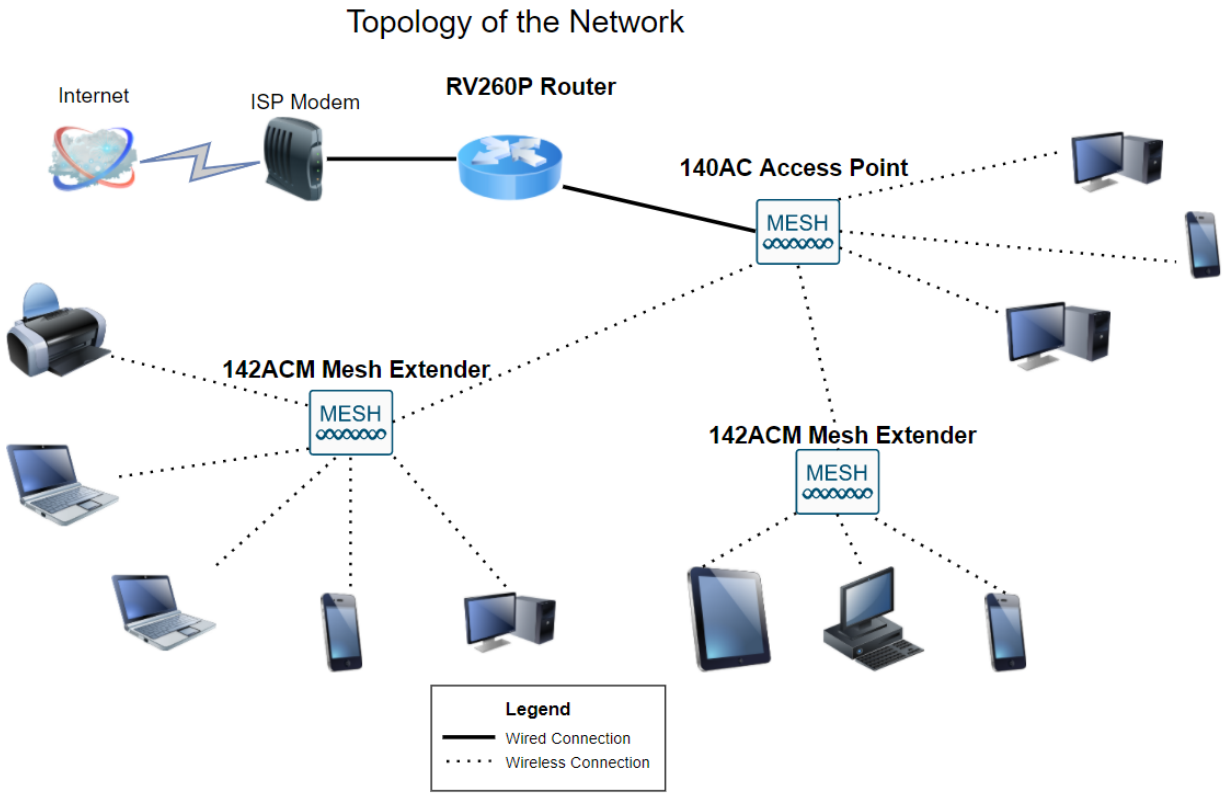
Configuración de red total: RV260P con Cisco Business Wireless y la interfaz de usuario web

Objetivo:

Esta guía le mostrará cómo configurar una red de malla inalámbrica mediante un router RV260P, un punto de acceso CBW140AC y dos extensores de malla CBW142ACM.

En este artículo se utiliza la interfaz de usuario web para configurar la red inalámbrica de malla. Si prefiere utilizar la aplicación móvil, que se recomienda para una configuración inalámbrica sencilla, haga clic para saltar al artículo que utiliza la aplicación móvil. Si desea utilizar la interfaz de usuario web, siga leyendo.

Topología:



Introducción

Aquí está, listo para configurar su nueva red. ¡Es un día emocionante! En esta situación, estamos utilizando un router RV260P. Este router proporciona alimentación a través de Ethernet (PoE), lo que le permite conectar el CBW140AC al router en lugar de un switch. Los extensores de malla CBW140AC y CBW142ACM se utilizarán para crear una red de malla inalámbrica.

Si no está familiarizado con algunos de los términos utilizados en este documento o desea obtener más información sobre Mesh Networking, consulte los siguientes

artículos:

- Cisco Business: Glosario de nuevos términos
- Bienvenido a Cisco Business Wireless Mesh Networking
- Preguntas frecuentes (FAQ) sobre una red inalámbrica empresarial de Cisco

¿Estás listo? ¡Vamos a ello!

Dispositivos aplicables | Versión de software

- RV260P |1.0.0.17
- CBW140AC |10.3.1.0
- CBW142ACM | 10.3.1.0 (se necesita al menos un extensor de malla para la red de malla)

Table Of Contents

Antes de empezar

1. Asegúrese de que dispone de una conexión a Internet actual para la configuración.
2. Póngase en contacto con el ISP para obtener información sobre las instrucciones especiales que tenga al utilizar el router RV260. Algunos ISP ofrecen puertas de enlace con routers integrados. Si dispone de una puerta de enlace con un router integrado, es posible que tenga que desactivar el router y pasar la dirección IP de la

red de área extensa (WAN) (la dirección de protocolo de Internet única que el proveedor de Internet asigna a su cuenta) y todo el tráfico de red a través del nuevo router.

3. Decida dónde colocar el router. Si es posible, querrá un área abierta. Esto puede no ser fácil porque debe conectar el router al gateway de banda ancha (módem) desde el ISP.

Configuración del router RV260P

Un router es esencial en una red porque enruta paquetes. Permite a un equipo comunicarse con otros equipos que no están en la misma red o subred. Un router accede a una tabla de ruteo para determinar dónde deben enviarse los paquetes. La tabla de ruteo enumera las direcciones de destino. Las configuraciones estáticas y dinámicas se pueden enumerar en la tabla de ruteo para que los paquetes lleguen a su destino específico.

El RV260P incluye parámetros predeterminados optimizados para muchas pequeñas empresas. Sin embargo, es posible que las demandas de la red o el proveedor de servicios de Internet (ISP) deban modificar algunos de estos parámetros. Después de ponerse en contacto con el ISP para obtener información sobre los requisitos, puede realizar cambios mediante la interfaz de usuario web.

RV260P fuera de la caja

Paso 1

Conecte el cable Ethernet desde uno de los puertos RV260P LAN (Ethernet) al puerto Ethernet del ordenador. Necesitará un adaptador si el ordenador no dispone de puerto Ethernet. El terminal debe estar en la misma subred con cables que el RV260P para realizar la configuración inicial.

Paso 2

Asegúrese de utilizar el adaptador de corriente suministrado con el RV260P. El uso de un adaptador de corriente diferente podría dañar el RV260P o hacer que los dongles USB fallen. El switch de alimentación está encendido de forma predeterminada.

Conecte el adaptador de corriente al puerto de 12 VCC del RV260P, pero no lo conecte a la alimentación todavía.

Paso 3

Asegúrese de que el módem está apagado.

Paso 4

Utilice un cable Ethernet para conectar el módem por cable o DSL al puerto WAN del RV260P.

Paso 5

Conecte el otro extremo del adaptador RV260P a una toma de corriente. Esto encenderá el RV260. Vuelva a conectar el módem para que también se pueda encender. La luz de alimentación del panel frontal está encendida en verde fijo cuando el adaptador de corriente está conectado correctamente y el RV260P ha finalizado el arranque.

Configuración del router

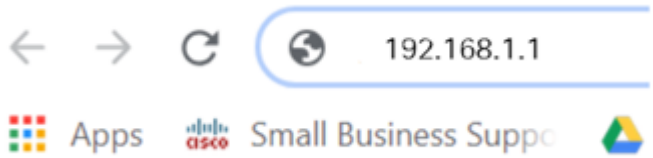
El trabajo preparatorio se ha realizado, ahora es el momento de realizar algunas configuraciones. Para iniciar la interfaz de usuario Web, siga estos pasos:

Paso 1

Si el equipo está configurado para convertirse en cliente de protocolo de configuración dinámica de host (DHCP), se asigna al PC una dirección IP del intervalo 192.168.1.x. DHCP automatiza el proceso de asignación de direcciones IP, máscaras de subred, gateways predeterminados y otros ajustes a los equipos. Los ordenadores deben estar configurados para participar en el proceso DHCP para obtener una dirección. Esto se hace seleccionando para obtener una dirección IP automáticamente en las propiedades de TCP/IP en el equipo.

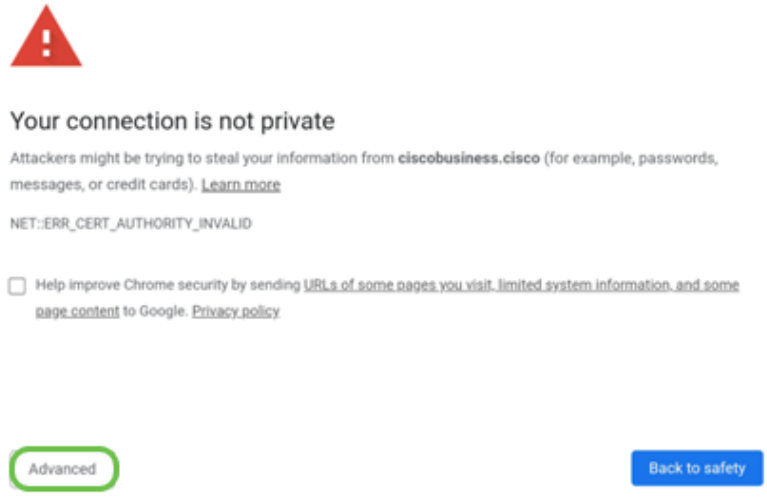
Paso 2

Abra un explorador web como Safari, Internet Explorer o Firefox. En la barra de direcciones, introduzca la dirección IP predeterminada del RV260P que es 192.168.1.1.



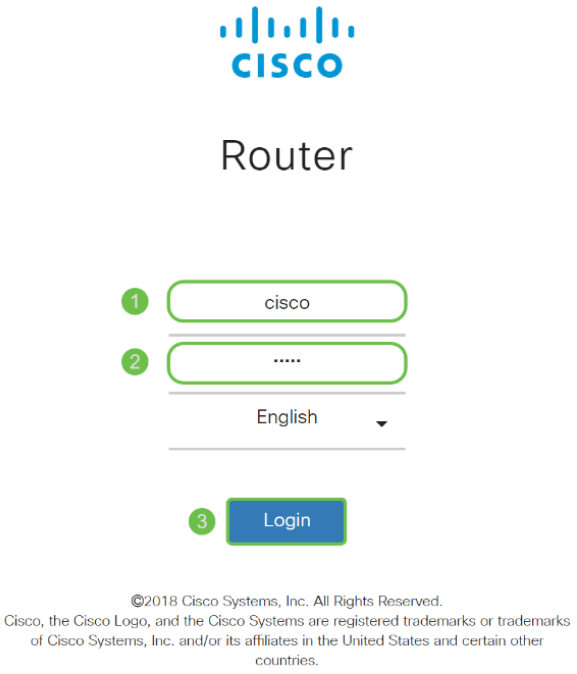
Paso 3

El explorador puede emitir una advertencia de que el sitio web no es de confianza. Continúe en el sitio web. Si no está conectado, vaya a Resolución de problemas de conexión a Internet.



Paso 4

Cuando aparezca la página de inicio de sesión, ingrese el nombre de usuario predeterminado cisco y la contraseña predeterminada *cisco*. Tanto el nombre de usuario como la contraseña distinguen entre mayúsculas y minúsculas.



Paso 5

Haga clic en Login (Conexión). Aparecerá la página *Introducción*. Ahora que ha confirmado la conexión y ha iniciado sesión en el router, vaya a la sección Configuración inicial de este artículo.

Resolución de problemas de la conexión a Internet

Colgar, si está leyendo esto probablemente tenga problemas para conectarse a Internet o a la interfaz de usuario web. Una de estas soluciones debería ayudar.

En el sistema operativo Windows conectado, puede probar la conexión de red abriendo el símbolo del sistema. Introduzca ping 192.168.1.1 (la dirección IP predeterminada del router). Si se agota el tiempo de espera de la solicitud, no podrá

comunicarse con el router.

Si no se produce la conectividad, puede desproteger la resolución de problemas en los routers RV160 y RV260.

Otras cosas que se deben intentar:

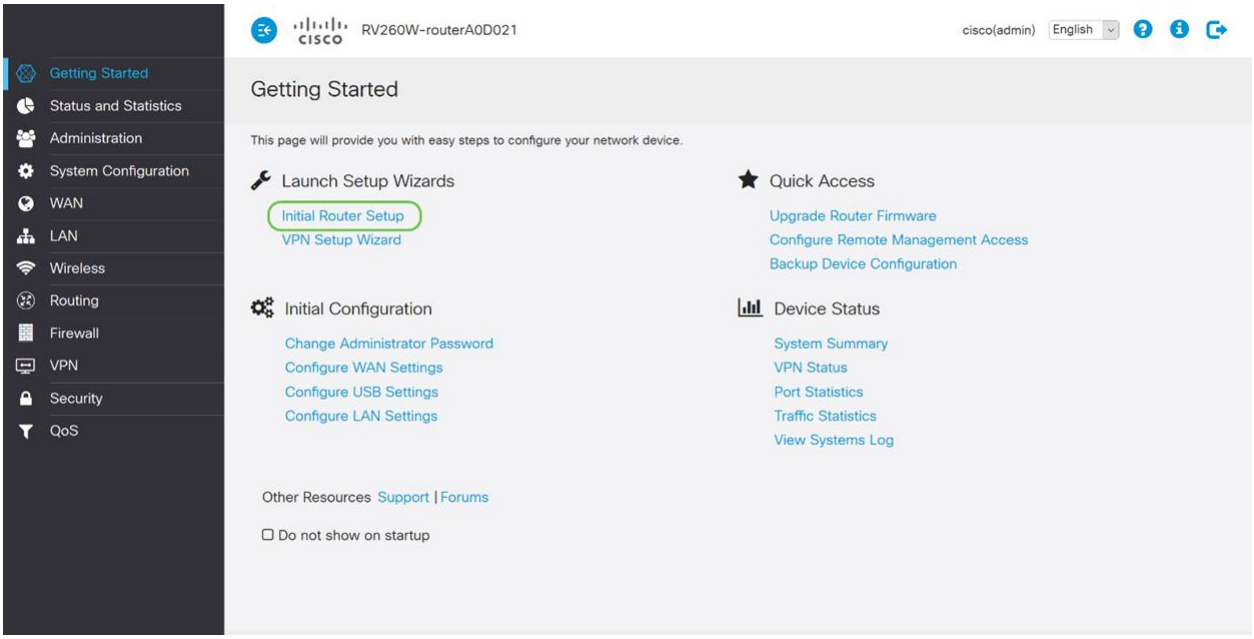
1. Compruebe que el explorador Web no está configurado en Trabajar sin conexión.
2. Compruebe los parámetros de conexión de red de área local del adaptador Ethernet. El PC debe obtener una dirección IP a través de DHCP. Alternativamente, el PC puede tener una dirección IP estática en el rango 192.168.1.x con el gateway predeterminado establecido en 192.168.1.1 (la dirección IP predeterminada del RV260P). Para conectarse, es posible que deba modificar los parámetros de red del RV260P. Si utiliza Windows 10, desproteja las instrucciones de Windows 10 para modificar los parámetros de red.
3. Si tiene equipos existentes ocupando la dirección IP 192.168.1.1, necesitará resolver este conflicto para que la red funcione. Más sobre esto al final de esta sección, o haga clic aquí para tomarlo directamente.
4. Reinicie el módem y el RV260P apagando ambos dispositivos. A continuación, encienda el módem y déjelo inactivo durante unos 2 minutos. A continuación, encienda el RV260P. Ahora debe recibir una dirección IP de WAN.
5. Si tiene un módem DSL, pida al ISP que ponga el módem DSL en modo de puente.

Configuración inicial

Le recomendamos que siga los pasos del Asistente de configuración inicial que se enumeran en esta sección. Puede cambiar estos parámetros en cualquier momento.

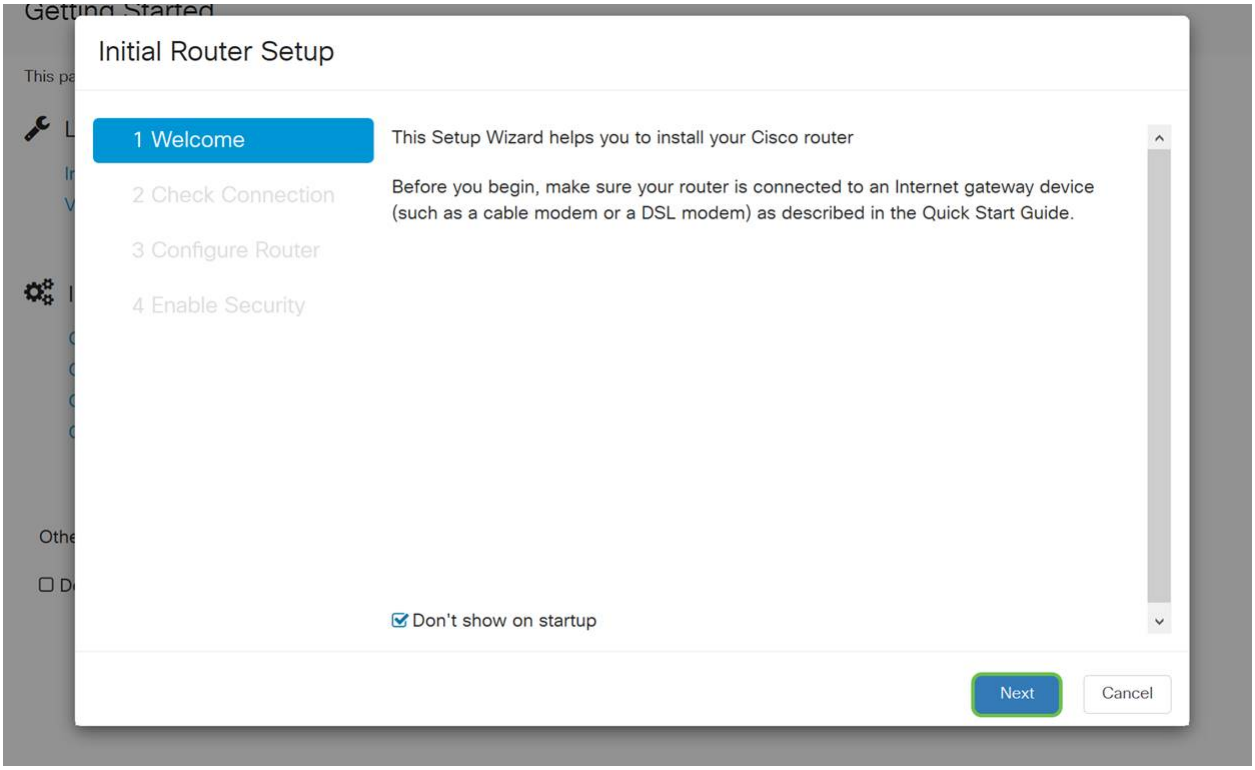
Paso 1

Haga clic en **Asistente de configuración inicial** en la página *Introducción*.



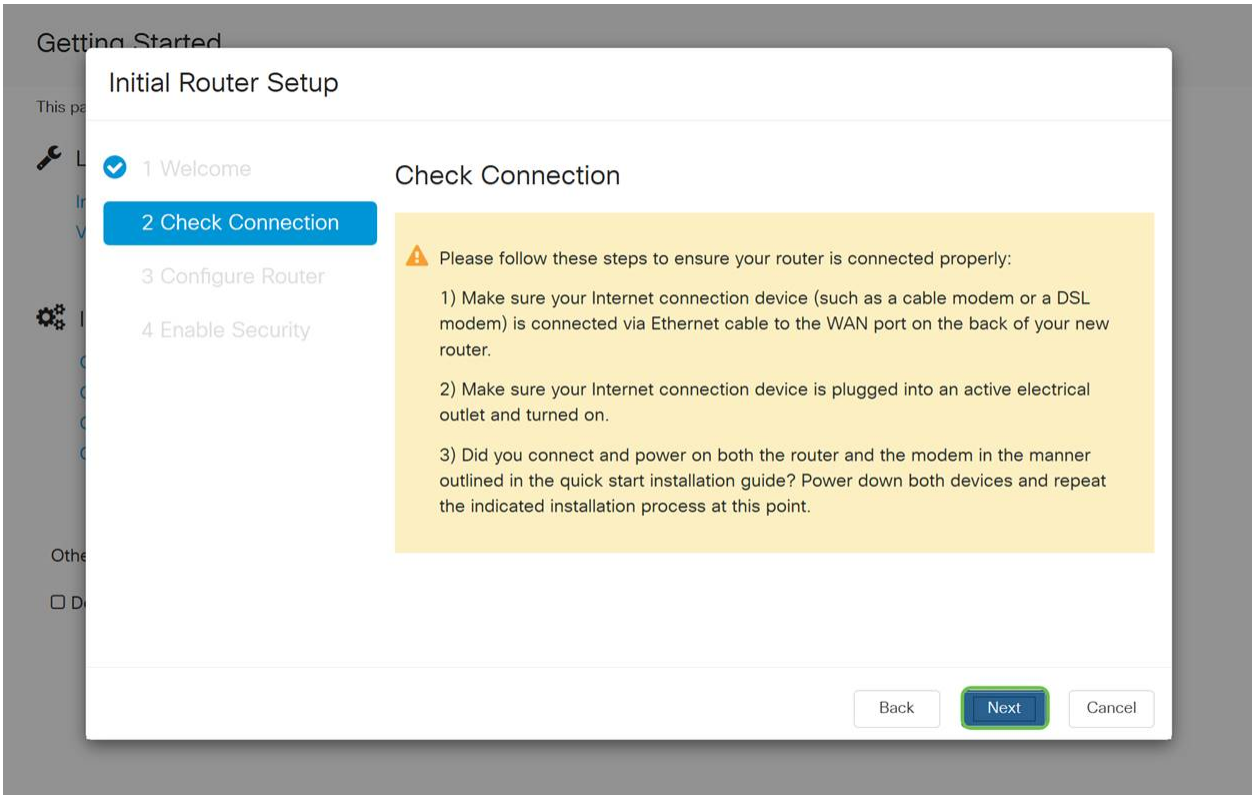
Paso 2

Este paso confirma que los cables están conectados. Como ya lo ha confirmado, haga clic en **Siguiente**.



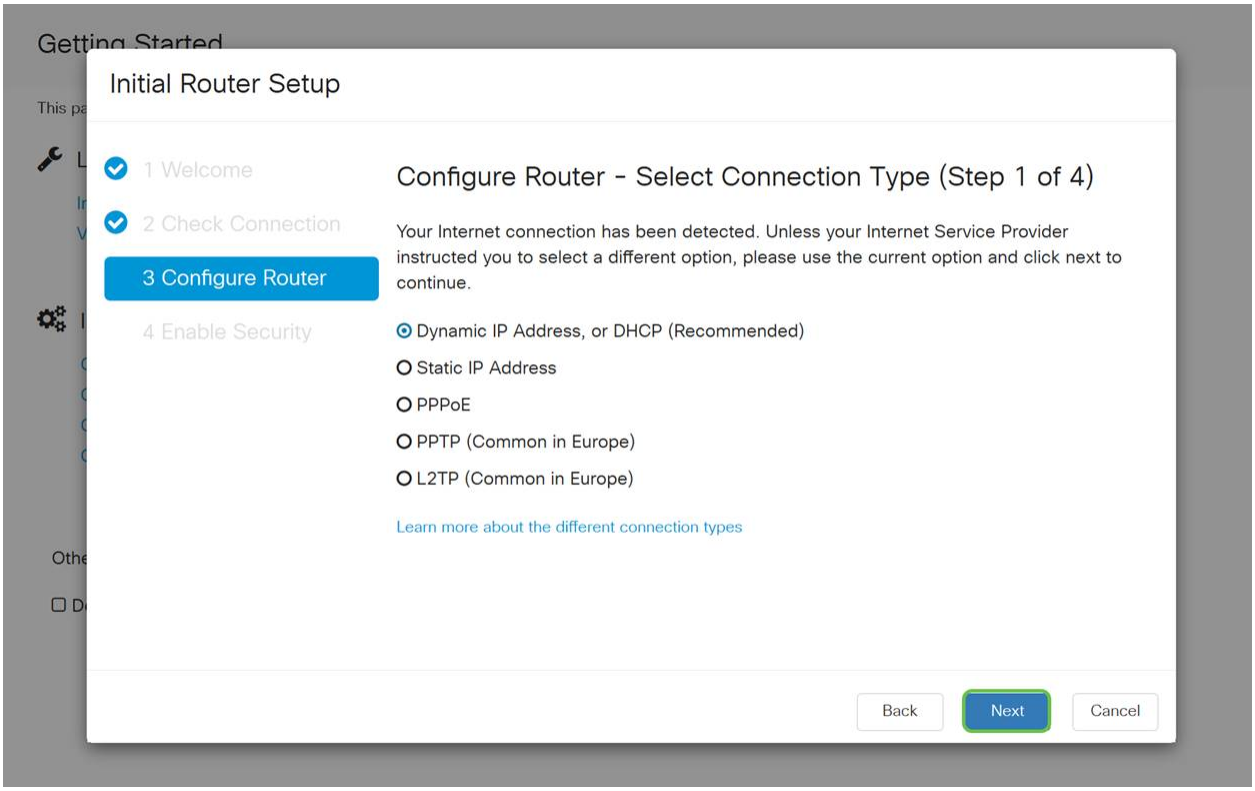
Paso 3

Este paso abarca los pasos básicos para asegurarse de que el router está conectado. Como ya lo ha confirmado, haga clic en **Siguiente**.



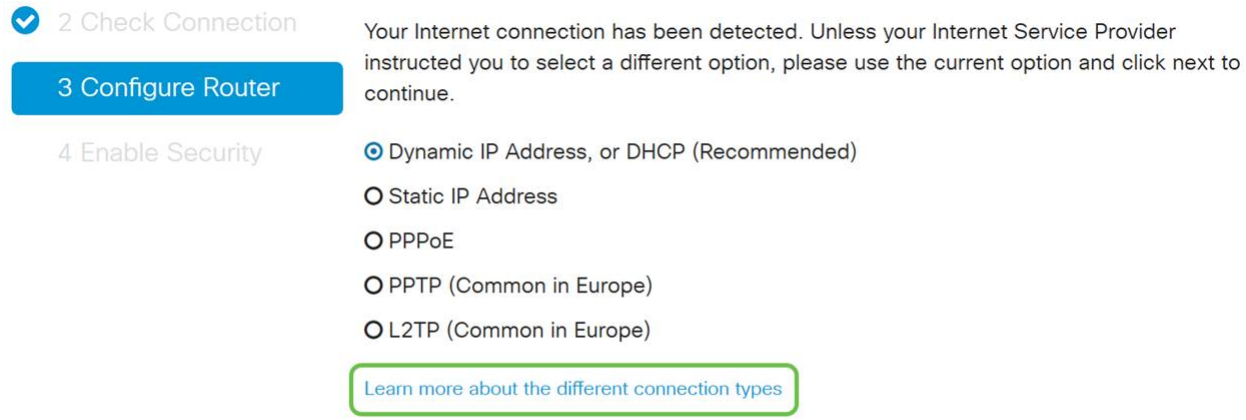
Paso 4

La siguiente pantalla muestra las opciones para asignar direcciones IP al router. Debe seleccionar DHCP en este escenario. Haga clic en Next (Siguiente).



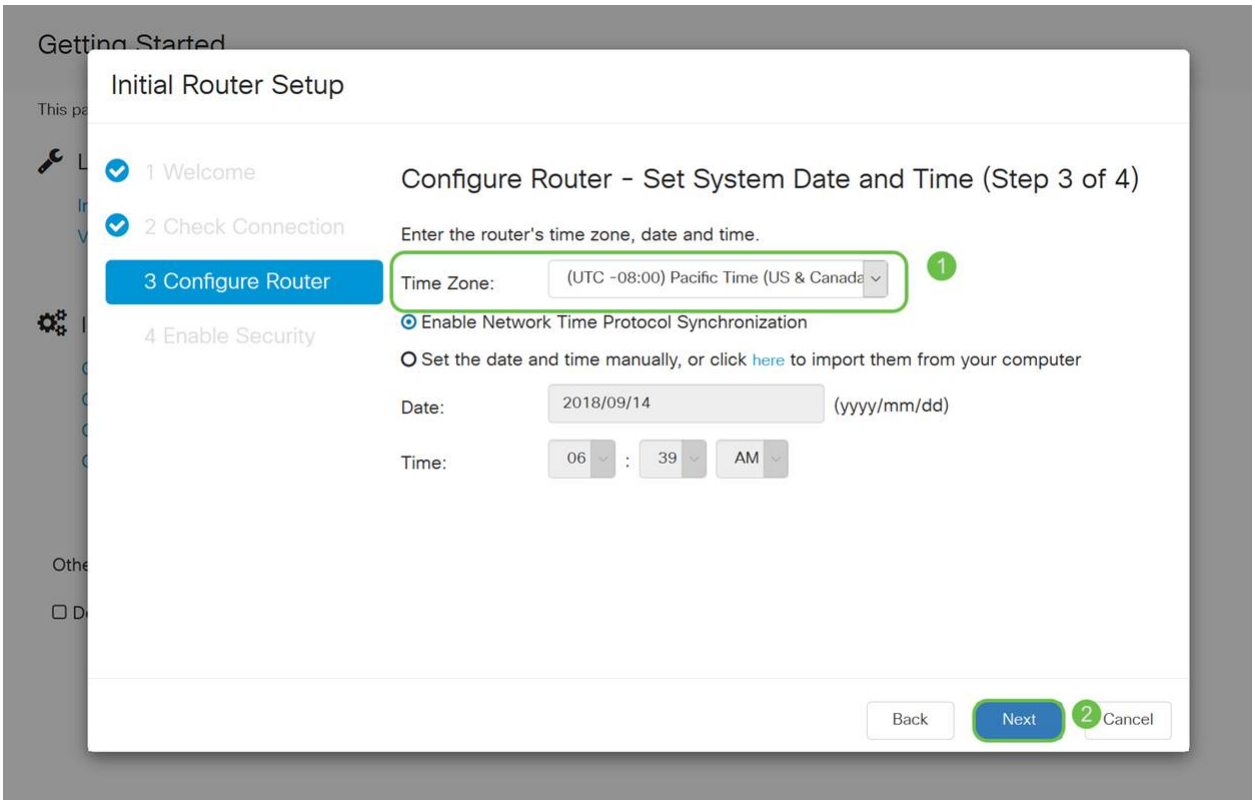
Aunque debe utilizar DHCP para esta configuración inicial, puede seleccionar para *obtener más información sobre los diferentes tipos de conexión* hacia la parte inferior de la pantalla y la referencia futura. Para obtener más información al respecto, consulte los siguientes artículos:

- Configuración de WAN en dispositivos RV160x y RV260x
- Configuración del Ruteo Estático en RV160 y RV260



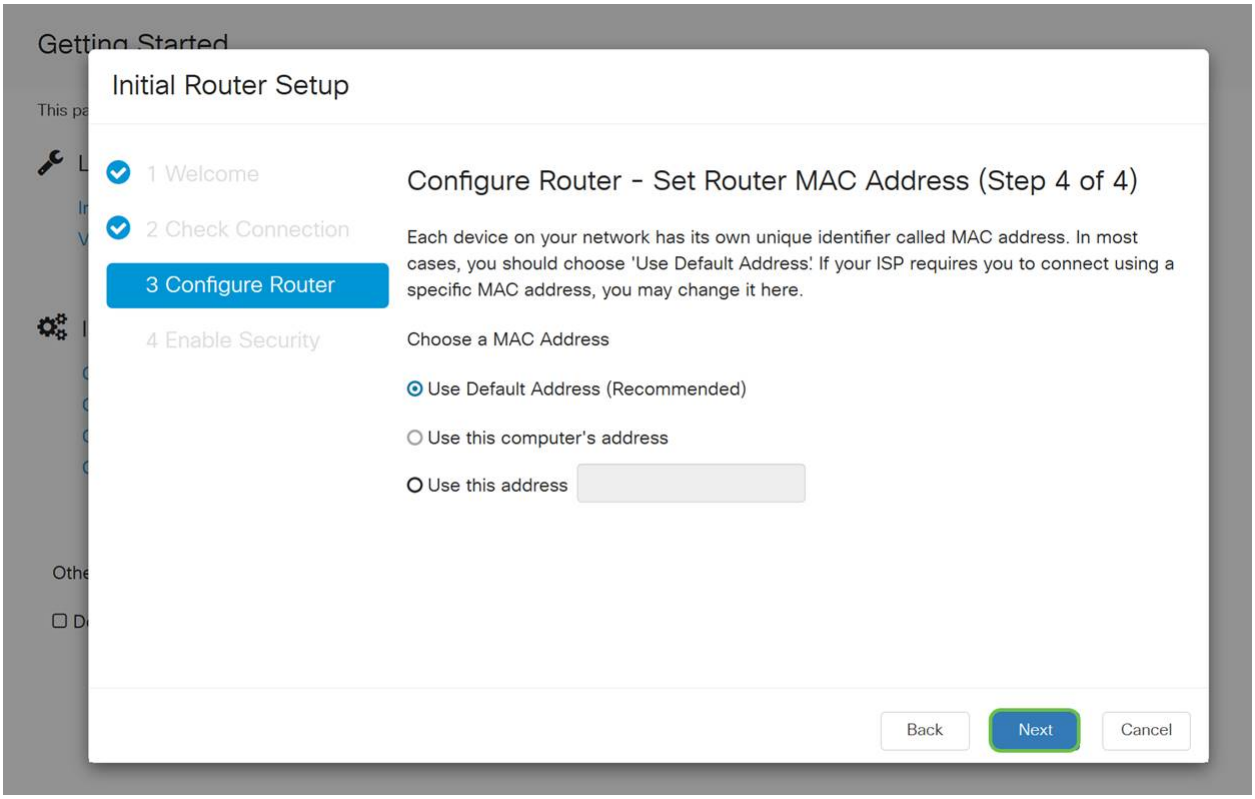
Paso 5

Aquí se le solicitará que establezca los parámetros de hora del router. Esto es importante porque permite la precisión al revisar registros o solucionar eventos. Seleccione su **zona horaria** y haga clic en **Siguiente**.



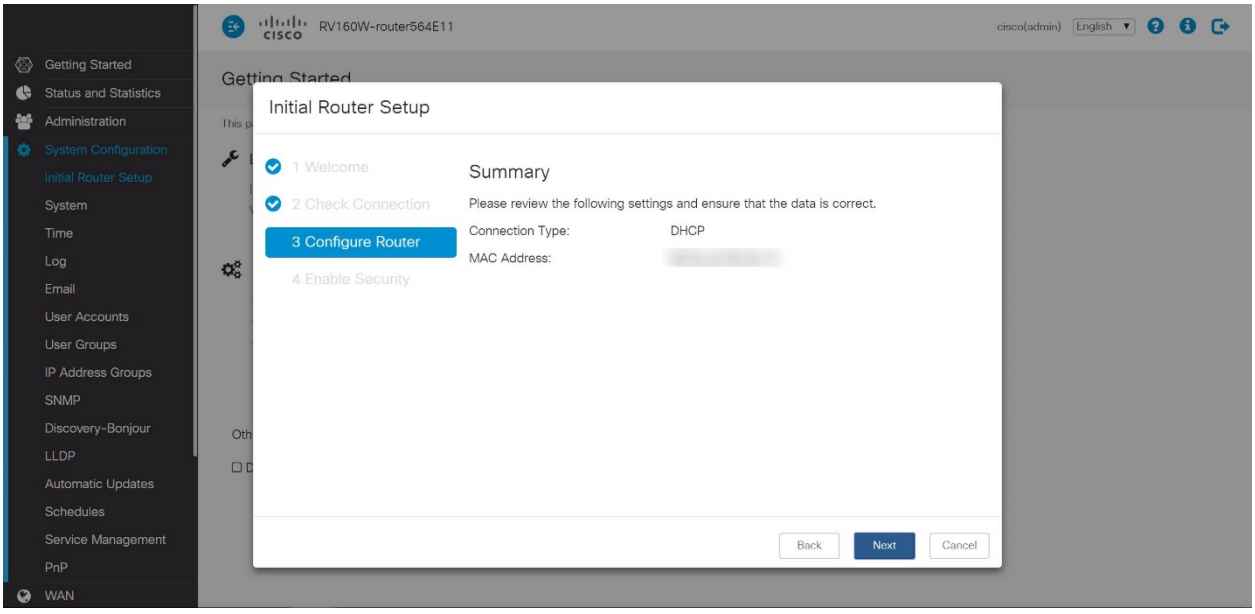
Paso 6

En esta pantalla, seleccionará las direcciones MAC que desea asignar a los dispositivos. La mayoría de las veces, utilizará la dirección predeterminada. Haga clic en Next (Siguiente).



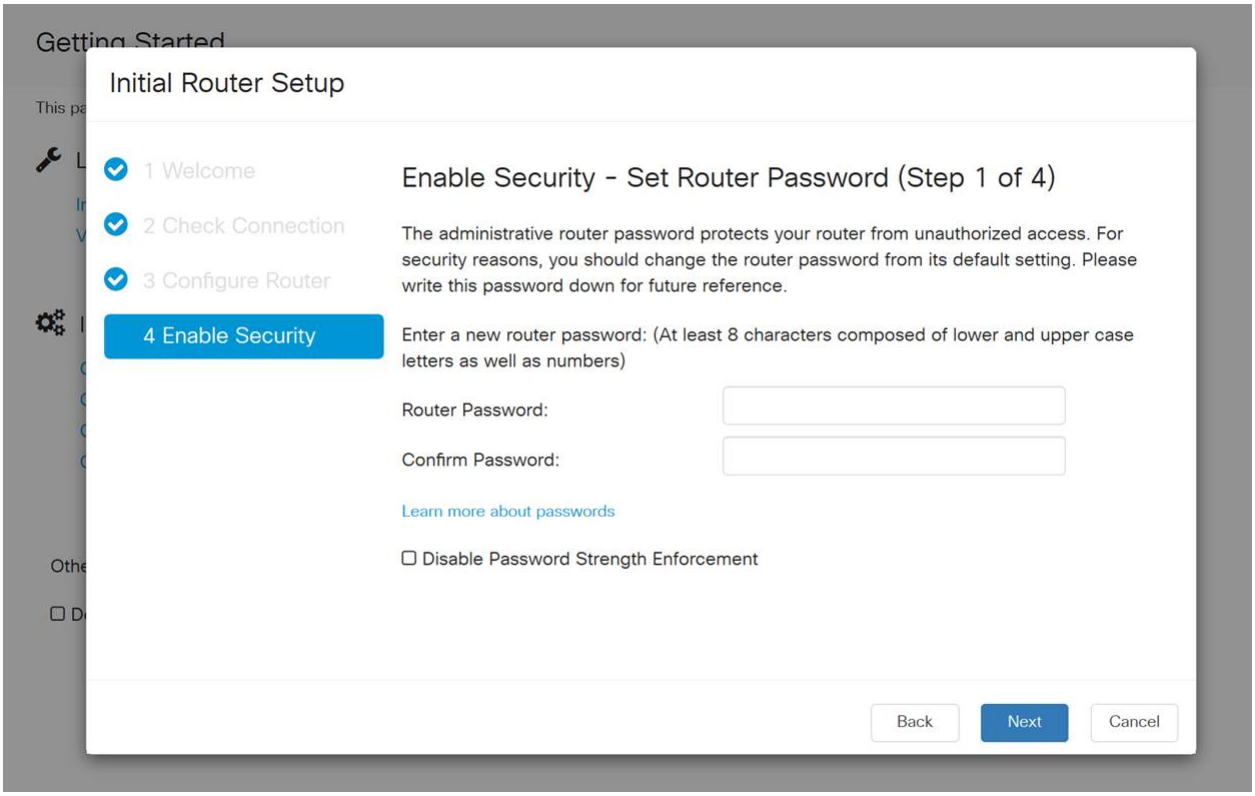
Paso 7

La página siguiente es un resumen de las opciones seleccionadas. Revise y haga clic en **Siguiente** si está satisfecho.



Paso 8

Para el paso siguiente, seleccionará una contraseña que se utilizará al iniciar sesión en el router. El estándar para las contraseñas debe contener al menos 8 caracteres (mayúsculas y minúsculas) e incluir números. **Introduzca una contraseña** que cumpla los requisitos de resistencia. Haga clic en Next (Siguiente). Tenga en cuenta su contraseña para los inicios de sesión futuros.



No se recomienda que seleccione Desactivar *aplicación de fuerza de contraseña*. Esta opción le permitiría seleccionar una contraseña tan simple como 123, que sería tan fácil como 1-2-3 para que los sujetos malintencionados se desmoronaran.

Paso 9

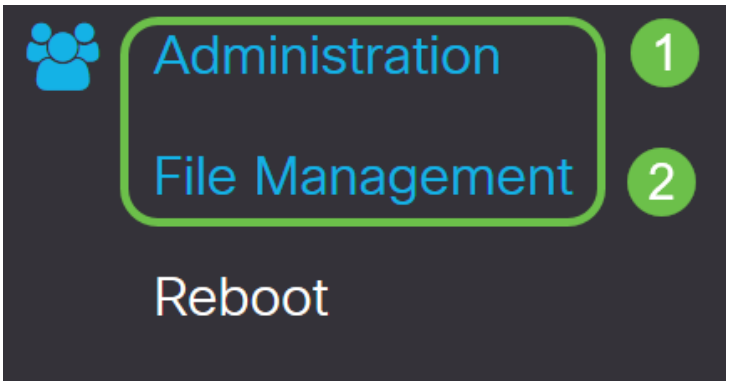
Haga clic en el **icono Guardar**.

Actualización del firmware si es necesario

Esta es una sección importante, ¡no lo omita!

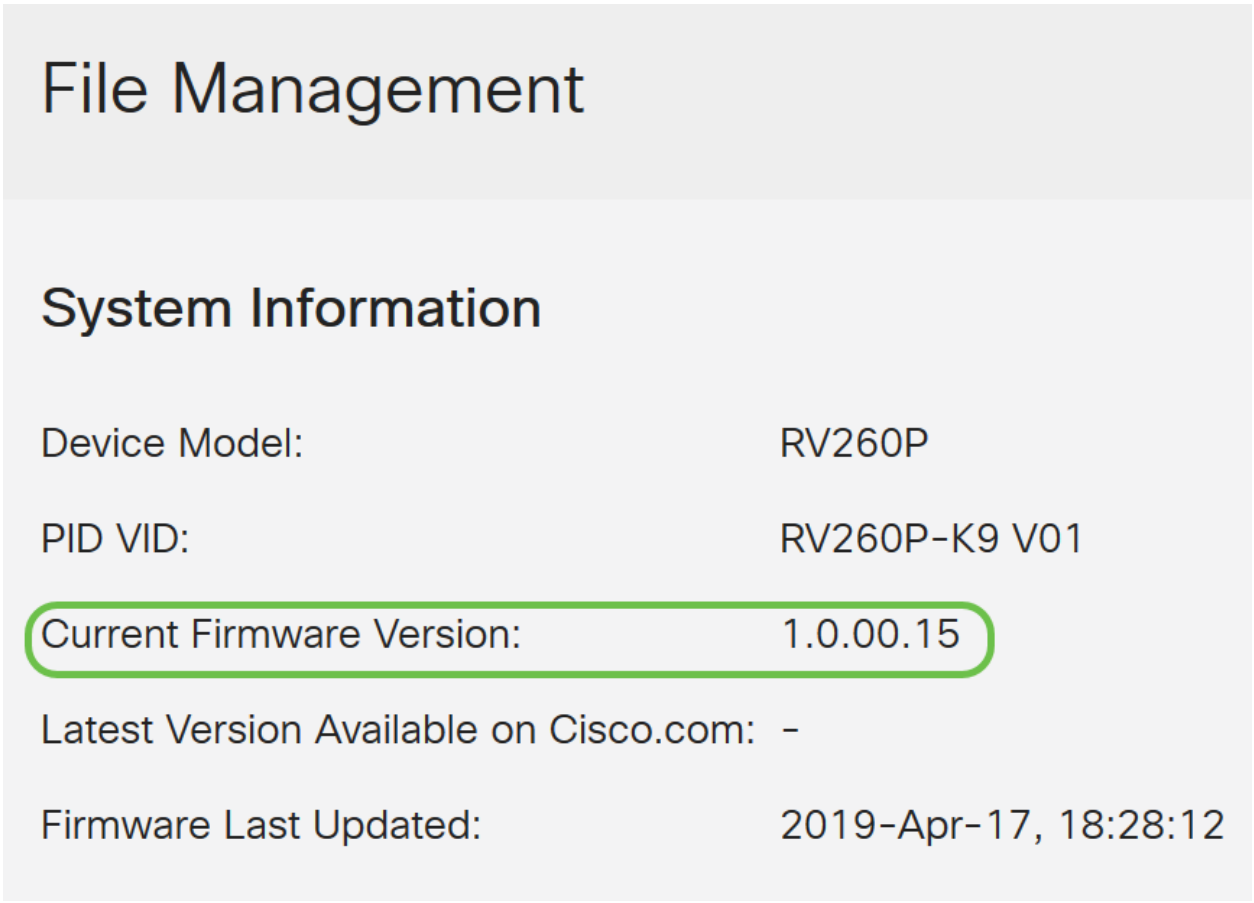
Paso 1

Elija **Administration > File Management**.



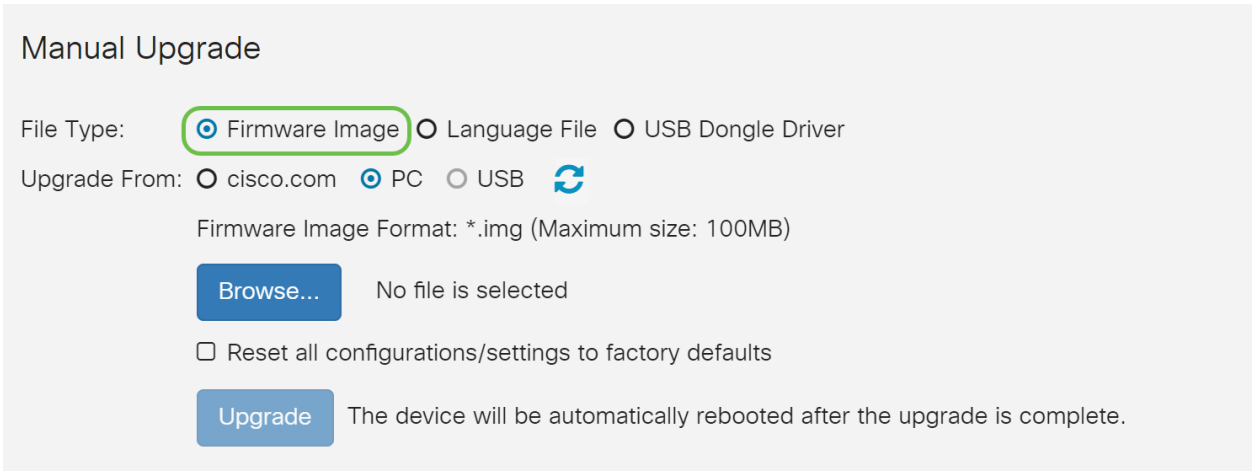
En el área *Información del sistema*, las siguientes subáreas describen lo siguiente:

- Device Model (Modelo de dispositivo): Muestra el modelo del dispositivo.
- PID VID: ID de producto e ID de proveedor del router.
- Versión actual del firmware: firmware que se está ejecutando actualmente en el dispositivo.
- Última versión disponible en Cisco.com: última versión del software disponible en el sitio web de Cisco.
- Última actualización del firmware: fecha y hora de la última actualización del firmware realizada en el router.



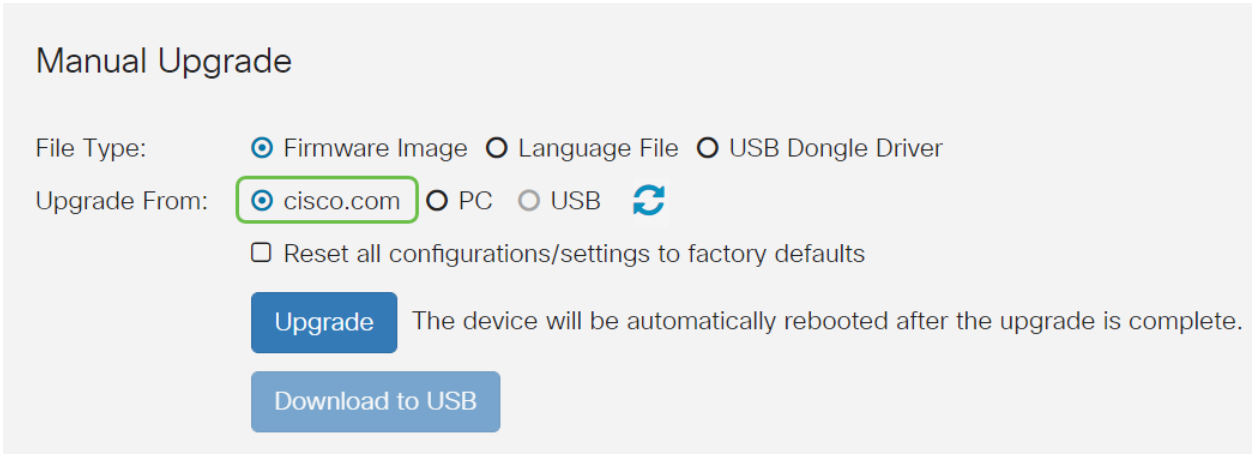
Paso 2

En la sección *Actualización manual*, haga clic en el botón de opción **Firmware Image** para *Tipo de archivo*.



Paso 3

En la página *Actualización manual*, haga clic en un botón de opción para seleccionar cisco.com. Hay otras opciones para esto, pero esta es la manera más fácil de hacer una actualización. Este proceso instala el archivo de actualización más reciente directamente desde la página web Descargas de software de Cisco.

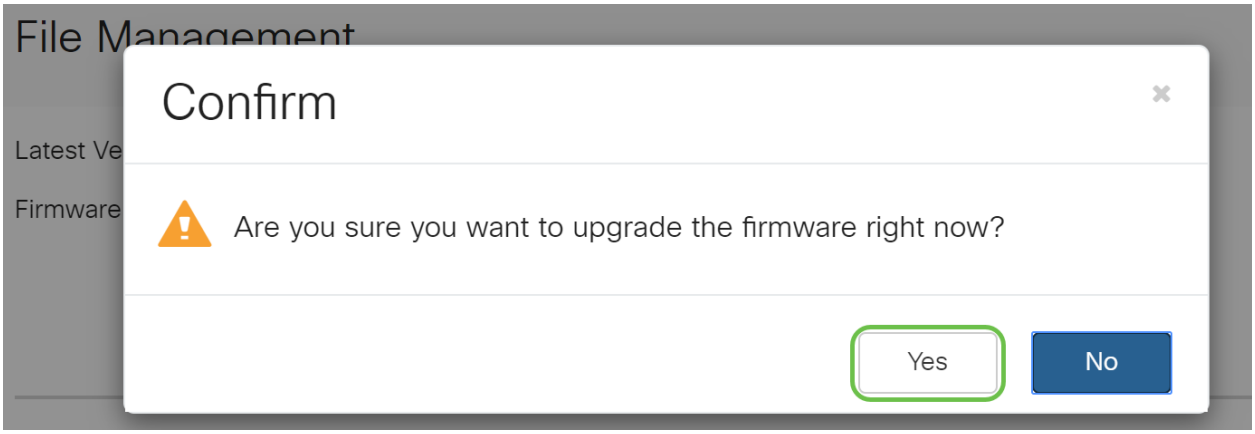


Paso 4

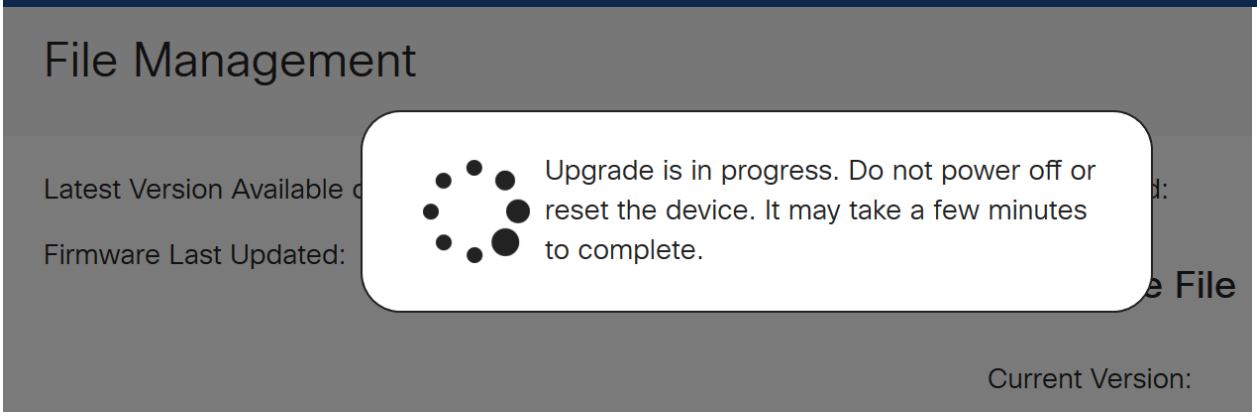
Haga clic en **Upgrade**.

Paso 5

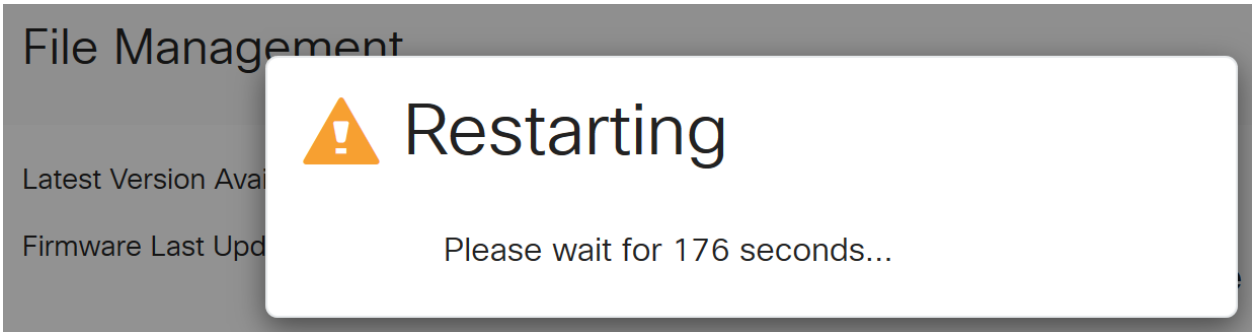
Haga clic en **Yes** en la ventana de confirmación para continuar.



El proceso de actualización debe ejecutarse sin interrupción. Aparece el siguiente mensaje en la pantalla mientras la actualización está en curso.

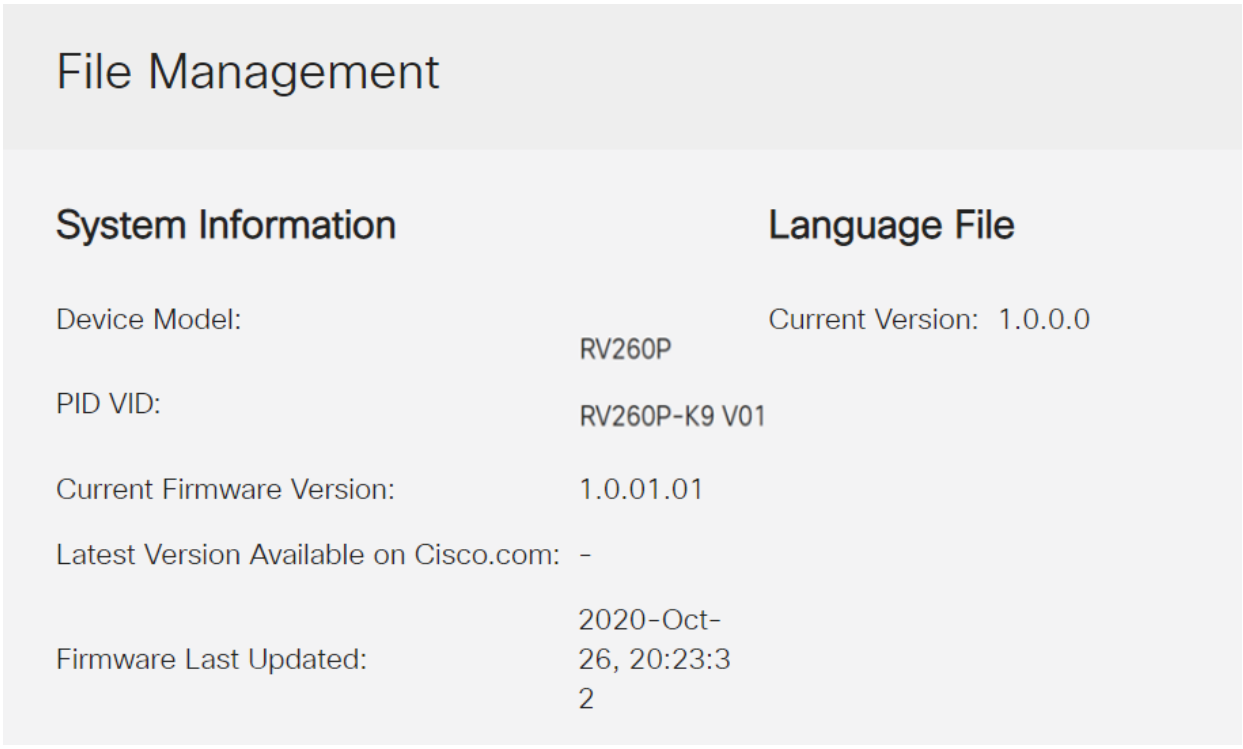


Una vez completada la actualización, aparecerá una ventana de notificación para informarle de que el router se *reiniciará* con una cuenta atrás del tiempo estimado para que el proceso termine. A continuación, se cerrará la sesión.



Paso 6

Vuelva a iniciar sesión en la utilidad basada en Web para verificar que se ha actualizado el firmware del router y desplácese hasta *Información del sistema*. El área *Current Firmware Version* (Versión actual del firmware) ahora debe mostrar la versión actualizada del firmware.



Enhorabuena, los parámetros básicos del router están completos. Hay algunas opciones de configuración en el futuro.

Le animo a que siga navegando por el artículo para obtener más información sobre estas opciones y si se aplican a usted. Si lo prefiere, puede hacer clic en cualquiera de los hipervínculos para saltar a una sección en su lugar.

- Configuración de VLAN (opcional)
- Editar dirección IP (opcional)
- Agregar direcciones IP estáticas (opcional)
- ¡Estoy listo para configurar la parte de red inalámbrica de malla de mi red!

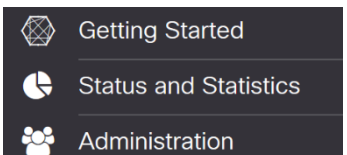
Configuración de VLAN (opcional)

Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En los escenarios donde los datos confidenciales se pueden difundir en una red, se pueden crear VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Las VLAN también se pueden utilizar para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusión a destinos innecesarios. Puede crear una VLAN, pero esto no tendrá efecto hasta que la VLAN esté conectada al menos a un puerto, ya sea manual o dinámicamente. Los puertos siempre deben pertenecer a una o más VLAN.

Si no desea crear VLAN, puede saltar a la siguiente sección.

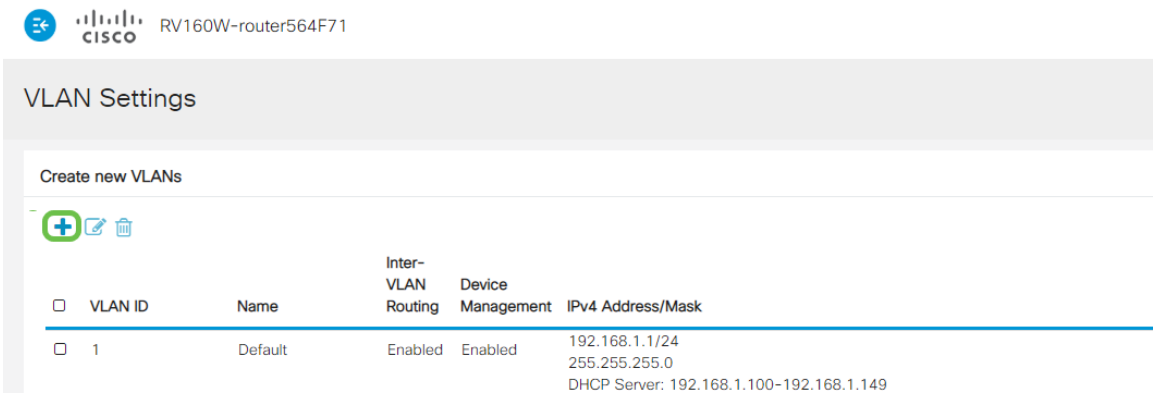
Paso 1

Vaya a **LAN > VLAN Settings**.



Paso 2

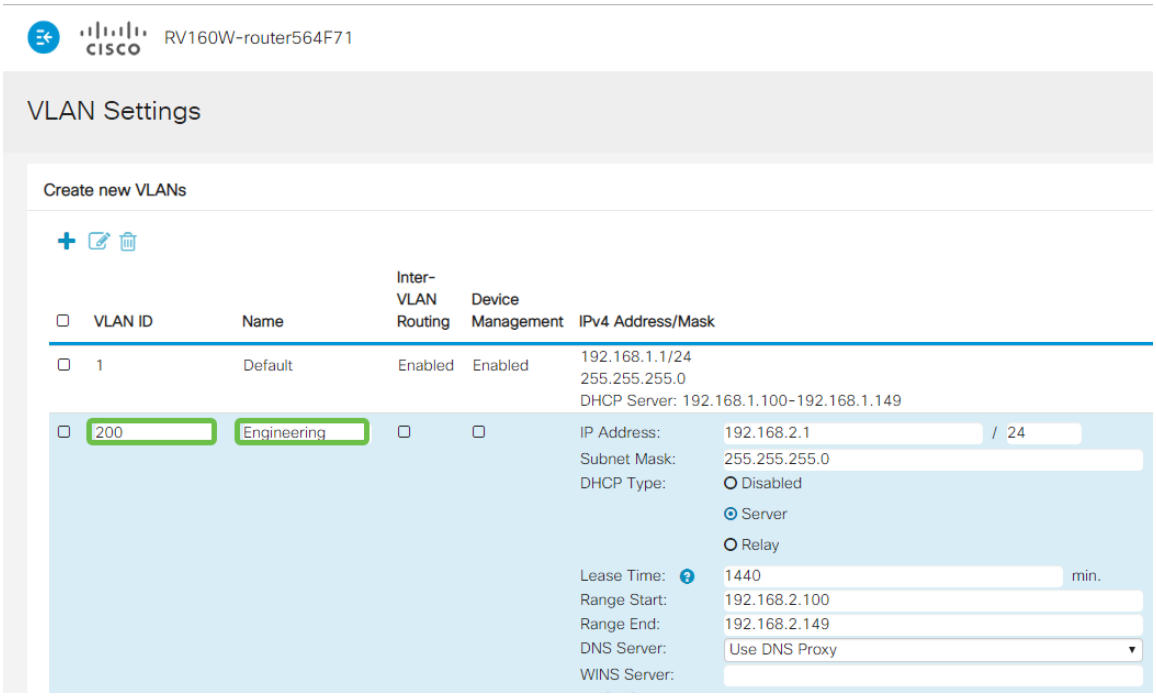
Haga clic en **Agregar** para crear una nueva VLAN.



Paso 3

Ingrese el *ID de VLAN* que desea crear y un *Nombre* para él. El rango de *ID de VLAN* es del 1 al 4093.

Ingresamos **200** como *ID de VLAN* e **Ingeniería** como *Nombre* para la VLAN.



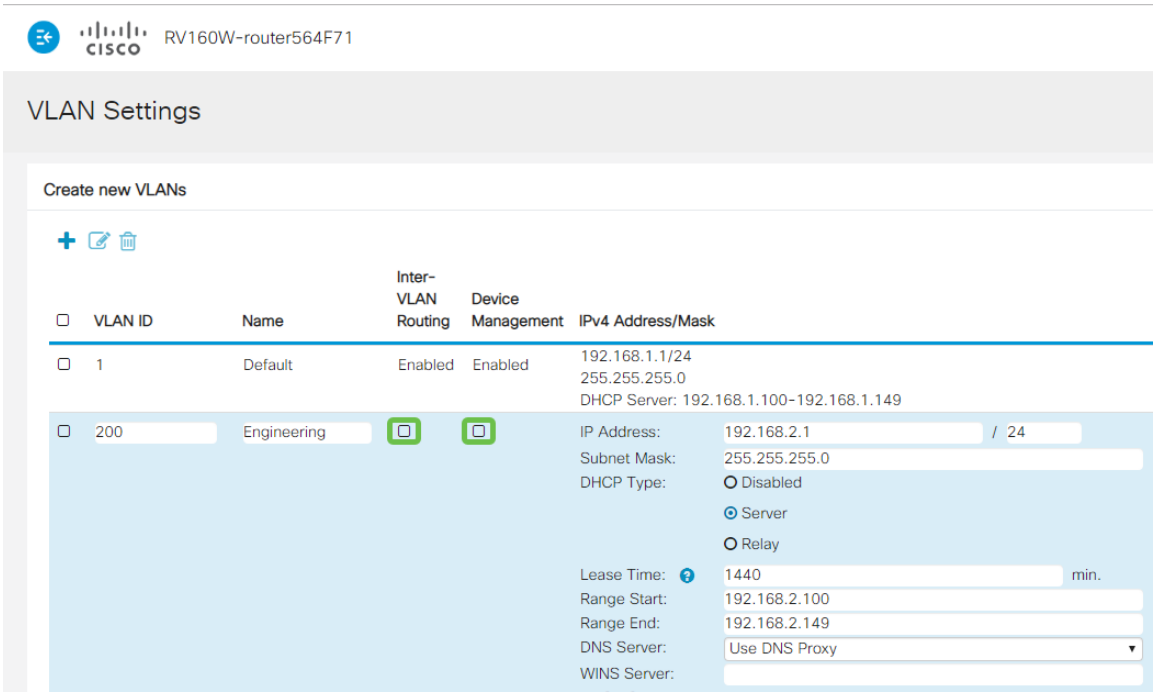
Paso 4

Desmarque la casilla *Enabled* para *Inter-VLAN Routing* y *Device Management* si lo desea.

El ruteo entre VLAN se utiliza para rutear paquetes de una VLAN a otra VLAN. En general, esto no se recomienda para las redes de invitados, ya que querrá aislar a los usuarios invitados, ya que deja las VLAN menos seguras. Hay momentos en los que puede ser necesario que las VLAN ruteen entre sí. Si este es el caso, desproteja Inter-VLAN Routing en un RV34x Router con Restricciones de ACL Dirigidas para configurar el tráfico específico que permite entre VLAN.

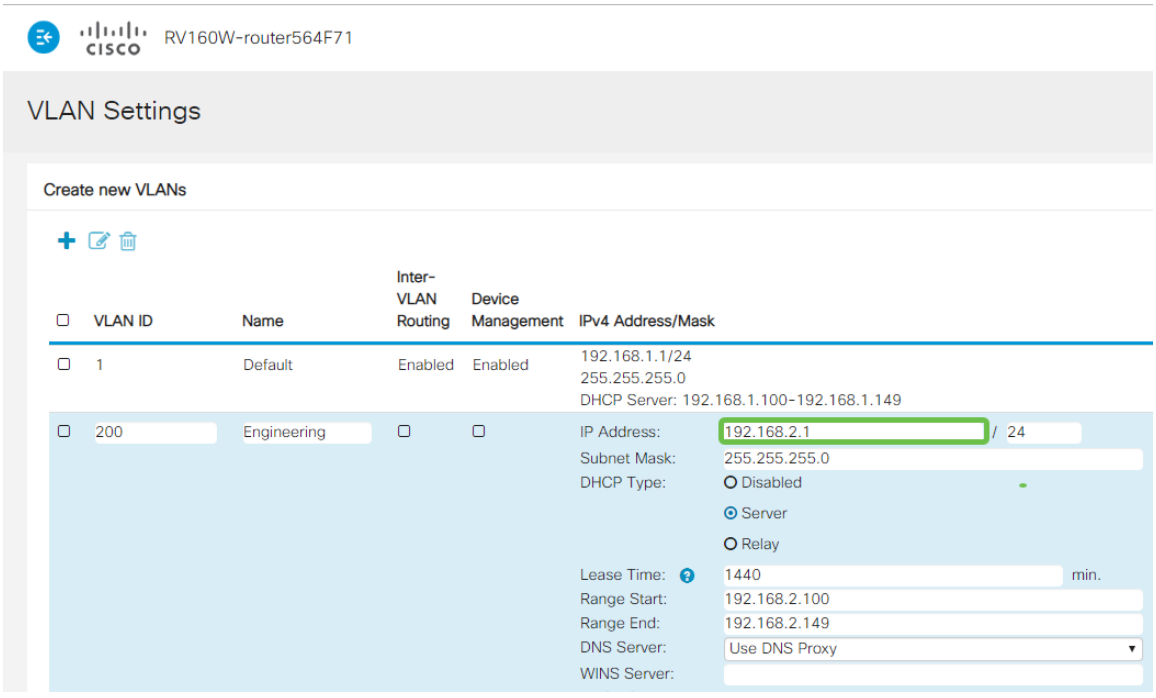
Device Management es el software que le permite utilizar el explorador para iniciar sesión en la interfaz de usuario web del RV260P, desde la VLAN y administrar el RV260P. Esto también debe desactivarse en las redes de invitado.

En este ejemplo, no habilitamos *Inter-VLAN Routing* ni *Device Management* para mantener la VLAN más segura.



Paso 5

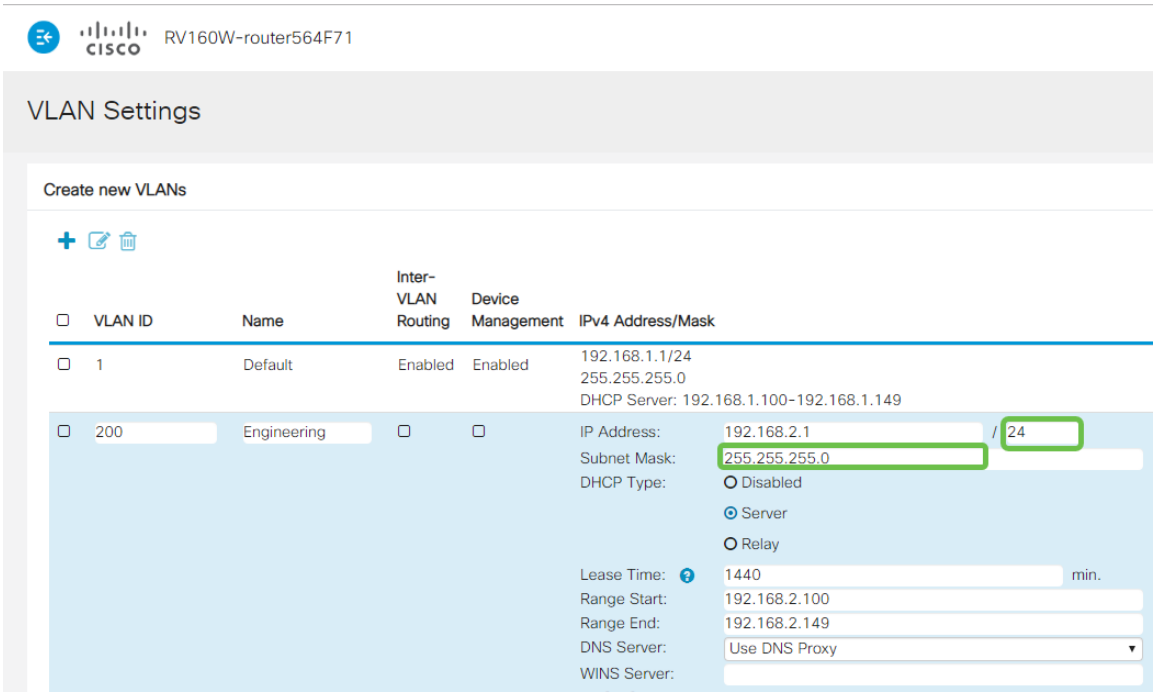
La dirección IPv4 privada se rellenará automáticamente en el campo *Dirección IP*. Puede ajustar esto si lo desea. En este ejemplo, la subred tiene direcciones IP 192.168.2.100-192.168.2.149 disponibles para DHCP. 192.168.2.1-192.168.2.99 y 192.168.2.150-192.168.2.254 están disponibles para las direcciones IP estáticas.



Paso 6

La máscara de subred bajo *Máscara de subred* se rellenará automáticamente. Si realiza cambios, el campo se ajustará automáticamente.

Para esta demostración, dejaremos la *máscara de subred* como **255.255.255.0** o **/24**.



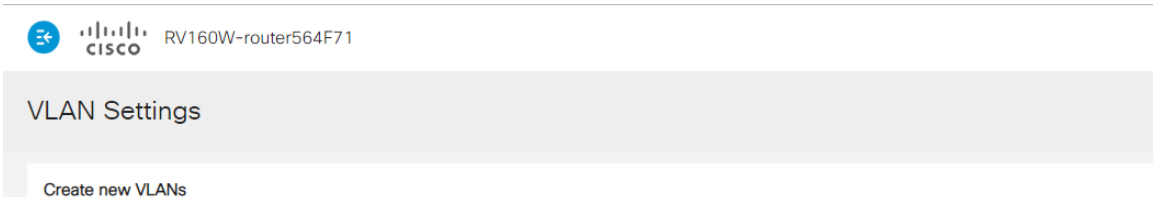
Paso 7

Seleccione un *tipo de protocolo de configuración dinámica de host (DHCP)*. Las siguientes opciones son:

Desactivado: desactiva el servidor DHCP IPv4 en VLAN. Esto se recomienda en un entorno de prueba. En este escenario, todas las direcciones IP tendrían que configurarse manualmente y toda la comunicación sería interna.

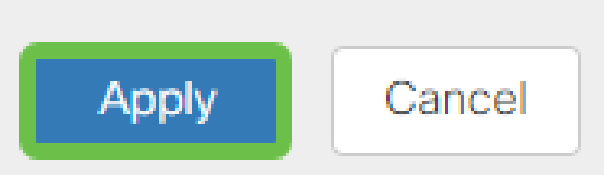
Servidor: esta es la opción más utilizada.

- Tiempo de concesión: introduzca un valor de tiempo de 5 a 43 200 minutos. El valor predeterminado es 1440 minutos (igual a 24 horas).
- Range Start and Range End (Fin de inicio y intervalo): Introduzca el inicio y el final del intervalo de direcciones IP que se pueden asignar dinámicamente.
- DNS Server (Servidor DNS): Seleccione esta opción para utilizar el servidor DNS como proxy o desde el ISP en la lista desplegable.
- Servidor WINS: introduzca el nombre del servidor WINS.
- Opciones de DHCP:
    - Opción 66: Introduzca la dirección IP del servidor TFTP.
    - Opción 150: Introduzca la dirección IP de una lista de servidores TFTP.
    - Opción 67: Introduzca el nombre del archivo de configuración.
- Relay (Retransmisión): Introduzca la dirección IPv4 del servidor DHCP remoto para configurar el agente de relé DHCP. Esta es una configuración más avanzada.



Paso 8

Haga clic en **Apply** para crear la nueva VLAN.



Asignar VLAN a puertos

Se pueden configurar 16 VLAN en el RV260, con una VLAN para la red de área extensa (WAN). Las VLAN que no están en un puerto deben ser *Excluidas*. Esto mantiene el tráfico en ese puerto exclusivamente para las VLAN/VLAN asignadas específicamente por el usuario. Se considera una práctica óptima.

Los puertos pueden configurarse como puerto de acceso o puerto troncal:

- Puerto de acceso: se ha asignado una VLAN. Se pasan las tramas sin etiquetas.
- Puerto troncal: puede transportar más de una VLAN. 802.1q. El enlace troncal permite que una VLAN nativa se desactive. Las VLAN que no desee en el troncal deben excluirse.

Una VLAN asignó su propio puerto:

- Se considera un puerto de acceso.
- La VLAN que se asigna a este puerto se debe etiquetar como Sin etiquetar.
- El resto de las VLAN se deben etiquetar como Excluidas para ese puerto.

Dos o más VLAN que comparten un puerto:

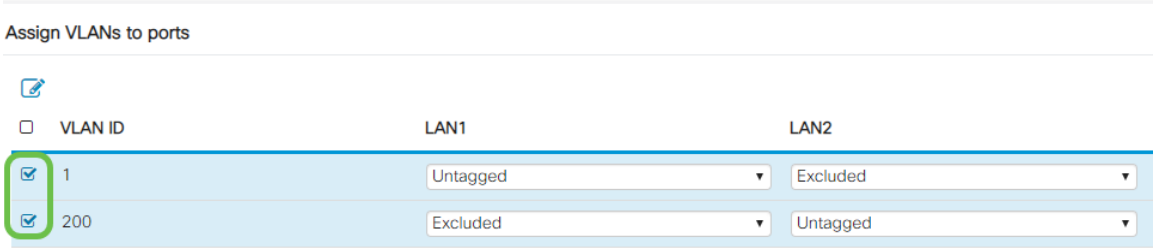
- Se considera un puerto troncal.
- Una de las VLAN se puede etiquetar como Sin etiquetar.
- El resto de las VLAN que forman parte del puerto troncal deben etiquetarse como Etiquetadas.
- Las VLAN que no forman parte del puerto troncal deben etiquetarse como Excluidas para ese puerto.

Nota: En este ejemplo, no hay trunks.

Paso 9

Seleccione los *IDs de VLAN* que desea editar. Haga clic en Editar.

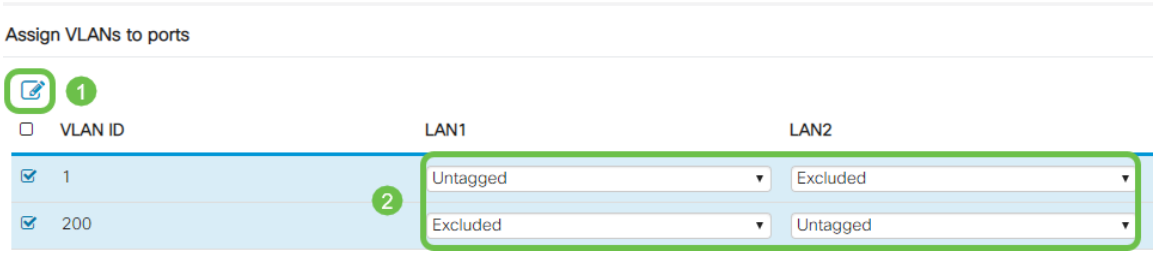
En este ejemplo, hemos seleccionado *VLAN 1* y *VLAN 200*.



Paso 10

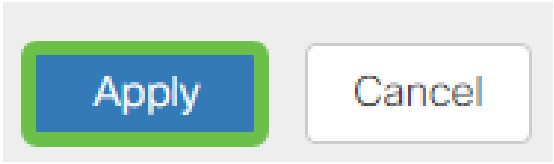
Haga clic en **Editar** para asignar una VLAN a un puerto LAN y especificar cada configuración como *Etiquetado*, *Sin etiquetar* o *Excluido*.

En este ejemplo, en LAN1 asignamos VLAN1 como **Sin etiquetar** y VLAN 200 como **Excluido**. Para LAN2 asignamos VLAN 1 como **Excluded** y VLAN 200 como **Untagged**.



Paso 11

Haga clic en **Aplicar** para guardar la configuración.



Ahora debería haber creado correctamente una nueva VLAN y configurado VLAN en los puertos del RV260. Repita el proceso para crear las otras VLAN. Por ejemplo, VLAN300 se crearía para el marketing con una subred de 192.168.3.x y VLAN400 se crearía para la contabilidad con una subred de 192.168.4.x.

Estos son los fundamentos de las VLAN. Haga clic en el hipervínculo para obtener más información sobre Prácticas recomendadas y consejos de seguridad de VLAN para los routers empresariales de Cisco.

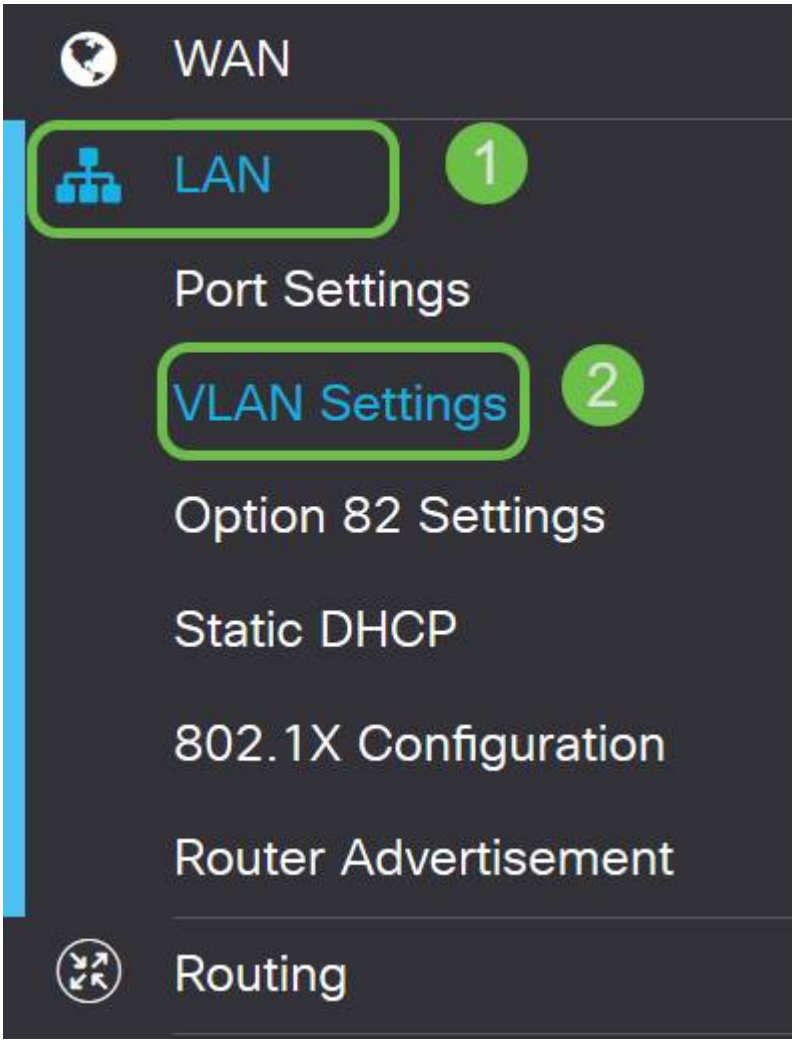
Editar una dirección IP (opcional)

Después de completar el *Asistente de configuración inicial*, puede establecer una dirección IP estática en el router editando los parámetros de VLAN. Omita la ejecución del asistente de configuración inicial. Para realizar este cambio, siga estos pasos.

Si no necesita editar una dirección IP, puede pasar a la siguiente sección de este artículo.

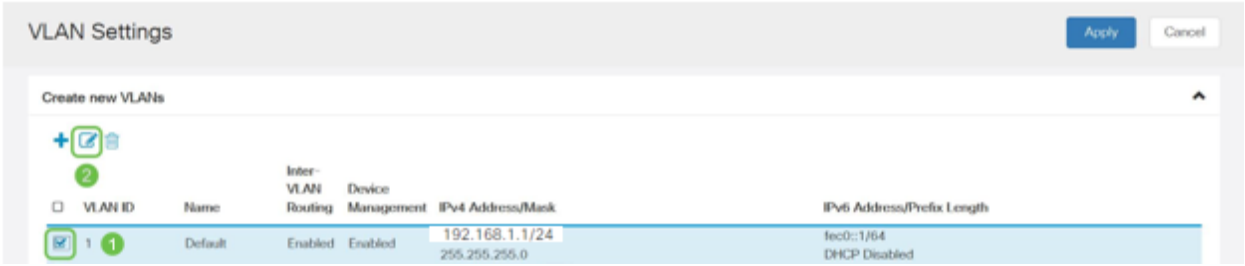
Paso 1

En la barra de menús izquierda, haga clic en **LAN > VLAN Settings**.



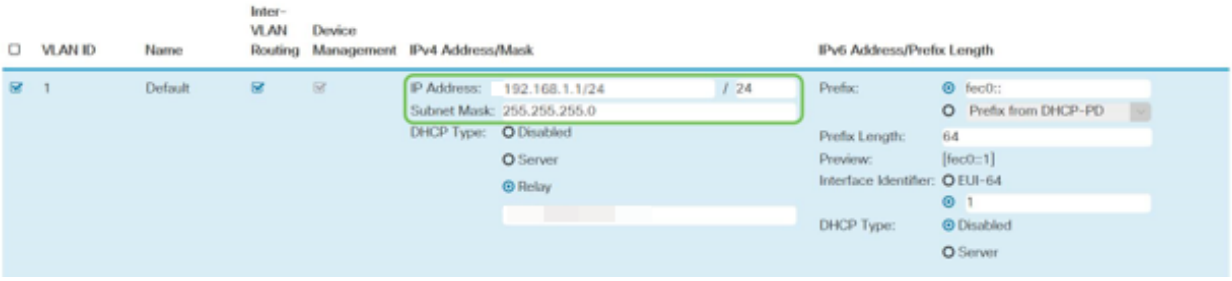
Paso 2

A continuación, seleccione la **VLAN** que contiene su dispositivo de ruteo y luego haga clic en el **icono de edición**.



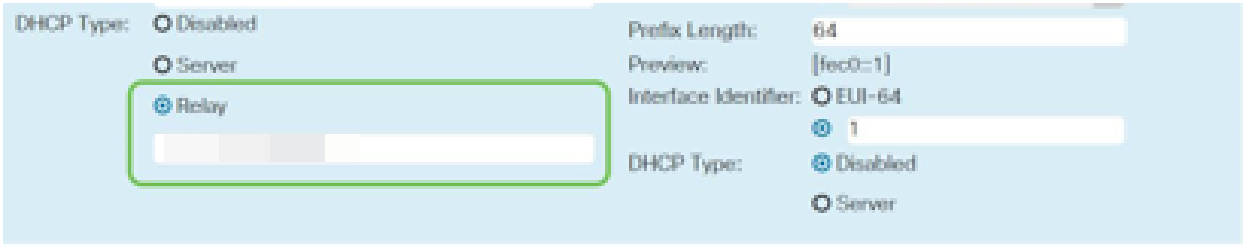
Paso 3

Introduzca la **dirección IP estática** que desee y haga clic en **Aplicar** en la esquina superior derecha.



Paso 4 (opcional)

Si el router no es el servidor/dispositivo DHCP que asigna direcciones IP, puede utilizar la función DHCP Relay para dirigir solicitudes DHCP a una dirección IP específica. Es probable que la dirección IP sea el router conectado a la WAN/Internet.



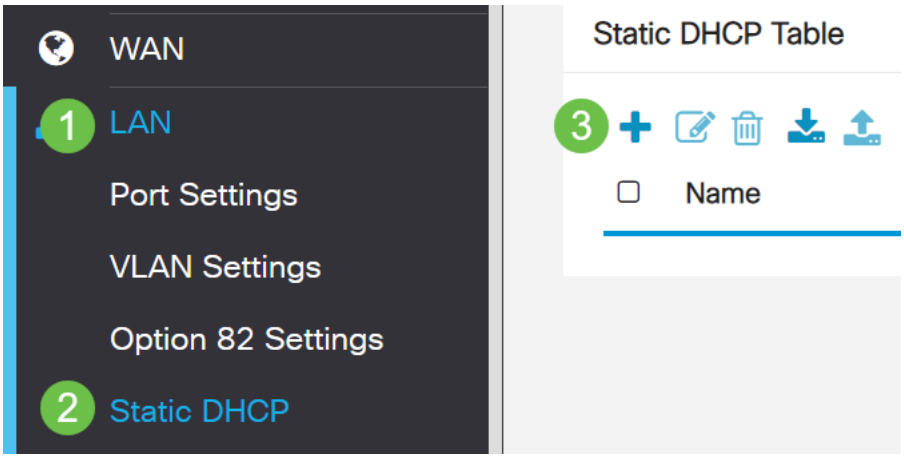
Agregar una IP estática

Si desea que un dispositivo determinado sea accesible a otras VLAN, puede darle una dirección IP local estática a ese dispositivo y crear una regla de acceso para que sea accesible. Esto sólo funciona si se habilita el ruteo entre VLAN. Hay otras situaciones en las que una IP estática puede ser útil. Para obtener más información sobre la configuración de direcciones IP estáticas, consulte Prácticas Recomendadas para Establecer Direcciones IP Estáticas en Cisco Business Hardware.

Si no necesita agregar una dirección IP estática, puede pasar a la siguiente sección de este artículo para configurar los puntos de acceso.

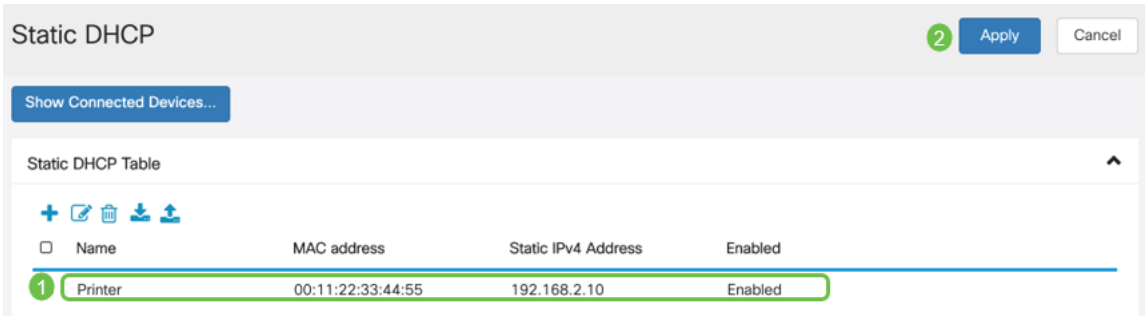
Paso 1

Vaya a **LAN > DHCP estático.** Haga clic en el **icono más**.



Paso 2

Agregue la información **DHCP estático** para el dispositivo. En este ejemplo, el dispositivo es una impresora.



Enhorabuena, ha completado la configuración del router RV260P. Ahora configuraremos sus dispositivos inalámbricos Cisco Business.

Configuración del CBW140AC

CBW140AC fuera de la caja

Comience conectando un cable Ethernet desde el puerto PoE del CBW140AC a un puerto PoE del RV260P. Los primeros 4 puertos del RV260P pueden suministrar PoE, por lo que se puede utilizar cualquiera de ellos.

Compruebe el estado de las luces indicadoras. El punto de acceso tardará unos 10 minutos en iniciarse. 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 de color del LED y el color de la unidad a la unidad. Cuando la luz LED parpadee en verde, vaya al siguiente paso.

El puerto de link ascendente Ethernet PoE en el AP primario SOLAMENTE se puede utilizar para proporcionar un link ascendente a la LAN, y NO para conectarse a cualquier otro dispositivo con capacidad principal o extensor de malla.

Si el punto de acceso no es nuevo, asegúrese de que se restablece a los parámetros predeterminados de fábrica para que el SSID *CiscoBusiness-Setup* aparezca en las opciones Wi-Fi. Para obtener ayuda con esto, consulte Cómo Reiniciar y Restablecer los Parámetros Predeterminados de Fábrica en Routers RV260.

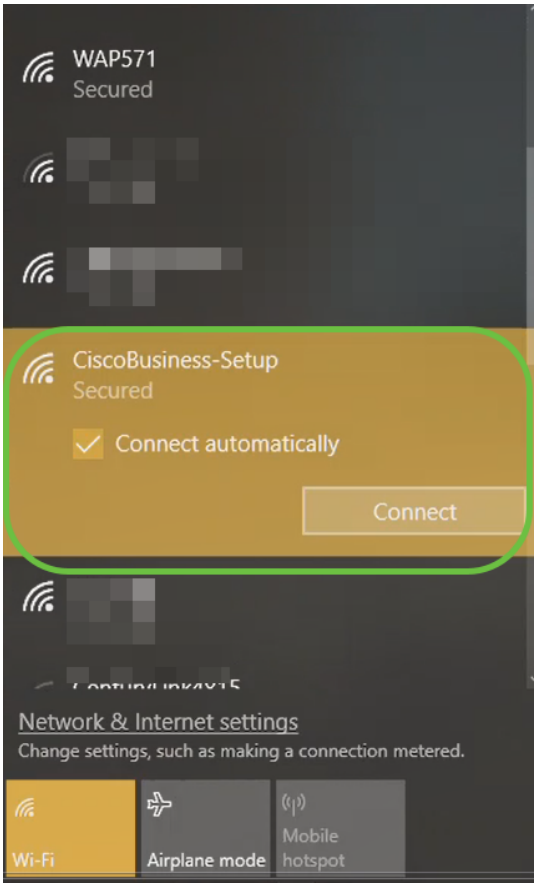
Configuración del punto de acceso inalámbrico primario 140AC en la interfaz de usuario web

Puede configurar el punto de acceso mediante la aplicación móvil o la interfaz de usuario Web. En este artículo se utiliza la interfaz de usuario web para la configuración, que ofrece más opciones de configuración pero es un poco más complicado. Si desea utilizar la aplicación móvil para las siguientes secciones, haga clic para acceder a las instrucciones de la aplicación móvil.

Si tiene problemas para conectarse, consulte la sección Consejos para la resolución de problemas inalámbricos de este artículo.

Paso 1

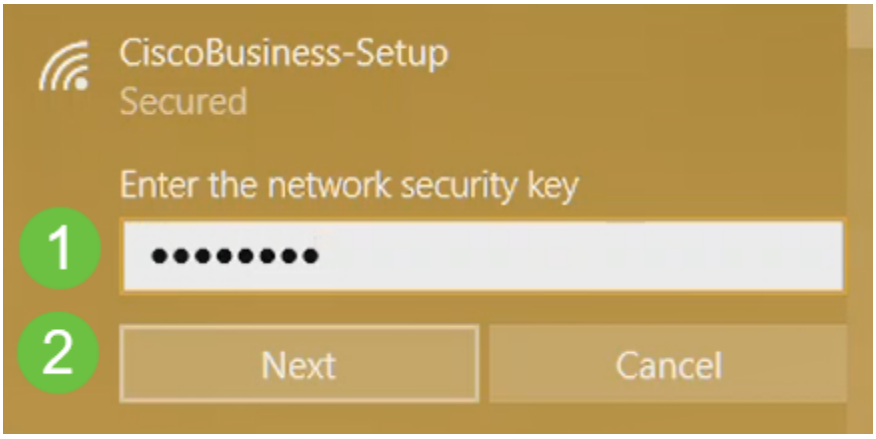
En el PC, haga clic en el **icono Wi-Fi** y elija la red inalámbrica *Cisco Business-Setup*. Haga clic en Connect (Conectar)



Si el punto de acceso no es nuevo, asegúrese de que se restablece a los parámetros predeterminados de fábrica para que el SSID *CiscoBusiness-Setup* aparezca en las opciones Wi-Fi.

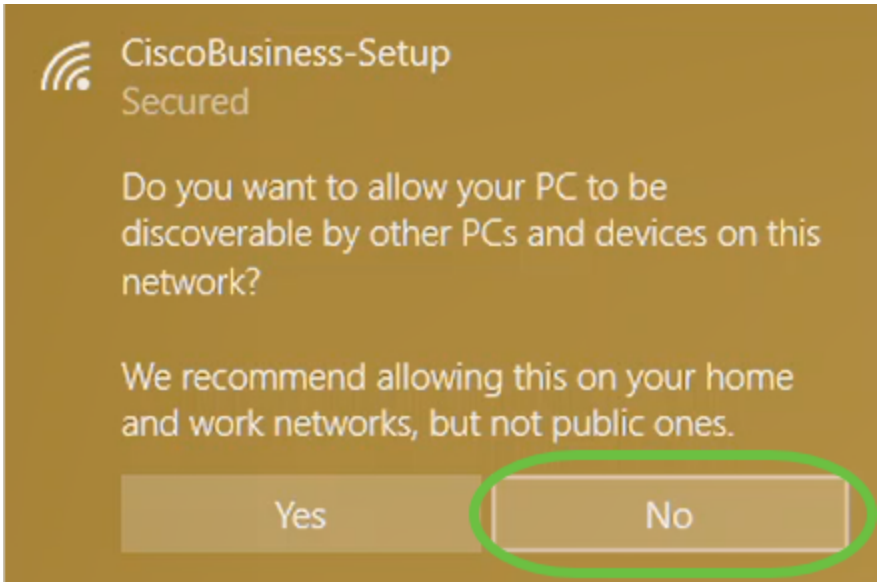
Paso 2

Introduzca la frase de paso **cisco123** y haga clic en **Next**.



Paso 3

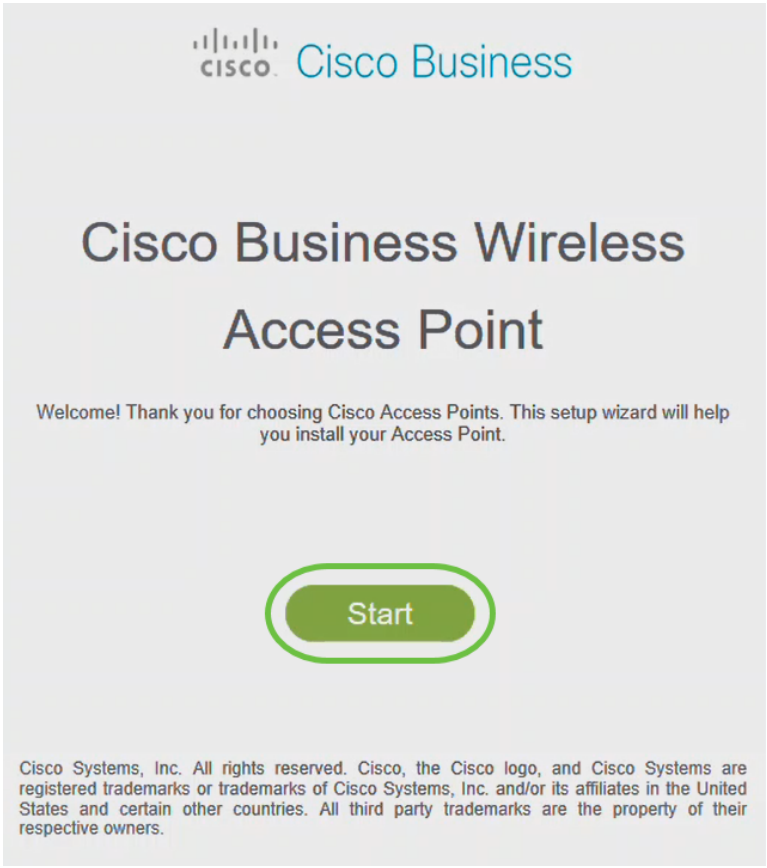
Aparecerá la siguiente pantalla. Dado que sólo puede configurar un dispositivo a la vez, haga clic en **No**.



Sólo se puede conectar un dispositivo al SSID *CiscoBusiness-Setup*. Si un segundo dispositivo intenta conectarse, no podrá hacerlo. Si no puede conectarse al SSID y ha validado la contraseña, es posible que otro dispositivo haya realizado la conexión. Reinicie el AP e inténtelo de nuevo.

Paso 4

Una vez conectado, el navegador web debe redirigir automáticamente al asistente de configuración de CBW AP. Si no es así, abra un explorador Web, como Internet Explorer, Firefox, Chrome o Safari. En la barra de direcciones, escriba **http://ciscobusiness.cisco** y presione **Enter**. Haga clic en **Inicio** en la página web.



Si no ve la página web, espere unos minutos más o vuelva a cargarla. Después de esta configuración inicial, utilizará https://ciscobusiness.cisco para iniciar sesión. Si su navegador web se rellena automáticamente con *http://*, debe escribir manualmente en *https://* para obtener acceso.

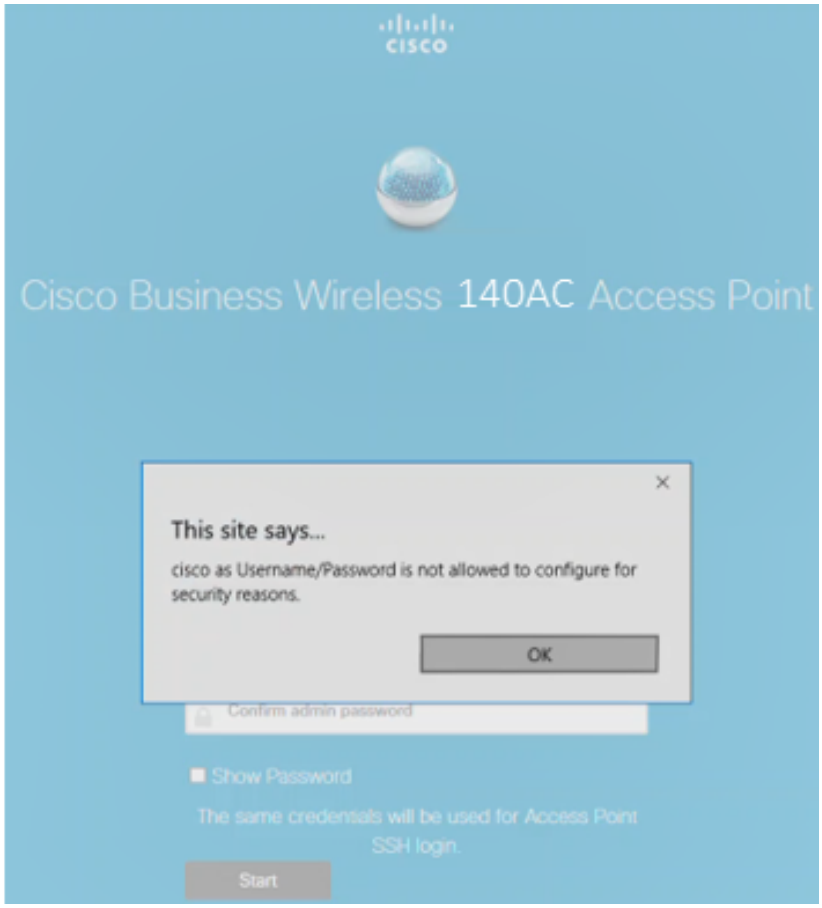
Paso 5

Cree una *cuenta de administrador* introduciendo lo siguiente:

- Nombre de usuario del administrador (máximo de 24 caracteres)
- Contraseña del administrador
- Confirmar contraseña de administrador

Puede optar por mostrar la contraseña activando la casilla de verificación junto a *Mostrar contraseña*. Haga clic en Start (Inicio).

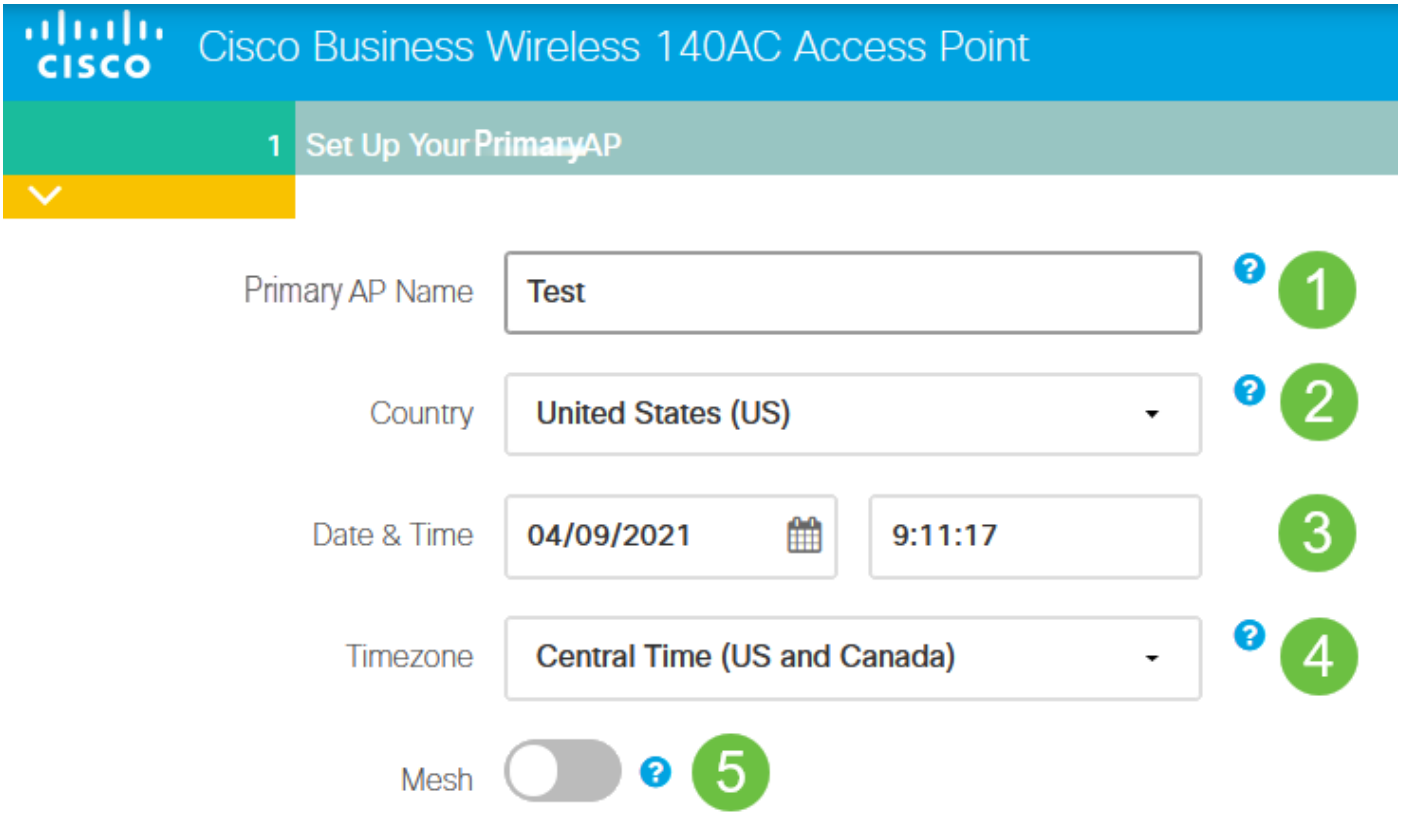
No utilice *cisco*, ni las variaciones en los campos de nombre de usuario o contraseña. Si lo hace, recibirá un mensaje de error como se muestra a continuación.



Paso 6

Configure su AP primario ingresando lo siguiente:

- Nombre del AP principal
- País
- Fecha y hora
- Zona horaria
- Malla



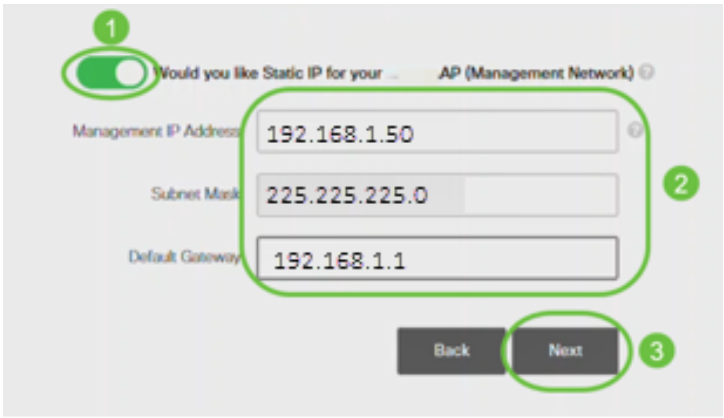
La malla sólo debe estar habilitada si planea crear una red de malla. De forma predeterminada, está desactivado.

Paso 7

(Opcional) Puede habilitar *Static IP para su* CBW140AC para fines de administración. Si no es así, la interfaz obtiene una dirección IP del servidor DHCP. Para configurar la IP estática, introduzca lo siguiente:

- Dirección IP de administración
- Máscara de subnet
- Gateway predeterminado

Haga clic en Next (Siguiente).



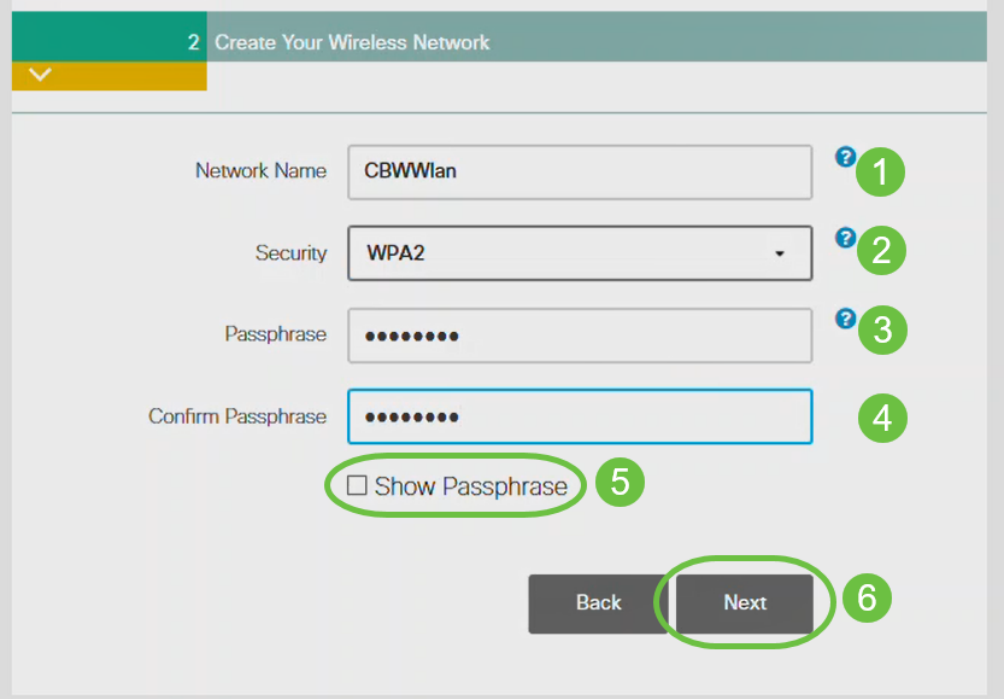
De forma predeterminada, esta opción está desactivada.

Paso 8

Cree sus redes inalámbricas introduciendo lo siguiente:

- Nombre de red
- Elegir seguridad
- Frase de paso
- Confirmar frase de paso
- (Opcional) Active la casilla de verificación para Mostrar frase de paso.

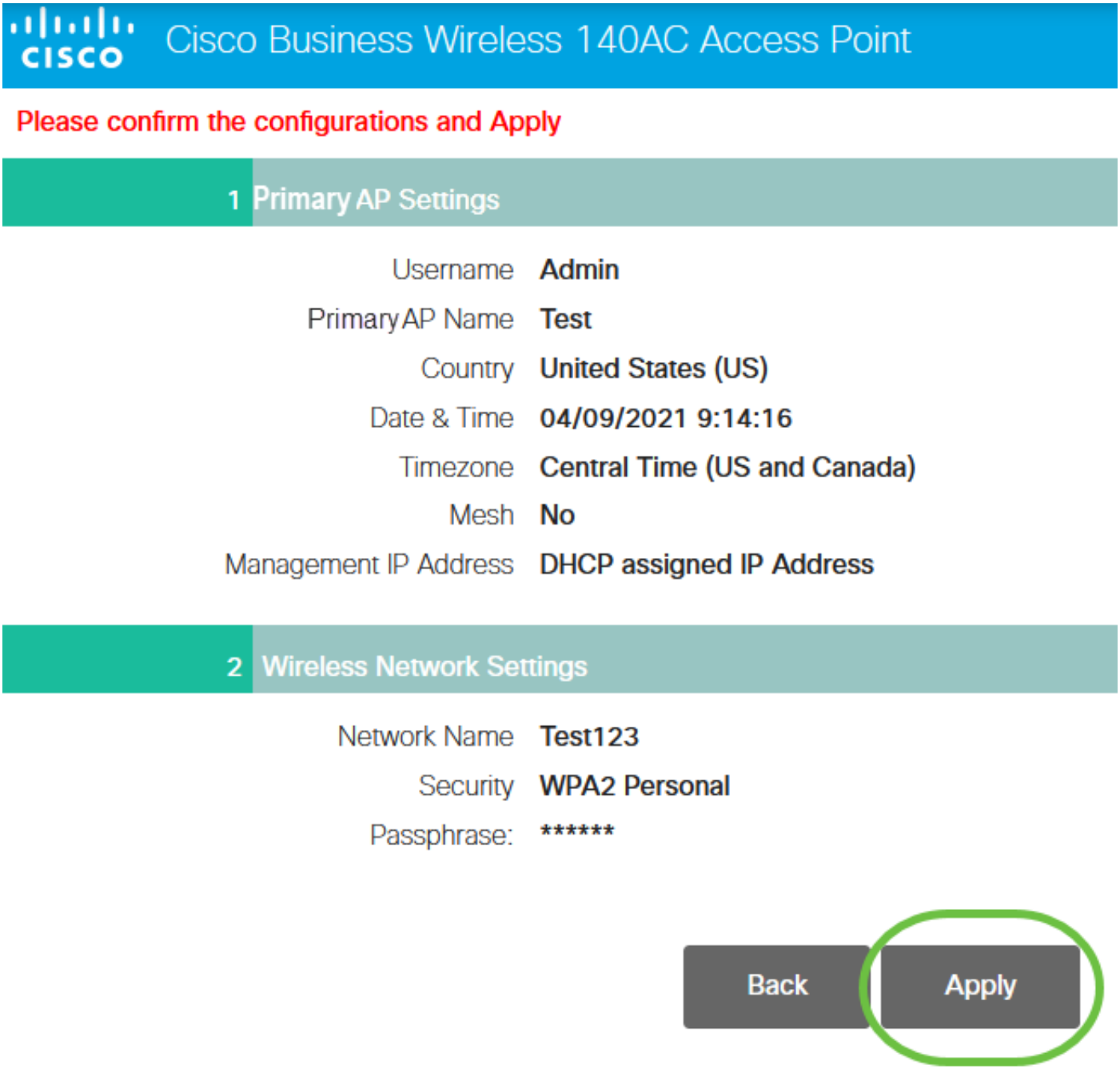
Haga clic en Next (Siguiente).



Wi-Fi Protected Access (WPA) versión 2 (WPA2), es el estándar actual para la seguridad Wi-Fi.

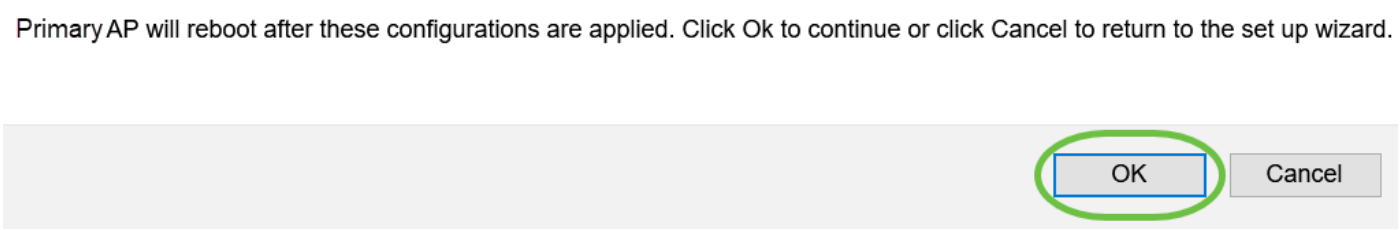
Paso 9

Confirme los parámetros y haga clic en **Aplicar**.

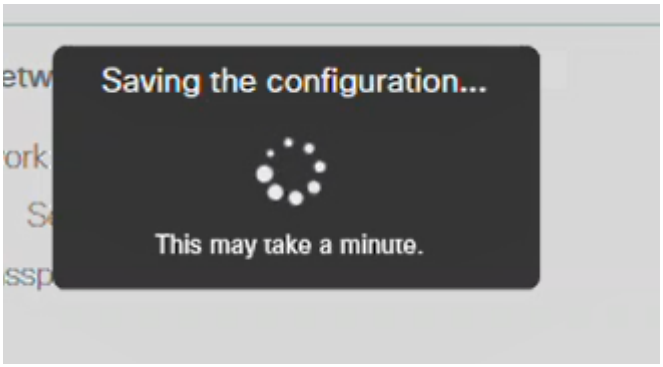


Paso 10

Haga clic en **Aceptar** para aplicar la configuración.



Verá la siguiente pantalla mientras se guardan las configuraciones y se reinicia el sistema. Esto puede tardar 10 minutos.

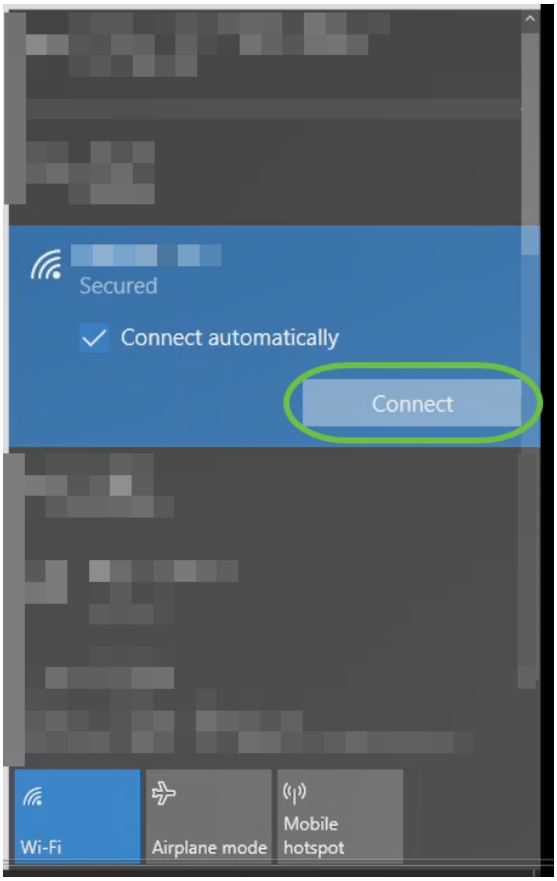


Durante el reinicio, la luz del punto de acceso pasará por varios patrones de color. Cuando la luz parpadee en verde, vaya al siguiente paso. Si la luz no supera el patrón rojo intermitente, indica que no hay ningún servidor DHCP en la red. Asegúrese de que el AP esté conectado a un switch o un router con un servidor DHCP.

Paso 11

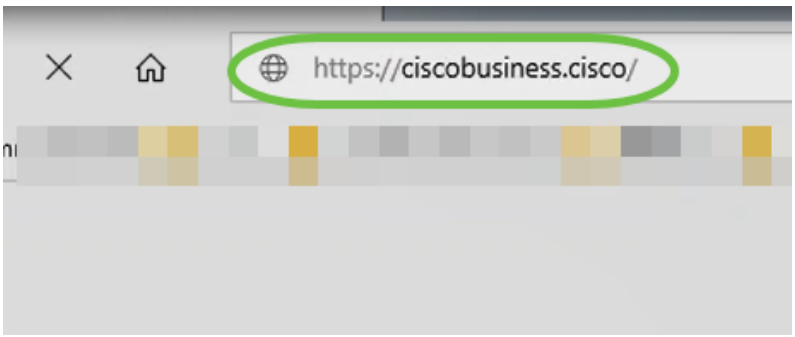
Vaya a las opciones inalámbricas del PC y elija la red que ha configurado. Haga clic en Connect (Conectar)

El SSID *CiscoBusiness-Setup* desaparecerá después del reinicio.



Paso 12

Abra un navegador web y escriba *https://[dirección IP del AP CBW]*. También puede escribir *https://ciscobusiness.cisco* en la barra de direcciones y pulsar Intro.



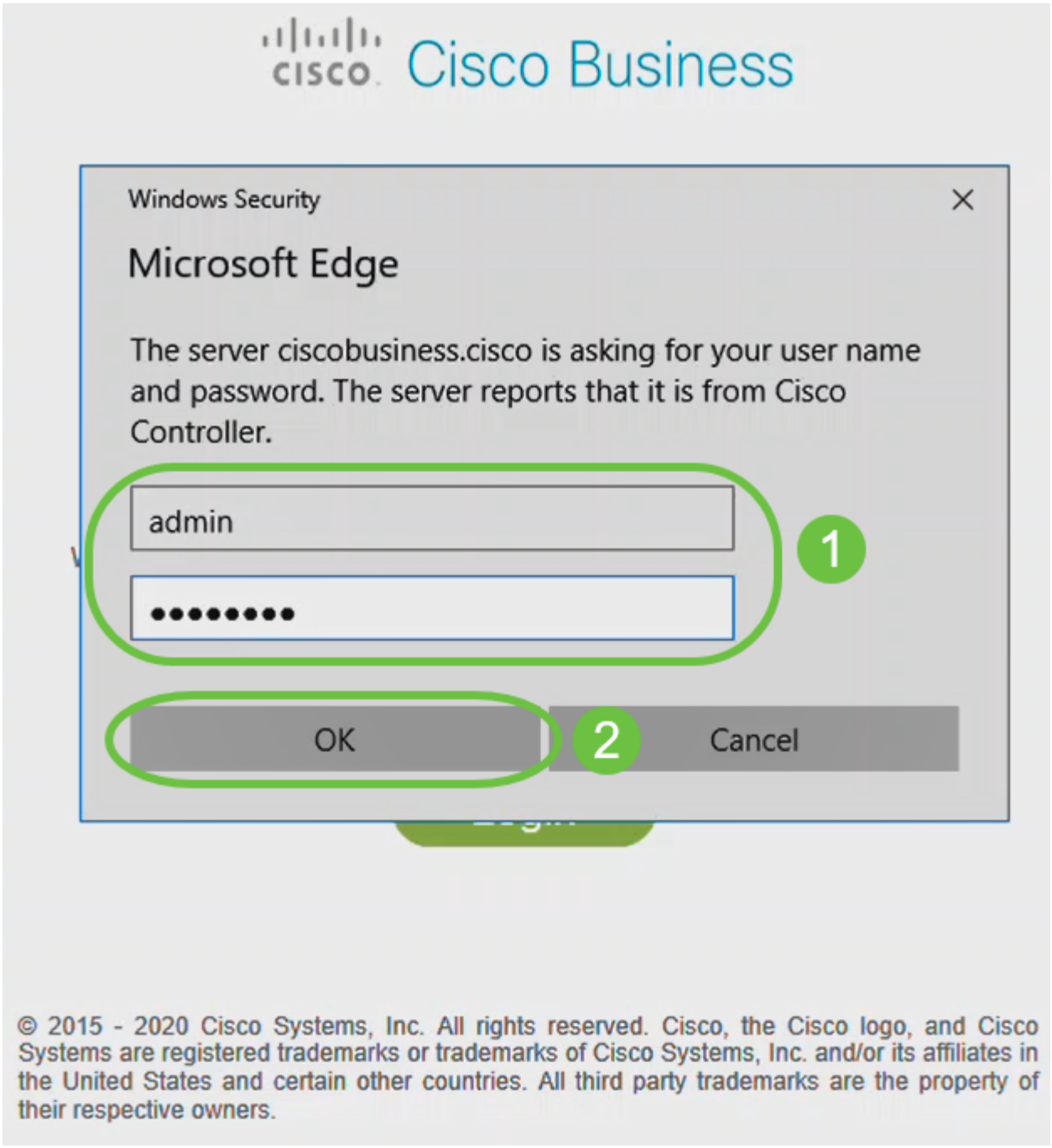
Asegúrese de escribir *https* y no *http* en este paso.

Paso 13

Haga clic en Login (Conexión).

Paso 14

Inicie sesión con las credenciales configuradas. Click OK.



Paso 15

Podrá acceder a la página de interfaz de usuario web del AP.

Consejos para la resolución de problemas inalámbricos

Si tiene algún problema, consulte los siguientes consejos:

- Asegúrese de que está seleccionado el identificador del conjunto de servicios (SSID) correcto. Este es el nombre que ha creado para la red inalámbrica.
- Desconecte cualquier VPN para la aplicación móvil o en un portátil. Es posible que incluso esté conectado a una VPN que su proveedor de servicios móviles utilice que puede que ni siquiera sepa. Por ejemplo, un teléfono Android (Pixel 3) con Google Fi como proveedor de servicios, hay una VPN integrada que se conecta automáticamente sin notificación. Esto tendría que ser inhabilitado para encontrar el AP primario.
- Inicie sesión en el AP primario con https://<dirección IP del AP primario>.
- Una vez que realice la configuración inicial, asegúrese de que https:// is se utiliza tanto si inicia sesión en *ciscobusiness.cisco* como si introduce la dirección IP en su navegador web. En función de la configuración, es posible que el ordenador se haya rellenado automáticamente con http:// since que es lo que utilizó la primera vez que se conectó.
- Para ayudar con problemas relacionados con el acceso a la interfaz de usuario web o problemas del navegador durante el uso del AP, en el navegador web (Firefox en este caso) haga clic en el menú Abrir, vaya a Ayuda > Información de Troubleshooting y haga clic en Actualizar Firefox.

Configuración de los extensores de malla CBW142ACM mediante la interfaz de usuario web

Se encuentra en el tramo de inicio de la configuración de esta red, solo tiene que agregar los extensores de malla.

Paso 1

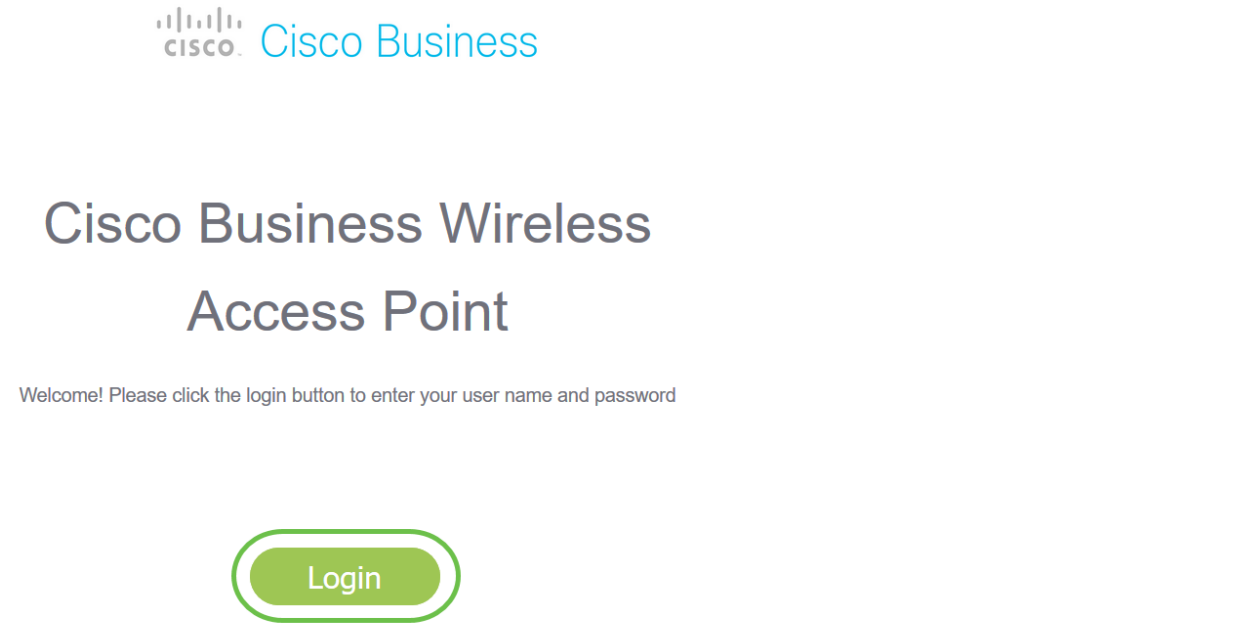
Conecte los dos ampliadores de malla a la pared en las ubicaciones que haya seleccionado. Anote la dirección MAC de cada extensor de malla.

Paso 2

Espere unos 10 minutos para que se inicien los extensores de malla.

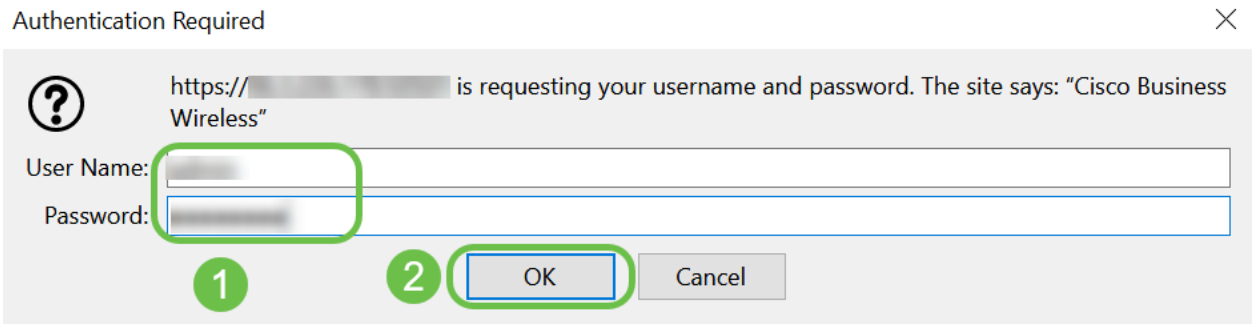
Paso 3

Introduzca la dirección IP de los puntos de acceso principales (AP) en el navegador web. Haga clic en **Login** para acceder al AP primario.



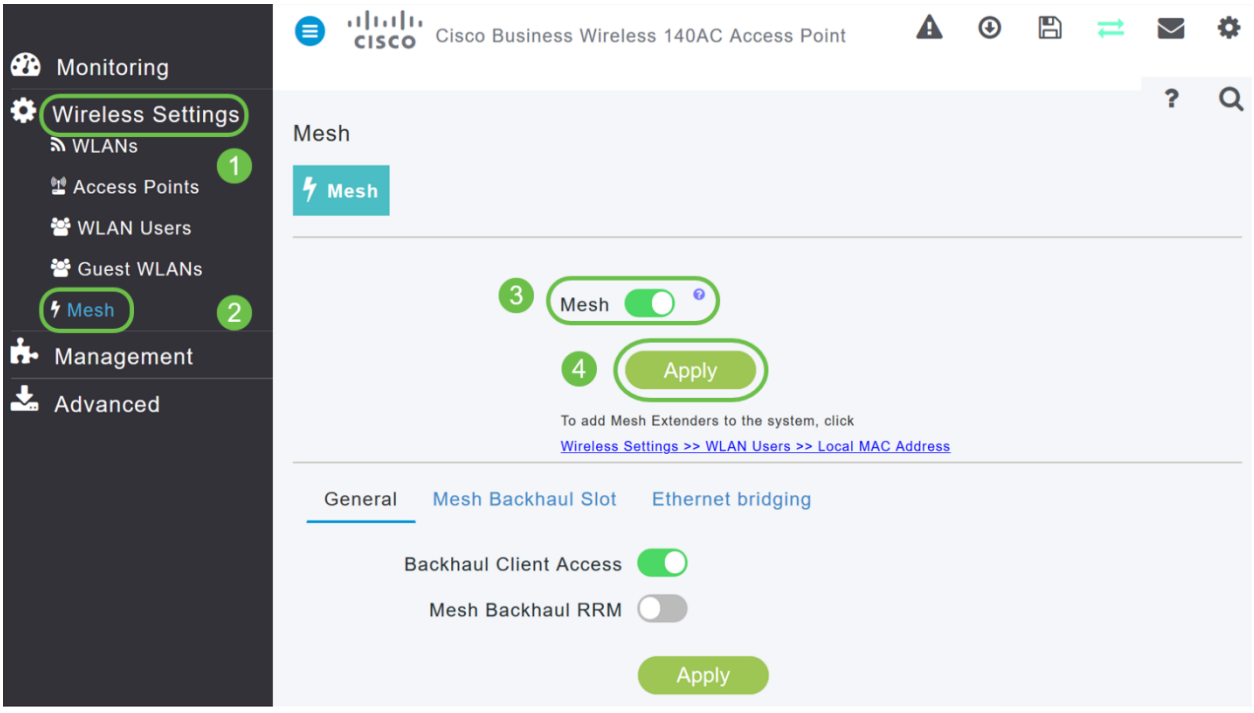
Paso 4

Ingrese sus credenciales *Nombre de usuario* y *Contraseña* para acceder al AP primario. Click OK.



Paso 5

Vaya a **Wireless Settings > Mesh** . Asegúrese de que la *malla* esté habilitada. Haga clic en Apply (Aplicar).

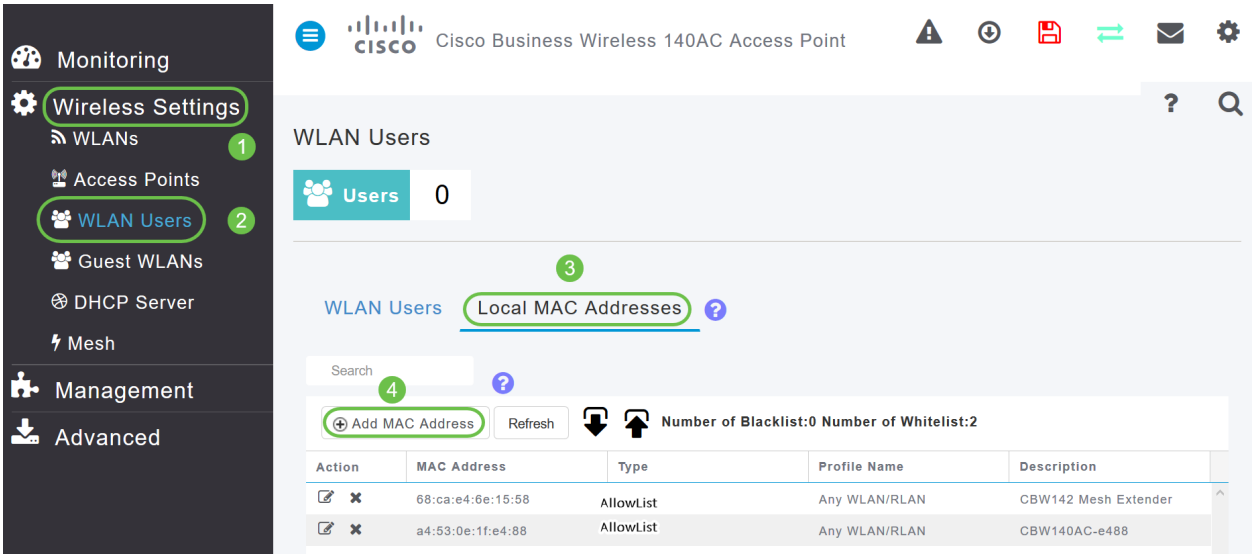


Paso 6

Si la malla aún no estaba activada, es posible que el WAP deba realizar un reinicio. Aparecerá una ventana emergente para reiniciar. Confirmar. Esto tardará unos 10 minutos. Durante un reinicio, 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 de color del LED y el color de la unidad a la unidad.

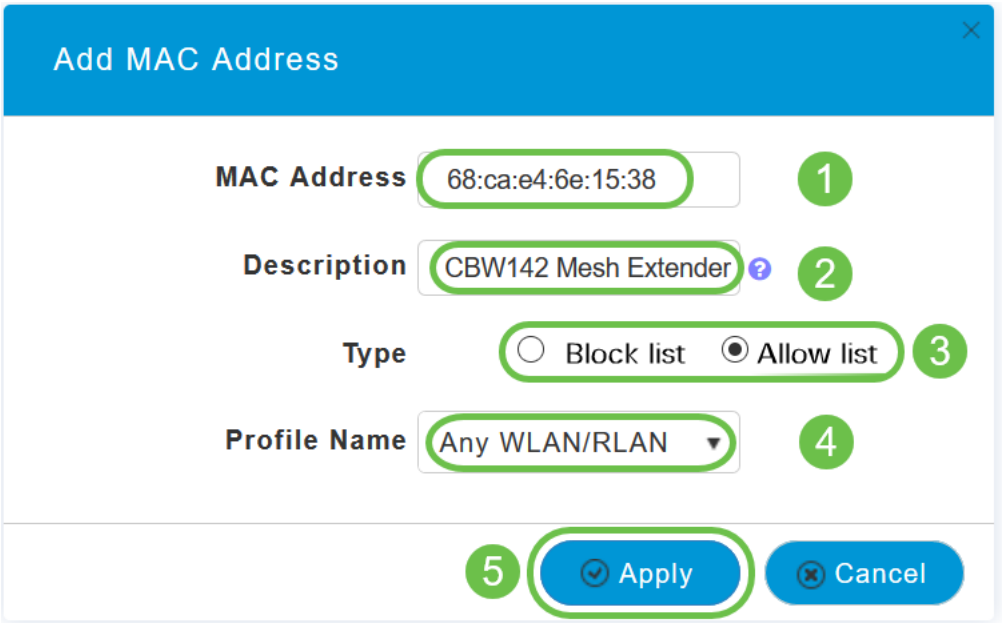
Paso 7

Vaya a **Wireless Settings > WLAN Users > Local MAC Addresses** . Haga clic en **Add MAC Address**.



Paso 8

Introduzca la dirección MAC y la descripción del ampliador de malla. Seleccione el *tipo* como lista Permitir. Seleccione el *nombre del perfil* en el menú desplegable. Haga clic en Apply (Aplicar).



Paso 9

Asegúrese de guardar todas las configuraciones pulsando el **icono Guardar** en el panel superior derecho de la pantalla.

Repita este procedimiento para cada extensor de malla.

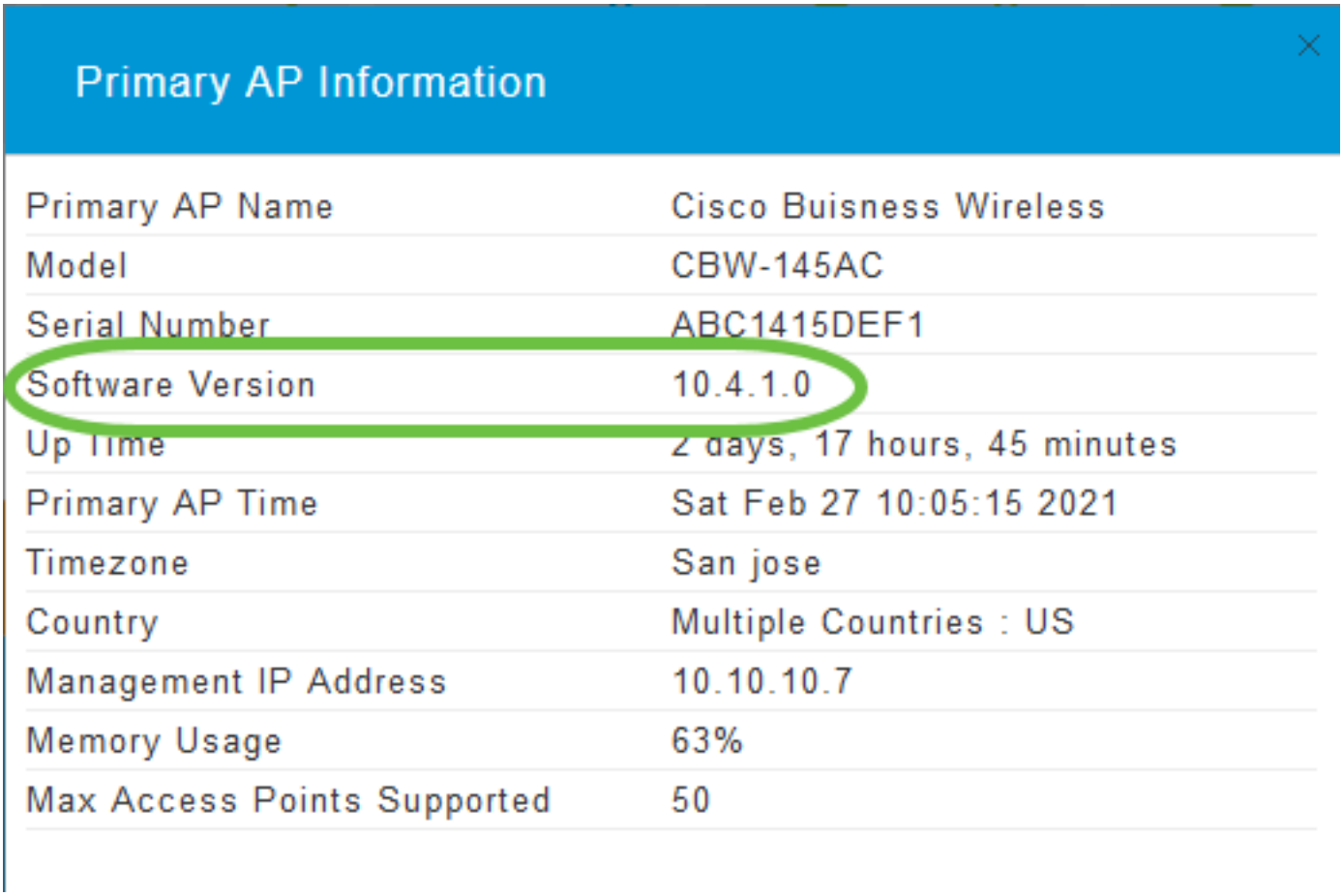
Comprobar y actualizar el software mediante la interfaz de usuario web

No se salte este paso importante. Hay algunas formas de actualizar el software, pero los pasos que se muestran a continuación se recomiendan como los más fáciles de ejecutar cuando se utiliza la interfaz de usuario web.

Para ver y actualizar la versión de software actual de su AP principal, realice los siguientes pasos.

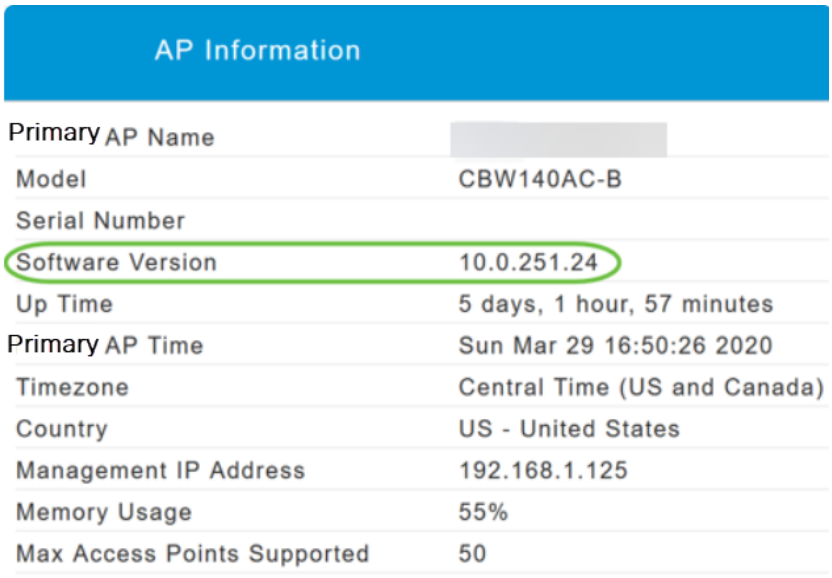
Paso 1

Haga clic en el **icono del engranaje** en la esquina superior derecha de la interfaz web y luego haga clic en **Información del AP primario**.



Paso 2

Compare la versión que se está ejecutando con la última versión de software. Cierre la ventana cuando sepa si necesita actualizar el software.



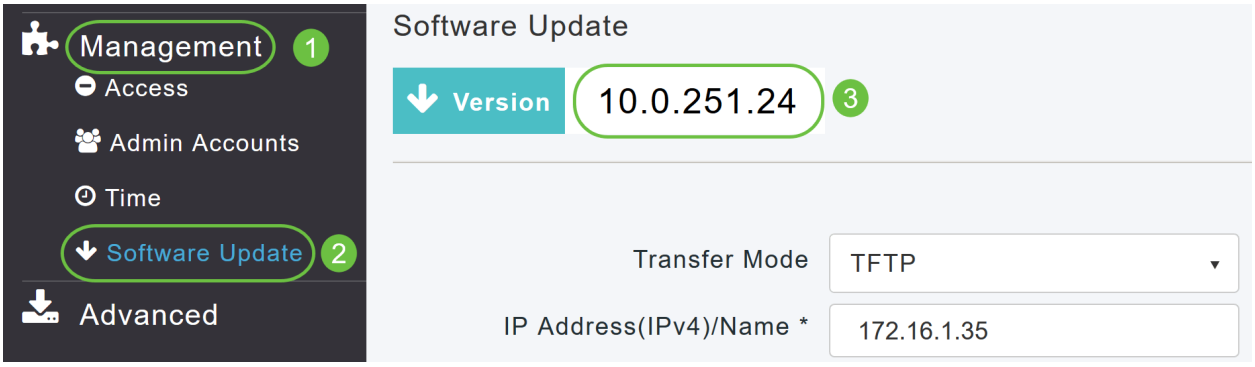
Si está ejecutando la última versión de software, puede saltar a la sección Creación de WLANs.

Paso 3

Elija **Management > Software Update** en el menú.

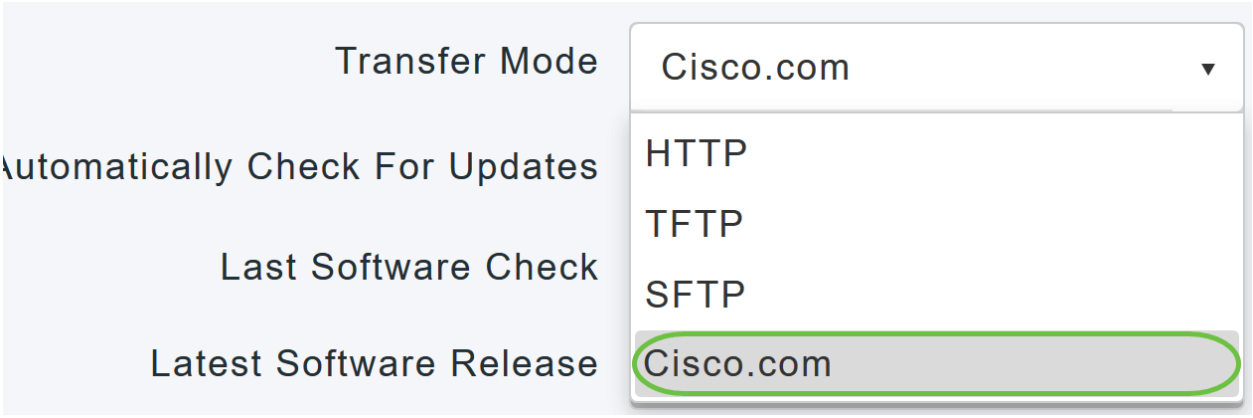
La ventana *Actualización de software* se muestra con el número de versión de

software actual en la parte superior.



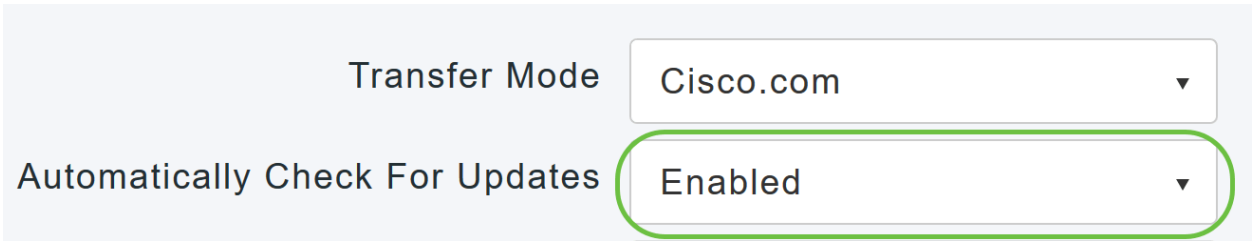
Puede actualizar el software CBW AP y las configuraciones actuales en el AP principal no se eliminarán.

En la lista desplegable *Modo de transferencia*, elija **Cisco.com**.



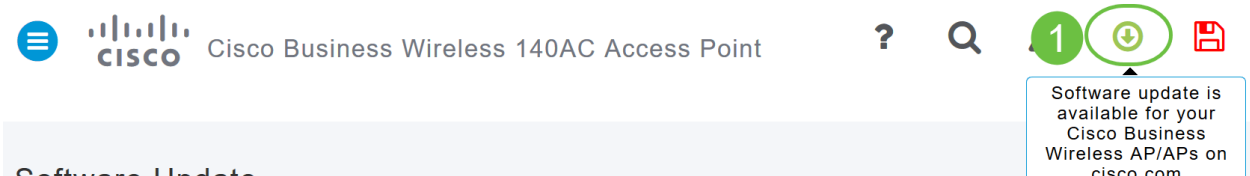
Paso 4

Para configurar el AP primario para que verifique automáticamente las actualizaciones de software, elija **Habilitado** en la lista desplegable *Verificar automáticamente actualizaciones*. Esto se activa como opción predeterminada.



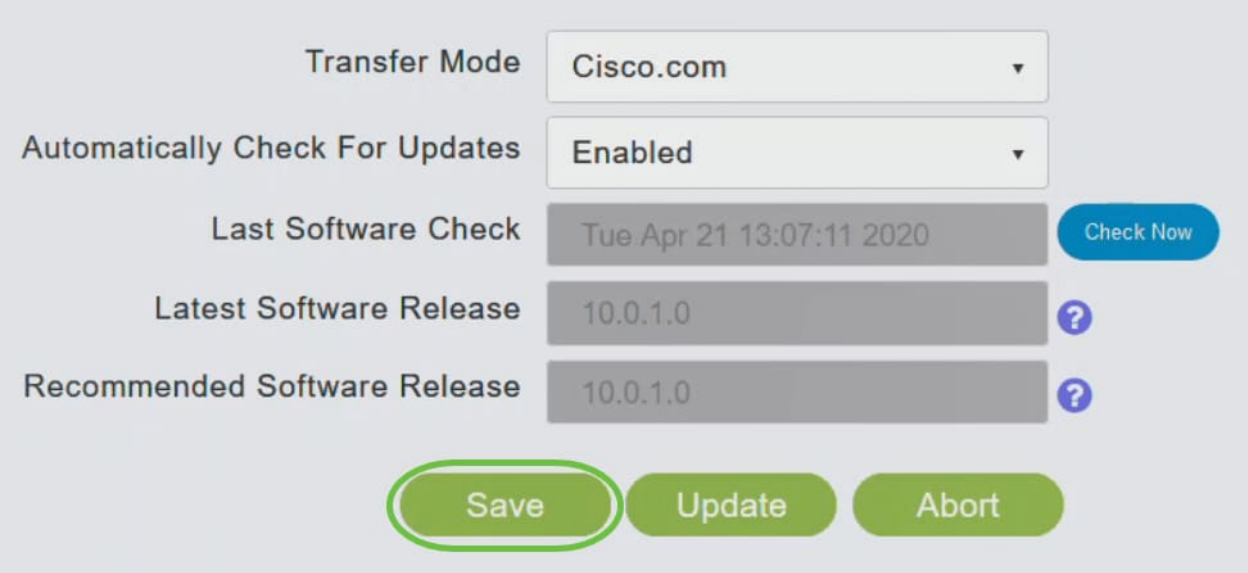
Cuando se realiza una comprobación de software y si hay disponible una actualización de software más reciente o recomendada en Cisco.com, entonces:

- El **icono Alerta de actualización de software** en la esquina superior derecha de la interfaz de usuario web será de color verde (o gris). Al hacer clic en el icono, accederá a la página Actualización de software.
- El botón Actualizar en la parte inferior de la página *Actualización de software* está habilitado.

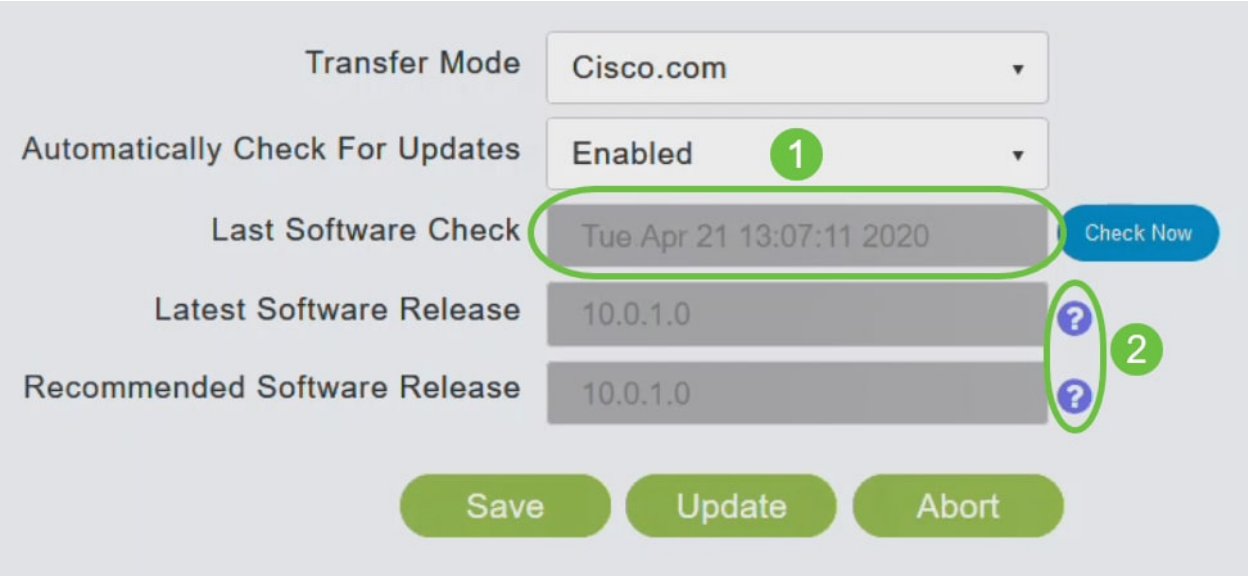


Paso 5

Click Save. Esto guarda las entradas o los cambios que ha realizado tanto en *Modo de transferencia* como *Comprobar actualizaciones automáticamente*.

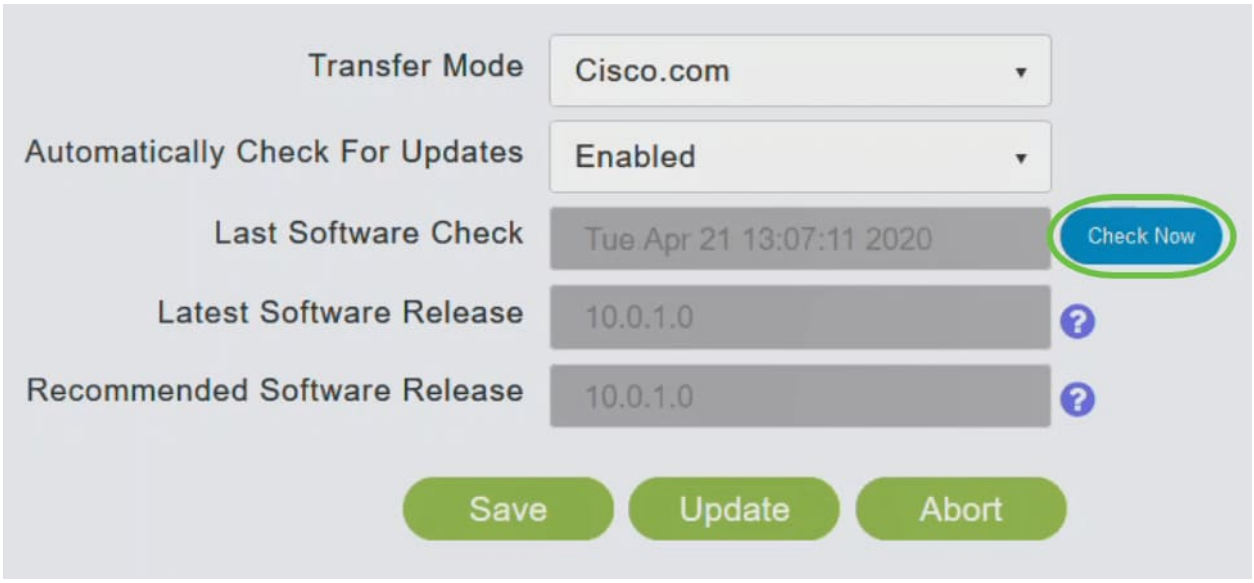


El campo *Last Software Check* muestra la marca de hora de la última comprobación automática o manual del software. Para ver las notas de las versiones mostradas, haga clic en el **icono del signo de interrogación** situado junto a él.



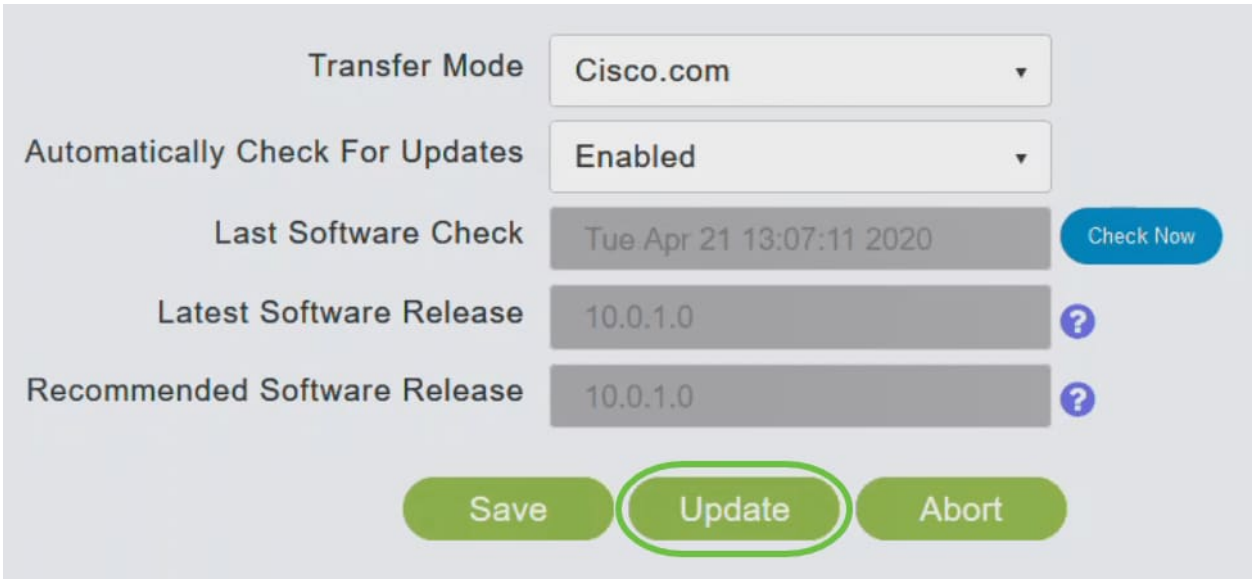
Paso 6

Puede ejecutar manualmente una comprobación de software en cualquier momento haciendo clic en *Comprobar ahora*.



Paso 7

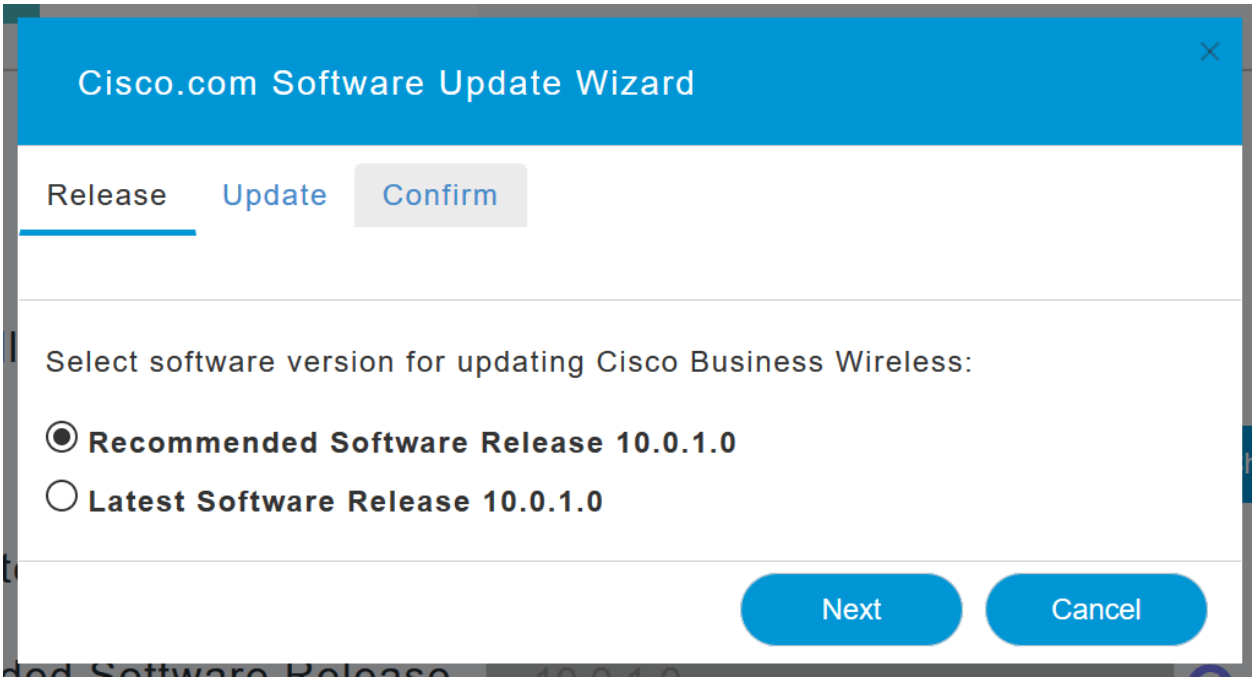
Para continuar con la actualización del software, haga clic en **Update**.



Aparecerá el *Asistente de actualización de software*. El asistente le guía por las tres fichas siguientes en secuencia:

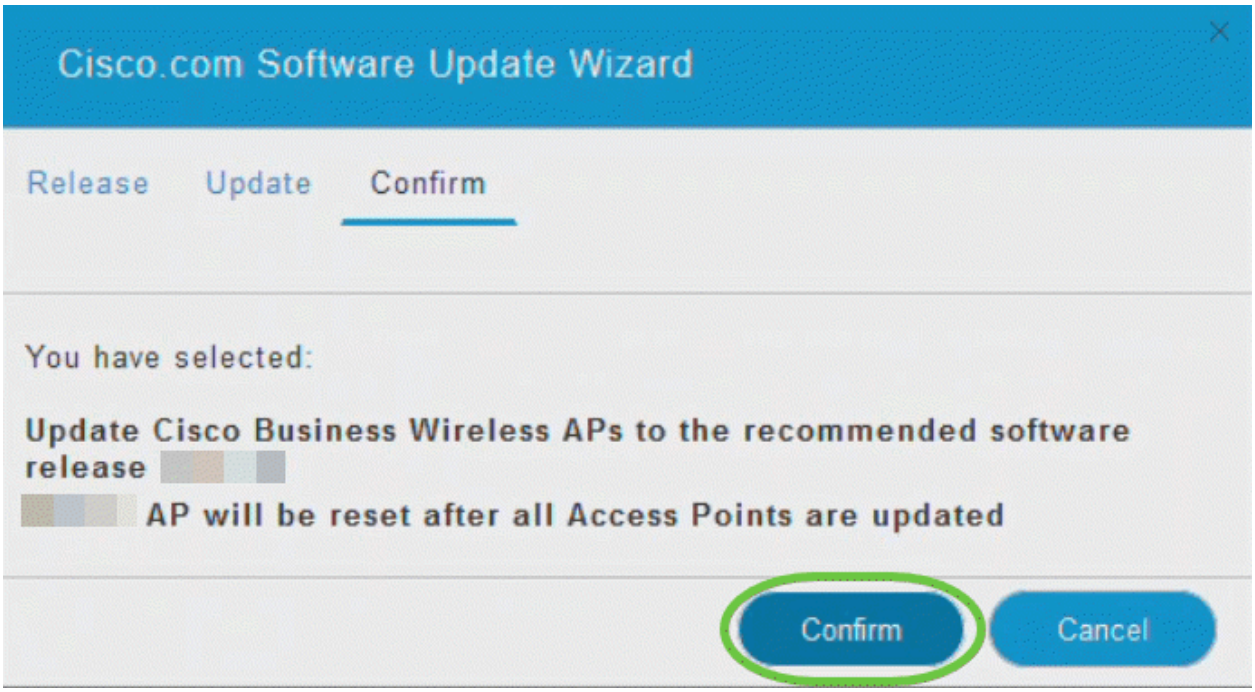
- Ficha Versión: especifique si desea actualizar a la versión de software recomendada o a la última versión de software.
- Ficha Actualizar - Especifique cuándo se deben restablecer los AP. Puede optar por hacerlo de inmediato o programarlo más adelante. Para configurar el AP primario para que se reinicie automáticamente después de que se complete la descarga previa de la imagen, marque la casilla Auto Restart .
- Ficha Confirmar - Confirme las selecciones.

Siga las instrucciones del asistente. Puede volver a cualquier pestaña en cualquier momento antes de hacer clic en *Confirmar*.



Paso 8

Haga clic en **Confirmar**.

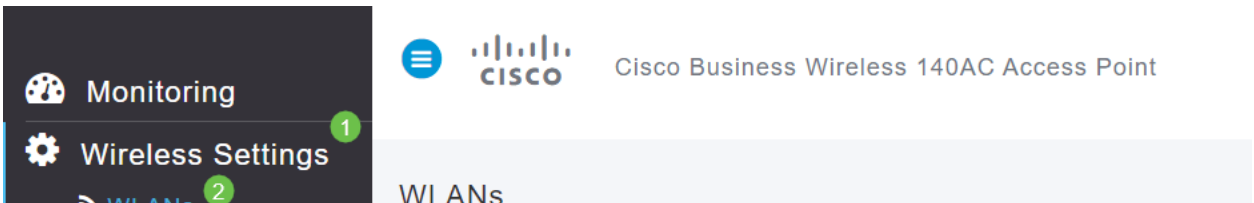


Crear WLANs en la interfaz de usuario web

Esta sección permite crear redes de área local inalámbricas (WLAN).

Paso 1

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



Paso 2

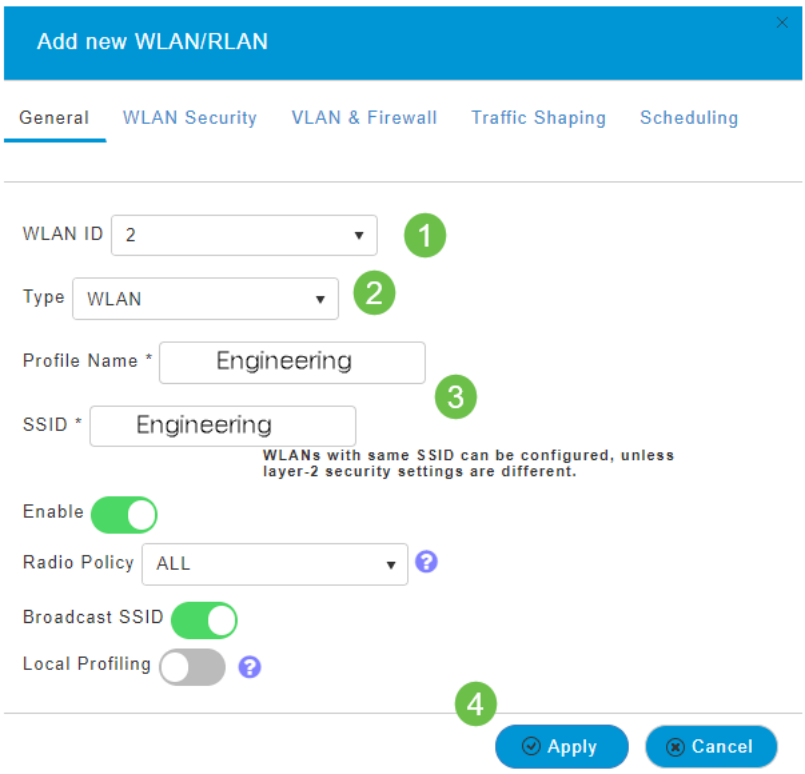
En la ficha *General*, introduzca la siguiente información:

- ID de WLAN: seleccione un número para la WLAN
- Tipo: Seleccione **WLAN**
- Profile Name (Nombre de perfil): al introducir un nombre, el SSID se rellenará automáticamente con el mismo nombre. El nombre debe ser único y no debe superar los 31 caracteres.

En este ejemplo se dejaron los campos siguientes como predeterminados, pero se muestran las explicaciones en caso de que desee configurarlos de forma diferente.

- SSID: el nombre del perfil también actúa como SSID. Puede cambiar esto si lo desea. El nombre debe ser único y no debe superar los 31 caracteres.
- Enable (Activar): Debe estar habilitado para que la WLAN funcione.
- Política de radio: normalmente, desea dejar esto como **Todo** para que los clientes de 2,4 GHz y 5 GHz puedan acceder a la red.
- Broadcast SSID (SSID de difusión): por lo general, desea que se detecte el SSID para que lo deje como habilitado.
- Perfiles locales: sólo desea activar esta opción para ver el sistema operativo que se está ejecutando en el cliente o para ver el nombre de usuario.

Haga clic en Apply (Aplicar).



Paso 3

Se le llevará a la pestaña *Seguridad WLAN*.

En este ejemplo, se dejaron las siguientes opciones como valor predeterminado:

- Guest Network (Red de invitados), Captive Network Assistant (Asistente de red cautiva) y MAC Filtering (Filtrado de MAC) quedaron desactivados. Los detalles para configurar una red de invitados se detallan en la siguiente sección.
- WPA2 Personal: acceso Wi-Fi protegido 2 con formato de frase de paso de clave precompartida (PSK): ASCII. Esta opción significa acceso Wi-Fi protegido 2 con clave precompartida (PSK).

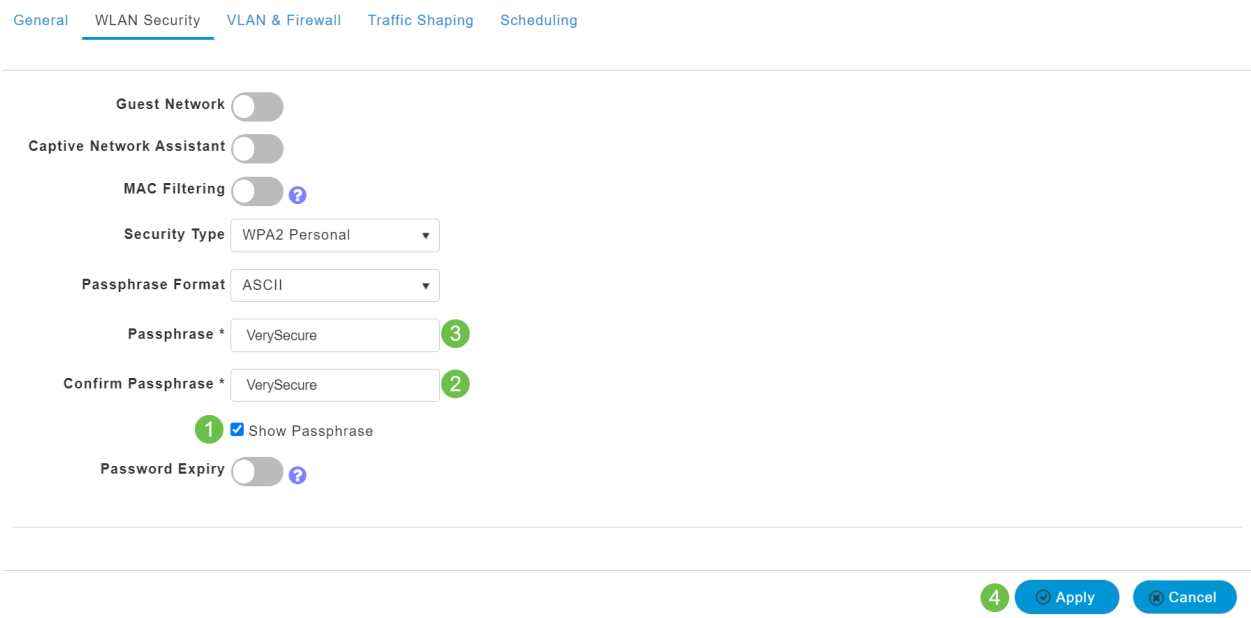
WPA2 Personal es un método utilizado para proteger la red mediante la autenticación PSK. El PSK se configura por separado en el AP primario, bajo la política de seguridad WLAN y en el cliente. WPA2 Personal no se basa en un servidor de autenticación de la red.

- Formato de frase de paso: **el ASCII se deja como valor predeterminado.**

En este escenario se han introducido los campos siguientes:

- Show Passphrase (Mostrar frase de paso): haga clic en la casilla de verificación para ver la frase de paso que introduzca.
- Passphrase (Frase de paso): Introduzca un nombre para la frase de paso (contraseña).
- Confirm Passphrase (Confirmar frase de paso): Vuelva a introducir la contraseña para confirmarla.

Haga clic en Apply (Aplicar). Esto activará automáticamente la nueva WLAN.

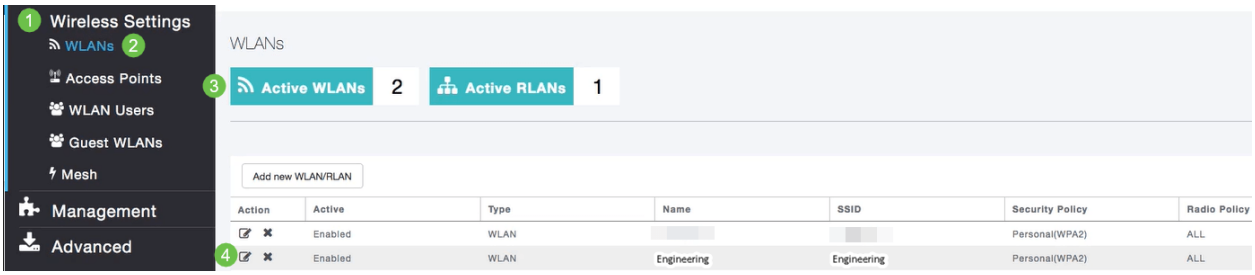


Paso 4

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

Paso 5

Para ver la WLAN que creó, seleccione **Wireless Settings > WLANs**. Verá el número de WLANs activas elevado a 2 y se mostrará la nueva WLAN.



Repita estos pasos para otras WLAN que desee crear.

Configuraciones inalámbricas opcionales

Ahora tiene todas las configuraciones básicas configuradas y listas para su lanzamiento. Dispone de algunas opciones, por lo que no dude en ir a cualquiera de las secciones siguientes:

- Crear una WLAN de invitado mediante la interfaz de usuario web (opcional)
- Definición de perfiles de aplicaciones (opcional)
- Perfiles de clientes (opcional)
- ¡Estoy listo para terminar esto y empezar a usar mi red!

Crear una WLAN de invitado mediante la interfaz de usuario web (opcional)

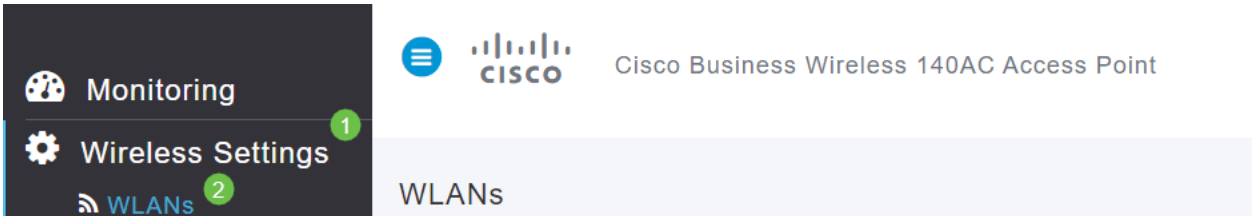
Una WLAN de invitado le permite a los invitados acceder a su red Cisco Business Wireless.

Paso 1

Inicie sesión en la interfaz de usuario web del AP principal. Abra un navegador web e ingrese www.https://ciscobusiness.cisco. Puede recibir una advertencia antes de continuar. Introduzca sus credenciales. También puede acceder a él ingresando la dirección IP del AP primario.

Paso 2

Se puede crear una red de área local inalámbrica (WLAN) navegando hasta **Parámetros inalámbricos > WLAN**. A continuación, seleccione **Add new WLAN/RLAN**.



Paso 3

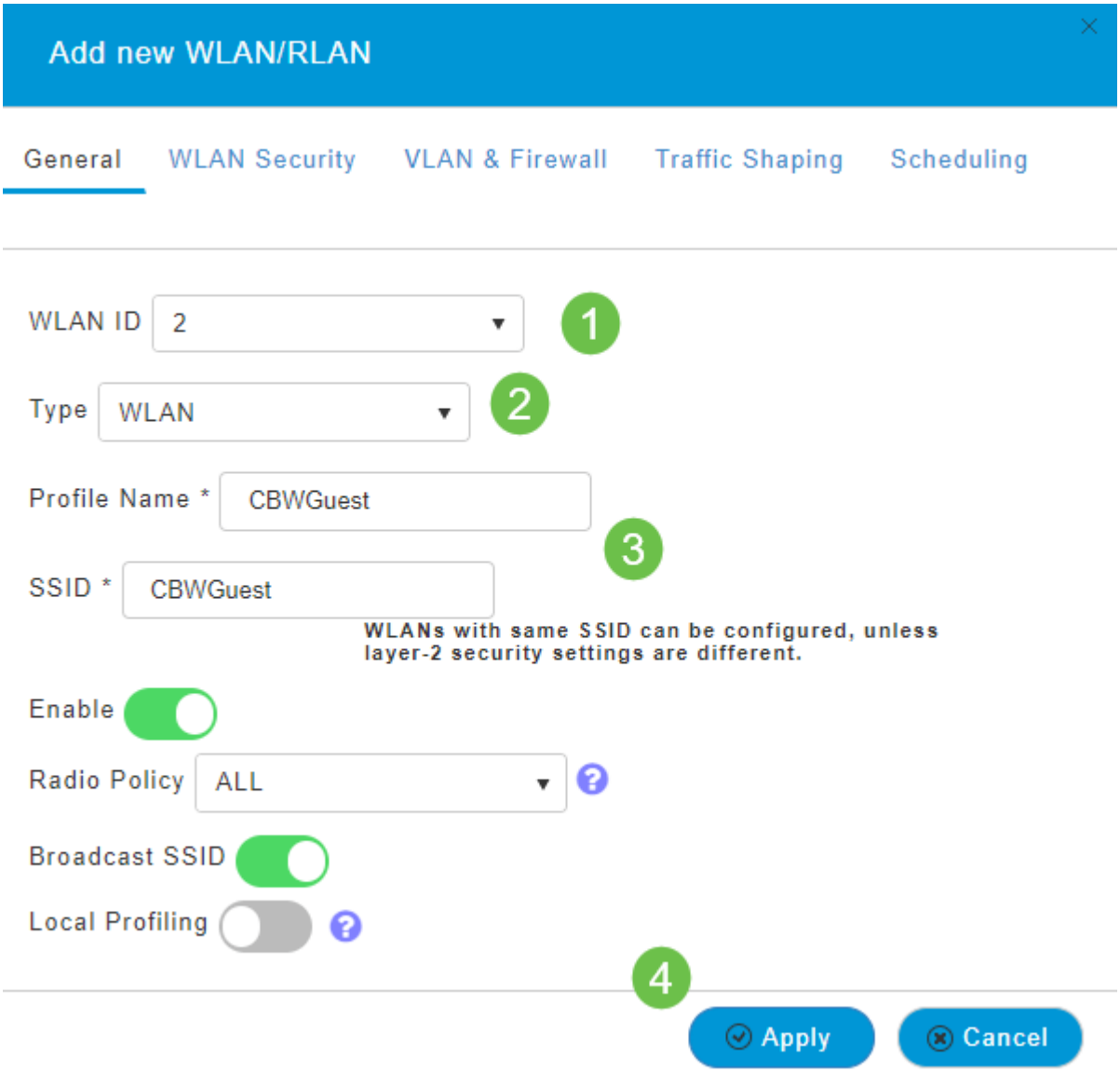
En la ficha *General*, introduzca la siguiente información:

WLAN ID: Seleccione un número para la WLAN
Tipo: Seleccione **WLAN**
Nombre de perfil: al introducir un nombre, el SSID se rellenará automáticamente con el mismo nombre. El nombre debe ser único y no debe superar los 31 caracteres.

En este ejemplo se dejaron los campos siguientes como predeterminados, pero se muestran las explicaciones en caso de que desee configurarlos de forma diferente.

SSID: el nombre del perfil también actúa como SSID. Puede cambiar esto si lo desea. El nombre debe ser único y no debe superar los 31 caracteres.
Enable (Activar): Debe estar habilitado para que la WLAN funcione.
Política de radio: normalmente desea dejar esto como **Todos** para que los clientes de 2,4 GHz y 5 GHz puedan acceder a la red.
Broadcast SSID: normalmente desea que se detecte el SSID para que desee dejarlo como habilitado.
Perfiles locales: sólo desea activar esta opción para ver el sistema operativo que se está ejecutando en el cliente o para ver el nombre de usuario.

Haga clic en Apply (Aplicar).

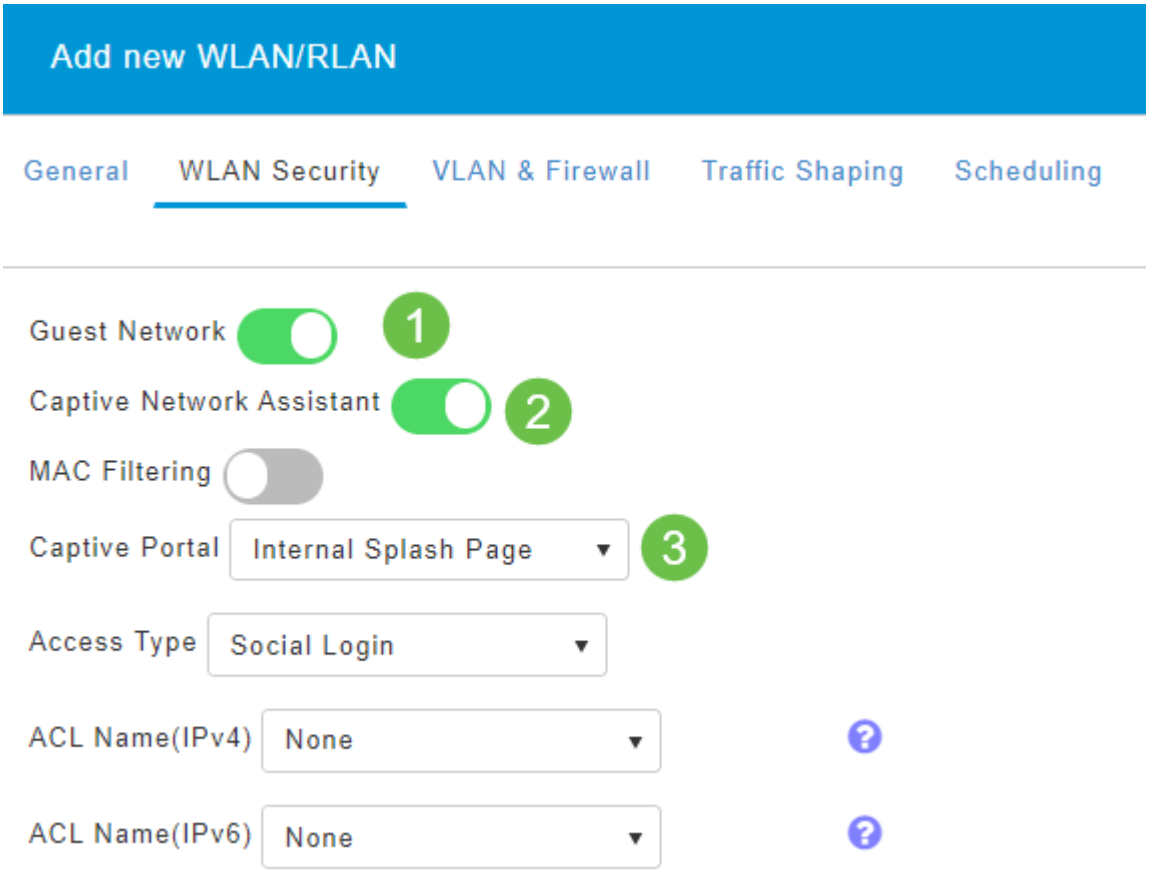


Paso 4

Se le llevará a la pestaña *Seguridad WLAN*. En este ejemplo, se seleccionaron las siguientes opciones.

- Red de invitado - Habilitar
- Captive Network Assistant: si utiliza Mac o IOS, probablemente desee habilitar esto. Esta función detecta la presencia de un portal cautivo enviando una solicitud web al conectarse a una red inalámbrica. Esta solicitud se dirige a un localizador uniforme de recursos (URL) para modelos de iPhone y, si se recibe una respuesta, se supone que el acceso a Internet está disponible y no se requiere ninguna interacción adicional. Si no se recibe ninguna respuesta, se supone que el acceso a Internet está bloqueado por el portal cautivo y el Asistente de red cautivo (CNA) de Apple inicia automáticamente el pseudo-navegador para solicitar el inicio de sesión del portal en una ventana controlada. El CNA puede romperse al redirigir a un portal cautivo de Identity Services Engine (ISE). El AP primario evita que aparezca este pseudo-navegador.
- Portal cautivo: este campo solo se muestra cuando la opción Red de invitado está activada. Esto se utiliza para especificar el tipo de portal web que se puede utilizar con fines de autenticación. Seleccione Internal Splash Page (Página de inicio interna) para utilizar la autenticación predeterminada basada en el portal web de Cisco. Elija External Splash Page si tendrá autenticación de portal cautiva, utilizando un servidor web fuera

de la red. También, especifique la dirección URL del servidor en el campo Dirección URL del sitio.



En este ejemplo, se creará la WLAN de invitado con un tipo de acceso de inicio de sesión social habilitado. Una vez que el usuario se conecte a esta WLAN de invitado, se le redirigirá a la página de inicio de sesión predeterminada de Cisco, donde podrá encontrar los botones de inicio de sesión de Google y Facebook. El usuario puede iniciar sesión usando su cuenta de Google o Facebook para obtener acceso a Internet.

Paso 5

En esta misma ficha, seleccione un *tipo de acceso* en el menú desplegable. En este ejemplo, se seleccionó *Inicio de sesión social*. Esta es la opción que permite a los invitados utilizar sus credenciales de Google o Facebook para autenticarse y obtener acceso a la red.

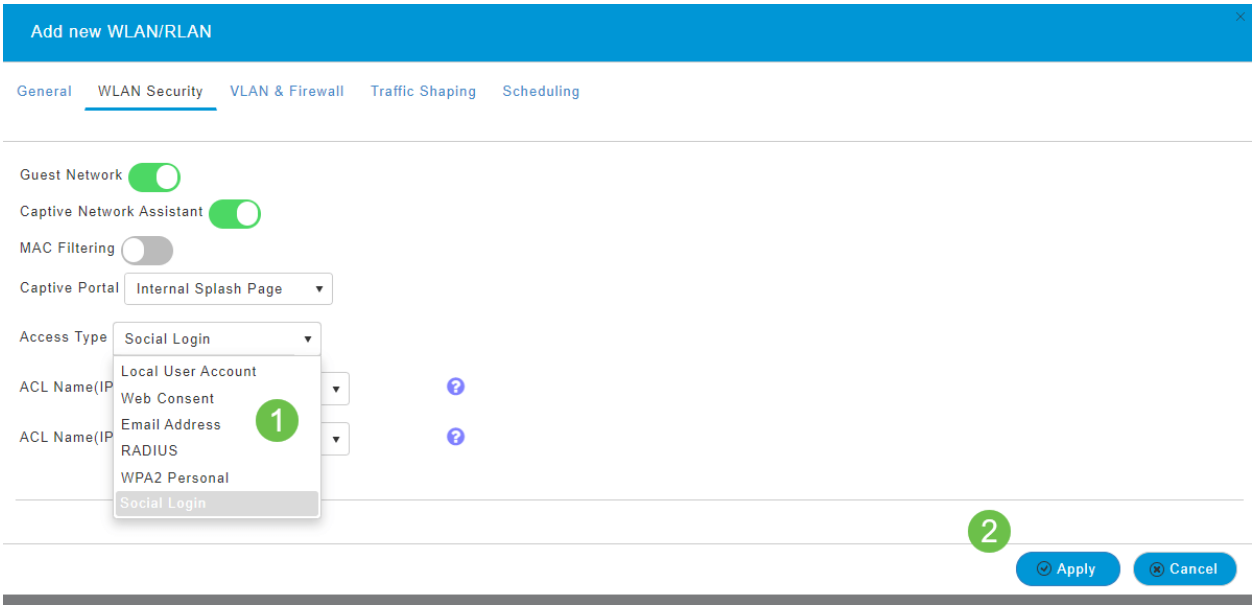
Otras opciones para el *tipo de acceso* incluyen:

Cuenta de usuario local: la opción predeterminada. Elija esta opción para autenticar invitados usando el nombre de usuario y la contraseña que puede especificar para los usuarios invitados de esta WLAN, en **Wireless Settings > WLAN Users**. Este es un ejemplo de la página de bienvenida interna predeterminada.

Puede personalizar esto navegando hasta **Wireless Settings > Guest WLANs**. Desde aquí puede introducir un *título de página* y un *mensaje de página*. Haga clic en Apply (Aplicar). Haga clic en **Vista previa**.

Web Consent: permite a los invitados acceder a la WLAN cuando aceptan los términos y condiciones mostrados. Los usuarios invitados pueden acceder a la WLAN sin introducir un nombre de usuario y una contraseña.
Dirección de correo electrónico: los usuarios invitados deberán introducir su dirección de correo electrónico para acceder a la red.
RADIUS: Utilice esto con un servidor de autenticación externo.
WPA2 Personal: acceso Wi-Fi protegido 2 con clave precompartida (PSK)

Haga clic en Apply (Aplicar).



Paso 6

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

Ahora ha creado una red de invitados que está disponible en su red CBW. Sus huéspedes apreciarán la comodidad.

Definición de perfiles de aplicaciones mediante la interfaz de usuario Web (opcional)

La definición de perfiles es un subconjunto de funciones que permite promulgar políticas organizativas. Le permite hacer coincidir y priorizar los tipos de tráfico. Al igual que las reglas, se toman decisiones sobre cómo clasificar o descartar el tráfico. El sistema Cisco Business Mesh Wireless incluye perfiles de clientes y aplicaciones. El acto de acceder a una red como usuario comienza con muchos intercambios de información, entre ellos está el tipo de tráfico. La política interrumpe el flujo de tráfico para dirigir el trayecto, de forma muy parecida a un diagrama de flujo. Otros tipos de

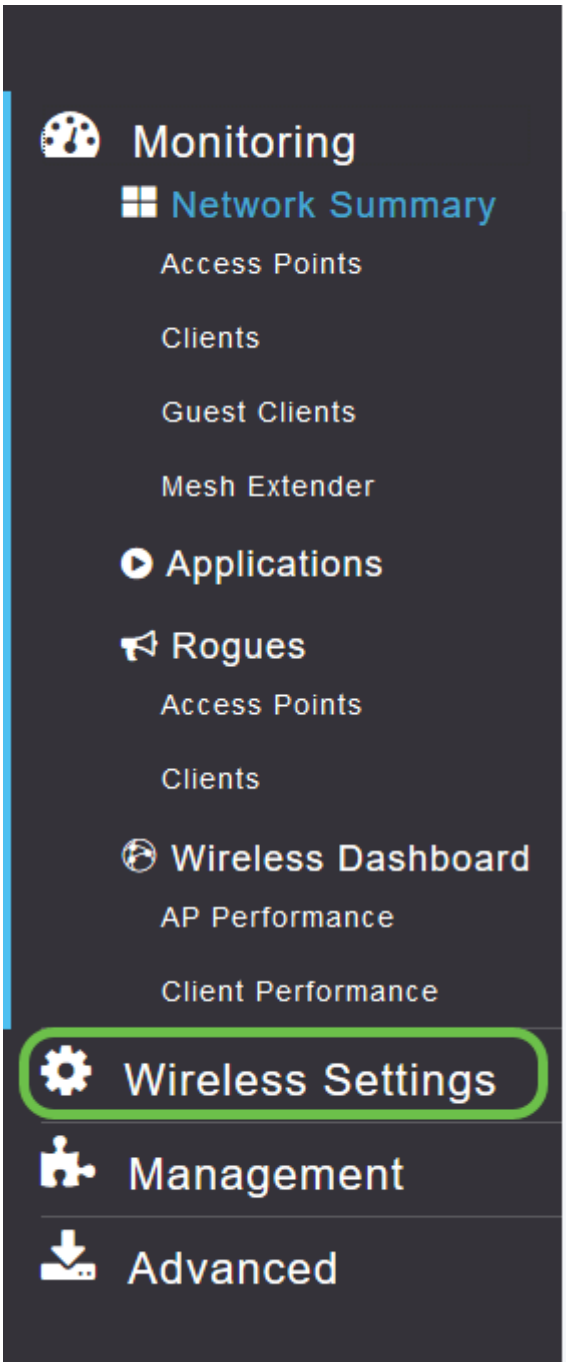
funciones de políticas son: acceso de invitado, listas de control de acceso y QoS.

Paso 1

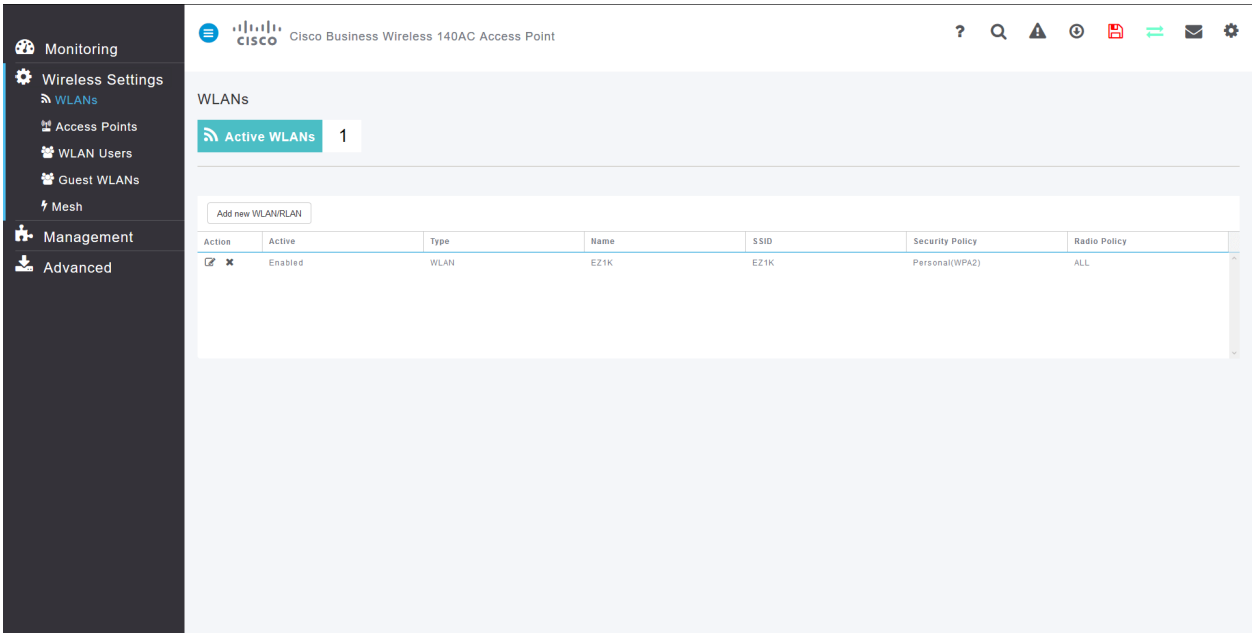
Desplácese hasta el menú situado en la parte izquierda de la pantalla si no ve la barra de menús izquierda.

Paso 2

El menú Monitoring se carga de forma predeterminada al iniciar sesión en el dispositivo. Deberá hacer clic en **Wireless Settings (Parámetros inalámbricos)**.

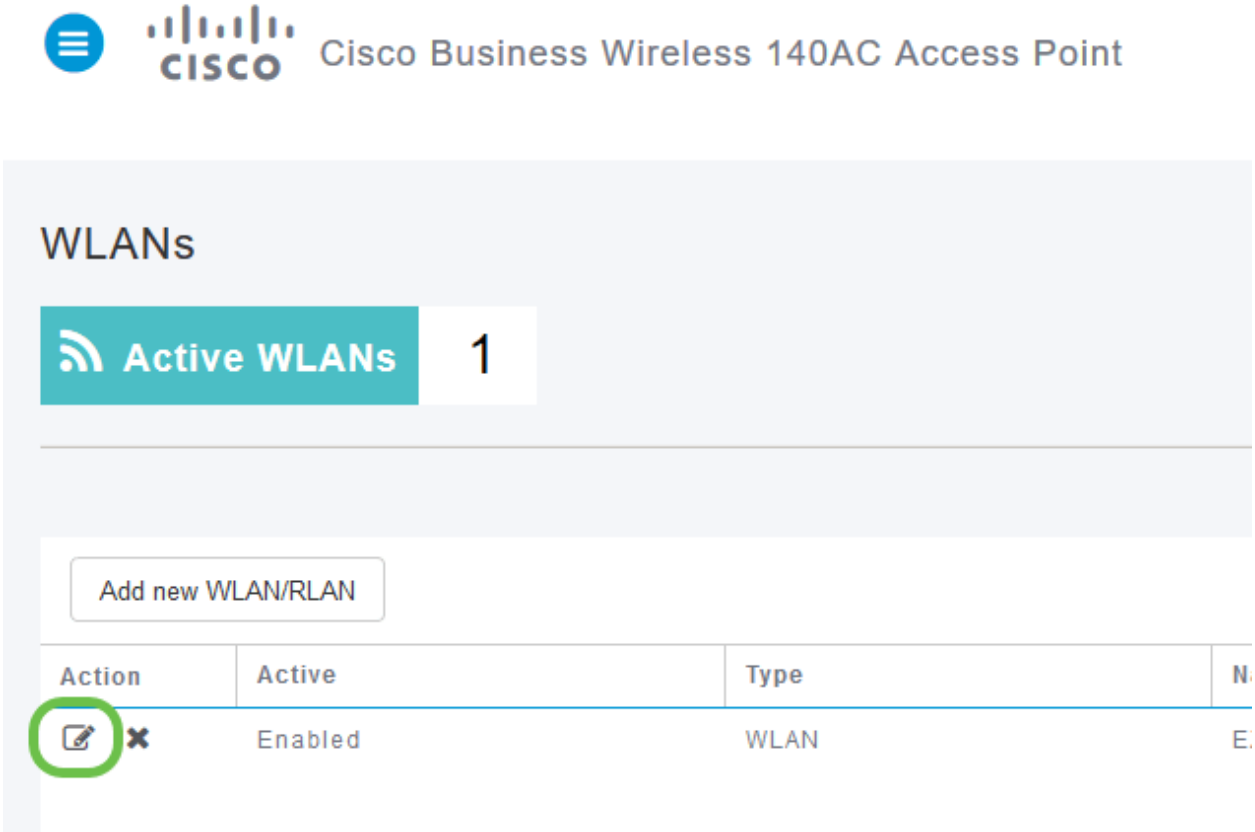


La siguiente imagen es similar a la que verá al hacer clic en el enlace Wireless Settings (Parámetros inalámbricos).

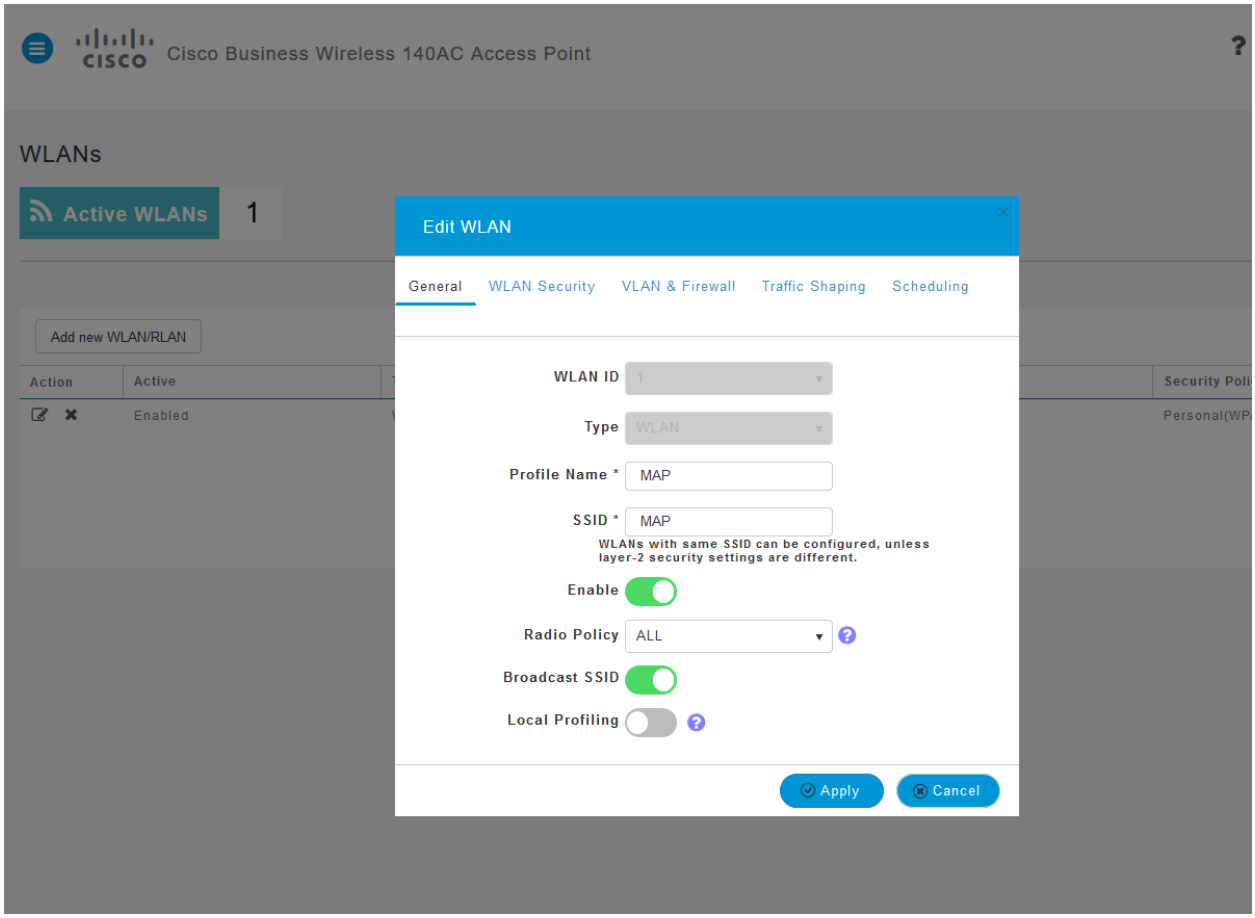


Paso 3

Haga clic en el **icono de edición** situado a la izquierda de la red de área local inalámbrica en la que desea activar la aplicación.

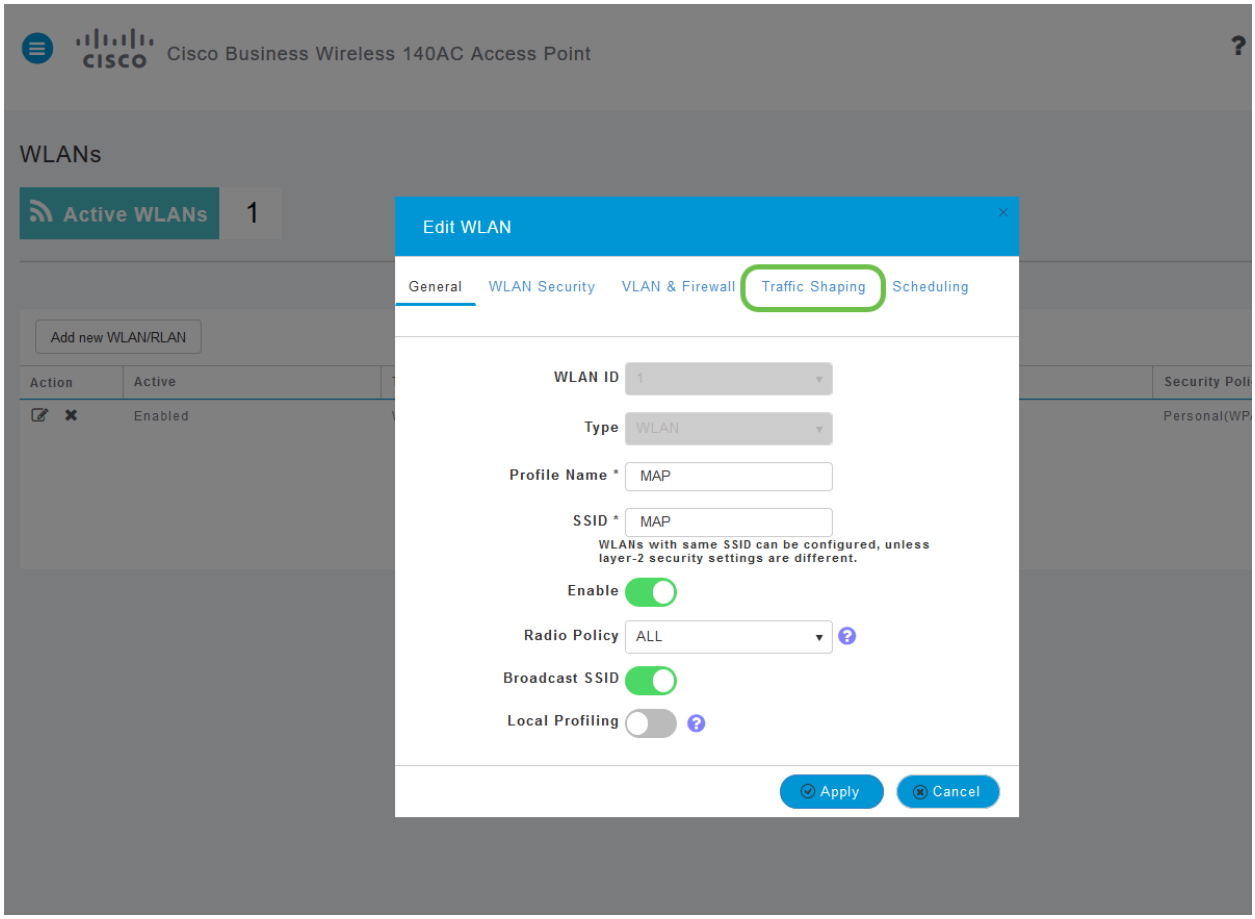


Desde que recientemente agregó la WLAN, su página *Editar WLAN* puede aparecer similar a la siguiente:

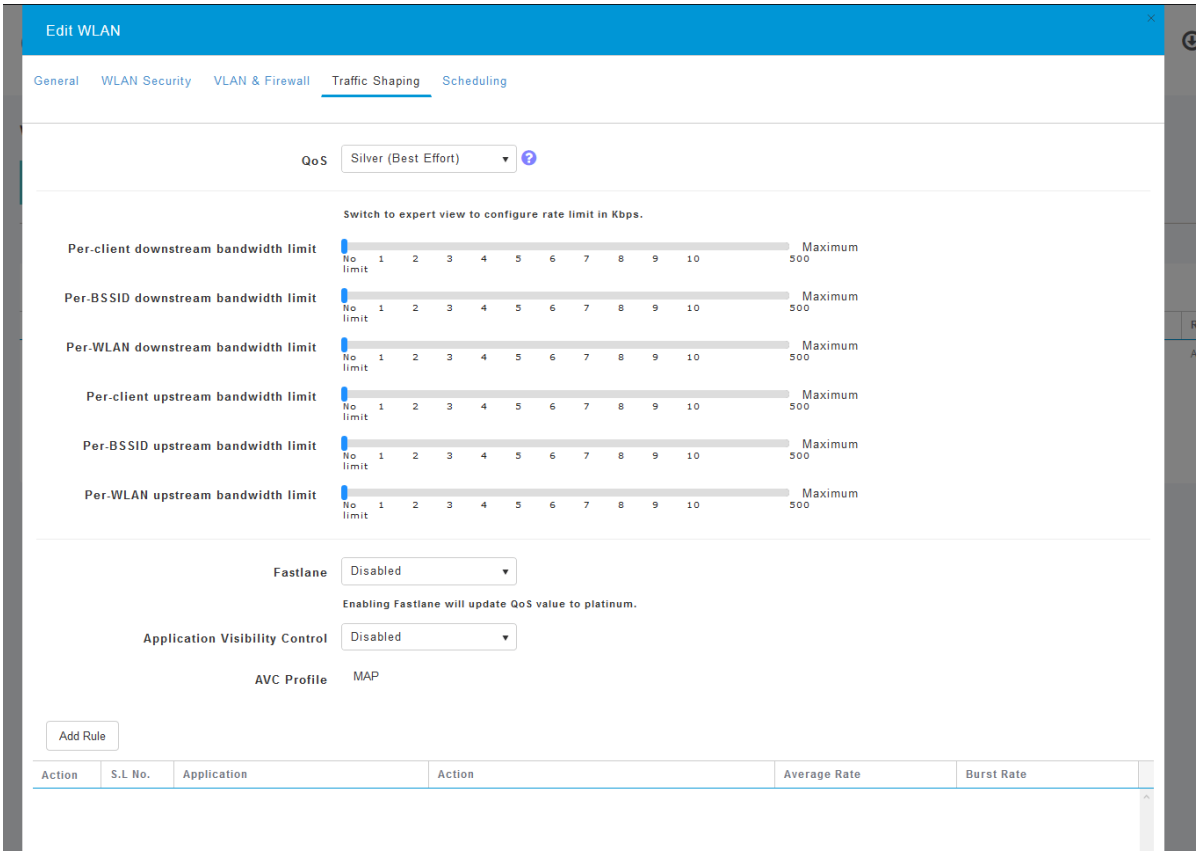


Paso 4

Vaya a la pestaña **Modelado de tráfico** haciendo clic en ella.

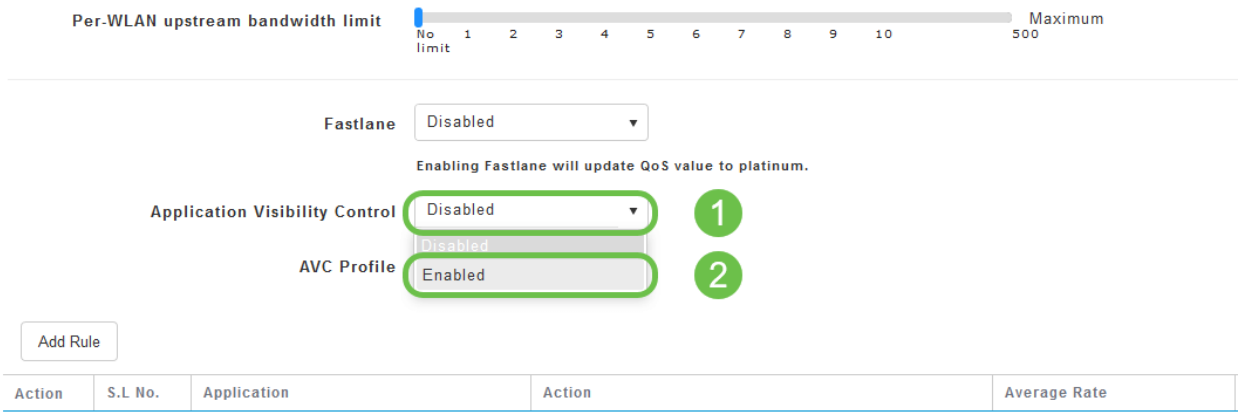


La pantalla puede aparecer de la siguiente manera:



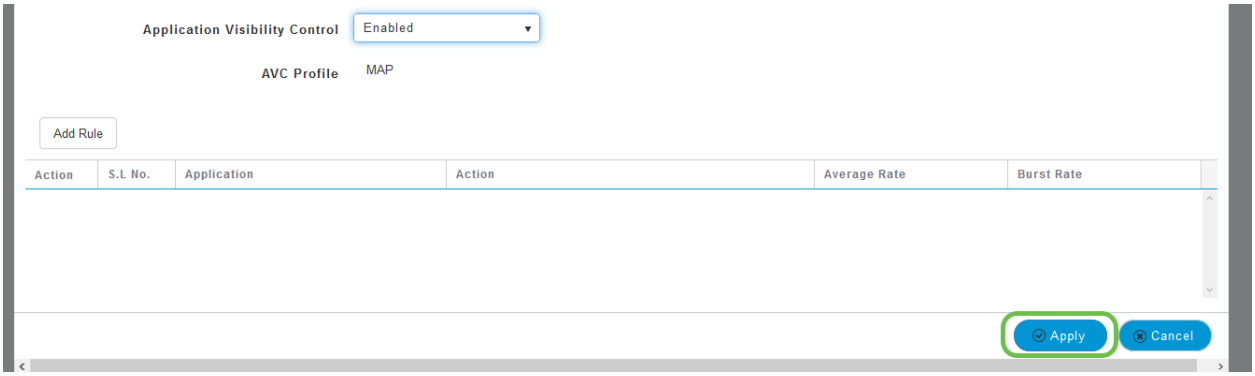
Paso 5

Hacia la parte inferior de la página, encontrará la función *Control de visibilidad de la aplicación*. Esto está desactivado de forma predeterminada. Haga clic en el menú desplegable y seleccione **Enabled**.



Paso 6

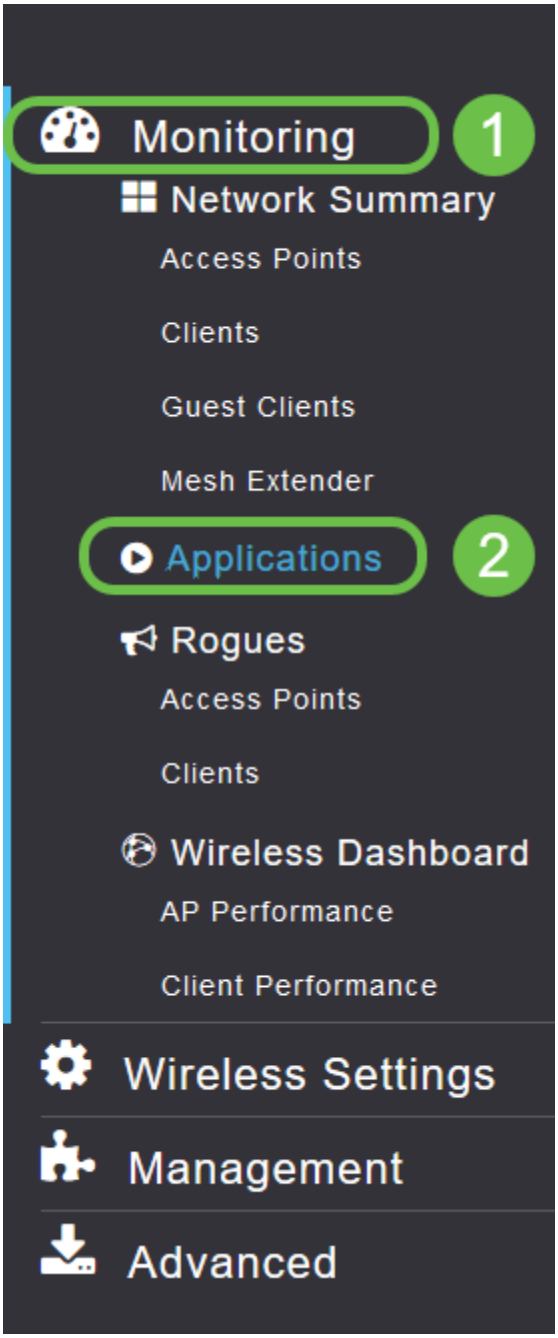
Haga clic en el botón **Aplicar**.



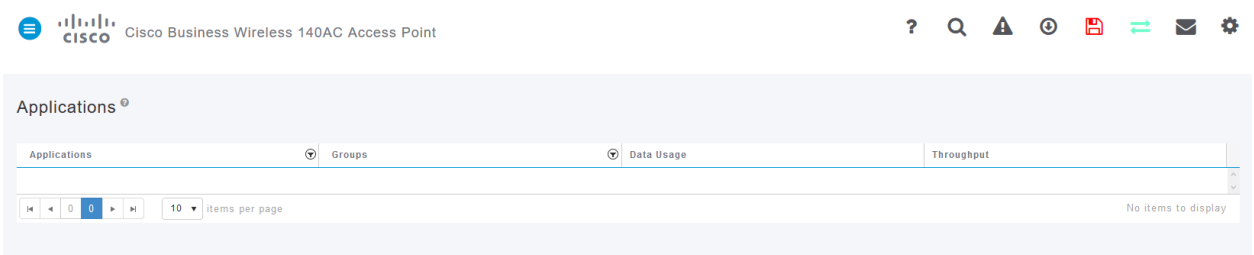
Esta configuración debe estar activada, de lo contrario la función no funcionará.

Paso 7

Haga clic en el botón Cancel (Cancelar) para cerrar el submenú WLAN. A continuación, haga clic en el menú **Supervisión** de la barra de menús izquierda. Una vez que pueda, haga clic en el elemento de menú **Aplicaciones**.



Si no ha tenido tráfico para ninguna fuente, la página estará en blanco, como se muestra a continuación.



Esta página mostrará la siguiente información:

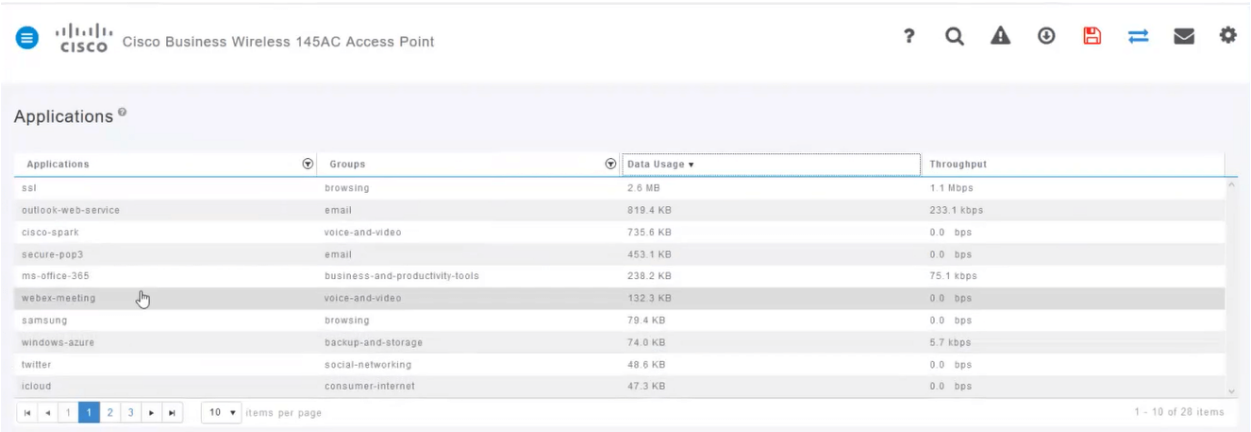
- Aplicación: incluye muchos tipos diferentes
- Grupos: indica el tipo de grupo de aplicaciones para una ordenación más sencilla
- Uso de datos: la cantidad de datos utilizados por este servicio en general
- Rendimiento: la cantidad de ancho de banda utilizada por la aplicación

Puede hacer clic en las pestañas para ordenar de mayor a menor, lo que puede ayudar a identificar a los mayores consumidores de recursos de red.

Esta función es muy eficaz para administrar los recursos WLAN en un nivel granular. A continuación se muestran algunos de los grupos y tipos de aplicaciones más comunes. Es probable que su lista incluya muchos más, incluidos los siguientes grupos y ejemplos:

- Navegación
    - EX: Específico del cliente, SSL
- Correo electrónico
    - EX: Outlook, Secure-pop3
- Voz y vídeo
    - EX: WebEx, Cisco Spark,
- Herramientas empresariales y de productividad
    - EX: Microsoft Office 365,
- Backup y almacenamiento
    - EX: Windows-Azure,
- Internet de consumo
    - iCloud, Google Drive
- Redes sociales
    - EX: Twitter, Facebook
- Actualizaciones de software
    - EX: Google-Play, IOS
- Mensajería instantánea
    - EX: Hangouts, mensajes

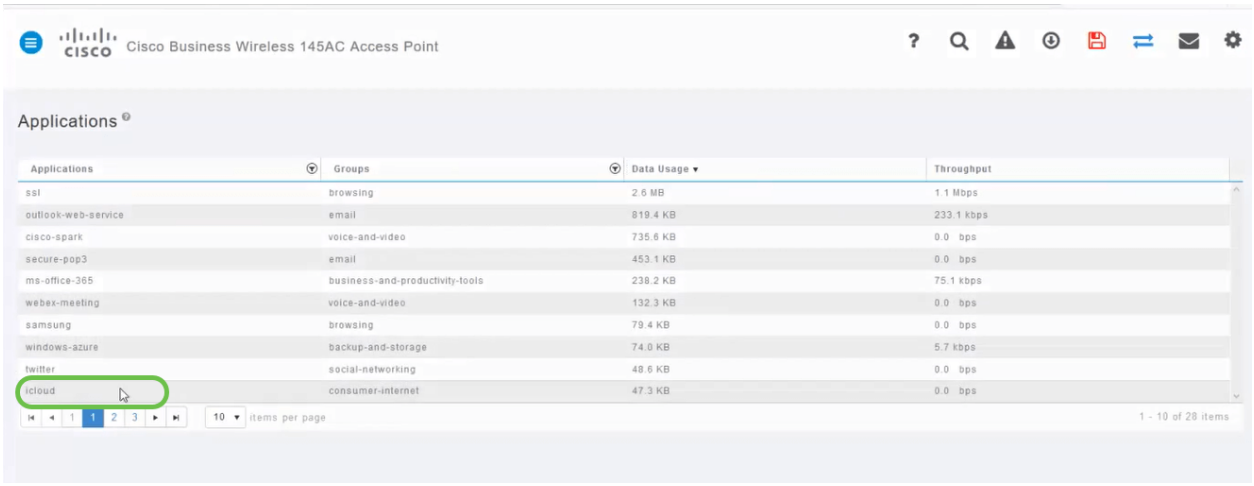
Muestra un ejemplo de cómo se verá la página cuando se rellene.



Cada encabezado de tabla se puede hacer clic para ordenar, lo que resulta especialmente útil para los campos *Uso de datos* y *Rendimiento*.

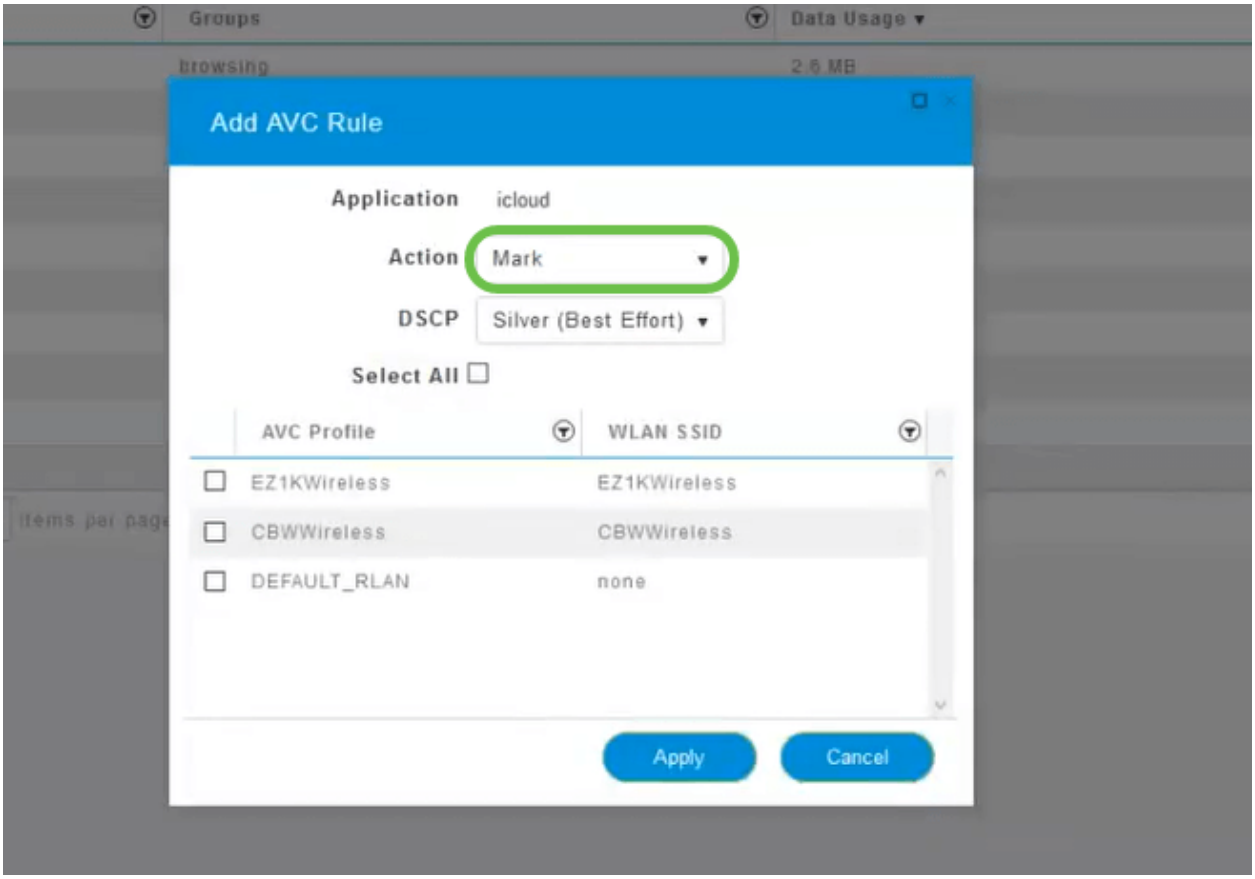
Paso 8

Haga clic en la fila del tipo de tráfico que desea administrar.



Paso 9

Haga clic en el cuadro desplegable **Acción** para seleccionar cómo tratará ese tipo de tráfico.



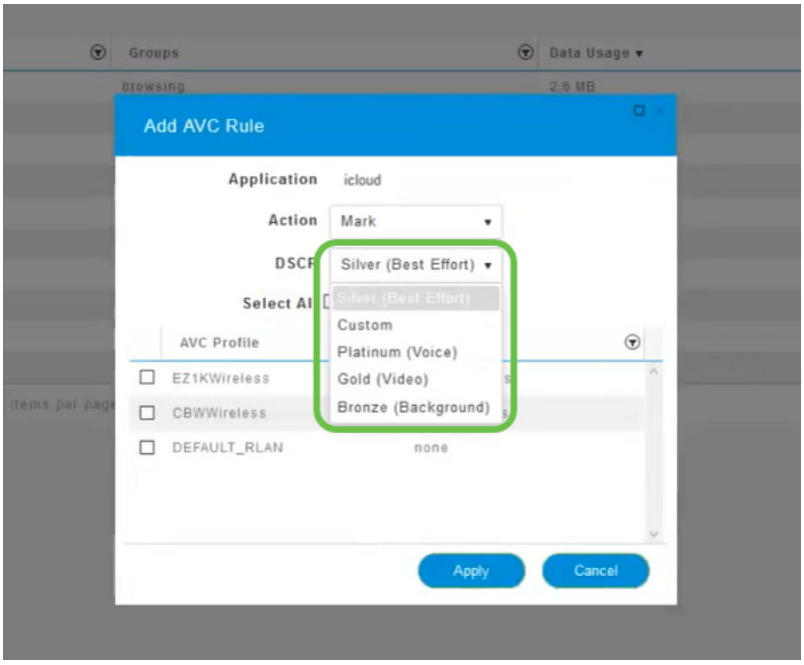
Para este ejemplo, dejamos esta opción en *Mark*.

Acción para tomar en el tráfico

- Marca: coloca el tipo de tráfico en uno de los niveles de punto de código de servicios diferenciados (DSCP) 3, que rigen la cantidad de recursos disponibles para el tipo de aplicación.
- Abandonar: no haga nada más que descartar el tráfico
- Límite de velocidad: permite establecer la velocidad media y la velocidad de ráfaga en Kbps

Paso 10

Haga clic en el cuadro desplegable del campo **DSCP** para seleccionar una de las siguientes opciones.



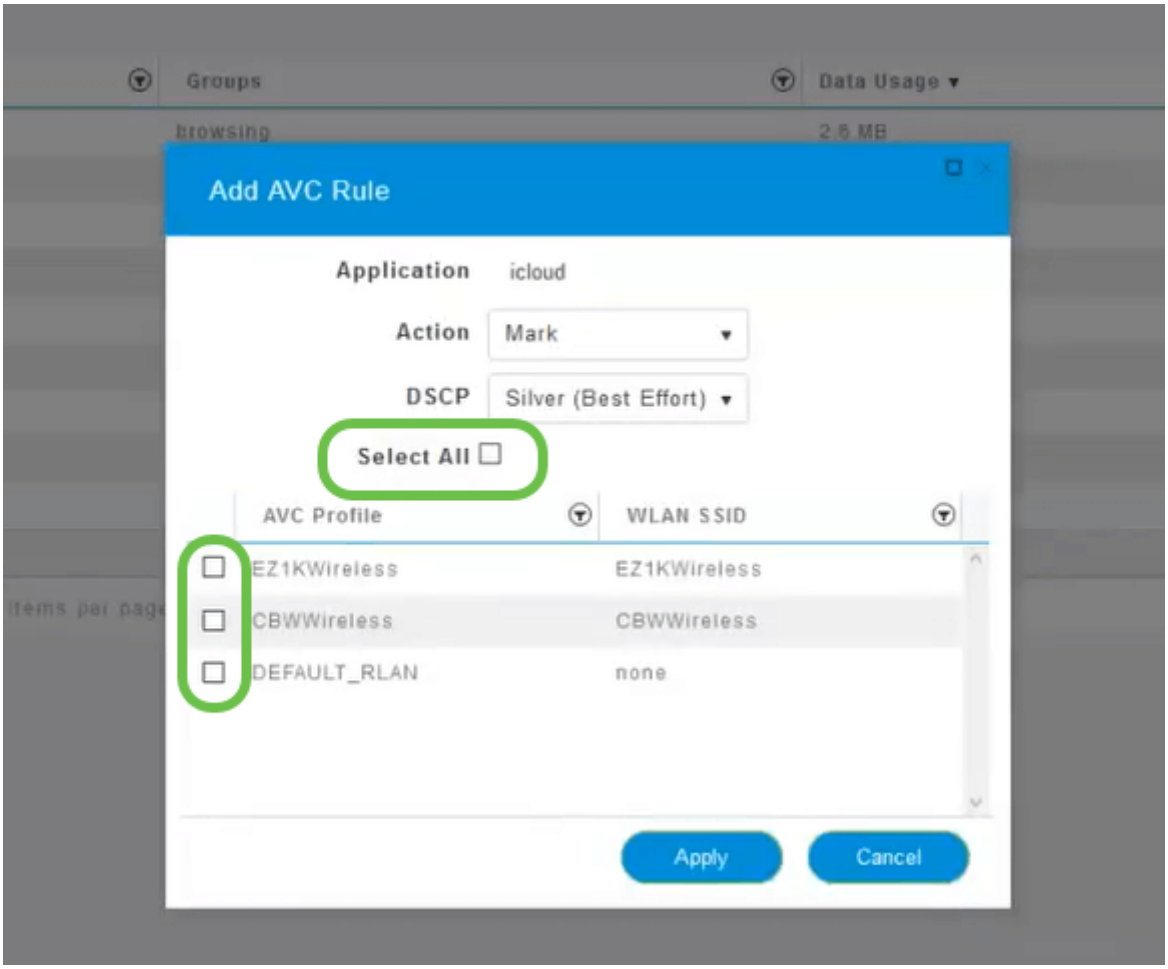
A continuación se muestran las opciones DSCP para que se marque el tráfico. Estas opciones van desde menos recursos a más recursos disponibles para el tipo de tráfico que está editando.

- Bronze (fondo) - Menos
- Silver (mejor esfuerzo)
- Gold (vídeo)
- Platinum (voz) más
- Personalizado - Conjunto de usuarios

Como convención web, el tráfico ha migrado hacia la navegación SSL, lo que le impide ver qué hay dentro de los paquetes a medida que se mueven de la red a la WAN. Como tal, una gran mayoría del tráfico web utilizará SSL. Configurar el tráfico SSL para una prioridad más baja puede afectar a su experiencia de navegación.

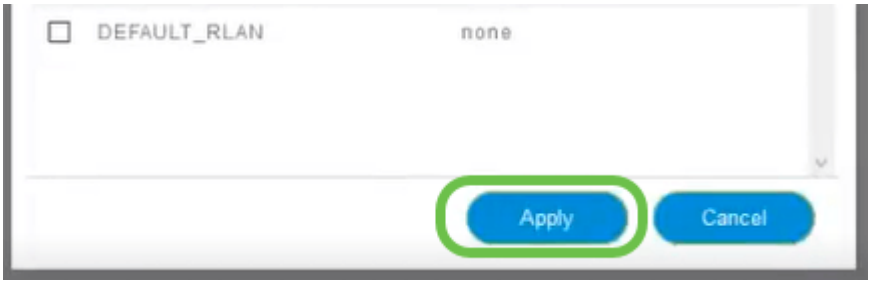
Paso 11

Ahora seleccione el SSID individual que desea ejecutar esta política o haga clic en **Seleccionar todo**.



Paso 12

Ahora haga clic en **Aplicar** para comenzar esta política.



Dos casos en los que podría aplicarse lo siguiente:

- Invitados/usuarios transmiten una gran cantidad de tráfico que impide el paso del tráfico crítico. Puede aumentar la prioridad de voz, reducir la prioridad del tráfico de Netflix para mejorar las cosas.
- Las actualizaciones de software de gran tamaño que se descargan durante el horario de oficina se pueden desasignar o limitar la tasa.

¡Lo hiciste! La creación de perfiles de aplicaciones es una herramienta muy potente que se puede habilitar aún más habilitando la creación de perfiles de clientes, como se detalla en la siguiente sección.

Definición de perfiles de cliente mediante la interfaz de usuario Web (opcional)

Al conectarse a una red, los dispositivos intercambian información de perfiles de cliente. De forma predeterminada, *Perfiles de cliente* está inhabilitado. Esta información puede incluir:

- Host Name (Nombre de host) o el nombre del dispositivo
- Sistema operativo: el software principal del dispositivo
- Versión del sistema operativo: iteración del software aplicable

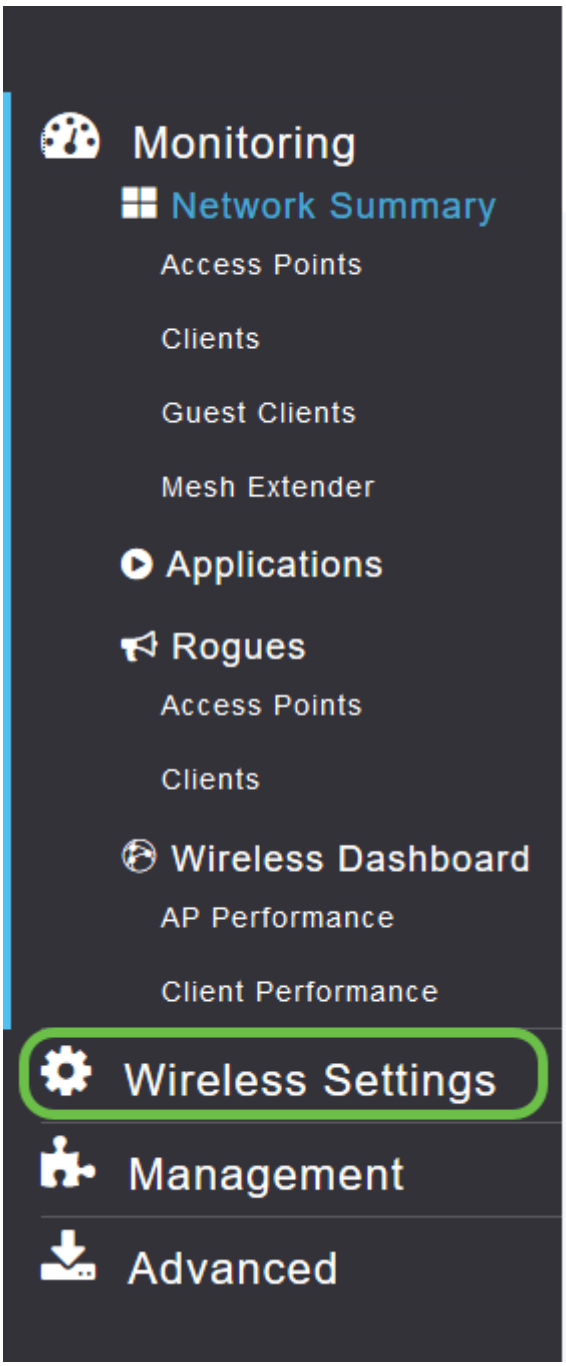
Las estadísticas sobre estos clientes incluyen la cantidad de datos utilizados y el rendimiento.

El seguimiento de perfiles de cliente permite un mayor control sobre la red de área local inalámbrica. O bien, podría utilizarlo como función de otra función. Por ejemplo, el uso de tipos de dispositivos de regulación de aplicaciones que no transportan datos críticos para su empresa.

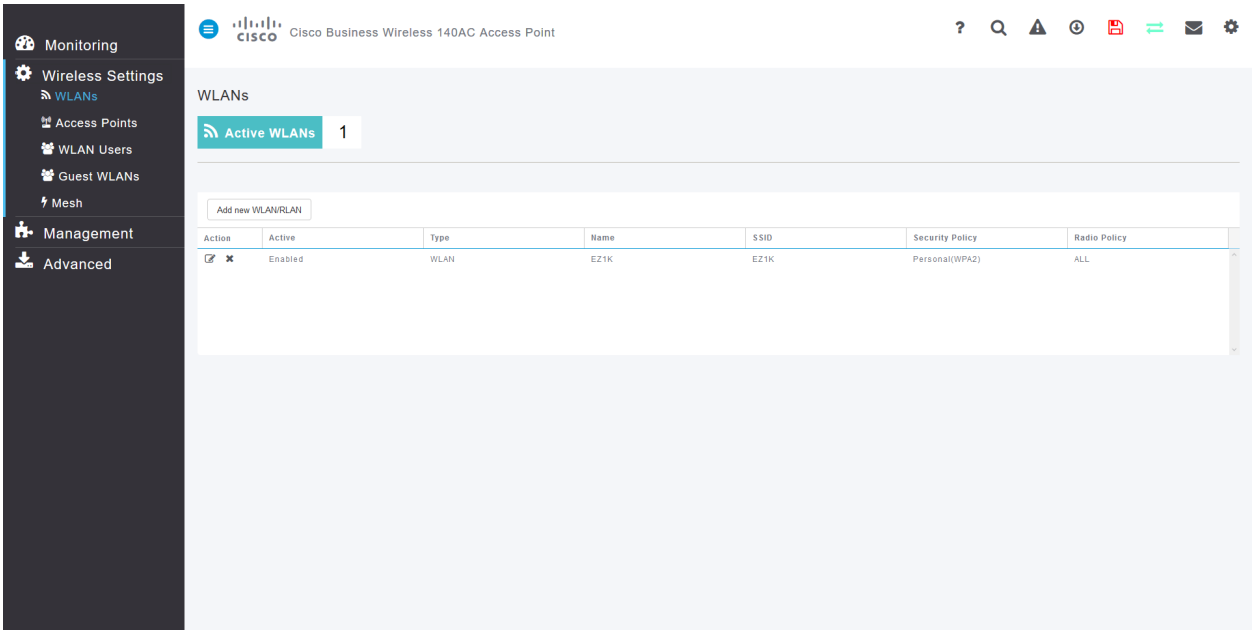
Una vez habilitada, los detalles del cliente de la red se pueden encontrar en la sección Supervisión de la interfaz de usuario web.

Paso 1

Haga clic en **Wireless Settings**.

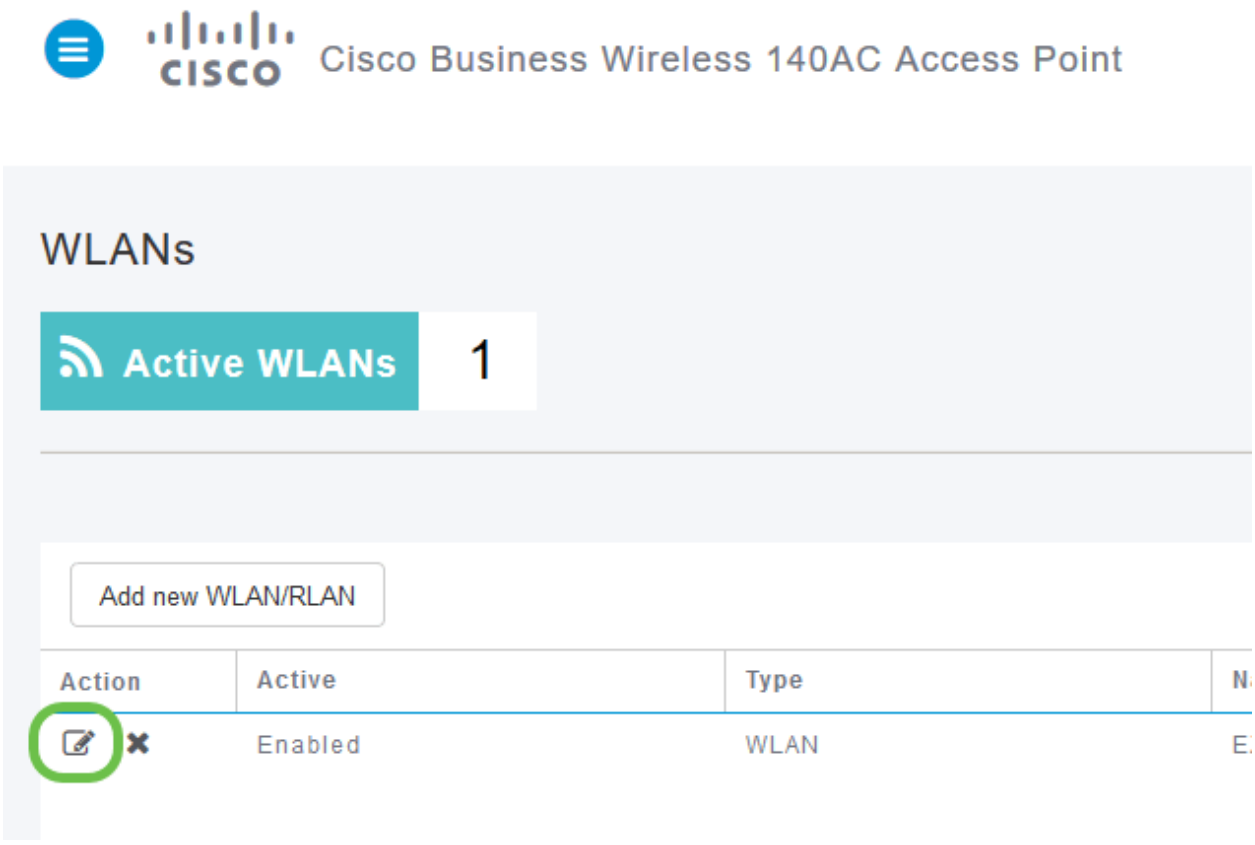


A continuación, se muestra una descripción similar a la que verá al hacer clic en el enlace Wireless Settings (Parámetros inalámbricos):



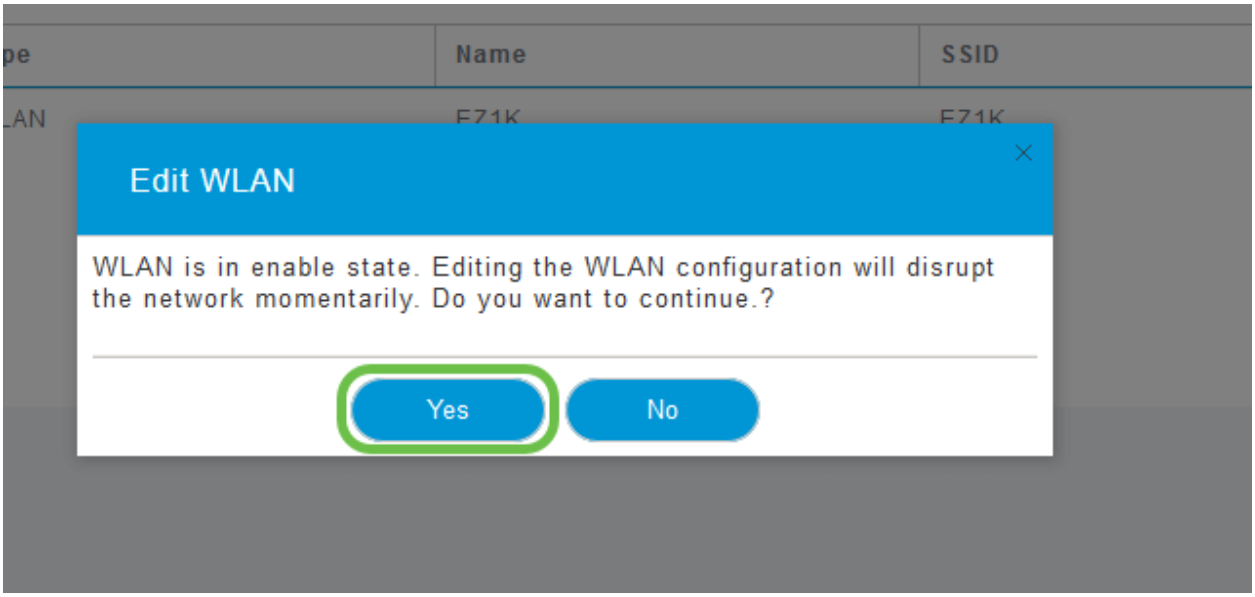
Paso 2

Decida qué WLAN desea utilizar para la aplicación y haga clic en el **icono de edición** que se encuentra a la izquierda.



Paso 3

Puede aparecer un menú emergente similar al que aparece a continuación. Este mensaje importante puede afectar temporalmente al servicio en su red. Haga clic en **Sí** para avanzar.

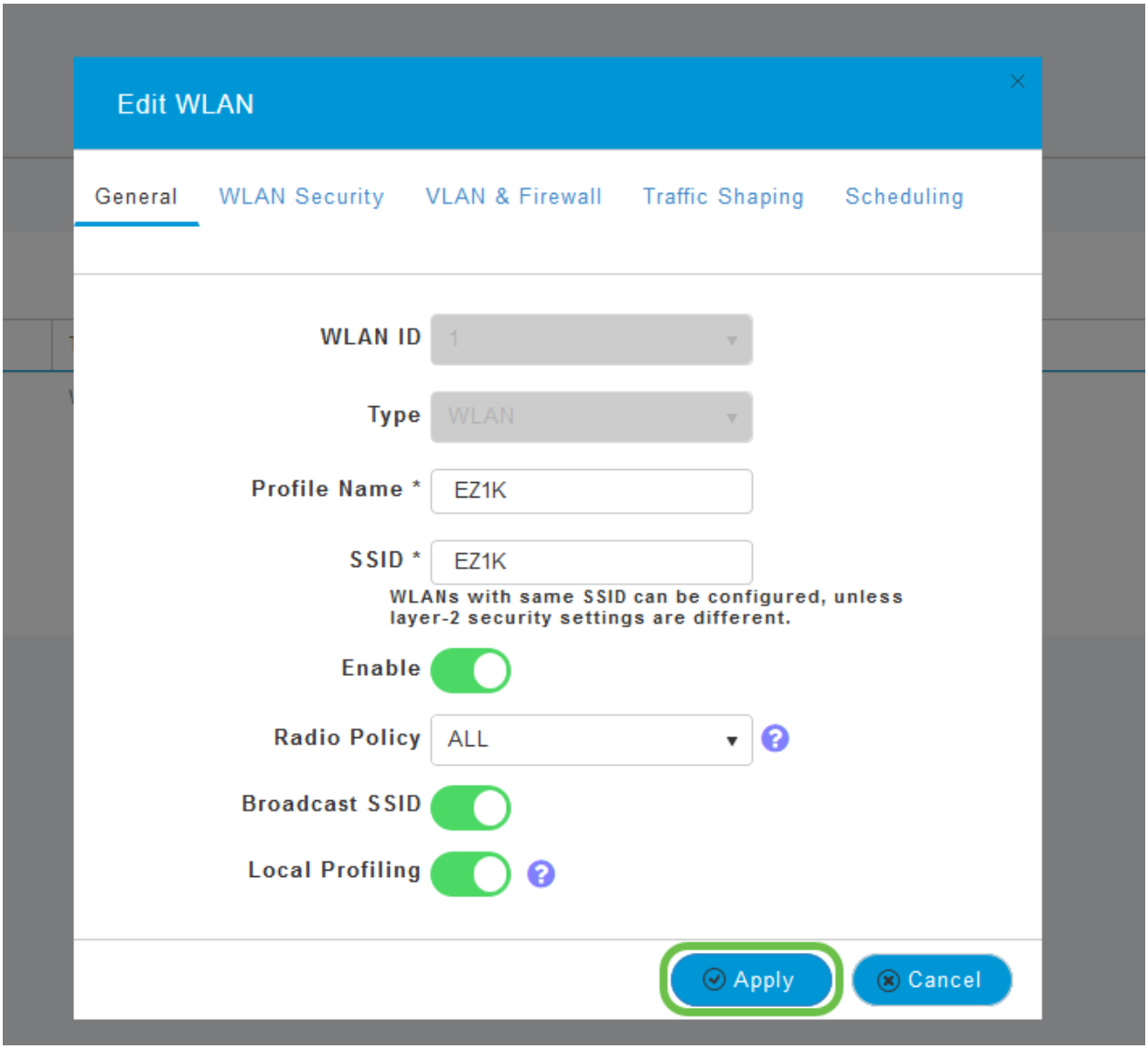


Paso 4

Cambie la definición de perfiles de cliente haciendo clic en el botón de alternancia **de perfiles locales**.

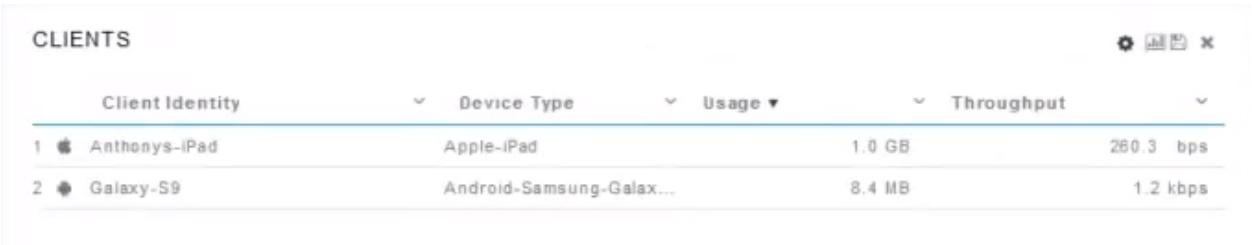
Paso 5

Haga clic en Apply (Aplicar).



Paso 6

Haga clic en el elemento de menú de la sección **Supervisión** en el lado izquierdo. Verá que los datos del cliente comienzan a aparecer en el Panel de la ficha *Supervisión*.



Conclusión

Ya ha completado la configuración de su red segura. ¡Qué gran sensación, ahora toma un minuto para celebrar y luego ponerte a trabajar!

Queremos lo mejor para nuestros clientes, así que tiene cualquier comentario o sugerencia sobre este tema, por favor envíenos un correo electrónico al equipo de contenido de Cisco.

Si desea leer otros artículos y documentación, consulte las páginas de soporte de su

hardware:

- Router VPN Cisco RV260P con PoE
- Punto de acceso Cisco Business 140AC
- Cisco Business 142ACM Mesh Extender