Configuración de Puerto con RLANs en una Red CBW

Objetivo

El objetivo de este artículo es crear una red de área local remota (RLAN) y asignar puertos y grupos de puntos de acceso en un punto de acceso principal (AP) Cisco Business Wireless (CBW).

Dispositivos aplicables | Versión de software

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

Introducción

Los AP CBW se basan en 802.11 a/b/g/n/ac (Wave 2), con antenas internas. Estos AP admiten el último estándar 802.11ac Wave 2 para redes de mayor rendimiento, mayor acceso y mayor densidad.

Los AP 145AC y 240AC a los que se hace referencia en este artículo tienen la capacidad de ser usados en una red tradicional o de malla. En este artículo se utiliza el equipo para una red inalámbrica tradicional.

Si desea conocer los aspectos básicos de las redes de malla, consulte Cisco Business: Bienvenido a Wireless Mesh Networking.

Si prefiere realizar la configuración de puertos en una red de malla, lea Configurar puertos Ethernet del punto de acceso inalámbrico Cisco Business en modo de malla.

En una red inalámbrica tradicional, se utiliza una RLAN para autenticar clientes cableados usando el AP primario. Una vez que el cliente cableado se une correctamente al AP primario, los puertos LAN conmutan el tráfico entre los modos de conmutación central o local. El tráfico del cliente por cable se trata como tráfico de cliente inalámbrico.

El RLAN envía la solicitud de autenticación para autenticar el cliente cableado. La autenticación del cliente por cable en una RLAN es similar al cliente inalámbrico central autenticado.

Si sólo necesita una red de área local virtual (VLAN), no necesita configurar una RLAN. Un RLAN se ingresa en el AP de forma predeterminada, la VLAN nativa 1. Tiene seguridad abierta y todos los puertos se asignan a esta RLAN de forma predeterminada.

Si no conoce los términos utilizados, consulte Cisco Business: Glosario de nuevos términos.

Los RLAN no funcionan en una red de interconexión. La malla no está habilitada de forma predeterminada, así que a menos que haya tenido el AP ejecutándose en modo de malla, está configurado para ir.

Configuration Steps

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

Encienda el punto de acceso si aún no está activado. Compruebe el estado de las luces indicadoras. Cuando la luz LED parpadee en verde, vaya al siguiente paso.

El arranque del punto de acceso tardará entre 8 y 10 minutos. La luz parpadeará en verde en varios patrones, alternando rápidamente entre verde, rojo y ámbar antes de volver a girar en verde. Puede haber pequeñas variaciones en la intensidad y el color del LED.

Paso 2

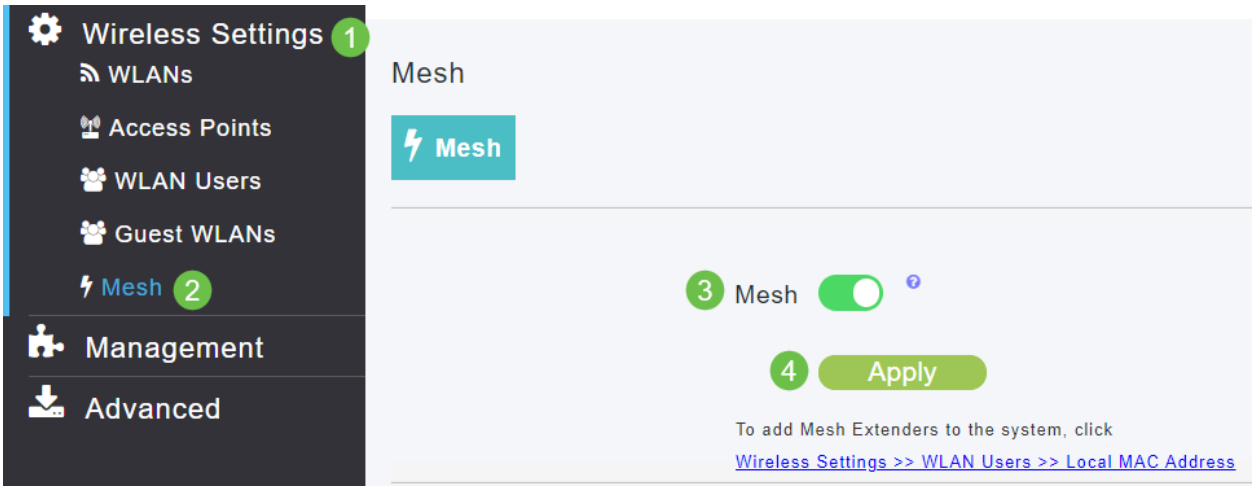
Inicie sesión en la interfaz de usuario web (IU) del AP principal. Abra un navegador web e ingrese https://ciscobusiness.cisco Puede recibir una advertencia antes de continuar. Introduzca sus credenciales.

También puede acceder a él ingresando la dirección IP del AP principal en un navegador web.

Paso 3

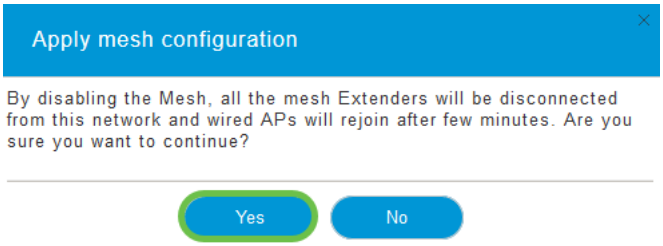
El AP no puede estar en modo de malla para que un RLAN funcione. Para desactivar el modo de

malla, navegue hasta **Wireless Settings > Mesh**. Seleccione esta opción para desactivar la malla. Si su AP es nuevo o sabe que el modo de malla no está activado, puede pasar al Paso 7.



Paso 4

Confirme que desea desactivar el modo de malla haciendo clic en **Sí**.

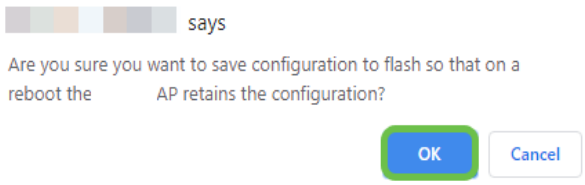


Paso 5

Asegúrese de guardar las configuraciones haciendo clic en el **icono Guardar** del panel superior derecho de la pantalla de la interfaz de usuario Web.

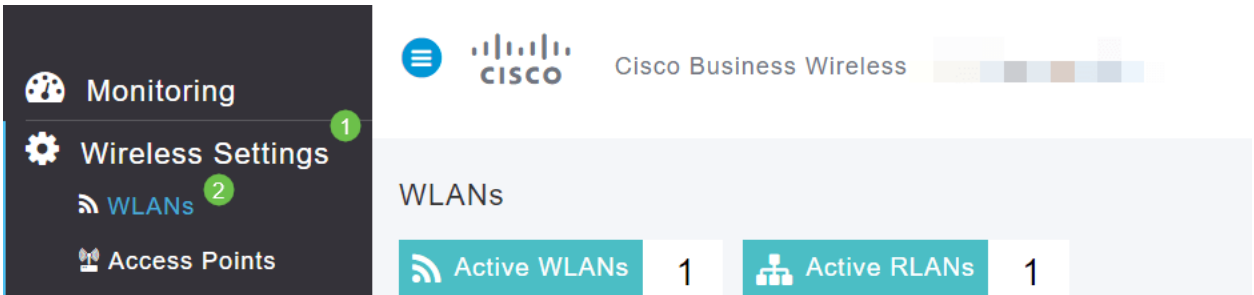
Paso 6

Confirme la opción Guardar haciendo clic en **Aceptar**. El AP se reiniciará. Esto tardará entre 8 y 10 minutos en completarse.



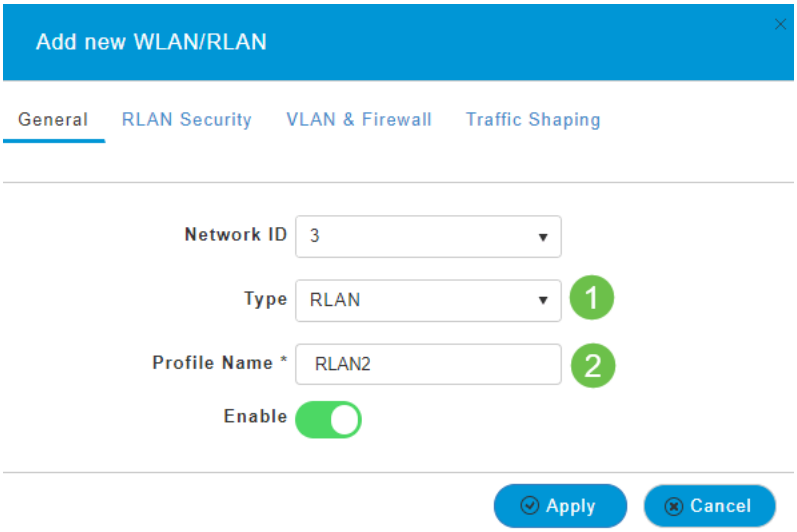
Paso 7

Se puede crear una RLAN navegando a **Wireless Settings > WLAN**. A continuación, seleccione **Add new WLAN/RLAN**.



Paso 8

Seleccione **RLAN**. Cree un nombre para el perfil.

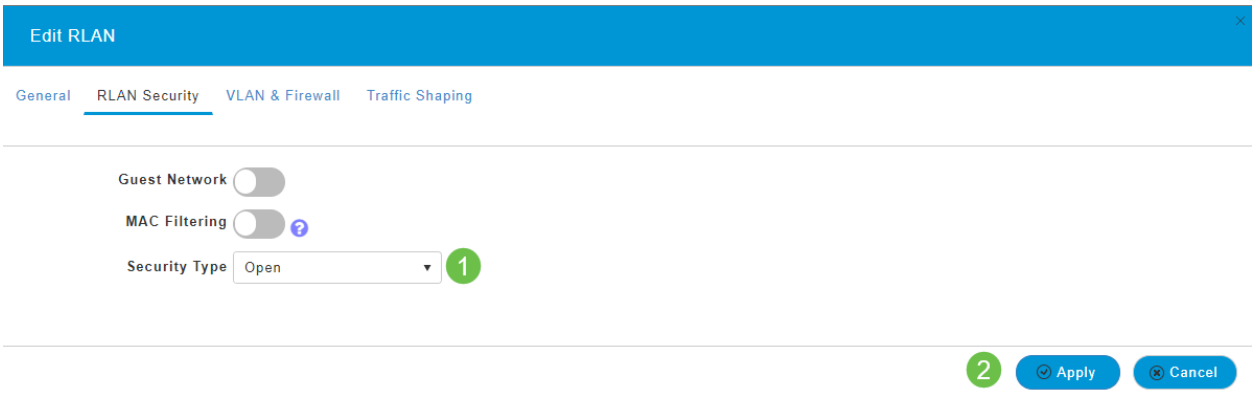


Paso 9 (Uso de la seguridad abierta)

En la pestaña *RLAN Security*. En *Tipo de seguridad*, puede seleccionar *Open* o *802.1X*.

En este ejemplo, el *tipo de seguridad* se dejó como valor predeterminado.

Haga clic en Apply (Aplicar). Esto activará automáticamente esta RLAN de seguridad abierta. Saltar al Paso 11.



Paso 10a (Uso de la seguridad 802.1X)

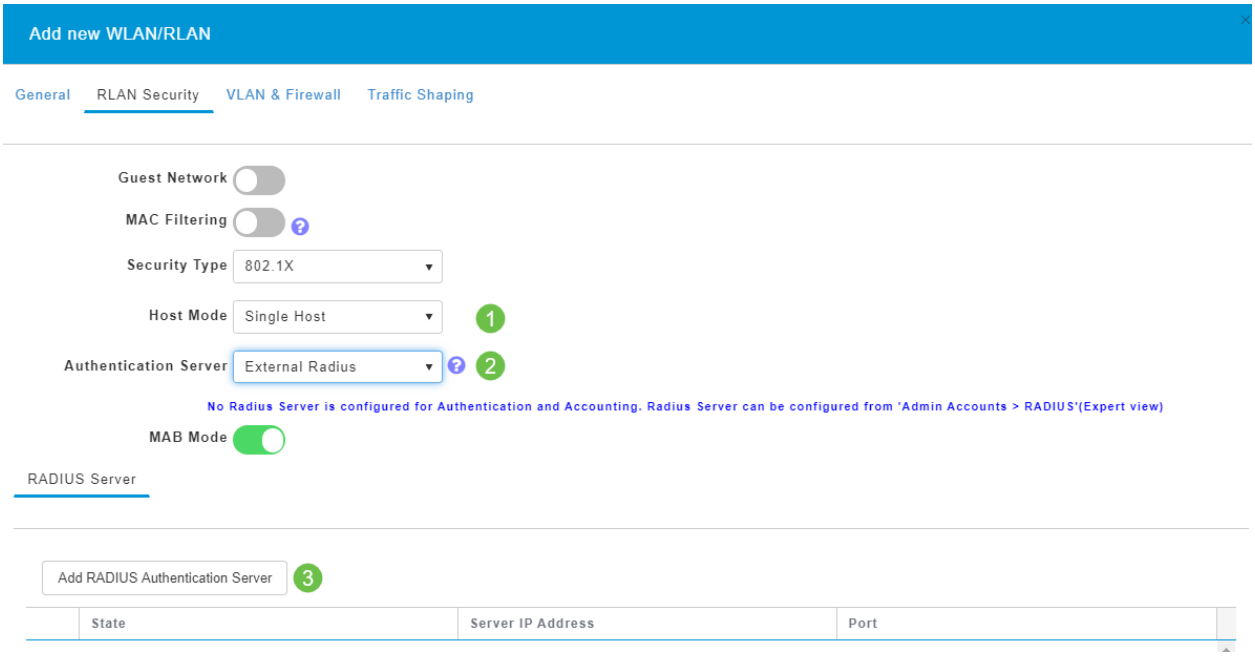
Para configurar Radius Externo, debe tener un Servidor Radius configurado en *Cuentas Admin* bajo *RADIUS* en *Vista Experta*. Haga clic en el **icono de flecha** en el menú superior derecho de la interfaz de usuario Web para cambiar a *Vista de expertos*. Para obtener detalles sobre la configuración de un servidor RADIUS, consulte Radius

Paso 10b (uso de la seguridad 802.1X)

Si elige 802.1X para el tipo de seguridad, se deben seleccionar más opciones. Debe seleccionar lo siguiente:

- *Modo host*: *Host único* o *Host múltiple*

- *Servidor de autenticación - RADIUS externo* o *AP*
- *Modo MAB: habilitado* o *desactivado.* Para agregar direcciones MAC, siga las instrucciones del paso siguiente.

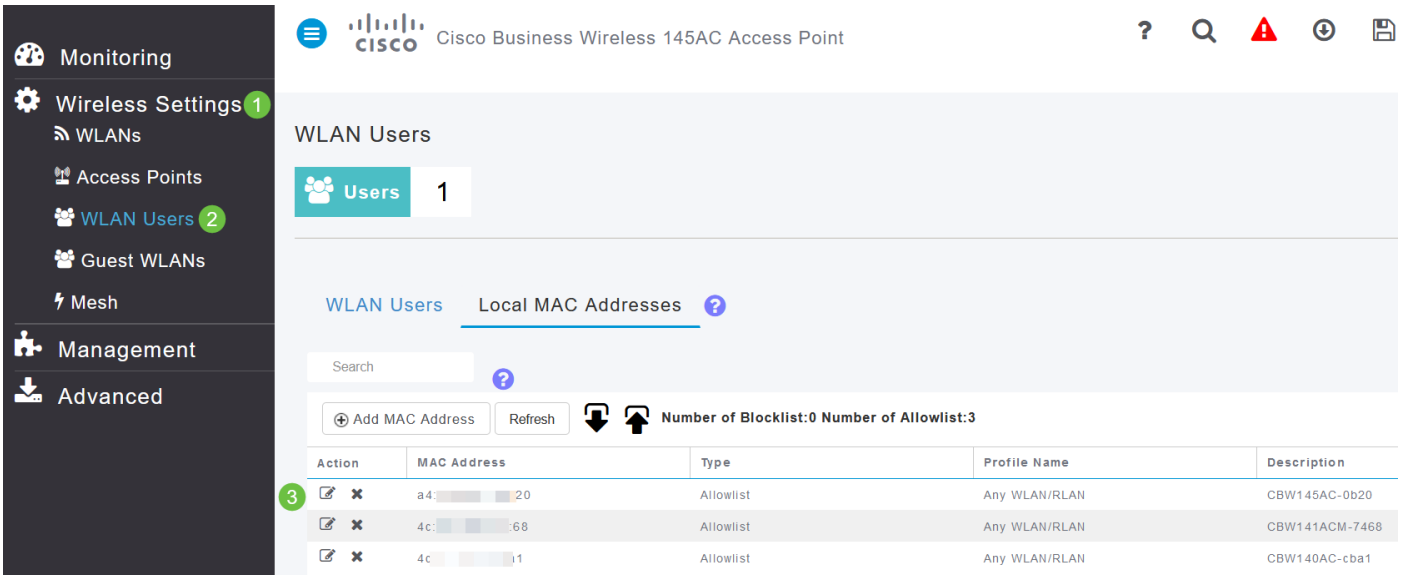


Paso 11 (opcional)

El modo de omisión de autenticación MAC (MAB) significa que si tiene una dirección MAC enumerada en Usuarios de WLAN, el dispositivo no necesita autenticarse. Las direcciones MAC enumeradas pueden eludir la autenticación para que se les conceda acceso automático a la red o se les deniegue automáticamente. Esto sería útil en un caso en el que un teléfono IP está conectado a un puerto PoE en un switch.

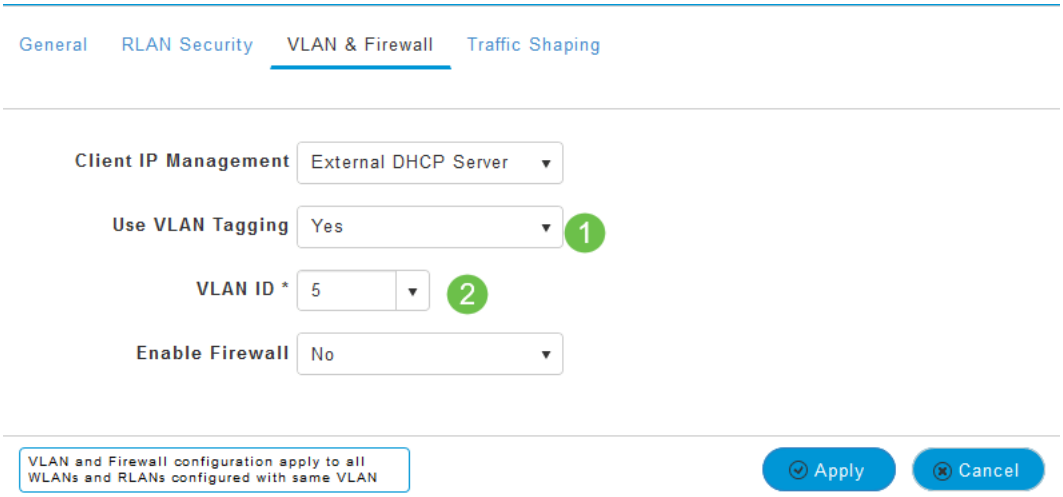
Puede etiquetar cada dirección MAC de una de las dos maneras siguientes:

1. *Allowlisted*: El dispositivo recibe acceso automático.
2. *Lista bloqueada*: se denegará automáticamente el acceso al dispositivo.



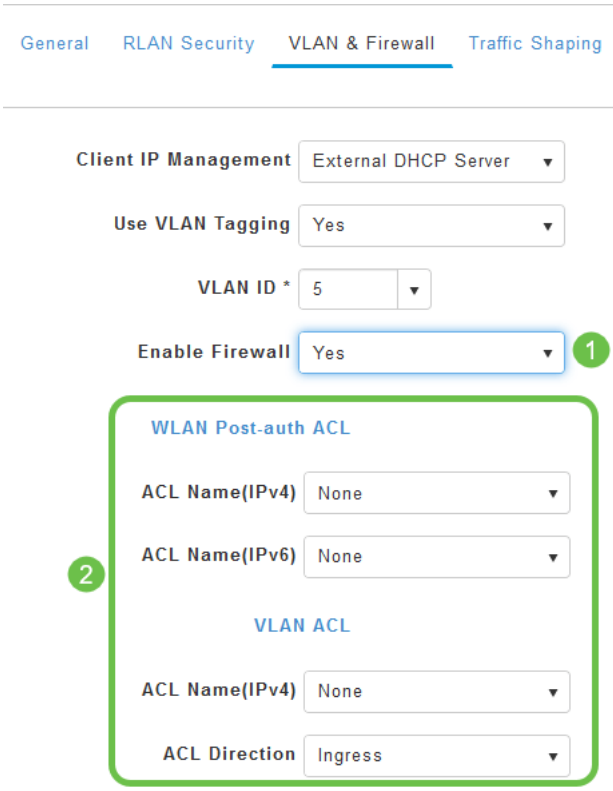
Paso 12

En la pestaña *VLAN & Firewall*, puede seleccionar Use *VLAN Tagging* y seleccionar un número *VLAN ID*.



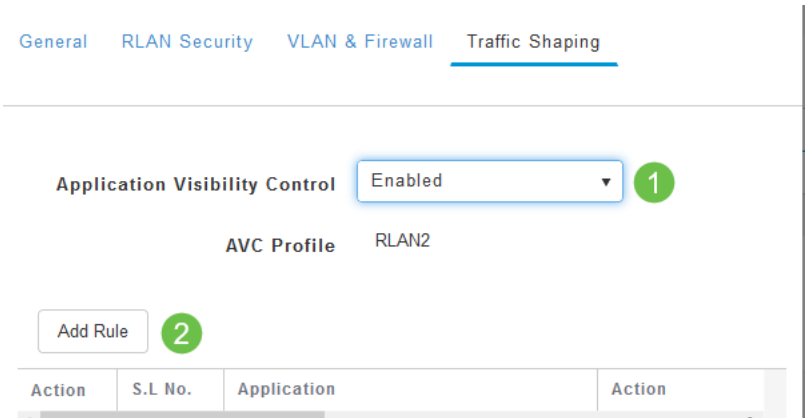
Paso 13 (opcional)

Puede seleccionar **Habilitar firewall** si desea configurar *Listas de control de acceso (ACL)* que le permitan permitir o rechazar el acceso para direcciones IP o VLAN específicas. Esto se utiliza si alguien se conecta al dispositivo de puerto de red para conectarse a la red.



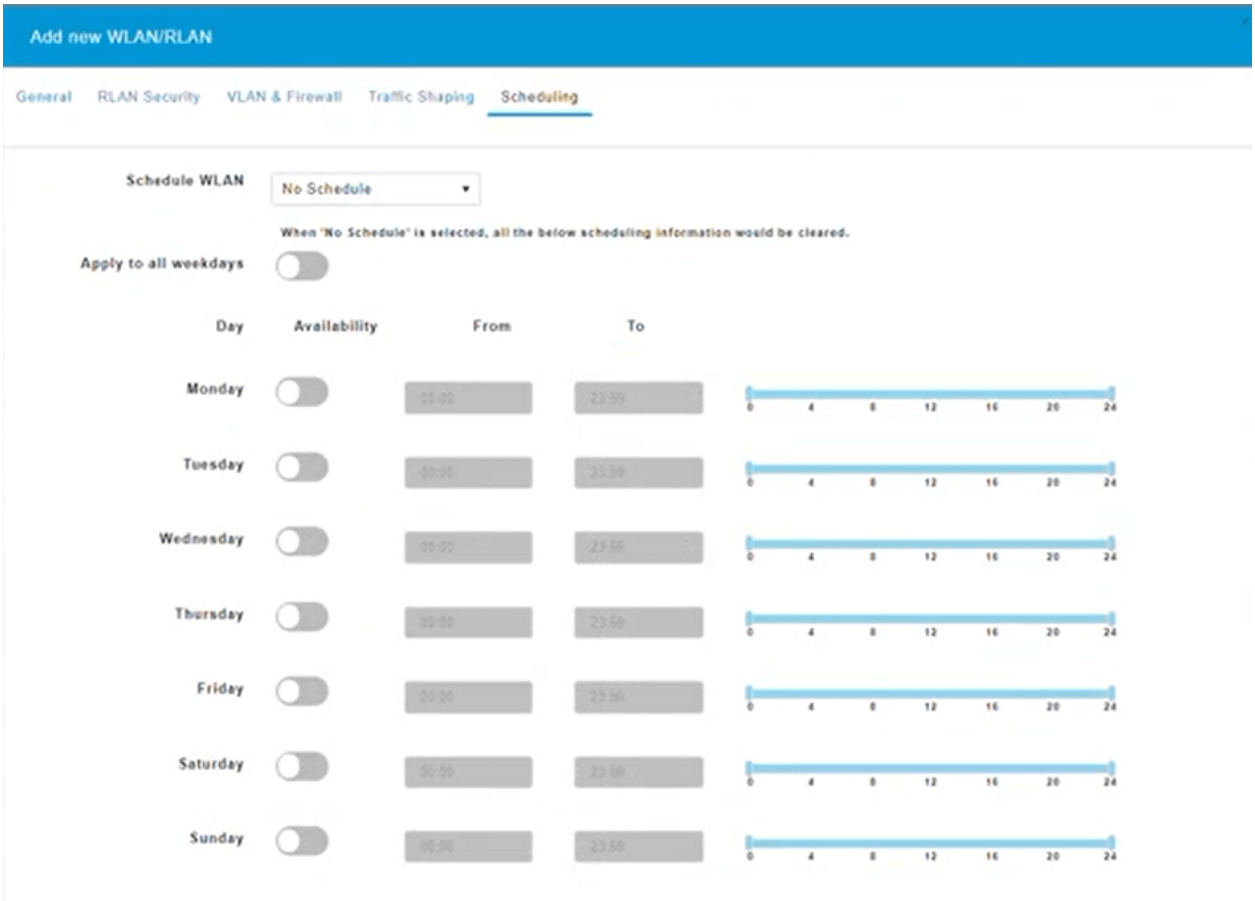
Paso 14 (opcional)

En la pestaña *Modelado de tráfico*, puede configurar el modelado de tráfico habilitando **Control de Visibilidad de Aplicación**. Esto establece la priorización del tráfico.



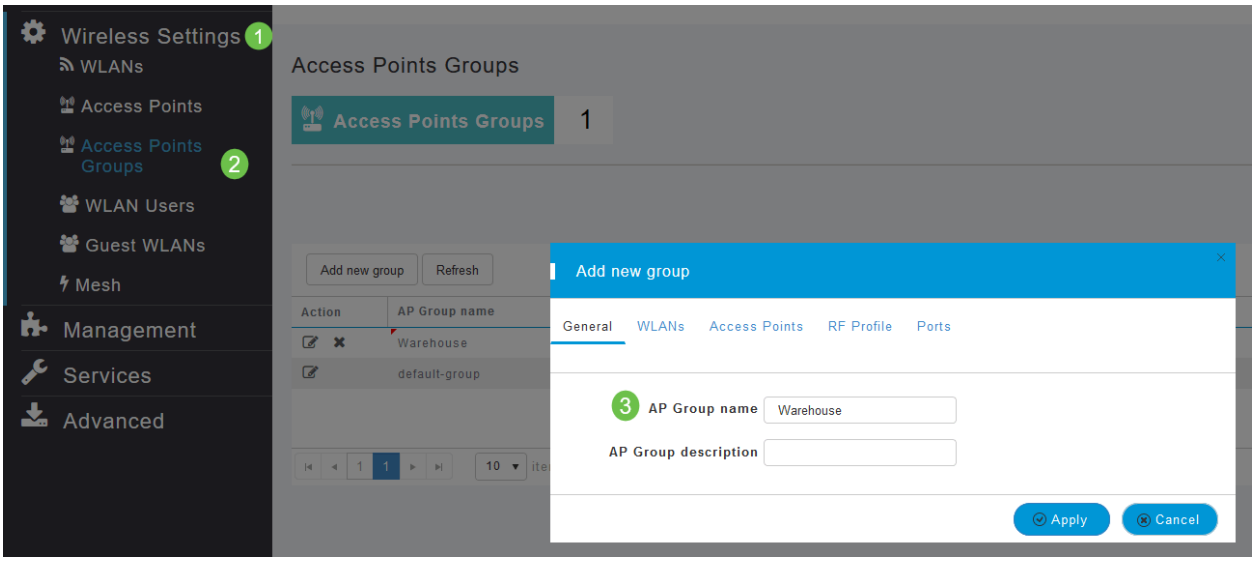
Paso 15 (opcional)

En la ficha *Programación*, puede seleccionar una programación. Esto establece el tiempo que el puerto tendrá la capacidad de estar conectado a la red.



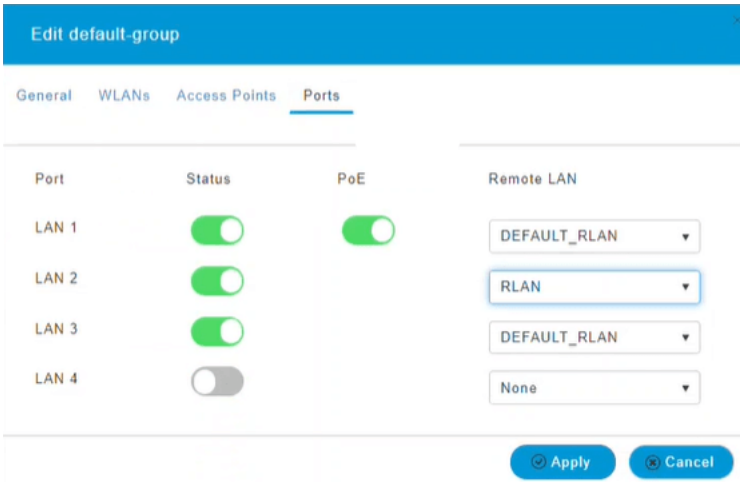
Paso 16 (opcional)

Ahora que se ha creado la RLAN, puede navegar hasta **Wireless Settings > Access Point Groups** . Aquí es donde puede agregar o editar grupos. Para ver esta pantalla, debe estar en la *Vista de expertos*, que seleccionó en el Paso 10a.



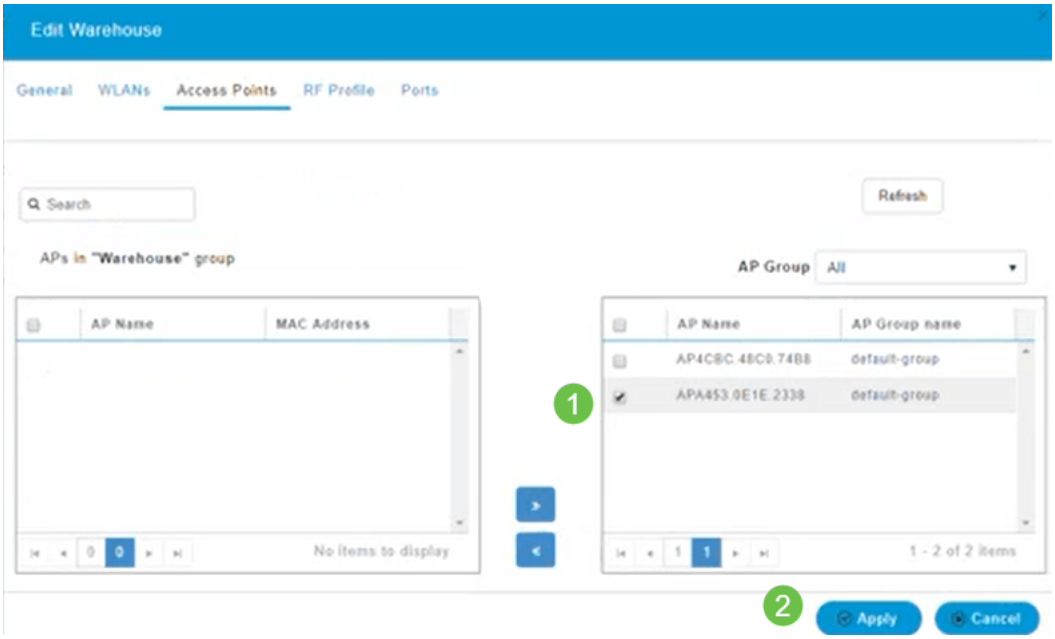
Paso 17

En la pestaña *Ports*, puede asignar los puertos en el AP a las LAN remotas específicas.



Paso 18

En la ficha *Puntos de acceso*, debe asignar un punto de acceso determinado a ese grupo de puntos de acceso. Haga clic en Apply (Aplicar).



Paso 19

Seleccione **Yes** para confirmar.

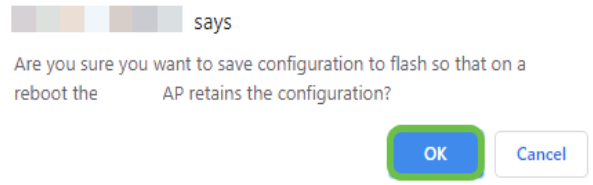
Paso 20

Asegúrese de guardar las configuraciones haciendo clic en el **icono Guardar** del panel superior derecho de la pantalla de la interfaz de usuario Web.

Paso 21

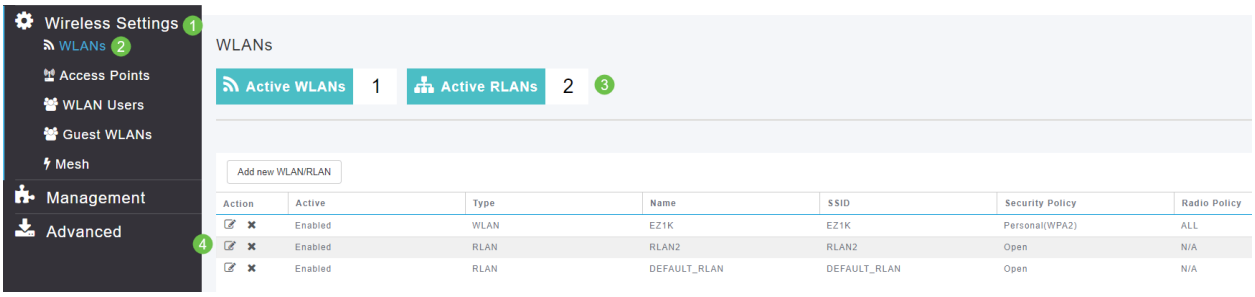
Confirme la opción Guardar haciendo clic en **Aceptar**. El AP se reiniciará. Esto tardará entre 8 y

10 minutos en completarse.



Ver el RLAN

Para ver la RLAN que ha creado, seleccione **Wireless Settings > WLANs**. Verá el número de RLAN activas elevado a 2 y se muestra la nueva RLAN.

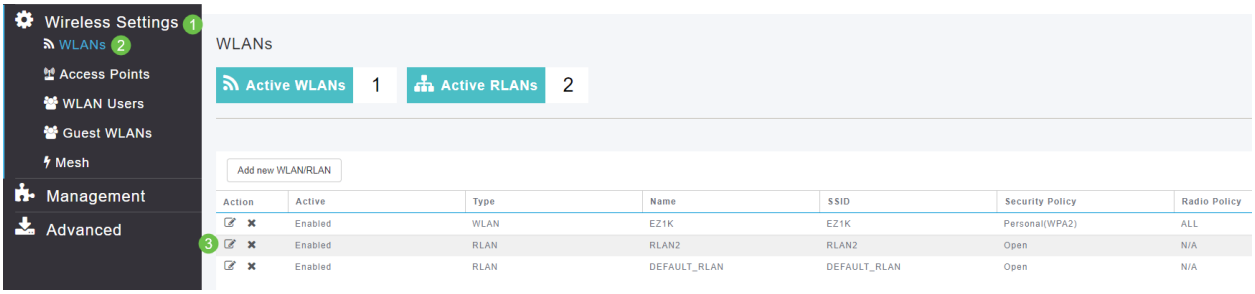


Editar RLAN

Cuando hizo clic en **Aplicar** al final de la configuración de su RLAN, el RLAN se activó automáticamente. Si alguna vez necesita inhabilitar la RLAN o realizar cualquier otro cambio, siga estos sencillos pasos a continuación.

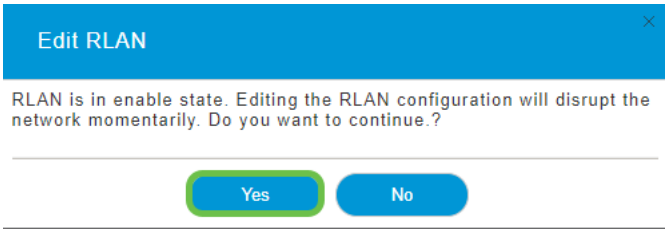
Paso 1

Seleccione **Wireless Settings > WLAN**. Haga clic en el **icono de edición**.



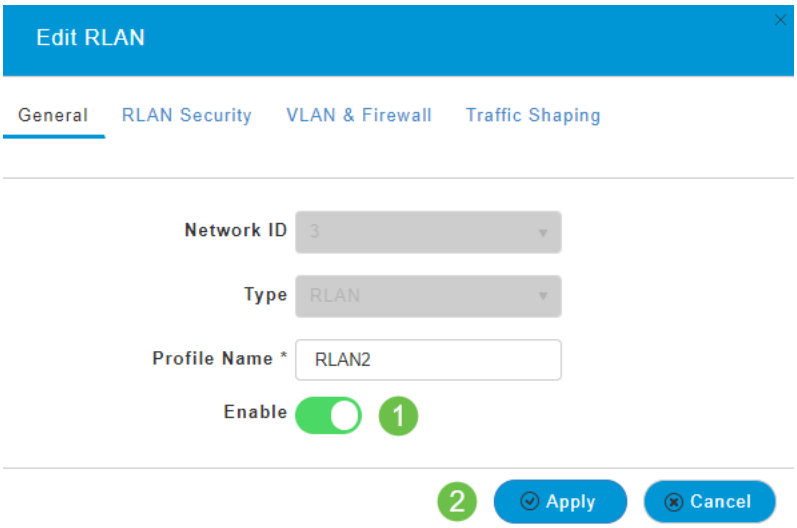
Paso 2

Recibirá una ventana emergente en la que se le notificará que la edición de la RLAN interrumpirá la red momentáneamente. Confirme que desea continuar haciendo clic en **Sí**.



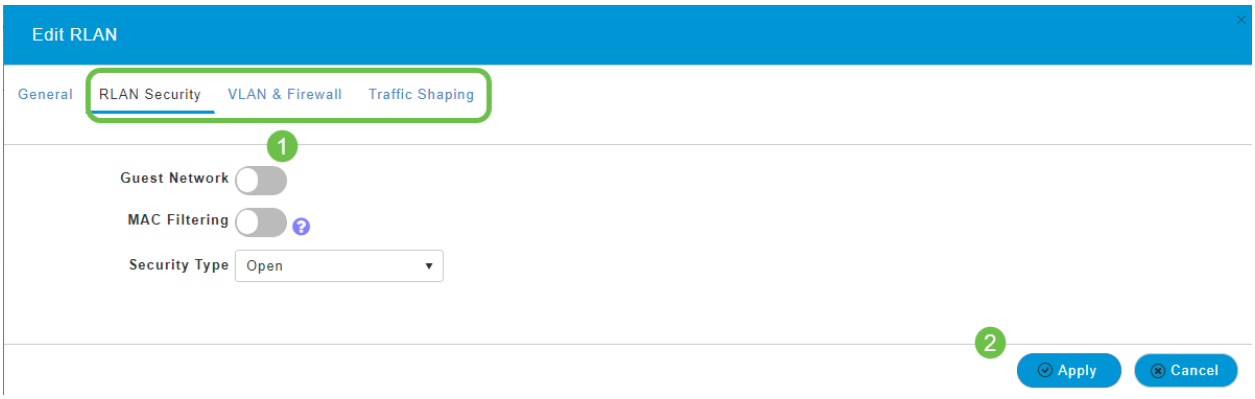
Paso 3 (Activar/Desactivar)

En la ventana **Edit WLAN/RLAN, en General**, seleccione ***Enabled*** o **Disabled** para habilitar/inhabilitar el RLAN. Haga clic en Apply (Aplicar).



Paso 4 (Edición de otros parámetros)

Navegue hasta las fichas *Seguridad RLAN*, *VLAN & Firewall*, o *Modelado de tráfico* si necesita cambiar la configuración. Haga clic en **Aplicar** una vez que haya realizado cambios.



Paso 5

Asegúrese de guardar las configuraciones haciendo clic en el **icono Guardar** del panel superior derecho de la pantalla de la interfaz de usuario Web.

Conclusión

Ahora ha creado una RLAN en su red CBW. Disfrute y siéntase libre de añadir más si se ajusta a sus necesidades.

Preguntas Frecuentes Radius 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 Bienvenido a CBW Mesh Networking Red de invitado con autenticación de correo electrónico y contabilidad RADIUS Resolución de problemas Uso de un router Draytek con CBW