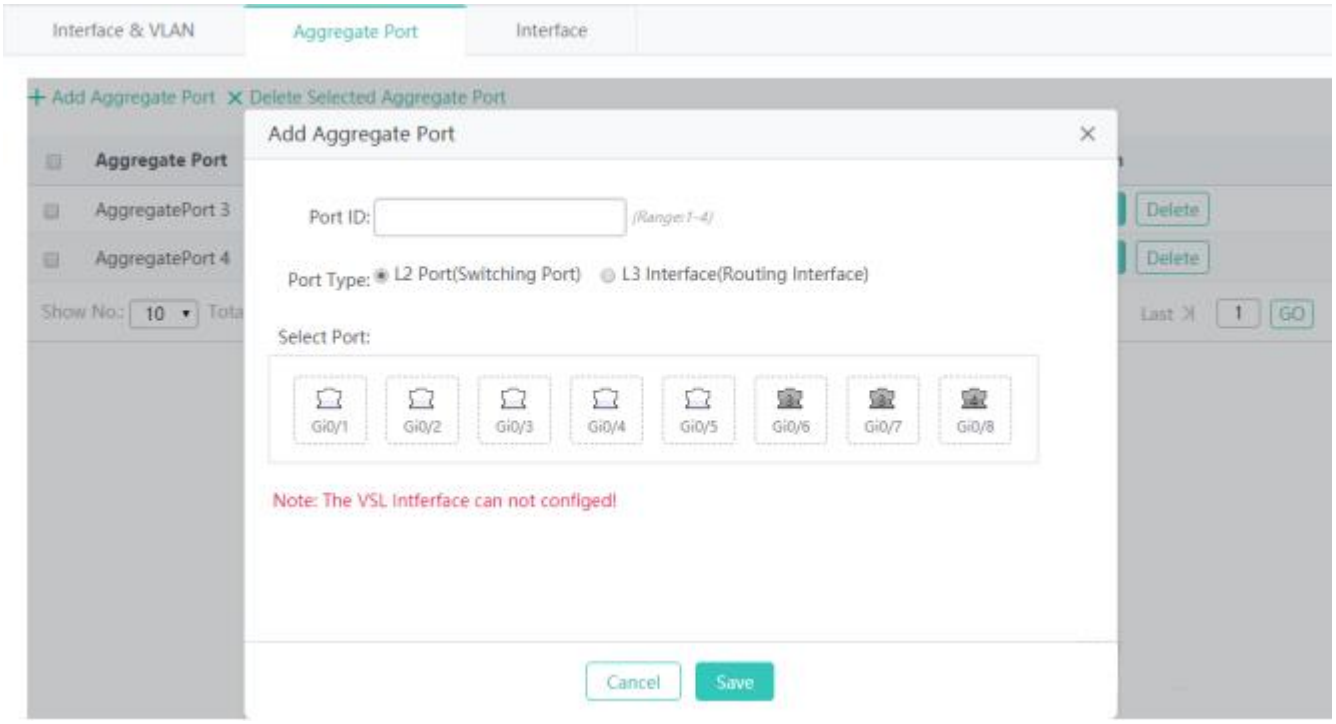
- Adding an aggregate port

Click **Add Aggregate Port**. In the displayed **Add Aggregate Port** window, set parameters and click **Save**. A setting success prompt is displayed and the new aggregate port is displayed in the aggregate port list.



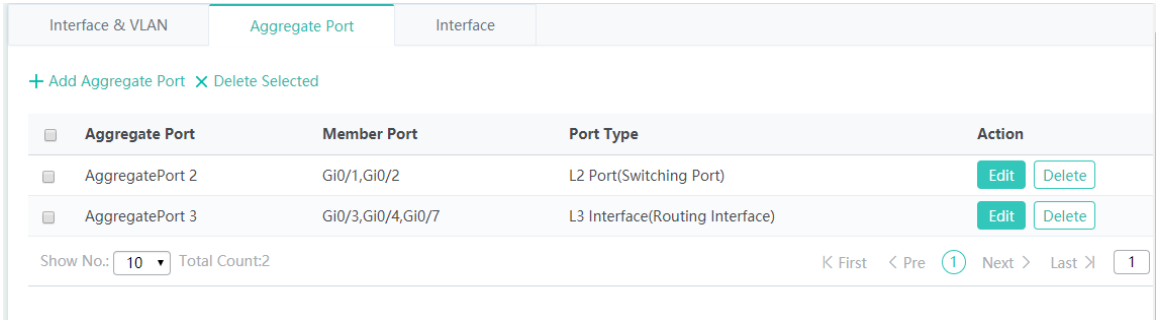
Port ID indicates the ID of an aggregate port.

Select Port shows the member interface selection panel. An interface in grey is an interface that has been added to an aggregate port. The value **1** indicates that the interface belongs to aggregate port 1.



- Batch deleting aggregate ports

Select aggregate ports to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.



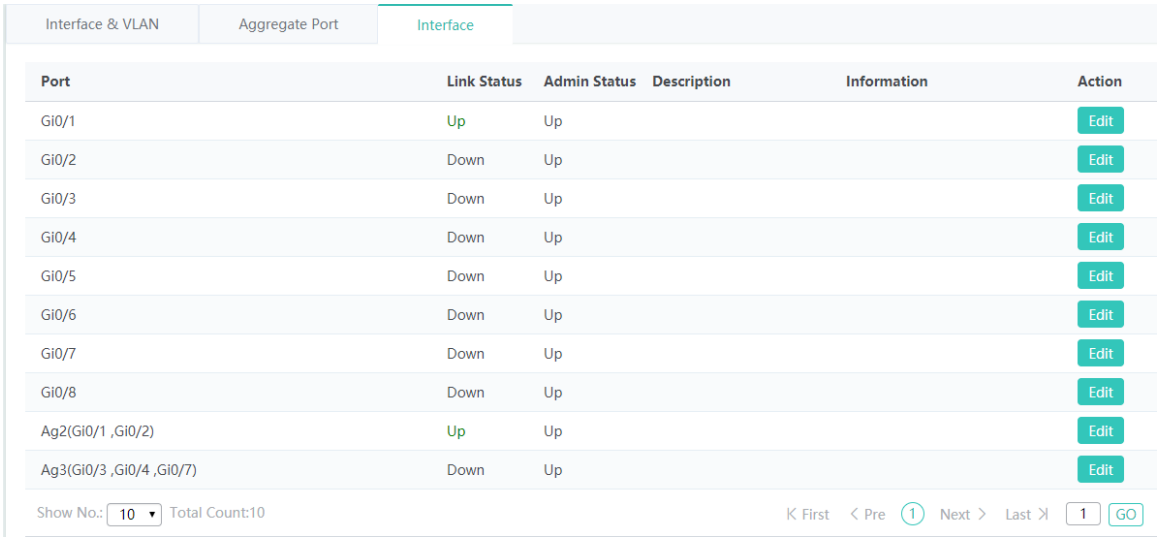
- Editing an aggregate port

Click **Edit** for an aggregate port in the list. The displayed window shows information about the aggregate port. Edit information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

- Deleting an aggregation port

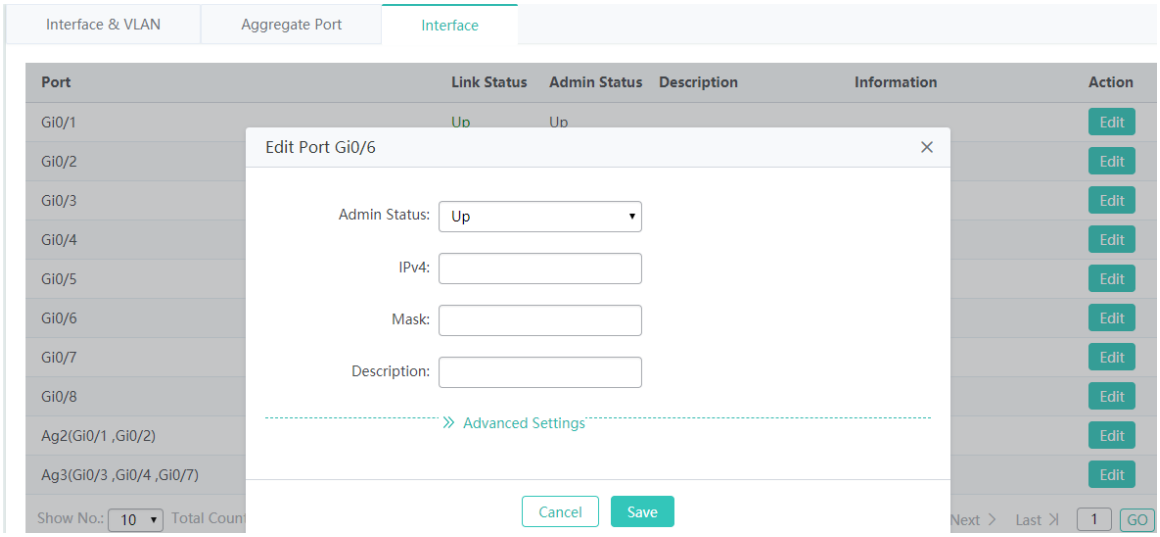
Click **Delete** for an aggregate port in the list. In the displayed confirmation window, click **Save** to complete the delete operation.

Interface



- Editing an interface

Click **Edit** for an interface in the list. The displayed window shows information about the interface. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.



Admin State

Indicates the management state of the interface.

IPv4

Indicates the IPv4 address of the interface.

Mask

Indicates the IPv4 mask of the interface.

Description

Indicates the description or alias of the interface.

Copper/Fiber Port

Indicates the optical/electrical attribute. It is set to the optical interface or electrical interface based on the product capability.

IPv6

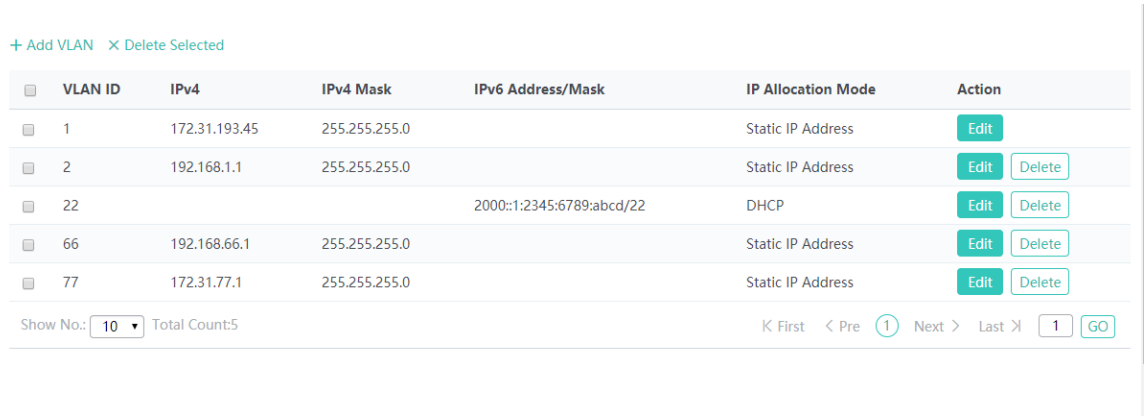
Indicates the IPv6 address of the interface.

Speed

Indicates the interface rate.

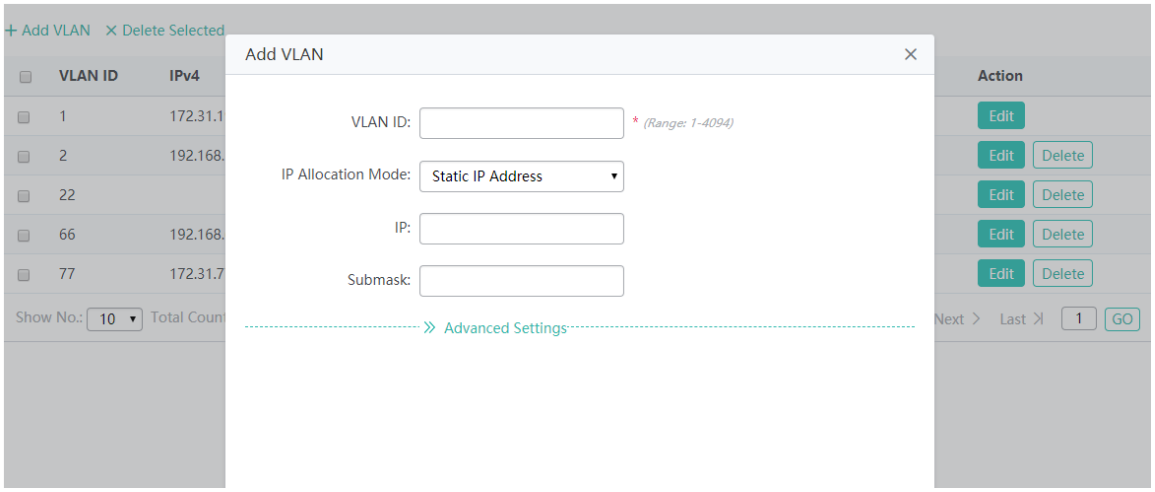
Working Mode Indicates the working mode of the interface. It can be set to **Auto**, **Duplex**, or **Half-Duplex**.

1.3.3.4.2 VLAN Management



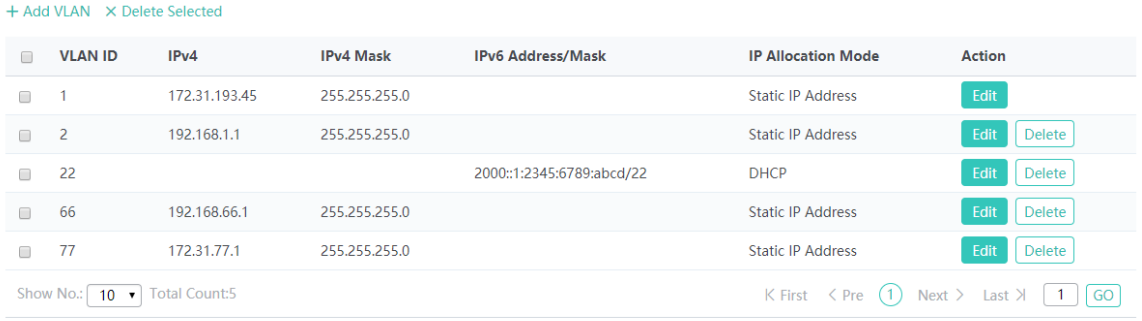
- Adding a VLAN

Click **Add VLAN**. In the displayed **Add VLAN** window, set parameters and click **Save**. A setting success prompt is displayed and the new VLAN is displayed in the VLAN list.



- Batch deleting VLANs

Select VLANs to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.



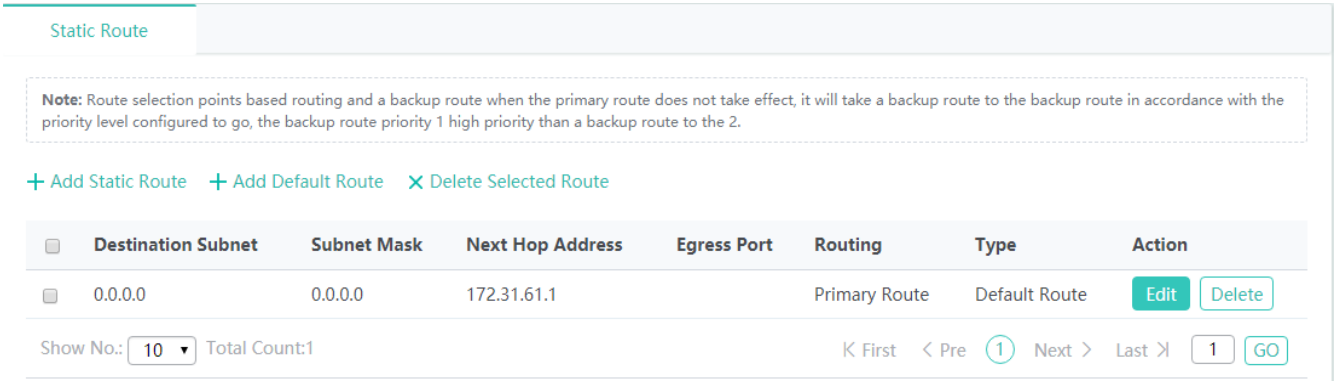
- Editing a VLAN

Click **Edit** for a VLAN in the list. The displayed window shows information about the VLAN. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

- Deleting a VLAN

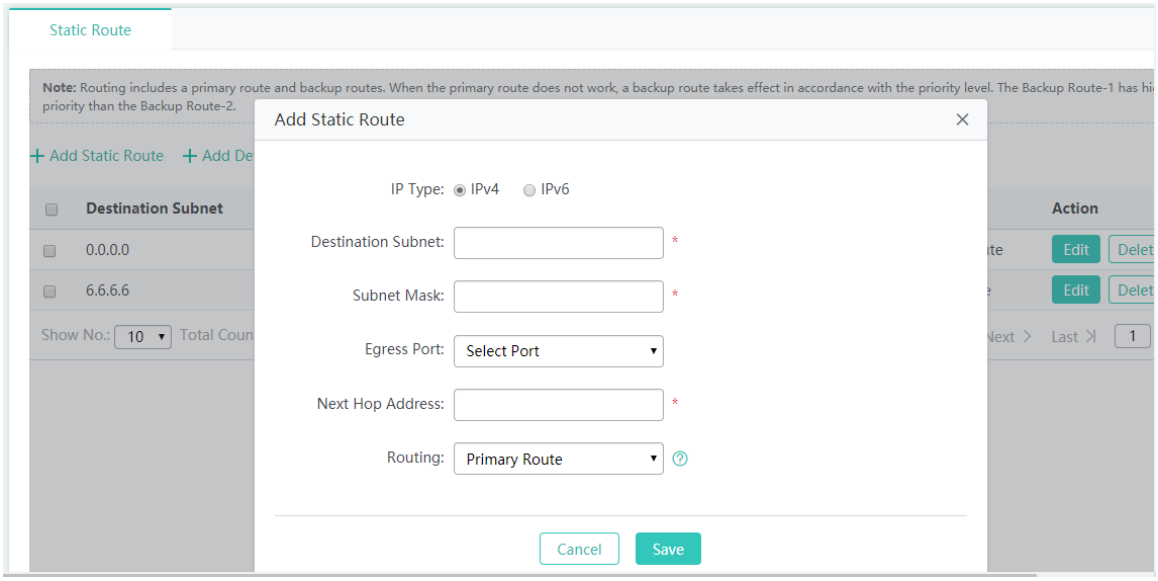
Click **Delete** for a VLAN in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

1.3.3.4.3 Route Management



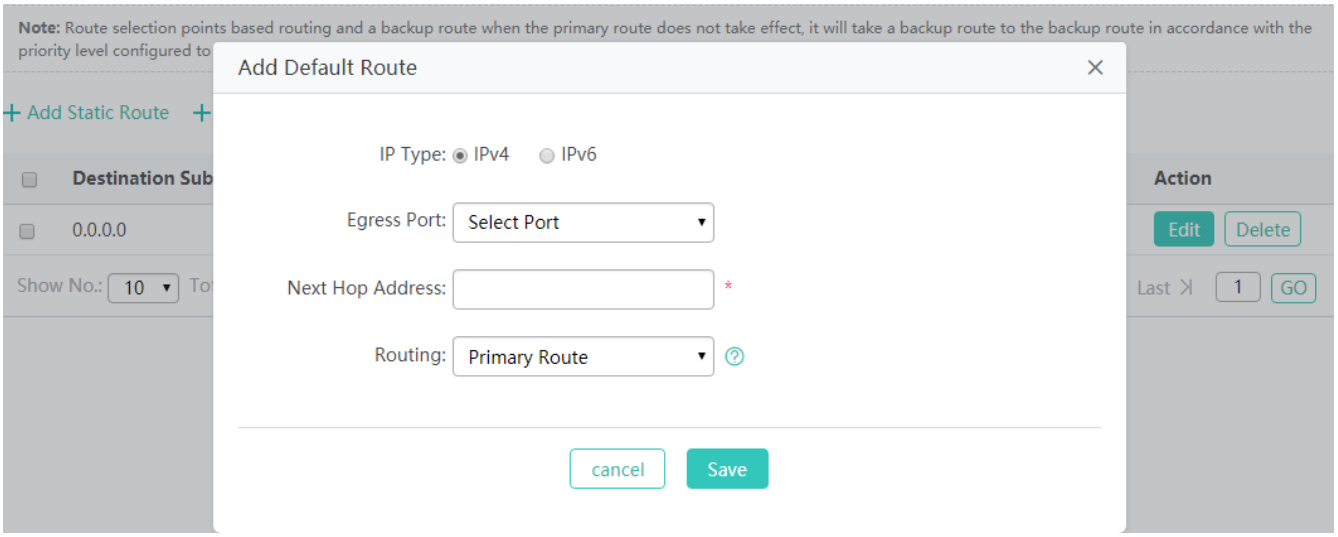
- Adding a static route

Click **Add Static Route**. In the displayed **Add Static Route** window, set parameters and click **Save**. A setting success prompt is displayed and the new static route is displayed in the route list.



- Adding a default route

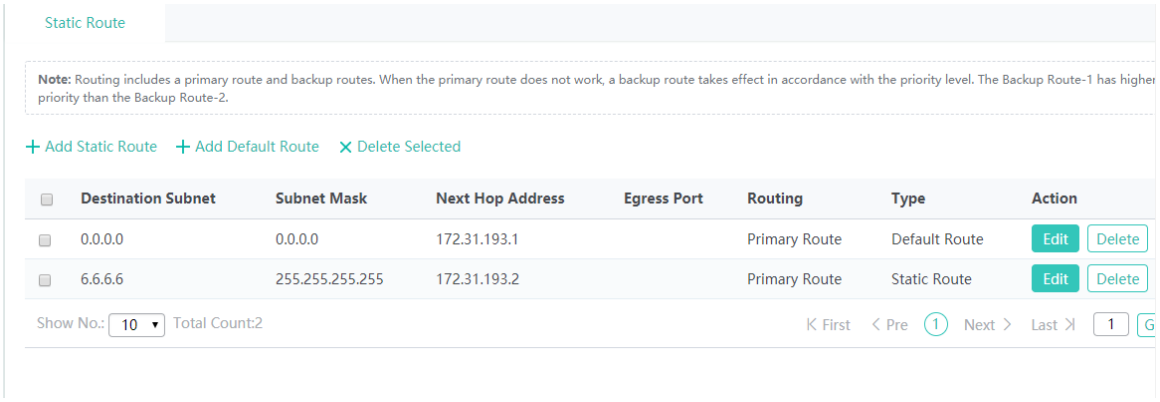
Click **Add Default Route**. In the displayed **Add Default Route** window, set parameters and click **Save**. A setting success prompt is displayed and the new default route is displayed in the route list.



Note: **Routing** can be set to **Primary Route** or **Backup Route**. When the primary route does not take effect, for example, the interface of the primary route is inactive, a backup route is adopted. A backup route is selected based on the configured priority. The priority of backup route 1 is higher than that of backup route 2.

- Batch deleting routes

Select routes to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.



- Editing a route

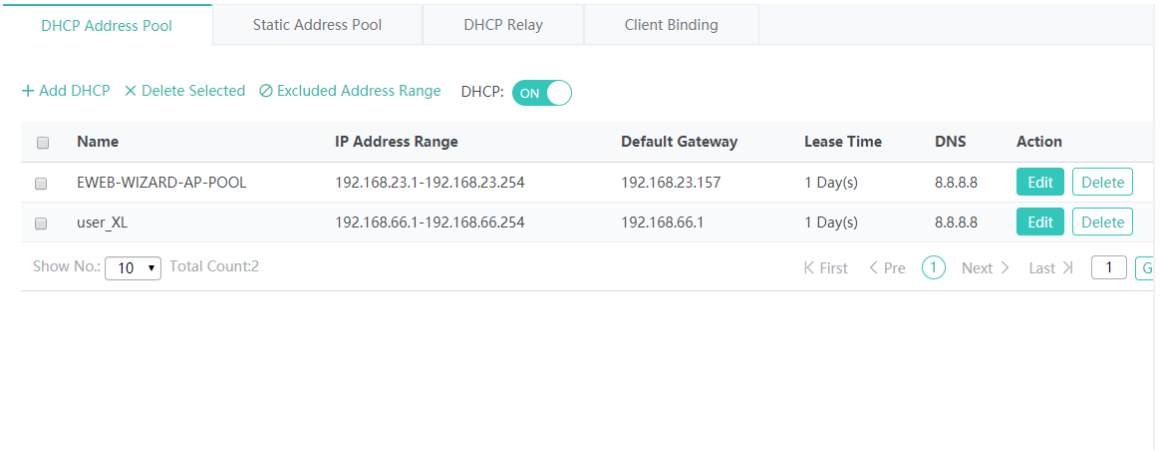
Click **Edit** for a route in the list. The displayed window shows information about the route. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

- Deleting a route

Click **Delete** for a route in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

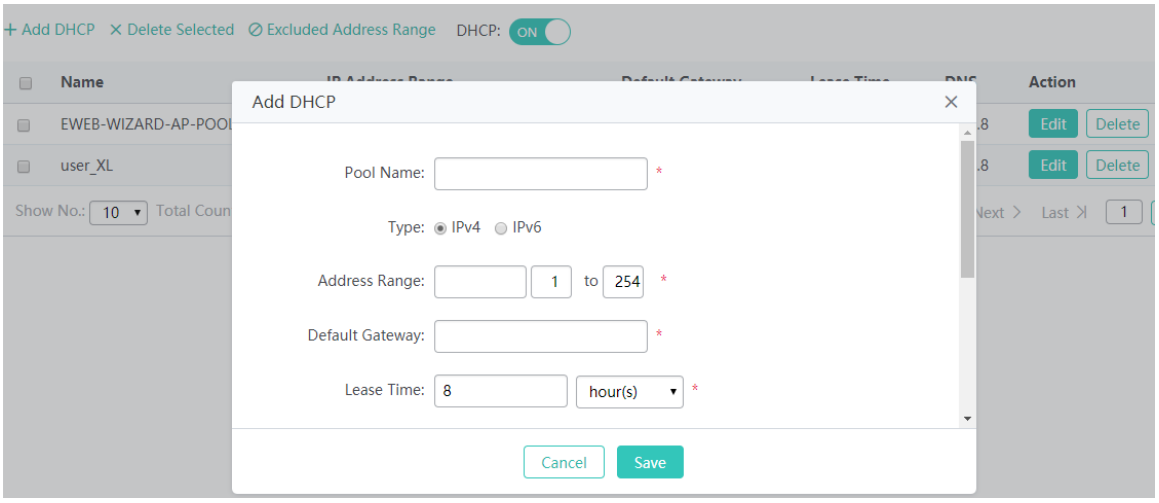
1.3.3.4.4 DHCP Configuration

DHCP Address Pool



- Adding a DHCP address pool

Click **Add DHCP**. In the displayed **Add DHCP** window, set parameters and click **Save**. A setting success prompt is displayed and the new DHCP address pool is displayed in the DHCP address pool list.



Pool Name

Indicates the identifier or name of the DHCP address pool.

Type

Type can be set to **IPv4** or **IPv6**.

Address Range

Indicates the range of the address pool.

Default Gateway

Indicates the default gateway of the address pool.

Lease Time

Indicates the lease time of the address pool. It can be set to permanent or a specific time period.

Preferred DNS Server

Indicates the preferred DNS server used by the address pool client.

Secondary DNS Server

Indicates the secondary DNS server of the address pool client.

Option 138

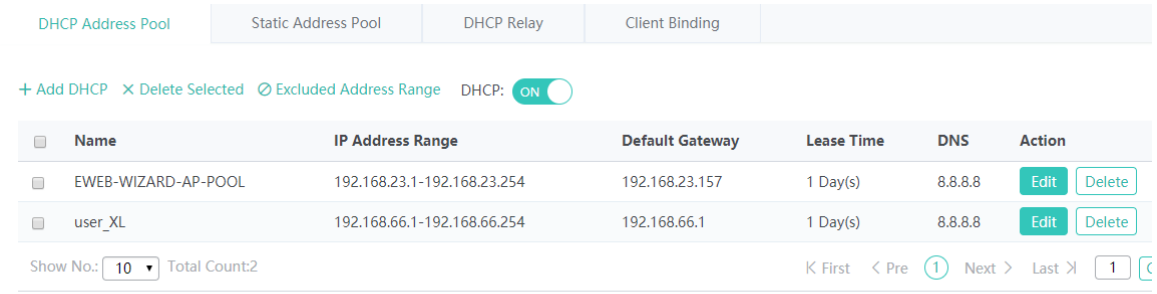
Notifies an AP of the AC IP address in WLAN management, so that the AP can register with the AC. It is generally set to the loopback address of the AC. This parameter is applicable to Ruijie products.

Option 43

Notifies an AP of the AC IP address in WLAN management, so that the AP can register with the AC. It is generally set to the loopback address of the AC. This is a common protocol option.

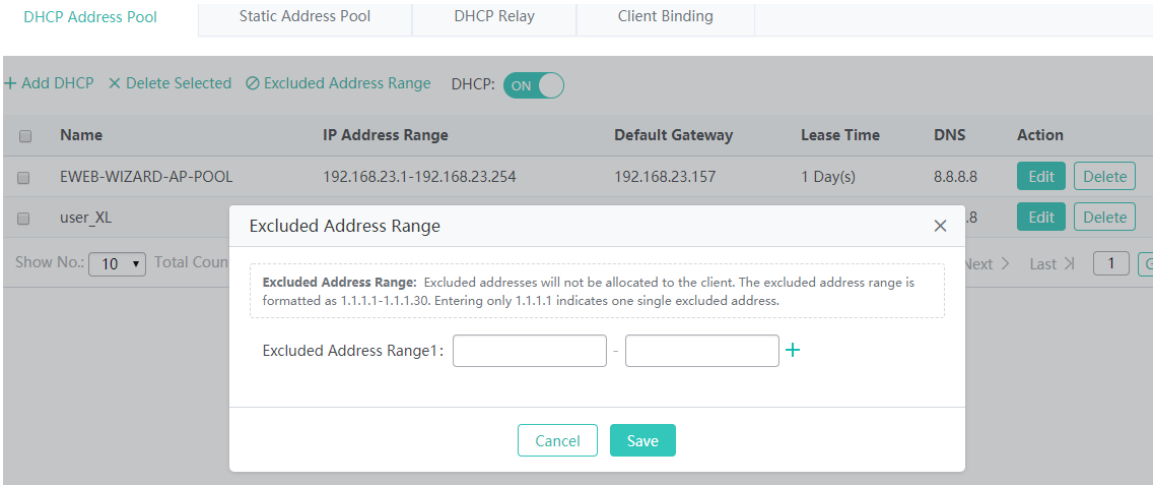
- Batch deleting DHCP address pools

Select DHCP address pools to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

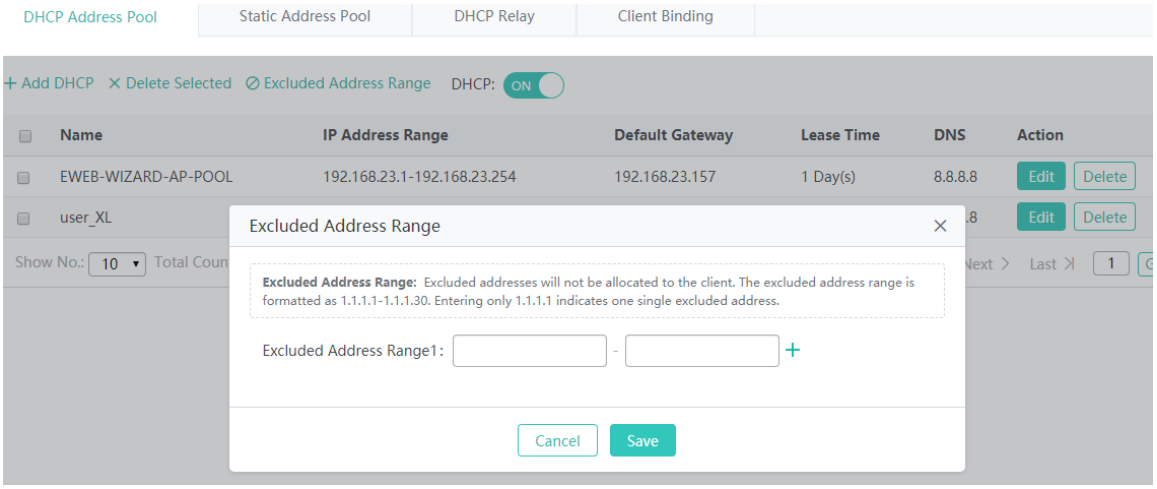


- Configuring an excluded IP address range

Click **Excluded Address Range**. In the displayed **Excluded Address Range** window, set parameters and click **Save**. A setting success prompt is displayed and the excluded address range is displayed in the DHCP list.

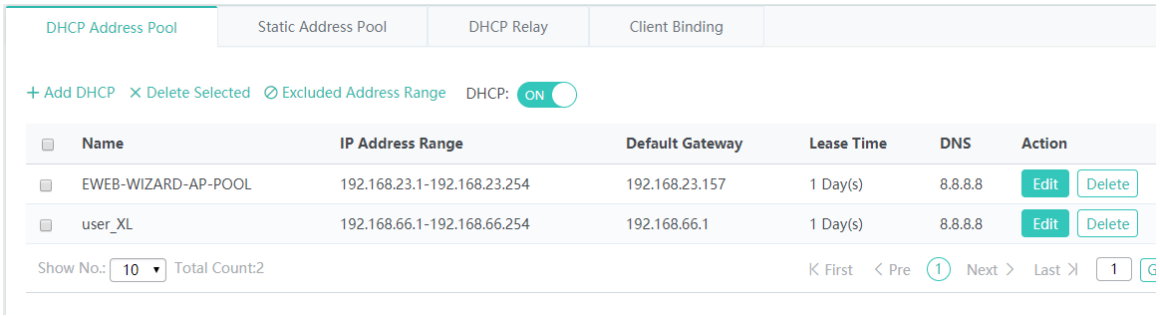


Excluded Address can be set to multiple IP address ranges. IP addresses in these ranges are not allocated to STAs.



- DHCP service switch

Click the icon next to **DHCP** to enable/disable the DHCP service.



- Editing a DHCP address pool

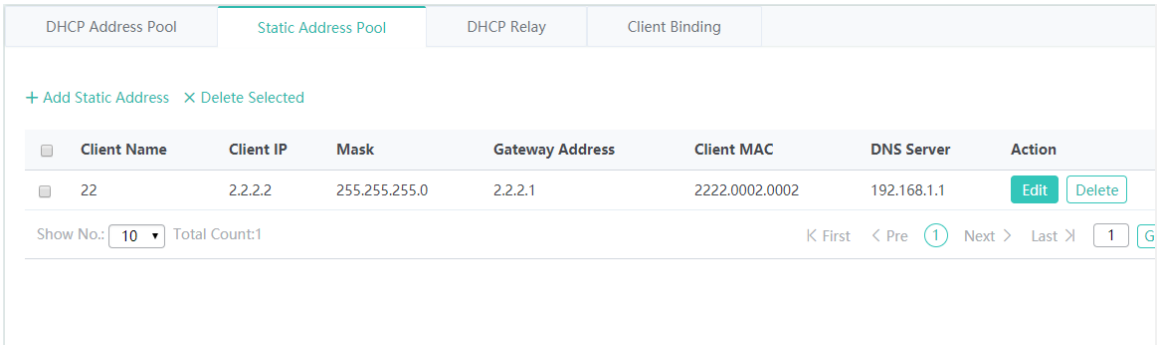
Click **Edit** for a DHCP address pool in the list. The displayed window shows information about the DHCP address pool. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

Parameters for editing a DHCP address pool are the same as those for adding a DHCP address pool and are not described again.

- Deleting a DHCP address pool

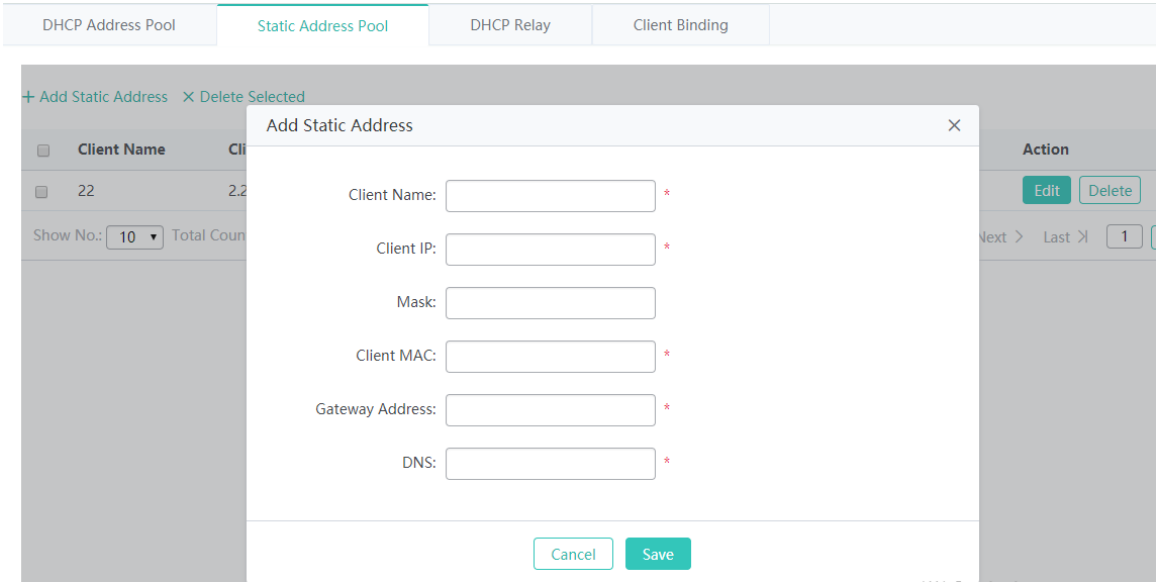
Click **Delete** for a DHCP address pool in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

Static Address Pool



- Adding a static address

Click **Add Static Address**. In the displayed **Add Static Address** window, set parameters and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.



Client Name

Indicates the name of a client to which a static address is to be allocated.

Client IP

Indicates the allocated IP address.

Mask

Indicates the IP address mask.

Client MAC

Indicates the MAC address bound to the client.

Gateway Address

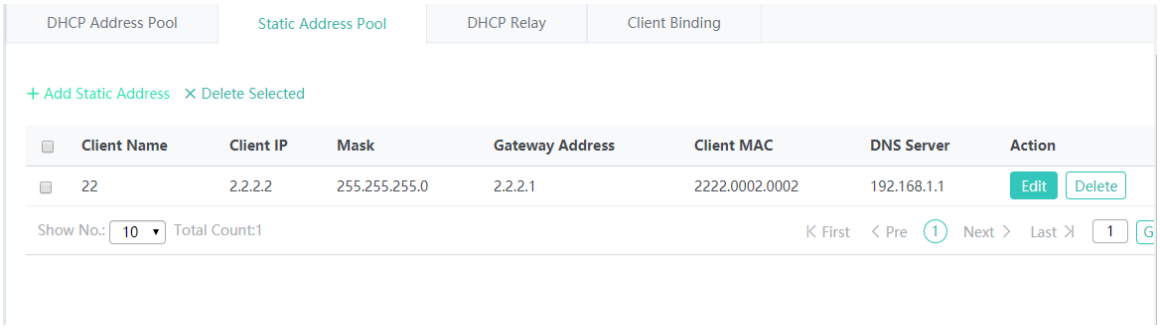
Indicates the egress gateway of the client. It is mandatory.

DNS

Indicates the egress DNS server of the client. It is mandatory.

- Batch deleting static addresses

Select static addresses to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.



- Editing a static address

Click **Edit** for a static address in the list. The displayed window shows information about the static address. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

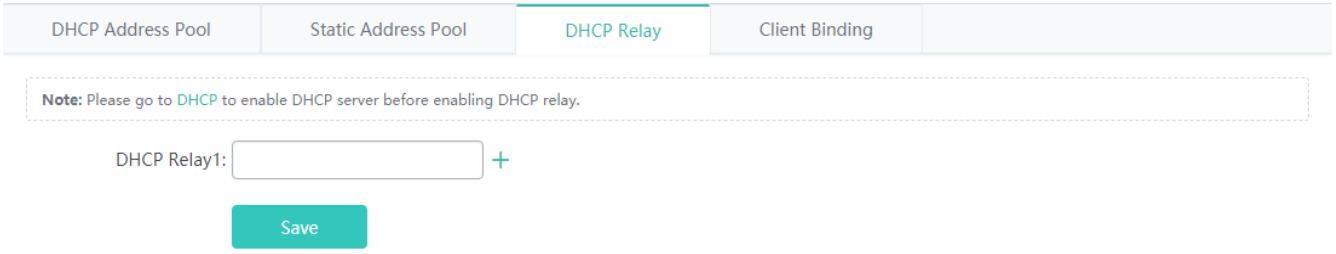
The parameters for editing a static address are the same as those for adding a static address and are not described again.

- Deleting a static address

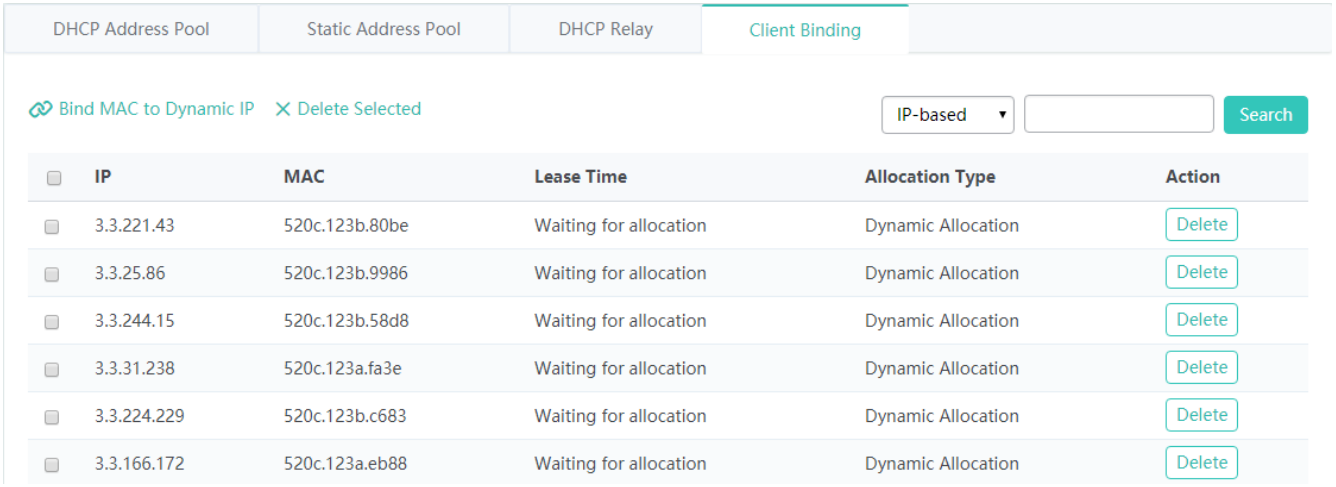
Click **Delete** for a static address in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

DHCP Relay

Enter the relay server in the text box and click **Save**. You can click **+** to add another relay server.

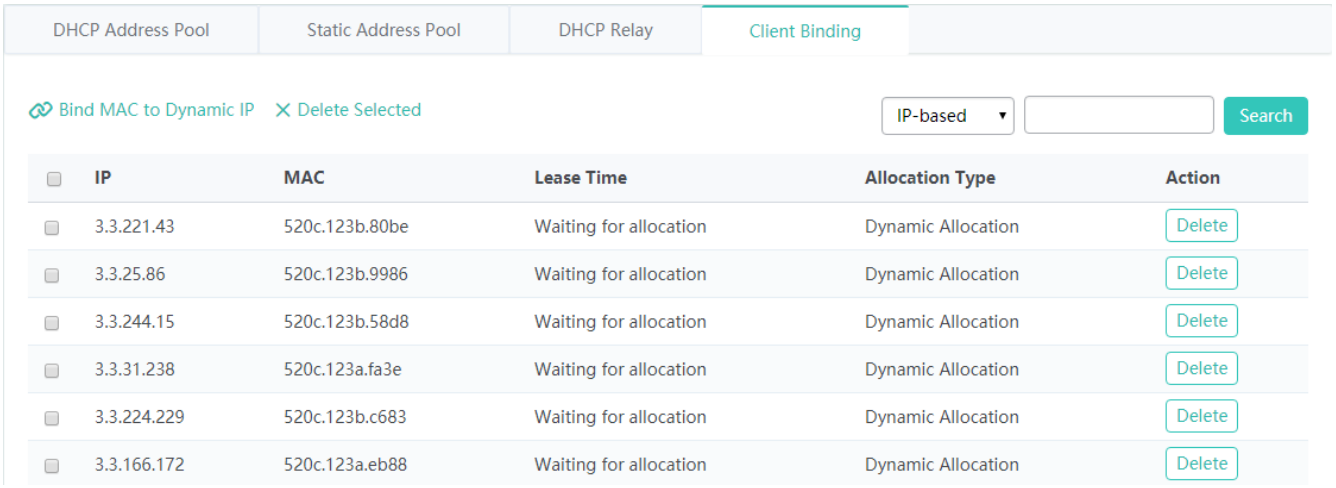


Client Binding



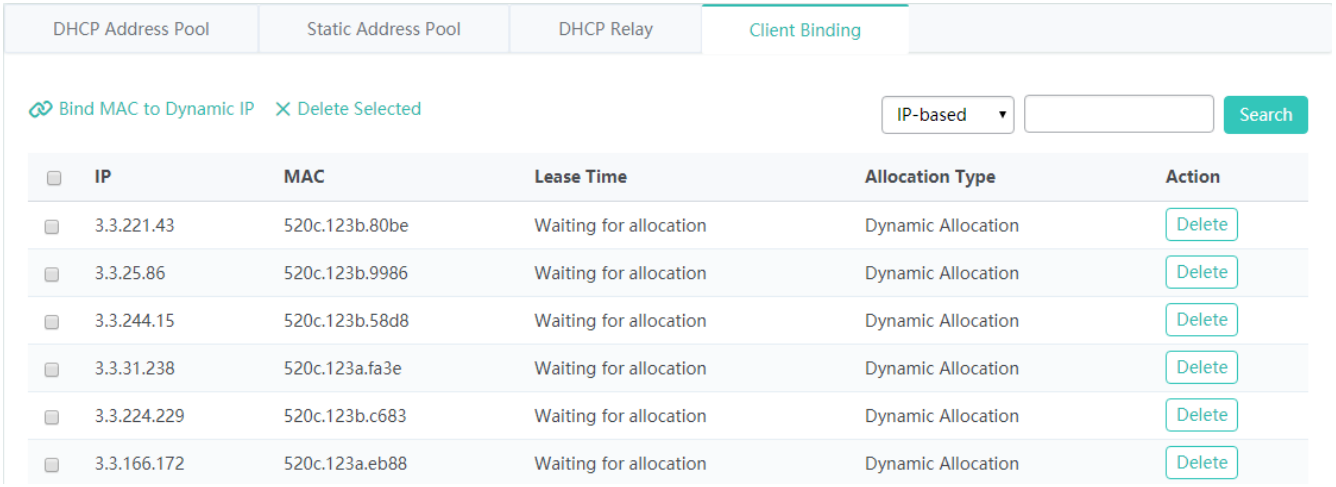
- Binding a MAC address to a dynamically obtained IP address

Select a static address to be bound from the list, click **Bind MAC to Dynamic IP**. In the displayed confirmation window, click **OK** to complete the operation.



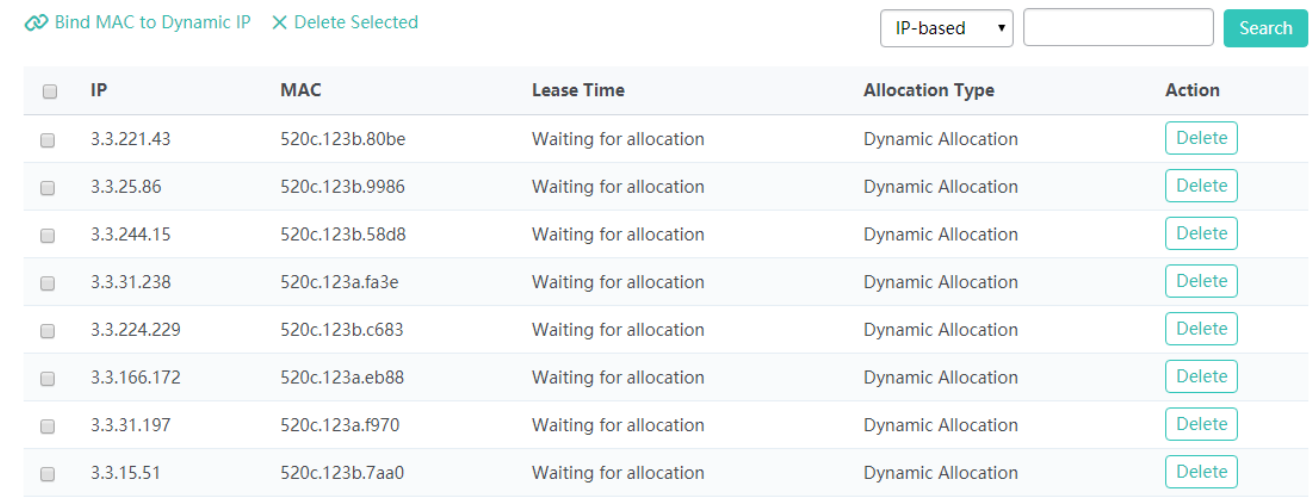
- Batch deleting client bindings

Select static addresses to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the operation.



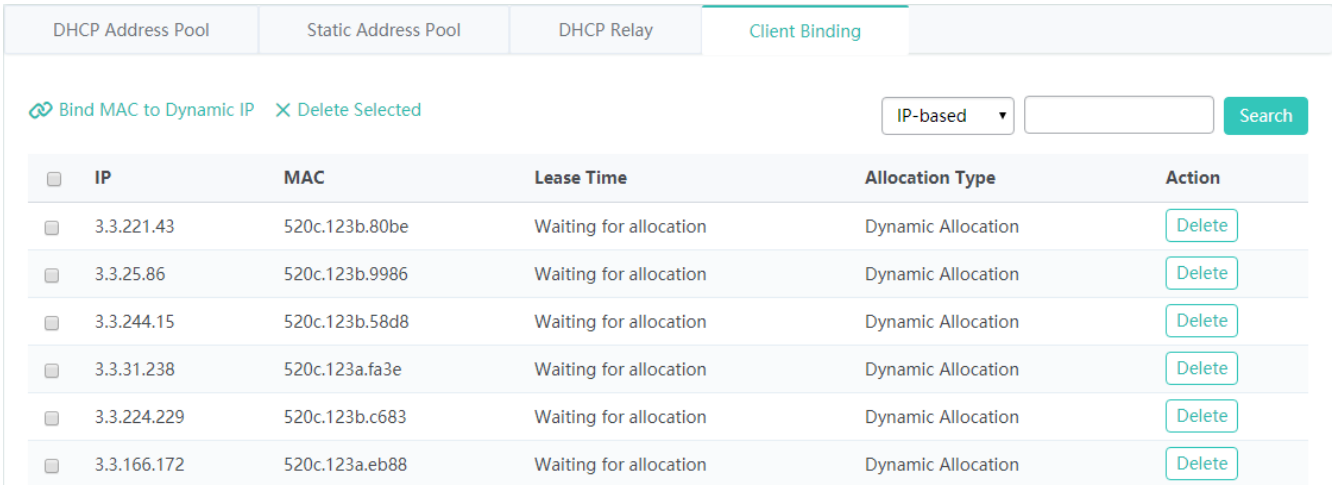
- Deleting a client binding

Click **Delete** for a bound client in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

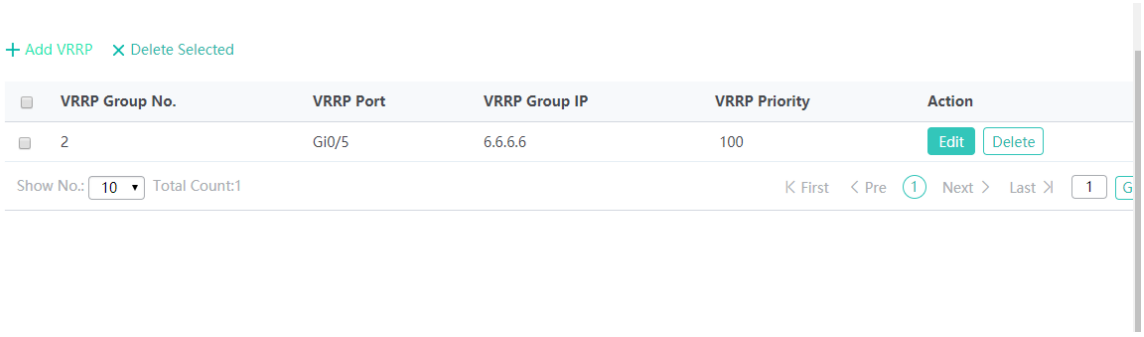


- Searching for clients by IP address

Enter the IP address to be searched for in the search box and click **Search**. Search results that meet the search condition are displayed in the list.

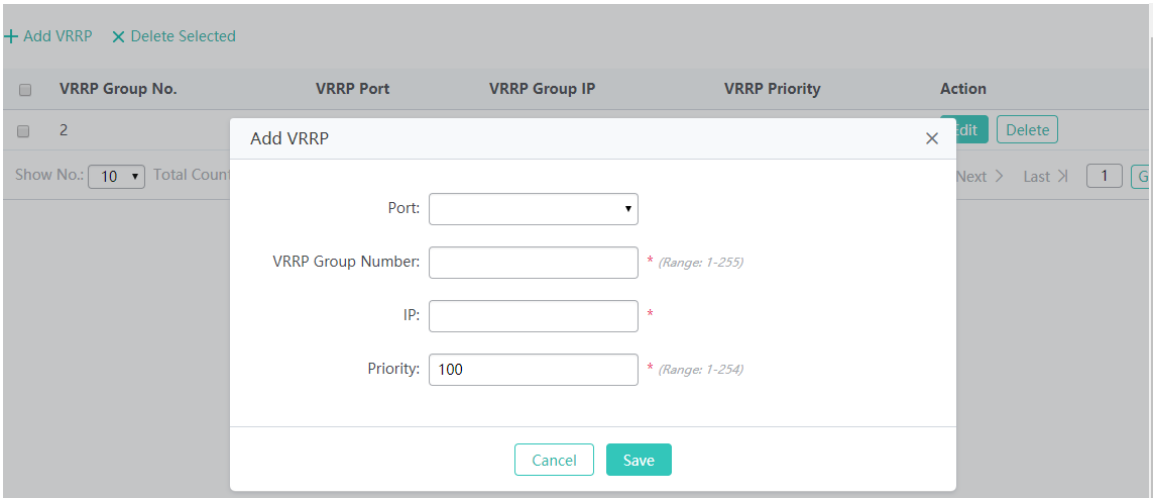


1.3.3.4.5 VRRP Configuration



- Adding a VRRP group

Click **Add VRRP**. In the displayed **Add VRRP** window, set parameters and click **Save**. A setting success prompt is displayed and the new VRRP group is displayed in the VRRP group list.



- Batch deleting VRRP groups

Select VRRP groups to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

- Editing a VRRP group

Click **Edit** for a VRRP group in the list. The displayed window shows information about the VRRP group. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

- Deleting a VRRP group

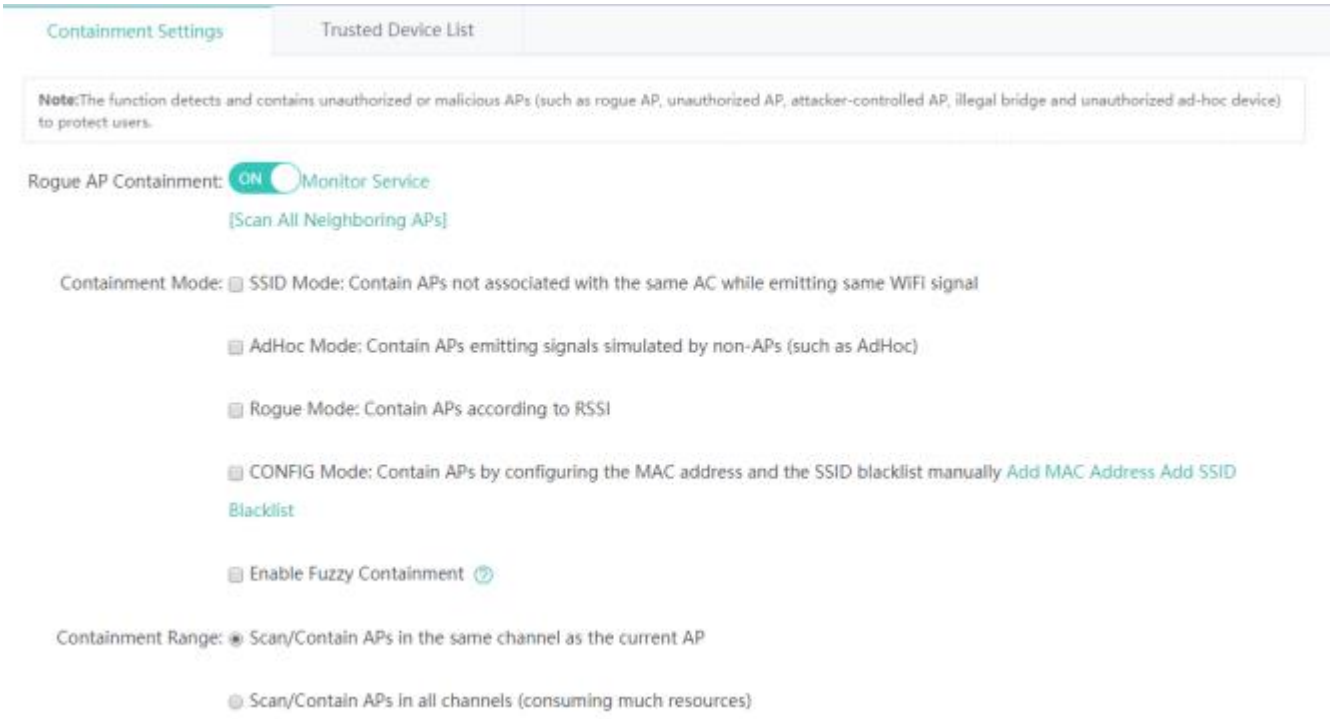
Click **Delete** for a VRRP group in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

1.3.3.5 Security

1.3.3.5.1 Rogue AP Containment

Rogue APs may exist on a WLAN, and may be vulnerable in security or controlled by attackers, seriously threatening or endangering the security of the user network. The containment function enabled on the AC can attack rogue APs so that STAs cannot associate with the rogue APs.

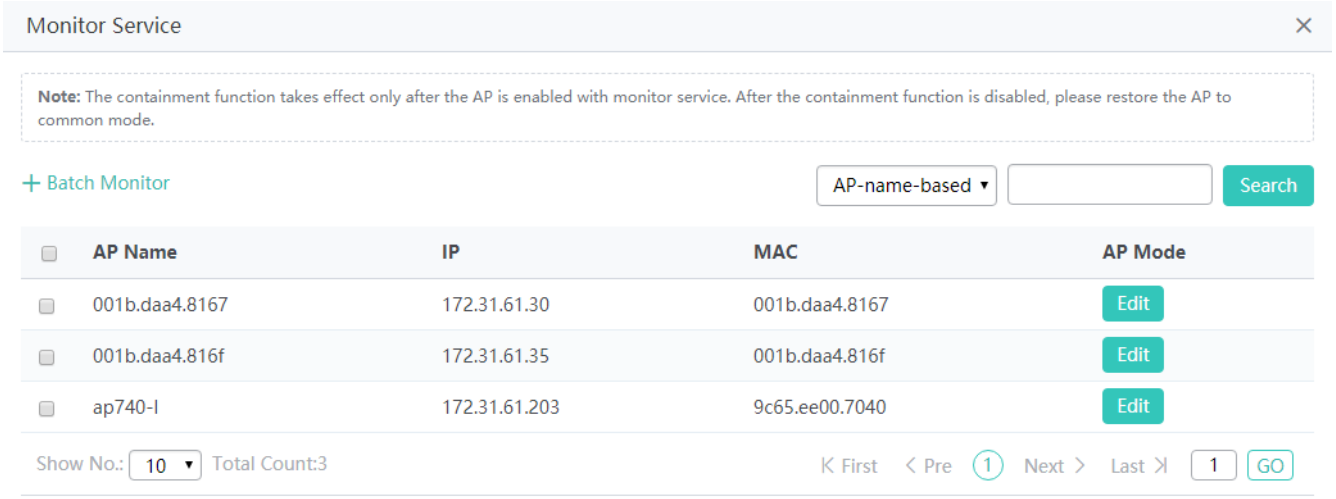
↘ Containment Settings



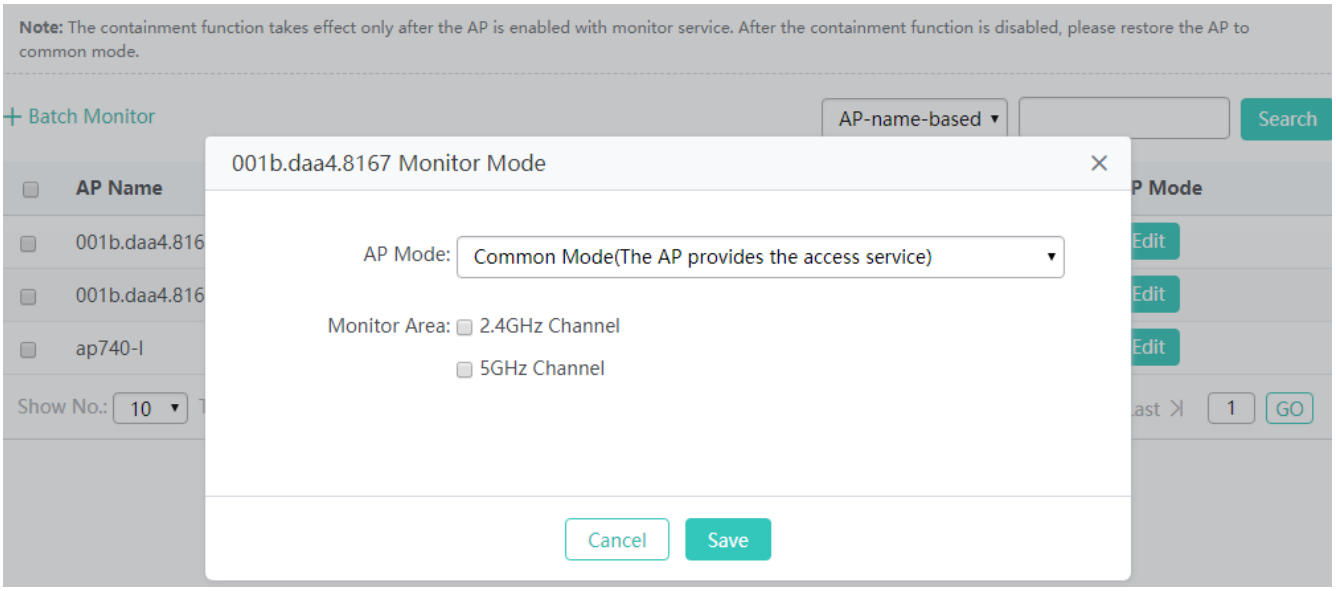
On this page, enable or disable the rogue AP containment function of the AC.

- Enabling the monitoring mode of a specified AP

The containment function on an AP takes effect only after the AP is configured to work in hybrid mode or monitoring mode.



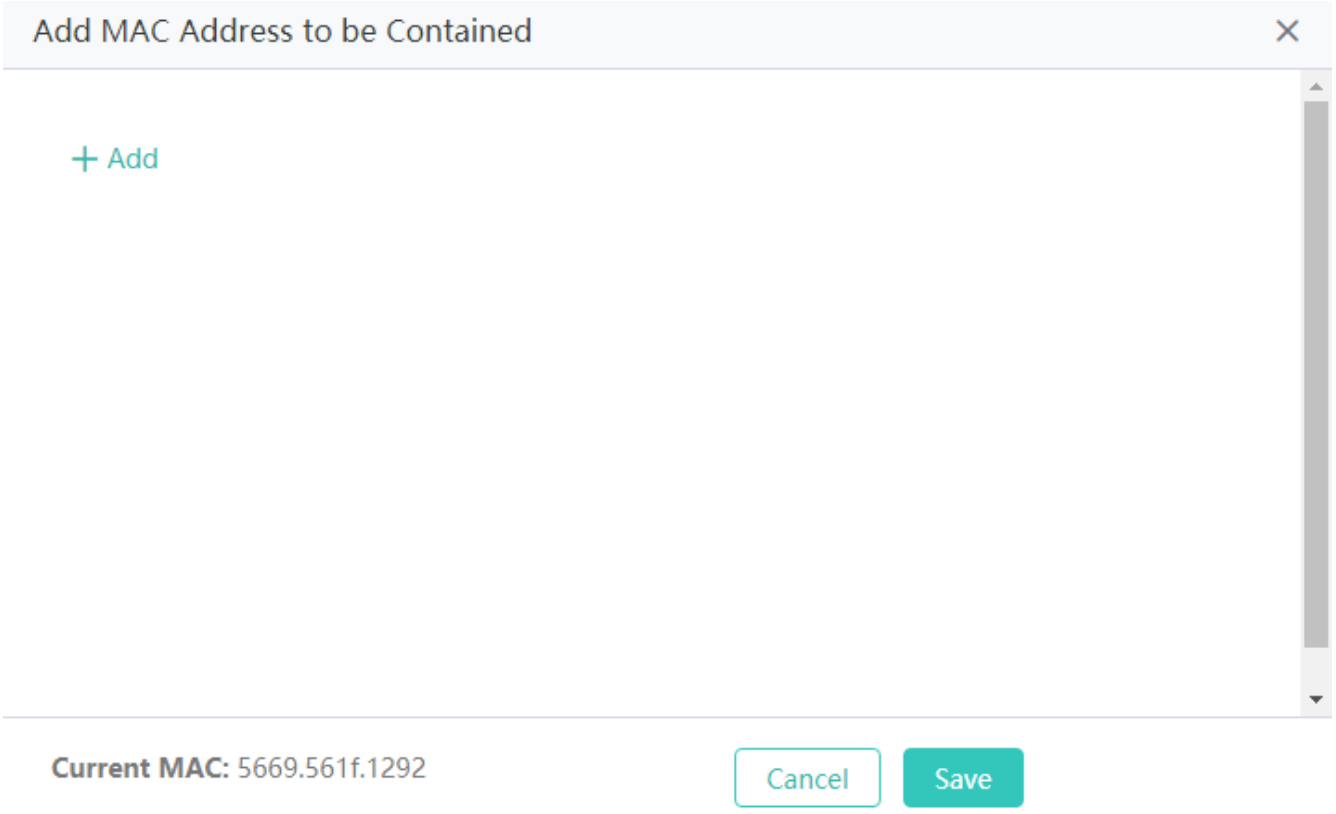
Click **Edit** for an AP in the list. The displayed window shows information about the AP. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.



- Adding the MAC address of a wireless AP

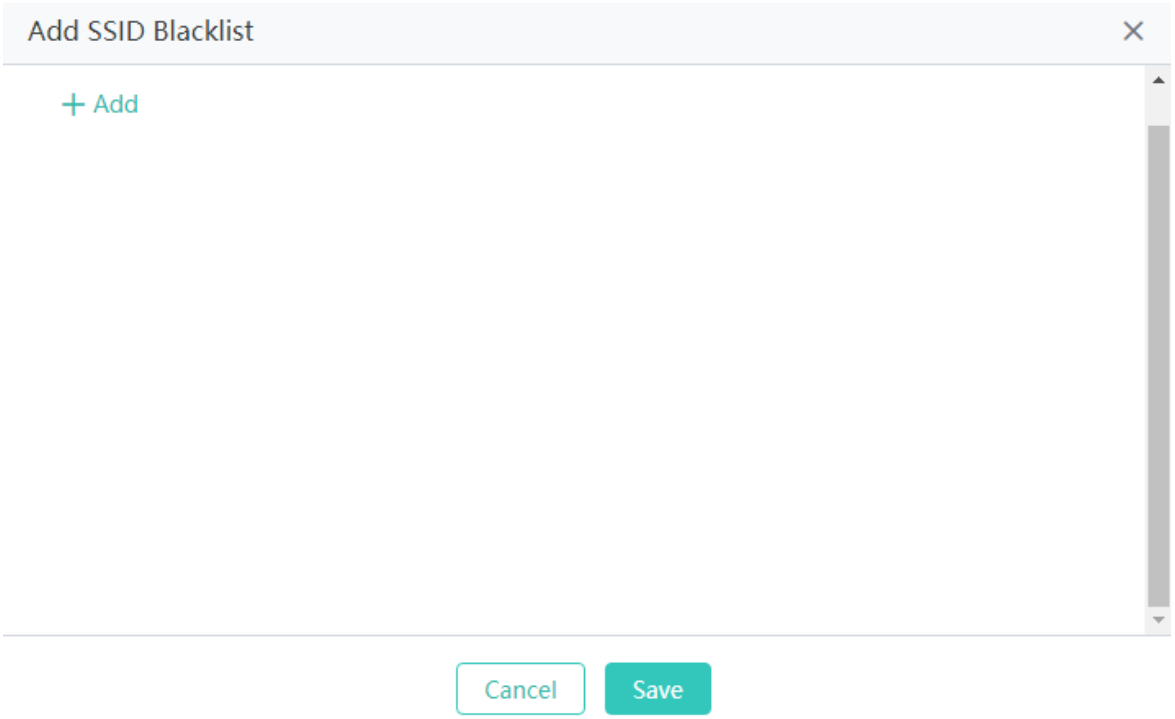
MAC addresses added in **Add MAC Address to be Configured** are MAC addresses to be contained.

Click **Add**, enter the MAC address to be added, and click **Save** to complete the operation.



- Blacklisting an SSID

Click **Add**, enter the SSID to be blacklisted, and click **Save** to complete the operation.



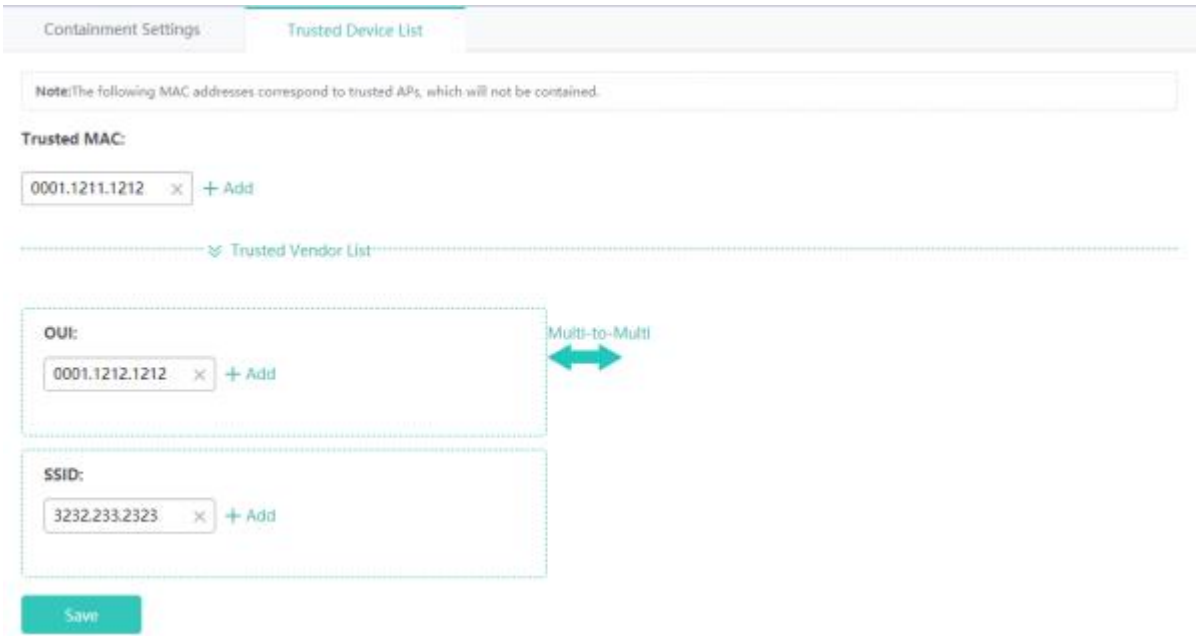
Trusted Device List

After the rogue AP containment is enabled on an AC, unauthorized APs are contained. Some APs are trusted devices and need special processing. You can configure the MAC address of a trusted device.

Click **+Add** below **Trusted MAC** to add the MAC addresses of multiple trusted devices.

Click **+Add** below **OUI** to add identifiers of multiple vendors.

Click **+Add** below **SSID** to add multiple WiFi networks.



1.3.3.5.2 Blacklist and Whitelist Configuration

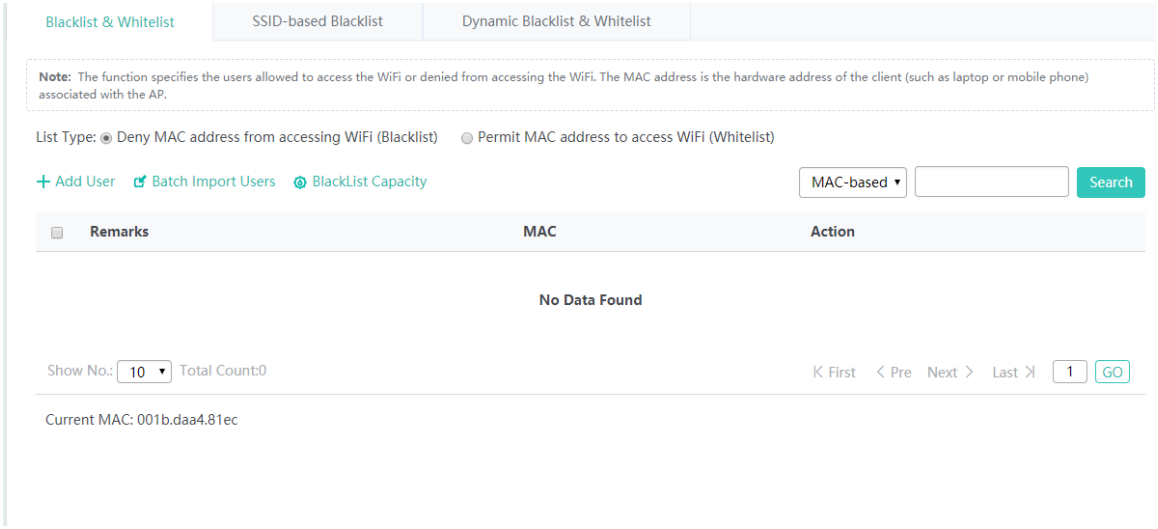
Blacklist & Whitelist

The access of wireless users can be controlled to allow or deny some specific users, to enhance the WLAN security.

A maximum of 1024 users are denied to access the WiFi network by default.

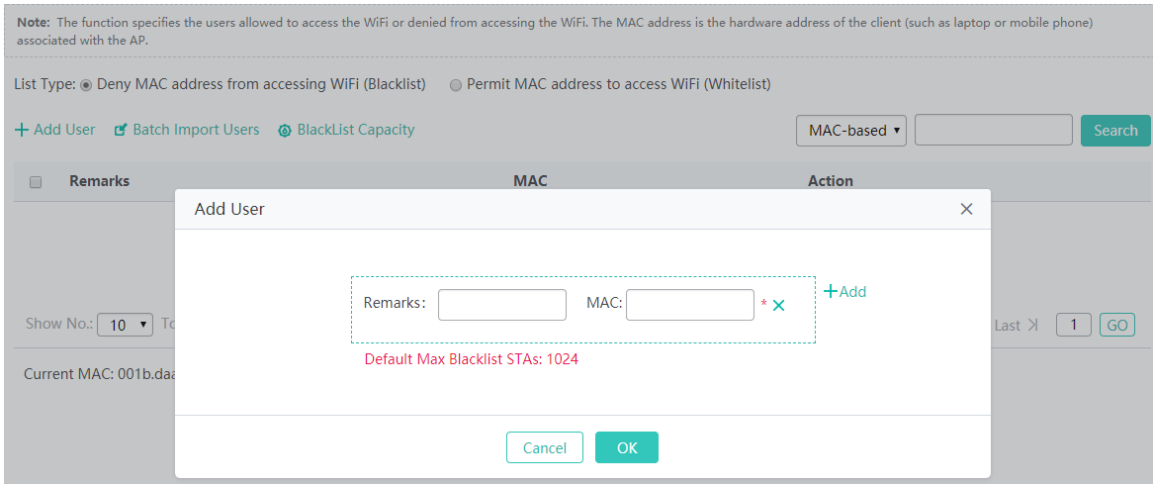
A maximum of 1024 users are allowed to access the WiFi network by default.

Specify the MAC address-based control type in **List Type**, that is, select the whitelist or blacklist.



- Adding a user

Click **Add User** and enter the MAC address of a user. Multiple MAC addresses can be added.



- Deleting a user

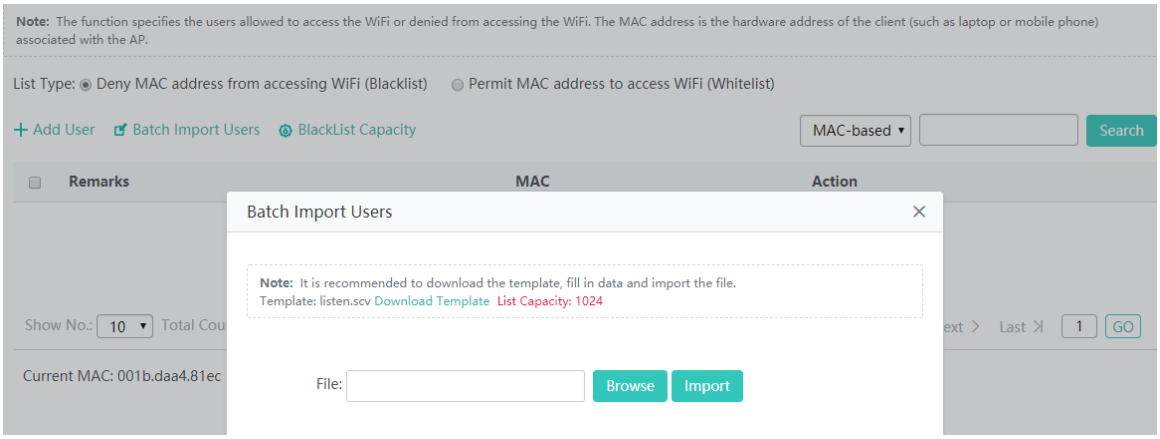
Click **Delete** for a user in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

- Batch deleting users

Select multiple records in the user list and click **Delete Selected** to batch delete users.

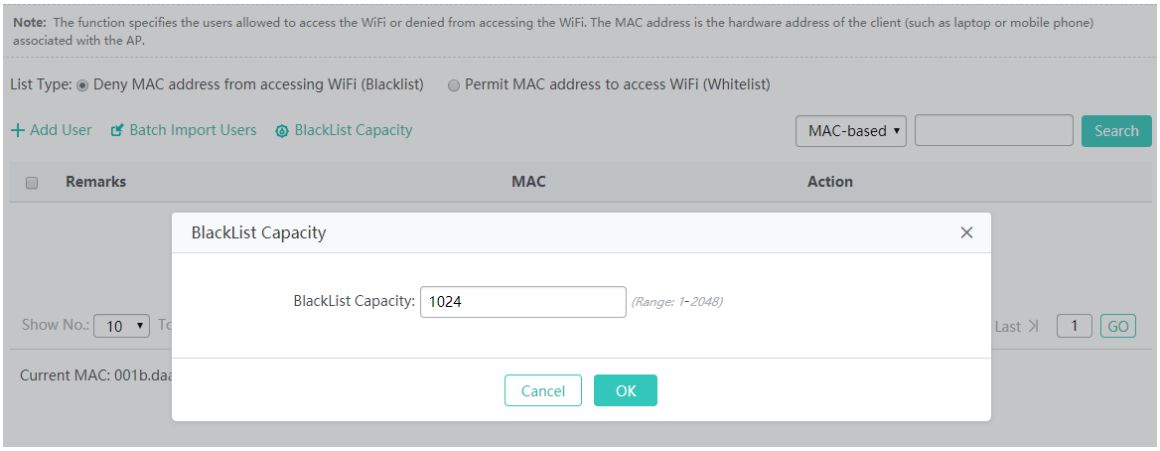
- Batch importing users

Click **Batch Import Users**. In the displayed window, click **Download Template** to download a template, enter data in the template, and click **Import** to import the template.



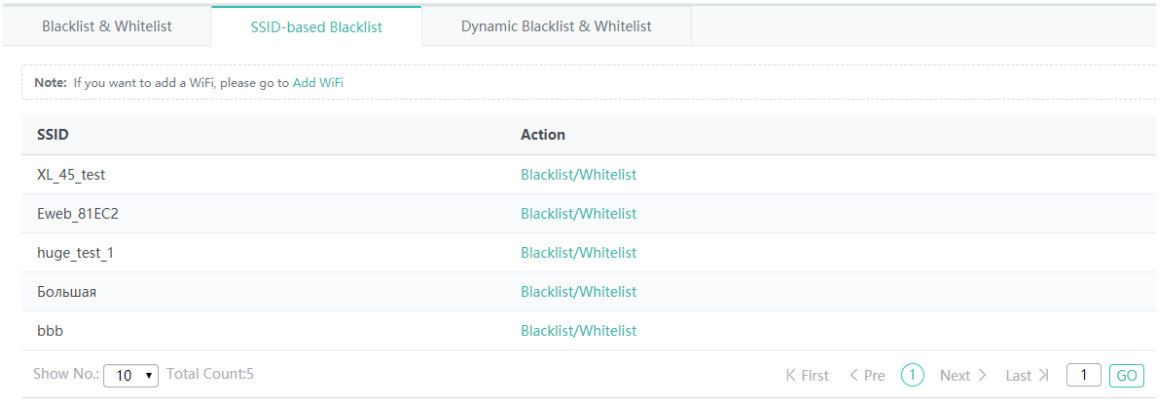
- Setting the blacklist capacity

Click **BlackList Capacity**. In the displayed window, enter the blacklist capacity and click **OK**. A setting success prompt is displayed, indicating that the operation is complete.



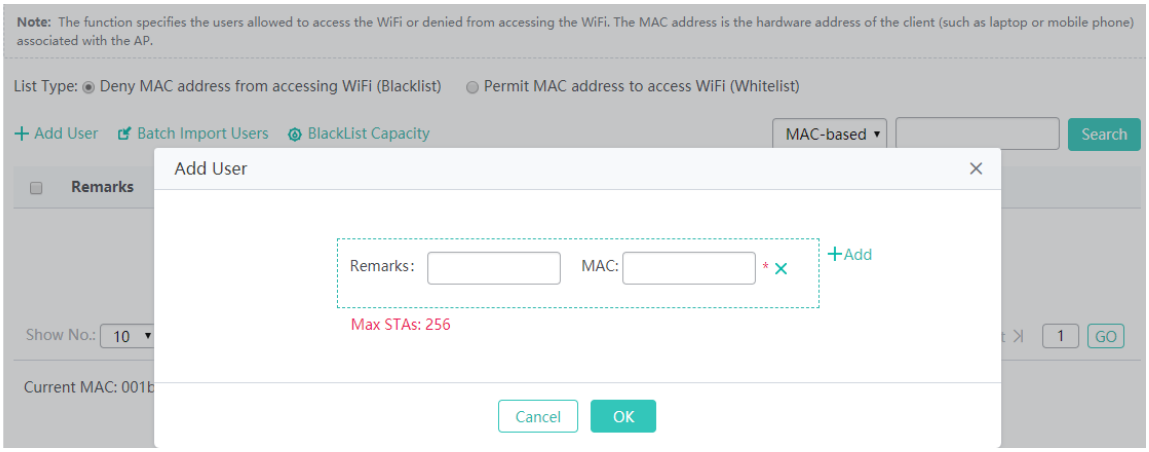
SSID-based Blacklist

Click **Blacklist/Whitelist** for an SSID to blacklist or whitelist the SSID.



- Adding a user

Click **Add User**. In the displayed **Add User** window, enter an MAC address and click **OK** to complete the operation. Multiple MAC addresses can be added.



- Deleting a user

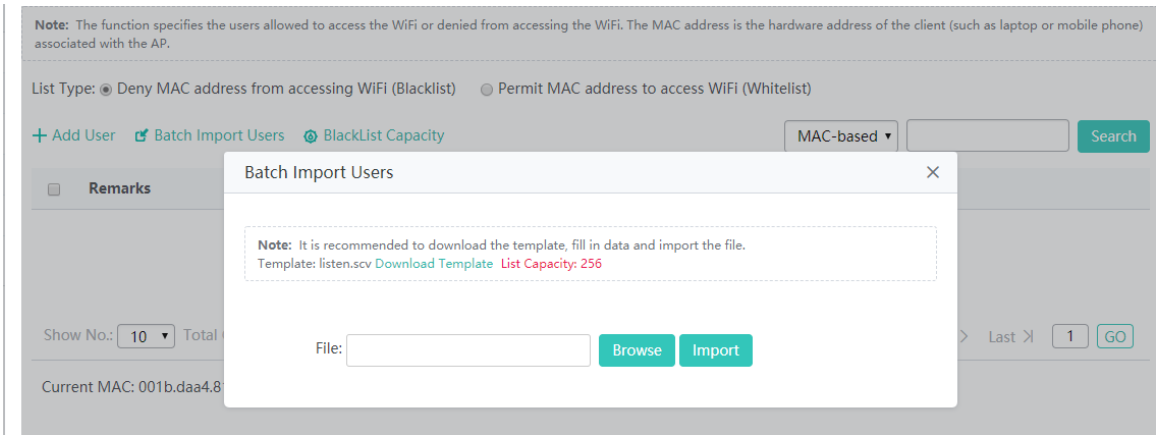
Click **Delete** for a user in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

- Batch deleting users

Select multiple records in the user list and click **Delete Selected** to batch delete users.

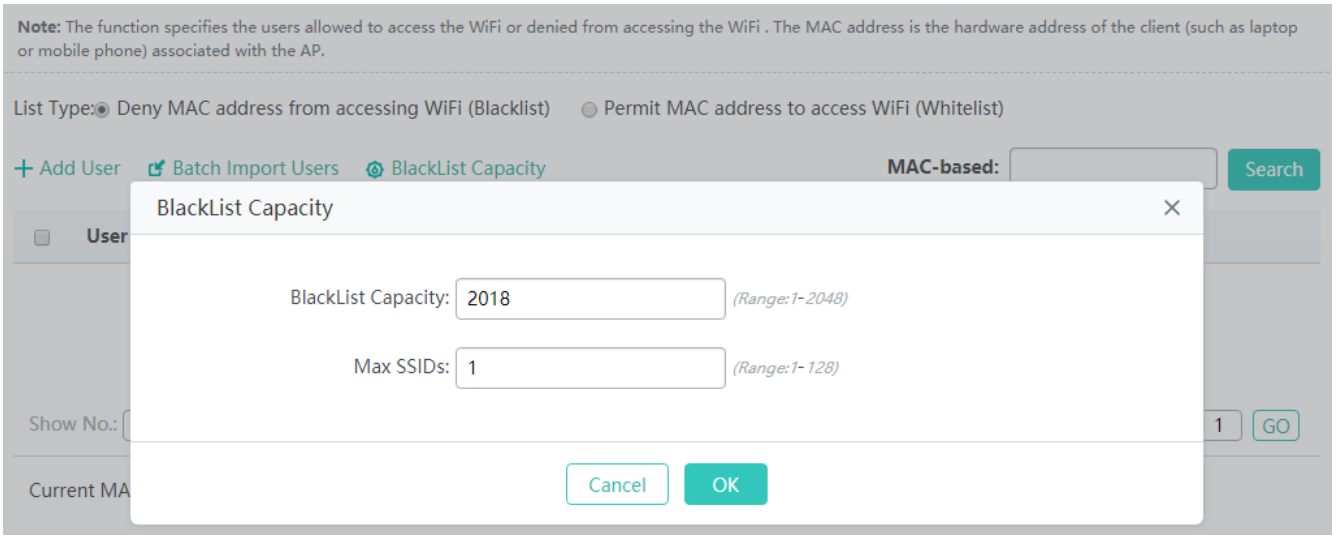
- Batch importing users

Click **Batch Import Users**. In the displayed window, click **Download Template** to download a template, enter data, and click **Import** to import the template.



- Setting the blacklist capacity

Click **BlackList Capacity**. In the displayed window, enter the blacklist capacity and click **OK**. A setting success prompt is displayed.

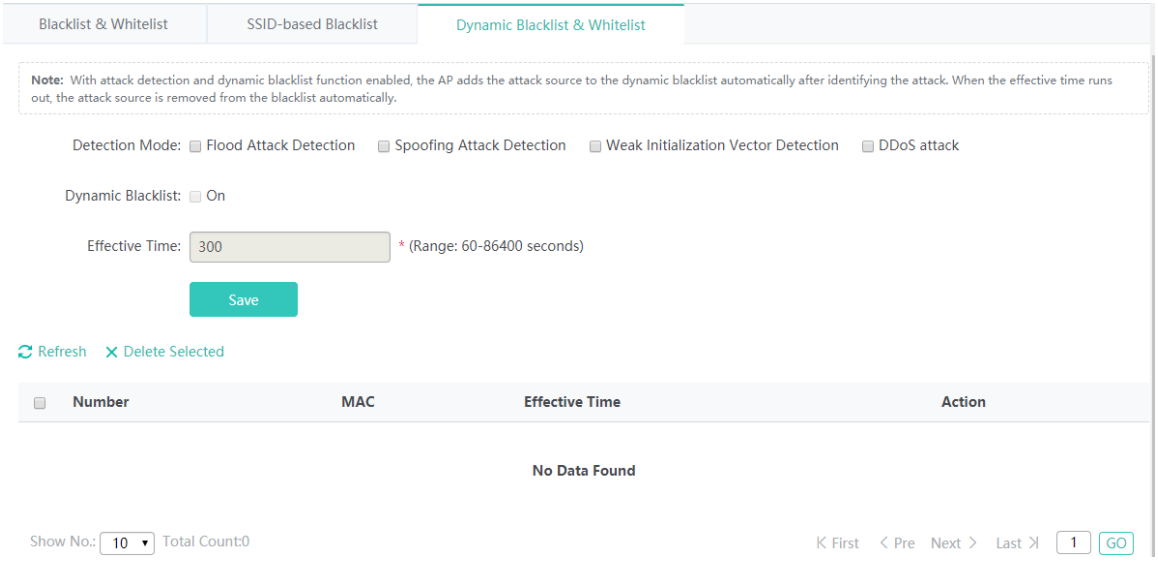


Dynamic Blacklist & Whitelist

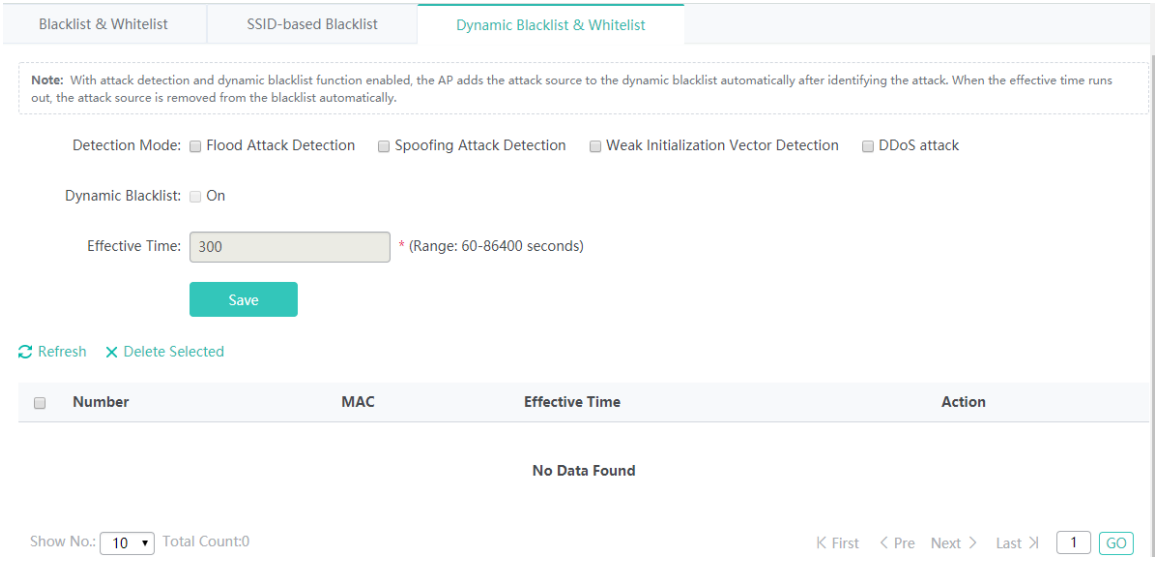
Add malicious attack sources to the dynamic blacklist to prevent their access.

Set **Detection Mode** to the required detection mode and enter the Time to Live (TTL) in **Effective Time**. A device is removed from the blacklist when the specified effective time expires. Click **Save** to complete the operation.

Click **Refresh** to refresh the list.



Select a blacklisted attack source from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

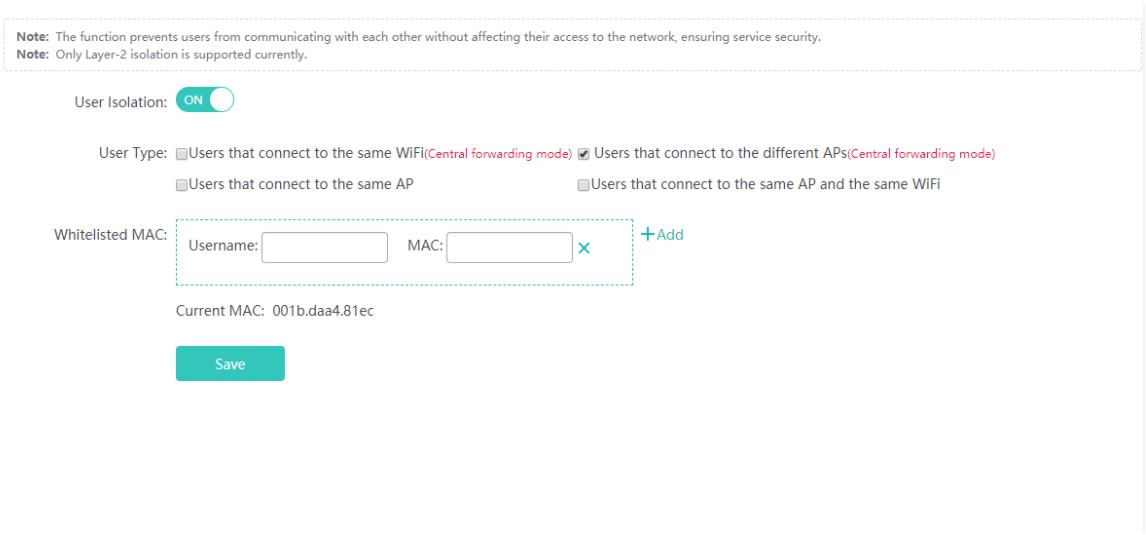


1.3.3.5.3 User Isolation

Communication between intranet users can be disabled to ensure network security and prevent unintended information transmission, and to identify special users (who can communicate with each other) by username or MAC address.

User Isolation can be set to **ON** or **OFF** to enable or disable the communication between intranet users.

In **Whitelisted MAC**, click ✕ to delete the MAC address of a user, and click **+Add** to add the MAC address of a user. Multiple MAC addresses can be added.



1.3.3.5.4 Attack Prevention

Some malicious attacks often occur in the network environment. These attacks overload the switch, resulting in high CPU usage and an operation failure of the switch.

Click **ARP-guard List** to display detected hosts encountering ARP attacks.

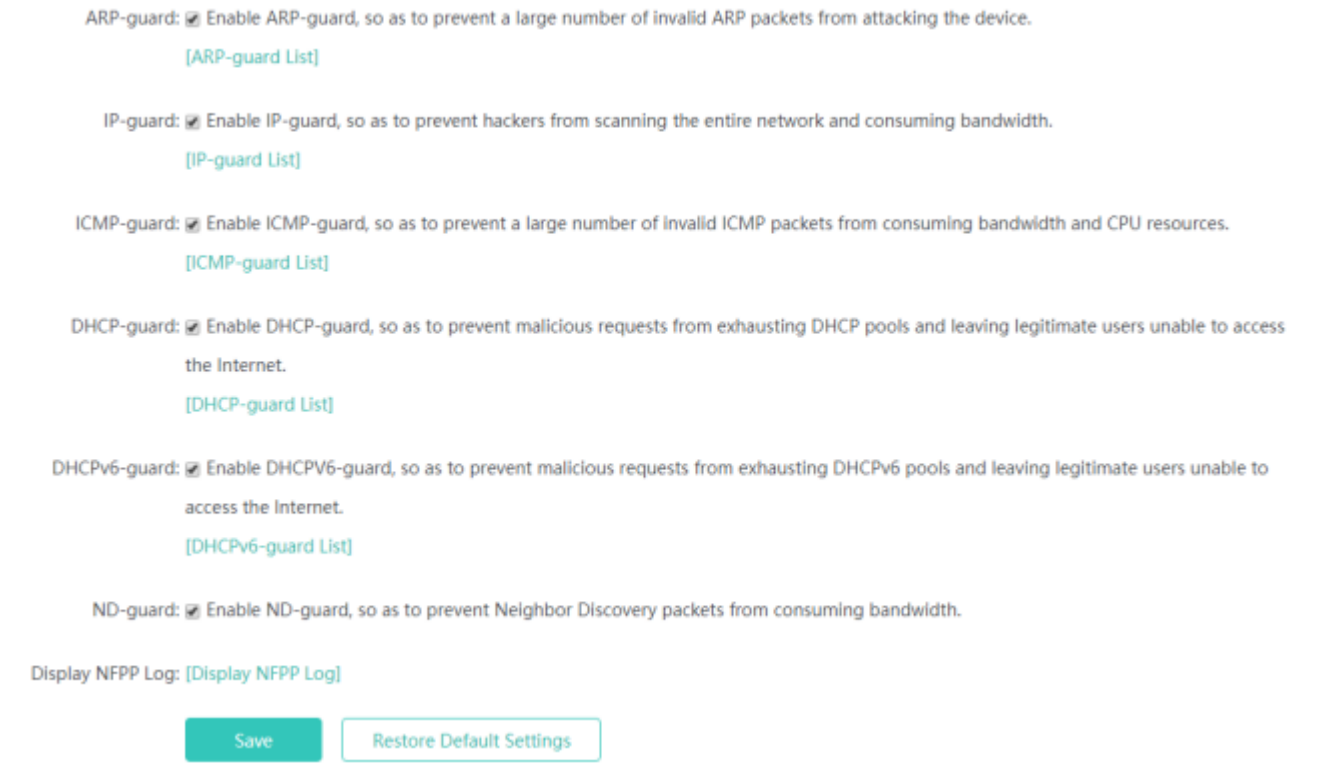
Click **IP-guard List** to display detected hosts encountering IP attacks.

Click **ICMP-guard List** to display detected hosts encountering ICMP attacks.

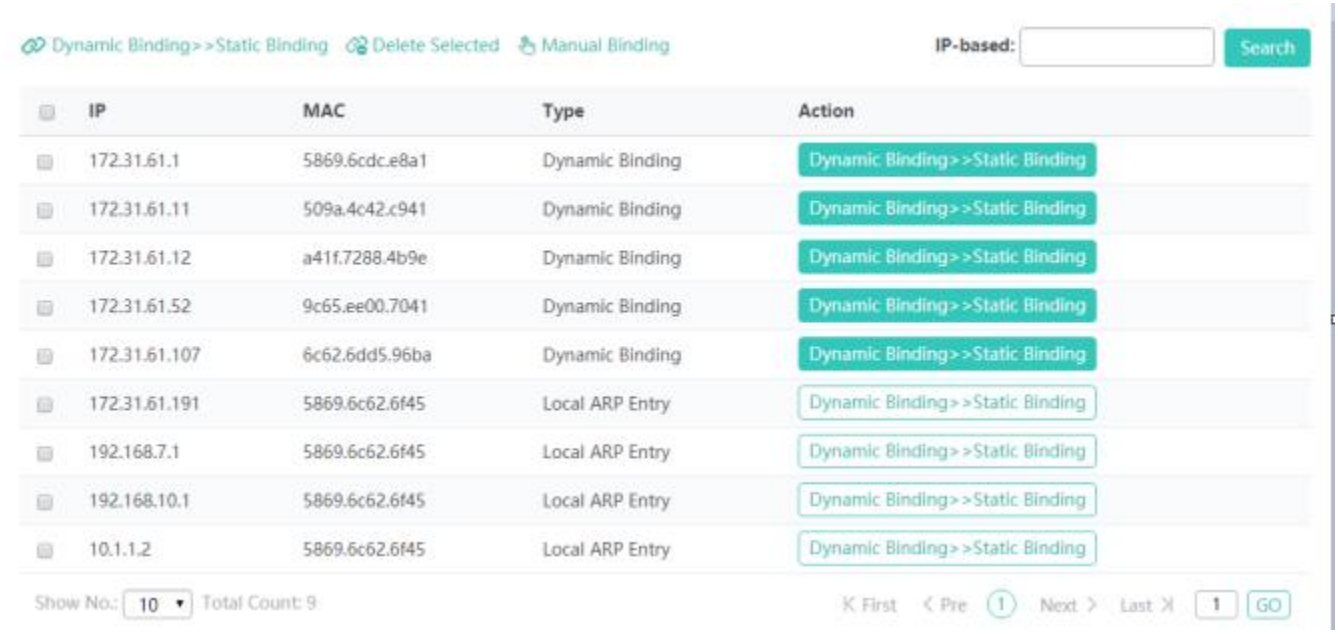
Click **DHCP-guard List** to display detected hosts encountering DHCPv4 attacks.

Click **DHCPv6-guard List** to display detected hosts encountering DHCPv6 attacks.

Click **Display NFPP Log** to display NFPP logs.



1.3.3.5.5 ARP Binding



- Converting dynamic bindings into static bindings

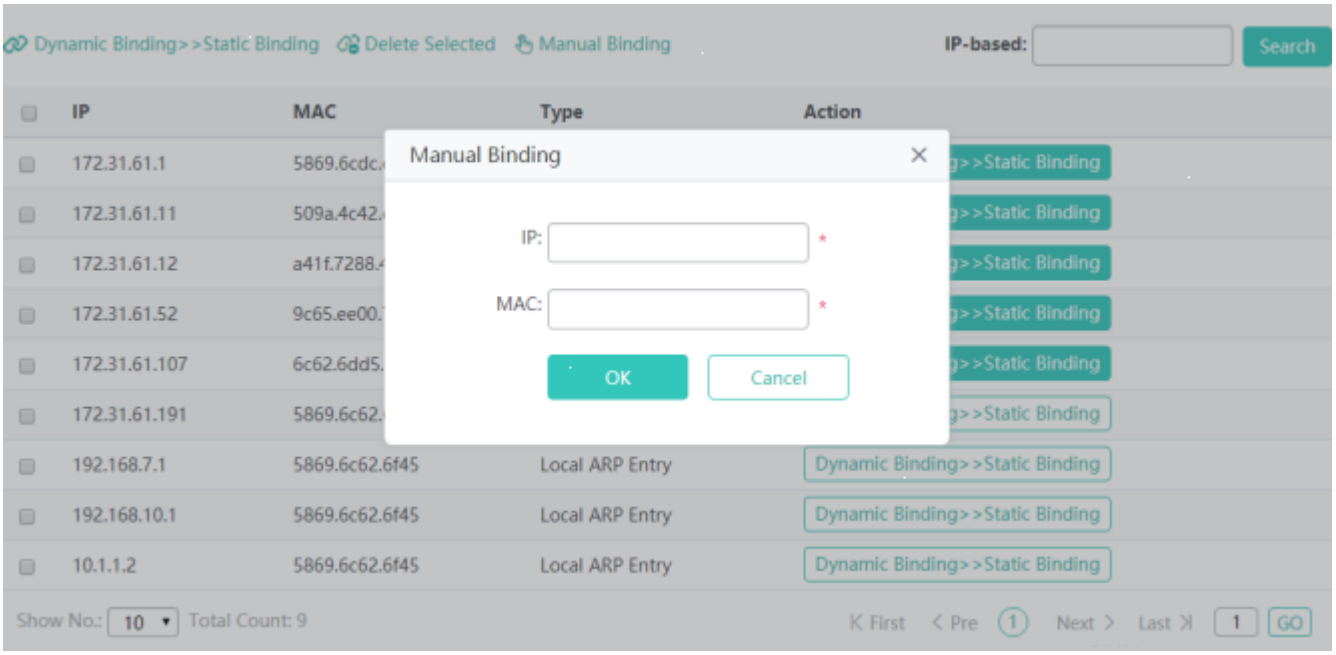
In the ARP list, select one or more records, and click **Dynamic Binding>>Static Binding** to convert dynamic bindings into static bindings.

- Deleting static bindings

In the ARP list, select one or more records, and click **Delete Selected** to delete static bindings.

- Performing manual binding

Click **Manual Binding**. In the displayed **Manual Binding** window, enter an IP address and a MAC address and click **OK**. A setting success prompt is displayed and the binding entry is displayed in the ARP
list.

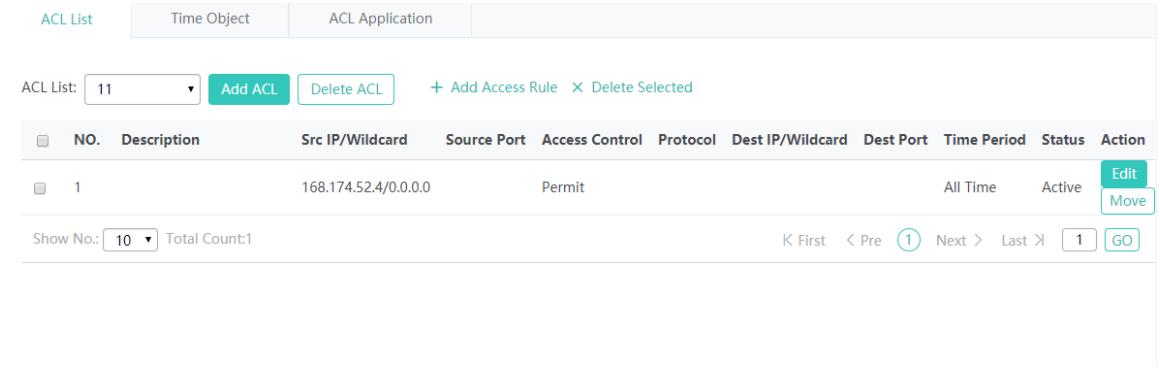


1.3.3.5.6 ACL

When receiving a packet, a device interface with an input ACL configured checks whether the packet matches an ACE in the input ACL. When sending out a packet, a device interface with an output ACL configured checks whether the packet matches an ACE in the output ACL.

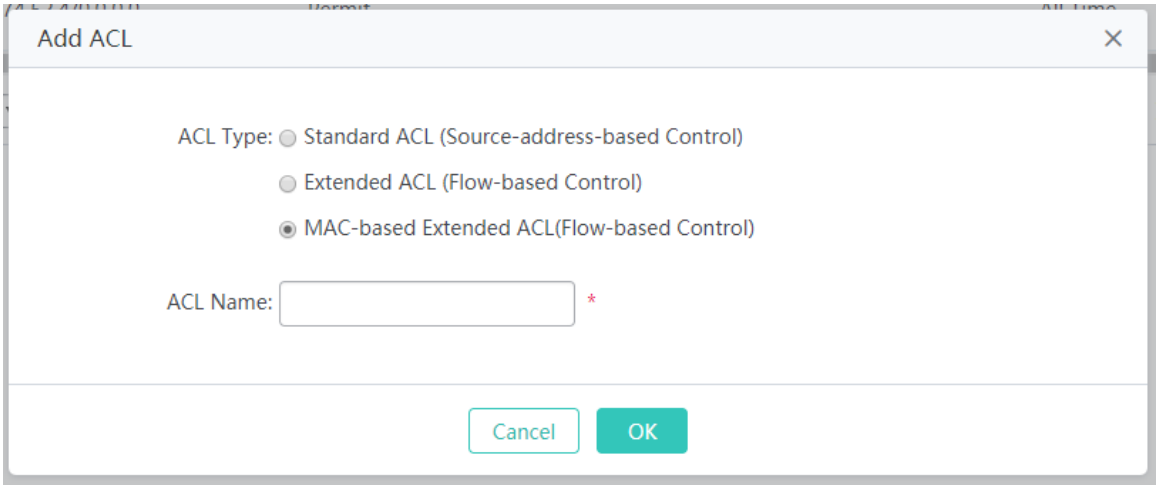
Packets matching an ACE are processed (permitted or denied) according to the ACE.

ACL List



- Adding an ACL

Click **Add ACL**. In the displayed **Add ACL** window, set parameters and click **OK**. A setting success prompt is displayed and the new ACL is displayed in the **ACL List** drop-down list on the left.



- Deleting an ACL

Select the ACL to be deleted from the **ACL List** drop-down list and click **Delete ACL**. In the displayed confirmation window, click **OK** to complete the delete operation.

- Adding an ACE

Select an ACL to which an ACE needs to be added from the **ACL List** drop-down list and click **+Add Access Rule**. In the displayed window, set parameters and click **OK**. A setting success prompt is displayed and the ACE is displayed in the ACE list.

- Editing an ACE

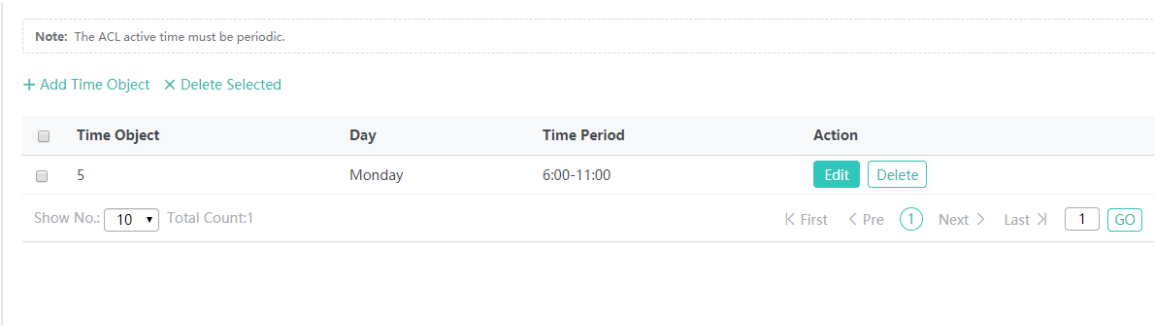
Click **Edit** for an ACE in the ACE list. The displayed window shows information about the ACE. Edit the information and click **OK**. A setting success prompt is displayed, indicating that the operation is complete.

- Deleting an ACE

Select one or more records from the ACE list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

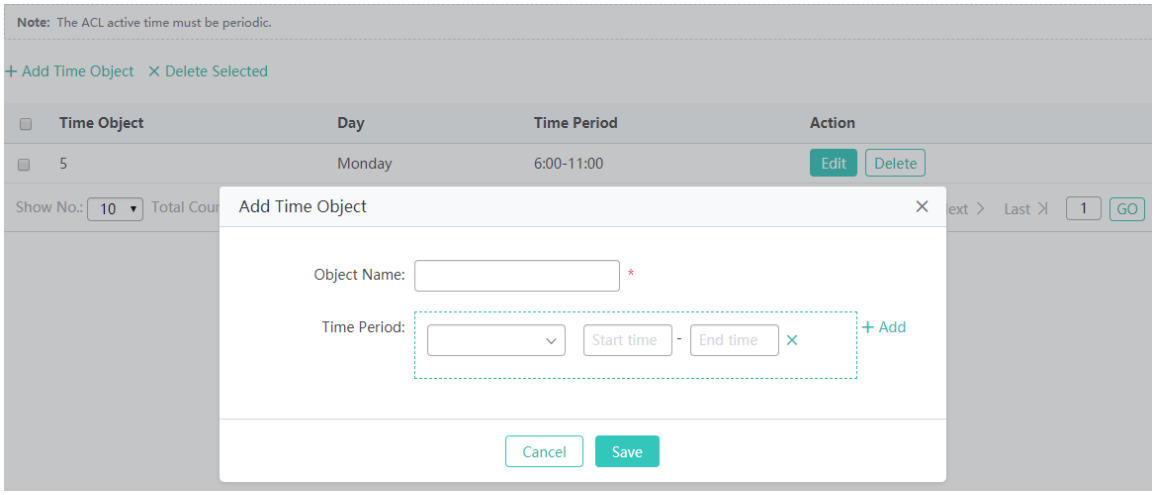
Time Object

You can make an ACL available based on time, for example, make an ACL take effect in some time ranges in a week. For this, you need to first configure a time object.



- Adding a time object

Click **Add Time Object**. In the displayed **Add Time Object** window, set parameters and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.



- Batch deleting time objects

Select time objects to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

- Editing a time object

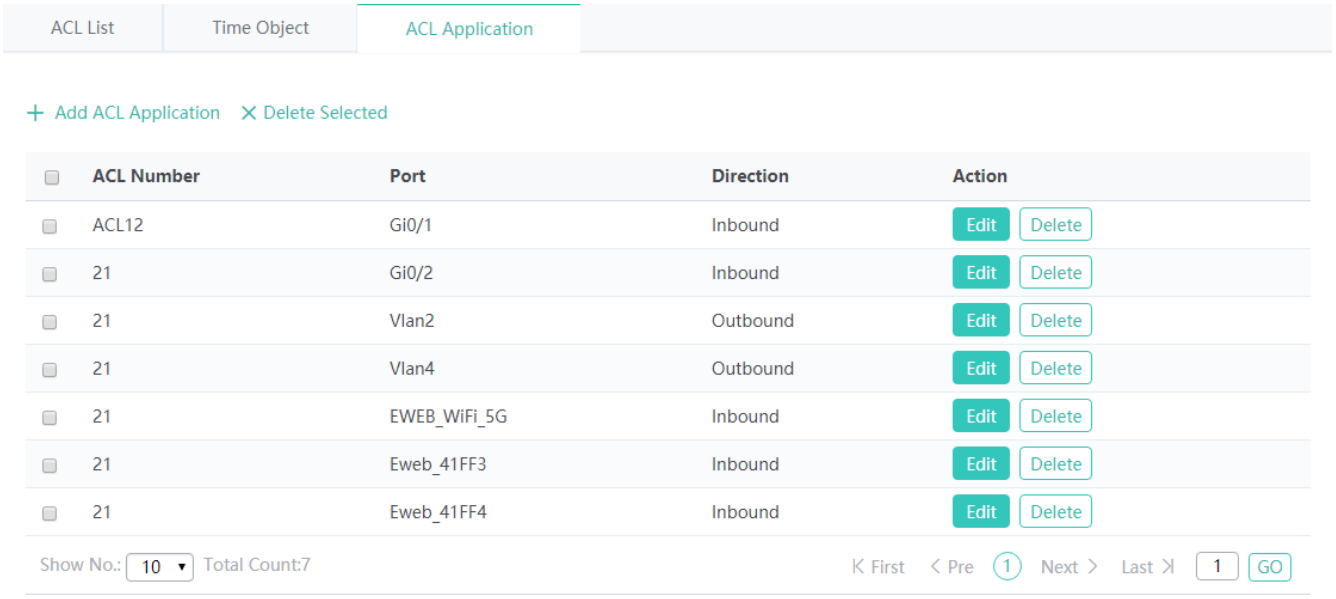
Click **Edit** for a time object in the list. The displayed window shows information about the time object. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

- Deleting a time object

Click **Delete** for a time object in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

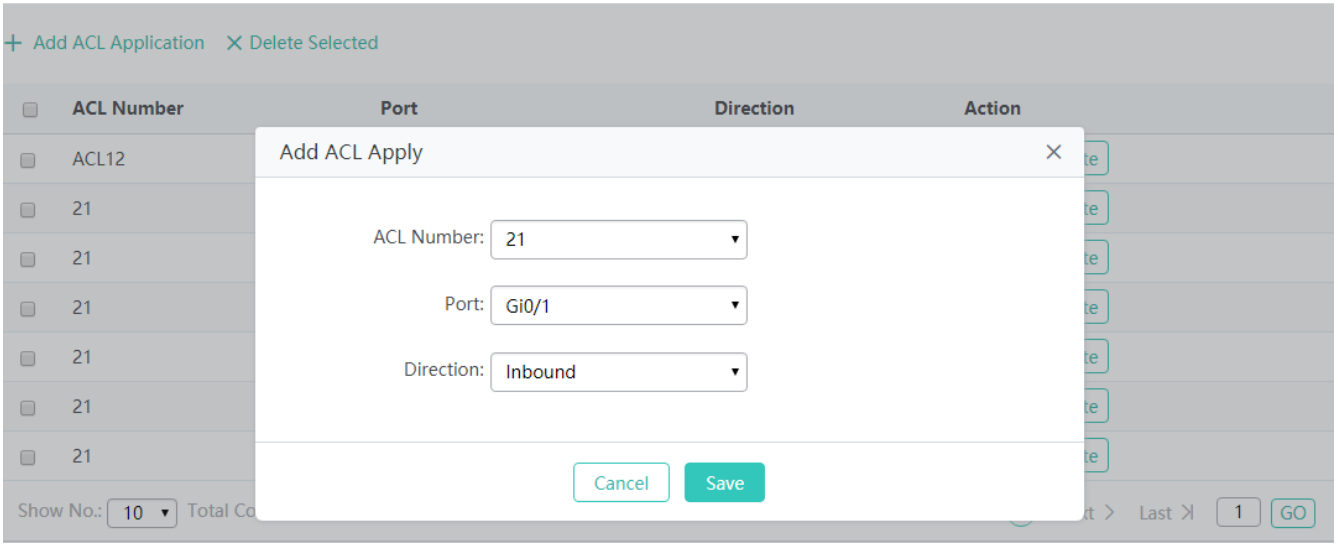
ACL Application

Configure ACEs and apply them to ports or WiFi networks, to restrict access of specific users or allow users to access specific networks.



- Adding an ACL application

Click **Add ACL Application**. In the displayed **Add ACL Apply** window, set parameters and click **Save**. A setting success prompt is displayed and the ACL is displayed in the ACL
list.



- Deleting ACLs

Select one or more records in the ACL application list, and click **Delete Selected** to delete data. In the displayed confirmation window, click **OK** to complete the delete operation.

- Editing an ACL application

Click **Edit** for an ACL application in the ACL application list. The displayed window shows information about the interface to which the ACL is applied. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

- Deleting an ACL application

Click **Delete** for an ACL application in the ACL application list. In the displayed confirmation window, click **OK** to complete the delete operation.

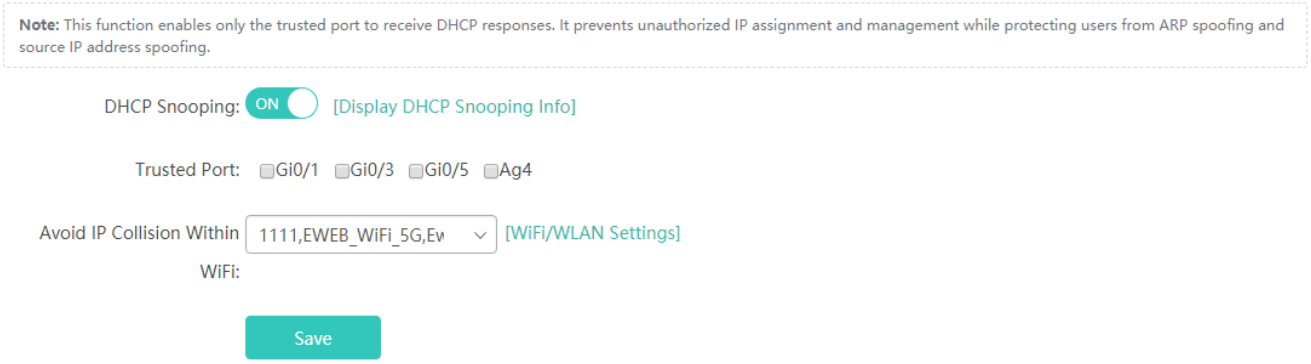
1.3.3.5.7 DHCP Security

DHCP Snooping can be set to **ON**/**OFF** to enable/disable the DHCP snooping function.

Click **Display DHCP Snooping Info** to display information about the bindings between users and IP addresses on the AC.

Set **Trusted Port**. The AC forwards only DHCP packets received by trusted ports.

Set **Avoid IP Collision Within WiFi** to specify the WiFi network on which IP collision prevention needs to be enabled. After IP collision prevention is enabled, the AC filters STAs that associate with the WiFi network based on information about the bindings between STAs and IP addresses.



1.3.3.6 Authentication

1.3.3.6.1 Web Authentication

Web authentication is an identity authentication method for controlling user permissions for network access. This authentication method does not need dedicated client authentication software and only a common browser can implement identity authentication. Real-name authentication for Internet access is more convenient for user management. Web authentication includes ePortal authentication and iPortal authentication based on the location of the authentication server.

↘ ePortal Authentication

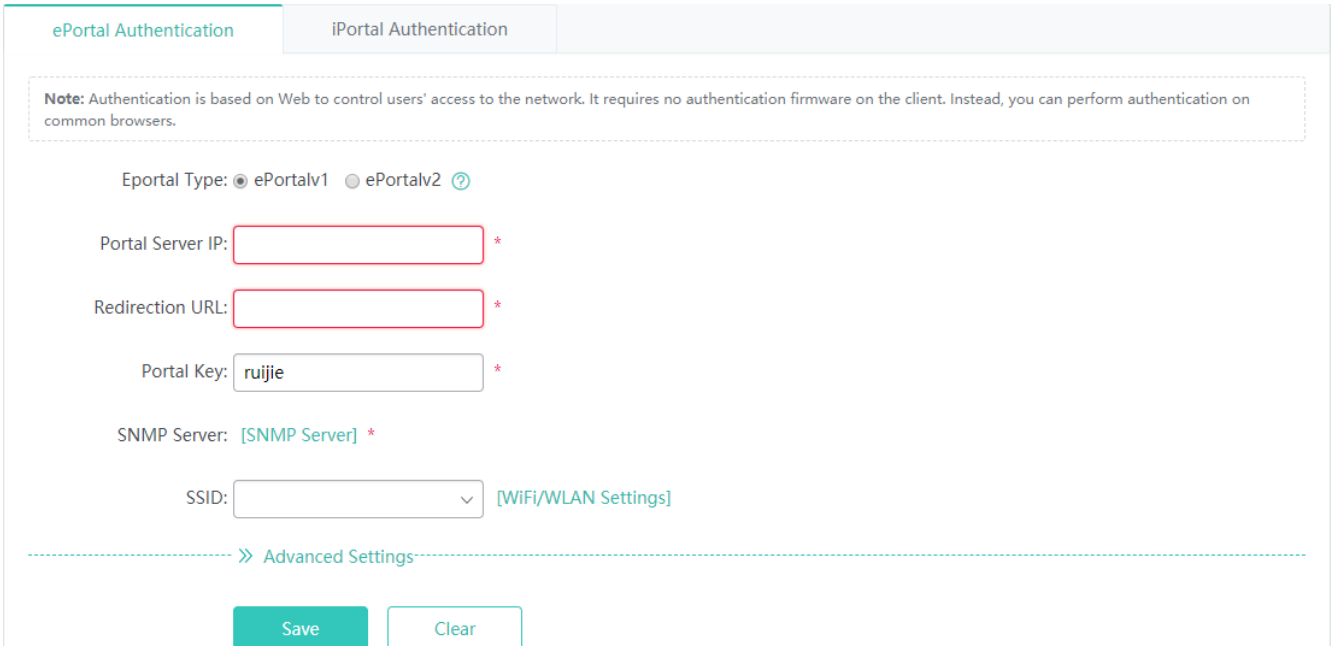
When unauthenticated users access the Internet by using browsers, the access device forcibly redirects the browsers to a specific website to perform authentication. When the portal (authentication pushing Web page) is configured on an independent device other than an AC, ePortal authentication is used.

- ePortalv1

Portal Server IP indicates the IP address of the authentication server.

Redirection URL indicates the redirection home page. To access the Internet, the browsers of unauthenticated users need to be redirected to this home page for authentication.

SNMP Server is used for information exchanging between the SNMP server and the authentication server.



Portal Server IP

Run the **ip** { *ip-address* } command to configure the server IP address in template configuration mode.

Server access requests are allowed by the device and rate limiting can be performed on requests transmitted to the server.

Redirection URL

Indicates the URL to which a browser is redirected. It is usually set to the address of the portal authentication page.

Portal Key

Indicates the key for the communication between the device and the authentication server.

SNMP Server

When identifying that a STA is offline, the device notifies the portal server that the STA is offline. The server instructs the device to delete user information via SNMP. The portal server displays the go-offline page to the STA.
Therefore, ePortal authentication needs the SNMP server.

SSID

Select a WiFi network to which ePortal authentication is to be applied.

⚠ Currently, authentication is configured globally and cannot be specific to WLANs.

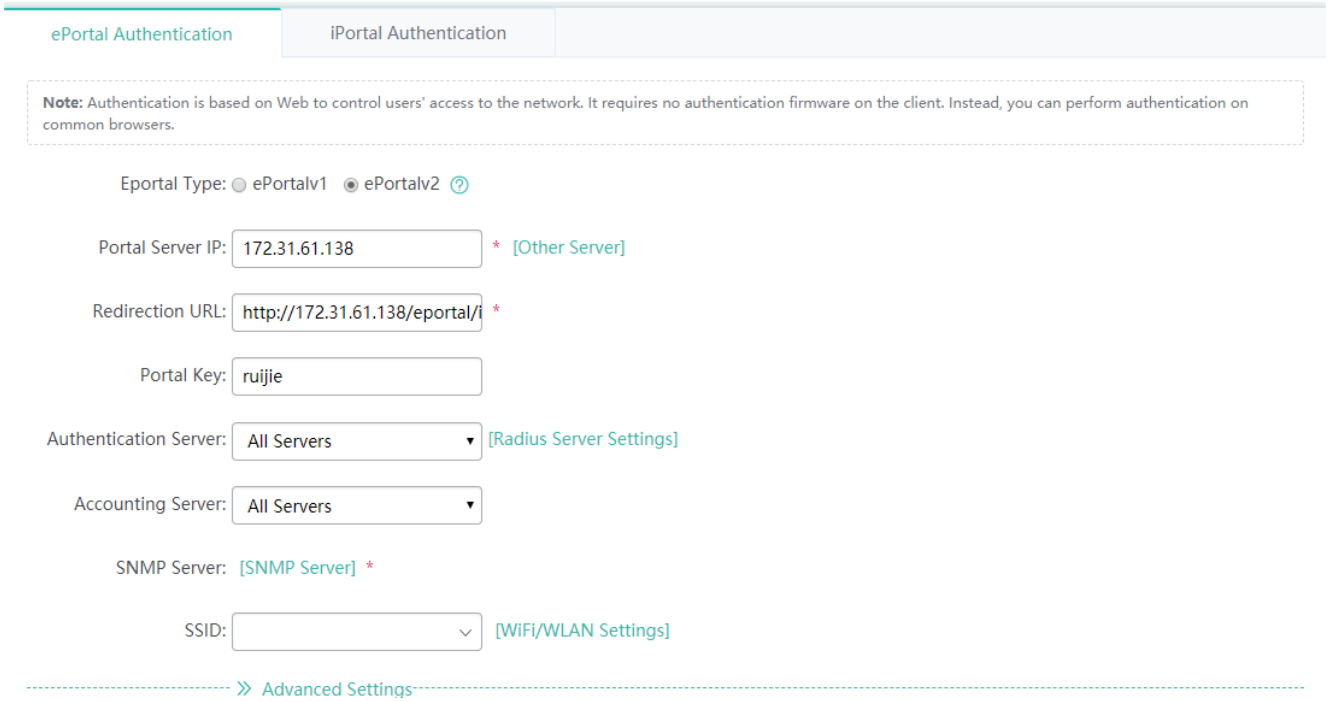
- ePortalv2

Portal Server IP indicates the IP address of the authentication server.

Redirection URL indicates the redirection home page. To access the Internet, the browsers of unauthenticated users need to be redirected to this home page for authentication.

SNMP Server is used for information exchanging between the SNMP server and the authentication server.

Click **WiFi/WLAN Settings** to add or modify WiFi networks.



Portal Server IP

Run the **ip** { *ip-address* } command to configure the server IP address in template configuration mode.

Server access requests are allowed by the device and rate limiting can be performed on requests transmitted to the server.

Redirection URL

Indicates the URL to which a browser is redirected. It is usually set to the address of the portal authentication page.

Portal Key

Indicates the key for the communication between the device and the authentication server.

Authentication Server

The AAA authentication method must be configured so that the ePortalv2 Web authentication function is applied successfully.

The authentication server list associates Web authentication requests with the RADIUS server. The device selects the authentication mode and server according to the authentication server list.

Accounting Server

Accounting Server is mandatory. The AAA network accounting method must be configured so that the ePortalv2 Web

authentication function is applied successfully.

The accounting server is used to associate the accounting mode with the server. The accounting function is required to record user information or fees in Web authentication.

SNMP Server

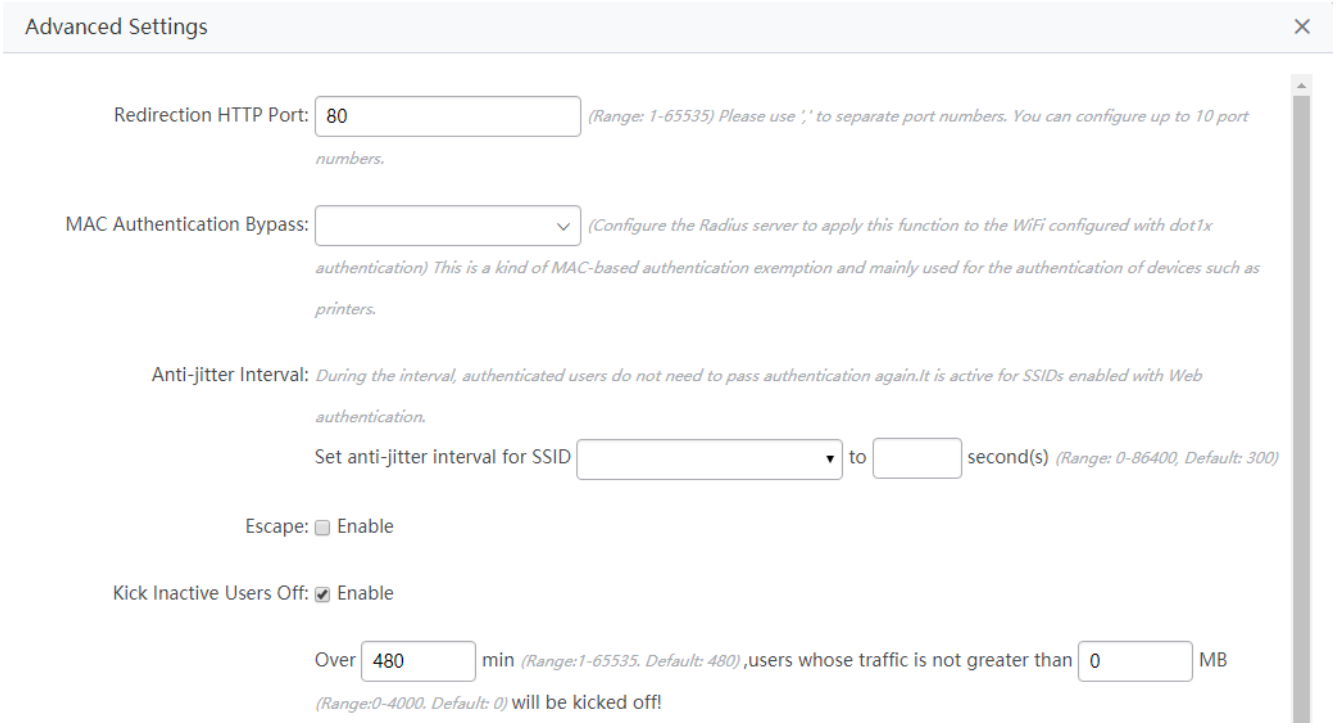
SNMP Server is used for information exchanging between the SNMP server and the authentication server.

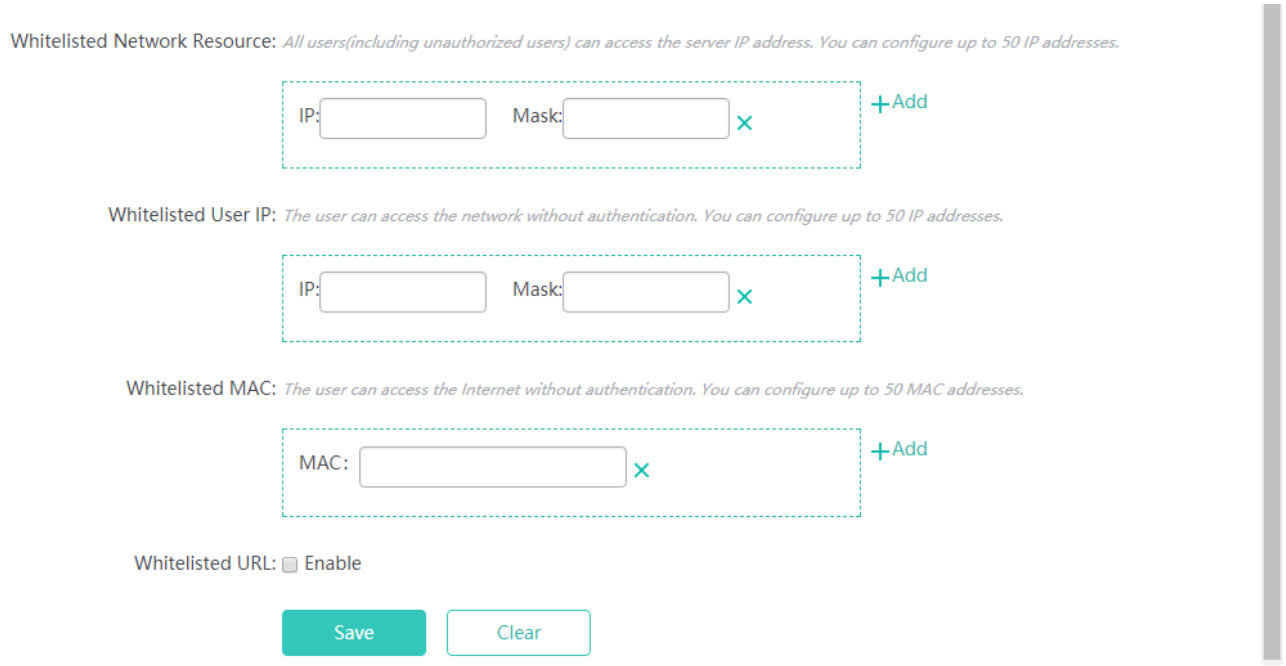
SSID

Select a WiFi network to which ePortalv2 authentication is to be applied.

- Advanced Settings

In **Advanced Settings**, set parameters and click **Save**. A configuration success prompt is displayed.





Redirection HTTP Port

When a STA accesses network resources (for example, the STA accesses the Internet by using a browser), the STA sends HTTP packets. The access/aggregation device intercepts the HTTP packets of the STA to determine whether the STA is accessing network resources. When detecting that an unauthenticated user is accessing network resources, the device prevents the user from accessing the network resources and displays the authentication page to the user. By default, the network device intercepts HTTP packets with the port ID being 80 from users, to detect whether the users are accessing network resources.

After the redirected HTTP port is set, the network device can redirect HTTP requests with a specific destination port ID from users.

MAC Authentication Bypass

MAC-based client authentication exemption is generally used for authentication of devices such as printers. Select the WiFi network to which the MAC Authentication Bypass (MAB) authentication is to be applied.

Anti-jitter Interval

Authenticated access users do not need to be verified within the anti-jitter interval, to enhance user experience. Specify the anti-jitter WiFi network and time.

Escape

New access users are exempted from authentication when the configured portal server becomes unavailable.

Kick Inactive Users Off

After the online detection function is configured, if the traffic of a user is lower than a threshold within a specified period, the device automatically kicks the user offline to prevent economic loss caused by continuous billing.

Whitelisted Network Resource

Enter the IP address of the network resource server. All users including unauthenticated users can access this IP address. A maximum of 50 entries can be configured.

Whitelisted User IP

Users with whitelisted IP addresses can access the Internet without authentication. A maximum of 50 entries can be configured.

Whitelisted MAC

Users with whitelisted MAC addresses can access the Internet without authentication. A maximum of 50 entries can be configured.

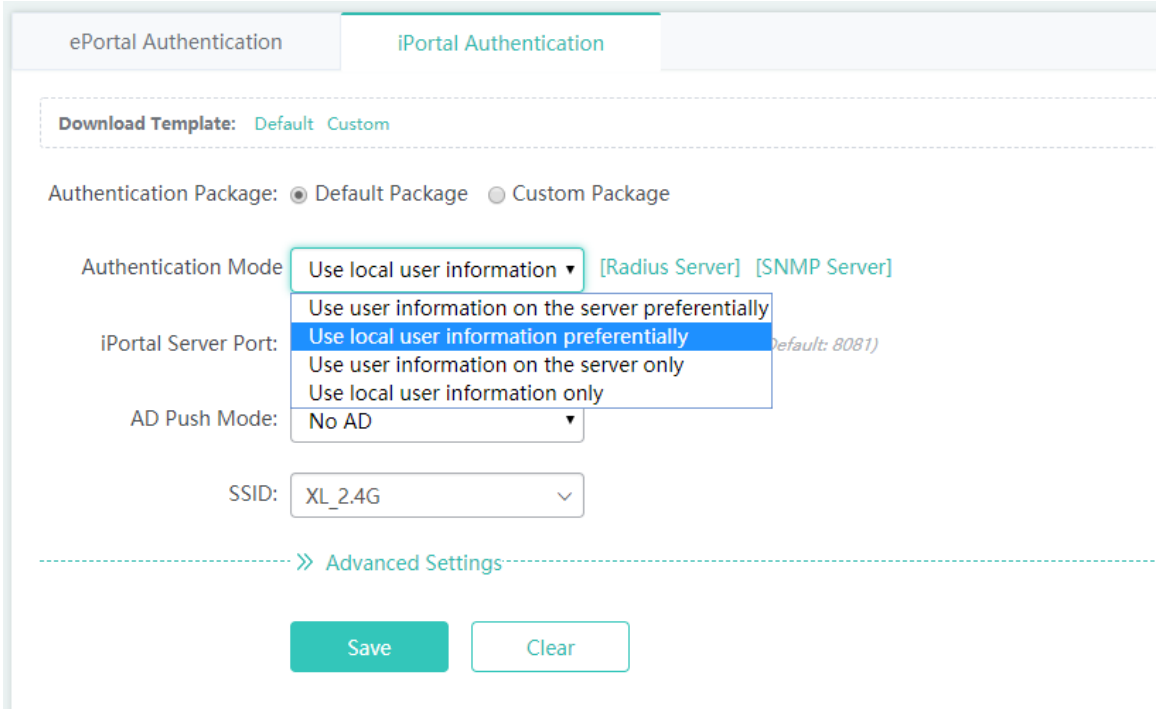
Whitelisted URL

Users can access these URLs without authentication. A maximum of 50 entries can be configured.

iPortal Authentication

When unauthenticated users access the Internet by using browsers, the access device forcibly redirects the browsers to a specific website to perform authentication.. When the portal (authentication pushing Web page) is embedded into an AC, iPortal authentication is used.

Set parameters and click **Save**. A configuration success prompt is displayed.



Authentication Package

You can use the default authentication page or customize an authentication page. The authentication page provided by the device is used by default.

Authentication Mode

The following authentication modes are available:

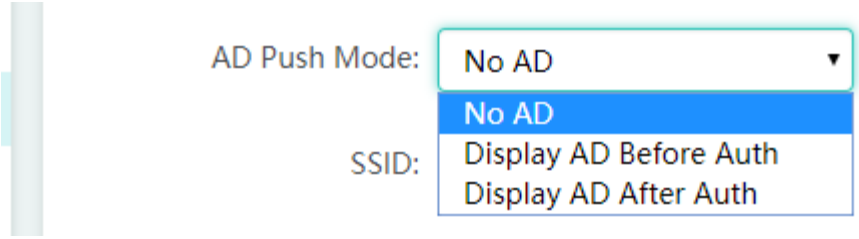
- Use user information on the server preferentially
- Use local user information preferentially
- Use user information on the server only
- Use local user information only

iPortal Server Port

Indicates the authentication page port of iPortal authentication. The default port ID is 8081.

AD Push Mode

AD Push Mode can be set to **No AD**, **Display AD Before Auth**, and **Display AD After Auth**. The default value is **No AD**.



SSID

Select the WiFi network to which iPortal authentication is to be applied.

1.3.3.6.2 WiFi Access Authentication via WeChat

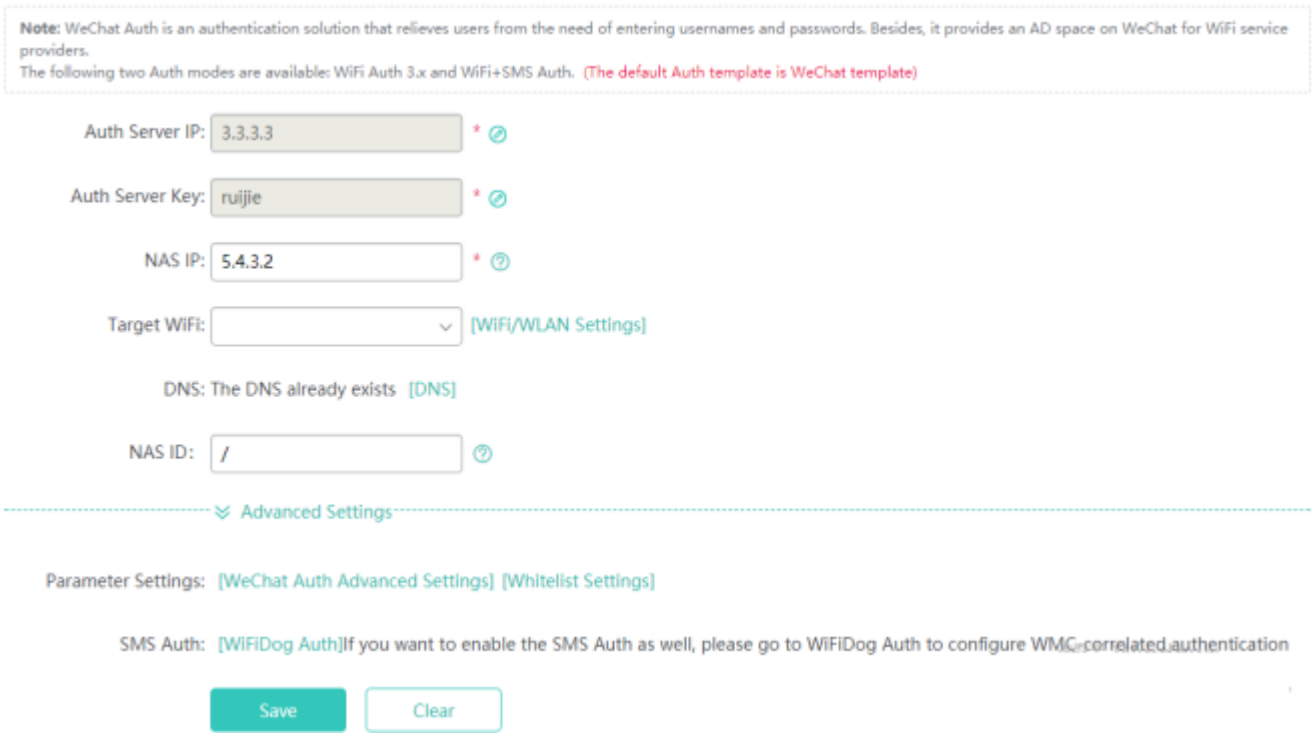
WiFi access authentication via WeChat is a solution to WiFi access authorization and authentication for conventional businesses. It replaces conventional Web authentication that requires a username and password, and provides an entry to an information display and AD position on the WeChat page for WiFi service providers that succeed in security authentication, to increase their commercial values.

Currently, authentication types supported by the device include WiFi access authentication via WeChat 3.X, and WiFi access authentication via WeChat + SMS-based authentication.

WiFi access authentication via WeChat is configured based on scenarios. WiFi access authentication via WeChat and CWMP protocol can be configured in one-click mode. It is not recommended to configure WiFi access authentication via WeChat in combination with the CLI (this function depends on the actual support status of the device).

Set parameters and click **Save.** Users can use WiFi access authentication via WeChat.

Click **Clear** to clear settings (configured through Web pages) for WiFi access authentication via WeChat.



Auth Server IP

Indicates the IP address of the WeChat authentication server. The IP address 112.124.31.88 is provided by default and you can modify this address.

Auth Server Key

Indicates the key for the communication between the device and the authentication server.

NAS IP

Indicates an IP address of the device for communicating with the WMC server.

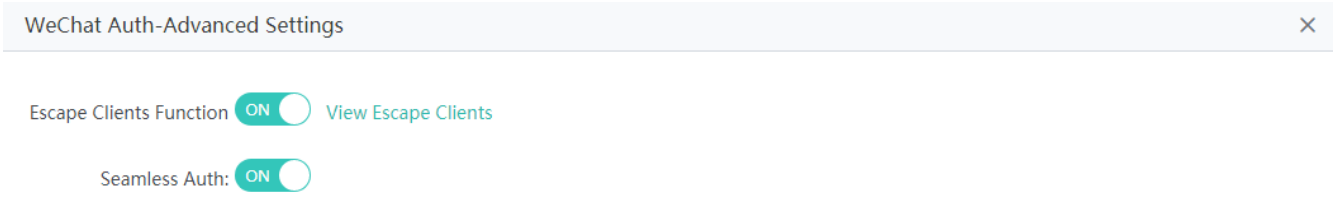
Target WiFi

Indicates the WiFi network to which authentication via WeChat is applied.

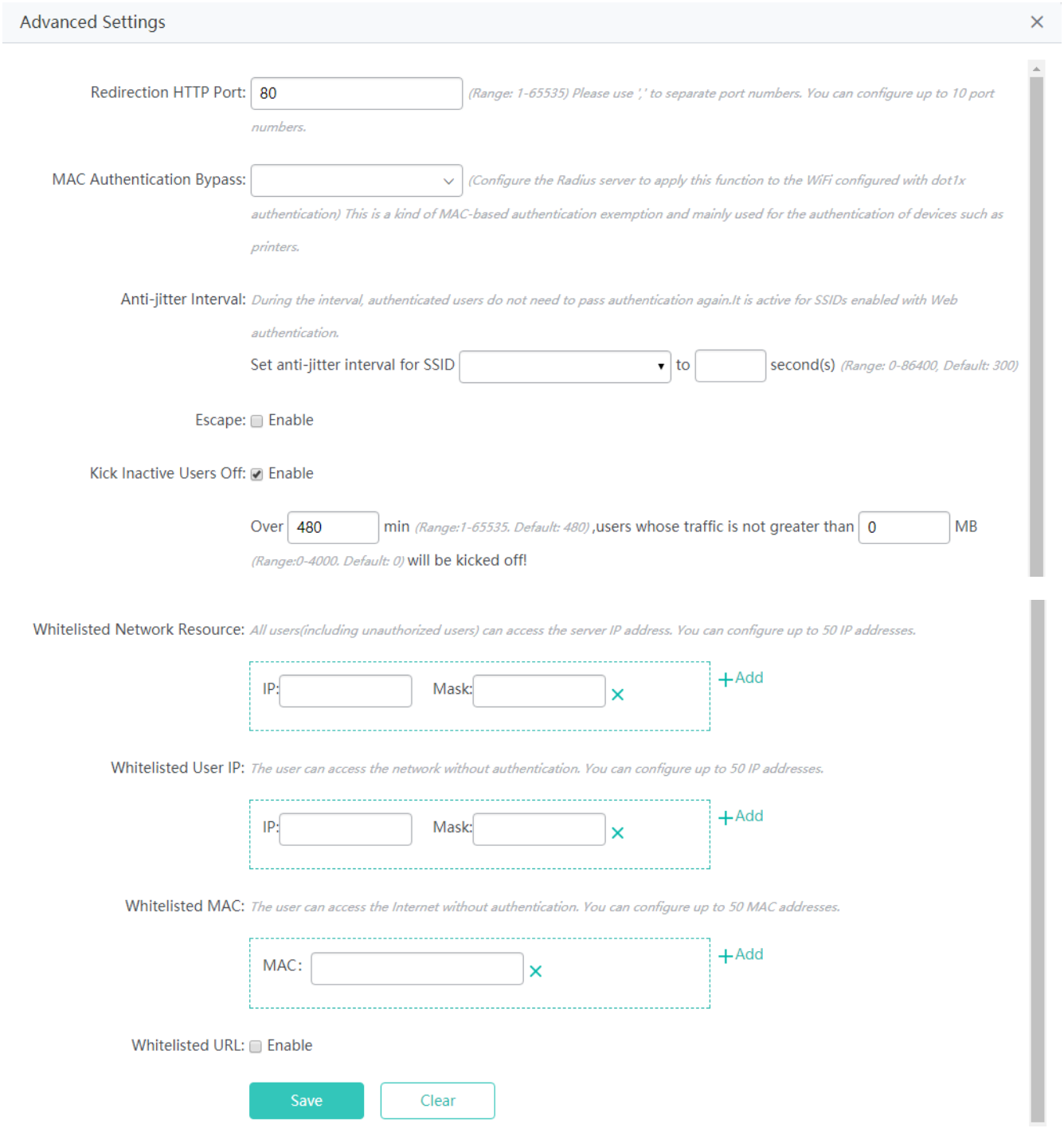
DNS

Indicates the DNS for communicating with an external network.

- WeChat Auth Advanced Settings



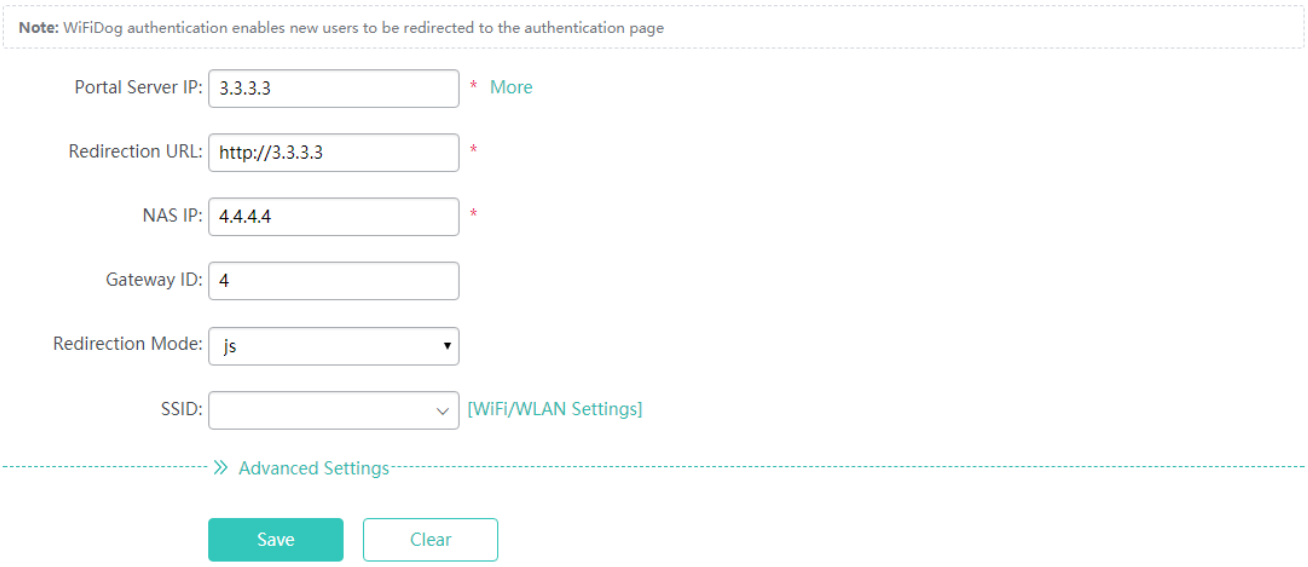
- Advanced Settings



The parameters above are the same as those for **Advanced Settings** of Web authentication and are not described again.

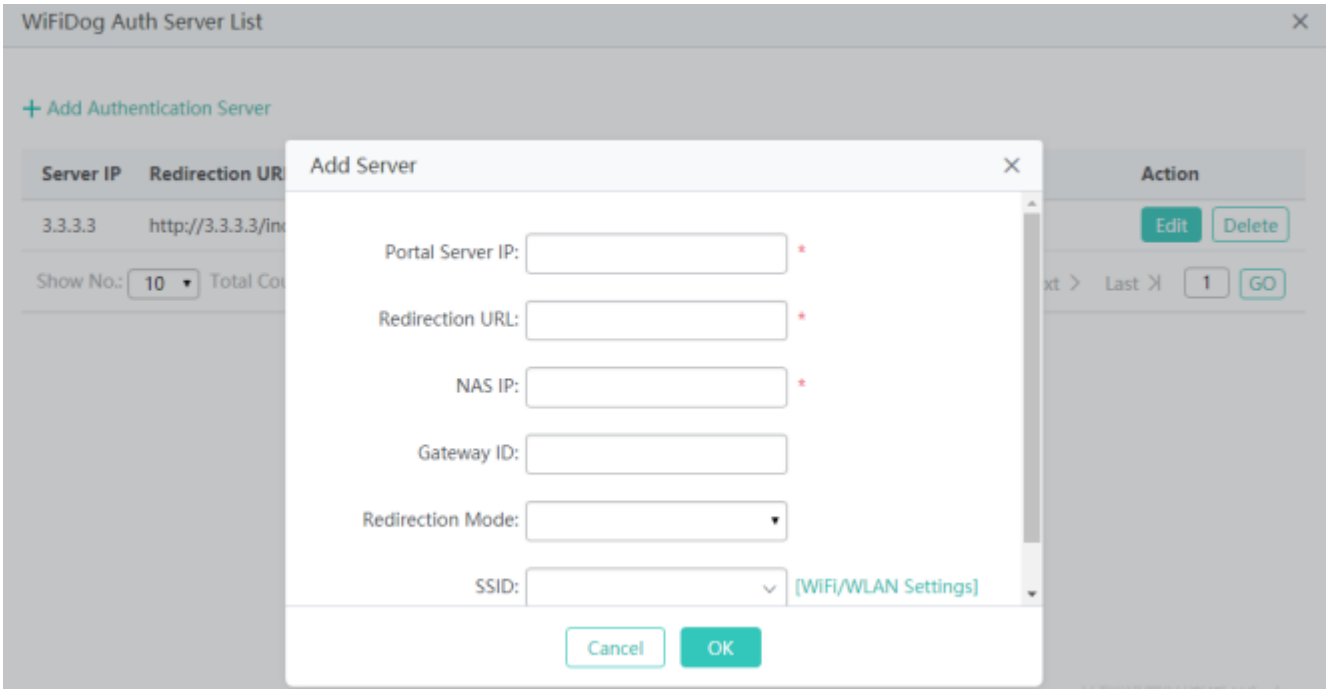
1.3.3.6.3 WiFiDog Authentication

Unauthenticated users can be redirected to the authentication page for authentication.



- Adding a WiFiDog authentication server

Click **Add Authentication Server**. In the displayed **Add Server** window, set parameters and click **OK**. A setting success prompt is displayed and the new authentication server is displayed in the server list.



Portal Server IP

Indicates the IP address of the portal server.

Redirection URL

Indicates the authentication page URL of the portal server.

NAS IP

Set the access service IP address of the WiFiDog-supported device so that the server communicates with the device through this IP address.

Redirection Mode

It can be set to HTTP protocol redirection or JavaScript redirection. JavaScript redirection is used by default.

Gateway ID

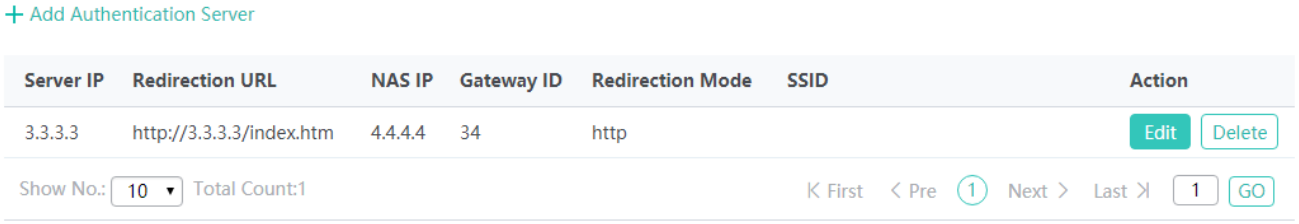
Indicates the gateway ID used by the WiFiDog protocol. It is the serial number of the device by default.

SSID

Select the WiFi networks to which WiFiDog authentication is to be applied.

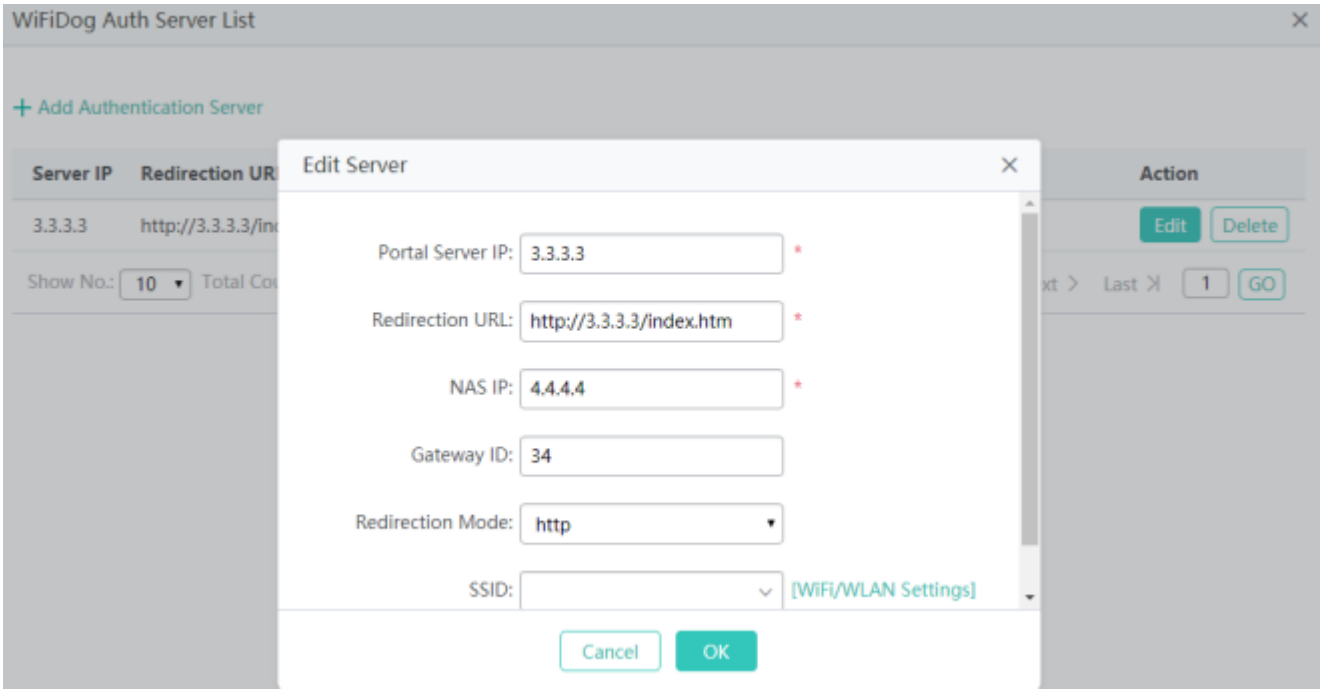
- Deleting a WiFiDog authentication server

Click **Delete** for a WiFiDog authentication server in the list. In the displayed confirmation window, click **OK** to complete the delete operation.



- Editing a WiFiDog authentication server

Click **Edit** for an authentication server in the server list. In the displayed **Edit Server** window, set parameters and click **OK**. A setting success prompt is displayed and the server is displayed in the server list.



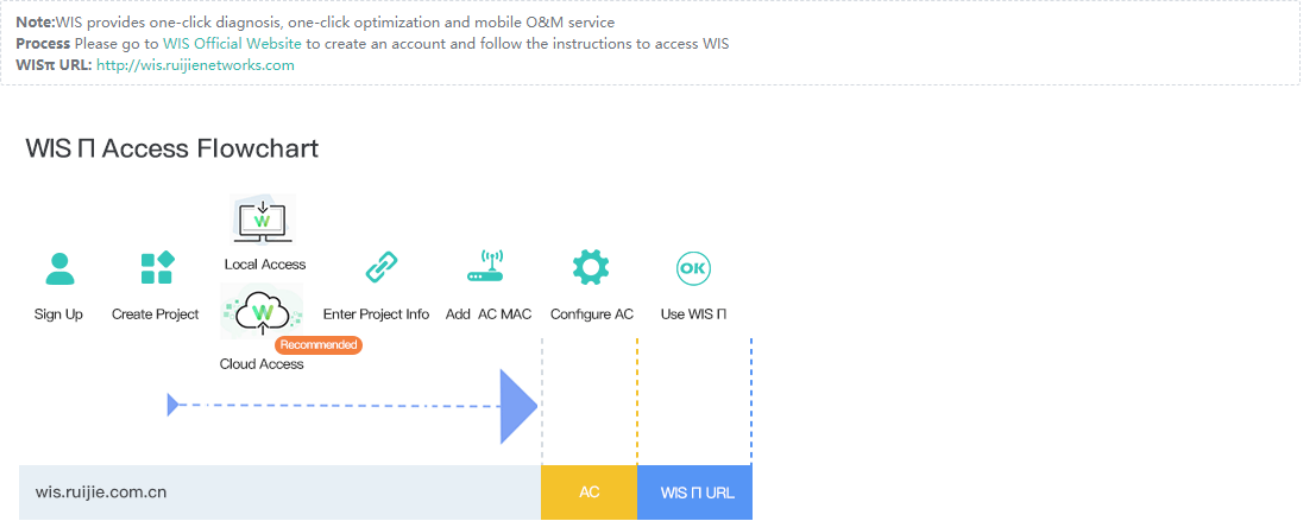
1.3.3.7 Optimization

1.3.3.7.1 WIS

After the WIS function is enabled, the device can detect the network operation status, identify possible problems on the network, provide warnings, and send them to a specified server. Then, users can view the status of the device, network condition, user experience, and other information in the WIS system.

Your AC may not support this function and the actual menu items shall prevail.

The WIS page provides guidance on how to interconnect an AC to the WIS system.

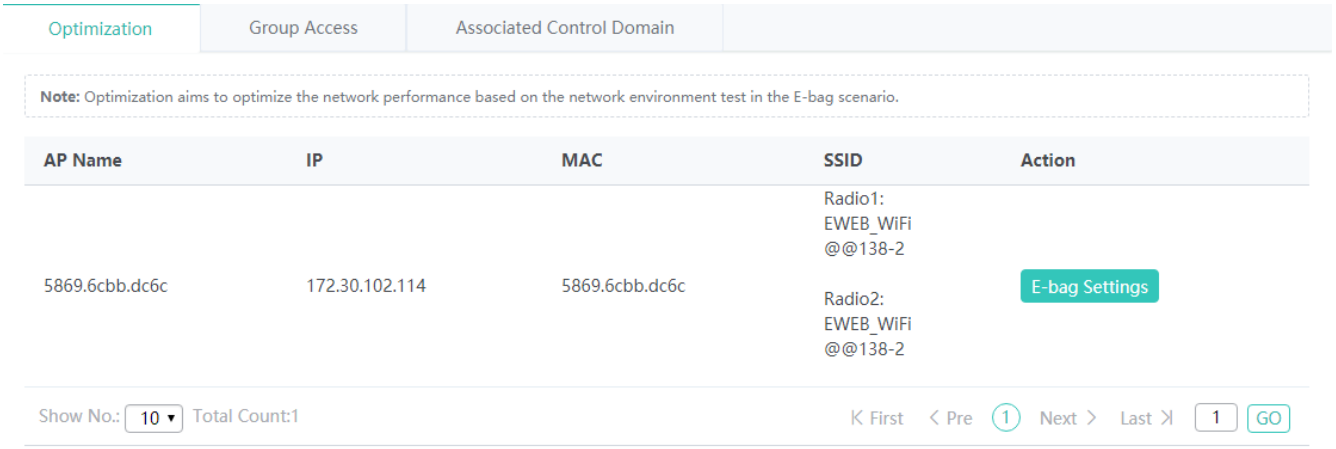


1.3.3.8 Solution

1.3.3.8.1 E-bag Configuration

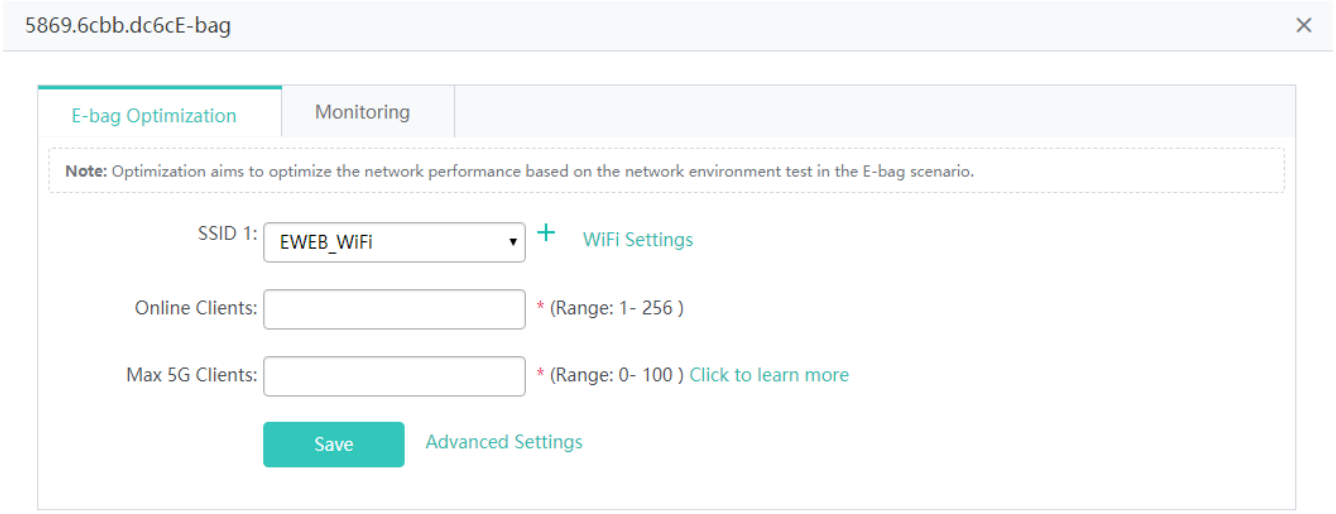
The E-bag function is mainly applicable to E-bag solutions in schools. With the balancing function enabled, users can access the network smoothly and are not kicked offline when using the E-bag.

Optimization



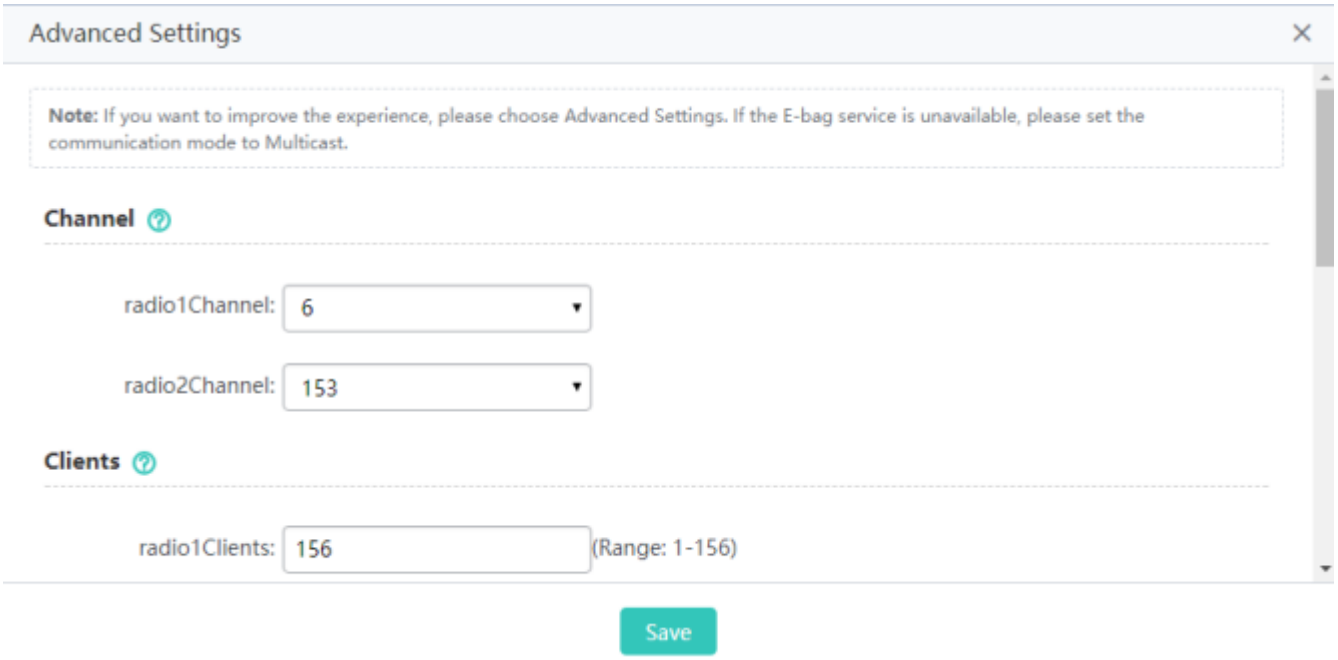
- E-bag Optimization

On the **E-bag Optimization** tab page, set parameters and click **Save**.

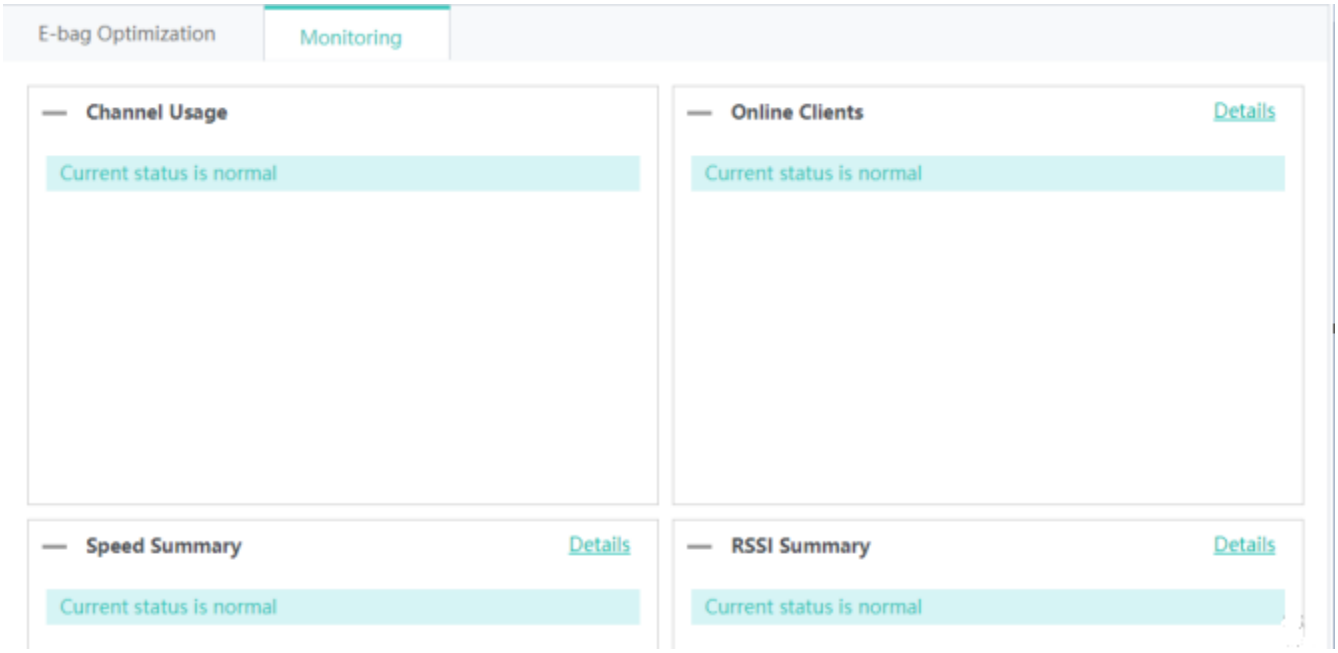


Advanced Settings

On the **Advanced Settings** page, set parameters and click **Save**.

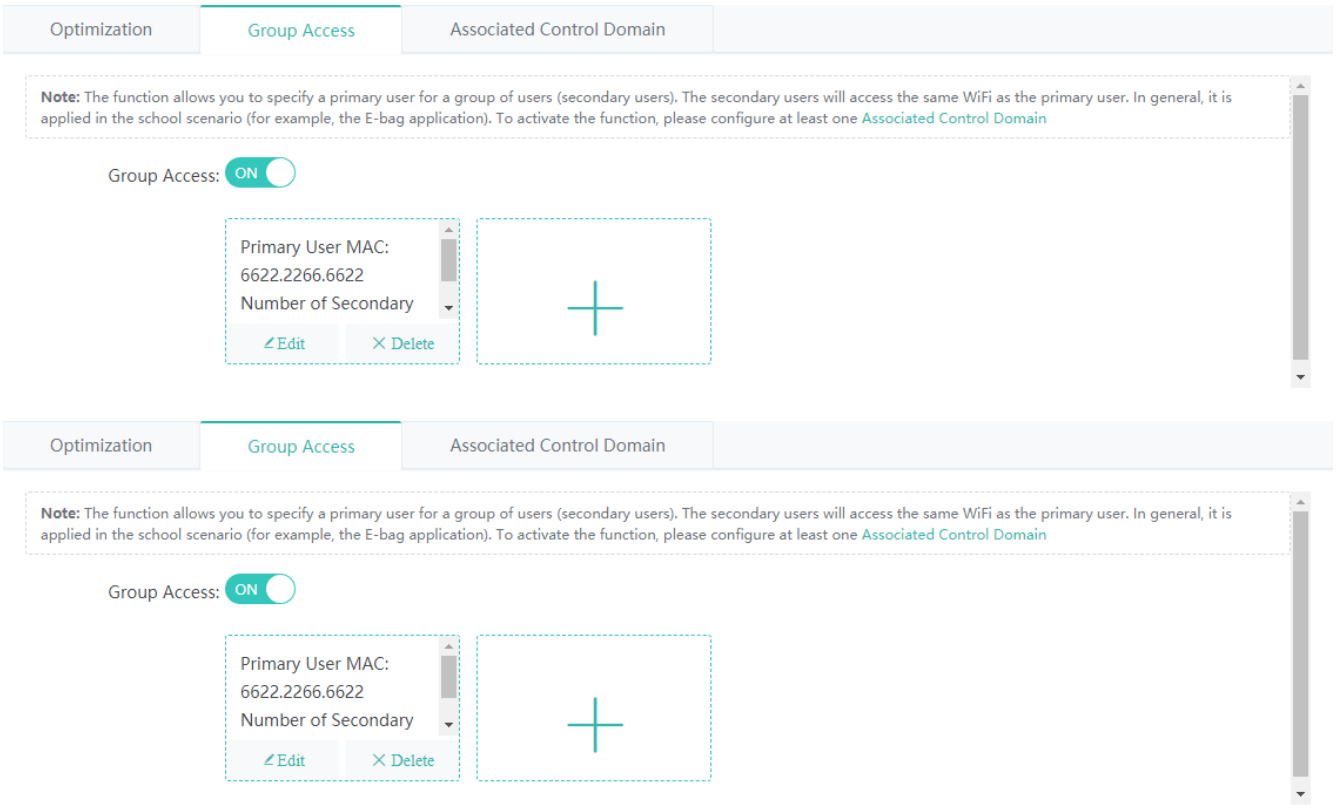


- Monitoring



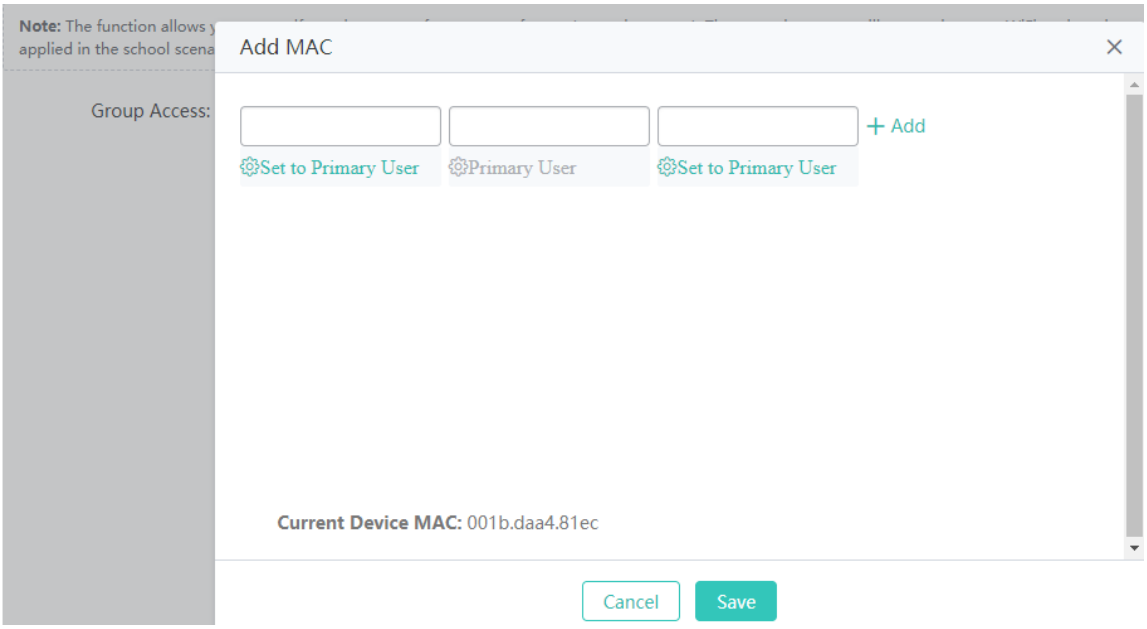
Group Access

Group Access can be set to **ON**/**OFF** to enable/disable the function of controlling a STA to access a specific WiFi network. Configure user bindings as well as the data of the primary user and secondary users.



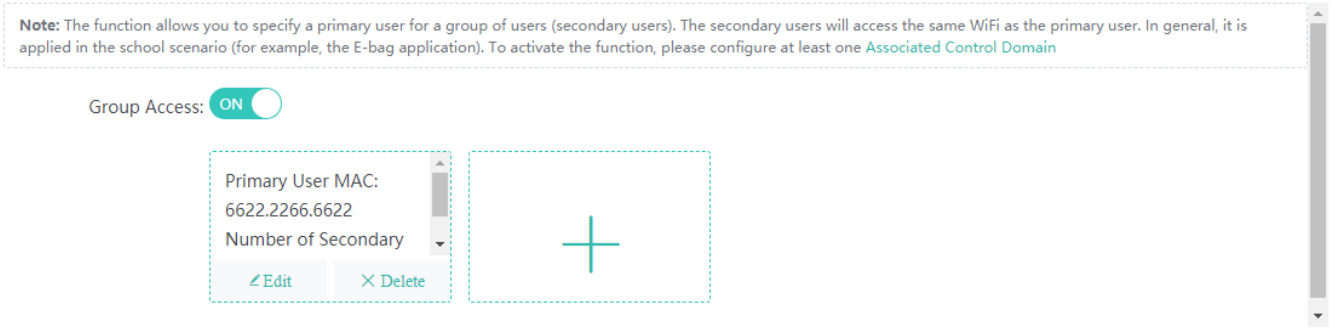
- Adding a STA package

Click + . In the displayed **Add MAC** window, set parameters and click **Save**. A setting success prompt is displayed and the new STA package is displayed in the associated control domain list.



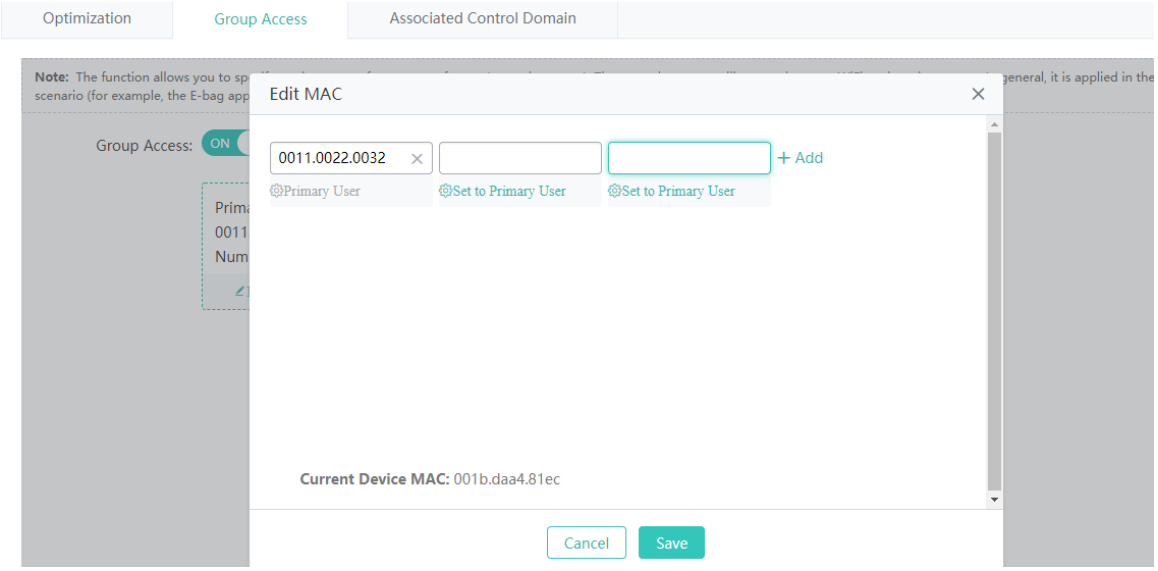
- Deleting a STA package

Click **Delete**. In the displayed confirmation window, click **OK** to complete the delete operation.

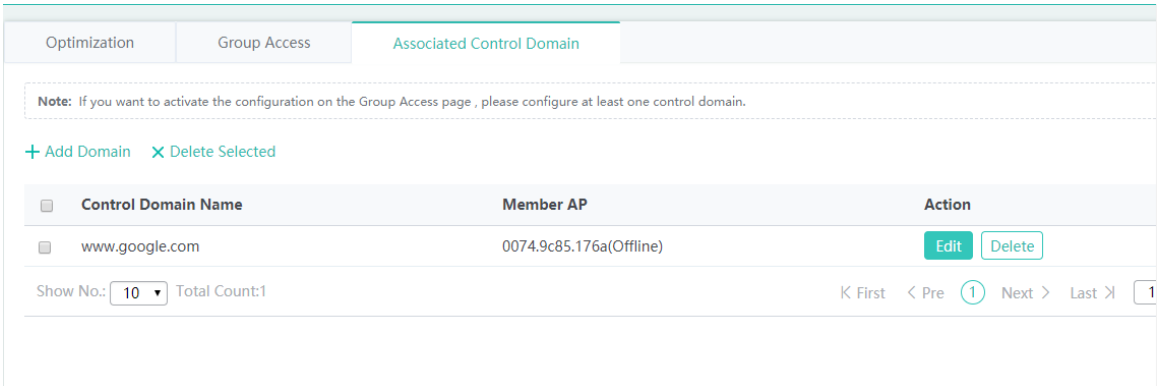


- Editing a STA package

Click **Edit**. In the displayed **Edit MAC** window, edit parameters and click **Save**. A setting success prompt is displayed and the modified STA package is displayed in the associated control domain list.

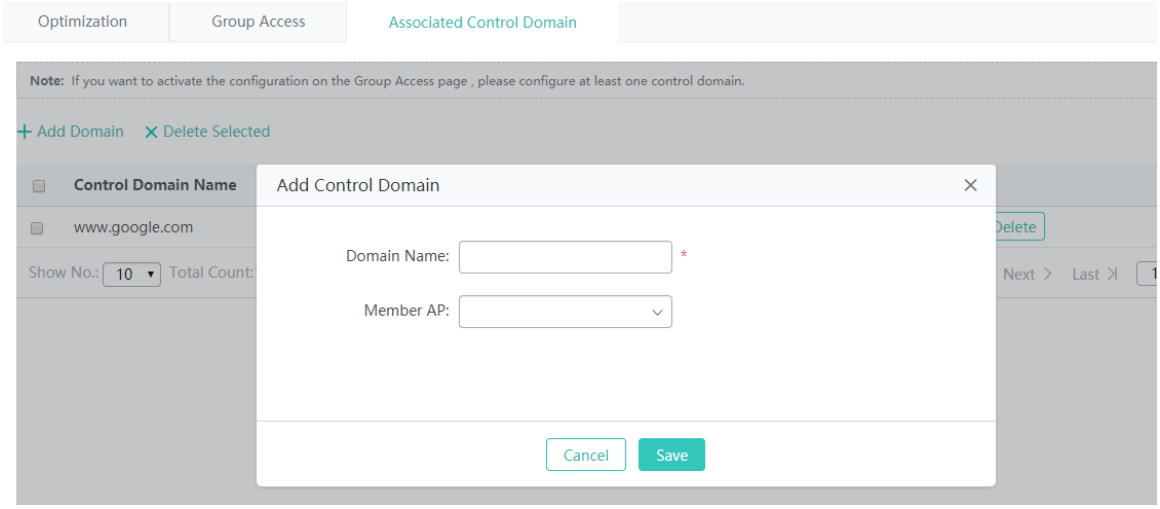


Associated Control Domain



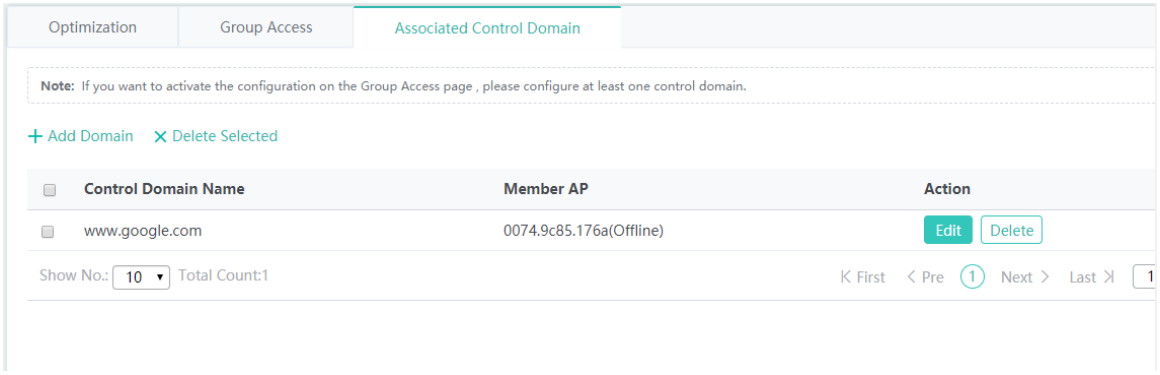
- Adding an associated control domain

Click **Add Domain**. In the displayed **Add Control Domain** window, set parameters and click **Save**. A setting success prompt is displayed and the new associated control domain is displayed in the associated control domain list.



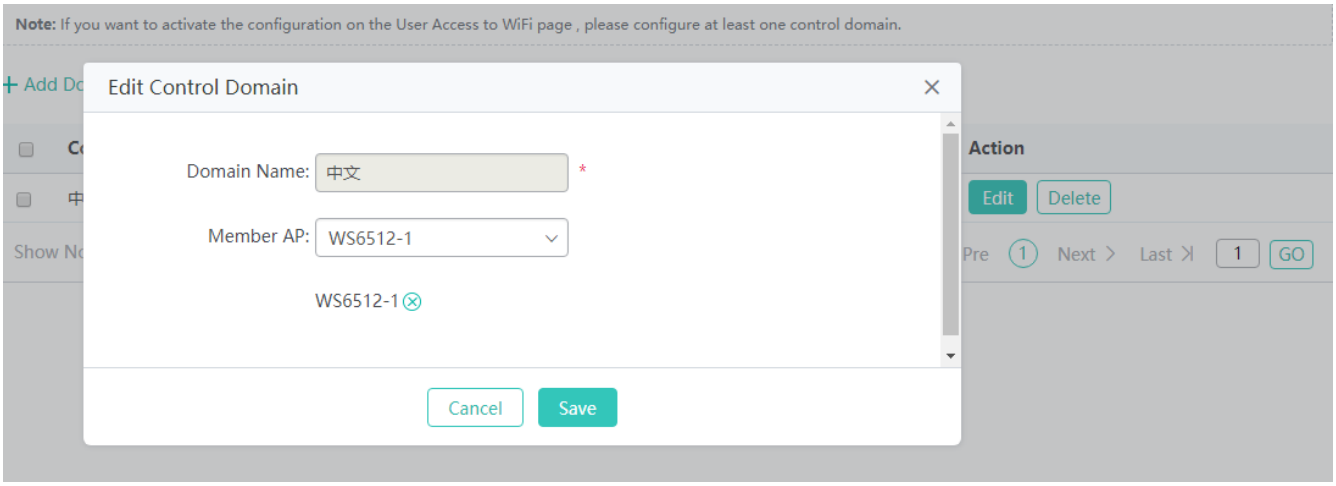
- Batch deleting associated control domains

Select associated control domains to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.



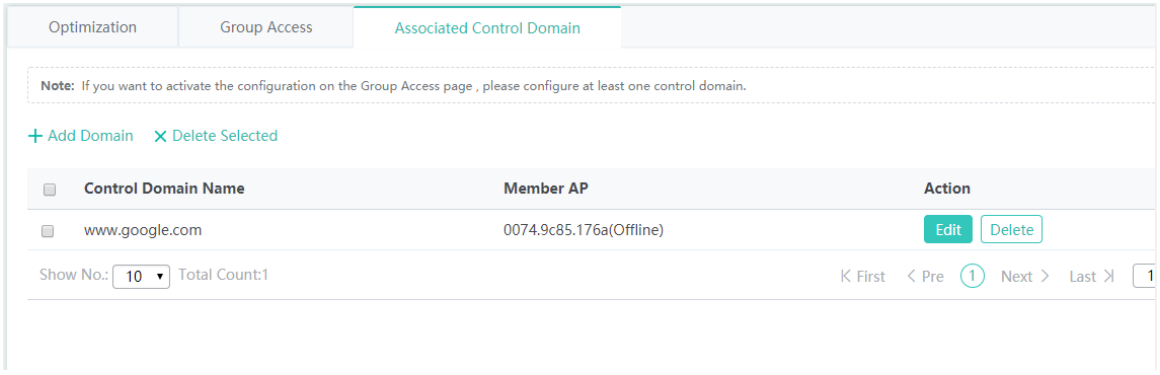
- Editing an associated control domain

Click **Edit** for an associated control domain in the list. The displayed window shows information about the associated control domain. Edit the information and click Save. A setting success prompt is displayed, indicating that the operation is complete.



- Deleting an associated control domain

Click **Delete** for an associated control domain in the list. In the displayed confirmation window, click **OK** to complete the delete operation.



1.3.3.9 Advanced

1.3.3.9.1 Unicast/Multicast

Three communication modes are supported: broadcast, multicast, and unicast.

Broadcast: It is generally used for broadcast teaching in classrooms. The teacher client (multicast) and student client are in the same broadcast domain. Multicast (broadcast) packets are directly pushed in the broadcast domain and multicast packets do not need to be transmitted across devices or network segments.

Multicast: This communication mode is generally used in universities and colleges. A multicast video server is deployed and pushes broadcast packets to the entire university or college in multicast mode.

Unicast: Information is received and transmitted between two nodes.

The following parameters need to be configured in multicast mode:

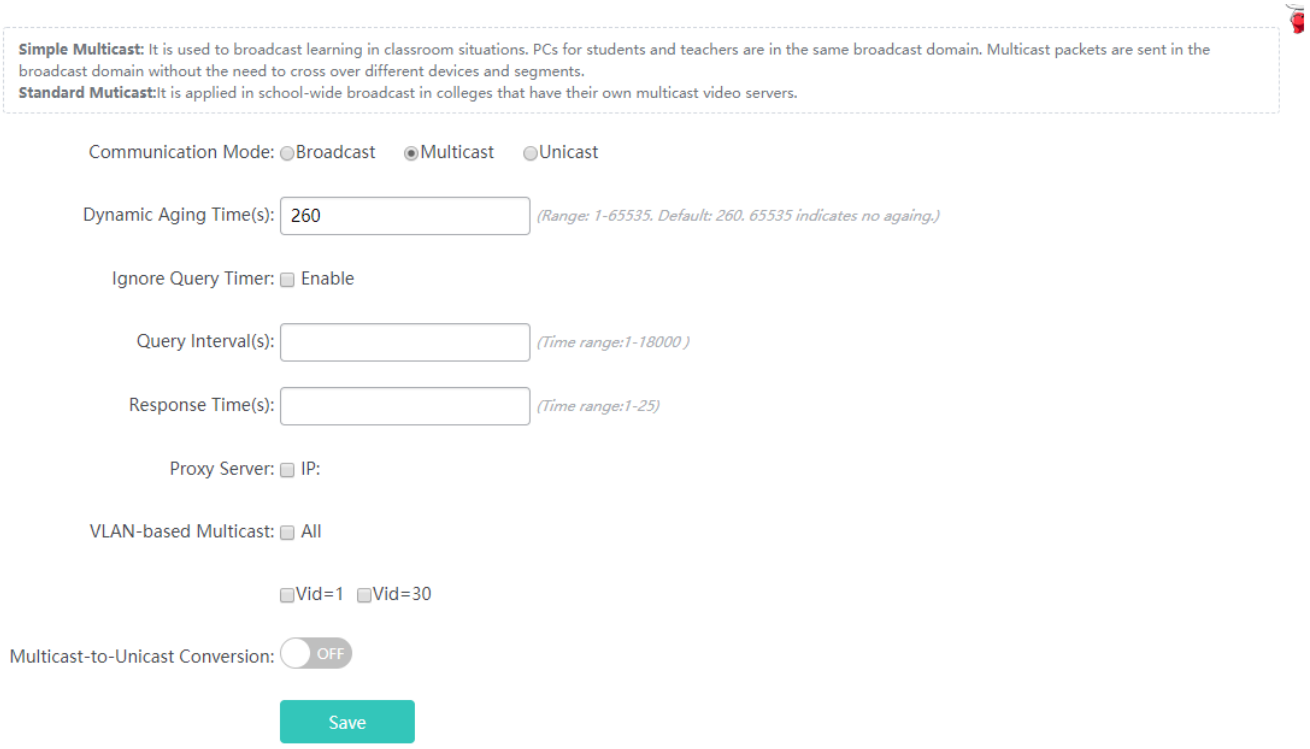
Dynamic Aging Time(s): If a multicast entry is not updated within the aging time, it ages and is deleted.

Query Interval(s): Configures the time period of **Ignore Query Timer**, so that a port is not aged within this period.

Proxy Server: Indicates the layer-3 proxy device. After it is selected, configure the IP address of the layer-3 device.

VLAN-based Multicast: Select a VLAN on which the multicast function needs to be enabled. The multicast function may be enabled on all VLANs.

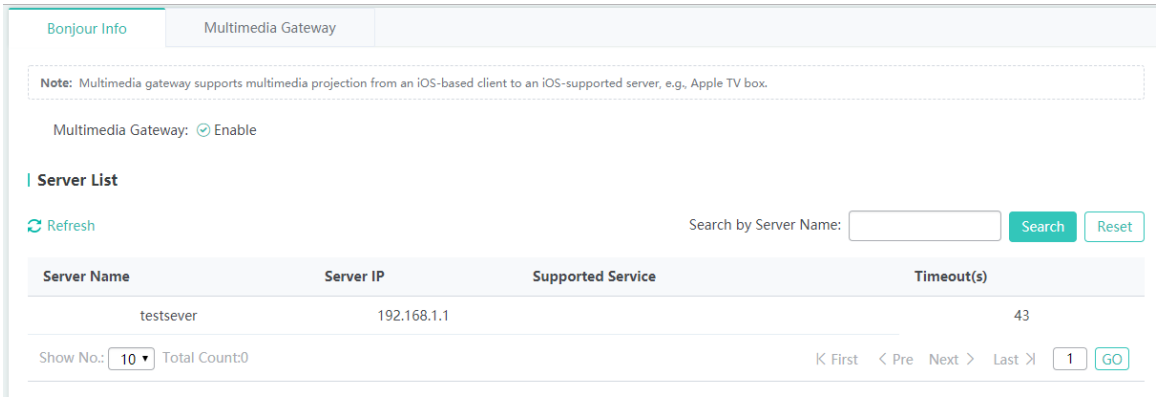
See the figure below.



1.3.3.9.2 Multicast Gateway

The multicast gateway is mainly used for the projection from an iOS-based client to an iOS-supported server, such as the TV box.

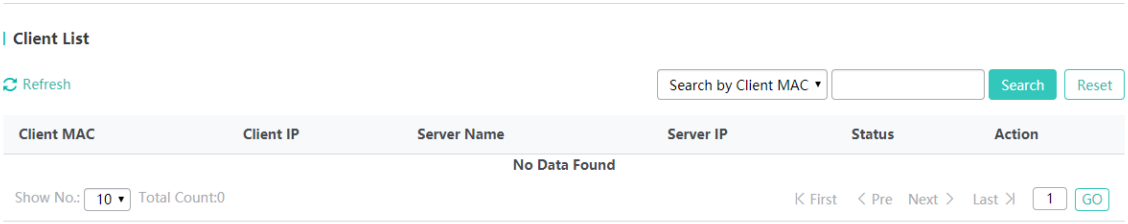
Bonjour Info



- Search

Select the client MAC address, client IP address, or server name from the drop-down list, enter a corresponding value in the

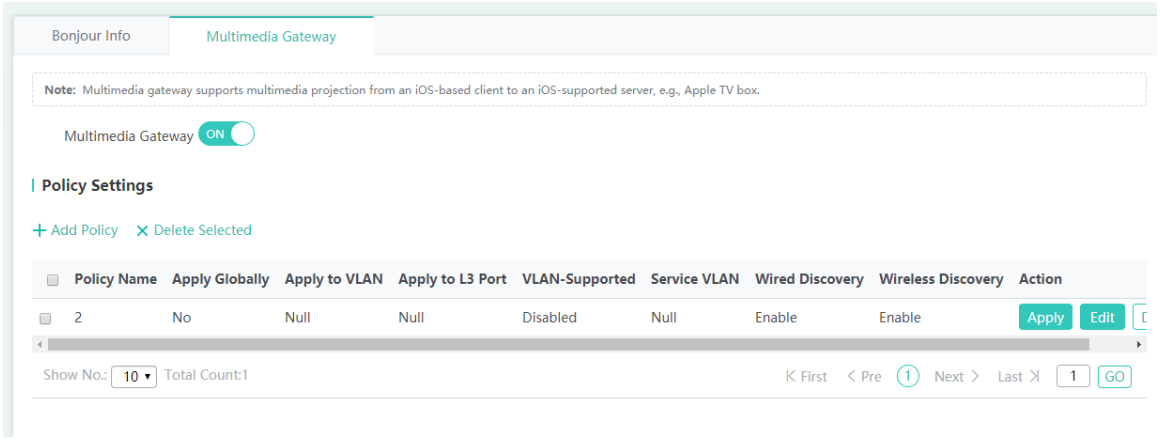
search box, and click **Search** to search for clients that meet the search condition.



- Reset

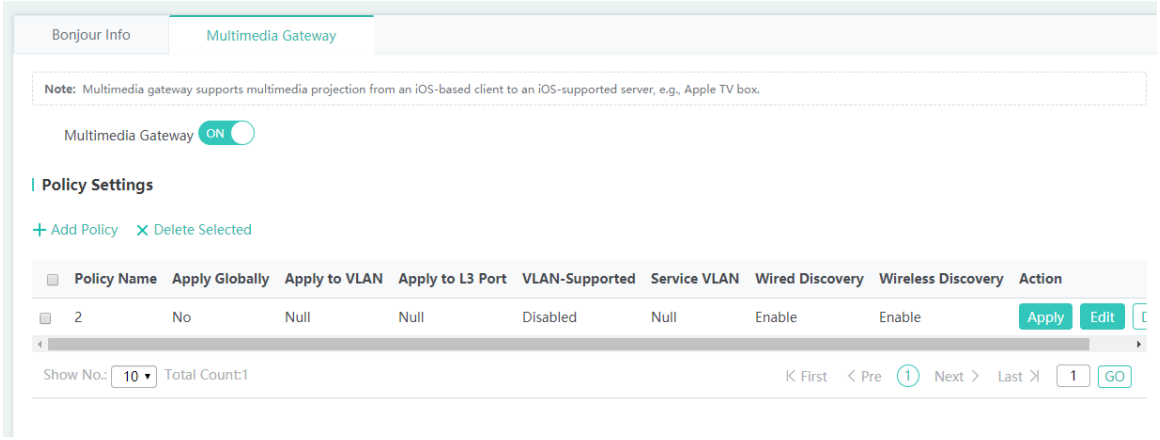
Click **Reset** to reset the search condition.

Multicast Gateway



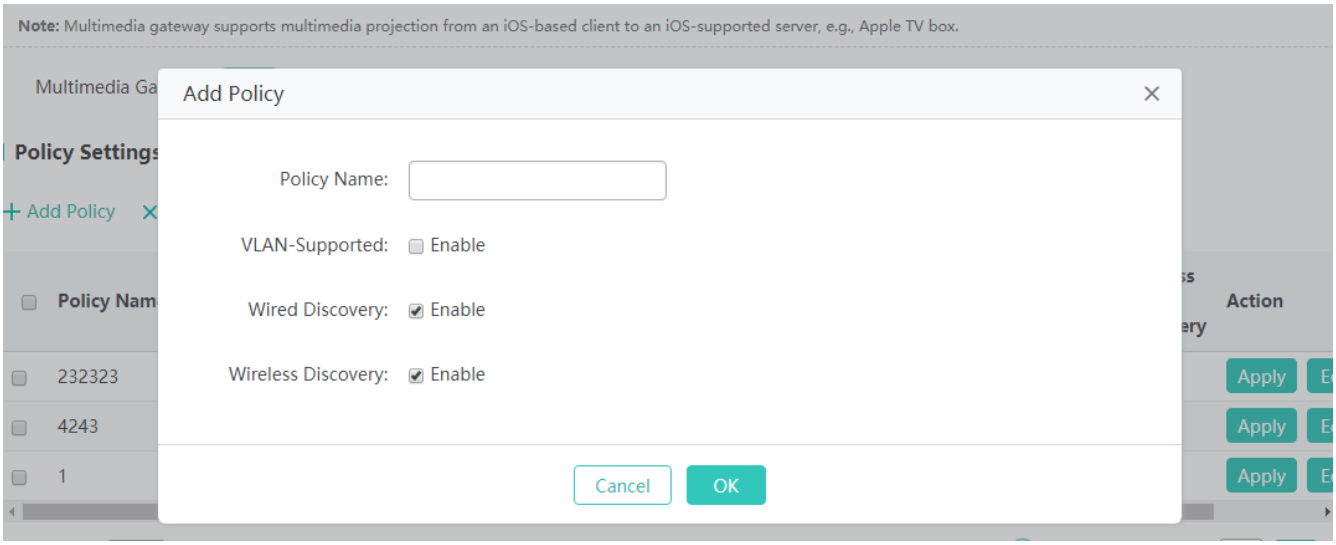
- Enabling/Disabling configuration

Multimedia Gateway can be set to **ON**/**OFF** to enable/disable the multimedia gateway function.



- Adding a policy

Click **Add Policy**. In the displayed **Add Policy** window, set parameters and click **OK**. A setting success prompt is displayed and the new policy is displayed in the policy list.



- Batch deleting policies

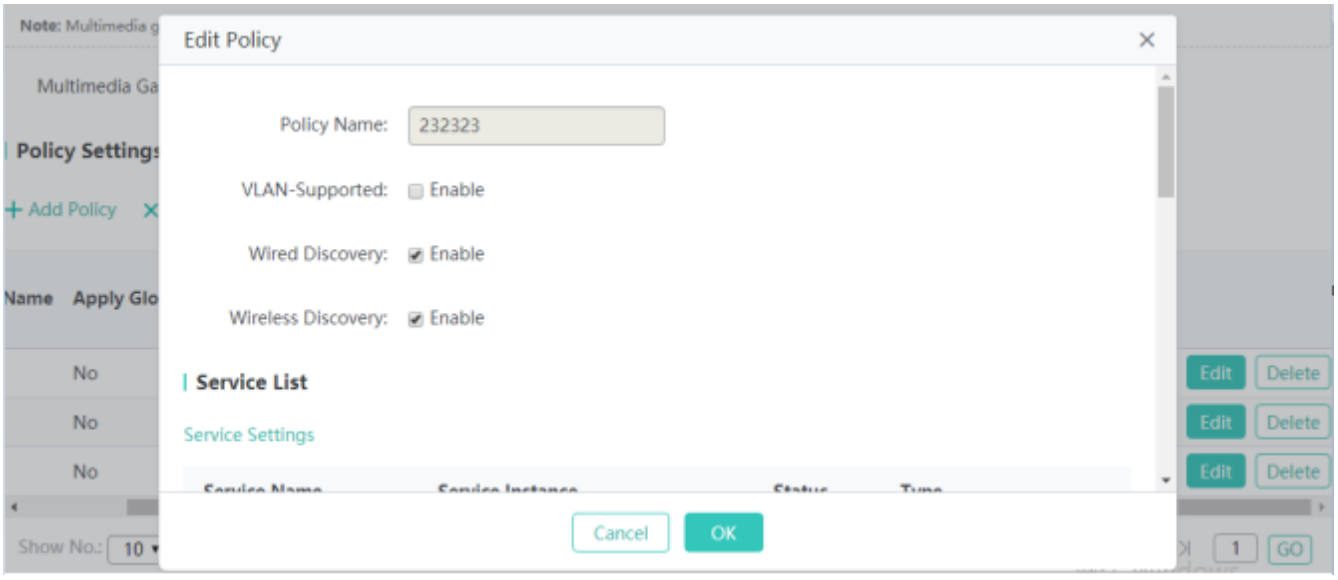
Select policies to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

- Applying a policy

Click **Apply** for a policy in the list. The displayed window shows application information of the policy. Edit the information and click **OK** to complete the operation.

- Editing a policy

Click **Edit** for a policy in the list. The displayed window shows information about the policy. Edit the information and click **OK**. A setting success prompt is displayed, indicating that the operation is complete.

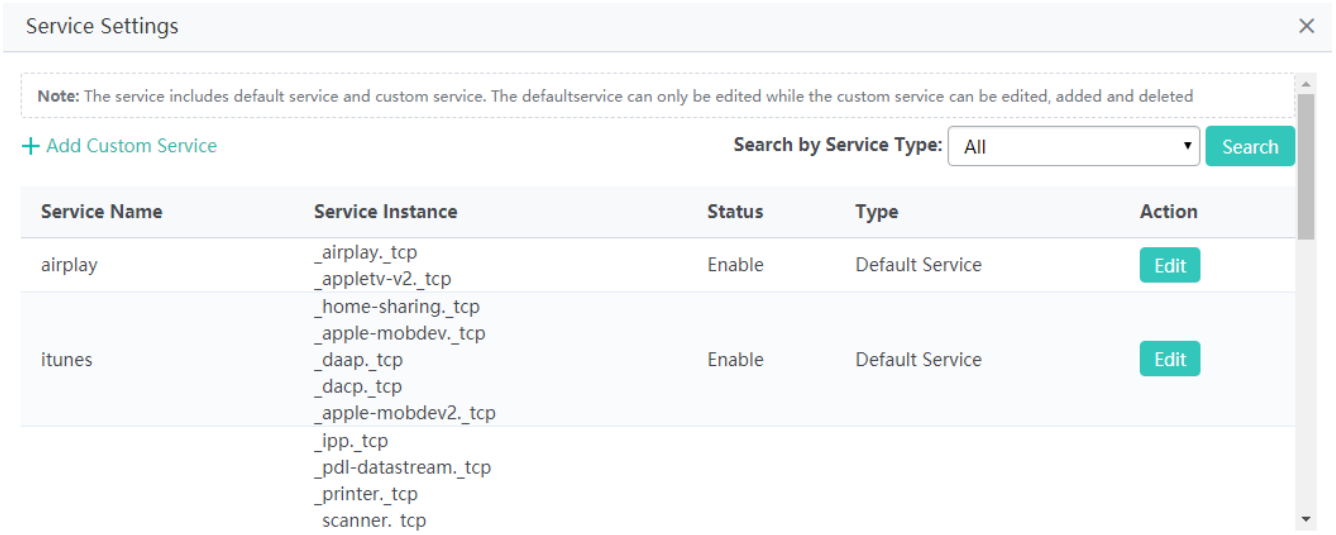


- Deleting a policy

Click **Delete** for a policy in the list. In the displayed confirmation window, click **OK** to complete the delete operation.

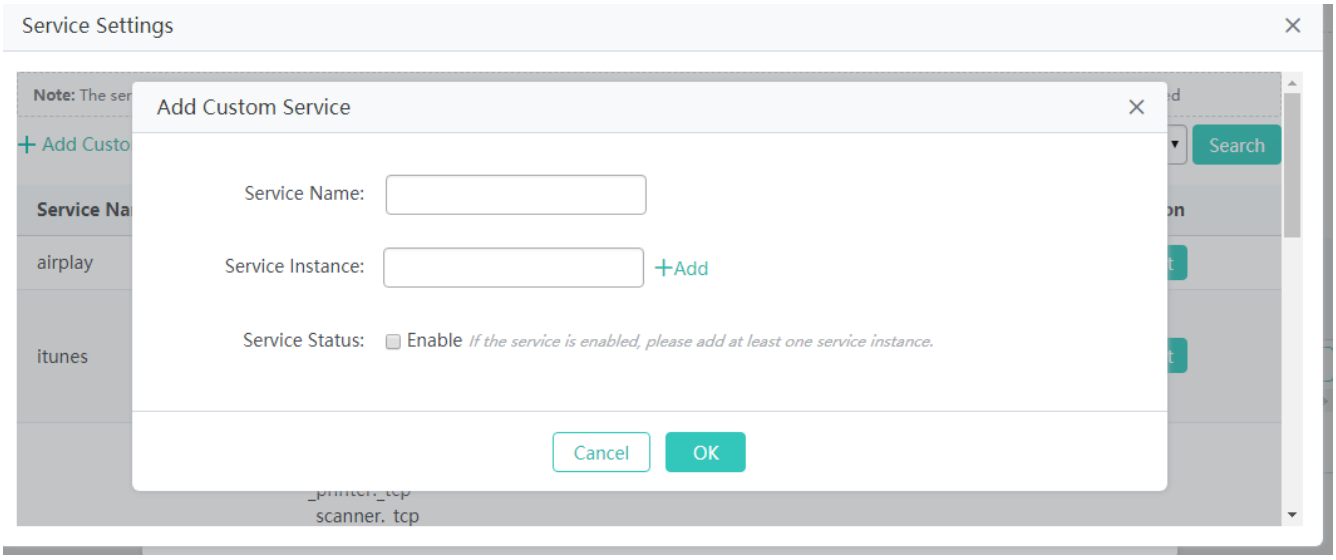
- Service Settings

The **Service Settings** button on the **Edit Policy** page is the service settings entry.



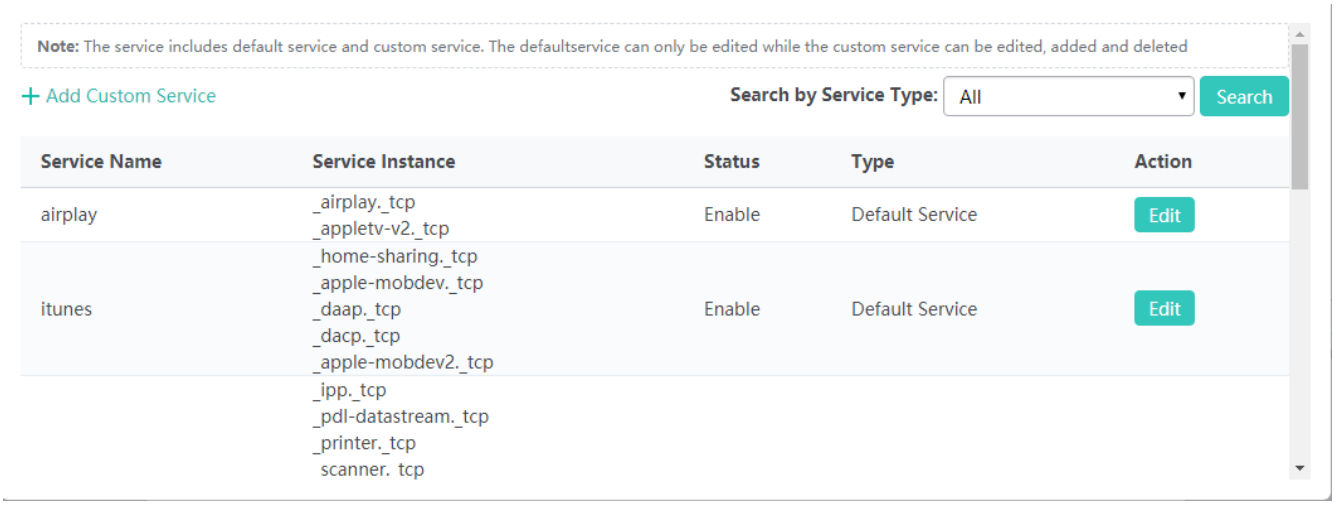
- Adding a custom service

Click **Add Custom Service**. In the displayed **Add Custom Service** window, set parameters and click **OK**. A setting success prompt is displayed and the new service is displayed in the service list.



- Searching for services

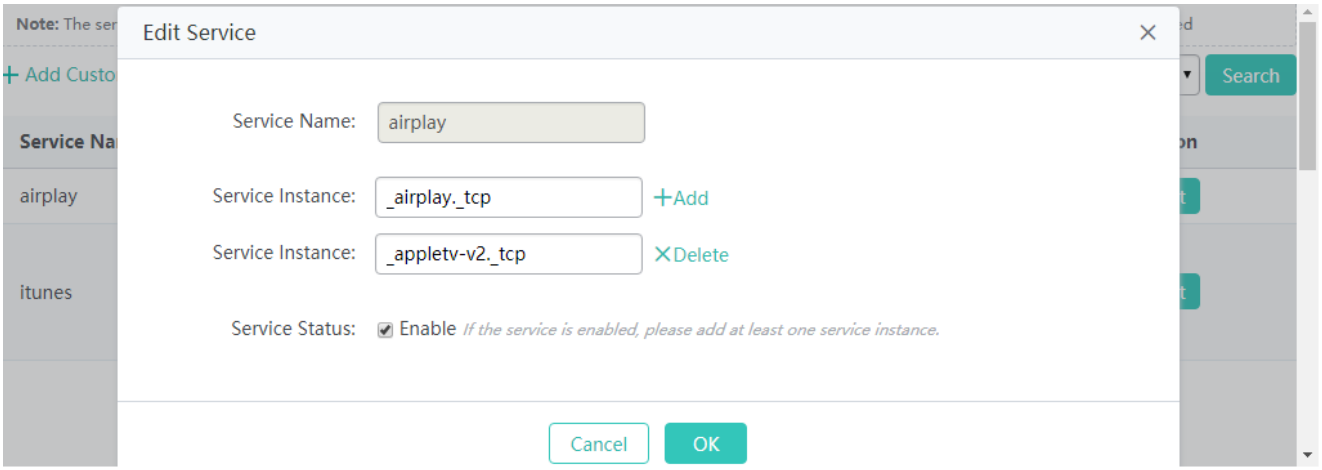
Select a search condition from the drop-down list and click **Search** to search for services that meet the search condition.



- Editing a service

Default service instances in the default service cannot be modified or deleted, and only custom service instances can be modified and deleted.

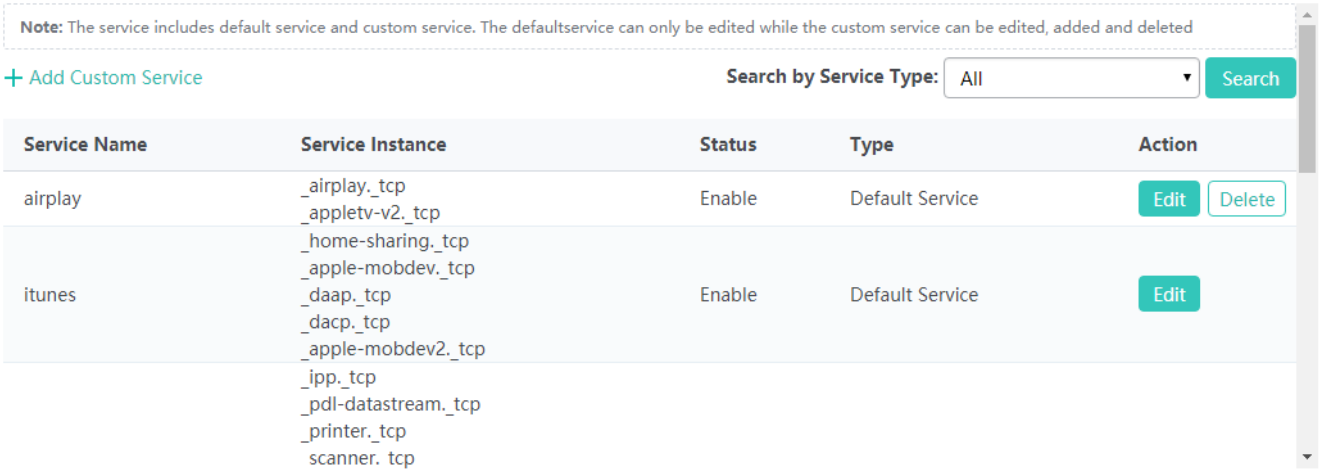
Click **Edit** for a service in the list. The displayed window shows information about the service. Edit the information and click **OK**. A setting success prompt is displayed, indicating that the operation is complete.



- Deleting a custom service

The default service cannot be deleted, and only custom services can be added or deleted.

Click **Delete** for a custom service in the list. In the displayed confirmation window, click **OK** to complete the delete operation.



Whether this function is supported is subject to actual products.

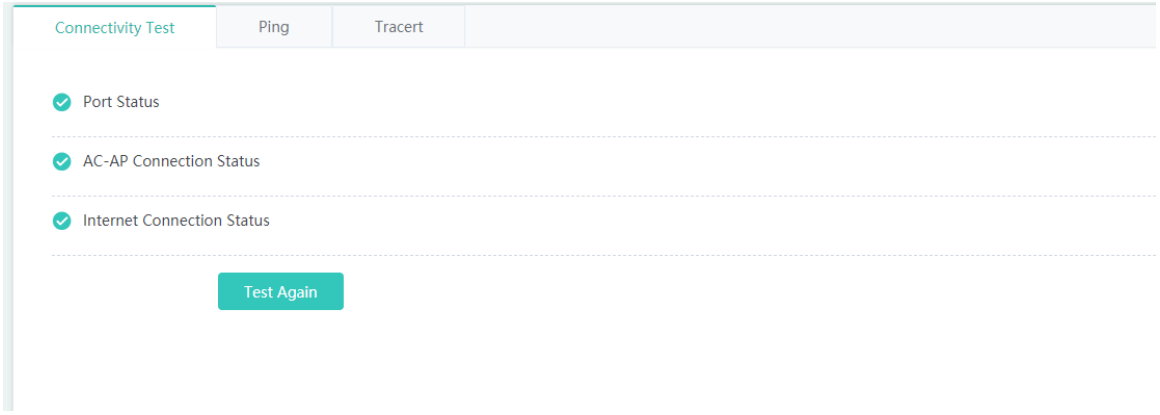
1.3.4 Diagnosis

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.



Port Status

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

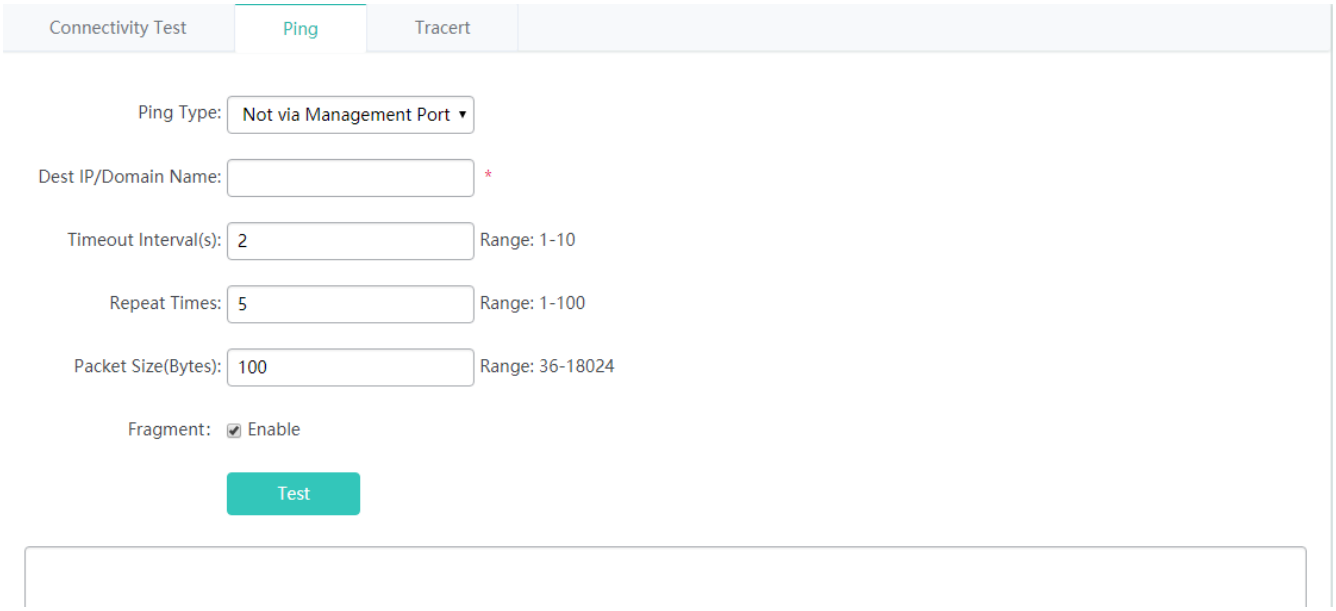
AC-AP Connection Status

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 outband 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.

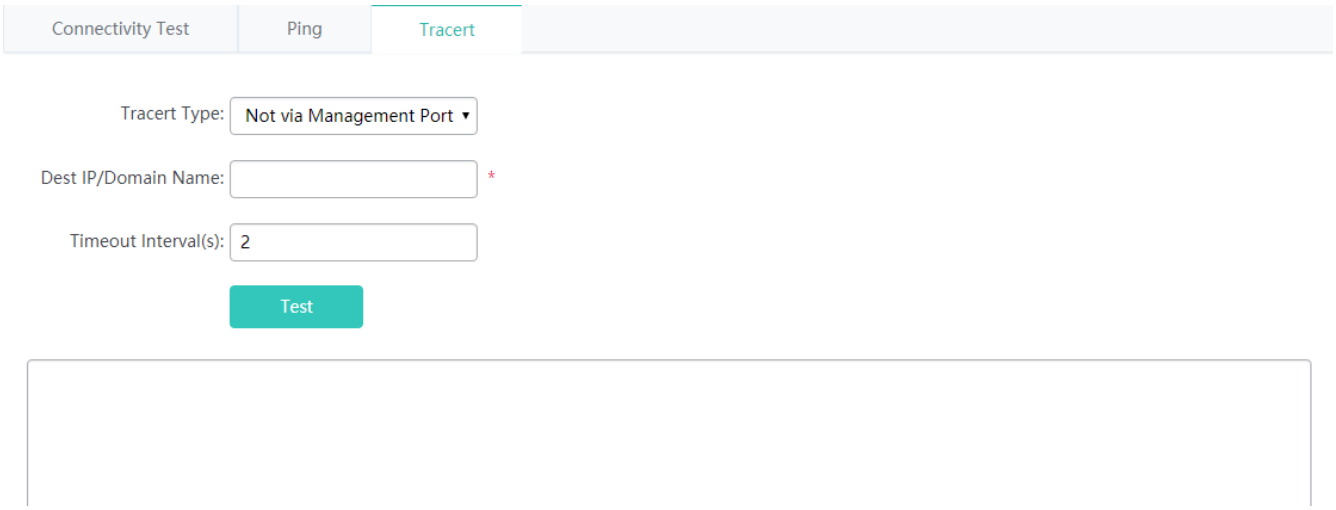
Packet Size(Bytes)

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 outband 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.

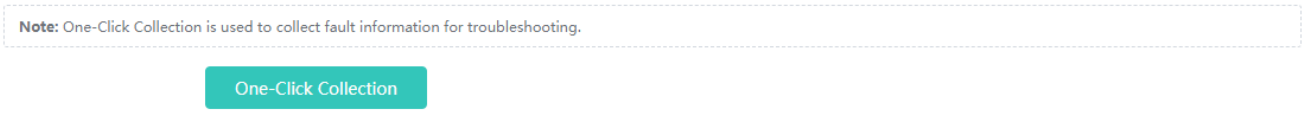
Timeout Interval(s)

Indicates the timeout interval.

1.3.4.2 One-click Collection

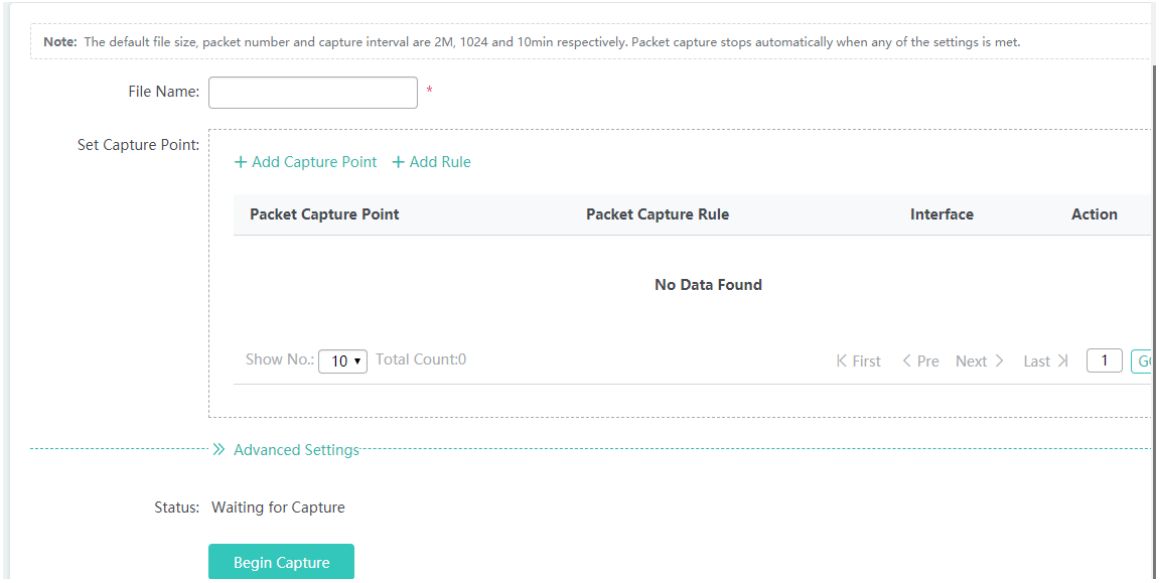
The one-click collection function collects device fault information for troubleshooting.

Your AC may not support this function and the actual menu items shall prevail.



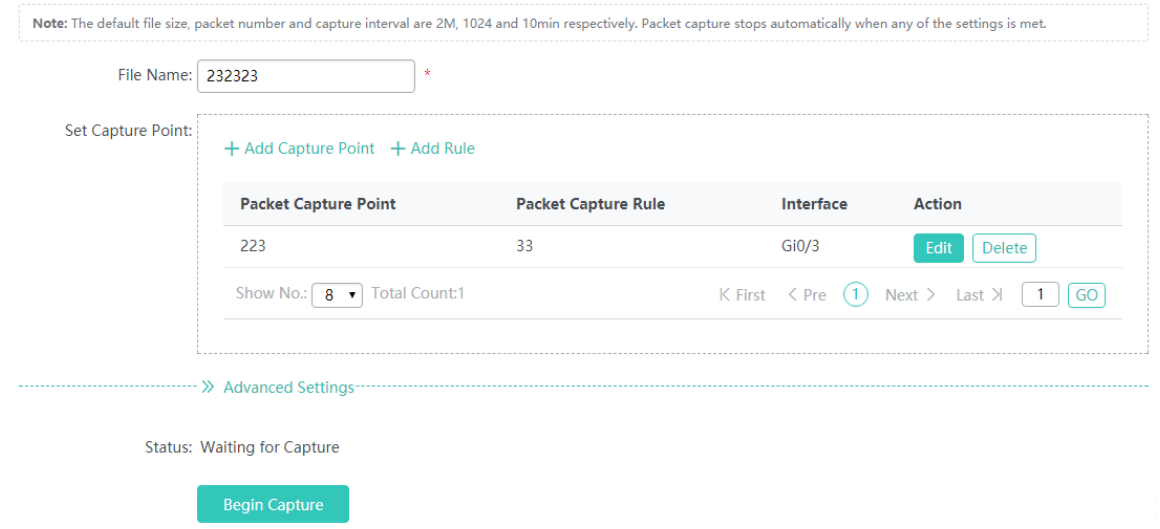
1.3.4.3 Packet Capture and Diagnosis

This function captures packets to collect diagnosis data when a device malfunctions.



- Starting packet capture

Set parameters on the page below and click **Begin Capture** to start packet capture.



Parameter description:

File Name

Indicates the name of the file for storing captured packets.

Packet Capture Point

Indicates a point for capturing packets.

Storage Path

Indicates the path for storing the file.

File Size(M)

Indicates the buffer size.

Packets

Indicates the number of captured packets.

Capture Interval(Min)

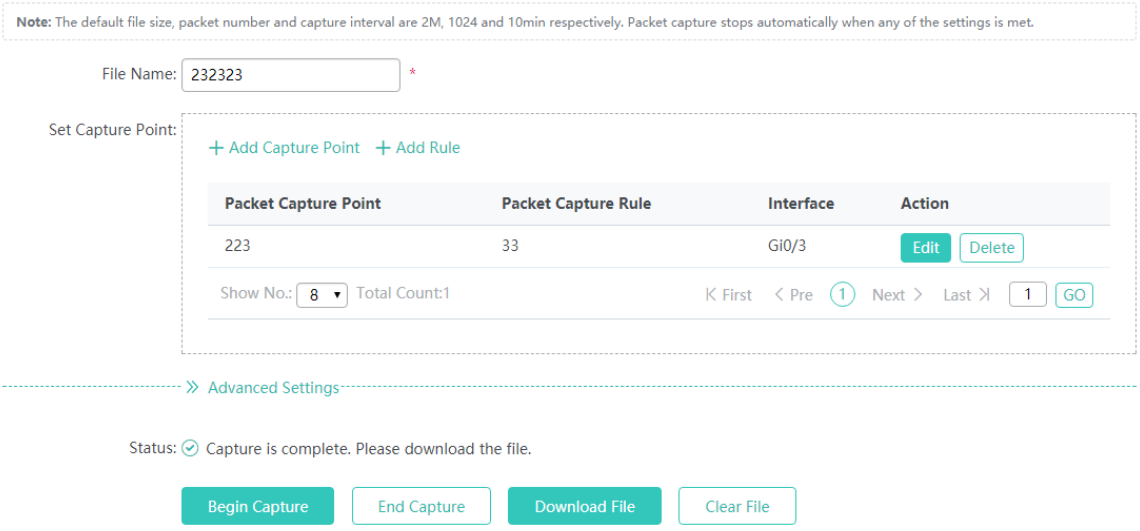
Indicates the packet capture timeout time. The device automatically stops packet capture after the timeout time expires.

- Stopping packet capture

Click **End Capture** to stop packet capture.

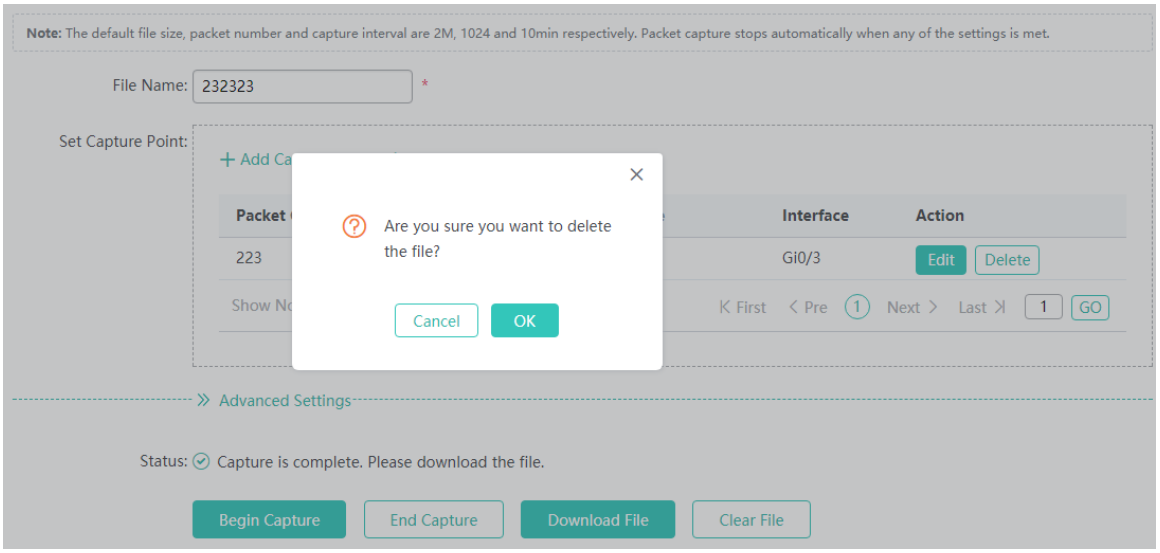
- Downloading a file

Click **Download File** to download the packet capture file to a PC.



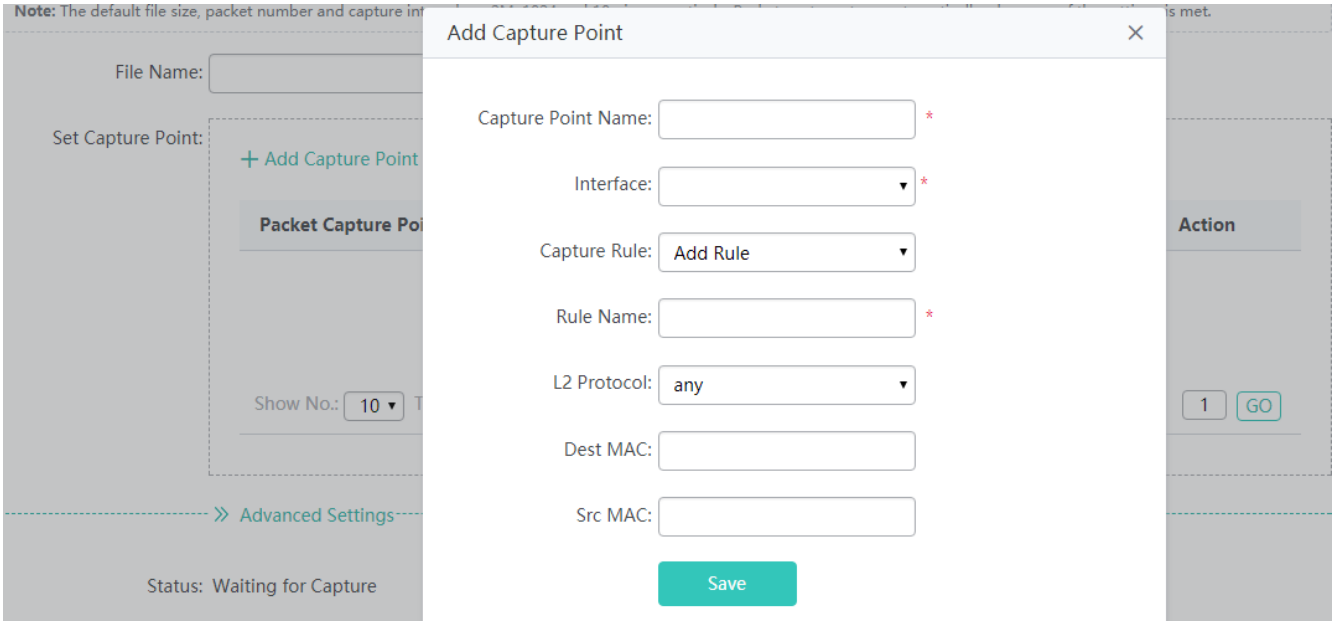
- Clearing a file

Click **Clear File** In the displayed window, click **OK** to clear the packet capture file of the device.



- Adding a capture point

Click **Add Capture Point**. In the displayed **Add Capture Point** window, set parameters and click **Save**. An adding success prompt is displayed.



Capture Point Name

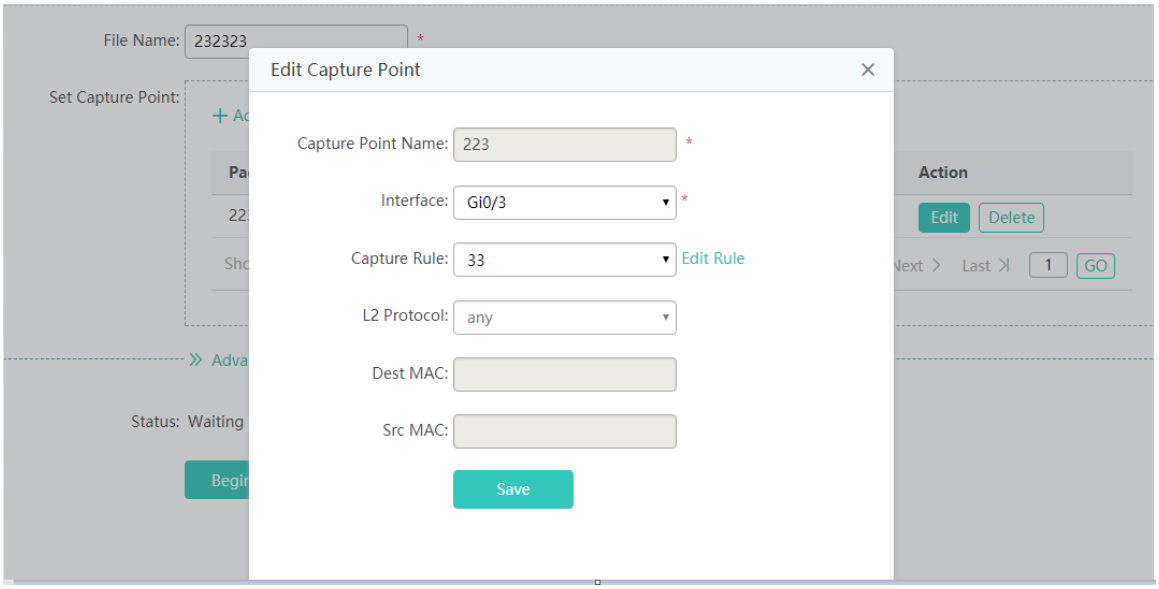
Indicates the name of the capture point.

Interface

Indicates the name of the interface for capturing packets.

- Editing a packet capture point

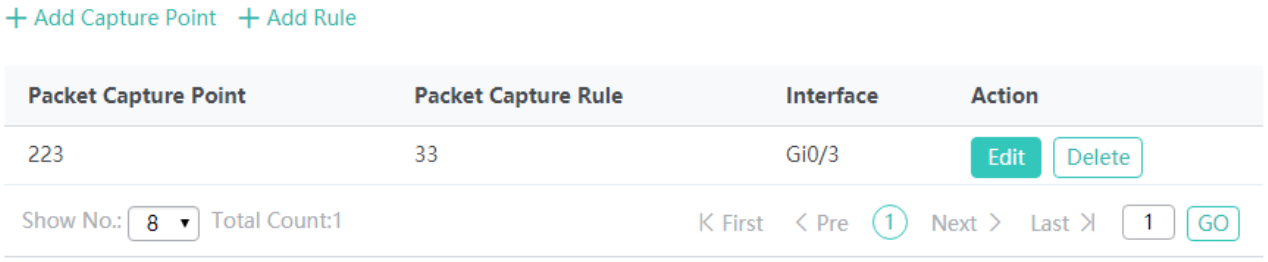
Click **Edit** for a capture point in the capture point list. In the displayed **Edit Capture Point** window, set parameters and click **Save**. An editing success prompt is displayed.



The parameters for editing a capture point are the same as those for adding a capture point and are not described again.

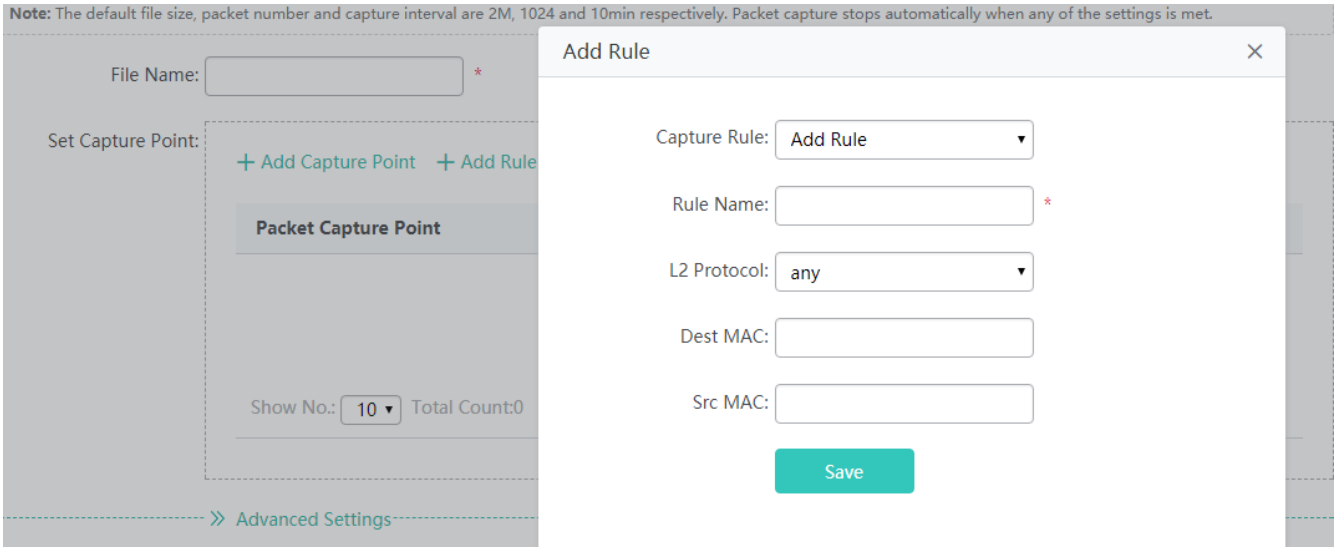
- Deleting a capture point

Click **Delete** for a capture point in the list. In the displayed confirmation window, click **OK** to complete the delete operation.



- Setting packet capture rules

Click **Add Rule**. In the displayed **Add Rule** window, set parameters and click **Save**. An adding success prompt is displayed.



Capture Rule

Specifies to add or edit a rule.

Rule Name Indicates the name of the match rule.

L2 Protocol

Indicates the type of the layer-2 protocol.

Dest MAC

Indicates the destination MAC address.

Src MAC

Indicates the source MAC address.

L3 Protocol

Indicates the type of the layer-3 protocol.

Dest IP (Port)

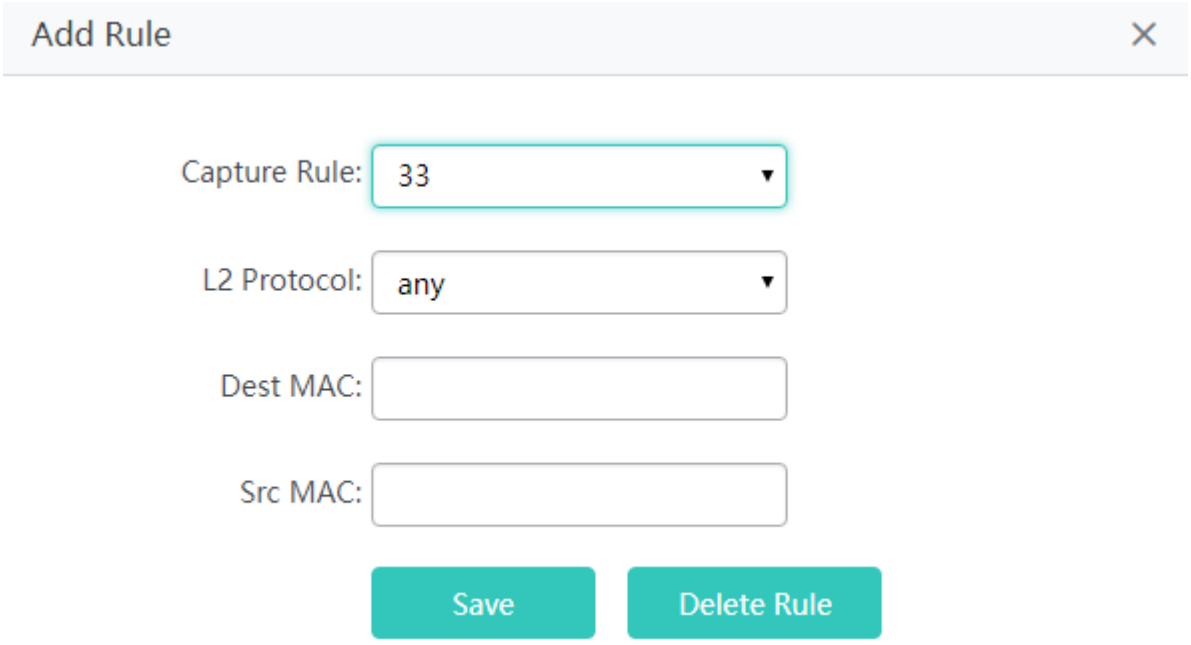
Indicates the destination port of the layer-3 TCP/UDP protocol.

Src IP (Port)

Indicates the source port of the layer-3 TCP/UDP protocol.

- Deleting a packet capture rule

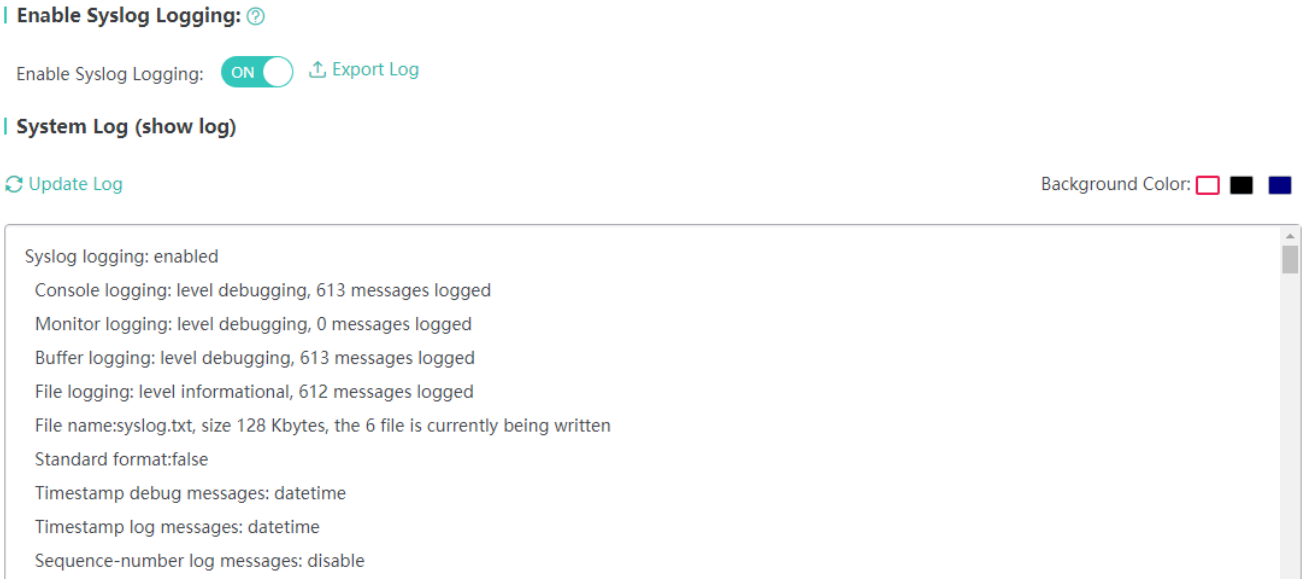
Select the packet capture rule to be deleted from the **Capture Rule** drop-down list and click **Delete Rule**. In the displayed confirmation window, click **OK** to complete the delete operation.



1.3.4.4 Log

1.3.4.4.1 System Log

Configure the syslog log function to help after-sales and R&D personnel locate problems.



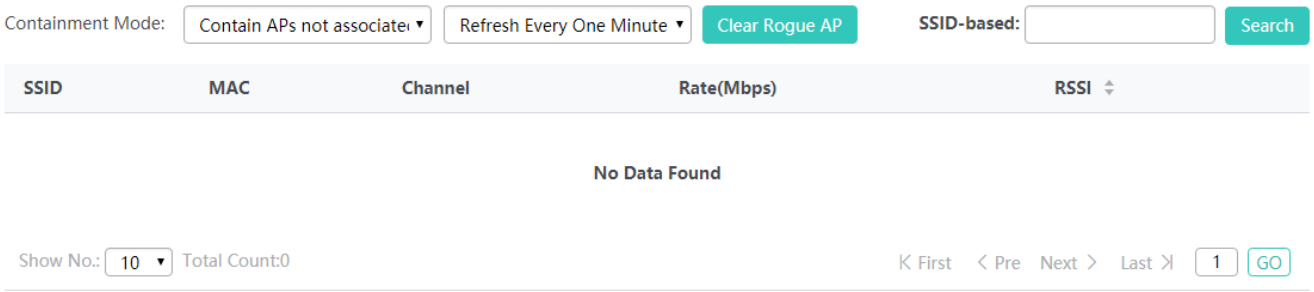
1.3.4.5 Wireless Intrusion Detection

1.3.4.5.1 Rogue AP

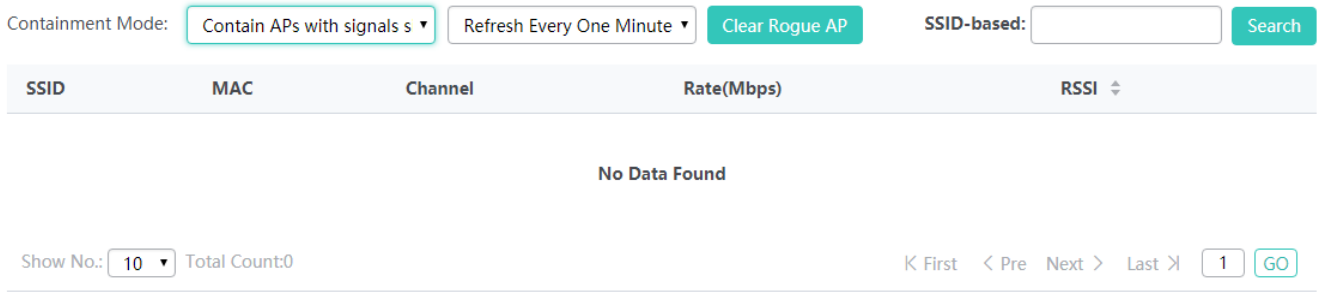
Rogue APs may exist on a WLAN, and may be vulnerable in security or controlled by attackers, seriously threatening or endangering the security of the user network.

The tables below list possible rogue APs that are identified after the containment function is enabled based on different containment modes.

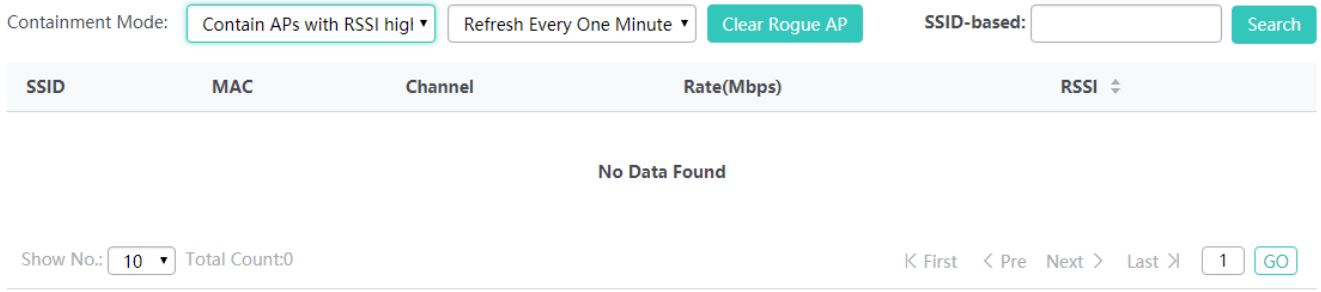
SSID-based mode: The system identifies signals with the same SSID sent by wireless devices associated with different ACs and performs containment on the signals.



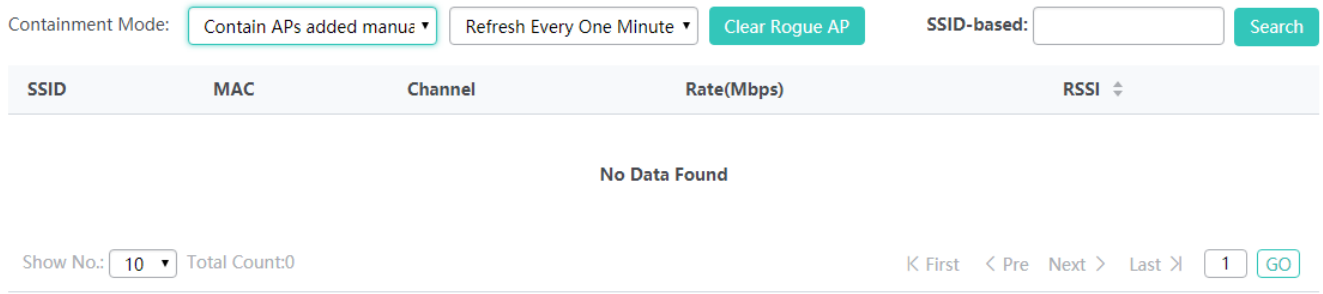
AdHoc mode: The system contains the signals simulated and sent by non-APs (such as AdHoc signals).



Rogue mode: The system contains signals based on the RSSI.



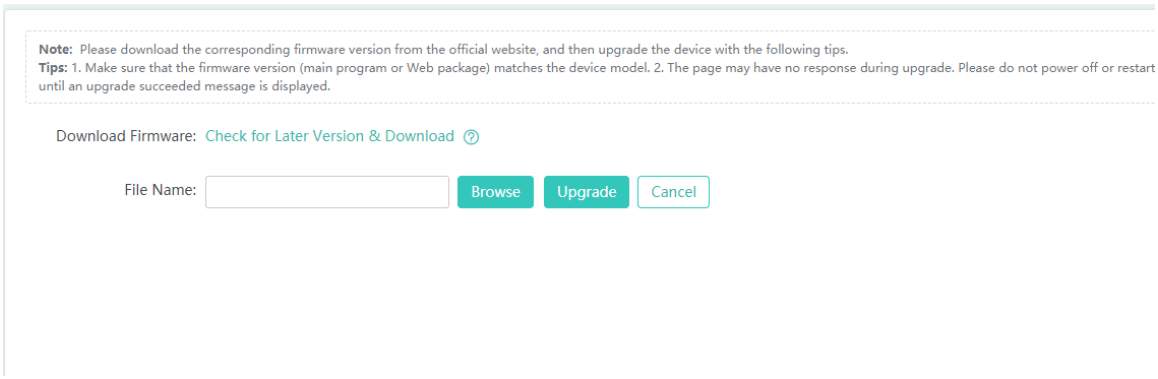
Config mode: The system contains APs with MAC addresses or SSIDs that are blacklisted.



1.3.5 Maintenance

1.3.5.1 AC Management

1.3.5.1.1 AC Upgrade

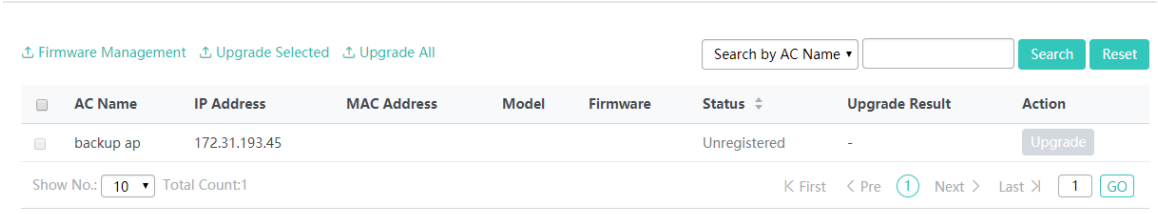


Select the BIN package used for upgrade from the administrator PC to upgrade the AC.

1.3.5.1.2 Branch AC Upgrade

The branch AC upgrade is available on the central AC. It is used to upgrade branch ACs in a unified manner to improve efficiency.

Click **Upgrade** for an AC in the AC list to upgrade a single online AC. You can also select multiple online ACs and click **Upgrade Selected** to batch upgrade the ACs, or click **Upgrade All** to upgrade all online ACs.

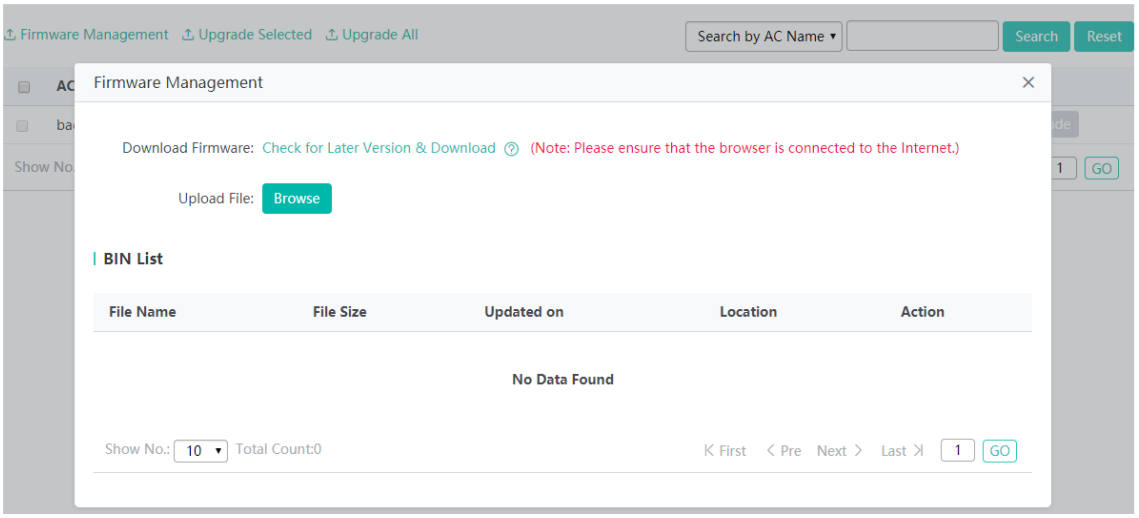


Firmware Management

Click **Check for Later Version & Download** to download a version from the official website.

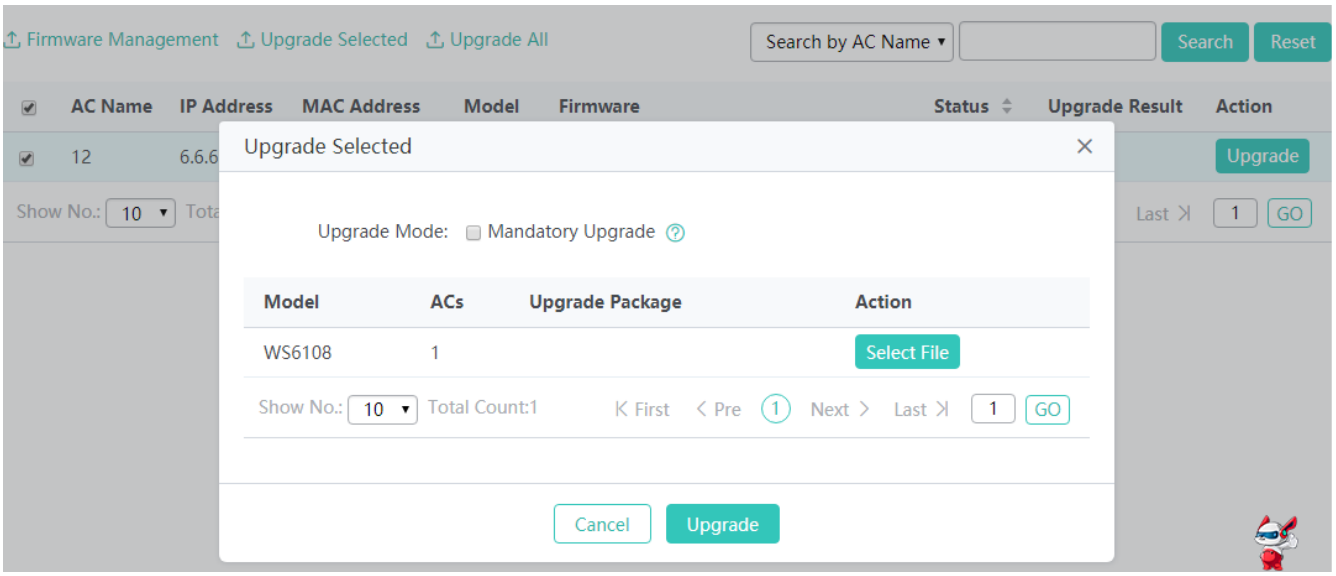
Click **Browse** to upload a version from the local device to perform the upgrade.

BIN List displays a list of existing versions of the device.



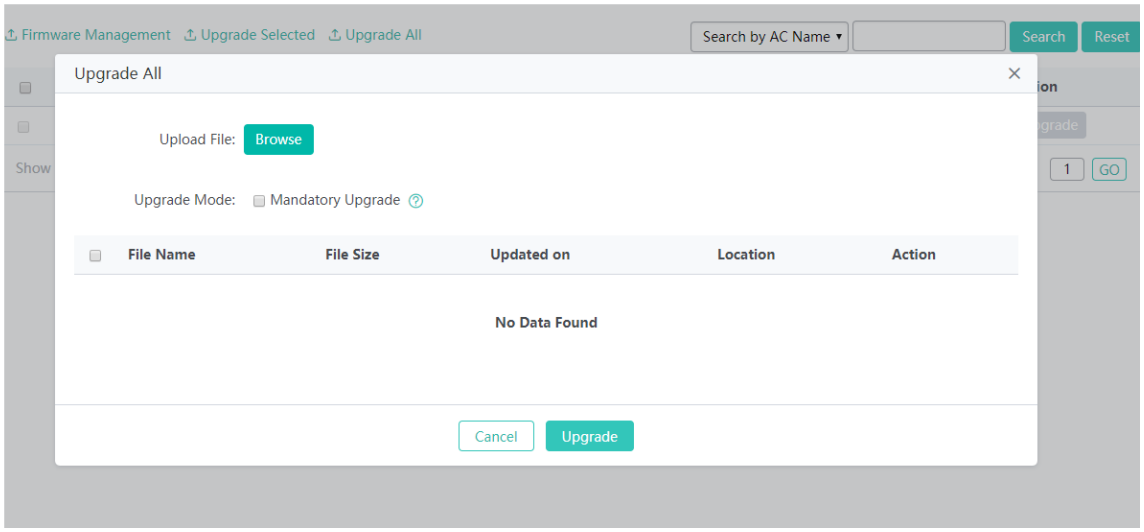
Batch upgrading ACs

In the AC list, select multiple ACs and click **Upgrade Selected**. In the **Upgrade Selected** window, click **Select File** to select a file for upgrade.



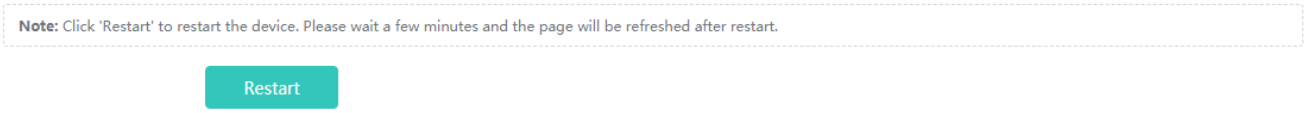
Upgrading all ACs

Click **Upgrade All**. In the displayed **Upgrade All** window, select **Browse** to select a file for upgrade.



1.3.5.1.3 AC Restart

Click **Restart** to restart the device conveniently.

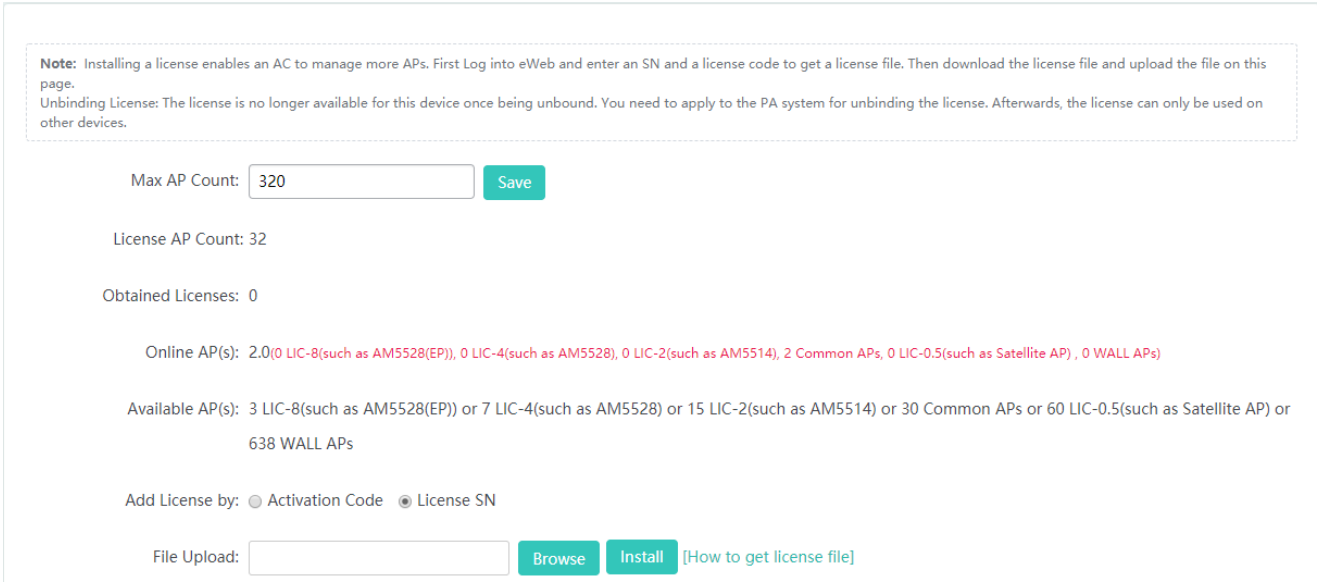


1.3.5.1.4 License Management

License management is used to protect the legitimate interest of authorized users. Licenses are used to control the upper limit of APs supported by an AC. Different devices have different upper limits of supported APs and different license types, and licenses of different types are embodied differently. The actual licenses supported by devices shall prevail.

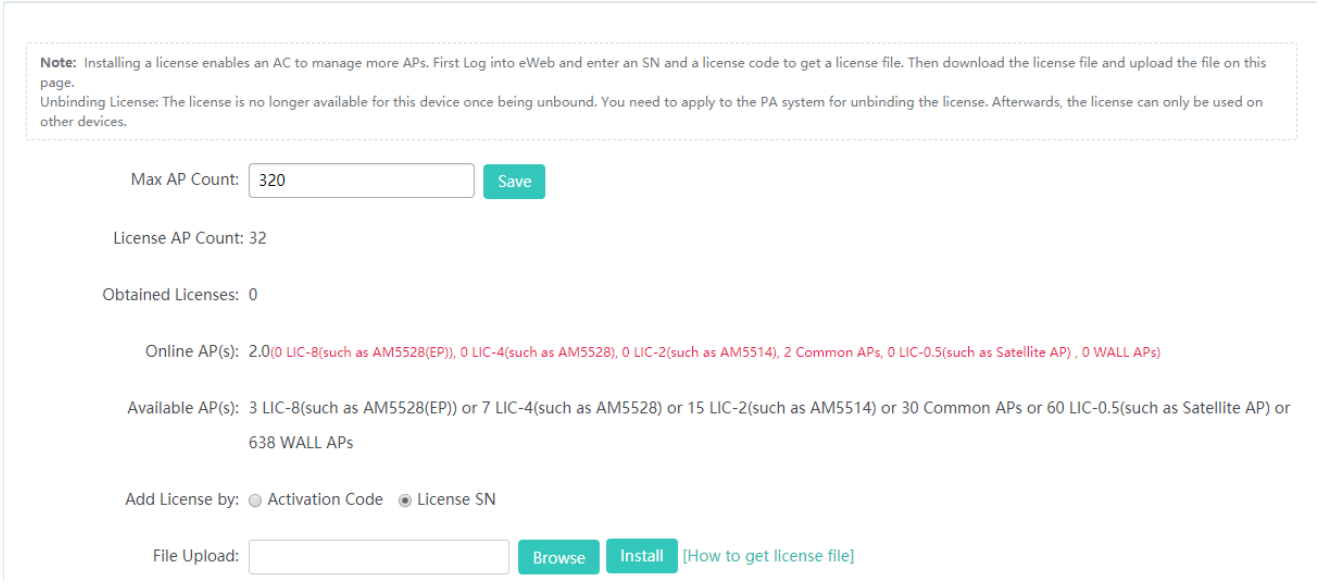
Whether this function is supported is subject to actual products.

This page shows the license usage of an AC.

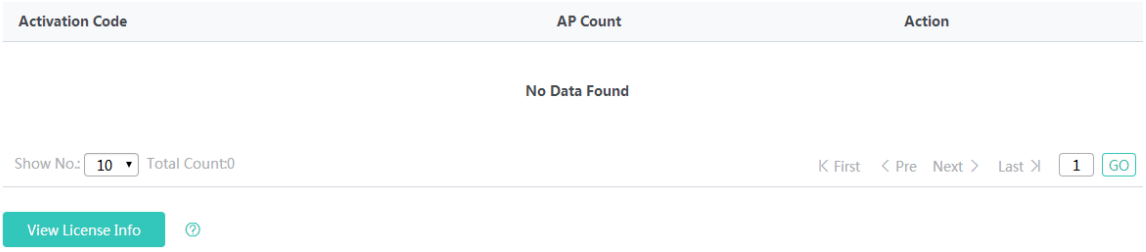


License management is performed based on the activation code mode and license SN mode.

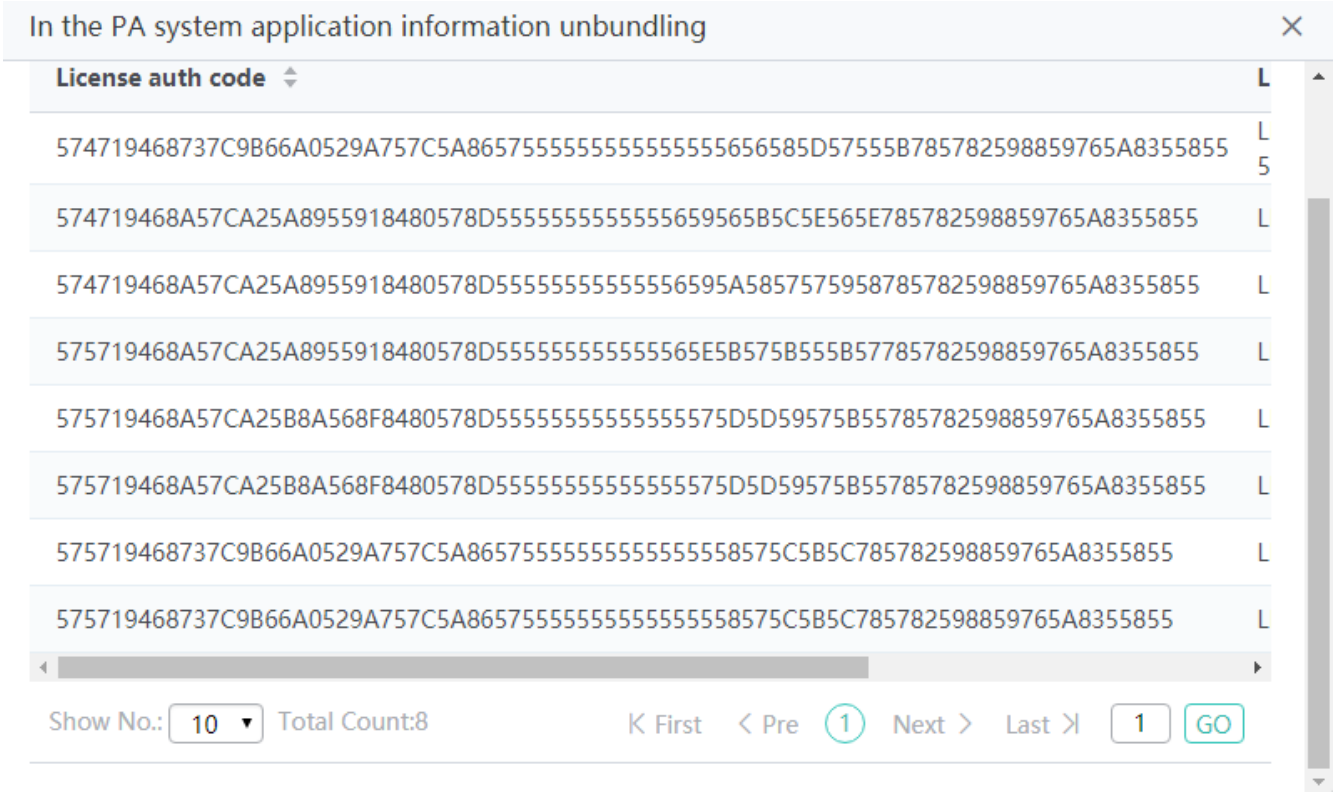
The figure below shows the license SN mode.



The figure below shows the license mode.



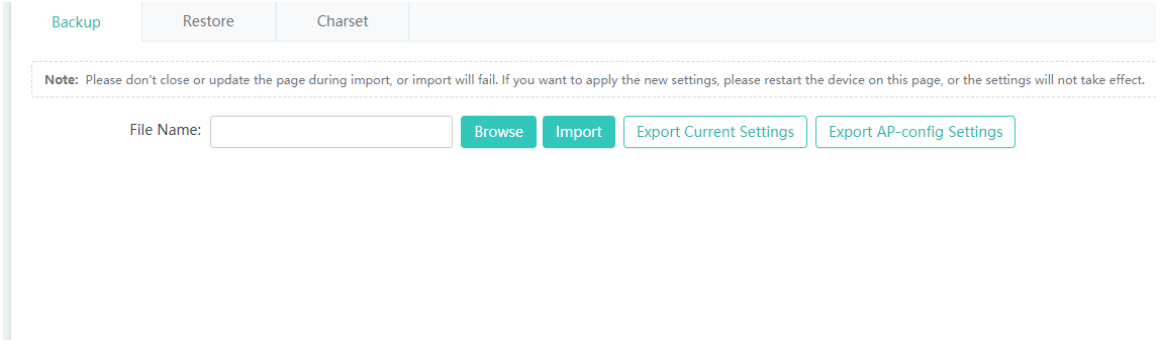
- Displaying the unbinding information in the PA system



1.3.5.1.5 Configuration Management

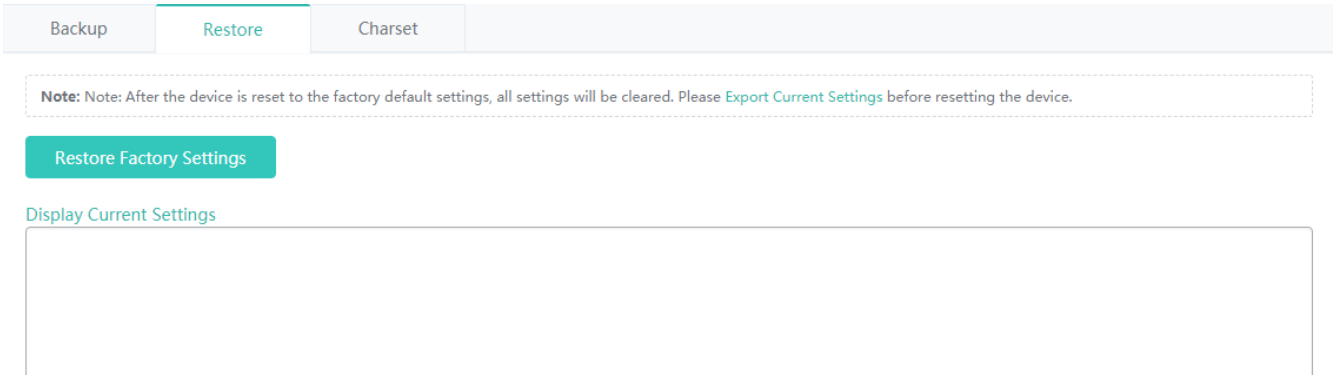
Backup

This function enables you to back up the configuration file on the device, and import or export configurations to batch perform operations, thereby facilitating user operations.



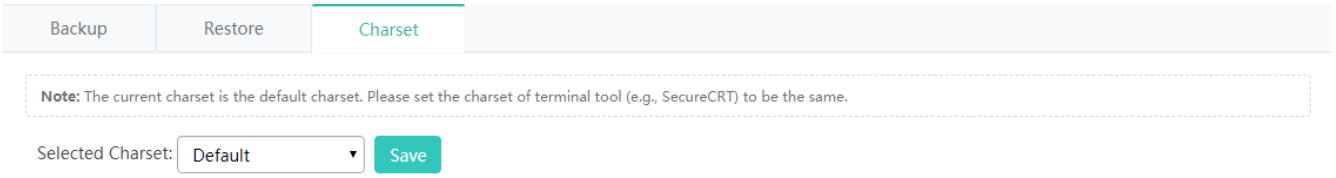
Restore

Click **Display Current Settings** to display the current configurations.



Clear the configurations to restore the system to the initial state. Use the IP address in the factory settings to access the Web-based management system.

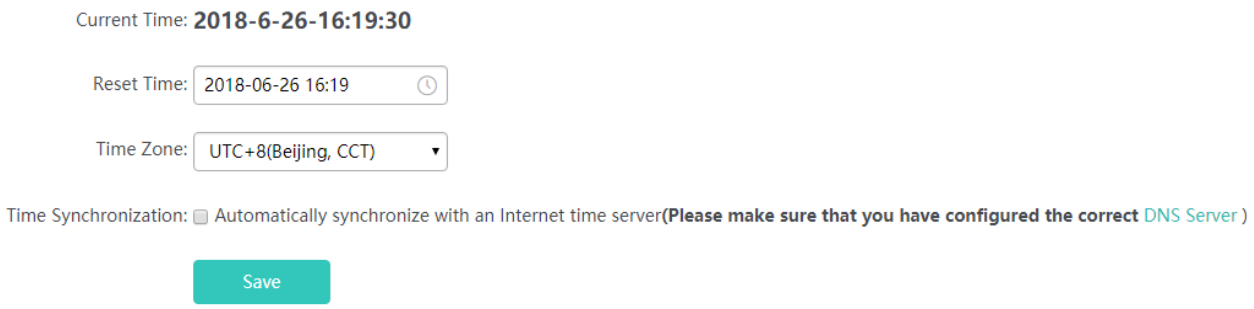
Charset



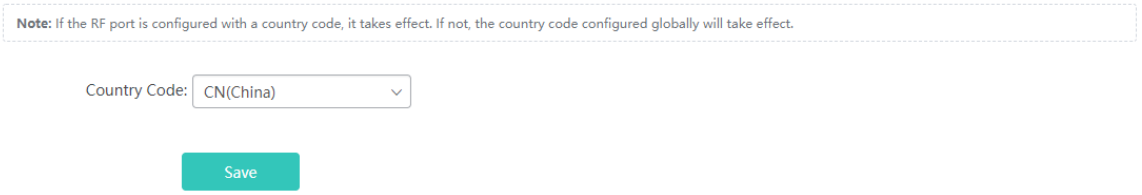
Selected Charset is set to **GBK**, **UTF-8** or **Default**. It is recommended to set it to **UTF-8** for the Web-based management system and keep consistent with the system charset on SecureCRT or other terminal tools. Otherwise, garble may occur.

1.3.5.1.6 System Time

Set the system time of the time zone where the device is located, so that the device information is clear.



1.3.5.1.7 Country Code Configuration

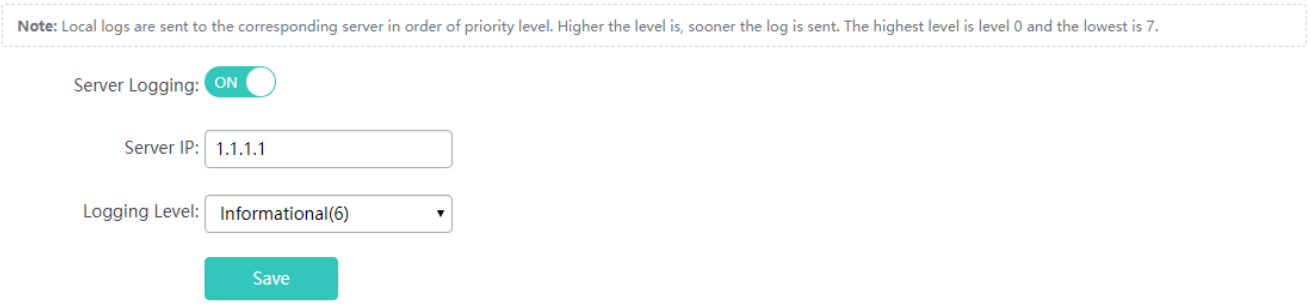


Configure the country code for the device. The country code is global. If another country code is set for an online AP, the global country code does not take effect.

1.3.5.1.8 Log Server

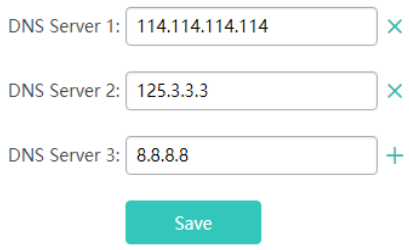
The device sends local logs to the server for storage. History logs are stored for ease of query.

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



1.3.5.1.9 DNS

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



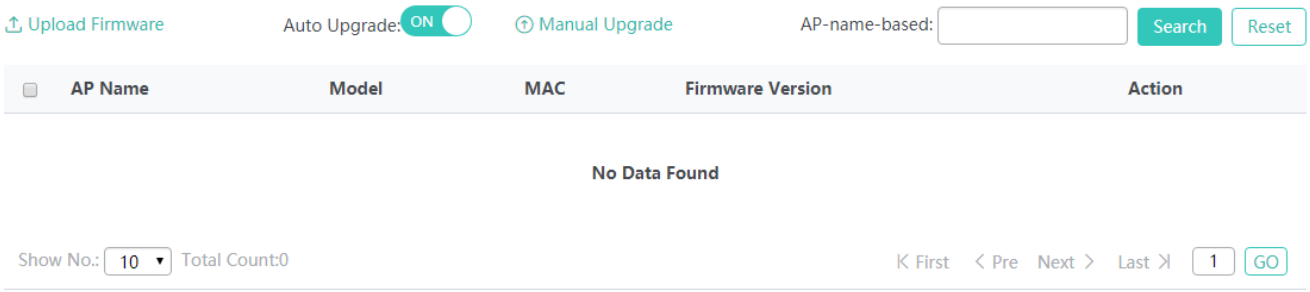
1.3.5.2 AP Management

1.3.5.2.1 AP Upgrade

An AC manages APs. Multiple APs can be upgraded simultaneously through the Web page, which is convenient.

Click **Upload Firmware** to upload the firmware version.

Auto Upgrade can be set to **ON**/**OFF** to enable/disable the automatic upgrade of APs.



- Search

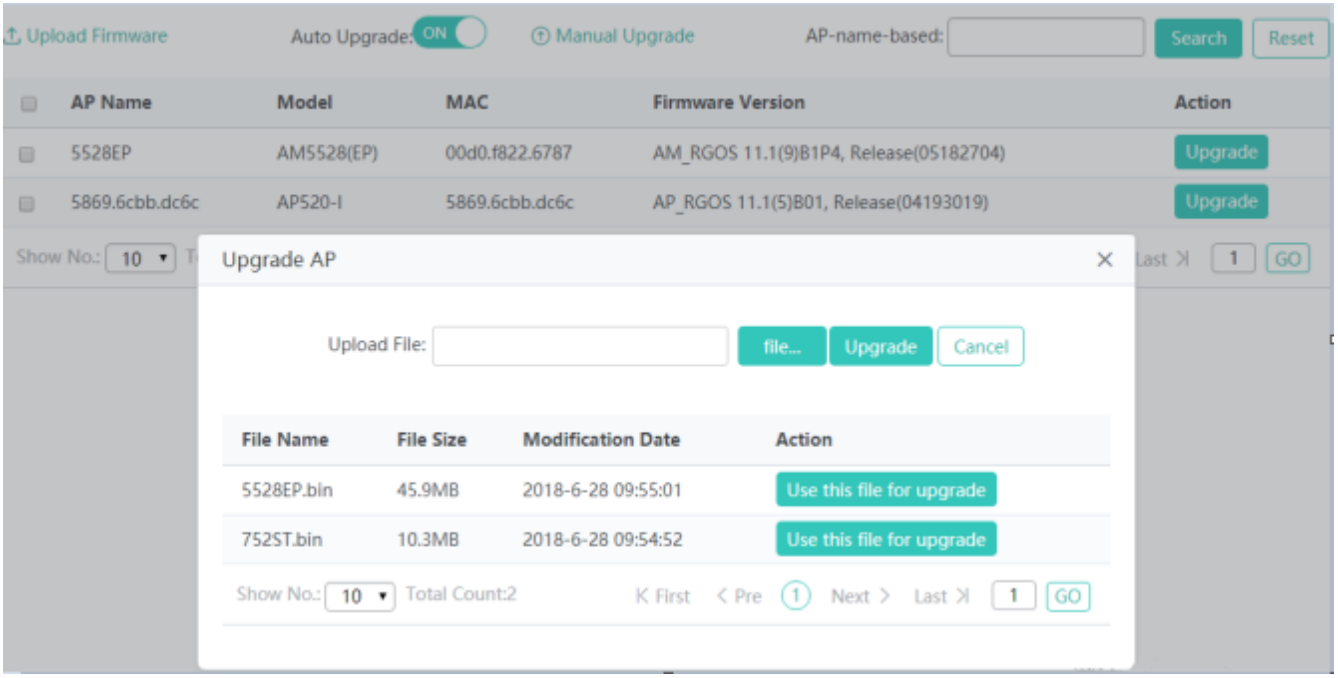
Enter a search condition in the search box and click **Search** to search for items meeting the search condition.

- Reset

Click **Reset** to reset the current list.

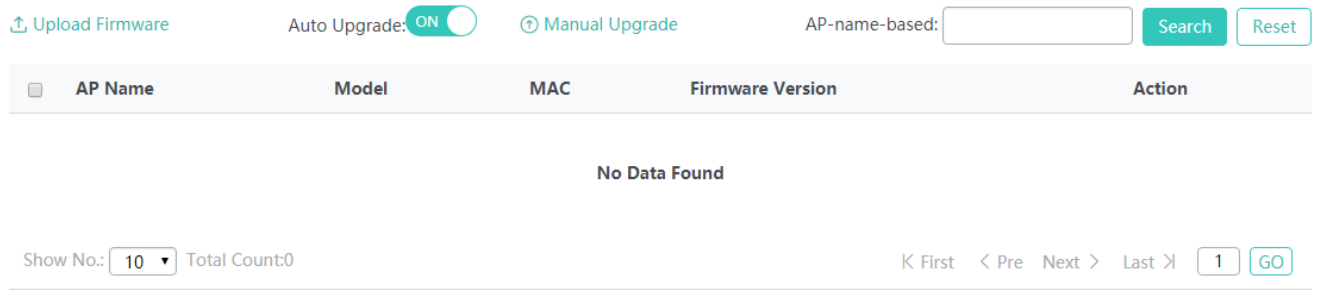
- Upgrading a single AP

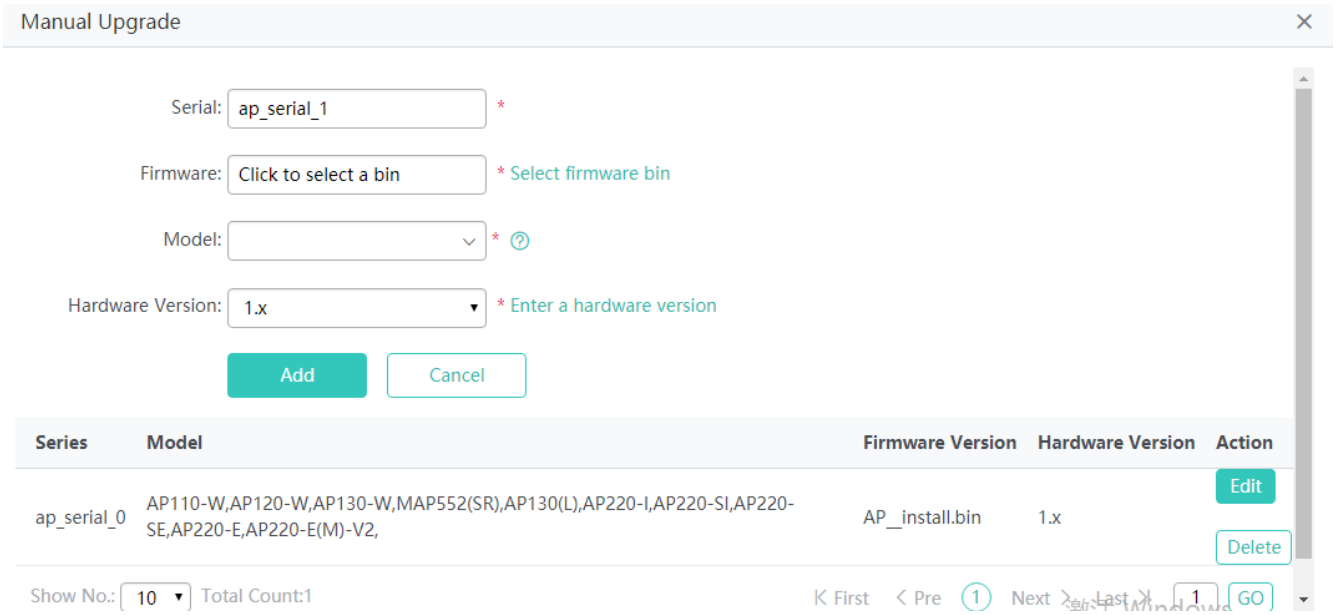
Select an AP in the AP list and click **Upgrade**. In the displayed **Upgrade AP** window, select or upload the .bin file for upgrade.



- Upgrading an AP manually

Click **Manual Upgrade**. In the **Manual Upgrade** window, upgrade the AP manually.

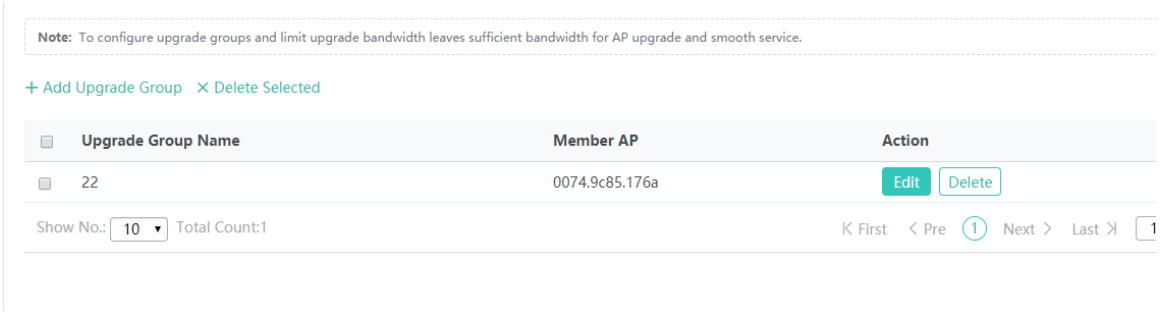




1.3.5.2.2 Bandwidth Control of an AP Upgrade Group

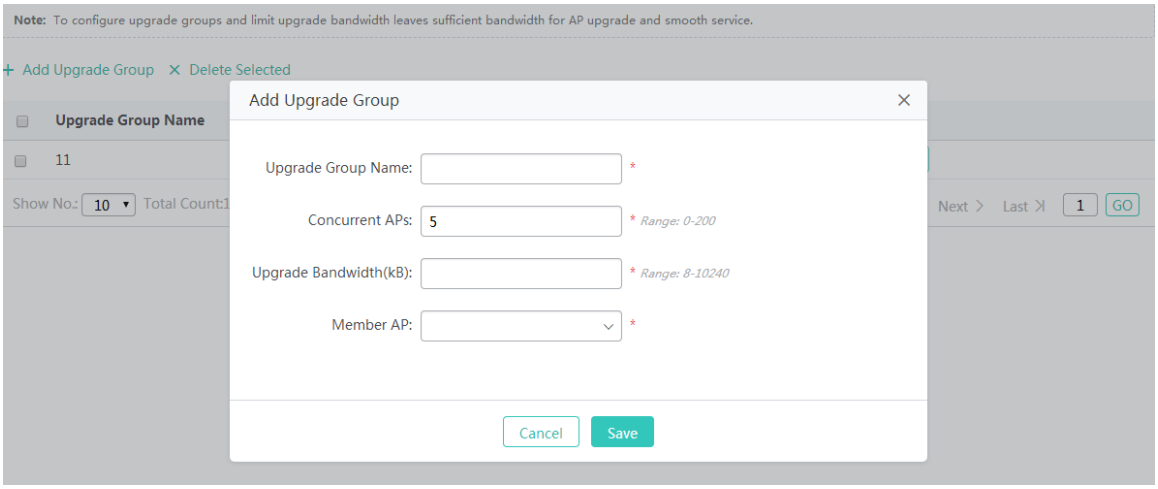
Configure an upgrade group and restrict the upgrade bandwidth to reserve sufficient bandwidth during AP upgrade, so that network performance is not greatly affected by the AP upgrade.

Your AC may not support this function and the actual menu items shall prevail.



- Adding an upgrade group

Click **Add Upgrade Group**. In the displayed **Add Upgrade Group** window, set parameters and click **Save**. A setting success prompt is displayed and the new upgrade group is displayed in the upgrade group list.



Upgrade Group Name

Indicates the name of an AP upgrade group.

Concurrent APs

Indicates the number of APs that can be upgraded simultaneously.

Upgrade Bandwidth (kB)

Indicates the bandwidth used for the AP upgrade.

Member AP

Indicates member APs in the upgrade group.

- Batch deleting upgrade groups

Select upgrade groups to be deleted from the list, and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

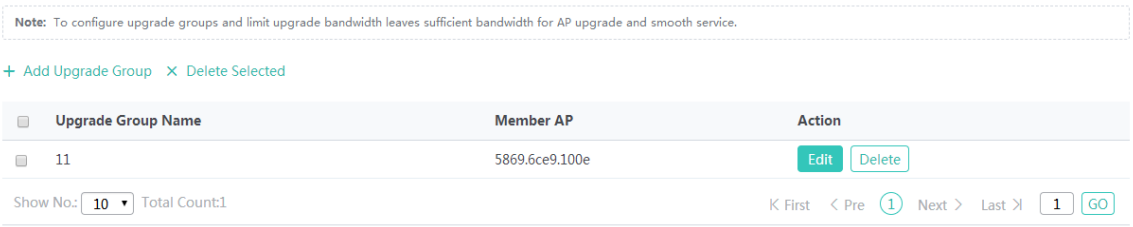
- Editing an upgrade group

Click **Edit** for an upgrade group in the list. The displayed window shows information about the upgrade group. Edit the information and click **Save**. A setting success prompt is displayed, indicating that the operation is complete.

Parameters for editing an upgrade group are the same as those for adding an upgrade group and are not described again.

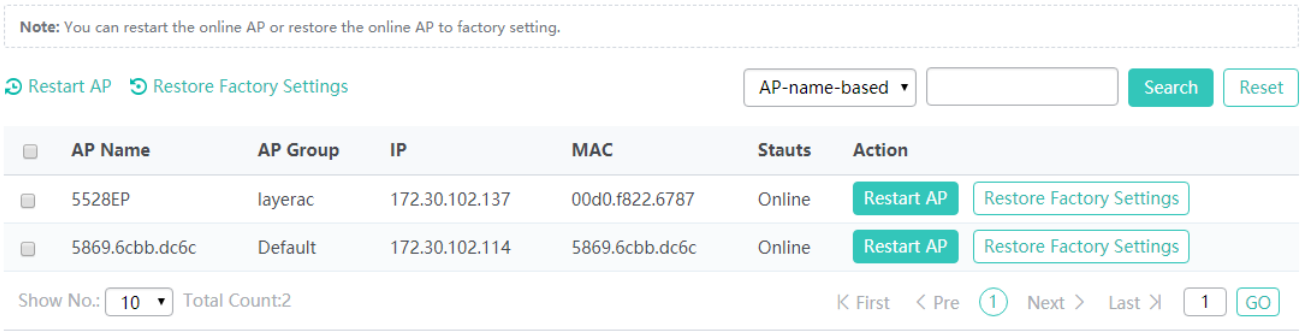
- Deleting an upgrade group

Click **Delete** for an upgrade group in the list. In the displayed confirmation window, click **OK** to complete the delete operation.



1.3.5.2.3 AP Restart/Factory Settings Restoration

This function is used to restart an online AP and restore factory settings.



- Restarting an AP

Click **Restart AP** for an AP in the AP list to restart the AP.

- Restoring factory settings

Select an AP in the AP list and click **Restore Factory Settings** to restore the factory settings of the AP.

- Batch restarting APs

Select multiple records in the AP list and click **Restart AP** to batch restart APs.

- Batch restoring factory settings

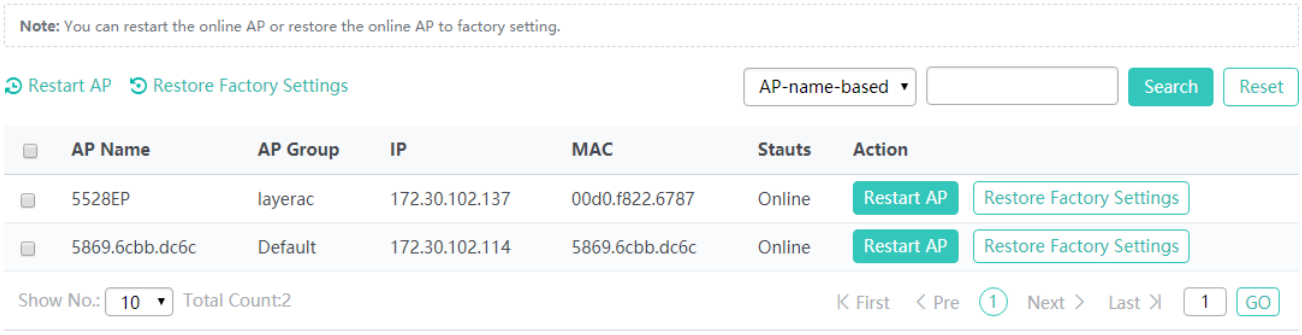
Select multiple records in the AP list and click **Restore Factory Settings** to batch restore factory settings of APs.

- Search

Select **AP-name-based** or other items from the search drop-down list, enter a search condition in the search box, and click **Search** to search for required records.

- Reset

Click **Reset** to reset the search condition.



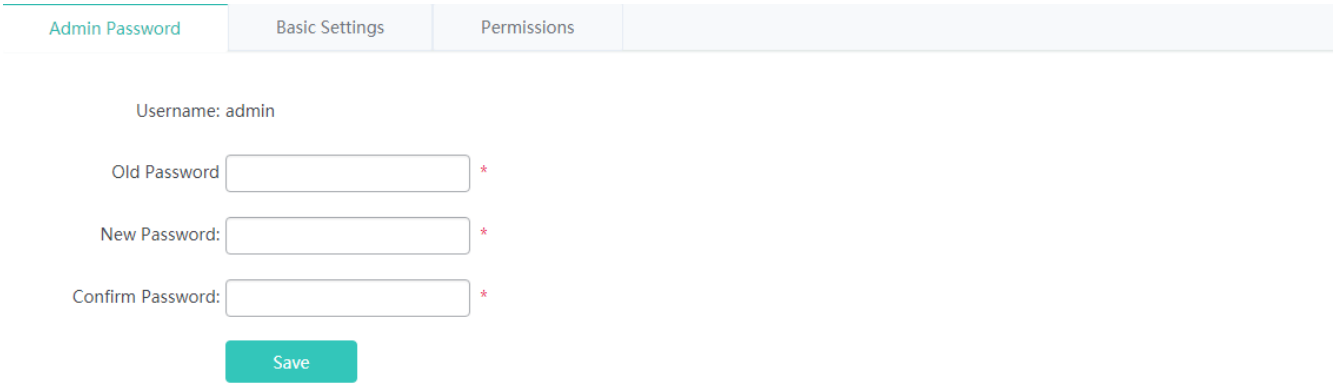
1.3.5.3 Network Management Configuration

1.3.5.3.1 Web-based Configuration 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**.

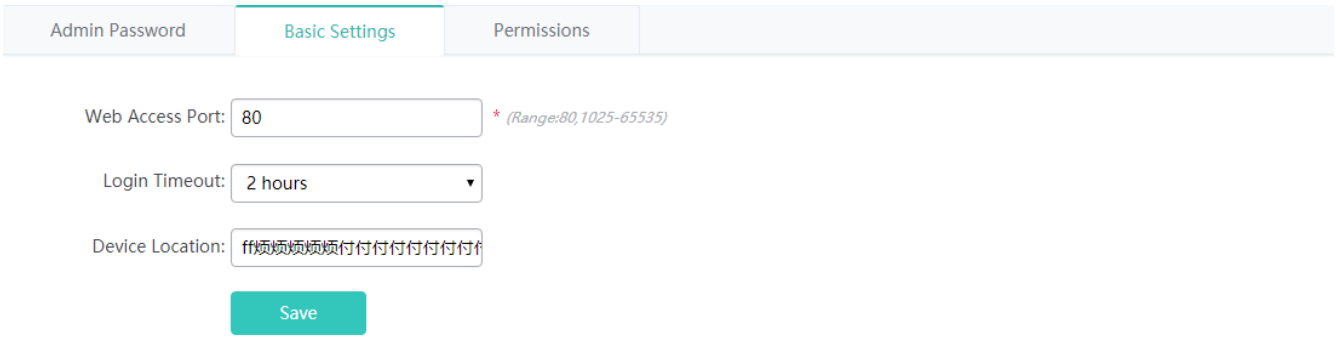


Basic Settings

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.

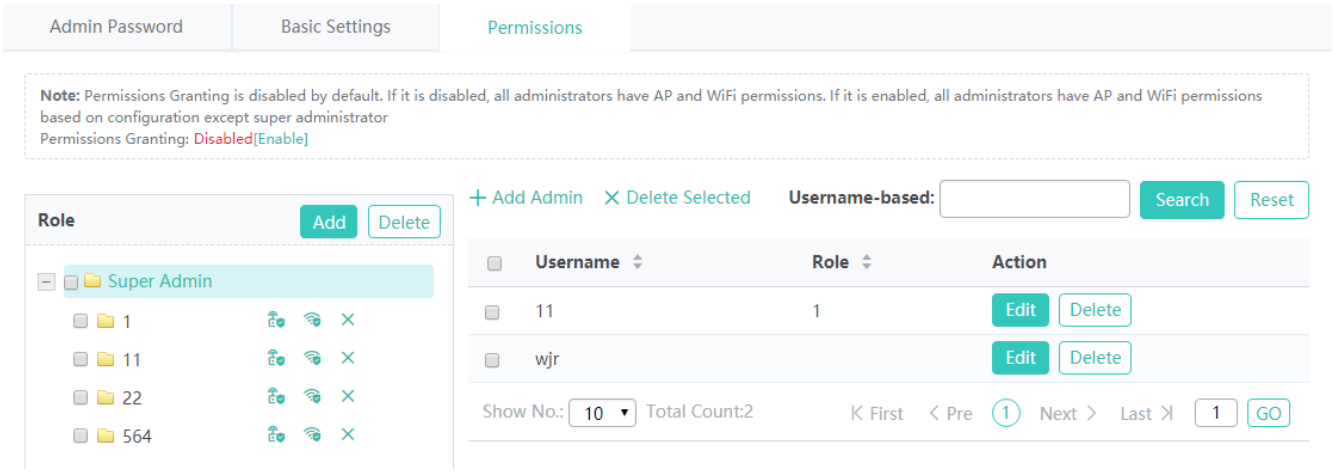
Device Location: Indicates the device location. Setting this parameter facilitates management.



Permissions (permissions granting)

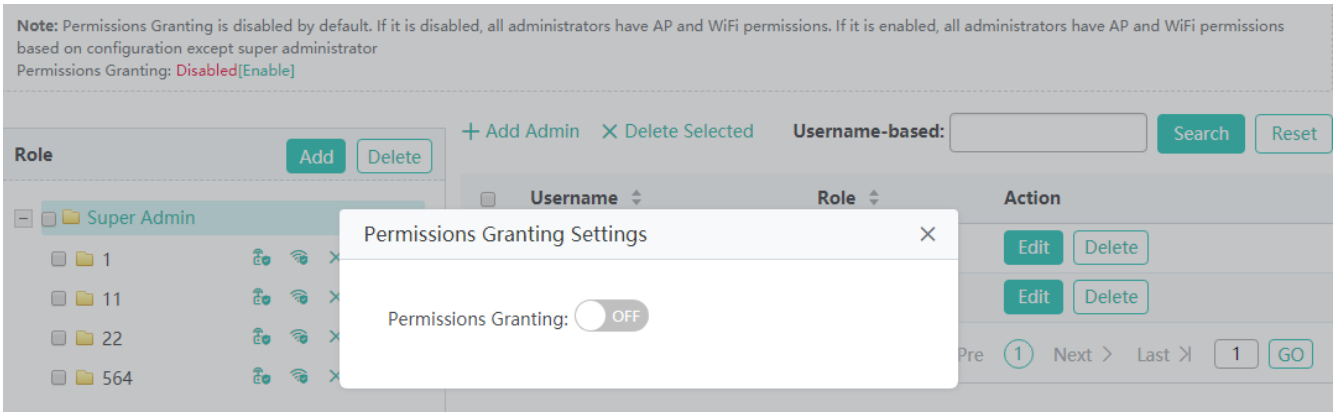
Users in a system can be grouped, and permissions for WLANs, APs, and AP groups can be granted to different groups. In this way, users in different role groups have different permissions for WLANs, APs, and AP groups.

Note: A page shown in the figure below is displayed if a product supports the permissions granting function.



- Enabling/Disabling permissions granting

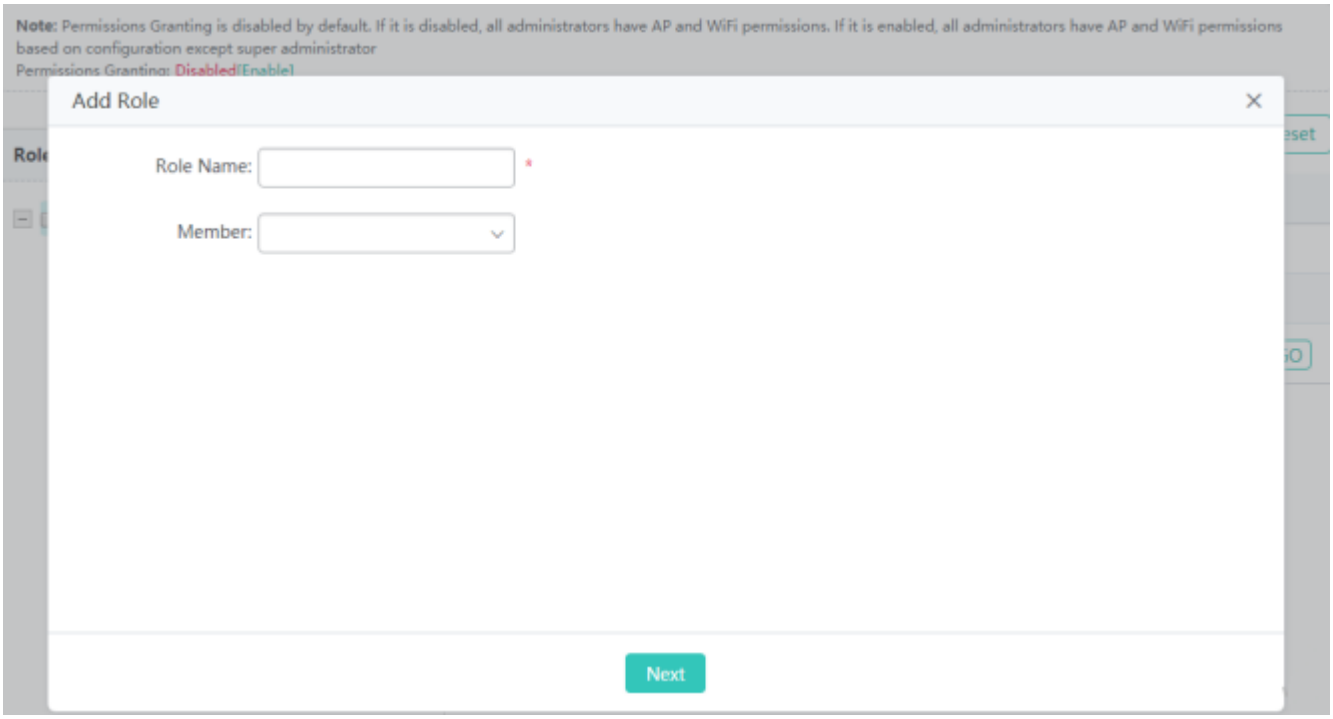
The permissions granting function takes effect only after being enabled.

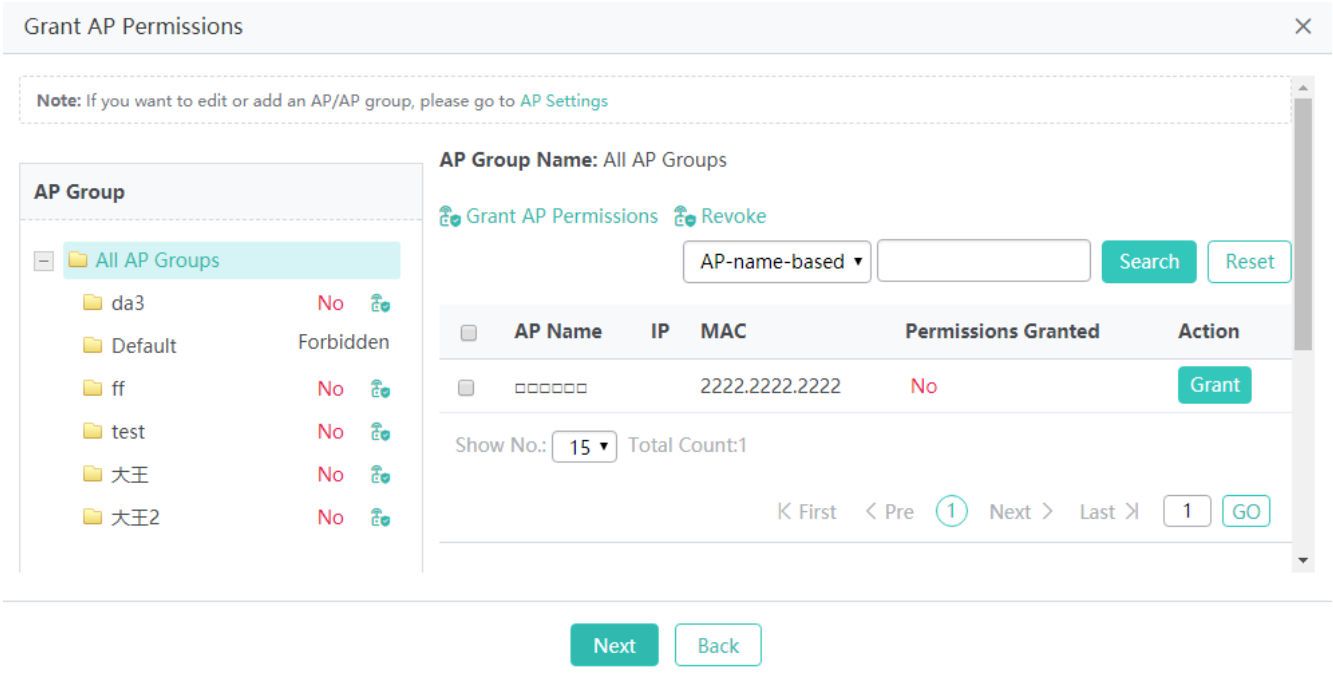


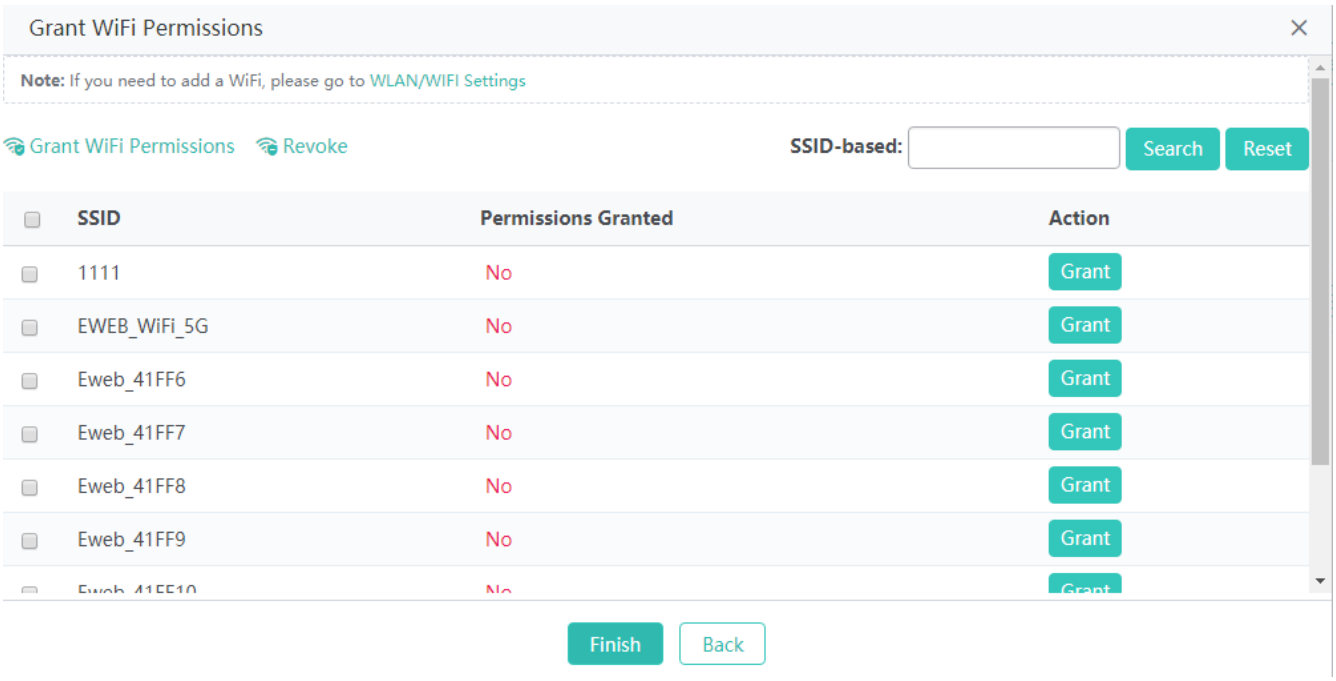
- Adding a role

A role can be added in three steps: adding a role, granting AP permissions, and granting WiFi permissions, to complete the role permission granting and role allocation at a time.

A common administrator of a role has all AP permissions and WiFi permissions of this role after login. Users without the AP permissions and WiFi permissions are not allowed to access the APs and WiFi networks.

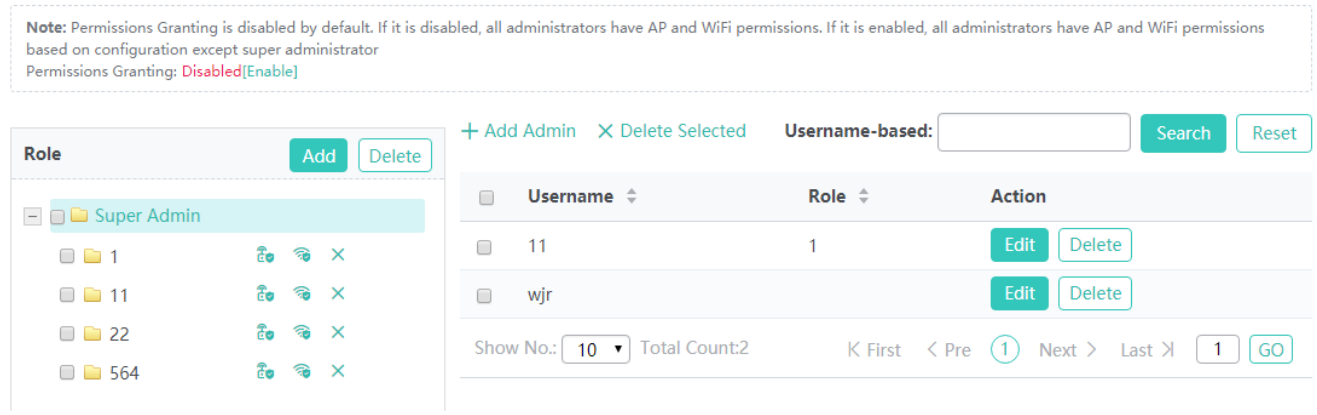

Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi permissions based on configuration except super administrator
Permissions Granting: Disabled(Enable)
Add Role
Role Name:
Member:
Next


Grant AP Permissions
Note: If you want to edit or add an AP/AP group, please go to AP Settings
AP Group
All AP Groups
da3 No
Default Forbidden
ff No
test No
大王 No
大王2 No
AP Group Name: All AP Groups
Grant AP Permissions
Revoke
AP-name-based
Search
Reset
AP Name
IP
MAC
Permissions Granted
Action
2222.2222.2222
No
Grant
Show No.: 15
Total Count:1
First
Pre
1
Next
Last
1
GO
Next
Back



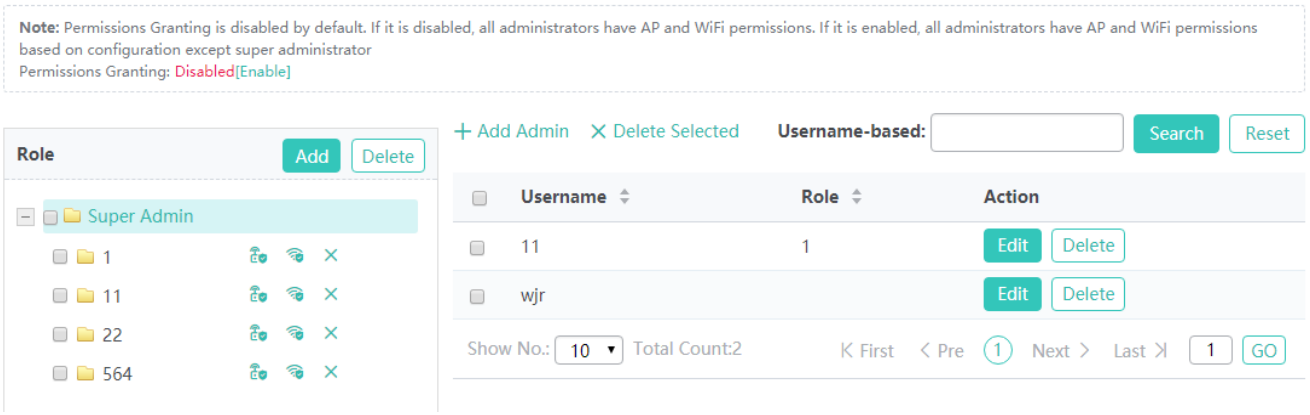
- Deleting a role

Click **Delete** above the role list or click **Delete** behind a role in the role list. In the displayed confirmation window, click **OK** to delete the role.



- Granting AP permissions to a role

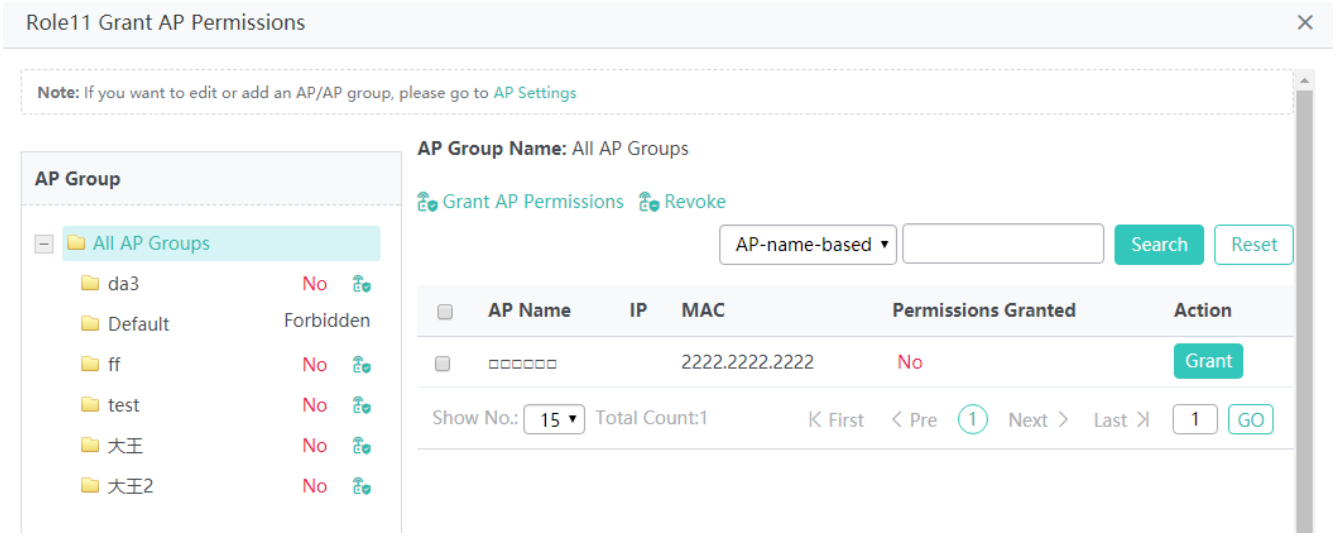
Click the AP permission granting icon for a role in the role list. The **Grant AP Permissions** window is displayed.



In the AP group list, select a group and click the authorization icon to grant permissions to the AP group or click the revocation icon to revoke permissions of the AP group.

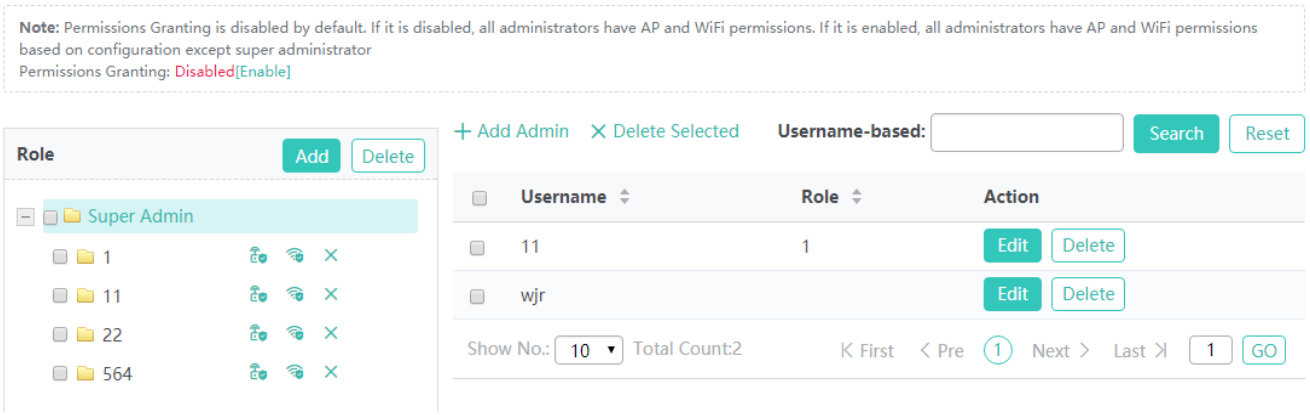
In the AP list of an AP group on the right side, select multiple APs and click **Grant AP Permissions** to batch grant permissions to APs or click **Revoke** to batch revoke permissions of the APs.

In the AP list of an AP group on the right side, click **Grant** for an AP to grant the operation permissions over this AP to the role, or click **Revoke** to revoke operation permissions over this AP from this role.



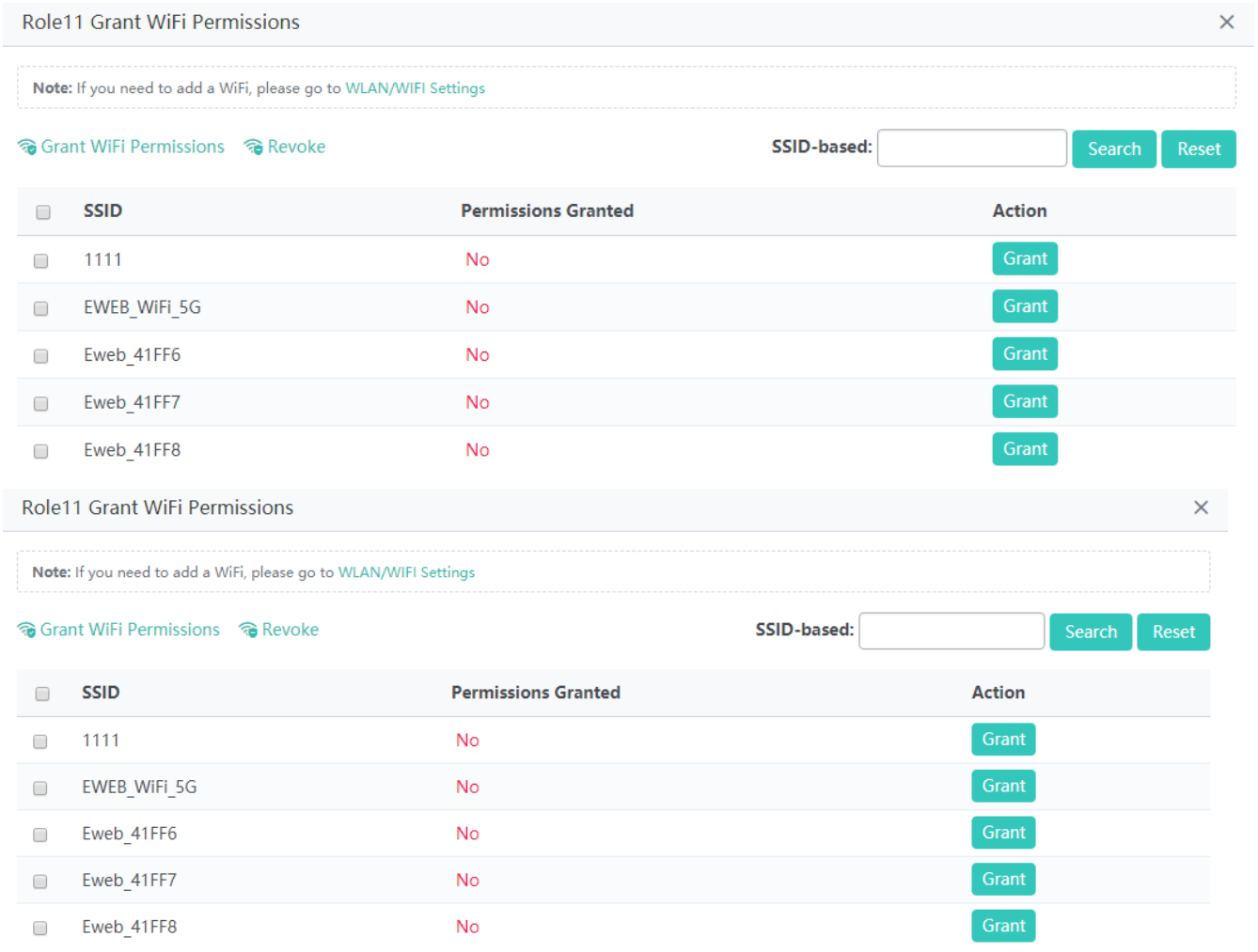
- Granting WiFi permissions to a role

In the role list on the left side, click the WiFi permission granting icon for a role. The **Grant WiFi Permissions** window is displayed.



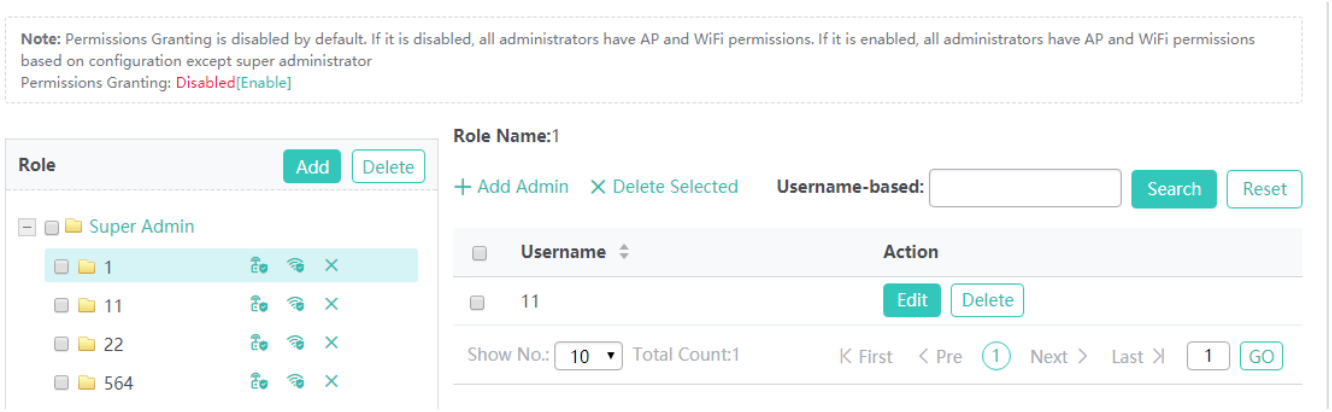
In the **Grant WiFi Permissions** window, select multiple WiFi networks and click **Grant WiFi Permissions** to batch grant WiFi permissions, or click **Revoke** to batch revoke WiFi permissions.

Click **Grant** for an SSID in the list to grant the WiFi operation permission to this role, or click **Revoke** to revoke the WiFi operation permission from the
role.



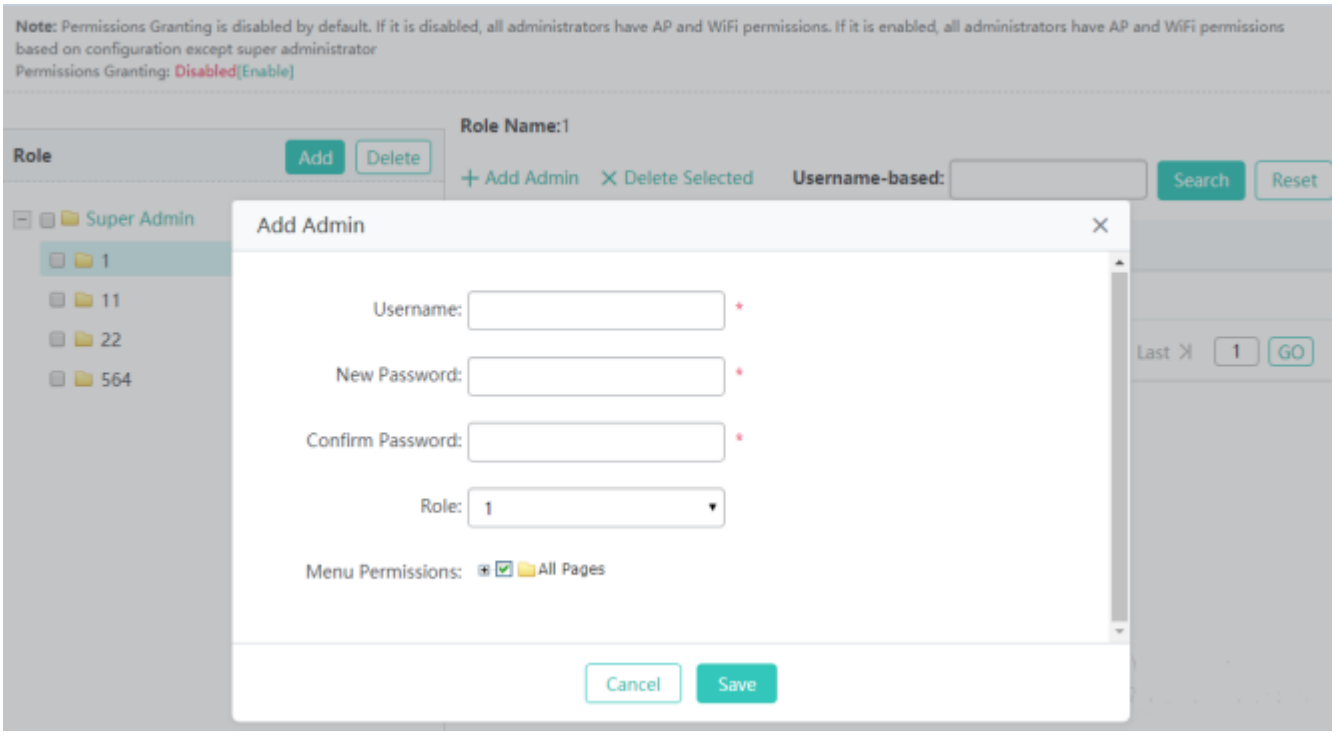
- Displaying administrators of a role

In the role list on the left side, select a role. The role and administrator members are updated on the right side.

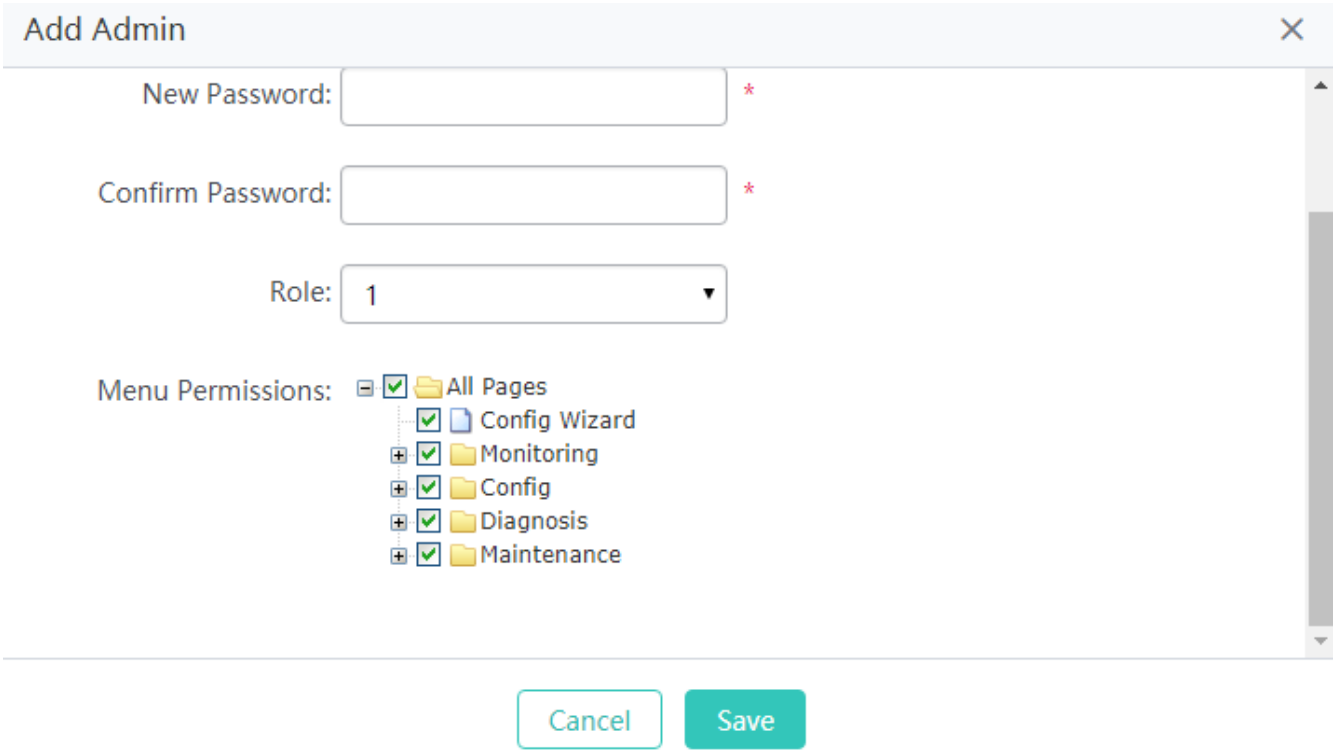


- Adding an administrator

Click **Add Admin**. In the displayed **Add Admin** window, set parameters and click **Save**. A setting success prompt is displayed and the new administrator is displayed in the administrator list.



Note: After the permissions granting function is configured, administrators have default permissions, as shown in the figure below.



Username

Indicates the administrator account.

New Password

Indicates the password of the administrator.

Confirm Password

Indicates the password for confirmation.

Menu Permissions

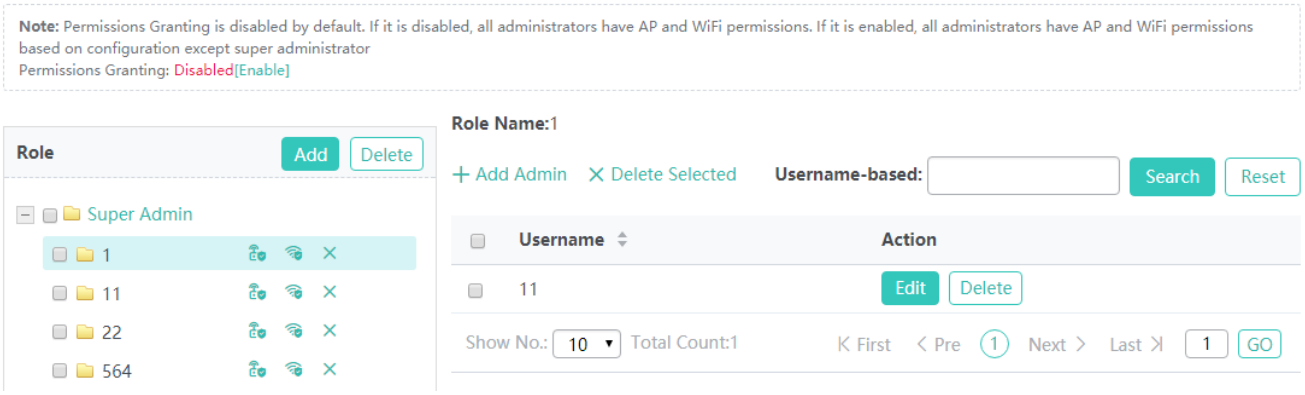
Indicates the pages allocated to the administrator for management.

Role

Indicates the management group role to which the administrator belongs.

- Deleting an administrator

Click **Delete** for an administrator in the list. In the displayed confirmation window, click **OK** to complete the delete operation.



- Batch deleting administrators

Select multiple records and click **Delete Selected**. In the displayed confirmation window, click **OK** to complete the delete operation.

- Editing an administrator

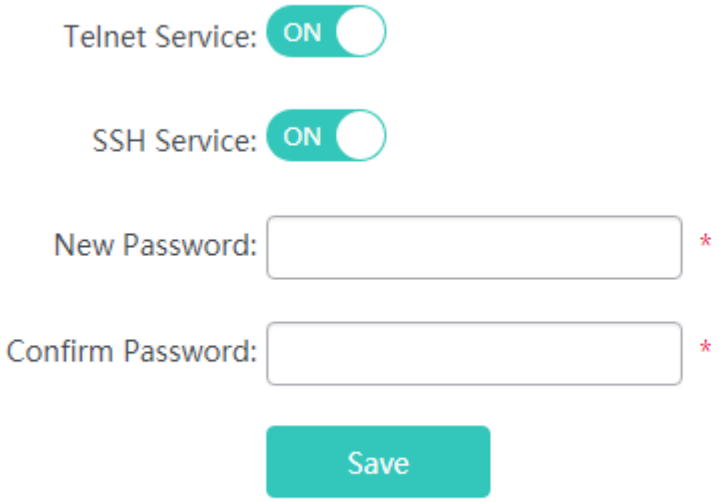
Click **Edit** for an administrator in the list. The displayed window shows information about the administrator. Edit the information and click **Save**. A setting success prompt is displayed and the administrator is displayed in the administrator list.

1.3.5.3.2 Telnet

To enhance the system security and information interaction security, you need to configure the Telnet function.

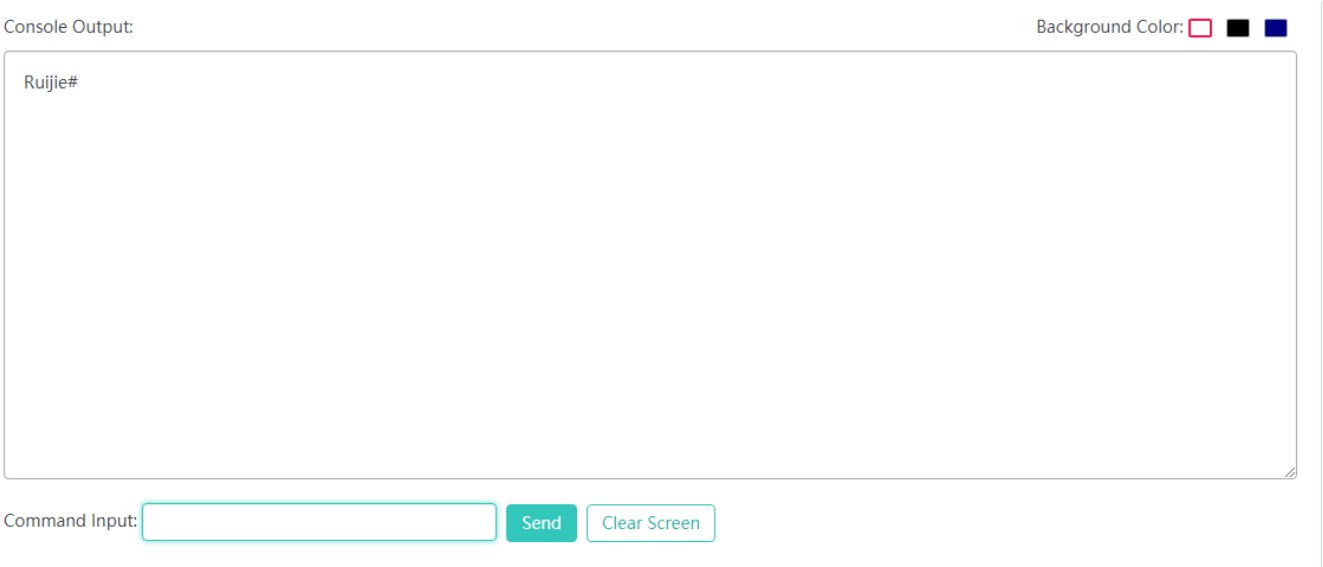
New Password: Indicates a new password.

Confirm Password: Indicates the password for confirmation.



1.3.5.3.3 Web Console

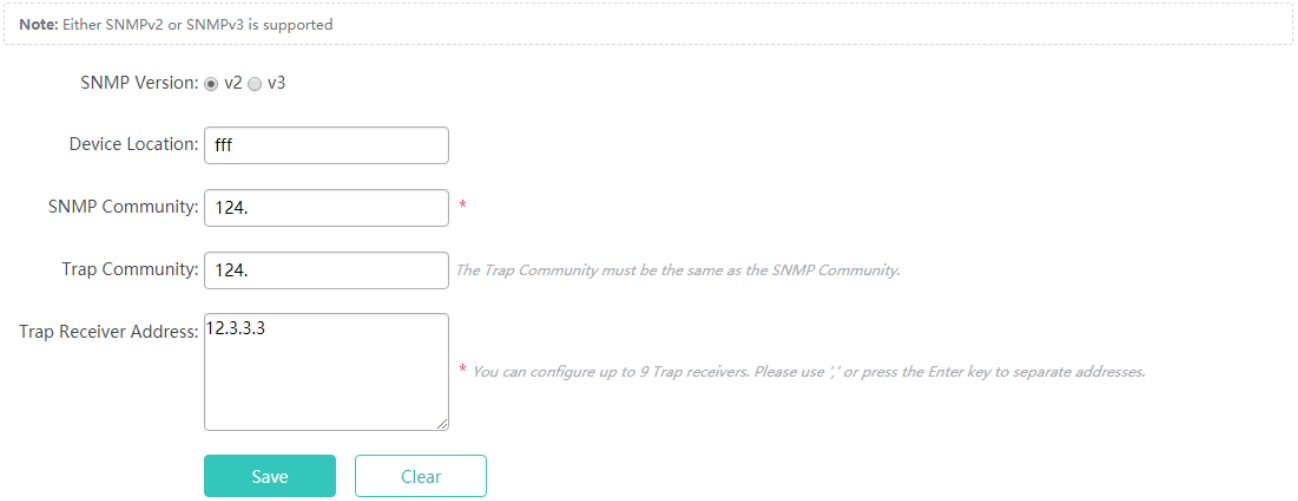
The Web console function is similar to the Telnet function and you can configure any command on the console. However, the Web console function does not support commands in shell mode, telnetting to APs, or batch refresh of commands.



1.3.5.3.4 SNMP

The Simple Network Management Protocol (SNMP) provides a method for collecting network management information from devices on the network. It can be used to manage a considerable quantity of network devices.

SNMP Version: Indicates the SNMP version. The fields to be configured vary with the SNMP version.



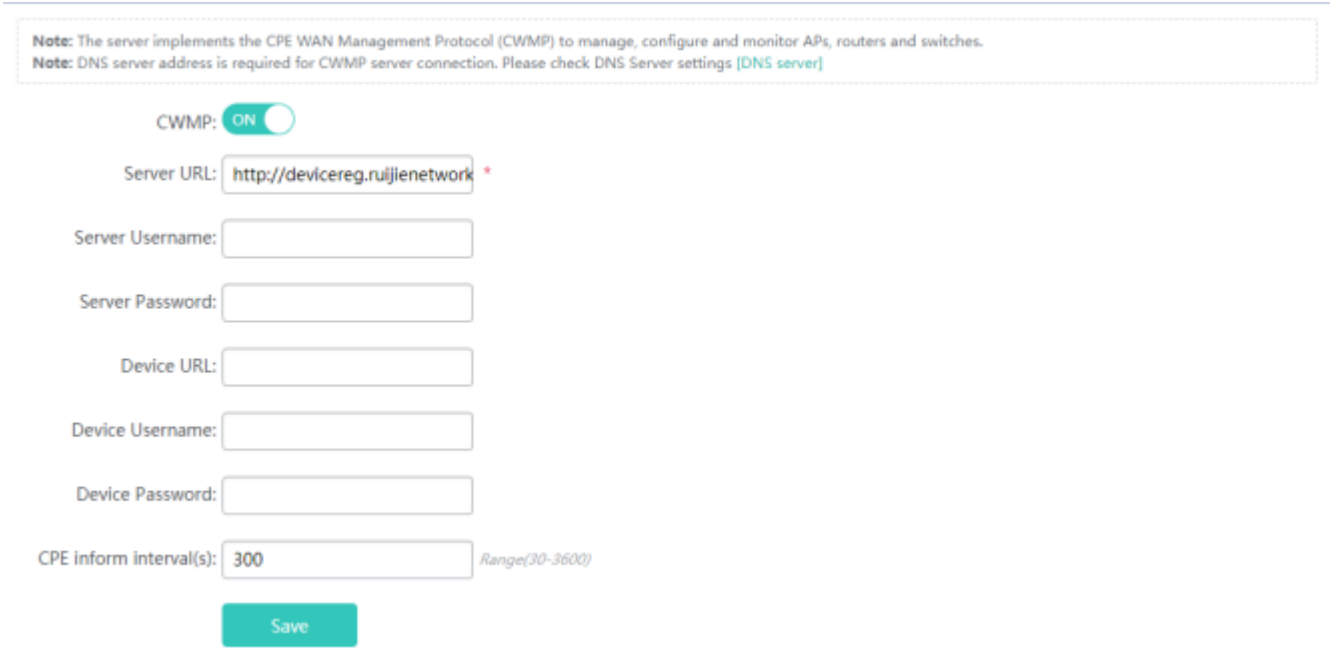
1.3.5.3.5 CWMP/MACC

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**.



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.

1.3.6 Other Functions

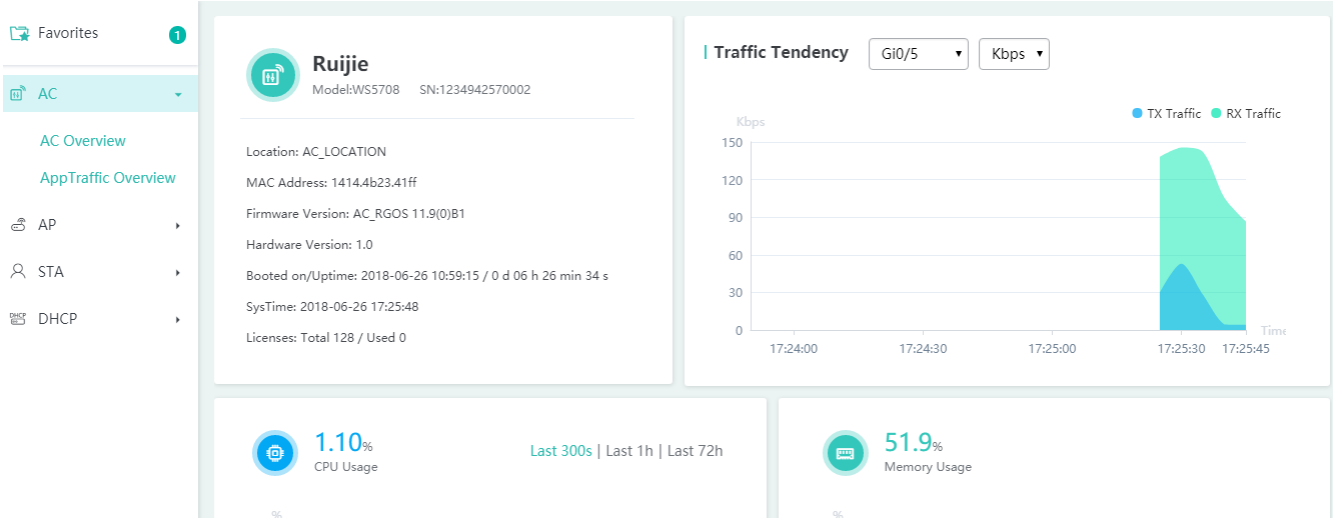
1.3.6.1 Favorites

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.

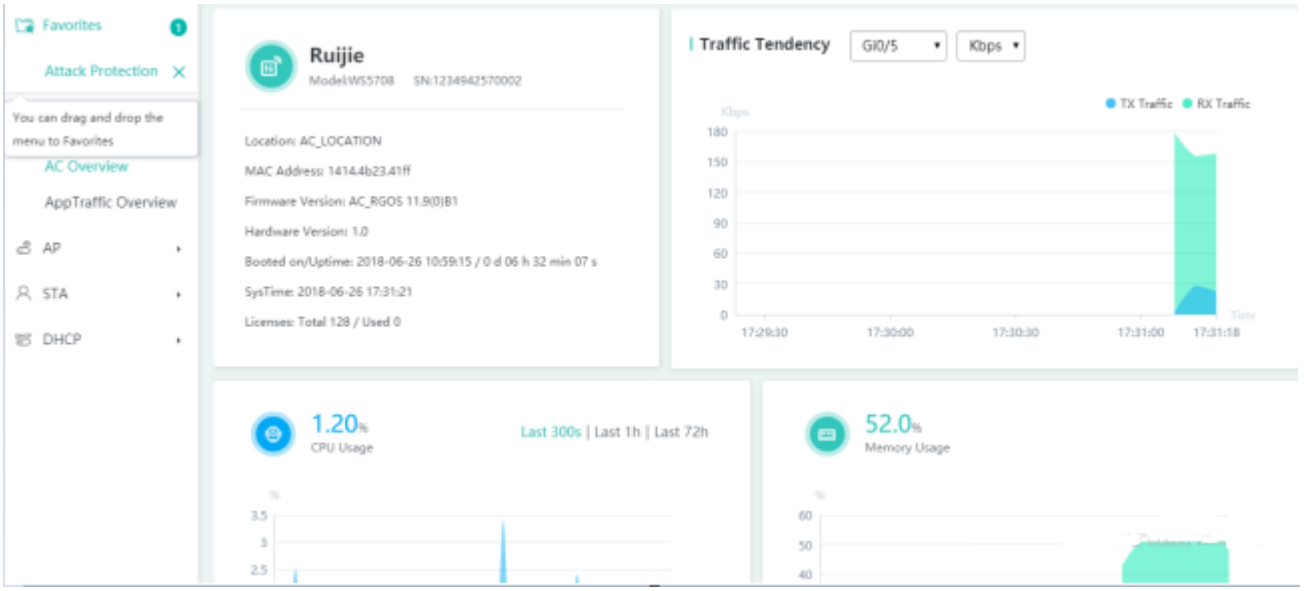
- Adding to favorites

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



- Canceling favorites

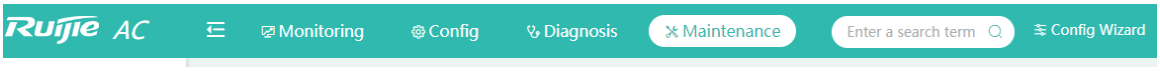
Click **Favorites** to display the favorites list. Select a menu item from the list and click the deletion icon. Confirm the delete operation to delete the menu item from the favorites.



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.

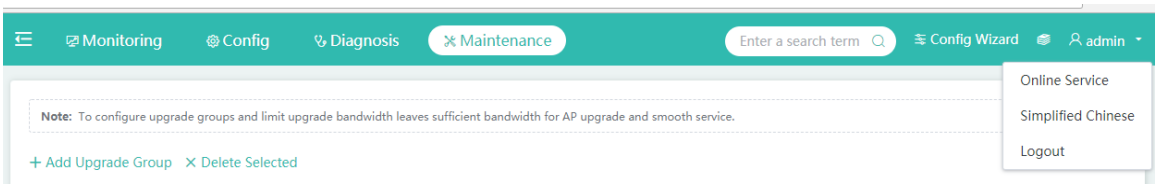
Enter a search condition in the search box on the home page. A list of records meeting the search condition is rapidly displayed. Click a function to redirect to the function page.



1.3.6.3 More Functions of the System

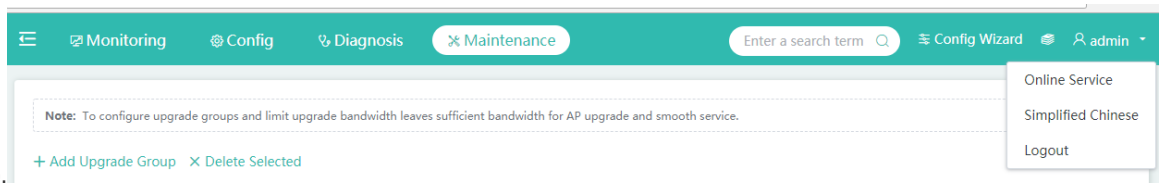
- Displaying the current account

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.



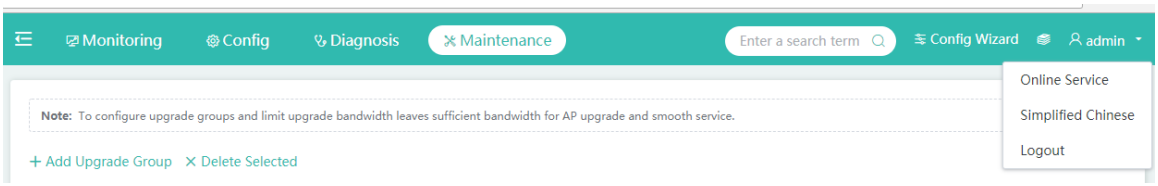
- Online Service

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

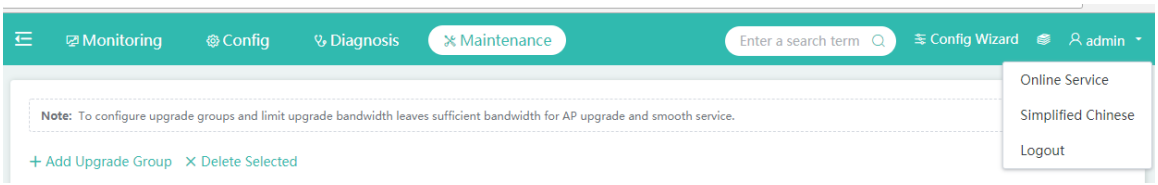
Click the current account icon in the upper right corner. A function drop-down list is displayed. The second item is used for language switching. If the system is in Chinese, click **English** to switch to the English edition; if the system is in English, click **Simplified Chinese** to switch to the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

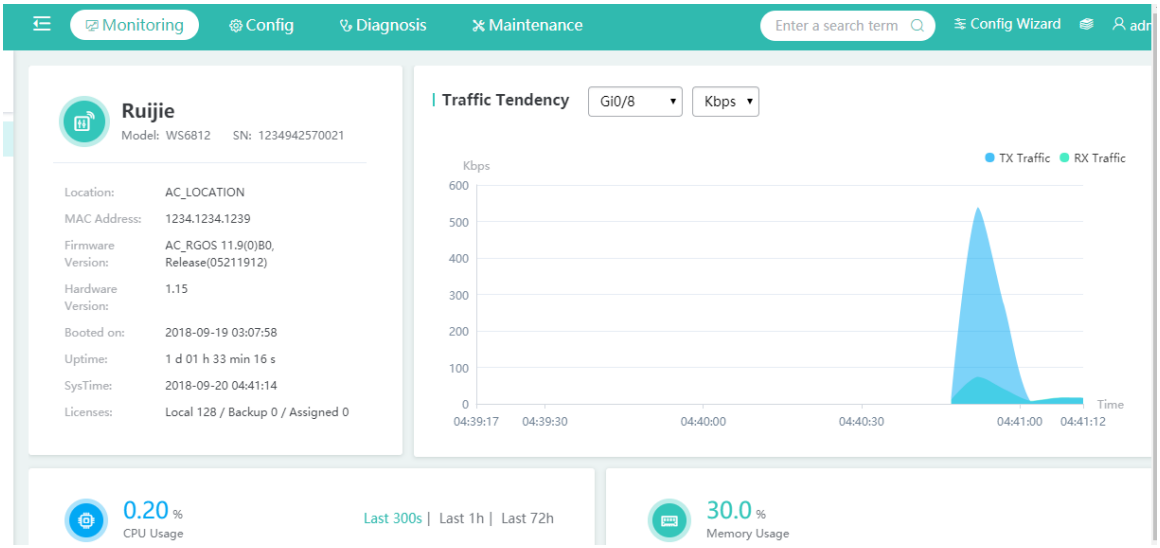
- Exiting the system

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.



1.3.6.4 Help Information

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



1.4 Configuring the Web Server

The Web service is enabled on an AC by default and the default IP address of the Web service is 192.168.110.1. The following describes how to enable the Web service on the CLI.

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

Configuration Steps

Enabling the Web Service

- Mandatory.
- Configure the Web service on an AC.

Configuring an IP Address

- Optional.

Configuring the Username and Password for Logging In to the Web-based Management System

- Optional.
- When the Web service is enabled, the administrator account/password (**admin**/**admin**) and guest account/password (**guest**/**guest**) are created by default. Both the accounts and passwords can be changed. Users can also create other Web-based management accounts.

Verification

Log in to the Web-based management system by using the configured IP address and Web-based management account and password to check whether the login is successful.

Related Commands

Enabling the Web Service

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

Configuring an IP Address

Command	**ip address** *ip-address ip-mask*
Parameter Description	*ip-address*: Indicates the IP address. *ip-mask*: Indicates the network mask.
Command Mode	Interface configuration mode

Configuring the Username and Password for Logging In to the Web-based Management System

Command	**webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-passw*
Parameter Description	*privilege-level*: Indicates the user binding permission level, which includes level 0, level 1, and level 2. A default super administrator account (**admin**) has level 0 permissions, a guest account (**guest**) has level 2 permissions, and other accounts created manually have level 1 permissions. *name*: Indicates the Web-based management account. *password*: Indicates the password of the Web-based management account. **0 | 7**: Indicates an encryption type of the password. **0** indicates no encryption, and **7** indicates simple encryption. The default value is **0**. *encrypted-password*: Indicates the password text.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Web Server

Configuration Steps	Enable the Web service. Configure the management IP address of the device. Set the default management VLAN to VLAN 1. Configure the IP address of VLAN 1 and ensure that users can ping the management IP address successfully from their PCs.

	Ruijie# configure terminal Ruijie(config)#enable service web-server Ruijie(config)# webmaster level 0 username test password test Ruijie(config)#interface vlan 1 Ruijie(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0 Ruijie(config)# end
Verification	Run the **show running-config** command to display related commands.
	Ruijie(config)#show running-config Building configuration... Current configuration : 6312 bytes ! hostname ruijie ! ! webmaster level 0 username test password test //Username and password for Web-based management authentication. The encrypted password is displayed. http update mode auto-detect ! ! interface VLAN 1 ip address 192.168.1.200 255.255.255.0 //Management IP address of the device no shutdown ! line con 0 line vty 0 4 login ! ! End

1.5 Example of Web-based Management Configuration

1.5.1 Deploying a Simple WLAN

Unpack the device and carry out initial deployment. Complete basic AC configuration and ensure that STAs can receive signals and obtain IP addresses.

1.5.1.1 Both the AP Address Pool and User Address Pool Are Configured on the Local Device

Example:

Configure the g0/1 interface as the uplink interface of the AC, set the management VLAN of the device to VLAN 1, management address to 192.168.23.157, gateway address to 192.168.23.1, and tunnel address to 192.168.23.157.

Configure the WiFi SSID Test_WiFi, and set the encryption mode to WPA/WPA2-PSK (universal edition) and password to 12345678.

Configure **Dual Radio Into One** for the Test_WiFi and set packet forwarding mode to centralized forwarding.

Add the IP address of the AP to VLAN 2, and set the address pool to the 192.168.2.0 network segment and the gateway to 192.168.2.1.

Add the IP address of the STA to VLAN 3, and set the address pool to the 192.168.3.0 network segment and the gateway to 192.168.3.1.

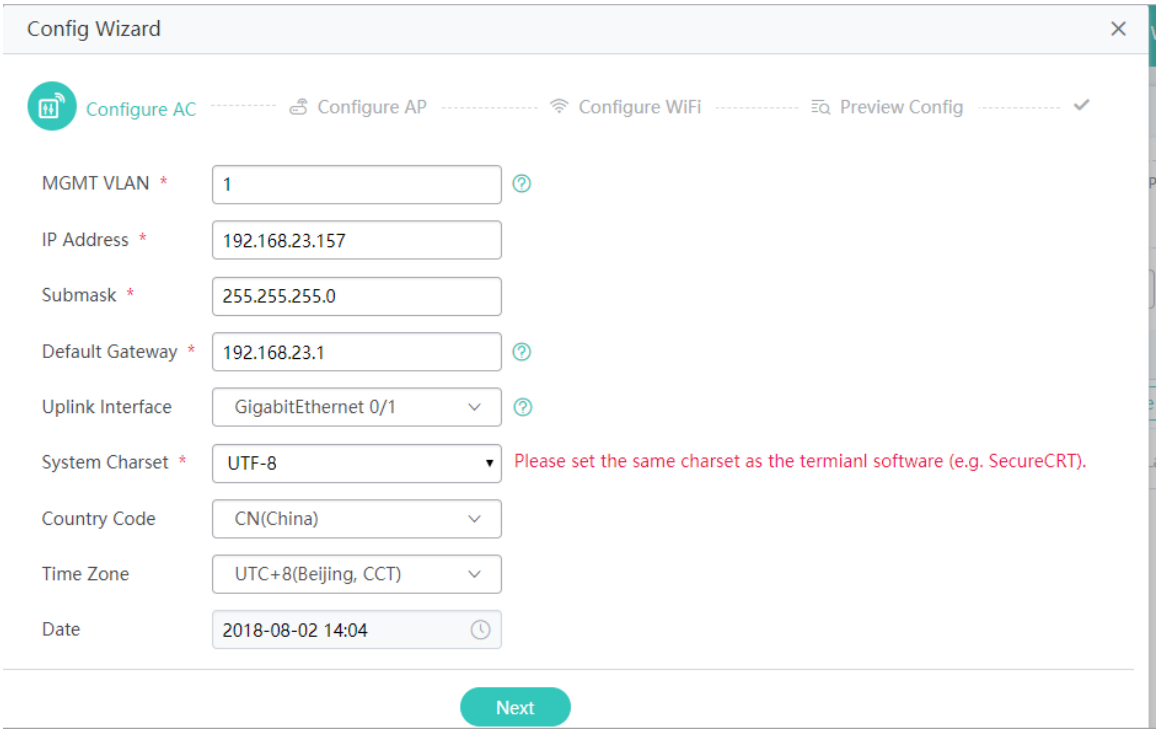
Configuration Steps

Configuring the AC

Complete basic configurations of the AC based on the scenario.

Configure the g0/1 interface as the uplink interface of the AC, set the management VLAN of the device to VLAN 1, management address to 192.168.23.157, gateway address to 192.168.23.1, and tunnel address to 192.168.23.157.

Set configuration items on the **Configure AC** page.

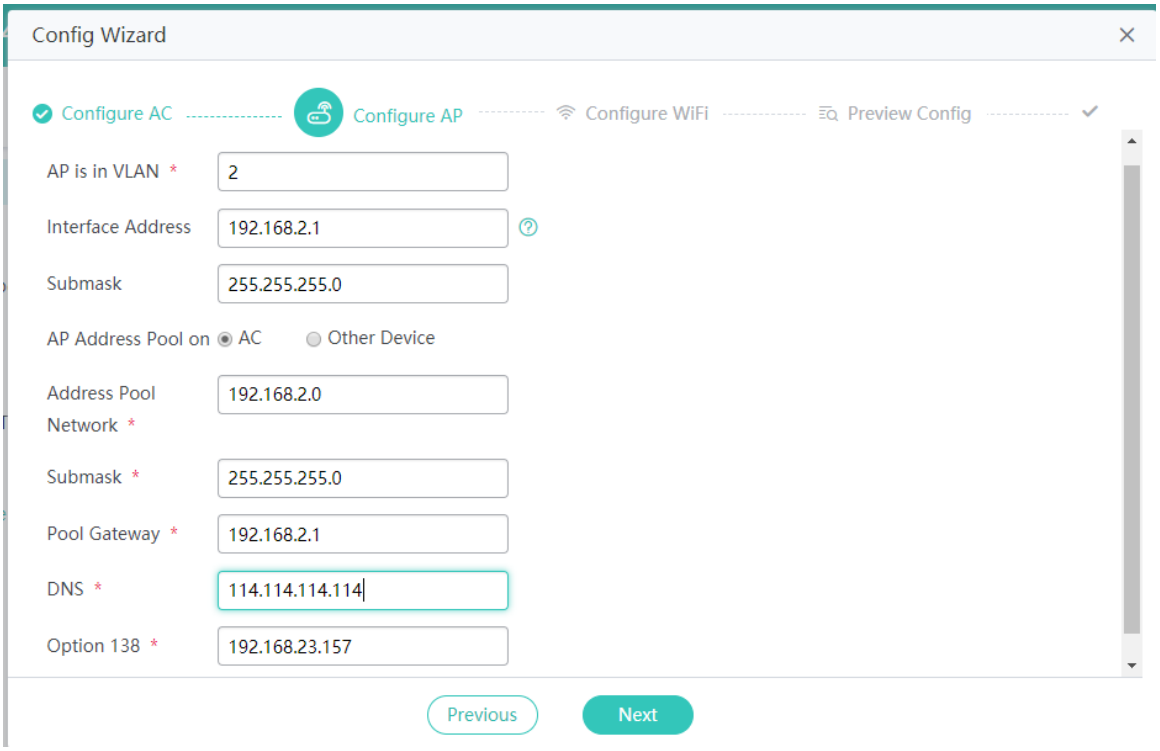


Note: The default tunnel IP address in the configuration wizard is the same as the management IP address. Therefore, the default tunnel IP address does not need to be entered.

The system charset is UTF-8 code by default. If a user needs to view or configure the system by using other terminal tools, it is recommended to set System Charset to UTF-8. Otherwise, code mixing may be incurred, resulting in the page configuration failure or garble.

Configuring the AP

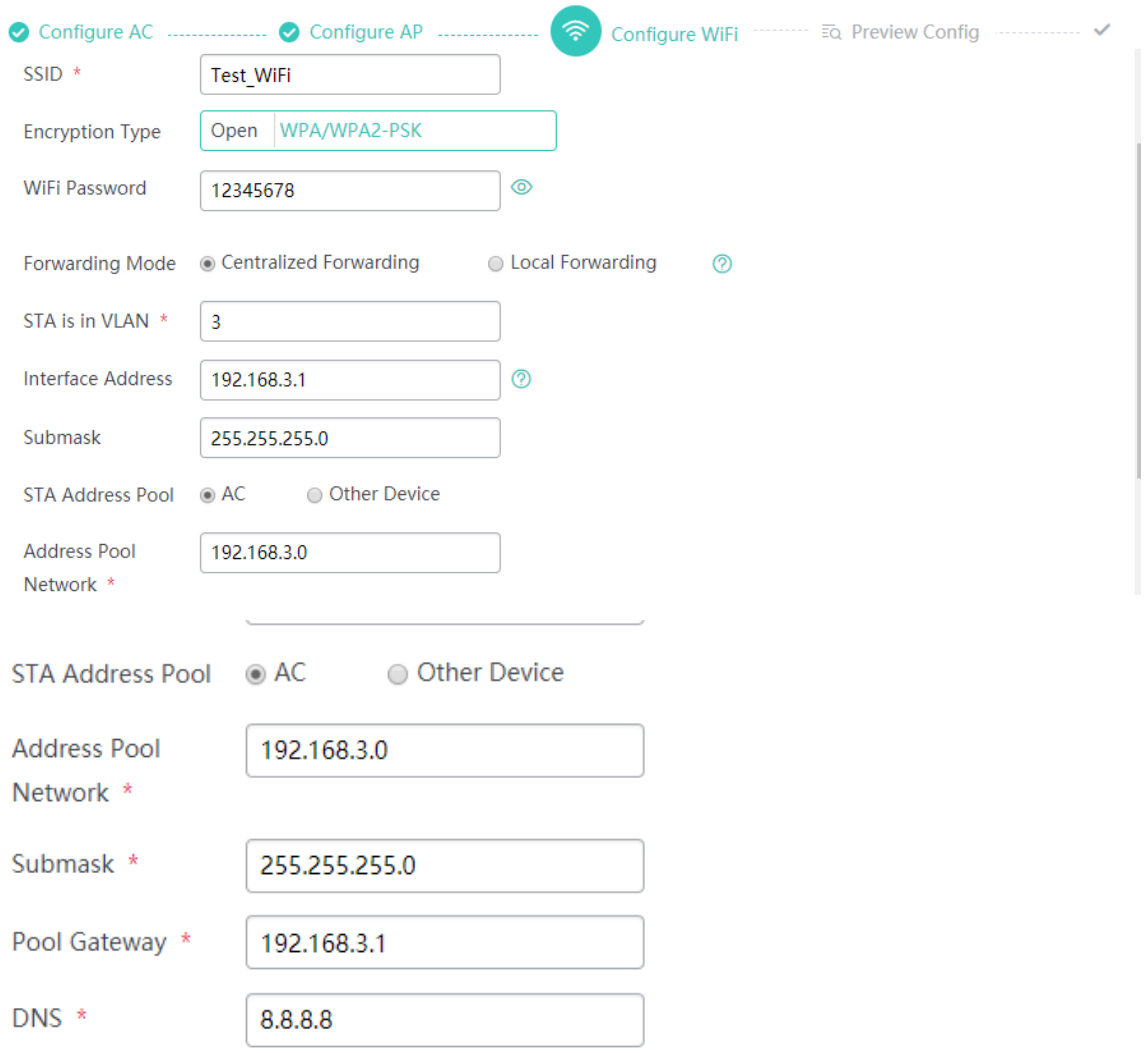
Add the IP address of the AP to VLAN 2, and set the address pool to the 192.168.2.0 network segment and the gateway to 192.168.2.1.



Configuring WiFi

Configure the WiFi SSID Test_WiFi, and set the encryption mode to WPA/WPA2-PSK (universal edition) and password to 12345678.

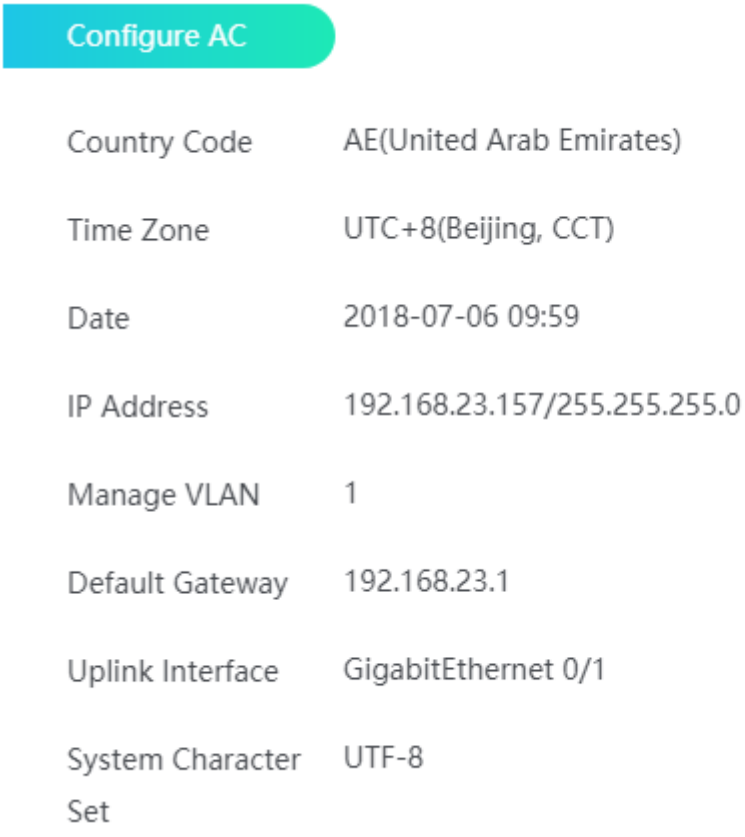
Add the IP address of the STA to VLAN 3, and set the address pool to the 192.168.3.0 network segment and the gateway to 192.168.3.1.



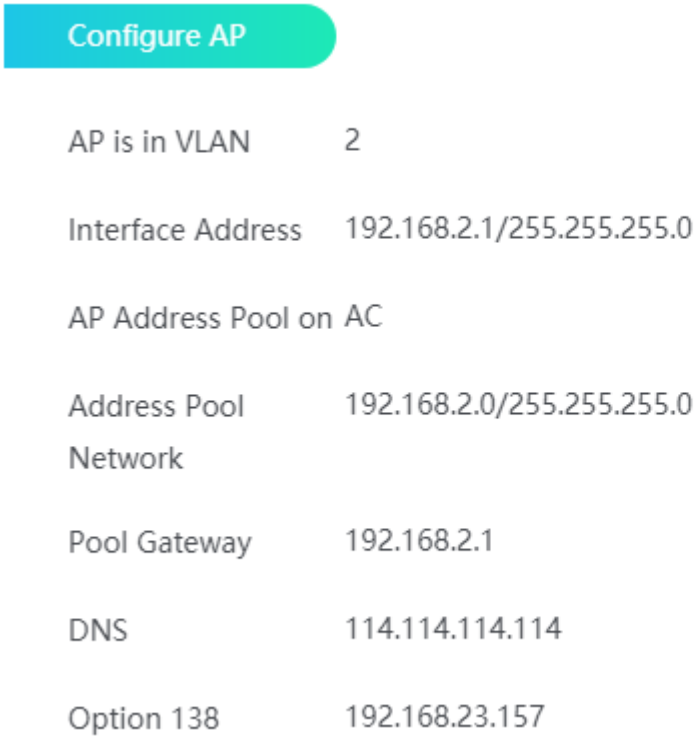
Previewing Configurations

Check whether the configurations are correct based on the preceding steps.

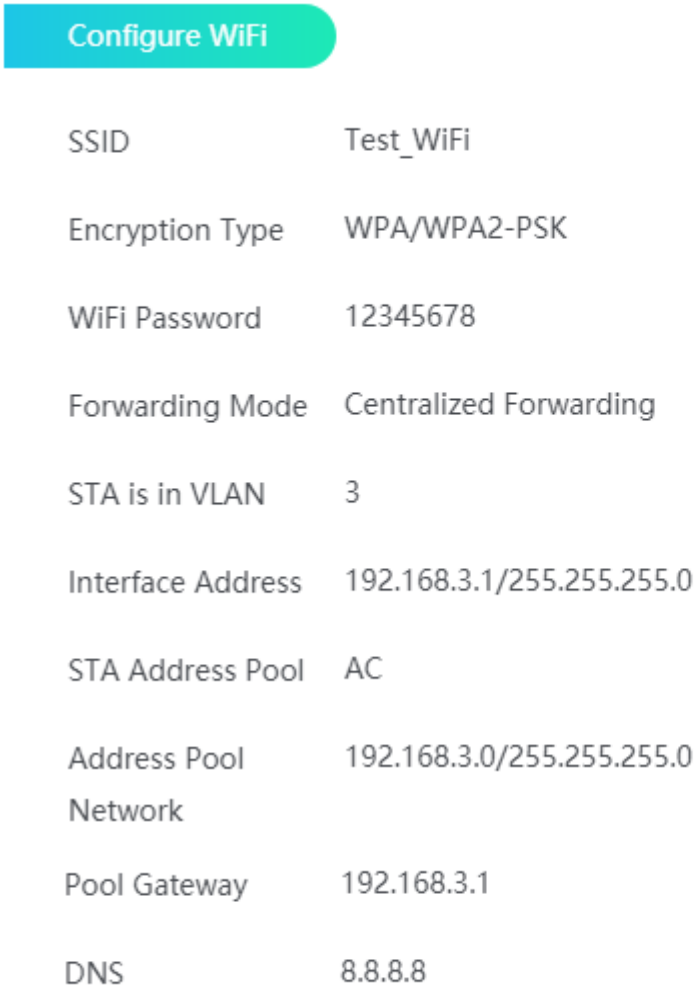
1. Basic AC configurations



2. AP access configurations



3. WiFi configurations

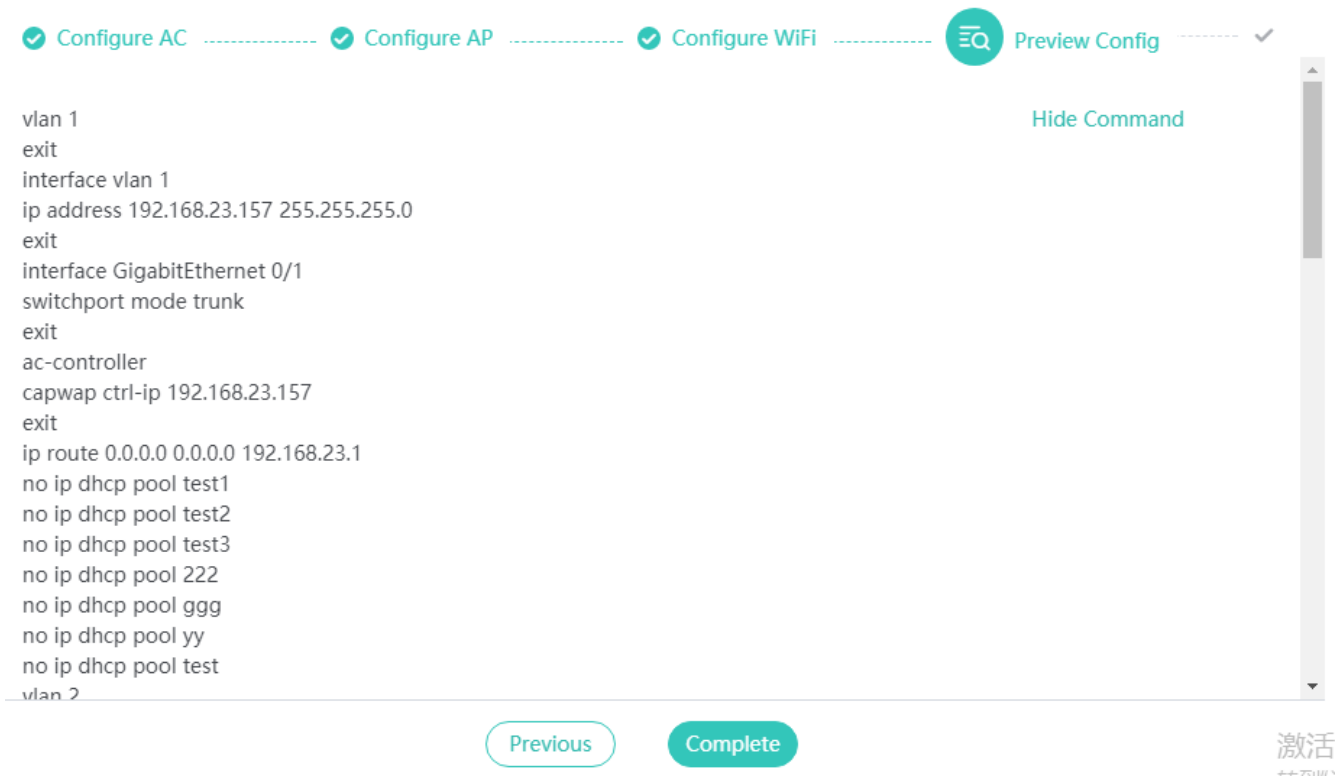


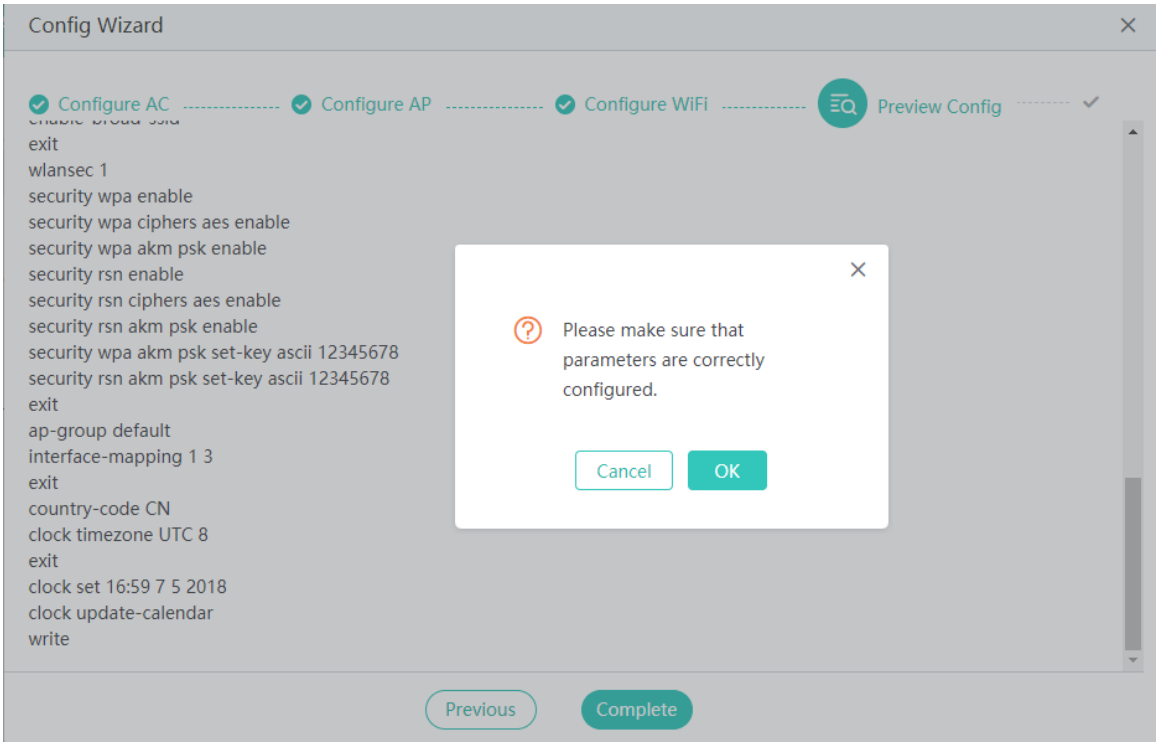
Users who are familiar with services can also click display commands to check whether the configurations to be delivered are correct. The following are commands to be delivered.

```
vlan 1
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/1
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.23.157
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
no ip dhcp pool EWEB-WIZARD-AP-POOL
```

```
no ip dhcp pool wewe
vlan 2
exit
interface vlan 2
ip address 192.168.2.1 255.255.255.0
exit
service dhcp
ip dhcp pool EWEB-WIZARD-AP-POOL
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 114.114.114.114
option 138 ip 192.168.23.157
exit
vlan 3
exit
interface vlan 3
ip address 192.168.3.1 255.255.255.0
exit
service dhcp
ip dhcp pool EWEB-WIZARD-STA-POOL
network 192.168.3.1 255.255.255.0
default-router 192.168.3.1
dns-server 114.114.114.114
exit
no wlan-config 1
wlan-config 1 Test_WiFi
ssid-code utf-8
enable-broad-ssid
exit
wlansec 1
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
security rsn akm psk enable
security wpa akm psk set-key ascii 12345678
security rsn akm psk set-key ascii 12345678
exit
ap-group default
interface-mapping 1 3
```

```
exit
language character-set UTF-8
clock timezone UTC +8
exit
clock set 15:31 3 1 2018
clock update-calendar
write
```





Click **OK** to complete the configuration.

Verification

- Check whether the STA associates with the WiFi network test_WiFi.
- Check whether the STA dynamically obtains an IP address.

1.5.1.2 Both the AP Address Pool and User Address Pool Are Configured on Other Devices

Example:

Configure the g0/1 interface as the uplink interface of the AC, set the management VLAN of the device to VLAN 1, management address to 192.168.23.157, gateway address to 192.168.23.1, and tunnel address to 192.168.23.157.

Configure a 2.4 GHz WiFi SSID EWEB_WiFi_2.4g, and set the encryption mode to WPA/WPA2-PSK (universal edition) and password to 12345678.

Configure a 5 GHz WiFi SSID EWEB_WiFi_5g, and set the encryption mode to WPA/WPA2-PSK (universal edition) and password to 12345678.

Add the IP address of the AP to VLAN 2, set the address pool to the 192.168.2.0 network segment and the gateway to 192.168.2.1, and configure the gateway on the local device and address pool on the switch.

For the EWEB_WiFi_2.4g, add the IP address of the STA to VLAN 3, set the address pool to the 192.168.3.0 network segment and the gateway to 192.168.3.1, and configure the gateway on the local device and address pool on the switch.

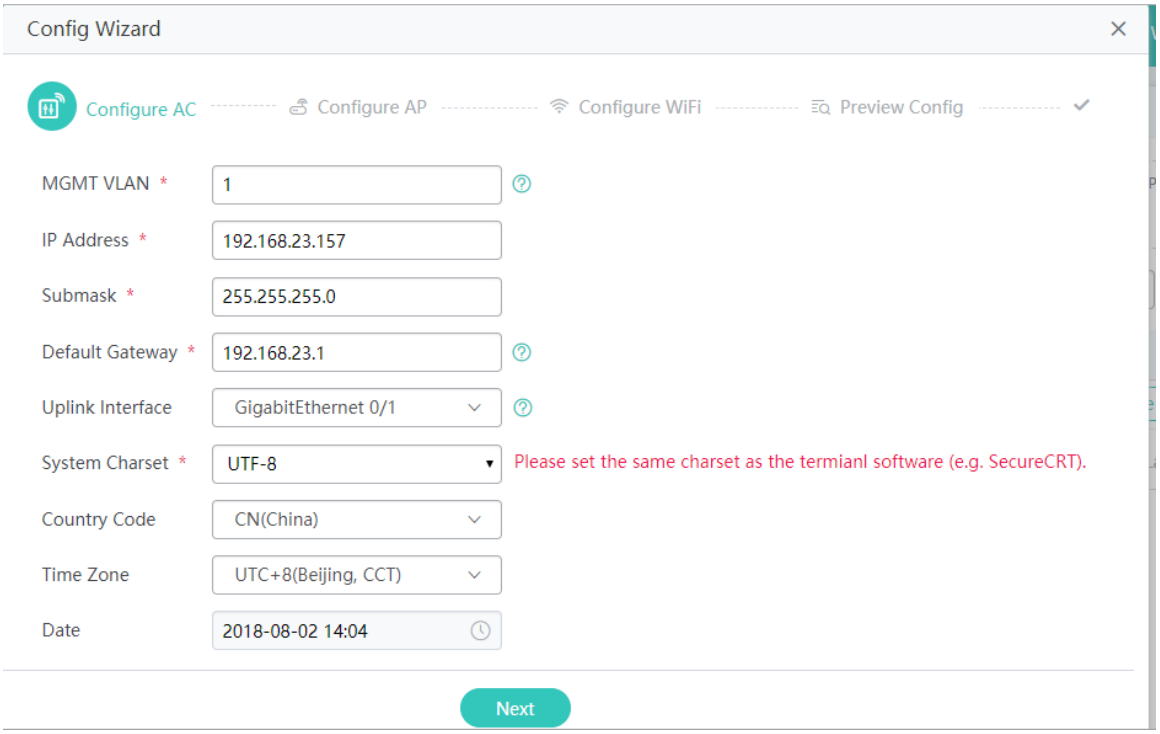
For EWEB_WiFi_5g, add the IP address of the STA to VLAN 4, set the address pool to the 192.168.3.0 network segment and the gateway to 192.168.3.1, and configure the gateway on the local device and address pool on the switch.

Configuration Steps

Configuring the AC

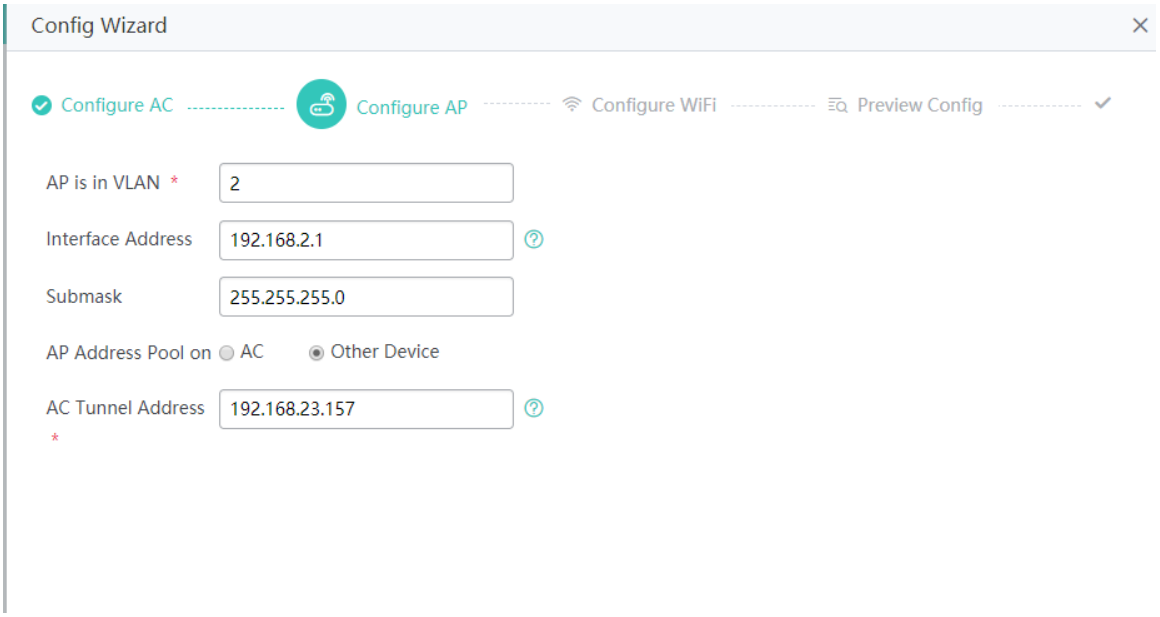
Complete basic configurations of the AC based on the scenario.

Configure the g0/1 interface as the uplink interface of the AC, set the management VLAN of the device to VLAN 1, management address to 192.168.23.157, gateway address to 192.168.23.1, and tunnel address to 192.168.23.157.

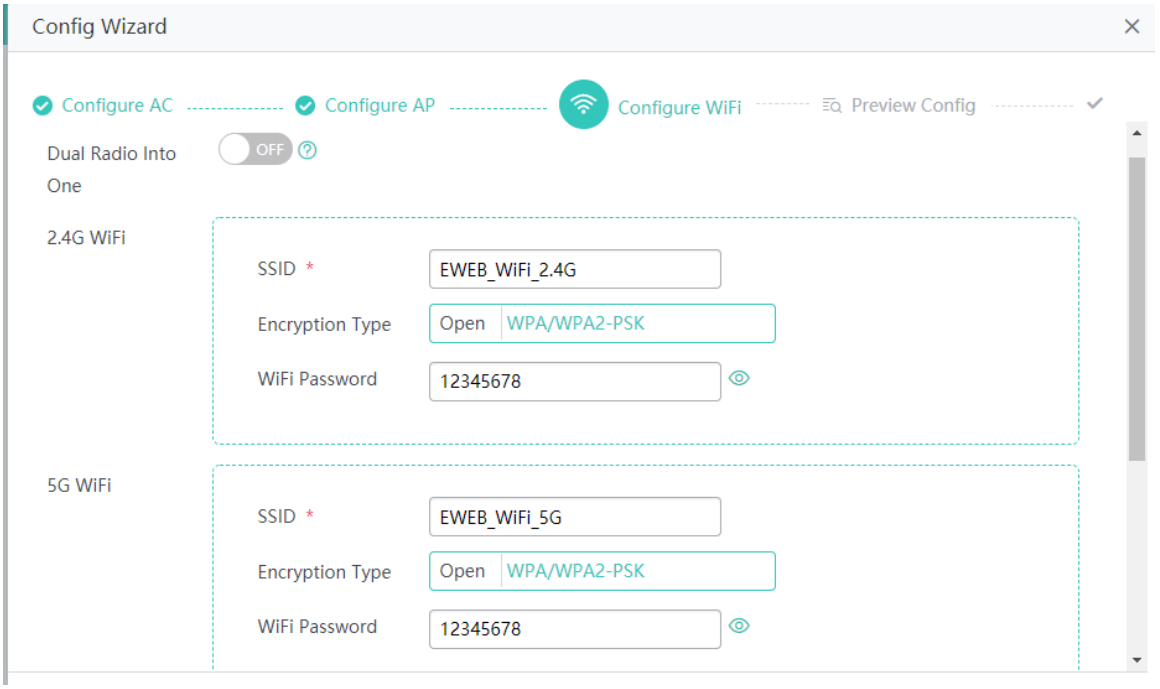


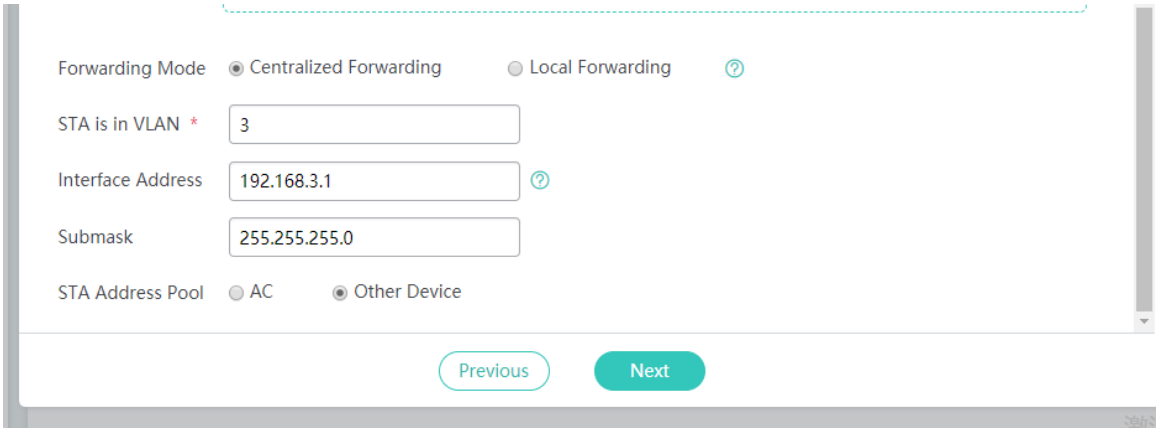
Configuring the AP

Add the IP address of the AP to VLAN 2, set the address pool to the 192.168.2.0 network segment and the gateway to 192.168.2.1, and configure the gateway on the local device and address pool on the switch.



Configuring WiFi

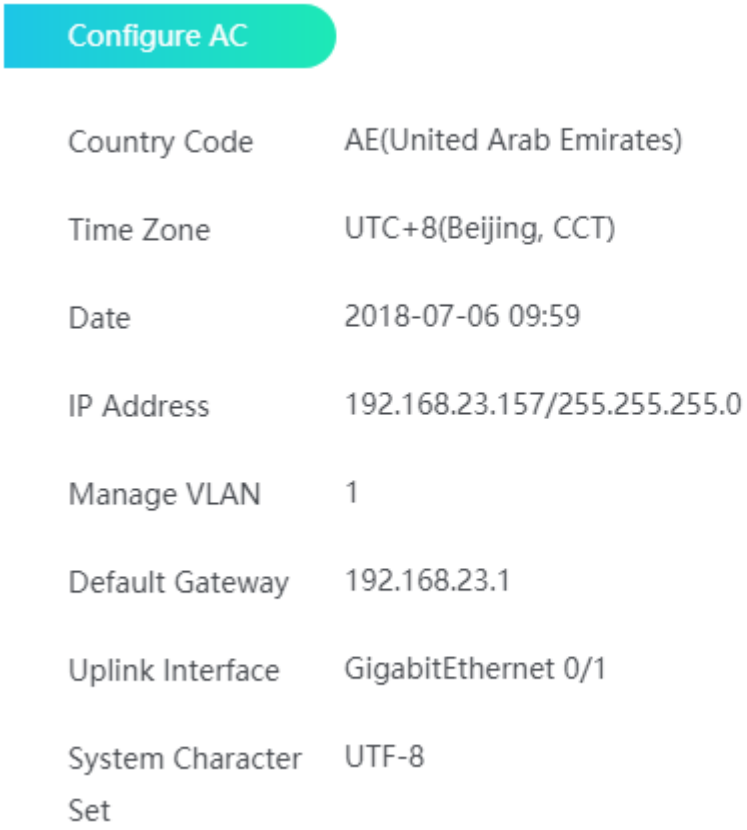




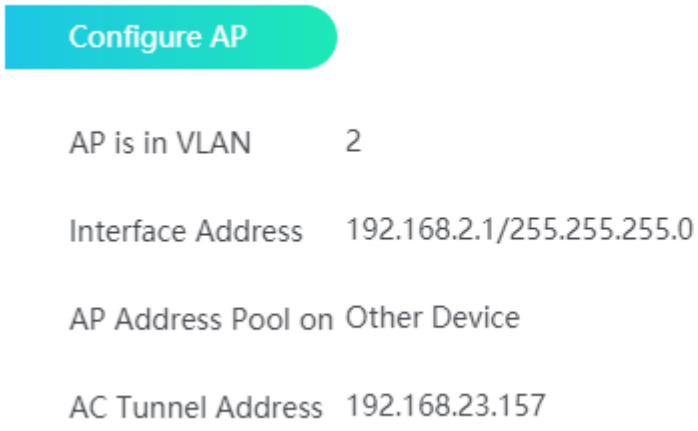
Previewing Configurations

Check whether the configurations are correct based on the preceding steps.

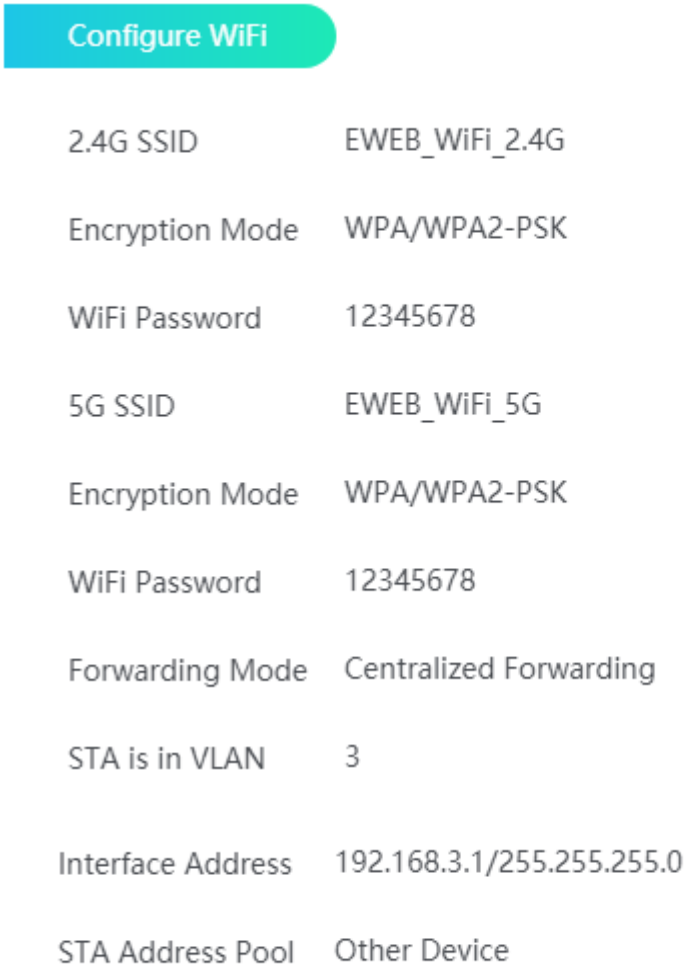
1. Basic AC configurations



2. AP access configurations



3. WiFi configurations

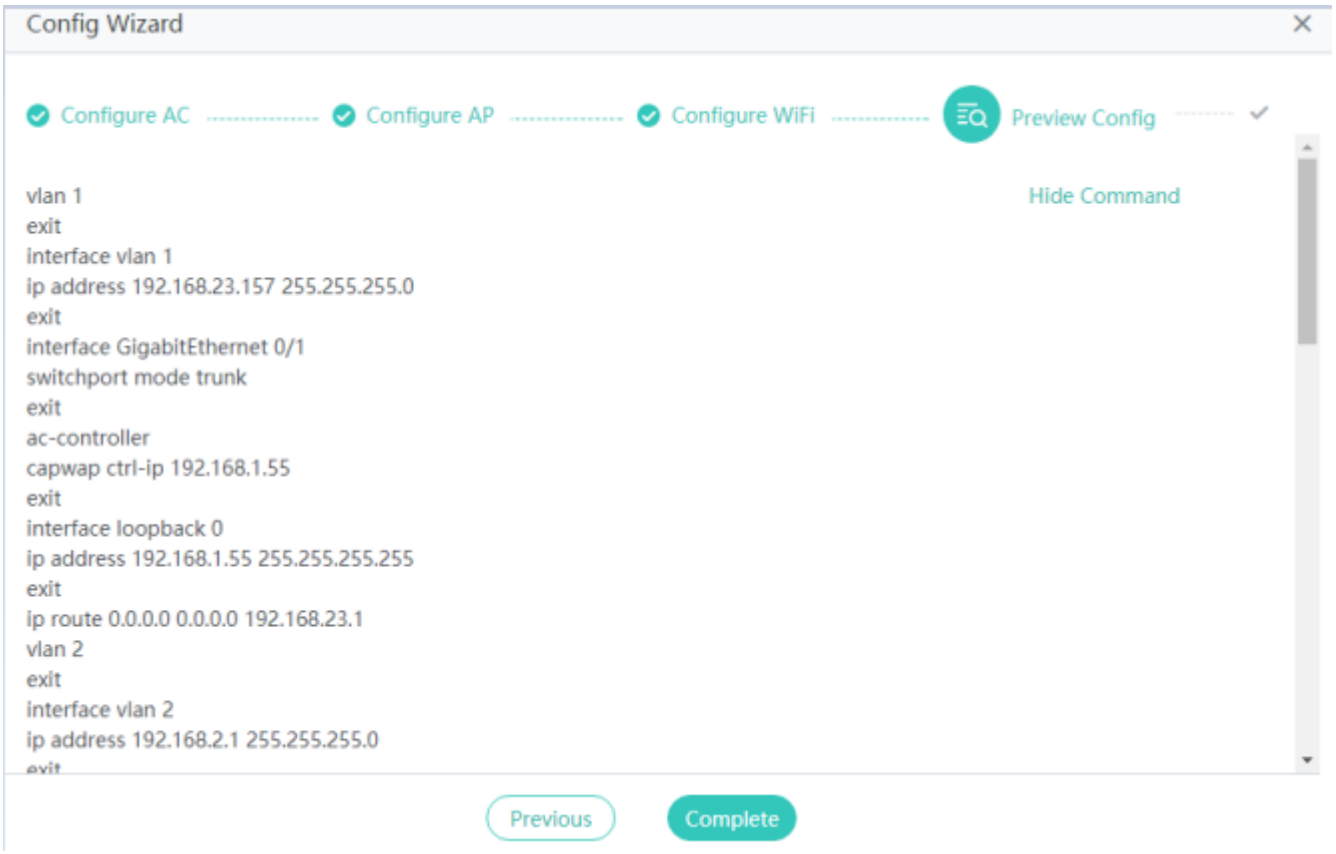


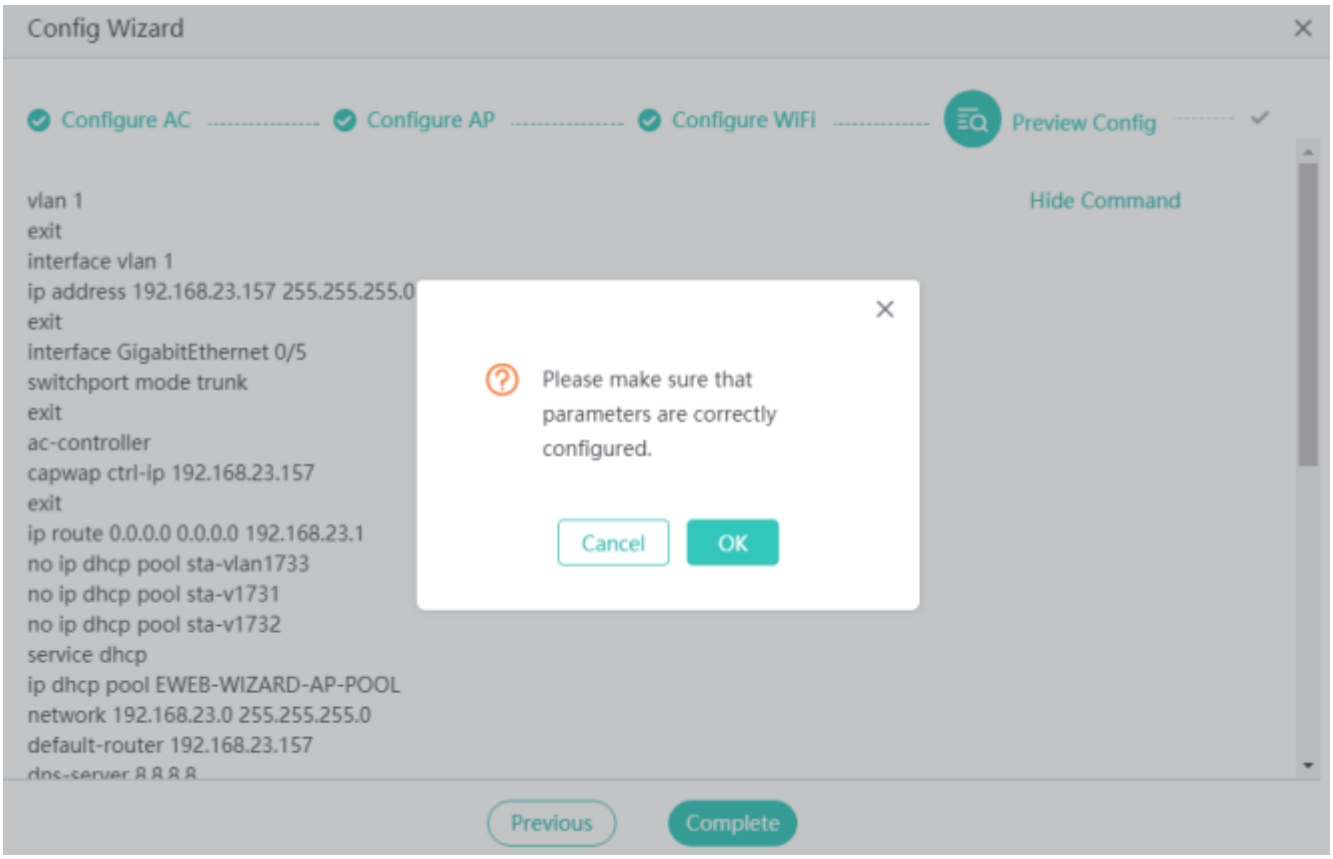
Users who are familiar with services can also click display commands to check whether the configurations to be delivered are correct. The following are commands to be delivered.

```
vlan 1
```

```
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/1
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.23.157
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
vlan 2
exit
interface vlan 2
ip address 192.168.2.1 255.255.255.0
exit
vlan 3
exit
interface vlan 3
ip address 192.168.3.1 255.255.255.0
exit
no wlan-config 1
wlan-config 1 EWEB_WiFi_2.4g
ssid-code utf-8
enable-broad-ssid
exit
wlansec 1
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
security rsn akm psk enable
security wpa akm psk set-key ascii 12345678
security rsn akm psk set-key ascii 12345678
exit
ap-group default
interface-mapping 1 3 radio 802.11b
exit
no wlan-config 2
wlan-config 2 EWEB_WiFi_5g
```

```
ssid-code utf-8
enable-broad-ssid
exit
wlansec 2
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
security rsn akm psk enable
security wpa akm psk set-key ascii 12345678
security rsn akm psk set-key ascii 12345678
exit
ap-group default
interface-mapping 2 3 radio 802.11a
exit
language character-set UTF-8
clock timezone UTC +8
exit
clock set 16:53 3 1 2018
clock update-calendar
write
```


Config Wizard
Configure AC
Configure AP
Configure WiFi
Preview Config
Hide Command
vlan 1
exit
interface vlan 1
ip address 192.168.23.157 255.255.255.0
exit
interface GigabitEthernet 0/1
switchport mode trunk
exit
ac-controller
capwap ctrl-ip 192.168.1.55
exit
interface loopback 0
ip address 192.168.1.55 255.255.255.255
exit
ip route 0.0.0.0 0.0.0.0 192.168.23.1
vlan 2
exit
interface vlan 2
ip address 192.168.2.1 255.255.255.0
exit
Previous
Complete



Click **OK** to complete the configuration.

After completing the configuration on the AC, perform configuration on the uplink switch.

```
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.2.2 255.255.255.0
!
interface VLAN 3
 no ip proxy-arp
 ip address 192.168.3.3 255.255.255.0
!
no service password-encryption
service dhcp
!
ip dhcp pool ap_pool
 option 138 ip 192.168.23.157
 network 192.168.2.0 255.255.255.0
 dns-server 114.114.114.114
 default-router 192.168.2.1
!
```

```
ip dhcp pool sta_pool
 network 192.168.3.0 255.255.255.0
 dns-server 114.114.114.114
 default-router 192.168.3.1
!
!
```

Verification

- Check whether the STA associates with the WiFi network 2.4GWiFi ruijie_test_2.4g.
- Check whether the STA associates with the WiFi network 5GWiFi ruijie_test_5g.
- Check whether the STA dynamically obtains an IP address.