EKSELANS BY ITS

MANUAL DE USUARIO

AX 3000 OLP

331021

Punto de Acceso WiFi de exterior
WiFi6 (802.11ax) 3000Mbps
Puerto de entrada PoE 1G
Puerto de enlace ascendente SFP 1G/2,5G
1 Puerto de Consola
PoE IN / DC-IN

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

Derechos de autor

Renuncia

Los productos, servicios o funciones que compre están sujetos a contratos y términos comerciales. Es posible que algunos o todos los productos, servicios o características descritos en este documento no estén dentro del alcance de su compra o uso. A menos que se acuerde lo contrario en el contrato, Ekselans by ITS no hace ninguna declaración o garantía expresa o implícita por el contenido de este documento.

Debido a actualizaciones de la versión del producto u otros motivos, el contenido de este documento se actualizará de vez en cuando. Ekselans by ITS se reserva el derecho de modificar el contenido del documento sin previo aviso ni aviso.

Este manual es solo para referencia. Ekselans by ITS se esfuerza por garantizar la exactitud del contenido y no asumirá ninguna responsabilidad por pérdidas y daños causados debido a omisiones, inexactitudes o errores en el contenido

Prefacio

Público al que va dirigido

Este documento está destinado a:

- Ingenieros de redes
- Soporte técnico e ingenieros de servicio
- Administradores de red

Soporte técnico

- Sitio web de la empresa: https://www.ek.plus/
- Consultar Sitio Web: https://www.ek.plus/contacto/
- Correo electrónico de soporte: soporte@ek.plus

Convenios

1. Signos

Los signos utilizados en este documento se describen de la siguiente manera:

Advertencia

Una alerta que llama la atención sobre reglas e información importantes que, si no se entienden o no se siguen, pueden provocar la pérdida de datos o daños en el equipo.

Cautela

Una alerta que llama la atención sobre información esencial que, si no se comprende o se sigue, puede provocar un error de función o una degradación del rendimiento.

Nota

Una alerta que contiene información adicional o complementaria que, si no se entiende o se sigue, no tendrá consecuencias graves.

Especificación

Una alerta que contiene una descripción de la compatibilidad con el producto o la versión.

2. Nota

El manual ofrece información de configuración (incluido el modelo, el tipo de puerto y la interfaz de línea de comandos) solo con fines indicativos. En caso de discrepancia o inconsistencia entre el manual y la versión real, prevalecerá la versión real.

1 Descripción general del producto

1.1 Acerca del punto de acceso AX 3000 OLP

El AX 3000 OLP es un punto de acceso de doble radio y flujo diseñado para cubrir áreas exteriores. Compatible con el estándar IEEE 802.11ax, el punto de acceso ofrece una velocidad de datos combinada de 2,976 Gbps, con hasta 574 Mbps en la banda de 2,4 GHz y 2,402 Gbps en la banda de 5 GHz. El punto de acceso proporciona un puerto SFP de 2,5 GE y un puerto eléctrico de 1 GE.

1.2 Características de hardware

El punto de acceso AX 3000 OLP proporciona dos conectores de radiofrecuencia (RF), un puerto Ethernet 10/100/1000 BASE-T con negociación automática, un puerto SFP 2.5GE, un puerto de consola y un conector de CC. El punto de acceso puede ser alimentado por una fuente de alimentación PoE o CC.

Figure 1-1 Apariencia

Figure 1-2 Vista frontal del punto de acceso

Figure 1-3 Vista lateral del punto de acceso

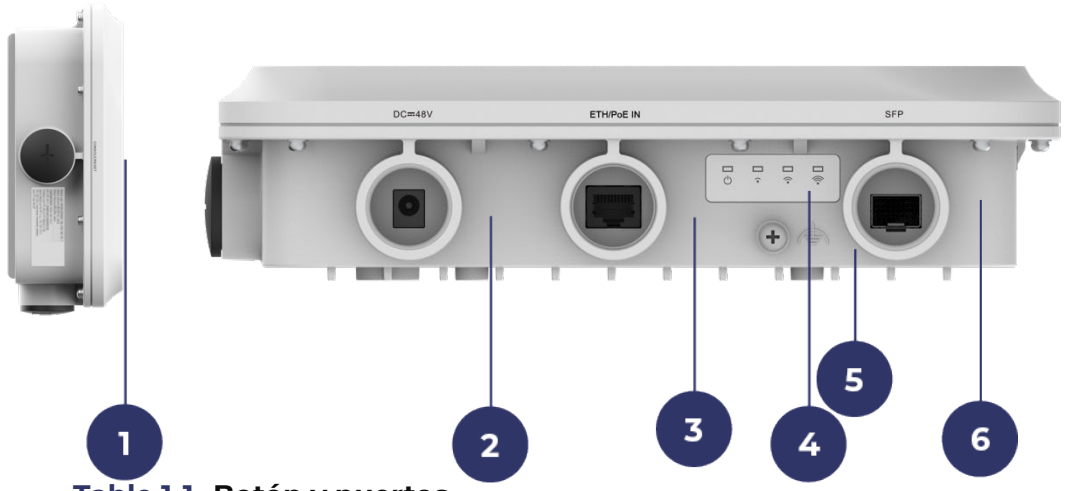


Table 1-1 Botón y puertos

No.	Artículo	Descripción
1	Consola/Reiniciar	El puerto de la consola se utiliza para administrar dispositivos. El botón de reinicio se utiliza para reiniciar el punto de acceso o restaurar el punto de acceso a la configuración de fábrica.

No.	Artículo	Descripción
2	Conector de CC	Conectado a la fuente de alimentación de CC
3	Puerto Ethernet/PoE	Puerto de servicio de enlace ascendente para la transmisión de datos, de conformidad con el estándar IEEE 802.3af/at
4	LED	Indica el estado del sistema, incluido un LED de estado del sistema y tres LED RSSI
5	Tornillo de conexión a tierra	Asegura el cable de conexión a tierra
6	Puerto SFP	Puerto de servicio de enlace ascendente para la transmisión de datos

Nota

La placa de identificación se encuentra en la parte inferior del punto de acceso.

1.3 Contenido del paquete

Table 1-2 Contenido del paquete

Artículo	Cantidad
Punto de acceso AX 3000 OLP	1
Conjunto de placa de montaje (incluye una placa de montaje y un brazo de montaje)	1
Soporte de montaje	1
Tornillo M5	4
Tornillo M8	2
Anclaje de expansión M6 x 50 mm	4
Abrazadera de manguera	2
Prensaestopas para cable Ethernet	2
Prensaestopas para cable de fibra óptica	1
Tapa antipolvo	3

Artículo	Cantidad
Cable de puesta a tierra	1
Tarjeta de garantía	1
Guía de referencia e instalación de hardware	1

1.4 Especificaciones técnicas

1.4.1 Dimensiones y peso

Table 1-3 Dimensiones y peso

Dimensiones y peso	AX 3000 OLP
Dimensiones físicas (ancho × alto)	Punto de acceso: 251 mm × 168 mm × 64 mm (9,88 pulgadas x 6,61 pulgadas x 2,52 pulgadas) Conjunto de la placa de montaje: 130 mm × 231 mm × 39 mm (5,12 pulgadas x 9,09 pulgadas x 1,54 pulgadas) Soporte de montaje: 120 mm × 124 mm × 43 mm (4,72 pulgadas × 4,88 pulgadas × 1,69 pulgadas)
Peso	Punto de acceso: 1,0 kg (2,20 libras) Montaje de la placa de montaje: 0,6 kg (1,32 libras) Soporte de montaje: 0,3 kg (0,66 libras)
Instalación	Montaje en techo/pared/poste
Opción de bloqueo	No se admite
Dimensiones del soporte de montaje (ancho × profundo × alto)	Montaje de la placa de montaje: 100 mm × 100 mm (3,94 pulgadas x 3,94 pulgadas) Soporte de montaje: 65 mm × 105 mm (2,56 pulgadas x 4,13 pulgadas)
Diámetro del orificio de montaje	Montaje de la placa de montaje: 7 mm (0,28 pulgadas) Soporte de montaje: 9 mm (0,35 pulgadas)
Patrón de poste de montaje	De 50 mm a 140 mm (1,97 pulgadas x 5,51 pulgadas)

1.4.2 Especificaciones de la radio

Table 1-4 Especificaciones de la radio

Especificaciones de la radio	AX 3000 OLP
Diseño de radio	Doble radio Hasta cuatro flujos espaciales Radio 1: 2,4 GHz, 2 flujos espaciales: 2 x 2, MU-MIMO Radio 2: 5 GHz, 2 flujos espaciales: 2 x 2, MU-MIMO
Radio en funcionamiento	Radio1: 802.11b/g/n/ax, de 2,400 GHz a 2,4835 GHz Radio2: 802.11a/n/ac/ax, 5.150 GHz a 5.350 GHz, 5.470GHz~5.850GHz Nota: La radio operativa es específica de cada país.
Velocidad de datos máx.	2,4 GHz: 574 Mbps 5 GHz: 2.402 Gbps Combinado: 2.976 Gbps
Tipo de antena	Antenas inteligentes incorporadas
Ganancia de antena	2,4 GHz: 4 dBi 5 GHz: 6 dBi
Máx. Potencia de transmisión	28 dBm Nota: La potencia de transmisión depende de cada país.
Ajuste de potencia	Configurable en incrementos de 1 dBm
Modulación	802.11b: BPSK, QPSK, CCK 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
Sensibilidad de recepción	802.11b: –91 dBm (1 Mbps), –88 dBm (5 Mbps), –85 dBm (11 Mbps) 802.11a/g: –89 dBm (6 Mbps), –80 dBm (24 Mbps), –76 dBm (36 Mbps), –71 dBm (54 Mbps) 802.11n: –83 dBm@MCS0, –65 dBm@MCS7, –83 dBm@MCS8, –65 dBm@MCS15 802.11ac HT20: –83 dBm (MCS0), –57 dBm (MCS9) 802.11ac HT40: –79 dBm (MCS0), –57 dBm (MCS9) 802.11ac HT80: –76 dBm (MCS0), –51 dBm (MCS9) 802.11ax HE80: –76 dBm (MCS0), –49 dBm (MCS11) 802.11ax HE160: –45 dBm (MCS10), –43 dBm (MCS11)

1.4.3 Especificaciones del puerto

Table 1-5 Especificaciones del puerto

Especificaciones del puerto	AX 3000 OLP
Bluetooth	Bluetooth 5.0
Puerto de servicio fijo	Uplink: Un puerto Ethernet 10/100/1000Base-T con negociación automática, compatible con IEEE 802.3af/at Un puerto SFP 2.5GE, conformidad con 1GE SFP
Puerto de administración fijo	Un puerto de consola RJ45
LED de estado	Un LED de estado del sistema Tres LED RSSI
Botón	Un botón de reinicio

1.4.4 Suministro y consumo de energía

Table 1-6 Suministro y consumo de energía

Suministro y consumo de energía	AX 3000 OLP
Fuente de alimentación de entrada	1. Fuente de alimentación de CC (48 V/0,35 A) 2. Fuente de alimentación PoE/PoE+ (compatible con IEEE 802.3af/at)
Consumo máx. de energía	12,95 W

Cautela

- Si el punto de acceso está alimentado por una fuente de alimentación PoE, asegúrese de que el equipo de suministro de energía (PSE) sea compatible con 802.3af.
- El punto de acceso adopta un diseño sin ventilador. Por lo tanto, mantenga suficiente espacio libre alrededor del punto de acceso para la circulación de aire.

1.4.5 Medio ambiente y confiabilidad

Table 1-7 Cumplimiento de la norma

Medio ambiente y confiabilidad	AX 3000 OLP
Temperatura	Temperatura de trabajo: –10 °C a +65 °C (14 °F a 149 °F) Temperatura de almacenamiento: –40 °C a +85 °C (–40 °F a +185 °F) A una altitud que oscila entre 3000 m y 5000 m (9842.52 pies a 16404.20 pies.), cada vez que la altitud aumenta en 166 m (546 pies), la temperatura máxima disminuye en 1 °C (1,8 °F).
Humedad	Humedad de funcionamiento: 0% a 100% HR (sin condensación) Humedad de almacenamiento: 0% a 100% HR (sin condensación)
Clasificación IP	IP68
Clasificación anticorrosión	24 Días
Cumplimiento normativo	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 Parte 15, EN IEC 62311, IEC 62368-1, EN 62368-1 e IEC 60950-22

1.5 LED y botón

Nota

La descripción del LED se aplica a los modos de ajuste y grasa, a menos que se especifique lo contrario.

Table 1-8 Estado del LED

Estado	Frecuencia	Descripción
Apagado	N/A	El punto de acceso no está encendido. El punto de acceso está encendido, pero el LED se apaga manualmente.
Verde firme	N/A	Se está inicializando el sistema de software del punto de acceso.
Rojo constante	N/A	El sistema funciona correctamente, pero el puerto de servicio de enlace ascendente está

Estado	Frecuencia	Descripción
		desvinculado.
Parpadeo en rojo en un intervalo de 1s	Encendido durante 3 segundos Apagado por 1s	En el modo de ajuste, se agota el tiempo de espera de la configuración de un túnel CAPWAP entre el punto de acceso y el controlador inalámbrico.
Parpadeo en azul a un intervalo de 0,2s	Encendido durante 0,2s Desactivado durante 0,2s	En el modo fit o en la nube, se está actualizando el sistema de software del AP.
Azul fijo	N/A	El sistema funciona correctamente, pero no hay ningún STA en línea.
Parpadeo en azul en un intervalo de 1s	Encendido por 1s Apagado por 1s	El sistema funciona correctamente y hay uno o más STA en línea.
Parpadeo en rojo a un intervalo de 0,2s	Encendido durante 0,2s Desactivado durante 0,2s	En el modo de ajuste, se está ubicando el punto de acceso.

Table 1-9 Botón de reinicio

Botón	Operación	Resultado
Botón de reinicio	Mantenga presionado el botón durante menos de 2 segundos.	Reinicie el punto de acceso.
	Mantenga presionado el botón durante más de 5 segundos.	Restaure el punto de acceso a la configuración de fábrica.

Table 1-10 RSSI LEDs

LED Color	No. de LEDs Steady-on	Descripción
N/A	N/A	La función de puente está desactivada en el punto de acceso. La función de puente está desactivada en el punto de acceso,

LED Color	No. de LEDs Steady-on	Descripción
		pero se produce un error en el puente.
Verde	1	El puenteo es exitoso y la intensidad de las señales inalámbricas dedicadas al puenteo es inferior a –70 dBm.
Verde	1, 2	El puenteo es exitoso y la intensidad de las señales inalámbricas dedicadas al puenteo oscila entre –70 dBm y –50 dBm.
Verde	1, 2, 3	El puenteo se realiza correctamente y la intensidad de las señales inalámbricas dedicadas al puenteo es superior a –50 dBm.

1.6 Módulo óptico

El tipo de puerto del dispositivo conectado directamente con el puerto SFP 2.5GE del punto de acceso puede ser un puerto óptico o un puerto eléctrico. Sin embargo, la velocidad de negociación está sujeta a la velocidad de puerto o al módulo óptico utilizado en ambos dispositivos. Para obtener más detalles, consulte la Tabla 1-11 y la Tabla 1-12.

Table 1-11 Negociación de velocidad para un puerto óptico en el dispositivo del mismo nivel

Velocidad de puerto óptico del punto de acceso	Velocidad del módulo óptico	Velocidad de negociación admitida por el puerto en el dispositivo del mismo nivel		
		1 Gbps	1 Gbps/10 Gbps/Negociación automática	1 Gbps/2,5 Gbps/10 Gbps/Negociación automática
2,5 Gbps	2,5 Gbps	No se admite	No se admite	2,5 Gbps
1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps

Table 1-12 Negociación de velocidad para un puerto eléctrico en el dispositivo del mismo nivel

Velocidad de puerto óptico del punto de acceso	Tasa del módulo de conversión O/E	Velocidad de negociación admitida por el puerto en el dispositivo del mismo nivel		
		1 Gbps	1 Gbps/10 Gbps/Negociación automática	1 Gbps/2,5 Gbps/10 Gbps/Negociación automática
1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps
2,5 Gbps	10 Gbps	1 Gbps	1 Gbps	2,5 Gbps

2 Preparación para la instalación

2.1 Precauciones de seguridad

Nota

- Para evitar lesiones personales y daños al dispositivo, lea atentamente las precauciones de seguridad antes de instalar el dispositivo.
- Es posible que las siguientes precauciones de seguridad no cubran todos los peligros posibles.

2.1.1 Precauciones generales de seguridad

- No exponga el punto de acceso a altas temperaturas, polvos o gases nocivos. No instale el punto de acceso en un entorno inflamable o explosivo. Mantenga el punto de acceso alejado de fuentes EMI, como grandes estaciones de radar, estaciones de radio y subestaciones. No someta el punto de acceso a voltajes inestables, vibraciones y ruidos.
- El sitio de instalación debe estar libre de inundaciones de agua, filtraciones, goteo o condensación. El sitio de instalación debe seleccionarse de acuerdo con la planificación de la red, las características del equipo de comunicaciones y consideraciones como el clima, la hidrología, la geología, los terremotos, la energía eléctrica y el transporte.
- El sitio de instalación debe estar seco. No se recomienda que el punto de acceso se instale en un lugar cercano al mar. Mantenga el dispositivo al menos a 500 metros del océano y no lo mire hacia la brisa marina.
- No coloque el dispositivo en áreas para caminar.
- Durante la instalación y el mantenimiento, no use ropa holgada, adornos o cualquier otra cosa que pueda engancharse con el chasis.
- Mantenga las herramientas y los componentes alejados de las áreas para caminar.

2.1.2 Seguridad en el manejo

- Evite que el punto de acceso se manipule con frecuencia.
- Corte todas las fuentes de alimentación y desconecte todos los cables de alimentación antes de mover o manipular el dispositivo.

2.1.3 Seguridad eléctrica

Advertencia

- Las operaciones eléctricas incorrectas o incorrectas pueden causar incendios, descargas eléctricas y otros accidentes, y provocar lesiones personales graves y mortales y daños al dispositivo.
- El contacto directo o indirecto con la fuente de alimentación de alto voltaje o de la red eléctrica a través de objetos mojados puede causar peligros fatales.

- Observe las regulaciones y especificaciones locales durante las operaciones eléctricas. Solo el

personal con las calificaciones pertinentes puede realizar tales operaciones.

- Compruebe si existen riesgos potenciales en el área de trabajo. Por ejemplo, compruebe si el suelo está mojado.
- Encuentre la posición del interruptor de alimentación de emergencia interior antes de la instalación. Corte el interruptor de alimentación en caso de accidentes.
- Verifique el punto de acceso cuidadosamente para obtener confirmación antes de apagar la fuente de alimentación.
- No coloque el dispositivo en un lugar húmedo o mojado. No permita que entre ningún líquido en el chasis.
- Mantenga el punto de acceso alejado de los dispositivos de conexión a tierra o de protección contra rayos para equipos eléctricos.
- Mantenga el punto de acceso alejado de estaciones de radio, estaciones de radar, dispositivos de alta frecuencia y alta corriente y hornos de microondas.

2.1.4 Seguridad de almacenamiento

Para el correcto funcionamiento del punto de acceso, el punto de acceso debe almacenarse en un entorno basado en los requisitos de temperatura/humedad de almacenamiento de las Especificaciones.

> ⚠ **Cautela**
>
> Si el punto de acceso se almacena durante más de 18 meses, encienda el punto de acceso y hágalo funcionar durante 24 horas consecutivas para activar el punto de acceso.

2.2 Requisitos del entorno de instalación

2.2.1 Requisitos de los rodamientos

Evalúe el peso del dispositivo y sus accesorios (como el soporte, el poste y el módulo de fuente de alimentación) y asegúrese de que el suelo del sitio de instalación cumpla con los requisitos.

2.2.2 Requisitos de ventilación

Reserve suficiente espacio frente a las rejillas de ventilación para garantizar la disipación normal del calor. Después de conectar varios cables, agrupe los cables o colóquelos en el soporte de administración de cables para evitar bloquear las entradas de aire.

2.2.3 Requisitos de espacio

Mantenga un espacio libre mínimo de 0,4 m (15,75 pulg.) alrededor del dispositivo para garantizar una refrigeración y ventilación adecuadas.

2.2.4 Requisitos de temperatura/humedad

Para garantizar un funcionamiento normal y una vida útil prolongada del punto de acceso, mantenga una temperatura y humedad adecuadas en el entorno de instalación.

El entorno de instalación con una temperatura y humedad demasiado altas o demasiado bajas durante un largo período de tiempo puede dañar el punto de acceso.

- En un ambiente con alta humedad relativa, el material aislante puede tener un mal aislamiento o incluso tener fugas de electricidad.
- En un ambiente con baja humedad relativa, la tira aislante puede secarse y encogerse, aflojando los tornillos.
- En un entorno seco, es probable que se produzca electricidad estática y se dañen los circuitos internos del punto de acceso.
- Las temperaturas demasiado altas pueden acelerar el envejecimiento de los materiales aislantes, reduciendo en gran medida la fiabilidad del punto de acceso y afectando gravemente a su vida útil.

Nota

La temperatura ambiente y la humedad del dispositivo se miden en el punto que está a 1,5 m (59,06 pulgadas) por encima del suelo y a 0,4 m (15,75 pulgadas) antes del dispositivo cuando no hay una placa protectora delante o detrás del dispositivo.

2.2.5 Requisitos de limpieza

El polvo representa la principal amenaza para el funcionamiento del dispositivo. El polvo interior que cae sobre el dispositivo puede ser adherido por la electricidad estática, causando un mal contacto de la junta metálica. Dicha adherencia electrostática puede ocurrir más fácilmente cuando la humedad relativa es baja, lo que no solo afecta la vida útil del dispositivo, sino que también causa fallas de comunicación. La siguiente tabla muestra los requisitos para el contenido de polvo y la granularidad en la sala de equipos.

Table 2-1 Requisitos para el polvo

Polvo	Unidad	Contenido
Partículas de polvo (diámetro ≤ 0,5 μm)	Partículas/m3	≤ 1.4×107
Partículas de polvo (0,5 μm ≤ diámetro ≤ 1 μm)	Partículas/m3	≤ 7×105
Partículas de polvo (1 μm ≤ diámetro ≤ 3 μm)	Partículas/m3	≤ 2.4×105
Partículas de polvo (3 μm ≤ diámetro ≤ 5 μm)	Partículas/m3	≤ 1.3×105

Además del polvo, la sal, el ácido y el sulfuro en el aire de la sala de equipos también deben cumplir requisitos estrictos, ya que estas sustancias venenosas pueden acelerar la corrosión del metal y el envejecimiento de algunas piezas. La sala de equipos debe estar protegida de la intrusión de gases nocivos (por ejemplo, SO2, H2S, NO2, NH3 y Cl2), cuyos requisitos se enumeran en la siguiente tabla.

Table 2-2 Requisitos para los gases

Gas	Promedio (mg/m3)	Máximo (mg/m3)
Dióxido de azufre (SO2)	0.2	1.5
Sulfuro de hidrógeno (H2S)	0.006	0.03
Dióxido de nitrógeno (NO2)	0.04	0.15
Gas amoníaco (NH3)	0.05	0.15
Cloro gaseoso (CI2)	0.01	0.3

Nota

El **promedio** se refiere al valor promedio de gas nocivo en una semana. El **valor máximo** es el límite superior del gas nocivo en una semana, y el valor máximo puede durar hasta 30 minutos todos los días.

2.2.6 Requisitos anti interferencias

- Tome medidas de prevención de interferencias para el sistema de suministro de energía.
- Mantenga el punto de acceso alejado del equipo de puesta a tierra o del equipo de puesta a tierra y rayos del dispositivo de alimentación tanto como sea posible.
- Mantenga el punto de acceso alejado de dispositivos de corriente de alta frecuencia, como la estación transmisora de radio de alta potencia y el lanzador de radar.
- Tome medidas de blindaje electromagnético cuando sea necesario.

2.2.7 Requisitos de protección contra rayos

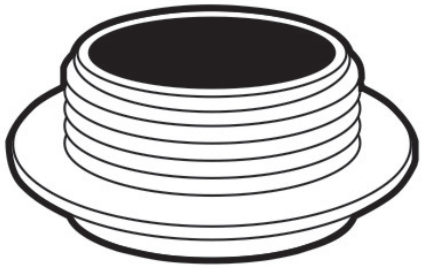
El AX 3000 OLP puede proteger contra los rayos. Como dispositivo eléctrico, los rayos demasiado fuertes pueden dañar el dispositivo. Tome las siguientes medidas de protección contra rayos:

- Asegúrese de que el punto neutro de la toma de corriente esté en buen contacto con el suelo.
- Se recomienda instalar un pararrayos eléctrico frente al extremo de entrada de alimentación para mejorar la prevención de rayos para la fuente de alimentación.

2.2.8 Requisitos de impermeabilidad

Tape los puertos no utilizados para garantizar la impermeabilidad.

Figure 2-1 Tapa antipolvo



Conecte el cable de red, el puente de fibra óptica y el cable de alimentación de CC al punto de acceso después de que pasen por los enchufes impermeables correspondientes para garantizar la impermeabilidad.

2.2.9 Otros requisitos

Independientemente de si el dispositivo se instala en la pared o en el poste, se deben cumplir las siguientes condiciones:

- Se reserva suficiente espacio en la entrada de aire y las rejillas de ventilación del dispositivo para facilitar la disipación de calor del dispositivo.
- El lugar de instalación permite una refrigeración y ventilación adecuadas.
- El lado de instalación es lo suficientemente resistente como para soportar el peso del dispositivo y sus accesorios.
- El punto de acceso está correctamente conectado a tierra.

2.3 Herramientas

Table 2-3 Herramientas

Herramientas comunes	Destornillador de cruz, cables Ethernet y fibras ópticas, tornillos, alicate diagonal y bridas
Herramientas especiales	Muñequera antiestática, alicate para pelar, alicate para engarzar y cortador de alambre
Metros	Multímetro y comprobador de tasa de error de bits (BERT)
Otras herramientas	PC, pantalla y teclado

Nota

El AX 3000 OLP se entrega sin un kit de herramientas. El kit de herramientas es suministrado por el cliente.

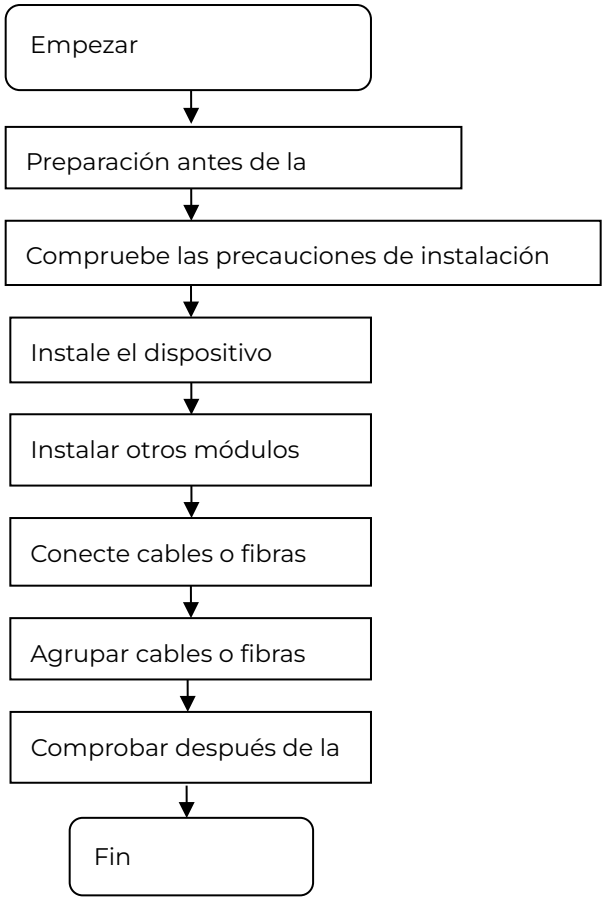
3 Instalación del punto de acceso

El punto de acceso AX 3000 OLP debe instalarse en una posición fija.

> ⚠ **Cautela**
>
> Antes de instalar el dispositivo, asegúrese de haber leído detenidamente los requisitos descritos en el Capítulo 2.

3.1 Diagrama de flujo de instalación

Figure 3-1 Diagrama de flujo de instalación



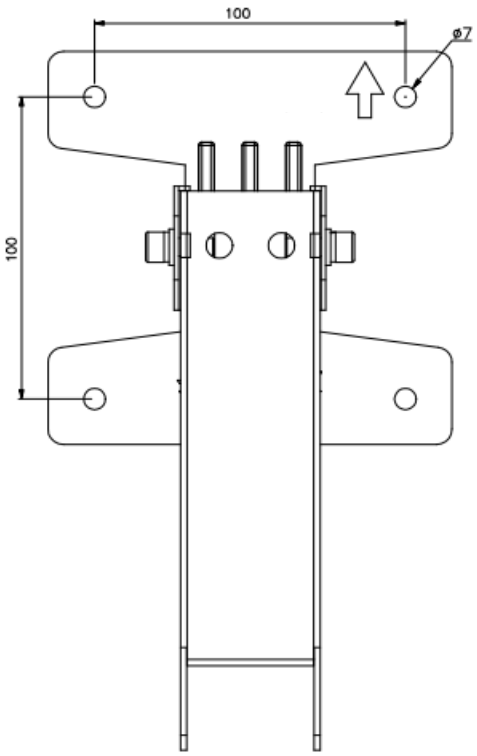
3.2 Antes de empezar

Planifique y organice cuidadosamente la ubicación de instalación, el modo de red, la fuente de alimentación y el cableado antes de instalar el dispositivo.

Confirme los siguientes requisitos antes de la instalación:

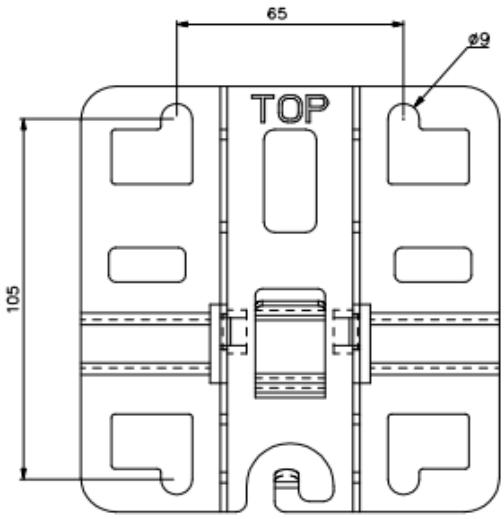
- La ubicación de la instalación proporciona suficiente espacio para la disipación de calor.
- La ubicación de la instalación cumple con los requisitos de temperatura y humedad del dispositivo.
- La fuente de alimentación y la corriente requerida están disponibles en la ubicación de la instalación.
- Los cables Ethernet se han instalado en el lugar de instalación.
- La fuente de alimentación seleccionada cumple con los requisitos de alimentación del sistema.
- La posición del interruptor de alimentación de emergencia se encuentra antes de la instalación, de modo que el interruptor de alimentación se puede cortar en caso de accidentes.
- El rango de diámetro del poste en el que se va a montar el dispositivo cumple con los requisitos de valor de los parámetros en las especificaciones.
- Para el punto de acceso montado en el techo, las dimensiones del soporte de montaje, el patrón del orificio de montaje y el diámetro del orificio de montaje deben cumplir con los requisitos de la siguiente figura.

Figure 3-2 Dimensiones del conjunto de la placa de montaje



- Para el punto de acceso montado en poste, el diámetro del poste debe cumplir con el requisito especificado.

Figure 3-3 Dimensiones del soporte de montaje



3.3 Precauciones

Para garantizar el funcionamiento normal y la vida útil prolongada del punto de acceso, observe las siguientes precauciones de seguridad:

- No encienda el dispositivo durante la instalación.
- Coloque el dispositivo en un ambiente bien ventilado.
- No exponga el dispositivo a altas temperaturas.
- Mantenga el dispositivo alejado de cables de alimentación de alto voltaje.
- Instale el punto de acceso en interiores.
- No exponga el dispositivo en una tormenta eléctrica o un campo eléctrico fuerte.
- Mantenga el dispositivo limpio y libre de polvo.
- Apague el interruptor de encendido antes de limpiar el dispositivo.
- No limpie el dispositivo con un paño húmedo.
- No lave el dispositivo con líquido.
- No abra la carcasa cuando el dispositivo esté funcionando.
- Sujete bien el dispositivo.

3.4 Instalación del punto de acceso

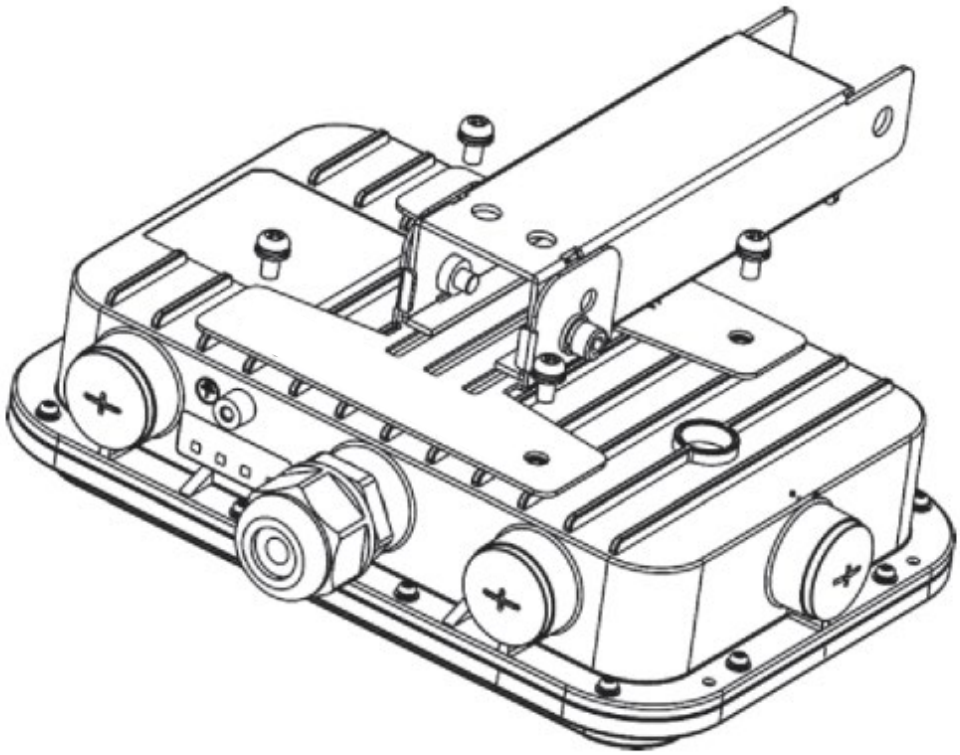
El punto de acceso se puede instalar en un poste o en el techo. Para obtener la cobertura Wi-Fi óptima, mantenga el panel frontal del punto de acceso paralelo al suelo. Se recomienda montar el punto de acceso horizontalmente a una altura que oscile entre 3 m (9,84 pies) y 5 m (16,40 pies) sobre el suelo. En un entorno ideal, el área de cobertura del punto de acceso es elíptica, con un eje mayor de 100 m (328,08 pies) y un eje menor de 50 m (164,04 pies). La implementación del punto de acceso está sujeta al entorno real.

Para áreas con interferencias ambientales severas, se recomienda reducir la distancia entre los dos puntos de acceso para mejorar la cobertura Wi-Fi en el área del borde.

3.4.1 Montaje del punto de acceso en un poste

(1) Fije el conjunto de la placa de montaje a la parte inferior del punto de acceso AX 3000 OLP con cuatro tornillos M5.

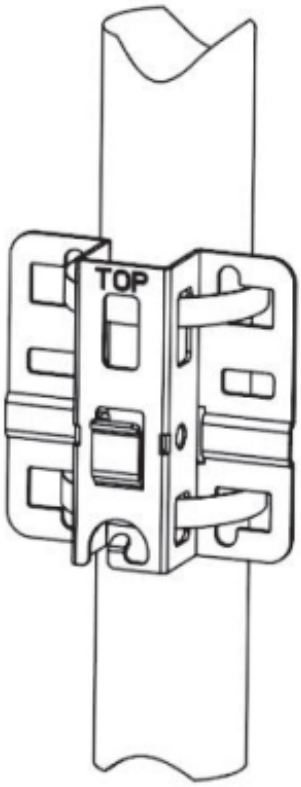
Figure 3-4 Fijación del conjunto de la placa de montaje al punto de acceso



(2) Asegure el soporte de montaje a un poste.

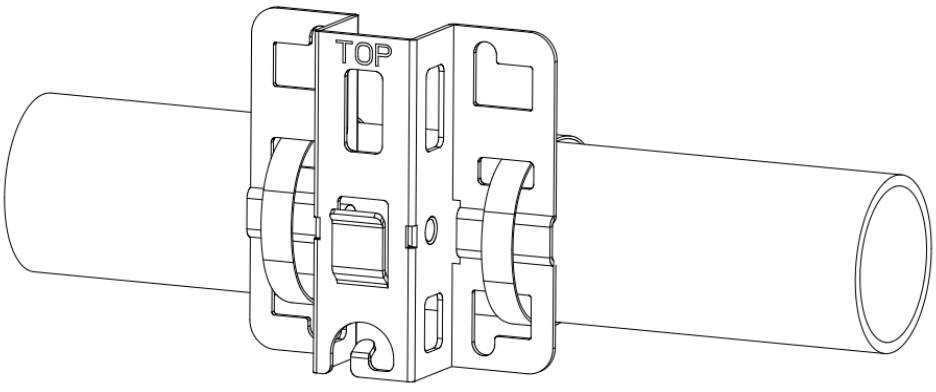
- Montaje en poste vertical: Asegure el soporte de montaje a un poste vertical enroscando dos abrazaderas de manguera a través de los orificios cuadrados del soporte de montaje. Mantenga la parte del soporte anotada por **TOP** en la parte superior.

Figure 3-5 Fijación del soporte de montaje al poste vertical



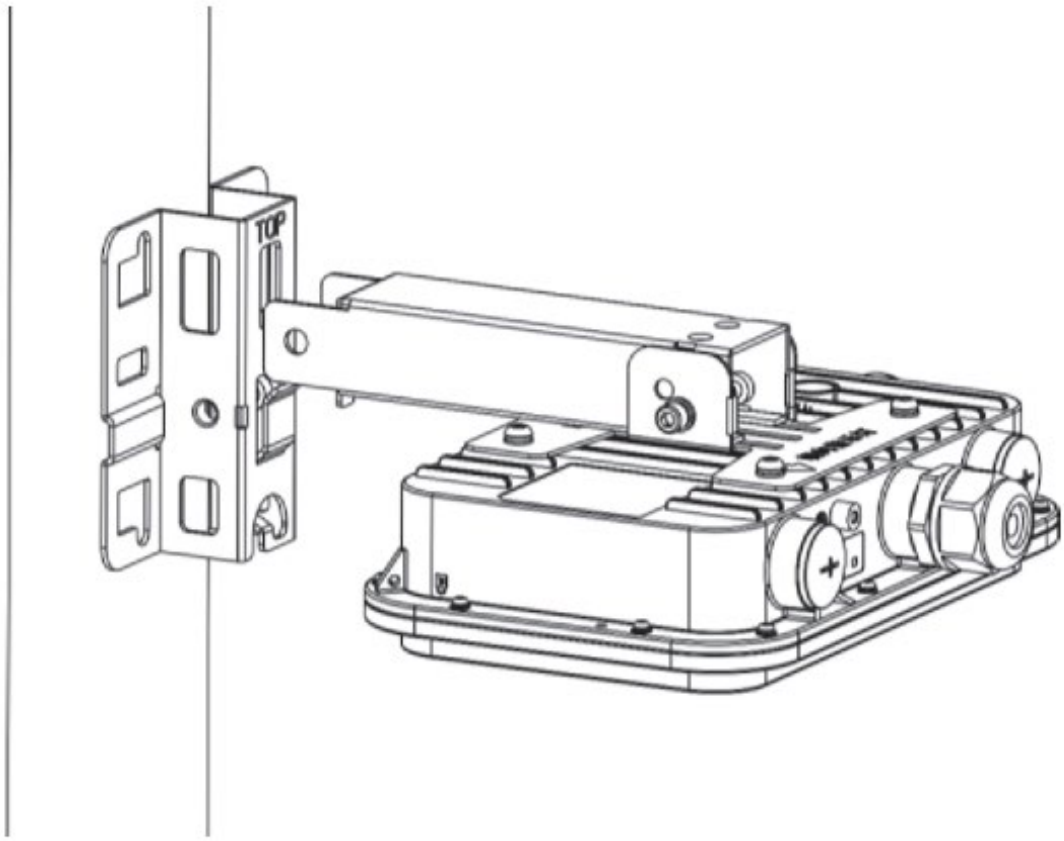
- Montaje en poste horizontal: Asegure el soporte de montaje a un poste horizontal enroscando dos abrazaderas de manguera a través de los orificios cuadrados del soporte de montaje. Mantenga la parte del soporte anotada por **TOP** en la parte superior.

Figure 3-6 Fijación del soporte de montaje al poste horizontal



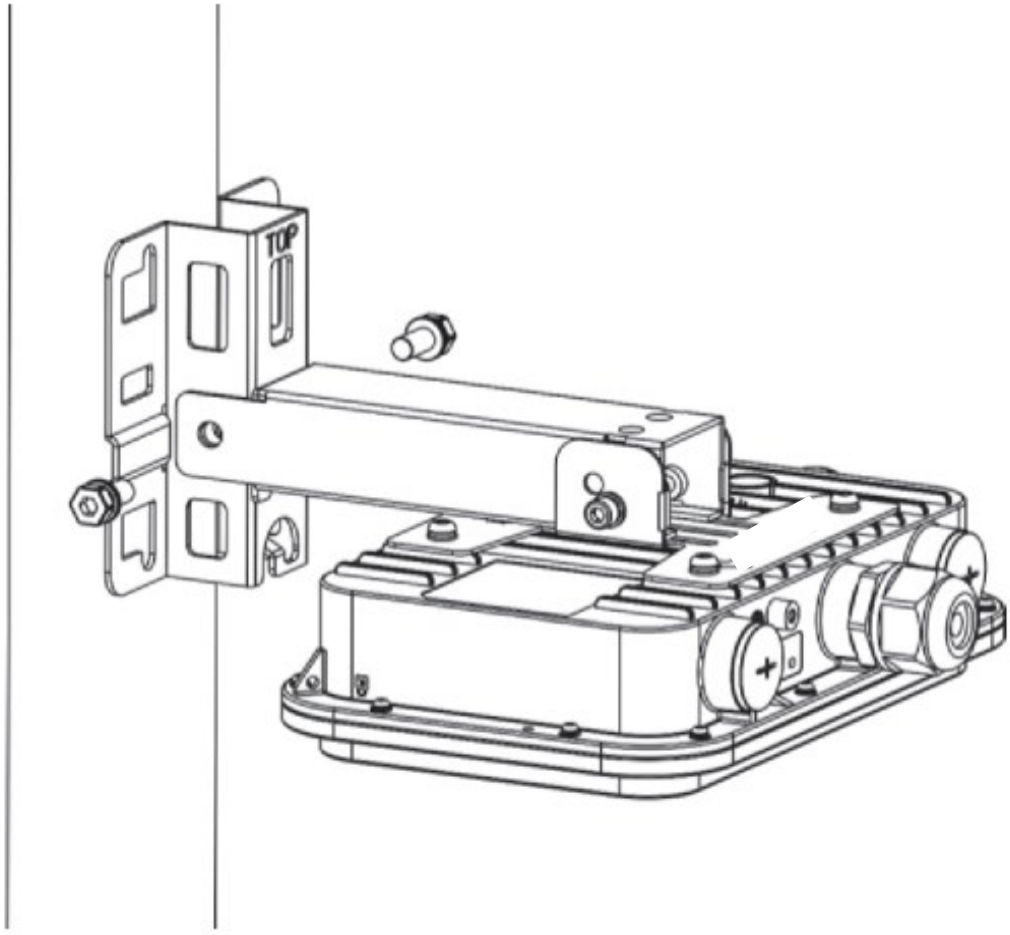
(3) Coloque el brazo de montaje en el soporte de montaje con sus dos orificios alineados con los orificios de los tornillos en el soporte de montaje.

Figure 3-7 Colocación del brazo de montaje en el soporte de montaje



(4) Utilice dos tornillos M8 para fijar el brazo de montaje al soporte de montaje.

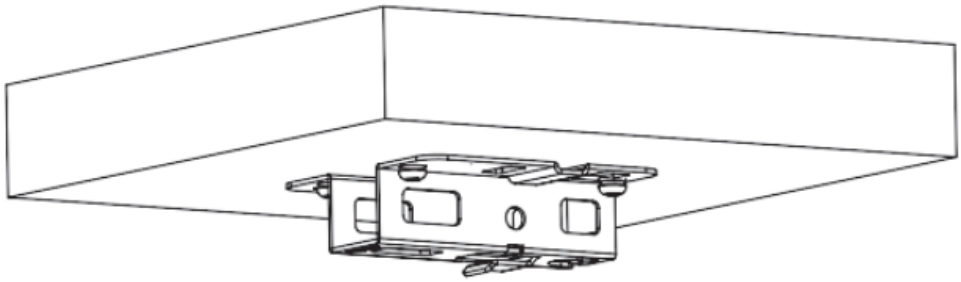
Figure 3-8 **Fijación del brazo de montaje al soporte de montaje**



3.4.2 Montaje del punto de acceso en el techo o en la pared

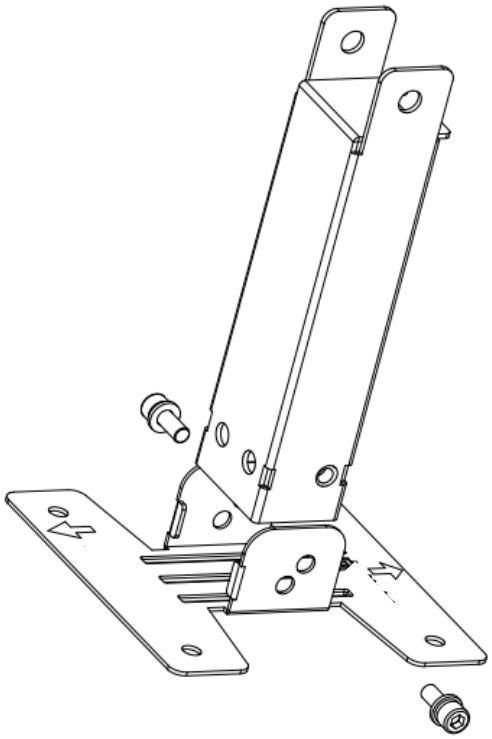
(1) Fije el soporte de montaje al techo o a la pared con cuatro anclajes de expansión M6.

Figure 3-9 **Fijación del soporte de montaje al techo**



(2) Afloje los dos tornillos M6 del conjunto de la placa de montaje para retirar el brazo de montaje. Gire el brazo de montaje 90 grados en el sentido de las agujas del reloj hasta que quede en posición vertical. Apriete dos tornillos M6 para asegurar el brazo de montaje a la placa de montaje.

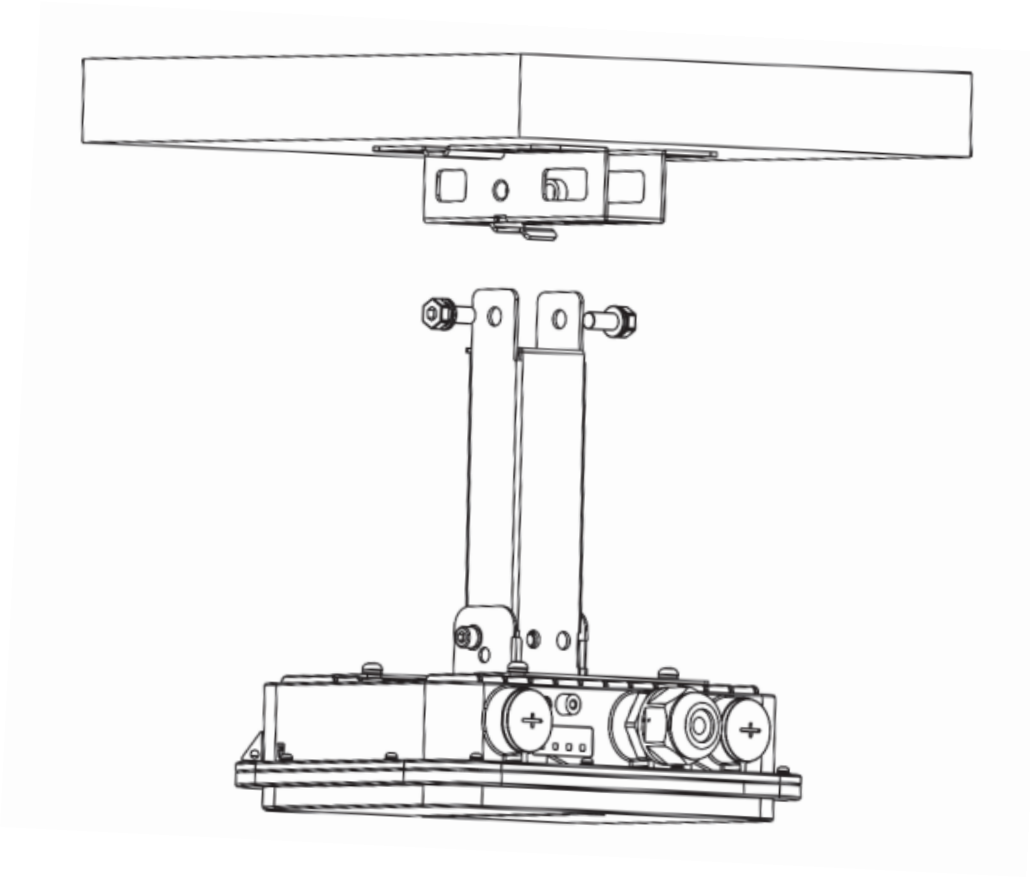
Figure 3-10 Brazo de montaje giratorio 90 grados en el sentido de las agujas del reloj



(3) Fije el conjunto de la placa de montaje a la parte inferior del punto de acceso AX 3000 OLP con cuatro tornillos M5.

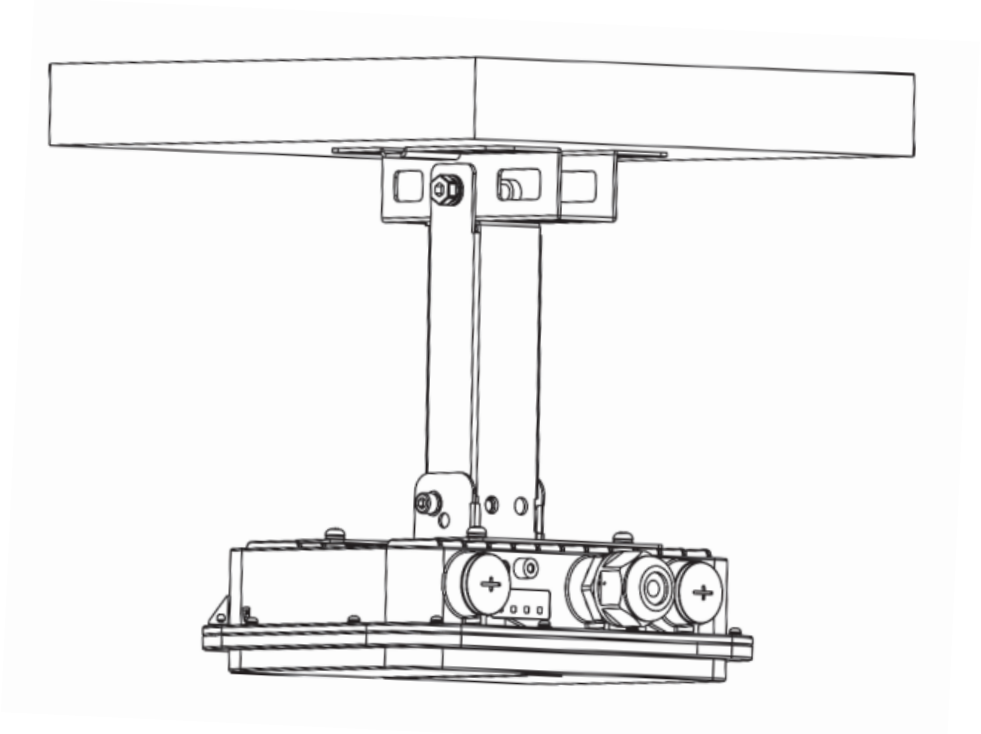
(4) Coloque el brazo de montaje en el soporte de montaje con sus dos orificios alineados con los orificios de los tornillos en el soporte de montaje.

Figure 3-11 Colocación del brazo de montaje en el soporte de montaje



(5) Utilice dos tornillos M8 para fijar el brazo de montaje al soporte de montaje.

Figure 3-12 Fijación del brazo de montaje al soporte de montaje



Cautela

- Utilice tornillos a juego para los orificios de los tornillos y apriete las piezas estructurales en diferentes eslabones de instalación.
- Apriete todos los tornillos de fijación. Si no se instala algún tornillo, el dispositivo puede vibrar violentamente, desplazarse o caerse.
- Después de la instalación, verifique que todos los tornillos estén apretados para evitar que el dispositivo se caiga.

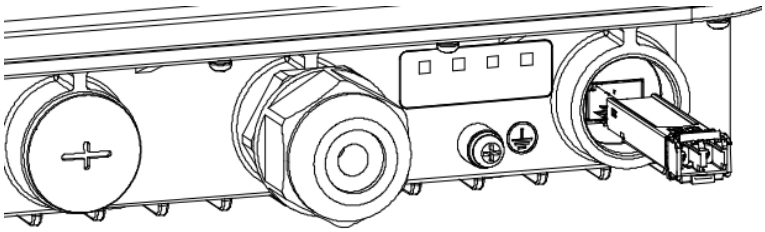
3.4.3 Eliminación del punto de acceso

Proceda en el orden inverso a la instalación para eliminar el punto de acceso.

3.5 Instalación de un módulo óptico

Inserte un módulo óptico en el puerto SFP del punto de acceso y asegúrese de que el módulo óptico esté instalado correctamente.

Figure 3-13 Instalación de un módulo óptico

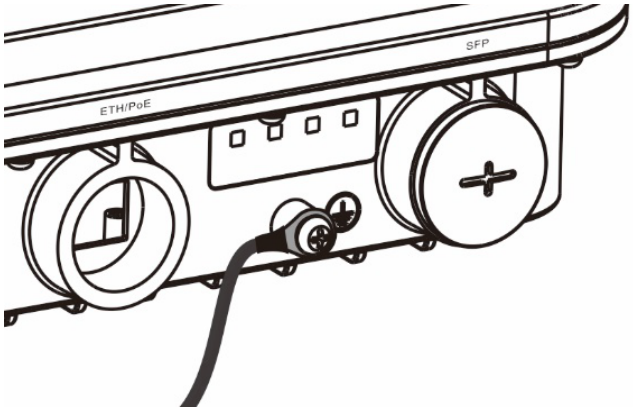


3.6 Instalación de los cables

3.6.1 Instalación del cable de conexión a tierra

El cable de conexión a tierra debe fabricarse en el sitio. Conecte un extremo del cable de conexión a tierra suministrado con el dispositivo al orificio de tierra del dispositivo a través de un terminal OT y el otro extremo a tierra a través de otro terminal OT. La longitud del cable se puede recortar en función de la situación in situ para evitar desperdicios.

Figure 3-14 Instalación del cable de conexión a tierra



3.6.2 Instalación del cable Ethernet

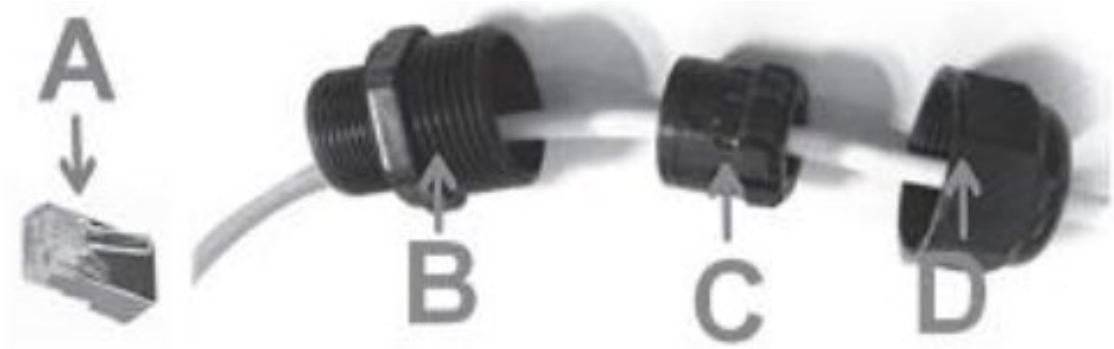
Cautela

- Asegúrese de que el conector RJ45 esté insertado correctamente en el punto de acceso. De lo contrario, el conector RJ45 se dañará cuando apriete el prensaestopas.
- Al quitar el cable Ethernet, retire primero el prensaestopas y luego el conector RJ45 que se conecta al punto de acceso.

(1) Ajuste un cable Ethernet de acuerdo con la distancia entre el punto de acceso y la fuente de alimentación.

(2) Inserte el extremo no terminado del cable Ethernet a través de la parte D (tapa de compresión), C (arandela) y B (junta dividida) en secuencia.

Figure 3-15 Vista despiece del conjunto de prensaestopas



(3) Instale un conector RJ45 en el extremo no terminado del cable Ethernet utilizando una herramienta de instalación de cable Ethernet. Envuelva materiales

impermeables alrededor del cable Ethernet entre la parte B (junta dividida) y C (arandela).

Figure 3-16 Envolver materiales impermeables alrededor del cable Ethernet

(4) Inserte el conector RJ45 en el puerto Ethernet/PoE del punto de acceso y apriete el conjunto del prensaestopas en secuencia de las partes B, C y D para completar la instalación.

3.6.3 Instalación del cable de fibra óptica

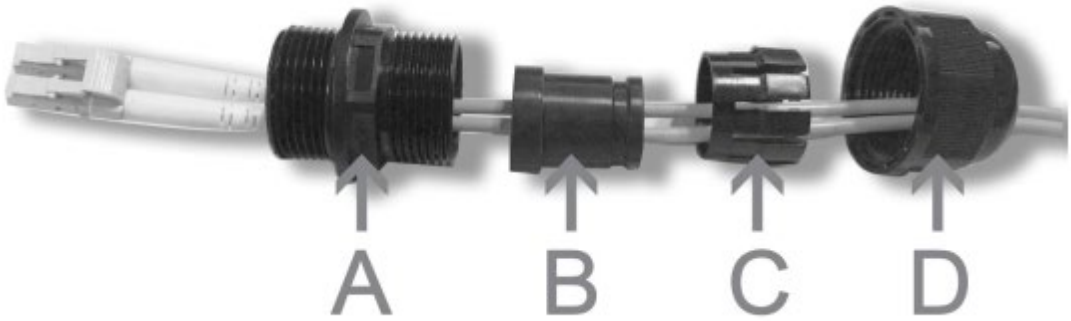
Nota

- El prensaestopas solo puede sujetar el cable de fibra óptica LC a LC con un diámetro que oscila entre 2,5 mm y 2,9 mm (0,10 pulg. a 0,11 pulg.).
- Conecte o retire el cable de fibra óptica LC a LC según la guía. De lo contrario, el cable de fibra óptica podría dañarse.

(1) Seleccione un cable de fibra óptica LC-LC con un diámetro que oscile entre 2,5 mm y 2,9 mm (0,10 pulg. a 0,11 pulg.).

(2) Un conjunto de prensaestopas incluye cuatro componentes: A (base adaptadora), B (junta dividida), C (arandela) y D (tapa de compresión). B (junta dividida) se puede presionar en C (arandela) y también se puede quitar de C (arandela). Inserte el extremo sin terminar de un cable de fibra óptica a través de las partes D, C, B y A en secuencia.

Figure 3-17 Vista despiece del conjunto de prensaestopas



(3) Instale un conector RJ-45 en el extremo no terminado del cable de fibra óptica. Inserte con cuidado el conector RJ-45 en el puerto SFP del punto de acceso. Enrosque A (base del adaptador) en el puerto SFP.

(4) Deslice B (junta dividida) y C (arandela) a lo largo del cable, presionando firmemente para asentar B (junta) completamente en C (arandela).

(5) Apriete D (tapa de compresión) hasta que C (ojal) y B (junta) se compriman en el cable y alivien la tensión del cable. Use una cinta impermeable para apretar el prensaestopas.

Cautela

Al retirar el prensaestopas, proceda en el orden inverso al de la instalación. Comience aflojando D (tapa de compresión). De lo contrario, el cable de fibra óptica podría dañarse.

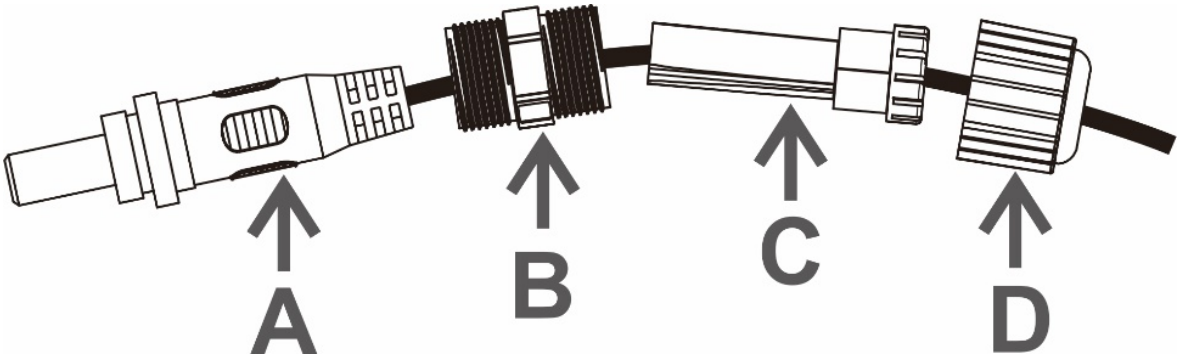
3.6.4 Instalación del cable de alimentación

Nota

Cuando el punto de acceso esté alimentado por la fuente de alimentación de CC, mantenga los puertos hacia abajo. En este caso, el punto de acceso solo se puede proteger contra salpicaduras de agua.

El cable de alimentación de CC debe usarse en combinación con el prensaestopas. Pinta cemento impermeable y envuelve las cintas impermeables alrededor del cable de alimentación de CC entre B (junta dividida) y C (ojal). El cable de alimentación resistente al agua debe tener al menos 5 mm (0,20 pulgadas) de diámetro.

Figure 3-18 Instalación del cable de alimentación de CC



3.7 Agrupación de cables

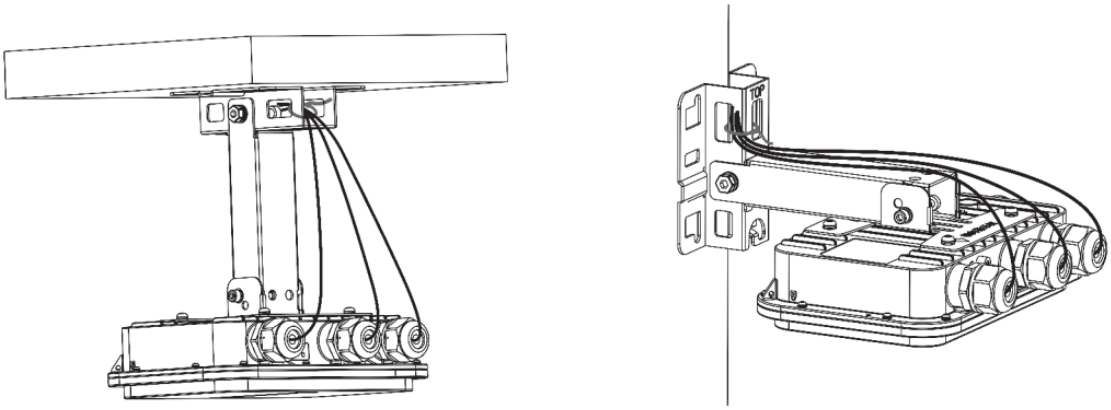
3.7.1 Precauciones

- Agrupe los cables de forma ordenada para garantizar la estética.
- Doble los pares trenzados de forma natural o a un radio grande cerca del conector.
- No apriete demasiado el paquete de par trenzado, ya que puede reducir la vida útil y el rendimiento del cable.

3.7.2 Descripción de la agrupación

Después de que los cables estén conectados con el dispositivo a través de los enchufes impermeables y el encendido sea normal, use una brida para agrupar los cables en la placa de montaje y luego fije los cables cuidadosamente.

Figure 3-19 Agrupación de cables en el soporte de montaje mediante bridas



Cautela

Una vez agrupados los cables, compruebe si se han tomado correctamente las medidas de impermeabilidad.

3.8 Lista de verificación después de la instalación

3.8.1 Comprobación del punto de acceso

- Verifique que la fuente de alimentación externa coincida con los requisitos del punto de acceso.
- Verifique que el punto de acceso esté bien sujeto.

3.8.2 Comprobación de la conexión del cable

- Verifique que el cable UTP/STP o el cable de fibra óptica coincida con el tipo de puerto.
- Verifique que los cables estén agrupados correctamente.

3.8.3 Comprobación de la fuente de alimentación

- Verifique que el cable de alimentación esté conectado correctamente y cumpla con los requisitos de seguridad.
- Verifique que el punto de acceso esté operativo después del encendido.

4 Verificación del estado de funcionamiento

4.1 Configuración del entorno de configuración

El punto de acceso puede ser alimentado por PoE o alimentación local.

- Cuando el punto de acceso se alimenta mediante CC o PoE, verifique que la fuente de alimentación funcione correctamente y cumpla con los requisitos de seguridad.
- Conecte el punto de acceso a un controlador de acceso a través de un cable de par trenzado.
- Cuando el puerto serie del punto de acceso esté conectado a una PC para la depuración, verifique que la PC y el conmutador PoE estén correctamente conectados a tierra.

4.2 Encendido del punto de acceso

4.2.1 Lista de verificación antes del encendido

- Verifique que el cable de alimentación esté conectado correctamente.
- Verifique que el voltaje de entrada cumpla con los requisitos del punto de acceso.

4.2.2 Lista de verificación después del encendido (recomendado)

Después de encenderlo, verifique los siguientes elementos:

- Verifique que haya registros del sistema impresos en la interfaz del terminal.
- Verifique el estado del LED del punto de acceso.

5 Monitorización y Mantenimiento

5.1 Monitorización

5.1.1 LED

Puede observar los LED para monitorear el estado del dispositivo.

5.1.2 Comandos CLI

Puede ejecutar comandos relacionados en la CLI para supervisar el dispositivo de forma remota, entre ellos:

- Configuración y estado de los puertos
- Registros del sistema

Nota

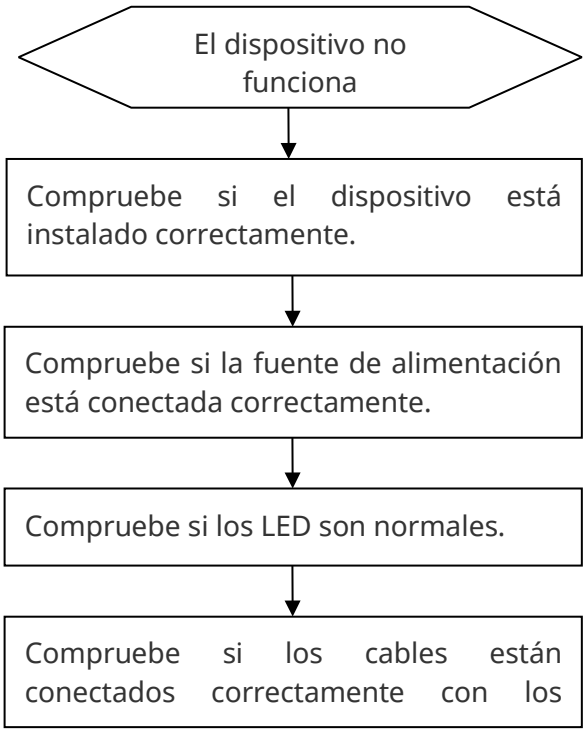
- Puede iniciar sesión en el AP a través de Telnet y utilizar comandos relacionados con la supervisión para mantener el AP.

5.2 Mantenimiento remoto

- Si el punto de acceso funciona en modo gordo, puede iniciar sesión en el punto de acceso para el mantenimiento remoto.
- Si el punto de acceso funciona en el modo de ajuste, puede utilizar un controlador inalámbrico para administrar y mantener el punto de acceso de manera uniforme.

6 Solución de problemas

6.1 Diagrama de flujo de solución de problemas



6.2 Fallas comunes

6.2.1 El puerto Ethernet no funciona después de conectar el cable Ethernet

Compruebe que el dispositivo del mismo nivel funciona correctamente. Y verifique que el cable Ethernet sea capaz de proporcionar la velocidad de datos requerida y esté conectado correctamente.

6.2.2 El LED está apagado durante mucho tiempo

- Alimentación de alimentación PoE: Compruebe si el otro extremo del cable PoE es compatible con los estándares PoE 802.11af o superiores y, a continuación, compruebe si el cable Ethernet está conectado correctamente.
- Fuente de alimentación de CC: Compruebe si hay fuente de alimentación y si la fuente de alimentación funciona normalmente.

6.2.3 El LED es rojo fijo

El LED permanece en rojo fijo durante mucho tiempo, lo que indica que el puerto Ethernet no está conectado. Verifique la conexión Ethernet.

6.2.4 El LED es verde fijo

El dispositivo realiza la inicialización después del encendido. Durante este período, el LED permanece en verde fijo y no se vuelve azul normal hasta que se completa la inicialización. Nota: Si el verde fijo persiste durante una hora, se produce un error en la inicialización del dispositivo y el dispositivo está defectuoso.

6.2.5 El LED sigue parpadeando en azul a un intervalo de 0,2 s (en modo de ajuste)

A veces, el punto de acceso realiza una actualización de software después del encendido. Durante este período, el LED sigue parpadeando en azul en un intervalo de 0,2 segundos y no se vuelve azul fijo hasta que se completa la actualización. Nota: No enchufe ni desconecte el cable de alimentación cuando el LED esté parpadeando, ya que la actualización del software lleva tiempo. Si el parpadeo persiste durante 10 minutos, el dispositivo no puede completar la actualización de software y está defectuoso.

6.2.6 El LED no se vuelve azul fijo ni parpadea en azul

Si el LED no se vuelve azul fijo o parpadea en azul después de iniciar el sistema, es probable que el punto de acceso no haya establecido una conexión CAPWAP adecuada con el controlador inalámbrico. Compruebe que el mando inalámbrico esté operativo y configurado correctamente.

6.2.7 Los clientes no pueden encontrar el punto de acceso

(1) Verifique que el punto de acceso esté alimentado correctamente.

(2) Verifique que el puerto Ethernet esté conectado correctamente.

(3) Verifique que el punto de acceso esté configurado correctamente.

(4) Mueva el punto de conexión del cliente para ajustar la distancia entre el cliente y el punto de acceso.

7 Apéndice

7.1 Conectores y medios

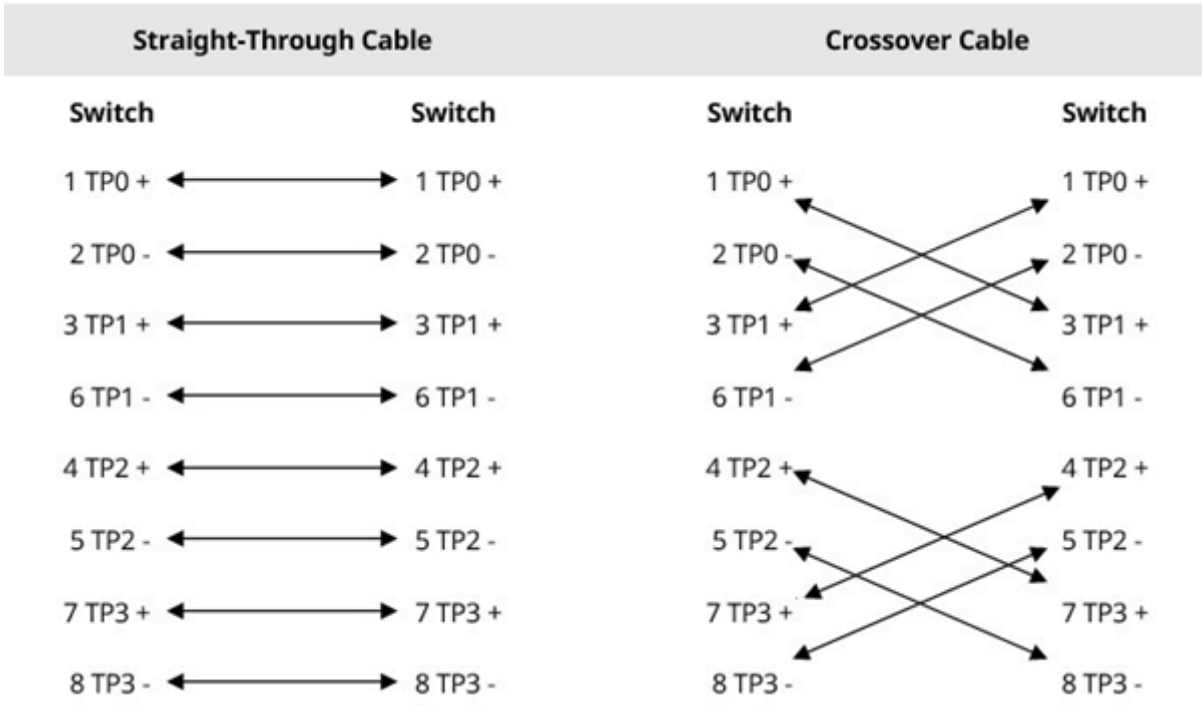
- Puerto 1000BASE-T/100BASE-TX/10BASE-T

El 1000BASE-T/100BASE-TX/10BASE-T es un puerto de 10/100/1000 Mbps que admite la negociación automática y el cruce automático MDI/MDIX.

Conforme a IEEE 802.3ab, el puerto 1000BASE-T requiere UTP o STP de categoría 5/5e de 100 ohmios con una distancia máxima de 100 metros (328,08 pies).

El puerto 1000BASE-T utiliza cuatro pares trenzados para la transmisión de datos. Los pares trenzados para el puerto 1000BASE-T están conectados como se muestra en la siguiente figura.

Figure 7-1 Conexión de pares trenzados 1000BASE-T



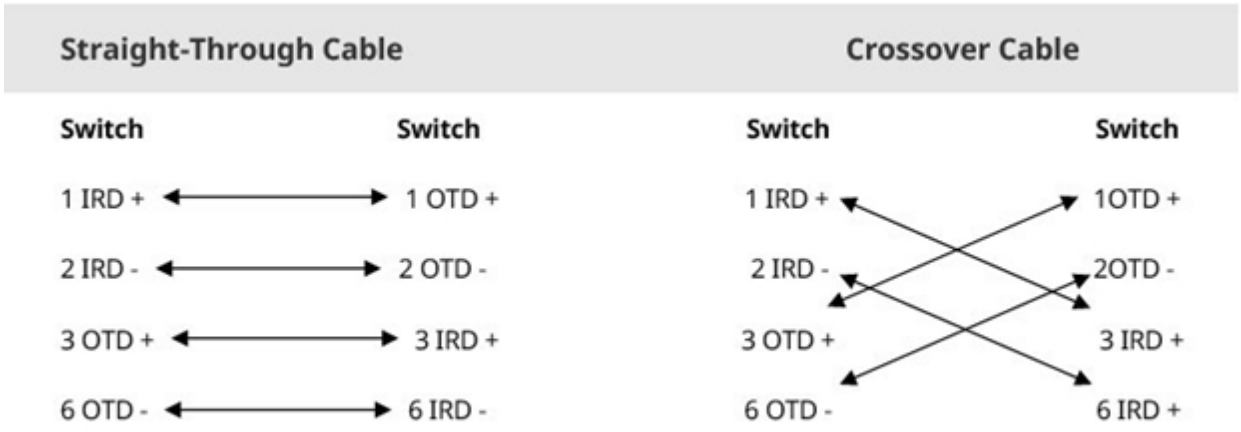
El puerto 100BASE-TX/10BASE-T también se puede conectar mediante cables de las especificaciones anteriores. Además, el puerto 10BASE-T se puede conectar mediante cables de 100 ohmios de categoría 3, categoría 4 y categoría 5 con una distancia máxima de 100 metros (328,08 pies). El puerto 100BASE-TX se puede conectar mediante cables de categoría 5 de 100 ohmios con una distancia máxima de 100 metros (328,08 pies). En la siguiente figura se enumeran las definiciones de las señales de pin para el puerto 100BASE-TX/10BASE-T.

Figure 7-2 Asignaciones de pines 100BASE-TX/10BASE-T

Anclar	Enchufe	Tapón
1	Entrada y recepción de datos+	Transmisión de datos de salida+
2	Entrada de datos de recepción-	Transmisión de datos de salida-
3	Transmisión de datos de salida+	Entrada y recepción de datos+
6	Transmisión de datos de salida-	Entrada de datos de recepción-
4, 5, 7, 8	No se utiliza	No se utiliza

La siguiente figura muestra las conexiones factibles de los pares trenzados directos y cruzados para un puerto 100BASE-TX/10BASE-T.

Figure 7-3 Conexión de pares trenzados 100BASE-TX/10BASE-T

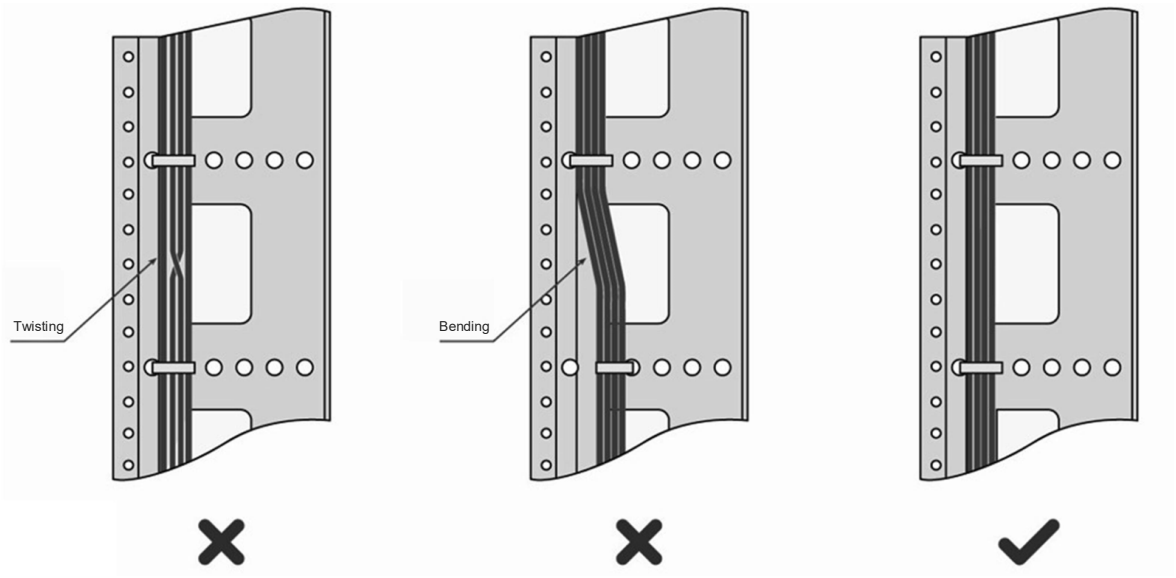


7.2 Cableado

Durante la instalación, dirija los haces de cables hacia arriba o hacia abajo a lo largo de los lados del bastidor en función de la situación real en la sala de equipos. Todos los conectores de cable deben colocarse en la parte inferior del gabinete en lugar de exponerse fuera del gabinete. Los cables de alimentación se enrutan al lado del gabinete, y el cableado superior o inferior se adopta de acuerdo con la situación real en la sala de equipos, como las posiciones de la caja de distribución de energía de CC, la toma de CA o la caja de protección contra rayos.

- Requisito para el radio mínimo de curvatura del cable
  - El radio de curvatura de un cable de alimentación, cable de comunicación o cable plano debe ser más de cinco veces mayor que sus respectivos diámetros. El radio de curvatura de estos cables que a menudo se doblan, se tapan o se desconectan debe ser más de siete veces mayor que sus respectivos diámetros.
  - El radio de curvatura de un cable coaxial común fijo debe ser más de siete veces mayor que su diámetro. El radio de curvatura del cable coaxial común que a menudo se dobla o se conecta debe ser más de 10 veces mayor que su diámetro.
  - El radio de curvatura mínimo de un cable de alta velocidad, como un cable SFP, debe ser más de cinco veces el diámetro total del cable. Si el cable se dobla, se enchufa o se desenchufa con frecuencia, el radio de curvatura debe ser más de 10 veces el diámetro total.
- Precauciones para el agrupamiento de cables
  - Antes de agrupar los cables, marque las etiquetas y péguelas a los cables donde corresponda.
  - Los cables deben estar agrupados de manera ordenada y adecuada en el gabinete sin torcerse ni doblarse, como se muestra en Figure 7-4.

Figure 7-4 Agrupación de cables

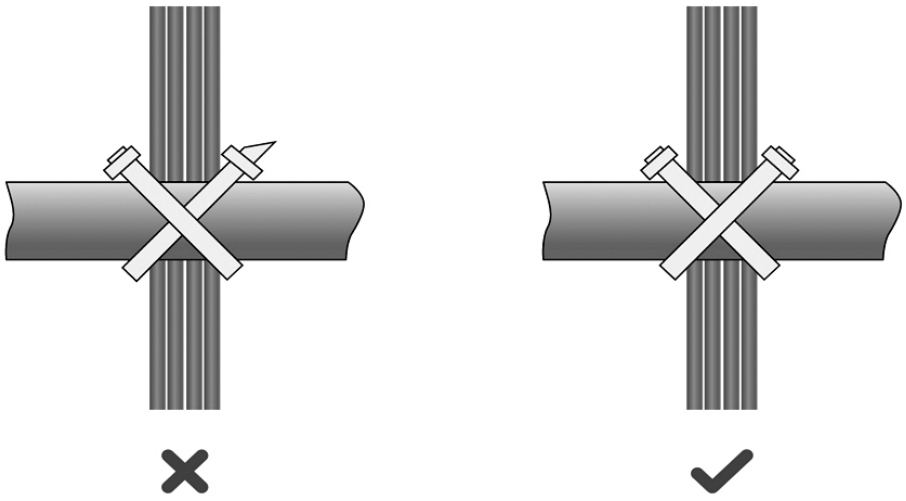


  - Los cables de diferentes tipos (como cables de alimentación, cables de señal y cables de

conexión a tierra) deben separarse en el cableado y la agrupación. No se permite la agrupación mixta. Cuando estén cerca uno del otro, se recomienda que se adopte un cableado cruzado. En el caso de cableado paralelo, mantenga una distancia mínima de 30 mm entre los cables de alimentación y los cables de señal.

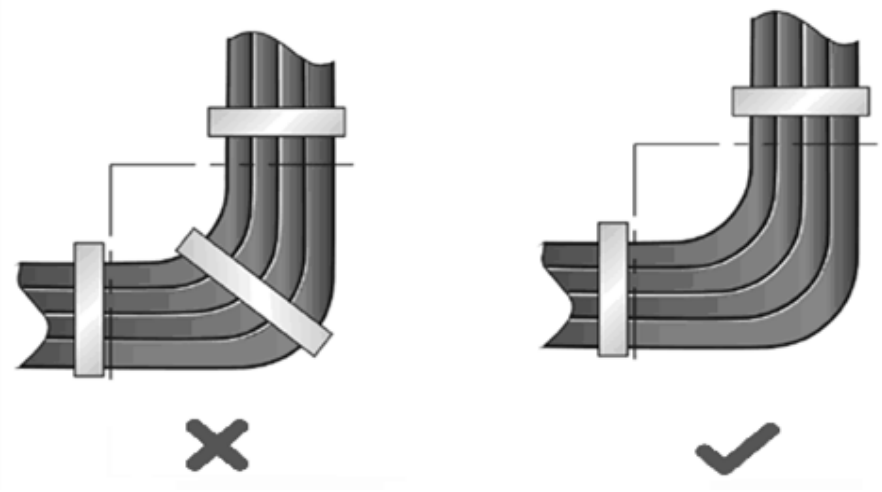
- Los soportes de gestión de cables y los canales de cableado dentro y fuera del gabinete deben ser lisos sin esquinas afiladas.
- El orificio metálico atravesado por los cables debe tener una superficie lisa y completamente redondeada o un revestimiento aislado.
- Se deben seleccionar bridas adecuadas para agrupar los cables. Está prohibido conectar dos o más bridas para agrupar los cables.
- Después de agrupar los cables con bridas, corte la parte restante. El corte debe ser liso y recortado, sin esquinas afiladas, como se muestra en Figure 7-5.

Figure 7-5 Cortar el exceso de bridas



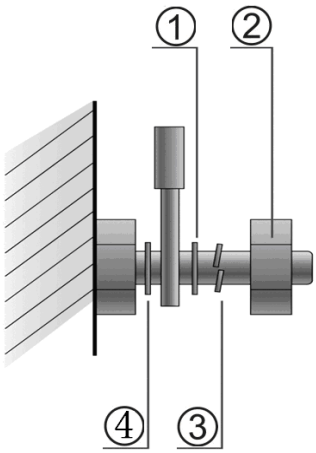
- Cuando sea necesario doblar los cables, átelos primero, pero no ate las bridas dentro de la curva. De lo contrario, se puede generar una tensión considerable en los cables, rompiendo los núcleos de los cables, como se muestra en Figure 7-6.

Figure 7-6 Cables de unión



- Los cables que no se van a ensamblar o las partes restantes de los cables deben doblarse y colocarse en una posición adecuada del gabinete o canal de cables. La posición correcta indica una posición que no afectará el funcionamiento del dispositivo ni causará daños al dispositivo o al cable durante la depuración.
- Los cables de alimentación de 220 V y –48 V no deben agruparse en los rieles guía de las piezas móviles.
- Los cables de alimentación que conectan las partes móviles, como los cables de conexión a tierra de las puertas, deben reservarse con algún acceso después de ensamblarlos para evitar sufrir tensión o estrés. Cuando una pieza móvil alcanza la posición de instalación, la parte restante del cable no debe tocar fuentes de calor, esquinas afiladas o bordes afilados. Si no se pueden evitar las fuentes de calor, se deben utilizar cables de alta temperatura.
- Cuando se utilizan roscas de tornillo para sujetar terminales de cable, el perno o tornillo debe estar bien apretado y se deben tomar medidas anti-aflojamiento, como se muestra en Figure 7-7.

Figure 7-7 Fijación de terminales de cable



① Arandela plana	③ Arandela de resorte
② Nuez	④ Arandela plana

- Los cables de alimentación duros deben sujetarse en el área de conexión del terminal para evitar tensiones en la conexión del terminal y el cable.
- No utilice tornillos autorroscantes para sujetar los terminales.
- Los cables de alimentación del mismo tipo y en la misma dirección de cableado deben agruparse en manojos de cables, con los cables en manojos de cables limpios y rectos.
- Agrupe los cables con bridas según la siguiente tabla.

Diámetro del manojo de cables	Distancia entre cada punto de unión
10 mm (0,39 pulg.)	De 80 mm a 150 mm (de 3,15" a 5,91")

De 10 mm a 30 mm (0,39 pulg. x 1,18 pulg.)	De 150 mm a 200 mm (5,91 pulg. x 7,87 pulg.)
30 mm (1,18 pulg.)	De 200 mm a 300 mm (7,87 pulg. x 11,81 pulg.)

- No se permite ningún nudo en el cableado o agrupación.
- Para el cableado de bloques de terminales (como disyuntores) con terminales de extremo de cable, la parte metálica del terminal de extremo de cable no debe exponerse fuera del bloque de terminales cuando esté ensamblado.

7.3 Módulos ópticos y especificaciones

Utilice módulos ópticos apropiados de acuerdo con los tipos de puerto. Puede seleccionar el módulo que mejor se adapte a sus necesidades específicas. Los tipos de módulos ópticos y las especificaciones correspondientes se proporcionan como referencia.

Table 7-1 Módulos y especificaciones de SFP

Longitud de onda (nm)	Tipo de fibra	DDM	Intensidad de la luz transmitida (dBm)		Intensidad de la luz recibida (dBm)	
			Min.	Máximo.	Min.	Máximo.
850 TX/850 Rx	MMF	Soportado	N/A	–4	N/A	–17
1310 TX/1310 Rx	SMF	Soportado	N/A	3	N/A	–3

Table 7-2 Especificaciones de cableado del módulo SFP

Tipo de interfaz	Tipo de fibra	Especificaciones principales (µm)	Distancia máx. de cableado
LC	MMF	50/125, 62.5/125	0,3 km (984,25 pies)
LC	SMF	9/125	40 km (131233.60 pies)

Cautela

- Para módulos ópticos con una distancia máxima de cableado de más de 40 km (24,85 millas), instale un atenuador óptico para evitar sobrecargas cuando utilice SMF de corta distancia.
- El módulo óptico es un dispositivo láser. Por favor, no mire directamente al rayo láser.
- Para mantener limpio el módulo óptico, asegúrese de que los puertos no utilizados permanezcan tapados.

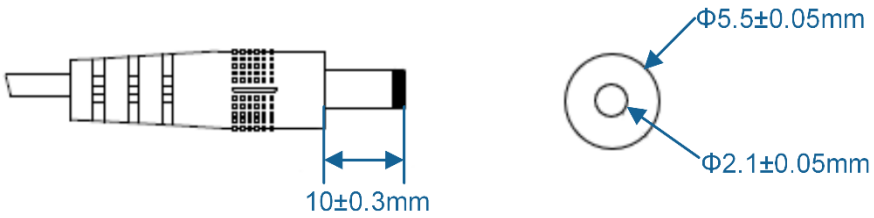
7.4 Especificaciones del conector de CC

- Voltaje de entrada: 48 V DC; corriente nominal: 0,35 A

Table 7-3 Especificaciones del conector de CC

Diámetro interior	Diámetro exterior	Profundidad	Polaridad
2,1 mm (0,09 pulg.)	5,5 mm (0,22 pulg.)	10 mm (0,40 pulg.)	Positivo Interno, Negativo Externo

Figure 7-8 Especificaciones del conector de CC



EKSELANS BY ITS

MANUAL DE USUARIO

Puntos de acceso de la serie AX basados en la web

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

Derechos de autor

Renuncia

Los productos, servicios o funciones que compre están sujetos a contratos y términos comerciales. Es posible que algunos o todos los productos, servicios o características descritos en este documento no estén dentro del alcance de su compra o uso. A menos que se acuerde lo contrario en el contrato, Ekselans by ITS no hace ninguna declaración o garantía expresa o implícita por el contenido de este documento.

Debido a actualizaciones de la versión del producto u otros motivos, el contenido de este documento se actualizará de vez en cuando. Ekselans by ITS se reserva el derecho de modificar el contenido del documento sin previo aviso ni aviso.

Este manual es solo para referencia. Ekselans by ITS se esfuerza por garantizar la exactitud del contenido y no asumirá ninguna responsabilidad por pérdidas y daños causados debido a omisiones, inexactitudes o errores en el contenido.

Prefacio

Público al que va dirigido

Este documento está destinado a:

- Ingenieros de redes
- Soporte técnico e ingenieros de servicio
- Administradores de red

Soporte técnico

- Sitio web de la empresa: https://www.ek.plus/
- Consultar Sitio Web: https://www.ek.plus/contacto/
- Correo electrónico de soporte: soporte@ek.plus

Convenios

1. Signos

Los signos utilizados en este documento se describen de la siguiente manera:

Advertencia

Una alerta que llama la atención sobre reglas e información importantes que, si no se entienden o no se siguen, pueden provocar la pérdida de datos o daños en el equipo.

Cautela

Una alerta que llama la atención sobre información esencial que, si no se comprende o se sigue, puede provocar un error de función o una degradación del rendimiento.

Nota

Una alerta que contiene información adicional o complementaria que, si no se entiende o se sigue, no tendrá consecuencias graves.

Especificación

Una alerta que contiene una descripción de la compatibilidad con el producto o la versión.

2. Nota

El manual proporciona información de configuración, incluidos modelos, tipos de puertos e interfaces de línea de comandos, solo con fines de referencia. En caso de discrepancia o incoherencia entre el manual y la versión real, prevalecerá la versión real.

1 Entorno operativo

1.1 Visión general

Puede acceder al sistema de administración web a través de un navegador web como Internet Explorer y Google Chrome para administrar los puntos de acceso (AP).

El sistema de gestión web consta de dos partes: servidor web y cliente web. Un servidor web está integrado en el dispositivo para recibir y procesar las solicitudes de un cliente y devolver el resultado del procesamiento al cliente. Normalmente, un cliente web se refiere a un navegador web, como Internet Explorer y Google Chrome.

1.2 Conexión al dispositivo

El sistema de gestión web consta de dos partes: servidor web y cliente web. Un servidor web está integrado en el dispositivo para recibir y procesar las solicitudes de un cliente y devolver el resultado del procesamiento al cliente.

Como se muestra en la siguiente figura, un administrador puede acceder y configurar el dispositivo en el sistema de administración web a través del navegador web. El sistema de gestión web integra comandos de configuración y los envía al dispositivo a través de solicitudes asíncronas de JavaScript y XML (AJAX). El servicio web está habilitado en el dispositivo para procesar solicitudes HTTP básicas y devolver los datos solicitados en función de los comandos.

Figure 1-1 Topología de la aplicación

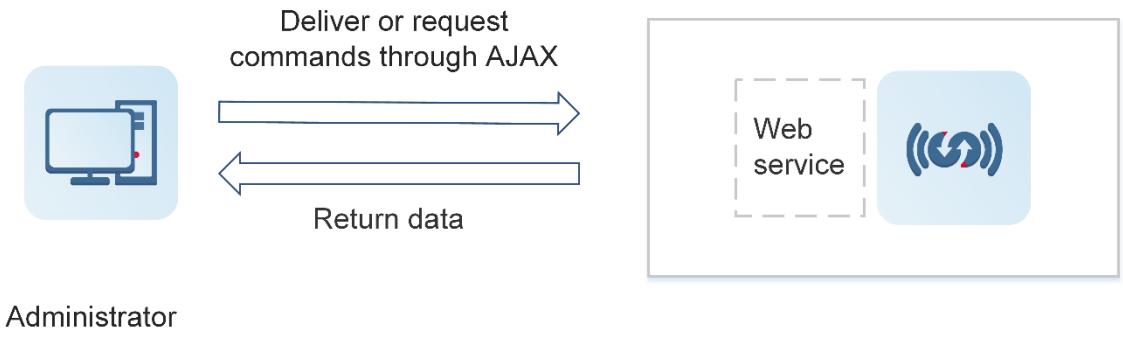
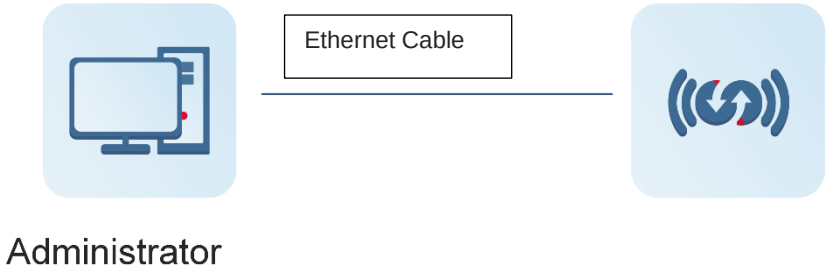


Figure 1-2 Topología simplificada



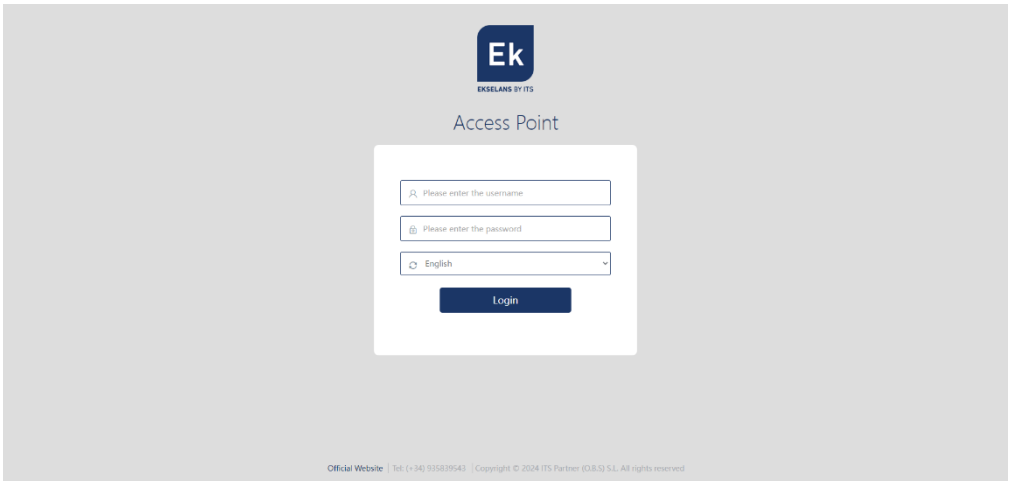
1.3 Entorno de configuración para clientes de PC

- Un administrador inicia sesión en el sistema de administración web para administrar el dispositivo a través del navegador web en un cliente. Normalmente, un cliente se refiere a un

PC. También puede ser otro terminal móvil como un ordenador portátil o un iPad. Los teléfonos móviles no son compatibles.

- Navegador web: Se recomienda Google Chrome. Internet Explorer 11 y 360 Secure Browser también son compatibles. Pueden producirse excepciones, como caracteres ilegibles o errores de formato, cuando se utilizan otros navegadores.
- Resolución: Se recomienda establecer la resolución en 1280 píxeles x 1024 píxeles, 1920 píxeles x 1080 píxeles o 1440 píxeles x 960 píxeles. Pueden producirse excepciones, como errores de alineación de fuentes y errores de formato, cuando se seleccionan otras resoluciones.

1.4 Entorno de servicio web para un AP



Introduzca el nombre de usuario y la contraseña y haga clic en **Iniciar sesión**. En la tabla siguiente se proporcionan el nombre de usuario y la contraseña predeterminados.

Nombre de usuario/contraseña predeterminada	**Descripción**
admin / admin	Superadministrador con todos los permisos.

1.5 Habilitación del servidor web

El AP está habilitado con el servicio web y configurado con la dirección IP 192.168.110.1 de forma predeterminada. A continuación, se describe cómo habilitar el servicio web mediante la interfaz de línea de comandos (CLI).

Configuración	**Mandar**	
Configuración del servidor web	**Habilitar servidor web de servicio**	Habilita el servicio web.
	dirección IP	(Opcional) Configura una dirección IP.
	Nombre de usuario de nivel webmaster Contraseña	(Opcional) Configura el nombre de usuario y la contraseña para iniciar sesión en el sistema de gestión web.

1.5.1 Pasos de configuración

Habilitación del servicio web

- Obligatorio.
- Habilite el servicio web en el AP.

Configuración de una dirección IP

- Opcional.

Configuración del nombre de usuario y la contraseña para iniciar sesión en el sistema de gestión web

- Opcional.
- Cuando el servicio web está habilitado, el nombre de usuario y la contraseña del administrador son **admin** y **admin** respectivamente, y el nombre de usuario y la contraseña del invitado son **invitado** e **invitado** respectivamente de forma predeterminada. Los usuarios pueden crear otras cuentas.

1.5.2 Verificación

Inicie sesión en el sistema de gestión web con la dirección IP, el nombre de usuario y la contraseña configurados para comprobar si puede iniciar sesión correctamente.

1.5.3 Comando relacionado

Habilitación del servicio web

Comando	**Habilitar servidor web de servicio** [**http** | **https** | **all**]
Descripción del parámetro	**http** | **https** | **all**: Habilita el servicio correspondiente. **http**: Habilita el servicio HTTP. **https**: Habilita el servicio HTTPS. **all**: Habilita los servicios HTTP y HTTPS. Los servicios HTTP y HTTPS están habilitados de forma predeterminada.
Modo de comando	Modo de configuración global

Configuración de una dirección IP

Comando	**dirección IP** *dirección IP máscara de IP*
Descripción del parámetro	*ip-address*: Indica la dirección IP. *mask*: Indica la máscara de subred.
Modo de comando	Modo de configuración de la interfaz

Configuración del nombre de usuario y la contraseña para iniciar sesión en el sistema de gestión web

Comando	**Nivel de webmaster** *Nombre de usuario de nivel de privilegio Nombre de* **usuario** *contraseña* **{** *contraseña* | [**0 | 7**] *contraseña-encriptada*
Descripción del parámetro	*privilege-level*: Indica el nivel de privilegio de los usuarios, incluidos los niveles de privilegio 0, 1 y 2. El administrador predeterminado de la cuenta **de administrador admin** y la cuenta de invitado guest tienen permisos de los niveles de privilegio 0 y 2 respectivamente. Otras cuentas creadas manualmente tienen permisos de nivel de privilegio 1. *name*: Indica el nombre de usuario. *password*: Indica la contraseña. **0 | 7**: Indica los tipos de cifrado de contraseña, **0** para ningún cifrado y **7** para el cifrado simple. El valor predeterminado es **0**. *encrypted-password*: Indica el texto de la contraseña.
Modo de comando	Modo de configuración global
Guía de uso	N/A

1.5.4 Ejemplos de configuración

Configuración del servidor web

Pasos de configuración	Habilite el servicio web. Configure una dirección IP de administración para el dispositivo. La VLAN de administración predeterminada es la VLAN 1. Configure una dirección IP para VLAN 1 y asegúrese de que los usuarios puedan hacer ping a la dirección IP de administración correctamente desde sus PC.
	Hostname# configurar terminal Hostname(config)# habilitar el servidor web del servicio Hostname(config)# webmaster nivel 0 nombre de usuario prueba de contraseña Nombre de host (configuración)#interface vlan 1 Hostname(config-if-VLAN 1)#ip dirección 192.168.1.200 255.255.255.0 Hostname(config)# end
Verificación	Ejecute el **comando show running-config** para mostrar la configuración.
	Hostname(config)#show running-config Configuración del edificio... Configuración actual : 6312 bytes ! hostname Nombre de host ! ! webmaster level 0 username test password test //Nombre de usuario y contraseña para la autenticación de gestión web Detección automática del modo de actualización HTTP ! ! VLAN de interfaz 1 Dirección IP 192.168.1.200 255.255.255.0 //Dirección IP de administración del dispositivo Sin apagado ! línea con 0 línea vty 0 4 Iniciar sesión ! ! Fin

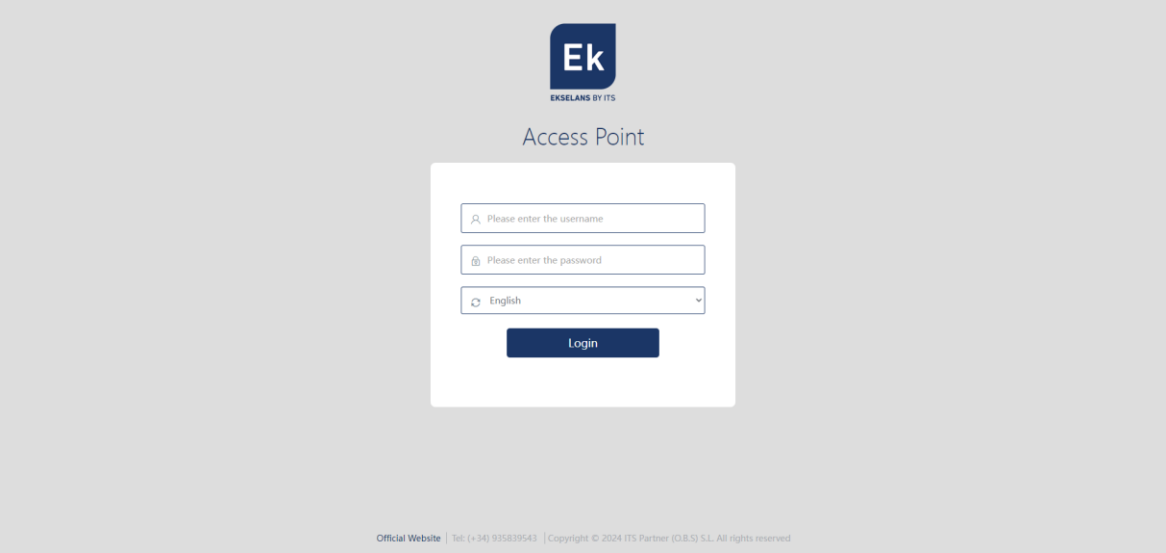
2 Configuración rápida

2.1 Inicio de sesión en el sistema de gestión web

Se le pedirá que cambie la contraseña la primera vez que inicie sesión en el sistema de gestión web. Se recomienda establecer una contraseña compleja. Utilice la nueva contraseña la próxima vez que inicie sesión.

⚠ Cautela

Si hay cinco intentos fallidos consecutivos de inicio de sesión en 10 minutos, su cuenta se bloqueará durante 10 minutos.



2.2 Asistente de configuración

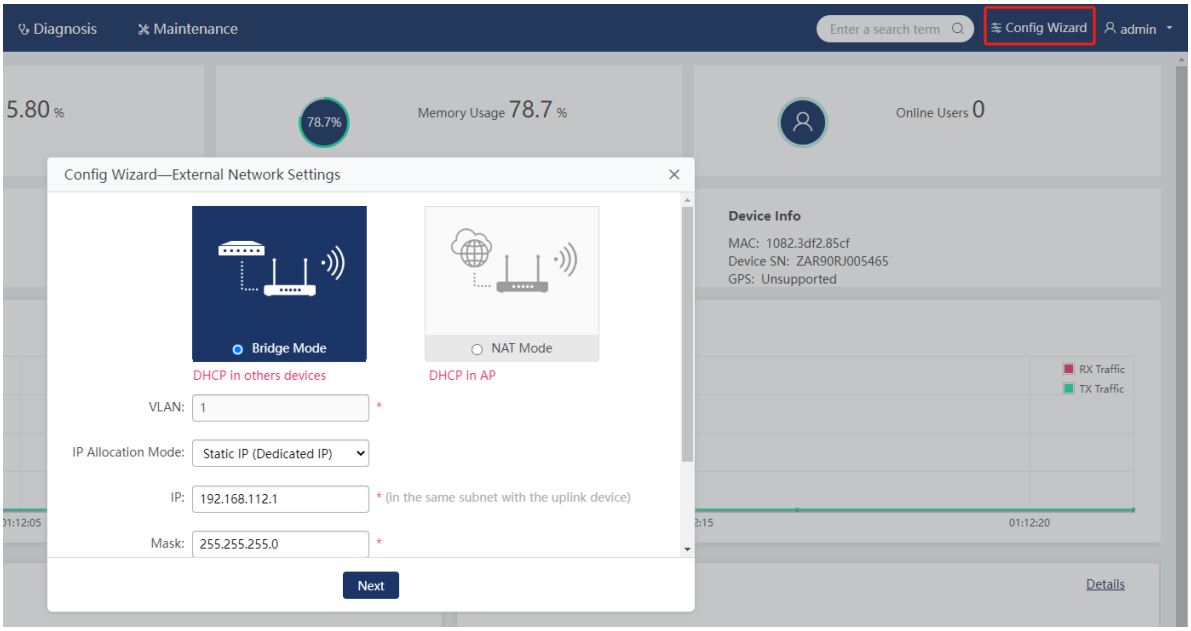
El asistente de configuración proporciona algunas configuraciones comunes basadas en escenarios. Por lo general, se usa para la primera configuración. Haga clic **en Asistente de configuración** en la barra de navegación.

1. Cuando inicie sesión en el sistema de administración web, el sistema identificará automáticamente si el dispositivo actual está configurado. Si no es así (no se encuentra ningún archivo config.text), aparecerá la ventana del **Asistente de configuración** para guiarlo a través de la configuración.
2. El **Asistente** de configuración permite la configuración de solo una o dos WLAN para configurar una red Wi-Fi.
3. Una vez completado el **Asistente de configuración**, se sobrescribirán las configuraciones existentes del dispositivo.

El **Asistente de configuración** incluye configuraciones de red externas y configuraciones de Wi-Fi.

2.2.1 Configuración de red externa

Establezca el modo de trabajo del dispositivo en **modo puente** o **modo NAT**.

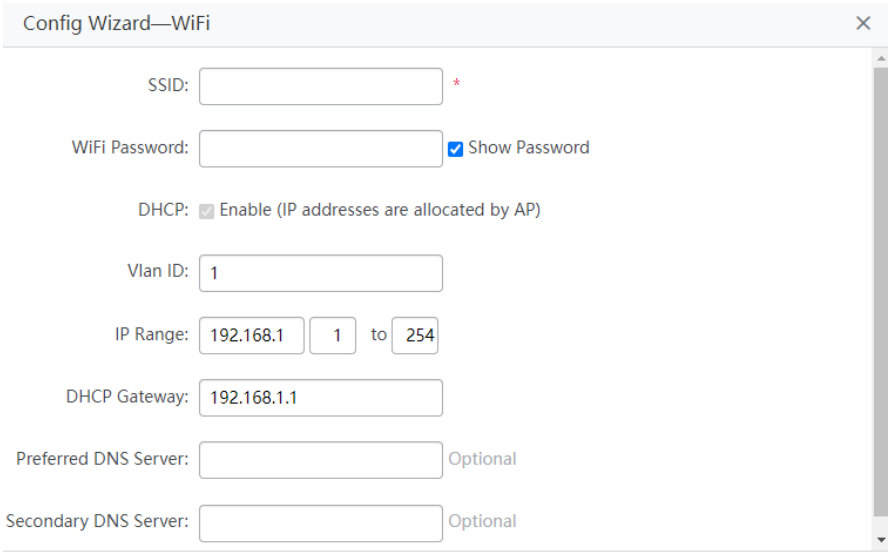


Modo de trabajo	Parámetro	Descripción		
Modo puente	**Nota** En el modo puente, la puerta de enlace y el servidor DHCP se despliegan en el dispositivo de enlace ascendente del AP.			
	VLAN	Ingrese la VLAN para que el AP se comunique con una red externa.		
	Modo de asignación de IP	IP estática (IP dedicada)	IP	Introduzca una dirección IP estática.
			Máscara	Introduzca la máscara de subred para la dirección IP estática.
		DHCP (IP dinámica)	DHCP IP	Muestra la dirección IP DHCP obtenida.
	Puerta de enlace predeterminada	(Opcional) Introduzca la dirección de gateway del AP.		

<table>
<tr><th>Modo de trabajo</th><th>Parámetro</th><th colspan="3">Descripción</th></tr>
<tr><td rowspan="11">Modo NAT</td><td colspan="4">Nota
En el modo NAT, la puerta de enlace y el servidor DHCP se configuran en el AP.</td></tr>
<tr><td>Puerto WAN</td><td colspan="3">Ingrese el puerto WAN para que el AP se comunique con una red externa.</td></tr>
<tr><td rowspan="9">Modo de asignación de IP</td><td rowspan="3">IP estática (IP dedicada)</td><td>IP</td><td>Introduzca una dirección IP estática.</td></tr>
<tr><td>Máscara IP</td><td>Introduzca la máscara de subred para la dirección IP estática.</td></tr>
<tr><td>Puerta de enlace predeterminada</td><td>Introduzca la dirección de gateway del AP.</td></tr>
<tr><td rowspan="3">PPPoE (línea ADSL)</td><td>Cuenta</td><td>Introduzca el nombre de usuario PPPoE para el acceso a Internet.</td></tr>
<tr><td>Contraseña</td><td>Introduzca la contraseña PPPoE para el acceso a Internet.</td></tr>
<tr><td>PPPoE IP</td><td>Muestra la dirección IP PPPoE obtenida.</td></tr>
<tr><td rowspan="2">DHCP (IP dinámica)</td><td>Puerta de enlace predeterminada</td><td>(Opcional) Introduzca la dirección de gateway del AP.</td></tr>
<tr><td>DHCP IP</td><td>Muestra la dirección IP DHCP obtenida.</td></tr>
<tr><td>NAT</td><td colspan="3">Habilite esta función cuando todas las direcciones IP internas deban traducirse a direcciones IP externas.</td></tr>
</table>

2.2.2 Wi-Fi

Establezca los parámetros de Wi-Fi y haga clic en **Finalizar**.

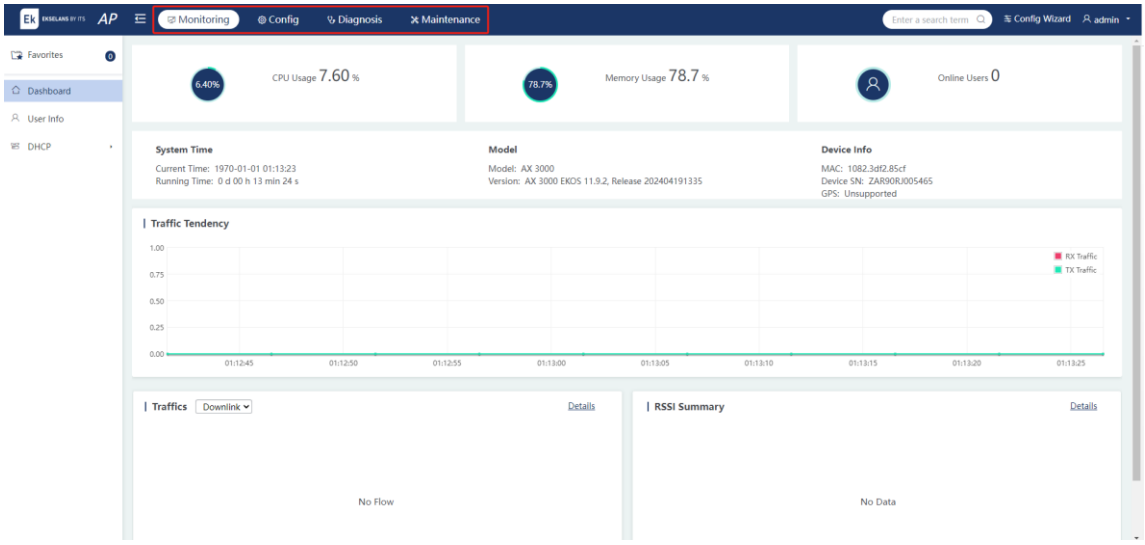


Parámetro	Descripción
SSID	Establezca el identificador de conjunto de servicios (SSID), es decir, el nombre de Wi-Fi.
Contraseña Wi-Fi	Establezca la contraseña de Wi-Fi.
DHCP	Una vez seleccionada esta opción, el servicio DHCP se habilita en el dispositivo.
Vlan ID	Introduzca la VLAN asociada al usuario.
Rango de IP	Introduzca el rango del grupo de direcciones utilizado por el usuario.
Puerta de enlace DHCP	Introduzca la dirección de puerta de enlace del grupo de direcciones utilizado por el usuario.
Servidor DNS preferido	Introduzca la dirección del servidor DNS principal del grupo de direcciones utilizado por el usuario.
Servidor DNS secundario	Introduzca la dirección del servidor DNS secundario del grupo de direcciones utilizado por el usuario.

3 Interfaz gráfica de usuario web

3.1 Página principal

La GUI web incluye cuatro módulos principales: **Supervisión**, **Configuración**, **Diagnóstico** y **Mantenimiento**. Haga clic en estos módulos en la barra de navegación para ver las configuraciones de cada módulo.



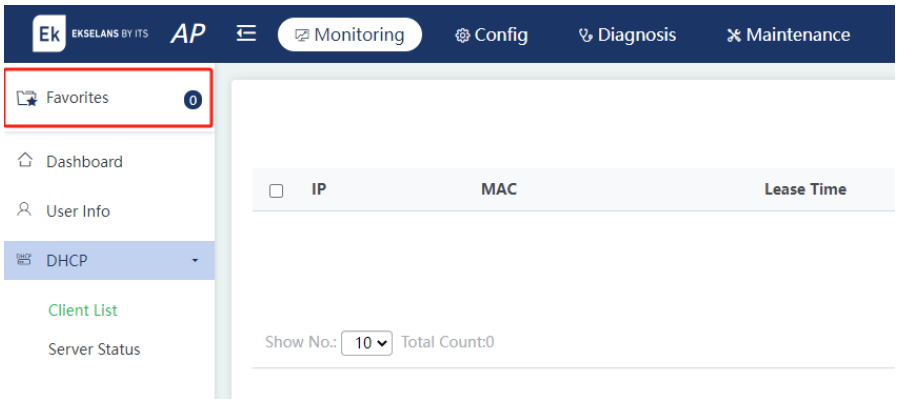
3.2 Favoritos

Esta función le permite marcar las funciones de uso frecuente. Haga clic en **Favoritos** para expandir la lista de elementos marcados e ingresar rápidamente a la página de configuración.

Nota

Se pueden agregar hasta 10 elementos de configuración a **Favoritos**.

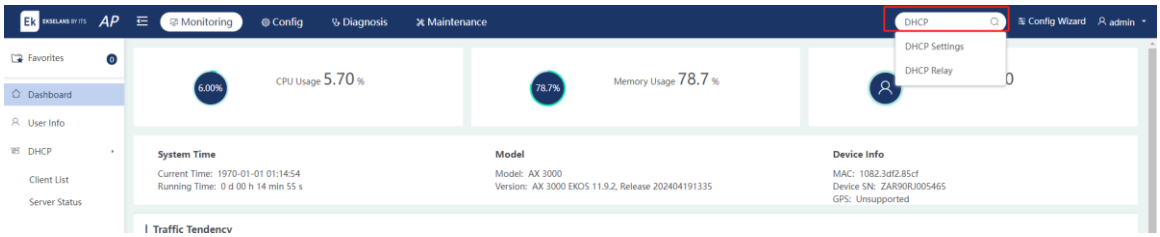
(1) Agregar a favoritos: haga clic y arrastre un elemento del menú a **Favoritos**.



(2) Eliminar de favoritos: seleccione un elemento y haga clic en el × icono. Haga clic en Aceptar para eliminar el elemento de **Favoritos**.

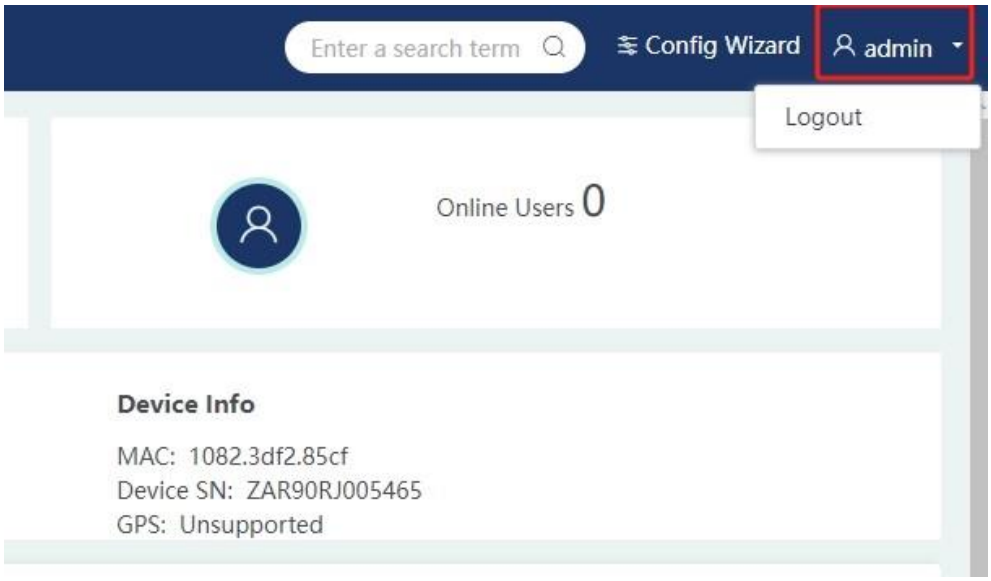
3.3 Barra de búsqueda

Dadas las amplias funciones del sistema, es posible que le resulte difícil localizar un elemento de configuración específico. Introduzca palabras clave en la barra de búsqueda para buscar los elementos de configuración e ingrese rápidamente a la página de configuración.



3.4 Otras funciones

(1) Visualización de la cuenta corriente.



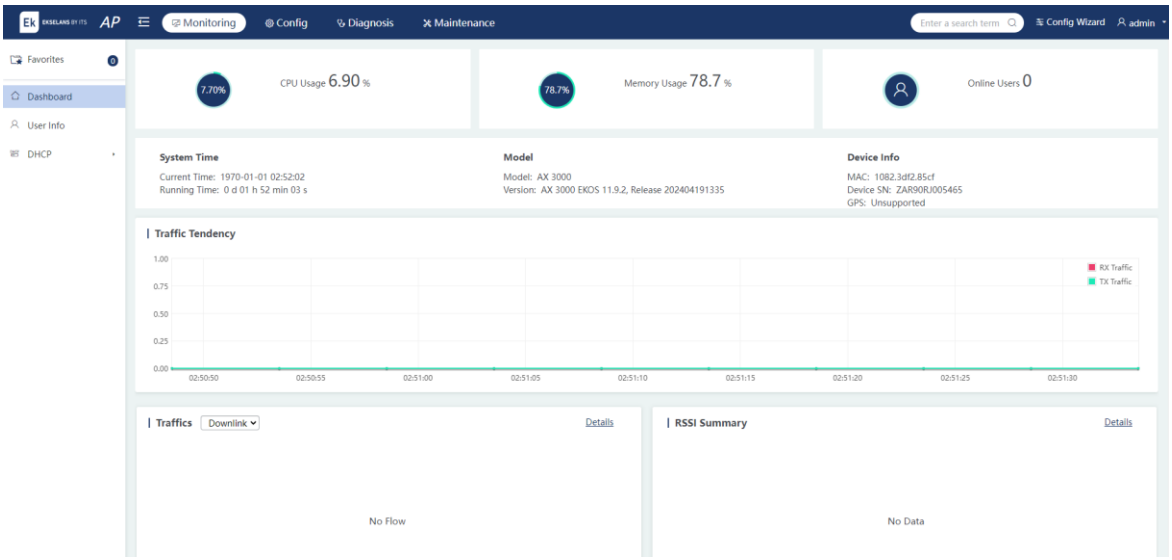
(2) Cerrar sesión: Haga clic en **Cerrar sesión** después de expandir el menú de la cuenta para cerrar sesión en el sistema de administración web.

4 Monitorización

4.1 Dashboard

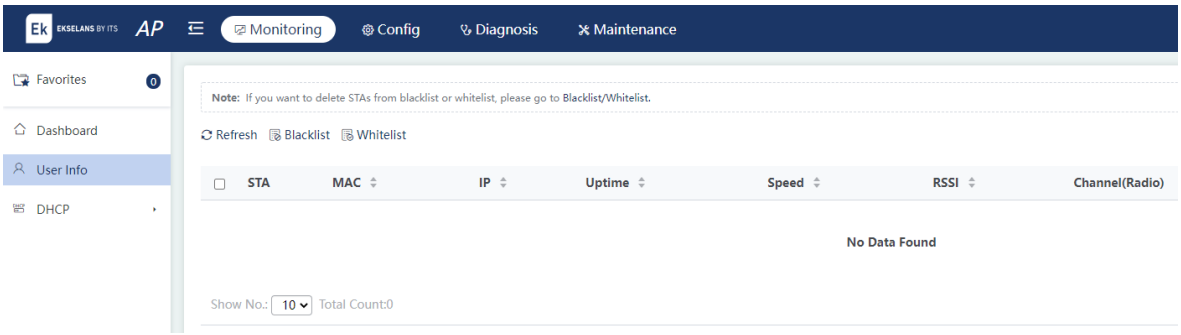
Elija **Monitoring >** Dashboard (Supervisión) (Supervisión **panel de control**).

En la página Panel **de control**, puede ver la información básica sobre el AP, incluido el uso de la CPU, el uso de la memoria, la cantidad de STA en línea, la hora del sistema, el modelo y la versión, la información del dispositivo, la tendencia del tráfico, el tráfico de usuarios y el resumen del indicador de intensidad de señal recibida (RSSI).



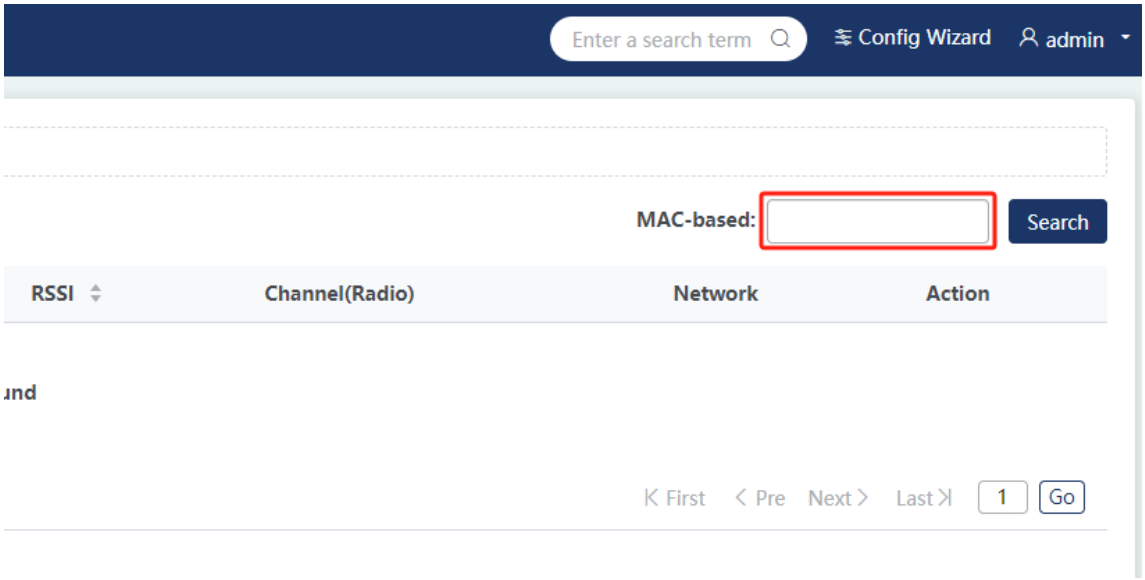
4.2 Información del usuario

Elija **Monitoring (Supervisión> User Info (Información de usuario**).



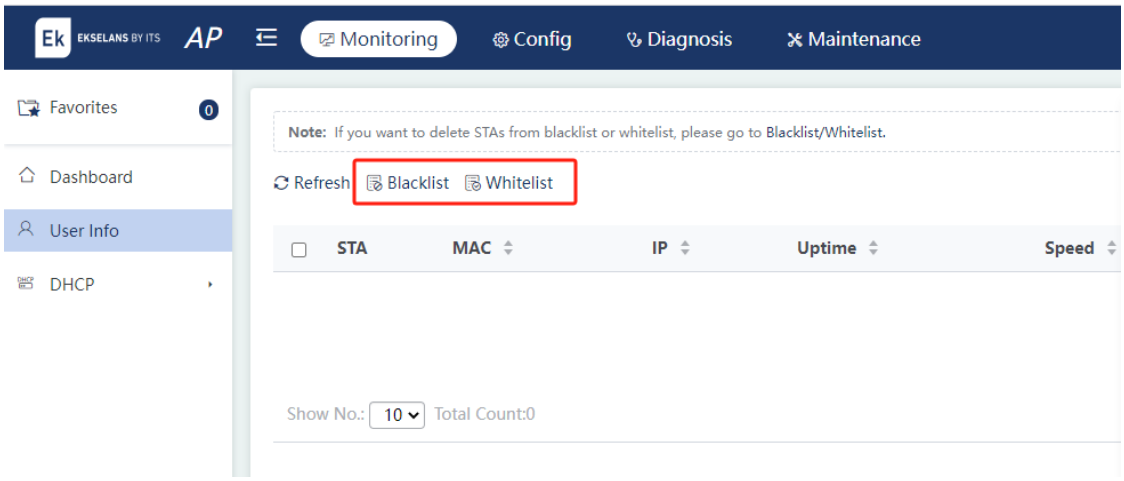
(1) Búsqueda de STA

Si hay numerosos STA, introduzca una dirección MAC en el cuadro de búsqueda y haga clic en **Buscar** para buscar un STA específico. Para mostrar todas las listas de STA, borre la dirección MAC en el cuadro de búsqueda y haga clic en **Actualizar**.



(2) Agregar a la lista negra o a la lista blanca

Seleccione los STA que se agregarán a la lista negra o a la lista blanca. Haga clic en **Lista negra** o **Lista blanca**.

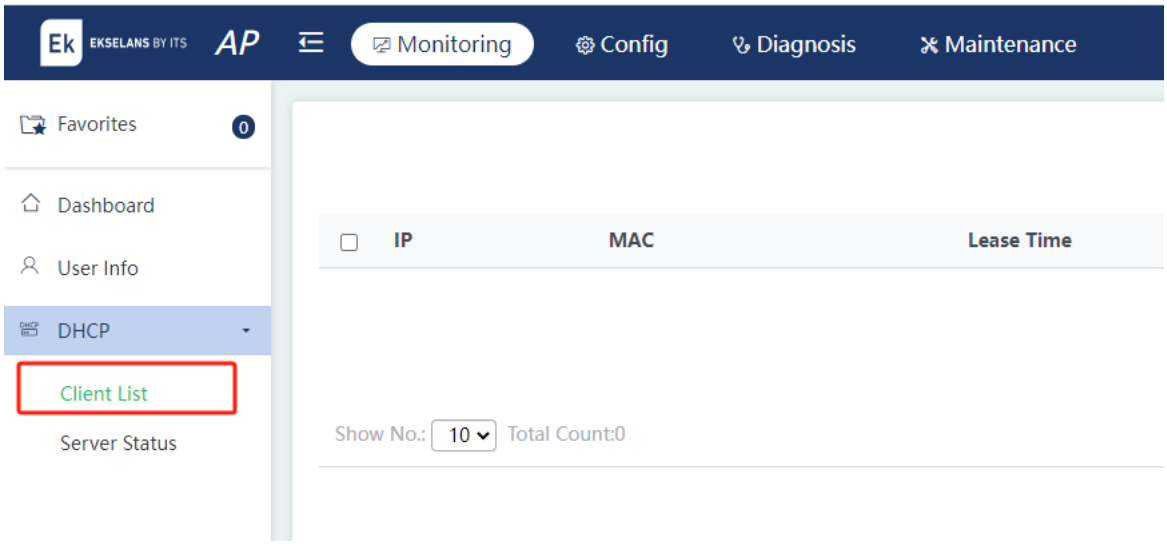


4.3 DHCP

4.3.1 Lista de clientes

Elija **Monitoring** > **DHCP** > **Client List**.

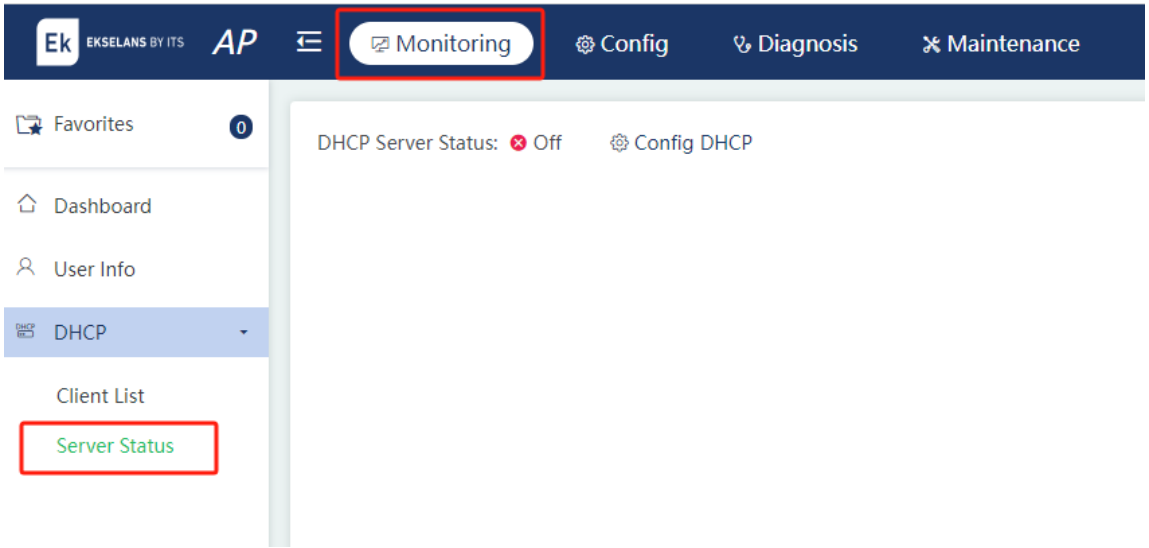
La página **Lista de clientes** muestra los clientes asignados con direcciones del grupo de direcciones.



4.3.2 Estado del servidor DHCP

Elija **Monitoring** > **DHCP** > **Server Status**.

La página **Estado del servidor** muestra el estado del servidor DHCP y el uso del grupo de direcciones.



5 Configuración

5.1 Configuración inalámbrica

5.1.1 Añadir Wi-Fi

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

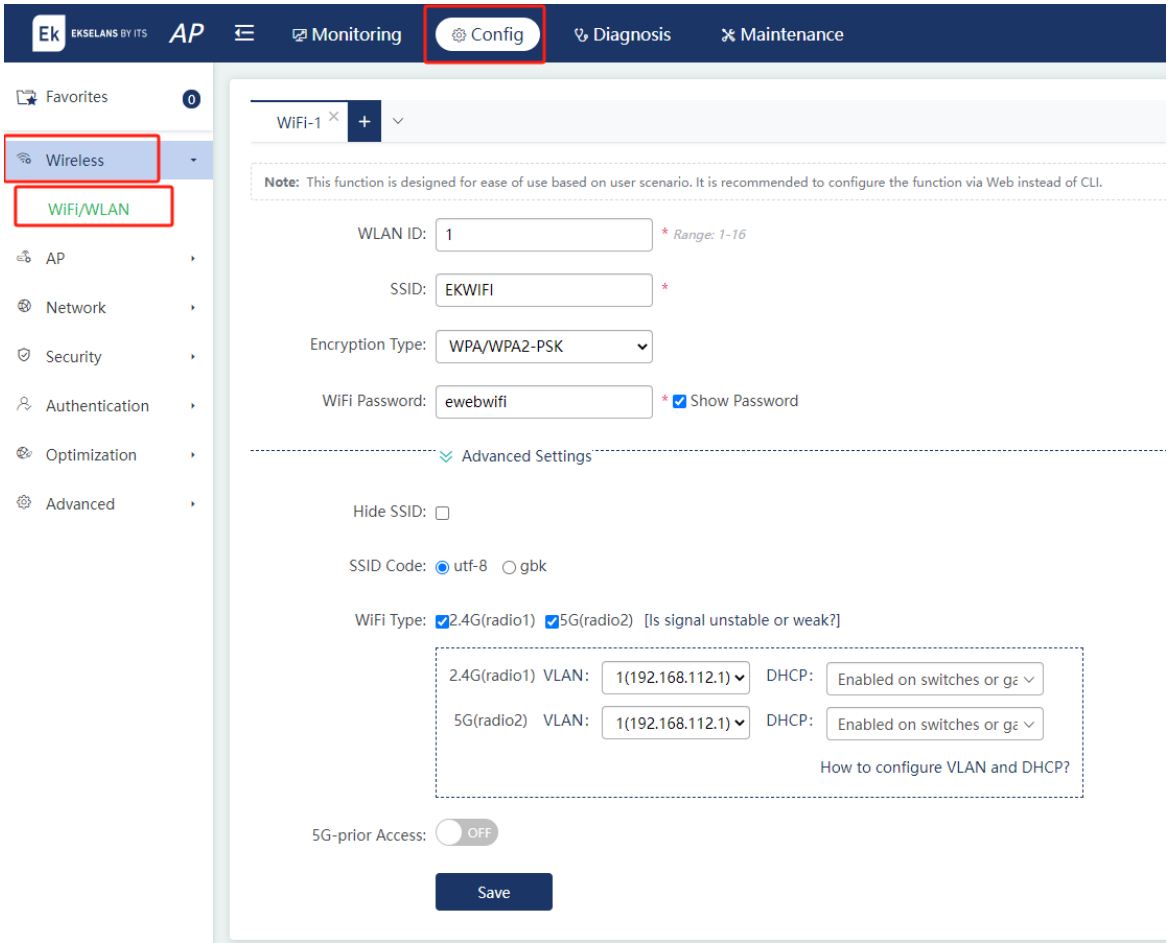
Una red Wi-Fi permite que los STA inalámbricos se asocien con el AP para el acceso a la red. Se pueden agregar o eliminar varias redes Wi-Fi.

Nota

El número máximo de redes Wi-Fi está sujeto a los modelos de dispositivo.

1. Agregar una red Wi-Fi

Haga clic en **+** para agregar una red Wi-Fi. Una vez configurados los parámetros de Wi-Fi, haga clic en **Guardar**.



Parámetro	Descripción
WLAN ID	Introduzca el ID de WLAN.
SSID (en inglés)	Introduzca el nombre de la red Wi-Fi.
Tipo de cifrado	**Abierto**: no se ha configurado ningún tipo de cifrado. No se requiere contraseña cuando un STA se asocia con la red Wi-Fi. **WPA/WPA2-PSK**: Modo WPA con clave precompartida de alta seguridad y fácil configuración, aplicable a hogares y pequeñas empresas. **WPA/WPA2-802.1X**: Modo WPA o WPA2 que utiliza un servidor RADIUS para la autenticación y la adquisición de claves. No se recomienda a los usuarios comunes que adopten este modo, ya que requiere un servidor de autenticación exclusivo. **WPA2-802.1X**: Modo WPA2 que utiliza un servidor RADIUS para la autenticación y la adquisición de claves. **WPA3-PERSONAL:** En comparación con WPA2, es más seguro y puede prevenir eficazmente los ataques de diccionario. **WPA3-ENTERPRISE-GCMP256**: WPA3-Enterprise está configurado con cifrado GCMP-256, lo que proporciona protección adicional para las redes en las que se transmiten datos confidenciales. Es aplicable a redes sensibles a los datos, como el gobierno o los sistemas financieros. **WPA3-ENTERPRISE-CCMP128**: WPA3-Enterprise está configurado con cifrado CCMP-128, lo que proporciona protección adicional para las redes en las que se transmiten datos confidenciales. Es aplicable a redes sensibles a los datos, como el gobierno o los sistemas financieros. **WPA2/WPA3**: Modo de transición WPA2/WPA3, que está determinado por un STA.
Contraseña de WiFi	Ingresa la contraseña de Wi-Fi.
Ocultar SSID	Si habilita Ocultar **SSID**, el SSID no se muestra en la lista de Wi-Fi de un STA. Solo puede buscar manualmente el SSID.
Código SSID	**UTF-8**: Se recomienda seleccionar **utf-8**, ya que la mayoría de los STA admiten la codificación UTF-8 de forma predeterminada. **GBK**: Algunos STA, PC y tarjetas de interfaz de red (NIC) admiten la codificación GBK. Puede especificar el modo de codificación según sea necesario.

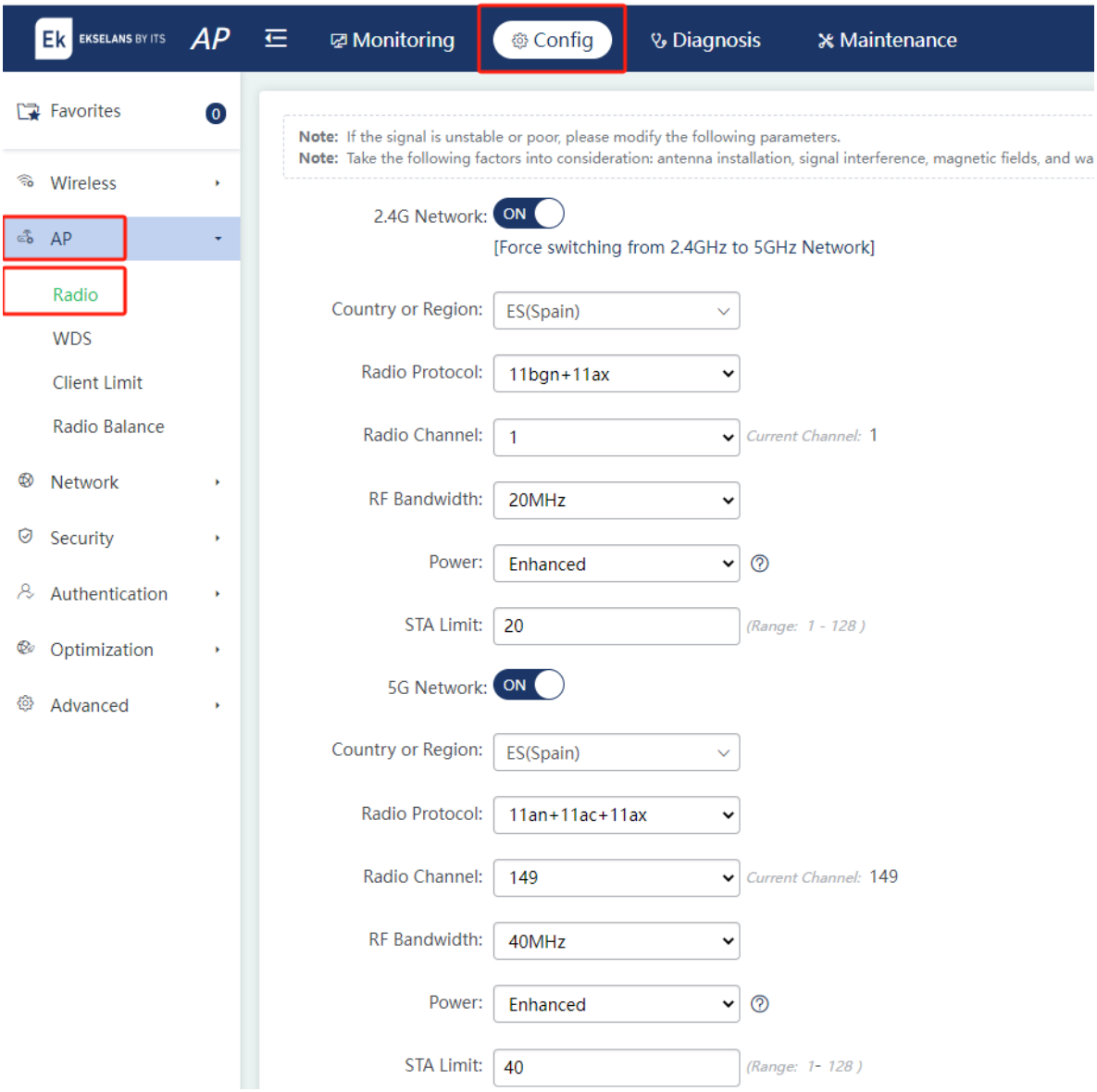
Parámetro	Descripción
Tipo de WiFi	Especifique los tipos de red compatibles con la red Wi-Fi. Puede seleccionar varios tipos de red. **Nota** • Haga clic en **¿La señal es inestable o débil?** para ir a la página **Radio**, donde puede configurar una radio. • Haga clic **en VLAN** para agregar una VLAN en la **página VLAN**. VLAN determina si el AP puede comunicarse con el switch de enlace ascendente o el dispositivo de salida, y si los STA conectados a la red Wi-Fi del AP pueden acceder a Internet. La dirección IP de la VLAN se puede utilizar como dirección de administración del AP. • Haga clic en **DHCP** para ir a la página **Configuración de DHCP**. En esta página, puede agregar un conjunto de direcciones DHCP para que el AP asigne direcciones IP a los STA conectados al AP (es necesario cuando el AP funciona en modo NAT). Si el AP funciona en modo puente, no es necesario configurar DHCP porque el servicio DHCP está configurado en el switch de enlace ascendente o de salida. En este caso, el AP solo desempeña una función inalámbrica y no funciona como puerta de enlace ni asigna direcciones IP.
Límite de velocidad	Si no establece un límite de frecuencia, la tarifa no está limitada de forma predeterminada. Para establecer las tarifas máximas de carga y descarga, haz clic en **Configuración del límite de frecuencia**.
5G-Acceso previo	Si esta función está habilitada, los STA accederán preferentemente a la radio de 5 GHz. Está deshabilitado de forma predeterminada.

5.2 AP

5.2.1 Radio

Elija **Config** > **AP** > **Radio**.

Si la señal es inestable o la intensidad de la señal es baja, puede modificar manualmente los parámetros de la radio para ajustar la intensidad de la señal de la transmisión Wi-Fi por el dispositivo.



Parámetro	Descripción
Interfaz inalámbrica	Radio del dispositivo. Si el dispositivo admite radios duales, es decir, **dot11radio 1/0** y **dot11radio 2/0**, no se muestra el campo **Interfaz inalámbrica**. Si el dispositivo admite tres radios, es decir, **dot11radio 1/0**, **dot11radio 2/0** y **dot11radio 3/0**, **se mostrará el campo** Interfaz inalámbrica.
Red 2.4G Red 5G	Habilite o deshabilite la radio de 2,4 GHz o 5 GHz.
País o región	Seleccione el código de país o región configurado para la radio.
Protocolo de radio	Seleccione los protocolos 802.11 configurados para la radio. ● Las opciones de protocolo disponibles en la radio de 2,4 GHz incluyen:

Parámetro	Descripción
	○ **11BGN** indica los protocolos 802.11b, 802.11g y 802.11n. ○ **11BGN+11AX** indica los protocolos 802.11b, 802.11g, 802.11n y 802.11ax. ● Las opciones de protocolo disponibles en la radio de 5 GHz incluyen: ○ **11an** indica los protocolos 802.11a y 802.11n. ○ **11an+11ac** indica los protocolos 802.11a, 802.11n y 802.11ac. ○ **11AN+11AC+11ax** indica los protocolos 802.11a, 802.11n, 802.11ac y 802.11ax.
Canal de radio	Seleccione el canal configurado para la radio.
Ancho de banda de RF	Seleccione el ancho de canal configurado para la radio.
Poder	Seleccione la alimentación de la radio. ● Ahorro de energía: 30 dBm. ● Estándar: 80 dBm. ● Mejorado: 100 dBm. ● Personalizado: Puede configurar la potencia de la radio.
Límite de STA	Introduzca el número máximo de STA asociados a la radio. **Nota** El número máximo de STA admitidos varía según el modelo de dispositivo. Prevalecerá el rango real que se muestra en la página.

5.2.2 WDS

Nota

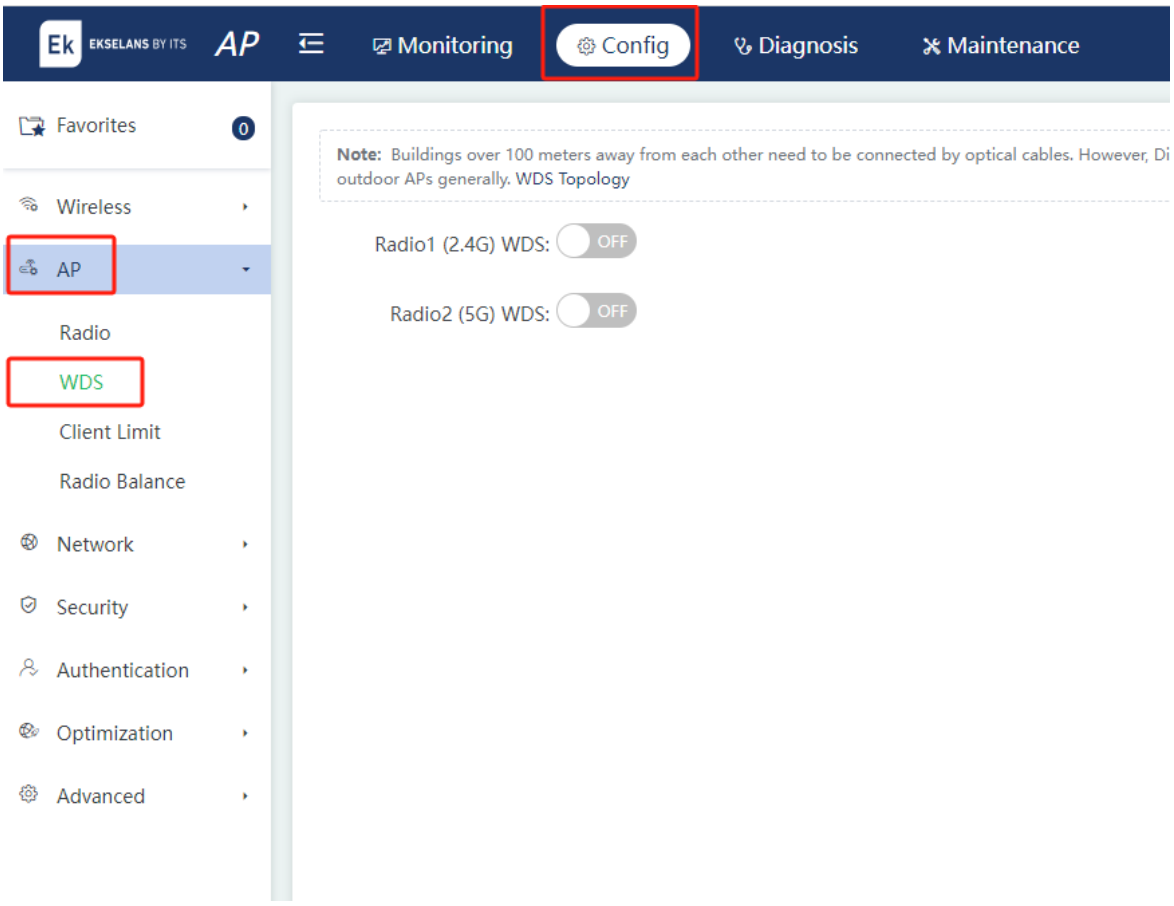
Es posible que algunos AP no admitan esta función. Prevalecerá el menú real.

Elija **Config** > **AP** > **WDS**.

Si la distancia entre edificios es de más de 100 metros (328,08 pies), es necesario desplegar cables ópticos. Para algunos edificios que se han construido, la excavación de carreteras o la instalación de líneas aéreas causarán una gran dificultad y costo de construcción, como entre los edificios de gran altura o entre dos edificios separados por un río. En este caso, se utiliza el sistema de distribución inalámbrica (WDS) para implementar la interconexión de red, lo que permite una implementación rentable y que ahorra esfuerzo. Se interconectan múltiples AP a través de WDS o modo de puente/repetidor inalámbrico para conectarse a redes distribuidas y extender las señales

inalámbricas. Un AP puede funcionar como un repetidor para ampliar el alcance de la red front-end y las señales Wi-Fi, lo que permite a los usuarios que se encuentran a una gran distancia conectarse a la red. WDS admite puentes en las radios de 2,4 GHz y 5 GHz.

Habilite la función de puente en la radio de 2,4 GHz o 5 GHz según sea necesario. Seleccione el modo de funcionamiento y configure los parámetros. Haga clic en **Guardar**.



Modo de funcionamiento	Parámetro	Descripción
Puente de raíz	Red de puente raíz	Seleccione la red en la que se deben extender las señales inalámbricas.
	Distancia	Introduzca la distancia entre dos dispositivos de puente inalámbrico (puente raíz y puente no raíz).
Puente no raíz	Elección de puente raíz	Elija el puente raíz en función de la dirección MAC o SSID.
	MAC de puente raíz	Introduzca la dirección MAC del puente raíz.
	Contraseña de	Establezca la contraseña del puente raíz Wi-Fi.

Modo de funcionamiento	Parámetro	Descripción
	Bridge WiFi	
	Distancia	Introduzca la distancia entre dos dispositivos de puente inalámbrico (puente raíz y puente no raíz).
	Otros WiFi permitidos	La radio se puede utilizar como puente o para transmitir señales Wi-Fi.

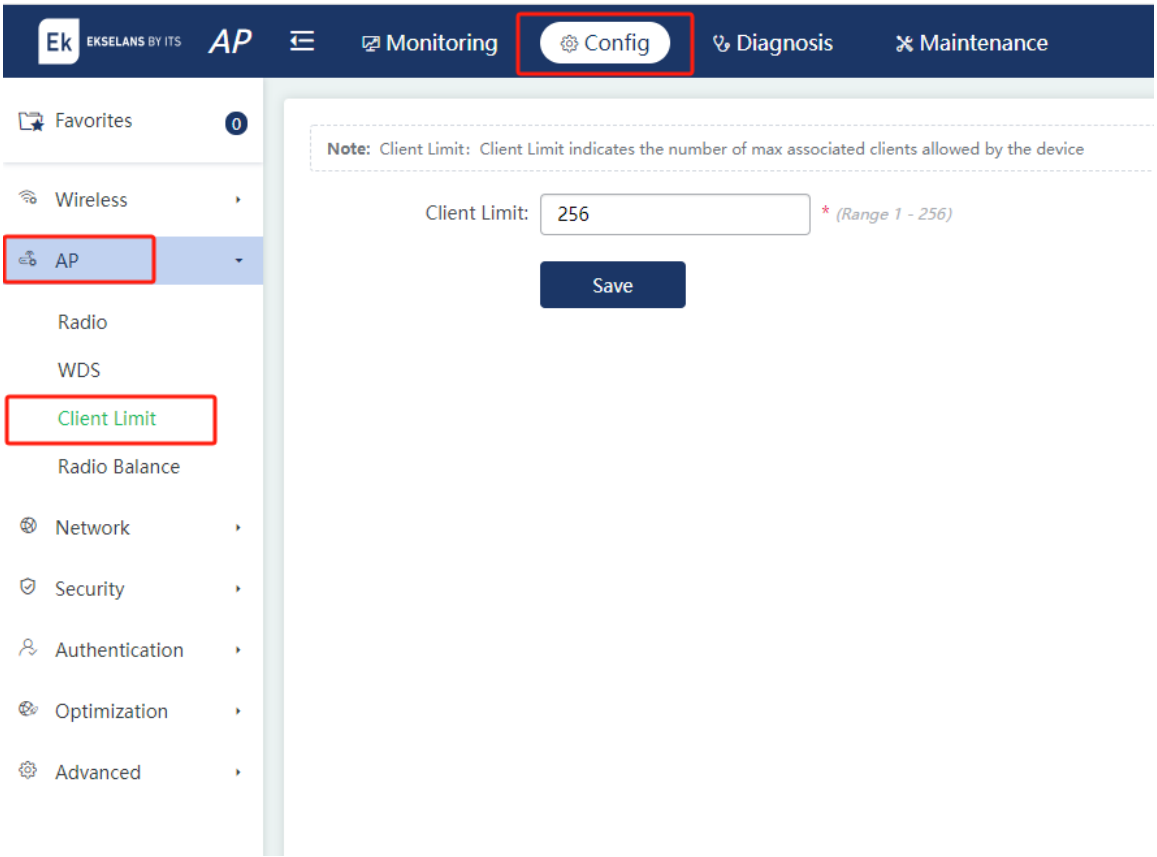
5.2.3 Límite de clientes

Elija **Config** > **AP** > **Client Limit**.

Esta función se utiliza para configurar el número máximo de clientes asociados con el AP.

Nota

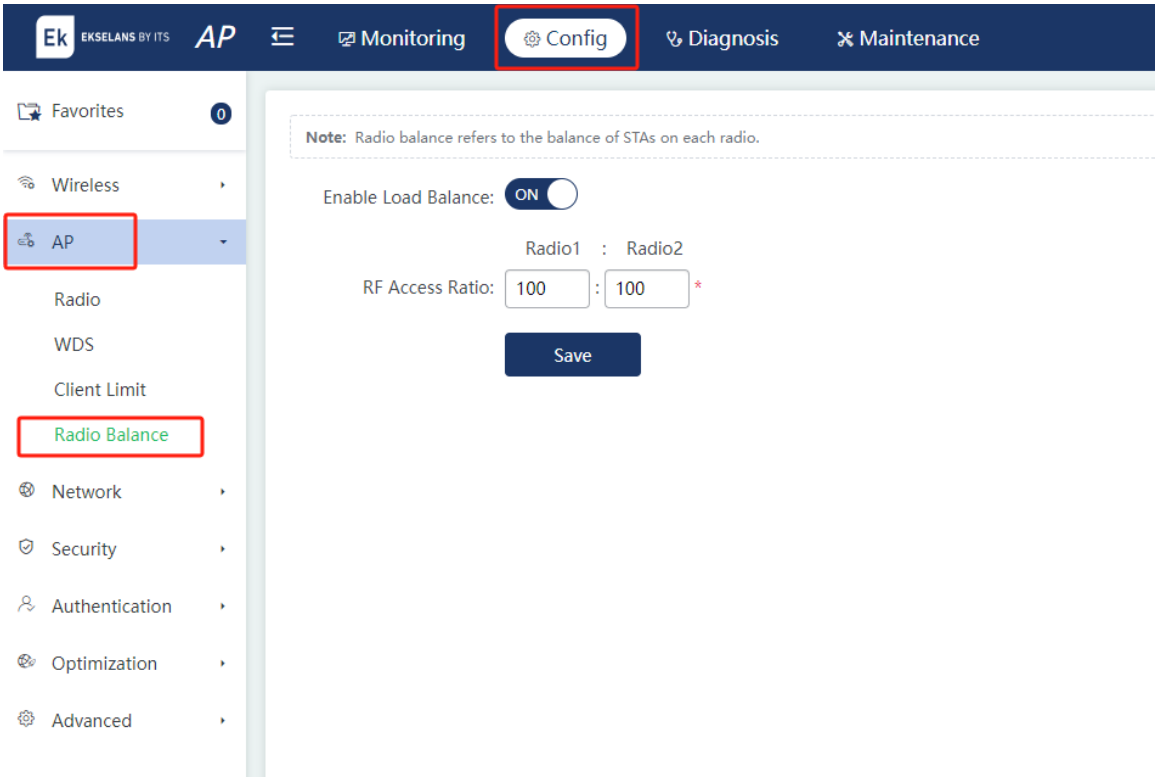
El número máximo de clientes asociados varía según el modelo de dispositivo. Prevalecerá el valor mostrado en la página.



5.2.4 Radio Balance

Elija **Config** > **AP** > **Radio Balance**.

Actualmente, el equilibrio de carga en las radios se implementa solo en función del número de STA. Una vez habilitada la función de equilibrio de carga, puede establecer la proporción de STA conectados a diferentes radios.



5.3 Red

5.3.1 Red externa

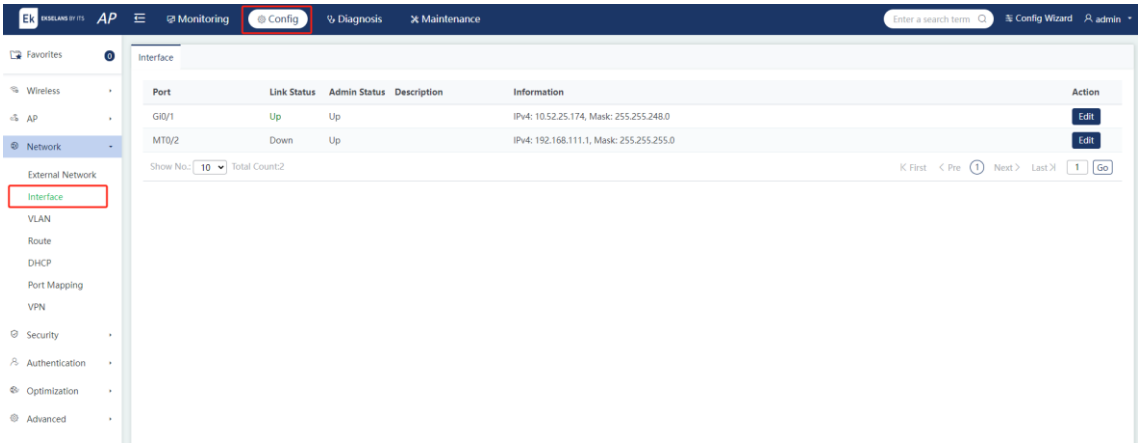
Elija **Config** > **Network > External Network (Red externa**).

Establezca el modo de trabajo del AP en **Modo puente** o **Modo NAT**. La configuración es la misma que la de la configuración de red externa del Capítulo 2. Para obtener más información, consulte2.2.1 Configuración de red externa.

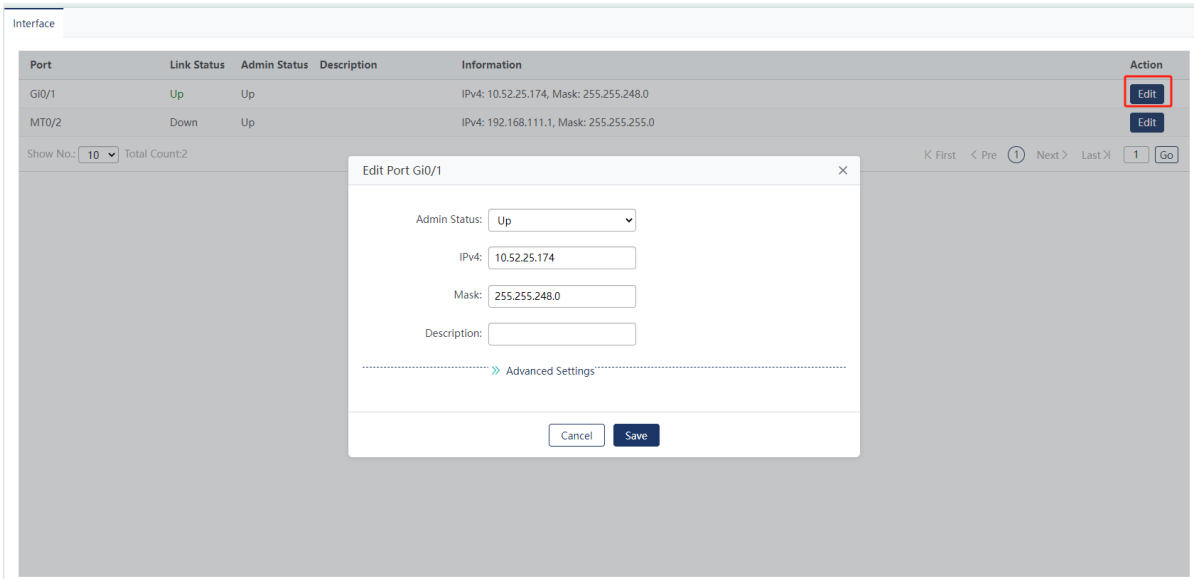
5.3.2 Interfaz

Elija **Config** > **Network** > **Interface** > **Interface**.

En la página **Interfaz**, se muestran los puertos y la información relacionada.



Haga clic **en Editar** en la columna **Acción** para editar información sobre un puerto específico.



Parámetro	Descripción
Estado del administrador	Seleccione el estado de administración del puerto.
IPv4	Introduzca la dirección IPv4 del puerto.
Máscara	Introduzca la máscara de subred IPv4 del puerto.
Descripción	Introduzca la descripción y el alias del puerto.
Puerto de cobre/fibra	Las opciones, incluido el **puerto de cobre** y el **puerto de fibra,** se muestran en función de la capacidad del hardware.
IPv6	Introduzca la dirección IPv6 del puerto.
Velocidad	Configure la velocidad del puerto.

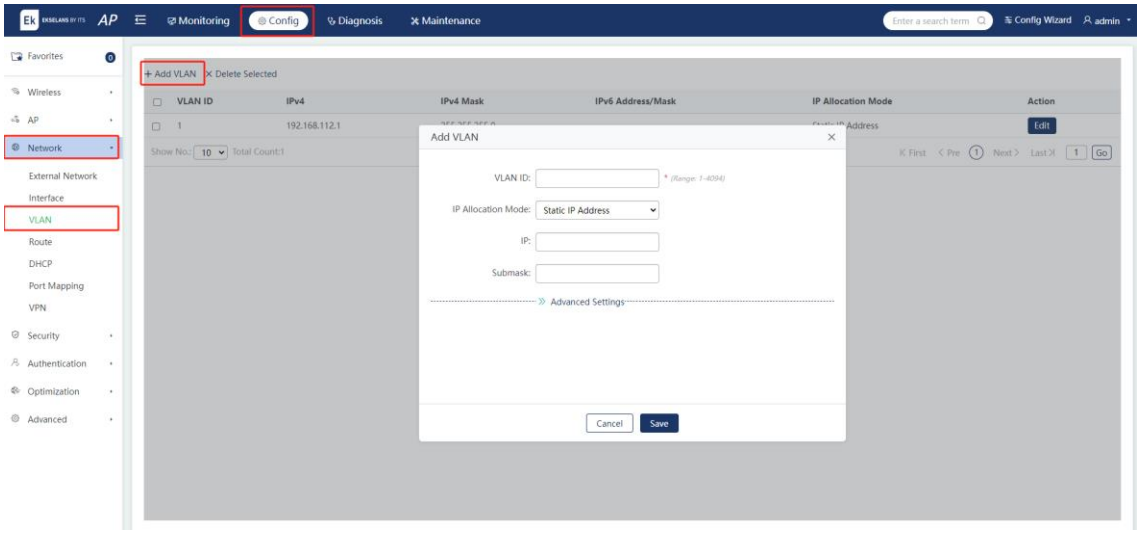
Parámetro	Descripción
Modo de trabajo	Configure el modo de trabajo del puerto, incluida la negociación automática, dúplex y semidúplex.

5.3.3 VLAN

Elija **Config** > **Network > VLAN.**

(1) Adición de una VLAN

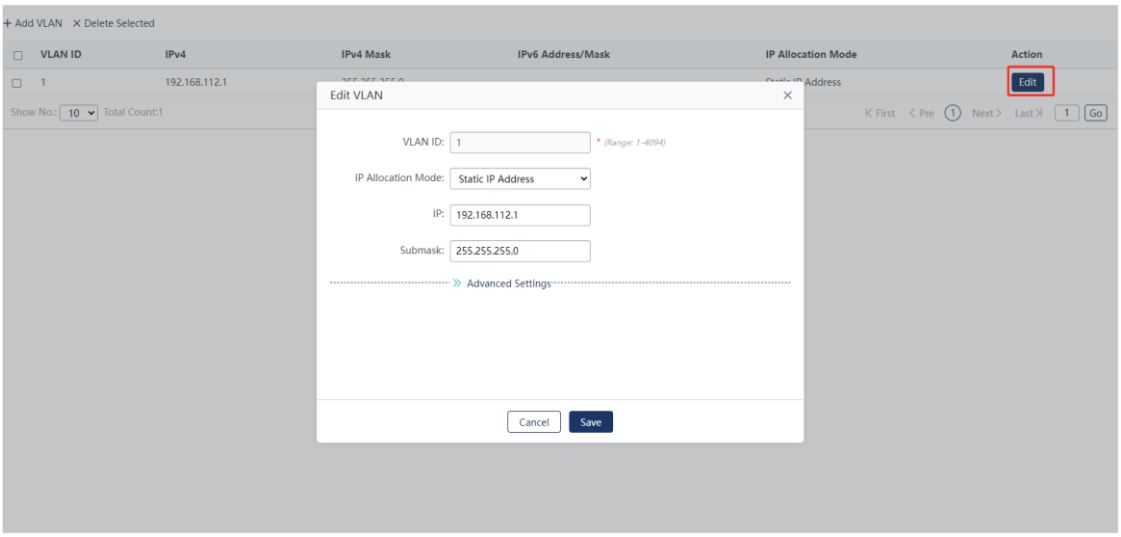
Haga clic en **Agregar VLAN** y edite los campos en la ventana emergente. Haga clic en Guardar y one se mostrará un mensaje que indica que la operación se ha realizado correctamente. La VLAN agregada se muestra en la lista de VLAN.



(2) Edición de una VLAN

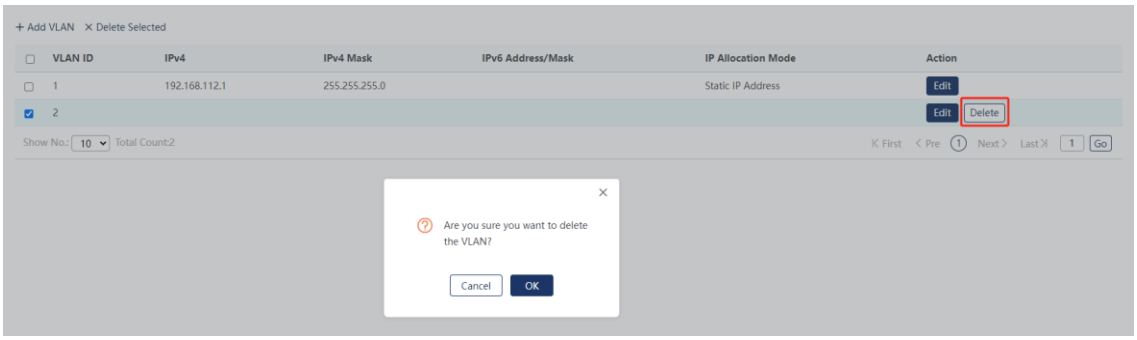
Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra información sobre la VLAN. Edite los campos de la ventana. Haga clic en **Guardar** y se mostrará un mensaje

que indica que la operación se ha realizado correctamente.



(3) Eliminación de una VLAN

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar una VLAN. Si es necesario eliminar varias VLAN, seleccione las VLAN de destino en la lista. Haga clic en **Eliminar seleccionado** y aparecerá una ventana. Haga clic en **Aceptar** para eliminar por lotes las VLAN.

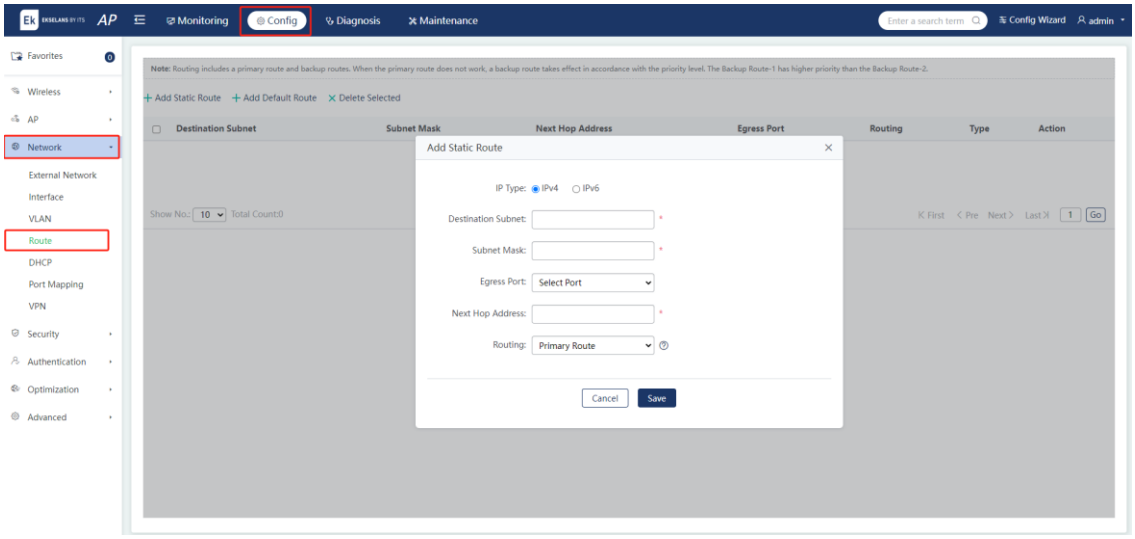


5.3.4 Ruta

Elija **Config** > **Network** > **Route (Ruta de red)**.

(1) Adición de una ruta estática

Haga clic en **Agregar ruta estática**. Edite los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La ruta estática agregada se mostrará en la lista de rutas. El tipo es **Ruta estática**.

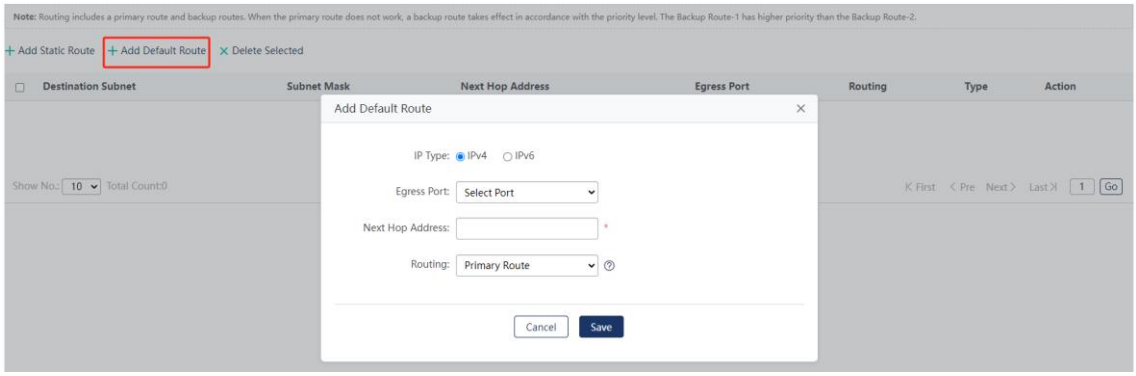


(2) Adición de una ruta predeterminada

Haga clic en **Agregar ruta predeterminada**. Edite los campos en la ventana emergente. Haga clic en **Guardar y** se mostrará un mensaje que indica que la operación se ha realizado correctamente. La ruta predeterminada agregada se mostrará en la lista de rutas. El tipo es **Ruta predeterminada**.

Nota

La selección de rutas implica una ruta principal y rutas de respaldo. Cuando la ruta principal no está disponible, por ejemplo, la interfaz de la ruta principal está inactiva, se adoptará la ruta de respaldo. La selección de la ruta de respaldo también está determinada por los niveles de prioridad. Por ejemplo, la ruta de copia de seguridad 1 tiene una prioridad más alta que la ruta de copia de seguridad 2.



(3) Edición de una ruta

Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra información sobre la ruta. Edite los campos de la ventana. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

(4) Eliminación de una ruta

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar una ruta. Para eliminar varias rutas, seleccione las rutas que desea eliminar en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar las rutas por lotes.

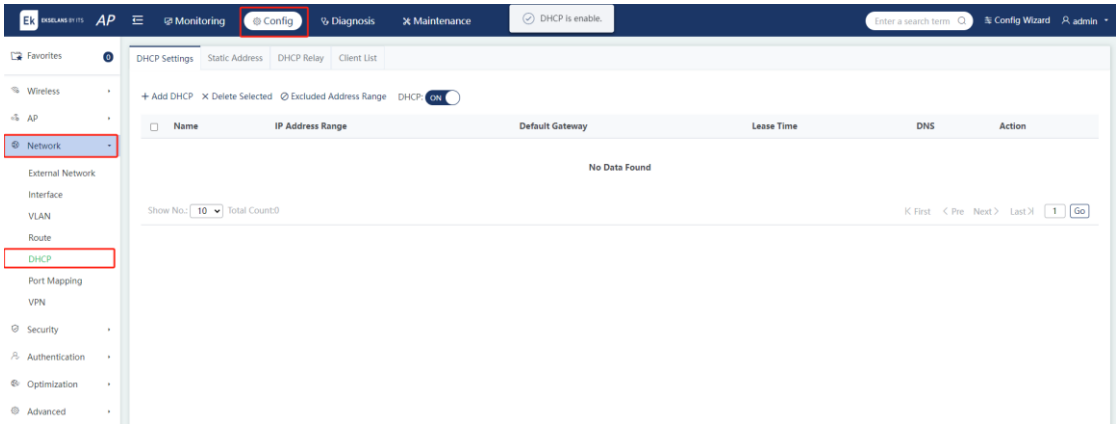
5.3.5 DHCP

1. Configuración de DHCP

Elija Config > **Network > DHCP** > **DHCP Settings**.

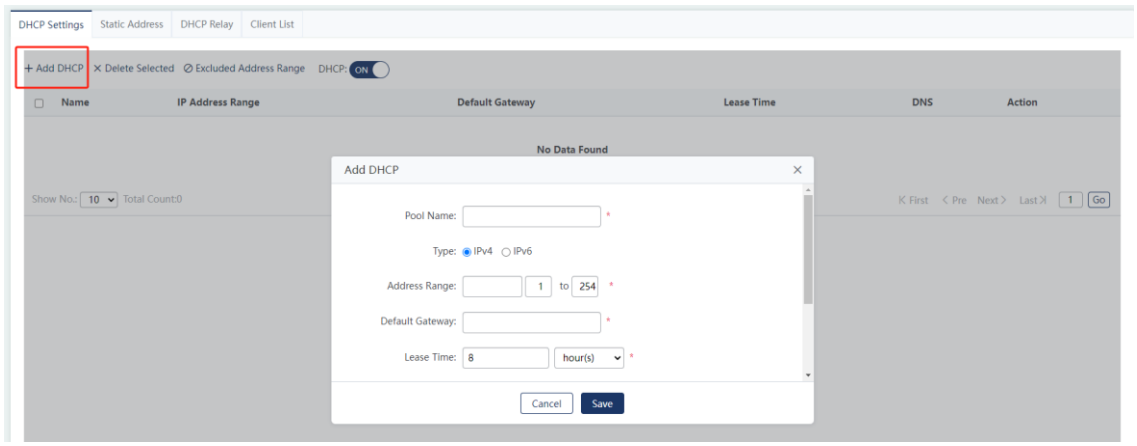
(1) Habilitación del servicio DHCP

Active el switch **DHCP** para habilitar el servicio DHCP.



(2) Adición de un grupo de direcciones DHCP

Haga clic en **Agregar DHCP** y edite los campos en la ventana emergente. Haga clic en **Guardar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente. El grupo de direcciones DHCP se mostrará en la lista.



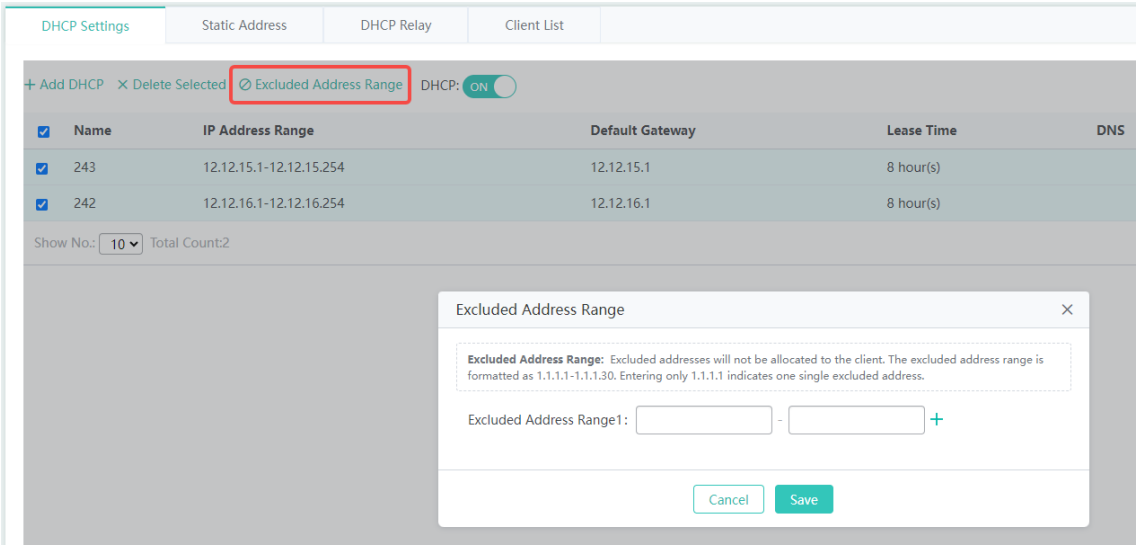
Parámetro	Descripción
Nombre del grupo	Introduzca el nombre del grupo de direcciones DHCP.
Tipo	Las opciones incluyen **IPv4** e **IPv6**.
Rango de direcciones	Configure el rango del grupo de direcciones DHCP.
Puerta de enlace predeterminada	Configure la puerta de enlace predeterminada para el grupo de direcciones DHCP.
Tiempo de arrendamiento	Configure el tiempo de concesión para el grupo de direcciones DHCP, ya sea un intervalo de tiempo limitado o sin límite de tiempo.
Servidor DNS preferido	Configure el servidor DNS preferido para los clientes que utilizan el grupo de direcciones DHCP.
Servidor DNS secundario	Configure el servidor DNS secundario para los clientes que utilizan el grupo de direcciones DHCP.

(3) Eliminación de un grupo de direcciones DHCP

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un grupo de direcciones DHCP. Para eliminar varios grupos de direcciones DHCP, seleccione los grupos de direcciones DHCP de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar por lotes los grupos de direcciones DHCP.

(4) Configuración de un intervalo de direcciones IP excluidas

Haga clic en **Rango de direcciones excluido.** Configure el rango de direcciones IP que no se asignarán a los clientes en la ventana emergente. Puede configurar varios rangos de direcciones excluidas. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente. El rango de direcciones excluido se mostrará en la lista.



(5) Edición de un grupo de direcciones DHCP

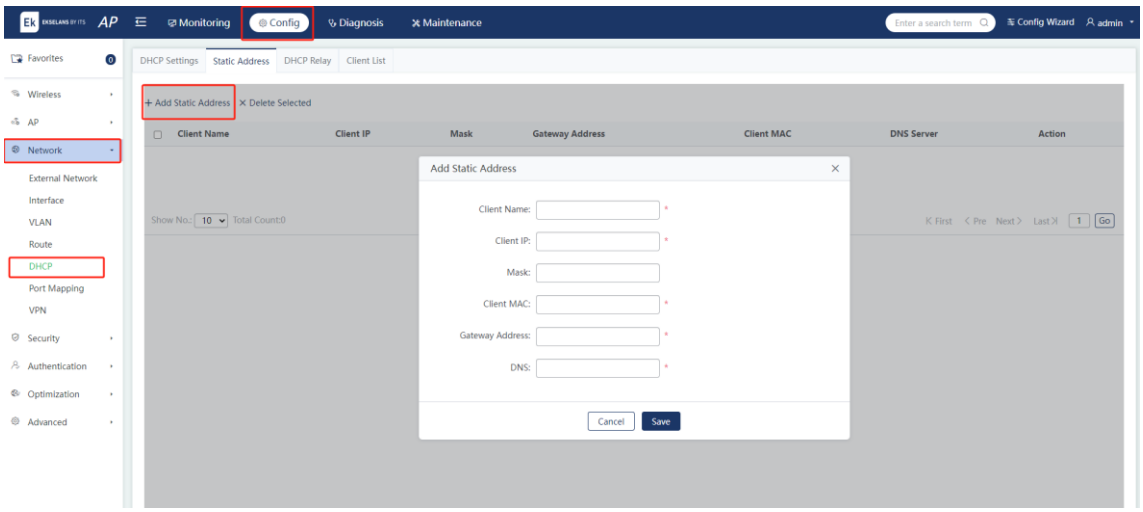
Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra información sobre el grupo de direcciones DHCP. Edite los campos de la ventana. Haga clic en **Guardar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

2. Dirección estática

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

(1) Agregar una dirección IP estática

Haga clic en **Agregar dirección estática** y edite los campos en la ventana emergente. Haga clic en **Guardar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



Parámetro	Descripción
Nombre del cliente	Introduzca el nombre del grupo de direcciones estáticas.
IP del cliente	Configure la dirección IP.
Máscara	Configure la máscara de subred.
MAC del cliente	Introduzca la dirección MAC del cliente.
Dirección de puerta de enlace	Configure la dirección IP de la puerta de enlace de salida. Este campo es obligatorio.
DNS	Configure la dirección del servidor DNS. Este campo es obligatorio.

(2) Eliminación de una dirección IP estática

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar una dirección IP estática. Para eliminar varias direcciones IP estáticas, seleccione las direcciones IP estáticas de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar por lotes las direcciones IP estáticas.

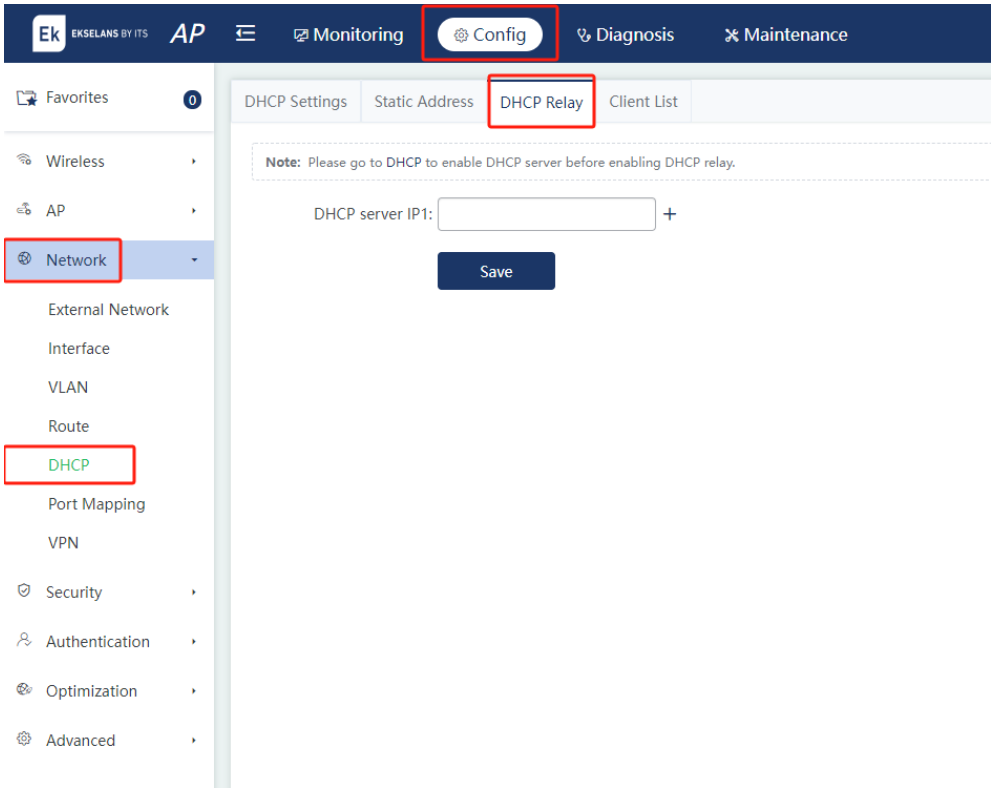
(3) Edición de una dirección IP estática

Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra información sobre la dirección IP estática. Edite los campos de la ventana. Haga clic en **Guardar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

3. Relé DHCP

Elija **Config** > **Network** > **DHCP** > **DHCP Relay**.

Introduzca la dirección IP del relé DHCP y haga clic en **Guardar**.

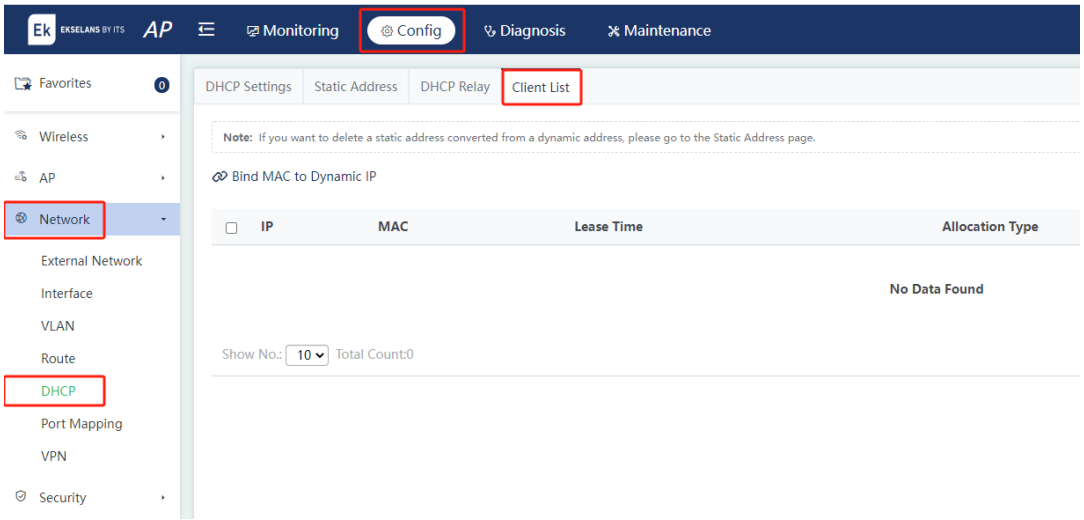


4. Lista de clientes

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

(1) Enlace de una dirección MAC a una dirección IP dinámica

Seleccione una dirección MAC de la lista y haga clic en **Vincular MAC a IP dinámica**. Haga clic en **Aceptar** en la ventana emergente para vincular la dirección MAC con la dirección IP dinámica.

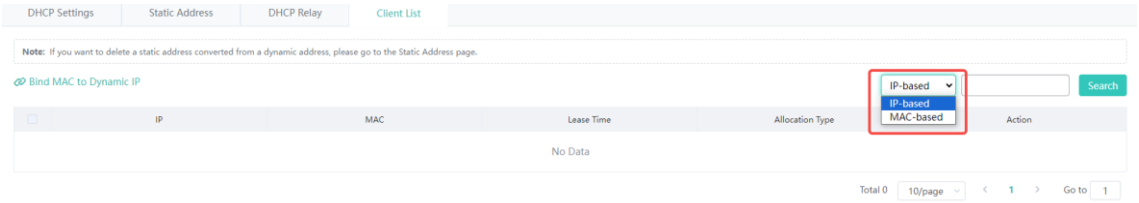


(2) Desvincular la dirección MAC de la dirección IP dinámica

Haga clic **en Eliminar** en la columna **Acción** y aparecerá una ventana. Haga clic en **Aceptar** para desvincular la dirección MAC.

(3) Búsqueda de clientes por dirección IP o dirección MAC

Introduzca la dirección IP o la dirección MAC en el cuadro de búsqueda. Haga clic **en Buscar** y el resultado se mostrará en la lista.



5.3.6 Mapeo de puertos

Elija **Config** > **Network > Port Mapping**.

Nota

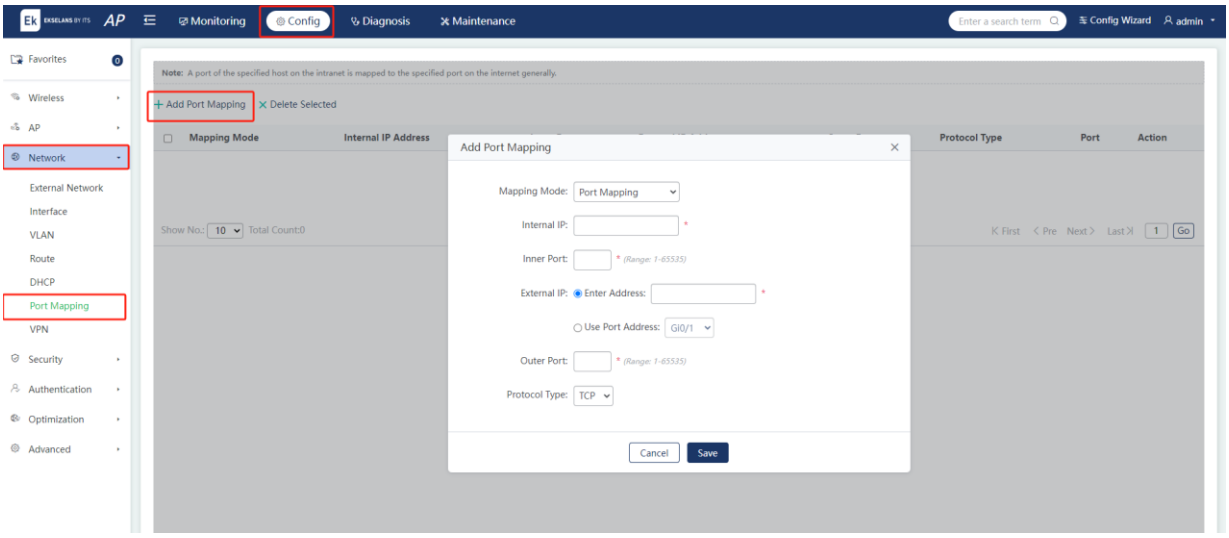
Es posible que algunos AP no admitan esta función. Prevalecerá el menú real.

La función de asignación de puertos asigna un puerto especificado de un host especificado en la intranet a un puerto especificado en la extranet.

Los modos de mapeo incluyen **mapeo de puertos** y **mapeo de host DMZ**.

1. Adición de una regla de asignación de puertos

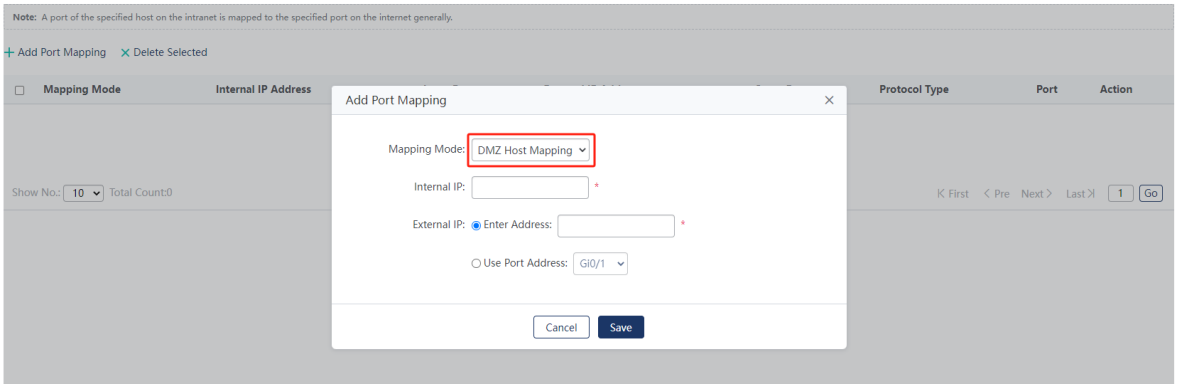
Haga clic en **Agregar asignación de puertos**. Establezca el modo de asignación en **Asignación de puertos** y edite los campos en la ventana emergente. Haga clic en **Guardar**.



Parámetro	Descripción
Modo de mapeo	Los modos de mapeo incluyen **mapeo de puertos** y **mapeo de host DMZ**.
IP interna	Introduzca la dirección IP interna que se asignará a la extranet, que suele ser la dirección IP del servidor.
Puerto interior	Introduzca el puerto que se asignará a la extranet.
IP externa	Introduzca la dirección IP de la red de área extensa (WAN). Si se selecciona **Usar dirección de puerto**, se asignan todas las direcciones IP del puerto WAN.
Puerto exterior	Introduzca el número de puerto WAN. El rango de valores es de 1 a 65535.
Tipo de protocolo	Seleccione TCP o UDP según sea necesario.

2. Adición de una regla de asignación de host DMZ

Haga clic en **Agregar asignación de puertos**. Establezca el modo de asignación en **DMZ Host Mapping**. Introduzca la dirección IP interna del servidor y la dirección IP externa o el puerto donde se aplica la regla. A continuación, haga clic en **Guardar**. Cuando un paquete de datos entrante no llega a ninguna regla de asignación de puertos, el paquete se redirige al servidor interno de acuerdo con la regla de zona desmilitarizada (DMZ). Es decir, todos los paquetes de datos enviados activamente desde Internet al dispositivo se reenvían al host DMZ especificado.



3. Edición de una regla de asignación de puertos

Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra información sobre la regla de asignación de puertos. Edite los campos de la ventana. Haga clic en **Guardar**.

4. Eliminación de una regla de asignación de puertos

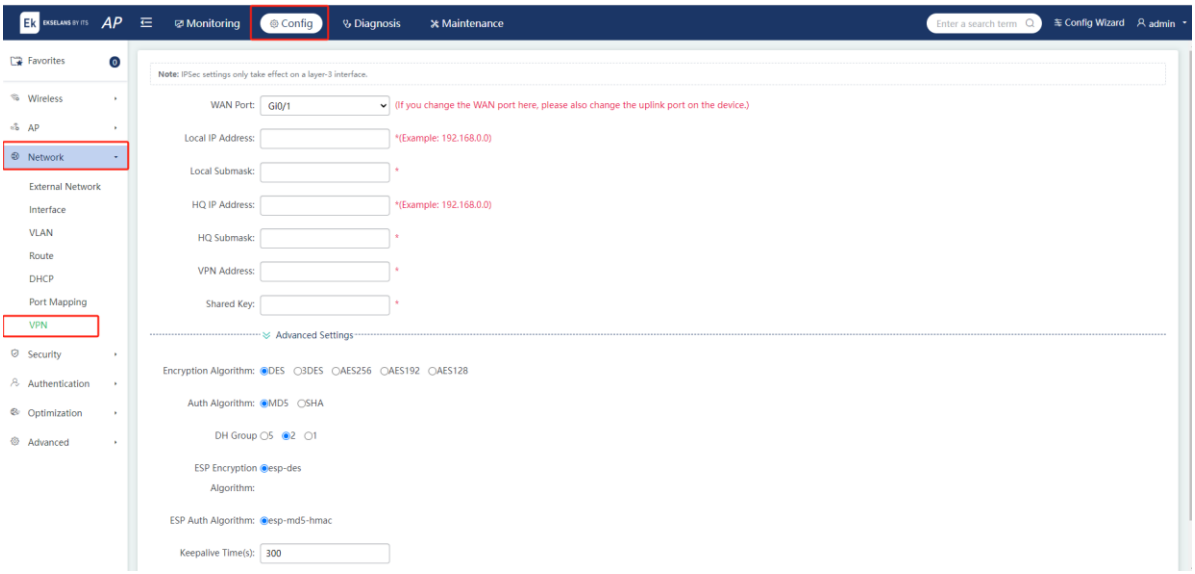
Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar una regla de asignación de puertos. Para eliminar varias reglas de asignación de puertos,

seleccione las reglas de asignación de puertos de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar por lotes las reglas de asignación de puertos.

5.3.7 VPN

Elija **Config** > **Network > VPN.**

Puede configurar VPN para un solo puerto WAN. Introduzca la dirección IP local, la máscara de subred local, la dirección IP de la sede central (HQ), la máscara de subred HQ, la dirección VPN y la clave compartida. Haga clic en **Configuración avanzada** para configurar los algoritmos. Se recomienda utilizar la configuración predeterminada.



5.4 Seguridad

5.4.1 Contención

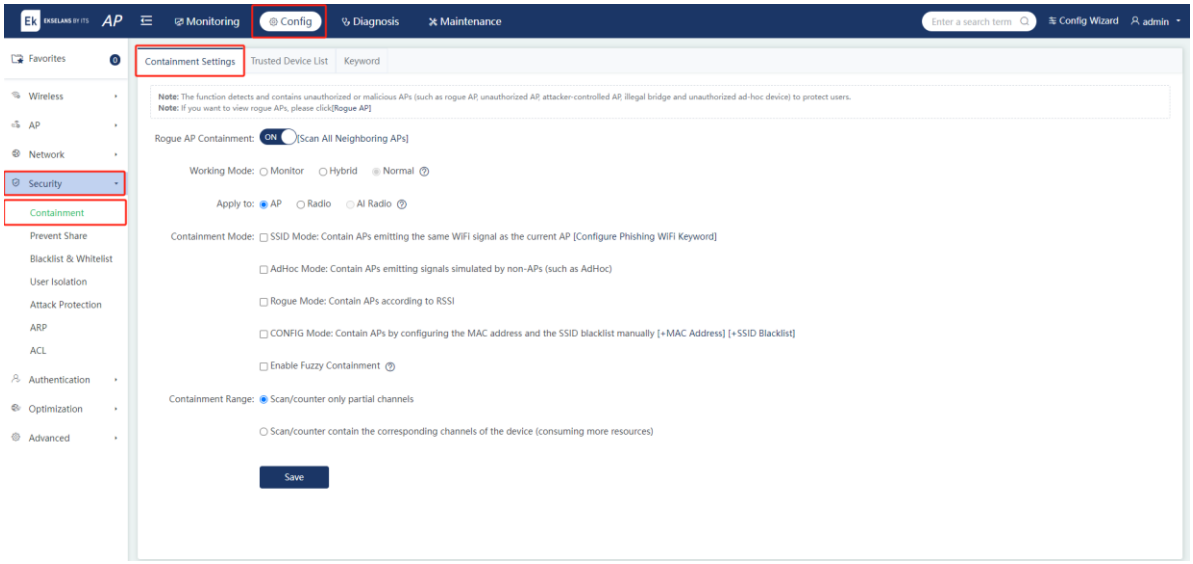
Elija **Config** > **Security** > **Containment (Contención**).

Es posible que existan puntos de acceso no autorizados en una red inalámbrica. Pueden tener vulnerabilidades de seguridad o estar controlados por atacantes, lo que representa una gran amenaza para la seguridad de la red. Habilite la función de contención en el AP para detectar de manera proactiva AP no autorizados o maliciosos en la red (como AP no autorizados, AP no configurados, AP controlados por atacantes, puentes no autorizados o dispositivos Ad-hoc no autorizados) e implemente la contención en ellos para evitar que los STA inalámbricos se asocien con AP no autorizados.

1. Configuración de contención

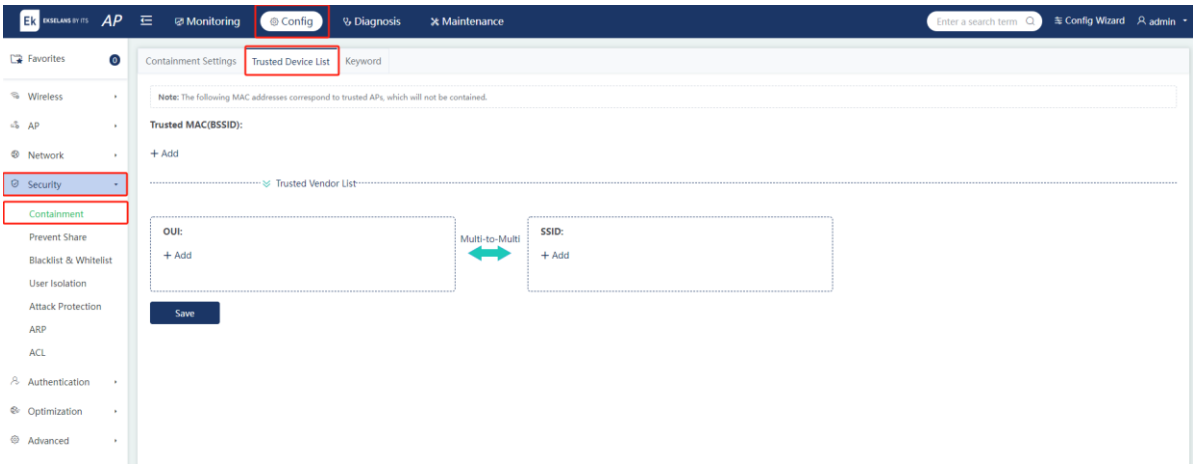
Cuando **Rogue AP Containment** está habilitado, debe configurar el modo de trabajo en **Monitor** o **Híbrido**.

El modo **híbrido** se aplica solo al AP, mientras que el modo monitor se puede aplicar al AP o a las radios seleccionadas. Haga clic en **Configurar palabra clave de phishing WiFi** para acceder a la página **Palabra clave** y configurar la palabra clave.



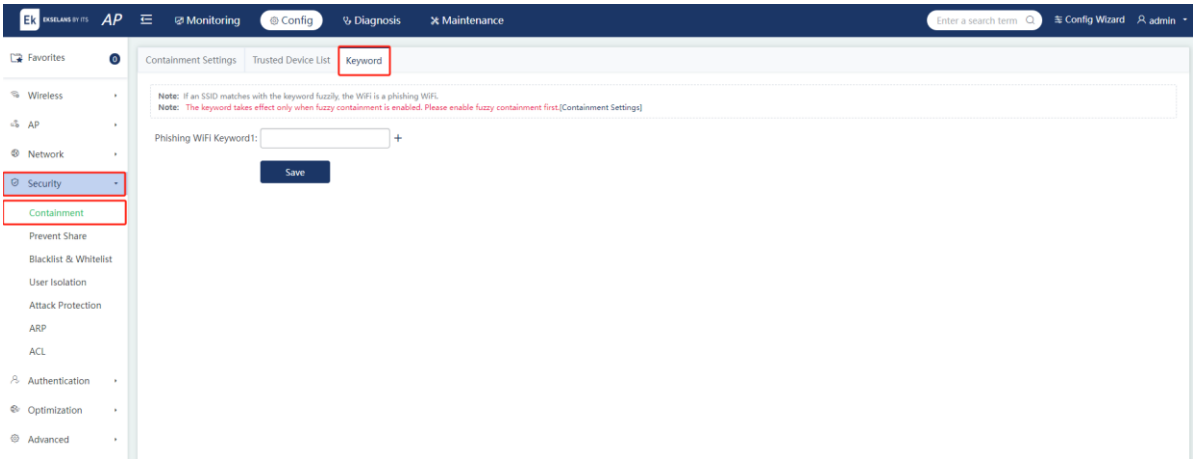
2. Lista de dispositivos de confianza

Cuando se habilita **la contención de AP no autorizados**, se contendrán los AP no autorizados. Sin embargo, algunos dispositivos son dispositivos de confianza. Puede configurar la dirección MAC de un dispositivo de confianza o la dirección MAC de un fabricante de confianza. Si un AP está configurado como un dispositivo de confianza, no se contendrá.



3. Palabra clave Wi-Fi de phishing

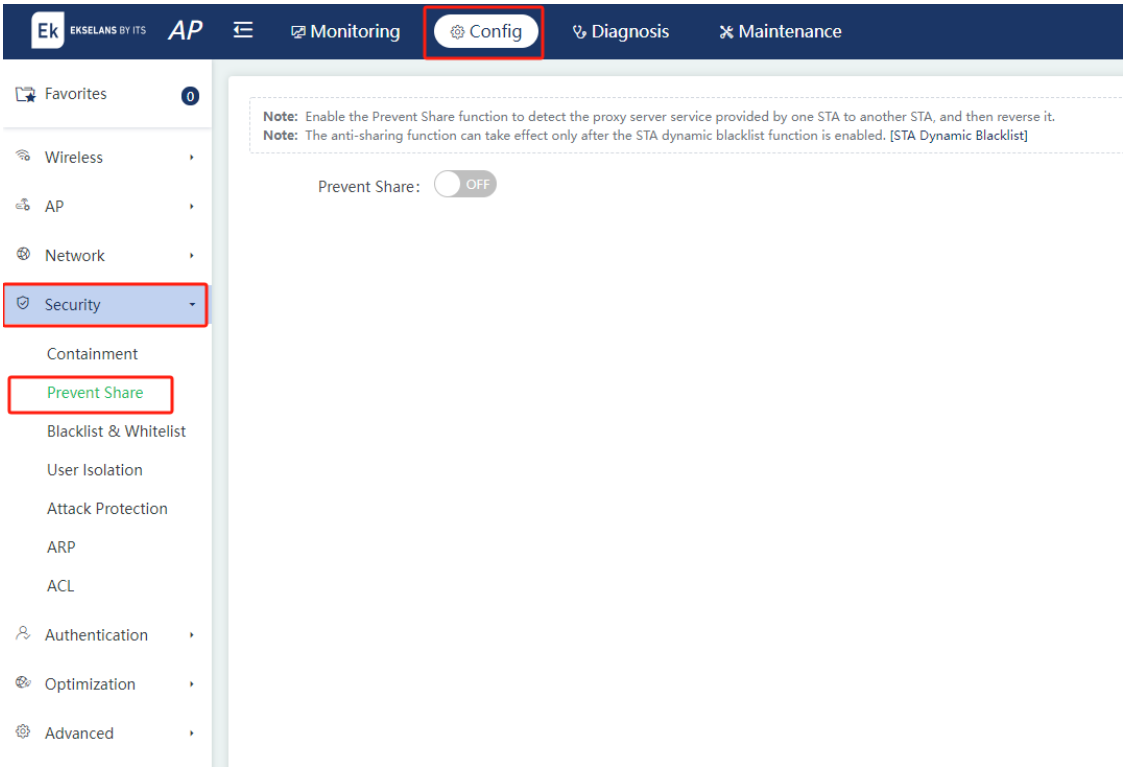
Las palabras clave de phishing de Wi-Fi se obtienen escaneando los SSID de la red. Haga coincidir los SSID escaneados con las palabras clave configuradas. Si un SSID coincide con la palabra clave de forma difusa, el Wi-Fi se considera un Wi-Fi de phishing.



5.4.2 Prevención de uso compartido

Elija **Config** > **Security** > **Prevent Share**.

Cuando **se habilita Evitar uso compartido, el sistema puede detectar si un STA proporciona el servicio de proxy a otro y agrega el STA que proporciona el servicio de proxy a la lista de contención.**



5.4.3 Lista negra y lista blanca

Elija **Configuración** > **seguridad** > **Lista negra y lista blanca**.

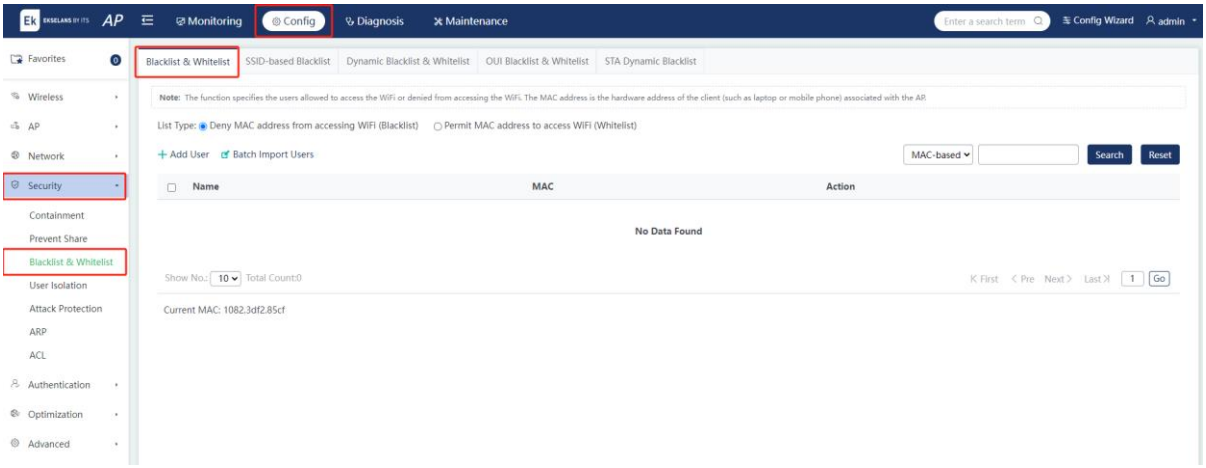
Para mejorar la seguridad inalámbrica, puede configurar una lista negra (a los usuarios de la lista negra se le niega el acceso a la red Wi-Fi) y una lista blanca (solo los usuarios de la lista blanca pueden acceder a la red Wi-Fi) para controlar el acceso de los usuarios inalámbricos. Un AP gordo admite la lista negra y la lista blanca globales, la lista negra y la lista blanca basadas en SSID, la lista negra y la lista blanca dinámicas, la lista negra y la lista blanca basadas en el identificador único de la organización (OUI) y la lista negra dinámica basada en STA.

Nota

- El número de usuarios a los que se les niega o se les permite acceder a la red Wi-Fi varía según los dispositivos. Prevalecerá el valor mostrado en la página.
- Las configuraciones de la lista negra y la lista blanca son las mismas. A continuación, se toma como ejemplo la configuración de la lista negra.

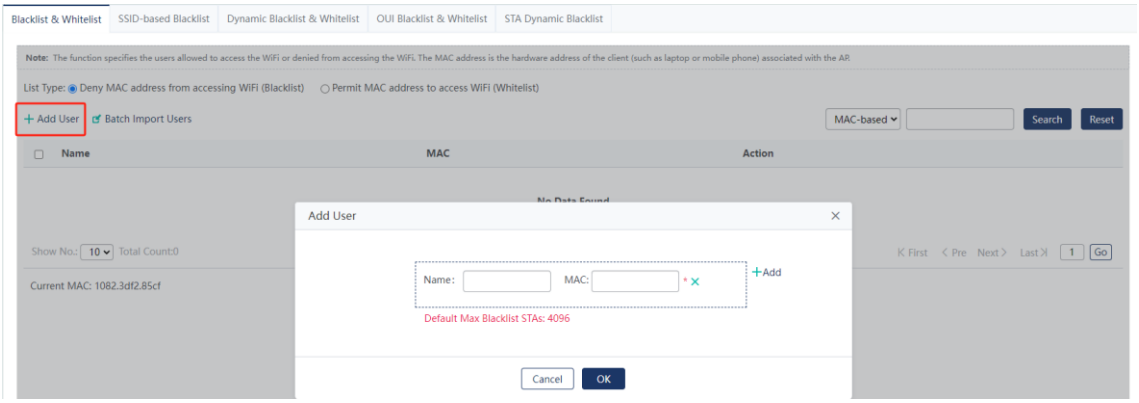
1. Configuración de la lista negra global o la lista blanca

A los usuarios inalámbricos de la lista negra global se le niega el acceso a cualquier red Wi-Fi del AP. Sin embargo, solo los usuarios inalámbricos de la lista blanca global pueden acceder a cualquier red Wi-Fi del AP.



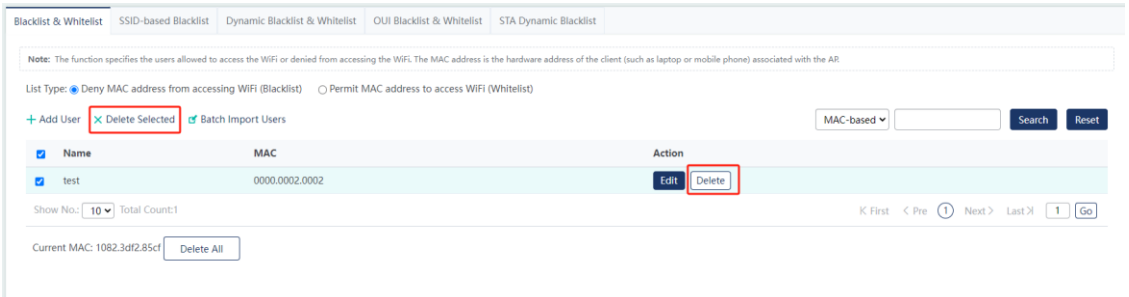
(1) Adición de un usuario

Haga clic en **Agregar usuario** para agregar la dirección MAC de un usuario. Se pueden agregar varias direcciones.



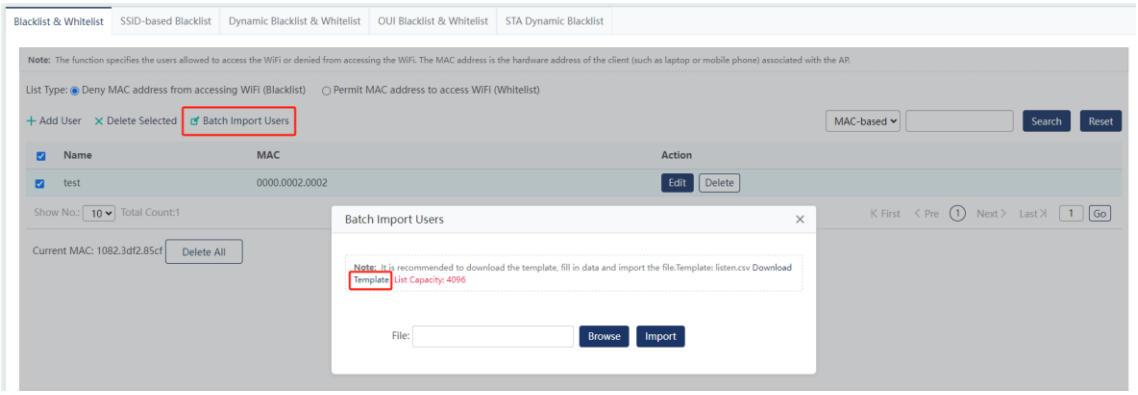
(2) Eliminación de un usuario

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un usuario. Para eliminar varios usuarios, seleccione los usuarios de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar por lotes a los usuarios.



(3) Usuarios de importación por lotes

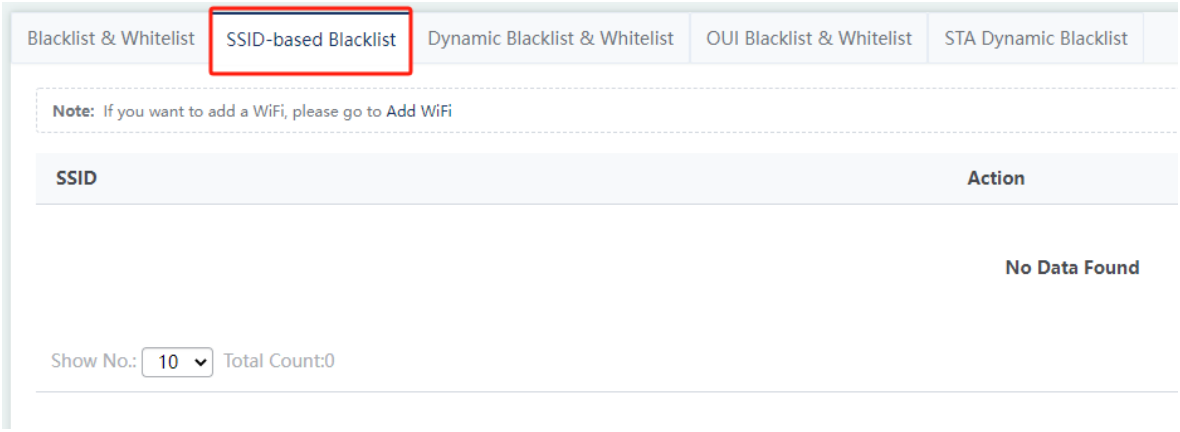
Haga clic en **Importar usuarios por lotes**. Descarga y rellena la plantilla. Importe el archivo de plantilla.



2. Configuración de la lista negra o la lista blanca basada en SSID

A los usuarios inalámbricos de la lista negra basada en SSID se le niega el acceso a una red Wi-Fi especificada. Sin embargo, solo los usuarios inalámbricos de la lista blanca basada en SSID pueden acceder a una red Wi-Fi específica.

Haga clic en **Lista negra/Lista blanca** de un SSID especificado para acceder a la página de configuración. Seleccione un tipo de lista.



(1) Adición de un usuario

Haga clic en **Agregar usuario** para agregar la dirección MAC de un usuario. Haga clic en **Aceptar**.

(2) Eliminación de un usuario

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un usuario. Para eliminar varios usuarios, seleccione los usuarios de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar por lotes a los usuarios.

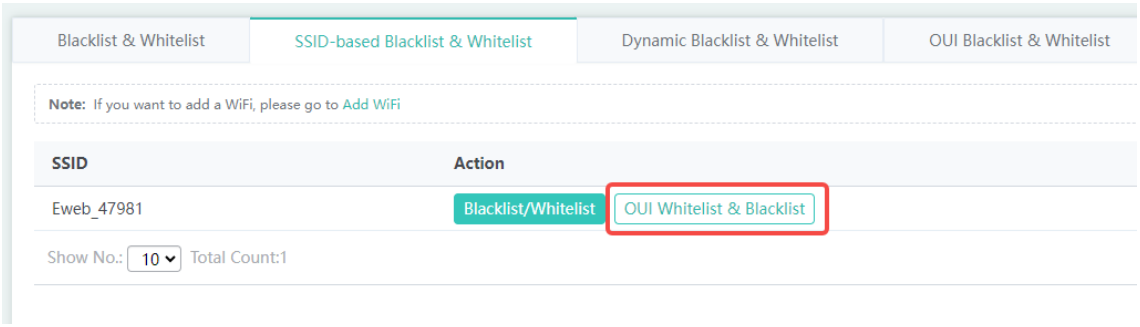
(3) Usuarios de importación por lotes

Haga clic en **Importar usuarios por lotes**. Descarga la plantilla. Rellena la plantilla y guárdala. Haga clic en **Examinar**. Seleccione el archivo de plantilla. Haga clic en **Importar**.

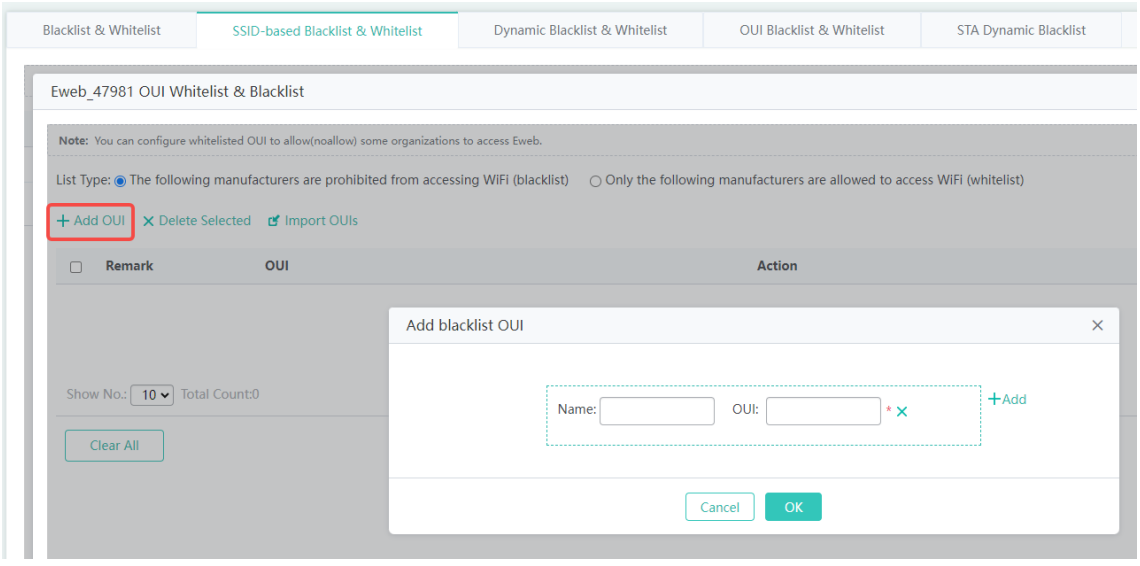
(4) Configuración de una OUI

Una OUI son los primeros 8 bits de la dirección MAC de un dispositivo. Si los dispositivos que se van a añadir a la lista negra o a la lista blanca pertenecen al mismo fabricante, añada su OUI directamente a la lista, eliminando la necesidad de añadir la dirección MAC de cada dispositivo uno por uno.

Haga clic en **Lista blanca y lista negra** de OUI para ingresar a la página de configuración.



Haga clic en **Agregar OUI.** Introduzca el nombre y la unidad organizativa del fabricante. Haga clic en **Aceptar**.

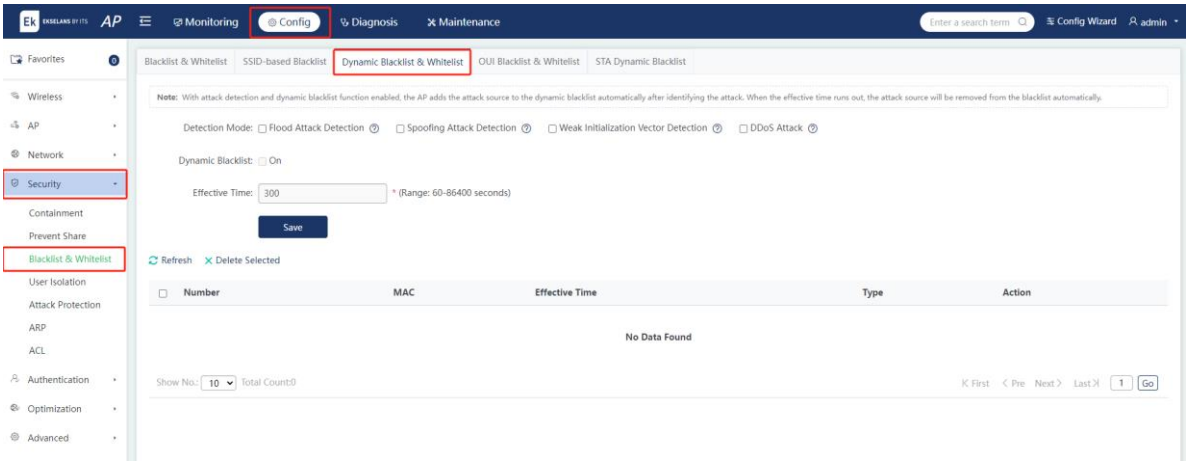


3. Configuración de la lista negra dinámica o la lista blanca

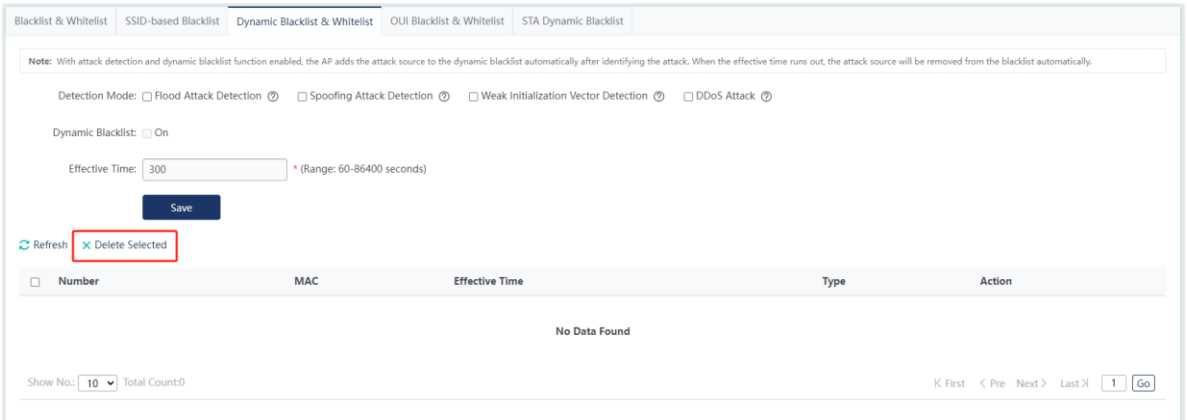
Lista negra dinámica: Agregue fuentes de ataque malicioso a la lista negra dinámica para evitar su acceso. Una vez configurado un modo de detección y habilitada la lista negra dinámica, el dispositivo agregará automáticamente la fuente de ataque a la lista negra dinámica cuando se

detecte un ataque. Una vez que expire el tiempo efectivo, la fuente de ataque se eliminará automáticamente de la lista negra.

Configuración de una lista negra dinámica: seleccione un modo de detección, habilite la lista negra dinámica y configure la hora efectiva. Haga clic en **Guardar**.



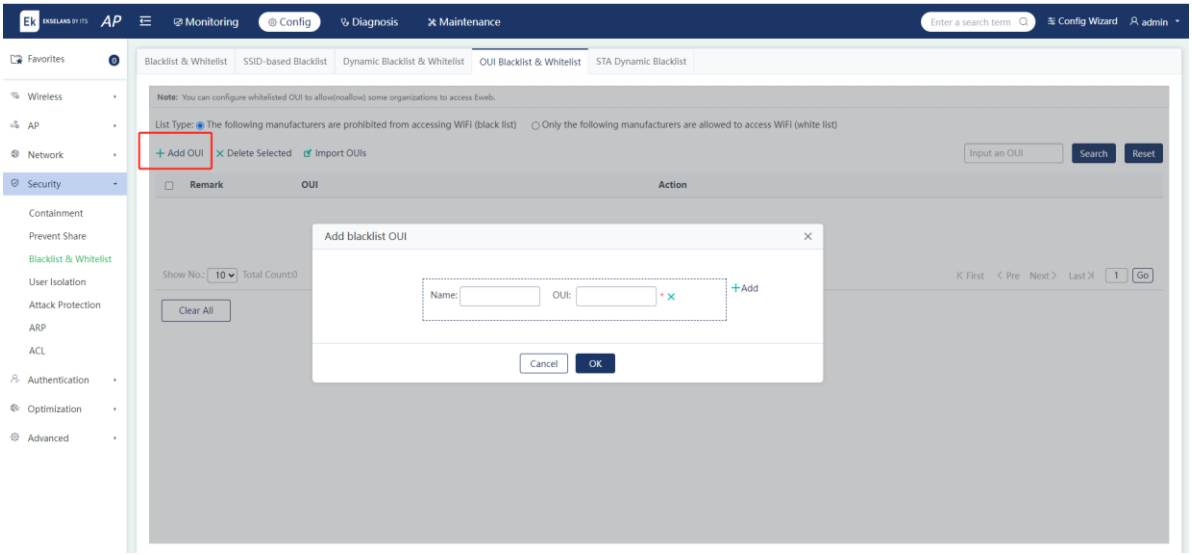
Eliminar una lista negra dinámica: haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar una lista negra dinámica. Para eliminar varias listas negras dinámicas, seleccione las listas negras dinámicas de destino. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar por lotes las listas negras dinámicas.



4. Configuración de la lista negra o lista blanca de OUI para el AP

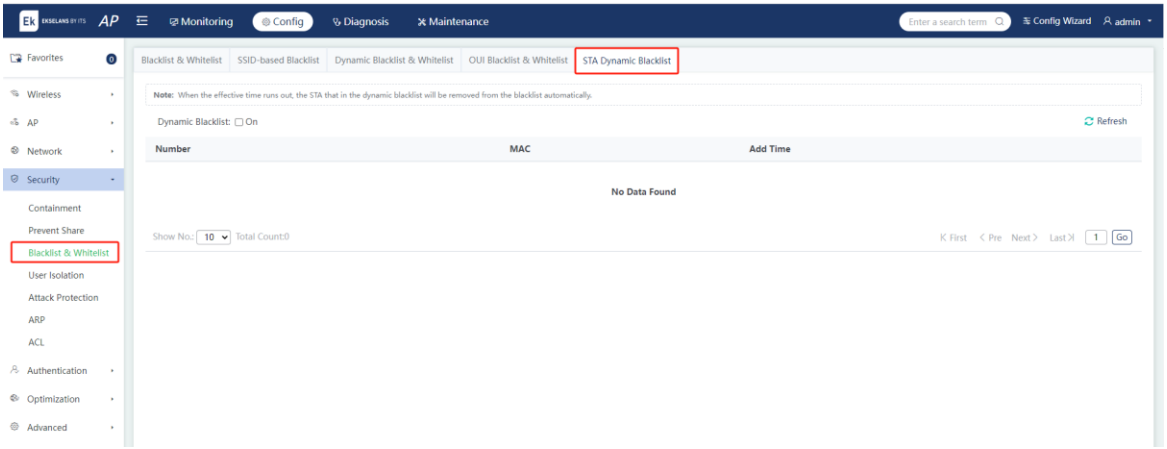
A los fabricantes de la lista negra de OUI se les niega el acceso a cualquier red Wi-Fi del AP, mientras que solo los fabricantes de la lista blanca de OUI pueden acceder a cualquier red Wi-Fi del AP.

Configuración de la información del fabricante: haga clic en **Agregar OUI.** Introduzca el nombre y la unidad organizativa del fabricante. Haga clic en **Aceptar**.



5. Configuración de la lista negra dinámica de STA

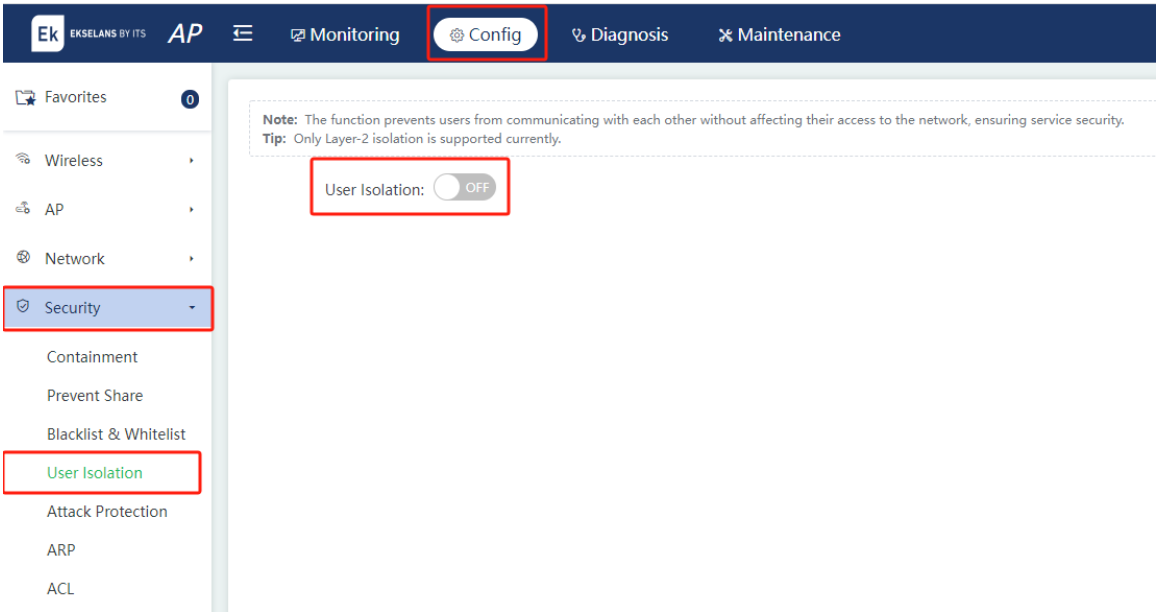
Agregue STA de fuentes de ataque maliciosas a la lista negra dinámica de STA para evitar que accedan a la red.



5.4.4 Aislamiento de usuarios

Elija **Config** > **Security** > **User Isolation**.

Para garantizar la seguridad de la red y la confidencialidad de la información, habilite **el aislamiento de usuario** para que los usuarios de la intranet no puedan comunicarse entre sí. Algunos usuarios especiales (usuarios que pueden acceder entre sí) se pueden identificar mediante el nombre de usuario y la dirección MAC. Haga clic en Agregar para agregar las direcciones MAC de los usuarios a la MAC incluida en la **lista blanca** para el acceso mutuo.

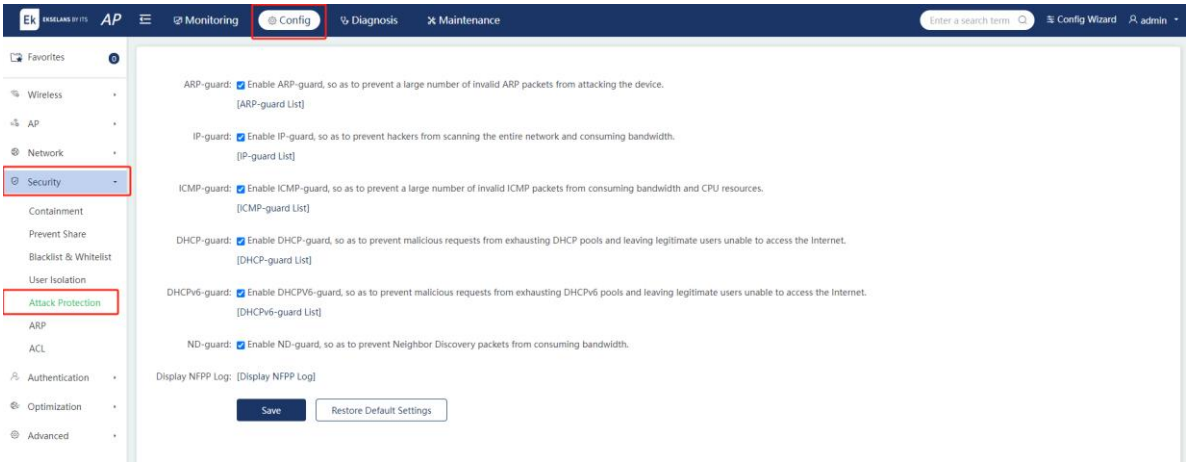


5.4.5 Prevención de ataques

Elija **Config** > **Security** > **Attack Protection**.

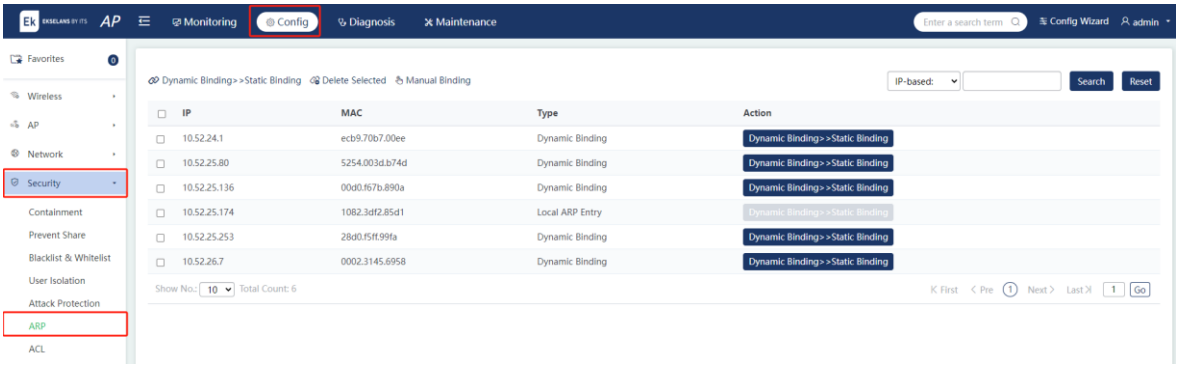
Los ataques maliciosos suelen producirse en un entorno de red. Estos ataques sobrecargan el dispositivo, lo que resulta en un uso elevado de la CPU y un error de funcionamiento del dispositivo.

Seleccione los tipos de prevención de ataques y haga clic en **Guardar**. Haga clic en el texto entre corchetes ([]) para mostrar la lista.



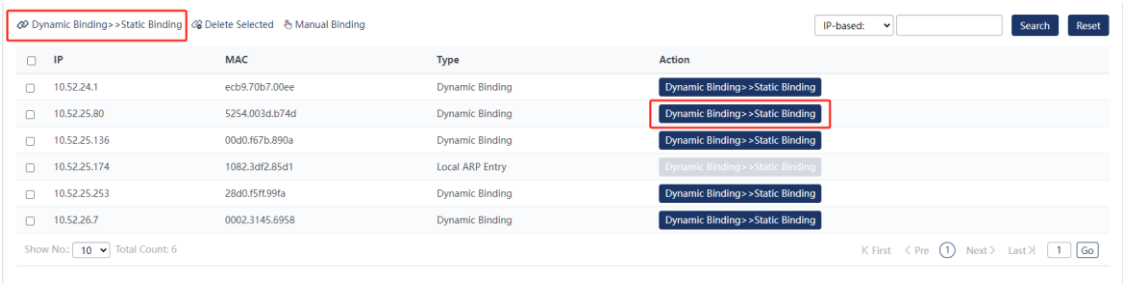
5.4.6 Enlace de entrada ARP

Elija **Config** > **Security** > **ARP**.



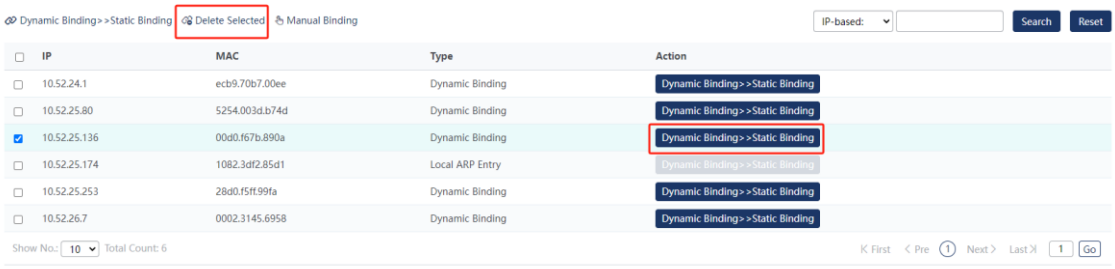
(1) Cambiar un enlace dinámico a un enlace estático

Seleccione una entrada en la lista ARP. Haga clic **en Enlace dinámico >> Enlace estático** en la columna **Acción** para cambiar el enlace dinámico por el enlace estático. También puede seleccionar más entradas en la lista ARP y hacer clic en **Enlace dinámico >> Enlace estático** junto a **Eliminar seleccionados** para cambiar por lotes los enlaces dinámicos a los enlaces estáticos.



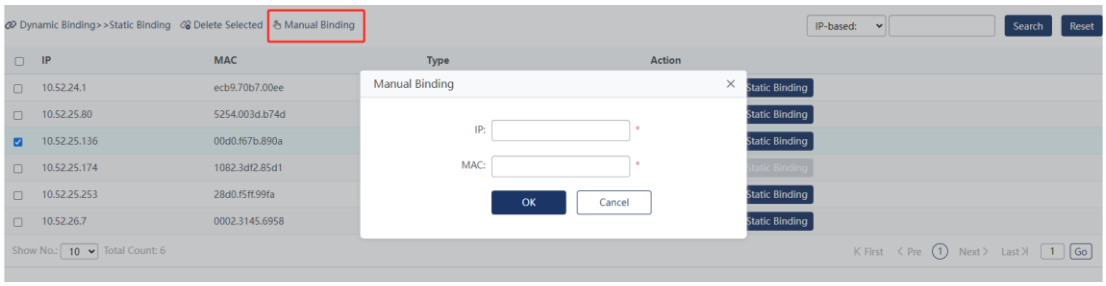
(2) Eliminación de un enlace estático

Seleccione una entrada en la lista ARP. Haga clic **en Enlace estático >> Enlace dinámico** en la columna **Acción** para cambiar el enlace estático por el enlace dinámico. Para eliminar varios enlaces estáticos, seleccione las direcciones IP de destino en la lista ARP. Haga clic en **Eliminar seleccionado** para eliminar por lotes los enlaces estáticos.



(3) Encuadernación manual

Haga clic en **Enlace manual**. Introduzca las direcciones IP y MAC. Haga clic en **Aceptar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La nueva entrada se muestra en la lista ARP.



5.4.7 ACL

Elija **Config** > **Security** > **ACL**.

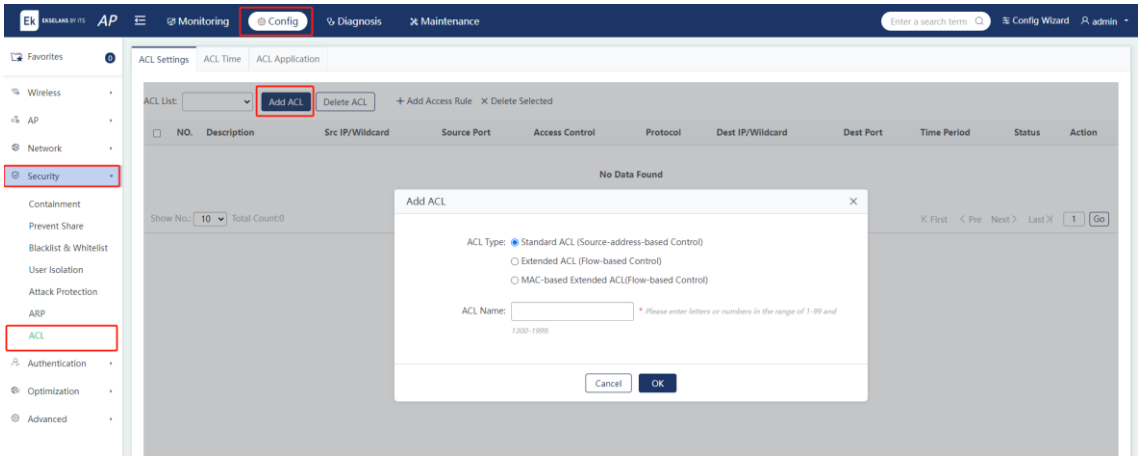
Al recibir un paquete, una interfaz de dispositivo en la que se configura una ACL de entrada comprueba si el paquete coincide con una entrada de control de acceso (ACE) en la ACL de entrada. Al enviar un paquete, una interfaz de dispositivo en la que se configura una ACL de salida comprueba si el paquete coincide con una ACE en la ACL de salida.

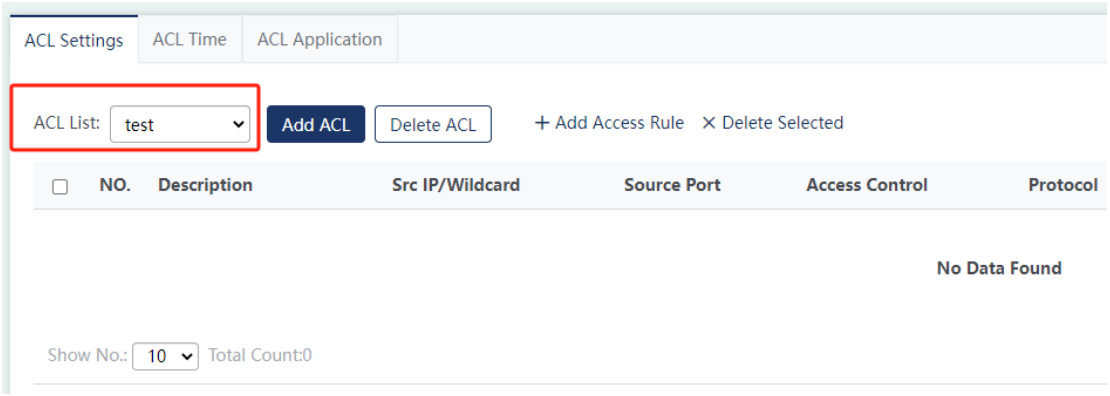
Cuando se configuran diferentes ACE, se pueden aplicar varias ACE al mismo tiempo, o solo se aplican algunas ACE. Los paquetes se procesan de acuerdo con la primera ACE coincidente (permitir o denegar).

1. Configuración de ACL

(1) Adición de una ACL

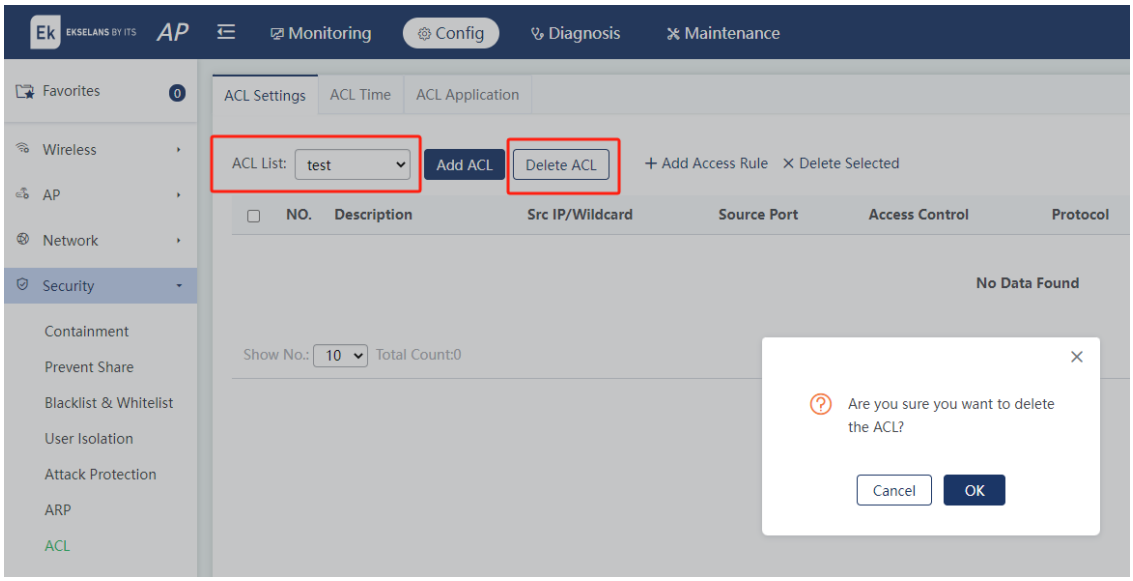
Haga clic en **Agregar ACL**. Introduzca los campos en la ventana emergente. Haga clic en **Aceptar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La nueva entrada se muestra en la lista desplegable de ACL en la esquina superior izquierda.





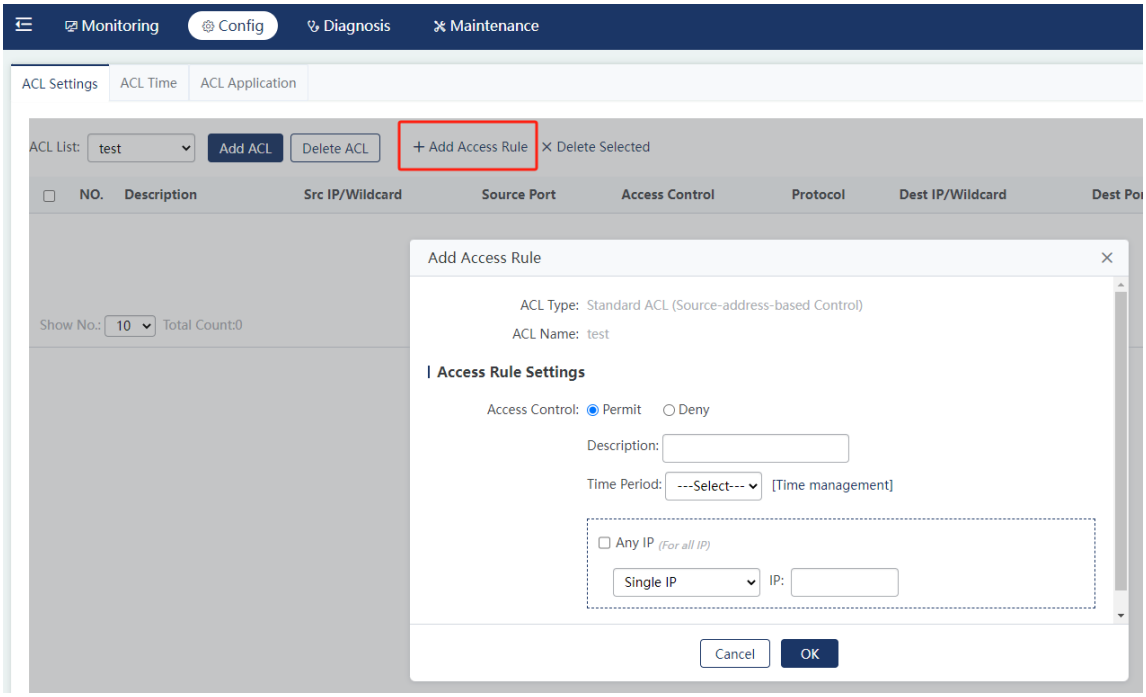
(2) Eliminación de una ACL

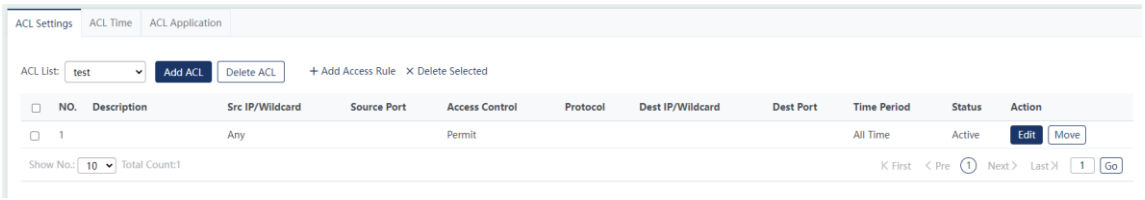
Seleccione la ACL que se eliminará de la lista desplegable de ACL. Haga clic en **Eliminar ACL**. Haga clic en **Aceptar** en la ventana emergente para eliminar la ACL.



(3) Adición de un ACE

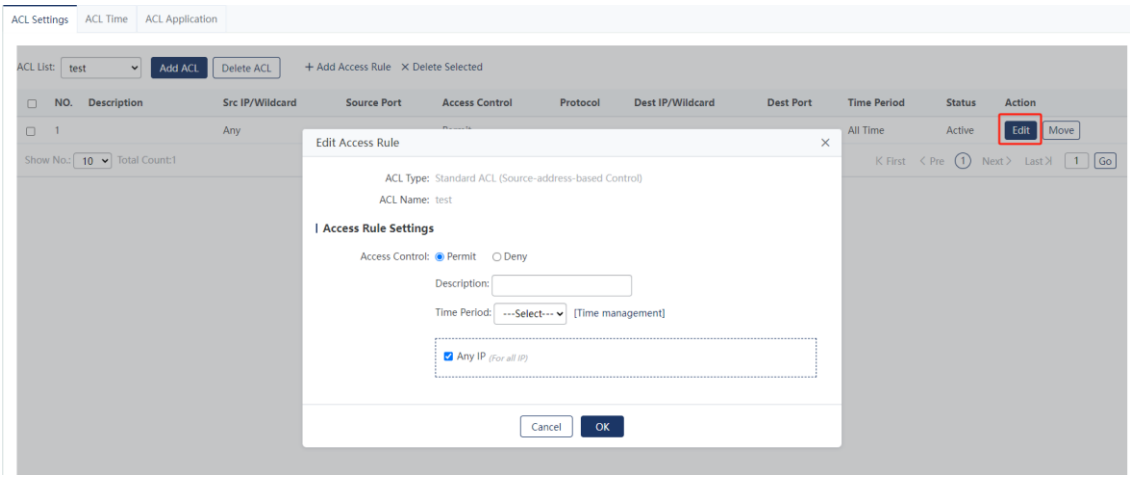
Seleccione una ACL a la que se debe agregar una ACE de la lista desplegable de ACL. Haga clic en **Agregar regla de acceso**. Introduzca los campos en la ventana emergente. Haga clic en **Aceptar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La nueva entrada se muestra en la lista de ACL.





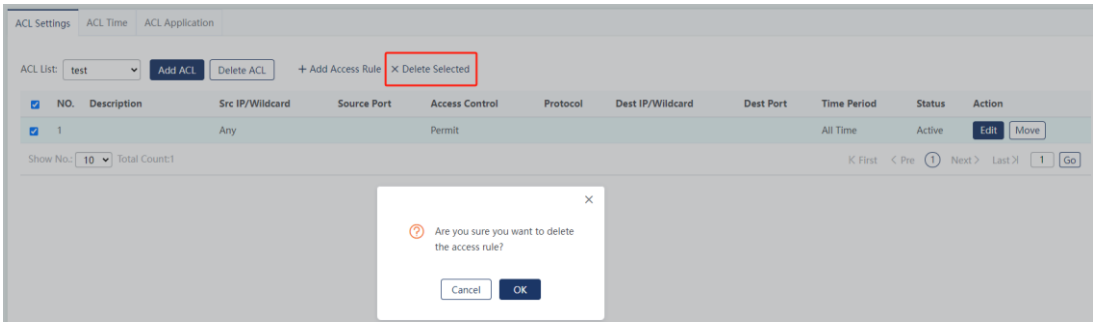
(4) Edición de un ACE

Haga clic **en Editar** en la columna **Acción** de una ACE en la lista ACL. Edite los campos en la ventana emergente. Haga clic en **Aceptar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



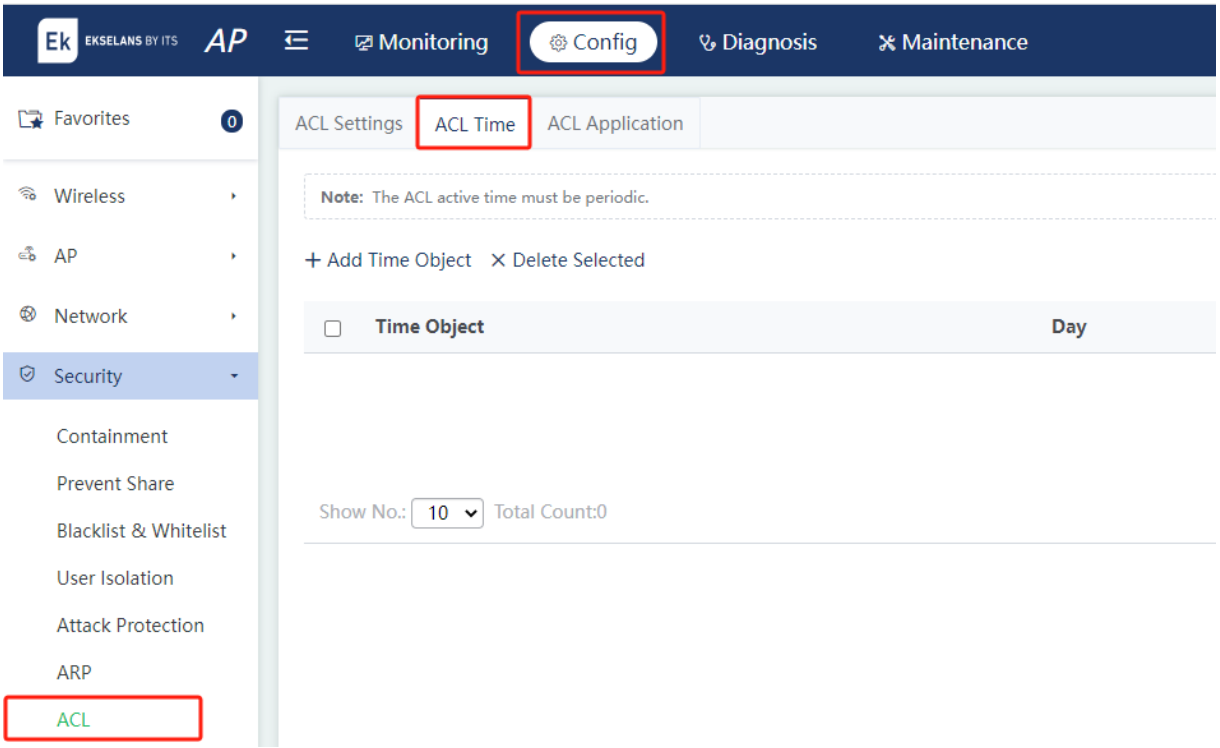
(5) Eliminación de una ACE

Seleccione una o más entradas en la lista de ACL. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para eliminar las ACE.



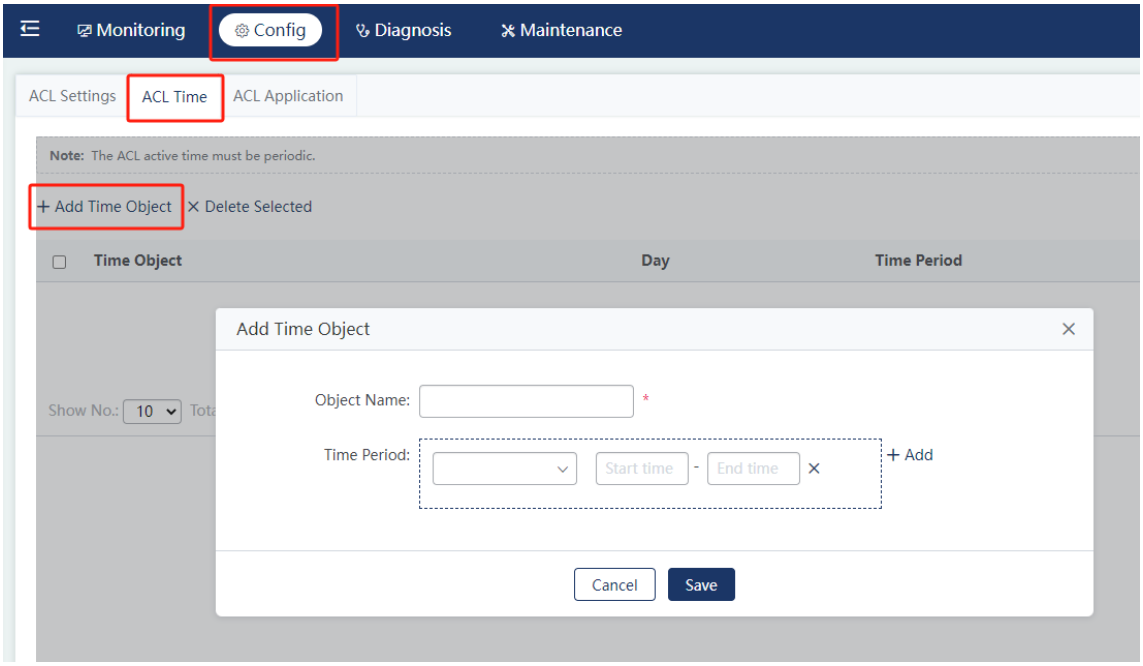
2. Tiempo de ACL

Una ACL se puede configurar para que surta efecto en función del tiempo, por ejemplo, en algunos períodos de tiempo de una semana. Para cumplir con este requisito, debe configurar un objeto de tiempo.



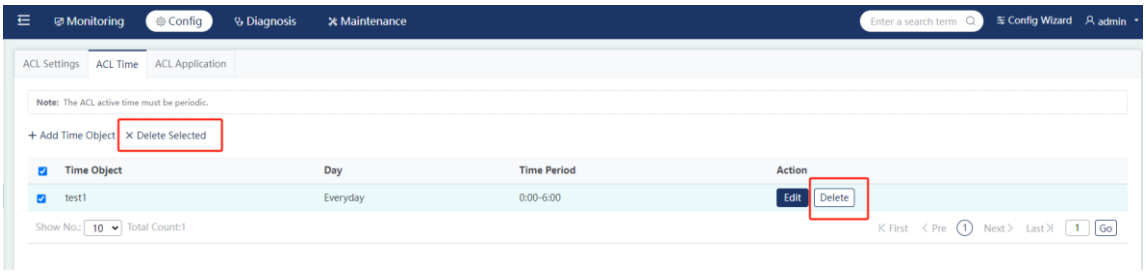
(1) Adición de un objeto de tiempo

Haga clic en **Agregar objeto de tiempo**. Edite los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



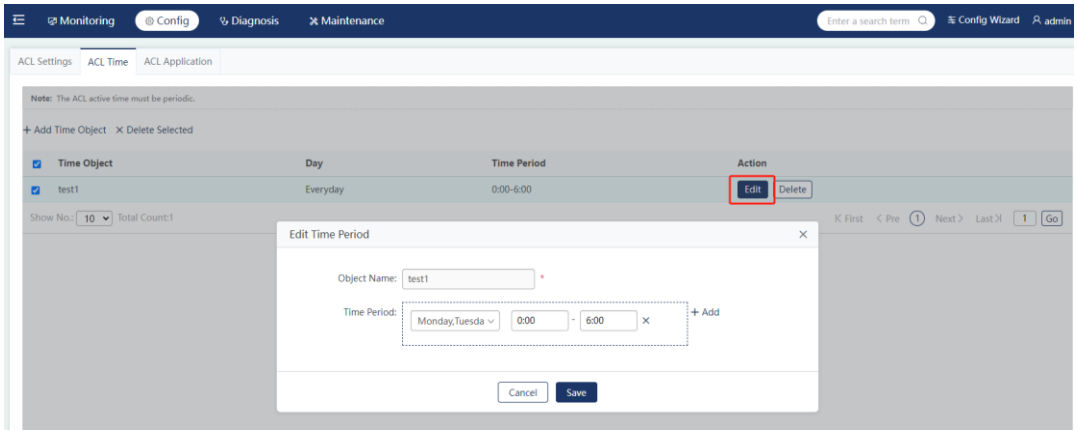
(2) Eliminación de un objeto de tiempo

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un objeto de tiempo. Para eliminar varios objetos de tiempo, seleccione los objetos de tiempo de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para agrupar los objetos de tiempo.



(3) Edición de un objeto de tiempo

Haga clic **en Editar** en la columna **Acción** de un objeto de tiempo. Edite los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

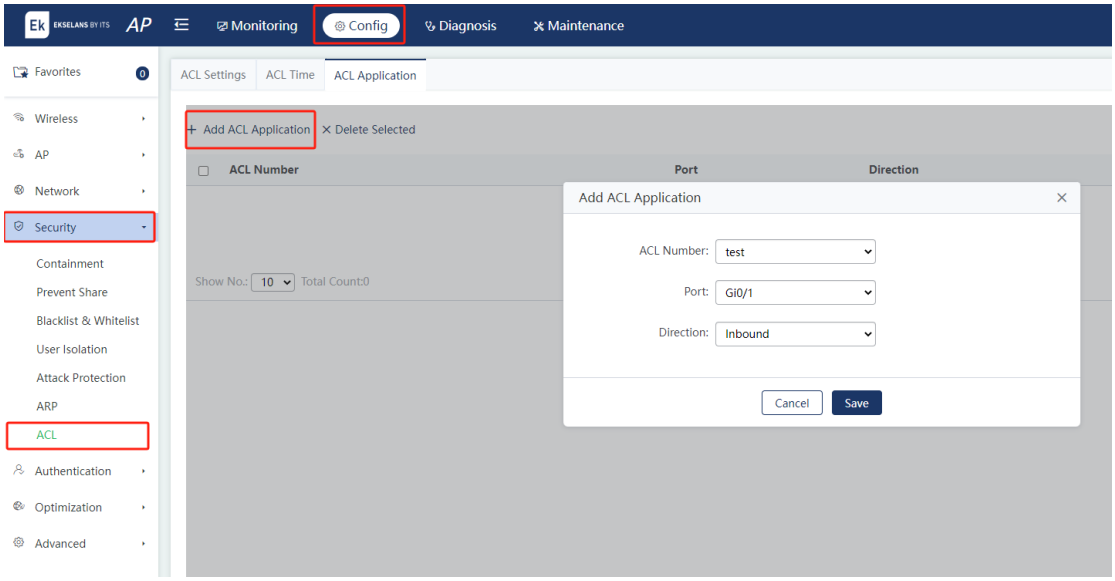


3. Aplicación de ACL

Puede configurar ACE y aplicarlas a interfaces o redes Wi-Fi para restringir el acceso de usuarios especificados o permitir que los usuarios accedan a redes especificadas.

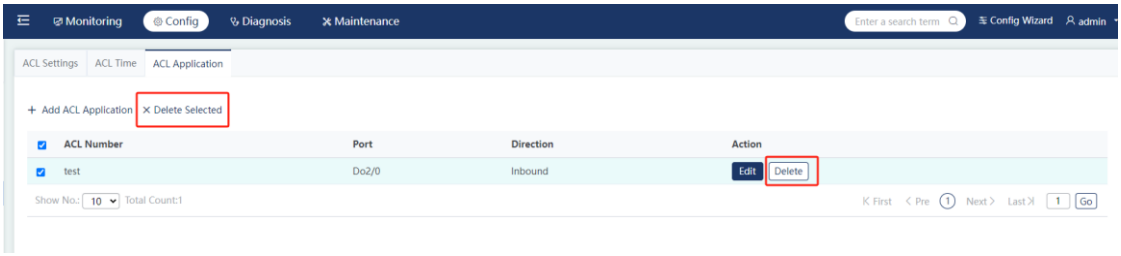
(1) Adición de una aplicación de ACL

Haga clic en **Agregar aplicación de ACL**. Introduzca los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La nueva entrada se muestra en la lista.



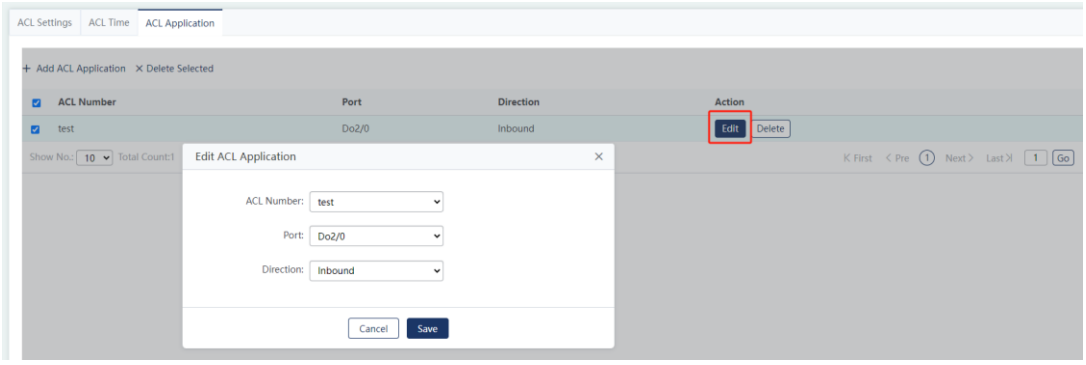
(2) Eliminación de una aplicación de ACL

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar una aplicación de ACL. Para eliminar varias aplicaciones de ACL, seleccione las aplicaciones de ACL de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para agrupar las aplicaciones de ACL.



(3) Edición de una aplicación de ACL

Haga clic **en Editar** en la columna **Acción** de una aplicación de ACL. Edite los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



5.5 Autenticación

5.5.1 Autenticación basada en la web

Elija **Config** > **Authentication** > **Web Auth**.

La autenticación basada en web le permite controlar el acceso de los usuarios a la red. Una vez habilitada la autenticación basada en web, cuando un cliente necesita acceder a la red, el dispositivo dirigirá al cliente para que acceda a un sitio web específico (servidor del portal) para la autenticación. El acceso a la red se concede al cliente solo tras una autenticación correcta.

La autenticación basada en web tiene las siguientes ventajas:

- Facilidad de uso: Los usuarios no necesitan instalar software cliente dedicado y pueden realizar la autenticación a través de un navegador.
- Servicios personalizados y expansión de servicios: A través de la interacción entre el navegador y el servidor del portal, los usuarios pueden personalizar servicios como anuncios, notificaciones y enlaces comerciales en la página del servidor del portal.

La autenticación basada en web se clasifica en **autenticación de ePortal** y **autenticación de iPortal**. Si se selecciona **Autenticación de iPortal**, no se requiere ningún servidor adicional, pero los

usuarios deben configurarse localmente para la autenticación. Si **se selecciona la autenticación de ePortal**, se requieren el servidor de ePortal y el servidor RADIUS.

1. Autenticación ePortal

La autenticación ePortal se clasifica en **ePortalv1** y **ePortalv2**:

- **ePortalv1**: Las funciones de autenticación y contabilidad son implementadas por el servidor ePortal.

  Proceso: Los usuarios envían la información de autenticación en la página de autenticación proporcionada por el software ePortal. El servidor ePortal solicita directamente la autenticación del servidor RADIUS correspondiente. Después de una autenticación exitosa, el servidor ePortal anuncia la información del usuario al dispositivo a través de SNMP y el dispositivo realiza el control de acceso para los usuarios.

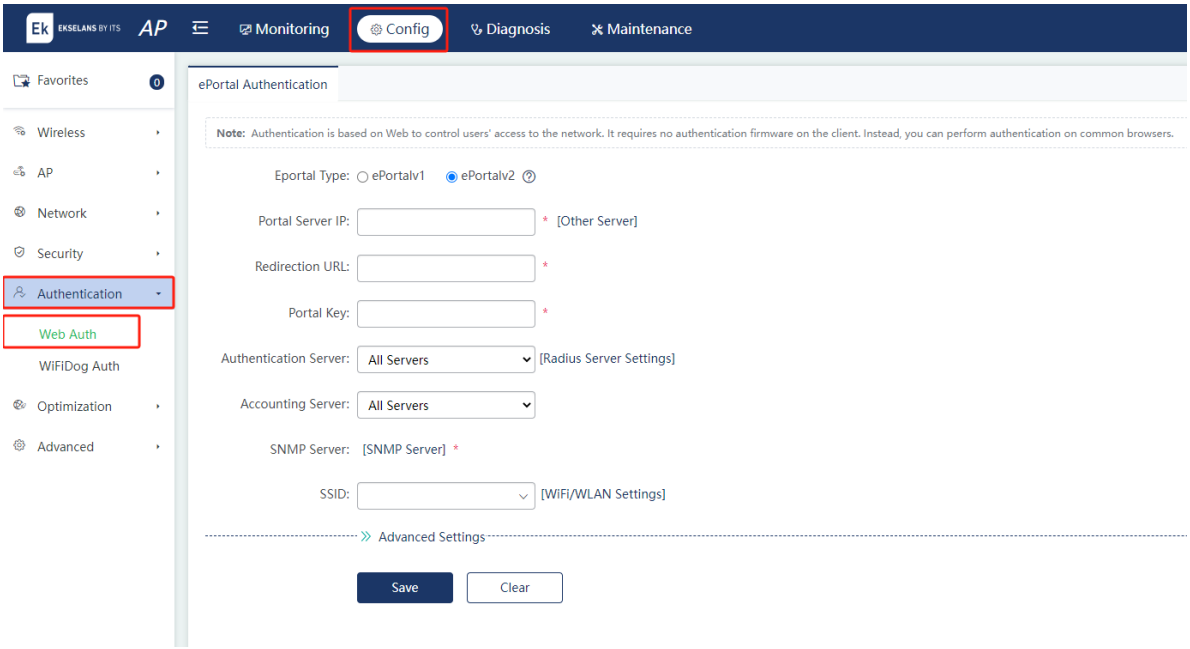
- **ePortalv2**: El servidor del portal es responsable solo de la interacción de la página de usuario y el proceso de autenticación principal se completa en el dispositivo.

  Los usuarios envían información de autenticación en la página de autenticación proporcionada por el servidor del portal, y el servidor del portal envía la información de identidad obtenida de los usuarios al dispositivo a través del protocolo del portal. El dispositivo inicia una solicitud de autenticación al servidor RADIUS utilizando la información de identidad, asigna permisos de acceso a los usuarios autenticados y devuelve los resultados de la autenticación al servidor del portal.

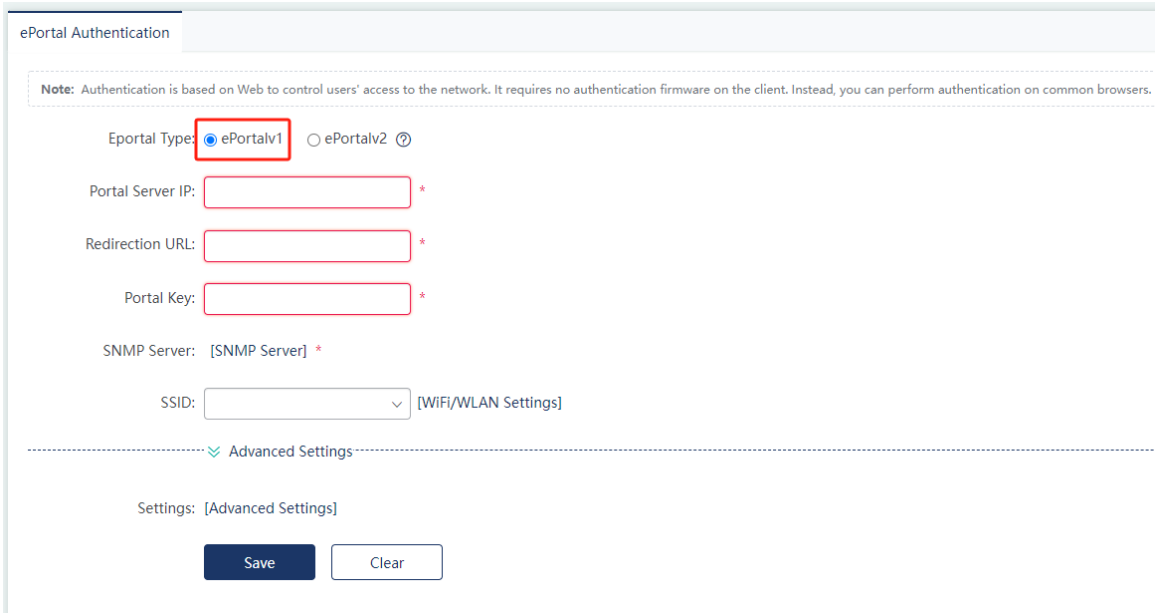
La selección de **ePortalv1** o **ePortalv2** depende del servidor del portal utilizado.

⚠ Cautela

Antes de configurar la autenticación de ePortal, debe configurar un servidor de autenticación de ePortal, incluida la implementación del servidor ePortal y la configuración de los usuarios autorizados en el servidor RADIUS.



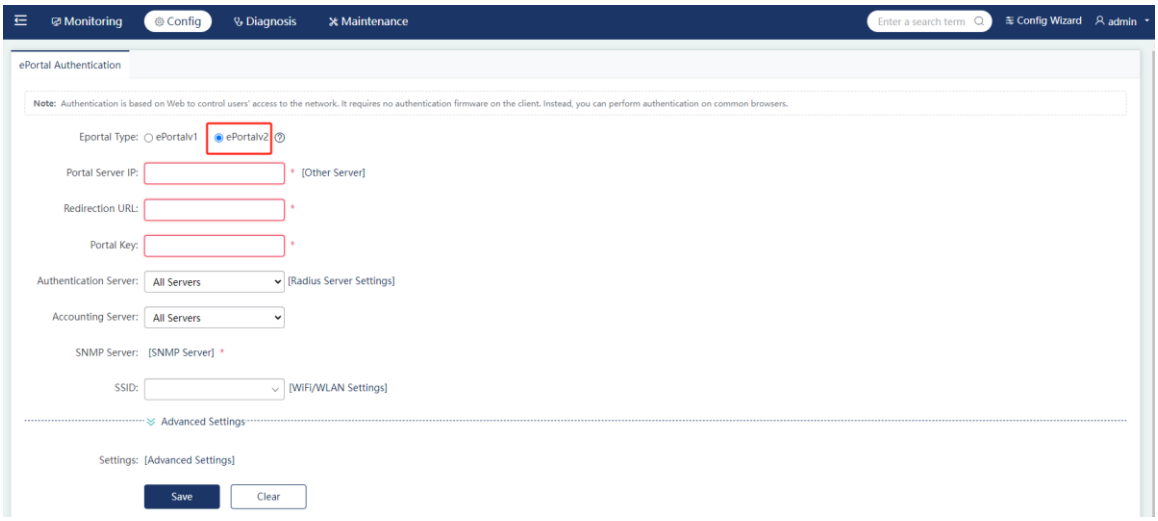
(1) **ePortalv1**:



Parámetro	Descripción
IP del servidor del portal	Introduzca la dirección IP del servidor del ePortal. Normalmente, la página de autenticación la proporciona el servidor del ePortal.
URL de redireccionamiento	Introduzca la URL de la página de autenticación. Cuando un usuario no autenticado accede a los recursos de red, el usuario se redirige automáticamente a esta página para la autenticación.

Parámetro	Descripción
Clave del portal	Configure una clave utilizada para la comunicación entre el dispositivo y el servidor de autenticación.
Servidor SNMP	Los usuarios del servidor SNMP intercambian información de configuración con el servidor del portal. Cuando el dispositivo detecta que un usuario se desconecta, notifica al servidor del portal. El servidor del portal configura el dispositivo para eliminar la información del usuario a través de SNMP. A continuación, el servidor del portal devuelve la página sin conexión al usuario.
SSID (en inglés)	Especifique la red Wi-Fi que se configurará con ePortalv1. Nota: Actualmente solo se admite el modo de autenticación global. El modo de autenticación basado en WLAN no está disponible.

(2) **ePortalv2**:



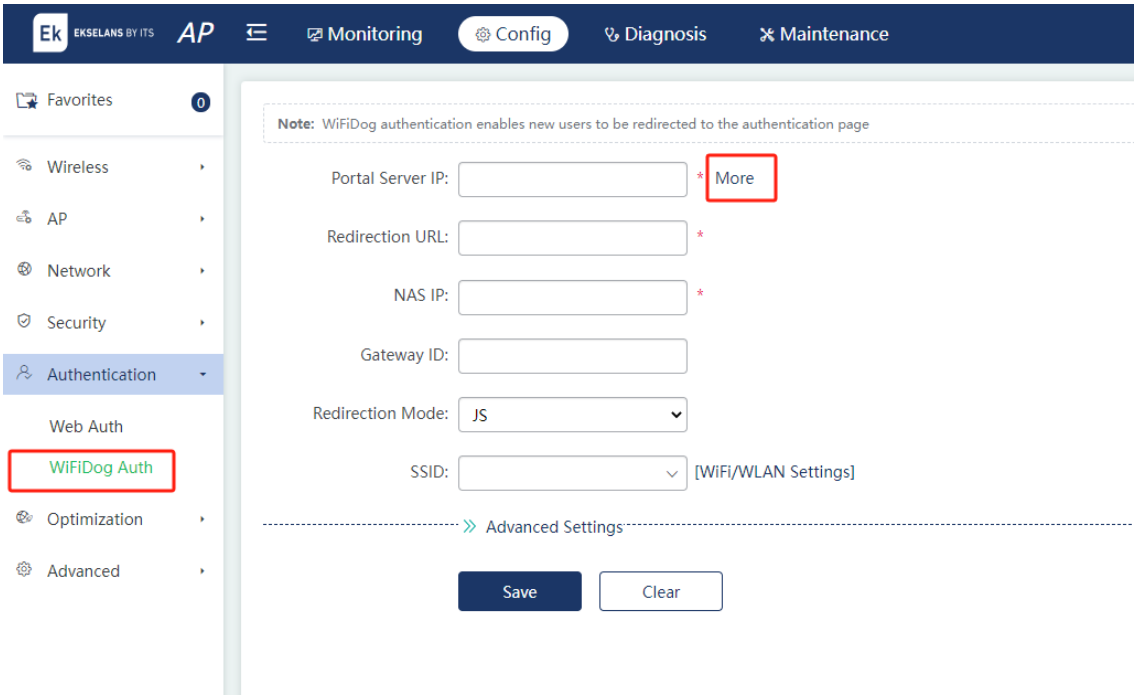
Parámetro	Descripción
IP del servidor del portal	En el modo de configuración de plantilla, ejecute el **comando ip { *ip-address* }** para configurar la dirección IP del servidor. Las solicitudes de acceso al servidor están permitidas por el dispositivo y la limitación de velocidad se puede realizar en las solicitudes transmitidas al servidor.
URL de redireccionamiento	Introduzca la dirección URL a la que se redirigirá a los usuarios, normalmente la dirección URL de la página de autenticación del portal.
Clave del portal	Configure una clave utilizada para la comunicación entre el dispositivo y

Parámetro	Descripción
	el servidor de autenticación.
Servidor de autenticación	Para aplicar correctamente ePortalv2, los usuarios deben configurar la autenticación, la autorización y la autenticación de contabilidad (AAA). La lista de métodos de autenticación asocia las solicitudes de autenticación basadas en web con el servidor RADIUS. El dispositivo selecciona el método de autenticación y el servidor en función de la lista de métodos de autenticación.
Servidor de contabilidad	(Obligatorio) Para aplicar correctamente ePortalv2, los usuarios deben configurar la contabilidad AAA. La contabilidad se utiliza para asociar un método de contabilidad con el servidor. En la autenticación basada en la web, la contabilidad se implementa para registrar la información del usuario o las tarifas.
Servidor SNMP	Los usuarios del servidor SNMP intercambian información de configuración con el servidor del portal. Cuando el dispositivo detecta que un usuario se desconecta, notifica al servidor del portal. El servidor del portal configura el dispositivo para eliminar la información del usuario a través de SNMP. A continuación, el servidor del portal devuelve la página sin conexión al usuario.
SSID (en inglés)	Especifique la red Wi-Fi que se configurará con el ePortalv2.

5.5.2 Autenticación WiFiDog

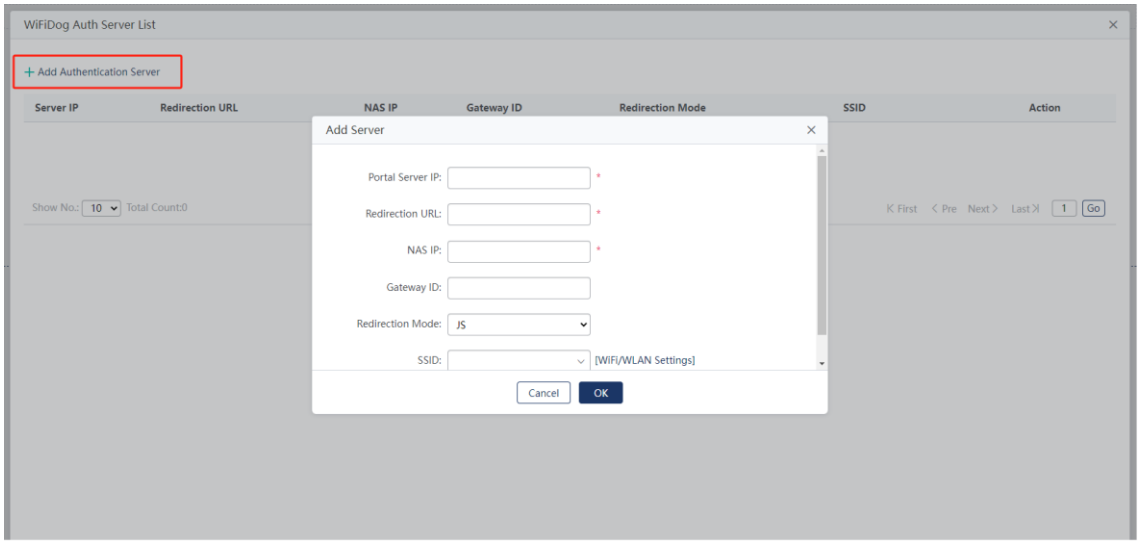
Elija **Config** > **Authentication** > **WiFiDog Auth**.

La autenticación WiFiDog permite que los usuarios no autenticados sean redirigidos a la página de autenticación para la autenticación. Haga clic en **Más** para acceder a la página Lista de **servidores de autenticación de WiFiDog**.



(1) Agregar un servidor de autenticación WiFiDog

Haga clic en **Agregar servidor de autenticación**. Introduzca los campos en la ventana emergente. Haga clic en **Aceptar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La nueva entrada se muestra en la lista



Parámetro	Descripción
IP del servidor del portal	Introduzca la dirección IP del servidor del portal.
URL de	Introduzca la URL de la página de autenticación del servidor del portal.

redireccionamiento	
NAS IP	Introduzca la dirección IP del dispositivo que va a gestionar WiFiDog, que se utiliza para la comunicación con el servidor.
ID de puerta de enlace	Introduzca el ID de una puerta de enlace utilizada por WiFiDog, que es el SN de la puerta de enlace de forma predeterminada.
Modo de redirección	Introduzca la redirección HTTP o la redirección JavaScript. La redirección de JavaScript se emplea de forma predeterminada.
SSID (en inglés)	Introduzca una red Wi-Fi que se configurará con la autenticación WiFiDog.

(2) Eliminación de un servidor de autenticación WiFiDog

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un servidor de autenticación WiFiDog.

(3) Editar un servidor de autenticación WiFiDog

Haga clic **en Editar** en la columna **Acción** de un servidor de autenticación WiFiDog. Edite los campos en la ventana emergente. Haga clic en **Aceptar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente. El servidor modificado se muestra en la lista de servidores.

5.6 Optimización de la red

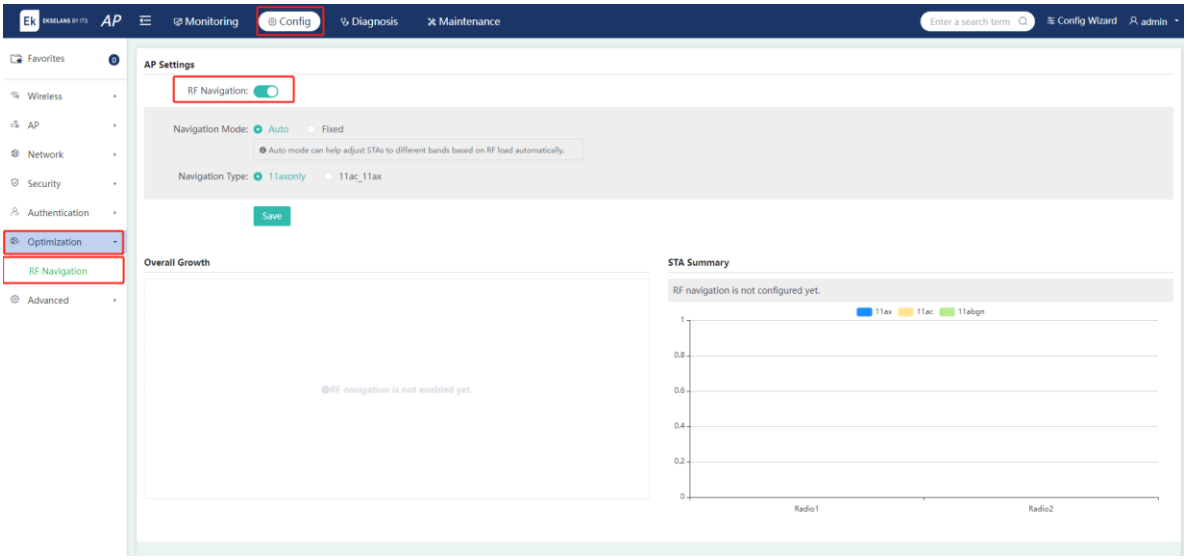
5.6.1 Navegación RF

Elija **Optimización de > configuración** > **Navegación de RF**

Nota

Es posible que algunos AP no admitan esta función. Prevalecerá el menú real.

Habilite la **navegación de RF** y configure el **modo de navegación** y el **tipo de navegación** para optimizar el rendimiento de RF.



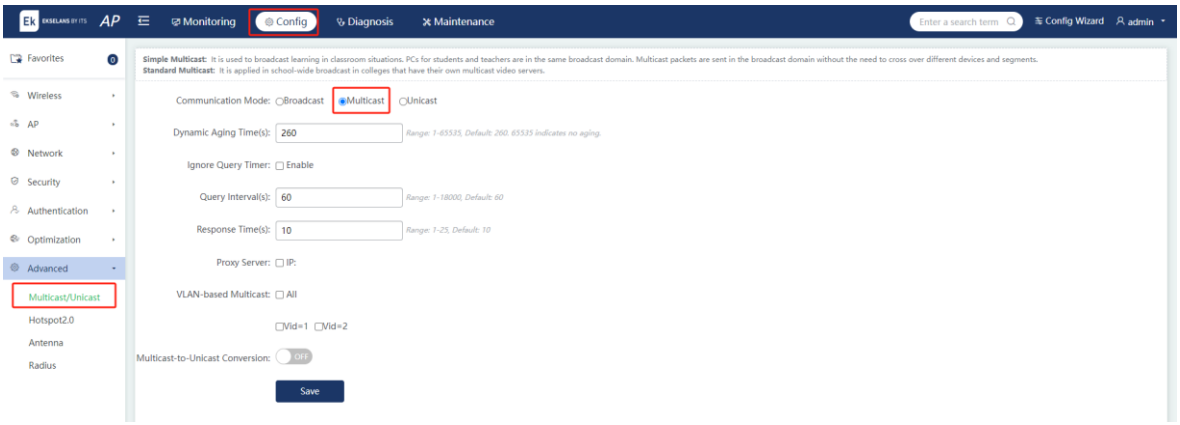
Parámetro	Descripción	
Modo de navegación	Automático	En este modo, el AP puede dirigir automáticamente un STA a la radio óptima en función de la utilización de la carga de radio.
	Fijo	En este modo, el AP dirige un STA a la radio correspondiente, que permanece sin cambios a pesar de las diferencias en los entornos de radio.
Tipo de navegación	Puede habilitar solo el protocolo 802.11ax o habilitar los protocolos 802.11ac y 802.11ax.	

5.7 Avanzado

5.7.1 Multidifusión/Unidifusión

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

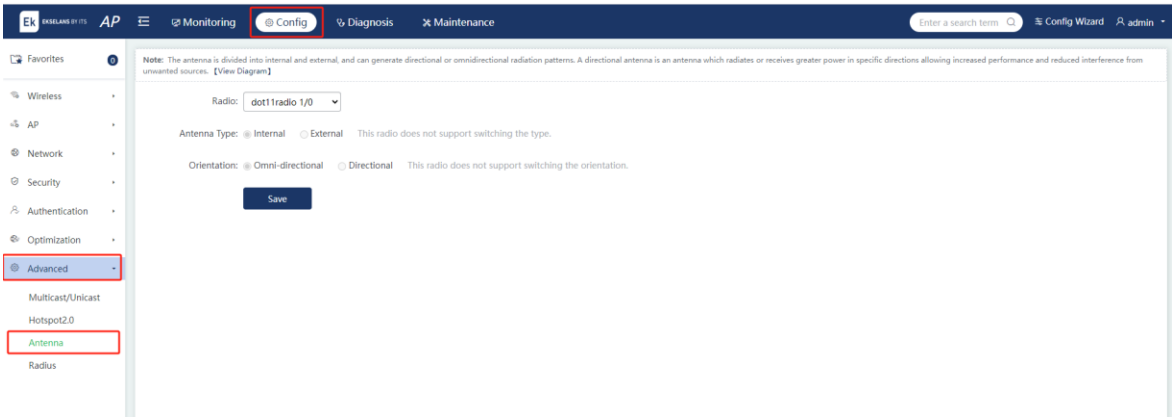
Esta función se utiliza para configurar el modo de comunicación de un dispositivo como difusión, multidifusión o unidifusión.



5.7.2 Antena

Elija **Config** > **Advanced** > **Antenna**.

Las antenas de RF se clasifican en antenas incorporadas y antenas externas. Las orientaciones de las antenas incluyen opciones direccionales y omnidireccionales. Las antenas direccionales irradian la señal dentro de un rango de ángulo específico, creando un patrón de radiación en forma de cono. El tipo y la dirección del conector de RF se pueden ajustar en función de la capacidad del conector de RF.



5.7.3 RADIO

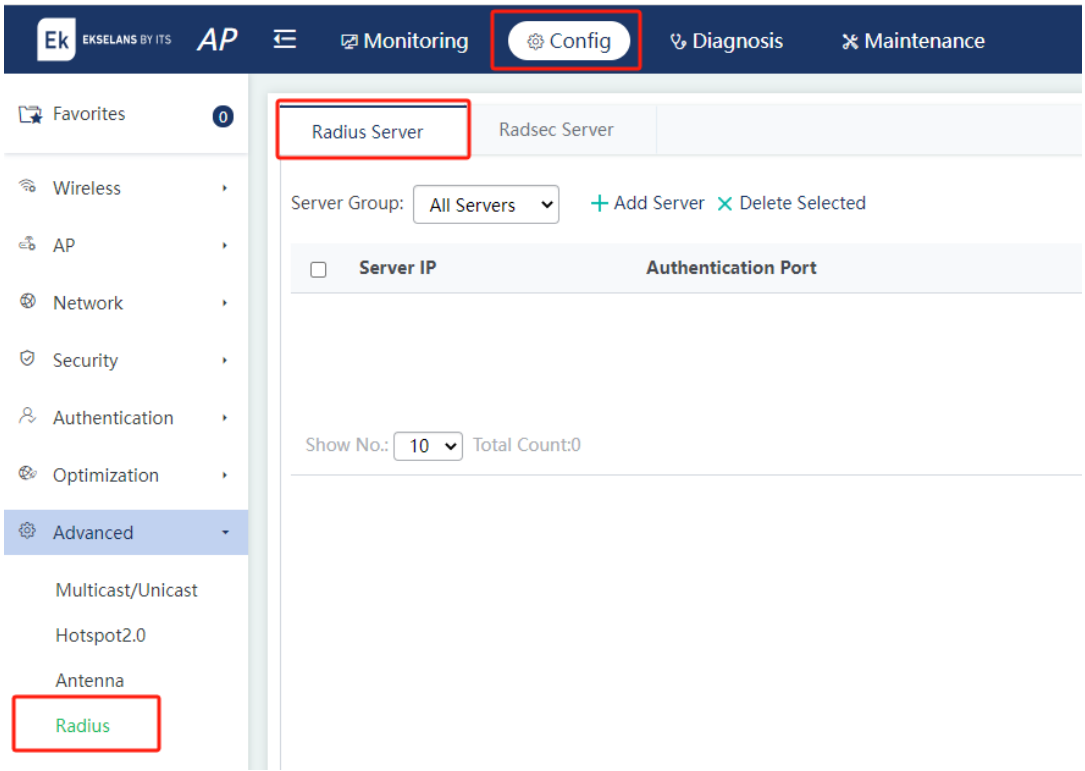
Elija **Config** > **Advanced** > **Radius**.

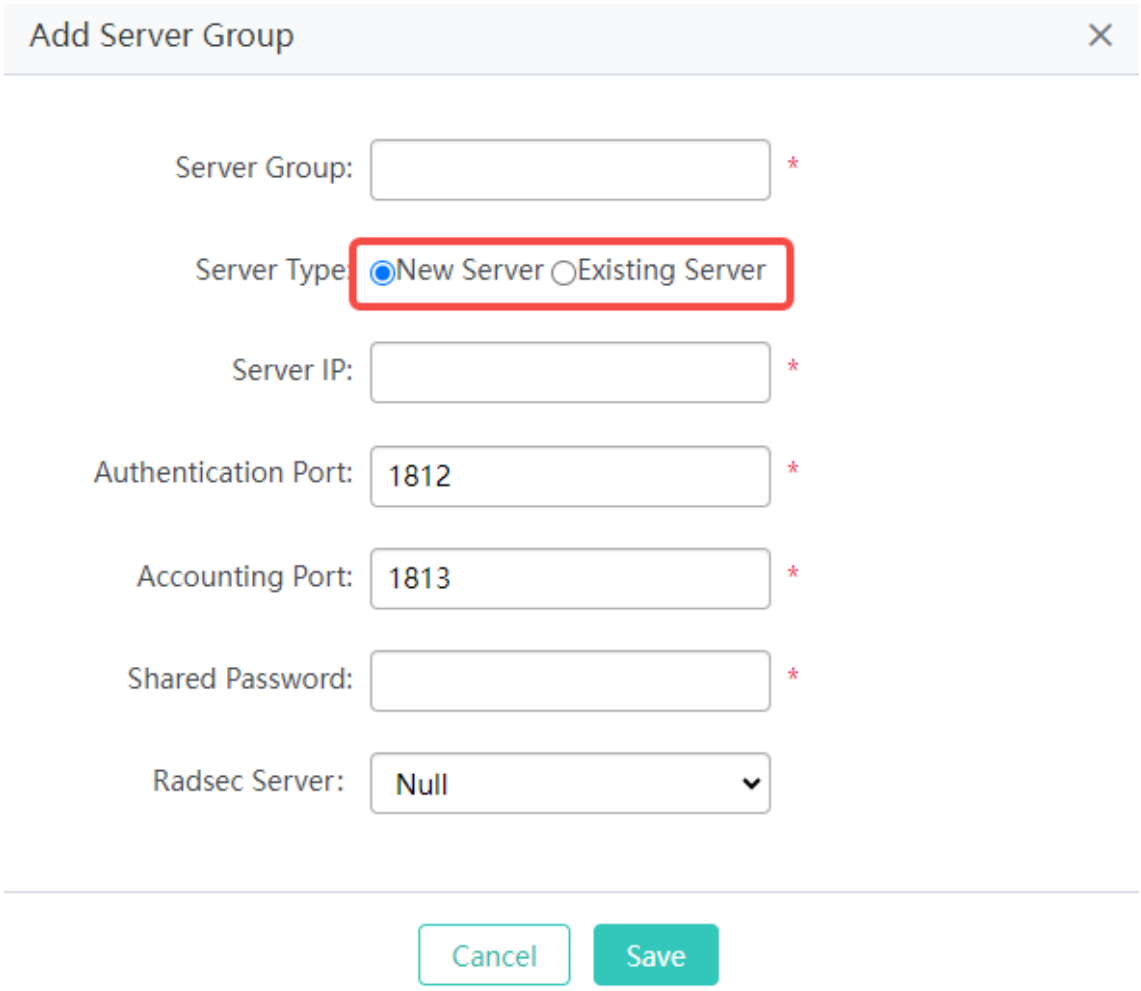
1. Servidor RADIUS

El servidor del servicio de usuario de acceso telefónico de autenticación remota (RADIUS) lleva a cabo la autenticación y la contabilidad de los usuarios de acceso para proteger la red y facilitar la administración para los administradores de red.

(1) Adición de un grupo de servidores

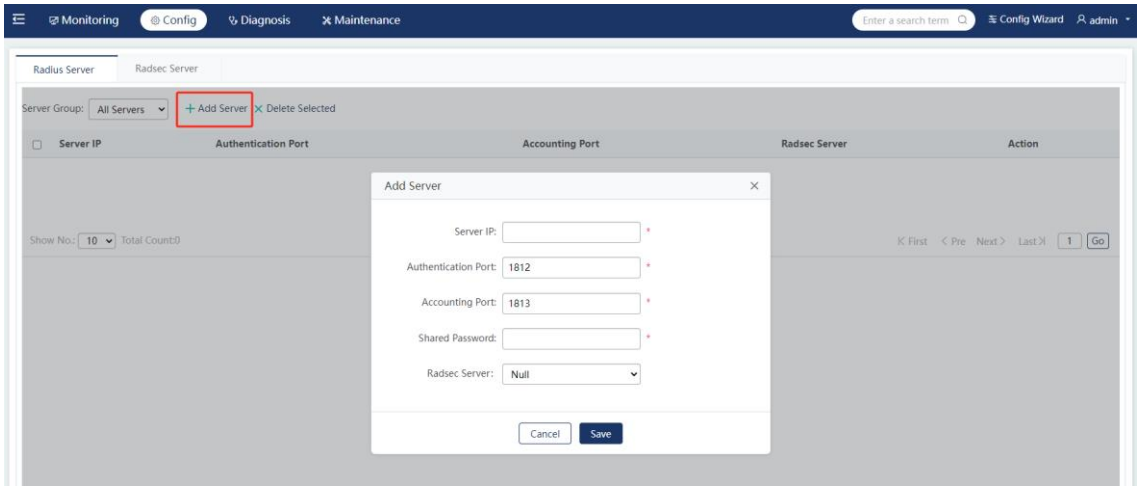
Haga clic en **Agregar grupo de servidores** en la lista desplegable. Introduzca los campos en la ventana emergente. Si selecciona **Nuevo servidor** para el tipo de **servidor** presentado, se agregará un grupo de servidores y un servidor y el servidor pertenecerá al grupo de servidores. Si selecciona **Servidor existente**, se agregará un servidor existente al grupo de servidores.





(2) Adición de un servidor

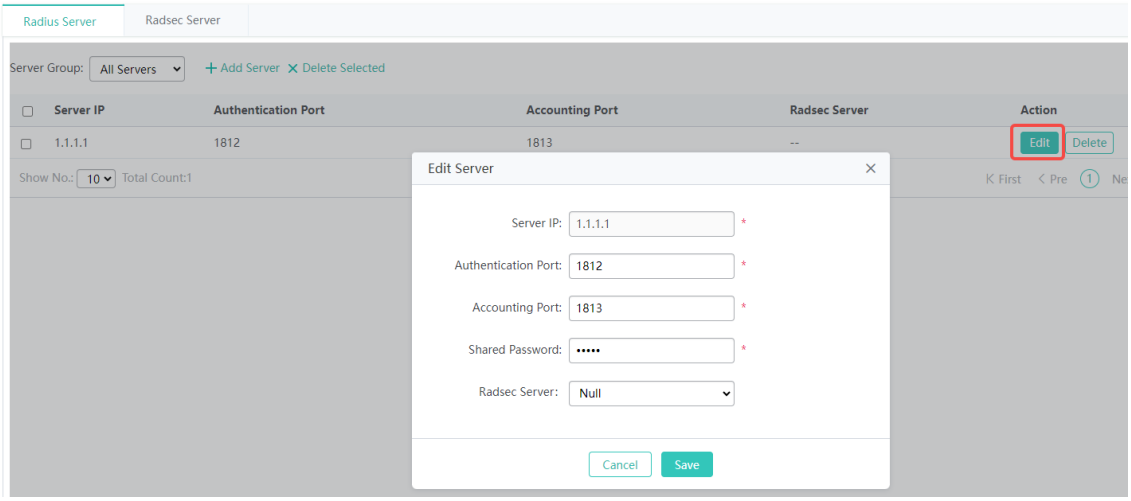
Seleccione **Todos los servidores** en el campo **Grupo de servidores**. Haga clic en **Agregar servidor**. Introduzca los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



Parámetro	Descripción
IP del servidor	Introduzca la dirección IP de un servidor RADIUS.
Puerto de autenticación	Introduzca el número de puerto UDP para la autenticación RADIUS. El rango de valores es de 0 a 65535. El valor 0 indica que el host no realiza la autenticación.
Puerto de contabilidad	Introduzca el número de puerto UDP para la contabilidad RADIUS. El rango de valores es de 0 a 65535. El valor 0 indica que el host no realiza la contabilidad.
Contraseña compartida	Introduzca la contraseña compartida para la comunicación entre el servidor de acceso a la red (dispositivo de enrutamiento) y el servidor RADIUS.
Servidor Radsec	(Opcional) Seleccione el ID del servidor RadSec, al que se redirige el tráfico desde el servidor RADIUS. **Nota** Este campo no se muestra si el dispositivo no es compatible con la función RadSec.

(3) Edición de un servidor

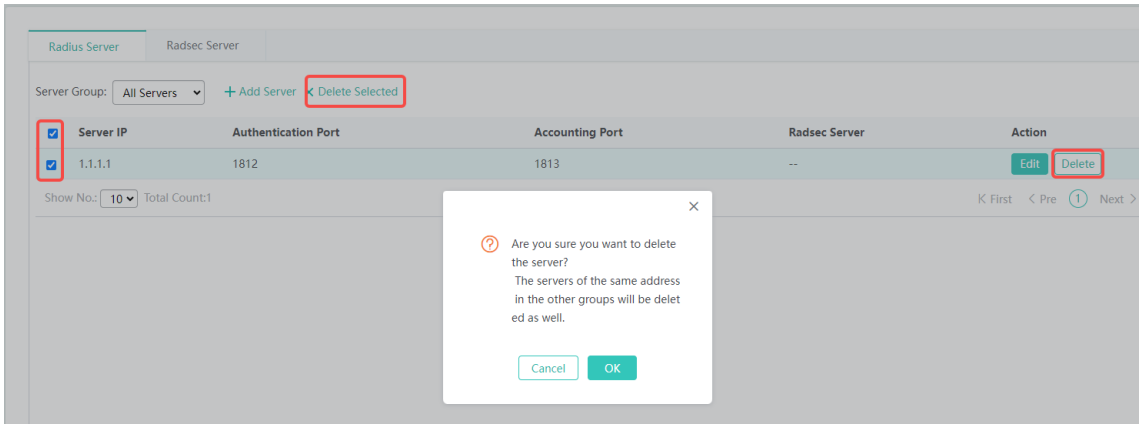
Haga clic **en Editar** en la columna **Acción**. Edite los parámetros en la ventana emergente. Haga clic en **Guardar**.



(4) Eliminación de un servidor

Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un servidor. Para eliminar varios servidores, seleccione los servidores de destino

en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para agrupar los servidores.

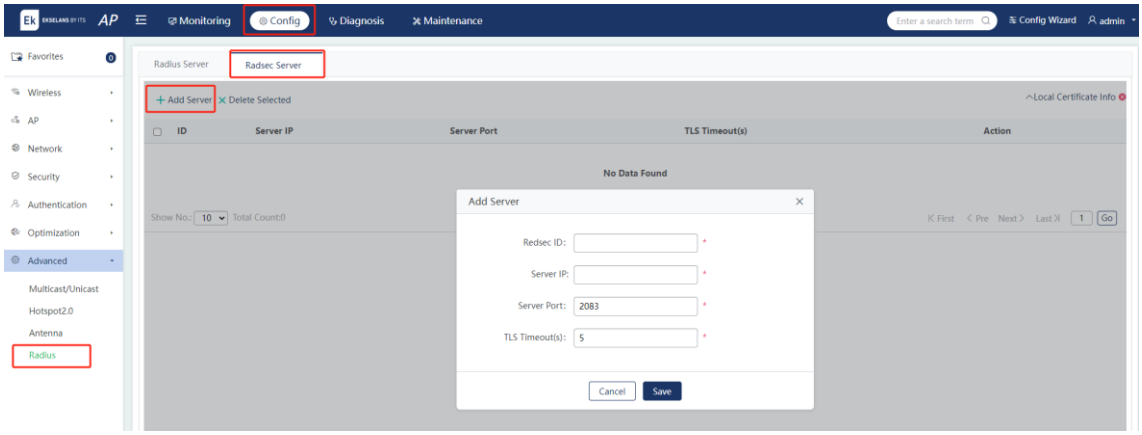


2. Servidor RadSec

RadSec proporciona una comunicación segura para las solicitudes RADIUS mediante el protocolo de seguridad de la capa de transporte (TLS) y permite que los datos de autenticación, autorización y contabilidad de RADIUS se transmitan de forma segura a través de redes que no son de confianza.

(1) Adición de un servidor

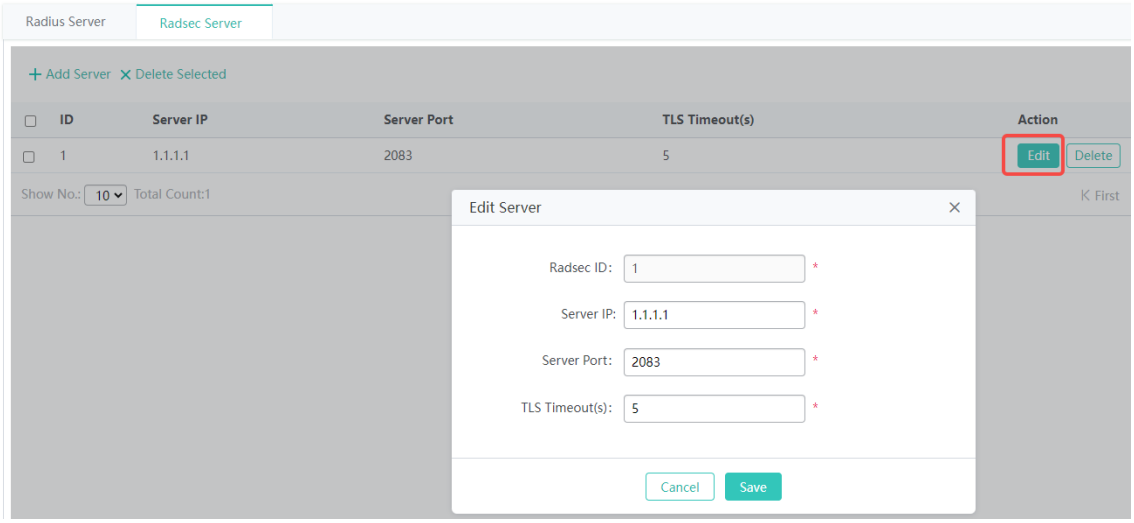
Haga clic en **Agregar servidor**. Introduzca los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



Parámetro	Descripción
Radsec ID	Introduzca el ID único de un servidor RadSec. El valor es un número entero en el intervalo de 1 a 255.
IP del servidor	Introduzca la dirección IP del servidor RadSec.
Puerto del servidor	Introduzca el número de puerto del servidor RadSec. El rango de valores es de 1 a 65535. El valor predeterminado es 2083.
Tiempo de espera de TLS	Introduzca el tiempo de espera de la conexión TLS. El rango de valores es de 1 a 1000. El valor predeterminado es 5.

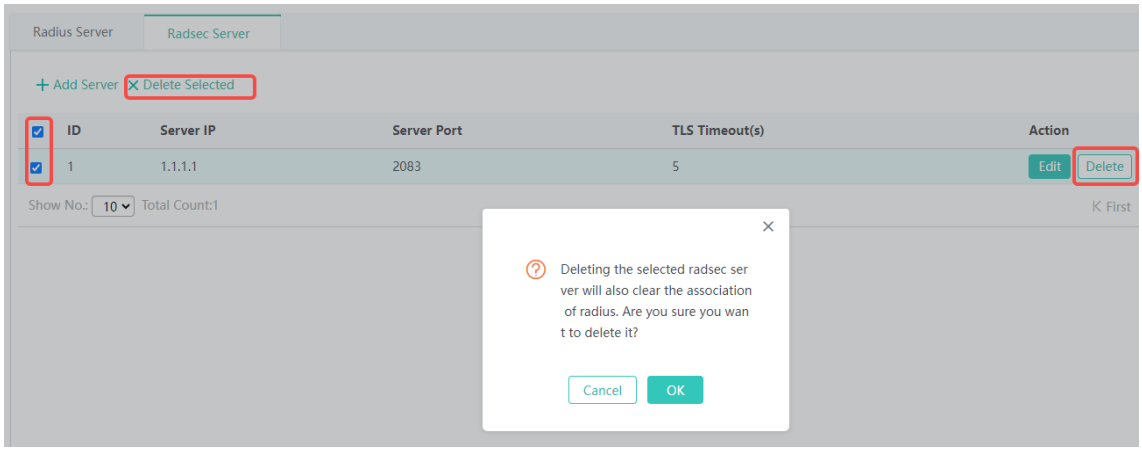
(2) Edición de un servidor

Haga clic **en Editar** en la columna **Acción**. Edite los parámetros en la ventana emergente. Haga clic en **Guardar**.



(3) Eliminación de un servidor

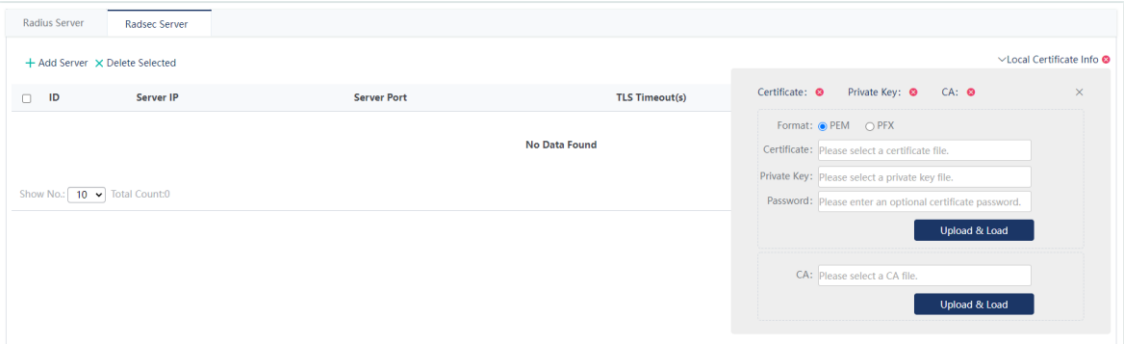
Haga clic **en Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un servidor. Para eliminar varios servidores, seleccione los servidores de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic **en Aceptar** en la ventana emergente para agrupar los servidores.



(4) Gestión de certificados locales

Haga clic en **Información de certificado local**. Aparecerá la ventana de administración de certificados locales. El icono de la derecha de Información del **certificado local** muestra el estado de carga del certificado. Seleccione un archivo de certificado y un archivo de clave privada. Introduzca la contraseña del certificado (si la hay). Haga clic en **Cargar y cargar**. Se muestra un mensaje que indica que la operación se ha realizado correctamente. Se admiten

los formatos PEM y PFX. Si el archivo de certificado no contiene información de CA, seleccione un archivo de CA y haga clic en **Cargar y cargar**.



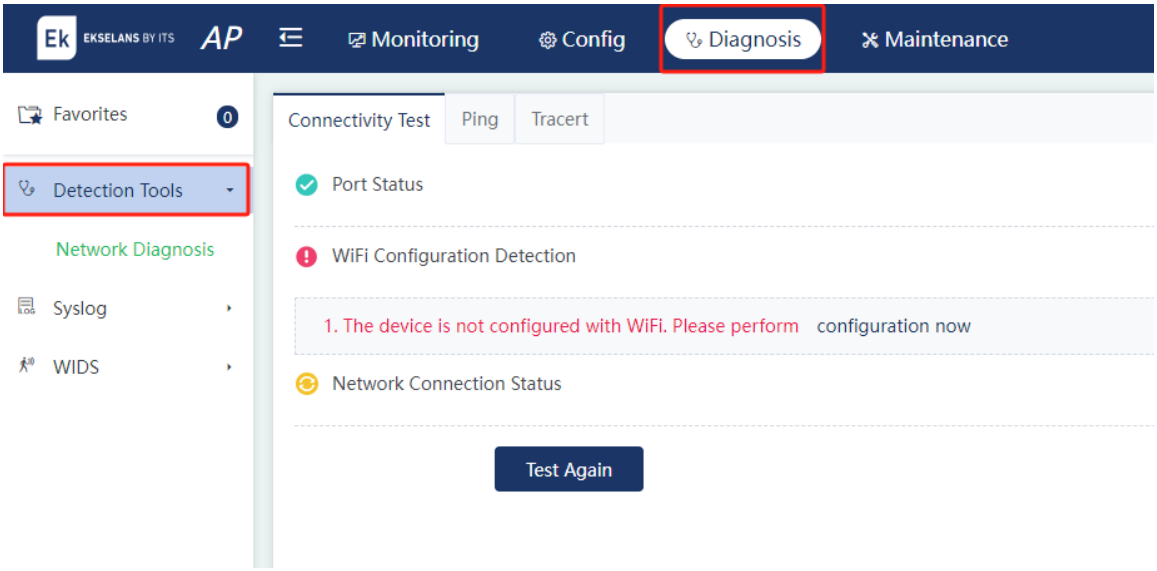
6 Diagnóstico

6.1 Herramientas de detección

6.1.1 Diagnóstico de red

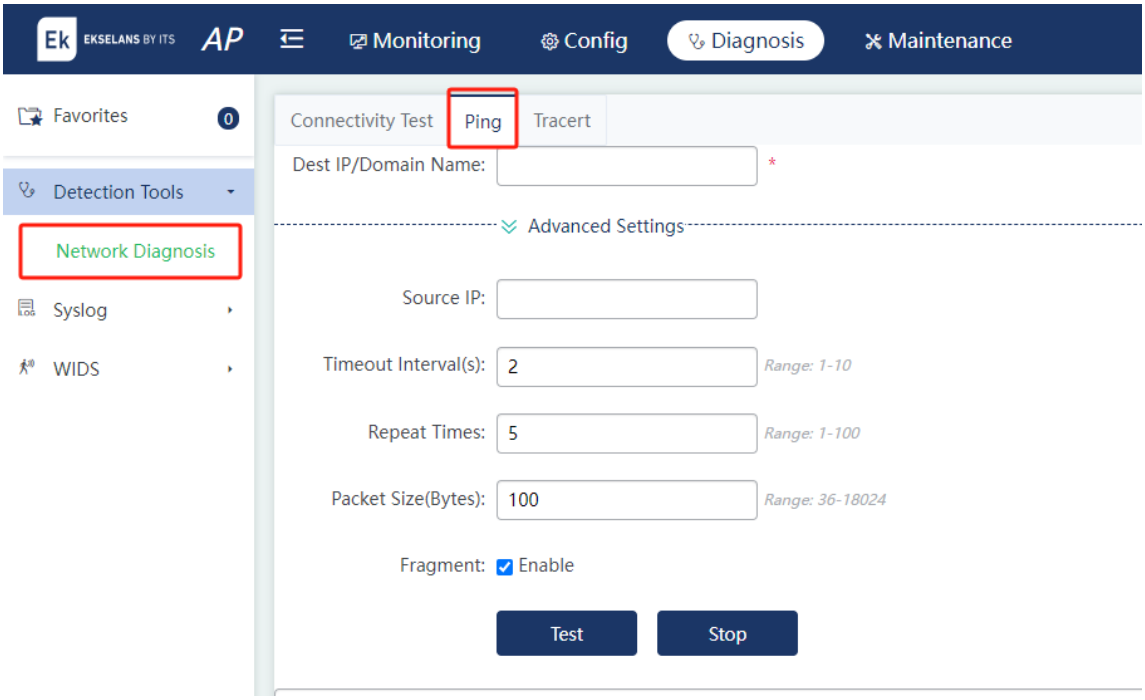
Elija **Diagnosis** > **Detection Tools** > **Network Diagnosis**.

1. Prueba de conectividad



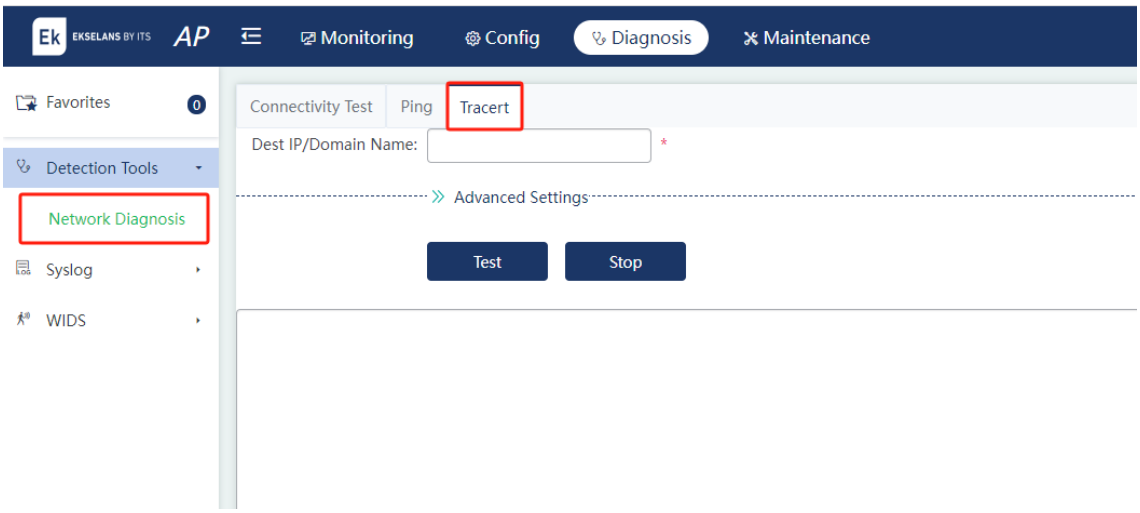
Elemento de detección	Descripción
Estado del puerto	Compruebe si un puerto del AP está activo.
Detección de configuración WiFi	Compruebe si hay una red Wi-Fi configurada en el AP.
Estado de la conexión de red	Compruebe si el AP puede comunicarse con una red externa.

2. Señal



Parámetro	Descripción
IP de destino/Nombre de dominio	Introduzca la dirección IP de destino o el nombre de dominio al que se va a hacer ping.
IP de origen	Introduzca la dirección IP de origen de los paquetes ping, es decir, la dirección de la interfaz local del dispositivo.
Intervalo(s) de tiempo de espera	Introduzca el intervalo de tiempo de espera.
Tiempos de repetición	Introduzca el número de paquetes de datos que se van a transmitir.
Tamaño del paquete (bytes)	Introduzca la longitud de la sección de relleno de datos en un paquete de datos que se va a transmitir.
Fragmento	Introduzca el bit de indicador DF de una dirección IP. Cuando el bit de indicador DF se establece en 1, los paquetes de datos no se fragmentan. El bit de indicador DF predeterminado es 0.

3. Tracert



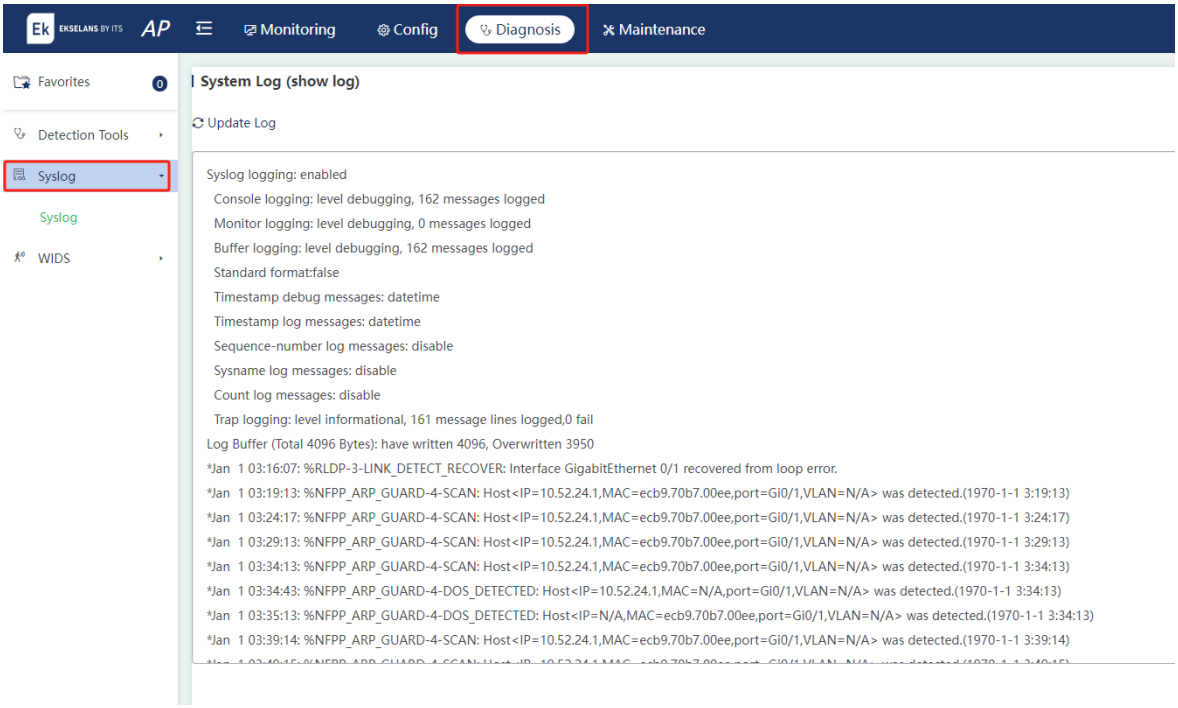
Parámetro	Descripción
IP de destino/Nombre de dominio	Introduzca la dirección de destino o el nombre de dominio de Tracert.
IP de origen	Introduzca la dirección de origen de Tracert, es decir, la dirección de la interfaz local del dispositivo.
Intervalo(s) de tiempo de espera	Introduzca el intervalo de tiempo de espera.

6.2 Registro

6.2.1 Registro del sistema

Elija **Diagnosis** > **Syslog** > **Syslog**.

Los registros del sistema se pueden utilizar para ayudar al personal de posventa y de investigación y desarrollo a localizar problemas. Haga clic en **Exportar syslog** para descargar el syslog en el equipo.



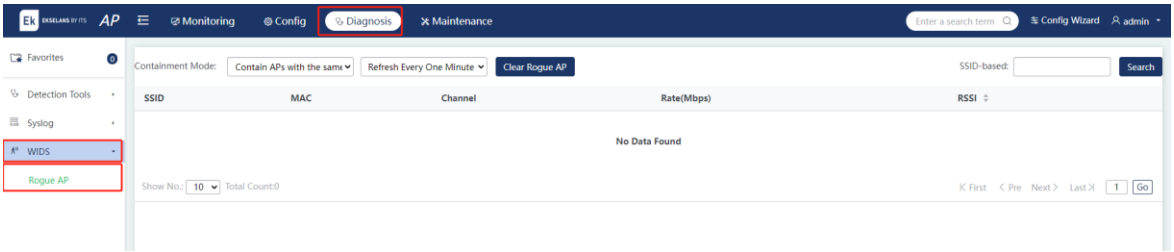
6.3 Sistema inalámbrico de detección de intrusos

6.3.1 AP pícaro

Elija **Diagnosis** > **WIDS** > **Rogue AP.**

Es posible que existan puntos de acceso no autorizados en una red inalámbrica. Pueden tener vulnerabilidades de seguridad o estar controlados por atacantes, lo que representa una gran amenaza para la seguridad de la red.

La siguiente página muestra los posibles AP no autorizados que se identifican cuando se habilita la contención de AP no autorizados.



7 Mantenimiento

7.1 Configuración

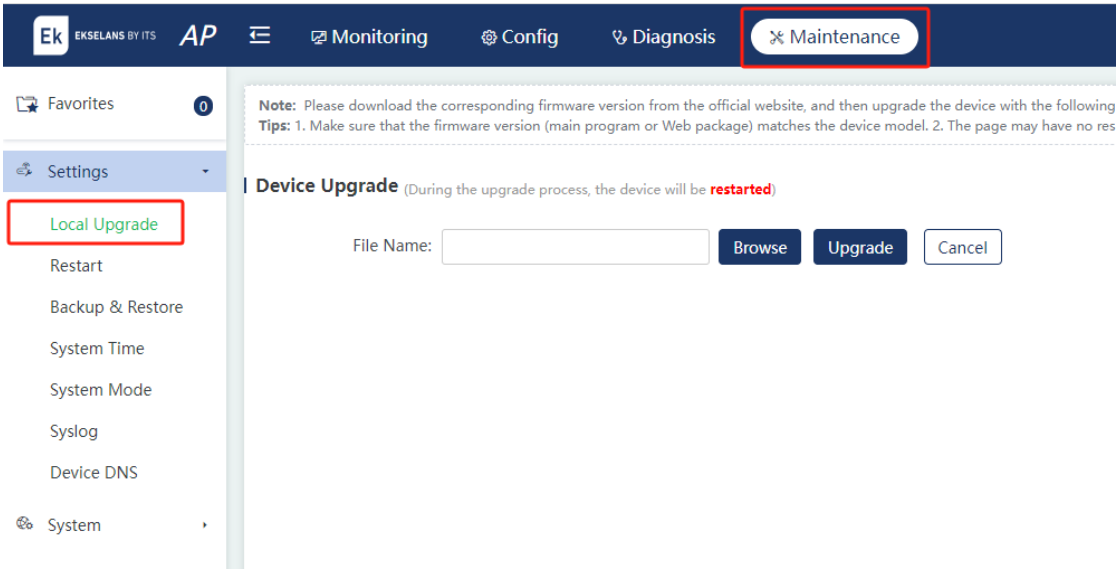
7.1.1 Actualización local

Elija **Mantenimiento** > **Configuración** > **Actualización local**.

Haga clic en **Examinar** para seleccionar el archivo .bin descargado. Haga clic en **Actualizar**.

Cautela

- Durante la actualización, el dispositivo se reiniciará, lo que provocará la desconexión de la red y la interrupción del servicio. Por lo tanto, actualice el dispositivo cuando los servicios no se vean afectados o durante las horas de menor actividad.
- El proceso de actualización lleva algún tiempo. Durante la actualización, evite realizar cualquier operación en la página web. De lo contrario, se interrumpirá el proceso de actualización.
- Durante la actualización, es posible que la página web no responda temporalmente. En este caso, no apague ni reinicie el dispositivo hasta que la actualización se realice correctamente.



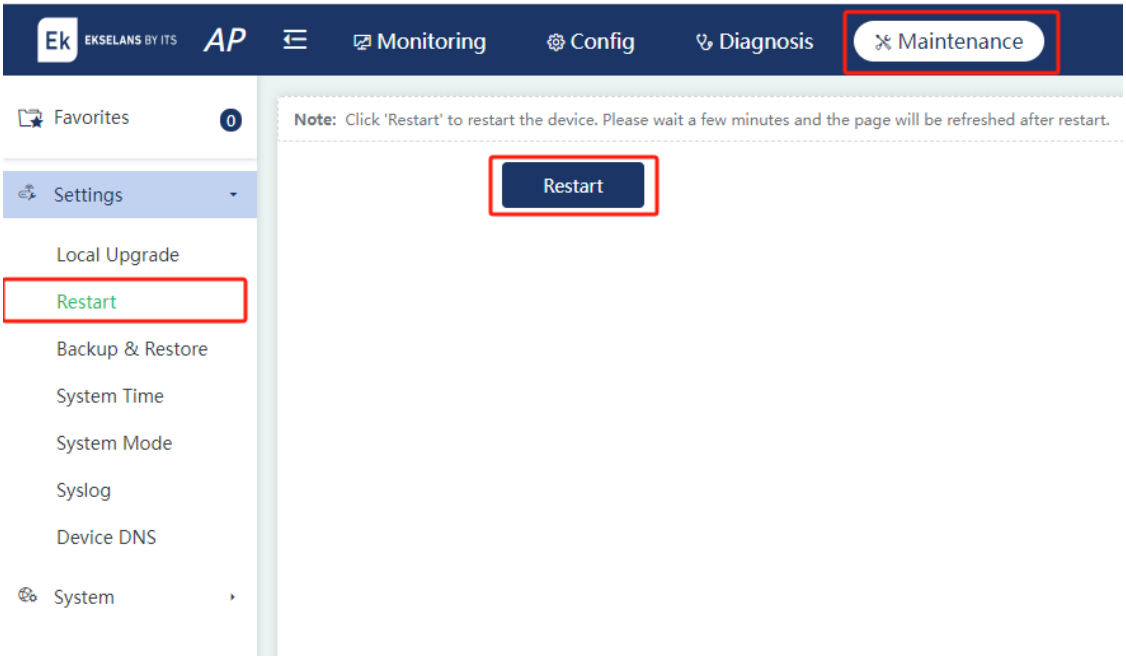
7.1.2 Reanudar

Elija **Mantenimiento** > **Configuración** > **Reiniciar**.

Haga clic en **Reiniciar** para reiniciar el AP.

Cautela

Reiniciar el dispositivo provocará la desconexión de la red y la interrupción del servicio. Por lo tanto, actualice el dispositivo cuando los servicios no se vean afectados o durante las horas de menor actividad.

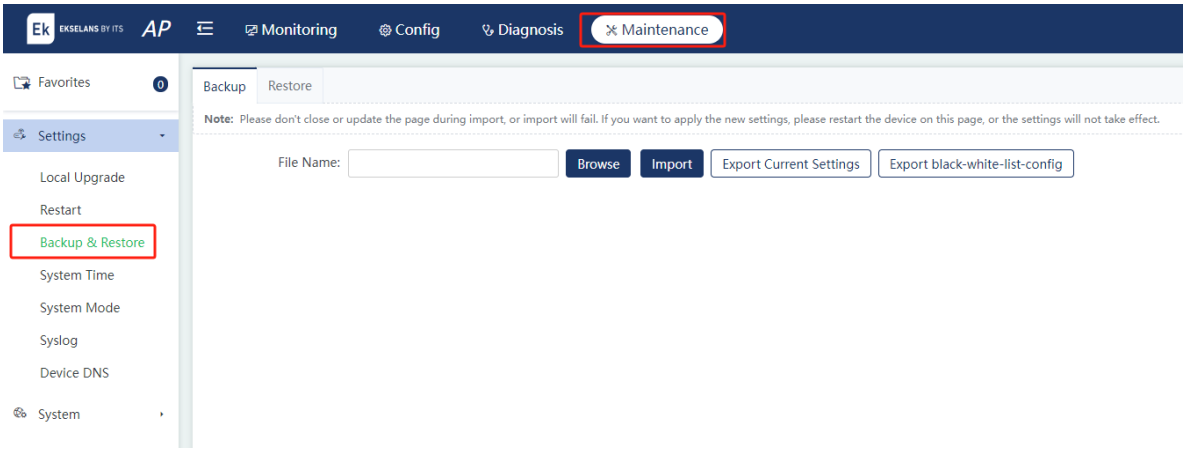


7.1.3 Gestión de la configuración

Elija **Mantenimiento** > **Configuración** > **Copia de seguridad y restauración**.

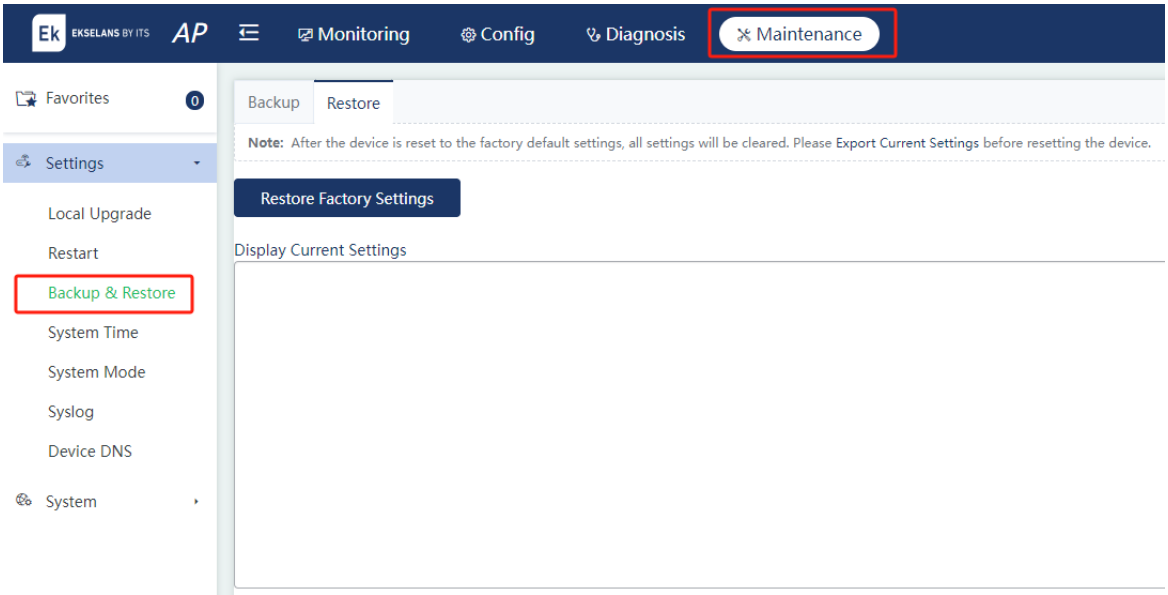
1. Copia de seguridad

Realice una copia de seguridad del archivo de configuración en el dispositivo. Puede importar o exportar configuraciones para realizar operaciones por lotes, lo que facilita la gestión de la configuración.



2. Restaurar

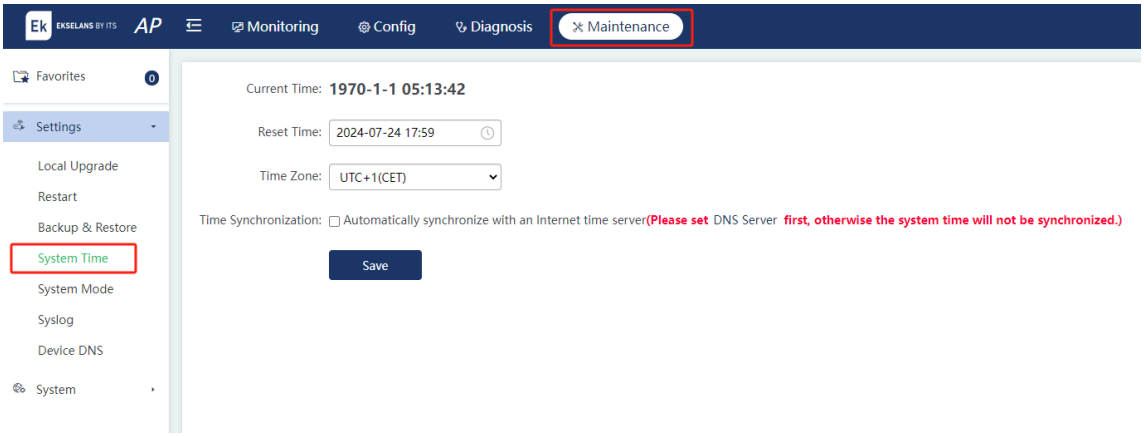
Después de restaurar el dispositivo a la configuración de fábrica, use la dirección IP predeterminada para acceder a la web. Al restaurar el dispositivo a la configuración de fábrica, se borrarán todas las configuraciones. Por lo tanto, haga ejercicio con precaución.



7.1.4 Hora del sistema

Seleccione **Mantenimiento** > **Configuración** > **Hora del sistema**.

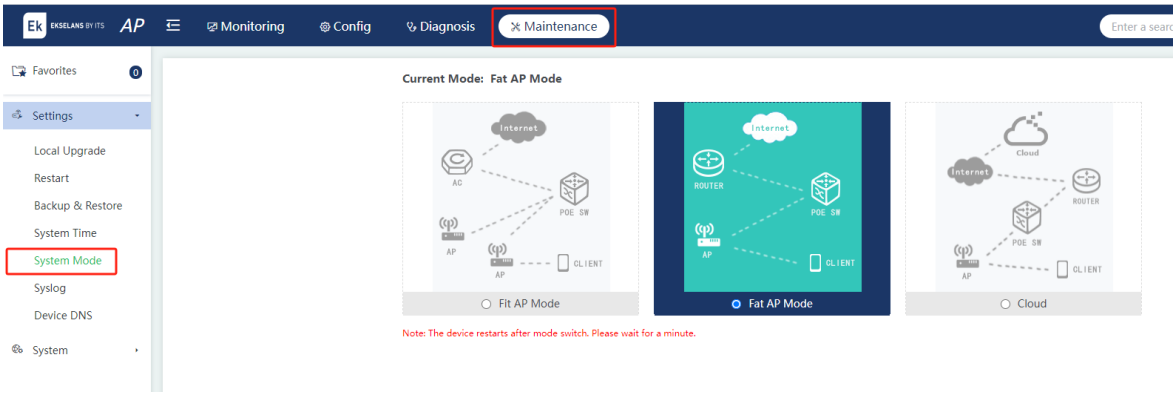
Establezca la hora del sistema en función de la zona horaria en la que se encuentra el dispositivo para garantizar una información precisa del dispositivo.



7.1.5 Modo de sistema

Seleccione **Mantenimiento** > **Configuración** > **Modo de sistema**.

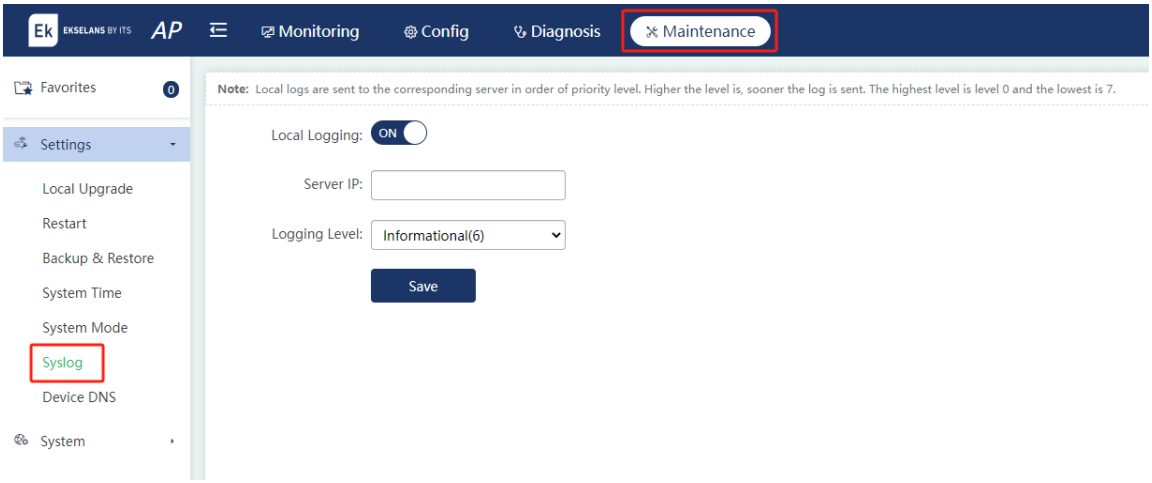
Seleccione el modo de sistema del AP. **Son compatibles con el modo Fit AP**, el **modo Fat AP** y el **modo Cloud**.



7.1.6 Servidor de registro

Seleccione **Mantenimiento** > **Configuración** > **Syslog**.

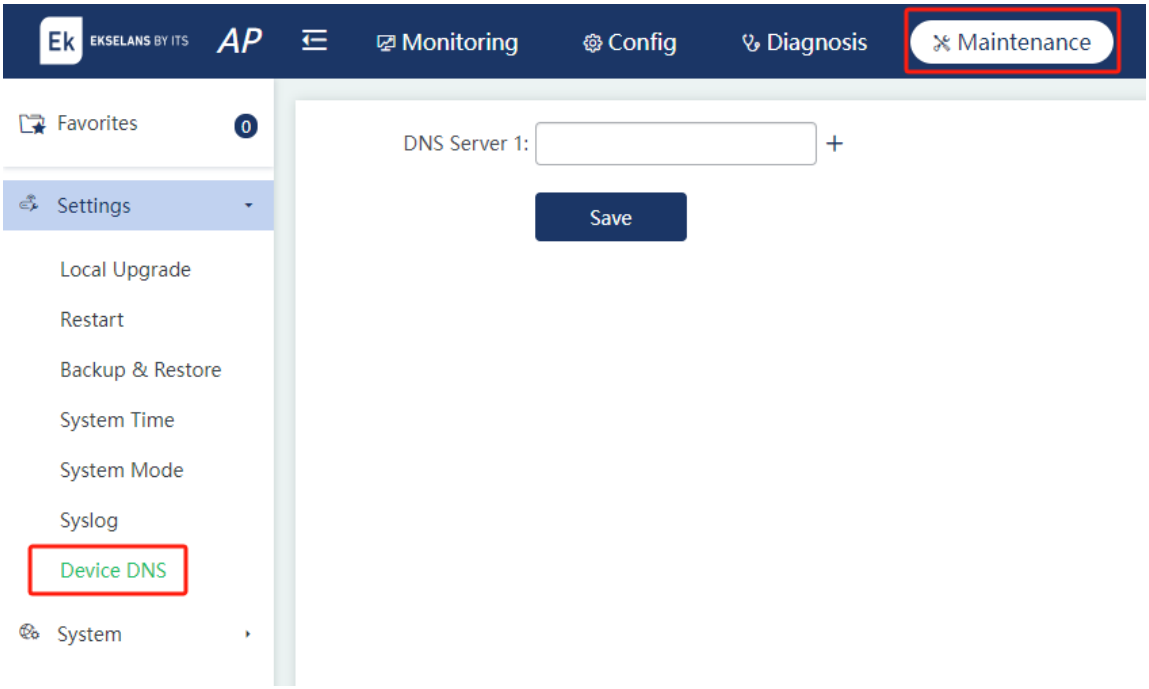
El dispositivo envía registros locales al servidor para su almacenamiento. Los registros históricos se almacenan para facilitar la consulta.



7.1.7 DNS

Elija **Mantenimiento** > **Configuración** > **DNS del dispositivo**.

Para implementar la resolución dinámica de nombres de dominio, se debe configurar un servidor DNS.



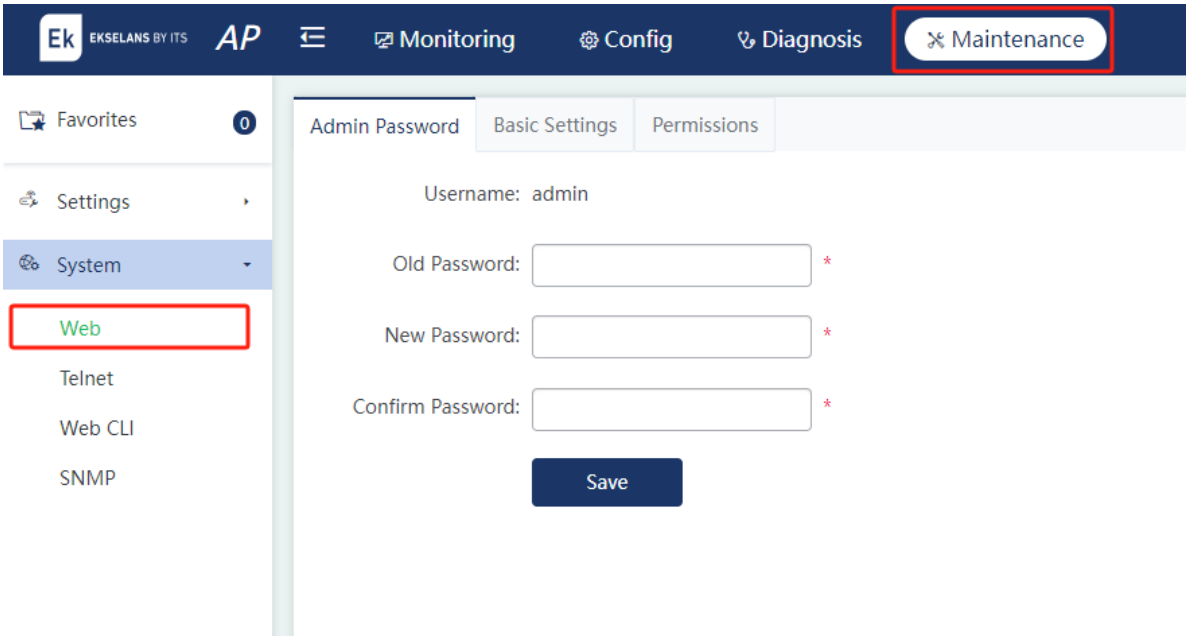
7.2 Sistema

7.2.1 Gestión Web

Seleccione **Mantenimiento** > **Sistema** > **Web**.

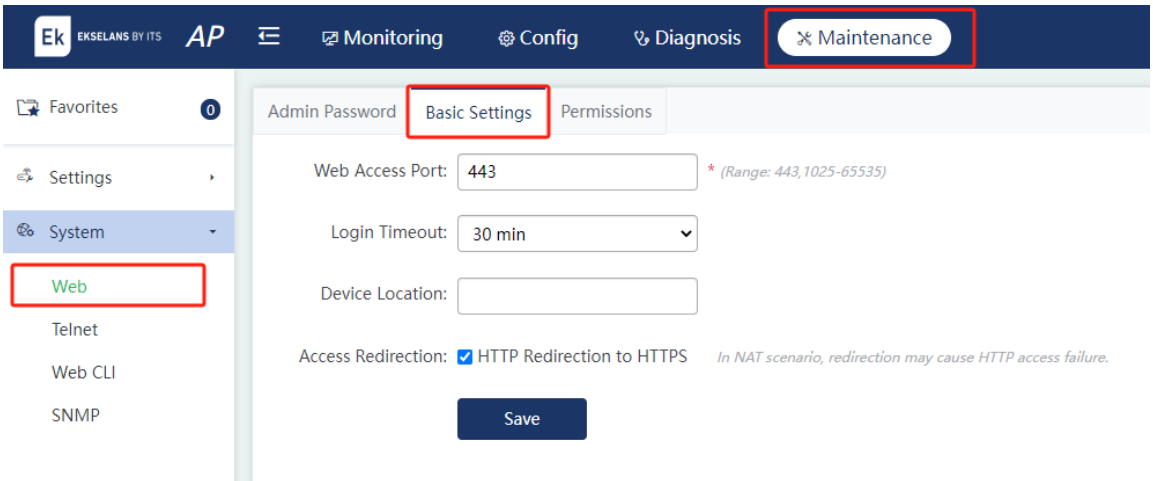
1. Contraseña de administrador

Para mejorar la seguridad del sistema y garantizar un intercambio seguro de información, se recomienda cambiar la contraseña predeterminada del sistema.



2. Ajustes básicos

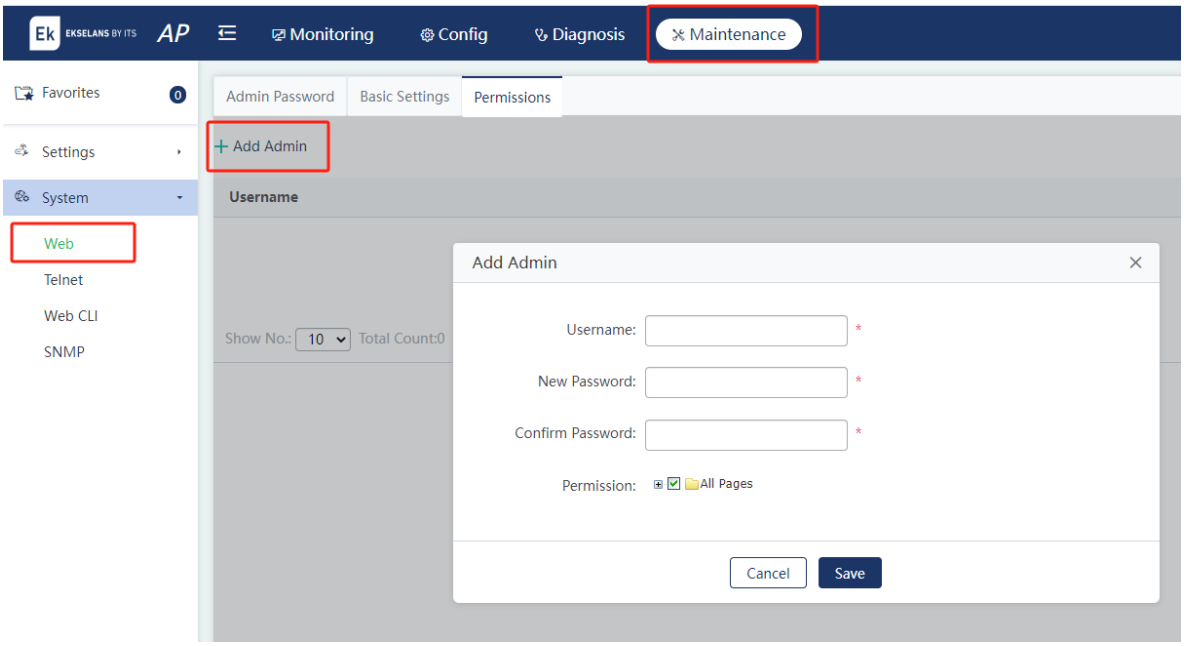
Para facilitar la administración de dispositivos, configure la ubicación del dispositivo en la **página Configuración básica**. Establezca el puerto de acceso web y el tiempo de espera de inicio de sesión. Cuando expira el tiempo de espera de inicio de sesión, el sistema web se cierra automáticamente para garantizar la seguridad del sistema. Si el dispositivo admite la configuración de **Limitar inicios de sesión**, establezca el número máximo de usuarios que pueden iniciar sesión en el dispositivo simultáneamente con la misma cuenta (el valor predeterminado es 10).



3. Permisos

Puede haber varios administradores en el sistema de gestión web. Los administradores de diferentes niveles tienen diferentes permisos de administración. Puede asignar el permiso de administración de una página especificada a un administrador especificado. El usuario predeterminado del sistema es admin.

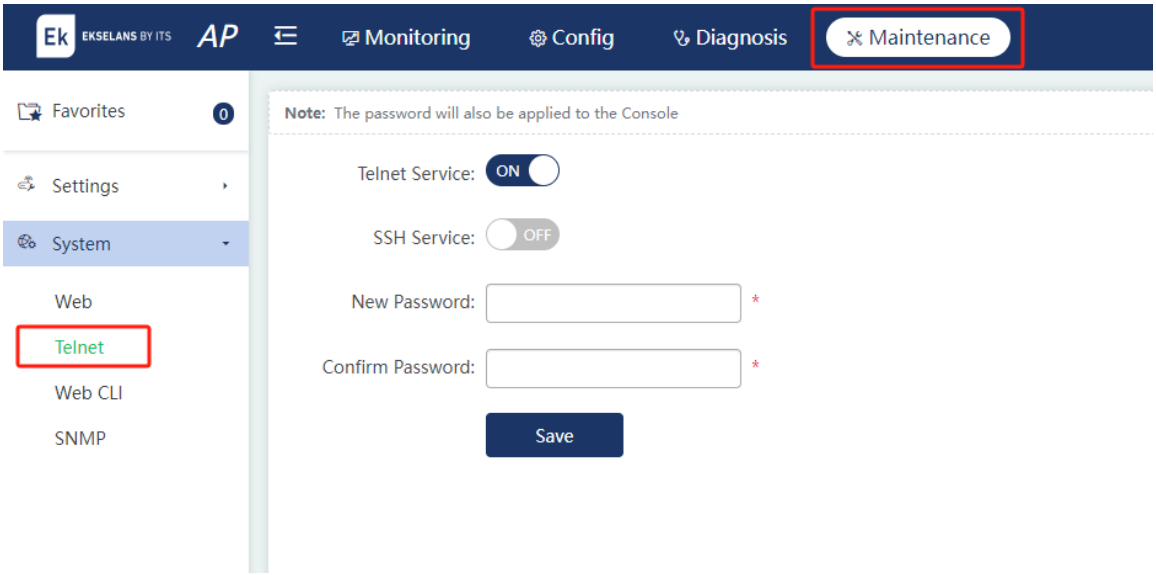
Haga clic en **Agregar administrador**. Establezca los campos para un administrador en la ventana emergente, incluidos el nombre de usuario, la contraseña y los permisos. Haga clic en **Guardar**.



7.2.2 Telnet

Seleccione **Mantenimiento** > **Sistema** > **Telnet**.

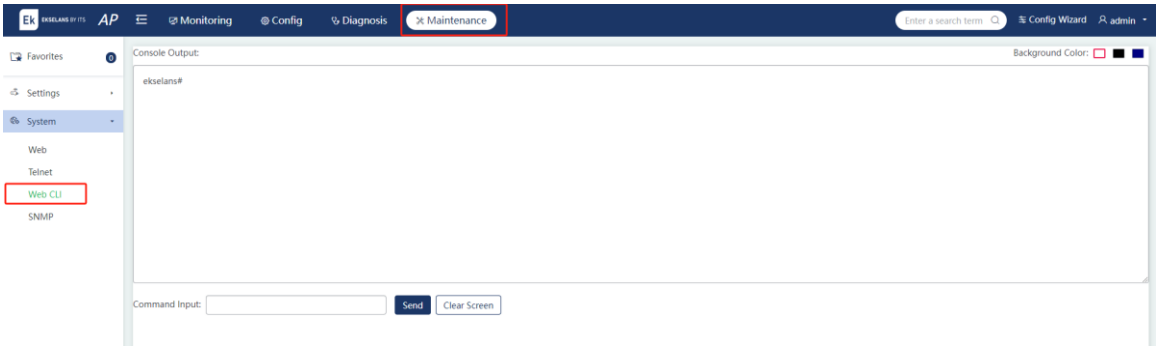
La función Telnet mejora la seguridad del sistema y garantiza un intercambio seguro de información. En la **página Telnet**, el **servicio Telnet** y el **servicio SSH** se pueden habilitar o deshabilitar, y se puede configurar la contraseña.



7.2.3 Web CLI

Elija **Mantenimiento** > **CLI web del sistema** >.

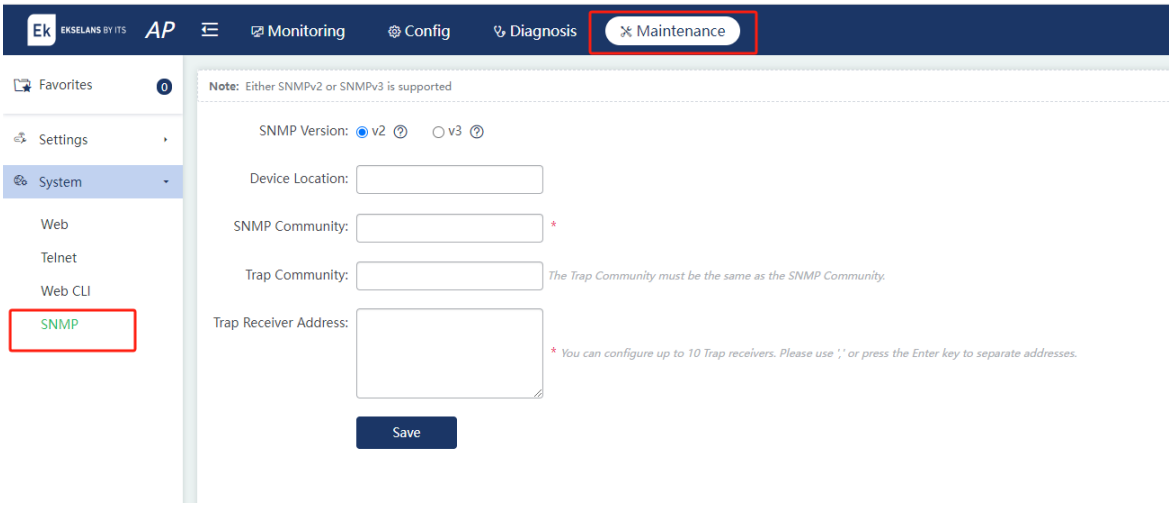
Los comandos CLI se pueden entregar a través de la CLI web.



7.2.4 SNMP

Seleccione **Mantenimiento** > **Sistema** > **SNMP.**

El protocolo simple de administración de red (SNMP) proporciona un método para recopilar información de administración de red de los dispositivos de la red. SNMP se puede utilizar para administrar numerosos dispositivos de red.


EKSELANS BY ITS
AP
Monitoring
Config
Diagnosis
Maintenance
Favorites
0
Settings
System
Web
Telnet
Web CLI
SNMP
Note: Either SNMPv2 or SNMPv3 is supported
SNMP Version: v2 v3
Device Location:
SNMP Community:
Trap Community:
The Trap Community must be the same as the SNMP Community.
Trap Receiver Address:
You can configure up to 10 Trap receivers. Please use ',' or press the Enter key to separate addresses.
Save