



EKSELANS BY ITS

USER MANUAL

UC AX **331022**

High-Performance WiFi Controller

Copyright

Copyright © 2024 Ekselans by ITS

All rights are reserved in this document and this statement.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Company Website: <https://www.ek.plus/>
- Consult Website: <https://www.ek.plus/contacto/>
- Support Email: soporte@ek.plus

Conventions

1. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

2. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Product Overview

The UC AX wireless LAN controller provides powerful access control capability for medium-large-sized wireless networks.

1.1 Product Appearance

Figure 1-1 Front Panel of UC AX

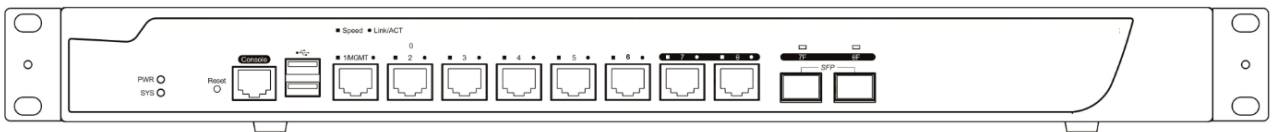
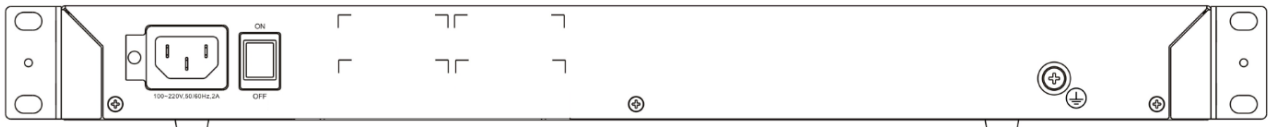


Figure 1-2 Rear Panel of UC AX



Note

The nameplate is at the bottom of the access controller.

1.2 LED Indicators

LED	State	Meaning
PWR	Off	The power module is NOT in the position or fails.
	Solid green	The power module is operational.
SYS	Blinking green	The system is being initialized.
	Solid green	The initialization process is complete.
	Solid red	The system sends out an alarm.
1-8 Gigabit copper ports (link/ACT)	Solid green	The copper port is connected at 10/100/1000 Mbps.
	Blinking green	The copper port is receiving or transmitting data.
1-8 Gigabit copper ports (speed)	Solid orange	The copper port is connected at 1000 Mbps.
	Off	The copper port is connected at 10/100 Mbps.
7F-8F Gigabit fiber ports	Solid green	The fiber port is connected.
	Blinking green	The fiber port is receiving or transmitting data.

1.3 Technical Specifications

Dimensions and Weight	UC AX
Physical Dimensions (W x D x H)	440 mm x 200 mm x 43.6 mm (excluding foot pad) (17.32 in. x 7.87 in. x 1.72 in.)
Rack Height	1 RU
Weight	Net weight: 2.9 kg (6.39 lbs.)
Port Specification	UC AX
Fixed Service Port	Six 10/100/1000Base-T Ethernet ports with auto-negotiation. Port 1 can serve as a management port. Two combo ports. When the electrical port works, 10/100/1000Base-T auto-negotiation is supported.
Fixed Management Port	One RJ45 console port Two USB ports
Status LED	One system status LED One power status LED 10 service port status LEDs
Button	One power switch One reset button
Power Supply and Consumption	UC AX
Max. Power Consumption	40 W
Input Voltage	100 V AC to 240 V AC, 50 Hz to 60 Hz
Output Voltage	12 V/3.33 A
Environment and Reliability	UC AX
Temperature	Operating temperature: -10°C to +40°C (14°F to 104°F) Storage temperature: -40°C to +70°C (-40°F to +158°F) At a height between 3000 m (9842.52 ft.) to 5000 m (16404.20 ft.) above the sea level, every time the altitude increases by 166 m (544.62 ft.), the maximum temperature decreases by 1°C (1.8°F).
Humidity	Operating humidity: 10% to 90% RH (non-condensing) Storage humidity: 5% to 95% RH (non-condensing)
Safety regulations	GB 4943.1 CE Marked, EN/IEC 62368-1 (replacing EN/IEC 60950-1) Low Voltage Directive 2014/35/EU
EMC regulations	EN 300 386, EN301 489, EN 55032 Class A, EN 55035, EN 61000-3-2, EN 61000-3-3, EN 61000-4-2, EN 61000-4-3,

	EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11
MTBF	≥ 200, 000 hours

Note

- A combo port consists of an optical port and an electrical port. The optical port and electrical port cannot work at the same time. If one port is enabled, the other is disabled. You can select the port type as required.
- Due to the variety of USB flash drives, not all of them are supported. A USB flash drive with the FAT32 file system format is recommended.

Caution

Please avoid vibration and shock when moving and using the device.

Warning

- The circuit breaker in the power module cannot be removed.
- This is a Class A product. In a domestic environment, this product may cause radio interference. In this case, users are advised to take proper measures against the interference.

2 Preparation for Installation

2.1 Precautions

The wireless controller acts as a network repeater and its working affects the normal operation of the whole network.

The following suggestions are advised for the installation and use of UC AX:

- Do not place the wireless controller in a damp/wet location. Do not let any liquid enter the chassis.
- Keep the wireless controller far away from the heat source.
- Ensure that the wireless controller is properly grounded.
- Wear an anti-static wrist strap during installation and maintenance.
- Do not wear loose clothes to avoid hooking any parts. Before operation, tighten your band, shawl, and sleeves.
- Put the tools and parts away from where people walk by.
- Use UPS to prevent power failure and other interferences.
- If the clock is not accurate, check whether the clock has been configured. If not, the inaccuracy is likely to occur. If the clock has been configured, the inaccuracy may be caused by the battery running out of power. In general, the button battery lasts about 10 years.
- To ensure proper operation of the device, store the device in an environment based on the storage temperature or humidity requirements in specifications.

Note

- Misuse of battery may cause damage to the device or hurt to people. Do not replace battery by yourself.
 - This device is not suitable for use in locations where children are likely to be present.
 - If the device has been powered off for over 18 months, power on the device and keep it run for over 24 hours consistently.
 - Keep the device within the restricted-access area.
 - The device should be installed by professionals or technicians.
-

2.2 Preparing Installation Site

UC AX is for indoor use only. To ensure its normal operation and prolong its life span, the installation site should meet the following requirement:

2.2.1 Temperature and Humidity Requirements

To ensure normal operation and service life of the device, maintain appropriate temperature and humidity levels in your equipment room. See Table 2-1. Improper room temperature and humidity can cause damages

to the device. High relative humidity may affect insulation materials, resulting in poor insulation and even electrical leakage, and sometimes may lead to change of mechanical properties of materials and corrosion of metal parts. Low relative humidity may dry and shrink insulation sheets and cause static electricity that can damage the circuitry inside the device. High temperature greatly reduces reliability of the device and shortens its service life.

Table 2-1 Required Temperature and Humidity for the UC AX

Relative Temperature				Relative Humidity			
Long-time Condition	Working	Short-time Condition	working	Long-time Condition	Working	Short-time Condition	Working
15°C to 86°F)	30°C (59°F to	0°C to 113°F)	45°C (32°F to	40%~65%		5%~95%	

Note

- The ambient temperature and humidity are measured at a point 1.5 meters (4.9 feet) above the ground and 0.4 meters (1.3 feet) before the device when there is no protective board in the front or back of the rack.
- The short-term working condition refers to a period no longer than consecutive 48 hours or accumulated 15 days a year.
- The extreme working condition refers to the temperature and humidity of the machine room where the air conditioner fails for no more than five hours.

2.2.2 Cleanness Requirements

Dust poses a serious threat to device operation. Dust that falls onto the surface of the device can be absorbed onto metal contact points by static electricity, resulting in poor contact. Electrostatic absorption of dust occurs more easily when the relative humidity is low, which may shorten the service life of the device and cause communication failures. Table 2-2 shows the maximum concentration and diameter of dust allowed in the equipment room.

Table 2-2

Maximum Diameter (µm)	0.5	1	3	5
Maximum Content (Number of Particles in one Cubic Meter)	1.4×10^7	7×10^5	2.4×10^5	1.3×10^5

Besides, the contents of salts, acids and sulfides in the air are also strictly limited for the equipment room. These substances can accelerate metal corrosion and the aging of some parts. Table 2-3 describes the limit of some hazardous gases such as SO₂, H₂S, NO₂ and Cl₂ in the equipment room.

Table 2-3

Gas	Average (mg/m ³)	Maximum (mg/m ³)
SO ₂	0.2	1.5
H ₂ S	0.006	0.03
NO ₂	0.04	0.15

NH ₃	0.05	0.15
Cl ₂	0.01	0.3

2.2.3 Static Discharge Damage Prevention

Although much has been done in UC AX to prevent static electricity, great damage may be caused to the circuitry when the static electricity exceeds a certain limit. Electrostatic induction may come from the following sources:

- External electric field produced by the high-voltage supply cable, lightning, etc.
- Internal systems such as the indoor floor and the entire structure.

To prevent damage from static electricity, you must pay attention to the following:

- Properly ground the equipment.
- Take dust prevention measures in the room.
- Maintain an appropriate humidity and temperature.
- Always wear an anti-static wrist strap when you touch any circuit board.
- Place the circuit board on an anti-static workbench or in an anti-static shielding bag.
- Try to hold a circuit board by its edges. Do not touch any components or the PCB.

2.2.4 Anti-Interference Requirements

The wireless controller is susceptible to external interference such as electromagnetic wave and current. Note that:

- Provide the power system with effective anti-interference measures.
- It is recommended that the wireless controller be installed far away from the grounding device.
- Keep the wireless controller away from high-power radio stations, radar stations, and high-frequency high-current devices.
- Use EMI shielding when necessary.

2.2.5 Installation Site Requirements

To install the wireless controller whether in the cabinet or on the workbench, pay attention to the following items:

- Ensure that enough space is reserved around the air inlet and exhaust vents for ventilation and heat dissipation. It is recommended that the wireless controller be installed in a standard 19-inch cabinet. Otherwise, use a clean platform as a workbench. It is recommended to equip the installation site with an air conditioner if it is hot.
- Ensure that the cabinet or the workbench is provided with proper ventilation and heat dissipation system.
- Ensure that the cabinet or the workbench is sound enough to bear the weight of the wireless controller and its accessories.

- Ensure that the cabinet or the workbench is properly grounded.

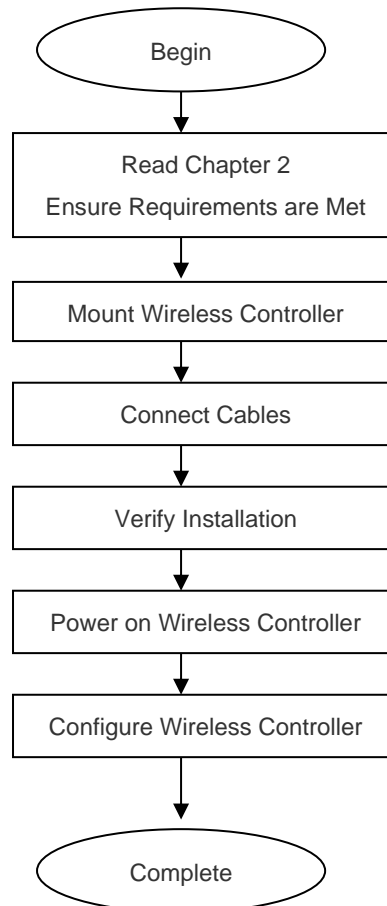
2.3 Installation Tools

Installation Tool	Cross screwdriver and anti-static wrist strap
Cable	Power cord, configuration cable, Ethernet cable and grounding cable
Device	Hub/switch, configuration terminal (such as PC with Hyperterm) and power socket

3 Installing Wireless Controller

3.1 Installation Flowchart

Please follow the following procedure to install the wireless controller to ensure the smooth installation and avoid any damage to the device.



3.2 Mounting Wireless Controller

Now the wireless controller is ready for installation. Mount it to either of these two places.

- A cabinet
- A workbench

3.2.1 Mounting UC AX in Cabinet

UC AX is designed according to the specification of 19-inch standard cabinet. Use the supplied mounting accessory for installation.

3.2.2 Mounting UC AX on Workbench

In the absence of a 19-inch standard cabinet, install the wireless controller on a clean workbench. During the operation, pay attention to the following items:

- The workbench is firm and well-grounded.
- The supplied plastic cushion is stuck to the small hole at the bottom of the wireless controller and a 10 cm clearance is reserved for dissipation.
- No weight is placed on the top of the wireless controller.

3.3 Installing Power Cable

UC AX supports AC (100 VAC to 240 VAC; 50/60 Hz). Make sure that your power supply meets the requirement.

Note

See Chapter 1 for details about the power module.

UC AX uses three-wire power cable. It is recommended to use single-phase three-wire power socket or multi-functional microcomputer socket with neutral-point connector. The neutral-point needs to be grounded safely. Check whether the power supply in your building is grounded properly.

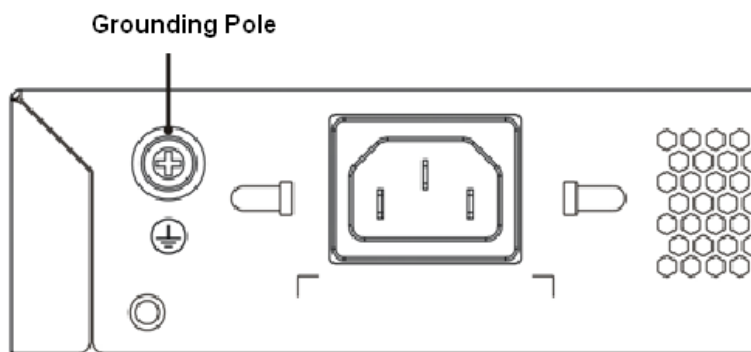
Follow the following steps to install the power cable:

1. Connect one end of the supplied power cable to the socket on the rear panel of the device and another to the AC power socket.
2. Check the power indicator on the front panel is on. If it is, it means that the power cable is correctly connected.

3.4 EMS & Secure Grounding

The ground required for EMC design includes shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The grounding resistance should be smaller than 1Ω . The UC AX wireless controller has a grounding pole on the rear panel, as shown in Figure 3-1.

Figure 3-1 UC AX Grounding



3.5 Connecting Console

UC AX supplies an EIA/TIA-232 configuration console for local configuration. If you configure UC AX through Web, skip this part.

Table 3-2 Console Attributes

Parameter	Description
Connector	RJ-45
Interface Standard	Asynchronous EIA/TIA-232
Baud Rate	57,600 bps, 115,200 bps, 9,600 bps (default)
Supported Services	<ol style="list-style-type: none"> 1. Command line interface 2. Connection to character terminals 3. Providing terminal access service as an asynchronous interface

Connect one end of the supplied configuration cable to the console port of the wireless controller, and the other end to the DB-9 male serial adapter of the microcomputer.

3.6 Verification

When you have installed the wireless controller, before powering on it, pay attention to the following items:

- If the wireless controller is stalled in a cabinet, check the mounting brackets of the cabinet and wireless controller are firm. If the wireless controller is installed on the workbench, check there is enough room around the wireless controller for heat dissipation and the workbench is firm.
- Check the power supply meets the requirements.
- Check the grounding cable is correctly connected.
- Check the wireless controller is connected correctly to other devices such as the configuration terminal.

⚠ Caution

To shut down the device, turn off the power switch on the rear panel of the device. Do not directly disconnect the 220 V power supply, such as directly cutting off the power or unplugging the power cord.

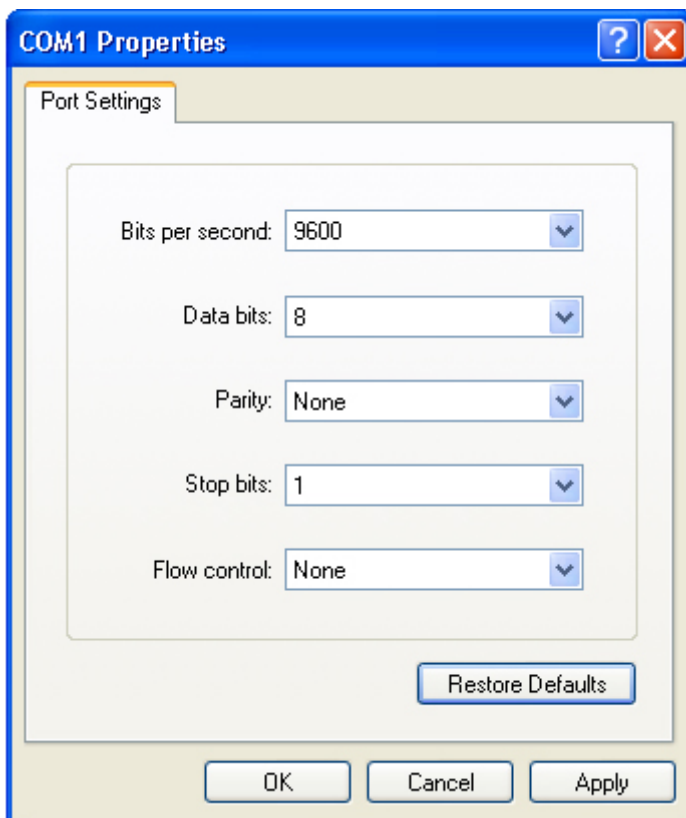
4 Configuration Guide

4.1 Setting up Configuration Environment

When you use the wireless controller for the very first time, you will need to configure it through a console port as follows:

- As shown in the following figure, connect the serial port of a character terminal or microcomputer to the console port through an RS232 cable.
- Set the communication parameters of the terminal. For a microcomputer, you will need to run a terminal emulation program like Windows operating system's Hyperterm. Take Hyperterm for example.
 - (1) Run Hyperterm and create a connection.
 - (2) Select the serial port to be connected with the console port of the wireless controller
 - (3) Set communication parameters as follows: baud rate to 9600, data bit to 8, stop bit to 1, parity to No, flow control to No, as shown in figure 4-1.

Figure 4-1 Setting Communication Parameters for Serial Port.



After building the configuration environment, you may power on the wireless controller

4.2 Powering on Wireless Controller

4.2.1 Verification Before Power-on

Before powering on the wireless controller, please check the following items:

- If the power cable and the grounding cable are connected correctly.
- If the power supply voltage meets the requirement.
- If the configuration cable is connected correctly, the microcomputer or terminal is turned on, and the setting is complete.

Note

Before powering on the wireless controller, check the position of the power switch so that you may cut power supply in time in case of accident.

4.2.2 Power-on

- Turn on the power supply.
- Turn the power switch of the wireless controller to the **on** position.

4.2.3 Verification After Power-on

After powering on the wireless controller, please check the following items:

- If the ventilation system is functional.

When the wireless controller is powered on, you will hear the fan working. Put your hand near the air inlet and exhaust vents, you will feel the air flowing.

- If the indicators on the front panel of the wireless controller are in the proper state.

See **LED Indicators** in Chapter 1.

- If the configuration terminal displays information as expected.

When the wireless controller is powered on, information on the software self-decompression will appear on the terminal display.

4.2.4 Startup Process

When the wireless controller is started for the first time, the following information appears:

```
*****
```

```
Boot 1.2.0-00346-g2d7093f (Build time: Mar 27 2024 - 16:04:49)
```

```
DRAM: 2 GiB
```

```
NAND: 512 MiB
Flash: 8 MiB
SETMAC: Setmac operation was performed at 2024-04-22 10:38:33 (version: 11.0)
Press Ctrl+C to enter Boot Menu
Bootloader: Done loading app on coremask: 0xffffffff
[ 0.000000] Linux version 2.6.32.13-Cavium-Octeon (ngcf@ngcf75) (gcc version 4.3.3 (Cavium Networks
Version: 2_0_0 build 95) ) #1 SMP Thu May 8 04:34:42 CST 2024
[ 0.000000] CVMSEG size: 2 cache lines (256 bytes)
[ 0.000000] Cavium Inc. SDK-2.3
[ 0.000000] bootconsole [early0] enabled
[ 0.000000] CPU revision is: 000d910a (Cavium Octeon II)
[ 0.000000] Checking for the multiply/shift bug... no.
[ 0.000000] Checking for the daddiu bug... no.
[ 0.000000] Determined physical RAM map:
[ 0.000000] memory: 00000000003f000 @ 0000000000dd1000 (usable after init)
[ 0.000000] memory: 000000000f000000 @ 0000000000f00000 (usable)
[ 0.000000] memory: 00000000d0000000 @ 0000000020000000 (usable)
[ 0.000000] memory: 00000000ffff000 @ 00000000f0001000 (usable)
[ 0.000000] memory: 0000000030efff000 @ 00000000100001000 (usable)
mount: Mounting /dev/sda1 on /var/storage failed: No such device or address
Starting rg_lowmem_killer... [ OK ]
.....
Starting snooping.elf... [ OK ]
Starting postgresql server...
/mnt/sata0/pgsql/bin/postgres not found... [ OK ]
Starting rg-mtdoops-cli... [ OK ]
Starting sntp.elf... [ OK ]
Press RETURN to get started
*May 15 11:08:01: %CAPWAP-4-NO_IP_ADDR: Please config the IP address for capwap.
```

Now the wireless controller is ready for configuration.

Note

- Such information may vary with hardware configuration or software version.
 - When using the wireless controller for the first time, it is recommended to set basic parameters during configuration.
-

5 Troubleshooting

5.1 Power Troubleshooting

You may use the power indicator on the front panel to decide if the power supply system is operating normally. For description of indicators, see Chapter 1. If a fault occurs, check the following items:

- If UC AX power switch is in the on position.
- If the power supply is turned on.
- If the power cord is connected correctly.
- If the power supply meets the requirements.

⚠ Caution

Never attempt hot swapping of the power cord. If the steps above did not solve your problem, contact your local distributor or technical support personnel.

5.2 System Troubleshooting

If the system is operational, relevant information is displayed on the terminal as described in chapter 4. Otherwise, nothing or gibberish is displayed. If nothing is displayed, please check the following items:

- Verify whether the system power supply is operational.
- Verify whether the cable is connected to the console port correctly.

If there is still nothing displayed, it may be due to improper cable connection or incorrect parameter settings. Please change the parameter settings.

If gibberish is displayed, it may be caused by incorrect parameter settings. Please check the following parameters:

- Baud rate: 9600
- Data bit: 8
- Parity check: None
- Stop bit: 1
- Flow control: None
- Terminal emulation: VT100

i Note

If the console port parameters are changed, it may cause no display on the terminal.



EKSELANS BY ITS

USER MANUAL

AX Series Access Controllers

Web-based

Copyright

Copyright © 2024 Ekselans by ITS

All rights are reserved in this document and this statement.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Company Website: <https://www.ek.plus/>
- Consult Website: <https://www.ek.plus/contacto/>
- Support Email: soporte@ek.plus

Conventions

1. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

2. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Operating Environment

1.1 Overview

You can access the Web management system through a web browser such as Internet Explorer and Google Chrome to manage AC.

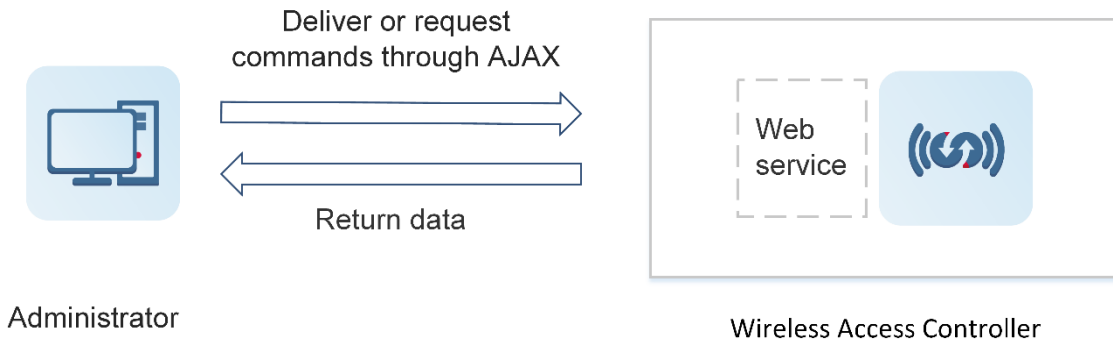
Web management system involves Web server and Web client. The Web server is integrated into the device to receive and process requests from a client. It then returns the processing results to the client. Web clients typically refer to web browsers, such as Internet Explorer and Google Chrome.

1.2 Connecting to the Device

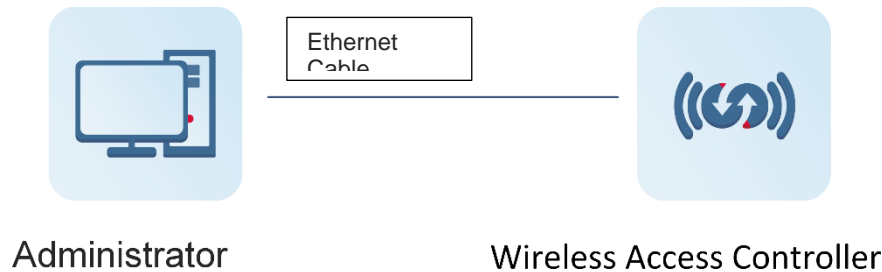
Web management system involves Web server and Web client. The Web server is integrated into the device to receive and process requests from a client. It then returns the processing results to the client. Web clients typically refer to web browsers, such as Internet Explorer and Google Chrome.

As shown in the following figure, the administrator configures devices through the Web management system on the web browser.

Application Topology



Simplified Topology



The Web management system works by assembling various device commands and sending them to the device via Asynchronous JavaScript and XML (AJAX) requests. The device responds with relevant data. Basic HTTP requests can be handled by the Web service on the device.

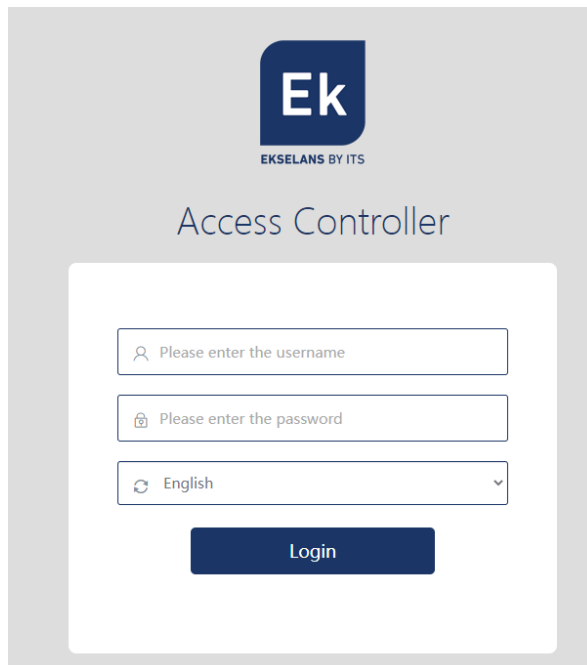
1.3 Configuration Environment for PC clients

- The administrator logs in to Web management system to manage devices through the web browser on the Web management client. Clients typically refer to PCs but may also include other mobile terminal devices such as laptops and iPads. Mobile phone is not supported for now.
- Web browser: Google Chrome is recommended, and Internet Explorer 11 is also supported. Exceptions such as garbled characters or format errors may occur if an unsupported browser is used.
- Resolution: You are advised to set the resolution to 1280 pixels x 1024 pixels, 1920 pixels x 1080 pixels, or 1440 pixels x 960 pixels. Using other resolutions may result in misaligned and less visually appealing formatting.

1.4 Web Service Environment for ACs

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

After the Web service is enabled and the IP address is correctly configured, enter the IP address in the address bar of your browser, such as <http://X.X.X.X> (management IP). Press **Enter** and the following page is displayed:



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

Default Username/Password	Description
---------------------------	-------------

admin/admin	Super administrator with full permissions.
-------------	--

1.5 Enabling the Web Service

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

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

1.5.1 Configuration Steps

↳ Enabling the Web Service

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

↳ Configuring the IP Address

- Optional.

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

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

1.5.2 Verification

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

1.5.3 Related Commands

↳ Enabling the Web Service

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

↳ Configuring the IP Address

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

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

Command	webmaster level <i>privilege-level</i> username <i>name</i> password { <i>password</i> [0 7] <i>encrypted-password</i> }
Parameter Description	<i>privilege-level:</i> Indicates the privilege level of users., including privilege levels 0, 1, and 2. Default administrator account admin and guest account guest have permissions of privilege levels 0 and 2 respectively. Other manually created accounts have permissions of privilege level 1. <i>name:</i> Indicates the username. <i>password:</i> Indicates the password. 0 7: Indicates the password encryption types, 0 for no encryption, and 7 for simple encryption. The default value is 0 . <i>encrypted-password:</i> Indicates the password text.
Command Mode	Global configuration mode
Usage Guide	N/A

1.5.4 Configuration Example

Configuration Steps	Enable the Web service.
----------------------------	-------------------------

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

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

Verification

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

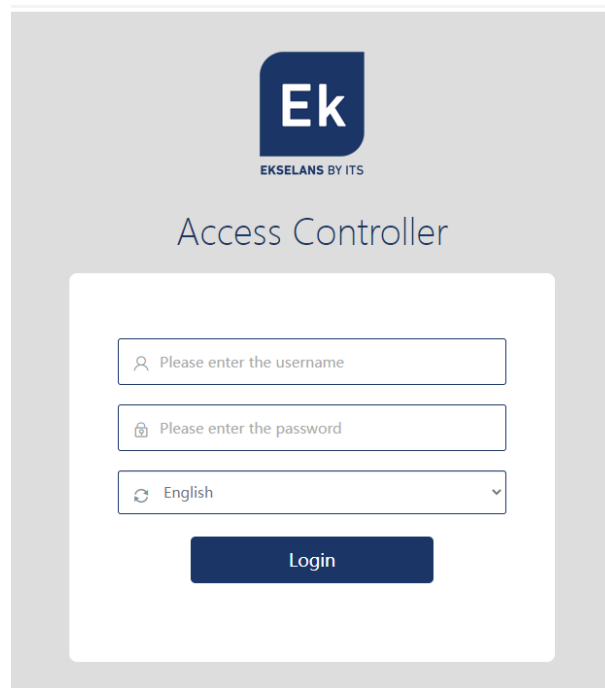
```
Hostname(config)# show running-config
Building configuration...
Current configuration : 6312 bytes

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

2 Quick Setup

2.1 Logging in to the Web Management System

You will be prompted to change the password upon your first login to the Web management system. You are advised to set a complex password. Use the new password upon next login. If you enter incorrect passwords for five consecutive times within 10 minutes, your account will be locked for 10 minutes.

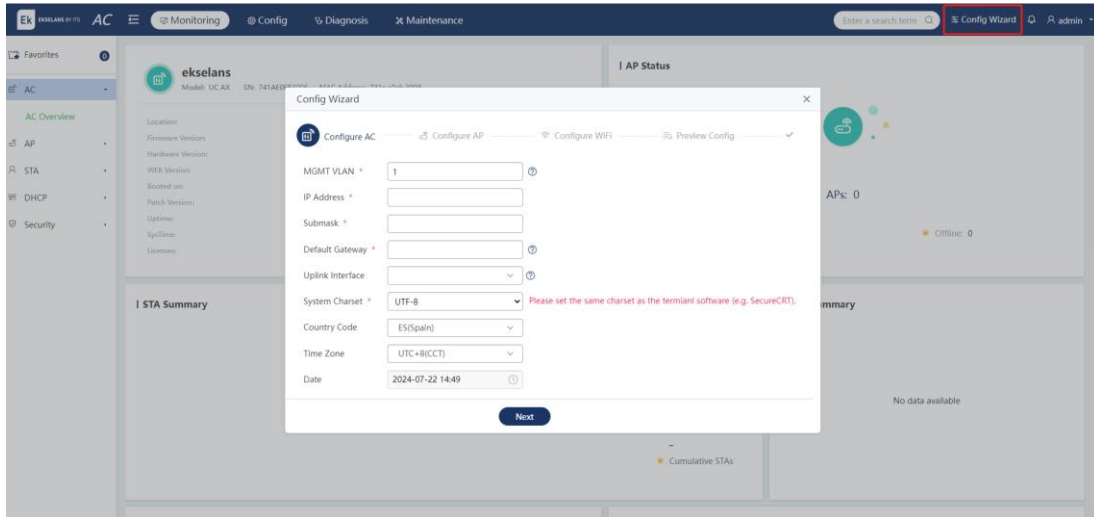


2.2 Config Wizard

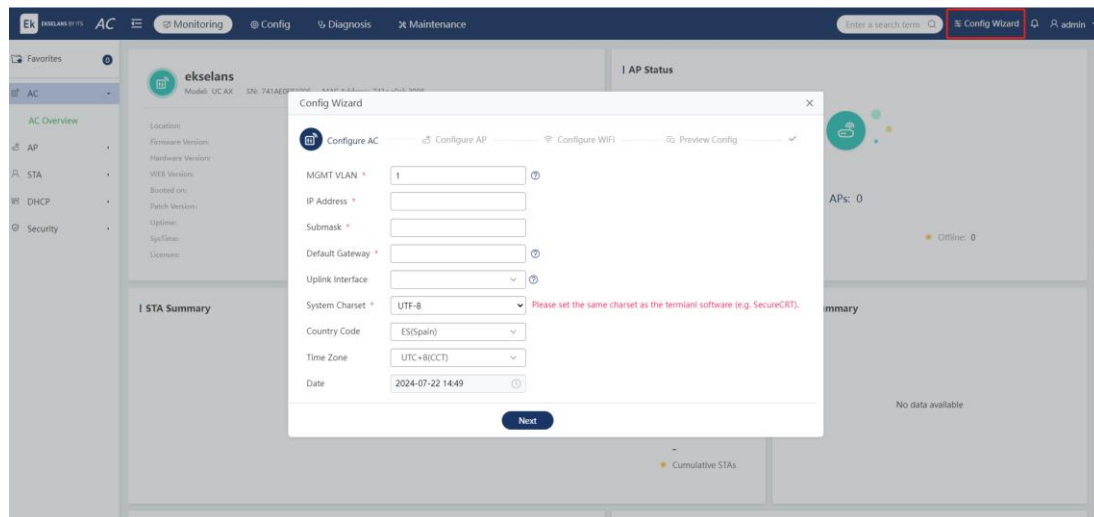
Quick wizard is typically used for first setup. Click **Config Wizard** on the navigation bar. It provides some common scenario-based configurations.

1. If no config.text file is found, that is, the current device is not configured yet, the **Config Wizard** window will pop up to guide you through configuration.
2. The **Config Wizard** allows the configuration of only one or two WLANs for setting up a Wi-Fi network.
3. Once the **Config Wizard** is completed, the existing configurations of the device will be overwritten.

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



2.2.1 Configure AC



Parameter	Description
MGMT VLAN	Enter the VLAN for the AC to communicate with an external network and for users to visit the Web management system.
IP Address	Enter the IP address for the AC to communicate with an external network and for users to visit the Web management system. It is also the default IP address of the tunnel between the AC and AP.
Submask	Enter the IP submask for the AC to communicate with an external network.
Default Gateway	Enter the egress gateway.
Uplink Interface	Enter the interface connecting the AC and its uplink device.
System Charset	Enter the system charset and the default is UTF-8 encoding. If you intend to use other client tools, you are advised to use UTF-8 encoding as well. Otherwise, code mixing may occur, resulting in configuration problems or garbled text on the page.

Country Code	Enter the country or region where the device is located. Regulations for RF bands, channels, and power vary in different countries or regions.
Time Zone	Enter the time zone where the device is located.
Date	Enter the time of the device.

2.2.2 Configure AP

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

(2) AP Address Pool on:

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

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

Config Wizard

Configure AC | **Configure AP** | Configure WiFi | Preview Config

AP is in VLAN * 1

Interface Address 10.52.24.237

Submask 255.255.248.0

AP Address Pool on AC Other Device

Address Pool 10.52.24.0

Network * 10.52.24.0

Submask * 255.255.248.0

Pool Gateway * 10.52.24.237

DNS * 8.8.8.8

Option 138 * 10.52.24.237

Previous Next

2.2.3 Configure Wi-Fi

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

Config Wizard

Configure AC | Configure AP | **Configure WiFi** | Preview Config

Dual Radio Into One ON

SSID * EKWiFi

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

WiFi Password ekwifi

Forwarding Mode Centralized Forwarding Local Forwarding

STA is in VLAN * 1

Interface Address 10.52.24.237

Submask 255.255.248.0

STA Address Pool AC Other Device

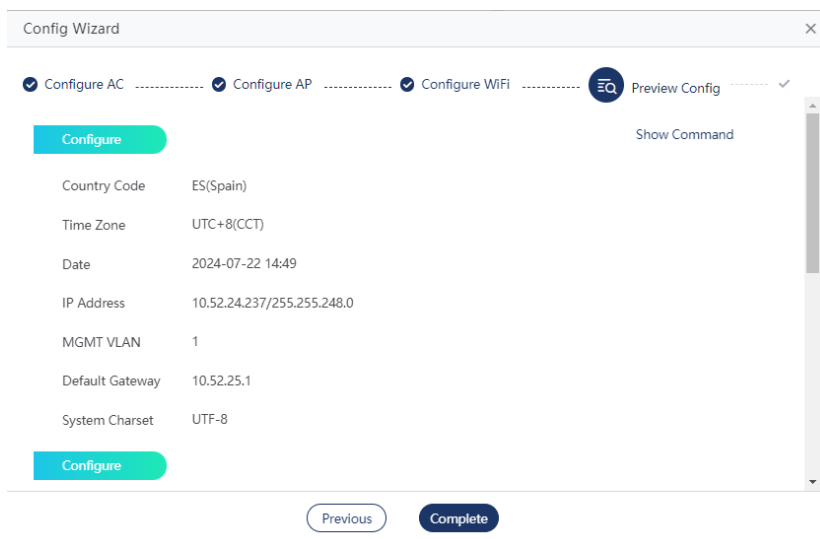
Previous Next

Parameter	Description
Dual Radio Into One	It is enabled by default, indicating that one Wi-Fi network broadcasts both 2.4 GHz and 5 GHz signals. If it is disabled, two Wi-Fi networks are configured, one for 2.4 GHz signals and the other for 5 GHz signals.
SSID	Set the SSID.
Encryption Type	Open: No encryption method is configured. No password is required when the STA connects to the Wi-Fi network.

	<p>WPA/WPA2-PSK: The WPA mode with a pre-shared key features high security and easy setup, applicable to homes and small-sized enterprises.</p> <p>WPA3-Personal: Compared with WPA2, it is more secure and capable of preventing dictionary attacks.</p>
Forwarding Mode	<p>Centralized Forwarding: All data is routed through the AC before being forwarded to other devices. This mode is configured by default.</p> <p>Local Forwarding: The data is forwarded to other devices directly from the switch, reducing the load on the AC.</p>
STA is in VLAN	Configure the VLAN for the STA.
STA Address Pool	STA address pool can be configured either on the AC or on other devices. If you choose to configure it on other devices, configure and verify the address pool settings on those devices after completing this process.

2.2.4 Preview Config

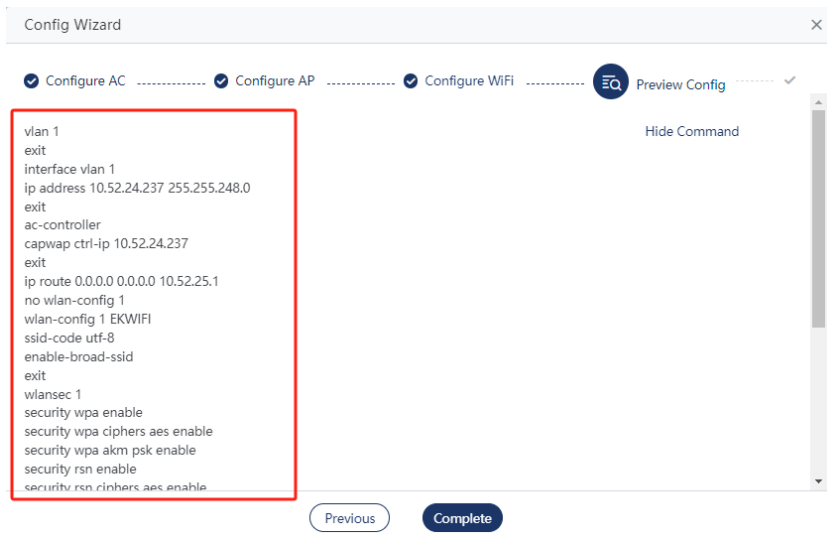
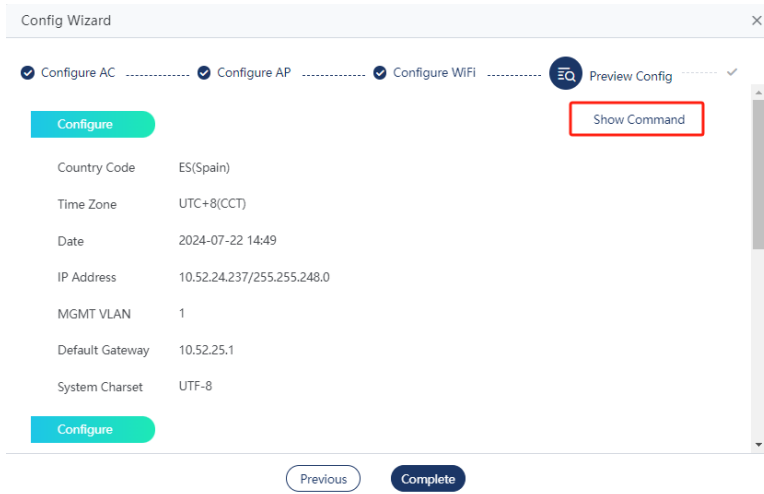
This process allows users to verify the configurations. Check the CLI commands for the current configurations by clicking **Show Command**.



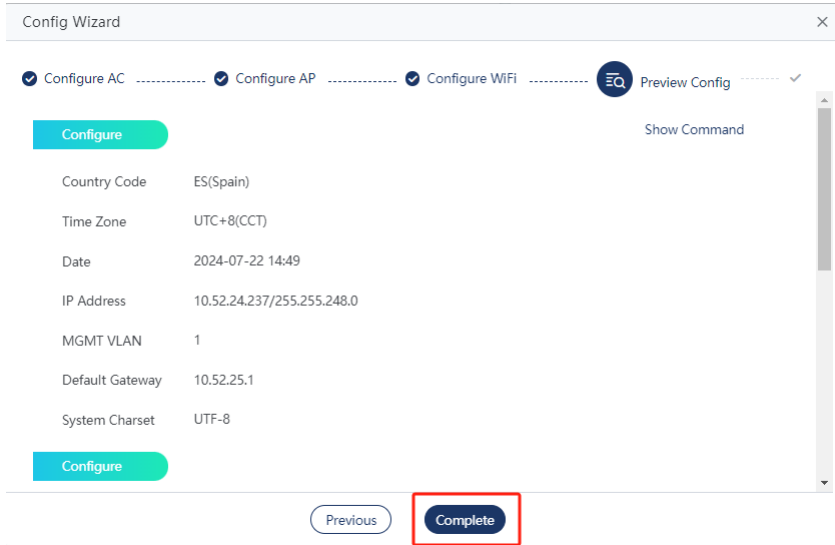
Configure	
AP is in VLAN	1
Interface Address	10.52.24.237/255.255.248.0
AP Address Pool on	Other Device
AC Tunnel Address	10.52.24.237

Configure	
SSID	EKWIFI
Encryption Type	WPA/WPA2-PSK
WiFi Password	ekwifisds
Forwarding Mode	Centralized Forwarding
STA is in VLAN	1
Interface Address	10.52.24.237/255.255.248.0
STA Address Pool	Other Device

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



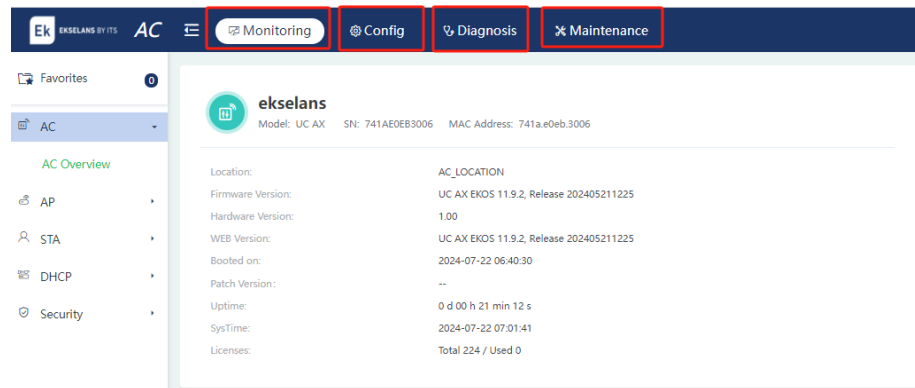
Once you confirm the configuration, click **Complete** and a window pops up, displaying the network deployment. You can test the network connectivity with the external network through network detection.



3 Web GUI

3.1 Home Page

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



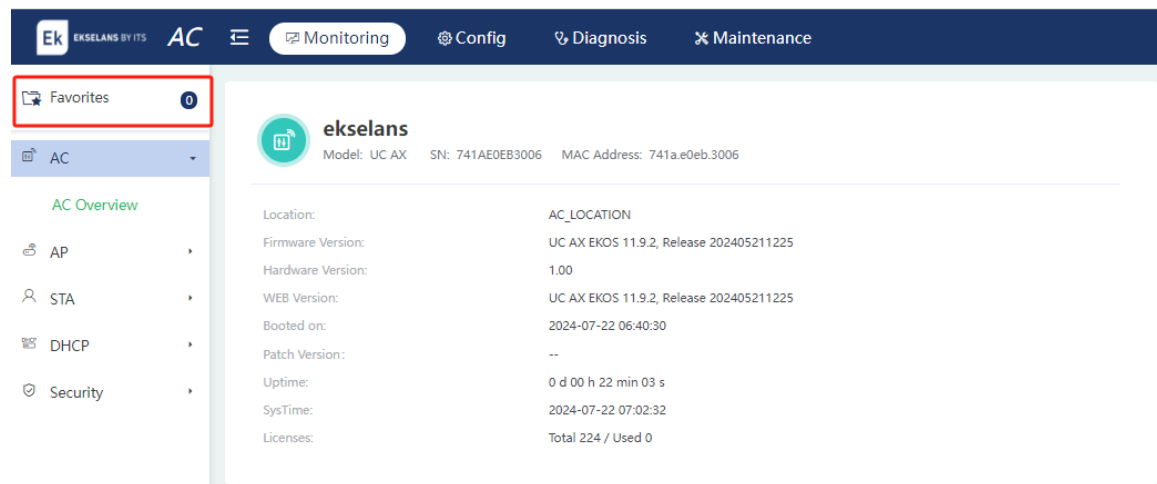
3.2 Favorites

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

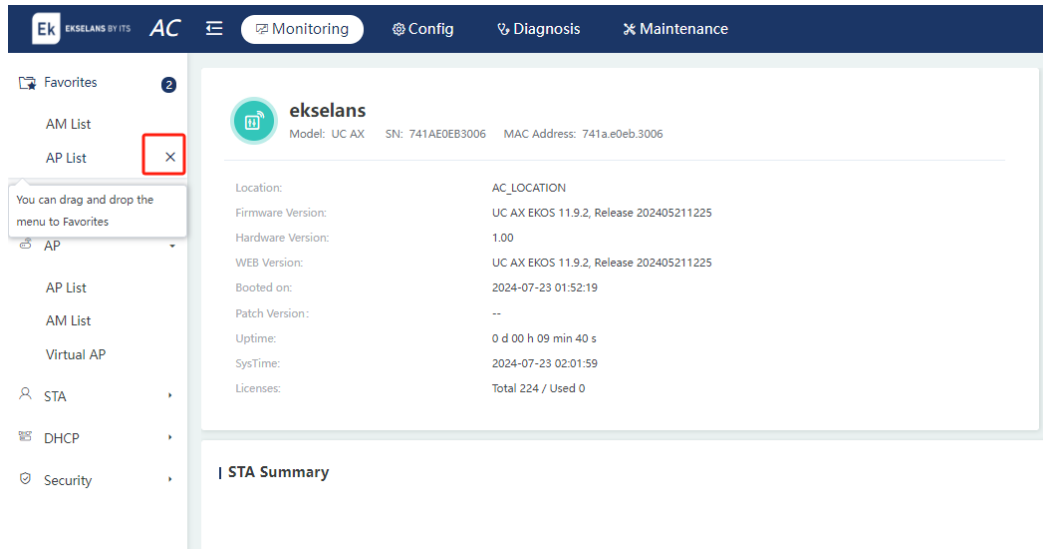
Note

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

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



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



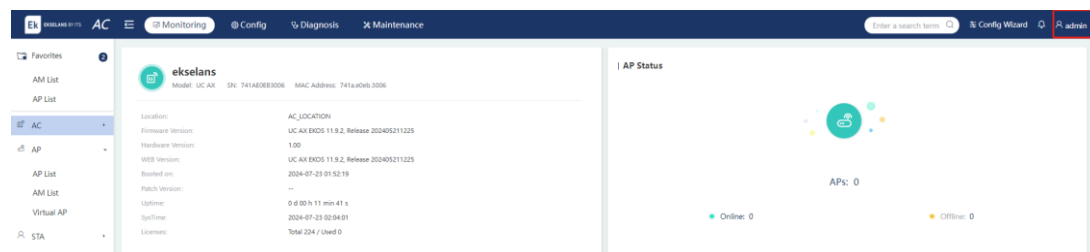
3.3 Menu Search Bar

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

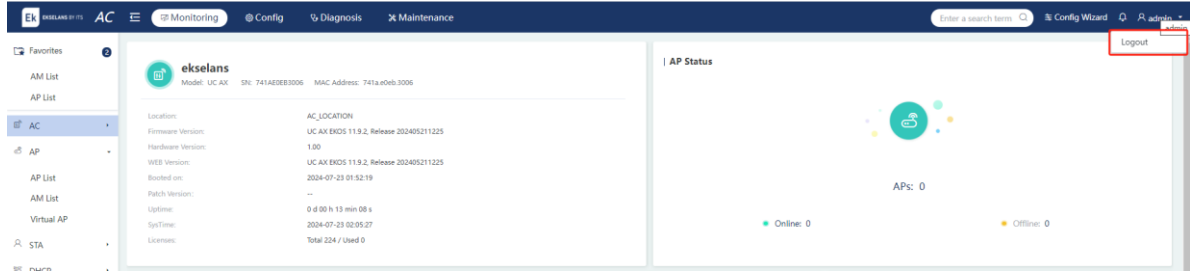


3.4 Other Functions

(1) Displaying the Current Account



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



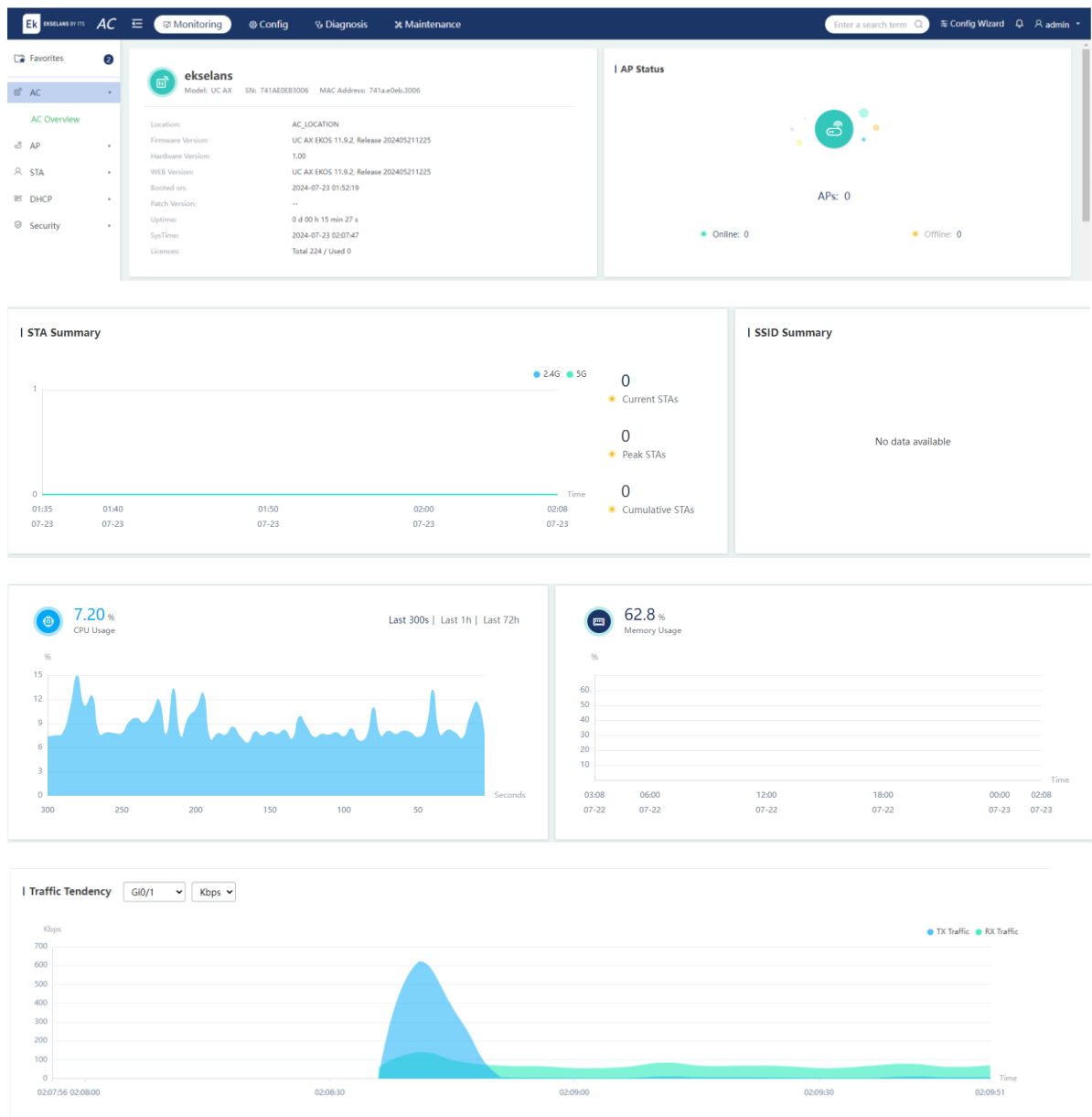
4 Monitoring

4.1 AC

4.1.1 Overview

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

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



Interface	Link Status	MGMT Status	Interface Info	Description
Gi0/2	Down	Up		
Gi0/3	Down	Up		
Gi0/4	Down	Up		
Gi0/5	Down	Up		
Gi0/6	Down	Up		
Gi0/7	Down	Up		
Gi0/8	Down	Up		

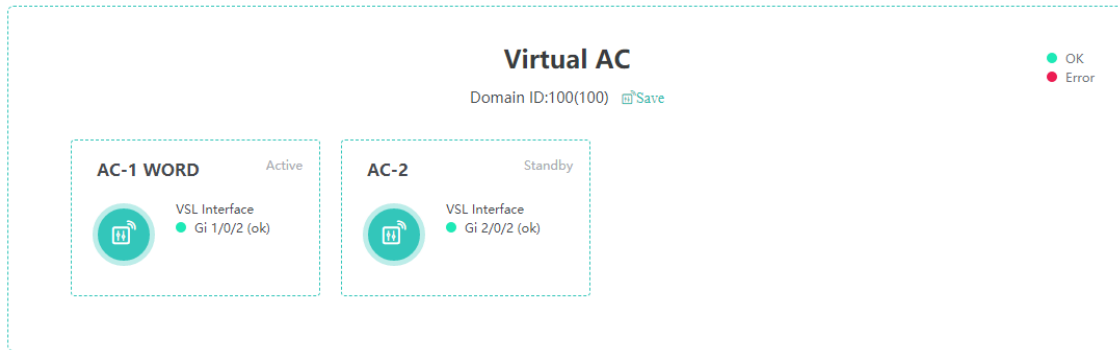
4.1.2 Virtual AC

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

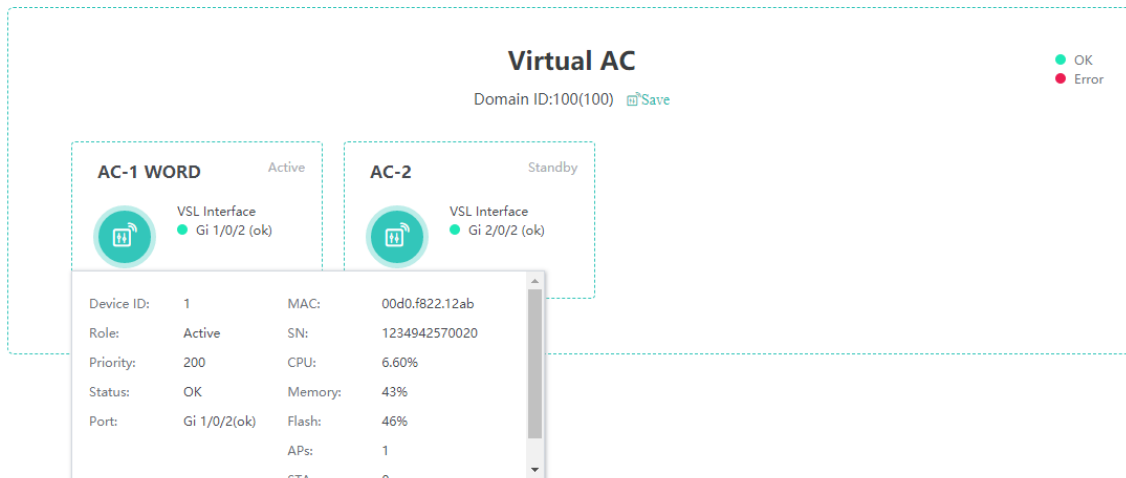
Note

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

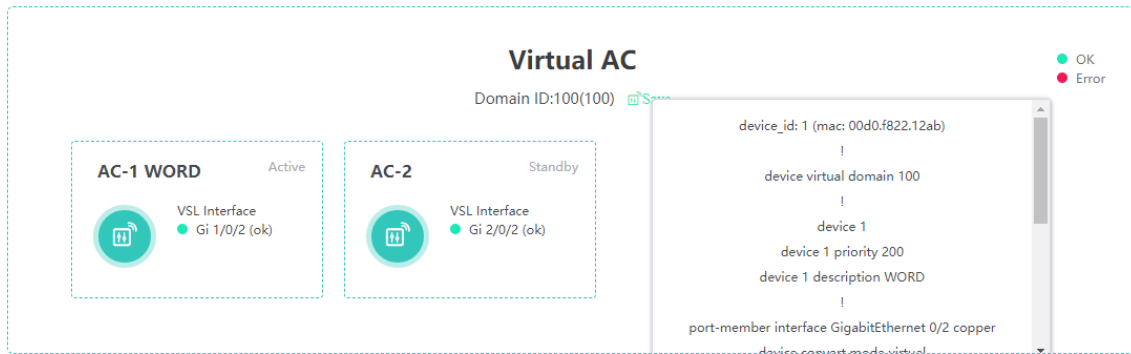
The virtual AC page displays the current virtual AC members and their basic information.



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



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

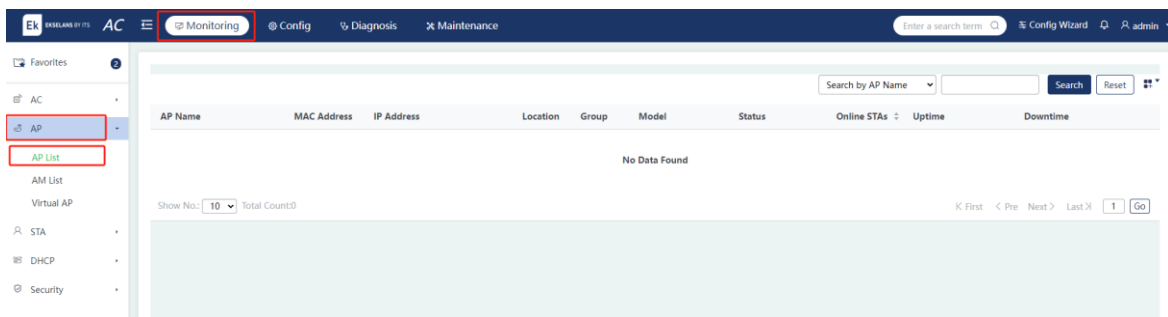


4.2 AP

4.2.1 AP List

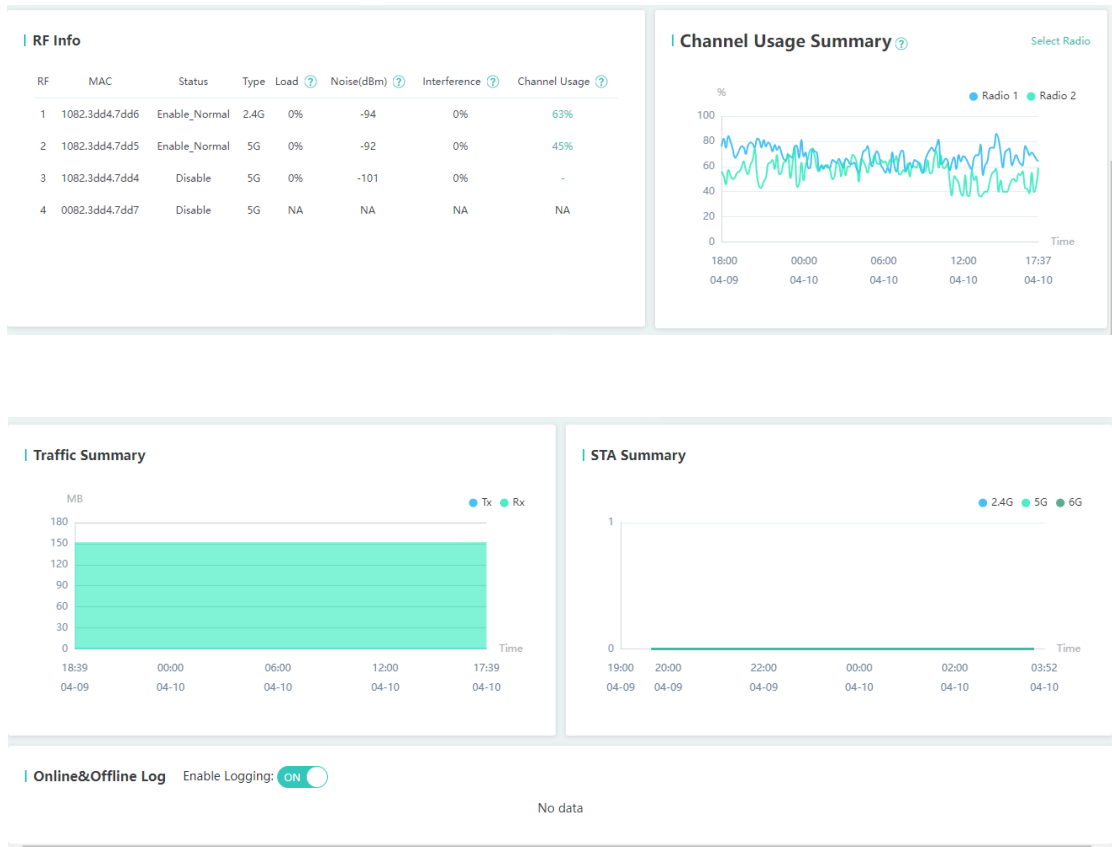
Choose **Monitoring > AP > AP List**.

The AP list displays the basic information, and RF and model details of APs connected with the device.



- (1) Searching for AP: Enter keywords in the search bar and click **Search**. Click **Reset** to clear the search criteria and display the list of all APs. If an AP is offline, its details cannot be viewed.
- (2) To display additional information about the APs, click and select the information you wish to view.
- (3) Viewing AP Details: Click the AP name to redirect to the AP page.

The RF information, channel usage summary, traffic summary, and other information are displayed on the AP page.



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

4.2.2 Virtual AP

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

This page displays details of virtual APs.

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

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

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

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

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

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

0074.9c23.e2dbDetails X

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

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

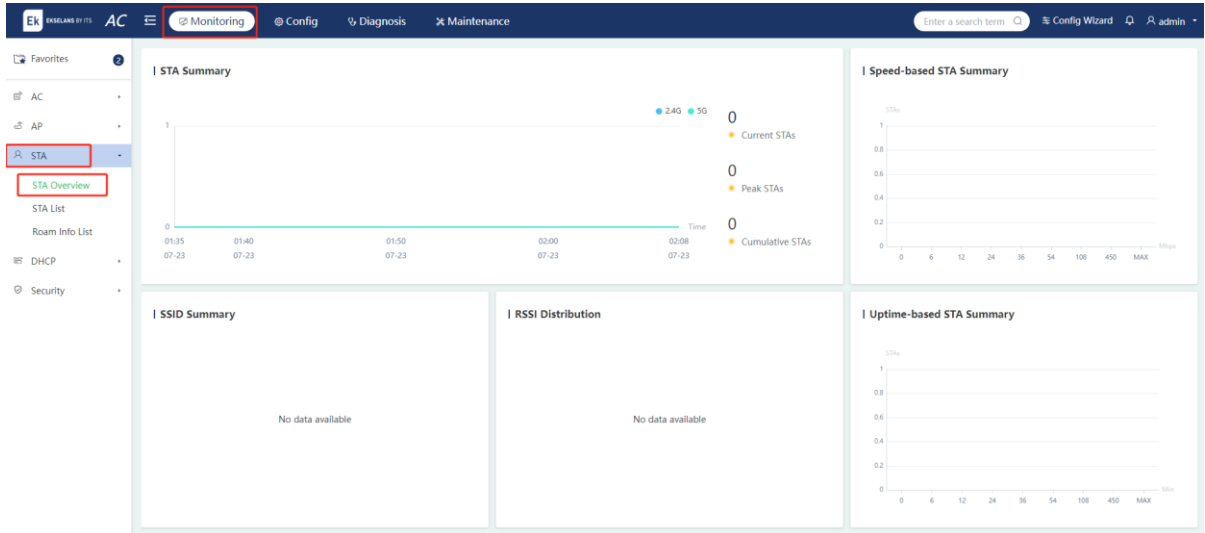
Show No.: Total Count:1 K First < Pre 1 Next > Last X

4.3 STA

4.3.1 Overview

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

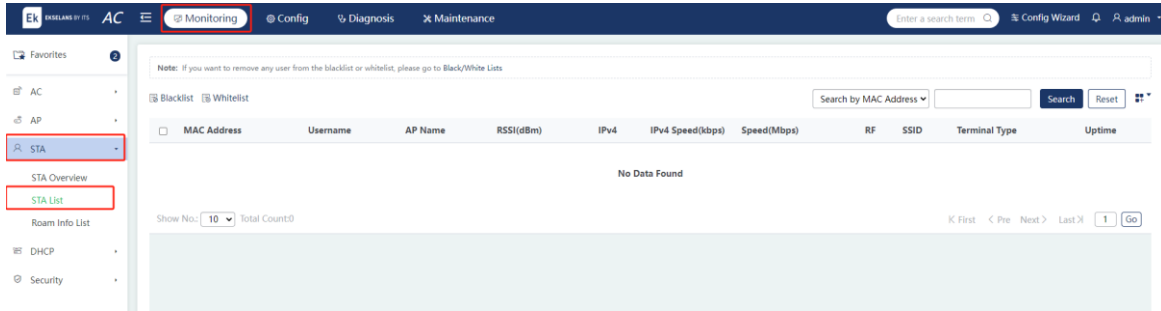
This page presents STA statistics from various perspectives, updated at an interval of 30s.



Page Name	Description
STA Summary	<p>Displays the summaries of STAs associated with 2.4 GHz, 5 GHz, and 6 GHz Wi-Fi respectively.</p> <p>Current STAs: Displays the number of current online STAs.</p> <p>Peak STAs: Displays the maximum number of online STAs within 24 hours.</p> <p>Cumulative STAs: Displays the cumulative number of online STAs within 24 hours. (The STAs that log in multiple times are counted only once.)</p>
Speed-based STA Summary	Displays the speed-based STA summary in a bar chart. Click the bar to redirect to the STA list.
SSID Summary	Displays the proportion of STAs associated with different Wi-Fi networks. Click the pie chart to redirect to the STA list.
RSSI Distribution	Displays the proportion of STAs' RSSIs.
Uptime-based STA Summary	Displays the uptime-based STA summary in a bar chart. Click the bar to redirect to the STA list.

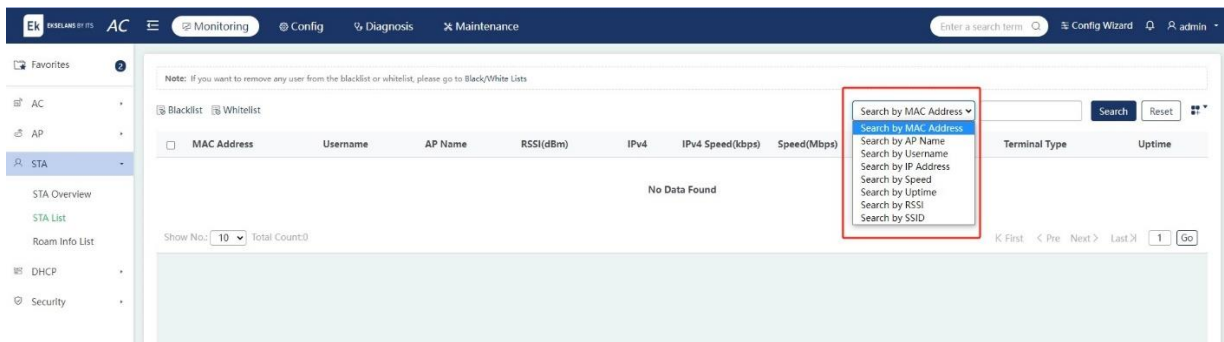
4.3.2 STA List


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

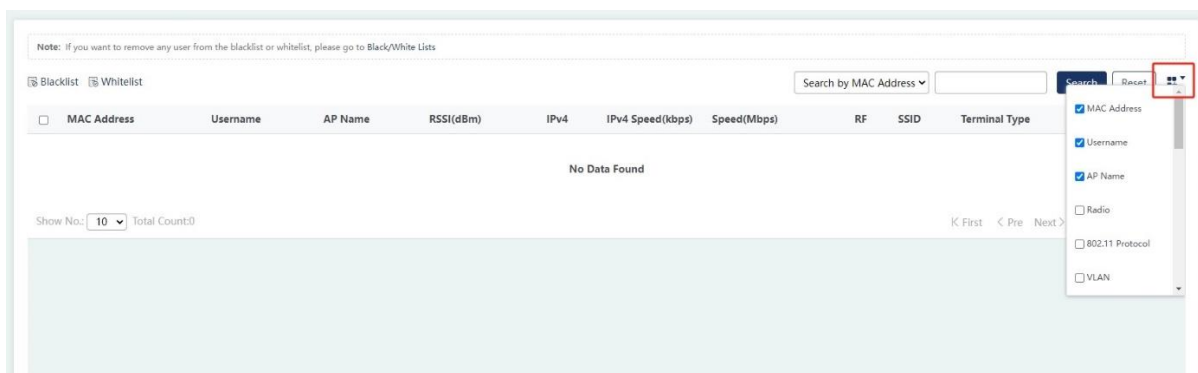


1. Searching for STAs

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



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



2. Adding to the Blacklist or Whitelist

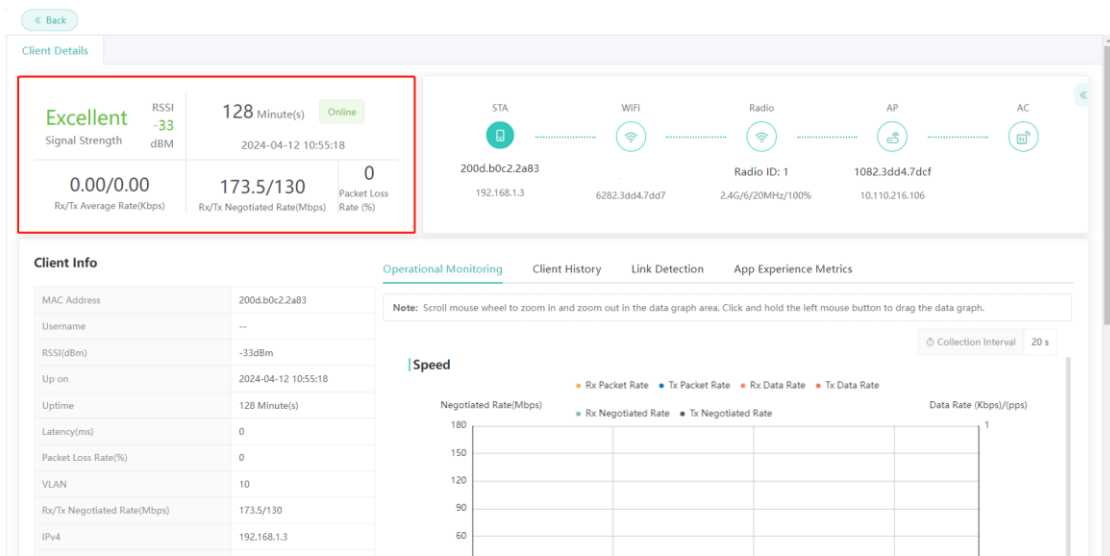
Select the STAs you want to add to the blacklist and click **Blacklist**.

3. View Client Details

Click **MAC Address** to go to the **Client Details** page. On the **Client Details** page, you can view the network information, topology, client information, speed tendency, RSSI, packet loss/retry rate, client history, link detection, and app experience metrics.

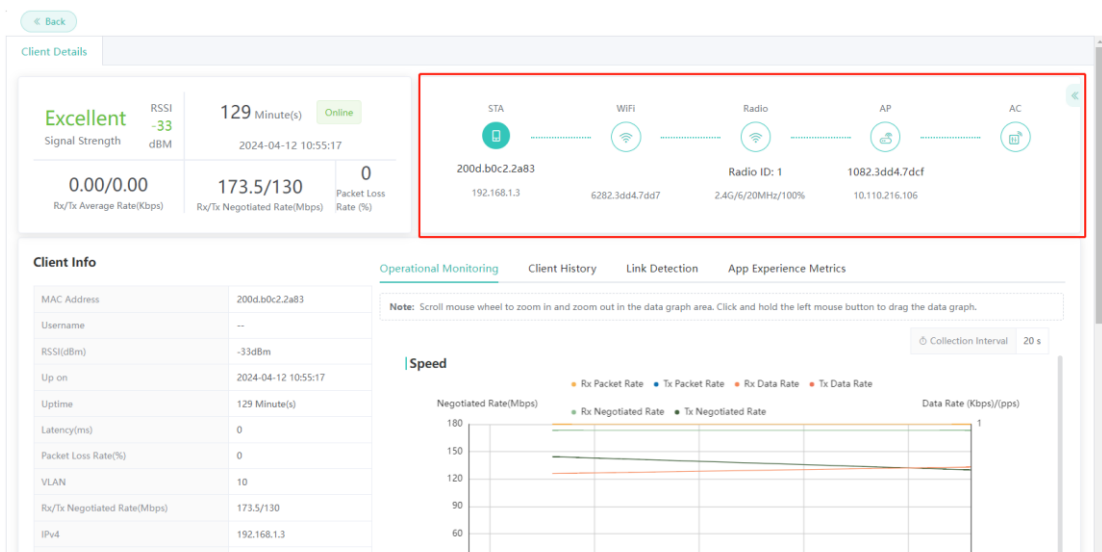
(1) Network Information

In the upper left corner of the **Client Details** page, you can view the RSSI, uptime, Rx/Tx average rate, Rx/Tx negotiated rate, and packet loss rate of the client.

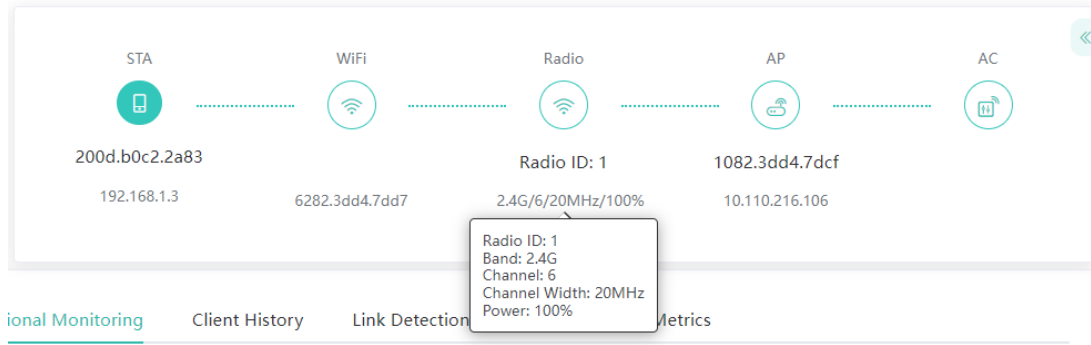


(2) Topology

In the upper right corner of the **Client Details** page, you can view the topology, including the Wi-Fi name, radio ID, AP, and AC associated with the STA.



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



Move the cursor to the icon in the upper right corner of the topology. Click **View Details** to view details about the radio, AP, and AC associated with the STA.

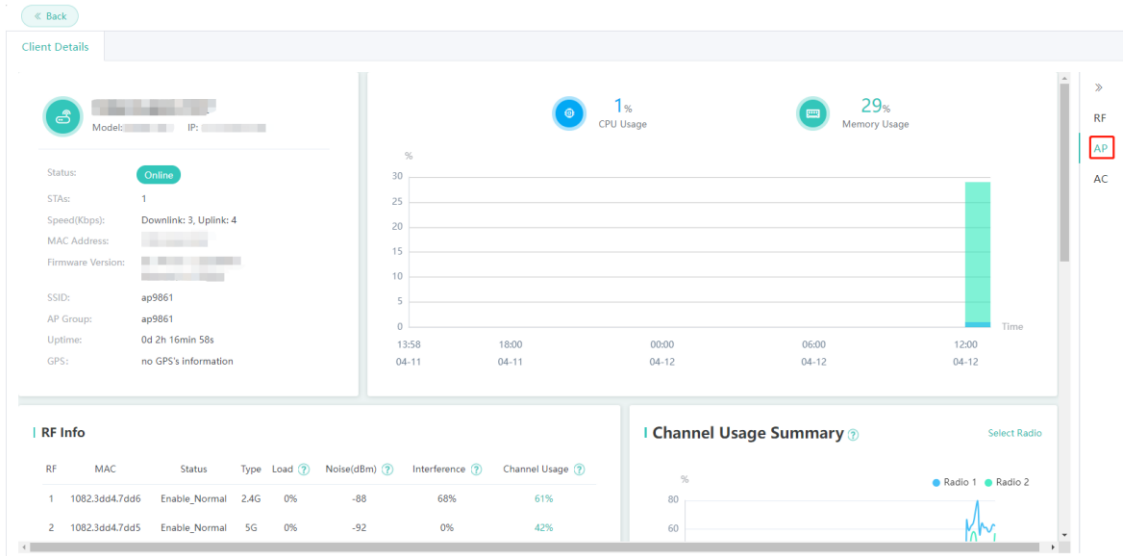
- Details about the radio associated with the STA:

The screenshot shows the 'Client Details' page for a radio. The 'RF Details' table is as follows:

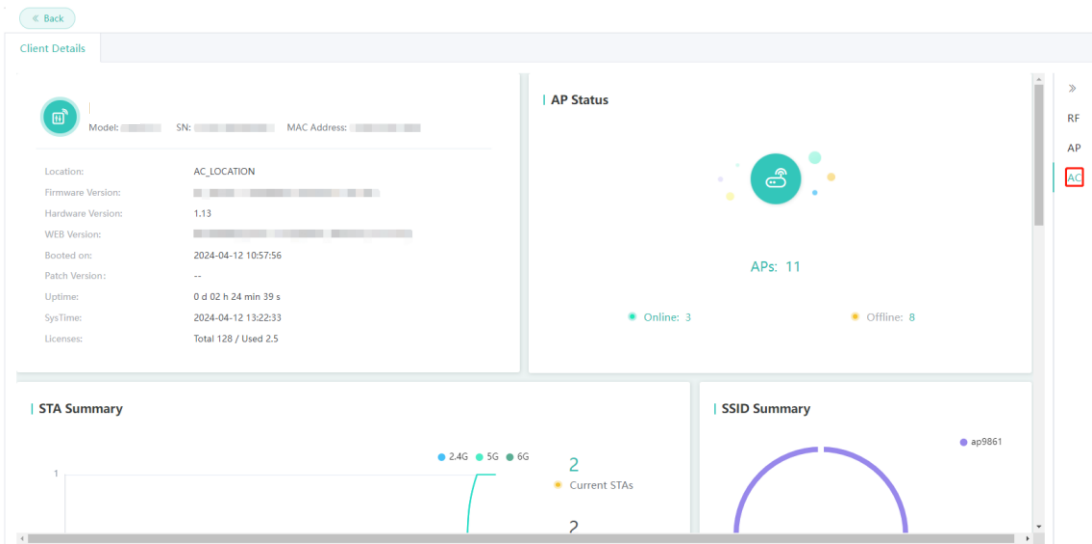
AP Name	1082.3dd4.7dcf
Radio ID	1
Radio Status	Enable
RF	2.4G
Wi-Fi Protocol Type	802.11b/g/n/ac
Work Mode	Access
Channel Width	20MHz
Channel	6
Power(%)	100%
Online STAs	1
Channel Usage(%)	61%
Transmit(%)	0%
Receive(%)	0%
Interfering(%)	61%
Free(%)	39%
Rx/Tx Rate(Kbps)	0.70 / 0.47

The 'Online STAs' graph shows a single data point at 2024/04/1 2 12:380. The 'Noise(dBm)' graph shows a value of approximately -100 dBm.

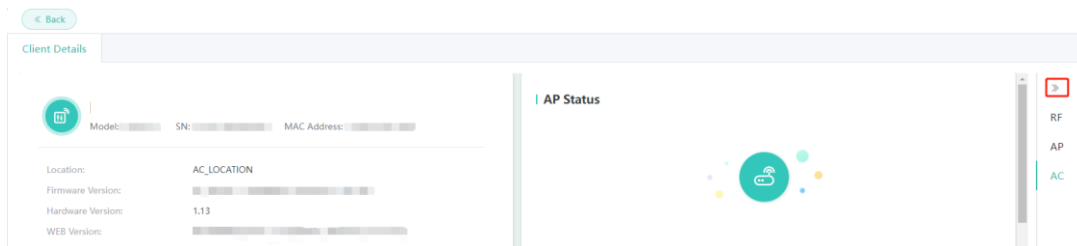
- Details about the AP associated with the STA:



- Details about the AC associated with the STA:

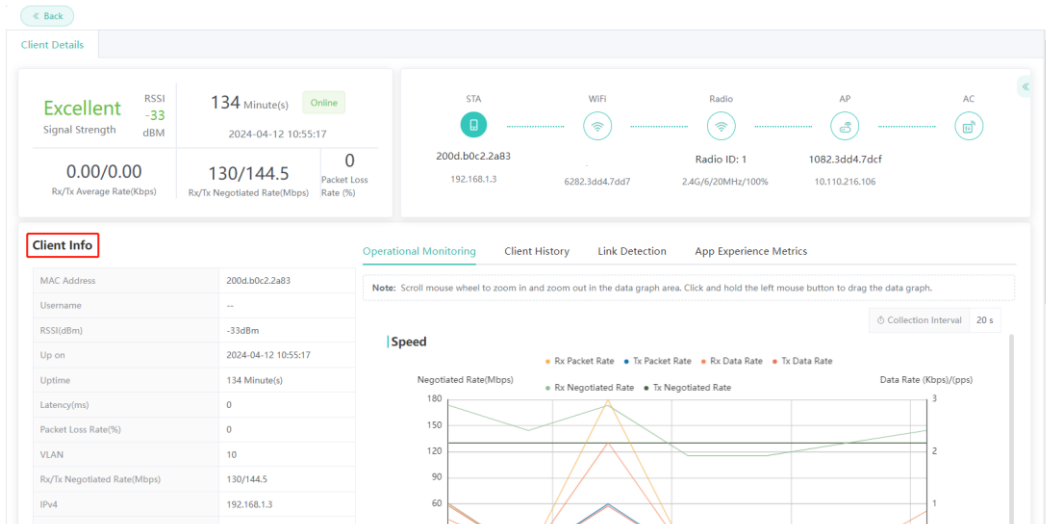


Click the icon to collapse the **RF**, **AP**, and **AC** details and return to the **Client Details** page.



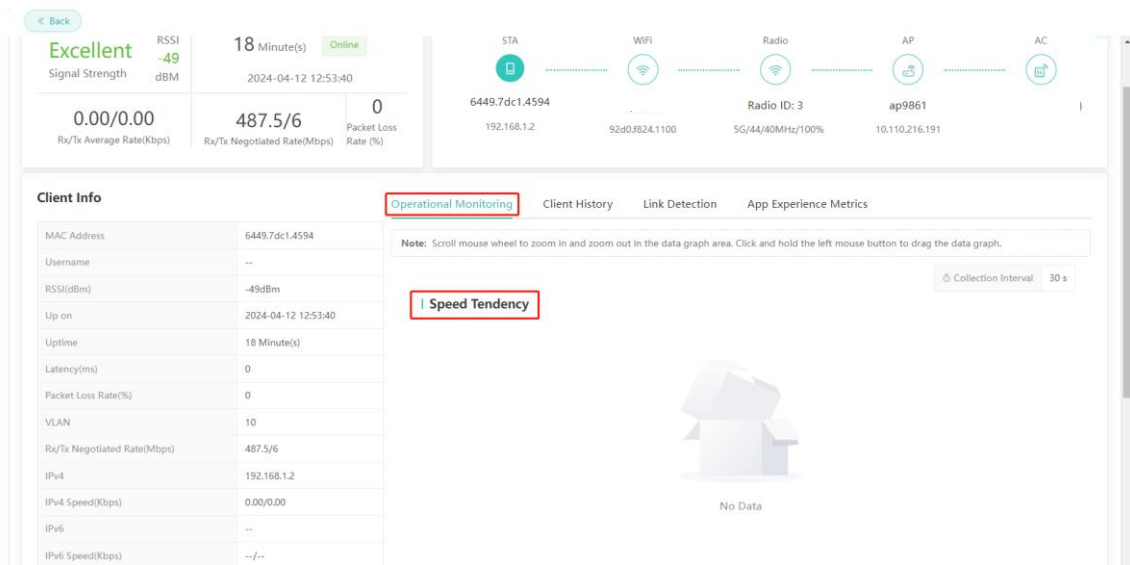
(3) Client Information

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

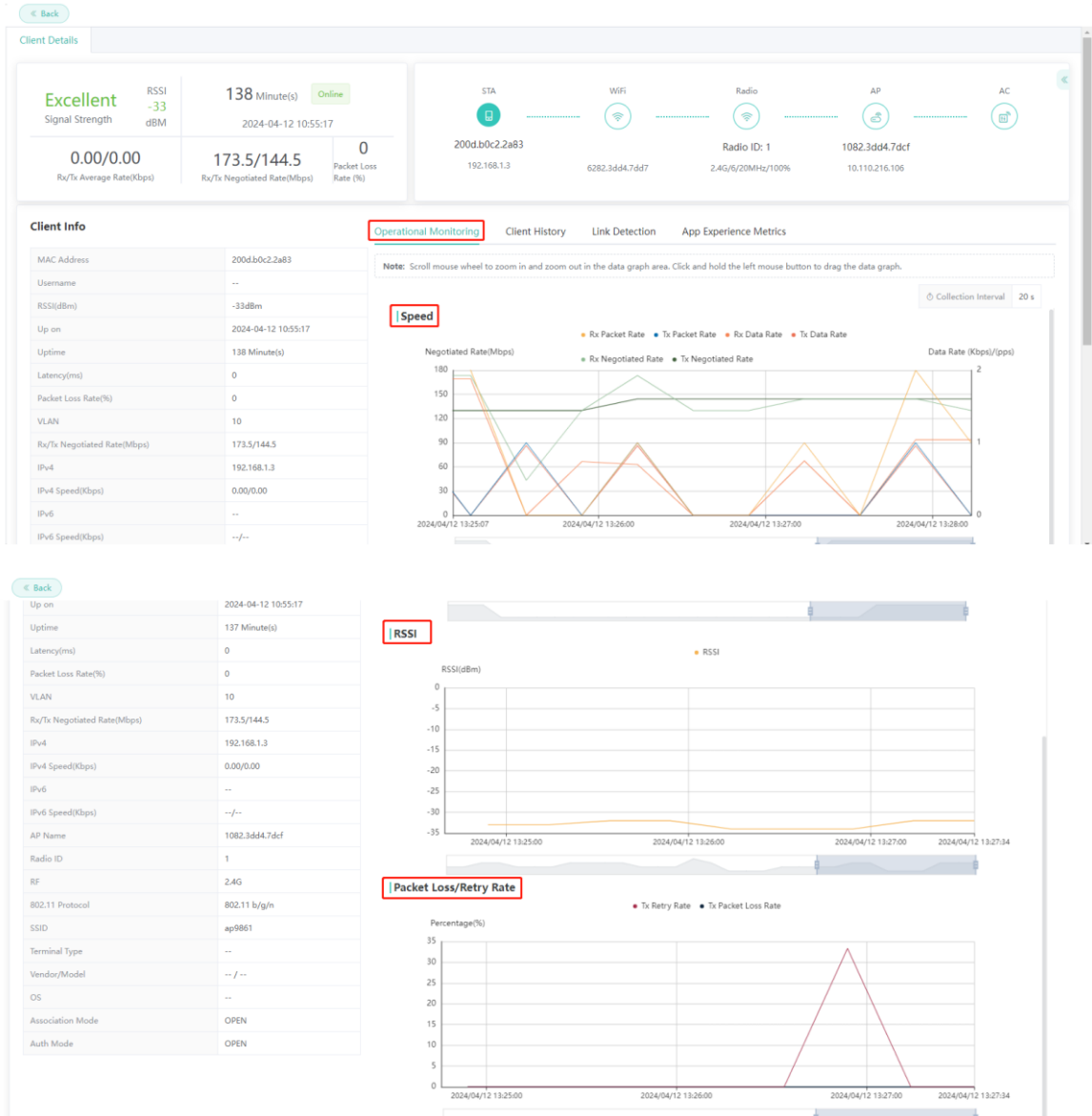


(4) Operational Monitoring

If the client is not enabled with high-frequency telemetry, the **Speed Tendency** chart of the client is displayed under the **Operational Monitoring** tab.

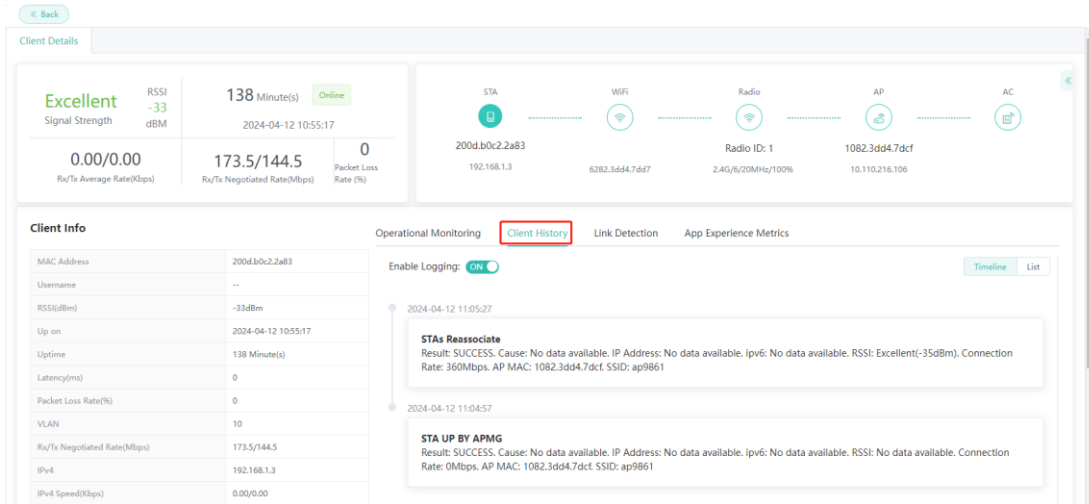


If the client is enabled with high-frequency telemetry and is in telemetry state, the **Speed**, **RSSI**, and **Packet Loss/Retry Rate** charts are displayed under the **Operational Monitoring** tab.



(5) Client History

The online and offline history of STAs is recorded and displayed under the **Client History** tab.

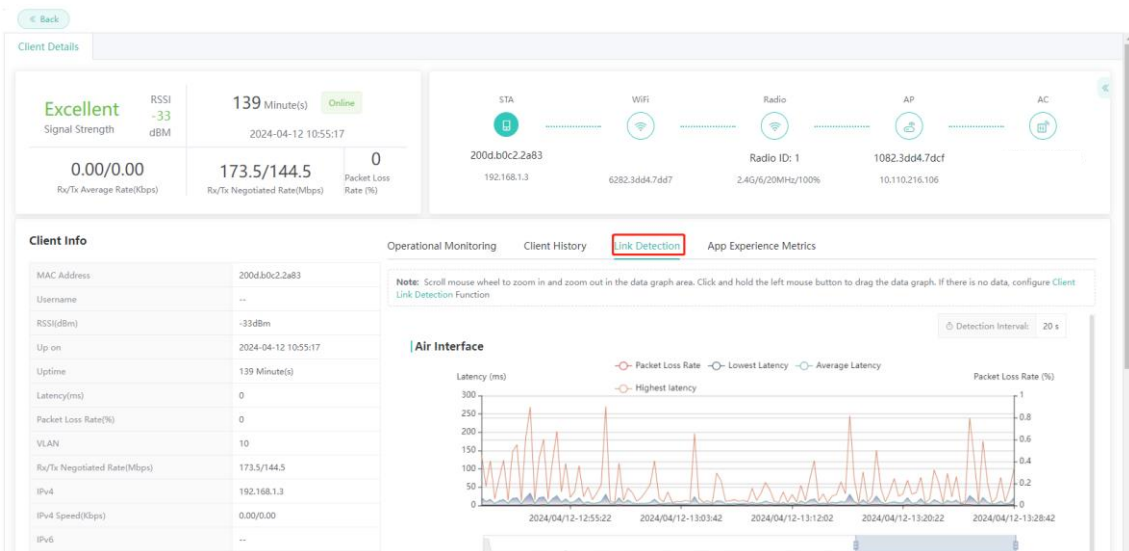


(6) Link Detection

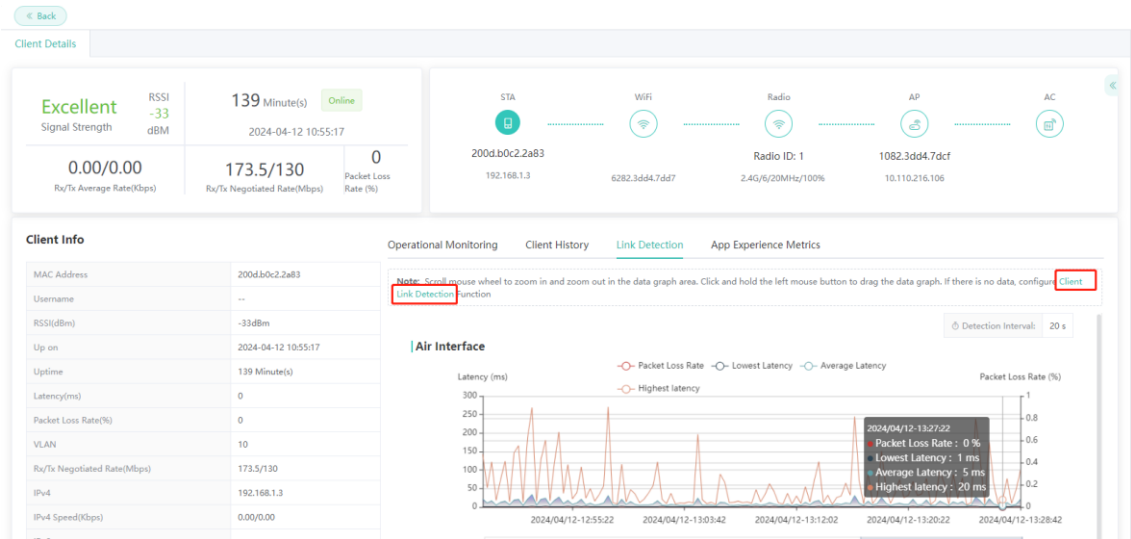
If the client is enabled with link detection, the **Packet Loss Rate, Lowest Latency, Average Latency, and Highest Latency** line charts of **Air Interface, Gateway, DHCP, and DNS** are displayed under the **Link Detection** tab. If the client is not enabled with link detection, no link detection information about the client is displayed under the **Link Detection** tab.

Note

Whether information about **Air Interface, Gateway, DHCP, or DNS** is displayed depends on the **Detection Target** configured by choosing **Diagnosis > STA Teach > Wlan-Sta-Link Check > Parameter Config**. For details, see: [Error! No se encuentra el origen de la referencia.](#)



To view the link detection data about the client, click **Client Link Detection**, or choose **Diagnosis > STA Teach > Wlan-Sta-Link Check** to enter the page and add the client. For details, see: [Error! No se encuentra el origen de la referencia.](#)

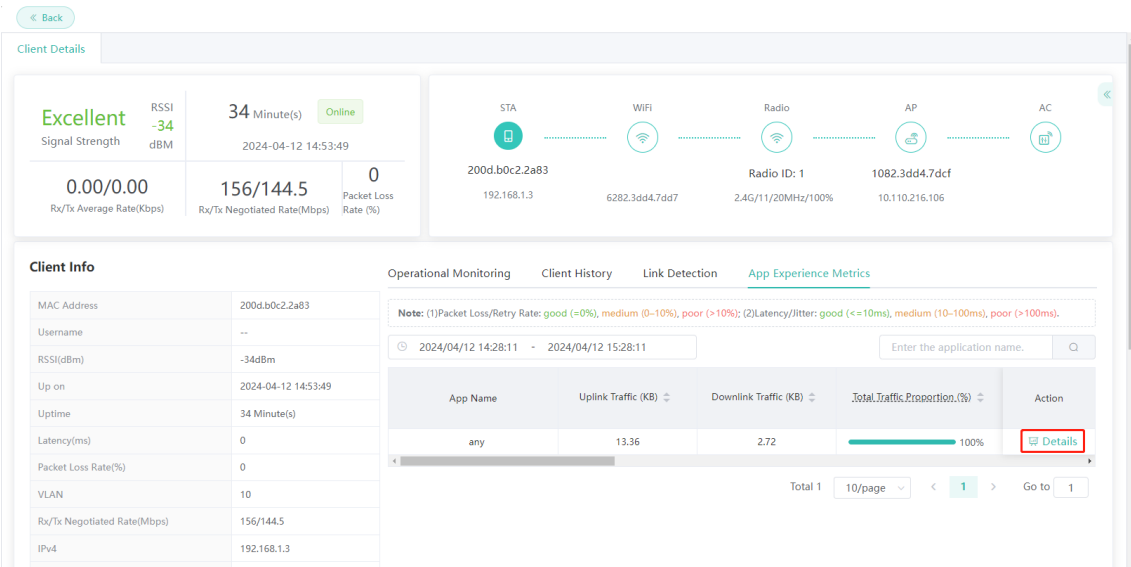


(7) App Experience Metrics

The traffic usage of various applications used by a user is displayed on the **App Experience Metrics** page. The list of applications used by a user in the last one hour is displayed by default (the time range can be customized).

Note

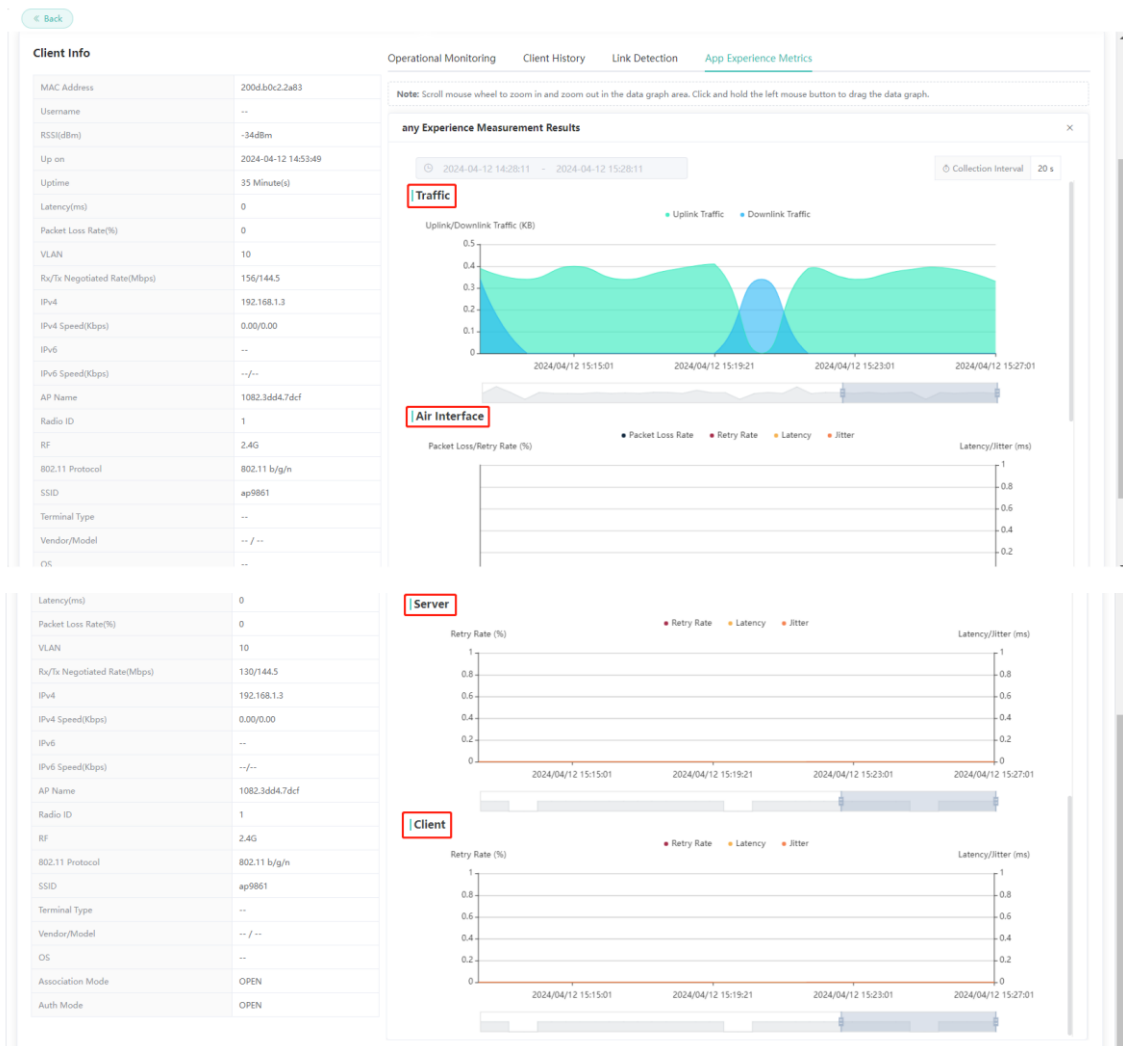
On the **STA List** page, only data about users whose MAC addresses marked with the high-frequency telemetry icon in the **MAC Address** column are displayed on this page.



Parameter	Parameter Description
Traffic	Displays the proportion of the total uplink and downlink traffic used by an

	application to the total traffic within the selected time period.
Server	Displays the latency, packet loss rate, and retry rate of TCP packets send from the AP to the server.
Client	Displays the latency, packet loss rate, and retry rate of TCP packets send from the AP to the client (different from the calculation model on the air interface side).
Air Interface	Displays the latency, packet loss rate, and retry rate of only downlink wireless request or response packets send from the AP to the client.

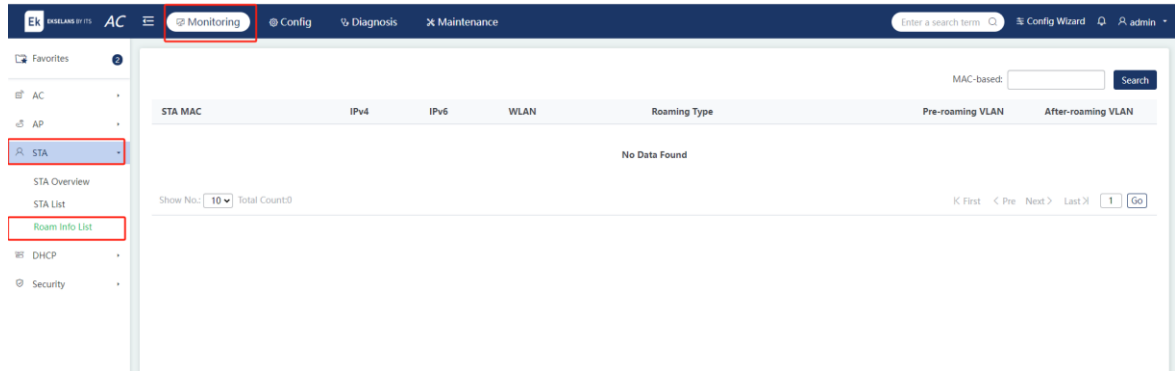
Click **Details** of a specified application to view the traffic trend chart of the application.



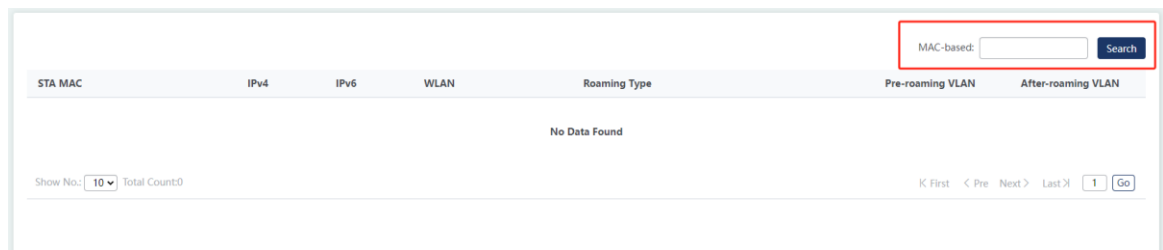
4.3.3 Roam Info List

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

The roam info list displays the list of roaming devices.



Enter the MAC address in the search bar and click **Search**. Click **Reset** to clear contents in the search bar.

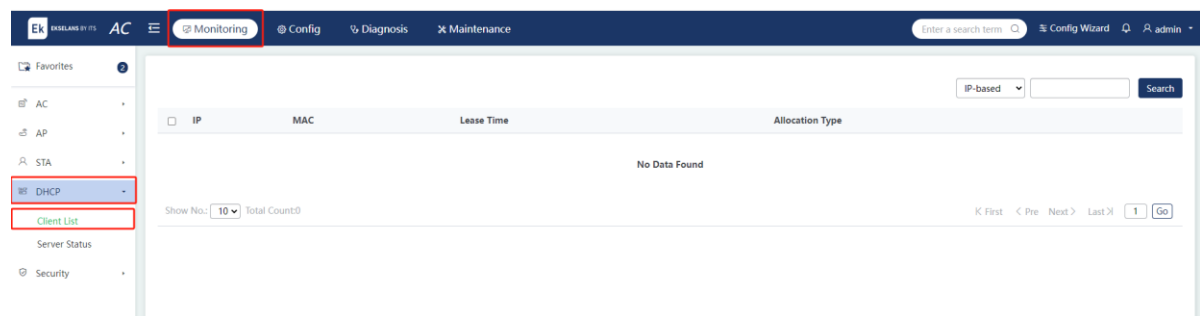


4.4 DHCP

4.4.1 DHCP Client List

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

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



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

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

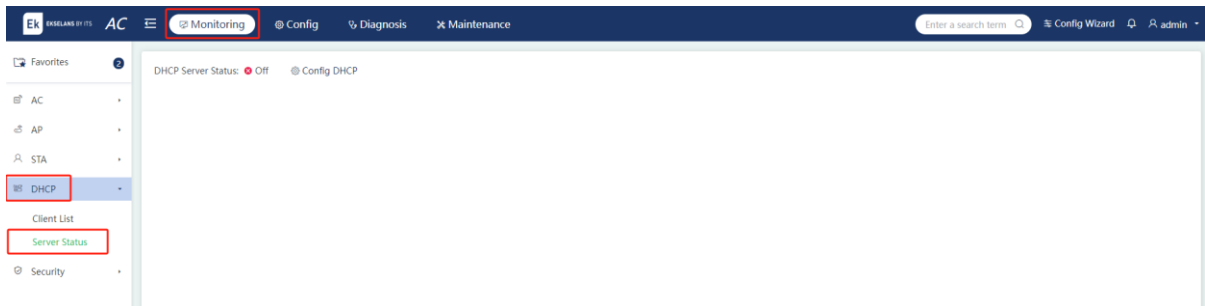
Show No.: 10 Total Count:147

K First < Pre 1 2 3 Next > Last 1 GO

4.4.2 DHCP Server Status

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

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

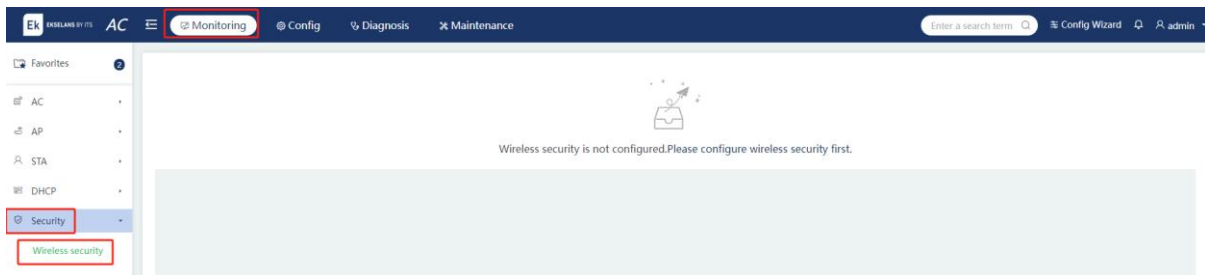


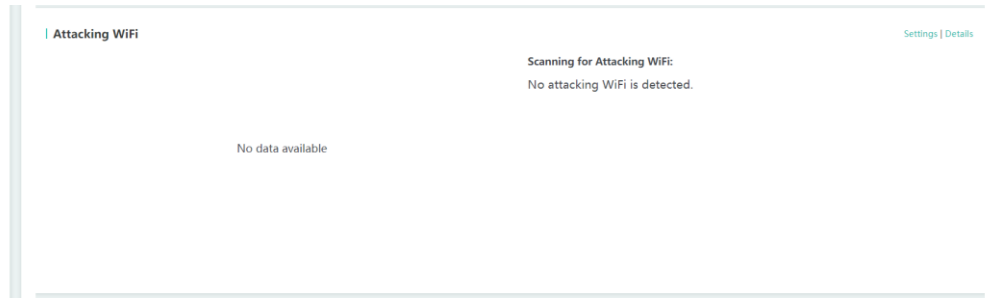
4.5 Security

4.5.1 Wireless Security

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

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





(1) Dangerous Wi-Fi List

Click **Details** on the **Dangerous WiFi** page to redirect to the **Dangerous WiFi List** page.

This function allows you to:

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

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

(2) Attacking WiFi

Click **Details** on the Attacking WiFi page to redirect to the Attacking WiFi List page.



This function allows you to:

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

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

5 Configuration


5.1 WLAN

5.1.1 Add WiFi

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

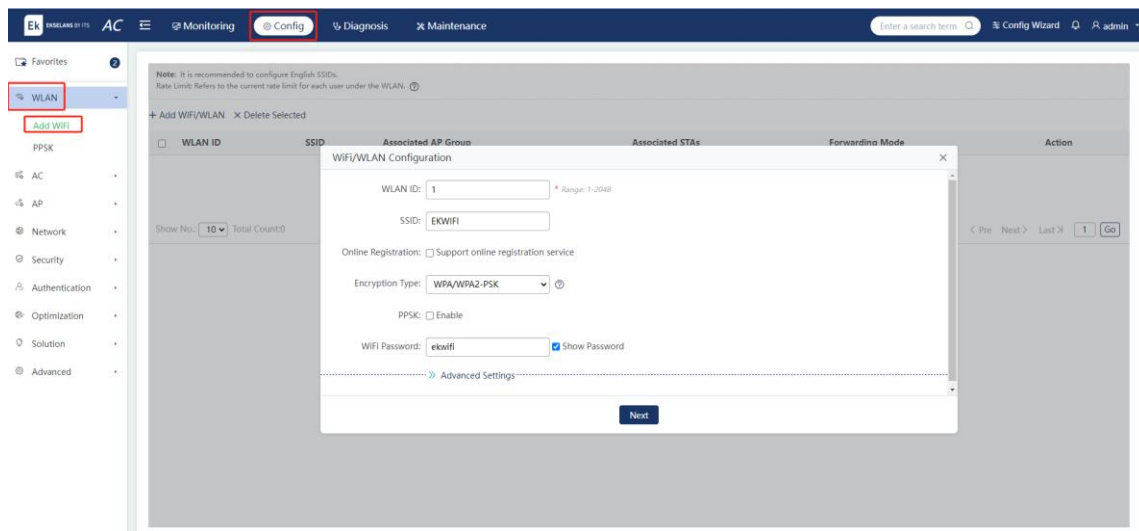
The Wi-Fi allows wireless STAs to be associated with the AP for network access. Multiple Wi-Fi networks can be added or deleted.

Note

- Click  to view the typical data rates in common scenarios.

1. Adding Wi-Fi

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



Parameter	Description
Online Registration	Enable or disable online registration.

<p>Encryption Type</p>	<p>Open: Indicates no encryption. No password is required when the STA connects to the Wi-Fi network.</p> <p>WPA/WPA2-PSK: Indicates WPA mode with a pre-shared key featuring high security and easy setup, applicable to homes and small-sized enterprises.</p> <p>WPA/WPA2 802.1X: Indicates WPA or WPA2 mode that implements identity authentication and key generation through a RADIUS server. Ordinary users are not advised to adopt this mode as it requires an exclusive authentication server.</p> <p>WPA2 802.1X: Indicates WPA2 mode that implements identity authentication and key generation through a RADIUS server.</p> <p>WPA2/WPA3: Indicates WPA2-WPA3 hybrid mode, which is determined by the STA.</p> <p>WPA3-PERSONAL: Provides higher security than WPA2 and effectively prevents dictionary attacks.</p> <p>WPA3-ENTERPRISE-CCMP256: Configures WPA3-Enterprise mode with GCMP-256 encryption, providing additional protection for networks transmitting sensitive data. It is applicable to data-sensitive networks like government or financial systems.</p> <p>WPA3-ENTERPRISE-CCMP128: Configures WPA3-Enterprise mode with CCMP-128 encryption, providing additional protection for networks transmitting sensitive data. It is applicable to data-sensitive networks like government or financial systems.</p>
<p>Packet Forwarding</p>	<p>Central Forwarding: All data is routed through the AC before being forwarded to other devices. This mode is configured by default.</p> <p>Local Forwarding: The data is forwarded to other devices directly from the switch, reducing the load on the AC.</p>
<p>SSID Code</p>	<p>UTF-8: You are advised to select utf-8, as most STAs support UTF-8 encoding by default.</p> <p>GBK: Some STAs, PCs, and Network Interface Cards (NICs) support GBK encoding.</p> <p>You can select encoding modes as required.</p>
<p>Hide SSID</p>	<p>If you enable Hide SSID, the SSID is not displayed on the STA. You can only find the SSID through searching.</p>
<p>STA Limit</p>	<p>Configure the maximum number of STAs that can be associated with this Wi-Fi. It is not configured by default, implying that there is no limit.</p>

Network OFF Period	Configure a period when the Wi-Fi is turned off. The default value is Never . Configure a period to turn off the Wi-Fi when it is necessary in specific scenarios.
NAS ID	Configure the NAS ID for the WLAN by entering a string of up to 32 bytes without spaces.
5G-prior Access	If this feature is enabled, the STA logs in to 5G networks preferentially. It is disabled by default.

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

×
Network Access Configuration

Associated AP Group ?	STA VLAN ID ?	STA DHCP Service ?	Network Type	Support Radio ?	Action
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Default</div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">ID</div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"></div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">2.4G&5G</div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"></div>	+ Add

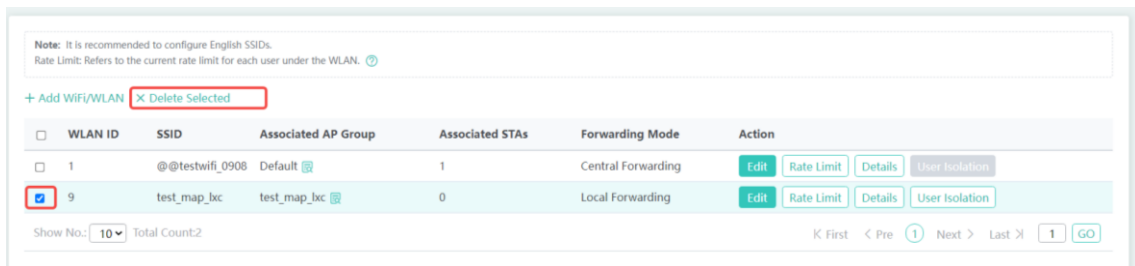
Finished
Previous

Parameter	Description
Associated AP Group	Specify which APs transmit the signals for this Wi-Fi. Typically, a single Wi-Fi hotspot's signal is broadcast by multiple APs. These APs are organized into one group for easy management. If no AP group is configured, all APs transmit the Wi-Fi signal by default.
STA VLAN ID	Enter the VLAN to which the STAs of this Wi-Fi belong.
STA DHCP Service	<p>The STAs connecting to this WLAN network can be allocated with IP addresses from an address pool that is configured on the local device or other devices. It is configured on other devices by default. If you choose to configure the address pool on the local device, click STA DHCP Service to redirect to the Configure DHCP on AC page.</p> <hr/> <p>i Note</p> <p>The IP addresses assigned by DHCP to STAs should be on the same network segment as the STA VLAN.</p>

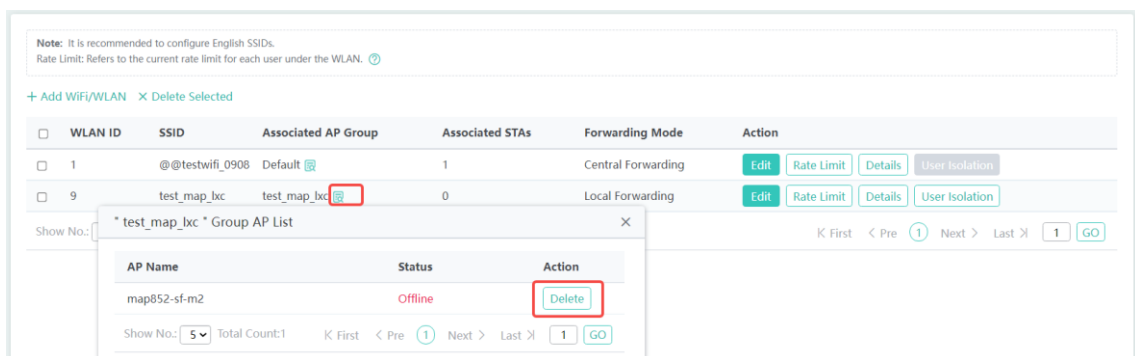
Network Type	Specify the network types supported by this Wi-Fi. By default, it supports both 2.4 GHz and 5 GHz bands.
Support Radio	Specify the radios supported by the AP for transmitting the Wi-Fi signal. All radios are supported by default.

2. Deleting WLAN

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

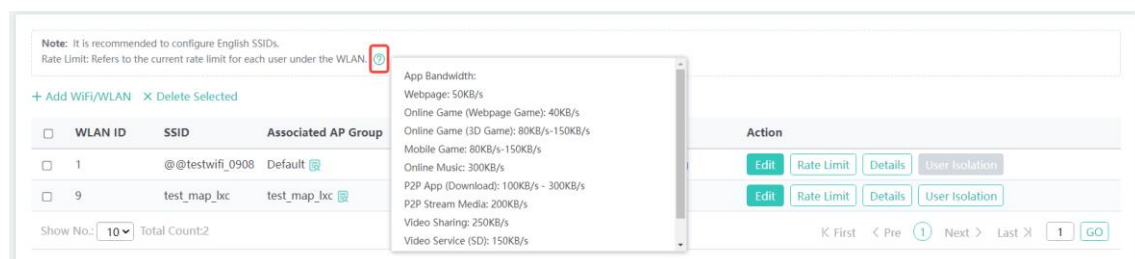


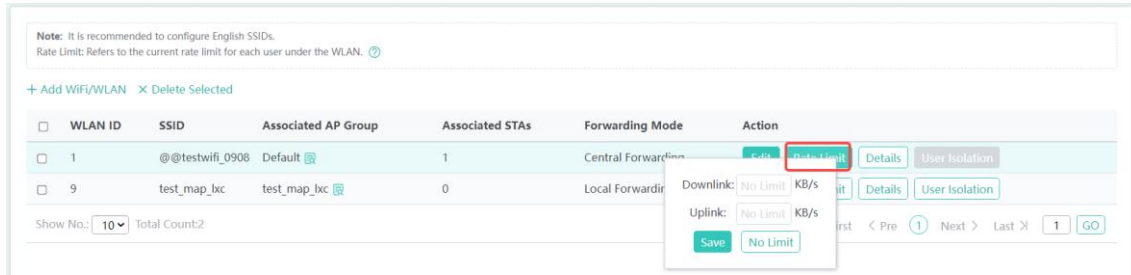
- (1) Viewing the associated AP group: Click in the **Associated AP Group** column to display or delete APs in the AP group.



3. Rate limiting

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

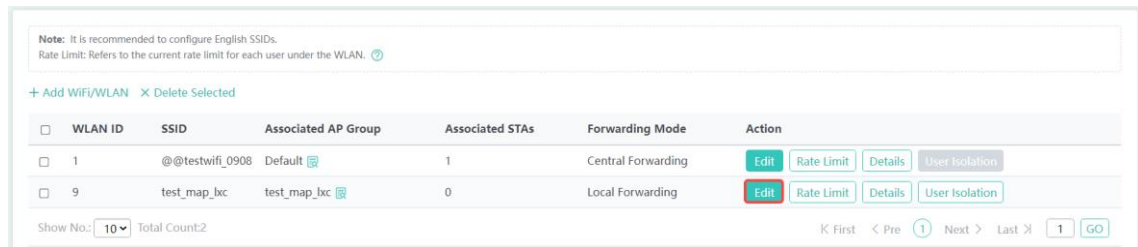




4. Editing WLAN

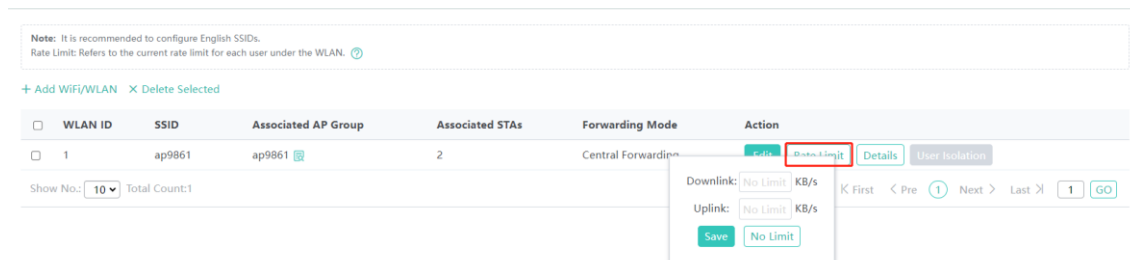
(1) Editing the information about the added WLAN

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



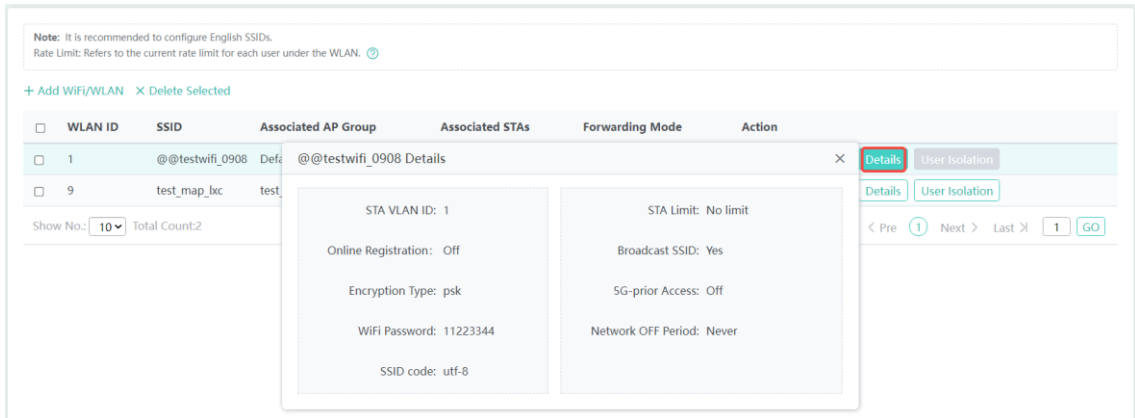
(2) Setting the rate limit for the added WLAN

To set upload and download rate limits for the added WLAN, click the icon to view the bandwidth required in common application download scenarios. Click **Rate Limit**. On the displayed page, set the maximum upload and download rates, and click **Save**.



(3) Viewing WLAN details

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

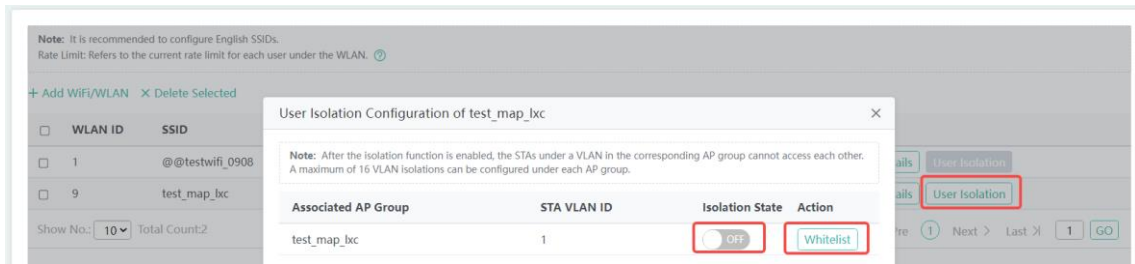


(4) Configuring user isolation

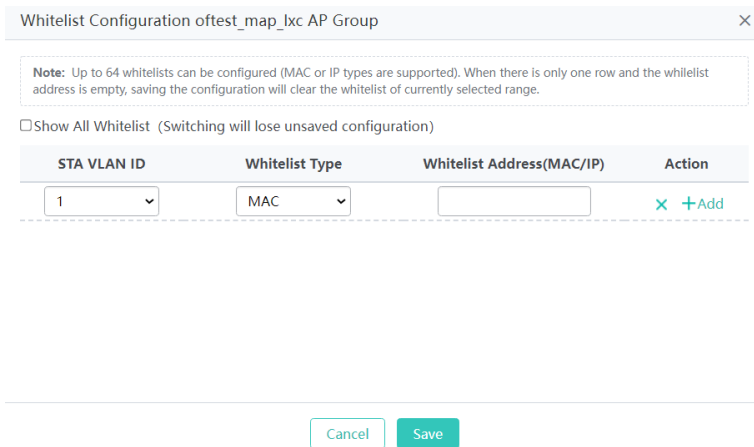
SSID-based isolation is equivalent to AP group-based VLAN isolation. Click **User Isolation** in the **Action** column and a window pops up, displaying the **User Isolation Configuration** page.

Currently, the user isolation configuration is only supported in the local forwarding mode.

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



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



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

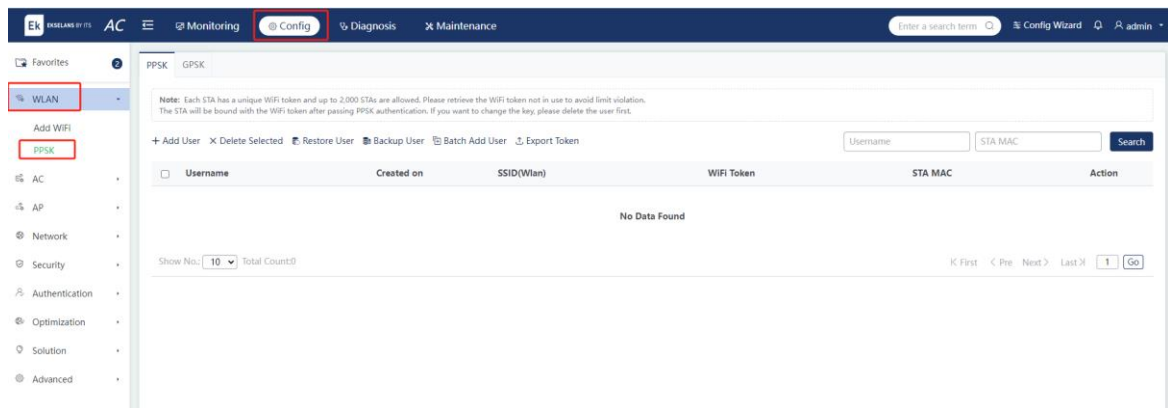
5.1.2 PPSK

Choose **Config > WLAN > PPSK**.

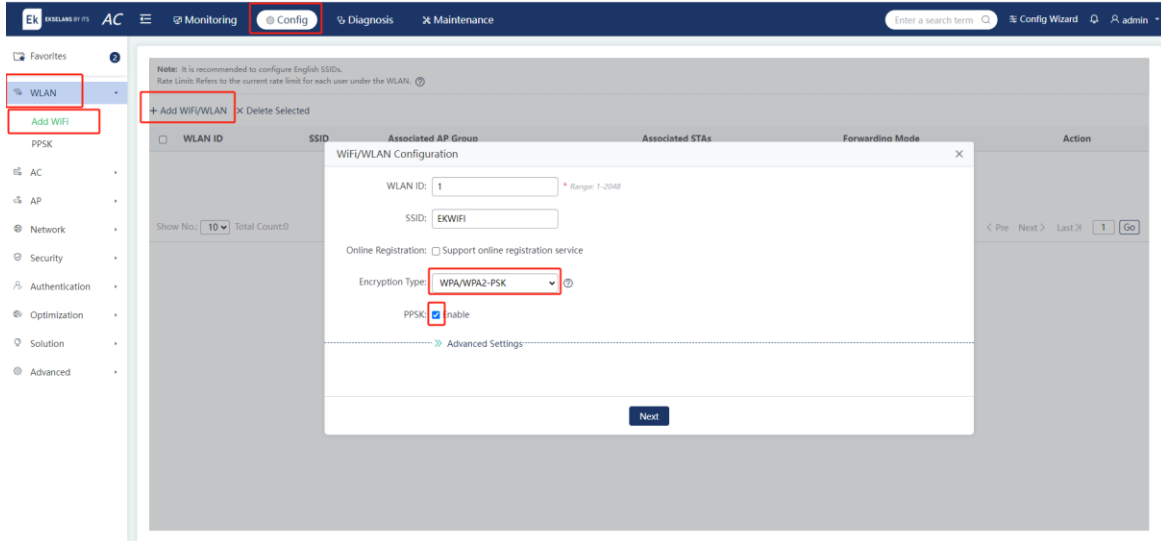
Private Pre-Shared Key (PPSK) includes two types: PPSK and Generalized Pre-Shared Key (GPSK), which are configured separately in two tabs. PPSK and GPSK supports up to 2,000 keys collectively.

1. PPSK

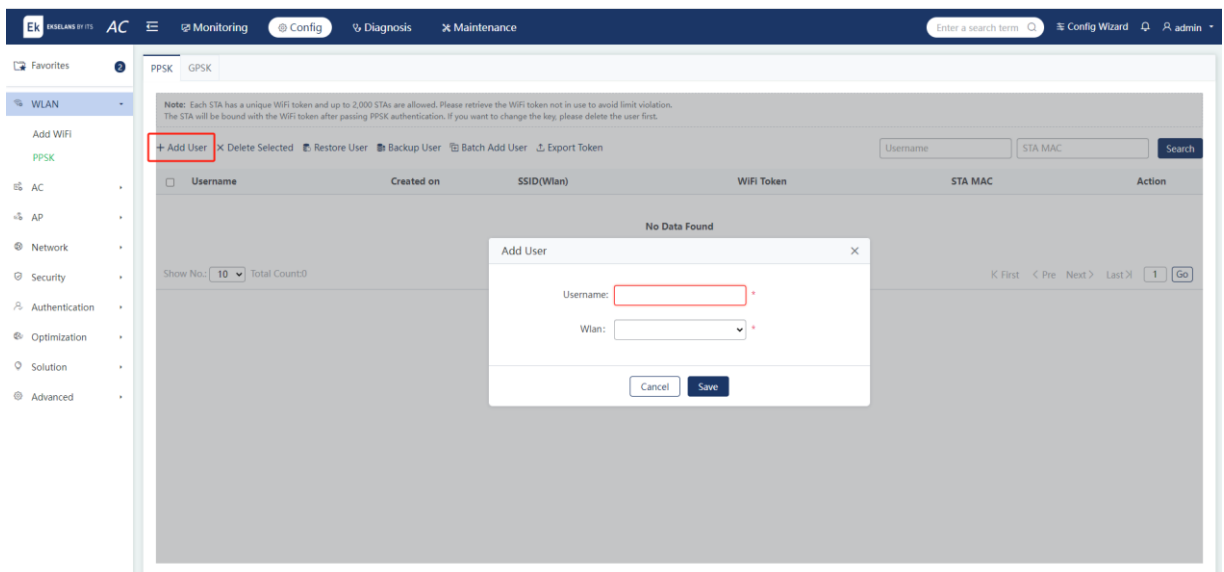
The administrator can configure user accounts here. Multiple keys can be generated based on one username.



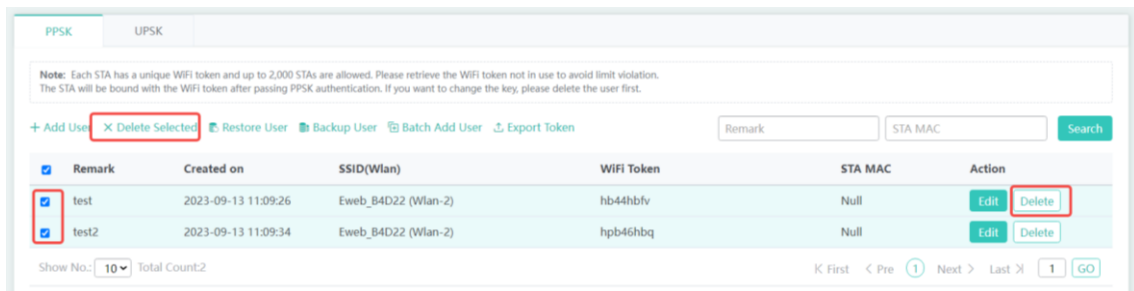
PPSK is only supported by WLANs using WPA/WPA2-PSK. Choose **WPA/WPA2-PSK** as the encryption type and enable PPSK on the **WiFi/WLAN Configuration** page.



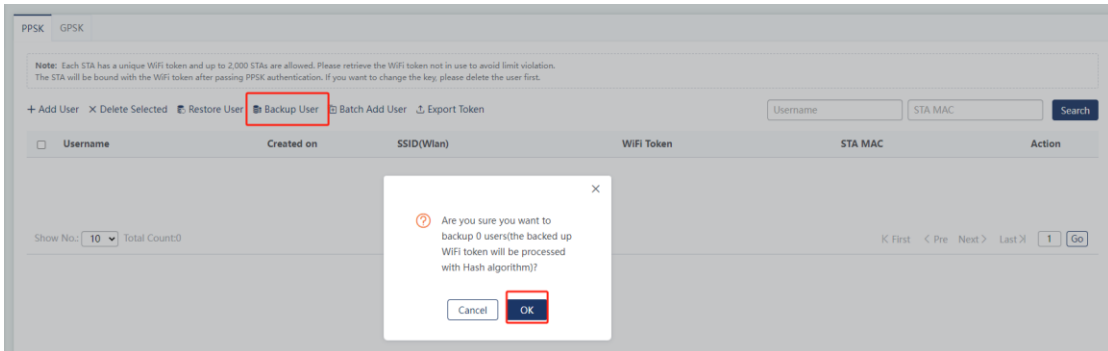
(1) Adding users: Click **Add User** and enter remarks in the pop-up window. Select a WLAN and click **Save**. A username can be added multiple times, with a unique key generated each time.



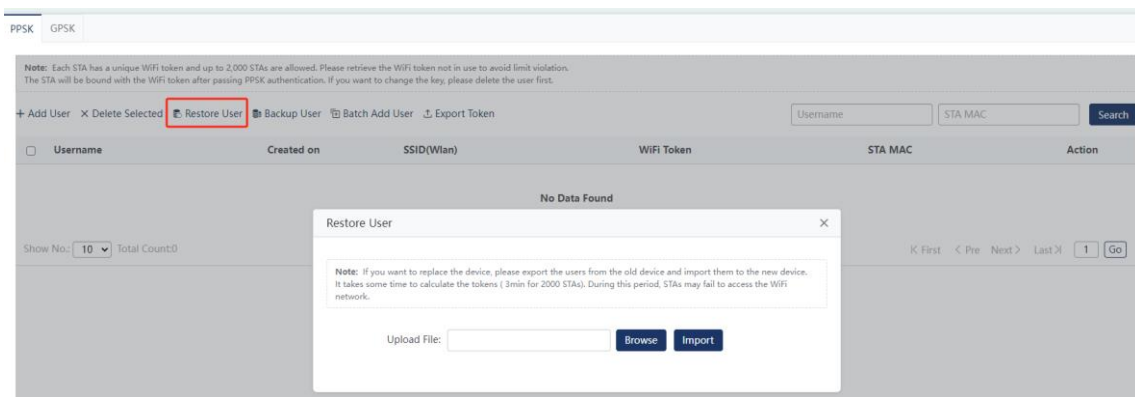
(2) Deleting users: Click **Delete** in the Action column to delete a user. Select multiple users and click **Delete Selected** to batch delete users.



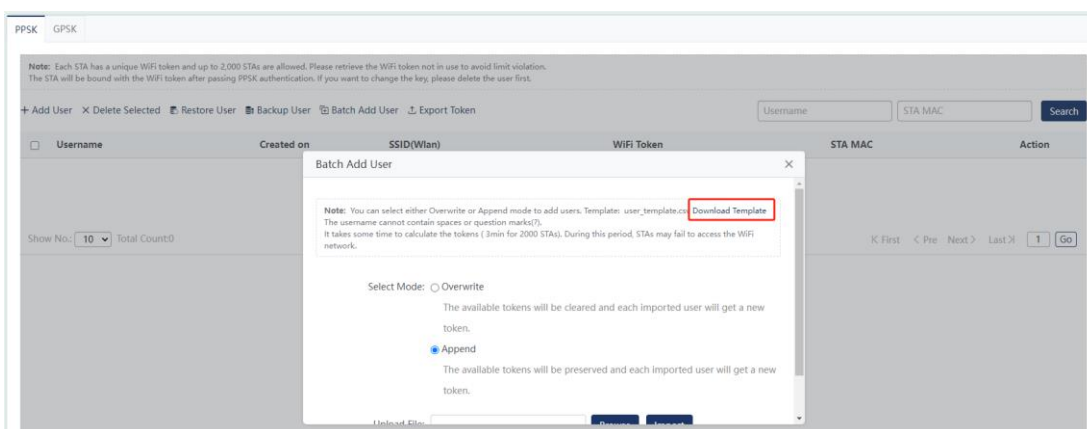
- (3) Backing up user data: Click **Backup User** and **OK** in the pop-up window to download data to the local device or upload the data to other devices for data backup.



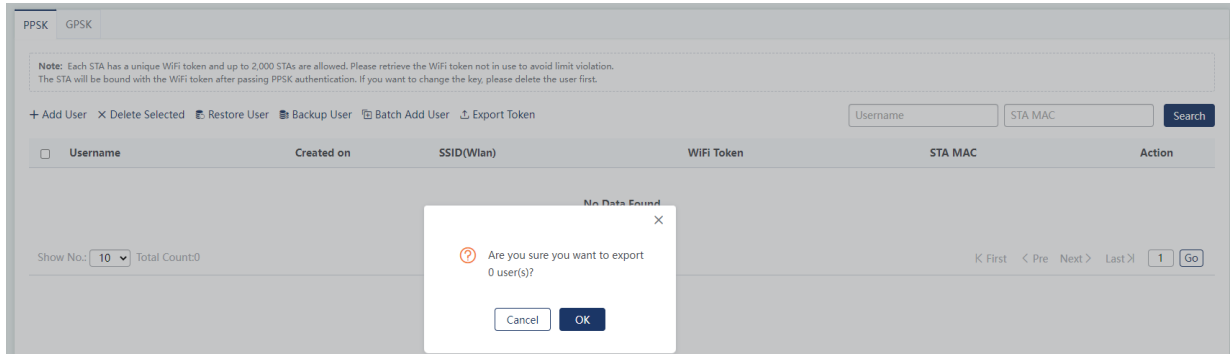
- (4) Restoring user data: Click **Restore User** to import the user data backup to the current device.



- (5) Batch adding users: Click **Batch Add User**. Click **Download Template** on the **Batch Add User** page. Add usernames in the template file. Select a method of adding users and click **Save**. Click **Browse** to select the template file and then click **Import** to import the template file to batch add users.



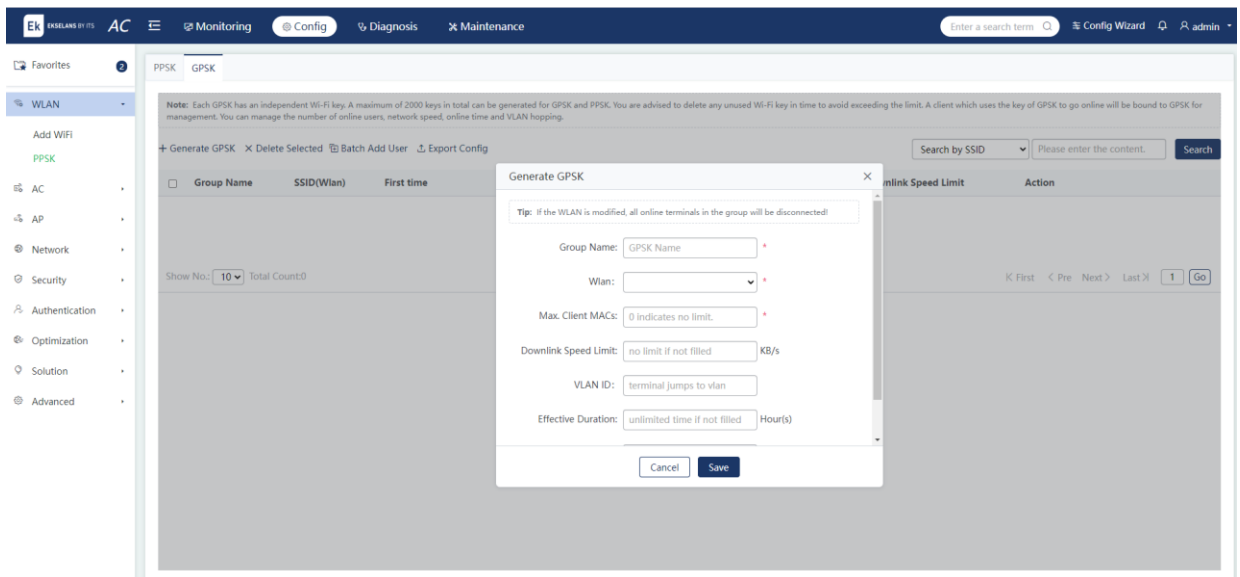
- (6) Exporting keys: Click **Export Token** to export all users and keys to the local device.



2. GPSK

Each GPSK is an independent Wi-Fi key. PPSK and GPSK supports up to 2,000 keys collectively. Promptly delete and recycle unused Wi-Fi keys to avoid exceeding the limit. STAs using the GPSK for login are managed based on the GPSK. The number of STAs, data rates, uptime, and VLAN redirection can be managed on this page.

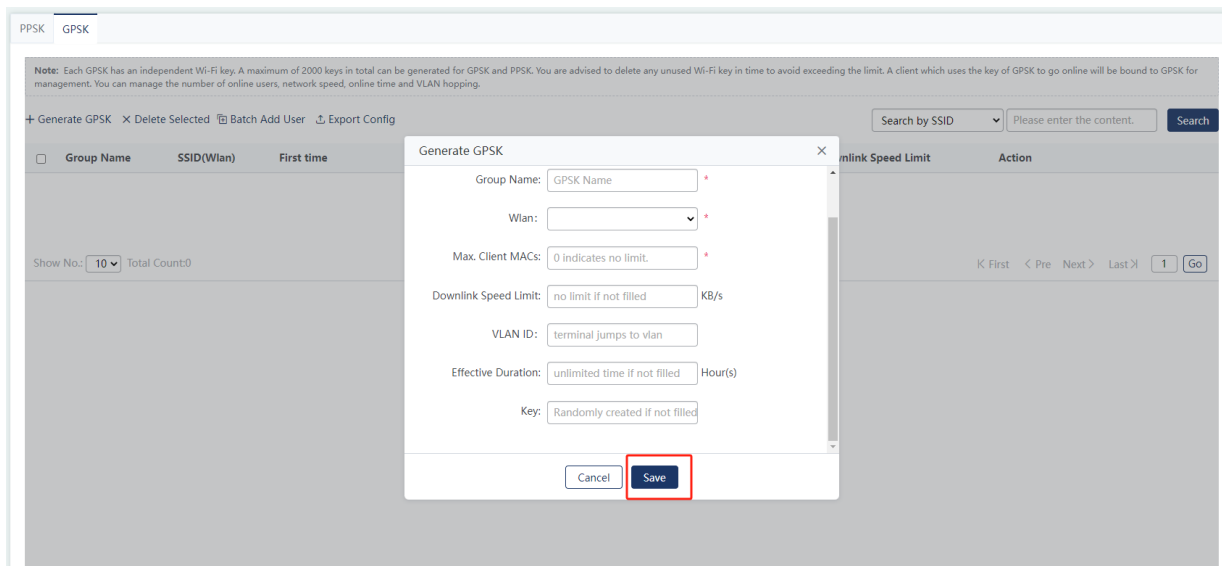
- (1) Generating a GPSK: Click **Generate GPSK** and edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.



Parameter	Description
Group Name	Enter a UPSK group name. Enter a string of 1 to 31 characters. Spaces, double quotes, commas, or full-width characters are not allowed.
WLAN	Select the WLAN ID to be associated with the UPSK. Only WLANs enabled with PPSK are available.
Max. Client MACs	Enter the maximum number of MAC addresses that can be associated. The value ranges from 0 to 65,535. Value 0 indicates no limit.
Downlink Speed Limit	Configure the downlink rate limit in KBs per second. The value ranges from 8 to 65,280. This field is optional.

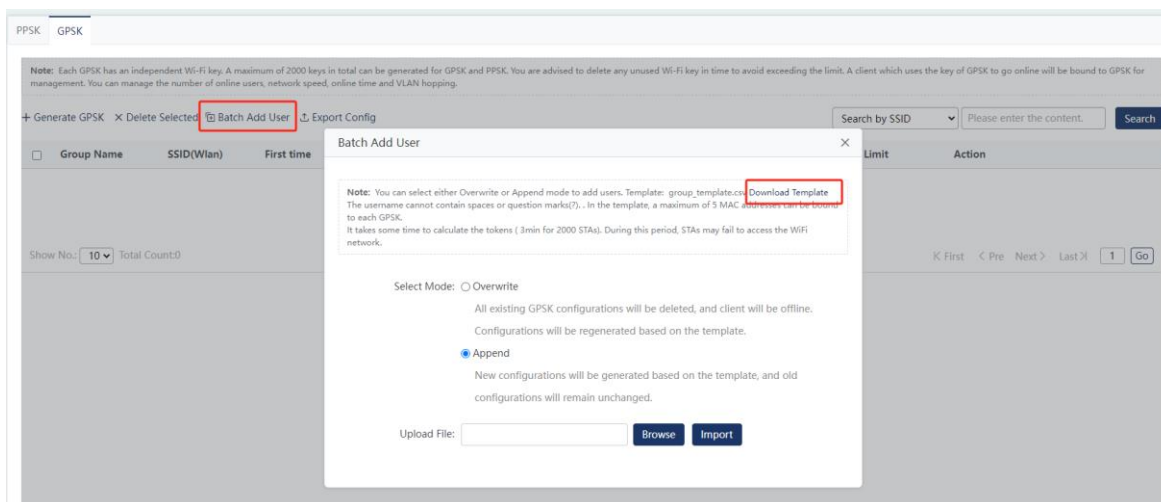
VLAN ID	After this parameter is configured, the STA will be redirected to this VLAN upon login. The value ranges from 1 to 4,096. This field is optional.
Effective Duration	Indicates the validity period of the key in hours. The value ranges from 1 to 100. This field is optional. The key is permanently valid if it is left blank.
Key	The key can be manually configured. Enter a string of 8 to 13 characters, consisting of numbers or letters. This field is optional. A random key will be generated if it is left blank.

(2) Editing users: Click **Edit** in the **Action** column. Edit the fields in the pop-up window and click **Save**.

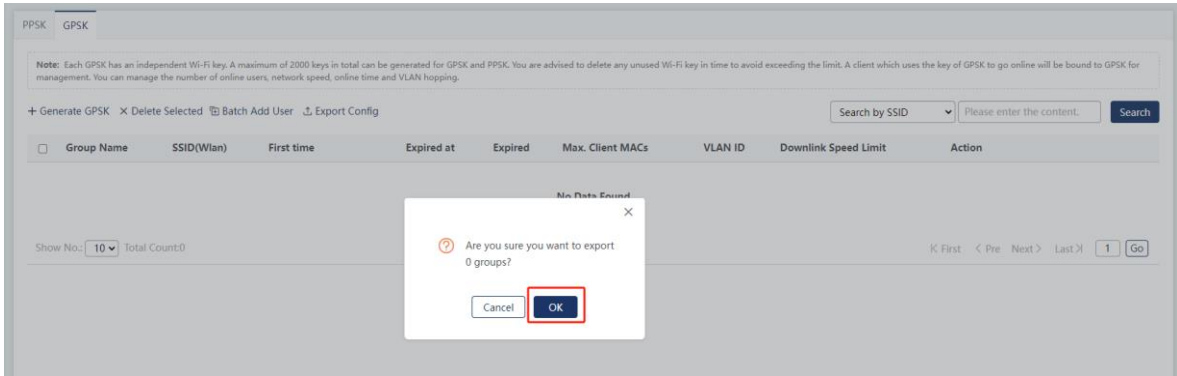


(3) Deleting users: Click **Delete** in the **Action** column to delete a user. Select multiple items and click **Delete Selected** to batch delete users.

(4) Batch adding users: Click **Batch Add User**. Click **Download Template** on the **Batch Add User** page. Add UPSK information into the template file. Select a method of adding users and click **Save**. Click **Browse** to select the template file and then click **Import** to import the template file to batch add users.



(5) Exporting configuration: Click **Export Config** to export all UPSK data to the local device.



(6) Managing client MAC addresses: Includes the management of dynamic and static clients. On the dynamic client management page, you can log out dynamic clients manually. On the static client management page, you can add or delete static clients.

5.2 AC

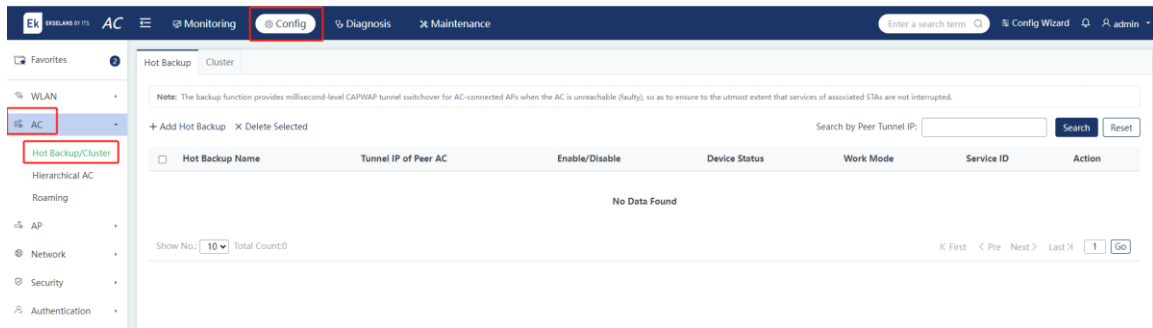
5.2.1 Hot Backup/Cluster

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

1. Hot Backup

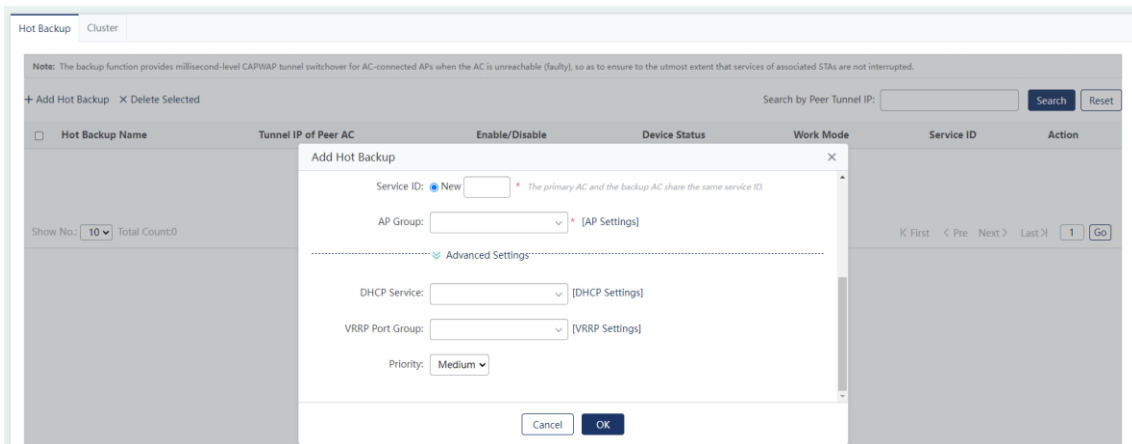
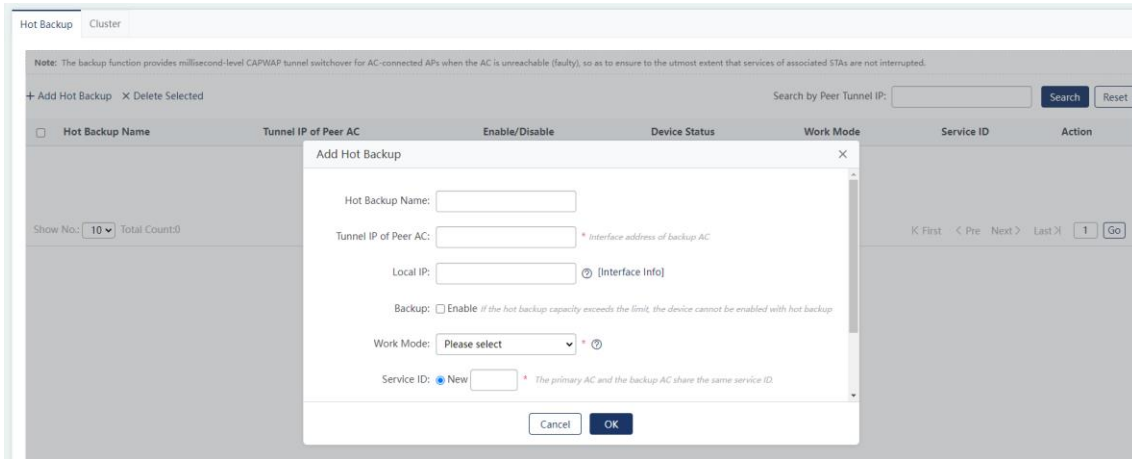
Choose **Config > AC > Hot Backup/Cluster > Hot Backup**.

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



(1) Adding the Hot Backup

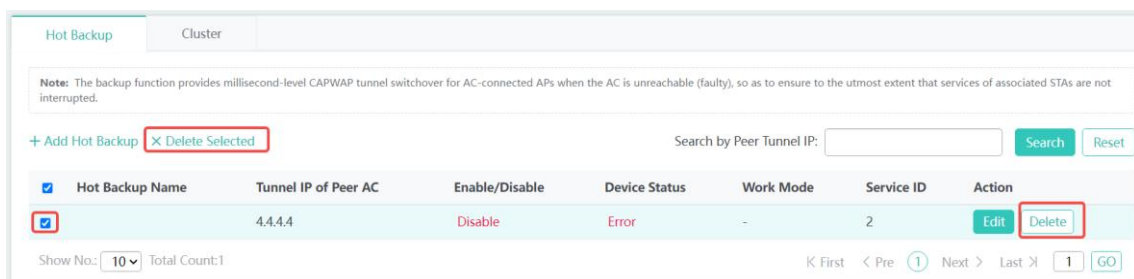
Click **Add Hot Backup** to enter the configuration page.



Parameter	Description
Hot Backup Name	Configure the hot backup name.
Tunnel IP of Peer AC	Enter the IP address on the peer side of the tunnel for communications between the AP and AC. The IP address of interface Loopback0 is configured as the tunnel IP address by default.
Local IP	If the communication is not established through interface Loopback0, configure the local IP address. Typically, the interface IP address is configured as the local IP address. Configure this parameter by clicking Interface Info to view interface details.
Backup	Enable or disable hot backup. This feature cannot be enabled if the number of hot backups reaches the limit.

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

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



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

Hot Backup Cluster

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

+ Add Hot Backup X Delete Selected

Search by Peer Tunnel IP: Search Reset

<input type="checkbox"/>	Hot Backup Name	Tunnel IP of Peer AC	Enable/Disable	Device Status	Work Mode	Service ID	Action
<input type="checkbox"/>		4.4.4.4	Disable	Error	-	2	Edit Delete

Show No.: 10 Total Count:1

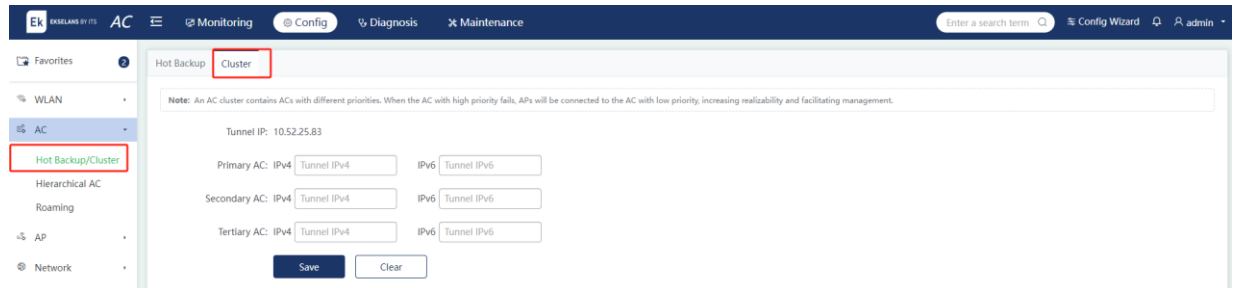
K First < Pre 1 Next > Last 1 GO

2. Cluster

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

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

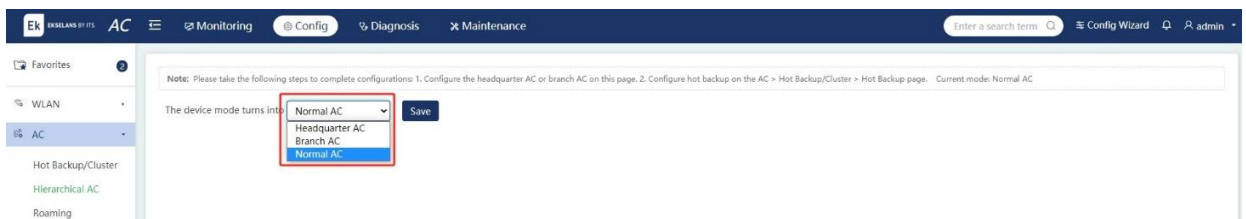
Configure up to three backup ACs based on IPv4 or IPv6 addresses.



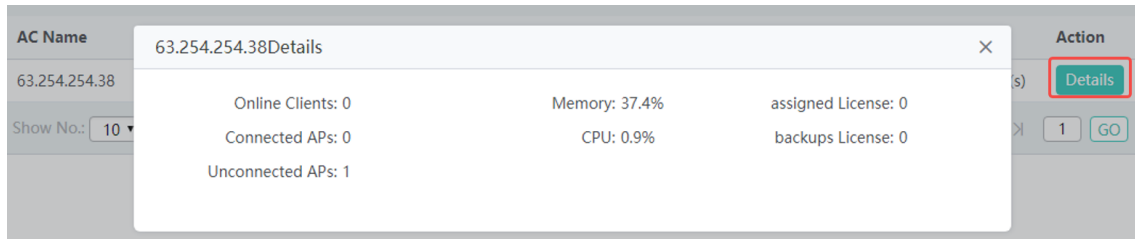
5.2.2 Hierarchical AC

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

Details of hierarchical ACs are displayed on this page.



(1) Viewing AC details: Click **Details** to view AC details.



5.2.3 Roaming

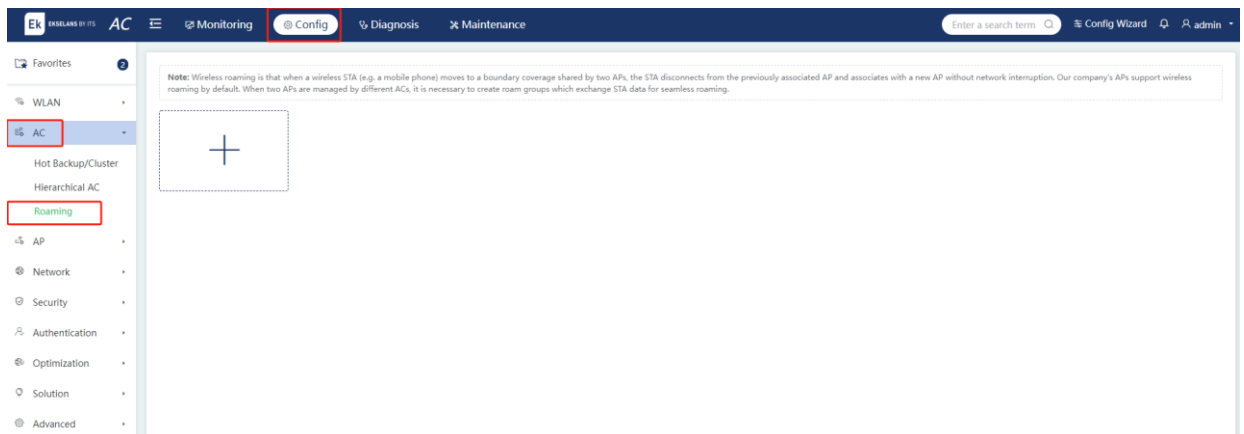
Choose **Config > AC > Roaming**.

Roaming refers to the ability of an STA to connect to and use the services of another AP outside its original network coverage area. The AC roam group allows STAs to roam across APs with consistent experience.

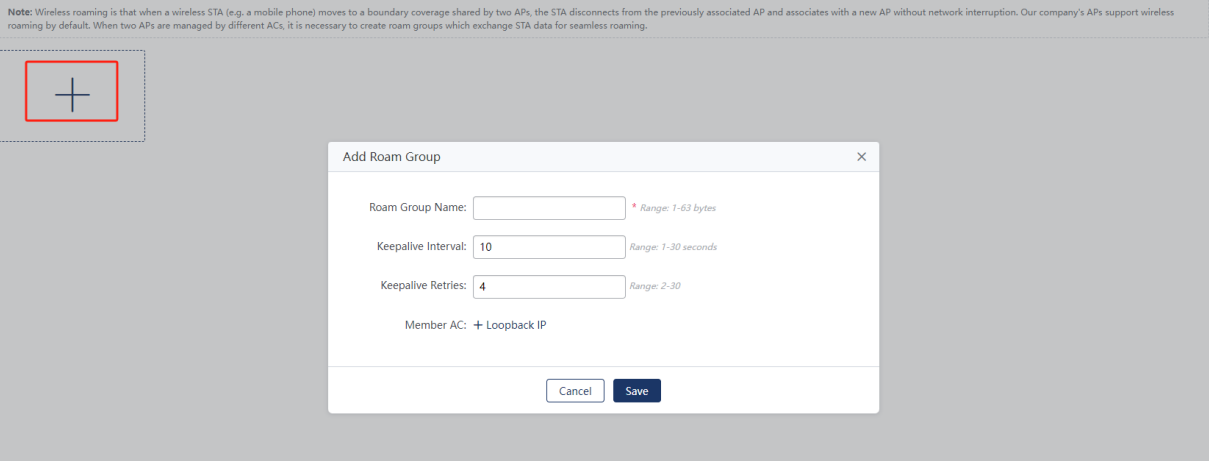
The roaming range for STAs cannot extend infinitely. To enable STAs to roam across APs associated with different ACs and manage the roaming range of STAs, the ACs in the area where the STA moves are moved into a roam group.

Note

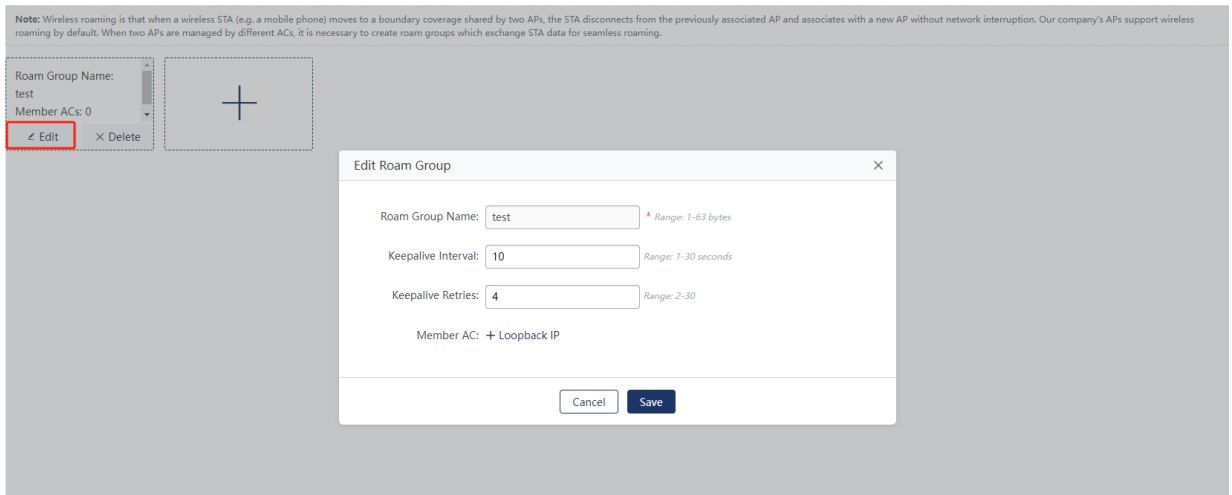
The number of member devices in the roam group is limited to ensure the efficiency and reliability of communications between ACs in a roam group. Each roam group contains a maximum of 24 AC members.



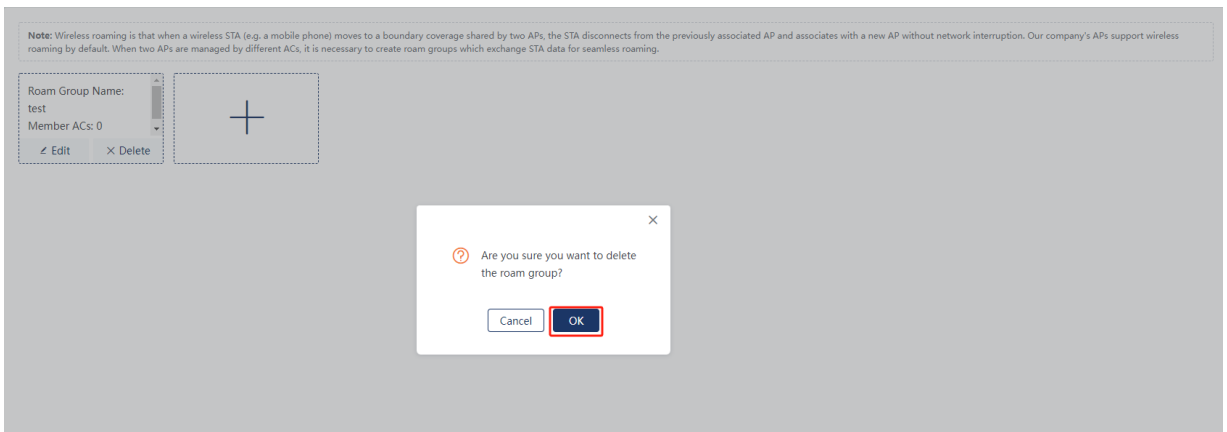
- (1) Adding roam groups: Click the **+** button on the **Roaming** page to add a roam group. The **Roam Group Name** field is mandatory, while other fields are optional. Multiple member ACs can be selected. Clicking **Save** and the roam group will be displayed on the **Roaming** page after a message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



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



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

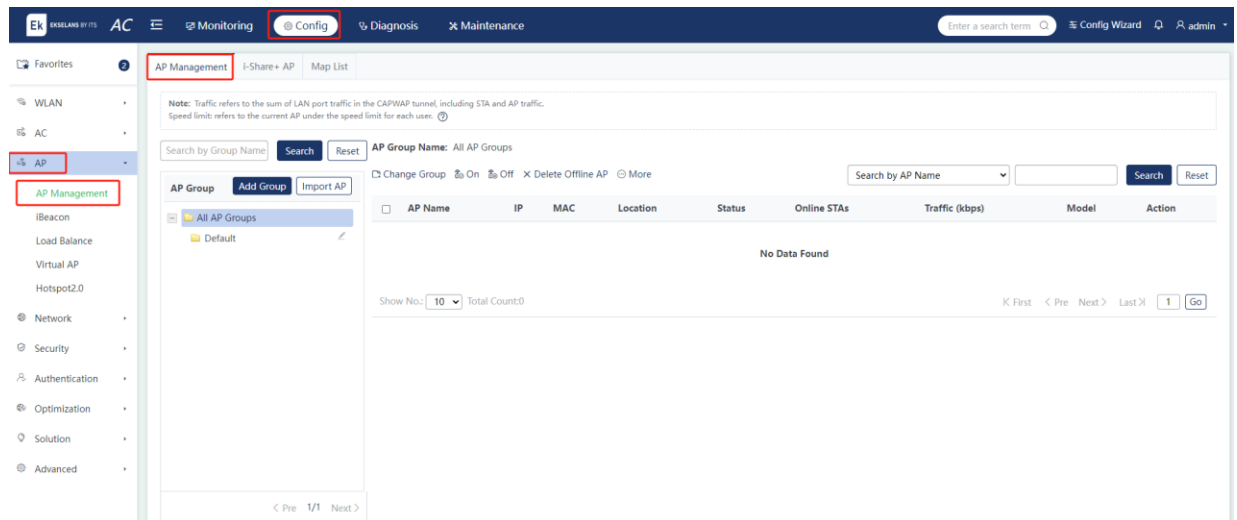


5.3 AP

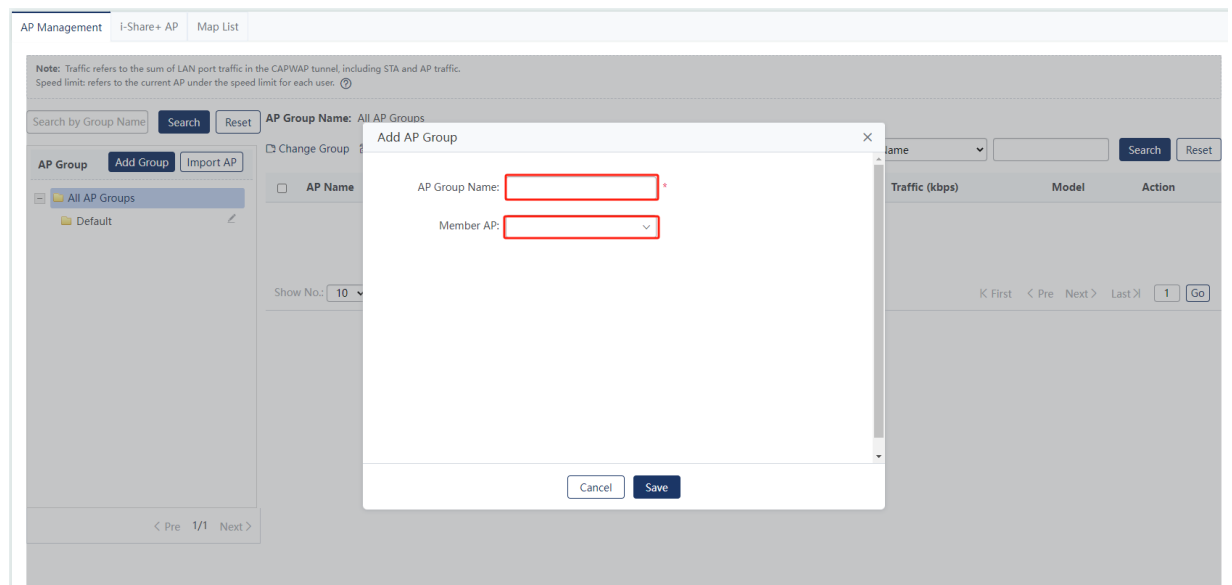
5.3.1 AP Management

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

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



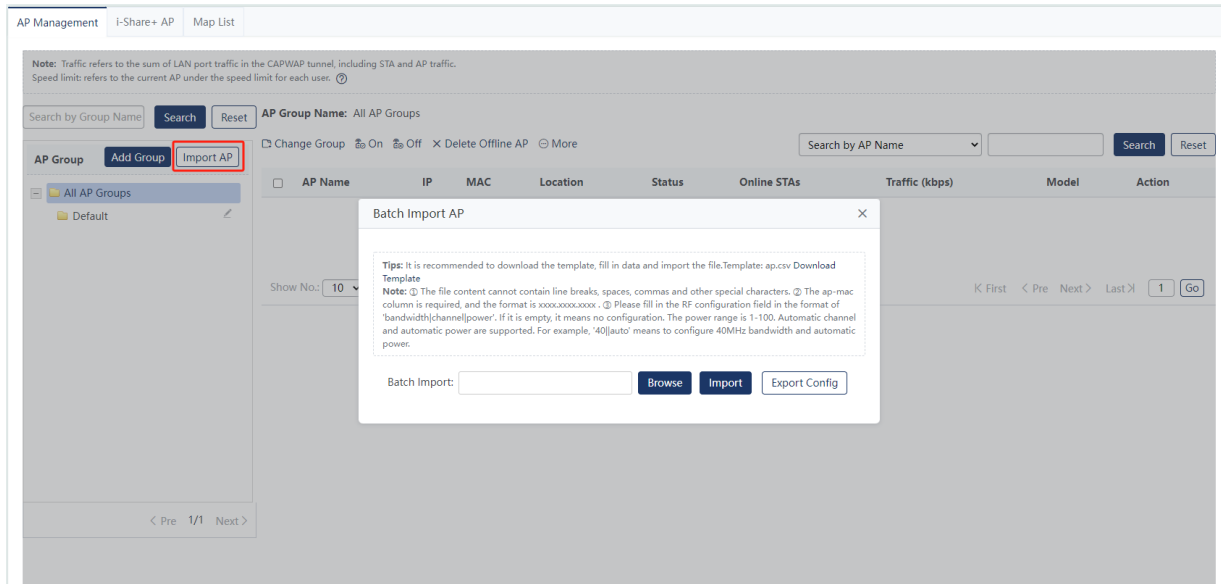
- (1) Adding AP groups: Click **Add Group** and the **Add AP Group** window pops up. Enter the AP group name, select member APs to be added to this AP group, and Click **Save**.



Parameter	Description
AP Group Name	This field is mandatory.

Member AP	Select member APs to be added to this AP group. An AP can be added to only one group. If APs are not added to any group, they are assigned to the default AP group.
-----------	---

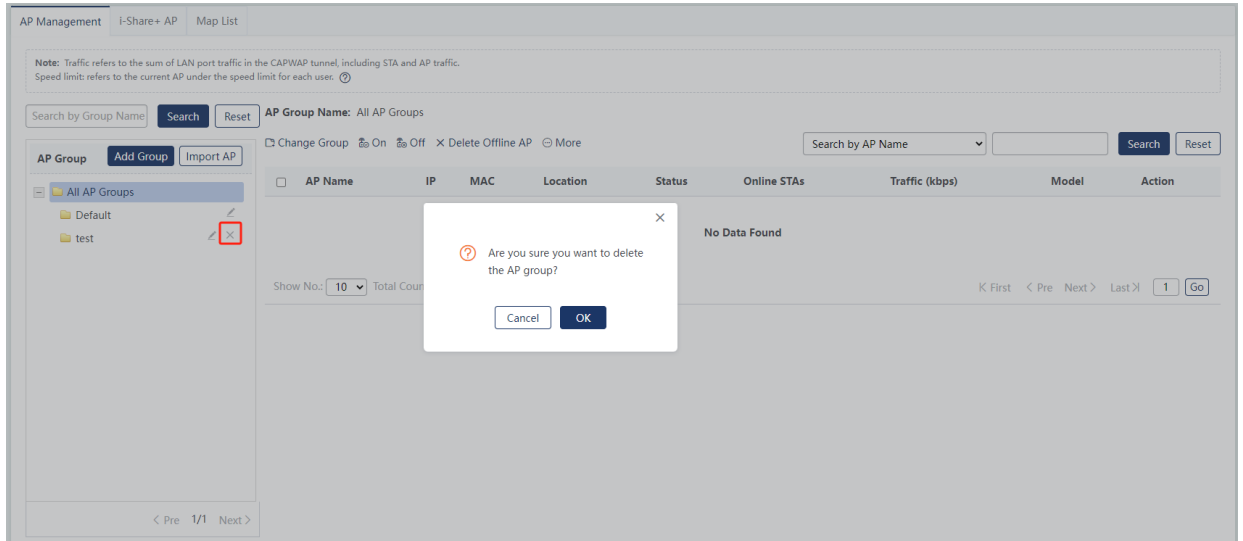
- (2) Batch importing APs: If many APs are to be imported, export the current configuration file. Edit configurations and import the edited file back to the device to realize batch configurations. You can also download the template file to edit configurations and import it back to the device.



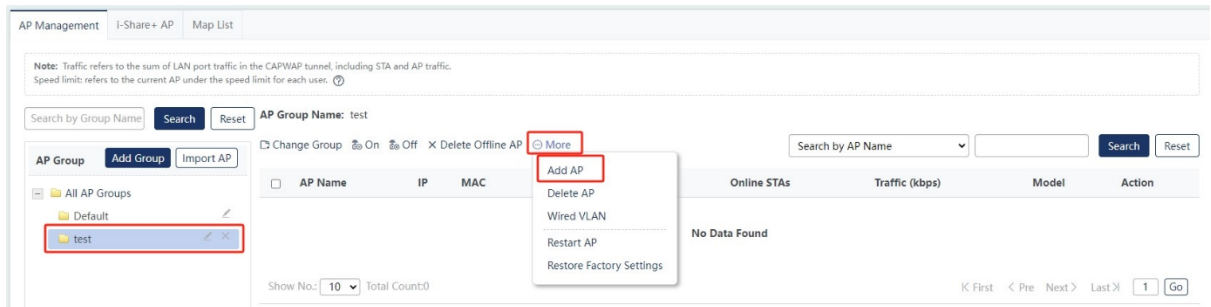
- (3) Deleting AP groups: Select the AP group you want to delete and click **x**. Click **OK** in the pop-up window to delete the AP group.

Note

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



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



Add AP ✕

AP Name: *

MAC: *

Location:

» Advanced Settings

AP Group: ⓘ

Telnet Account:

Telnet Password: Show Password

Tunnel IP: ⓘ

Parameter	Description
AP Name	Enter the name of the AP. If the AP is offline, the AP name cannot be edited.

MAC	Enter the MAC address of the AP. The MAC address cannot be edited if the AP is online.
Location	Enter the location of the AP. For instance, if the AP is deployed in Room 201 on the 19th floor, enter 19#201 in this field.
AP Group	Enter the group of the AP. An AP can belong to only one group. By default, an AP belongs to the default group.
Telnet Account	Enter the account for logging into the AP. Both Telnet account and password are mandatory.
Telnet Password	Enter the password for logging into the AP. Both Telnet account and password are mandatory.
Tunnel IP	<p>The AP can be assigned with an IP address through DHCP. You can also configure a static IP address, which requires the configuration of the gateway address, tunnel IP address, IPv4 address, and IPv4 subnet mask.</p> <hr/> <p> Caution</p> <p>This configuration may cause an AP disconnection.</p>

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

Parameter	Description
Wired Port	The wired port is enabled by default.
AP IPv4	<p>The AP can be assigned with an IP address through DHCP or manually specified with a static gateway address, a tunnel IP address, an AP IPv4 address, and an AP IPv4 subnet mask. The AP IPv4 gateway is the parameter for configuring the static IP address. You can configure the AP IPv4 address, AP IPv4 subnet mask, and AP IPv4 gateway by running command <code>ip address 2.2.2.2 255.255.255.0 2.2.2.1</code>.</p> <hr/> <p> Caution</p> <p>This configuration may cause an AP disconnection.</p>
AP IPv4 Mask	
AP IPv4 Gateway	
Offline SSID	Enter the SSID broadcast by the AP when it is disconnected.
Hide Offline SSID	Display or hide the SSID broadcast by the AP when it is disconnected.

Note

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

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

 **Caution**

This configuration may cause an AP disconnection.

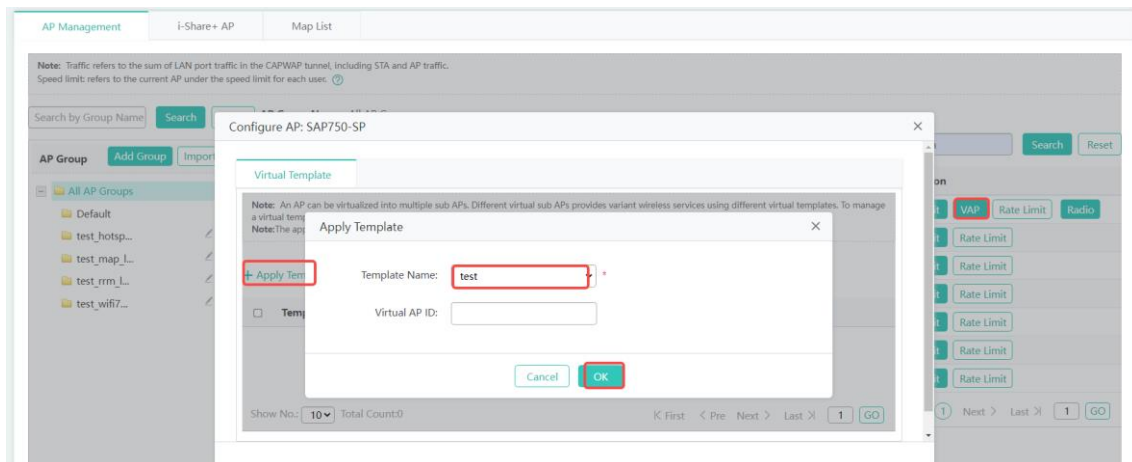
- (8) Restoring factory settings: Select one or multiple items in the AP list and click **Restore Factory Settings**. Click **OK** in the pop-up window to restore the APs to factory settings.
- (9) Configuring wired VLAN: Click **Wired VLAN** and the **Wired VLAN** window pops up. Enter the VLAN ID, select the wired port, and click **Save**.
- (10) Enabling APs: Select one or multiple items in the AP list and click **On** to batch enable AP radios.
- (11) Disabling APs: Select one or multiple items in the AP list and click **Off** to batch disable AP radios.
- (12) Deleting offline APs: Click **Delete Offline AP** to delete all offline APs.
- (13) Configuring radio: Click **Radio** in the **Action** column and the **WiFi Radio Settings** window pops up.

Parameter	Description
RF Port	This field is displayed only when the AP has at least three radios.
2.4G Network	Enable or disable the radio.
5G Network	
Country or Region	Configure the country or region code for the AP. It is consistent with the country or region code of the AC by default.
WiFi Protocol	Select the IEEE 802.11 standard that the RF card complies with. The options for the 2.4 GHz network include: 11bgn, indicating IEEE 802.11b/g/n. 11bgn+11ax, indicating IEEE 802.11b/g/n/ax The options for the 5 GHz network include: 11an, indicating IEEE 802.11a/n. 11an+11ac, indicating IEEE 802.11a/n/ac. 11an+11ac+11ax, indicating IEEE 802.11a/n/ac/ax.
WiFi Channel	Select the Wi-Fi channel based on the country or region and network type.

Power	Options: Auto: Auto Power Saving: The power value is 30. Standard: The power value is 80. Enhanced: The power value is 100. Custom: The power value is customized.
STA Limit	Configure the maximum number of STAs supported by the radio.
Frequency Bandwidth	Specify the channel bandwidth supported by the radio.
Receiving/Sending	Enable or disable the receive or transmit antenna.

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

(15) Configuring VAP: Click **VAP** in the **Action** column to enter the **Virtual Template** page. Click **Apply Template** and select a template name. Configure the virtual AP ID and click **OK**.

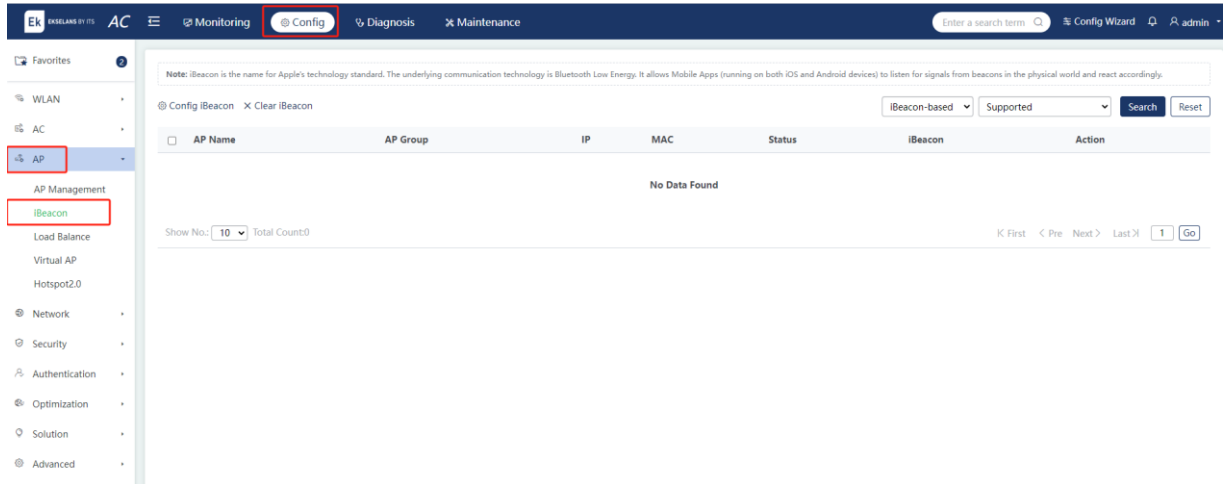


5.3.2 iBeacon

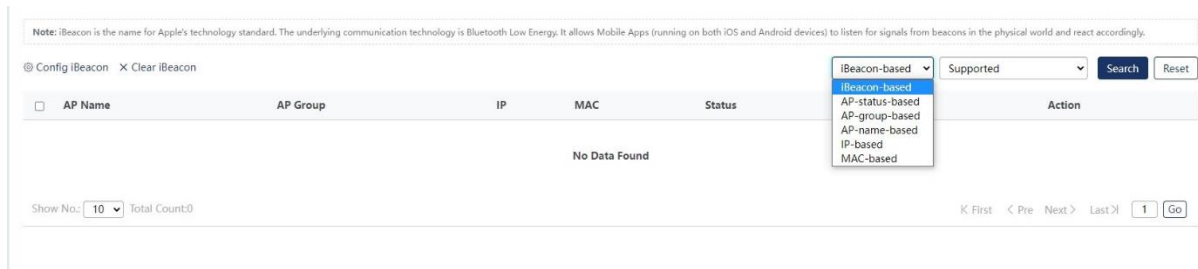
Choose **Config > AP > iBeacon**.

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

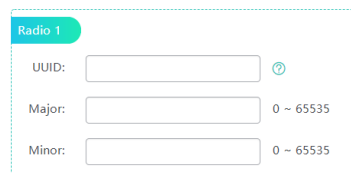
Example: The shopping mall can apply iBeacon to push ads to customers.



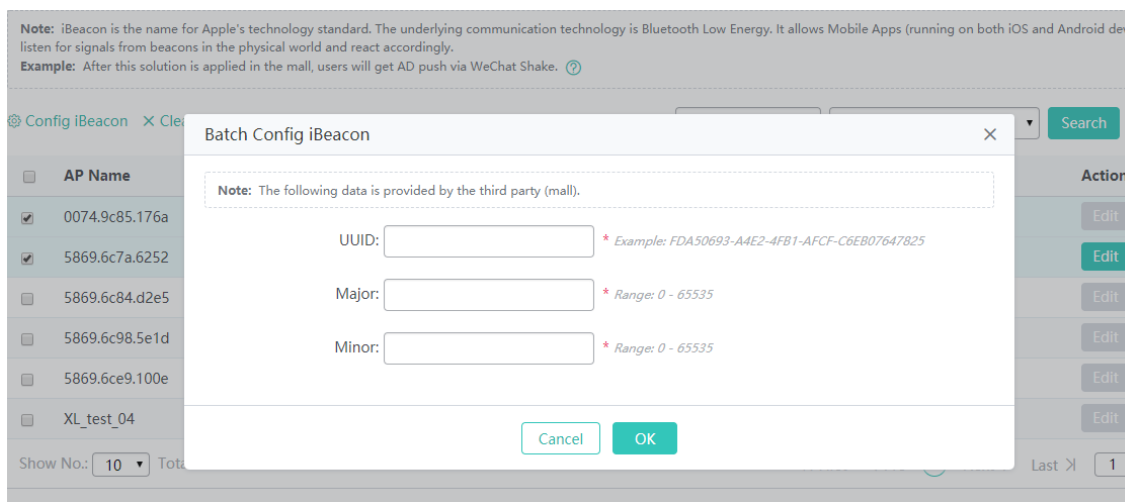
(1) Searching for APs: Search for APs using the filter or entering keywords. Click **Reset** to clear the search criteria.



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



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

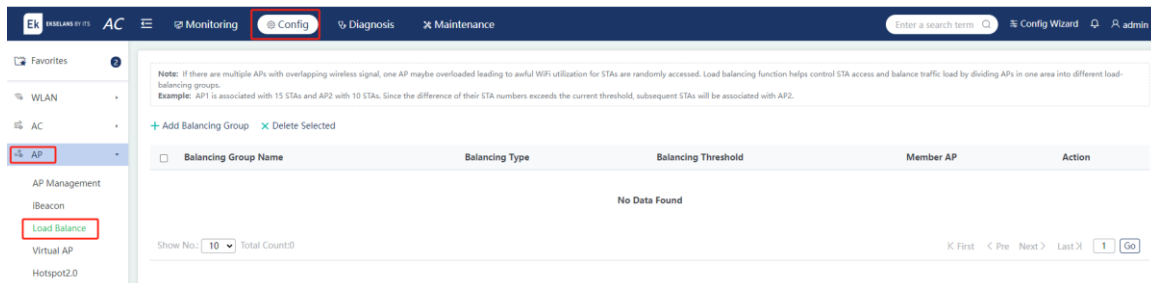


(4) Batching deleting iBeacon: Select the items in the list and click **Clear iBeacon**.

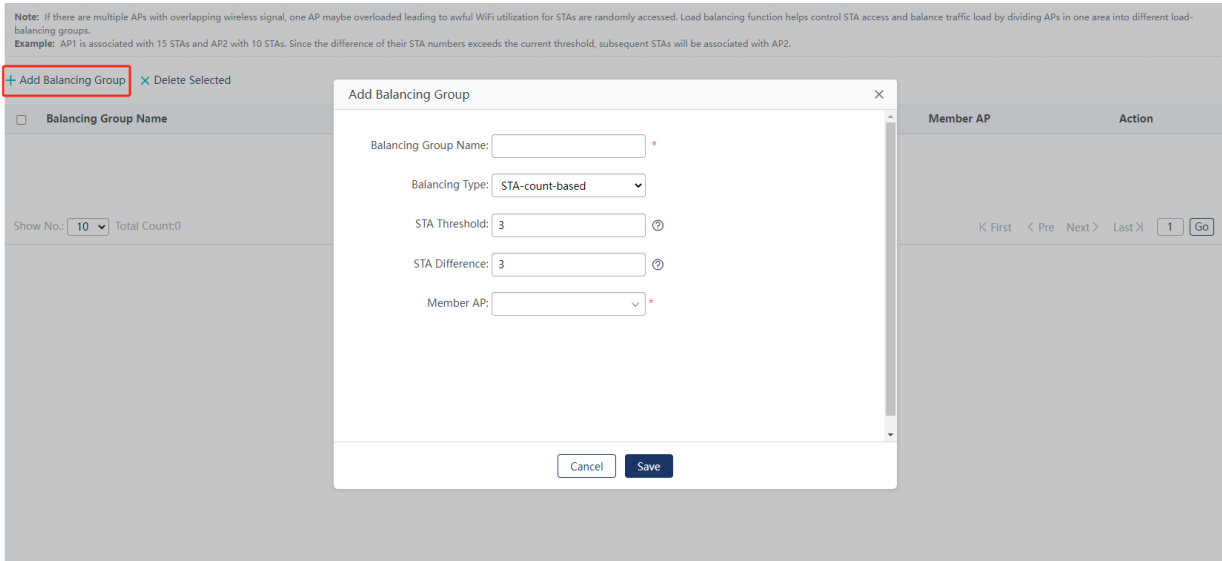
5.3.3 Load Balance

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

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



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



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

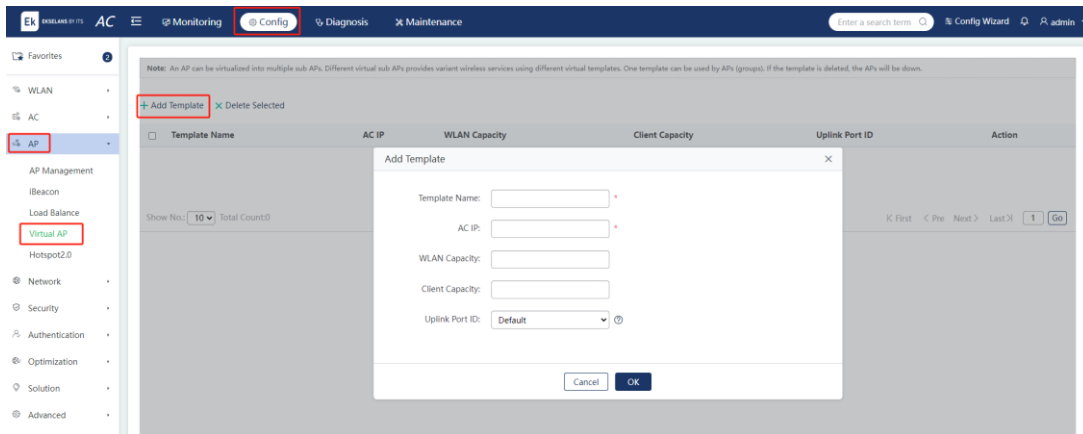
- (2) Deleting load balancing groups: Click **Delete** in the **Action** column to delete a load balancing group. Select load balancing groups in the list and click **Delete Selected**. Click **OK** in the pop-up window to batch delete load balancing groups.
- (3) Editing load balancing groups: Click **Edit** in the **Action** column and edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.

5.3.4 Virtual AP

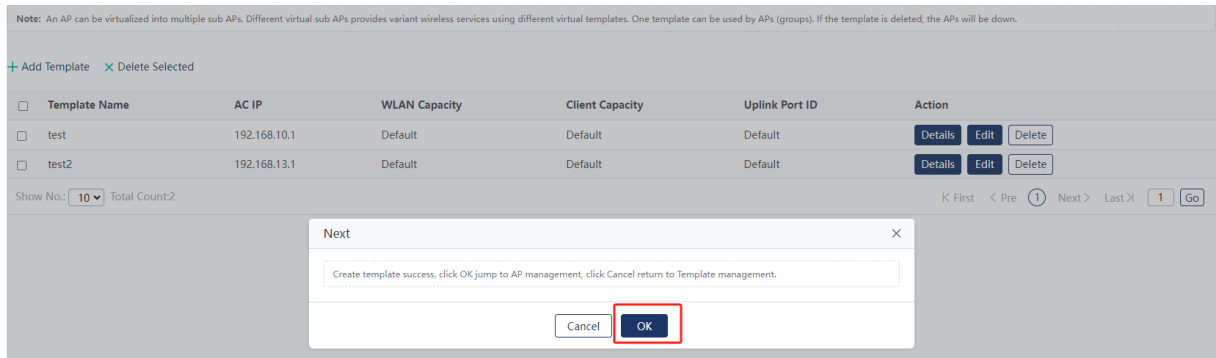
Choose **Config > AP > Virtual AP**.

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

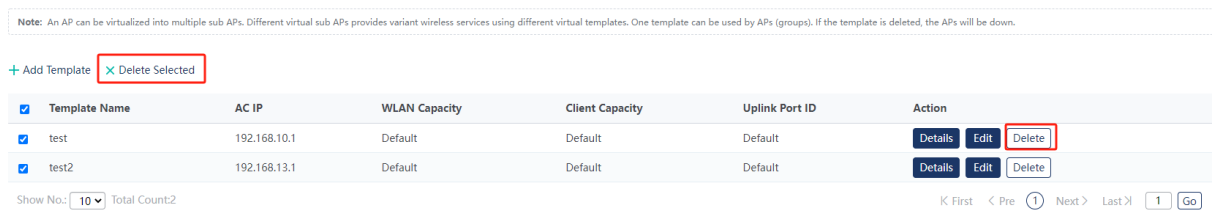
- Adding templates: Click **Add Template** and configure the parameters on the **Add Template** page. Click **OK** to create the template. After the template is added, click **OK** to redirect to the **AP Management** page to apply the template. Click **Cancel** to return to the **Virtual AP** page.



Parameter	Description
Template Name	Enter the template name for virtual AP management. This field is mandatory.
AC IP	Enter the tunnel IP address of the AC for AP management.
WLAN Capacity	Enter the maximum number of WLANs supported by this template.
Client capacity	Enter the maximum number of clients supported by this template.
Uplink port ID	Virtual APs use the uplink port ID used by the active AP by default.



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



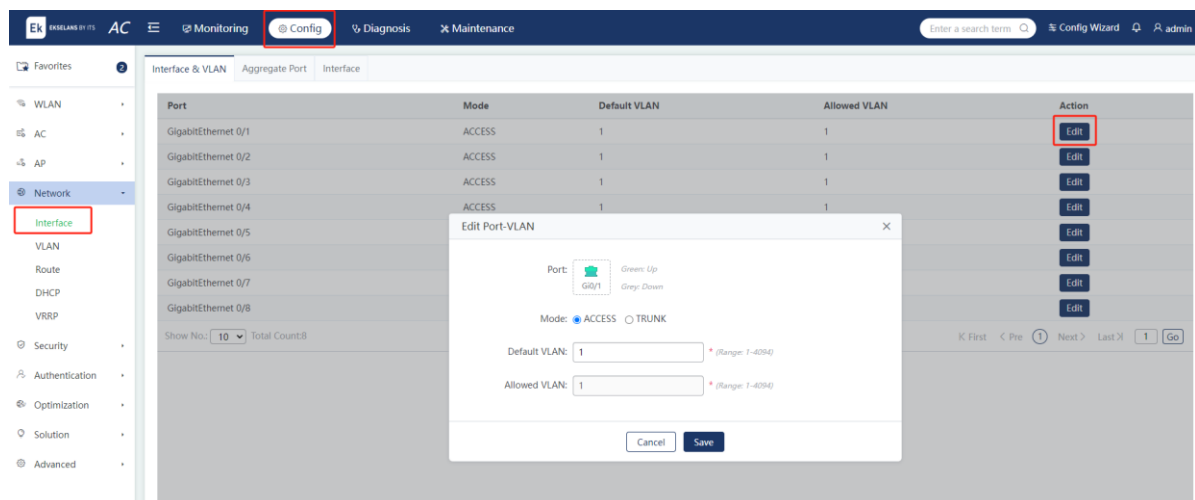
5.4 Network

5.4.1 Interface

Choose **Config > Network > Interface**.

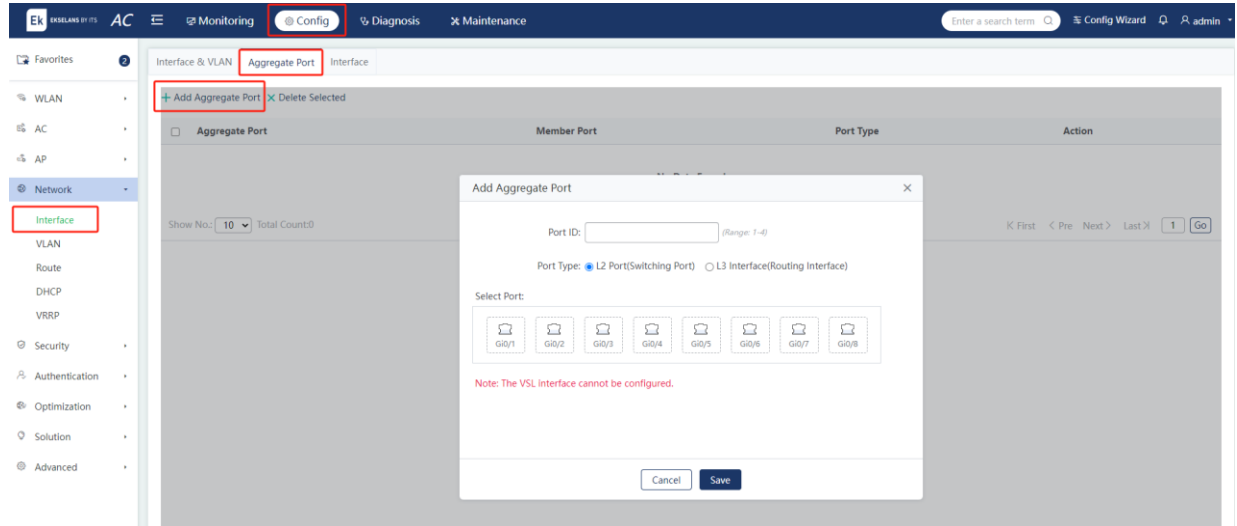
1. Interface & VLAN

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

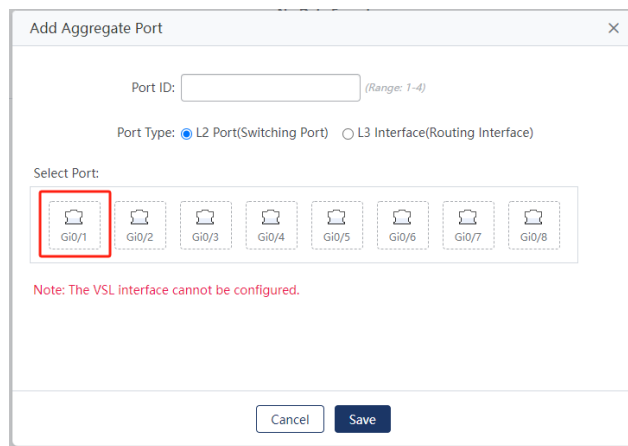


2. Aggregate Port

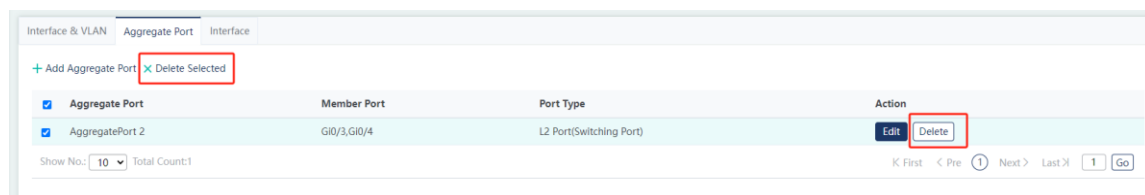
- (1) Adding aggregate ports: Click **Add Aggregate Port**. Edit the fields in the pop-up window. Click **Save** and the aggregate port will be displayed in the list of aggregate ports after a message indicating operation success is displayed.



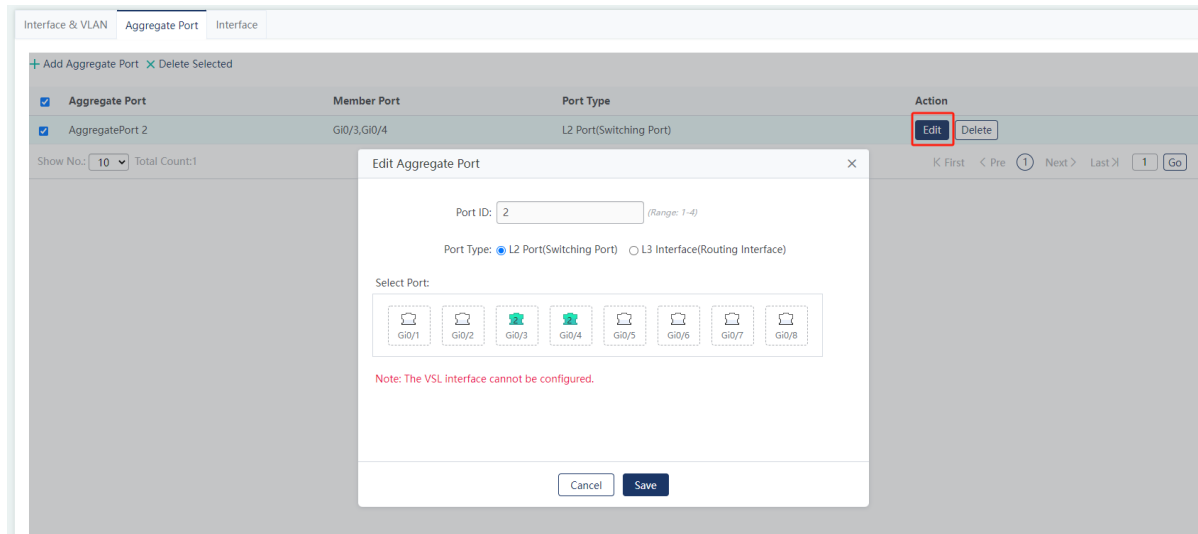
The following figure shows the panel where you can select member ports. The ports in gray have been configured as member ports of an aggregate port. The number under the port icon indicates that this port is a member port of the specified aggregate port.



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

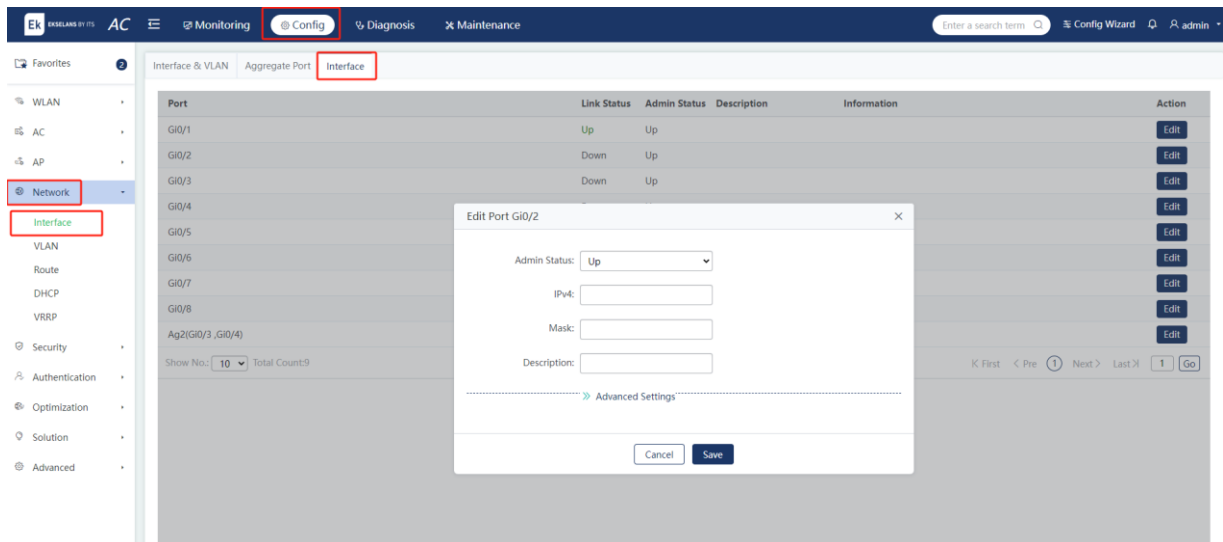


- (3) Editing aggregate ports: Click **Edit** in the **Action** column. A window pops up displaying the information about the aggregate port and edit the fields in the window. Click **Save** and a message indicating operation success is displayed.



3. Interface

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



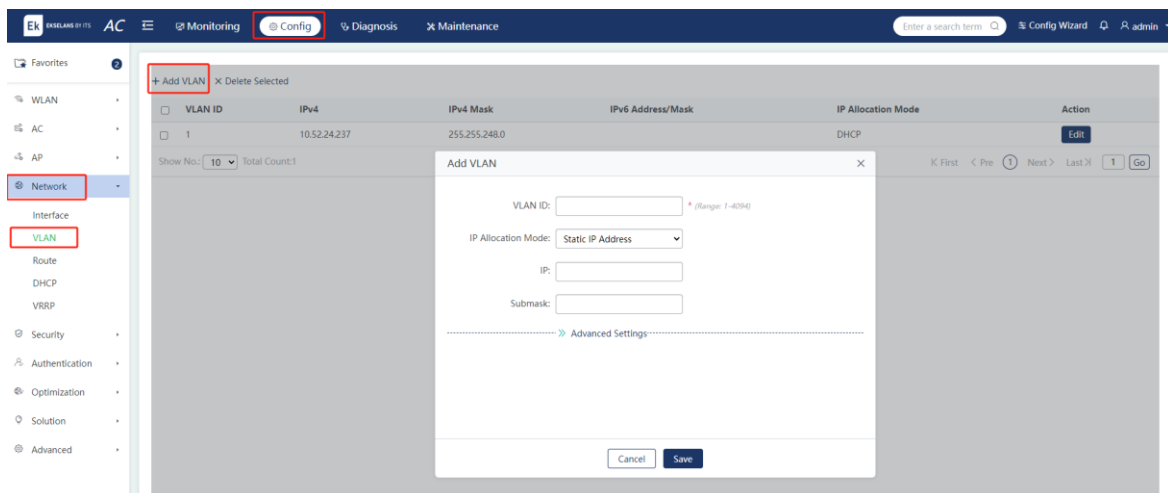
Parameter	Description
Admin Status	Select the status of the interface.
IPv4	Enter the IPV4 address of the interface.
Mask	Enter the IPV4 subnet mask of the interface.

Description	Enter the description or alias of the interface.
Copper/Fiber Port	The options including Copper Port and Fiber Port are displayed based on the hardware capability.
IPv6	Enter the IPv6 address of the interface.
Speed	Configure the rate of the interface.
Working Mode	The work modes of the interface include negotiation, duplex, and half-duplex modes.

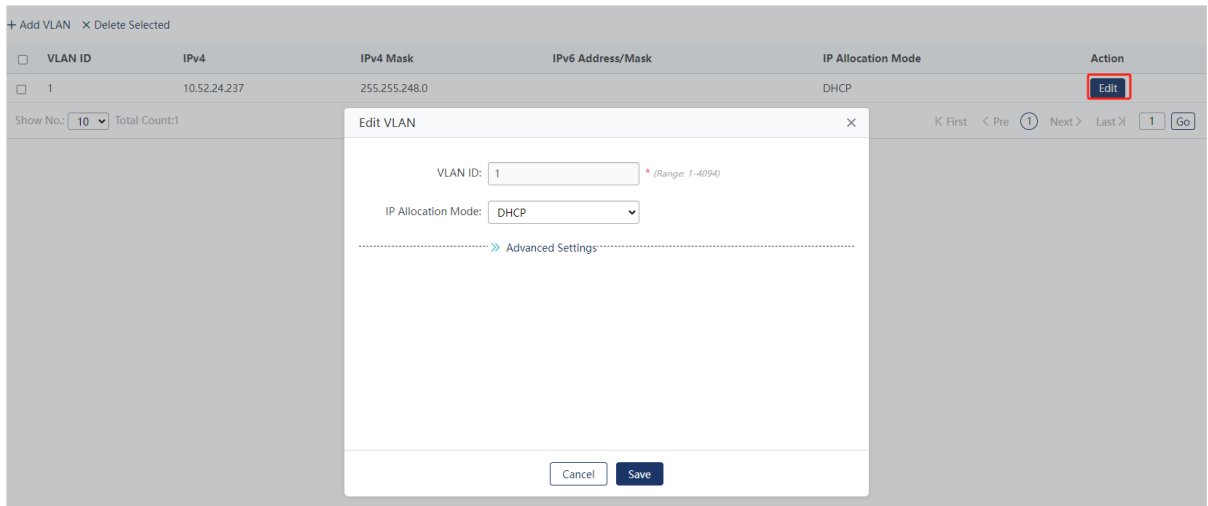
5.4.2 VLAN

Choose **Config > Network > VLAN**.

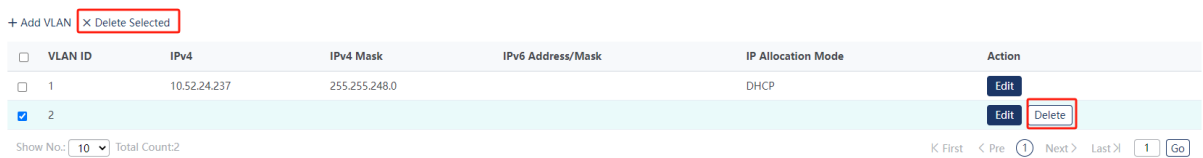
- (1) Adding VLANs: Click **Add VLAN** and edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed. The added VLAN is displayed in the VLAN list.



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



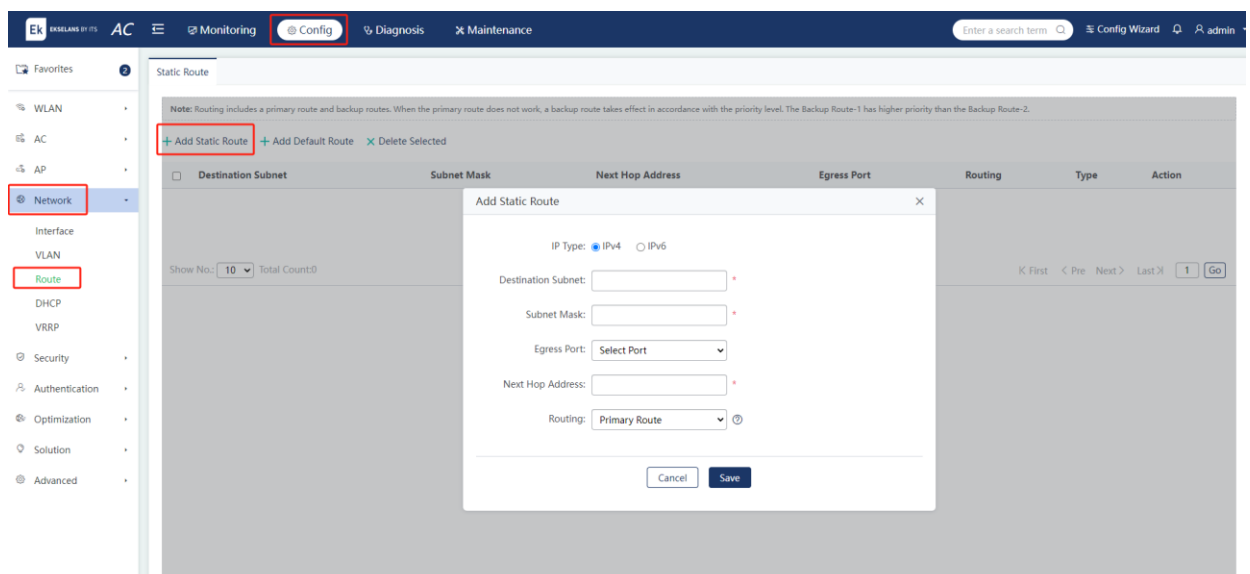
- (3) Deleting VLANs: Click **Delete** in the **Action** column and click OK in the pop-up window to delete a VLAN. Select multiple items in the list. Click **Delete Selected** and a window pops up. Click **OK** to batch delete VLANs.



5.4.3 Route

Choose **Config > Network > Route**.

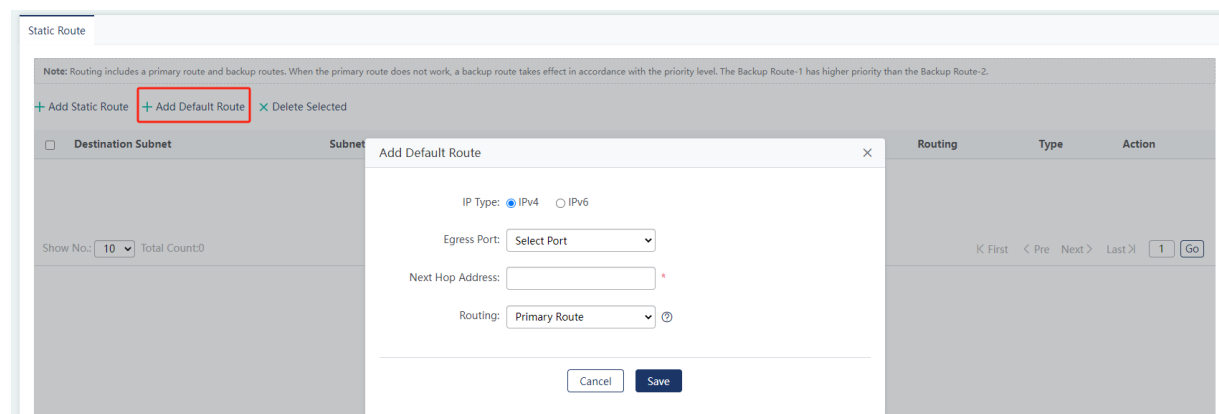
- (1) Adding static routes: Click **Add Static Route**. Edit the fields in the pop-up window. Click **Save** and the static route will be displayed in the route list after a message indicating operation success appears.



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

Note

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



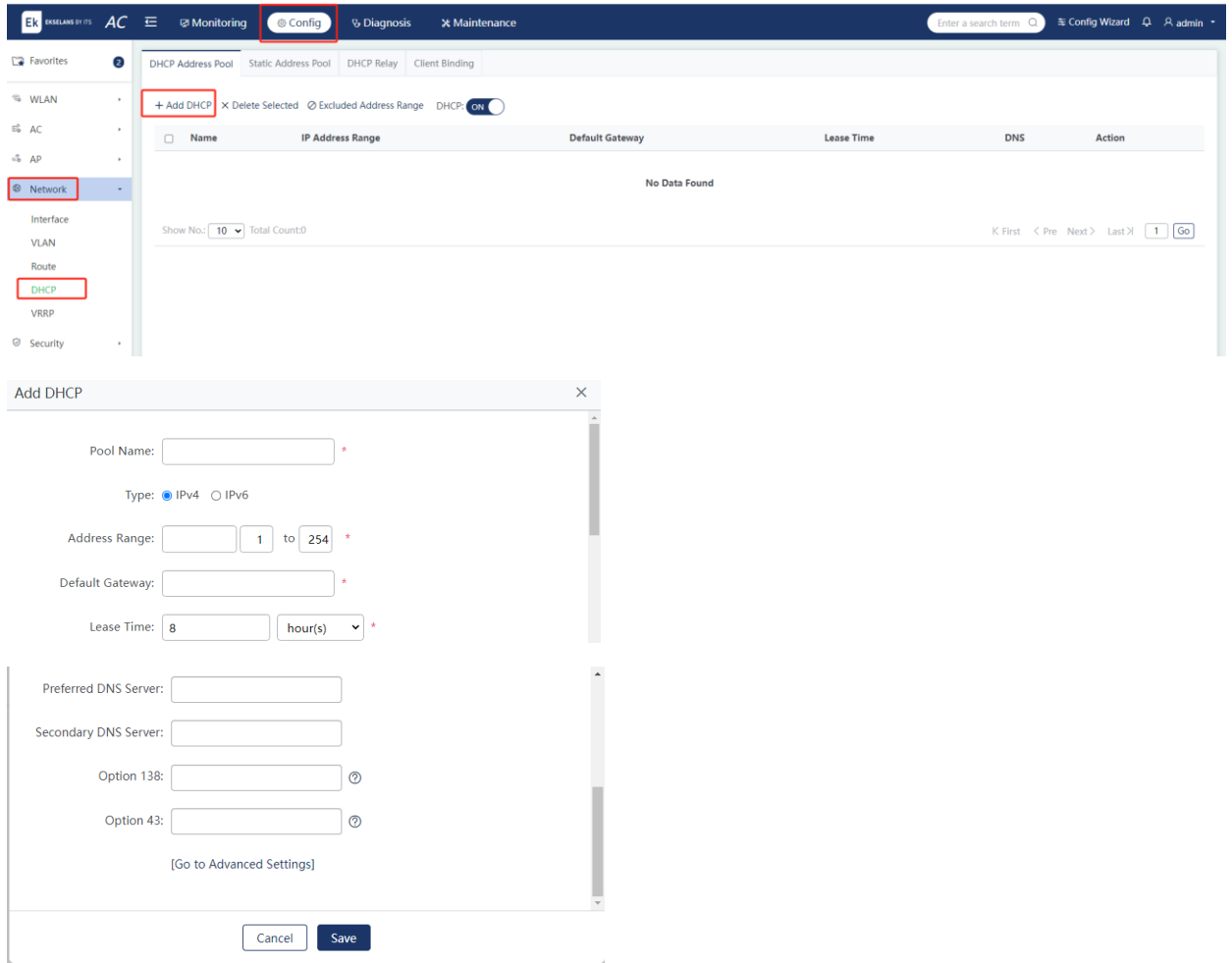
- (3) Editing routes: Click **Edit** in the **Action** column, and a window pops up displaying the information about the route. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.
- (4) Deleting routes: Click **Delete** in the **Action** column to delete a route. Select multiple items and click **Delete Selected**. Click **OK** in the pop-up window to batch delete routes.

5.4.4 DHCP

1. DHCP Address Pool

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

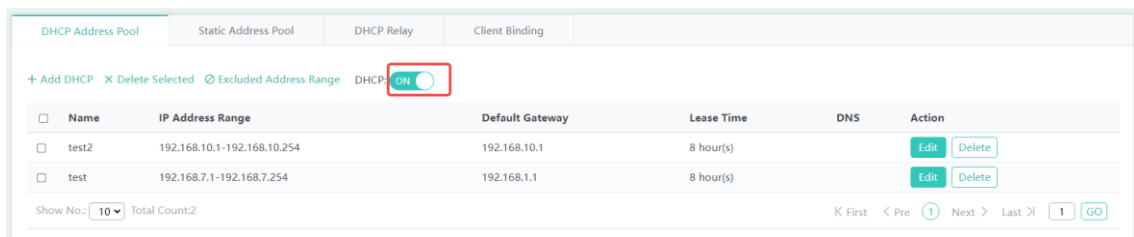
- (1) Adding DHCP address pools: Click **Add DHCP** and edit the fields in the pop-up window. Click **Save** and the DHCP address pool will be displayed in the list after a message indicating operation success appears.



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

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

- (2) Deleting DHCP pools: Click **Delete** in the **Action** column to delete a DHCP address pool. Select multiple items and click **Delete Selected**. Click **OK** in the pop-up window to batch delete DHCP address pools.
- (3) Configuring excluded address ranges: Click **Excluded Address Range**. Configure the range of IP addresses that will not be allocated to clients in the pop-up window. You can configure multiple excluded address ranges. Click **OK** and the excluded address ranges will be displayed in the list after a message indicating operation success appears.
- (4) Enabling or disabling DHCP service: Toggle on or off the button beside **DHCP** to enable or disable the DHCP service.

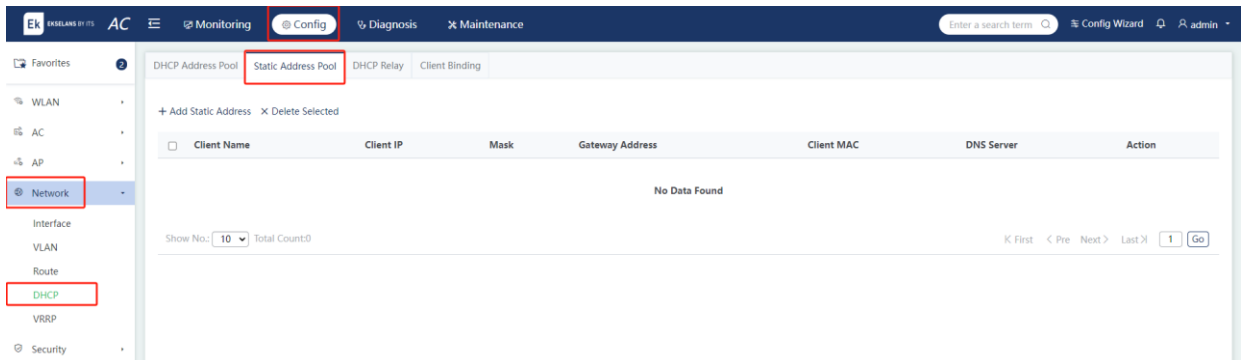


- (5) Editing DHCP address pools: Click **Edit** in the **Action** column and a window pops up displaying the information about the DHCP address pool. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.

2. Static Address Pool

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

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



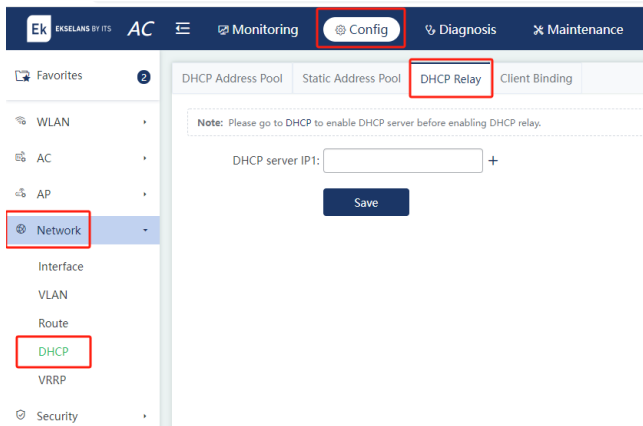
Parameter	Description
Client Name	Enter the name of the static address pool.
Client IP	Configure the IP address.
Mask	Configure the subnet mask.
Client MAC	Enter the MAC address of the client.
Gateway Address	Configure the IP address of the egress gateway. This field is mandatory.
DNS	Configure the DNS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

- (2) Deleting static IP address: Click **Delete** in the **Action** column to delete a static IP address. Select multiple items and click **Delete Selected**. Click **OK** in the pop-up window to batch delete static IP addresses.
- (3) Editing static IP address: Click **Edit** in the **Action** column and a window pops up displaying the information about the static IP address. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.

3. DHCP Relay

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

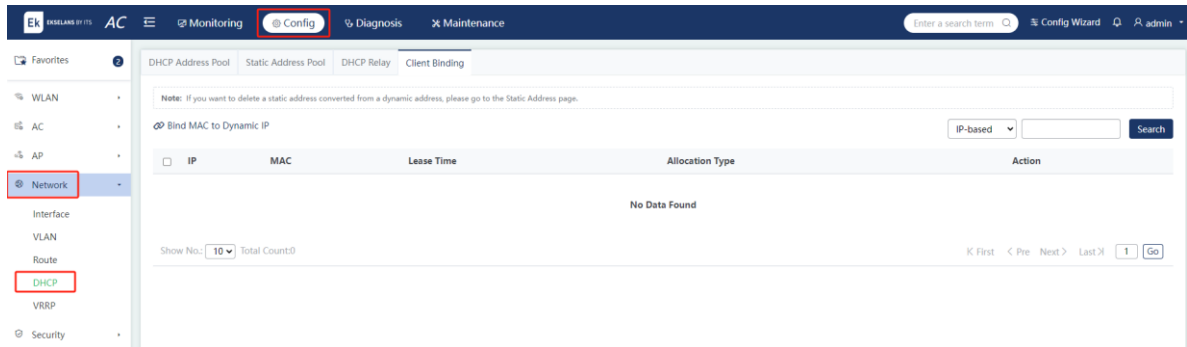
Enter the IP address of the DHCP relay and click **Save**.



4. Client Binding

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

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

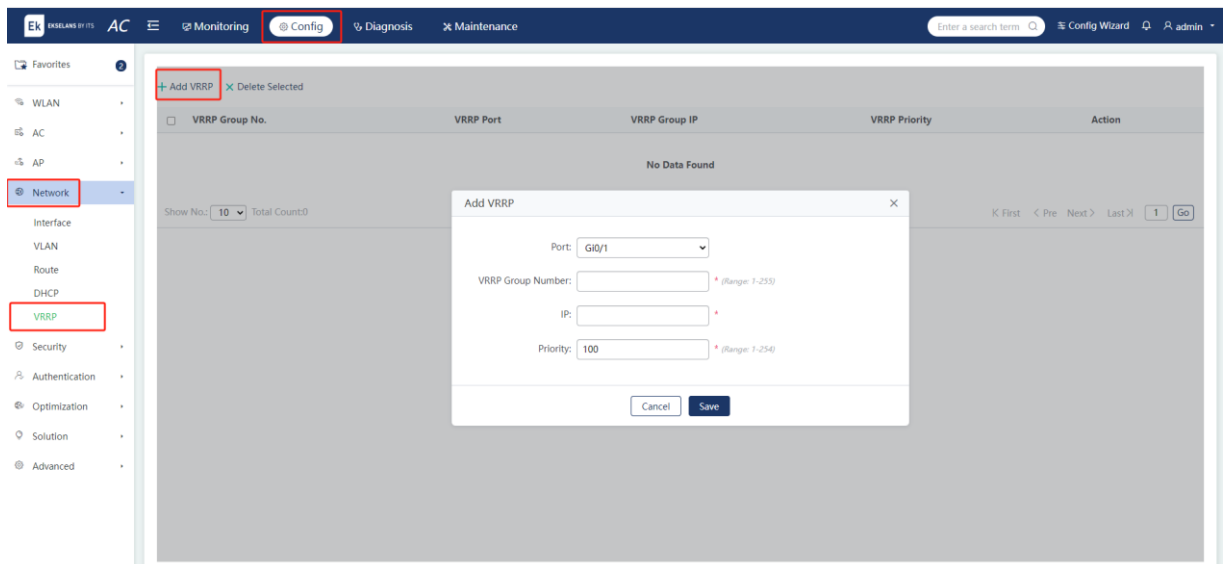


- (2) Unbinding MAC address with dynamic IP address: Click **Delete** in the **Action** column and a window pops up. Click **OK** to unbind the MAC address.
- (3) Searching for clients by IP address or MAC address: Enter the IP address or MAC address in the search bar. Click **Search** and the results are displayed in the list.

5.4.5 VRRP

Choose **Config > Network > VRRP**.

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



- (2) Deleting VRRP groups: Select the VRRP groups in the list and click **Delete Selected**. Click **OK** in the pop-up window to delete VRRP groups.
- (3) Editing VRRP groups: Click **Edit** in the **Action** column and a window pops up displaying the information about the VRRP group. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.

5.5 Security

5.5.1 Containment

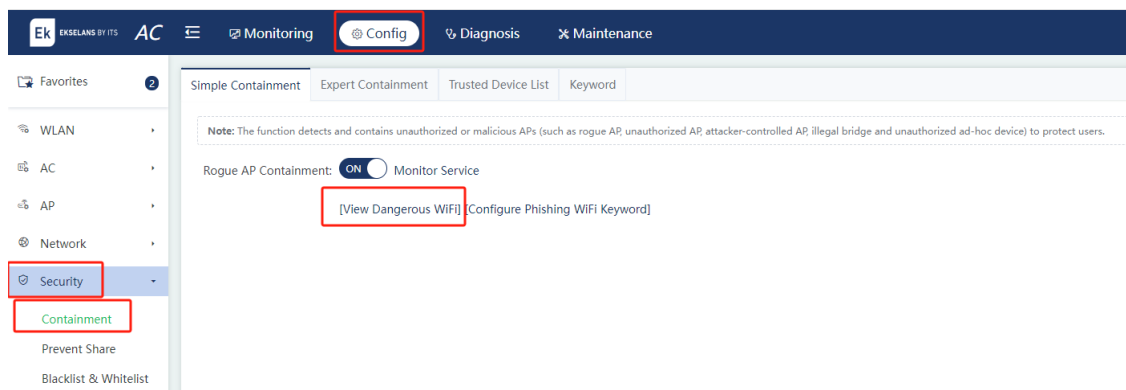
Choose **Config > Security > Containment**.

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

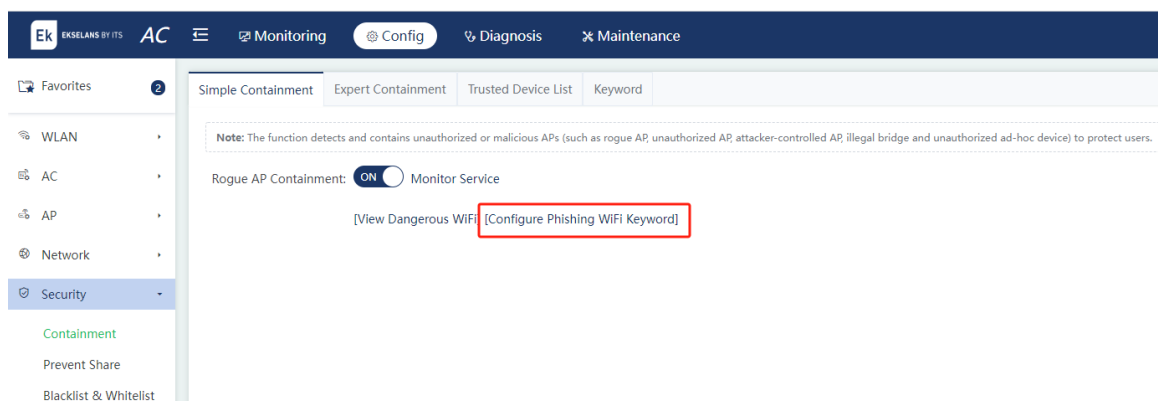
1. Basic Configuration for Containment

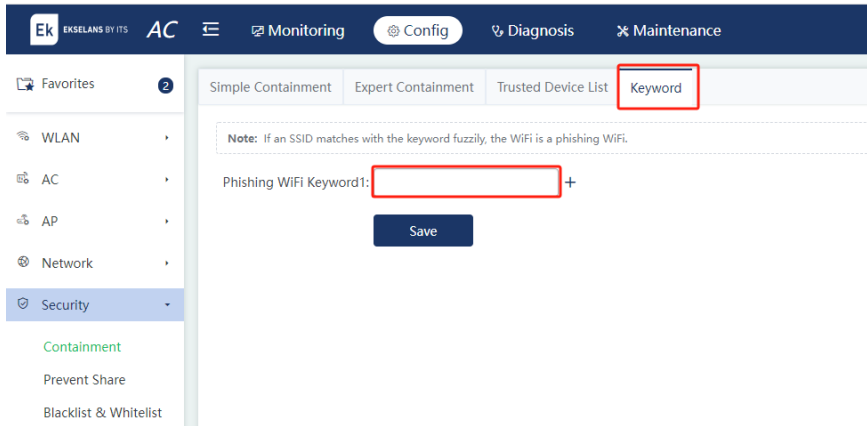
When containment is currently disabled, and no AP in monitoring or hybrid mode is detected, a pop-up window is displayed to ask users to enable the AP monitoring feature. Click **OK** to jump to the **Monitor Service** page.

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



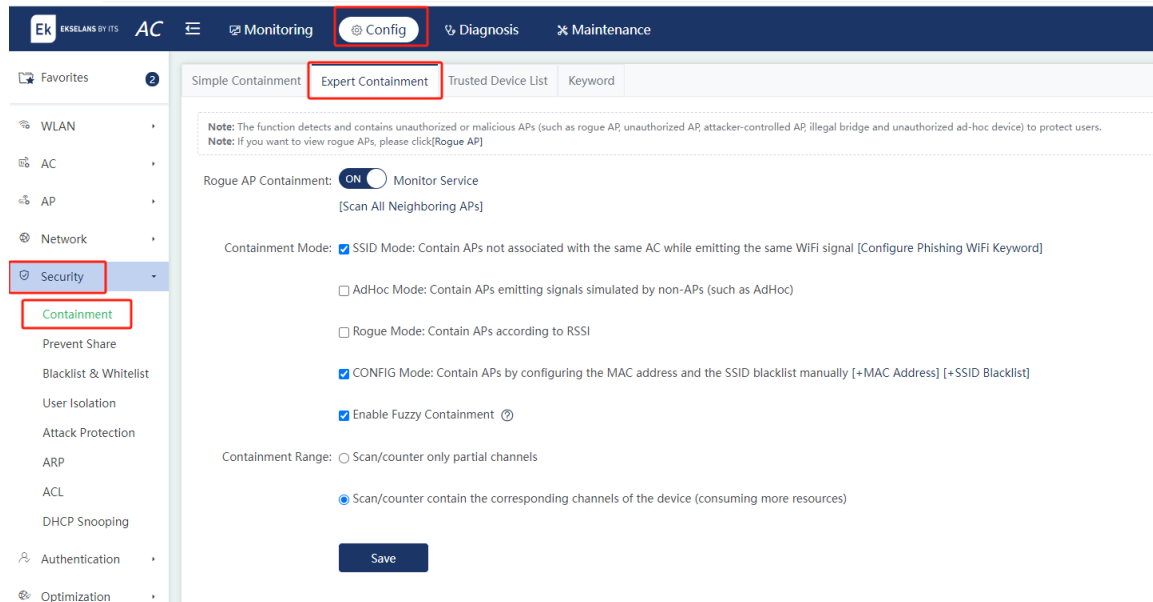
Click **Configure Phishing WiFi Keyword** to access the **Keyword** page and configure the keyword.





2. Specialized Configuration for Containment

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



- (1) Enable the monitoring mode for a specified AP: The AP must be configured with the hybrid or monitoring mode before the containment feature takes effect. Click **Monitor Service** to access the **Monitor Service** page. Click **Monitor** or **Hybrid** to configure the AP mode. The AP information is displayed on the pop-up dialog box. Edit the information. When the AP that provides the AI radio feature is configured with the monitoring mode, the AI radio should be monitored and contained first.

Simple Containment | **Expert Containment** | Trusted Device List | Keyword

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

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

Containment Mode: SSID Mode: Contain APs not associated with the same AC while emitting the same WIFI signal [Configure Phishing WIFI Keyword]
 AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)
 Rogue Mode: Contain APs according to RSSI
 CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [+MAC Address] [+SSID Blacklist]
 Enable Fuzzy Containment ⓘ

Containment Range: Scan/counter only partial channels
 Scan/counter contain the corresponding channels of the device (consuming more resources)

Save

Monitor Service

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

+ Batch Monitor AP-name-based **Search** **Reset**

<input type="checkbox"/>	AP Name	IP	MAC	Status	Work Mode	AP Mode
No Data Found						

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

Click **Save**. The **Save succeeded.** message is displayed.

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

Simple Containment | **Expert Containment** | Trusted Device List | Keyword

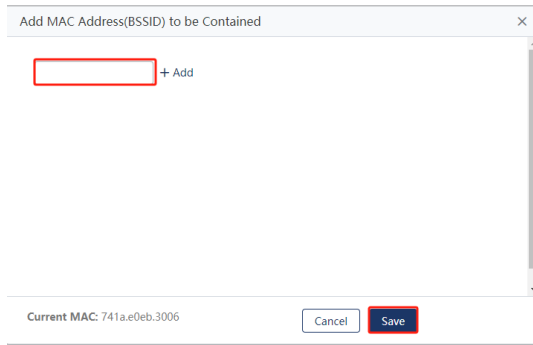
Note: The function detects and contains unauthorized or malicious APs (such as rogue AP, unauthorized AP, attacker-controlled AP, illegal bridge and unauthorized ad-hoc device) to protect users.
Note: If you want to view rogue APs, please click[Rogue AP]

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

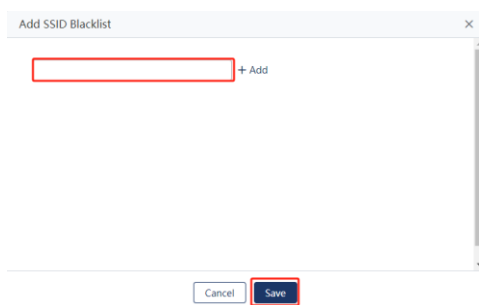
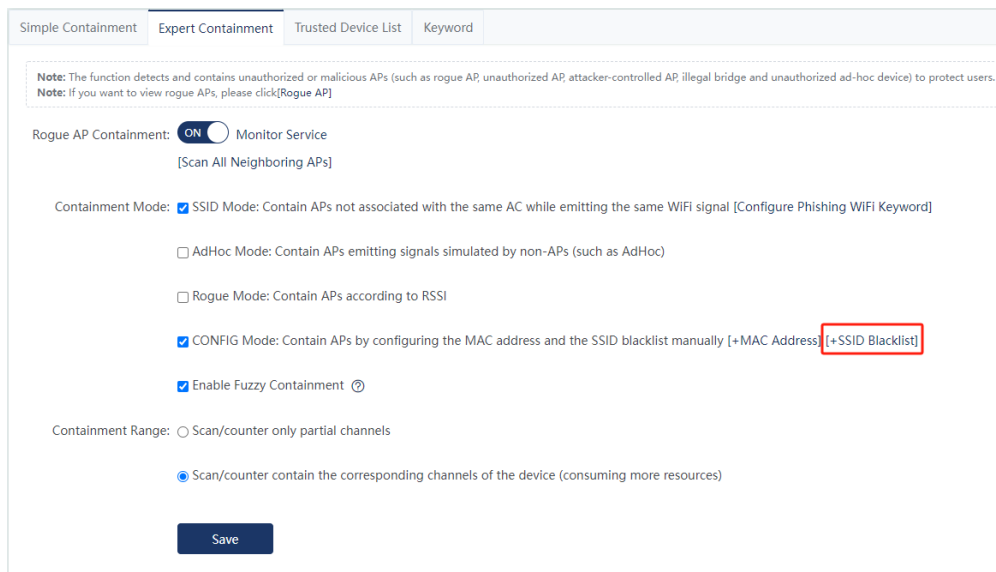
Containment Mode: SSID Mode: Contain APs not associated with the same AC while emitting the same WIFI signal [Configure Phishing WIFI Keyword]
 AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)
 Rogue Mode: Contain APs according to RSSI
 CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [+MAC Address] [+SSID Blacklist]
 Enable Fuzzy Containment ⓘ

Containment Range: Scan/counter only partial channels
 Scan/counter contain the corresponding channels of the device (consuming more resources)

Save

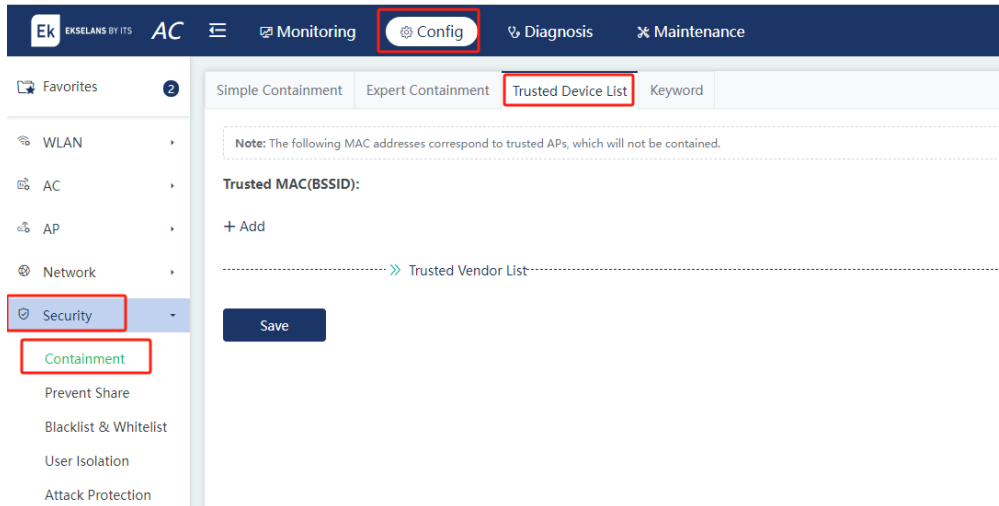


(3) Add an SSID blacklist:



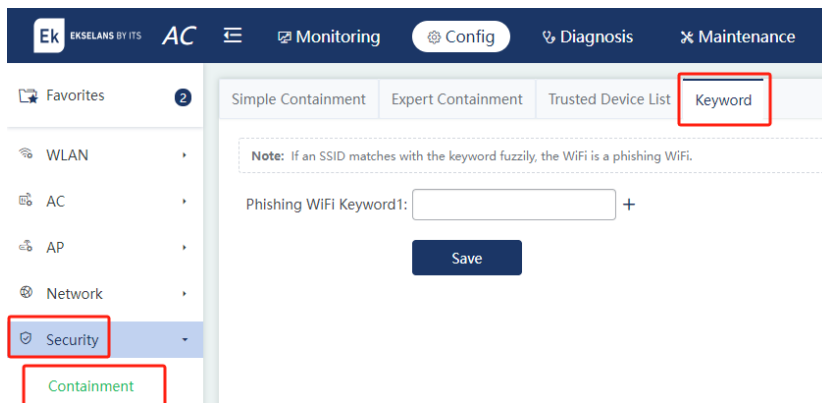
3. Trusted Device List

When the rogue AP containment feature is enabled on the AC, unauthorized APs will be contained, while some APs are trusted devices and should be treated differently. The MAC address of a trusted device can be configured.



4. Phishing Wi-Fi Keyword

Fuzzy matching of a phishing Wi-Fi keyword helps scan Wi-Fi signals on a network. If an SSID of a Wi-Fi network matches the keyword fuzzily, the Wi-Fi network is regarded as a phishing network.

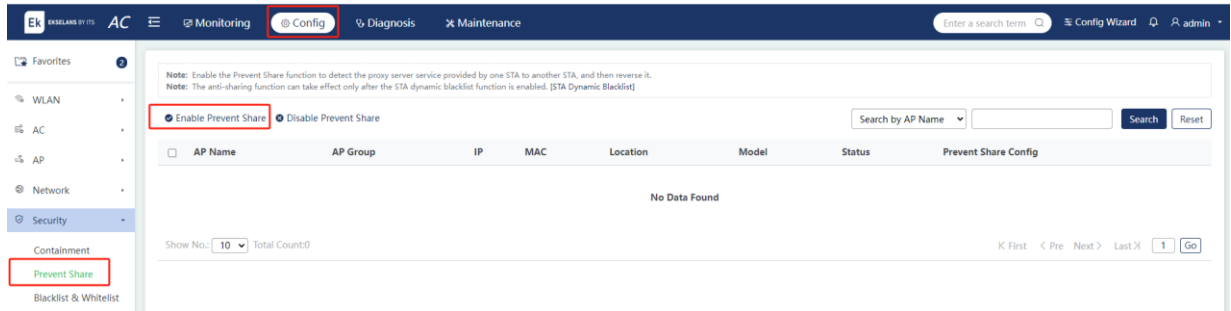


5.5.2 Sharing Prevention

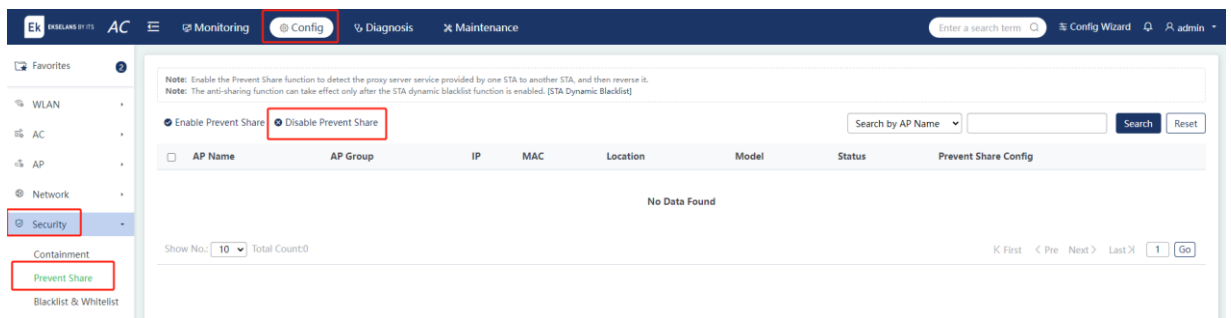
Choose **Config > Security > Prevent Share**.

After sharing prevention is enabled, the system detects whether one STA provides the proxy service to another and adds the STA providing the proxy service into the containment list.

- (1) Enable sharing prevention: Select APs to be enabled with sharing prevention in the list. Click **Enable Prevent Share**. In the pop-up confirmation dialog box, click **OK** to enable sharing prevention.



(2) Disable sharing prevention: Select APs for which sharing prevention needs to be disabled in the list. Click **Disable Prevent Share**. In the pop-up confirmation dialog box, click **OK** to disable sharing prevention.

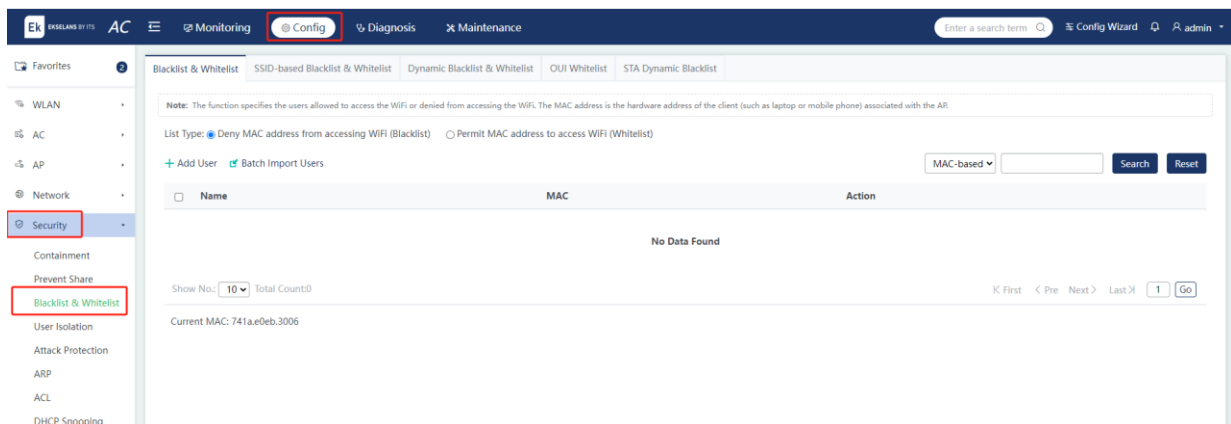


5.5.3 Configuring the Blocklist/Allowlist

Choose **Config > Security > Blacklist & Whitelist**.

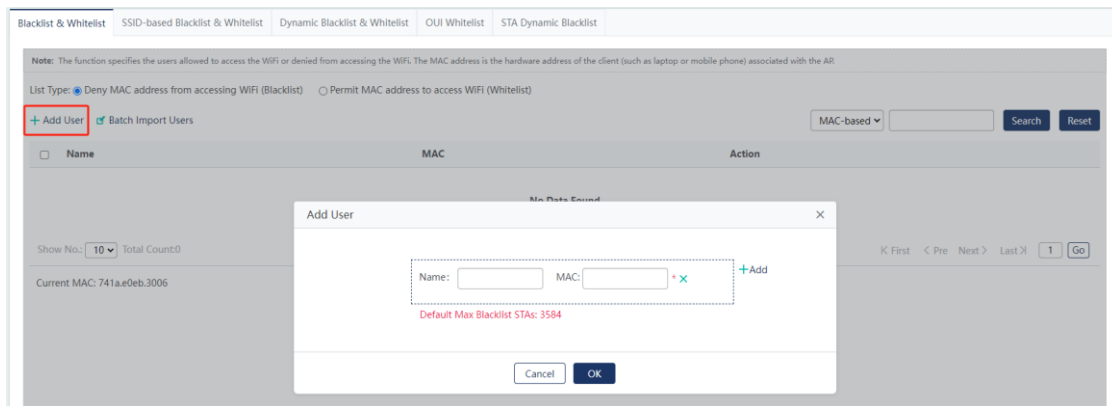
1. Configuring the Blocklist or Allowlist for the AC

To enhance wireless security, control the access of wireless users by assigning wireless access to certain users or prohibiting certain users from accessing the wireless network. The number of users that is allowed to access to Wi-Fi or rejected is 1,024 by default.

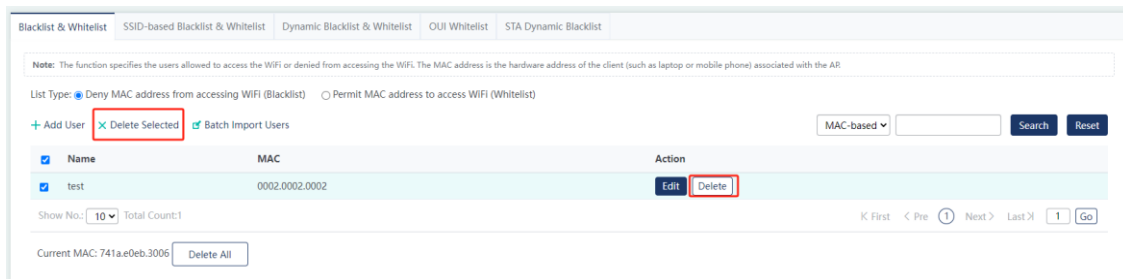


Add a MAC address to the blocklist or allowlist.

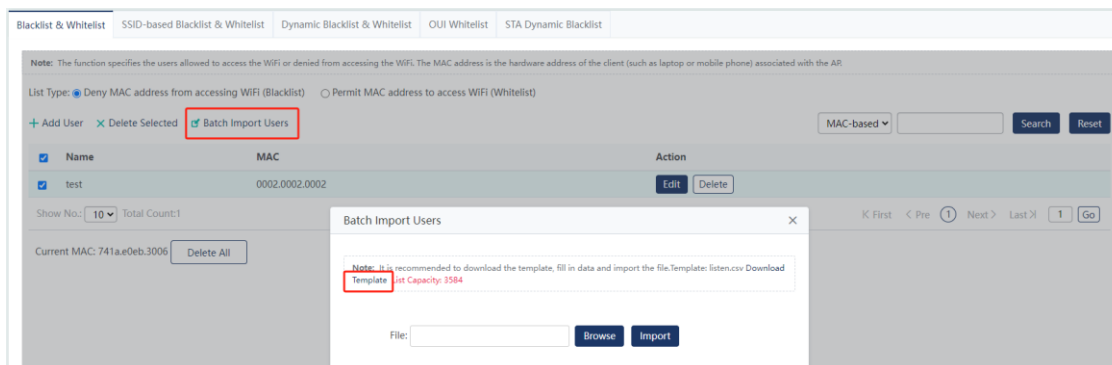
(1) Add a list: Click **Add User** to add the MAC address of a user. Multiple addresses can be added.



(2) Delete a list: Click **Delete** behind a specified list. The confirmation dialog box pops up. Click **OK** to finish the operation.

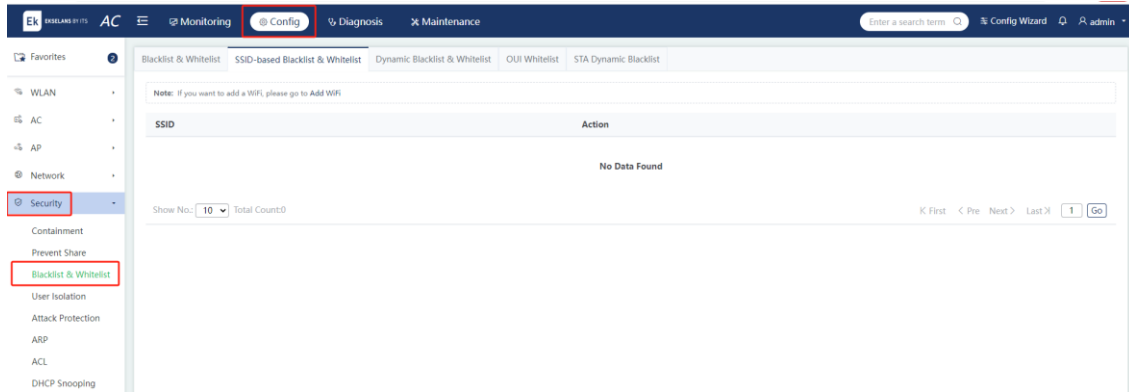


(3) Batch import lists: Click **Batch Import Users**. Download and fill in the template. Import the file.

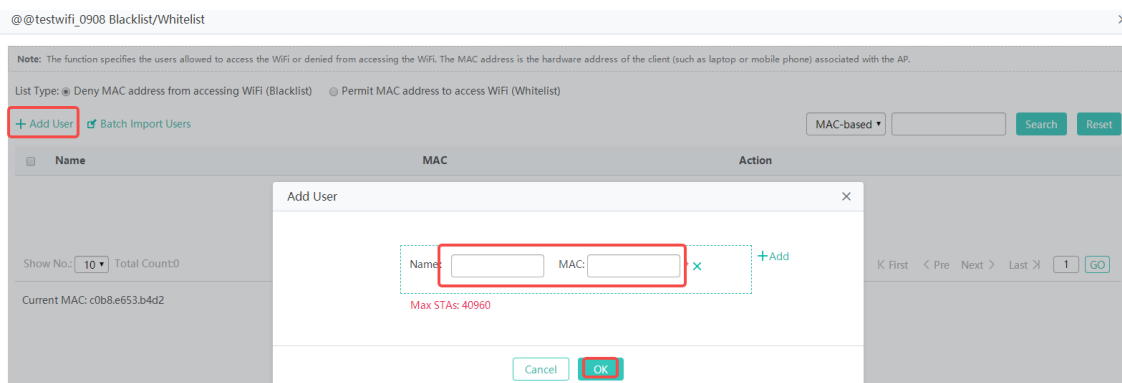


2. Configuring the SSID-based Blacklist or Allowlist

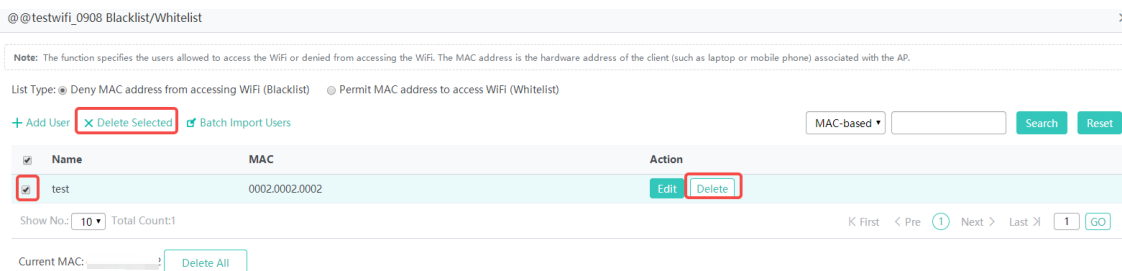
Click **Blacklist/Whitelist** for a specified Wi-Fi to access the configuration page. Select one list type.



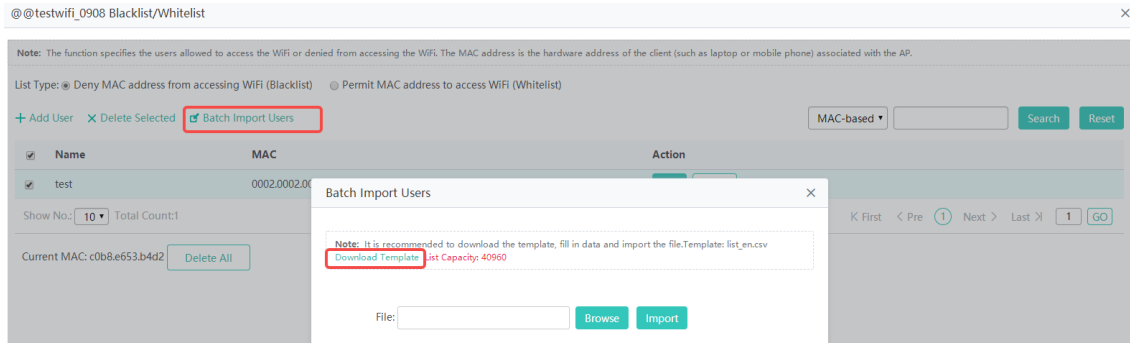
(1) Add a list: Click **Add User**. Add the MAC address of a device. Click **OK**.



(2) Delete a list: Click **Delete** behind a specified list. The confirmation dialog box pops up. Click **OK** to finish the operation.



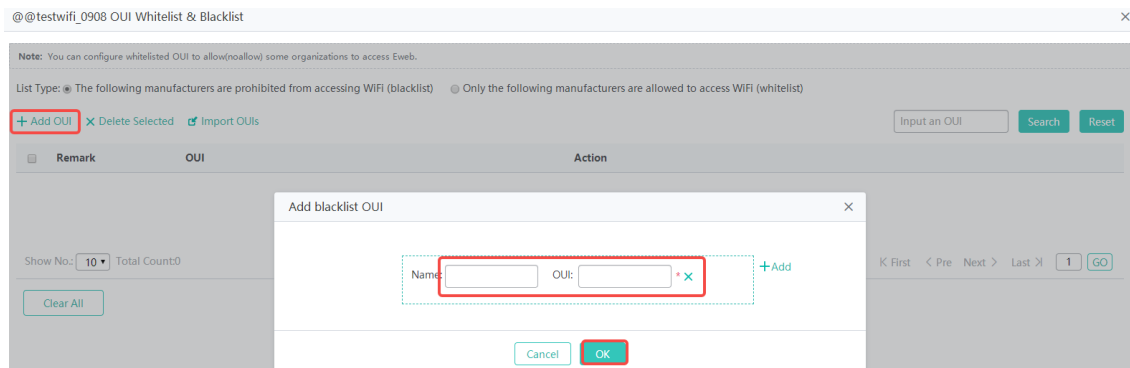
(3) Batch import blocklists: Click **Batch Import Users**. Download the template. Fill in the template and save it. Click **Browse**. Select the preceding saved template. Click **Import**.



(4) Configure Organizationally Unique Identifiers (OUIs): An OUI is the first 8 bits of the MAC address of a device. If devices to be added to the blacklist or allowlist belong to the same manufacturer, add their OUI into the list directly, without the need to add the MAC address of each device one by one.

Click **Add OUI**. Access the **Add blacklist OUI** page.

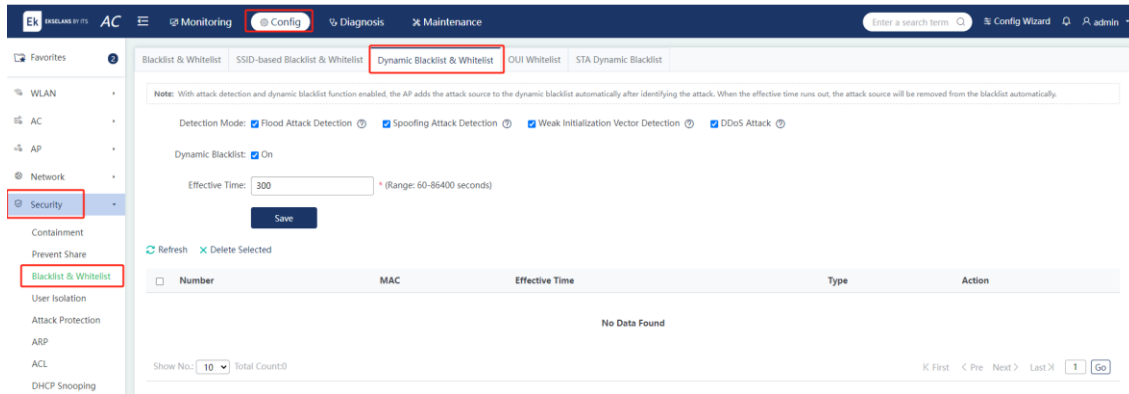
Click **Add**. Enter the name and OUI of a manufacturer. Click **OK**.



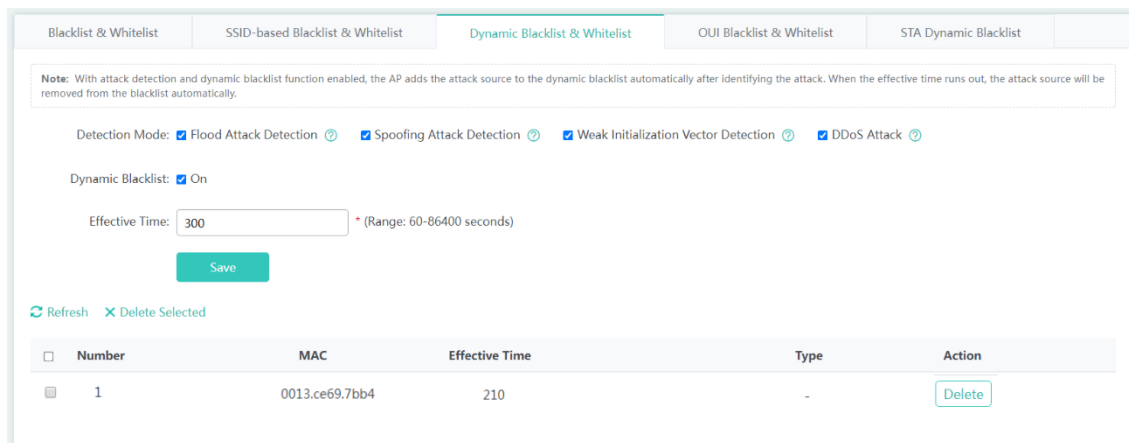
3. Dynamic Blacklist

Dynamic blacklist: Add malicious attack sources to the dynamic blacklist to prevent their access. After a detection mode is configured and dynamic blacklist is enabled, the device will automatically add the attack source to the dynamic blacklist when an attack is detected. After the effective time expires, the attack source will be automatically deleted from the blacklist.

Configure dynamic blacklist: Select a detection mode, enable dynamic blacklist, configure the effective time, and click **Save**.

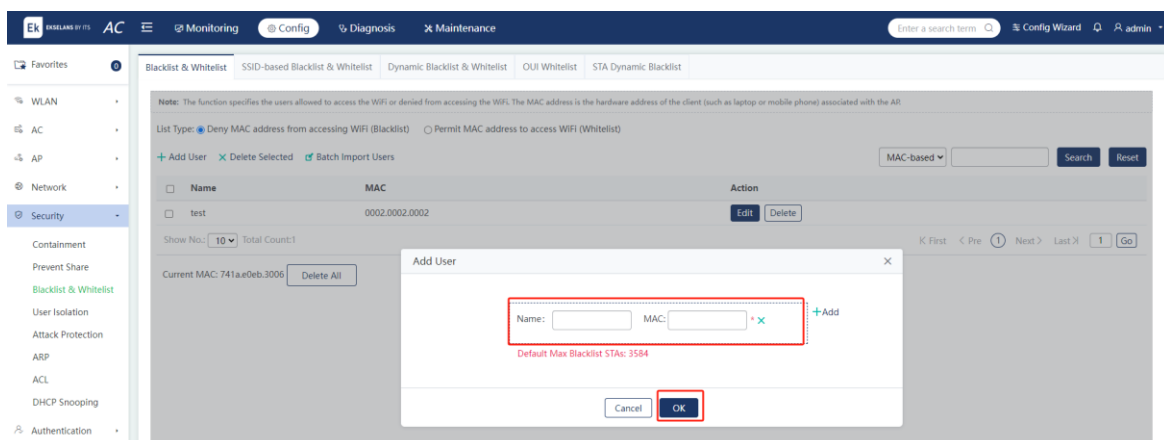


Delete a blocklist: Select the blocklist to be deleted from the list. Click **Delete Selected**. The confirmation dialog box pops up. Click **OK** to finish the operation.



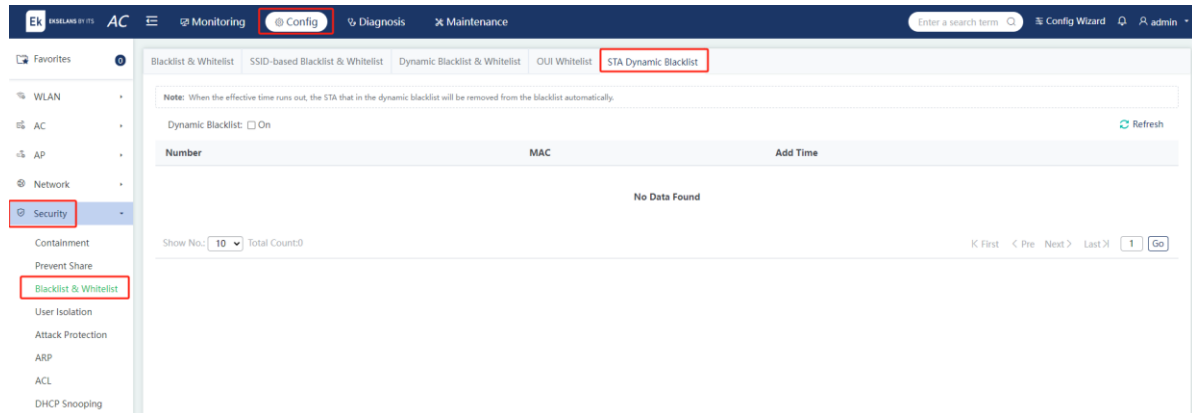
4. Configuring the OUI Blacklist or Allowlist for the AC

Configure manufacturer information: Click **Add OUI**. Enter the name and OUI of a manufacturer. Click **OK**.



5. STA Dynamic Blacklist

Add STAs from malicious attack sources to the STA dynamic blacklist to prevent them from accessing the network.

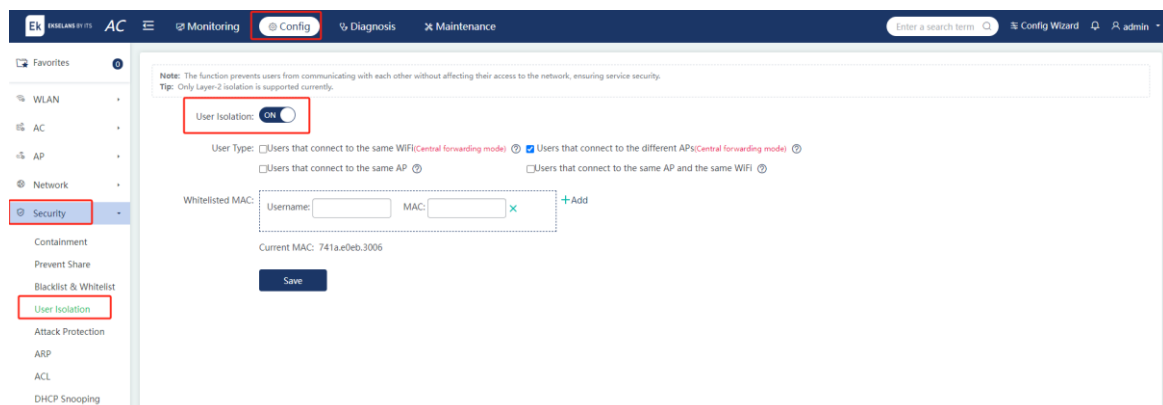


5.5.4 User Isolation

Choose **Config > Security > User Isolation**.

To ensure network security and information confidentiality, intranet users can be configured not to communicate with each other. Some special users (users who can access each other) can be identified by user name and MAC address.

Toggle on or off the user isolation switch to enable or disable mutual access between intranet users. Select the types of users to be isolated. Click **Add** to add MAC addresses of users for mutual access. Click **x** to delete a specified user MAC address.

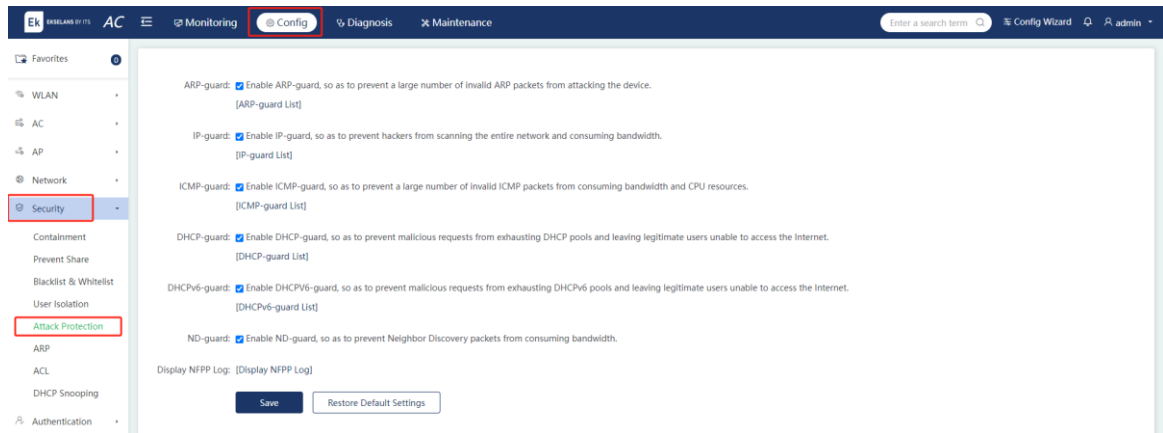


5.5.5 Attack Prevention

Choose **Config > Security > Attack Protection**.

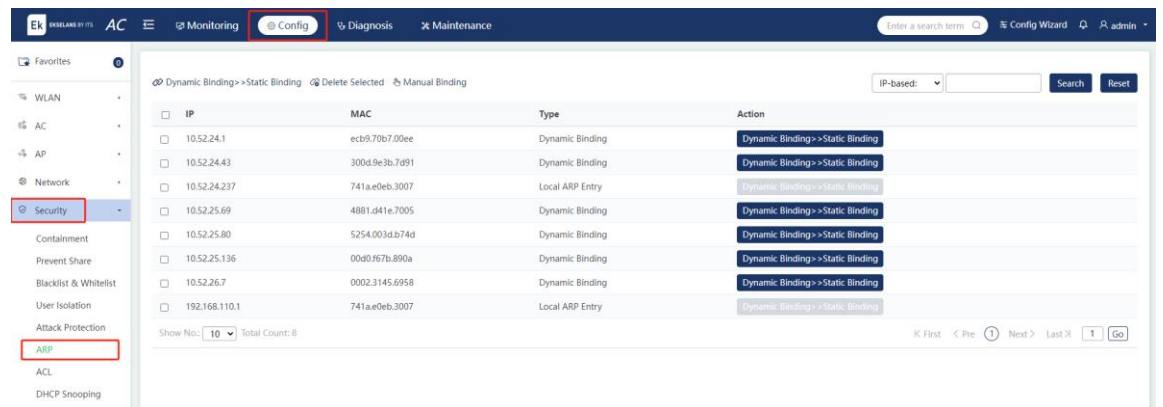
Malicious attacks often occur in a network environment. These attacks overload the switch, resulting in high CPU usage and an operation failure of the switch.

Select attack prevention types and click **Save**. Click the text within square brackets ([]) to display the list.

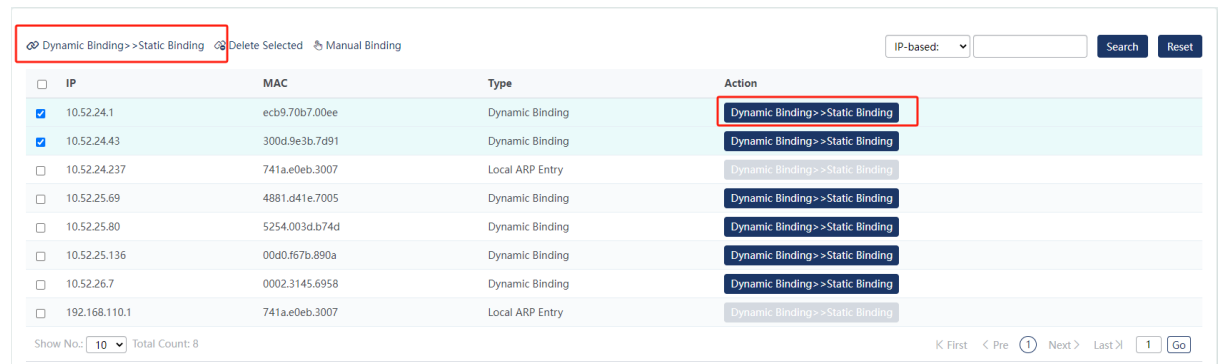


5.5.6 ARP Entry Binding

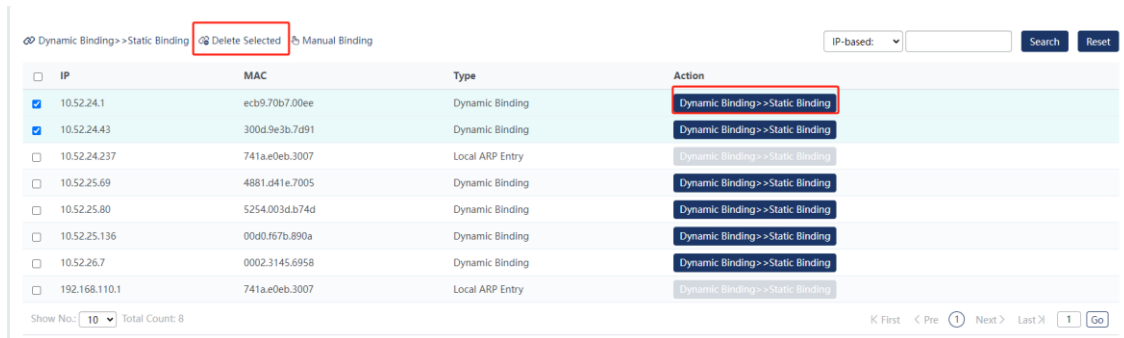
Choose **Config > Security > ARP**.



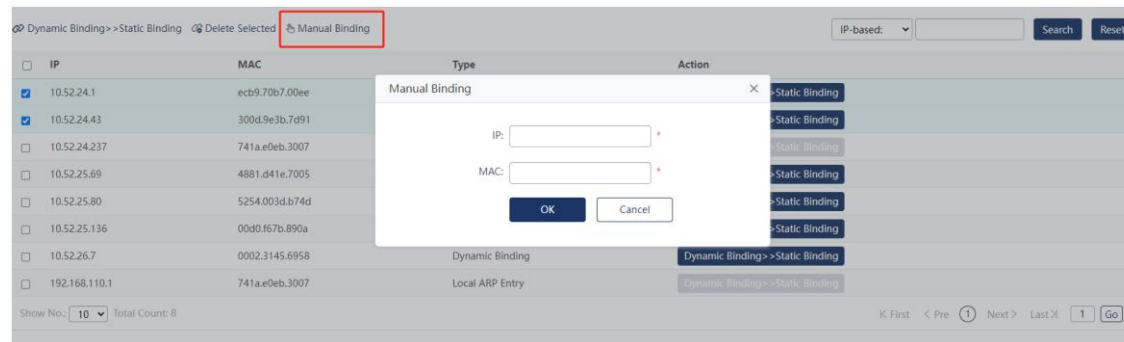
(1) Convert dynamic bindings to static bindings: Select one or more records in the ARP list. Click **Dynamic Binding >> Static Binding** to batch convert dynamic bindings to static bindings.



- (2) Delete static bindings: Select one or more records in the ARP list. Click **Delete Selected** to batch delete the static bindings.



- (3) Manual binding: Click **Manual Binding**. Enter the IP and MAC addresses. Click **OK**. The **Configuration succeeded.** message is displayed. The new entry is displayed in the ARP list.



5.5.7 ACL

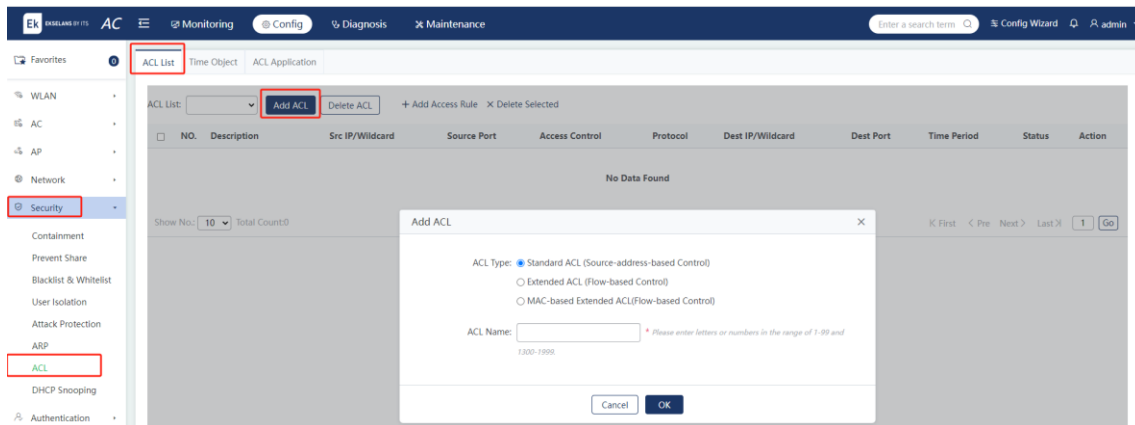
Choose **Config > Security > ACL**.

When receiving a packet, a device interface on which an ingress ACL is configured checks whether the packet matches an access control entry (ACE) in the ingress ACL. When sending out a packet, a device interface on which an egress ACL is configured checks whether the packet matches an ACE in the egress ACL.

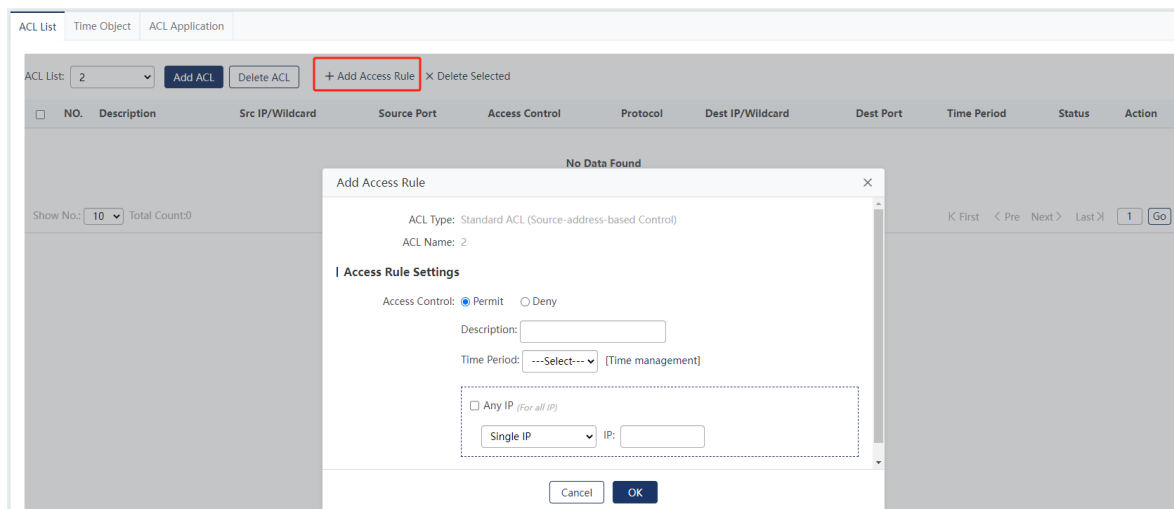
When different ACEs are configured, multiple ACEs may be applied at the same time, or only some ACEs are applied. Packets are processed according to the first matched ACE (permit or deny).

1. ACL List

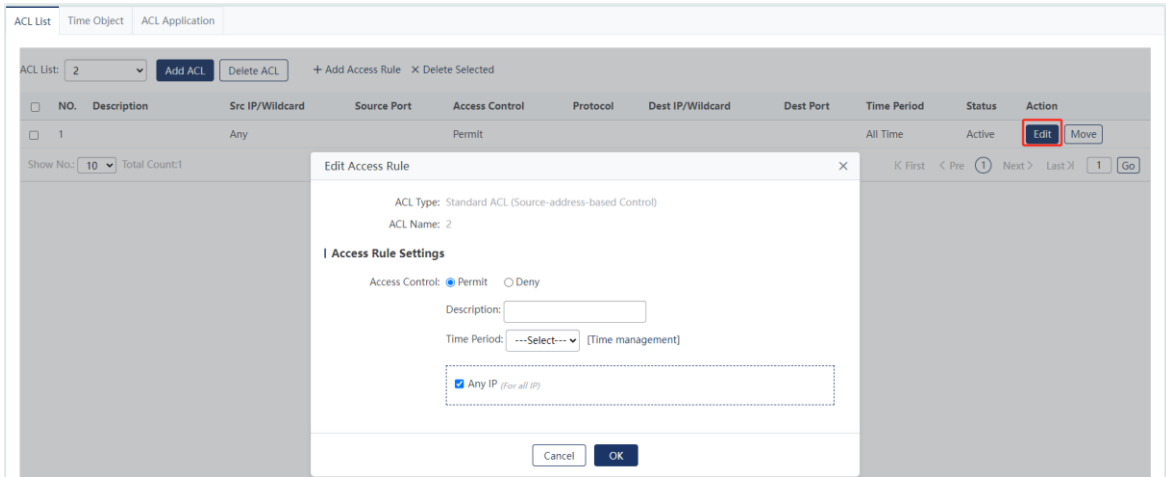
- (1) Add an ACL: Click **Add ACL**. Configure ACL information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added ACL is displayed in the drop-down ACL list in the upper left corner.



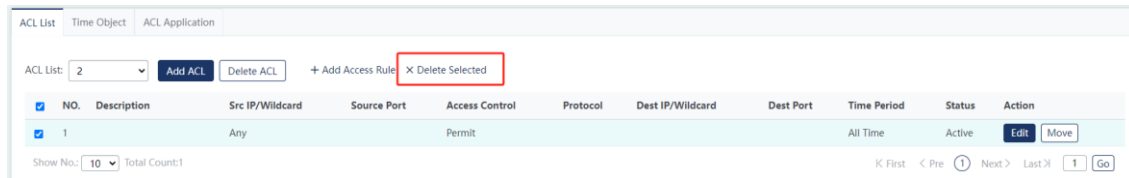
- (2) Delete an ACL: Select the ACL to be deleted from the drop-down ACL list. Click **Delete ACL**. The confirmation dialog box pops up. Click **OK** to finish the operation.
- (3) Add an ACE: Select an ACL to which an ACE needs to be added from the drop-down ACL list. Click **Add Access Rule**. Configure ACE information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added ACE is displayed in the ACL list.



- (4) Edit an ACE: Click **Edit** behind a specified ACE in the ACL list. The pop-up dialog box displays the information about the ACE. Edit the information. Click **OK**. A message indicating the configuration has been saved is displayed.

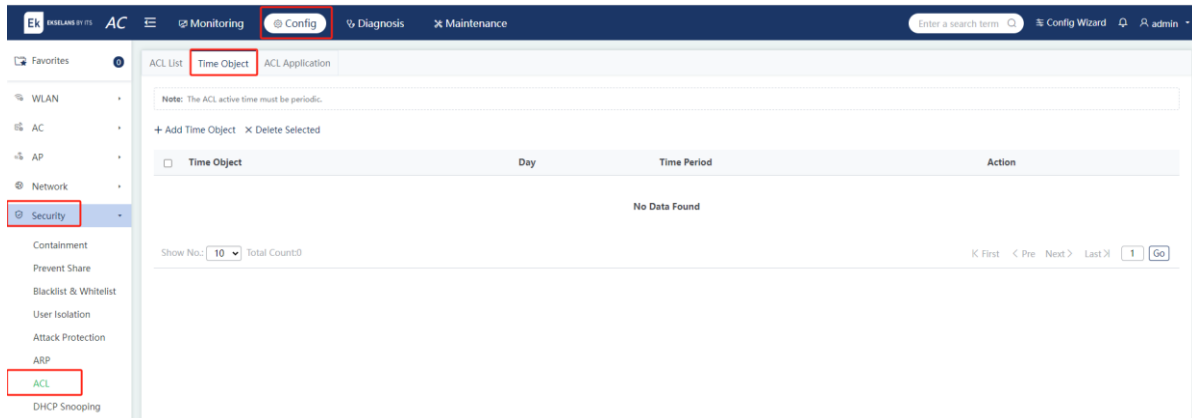


(5) Delete an ACE: Select one or more records in the ACL list. Click **Delete Selected**. The confirmation dialog box pops up. Click **OK** to finish the operation.

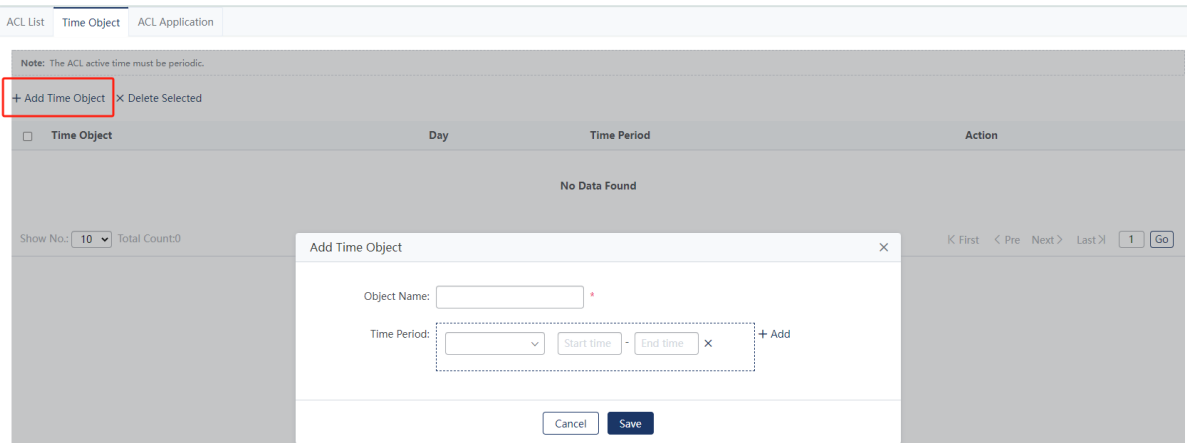


2. ACL Time Period

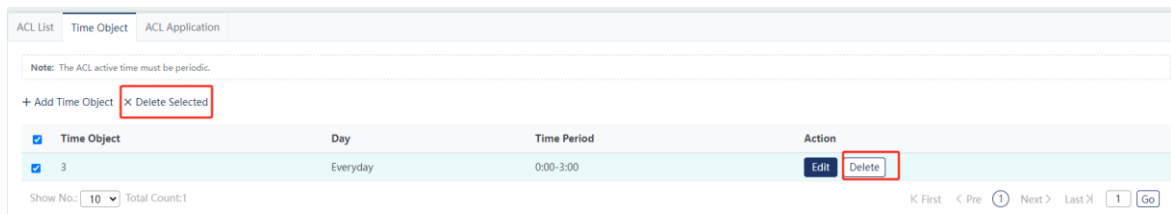
An ACL can be configured to take effect based on time, for example, in some time periods of a week. To enable this function, you must configure a time object first.



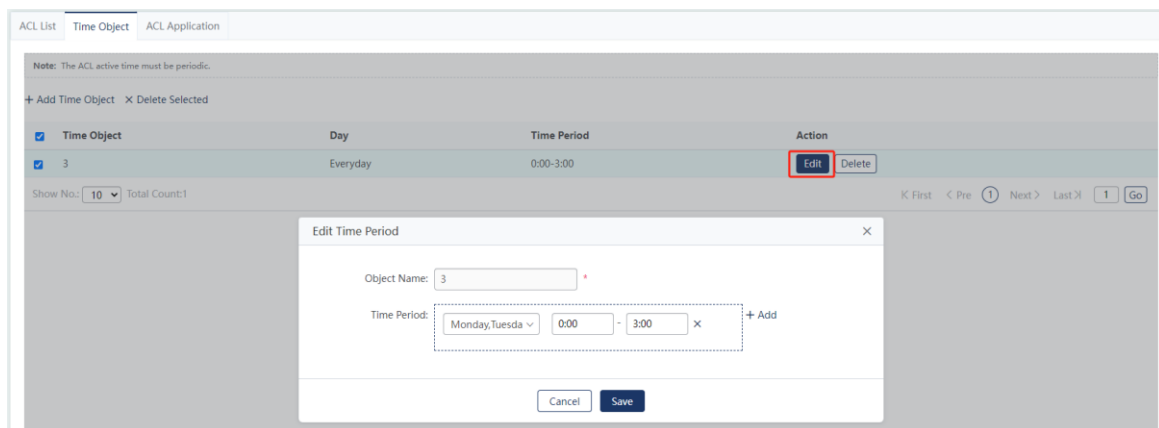
(1) Add a time object: Click **Add Time Object**. Configure the time object information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed.



- (2) Delete a time object: Click **Delete** behind a specified time object in the list. The confirmation dialog box pops up. Click **OK** to finish the operation. To delete multiple time objects, select time objects to be deleted in the list. Click **Delete Selected**. The confirmation dialog box pops up. Click **OK** to finish the operation.



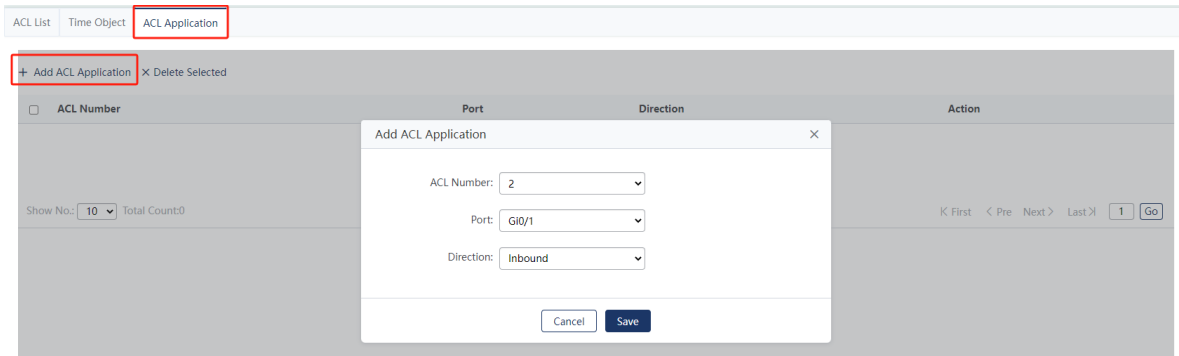
- (3) Edit a time object: Click **Edit** behind a specified time object in the list. The pop-up dialog box displays the information about the time object. Edit the information. Click **OK**. A message indicating the configuration has been saved is displayed.



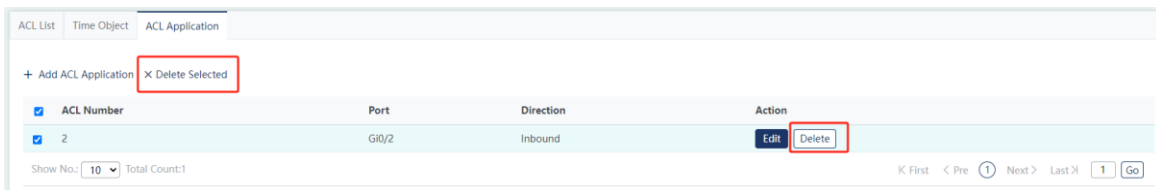
3. ACL Application

You can configure ACEs and apply them to interfaces or Wi-Fis to restrict the access of specified users or allow users to access specified networks.

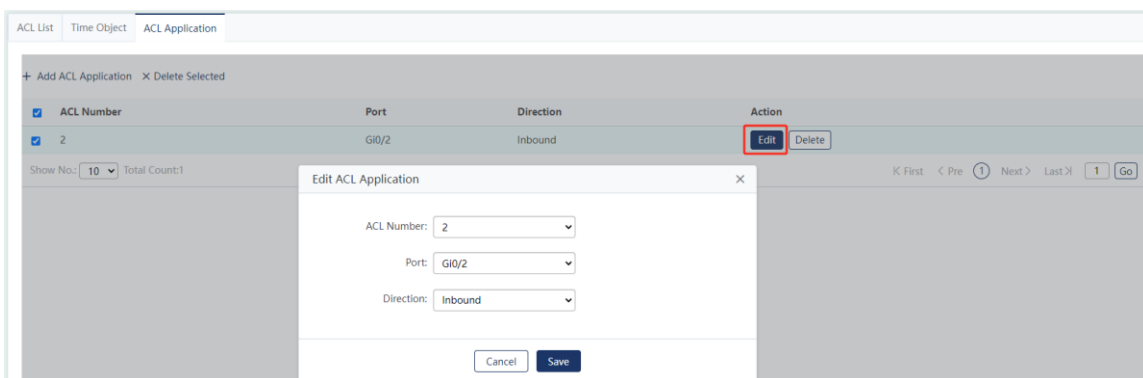
- (1) Add ACL application: Click **Add ACL Application**. The **Add ACL Application** dialog box pops up. Configure the information. Click **Save**. A message indicating the configuration has been saved is displayed. The newly added ACL application entry is displayed in the list.



- (2) Delete ACL application: Click **Delete** behind a specified ACL application entry in the list. The confirmation dialog box pops up. Click **OK** to finish the operation. To delete multiple ACL application entries, select one or more records in the ACL application list. Click **Delete Selected** to batch delete the records. The confirmation dialog box pops up. Click **OK** to finish the operation.

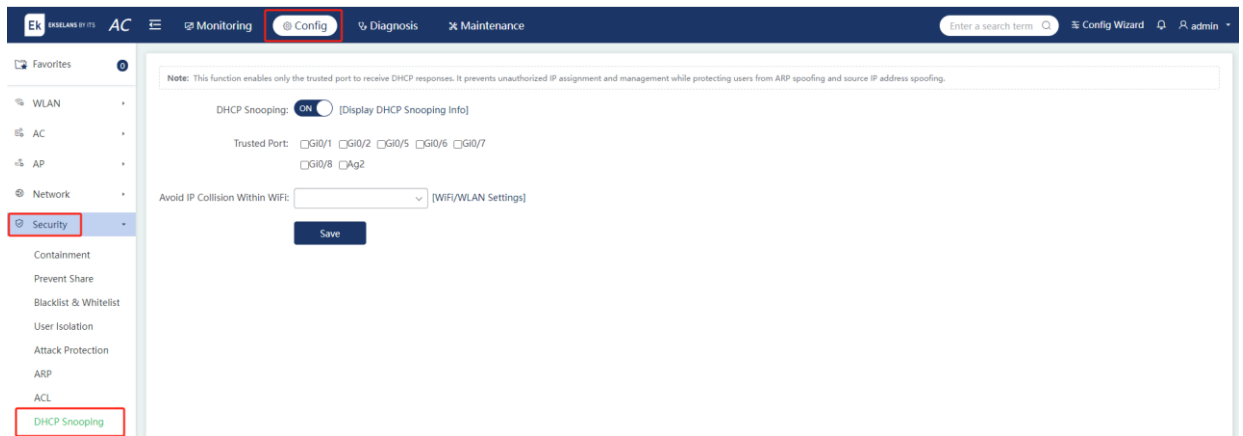


- (3) Edit ACL application: Click **Edit** behind a specified ACL application entry in the list. The pop-up dialog box displays the information about the ACL application. Edit the information. Click **Save**. A message indicating the configuration has been saved is displayed.



5.5.8 DHCP Security

Click **Config > Security > DHCP Snooping**.



Parameter	Description
DHCP Snooping	Enables or disables the DHCP snooping feature.
Display DHCP Snooping Info	Displays the information about users and bounded IP addresses saved on the AC.
Trusted Port	Enables the AC to only forward DHCP packets received on trusted ports.
Avoid IP Collision Within WiFi	Specifies the Wi-Fi network to be enabled with the IP address conflict prevention feature. After this feature is enabled, the AC will filter users connecting to the Wi-Fi based on the information about users and bounded IP addresses.

5.6 Authentication

5.6.1 Web-based Authentication

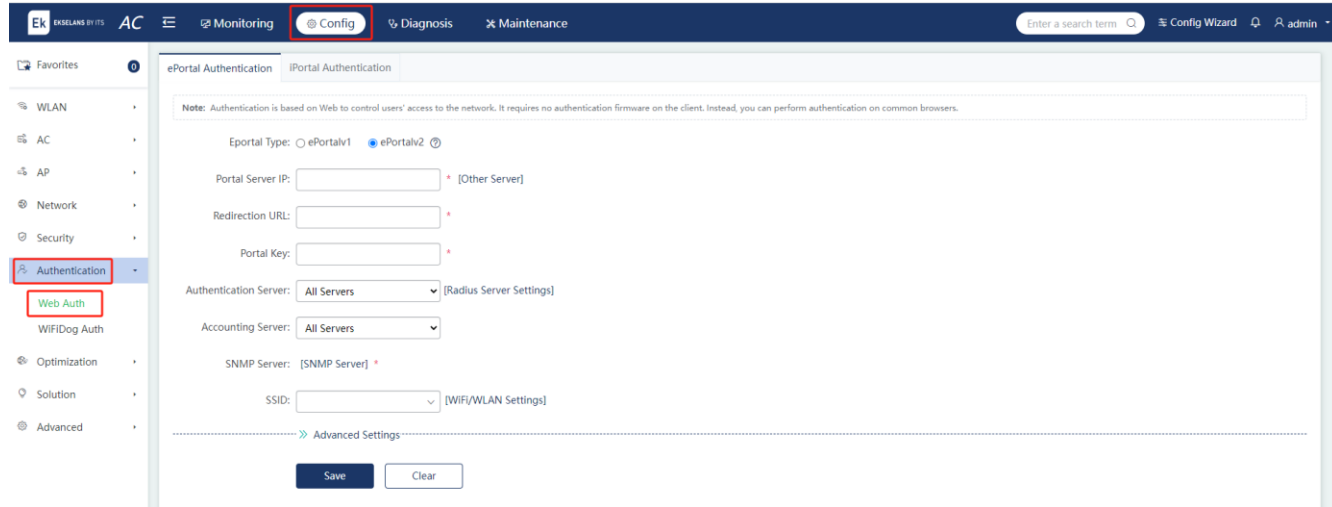
Choose **Config > Authentication > Web Auth**.

Web-based authentication is an identity authentication method for controlling user permissions for network access. This authentication method does not require dedicated client authentication software. Identity authentication can be implemented using a common browser. Real-name authentication facilitates user management. Based on the location of the authentication server, web-based authentication is classified into **ePortal Authentication** and **iPortal Authentication**.

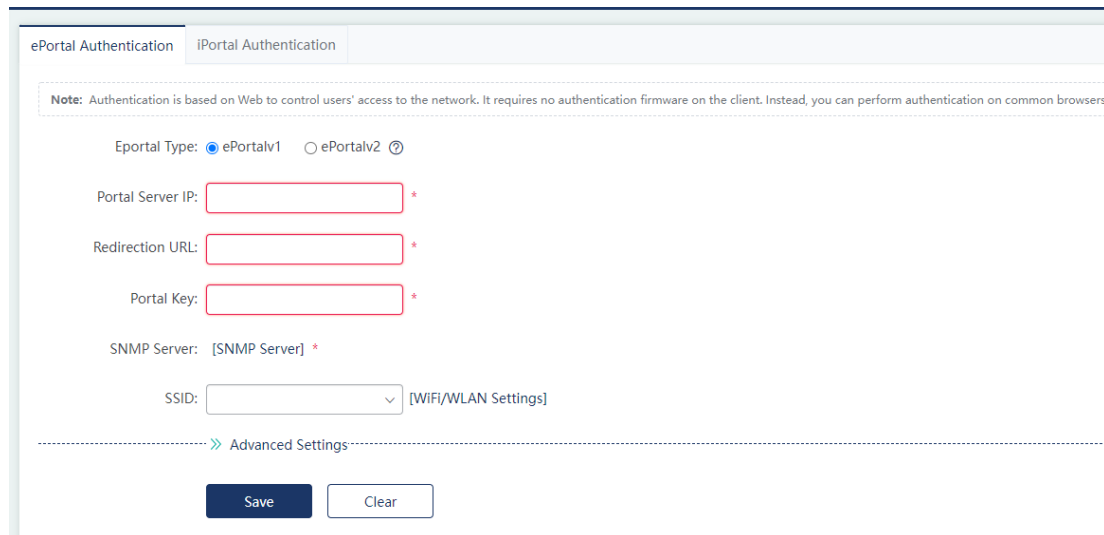
1. ePortal Authentication

When unauthenticated users access the Internet through a browser, the access device forcibly redirects the browser to a specified URL to perform authentication. When the portal (the

authentication web page) is located in a separate device outside the AC, the authentication is external web-based authentication.



(1) **ePortalv1:**



Parameter	Description
Portal Server IP	In template configuration mode, use the ip { ip-address } command to configure the server IP address. 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 that users will be redirected to, typically the portal authentication page.
Portal Key	Configures a key for the communication between the device and the authentication server.

SNMP Server	When the device detects that a user goes offline, it notifies the portal server. The server sets the device to delete user information (through the SNMP protocol). The portal server returns the offline page to the user. Therefore, an SNMP server should be configured for the ePortalv1 .
SSID	Specifies the Wi-Fi network to be configured with the ePortalv1 . Note: Only global authentication mode is supported currently. WLAN-based authentication mode is not available.

(2) **ePortalv2:**

ePortal Authentication

iPortal Authentication

Note: Authentication is based on Web to control users' access to the network. It requires no authentication firmware on the client. Instead, you can perform authentication on common browsers.

Eportal Type: ePortalv1 ePortalv2 ?

Portal Server IP: * [Other Server]

Redirection URL: *

Portal Key: *

Authentication Server: All Servers v [Radius Server Settings]

Accounting Server: All Servers v

SNMP Server: [SNMP Server] *

SSID: v [WiFi/WLAN Settings]

>> Advanced Settings <<<

Save

Clear

Parameter	Description
Portal Server IP	In template configuration mode, use the ip { ip-address } command to configure the server IP address. 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 that users will be redirected to, typically the portal authentication page.
Portal Key	Configures a key for the communication between the device and the authentication server.
Authentication Server	To successfully apply second-generation web authentication, Authentication, Authorization, and Accounting (AAA) authentication must be configured.

	The authentication method list associates web-based authentication requests with the RADIUS server. The NAS selects the authentication method and server based on the web authentication method list.
Accounting Server	Mandatory. To successfully apply second-generation web-based authentication, AAA accounting must be configured. Accounting is used to associate an accounting method with the server. In web authentication, accounting is implemented to record user information or fees.
SNMP Server	The SNMP server is used for the communication between users and the portal server.
SSID	Second-generation authentication is applied to Wi-Fi networks.

2. iPortal Authentication

When unauthenticated users access the Internet through a browser, the access device forcibly redirects the browser to a specified URL to perform authentication. When the portal (the authentication web page) is located within the AC, the authentication is internal web-based authentication. The authentication page allows for partial custom settings, including the custom logo, title, and disclaimer. When the one-click Internet access feature is enabled, users can click **Log In** on the authentication page to pass authentication without inputting a username and password. This feature takes effect only when the authentication page is set to the system default or partial custom mode.

ePortal Authentication
iPortal Authentication

Download Template: Default

Select WiFi:

One-Click Auth: Enable ?

Auth Account: Local User Management

Auth Page Settings: Default Partially Custom Fully Custom

∨ Advanced Settings

AD Push Mode:

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

Settings: [Advanced Settings]

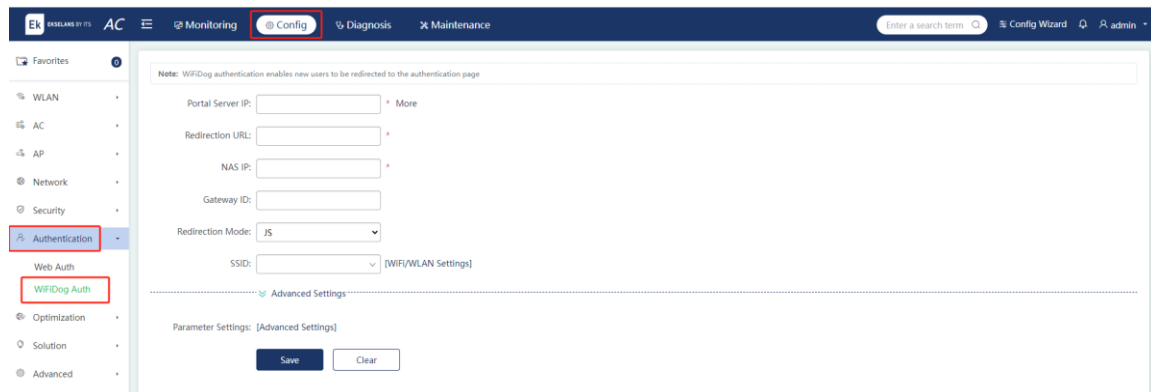
Save
Clear

Parameter	Description
Auth Account	The following authentication account sources are supported: Use user information on the server preferentially Use local user information preferentially Use user information on the server only User local user information only
Auth Page Settings	Supports system default settings, partial custom settings, and full custom settings.
AD Push Mode	The advertisement push mode includes advertisement push before or after authentication. No advertisement is configured by default.
iPortal Server Port	Configures the port number of the authentication page for internal portal authentication. The default port number is 8,081.

5.6.2 WiFiDog Authentication

Choose **Config > Authentication > WiFiDog Auth**.

Unauthenticated users can be redirected to the authentication page for authentication. Click **More** to access the **WiFiDog Auth Server List** page.



- (1) Add a WiFiDog authentication server: Click **Add Authentication Server**. Configure the ACL information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added server is displayed in the server list.

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

Portal Server IP: * **More**

Redirection URL: *

NAS IP: *

Gateway ID:

Redirection Mode: JS

SSID: [WiFi/WLAN Settings]

Advanced Settings

Parameter Settings: [Advanced Settings]

Save

WiFiDog Auth Server List

+ Add Authentication Server

Server IP	Redirection URL	NAS IP	Gateway ID	Redirection Mode	SSID	Action
<div style="border: 1px solid gray; padding: 5px;"> <p>Add Server</p> <p>Portal Server IP: <input type="text"/> *</p> <p>Redirection URL: <input type="text"/> *</p> <p>NAS IP: <input type="text"/> *</p> <p>Gateway ID: <input type="text"/></p> <p>Redirection Mode: JS</p> <p>SSID: <input type="text"/> [WiFi/WLAN Settings]</p> <p><input type="button" value="Cancel"/> <input type="button" value="OK"/></p> </div>						

Show No.: 10 Total Count: 0

K First < Pre Next > Last X 1 Go

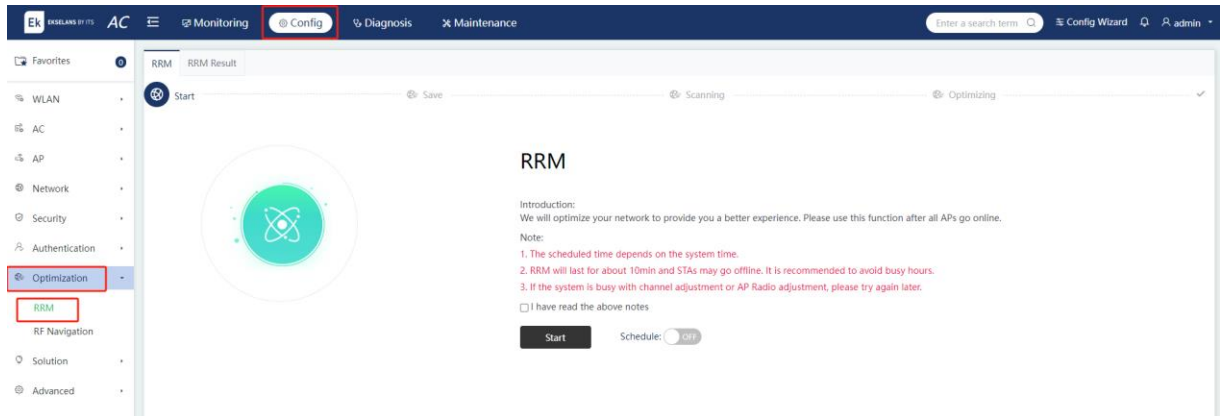
Parameter	Description
Portal Server IP	Indicates the IP address of a portal server.
Redirection URL	Indicates the portal server URL for authentication.
NAS IP	Specifies the IP address of a device to be managed by WiFiDog, which is used for communication from the server.
Redirection Mode	Specifies HTTP redirection or JavaScript redirection. JavaScript redirection is employed by default.
Gateway ID	Specifies the ID of a gateway used by WiFiDog, which is the gateway SN by default.
SSID	Specifies a Wi-Fi network to be configured with WiFiDog authentication.

- (2) Delete a WiFiDog authentication server: Click **Delete** behind a specified authentication server. The confirmation dialog box pops up. Click **OK** to finish the operation.
- (3) Edit a WiFiDog authentication server: Click **Edit**. Configure the information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The modified server is displayed in the server list.

5.7 Network Optimization

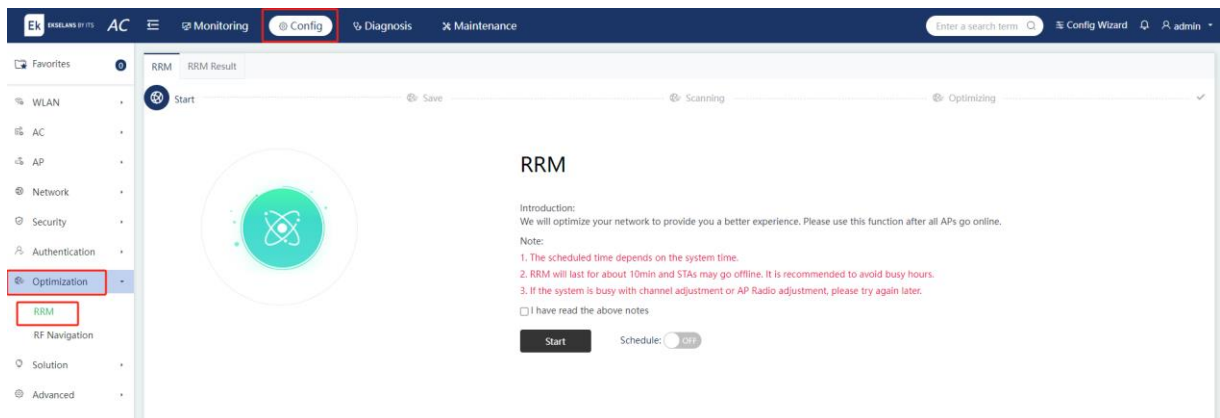
5.7.1 RRM

Choose **Config > Optimization > RRM**.

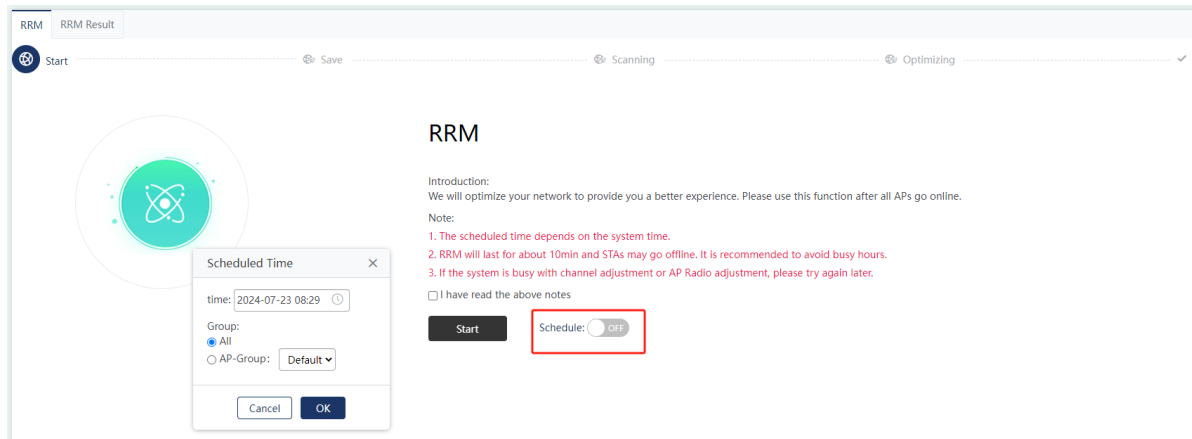


1. One-Click RRM

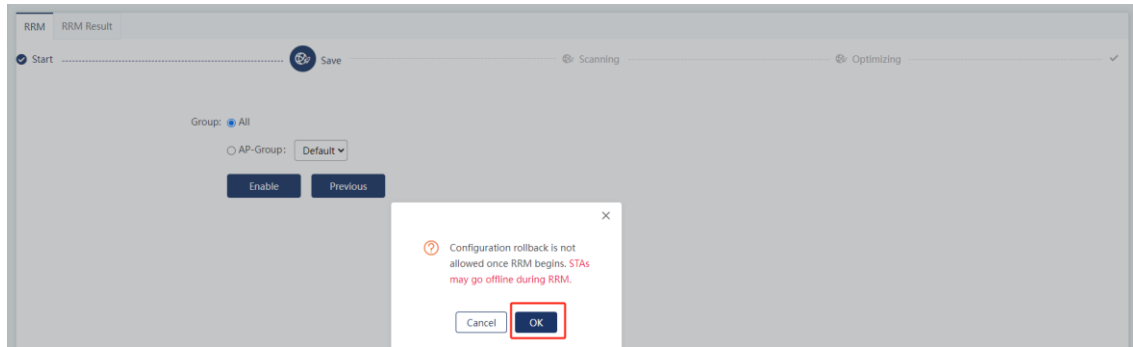
One-click RRM is used to optimize the network for maximum wireless performance. You are advised to use this feature after all APs in the area to be optimized go online. Before performing one-click RRM, read relevant precautions. Toggle on the **Schedule**: switch. The **Scheduled Time** dialog box will pop up. Choose a suitable time for network optimization as required.



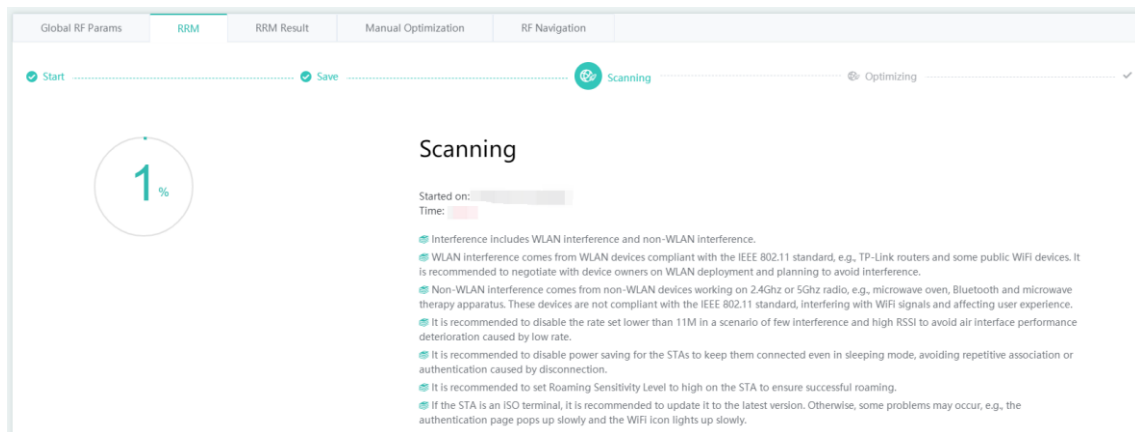
Read the notes and tick **I have read the above notes** to move to the automatic scanning and optimization stage. Please wait until the optimization result is generated.



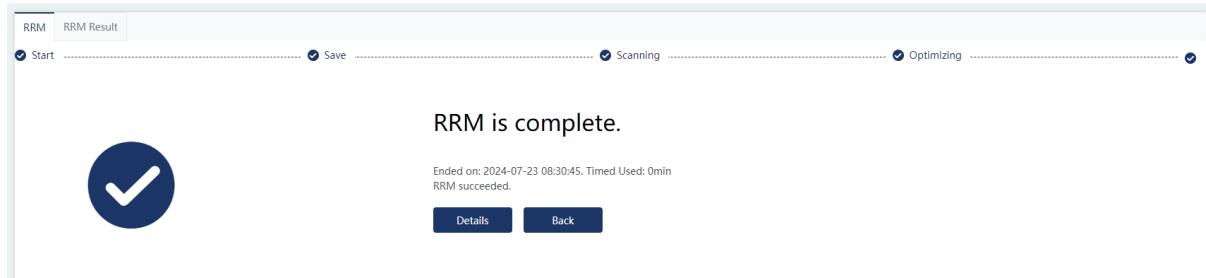
Select to optimize all APs or a specified AP group. Click **Enable**. Online APs that support network optimization will be scanned out. Once the RRM is started, the configuration cannot be rolled back. During the optimization, users may be disconnected.



The channel, channel width, and power will be optimized for supported APs.



After the RRM is complete, click **Back** to return to the **RRM** page. Click **Details** to be redirected to the **RRM Result** page and check the optimization.

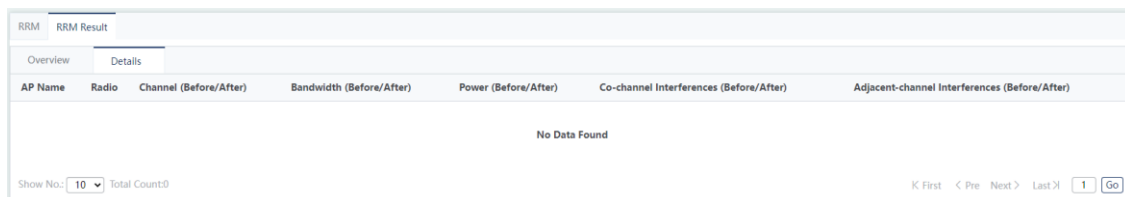


2. RRM Result

Overview: Display the number of signal interferences before and after the RRM in the form of a bar chart (the top 20 most significant changes).

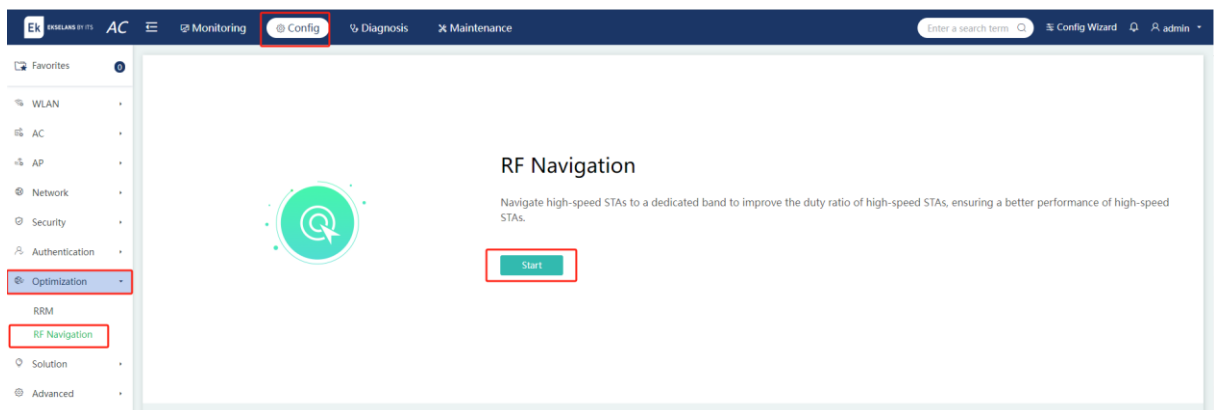


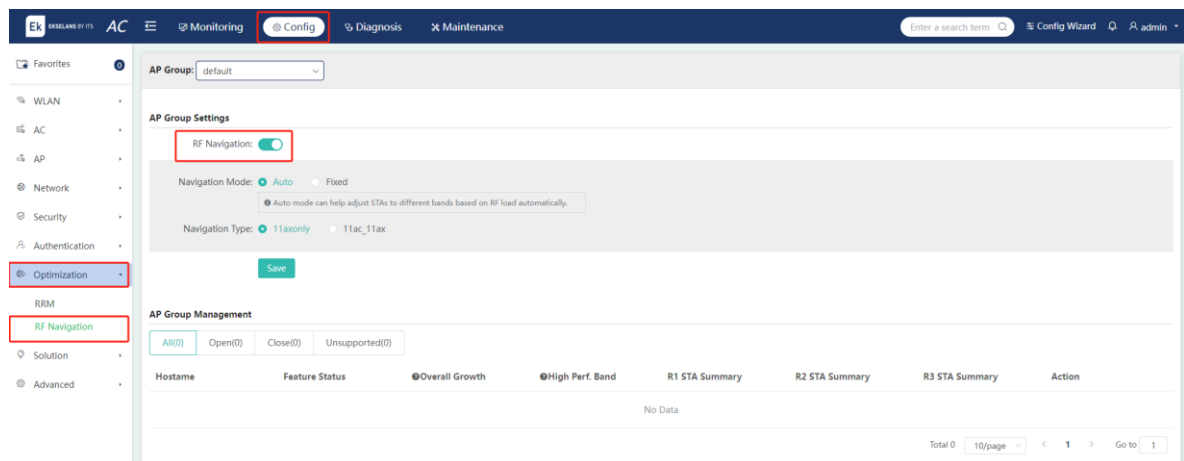
Details: Display all RRM results in a list format, with changes in data before and after the RRM highlighted in red font.



3. RF Navigation

When multiple types of clients coexist, high-performance clients are navigated to a dedicated high-efficiency frequency band. This prevents low-speed clients from occupying the air interface for a long time and improves the duty ratio of high-performance clients. RF navigation ensures that high-performance clients have a better experience in the Wi-Fi 6 frequency band.



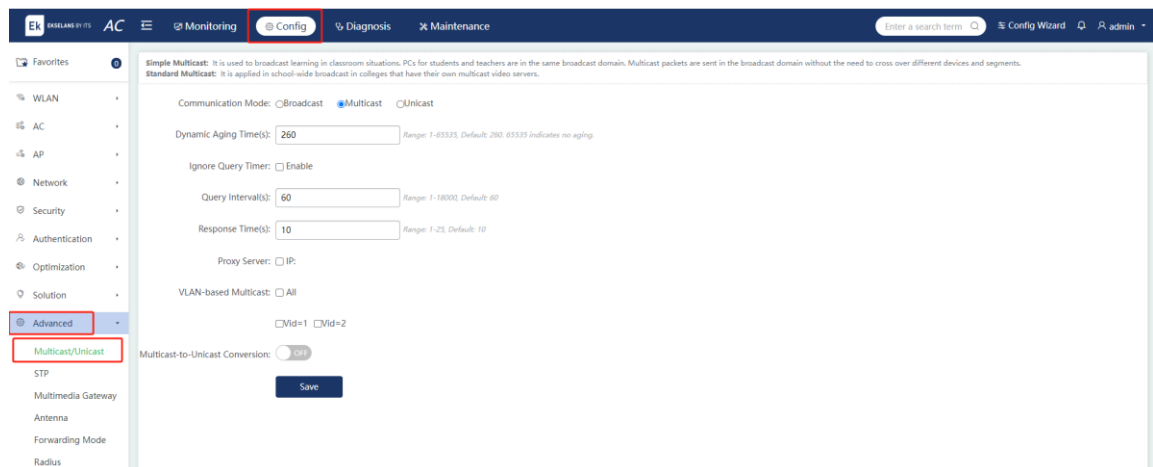


5.8 Advanced

5.8.1 Multicast/Unicast

Choose **Config > Advanced > Multicast/Unicast**.

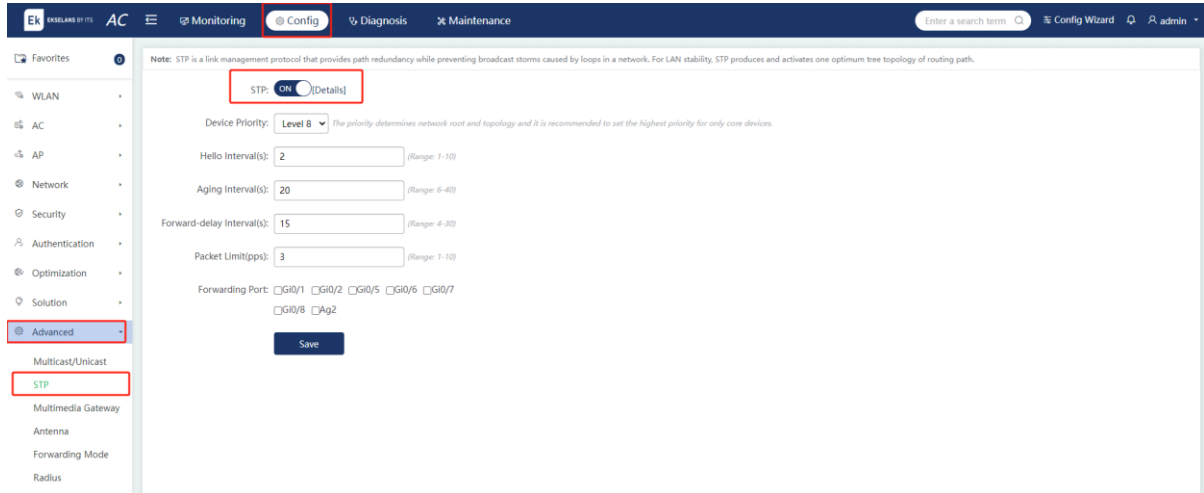
This feature is used to configure the communication mode of a device as broadcast, multicast, or unicast.



5.8.2 STP

Choose **Config > Advanced > STP**.

Spanning Tree Protocol (STP) is a protocol used to avoid broadcast storms caused by link loops and provide link redundancy backup; its function is to discover and activate an optimal tree topology of the local area network (LAN) to ensure the stability of the network.



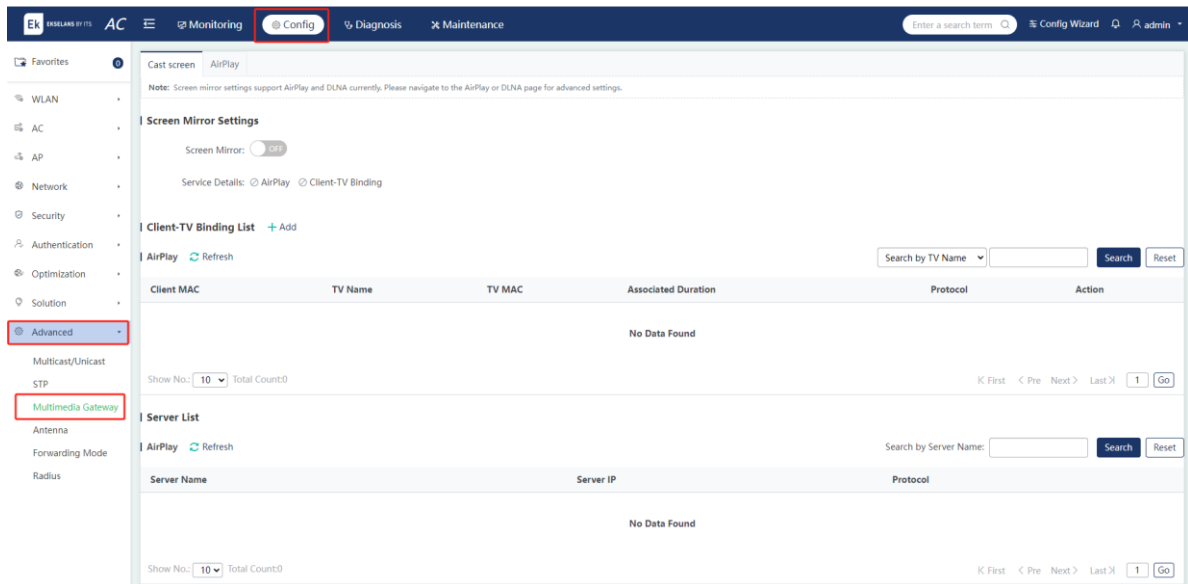
5.8.3 Multimedia Gateway

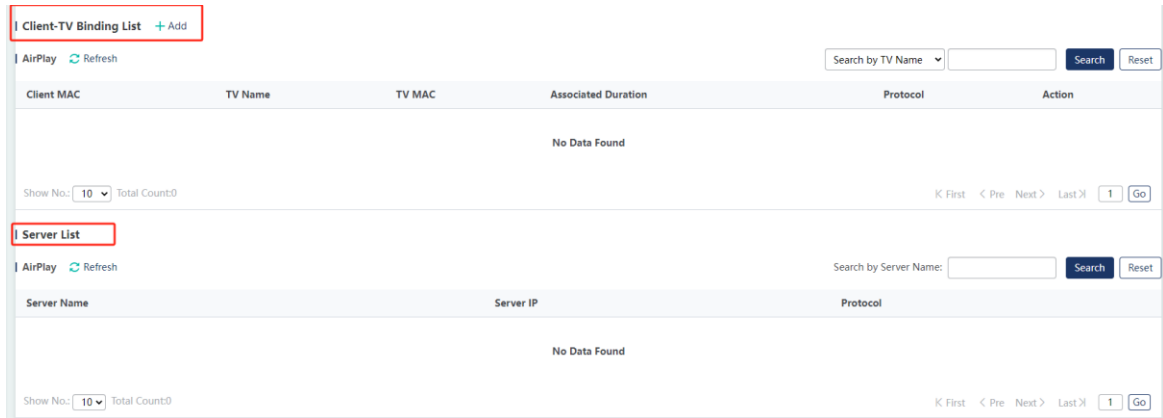
Choose **Config > Advanced > Multimedia Gateway**.

Multimedia gateway is mainly used by iOS and Android clients for screen mirroring to device servers that support AirPlay and DLNA protocols, such as TV boxes.

1. Cast Screen

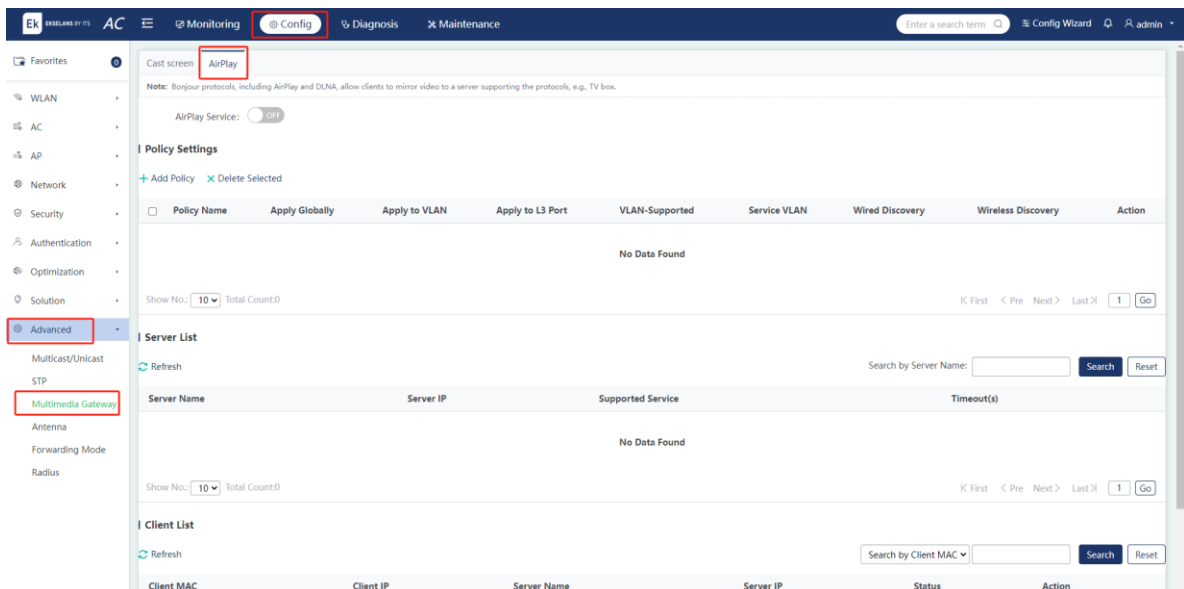
Accurate screen mirroring solutions can be configured conveniently. Currently, AirPlay and DLNA protocols are supported. If you need more advanced and professional configuration, go to the corresponding page to configure protocols and standards.



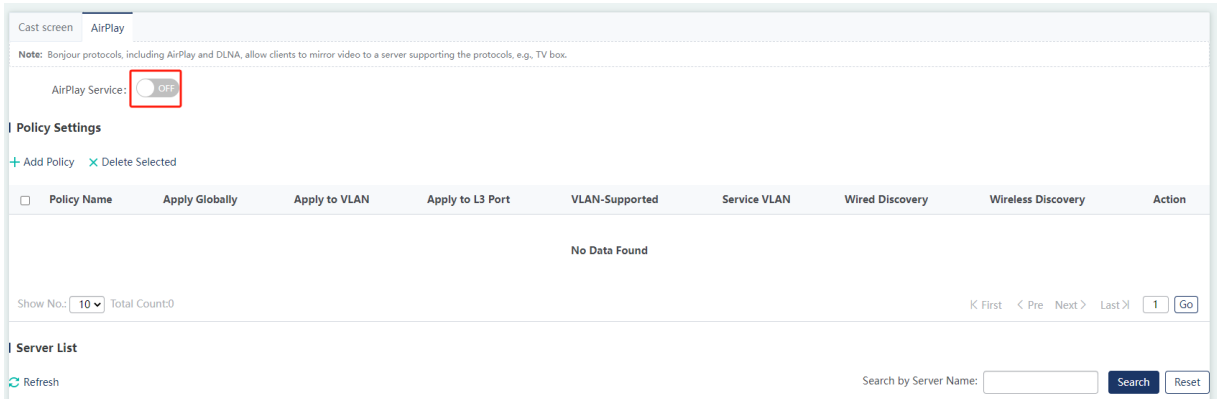


2. Airplay

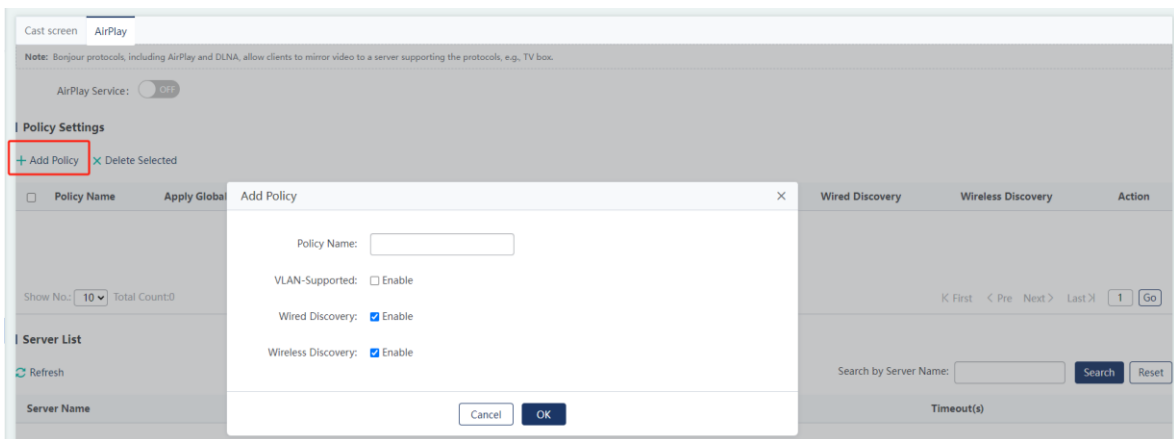
Multimedia gateway protocols mainly include AirPlay and DLNA, which are used for screen mirroring from mobile clients to device servers that support the protocols, such as TV boxes.



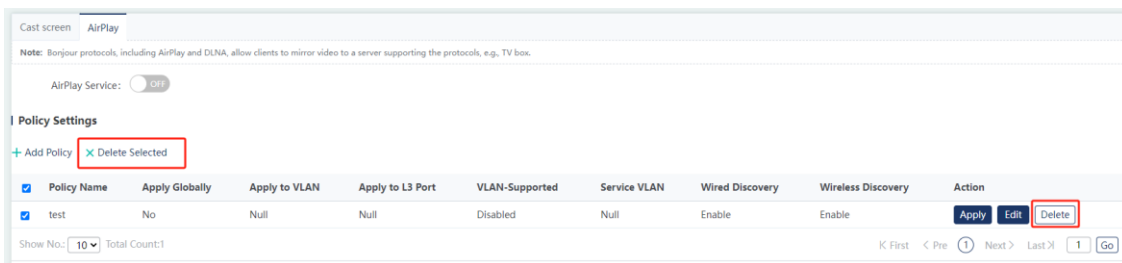
- (1) Enable **AirPlay Service**: Enable the AirPlay or DLNA protocol for the multimedia gateway as required. When the protocol is disabled, the corresponding policy will not take effect. The policy corresponding to the enabled protocol is displayed.



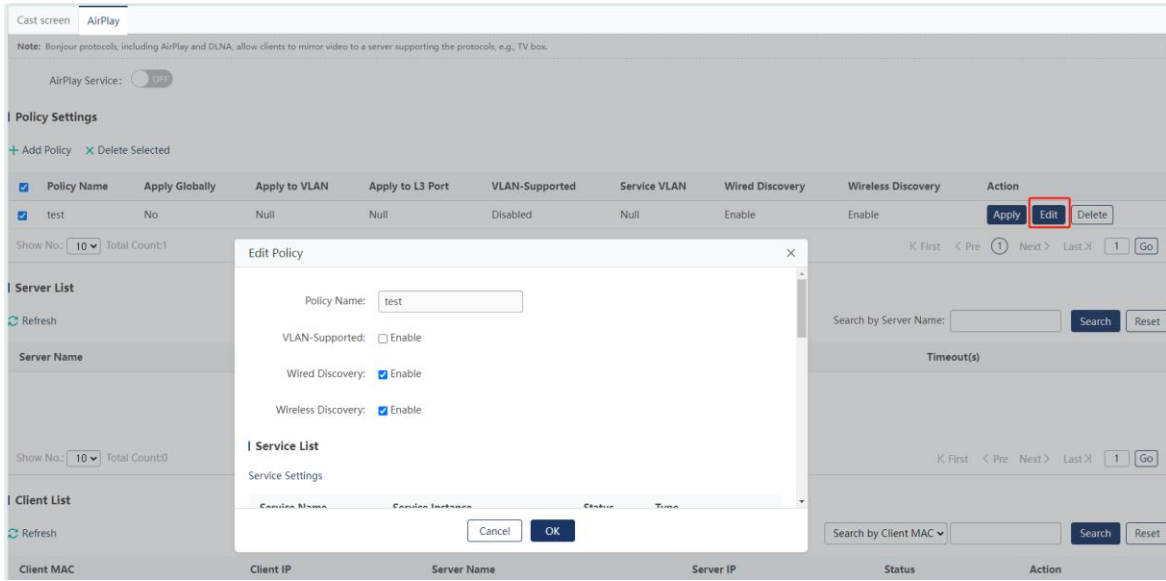
(2) Add a policy: Choose **Policy Settings** > **Add Policy**. Configure the information in the pop-up dialog box. Click **OK**. A message indicating the configuration has been saved is displayed. The newly added policy is displayed in the policy list.



(3) Delete a policy: Click **Delete** of a specified policy in the list. The confirmation dialog box pops up. Click **OK** to finish the operation. To delete multiple policies, select policies to be deleted from the list. Click **Delete Selected**. The confirmation dialog box pops up. Click **OK** to finish the operation.



(4) Edit a policy: Click **Edit** of a specified policy in the list. The pop-up dialog box displays the information about the policy. Edit the information. Click **OK**. A message indicating the configuration has been saved is displayed.

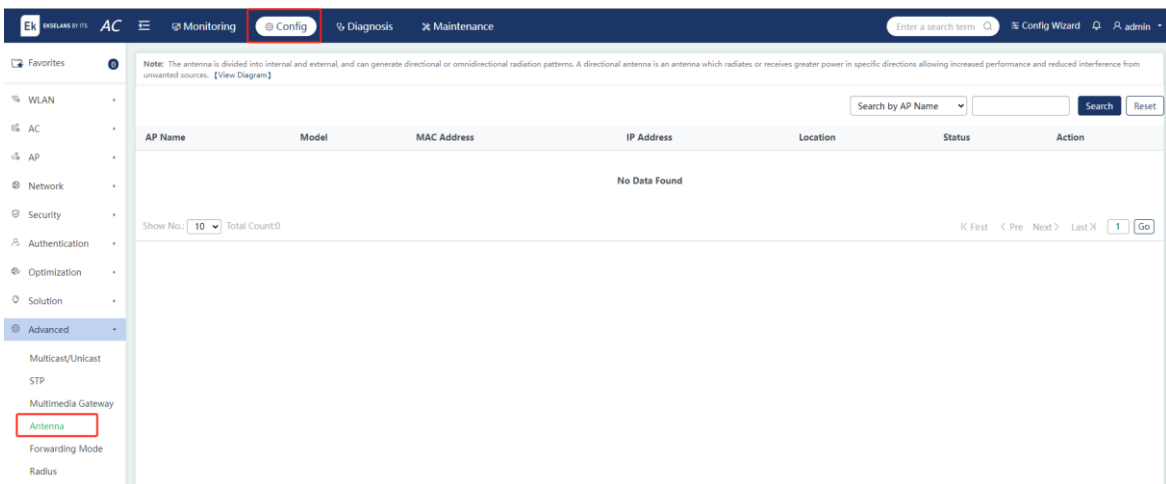


5.8.4 Antenna

Choose **Config > Advanced > Antenna**.

RF antennas are classified into two types: built-in antennas and external antennas. Antenna orientations include two types: directional and omnidirectional. Directional antennas radiate the signal within a certain angle range. The radiation range is like a cone.

Click **Edit** in the AP list to access the antenna setting page. The antenna types include built-in antennas and external antennas. The antenna orientation is divided into omnidirectional and directional. Whether the RF port supports type/orientation switching depends on its own capabilities. If the RF port does not support type/orientation switching, the web system will prompt the message **This radio does not support switch the style.** or **This radio does not support switch the direction.** to the user.



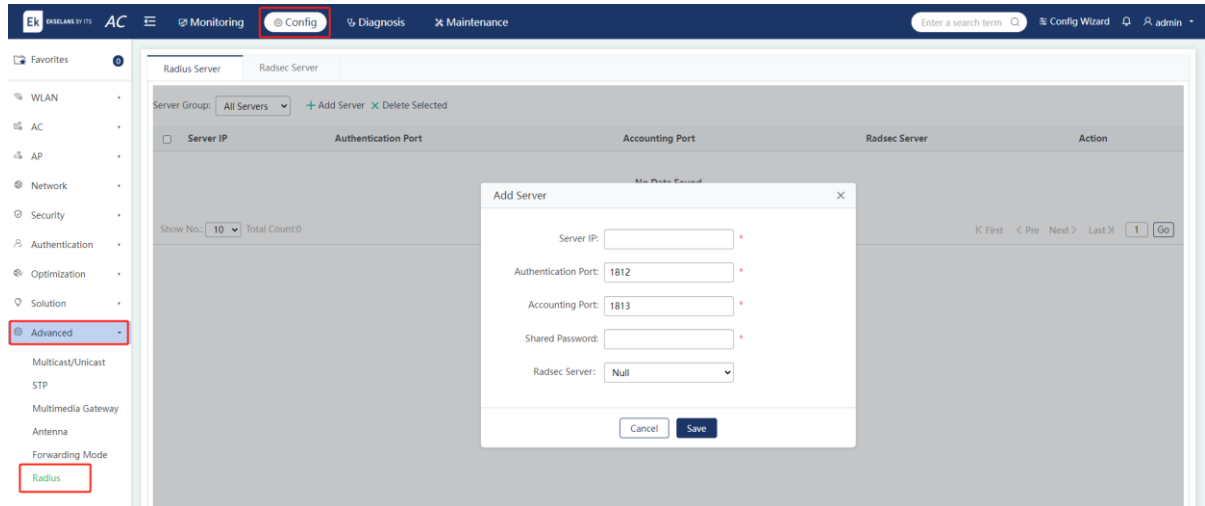
5.8.5 RADIUS

Choose **Config > Advanced > Radius**.

1. RADIUS Server

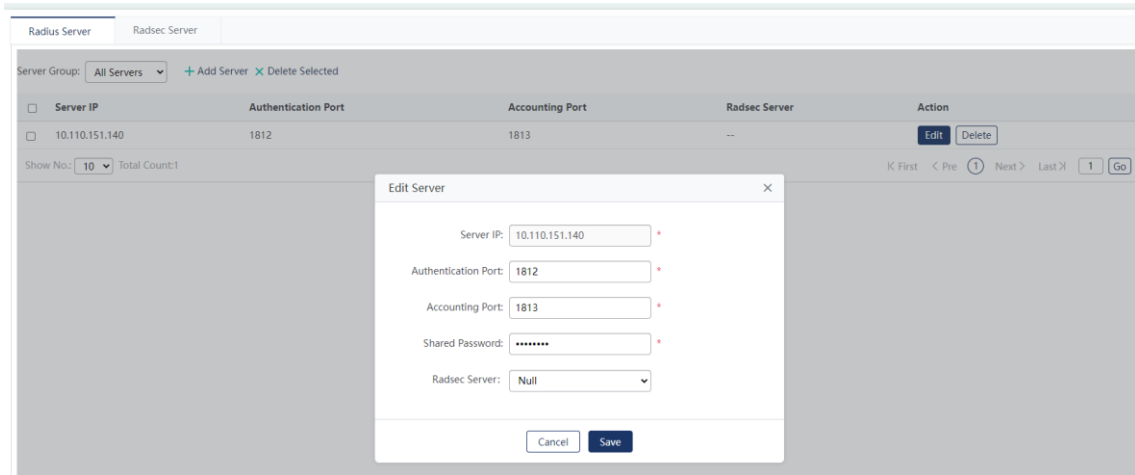
The RADIUS server conducts identity authentication and accounting on access users to protect network security and facilitate management for network administrators.

- (1) Add a server: Click **Add Server**. Set fields and click **Save**. A message indicating the configuration has been saved is displayed.

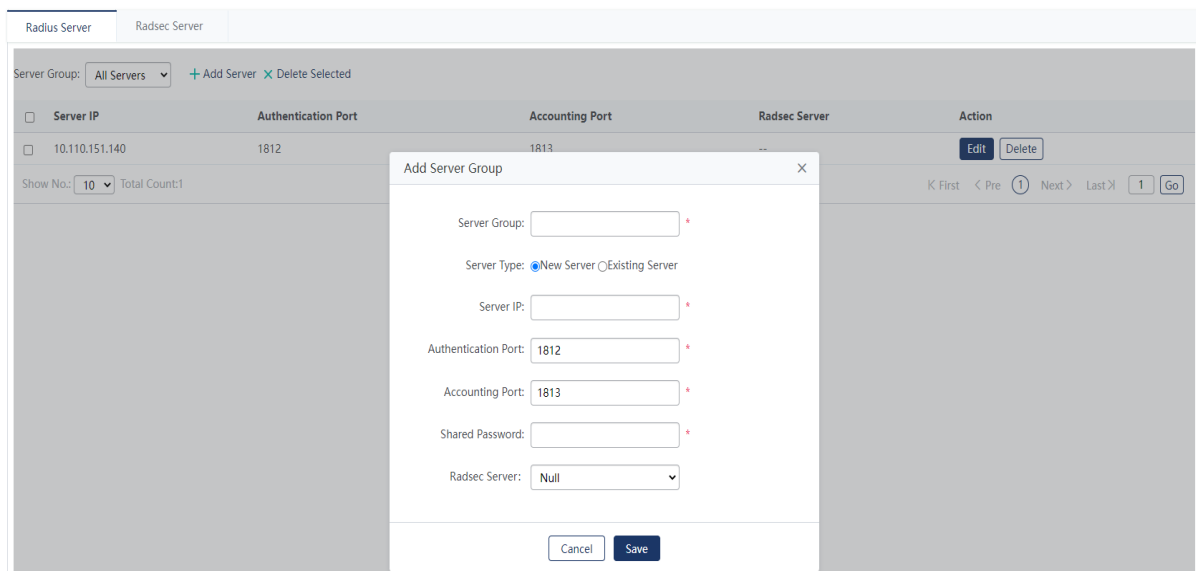


Parameter	Description
Server IP	Indicates the IP address of a RADIUS server.
Authentication Port	Indicates the UDP port ID for RADIUS authentication. The value range is from 0 to 65,535. 0 indicates that the server does not perform identity authentication.
Accounting Port	Indicates the UDP port ID for RADIUS accounting. The value range is from 0 to 65,535. 0 indicates that the server does not perform accounting.
Shared Password	Indicates the shared key for the communication between the network access server (router) and the RADIUS server.
Radsec Server	(Optional) Indicates the ID of the RadSec server, to which traffic is redirected from the RADIUS server.

- (2) Edit a server: Click **Edit** for an existing server. Edit the parameter values. Click **Save**.



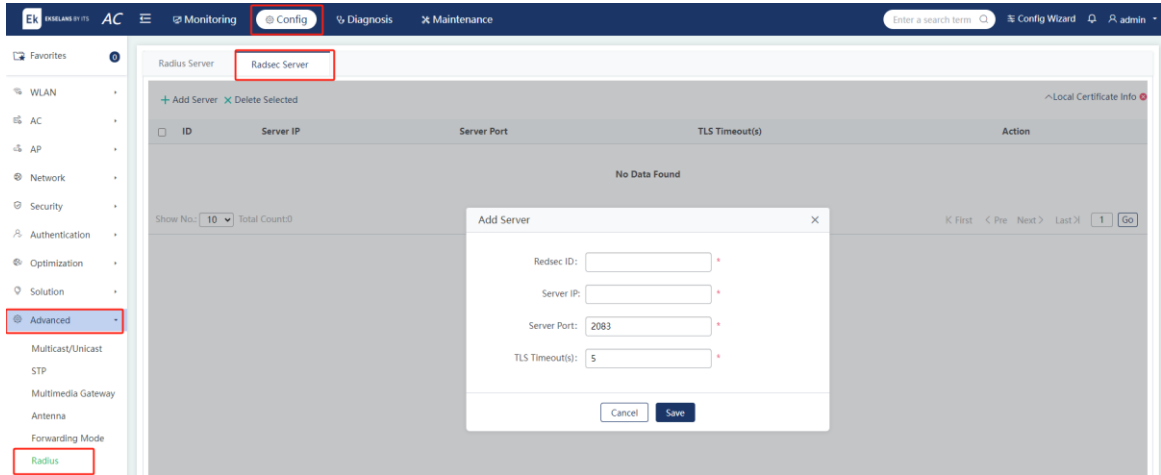
- (3) Add a server group: Click the **Server Group** drop-down list and select **Add Server Group**. The **Add Server Group** dialog box pops up. If you select **New Server**, one server group and one server will be added and the server belongs to the server group. If you select **Existing Server**, an existing server will be added to the server group.



2. RadSec Server

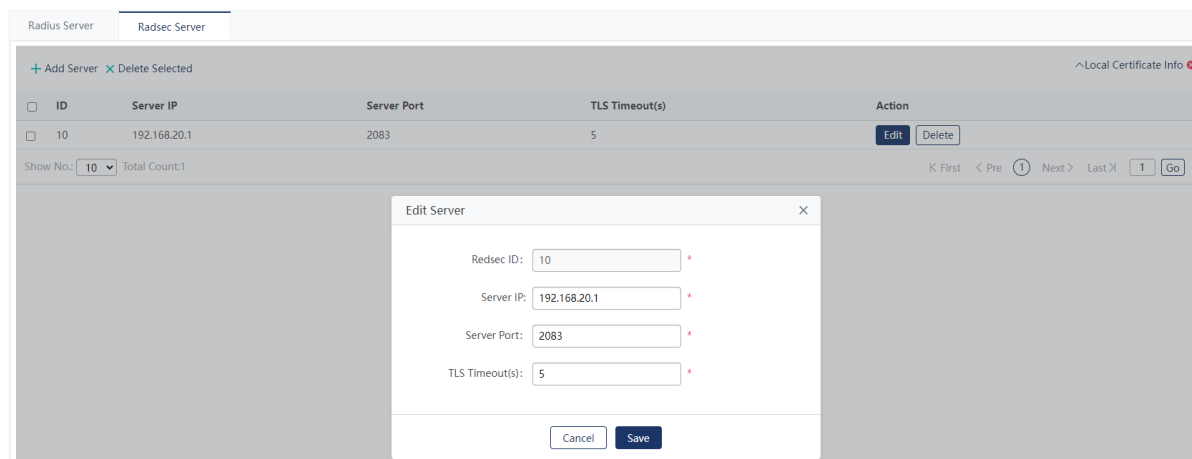
RadSec provides secure communication for RADIUS requests by using the Transport Layer Security (TLS) protocol and allows RADIUS authentication, authorization, and accounting data to be securely transmitted over untrusted networks.

- (1) Add a server: Click **Add Server**. Set fields and click **Save**. A message indicating the configuration has been saved is displayed.

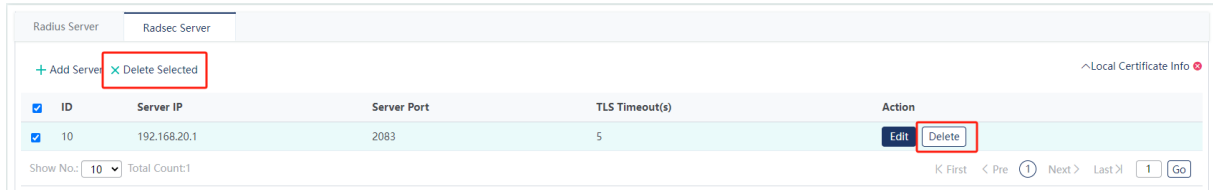


Parameter	Description
Radsec ID	Indicates the unique ID of a RadSec server. The value is an integer in the range from 1 to 255.
Server IP	Indicates the IP address of the RadSec server.
Server Port	Specifies the port ID of the RadSec server. The value range is from 1 to 65,535. The default value is 2,083 .
TLS Timeout(s)	Specifies the TLS connection timeout. The value range is from 1 to 1,000. The default value is 5 .

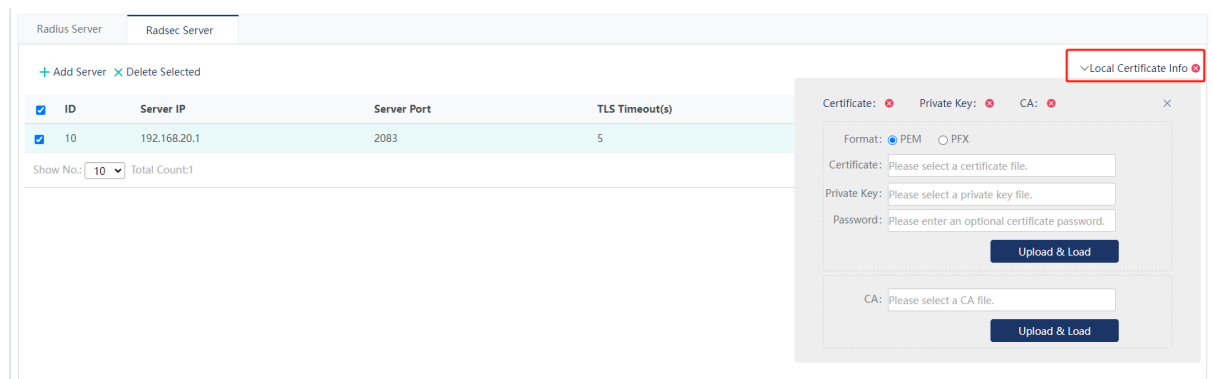
(2) Edit a server: Click **Edit** behind a specified server. Modify the parameter values and click **Save**.



(3) Delete a server: Click **Delete** behind a specified server. If you need to delete multiple servers, select the servers to be deleted and click **Deleted Selected** to batch delete them.



(4) Local certificate management: Click **Local Certificate Info**. The local certificate management dialog box pops up. The icon on the right of **Local Certificate Info** shows the certificate loading status. Select a certificate file and private key file. Enter the certificate password (if any). Click **Upload & Load**. A message is displayed, indicating that the certificate is loaded successfully. The PEM and PFX formats are supported. If the certificate file does not contain CA information, select a CA file and click **Upload & Load**.



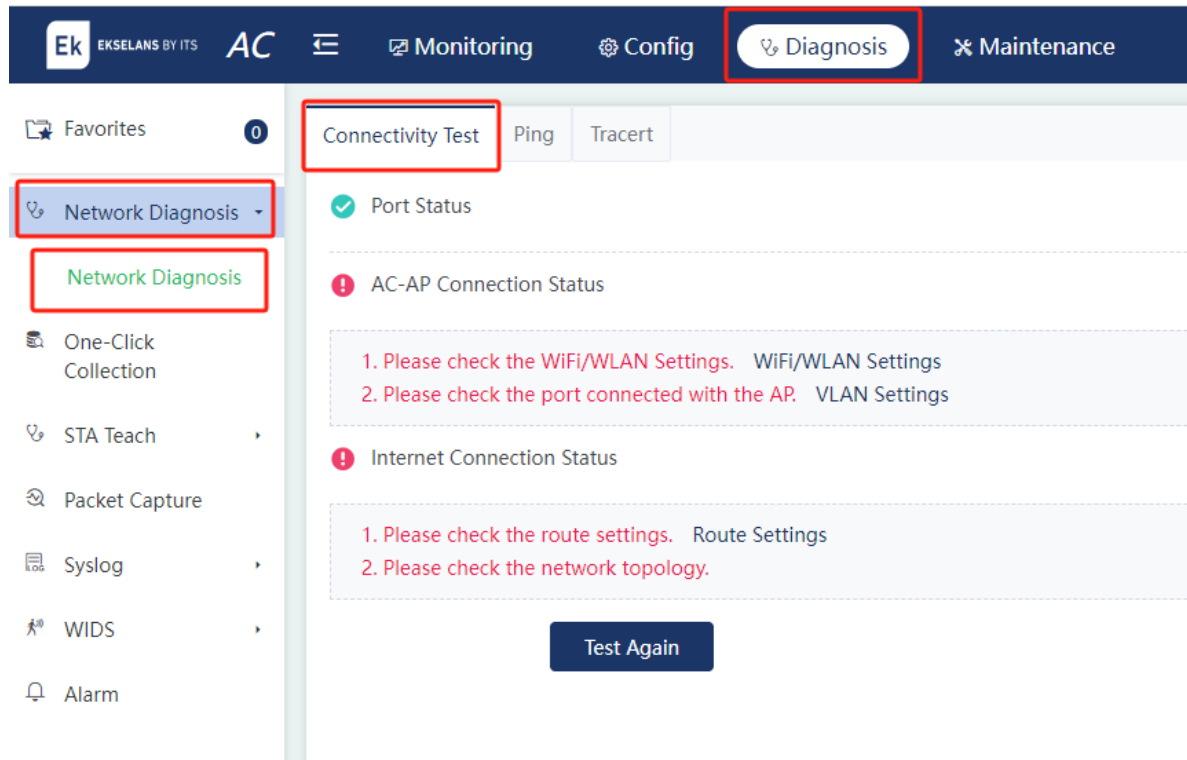
6 Diagnosis

6.1 Network Diagnosis

6.1.1 Network Diagnosis

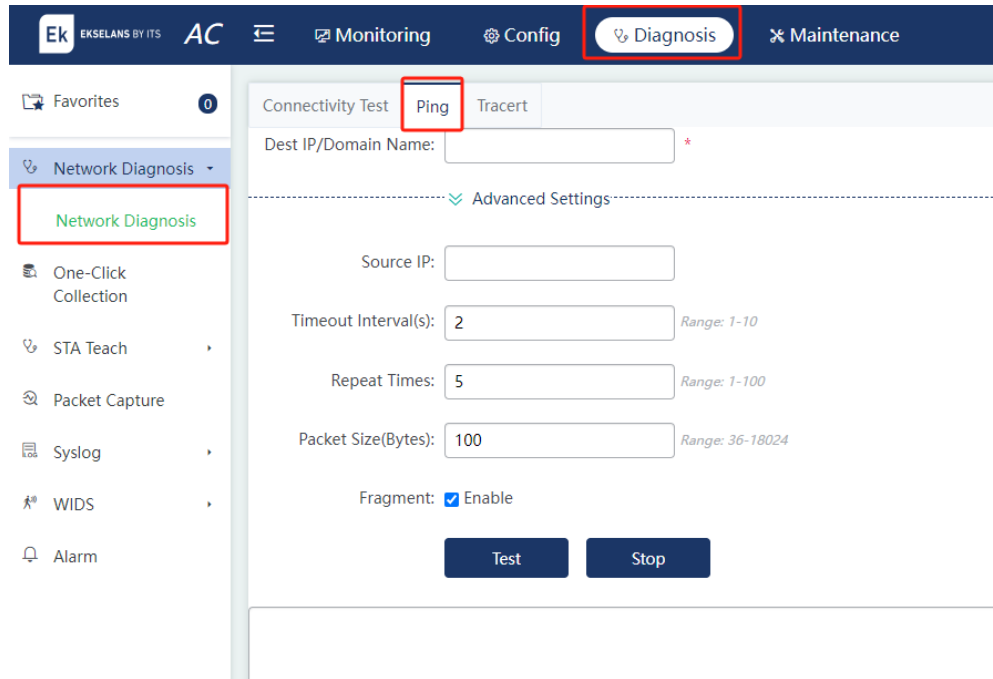
Choose **Diagnosis > Network Diagnosis > Network Diagnosis**.

1. Connectivity Test



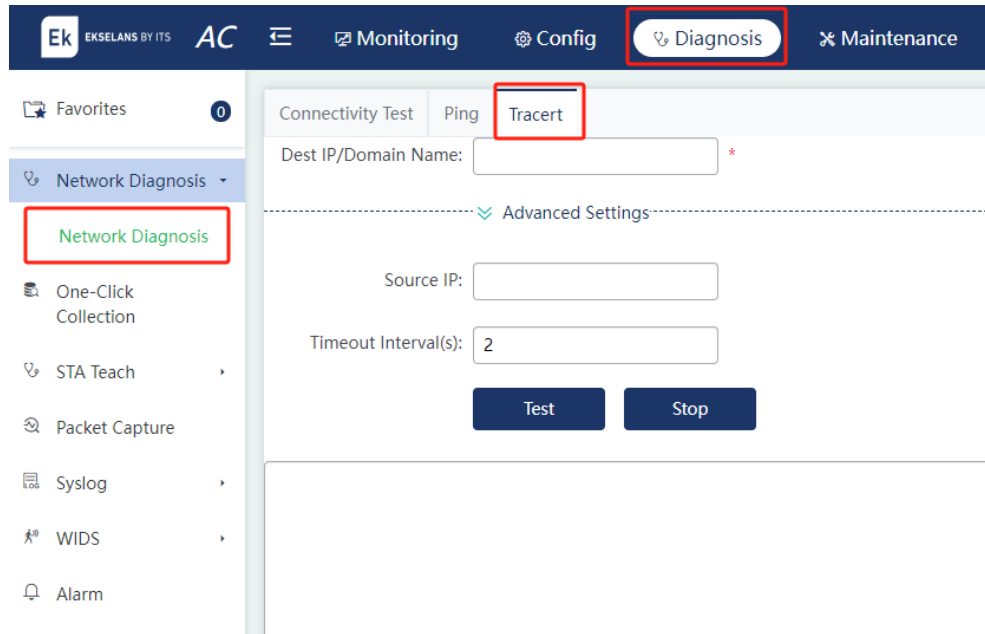
Detection Item	Description
Port Status	Checks whether any interface on the AC is in Up status.
AC-AP Connection Status	Checks whether any AP connected to the AC goes online.
Internet Connection Status	Checks the connectivity between the AC and external networks. Ping the IP address of 8.8.8.8.

2. Ping



Parameter	Description
Dest IP/Domain Name	Indicates the address or domain name to be pinged.
Source IP	Indicates the source address of ping packets, namely, the local interface address of a device.
Timeout Interval(s)	Indicates the timeout duration.
Repeat Times	Indicates the number of data packets to be transmitted.
Packet Size(Bytes)	Indicates the length of the data padding section in a data packet to be transmitted.
Fragment	Indicates the DF flag bit of an IP address. When the DF flag bit is set to 1, data packets are not fragmented. The default DF flag bit is 0.

3. Tracert

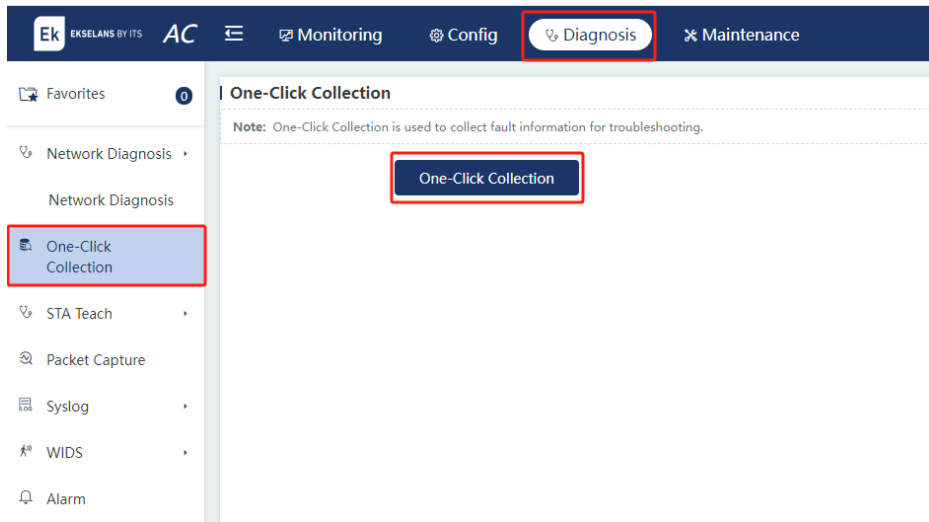


Parameter	Description
Dest IP/Domain Name	Indicates the tracert destination or domain name address.
Source IP	Indicates the tracert source address, namely, the local interface address of a device.
Timeout Interval(s)	Indicates the timeout duration.

6.2 One-Click Collection

Choose **Diagnosis > One-Click Collection**.

You can use the one-click collection feature to collect device fault information for troubleshooting.



6.3 Client Diagnosis

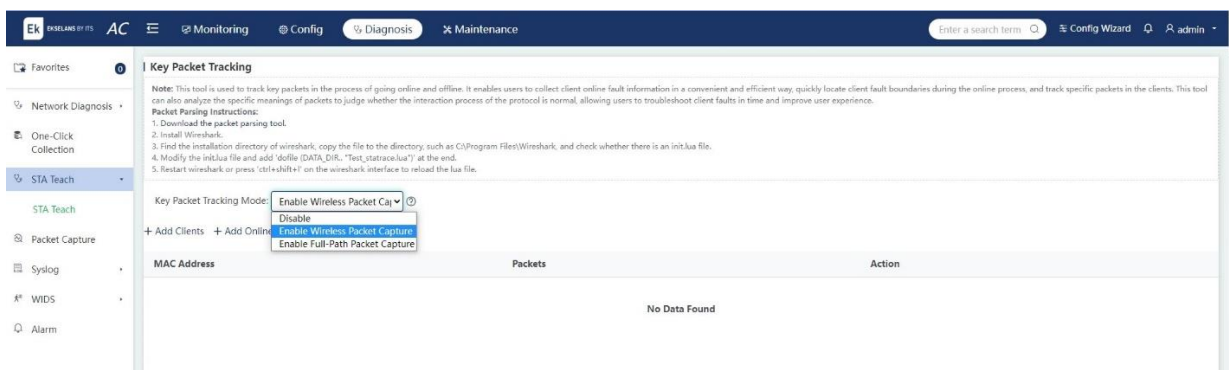
6.3.1 Key Packet Tracking

Choose **Diagnosis > STA Teach > STA Teach**.

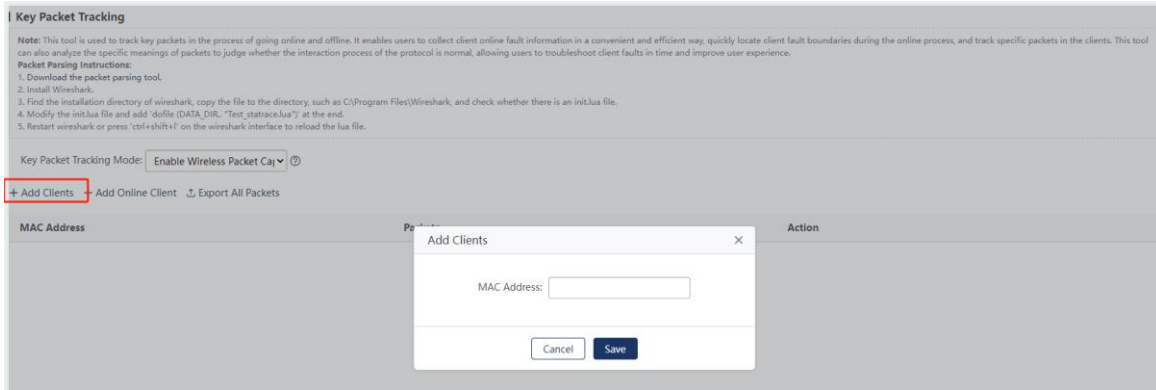
This feature enables users to easily and quickly collect fault information, locate fault scope during the go-online process of clients, and track key packets of the clients. Key packet tracking identifies key packets and analyzes the key fields and meanings of the packets to determine whether the interaction process of the protocol is normal. It enables users to collect fault information conveniently and quickly and troubleshoot client faults in time, thus improving user experience.

Enable Wireless Packet Obtain: obtains packets on the wireless driver side.

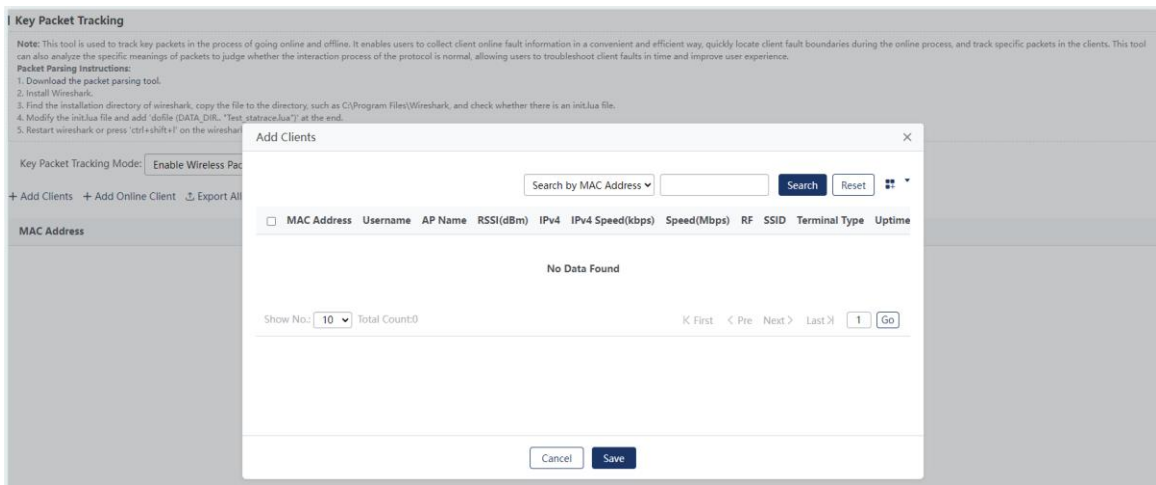
Enable Full-Path Packet Obtain: obtains packets on the entire path that the packets pass through.



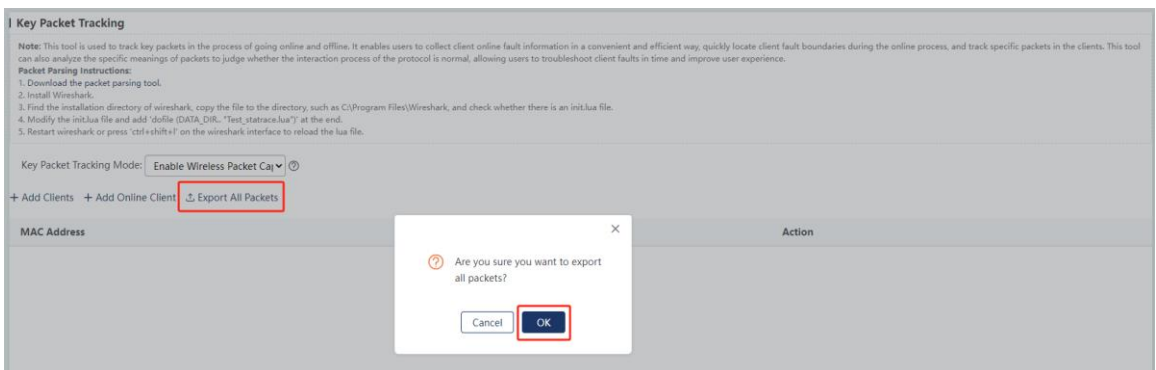
- (1) Add a client manually: Click **Add Clients**. Enter the MAC address of a client. Click **Save**. The system verifies the validity of the MAC address. If the MAC address is valid, the client will be added.



(2) Select and add an online client: Click **Add Online Client**. Select an online client for packet tracking.



(3) Export packets: Click **Export Packet** behind a specified client. If all client packets need to be exported, click **Export All Packets** to compress all the received packets into a **.tar** file and export the file to users.

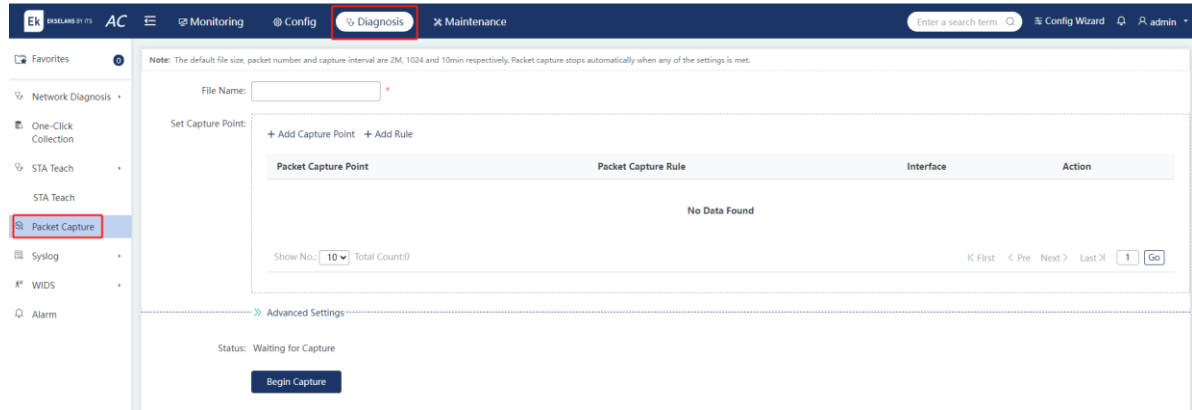


(4) Cancel packet tracking: Click **Cancel Detection** behind a specified client.

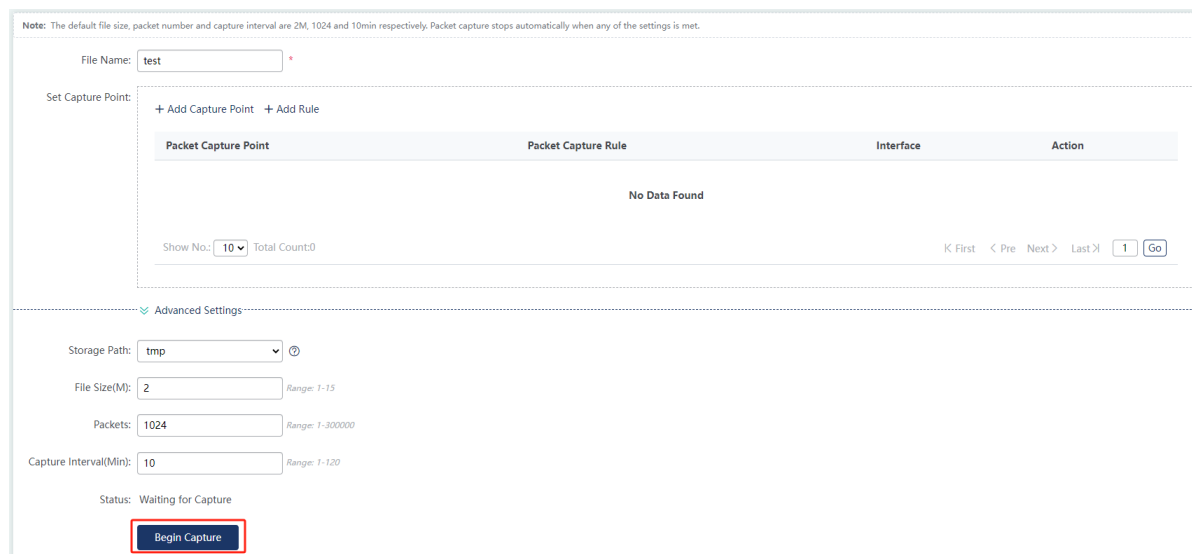
6.4 Packet Obtaining

Choose **Diagnosis > Packet Capture**.

This feature is generally used to obtain packets to collect diagnostic data when problems occur with after-sales devices.



(1) Start packet obtaining: Edit the fields on the configuration page. Click **Begin Obtain**.

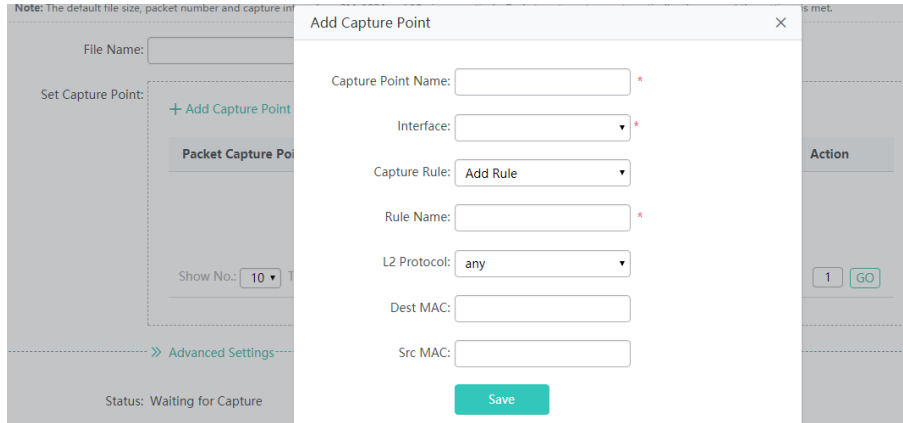


Parameter	Description
File Name	Specifies the name of the file to be saved.
Set Obtain Point	Specifies the packet obtaining location.
Storage Path	Specifies the storage path of the obtained packet file.
File Size(M)	Specifies the buffer size.
Packets	Specifies the number of packets to be obtained.
Obtain Interval (Min)	Specifies the timeout duration. The packet obtaining is automatically stopped when the timeout duration expires.

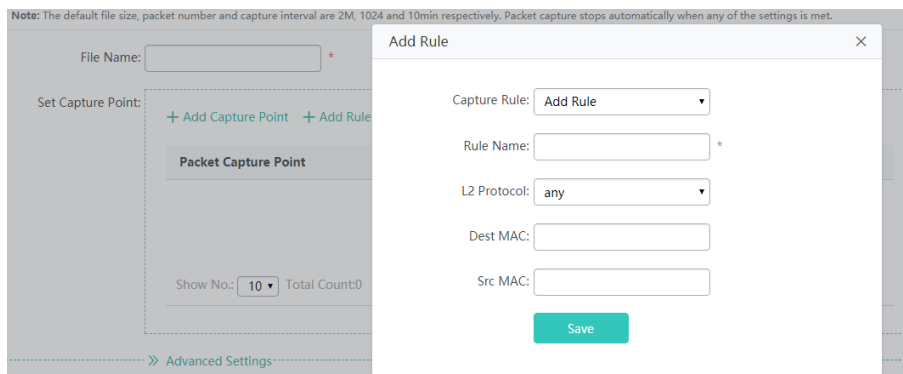
(2) Stop packet obtaining: During packet obtaining, click **End Capture** to stop packet obtaining.

(3) Download the file: Click **Download File** to download the obtained file to the computer.

- (4) Clear the file: Click **Clear File** to remove the obtained file from the device.
- (5) Add a capture point: Click **Add Capture Point**. The configuration dialog box pops up. Configure the parameters and click **Save**. A message indicating the point has been successfully added is displayed.



- (6) Delete a capture point: Click **Delete** behind a specified capture point.
- (7) Set rules for packet obtaining: Click **Add Rule**. The configuration dialog box pops up. Configure the parameters and click **Save**. A message indicating the rule has been successfully added is displayed.

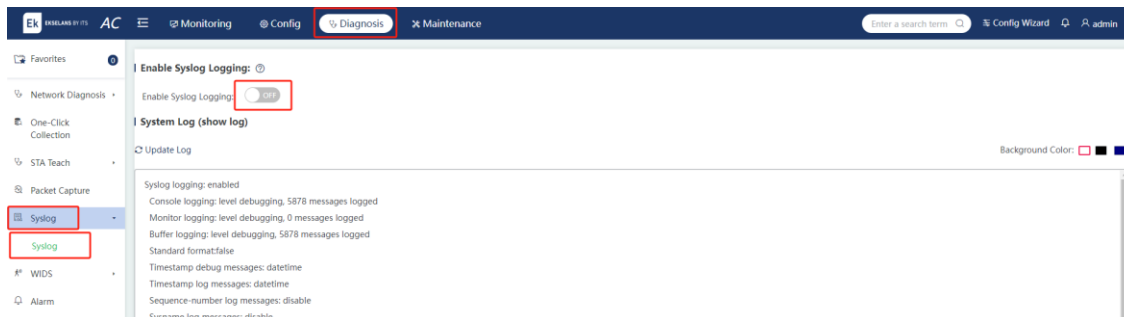


6.5 Log

6.5.1 Syslog

Choose **Diagnosis > Syslog > Syslog**.

You can configure the syslog feature to help after-sales and R&D personnel locate problems. Click **Export Syslog** to download the syslog to the computer.



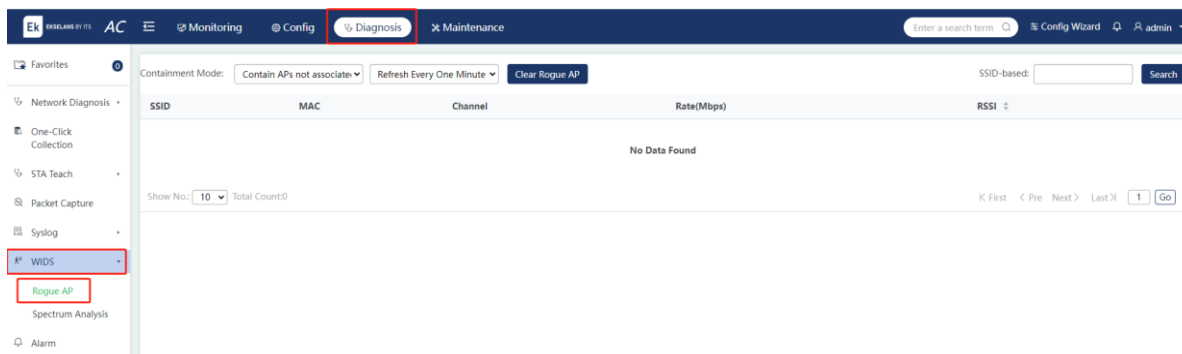
6.6 Air Interface Detection

6.6.1 Rogue AP

Choose **Diagnosis > WIDS > Rogue AP**.

Rogue APs may exist on a wireless network. They may have security vulnerabilities or may be controlled by attackers, seriously threatening the security of user networks.

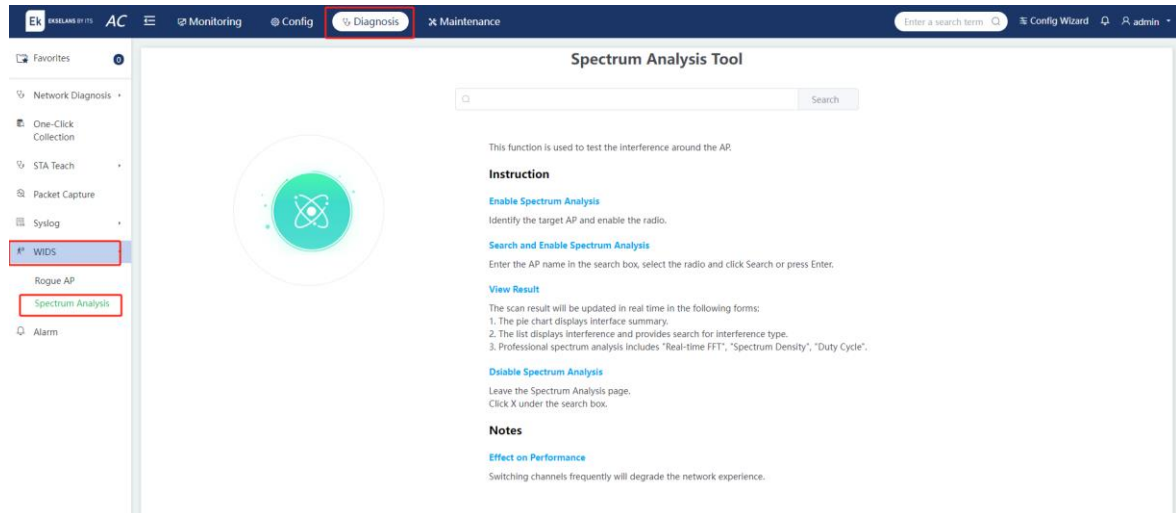
The following page displays possible rogue APs that are identified after the containment feature is enabled.



6.6.2 Spectrum Analysis

Choose **Diagnosis > WIDS > Spectrum Analysis**.

When the network quality is poor, the system can detect network interference and determine whether interference exists on the network based on **Real-time FFT**, **Spectrum Density**, and other spectrum diagrams. The interference information is recorded.



Note

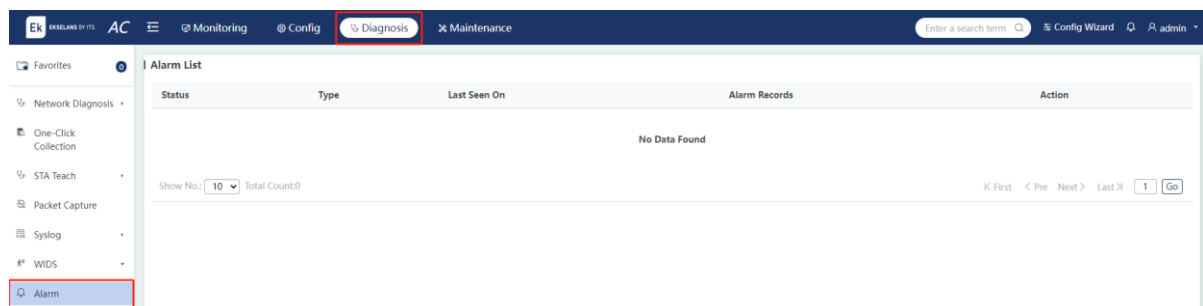
To perform spectrum analysis, the AP must go online.

When you switch to view the spectrum analysis result of another AP, the real-time spectrum analysis feature is automatically disabled and needs to be manually enabled.

6.7 Alarm

Choose **Diagnosis > Alarm**.

When alarm records exist on the system, the alarm clock icon in the upper right corner of the page will be marked with a red number indicating the number of alarm types. Click the alarm clock icon to jump to the **Alarm List** page and check detailed alarm information.



The list displays an overview of various alarms, mainly including AP offline alarms, AP access failure alarms, alarms about the number of AP/RF user access exceeding the threshold (90%), and AP power saving alarms. The number of alarms of each type and the latest occurrence time of each alarm type are also displayed. For example, if two APs go offline, the displayed number of this type of alarm is 2.



Click **Unread**. A confirmation dialog box is displayed, requesting you to confirm whether to mark the record as a read one. If you confirm the operation, the number of alarms displayed in the upper right corner decreases by 1. Click **Details** to display the alarm details. Click **Delete** to delete this type of alarm.

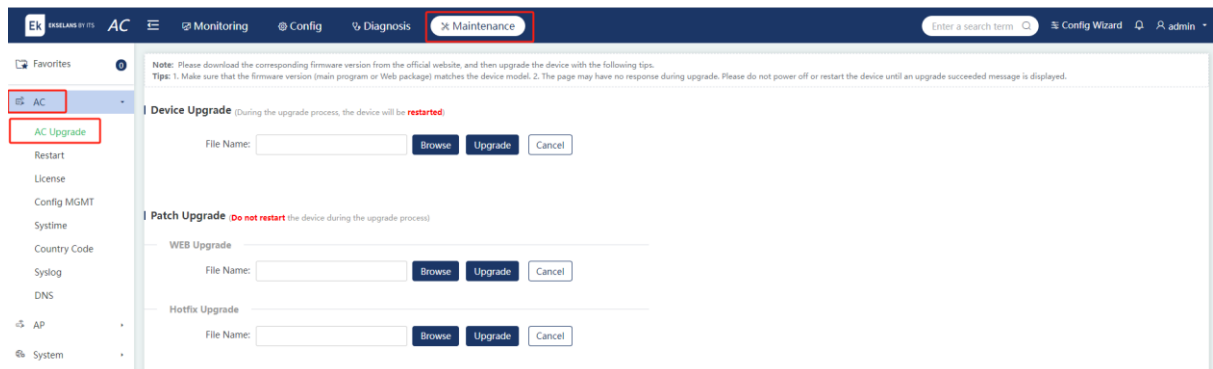
7 Maintenance

7.1 AC Management

7.1.1 AC Upgrade

Choose **Maintenance > AC > AC Upgrade**.

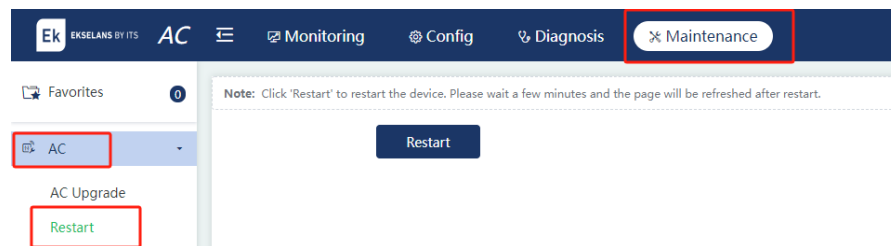
Or choose **System Upgrade > AC Upgrade** in the navigation bar to access the **AC Upgrade** page quickly.



7.1.2 AC Restart

Choose **Maintenance > AC > Restart**.

Click **Restart** to restart the current AC.

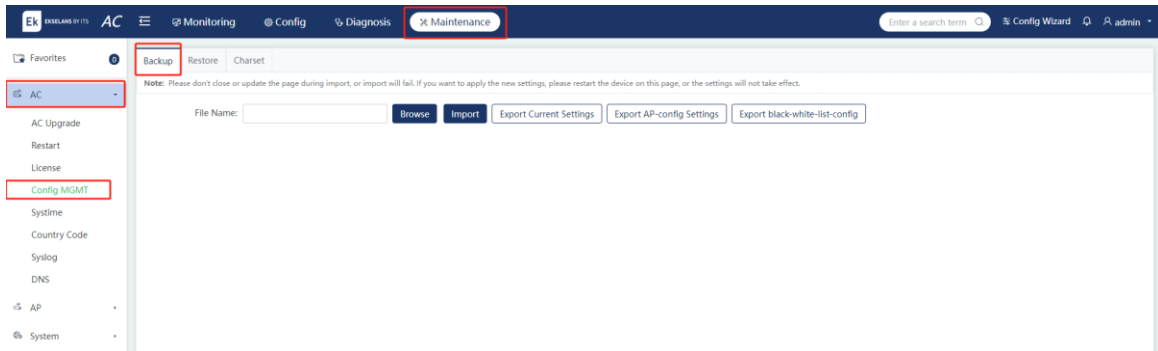


7.1.3 Configuration Management

Choose **Maintenance > AC > Config MGMT**.

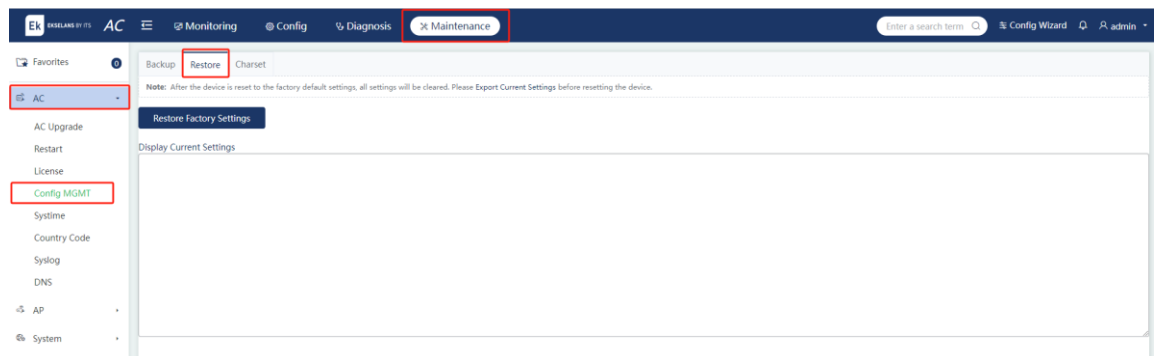
1. Backup

You can back up the configuration file on the device and import or export configurations to perform batch operations on the configurations, thereby facilitating user operations.



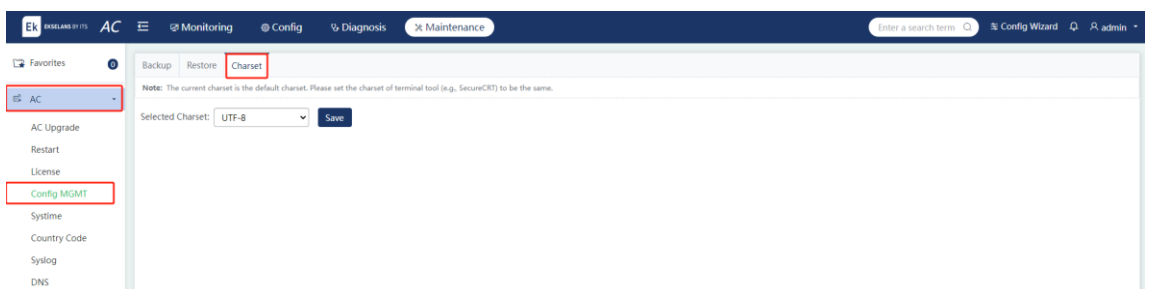
2. Restore

You can clear the configurations to restore the system to the initial state. You need to use the IP address in the factory settings to access the web system. Restoring factory settings will delete all configurations. Therefore, exercise caution when performing this operation.



3. Charset

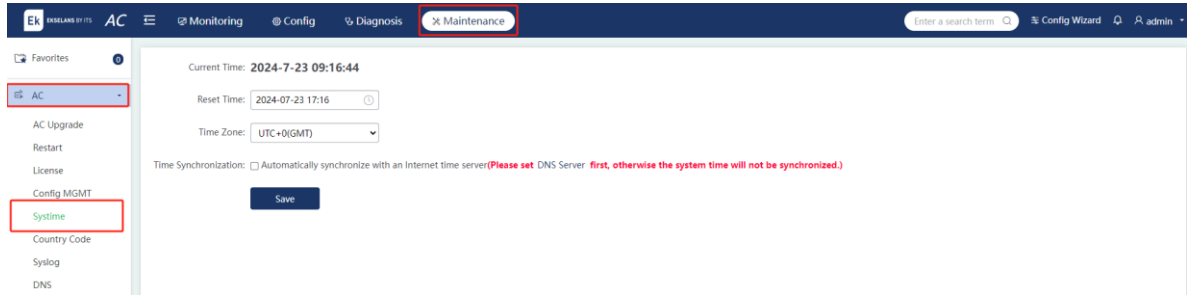
The system charset can be set to GBK or UTF-8. The UTF-8 is used for the web system by default. You are advised to keep the system charset on the SecureCRT or other client tools consistent with the charset on the system. Otherwise, garbled and hybrid characters may occur.



7.1.4 System Time

Choose **Maintenance > AC > System**.

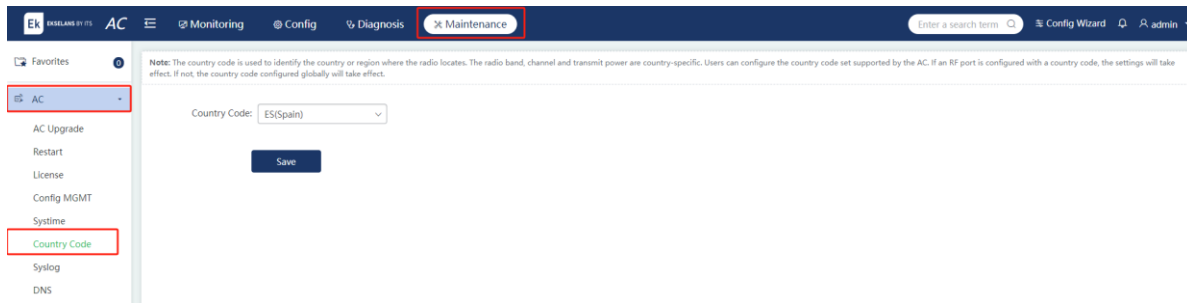
You can set the system time of the time zone where the device is located so that the device information is accurate.



7.1.5 Country Code

Choose **Maintenance > AC > Country Code**.

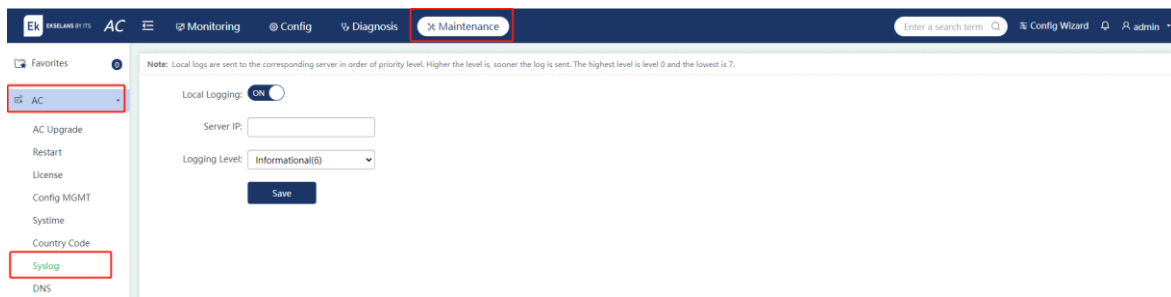
You can set the country or region where the device is located. The required RF band, channel, and power are subject to different countries or regions.



7.1.6 Log Server

Choose **Maintenance > AC > Syslog**.

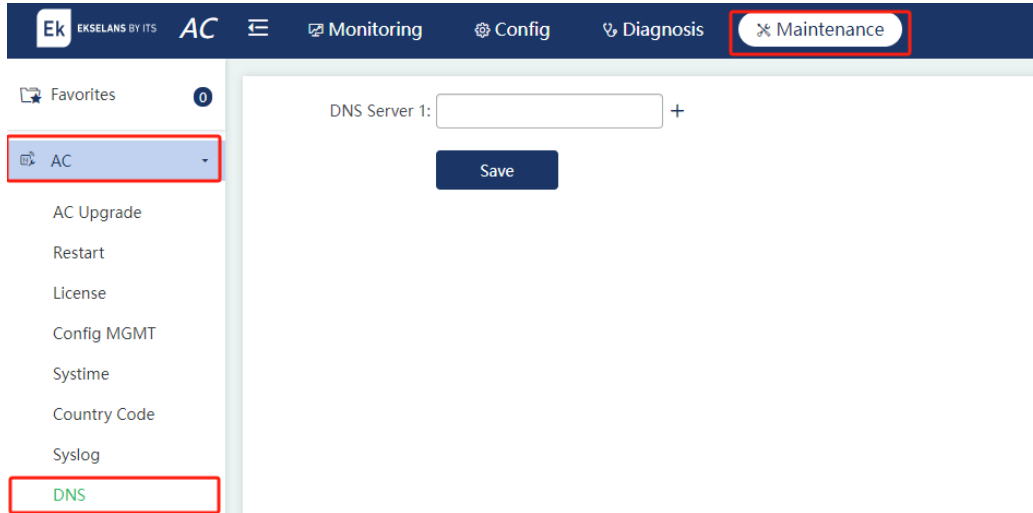
The device can be configured to send local logs to the server for storage and easy query.



7.1.7 DNS

Choose **Maintenance > AC > DNS**.

To implement dynamic domain name resolution, a DNS server must be configured.

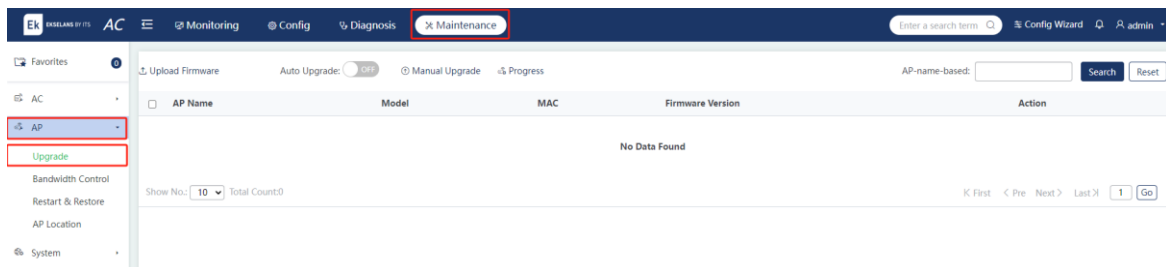


7.2 AP Management

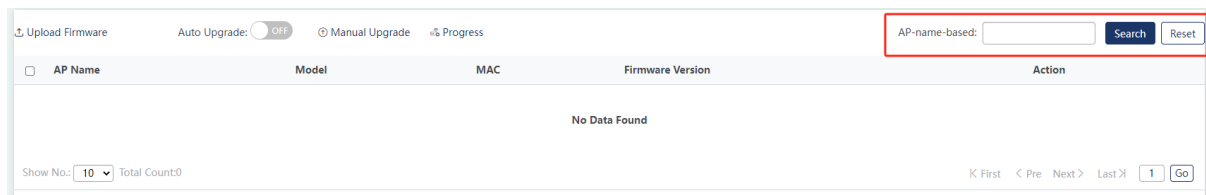
7.2.1 AP Upgrade

Choose **Maintenance > AP > Upgrade**.

Multiple APs can be managed on the AC through the web system, which is quick and convenient.



- (1) Search for an AP: If there are many APs on the page, you can search for a specified AP by the AP name in the upper right corner of the page. Click **Reset** to clear the content in the search box.



- (2) Automatic upgrade: You can toggle on **Auto Upgrade**. The AP will be automatically upgraded to the latest version when a later version is available.

Note

Before upgrading APs on the AC, ensure that the APs can ping each other. Otherwise, the distributed upgrade may fail, which may prolong the upgrade process.

- (3) Single AP upgrade: Click **Upgrade** next to an AP. Upload the AP upgrade file and click **Upgrade**.
- (4) Manual upgrade: Click **Manual Upgrade** to access the **Manual Upgrade** page.

Manual Upgrade ✕

Serial: *

Firmware: * Select firmware bin

Model: * ⓘ

Hardware Version: * Enter a hardware version

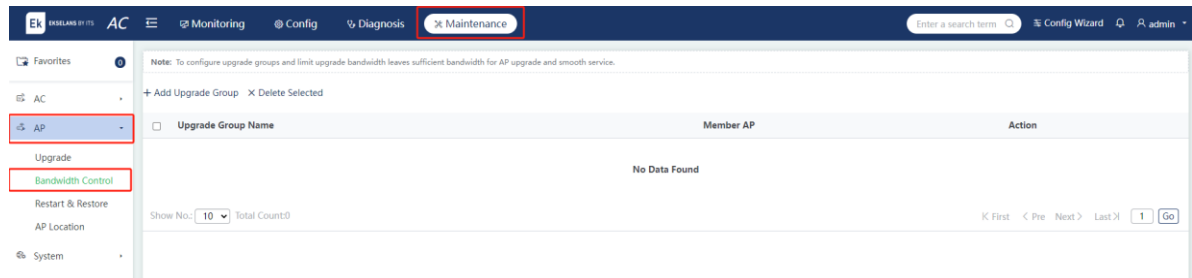
Series	Model	Firmware Version	Hardware Version	Action
No Data Found				

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

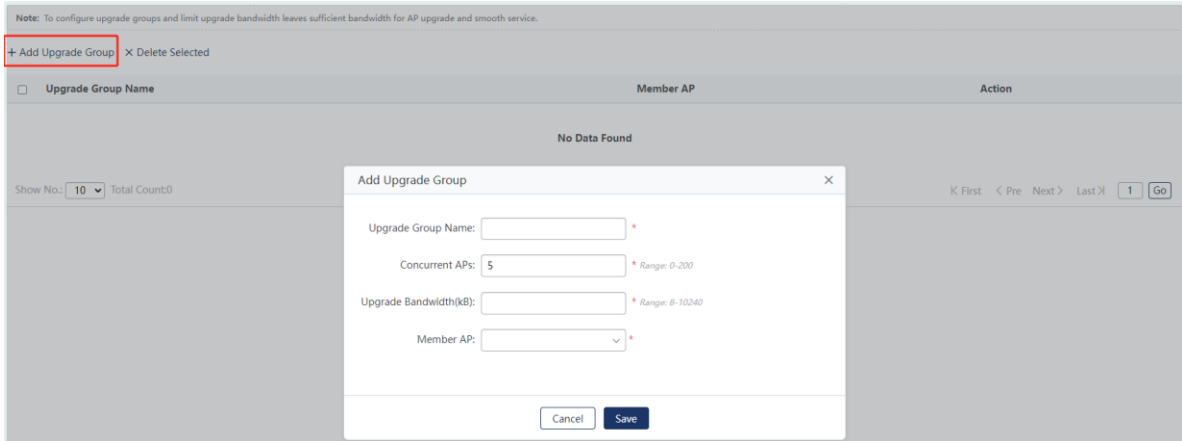
7.2.2 Bandwidth Control

Choose **Maintenance > AP > Bandwidth Control**.

By configuring the upgrade group and limiting the upgrade bandwidth, sufficient bandwidth is reserved when the AP is being upgraded, so that network performance will not be greatly affected by the AP upgrade.



- (1) Add an upgrade group: Click **Add Upgrade Group**. Edit the fields in the pop-up dialog box. Click **Save**. A message indicating the configuration has been saved is displayed. The newly added upgrade group is displayed in the upgrade group list.



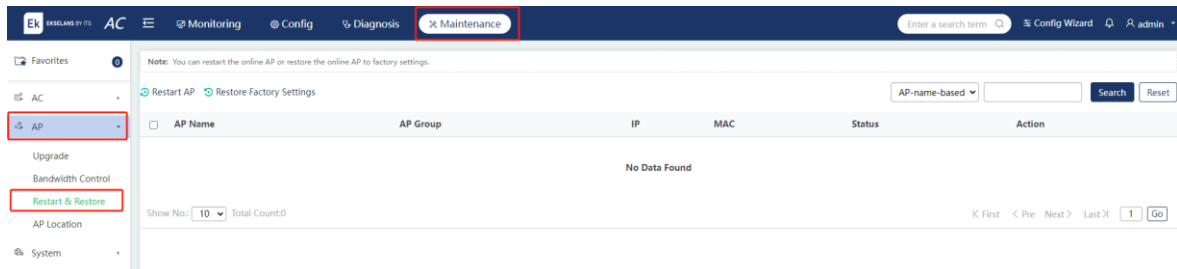
Parameter	Description
Upgrade Group Name	Specifies the name of an upgrade group name.
Concurrent APs	Specifies the number of APs being upgraded concurrently.
Upgrade Bandwidth(kB)	Specifies the bandwidth for AP upgrade.
Member AP	Specifies the member APs in the upgrade group.

- (2) Delete an upgrade group: Click **Delete** next to an upgrade group. Click **OK** in the pop-up dialog box.
- (3) Edit an upgrade group: Click **Edit** next to an upgrade group. The pop-up dialog box displays the information about the upgrade group. You can edit the information. Click **Save**. A message indicating the configuration has been saved is displayed.

7.2.3 AP Restart/Restore

Choose **Maintenance > AP > Restart & Restore**.

Restart online APs or restore them to factory settings.



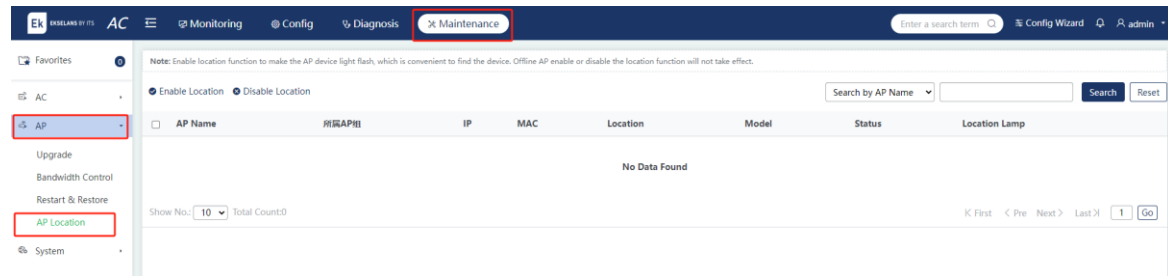
- (1) Restart the AP: Click **Restart AP** next to an AP. If multiple APs need to be restarted, select the APs and click **Restart AP**.

- (2) Restore factory settings: Click **Restore Factory Settings** next to an AP. If multiple APs need to be restored to factory settings, select the APs and click **Restore Factory Settings**.

7.2.4 AP Location

Choose **Maintenance > AP > AP Location**.

When the AP Location feature is enabled, the system LED on the AP flashes to help locate the AP. If an AP goes offline, an attempt to enable or disable AP location will fail.



Enable/Disable AP location: Click the location icon next to an AP to enable/disable the AP Location feature. If the AP Location feature needs to be enabled/disabled for multiple APs, select the APs and click **Enable Location Disable Location**.

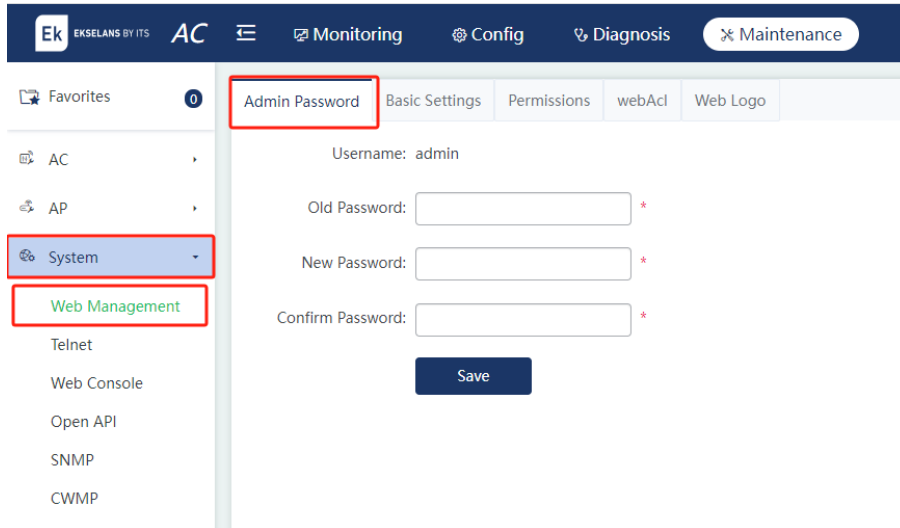
7.3 System

7.3.1 Web Management

Choose **Maintenance > System > Web Management**.

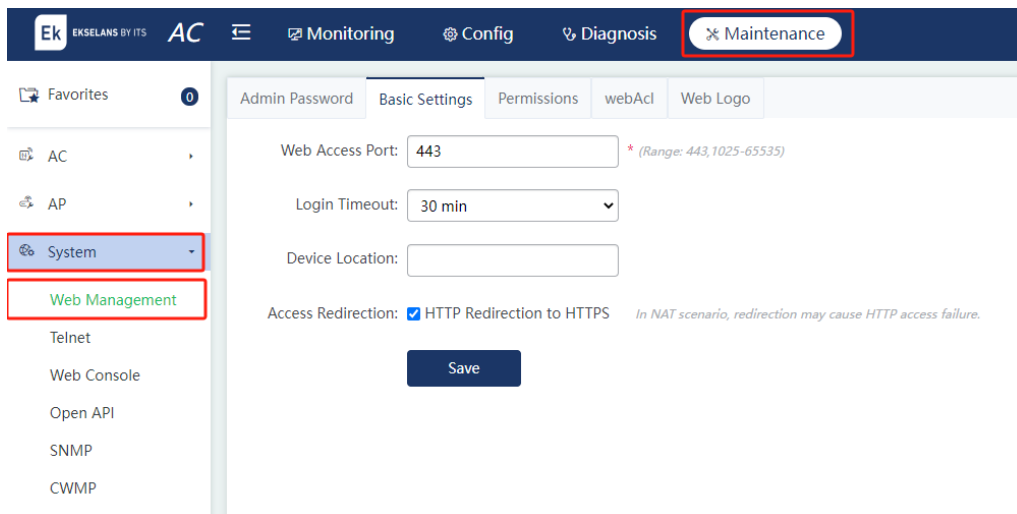
1. Admin Password

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



2. Basic Settings

To facilitate device management, you can enter the device location on the **Basic Settings** page. Set the values of **Web Access Port** and **Login Timeout**. When the login times out, the web page will be automatically exited. If the device supports the login limit, you can set the maximum number of users who can log in to the device simultaneously using the same account (the default maximum number is 10).

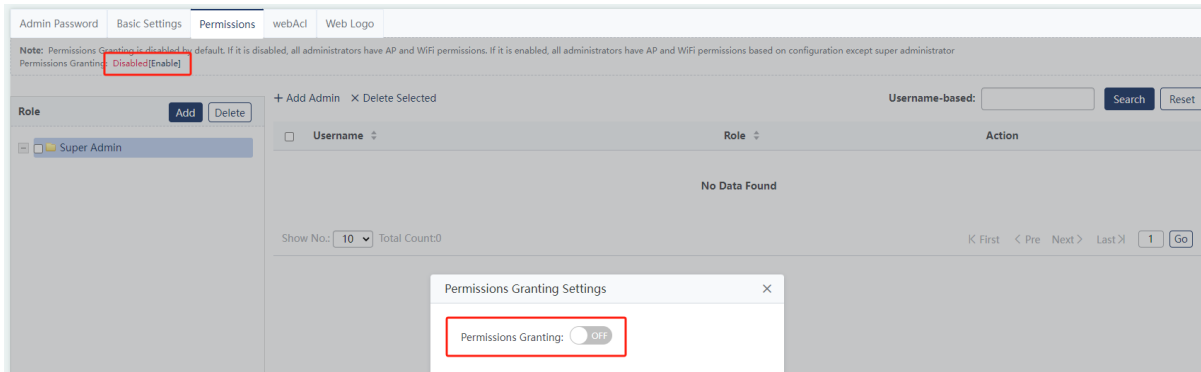


3. Permissions

Multiple administrators can exist on one system. Administrators of different levels have different management permissions. The default user of the system is **admin**.

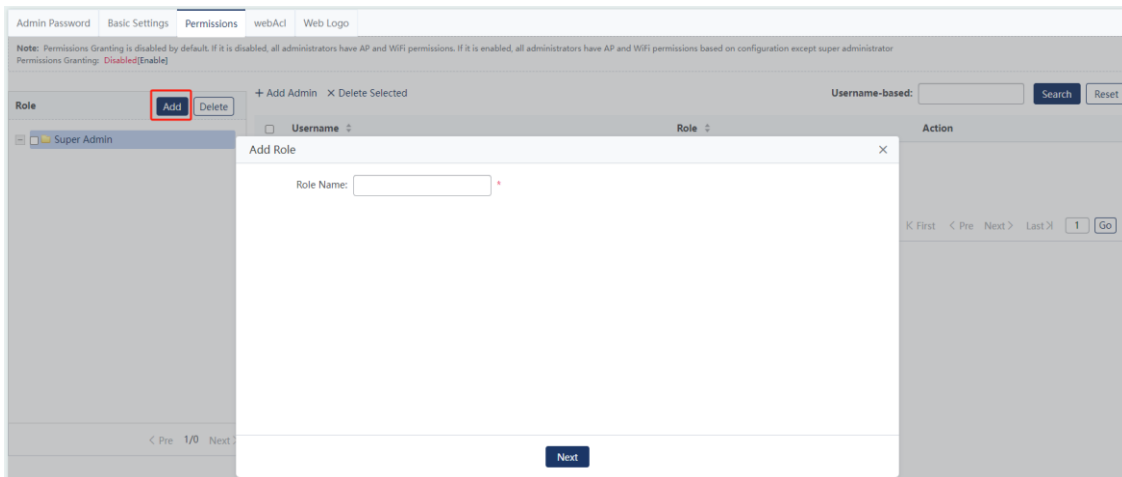
- (1) Administrator permissions (hierarchical and decentralized management): Multiple users can exist on one system, and users can be grouped. Different user groups can be granted with different permissions for WLANs, APs, and AP groups, so that users in different groups have different permissions for WLANs, APs, and AP groups.

Enable/Disable hierarchical and decentralized management: To enable the hierarchical and decentralized feature, toggle on the switch.

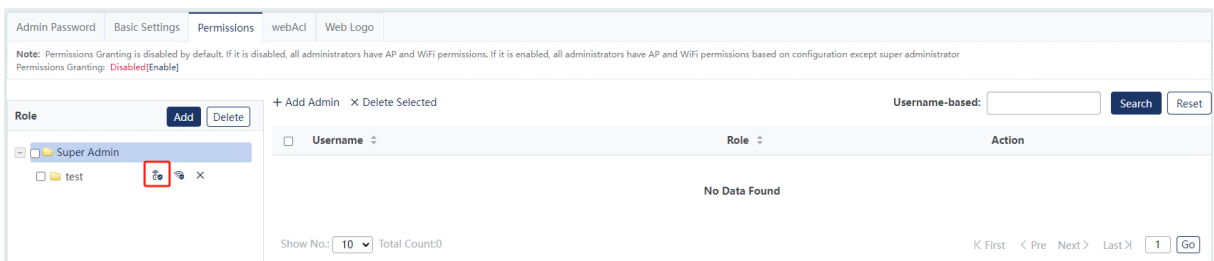


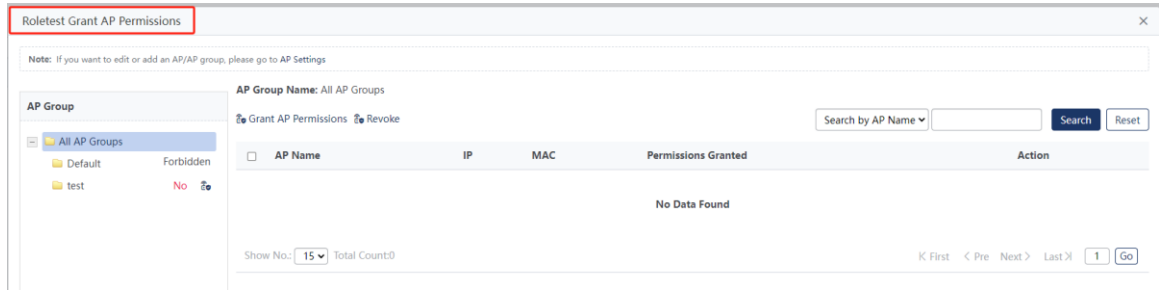
Add a role: Adding a role includes three steps: role adding, AP authorization, and Wi-Fi authorization. You can assign permissions to one role at a time.

Common administrators who belong to this role will have all AP and Wi-Fi permissions for this role. They have no permissions for other APs and Wi-Fi networks to which this role is not allowed to access.

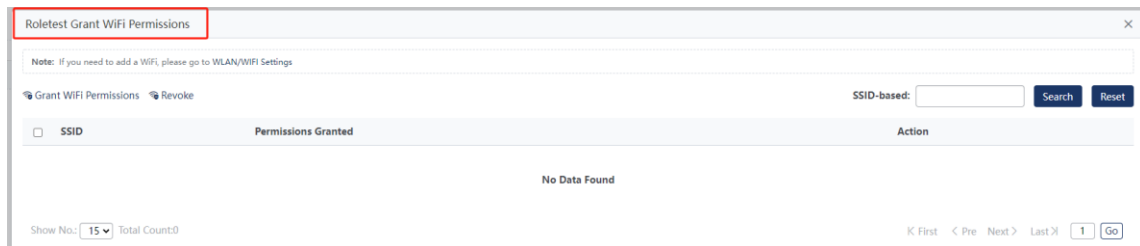
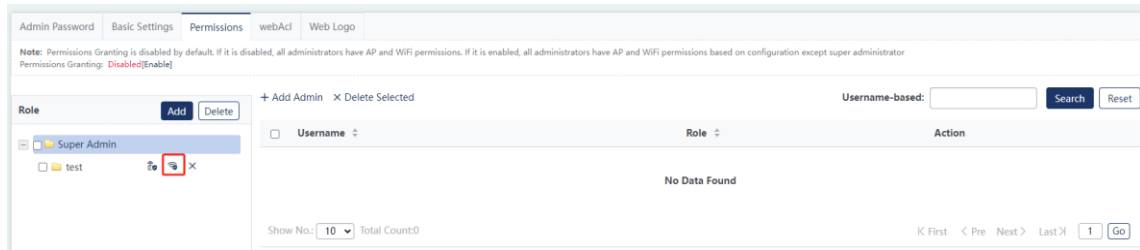


Grant AP permissions:



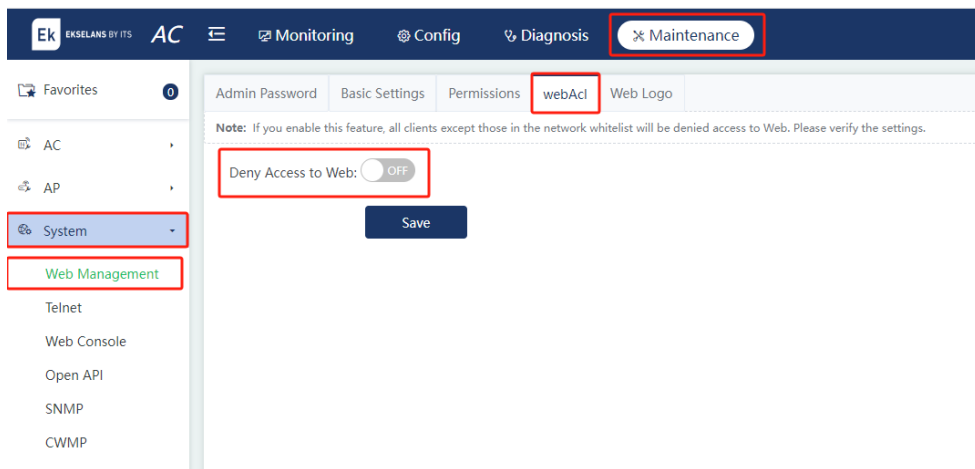


Grant Wi-Fi permissions:



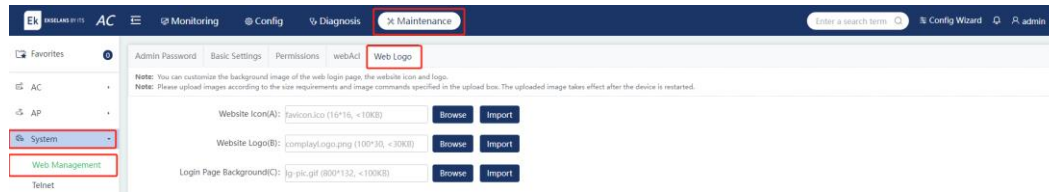
4. Web Access Permission Management

This feature is used to manage login permissions for the web system. When **Deny Access to Web** is enabled, the web system cannot be logged in to.



5. Web Logo

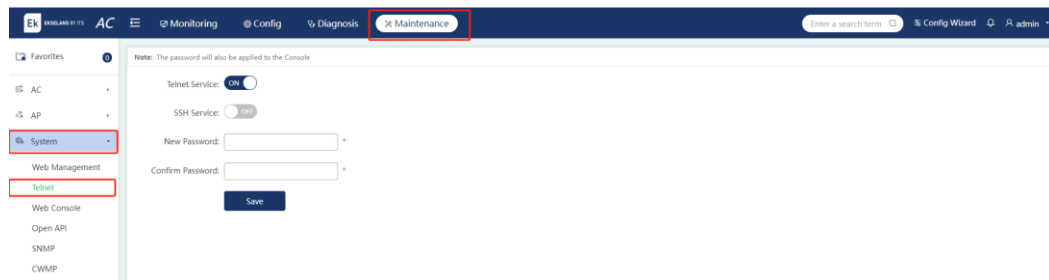
With this feature, you can customize the login page of the web system and the logo in the upper left corner of the menu.



7.3.2 Telnet

Choose **Maintenance > System > Telnet**.

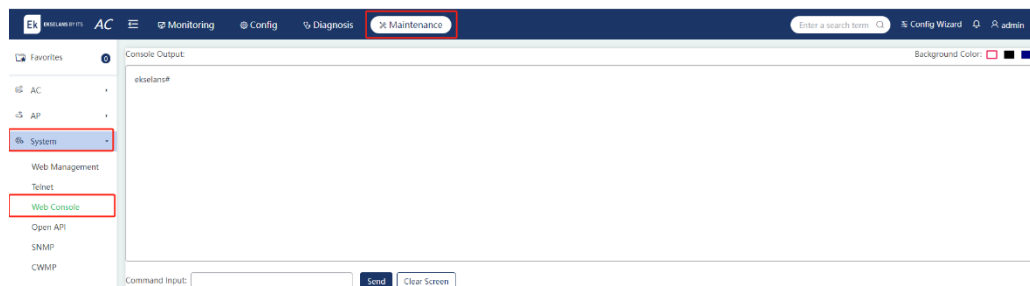
The Telnet feature enhances the system security and information interaction security. The Telnet and SSH services can be enabled/disabled and the password can be configured on the Telnet configuration page.



7.3.3 Web Console

Choose **Maintenance > System > Web Console**.

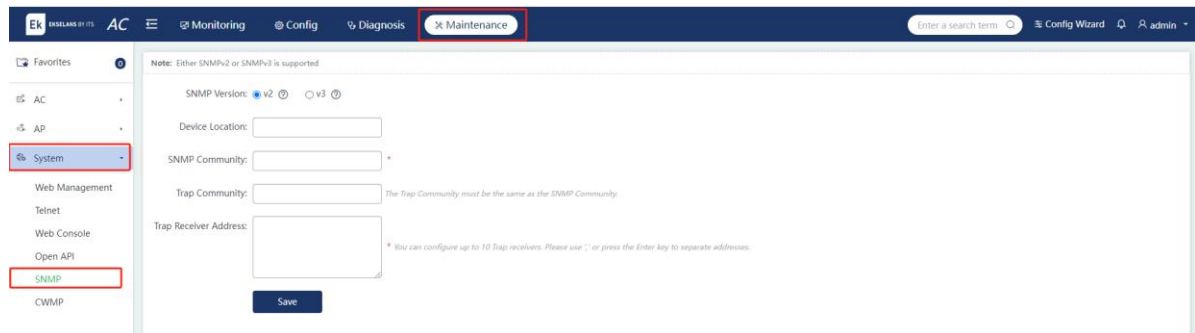
You can send CLI commands through the web console.



7.3.4 SNMP

Choose **Maintenance > System > SNMP**.

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



7.3.5 CWMP

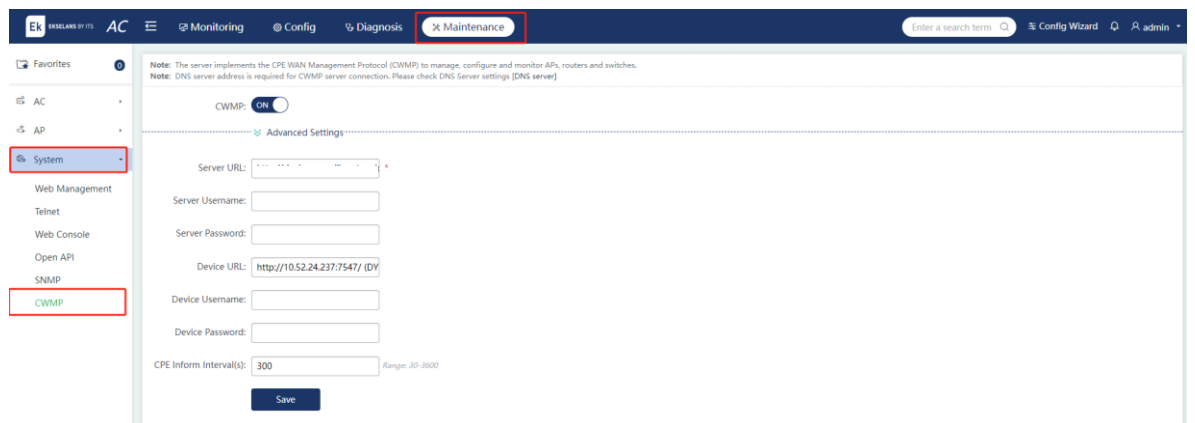
Choose **Maintenance > System > CWMP**.

The CWMP protocol is the CPE WAN Management Protocol. The server can manage, configure, and monitor devices such as ACs, APs, or switches through this protocol.

Through configuration, the device can be connected to and managed by a cloud platform or other servers.

Note

When connecting to a server through the CWMP protocol, you need to configure the correct DNS server so that the device can correctly resolve the server's domain name. Therefore, check whether the DNS server is correctly configured.



Parameter	Description
CWMP	The CWMP switch is used to enable/disable the CWMP feature.

Server URL	Specifies the IP address of the server.
Server Username	Specifies the server username, which can be used for verification.
Server Password	Specifies the server password, which can be used for verification.
Device URL	Specifies the device URL, which can be used to actively connect to the server on the same LAN.
Device Username	Specifies the device username, which can be used for verification.
Device Password	Specifies the device password, which can be used for verification.
CPE Inform Interval(s)	Specifies the interval for connecting to the server, namely, the interval of heartbeat packets.