



EKSELANS BY ITS

MANUAL DE USUARIO

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

1 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 AC.

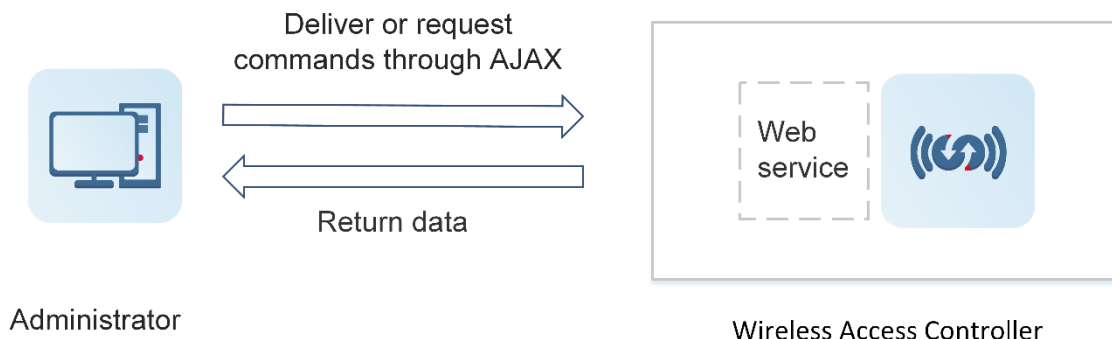
El sistema de gestión web involucra un servidor web y un cliente web. El servidor web está integrado en el dispositivo para recibir y procesar las solicitudes de un cliente. A continuación, devuelve los resultados del procesamiento al cliente. Los clientes web suelen referirse a navegadores web, como Internet Explorer y Google Chrome.

1.2 Conexión al dispositivo

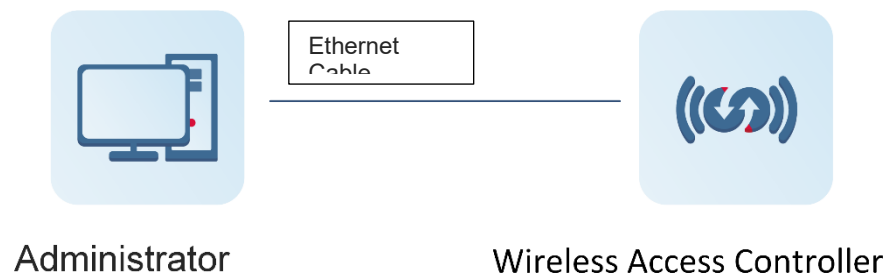
El sistema de gestión web involucra un servidor web y un cliente web. El servidor web está integrado en el dispositivo para recibir y procesar las solicitudes de un cliente. A continuación, devuelve los resultados del procesamiento al cliente. Los clientes web suelen referirse a navegadores web, como Internet Explorer y Google Chrome.

Como se muestra en la siguiente figura, el administrador configura los dispositivos a través del sistema de administración web en el navegador web.

Topología de la aplicación



Topología simplificada



El sistema de administración web funciona ensamblando varios comandos de dispositivo y enviándolos al dispositivo a través de solicitudes asíncronas de JavaScript y XML (AJAX). El

dispositivo responde con datos relevantes. Las solicitudes HTTP básicas pueden ser controladas por el servicio web en el dispositivo.

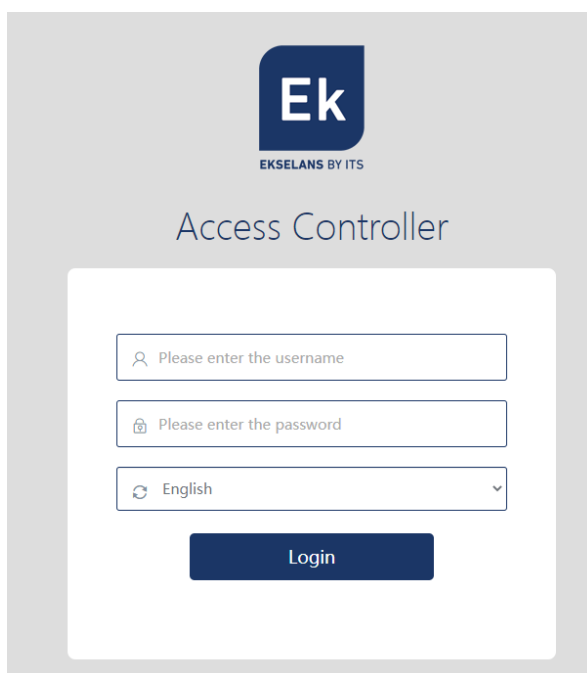
1.3 Entorno de configuración para clientes de PC

- El administrador inicia sesión en el sistema de administración web para administrar dispositivos a través del explorador web en el cliente de administración web. Los clientes generalmente se refieren a PC, pero también pueden incluir otros dispositivos terminales móviles, como computadoras portátiles y iPads. El teléfono móvil no es compatible por ahora.
- Navegador web: se recomienda Google Chrome e Internet Explorer 11 también es compatible. Pueden producirse excepciones, como caracteres ilegibles o errores de formato, si se utiliza un navegador no compatible.
- Resolución: Se recomienda establecer la resolución en 1280 píxeles x 1024 píxeles, 1920 píxeles x 1080 píxeles o 1440 píxeles x 960 píxeles. El uso de otras resoluciones puede dar lugar a un formato desalineado y menos atractivo visualmente.

1.4 Entorno de servicios web para AC

- El AC está habilitado con el servicio web.
- El AC se configura con el nombre de usuario y la contraseña para registrar la autenticación.
- El AC se configura con una dirección IP de administración.

Una vez que el servicio web esté habilitado y la dirección IP esté configurada correctamente, introduzca la dirección IP en la barra de direcciones del explorador, como <http://X.X.X.X> (IP de administración). Pulse **Intro** y se mostrará la siguiente página:



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 predeterminado	Descripción
admin/admin	Superadministrador con permisos completos.

1.5 Habilitación del servicio web

El AC 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).

Elemento de configuración	Mandar	
Configura el 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 administración web.

1.5.1 Pasos de configuración

➤ Habilitación del servicio web

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

➤ Configuración de la 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 **guest** e **guest** respectivamente de forma predeterminada. Los usuarios pueden cambiar y crear cuentas.

1.5.2 Verificación

Inicie sesión en el sistema de administración web con la dirección IP configurada y la cuenta de administración web para comprobar si puede iniciar sesión correctamente.

1.5.3 Comandos relacionados

➤ Habilitación del servicio web

Mandar	Habilitar servidor web de servicio [todos http https]
Descripción del parámetro	Todos http https: Indica la habilitación de diferentes servicios . all indica la habilitación de los servicios HTTP y HTTPS. http indica la habilitación del servicio HTTP. https indica la habilitación del servicio HTTPS. Los servicios HTTP y HTTPS están habilitados de forma predeterminada.
Modo de comando	Modo de configuración global

↘ Configuración de la dirección IP

Mandar	dirección IP dirección IP máscara de IP
Descripción del parámetro	<i>ip-address:</i> Indica la dirección IP. <i>mask:</i> Indica la máscara de red.
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

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

1.5.4 Ejemplo de configuración

Pasos de configuración	<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 Hostname(config)# interfaz vlan 1 Hostname(config-if-VLAN 1)# dirección ip 192.168.1.200 255.255.255.0 Hostname(config)# end </pre>
-------------------------------	---

Verificación

Ejecute el **comando show running-config** para verificar el resultado de la configuración.

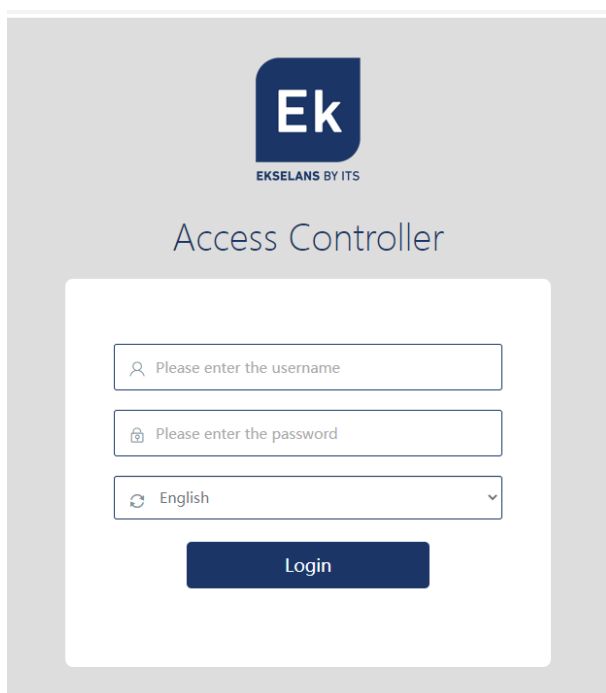
```
Hostname(config)# show running-config
Configuración del edificio...
Configuración actual : 6312 bytes

!
hostname Nombre de host
!
!
webmaster level 0 username test password test //Indica el nombre de
usuario y la contraseña para la autenticación de administración web. La
contraseña está encriptada.
Detección automática del modo de actualización HTTP
!
!
VLAN de interfaz 1
    dirección IP 192.168.1.200 255.255.255.0 //Indica la dirección IP de
administración del dispositivo.
    Sin apagado
!
línea con 0
línea vty 0 4
    Iniciar sesión
!
!
Fin
```

2 Configuración rápida

2.1 Inicio de sesión en el sistema de gestión web

Se le pedirá que cambie la contraseña la primera vez que inicie sesión en el sistema de administración web. Se recomienda establecer una contraseña compleja. Utilice la nueva contraseña la próxima vez que inicie sesión. Si ingresa contraseñas incorrectas cinco veces consecutivas en 10 minutos, su cuenta se bloqueará durante 10 minutos.

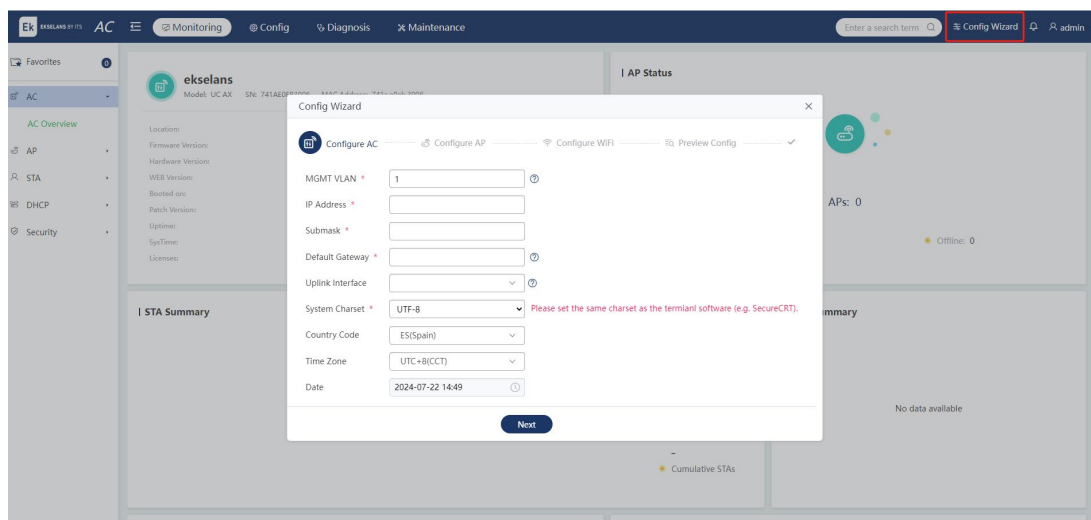


2.2 Asistente de configuración

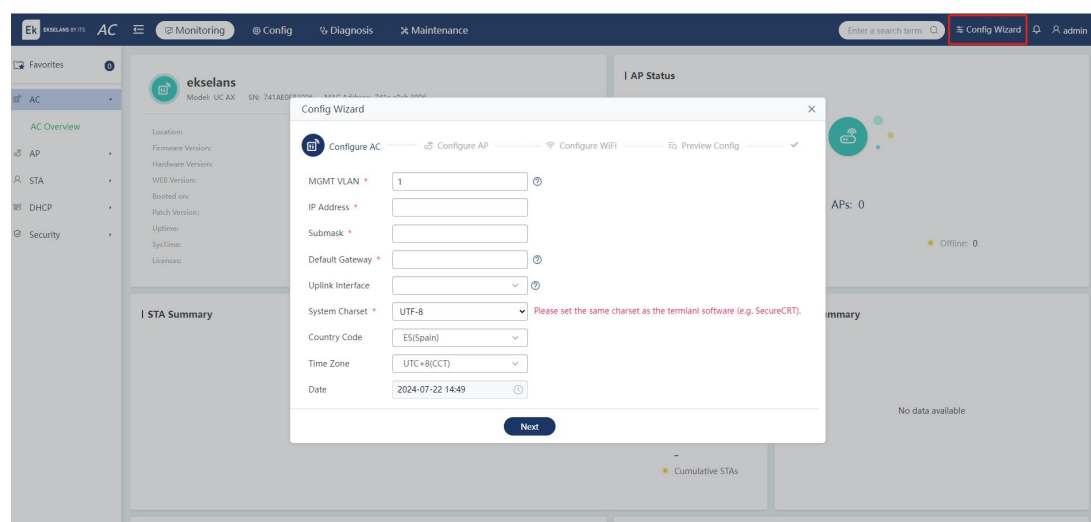
El asistente rápido se utiliza normalmente para la primera configuración. Haga clic en **Asistente de configuración** en la barra de navegación. Proporciona algunas configuraciones comunes basadas en escenarios.

1. Si no se encuentra ningún archivo config.text, es decir, el dispositivo actual aún no está configurado, 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 cuatro pasos: Configurar CA, Configurar AP, Configurar Wi-Fi y Vista previa de la configuración.



2.2.1 Configurar AC



Parámetro	Descripción
MGMT VLAN	Introduzca la VLAN para que la AC se comunice con una red externa y para que los usuarios visiten el sistema de gestión web.
Dirección IP	Introduzca la dirección IP para que el AC se comunice con una red externa y para que los usuarios visiten el sistema de gestión web. También es la dirección IP predeterminada del túnel entre el AC y el AP.
Submascarilla	Introduzca la submáscara IP para que el AC se comunice con una red externa.
Puerta de enlace predeterminada	Introduzca la puerta de enlace de salida.
Interfaz de enlace ascendente	Ingresa a la interfaz que conecta la AC y su dispositivo de enlace ascendente.

Juego de caracteres del sistema	Introduzca el conjunto de caracteres del sistema y el valor predeterminado es la codificación UTF-8. Si tiene la intención de utilizar otras herramientas cliente, se recomienda utilizar también la codificación UTF-8. De lo contrario, puede producirse una mezcla de código, lo que puede dar lugar a problemas de configuración o texto ilegible en la página.
Código de país	Introduzca el país o la región en la que se encuentra el dispositivo. Las regulaciones para las bandas, los canales y la potencia de RF varían en diferentes países o regiones.
Huso horario	Introduzca la zona horaria en la que se encuentra el dispositivo.
Fecha	Introduzca la hora del dispositivo.

2.2.2 Configurar AP

(1) **El AP está en VLAN:** Configure la VLAN para el AP. De forma predeterminada, es lo mismo que la VLAN de administración.

(2) Conjunto de direcciones AP en:

Si selecciona **Otro dispositivo**, configure el grupo de direcciones AP en otros dispositivos después de finalizar este proceso.

Config Wizard

✓ Configure AC **Configure AP** Configure WiFi Preview Config ✓

AP is in VLAN *

Interface Address ?

Submask

AP Address Pool on ☐ AC ☒ Other Device

AC Tunnel Address * ?

Previous Next

Si selecciona **CA**, configure la red del grupo de direcciones, la submáscara, la puerta de enlace del grupo y otros parámetros. La dirección de servidor DNS predeterminada es 8.8.8.8.

Config Wizard

Configure AC (selected) | Configure AP | Configure WiFi | Preview Config

AP is in VLAN * 1

Interface Address 10.52.24.237 ⓘ

Submask 255.255.248.0

AP Address Pool on ☒ AC ☐ Other Device

Address Pool 10.52.24.0

Network *

Submask * 255.255.248.0

Pool Gateway * 10.52.24.237

DNS * 8.8.8.8

Option 138 * 10.52.24.237

Previous Next

2.2.3 Configurar Wi-Fi

Las redes Wi-Fi están asociadas con grupos de puntos de acceso predeterminados en **el Asistente de configuración**.

Config Wizard

Configure AC | Configure AP (selected) | Configure WiFi | Preview Config

Dual Radio Into One ☒ ON ⓘ

SSID * EKWIFI

Encryption Type Open WPA/WPA2-PSK WPA3-PERSONAL

WiFi Password ekwifi ⓘ

Forwarding Mode ☒ Centralized Forwarding ☐ Local Forwarding ⓘ

STA is in VLAN * 1

Interface Address 10.52.24.237 ⓘ

Submask 255.255.248.0

STA Address Pool ☐ AC ☒ Other Device

Previous Next

Parámetro	Descripción
Radio dual en una	Está habilitado de forma predeterminada, lo que indica que una red Wi-Fi transmite señales de 2,4 GHz y 5 GHz. Si está desactivado, se configuran dos redes Wi-Fi, una para señales de 2,4 GHz y otra para señales de 5 GHz.
SSID	Establezca el SSID.

Tipo de cifrado	<p>Abierto: no se ha configurado ningún método de cifrado. No se requiere contraseña cuando el STA se conecta a la red Wi-Fi.</p> <p>WPA/WPA2-PSK: El modo WPA con una clave precompartida presenta alta seguridad y fácil configuración, aplicable a hogares y pequeñas empresas.</p> <p>WPA3-Personal: En comparación con WPA2, es más seguro y capaz de prevenir ataques de diccionario.</p>
Modo de reenvío	<p>Reenvío centralizado: Todos los datos se enrutan a través de la AC antes de ser reenviados a otros dispositivos. Este modo está configurado de forma predeterminada.</p> <p>Reenvío local: Los datos se reenvían a otros dispositivos directamente desde el switch, lo que reduce la carga en la CA.</p>
STA está en VLAN	Configure la VLAN para el STA.
Grupo de direcciones de STA	El grupo de direcciones STA se puede configurar en el AC o en otros dispositivos. Si elige configurarlo en otros dispositivos, configure y verifique la configuración del grupo de direcciones en esos dispositivos después de completar este proceso.

2.2.4 Vista previa de la configuración

Este proceso permite a los usuarios verificar las configuraciones. Verifique los comandos de la CLI para las configuraciones actuales haciendo clic en **Mostrar comando**.

Config Wizard

✓ Configure AC ✓ Configure AP ✓ Configure WiFi **Preview Config** ✓

Configure Show Command

Country Code ES(Spain)

Time Zone UTC+8(CCT)

Date 2024-07-22 14:49

IP Address 10.52.24.237/255.255.248.0

MGMT VLAN 1

Default Gateway 10.52.25.1

System Charset UTF-8

Configure

Previous Complete

Configure

AP is in VLAN 1

Interface Address 10.52.24.237/255.255.248.0

AP Address Pool on Other Device

AC Tunnel Address 10.52.24.237

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

Haga clic en **Mostrar comando** para mostrar los comandos de la CLI para las configuraciones actuales.

Config Wizard

☒ Configure AC ☒ Configure AP ☒ Configure WiFi ☒ Preview Config

Configure

Country Code ES(Spain)
Time Zone UTC+8(CCT)
Date 2024-07-22 14:49
IP Address 10.52.24.237/255.255.248.0
MGMT VLAN 1
Default Gateway 10.52.25.1
System Charset UTF-8

Configure

Show Command

Previous

Complete

Config Wizard

☒ Configure AC ☒ Configure AP ☒ Configure WiFi ☒ Preview Config

```
vlan 1
exit
interface vlan 1
ip address 10.52.24.237 255.255.248.0
exit
ac-controller
capwap ctrl-ip 10.52.24.237
exit
ip route 0.0.0.0 0.0.0.0 10.52.25.1
no wlan-config 1
wlan-config 1 EKWIFI
ssid-code utf-8
enable-broad-ssid
exit
wlansec 1
security wpa enable
security wpa ciphers aes enable
security wpa akm psk enable
security rsn enable
security rsn ciphers aes enable
```

Hide Command

Previous

Complete

Una vez que confirme la configuración, haga clic en Completar y aparecerá una ventana que muestra la implementación de la red. Puede probar la conectividad de red con la red externa a través de la detección de red.

Config Wizard

✓ Configure AC ✓ Configure AP ✓ Configure WiFi **Preview Config** ✓

Configure Show Command

Country Code	ES(Spain)
Time Zone	UTC+8(CCT)
Date	2024-07-22 14:49
IP Address	10.52.24.237/255.255.248.0
MGMT VLAN	1
Default Gateway	10.52.25.1
System Charset	UTF-8

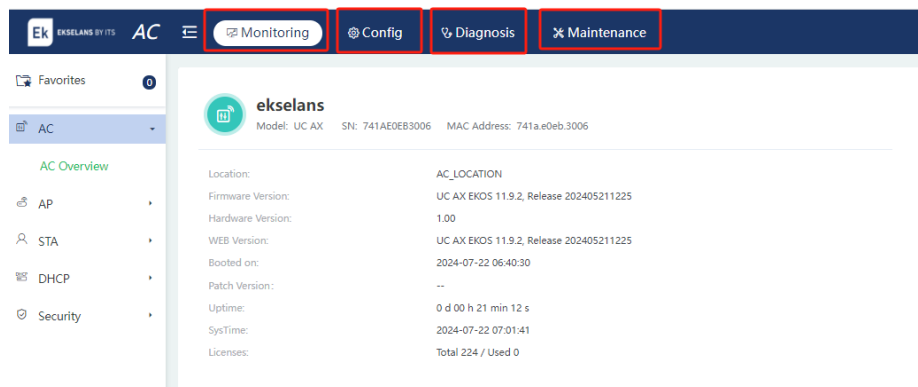
Configure

Previous **Complete**

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 dentro de cada módulo.



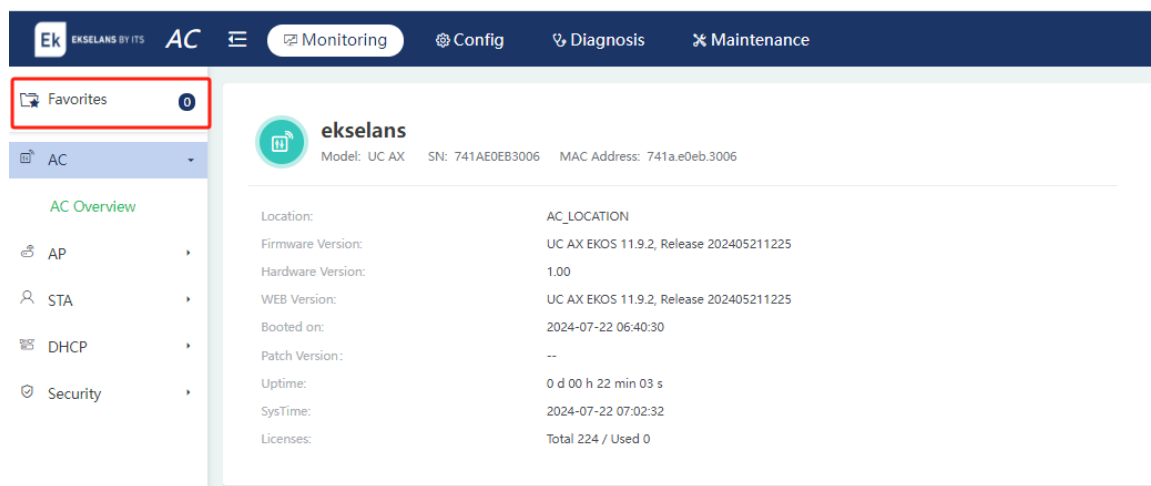
3.2 Favoritos


La 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.

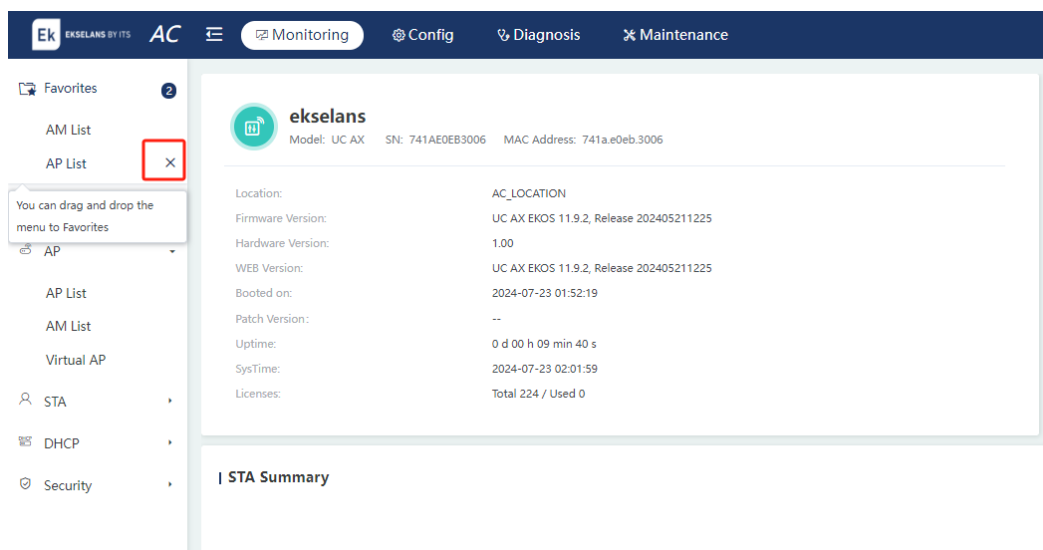
Nota

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

(1) Agregar a favoritos: arrastre y suelte los elementos del menú en Favoritos.

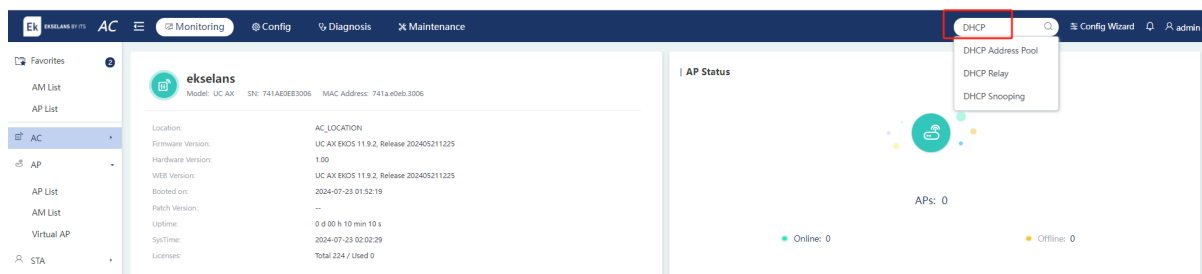


(2) Eliminar de favoritos: seleccione los elementos del menú y haga clic en el  icono. Haga clic en Aceptar para eliminar el elemento de Favoritos.



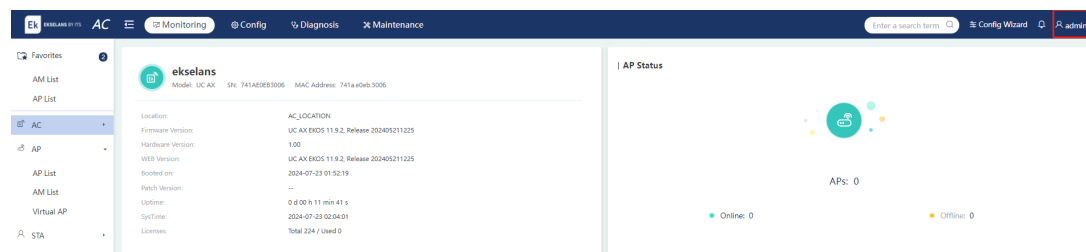
3.3 Barra de búsqueda de menú

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

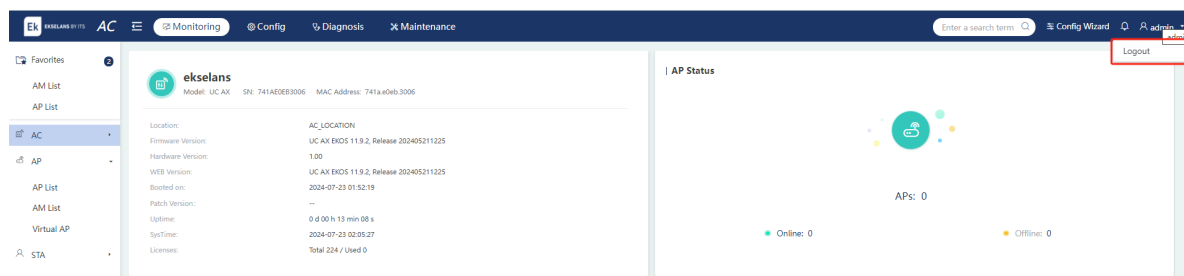


3.4 Otras funciones

(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.



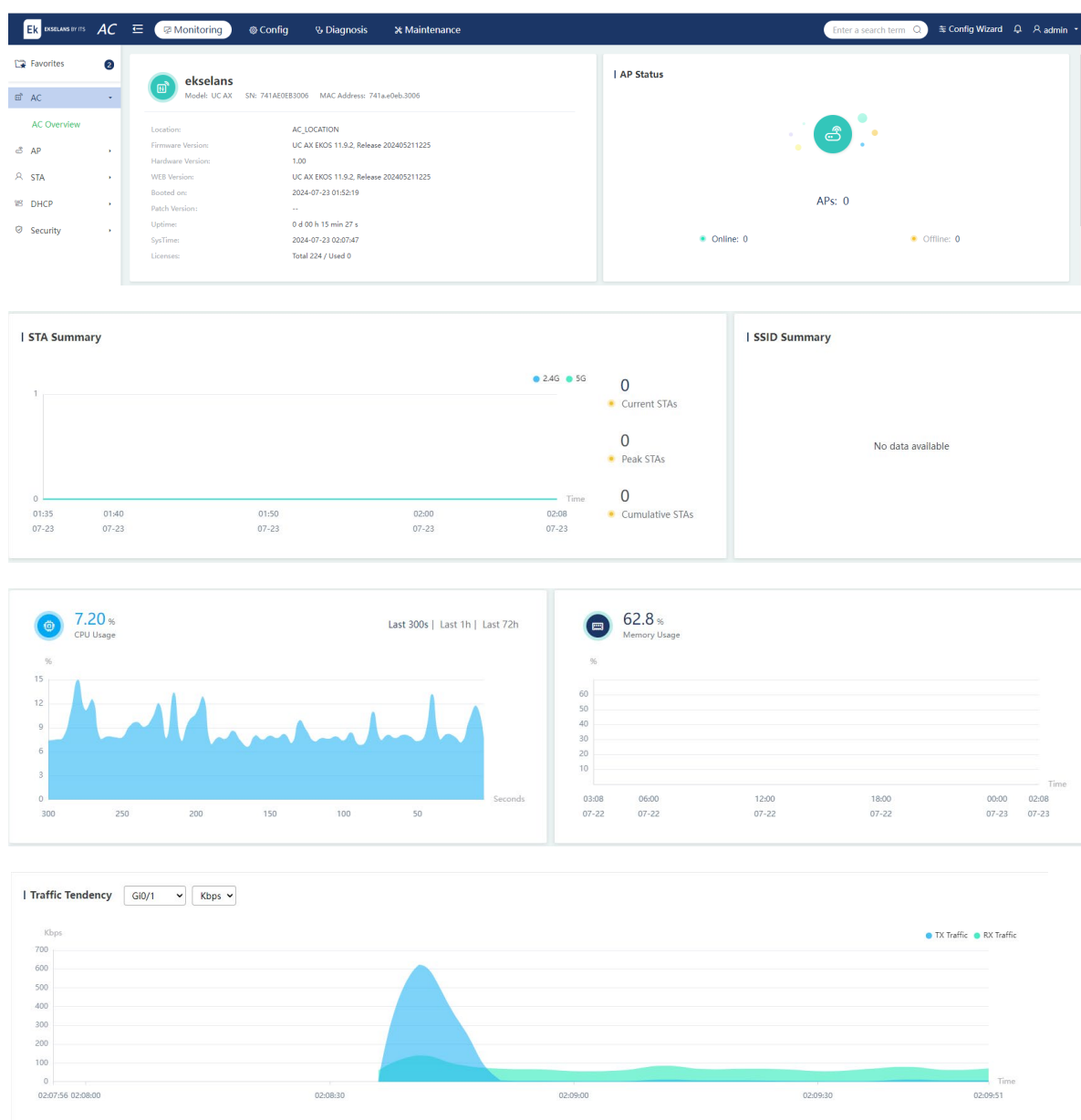
4 Monitorización

4.1 Corriente alterna

4.1.1 Visión general

Elija **Monitoring > AC > AC Overview**.

La página **Descripción general** de la AC muestra la información básica sobre la CA, como la dirección MAC, el modelo y los detalles de la versión. También le permite verificar el estado del AP, el resumen de STA, el resumen de SSID, el uso de la CPU, el uso de la memoria, la tendencia del tráfico y la información de la interfaz de CA.



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

4.1.2 AC virtual


Elija **Monitoring > AC > Virtual AC**.

Nota

El menú de AC virtual se muestra en función de la configuración del dispositivo. Este menú solo está disponible cuando el dispositivo está configurado con el **comando device convert mode virtual**.


La página de AC virtual muestra los miembros actuales de AC virtual y su información básica.

Virtual AC

Domain ID:100(100) 

AC-1 WORD


Active



VSL Interface
● Gi 1/0/2 (ok)

AC-2


Standby



VSL Interface
● Gi 2/0/2 (ok)


Haga clic en una AC virtual específica para ver la información detallada sobre sus miembros de CA.

Virtual AC

Domain ID:100(100) 

AC-1 WORD


Active



VSL Interface
● Gi 1/0/2 (ok)

AC-2

Standby



VSL Interface
● Gi 2/0/2 (ok)

Device ID: 1 MAC: 00d0.f822.12ab

Role: Active SN: 1234942570020

Priority: 200 CPU: 6.60%

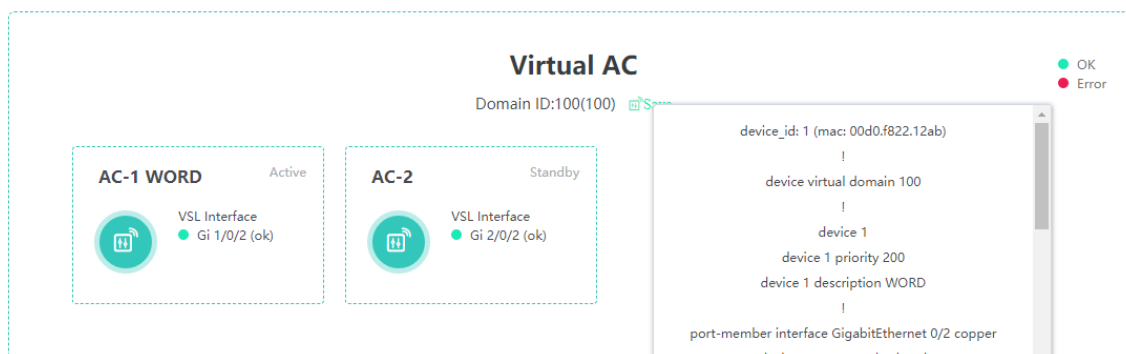
Status: OK Memory: 43%

Port: Gi 1/0/2(ok) Flash: 46%

APs: 1

CTA: 0

Haga clic en **Guardar** para ver las configuraciones del AC virtual.

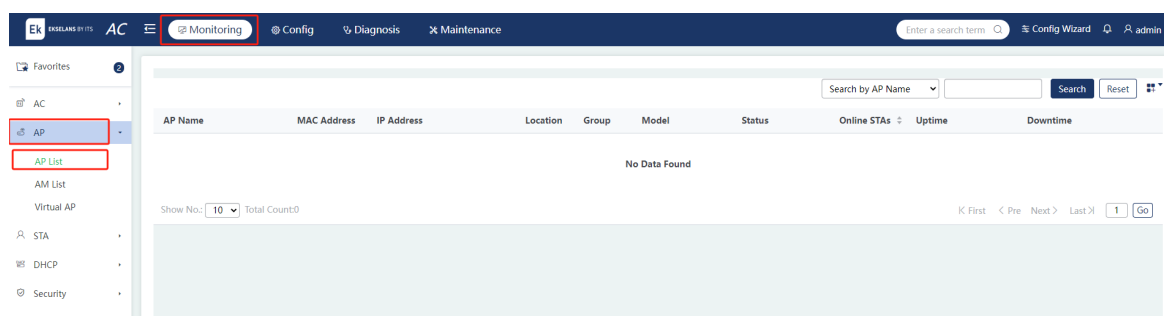



4.2 AP

4.2.1 Lista de AP

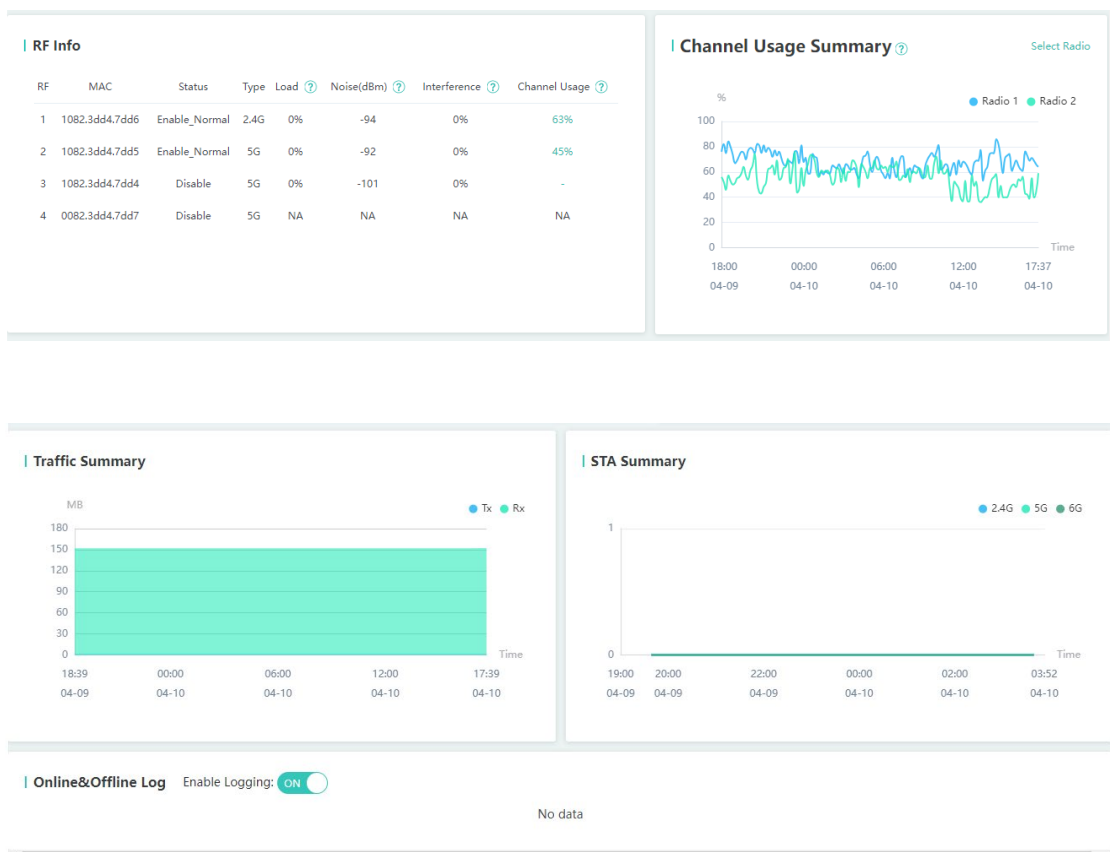
Elija **Monitoring > AP > AP List**.

La lista de AP muestra la información básica y los detalles de RF y modelo de los AP conectados con el dispositivo.



- (1) Búsqueda de AP: Introduzca las palabras clave en la barra de búsqueda y haga clic en **Buscar**. Haga clic en **Restablecer** para borrar los criterios de búsqueda y mostrar la lista de todos los AP. Si un AP está fuera de línea, no se pueden ver sus detalles.
- (2) Para mostrar información adicional sobre los AP, haga clic  y seleccione la información que desea ver.
- (3) Visualización de detalles de AP: Haga clic en el nombre de AP para redirigir a la página de AP.

La información de RF, el resumen de uso del canal, el resumen de tráfico y otra información se muestran en la página AP.



Nombre de la página	Descripción
Información de RF	Muestra el ID de radio, la dirección MAC, el estado, el tipo, la carga, la interferencia, el uso del canal y el ruido, y las proporciones de paquetes de salida, paquetes de entrada, interferencia y canales inactivos en relación con el uso del canal.
Resumen de uso del canal	Muestra el resumen del uso del canal.
Resumen de tráfico	Muestra el resumen de tráfico de las interfaces cableadas en el AP.
Resumen de STA	Muestra el número de STA asociados con el AP.
Registro en línea y fuera de línea	Muestra el motivo del cierre de sesión, el uso de memoria, el uso de CPU y el número de STA asociados con este AP.

4.2.2 Virtual AP

Elija **Monitoring > AP > Virtual AP**.

Esta página muestra detalles de los AP virtuales.

AP Name	AP Group	IP	MAC	Type	Action
0074.9c23.e2db	Default	172.31.61.183	0074.9c23.e2db	Virtual AP	Details
Show No.: <input type="text" value="10"/> Total Count:1 ⏪ First < Pre 1 Next > Last ⏩ <input type="text" value="1"/> GO 					

Búsqueda de AP: Introduzca las palabras clave en la barra de búsqueda y haga clic en **Buscar**. Haga clic en **Restablecer** para borrar los criterios de búsqueda y mostrar la lista de todos los AP.

AP Name	AP Group	IP	MAC	Type	Action
0074.9c23.e2db	Default	172.31.61.183	0074.9c23.e2db	Virtual AP	Details
Show No.: <input type="text" value="10"/> Total Count:1 ⏪ First < Pre 1 Next > Last ⏩ <input type="text" value="1"/> GO 					

Detalles: Haga clic en **Detalles** en la columna Acción y aparecerá una ventana que muestra los detalles del AP virtual.

0074.9c23.e2dbDetails

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

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

Show No.: 10 Total Count:1

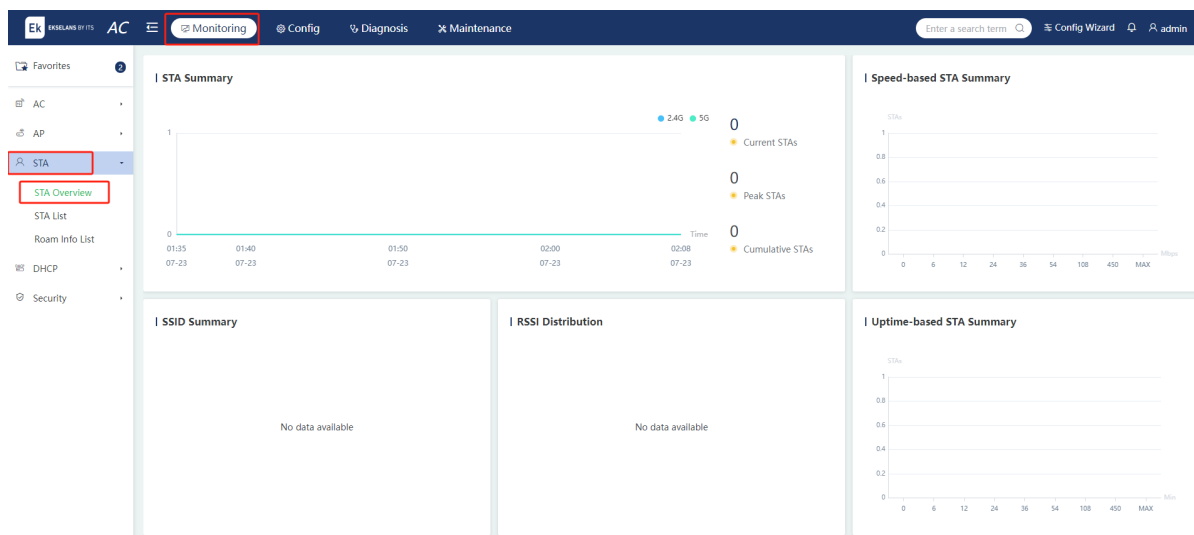
K First < Pre 1 Next > Last > 1 GO

4.3 STA

4.3.1 Visión general

Seleccione **Supervisión > STA > Descripción general de STA**.

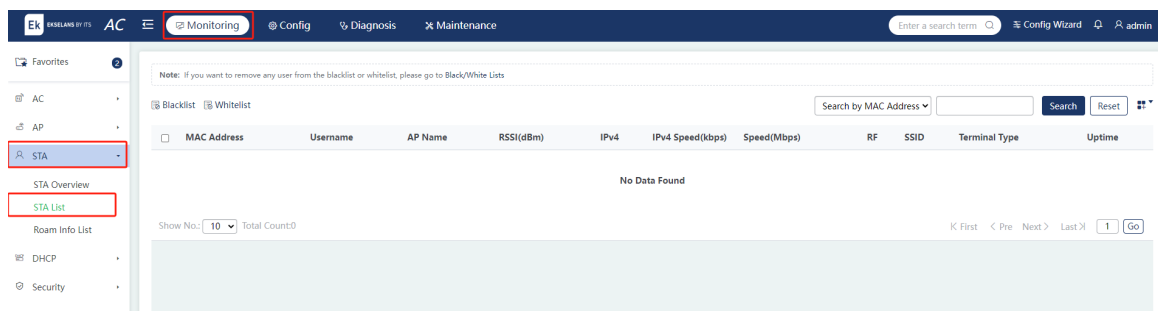
Esta página presenta las estadísticas de STA desde varias perspectivas, actualizadas a un intervalo de 30 segundos.



Nombre de la página	Descripción
Resumen de STA	<p>Muestra los resúmenes de los STA asociados con Wi-Fi de 2,4 GHz, 5 GHz y 6 GHz, respectivamente.</p> <p>STA actuales: muestra el número de STA en línea actuales.</p> <p>STA máximos: muestra el número máximo de STA en línea en un plazo de 24 horas.</p> <p>STA acumulativos: muestra el número acumulado de STA en línea en un plazo de 24 horas. (Los STA que inician sesión varias veces se cuentan solo una vez).</p>
Resumen de STA basado en la velocidad	Muestra el resumen de STA basado en la velocidad en un gráfico de barras. Haga clic en la barra para redirigir a la lista de STA.
Resumen de SSID	Muestra la proporción de STA asociados a diferentes redes Wi-Fi. Haga clic en el gráfico circular para redirigir a la lista de STA.
Distribución RSSI	Muestra la proporción de RSSI de las STA.
Resumen de STA basado en tiempo de actividad	Muestra el resumen de STA basado en el tiempo de actividad en un gráfico de barras. Haga clic en la barra para redirigir a la lista de STA.

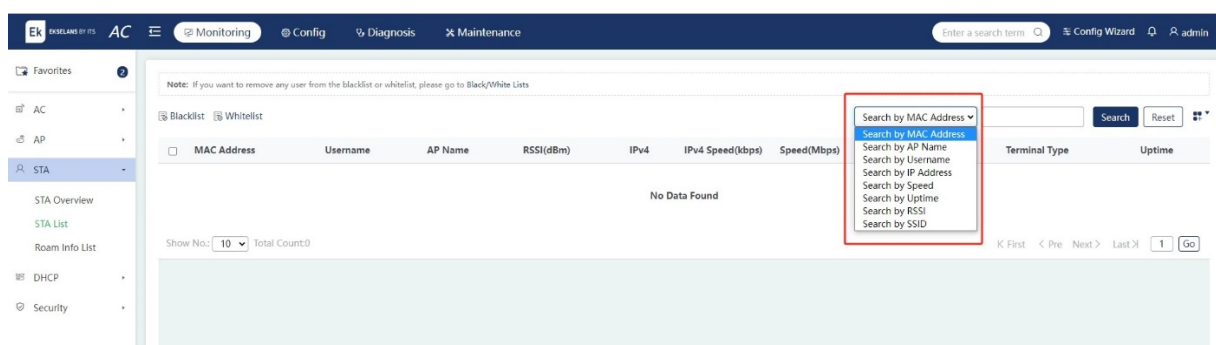
4.3.2 Lista de STA

Elija **Supervisión > STA > Lista de STA**.

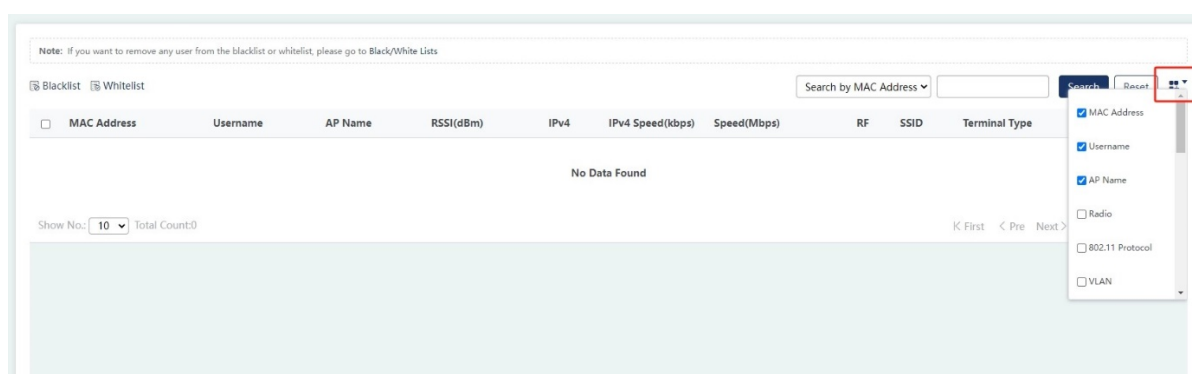


1. Búsqueda de STA

Introduzca las palabras clave en la barra de búsqueda y haga clic en **Buscar**. Haga clic en **Restablecer** para borrar los criterios de búsqueda y mostrar la lista de todos los STA.



Para mostrar información adicional sobre los STA enumerados, haga clic y seleccione la información que desea ver.



2. Agregar a la lista negra o a la lista blanca

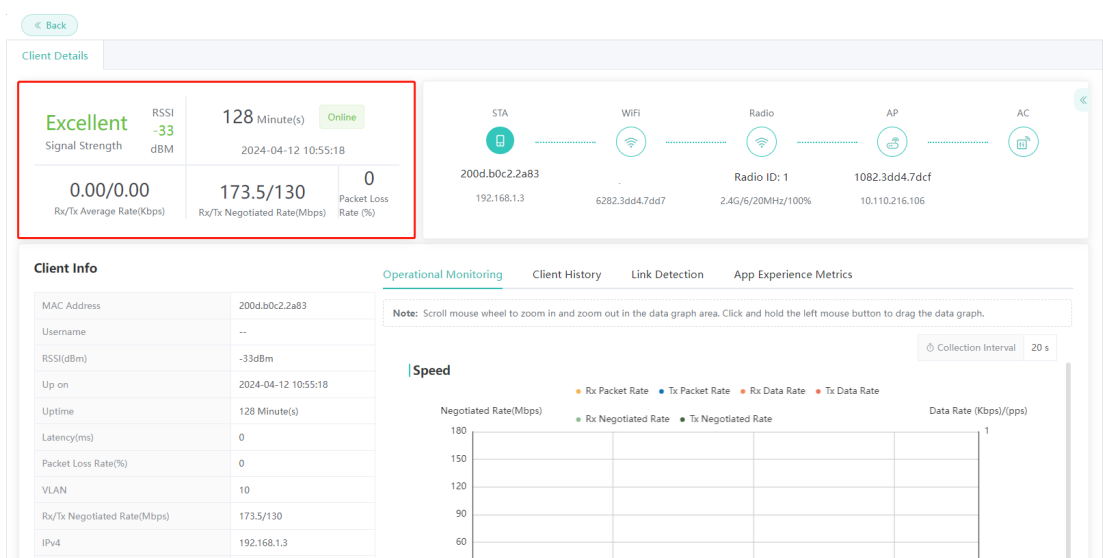
Selecione los STA que desea agregar a la lista negra y haga clic en **Lista negra**.

3. Ver detalles del cliente

Haga clic en **Dirección MAC** para ir a la página **Detalles del cliente**. En la página **Detalles del cliente**, puede ver la información de red, la topología, la información del cliente, la tendencia a la velocidad, el RSSI, la tasa de pérdida/reintento de paquetes, el historial del cliente, la detección de vínculos y las métricas de experiencia de la aplicación.

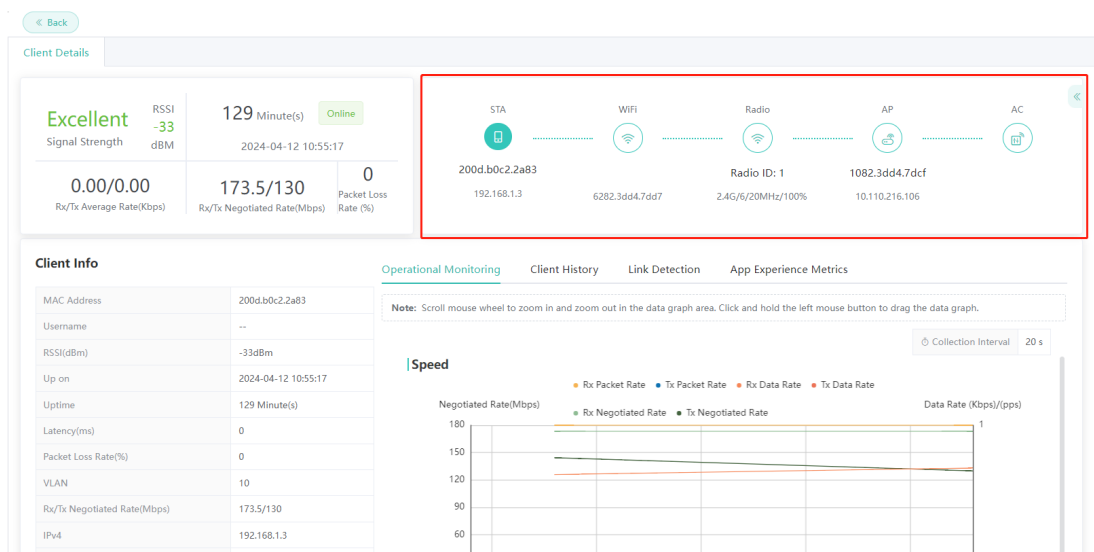
(1) Información de la red

En la esquina superior izquierda de la **página** Detalles del cliente, puede ver el RSSI, el tiempo de actividad, la tasa promedio de Rx/Tx, la tasa negociada de Rx/Tx y la tasa de pérdida de paquetes del cliente.

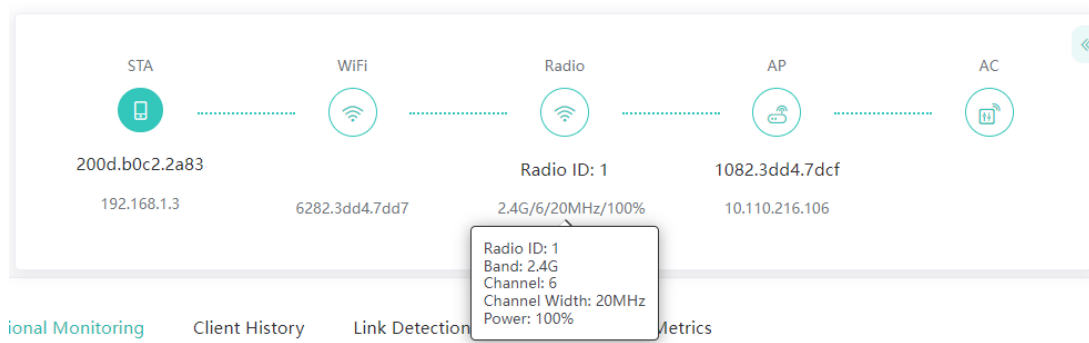


(2) Topología

En la esquina superior derecha de la **página** Detalles del cliente, puede ver la topología, incluido el nombre de Wi-Fi, el ID de radio, el AP y el AC asociados con el STA.

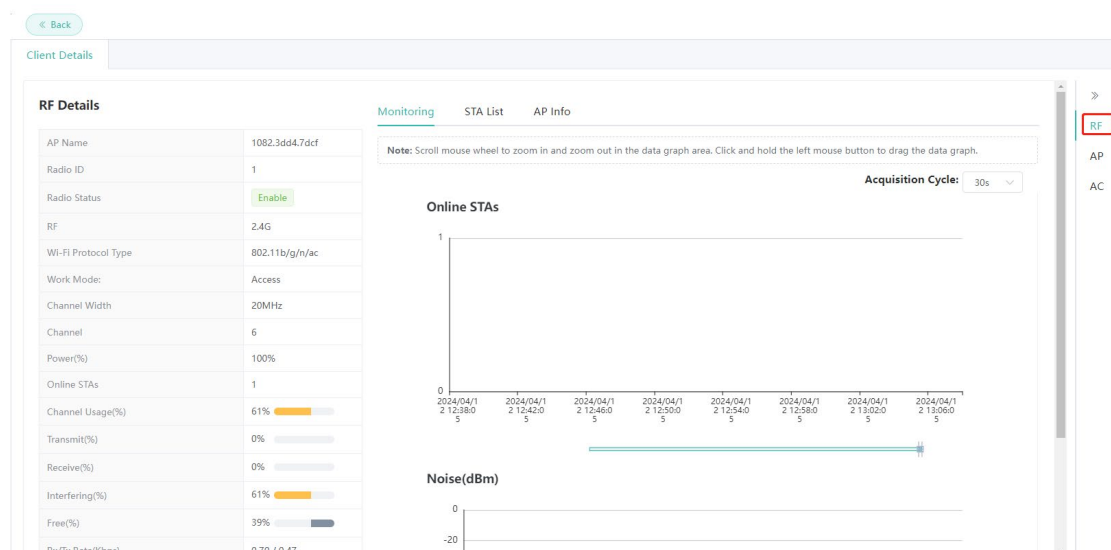


Mueva el cursor a un nodo de la topología para ver información detallada sobre el nodo de conexión.

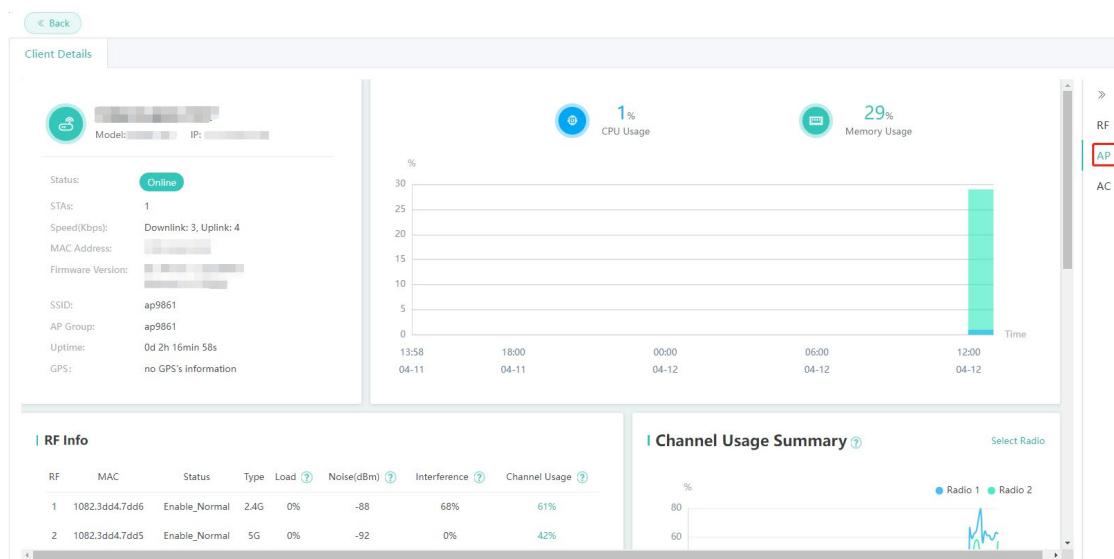


Mueva el cursor al « icono de la esquina superior derecha de la topología. Haga clic en **Ver detalles** para ver detalles sobre la radio, el AP y el AC asociados con el STA.

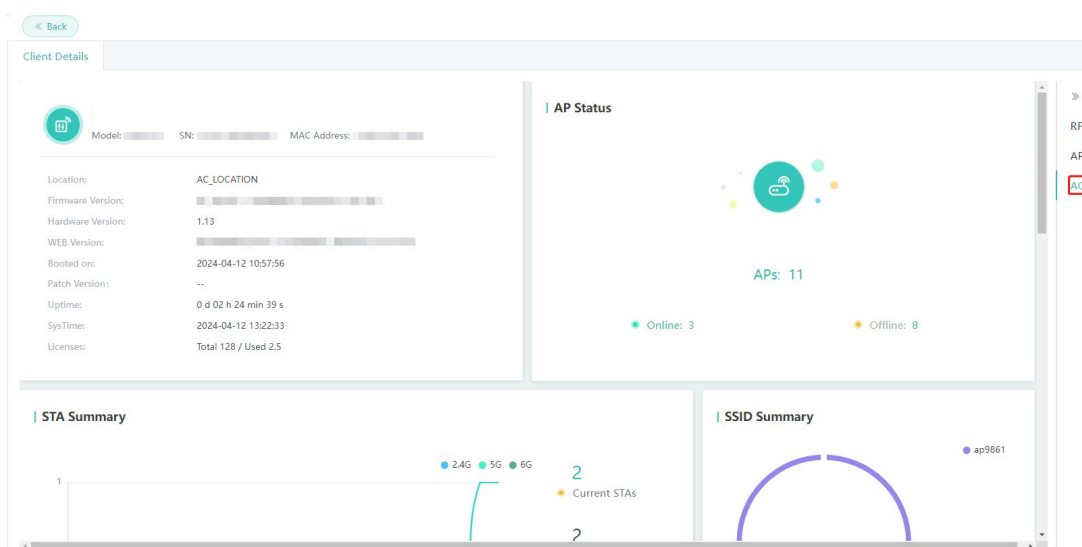
- Detalles sobre la radio asociada a la STA:



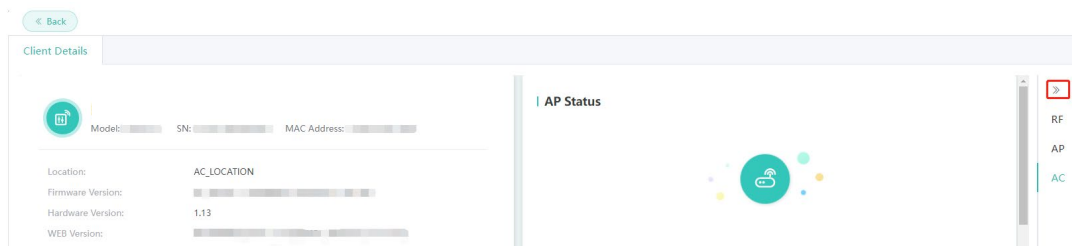
- Detalles sobre el AP asociado con el STA:



- Detalles sobre el AC asociado con el STA:

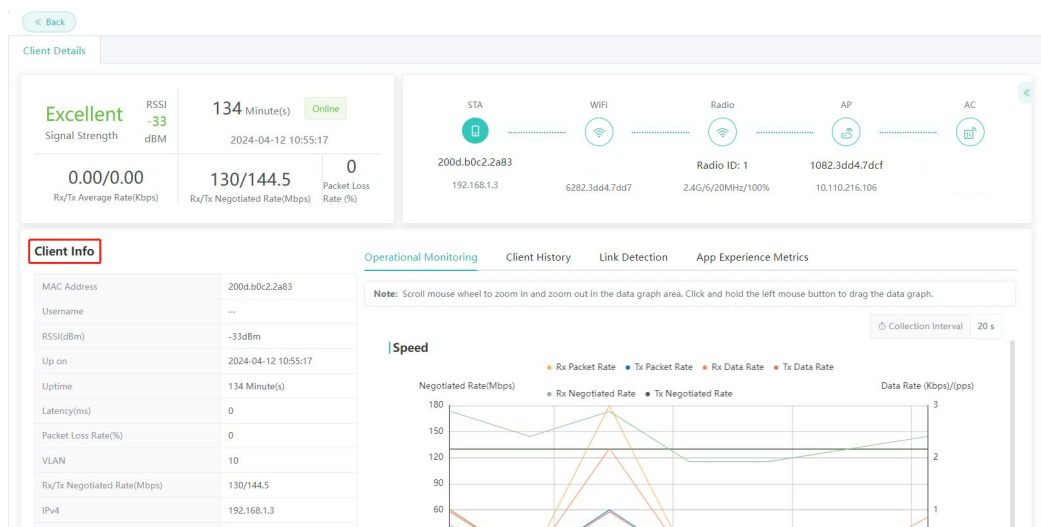


Haga clic en el » icono para contraer los detalles de RF, AP y AC y volver a la página **Detalles del cliente**.



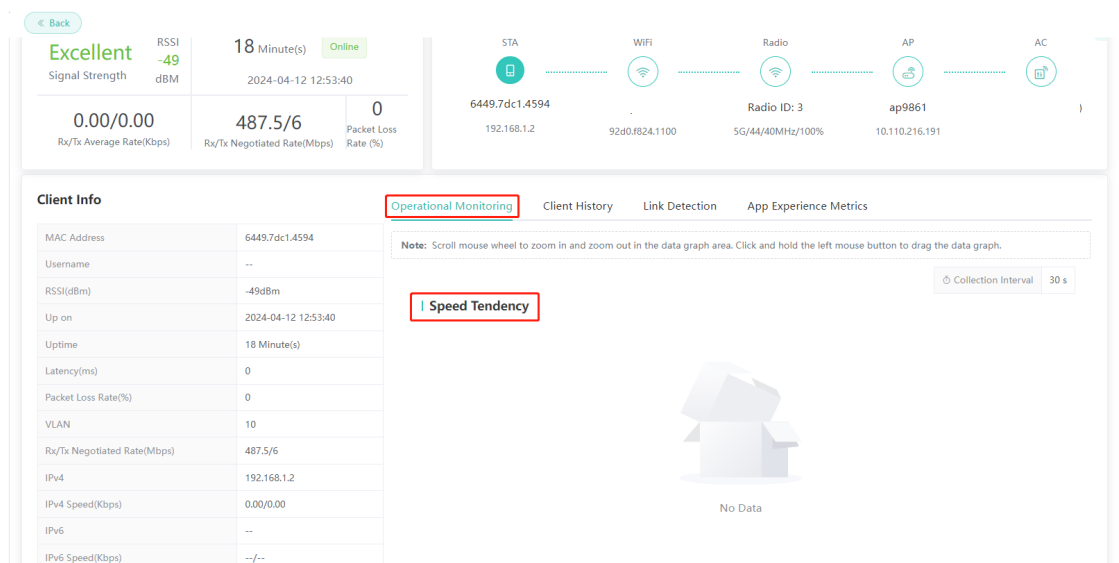
(3) Información del cliente

En la esquina inferior izquierda de la **página Detalles** del cliente, puede ver información detallada sobre el cliente.

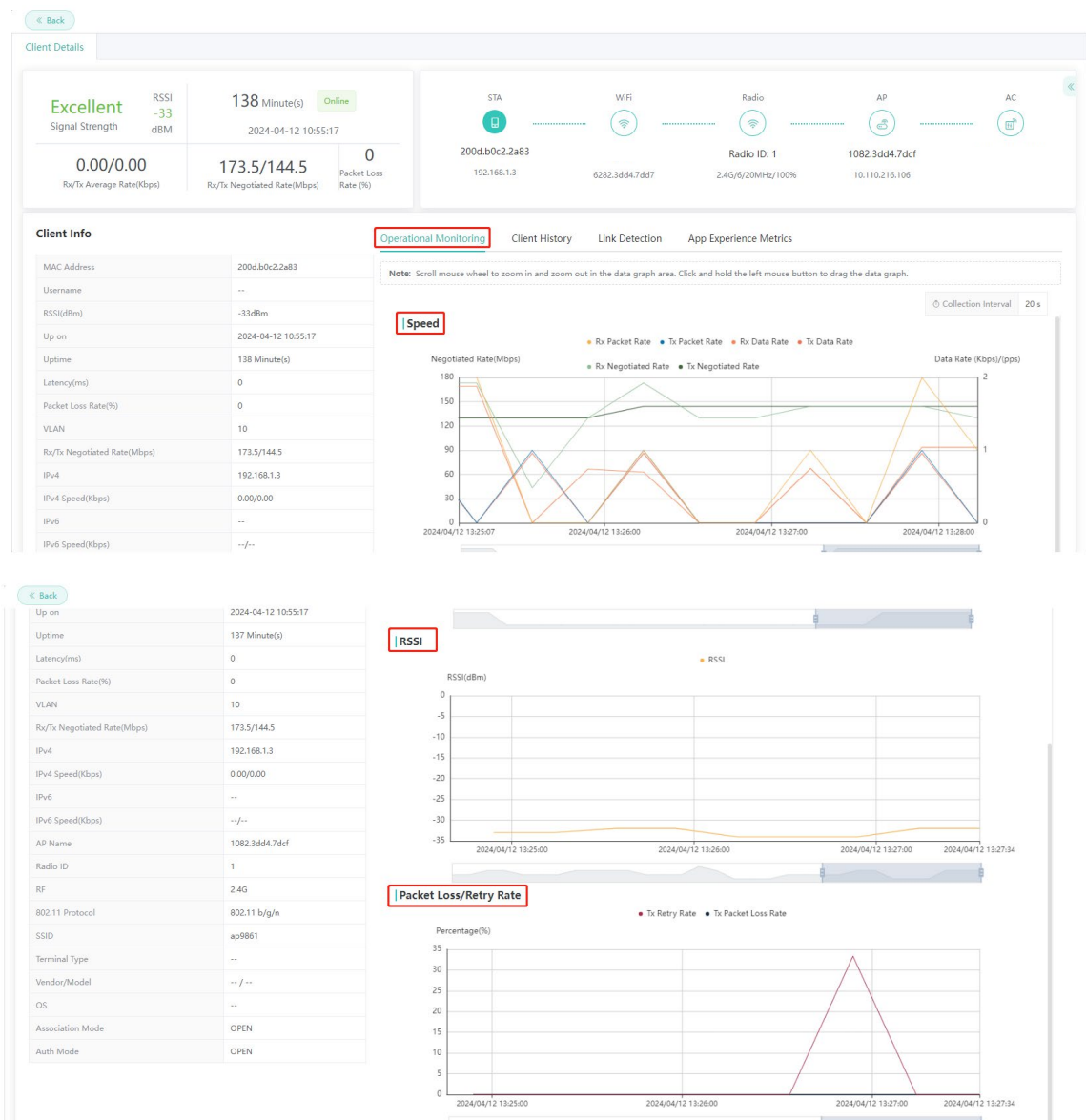


(4) Monitoreo Operacional

Si el cliente no está habilitado con telemetría de alta frecuencia, el gráfico **de tendencia de velocidad** del cliente se muestra en la pestaña **Supervisión operativa**.

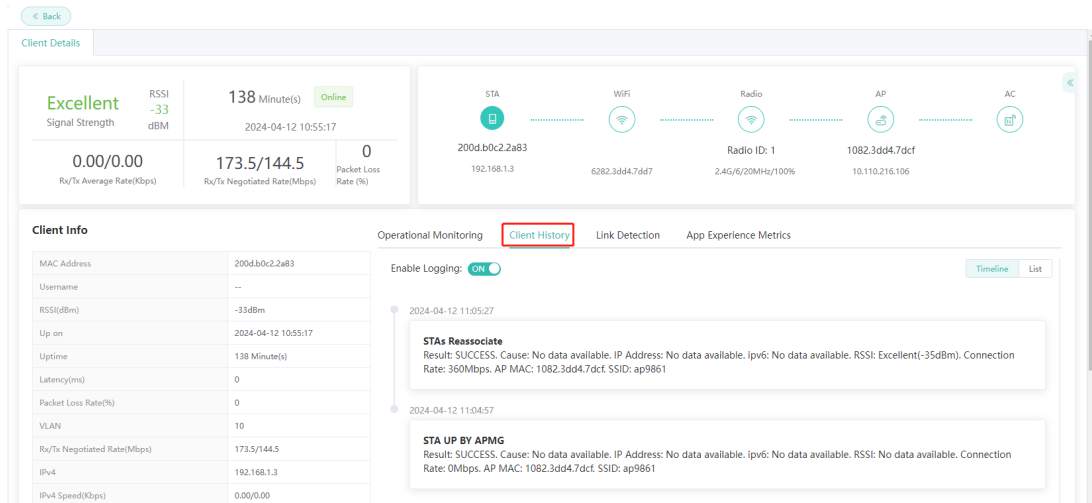


Si el cliente está habilitado con telemetría de alta frecuencia y está en estado de telemetría, los **gráficos Velocidad, RSSI y Tasa de pérdida/reintento de paquetes** se muestran en la pestaña **Supervisión operativa**.



(5) Historia del cliente

El historial en línea y fuera de línea de los STA se registra y se muestra en la pestaña **Historial del cliente**.

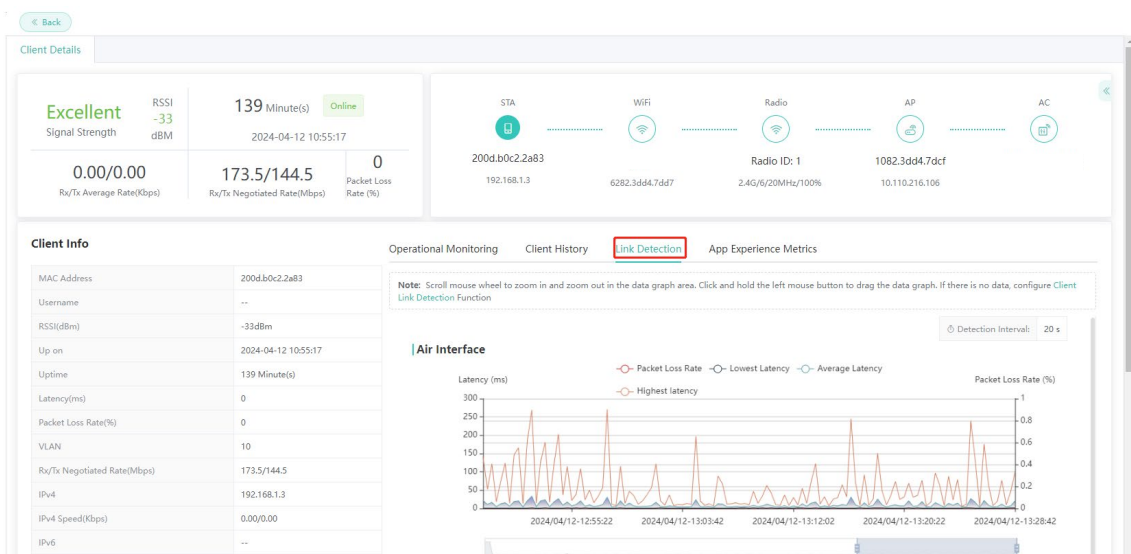


(6) Detección de enlaces

Si el cliente está habilitado con detección de enlaces, los **gráficos de líneas Tasa de pérdida de paquetes**, Latencia más baja, Latencia promedio y Latencia más alta de **Air Interface**, **Gateway**, **DHCP** y **DNS** se muestran en la **Detección de vínculos** pestaña. Si el cliente no está habilitado con la detección de vínculos, no se muestra ninguna información de detección de vínculos sobre el cliente en la **pestaña Detección de vínculos**.

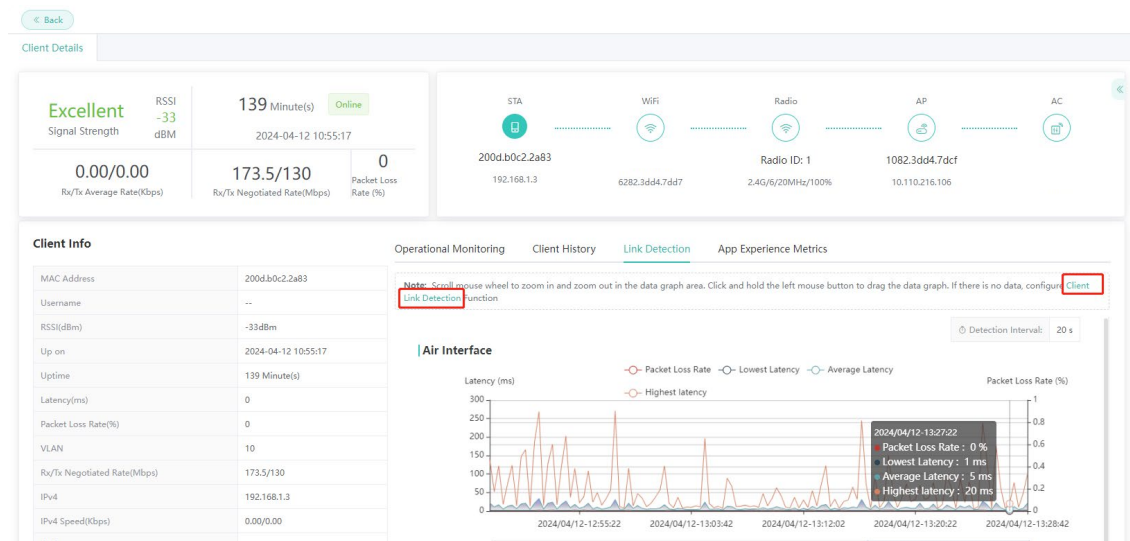
Nota

Ya sea que la información sobre **Interfaz aérea**, **Entrada**, **DHCP** o **DNS** se muestra en función de la **Objetivo de detección** configurado eligiendo **Diagnóstico > Enseñar STA > Comprobación de Wlan-Sta-Link > Configuración de parámetros**. Para obtener más información, consulte [Error! Reference source not found.](#)



Para ver los datos de detección de vínculos sobre el cliente, haga clic en **Detección de enlaces de clienteo** elija **Diagnóstico > Enseñar STA > Comprobación de Wlan-Sta-Link** para ingresar


a la página y agregar el cliente. Para obtener más información, consulte [Error! Reference source not found.](#)

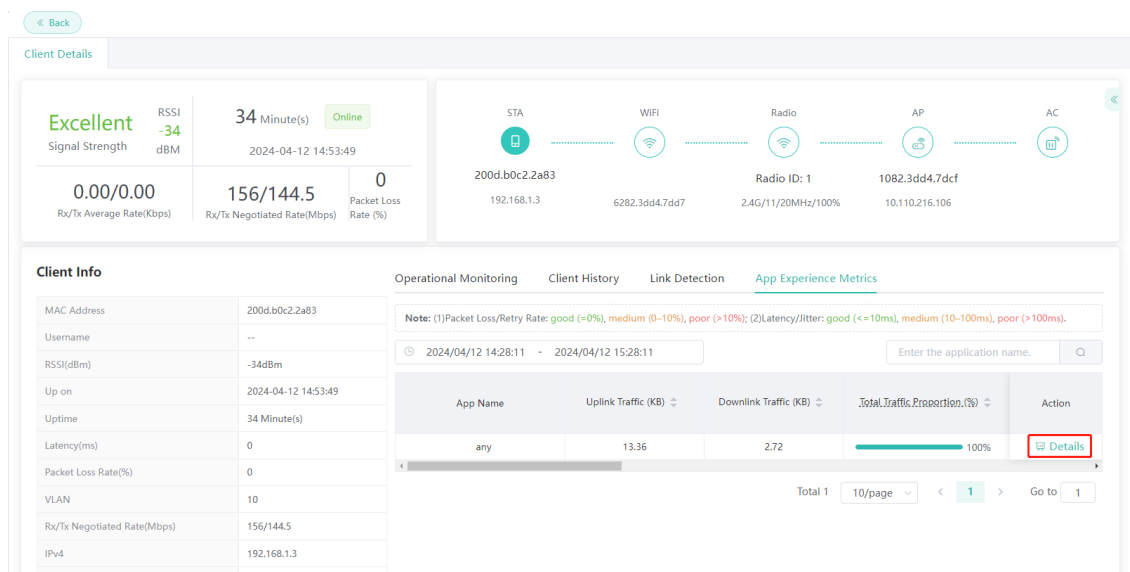


(7) Métricas de experiencia de la aplicación

El uso del tráfico de varias aplicaciones utilizadas por un usuario se muestra en la página Métricas de experiencia de **la aplicación**. La lista de aplicaciones utilizadas por un usuario en la última hora se muestra de forma predeterminada (el rango de tiempo se puede personalizar).

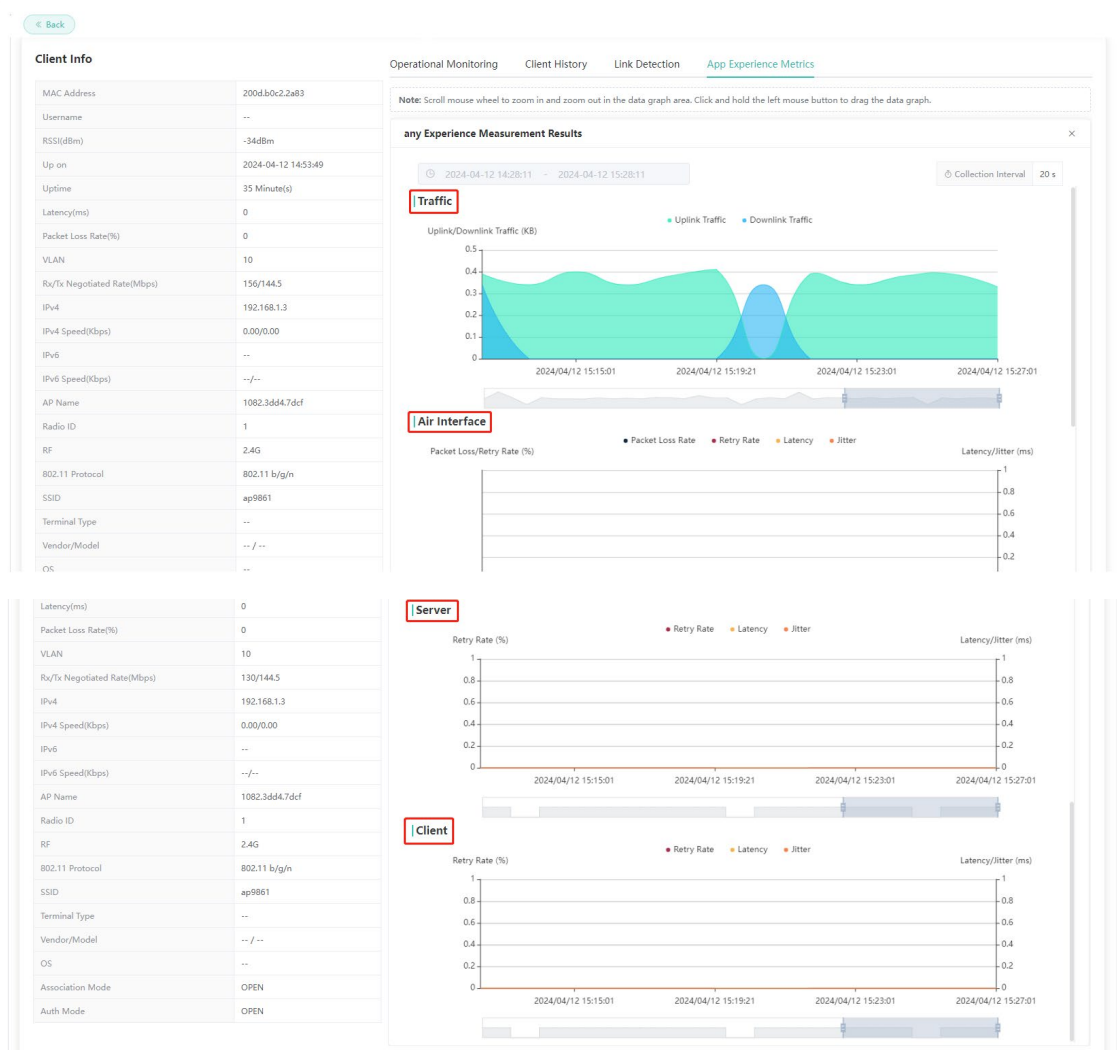
i Nota

En la página Lista de **STA**, **solo se muestran los** datos sobre los usuarios cuyas direcciones MAC marcadas con el  icono de telemetría de alta frecuencia en la **columna Dirección MAC** se muestran en esta página.



Parámetro	Descripción del parámetro
Tráfico	Muestra la proporción del tráfico total de enlaces ascendentes y descendentes utilizado por una aplicación con respecto al tráfico total dentro del período de tiempo seleccionado.
Servidor	Muestra la latencia, la tasa de pérdida de paquetes y la tasa de reintentos de los paquetes TCP enviados desde el AP al servidor.
Cliente	Muestra la latencia, la tasa de pérdida de paquetes y la tasa de reintentos de los paquetes TCP enviados desde el AP al cliente (diferente del modelo de cálculo en el lado de la interfaz aérea).
Interfaz aérea	Muestra la latencia, la tasa de pérdida de paquetes y la tasa de reintentos de solo los paquetes de solicitud o respuesta inalámbrica de enlace descendente enviados desde el AP al cliente.

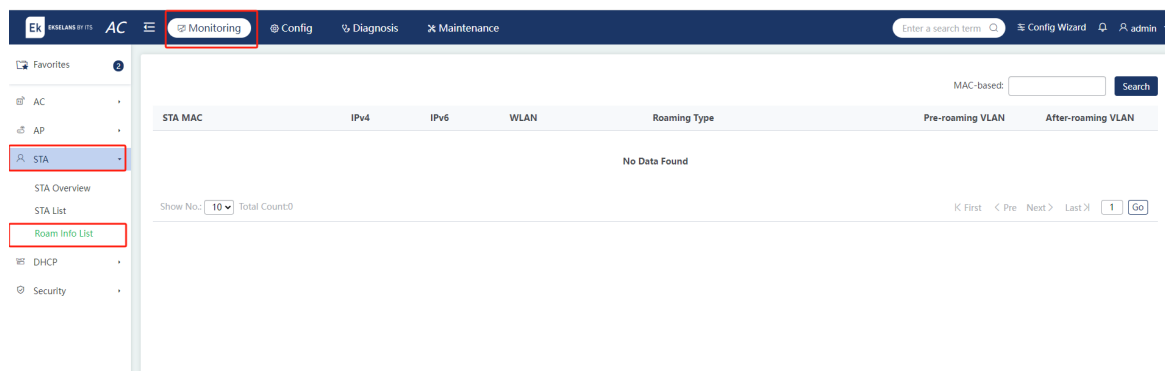
Haga clic en **Detalles** de una aplicación especificada para ver el gráfico de tendencias de tráfico de la aplicación.



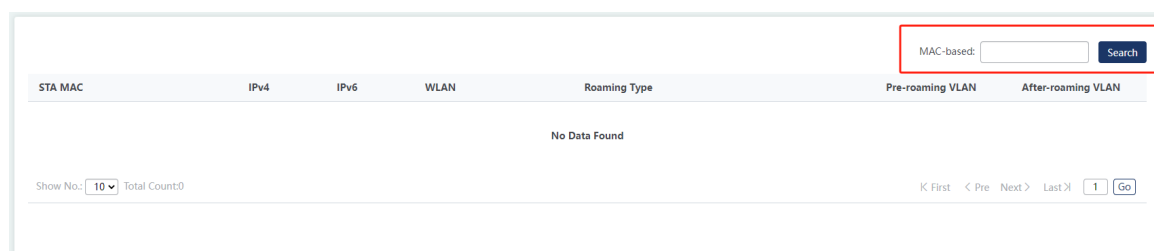
4.3.3 Lista de información de itinerancia

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

La lista de información de itinerancia muestra la lista de dispositivos de itinerancia.



Ingresa la dirección MAC en la barra de búsqueda y haga clic en **Buscar**. Haga clic en **Restablecer** para borrar el contenido en la barra de búsqueda.

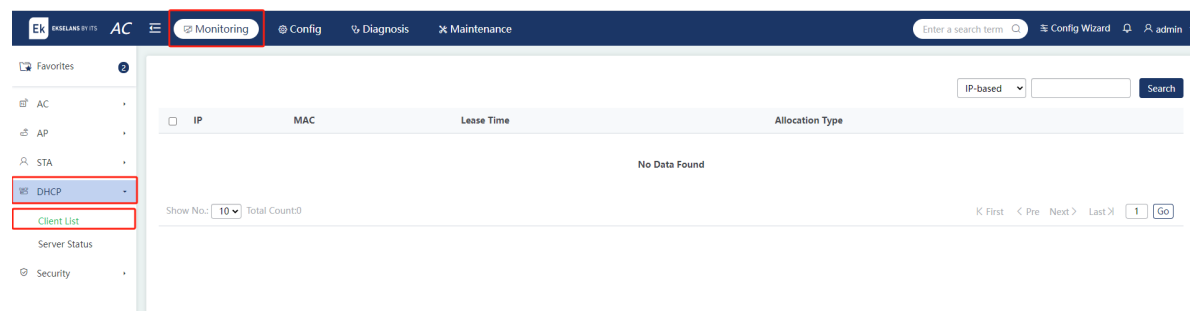


4.4 DHCP

4.4.1 Lista de clientes DHCP

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

La lista de clientes DHCP muestra los clientes asignados con direcciones del grupo de direcciones.



Búsqueda de STA: Si hay un gran número de STA, busque las STA por la dirección MAC o la dirección IP. Introduzca las palabras clave en el cuadro de entrada y haga clic en **buscar**.

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

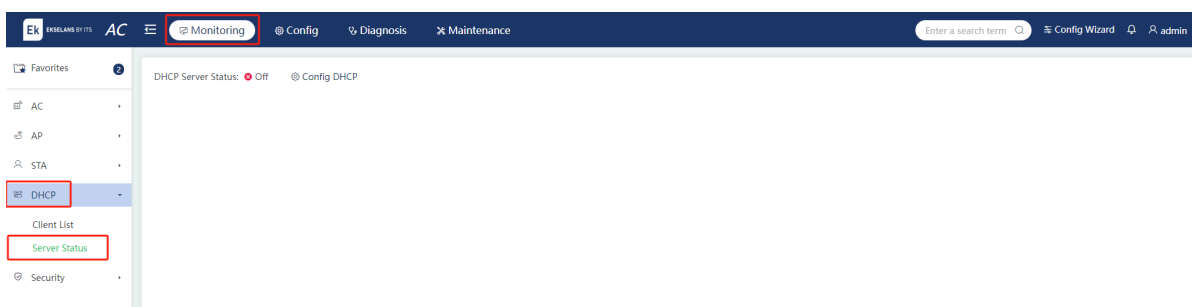
Show No.: Total Count:147

K First < Pre ① 2 3 Next > Last 1 GO

4.4.2 Estado del servidor DHCP

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

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

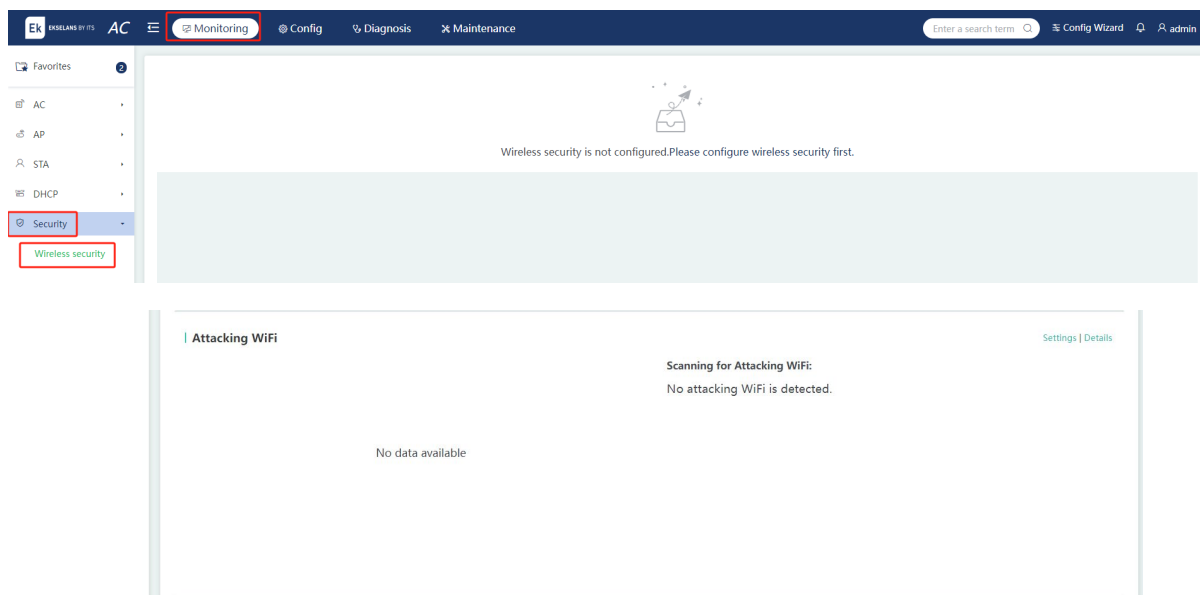


4.5 Seguridad

4.5.1 Seguridad inalámbrica

Elija **Monitoring > Security (Supervisión) > Wireless security (Seguridad inalámbrica)**.

La página **Seguridad inalámbrica** muestra la situación de seguridad y el número de eventos de seguridad controlados por el dispositivo. La **página Wi-Fi peligroso** muestra categorías de señales de Wi-Fi peligrosas y alarmas de Wi-Fi peligrosas. La **página Ataque a WiFi** muestra los ataques de Wi-Fi y las alarmas de ataque.



(1) Lista de Wi-Fi peligrosas

Haga clic en **Detalles** en la página **Wi-Fi peligroso** para redirigir a la página **Lista de Wi-Fi peligroso**.

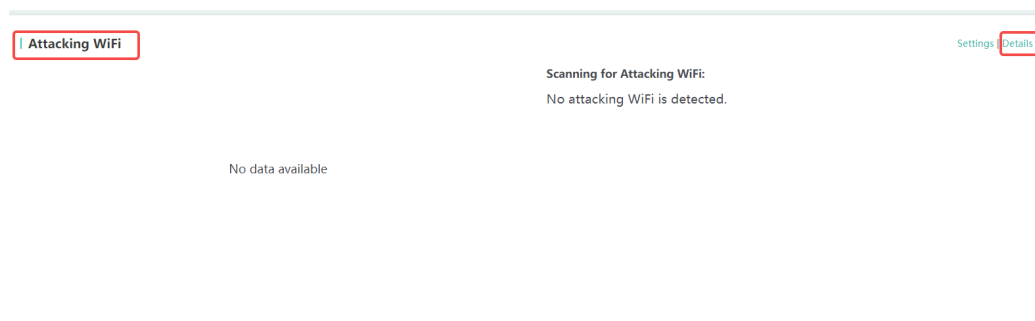
Esta función le permite:

- o Muestra la información sobre las señales Wi-Fi peligrosas.
- o Busque señales de Wi-Fi por SSID, tipo de seguridad y estado.
- o Contener o confiar en los dispositivos con un BSSID determinado.
- o Contener un SSID o deshabilitar la contención.

Haga clic en **Atrás** para volver a la página **Seguridad inalámbrica**.

(2) Ataque a la WiFi

Haga clic en **Detalles** en la página **WiFi atacante** para redirigir a la página **Lista de WiFi atacante**.



Esta función le permite:

- o Muestra la información sobre las redes Wi-Fi.

- o Ordene las redes Wi-Fi por el número de ataques.
- o Busque por dirección MAC, tipo, ubicación y estado.

Haga clic en **Atrás** para volver a la página **Seguridad inalámbrica**.

5 Configuración

5.1 WLAN (Conexión WLAN)

5.1.1 Agregar WiFi

Elija **Config > WLAN > Add WiFi**.

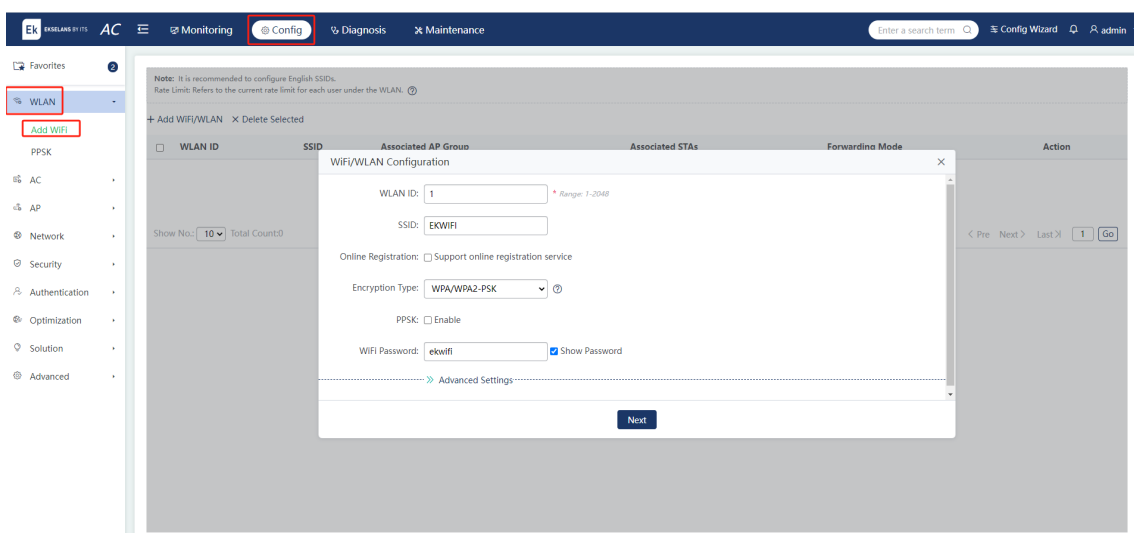
El Wi-Fi permite que los STA inalámbricos se asocien con el AP para el acceso a la red. Se pueden agregar o eliminar varias redes Wi-Fi.

Nota

- Haga clic  para ver las velocidades de datos típicas en escenarios comunes.

1. Adición de Wi-Fi

Haga clic en Agregar WiFi/WLAN y aparecerá la ventana Configuración de WiFi/WLAN.



Parámetro	Descripción
Inscripción en línea	Habilite o deshabilite el registro en línea.

Tipo de cifrado	<p>Abierto: Indica que no hay cifrado. No se requiere contraseña cuando el STA se conecta a la red Wi-Fi.</p> <p>WPA/WPA2-PSK: Indica el modo WPA con una clave precompartida de alta seguridad y fácil configuración, aplicable a hogares y pequeñas empresas.</p> <p>WPA/WPA2 802.1X: Indica el modo WPA o WPA2 que implementa la autenticación de identidad y la generación de claves a través de un servidor RADIUS. No se recomienda a los usuarios comunes que adopten este modo, ya que requiere un servidor de autenticación exclusivo.</p> <p>WPA2 802.1X: Indica el modo WPA2 que implementa la autenticación de identidad y la generación de claves a través de un servidor RADIUS.</p> <p>WPA2/WPA3: Indica el modo híbrido WPA2-WPA3, que está determinado por la STA.</p> <p>WPA3-PERSONAL: Proporciona mayor seguridad que WPA2 y evita eficazmente los ataques de diccionario.</p> <p>WPA3-ENTERPRISE-CCMP256: Configura el modo WPA3-Enterprise con cifrado GCMP-256, lo que proporciona protección adicional para las redes que transmiten datos confidenciales. Es aplicable a redes sensibles a los datos, como el gobierno o los sistemas financieros.</p> <p>WPA3-ENTERPRISE-CCMP128: Configura el modo WPA3-Enterprise con cifrado CCMP-128, lo que proporciona protección adicional para las redes que transmiten datos confidenciales. Es aplicable a redes sensibles a los datos, como el gobierno o los sistemas financieros.</p>
Reenvío de paquetes	<p>Reenvío central: Todos los datos se enrutan a través de la AC antes de ser reenviados a otros dispositivos. Este modo está configurado de forma predeterminada.</p> <p>Reenvío local: Los datos se reenvían a otros dispositivos directamente desde el switch, lo que reduce la carga en la CA.</p>
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: Algunas STA, PC y tarjetas de interfaz de red (NIC) admiten la codificación GBK.</p> <p>Puede seleccionar los modos de codificación según sea necesario.</p>
Ocultar SSID	Si habilita Ocultar SSID , el SSID no se muestra en el STA. Solo puede encontrar el SSID a través de la búsqueda.
Límite de STA	Configure el número máximo de STA que se pueden asociar con esta red Wi-Fi. No está configurado de forma predeterminada, lo que implica que no hay límite.

Período de desactivación de la red	Configure un período en el que la red Wi-Fi esté apagada. El valor predeterminado es Nunca . Configure un período para apagar el Wi-Fi cuando sea necesario en escenarios específicos.
NAS ID	Configure el ID de NAS para la WLAN introduciendo una cadena de hasta 32 bytes sin espacios.
5G-Acceso previo	Si esta función está habilitada, STA inicia sesión preferentemente en redes 5G. Está deshabilitado de forma predeterminada.

Una vez completada la configuración, haga clic en **Siguiente** para entrar en la página Configuración de acceso a la **red**.

Network Access Configuration

Associated AP Group ?	STA VLAN ID ?	STA DHCP Service ?	Network Type	Support Radio ?	Action
Default	ID		2.4G&5G		+ Add

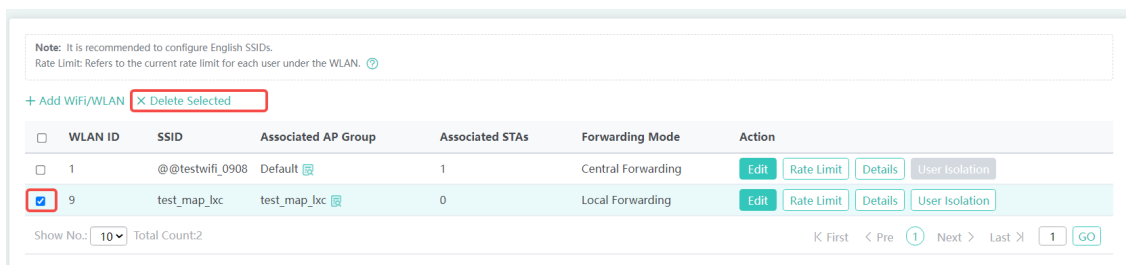
Finished
Previous

Parámetro	Descripción
Grupo de AP asociado	Especifique qué AP transmiten las señales para este Wi-Fi. Por lo general, la señal de un solo punto de acceso Wi-Fi es transmitida por varios puntos de acceso. Estos AP están organizados en un grupo para facilitar la administración. Si no se configura ningún grupo de puntos de acceso, todos los puntos de acceso transmiten la señal Wi-Fi de forma predeterminada.
STA VLAN ID	Introduzca la VLAN a la que pertenecen las STA de este Wi-Fi.

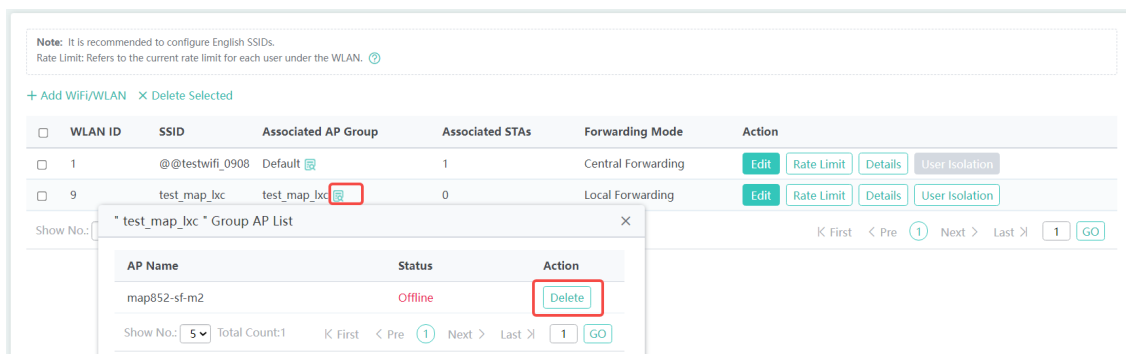
Servicio DHCP de STA	<p>Los STA que se conectan a esta red WLAN se pueden asignar con direcciones IP de un grupo de direcciones configurado en el dispositivo local u otros dispositivos. Está configurado en otros dispositivos de forma predeterminada. Si elige configurar el grupo de direcciones en el dispositivo local, haga clic en Servicio DHCP de STA para redirigir a la página Configurar DHCP en CA.</p> <hr/> <p>Nota</p> <p>Las direcciones IP asignadas por DHCP a los STA deben estar en el mismo segmento de red que la VLAN de STA.</p>
Tipo de red	Especifique los tipos de red compatibles con este Wi-Fi. De forma predeterminada, admite las bandas de 2,4 GHz y 5 GHz.
Radio de apoyo	Especifique las radios compatibles con el AP para transmitir la señal Wi-Fi. Todas las radios son compatibles de forma predeterminada.

2. Eliminación de WLAN


Seleccione la WLAN que desea eliminar y haga clic en **Eliminar seleccionados**. Haga clic en **Aceptar** en la ventana emergente.

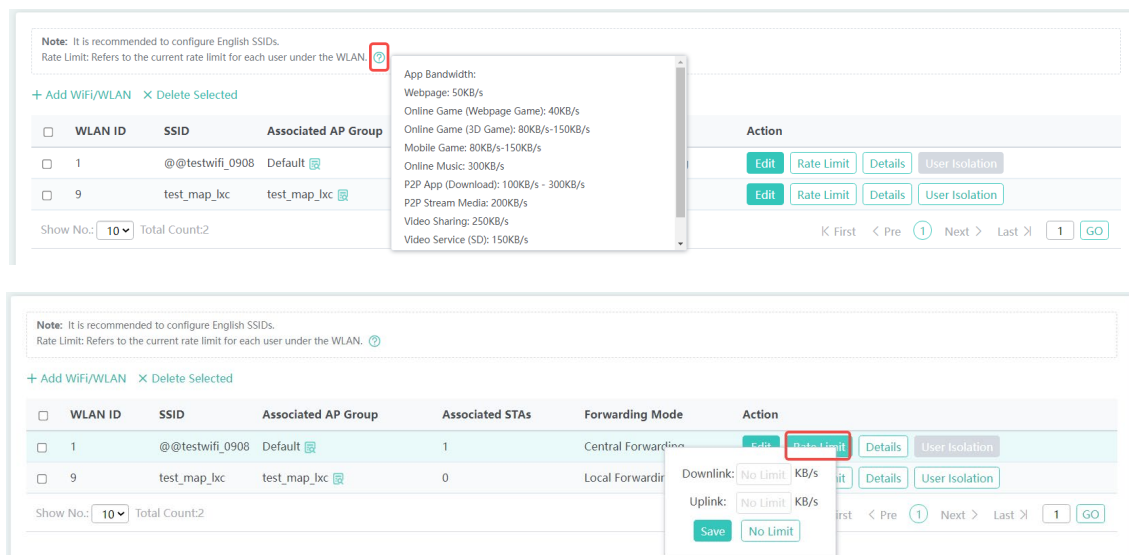


- (1) Visualización del grupo AP asociado: Haga clic  en la **columna Grupo AP asociado** para mostrar o eliminar AP en el grupo AP.



3. Limitación de velocidad

Para configurar los límites de velocidad de enlace ascendente y descendente para una red Wi-Fi, haga clic para  ver el ancho de banda típico para escenarios comunes de descarga de aplicaciones. Haga clic en **Límite de velocidad** para configurar la velocidad máxima de enlace ascendente y descendente en la ventana emergente y haga clic en **Guardar**.

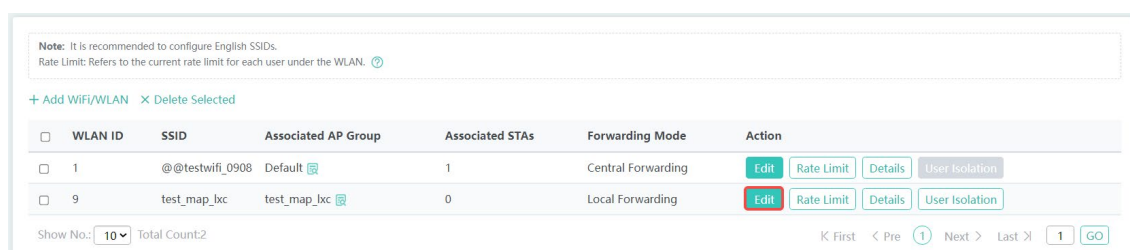


The screenshot shows the WLAN configuration interface. A table lists WLANs with columns: WLAN ID, SSID, Associated AP Group, and Action. Two WLANs are listed: ID 1 with SSID @@testwifi_0908 and ID 9 with SSID test_map_lxc. The 'Action' column for each WLAN has buttons: Edit, Rate Limit, Details, and User Isolation. The 'Rate Limit' button for WLAN 1 is highlighted with a red box. A dialog box titled 'Rate Limit' is open, showing typical bandwidths for various applications: App Bandwidth, Webpage (50KB/s), Online Game (40KB/s), Online Game (3D Game) (80KB/s-150KB/s), Mobile Game (80KB/s-150KB/s), Online Music (300KB/s), P2P App (Download) (100KB/s - 300KB/s), P2P Stream Media (200KB/s), Video Sharing (250KB/s), and Video Service (SD) (150KB/s). The dialog also has 'Downlink' and 'Uplink' sections, each with 'No Limit' and 'KB/s' options, and a 'Save' button.

4. Edición de WLAN


(1) Edición de la información sobre la WLAN añadida

Haga clic en **Editar** en la columna **Acción** para editar la WLAN existente. Una ventana emergente mostrará la información sobre esta WLAN. Una vez editada la información sobre la WLAN, haga clic en **Finalizar**. Se muestra un mensaje que indica que la operación se ha realizado correctamente.



The screenshot shows the WLAN configuration interface. The table is the same as in the previous screenshot. The 'Edit' button in the 'Action' column for WLAN 1 is highlighted with a red box. The dialog box is not visible in this screenshot.

(2) Establecer el límite de velocidad para la WLAN agregada

Para establecer los límites de velocidad de carga y descarga para la WLAN agregada, haga clic en el  icono para ver el ancho de banda requerido en escenarios comunes de descarga de aplicaciones. Haga clic en **Límite de frecuencia**. En la página que se muestra, establezca las tasas máximas de carga y descarga y haga clic en **Guardar**.

Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.

+ Add WiFi/WLAN × Delete Selected

WLAN ID	SSID	Associated AP Group
1	ap9861	ap9861

Show No.: 10 Total Count: 1

App Bandwidth:

- Webpage: 50KB/s
- Online Game (Webpage Game): 40KB/s
- Online Game (3D Game): 80KB/s-150KB/s
- Mobile Game: 80KB/s-150KB/s
- Online Music: 300KB/s
- P2P App (Download): 100KB/s - 300KB/s
- P2P Stream Media: 200KB/s
- Video Sharing: 250KB/s
- Video Service (SD): 150KB/s

Mode: Edit Rate Limit Details User Isolation

K First < Pre 1 Next > Last 1 GO

(3) Visualización de los detalles de la WLAN

Haga clic **en Detalles** en la columna Acción y aparecerá una ventana que muestra los detalles de la WLAN.

Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.

+ Add WiFi/WLAN × Delete Selected

WLAN ID	SSID	Associated AP Group	Associated STAs	Forwarding Mode	Action
1	@@testwifi_0908	Defa	@@testwifi_0908	Details	Details User Isolation
9	test_map_lxc	test			Details User Isolation

Show No.: 10 Total Count: 2

Details

STA VLAN ID: 1

Online Registration: Off

Encryption Type: psk

WiFi Password: 11223344

SSID code: utf-8

STA Limit: No limit

Broadcast SSID: Yes

5G-prior Access: Off

Network OFF Period: Never

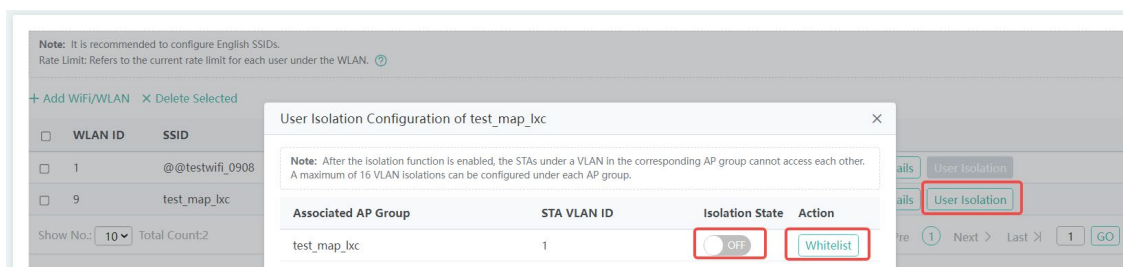
< Pre 1 Next > Last 1 GO

(4) Configuración del aislamiento de usuario

El aislamiento basado en SSID es equivalente al aislamiento de VLAN basado en grupo AP. Haga clic **en Aislamiento de usuario** en la columna **Acción** y aparecerá una ventana emergente que muestra la **página Configuración de aislamiento de usuario**.

Actualmente, la configuración de aislamiento de usuario solo se admite en el modo de reenvío local.

Activa o desactiva el interruptor **Estado de aislamiento**. Haga clic en **Lista blanca y** aparecerá la ventana **Configuración de lista blanca**.



Configure la lista blanca y surtirá efecto en función del grupo AP asociado.

Whitelist Configuration of test_map_lxc AP Group

Note: Up to 64 whitelists can be configured (MAC or IP types are supported). When there is only one row and the whitelist address is empty, saving the configuration will clear the whitelist of currently selected range.

☐ Show All Whitelist (Switching will lose unsaved configuration)

STA VLAN ID	Whitelist Type	Whitelist Address(MAC/IP)	Action
1	MAC		+Add

[Cancel](#) [Save](#)

Parámetro	Descripción
STA VLAN ID	Seleccione la VLAN a la que se aplica la lista blanca. Seleccione solo las VLAN ya asignadas en este grupo de AP.
Tipo de lista blanca	Se admiten listas blancas basadas en direcciones MAC y direcciones IP.
Dirección de lista blanca (MAC/IP)	Al establecer Tipo de lista blanca en MAC , no se admiten las direcciones de difusión y multidifusión. Al establecer el tipo de lista blanca en IP , no se admiten las direcciones IP 0.0.0.0 y 255.255.255.255.

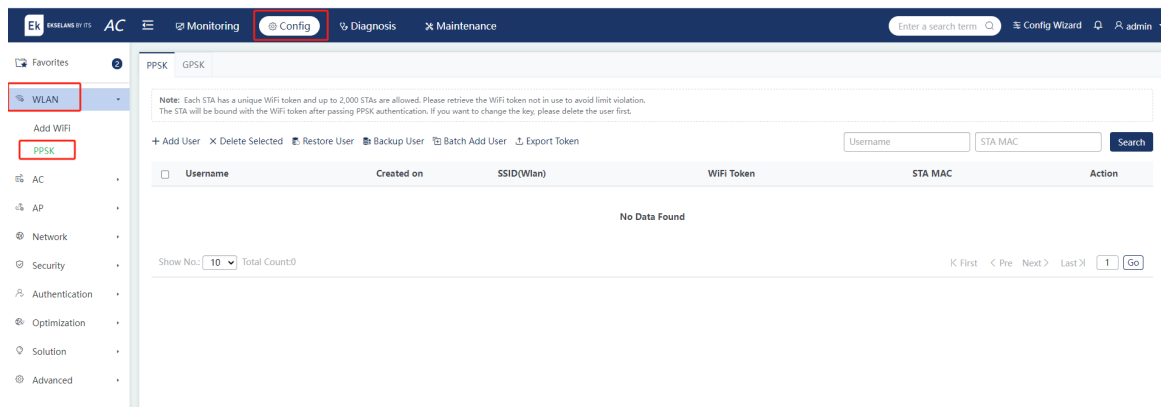
5.1.2 PPSK (en inglés)

Elija **Config > WLAN > PPSK**.

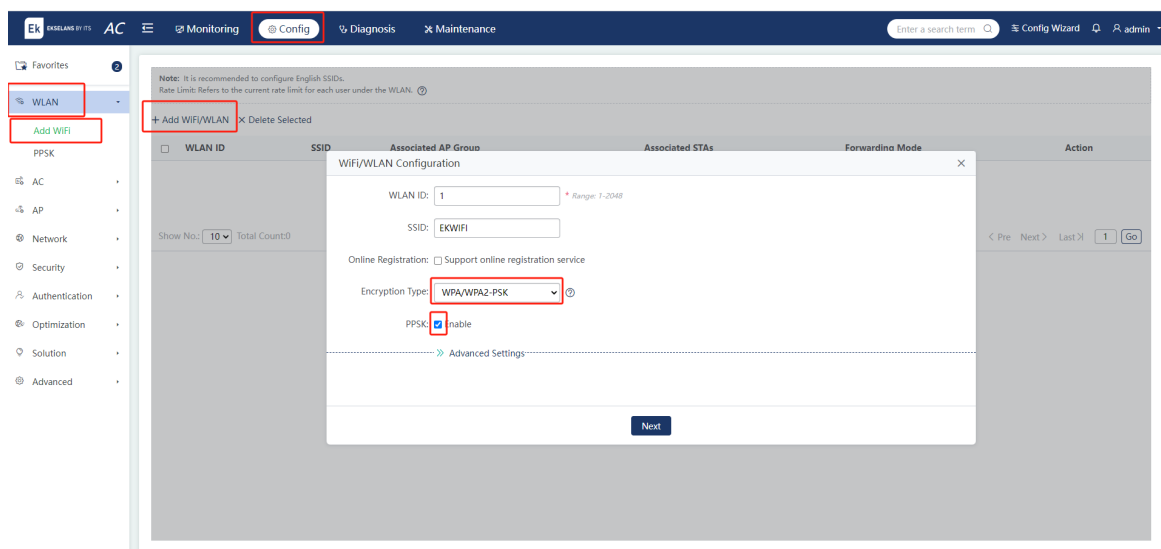
La clave privada precompartida (PPSK) incluye dos tipos: PPSK y la clave precompartida generalizada (GPSK), que se configuran por separado en dos pestañas. PPSK y GPSK admiten hasta 2.000 claves en conjunto.

1. PPSK (en inglés)

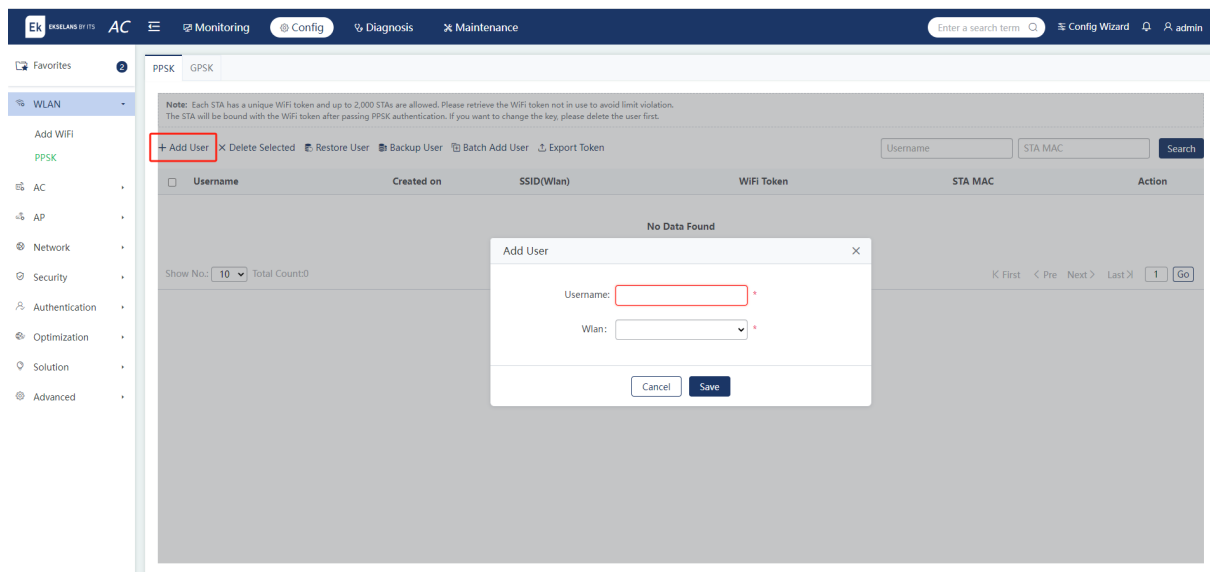
El administrador puede configurar cuentas de usuario aquí. Se pueden generar varias claves en función de un nombre de usuario.



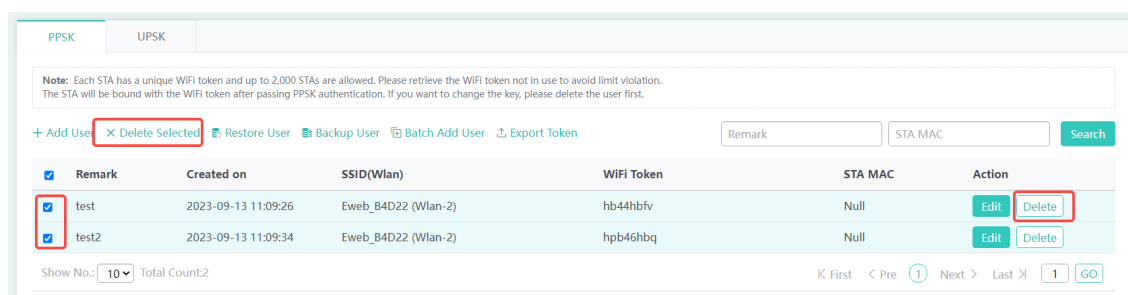
PPSK solo es compatible con WLAN que utilizan WPA/WPA2-PSK. Elija **WPA/WPA2-PSK** como tipo de cifrado y habilite PPSK en la página **Configuración de WiFi/WLAN**.



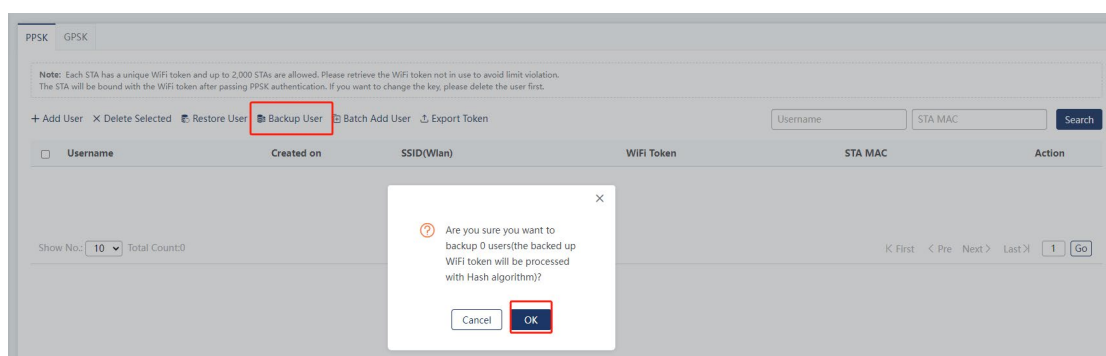
- (1) Agregar usuarios: haga clic en **Agregar usuario** e ingrese comentarios en la ventana emergente. Seleccione una WLAN y haga clic en **Guardar**. Un nombre de usuario se puede agregar varias veces, con una clave única generada cada vez.



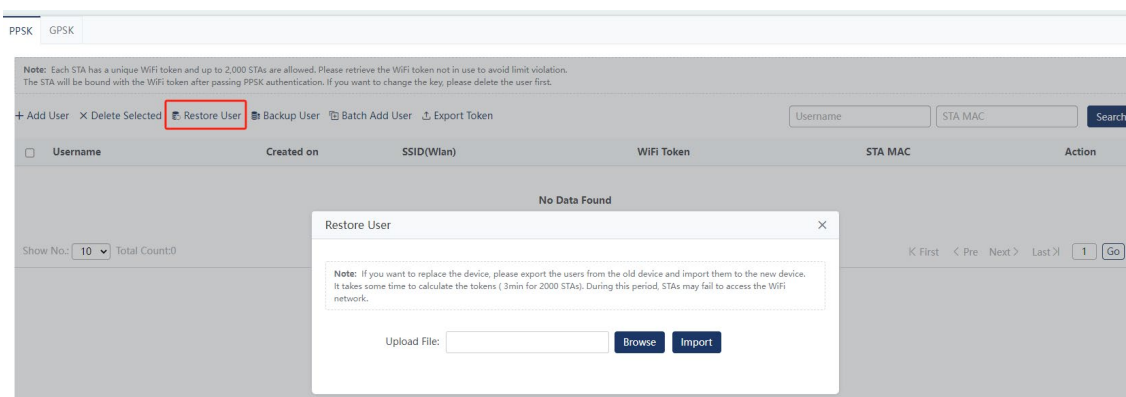
- (2) Eliminación de usuarios: haga clic en **Eliminar** en la columna Acción para eliminar un usuario. Seleccione varios usuarios y haga clic en **Eliminar seleccionados** para eliminar usuarios por lotes.



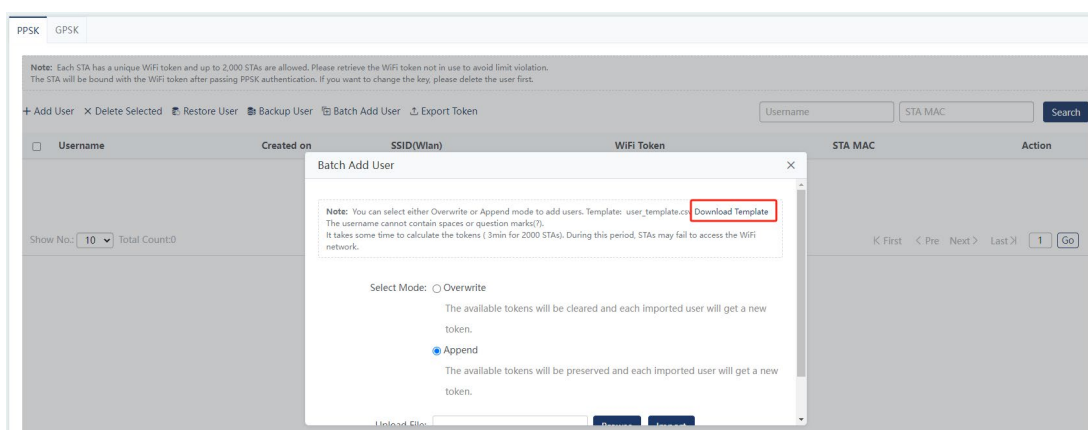
- (3) Copia de seguridad de los datos del usuario: Haga clic en **Copia de seguridad del usuario** y en **Aceptar** en la ventana emergente para descargar los datos en el dispositivo local o cargar los datos en otros dispositivos para realizar una copia de seguridad de los datos.



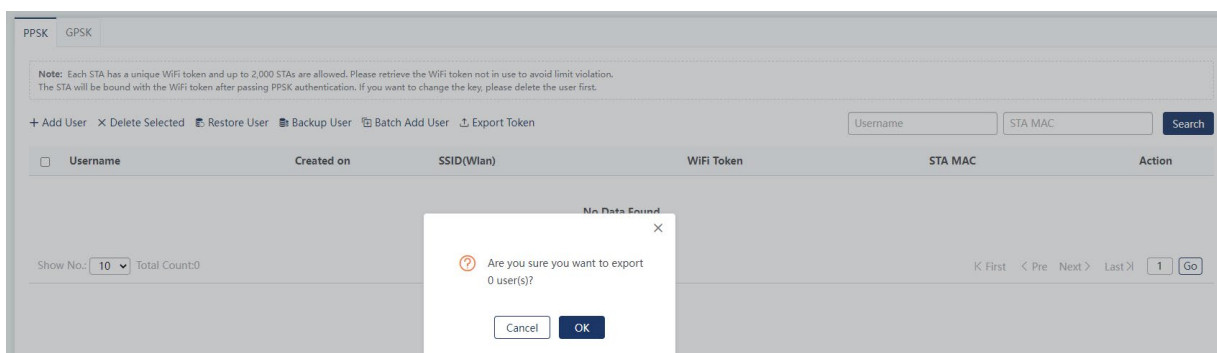
- (4) Restaurar datos de usuario: Haga clic en **Restaurar usuario** para importar la copia de seguridad de los datos de usuario en el dispositivo actual.



- (5) Agregar usuarios por lotes: haga clic en **Agregar usuario por lotes**. Haga clic en **Descargar plantilla** en la página **Agregar usuario por lotes**. Agregue nombres de usuario en el archivo de plantilla. Seleccione un método para agregar usuarios y haga clic en **Guardar**. Haga clic en **Examinar** para seleccionar el archivo de plantilla y, a continuación, haga clic en **Importar** para importar el archivo de plantilla para agregar usuarios por lotes.



- (6) Exportación de claves: haga clic en **Exportar token** para exportar todos los usuarios y claves al dispositivo local.

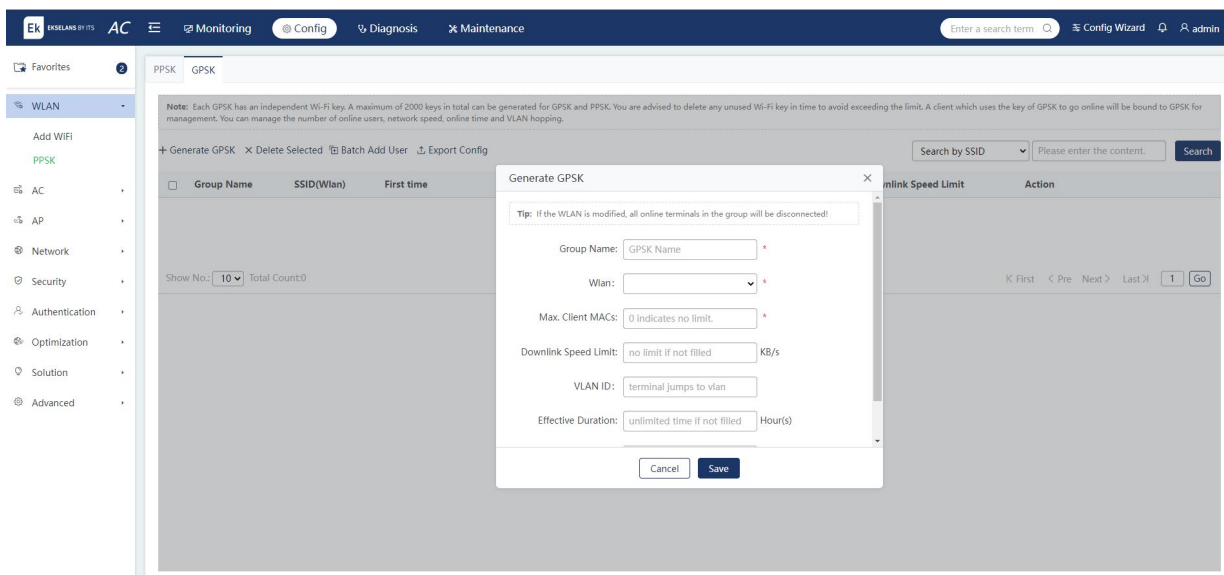


2. GPSK (en inglés)

Cada GPSK es una llave Wi-Fi independiente. PPSK y GPSK admiten hasta 2.000 claves en conjunto. Elimine y recicle rápidamente las claves de Wi-Fi no utilizadas para evitar exceder el límite. Los STA que utilizan el GPSK para el inicio de sesión se administran en función del GPSK. El número de STA,

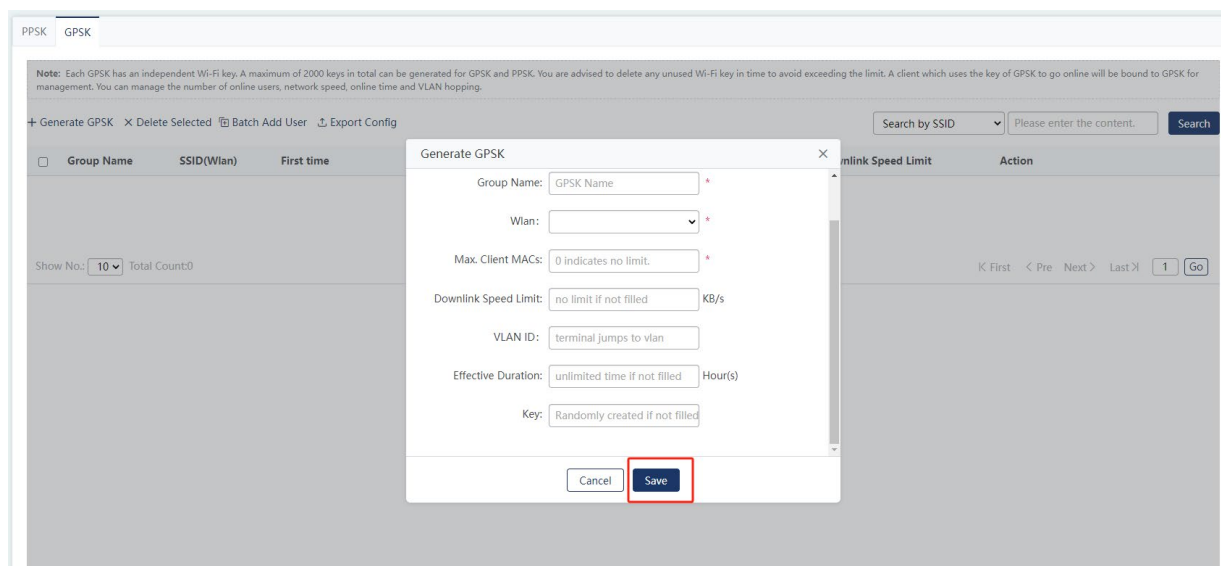
las velocidades de datos, el tiempo de actividad y la redirección de VLAN se pueden administrar en esta página.

- (1) Generar un GPSK: Haga clic en **Generar GPSK** 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.

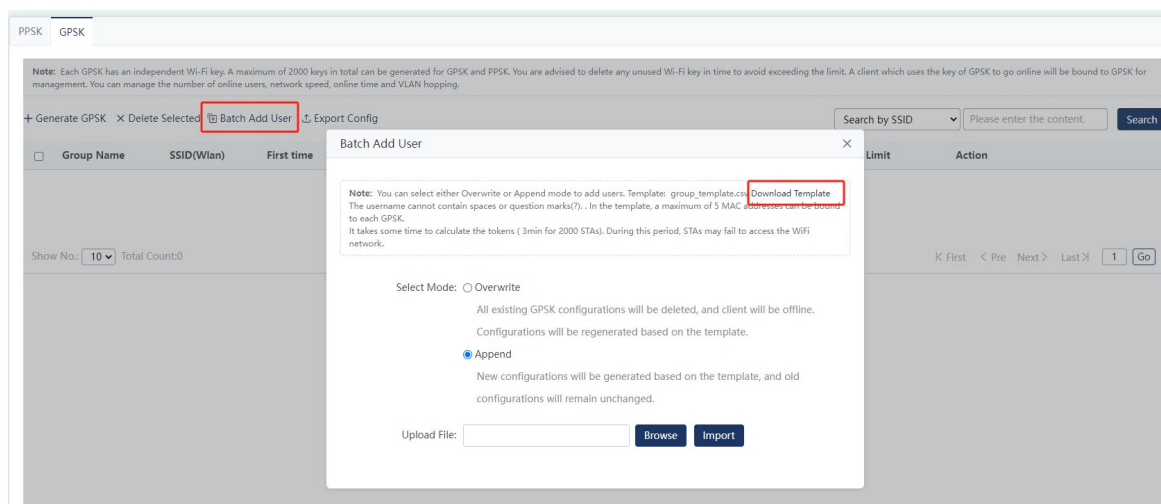


Parámetro	Descripción
Nombre del grupo	Introduzca un nombre de grupo UPSK. Introduzca una cadena de 1 a 31 caracteres. No se permiten espacios, comillas dobles, comas ni caracteres de ancho completo.
WLAN (Conexión WLAN)	Seleccione el ID de WLAN que se asociará con el UPSK. Solo están disponibles las WLAN habilitadas con PPSK.
Máx. MAC de cliente	Introduzca el número máximo de direcciones MAC que se pueden asociar. El valor oscila entre 0 y 65.535. El valor 0 indica que no hay límite.
Límite de velocidad de enlace descendente	Configure el límite de velocidad de enlace descendente en KB por segundo. El valor oscila entre 8 y 65.280. Este campo es opcional.
VLAN ID	Una vez configurado este parámetro, el STA se redirigirá a esta VLAN al iniciar sesión. El valor oscila entre 1 y 4.096. Este campo es opcional.
Duración efectiva	Indica el período de validez de la clave en horas. El valor oscila entre 1 y 100. Este campo es opcional. La clave es válida de forma permanente si se deja en blanco.
Llave	La llave se puede configurar manualmente. Introduzca una cadena de 8 a 13 caracteres, que conste de números o letras. Este campo es opcional. Se generará una clave aleatoria si se deja en blanco.

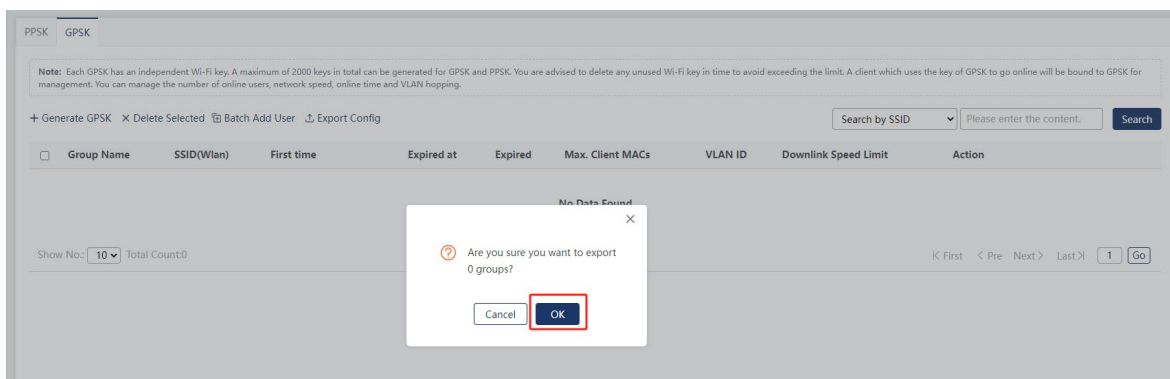
- (2) Usuarios de edición: haga clic en **Editar** en la columna **Acción**. Edite los campos en la ventana emergente y haga clic en **Guardar**.



- (3) Eliminación de usuarios: haga clic en **Eliminar** en la columna **Acción** para eliminar un usuario. Seleccione varios elementos y haga clic en **Eliminar seleccionados** para eliminar usuarios por lotes.
- (4) Agregar usuarios por lotes: haga clic en **Agregar usuario por lotes**. Haga clic en **Descargar plantilla** en la página **Agregar usuario por lotes**. Agregue información de UPSK en el archivo de plantilla. Seleccione un método para agregar usuarios y haga clic en **Guardar**. Haga clic en **Examinar** para seleccionar el archivo de plantilla y, a continuación, haga clic en **Importar** para importar el archivo de plantilla para agregar usuarios por lotes.



- (5) Exportación de configuración: Haga clic en **Exportar configuración** para exportar todos los datos de UPSK al dispositivo local.



- (6) Gestión de direcciones MAC de clientes: Incluye la gestión de clientes dinámicos y estáticos. En la página de administración de clientes dinámicos, puede cerrar la sesión de los clientes dinámicos manualmente. En la página de administración de clientes estáticos, puede agregar o eliminar clientes estáticos.

5.2 Corriente alterna

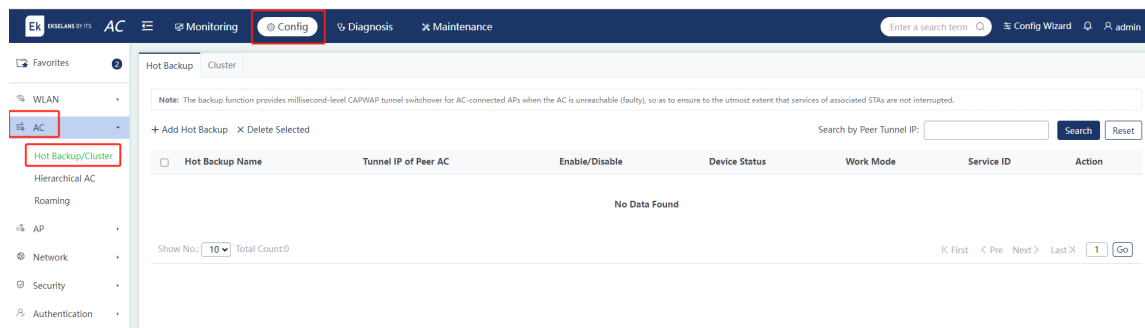
5.2.1 Copia de seguridad en caliente/clúster

La **página Copia de seguridad en caliente/Clúster** incluye **las pestañas** Copia de seguridad en caliente y Clúster.

1. Copia de seguridad en caliente

Elija Config > AC > Hot Backup/Cluster > Hot Backup.

En el modo Fit AP, el AP tiene que establecer un túnel CAPWAP con la AC para funcionar normalmente. La copia de seguridad en caliente permite que el AP interconectado con la AC cambie el túnel CAPWAP en milisegundos cuando falla la CA. Esto permite que el STA cambie rápidamente al AC de respaldo y garantiza servicios ininterrumpidos, asegurando la disponibilidad y estabilidad de los STA.



- (1) Adición de la copia de seguridad en caliente

Haga clic en **Agregar copia de seguridad activa** para ingresar a la página de configuración.

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

+ Add Hot Backup × Delete Selected

Search by Peer Tunnel IP:

Hot Backup Name	Tunnel IP of Peer AC	Enable/Disable	Device Status	Work Mode	Service ID	Action
<div> <div>Show No.: 10 ▼ Total Count: 0</div> <div> <div>Hot Backup Name</div> <div>Tunnel IP of Peer AC</div> <div>Local IP</div> <div>Backup: <input type="checkbox"/> Enable If the hot backup capacity exceeds the limit, the device cannot be enabled with hot backup</div> <div>Work Mode: Please select ▼</div> <div>Service ID: New <input type="text"/></div> </div> <div> <div>AP Group: ▼ [AP Settings]</div> <div> <div>DHCP Service: ▼ [DHCP Settings]</div> <div>VRRP Port Group: ▼ [VRRP Settings]</div> <div>Priority: Medium ▼</div> </div> </div> </div>						

K First < Pre Next > Last 1 Go

Parámetro	Descripción
Nombre de la copia de seguridad en caliente	Configure el nombre de la copia de seguridad en caliente.
IP de túnel de AC par	Ingresa la dirección IP en el lado del par del túnel para las comunicaciones entre el AP y la CA. La dirección IP de la interfaz Loopback0 se configura como la dirección IP del túnel de forma predeterminada.
Local IP	Si la comunicación no se establece a través de la interfaz Loopback0, configure la dirección IP local. Normalmente, la dirección IP de la interfaz se configura como la dirección IP local. Configure este parámetro haciendo clic en Información de la interfaz para ver los detalles de la interfaz.
Copia de seguridad	Habilite o deshabilite la copia de seguridad en caliente. Esta función no se puede habilitar si el número de copias de seguridad en caliente alcanza el límite.

Modo de trabajo	<p>El modo de copia de seguridad en caliente y el modo de conmutación rápida son compatibles con una AC normal.</p> <p>Los modos de trabajo se describen de la siguiente manera:</p> <p>Modo de copia de seguridad en caliente: se aplica a escenarios con requisitos de rendimiento estable. Para evitar el aleteo en modo de espera en caliente, se recomienda adoptar este modo.</p> <p>Modo de conmutación rápida: se aplica a escenarios con altos requisitos de rendimiento de conmutación. Este modo puede dar lugar a un cambio frecuente de copia de seguridad en caliente.</p> <p>Modo frío: se aplica a escenarios de AC jerárquicos.</p>
ID de servicio	Introduzca el ID de servicio, es decir, el ID de contexto. Este campo es opcional.
Grupo AP	Los grupos de AP para dispositivos activos y de respaldo deben configurarse de manera consistente. Haga clic en Configuración de AP para agregar grupos de AP para el dispositivo actual.
Ajustes avanzados	<p>La configuración avanzada no se admite en escenarios de AC virtual (VAC) y AC jerárquica (CA de sede central y AC de sucursales).</p> <p>Solo son compatibles con AC normales.</p>
Grupo de puertos VRRP	Los grupos VRRP para dispositivos activos y de respaldo deben configurarse de manera coherente. Haga clic en Configuración de VRRP para agregar VRRP para el dispositivo actual.
Servicio DHCP	El DHCP para los dispositivos activos y de respaldo debe configurarse de forma coherente. Haga clic en Configuración de DHCP para agregar DHCP para el dispositivo actual.
Prioridad	Seleccione las prioridades de los dispositivos de copia de seguridad en caliente, incluidas tres opciones: media, alta y baja.

- (2) Eliminación de dispositivos de copia de seguridad en caliente: haga clic en **Eliminar** en la columna **Acción** para eliminar un elemento. Seleccione varios elementos y haga clic en **Eliminar seleccionados** para eliminar elementos por lotes.

Hot Backup Cluster

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

+ Add Hot Backup **X Delete Selected**

Search by Peer Tunnel IP:

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

Show No.: Total Count: 1

K First < Pre **1** Next > Last X

- (3) Edición de dispositivos de copia de seguridad en caliente: haga clic en **Editar** en la columna **Acción**. Edite los campos en la ventana emergente y haga clic en **Guardar**.

Hot Backup

Cluster

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

+ Add Hot Backup

✕ Delete Selected

Search by Peer Tunnel IP:

SearchReset

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

Show No.: 10▼Total Count:1

K First

< Pre

1

Next >

Last X

1

GO

2. Clúster

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

Un clúster de AC incluye varias AC para un AP. Cuando el AP no se puede interconectar con una CA, el AP puede usar una AC de respaldo. Evita la indisponibilidad de los puntos de acceso debido a una falla de CA, lo que mejora la confiabilidad de las redes inalámbricas.

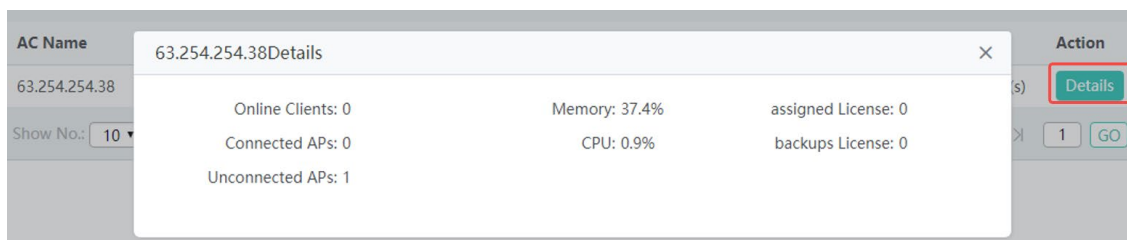
Configure hasta tres AC de respaldo basadas en direcciones IPv4 o IPv6.

5.2.2 CA jerárquica

Elija **Config > AC > Hierarchical AC**.

Los detalles de los AC jerárquicos se muestran en esta página.

- (1) Visualización de detalles de CA: Haga clic en **Detalles** para ver los detalles de CA.



5.2.3 Itinerancia

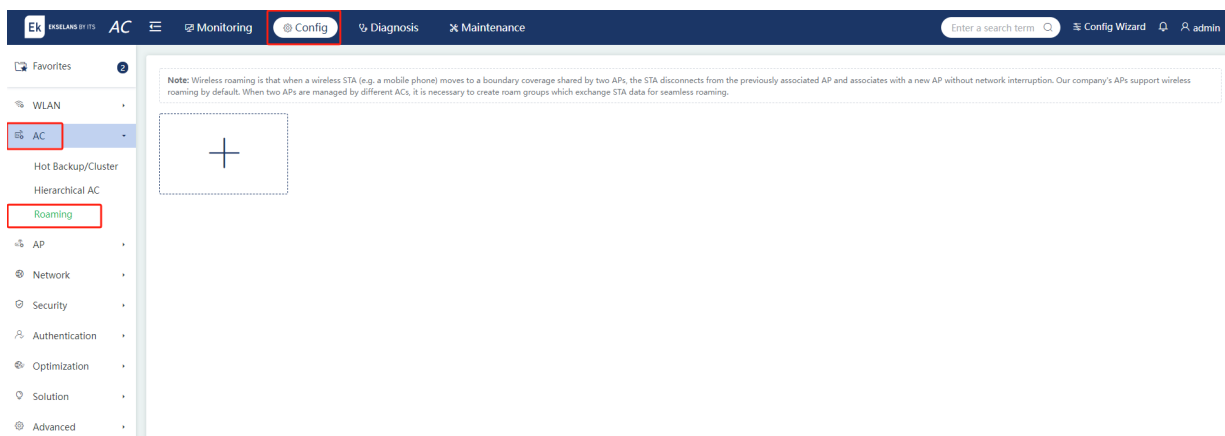
Elija **Config > AC > Roaming**.

Roaming se refiere a la capacidad de un STA para conectarse y utilizar los servicios de otro AP fuera de su área de cobertura de red original. El grupo de itinerancia de AC permite a los STA desplazarse a través de AP con experiencia consistente.

El alcance de itinerancia de los STA no puede extenderse infinitamente. Para permitir que los STA se muevan a través de los AP asociados con diferentes AC y administren el rango de roaming de los STA, los AC en el área donde se mueve el STA se mueven a un grupo de roaming.

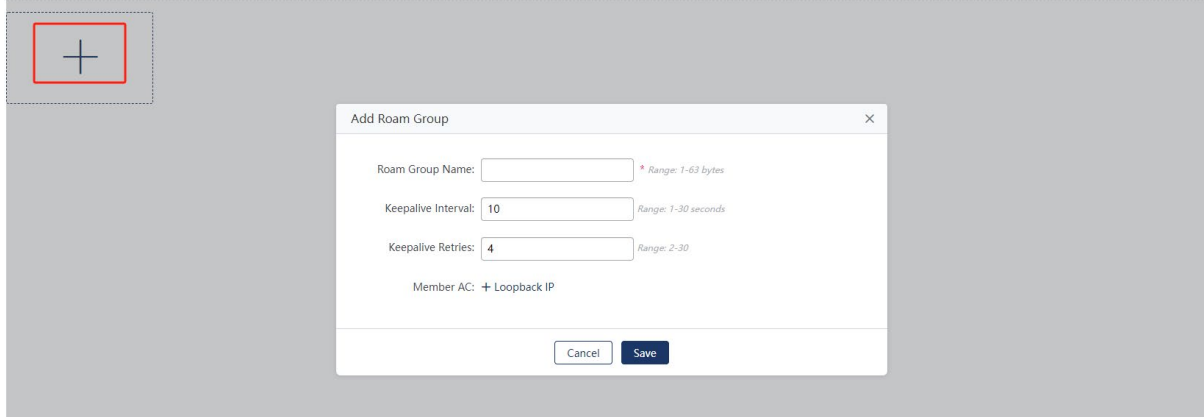
Nota

El número de dispositivos miembros en el grupo de itinerancia está limitado para garantizar la eficiencia y la fiabilidad de las comunicaciones entre los AC de un grupo de itinerancia. Cada grupo de itinerancia contiene un máximo de 24 miembros de CA.

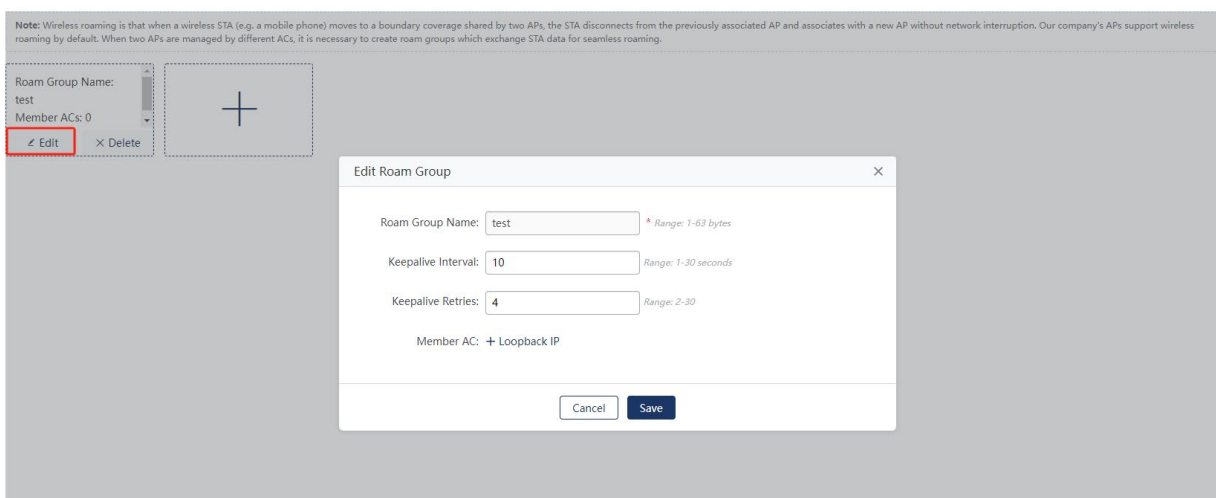


- (1) Adición de grupos de itinerancia: haga clic en el **botón +** de la página **Itinerancia** para añadir un grupo de itinerancia. El campo **Nombre del grupo de itinerancia** es obligatorio, mientras que los demás campos son opcionales. Se pueden seleccionar AC de varios miembros. Al hacer clic en **Guardar**, el grupo de itinerancia se mostrará en la página **Itinerancia** después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.

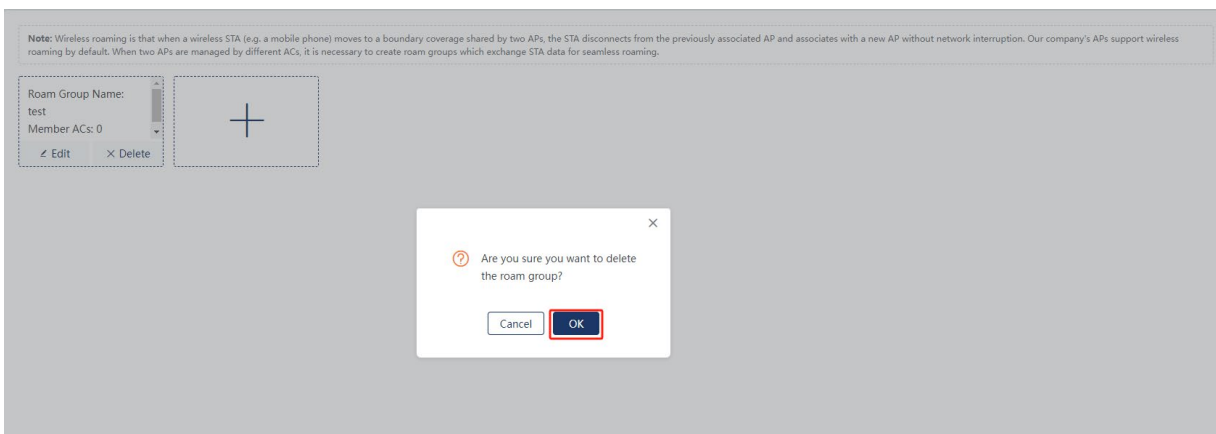
Note: Wireless roaming is that when a wireless STA (e.g. a mobile phone) moves to a boundary coverage shared by two APs, the STA disconnects from the previously associated AP and associates with a new AP without network interruption. Our company's APs support wireless roaming by default. When two APs are managed by different ACs, it is necessary to create roam groups which exchange STA data for seamless roaming.



- (2) Edición de grupos móviles: haz clic **en Editar** en el cuadro de un grupo móvil. Edite los campos en la ventana **Editar grupo de itinerancia** y haga clic en **Guardar**.



- (3) Eliminación de grupos móviles: haga clic **en Eliminar** en el cuadro del grupo móvil que desea eliminar y haga clic en **Aceptar** en la ventana emergente.

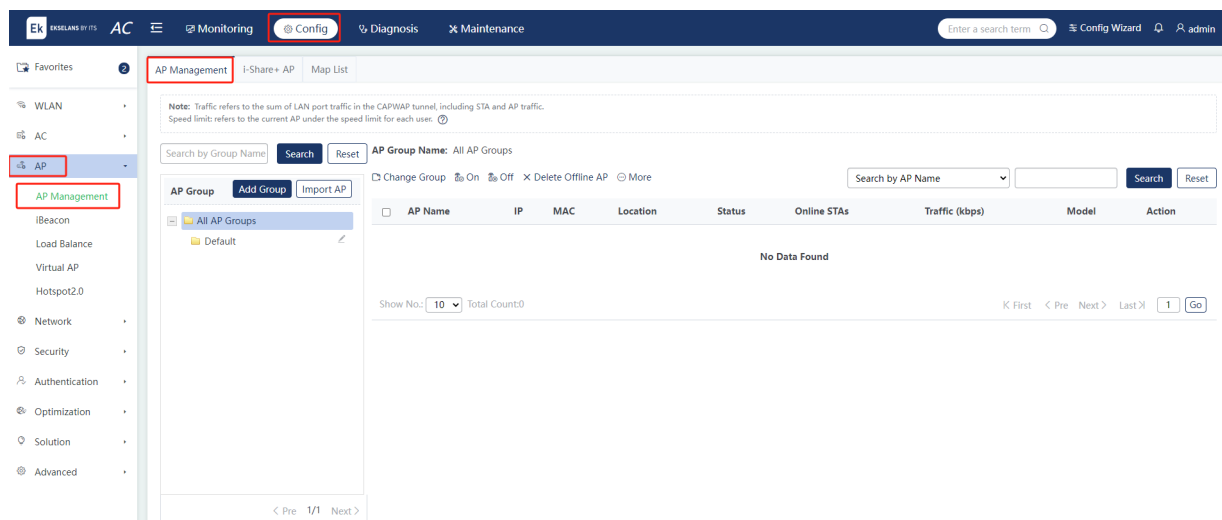


5.3 AP

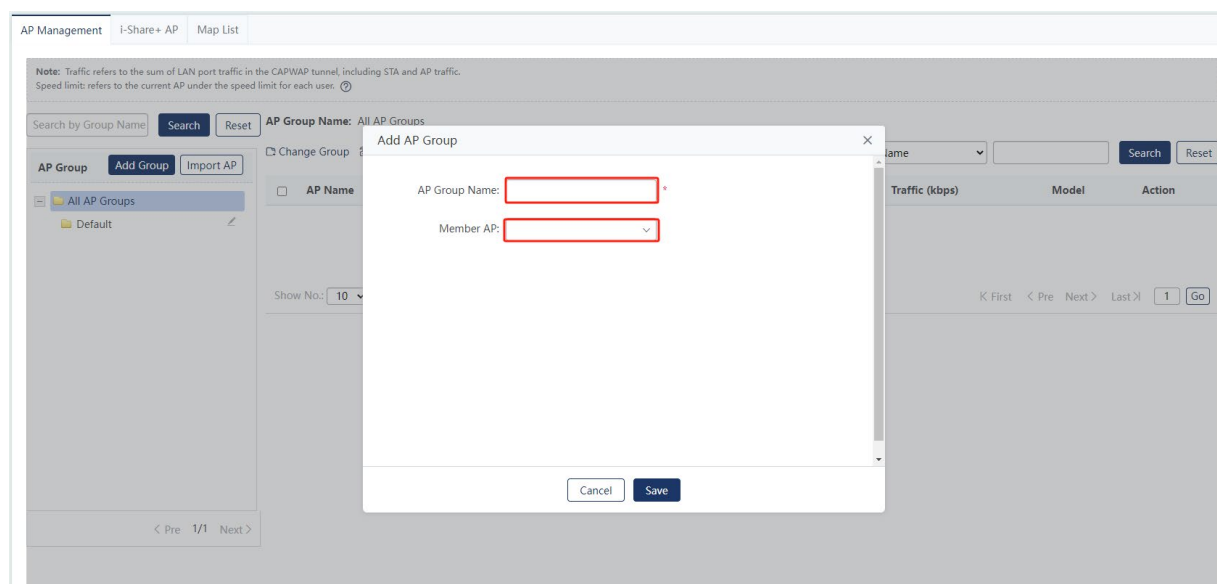
5.3.1 Gestión de AP

Elija **Config > AP > AP Management**.

Los AP deben asociarse con una AC y agregarse a un grupo de AP antes de proporcionar servicios STA inalámbricos. Todos los AP recién agregados se asignan al grupo de AP predeterminado.



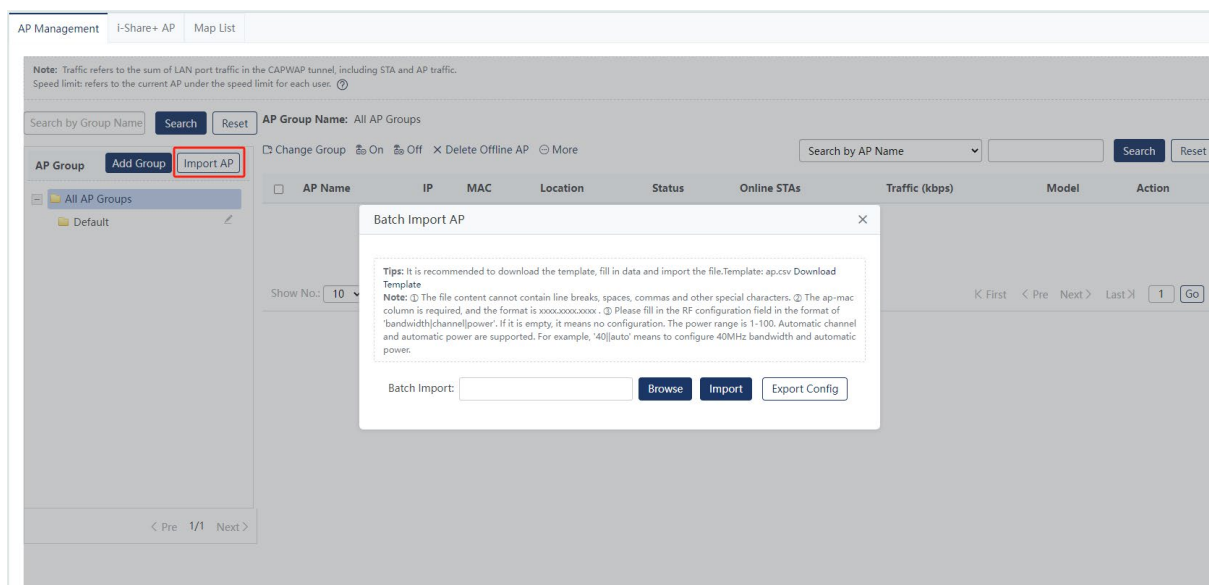
- (1) Agregar grupos de AP: Haga clic en Agregar grupo y aparecerá la **ventana Agregar grupo de AP**. Ingrese el nombre del grupo de AP, seleccione los AP miembros que se agregarán a este grupo de AP y haga clic en **Guardar**.



Parámetro	Descripción
Nombre del grupo	Este campo es obligatorio.

AP	
Miembro AP	Seleccione los AP miembros que se agregarán a este grupo de AP. Un AP solo se puede agregar a un grupo. Si los AP no se agregan a ningún grupo, se asignan al grupo AP predeterminado.

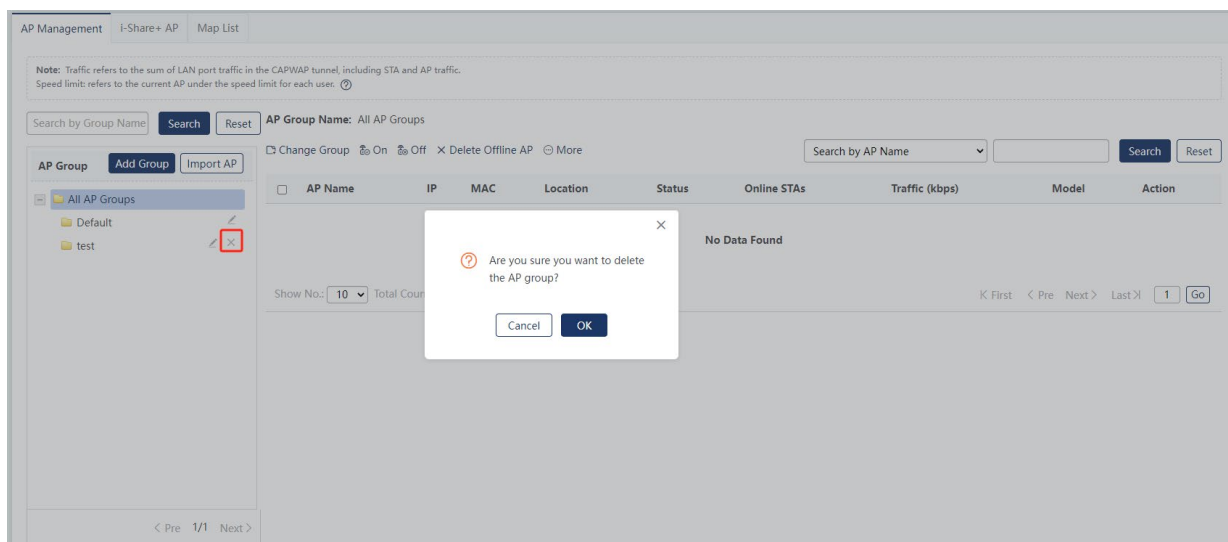
- (2) Importación por lotes de APs: Si se van a importar muchos APs, exporte el archivo de configuración actual. Edite las configuraciones e importe el archivo editado de nuevo al dispositivo para realizar configuraciones por lotes. También puede descargar el archivo de plantilla para editar las configuraciones e importarlo de nuevo al dispositivo.



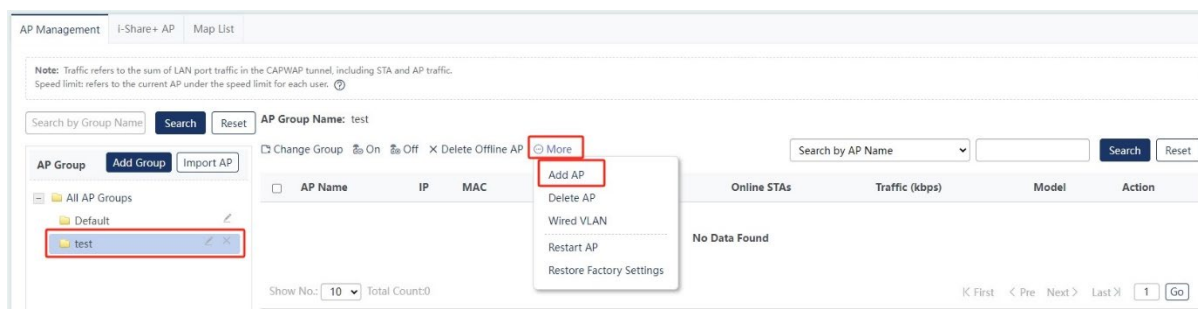
- (3) Eliminación de grupos AP: Seleccione el grupo AP que desea eliminar y haga clic en **x**. Haga clic en **Aceptar** en la ventana emergente para eliminar el grupo AP.

Nota

- El grupo predeterminado no se puede eliminar.
- Después de eliminar un grupo de AP, los AP de este grupo se asignan automáticamente al grupo predeterminado.



- (4) Adición de AP: Haga clic en **Agregar AP** para agregar AP a un grupo. Los **campos AP, Nombre y MAC** son obligatorios, mientras que otros campos son opcionales. Haga clic en **Aceptar** y el AP se mostrará en la lista de AP después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.




Add AP


AP Name:
MAC:
Location: admin

» Advanced Settings

AP Group: test_hotspot_bxc
Telnet Account: admin
Telnet Password:
Tunnel IP:

Parámetro	Descripción
Nombre de AP	Introduzca el nombre del AP. Si el AP está fuera de línea, el nombre del AP no se puede editar.
MAC	Introduzca la dirección MAC del AP. La dirección MAC no se puede editar si el AP está en línea.
Ubicación	Introduzca la ubicación del AP. Por ejemplo, si el AP se implementa en la sala 201 en el piso 19, ingrese 19#201 en este campo.
Grupo AP	Entra en el grupo de los AP. Un AP solo puede pertenecer a un grupo. De forma predeterminada, un AP pertenece al grupo predeterminado .
Cuenta Telnet	Introduzca la cuenta para iniciar sesión en el AP. Tanto la cuenta Telnet como la contraseña son obligatorias.
Contraseña de Telnet	Introduzca la contraseña para iniciar sesión en el AP. Tanto la cuenta Telnet como la contraseña son obligatorias.
IP de túnel	<p>Al AP se le puede asignar una dirección IP a través de DHCP. También puede configurar una dirección IP estática, que requiere la configuración de la dirección de puerta de enlace, la dirección IP del túnel, la dirección IPv4 y la máscara de subred IPv4.</p> <hr/> <p> Cautela</p> <p>Esta configuración puede provocar una desconexión del AP.</p> <hr/>

- (5) Edición de AP: Haga clic **en Editar** en la columna **Acción** y edite la información de AP en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

Parámetro	Descripción
Puerto cableado	El puerto cableado está habilitado de forma predeterminada.
AP IPv4	<p>El AP se puede asignar con una dirección IP a través de DHCP o se puede especificar manualmente con una dirección de puerta de enlace estática, una dirección IP de túnel, una dirección IPv4 de AP y una máscara de subred IPv4 de AP. La puerta de enlace IPv4 AP es el parámetro para configurar la dirección IP estática. Puede configurar la dirección IPv4 de AP, la máscara de subred IPv4 de AP y la puerta de enlace IPv4 de AP ejecutando el comando ip address 2.2.2.2 255.255.255.0 2.2.2.1.</p> <hr/> <p> Cautela</p> <p>Esta configuración puede provocar una desconexión del AP.</p> <hr/>
Máscara IPv4 AP	
Puerta de enlace IPv4 de AP	
SSID sin conexión	Ingrese el SSID transmitido por el AP cuando está desconectado.
Ocultar SSID sin conexión	Muestra u oculta la transmisión SSID por el AP cuando está desconectado.

i Nota

La ventana **Editar AP** muestra las configuraciones en lugar del estado del AP. Ejecute el comando **show ap-config running +name** para mostrar las configuraciones. La lista de AP muestra el estado de AP a través de **getAPList**.

- (6) Eliminación de AP: Seleccione uno o varios elementos en la lista de AP y haga clic en **Eliminar AP**. Haga clic en **Aceptar** en la ventana emergente para eliminar por lotes los AP.
- (7) Reiniciar AP: Seleccione uno o varios elementos en la lista de AP y haga clic en **Reiniciar AP**. Haga clic en **Aceptar** en la ventana emergente para reiniciar los AP.

⚠ Cautela

Esta configuración puede provocar una desconexión del AP.

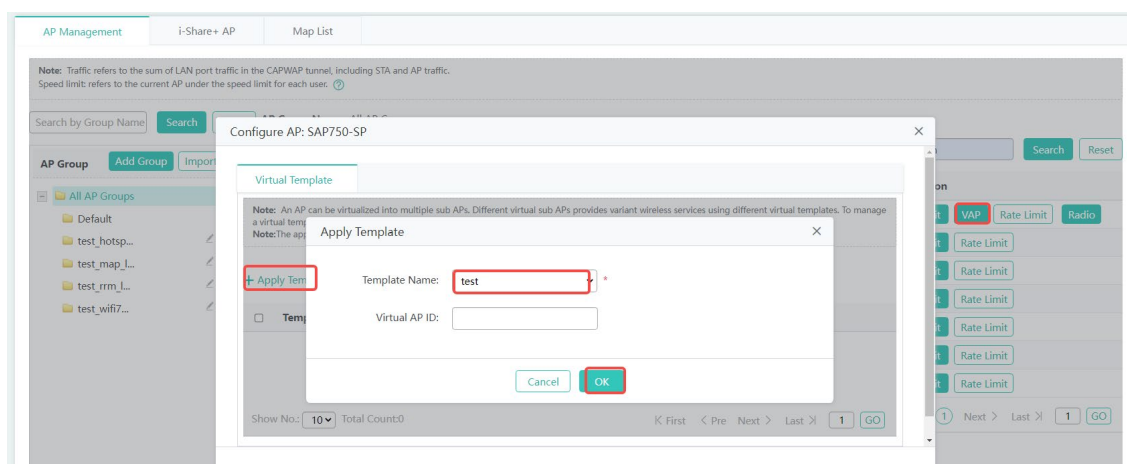
- (8) Restauración de la configuración de fábrica: Seleccione uno o varios elementos en la lista de AP y haga clic en **Restaurar la configuración de fábrica**. Haga clic en **Aceptar** en la ventana emergente para restaurar los AP a la configuración de fábrica.
- (9) Configuración de VLAN cableada: Haga clic en **VLAN cableada** y aparecerá la **ventana VLAN cableada**. Introduzca el ID de VLAN, seleccione el puerto cableado y haga clic en **Guardar**.
- (10) Habilitación de AP: Seleccione uno o varios elementos en la lista de AP y haga clic en **Activado** para habilitar por lotes los radios AP.
- (11) Desactivación de AP: Seleccione uno o varios elementos de la lista de AP y haga clic en **Desactivado** para desactivar por lotes los radios AP.
- (12) Eliminación de puntos de acceso sin conexión: Haga clic en **Eliminar puntos de acceso sin conexión** para eliminar todos los puntos de acceso sin conexión.
- (13) Configuración de la radio: Haga clic en **Radio** en la columna **Acción** y aparecerá la **ventana Configuración de radio WiFi**.

Parámetro	Descripción
Puerto RF	Este campo se muestra solo cuando el AP tiene al menos tres radios.
Red 2.4G	Habilite o deshabilite la radio.
Red 5G	
País o región	Configure el código de país o región para el AP. Es coherente con el código de país o región del AC de forma predeterminada.
Protocolo WiFi	Seleccione el estándar IEEE 802.11 con el que cumple la tarjeta de RF. Las opciones para la red de 2,4 GHz incluyen:

	<p>11bgn, que indica IEEE 802.11b/g/n.</p> <p>11bgn+11ax, que indica IEEE 802.11b/g/n/ax</p> <p>Las opciones para la red de 5 GHz incluyen:</p> <p>11an, que indica IEEE 802.11a/n.</p> <p>11an+11ac, que indica IEEE 802.11a/n/ac.</p> <p>11an+11ac+11ax, lo que indica IEEE 802.11a/n/ac/ax.</p>
Canal WiFi	Seleccione el canal Wi-Fi según el país o la región y el tipo de red.
Poder	<p>Opciones:</p> <p>Automático: Auto</p> <p>Ahorro de energía: el valor de energía es 30.</p> <p>Estándar: El valor de potencia es 80.</p> <p>Mejorado: El valor de potencia es 100.</p> <p>Personalizado: El valor de potencia se personaliza.</p>
Límite de STA	Configure el número máximo de STA admitidos por la radio.
Ancho de banda de frecuencia	Especifique el ancho de banda del canal admitido por la radio.
Recibiendo/Enviando	Habilite o deshabilite la antena de recepción o transmisión.

(14) Limitación de velocidad: haga clic en **Límite de velocidad** en la columna **Acción** para configurar el límite de velocidad de enlace ascendente y descendente.

(15) Configuración de VAP: Haga clic en **VAP** en la columna **Acción** para ingresar a la página **Plantilla virtual**. Haga clic en **Aplicar plantilla** y seleccione un nombre de plantilla. Configure el ID de AP virtual y haga clic en **Aceptar**.

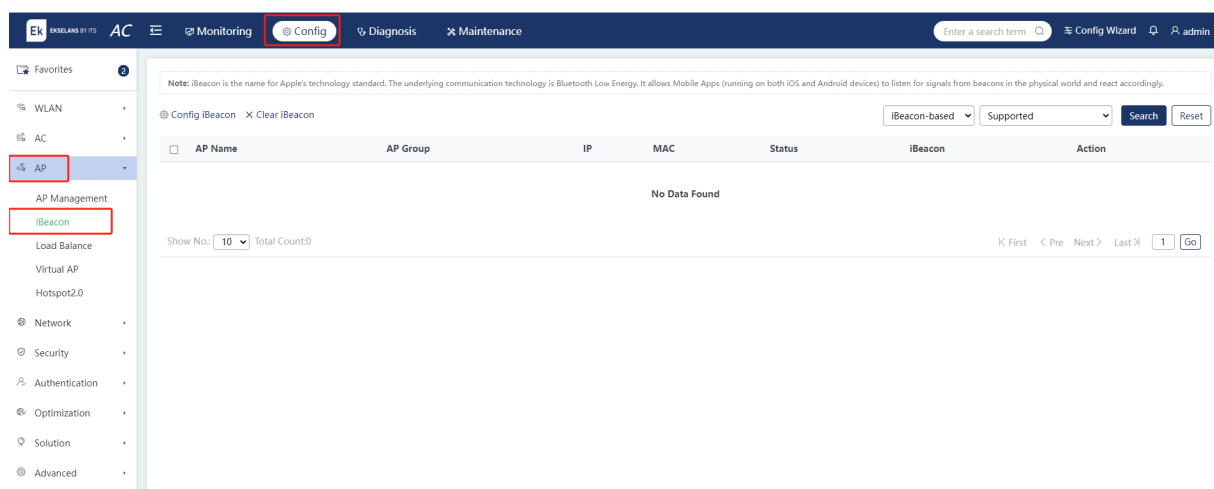


5.3.2 Baliza

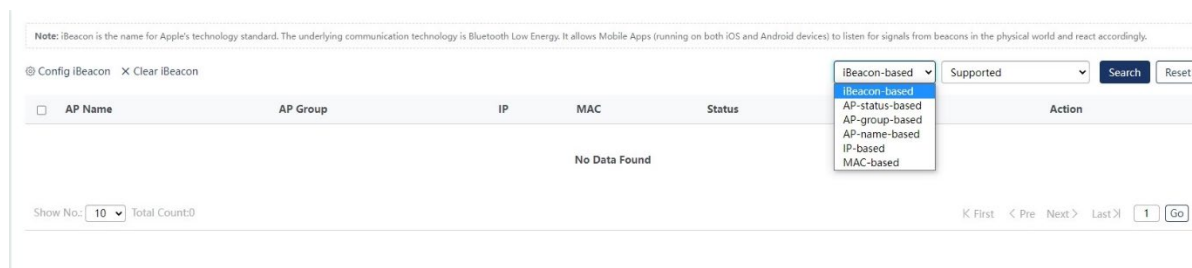
Elija **Config > AP > iBeacon**.

iBeacon es un protocolo basado en la tecnología Bluetooth Low Energy (BLE). Los AP habilitados con iBeacon pueden transmitir un ID especificado generado por un tercero y el software de los clientes responde en consecuencia después de recibir el ID.

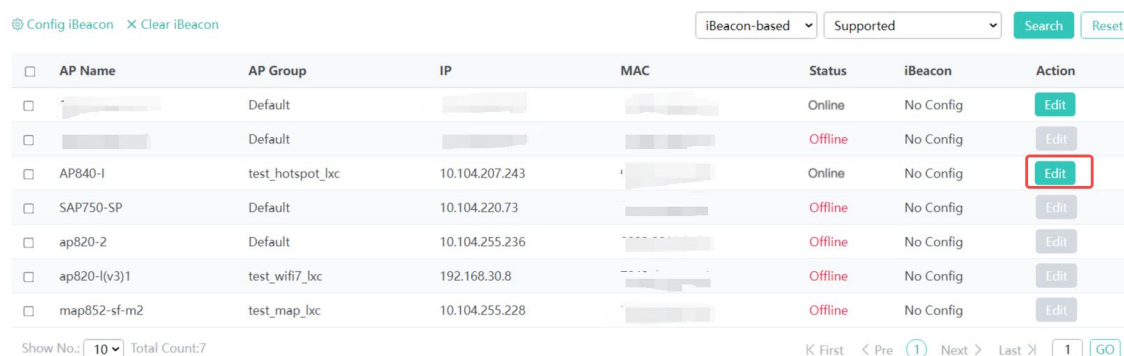
Ejemplo: El centro comercial puede aplicar iBeacon para enviar anuncios a los clientes.



- (1) Búsqueda de AP: Busque AP utilizando el filtro o introduciendo palabras clave. Haga clic en **Restablecer** para borrar los criterios de búsqueda.



- (2) Configuración de iBeacon: Haga clic en Editar en la **columna Acción** para ingresar a la página de configuración de iBeacon. Rellene los parámetros y haga clic en **Guardar**.



Radio 1

UUID:

Major: 0 ~ 65535

Minor: 0 ~ 65535

- (3) Configuración de iBeacon por lotes: Seleccione los elementos de la lista y edite los campos en la **ventana emergente Configuración de lotes de iBeacon**.

Batch Config iBeacon

Note: The following data is provided by the third party (mall).

UUID: * Example: FDA50693-A4E2-4FB1-AFCF-C6EB07647825

Major: * Range: 0 ~ 65535

Minor: * Range: 0 ~ 65535

Cancel OK

- (4) Procesamiento por lotes eliminando iBeacon: Seleccione los elementos de la lista y haga clic en **Borrar iBeacon**.

5.3.3 Equilibrio de carga

Elija **Config > AP > Load Balance**.

Si hay varios AP en la WLAN, se produce una superposición de señales. Los STA se asocian con los AP aleatoriamente, lo que genera una mayor carga en algunos AP y una peor utilización de la red. Para realizar el equilibrio de carga, asigne los AP dentro de un área a un grupo para coordinar el acceso STA.

Config

Note: If there are multiple APs with overlapping wireless signal, one AP maybe overloaded leading to awful WiFi utilization for STAs are randomly accessed. Load balancing function helps control STA access and balance traffic load by dividing APs in one area into different load-balancing groups.
Example: AP1 is associated with 15 STAs and AP2 with 10 STAs. Since the difference of their STA numbers exceeds the current threshold, subsequent STAs will be associated with AP2.

+ Add Balancing Group -X Delete Selected

Balancing Group Name	Balancing Type	Balancing Threshold	Member AP	Action
No Data Found				

Show No.: 10 Total Count: 0

K First < Pre Next > Last 1 Go

- (1) Agregar grupos de equilibrio: haga clic en **Agregar grupo de equilibrio** y edite los campos en la ventana emergente. Haga clic en **Guardar** y el grupo de equilibrio se mostrará en la lista después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.

Note: If there are multiple APs with overlapping wireless signal, one AP may be overloaded leading to awful WiFi utilization for STAs are randomly accessed. Load balancing function helps control STA access and balance traffic load by dividing APs in one area into different load-balancing groups.
 Example: AP1 is associated with 15 STAs and AP2 with 10 STAs. Since the difference of their STA numbers exceeds the current threshold, subsequent STAs will be associated with AP2.

+ Add Balancing Group X Delete Selected

☐ Balancing Group Name

Show No.: 10 Total Count: 0

Add Balancing Group

Balancing Group Name: *

Balancing Type: STA-count-based ▼

STA Threshold: 3 ⓘ

STA Difference: 3 ⓘ

Member AP: ▼ *

Cancel Save

Member AP Action

K First < Pre Next > Last X 1 Go

Parámetro	Descripción
Nombre del grupo de equilibrio	Este campo es obligatorio. Este parámetro no se puede modificar en el modo de edición.
Tipo de equilibrio	Seleccione Basado en recuento de STA o Basado en tráfico de AP . Este parámetro no se puede modificar en el modo de edición.
Umbral de STA	Para realizar el equilibrio de carga, el número de STA asociados con cada AP debe exceder el umbral de STA.
Diferencia de STA	Para realizar el equilibrio de carga, la diferencia en el número de STA asociados con los AP debe exceder el valor de la diferencia de STA.
Umbral de tráfico	Para realizar el equilibrio de carga, el tráfico de datos en cada AP debe superar el umbral de tráfico. La carga de tráfico se equilibra cuando la diferencia de tráfico en los AP se reduce a un cierto valor.
Miembro AP	Seleccione los miembros AP en este grupo de equilibrio de carga. Cada AP se puede asignar a un solo grupo.

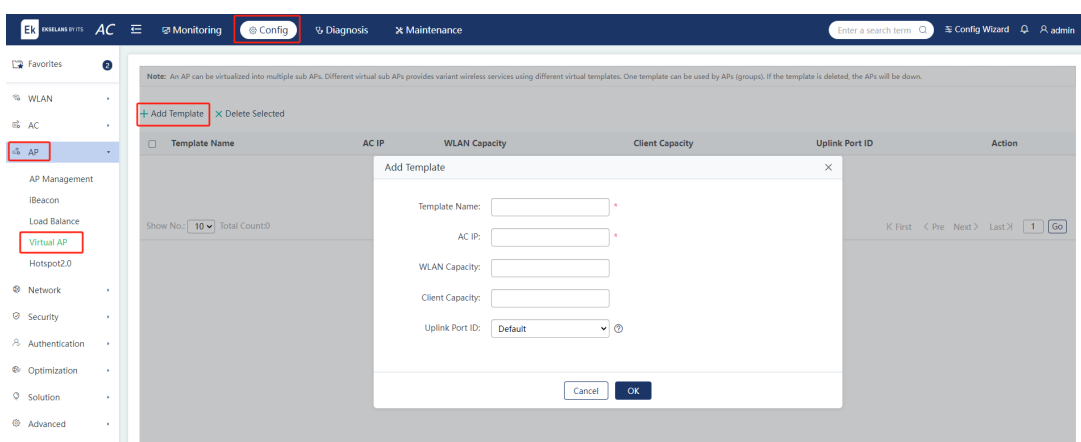
- Eliminación de grupos de equilibrio de carga: haga clic en **Eliminar** en la columna **Acción** para eliminar un grupo de equilibrio de carga. Seleccione grupos de equilibrio de carga en la lista y haga clic en **Eliminar seleccionados**. Haga clic en **Aceptar** en la ventana emergente para eliminar por lotes los grupos de equilibrio de carga.
- Edición de grupos de equilibrio de carga: haz clic en **Editar** en la columna **Acción** y edita los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

5.3.4 Virtual AP

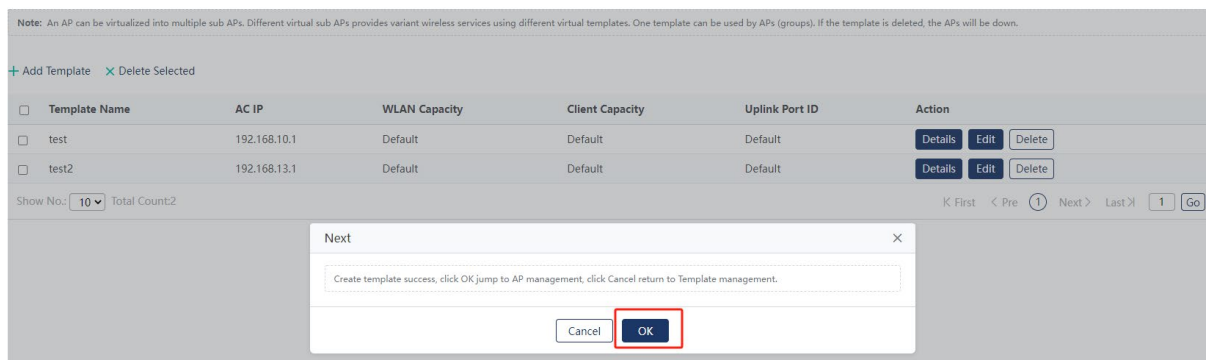
Elija **Config > AP > Virtual AP**.

Agregue y configure una plantilla y aplique la plantilla a un grupo de AP o a un AP para realizar la virtualización de AP.

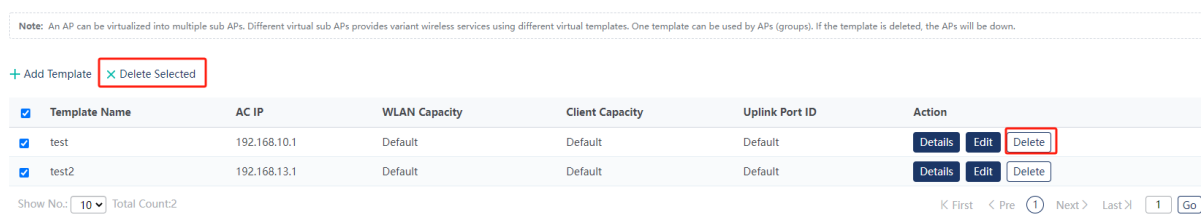
- (1) Agregar plantillas: haga clic en **Agregar plantilla** y configure los parámetros en la página **Agregar plantilla**. Haga clic en **Aceptar** para crear la plantilla. Después de agregar la plantilla, haga clic en **Aceptar** para redirigir a la página **Administración de AP** para aplicar la plantilla. Haga clic en **Cancelar** para volver a la página **AP virtual**.



Parámetro	Descripción
Nombre de la plantilla	Introduzca el nombre de la plantilla para la administración de AP virtual. Este campo es obligatorio.
IP de CA	Introduzca la dirección IP del túnel de la AC para la gestión de AP.
Capacidad de WLAN	Introduzca el número máximo de WLAN compatibles con esta plantilla.
Capacidad del cliente	Introduzca el número máximo de clientes admitidos por esta plantilla.
ID de puerto de enlace ascendente	Los AP virtuales utilizan el ID de puerto de enlace ascendente utilizado por el AP activo de forma predeterminada.



- (2) Eliminar plantillas: haga clic en **Eliminar** en la columna **Acción** para eliminar una plantilla. Seleccione varios elementos y haga clic en **Eliminar seleccionados** para eliminar plantillas por lotes.



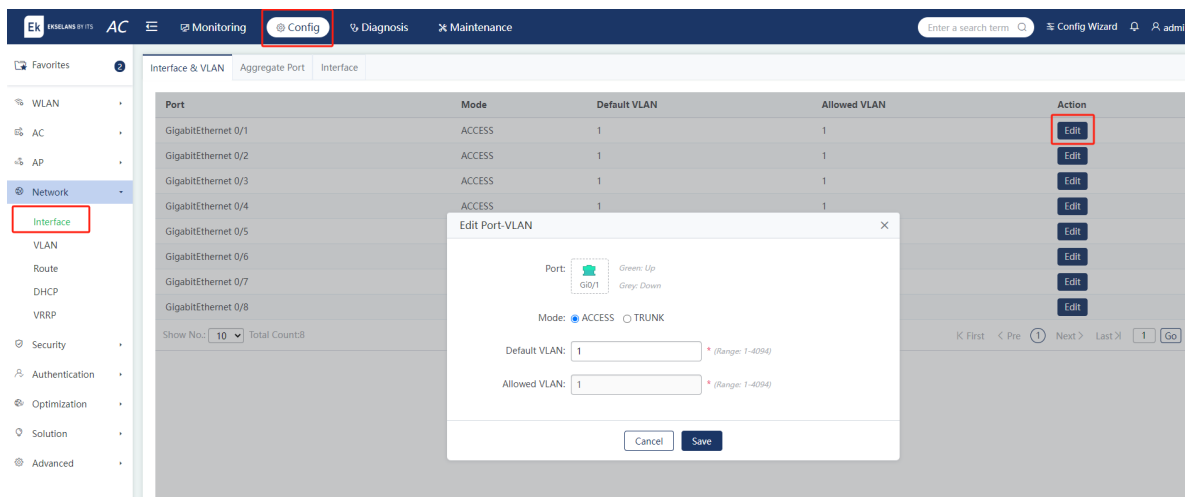
5.4 Red

5.4.1 Interfaz

Elija **Config** > **Network** > Interface (Interfaz de **de red**).

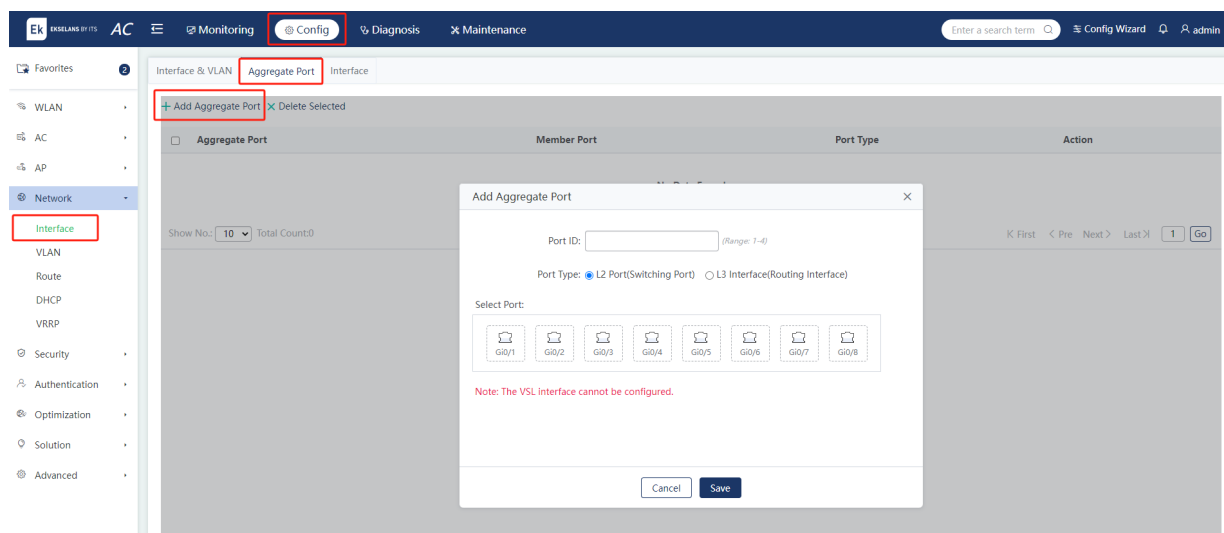
1. Interfaz y VLAN

Haga clic en **Editar** en la columna **Acción**. Aparece una ventana que muestra la información sobre la VLAN a la que pertenece el puerto. Edite los campos de la ventana. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

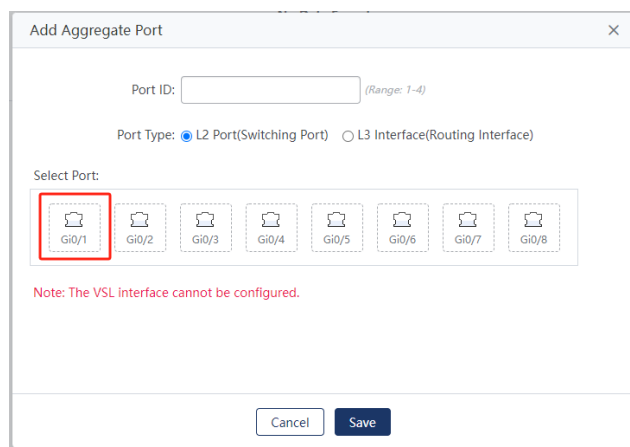


2. Puerto agregado

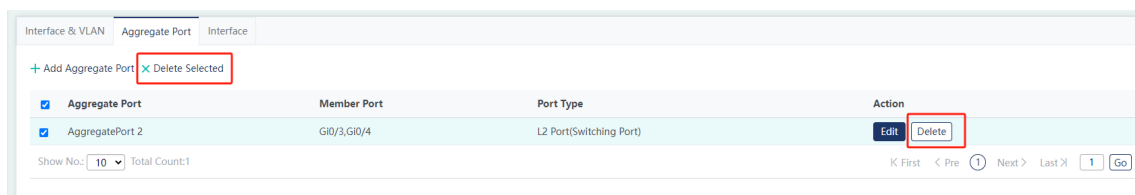
- (1) Adición de puertos agregados: haga clic en **Agregar puerto agregado**. Edite los campos en la ventana emergente. Haga clic en **Guardar** y el puerto agregado se mostrará en la lista de puertos agregados después de que se muestre un mensaje que indica que la operación se ha realizado correctamente.



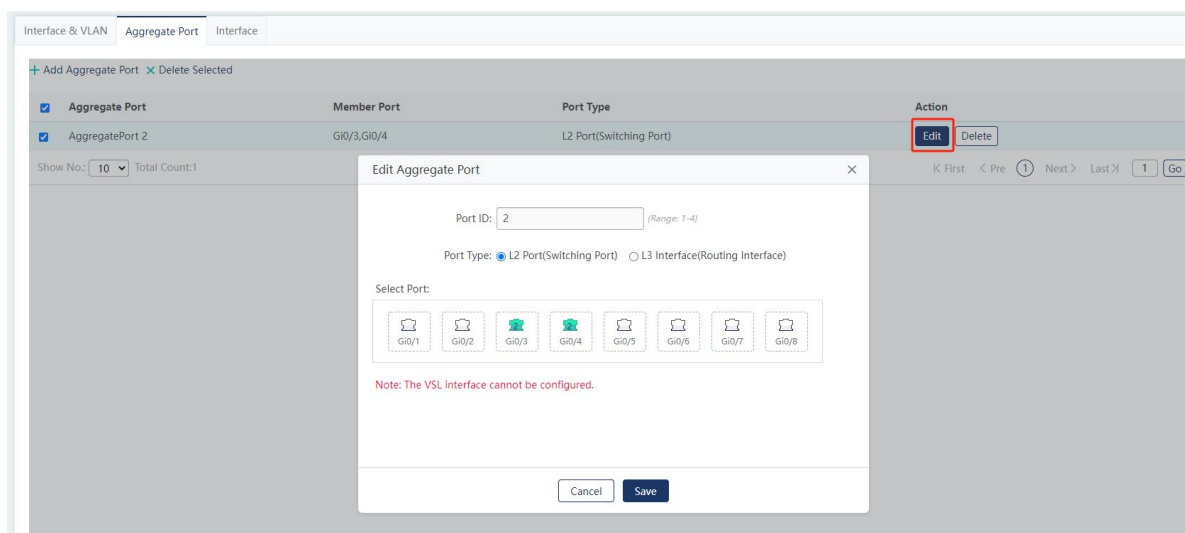
En la siguiente figura se muestra el panel en el que puede seleccionar los puertos miembro. Los puertos en gris se han configurado como puertos miembro de un puerto agregado. El número debajo del icono de puerto indica que este puerto es un puerto miembro del puerto agregado especificado.



- (2) Eliminación de puertos agregados: seleccione los puertos agregados en la lista. Haga clic en **Eliminar seleccionados** y haga clic en **Aceptar** en la ventana emergente para eliminar los puertos agregados.

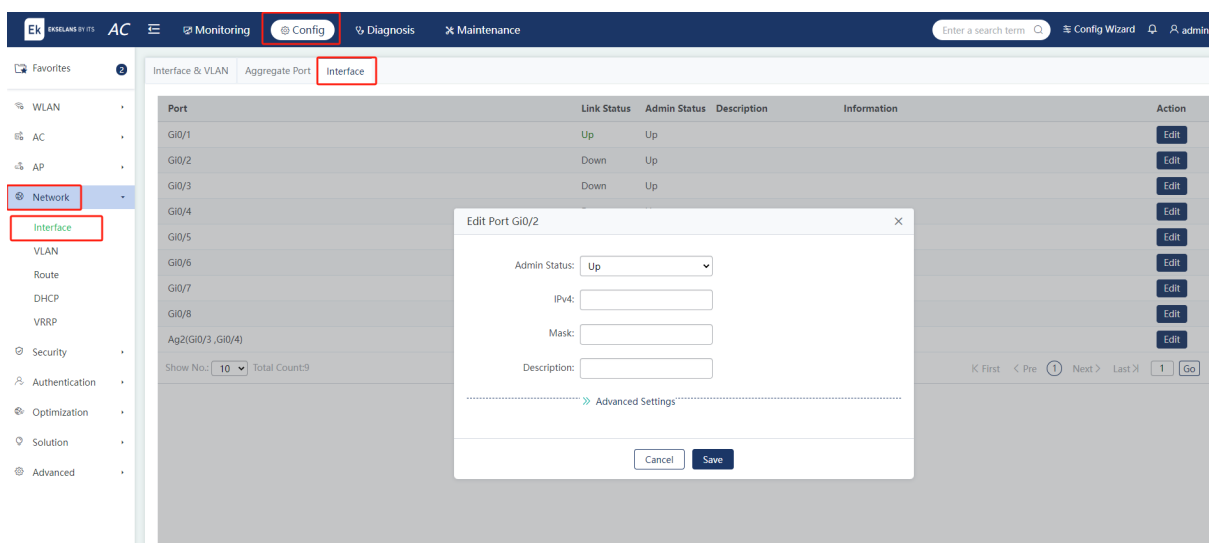


- (3) Edición de puertos agregados: haga clic **en Editar** en la columna **Acción**. Aparece una ventana que muestra la información sobre el puerto agregado y edita los campos de la ventana. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.



3. Interfaz

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

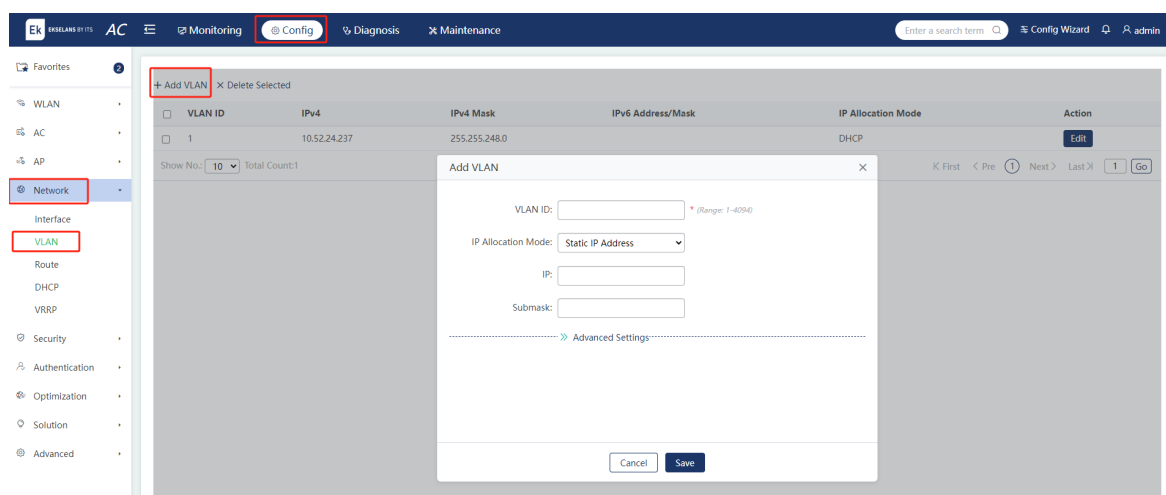


Parámetro	Descripción
Estado del administrador	Seleccione el estado de la interfaz.
IPv4	Introduzca la dirección IPv4 de la interfaz.
Máscara	Introduzca la máscara de subred IPv4 de la interfaz.
Descripción	Introduzca la descripción o el alias de la interfaz.
Puerto de cobre/fibra	Las opciones, incluido el puerto de cobre y el puerto de fibra, se muestran en función de la capacidad del hardware.
IPv6	Introduzca la dirección IPv6 de la interfaz.
Velocidad	Configure la velocidad de la interfaz.
Modo de trabajo	Los modos de trabajo de la interfaz incluyen los modos de negociación, dúplex y semidúplex.

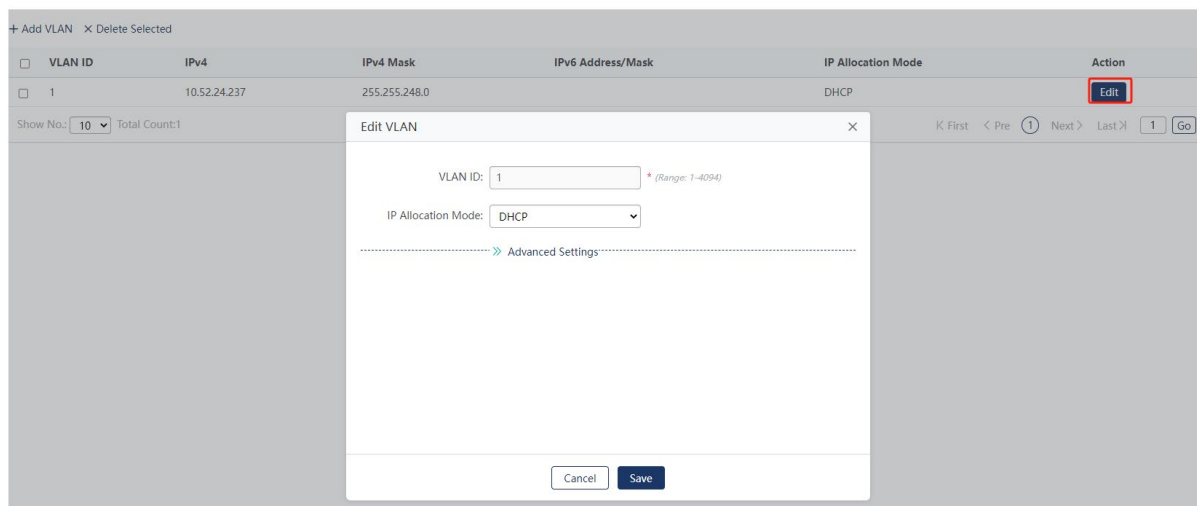
5.4.2 VLAN

Elija **Config > Network > VLAN**.

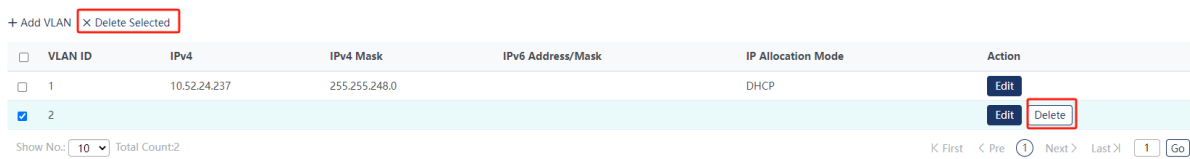
- (1) Adición de VLAN: Haga clic **en Agregar VLAN** y edite los campos en la ventana emergente. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente. La VLAN agregada se muestra en la lista de VLAN.



- (2) Edición de VLAN: Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra la 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.



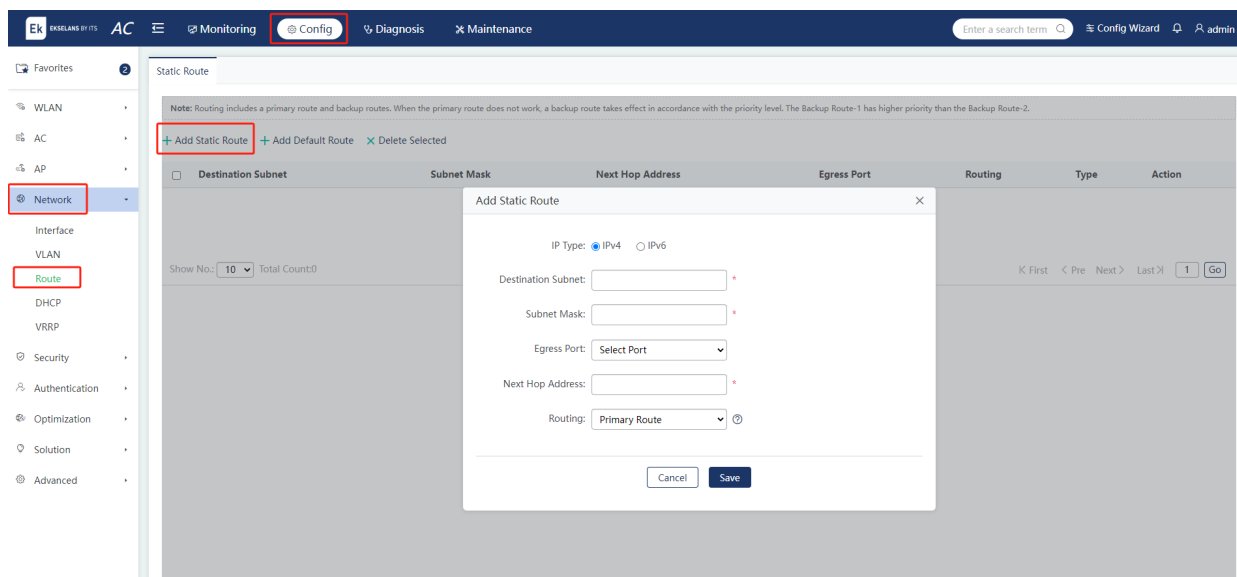
- (3) Eliminación de VLAN: Haga clic en **Eliminar** en la columna **Acción** y haga clic en Aceptar en la ventana emergente para eliminar una VLAN. Seleccione varios elementos de la lista. Haga clic en **Eliminar seleccionado** y aparecerá una ventana. Haga clic en Aceptar para eliminar por lotes las VLAN.



5.4.3 Ruta

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

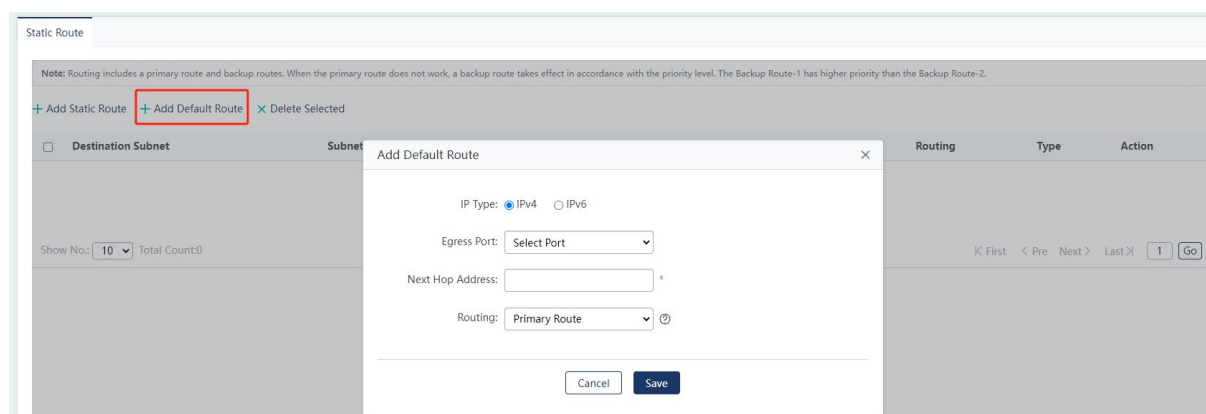
- (1) Agregar rutas estáticas: haz clic en **Agregar ruta estática**. Edite los campos en la ventana emergente. Haga clic en **Guardar** y la ruta estática se mostrará en la lista de rutas después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.



- (2) Agregar rutas predeterminadas: haga clic en **Agregar ruta predeterminada**. Edite los campos en la ventana emergente. Haga clic en **Guardar** y la ruta predeterminada se mostrará en la lista de rutas después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.

Nota

La selección de rutas implica una ruta principal y rutas de respaldo. Cuando la ruta principal no esté disponible, 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 rutas: Haga clic en **Editar** en la columna **Acción** y aparecerá una ventana que muestra la 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 rutas: haga clic **en Eliminar** en la columna **Acción** para eliminar una ruta. Seleccione varios elementos y haga clic en **Eliminar seleccionados**. Haga clic en **Aceptar** en la ventana emergente para eliminar rutas por lotes.

5.4.4 DHCP

1. Grupo de direcciones DHCP

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

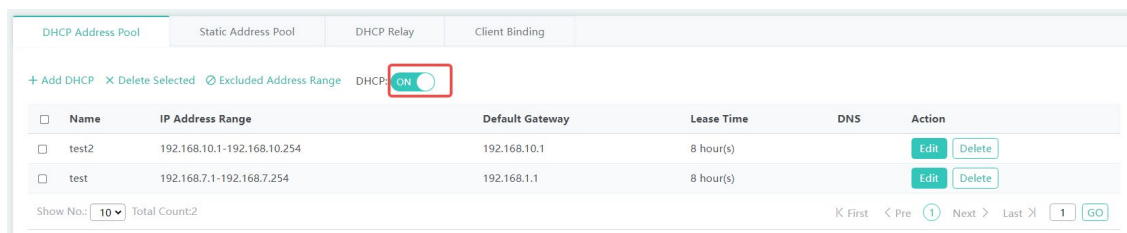
- (1) Adición de grupos de direcciones DHCP: Haga clic **en Agregar DHCP** y edite los campos en la ventana emergente. Haga clic **en Guardar** y el grupo de direcciones DHCP se mostrará en la lista después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.

The screenshot displays the 'DHCP Address Pool' configuration page. The left sidebar shows the navigation menu with 'Network' and 'DHCP' highlighted. The main area shows a table with columns: Name, IP Address Range, Default Gateway, Lease Time, DNS, and Action. A '+ Add DHCP' button is visible. Below the table, the 'Add DHCP' dialog box is open, showing fields for Pool Name, Type (IPv4 selected), Address Range (1 to 254), Default Gateway, Lease Time (8 hours), Preferred DNS Server, Secondary DNS Server, Option 138, and Option 43. There are 'Cancel' and 'Save' buttons at the bottom.

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.
Opción 138	La opción DHCP 138 se utiliza para informar al AP de la dirección IP de la AC para asociar el AP con la CA. Por lo general, este campo se completa con la dirección IP de la interfaz de bucle invertido de la CA.
Opción 43	La opción DHCP 43 se utiliza para informar al AP de la dirección IP de la AC para asociar el AP con la CA. Por lo general, este campo se rellena con la dirección IP de la interfaz de bucle invertido de la CA. Es de uso común.

- (2) Eliminación de grupos DHCP: haga clic en **Eliminar** en la columna **Acción** para eliminar un grupo de direcciones DHCP. Seleccione varios elementos y haga clic en **Eliminar seleccionados**. Haga clic en **Aceptar** en la ventana emergente para eliminar por lotes los grupos de direcciones DHCP.
- (3) Configuración de rangos de direcciones excluidas: haga clic en **Rango de direcciones excluidas**. 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 **Aceptar** y los rangos de direcciones excluidos se mostrarán en la lista después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.
- (4) Activar o desactivar el servicio DHCP: Activa o desactiva el botón situado junto a **DHCP** para activar o desactivar el servicio DHCP.

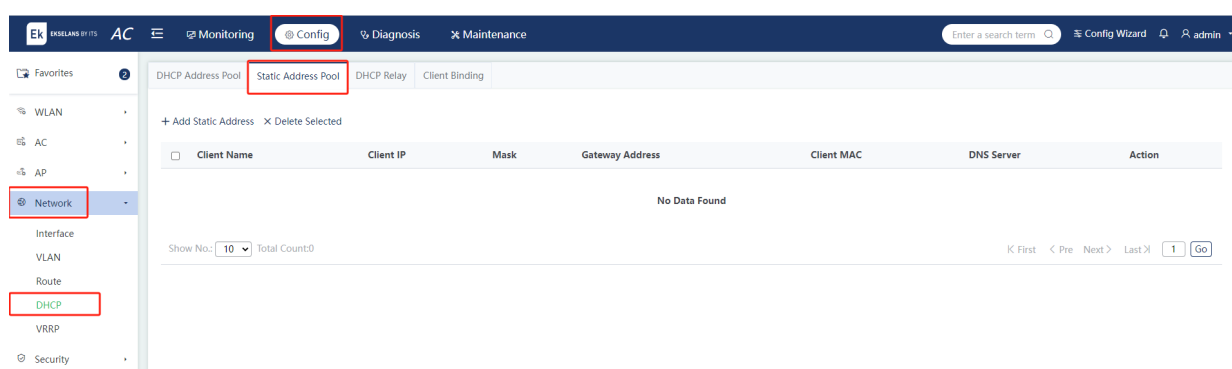


- (5) Edición de grupos de direcciones DHCP: Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra la información sobre el grupo de direcciones DHCP. Edite los campos de la ventana. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado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

2. Grupo de direcciones estáticas

Elija Config > Network > DHCP > Static Address Pool.

- (1) Agregar grupos de direcciones estáticas: 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.



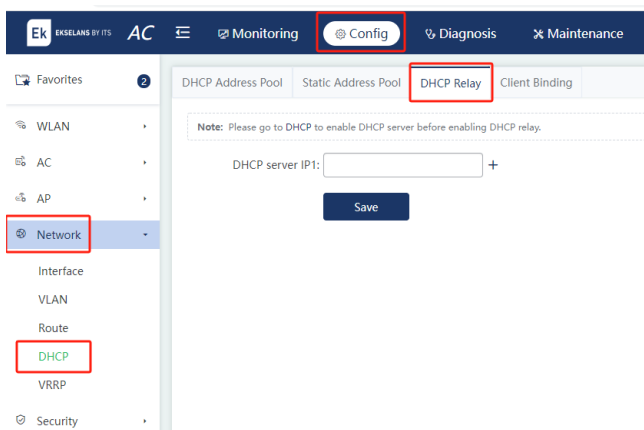
Parámetro	Descripción
Nombre del cliente	Introduzca el nombre del grupo de direcciones estáticas.
IP del cliente	Configure la dirección IP.
Máscara	Configure la máscara de subred.
MAC del cliente	Introduzca la dirección MAC del cliente.
Dirección de puerta de enlace	Configure la dirección IP de la puerta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

- (2) Eliminación de direcciones IP estáticas: haga clic **en Eliminar** en la columna **Acción** para eliminar una dirección IP estática. Seleccione varios elementos y haga clic en **Eliminar seleccionados**. Haga clic en **Aceptar** en la ventana emergente para eliminar por lotes las direcciones IP estáticas.
- (3) Edición de la dirección IP estática: Haga clic **en Editar** en la columna **Acción** y aparecerá una ventana que muestra la información sobre la dirección IP estática. Edite los campos de la ventana. Haga clic en Guardar y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

3. Relé DHCP

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

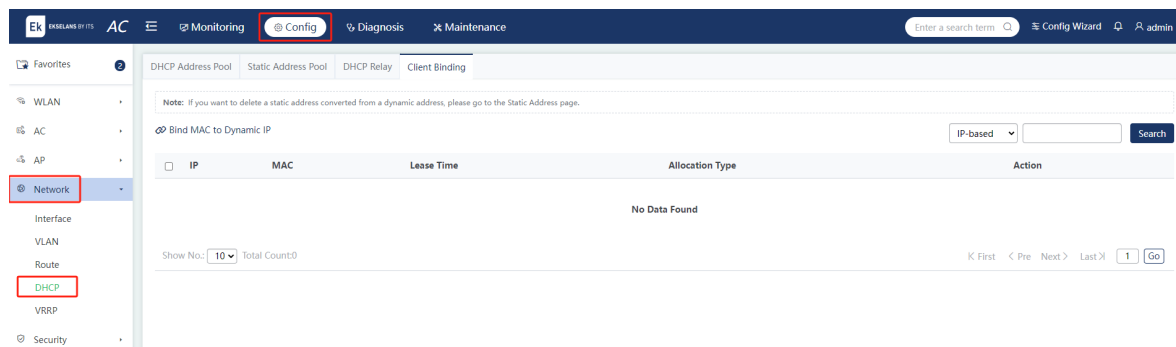
Introduzca la dirección IP del relé DHCP y haga clic en **Guardar**.



4. Enlace de cliente

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

- (1) Vincular dirección MAC con dirección IP dinámica: seleccione las direcciones MAC de la lista y haga clic en **Vincular MAC a IP dinámica**. Haga clic en **Aceptar** en la ventana emergente para vincular las direcciones MAC con direcciones IP dinámicas.

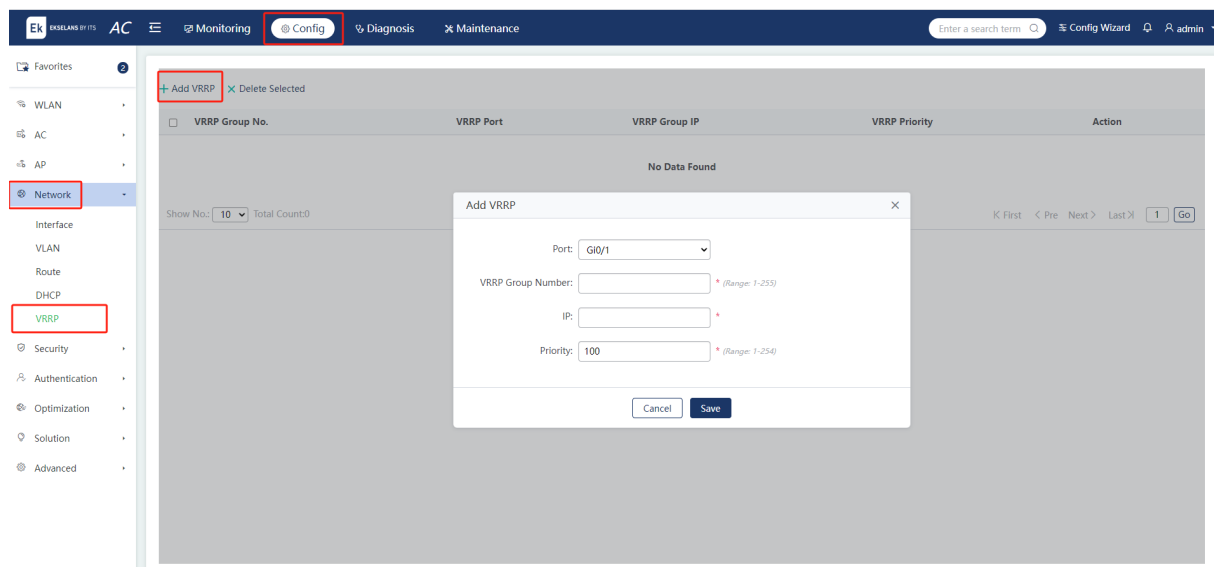


- (2) Desvincular la dirección MAC con la dirección IP dinámica: haga clic en **Eliminar** en la columna **Acción** y aparecerá una ventana. Haga clic en **Aceptar** para desvincular la dirección MAC.
- (3) Búsqueda de clientes por dirección IP o dirección MAC: Introduzca la dirección IP o la dirección MAC en la barra de búsqueda. Haga clic en **Buscar** y los resultados se mostrarán en la lista.

5.4.5 VRRP

Elija **Config > Network > VRRP**.

- (1) Agregar grupos de VRRP: Haga clic en **Agregar VRRP**. Edite los campos en la ventana emergente. Haga clic en **Guardar** y el grupo VRRP se mostrará en la lista después de que aparezca un mensaje que indica que la operación se ha realizado correctamente.



- (2) Eliminación de grupos VRRP: seleccione los grupos VRRP de la lista y haga clic en **Eliminar seleccionados**. Haga clic en **Aceptar** en la ventana emergente para eliminar los grupos VRRP.
- (3) Edición de grupos VRRP: Haga clic en **Editar** en la columna **Acción** y aparecerá una ventana que muestra la información sobre el grupo VRRP. Edite los campos de la ventana. Haga clic en **Guardar** y se mostrará un mensaje que indica que la operación se ha realizado correctamente.

5.5 Seguridad

5.5.1 Contención

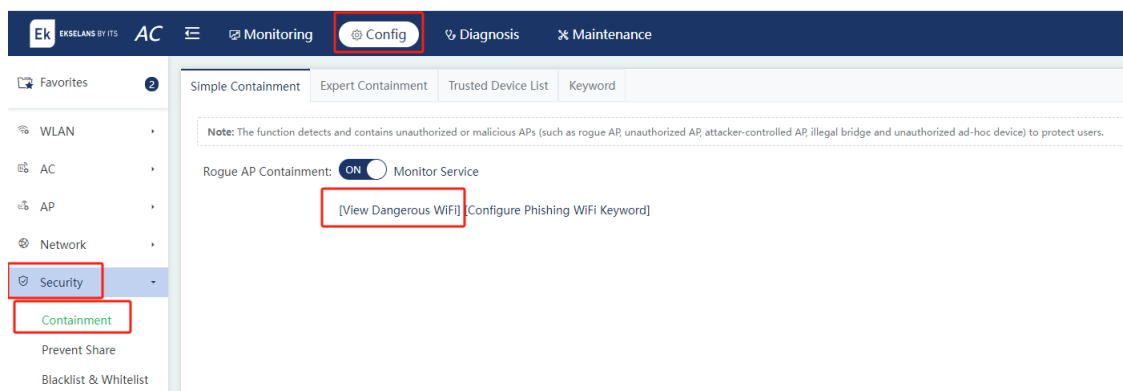
Elija **Config > Security > Containment (Contención)**.

Es posible que existan puntos de acceso no autorizados en una red inalámbrica. Pueden tener vulnerabilidades de seguridad o estar controlados por atacantes, amenazando seriamente la seguridad de las redes de los usuarios. Habilite la función de contención en el AC para atacar a los AP no autorizados de modo que otros clientes inalámbricos no puedan asociarse con los AP no autorizados.

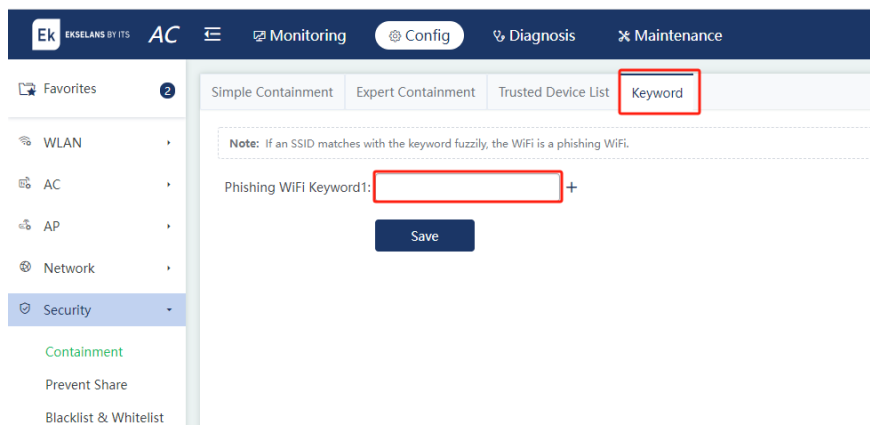
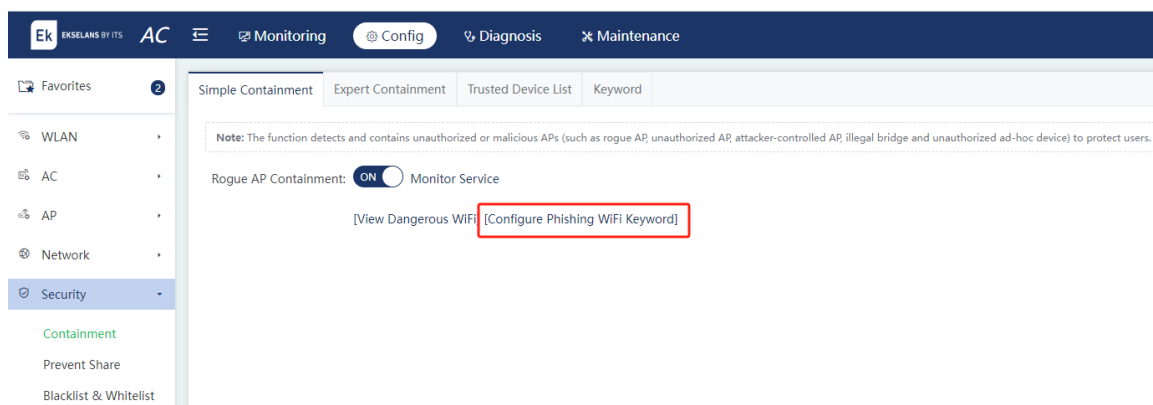
1. Configuración básica para la contención

Cuando la contención está actualmente deshabilitada y no se detecta ningún AP en modo de monitoreo o híbrido, se muestra una ventana emergente para solicitar a los usuarios que habiliten la función de monitoreo de AP. Haga clic en **Aceptar** para ir a la página **Servicio de supervisión**.

Después de habilitar la contención, haga clic en **Ver Wi-Fi peligrosa** para acceder a la página Lista de **Wi-Fi peligroso** y confiar o contener redes Wi-Fi.



Haga clic en **Configurar palabra clave de phishing WiFi** para acceder a la página **Palabra clave** y configurar la palabra clave.



2. Configuración especializada para la contención

Habilite o deshabilite la función de contención de AP no autorizada en el CA.

Ek EKSELANS BY ITS AC Monitoring **Config** Diagnosis Maintenance

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

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

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

Containment Mode: ☒ SSID Mode: Contain APs not associated with the same AC while emitting the same WiFi signal [Configure Phishing WiFi Keyword]

☐ AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)

☐ Rogue Mode: Contain APs according to RSSI

☒ CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [+MAC Address] [+SSID Blacklist]

☒ Enable Fuzzy Containment ⓘ

Containment Range: ☐ Scan/counter only partial channels

☒ Scan/counter contain the corresponding channels of the device (consuming more resources)

Save

- (1) Habilitar el modo de monitoreo para un AP especificado: El AP debe configurarse con el modo híbrido o de monitoreo antes de que la función de contención surta efecto. Haga clic en **Supervisar servicio** para acceder a la página **Supervisar servicio**. Haga clic en **Monitor** o **Híbrido** para configurar el modo AP. La información de AP se muestra en el cuadro de diálogo emergente. Edita la información. Cuando el AP que proporciona la función de radio AI está configurado con el modo de monitoreo, la radio AI debe monitorearse y contenerse primero.

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

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

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

Containment Mode: ☒ SSID Mode: Contain APs not associated with the same AC while emitting the same WiFi signal [Configure Phishing WiFi Keyword]

☐ AdHoc Mode: Contain APs emitting signals simulated by non-APs (such as AdHoc)

☐ Rogue Mode: Contain APs according to RSSI

☒ CONFIG Mode: Contain APs by configuring the MAC address and the SSID blacklist manually [+MAC Address] [+SSID Blacklist]

☒ Enable Fuzzy Containment ⓘ

Containment Range: ☐ Scan/counter only partial channels

☒ Scan/counter contain the corresponding channels of the device (consuming more resources)

Save

Monitor Service

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

+ Batch Monitor

AP-name-based Search Reset

AP Name	IP	MAC	Status	Work Mode	AP Mode
No Data Found					

Show No.: 10 Total Count: 0

First < Pre Next > Last 1 Go

Haga clic en **Guardar**. El **guardado se realizó correctamente**. se muestra el mensaje.

- (2) Agregar la dirección MAC de un dispositivo inalámbrico: Se incluirán las siguientes direcciones MAC configuradas.

Simple Containment Expert Containment Trusted Device List Keyword

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

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

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

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

Save

Add MAC Address(BSSID) to be Contained

+ Add

Current MAC: 741a.e0eb.3006 Cancel Save

- (3) Agregue una lista de bloqueo de SSID:

Simple Containment Expert Containment Trusted Device List Keyword

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

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

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

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

Save

Add SSID Blacklist

+ Add

Cancel Save

3. Lista de dispositivos de confianza

Cuando la función de contención de AP no autorizada está habilitada en el CA, se contendrán AP no autorizados, mientras que algunos AP son dispositivos confiables y deben tratarse de manera diferente. Se puede configurar la dirección MAC de un dispositivo de confianza.

Ek EKSELANS BY ITS AC Monitoring **Config** Diagnosis Maintenance

Favorites 2

WLAN AC AP Network **Security** Containment Prevent Share Blacklist & Whitelist User Isolation Attack Protection

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

Note: The following MAC addresses correspond to trusted APs, which will not be contained.

Trusted MAC(BSSID):

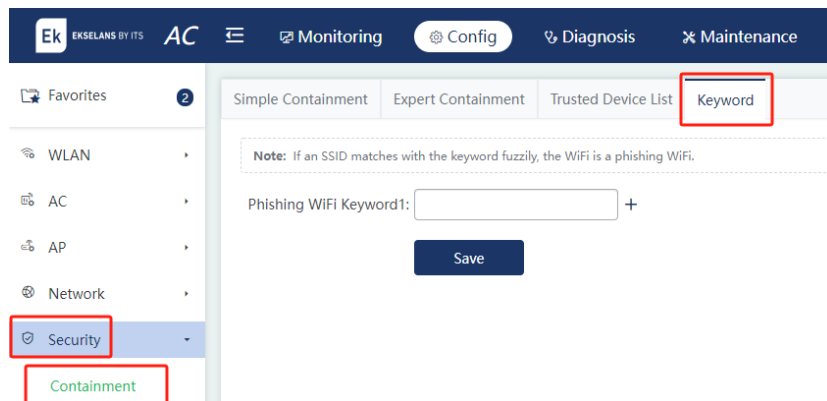
+ Add

Trusted Vendor List

Save

4. Palabra clave Wi-Fi de phishing

La coincidencia aproximada de una palabra clave de phishing de Wi-Fi ayuda a escanear las señales de Wi-Fi en una red. Si un SSID de una red Wi-Fi coincide con la palabra clave de forma difusa, la red Wi-Fi se considera una red de phishing.

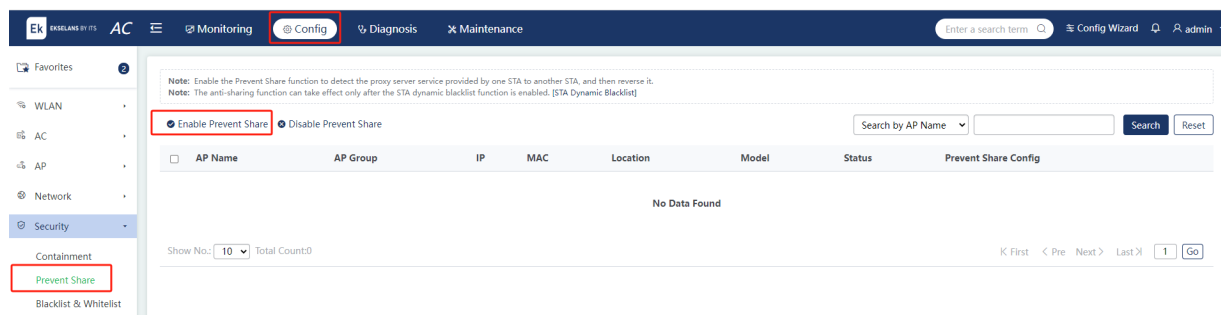


5.5.2 Prevención de uso compartido

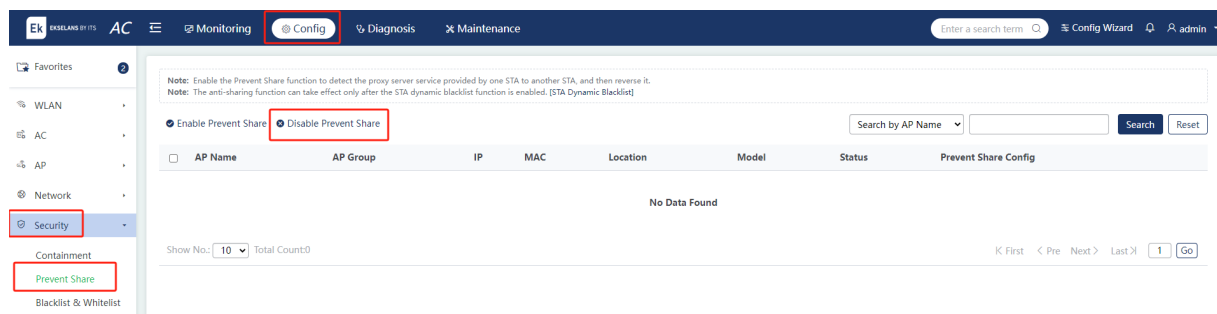
Elija **Config > Security > Prevent Share (Evitar compartir)**.

Una vez habilitada la prevención de uso compartido, el sistema detecta 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.

- (1) Habilitar la prevención de uso compartido: seleccione los AP que se habilitarán con la prevención de uso compartido en la lista. Haga clic en **Habilitar Impedir uso compartido**. En el cuadro de diálogo de confirmación emergente, haga clic en **Aceptar** para habilitar la prevención de uso compartido.



- (2) Deshabilitar la prevención de uso compartido: seleccione los AP para los que la prevención de uso compartido debe deshabilitarse en la lista. Haga clic en **Desactivar impedir uso compartido**. En el cuadro de diálogo de confirmación emergente, haga clic en **Aceptar** para deshabilitar la prevención de uso compartido.

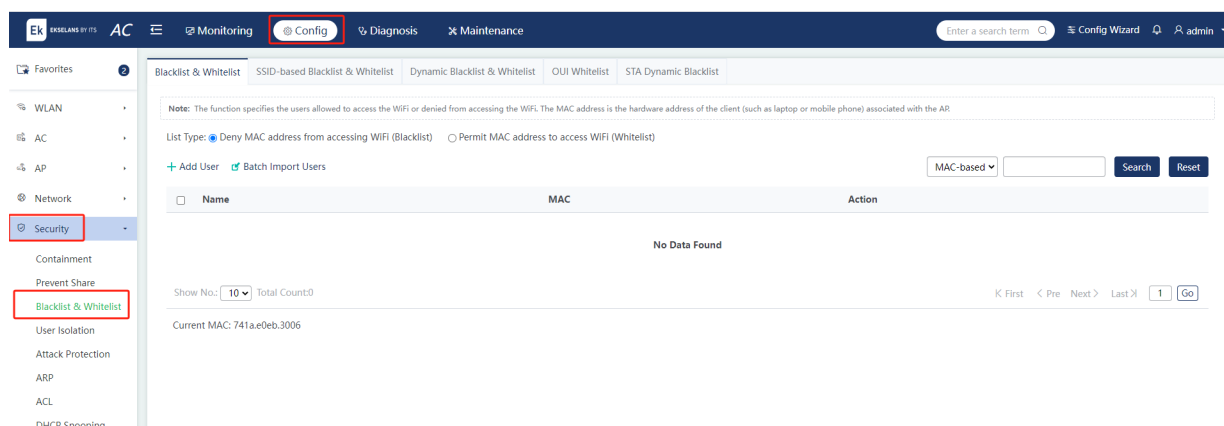


5.5.3 Configuración de la lista de bloqueo/lista de permitidos

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

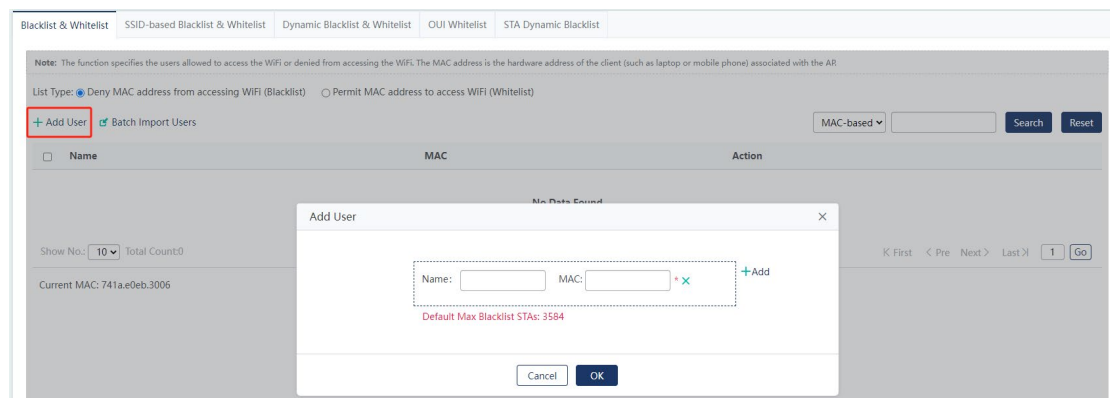
1. Configuración de la lista de bloqueo o la lista de permitidos para el CA

Para mejorar la seguridad inalámbrica, controle el acceso de los usuarios inalámbricos asignando acceso inalámbrico a ciertos usuarios o prohibiendo a ciertos usuarios el acceso a la red inalámbrica. El número de usuarios que pueden acceder a Wi-Fi o que se rechazan es 1.024 de forma predeterminada.



Agregue una dirección MAC a la lista de bloqueo o a la lista de permitidos.

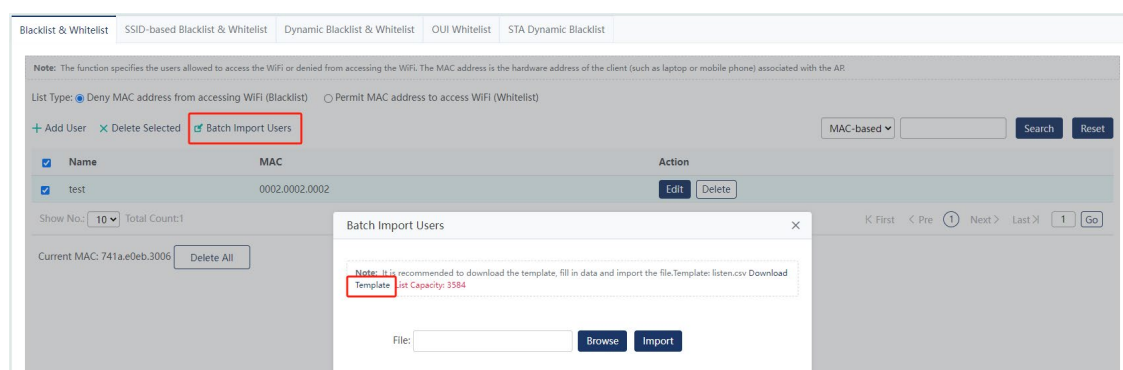
- (1) Agregar una lista: haga clic en **Agregar usuario** para agregar la dirección MAC de un usuario. Se pueden agregar varias direcciones.



- (2) Eliminar una lista: haz clic en **Eliminar** detrás de una lista especificada. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.

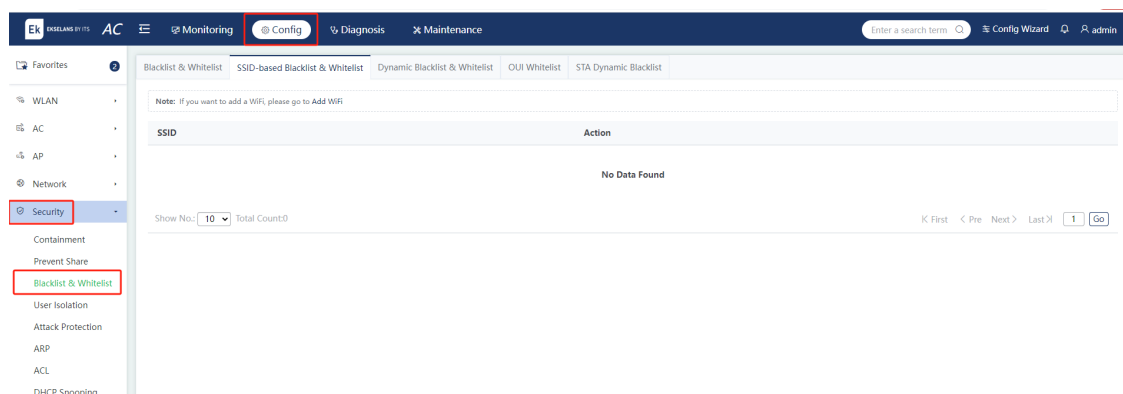


- (3) Listas de importación por lotes: haga clic en **Usuarios de importación por lotes**. Descarga y rellena la plantilla. Importe el archivo.



2. Configuración de la lista de bloqueo o la lista de permitidos basada en SSID

Haga clic en **Lista negra/Lista blanca** de una red Wi-Fi especificada para acceder a la página de configuración. Seleccione un tipo de lista.



- (1) Agregar una lista: haz clic en **Agregar usuario**. Agregue la dirección MAC de un dispositivo. Haga clic en **Aceptar**.

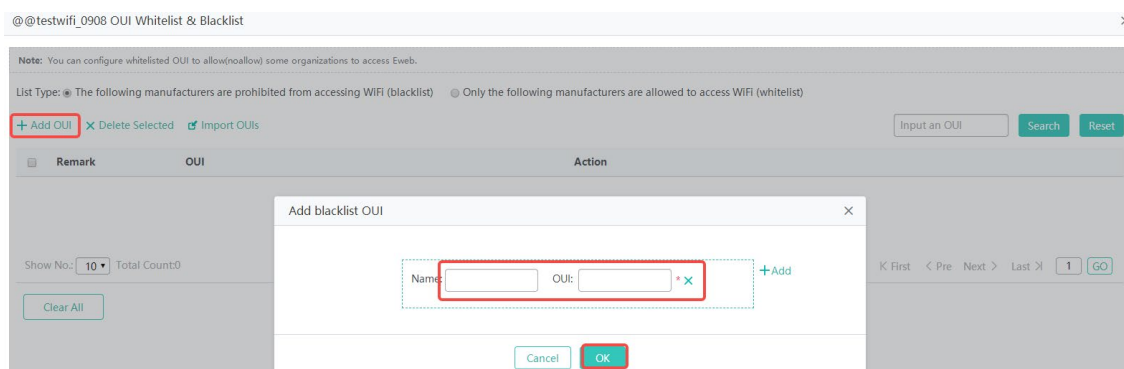
- (2) Eliminar una lista: haz clic en **Eliminar** detrás de una lista especificada. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.

- (3) Listas de bloqueo de importación por lotes: haga clic en **Importar usuarios por lotes**. Descarga la plantilla. Rellena la plantilla y guárdala. Haga clic en **Examinar**. Seleccione la plantilla guardada anterior. Haga clic en **Importar**.

- (4) Configurar identificadores únicos de la organización (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 de bloqueo o a la lista de permitidos pertenecen al mismo fabricante, añada su OUI a la lista directamente, sin necesidad de añadir la dirección MAC de cada dispositivo uno por uno.

Haga clic en **Agregar OUI**. Acceda a la página **Agregar OUI de lista negra**.

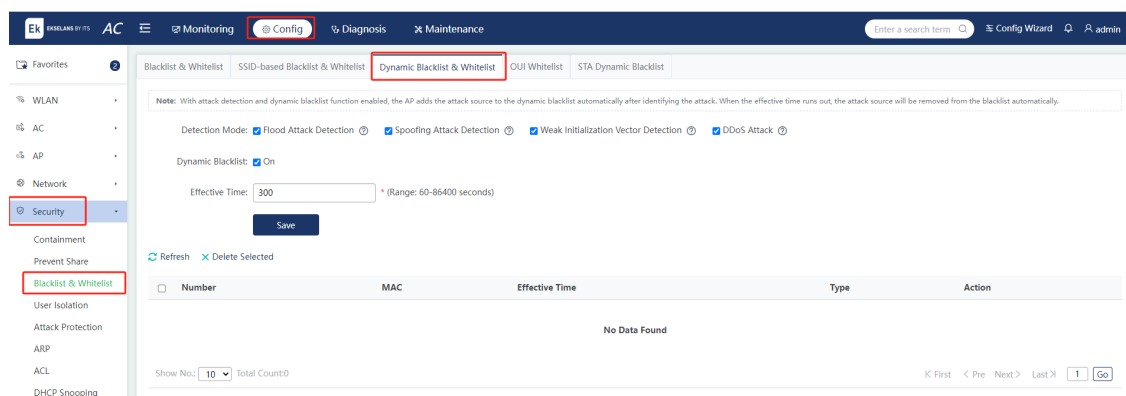
Haga clic en **Agregar**. Introduzca el nombre y la unidad organizativa del fabricante. Haga clic en **Aceptar**.



3. Lista de bloqueo dinámica

Lista de bloqueo dinámica: agregue fuentes de ataque maliciosas a la lista de bloqueo dinámica para evitar su acceso. Una vez configurado un modo de detección y habilitada la lista de bloqueo dinámica, el dispositivo agregará automáticamente la fuente de ataque a la lista de bloqueo dinámica cuando se detecte un ataque. Una vez que expire el tiempo efectivo, la fuente de ataque se eliminará automáticamente de la lista de bloqueo.

Configurar lista de bloqueo dinámica: seleccione un modo de detección, habilite la lista de bloqueo dinámica, configure el tiempo efectivo y haga clic en **Guardar**.



Eliminar una lista de bloqueo: seleccione la lista de bloqueo que desea eliminar de la lista. Haga clic en **Eliminar** seleccionados. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.

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

Note: With attack detection and dynamic blacklist function enabled, the AP adds the attack source to the dynamic blacklist automatically after identifying the attack. When the effective time runs out, the attack source will be removed from the blacklist automatically.

Detection Mode: ☒ Flood Attack Detection ☒ Spoofing Attack Detection ☒ Weak Initialization Vector Detection ☒ DDoS Attack

Dynamic Blacklist: ☒ On

Effective Time: * (Range: 60-86400 seconds)

Save

[Refresh](#) [Delete Selected](#)

Number	MAC	Effective Time	Type	Action
1	0013.ce69.7bb4	210	-	Delete

4. Configuración de la lista de bloqueo o la lista de permitidos de OUI para el CA

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

Ek EKSELANS BY ITS AC Monitoring **Config** Diagnosis Maintenance

Enter a search term Config Wizard admin

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

Note: The function specifies the users allowed to access the WIFI or denied from accessing the WIFI. The MAC address is the hardware address of the client (such as laptop or mobile phone) associated with the AP.

List Type: ☒ Deny MAC address from accessing WIFI (Blacklist) ☐ Permit MAC address to access WIFI (Whitelist)

[+ Add User](#) [Delete Selected](#) [Batch Import Users](#) MAC-based [Search](#) [Reset](#)

Name	MAC	Action
test	0002.0002.0002	Edit Delete

Show No: Total Count: 1

Current MAC: 741a.e0eb.3006 [Delete All](#)

Add User

Name: MAC: [+ Add](#)

Default Max Blacklist STAs: 3584

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

5. Lista de bloqueo dinámica de STA

Agregue STA de fuentes de ataque malintencionadas a la lista de bloqueo dinámico de STA para evitar que accedan a la red.

Ek EKSELANS BY ITS AC Monitoring **Config** Diagnosis Maintenance

Enter a search term Config Wizard admin

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

Note: When the effective time runs out, the STA that in the dynamic blacklist will be removed from the blacklist automatically.

Dynamic Blacklist: ☐ On [Refresh](#)

Number	MAC	Add Time
No Data Found		

Show No: Total Count: 0

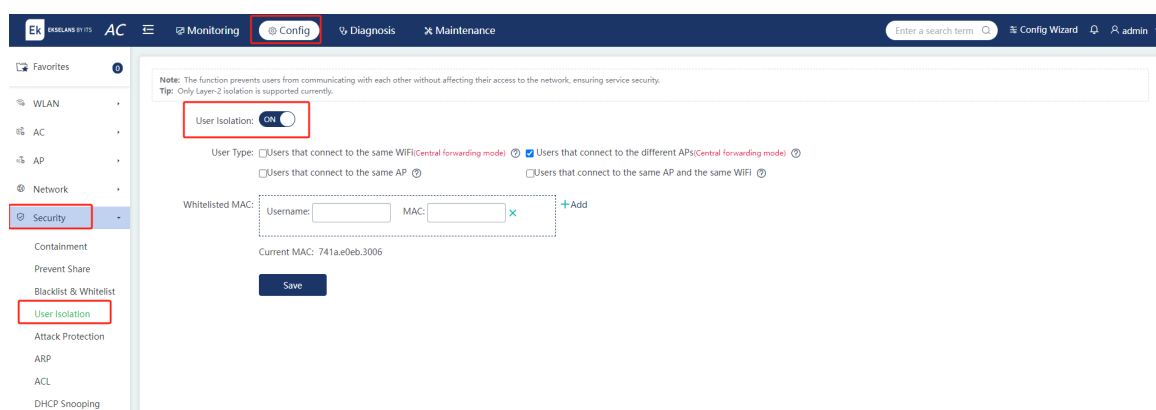
K First < Pre Next > Last 1 [Go](#)

5.5.4 Aislamiento de usuarios

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

Para garantizar la seguridad de la red y la confidencialidad de la información, los usuarios de la intranet se pueden configurar para que no se comuniquen entre sí. Algunos usuarios especiales (usuarios que pueden acceder entre sí) se pueden identificar mediante el nombre de usuario y la dirección MAC.

Active o desactive el conmutador de aislamiento de usuario para habilitar o deshabilitar el acceso mutuo entre usuarios de intranet. Seleccione los tipos de usuarios que se van a aislar. Haga clic en **Agregar** para agregar direcciones MAC de usuarios para el acceso mutuo. Haga clic en **x** para eliminar una dirección MAC de usuario especificada.

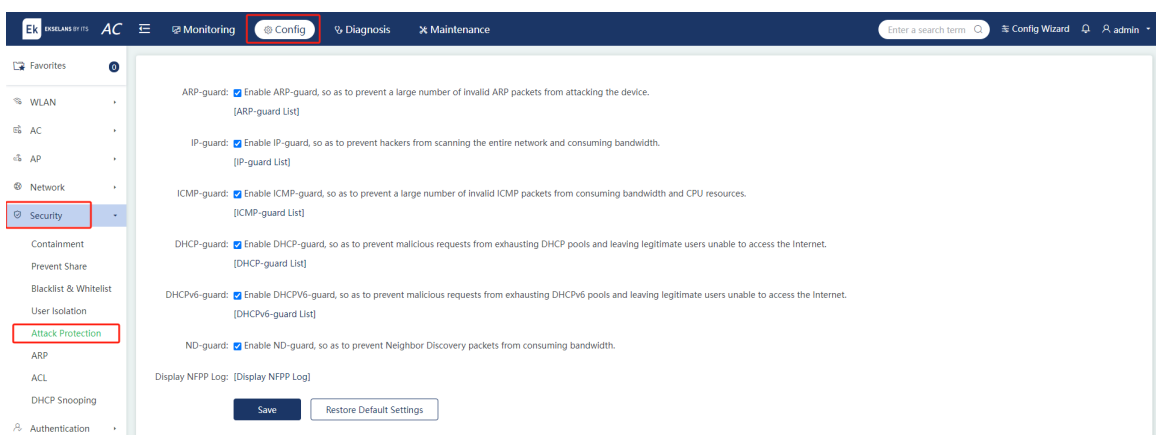


5.5.5 Prevención de ataques

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

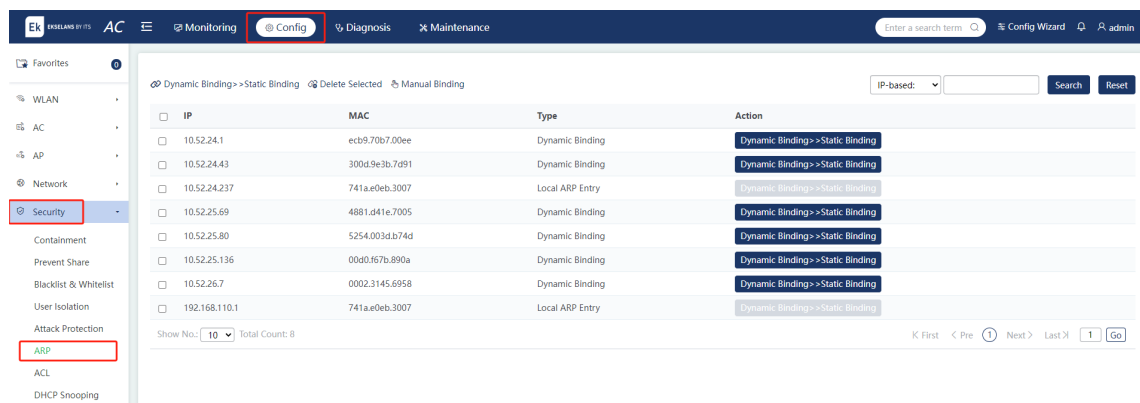
Los ataques maliciosos suelen producirse en un entorno de red. Estos ataques sobrecargan el switch, lo que resulta en un uso elevado de la CPU y una falla de operación del switch.

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

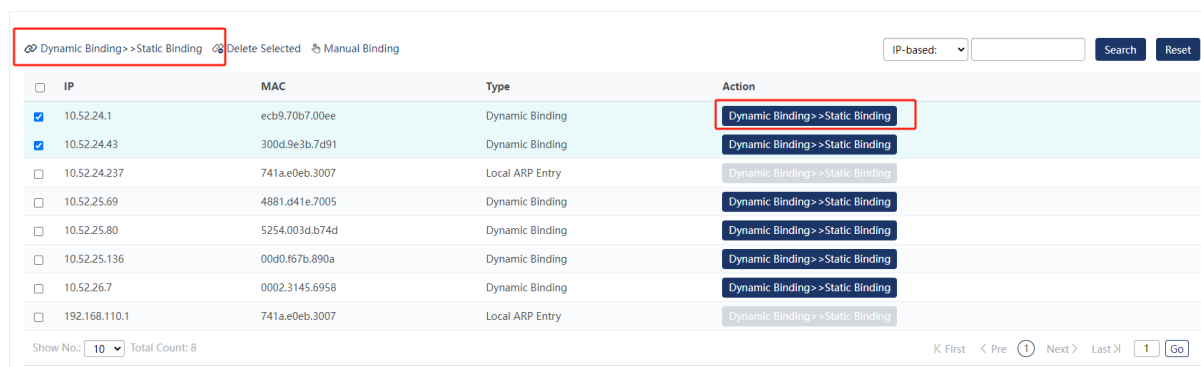


5.5.6 Enlace de entrada ARP

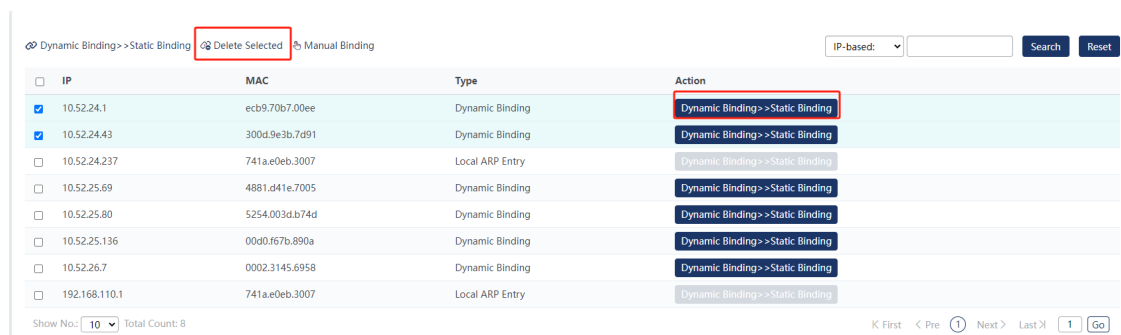
Elija **Config > Security > ARP**.



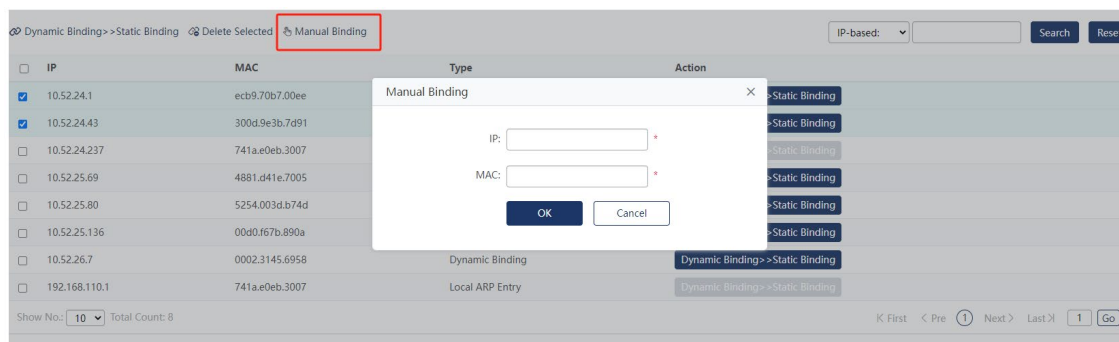
- (1) Convertir enlaces dinámicos en enlaces estáticos: seleccione uno o más registros en la lista ARP. Haga clic en **Enlace dinámico>>Enlace estático** para convertir por lotes los enlaces dinámicos en enlaces estáticos.



- (2) Eliminar enlaces estáticos: seleccione uno o más registros en la lista ARP. Haga clic en **Eliminar seleccionado** para eliminar por lotes los enlaces estáticos.



- (3) Encuadernación manual: haga clic en **Encuadernación manual**. Introduzca las direcciones IP y MAC. Haga clic en **Aceptar**. La **configuración se ha realizado correctamente**. se muestra el mensaje. La nueva entrada se muestra en la lista ARP.



5.5.7 ACL

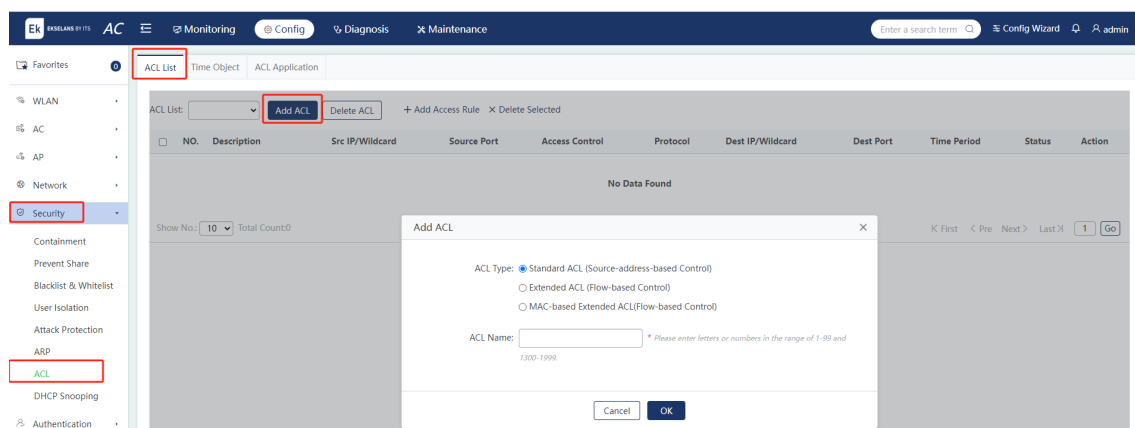
Elija **Config > Security > ACL**.

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 verifica 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).

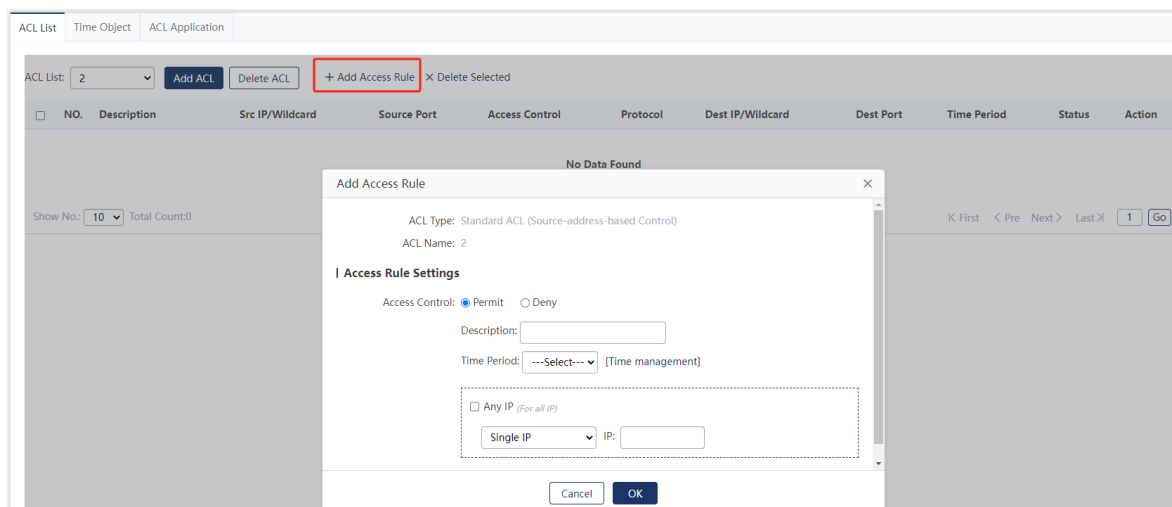
1. Lista de ACL

- (1) Agregar una ACL: Haga clic en **Agregar ACL**. Configure la información de ACL en el cuadro de diálogo emergente. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado. La ACL recién agregada se muestra en la lista desplegable de ACL en la esquina superior izquierda.

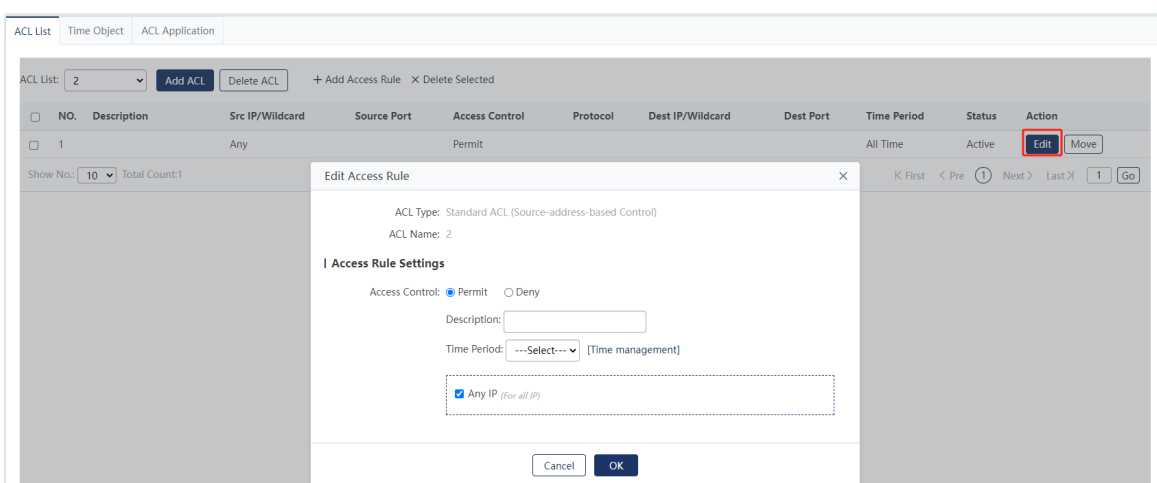


- (2) Eliminar una ACL: seleccione la ACL que se eliminará de la lista desplegable de ACL. Haga clic en **Eliminar ACL**. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.
- (3) Agregar una ACE: Seleccione una ACL a la que se debe agregar una ACE de la lista desplegable de ACL. Haga clic en **Agregar regla de acceso**. Configure la información de ACE en el cuadro de

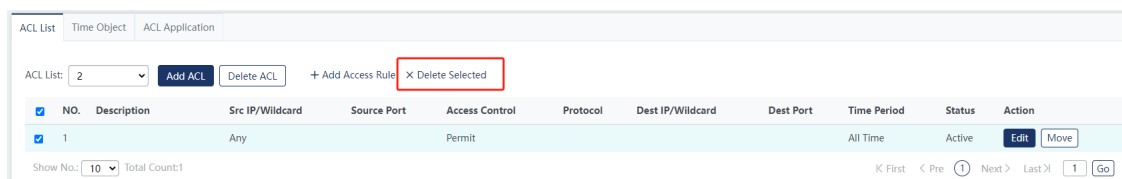
diálogo emergente. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado. La ACE recién agregada se muestra en la lista de ACL.



- (4) Editar una ACE: Haga clic **en Editar** detrás de una ACE especificada en la lista de ACL. El cuadro de diálogo emergente muestra la información sobre la ACE. Edita la información. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado.

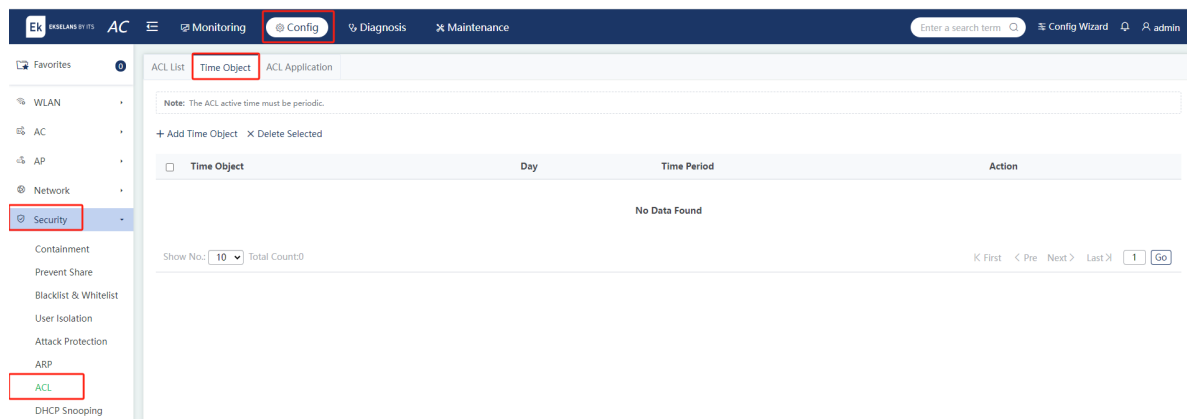


- (5) Eliminar una ACE: seleccione uno o más registros en la lista de ACL. Haga clic en **Eliminar** seleccionados. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.

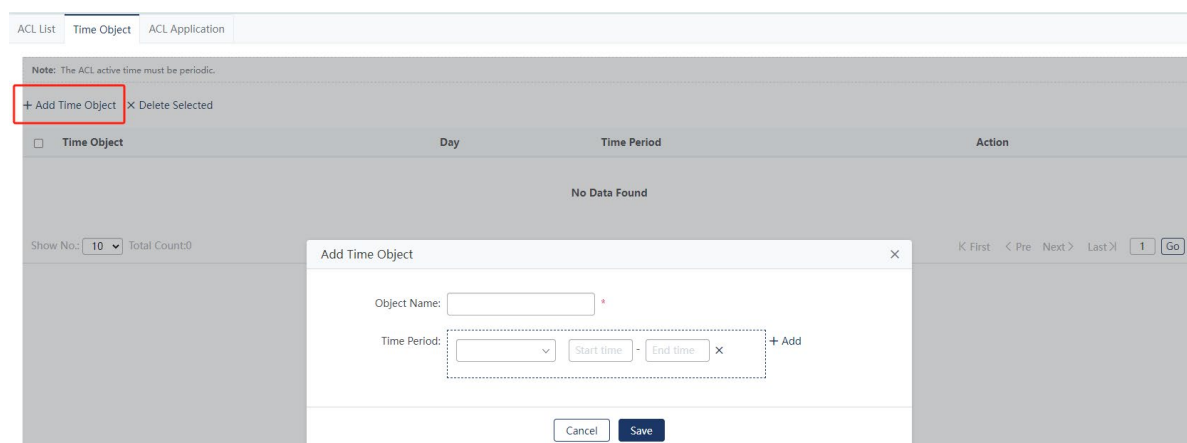


2. Período de tiempo de ACL

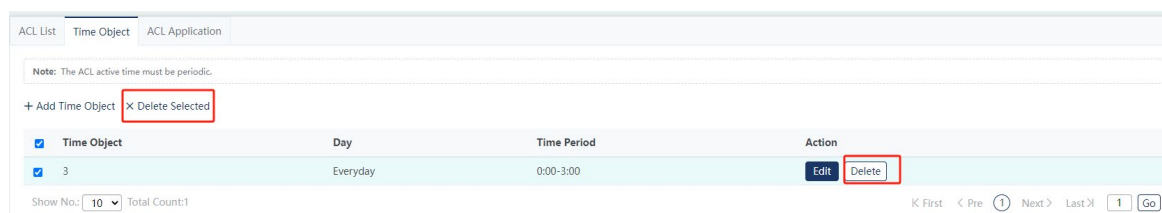
Una ACL se puede configurar para que surta efecto en función del tiempo, por ejemplo, en algunos períodos de tiempo de una semana. Para habilitar esta función, primero debe configurar un objeto de tiempo.



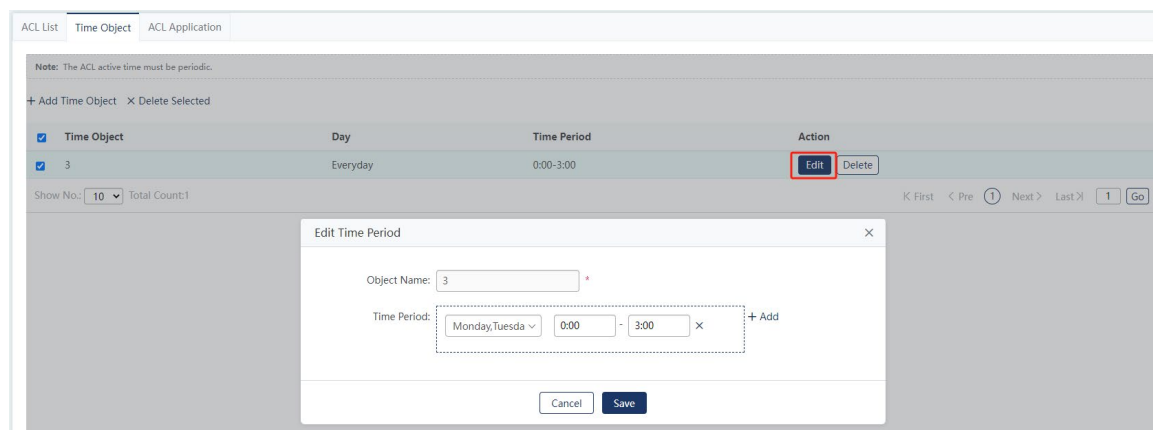
- (1) Añadir un objeto de tiempo: haz clic en **"Añadir objeto de tiempo"**. Configure la información del objeto de tiempo en el cuadro de diálogo emergente. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado.



- (2) Eliminar un objeto de tiempo: haz clic en **Eliminar** detrás de un objeto de tiempo especificado en la lista. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación. Para eliminar varios objetos de tiempo, seleccione los objetos de tiempo que desea eliminar en la lista. Haga clic en **Eliminar** seleccionados. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.



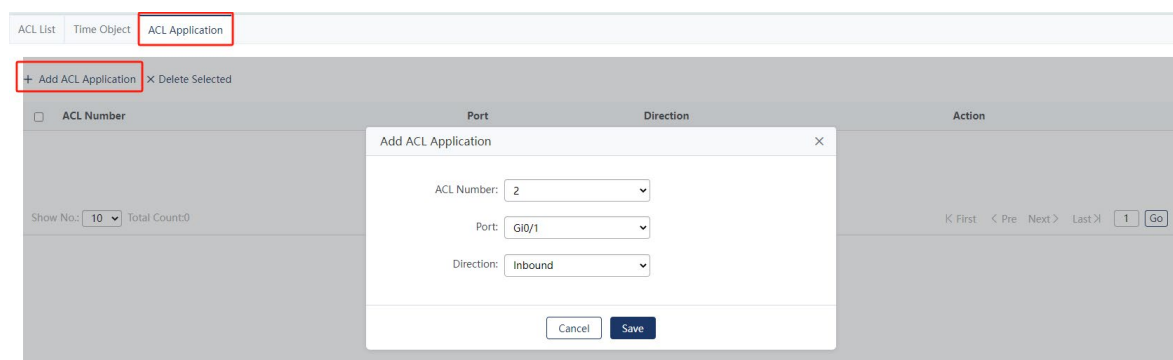
- (3) Editar un objeto de tiempo: haz clic en **Editar** detrás de un objeto de tiempo especificado en la lista. El cuadro de diálogo emergente muestra la información sobre el objeto de tiempo. Edita la información. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado.



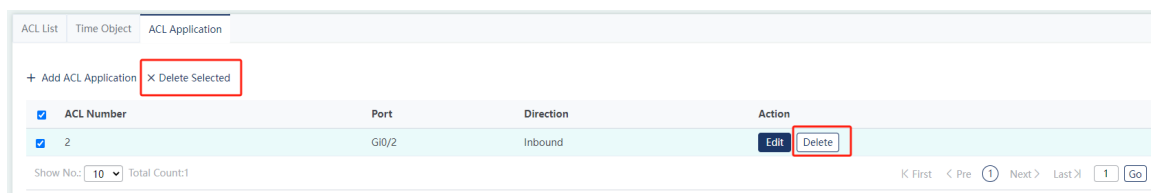
3. Aplicación de ACL

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

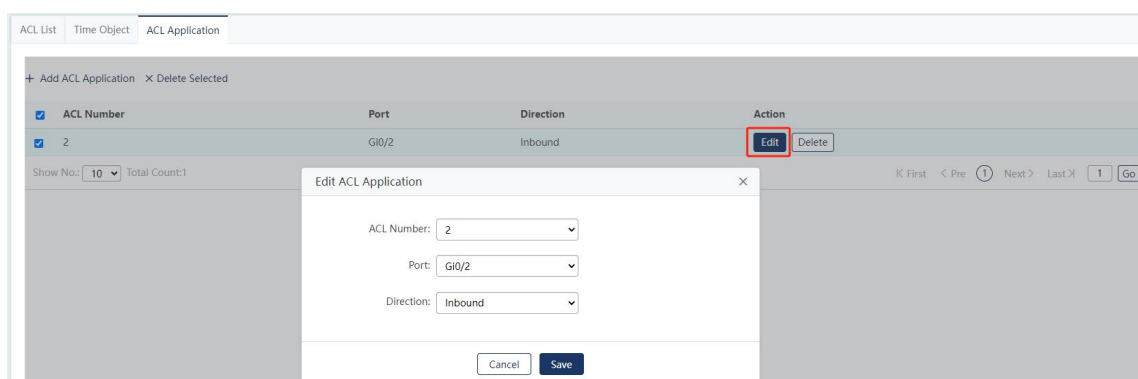
- (1) Agregar aplicación de ACL: Haga clic en **Agregar aplicación de ACL**. Aparece el **cuadro de diálogo Agregar aplicación de ACL**. Configure la información. Haga clic en **Guardar**. Se muestra un mensaje que indica que la configuración se ha guardado. La entrada de la aplicación ACL recién agregada se muestra en la lista.



- (2) Eliminar aplicación de ACL: Haga clic en **Eliminar** detrás de una entrada de aplicación de ACL especificada en la lista. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación. Para eliminar varias entradas de aplicación de ACL, seleccione uno o más registros en la lista de aplicaciones de ACL. Haga clic en **Eliminar seleccionado** para eliminar por lotes los registros. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.

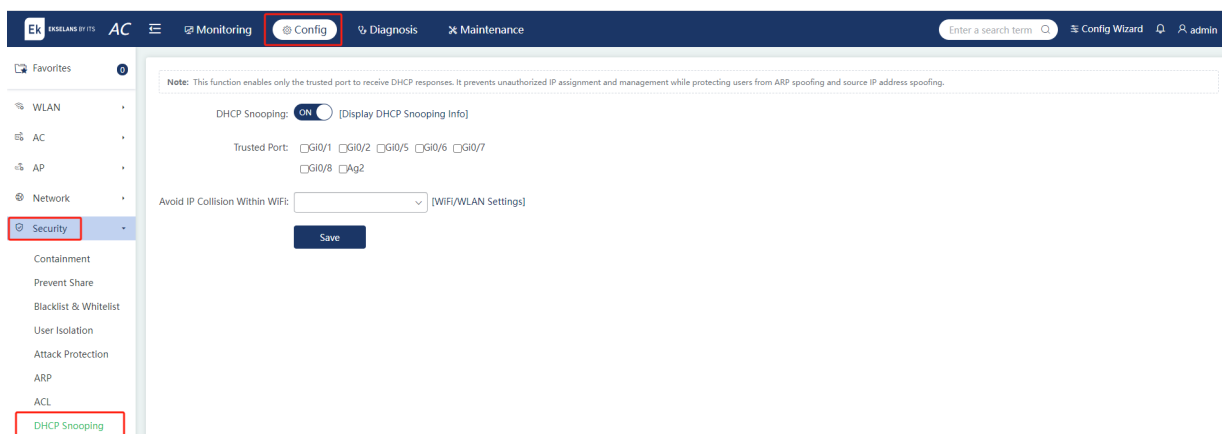


- (3) Editar aplicación de ACL: Haga clic en **Editar** detrás de una entrada de aplicación de ACL especificada en la lista. El cuadro de diálogo emergente muestra la información sobre la aplicación ACL. Edita la información. Haga clic en **Guardar**. Se muestra un mensaje que indica que la configuración se ha guardado.



5.5.8 Seguridad DHCP

Haga clic en **Configuración > seguridad > indagación DHCP**.



Parámetro	Descripción
Indagación DHCP	Habilita o deshabilita la función de indagación DHCP.
Mostrar información de indagación DHCP	Muestra la información sobre los usuarios y las direcciones IP delimitadas guardadas en el AC.

Puerto de confianza	Permite que la AC solo reenvíe los paquetes DHCP recibidos en puertos de confianza.
Evite la colisión de IP dentro de Wi-Fi	Especifica la red Wi-Fi que se habilitará con la función de prevención de conflictos de direcciones IP. Una vez habilitada esta función, el AC filtrará a los usuarios que se conecten a la red Wi-Fi en función de la información sobre los usuarios y las direcciones IP delimitadas.

5.6 Autenticación

5.6.1 Autenticación basada en la web

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

La autenticación basada en web es un método de autenticación de identidad para controlar los permisos de los usuarios para el acceso a la red. Este método de autenticación no requiere un software de autenticación de cliente dedicado. La autenticación de identidad se puede implementar mediante un navegador común. La autenticación de nombre real facilita la gestión de usuarios. En función de la ubicación del servidor de autenticación, la autenticación basada en web se clasifica en **autenticación de ePortal** y **autenticación de iPortal**.

1. Autenticación ePortal

Cuando los usuarios no autenticados acceden a Internet a través de un navegador, el dispositivo de acceso redirige a la fuerza el navegador a una URL especificada para realizar la autenticación. Cuando el portal (la página web de autenticación) se encuentra en un dispositivo independiente fuera de la CA, la autenticación es una autenticación externa basada en web.

The screenshot shows the web management interface of an EKSELANS BY ITS AC device. The top navigation bar includes 'Monitoring', 'Config' (highlighted with a red box), 'Diagnosis', and 'Maintenance'. On the left sidebar, 'Authentication' is selected, and 'Web Auth' is highlighted with a red box. The main content area is titled 'ePortal Authentication' and contains the following fields:

- Note:** Authentication is based on Web to control users' access to the network. It requires no authentication firmware on the client. Instead, you can perform authentication on common browsers.
- Eportal Type:** Radio buttons for 'ePortalv1' and 'ePortalv2' (selected).
- Portal Server IP:** Text input field with a red asterisk and '[Other Server]' label.
- Redirection URL:** Text input field with a red asterisk.
- Portal Key:** Text input field with a red asterisk.
- Authentication Server:** Dropdown menu set to 'All Servers' with '[Radius Server Settings]' label.
- Accounting Server:** Dropdown menu set to 'All Servers'.
- SNMP Server:** Text input field with a red asterisk and '[SNMP Server]' label.
- SSID:** Text input field with a red asterisk and '[WiFi/WLAN Settings]' label.

At the bottom, there is an 'Advanced Settings' section (collapsed) and 'Save' and 'Clear' buttons.

(1) **ePortalv1:**

ePortal Authentication
iPortal Authentication

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

Eportal Type: ☒ ePortalv1 ☐ ePortalv2 ?

Portal Server IP: *

Redirection URL: *

Portal Key: *

SNMP Server: [SNMP Server] *

SSID: [WiFi/WLAN Settings]

[Advanced Settings](#)

Parámetro	Descripción
IP del servidor del portal	<p>En el modo de configuración de plantilla, utilice el comando ip { ip-address } para configurar la dirección IP del servidor.</p> <p>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.</p>
URL de redireccionamiento	Indica la dirección URL a la que se redirigirá a los usuarios, normalmente la página de autenticación del portal.
Clave del portal	Configura una clave para la comunicación entre el dispositivo y el servidor de autenticación.
Servidor SNMP	<p>Cuando el dispositivo detecta que un usuario se desconecta, notifica al servidor del portal. El servidor configura el dispositivo para eliminar la información del usuario (a través del protocolo SNMP). El servidor del portal devuelve la página sin conexión al usuario.</p> <p>Por lo tanto, se debe configurar un servidor SNMP para ePortalv1.</p>
SSID (en inglés)	<p>Especifica la red Wi-Fi que se va a configurar con ePortalv1.</p> <p>Nota: Actualmente solo se admite el modo de autenticación global. El modo de autenticación basado en WLAN no está disponible.</p>

(2) ePortalv2:

ePortal Authentication
iPortal Authentication

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

Eportal Type: ☐ ePortalv1 ☒ ePortalv2 ?

Portal Server IP: * [Other Server]

Redirection URL: *

Portal Key: *

Authentication Server: [Radius Server Settings]

Accounting Server:

SNMP Server: *

SSID: [WiFi/WLAN Settings]

» Advanced Settings

Save Clear

Parámetro	Descripción
IP del servidor del portal	<p>En el modo de configuración de plantilla, utilice el comando ip { ip-address } para configurar la dirección IP del servidor.</p> <p>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.</p>
URL de redireccionamiento	Indica la dirección URL a la que se redirigirá a los usuarios, normalmente la página de autenticación del portal.
Clave del portal	Configura una clave para la comunicación entre el dispositivo y el servidor de autenticación.
Servidor de autenticación	<p>Para aplicar correctamente la autenticación web de segunda generación, se debe configurar la autenticación de autenticación, autorización y contabilidad (AAA).</p> <p>La lista de métodos de autenticación asocia las solicitudes de autenticación basadas en web con el servidor RADIUS. El NAS selecciona el método de autenticación y el servidor en función de la lista de métodos de autenticación web.</p>
Servidor de contabilidad	<p>Obligatorio. Para aplicar correctamente la autenticación basada en web de segunda generación, se debe configurar la contabilidad AAA.</p> <p>La contabilidad se utiliza para asociar un método de contabilidad con el servidor. En la autenticación web, la contabilidad se implementa para registrar la información del usuario o las tarifas.</p>

Servidor SNMP	El servidor SNMP se utiliza para la comunicación entre los usuarios y el servidor del portal.
SSID (en inglés)	La autenticación de segunda generación se aplica a las redes Wi-Fi.

2. Autenticación de iPortal

Cuando los usuarios no autenticados acceden a Internet a través de un navegador, el dispositivo de acceso redirige a la fuerza el navegador a una URL especificada para realizar la autenticación. Cuando el portal (la página web de autenticación) se encuentra dentro de la AC, la autenticación es una autenticación interna basada en web. La página de autenticación permite configuraciones personalizadas parciales, incluido el logotipo personalizado, el título y el descargo de responsabilidad. Cuando la función de acceso a Internet con un solo clic está habilitada, los usuarios pueden hacer clic **en Iniciar sesión** en la página de autenticación para pasar la autenticación sin ingresar un nombre de usuario y contraseña. Esta función solo surte efecto cuando la página de autenticación se establece en el modo predeterminado del sistema o en el modo personalizado parcial.

ePortal Authentication
iPortal Authentication

Download Template: Default

Select WiFi:

One-Click Auth: ☐ Enable ?

Auth Account: Use local user information Local User Management

Auth Page Settings: ☒ Default ☐ Partially Custom ☐ Fully Custom

Advanced Settings

AD Push Mode: No AD

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

Settings: [Advanced Settings]

Save Clear

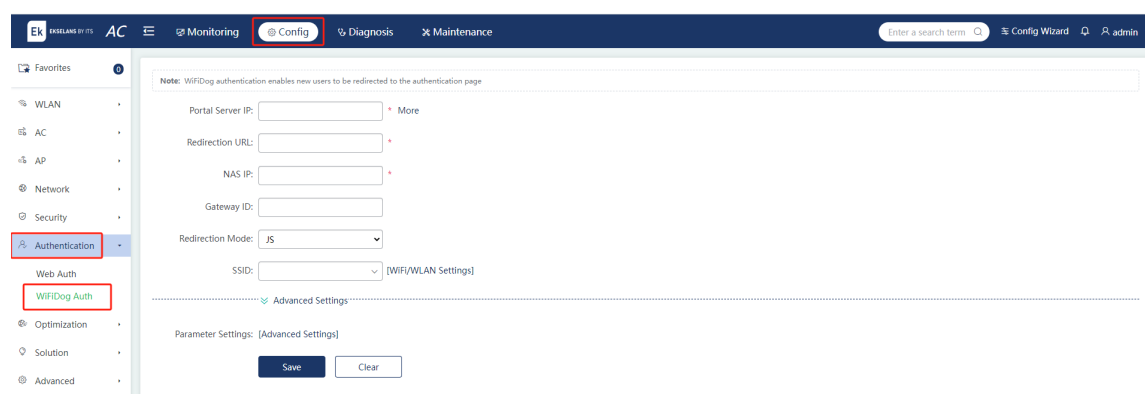
Parámetro	Descripción
Cuenta de autenticación	<p>Se admiten los siguientes orígenes de cuentas de autenticación:</p> <p>Utilizar preferentemente la información del usuario en el servidor</p> <p>Utilizar preferentemente la información de los usuarios locales</p> <p>Usar información de usuario solo en el servidor</p> <p>Solo información de usuario local</p>

Configuración de la página de autenticación	Admite la configuración predeterminada del sistema, la configuración personalizada parcial y la configuración personalizada completa.
Modo de empuje AD	El modo de inserción de anuncios incluye la inserción de anuncios antes o después de la autenticación. De forma predeterminada, no se ha configurado ningún anuncio.
Puerto de servidor iPortal	Configura el número de puerto de la página de autenticación para la autenticación interna del portal. El número de puerto predeterminado es 8.081.

5.6.2 Autenticación WiFiDog

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

Los usuarios no autenticados pueden ser 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: haz clic en **Agregar servidor de autenticación**. Configure la información de ACL en el cuadro de diálogo emergente. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado. El servidor recién agregado se muestra en la lista de servidores.

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

Portal Server IP: * **More**

Redirection URL: *

NAS IP: *

Gateway ID:

Redirection Mode: ▼

SSID: ▼ [WiFi/WLAN Settings]

✓ Advanced Settings

Parameter Settings: [Advanced Settings]

Save **Clear**

WiFiDog Auth Server List

+ Add Authentication Server

Server IP	Redirection URL	NAS IP	Gateway ID	Redirection Mode	SSID	Action
<p>Show No.: <input type="text" value="10"/> Total Count: 0</p> <p>K First < Pre Next > Last 1 Go</p>						

Add Server

Portal Server IP: *

Redirection URL: *

NAS IP: *

Gateway ID:

Redirection Mode: ▼

SSID: ▼ [WiFi/WLAN Settings]

Cancel **OK**

Parámetro	Descripción
IP del servidor del portal	Indica la dirección IP de un servidor del portal.
URL de redireccionamiento	Indica la dirección URL del servidor del portal para la autenticación.
NAS IP	Especifica la dirección IP de un dispositivo que va a administrar WiFiDog, que se utiliza para la comunicación desde el servidor.
Modo de redirección	Especifica el redireccionamiento HTTP o el redireccionamiento de JavaScript. La redirección de JavaScript se emplea de forma predeterminada.

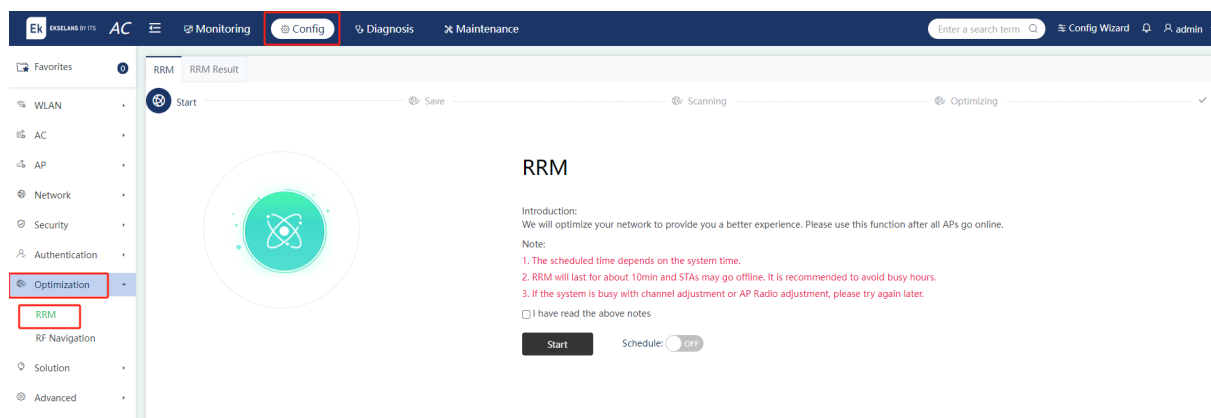
ID de puerta de enlace	Especifica el ID de una puerta de enlace utilizada por WiFiDog, que es el SN de la puerta de enlace de forma predeterminada.
SSID (en inglés)	Especifica una red Wi-Fi que se configurará con la autenticación WiFiDog.

- (2) Eliminar un servidor de autenticación WiFiDog: haz clic en **Eliminar** detrás de un servidor de autenticación especificado. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.
- (3) Editar un servidor de autenticación WiFiDog: haz clic en **Editar**. Configure la información en el cuadro de diálogo emergente. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado. El servidor modificado se muestra en la lista de servidores.

5.7 Optimización de la red

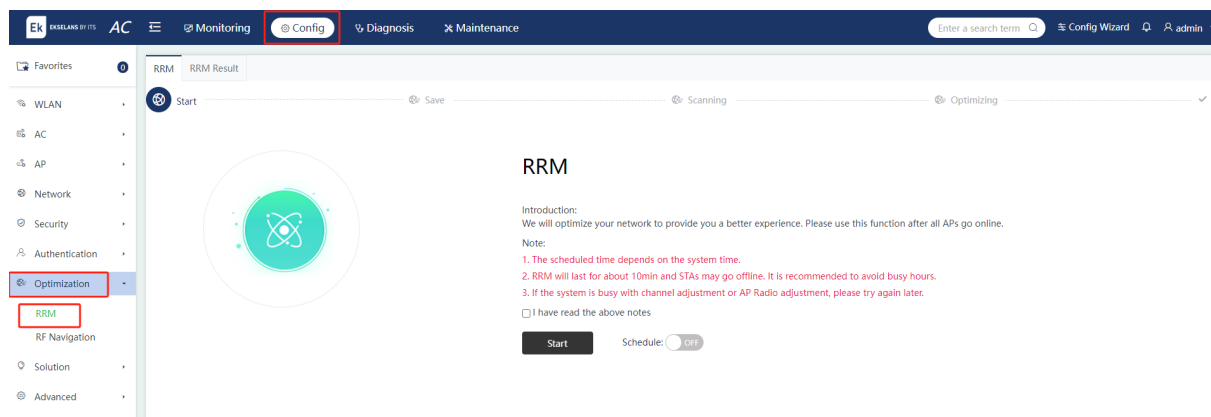
5.7.1 RRM

Elija **Config > Optimization > RRM**.

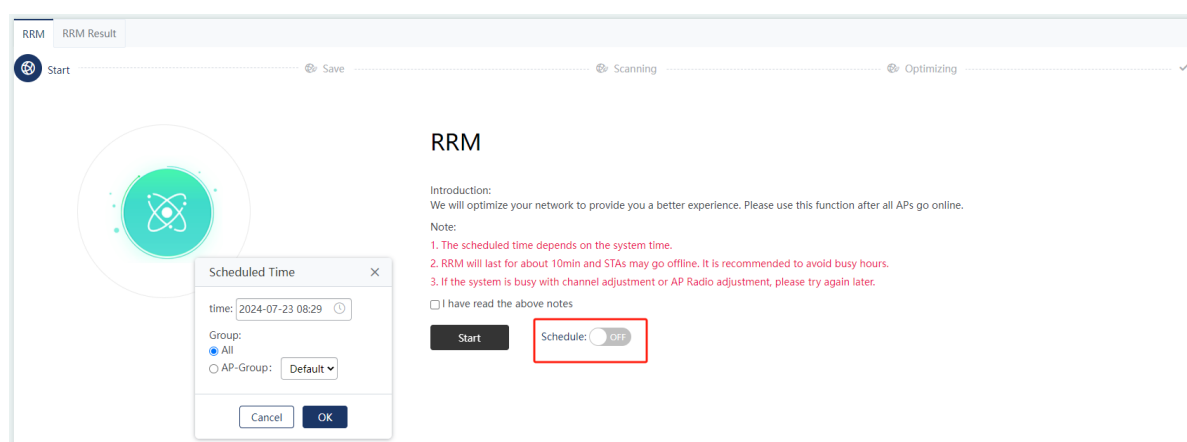


1. RRM con un solo clic

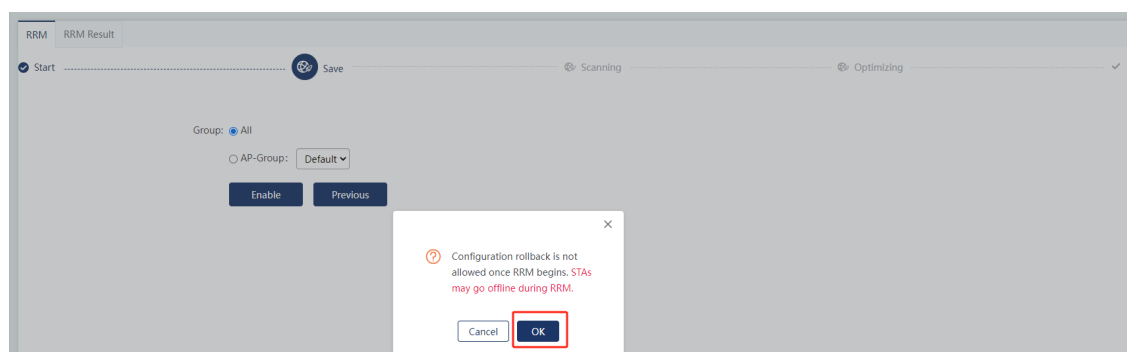
El RRM de un solo clic se utiliza para optimizar la red y obtener el máximo rendimiento inalámbrico. Se recomienda utilizar esta función después de que todos los AP en el área que se va a optimizar se conecten. Antes de realizar RRM con un solo clic, lea las precauciones pertinentes. Activa el **interruptor Programar**. Aparecerá el **cuadro de diálogo Hora** programada. Elija un momento adecuado para la optimización de la red según sea necesario.



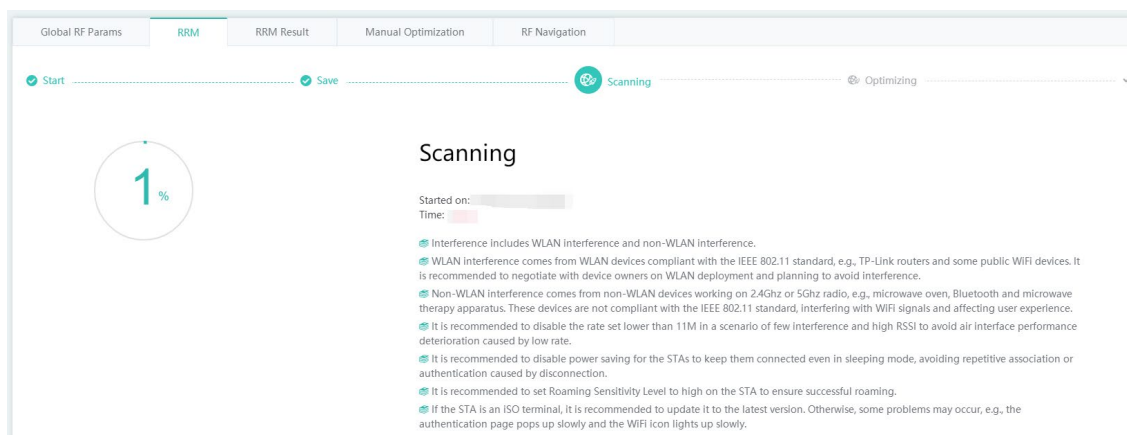
Lea las notas y marque **He leído las notas anteriores** para pasar a la etapa de escaneo automático y optimización. Espere hasta que se genere el resultado de la optimización.



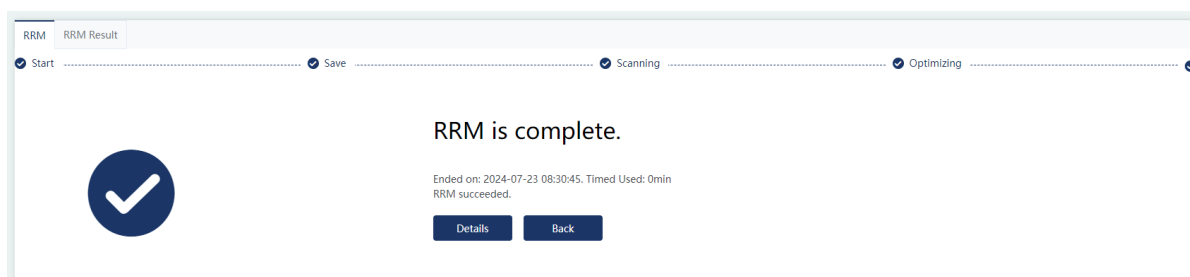
Seleccione esta opción para optimizar todos los AP o un grupo de AP especificado. Haga clic en **Habilitar**. Se analizarán los puntos de acceso en línea que admitan la optimización de la red. Una vez que se inicia el RRM, la configuración no se puede revertir. Durante la optimización, es posible que los usuarios se desconecten.



El canal, el ancho del canal y la potencia se optimizarán para los AP compatibles.



Una vez completado el RRM, haga clic en **Atrás** para volver a la página del **RRM**. Haga clic en **Detalles** para ser redirigido a la página **de resultados de RRM** y comprobar la optimización.

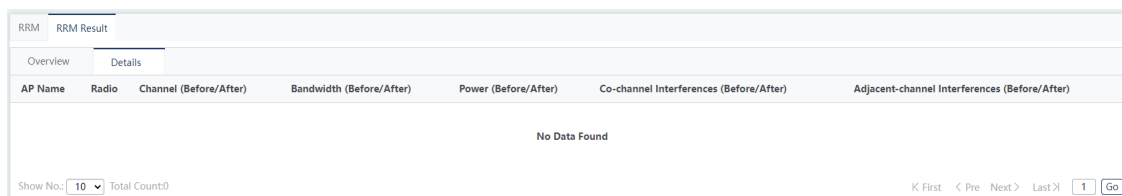


2. Resultado RRM

Visión general: Muestra el número de interferencias de señal antes y después del RRM en forma de gráfico de barras (los 20 cambios más significativos).

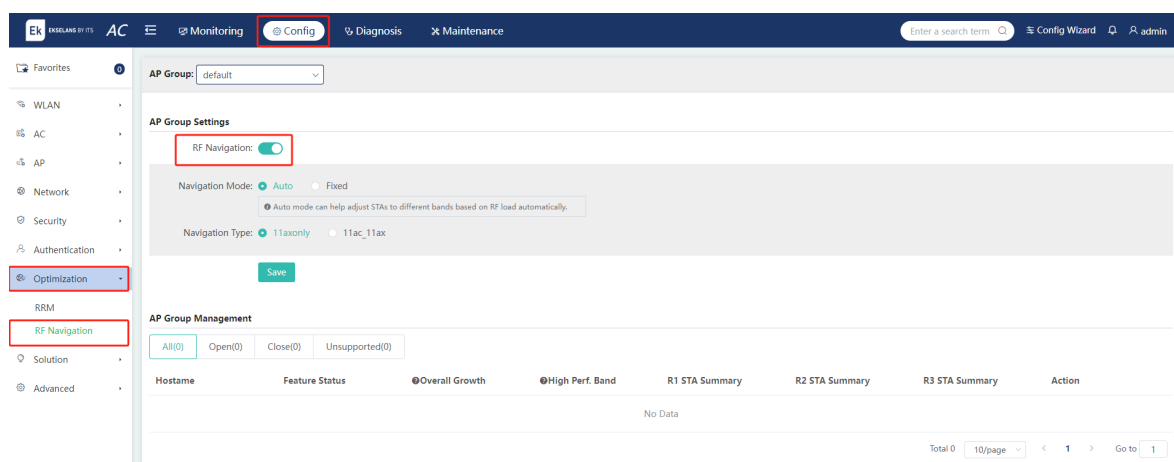
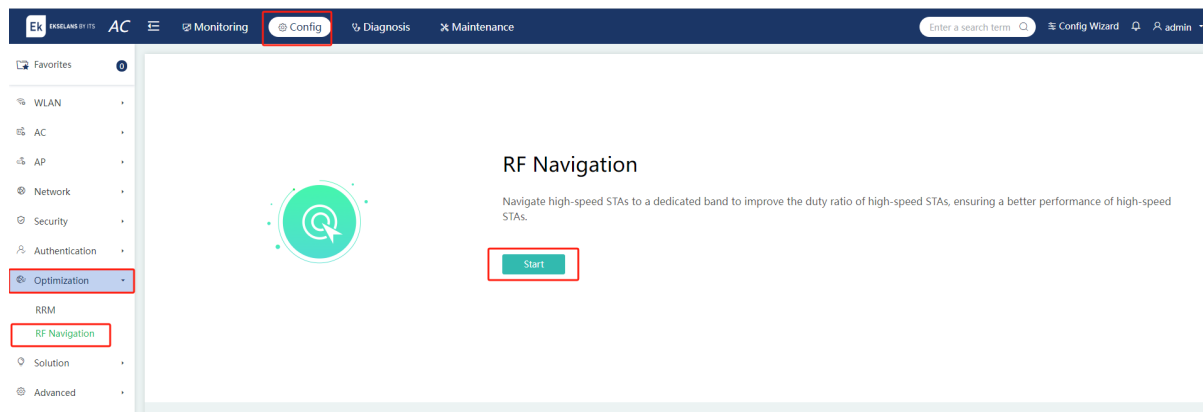


Detalles: Muestra todos los resultados de RRM en un formato de lista, con los cambios en los datos antes y después del RRM resaltados en fuente roja.



3. Navegación RF

Cuando coexisten varios tipos de clientes, los clientes de alto rendimiento se navegan a una banda de frecuencia dedicada de alta eficiencia. Esto evita que los clientes de baja velocidad ocupen la interfaz aérea durante mucho tiempo y mejora la relación de trabajo de los clientes de alto rendimiento. La navegación por RF garantiza que los clientes de alto rendimiento tengan una mejor experiencia en la banda de frecuencia de Wi-Fi 6.

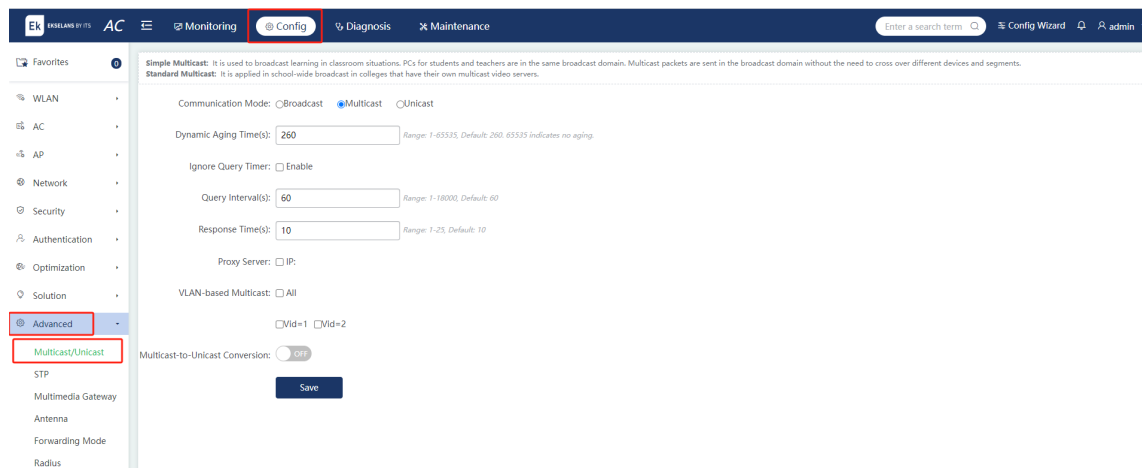


5.8 Avanzado

5.8.1 Multidifusión/Unidifusión

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

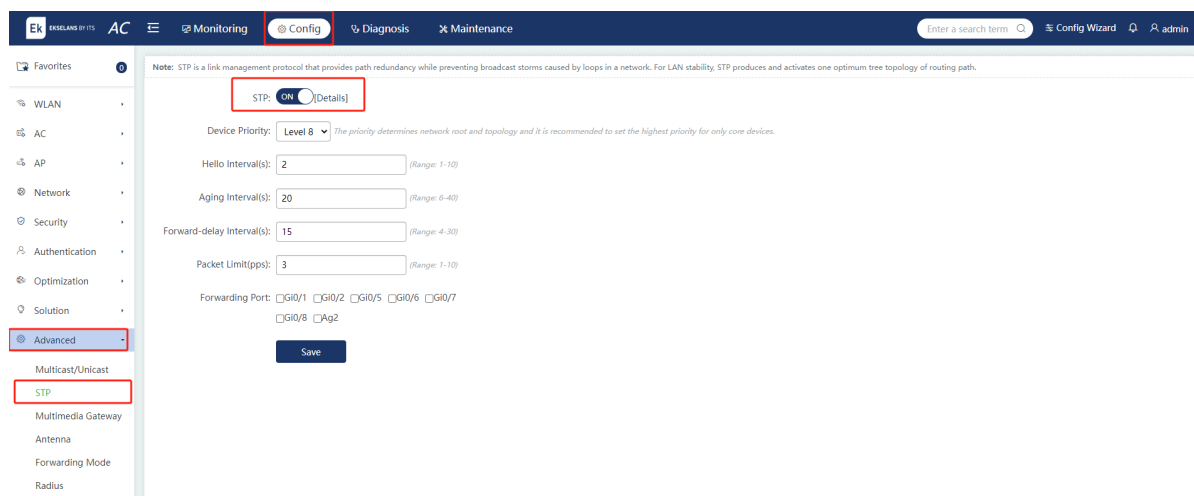
Esta función se utiliza para configurar el modo de comunicación de un dispositivo como difusión, multidifusión o unidifusión.



5.8.2 STP

Elija **Config > Advanced > STP**.

El protocolo de árbol de expansión (STP) es un protocolo utilizado para evitar tormentas de difusión causadas por bucles de enlace y proporcionar respaldo de redundancia de enlace; su función es descubrir y activar una topología de árbol óptima de la red de área local (LAN) para garantizar la estabilidad de la red.



5.8.3 Pasarela multimedia

Elija **Config > Advanced > Multimedia Gateway**.

La puerta de enlace multimedia es utilizada principalmente por clientes iOS y Android para la duplicación de pantalla en servidores de dispositivos que admiten los protocolos AirPlay y DLNA, como los decodificadores de TV.

1. Pantalla de transmisión

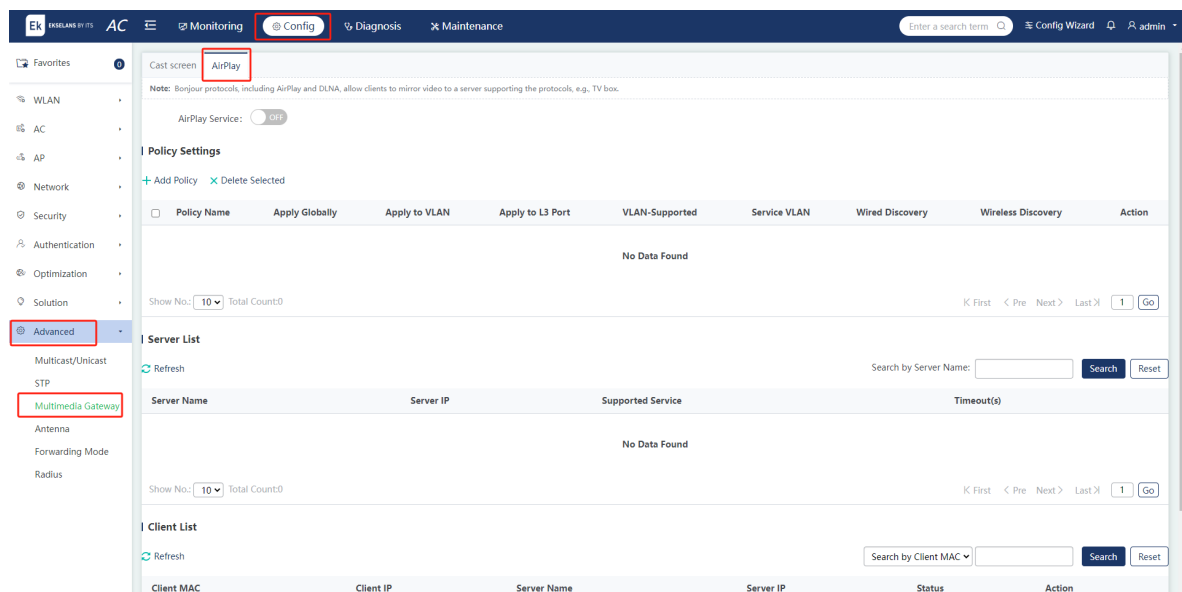
Las soluciones precisas de duplicación de pantalla se pueden configurar convenientemente. Actualmente, se admiten los protocolos AirPlay y DLNA. Si necesita una configuración más avanzada y profesional, vaya a la página correspondiente para configurar protocolos y estándares.

The screenshot shows the 'Config' tab selected in the top navigation bar. The left sidebar has 'Advanced' and 'Multimedia Gateway' highlighted. The main content area displays the 'Screen Mirror Settings' section, which includes a 'Screen Mirror' toggle switch (currently off) and 'Service Details' for 'AirPlay' and 'Client-TV Binding'. Below this is the 'Client-TV Binding List' with an '+ Add' button. The 'AirPlay' section is expanded, showing a search bar for 'TV Name' and a table with columns: Client MAC, TV Name, TV MAC, Associated Duration, Protocol, and Action. The table is currently empty, displaying 'No Data Found'. Below the table is a pagination control showing 'Show No.: 10' and 'Total Count:0'. The 'Server List' section is also expanded, showing a search bar for 'Server Name' and a table with columns: Server Name, Server IP, and Protocol. This table is also empty, displaying 'No Data Found'. Below the table is a pagination control showing 'Show No.: 10' and 'Total Count:0'.

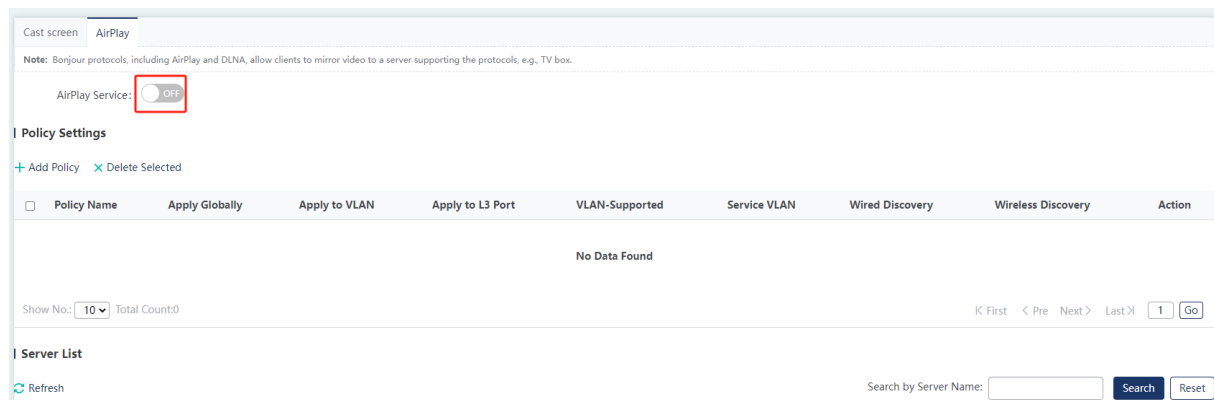
This screenshot is a zoomed-in view of the 'Client-TV Binding List' and 'Server List' sections from the previous image. The 'Client-TV Binding List' section has a red box around the '+ Add' button. The 'Server List' section has a red box around the 'Server List' header. Both sections show search bars and empty tables with 'No Data Found' messages. The pagination controls at the bottom of each section show 'Show No.: 10' and 'Total Count:0'.

2. Airplay

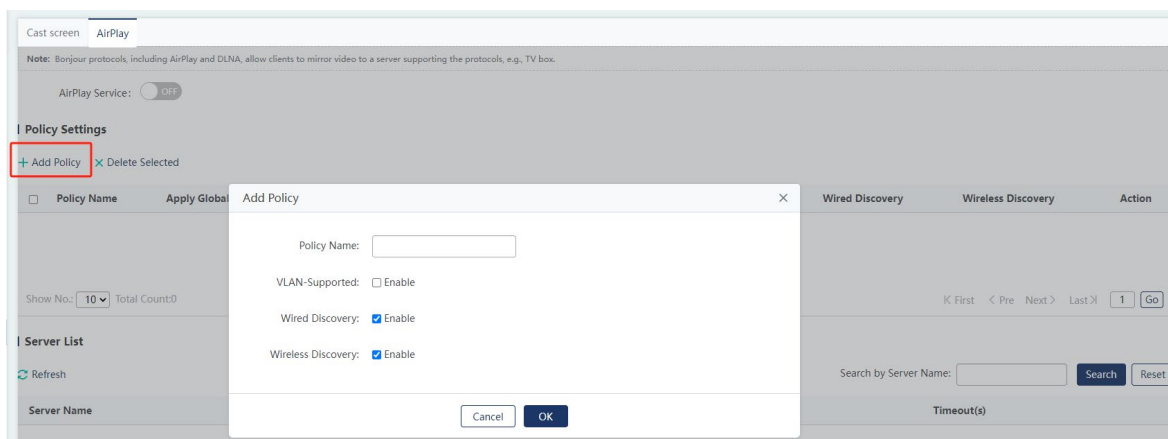
Los protocolos de puerta de enlace multimedia incluyen principalmente AirPlay y DLNA, que se utilizan para la duplicación de pantalla desde clientes móviles hasta servidores de dispositivos que admiten los protocolos, como los decodificadores de TV.



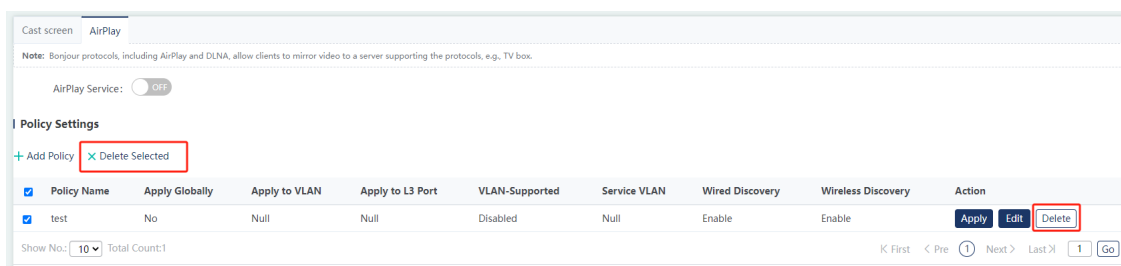
- (1) Habilitar **el servicio AirPlay**: habilite el protocolo AirPlay o DLNA para la puerta de enlace multimedia según sea necesario. Cuando el protocolo está deshabilitado, la política correspondiente no surtirá efecto. Se muestra la política correspondiente al protocolo habilitado.



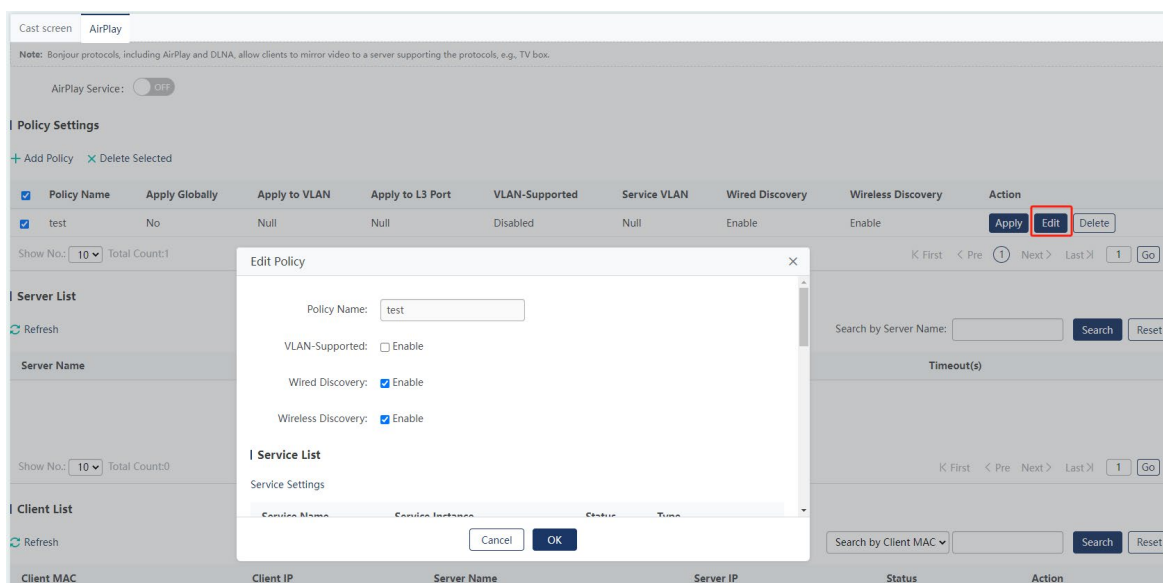
- (2) Agregar una política: elija **Configuración de política > Agregar política**. Configure la información en el cuadro de diálogo emergente. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado. La política recién agregada se muestra en la lista de políticas.



- (3) Eliminar una política: haga clic **en Eliminar** una política especificada en la lista. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación. Para eliminar varias directivas, seleccione las directivas que desea eliminar de la lista. Haga clic en **Eliminar** seleccionados. Aparece el cuadro de diálogo de confirmación. Haga clic en **Aceptar** para finalizar la operación.



- (4) Editar una política: haga clic **en Editar** una política especificada en la lista. El cuadro de diálogo emergente muestra la información sobre la política. Edita la información. Haga clic en **Aceptar**. Se muestra un mensaje que indica que la configuración se ha guardado.

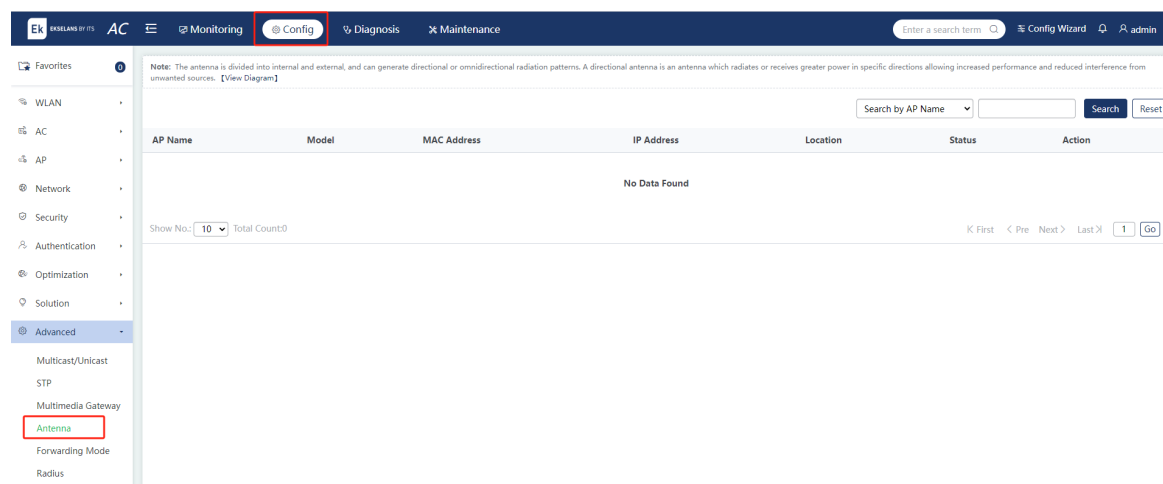


5.8.4 Antena

Elija **Config > Advanced > Antenna**.

Las antenas de RF se clasifican en dos tipos: antenas incorporadas y antenas externas. Las orientaciones de las antenas incluyen dos tipos: direccionales y omnidireccionales. Las antenas direccionales irradian la señal dentro de un cierto rango de ángulo. El rango de radiación es como un cono.

Haga clic en **Editar** en la lista de AP para acceder a la página de configuración de la antena. Los tipos de antena incluyen antenas incorporadas y antenas externas. La orientación de la antena se divide en omnidireccional y direccional. El hecho de que el puerto de RF admita la conmutación de tipo/orientación depende de sus propias capacidades. Si el puerto RF no admite el cambio de tipo/orientación, el sistema web mostrará el mensaje **Esta radio no admite cambiar el estilo.** o **Esta radio no es compatible con el cambio de dirección.** al usuario.



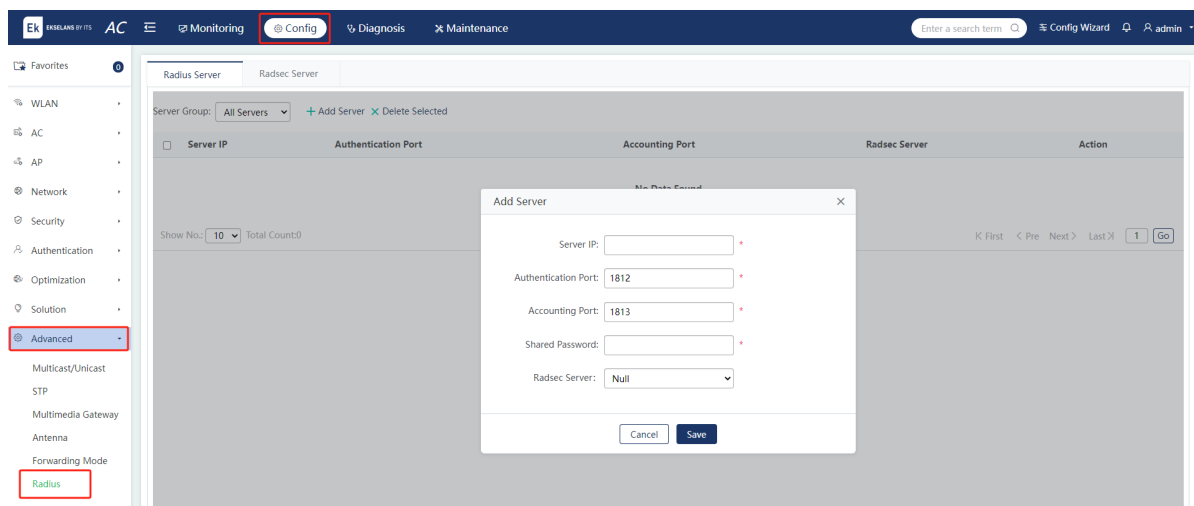
5.8.5 RADIO

Elija **Config > Advanced > Radius**.

1. Servidor RADIUS

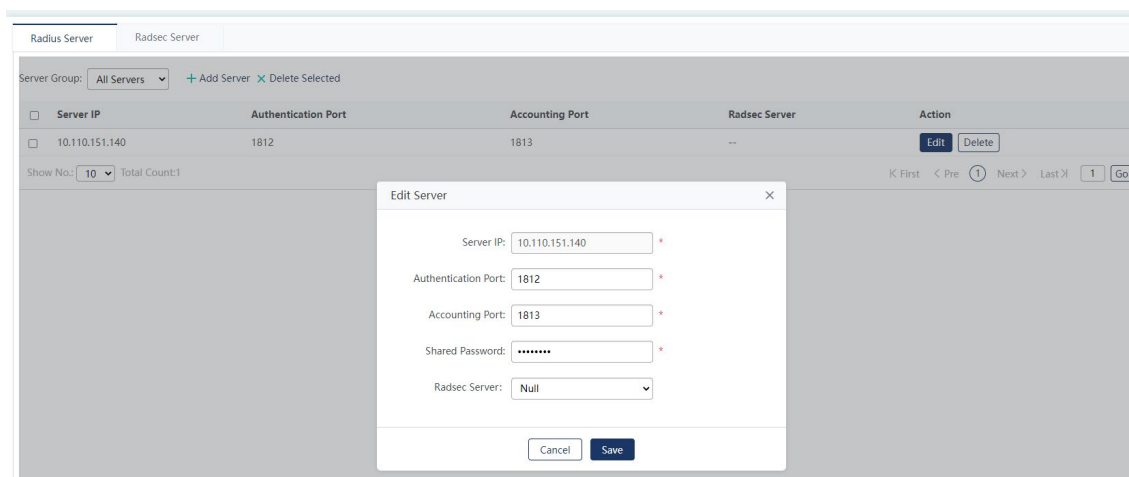
El servidor RADIUS lleva a cabo la autenticación de identidad y la contabilidad de los usuarios de acceso para proteger la seguridad de la red y facilitar la administración para los administradores de red.

- (1) Agregar un servidor: haz clic en **Agregar servidor**. Establezca los campos y haga clic en **Guardar**. Se muestra un mensaje que indica que la configuración se ha guardado.

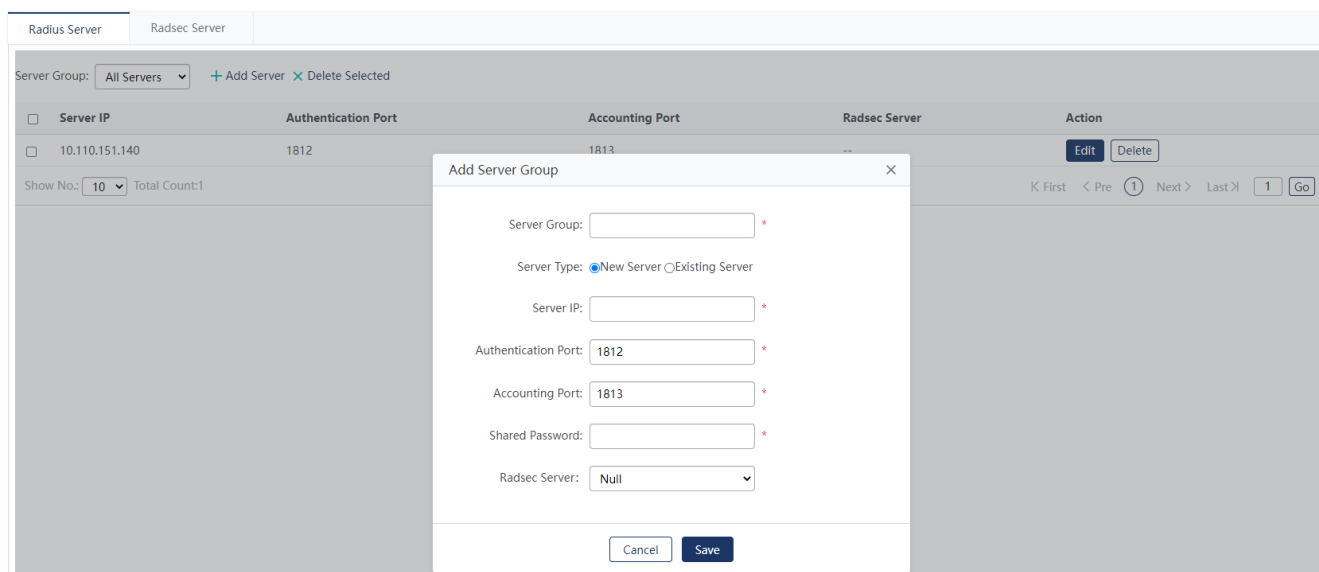


Parámetro	Descripción
IP del servidor	Indica la dirección IP de un servidor RADIUS.
Puerto de autenticación	Indica el ID de puerto UDP para la autenticación RADIUS. El rango de valores es de 0 a 65.535. 0 indica que el servidor no realiza la autenticación de identidad.
Puerto de contabilidad	Indica el ID de puerto UDP para la contabilidad RADIUS. El rango de valores es de 0 a 65.535. 0 indica que el servidor no realiza la contabilidad.
Contraseña compartida	Indica la clave compartida para la comunicación entre el servidor de acceso a la red (router) y el servidor RADIUS.
Servidor Radsec	(Opcional) Indica el ID del servidor RadSec, al que se redirige el tráfico desde el servidor RADIUS.

- (2) Editar un servidor: haz clic en **Editar** para un servidor existente. Edite los valores de los parámetros. Haga clic en **Guardar**.



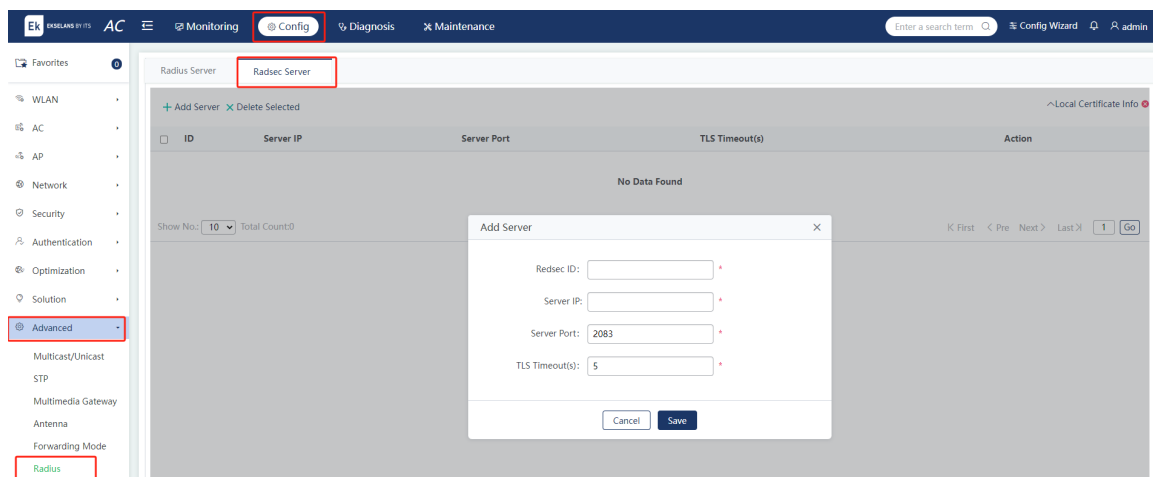
- (3) Agregar un grupo de servidores: haga clic en la lista desplegable Grupo de servidores y seleccione **Agregar grupo de servidores**. Aparece el **cuadro de diálogo Agregar grupo de servidores**. Si selecciona **Nuevo servidor**, se agregará un grupo de servidores y un servidor y el servidor pertenece al grupo de servidores. Si selecciona **Servidor existente**, se agregará un servidor existente al grupo de servidores.



2. Servidor RadSec

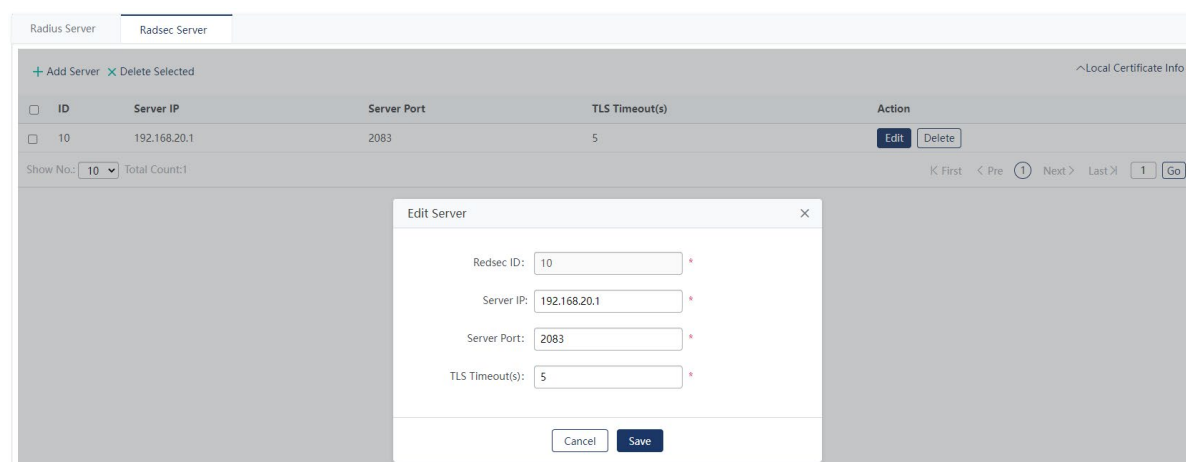
RadSec proporciona una comunicación segura para las solicitudes RADIUS mediante el protocolo de seguridad de la capa de transporte (TLS) y permite que los datos de autenticación, autorización y contabilidad de RADIUS se transmitan de forma segura a través de redes que no son de confianza.

- (1) Agregar un servidor: haz clic en **Agregar servidor**. Establezca los campos y haga clic en **Guardar**. Se muestra un mensaje que indica que la configuración se ha guardado.

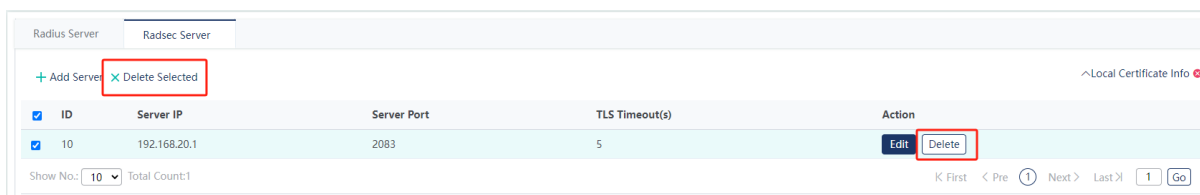


Parámetro	Descripción
Radsec ID	Indica el ID único de un servidor RadSec. El valor es un número entero en el intervalo de 1 a 255.
IP del servidor	Indica la dirección IP del servidor RadSec.
Puerto del servidor	Especifica el ID de puerto del servidor RadSec. El rango de valores es de 1 a 65.535. El valor predeterminado es 2083 .
Tiempo de espera de TLS	Especifica el tiempo de espera de la conexión TLS. El rango de valores es de 1 a 1.000. El valor predeterminado es 5 .

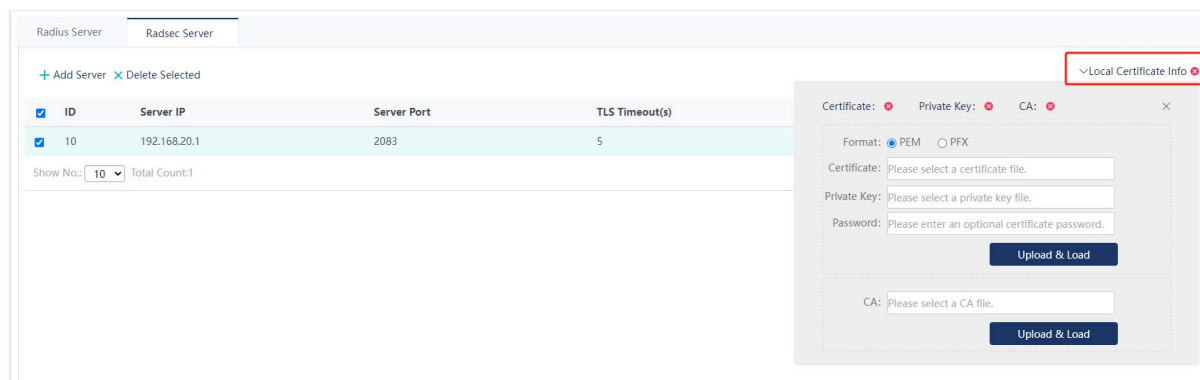
- (2) Editar un servidor: haz clic en **Editar** detrás de un servidor especificado. Modifique los valores de los parámetros y haga clic en **Guardar**.



- (3) Eliminar un servidor: haz clic en **Eliminar** detrás de un servidor especificado. Si necesita eliminar varios servidores, seleccione los servidores que desea eliminar y haga clic en **Eliminados seleccionados** para eliminarlos por lotes.



- (4) Administración de certificados locales: haga clic en **Información de certificado local**. Aparece el cuadro de diálogo 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 el certificado se ha cargado correctamente. Se admiten los formatos PEM y PFX. Si el archivo de certificado no contiene información de CA, seleccione un archivo de AC y haga clic en **Cargar y cargar**.



6 Diagnóstico

6.1 Diagnóstico de red

6.1.1 Diagnóstico de red

Elija **Diagnóstico** > **Diagnóstico en red** > **Diagnóstico en red**.

1. Prueba de conectividad

The screenshot displays the 'Network Diagnosis' interface. The top navigation bar includes 'Monitoring', 'Config', 'Diagnosis' (selected), and 'Maintenance'. The left sidebar lists various tools, with 'Network Diagnosis' selected. The main panel shows the 'Connectivity Test' results. 'Port Status' is successful. 'AC-AP Connection Status' shows a failure with instructions to check WiFi/WLAN and VLAN settings. 'Internet Connection Status' also shows a failure with instructions to check route settings and network topology. A 'Test Again' button is available at the bottom.

Elemento de detección	Descripción
Estado del puerto	Comprueba si alguna interfaz de la AC está en estado Activo.
Estado de la conexión AC-AP	Comprueba si algún AP conectado a la AC se conecta.
Estado de la conexión a Internet	Comprueba la conectividad entre la AC y las redes externas. Haga ping a la dirección IP de 8.8.8.8.

2. Señal

Ek EKSELANS BY ITS AC Monitoring Config **Diagnosis** Maintenance

Favorites 0

Network Diagnosis

Network Diagnosis

One-Click Collection

STA Teach

Packet Capture

Syslog

WIDS

Alarm

Connectivity Test **Ping** Tracert

Dest IP/Domain Name: *

Advanced Settings

Source IP:

Timeout Interval(s): 2 Range: 1-10

Repeat Times: 5 Range: 1-100

Packet Size(Bytes): 100 Range: 36-18024

Fragment: ☒ Enable

Test Stop

Parámetro	Descripción
IP de destino/Nombre de dominio	Indica la dirección o el nombre de dominio a los que se va a hacer ping.
IP de origen	Indica la dirección de origen de los paquetes de ping, es decir, la dirección de la interfaz local de un dispositivo.
Intervalo(s) de tiempo de espera	Indica la duración del tiempo de espera.
Tiempos de repetición	Indica el número de paquetes de datos que se van a transmitir.
Tamaño del paquete (bytes)	Indica la longitud de la sección de relleno de datos en un paquete de datos que se va a transmitir.
Fragmento	Indica el bit de marca 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

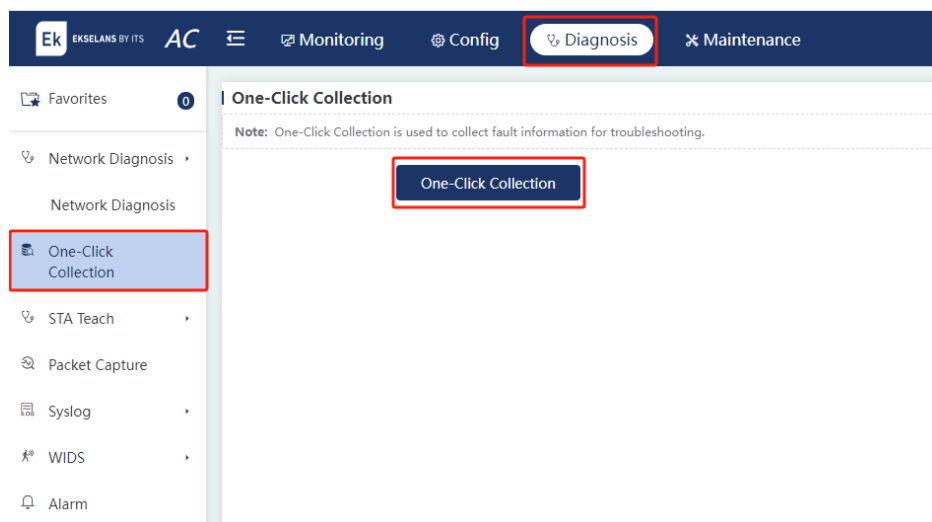
The screenshot shows the EkSELANS BY ITS web interface. The top navigation bar includes 'Monitoring', 'Config', 'Diagnosis' (highlighted), and 'Maintenance'. The left sidebar lists various tools, with 'Network Diagnosis' selected. The main content area displays the 'Tracert' configuration page. It features a 'Dest IP/Domain Name' field, a 'Source IP' field, and a 'Timeout Interval(s)' field set to 2. Below these fields are 'Test' and 'Stop' buttons.

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

6.2 Colección con un solo clic

Elija **Diagnóstico > Colección con un solo clic**.

Puede utilizar la función de recopilación con un solo clic para recopilar información sobre fallas del dispositivo para la resolución de problemas.



6.3 Diagnóstico del cliente

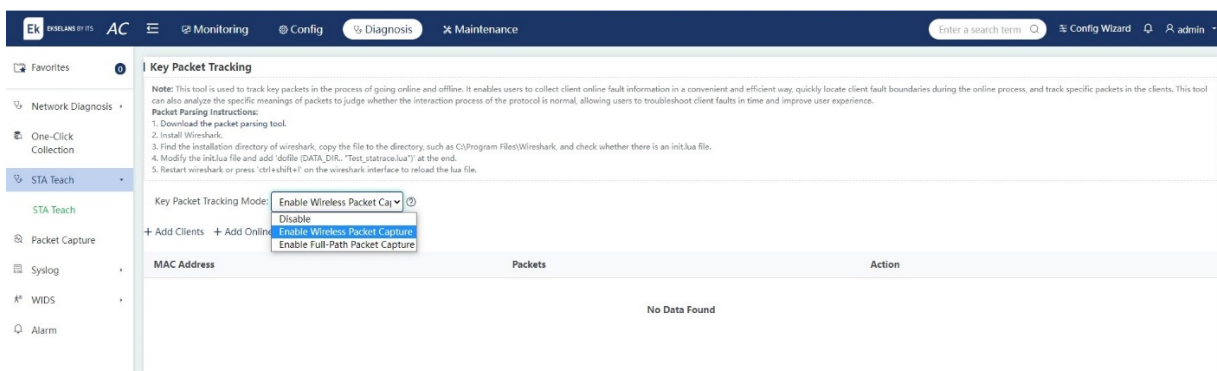
6.3.1 Seguimiento de paquetes de claves

Elija **Diagnóstico > STA Teach > STA Teach**.

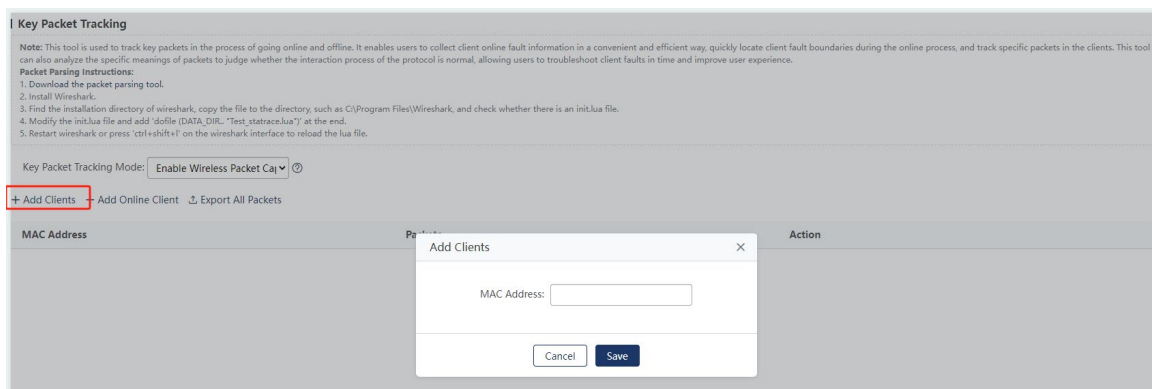
Esta función permite a los usuarios recopilar fácil y rápidamente información de fallas, localizar el alcance de las fallas durante el proceso de puesta en línea de los clientes y realizar un seguimiento de los paquetes de claves de los clientes. El seguimiento de paquetes de claves identifica los paquetes de claves y analiza los campos clave y los significados de los paquetes para determinar si el proceso de interacción del protocolo es normal. Permite a los usuarios recopilar información sobre fallos de forma cómoda y rápida y solucionar los fallos de los clientes a tiempo, mejorando así la experiencia del usuario.

Enable Wireless Packet Obtain: obtiene paquetes en el lado del controlador inalámbrico.

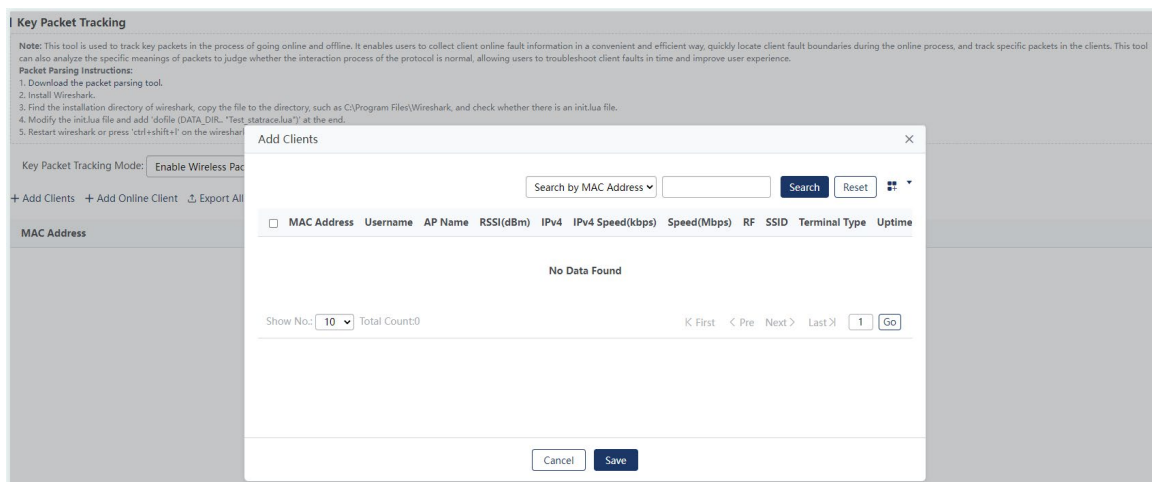
Enable Full-Path Packet Obtain: obtiene paquetes en toda la ruta por la que pasan los paquetes.



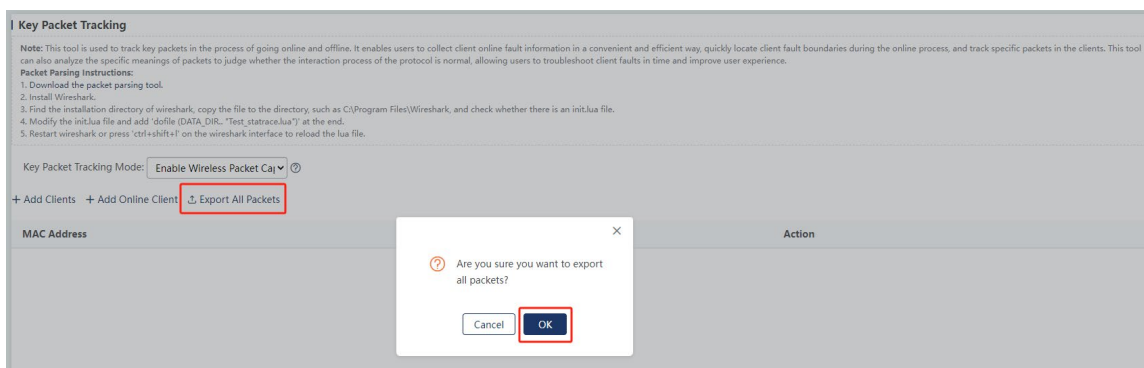
- (1) Agregar un cliente manualmente: haz clic en **Agregar clientes**. Introduzca la dirección MAC de un cliente. Haga clic en **Guardar**. El sistema verifica la validez de la dirección MAC. Si la dirección MAC es válida, se agregará el cliente.



- (2) Seleccionar y agregar un cliente en línea: haz clic en **Agregar cliente en línea**. Seleccione un cliente en línea para el seguimiento de paquetes.



- (3) Exportar paquetes: haga clic en **Exportar paquete** detrás de un cliente especificado. Si es necesario exportar todos los paquetes de cliente, haga clic en **Exportar todos los paquetes** para comprimir todos los paquetes recibidos en un **archivo de .tar** y exportar el archivo a los usuarios.



- (4) Cancelar seguimiento de paquetes: haga clic en **Cancelar detección** detrás de un cliente especificado.

6.4 Obtención de paquetes

Elija **Diagnosis > Packet Capture (Captura de paquetes)**.

Esta función se utiliza generalmente para obtener paquetes para recopilar datos de diagnóstico cuando se producen problemas con los dispositivos posventa.

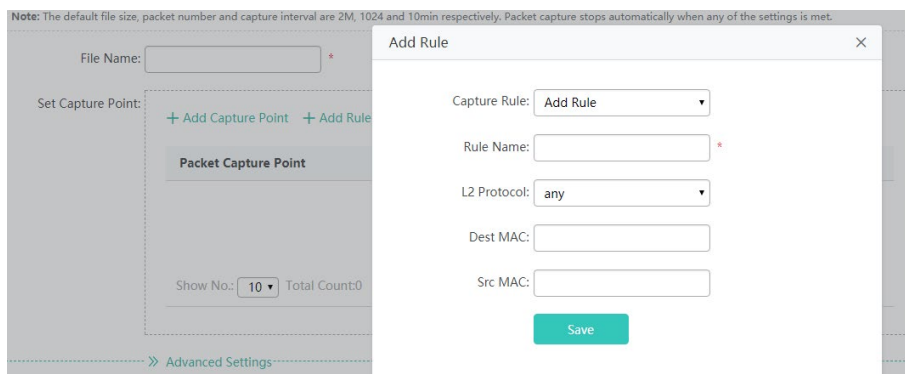
- (1) Iniciar la obtención de paquetes: Edite los campos en la página de configuración. Haga clic en **Comenzar obtener**.

Parámetro	Descripción
Nombre de archivo	Especifica el nombre del archivo que se va a guardar.
Establecer punto de obtención	Especifica la ubicación de obtención del paquete.
Ruta de almacenamiento	Especifica la ruta de almacenamiento del archivo de paquetes obtenido.

Tamaño del archivo (M)	Especifica el tamaño del búfer.
Paquetes	Especifica el número de paquetes que se van a obtener.
Intervalo de obtención (min)	Especifica la duración del tiempo de espera. La obtención de paquetes se detiene automáticamente cuando expira la duración del tiempo de espera.

- (2) Detener la obtención de paquetes: Durante la obtención de paquetes, haga clic en **Finalizar captura** para detener la obtención de paquetes.
- (3) Descargar el archivo: Haga clic en **Descargar archivo** para descargar el archivo obtenido en la computadora.
- (4) Borrar el archivo: Haga clic en **Borrar archivo** para eliminar el archivo obtenido del dispositivo.
- (5) Añadir un punto de captura: haz clic en **"Añadir punto de captura"**. Aparece el cuadro de diálogo de configuración. Configure los parámetros y haga clic en **Guardar**. Se muestra un mensaje que indica que el punto se ha agregado correctamente.

- (6) Eliminar un punto de captura: haz clic en **Eliminar** detrás de un punto de captura especificado.
- (7) Establecer reglas para la obtención de paquetes: haga clic en **Agregar regla**. Aparece el cuadro de diálogo de configuración. Configure los parámetros y haga clic en **Guardar**. Se muestra un mensaje que indica que la regla se ha agregado correctamente.

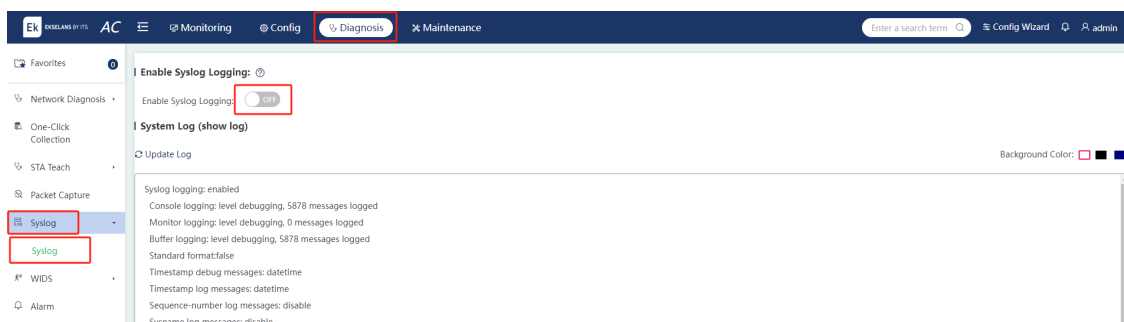


6.5 Registro

6.5.1 Registro del sistema

Elija **Diagnosis > Syslog > Syslog**.

Puede configurar la función de registro del sistema 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.



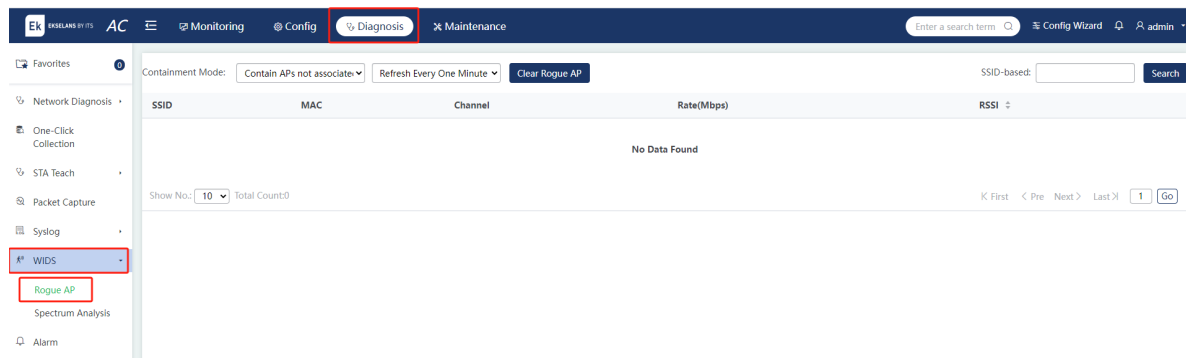
6.6 Detección de interfaz aérea

6.6.1 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 pueden estar controlados por atacantes, amenazando seriamente la seguridad de las redes de los usuarios.

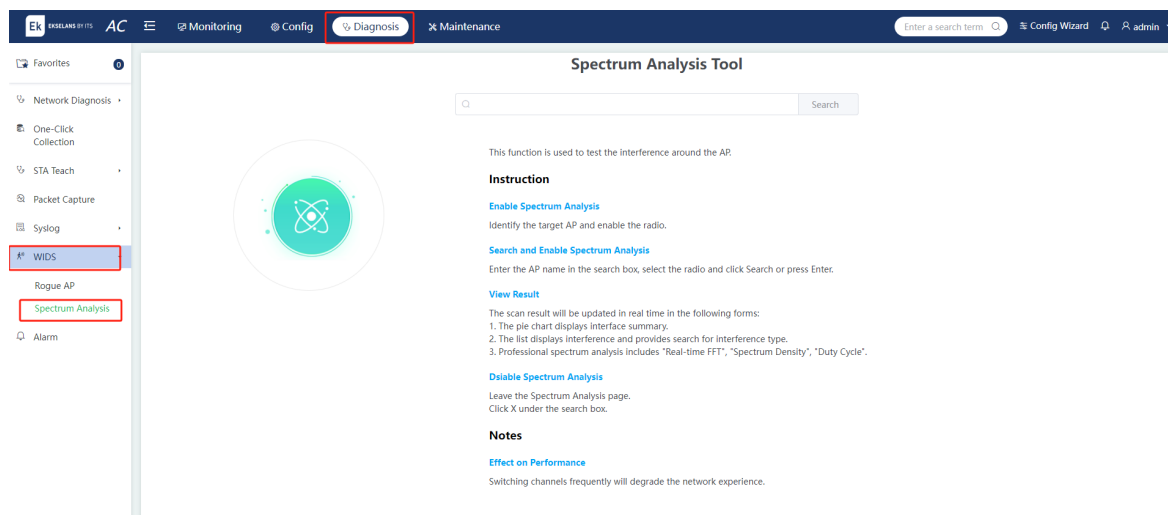
La siguiente página muestra los posibles AP no autorizados que se identifican después de habilitar la función de contención.



6.6.2 Análisis del espectro

Elige **Diagnóstico > WIDS > Análisis de espectro**.

Cuando la calidad de la red es mala, el sistema puede detectar interferencias en la red y determinar si existen interferencias en la red basándose en **FFT en tiempo real, densidad de espectro** y otros diagramas de espectro. Se registra la información de interferencia.



Nota

Para realizar el análisis de espectro, el AP debe conectarse a Internet.

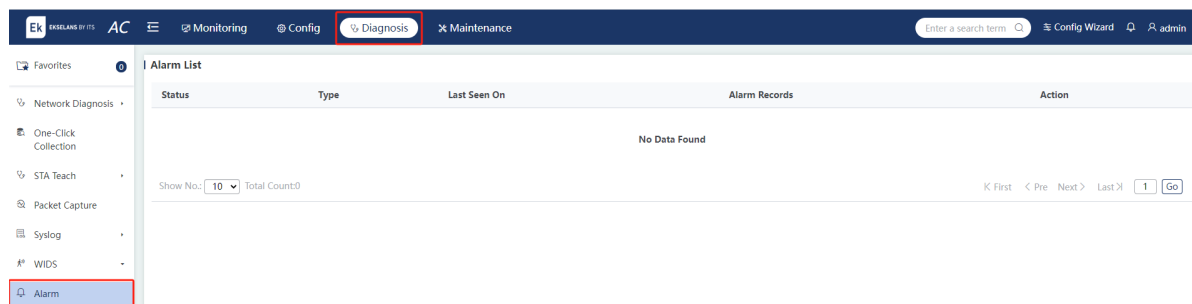
Cuando cambia para ver el resultado del análisis de espectro de otro AP, la función de análisis de espectro en tiempo real se deshabilita automáticamente y debe habilitarse manualmente.

6.7 Alarma

Elige **Diagnóstico > alarma**.

Cuando existan registros de alarma en el sistema, el icono del despertador en la esquina superior derecha de la página estará marcado con un número rojo que indica el número de tipos de alarmas.

Haga clic en el icono del reloj de alarma para ir a la página Lista de **alarmas** y comprobar la información detallada de la alarma.



La lista muestra una descripción general de varias alarmas, incluidas principalmente las alarmas fuera de línea de AP, las alarmas de falla de acceso de AP, las alarmas sobre la cantidad de acceso de usuarios de AP / RF que exceden el umbral (90%) y las alarmas de ahorro de energía de AP. También se muestra el número de alarmas de cada tipo y la última hora de aparición de cada tipo de alarma. Por ejemplo, si dos AP se desconectan, el número mostrado de este tipo de alarma es 2. Haga clic en **No leído**. Aparecerá un cuadro de diálogo de confirmación, en el que se le solicitará que confirme si desea marcar el registro como leído. Si confirma la operación, el número de alarmas que se muestran en la esquina superior derecha disminuye en 1. Haga clic en **Detalles** para mostrar los detalles de la alarma. Haga clic en **Eliminar** para eliminar este tipo de alarma.

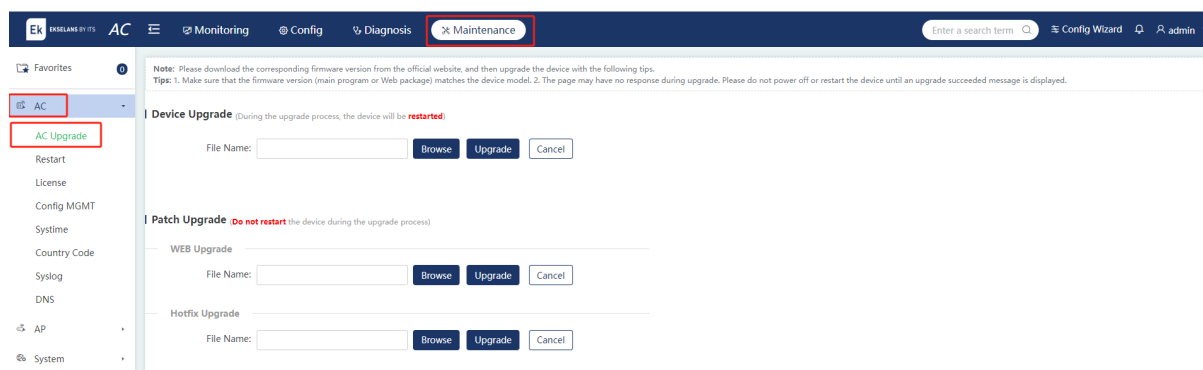
7 Mantenimiento

7.1 Gestión AC

7.1.1 Actualización de AC

Elija **Mantenimiento** > **Actualización de AC** > **AC**.

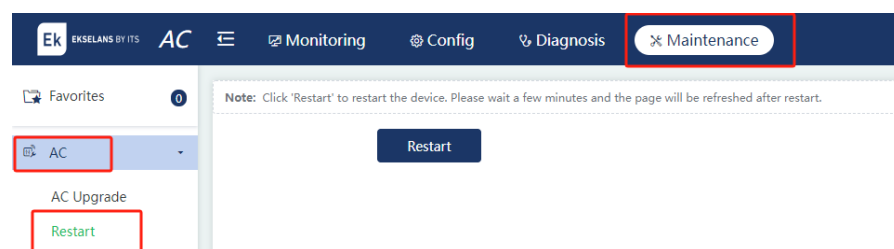
O elija **Actualización del sistema** > **Actualización de AC** en la barra de navegación para acceder rápidamente a la **página Actualización de AC**.



7.1.2 Reinicio de CA

Elija **Maintenance** > **AC** > **Reiniciar**.

Haga clic en **Reiniciar** para reiniciar el AC actual.

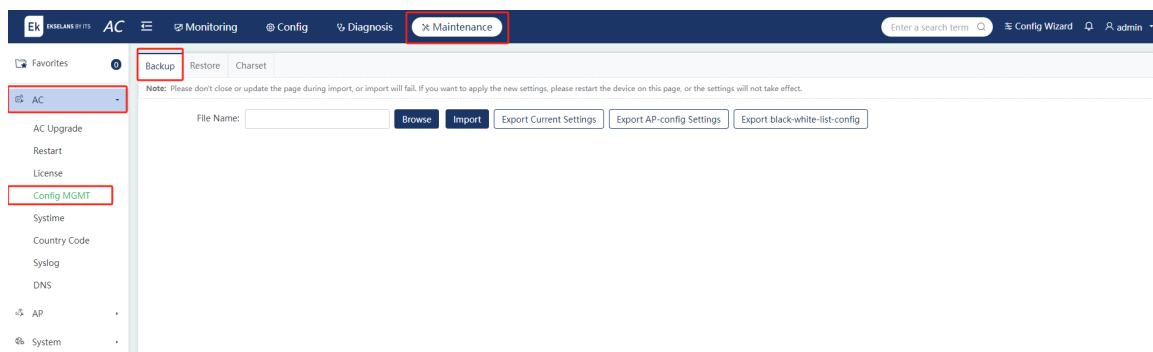


7.1.3 Gestión de la configuración

Seleccione **Maintenance** > **AC** > **Config MGMT**.

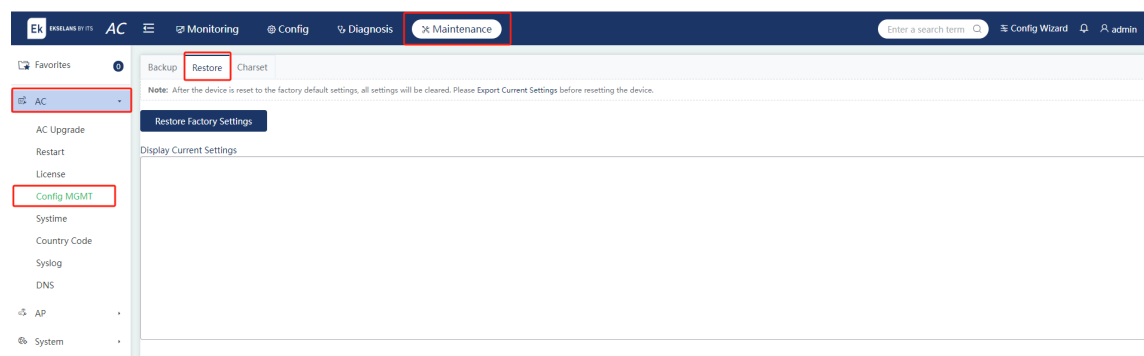
1. Copia de seguridad

Puede hacer una copia de seguridad del archivo de configuración en el dispositivo e importar o exportar configuraciones para realizar operaciones por lotes en las configuraciones, lo que facilita las operaciones del usuario.



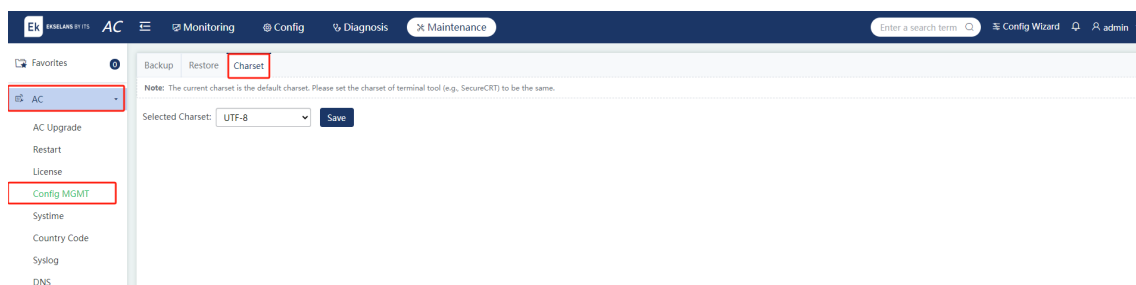
2. Restaurar

Puede borrar las configuraciones para restaurar el sistema al estado inicial. Debe utilizar la dirección IP en la configuración de fábrica para acceder al sistema web. Al restaurar la configuración de fábrica, se eliminarán todas las configuraciones. Por lo tanto, tenga cuidado al realizar esta operación.



3. Conjunto de caracteres

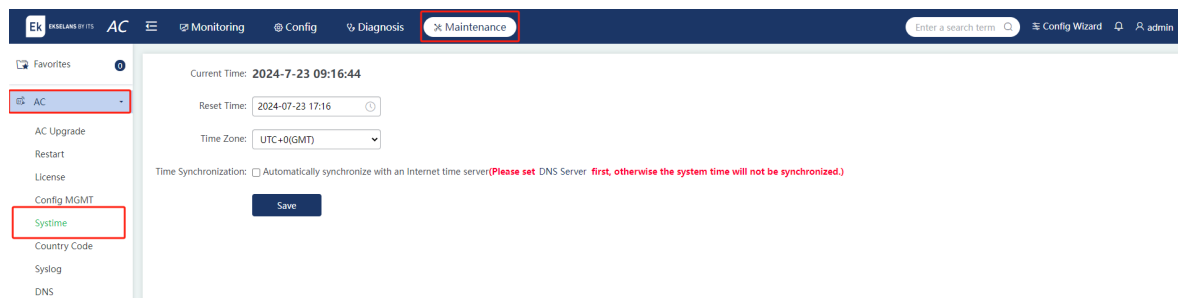
El conjunto de caracteres del sistema se puede establecer en GBK o UTF-8. El UTF-8 se utiliza para el sistema web de forma predeterminada. Se recomienda mantener el conjunto de caracteres del sistema en SecureCRT u otras herramientas cliente coherente con el conjunto de caracteres del sistema. De lo contrario, pueden aparecer caracteres ilegibles e híbridos.



7.1.4 Hora del sistema

Seleccione **Maintenance > AC > System**.

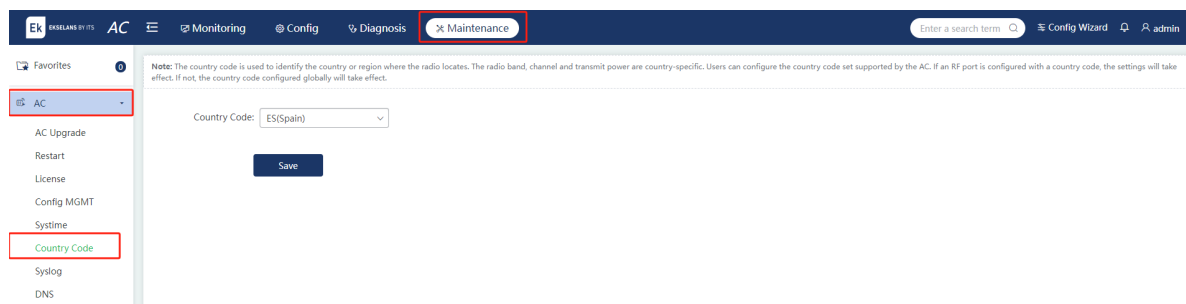
Puede establecer la hora del sistema de la zona horaria donde se encuentra el dispositivo para que la información del dispositivo sea precisa.



7.1.5 Código de país

Seleccione **Mantenimiento > AC > Código de país**.

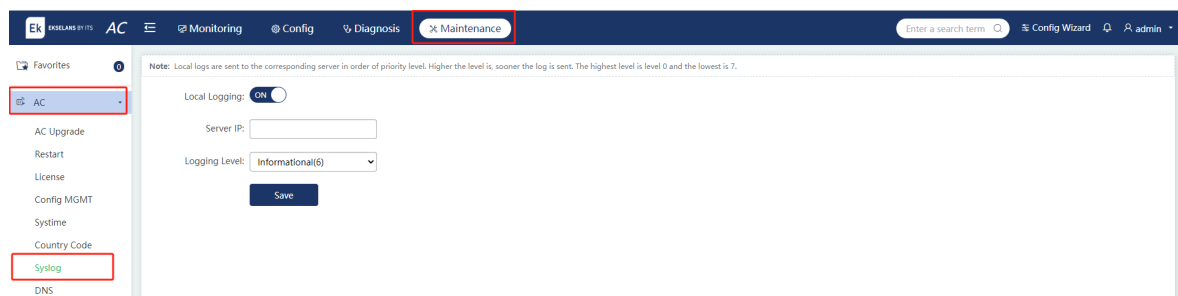
Puede establecer el país o la región donde se encuentra el dispositivo. La banda, el canal y la potencia de RF requeridos están sujetos a diferentes países o regiones.



7.1.6 Servidor de registro

Seleccione **Maintenance > AC > Syslog**.

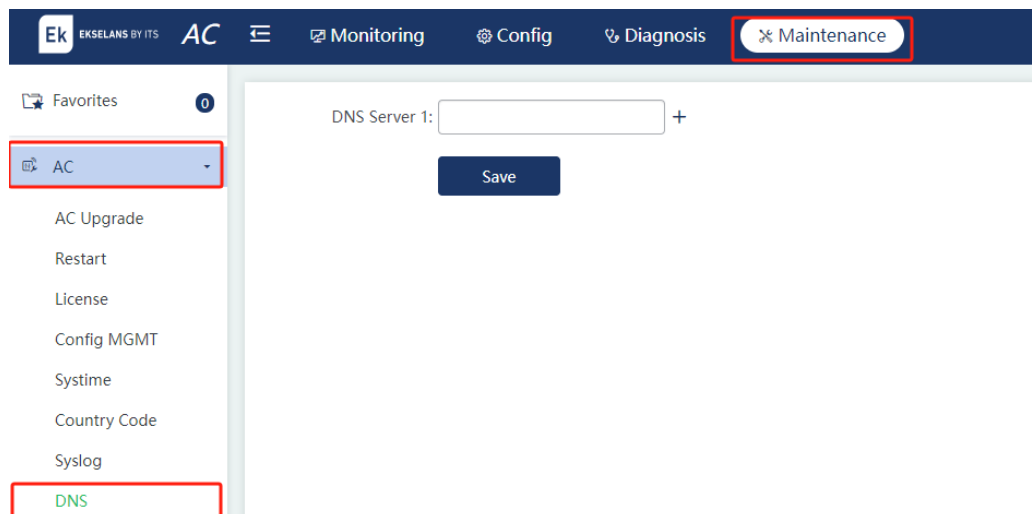
El dispositivo se puede configurar para enviar registros locales al servidor para su almacenamiento y fácil consulta.



7.1.7 DNS

Elija **Mantenimiento > AC > DNS**.

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

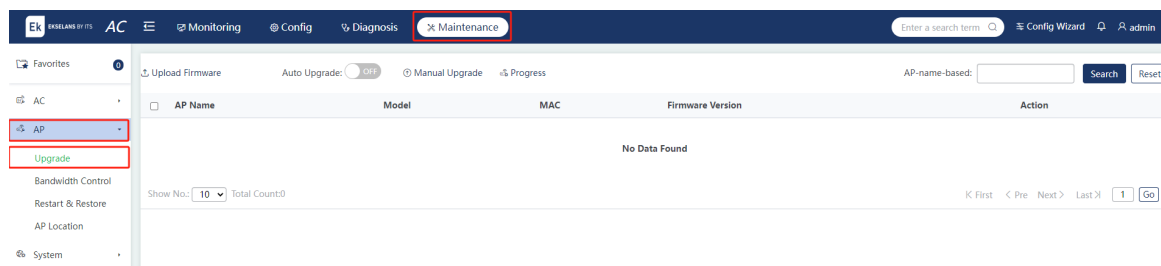


7.2 Gestión de AP

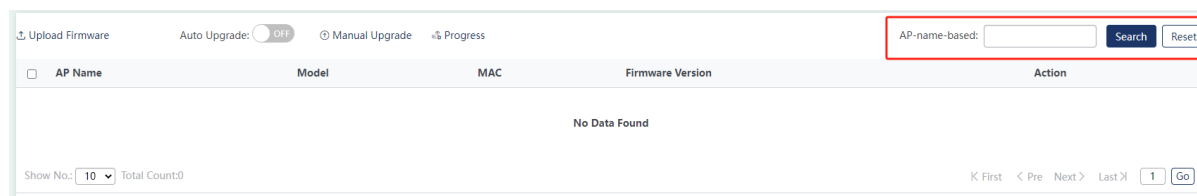
7.2.1 Actualización de AP

Seleccione **Mantenimiento > Actualización de > de AP**.

Se pueden administrar múltiples AP en el AC a través del sistema web, lo cual es rápido y conveniente.



- (1) Buscar un AP: Si hay muchos AP en la página, puede buscar un AP especificado por el nombre del AP en la esquina superior derecha de la página. Haga clic en **Restablecer** para borrar el contenido del cuadro de búsqueda.



- (2) Actualización automática: Puede activar la **actualización automática**. El AP se actualizará automáticamente a la última versión cuando esté disponible una versión posterior.

i Nota

Antes de actualizar los AP en el CA, asegúrese de que los AP puedan hacer ping entre sí. De lo contrario, se puede producir un error en la actualización distribuida, lo que puede prolongar el proceso de actualización.

- (3) Actualización de AP único: Haga clic en **Actualizar** junto a un AP. Cargue el archivo de actualización de AP y haga clic en **Actualizar**.
- (4) Actualización manual: haga clic en **Actualización manual** para acceder a la página **Actualización manual**.

Manual Upgrade ×

Serial: *
 Firmware: * Select firmware bin
 Model: * ?
 Hardware Version: * Enter a hardware version

Series	Model	Firmware Version	Hardware Version	Action
No Data Found				

Show No.: Total Count:0

 K First < Pre Next > Last X 1

7.2.2 Control de ancho de banda

Elija **Mantenimiento > AP > Control de ancho de banda**.

Al configurar el grupo de actualización y limitar el ancho de banda de actualización, se reserva suficiente ancho de banda cuando se actualiza el AP, de modo que el rendimiento de la red no se vea afectado en gran medida por la actualización del AP.

EK EKSELANS BY ITS AC
 Monitoring
Config
Diagnosis
Maintenance
Enter a search term
Config Wizard
admin

Favorites

- AC
- AP
- Upgrade
- Bandwidth Control
- Restart & Restore
- AP Location
- System

Note: To configure upgrade groups and limit upgrade bandwidth leaves sufficient bandwidth for AP upgrade and smooth service.

+ Add Upgrade Group X Delete Selected

Upgrade Group Name	Member AP	Action
No Data Found		

Show No.: Total Count:0

 K First < Pre Next > Last X 1

- (1) Agregar un grupo de actualización: haz clic en **Agregar grupo de actualización**. Edite los campos en el cuadro de diálogo emergente. Haga clic en **Guardar**. Se muestra un mensaje que indica que la configuración se ha guardado. El grupo de actualización recién agregado se muestra en la lista de grupos de actualización.

Note: To configure upgrade groups and limit upgrade bandwidth leaves sufficient bandwidth for AP upgrade and smooth service.

+ Add Upgrade Group X Delete Selected

Upgrade Group Name	Member AP	Action
No Data Found		

Show No: 10 Total Count: 0

Add Upgrade Group

Upgrade Group Name:

Concurrent APs: * Range: 0-200

Upgrade Bandwidth(kB): * Range: 8-10240

Member AP:

Cancel Save

K First < Pre Next > Last 1 Go

Parámetro	Descripción
Nombre del grupo de actualización	Especifica el nombre de un nombre de grupo de actualización.
AP concurrentes	Especifica el número de AP que se actualizan simultáneamente.
Ancho de banda de actualización (kB)	Especifica el ancho de banda para la actualización de AP.
Miembro AP	Especifica los AP miembros en el grupo de actualización.

- Eliminar un grupo de actualización: haz clic en **Eliminar** junto a un grupo de actualización. Haga clic en **Aceptar** en el cuadro de diálogo emergente.
- Editar un grupo de actualización: haz clic en **Editar** junto a un grupo de actualización. El cuadro de diálogo emergente muestra la información sobre el grupo de actualización. Puede editar la información. Haga clic en **Guardar**. Se muestra un mensaje que indica que la configuración se ha guardado.

7.2.3 Reinicio/restauración de AP

Elija **Mantenimiento > AP > Reiniciar y restaurar**.

Reinicie los AP en línea o restáurelos a la configuración de fábrica.

Ek EKSELANS BY ITS AC Monitoring Config Diagnosis Maintenance

Note: You can restart the online AP or restore the online AP to factory settings.

Restart AP Restore Factory Settings

AP-name-based Search Reset

AP Name	AP Group	IP	MAC	Status	Action
No Data Found					

Show No: 10 Total Count: 0

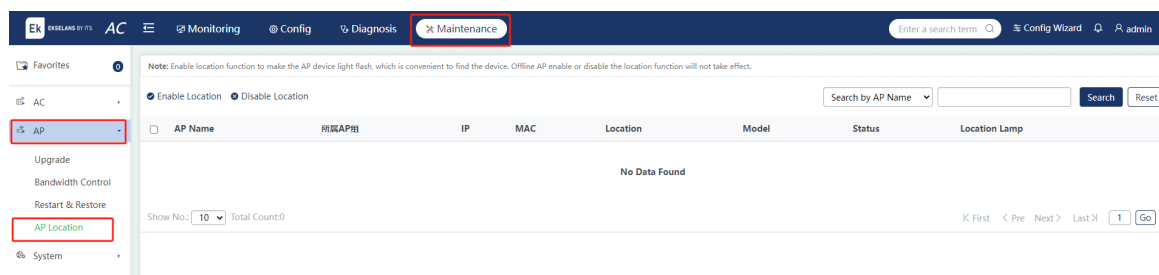
K First < Pre Next > Last 1 Go

- (1) Reiniciar el AP: Haga clic en **Reiniciar AP** junto a un AP. Si es necesario reiniciar varios AP, seleccione los AP y haga clic en **Reiniciar AP**.
- (2) Restaurar la configuración de fábrica: Haga clic en **Restaurar la configuración de fábrica** junto a un AP. Si es necesario restaurar varios AP a la configuración de fábrica, seleccione los AP y haga clic en **Restaurar configuración de fábrica**.

7.2.4 Ubicación de AP

Seleccione **Mantenimiento > AP > Ubicación de AP**.

Cuando la función de ubicación de AP está habilitada, el LED del sistema en el AP parpadea para ayudar a localizar el AP. Si un AP se desconecta, fallará un intento de habilitar o deshabilitar la ubicación del AP.



Habilitar/deshabilitar la ubicación del AP: Haga clic en el icono de ubicación junto a un AP para habilitar/deshabilitar la función de ubicación del AP. Si la función de ubicación de AP debe habilitarse/deshabilitarse para varios AP, seleccione los AP y haga clic en **Habilitar ubicación** **Deshabilitar ubicación**.

7.3 Sistema

7.3.1 Gestión Web

Seleccione **Mantenimiento > Gestión de > Web del sistema**.

1. Contraseña de administrador

Para mejorar la seguridad del sistema y la seguridad de la interacción con la información, se recomienda cambiar la contraseña predeterminada del sistema.

Ek EKSELANS BY ITS AC Monitoring Config Diagnosis Maintenance

Favorites 0

AC

AP

System

Web Management

Telnet

Web Console

Open API

SNMP

CWMP

Admin Password Basic Settings Permissions webAcl Web Logo

Username: admin

Old Password: *

New Password: *

Confirm Password: *

Save

2. Ajustes básicos

Para facilitar la administración del dispositivo, puede introducir la ubicación del dispositivo en la **página Configuración básica**. Establezca los valores de Puerto de **acceso web** y **Tiempo de espera de inicio de sesión**. Cuando se agote el tiempo de espera del inicio de sesión, la página web se cerrará automáticamente. Si el dispositivo admite el límite de inicio de sesión, puede establecer el número máximo de usuarios que pueden iniciar sesión en el dispositivo simultáneamente con la misma cuenta (el número máximo predeterminado es 10).

Ek EKSELANS BY ITS AC Monitoring Config Diagnosis Maintenance

Favorites 0

AC

AP

System

Web Management

Telnet

Web Console

Open API

SNMP

CWMP

Admin Password Basic Settings Permissions webAcl Web Logo

Web Access Port: 443 * (Range: 443,1025-65535)

Login Timeout: 30 min

Device Location:

Access Redirection: ☒ HTTP Redirection to HTTPS In NAT scenario, redirection may cause HTTP access failure.

Save

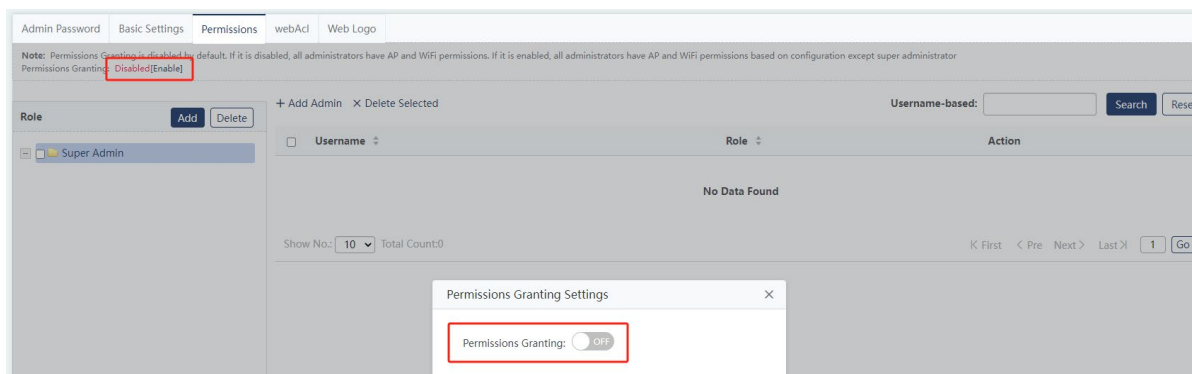
3. Permisos

Pueden existir varios administradores en un sistema. Los administradores de diferentes niveles tienen diferentes permisos de administración. El usuario predeterminado del sistema es **admin**.

- (1) Permisos de administrador (gestión jerárquica y descentralizada): pueden existir varios usuarios en un sistema y los usuarios se pueden agrupar. Se pueden conceder diferentes grupos de

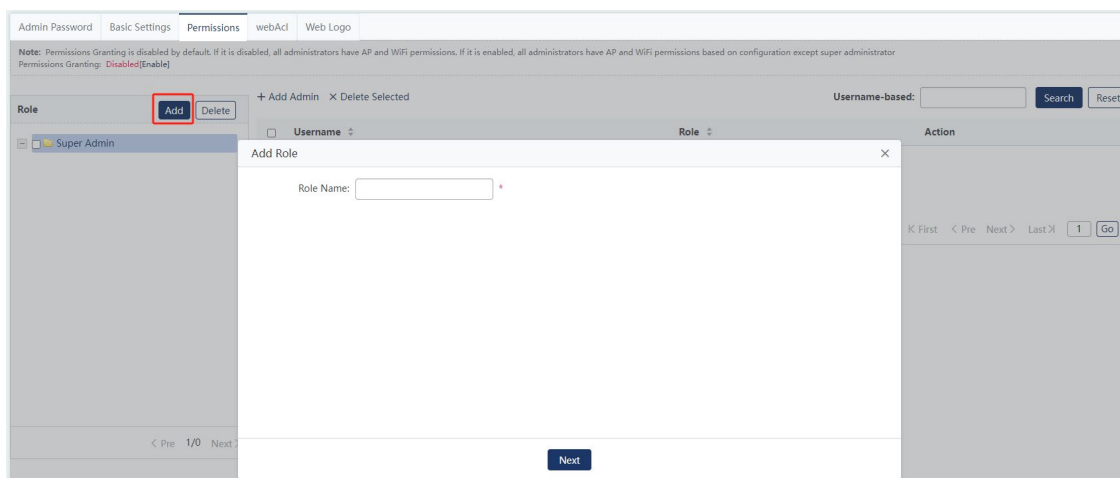
usuarios con diferentes permisos para WLAN, AP y grupos de AP, de modo que los usuarios de diferentes grupos tengan diferentes permisos para WLAN, AP y grupos de AP.

Habilitar/deshabilitar la administración jerárquica y descentralizada: Para habilitar la función jerárquica y descentralizada, active el interruptor.

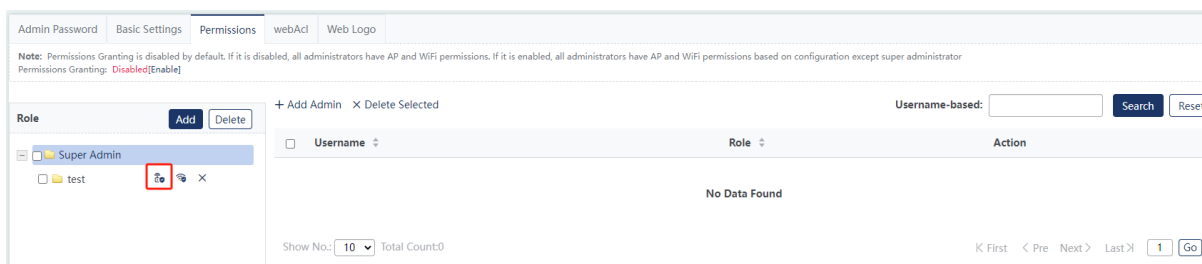


Agregar una función: La adición de una función incluye tres pasos: adición de funciones, autorización de AP y autorización de Wi-Fi. Puede asignar permisos a un rol a la vez.

Los administradores comunes que pertenezcan a este rol tendrán todos los permisos de AP y Wi-Fi para este rol. No tienen permisos para otros AP y redes Wi-Fi a los que no puede acceder este rol.



Conceder permisos de AP:



Roletest Grant AP Permissions

Note: If you want to edit or add an AP/AP group, please go to AP Settings

AP Group Name: All AP Groups

Grant AP Permissions Revoke

Search by AP Name Search Reset

AP Name	IP	MAC	Permissions Granted	Action
No Data Found				

Show No: 15 Total Count: 0

K First < Pre Next > Last 1 Go

Otorgar permisos de Wi-Fi:

Admin Password Basic Settings Permissions webAc Web Logo

Note: Permissions Granting is disabled by default. If it is disabled, all administrators have AP and WiFi permissions. If it is enabled, all administrators have AP and WiFi permissions based on configuration except super administrator

Permissions Granting: Disabled Enable

Role Add Delete

+ Add Admin X Delete Selected

Username-based: Search Reset

Username	Role	Action
No Data Found		

Show No: 10 Total Count: 0

K First < Pre Next > Last 1 Go

Roletest Grant WiFi Permissions

Note: If you need to add a WiFi, please go to WLAN/WiFi Settings

Grant WiFi Permissions Revoke

SSID-based: Search Reset

SSID	Permissions Granted	Action
No Data Found		

Show No: 15 Total Count: 0

K First < Pre Next > Last 1 Go

4. Gestión de permisos de acceso web

Esta función se utiliza para administrar los permisos de inicio de sesión para el sistema web. Cuando la opción **Denegar acceso a la web** está habilitada, no se puede iniciar sesión en el sistema web.

Ek EKSELANS BY ITS AC Monitoring Config Diagnosis Maintenance

Admin Password Basic Settings Permissions webAc Web Logo

Note: If you enable this feature, all clients except those in the network whitelist will be denied access to Web. Please verify the settings.

Deny Access to Web: OFF

Save

System

Web Management

Telnet

Web Console

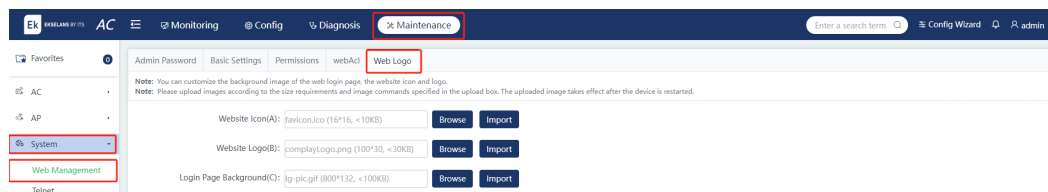
Open API

SNMP

CWMP

5. Logotipo web

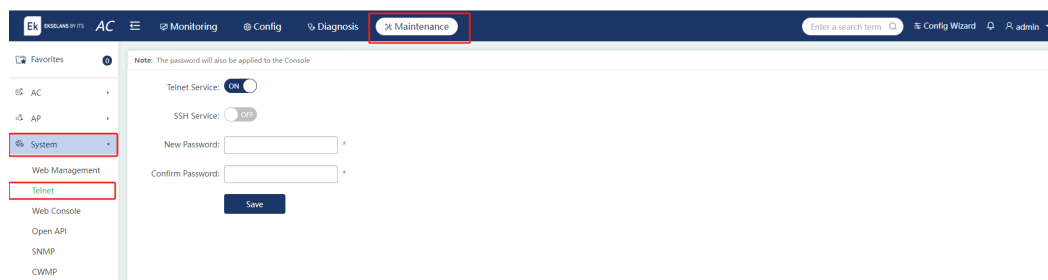
Con esta función, puede personalizar la página de inicio de sesión del sistema web y el logotipo en la esquina superior izquierda del menú.



7.3.2 Telnet

Seleccione **Mantenimiento > Sistema > Telnet**.

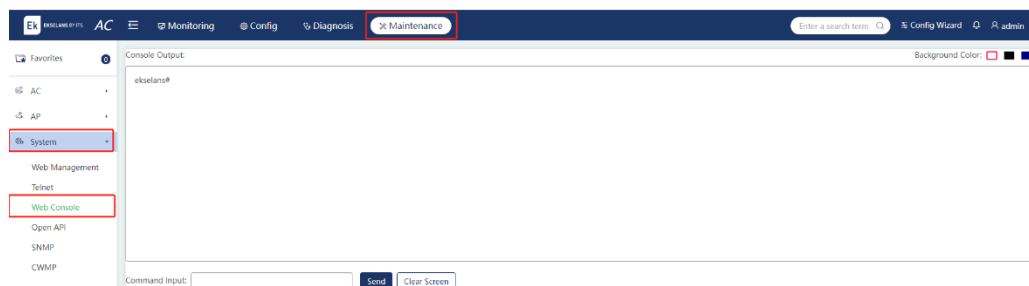
La función Telnet mejora la seguridad del sistema y la seguridad de la interacción de la información. Los servicios Telnet y SSH se pueden habilitar/deshabilitar y la contraseña se puede configurar en la página de configuración de Telnet.



7.3.3 Consola web

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

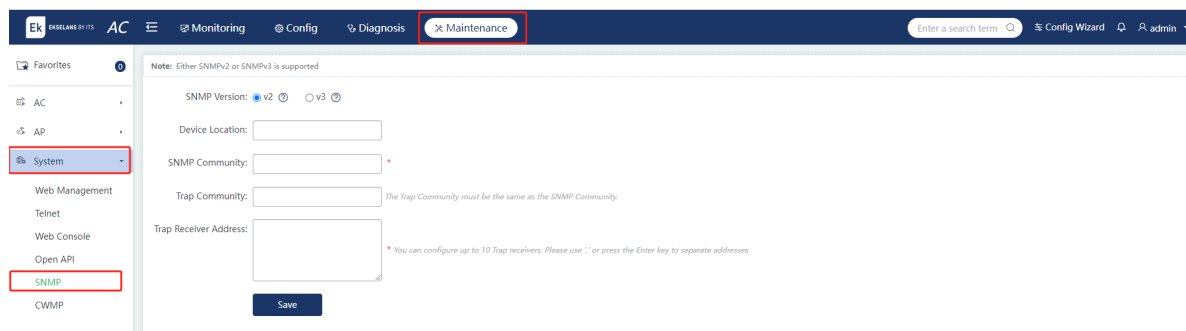
Puede enviar comandos CLI a través de la consola web.



7.3.4 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. Se puede utilizar para administrar una gran cantidad de dispositivos de red.



7.3.5 CWMP (en inglés)

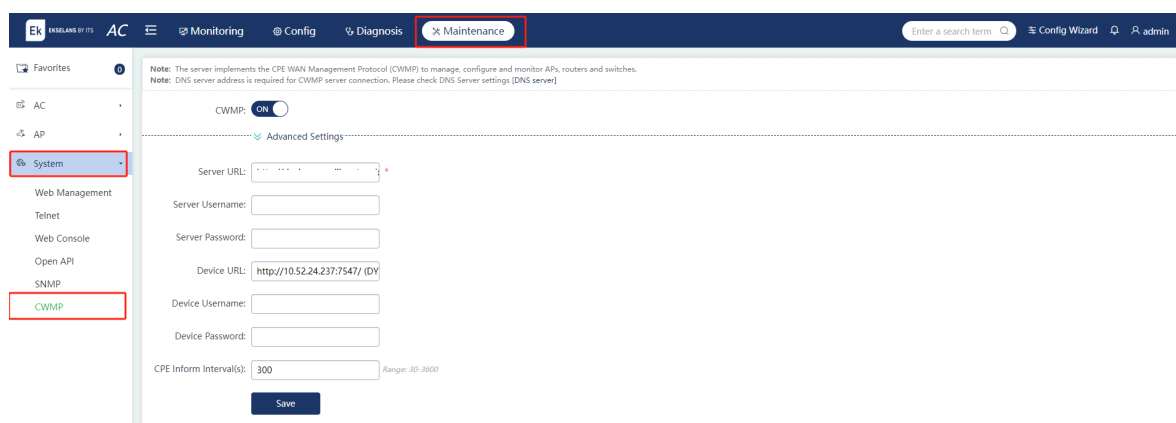
Seleccione **Mantenimiento > Sistema > CWMP**.

El protocolo CWMP es el protocolo de administración de WAN de CPE. El servidor puede administrar, configurar y monitorear dispositivos como CA, AP o conmutadores a través de este protocolo.

A través de la configuración, el dispositivo se puede conectar y administrar mediante una plataforma en la nube u otros servidores.

Nota

Al conectarse a un servidor a través del protocolo CWMP, debe configurar el servidor DNS correcto para que el dispositivo pueda resolver correctamente el nombre de dominio del servidor. Por lo tanto, compruebe si el servidor DNS está configurado correctamente.



Parámetro	Descripción
CWMP (en inglés)	El switch CWMP se utiliza para

	habilitar/deshabilitar la función CWMP.
URL del servidor	Especifica la dirección IP del servidor.
Nombre de usuario del servidor	Especifica el nombre de usuario del servidor, que se puede utilizar para la verificación.
Contraseña del servidor	Especifica la contraseña del servidor, que se puede utilizar para la verificación.
URL del dispositivo	Especifica la URL del dispositivo, que se puede utilizar para conectarse activamente al servidor en la misma LAN.
Nombre de usuario del dispositivo	Especifica el nombre de usuario del dispositivo, que se puede utilizar para la verificación.
Contraseña del dispositivo	Especifica la contraseña del dispositivo, que se puede utilizar para la verificación.
Intervalo(s) de información de CPE	Especifica el intervalo para conectarse al servidor, es decir, el intervalo de los paquetes de latidos.