Configuración de red total: RV345P y Cisco Business Wireless con la interfaz de usuario web

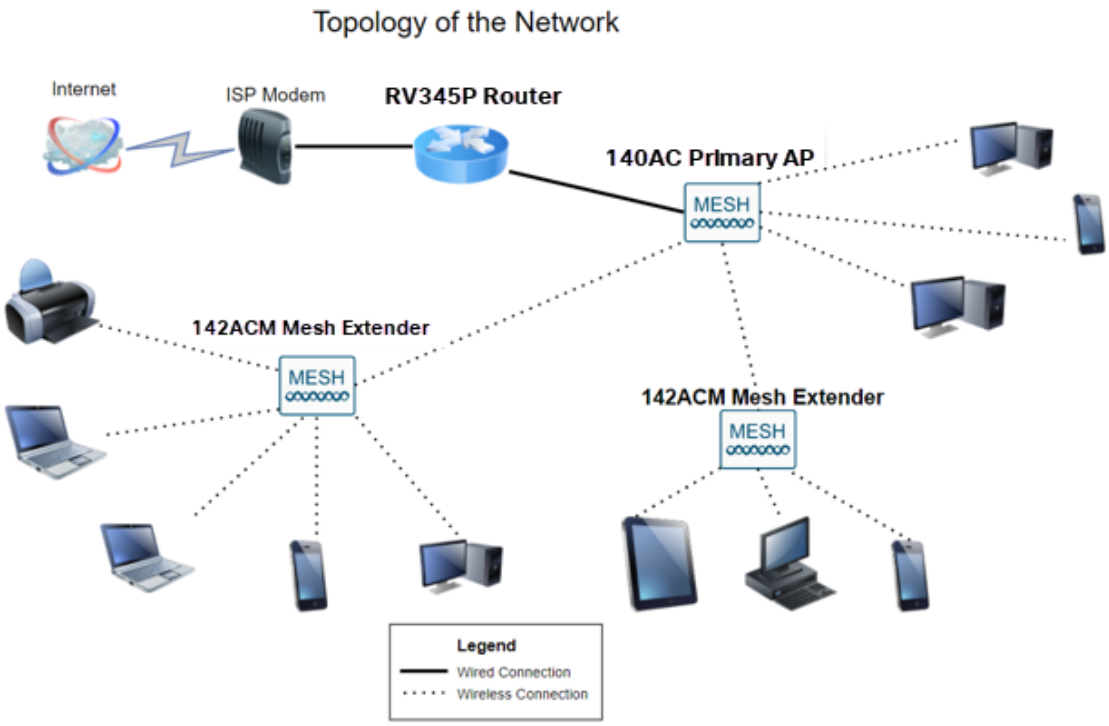
Objetivo

Esta guía le mostrará cómo configurar una red de malla inalámbrica mediante un router RV345P, 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.

Table Of Contents

Topología



Introducción

Todas sus investigaciones se han unido y ha adquirido sus equipos de Cisco, ¡qué emocionante! En esta situación, estamos utilizando un router RV345P. 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.

Este router avanzado también ofrece la opción de funciones adicionales.

1. El control de aplicaciones permite controlar el tráfico. Esta función se puede configurar para permitir el tráfico pero para registrarlo, bloquear el tráfico y registrarlo, o simplemente para bloquear el tráfico.
2. El filtrado web se utiliza para evitar que el tráfico web llegue a sitios web inseguros o inadecuados. No hay registro con esta función.

3. AnyConnect es una red privada virtual (VPN) de capa de conexión segura (SSL) disponible en Cisco. Las VPN permiten que los usuarios y sitios remotos se conecten a la oficina de su empresa o a los Data Centers creando un túnel seguro a través de Internet.

Si desea utilizar estas funciones, deberá adquirir una licencia. Los routers y las licencias se registran en línea, lo que se tratará en esta guía.

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

Dispositivos aplicables | Versión de software

- RV345P |1.0.03.21
- CBW140AC |10.4.1.0
- CBW142ACM | 10.4.1.0 (se necesita al menos un extensor de malla para la red de malla)

Prerequisites

Preparación del router

1. Asegúrese de que dispone de una conexión a Internet actual para la configuración.
2. Póngase en contacto con el distribuidor de servicios de Internet (ISP) para obtener información sobre las instrucciones especiales que tenga al utilizar el router RV345P. 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.

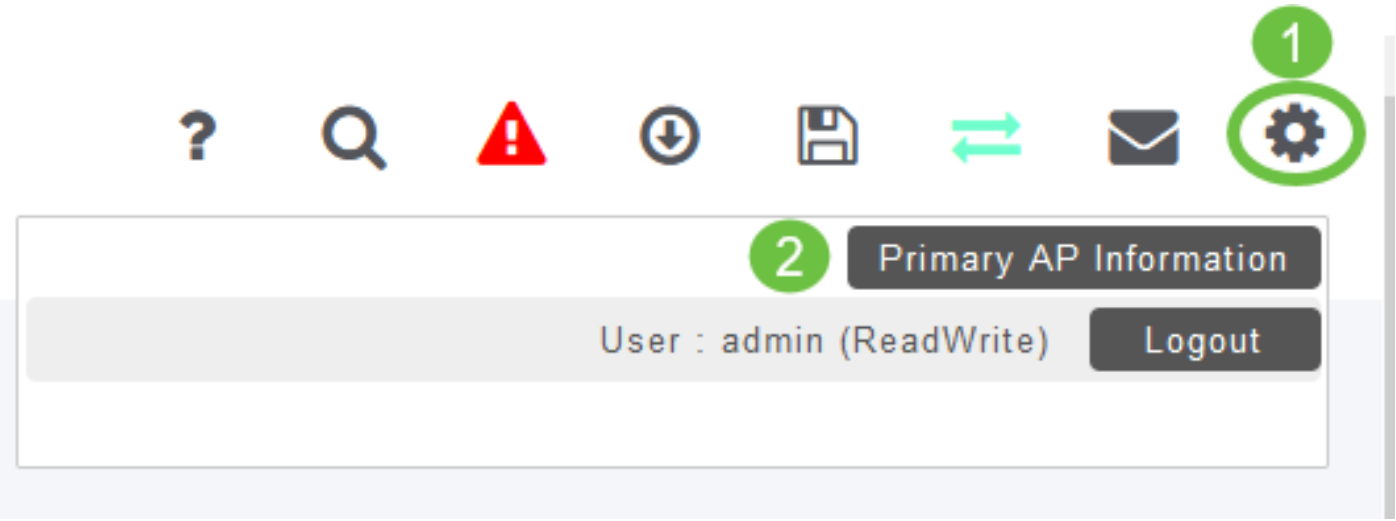
Obtener una cuenta de Cisco.com

Ahora que posee equipos de Cisco, necesita obtener una cuenta de Cisco.com, a veces denominada identificación online de conexión de Cisco (ID de CCO). No hay cargos por una cuenta.

Si ya tiene una cuenta, puede saltar a la siguiente sección de este artículo.

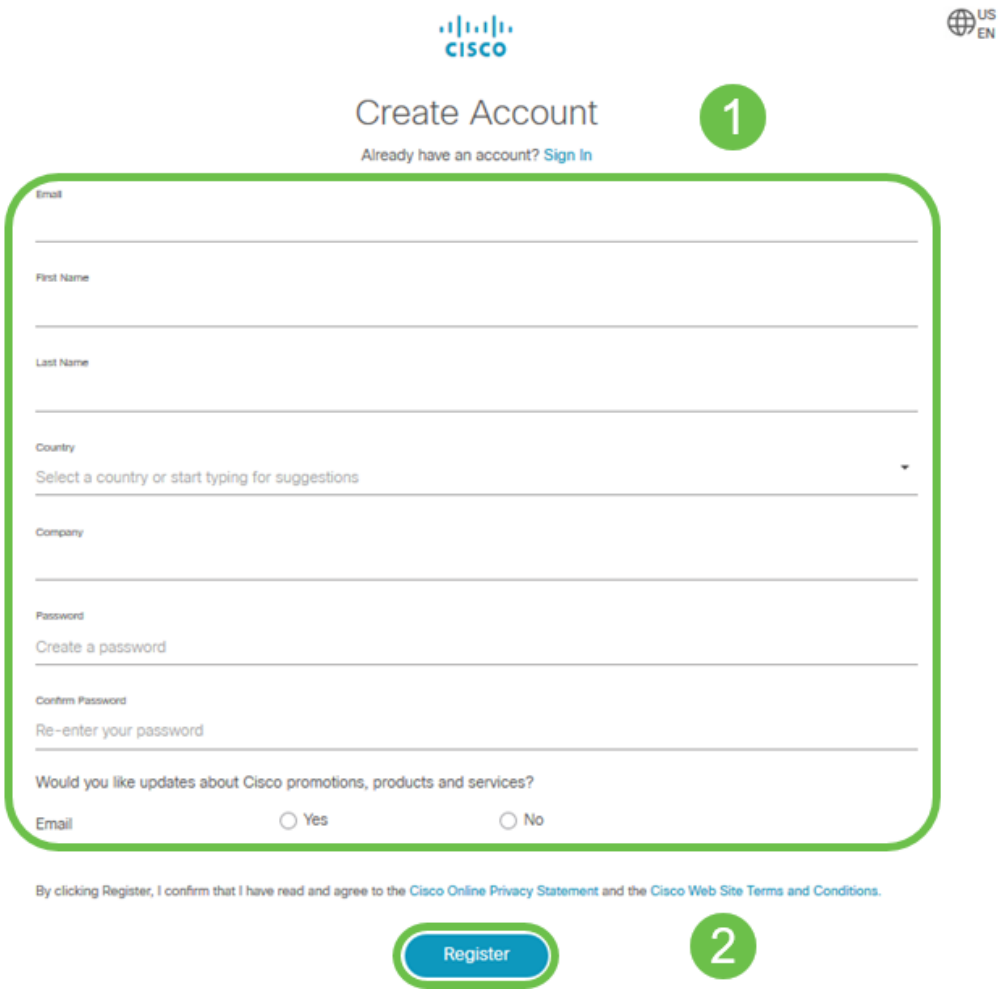
Paso 1

Vaya a Cisco.com. Haga clic en el **icono de persona** y, a continuación, **Crear una cuenta**.



Paso 2

Introduzca los detalles necesarios para crear la cuenta y haga clic en **Registrarse**. Siga las instrucciones para completar el proceso de registro.



Si tiene algún problema, haga clic para saltar a la página de ayuda de Registro de cuenta de Cisco.com.

Configuración del router RV345P

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 RV345P incluye parámetros predeterminados optimizados para muchas pequeñas empresas. Sin embargo, las demandas de la red o el proveedor de servicios de Internet (ISP) puede requerir que modifique 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.

¿Estás listo? ¡Vamos a ello!

RV345P fuera de la caja

Paso 1

Conecte el cable Ethernet desde uno de los puertos RV345P 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 RV345P para realizar la configuración inicial.

Paso 2

Asegúrese de utilizar el adaptador de corriente suministrado con el RV345P. El uso de un adaptador de corriente diferente podría dañar el RV345P 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 RV345P, 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 RV345P.

Paso 5

Conecte el otro extremo del adaptador RV345P a una toma de corriente. Esto encenderá el RV345P. 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 RV345P ha finalizado el arranque.

Configuración del router

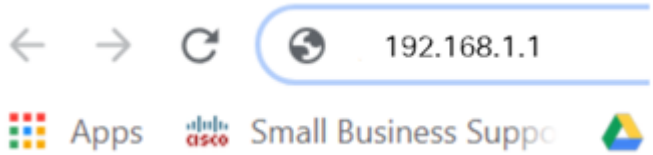
El trabajo preparatorio se ha realizado, ahora es el momento de llegar a algunas configuraciones. Para iniciar la interfaz de usuario Web, siga estos pasos.

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.

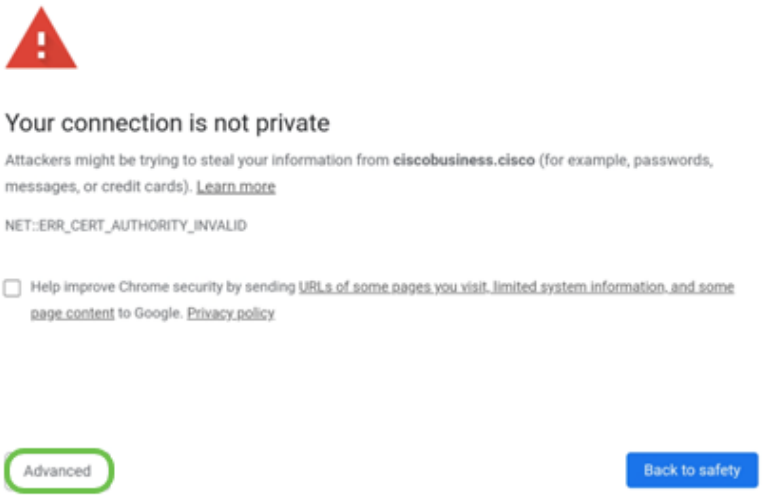
Paso 2

Abra un explorador web como Safari, Internet Explorer o Firefox. En la barra de direcciones, introduzca la dirección IP predeterminada del RV345P, 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.

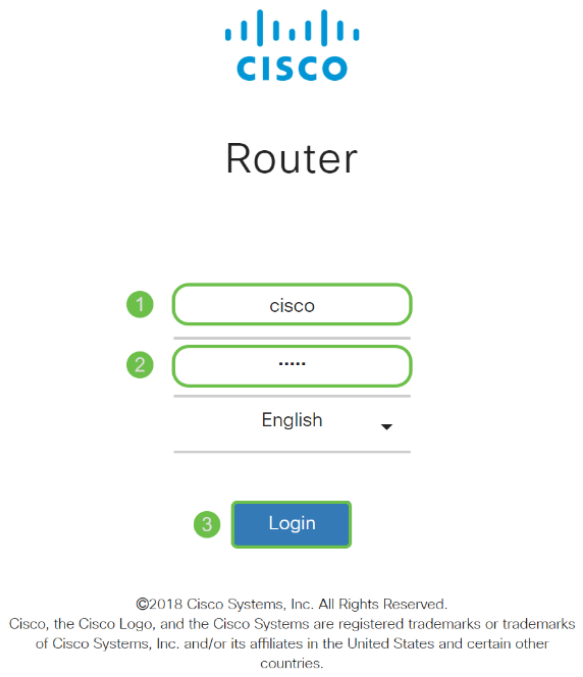


Paso 4

Cuando aparezca la página de inicio de sesión, ingrese el nombre de usuario predeterminado *cisco* y la contraseña predeterminada *cisco*.

Haga clic en Login (Conexión).

Para obtener información detallada, haga clic en Cómo acceder a la página de configuración basada en web de los Cisco RV340 Series VPN Routers.



Paso 5

Haga clic en Login (Conexión). Aparecerá la página *Introducción*. Si el panel de navegación no está abierto, puede abrirlo haciendo clic en el **icono del menú**.

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 la conectividad no ocurre, puede ver este artículo Resolución de problemas.

Otras cosas que se deben intentar:

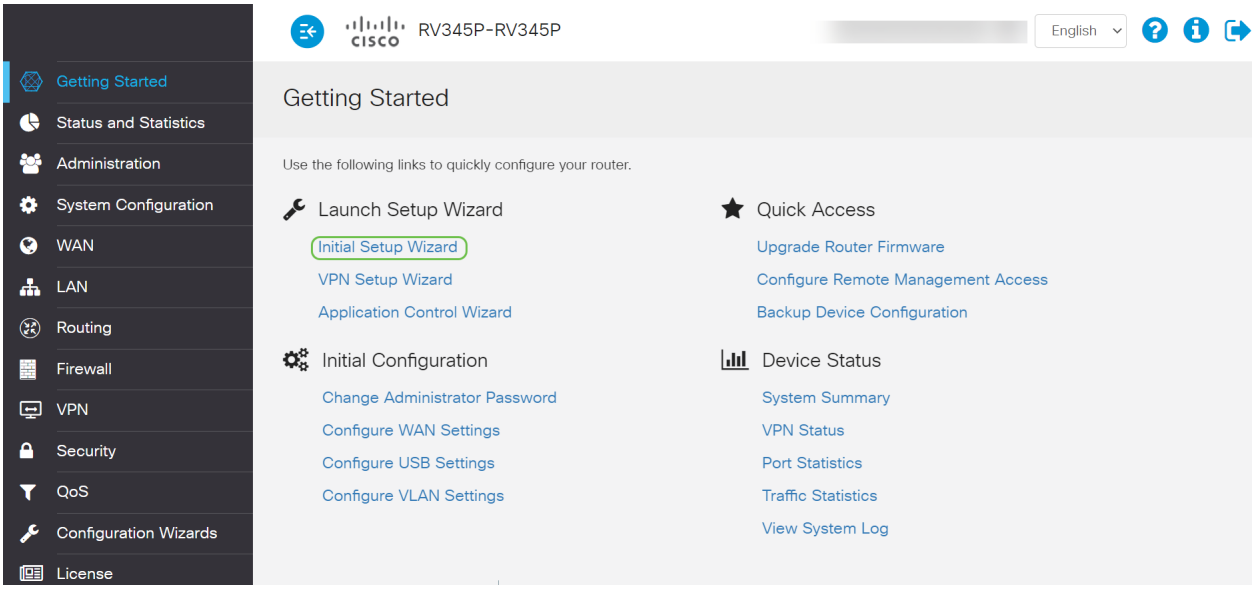
1. Compruebe que el explorador Web no está configurado en Trabajar sin conexión.
2. Compruebe los parámetros de conexión de red de área local del adaptador Ethernet. El PC debe obtener una dirección IP a través de DHCP. Alternativamente, el PC puede tener una dirección IP estática en el rango 192.168.1.x con el gateway predeterminado establecido en 192.168.1.1 (la dirección IP predeterminada del RV345P). Para conectarse, es posible que deba modificar los parámetros de red del RV345P. 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 RV345P apagando ambos dispositivos. A continuación, encienda el módem y déjelo inactivo durante unos 2 minutos. A continuación, encienda el RV345P. 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* enumerados en esta sección. Puede cambiar estos parámetros en cualquier momento.

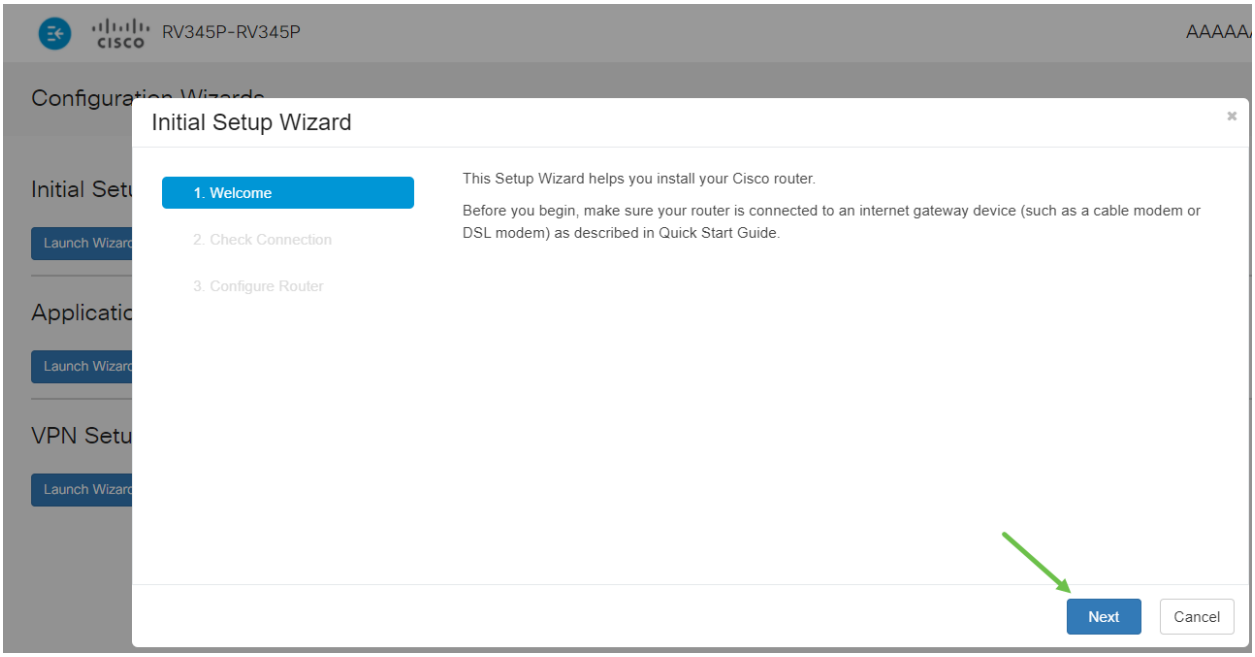
Paso 1

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



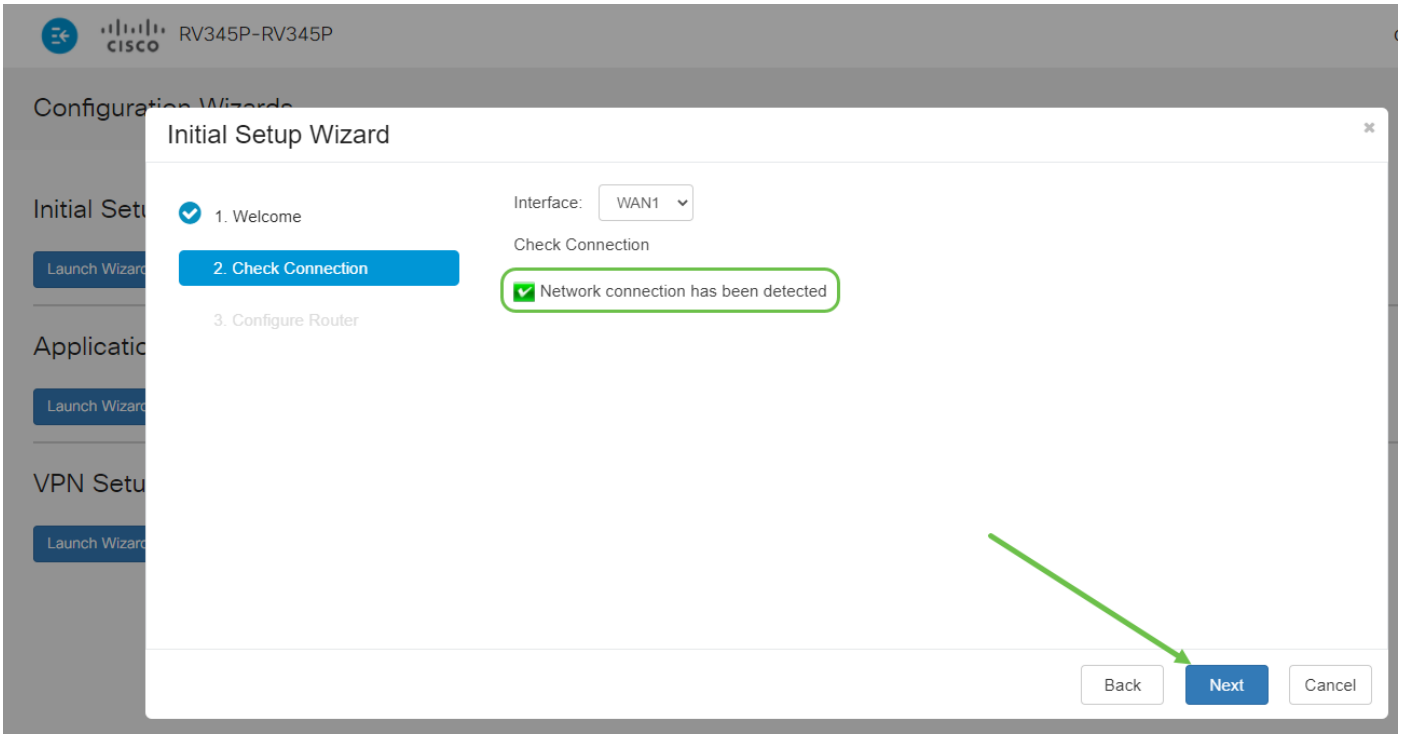
Paso 2

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



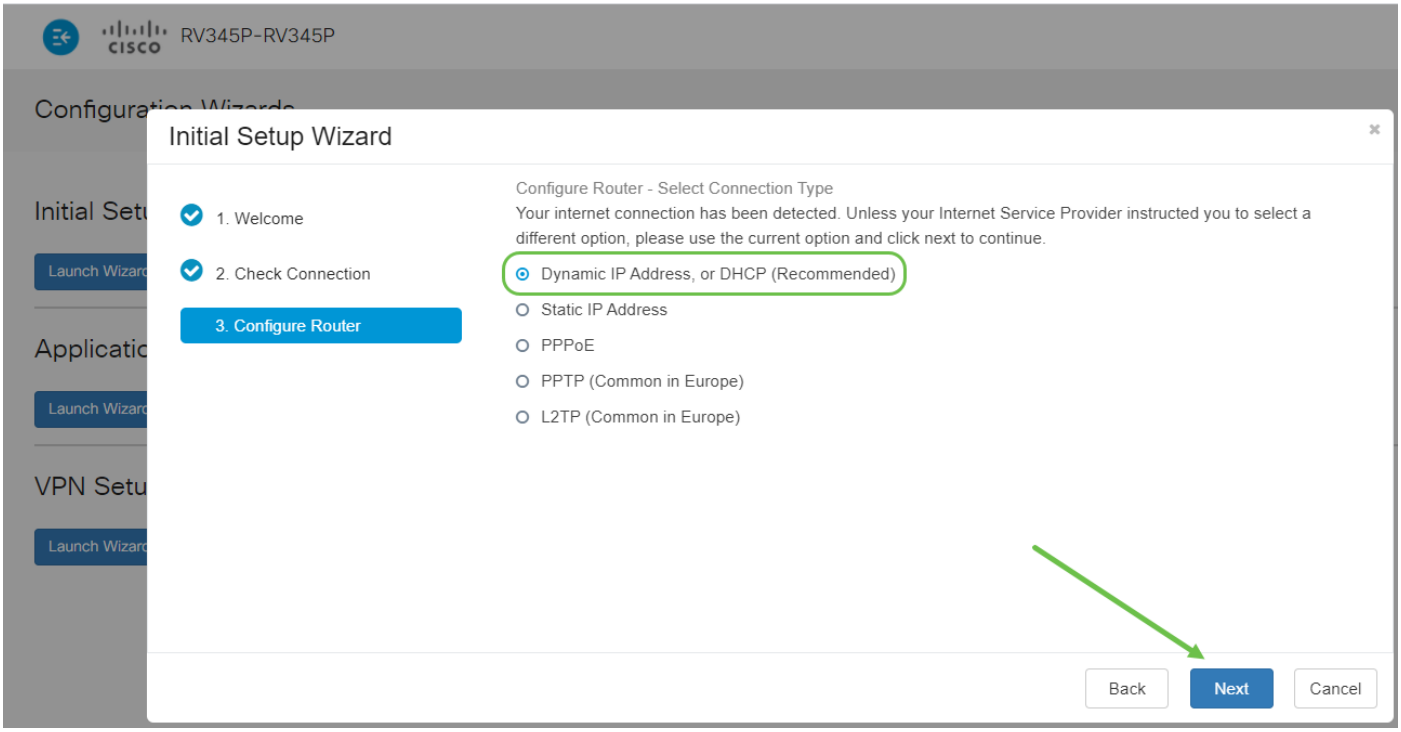
Paso 3

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



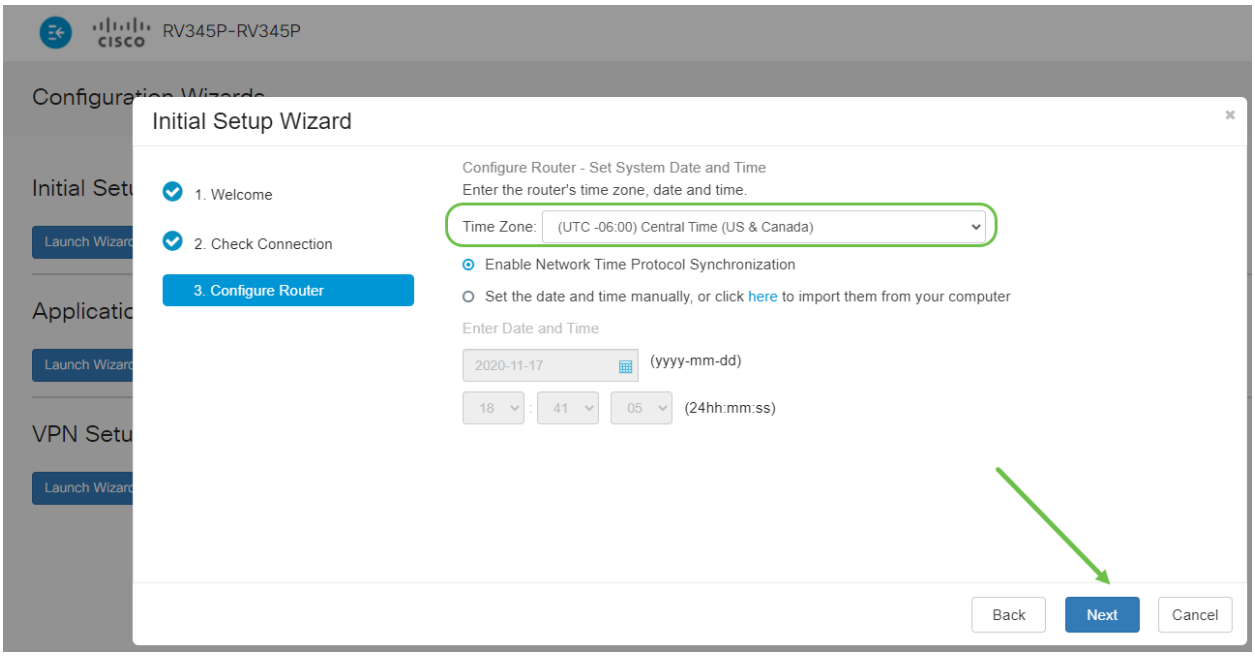
Paso 4

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



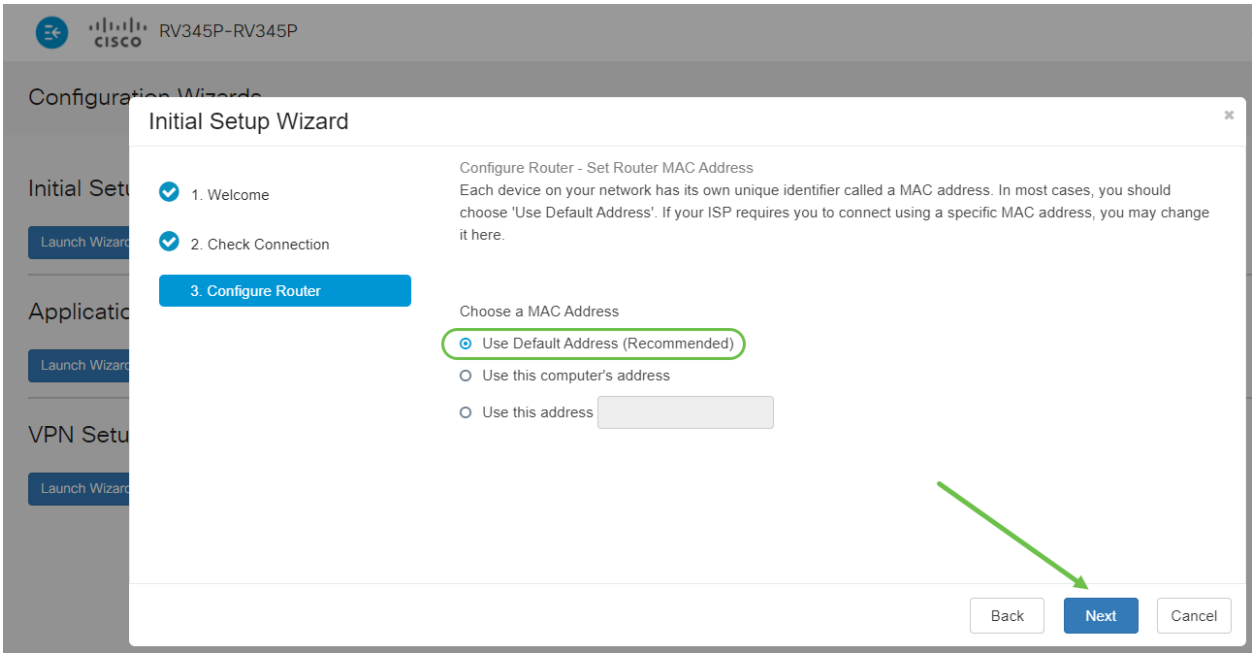
Paso 5

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**.



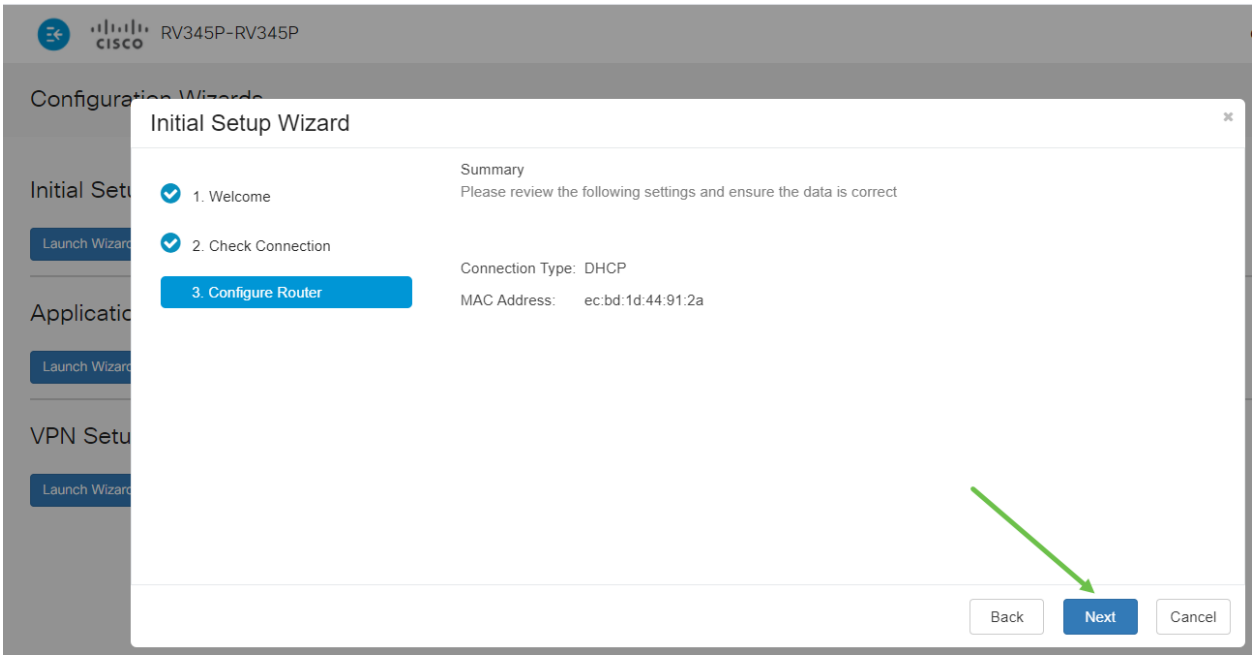
Paso 6

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



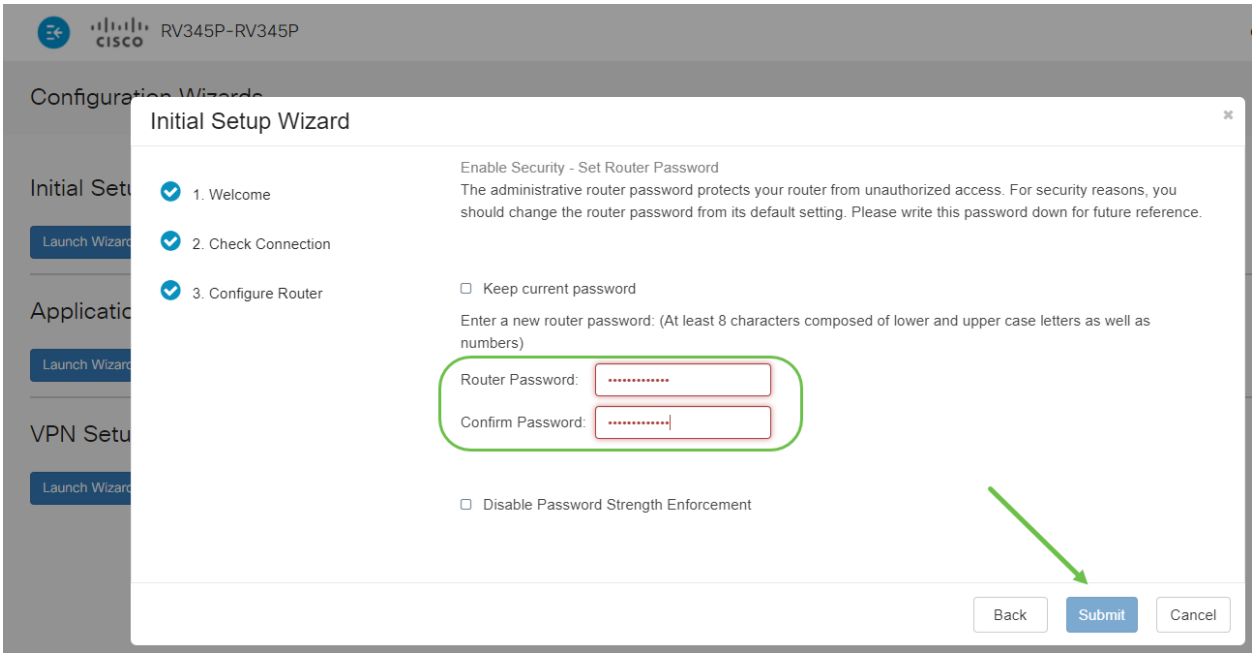
Paso 7

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**.

Si desea obtener más información sobre estos parámetros, puede leer Configuración de DHCP WAN Settings en el router RV34x.

El RV345P tiene la alimentación a través de Ethernet (PoE) activada de forma predeterminada, pero puede realizar algunos ajustes en ellos. Si necesita personalizar los parámetros, consulte Configuración de los parámetros de alimentación a través de Ethernet (PoE) en el router RV345P.

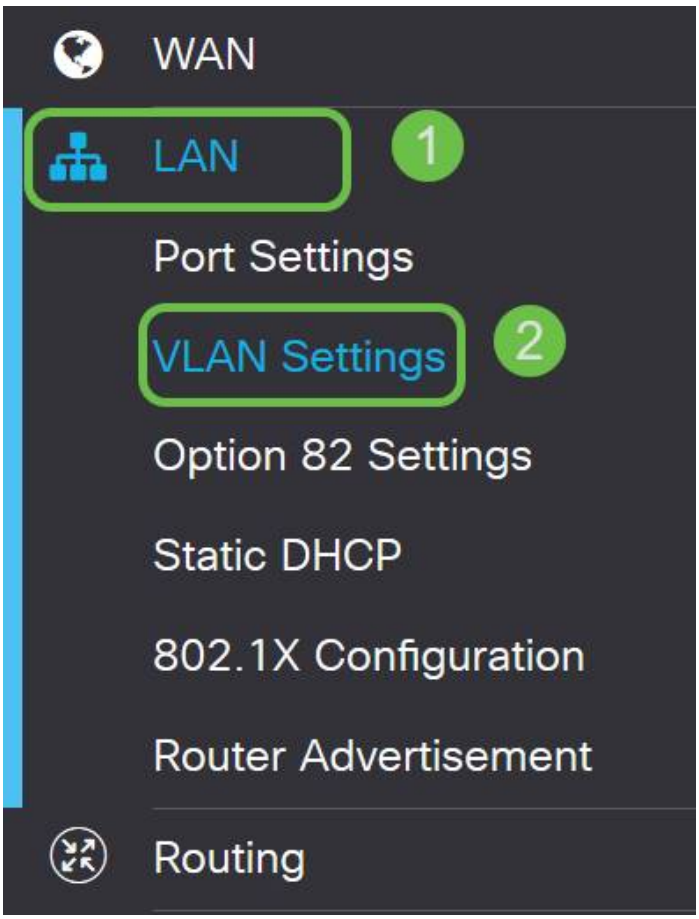
Editar una dirección IP si es necesario (opcional)

Después de completar el *Asistente de configuración inicial*, puede establecer una dirección IP estática en el router editando los parámetros de VLAN.

Este proceso sólo es necesario si la dirección IP del router necesita que se le asigne una dirección específica en la red existente. Si no necesita editar una dirección IP, puede pasar a la siguiente sección de este artículo.

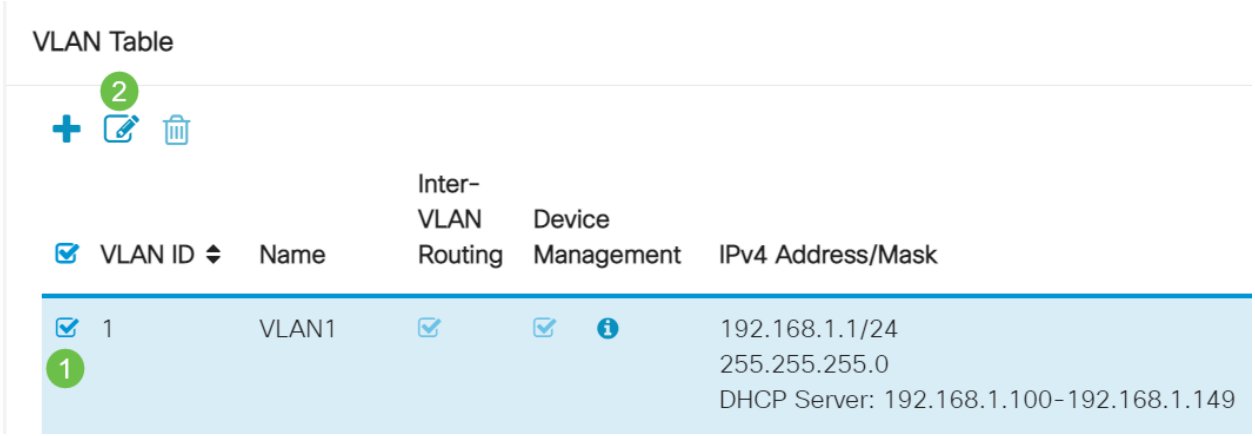
Paso 1

En el menú de la izquierda, haga clic en **LAN > VLAN Settings**.



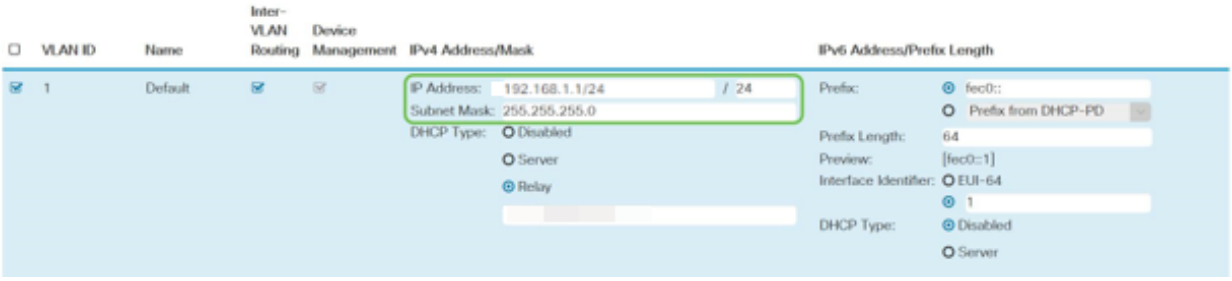
Paso 2

Seleccione la **VLAN** que contiene su dispositivo de ruteo y luego haga clic en el **icono de edición**.



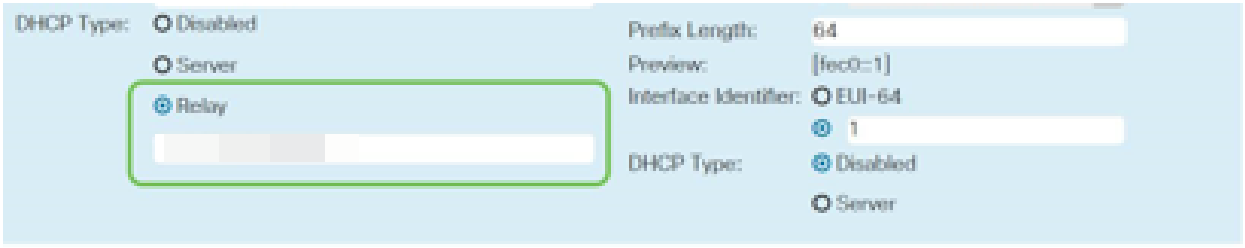
Paso 3

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.

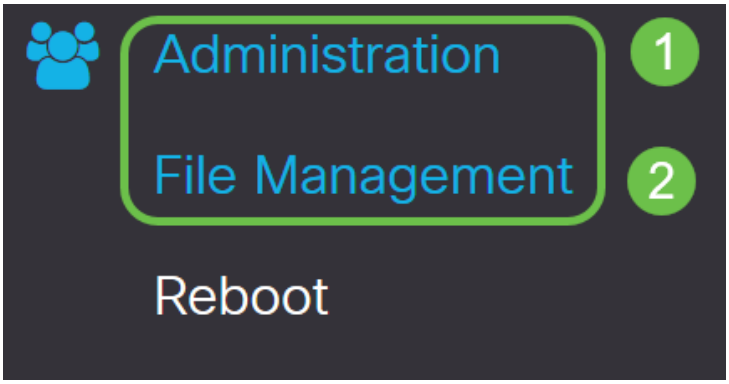


Actualización del firmware si es necesario

Este es un paso importante, ¡no lo omita!

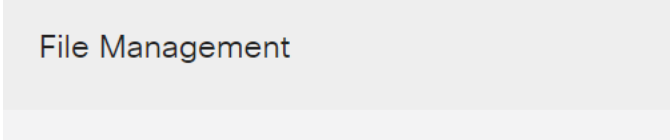
Paso 1

Elija **Administration > File Management**.



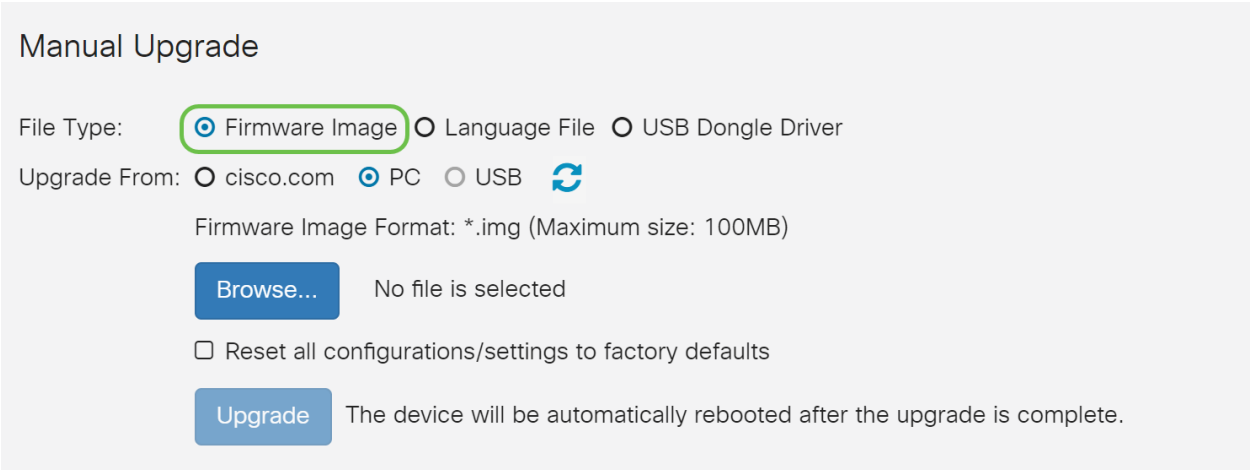
En el área *Información del sistema*, las siguientes subáreas describen lo siguiente:

- 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

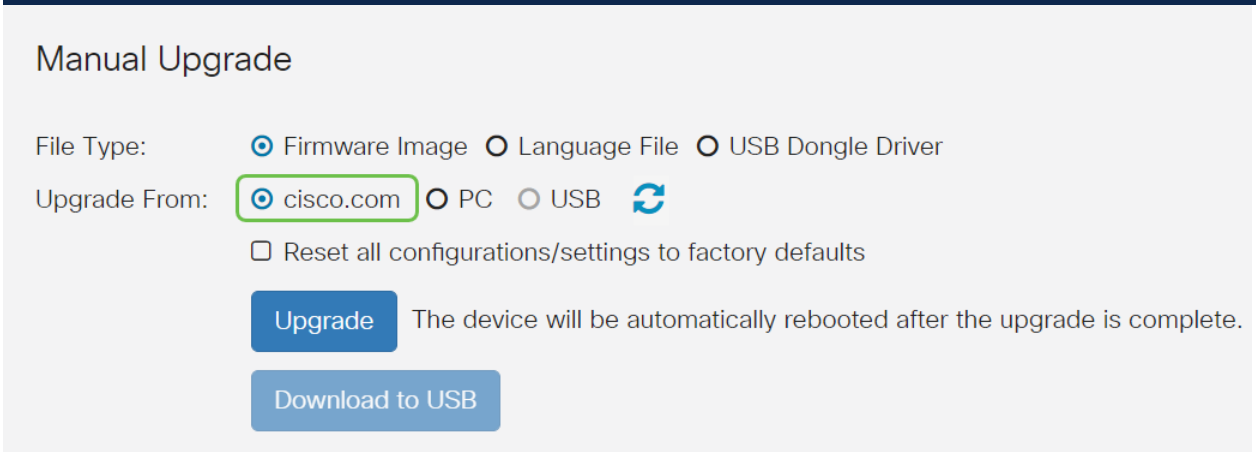
En la sección *Actualización manual*, haga clic en el botón de opción **Firmware Image** para *Tipo de archivo*.



Paso 3

En la página *Actualización manual*, haga clic en el 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.

Si su dispositivo no está conectado a Internet o sufre desconexiones a Internet, no podrá actualizar desde cisco.com. Si esto le concierne, las opciones alternativas se pueden encontrar aquí.

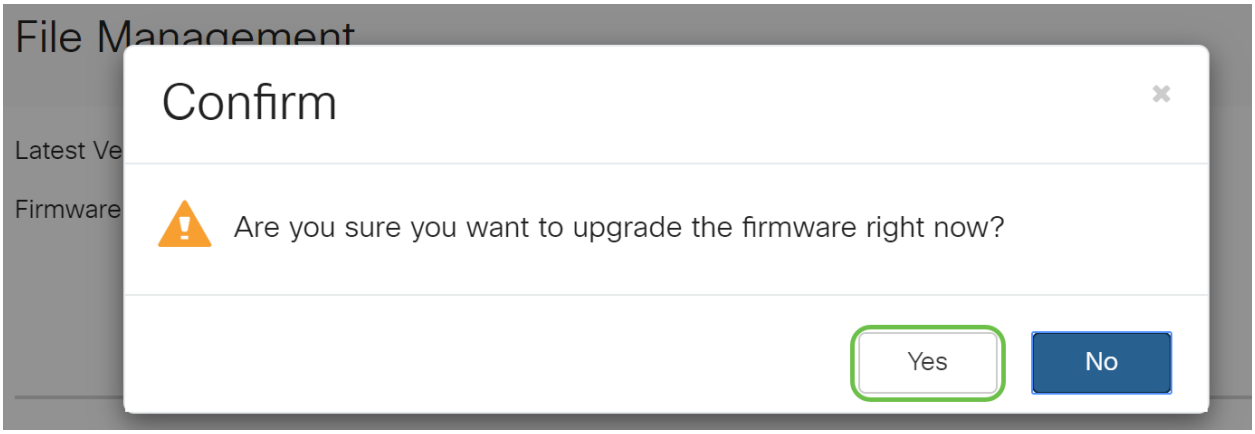


Paso 4

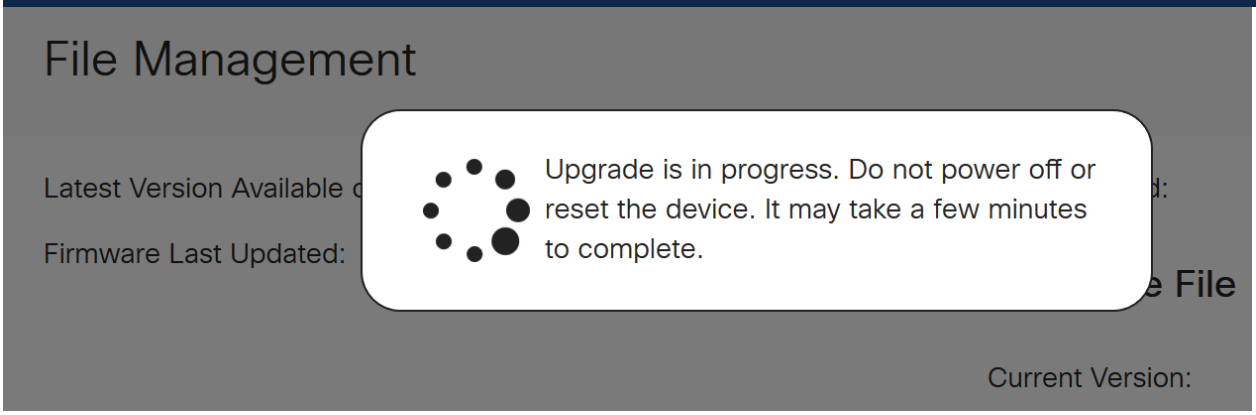
Haga clic en Upgrade.

Paso 5

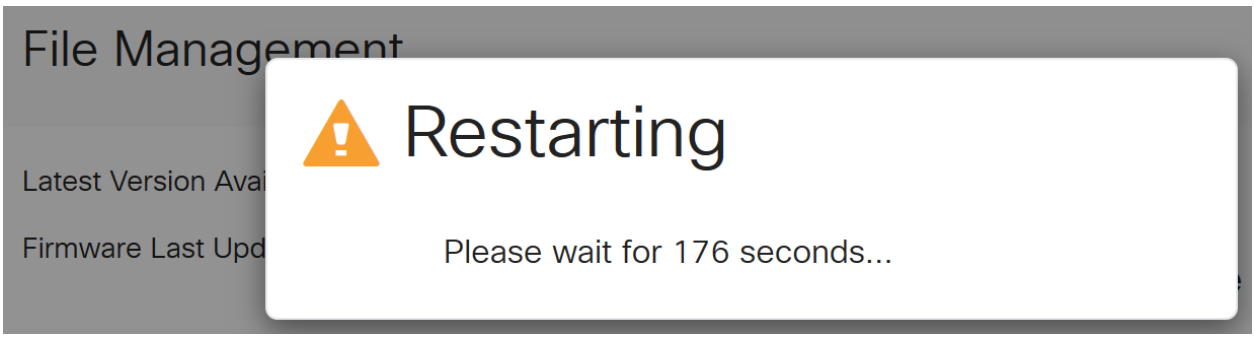
Haga clic en **Yes** en la ventana de confirmación para continuar.



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

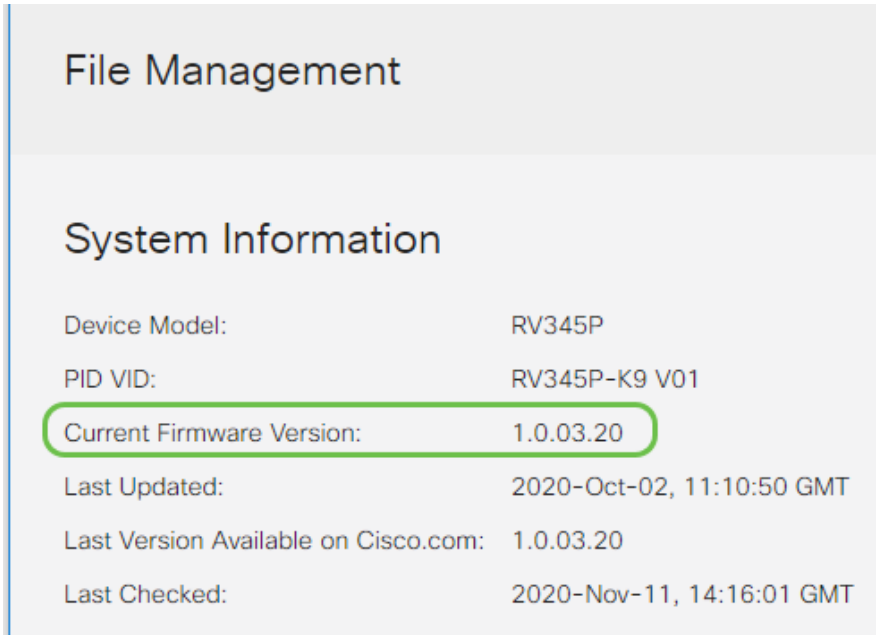


Una vez completada la actualización, aparecerá una ventana de notificación para informarle de que el router se *reiniciará* con una cuenta atrás del tiempo estimado para que el proceso termine. A continuación, se cerrará la sesión.



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.

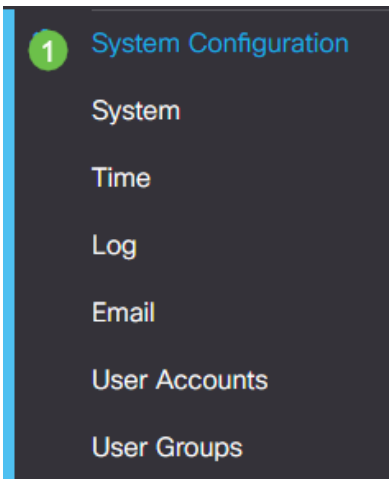


Configuración de actualizaciones automáticas en el router serie RV345P

Puesto que las actualizaciones son tan importantes y usted es una persona ocupada, tiene sentido configurar las actualizaciones automáticas desde aquí en adelante.

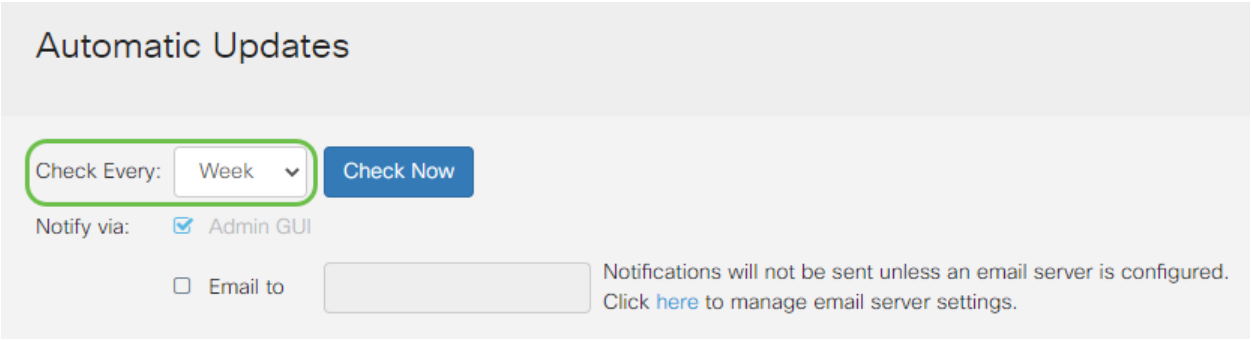
Paso 1

Inicie sesión en la utilidad basada en web y elija **Configuración del sistema > Actualizaciones automáticas**.



Paso 2

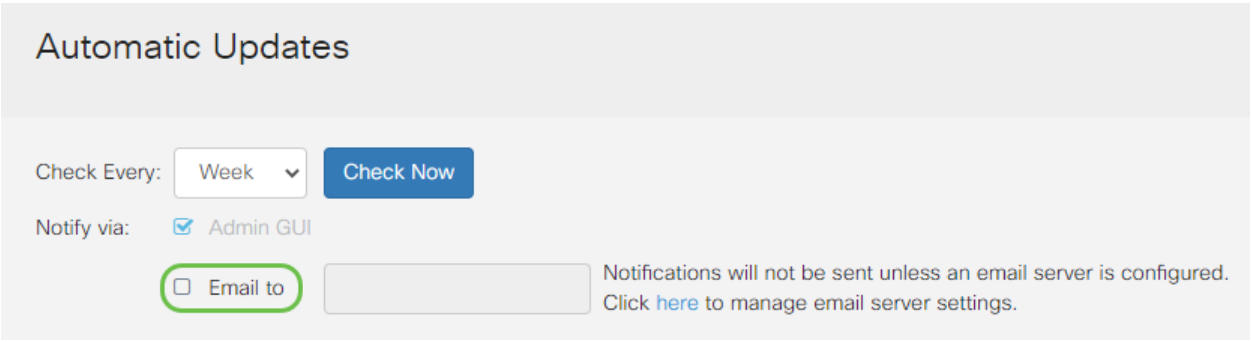
En la lista desplegable *Verificar cada*, elija la frecuencia con la que el router debe buscar actualizaciones.



Paso 3

En el área *Notify via* , marque la **casilla Email to** para recibir actualizaciones por correo electrónico. La casilla de verificación *Admin GUI* está habilitada de forma predeterminada y no se puede inhabilitar. Una vez disponible una actualización, aparecerá una notificación en la configuración basada en Web.

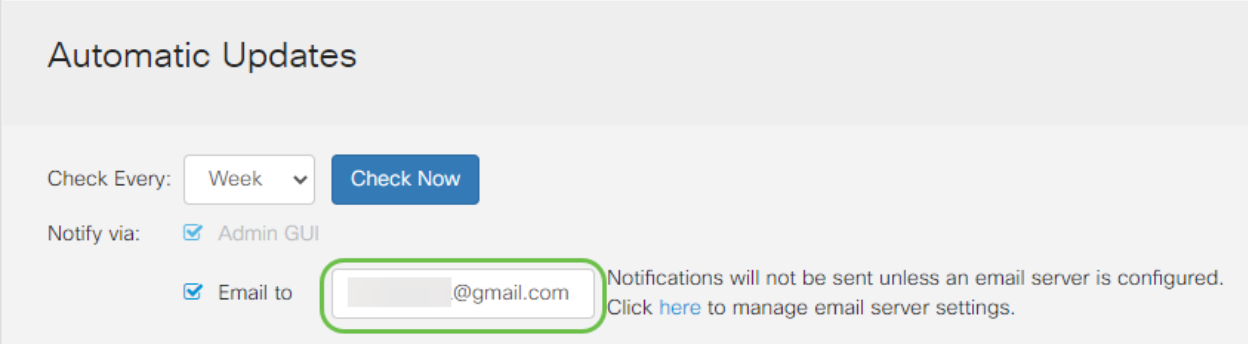
Si desea configurar la configuración del servidor de correo electrónico, haga clic aquí para saber cómo.



Paso 4

Introduzca una dirección de correo electrónico en el campo *Correo electrónico para* dirección.

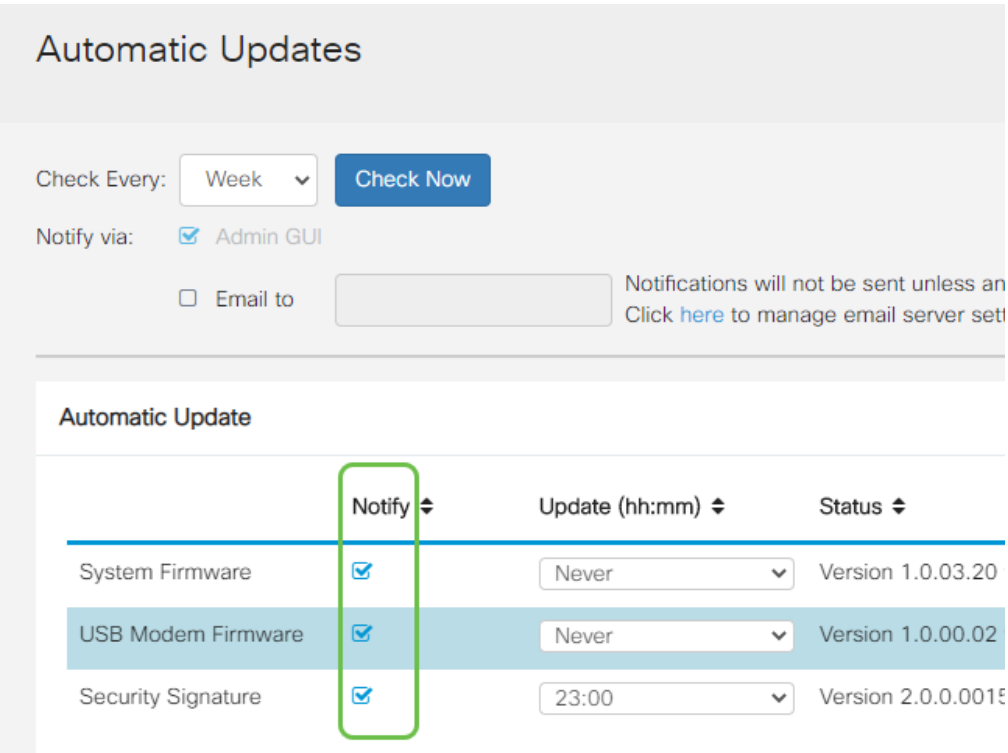
Se recomienda encarecidamente utilizar una cuenta de correo electrónico independiente en lugar de utilizar su correo electrónico personal para mantener la privacidad.



Paso 5

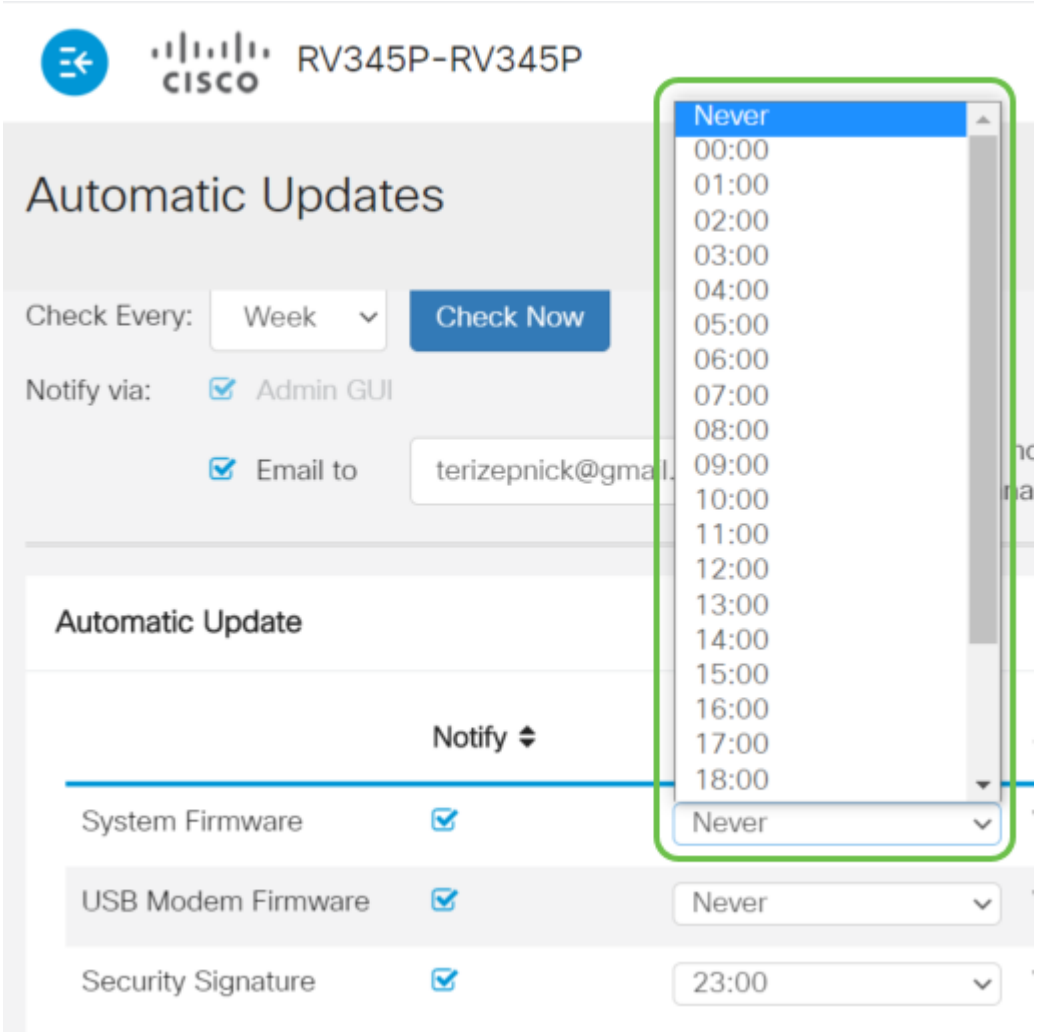
En el área *Actualización automática*, active las **casillas de verificación Notificar** del tipo de actualizaciones sobre las que desea que se le notifique. Las opciones son:

- Firmware del sistema: programa de control principal para el dispositivo.
- Firmware del módem USB: programa de control o controlador para el puerto USB.
- Firma de seguridad: contendrá firmas para el control de aplicaciones para identificar aplicaciones, tipos de dispositivos, sistemas operativos, etc.



Paso 6

En la lista desplegable *Actualización automática*, elija la hora del día que desea que se realice la actualización automática. Algunas opciones pueden variar según el tipo de actualización que haya seleccionado. Firma de seguridad es la única opción para tener una actualización inmediata. Se recomienda que establezca una hora en la que la oficina está cerrada para que el servicio no se interrumpa en un momento inconveniente.



El estado muestra la versión en ejecución actual del firmware o la firma de seguridad.

Paso 7

Haga clic en Apply (Aplicar).

Paso 8

Para guardar la configuración de forma permanente, vaya a la página Copiar/Guardar configuración o haga clic en el **icono Guardar** en la parte superior de la página.

Increíblemente, los parámetros básicos del router están completos. Ahora tiene algunas opciones de configuración que explorar.

Opciones de seguridad

Por supuesto, desea que su red esté a salvo. Hay algunas opciones sencillas, como tener una contraseña compleja, pero si desea tomar medidas para una red aún más

segura, consulte esta sección sobre seguridad.

Licencia de seguridad de RV (opcional)

Las funciones de esta licencia de seguridad de RV protegen su red de ataques desde Internet:

- Sistema de prevención de intrusiones (IPS): Inspecciona paquetes de red, registra y/o bloquea una amplia gama de ataques de red. Ofrece una mayor disponibilidad de la red, una remediación más rápida y una protección completa contra amenazas.
- Antivirus: Protección frente a virus mediante el análisis de las aplicaciones para varios protocolos, como HTTP, FTP, adjuntos de correo electrónico SMTP, adjuntos de correo electrónico POP3 y archivos adjuntos de correo electrónico IMAP que se transmiten a través del router.
- Seguridad web: Permite la eficacia y la seguridad empresariales mientras se conecta a Internet, permite que las políticas de acceso a Internet para los dispositivos finales y las aplicaciones de Internet ayuden a garantizar el rendimiento y la seguridad. Se basa en la nube y contiene más de 80 categorías con más de 450 millones de dominios clasificados.
- Identificación de la aplicación: Identifique y asigne políticas a las aplicaciones de Internet. Se identifican automáticamente 500 aplicaciones únicas.
- Identificación del cliente: Identifique y clasifique a los clientes de forma dinámica. Capacidad para asignar políticas basadas en la categoría de dispositivos finales y el sistema operativo.

La licencia de seguridad de RV proporciona filtrado web. El filtrado web es una función que permite administrar el acceso a sitios web inapropiados. Puede examinar las solicitudes de acceso a la Web de un cliente para determinar si se debe permitir o denegar dicho sitio.

Las funciones de seguridad con licencia se pueden probar sin coste alguno durante 90 días. Si desea continuar utilizando las funciones de seguridad avanzadas del router después del período de evaluación, debe adquirir y activar una licencia.

Otra opción de seguridad es Cisco Umbrella. Haga clic aquí si desea saltar a la sección de los paraguas.

Si no desea ninguna licencia de seguridad, haga clic para saltar a la sección VPN de este documento.

Introducción a las cuentas inteligentes

Para adquirir la licencia de seguridad de RV, necesita una cuenta inteligente.

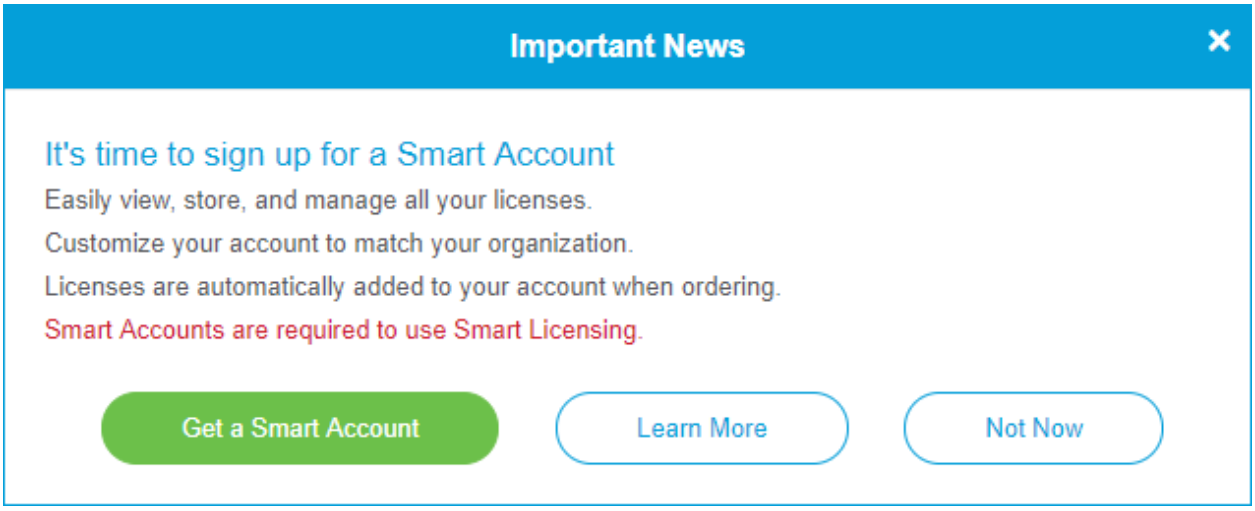
Al autorizar la activación de esta cuenta inteligente, acepta que está autorizado para crear cuentas y gestionar derechos de productos y servicios, acuerdos de licencia y

acceso de usuarios a cuentas en nombre de su organización. Los partners de Cisco no pueden autorizar la creación de cuentas en nombre de los clientes.

La creación de una nueva cuenta Smart Account es un evento único y la administración desde ese punto hacia adelante se proporciona a través de la herramienta.

Creación de una cuenta inteligente

Cuando acceda a su cuenta general de Cisco mediante su cuenta de Cisco.com o ID de CCO (la que creó al principio de este documento), puede recibir un mensaje para crear una cuenta inteligente.



Si no ha visto esta ventana emergente, puede hacer clic para ir a la página de creación de cuenta inteligente. Es posible que deba iniciar sesión con las credenciales de su cuenta de Cisco.com.

Para obtener más información sobre los pasos necesarios para solicitar su cuenta inteligente, haga clic aquí.

Asegúrese de anotar el nombre de su cuenta junto con otros detalles de registro.

Sugerencia rápida: Si se le solicita que introduzca un dominio y no tiene uno, puede introducir su dirección de correo electrónico en la forma de *name@domain.com*. Los dominios comunes son gmail, yahoo, etc. dependiendo de su empresa o proveedor.

Es muy importante que tenga una cuenta Cisco.com (ID de CCO) y una cuenta Cisco Smart Account antes de adquirir la licencia de seguridad de RV.

Licencia de seguridad de RV de compra

Debe comprar una licencia a su distribuidor de Cisco o a su partner de Cisco. Para localizar un partner de Cisco, haga clic aquí.

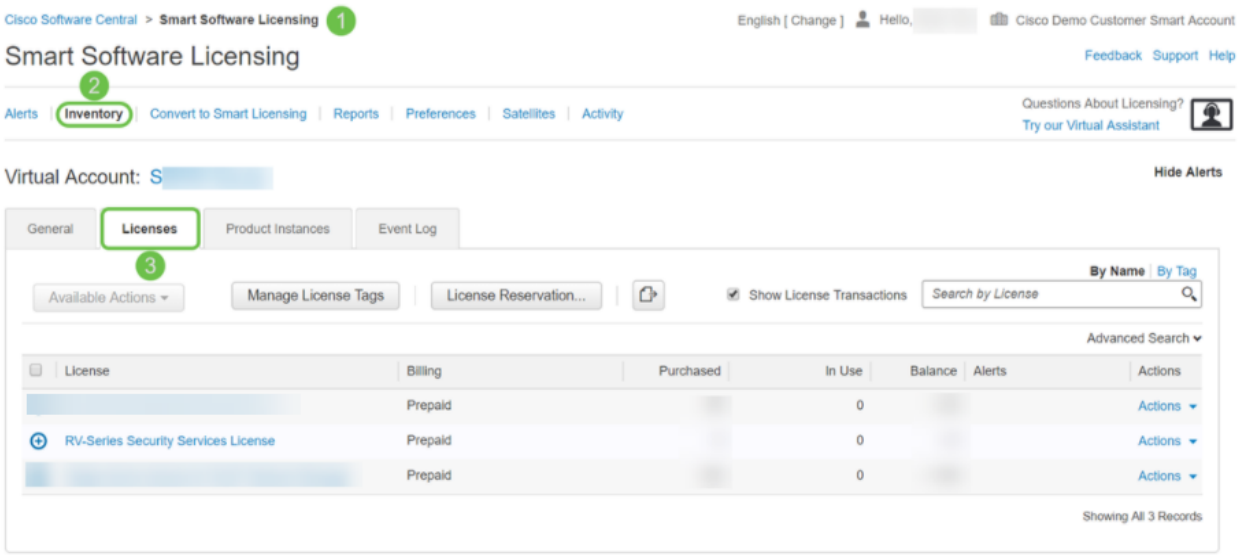
En la tabla siguiente se muestra el número de pieza de la licencia.

Tipo	ID del producto	Descripción
Licencia de seguridad de RV	LS-RV34X-SEC-1YR=	Seguridad de RV: 1 año: Filtrado web dinámico, visibilidad de aplicaciones, identificación y estadísticas de clientes, antivirus de gateway e IPS del sistema de prevención de intrusiones.

La clave de licencia no se introduce directamente en el router, pero se asignará a su cuenta Cisco Smart Account después de solicitar la licencia. La cantidad de tiempo que tarda la licencia en aparecer en su cuenta depende de cuándo el partner acepte el pedido y cuándo el revendedor vincule las licencias a su cuenta, que suele ser de 24 a 48 horas.

Confirmar licencia en Smart Account

Desplácese a la página de cuenta de Smart License y, a continuación, haga clic en **Smart Software License page > Inventory > Licenses**.

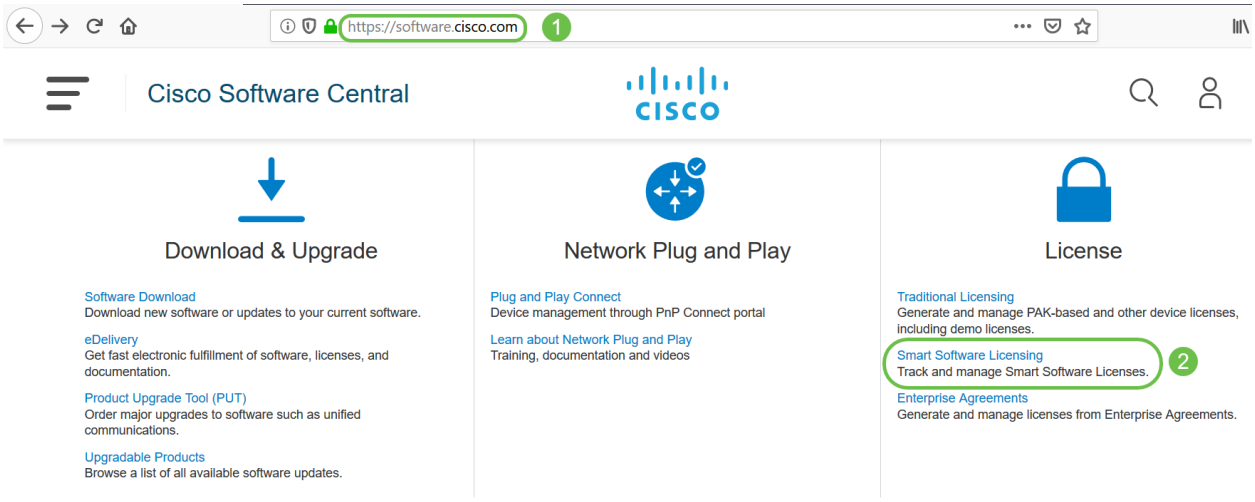


Si no ve su licencia en su cuenta inteligente, póngase en contacto con su partner de Cisco.

Configuración de la licencia de seguridad de RV en el router serie RV345P

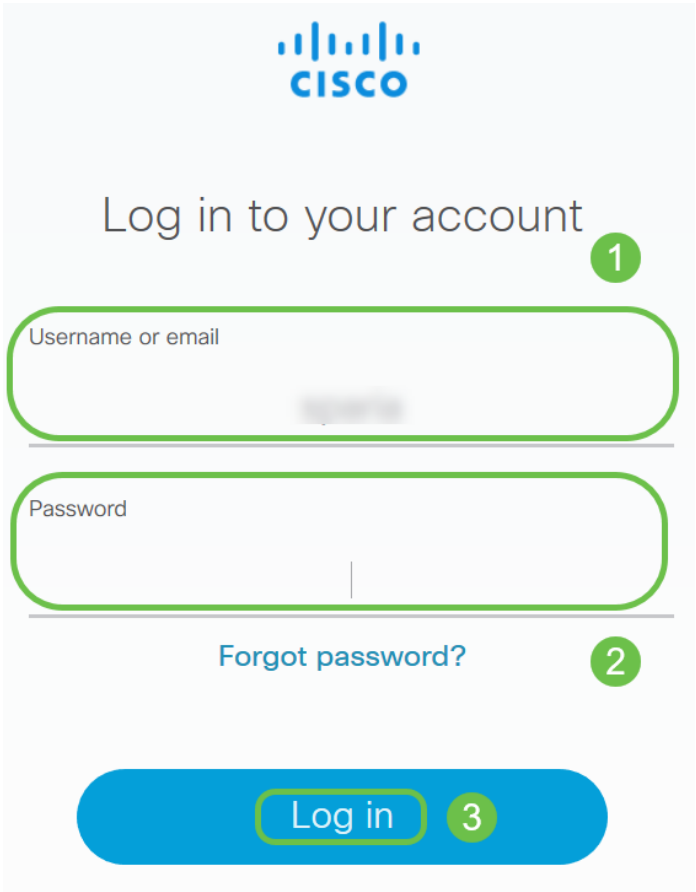
Paso 1

Acceda a Cisco Software y navegue hasta **Smart Software Licensing**.



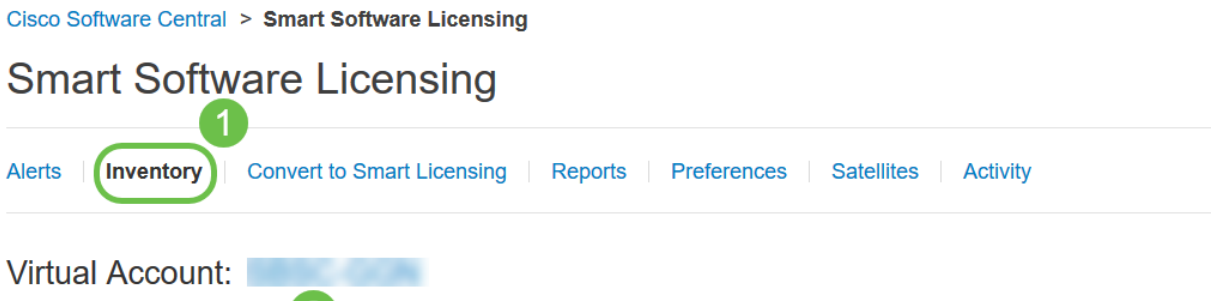
Paso 2

Introduzca su *nombre de usuario o correo electrónico* y *contraseña* para iniciar sesión en su cuenta inteligente. Haga clic en **Iniciar sesión**.



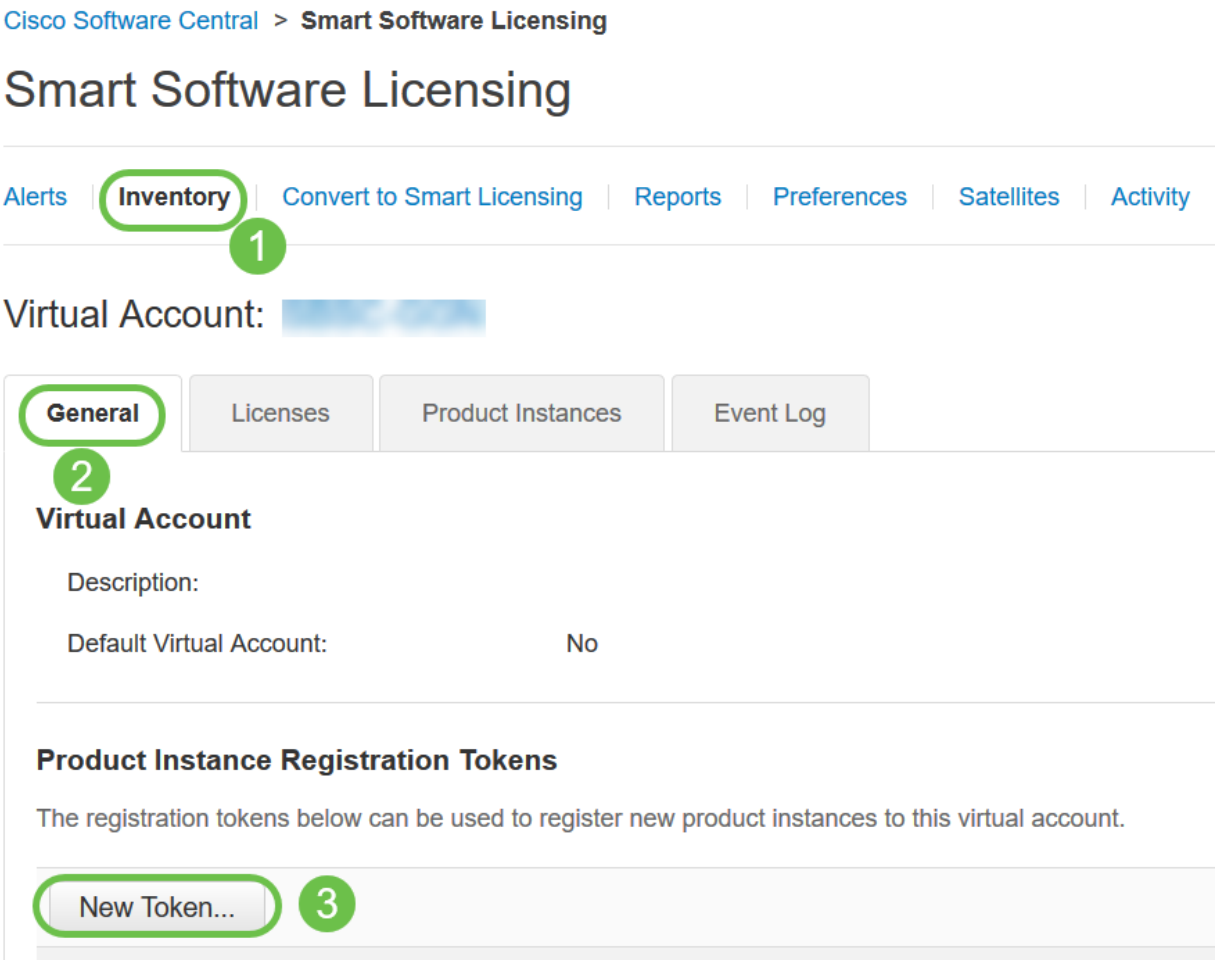
Paso 3

Navegue hasta **Inventario > Licencias** y verifique que la *Licencia de Servicios de Seguridad de la Serie RV* aparezca en su cuenta inteligente. Si no ve la licencia mostrada, póngase en contacto con su partner de Cisco.



Paso 4

Vaya a **Inventario > General**. En *Product Instance Registration Tokens*, haga clic en **New Token**.



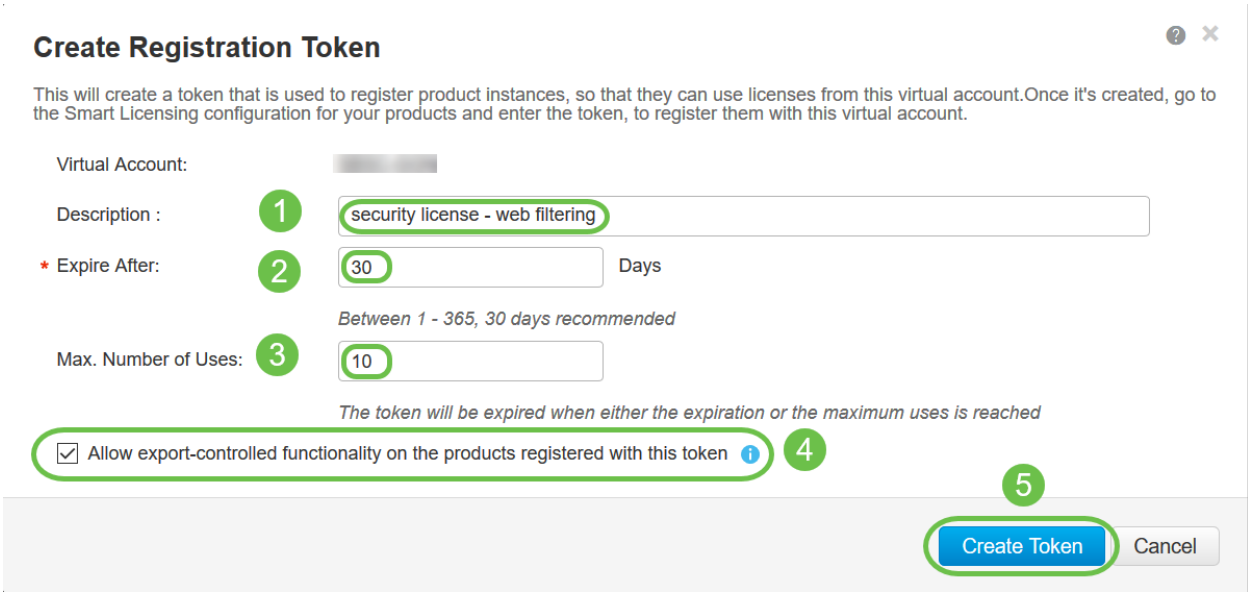
Paso 5

Aparecerá una ventana Create Registration Token (Crear token de registro). El área *Cuenta virtual* muestra la cuenta virtual bajo la cual se creará el token de registro. En la página *Crear token de registro*, complete lo siguiente:

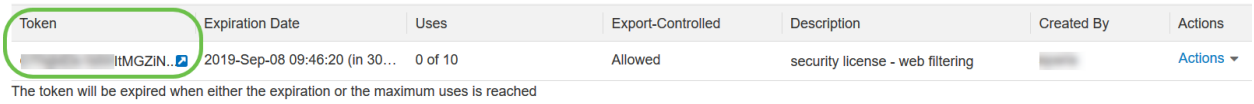
- En el campo Descripción, introduzca una descripción única para el token. En este ejemplo, se ingresa la licencia de seguridad - filtrado web.
- En el campo Expire After (Caducar después), introduzca un valor entre 1 y 365 días. Cisco recomienda el valor 30 días para este campo; sin embargo, puede editar el valor según sus necesidades.
- En el Max. El campo Número de usos especifica un valor para definir el número de veces que desea utilizar ese token. El token caducará cuando se alcance la cantidad de días o el número máximo de usos.
- Active la casilla de verificación Permitir la funcionalidad controlada por exportación en los productos registrados con este token para habilitar la funcionalidad controlada por exportación para los tokens de una instancia de producto en su cuenta virtual. Desactive la casilla de verificación si no desea permitir que la funcionalidad controlada por exportación esté disponible para su uso con este token. Utilice esta opción sólo si

cumple con la funcionalidad controlada por exportación. El Departamento de Comercio de los Estados Unidos restringe algunas funciones controladas por las exportaciones. Estas funciones están restringidas para los productos registrados con este token cuando desmarca la casilla de verificación. Toda violación está sujeta a sanciones y cargos administrativos.

- Haga clic en **Create Token** para generar el token.

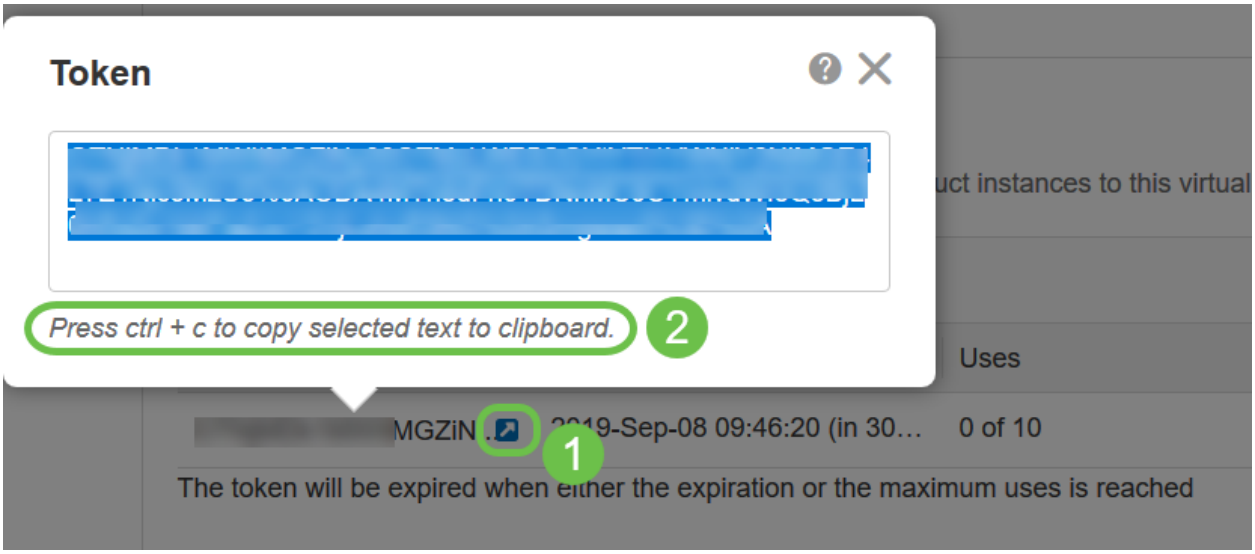


Ahora ha generado correctamente un token de registro de instancia de producto.



Paso 6

Haga clic en el **icono de flecha** en la *columna Token*, para copiar el token al portapapeles presione **Ctrl + c** en el teclado.

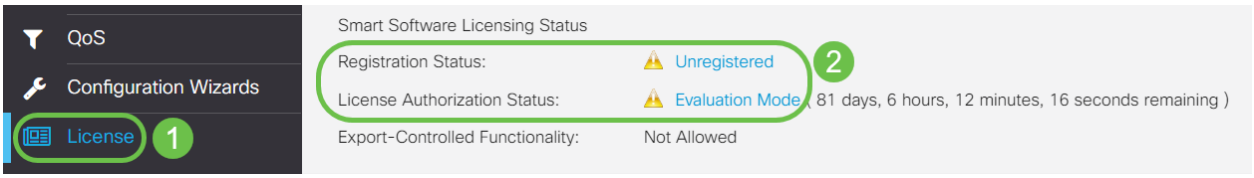


Paso 7 (opcional)

Haga clic en el menú desplegable **Acciones**, elija **Copiar** para copiar el token al portapapeles o **Descargar...** para descargar una copia del archivo de texto del token del que puede copiar.

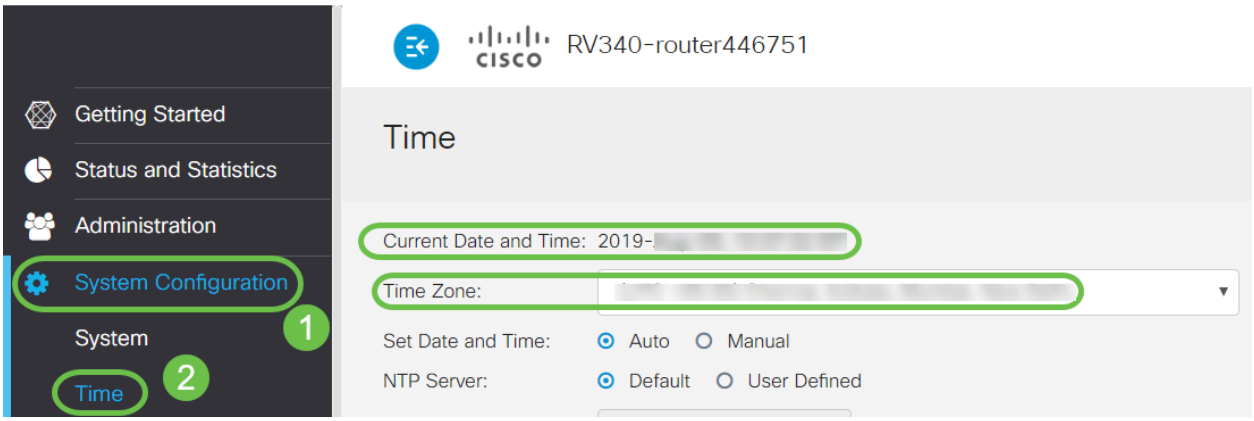
Paso 8

Navegue hasta Licencia y verifique que el *Estado de Registro* se muestre como *No Registrado* y *Estado de Autorización de Licencia* se muestra como *Modo de Evaluación*.



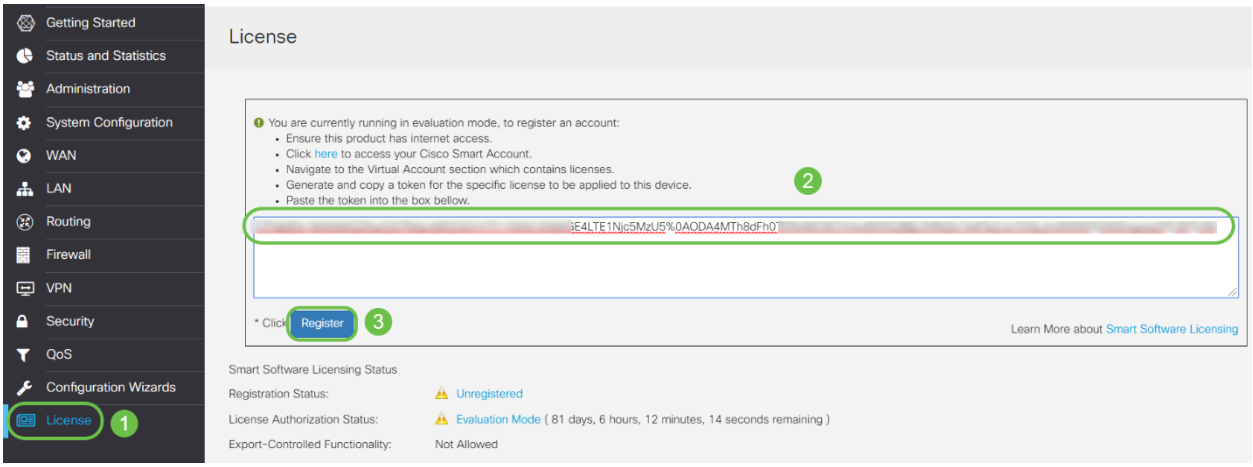
Paso 9

Navegue hasta **Configuración del sistema > Hora** y verifique que la *Fecha y hora actuales* y *Zona horaria* se reflejen correctamente según su zona horaria.



Paso 10

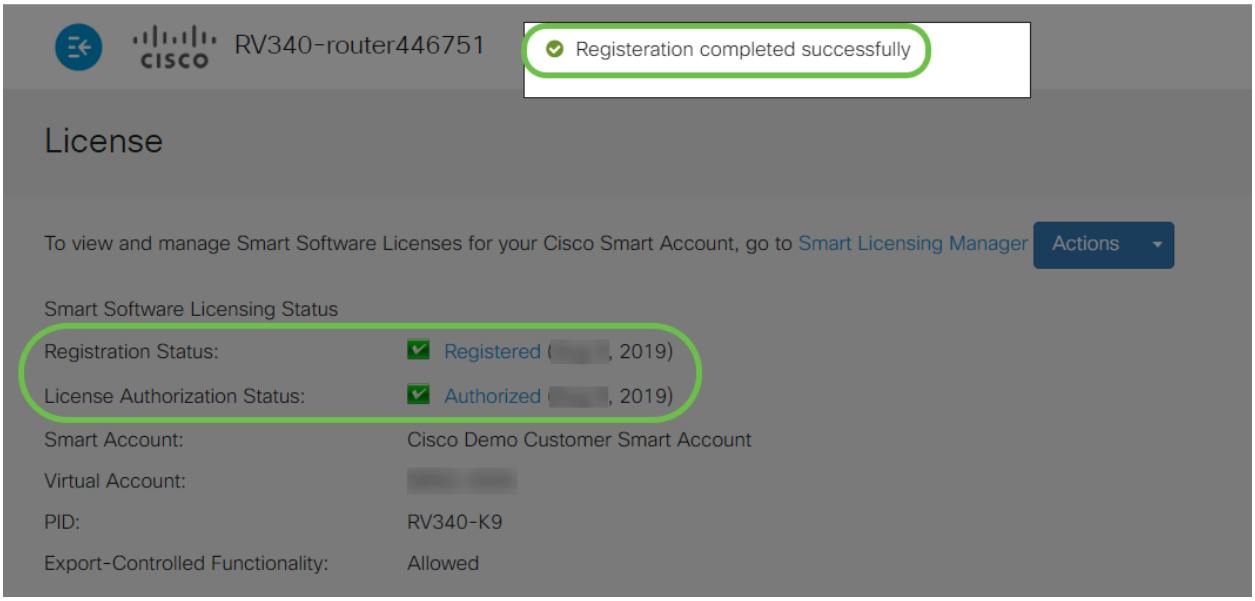
Vaya a **Licencia**. Pegue el token copiado en el paso 6 en el cuadro de texto bajo la ficha *Licencia* seleccionando **Ctrl + v** en el teclado. Haga clic en **Register**.



El registro puede tardar unos minutos. No deje la página mientras el router intenta ponerse en contacto con el servidor de licencias.

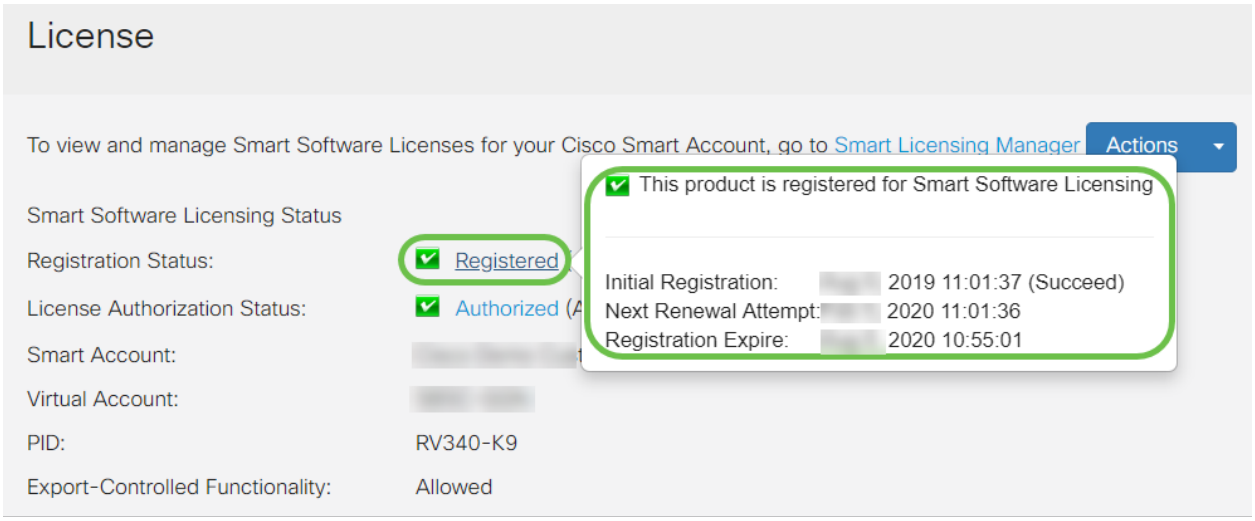
Paso 11

Ahora debería haber registrado y autorizado correctamente el router de la serie RV345P con una licencia inteligente. Recibirá una notificación en la pantalla *Registro completado correctamente*. Además, podrá ver que el *Estado de registro* se muestra como *Registrado* y *Estado de autorización de licencia* se muestra como *Autorizado*.



Paso 12 (opcional)

Para ver más detalles sobre el *Estado de registro* de la licencia, sitúe el puntero sobre el estado *Registrado*. Aparece un mensaje de diálogo con la siguiente información:

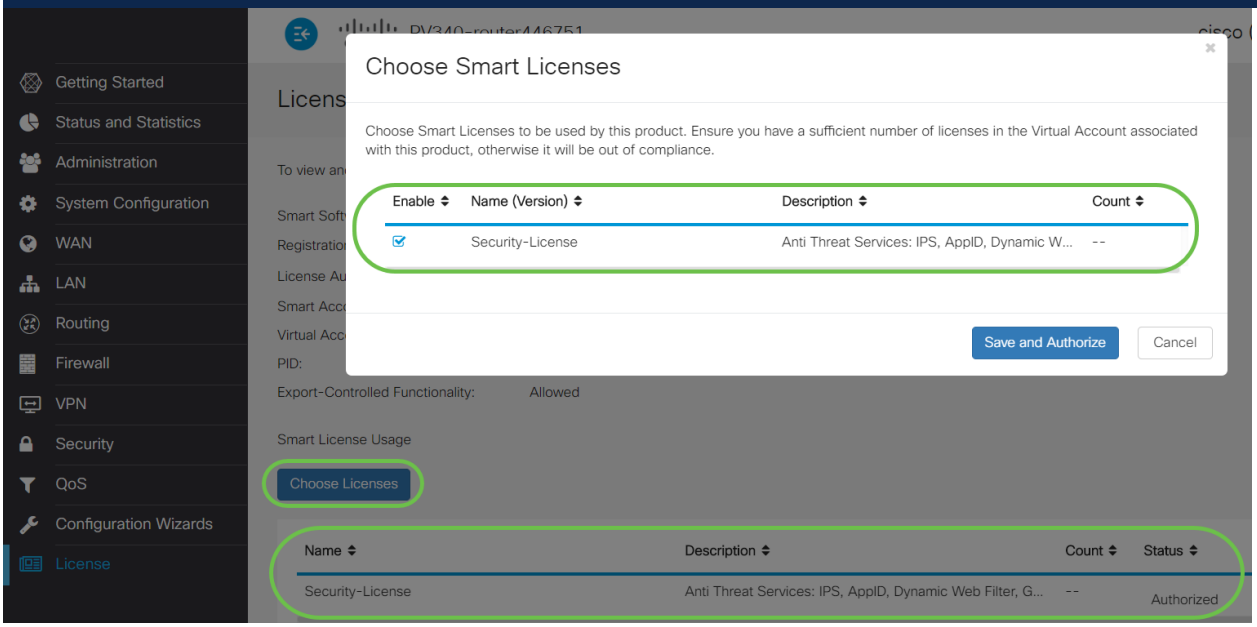


- Registro inicial: esta área indica la fecha y la hora en que se registró la licencia.
- Próximo intento de renovación: esta área indica la fecha y hora en que el router intentará renovar la licencia.
- Caducidad del registro: esta área indica la fecha y la hora a la que vence el registro.

Paso 13

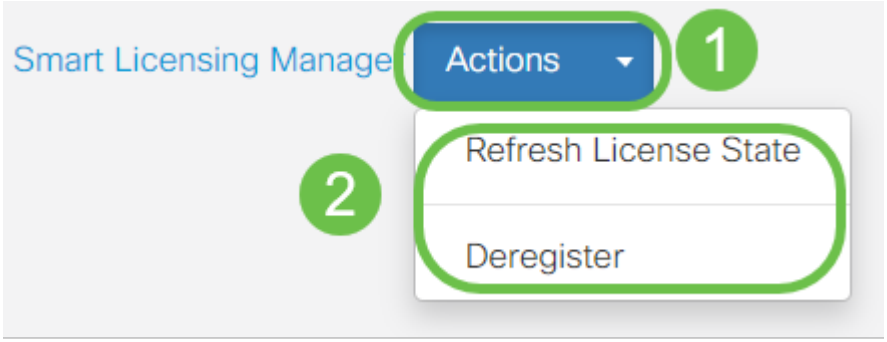
En la página *Licencia, verifique que el estado Licencia de seguridad* muestre *Autorizado*. También puede hacer clic en el botón **Choose License** para verificar que *Security-License* esté habilitado.

Si tiene algún problema en este paso, es posible que deba reiniciar el router.



Paso 14 (opcional)

Para *Actualizar estado de licencia* o *Anular registro* de la licencia desde el router, haga clic en el menú desplegable *Smart Licensing Manager* Acciones y seleccione un elemento de acción.



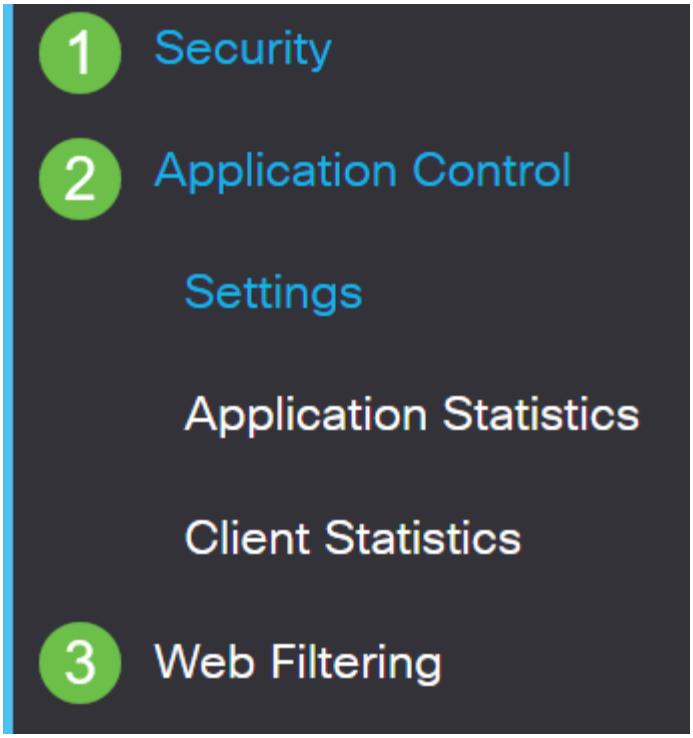
Ahora que tiene su licencia en el router, debe completar los pasos de la siguiente sección.

Filtrado de Web en el router RV345P

Dispone de 90 días después de la activación para utilizar el filtrado web sin coste alguno. Después de la prueba gratuita, si desea continuar utilizando esta función, debe comprar una licencia. Haga clic para volver a esa sección.

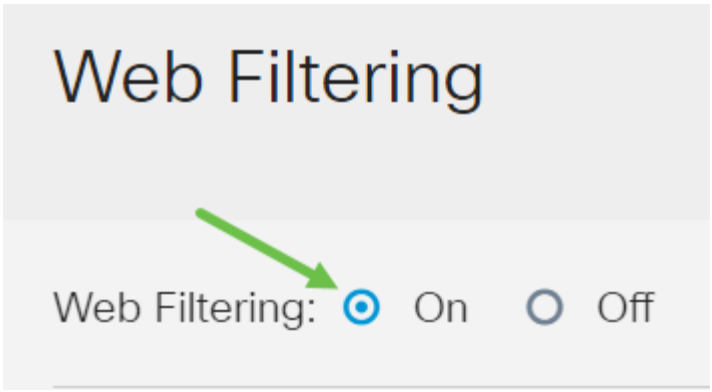
Paso 1

Inicie sesión en la utilidad basada en Web y elija **Security > Application Control > Web Filtering**.



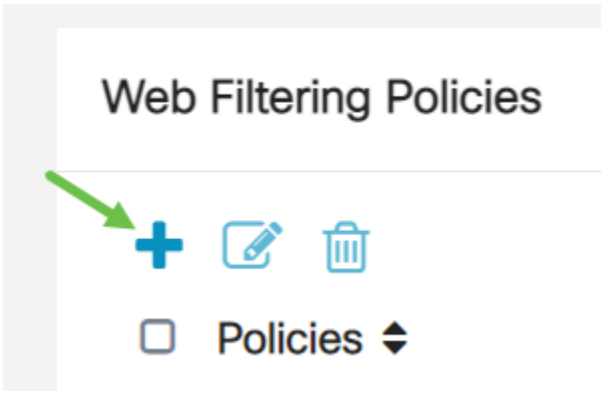
Paso 2

Seleccione el botón de opción **On**.



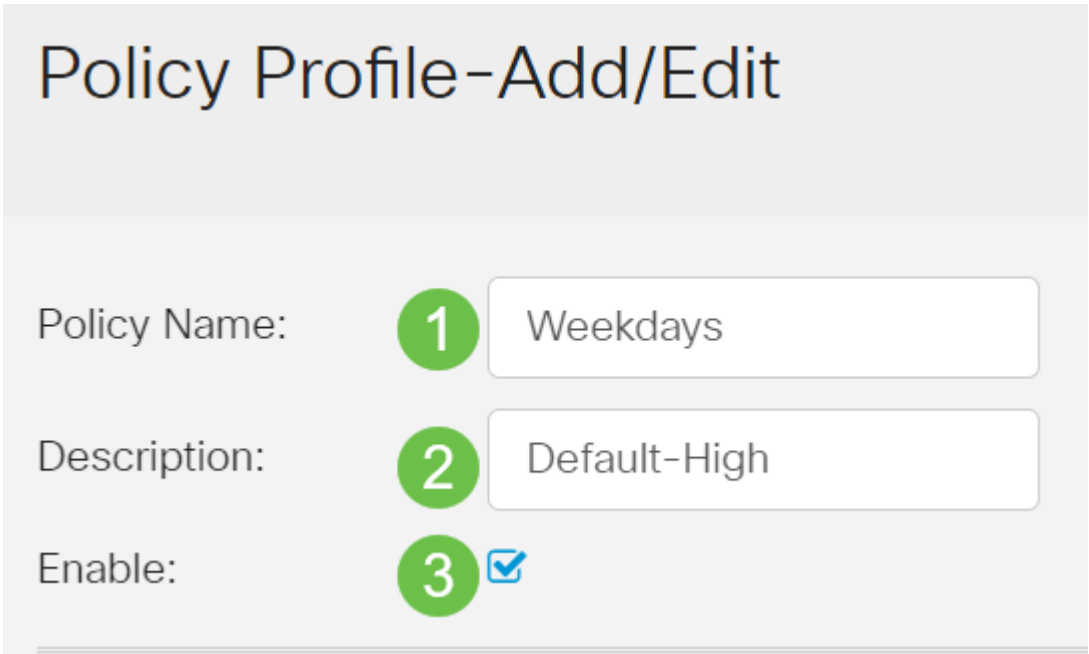
Paso 3

Haga clic en el **icono Add**.



Paso 4

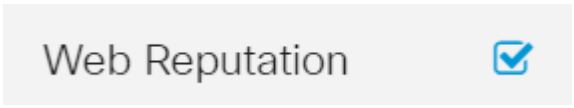
Ingrese un *Nombre de Política*, una *Descripción* y la *casilla de verificación Habilitar*.



Si el filtrado de contenido está activado en el router, aparecerá una notificación para informarle de que el filtrado de contenido se ha desactivado y de que las dos funciones no se pueden habilitar simultáneamente. Haga clic en **Aplicar** para continuar con la configuración.

Paso 5

Marque la casilla de verificación Web Reputation para activar el filtrado basado en un índice de reputación web.

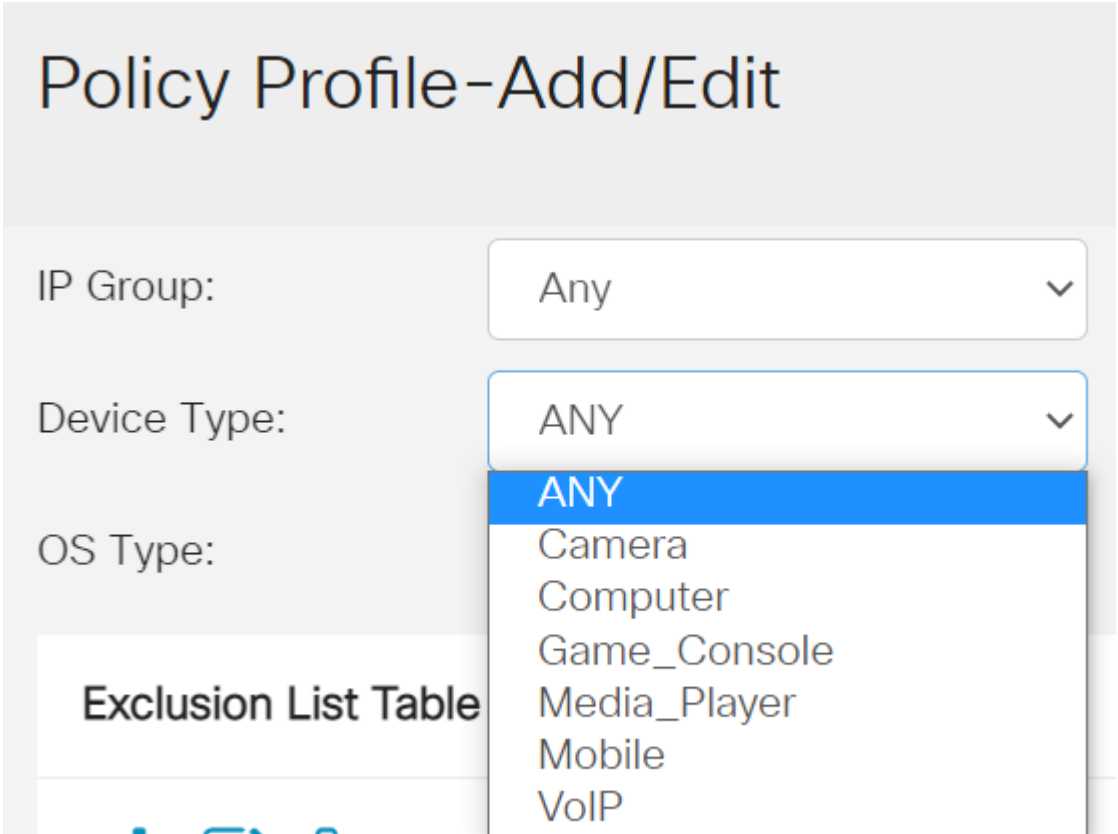


El contenido se filtrará según la notoriedad de un sitio web o URL según un índice de reputación web. Si la puntuación es inferior a 40, el sitio web será bloqueado. Para obtener más información sobre la tecnología de reputación web, haga clic aquí para obtener más detalles.

Paso 6

En la lista desplegable *Tipo de dispositivo*, seleccione el origen/destino de los paquetes que se filtrarán. Sólo se puede seleccionar una opción a la vez. Las opciones son:

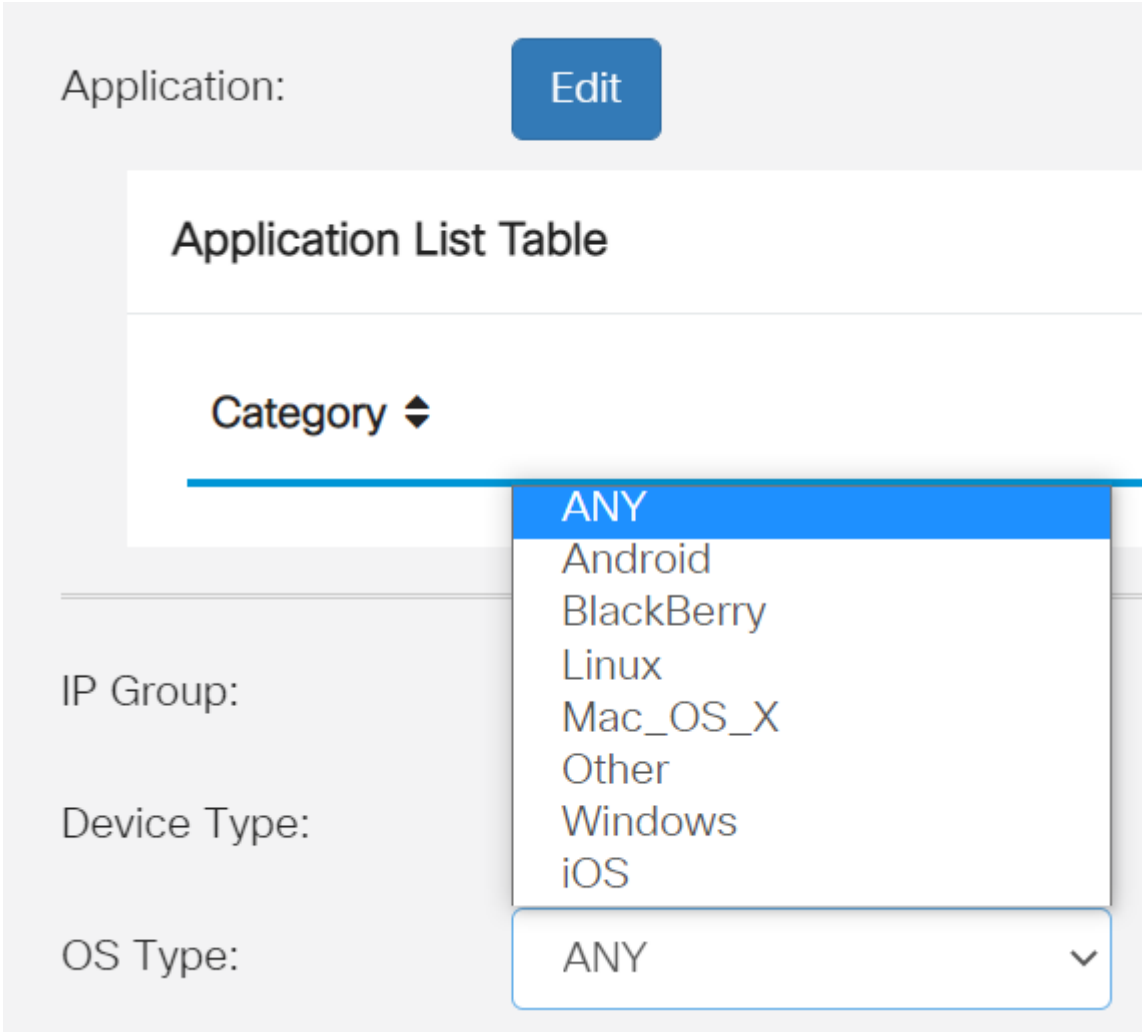
- ANY: elija esta opción para aplicar la política a cualquier dispositivo.
- Cámara: seleccione esta opción para aplicar la política a las cámaras (como las cámaras de seguridad IP).
- Equipo: seleccione esta opción para aplicar la directiva a los equipos.
- Game_Console: elija esta opción para aplicar la política a las consolas de juegos.
- Media_Player: seleccione esta opción para aplicar la política a los reproductores multimedia.
- Móvil: seleccione esta opción para aplicar la política a los dispositivos móviles.
- VoIP: seleccione esta opción para aplicar la política a los dispositivos del protocolo de voz sobre Internet .



Paso 7

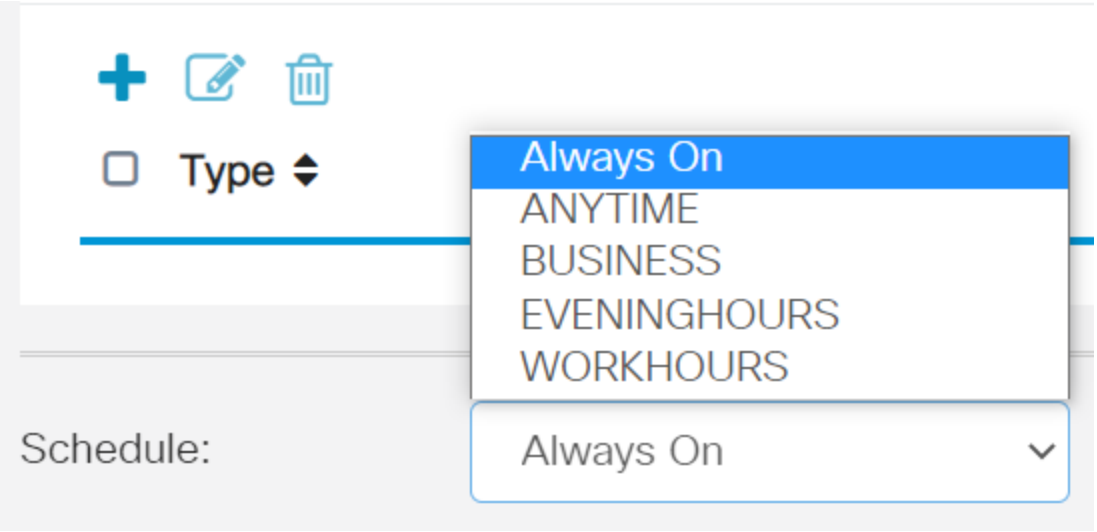
En la lista desplegable *Tipo de sistema operativo*, elija un sistema operativo (SO) al que deba aplicarse la política. Sólo se puede seleccionar una opción a la vez. Las opciones son:

- ANY: aplica la política a cualquier tipo de sistema operativo. Este es el valor predeterminado.
- Android: aplica la política únicamente al sistema operativo Android.
- BlackBerry: aplica la política únicamente al sistema operativo Blackberry.
- Linux: aplica la política sólo al sistema operativo Linux.
- Mac_OS_X: aplica la política sólo al sistema operativo Mac.
- Otro: aplica la política a un SO que no aparece en la lista.
- Windows: aplica la directiva al sistema operativo Windows.
- iOS: aplica la política sólo al sistema operativo iOS.



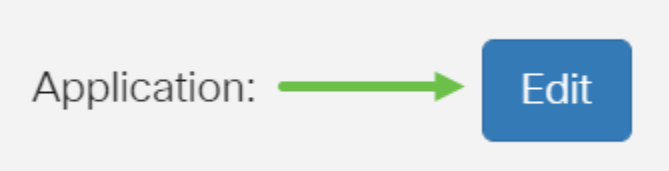
Paso 8

Desplácese hasta la sección *Programación* y seleccione la opción que mejor se adapte a sus necesidades.



Paso 9

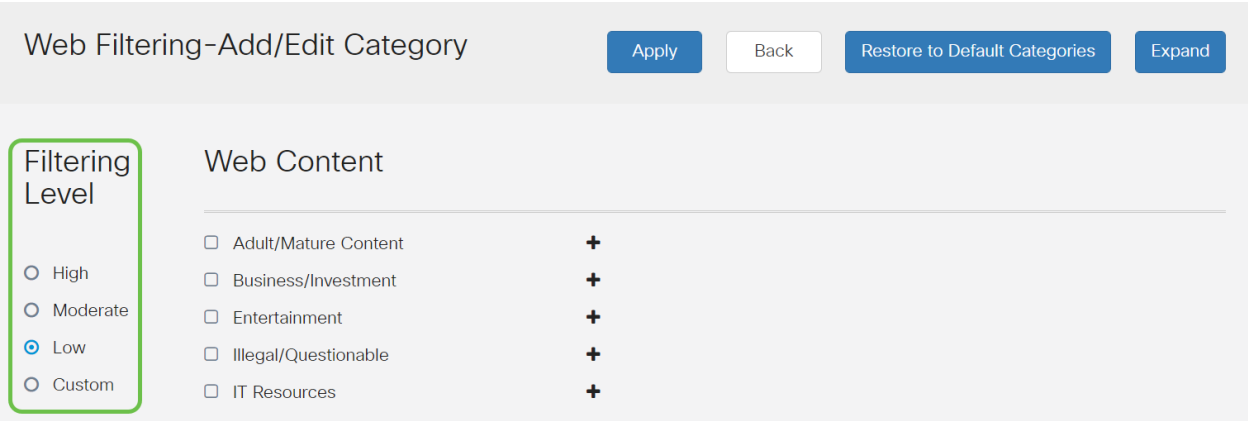
Haga clic en el **icono de edición**.



Paso 10

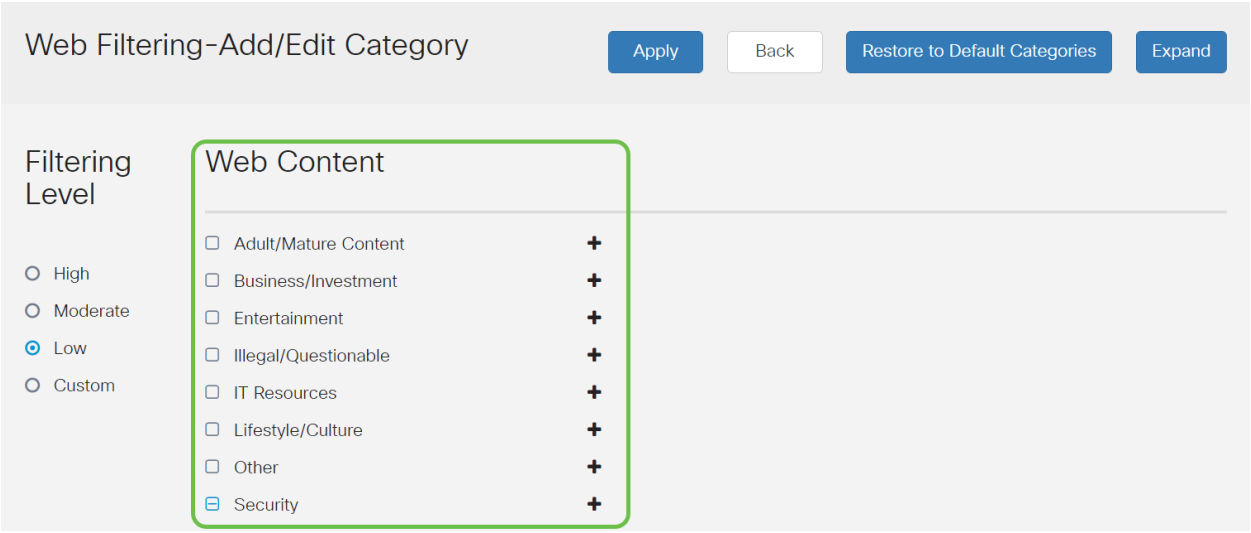
En la columna Nivel de filtrado, haga clic en un botón de opción para definir rápidamente el grado de filtrado que mejor se ajuste a las políticas de red. Las opciones son High (Alta), Moderate (Moderada), Low (Baja) y Custom (Personalizada). Haga clic en cualquiera de los niveles de filtrado siguientes para conocer las subcategorías predefinidas específicas filtradas a cada una de sus categorías de contenido web habilitadas. Los filtros predefinidos no se pueden modificar más y están atenuados.

- Baja: esta es la opción predeterminada. La seguridad está activada con esta opción.
- Moderado: contenido adulto/maduro, ilegal/cuestionable y seguridad se habilitan con esta opción.
- Alta: contenido adulto/maduro, empresa/inversión, ilegal/cuestionable, recursos de TI y seguridad están habilitados con esta opción.
- Personalizado: no hay valores predeterminados establecidos para permitir los filtros definidos por el usuario.



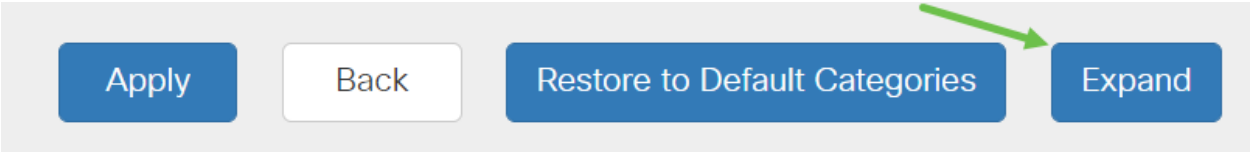
Paso 11

Introduzca el contenido web que desea filtrar. Haga clic en el **icono más** si desea obtener más detalles en una sección.



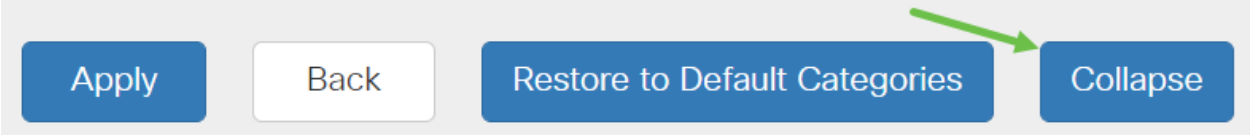
Paso 12 (opcional)

Para ver todas las subcategorías y descripciones de contenido web, puede hacer clic en el botón **Expandir**.



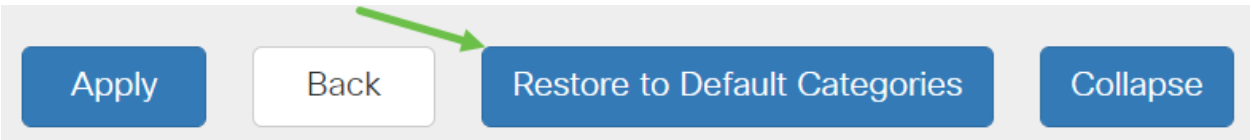
Paso 13 (opcional)

Haga clic en **Contraer** para contraer las subcategorías y descripciones.



Paso 14 (opcional)

Para volver a las categorías predeterminadas, haga clic en **Restaurar a categorías predeterminadas**.



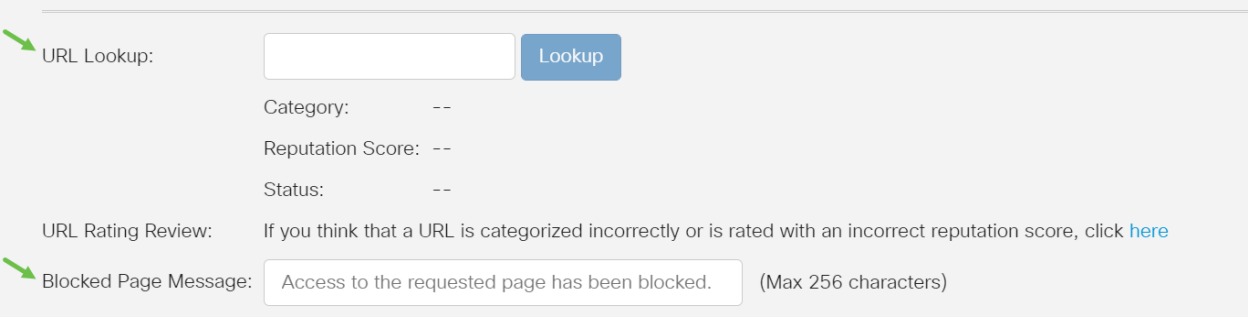
Paso 15

Haga clic en **Aplicar** para guardar la configuración y volver a la página Filtro para continuar con la configuración.

En la tabla de lista de aplicaciones, las subcategorías correspondientes basadas en el nivel de filtrado elegido completarán la tabla.

Paso 16 (opcional)

Otras opciones incluyen la búsqueda de URL y el mensaje que muestra cuándo se ha bloqueado una página solicitada.



Paso 17 (opcional)

Haga clic en Apply (Aplicar).

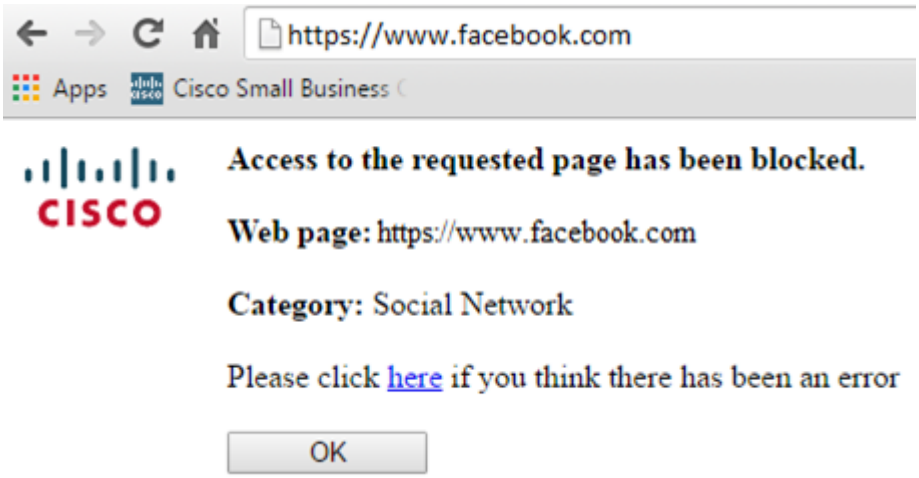
Paso 18

Para guardar la configuración de forma permanente, vaya a la página *Copiar/Guardar configuración* o haga clic en el **icono Guardar** en la parte superior de la página.

Paso 19 (opcional)

Para comprobar que un sitio web o URL se ha filtrado o bloqueado, inicie un navegador web o abra una nueva pestaña en el navegador. Introduzca el nombre de dominio que ha bloqueado o que ha filtrado para ser bloqueado o denegado.

En este ejemplo, usamos www.facebook.com.



Ahora debería haber configurado correctamente el filtrado web en el router RV345P. Puesto que utiliza la licencia de seguridad de RV para el filtrado web, probablemente no necesite Umbrella. Si también desea utilizar Umbrella, haga clic aquí. Si tiene suficiente seguridad, haga clic para saltar a la siguiente sección.

Resolución de problemas

Si ha adquirido una licencia pero no aparece en su cuenta virtual, dispone de dos opciones:

1. Realice un seguimiento con el revendedor para solicitar que realice la transferencia.
2. Póngase en contacto con nosotros y nos pondremos en contacto con el revendedor.

Lo ideal sería que no tuviera que hacer ninguna de las dos cosas, pero si llega a esta encrucijada, ¡estamos encantados de ayudarle! Para que el proceso sea lo más oportuno posible, necesitará las credenciales que figuran en la tabla anterior, así como las que se describen a continuación.

Información requerida	Localización de la información
Factura de licencia	Se le debe enviar por correo electrónico después de completar la compra de las licencias.
Número de pedido de venta de Cisco	Es posible que tenga que volver al revendedor para obtener esto.
Captura de pantalla de la página de licencia de Smart Account	Al realizar una captura de pantalla, se captura el contenido de la pantalla para compartirlo con nuestro equipo. Si no está familiarizado con las capturas de pantalla, puede utilizar los siguientes métodos.

Capturas de pantalla

Una vez que tenga un token o esté solucionando problemas, se recomienda que tome una captura de pantalla para capturar el contenido de la pantalla.

Dadas las diferencias en el procedimiento necesario para capturar una captura de pantalla, consulte a continuación los enlaces específicos de su sistema operativo.

- Windows:
- MAC
- iPhone/iPad
- Android

Licencia de sucursal RV de Umbrella (opcional)

Umbrella es una plataforma de seguridad en la nube sencilla pero muy eficaz de Cisco.

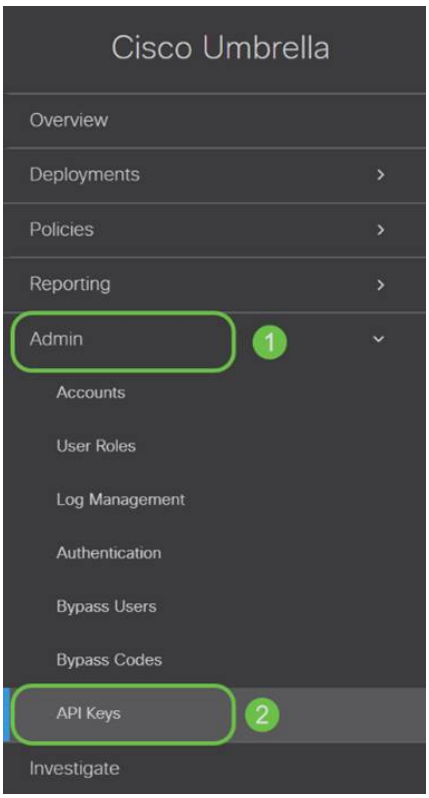
Umbrella funciona en la nube y realiza muchos servicios relacionados con la seguridad. De una amenaza emergente a una investigación posterior al evento. Umbrella detecta y previene ataques en todos los puertos y protocolos.

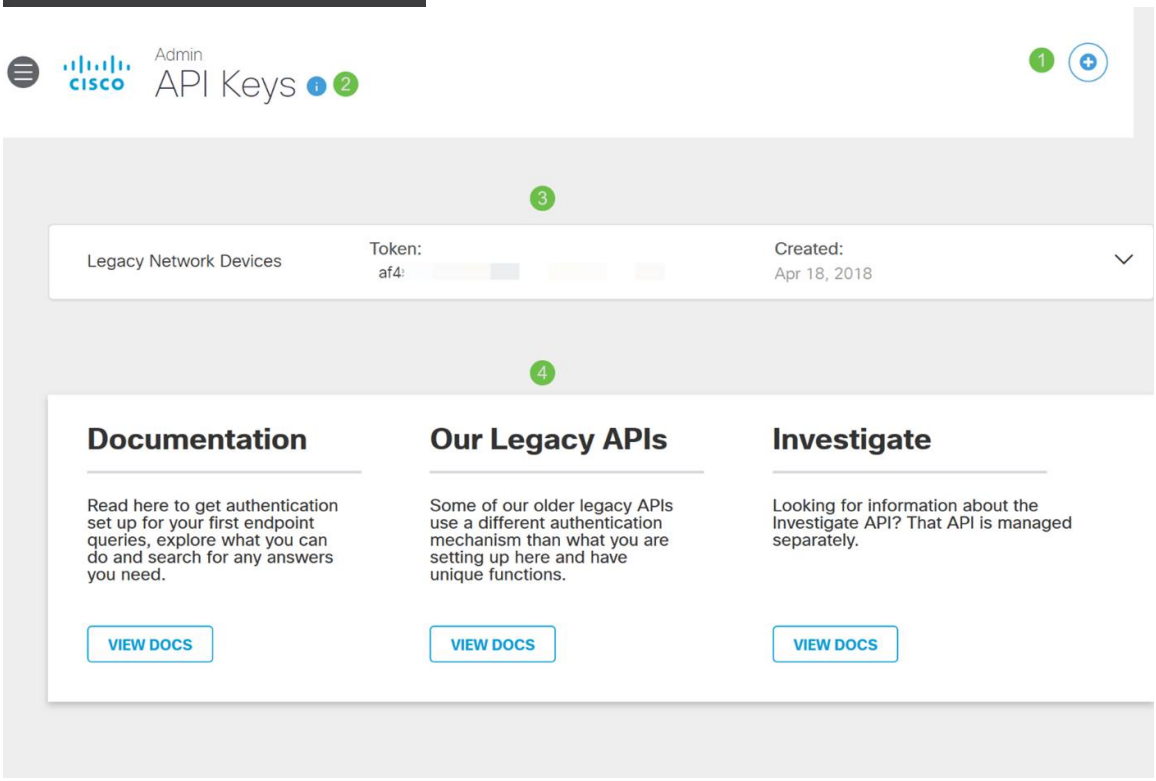
Umbrella utiliza DNS como su principal vector de defensa. Cuando los usuarios ingresan una URL en su barra de explorador y hacen clic en *Enter*, Umbrella participa en la transferencia. Esa URL pasa a la resolución DNS de Umbrella y, si se asocia una advertencia de seguridad al dominio, la solicitud se bloquea. Estos datos de telemetría se transfieren y se analizan en microsegundos, con lo que se agrega prácticamente ninguna latencia. Los datos de telemetría utilizan registros e instrumentos para el seguimiento de miles de millones de solicitudes DNS en todo el mundo. Cuando estos datos están omnipresentes, su correlación en todo el mundo permite una respuesta rápida a los ataques a medida que comienzan. Consulte la política de privacidad de Cisco aquí para obtener más información: política completa, versión resumida. Piense en los datos de telemetría como datos derivados de herramientas y registros.

Visite Cisco Umbrella para obtener más información y crear una cuenta. Si tiene algún problema, consulte aquí la documentación y aquí las opciones de Soporte de Umbrella .

Paso 1

Después de iniciar sesión en su cuenta principal, desde la pantalla *Panel* haga clic en **Admin > API Keys**.



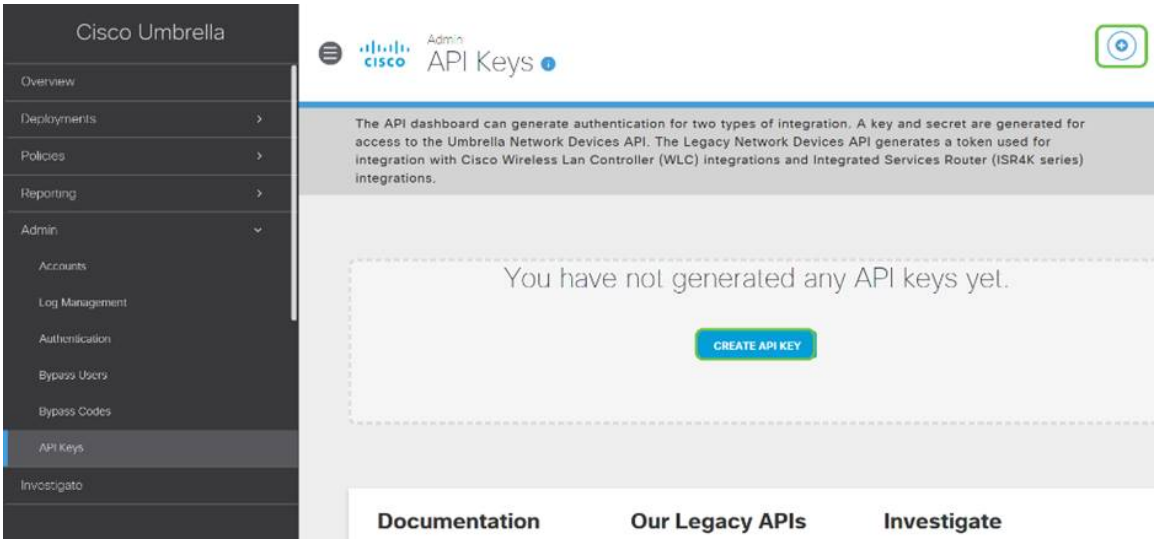


Anatomía de la pantalla API Keys (con la clave API existente)

1. Agregar clave de API: inicia la creación de una nueva clave para su uso con la API Umbrella.
2. Información adicional: se desliza hacia abajo/hacia arriba con un explicador para esta pantalla.
3. Token Well: contiene todas las claves y fichas creadas por esta cuenta. (Rellena una vez que se ha creado una clave)
4. Documentos de soporte: vínculos a la documentación del sitio principal relativa a los temas de cada sección.

Paso 2

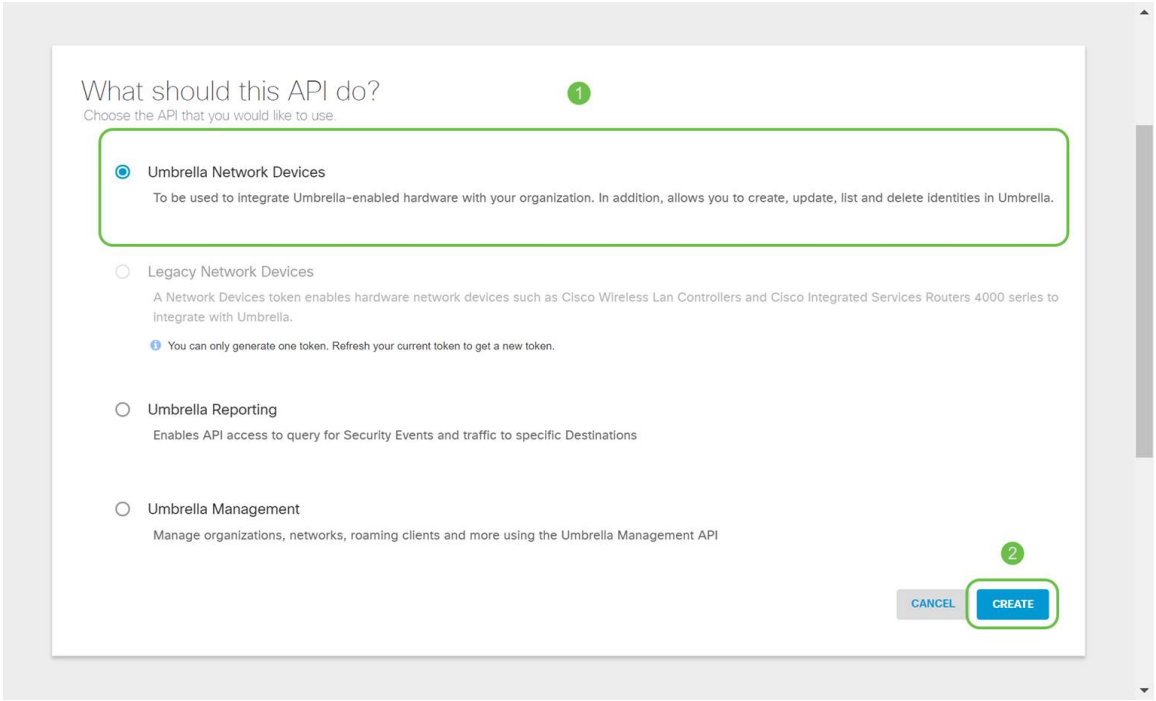
Haga clic en el botón **Add API Key** en la esquina superior derecha o haga clic en el botón **Create API Key**. Ambos funcionan igual.



La captura de pantalla anterior sería similar a lo que vería abrir este menú por primera vez.

Paso 3

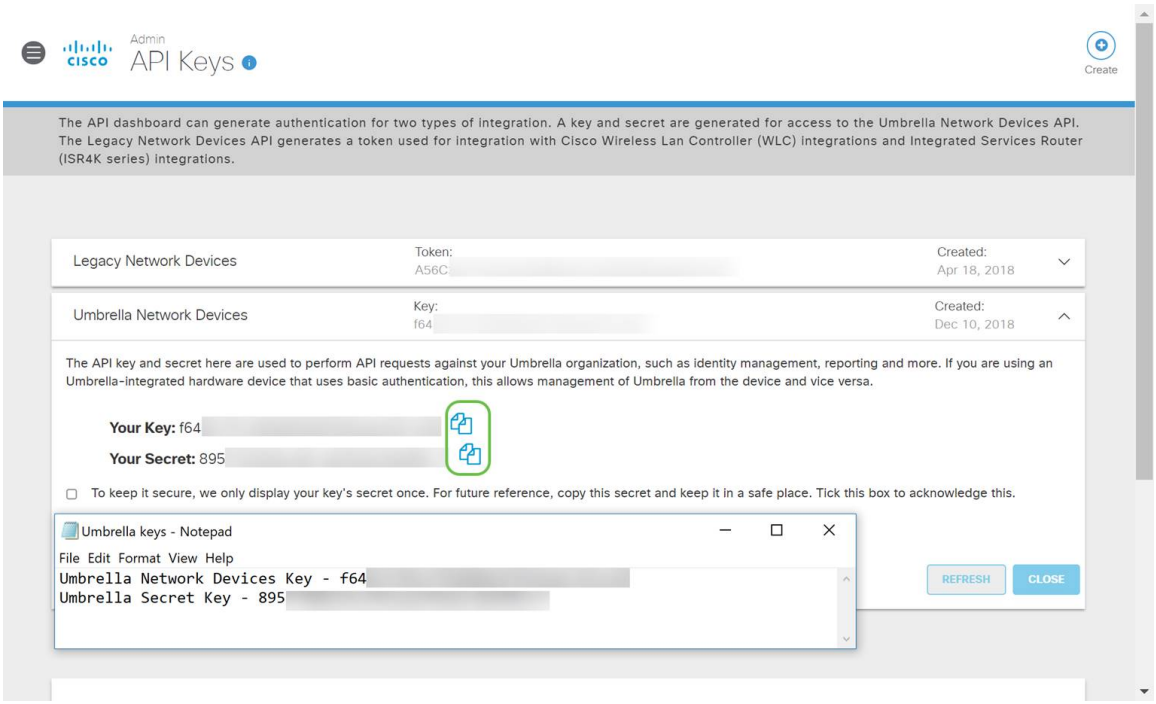
Seleccione **Umbrella Network Devices** y luego haga clic en el **botón Create**.



Paso 4

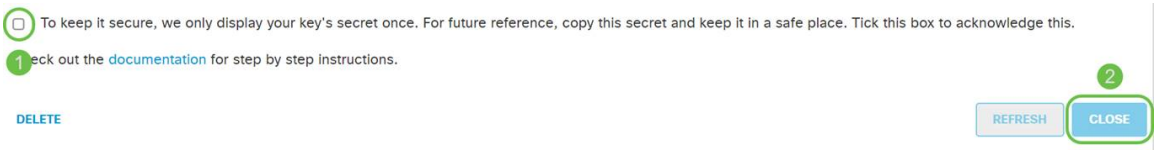
Abra un editor de texto como el bloc de notas y haga clic en el **icono de copia** a la derecha de su API y *clave secreta de* API*;* una notificación emergente confirmará que la clave se ha copiado en el portapapeles. De uno en uno, pegue el secreto y la clave API en el documento, etiquetándolos como referencia futura. En este caso, su etiqueta

es "Clave de dispositivos de red de Umbrella". A continuación, guarde el archivo de texto en una ubicación segura a la que sea fácil acceder más adelante.



Paso 5

Después de copiar la clave y la clave secreta en una ubicación segura, desde la *pantalla Umbrella API* haga clic en la **casilla de verificación** para confirmar que se ha completado el reconocimiento de la visualización temporal de la clave secreta y, a continuación, haga clic en el botón **Cerrar**.



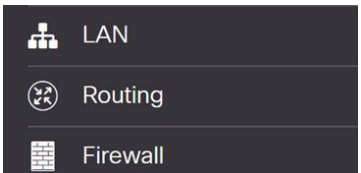
Si pierde o elimina accidentalmente la clave secreta, no hay ninguna función o número de soporte al que llamar para recuperar esta clave. Si se pierde, deberá eliminar la clave y volver a autorizar la nueva clave de API con cada dispositivo que desee proteger con Umbrella.

Configuración de Umbrella en su RV345P

Ahora que hemos creado claves API en Umbrella, puede tomar esas claves e instalarlas en su RV345P.

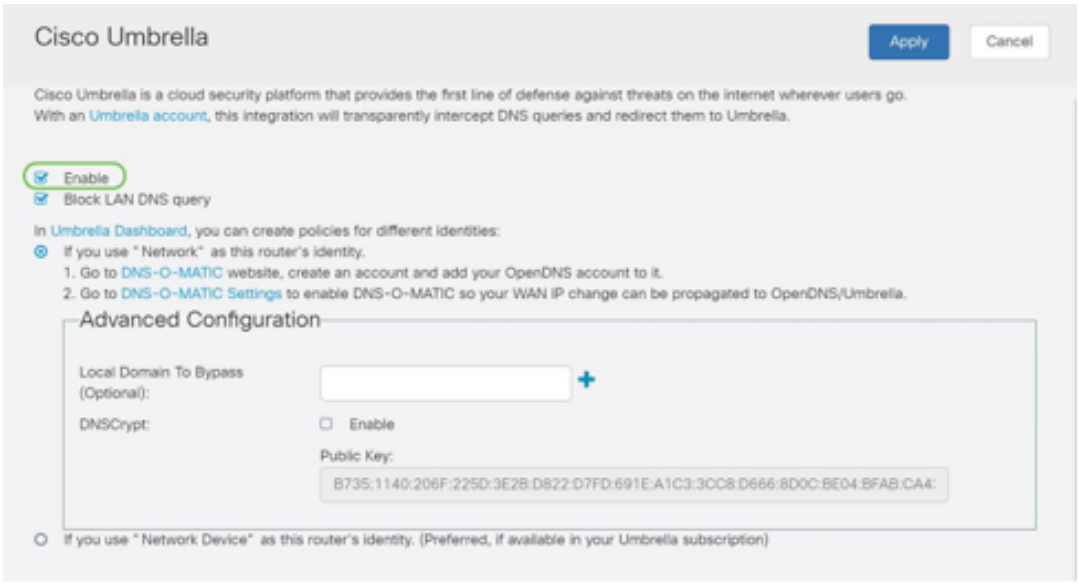
Paso 1

Después de iniciar sesión en el router RV345P, haga clic en **Security > Umbrella** en el menú de la barra lateral.



Paso 2

La pantalla Umbrella API (API del paraguas) tiene una amplia gama de opciones y comienza a activar Umbrella haciendo clic en la casilla de verificación **Enable (Activar)**.

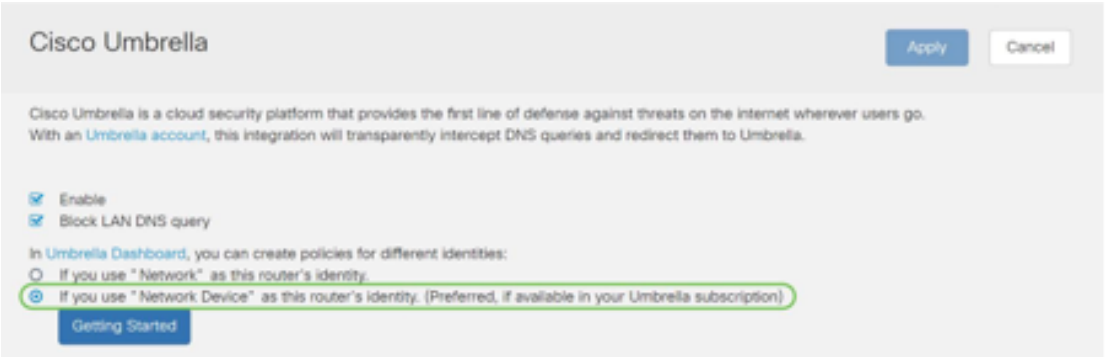


Paso 3 (opcional)

De forma predeterminada, el cuadro *Block LAN DNS Queries* (Bloquear consultas DNS de LAN) está seleccionado. Esta característica clara crea automáticamente listas de control de acceso en el router, lo que impedirá que el tráfico DNS salga a Internet. Esta función obliga a que todas las solicitudes de traducción de dominios se dirijan a través del RV345P y es una buena idea para la mayoría de los usuarios.

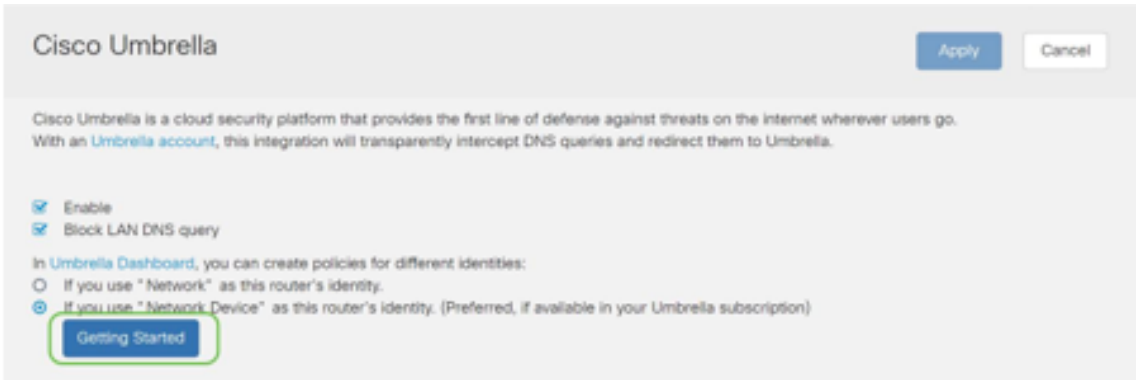
Paso 4

El siguiente paso se desarrolla de dos maneras diferentes. Ambos dependen de la configuración de la red. Si utiliza un servicio como DynDNS o NoIP, deja el esquema de nombres predeterminado de "Red". Deberá iniciar sesión en esas cuentas para asegurarse de que Umbrella interactúa con esos servicios a medida que proporciona protección. Para ello, confiamos en el "dispositivo de red", por lo que hacemos clic en el botón de opción inferior.



Paso 5

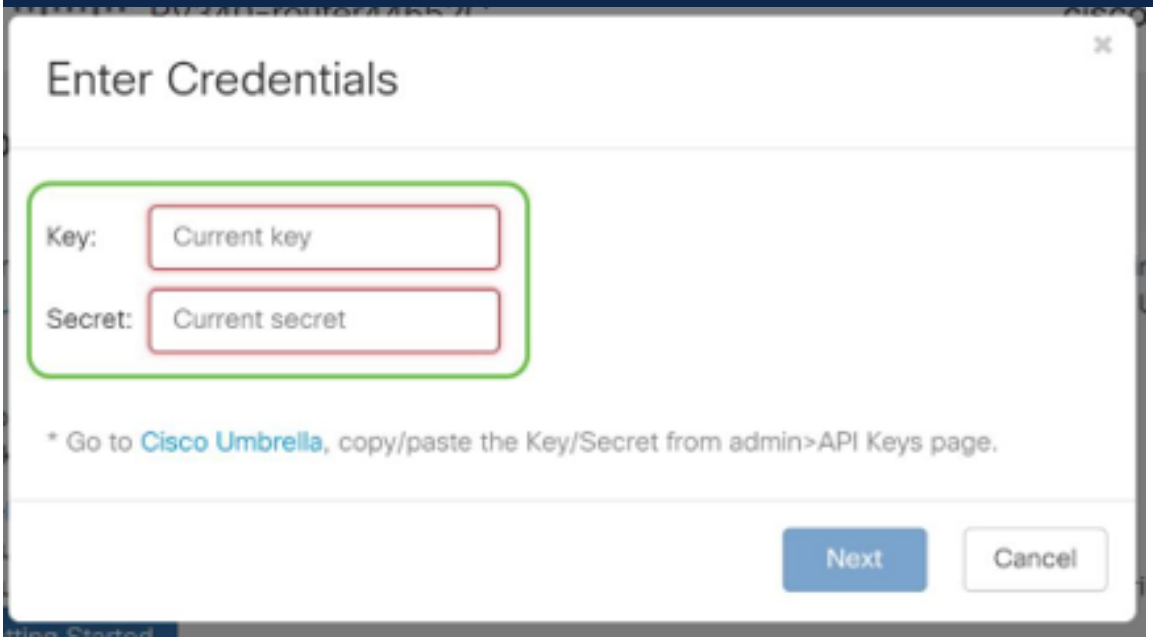
Haga clic en **Introducción**.



Paso 6

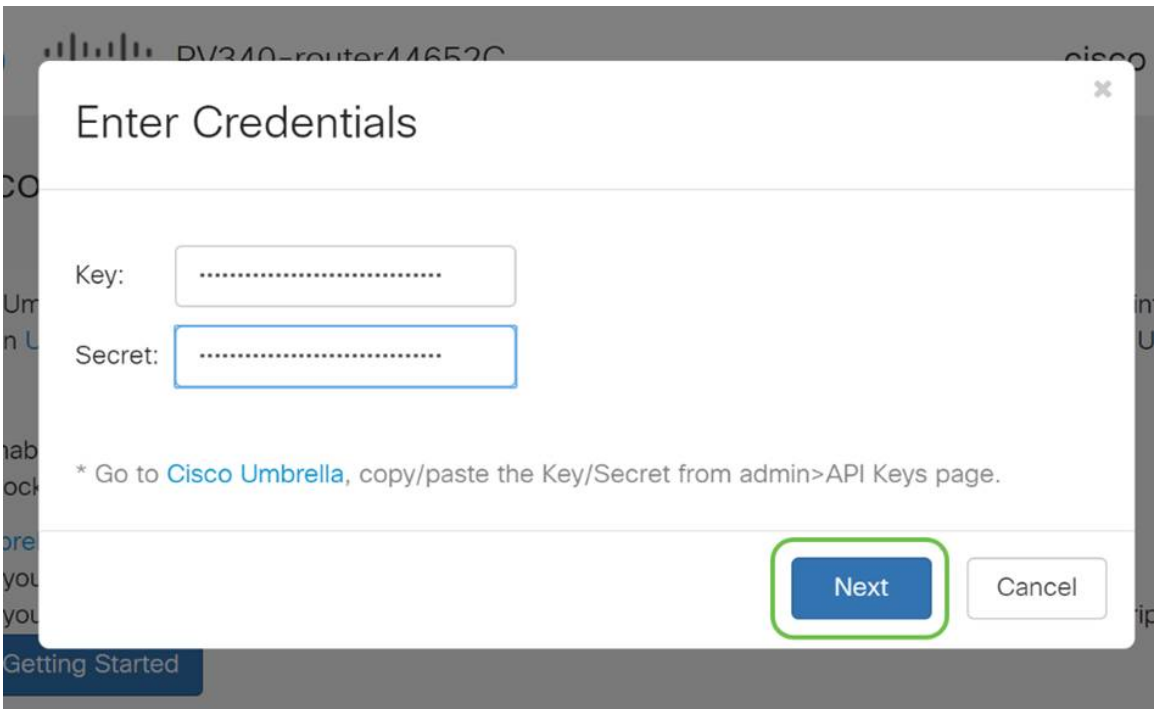
Ingrese la **clave API** y la **clave secreta** en los cuadros de texto.

¡Llamarlo dos veces para que sepas que es importante! Si pierde o elimina accidentalmente la clave secreta, no hay ninguna función o número de soporte al que llamar para recuperar esta clave. Manténgalo en secreto y a salvo. Si se pierde, deberá eliminar la clave y volver a autorizar la nueva clave de API con cada dispositivo que desee proteger con Umbrella.



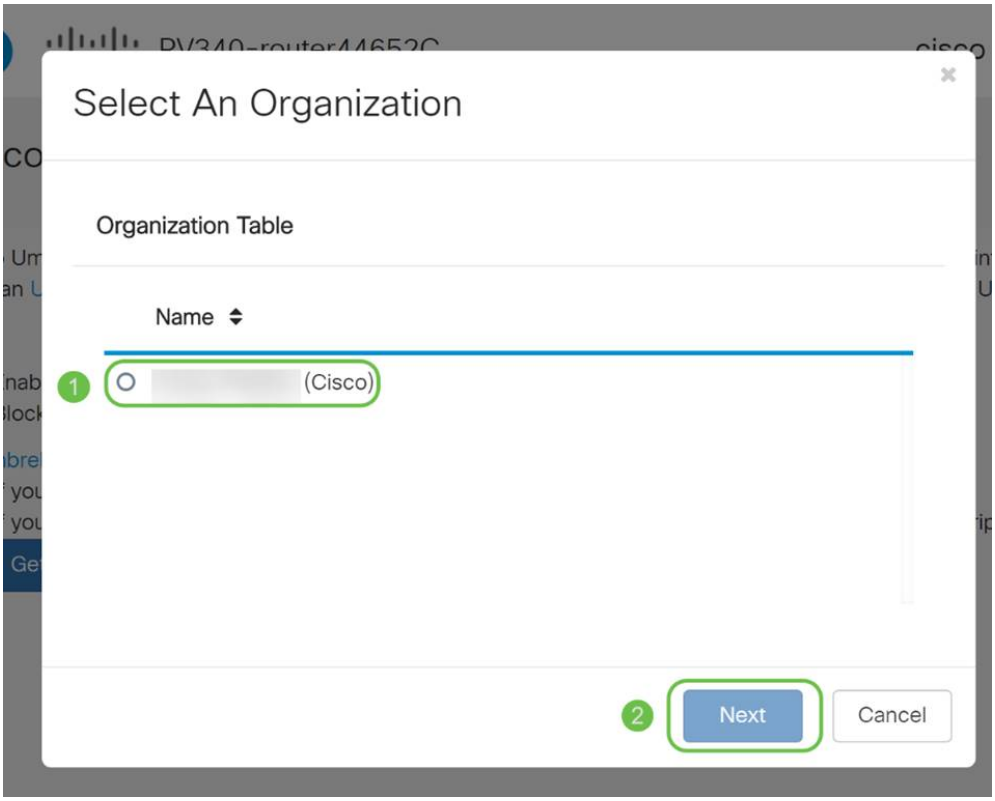
Paso 7

Después de introducir la API y la clave secreta, haga clic en el botón **Next**.



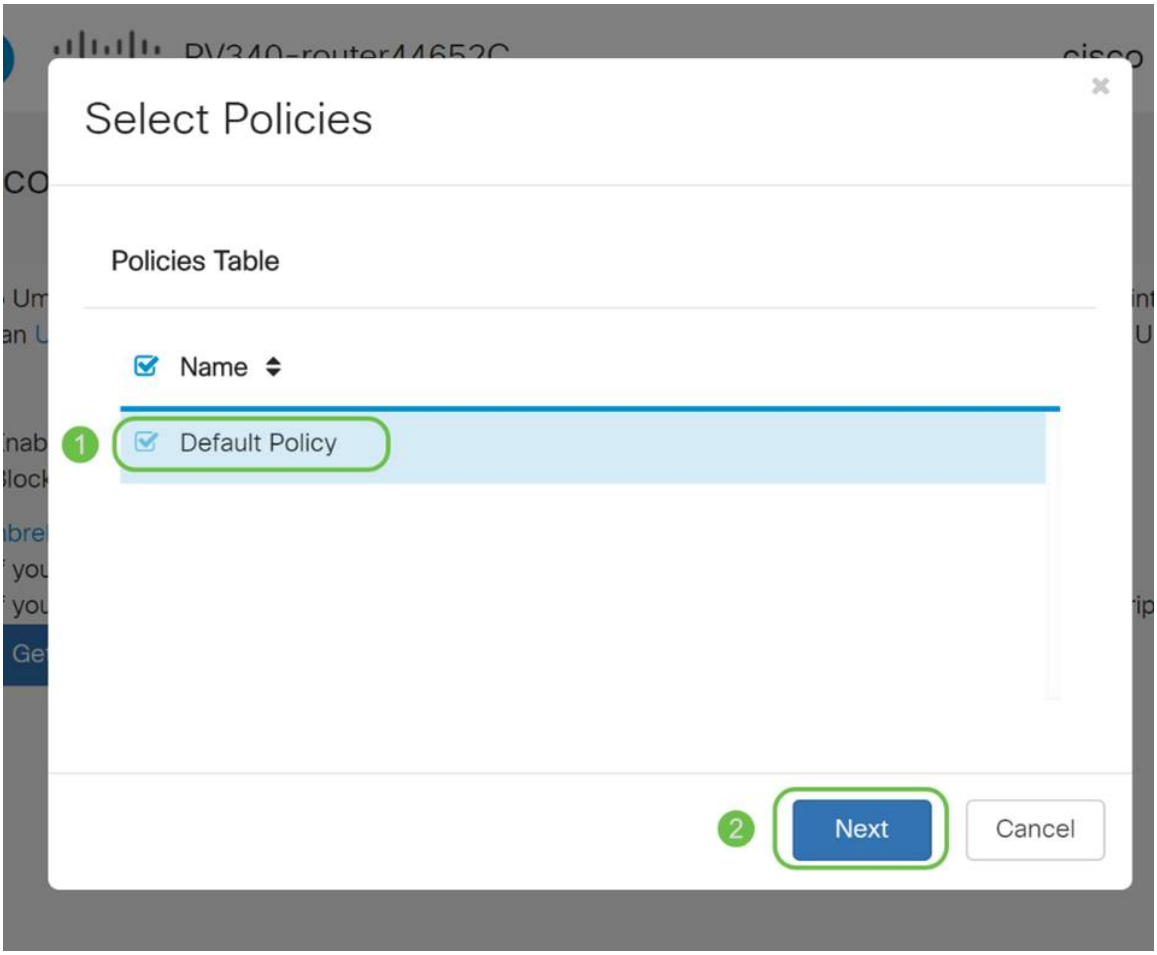
Paso 8

En la siguiente pantalla, seleccione la **organización** que desea asociar al router. Haga clic en Next (Siguiente).



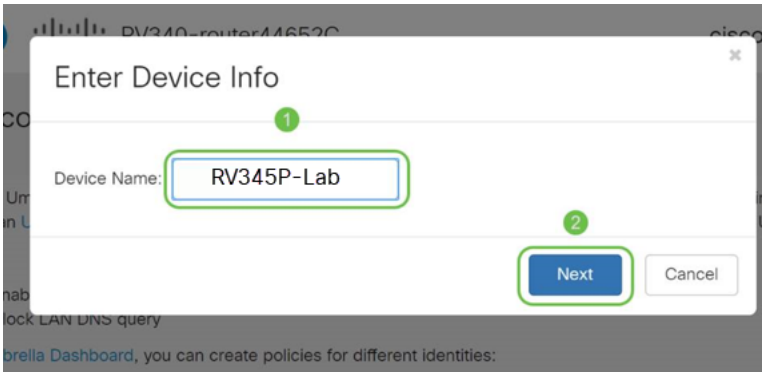
Paso 9

Seleccione la política que se aplicará al tráfico ruteado por el RV345P. Para la mayoría de los usuarios, la política predeterminada proporcionará suficiente cobertura.



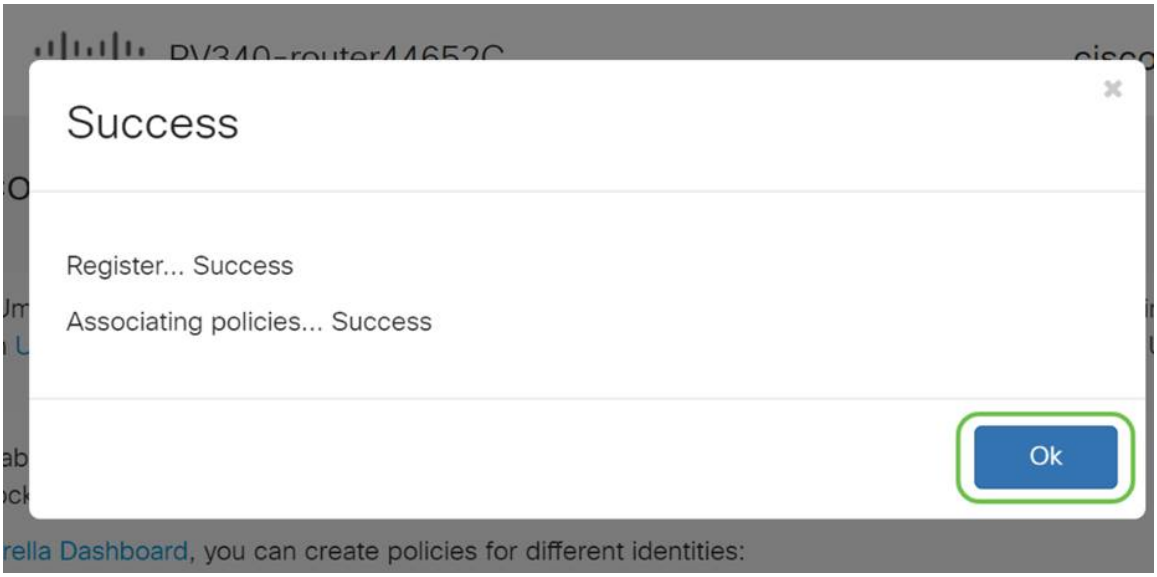
Paso 10

Asigne un nombre al dispositivo para que se pueda designar en Informes de Umbrella. En nuestra configuración, lo hemos llamado *RV345P-Lab*.



Paso 11

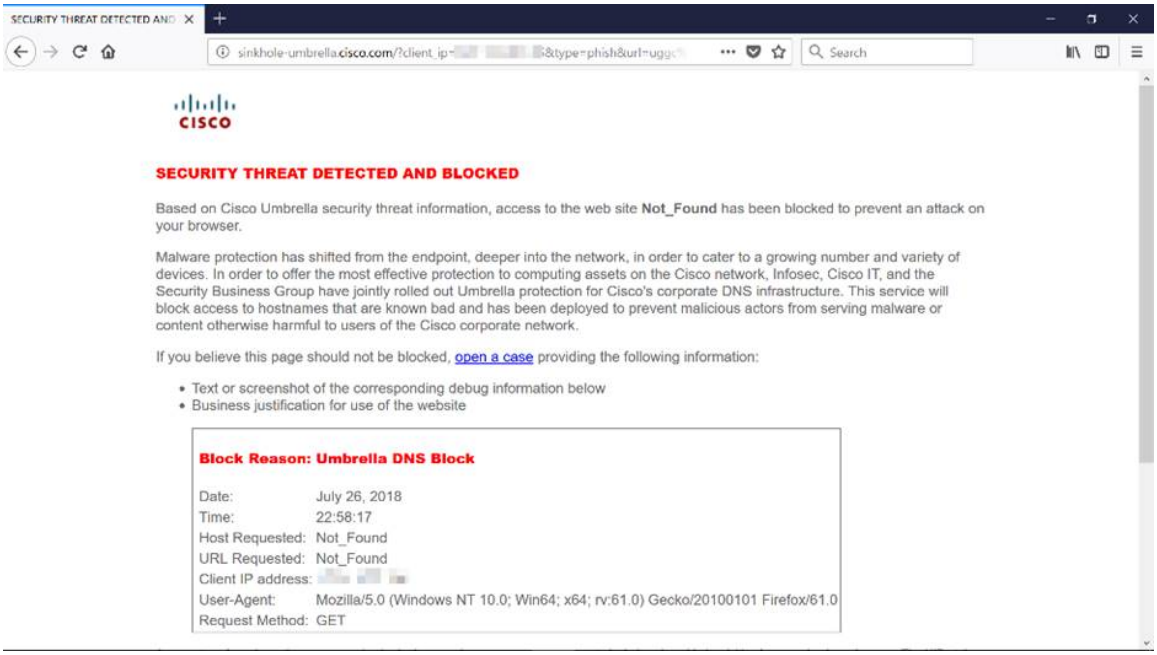
La siguiente pantalla validará los parámetros seleccionados y proporcionará una actualización cuando se asocie correctamente. Click OK.



Confirmación

Enhorabuena, ahora está protegido por Cisco Umbrella. ¿O sí? Asegúrese de que mediante la doble comprobación con un ejemplo en directo, Cisco ha creado un sitio web dedicado a determinar esto tan rápido como se carga la página. Haga clic aquí o escriba https://InternetBadGuys.com en la barra del explorador.

Si Umbrella está configurado correctamente, será recibido por una pantalla similar a esta.



Otras opciones de seguridad

¿Le preocupa que alguien intente acceder sin autorización a la red desconectando un cable Ethernet de un dispositivo de red y conectándolo? En este caso, es importante registrar una lista de hosts permitidos para conectarse directamente al router con sus respectivas direcciones IP y MAC. Se pueden encontrar instrucciones en el artículo Configure IP Source Guard en el RV34x Series Router.

Opciones de VPN

Una conexión de red privada virtual (VPN) permite a los usuarios acceder, enviar y recibir datos desde y hacia una red privada a través de una red pública o compartida, como Internet, pero garantiza una conexión segura a una infraestructura de red subyacente para proteger la red privada y sus recursos.

Un túnel VPN establece una red privada que puede enviar datos de forma segura mediante cifrado y autenticación. Las oficinas corporativas utilizan principalmente la conexión VPN, ya que es útil y necesario permitir que sus empleados tengan acceso a su red privada aunque se encuentren fuera de la oficina.

La VPN permite que un host remoto actúe como si se encontrara en la misma red local. El router admite hasta 50 túneles. Se puede configurar una conexión VPN entre el router y un terminal después de que el router se haya configurado para la conexión a Internet. El cliente VPN depende completamente de la configuración del router VPN para poder establecer una conexión.

Si no está seguro de qué VPN se ajusta mejor a sus necesidades, consulte Descripción General y Prácticas Recomendadas de Cisco Business VPN.

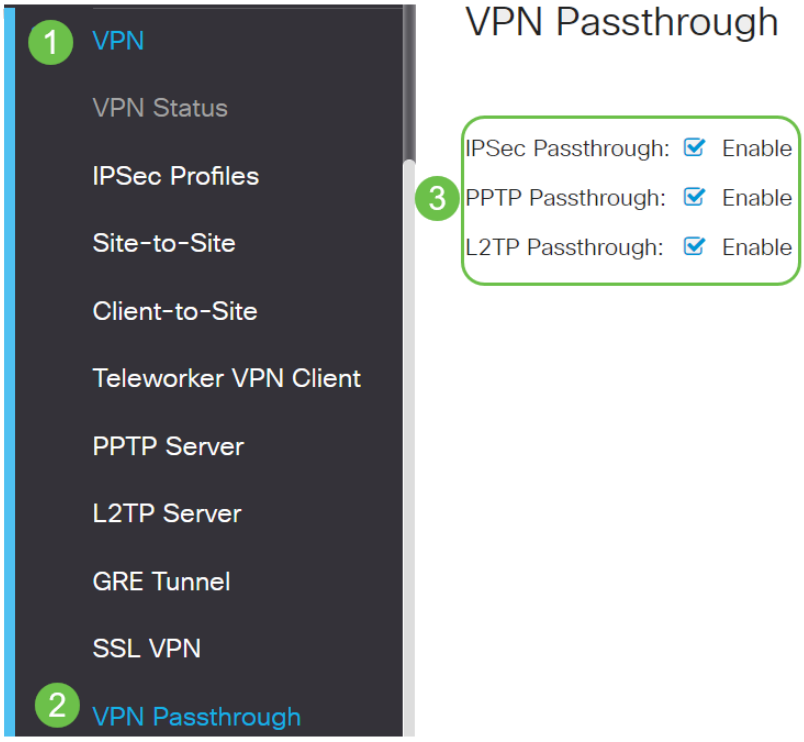
AnyConnect VPN es el único producto compatible con Cisco VPN que se muestra en esta guía de configuración. Cisco no admite productos de terceros que no sean de Cisco, incluidos TheGreenBow y Shrew Soft. Se incluyen estrictamente con fines de orientación. Si necesita soporte para estos productos más allá del artículo, debe ponerse en contacto con ese tercero para obtener soporte.

Si no tiene previsto configurar una VPN, puede hacer clic para ir a la siguiente sección.

Paso a través de VPN

Por lo general, cada router admite la traducción de direcciones de red (NAT) para conservar las direcciones IP cuando desee admitir varios clientes con la misma conexión a Internet. Sin embargo, el protocolo de túnel punto a punto (PPTP) y la VPN de seguridad de protocolo de Internet (IPsec) no admiten NAT. Aquí es donde entra el paso a través de VPN. Un paso a través de VPN es una función que permite que el tráfico VPN generado a partir de clientes VPN conectados a este router pase a través de este router y se conecte a un punto final de VPN. El paso a través de VPN permite que PPTP y VPN IPsec pasen solamente a Internet, que se inicia desde un cliente VPN, y luego alcancen el gateway VPN remoto. Esta función se encuentra comúnmente en los routers domésticos que soportan NAT.

De forma predeterminada, IPsec, PPTP y L2TP Passthrough están habilitados. Si desea ver o ajustar estos parámetros, seleccione **VPN > VPN Passthrough**. Ver o ajustar según sea necesario.



VPN AnyConnect

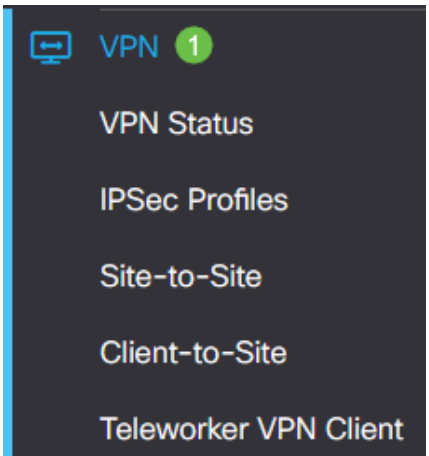
El uso de Cisco AnyConnect presenta varias ventajas:

1. Conectividad segura y persistente
2. Seguridad persistente y aplicación de políticas
3. Implementable desde Adaptive Security Appliance (ASA) o desde sistemas de implementación de software empresarial
4. Personalizable y traducible
5. Configuración sencilla
6. Admite seguridad de protocolo de Internet (IPsec) y capa de sockets seguros (SSL)
7. Admite el protocolo Internet Key Exchange versión 2.0 (IKEv2.0)

Configuración de AnyConnect SSL VPN en el RV345P

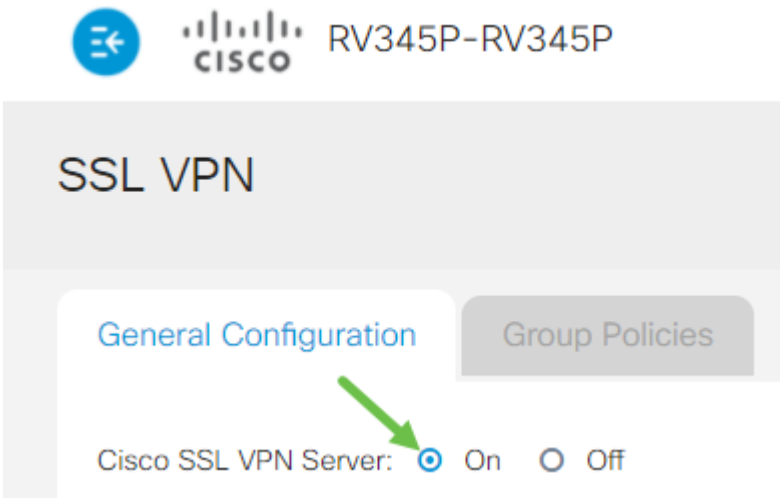
Paso 1

Acceda a la utilidad basada en web del router y elija **VPN > SSL VPN**.



Paso 2

Haga clic en el botón de opción **On** para habilitar Cisco SSL VPN Server.



Configuración de gateway obligatoria

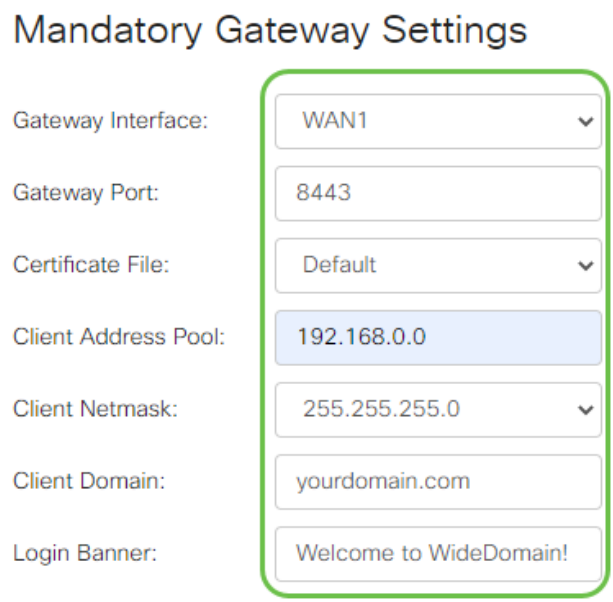
Paso 1

Los siguientes parámetros de configuración son obligatorios:

1. Elija Gateway Interface en la lista desplegable. Este será el puerto que se utilizará para pasar el tráfico a través de los túneles SSL VPN. Entre las opciones se incluyen: WAN1, WAN2, USB1, USB2
2. Introduzca el número de puerto que se utiliza para el gateway VPN SSL en el campo Puerto de la puerta de enlace que va del 1 al 65535.
3. Elija el archivo de certificado de la lista desplegable. Este certificado autentica a los usuarios que intentan acceder al recurso de red a través de los túneles SSL VPN. La lista desplegable contiene un certificado predeterminado y los certificados que se importan.
4. Ingrese la dirección IP del conjunto de direcciones del cliente en el campo *Conjunto de direcciones del cliente*. Este conjunto será el rango de direcciones IP que se asignarán a clientes VPN remotos.

   Asegúrese de que el rango de direcciones IP no se superpone con ninguna de las direcciones IP de la red local.

6. Elija la máscara de red del cliente en la lista desplegable.
7. Ingrese el nombre de dominio del cliente en el campo *Dominio del cliente*. Este será el nombre de dominio que se debe enviar a los clientes SSL VPN.
8. Introduzca el texto que aparecería como banner de inicio de sesión en el campo *Banner de inicio de sesión*. Este será el banner que se mostrará cada vez que un cliente inicie sesión.



Paso 2

Haga clic en Apply (Aplicar).

Parámetros de puerta de enlace opcionales

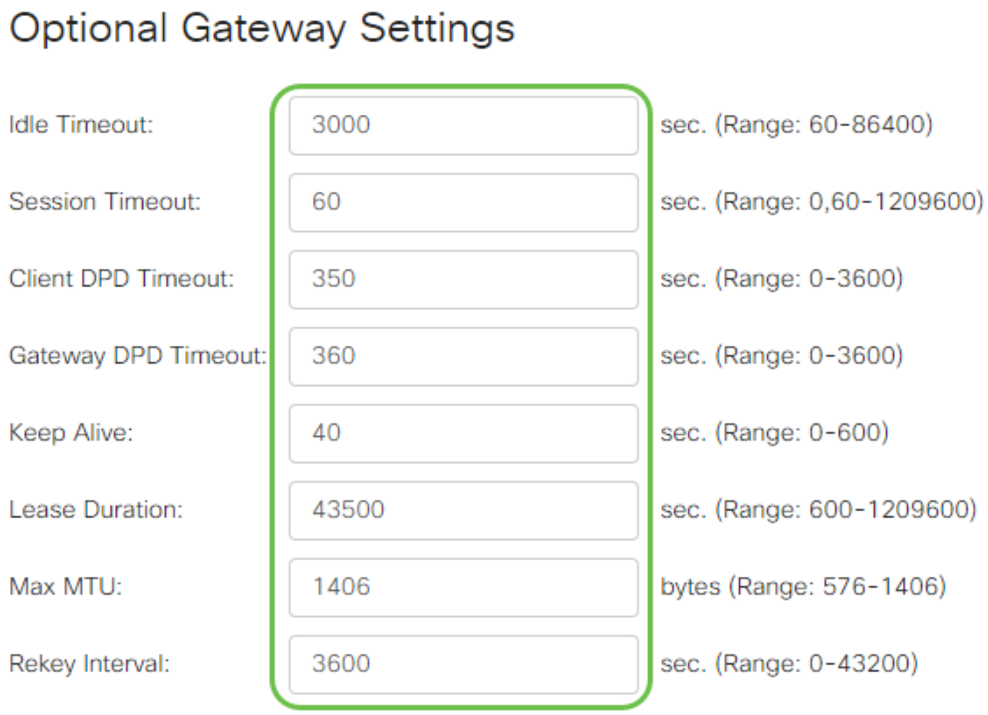
Paso 1

Los siguientes parámetros de configuración son opcionales:

1. Introduzca un valor en segundos para el tiempo de espera inactivo comprendido entre 60 y 86400. Este será el tiempo que la sesión SSL VPN puede permanecer inactiva.
2. Introduzca un valor en segundos en el campo *Tiempo de espera de sesión*. Este es el tiempo que tarda la sesión del protocolo de control de transmisión (TCP) o del protocolo de datagramas de usuario (UDP) en agotarse después del tiempo de inactividad especificado. El rango va de 60 a 1209600.
3. Ingrese un valor en segundos en el campo *ClientDPD Timeout* entre 0 y 3600. Este valor especifica el envío periódico de mensajes HELLO/ACK para verificar el estado del túnel VPN. Esta función debe estar habilitada en ambos extremos del túnel VPN.
4. Ingrese un valor en segundos en el campo *GatewayDPD Timeout* entre 0 y 3600. Este valor especifica el envío periódico de mensajes HELLO/ACK para verificar el estado del túnel VPN. Esta función debe estar habilitada en ambos extremos del túnel VPN.
5. Introduzca un valor en segundos en el campo *Mantener activo* entre 0 y 600. Esta función garantiza que el router siempre esté conectado a Internet. Intentará restablecer la conexión VPN si se interrumpe.
6. Introduzca un valor en segundos para la duración del túnel que se conectará en el campo *Duración del arrendamiento*. El rango va de 600 a 1209600.
7. Introduzca el tamaño del paquete en bytes que se puede enviar a través de la red. El

rango va de 576 a 1406.

8. Ingrese el tiempo del intervalo de relevo en el campo *Intervalo de actualización*. La función Rekey permite que las claves SSL se renegocien después de que se haya establecido la sesión. El rango está entre 0 y 43200.



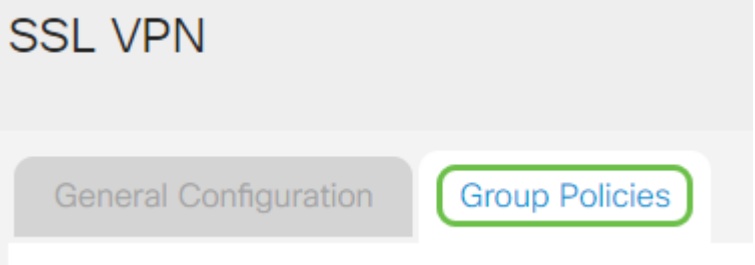
Paso 2

Haga clic en Apply (Aplicar).

Configurar políticas de grupo

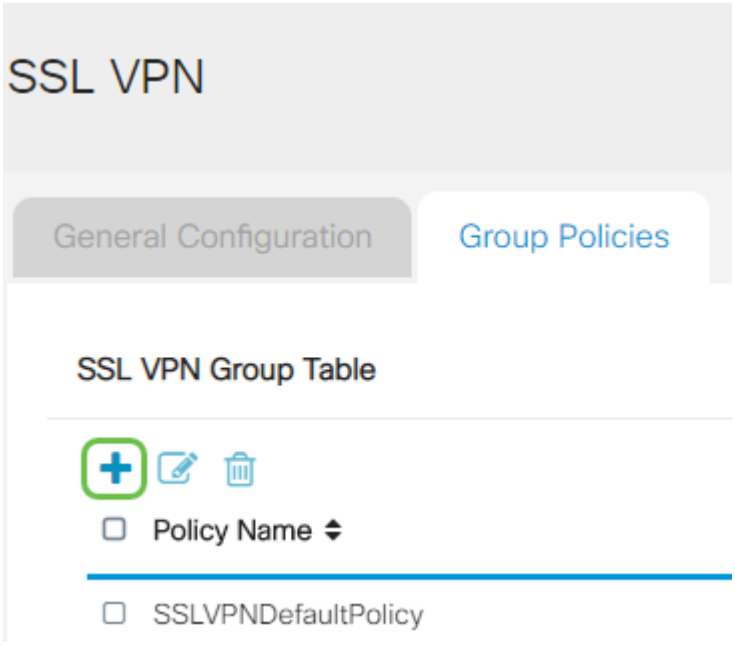
Paso 1

Haga clic en la ficha **Políticas de grupo**.



Paso 2

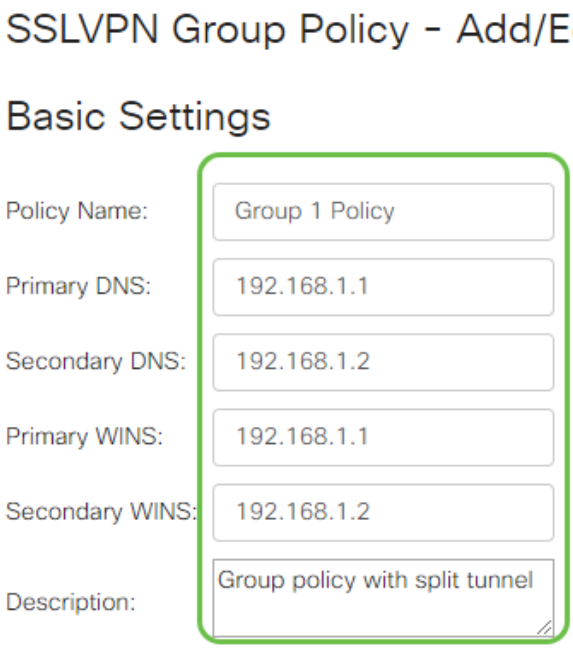
Haga clic en el **icono add** bajo la Tabla SSL VPN Group para agregar una política de grupo.



La tabla SSL VPN Group mostrará la lista de políticas de grupo en el dispositivo. También puede editar la primera política de grupo de la lista, que se denomina SSLVPNDefaultPolicy. Ésta es la política predeterminada proporcionada por el dispositivo.

Paso 3

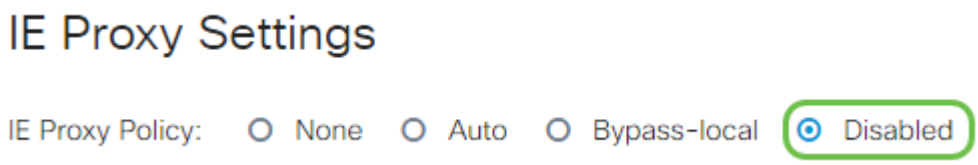
1. Introduzca el nombre de política preferido en el campo *Policy Name*.
2. Introduzca la dirección IP del DNS principal en el campo proporcionado. De forma predeterminada, esta dirección IP ya se ha suministrado.
3. *(Opcional) Introduzca la dirección IP del DNS secundario en el campo proporcionado. Esto servirá como copia de seguridad en caso de que el DNS primario falle.*
4. (Opcional) Introduzca la dirección IP del WINS principal en el campo proporcionado.
5. (Opcional) Introduzca la dirección IP del WINS secundario en el campo proporcionado.
6. (Opcional) Introduzca una descripción de la política en el campo *Descripción*.



Paso 4 (opcional)

Haga clic en un botón de opción para elegir la política de proxy de IE para habilitar los parámetros de proxy de Microsoft Internet Explorer (MSIE) para establecer el túnel VPN. Las opciones son:

- Ninguno: permite que el explorador no utilice ninguna configuración de proxy.
- Auto (Automático): Permite al explorador detectar automáticamente los parámetros del proxy.
- Bypass-local: permite al explorador omitir los parámetros de proxy configurados en el usuario remoto.
- Desactivado: desactiva la configuración del proxy MSIE.



Paso 5 (opcional)

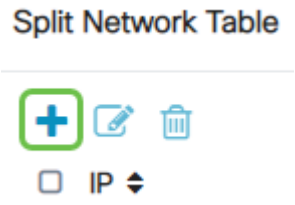
En el área Configuración de Tunelización Dividida, marque la casilla **Habilitar Tunelización Dividida** para permitir que el tráfico destinado a Internet se envíe sin cifrar directamente a Internet. La tunelización completa envía todo el tráfico al dispositivo final donde luego se enruta a los recursos de destino, eliminando la red corporativa de la ruta para el acceso web.

Paso 6 (opcional)

Haga clic en un botón de opción para elegir si incluir o excluir el tráfico al aplicar la tunelización dividida.

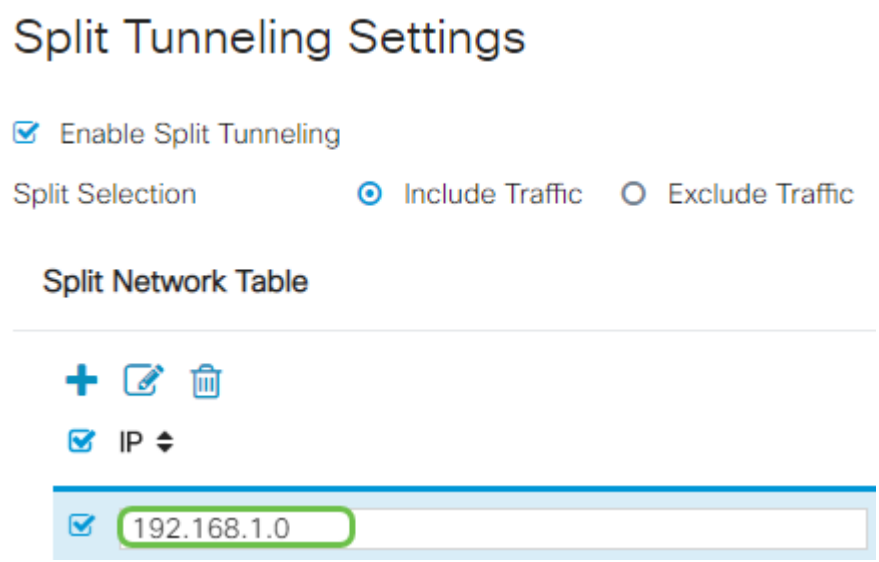
Paso 7

En Split Network Table (Tabla de red dividida), haga clic en el **icono add** para agregar una excepción split Network (Red dividida).



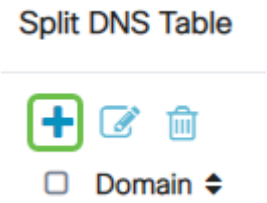
Paso 8

Introduzca la dirección IP de la red en el campo proporcionado.



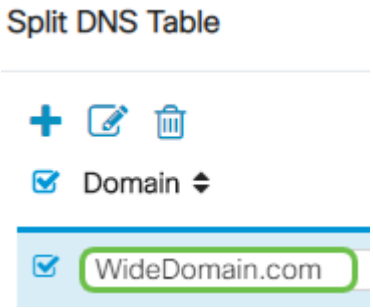
Paso 9

En Split DNS Table (Dividir tabla DNS), haga clic en el **icono add** para agregar una excepción de DNS dividido.



Paso 10

Introduzca el nombre de dominio en el campo proporcionado y, a continuación, haga clic en **Aplicar**.



El router incluye 2 licencias de servidor AnyConnect de forma predeterminada. Esto significa que una vez que tenga licencias de cliente de AnyConnect, puede establecer 2 túneles VPN simultáneamente con cualquier otro router de la serie RV340.

En resumen, el router RV345P no necesita una licencia, pero todos los clientes necesitarán una. Las licencias de cliente AnyConnect permiten a los clientes móviles y de escritorio acceder a la red VPN de forma remota.

En esta sección se explica cómo obtener licencias para sus clientes.

Cliente de movilidad AnyConnect

Un cliente VPN es un software instalado y ejecutado en un equipo que desea conectarse a la red remota. Este software cliente debe configurarse con la misma configuración que la del servidor VPN, como la dirección IP y la información de autenticación. Esta información de autenticación incluye el nombre de usuario y la clave previamente compartida que se utilizará para cifrar los datos. Según la ubicación física de las redes que se conecten, un cliente VPN también puede ser un dispositivo de hardware. Esto suele suceder si la conexión VPN se utiliza para conectar dos redes que se encuentran en ubicaciones separadas.

Cisco AnyConnect Secure Mobility Client es una aplicación de software para conectarse a una VPN que funciona en diversos sistemas operativos y configuraciones de hardware. Esta aplicación de software permite que los recursos remotos de otra red sean accesibles como si el usuario estuviera conectado directamente a su red, pero de forma segura.

Una vez que el router está registrado y configurado con AnyConnect, el cliente puede instalar licencias en el router desde el conjunto de licencias disponible que adquiera, que se detalla en la siguiente sección.

Licencia de compra

Debe comprar una licencia a su distribuidor de Cisco o a su partner de Cisco. Al solicitar una licencia, debe proporcionar su ID de cuenta inteligente o ID de dominio de Cisco en la forma de *name@domain.com*.

Si no tiene un distribuidor o partner de Cisco, puede encontrar uno aquí.

En el momento de escribir este artículo, se pueden utilizar las siguientes SKU de producto para adquirir licencias adicionales en paquetes de 25. Tenga en cuenta que hay otras opciones para las licencias de cliente de AnyConnect, como se describe en la Guía de pedidos de Cisco AnyConnect; sin embargo, la ID de producto que se muestra sería el requisito mínimo para la funcionalidad completa.

Tenga en cuenta que la SKU del producto de la licencia del cliente de AnyConnect se muestra en primer lugar, proporciona licencias por un período de 1 año y requiere una compra mínima de 25 licencias. Otras SKU de productos aplicables a los routers de la serie RV340 también están disponibles con distintos niveles de suscripción, como se indica a continuación:

- **LS-AC-PLS-1Y-S1**: licencia de cliente Cisco AnyConnect Plus de 1 año
- **LS-AC-PLS-3Y-S1**: licencia de cliente de 3 años de Cisco AnyConnect Plus
- **LS-AC-PLS-5Y-S1**: licencia de cliente Cisco AnyConnect Plus de 5 años
- **LS-AC-PLS-P-25-S**: 25 paquetes de licencia de cliente perpetua de Cisco AnyConnect Plus
- **LS-AC-PLS-P-50-S**: 50 paquetes de licencia de cliente perpetua de Cisco AnyConnect Plus

Información del cliente

Cuando su cliente configure uno de los siguientes links, debería enviarles estos links:

- Windows: AnyConnect en un equipo Windows
- Mac: Instale AnyConnect en Mac.
- Escritorio Ubuntu: Instalación y uso de AnyConnect en el escritorio Ubuntu
- Si tiene problemas, puede ir a Recopilar información para la resolución de problemas básicos de errores de Cisco AnyConnect Secure Mobility Client.

Verificar la conectividad VPN de AnyConnect

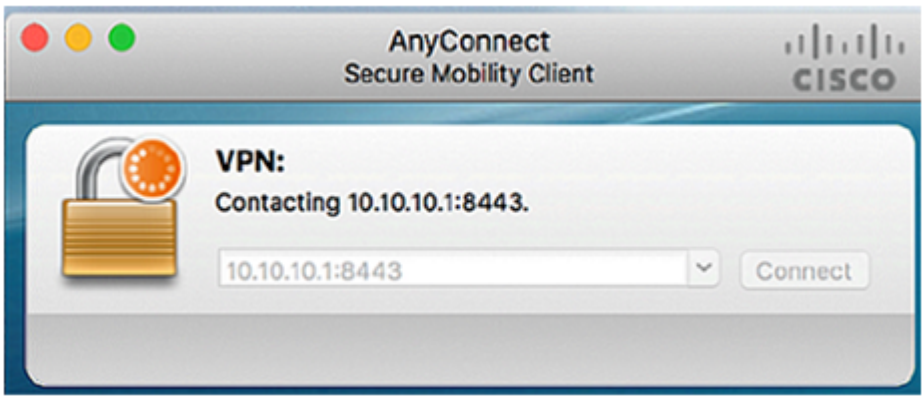
Paso 1

Haga clic en el **icono AnyConnect Secure Mobility Client**.

Paso 2

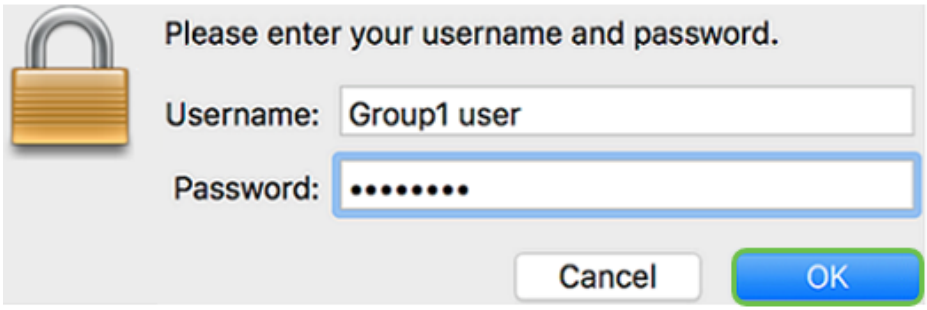
En la ventana AnyConnect Secure Mobility Client, ingrese la dirección IP de la gateway y el número de puerto de la gateway separados por dos puntos (:) y luego haga clic en **Connect**.

El software mostrará ahora que se está poniendo en contacto con la red remota.



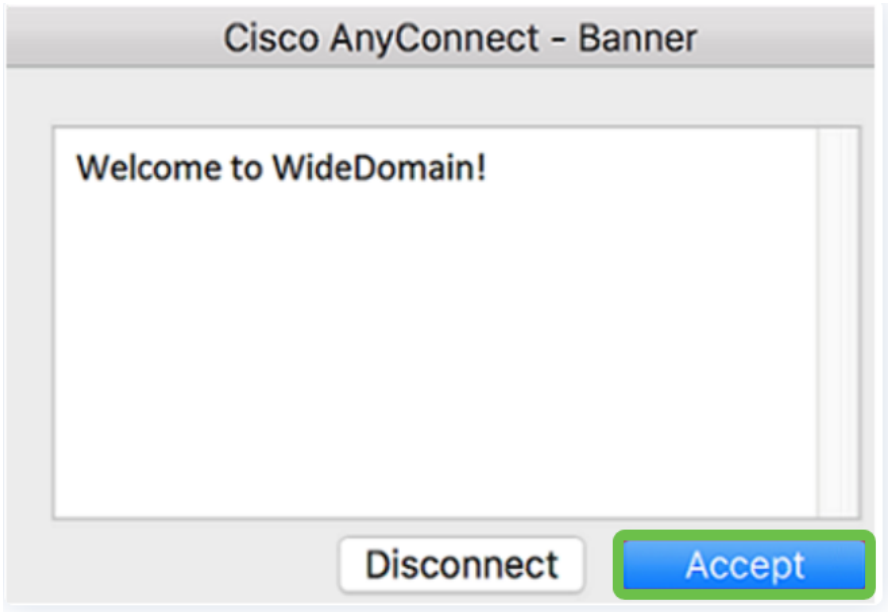
Paso 3

Introduzca el nombre de usuario y la contraseña del servidor en los campos correspondientes y, a continuación, haga clic en **Aceptar**.

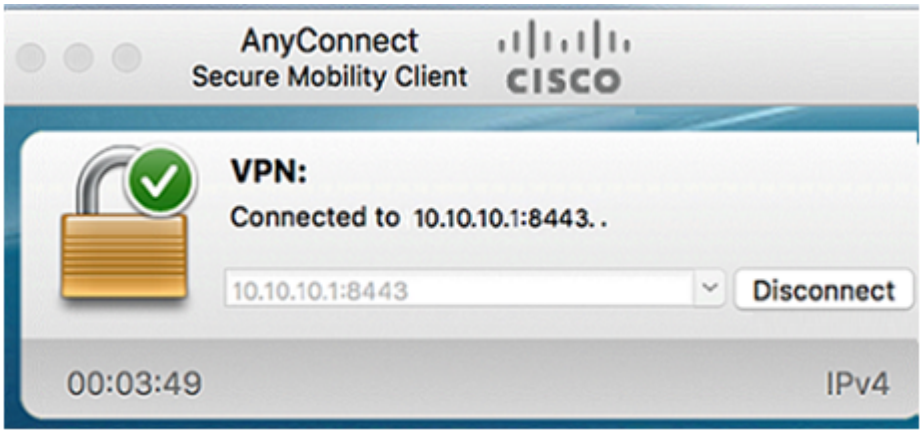


Paso 4

Tan pronto como se establezca la conexión, aparecerá el banner de inicio de sesión. Haga clic en **Aceptar**.



La ventana de AnyConnect debe indicar la conexión VPN correcta a la red.



Si ahora está utilizando AnyConnect VPN, puede omitir otras opciones de VPN y pasar a la siguiente sección.

Shrew Soft VPN

Una VPN IPsec le permite obtener de forma segura recursos remotos mediante el establecimiento de un túnel cifrado a través de Internet. Los routers de la serie RV34X funcionan como servidores VPN IPsec y admiten el Cisco Soft VPN Client. En esta sección se muestra cómo configurar el router y el cliente de software de Cisco para

asegurar una conexión a una VPN.

Cisco no admite Shrew Soft. Este ejemplo se proporciona únicamente con fines de demostración. Si tiene problemas con Shrew Soft, póngase en contacto con ellos para obtener asistencia.

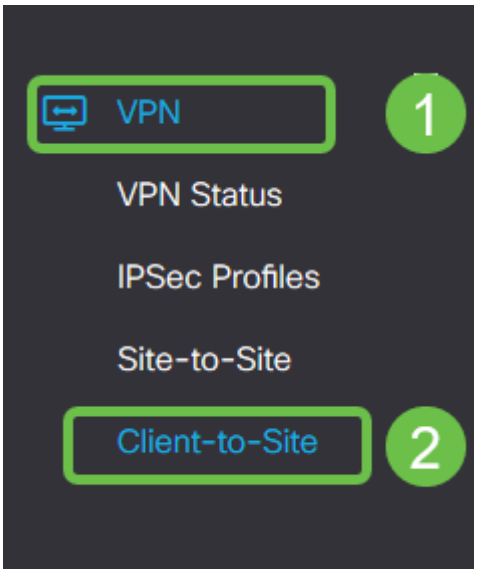
Puede descargar la versión más reciente del software de cliente Shrew Soft VPN aquí: https://www.shrew.net/download/vpn

Configuración de Shrew Soft en el RV345P Series Router

Comenzaremos configurando la **VPN cliente-sitio** en el RV345P.

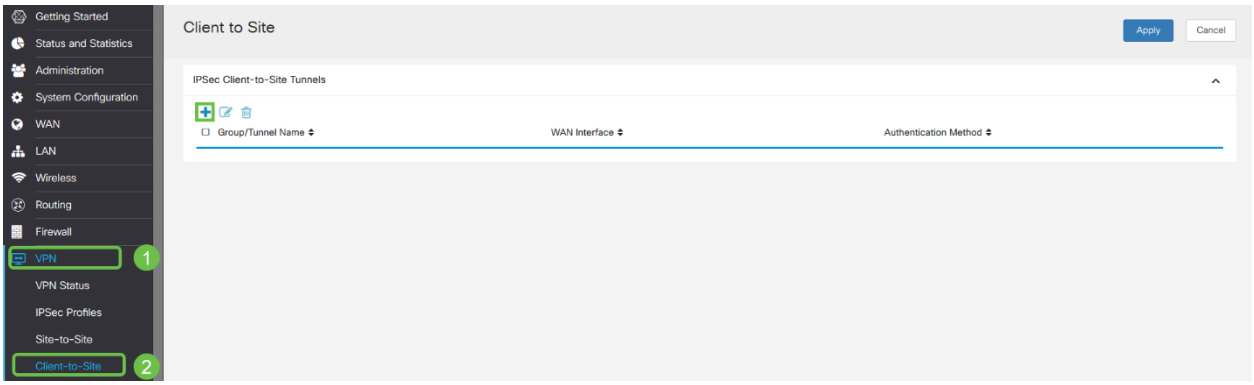
Paso 1

Navegue hasta **VPN > Cliente a Sitio.**



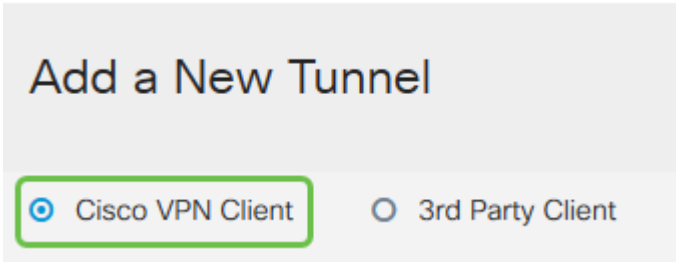
Paso 2

Agregue un perfil VPN **cliente-a-sitio**.



Paso 3

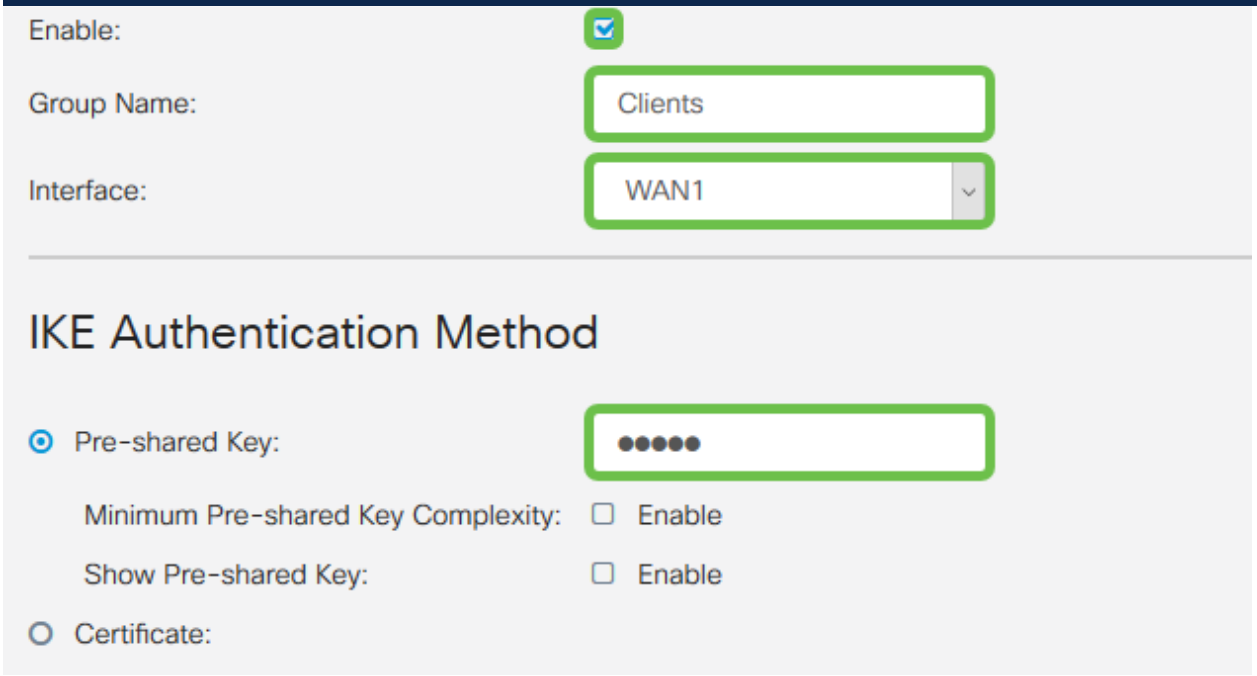
Seleccione la opción **Cisco VPN Client**.



Paso 4

Marque la casilla **Enable** para activar el perfil de cliente VPN. También configuraremos el *nombre del grupo*, seleccionaremos la **interfaz WAN** e introduciremos una **clave precompartida**.

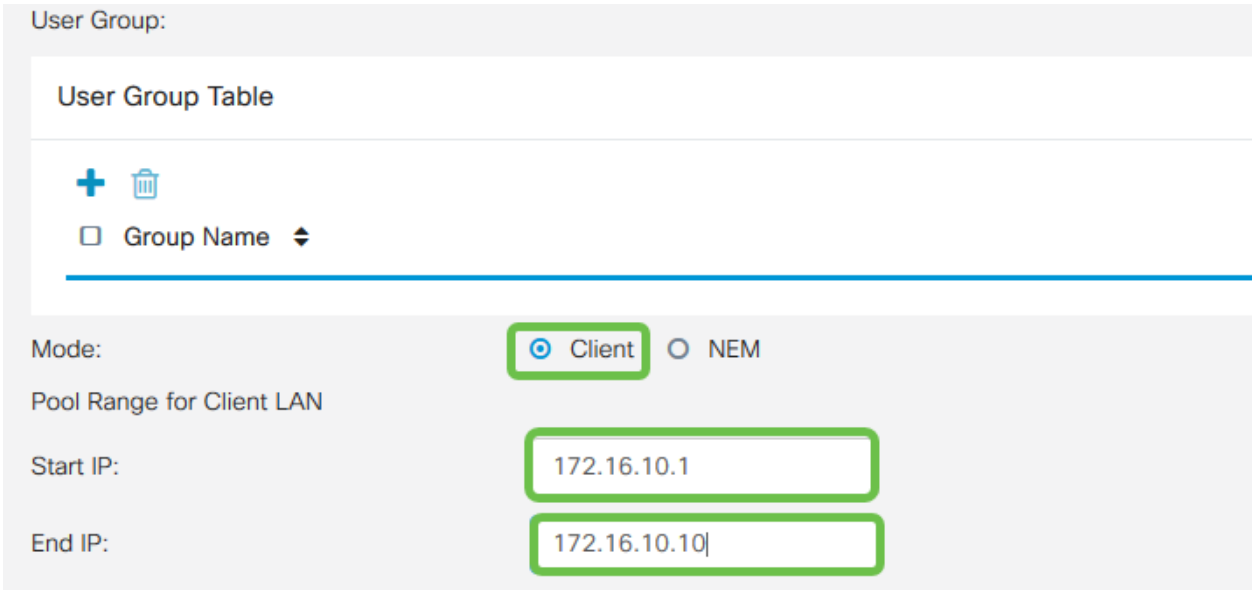
Tenga en cuenta el *nombre del grupo* y la *clave precompartida*, ya que se utilizarán más adelante al configurar el cliente.



Paso 5

Deje la **tabla de grupo de usuarios** en blanco por ahora. Esto es para el *grupo de usuarios* en el router, pero aún no lo hemos configurado. Asegúrese de que el **Modo** esté configurado en **Cliente**. Ingrese el **Rango del Conjunto para LAN del Cliente**. Utilizaremos de 172.16.10.1 a 172.16.10.10.

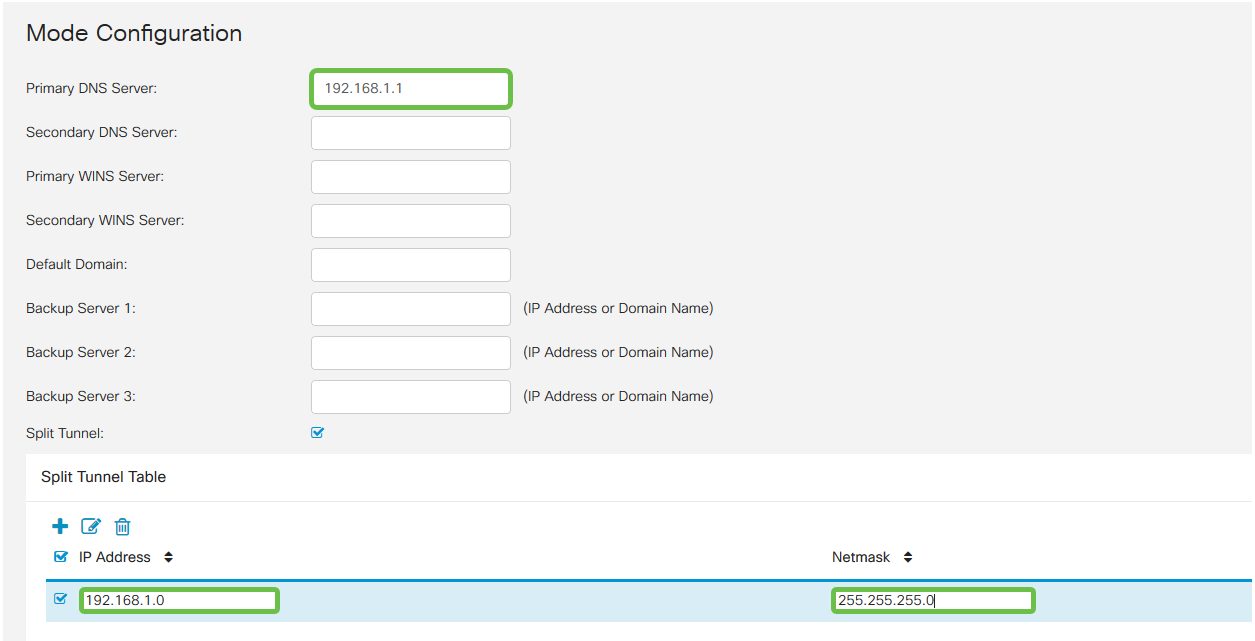
El rango del grupo debe utilizar una subred única que no se utiliza en ninguna otra parte de la red.



Paso 6

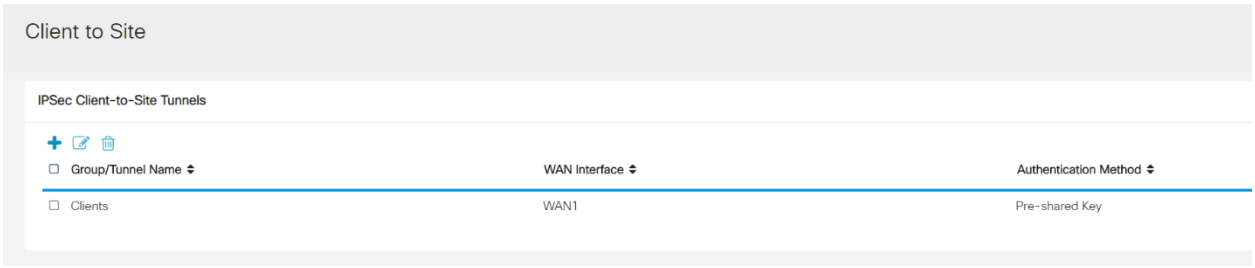
Aquí es donde configuramos la configuración **de modo**. Estos son los ajustes que utilizaremos:

- **Servidor DNS primario**: Si tiene un servidor DNS interno o desea utilizar un servidor DNS externo, puede introducirlo aquí. De lo contrario, el valor predeterminado se establece en la dirección IP de LAN RV345P. Utilizaremos el valor predeterminado en nuestro ejemplo.
- **Túnel dividido:** active esta opción para habilitar la tunelización dividida. Esto se utiliza para especificar qué tráfico pasará por el túnel VPN. Utilizaremos el túnel dividido en nuestro ejemplo.
- **Tabla de Túnel Dividido:** Introduzca las redes a las que el cliente VPN debe tener acceso a través de la VPN. Este ejemplo utiliza la red LAN RV345P.



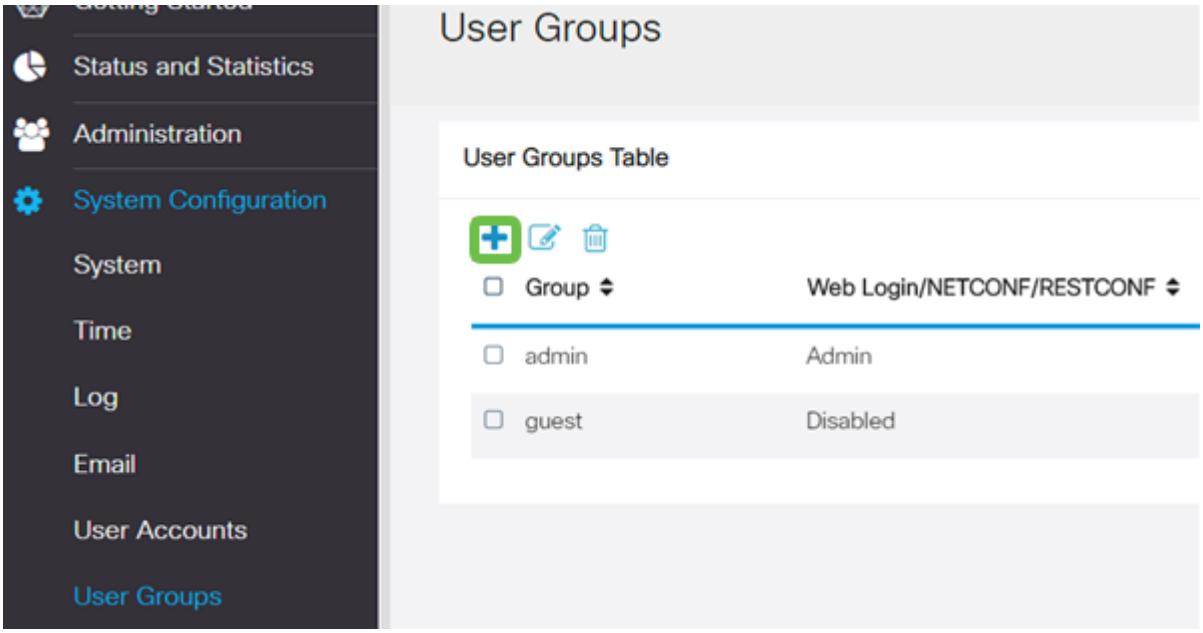
Paso 7

Después de hacer clic en **Guardar**, podemos ver el perfil en la **lista IPsec Client-to-Site Groups**.



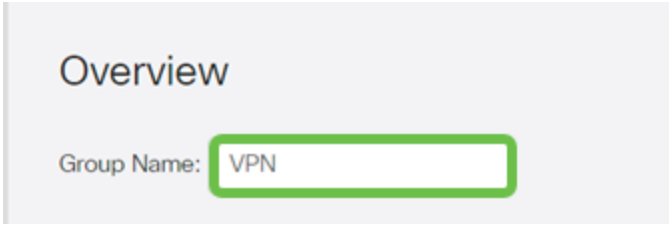
Paso 8

Configure un **grupo de usuarios** para utilizar para autenticar usuarios de clientes VPN. En **Configuración del sistema > Grupos de usuarios**, haga clic en el **icono más** para agregar un grupo de usuarios.



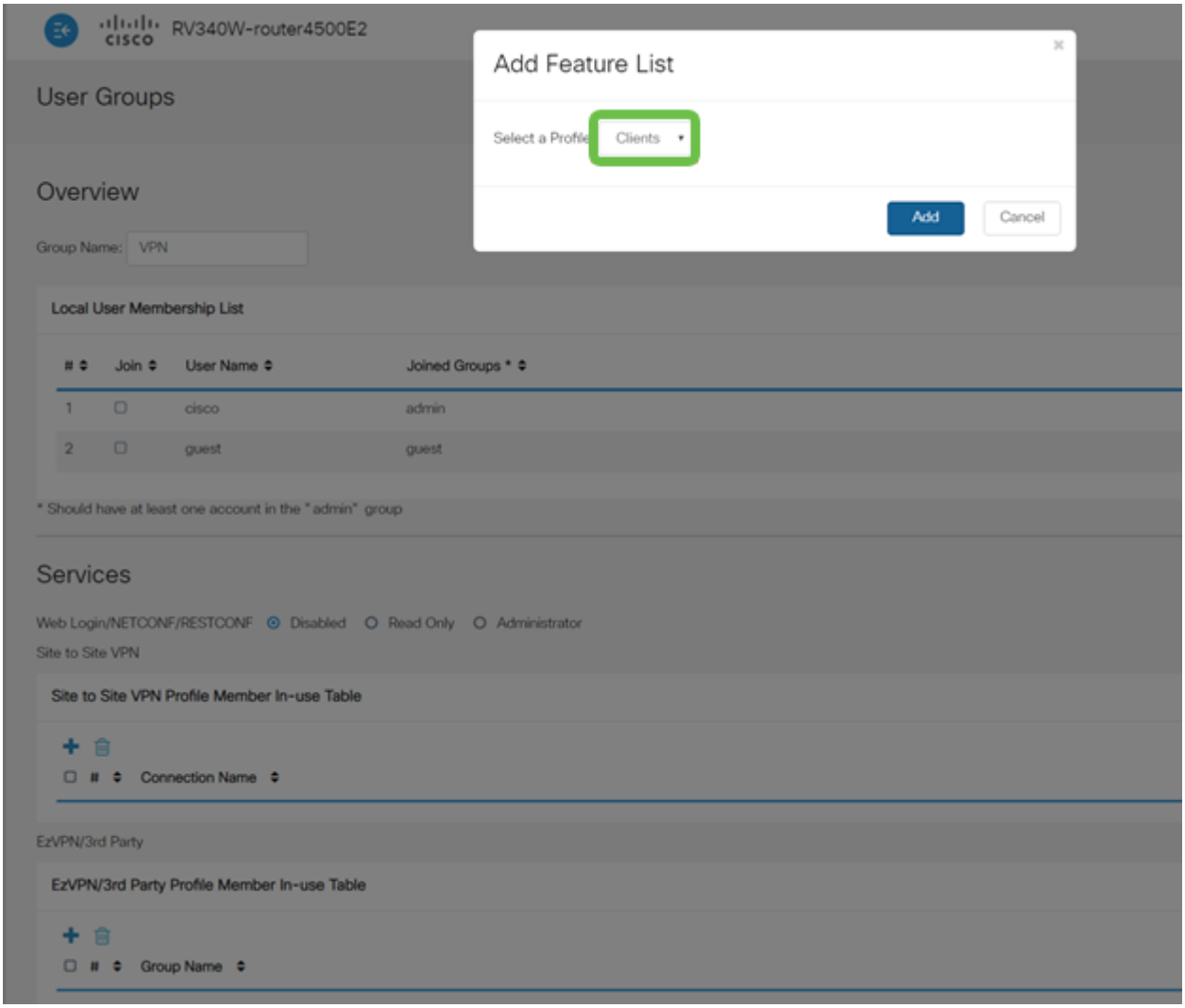
Paso 9

Introduzca un **nombre de grupo**.



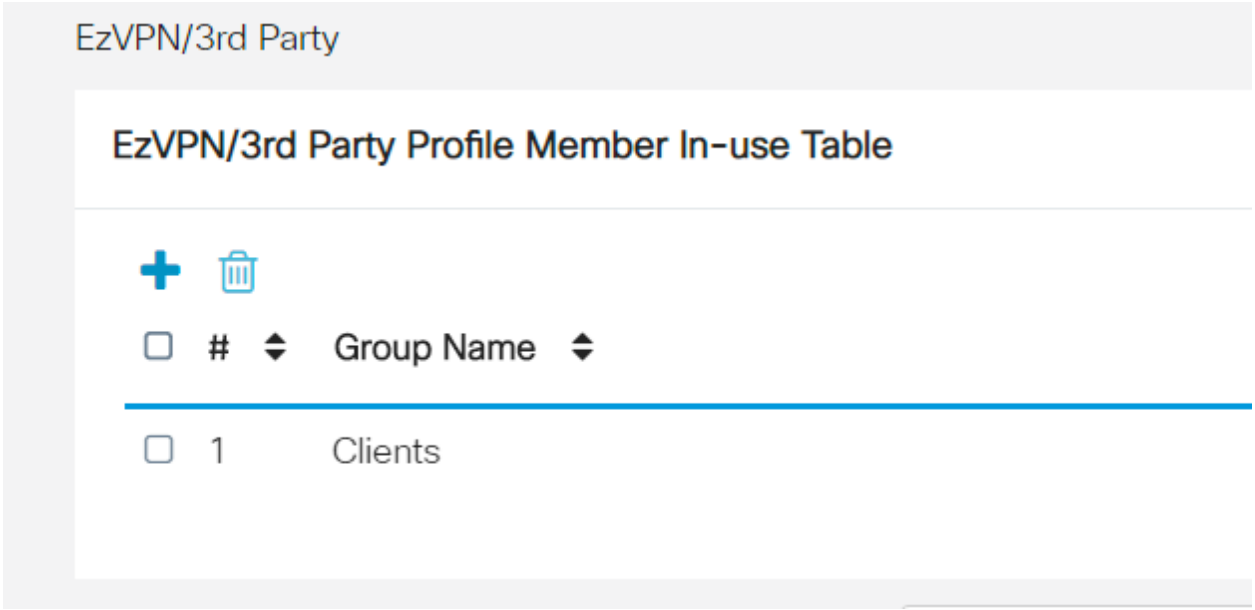
Paso 10

En **Services > EzVPN/3rd Party, haga clic en Add** para vincular este grupo de usuarios al perfil de **cliente a sitio** que se configuró anteriormente.



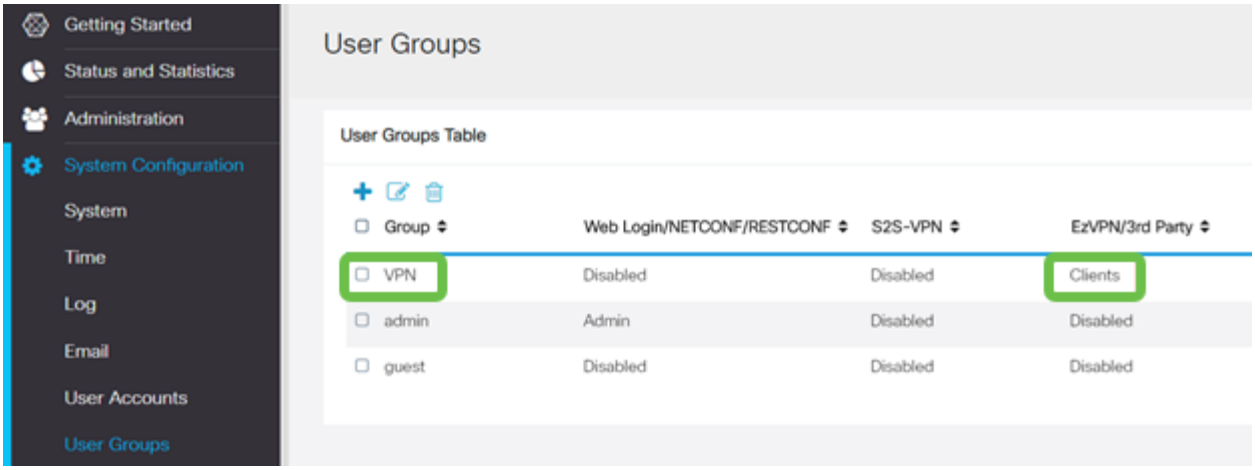
Paso 11

Ahora debería ver el nombre de grupo **cliente a sitio** en la lista de **EzVPN/terceros.**



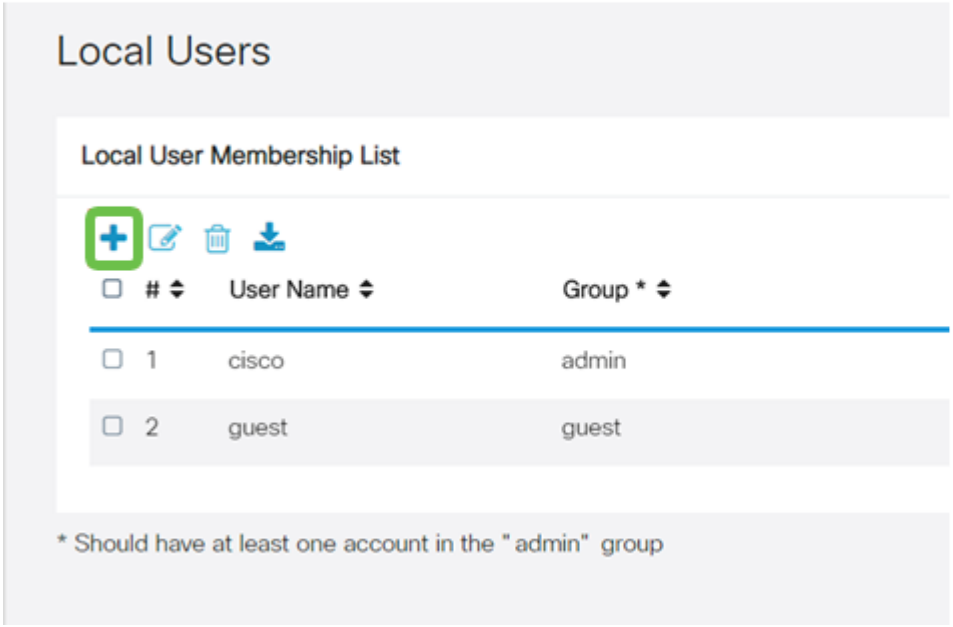
Paso 12

Después de **Aplicar** la configuración de grupo de usuarios, la verá en la lista **Grupos de usuarios** y mostrará que el nuevo grupo de usuarios se utilizará con el perfil cliente a sitio que creó anteriormente.



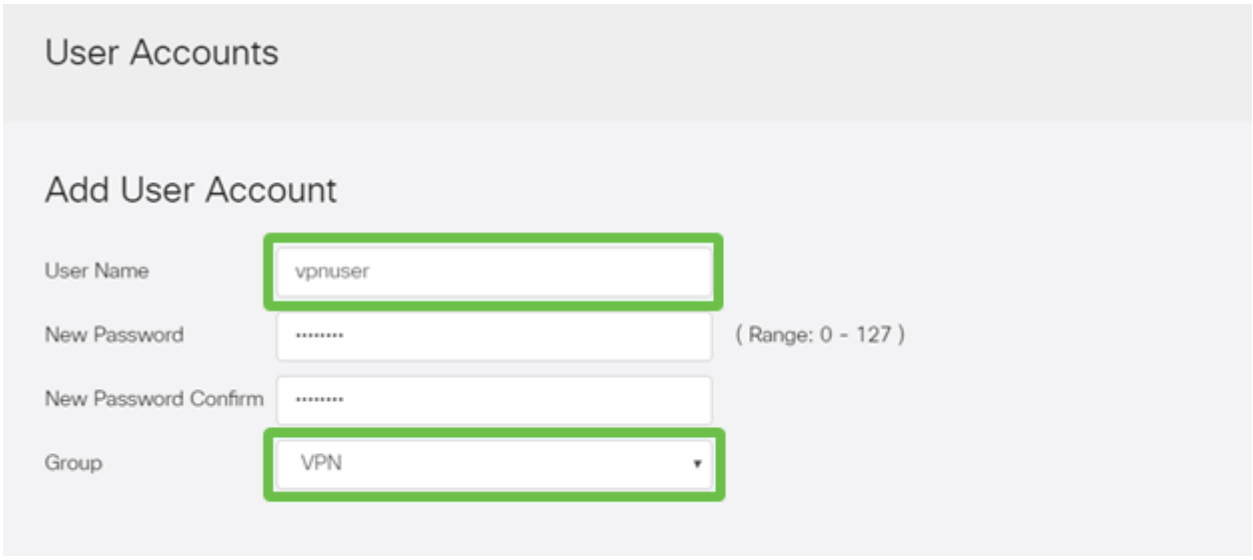
Paso 13

Configure un usuario nuevo en **Configuración del sistema > Cuentas de usuario**. Haga clic en el **icono más** para crear un nuevo usuario.



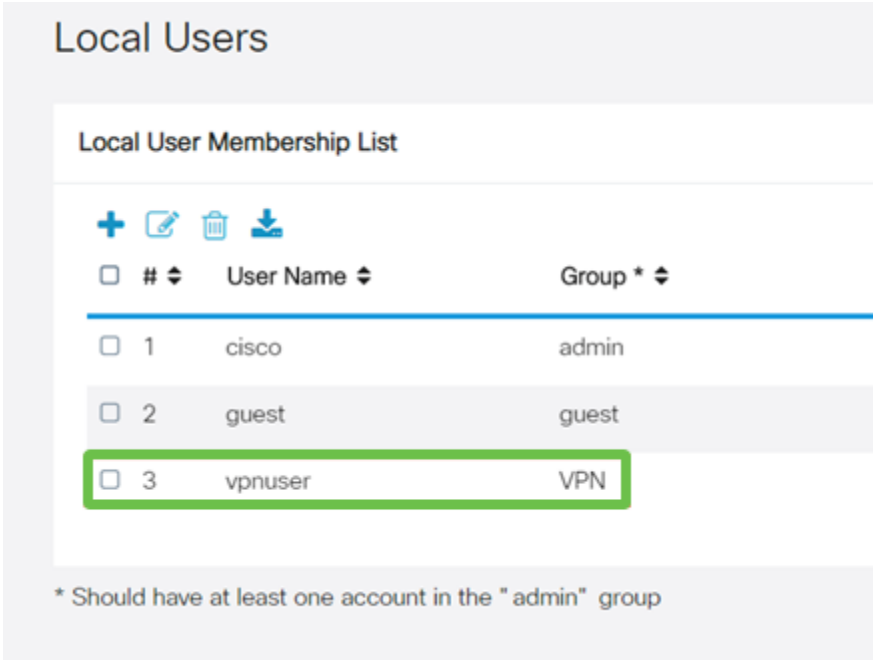
Paso 14

Introduzca el nuevo **nombre de usuario** junto con la **nueva contraseña**. Verifique que el **grupo** esté configurado en el nuevo **grupo de usuarios** que acaba de configurar. Haga clic en **Aplicar** cuando haya terminado.



Paso 15

El nuevo **Usuario** aparecerá en la lista de **Usuarios Locales**.



Esto completa la configuración en el RV345P Series Router. A continuación, configurará el cliente Shrew Soft VPN.

Configuración del cliente de Shrew Soft VPN

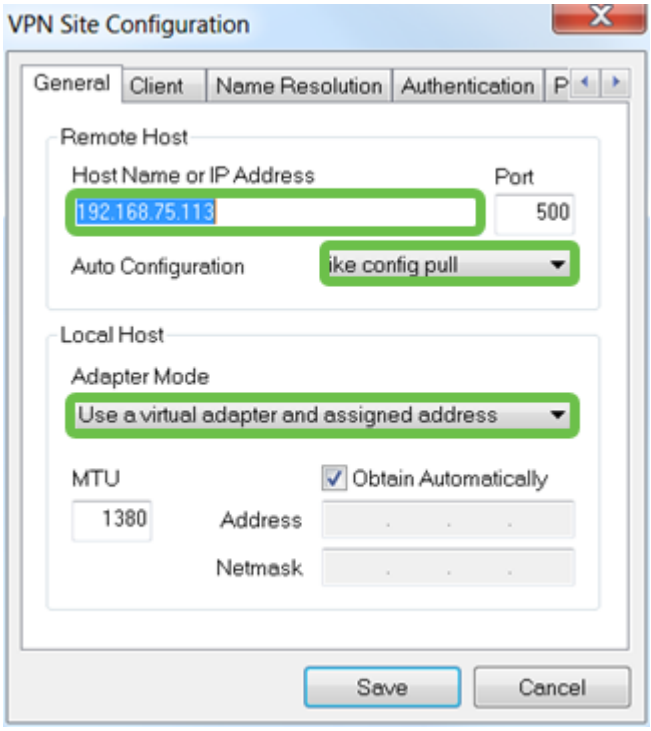
Siga los pasos descriptos a continuación.

Paso 1

Abra el *administrador de acceso VPN* de software de Cisco y haga clic en **Agregar** para agregar un perfil. En la ventana *VPN Site Configuration* que aparece, configure la **ficha General**:

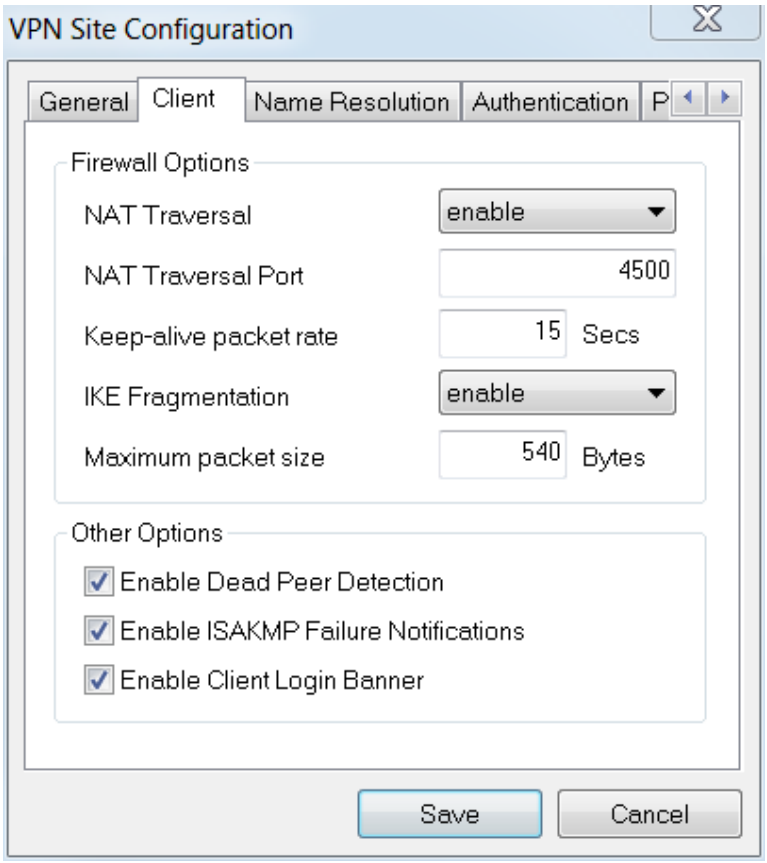
- **Nombre de host o dirección IP**: Utilice la dirección IP de WAN (o el nombre de host del RV345P)

- **Configuración automática**: Seleccione **ike config pull**
- **Modo adaptador**: Seleccione **Usar un adaptador virtual y dirección asignada**



Paso 2

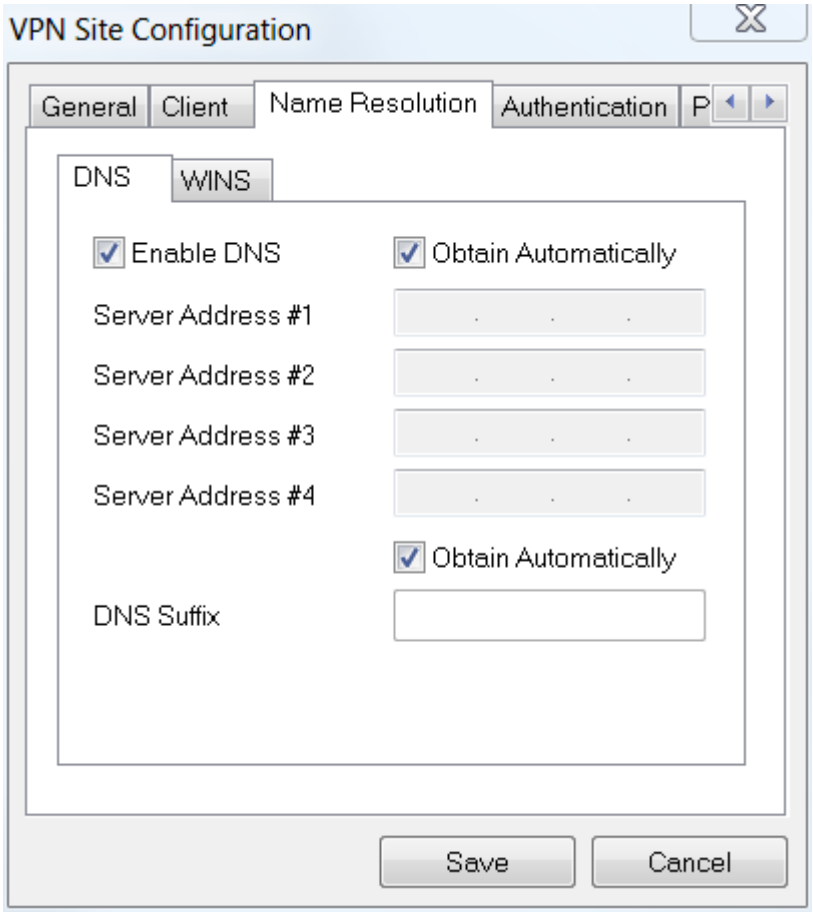
Configure la pestaña **Cliente**. En este ejemplo, conservamos la configuración predeterminada.



Paso 3

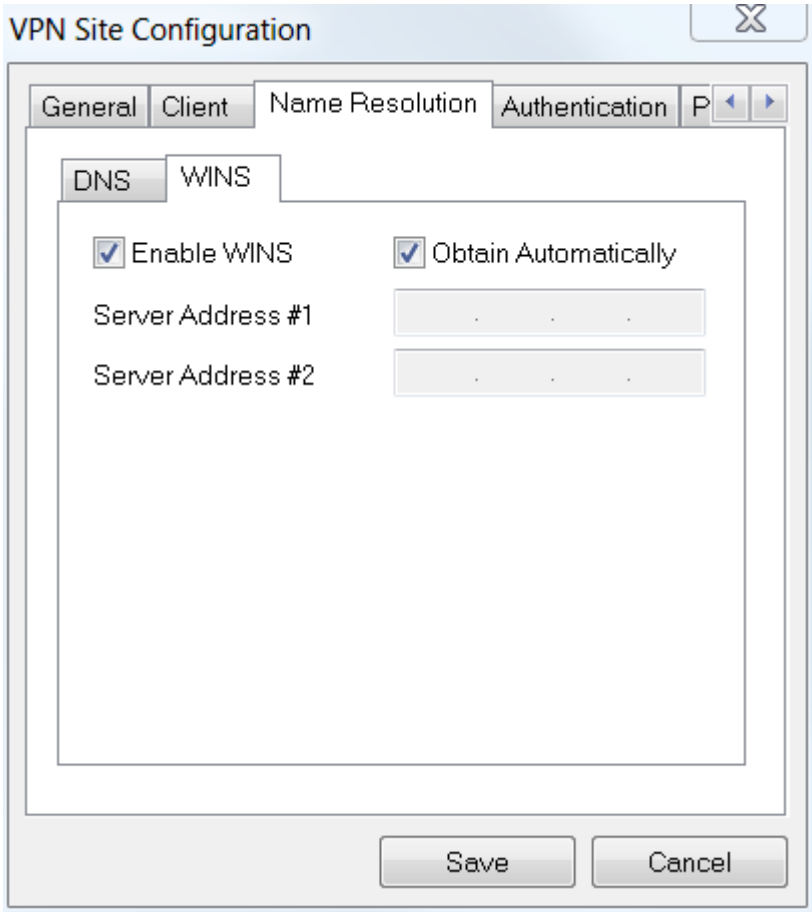
En **Resolución de nombres > DNS**, marque la casilla **Habilitar DNS** y deje las casillas

Obtener automáticamente marcadas.



Paso 4

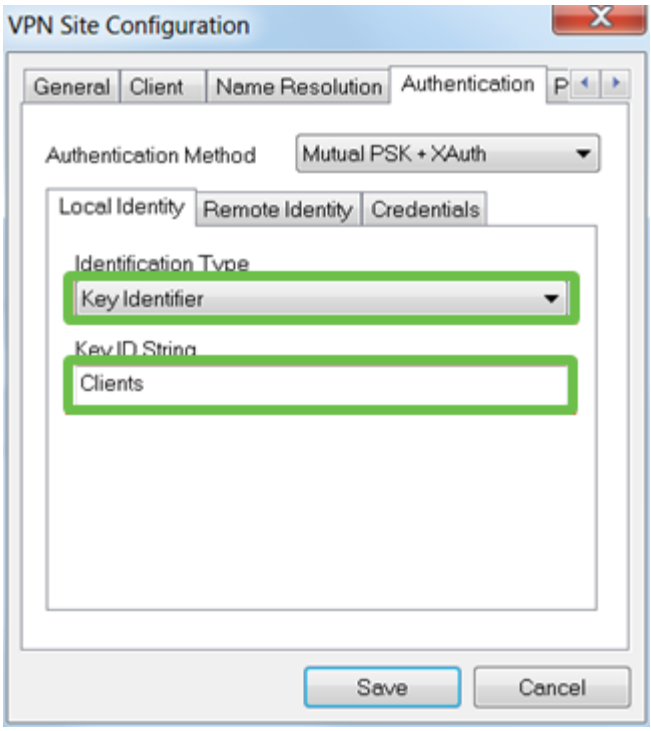
En **Resolución de nombres > ficha WINS**, active la casilla **Habilitar WINS** y deje la casilla **Obtener automáticamente** marcada.



Paso 5

Haga clic en **Authentication > Local Identity**.

- **Tipo de identificación**: Seleccionar **identificador de clave**
- **Cadena de ID de clave**: Introduzca el **nombre de grupo** configurado en el RV345P

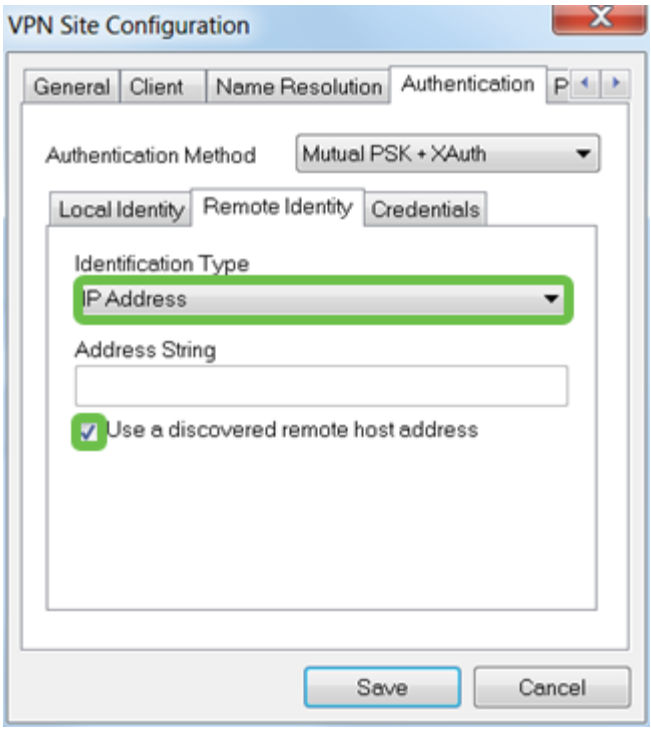


Paso 6

En **Authentication > Remote Identity**. En este ejemplo, conservamos la configuración

predeterminada.

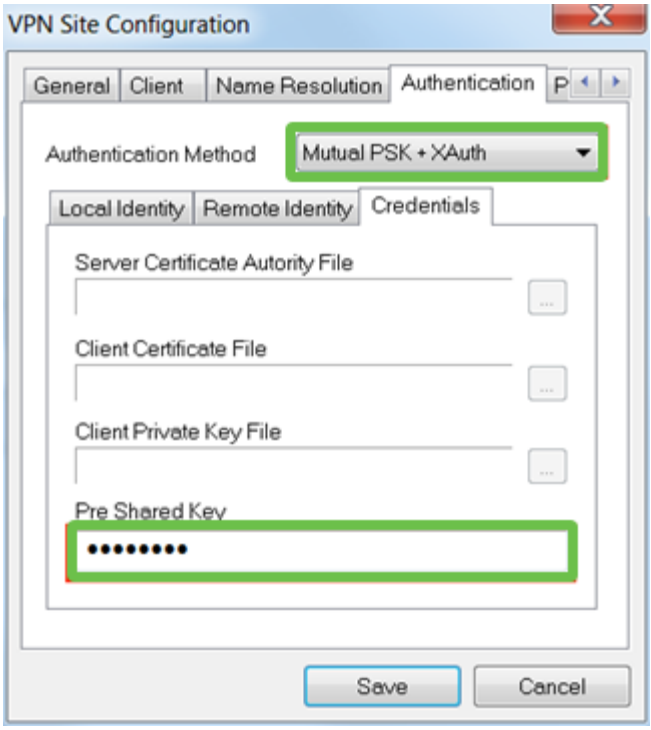
- **Tipo de identificación**: IP Address
- **Cadena de dirección**: <blank>
- **Utilice un** cuadro **de dirección de host remoto detectado**: Activado



Paso 7

En **Autenticación > Credenciales**, configure lo siguiente:

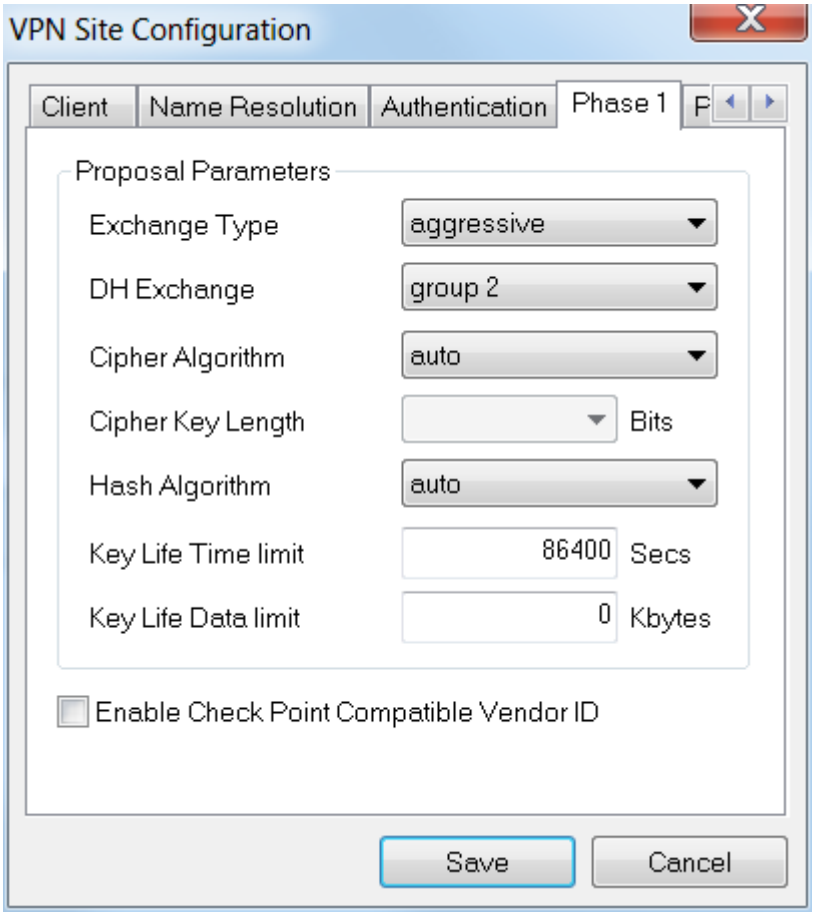
- **método de autentificación:** Seleccionar **PSK mutuo + XAuth**
- **Clave precompartida**: Introduzca la **clave precompartida** configurada en el perfil del cliente RV345P



Paso 8

Para la pestaña **Fase 1**. En este ejemplo, se conservaron los valores predeterminados:

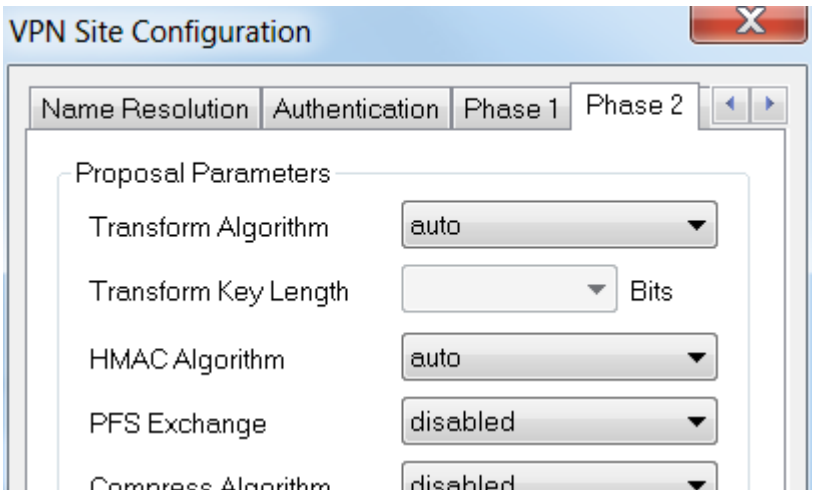
- **Tipo de intercambio:** Agresivo
- **Intercambio DH:** grupo 2
- **Algoritmo del cifrado:** Automático
- **Algoritmo hash:** Automático



Paso 9

En este ejemplo, los valores predeterminados de la ficha **Fase 2** se mantuvieron igual.

- **Algoritmo de transformación:** Automático
- **Algoritmo HMAC:** Automático
- **Intercambio PFS:** Desactivado
- **Comprimir algoritmo:** Desactivado

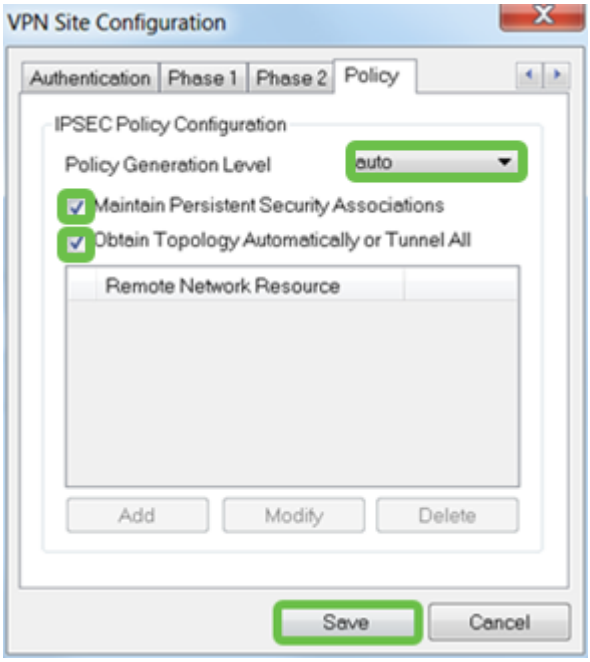


Paso 10

Para el ejemplo de la ficha **Policy**, utilizamos la siguiente configuración:

- **Nivel de generación de políticas:** Automático
- **Mantener asociaciones de seguridad persistentes:** Activado
- **Obtener topología automáticamente o Túnel todo:** Activado

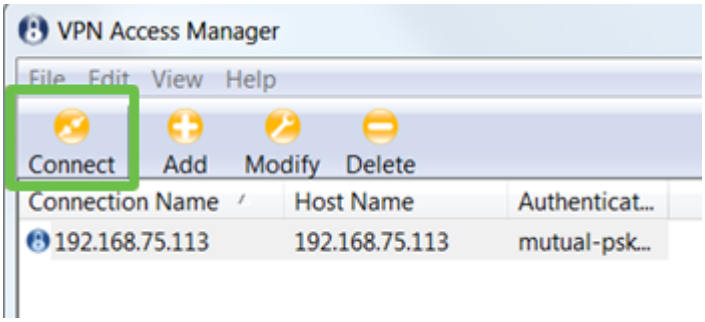
Ya que configuramos la **tunelización dividida** en el RV345P, no necesitamos configurarlo aquí.



Cuando haya terminado, haga clic en Guardar.

Paso 11

Ya está listo para probar la conexión. En *VPN Access Manager*, resalte el perfil de conexión y haga clic en el **botón Connect**.

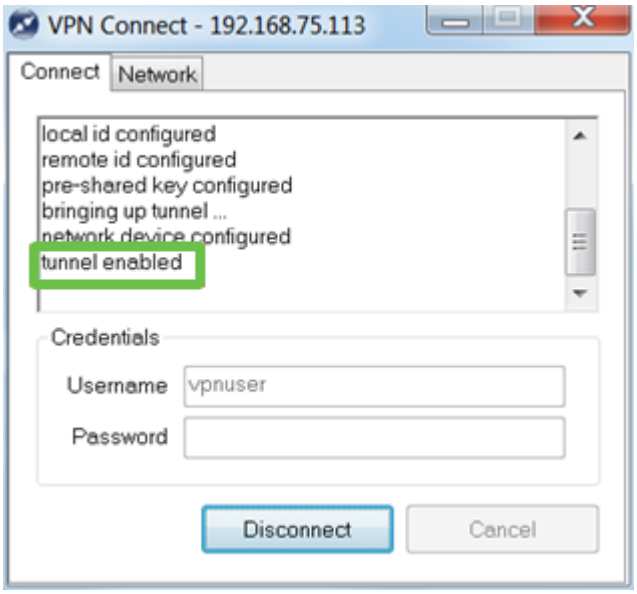


Paso 12

En la ventana **VPN Connect** que aparece, ingrese el **nombre de usuario** y la **contraseña** usando las credenciales para la **cuenta de usuario** que creó en el RV345P (pasos 13 y 14). Cuando haya terminado, haga clic en **Connect**.

Paso 13

Verifique que el túnel esté conectado. Debería ver **túnel habilitado**.



Shrew Soft se utilizó como ejemplo en esta configuración. Puesto que Shrew Soft no es un producto de Cisco, póngase en contacto con este tercero si necesita asistencia técnica.

Otras opciones de VPN

Hay otras opciones para utilizar una VPN. Haga clic en los siguientes enlaces para obtener más información:

- Utilice el cliente VPNGreenBow para conectarse con el router serie RV34x
- Configuración de un cliente VPN de teletrabajador en el router serie RV34x
- Configuración de un servidor de protocolo de túnel punto a punto (PPTP) en el router serie Rv34x
- Configuración de un perfil de seguridad de protocolo de Internet (IPsec) en un router serie RV34x

- Configuración de los parámetros de WAN L2TP en el router RV34x
- Configuración de VPN de sitio a sitio en el RV34x

Configuraciones adicionales en el router RV345P

Configuración de VLAN (opcional)

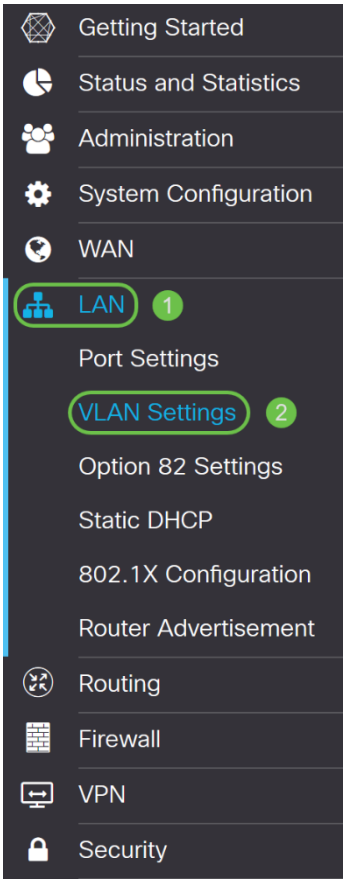
Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En los escenarios donde los datos confidenciales se pueden difundir en una red, se pueden crear VLAN para mejorar la seguridad mediante la designación de una transmisión 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.

Puede consultar Prácticas recomendadas y consejos de seguridad de VLAN para obtener orientación adicional.

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

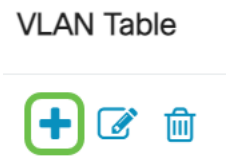
Paso 1

Vaya a **LAN > VLAN Settings**.



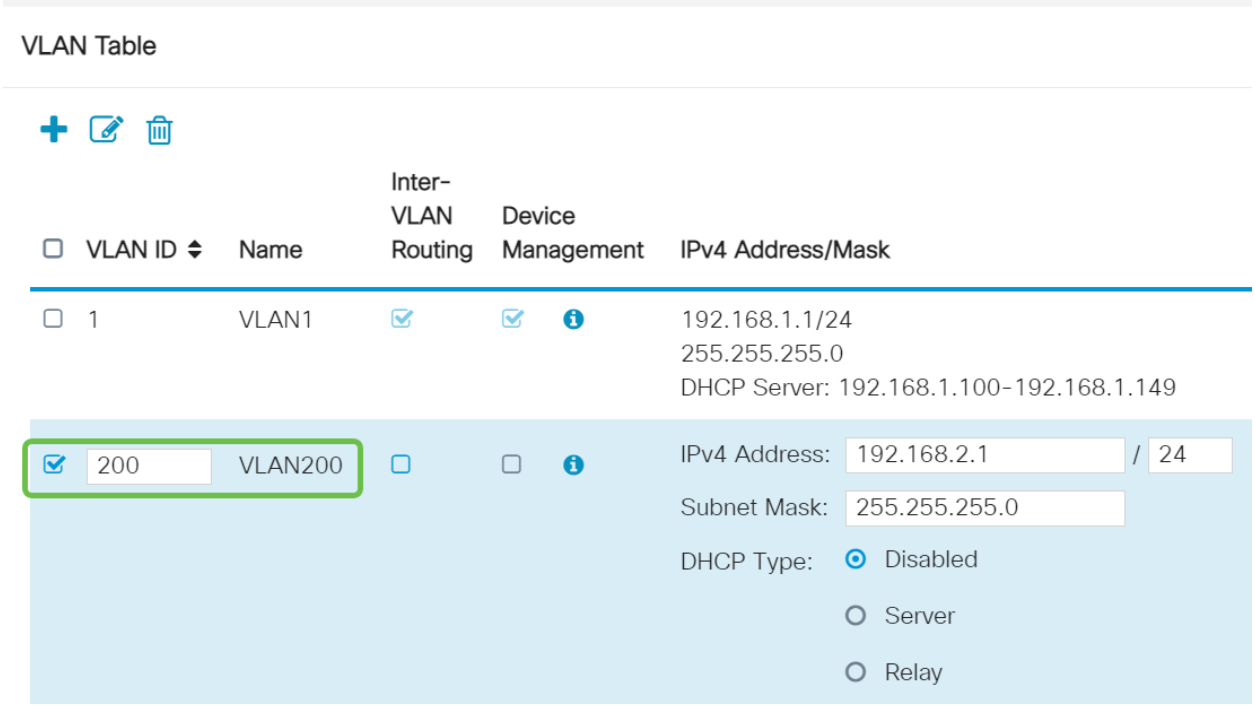
Paso 2

Haga clic en el **icono Add** 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.



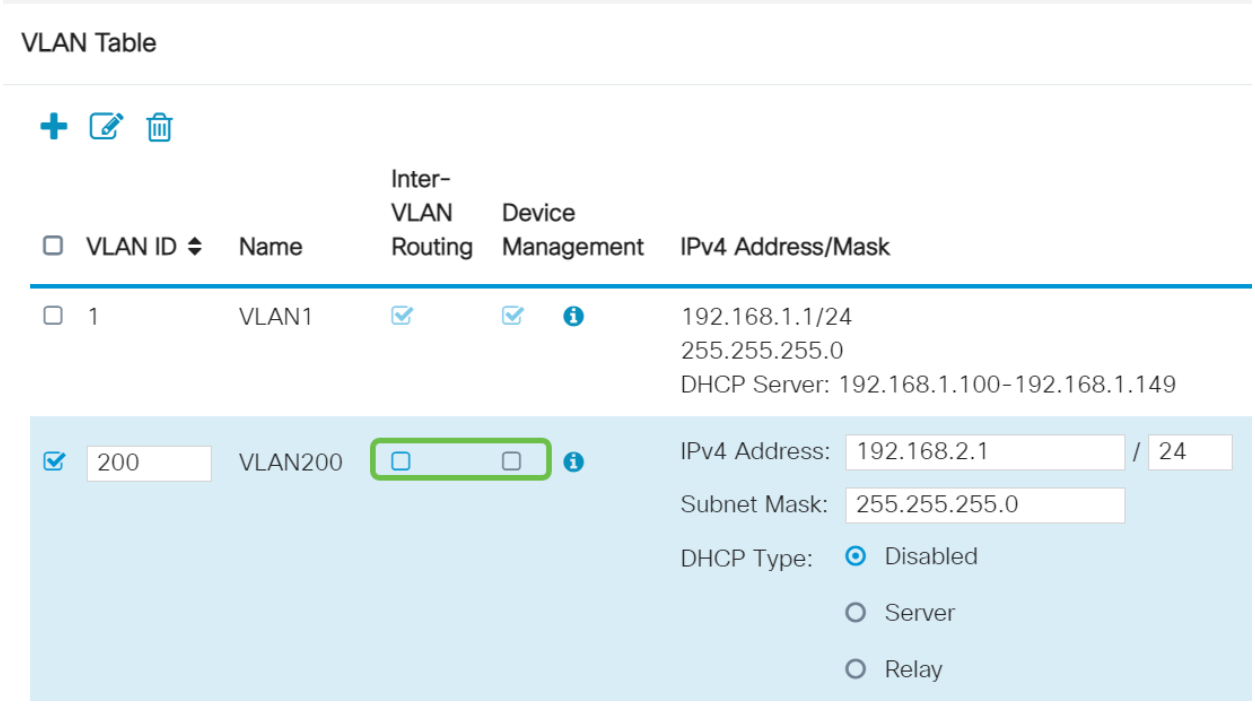
Paso 4

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.

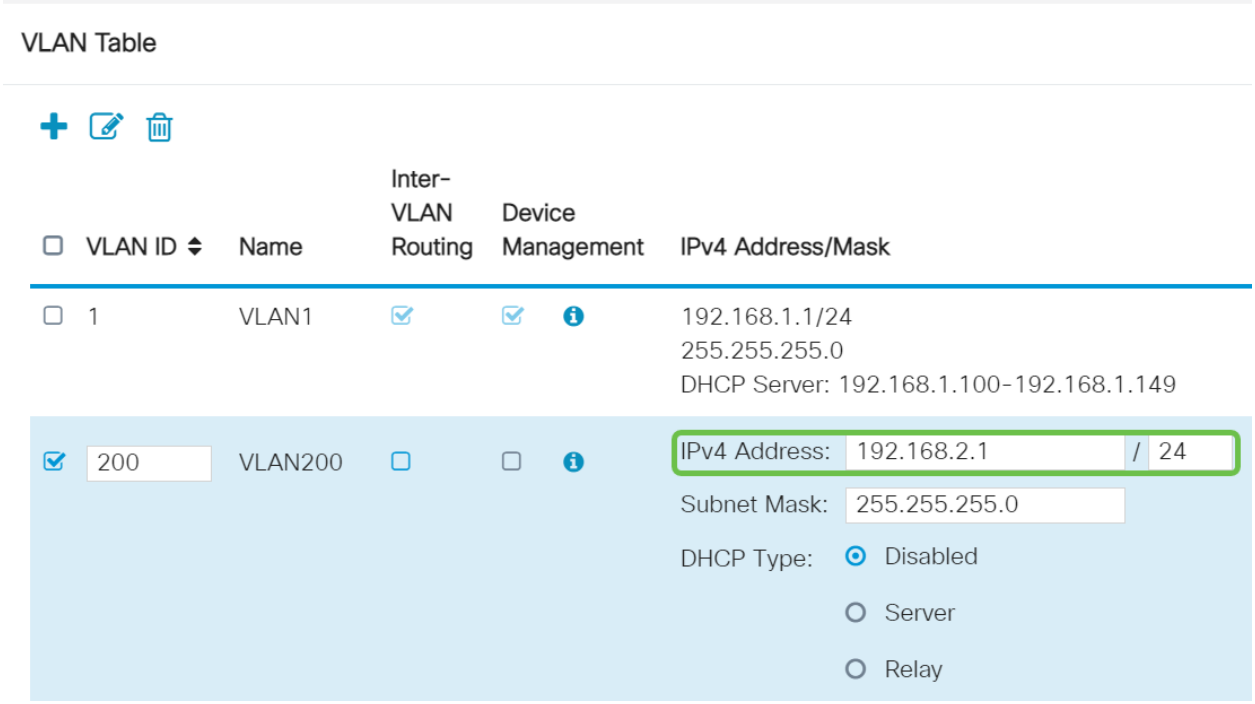
Device Management es el software que permite utilizar el explorador para iniciar sesión en la interfaz de usuario web del RV345P, desde la VLAN y administrar el RV345P. Esto también debe desactivarse en las redes de invitado.

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



Paso 5

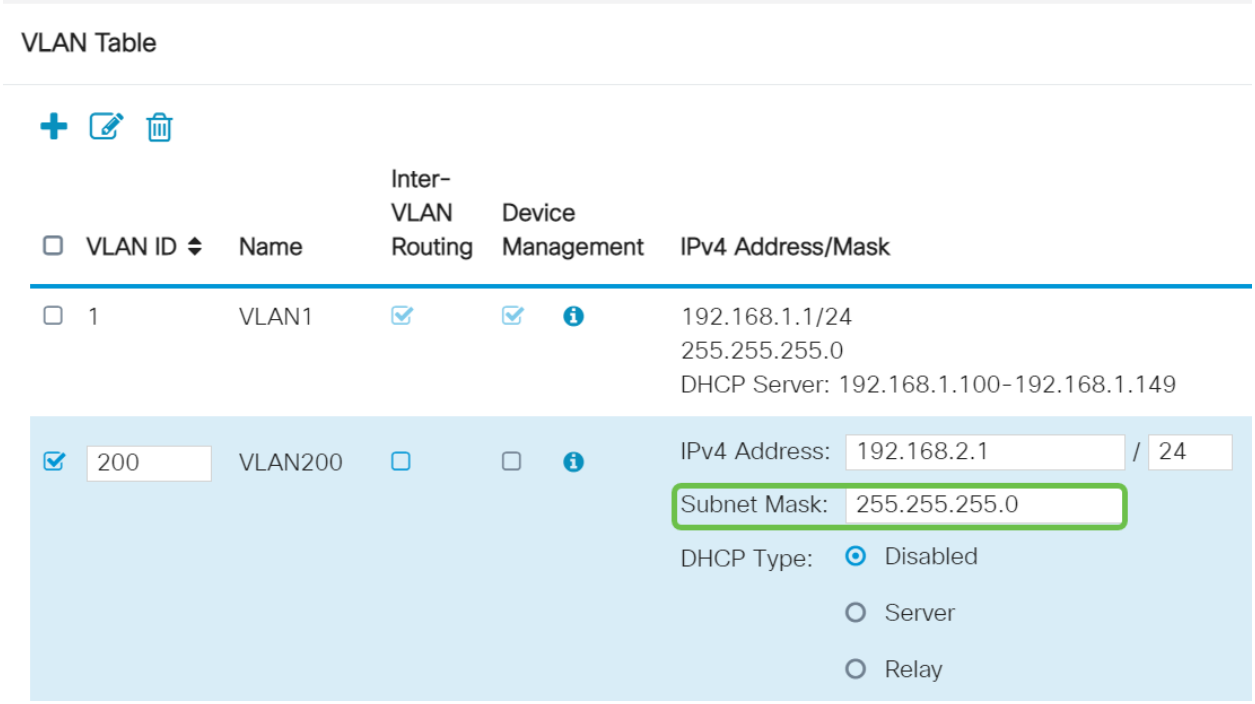
La dirección IPv4 privada se rellenará automáticamente en el campo *Dirección IP*. Puede ajustar esto si lo desea. En este ejemplo, la subred tiene direcciones IP 192.168.2.100-192.168.2.149 disponibles para DHCP. 192.168.2.1-192.168.2.99 y 192.168.2.150-192.168.2.254 están disponibles para las direcciones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



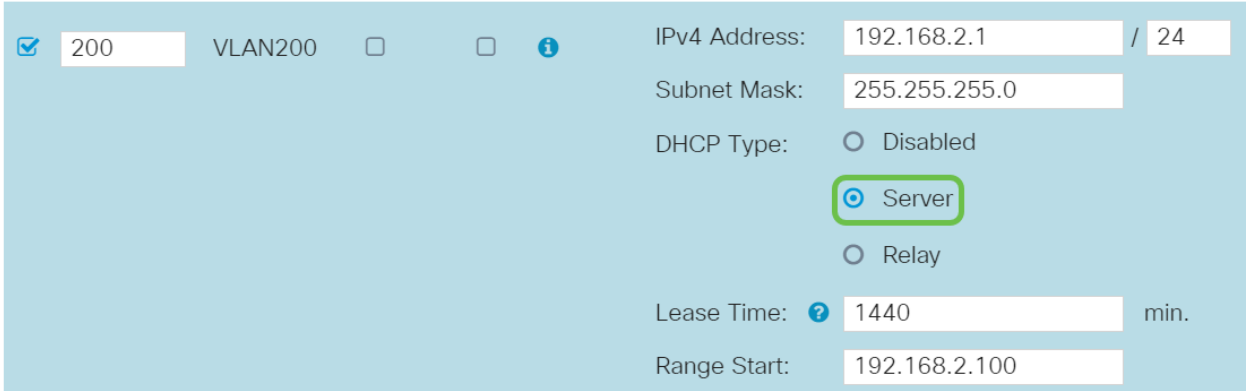
Paso 7

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.

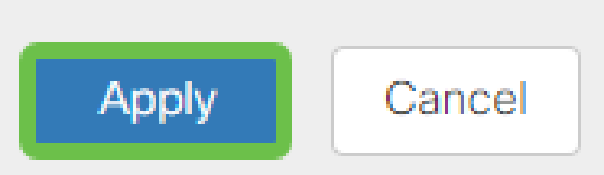
Servidor: esta es la opción más utilizada.

- 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.



Asignación de VLAN a puertos (opcional)

Se pueden configurar 16 VLAN en el RV345P, 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 trunking permite que una VLAN nativa esté sin etiquetar. Las VLAN que no desee en el tronco 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:

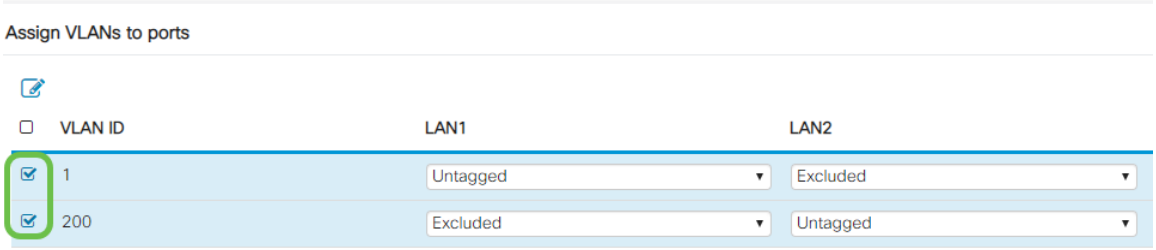
- Se considera un puerto troncal.
- Una de las VLAN se puede etiquetar como Sin etiquetar.
- El resto de las VLAN que forman parte del puerto troncal deben etiquetarse como Etiquetadas.
- Las VLAN que no forman parte del puerto troncal deben etiquetarse como Excluidas para ese puerto.

En este ejemplo, no hay troncales.

Paso 1

Seleccione los *IDs de VLAN* que desea editar.

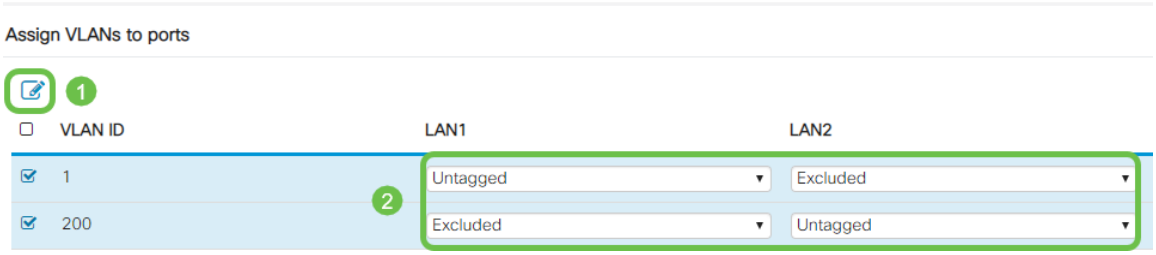
En este ejemplo, hemos seleccionado *VLAN 1* y *VLAN 200*.



Paso 2

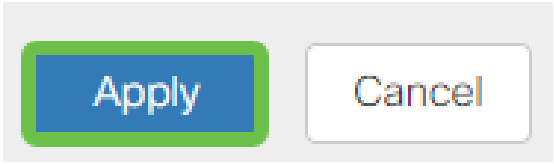
Haga clic en **Editar** para asignar una VLAN a un puerto LAN y especificar cada configuración como *Etiquetado*, *Sin etiquetar* o *Excluido*.

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 3

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



Ahora debería haber creado correctamente una nueva VLAN y configurado VLAN en los puertos del RV345P. 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.

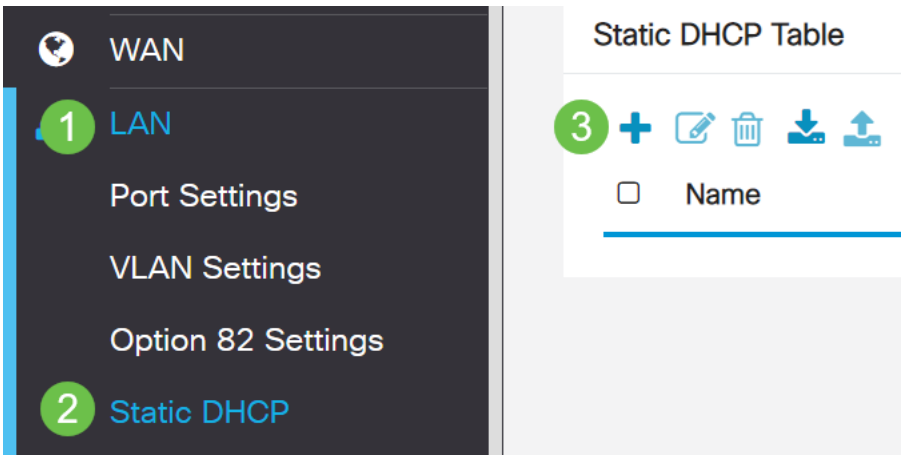
Agregar una IP estática (opcional)

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.

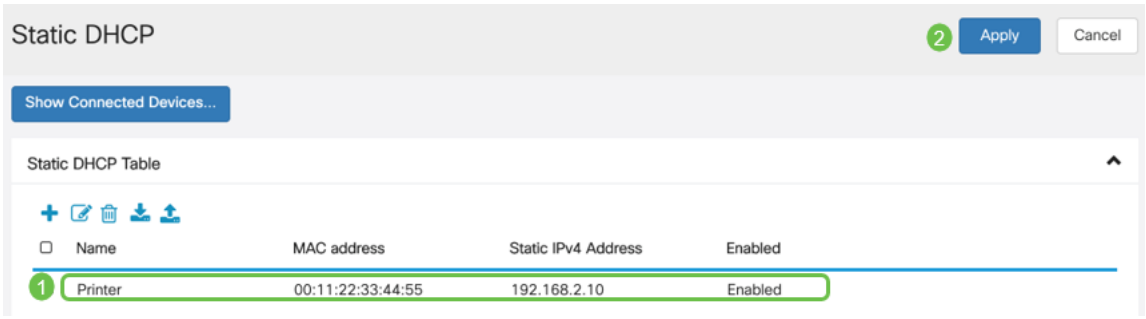
Paso 1

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.



Administración de certificados (opcional)

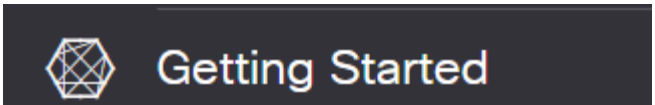
Un certificado digital certifica la propiedad de una clave pública por el sujeto designado del certificado. Esto permite que las partes que confían en ellas dependan de las firmas o afirmaciones hechas por la clave privada que corresponde a la clave pública certificada. Un router puede generar un certificado autofirmado, un certificado creado por un administrador de red. También puede enviar solicitudes a las autoridades de certificación (CA) para solicitar un certificado de identidad digital. Es importante disponer de certificados legítimos de aplicaciones de terceros.

Se utiliza una autoridad certificadora (CA) para la autenticación. Los certificados se pueden adquirir en cualquier número de sitios de terceros. Es una manera oficial de probar que su sitio es seguro. Básicamente, la CA es una fuente de confianza que verifica que usted es una empresa legítima y de confianza. Según sus necesidades, un certificado a un coste mínimo. La CA le desprotege y, una vez que verifiquen su información, le emitirán el certificado. Este certificado se puede descargar como un archivo en su equipo. A continuación, puede ir al router (o al servidor VPN) y cargarlo allí.

Generar CSR/Certificado

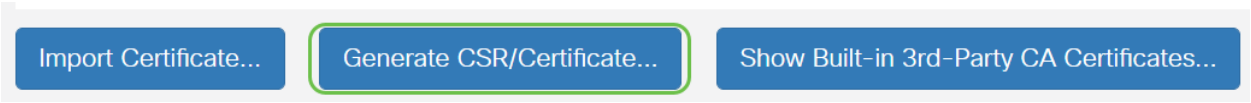
Paso 1

Inicie sesión en la utilidad basada en web del router y elija **Administration > Certificate**.



Paso 2

Haga clic en **Generar CSR/Certificado**. Accederá a la página Generar CSR/Certificado.



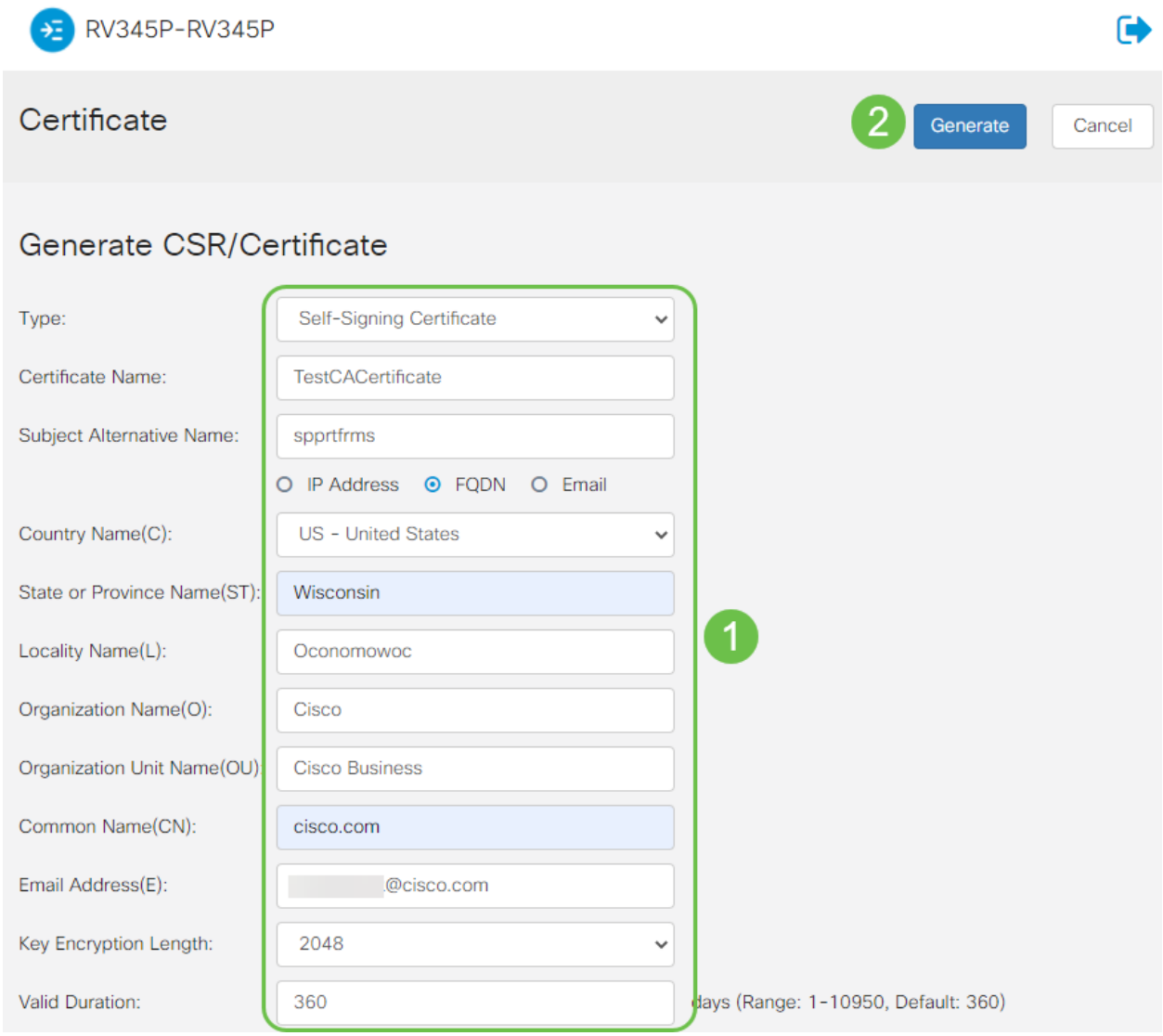
Paso 3

Rellene los cuadros con lo siguiente:

- Elija el tipo de certificado adecuado
    - Certificado de firma automática: este es un certificado de capa de socket seguro (SSL) firmado por su propio creador. Este certificado es menos confiable, ya que no se puede cancelar si la clave privada está comprometida de alguna manera por un atacante.
    - Solicitud de firma certificada: se trata de una infraestructura de clave pública (PKI) que se envía a la autoridad certificadora para solicitar un certificado de identidad digital. Es más seguro que autofirmado, ya que la clave privada se mantiene en secreto.
- Introduzca un nombre para el certificado en el campo Nombre de certificado para identificar la solicitud. Este campo no puede estar en blanco ni contener espacios ni caracteres especiales.
- (Opcional) En el área Nombre alternativo del sujeto, haga clic en un botón de opción. Las opciones son:
    - Dirección IP: introduzca una dirección de protocolo de Internet (IP)
    - FQDN: introduzca un nombre de dominio completo (FQDN)
    - Correo electrónico: introduzca una dirección de correo electrónico
- En el campo Subject Alternative Name (Nombre alternativo del asunto), introduzca el FQDN.
- Elija un nombre de país en el que su organización esté registrada legalmente en la lista desplegable Nombre de país.
- Introduzca un nombre o abreviatura del estado, provincia, región o territorio en el que se encuentra su organización en el campo Nombre de estado o provincia (ST).
- Introduzca un nombre de la localidad o ciudad en la que está registrada su organización o ubicada en el campo Nombre de localidad.
- Introduzca un nombre con el que se registre legalmente su empresa. Si se está inscribiendo como pequeña empresa o propietario exclusivo, introduzca el nombre del solicitante del certificado en el campo Organization Name (Nombre de la organización). No se pueden utilizar caracteres especiales.
- Introduzca un nombre en el campo Organization Unit Name (Nombre de unidad de organización) para diferenciar las divisiones de una organización.
- Introduzca un nombre en el campo Nombre común. Este nombre debe ser el nombre de dominio completo del sitio web para el que utiliza el certificado.
- Introduzca la dirección de correo electrónico de la persona que desea generar el certificado.
- En la lista desplegable Key Encryption Length (Longitud de cifrado de la clave), elija una

longitud de clave. Las opciones son 512, 1024 y 2048. Cuanto mayor sea la longitud de la clave, más seguro será el certificado.

- En el campo Duración válida, introduzca el número de días que el certificado será válido. El valor predeterminado es 360.
- Haga clic en **Generar**.



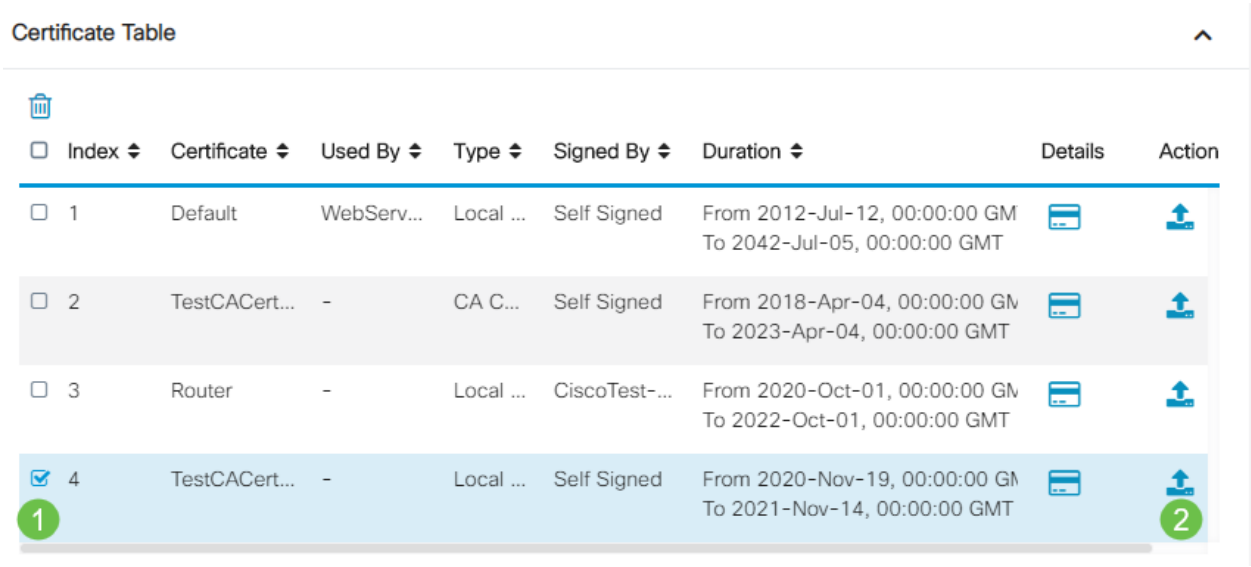
El certificado generado debe aparecer ahora en la tabla de certificados.

Ahora debería haber creado correctamente un certificado en el router RV345P.

Exportar un certificado

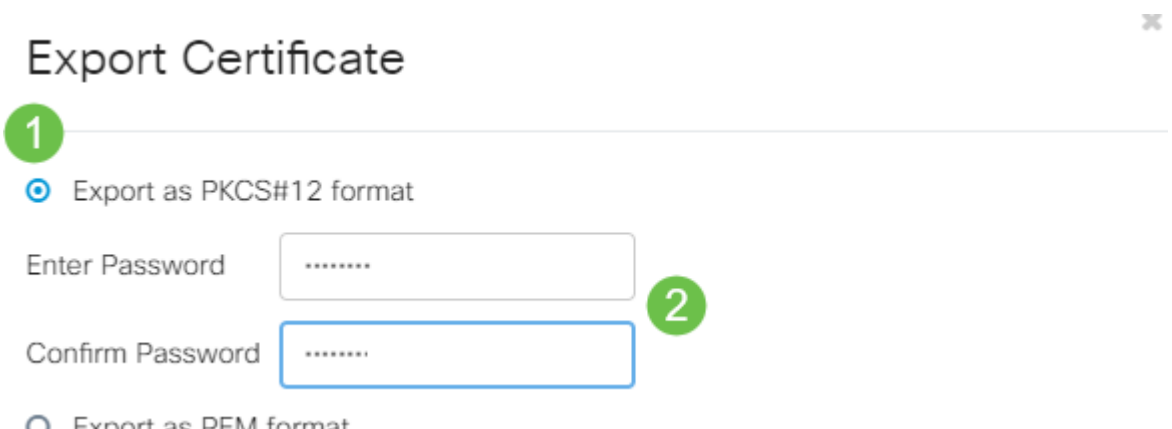
Paso 1

En la tabla de certificados, active la casilla del certificado que desea exportar y haga clic en el **icono de exportación**.



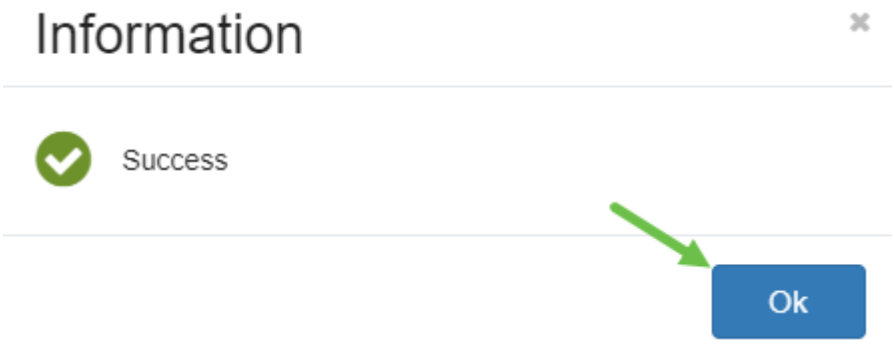
Paso 2

- Haga clic en un formato para exportar el certificado. Las opciones son:
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 es un certificado exportado que viene en una extensión .p12. Se requerirá una contraseña para cifrar el archivo para protegerlo a medida que se exporta, importa y elimina.
  - PEM: el correo mejorado de privacidad (PEM) se utiliza con frecuencia en los servidores web para que puedan traducirse fácilmente a datos legibles mediante un editor de texto simple, como el bloc de notas.
- Si selecciona PEM, haga clic en **Exportar**.
- Introduzca una contraseña para proteger el archivo que se va a exportar en el campo Introducir contraseña.
- Vuelva a introducir la contraseña en el campo Confirm Password (Confirmar contraseña).
- En el área Seleccionar destino, se ha seleccionado PC y es la única opción disponible actualmente.
- Haga clic en **Exportar**.



Paso 3

Debajo del botón Download (Descargar) aparecerá un mensaje que indica el éxito de la descarga. Un archivo comenzará a descargarse en el explorador. Click OK.

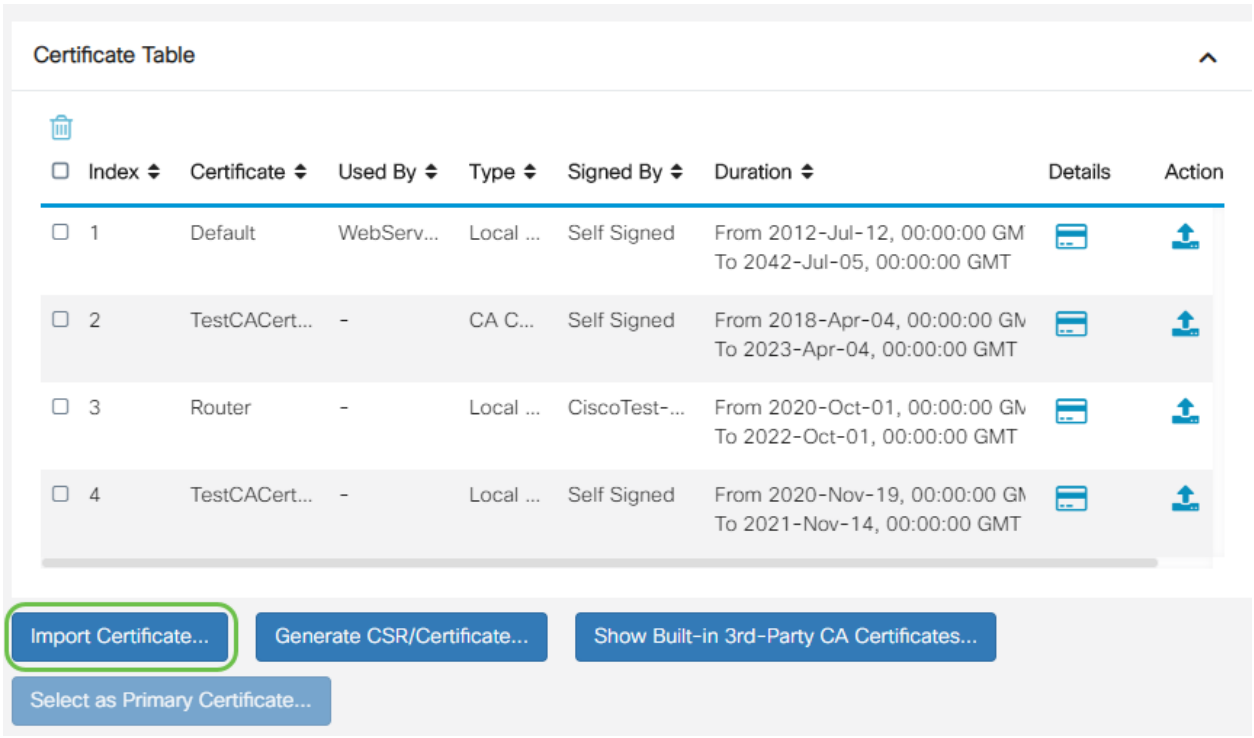


Ahora debería haber exportado correctamente un certificado en el router serie RV345P.

Importar un certificado

Paso 1

Haga clic en **Importar certificado...**.



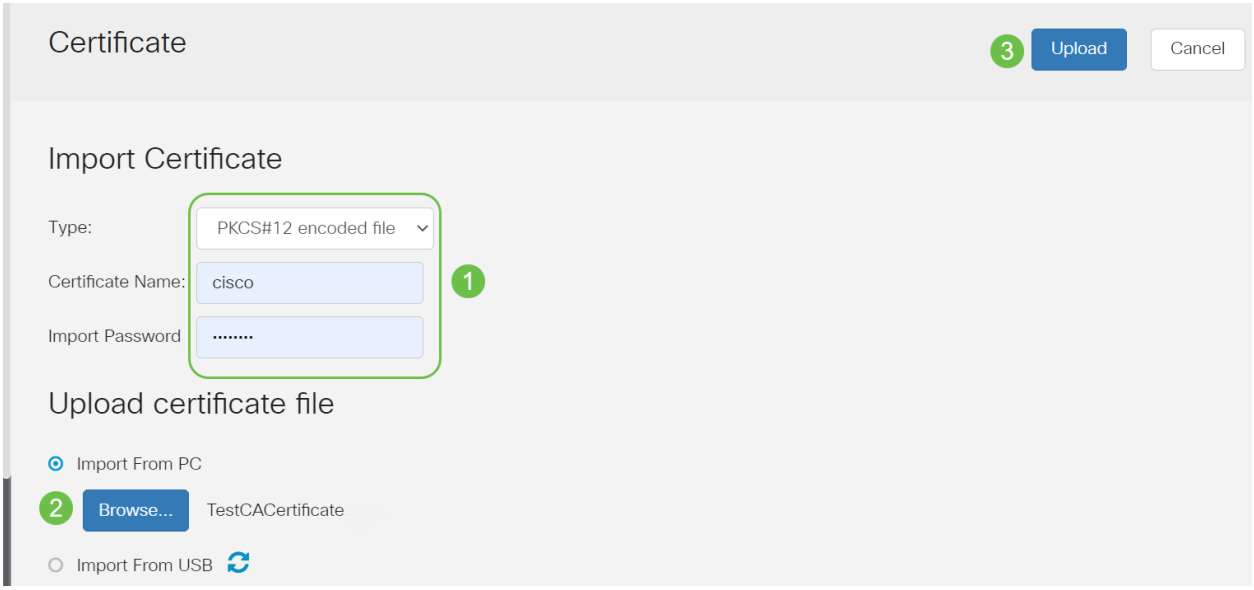
Paso 2

- Elija el tipo de certificado que desea importar en la lista desplegable. Las opciones son:
  - Certificado local: certificado generado en el router.
  - Certificado CA: certificado certificado certificado por una autoridad de terceros de confianza que ha confirmado que la información contenida en el certificado es exacta.
  - Archivo PKCS #12 codificado — Public Key Cryptography Standards (PKCS)

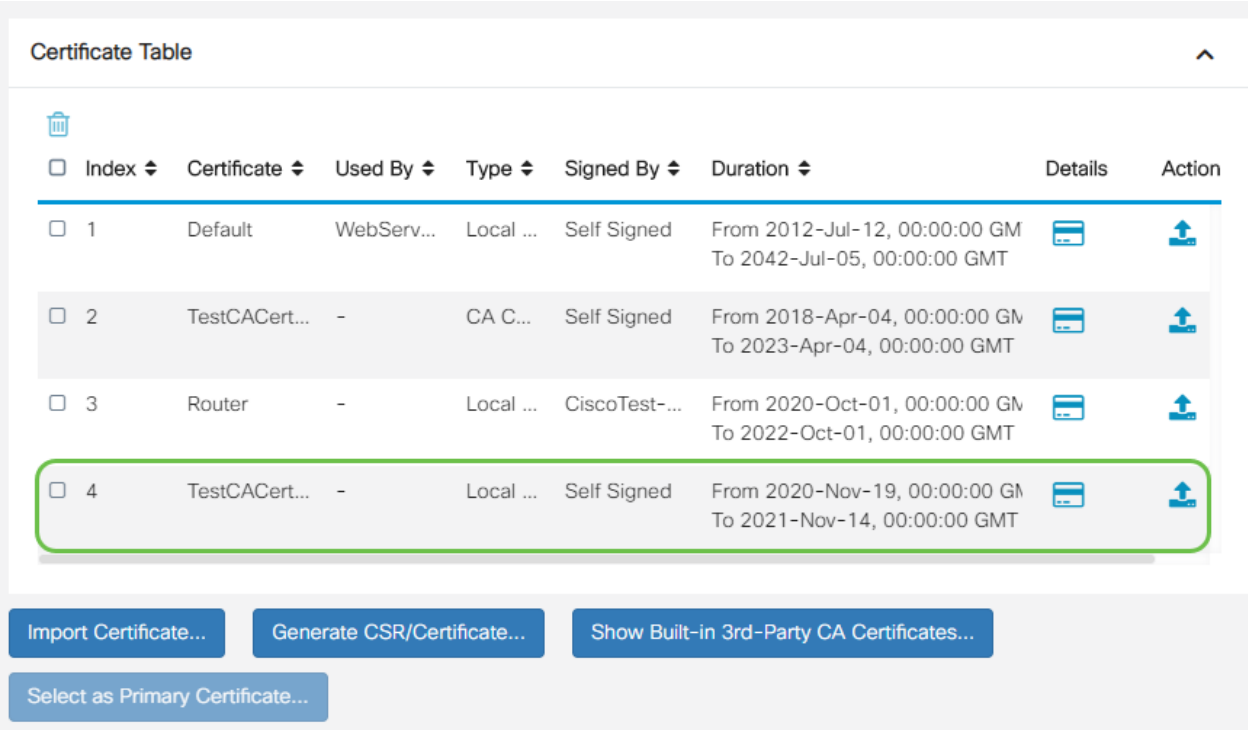
#12 es un formato para almacenar un certificado de servidor.

- Introduzca un nombre para el certificado en el campo Nombre del certificado.
- Si se eligió PKCS #12, introduzca una contraseña para el archivo en el campo Importar contraseña. Caso contrario, siga con el paso 3.
- Haga clic en un origen para importar el certificado. Las opciones son:
    - Importar desde PC
    - Importar desde USB

- Si el router no detecta una unidad USB, la opción Importar desde USB se atenuará.
- Si ha seleccionado Importar desde USB y el router no reconoce el USB, haga clic en Actualizar.
- Haga clic en el botón Choose File (Elegir archivo) y elija el archivo adecuado.
- Haga clic en Cargar.



Una vez realizado correctamente, se le llevará automáticamente a la página principal de certificados. La tabla de certificados se rellenará con el certificado recientemente importado.



Ahora debería haber importado correctamente un certificado en el router RV345P.

Configuración de una red móvil con un Dongle y un router serie RV345P (opcional)

Tal vez desee configurar una red móvil de respaldo usando un mecanismo de seguridad y su router RV345P. Si este es el caso, debe leer Configure a Mobile Network Using a Dongle and an RV34x Series Router.

Enhorabuena, ha completado la configuración del router RV345P. Ahora configurará los 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 RV345P. Los primeros 4 puertos del RV345P 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 RV345x.

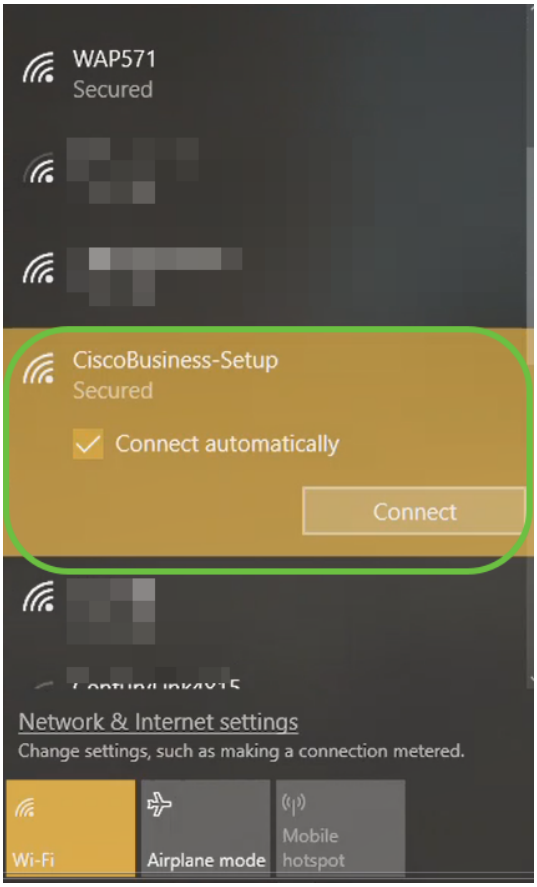
Configuración del punto de acceso inalámbrico primario 140AC en la interfaz de usuario web

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

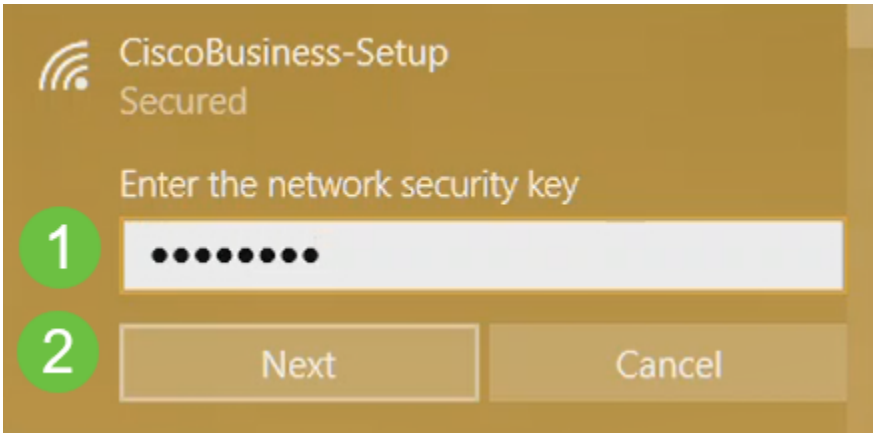
En el PC, haga clic en el **icono Wi-Fi** y elija la red inalámbrica *Cisco Business-Setup*. Haga clic en Connect (Conectar)



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.

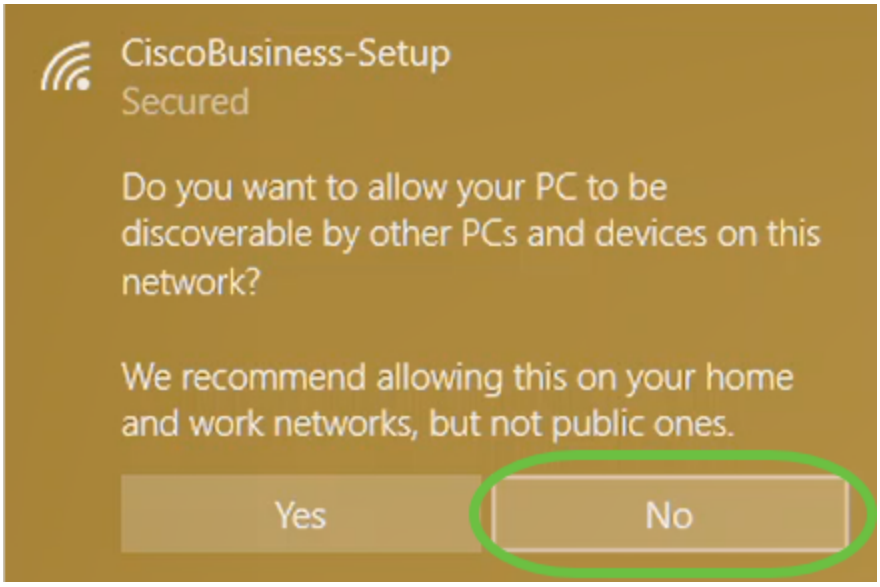
Paso 2

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



Paso 3

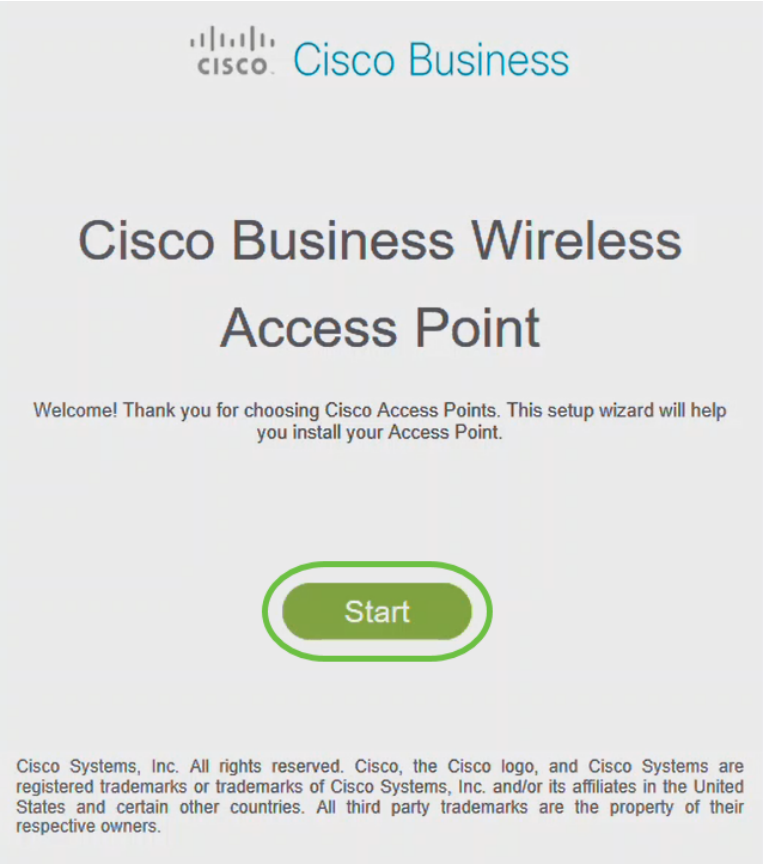
Aparecerá la siguiente pantalla. Dado que sólo puede configurar un dispositivo a la vez, haga clic en **No**.



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.

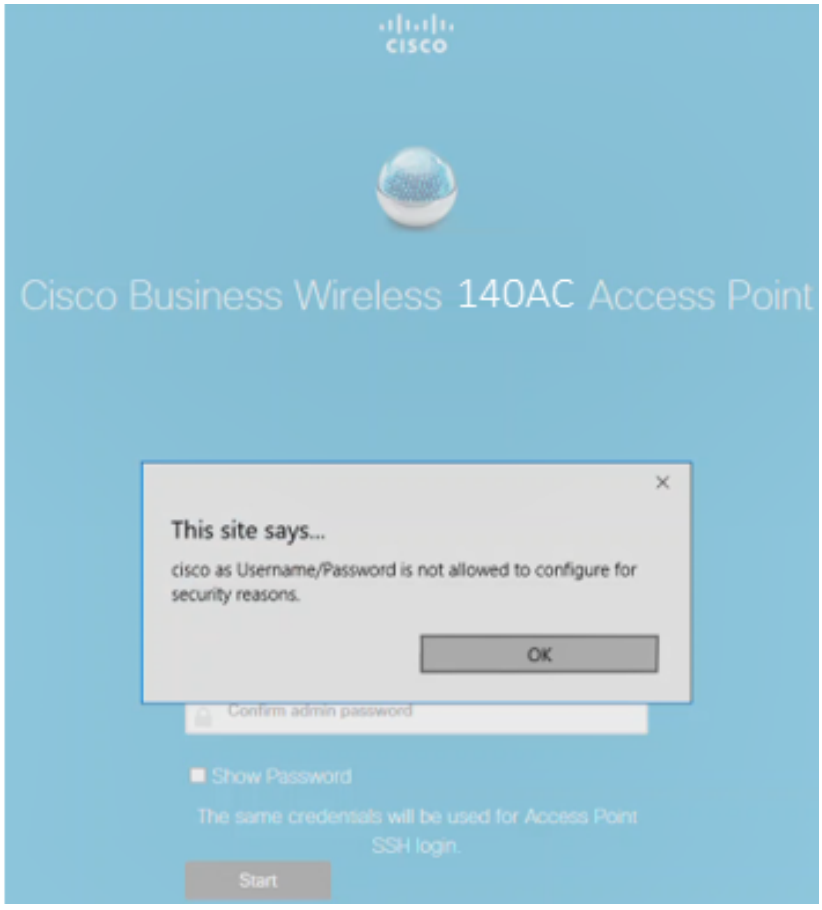
Paso 5

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.

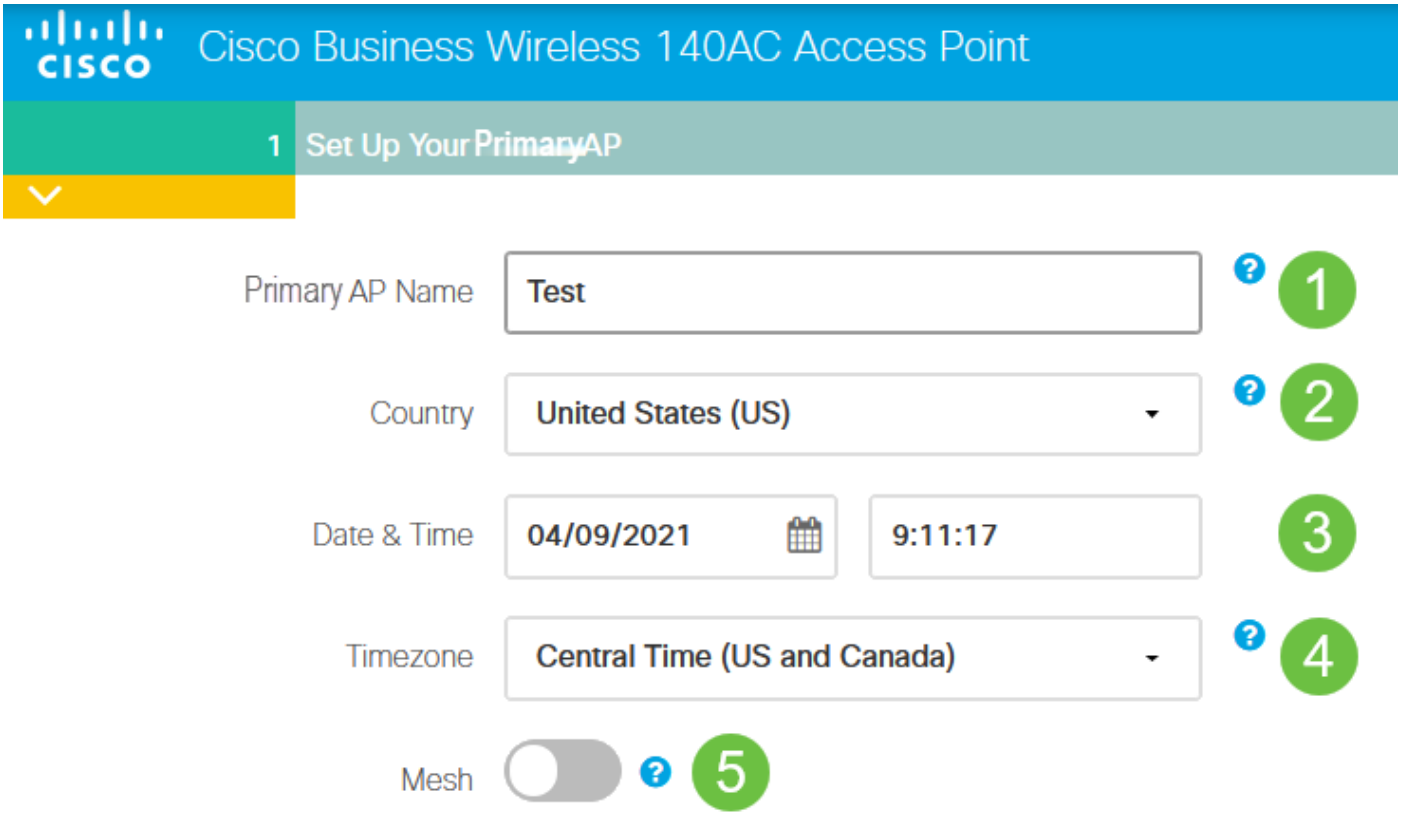


Paso 6

Configure su AP primario ingresando lo siguiente:

- Nombre del AP principal
- País

- Fecha y hora
- Zona horaria
- Malla



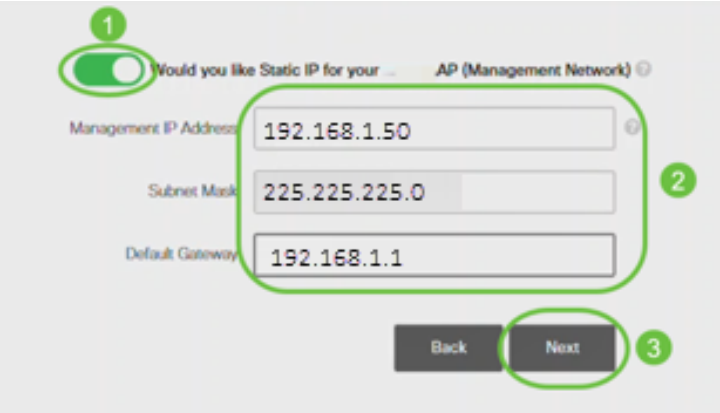
La malla sólo debe estar habilitada si planea crear una red de malla. De forma predeterminada, está desactivado.

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).



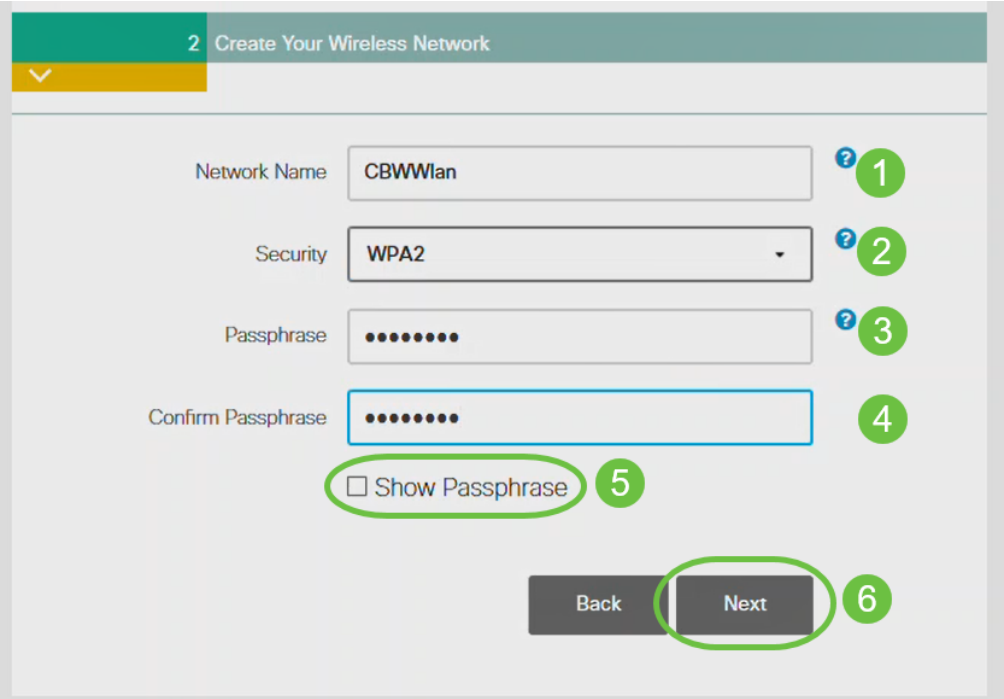
De forma predeterminada, esta opción está desactivada.

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.

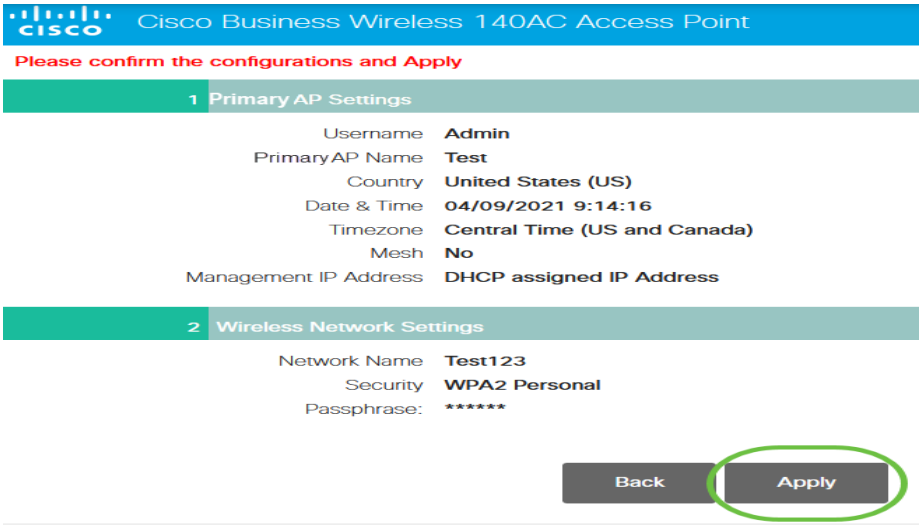
Haga clic en Next (Siguiente).



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

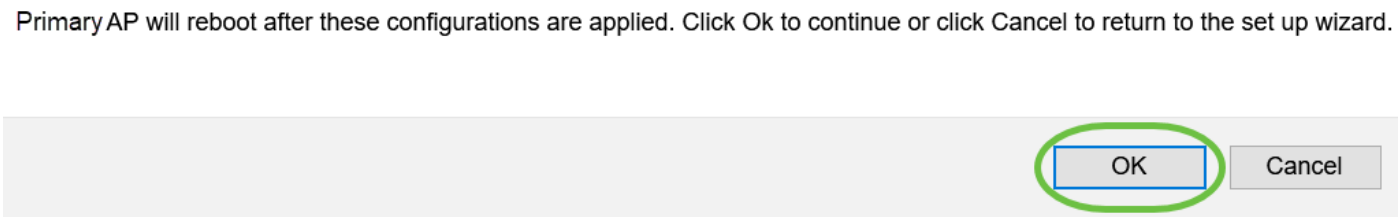
Paso 9

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

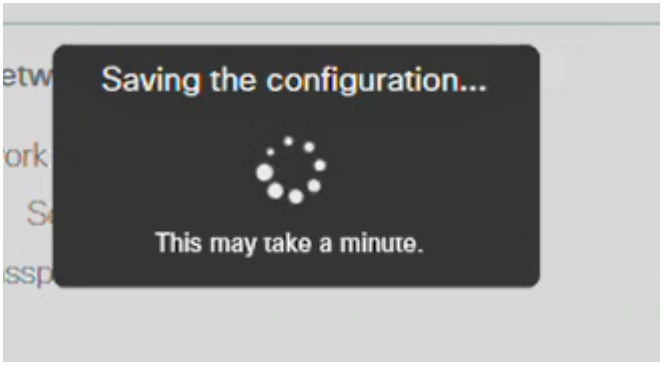


Paso 10

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.

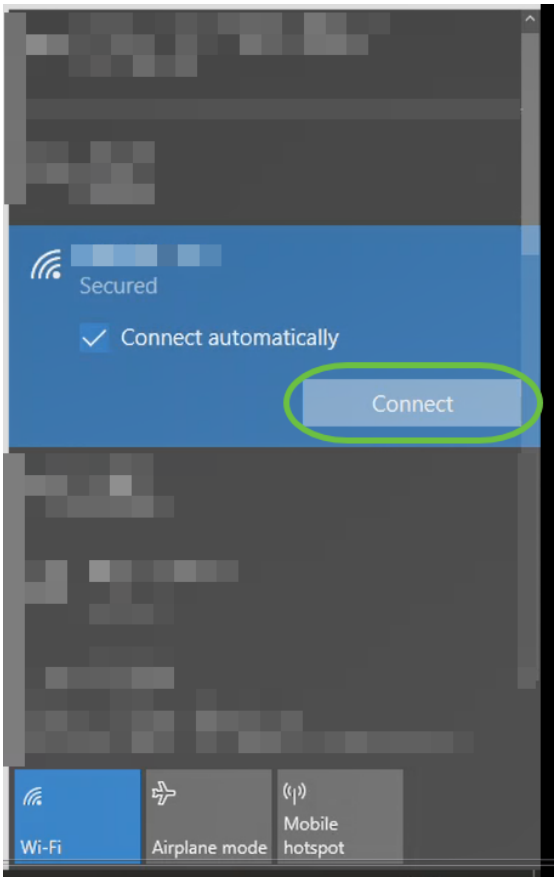


Durante el reinicio, la luz del punto de acceso pasará por varios patrones de color. Cuando la luz parpadee en verde, vaya al siguiente paso. Si la luz no supera el patrón rojo intermitente, indica que no hay ningún servidor DHCP en la red. Asegúrese de que el AP esté conectado a un switch o un router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

Paso 11

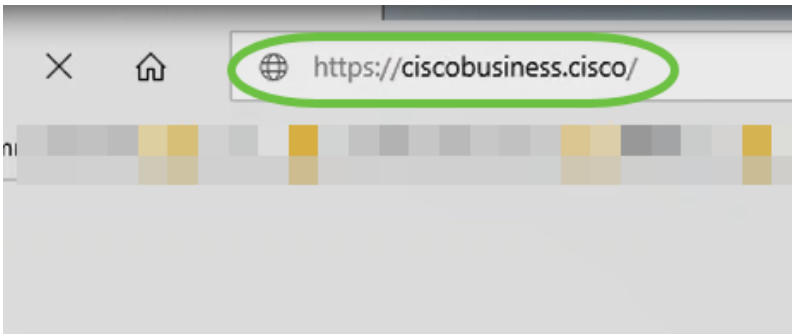
Vaya a las opciones inalámbricas del PC y elija la red que ha configurado. Haga clic en Connect (Conectar)

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.



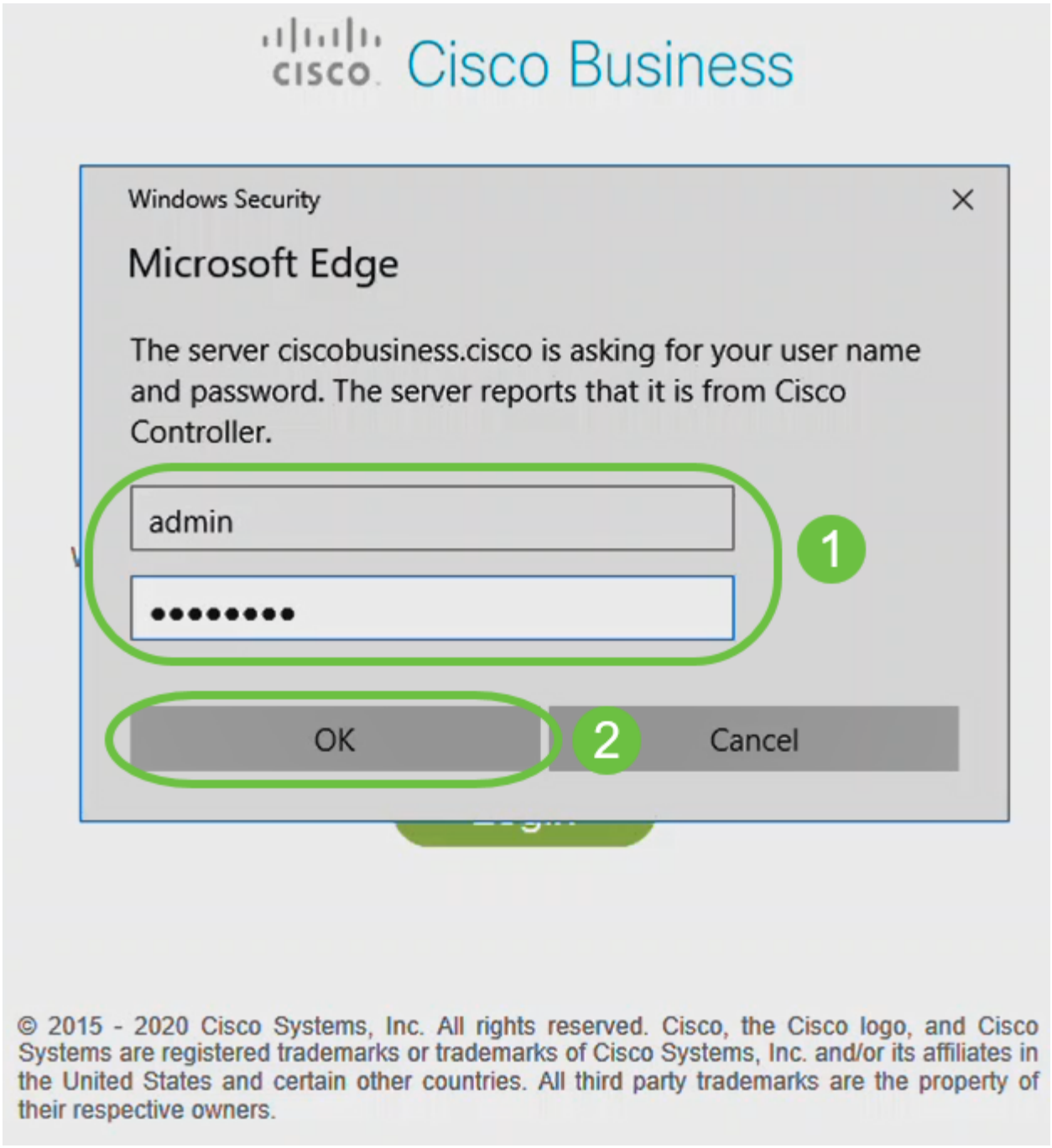
Asegúrese de escribir *https* y no *http* en este paso.

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

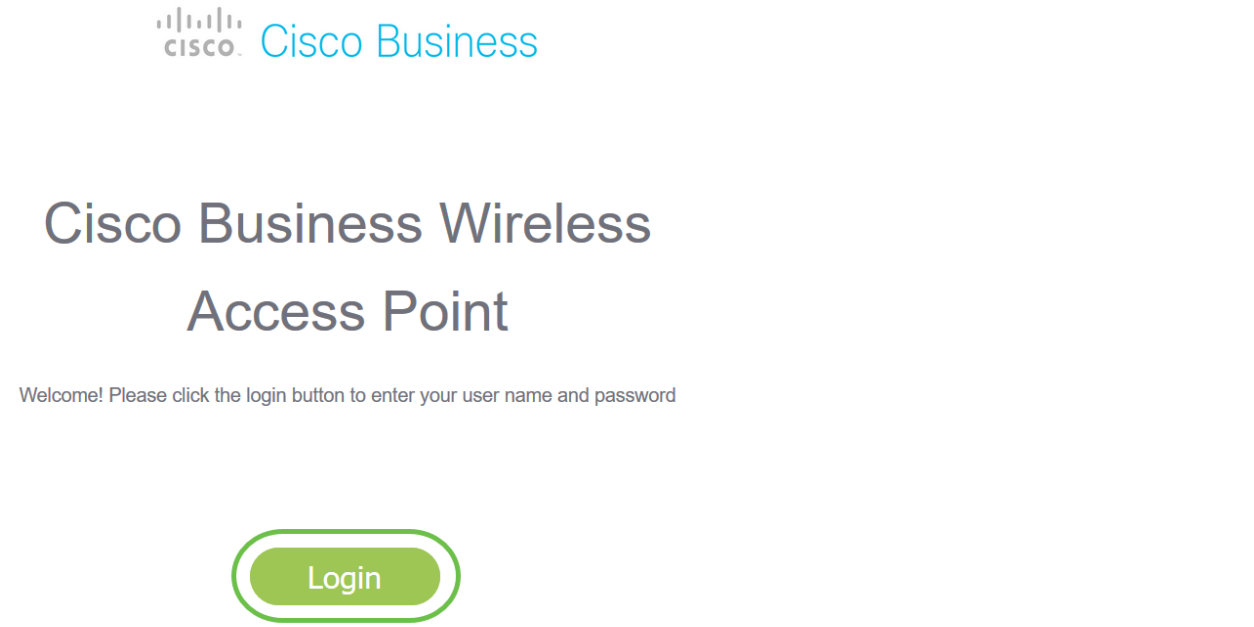
Conecte los dos ampliadores de malla a la pared en las ubicaciones que haya seleccionado. Anote la dirección MAC de cada extensor de malla.

Paso 2

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

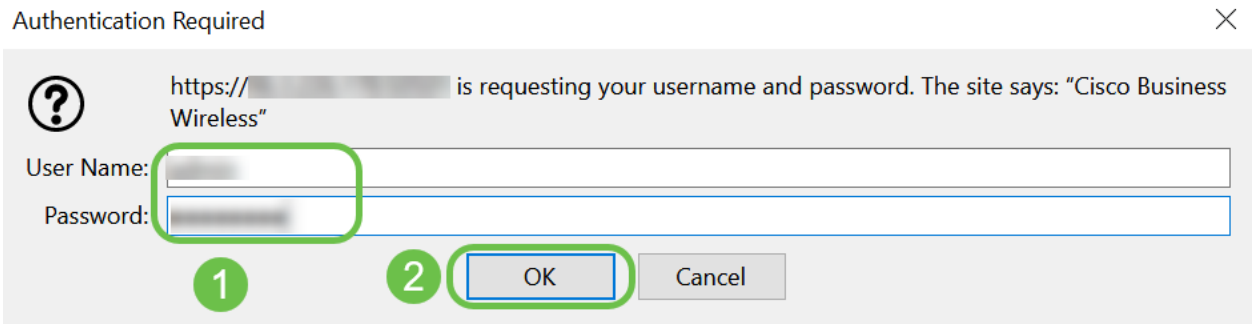
Paso 3

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



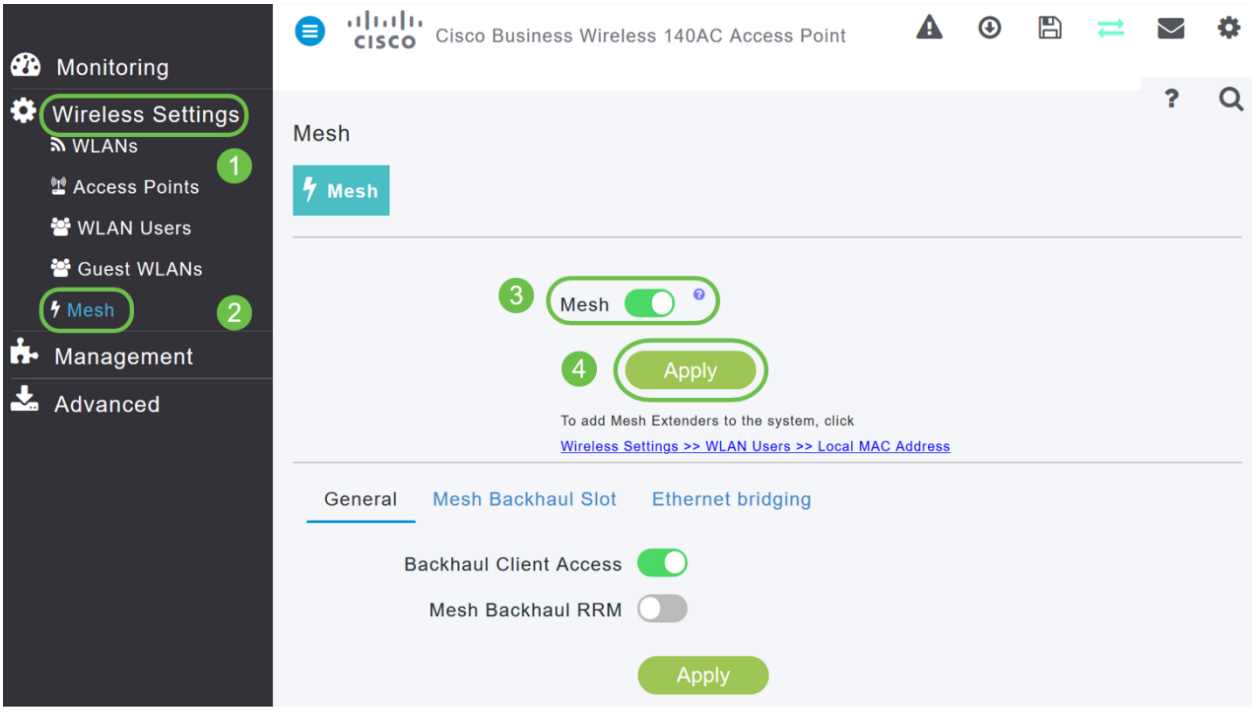
Paso 4

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).

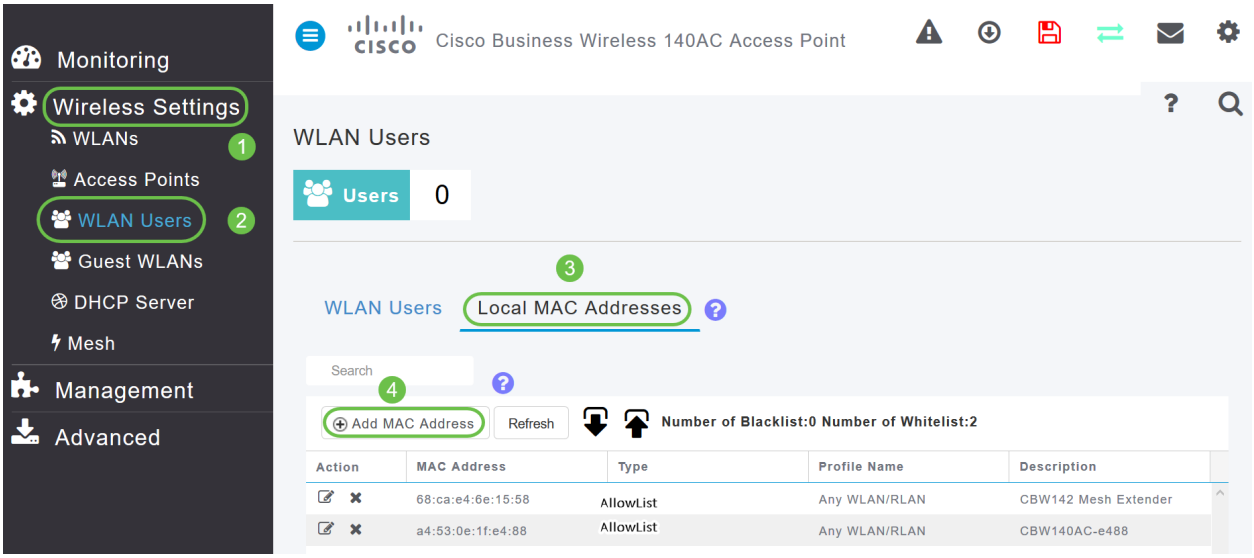


Paso 6

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.

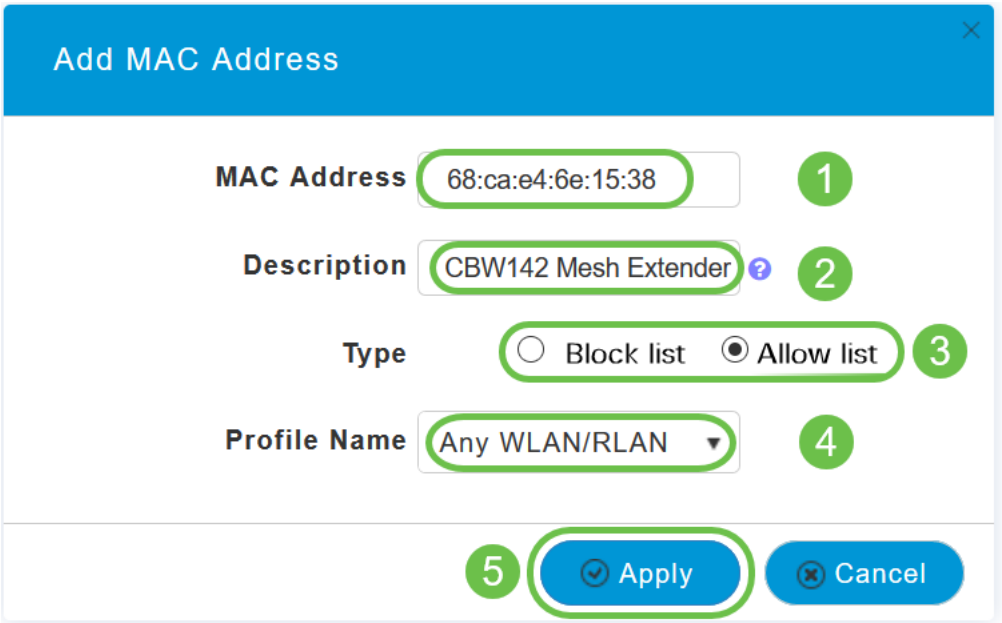
Paso 7

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.

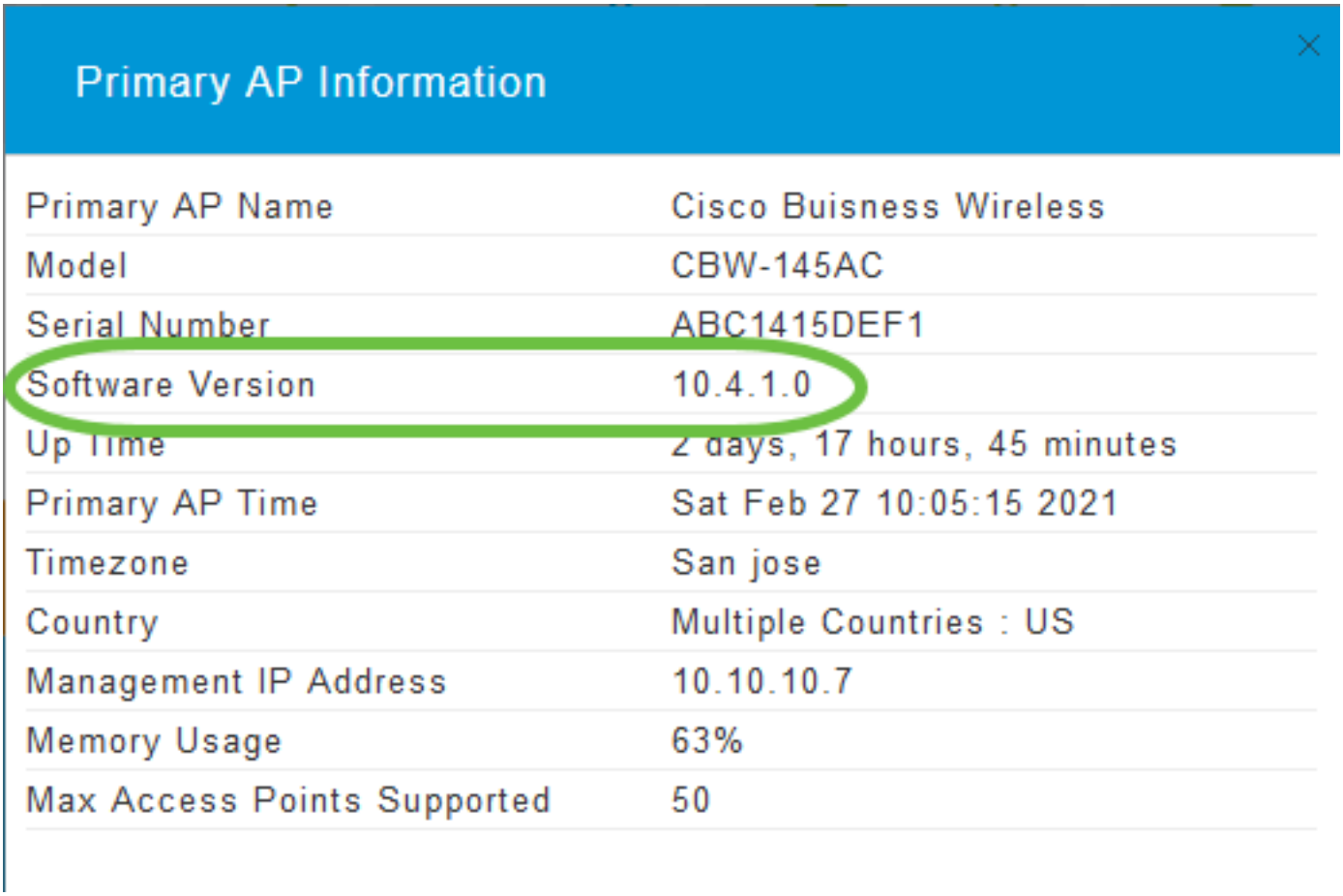
Comprobar y actualizar el software mediante la interfaz de usuario web

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.

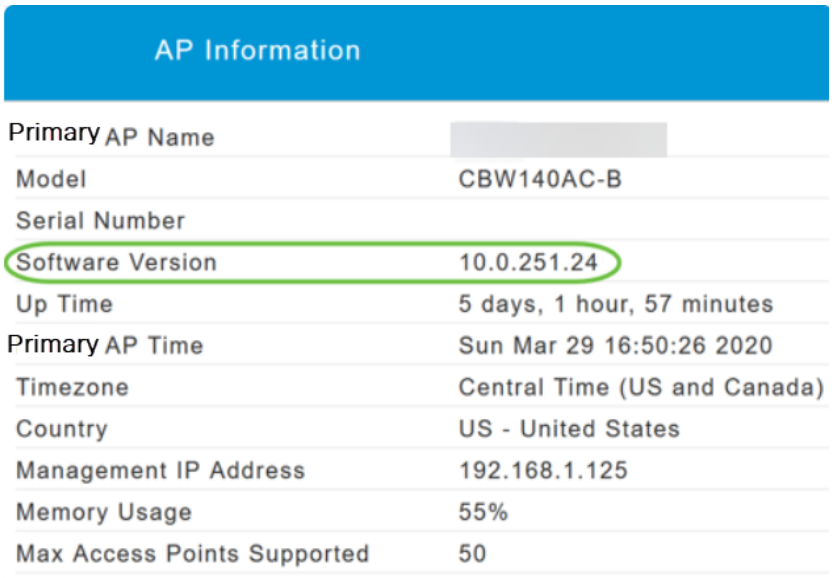
Paso 1

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.



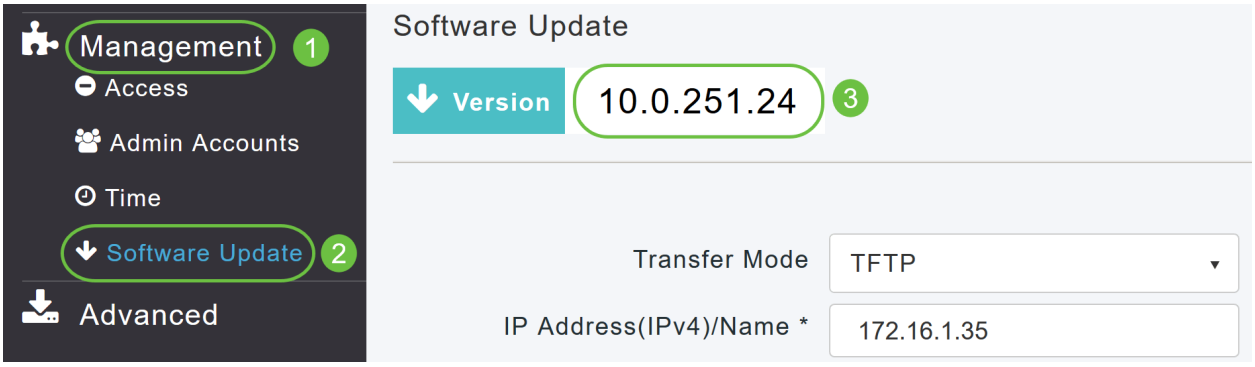
Si está ejecutando la última versión de software, puede saltar a la sección Creación de WLANs.

Paso 3

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

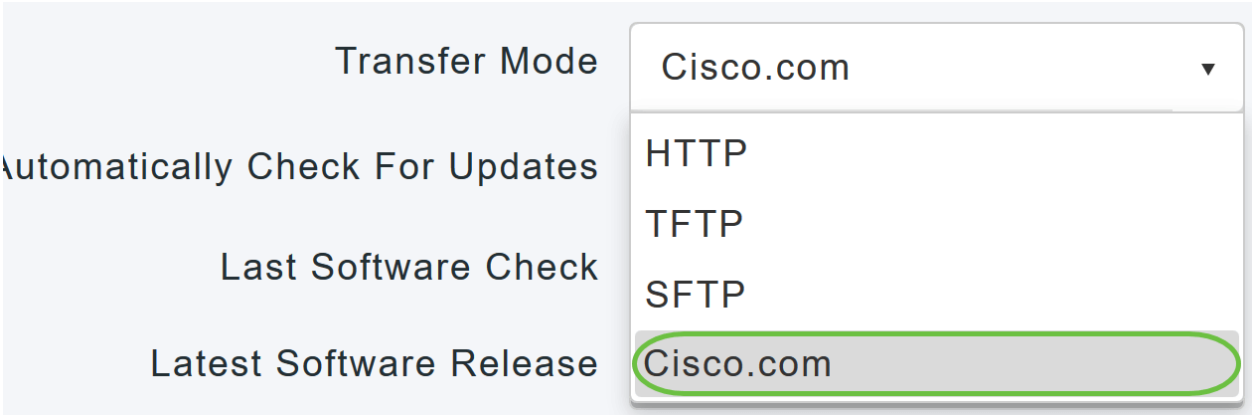
La ventana *Actualización de software* se muestra con el número de versión de

software actual en la parte superior.



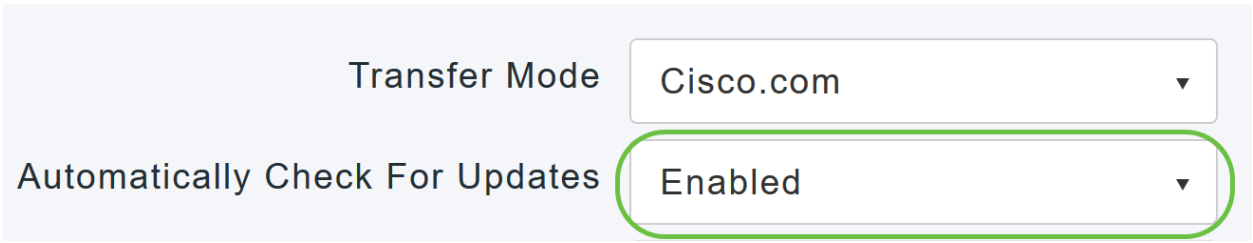
Puede actualizar el software CBW AP y las configuraciones actuales en el AP principal no se eliminarán.

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



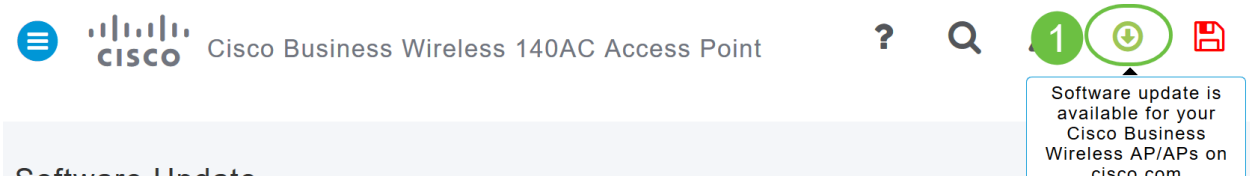
Paso 4

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.



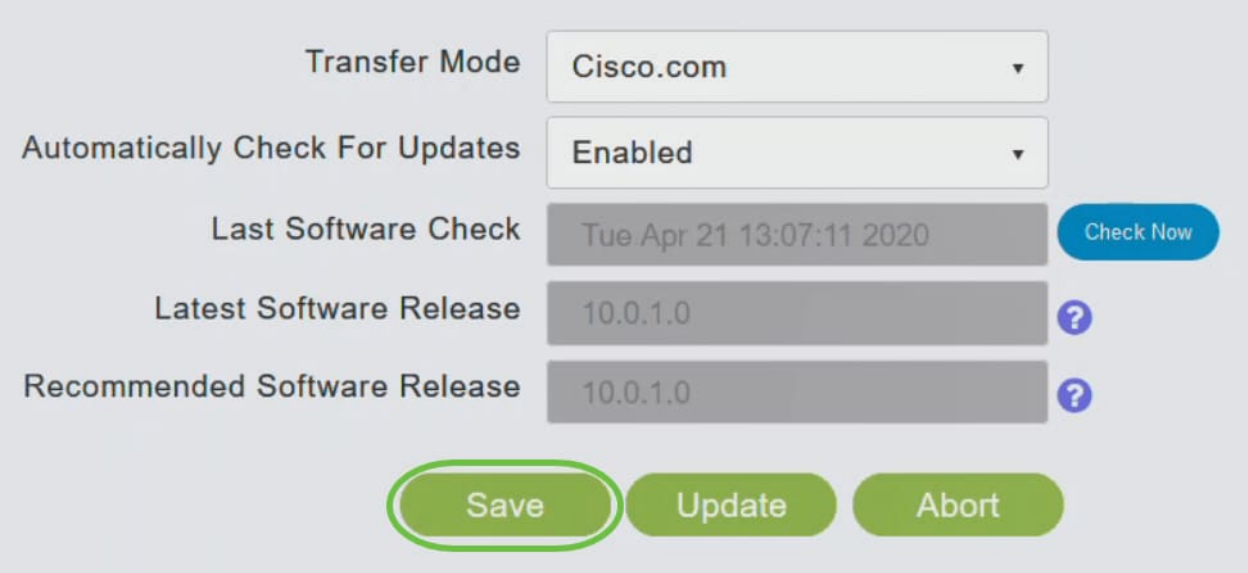
Cuando se realiza una comprobación de software y si hay disponible una actualización de software más reciente o recomendada en Cisco.com, entonces:

- 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.

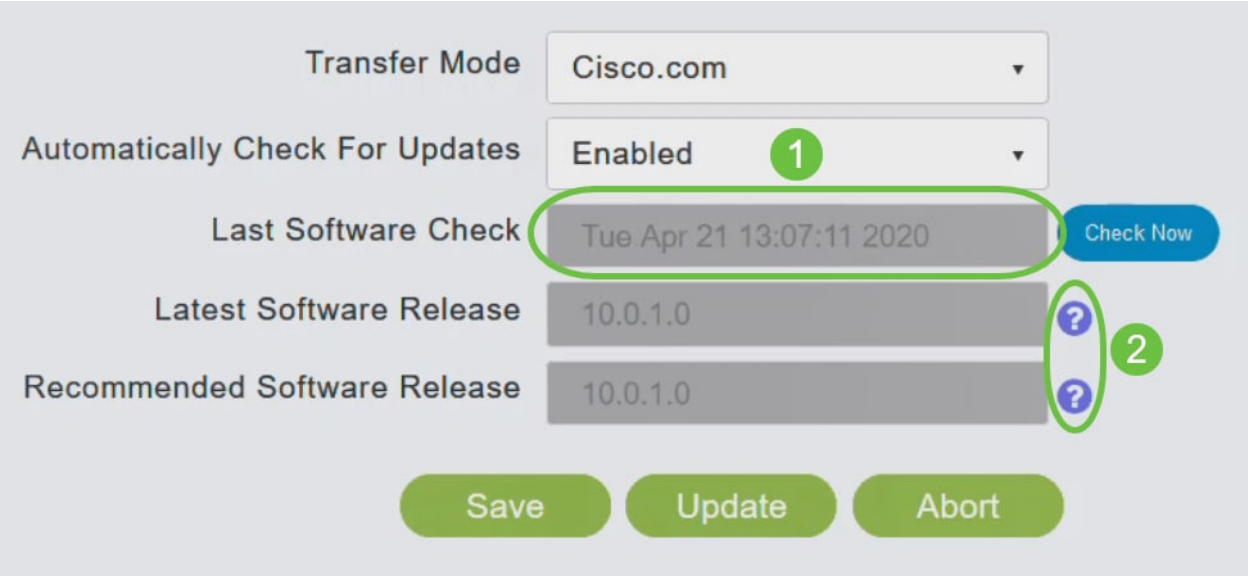


Paso 5

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

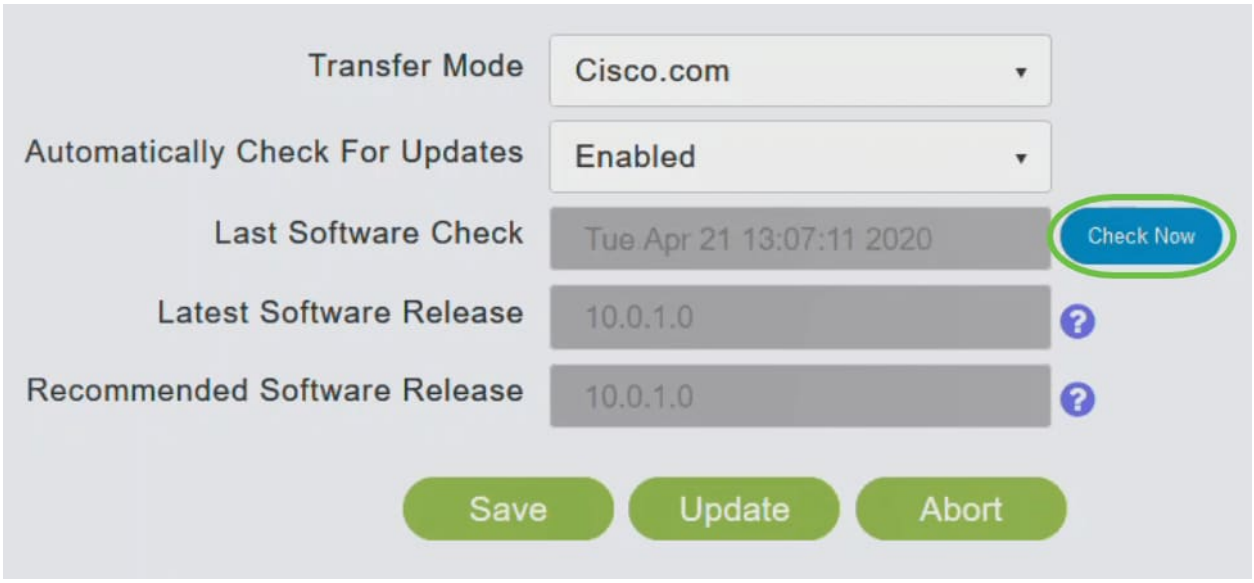


El campo *Last Software Check* muestra la marca de hora de la última comprobación automática o manual del software. Para ver las notas de las versiones mostradas, haga clic en el **icono del signo de interrogación** situado junto a él.



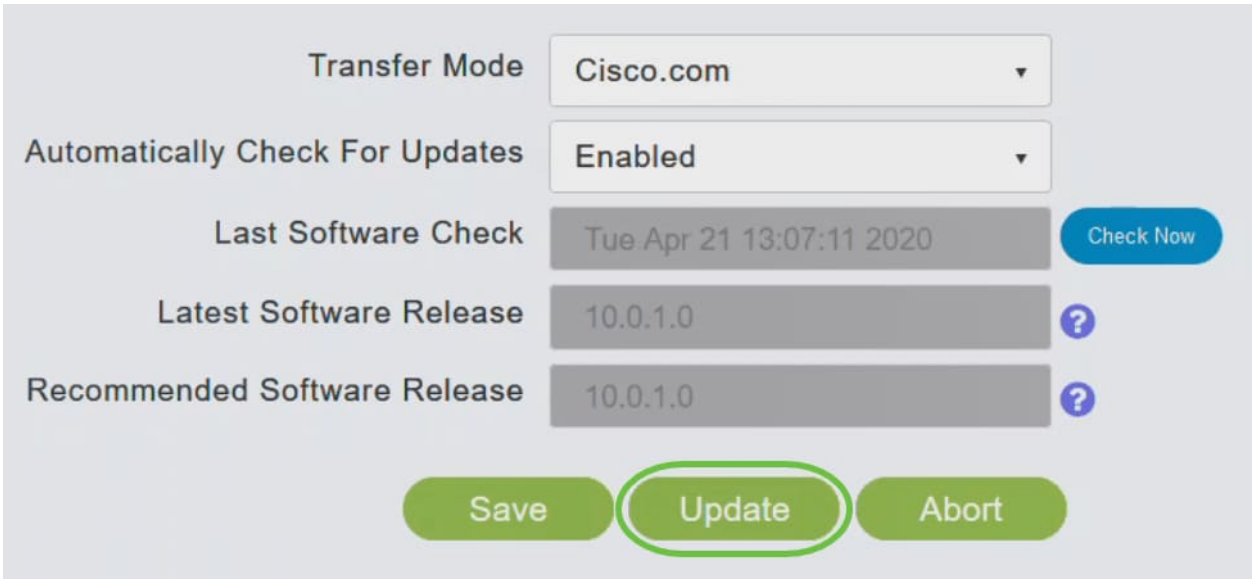
Paso 6

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



Paso 7

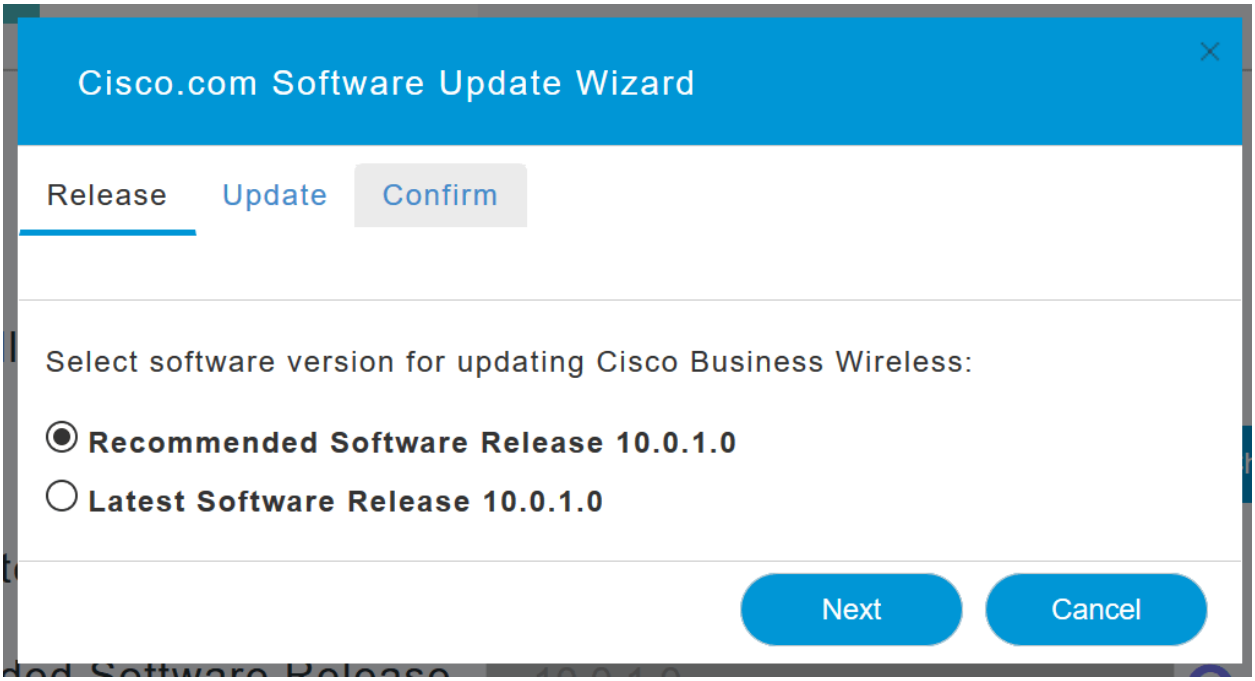
Para continuar con la actualización del software, haga clic en **Update**.



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

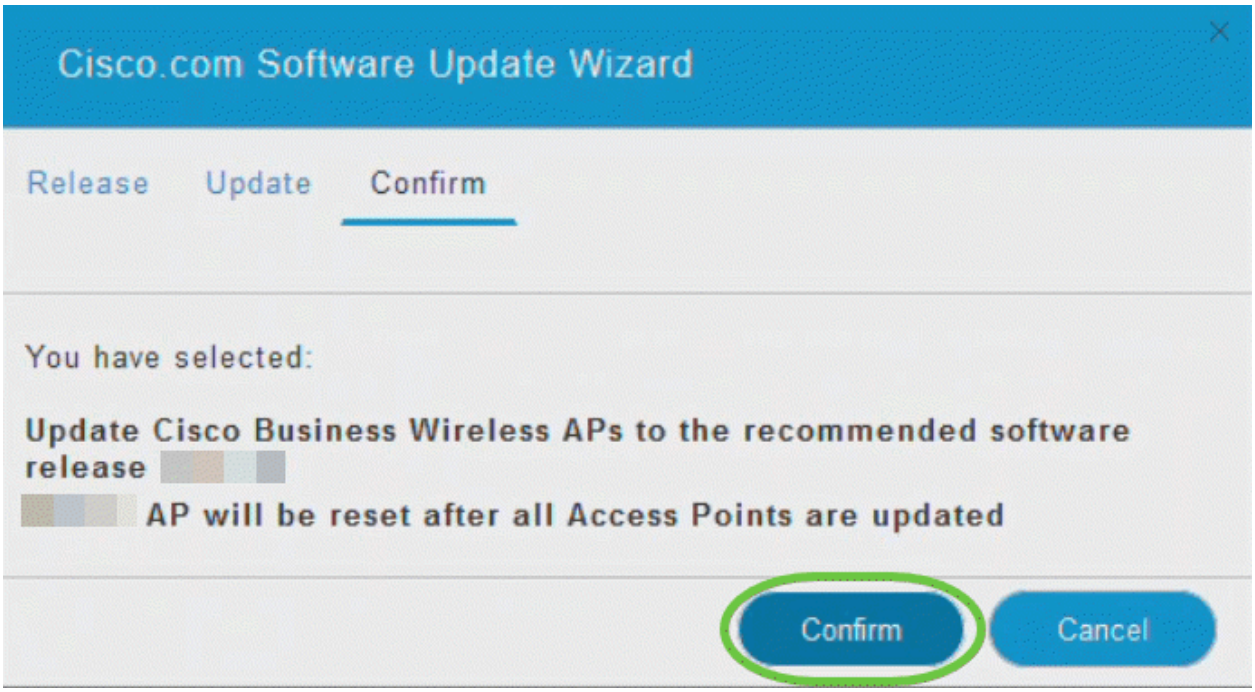
- Ficha Versión: especifique si desea actualizar a la versión de software recomendada o a la última versión de software.
- Ficha Actualizar - Especifique cuándo se deben restablecer los AP. Puede optar por hacerlo de inmediato o programarlo más adelante. Para configurar el AP primario para que se reinicie 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**.

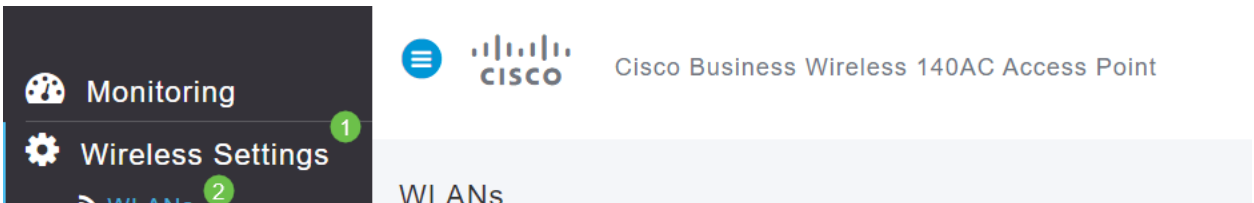


Crear WLANs en la interfaz de usuario web

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

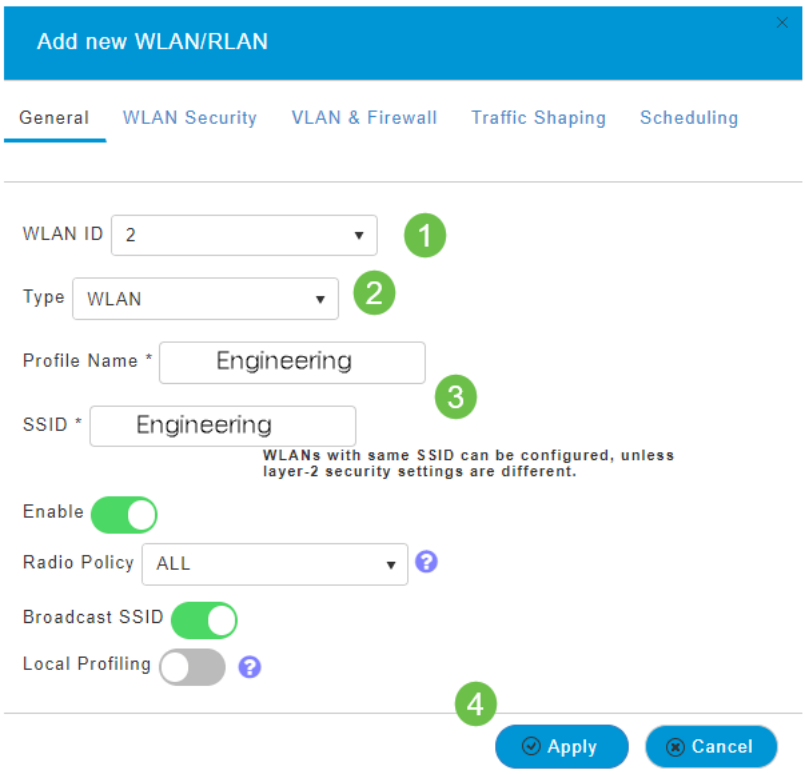
En la ficha *General*, introduzca la siguiente información:

- 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).

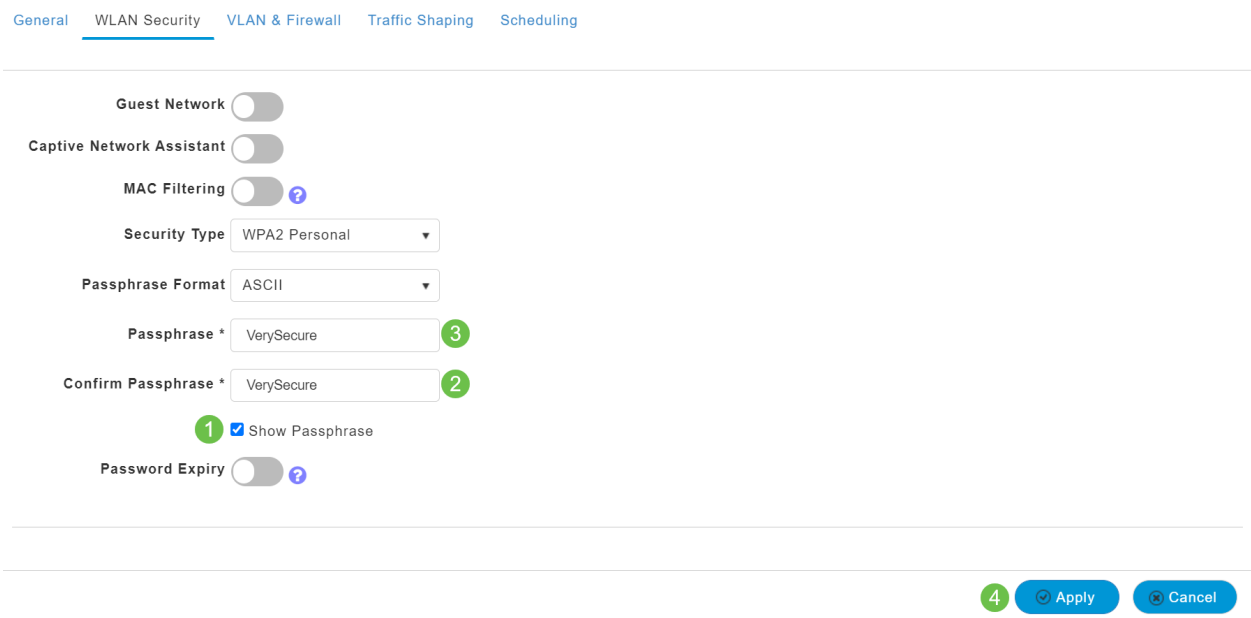
WPA2 Personal es un método utilizado para proteger la red mediante la autenticación PSK. El PSK se configura por separado en el AP primario, bajo la política de seguridad WLAN y en el cliente. WPA2 Personal no se basa en un servidor de autenticación de la red.

- 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.

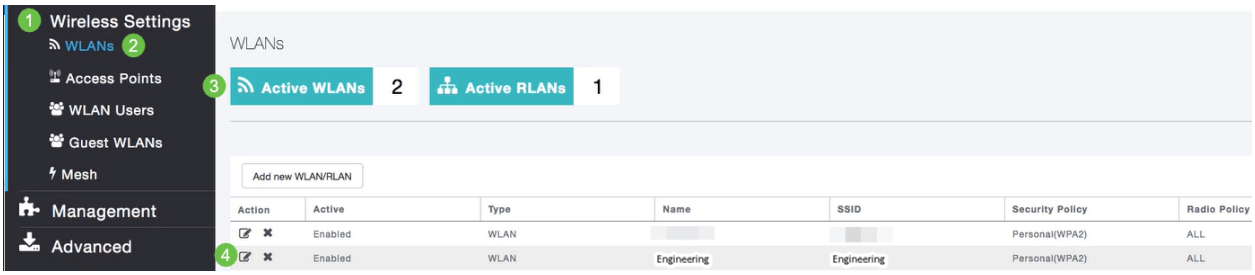


Paso 4

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)

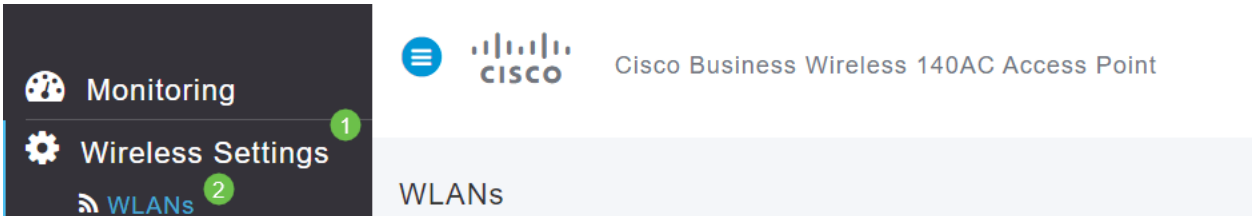
Una WLAN de invitado le permite a los invitados acceder a su red Cisco Business Wireless.

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

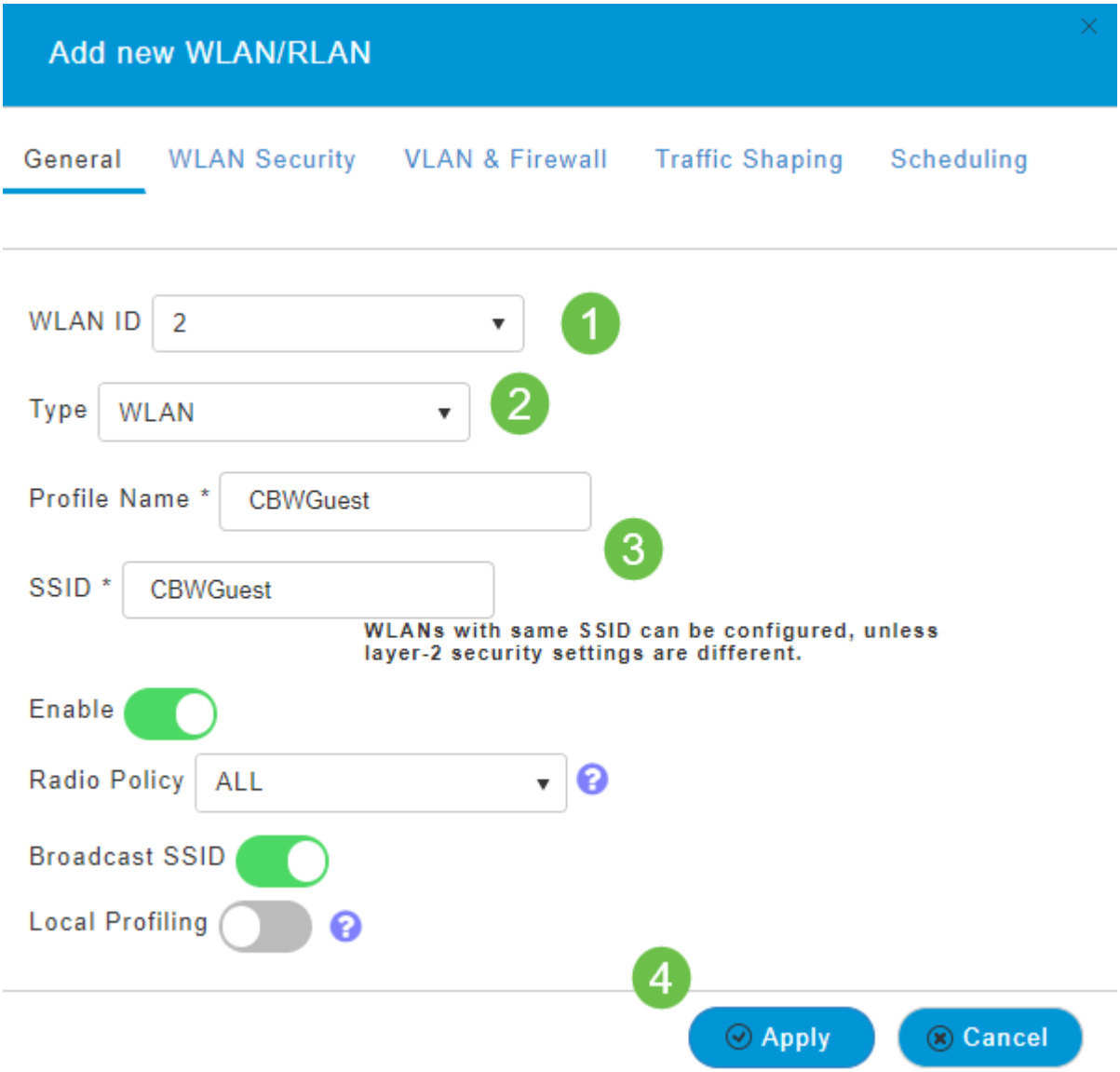
En la ficha *General*, introduzca la siguiente información:

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).

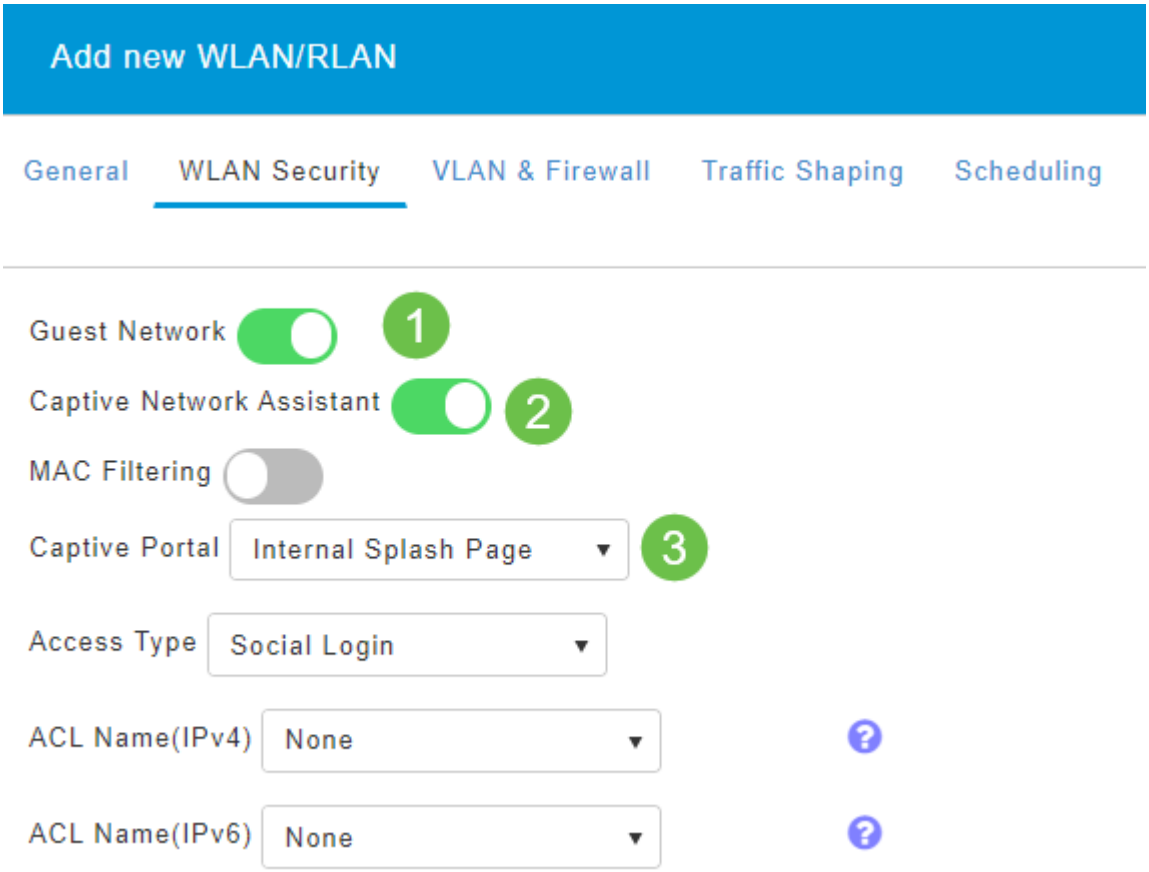


Paso 4

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.

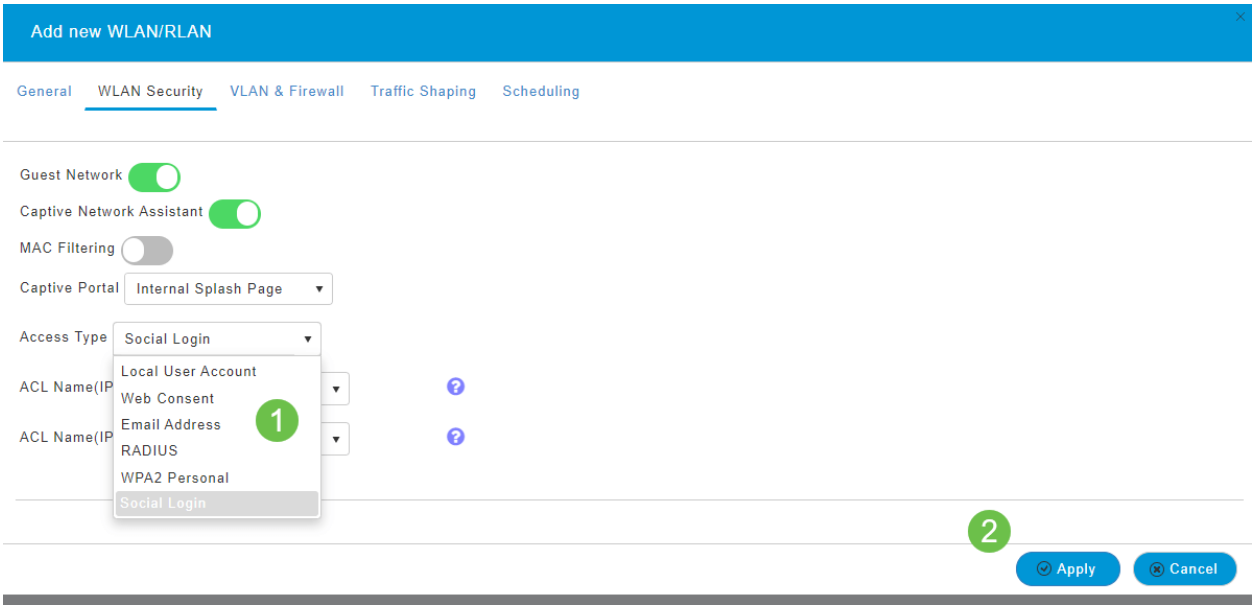
Otras opciones para el *tipo de acceso* incluyen:

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

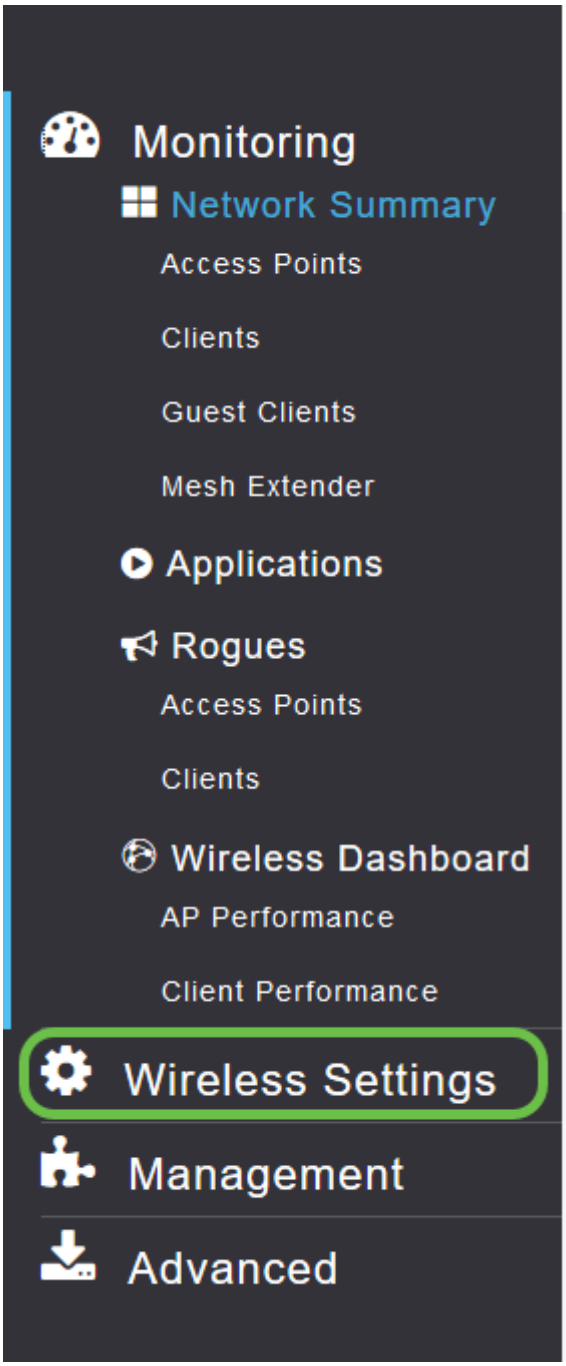
funciones de políticas son: acceso de invitado, listas de control de acceso y QoS.

Paso 1

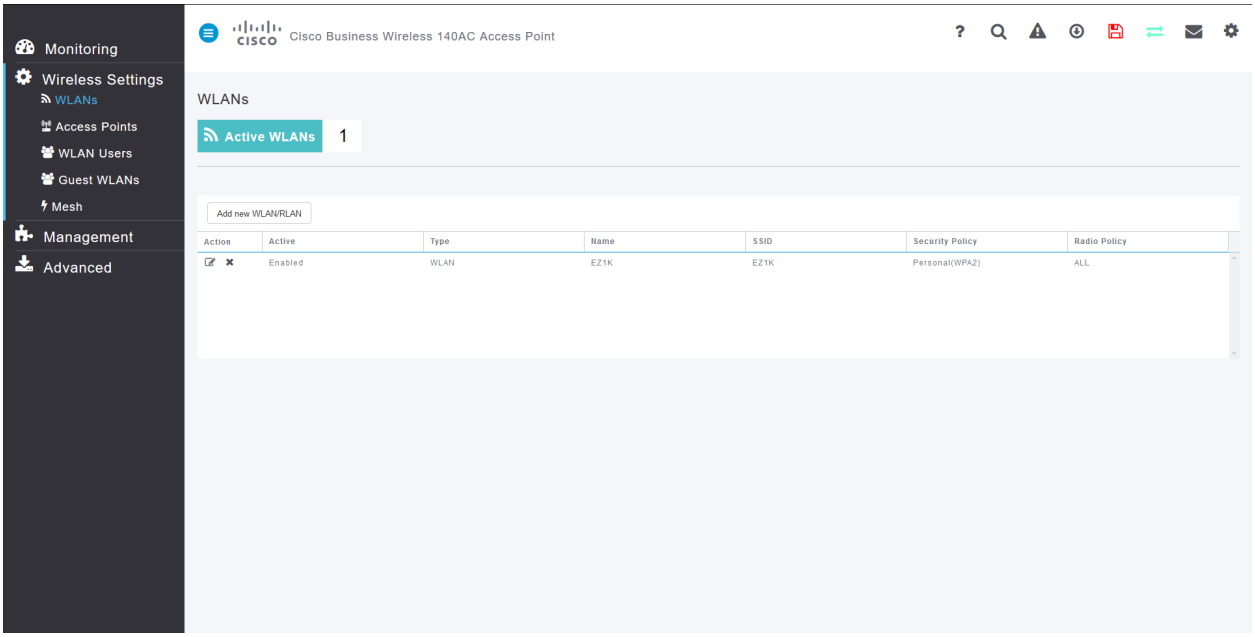
Desplácese hasta el menú situado en la parte izquierda de la pantalla si no ve la barra de menús izquierda.

Paso 2

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

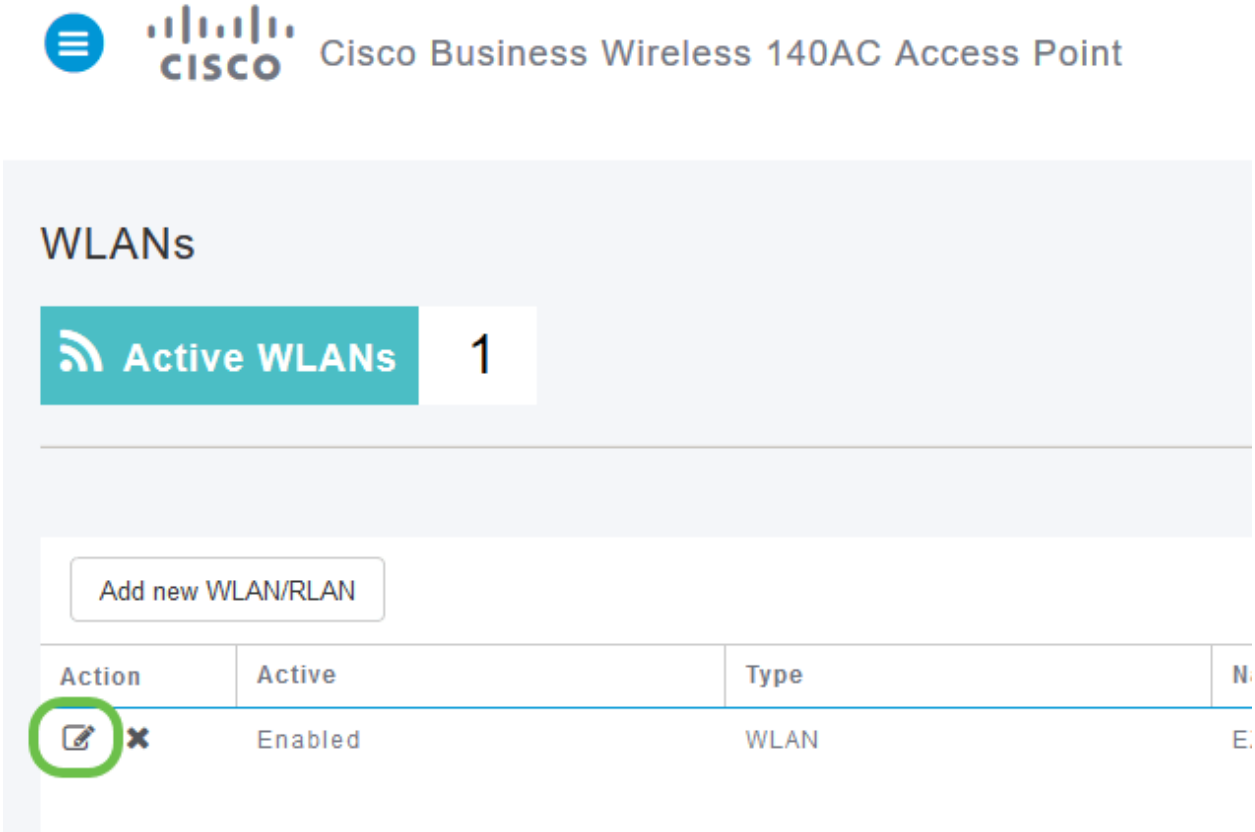


La siguiente imagen es similar a la que verá al hacer clic en el enlace Wireless Settings (Parámetros inalámbricos).

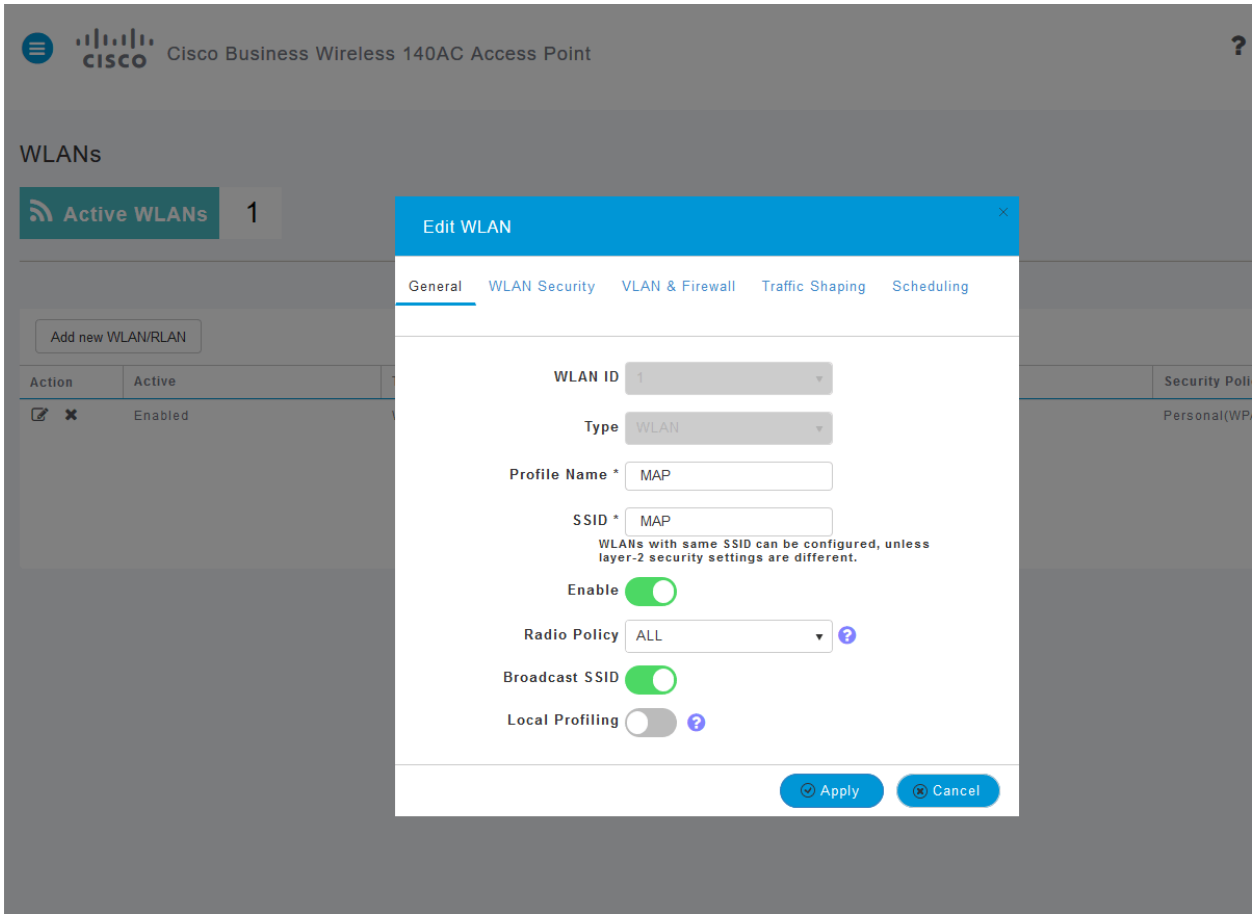


Paso 3

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.

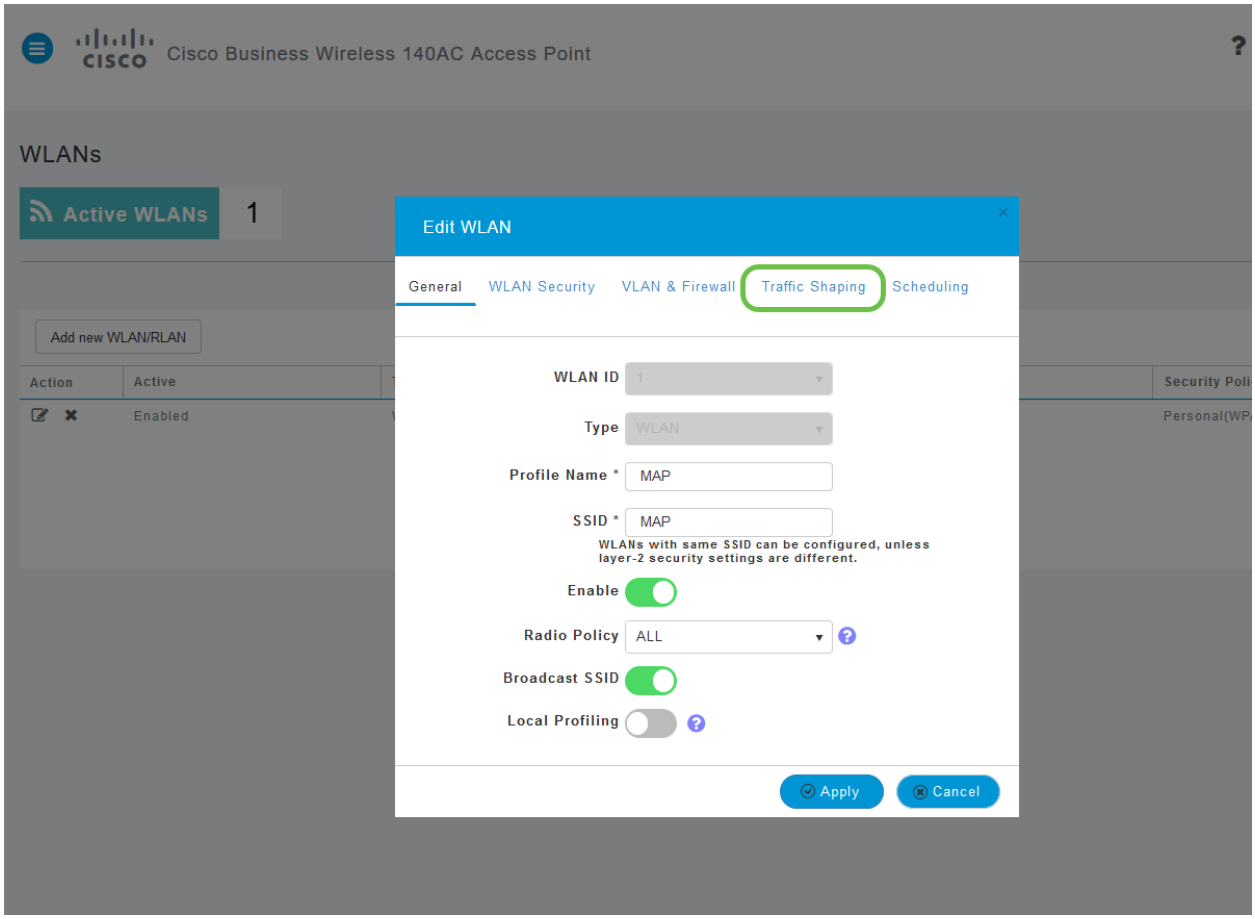


Desde que recientemente agregó la WLAN, su página *Editar WLAN* puede aparecer similar a la siguiente:

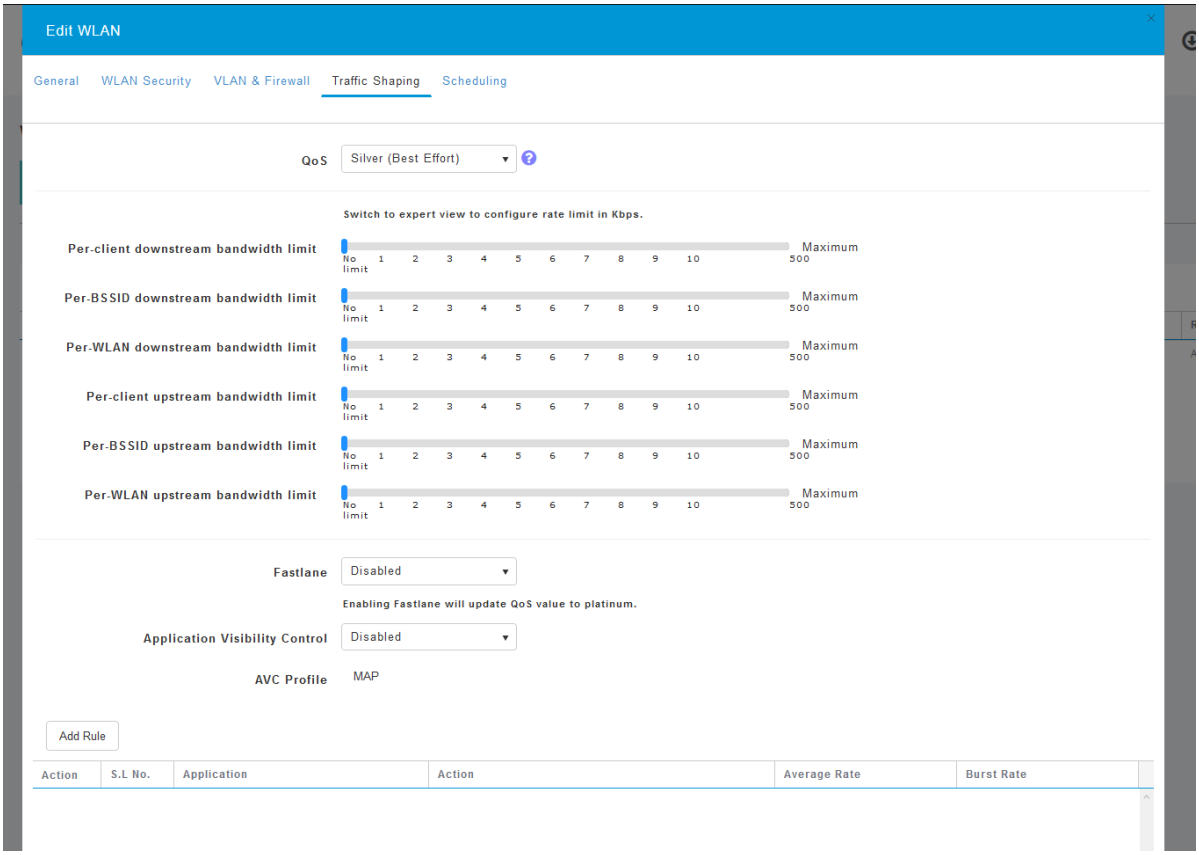


Paso 4

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

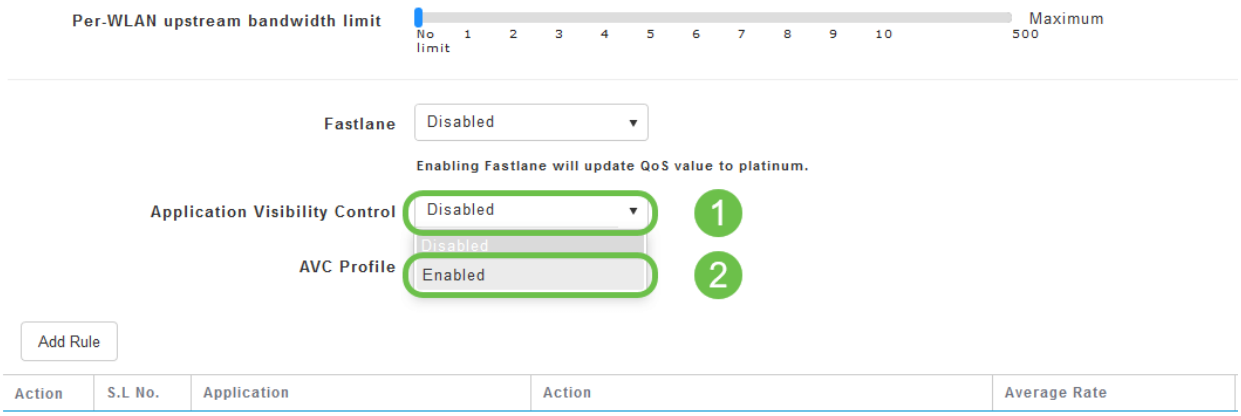


La pantalla puede aparecer de la siguiente manera:



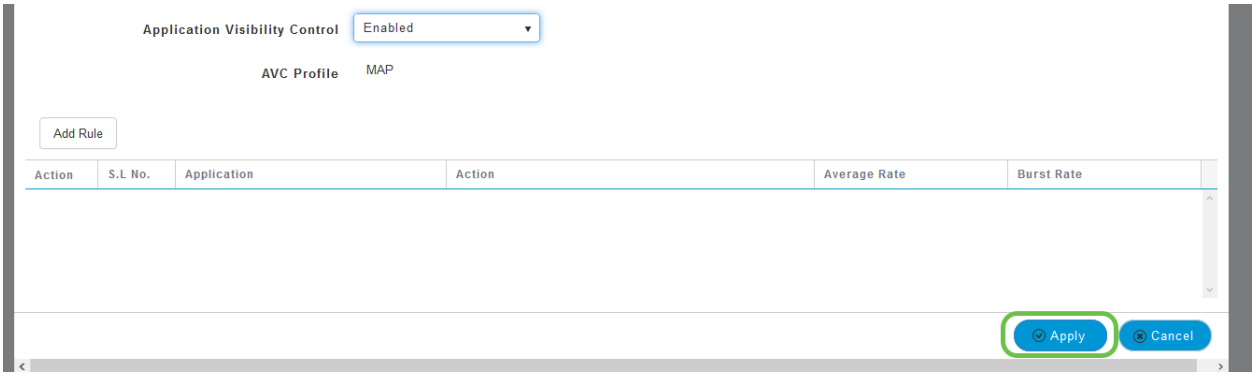
Paso 5

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

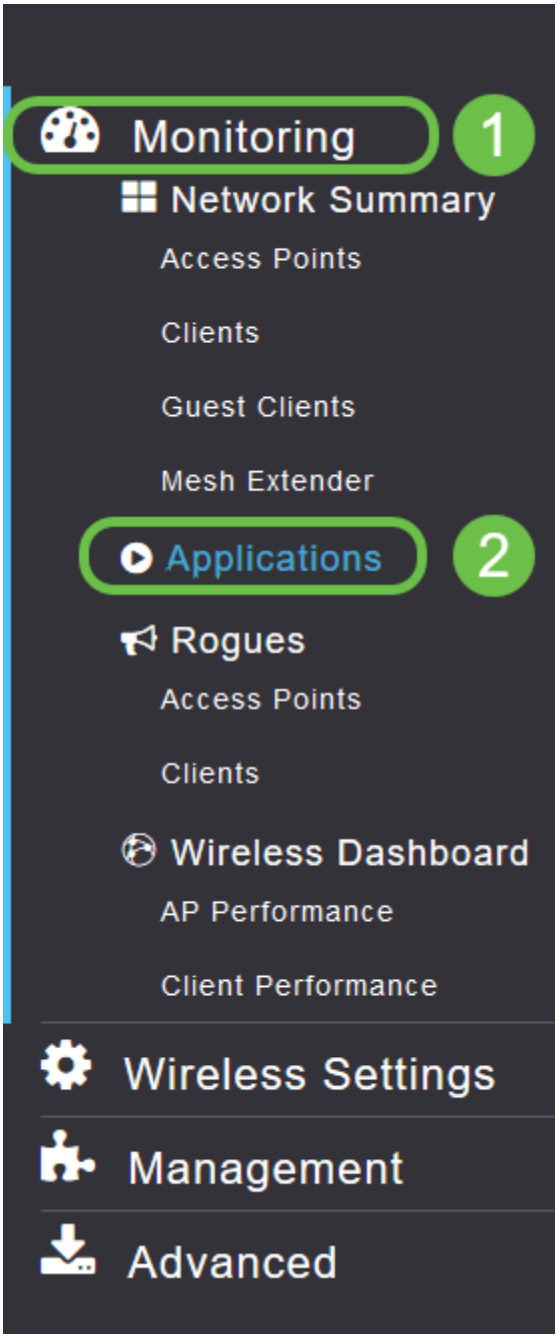
Haga clic en el botón **Aplicar**.



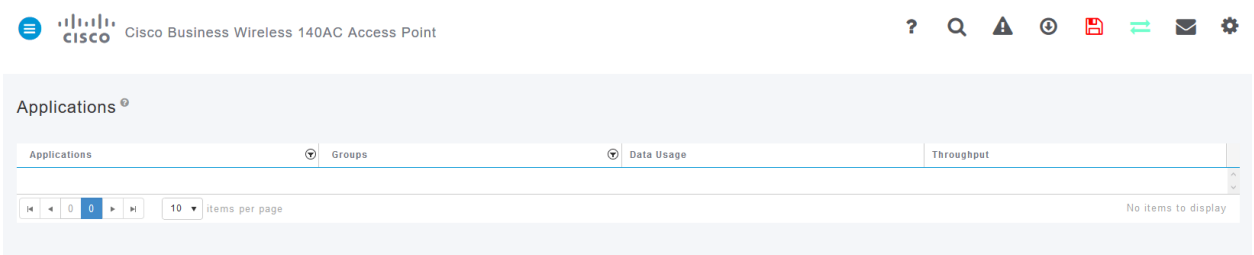
Esta configuración debe estar activada, de lo contrario la función no funcionará.

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:

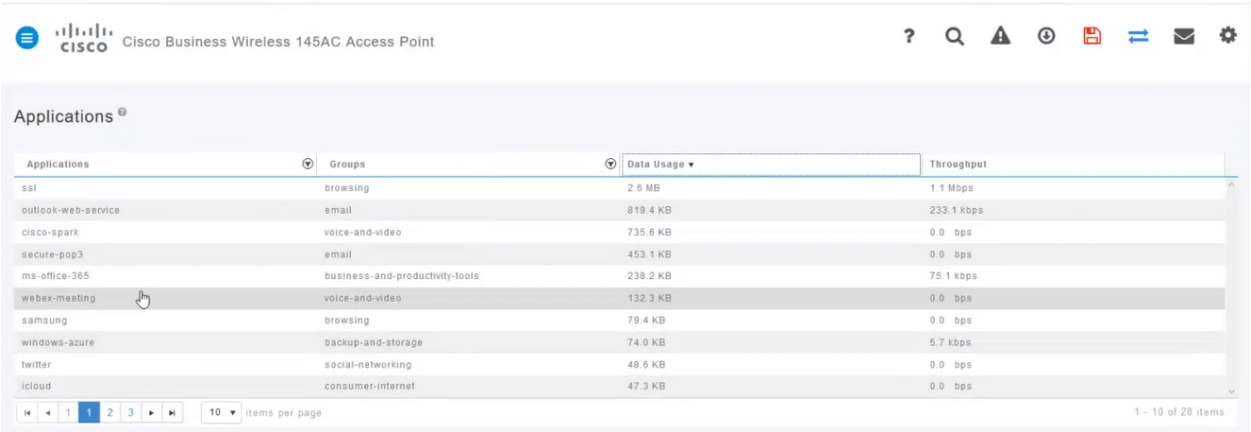
- Aplicación: incluye muchos tipos diferentes
- Grupos: indica el tipo de grupo de aplicaciones para una ordenación más sencilla
- Uso de datos: la cantidad de datos utilizados por este servicio en general
- Rendimiento: la cantidad de ancho de banda utilizada por la aplicación

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

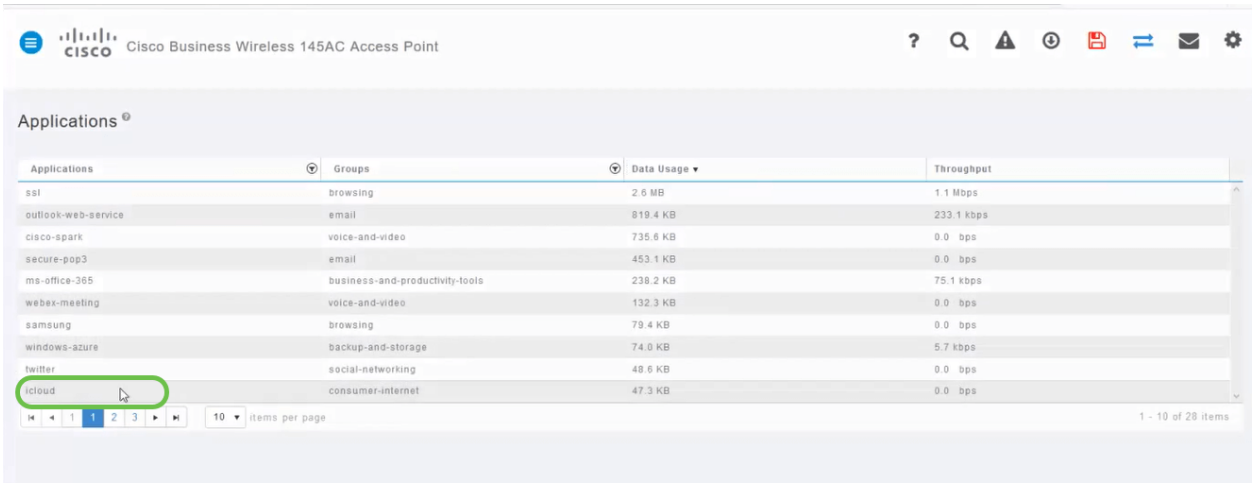
Muestra un ejemplo de cómo se verá la página cuando se rellene.



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

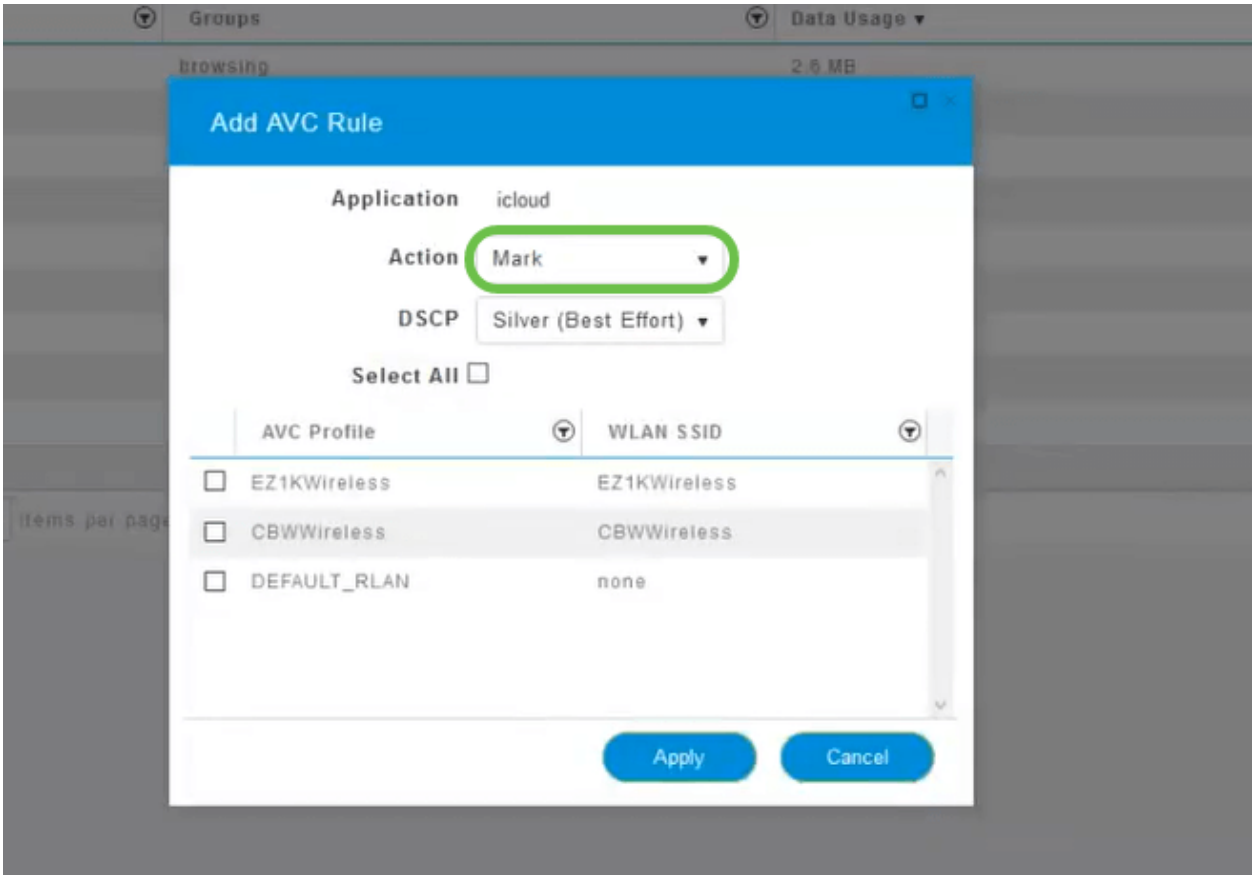
Paso 8

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.



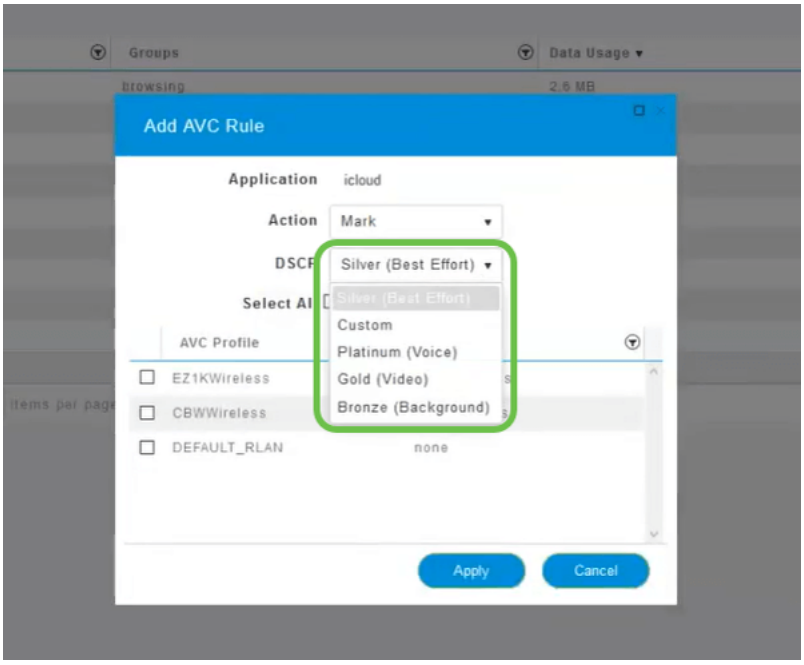
Para este ejemplo, dejamos esta opción en *Mark*.

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.



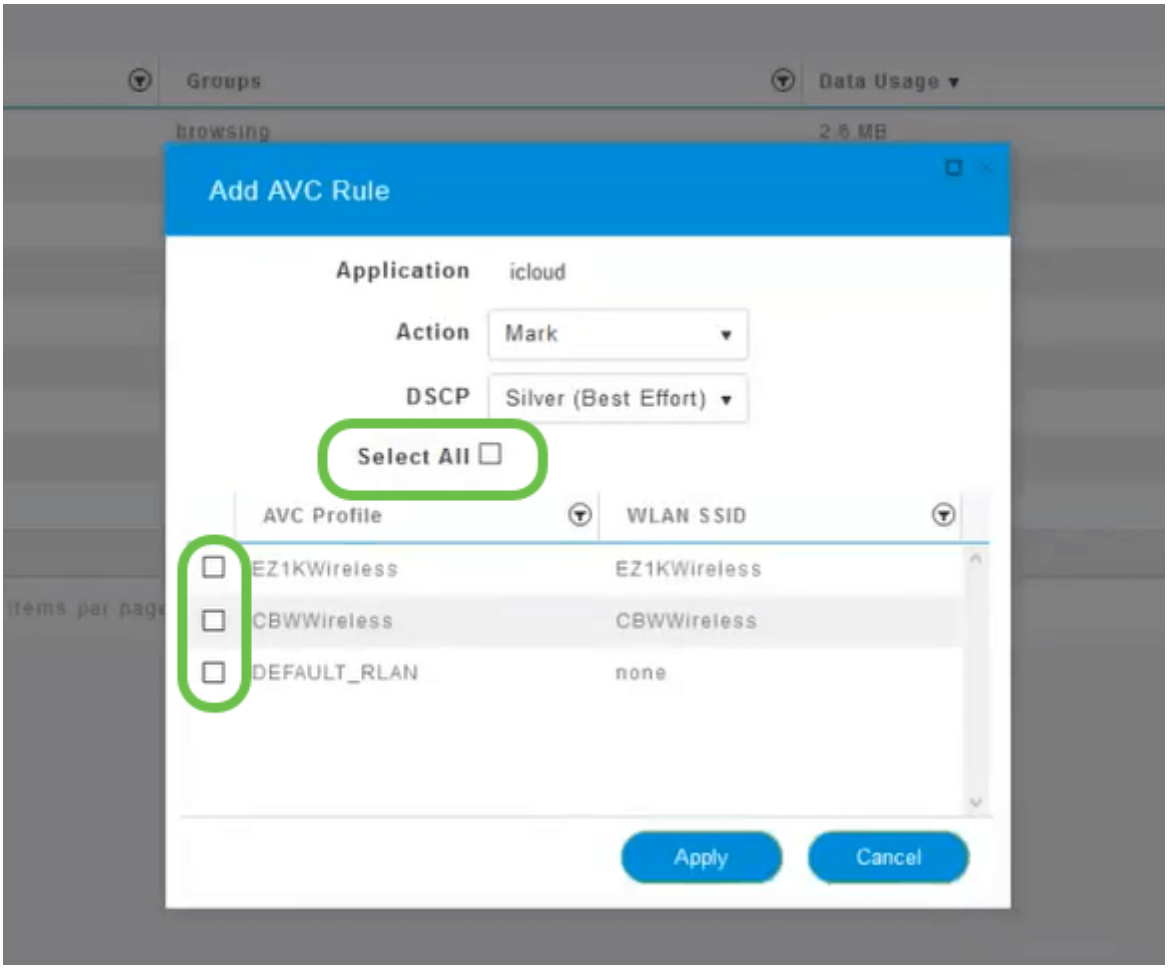
A continuación se muestran las opciones DSCP para que se marque el tráfico. Estas opciones van desde menos recursos a más recursos disponibles para el tipo de tráfico que está editando.

- 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.

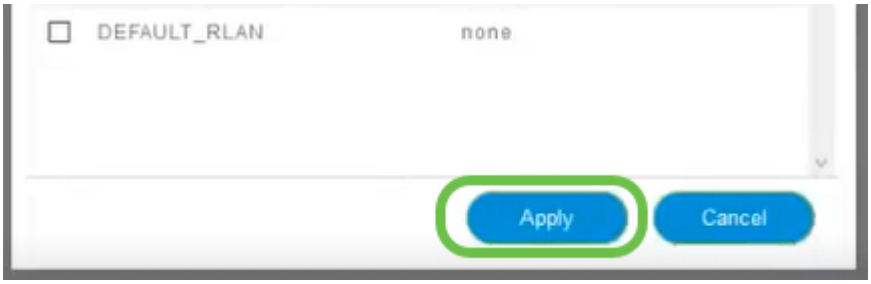
Paso 11

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

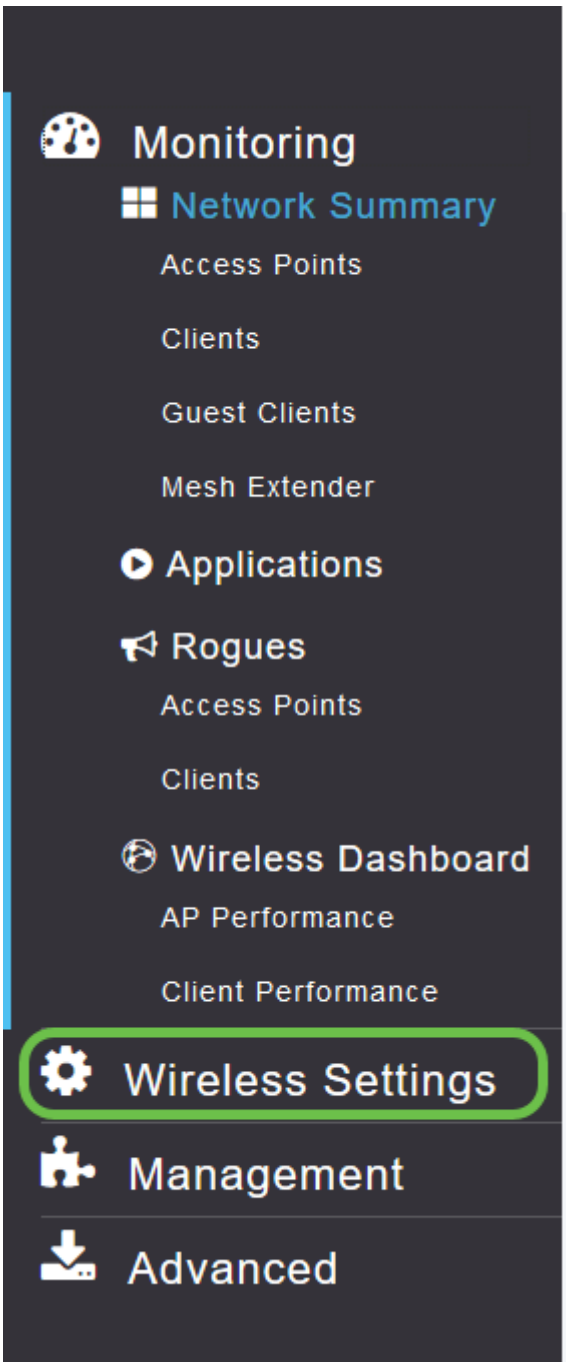
Las estadísticas sobre estos clientes incluyen la cantidad de datos utilizados y el rendimiento.

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.

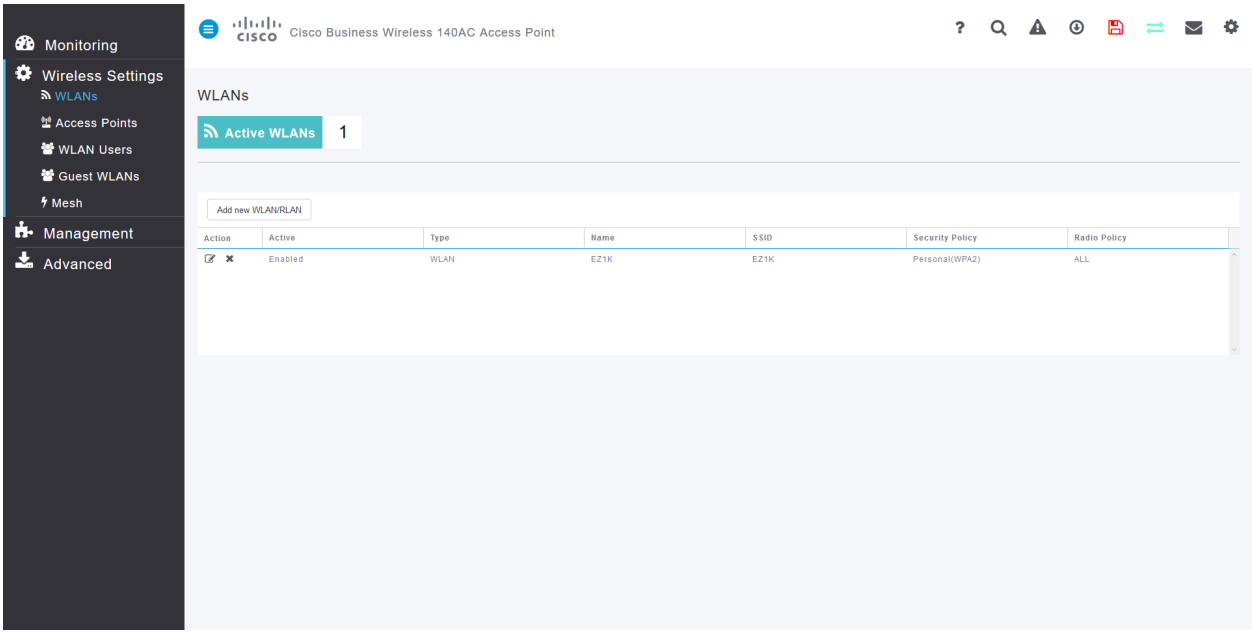
Una vez habilitada, los detalles del cliente de la red se pueden encontrar en la sección Supervisión de la interfaz de usuario web.

Paso 1

Haga clic en **Wireless Settings**.

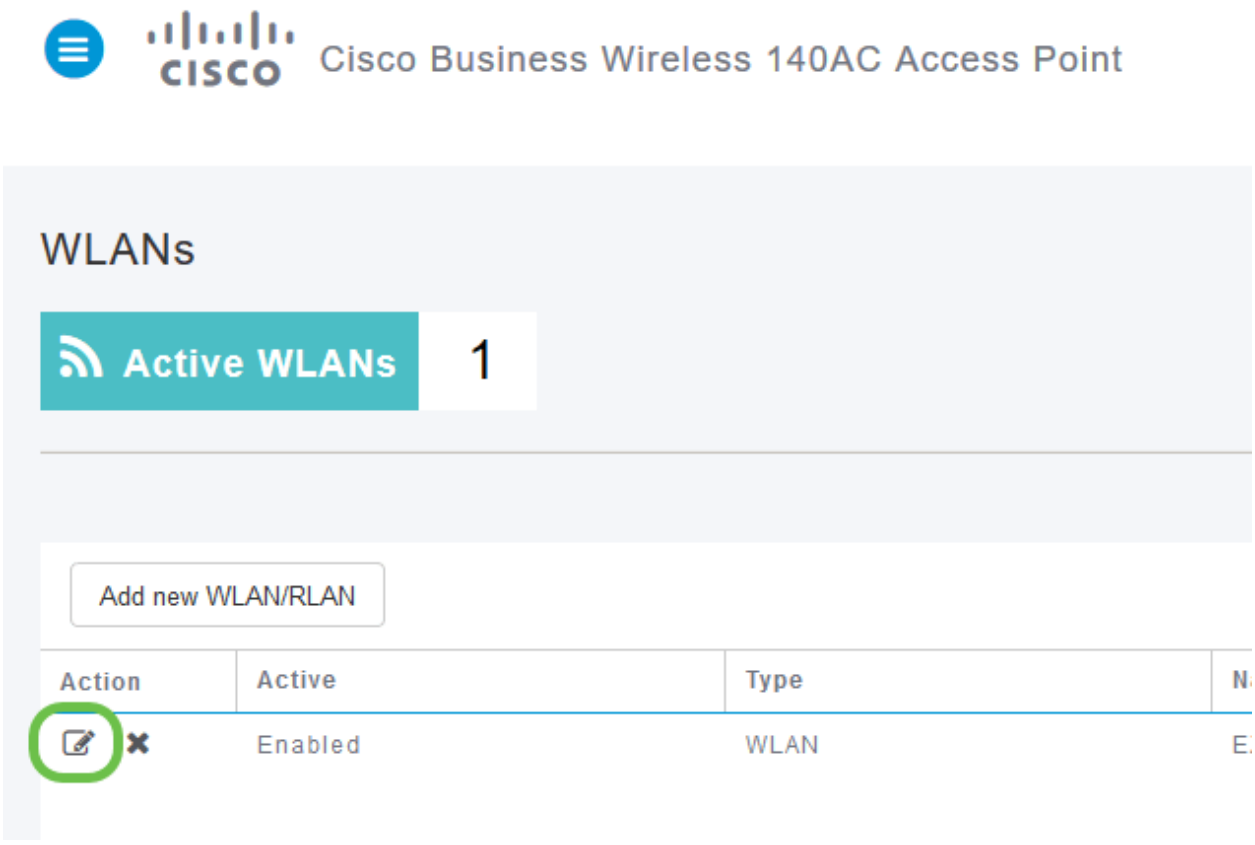


A continuación, se muestra una descripción similar a la que verá al hacer clic en el enlace Wireless Settings (Parámetros inalámbricos):



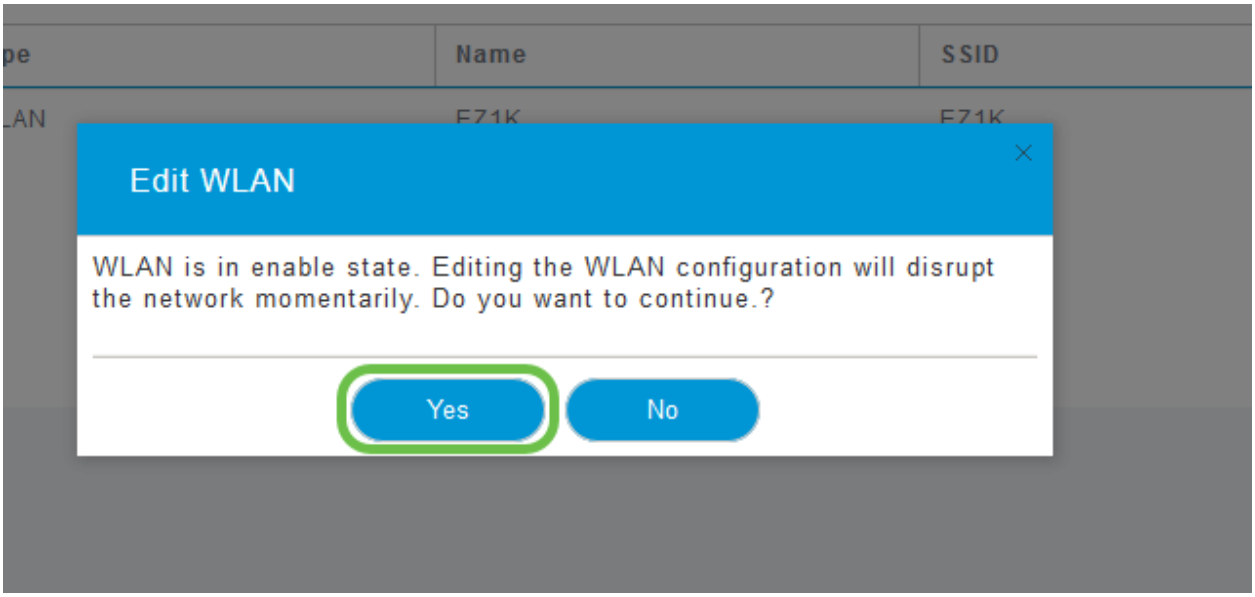
Paso 2

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.

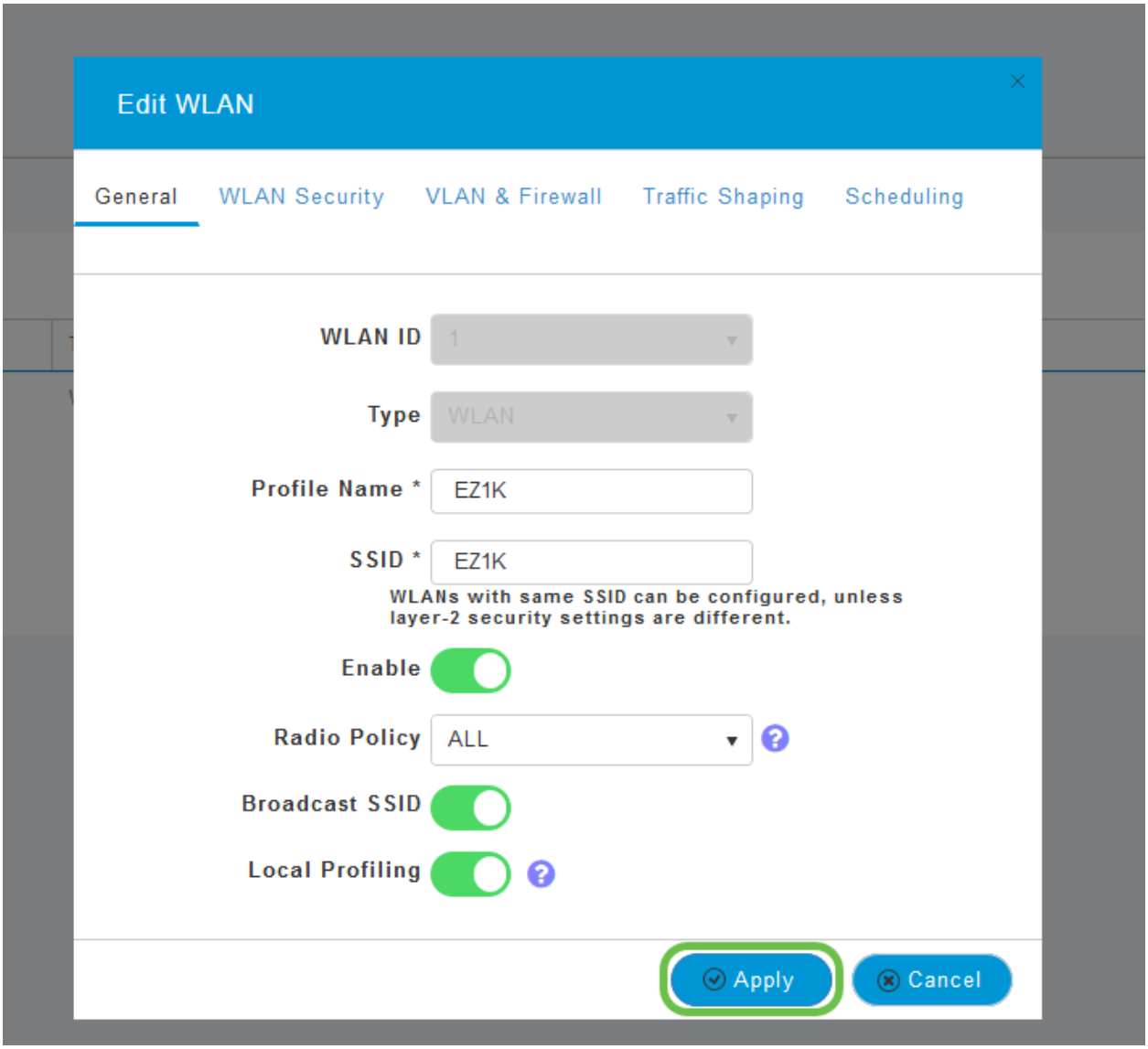


Paso 4

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

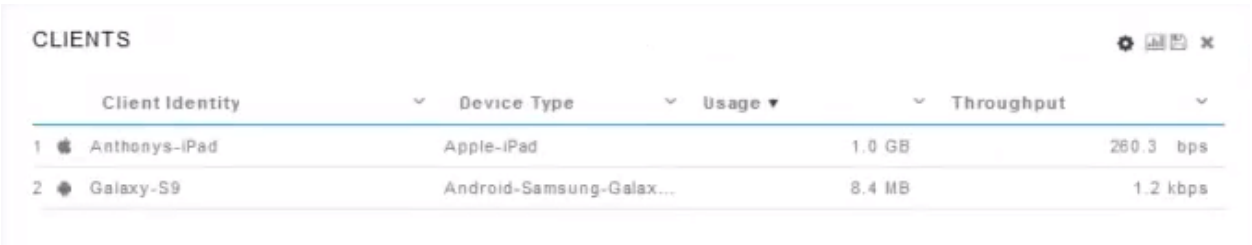
Paso 5

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 RV345P con PoE
- Punto de acceso Cisco Business 140AC
- Cisco Business 142ACM Mesh Extender