



EKSELANS BY ITS

MANUAL DE USUARIO

AX 3000

331019

Punto de Acceso WiFi 6 de interior

WiFi6 (802.11ax) 3000Mbps

Puerto de entrada PoE 1G

Puerto de enlace ascendente SFP 1G/2,5G

Entrada PoE / Entrada de corriente continua

(DC-IN)

Derechos de autor

Derechos de autor © 2024 Ekselans por ITS

Todos los derechos están reservados en este documento y en esta declaración.

Queda prohibida cualquier reproducción, extracción, copia de seguridad, modificación, transmisión, traducción o uso comercial de este documento o de cualquier parte de este documento, en cualquier forma o por cualquier medio, sin el consentimiento previo por escrito de Ekselans por parte de ITS.

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 símbolos utilizados en este documento se describen a continuación:

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

Este manual proporciona los pasos de instalación del dispositivo, la solución de problemas de hardware, las especificaciones técnicas del módulo y las especificaciones y pautas de uso para cables y conectores. Está destinado a los usuarios que tienen cierta experiencia en la instalación y el mantenimiento de hardware de red. Al mismo tiempo, se supone que los usuarios ya están familiarizados con los términos y conceptos relacionados.

1 Descripción general del producto

El AX 3000 es un punto de acceso de doble banda y doble radio que cumple con el estándar IEEE 802.11ax. El AX 3000 proporciona 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. Diseñado para implementaciones flexibles en el campo de la educación, el gobierno, las finanzas y los negocios, el AX 3000 AP ofrece un puerto combinado.

1.1 Apariencia

El AX 3000 proporciona dos conectores de radiofrecuencia (RF), un puerto Ethernet 10/100/1000 BASE-T, un puerto SFP 2.5G, un puerto de consola y un enchufe de alimentación de CC. El AP admite fuente de alimentación PoE o CC.

Figura 1-1 Apariencia



Figura 1-2 Panel frontal



Tabla 1-1 Panel frontal

No.	Artículo	Descripción
1	LED	Indica el estado de funcionamiento del dispositivo.

Figura 1-3 Perfil

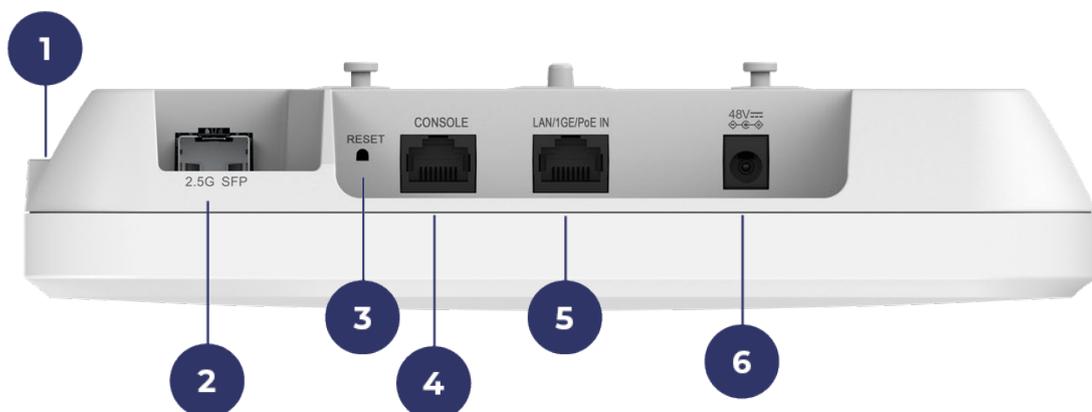


Tabla 1-2 Perfil

No.	Botón y puerto	Descripción
1	Orificio de bloqueo antirrobo	Conéctelo a la cerradura antirrobo.
2	Puerto SFP 2.5G	El puerto SFP de enlace ascendente para la transmisión de datos de servicio.
3	Botón de reinicio	Reinicie el dispositivo o restaure el dispositivo a la configuración de fábrica.
4	Puerto de consola	Conéctese al dispositivo que se administra con el cable serie.
5	Puerto Ethernet 1000 BASE-T	El puerto Ethernet adaptable de enlace ascendente para la transmisión de datos de servicio. Admite fuente de alimentación PoE estándar IEEE 802.3af.
6	Enchufe de alimentación de CC	Conéctelo al adaptador de alimentación de CC para suministrar energía al AP.

Nota

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

1.2 Contenido del paquete

Tabla 1-3 Contenido del paquete

Artículo	Cantidad
Punto de acceso AX 3000	1
Soporte de montaje	1
Pared Ancla	2
Tornillos de cabeza plana Phillips M4 x 20	4
Tarjeta de garantía	1
Guía de instalación	1

1.3 Especificaciones técnicas

1.3.1 Tamaño y peso

Tabla 1-4 Tamaño y peso

Artículo	Parámetro
Dimensiones de la unidad principal (ancho x profundo x alto)	220 mm x 220 mm x 49 mm (8,66 pulgadas x 8,66 pulgadas x 1,93 pulgadas)
Peso	Unidad principal: 0,6 kg (1,33 libras) Soporte: 0,2 kg (0,44 libras)
Montura	Capacidad de montaje en techo/pared
Cerradura antirrobo	Cerradura Kensington Tornillo de seguridad
Dimensiones del soporte (ancho x profundo x alto)	120 mm x 120 mm x 8 mm (4,72 pulgadas x 4,72 pulgadas x 0,31 pulgadas)
Patrón de orificios de montaje	53 mm (2,09 pulg.)
Diámetro del orificio de montaje	6,5 mm (0,26 pulg.)

1.3.2 RF

Tabla 1-5 RF

Artículo	Parámetro
Diseño de RF	2 conectores RF, 2 conectores RF inalámbricos Radio1: 2,4 GHz, 2x2 MIMO (2 flujos espaciales) Radio2: 5 GHz, 2x2 MIMO (2 flujos espaciales) Doble banda combinada: 4 flujos espaciales

Frecuencia de funcionamiento	Radio1: 802.11b/g/n/ax, 2,4 GHz-2,4835 GHz, HE40 Radio2: 802.11a/n/ac/ax, 5,150 GHz-5,350 GHz, HE80/HE160 802.11a/n/ac, 5,470 GHz-5,725 GHz, 5,725 GHz-5,850 GHz, HE80 (se aplican restricciones específicas de cada país)
Velocidad de datos máx.	Radio1: 2,4 GHz, 574 Mbps Radio2: 5 GHz, 2.402 Gbps Doble banda combinada: 2,976 Gbps
Tipo de antena	Antena inteligente incorporada
Ganancia de antena	2,4 GHz: 3 dBi 5 GHz: 3 dBi
Máx. Potencia de transmisión	20 dBm (se aplican restricciones específicas de cada país)
Ajuste de la potencia de transmisión	Configurable en incrementos de 1 dBm
Modulación	OFDM: BPSK@6/9 Mbps, QPSK@12/18 Mbps, 16 QAM@24Mbps, 64 QAM@48/54 Mbps DSSS: DBPSK@1Mbps, DQPSK@2Mbps y CCK@5,5/11 Mbps MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM y 1024QAM AMDFO
Sensibilidad de recepción	11b: -96 dBm (1 Mbps), -93 dBm (5 Mbps), -89 dBm (11 Mbps) 11a/g: -91 dBm (6 Mbps), -85 dBm (24 Mbps), -80 dBm (36 Mbps), -74 dBm (54 Mbps) 11n: -90dBm@MCS0, -70dBm@MCS7, -89dBm@MCS8, -68dBm@MCS15 11ac: HT20: -88 dBm (MCS0), -63 dBm (MCS9) 11ac: HT40: -85 dBm (MCS0), -60 dBm (MCS9) 11ac: HT80: -82 dBm (MCS0), -57 dBm (MCS9) 11ax: HE80: -82dBm (MCS0), -57dBm (MCS9), -52dBm (MCS11) 11ax: 160MHz: -77dBm (MCS0), -50dBm (MCS11)

1.3.3 Puertos

Tabla 1-6 Puertos

Artículo	Descripción
Bluetooth	Bluetooth 5.1

Puerto de servicio fijo	Un puerto Ethernet 10/100/1000 Base-T (PoE compatible con IEEE 802.3af) Un puerto SFP 2.5G (compatibilidad con SFP 1GE)
Puerto de administración fijo	Un puerto de consola RJ45
GPS	No se admite
LED	Un LED de estado del sistema
Botón	Un botón de reinicio

1.3.4 Fuente de alimentación

Tabla 1-7 Fuente de alimentación

Artículo	Descripción
Fuente de alimentación	1. Adaptador de corriente continua: 48 V/0,6 A (opcional. Por favor, refiérase a Fuente de alimentación para obtener más detalles). 2. PoE: Cumple con IEEE 802.3af
Consumo máx. de energía	12,95 W

Cautela

El adaptador de corriente es opcional. Si necesita utilizar un adaptador de alimentación de CC para la fuente de alimentación, compre un adaptador que cumpla con los requisitos de seguridad correspondientes.

1.3.5 Medio ambiente y confiabilidad

Tabla 1-8 Medio ambiente y confiabilidad

Artículo	Descripción
Temperatura	En funcionamiento: -10 °C a +50 °C (14 °F a 122 °F) Almacenamiento: -40 °C a +70 °C (-40 °F a +158 °F) A una altura entre 3000 m (9842.52 pies) y 5000 m (16404.20 pies) sobre el nivel del mar, cada vez que la altitud aumenta 166 m (546 pies), la temperatura máxima disminuye 1 °C (1.8 °F).
Humedad	En funcionamiento: 5 % a 95 % (HR), sin condensación Almacenamiento: 5% a 95% (HR), sin condensación)

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 y EN 62368-1
-------------------------------	---

1.4 LEDs y botón

i Nota

- La descripción del estado del LED se aplica tanto a Fit AP como a Fat AP, a menos que se indique lo contrario.

Tabla 1-9 Estado del LED del sistema

Color	Frecuencia	Descripción del estado
Apagado	N/A	El AP NO está recibiendo energía, o el AP está recibiendo energía, pero el LED está deshabilitado por software.
Verde sólido	N/A	La inicialización del sistema del programa está en curso.
Rojo sólido	N/A	El sistema está en funcionamiento normal, pero el puerto de servicio de enlace ascendente del AP está inactivo.
Parpadeo lento en rojo	Encendido durante 3 segundos y apagado durante 1 segundo	En el modo Ajustar AP, se agota el tiempo de espera del establecimiento de un túnel CAPWAP entre el AP y la CA.
Parpadeo rápido en azul	Encendido durante 0,2 s y apagado durante 0,2 s	En el modo Fit AP o Cloud AP, el AP está en proceso de actualización de software
Azul sólido	N/A	El sistema y el AP están en funcionamiento normal, pero no hay clientes inalámbricos en línea.
Azul parpadeante	Encendido por 1 s y apagado por 1 s	El sistema y el AP están en funcionamiento normal, y al menos un cliente inalámbrico está actualmente en línea.
Parpadeo rápido en rojo	Encendido durante 0,2 s y apagado durante 0,2 s	En el modo Fit AP, la función de ubicación LED está habilitada para ubicar un AP específico.

Tabla 1-10 Botón de reinicio

Botón de reinicio	Mantenga presionado durante menos de 2 segundos	Reinicie el dispositivo.
	Mantenga presionado durante más de 3 segundos	Restaurar la configuración predeterminada.

1.5 Módulos SFP

El puerto SFP 2.5G del AP admite enlaces de cobre y fibra. La velocidad de negociación puede variar según el tipo de módulo SFP y las velocidades a ambos lados del enlace. Consulte la Tabla 1-11 y la Tabla 1-12.

Tabla 1-11 Velocidad de negociación cuando se conecta con el puerto SFP en el dispositivo del mismo nivel

Velocidad del puerto AP SFP	Velocidad del módulo de fibra SFP	Velocidad de negociación		
		1 Gbps	1 Gbps/10 Gbps/automático	1 Gbps/2,5 Gbps/10 Gbps/automático
1 Gbps	3 Gbps	1 Gbps	1 Gbps	1 Gbps
1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps
2,5 Gbps	3 Gbps	No se admite	No se admite	2,5 Gbps
2,5 Gbps	1 Gbps	No se admite	No se admite	1 Gbps

Tabla 1-12 Velocidad de negociación cuando se conecta con el puerto de cobre en el dispositivo del mismo nivel

Velocidad del puerto AP SFP	Velocidad del módulo de cobre SFP	Velocidad de negociación		
		1 Gbps	1 Gbps/10 Gbps/automático	1 Gbps/2,5 Gbps/10 Gbps/automático
1 Gbps	2,5 Gbps	No se admite	No se admite	No se admite
1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps
2,5 Gbps	2,5 Gbps	No se admite	No se admite	2,5 Gbps
2,5 Gbps	1 Gbps	No se admite	No se admite	No se admite

Cautela

- El puerto SFP 2.5G del AP no admite la negociación de velocidad. Cuando utiliza el módulo transceptor, la velocidad del AP, el módulo y el puerto del dispositivo par deben ser los mismos.
- El puerto SFP y el puerto de cobre se pueden multiplexar como un puerto combinado. Si dos puertos están conectados con cables al mismo tiempo, el AP seleccionará preferentemente el puerto SFP para la transmisión de datos (el puerto de cobre se desactiva automáticamente). Cuando el cable del puerto SFP está desenchufado, el puerto de cobre se habilita automáticamente.

2 Preparación para la instalación

2.1 Precauciones de seguridad

i 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 AP a altas temperaturas, polvos o gases nocivos.
- No instale el AP en un entorno inflamable o explosivo.
- Mantenga el AP alejado de fuentes EMI, como grandes estaciones de radar, estaciones de radio y subestaciones.
- No someta el AP 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 y las características del equipo de comunicaciones, y consideraciones como el clima, la hidrología, la geología, los terremotos, la energía eléctrica y el transporte.
- Mantenga el AP 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 dispositivo 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, verifique si la fuente de alimentación está conectada a tierra, si la conexión a tierra es confiable y si la conexión a tierra está mojada.
 - Obtenga información sobre la posición del interruptor de alimentación de emergencia interior antes de la instalación. Corte el interruptor de alimentación en caso de accidentes.
 - Revise el dispositivo cuidadosamente 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 dispositivo alejado de dispositivos de conexión a tierra o de protección contra rayos para equipos eléctricos.
 - Mantenga el dispositivo alejado de estaciones de radio, estaciones de radar, dispositivos de alta frecuencia y alta corriente y hornos microondas.

2.1.4 Seguridad de almacenamiento

Para garantizar el funcionamiento normal del dispositivo después del almacenamiento, consulte los requisitos de temperatura/humedad de almacenamiento en las especificaciones para el entorno de almacenamiento.

⚠ Cautela

Si el dispositivo ha estado almacenado durante más de 18 meses, el dispositivo debe estar encendido y funcionar durante 24 horas sin interrupción para completar la activación del dispositivo.

2.2 Requisitos del entorno de instalación

Instale el dispositivo en interiores para garantizar su funcionamiento normal y una vida útil prolongada.

El sitio de instalación debe cumplir con los siguientes requisitos.

2.2.1 Requisitos de los rodamientos

Evalúe la capacidad de carga del sitio de instalación en función del peso real del dispositivo y sus accesorios (por ejemplo, el soporte y los módulos de fuente de alimentación) y asegúrese de que el sitio de instalación cumpla con los requisitos de rodamiento.

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 cm (15,75 pulgadas) alrededor del dispositivo para garantizar una refrigeración y ventilación adecuadas.

2.2.4 Requisitos de temperatura/humedad

Para garantizar el funcionamiento normal y la vida útil prolongada del dispositivo, mantenga una temperatura y humedad adecuadas en la sala de equipos.

La sala de equipos con una temperatura y humedad demasiado altas o demasiado bajas durante un período prolongado puede dañar el dispositivo.

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

i 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 una gran amenaza para el dispositivo. El polvo interior adquiere una carga eléctrica estática positiva o negativa al caer sobre el dispositivo, lo que provoca un mal contacto de la junta metálica. Dicha adhesión 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 Tabla 2-1 describe 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 $\leq 0,5 \mu\text{m}$)	Partículas/m ³	$\leq 1.4 \times 10^7$
Partículas de polvo ($0,5 \mu\text{m} \leq$ diámetro $\leq 1 \mu\text{m}$)	Partículas/m ³	$\leq 7 \times 10^5$
Partículas de polvo ($1 \mu\text{m} \leq$ diámetro $\leq 3 \mu\text{m}$)	Partículas/m ³	$\leq 2.4 \times 10^5$

Partículas de polvo (3 µm ≤ diámetro ≤ 1 µm)	Partículas/m ³	≤1.3×10 ⁵
--	---------------------------	----------------------

Además del polvo, la sal, el ácido y el sulfuro en el aire de la sala de equipos deben cumplir con requisitos estrictos. Estas sustancias nocivas acelerarán la corrosión del metal y el envejecimiento de los componentes. Por lo tanto, la sala de equipos debe estar debidamente protegida contra la intrusión de gases nocivos, como dióxido de azufre, sulfuro de hidrógeno, dióxido de nitrógeno y cloro gaseoso. En la Tabla 2-2 se enumeran los valores límite para los gases nocivos.

Table 2-2 Requisitos para los gases

Gas	Promedio (mg/m ³)	Máximo (mg/m ³)
Dióxido de azufre (SO ₂)	0.2	1.5
Sulfuro de hidrógeno (HS)	0.006	0.03
Dióxido de nitrógeno (NO ₂)	0.04	0.15
Gas amoníaco (NH ₃)	0.05	0.15
Cloro gaseoso (Cl ₂)	0.01	0.3

Nota

El promedio se refiere al valor promedio de los gases nocivos medido en una semana. **El máximo** se refiere al límite superior de gases nocivos medido en una semana, y el valor máximo dura 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 dispositivo alejado del equipo de puesta a tierra o del equipo de conexión a tierra y rayos del dispositivo de alimentación tanto como sea posible.
- Mantenga el dispositivo 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 dispositivo puede proteger contra la caída de rayos. Como dispositivo eléctrico, aún puede dañarse por fuertes rayos. Se deben tomar las siguientes medidas de protección contra el rayo:

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

2.2.8 Requisitos del sitio de instalación

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

- Se debe reservar suficiente espacio en las entradas y salidas de aire del dispositivo para garantizar la disipación del calor.
- El lugar de instalación debe estar adecuadamente ventilado.
- El sitio de instalación es lo suficientemente resistente como para soportar el peso del dispositivo y sus accesorios.

2.3 Herramientas

Table 2-3 Herramientas

Herramientas comunes	Destornilladores Phillips, alambres, cable Ethernet, pernos de fijación, alicates diagonales y correas de encuadernación Phillips
Herramientas especiales	Guantes antiestáticos, pelacables, alicates de engarzado, alicates de engarzado de conector de cristal y cortador de alambre
Metro	Multímetro y comprobador de tasa de error de bits (BERT)
Dispositivos relevantes	PC, pantalla y teclado

i Nota

El dispositivo se entrega sin un kit de herramientas. El kit de herramientas y los cables son suministrados por el cliente.

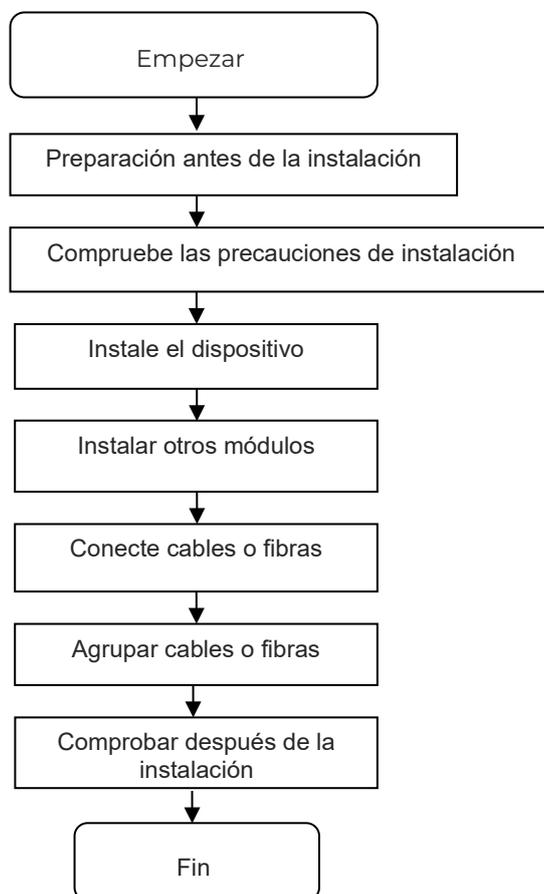
3 Instalación del punto de acceso

El AX 3000 AP debe fijarse e instalarse en interiores.

⚠ 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



3.2 Antes de empezar

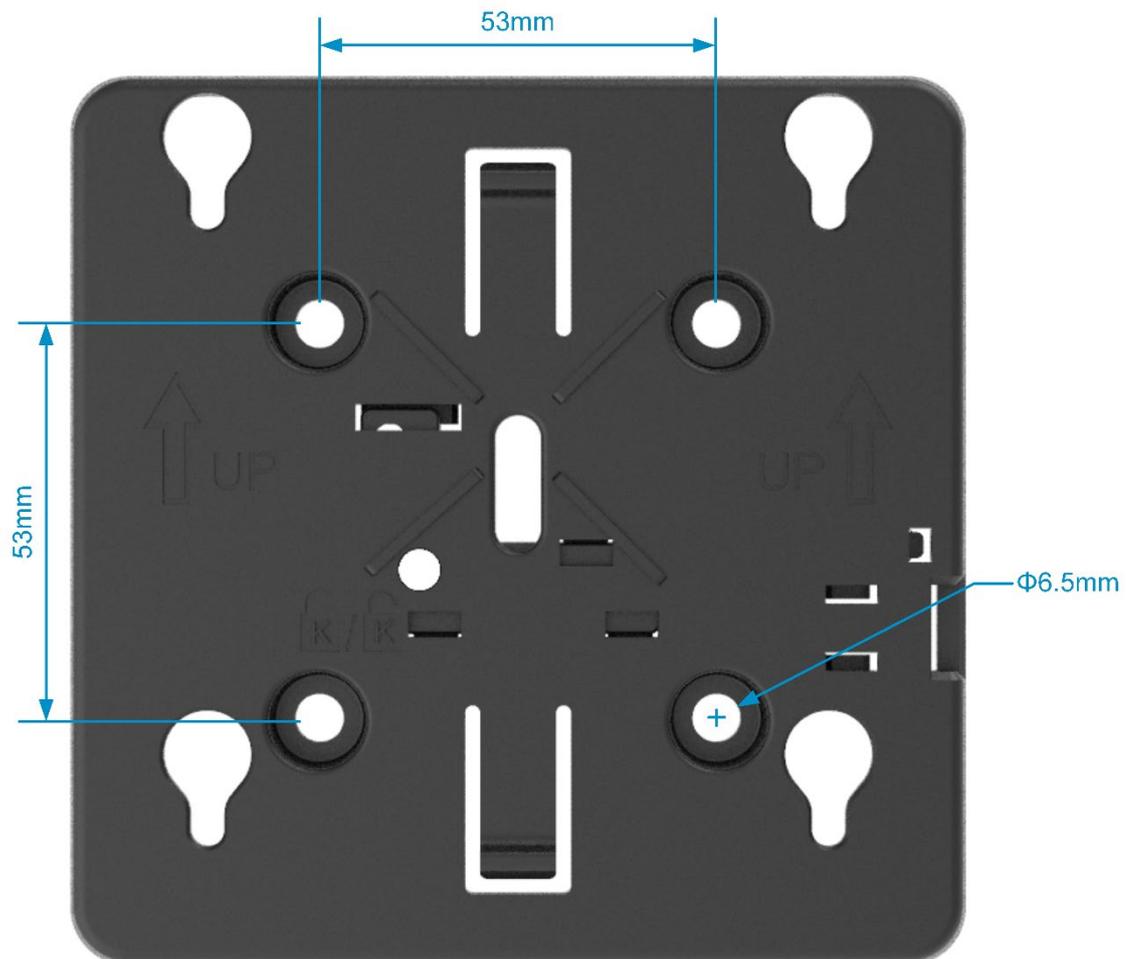
Antes de instalar el dispositivo, compruebe que todas las partes del contenido del paquete estén allí y asegúrese de que:

- La posición de instalación proporciona suficiente espacio para la disipación del calor.
- La posición de instalación cumple con los requisitos de temperatura y humedad del

dispositivo.

- La fuente de alimentación y la corriente requerida están disponibles en la posición de instalación.
- El cable Ethernet se ha desplegado en la posición de instalación.
- Los módulos de alimentación seleccionados cumplen con los requisitos de alimentación del sistema.
- La posición del interruptor de alimentación de emergencia interior se aprende antes de la instalación. El interruptor de encendido se corta en caso de accidentes.
- Para AP montado en el techo o en la pared, el tamaño del soporte de montaje, el patrón del orificio de montaje y el diámetro deben cumplir con los requisitos de **Tabla 14 Tamaño y peso**, como se muestra en la Figura 3-1.

Figura 3-1 Soporte de montaje



3.3 Precauciones

Para evitar daños en el AP, observe las siguientes precauciones de seguridad:

- No encienda el dispositivo durante la instalación.
- Instale el dispositivo en un lugar bien ventilado.
- No exponga el dispositivo a altas temperaturas.

- Manténgase alejado de cables de alto voltaje.
- Instale el dispositivo en interiores.
- No exponga el dispositivo en una tormenta eléctrica o un campo eléctrico fuerte.
- Mantenga el dispositivo limpio y libre de polvo.
- Desconecte el dispositivo antes de limpiarlo.
- 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

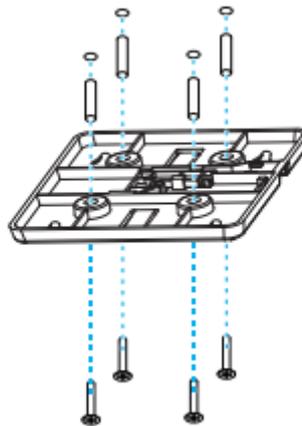
i Nota

- **Se recomienda instalar el dispositivo donde pueda obtener la cobertura óptima.**
- En el área interior, la cobertura de la señal del dispositivo montado en el techo es mayor que la del dispositivo montado en la pared. Elija primero el método de montaje en el techo.

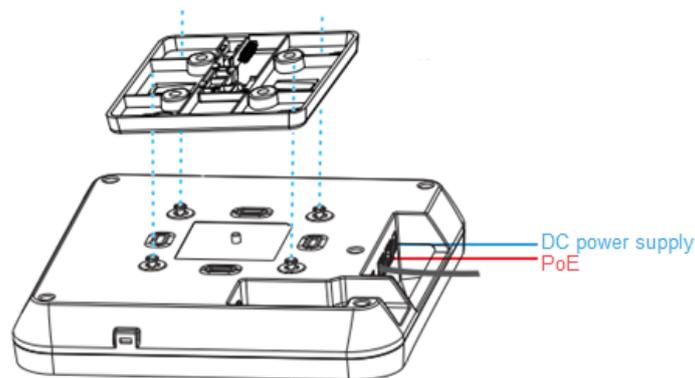
3.4.1 Montaje en techo

- (1) Taladre cuatro agujeros de 6,5 mm (0,26 pulgadas) de diámetro en el techo, a 53 mm (2,09 pulgadas) de distancia. Golpee los anclajes de pared en los orificios y atornille a través del soporte de montaje en los anclajes para asegurar el soporte.

Figura 3-2 Fijación del soporte de montaje al techo

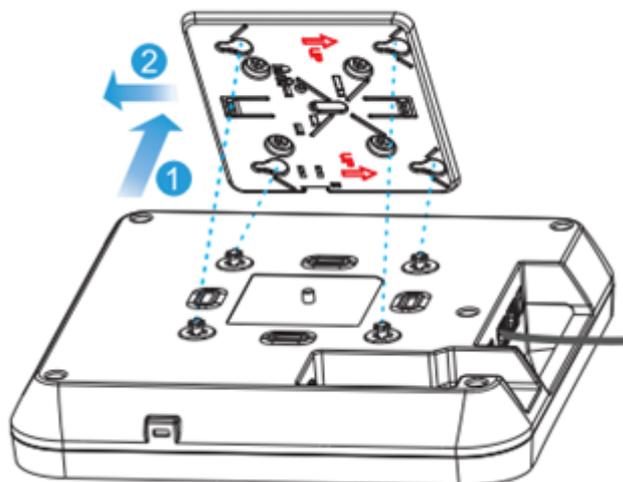


- (2) Alinee los pies cuadrados en la parte posterior del AP con los orificios de montaje en el soporte.

Figura 3-3 Alinear los pies cuadrados con los orificios de montaje**⚠ Cautela**

Instale los cables Ethernet antes de montar el AP en el soporte.

- (3) Deslice el AP sobre el soporte en la dirección opuesta a la flecha en el soporte de montaje hasta que encaje en su lugar.

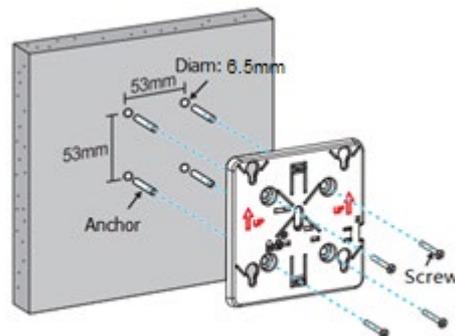
Figura 3-4 Montaje del AP en el soporte**⚠ Cautela**

- El AP se puede instalar en cualquiera de las cuatro direcciones en el soporte de montaje, dependiendo de cómo enrute el cable Ethernet.
- Los pies cuadrados deben caber fácilmente en las ranuras de montaje. No empuje a la fuerza el AP en las ranuras.
- Después de la instalación, verifique que el AP esté bien sujeto.

3.4.2 Montaje en pared

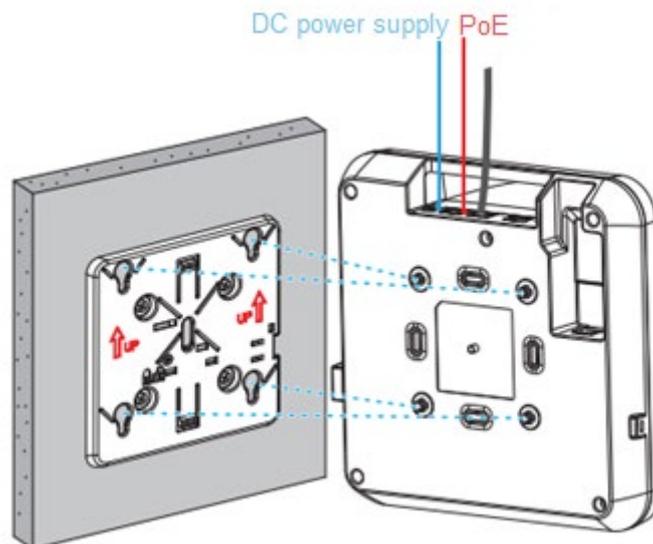
- (1) Taladre cuatro orificios de 6,5 mm (0,26 pulg.) de diámetro en la pared y a 53 mm (2,09 pulg.) de distancia, con la flecha del soporte de montaje hacia arriba. Golpee los anclajes de pared en los orificios y atornille a través del soporte de montaje en los anclajes para asegurar el soporte.

Figura 3-5 Fijación del soporte de montaje a la pared



- (2) Alinee los pies cuadrados en la parte posterior del AP con los orificios de montaje en el soporte.

Figura 3-6 Alinear los pies cuadrados con los orificios de montaje



⚠ Cautela

Instale los cables Ethernet antes de montar el AP en el soporte.

- (3) Deslice el AP en los orificios en la dirección opuesta a las flechas del soporte de montaje hasta que encaje en su lugar.

⚠ Cautela

- Cuando monte el AP en la pared, mantenga el logotipo de EK apuntando hacia arriba.
- Los pies cuadrados deben caber fácilmente en las ranuras de montaje. No empuje a la fuerza el AP en las ranuras.
- Después de la instalación, verifique que el AP esté bien sujeto.

3.4.3 Eliminación del punto de acceso

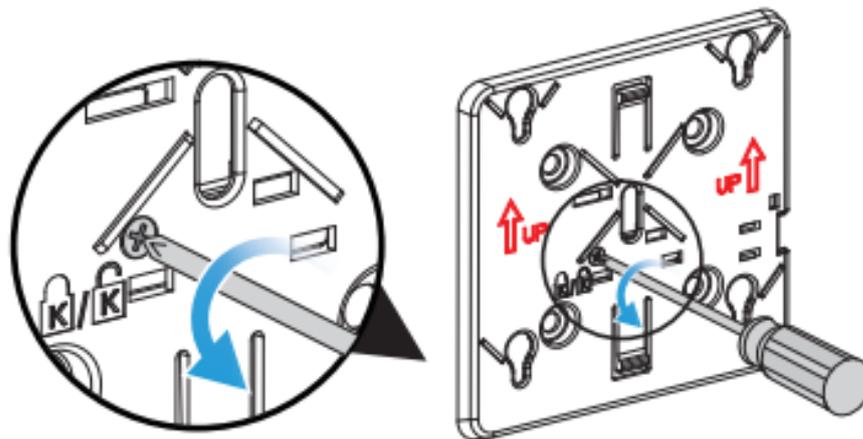
- (1) Si el AP está instalado en el techo, sostenga el AP con las manos y deslícelo hacia los lados y lejos del soporte en la dirección del puerto LAN.
- (2) Si el AP está instalado en la pared, sostenga el AP con las manos y empújelo hacia arriba y lejos del soporte en la dirección del puerto LAN.

3.5 Instalación de otros módulos

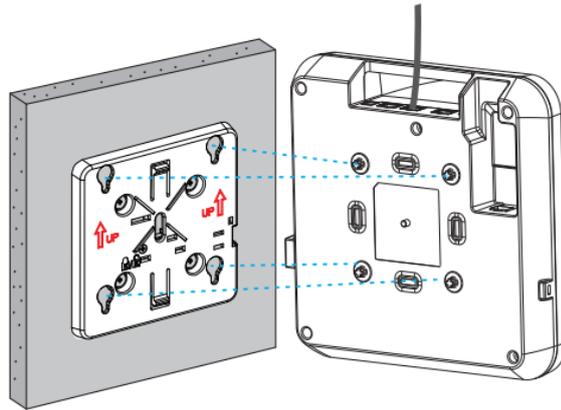
3.5.1 Protección del punto de acceso

- (1) Afloje el tornillo del soporte de montaje y enganche el tornillo de seguridad.

Figura 3-7 Acoplar el tornillo de seguridad



- (2) Alinee los pies cuadrados en la parte posterior del AP sobre los orificios de montaje en el soporte, deslice el AP en la dirección opuesta a las flechas en el soporte de montaje hasta que encaje en su lugar.

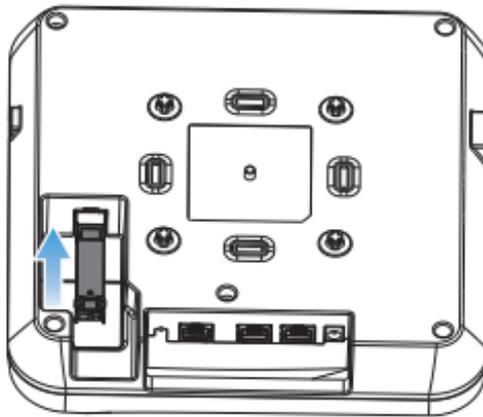
Figura 3-8 Montaje del AP en el soporte

⚠ Cautela

Instale los cables Ethernet antes de montar el AP en el soporte.

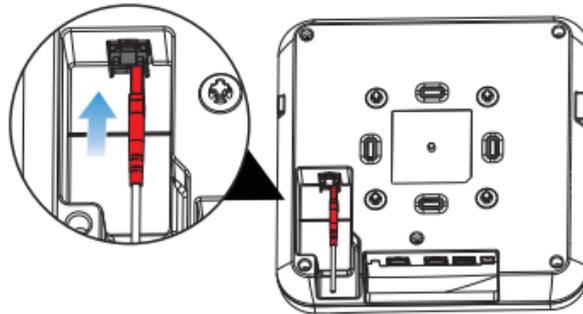
3.5.2 Instalación del módulo SFP

- (1) Inserte el módulo SFP.

Figura 3-9 Inserción del módulo SFP

- (2) Conecte la fibra.

Figura 3-10 Conexión de la fibra



3.6 Cables de conexión

Conecte UTP/STP al puerto LAN/PoE del AP. Consulte [Connectors and Media](#) para conocer el cableado compatible de pares trenzados.

⚠ Cautela

De forma predeterminada, la velocidad en baudios se establece en 9600, el bit de datos 8, la paridad ninguno, los bits de parada 1 y el control de flujo ninguno en el puerto de consola del AP. El puerto de la consola se utiliza solo cuando desea configurar el AP manualmente.

3.7 Agrupación de cables

3.7.1 Precauciones

- Asegúrese de que los haces de cables estén limpios y ordenados.
- Doble los pares trenzados de forma natural o a un radio grande cerca del conector.
- No apriete demasiado el haz de cables, ya que puede reducir la vida útil y el rendimiento del cable.

3.7.2 Pasos de agrupación

- Agrupe los cables UTP/STP de bajada y enróselos al puerto LAN/PoE.
- Conecte los cables en la bandeja de cables del bastidor.
- Extienda los cables por debajo del AP y páselos en línea recta.

3.8 Comprobación después de la instalación

3.8.1 Comprobación del punto de acceso

- Asegúrese de que la fuente de alimentación externa coincida con el AP.
- Asegúrese de que el dispositivo esté completamente fijo y no se mueva.

3.8.2 Comprobación de la conexión del cable

- Asegúrese de que el cable UTP/STP coincida con el tipo de interfaz.
- Asegúrese de que los cables estén agrupados correctamente.

3.8.3 Comprobación de la fuente de alimentación

- Asegúrese de que todos los puertos de alimentación estén conectados correctamente y cumplan con los requisitos de seguridad.
- Asegúrese de que el AP esté operativo después del encendido.

4 Verificación del estado de funcionamiento

4.1 Configuración del entorno

Utilice un adaptador de corriente o PoE para alimentar el AP.

Configuración del entorno

- Verifique que el AP esté conectado correctamente a la fuente de alimentación.
- Conecte el AP a una CA a través de un cable de par trenzado.
- Cuando el AP esté conectado a una PC, verifique que la PC y el switch PoE estén correctamente conectados a tierra.

4.2 Encendido del AP

4.2.1 Comprobación del entorno antes del encendido

- Verifique que la fuente de alimentación esté conectada correctamente.
- Verifique que el voltaje de entrada coincida con la especificación del AP.

4.2.2 Comprobación del entorno después del encendido

Después del encendido, se recomienda verificar lo siguiente para garantizar el funcionamiento normal del AP.

- Compruebe si hay algún mensaje impreso en la interfaz de configuración basada en web del dispositivo.
- Compruebe si el LED funciona normalmente.

5 Monitoreo y Mantenimiento

5.1 Monitorización

5.1.1 LED

Puede observar el LED para monitorear el AP en funcionamiento.

5.1.2 Comandos CLI

Puede ejecutar comandos relacionados en la interfaz de línea de comandos (CLI) del dispositivo para monitorear de forma remota las configuraciones y el estado del AP.

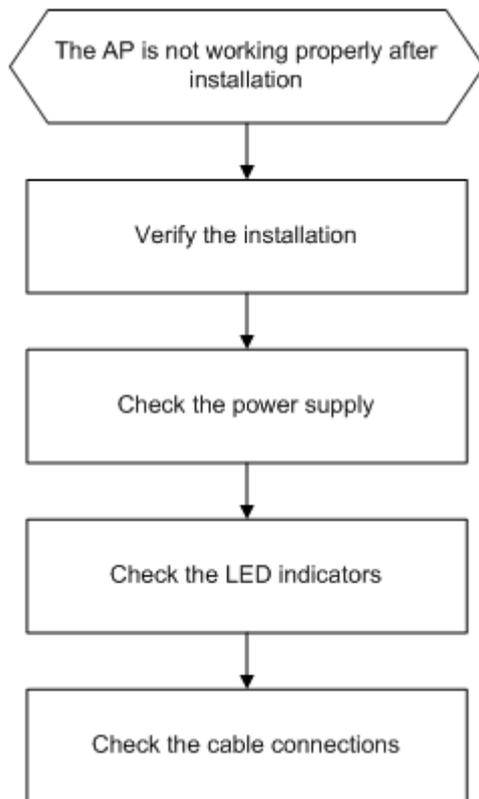
i Nota

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 AP funciona como un AP Fat, puede iniciar sesión en el AP de forma remota para el mantenimiento.
- Si el AP funciona como un AP de ajuste, puede utilizar AC para administrar y mantener el AP de forma centralizada.

6 Solución de problemas



6.1 Fallas comunes

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

Verifique que el dispositivo en el otro extremo del cable Ethernet funcione correctamente. Y luego verifique que el cable Ethernet sea capaz de proporcionar la velocidad de datos requerida y esté conectado correctamente.

6.1.2 El LED está apagado durante mucho tiempo

- Si utiliza una fuente de alimentación PoE, compruebe que la fuente de alimentación es compatible con IEEE 802.11af y, a continuación, compruebe que el cable está conectado correctamente.
- Si utiliza un adaptador de corriente, compruebe que el adaptador de corriente esté conectado a una toma de corriente activa y, a continuación, compruebe que el adaptador de corriente funciona correctamente.

6.1.3 El LED permanece en rojo fijo durante mucho tiempo

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

6.1.4 El LED permanece verde fijo durante mucho tiempo

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

6.1.5 El LED permanece parpadeando rápidamente en azul durante mucho tiempo (ajuste del modo AP)

A veces, el AP realiza una actualización de firmware después del encendido. Durante este período, el LED permanece parpadeando rápidamente en azul y no se vuelve fijo hasta que se completa la actualización. **Nota:** No enchufe ni desconecte el cable de alimentación cuando el LED de estado esté parpadeando, ya que la actualización del firmware tarda en actualizarse. Si el parpadeo persiste durante diez minutos, indica que el dispositivo no puede completar la actualización del firmware y está defectuoso.

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

Después de que se inicia el sistema y el LED no se vuelve azul fijo o parpadea en azul, esto puede deberse a que el AP no ha establecido una conexión CAPWAP adecuada con la CA. Verifique que la CA esté funcionando y configurada correctamente.

6.1.7 El cliente no puede encontrar la red inalámbrica

- (1) Verifique que el dispositivo esté encendido correctamente.
- (2) Verifique que el puerto Ethernet esté conectado correctamente.
- (3) Verifique que el AP esté configurado correctamente.
- (4) Ajuste la distancia entre el cliente y el AP acercando el dispositivo cliente al AP.

7 Apéndice

7.1 Conectores y medios

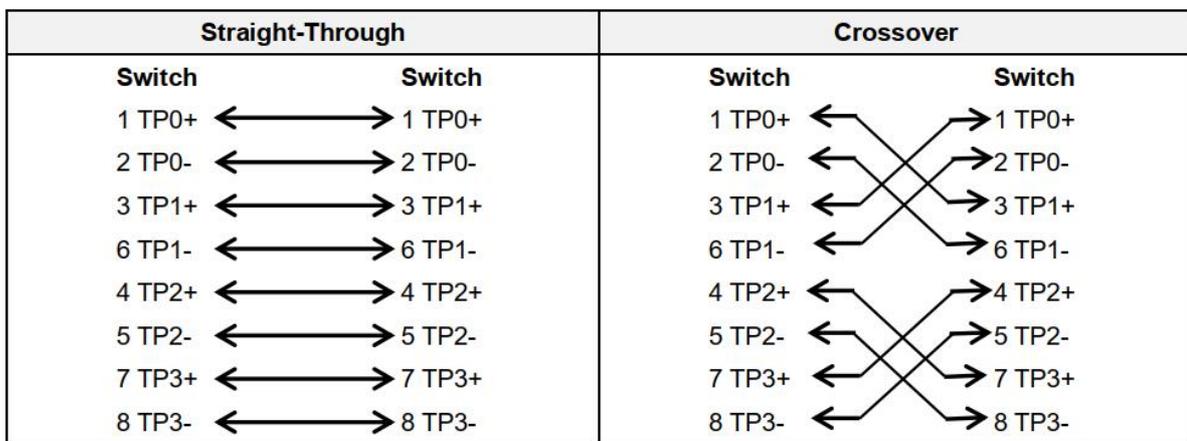
1000BASE-T/100BASE-TX/10BASE-T

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

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

1000BASE-T requiere que los cuatro pares de cables estén conectados para la transmisión de datos, como se muestra en **Figura 7-1**.

Figura 7-1 Conexión 1000BASE-T



10BASE-T utiliza UTP/STP de 100 ohmios de categoría 3, 4, 5 y 1000BASE-T utiliza UTP/STP de 100 ohmios de categoría 5 para las conexiones. Ambos soportan una longitud máxima de 100 metros.

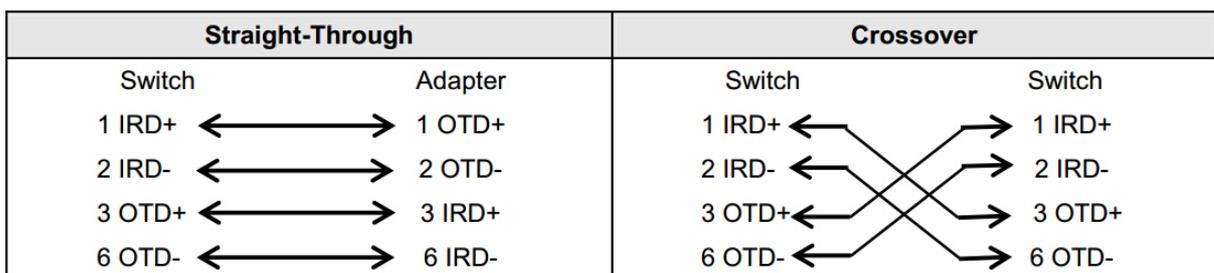
Figura 7-2 muestra las asignaciones de pines 100BASE-TX/10BASE-T.

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

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

Figura 7-3 muestra el cableado de cables directos y cruzados para 100BASE-TX/10BASE-T.

Figura 7-3 Conexión 100BASE-TX/10BASE-T



7.2 Módulos Mini-GBIC

Utilice los módulos SFP (Mini-GBIC) adecuados según los tipos de puerto. Puede seleccionar el módulo que mejor se adapte a sus necesidades específicas. Los siguientes modelos y especificaciones técnicas de algunos módulos SFP se enumeran para su referencia.

Tabla 7-1 Modelos y especificaciones técnicas del módulo SFP

Longitud de onda (nm)	Tipo de medio	Soport a DDM (Sí/No)	Intensidad de la luz transmitida (dBm)		Intensidad de la luz recibida (dBm)	
			min	máximo	min	máximo
1310Tx/1550Rx	Fibra monomodo	No	-9	-3	-	-18

Tabla 7-2 Especificaciones de cableado del módulo SFP

Puerto	Tipo de medio	Tamaño del núcleo (µm)	Distancia de cableado
LC	Fibra monomodo	9/125	0.3 km

⚠ Cautela

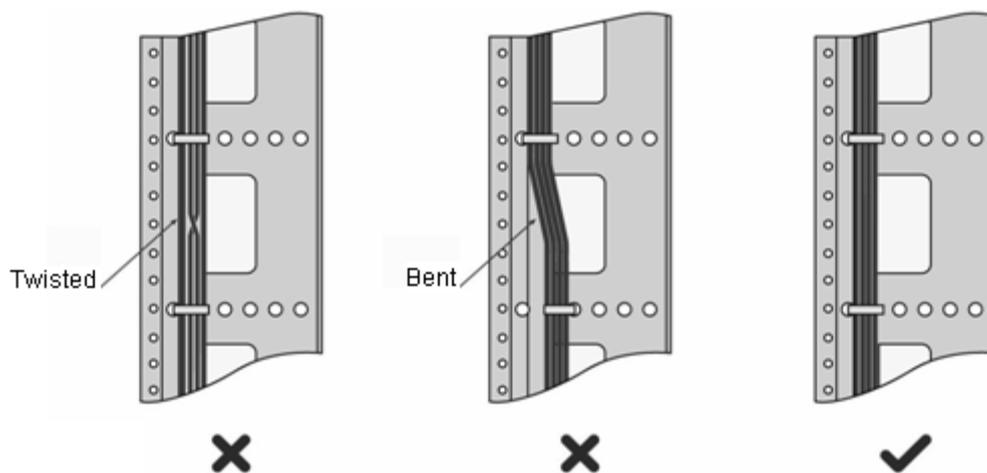
- Para el módulo de fibra con una distancia de transmisión superior a 40 km y más, se debe agregar un atenuador óptico en línea en el enlace para evitar la sobrecarga del receptor óptico cuando se utilizan fibras ópticas monomodo cortas.
- Los módulos de fibra generan láser. No mire fijamente a la fuente de luz.
- Para mantener limpios los módulos de fibra, use tapas antipolvo cuando los módulos no estén conectados con fibras.

7.3 Recomendaciones de 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 deben colocarse hacia arriba o hacia abajo al lado del gabinete cerca de la ubicación del gabinete de distribución de energía de CC, la toma de corriente de CA o la caja de protección contra rayos.

- Radio de curvatura de cable mínimo requerido
 - El radio de curvatura mínimo de un cable de alimentación, de comunicación o plano debe ser 5 veces el diámetro total del cable. Si el cable está constantemente doblado, enchufado o desenchufado, el radio de curvatura debe ser 7 veces el diámetro total.
 - El radio de curvatura mínimo de un cable coaxial debe ser 7 veces el diámetro total del cable. Si el cable está constantemente doblado, enchufado o desenchufado, el radio de curvatura debe ser 10 veces el diámetro total.
 - El radio de curvatura mínimo de un cable de alta velocidad, como un cable SFP, debe ser 5 veces el diámetro total del cable. Si el cable está constantemente doblado, enchufado o desenchufado, el radio de curvatura debe ser 10 veces el diámetro total.
- Precauciones para el agrupamiento de cables
 - Antes de agrupar los cables, marque correctamente las etiquetas y péguelas a los cables cuando corresponda.
 - Los cables deben estar agrupados de forma ordenada y adecuada, como se muestra en **Figura 7.4**.

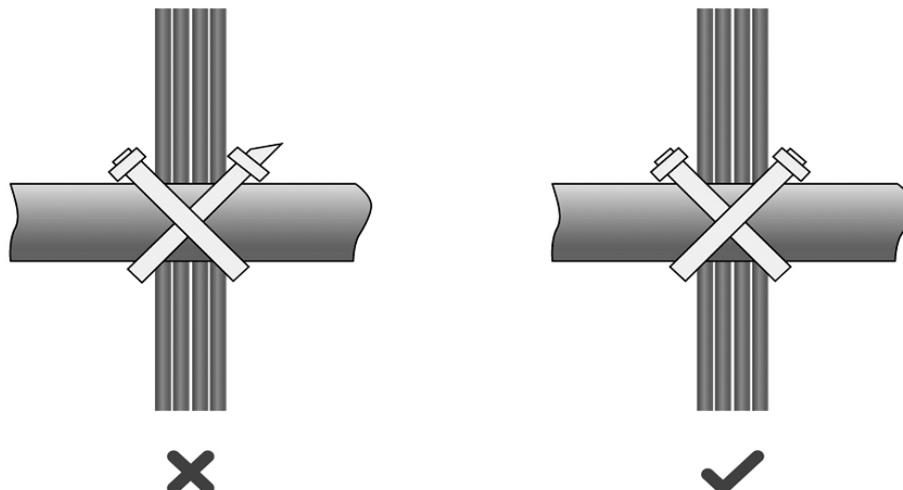
Figura 7-4 Agrupación de cables



- Enrute y agrupe los cables de alimentación, señal y tierra por separado. Cuando los cables estén cerca unos de otros, crúzalos. Cuando los cables de alimentación corren paralelos a los cables de señal, la distancia entre ellos debe ser superior a 30 mm.
- Todas las bandejas portacables y sus accesorios deben ser lisos y no tener bordes afilados.
- Los orificios metálicos a través de los cuales pasan los cables deben tener superficies lisas y bien redondeadas o estar protegidos con casquillos aislantes.
- Use bridas adecuadas para unir los cables. No ate dos o más bridas para atar los cables.

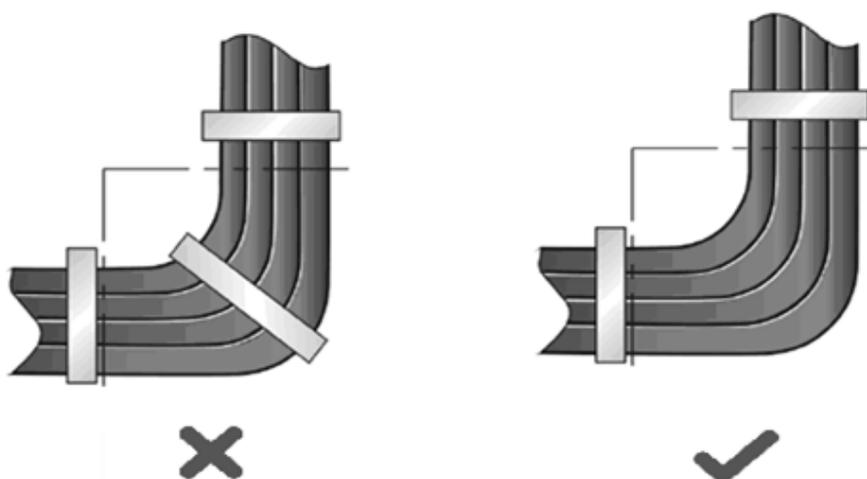
- Corte el exceso de bridas limpiamente sin bordes afilados después de agrupar los cables, como se muestra en la **Figura 7-5**.

Figura 7-5 Cortar el exceso de bridas



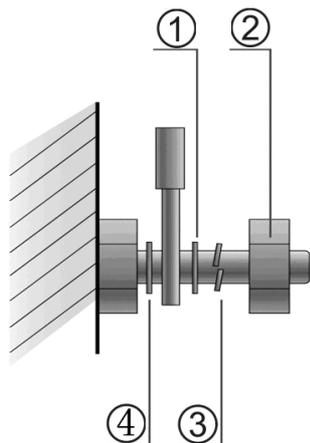
- Si los cables se van a doblar, átelos primero, pero no ate las bridas dentro de la curva para evitar tensiones en los cables, que de lo contrario pueden hacer que los cables internos se rompan, como se muestra en **Figura 76**.

Figura 7-6 No ate bridas dentro de la curva



- Enrolle los cables innecesarios o en exceso y únalos a la posición de bastidor adecuada, donde el funcionamiento del dispositivo no se vea afectado y no se produzcan daños en el dispositivo y los cables durante la depuración.
- No ate los cables de alimentación a los rieles de las piezas móviles.
- Deje una cierta longitud del cable que conecta las partes móviles, como el cable de tierra de la puerta del gabinete, para evitar tensiones en el cable; Cuando las piezas móviles estén en su lugar, asegúrese de que la longitud excesiva del cable no entre en contacto con fuentes de calor, esquinas o bordes afilados. Si las fuentes de calor son inevitables, utilice cables de alta temperatura en su lugar.
- Cuando se utilicen tornillos para sujetar los terminales de los cables, los pernos o tuercas deben apretarse y evitar que se aflojen, como se muestra en **Figura 77**.

Figura 7-7 Fijación de terminales de cable



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

- o Cuando utilice un cable rígido, fíjelo cerca del terminal del cable para evitar tensiones en el terminal y el cable.
- o No utilice tornillos autorroscantes para sujetar los terminales.
- o Agrupe los cables del mismo tipo y que vayan en la misma dirección en grupos. Mantenga los cables limpios y rectos.
- o Los cables se atarán de acuerdo con la siguiente tabla.

Díámetro del haz de cables (mm)	Espacio entre paquetes (mm)
10	De 80 a 150
De 10 a 30	De 150 a 200
30	De 200 a 300

- o No haga nudos para cables o haces de cables.
- o Las partes metálicas de los bloques de terminales prensados en frío, como los disyuntores de aire, no deben exponerse fuera de los bloques.

7.4 Fuente de alimentación

- Adaptador de corriente continua:

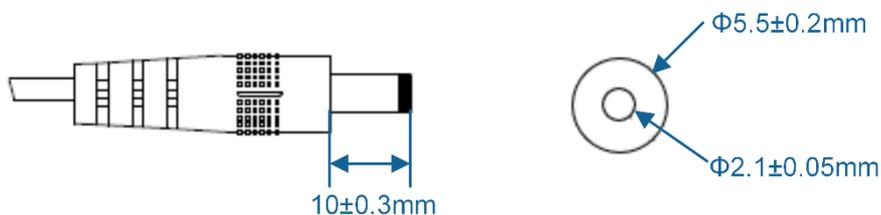
Voltaje de entrada: 48 V

Corriente nominal: 0,6 A

Table 7-3 Especificaciones técnicas del conector de alimentación de CC

Diámetro interior	Diámetro exterior	Profundidad	Polaridad
2,1 mm (0,08 pulg.)	5,5 mm (0,25 pulg.)	10 mm (0,39 pulg.)	Polo interior: positivo Polo exterior: negativo

Figura 7-8 Tamaño del adaptador de corriente continua



MANUAL DE USUARIO

Puntos de acceso de la serie AX basados en la web

Derechos de autor

Derechos de autor © 2024 Ekselans por ITS

Todos los derechos están reservados en este documento y en esta declaración.

Queda prohibida cualquier reproducción, extracción, copia de seguridad, modificación, transmisión, traducción o uso comercial de este documento o de cualquier parte de este documento, en cualquier forma o por cualquier medio, sin el consentimiento previo por escrito de Ekselans por parte de ITS.

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

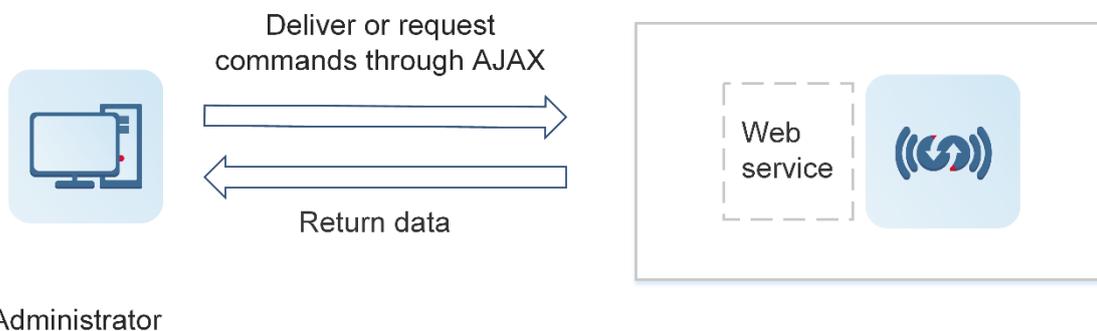
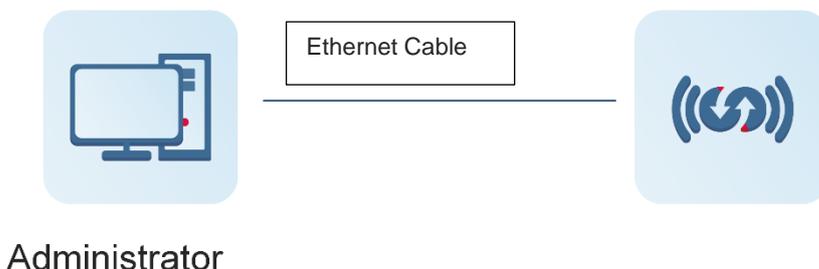


Figure 1-2 Topología simplificada



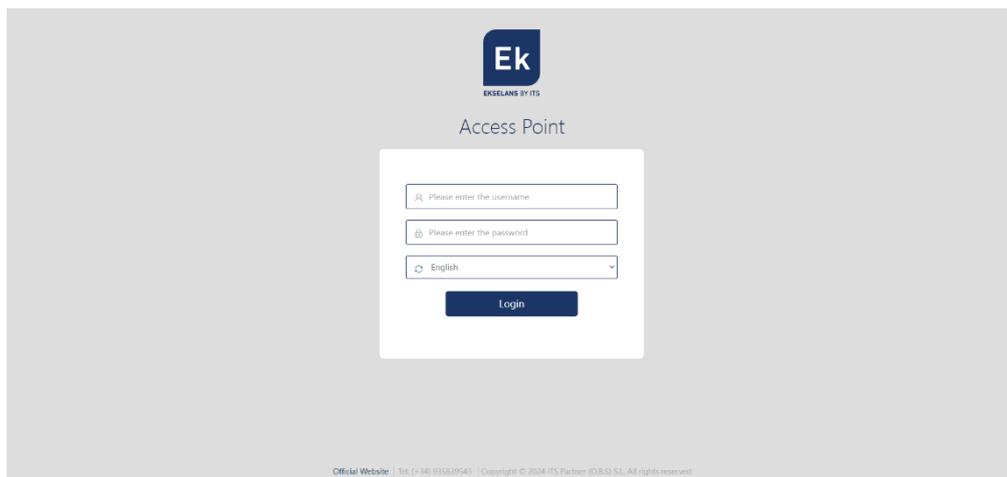
1.3 Entorno de configuración para clientes de PC

- 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	<p>http https all: Habilita el servicio correspondiente.</p> <p>http: Habilita el servicio HTTP.</p> <p>https: Habilita el servicio HTTPS.</p> <p>all: Habilita los servicios HTTP y HTTPS. Los servicios HTTP y HTTPS están habilitados de forma predeterminada.</p>
Modo de comando	Modo de configuración global

↳ **Configuración de una dirección IP**

Comando	dirección IP <i>dirección IP máscara de IP</i>
Descripción del parámetro	<p><i>ip-address:</i> Indica la dirección IP.</p> <p><i>mask:</i> Indica la máscara de subred.</p>
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 <i>Nombre de usuario de nivel de privilegio</i> <i>Nombre de usuario contraseña { contraseña [0 7] contraseña-encryptada</i>
Descripción del parámetro	<p><i>privilege-level</i>: 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 <i>guest</i> tienen permisos de los niveles de privilegio 0 y 2 respectivamente. Otras cuentas creadas manualmente tienen permisos de nivel de privilegio 1.</p> <p><i>name</i>: Indica el nombre de usuario.</p> <p><i>password</i>: Indica la contraseña.</p> <p>0 7: Indica los tipos de cifrado de contraseña, 0 para ningún cifrado y 7 para el cifrado simple. El valor predeterminado es 0.</p> <p><i>encrypted-password</i>: Indica el texto de la contraseña.</p>
Modo de comando	Modo de configuración global
Guía de uso	N/A

1.5.4 Ejemplos de configuración

↳ Configuración del servidor web

<p>Pasos de configuración</p>	<p>Habilite el servicio web.</p> <p>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.</p>
	<pre> 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 </pre>
<p>Verificación</p>	<p>Ejecute el comando show running-config para mostrar la configuración.</p>
	<pre> 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 </pre>

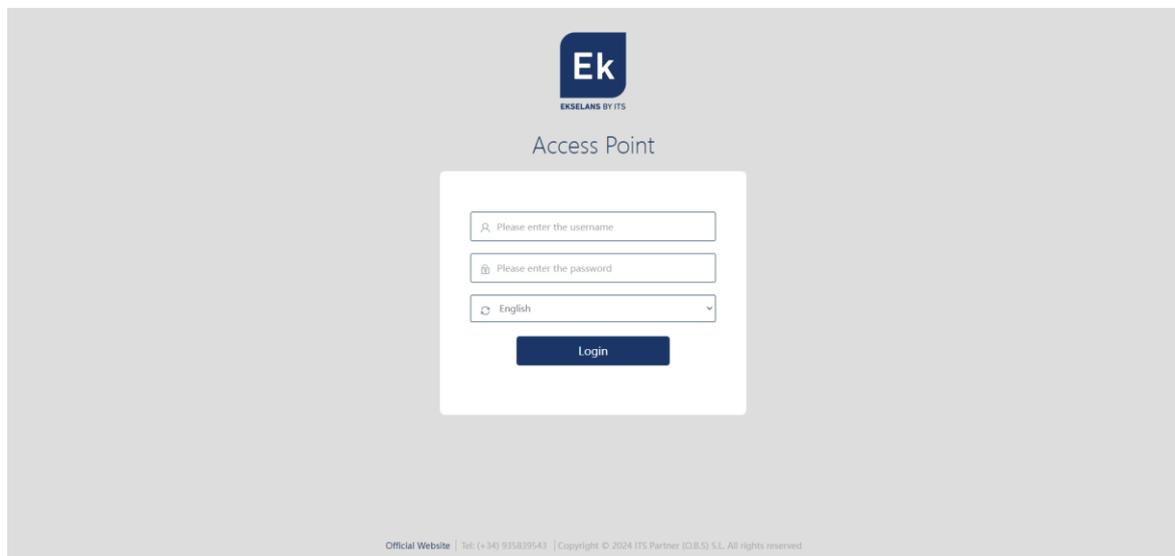
2 Configuración rápida

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

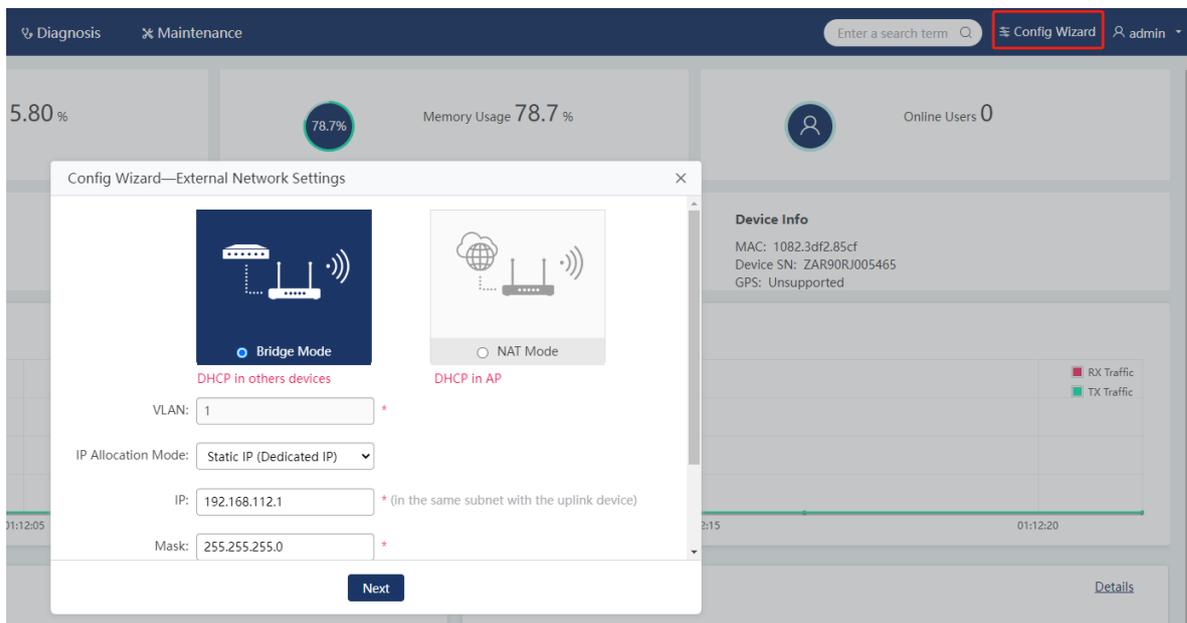
El asistente de configuración proporciona algunas configuraciones comunes basadas en escenarios. Por lo general, se usa para la primera configuración. Haga clic **en Asistente de configuración** en la barra de navegación.

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	<p>Nota</p> <p>En el modo puente, la puerta de enlace y el servidor DHCP se despliegan en el dispositivo de enlace ascendente del AP.</p>				
	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.				

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

2.2.2 Wi-Fi

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

Config Wizard—WiFi
✕

SSID: *

WiFi Password: Show Password

DHCP: Enable (IP addresses are allocated by AP)

Vlan ID:

IP Range: to

DHCP Gateway:

Preferred DNS Server: Optional

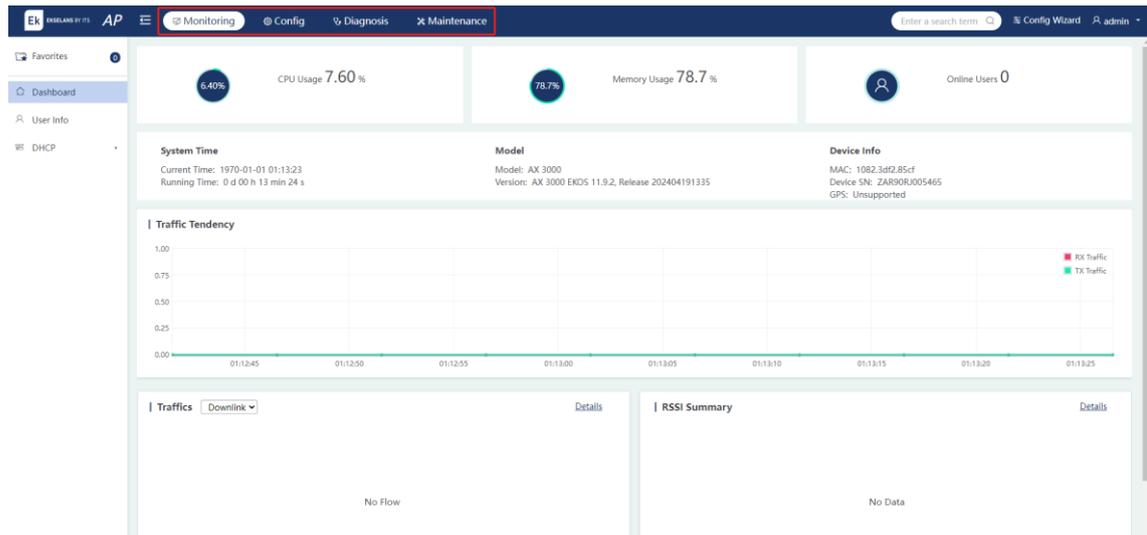
Secondary DNS Server: Optional

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.



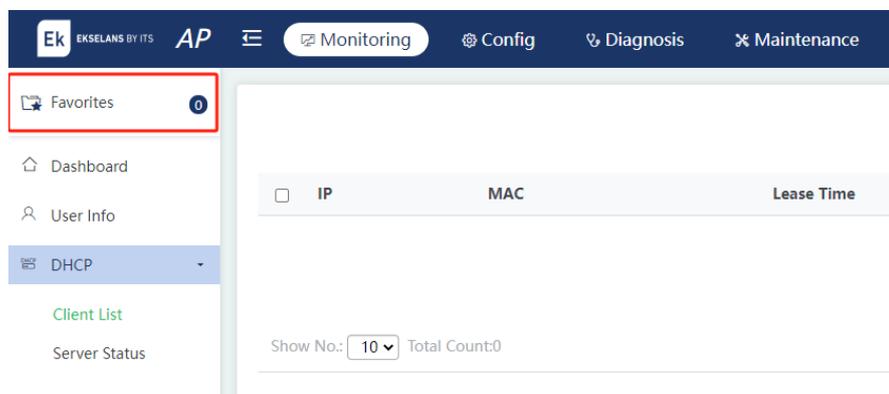
3.2 Favoritos

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**.

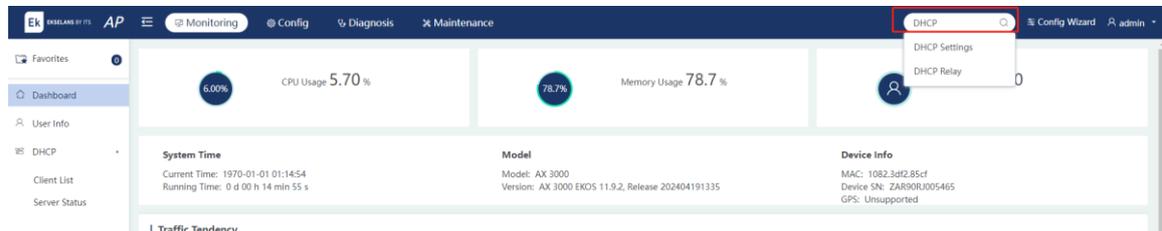
- (1) Agregar a favoritos: haga clic y arrastre un elemento del menú a **Favoritos**.



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

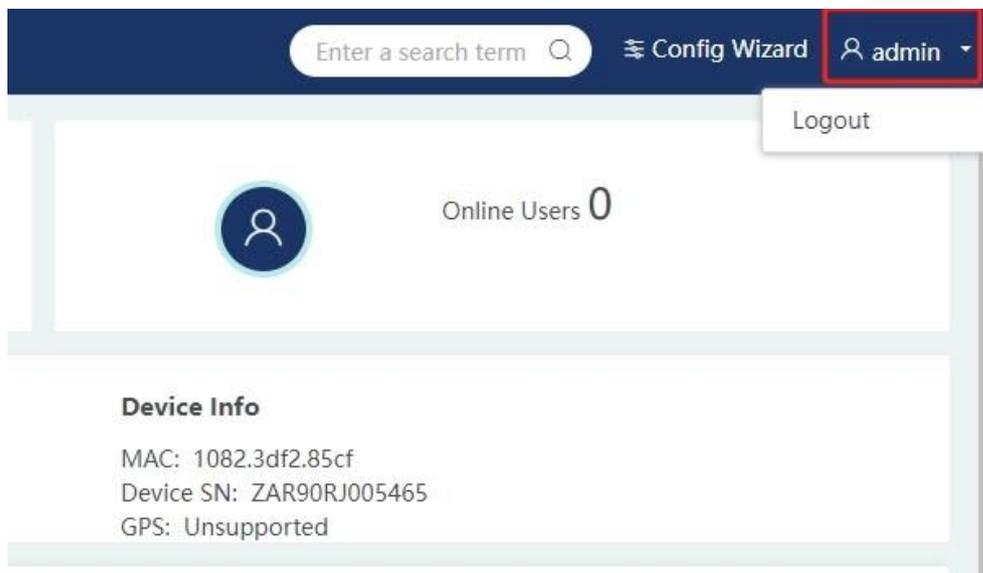
3.3 Barra de búsqueda

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.



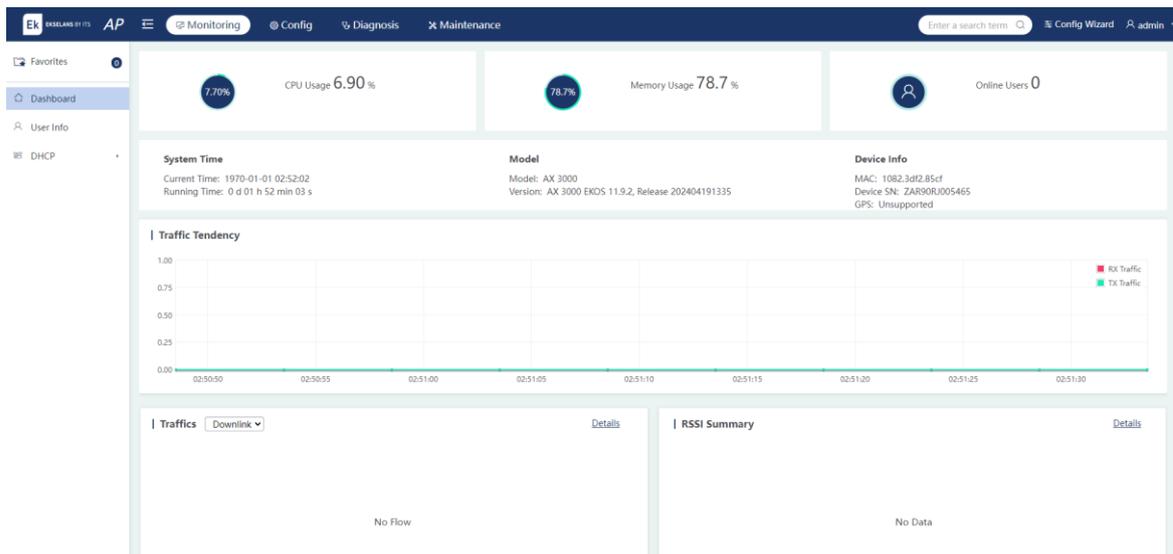
- (2) Cerrar sesión: Haga clic en **Cerrar sesión** después de expandir el menú de la cuenta para cerrar sesión en el sistema de administración web.

4 Monitorización

4.1 Dashboard

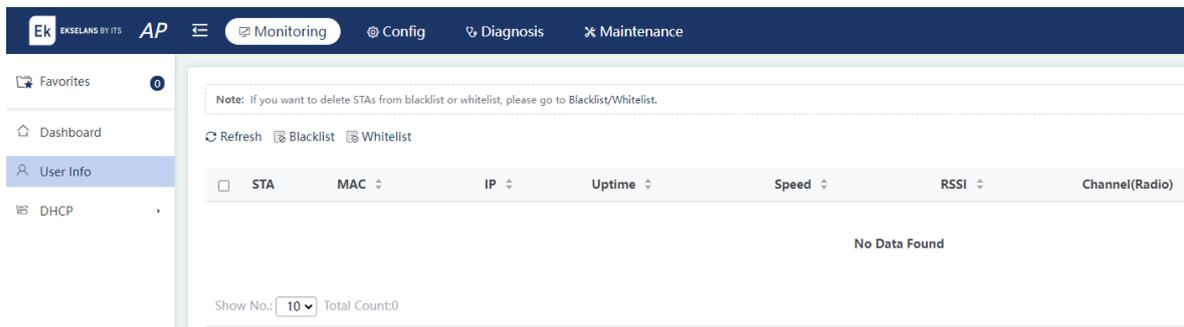
Elija **Monitoring** > Dashboard (Supervisión) (Supervisión **panel de control**).

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).



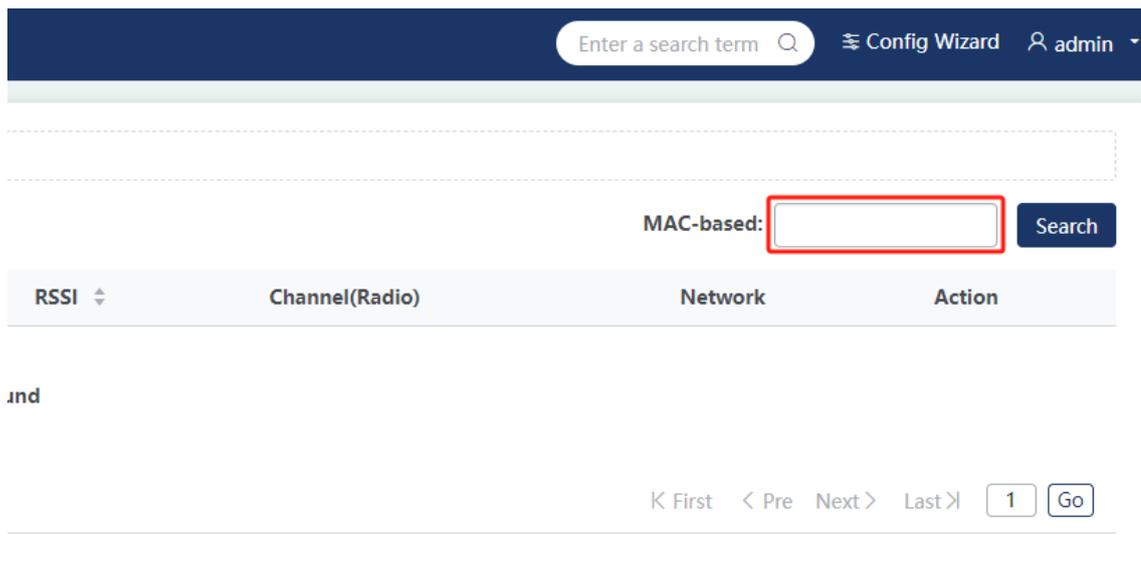
4.2 Información del usuario

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



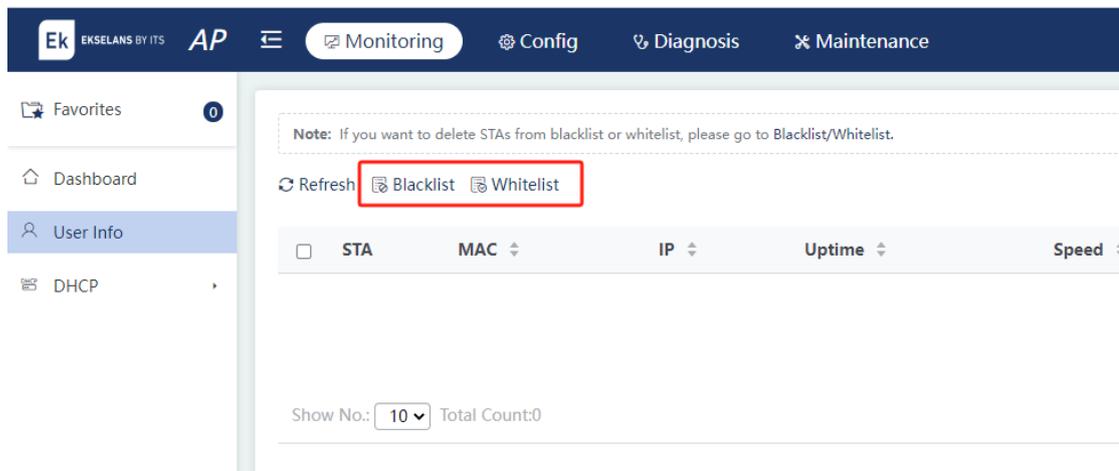
(1) Búsqueda de STA

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.

The screenshot shows the Ek interface with the following elements:

- Top navigation bar: Ek EKSELANS BY ITS, AP, Monitoring (selected), Config, Diagnosis, Maintenance.
- Left sidebar: Favorites (0), Dashboard, User Info, DHCP (selected), Client List (highlighted with a red box), Server Status.
- Main content area: A table with columns IP, MAC, and Lease Time. Below the table, there is a 'Show No.' dropdown set to 10 and 'Total Count:0'.

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.

The screenshot shows the Ek interface with the following elements:

- Top navigation bar: Ek EKSELANS BY ITS, AP, Monitoring (selected), Config, Diagnosis, Maintenance.
- Left sidebar: Favorites (0), Dashboard, User Info, DHCP (selected), Client List, Server Status (highlighted with a red box).
- Main content area: DHCP Server Status: Off (with a red 'x' icon), Config DHCP.

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.

i 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**.

The screenshot shows the configuration page for adding a new Wi-Fi network. The interface includes a top navigation bar with 'Config' highlighted, a left sidebar with 'Wireless' and 'WiFi/WLAN' selected, and a main configuration area. The configuration area contains the following fields and options:

- WLAN ID:** 1 (Range: 1-16)
- SSID:** EKWIFI
- Encryption Type:** WPA/WPA2-PSK
- WiFi Password:** ewebwifi (Show Password checked)
- Advanced Settings:**
 - Hide SSID:
 - SSID Code: utf-8 gbk
 - WiFi Type: 2.4G(radio1) 5G(radio2) [Is signal unstable or weak?]
 - 2.4G(radio1) VLAN: 1(192.168.112.1) DHCP: Enabled on switches or ge
 - 5G(radio2) VLAN: 1(192.168.112.1) DHCP: Enabled on switches or ge
 - How to configure VLAN and DHCP?
- 5G-prior Access: OFF
- Save** button

Parámetro	Descripción
WLAN ID	Introduzca el ID de WLAN.
SSID (en inglés)	Introduzca el nombre de la red Wi-Fi.
Tipo de cifrado	<p>Abierto: no se ha configurado ningún tipo de cifrado. No se requiere contraseña cuando un STA se asocia con la red Wi-Fi.</p> <p>WPA/WPA2-PSK: Modo WPA con clave precompartida de alta seguridad y fácil configuración, aplicable a hogares y pequeñas empresas.</p> <p>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.</p> <p>WPA2-802.1X: Modo WPA2 que utiliza un servidor RADIUS para la autenticación y la adquisición de claves.</p> <p>WPA3-PERSONAL: En comparación con WPA2, es más seguro y puede prevenir eficazmente los ataques de diccionario.</p> <p>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.</p> <p>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.</p> <p>WPA2/WPA3: Modo de transición WPA2/WPA3, que está determinado por un STA.</p>
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	<p>UTF-8: Se recomienda seleccionar utf-8, ya que la mayoría de los STA admiten la codificación UTF-8 de forma predeterminada.</p> <p>GBK: Algunos STA, PC y tarjetas de interfaz de red (NIC) admiten la codificación GBK.</p> <p>Puede especificar el modo de codificación según sea necesario.</p>

Parámetro	Descripción
Tipo de WiFi	<p>Especifique los tipos de red compatibles con la red Wi-Fi. Puede seleccionar varios tipos de red.</p> <hr/> <p>Nota</p> <ul style="list-style-type: none"> ● 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	<p>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.</p>
5G-Acceso previo	<p>Si esta función está habilitada, los STA accederán preferentemente a la radio de 5 GHz. Está deshabilitado de forma predeterminada.</p>

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.

The screenshot shows the configuration page for an Ek access point. The 'Config' tab is selected. In the left sidebar, 'AP' and 'Radio' are highlighted. The main content area shows settings for two radio networks:

- 2.4G Network:** ON. [Force switching from 2.4GHz to 5GHz Network]
 - Country or Region: ES(Spain)
 - Radio Protocol: 11bgn+11ax
 - Radio Channel: 1 (Current Channel: 1)
 - RF Bandwidth: 20MHz
 - Power: Enhanced
 - STA Limit: 20 (Range: 1 - 128)
- 5G Network:** ON
 - Country or Region: ES(Spain)
 - Radio Protocol: 11an+11ac+11ax
 - Radio Channel: 149 (Current Channel: 149)
 - RF Bandwidth: 40MHz
 - Power: Enhanced
 - STA Limit: 40 (Range: 1 - 128)

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. <ul style="list-style-type: none"> Las opciones de protocolo disponibles en la radio de 2,4 GHz incluyen:

Parámetro	Descripción
	<ul style="list-style-type: none"> o 11BGN indica los protocolos 802.11b, 802.11g y 802.11n. o 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: <ul style="list-style-type: none"> o 11an indica los protocolos 802.11a y 802.11n. o 11an+11ac indica los protocolos 802.11a, 802.11n y 802.11ac. o 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. <ul style="list-style-type: none"> ● 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. <hr/> <p>i Nota</p> El número máximo de STA admitidos varía según el modelo de dispositivo. Prevalecerá el rango real que se muestra en la página. <hr/>

5.2.2 WDS

i Nota

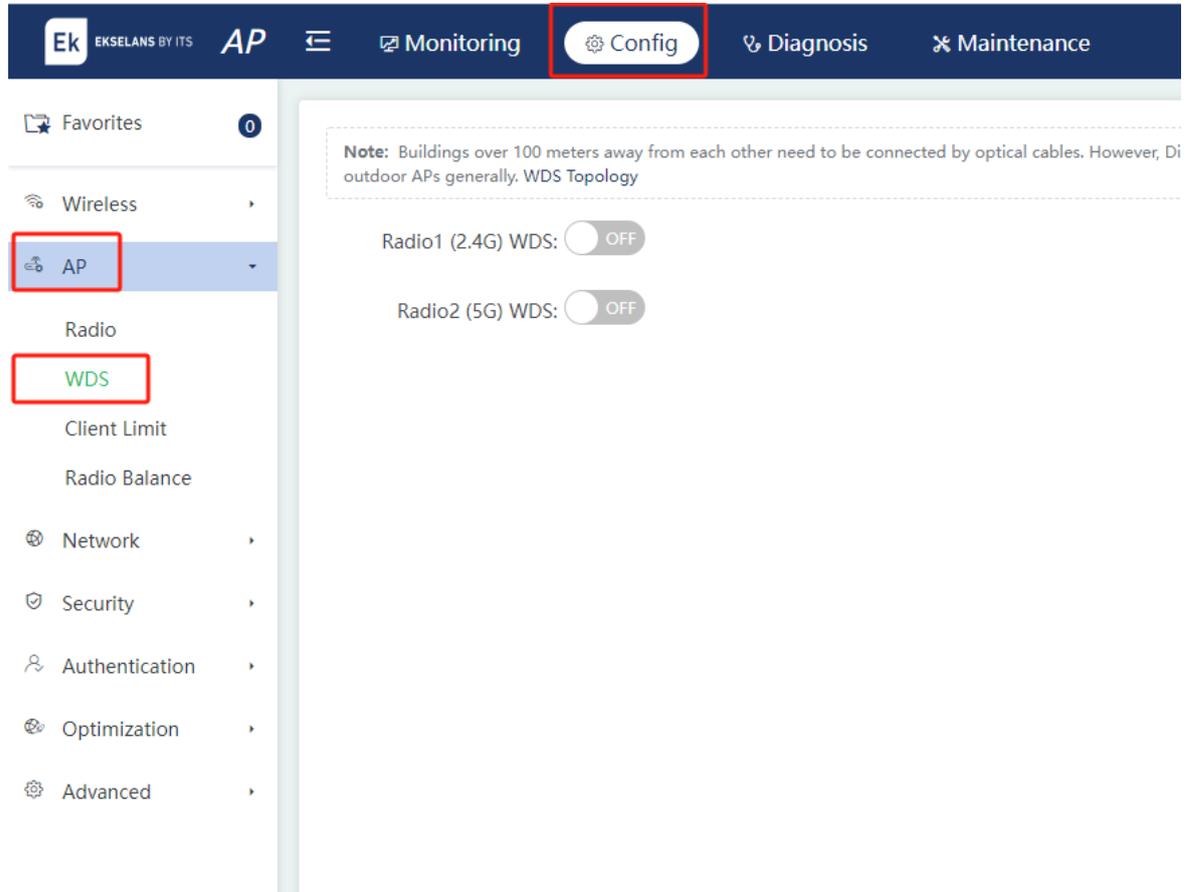
Es posible que algunos AP no admitan esta función. Prevalecerá el menú real.

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.

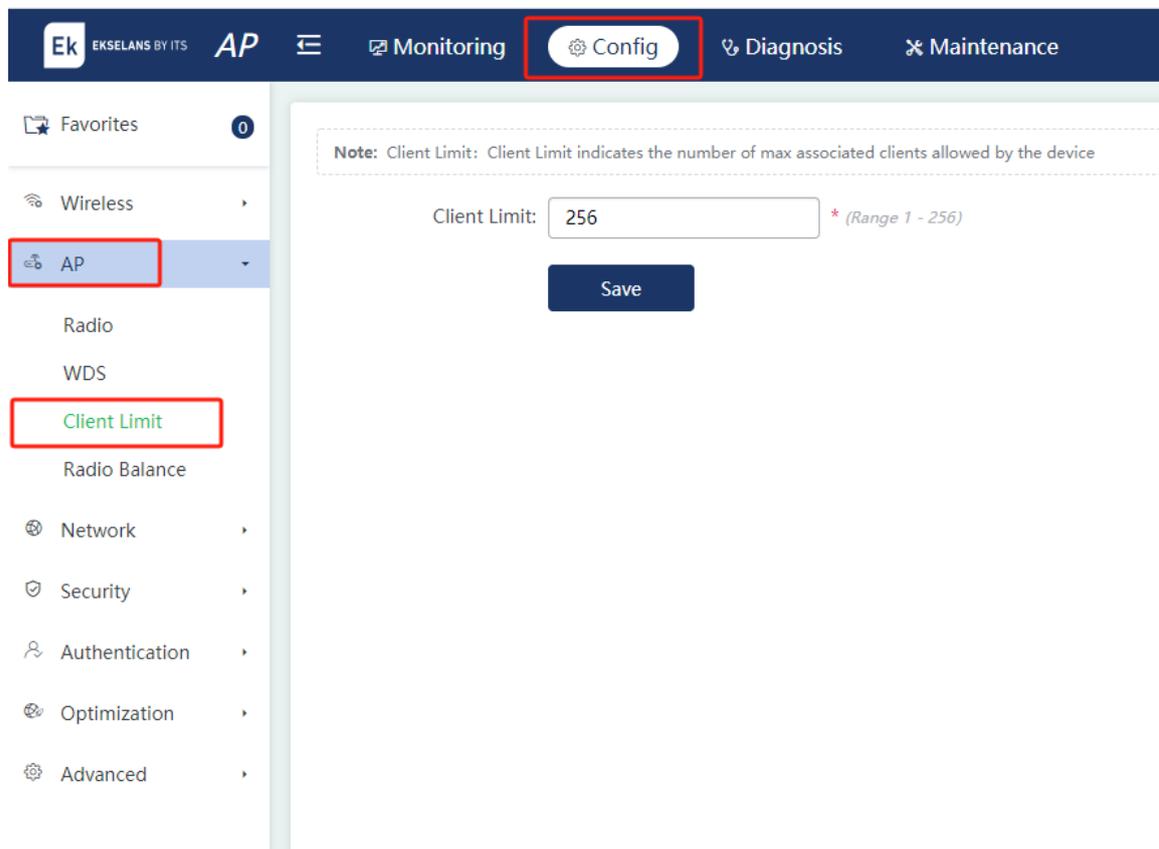
5.2.3 Límite de clientes

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

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

i 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.

The screenshot shows the configuration interface for an Ek AP. The top navigation bar includes 'Ek EKSELANS BY ITS', 'AP', 'Monitoring', 'Config' (highlighted with a red box), 'Diagnosis', and 'Maintenance'. The left sidebar shows a menu with 'Wireless', 'AP' (highlighted with a red box), 'Radio', 'WDS', 'Client Limit', 'Radio Balance' (highlighted with a red box), 'Network', 'Security', 'Authentication', 'Optimization', and 'Advanced'. The main content area displays the 'Radio Balance' configuration page. It features a note: 'Note: Radio balance refers to the balance of STAs on each radio.' Below the note, there is a toggle for 'Enable Load Balance' which is currently turned 'ON'. Underneath, the 'RF Access Ratio' is set to '100 : 100' for 'Radio1' and 'Radio2'. A 'Save' button is located at the bottom of the configuration area.

5.3 Red

5.3.1 Red externa

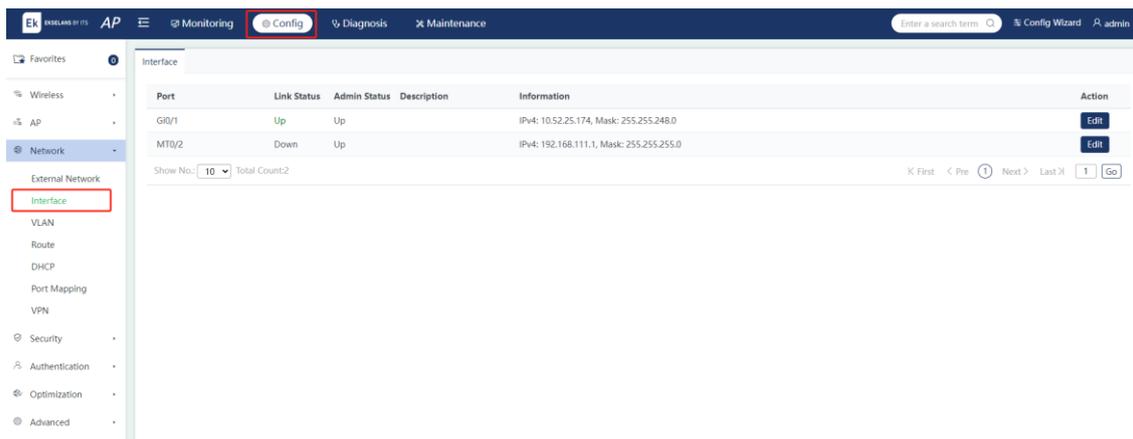
Elija **Config** > **Network** > **External Network (Red externa)**.

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, consulte [2.2.1 Configuración de red externa](#).

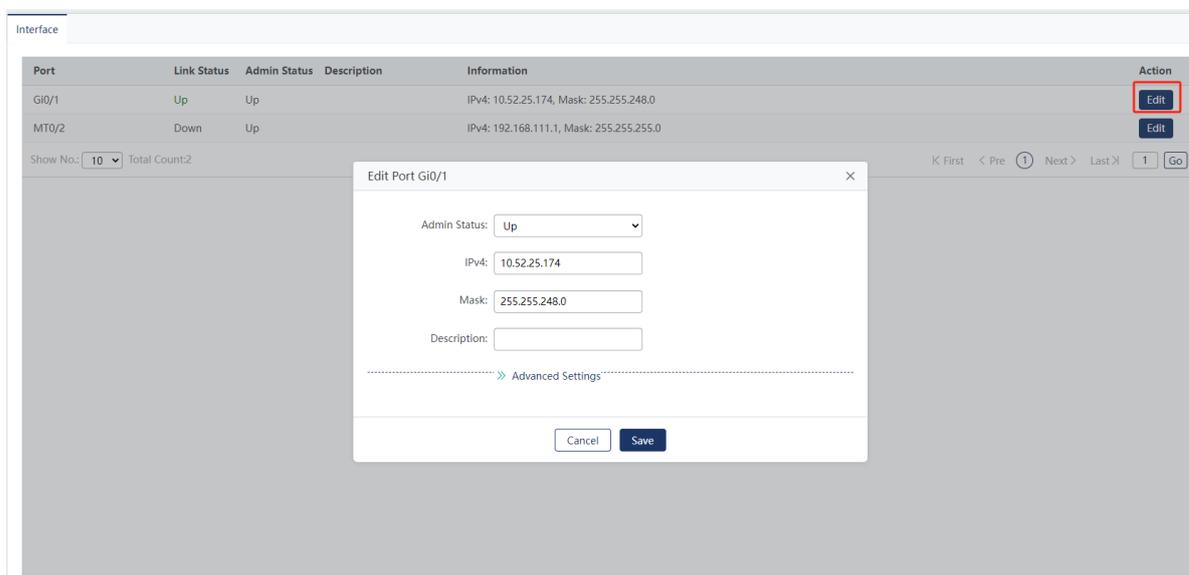
5.3.2 Interfaz

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.

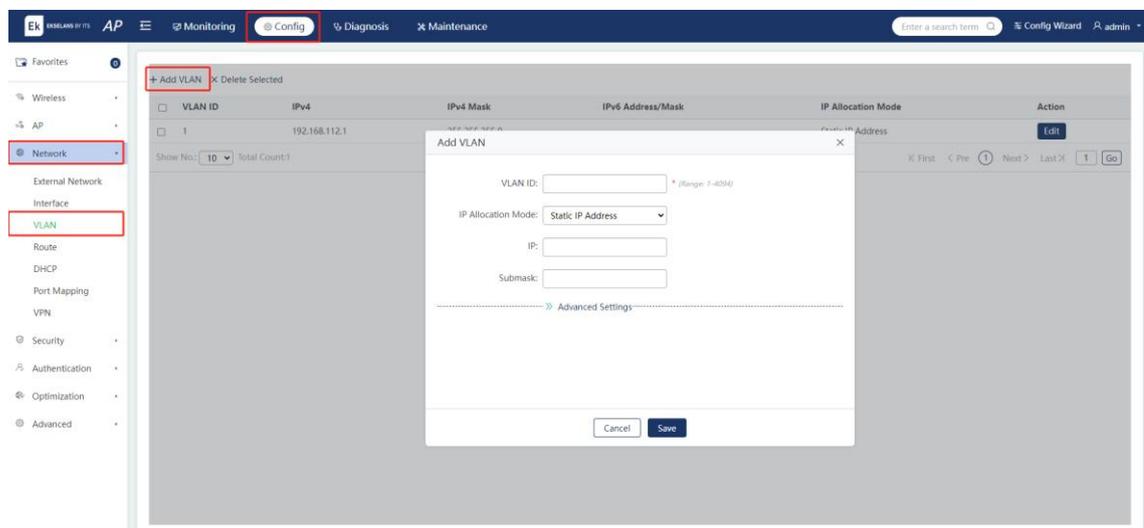
Parámetro	Descripción
Modo de trabajo	Configure el modo de trabajo del puerto, incluida la negociación automática, dúplex y semidúplex.

5.3.3 VLAN

Elija **Config > Network > VLAN**.

(1) Adición de una VLAN

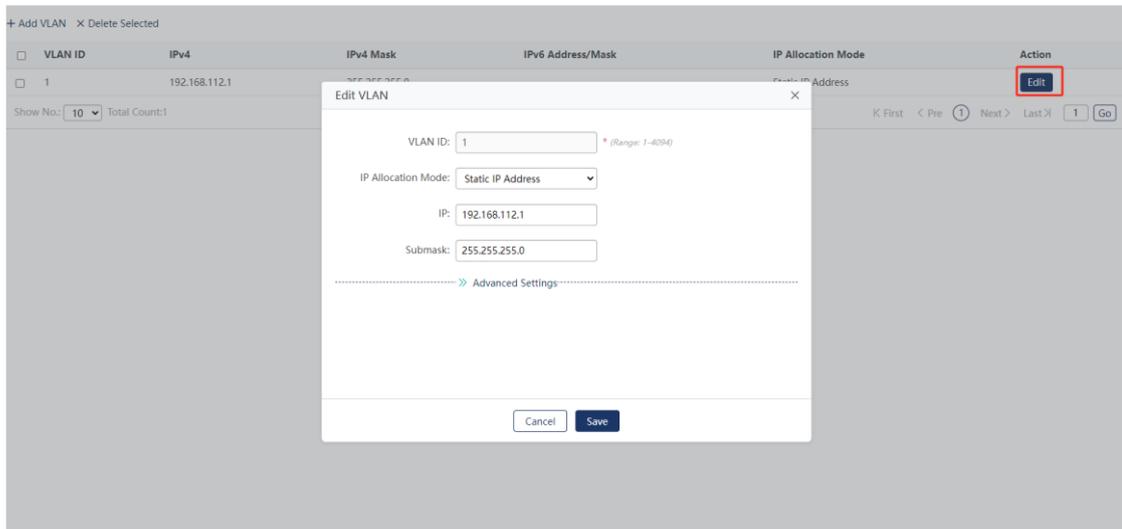
Haga clic en **Agregar VLAN** y edite los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La VLAN agregada se muestra en la lista de VLAN.



(2) Edición de una VLAN

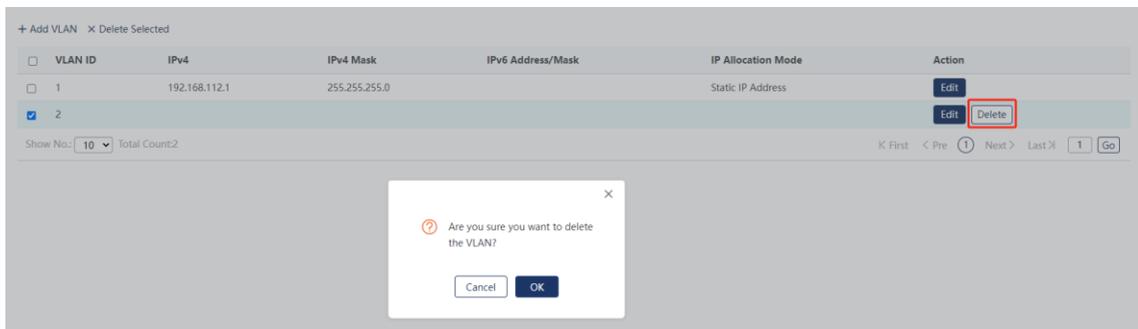
Haga clic en **Editar** en la columna **Acción** y aparecerá una ventana que muestra información sobre la VLAN. Edite los campos de la ventana. Haga clic en **Guardar** y se mostrará un mensaje

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.

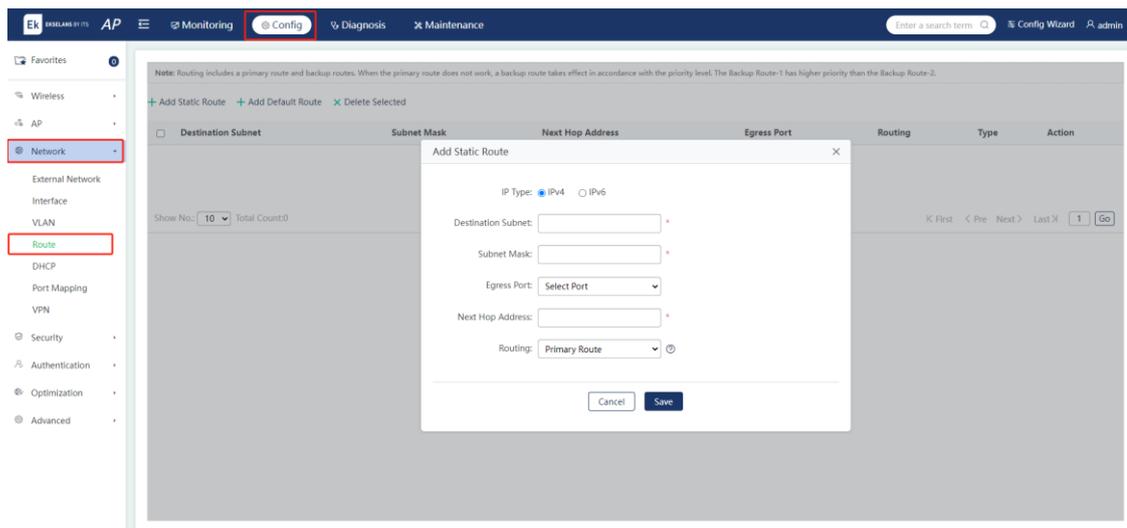


5.3.4 Ruta

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**.

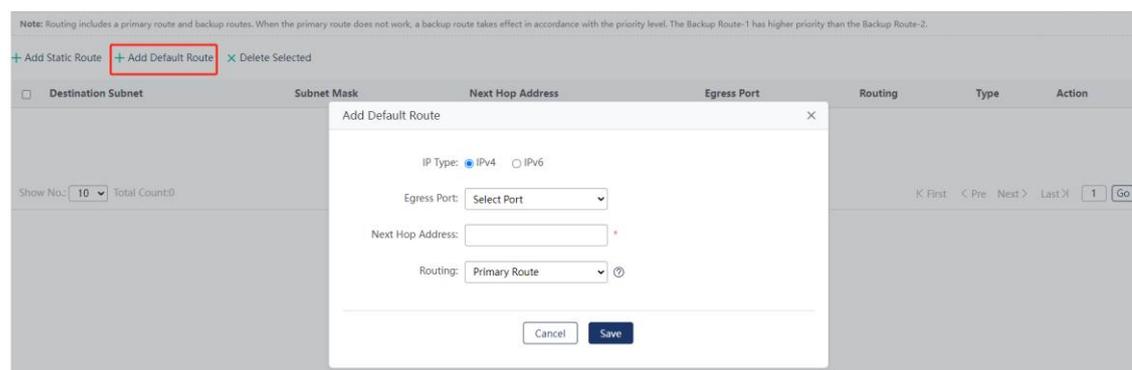


(2) Adición de una ruta predeterminada

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**.

i 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.

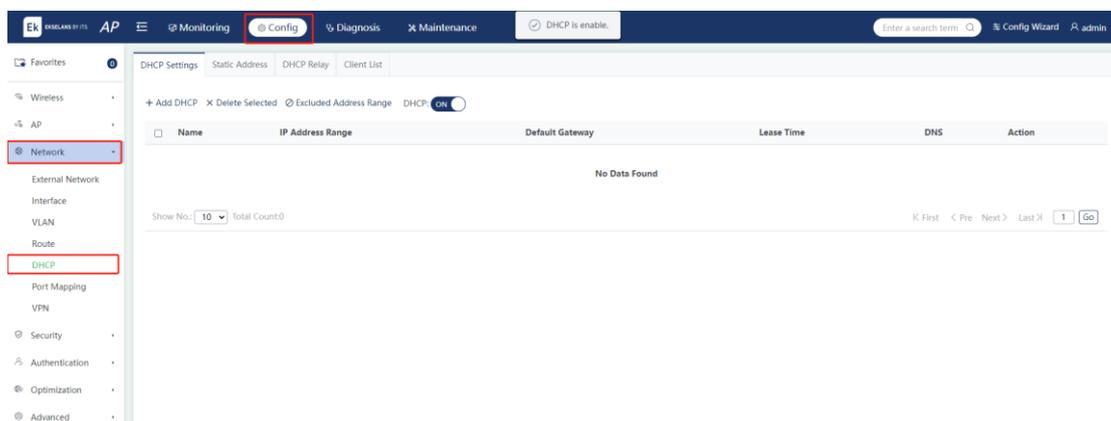
5.3.5 DHCP

1. Configuración de DHCP

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

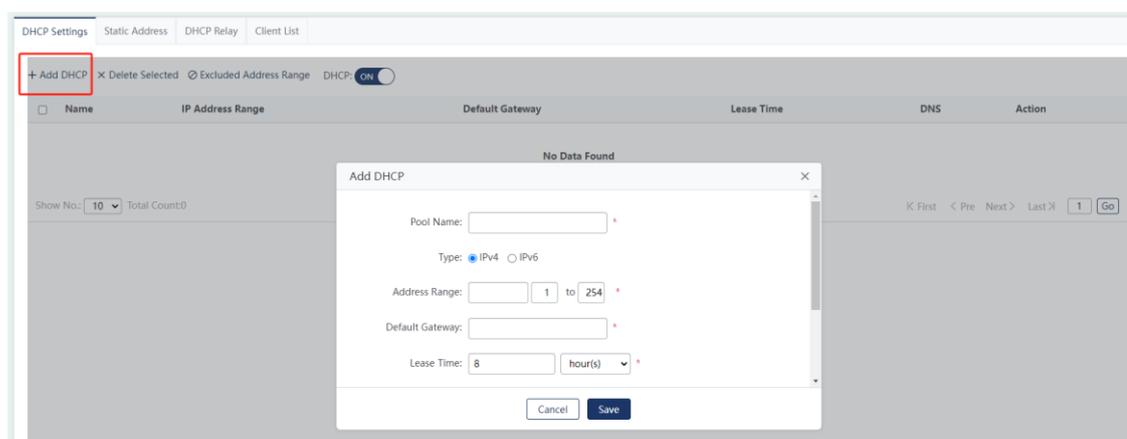
(1) Habilitación del servicio DHCP

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.



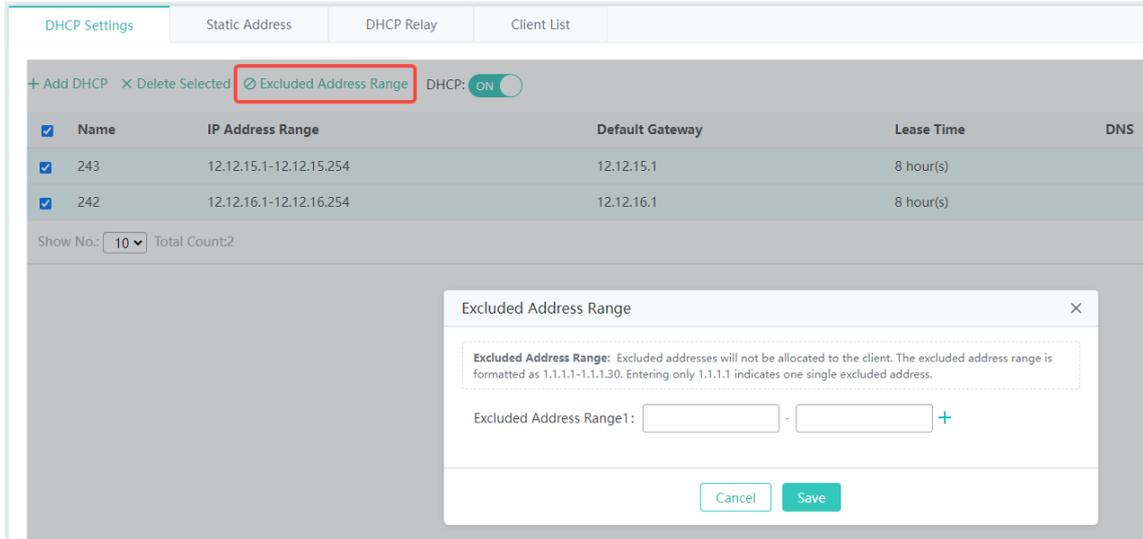
Parámetro	Descripción
Nombre del grupo	Introduzca el nombre del grupo de direcciones DHCP.
Tipo	Las opciones incluyen IPv4 e IPv6 .
Rango de direcciones	Configure el rango del grupo de direcciones DHCP.
Puerta de enlace predeterminada	Configure la puerta de enlace predeterminada para el grupo de direcciones 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

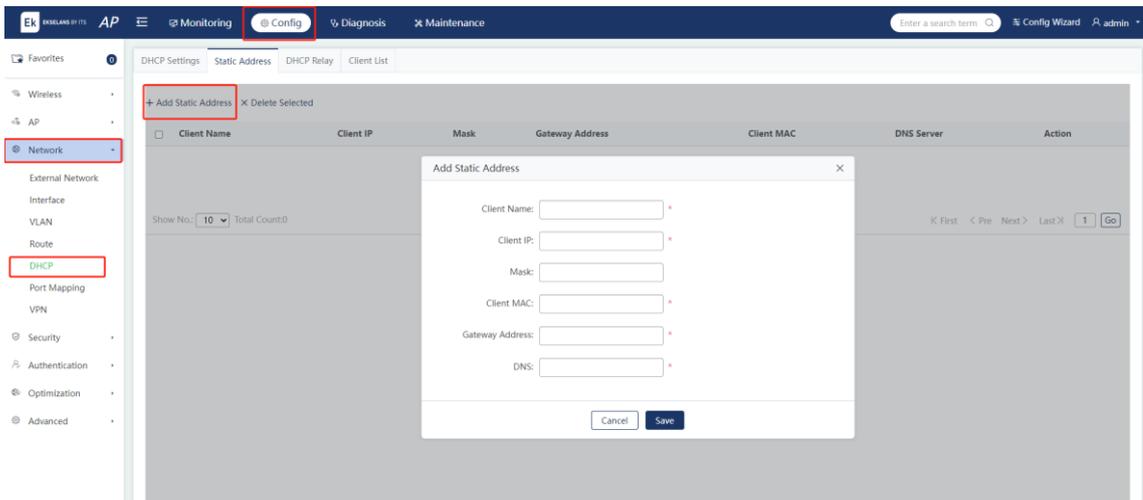
Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra información sobre el grupo de direcciones DHCP. Edite los campos de la ventana. Haga clic en **Guardar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

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**.

The screenshot shows the Ek configuration interface. The top navigation bar includes 'Monitoring', 'Config', 'Diagnosis', and 'Maintenance'. The 'Config' tab is active. On the left sidebar, 'Network' is selected, and 'DHCP' is highlighted. The main content area shows the 'DHCP Relay' configuration page. A note states: 'Please go to DHCP to enable DHCP server before enabling DHCP relay.' Below the note is a text input field for 'DHCP server IP1:' with a '+' icon to its right and a 'Save' button below it.

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.

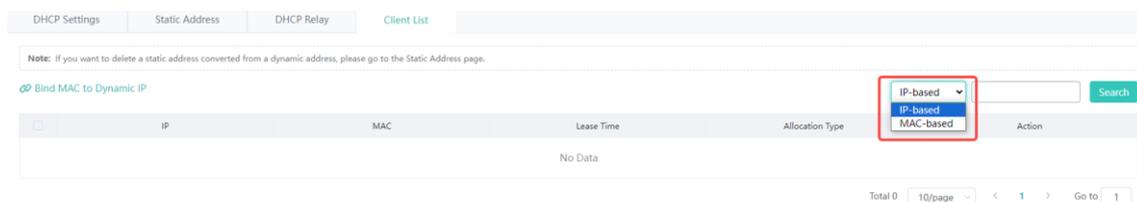
The screenshot shows the Ek configuration interface with the 'Client List' page selected. A note states: 'If you want to delete a static address converted from a dynamic address, please go to the Static Address page.' Below the note is a checkbox labeled 'Bind MAC to Dynamic IP'. A table with the following columns is shown: 'IP', 'MAC', 'Lease Time', and 'Allocation Type'. The table is currently empty, displaying 'No Data Found'. At the bottom, there is a 'Show No.' dropdown menu set to '10' and 'Total Count:0'.

(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

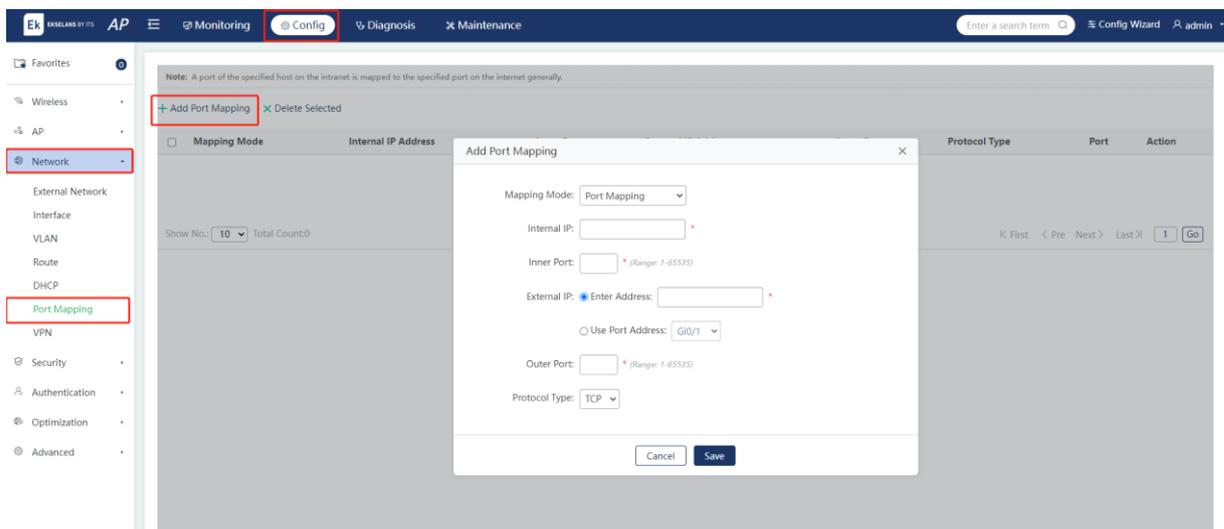
Es posible que algunos AP no admitan esta función. Prevalecerá el menú real.

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

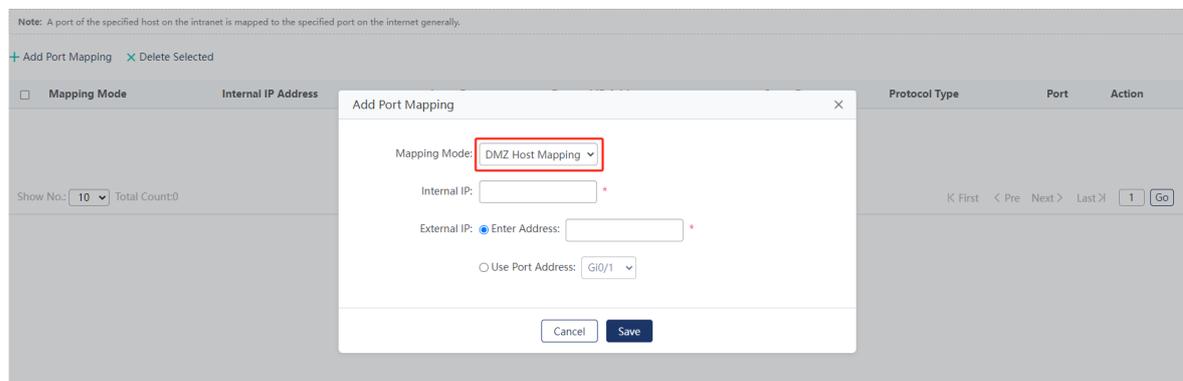
Haga clic en **Agregar asignación de puertos**. Establezca el modo de asignación en **Asignación de puertos** y edite los campos en la ventana emergente. Haga clic en **Guardar**.



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.

The screenshot displays the VPN configuration interface. The left sidebar has 'VPN' selected under the 'Network' category. The main content area includes a 'WAN Port' dropdown set to 'Gi0/1'. Below are input fields for 'Local IP Address', 'Local Submask', 'HQ IP Address', 'HQ Submask', 'VPN Address', and 'Shared Key', each with a red asterisk indicating a required field. The 'Advanced Settings' section is expanded, showing radio button options for 'Encryption Algorithm' (DES, 3DES, AES256, AES192, AES128), 'Auth Algorithm' (MD5, SHA), 'DH Group' (C5, C1), 'ESP Encryption Algorithm' (esp-des), and 'ESP Auth Algorithm' (esp-md5-hmac). A 'Keepalive Time(s)' field is set to 300.

5.4 Seguridad

5.4.1 Contención

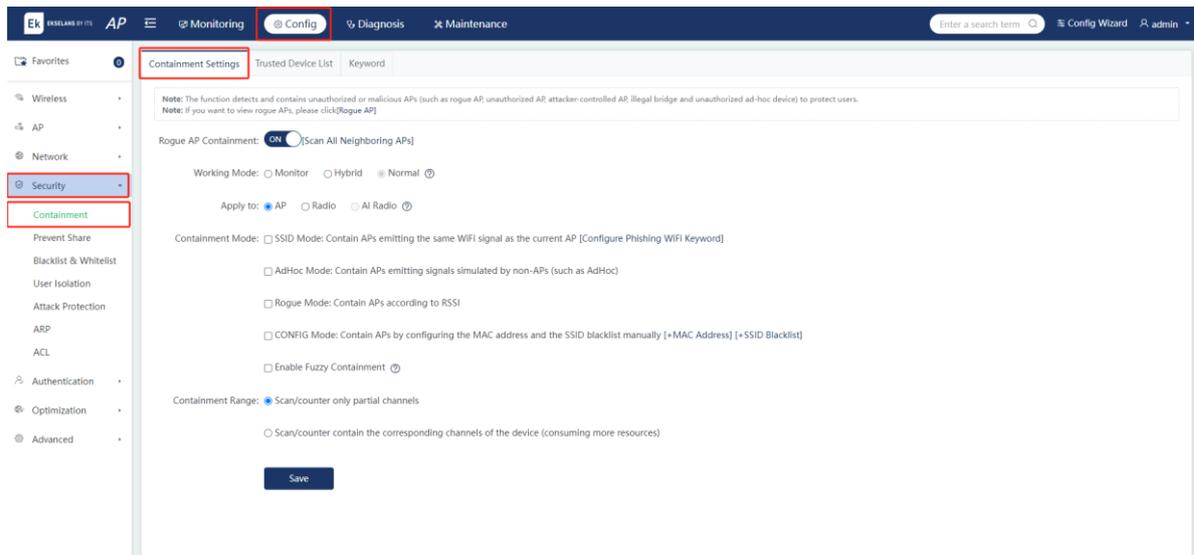
Elija **Config > Security > Containment (Contención)**.

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

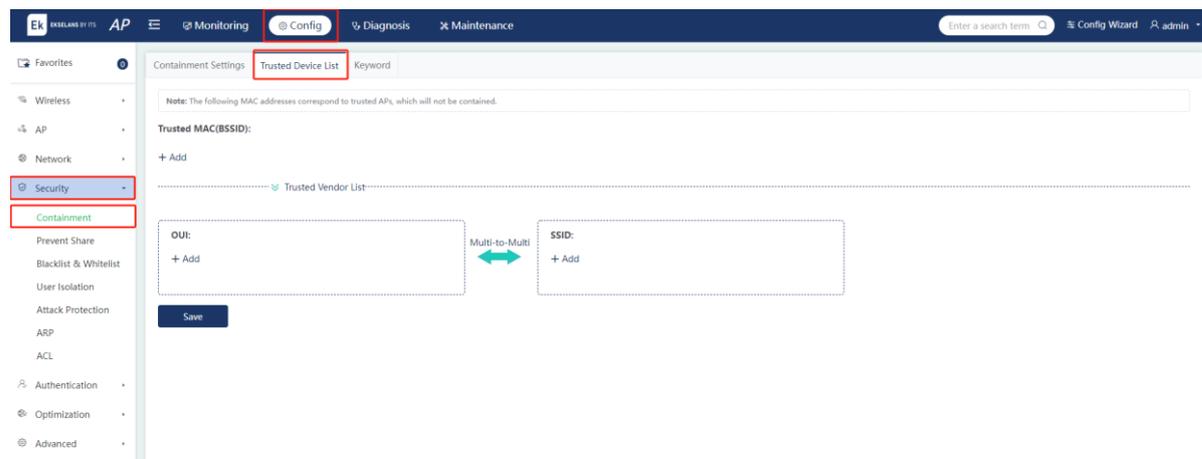
Cuando **Rogue AP Containment** está habilitado, debe configurar el modo de trabajo en **Monitor** o **Híbrido**.

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.



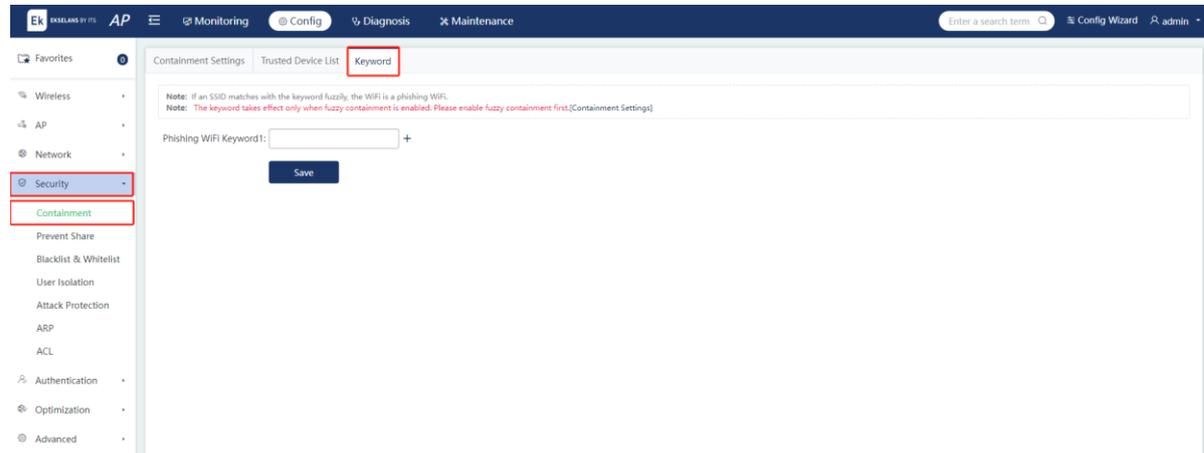
2. Lista de dispositivos de confianza

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

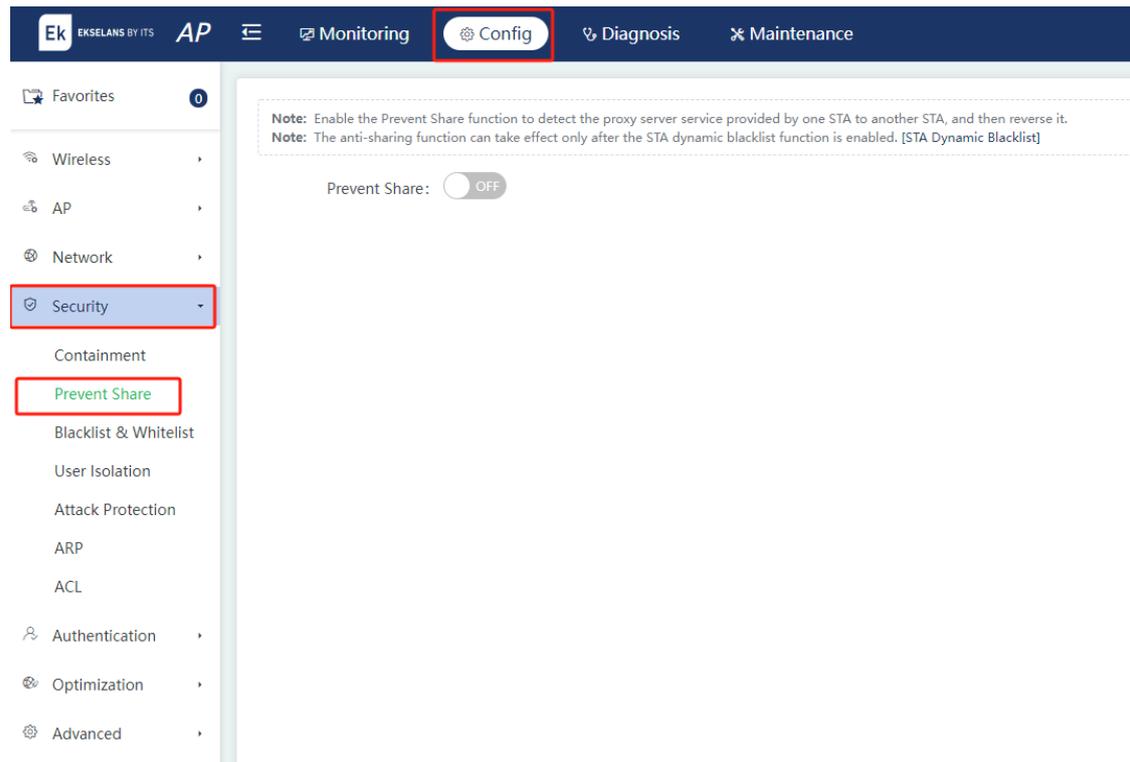
Las palabras clave de phishing de Wi-Fi se obtienen escaneando los SSID de la red. Haga coincidir los SSID escaneados con las palabras clave configuradas. Si un SSID coincide con la palabra clave de forma difusa, el Wi-Fi se considera un Wi-Fi de phishing.



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**.

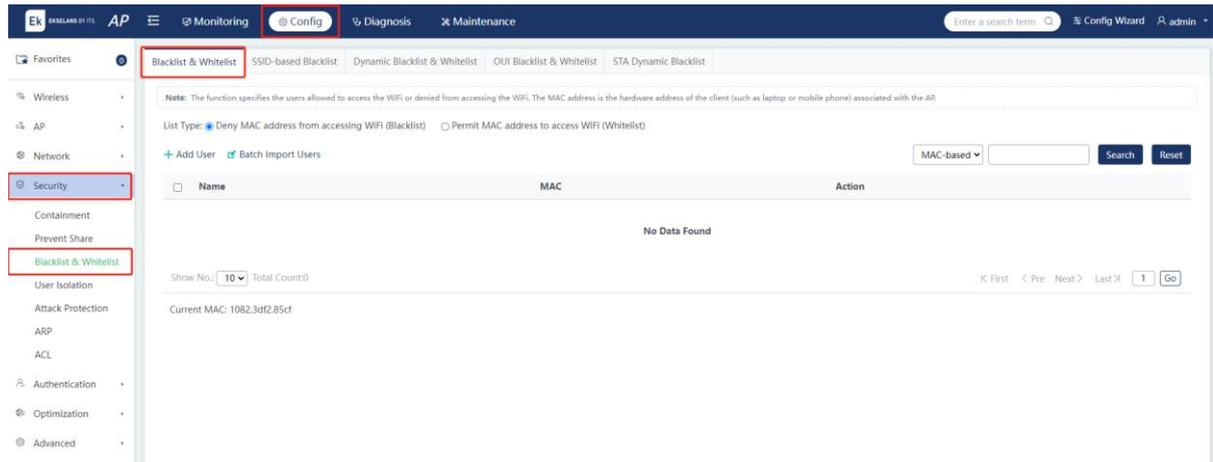
Para mejorar la seguridad inalámbrica, puede configurar una lista negra (a los usuarios de la lista negra se le niega el acceso a la red Wi-Fi) y una lista blanca (solo los usuarios de la lista blanca pueden acceder a la red Wi-Fi) para controlar el acceso de los usuarios inalámbricos. Un AP gordo admite 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.

i 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. Prevalerá 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.

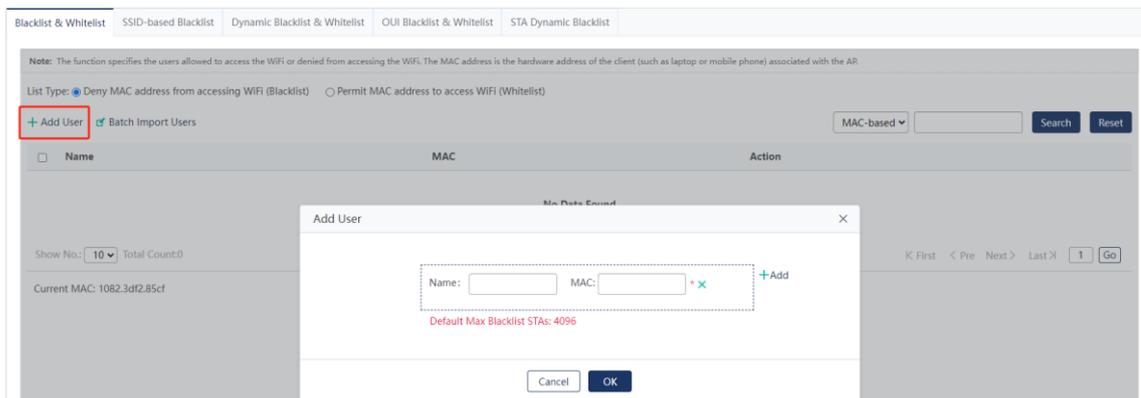
1. Configuración de la lista negra global o la lista blanca

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.



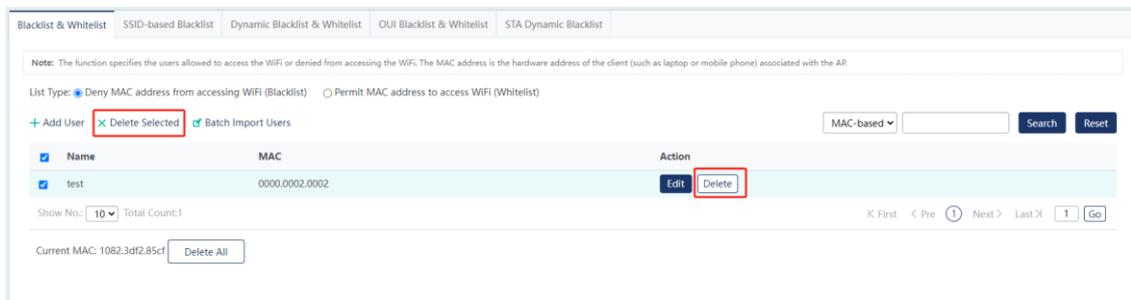
(1) Adición de un usuario

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.

The screenshot shows the 'Batch Import Users' dialog box. It contains a note: 'Note: It is recommended to download the template, fill in data and import the file. Template: listen.csv Download Template List Capacity: 4096'. Below the note is a 'File:' input field with 'Browse' and 'Import' buttons. The background interface shows a table with columns 'Name' and 'MAC', and a 'Batch Import Users' button highlighted with a red box.

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.

The screenshot shows the 'SSID-based Blacklist' configuration page. It features a note: 'Note: If you want to add a WiFi, please go to Add WiFi'. Below the note is a table with columns 'SSID' and 'Action'. The table is currently empty, displaying 'No Data Found'. At the bottom, there is a 'Show No.: 10' dropdown and 'Total Count:0'.

(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.

Blacklist & Whitelist **SSID-based Blacklist & Whitelist** Dynamic Blacklist & Whitelist OUI Blacklist & Whitelist

Note: If you want to add a WiFi, please go to [Add WiFi](#)

SSID	Action
Eweb_47981	Blacklist/Whitelist OUI Whitelist & Blacklist

Show No.: 10 Total Count:1

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

Blacklist & Whitelist **SSID-based Blacklist & Whitelist** Dynamic Blacklist & Whitelist OUI Blacklist & Whitelist STA Dynamic Blacklist

Eweb_47981 OUI Whitelist & Blacklist

Note: You can configure whitelisted OUI to allow(noallow) some organizations to access Eweb.

List Type: The following manufacturers are prohibited from accessing WIFI (blacklist) Only the following manufacturers are allowed to access WIFI (whitelist)

[+ Add OUI](#) [X Delete Selected](#) [Import OUIs](#)

Remark	OUI	Action
--------	-----	--------

Show No.: 10 Total Count:0

[Clear All](#)

Add blacklist OUI

Name: OUI: * [X](#) [+Add](#)

[Cancel](#) [OK](#)

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**.

The screenshot shows the configuration page for 'Dynamic Blacklist & Whitelist'. The 'Dynamic Blacklist' checkbox is checked. The 'Effective Time' is set to 300 seconds. The 'Save' button is highlighted. The table below shows 'No Data Found'.

Number	MAC	Effective Time	Type	Action
No Data Found				

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.

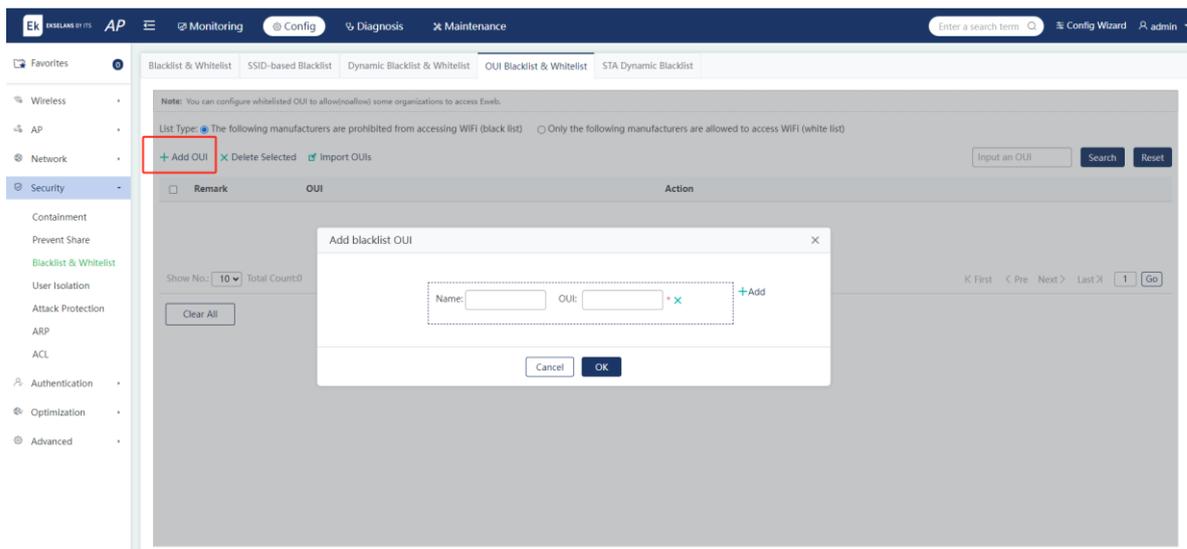
The screenshot shows the configuration page for 'Dynamic Blacklist & Whitelist'. The 'Delete Selected' button is highlighted. The table below shows 'No Data Found'.

Number	MAC	Effective Time	Type	Action
No Data Found				

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

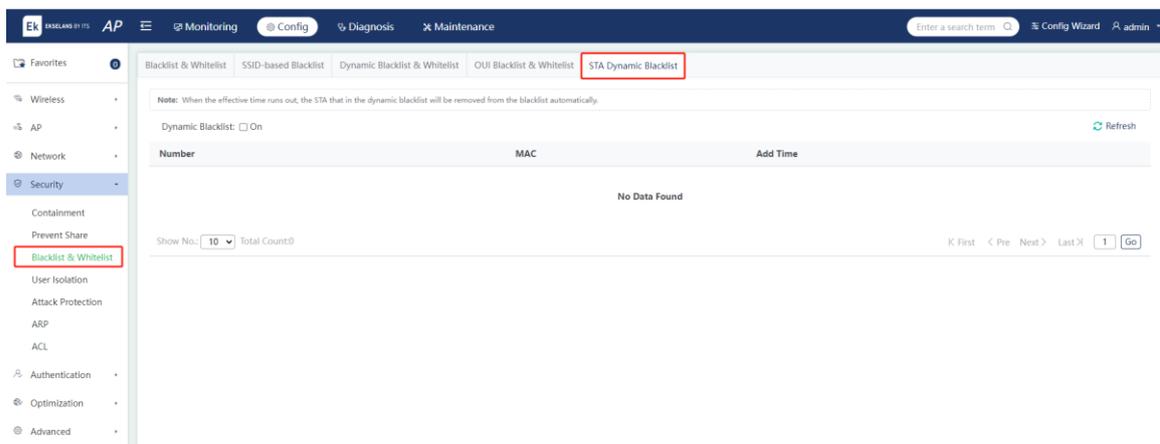
A los fabricantes de la lista negra de OUI se les niega el acceso a cualquier red Wi-Fi del AP, mientras que solo los fabricantes de la lista blanca de OUI pueden acceder a cualquier red Wi-Fi del AP.

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

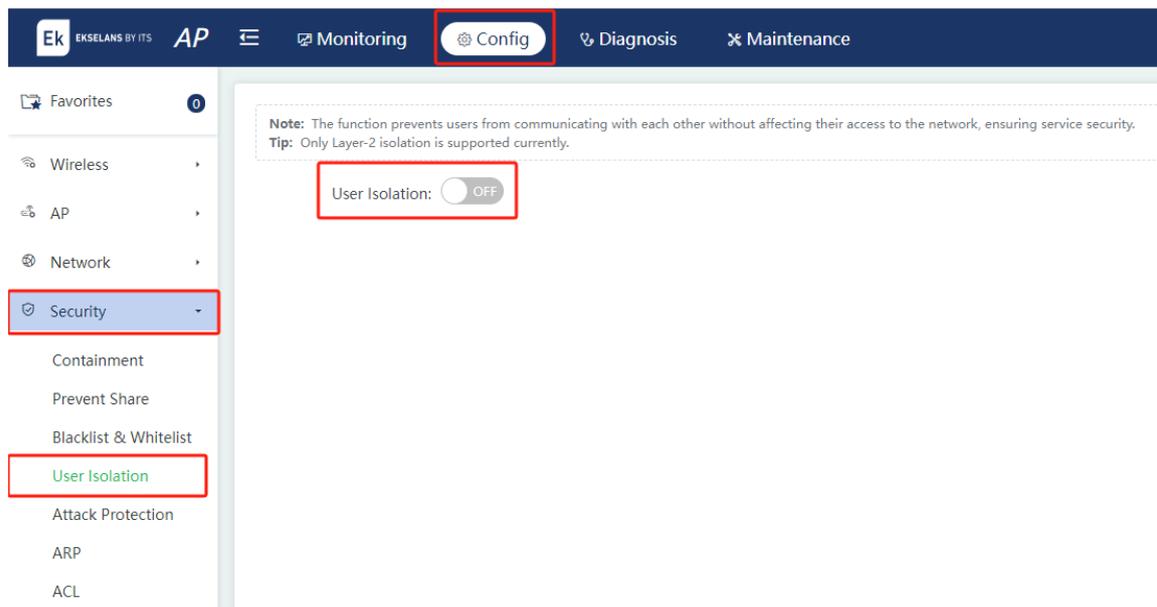
Agregue STA de fuentes de ataque maliciosas a la lista negra dinámica de STA para evitar que accedan a la red.



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.

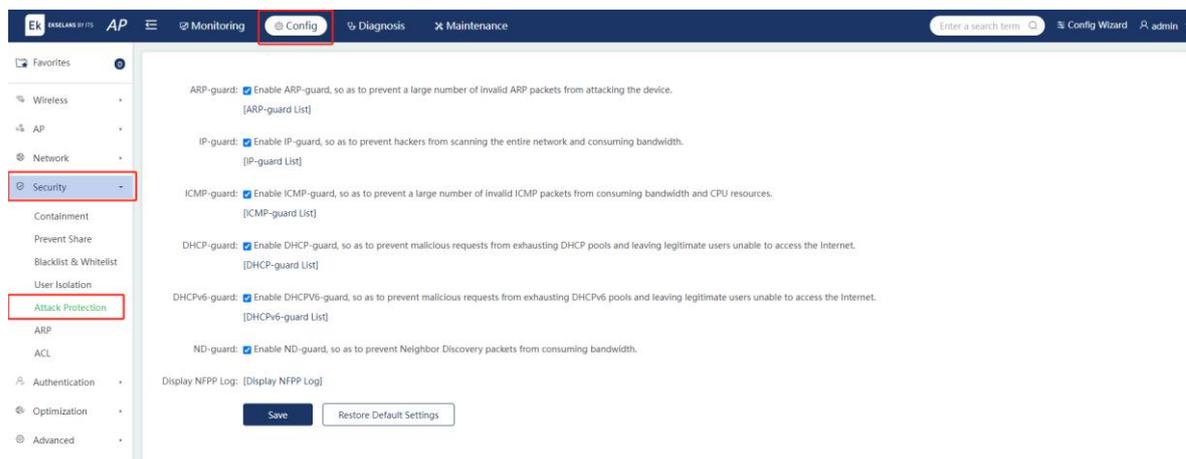


5.4.5 Prevención de ataques

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

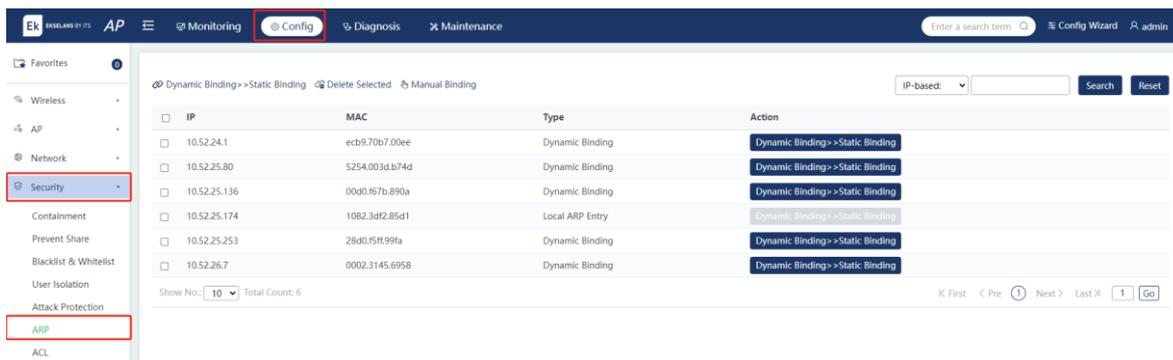
Los ataques maliciosos suelen producirse en un entorno de red. Estos ataques sobrecargan el dispositivo, lo que resulta en un uso elevado de la CPU y un error de funcionamiento del dispositivo.

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



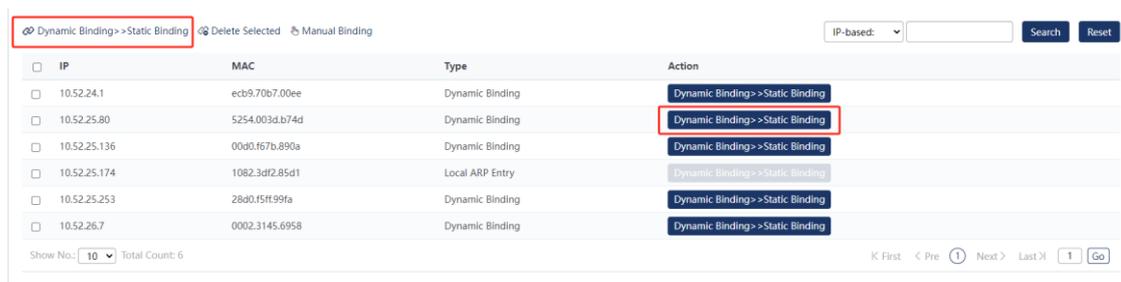
5.4.6 Enlace de entrada ARP

Elija **Config > Security > ARP**.



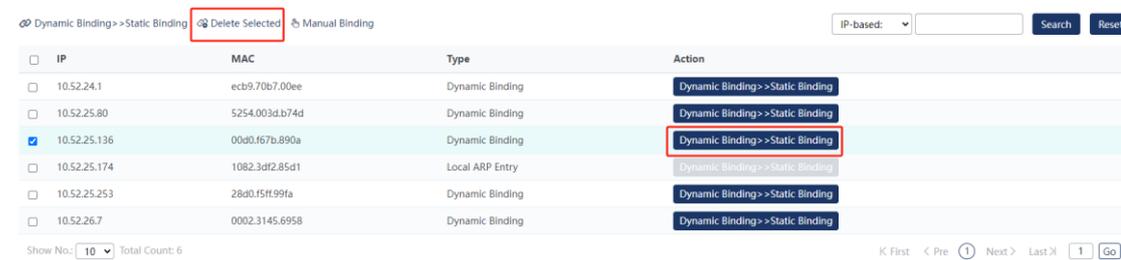
(1) Cambiar un enlace dinámico a un enlace estático

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.



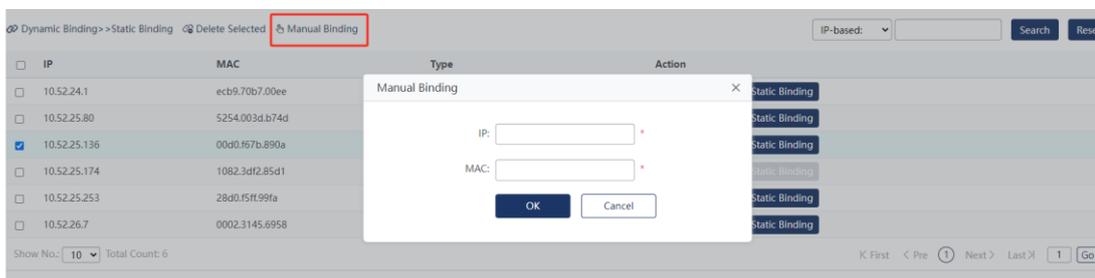
(2) Eliminación de un enlace estático

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**.

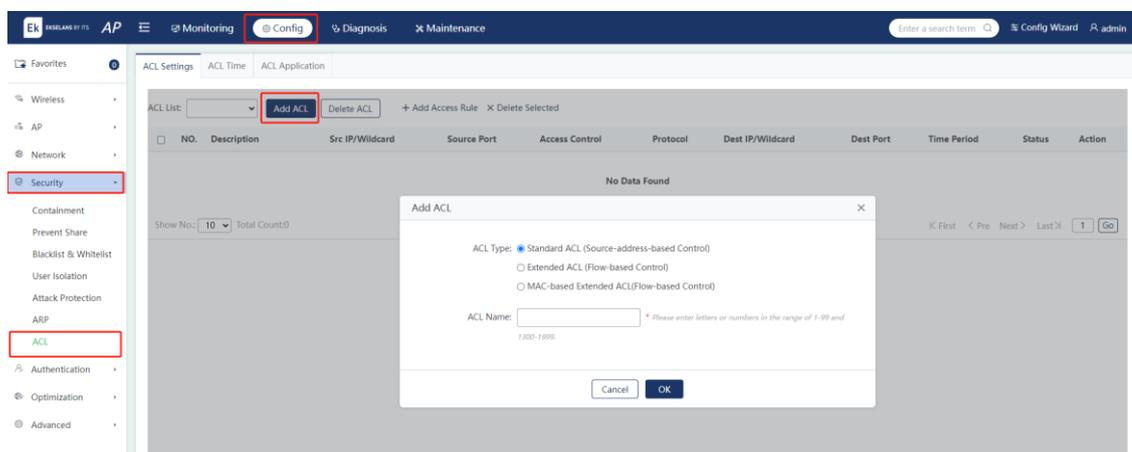
Al recibir un paquete, una interfaz de dispositivo en la que se configura una ACL de entrada comprueba si el paquete coincide con una entrada de control de acceso (ACE) en la ACL de entrada. Al enviar un paquete, una interfaz de dispositivo en la que se configura una ACL de salida comprueba si el paquete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

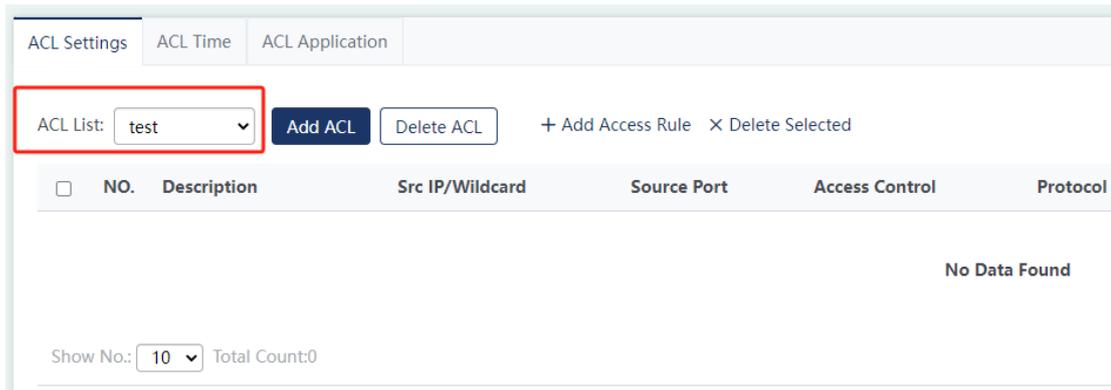
Cuando se configuran diferentes ACE, se pueden aplicar varias ACE al mismo tiempo, o solo se aplican algunas ACE. Los paquetes se procesan de acuerdo con la primera ACE coincidente (permitir o denegar).

1. Configuración de ACL

(1) Adición de una ACL

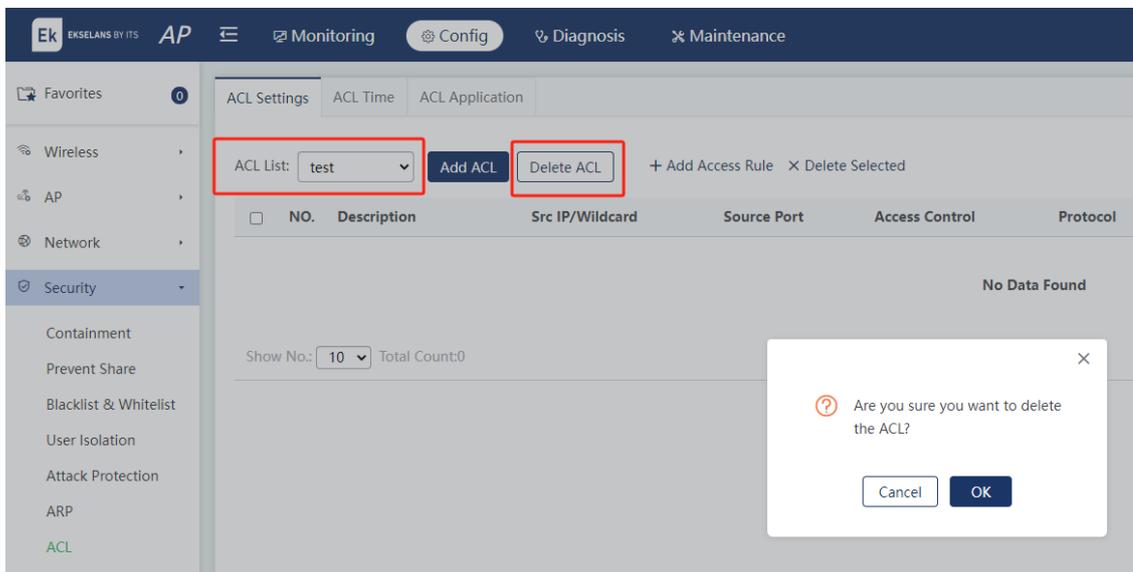
Haga clic en **Agregar ACL**. Introduzca los campos en la ventana emergente. Haga clic en **Aceptar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La nueva entrada se muestra en la lista desplegable de ACL en la esquina superior izquierda.





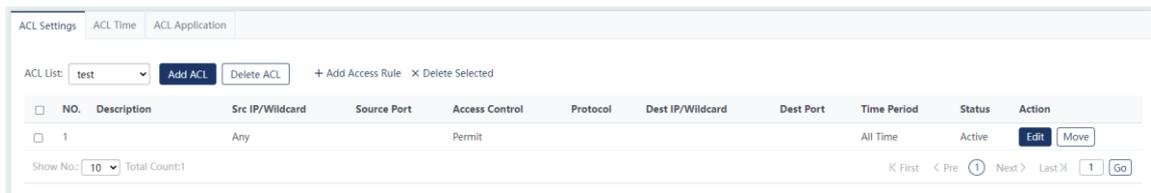
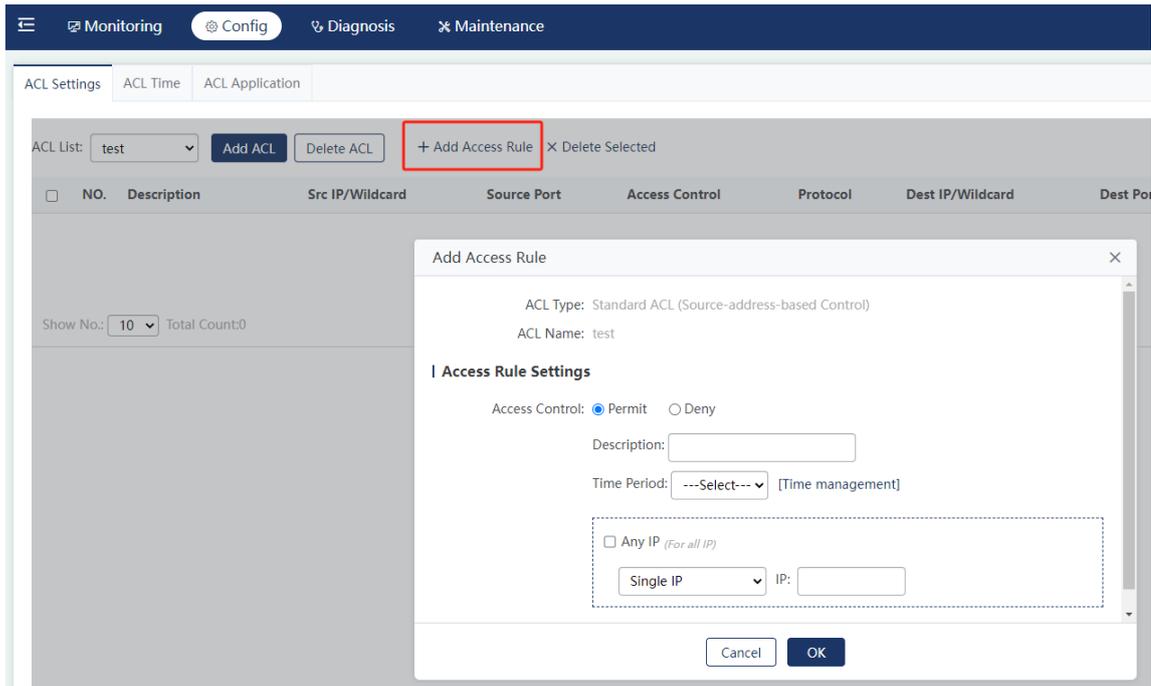
(2) Eliminación de una ACL

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.



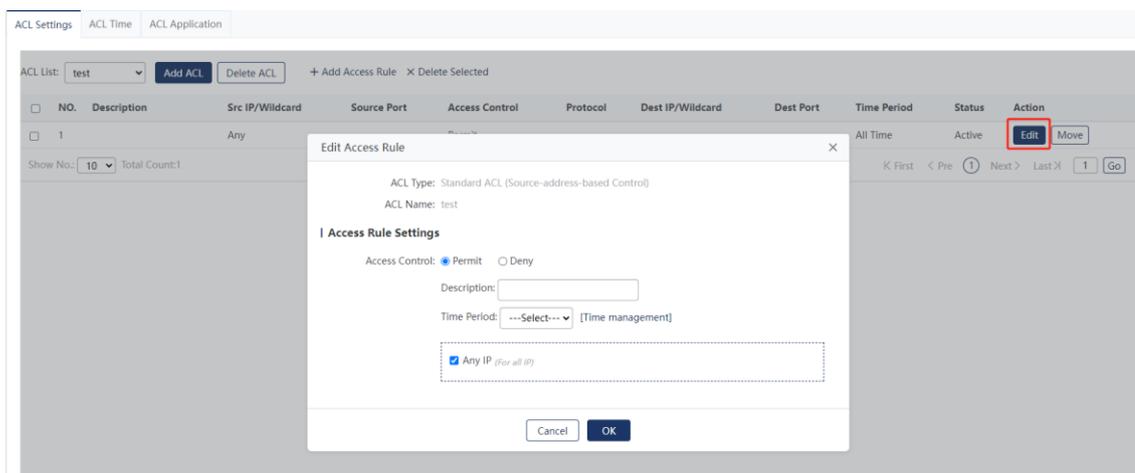
(3) Adición de un ACE

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.



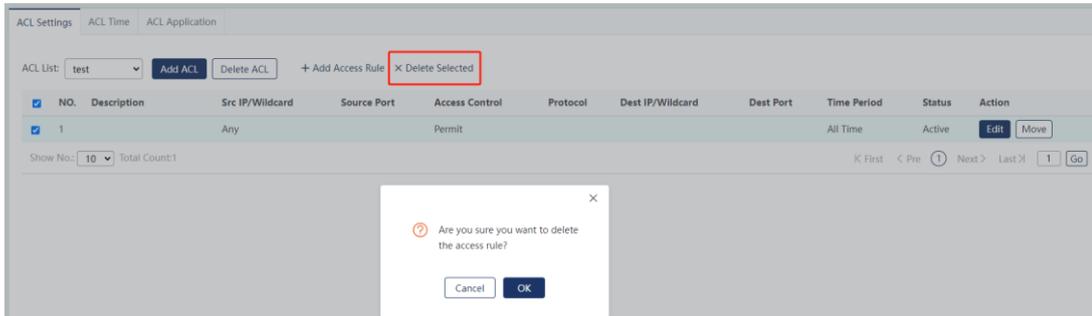
(4) Edición de un ACE

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.



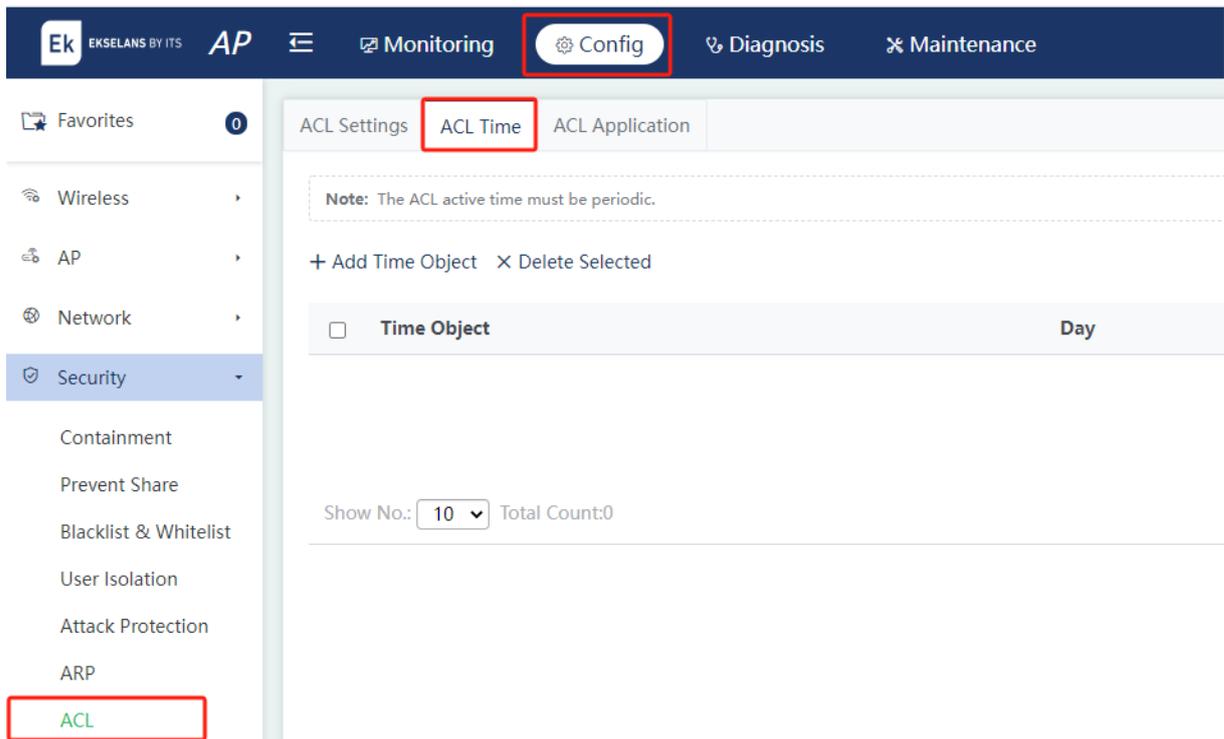
(5) Eliminación de una ACE

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.



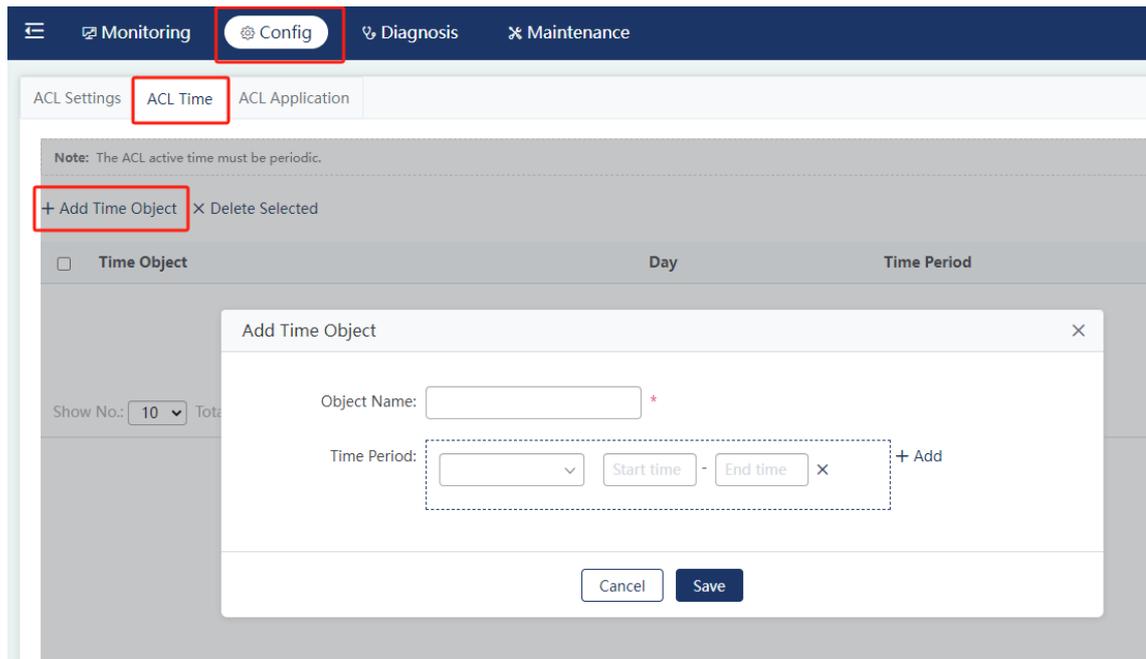
2. Tiempo de ACL

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.



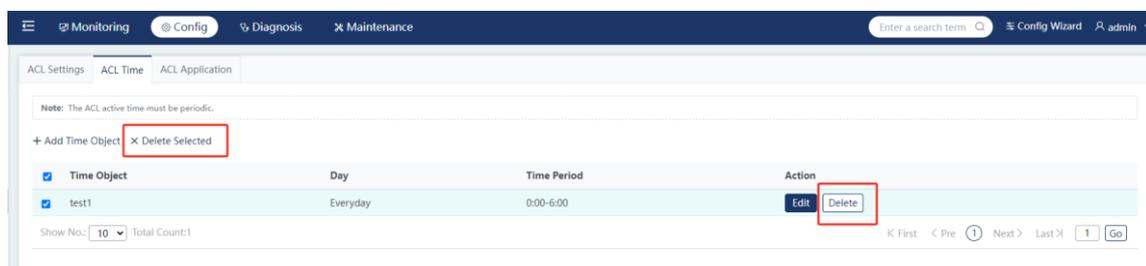
(1) Adición de un objeto de tiempo

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.



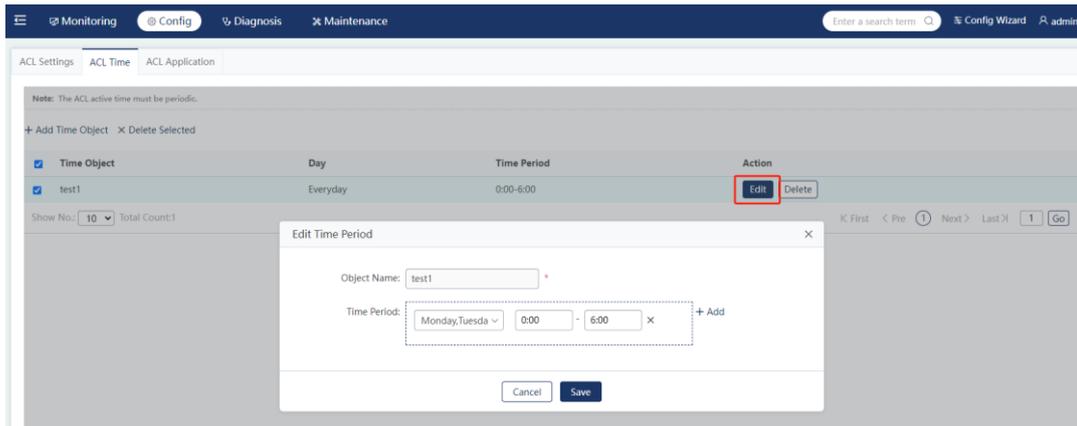
(2) Eliminación de un objeto de tiempo

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.

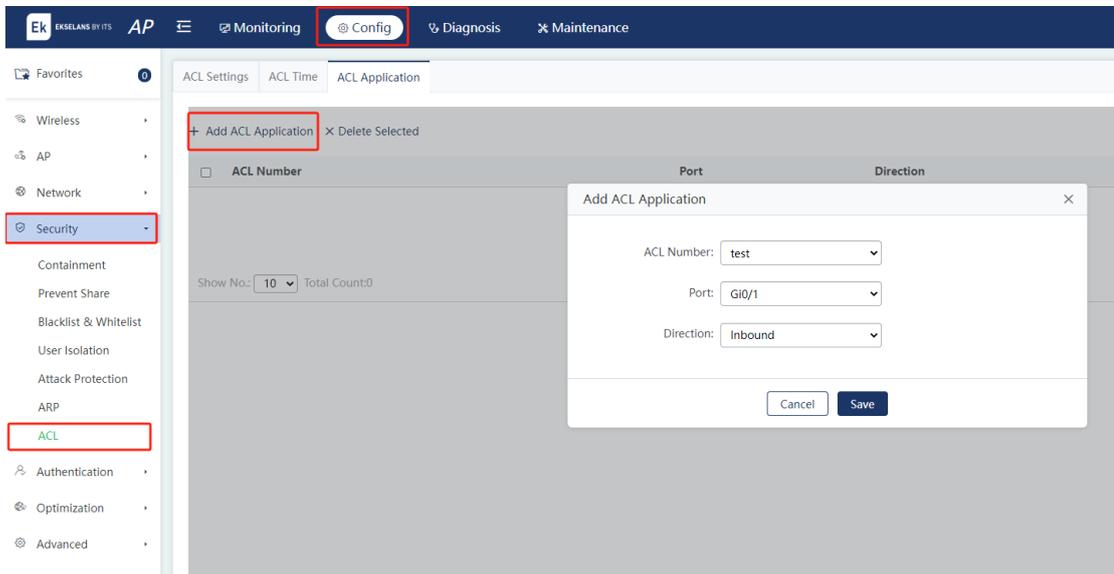


3. Aplicación de ACL

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.

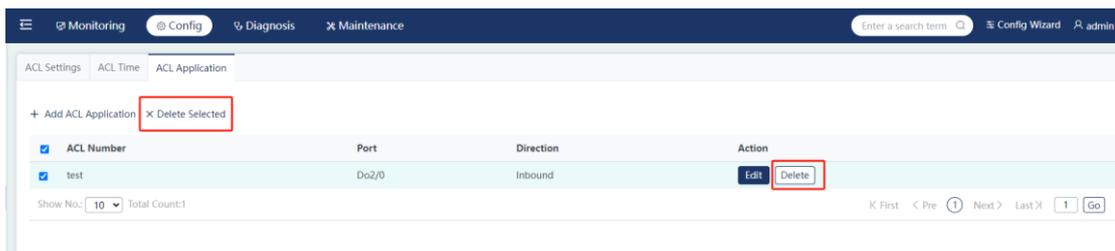
(1) Adición de una aplicación de ACL

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.



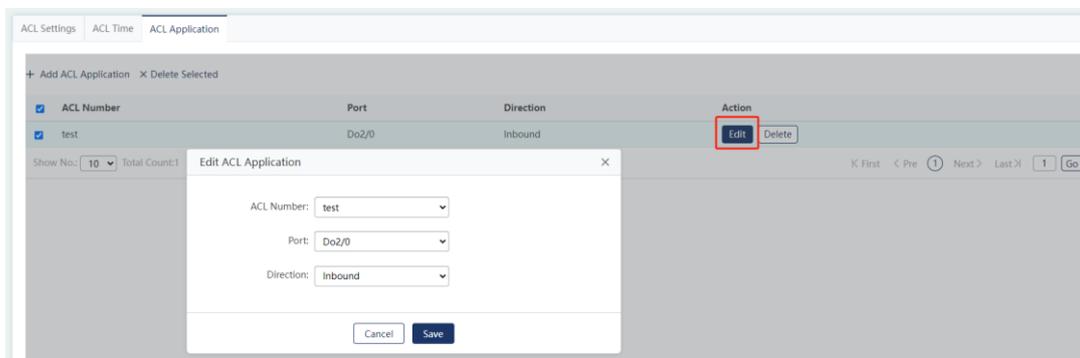
(2) Eliminación de una aplicación de ACL

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 **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.

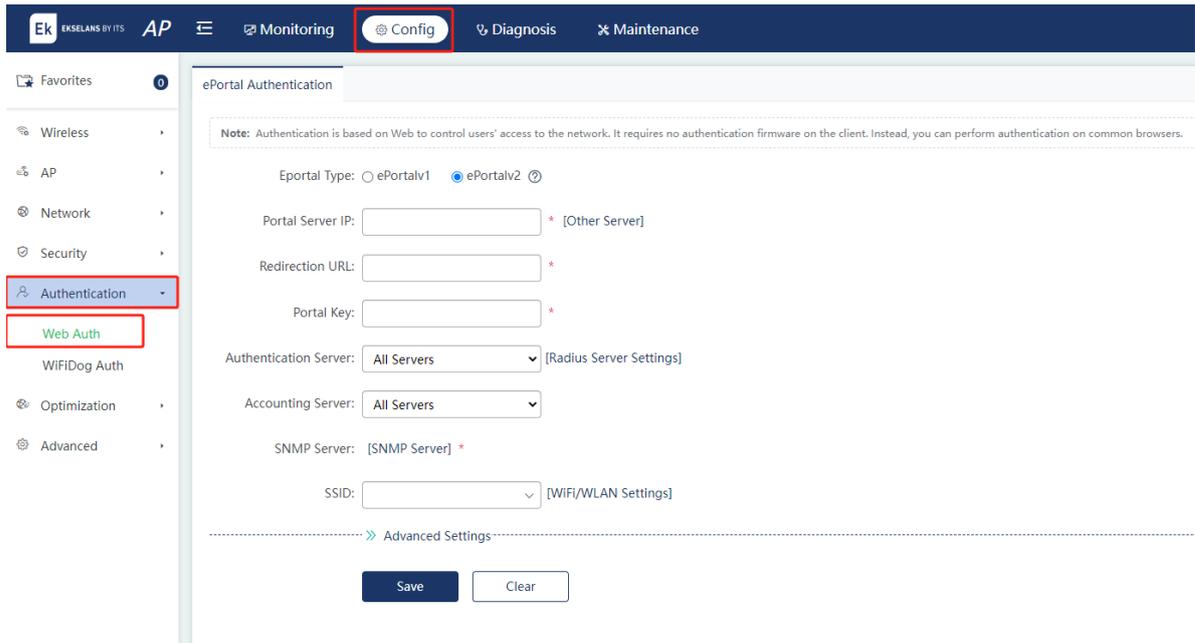
- **ePortalv2**: El servidor del portal es responsable solo de la interacción de la página de usuario y el proceso de autenticación principal se completa en el dispositivo.

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.

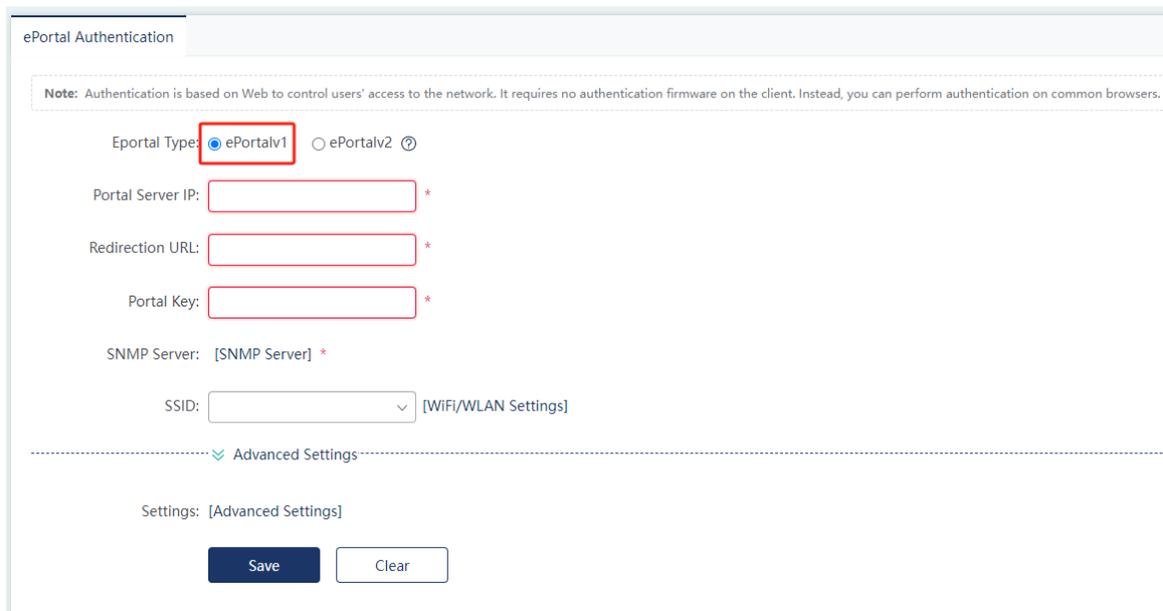
La selección de **ePortalv1** o **ePortalv2** depende del servidor del portal utilizado.

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:

The screenshot shows the 'ePortal Authentication' configuration page. At the top, there are navigation tabs: Monitoring, Config (selected), Diagnosis, and Maintenance. A search bar and 'Config Wizard' are also present. The main content area has a note about authentication being based on Web to control users' access. Below the note, the 'Eportal Type' is set to 'ePortalv2' (highlighted with a red box). Other fields include 'Portal Server IP' (with a red asterisk and '[Other Server]'), 'Redirection URL' (with a red asterisk), and 'Portal Key' (with a red asterisk). There are also dropdown menus for 'Authentication Server' (set to 'All Servers'), 'Accounting Server' (set to 'All Servers'), and 'SSID' (set to '[WIFI/WLAN Settings]'). At the bottom, there are 'Save' and 'Clear' buttons.

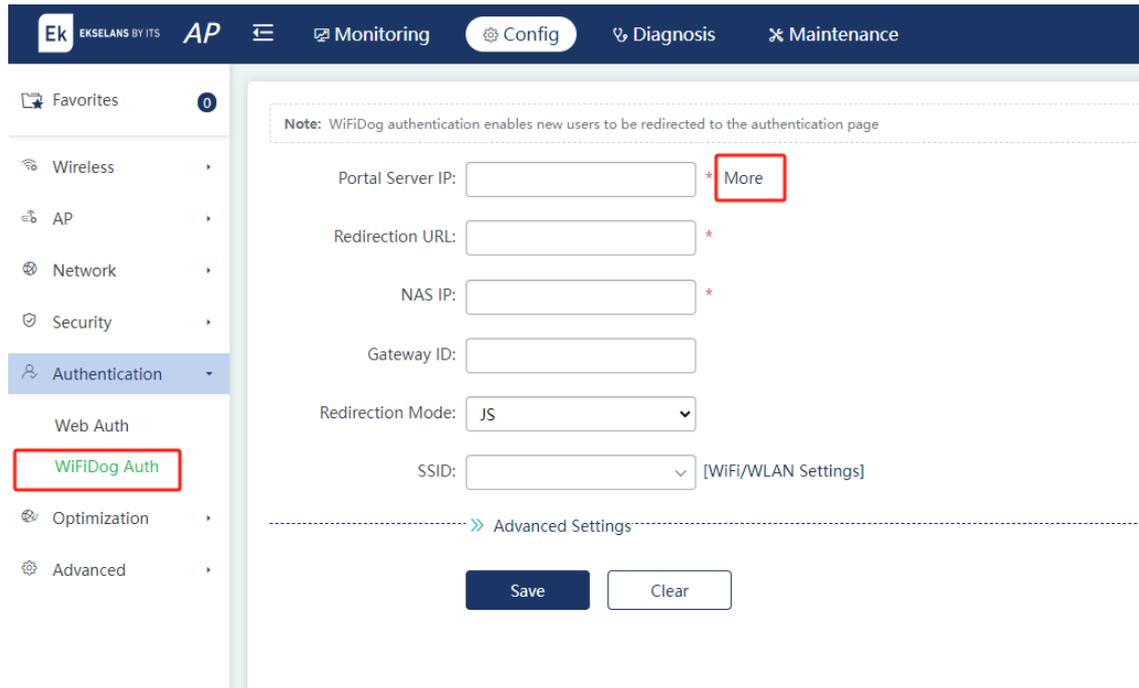
Parámetro	Descripción
IP del servidor del portal	En el modo de configuración de plantilla, ejecute el comando ip { ip-address } para configurar la dirección IP del servidor. Las solicitudes de acceso al servidor están permitidas por el dispositivo y la limitación de velocidad se puede realizar en las 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

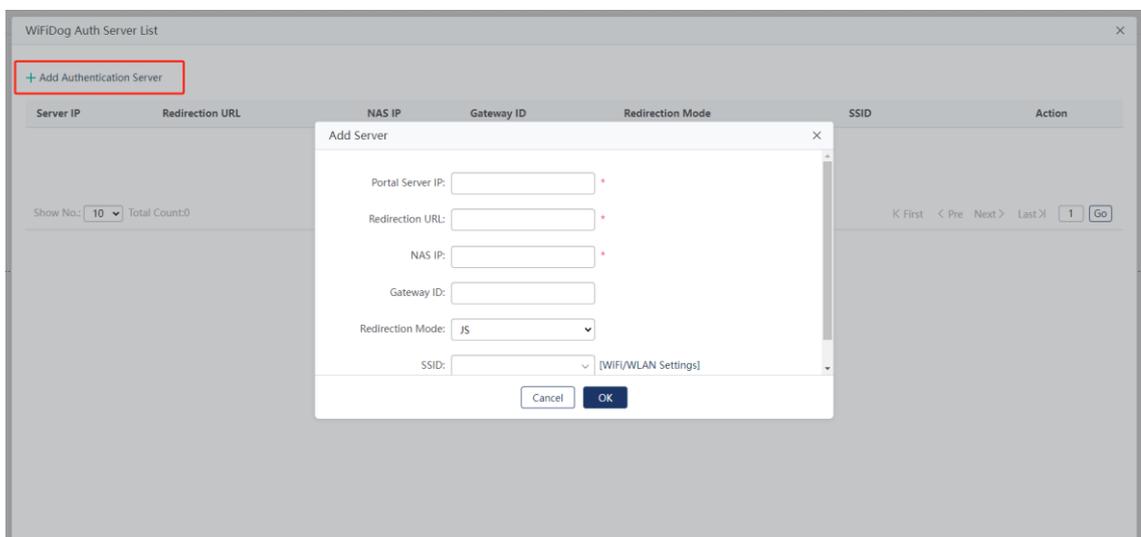
Elija **Config > Authentication > WiFiDog Auth.**

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

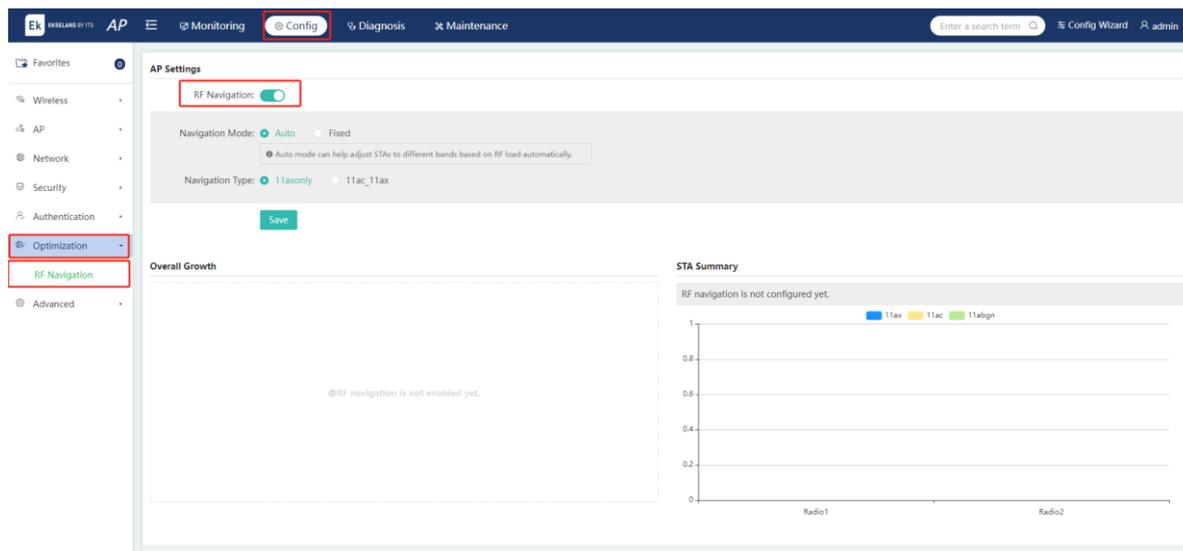
5.6.1 Navegación RF

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

i Nota

Es posible que algunos AP no admitan esta función. Prevalcerá 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.



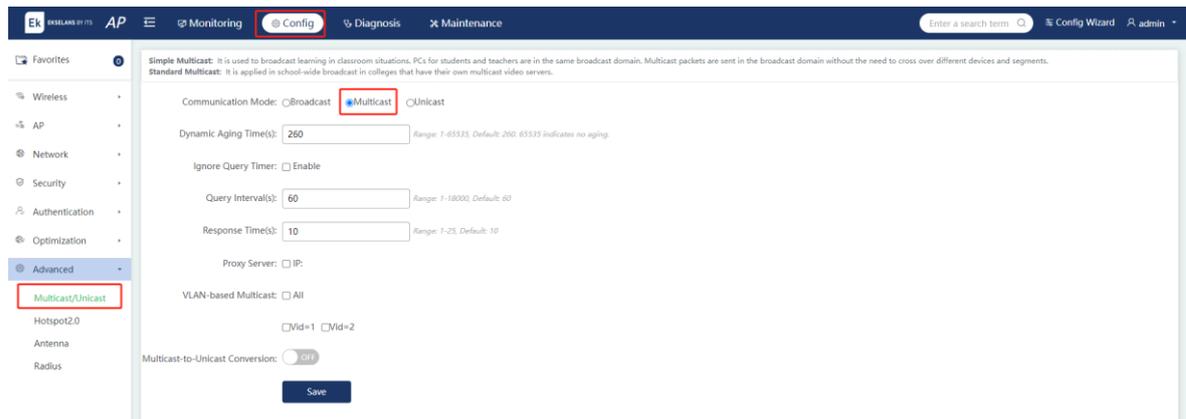
Parámetro	Descripción	
Modo de navegación	Automático	En este modo, el AP puede dirigir automáticamente un STA a la radio óptima en función de la utilización de la carga de radio.
	Fijo	En este modo, el AP dirige un STA a la radio correspondiente, que permanece sin cambios a pesar de las diferencias en 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**.

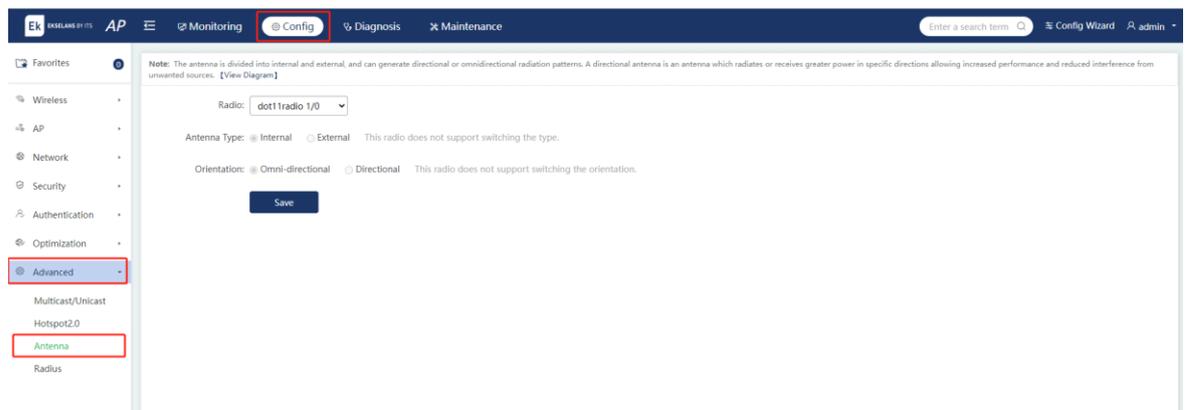
Esta función se utiliza para configurar el modo de comunicación de un dispositivo como difusión, multidifusión o unidifusión.



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.

The screenshot displays the Ek management interface. At the top, the navigation bar includes 'Monitoring', 'Config' (highlighted with a red box), 'Diagnosis', and 'Maintenance'. The left sidebar shows a menu with 'Advanced' selected, and 'Radius' highlighted with a red box. The main content area shows the 'Radius Server' configuration page. It features a 'Server Group' dropdown menu set to 'All Servers', with '+ Add Server' and 'X Delete Selected' buttons. Below this is a table with columns 'Server IP' and 'Authentication Port'. At the bottom, there is a 'Show No.' dropdown set to '10' and a 'Total Count:0' indicator.

Add Server Group✕

Server Group: *

Server Type: New Server Existing Server

Server IP: *

Authentication Port: *

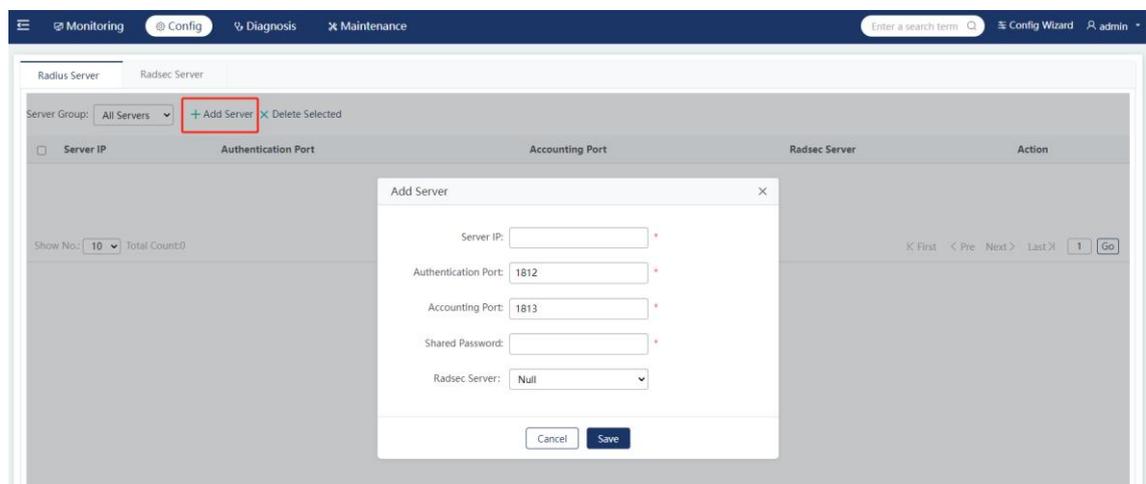
Accounting Port: *

Shared Password: *

Radsec Server: ▼

(2) Adición de un servidor

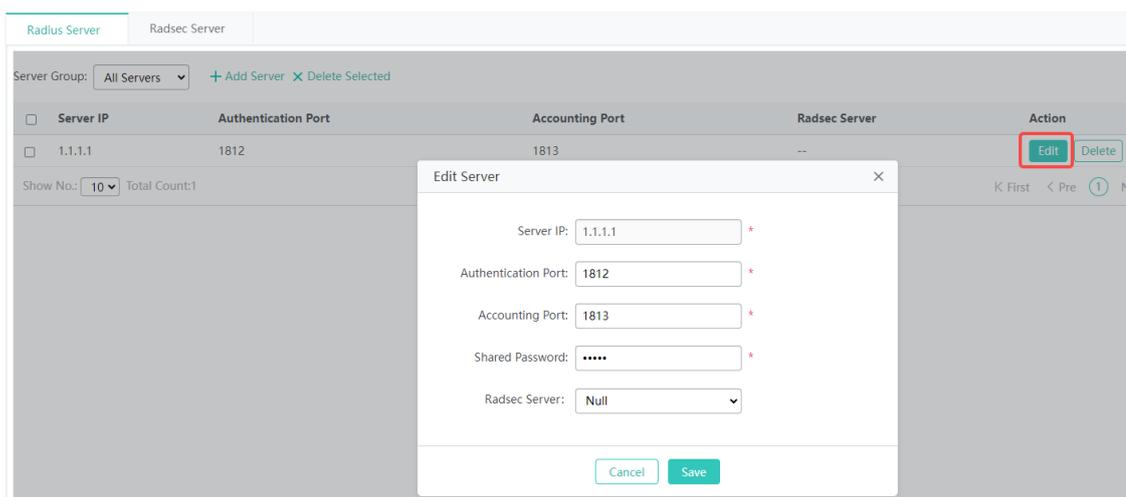
Seleccione **Todos los servidores** en el campo **Grupo de servidores**. Haga clic en **Agregar servidor**. Introduzca los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



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. <hr/> Nota Este campo no se muestra si el dispositivo no es compatible con la función RadSec.

(3) Edición de un servidor

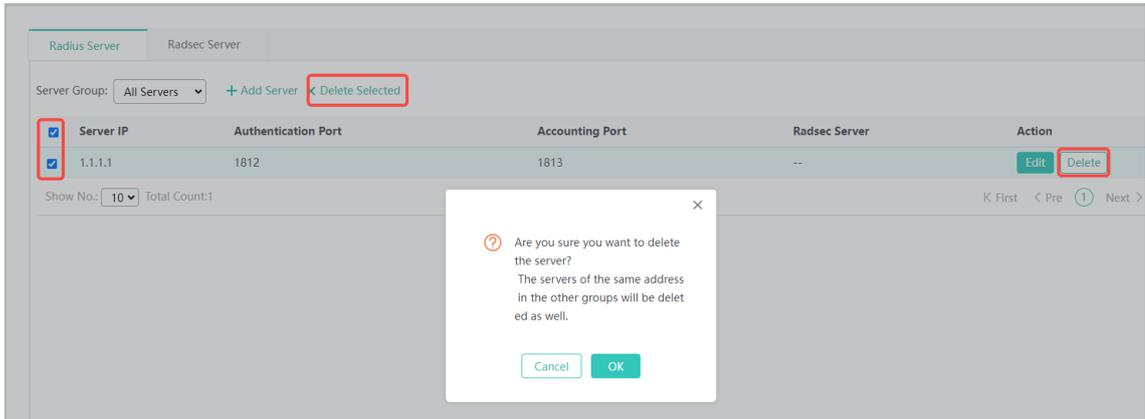
Haga clic **en Editar** en la columna **Acción**. Edite los parámetros en la ventana emergente. Haga clic en **Guardar**.



(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.

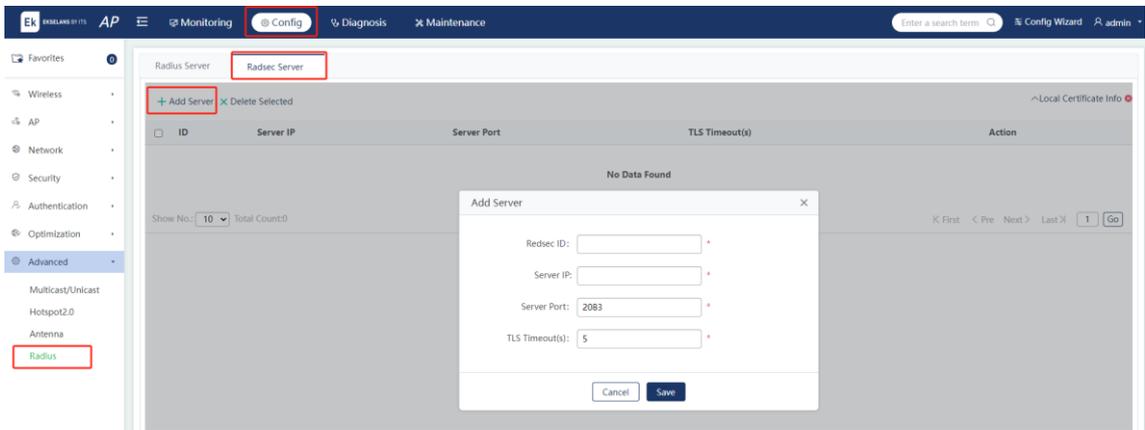


2. Servidor RadSec

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

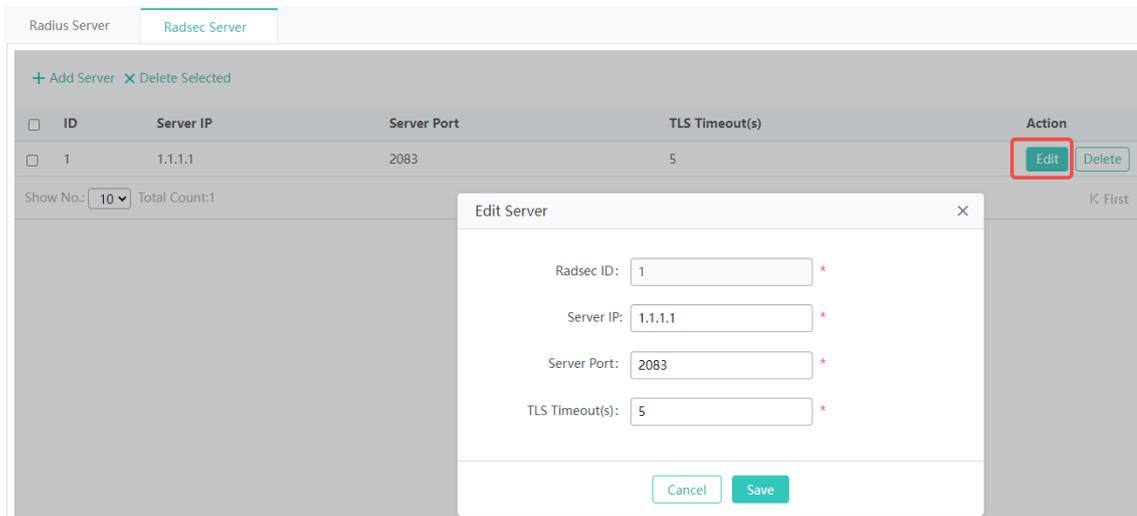
Haga clic en **Agregar servidor**. Introduzca los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



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.

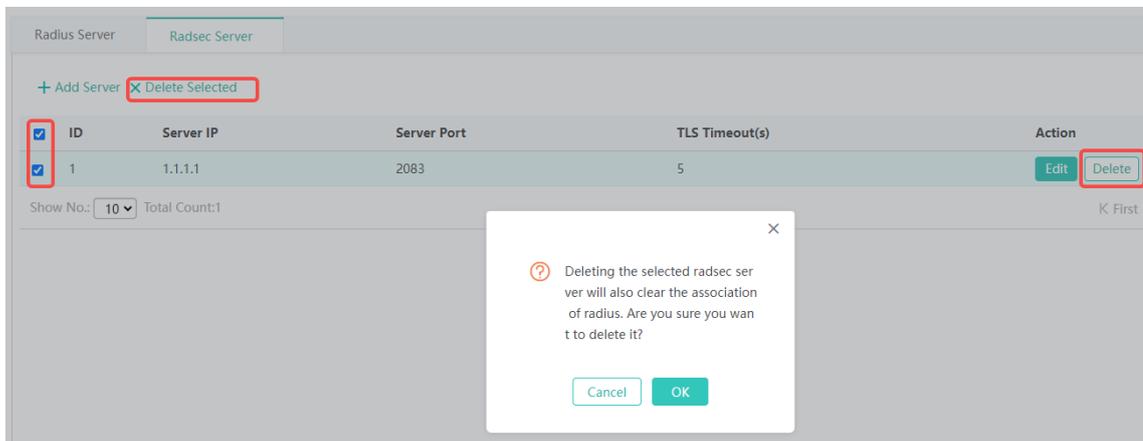
(2) Edición de un servidor

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



(3) Eliminación de un servidor

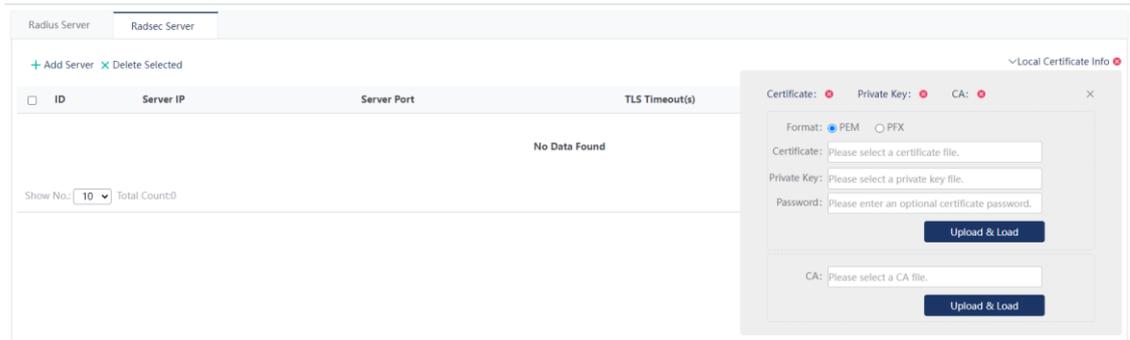
Haga clic en **Eliminar** en la columna **Acción** y haga clic en **Aceptar** en la ventana emergente para eliminar un servidor. Para eliminar varios servidores, seleccione los servidores de destino en la lista. Haga clic en **Eliminar** seleccionados. Haga clic en **Aceptar** en la ventana emergente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



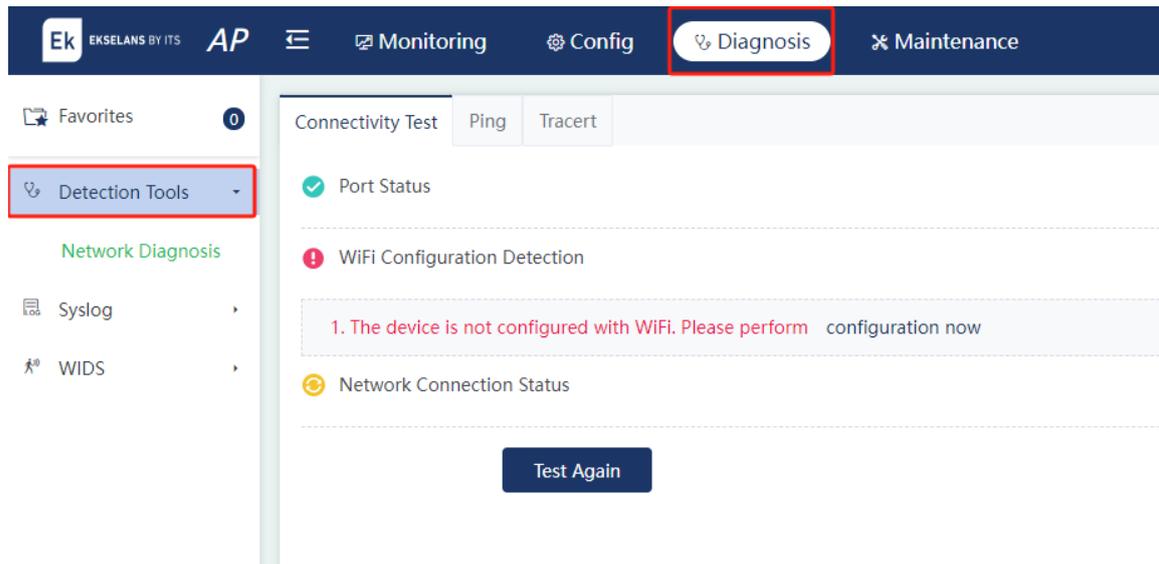
6 Diagnóstico

6.1 Herramientas de detección

6.1.1 Diagnóstico de red

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

1. Prueba de conectividad

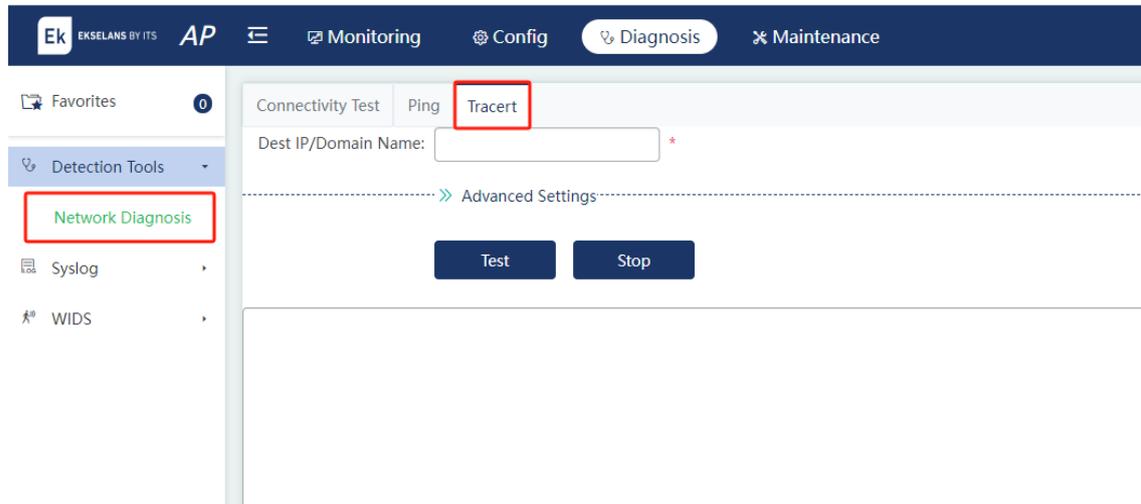


Elemento de detección	Descripción
Estado del puerto	Compruebe si un puerto del AP está activo.
Detección de configuración WiFi	Compruebe si hay una red Wi-Fi configurada en el AP.
Estado de la conexión de red	Compruebe si el AP puede comunicarse con una red externa.

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



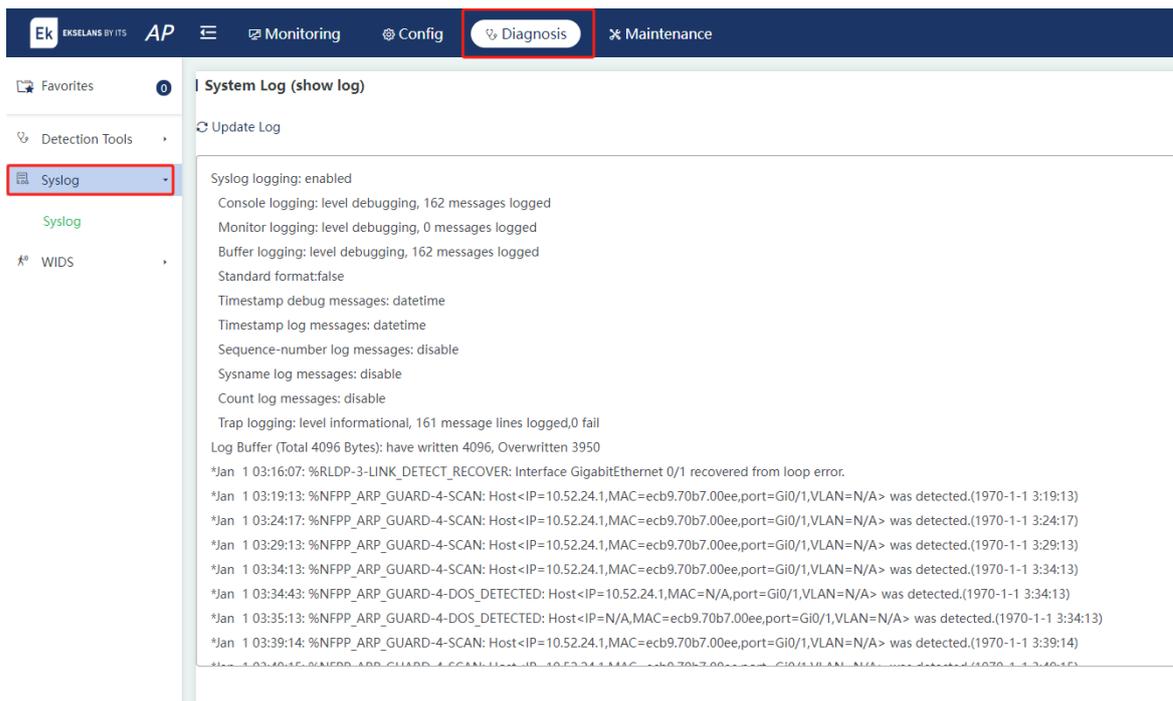
Parámetro	Descripción
IP de destino/Nombre de dominio	Introduzca la dirección de destino o el nombre de dominio de Tracert.
IP de origen	Introduzca la dirección de origen de Tracert, es decir, la dirección de la interfaz local del dispositivo.
Intervalo(s) de tiempo de espera	Introduzca el intervalo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



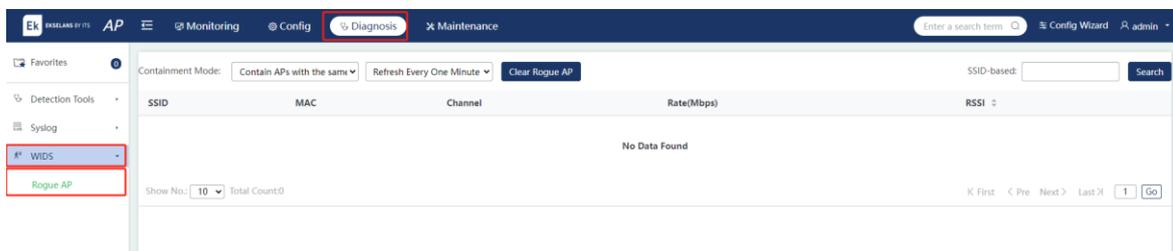
6.3 Sistema inalámbrico de detección de intrusos

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

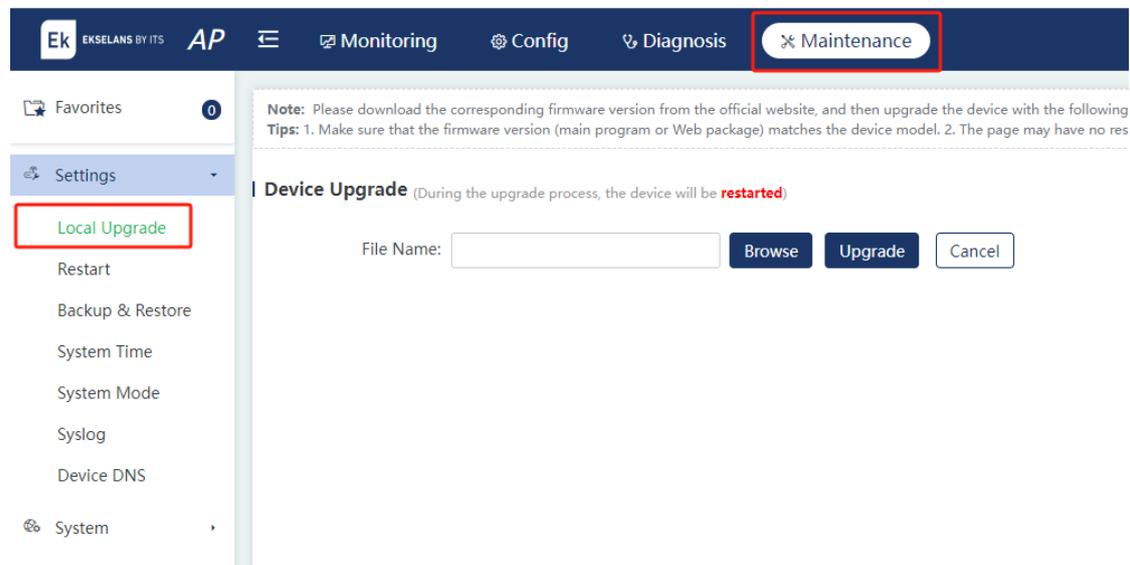
7.1.1 Actualización local

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.



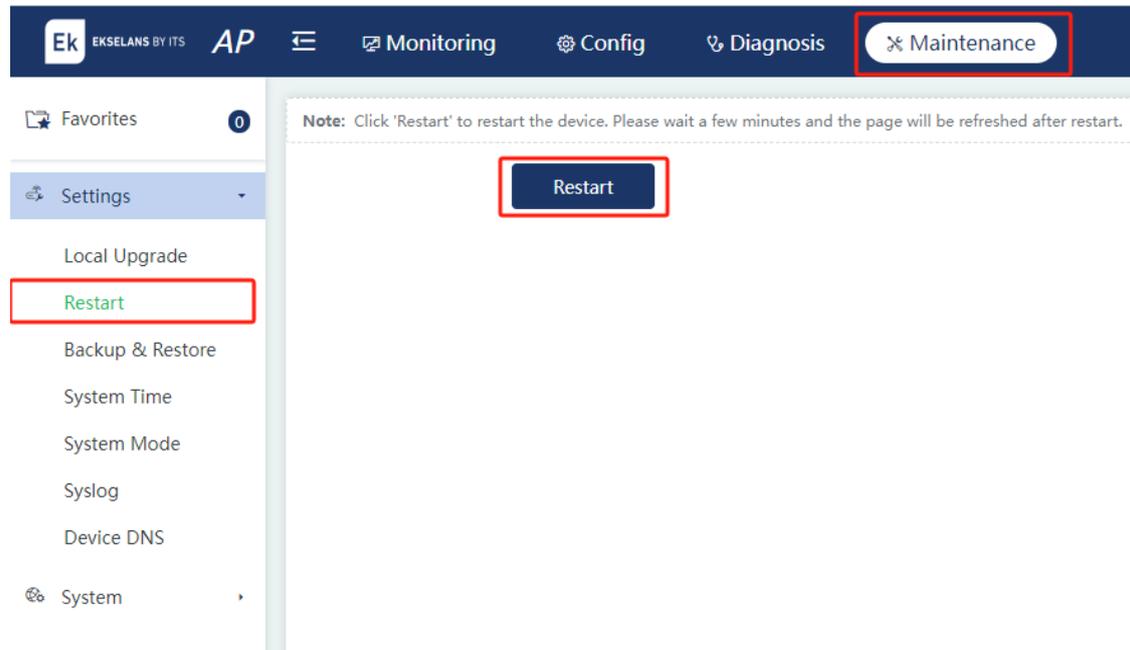
7.1.2 Reanudar

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.

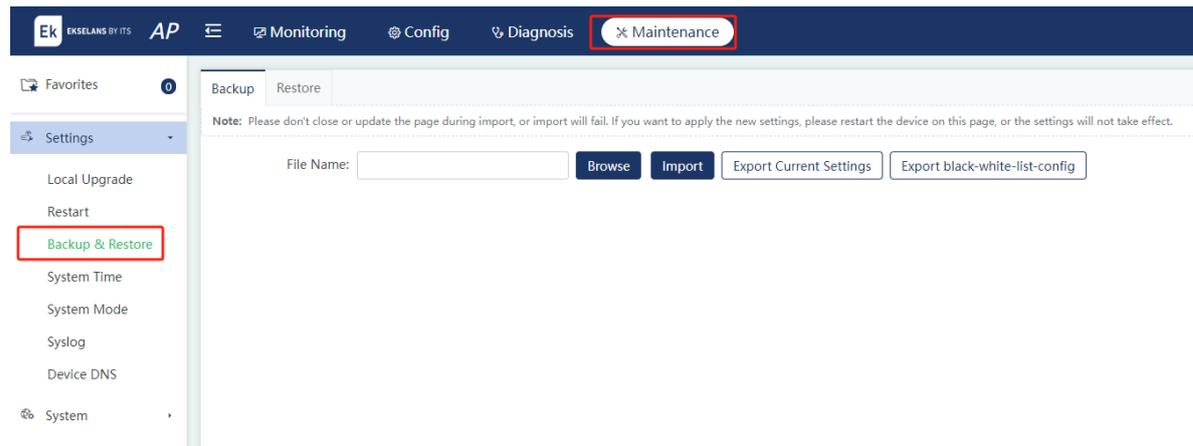


7.1.3 Gestión de la configuración

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

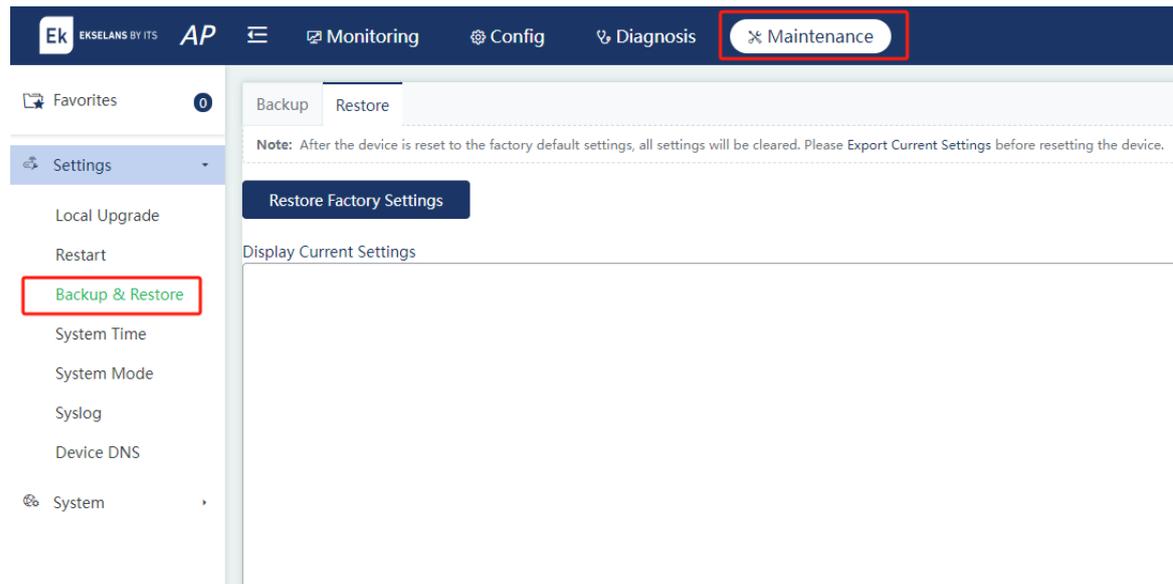
1. Copia de seguridad

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

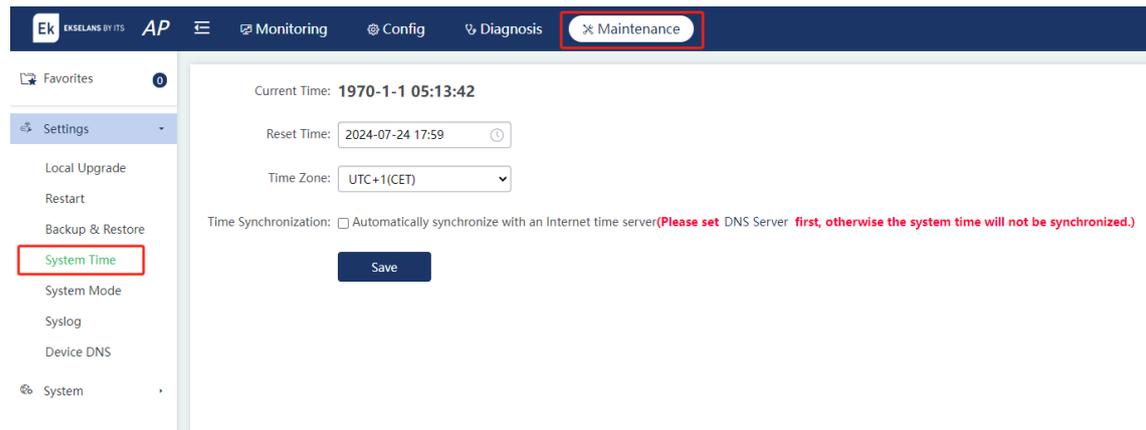
Después de restaurar el dispositivo a la configuración de fábrica, use la dirección IP predeterminada para acceder a la web. Al restaurar el dispositivo a la configuración de fábrica, se borrarán todas las configuraciones. Por lo tanto, haga ejercicio con precaución.



7.1.4 Hora del sistema

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

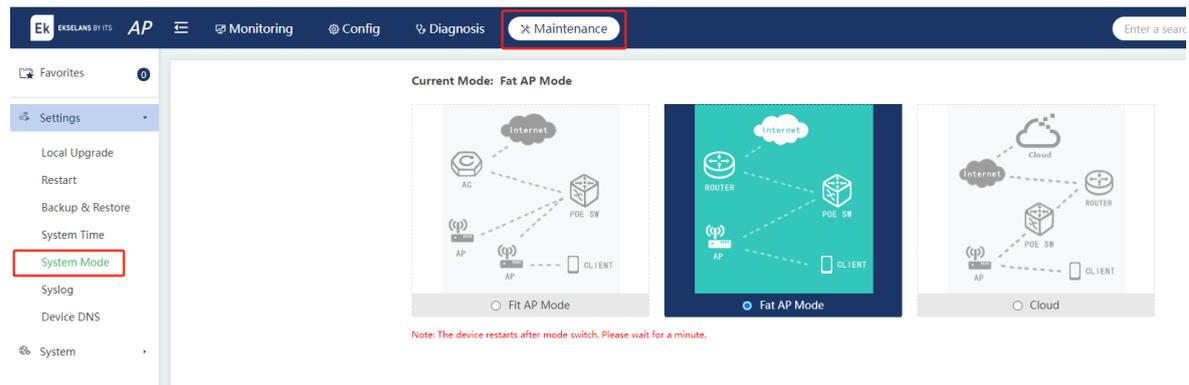
Establezca la hora del sistema en función de la zona horaria en la que se encuentra el dispositivo para garantizar una información precisa del dispositivo.



7.1.5 Modo de sistema

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

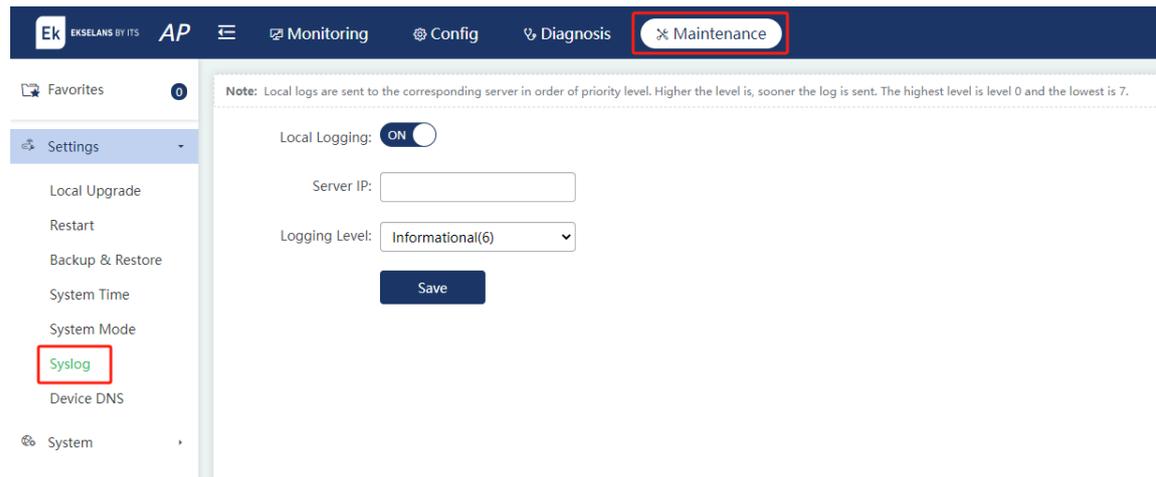
Seleccione el modo de sistema del AP. **Son compatibles con el modo Fit AP, el modo Fat AP y el modo Cloud.**



7.1.6 Servidor de registro

Seleccione **Mantenimiento > Configuración > Syslog**.

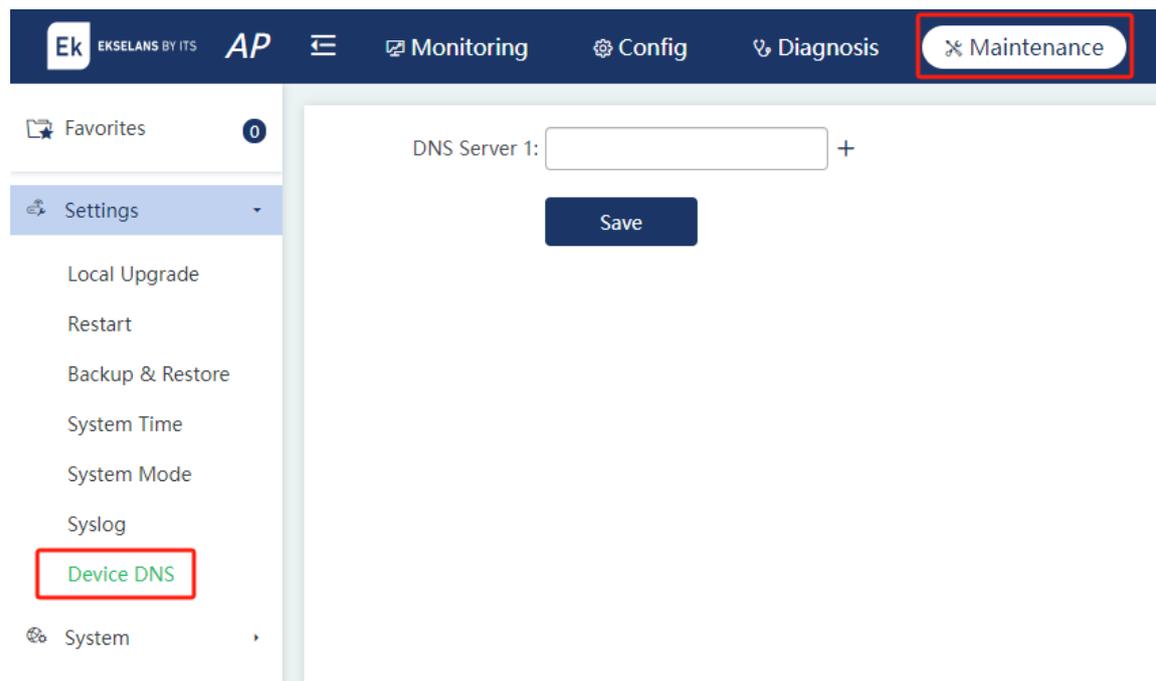
El dispositivo envía registros locales al servidor para su almacenamiento. Los registros históricos se almacenan para facilitar la consulta.



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.

The screenshot shows the Ek web interface. The top navigation bar includes 'Ek EKSELANS BY ITS', 'AP', 'Monitoring', 'Config', 'Diagnosis', and 'Maintenance' (highlighted with a red box). The left sidebar shows 'Favorites', 'Settings', 'System', and 'Web' (highlighted with a red box). The main content area displays the 'Admin Password' configuration page with the following fields:

- Username: admin
- Old Password: *
- New Password: *
- Confirm Password: *

A 'Save' button is located at the bottom of the form.

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).

The screenshot shows the Ek web interface. The top navigation bar includes 'Ek EKSELANS BY ITS', 'AP', 'Monitoring', 'Config', 'Diagnosis', and 'Maintenance' (highlighted with a red box). The left sidebar shows 'Favorites', 'Settings', 'System', and 'Web' (highlighted with a red box). The main content area displays the 'Basic Settings' configuration page with the following fields:

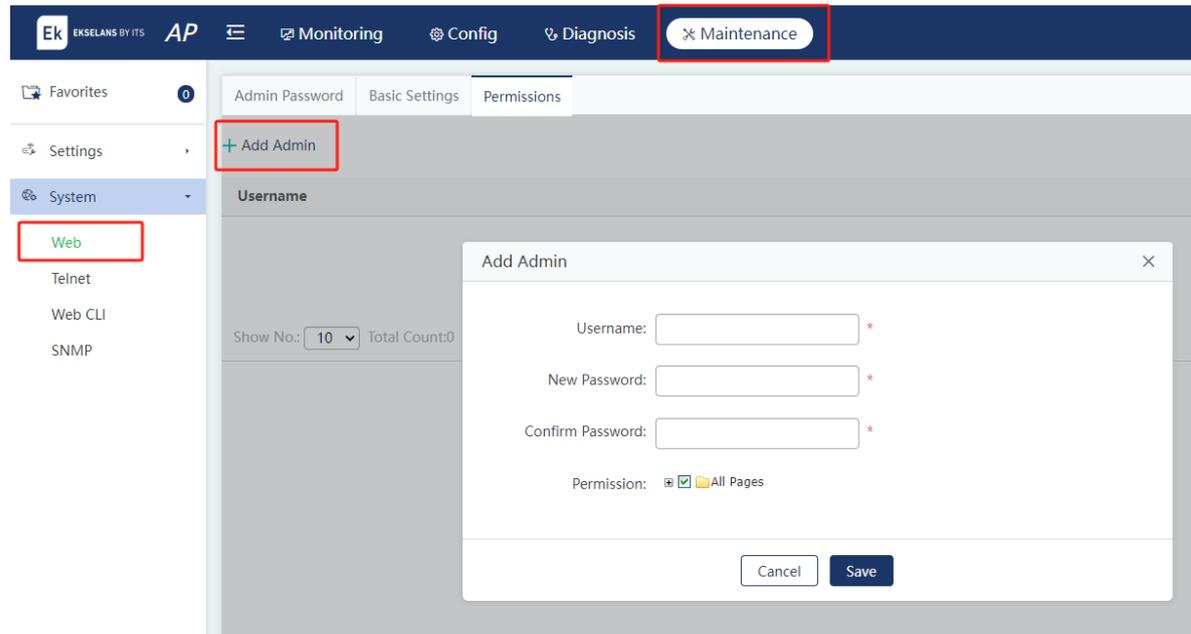
- Web Access Port: * (Range: 443,1025-65535)
- Login Timeout: ▼
- Device Location:
- Access Redirection: HTTP Redirection to HTTPS In NAT scenario, redirection may cause HTTP access failure.

A 'Save' button is located at the bottom of the form.

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.

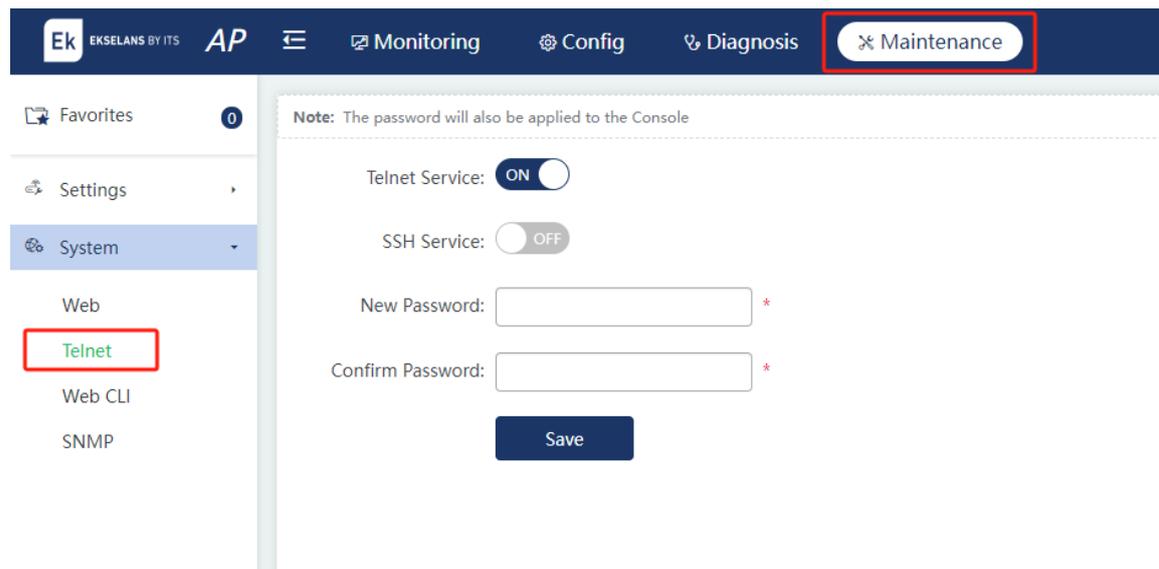
Haga clic en **Agregar administrador**. Establezca los campos para un administrador en la ventana emergente, incluidos el nombre de usuario, la contraseña y los permisos. Haga clic en **Guardar**.



7.2.2 Telnet

Seleccione **Mantenimiento > Sistema > Telnet**.

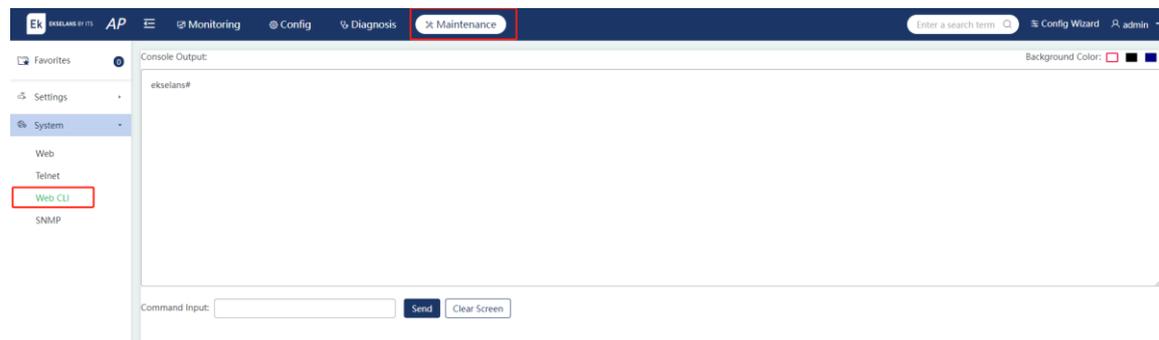
La función Telnet mejora la seguridad del sistema y garantiza un intercambio seguro de información. En la **página Telnet**, el **servicio Telnet** y el **servicio SSH** se pueden habilitar o deshabilitar, y se puede configurar la contraseña.



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.

The screenshot shows the Ek web interface. At the top, there is a navigation bar with the Ek logo, 'EKSELANS BY ITS', 'AP', and menu items: Monitoring, Config, Diagnosis, and Maintenance (highlighted with a red box). On the left, a sidebar contains 'Favorites', 'Settings', 'System' (expanded), 'Web', 'Telnet', 'Web CLI', and 'SNMP' (highlighted with a red box). The main content area is the 'SNMP' configuration page. It features a note: 'Note: Either SNMPv2 or SNMPv3 is supported'. Below this, there are radio buttons for 'v2' (selected) and 'v3'. The configuration fields include: 'Device Location' (text input), 'SNMP Community' (text input with a red asterisk), 'Trap Community' (text input with a note: 'The Trap Community must be the same as the SNMP Community.'), and 'Trap Receiver Address' (text area with a note: '* You can configure up to 10 Trap receivers. Please use ";" or press the Enter key to separate addresses.'). A 'Save' button is located at the bottom of the configuration area.