Configuración de RADIUS en el punto de acceso inalámbrico Cisco Business

Objetivo

El objetivo de este documento es mostrarle cómo configurar RADIUS en el punto de acceso (AP) Cisco Business Wireless (CBW).

Dispositivos aplicables | Versión del firmware

- 140AC (Ficha técnica) | 10.4.1.0 (Descargar última)
- 145AC (Ficha técnica) | 10.4.1.0 (Descargar última)
- 240AC (Ficha técnica) | 10.4.1.0 (última descarga)

Introducción

Si desea configurar RADIUS en su CBW AP, ha llegado al lugar correcto. Los puntos de acceso CBW admiten el último estándar 802.11ac Wave 2 para redes de mayor rendimiento, mayor acceso y mayor densidad. Ofrecen un rendimiento líder del sector con conexiones inalámbricas muy seguras y fiables, lo que ofrece una experiencia de usuario final sólida y móvil.

El servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un mecanismo de autenticación para que los dispositivos se conecten y utilicen un servicio de red. Se utiliza para fines de autenticación, autorización y contabilidad centralizados. Un servidor RADIUS regula el acceso a la red mediante la verificación de la identidad de los usuarios a través de las credenciales de inicio de sesión introducidas. Por ejemplo, una red Wi-Fi pública se instala en un campus universitario. Sólo los alumnos que tienen la contraseña pueden acceder a estas redes. El servidor RADIUS verifica las contraseñas introducidas por los usuarios y concede o deniega el acceso a la red de área local inalámbrica (WLAN) según corresponda.

Si está listo para configurar RADIUS en su CBW AP, ¡empecemos!

Table Of Contents

Configure RADIUS en su punto de acceso CBW

Esta sección alterada resalta consejos para principiantes.

Conexión

Inicie sesión en la interfaz de usuario web (IU) del AP principal. Para ello, abra un navegador web e introduzca https://ciscobusiness.cisco. Puede recibir una advertencia antes de continuar. Ingrese sus credenciales.También puede acceder al AP principal ingresando https://[ipaddress] (del AP principal) en un navegador web.

Consejos sobre herramientas

Si tiene preguntas sobre un campo en la interfaz de usuario, busque una sugerencia de herramienta que tenga el siguiente aspecto:

¿Desea localizar el icono Expandir menú principal?

Desplácese hasta el menú situado en la parte izquierda de la pantalla, si no ve el botón de menú, haga clic en este icono para abrir el menú de la barra lateral.

Aplicación empresarial de Cisco

Estos dispositivos tienen aplicaciones complementarias que comparten algunas funciones de gestión con la interfaz de usuario web. No todas las funciones de la interfaz de usuario Web estarán disponibles en la aplicación.

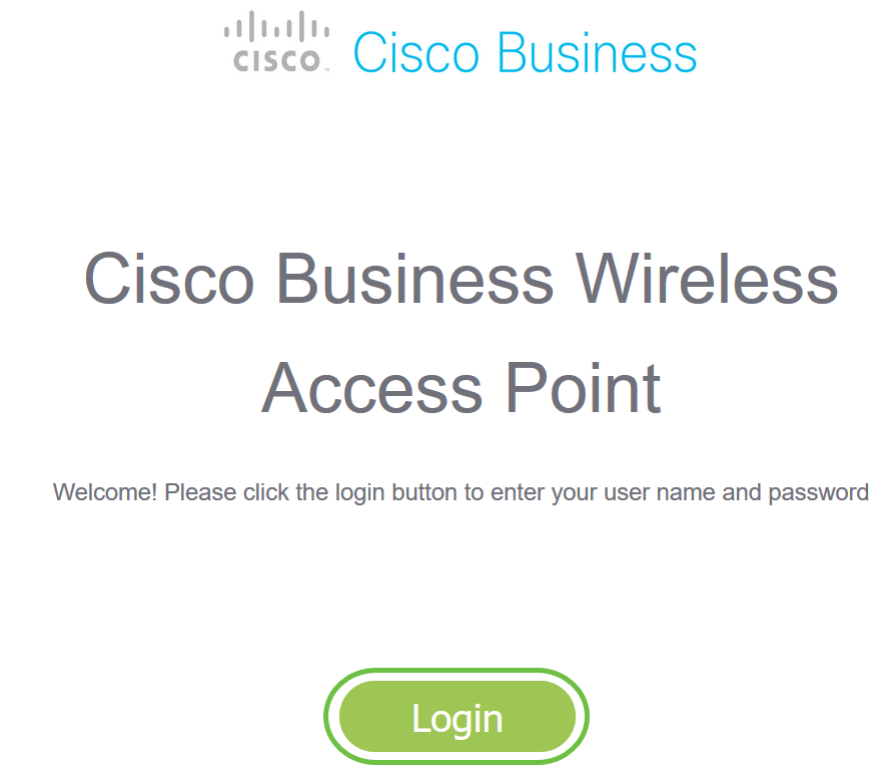
Descargar aplicación iOS Descargar la aplicación Android

Preguntas Frecuentes

Si todavía tiene preguntas sin responder, puede consultar nuestro documento de preguntas frecuentes. Preguntas frecuentes

Paso 1

Inicie sesión en su CBW AP usando un nombre de usuario y una contraseña válidos.

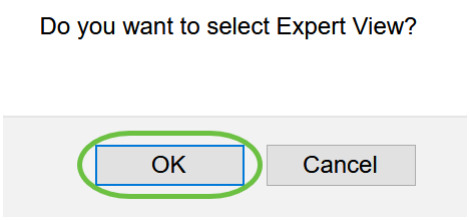


Paso 2

Haga clic en el símbolo de **flecha bidireccional** en la parte superior de la interfaz de usuario web

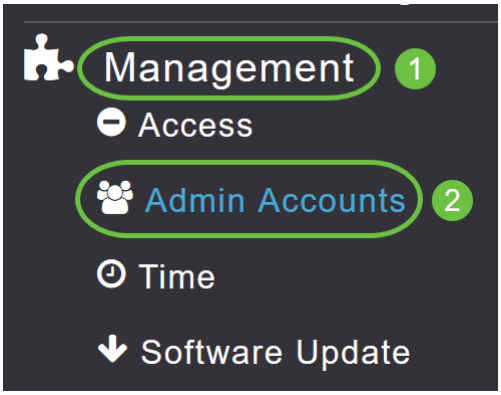
para *cambiar a la vista de expertos*.

Aparecerá la siguiente pantalla emergente. Haga clic en **Aceptar** para continuar.



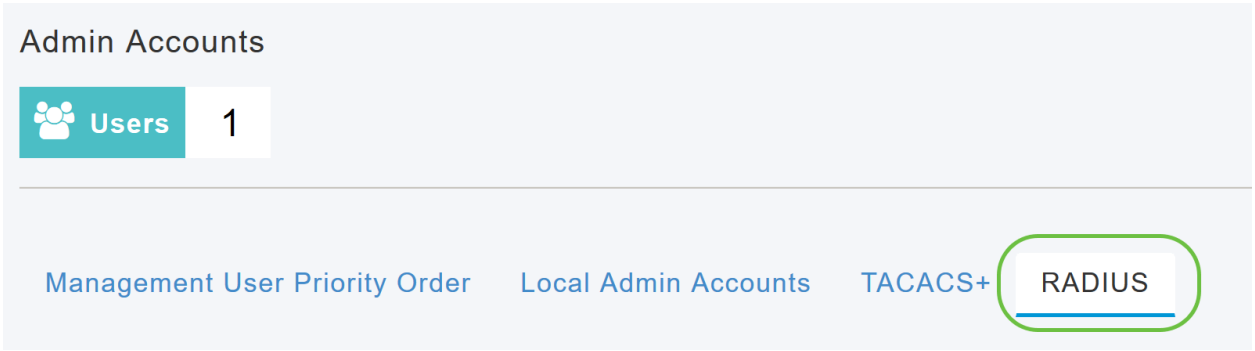
Paso 3

Vaya a **Administración > Cuentas de administración**.



Paso 4

Para agregar los servidores RADIUS, haga clic en la pestaña **RADIUS**.

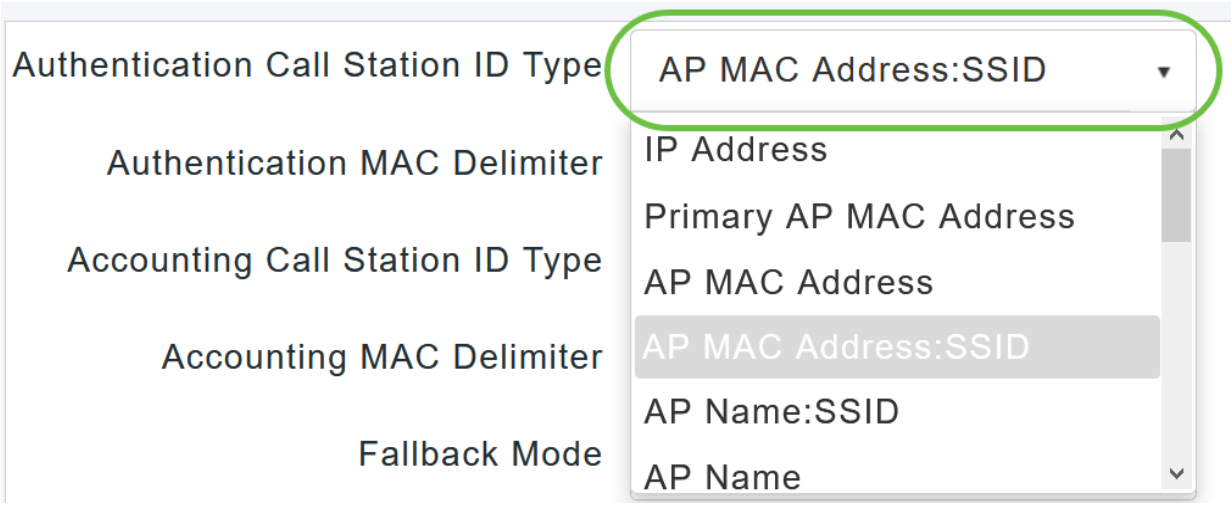


Paso 5

En la lista desplegable *Authentication Call Station ID Type* , elija la opción que se envía al servidor RADIUS en el mensaje Access-Request . Las opciones disponibles son las siguientes:

- *IP Address*

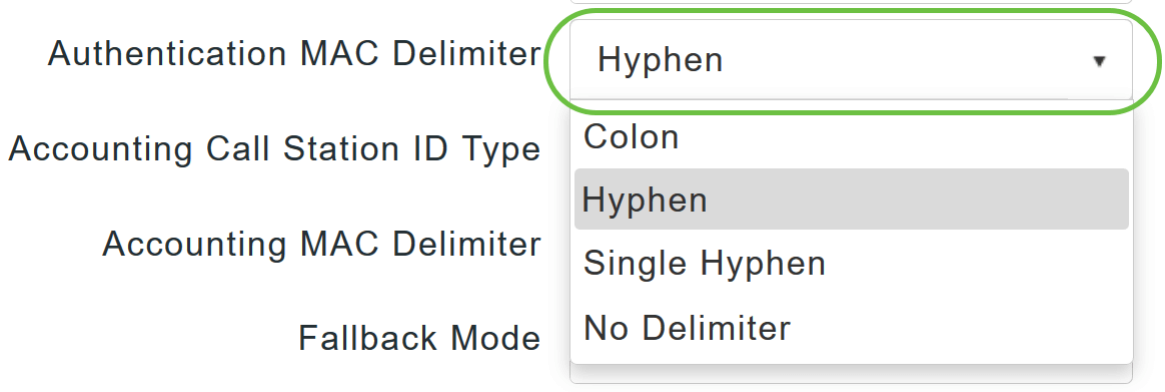
- *Dirección MAC del AP principal*
- *Dirección MAC de AP*
- *Dirección MAC de punto de acceso:SSID*
- *Nombre de AP:SSID*
- *Nombre de AP*
- *Grupo AP*
- *Grupo Flex*
- *Ubicación de AP*
- *ID DE VLAN*
- *Dirección MAC Ethernet AP*
- *Dirección MAC Ethernet AP:SSID*
- *Dirección de la etiqueta AP*
- *Dirección de etiqueta de punto de acceso:SSID*
- *MAC de punto de acceso:grupo de punto de acceso SSID*
- *AP Eth MAC:SSID AP Group*



Paso 6

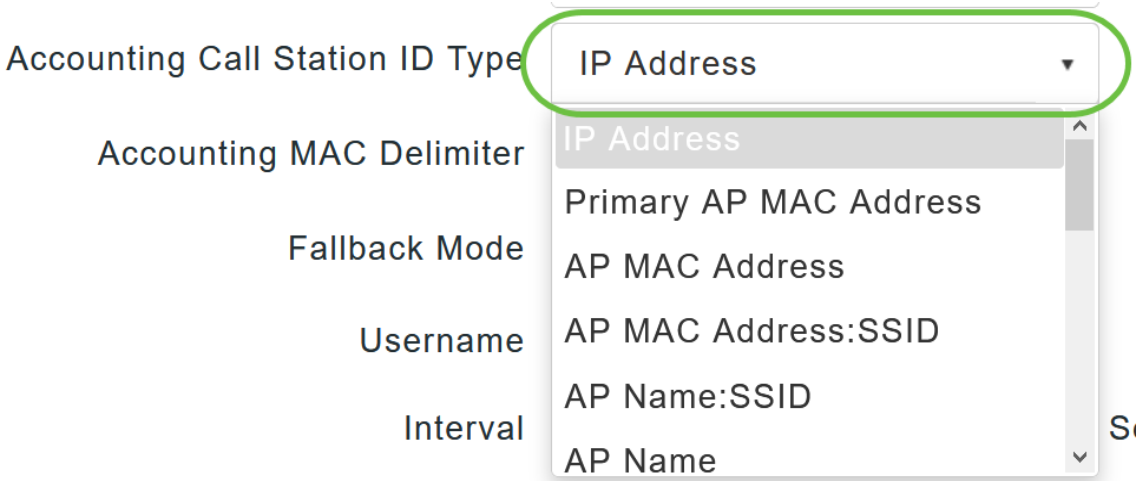
Seleccione *Authentication MAC Delimiter* en la lista desplegable. Las opciones son:

- *Colón*
- *Guión*
- *Un solo guión*
- *Sin delimitador*



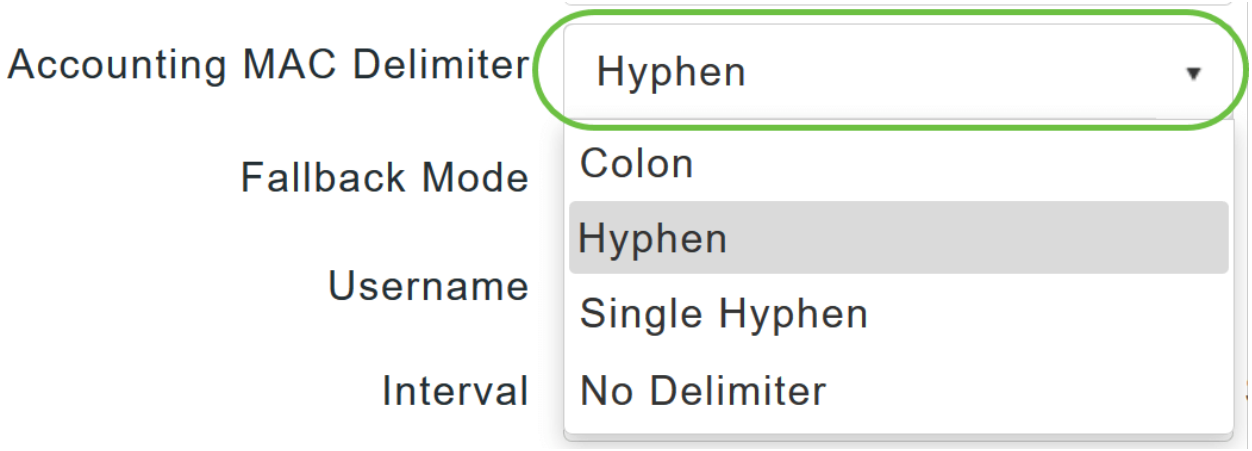
Paso 7

Elija el *Tipo de ID de estación de llamadas de contabilidad* de la lista desplegable.



Paso 8

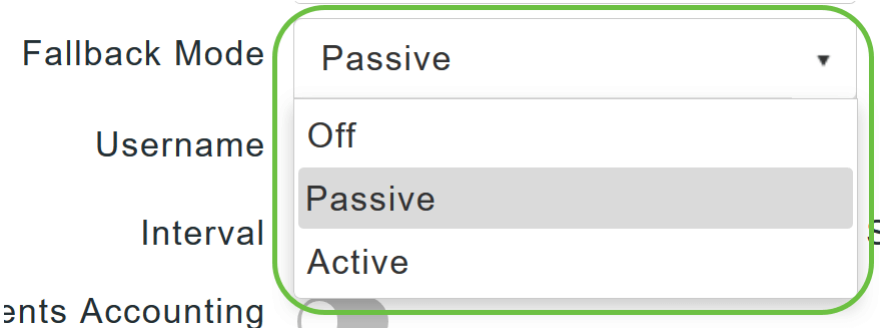
Elija el *Delimitador MAC de Contabilización* de la lista desplegable.



Paso 9

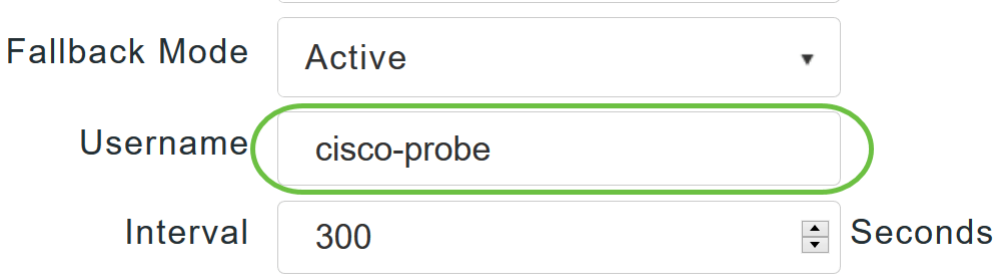
Especifique el *modo de reserva* del servidor RADIUS de la lista desplegable. Puede ser una de las siguientes:

- *Off* - Inhabilita la reserva del servidor RADIUS. Este es el valor predeterminado.
- *Pasivo* - Hace que el AP primario regrese a un servidor con una prioridad menor de los servidores de respaldo disponibles sin usar mensajes de sonda extraños. El AP primario ignora todos los servidores inactivos durante un período de tiempo y reintenta más tarde cuando se necesita enviar un mensaje RADIUS.
- *Activo* - Hace que el AP primario regrese a un servidor con una prioridad menor de los servidores de respaldo disponibles usando los mensajes de sonda RADIUS para determinar proactivamente si un servidor que ha sido marcado como inactivo está nuevamente en línea. El AP primario ignora todos los servidores inactivos para todas las solicitudes RADIUS activas. Una vez que el servidor primario recibe una respuesta del servidor ACS recuperado, el servidor RADIUS de retorno activo ya no envía mensajes de sonda al servidor que solicita la autenticación de sonda activa.



Paso 10

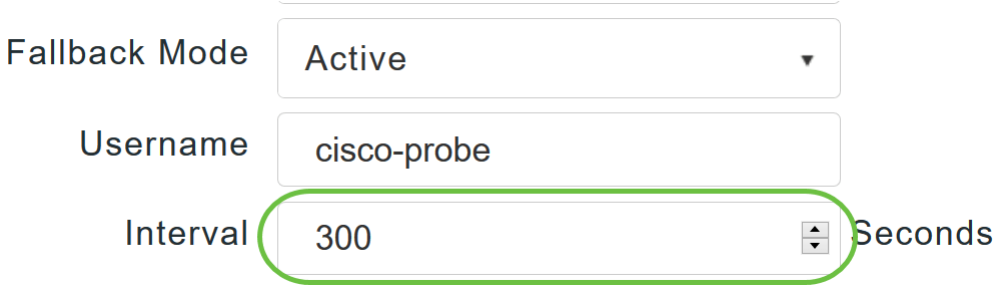
Si ha habilitado el *modo de reserva activa*, introduzca el nombre que se enviará en las sondas de servidor inactivas en el campo *Nombre de usuario*.



Puede introducir hasta 16 caracteres alfanuméricos. El valor predeterminado es **cisco-probe**.

Paso 11

Si ha activado el *modo de reserva activa*, introduzca el valor del intervalo de sonda (en segundos) en el campo Intervalo. El intervalo funciona como tiempo inactivo en modo pasivo e intervalo de sonda en modo activo.

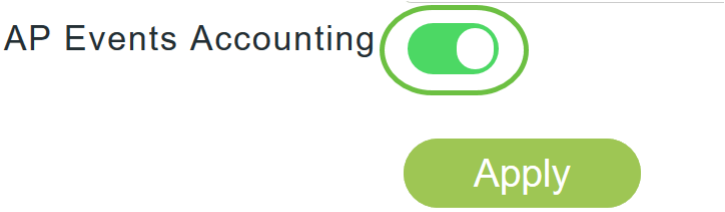


El rango válido es de 180 a 3600 segundos y el valor predeterminado es **300** segundos.

Paso 12

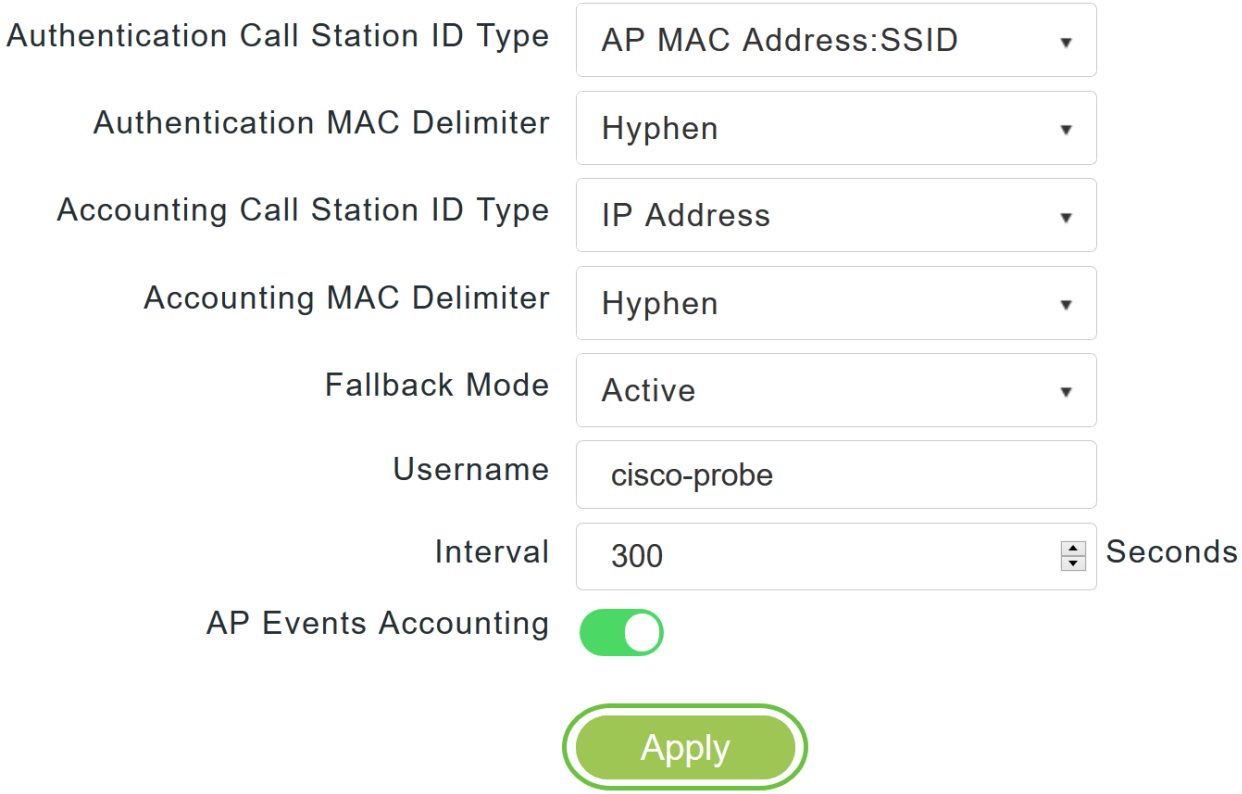
Habilite el botón deslizante *AP Events Accounting* para activar el envío de solicitudes de contabilización al servidor RADIUS.

Durante los problemas de red, los AP se unen/se desconectan del AP primario. Al activar esta opción, se garantiza que estos eventos se supervisan y que las solicitudes de contabilización se envían al servidor RADIUS para ayudarle a detectar los problemas de red.



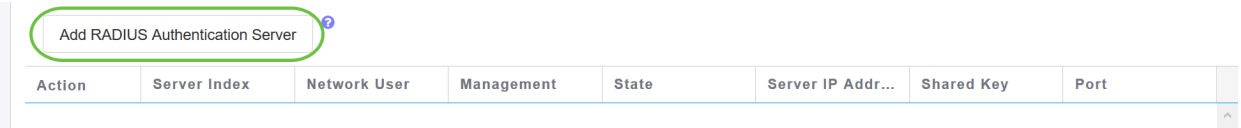
Paso 13

Haga clic en Apply (Aplicar).



Paso 14

Para configurar el servidor de autenticación RADIUS, haga clic en **Agregar servidor de autenticación RADIUS**.



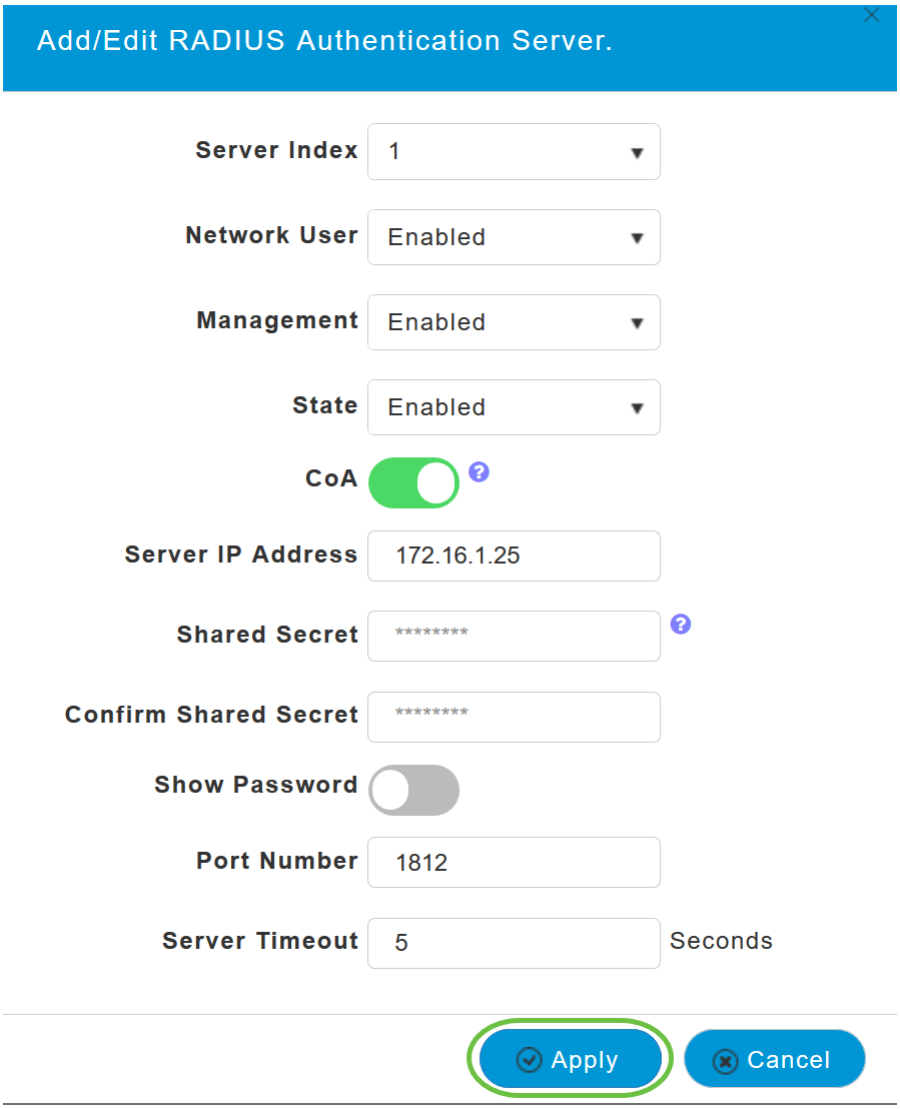
Paso 15

En la ventana emergente *Agregar/Editar autenticación RADIUS*, configure lo siguiente:

- *Índice de servidores*: seleccione de 1 a 6
- *Usuario de red*: active el estado. De forma predeterminada, está activado
- *Administración*: habilita el estado. De forma predeterminada, está activado
- *Estado*: habilita el estado. De forma predeterminada, está activado
- *CoA*: puede activar esta opción moviendo el botón del control deslizante
- *Dirección IP del servidor*: introduzca la dirección IPv4 del servidor RADIUS

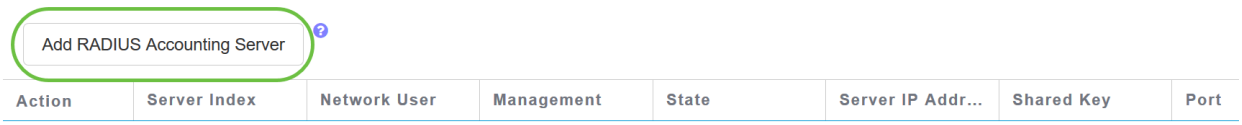
- *Secreto compartido*: introduzca el secreto compartido
- *Número de puerto*: introduzca el número de puerto que se utiliza para comunicarse con el servidor RADIUS.
- *Tiempo de espera del servidor*: introduzca el tiempo de espera del servidor

Haga clic en Apply (Aplicar).



Paso 16

Para agregar *RADIUS Accounting Server*, seguiría los mismos pasos que en el Paso 15, ya que la página contiene campos similares.

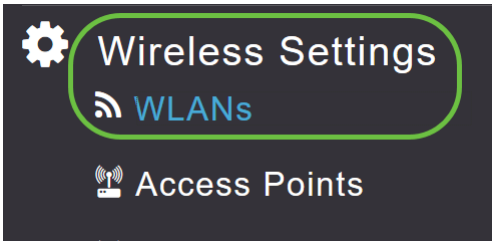


Configuración de WLAN

Paso 1

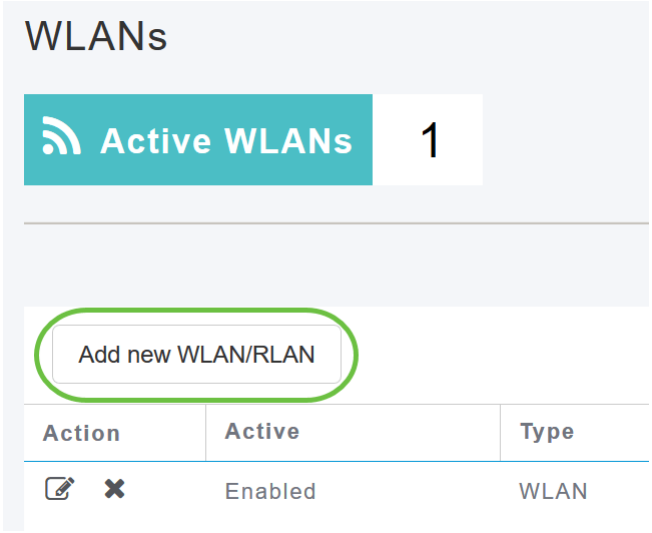
Para configurar la WLAN que va a manejar la autenticación WPA2 con RADIUS, navegue hasta

Wireless settings > WLAN.



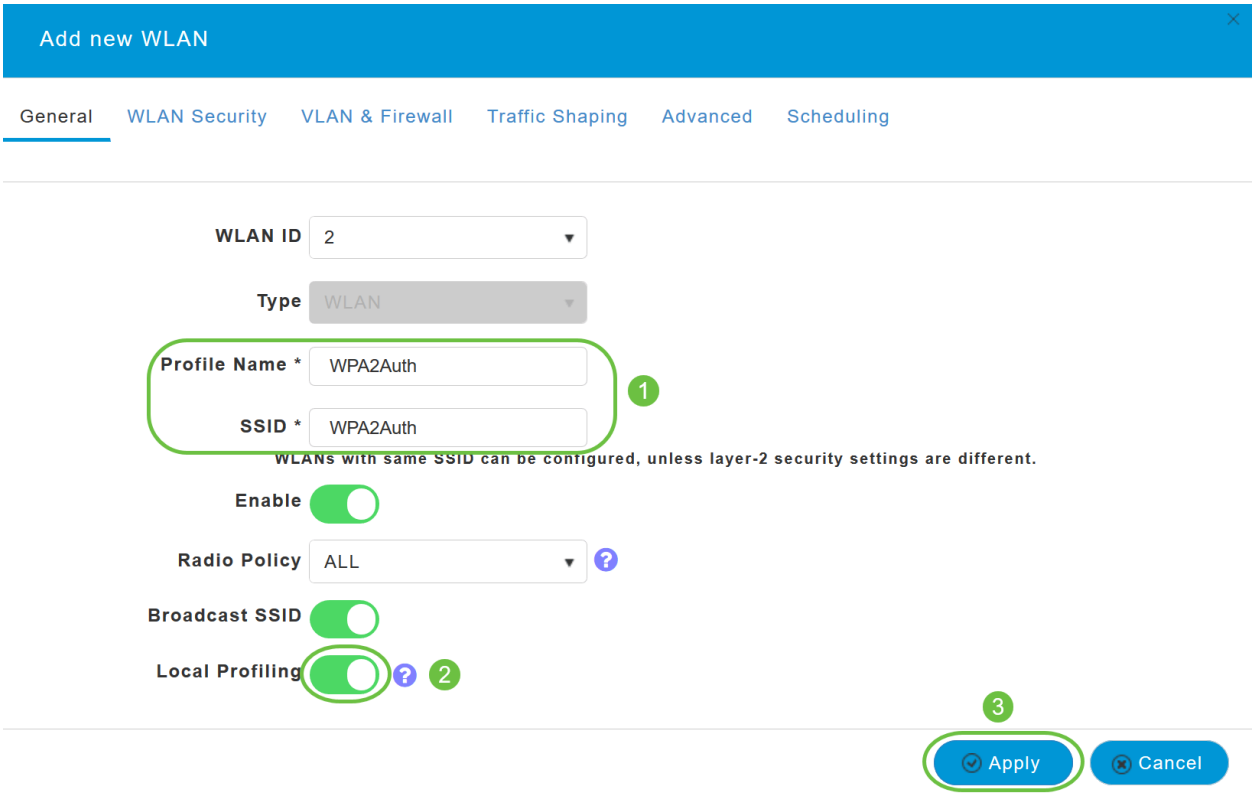
Paso 2

Haga clic en **Add New WLAN/RLAN**.



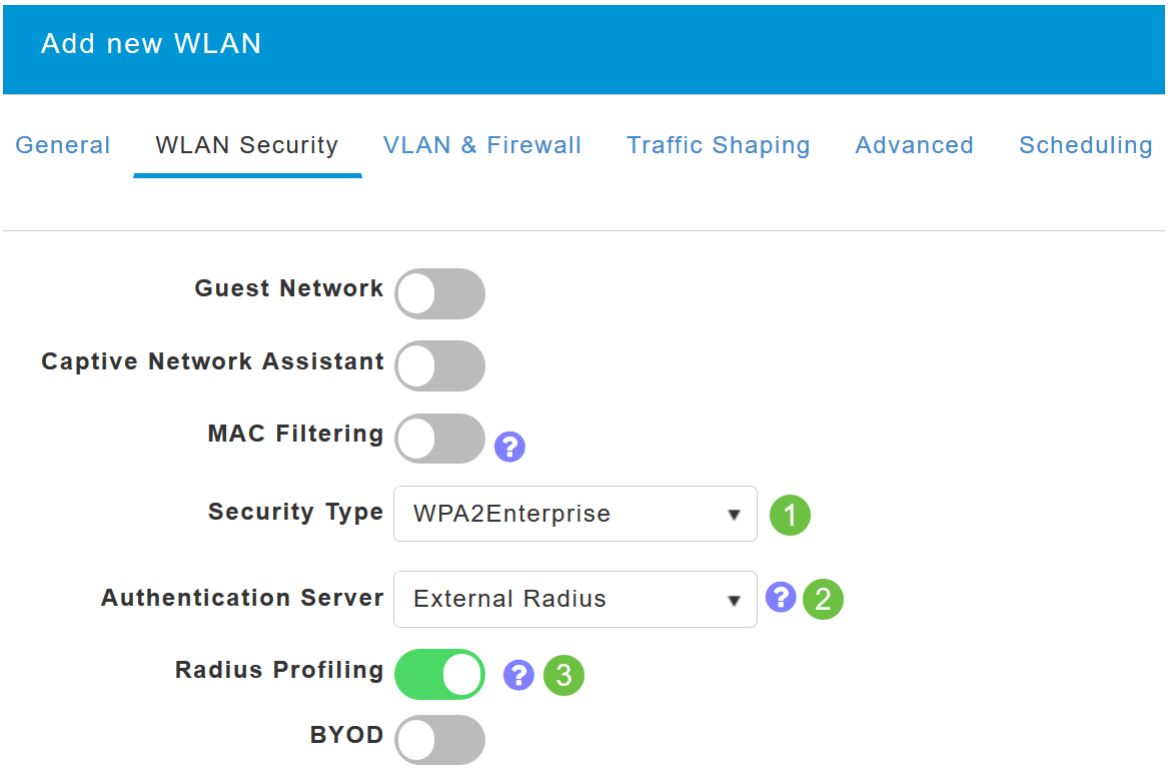
Paso 3

En la pestaña *General*, ingrese el *Nombre del Perfil*. El campo *SSID* se rellenará automáticamente. Puede optar por habilitar *Perfiles locales*. Haga clic en Apply (Aplicar).



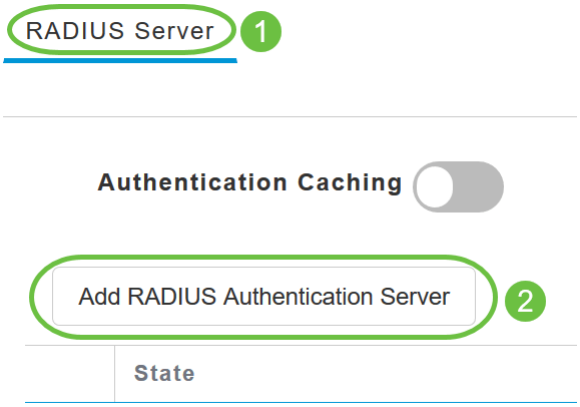
Paso 4

Vaya a la pestaña *Seguridad WLAN*. En el menú desplegable *Tipo de seguridad*, elija **WPA2Enterprise**. Seleccione **External Radius** como *Authentication Server*. Puede optar por habilitar la *definición de perfiles de RADIUS*.



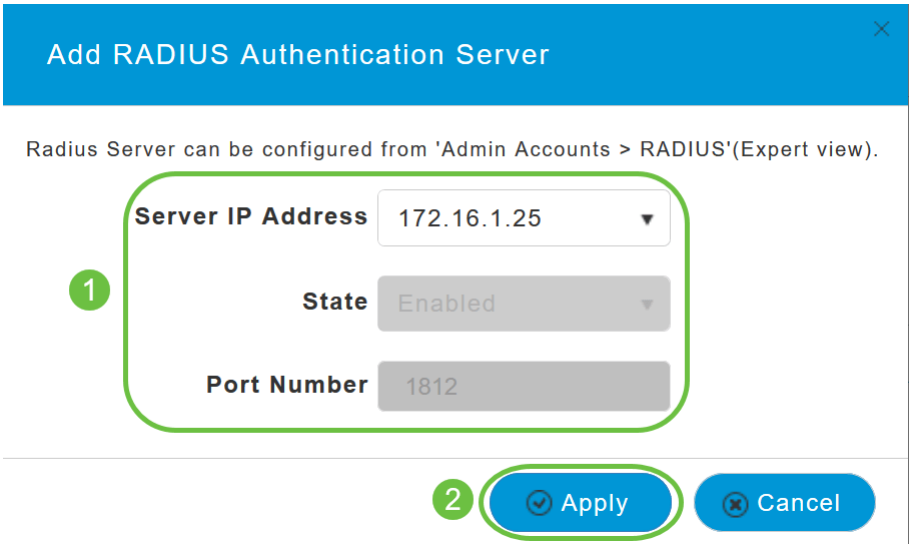
Paso 5

Vaya a la sección *Servidor RADIUS*. Haga clic en **Add RADIUS Authentication Server**.



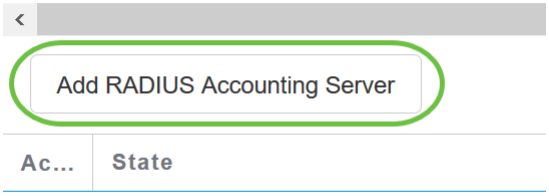
Paso 6

Verifique los detalles del servidor de autenticación RADIUS que ha configurado y haga clic en **Aplicar**.



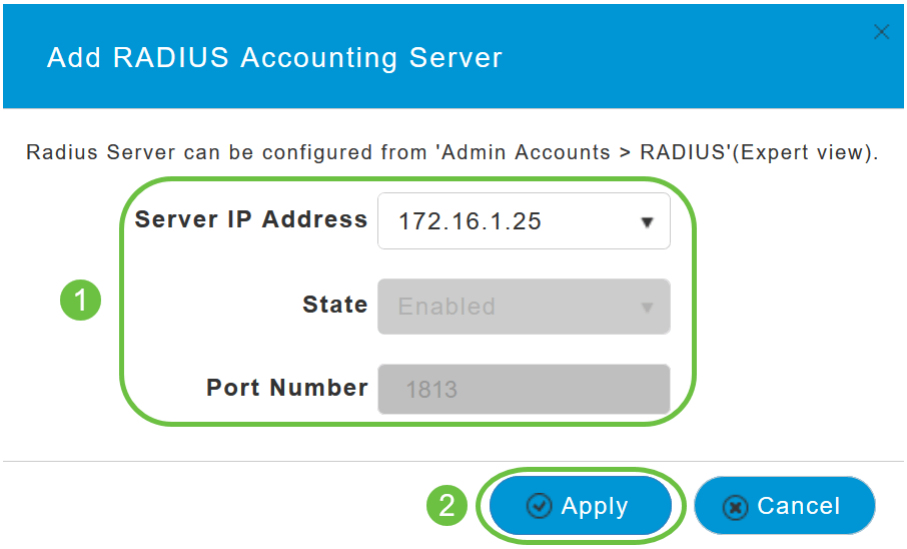
Paso 7

Haga clic en **Add RADIUS Accounting Server**.



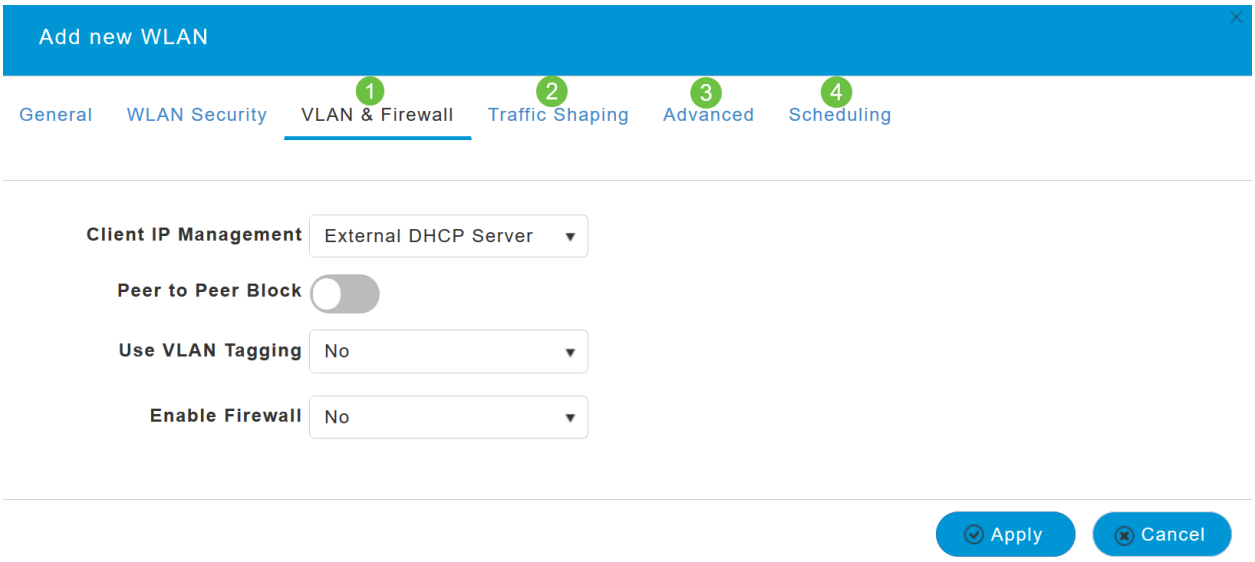
Paso 8

Verifique los detalles del servidor de contabilidad RADIUS que ha configurado y haga clic en **Aplicar**.



Paso 9

Navegue hasta las pestañas *VLAN & Firewall*, *Modelado de tráfico*, *Avanzado* y *Programación* para configurar los ajustes según sus preferencias de red. Haga clic en Apply (Aplicar).

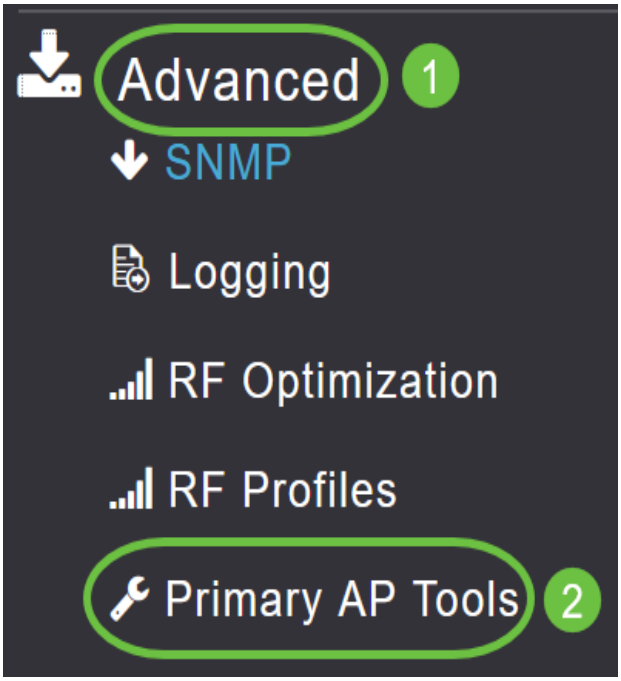


Verificación

Para probar la autenticación RADIUS, haga lo siguiente:

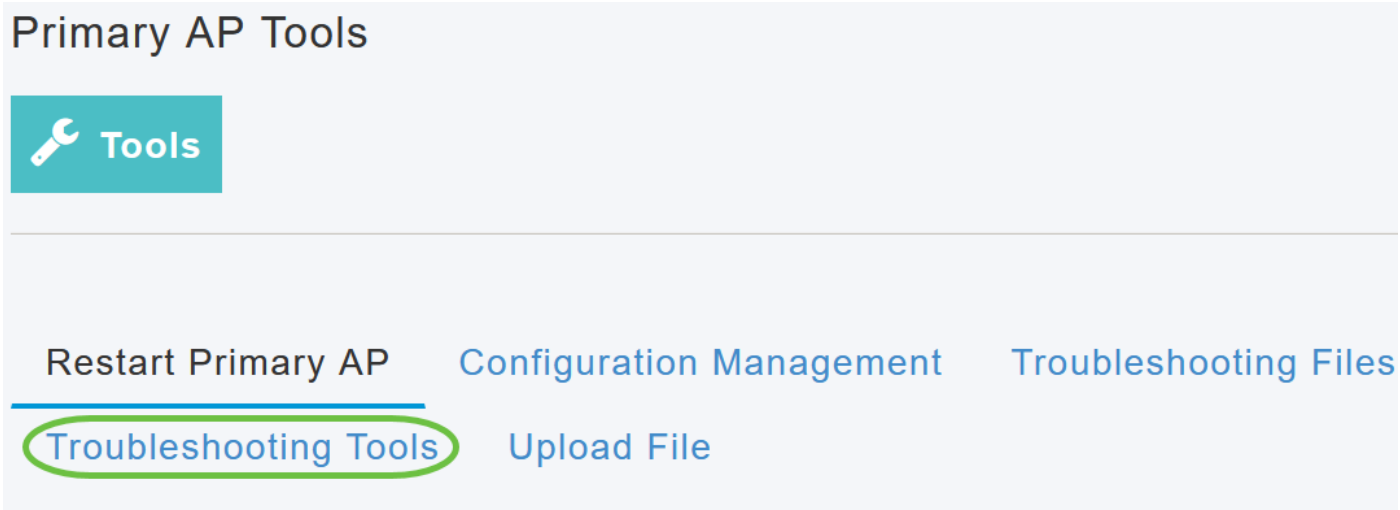
Paso 1

Navegue hasta **Avanzadas > Herramientas de AP principales**.



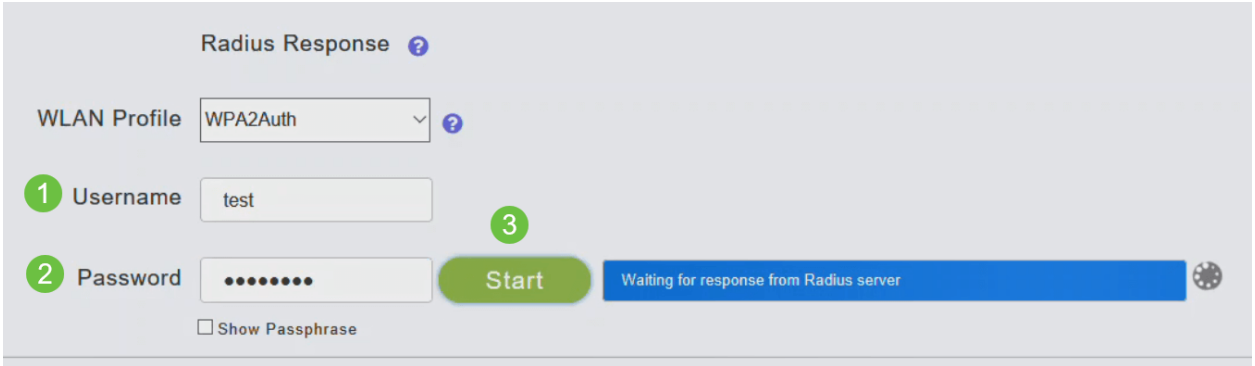
Paso 2

Haga clic en **Herramientas de resolución de problemas**.



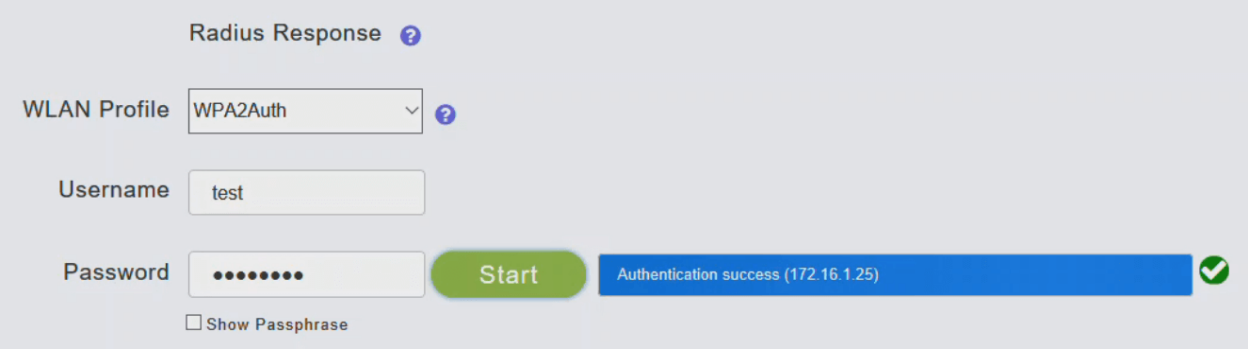
Paso 3

En la sección *Respuesta de RADIUS*, ingrese el *Nombre de Usuario* y la *Contraseña* para el Perfil de WLAN que ha configurado previamente y haga clic en *Inicio*.



Paso 4

Cuando la verificación se complete correctamente, verá la siguiente notificación en la pantalla.



Conclusión

¡Ahí lo tienes! Ahora ha aprendido los pasos para configurar RADIUS en su CBW AP. Para obtener más configuraciones avanzadas, consulte la *Guía de administración del punto de acceso inalámbrico Cisco Business.*

Preguntas Frecuentes Actualización del firmware RLAN Definición de perfiles de aplicaciones Perfiles de clientes Herramientas principales de AP Umbrella Usuarios de WLAN Registro Modelado de tráfico Rogues Interferentes Administración de la Configuración Modo de malla de configuración de puertos