EKSELANS BY ITS

USER MANUAL

AX 3000

331019

Indoor WiFi Access Point
WiFi6 (802.11ax) 3000Mbps
1G PoE IN port + 1G/2,5G SFP uplink port
PoE IN / DC-IN

ITS Partner O.B.S S.L · Av. Cerdanyola 79-81 Local C
08172 Sant Cugat del Vallés · Barcelona (Spain)
Phone:+34935839543 · info@ek.plus · www.ek.plus

Copyright

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 statementor 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 error

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 symbols 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

This manual provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors. It is intended for the users who have some experience in installing and maintaining network hardware. At the same time, it is assumed that the users are already familiar with the related terms and concepts.

1 Product Overview

The AX 3000 is a dual-band dual-radio access point compliant with the IEEE 802.11ax standard. The AX 3000 AP provides a combined data rate of 2.976 Gbps, with up to 574 Mbps in the 2.4 GHz band and 2.402 Gbps in the 5 GHz band. Designed for flexible deployments in the field of education, government, finance and business, the AX 3000 AP offers one combo port.

1.1 Appearance

The AX 3000 provides two radio frequency (RF) connectors, one 10/100/1000 BASE-T Ethernet port, one 2.5G SFP port, one Console port and one DC power plug. The AP supports PoE or DC power supply.

Figure 1-1 Appearance

Figure 1-2 Front Panel

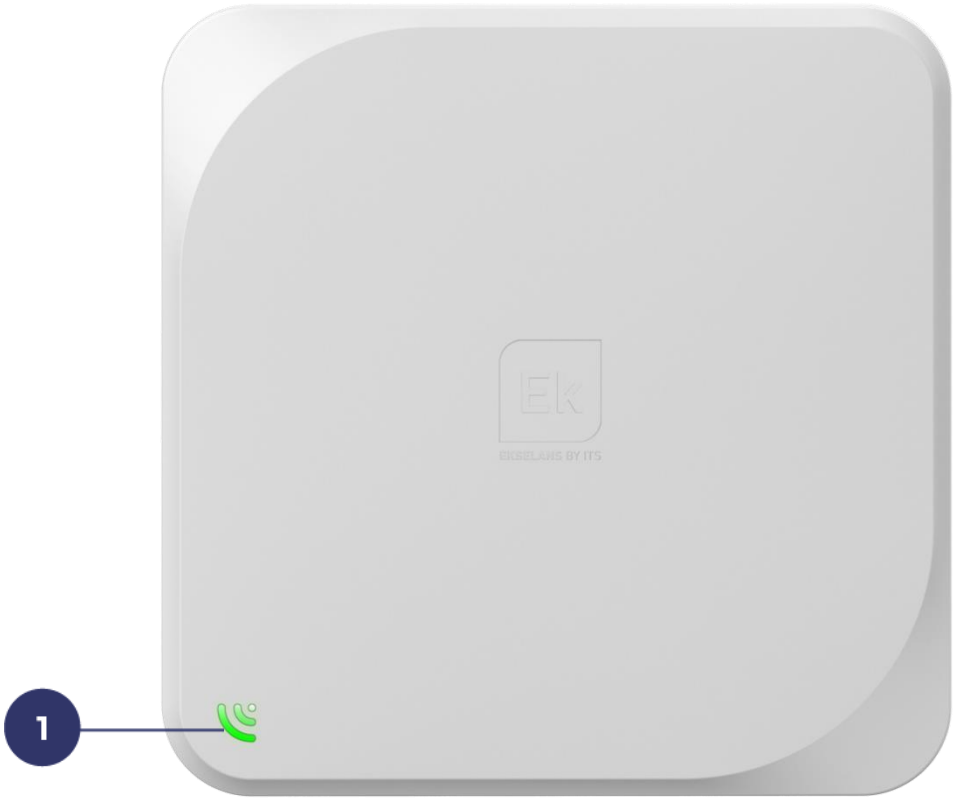


Table 1-1 Front Panel

No.	Item	Description
1	LED	Indicate the operation status of device.

Figure 1-3 Side View

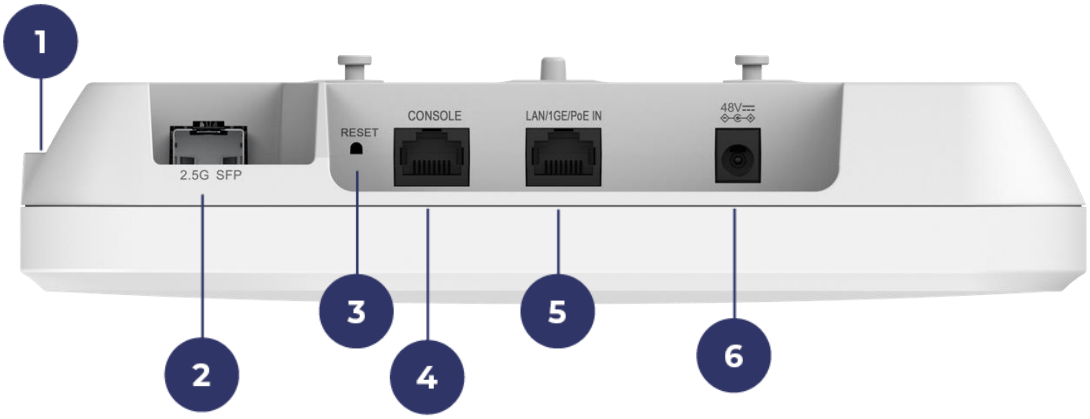


Table 1-2 Side View

No.	Button and Port	Description
1	Anti-theft lock hole	Connect to the anti-theft lock.
2	2.5G SFP port	The uplink SFP port for service data transmission.
3	Reset button	Reboot the device or restore the device to factory settings.
4	Console port	Connect to the device that is managed with the serial cable.
5	1000 BASE-T Ethernet port	The uplink adaptive Ethernet port for service data transmission. Support IEEE 802.3af standard PoE power supply.
6	DC power plug	Connect to the DC power adapter to supply power to the AP.

Note

The nameplate is at the bottom of the access point.

1.2 Package Contents

Table 1-3 Package Contents

Item	**Quantity**
AX 3000 Access Point	1
Mounting Bracket	1
Wall Anchor	2
Phillips Pan Head Screws M4 x 20	4
Warranty Card	1
Installation Guide	1

1.3 Technical Specifications

1.3.1 Size and Weight

Table 1-4 Size and Weight

Item	Parameter
Main Unit Dimensions (W x D x H)	220 mm × 220 mm × 49 mm (8.66 in. x 8.66 in. x 1.93 in.)
Weight	Main Unit: 0.6 kg (1.33 lbs.) Bracket: 0.2 kg (0.44 lbs.)
Mounting	Ceiling/wall mount capable
Anti-theft Lock	Kensington lock Security screw
Bracket Dimensions (W x D x H)	120 mm×120 mm×8 mm (4.72 in. x 4.72 in. x 0.31 in.)
Mounting Hole Pattern	53 mm (2.09 in.)
Mounting Hole Diameter	6.5 mm (0.26 in.)

1.3.2 RF

Table 1-5 RF

Item	Parameter
RF Design	2 RF, 2 Wireless RF connectors Radio1: 2.4 GHz, 2×2 MIMO (2 spatial streams) Radio2: 5 GHz, 2×2 MIMO (2 spatial streams) Combined dual-band:4 spatial streams
Operating Frequency	Radio1: 802.11b/g/n/ax, 2.4 GHz-2.4835 GHz, HE40 Radio2: 802.11a/n/ac/ax, 5.150 GHz-5.350 GHz, HE80/HE160 802.11a/n/ac, 5.470 GHz-5.725 GHz, 5.725 GHz-5.850 GHz, HE80 (country-specific restrictions apply)

Max. Data Rate	Radio1: 2.4 GHz, 574 Mbps Radio2: 5 GHz, 2.402 Gbps Combined dual-band: 2.976Gbps
Antenna Type	Built-in smart antenna
Antenna Gain	2.4 GHz: 3 dBi 5 GHz: 3 dBi
Max. Transmit Power	20 dBm (country-specific restrictions apply)
Transmit Power Adjustment	Configurable in increments of 1 dBm
Modulation	OFDM: BPSK@6/9Mbps, QPSK@12/18Mbps, 16-QAM@24Mbps, 64-QAM@48/54Mbps DSSS: DBPSK@1Mbps, DQPSK@2Mbps, and CCK@5.5/11Mbps MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM and 1024QAM OFDMA
Receive Sensitivity	11b: -96dBm(1Mbps), -93dBm(5Mbps), -89dBm(11Mbps) 11a/g: -91dBm(6Mbps), -85dBm(24Mbps), -80dBm(36Mbps), -74dBm(54Mbps) 11n: -90dBm@MCS0, -70dBm@MCS7, -89dBm@MCS8, -68dBm@MCS15 11ac: HT20: -88dBm(MCS0), -63dBm(MCS9) 11ac: HT40: -85dBm(MCS0), -60dBm(MCS9) 11ac: HT80: -82dBm(MCS0), -57dBm(MCS9) 11ax: HE80: -82dBm(MCS0), -57dBm(MCS9),-52dBm(MCS11) 11ax: 160MHz: -77dBm(MCS0), -50dBm(MCS11)

1.3.3 Ports

Table 1-6 Ports

Item	Description
Bluetooth	Bluetooth 5.1
Fixed Service Port	One 10/100/1000 Base-T Ethernet port (IEEE 802.3af-compliant PoE) One 2.5G SFP port (compatibility with 1GE SFP)
Fixed Management Port	One RJ45 Console port

GPS	Not supported
LED	One system status LED
Button	One reset button

1.3.4 Power Supply

Table 1-7 Power Supply

Item	Description
Power Supply	1. DC power adapter: 48 V/0.6 A (Optional. Please refer to Power Supply for details.) 2. PoE: IEEE 802.3af-compliant
Max. Power Consumption	12.95 W

⚠ Caution

The power adapter is optional. If you need to use a DC power adapter for power supply, please purchase an adapter that meets the corresponding safety requirements.

1.3.5 Environment and Reliability

Table 1-8 Environment and Reliability

Item	Description
Temperature	Operating: -10°C to +50°C (14°F to 122°F) Storage: -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 (546 ft.), the maximum temperature decreases by 1°C (1.8°F).
Humidity	Operating: 5% to 95% (RH), non-condensing Storage: 5% to 95% (RH), non-condensing)
Regulatory compliance	EN 55032, EN 55035, EN 61000-3-3, EN IEC 61000-3-2, EN 301 489-1, EN 301 489-3, EN 301 489-17, EN 300 328, EN 301 893, EN 300 440, FCC Part 15, EN IEC 62311, IEC 62368-1, and EN 62368-1

1.4 LEDs and Button

Note

- The description of LED status applies to both Fit AP and Fat AP, unless otherwise noted.

Table 1-9 System LED Status

Color	Frequency	Status Description
Off	N/A	The AP is NOT receiving power, or the AP is receiving power, but the LED is disabled by software.
Solid green	N/A	Program system initialization is in progress.
Solid red	N/A	The system is in normal operation, but the uplink service port of the AP is down.
Slow blinking red	On for 3s and off for 1s	In Fit AP mode, the establishment of a CAPWAP tunnel between the AP and the AC times out.
Fast blinking blue	On for 0.2s and off for 0.2s	In Fit AP or Cloud AP mode, the AP is in the process of software update
Solid blue	N/A	The system and the AP are in normal operation, but no wireless clients are currently online.
Blinking blue	On for 1s and off for 1s	The system and the AP are in normal operation, and at least one wireless client is currently online.
Fast blinking red	On for 0.2s and off for 0.2s	In Fit AP mode, LED location function is enabled to locate a specific AP.

Table 1-10 Reset Button

Reset button	Press and hold for less than 2s	Reboot the device.
	Press and hold for more than 3s	Restore default settings.

1.5 SFP Modules

The 2.5G SFP port of the AP supports both copper and fiber links. The negotiation speed may vary with the SFP module type and the speeds on both sides of the link. Please refer to Table 1-11 and Table 1-12.

Table 1-11 Negotiation Speed When Connected with SFP Port on Peer Device

AP SFP Port Speed	SFP Fiber Module Speed	Negotiation Speed		
		1 Gbps	1 Gbps/10 Gbps/Auto	1 Gbps/2.5 Gbps/10 Gbps/Auto
1 Gbps	3 Gbps	1 Gbps	1 Gbps	1 Gbps
1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps

2.5 Gbps	3 Gbps	Not supported	Not supported	2.5 Gbps
2.5 Gbps	1 Gbps	Not supported	Not supported	1 Gbps

Table 1-12 Negotiation Speed When Connected with Copper Port on Peer Device

AP SFP Port Speed	SFP Copper Module Speed	Negotiation Speed		
		1 Gbps	1 Gbps/10 Gbps/Auto	1 Gbps/2.5 Gbps/10 Gbps/Auto
1 Gbps	2.5 Gbps	Not supported	Not supported	Not supported
1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps
2.5 Gbps	2.5 Gbps	Not supported	Not supported	2.5 Gbps
2.5 Gbps	1 Gbps	Not supported	Not supported	Not supported

⚠ Caution

- The 2.5G SFP port of the AP does not support speed negotiation. When you use the transceiver module, the speed of the AP, the module, and the port of peer device must be the same.
- The SFP port and copper port can be multiplexed as a combo port. If two ports are connected with cables at the same time, AP will preferentially select the SFP port for data transmission (the copper port is automatically disabled). When the cable of SFP port is unplugged, the copper port is automatically enabled.

2 Preparing for Installation

2.1 Safety Precautions

Note

- To avoid personal injury and device damage, carefully read the safety precautions before you install the device.
- The following safety precautions may not cover all possible dangers.

2.1.1 General Safety Precautions

- Do not expose the AP to high temperature, dusts, or harmful gases.
- Do not install the AP in an inflammable or explosive environment.
- Keep the AP away from EMI sources such as large radar stations, radio stations, and substations.
- Do not subject the AP to unstable voltage, vibration, and noises.
- The installation site should be free from water flooding, seepage, dripping, or condensation. The installation site should be selected according to network planning and communications equipment features, and considerations such as climate, hydrology, geology, earthquake, electrical power, and transportation.
- Keep the AP at least 500 meters away from the ocean and do not face it towards the sea breeze.
- Do not place the device in walking areas.
- During the installation and maintenance, do not wear loose clothes, ornaments, or any other things that may be hooked by the chassis.
- Keep tools and components away from walking areas.

2.1.2 Handling Safety

- Prevent the device from being frequently handled.
- Cut off all the power supplies and unplug all power cords before moving or handling the device.

2.1.3 Electric Safety

Warning

- Improper or incorrect electric operations may cause a fire, electric shock, and other accidents, and lead to severe and fatal personal injury and device damage.

- Direct or indirect contact with high voltage or mains power supply via wet objects may cause fatal dangers.

- Observe local regulations and specifications during electric operations. Only personnel with relevant qualifications can perform such operations.
- Check whether there are potential risks in the work area. For example, check whether the power supply is grounded, whether the grounding is reliable, and whether the ground is wet.
- Learn about the position of the indoor emergency power switch before installation. Cut off the power switch in case of accidents.
- Check the device carefully before shutting down the power supply.
- Do not place the device in a damp/wet location. Do not let any liquid enter the chassis.
- Keep the device far away from grounding or lightning protection devices for power equipment.
- Keep the device away from radio stations, radar stations, high-frequency high-current devices, and microwave ovens.

2.1.4 Storage Safety

To ensure the normal operation of the device after storage, please refer to the storage temperature/humidity requirements in the specifications for the storage environment.

⚠ Caution

If the device has been stored for more than 18 months, the device needs to be powered on and run for 24 hours without interruption to complete the activation of the device.

2.2 Installation Environment Requirements

Install the device indoors to ensure its normal operation and prolonged service life.

The installation site must meet the following requirements.

2.2.1 Bearing Requirements

Evaluate the bearing capacity of the installation site based on the actual weight of the device and its accessories (for example, the bracket and power supply modules), and ensure that the installation site meets the bearing requirements.

2.2.2 Ventilation Requirements

Reserve sufficient space in front of the air vents to ensure normal heat dissipation. After various cables are connected, bundle the cables or place them in the cable management bracket to avoid blocking air inlets.

2.2.3 Space Requirement

Maintain a minimum clearance of 0.4 cm (15.75 in.) around the device to ensure proper cooling and ventilation.

2.2.4 Temperature/Humidity Requirements

To ensure the normal operation and prolonged service life of the device, maintain an appropriate temperature and humidity in the equipment room.

The equipment room with too high or too low temperature and humidity for a long period may damage the device.

- In an environment with high humidity, the insulating material may have poor insulation or even leak electricity.
- In an environment with low humidity, the insulating strip may dry and shrink, loosening screws.
- In a dry environment, static electricity is prone to occur and damage the internal circuits of the device.
- Too high temperatures can accelerate the aging of insulation materials, greatly reducing the reliability of the device and severely affecting its service life.

Note

The ambient temperature and humidity of the device are measured at the point that is 1.5 m (59.06 in.) above the floor and 0.4 m (15.75 in.) before the device when there is no protective plate in front or at the back of the device.

2.2.5 Cleanliness Requirements

Dust poses a major threat to the device. The indoor dust takes on a positive or negative static electric charge when falling on the device, causing poor contact of the metallic joint. Such electrostatic adhesion may occur more easily when the relative humidity is low, not only affecting the service life of the device, but also causing communication faults. Table 2-1 describes the requirements for the dust content and granularity in the equipment room.

Table 2-1 Requirements for Dust

Dust	Unit	Content
Dust particles (diameter ≤ 0.5 μm)	Particles/m^3	≤1.4×10^7
Dust particles (0.5 μm ≤ diameter ≤ 1 μm)	Particles/m^3	≤7×10^5
Dust particles (1 μm ≤ diameter ≤ 3 μm)	Particles/m^3	≤2.4×10^5
Dust particles (3 μm ≤ diameter ≤ 1 μm)	Particles/m^3	≤1.3×10^5

Apart from dust, the salt, acid, and sulfide in the air in the equipment room must meet strict requirements. These harmful substances will accelerate metal corrosion and component aging. Therefore, the equipment room should be properly protected against the intrusion of harmful gases, such as sulfur dioxide, hydrogen sulfide, nitrogen dioxide, and chlorine gas. Table 2-2 lists limit values for harmful gases.

Table 2-2 Requirements for Gases

Gas	Average (mg/m³)	Maximum (mg/m³)
Sulfur dioxide (SO_2)	0.2	1.5
Hydrogen sulfide (HS)	0.006	0.03
Nitrogen dioxide (NO_2)	0.04	0.15
Ammonia gas (NH_3)	0.05	0.15
Chlorine gas (Cl_2)	0.01	0.3

Note

Average refers to the average value of harmful gases measured in one week. **Maximum** refers to the upper limit of harmful gases measured in one week, and the maximum value lasts up to 30 minutes every day.

2.2.6 Anti-interference Requirements

- Take interference prevention measures for the power supply system.
- Keep the device away from the grounding equipment or lightning and grounding equipment of the power device as much as possible.
- Keep the device far away from high-frequency current devices such as high-power radio transmitting station and radar launcher.
- Take electromagnetic shielding measures when necessary.

2.2.7 Lightning Protection Requirements

The device can guard against lightning strikes. As an electric device, it may still be damaged by strong lightning strikes. The following lightning protection measures should be taken:

- Ensure that the neutral point of the AC power socket is in good contact with the ground.
- You are advised to install a power lightning arrester in front of the power input end to enhance the lightning prevention for the power supply.

2.2.8 Installation Site Requirements

Regardless of whether the device is installed on the wall or ceiling, the following conditions must be met:

- Sufficient space should be reserved at the air inlets and outlets of the device to ensure heat dissipation.
- The installation site should be properly ventilated.
- The installation site is sturdy enough to support the weight of the device and its accessories.

2.3 Tools

Table 2-3 Tools

Common Tools	Phillips screwdrivers, wires, Ethernet cable, fastening bolts, diagonal pliers, and binding straps
Special Tools	Antistatic gloves, wire stripper, crimping pliers, crystal connector crimping pliers, and wire cutter
Meter	Multimeter, and bit error rate tester (BERT)
Relevant Devices	PC, display, and keyboard

Note

The device is delivered without a tool kit. The tool kit and cables are customer-supplied.

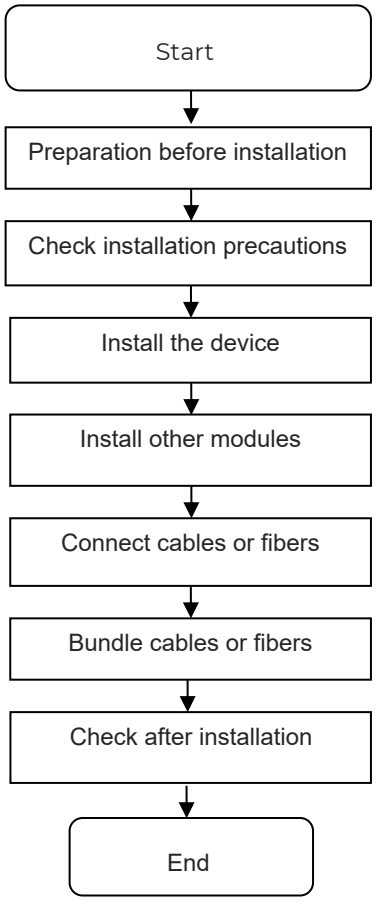
3 Installing the Access Point

The AX 3000 AP must be fixed and installed indoors.

⚠ Caution

Before installing the device, make sure you have carefully read the requirements described in Chapter 2.

3.1 Installation Flowchart



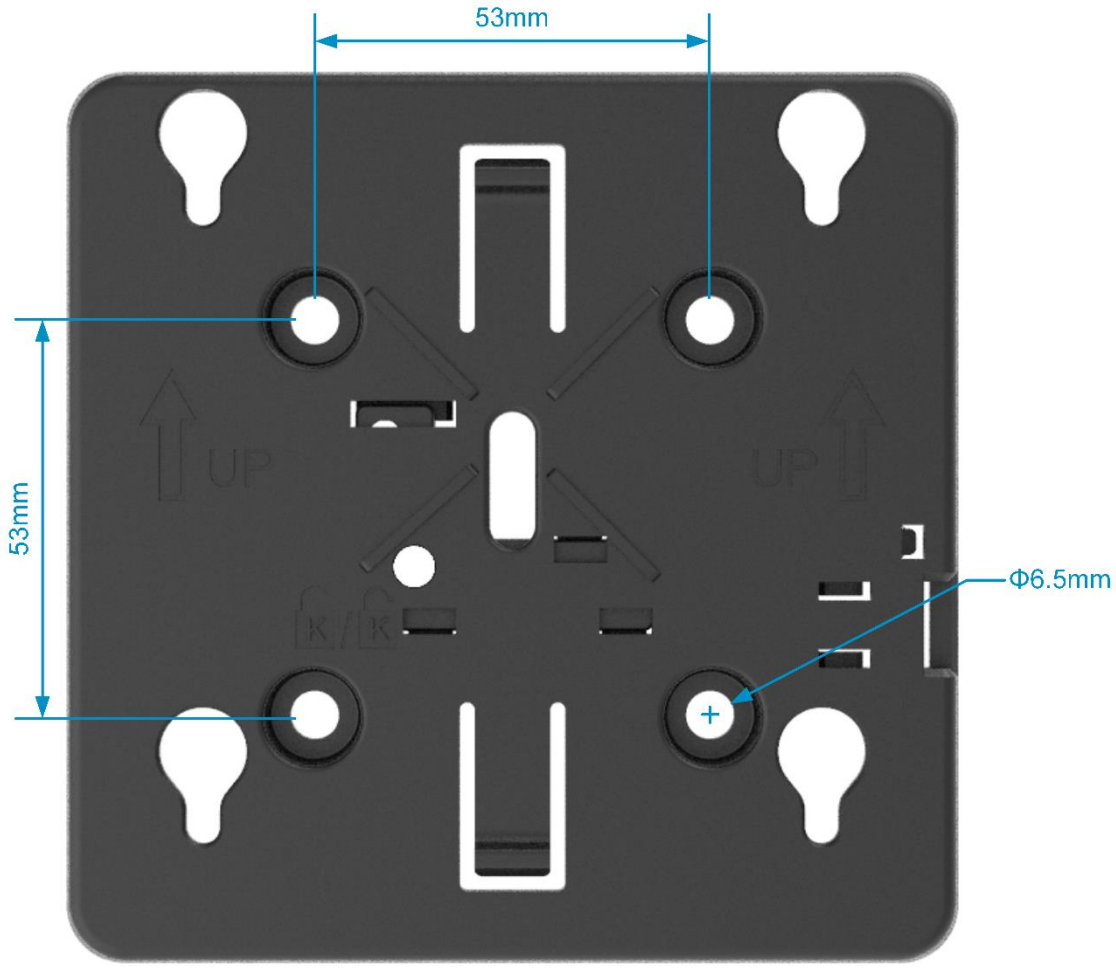
3.2 Before You Begin

Before you install the device, verify that all the parts in the package contents are there and make sure that:

- The installation position provides sufficient space for heat dissipation.
- The installation position meets the temperature and humidity requirements of the device.

- The power supply and required current are available in the installation position.
- The Ethernet cable have been deployed in the installation position.
- The selected power supply modules meet the system power requirements.
- The position of the indoor emergency power switch is learned before installation. The power switch is cut off in case of accidents.
- For ceiling-mounted or wall-mounted AP, the mounting bracket size, mounting hole pattern and diameter should meet the requirements in **Table 1-4 Size and Weight**, as shown in Figure 3-1.

Figure 3-1 Mounting Bracket



3.3 Precautions

To avoid damage to the AP, observe the following safety precautions:

- Do not power on the device during installation.
- Install the device in a well-ventilated location.
- Do not subject the device to high temperatures.
- Keep away from high voltage cables.
- Install the device indoors.

- Do not expose the device in a thunderstorm or strong electric field.
- Keep the device clean and dust-free.
- Disconnect the device before cleaning it.
- Do not wipe the device with a damp cloth.
- Do not wash the device with liquid.
- Do not open the enclosure when the device is working.
- Fasten the device tightly.

3.4 Installing the Access Point

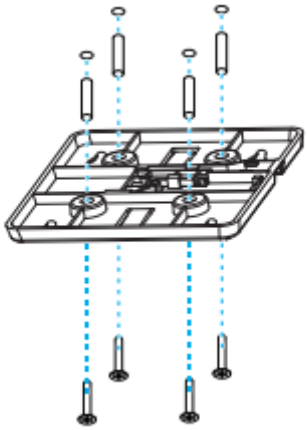
Note

- **You are advised to install the device where you can get the optimal coverage.**
- In the indoor area, the signal coverage of the ceiling-mounted device is larger than that of the wall-mounted device. Please choose the ceiling-mounting method first.

3.4.1 Ceiling Mounting

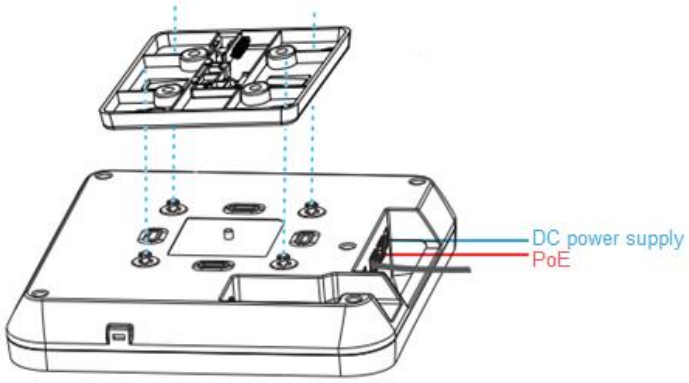
(1) Drill four 6.5 mm (0.26 in.) diameter holes in the ceiling, 53 mm (2.09 in.) apart. Tap wall anchors into the holes, and drive screws through the mounting bracket into the anchors to secure the bracket.

Figure 3-2 Attaching the Mounting Bracket to the Ceiling



(2) Align the square feet on the rear of the AP with the mounting holes on the bracket.

Figure 3-3 Aligning the Square Feet with the Mounting Holes

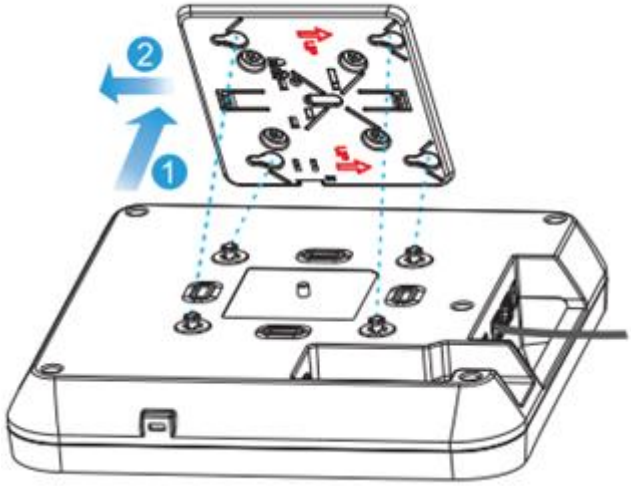


⚠ Caution

Install the Ethernet cables before mounting the AP on the bracket.

(3) Slide the AP onto the bracket in the opposite direction of the arrow on the mounting bracket until it clicks into place.

Figure 3-4 Mounting the AP on the Bracket



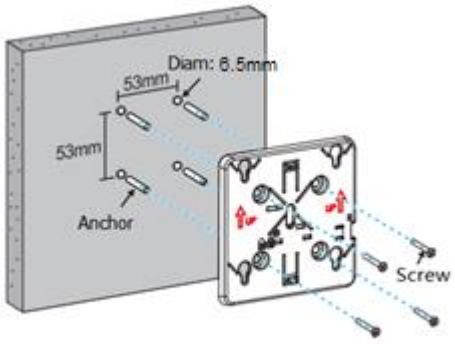
⚠ Caution

- The AP can be installed in any of four directions on the mounting bracket depending on how you route the Ethernet cable.
- The square feet should fit easily into the mounting slots. Do not forcibly push the AP into the slots.
- After installation, verify that the AP is securely fastened.

3.4.2 Wall Mounting

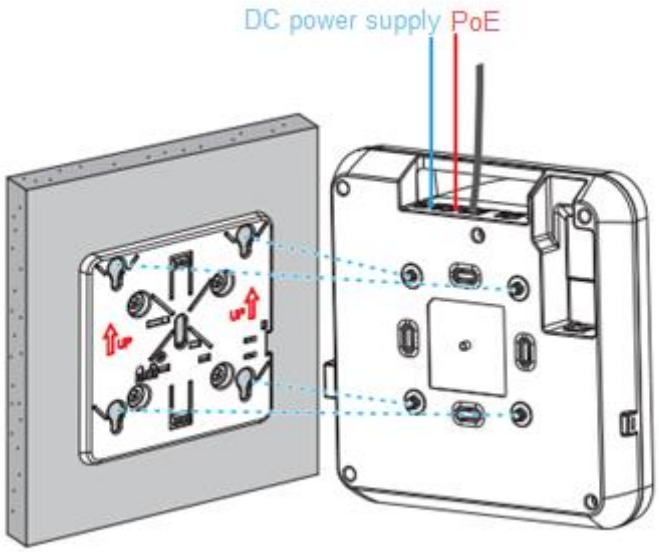
(1) Drill four 6.5 mm (0.26 in.) diameter holes in the wall and 53 mm (2.09 in.) apart, with the arrow on the mounting bracket facing up. Tap wall anchors into the holes, and drive screws through the mounting bracket into the anchors to secure the bracket.

Figure 3-5 Attaching the Mounting Bracket to the Wall



(2) Align the square feet on the rear of the AP with the mounting holes on the bracket.

Figure 3-6 Aligning the Square Feet with the Mounting Holes



⚠ Caution

Install the Ethernet cables before mounting the AP on the bracket.

(3) Slide the AP into the holes in the opposite direction of the arrows on the mounting bracket until it clicks into place.

⚠ Caution

- When mounting the AP on the wall, keep the EK logo pointed upwards.
- The square feet should fit easily into the mounting slots. Do not forcibly push the AP into the slots.
- After installation, verify that the AP is securely fastened.

3.4.3 Removing the Access Point

(1) If the AP is installed on the ceiling, hold the AP with your hands and slide it sideways and away from the bracket in the LAN port direction.

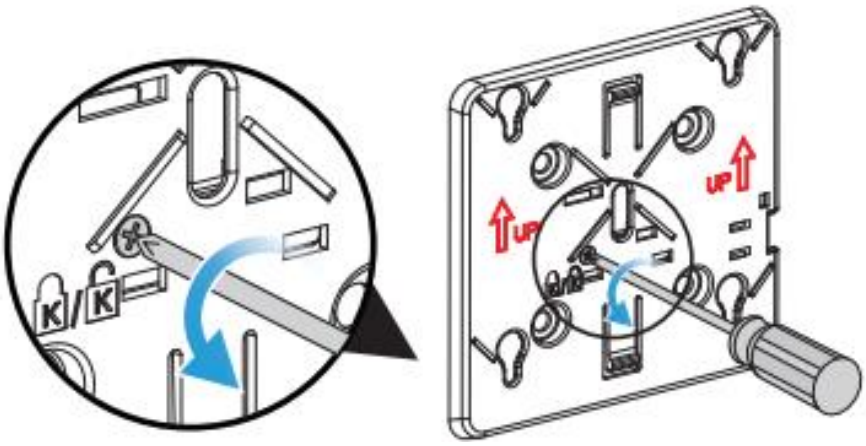
(2) If the AP is installed on the wall, hold the AP with your hands and push it upward and away from the bracket in the LAN port direction.

3.5 Installing other modules

3.5.1 Securing the Access Point

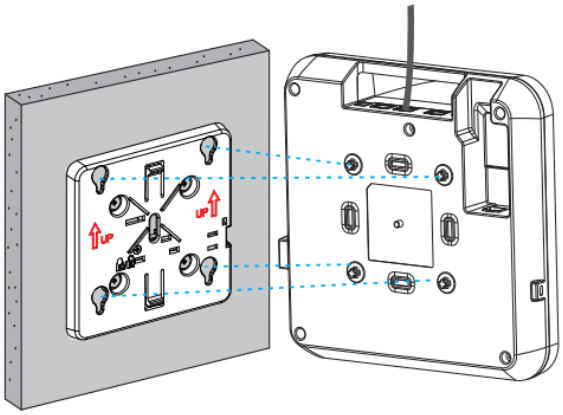
(1) Loosen the screw on the mounting bracket and engage the security screw.

Figure 3-7 Engaging the Security Screw



(2) Align the square feet on the rear of the AP over the mounting holes on the bracket, slide the AP in the opposite direction of the arrows on the mounting bracket until it clicks into place.

Figure 3-8 Mounting the AP on the Bracket



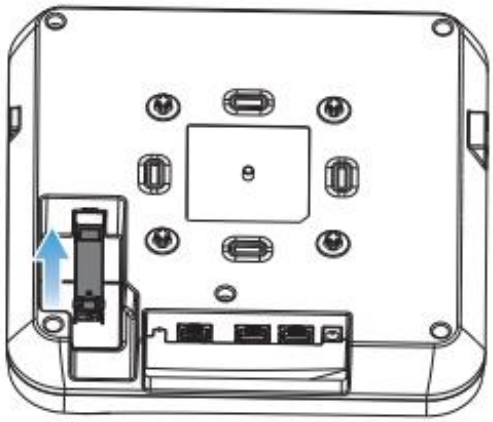
⚠ Caution

Install the Ethernet cables before mounting the AP on the bracket.

3.5.2 Installing the SFP Module

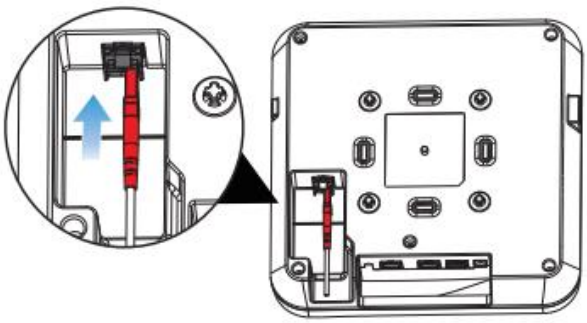
(1) Insert the SFP module.

Figure 3-9 Inserting the SFP Module



(2) Connect the fiber.

Figure 3-10 Connecting the Fiber



3.6 Connecting Cables

Connect UTP/STP to the LAN/PoE port on the AP. See Connectors_and_Media for supported wiring of twisted pairs.

⚠ Caution

By default, baud rate is set to 9600, data bit 8, parity none, stop bits 1 and flow control none on the Console port of the AP. The console port is used only when you want to configure the AP manually.

3.7 Bundling Cables

3.7.1 Precautions

- Make sure the cable bundles are neat and orderly.
- Bend twisted pairs naturally or to a large radius close to the connector.
- Do not over tighten cable bundle as it may reduce the cable life and performance.

3.7.2 Bundling Steps

- Bundle the drop UTP/STP cables and route them to the LAN/PoE port.
- Attach the cables in the cable tray of the rack.
- Extend the cables under the AP and run in straight line.

3.8 Checking after Installation

3.8.1 Checking the Access Point

- Make sure the external power supply matches with the AP.
- Make sure the device is completely fixed and does not move.

3.8.2 Checking Cable Connection

- Make sure the UTP/STP cable matches the interface type.
- Make sure cables are properly bundled.

3.8.3 Checking Power Supply

- Make sure all power ports are properly connected and compliant with safety requirement.
- Make sure the AP is operational after power-on.

4 Verifying Operating Status

4.1 Configuring the Environment

Use a power adapter or PoE to power the AP.

Setting up the Environment

- Verify that the AP is properly connected to the power source.
- Connect the AP to an AC through a twisted pair cable.
- When the AP is connected to a PC, verify that the PC and PoE switch are properly grounded.

4.2 Powering up the AP

4.2.1 Checking Environment before Power-on

- Verify that the power supply is properly connected.
- Verify that the input voltage matches the specification of the AP.

4.2.2 Checking Environment after Power-on

After power-on, you are advised to check the following to ensure normal operation of the AP.

- Check if any message is printed on the Web-based configuration interface of the device.
- Check if the LED works normally.

5 Monitoring and Maintenance

5.1 Monitoring

5.1.1 LED

You can observe the LED to monitor the AP in operation.

5.1.2 CLI Commands

You can run related commands on the command line interface (CLI) of the device to remotely monitor the configurations and status of the AP.

Note

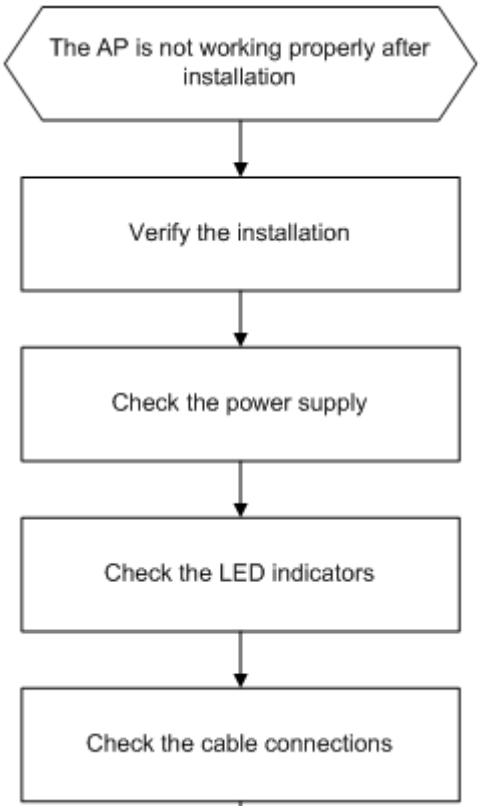
You can log in to the AP via Telnet and use monitoring related commands to maintain the AP.

5.2 Remote Maintenance

- If the AP operates as a Fat AP, you can log in to the AP remotely for maintenance.
- If the AP operates as a Fit AP, you can use AC to centrally manage and maintain the AP.

6 Troubleshooting

6.1 Troubleshooting Flowchart



6.2 Common Faults

6.2.1 Ethernet port is not working after the Ethernet cable is plugged in

Verify that the device at the other end of the Ethernet cable is working properly. And then verify that the Ethernet cable is capable of providing the required data rate and is properly connected.

6.2.2 LED is off for a long time

- If you use PoE power supply, verify that the power source is IEEE 802.11af compliant, and then verify that the cable is connected properly.
- If you use a power adapter, verify that the power adapter is connected to an active power outlet, and then verify that the power adapter works properly.

6.2.3 LED stays solid red for a long time

The LED stays solid red for a long time, indicating the Ethernet port is not connected. Verify the Ethernet connection.

6.2.4 LED stays solid green for a long time

The AP performs initialization after power on. During this period, the LED stays solid green and does not turn blue until the initialization is completed. **Note**: If the solid green persists for an hour, it indicates the device initialization fails, and the device is faulty.

6.2.5 LED stays fast blinking blue for a long time (Fit AP mode)

Sometimes the AP performs firmware upgrade after power on. During this period, the LED stays fast blinking blue and does not turn solid until the upgrade is completed. **Note**: Do not plug or unplug the power cord when the Status LED is blinking as firmware update takes time. If the blinking persists for ten minutes, it indicates the device fails to complete firmware upgrade and is faulty.

6.2.6 LED does not turn solid blue or blinking blue

After the system is booted and the LED does not turn solid blue or blinking blue, this may be because the AP has not established a proper CAPWAP connection with the AC. Verify that the AC is functioning and configured properly.

6.2.7 Client cannot find wireless network

(1) Verify that the device is properly powered.

(2) Verify that the Ethernet port is correctly connected.

(3) Verify that the AP is correctly configured.

(4) Adjust the distance between the client and the AP by moving the client device closer to the AP.

7 Appendix

7.1 Connectors and Media

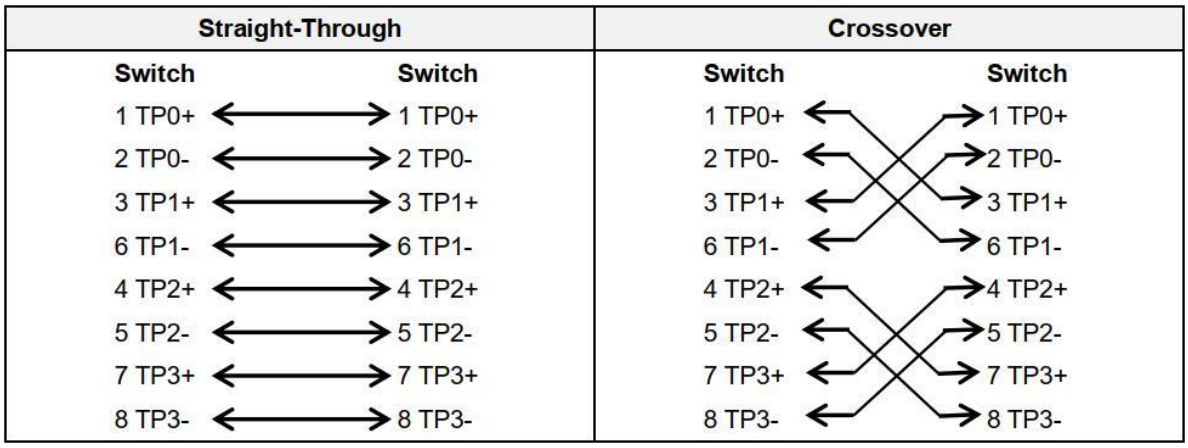
1000BASE-T/100BASE-TX/10BASE-T

The 1000BASE-T/100BASE-TX/10BASE-T is a 10/100/1000 Mbps auto-negotiation port that supports auto MDI/MDIX.

Compliant with IEEE 802.3ab, 1000BASE-T requires Category 5e 100-ohm UTP or STP (STP is recommended) with a maximum distance of 100 meters (328 feet).

1000BASE-T requires all four pairs of wires be connected for data transmission, as shown in **Figure 7-1**.

Figure 7-1 1000BASE-T Connection



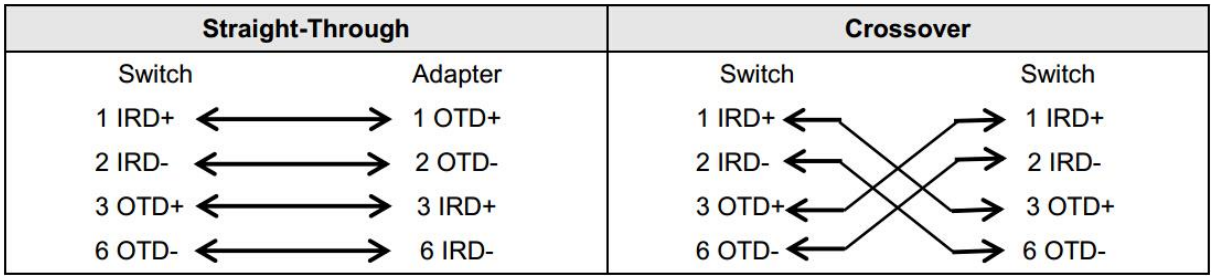
10BASE-T uses Category 3, 4, 5 100-ohm UTP/STP and 1000BASE-T uses Category 5 100-ohm UTP/STP for connections. Both support a maximum length of 100 meters. **Figure 7-2** shows 100BASE-TX/10BASE-T pin assignments.

Figure 7-2 100BASE-TX/10BASE-T Pin Assignments

Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-
4,5,7,8	Not used	Not used

Figure 7-3 shows wiring of straight-through and crossover cables for 100BASE-TX/10BASE-T.

Figure 7-3 100BASE-TX/10BASE-T Connection



7.2 Mini-GBIC Modules

Use appropriate SFP (Mini-GBIC) modules according to the port types. You can select the module to suit your specific needs. The following models and technical specifications of some SFP modules are listed for your reference.

Table 7-1 Models and Technical Specifications of the SFP Module

Wavelength (nm)	Media Type	Support DDM (Yes/No)	Intensity of Transmitted Light (dBm)		Intensity of Received Light (dBm)	
			min	max	min	max
1310Tx/1550Rx	Single-mode fiber	No	-9	-3	-	-18

Table 7-2 Cabling Specifications of the SFP Module

Port	Media Type	Core Size (μm)	Cabling Distance
LC	Single-mode fiber	9/125	0.3 km

⚠ Caution

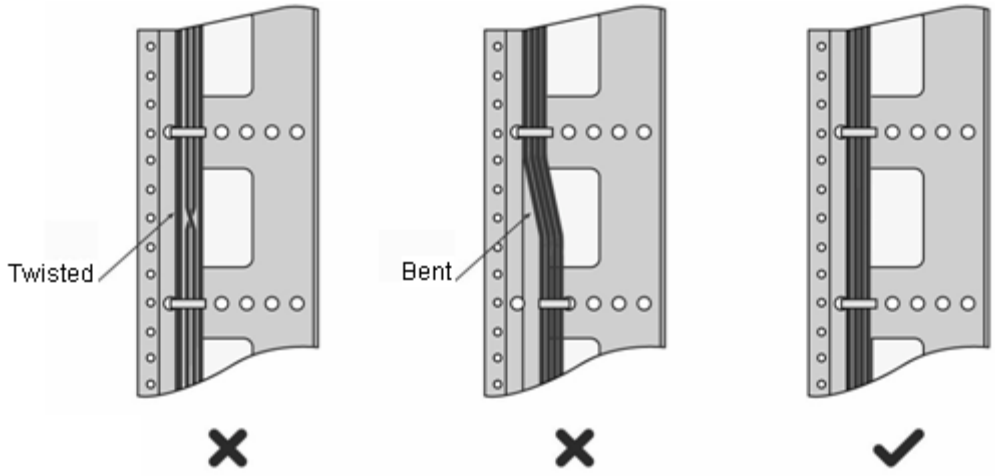
- For the fiber module with transmission distance exceeding 40 km and more, one on-line optical attenuator should be added on the link to avoid the overload of the optical receiver when short single-mode optical fibers are used.
- Fiber modules generate laser. Do not stare at light source.
- To keep fiber modules clean, please use dust caps when the modules are not connected with fibers.

7.3 Cabling Recommendations

During installation, route cable bundles upward or downward along the sides of the rack depending on the actual situation in the equipment room. All cable connectors should be placed at the bottom of the cabinet rather than be exposed outside of the cabinet. Power cords should be routed upward or downward beside the cabinet close to the location of the DC power distribution cabinet, AC power outlet, or lightning protection box.

- Required Minimum Cable Bend Radius
  - The minimum bend radius of a power, communication or flat cable should be 5 times the overall diameter of the cable. If the cable is constantly bent, plugged or unplugged, the bend radius should be 7 times the overall diameter.
  - The minimum bend radius of a coaxial cable should be 7 times the overall diameter of the cable. If the cable is constantly bent, plugged or unplugged, the bend radius should be 10 times the overall diameter.
  - The minimum bend radius of a high-speed cable, such as an SFP cable should be 5 times the overall diameter of the cable. If the cable is constantly bent, plugged or unplugged, the bend radius should be 10 times the overall diameter.
- Precautions for Cable Bundling
  - Before bundling cables, correctly mark labels and stick the labels to cables where appropriate.
  - Cables should be neatly and properly bundled, as shown in **Figure 7-4**.

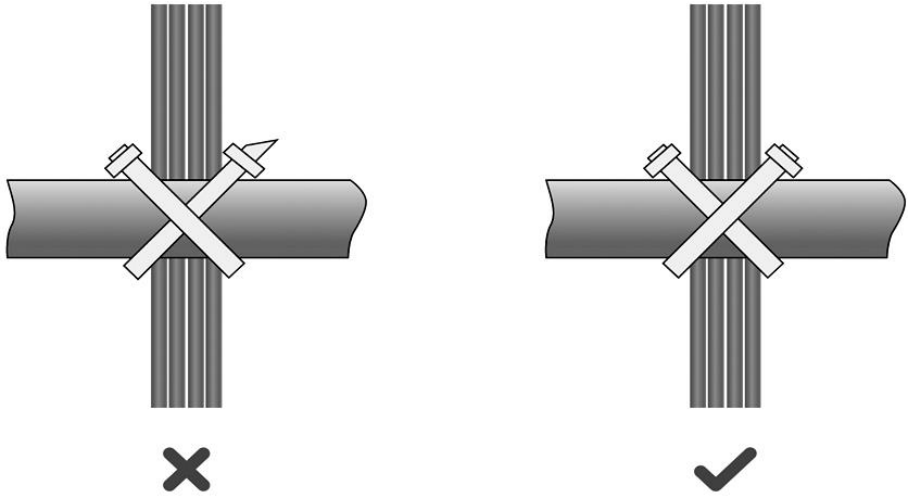
Figure 7-4 Bundling Cables



  - Route and bundle power, signal, ground cables separately. When the cables are close to each other, cross them. When power cords run parallel to signal cables, the distance between them must be greater than 30 mm.
  - All cable trays and their accessories shall be smooth and free from sharp edges.
  - Holes in metal, through which cables pass shall have smooth, well-rounded surfaces or be protected with insulating bushings.
  - Use proper cable ties to bind cables together. Do not tie two or more cable ties to bind cables.

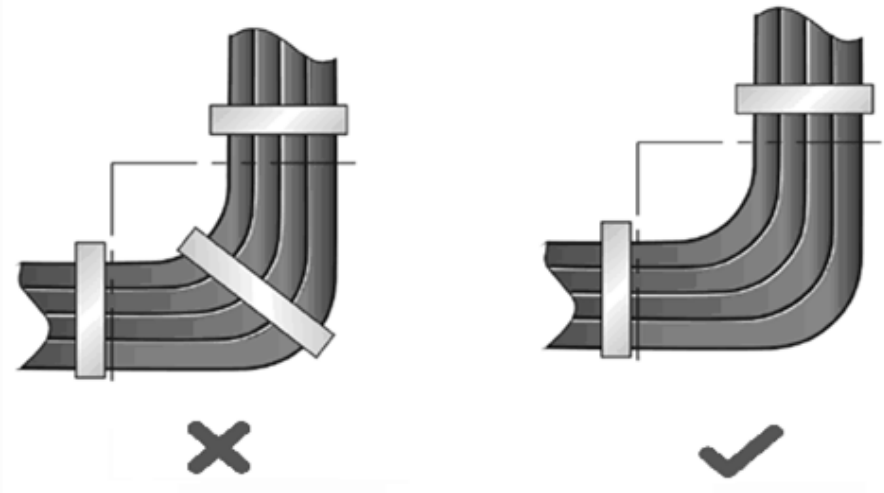
- Cut off excess cable tie cleanly with no sharp edges after bundling cables, as shown in **Figure 7-5**.

Figure 7-5 Cutting off Excess Cable Tie



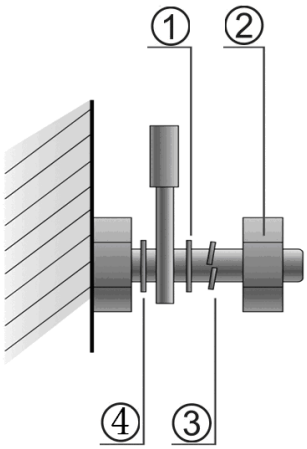
- If cables are to be bent, bind them first but do not tie cable ties within the bend to avoid stress on the cables, which may otherwise cause the wires inside to break, as shown in **Figure 7-6**.

Figure 7-6 Do Not Tie Cable Ties within the Bend



- Wrap up unnecessary or excess cables and bind them to the appropriate rack position, where device operation is not affected, and no damages occur to the device and cables during debugging.
- Do not bind power cords to the rails for moving parts.
- Leave a certain length of the cable connecting moving parts, such as the ground wire of the cabinet door, to avoid stress on the cable; when moving parts are in place, ensure the excess cable length shall not contact heat sources, sharp corners or edges. If heat sources are unavoidable, use high-temperature cables instead.
- When using screws to fasten cable lugs, the bolts or nuts shall be tightened and prevented from loosening, as shown in **Figure 7-7**.

Figure 7-7 Fastening Cable Lugs



Note	1. Flat washer	3. Spring washer
	2. Nut	4. Flat washer

- When using a stiff cable, fix it near the cable lug to avoid stress on the lug and cable.
- Do not use self-tapping screws to fasten terminals.
- Bundle cables of the same type and running in the same direction into groups. Keep cables clean and straight.
- Cables shall be tied according to the following table.

Diameter of Cable Bundle (mm)	Space between Bundles (mm)
10	80 to 150
10 to 30	150 to 200
30	200 to 300

- Do not tie knots for cables or cable bundles.
- The metal parts of the cold-pressed terminal blocks, such as air circuit breakers, shall not be exposed outside of the blocks.

7.4 Power Supply

- DC power adapter:

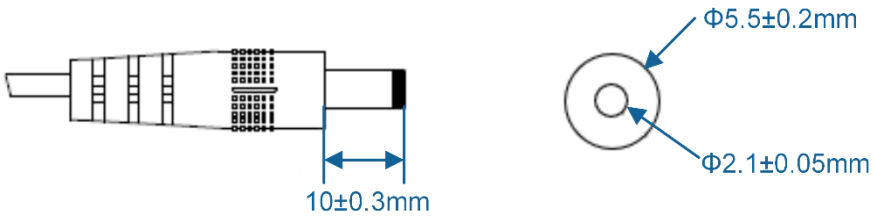
Input voltage: 48 V

Rated current: 0.6 A

Table 7-3 Technical Specifications of the DC Power Connector

Inner Diameter	Outer Diameter	Depth	Polarity
2.1 mm (0.08 in.)	5.5 mm (0.25 in.)	10 mm (0.39 in.)	Inner pole: positive Outer pole: negative

Figure 7-8 Size of DC Power Adapter



EKSELANS BY ITS

USER MANUAL

AX Series Access Points Web-based

ITS Partner O.B.S S.L · Av. Cerdanyola 79-81 Local C
08172 Sant Cugat del Vallés · Barcelona (Spain)
Phone:+34935839543 · info@ek.plus · www.ek.plus

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all ofthe 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 statementor 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 provides configuration information, including models, port types, and command line interfaces, for reference purposes only. In the event of any discrepancy or inconsistency between the manual and the actual version, the actual version shall take precedence.

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 access points (APs).

The web management system involves two parts: web server and web client. A web server is integrated into the device to receive and process requests from a client, and return the processing result to the client. Typically, a web client refers to a web browser, such as Internet Explorer and Google Chrome.

1.2 Connecting to the Device

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

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

Figure 1-1 Application Topology

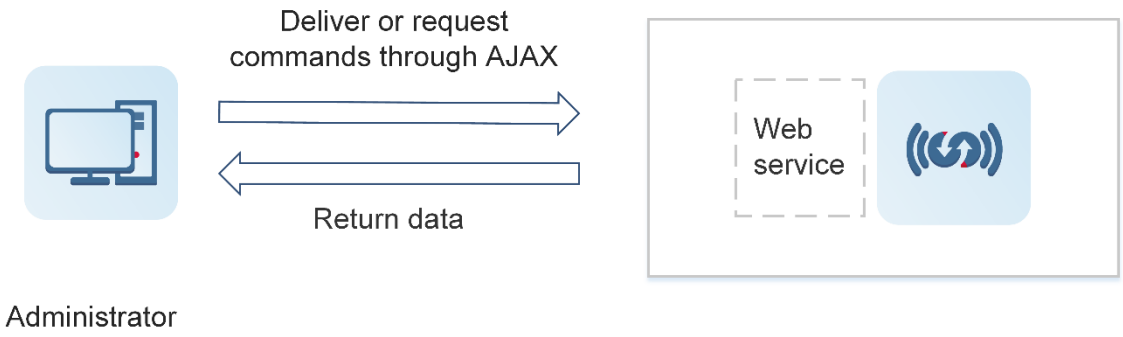
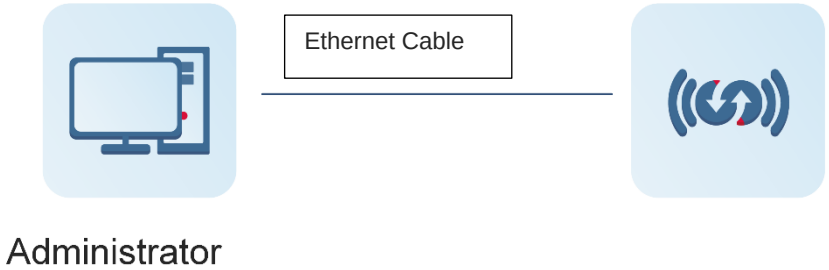


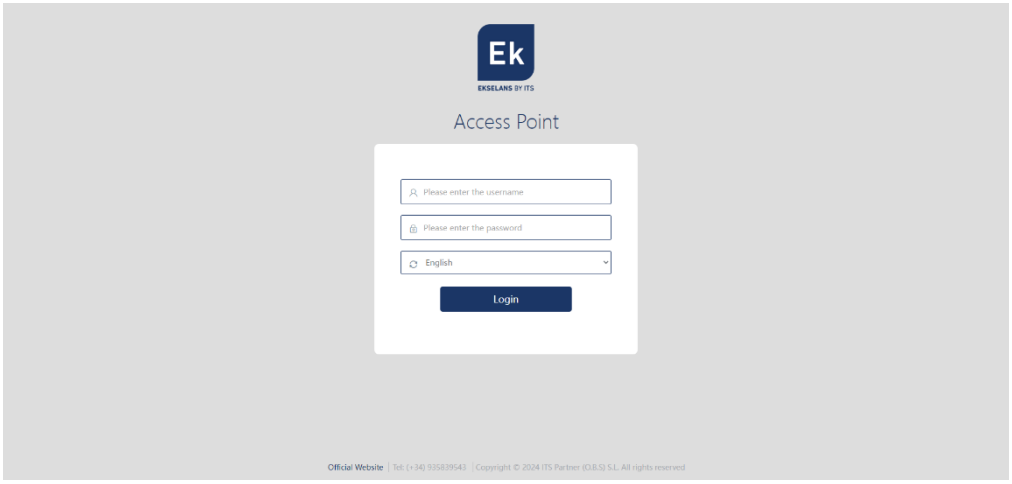
Figure 1-2 Simplified Topology



1.3 Configuration Environment for PC Clients

- An administrator logs in to the web management system to manage the device through the web browser on a client. Typically, a client refers to a PC. It may also be other mobile terminal such as a laptop or iPad. Mobile phones are not supported.
- Web browser: Google Chrome is recommended. Internet Explorer 11 and 360 Secure Browser are also supported. Exceptions such as garbled characters or format errors may occur when other browsers are used.
- Resolution: You are advised to set the resolution to 1280 pixels x 1024 pixels, 1920 pixels x 1080 pixels, or 1440 pixels x 960 pixels. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

1.4 Web Service Environment for an AP



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 all permissions.

1.5 Enabling the Web Server

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

1.5.1 Configuration Steps

Enabling the Web Service

- Mandatory.
- Enable the web service on the AP.

Configuring an IP Address

- Optional.

Configuring the Username and Password for Logging In to 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 create other accounts.

1.5.2 Verification

Log in to the web management system using the configured IP address, username, and password to check whether you can log in successfully.

1.5.3 Related Command

Enabling the Web Service

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

Configuring an IP Address

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

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

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

1.5.4 Configuration Examples

Configuring the Web Server

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 display the configuration.
	Hostname(config)#show running-config Building configuration... Current configuration : 6312 bytes ! hostname Hostname ! ! webmaster level 0 username test password test //Username and password for web management authentication http update mode auto-detect ! ! interface VLAN 1 Ip address 192.168.1.200 255.255.255.0 //Management IP address of the device no shutdown ! line con 0 line vty 0 4 login ! ! End

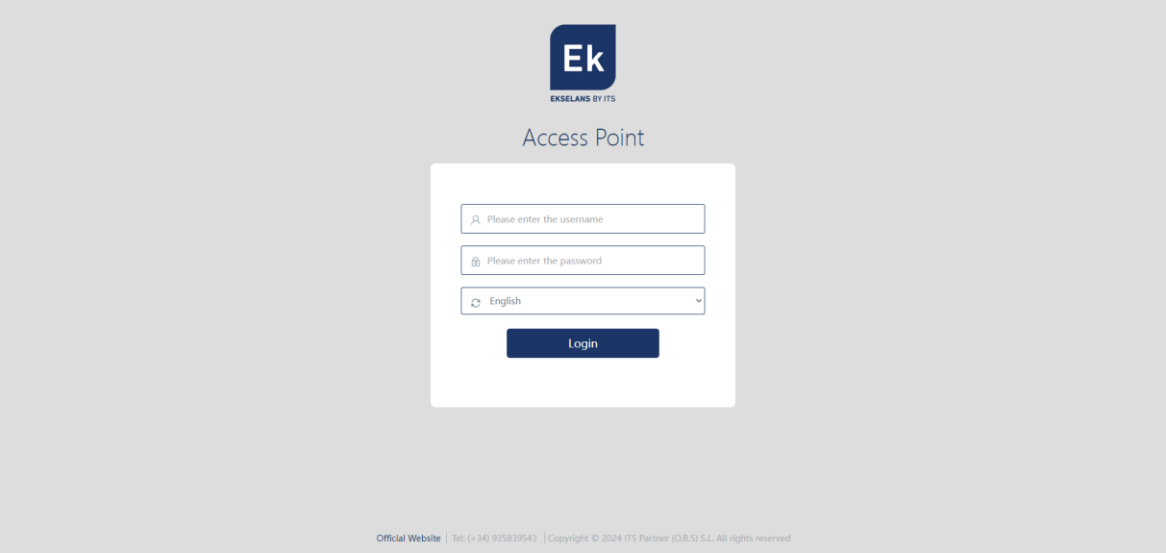
2 Quick Setup

2.1 Logging In to the Web Management System

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

Caution

If there are five consecutive failed login attempts within 10 minutes, your account will be locked for 10 minutes.



2.2 Config Wizard

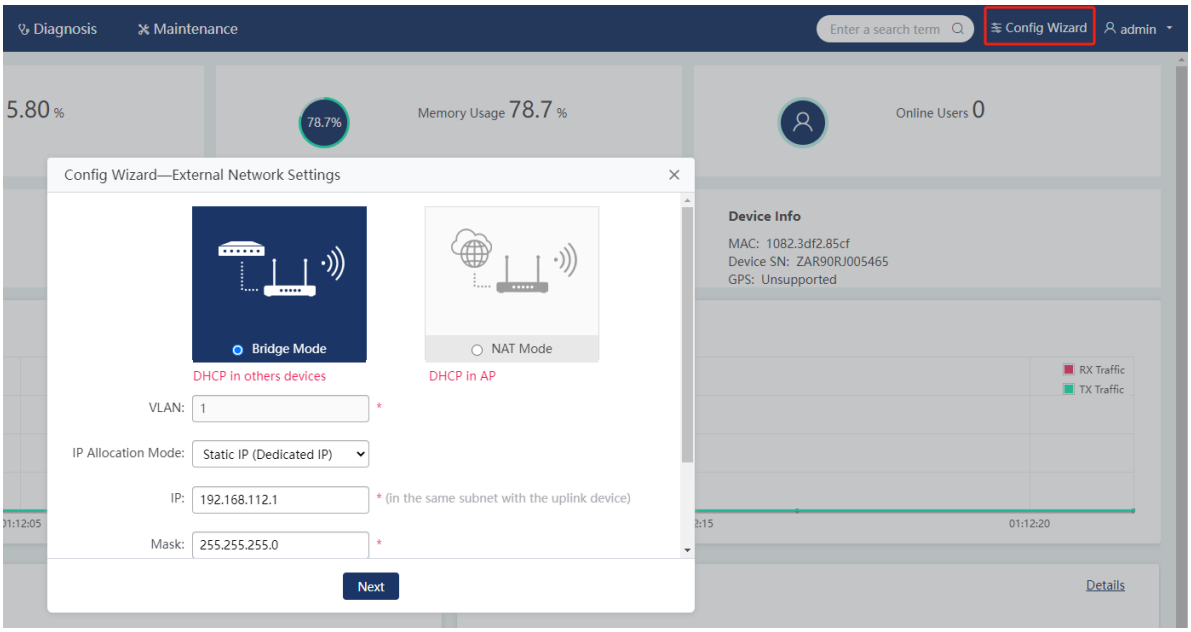
The configuration wizard provides some common scenario-based configurations. It is typically used for first setup. Click **Config Wizard** in the navigation bar.

1. When you log in to the web management system, the system will automatically identify whether the current device is configured. If not (no config.text file is found), 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 external network settings and Wi-Fi settings.

2.2.1 External Network Settings

Set the working mode of the device to **Bridge Mode** or **NAT Mode**.

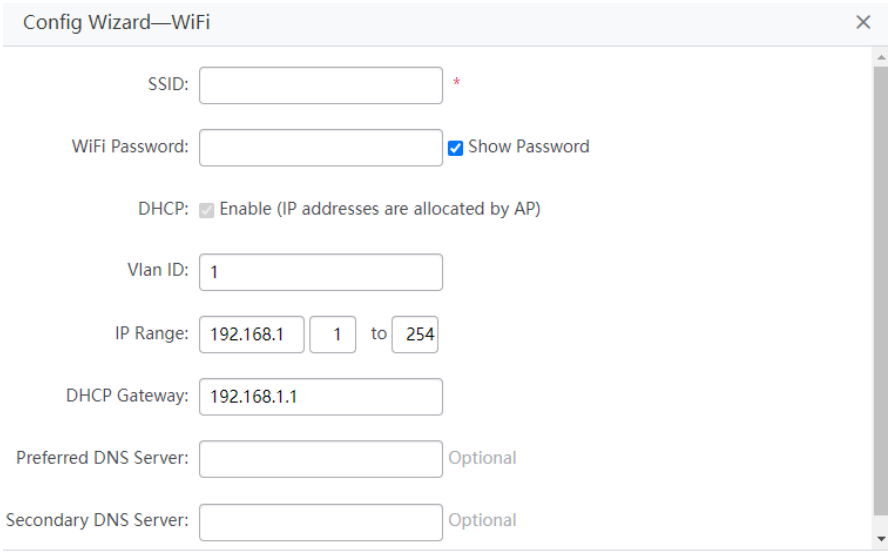


Working Mode	Parameter	Description		
Bridge Mode	**Note** In bridge mode, the gateway and DHCP server are deployed on the uplink device of the AP.			
	VLAN	Enter the VLAN for the AP to communicate with an external network.		
	IP Allocation Mode	Static IP (Dedicated IP)	IP	Enter a static IP address.
			Mask	Enter the subnet mask for the static IP address.
		DHCP (Dynamic IP)	DHCP IP	Display the obtained DHCP IP address.
	Default Gateway	(Optional) Enter the gateway address of the AP.		
NAT Mode	**Note** In NAT mode, the gateway and DHCP server are configured on the AP.			
	WAN Port	Enter the WAN port for the AP to communicate with an external network.		
	IP Allocation	Static IP	IP	Enter a static IP address.

Working Mode	Parameter	Description		
	Mode	(Dedicated IP)	IP Mask	Enter the subnet mask for the static IP address.
			Default Gateway	Enter the gateway address of the AP.
		PPPoE (ADSL Line)	Account	Enter the PPPoE username for Internet access.
			Password	Enter the PPPoE password for Internet access.
			PPPoE IP	Display the obtained PPPoE IP address.
		DHCP (Dynamic IP)	Default Gateway	(Optional) Enter the gateway address of the AP.
			DHCP IP	Display the obtained DHCP IP address.
	NAT	Enable this function when all internal IP addresses need to be translated into external IP addresses.		

2.2.2 Wi-Fi

Set the Wi-Fi parameters and click **Finish**.

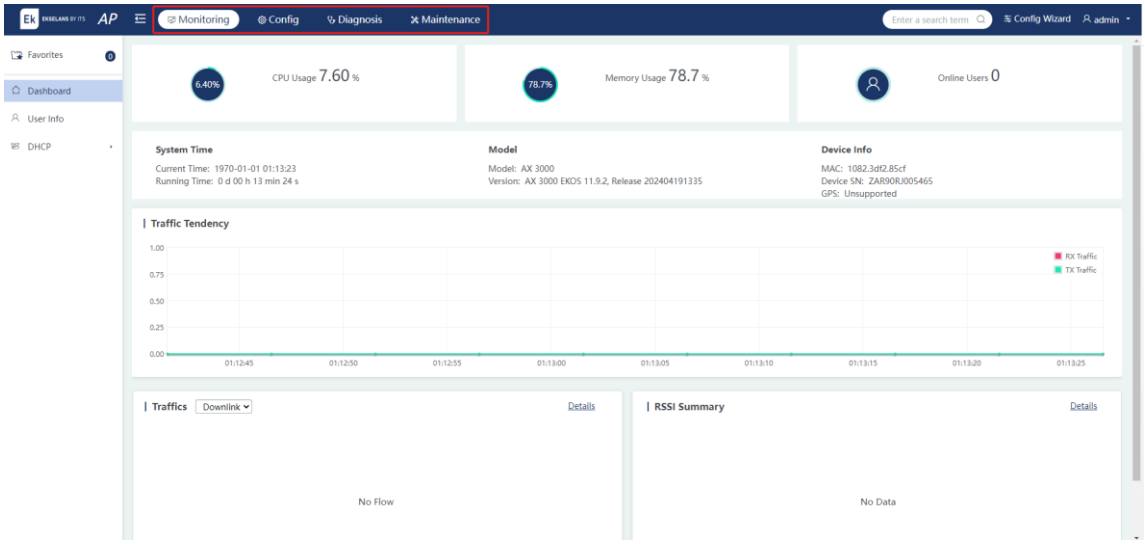


Parameter	Description
SSID	Set the Service Set Identifier (SSID), that is, Wi-Fi name.
Wi-F Password	Set the Wi-Fi password.
DHCP	After this option is selected, the DHCP service is enabled on the device.
Vlan ID	Enter the VLAN associated with the user.
IP Range	Enter the range of the address pool used by the user.
DHCP Gateway	Enter the gateway address of the address pool used by the user.
Preferred DNS Server	Enter the primary DNS server address of the address pool used by the user.
Secondary DNS Server	Enter the secondary DNS server address of the address pool used by the user.

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 in each module.



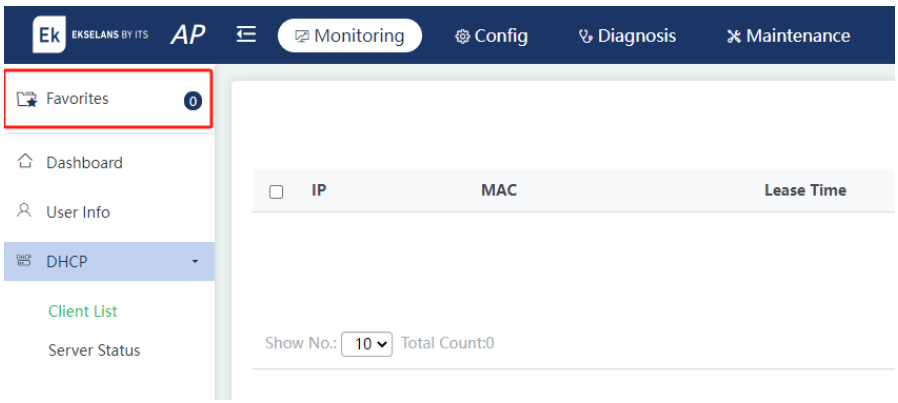
3.2 Favorites

This 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**.

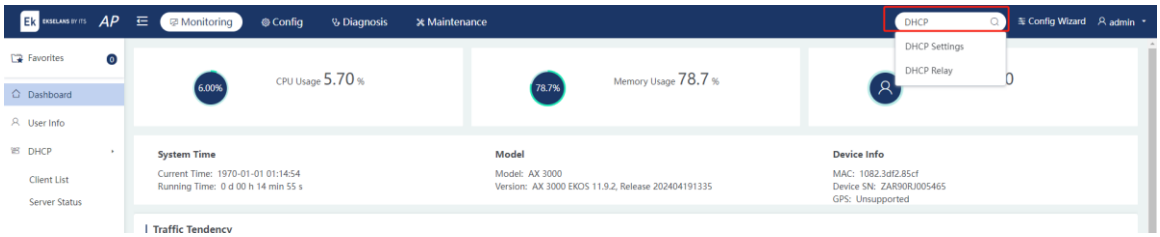
(1) Adding to Favorites: Click and drag an item form the menu to **Favorites**.



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

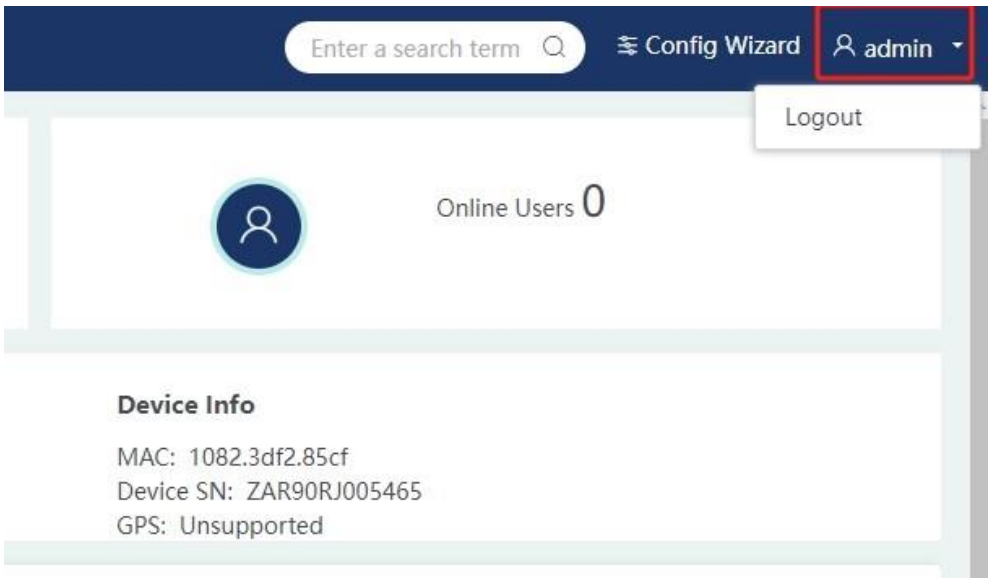
3.3 Search Bar

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



3.4 Other Functions

(1) Displaying the current account.



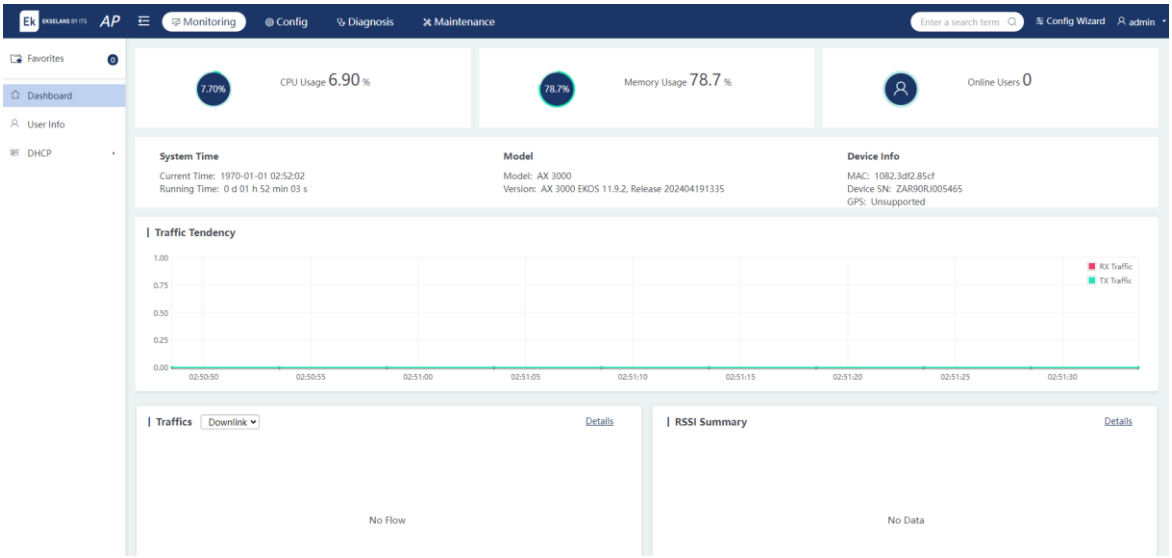
(2) Logout: Click **Logout** after expanding the account menu to log out of the web management system.

4 Monitoring

4.1 Dashboard

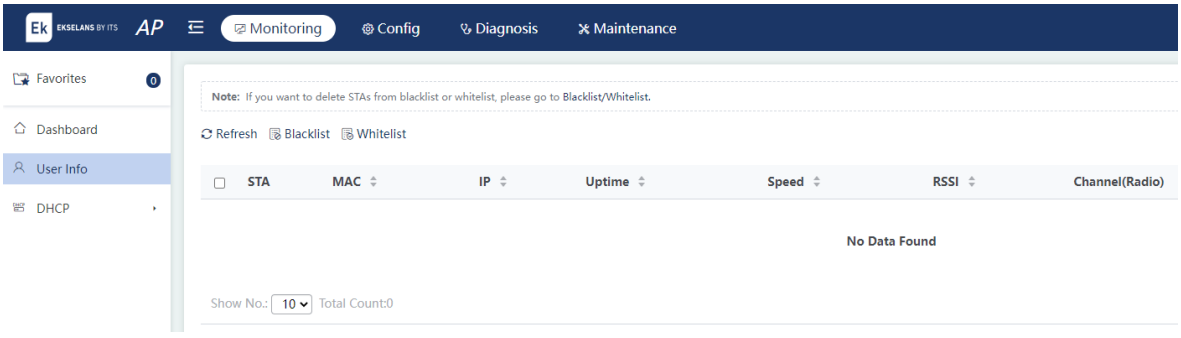
Choose **Monitoring** > **Dashboard**.

On the **Dashboard** page, you can view the basic information about the AP, including CPU usage, memory usage, number of online STAs, system time, model and version, device information, traffic tendency, user traffic, and Received Signal Strength Indicator (RSSI) summary.



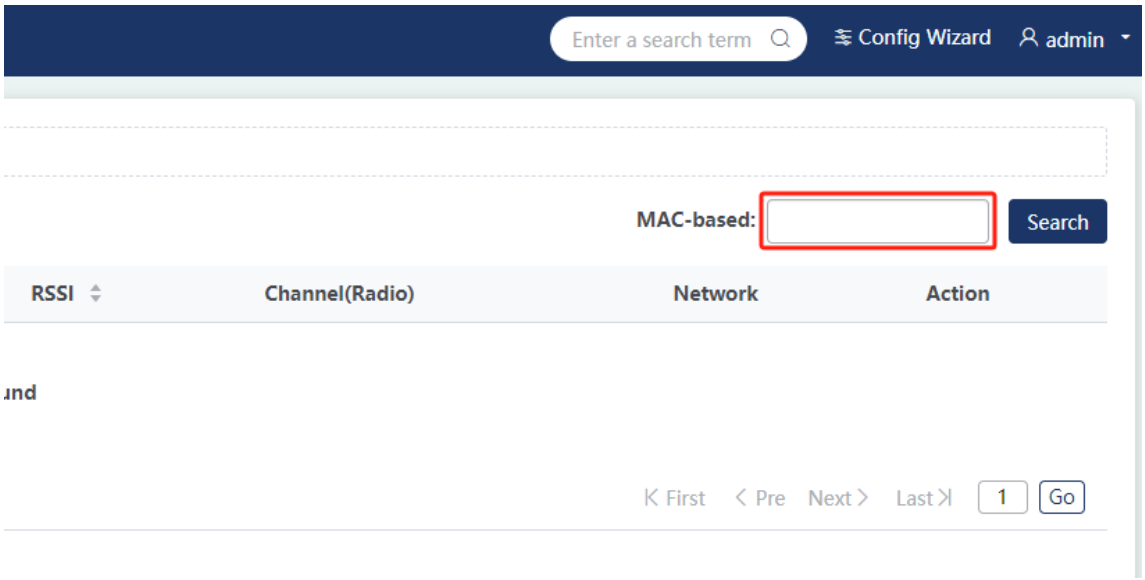
4.2 User Info

Choose **Monitoring** > **User Info**.



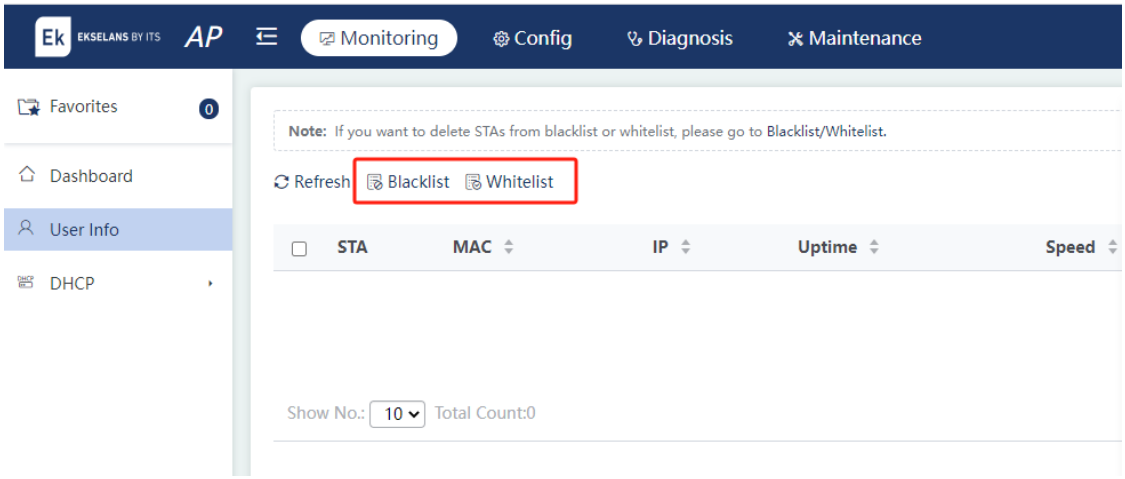
(1) Searching for STAs

If there are numerous STAs, enter a MAC address in the search box and click **Search** to search for a specific STA. To display all STA lists, clear the MAC address in the search box and click **Refresh**.



(2) Adding to the Blacklist or Whitelist

Select the STAs to be added to the blacklist or whitelist. Click **Blacklist** or **Whitelist**.

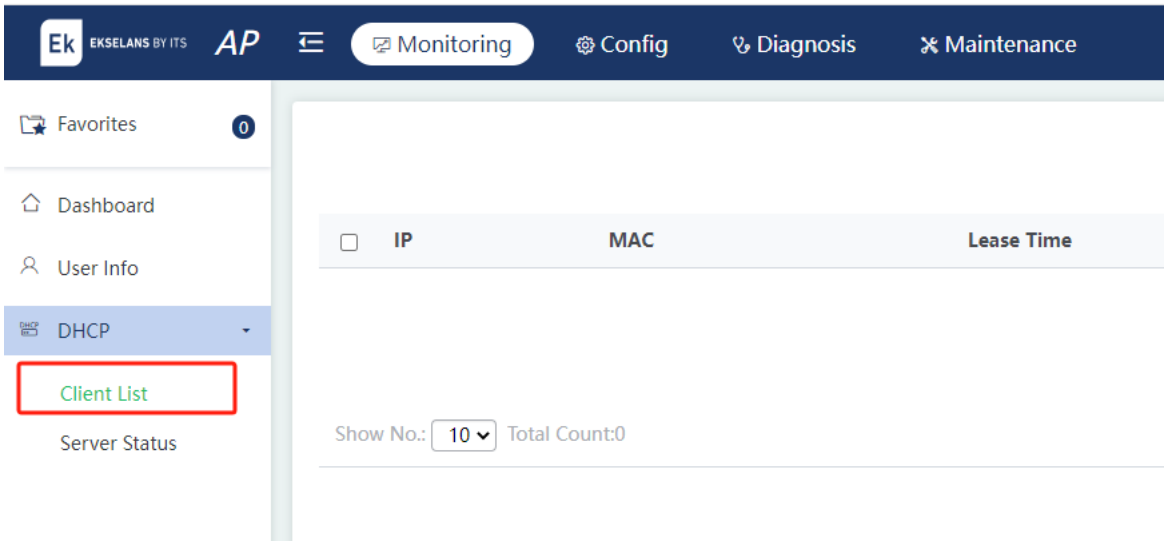


4.3 DHCP

4.3.1 Client List

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

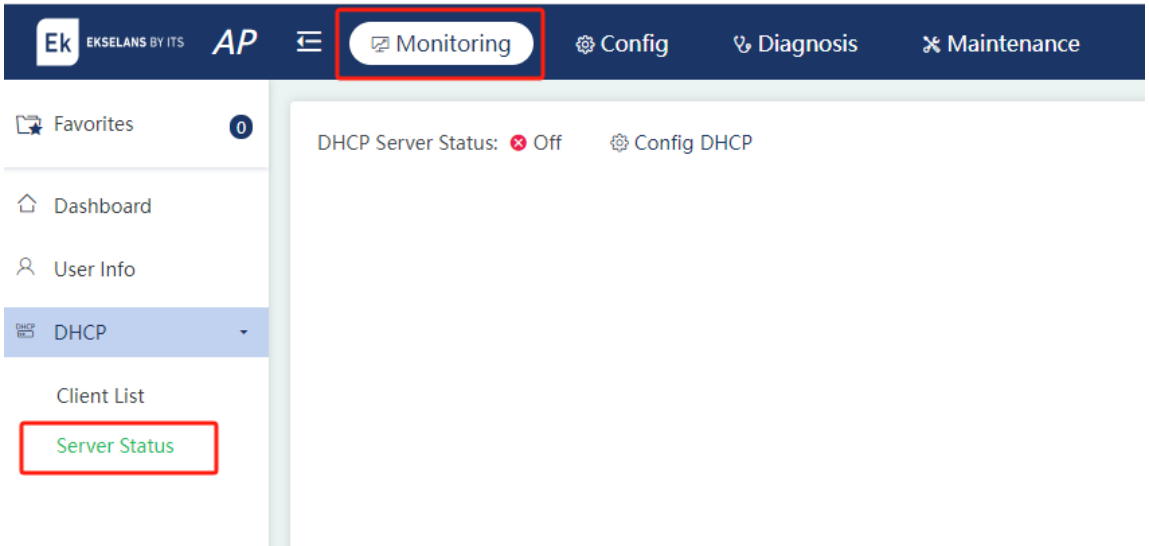
The **Client List** page displays the clients allocated with addresses from the address pool.



4.3.2 DHCP Server Status

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

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



5 Configuration

5.1 Wireless Configuration

5.1.1 Adding Wi-Fi

Choose **Config** > **Wireless** > **WiFi/WLAN**.

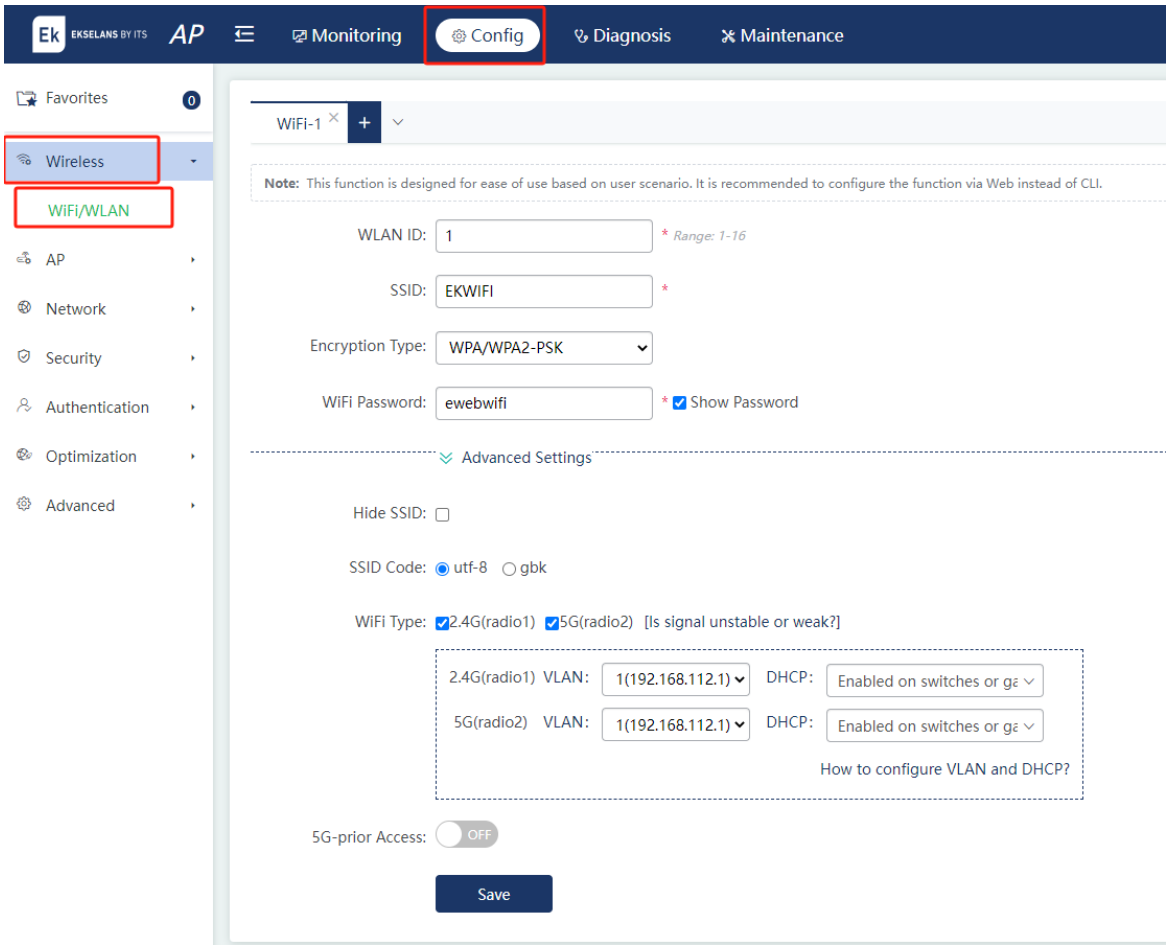
A Wi-Fi network allows wireless STAs to be associated with the AP for network access. Multiple Wi-Fi networks can be added or deleted.

Note

The maximum number of Wi-Fi networks is subject to device models.

1. Adding a Wi-Fi Network

Click **+** to add a Wi-Fi network. After the Wi-Fi parameters are set, click **Save**.



Parameter	Description
WLAN ID	Enter the WLAN ID.
SSID	Enter the Wi-Fi name.
Encryption Type	**Open**: No encryption type is configured. No password is required when a STA associates with the Wi-Fi network. **WPA/WPA2-PSK**: WPA mode with a pre-shared key featuring high security and easy setup, applicable to homes and small-sized enterprises. **WPA/WPA2-802.1X**: WPA or WPA2 mode that uses a RADIUS server for authentication and key acquisition. Ordinary users are not advised to adopt this mode as it requires an exclusive authentication server. **WPA2-802.1X**: WPA2 mode that uses a RADIUS server for authentication and key acquisition. **WPA3-PERSONAL**: Compared with WPA2, it is more secure and can effectively prevent dictionary attacks. **WPA3-ENTERPRISE-GCMP256**: WPA3-Enterprise is configured with GCMP-256 encryption, providing additional protection for networks where sensitive data is transmitted. It is applicable to data-sensitive networks like government or financial systems. **WPA3-ENTERPRISE-CCMP128**: WPA3-Enterprise is configured with CCMP-128 encryption, providing additional protection for networks where sensitive data is transmitted. It is applicable to data-sensitive networks like government or financial systems. **WPA2/WPA3**: WPA2/WPA3 transition mode, which is determined by a STA.
WiFi Password	Enter the Wi-Fi password.
Hide SSID	If you enable **Hide SSID**, the SSID is not displayed in the Wi-Fi list of a STA. You can only manually search for the SSID.
SSID Code	**UTF-8**: You are advised to select **utf-8**, as most STAs support UTF-8 encoding by default. **GBK**: Some STAs, PCs, and network interface cards (NICs) support GBK encoding. You can specify the encoding mode as required.

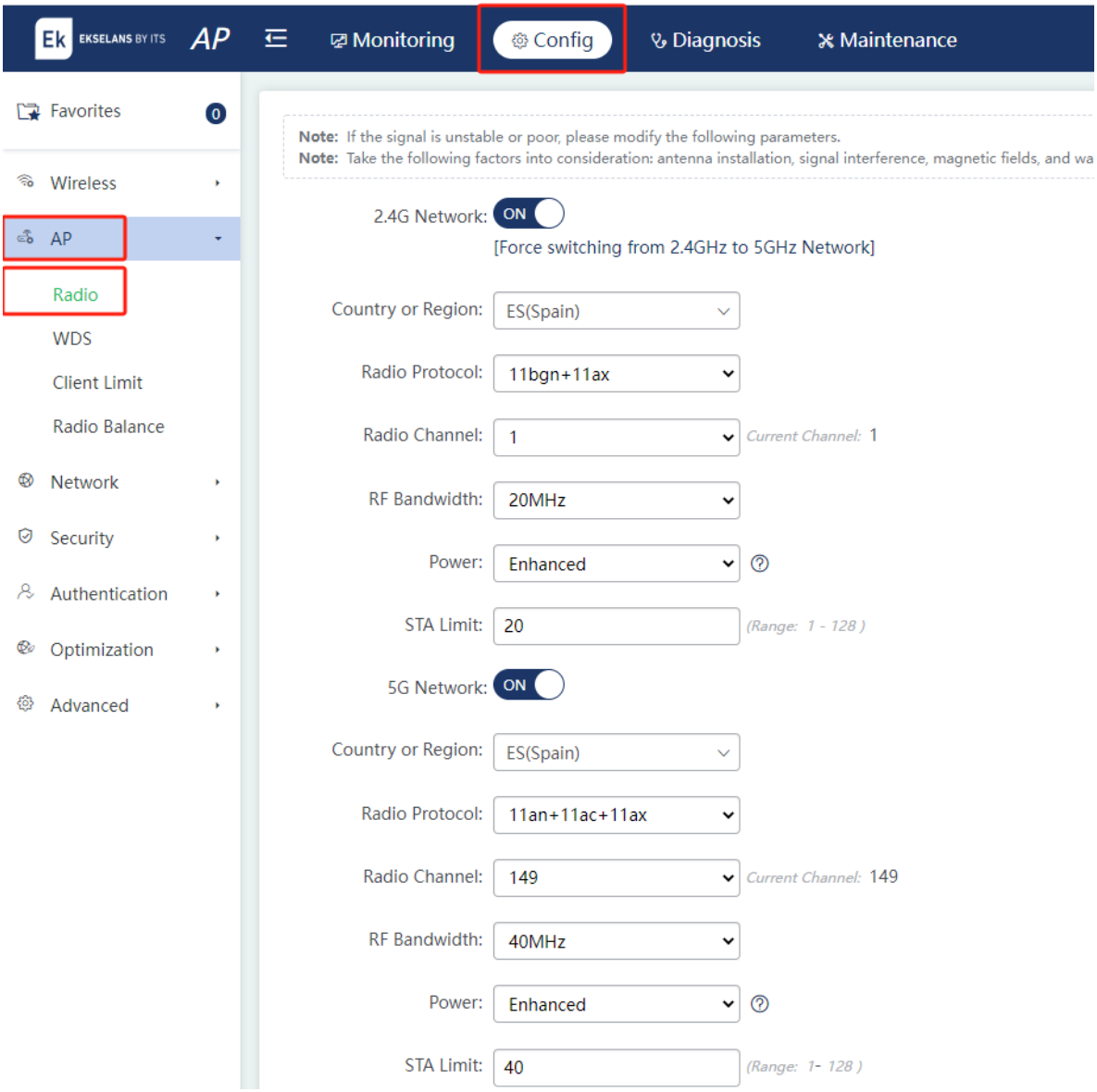
Parameter	Description
WiFi Type	Specify the network types supported by the Wi-Fi network. You can select multiple network types. **Note** ● Click **Is signal unstable or weak?** to go to the **Radio** page, where you can configure a radio. ● Click **VLAN** to add a VLAN on the **VLAN** page. VLAN determines whether the AP can communicate with the uplink switch or egress device, and whether STAs connected to the Wi-Fi network of the AP can access the Internet. The IP address of the VLAN can be used as the management address of the AP. ● Click **DHCP** to go to the **DHCP Settings** page. On this page, you can add a DHCP address pool for the AP to assign IP addresses to STAs connected to the AP (it is required when the AP works in NAT mode). If the AP works in bridge mode, you do not need to configure DHCP because the DHCP service is configured on the uplink switch or egress. In this case, the AP only plays a wireless role and does not function as a gateway or allocate IP addresses.
Rate Limit	If you do not set a rate limit, the rate is not limited by default. To set the maximum upload and download rates, click **Rate Limit Settings**.
5G-prior Access	If this function is enabled, STAs will preferentially access the 5 GHz radio. It is disabled by default.

5.2 AP

5.2.1 Radio

Choose **Config** > **AP** > **Radio**.

If the signal is unstable or the signal strength is low, you can manually modify the radio parameters to adjust the signal strength of the Wi-Fi broadcast by the device.



Parameter	Description
Wireless Interface	Radio of the device. If the device supports dual radios, that is, **dot11radio 1/0** and **dot11radio 2/0**, the **Wireless Interface** field is not displayed. If the device supports three radios, that is, **dot11radio 1/0**, **dot11radio 2/0**, and **dot11radio 3/0**, the **Wireless Interface** field will be displayed.
2.4G Network 5G Network	Enable or disable the 2.4 GHz or 5 GHz radio.
Country or Region	Select the country or region code configured for the radio.
Radio Protocol	Select 802.11 protocols configured for the radio.

Parameter	Description
	● The protocol options available on the 2.4 GHz radio include: o **11bgn** indicates 802.11b, 802.11g, and 802.11n protocols. o **11bgn+11ax** indicates 802.11b, 802.11g, 802.11n, and 802.11ax protocols. ● The protocol options available on the 5 GHz radio include: o **11an** indicates 802.11a and 802.11n protocols. o **11an+11ac** indicates 802.11a, 802.11n, and 802.11ac protocols. o **11an+11ac+11ax** indicates 802.11a, 802.11n, 802.11ac, and 802.11ax protocols.
Radio Channel	Select the channel configured for the radio.
RF Bandwidth	Select the channel width configured for the radio.
Power	Select the power for the radio. ● Power Saving: 30 dBm. ● Standard: 80 dBm. ● Enhanced: 100 dBm. ● Custom: You can set the power for the radio.
STA Limit	Enter the maximum number of STAs associated with the radio. **Note** The maximum number of STAs supported varies with the device model. The actual range displayed on the page shall prevail.

5.2.2 WDS

Note

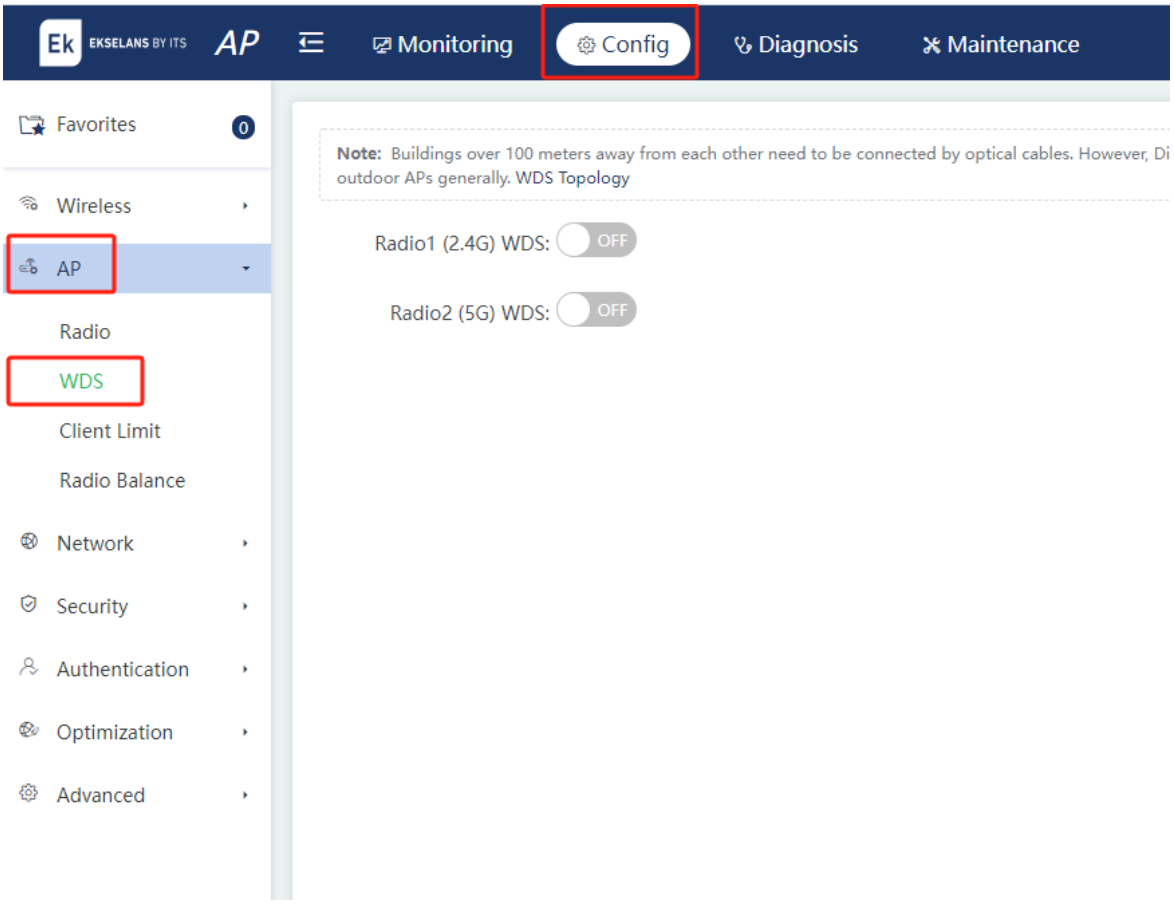
Some APs may not support this function. The actual menu shall prevail.

Choose **Config** > **AP** > **WDS**.

If the distance between buildings is more than 100 meters (328.08 feet), optical cables need to be deployed. For some buildings that have been built, digging roads or installing overhead lines will cause high construction difficulty and cost, such as between the high-rise buildings, or between two buildings separated by a river. In this case, Wireless Distribution System (WDS) is used to implement network interconnection, enabling cost-effective and effort-saving deployment. Multiple APs are interconnected through WDS or wireless bridge/repeater mode to connect to distributed networks and extend wireless signals. An AP can function as a repeater to extend the

range of the front-end network and the Wi-Fi signals, allowing users at a great distance to connect to the network. WDS supports bridging on the 2.4 GHz and 5 GHz radios.

Enable the bridging function on the 2.4 GHz or 5 GHz radio as required. Select the operating mode and configure the parameters. Click **Save**.



Operating Mode	Parameter	Description
Root Bridge	Root Bridge Network	Select the network where wireless signals need to be extended.
	Distance	Enter the distance between two wireless bridge devices (root bridge and non-root bridge).
Non-root Bridge	Root-bridge Election	Elect the root bridge based on the MAC address or SSID.
	Root Bridge MAC	Enter the MAC address of the root bridge.
	Bridge WiFi Password	Set the password of the root bridge Wi-Fi.

Operating Mode	Parameter	Description
	Distance	Enter the distance between two wireless bridge devices (root bridge and non-root bridge).
	Other WiFi Allowed	The radio can be used as a bridge or to broadcast Wi-Fi signals.

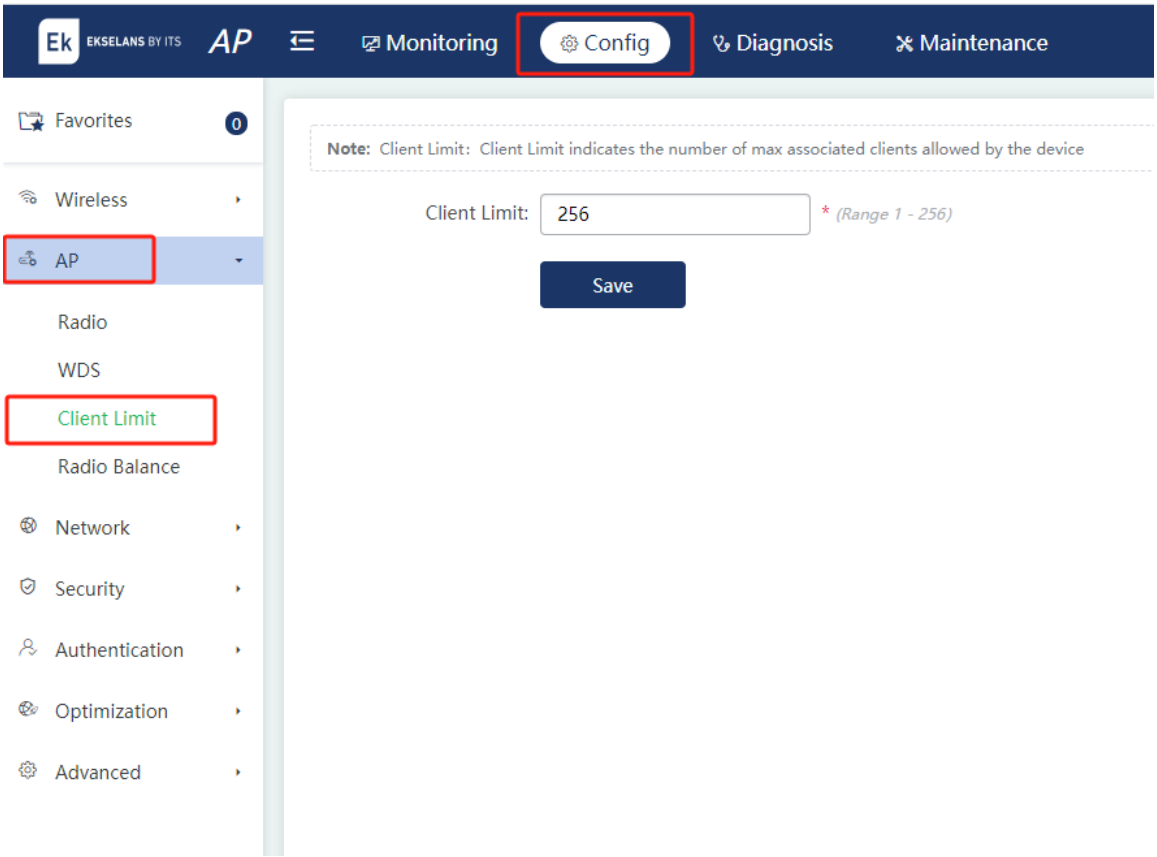
5.2.3 Client Limit

Choose **Config** > **AP** > **Client Limit**.

This function is used to configure the maximum number of clients associated with the AP.

Note

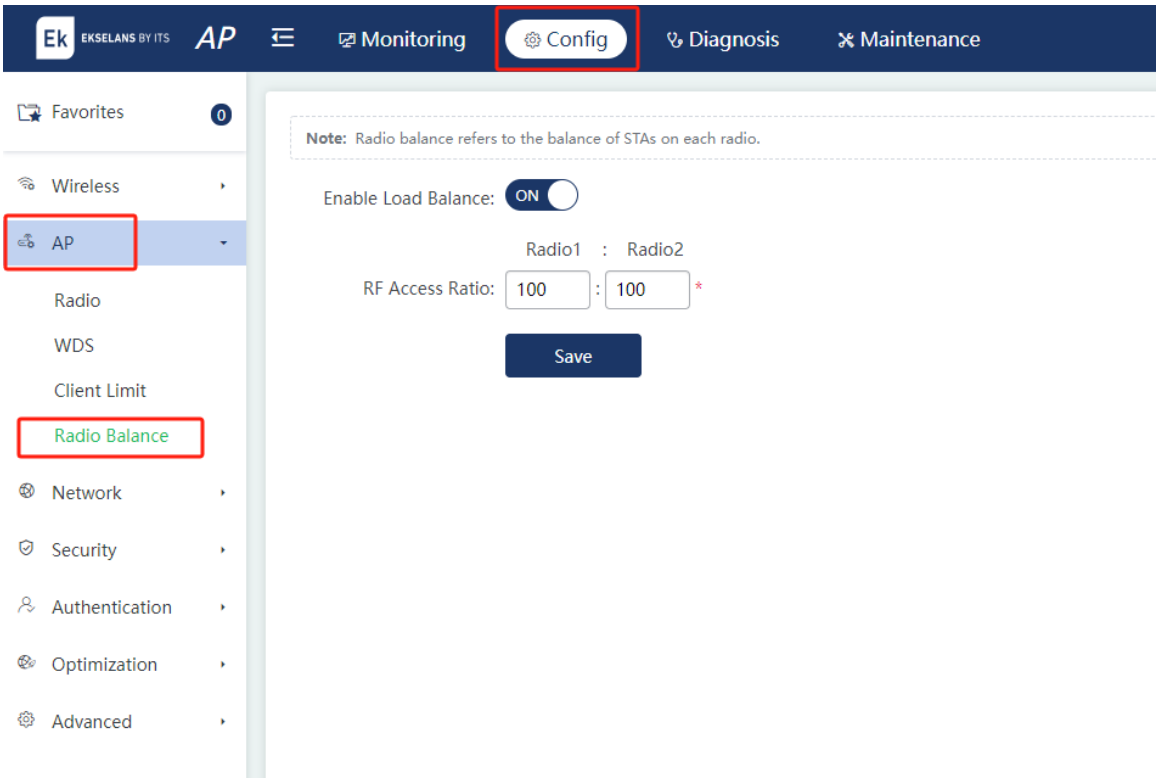
The maximum number of associated clients varies with the device model. The value displayed on the page shall prevail.



5.2.4 Radio Balance

Choose **Config** > **AP** > **Radio Balance**.

Currently, load balancing on radios is implemented only based on the number of STAs. After the load balancing function is enabled, you can set the ratio of STAs connected to different radios.



5.3 Network

5.3.1 External Network

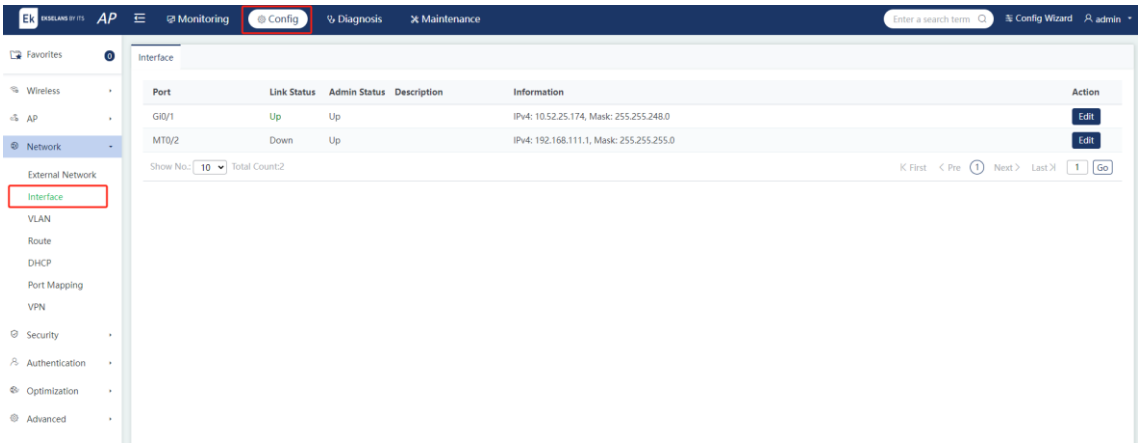
Choose **Config** > **Network** > **External Network**.

Set the working mode of the AP to **Bridge Mode** or **NAT Mode**. The settings are the same as those in the external network settings in Chapter 2. For details, see2.2.1 External Network .

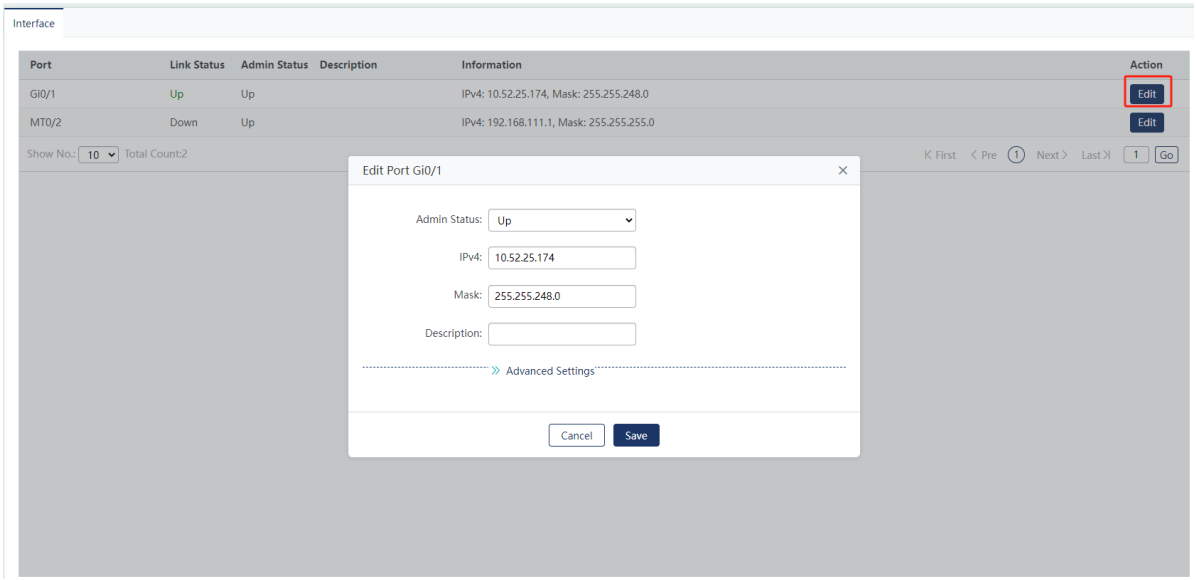
5.3.2 Interface

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

On the **Interface** page, the ports and related information are displayed.



Click **Edit** in the **Action** column to edit information about a specific port.



Parameter	Description
Admin Status	Select the management status of the port.
IPv4	Enter the IPv4 address of the port.
Mask	Enter the IPv4 subnet mask of the port.
Description	Enter the description and alias of the port.
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 port.
Speed	Configure the rate of the port.
Working Mode	Configure the working mode of the port, including auto-negotiation, duplex,

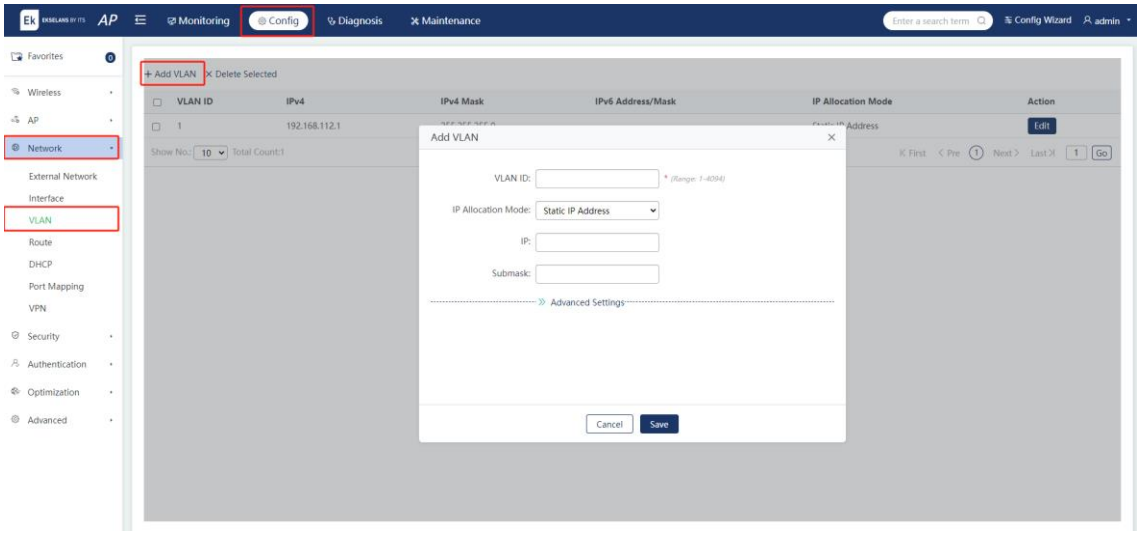
Parameter	Description
	and half-duplex.

5.3.3 VLAN

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

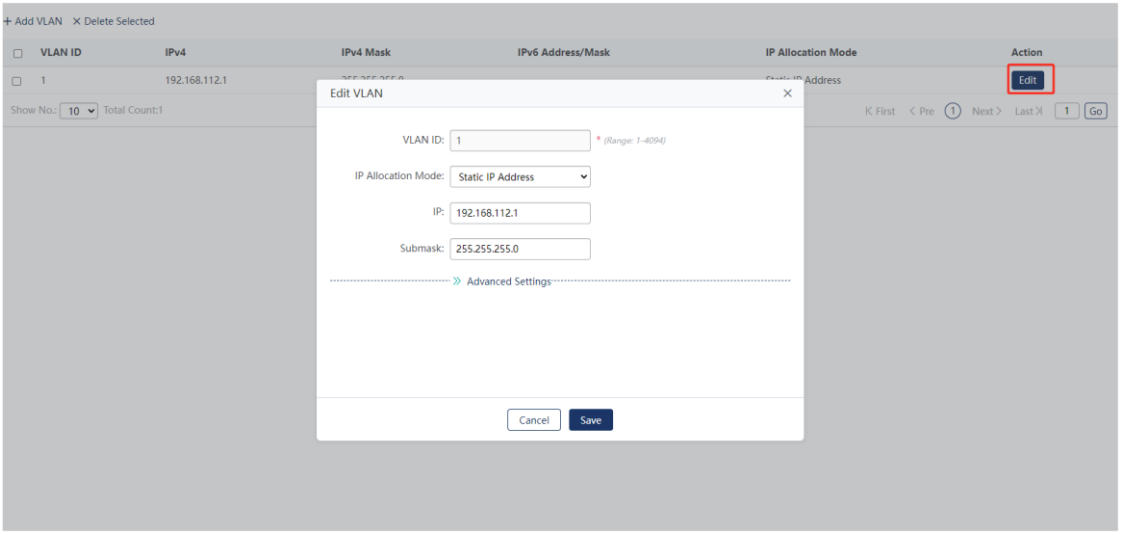
(1) Adding a VLAN

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.



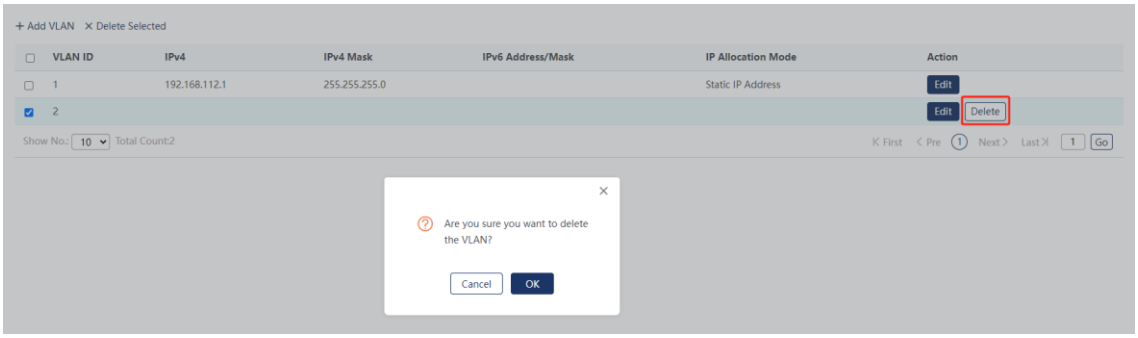
(2) Editing a VLAN

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



(3) Deleting a VLAN

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a VLAN. If multiple VLANs need to be deleted, select the target VLANs in the list. Click **Delete Selected** and a window pops up. Click **OK** to batch delete the VLANs.

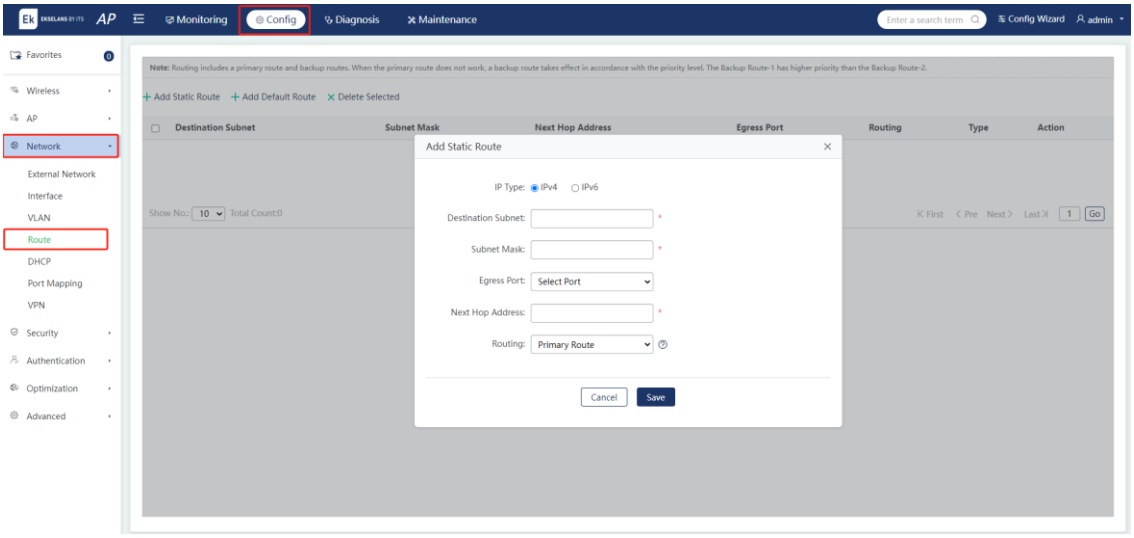


5.3.4 Route

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

(1) Adding a Static Route

Click **Add Static Route**. Edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed. The added static route will be displayed in the route list. The type is **Static Route**.

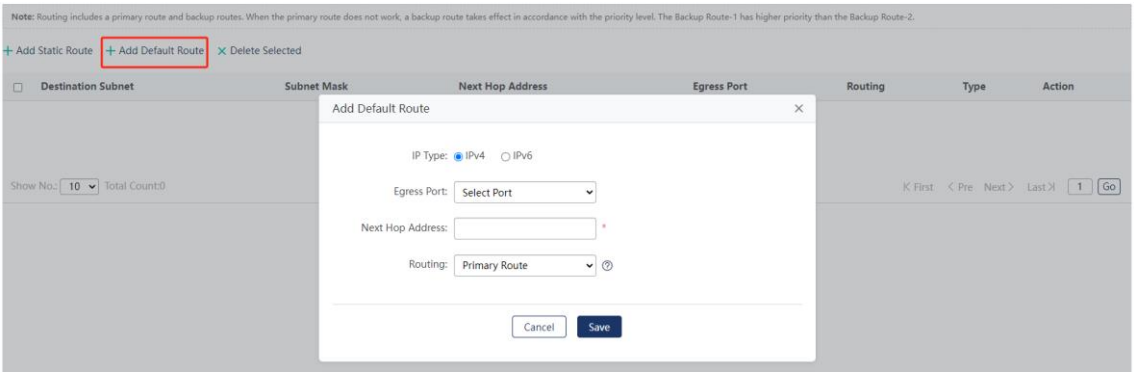


(2) Adding a Default Route

Click **Add Default Route**. Edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed. The added default route will be displayed in the route list. The type is **Default Route**.

Note

Route selection involves a primary route and backup routes. When the primary route is unavailable, for example, the interface of the primary route is inactive, 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 a Route

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

(4) Deleting a Route

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a route. To delete multiple routes, select the routes to be deleted in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the routes.

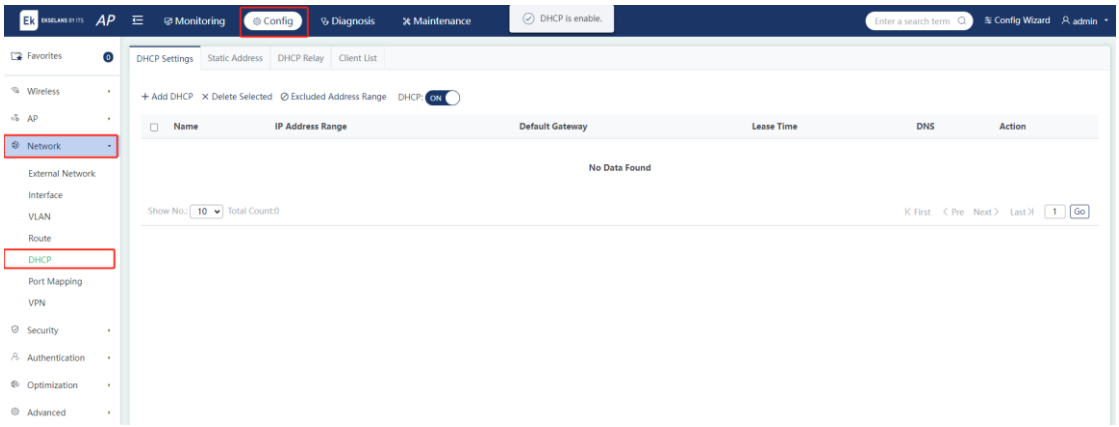
5.3.5 DHCP

1. DHCP Settings

Choose **Config** > **Network** > **DHCP** > **DHCP Settings**.

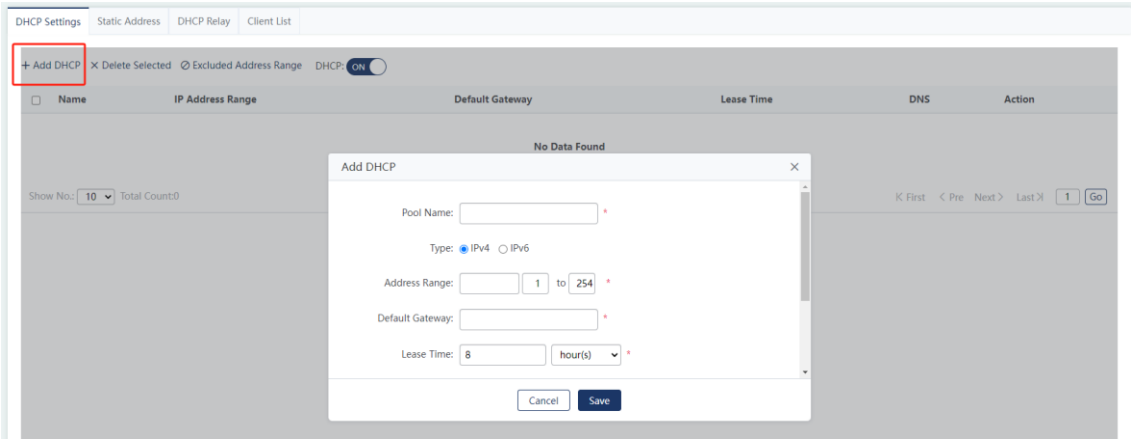
(1) Enabling the DHCP Service

Toggle on the **DHCP** switch to enable the DHCP service.



(2) Adding a DHCP Address Pool

Click **Add DHCP** and edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed. The DHCP address pool will be displayed in the list.



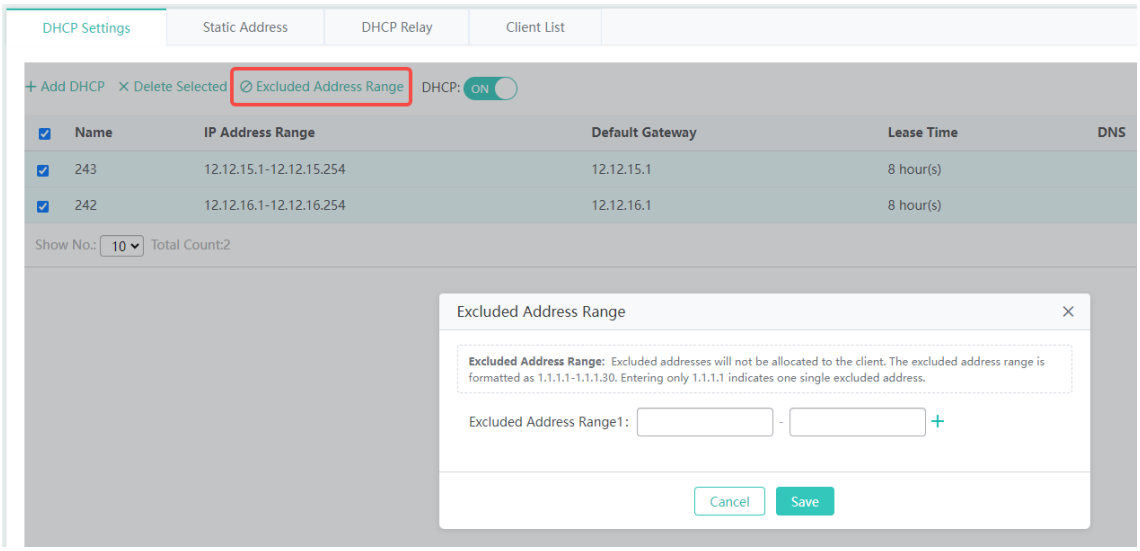
Parameter	Description
Pool Name	Enter the name of the DHCP address pool.
Type	The options include **IPv4** and **IPv6**.
Address Range	Configure the range of the DHCP address pool.
Default Gateway	Configure the default gateway for the DHCP address pool.
Lease Time	Configure the lease time for the DHCP 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.

(3) Deleting a DHCP Address Pool

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a DHCP address pool. To delete multiple DHCP address pools, select the target DHCP address pools in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the DHCP address pools.

(4) Configuring an Excluded IP Address Range

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 **Save** and a message indicating operation success is displayed. The excluded address range will be displayed in the list.



(5) Editing a DHCP Address pool

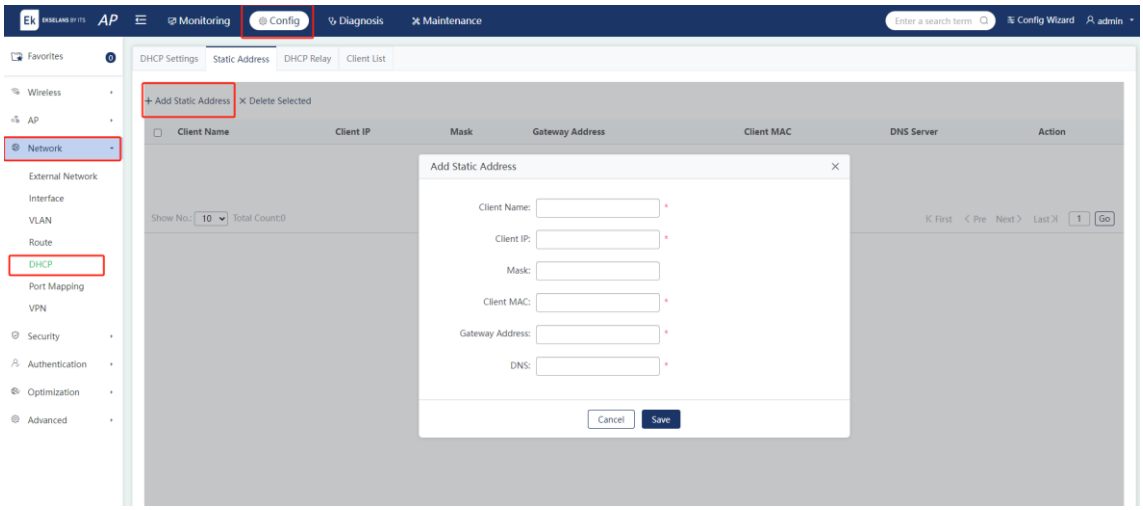
Click **Edit** in the **Action** column and a window pops up displaying information about the DHCP address pool. Edit the fields in the window. Click **Save** and a message indicating operation success is displayed.

2. Static Address

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

(1) Add a Static IP Address

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 a Static IP Address

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a static IP address. To delete multiple static IP addresses, select the target static IP addresses in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the static IP addresses.

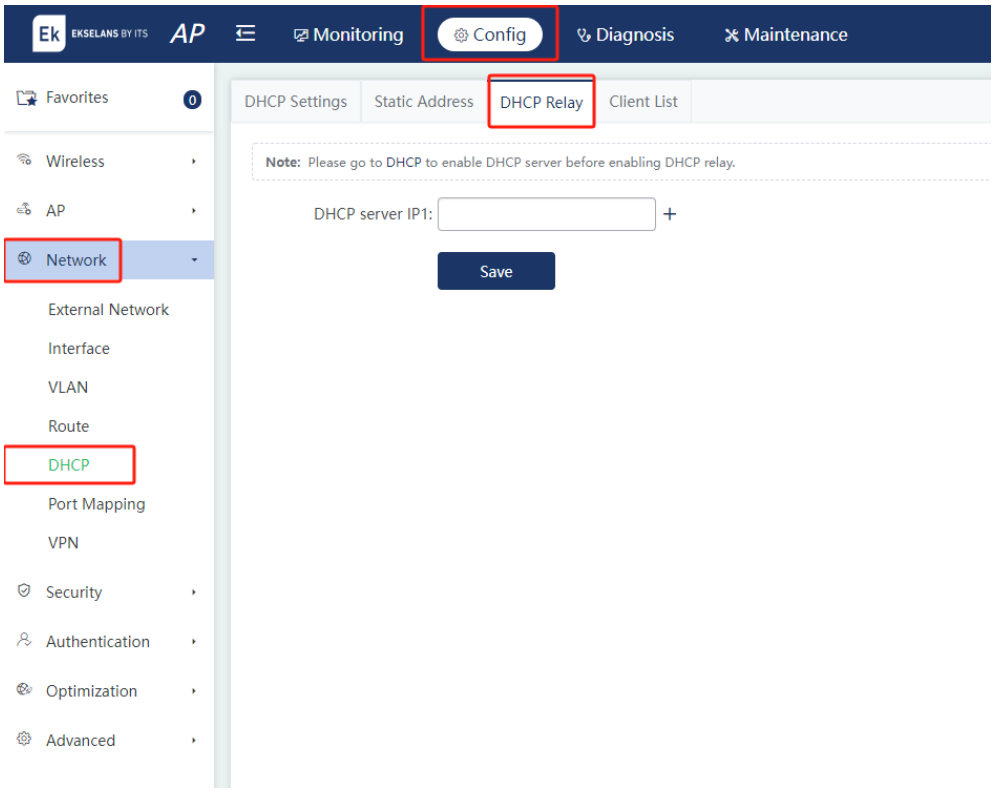
(3) Editing a Static IP Address

Click **Edit** in the **Action** column and a window pops up displaying 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**.

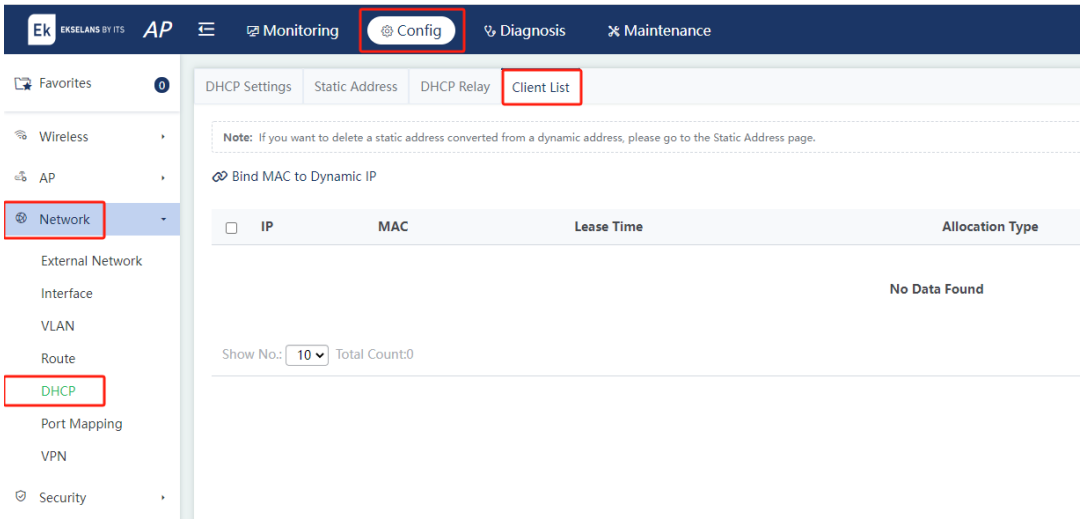


4. Client List

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

(1) Binding a MAC Address to a Dynamic IP Address

Select a MAC address in the list and click **Bind MAC to Dynamic IP**. Click **OK** in the pop-up window to bind the MAC address with the dynamic IP address.

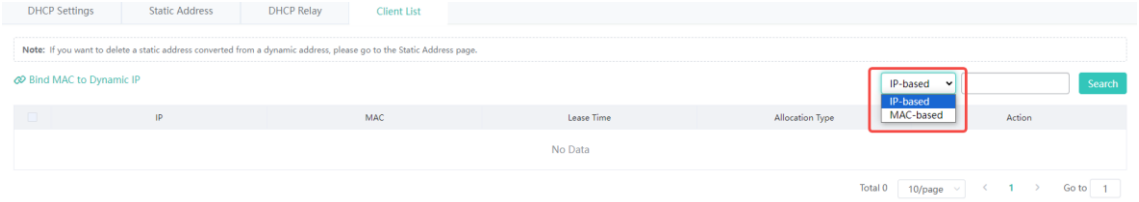


(2) Unbinding the MAC Address from the Dynamic IP Address

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 box. Click **Search** and the result is displayed in the list.



5.3.6 Port Mapping

Choose **Config** > **Network** > **Port Mapping**.

Note

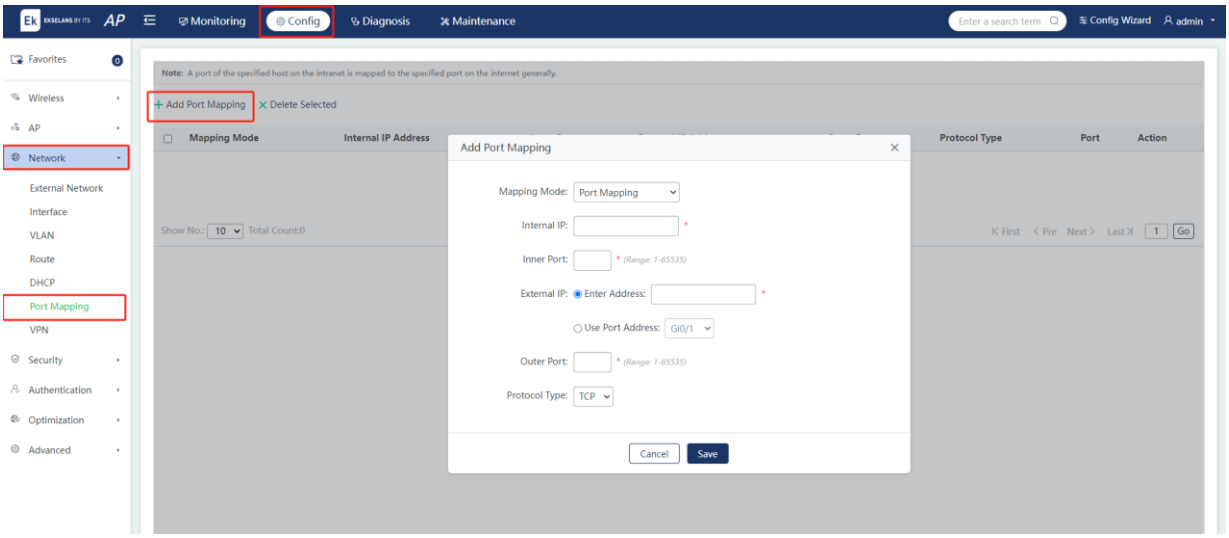
Some APs may not support this function. The actual menu shall prevail.

The port mapping function maps a specified port of a specified host on the intranet to a specified port on the extranet.

The mapping modes includes **Port Mapping** and **DMZ Host Mapping**.

1. Adding a Port Mapping Rule

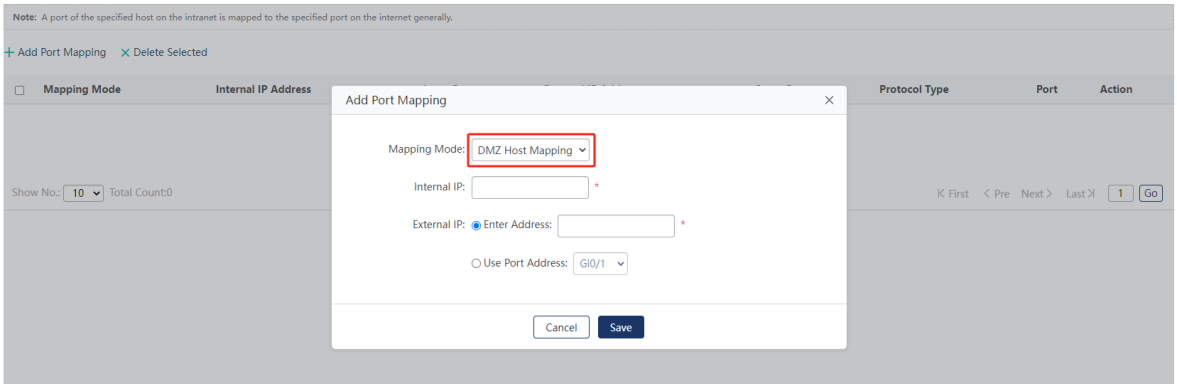
Click **Add Port Mapping**. Set the mapping mode to **Port Mapping**, and edit the fields in the pop-up window. Click **Save**.



Parameter	Description
Mapping Mode	The mapping modes includes **Port Mapping** and **DMZ Host Mapping**.
Internal IP	Enter the internal IP address to be mapped to the extranet, which is typically the IP address of the server.
Inner Port	Enter the port to be mapped to the extranet.
External IP	Enter the IP address of the Wide Area Network (WAN). If **Use Port Address** is selected, all IP addresses on the WAN port are mapped.
Outer Port	Enter the WAN port number. The value range is from 1 to 65535.
Protocol Type	Select TCP or UDP as required.

2. Adding a DMZ Host Mapping Rule

Click **Add Port Mapping**. Set the mapping mode to **DMZ Host Mapping**. Enter the internal server IP address and external IP address or port where the rule takes effect. Then click **Save**. When an incoming data packet does not hit any port mapping rule, the packet is redirected to the internal server according to the Demilitarized Zone (DMZ) rule. That is, all data packets actively sent from the Internet to the device are forwarded to the specified DMZ host.



3. Editing a Port Mapping Rule

Click **Edit** in the **Action** column and a window pops up displaying information about the port mapping rule. Edit the fields in the window. Click **Save**.

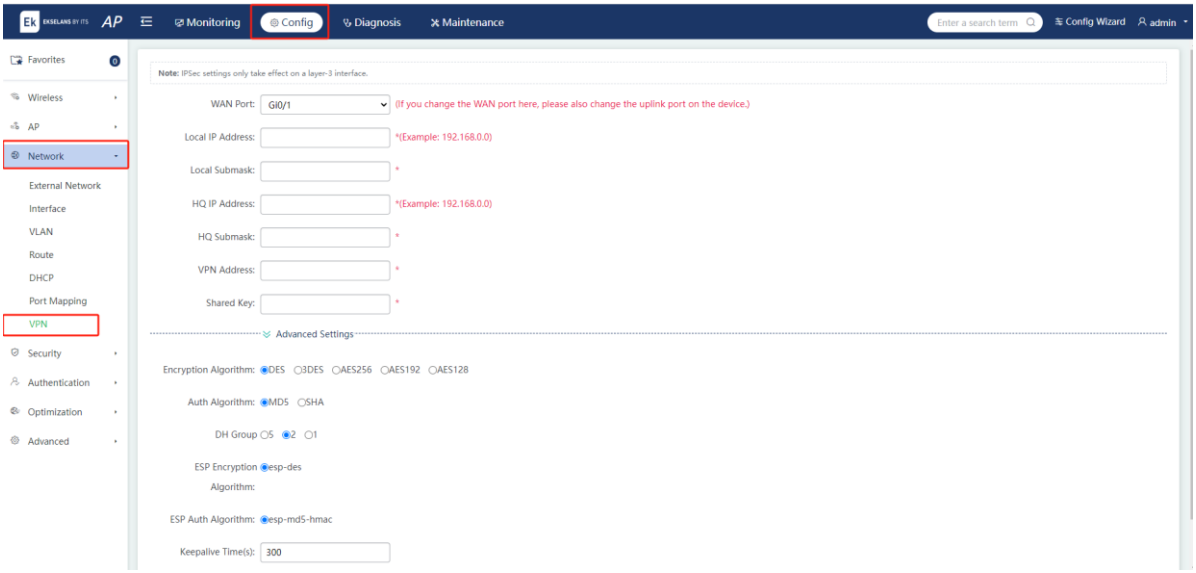
4. Deleting a Port Mapping Rule

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a port mapping rule. To delete multiple port mapping rules, select the target port mapping rules in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the port mapping rules.

5.3.7 VPN

Choose **Config** > **Network** > **VPN**.

You can configure VPN for only one WAN port. Enter the local IP address, local subnet mask, headquarters (HQ) IP address, HQ subnet mask, VPN address, and shared key. Click **Advanced Settings** to configure the algorithms. You are advised to use the default settings.



5.4 Security

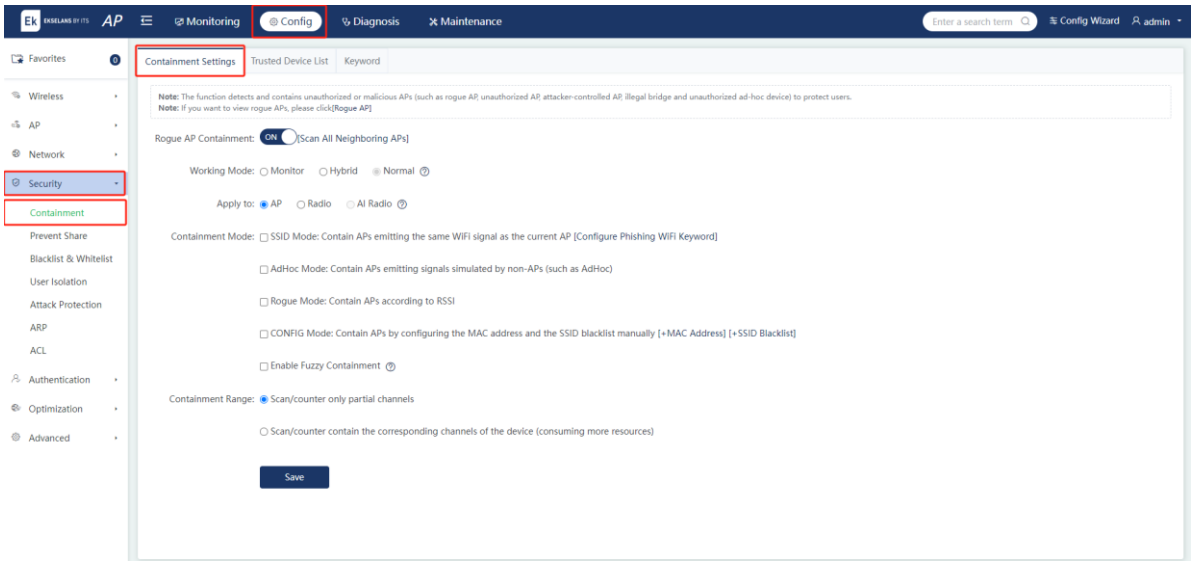
5.4.1 Containment

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

Rogue APs may exist on a wireless network. They may have security vulnerabilities or be controlled by attackers, posing great threat to network security. Enable the containment feature on the AP to proactively detect unauthorized or malicious APs on the network (such as rogue APs, unconfigured APs, APs controlled by attackers, rogue bridges, or unauthorized Ad-hoc devices), and implement containment on them to prevent wireless STAs from associating with unauthorized APs.

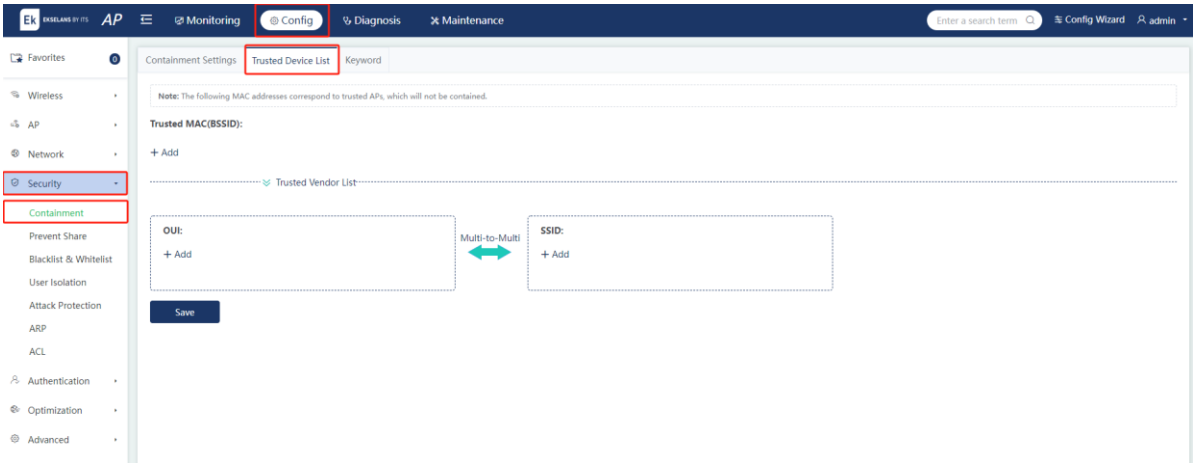
1. Containment Settings

When **Rogue AP Containment** is enabled, you need to set the working mode to **Monitor** or **Hybrid**. The **Hybrid** mode is applied to the AP only, while the Monitor mode can be applied to the AP or selected radios. Click **Configure Phishing WiFi Keyword** to access the **Keyword** page and configure the keyword.



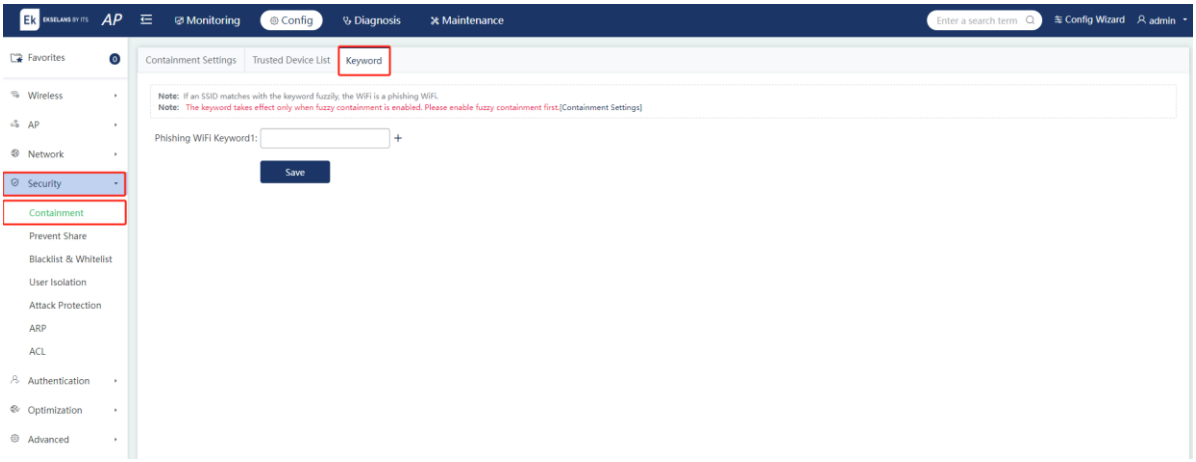
2. Trusted Device List

When **Rogue AP Containment** is enabled, unauthorized APs will be contained. However, some devices are trusted devices. You can configure the MAC address of a trusted device or the MAC address of a trusted manufacturer. If an AP is configured as a trusted device, it will not be contained.



3. Phishing Wi-Fi Keyword

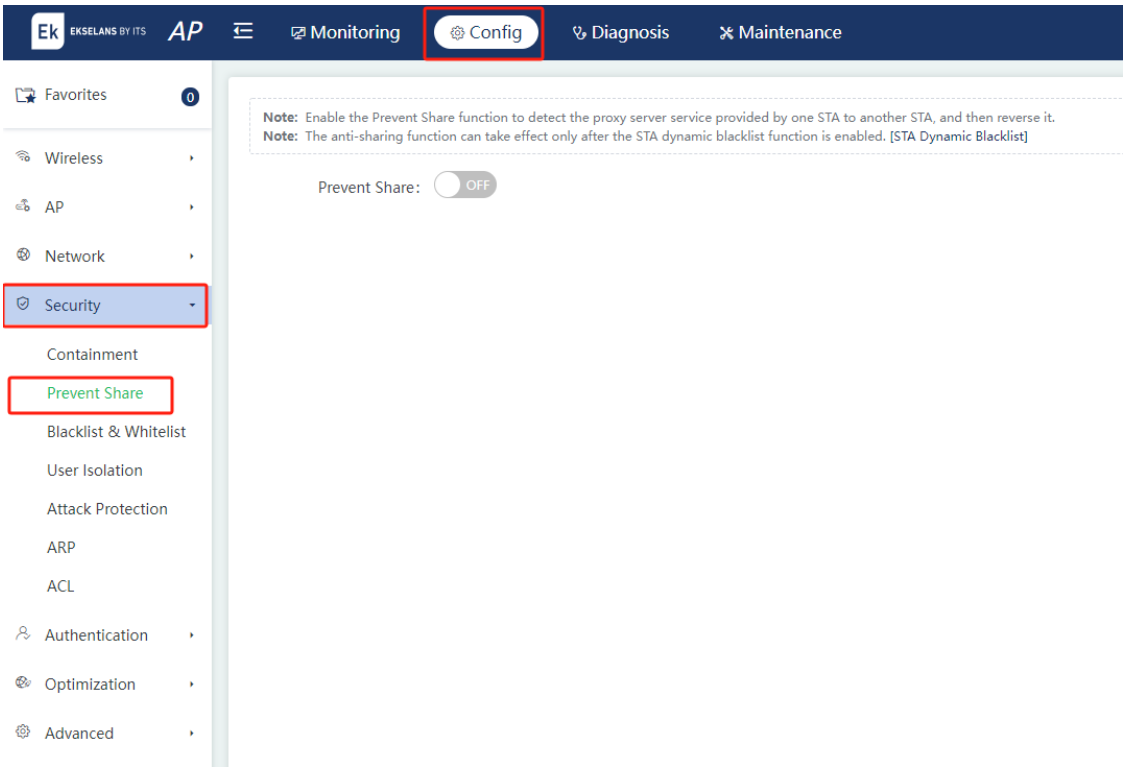
Phishing Wi-Fi keywords are obtained by scanning SSIDs on the network. Match the scanned SSIDs against the configured keywords. If an SSID matches the keyword fuzzily, the Wi-Fi is considered as a phishing Wi-Fi.



5.4.2 Sharing Prevention

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

When **Prevent Share** is enabled, the system can detect whether one STA provides the proxy service to another and adds the STA providing the proxy service into the containment list.



5.4.3 Blacklist & Whitelist

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

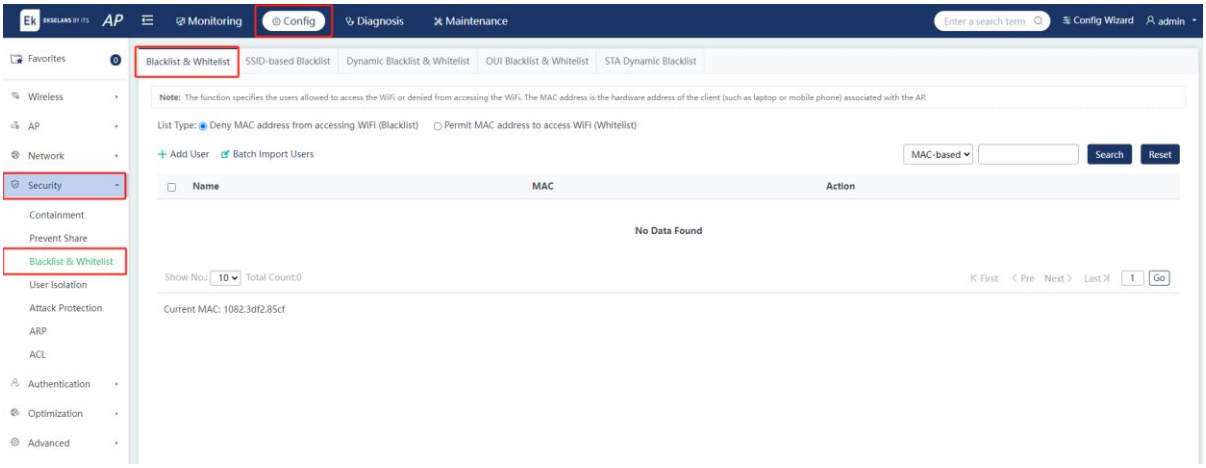
To enhance wireless security, you can configure a blacklist (users in the blacklist are denied from accessing the Wi-Fi network) and a whitelist (only users in the whitelist are allowed to access the Wi-Fi network) to control the access of wireless users. A fat AP supports the global blacklist and whitelist, SSID-based blacklist and whitelist, dynamic blacklist and whitelist, Organizationally Unique Identifier (OUI)-based blacklist and whitelist, and STA-based dynamic blacklist.

Note

- The number of users that are denied or permitted to access the Wi-Fi network varies with devices. The value displayed on the page shall prevail.
- The configurations of the blacklist and whitelist are the same. The following takes the blacklist configuration as an example.

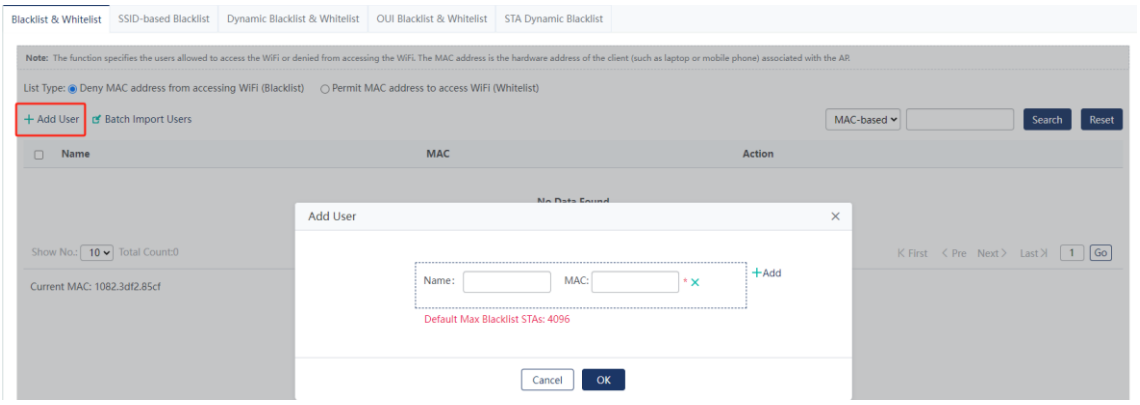
1. Configuring the Global Blacklist or Whitelist

The wireless users in the global blacklist are denied from accessing any Wi-Fi network of the AP. However, only the wireless users in the global whitelist are permitted to access any Wi-Fi network of the AP.



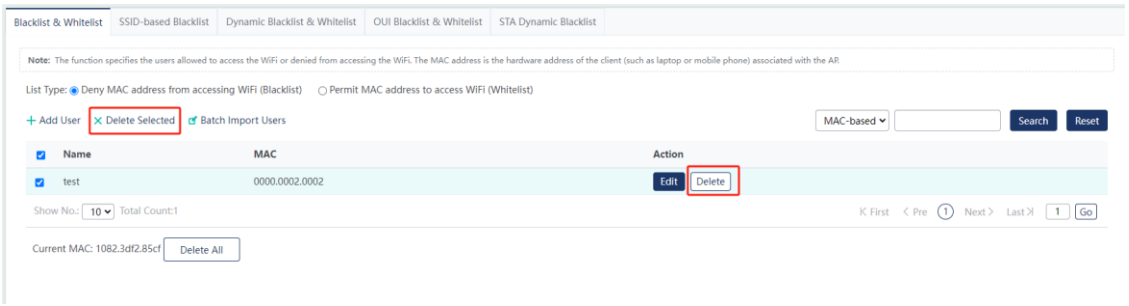
(1) Adding a User

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



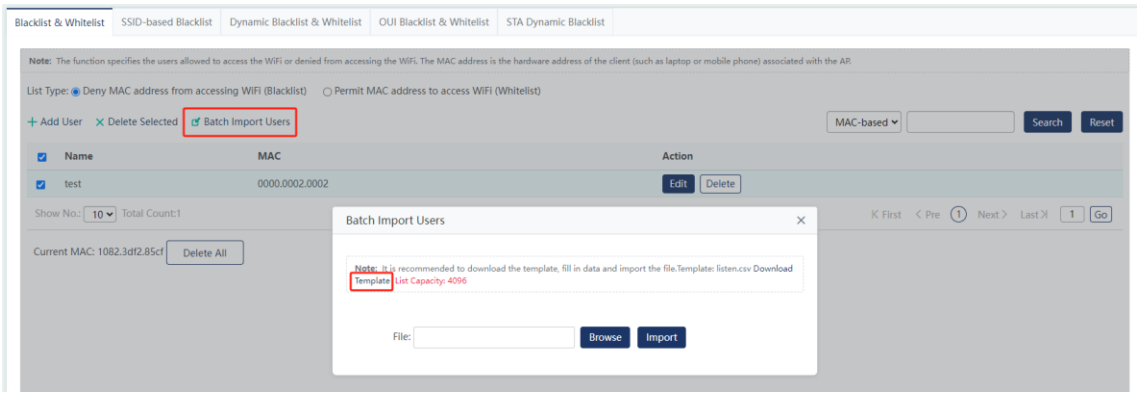
(2) Deleting a User

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a user. To delete multiple users, select the target users in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the users.



(3) Batch Importing Users

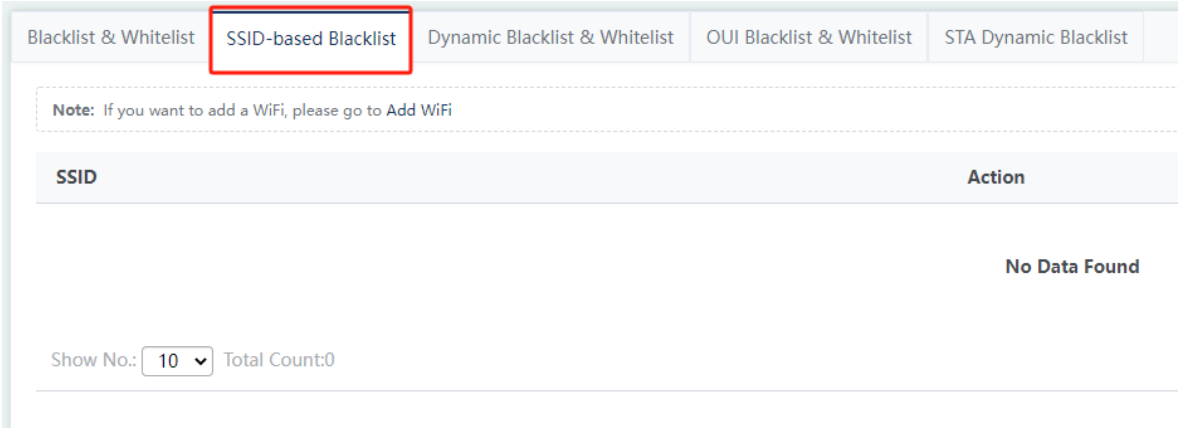
Click **Batch Import Users**. Download and fill in the template. Import the template file.



2. Configuring the SSID-based Blacklist or Whitelist

The wireless users in the SSID-based blacklist are denied from accessing a specified Wi-Fi network. However, only the wireless users in the SSID-based whitelist are permitted to access a specified Wi-Fi network.

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



(1) Adding a User

Click **Add User** to add the MAC address of a user. Click **OK**.

(2) Deleting a User

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a user. To delete multiple users, select the target users in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the users.

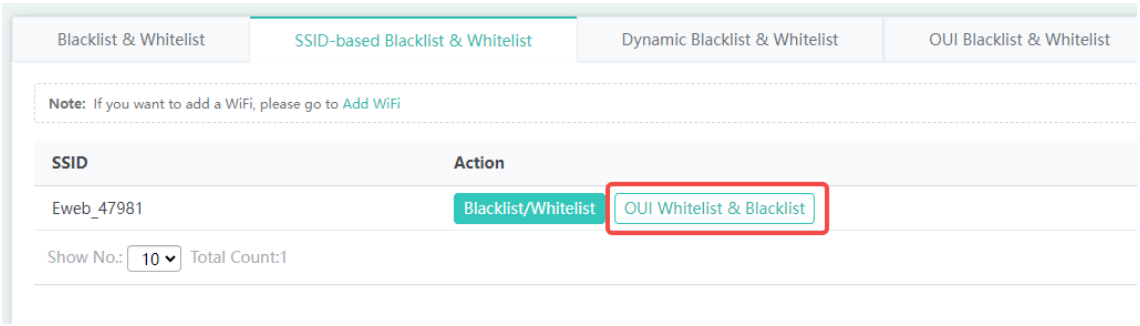
(3) Batch Importing Users

Click **Batch Import Users**. Download the template. Fill in the template and save it. Click **Browse**. Select the template file. Click **Import**.

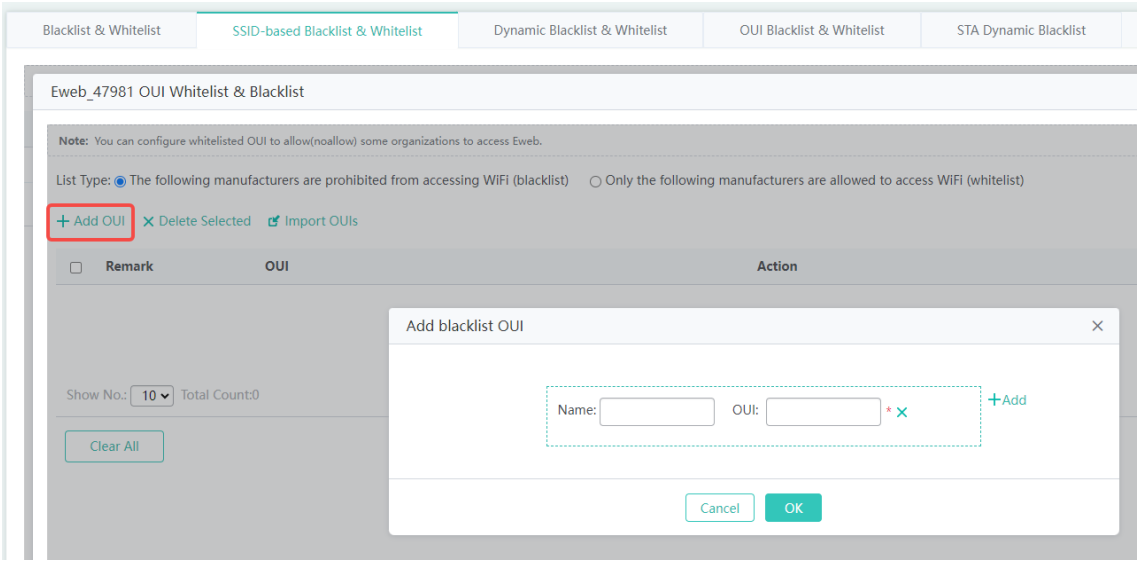
(4) Configuring an OUI

An OUI is the first 8 bits of the MAC address of a device. If devices to be added to the blacklist or whitelist belong to the same manufacturer, add their OUI to the list directly, eliminating the need to add the MAC address of each device one by one.

Click **OUI Whitelist & Blacklist** to enter the configuration page.



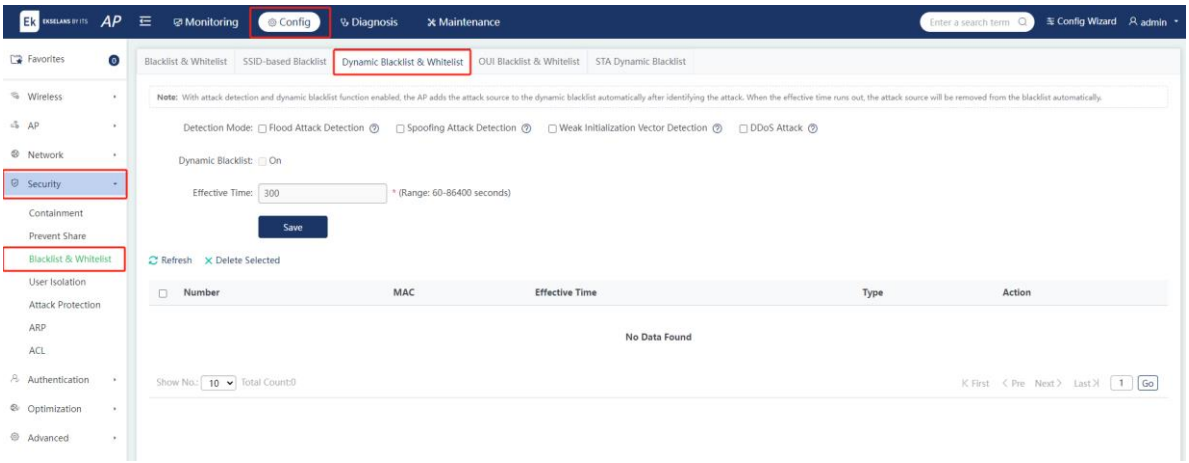
Click **Add OUI**. Enter the name and OUI of a manufacturer. Click **OK**.



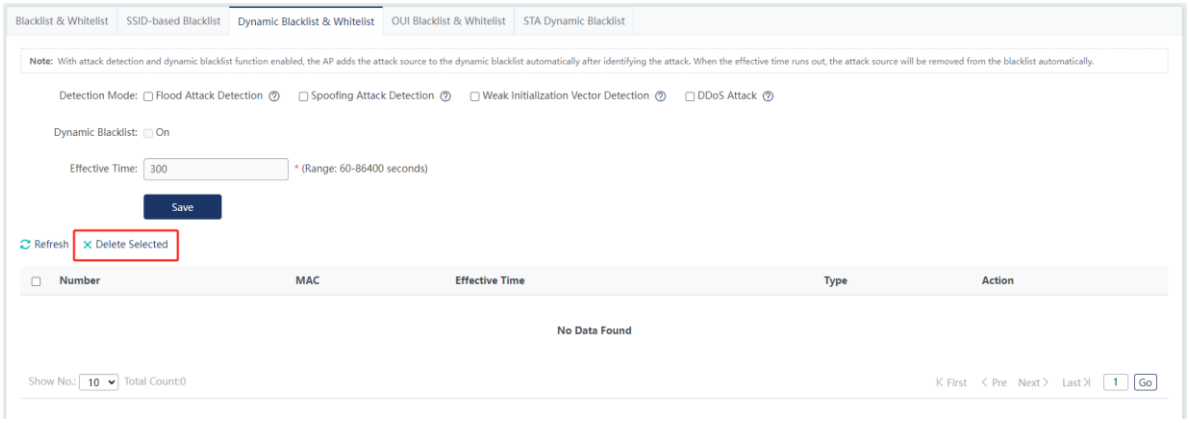
3. Configuring the Dynamic Blacklist or Whitelist

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.

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



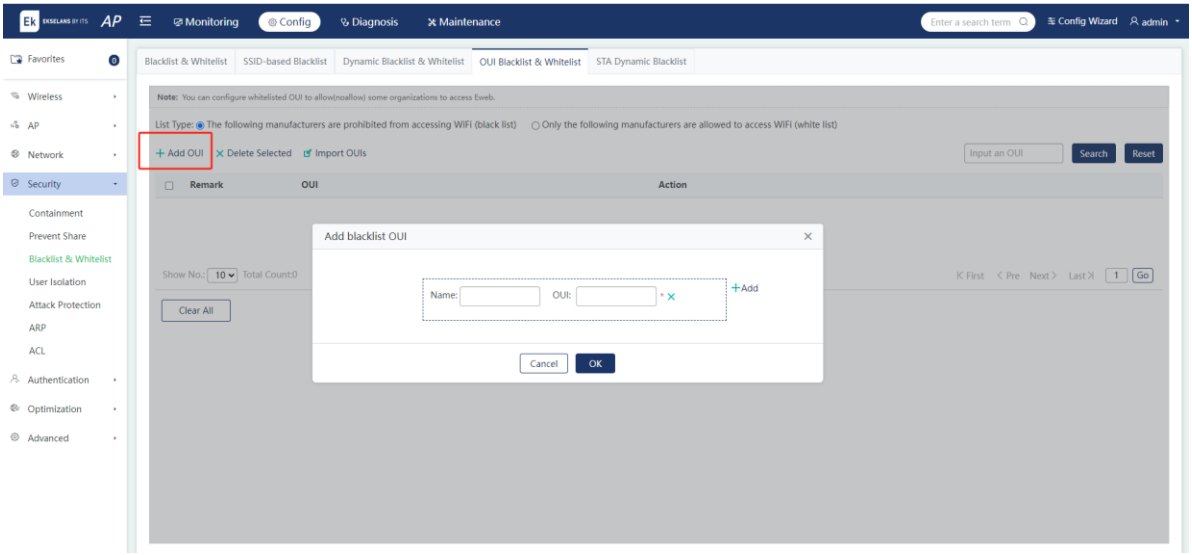
Deleting a dynamic blacklist: Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a dynamic blacklist. To delete multiple dynamic blacklists, select the target dynamic blacklists. Click **Delete Selected**. Click **OK** in the pop-up window to batch delete the dynamic blacklists.



4. Configuring the OUI Blacklist or Whitelist for the AP

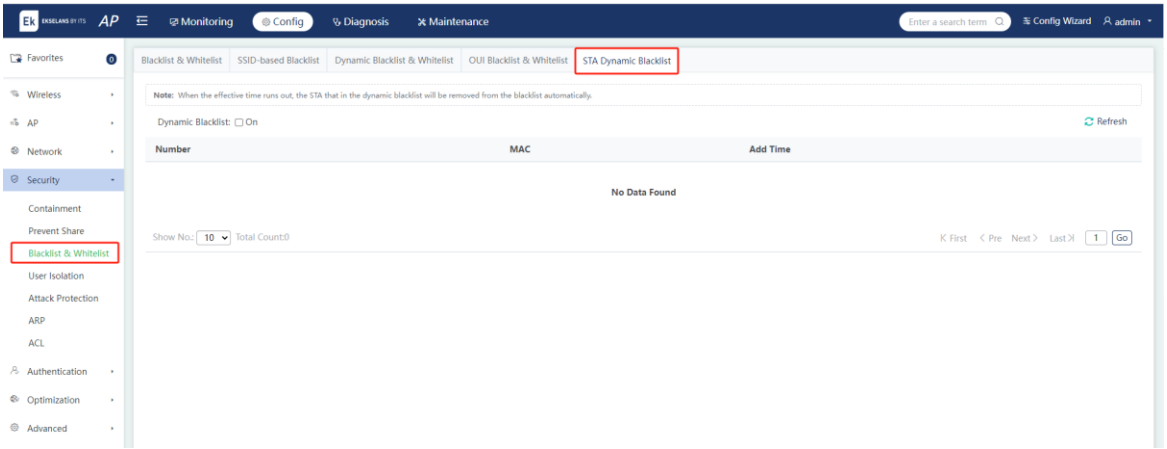
The manufacturers in the OUI blacklist are denied from accessing any Wi-Fi network of the AP, while only the manufacturers in the OUI whitelist are allowed to access any Wi-Fi network of the AP.

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



5. Configuring the STA Dynamic Blacklist

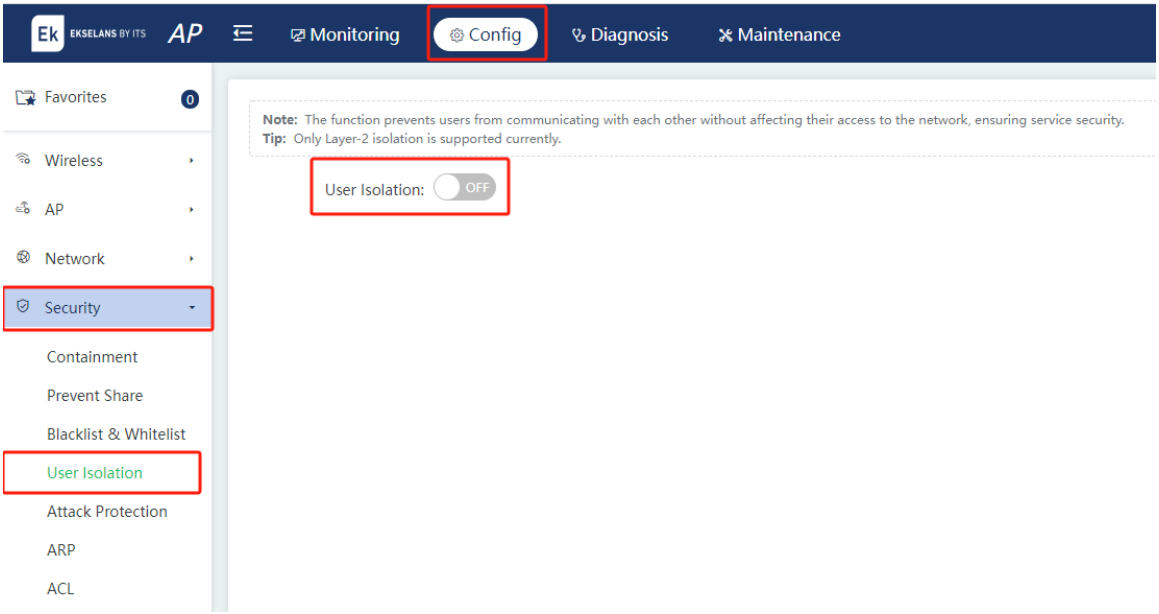
Add STAs from malicious attack sources to the STA dynamic blacklist to prevent them from accessing the network.



5.4.4 User Isolation

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

To ensure network security and information confidentiality, enable **User Isolation** so that intranet users cannot communicate with each other. Some special users (users who can access each other) can be identified by user name and MAC address. Click **Add** to add MAC addresses of users to **Whitelisted MAC** for mutual access.

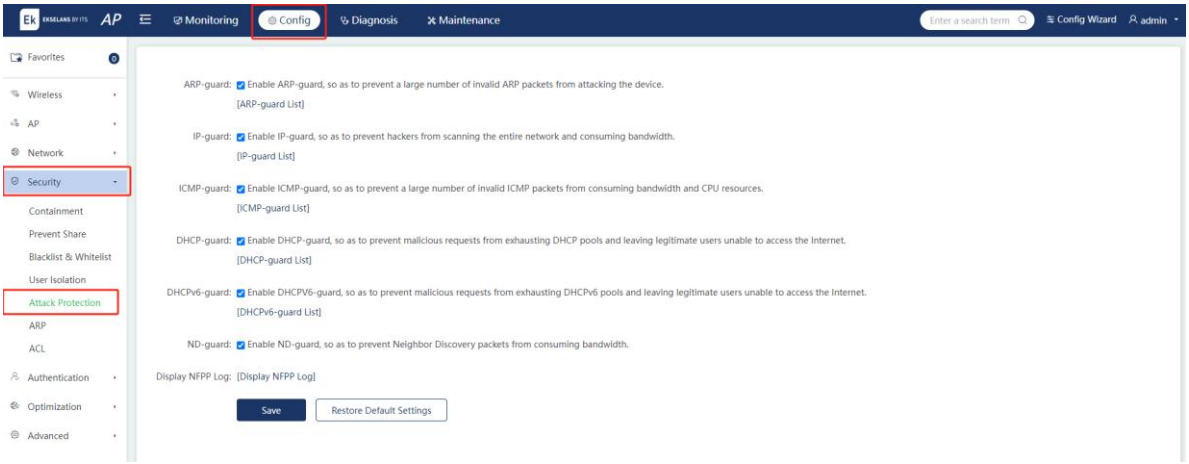


5.4.5 Attack Prevention

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

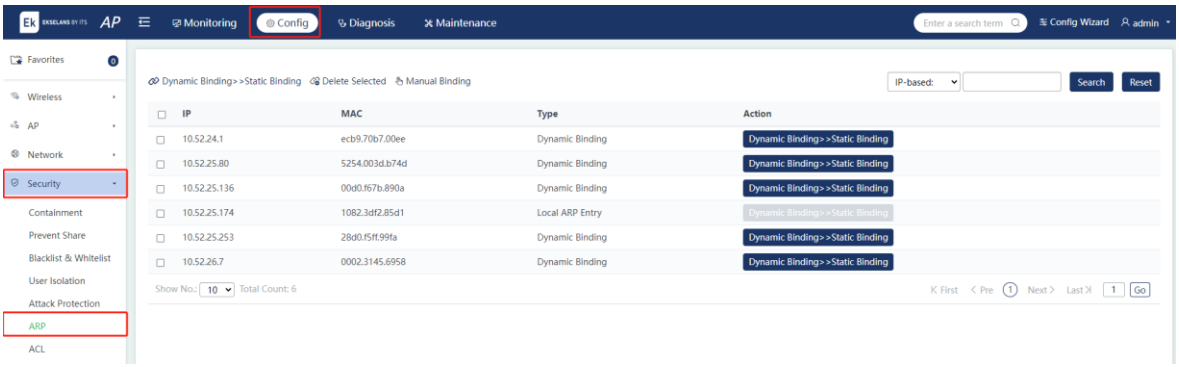
Malicious attacks often occur in a network environment. These attacks overload the device, resulting in high CPU usage and an operation failure of the device.

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



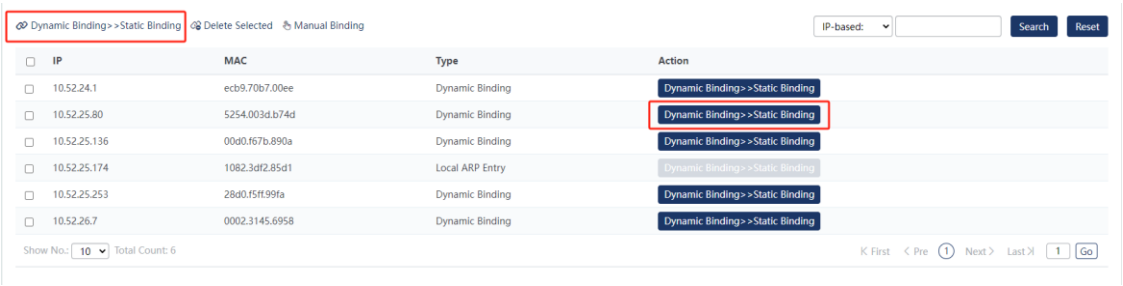
5.4.6 ARP Entry Binding

Choose **Config** > **Security** > **ARP**.



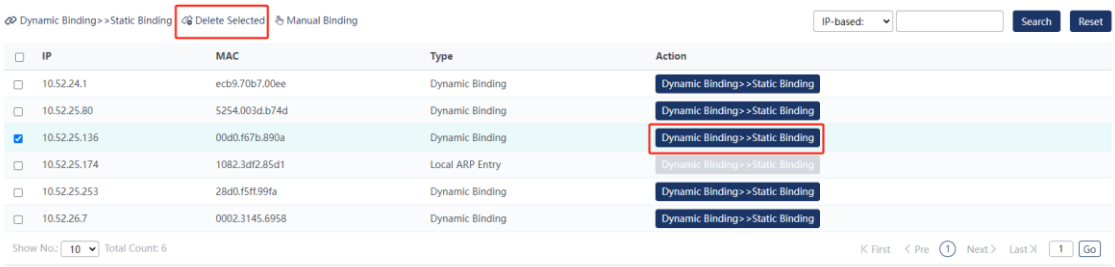
(1) Switching a Dynamic Binding to a Static Binding

Select one entry in the ARP list. Click **Dynamic Binding >> Static Binding** in the **Action** column to switch the dynamic binding to the static binding. You can also select more entries in the ARP list and click **Dynamic Binding >> Static Binding** next to **Delete Selected** to batch switch the dynamic bindings to the static bindings.



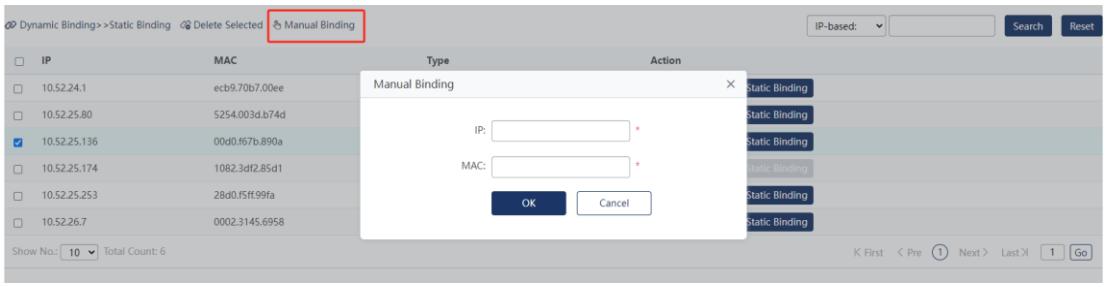
(2) Deleting a Static Binding

Select one entry in the ARP list. Click **Static Binding >> Dynamic Binding** in the **Action** column to switch the static binding to the dynamic binding. To delete multiple static bindings, select the target IP addresses in the ARP list. Click **Delete Selected** to batch delete the static bindings.



(3) Manual Binding

Click **Manual Binding**. Enter the IP and MAC addresses. Click **OK** and a message indicating operation success is displayed. The new entry is displayed in the ARP list.



5.4.7 ACL

Choose **Config** > **Security** > **ACL**.

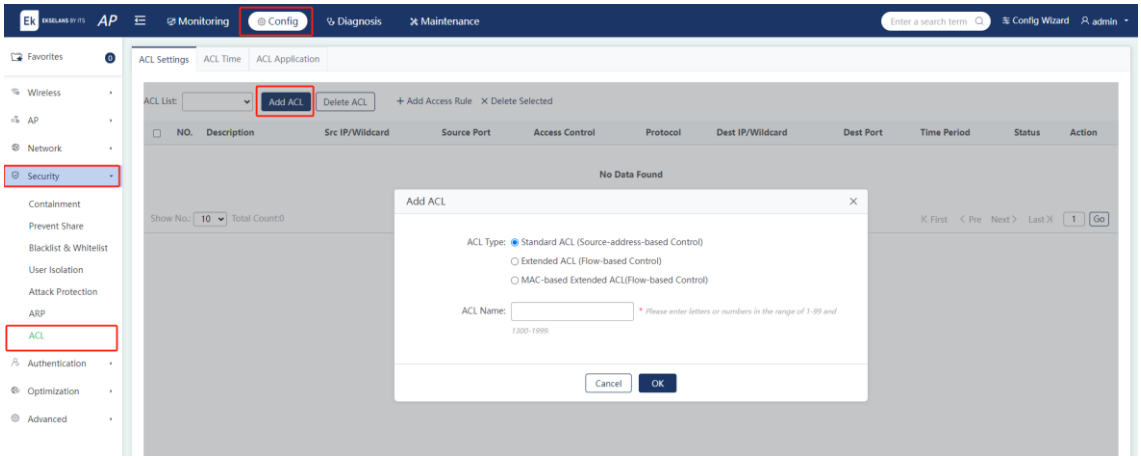
When receiving a packet, a device interface on which an ingress ACL is configured checks whether the packet matches an access control entry (ACE) in the ingress ACL. When sending a packet, a device interface on which an egress ACL is configured checks whether the packet matches an ACE in the egress ACL.

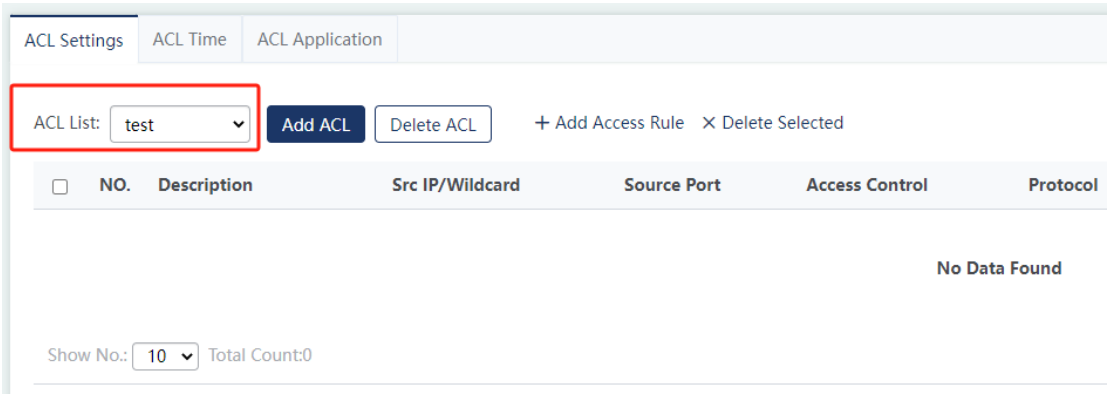
When different ACEs are configured, multiple ACEs may be applied at the same time, or only some ACEs are applied. Packets are processed according to the first matched ACE (permit or deny).

1. ACL Settings

(1) Adding an ACL

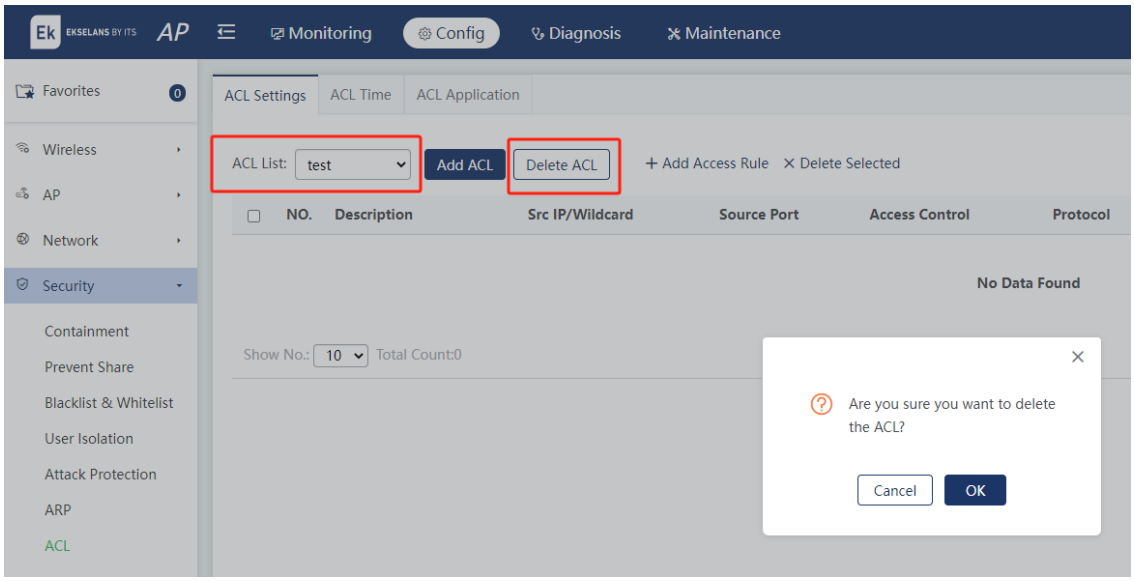
Click **Add ACL**. Enter the fields in the pop-up window. Click **OK** and a message indicating operation success is displayed. The new entry is displayed in the drop-down ACL list in the upper left corner.





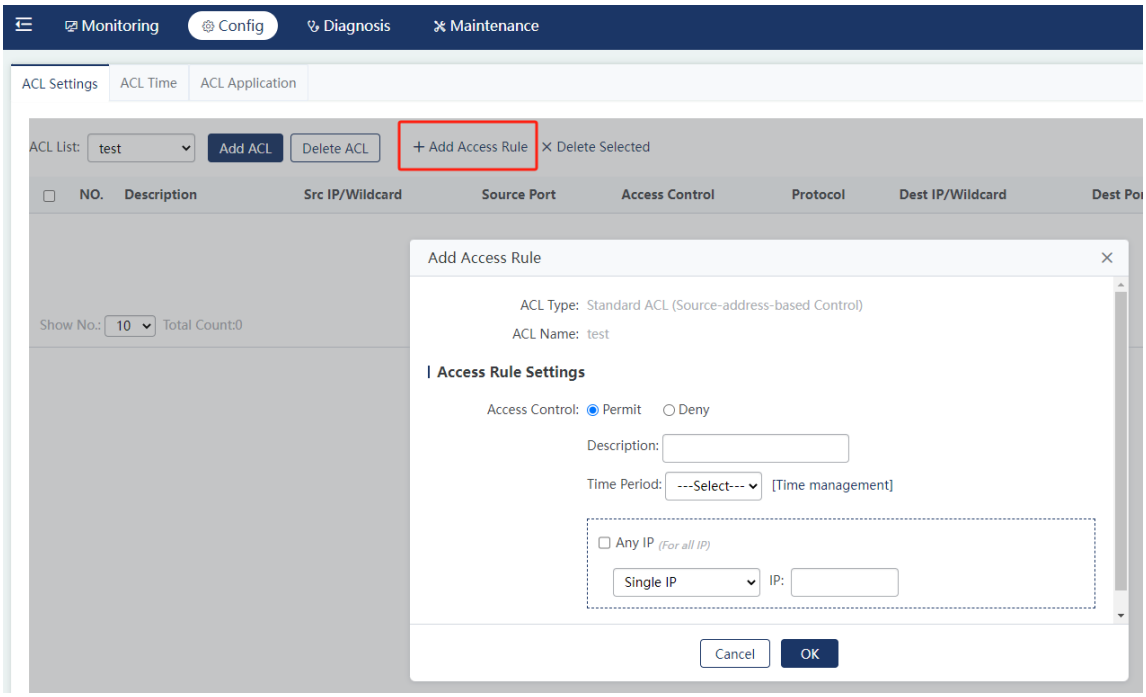
(2) Deleting an ACL

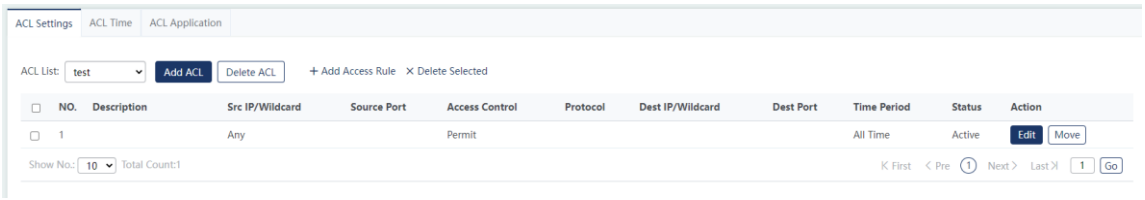
Select the ACL to be deleted from the drop-down ACL list. Click **Delete ACL**. Click **OK** in the pop-up window to delete the ACL.



(3) Adding an ACE

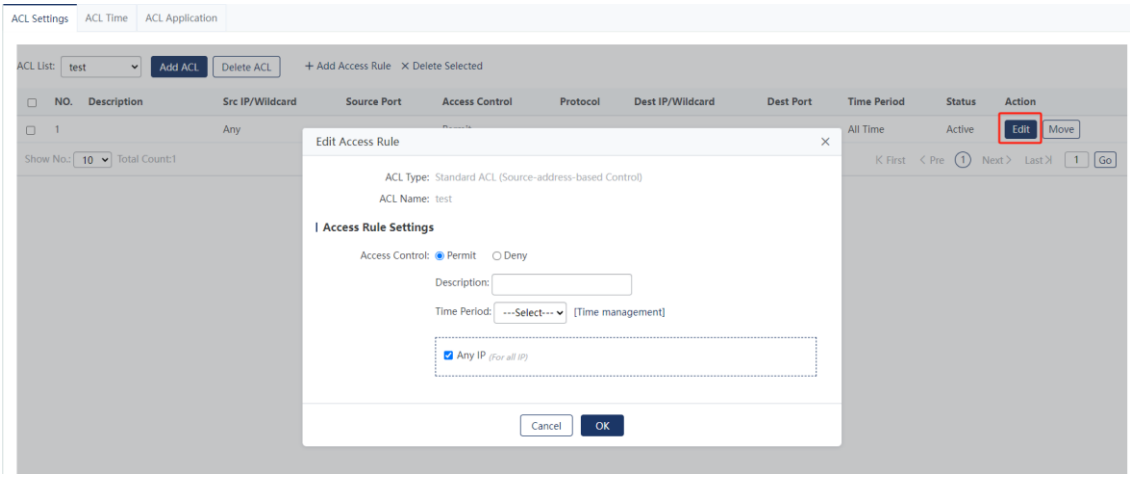
Select an ACL to which an ACE needs to be added from the drop-down ACL list. Click **Add Access Rule**. Enter the fields in the pop-up window. Click **OK** and a message indicating operation success is displayed. The new entry is displayed in the ACL list.





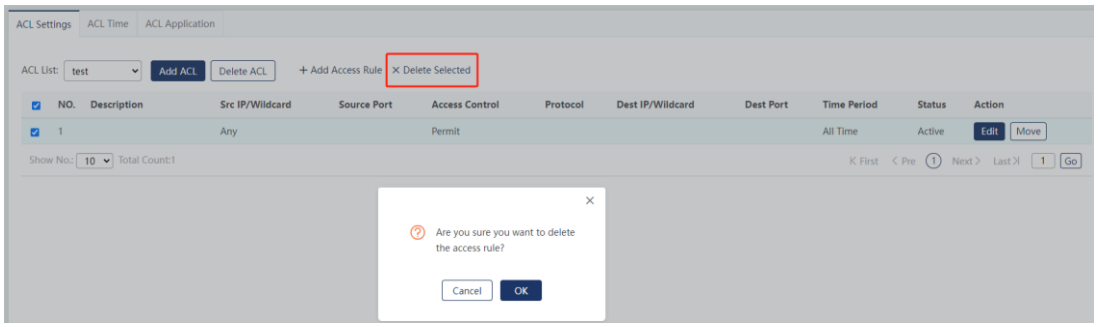
(4) Editing an ACE

Click **Edit** in the **Action** column of an ACE in the ACL list. Edit the fields in the pop-up window. Click **OK** and a message indicating operation success is displayed.



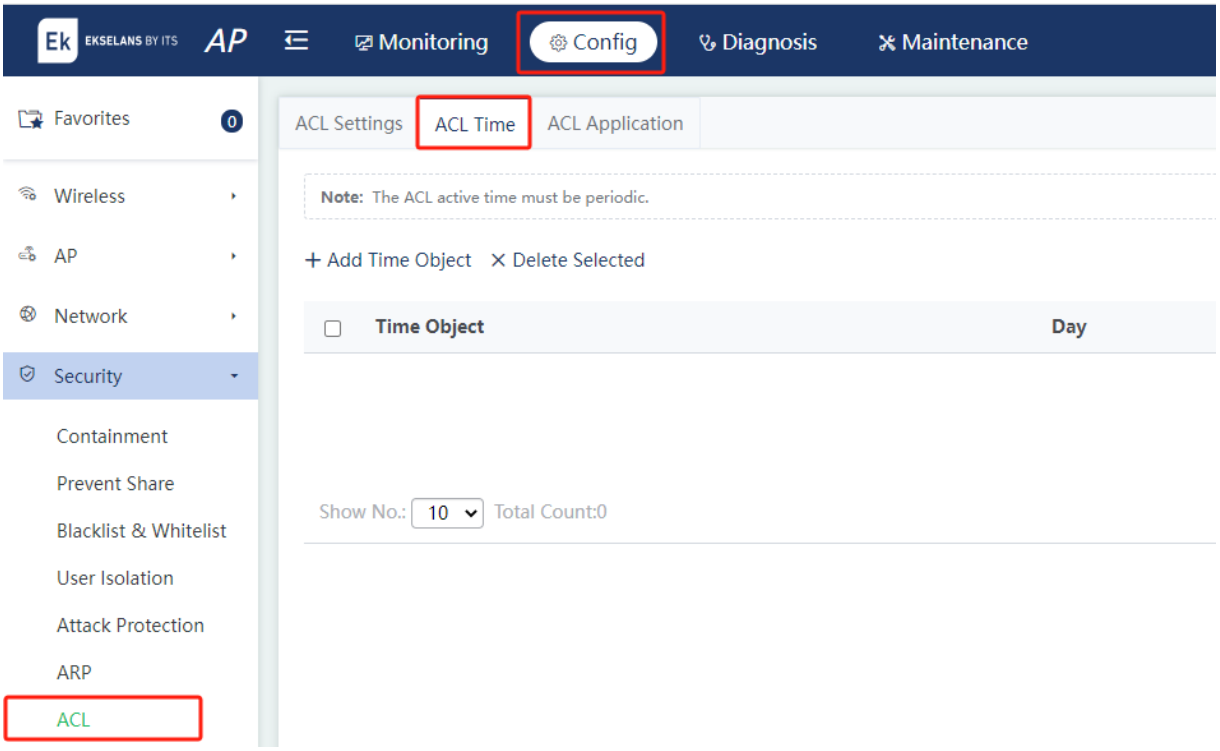
(5) Deleting an ACE

Select one or more entries in the ACL list. Click **Delete Selected**. Click **OK** in the pop-up window to delete the ACE(s).



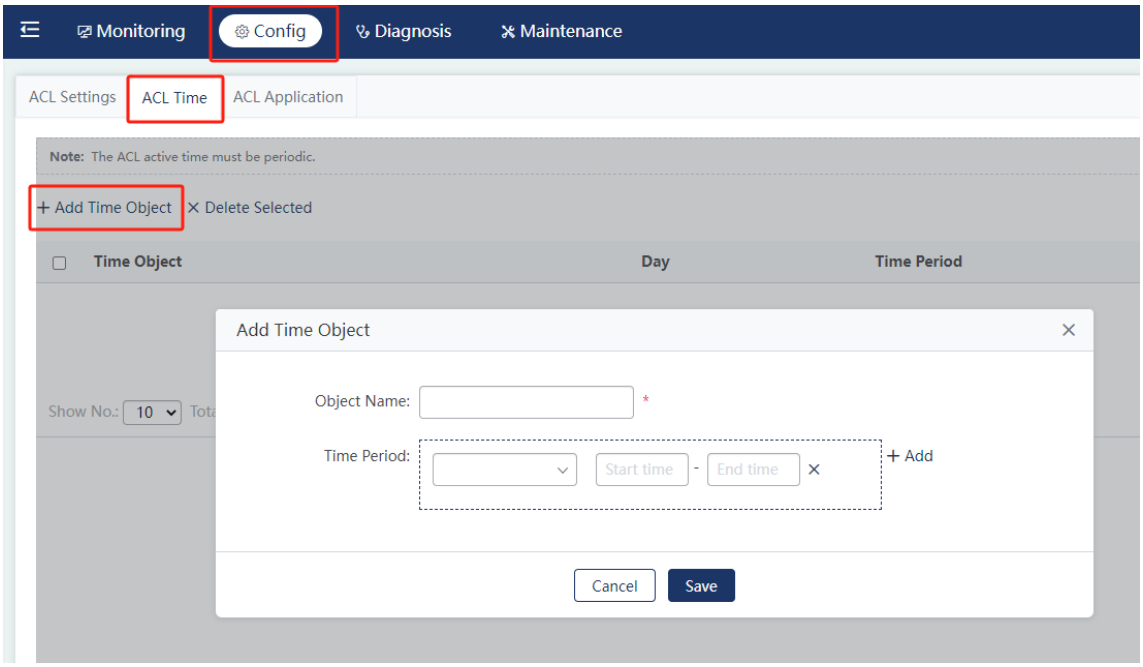
2. ACL Time

An ACL can be configured to take effect based on time, for example, in some time periods of a week. To meet this requirement, you need to configure a time object.



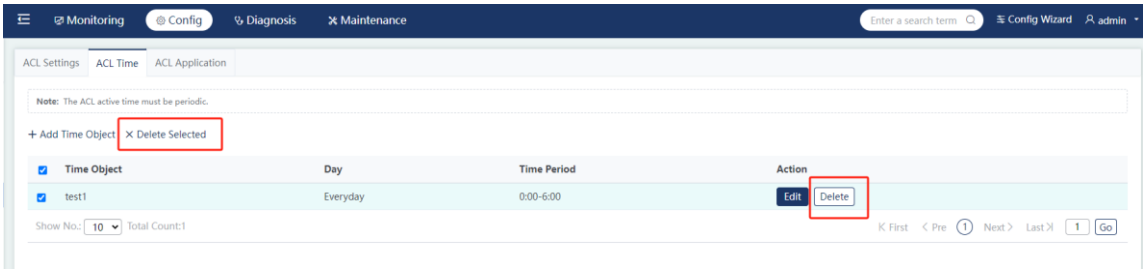
(1) Adding a Time Object

Click **Add Time Object**. Edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.



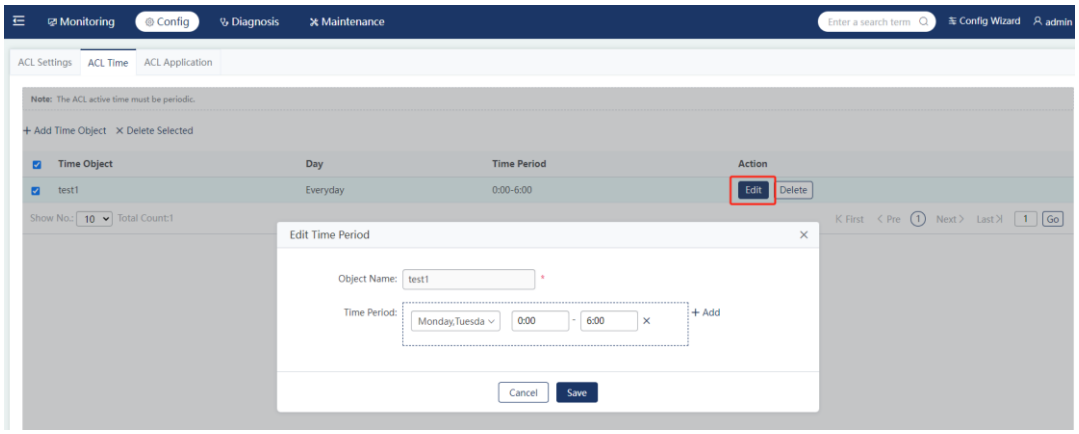
(2) Deleting a Time Object

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a time object. To delete multiple time objects, select the target time objects in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch the time objects.



(3) Editing a Time Object

Click **Edit** in the **Action** column of a time object. Edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.

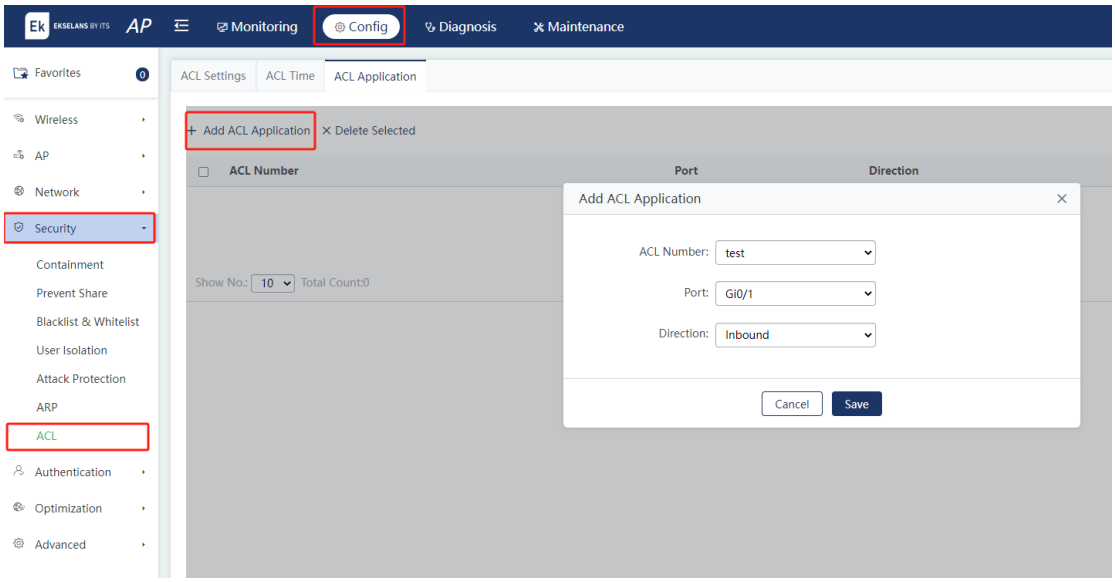


3. ACL Application

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

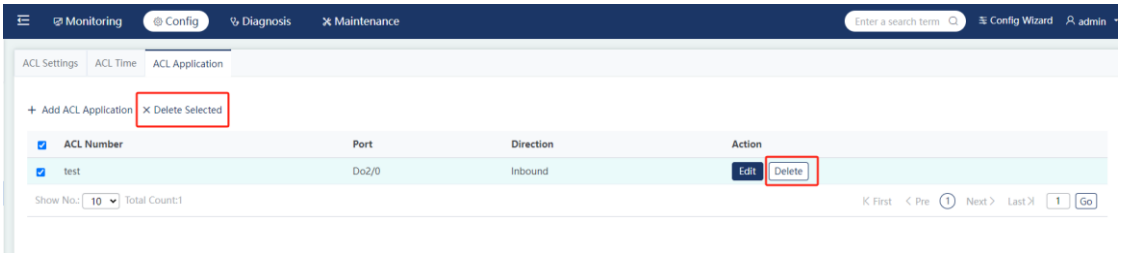
(1) Adding an ACL Application

Click **Add ACL Application**. Enter the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed. The new entry is displayed in the list.



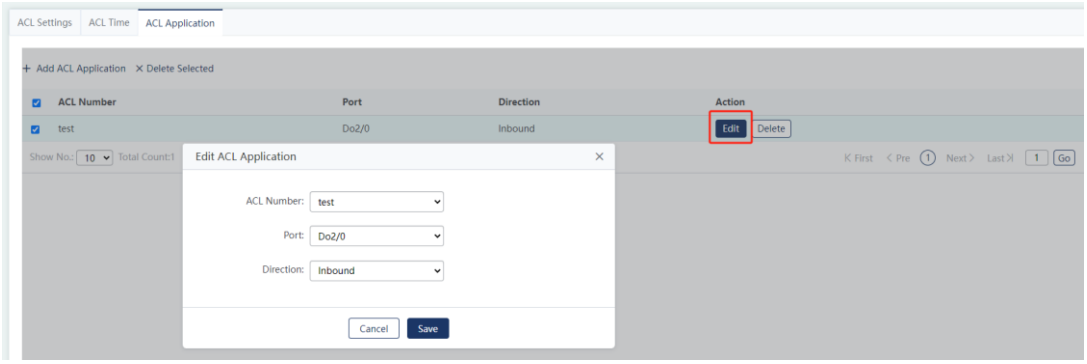
(2) Deleting an ACL Application

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete an ACL application. To delete multiple ACL applications, select the target ACL applications in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch the ACL applications.



(3) Editing an ACL Application

Click **Edit** in the **Action** column of an ACL application. Edit the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.



5.5 Authentication

5.5.1 Web-based Authentication

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

Web-based authentication allows you to control user access to the network. After web-based authentication is enabled, when a client needs to access the network, the device will steer the client to access a specific website (portal server) for authentication. Network access is granted to the client only upon successful authentication.

Web-based authentication has the following advantages:

- Ease of use: Users do not need to install dedicated client software and can perform authentication through a browser.
- Custom services and service expansion: Through interaction between the browser and the portal server, users can customize services such as advertisements, notifications, and business links on the portal server page.

Web-based authentication is classified into **ePortal Authentication** and **iPortal Authentication**. If **iPortal Authentication** is selected, no additional server is required, but users need to be configured locally for authentication. If **ePortal Authentication** is selected, the ePortal server and RADIUS server are required.

1. ePortal Authentication

ePortal authentication is classified into **ePortalv1** and **ePortalv2**:

- **ePortalv1**: The authentication and accounting functions are implemented by the ePortal server.

  Process: Users submit authentication information on the authentication page provided by the ePortal software. The ePortal server directly requests authentication from the corresponding RADIUS server. After successful authentication, the ePortal server advertises user information to the device through SNMP, and the device performs access control for users.

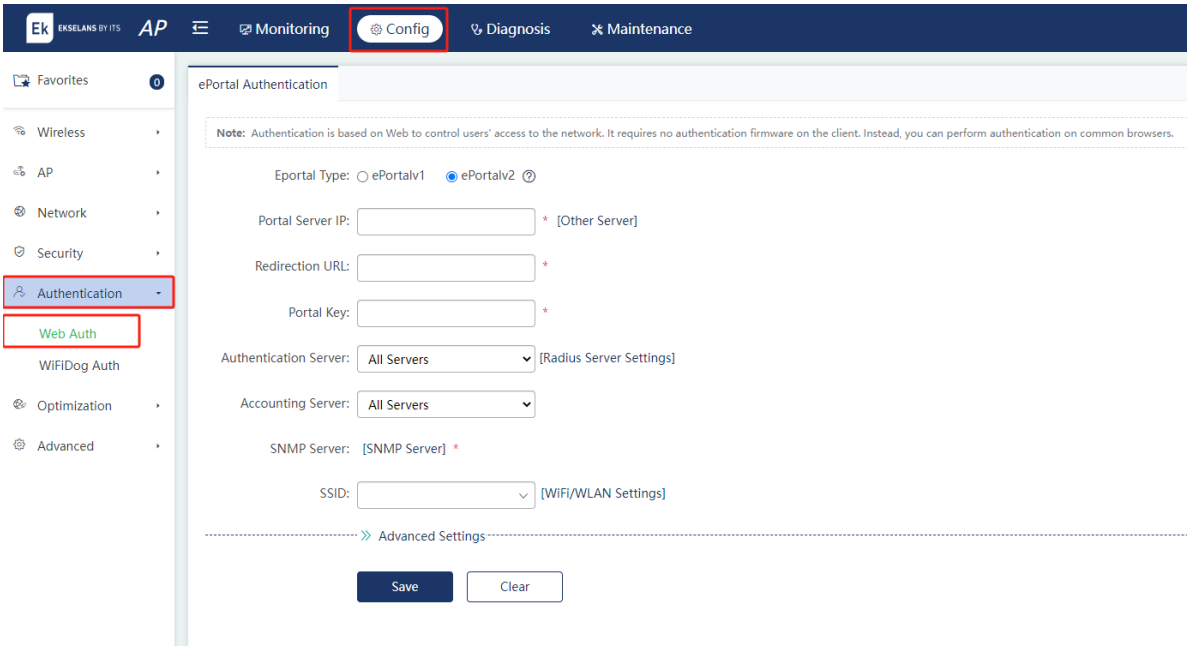
- **ePortalv2**: The portal server is responsible only for user page interaction, and the main authentication process is completed on the device.

  Users submit authentication information on the authentication page provided by the portal server, and the portal server sends the obtained identity information of users to the device through the portal protocol. The device initiates an authentication request to the RADIUS server using the identity information, assigns access permissions to authenticated users, and returns authentication results to the portal server.

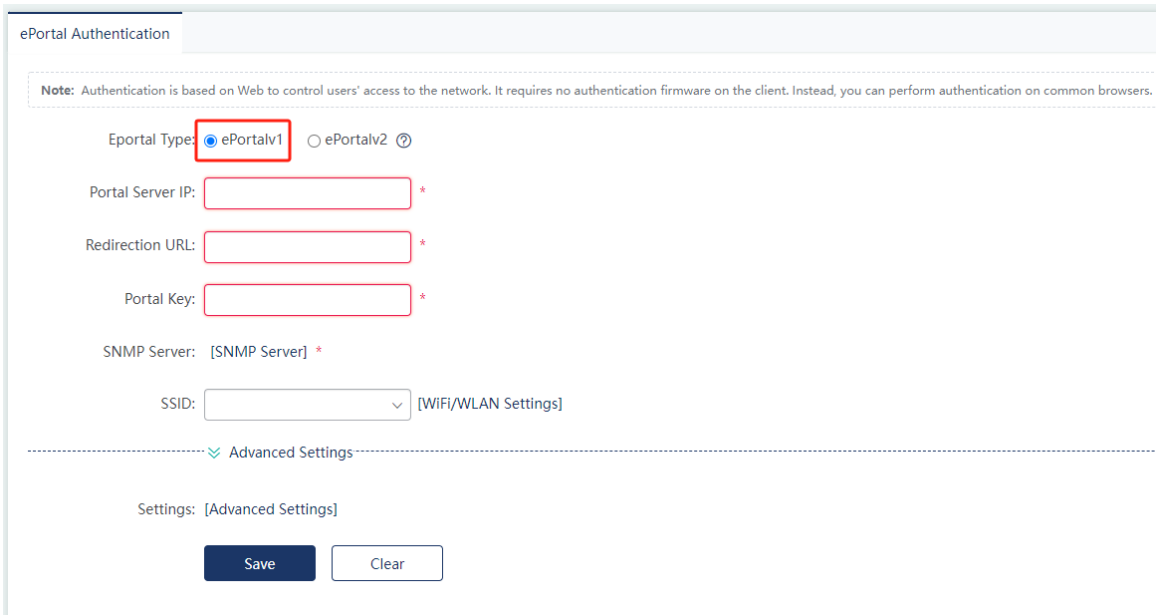
Whether **ePortalv1** or **ePortalv2** is selected depends on the portal server used.

Caution

Before configuring ePortal authentication, you need to set up an ePortal authentication server, including the deployment of the ePortal server and the configuration of authorized users on the RADIUS server.

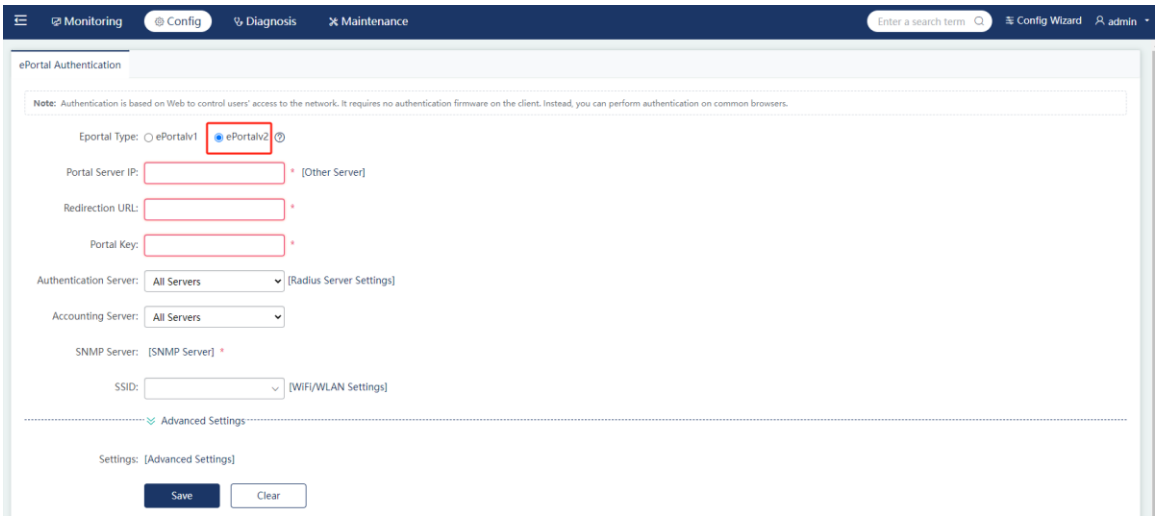


(1) **ePortalv1**:



Parameter	Description
Portal Server IP	Enter the IP address of the ePortal server. Typically, the authentication page is provided by the ePortal server.
Redirection URL	Enter the URL of the authentication page. When an unauthenticated user accesses network resources, the user is automatically redirected to this page for authentication.
Portal Key	Configure a key used for the communication between the device and the authentication server.
SNMP Server	Users of the SNMP server exchange configuration information with the portal server. When the device detects that a user goes offline, it notifies the portal server. The portal server configures the device to delete user information through SNMP. Then, the portal server returns the offline page to the user.
SSID	Specify 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**:



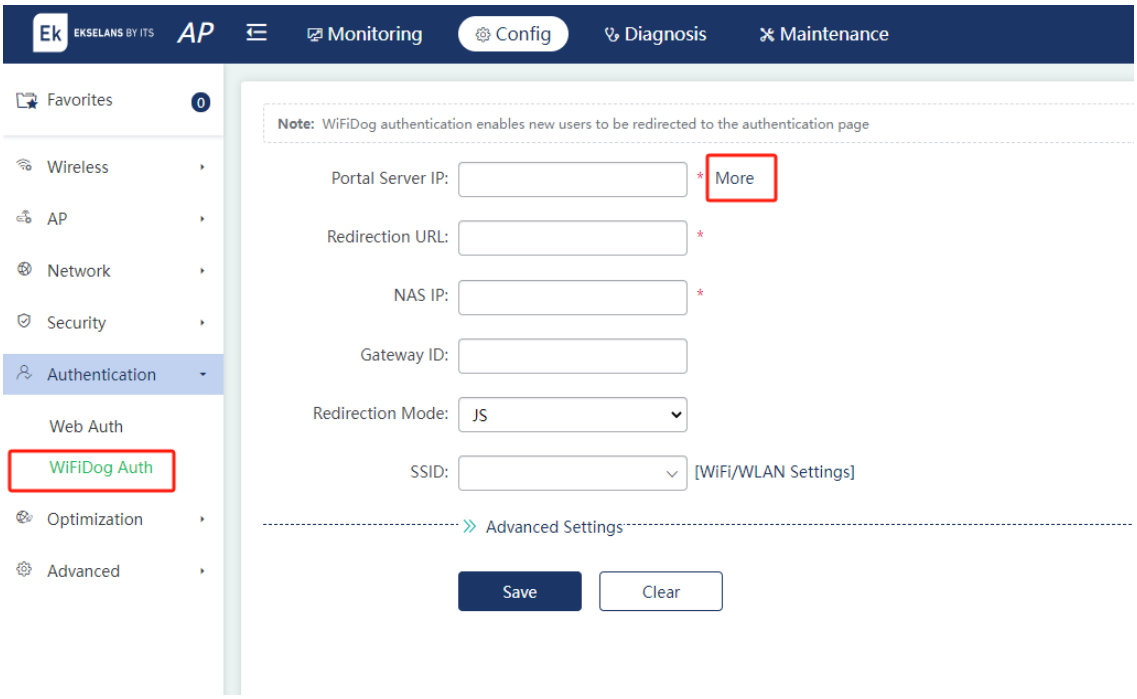
Parameter	Description
Portal Server IP	In template configuration mode, run the **ip { *ip-address* }** command to configure the server IP address. Server access requests are permitted by the device and rate limiting can be performed on requests transmitted to the server.

Parameter	Description
Redirection URL	Enter the URL that users will be redirected to, typically the URL of the portal authentication page.
Portal Key	Configure a key used for the communication between the device and the authentication server.
Authentication Server	To successfully apply ePortalv2, users need to configure authentication, authorization, and accounting (AAA) authentication. The authentication method list associates web-based authentication requests with the RADIUS server. The device selects the authentication method and server based on the authentication method list.
Accounting Server	(Mandatory) To successfully apply ePortalv2, users need to configure AAA accounting. Accounting is used to associate an accounting method with the server. In web-based authentication, accounting is implemented to record user information or fees.
SNMP Server	Users of the SNMP server exchange configuration information with the portal server. When the device detects that a user goes offline, it notifies the portal server. The portal server configures the device to delete user information through SNMP. Then, the portal server returns the offline page to the user.
SSID	Specify the Wi-Fi network to be configured with the ePortalv2.

5.5.2 WiFiDog Authentication

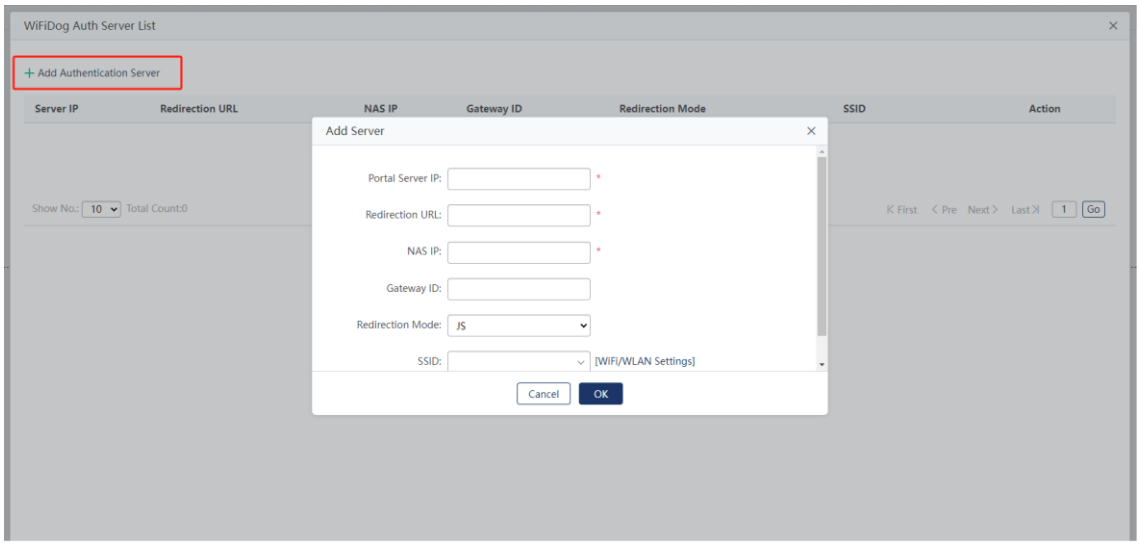
Choose **Config** > **Authentication** > **WiFiDog Auth**.

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



(1) Adding a WiFiDog Authentication Server

Click **Add Authentication Server**. Enter the fields in the pop-up window. Click **OK** and a message indicating operation success is displayed. The new entry is displayed in the list



Parameter	Description
Portal Server IP	Enter the IP address of the portal server.
Redirection URL	Enter the URL of the authentication page of the portal server.
NAS IP	Enter the IP address of the device to be managed by WiFiDog, which is

	used for communication with the server.
Gateway ID	Enter the ID of a gateway used by WiFiDog, which is the gateway SN by default.
Redirection Mode	Enter HTTP redirection or JavaScript redirection. JavaScript redirection is employed by default.
SSID	Enter a Wi-Fi network to be configured with WiFiDog authentication.

(2) Deleting a WiFiDog Authentication Server

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a WiFiDog authentication server.

(3) Edit a WiFiDog Authentication Server

Click **Edit** in the **Action** column of a WiFiDog authentication server. Edit the fields in the pop-up window. Click **OK** and a message indicating operation success is displayed. The modified server is displayed in the server list.

5.6 Network Optimization

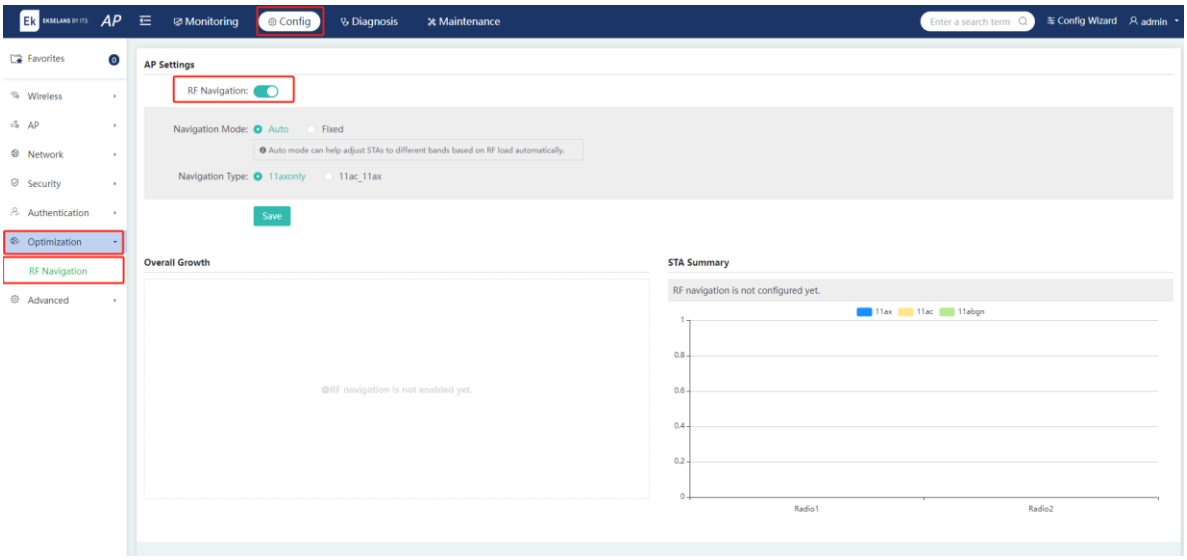
5.6.1 RF Navigation

Choose **Config** > **Optimization** > **RF Navigation**

Note

Some APs may not support this function. The actual menu shall prevail.

Enable **RF Navigation** and configure the **Navigation Mode** and **Navigation Type** to optimize RF performance.



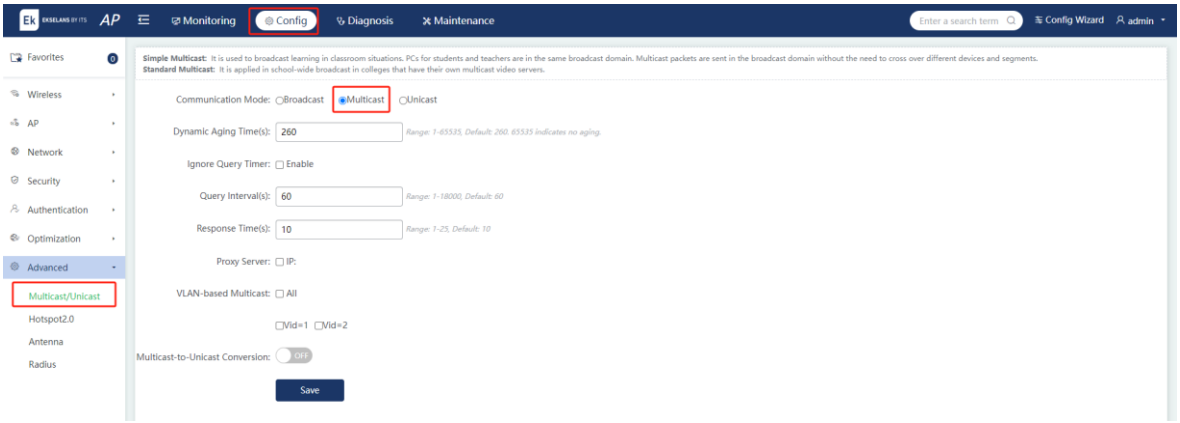
Parameter	Description	
Navigation Mode	Auto	In this mode, the AP can automatically steer a STA to the optimal radio based on the radio load utilization.
	Fixed	In this mode, the AP steers a STA to the corresponding radio, which remains unchanged despite differences in radio environments.
Navigation Type	You can enable the 802.11ax protocol only, or enable both 802.11ac and 802.11ax protocols.	

5.7 Advanced

5.7.1 Multicast/Unicast

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

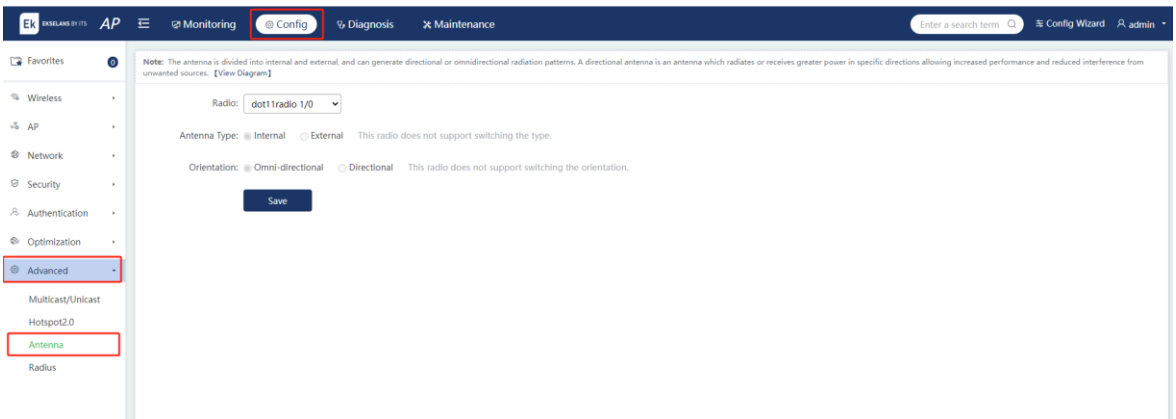
This function is used to configure the communication mode of a device as broadcast, multicast, or unicast.



5.7.2 Antenna

Choose **Config** > **Advanced** > **Antenna**.

RF antennas are categorized into built-in antennas and external antennas. Antenna orientations include directional and omnidirectional options. Directional antennas radiate the signal within a specific angle range, creating a cone-like radiation pattern. The type and direction of the RF connector can be adjusted based on the capability of the RF connector.



5.7.3 RADIUS

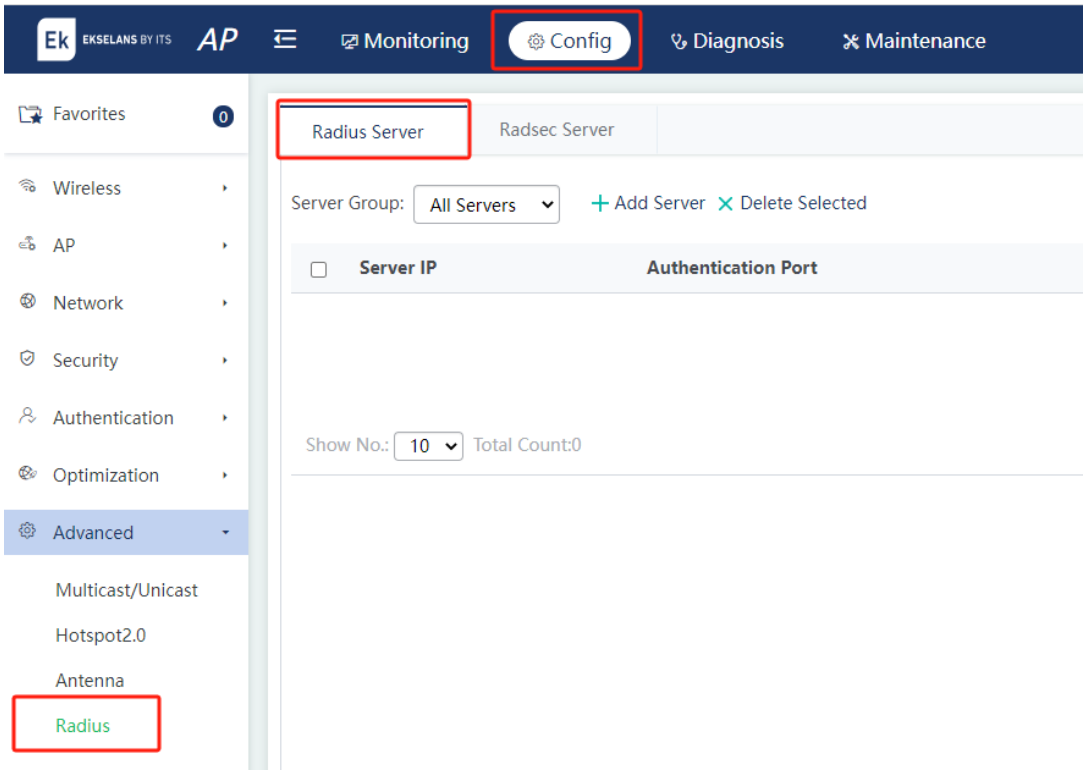
Choose **Config** > **Advanced** > **Radius**.

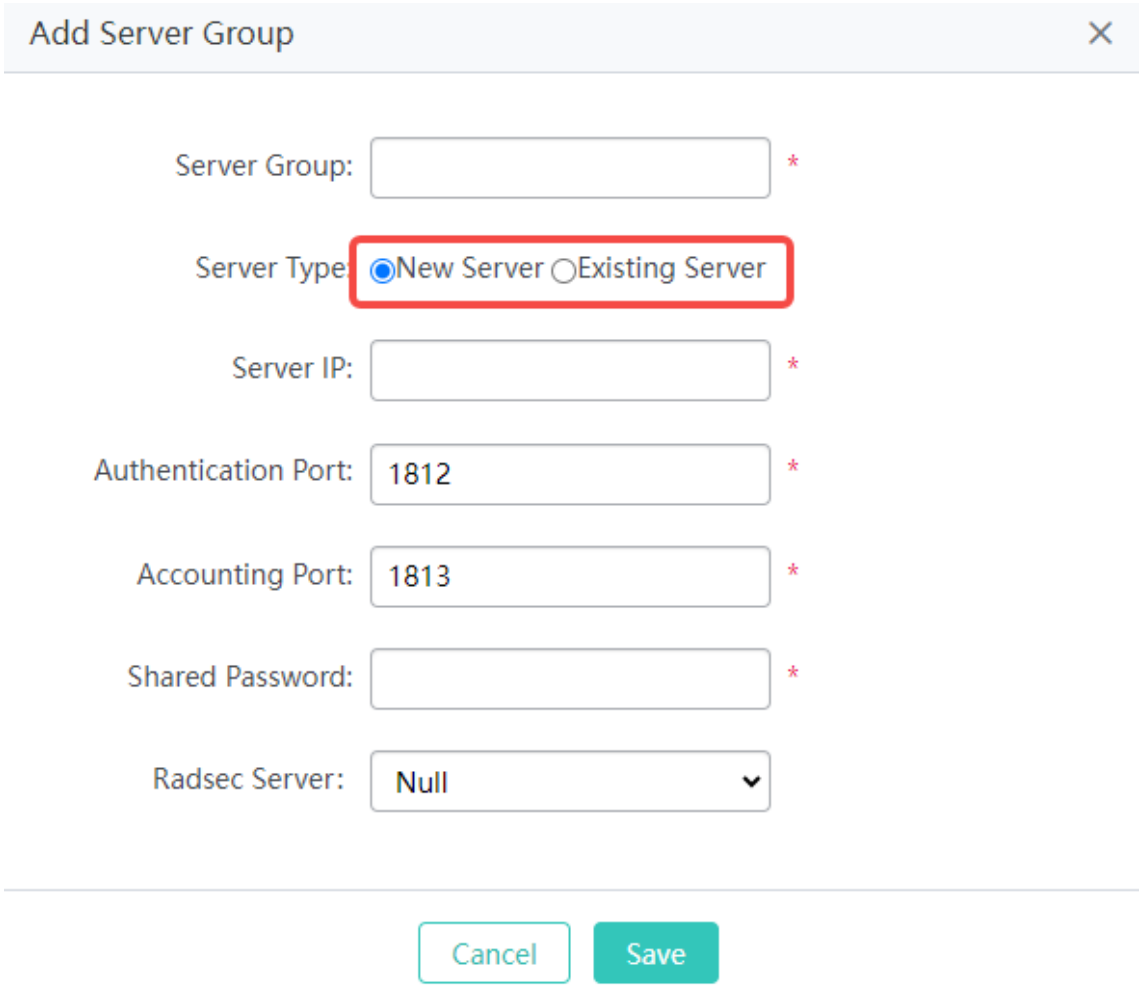
1. RADIUS Server

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

(1) Adding a Server Group

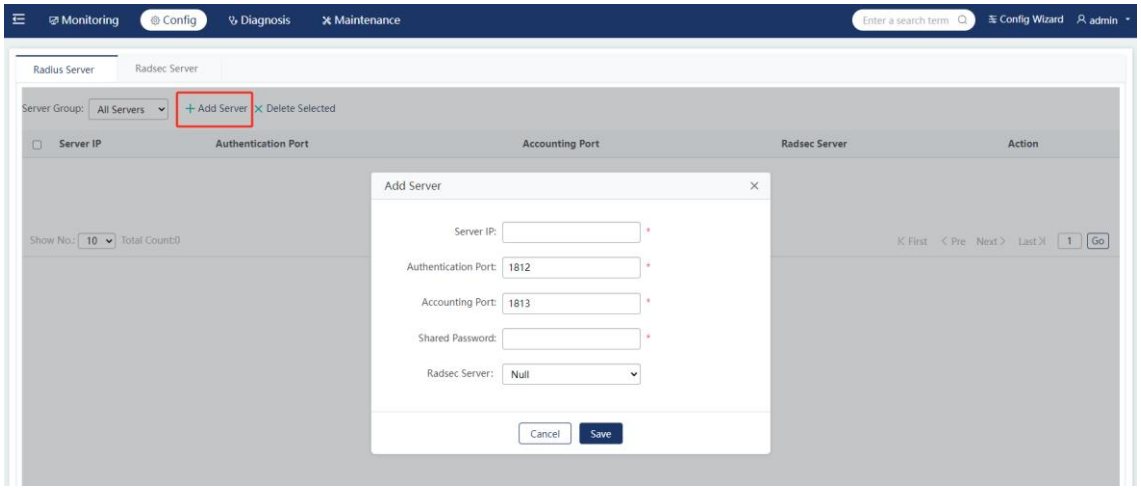
Click **Add Server Group** in the drop-down list. Enter the fields in the pop-up window. If you select **New Server** for the **Server Type** filed, one server group and one server will be added and the server belongs to the server group. If you select **Existing Server**, an existing server will be added to the server group.





(2) Adding a Server

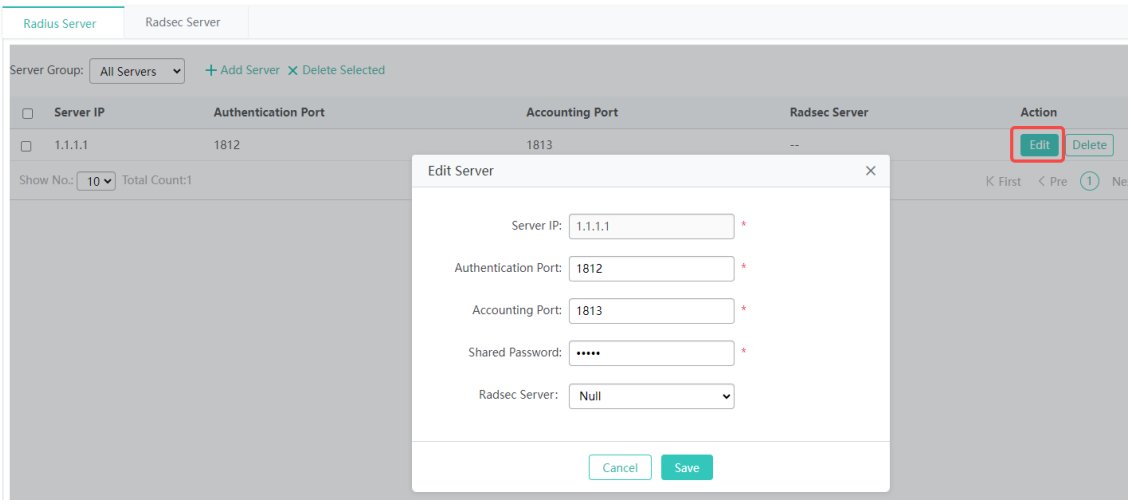
Select **All Servers** for the **Server Group** field. Click **Add Server**. Enter the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.



Parameter	Description
Server IP	Enter the IP address of a RADIUS server.
Authentication Port	Enter the UDP port number for RADIUS authentication. The value range is from 0 to 65535. The value 0 indicates that the host does not perform authentication.
Accounting Port	Enter the UDP port number for RADIUS accounting. The value range is from 0 to 65535. The value 0 indicates that the host does not perform accounting.
Shared Password	Enter the shared password for the communication between the network access server (routing device) and the RADIUS server.
Radsec Server	(Optional) Select the ID of the RadSec server, to which traffic is redirected from the RADIUS server. **Note** This field is not displayed if the device does not support the RadSec function.

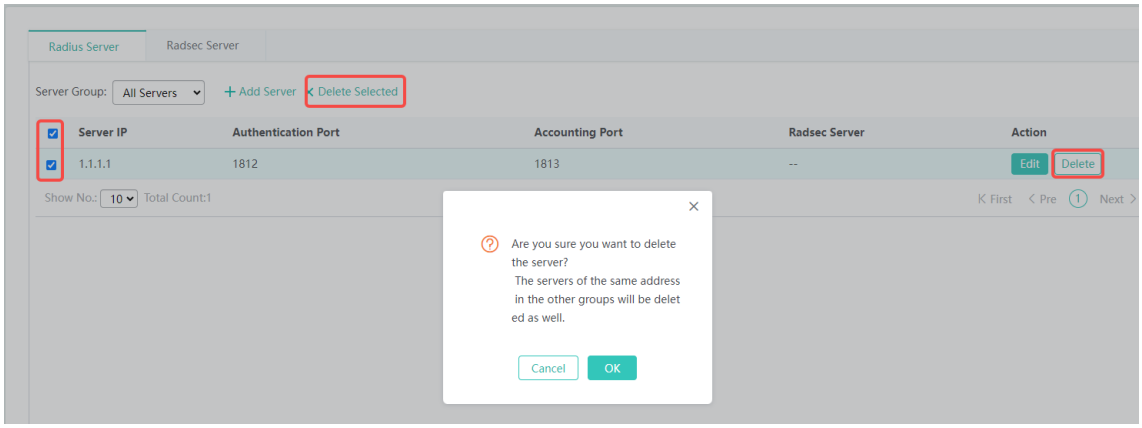
(3) Editing a Server

Click **Edit** in the **Action** column. Edit the parameters in the pop-up window. Click **Save**.



(4) Deleting a Server

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a server. To delete multiple servers, select the target servers in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch the servers.

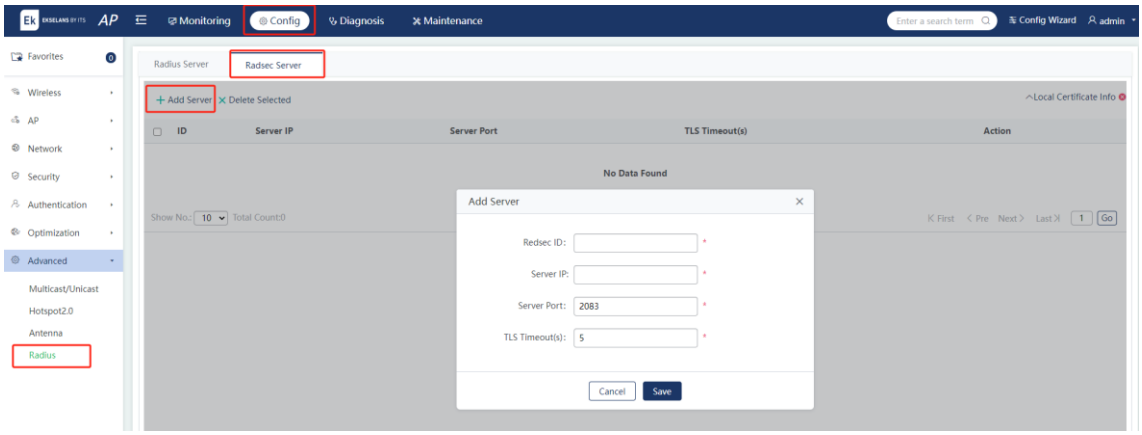


2. RadSec Server

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) Adding a Server

Click **Add Server**. Enter the fields in the pop-up window. Click **Save** and a message indicating operation success is displayed.

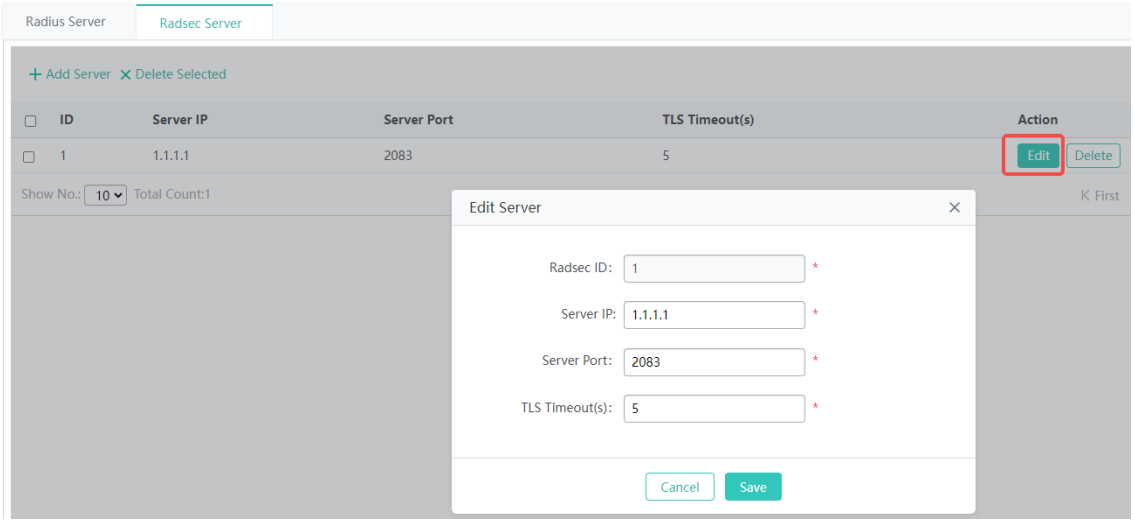


Parameter	Description
Radsec ID	Enter the unique ID of a RadSec server. The value is an integer in the range from 1 to 255.
Server IP	Enter the IP address of the RadSec server.
Server Port	Enter the port number of the RadSec server. The value range is from

	1 to 65535. The default value is 2083.
TLS Timeout(s)	Enter the TLS connection timeout. The value range is from 1 to 1000. The default value is 5.

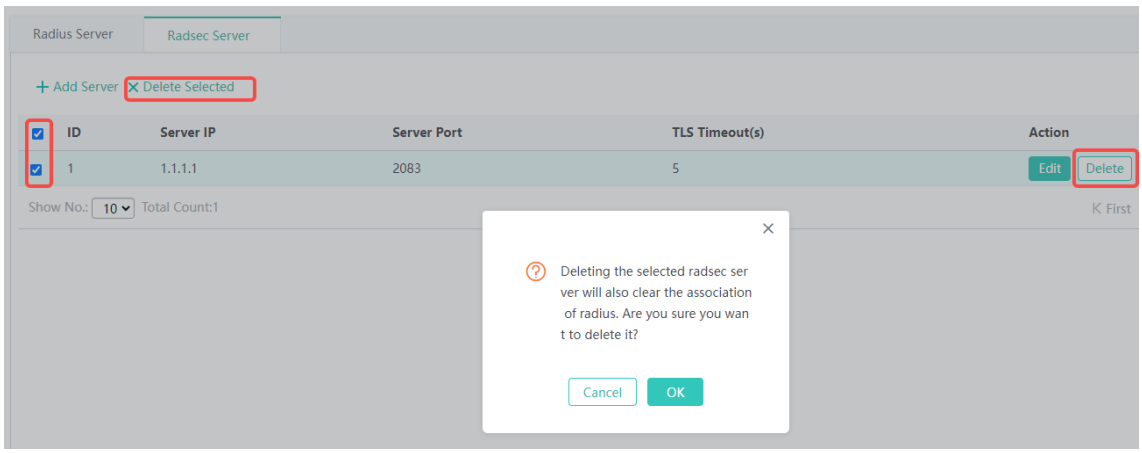
(2) Editing a Server

Click **Edit** in the **Action** column. Edit the parameters in the pop-up window. Click **Save**.



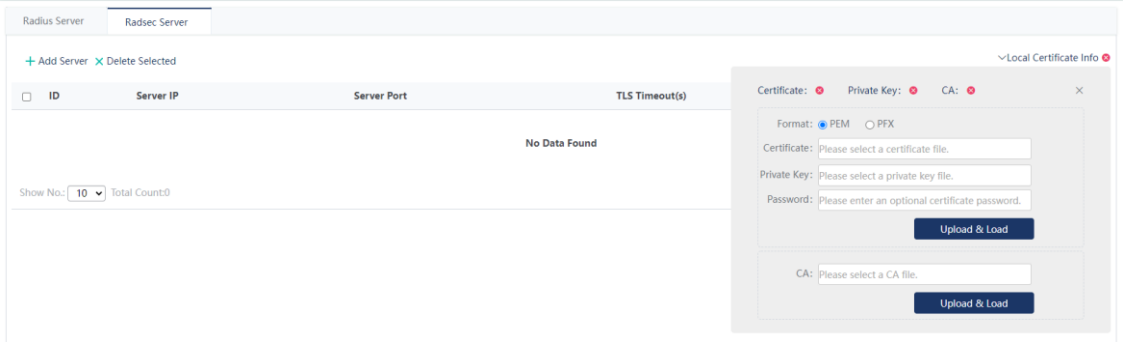
(3) Deleting a Server

Click **Delete** in the **Action** column and click **OK** in the pop-up window to delete a server. To delete multiple servers, select the target servers in the list. Click **Delete Selected**. Click **OK** in the pop-up window to batch the servers.



(4) Local Certificate Management

Click **Local Certificate Info**. The local certificate management window 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 indicating operation success is displayed. The PEM and PFX formats are supported. If the certificate file does not contain CA information, select a CA file and click **Upload & Load**.



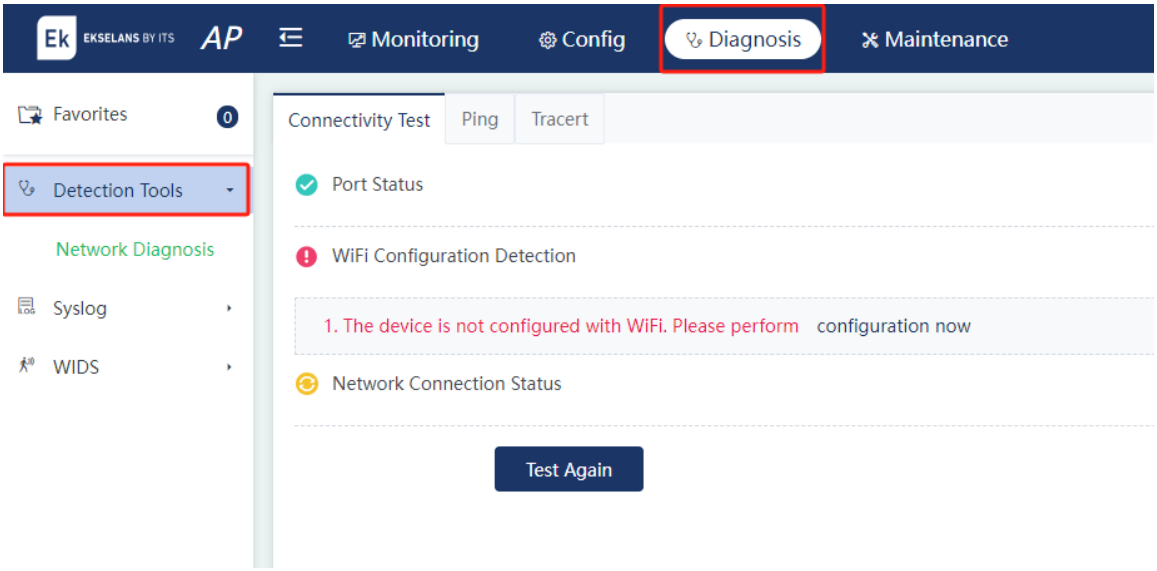
6 Diagnosis

6.1 Detection Tools

6.1.1 Network Diagnosis

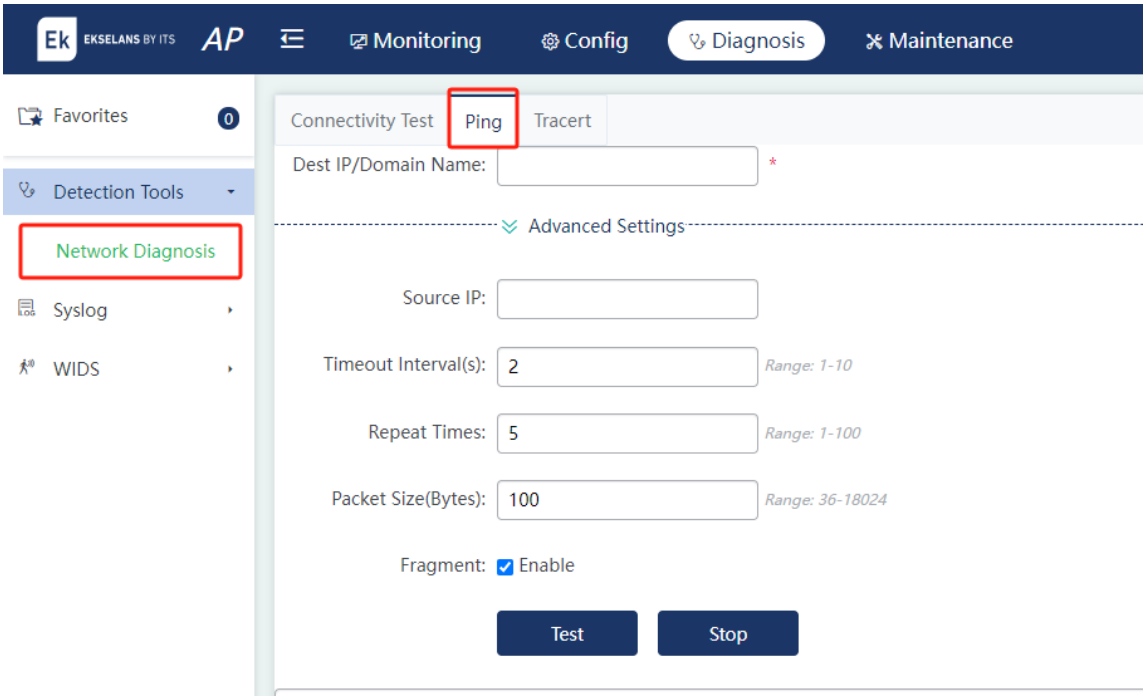
Choose **Diagnosis** > **Detection Tools** > **Network Diagnosis**.

1. Connectivity Test



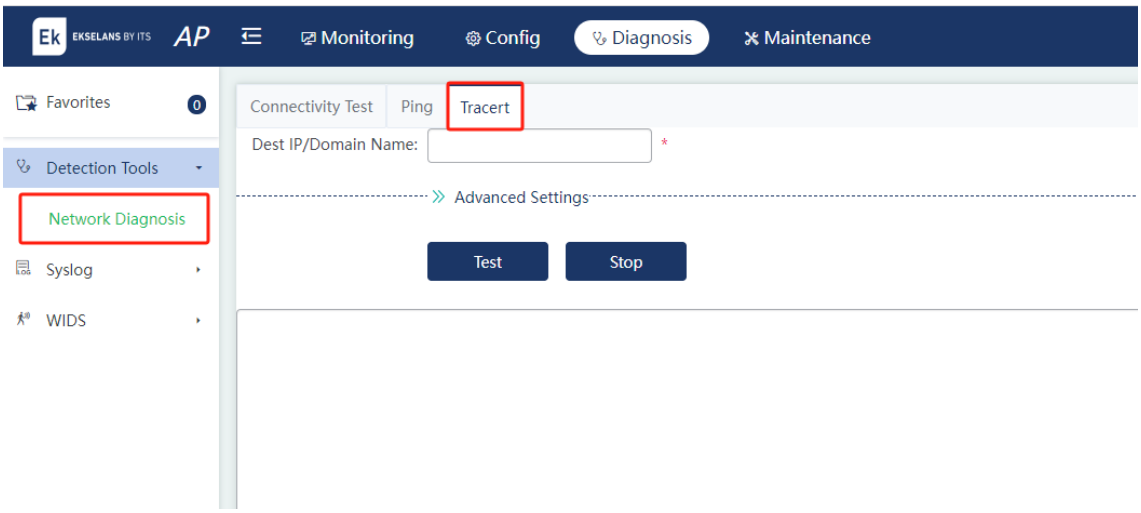
Detection Item	Description
Port Status	Check whether a port on the AP is Up.
WiFi Configuration Detection	Check whether a Wi-Fi network is configured on the AP.
Network Connection Status	Check whether the AP can communicate with an external network.

2. Ping



Parameter	Description
Dest IP/Domain Name	Enter the destination IP address or domain name to be pinged.
Source IP	Enter the source IP address of ping packets, that is, the local interface address of the device.
Timeout Interval(s)	Enter the timeout interval.
Repeat Times	Enter the number of data packets to be transmitted.
Packet Size(Bytes)	Enter the length of the data padding section in a data packet to be transmitted.
Fragment	Enter 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



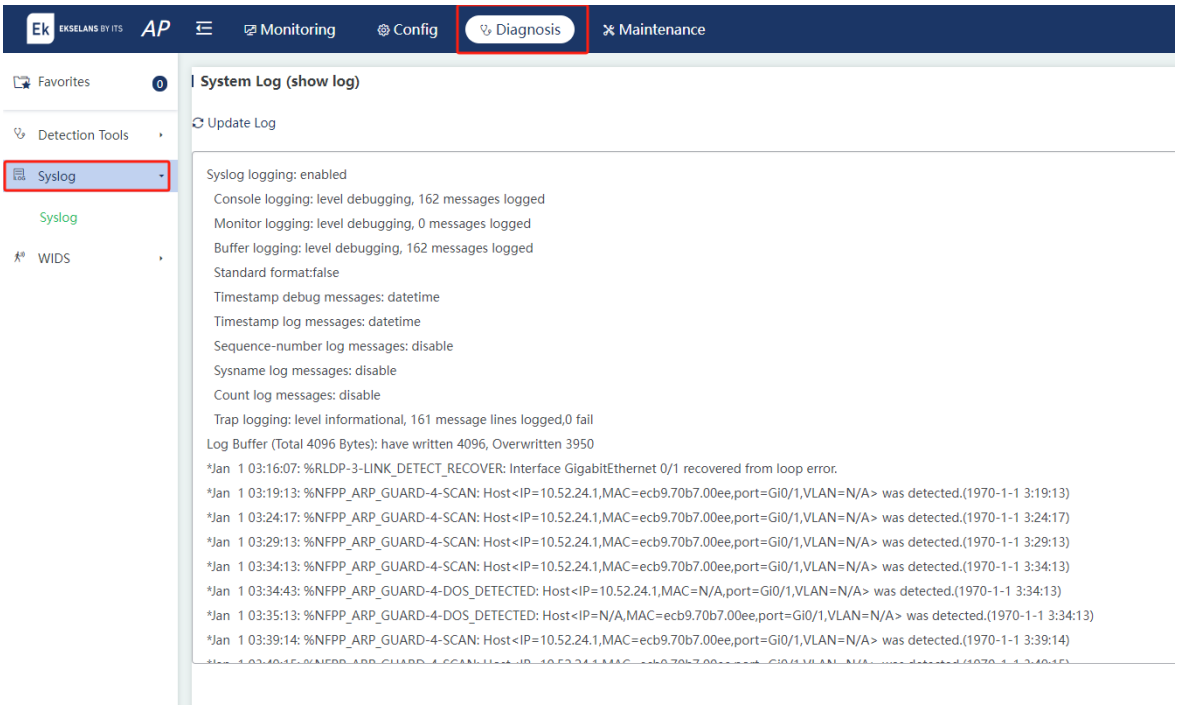
Parameter	Description
Dest IP/Domain name	Enter the Tracert destination address or domain name.
Source IP	Enter the Tracert source address, that is, the local interface address of the device.
Timeout Interval(s)	Enter the timeout interval.

6.2 Log

6.2.1 Syslog

Choose **Diagnosis** > **Syslog** > **Syslog**.

System logs can be used to help after-sales and R&D personnel locate problems. Click **Export Syslog** to download the syslog to the computer.



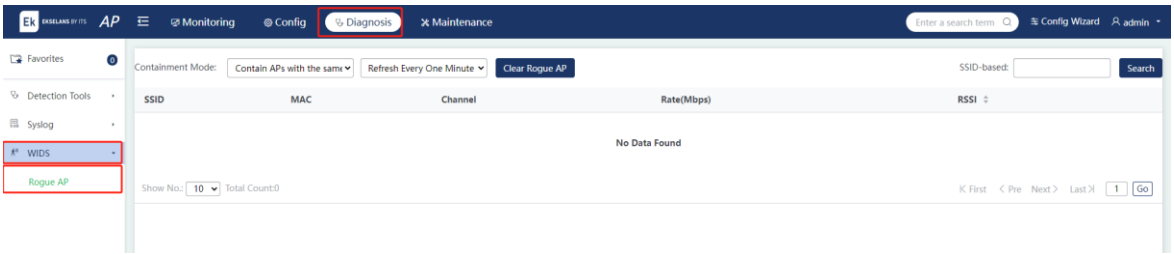
6.3 Wireless Intrusion Detection System

6.3.1 Rogue AP

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

Rogue APs may exist on a wireless network. They may have security vulnerabilities or be controlled by attackers, posing great threat to network security.

The following page displays potential rogue APs that are identified when rogue AP containment is enabled.



7 Maintenance

7.1 Settings

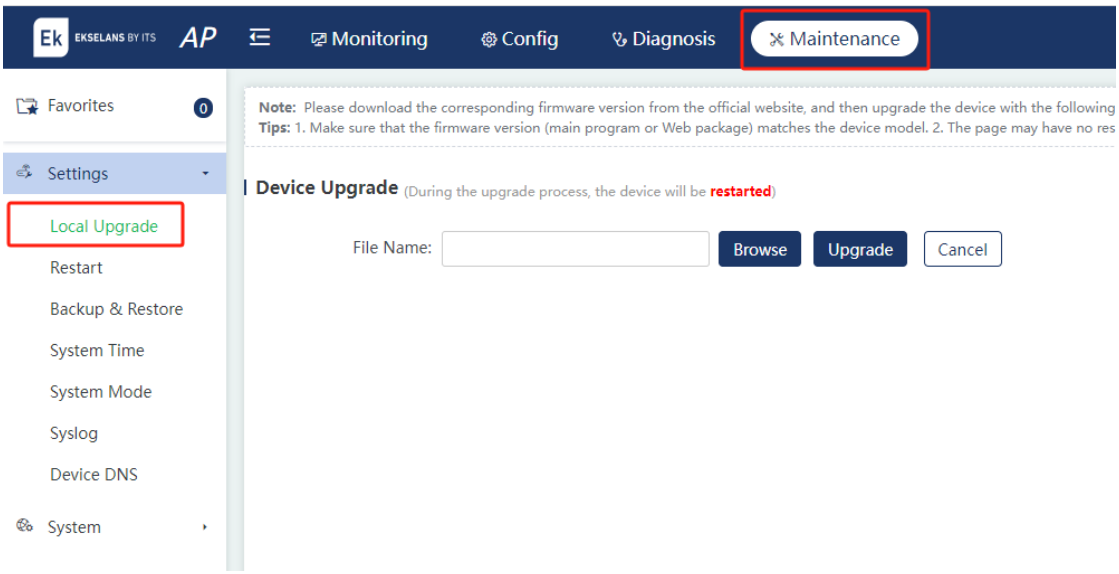
7.1.1 Local Update

Choose **Maintenance** > **Settings** > **Local Upgrade**.

Click **Browse** to select the downloaded .bin file. Click **Upgrade**.

Caution

- During the upgrade, the device will be restarted, causing network disconnection and service disruption. Therefore, upgrade the device when services are not affected or during off-peak hours.
- The upgrade process takes some time. During the upgrade, avoid performing any operation on the web page. Otherwise, the upgrade process will be interrupted.
- During the upgrade, the web page may not respond temporarily. In this case, do not power off or restart the device until the upgrade is successful.



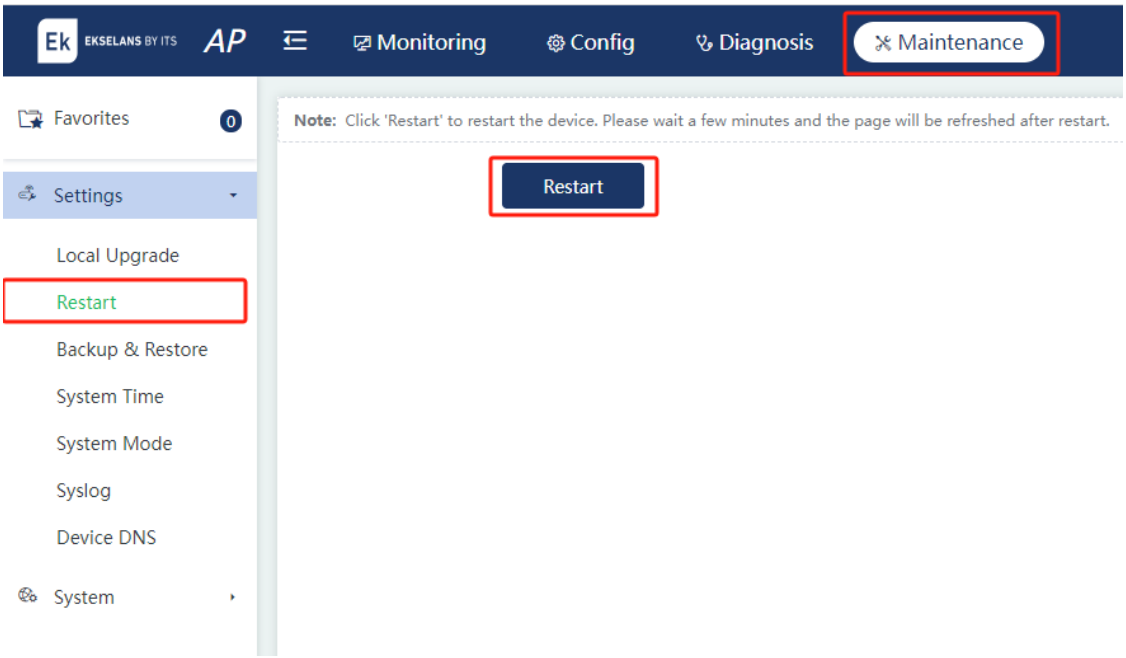
7.1.2 Restart

Choose **Maintenance** > **Settings** > **Restart**.

Click **Restart** to restart the AP.

Caution

Restarting the device will cause network disconnection and service disruption. Therefore, upgrade the device when services are not affected or during off-peak hours.

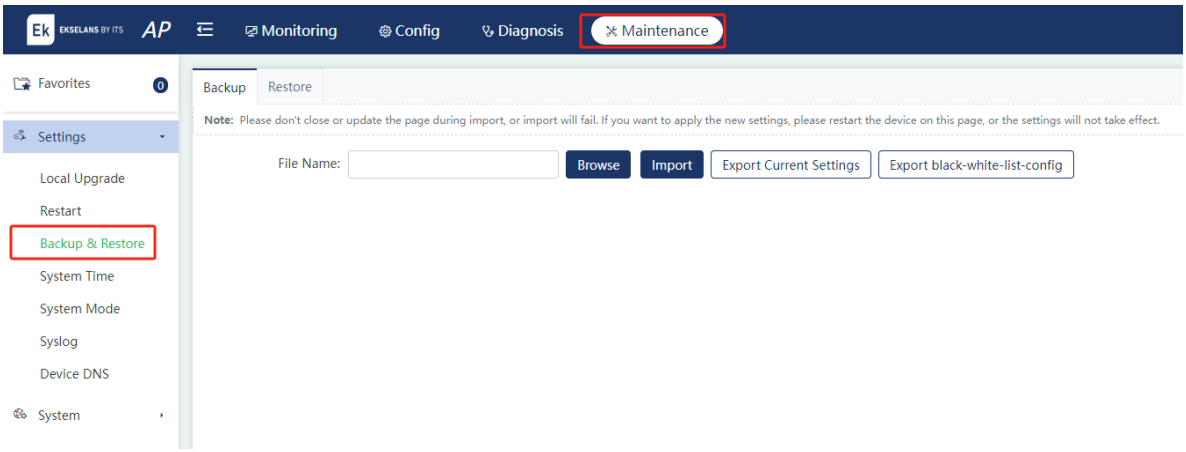


7.1.3 Configuration Management

Choose **Maintenance** > **Settings** > **Backup & Restore**.

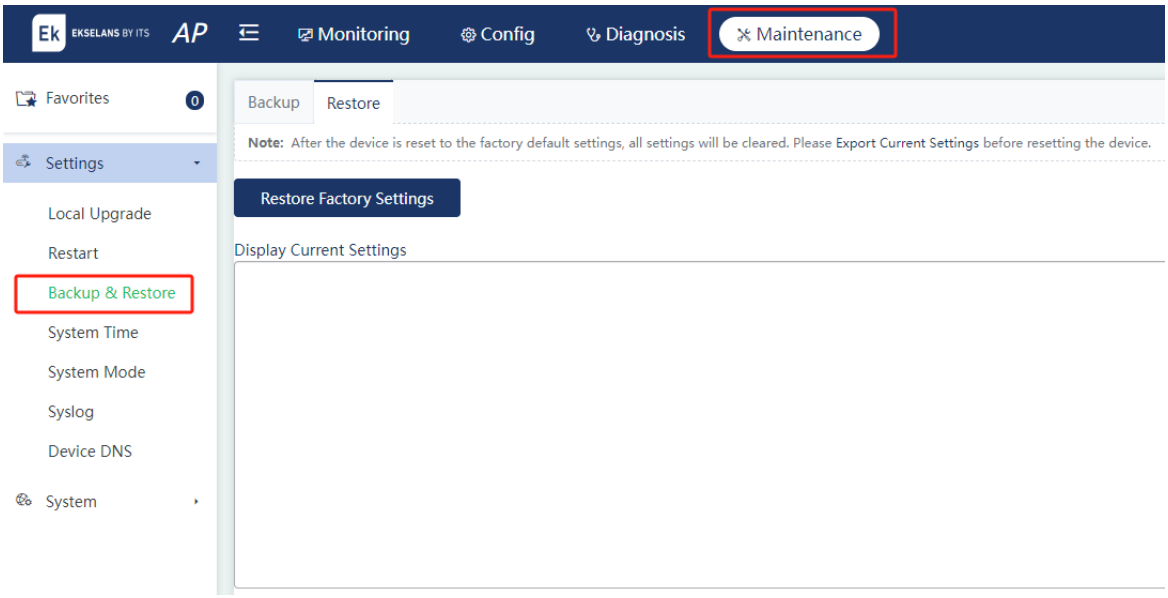
1. Backup

Back up the configuration file on the device. You can import or export configurations to perform batch operations, facilitating configuration management.



2. Restore

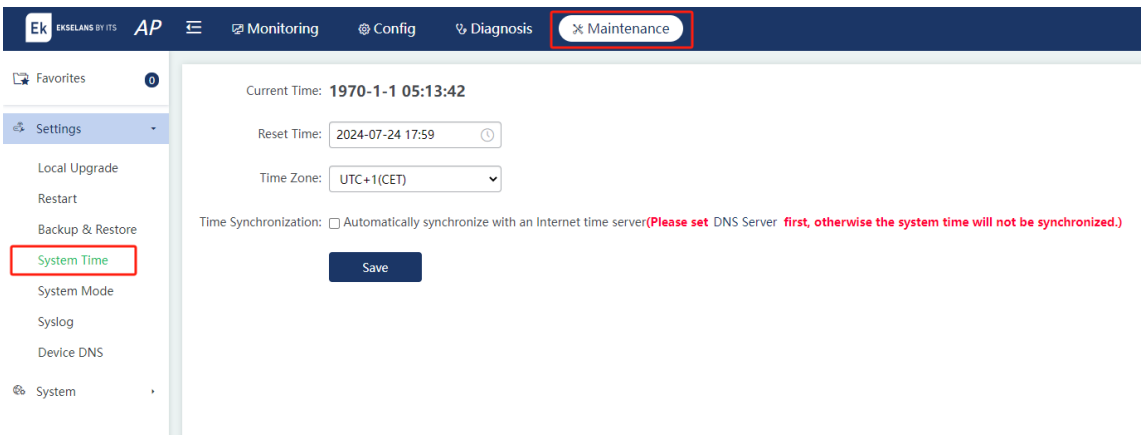
After restoring the device to factory settings, use the default IP address to access web. Restoring the device to factory settings will clear all configurations. Therefore, exercise with caution.



7.1.4 System Time

Choose **Maintenance** > **Settings** > **System Time**.

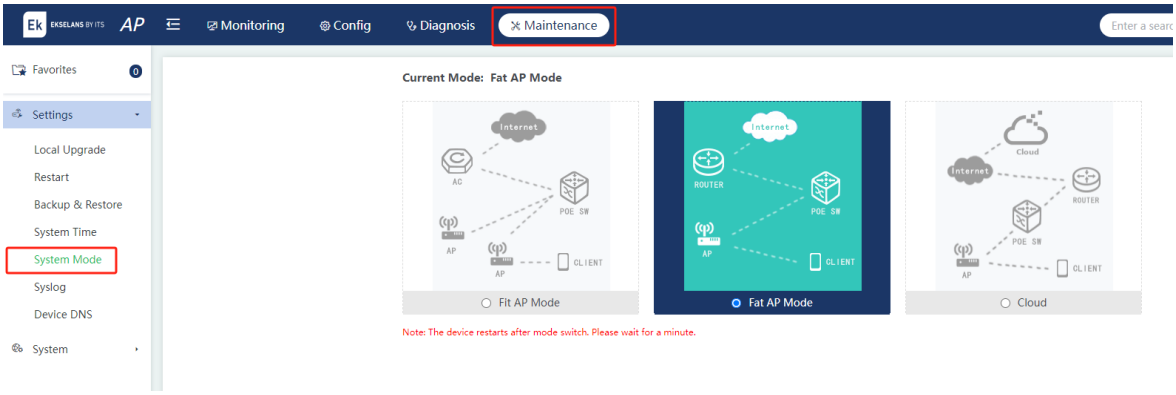
Set the system time based on the time zone where the device is located to ensure accurate device information.



7.1.5 System Mode

Choose **Maintenance** > **Settings** > **System Mode**.

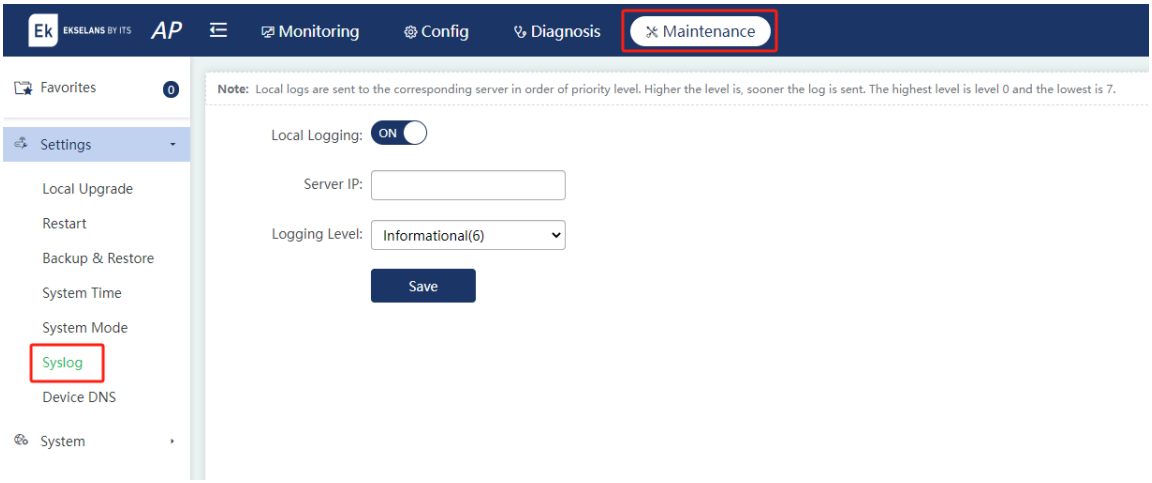
Select the system mode of the AP. **Fit AP Mode**, **Fat AP Mode**, and **Cloud Mode** are supported.



7.1.6 Log Server

Choose **Maintenance** > **Settings** > **Syslog**.

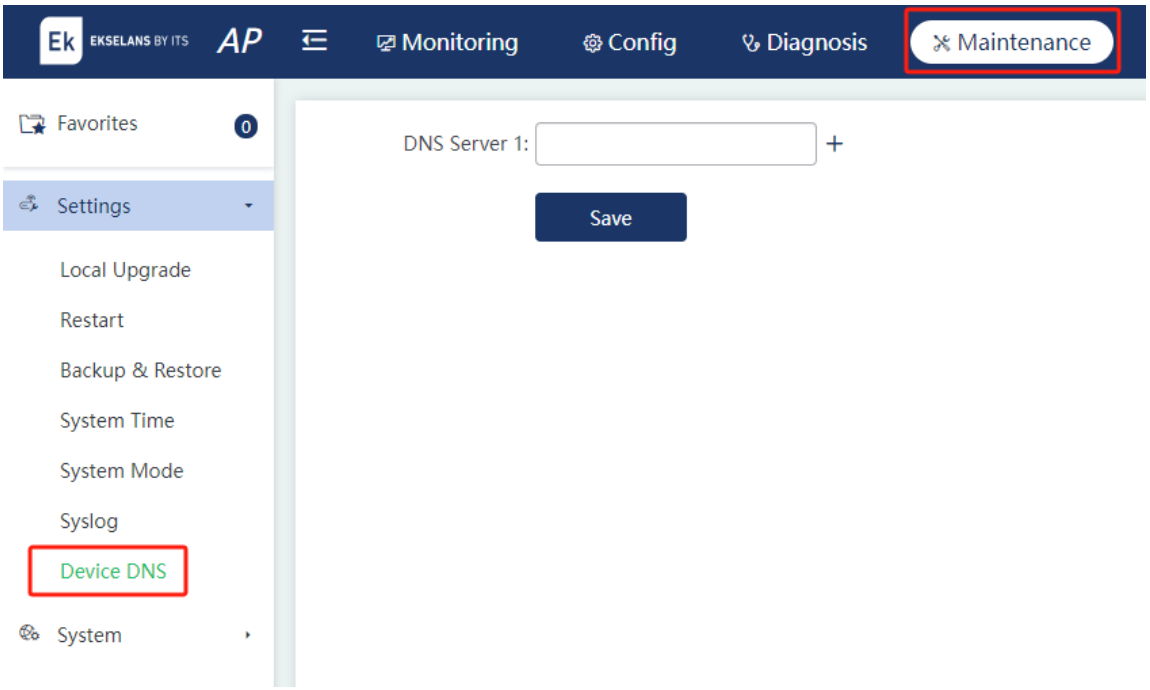
The device sends local logs to the server for storage. Historical logs are stored for ease of query.



7.1.7 DNS

Choose **Maintenance** > **Settings** > **Device DNS**.

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



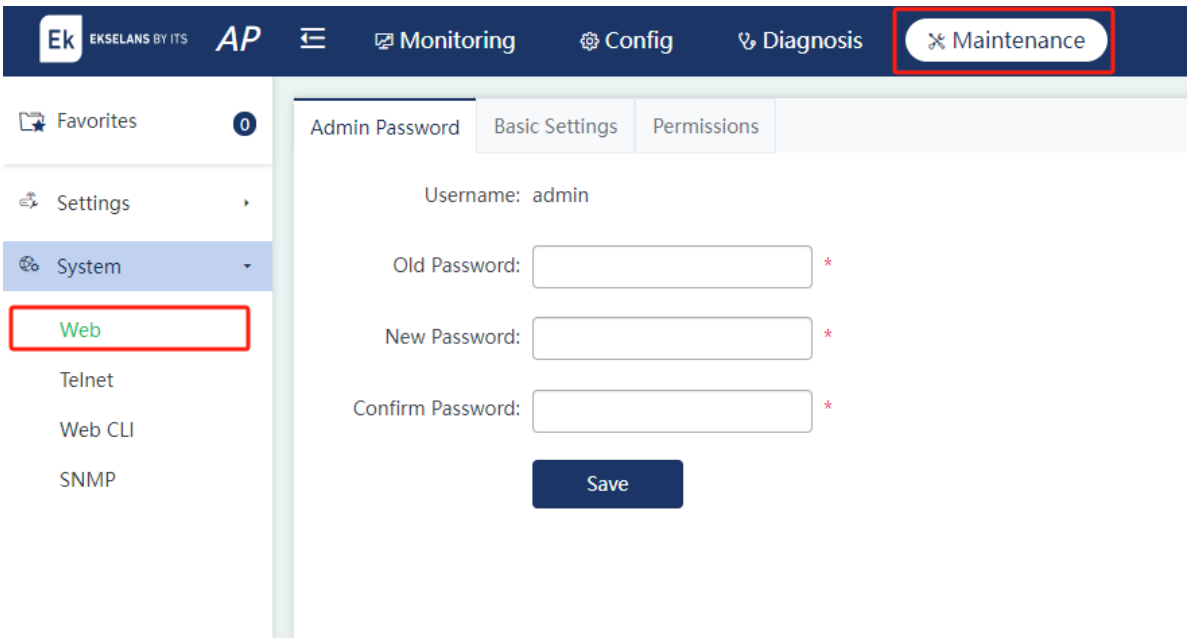
7.2 System

7.2.1 Web Management

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

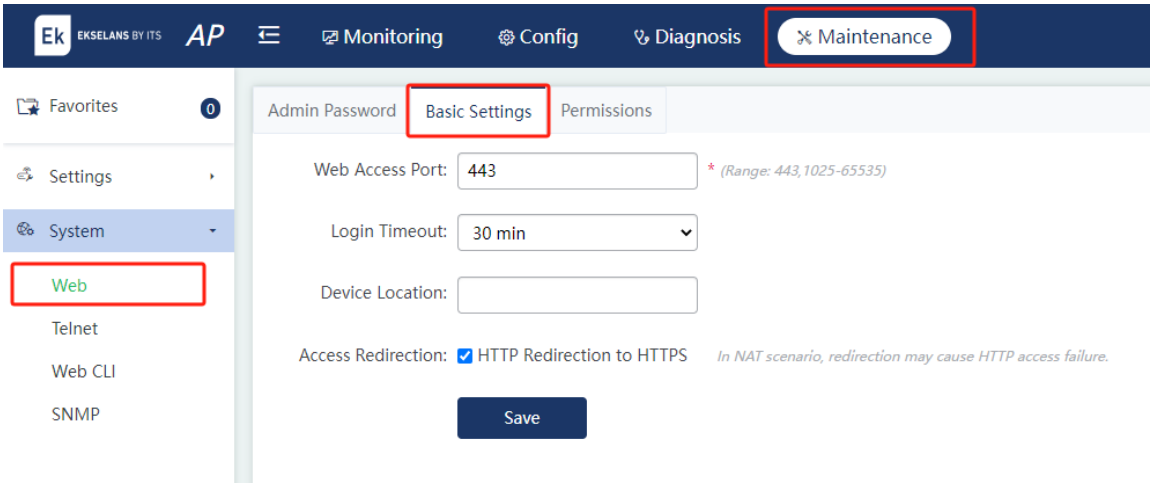
1. Admin Password

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



2. Basic Settings

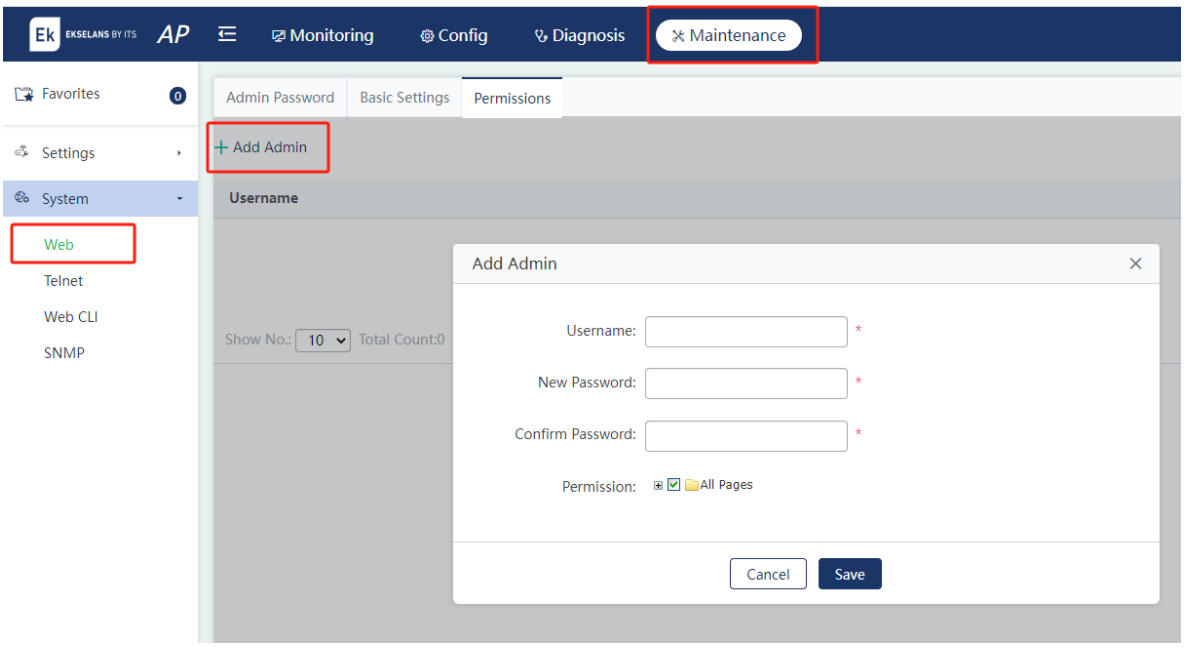
To facilitate device management, configure the device location on the **Basic Settings** page. Set the web access port and login timeout. When the login timeout expires, the web system automatically exits to ensure system security. If the device supports the configuration of **Limit logins**, set the maximum number of users who can log in to the device simultaneously using the same account (the default value is 10).



3. Permissions

There can be multiple administrators on the web management system. Administrators at different levels have different management permissions. You can assign the management permission of a specified page to a specified administrator. The default user of the system is admin.

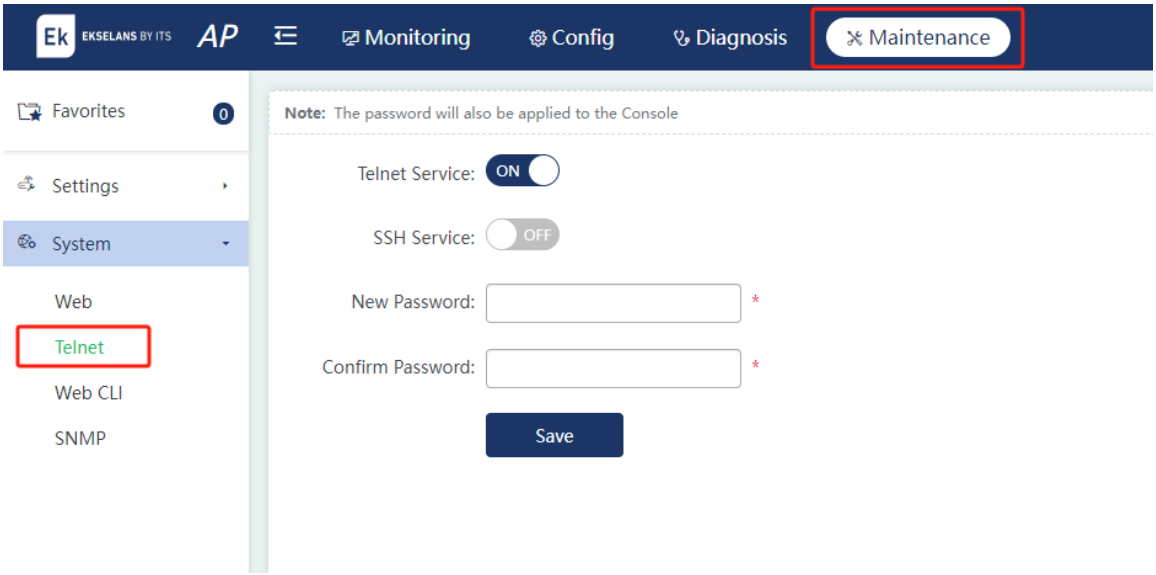
Click **Add Admin**. Set the fields for an administrator in the pop-up window, including the username, password, and permissions. Click **Save**.



7.2.2 Telnet

Choose **Maintenance** > **System** > **Telnet**.

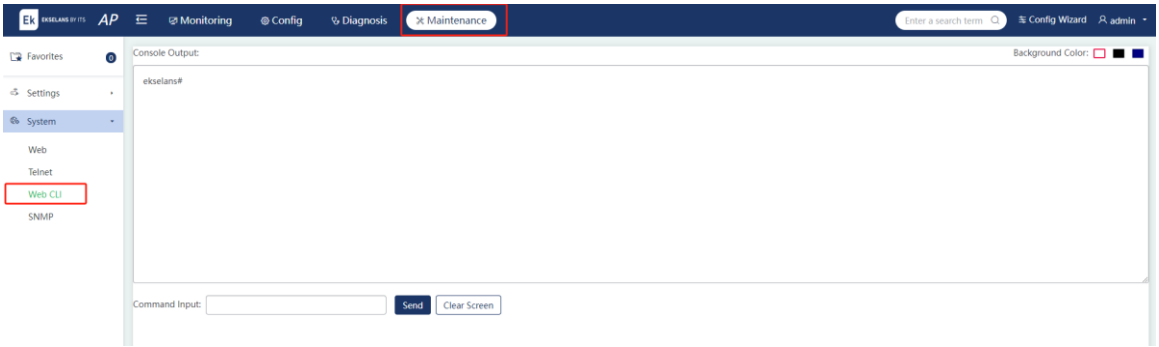
The Telnet feature enhances the system security and ensures secure information exchange. On the **Telnet** page, **Telnet Service** and **SSH Service** can be enabled or disabled, and the password can be configured.



7.2.3 Web CLI

Choose **Maintenance** > **System** > **Web CLI**.

CLI commands can be delivered through the web CLI.



7.2.4 SNMP

Choose **Maintenance** > **System** > **SNMP**.

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