Configuración de red total: RV345P y tecnología inalámbrica empresarial de Cisco con la aplicación móvil

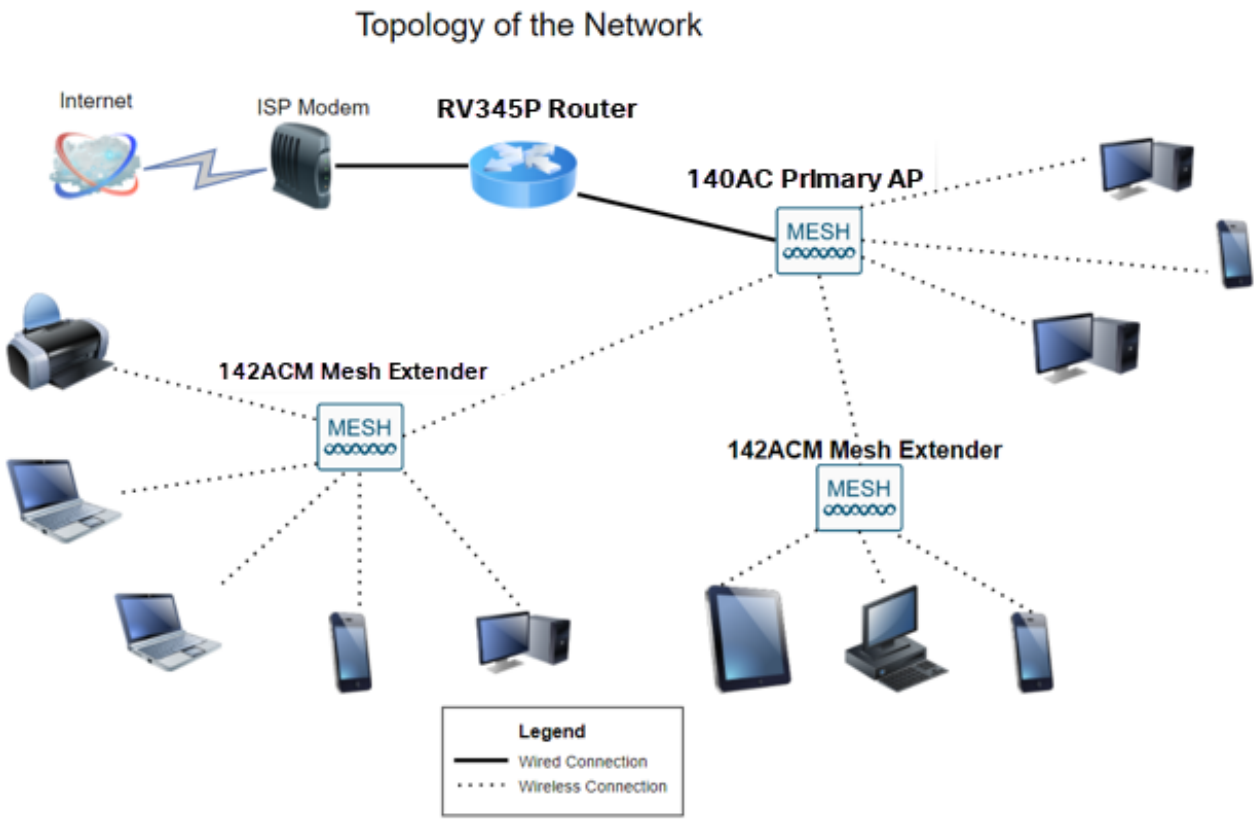
Objetivo

En esta guía se muestra 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 aplicación móvil, recomendada para una configuración sencilla en la red inalámbrica de malla. Si prefiere utilizar la interfaz de usuario Web (UI) para todas las configuraciones, haga clic para saltar al artículo que utiliza la interfaz de usuario Web.

Table Of Contents

Topología



Introducción

Toda su investigación se ha reunido y ha adquirido su equipo de Cisco, ¡qué interesante! 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 a 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, bloquearlo y registrarlo, o simplemente para bloquear el tráfico.
2. El filtrado web se utiliza para evitar que el tráfico web se dirija 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) que está disponible en Cisco. Las VPN permiten que los usuarios y sitios remotos se conecten a la oficina o los Data Centers de la empresa mediante 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, y se explican en esta guía.

Si no está familiarizado con algunos de los términos utilizados en este documento o desea obtener más detalles sobre las redes de malla, 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 del 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 para la configuración.
2. Póngase en contacto con el distribuidor de servicios de Internet (ISP) para obtener más información sobre las instrucciones especiales que puede utilizar cuando utilice el router RV345P. Algunos ISP ofrecen puertas de enlace con routers integrados. Si dispone de una puerta de enlace con un router integrado, puede que tenga que desactivar el router y pasar la dirección IP de la red de área extensa (WAN) (la dirección de protocolo de Internet exclusiva que el proveedor de Internet asigna a la 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 distribuidor de servicios de Internet (ISP).

Obtenga una cuenta Cisco.com

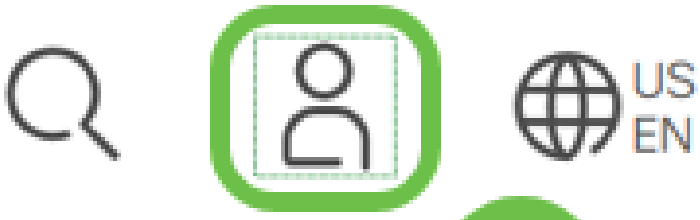
Ahora que es propietario de un equipo de Cisco, debe obtener una cuenta Cisco.com, a

veces denominada identificación en línea de Cisco Connection (ID de CCO). No se cobra por una cuenta.

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

Paso 1

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



1

Have an account?

- Personalized content
- Your products and support

Log In

Forgot your user ID and/or password?

Manage account

My Cisco

Need an account?

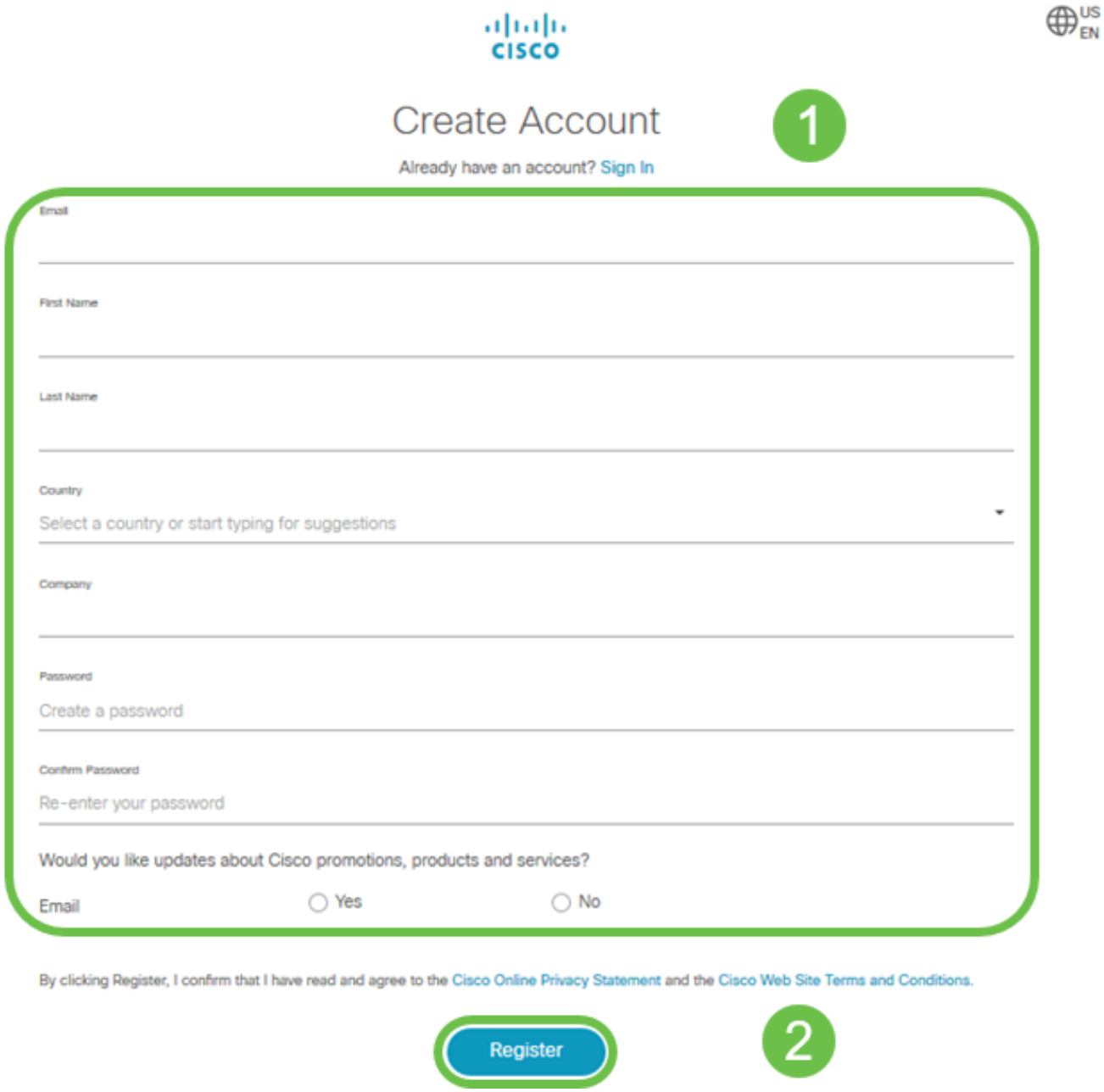
Create an account

2

Help

Paso 2

Introduzca los detalles necesarios para crear la cuenta y haga clic en Register (Registrar). Siga las instrucciones para completar el proceso de registro.



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

Configuración del router RV345P

Un router es esencial en una red porque rutea paquetes. Permite a un equipo comunicarse con otros equipos que no se encuentran 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 obtener los paquetes 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) pueden requerir que modifique algunos de estos parámetros. Una vez que se haya puesto 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 listo para usar

Paso 1

Conecte el cable Ethernet de uno de los puertos LAN (Ethernet) RV345P 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 distinto podría dañar el RV345P o hacer que fallaran los dongles USB. El interruptor de alimentación está activado de forma predeterminada.

Conecte el adaptador de corriente al puerto de 12 VCC del RV345P, pero no lo enchufe todavía a la alimentación.

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. Se encenderá el RV345P. Vuelva a conectar el módem para que también se pueda encender. La luz de alimentación del panel frontal se ilumina en verde fijo cuando el adaptador de corriente está conectado correctamente y el RV345P ha terminado de arrancar.

Configuración del router

El trabajo de preparación ha terminado, ¡ha llegado el momento de realizar algunas

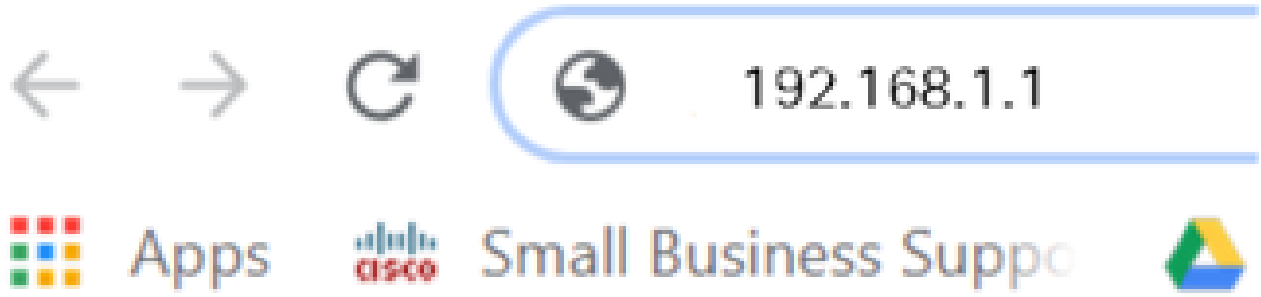
configuraciones! Para iniciar la interfaz de usuario web, siga estos pasos.

Paso 1

Si el equipo está configurado para convertirse en un cliente de protocolo de configuración dinámica de host (DHCP), se asignará al equipo una dirección IP en el intervalo 192.168.1.x. DHCP automatiza el proceso de asignación de direcciones IP, máscaras de subred, puertas de enlace predeterminadas y otros parámetros a los equipos. Los ordenadores deben estar configurados para participar en el proceso DHCP para obtener una dirección. Para ello, seleccione obtener una dirección IP automáticamente en las propiedades de TCP/IP del equipo.

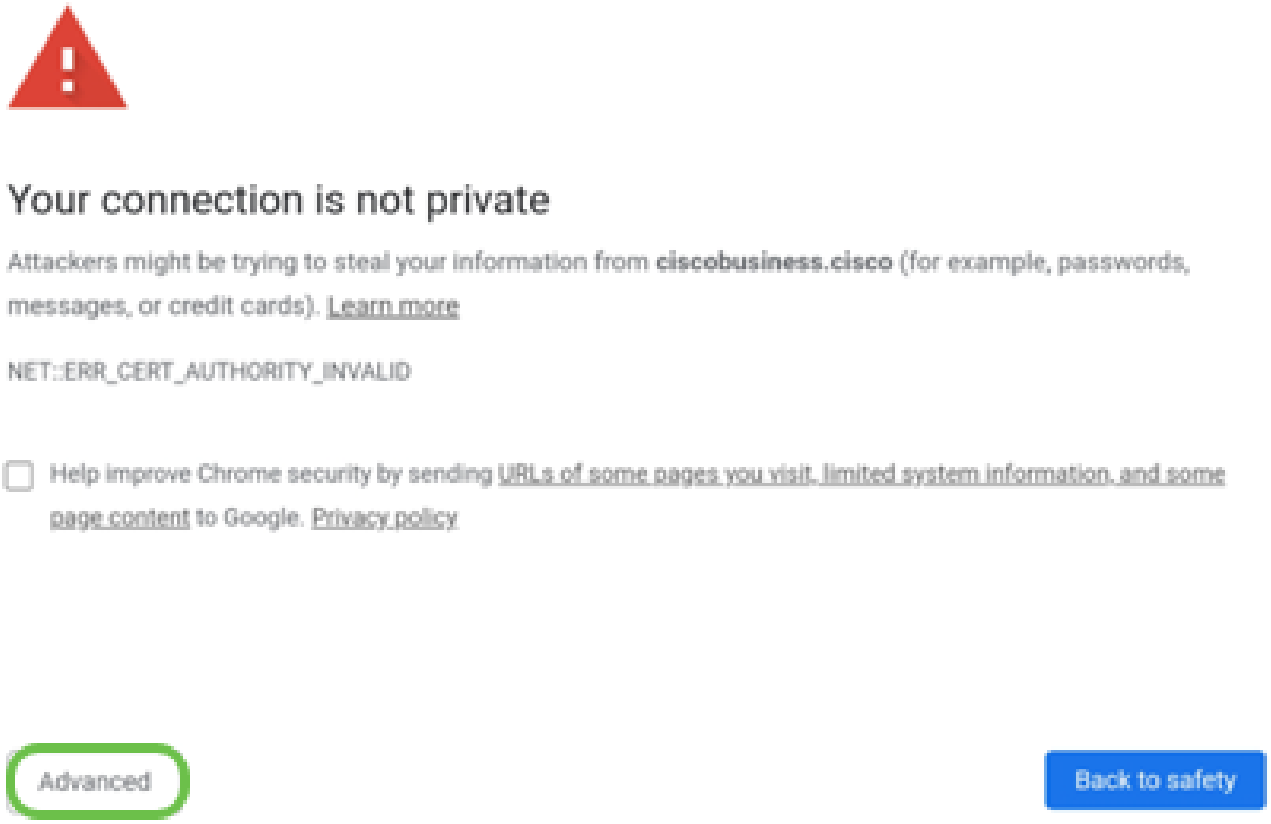
Paso 2

Abra un navegador 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 la conexión a Internet.

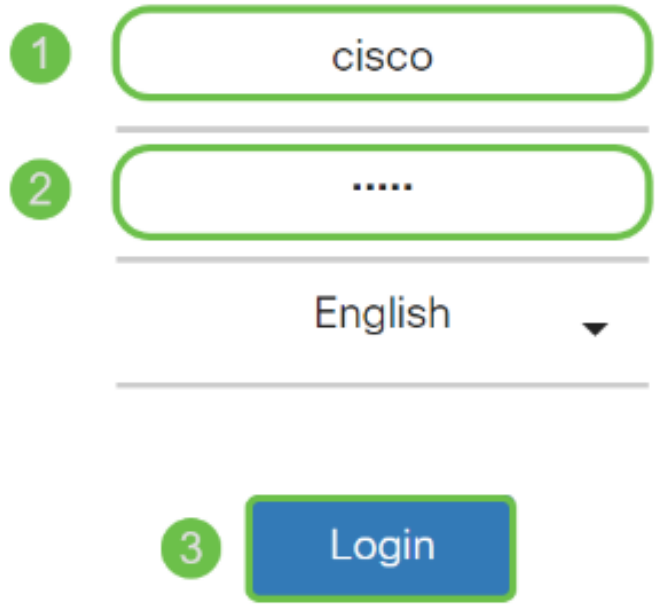


Paso 4

Cuando aparezca la página de inicio de sesión, introduzca 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 routers VPN de la serie Cisco RV340.



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.

Solución de problemas de conexión a Internet

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

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

Si no hay conectividad, puede consultar este artículo sobre resolución de problemas.

Otras cosas que debe probar:

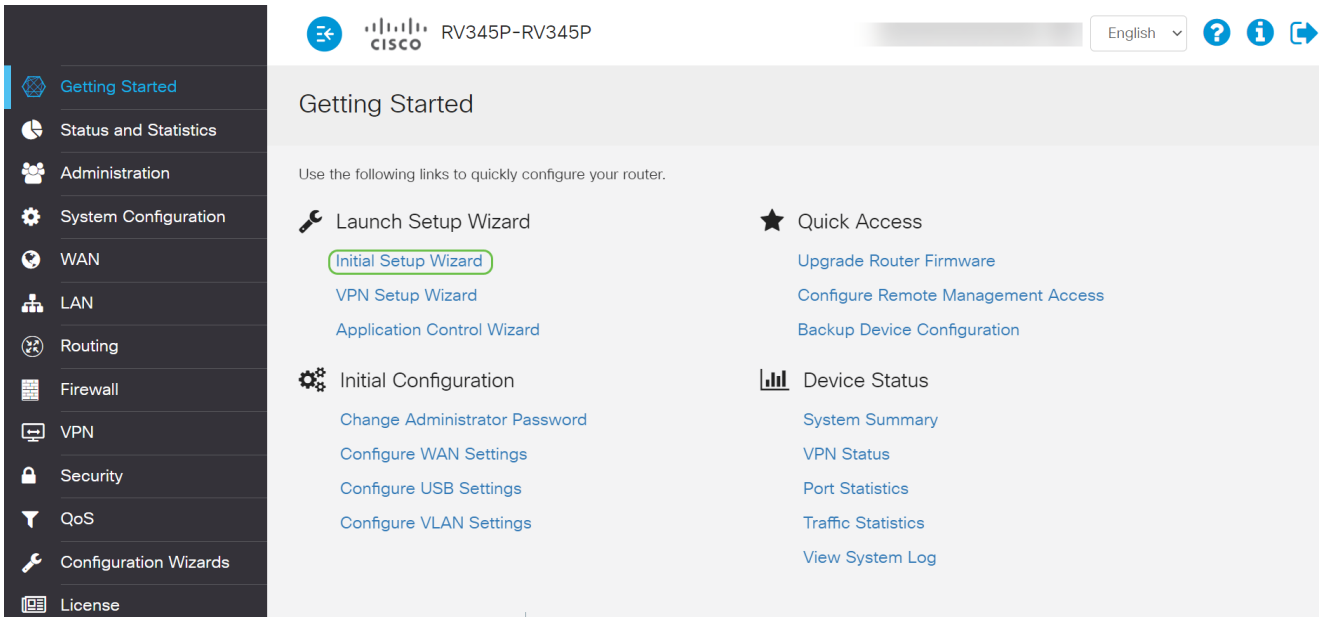
1. Compruebe que el explorador Web no está configurado para trabajar sin conexión.
2. Compruebe los parámetros de conexión de red de área local del adaptador Ethernet. El PC debe obtener una dirección IP mediante DHCP. Como alternativa, el PC puede tener una dirección IP estática en el intervalo 192.168.1.x con la puerta de enlace predeterminada establecida en 192.168.1.1 (la dirección IP predeterminada del RV345P). Para conectarse, puede que tenga que modificar los parámetros de red del RV345P. Si utiliza Windows 10, consulte las instrucciones de Windows 10 para modificar la configuración de la red.
3. Si tiene un equipo existente que ocupa la dirección IP 192.168.1.1, deberá resolver este conflicto para que la red funcione. Más información al final de esta sección, o haga clic aquí para ir directamente allí.
4. Reinicie el módem y el RV345P apagando ambos dispositivos. A continuación, encienda el módem y déjelo inactivo durante unos 2 minutos. Encienda el RV345P. Ahora debe recibir una dirección IP de WAN.
5. Si dispone de un módem DSL, solicite al ISP que ponga el módem DSL en modo puente.

Configuración inicial

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

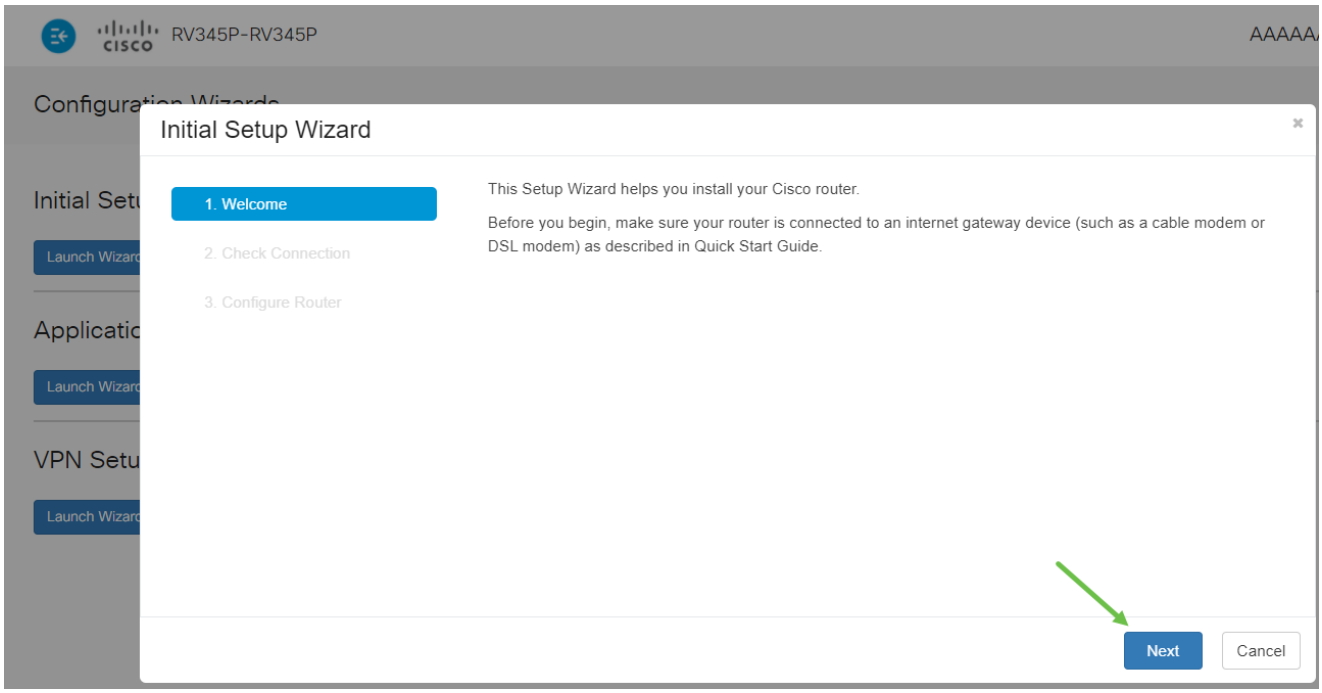
Paso 1

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



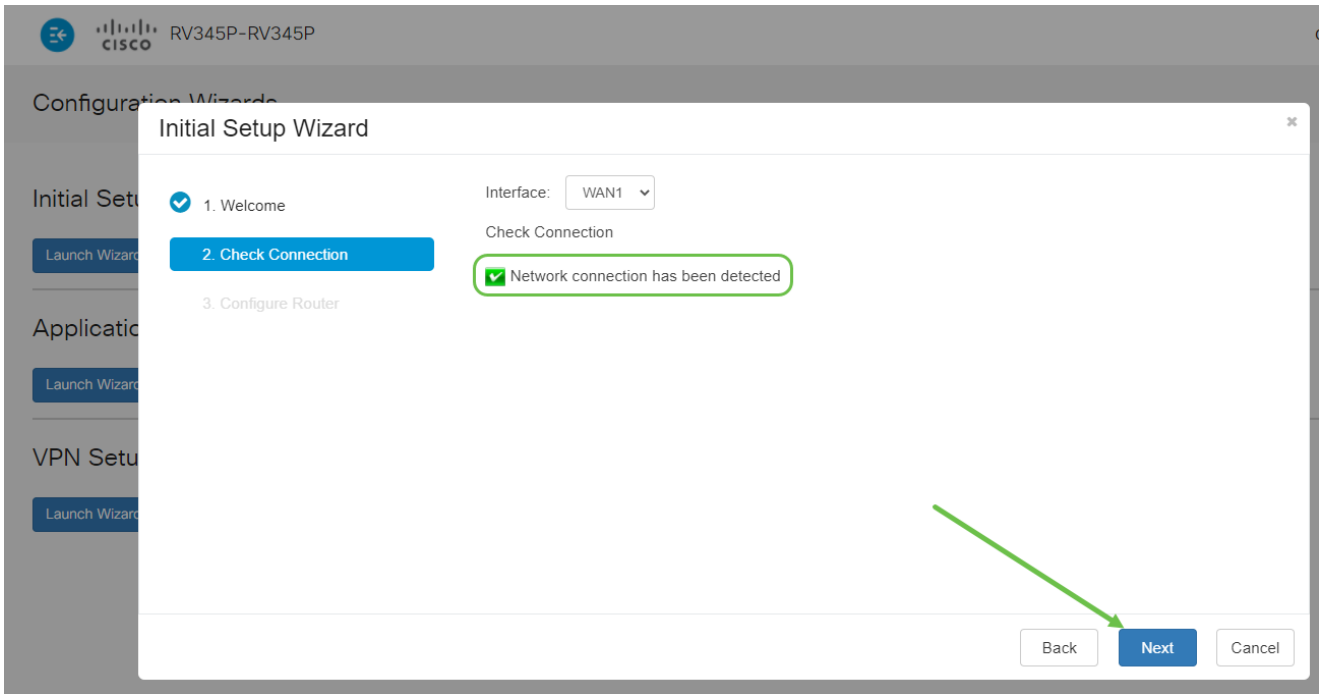
Paso 2

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



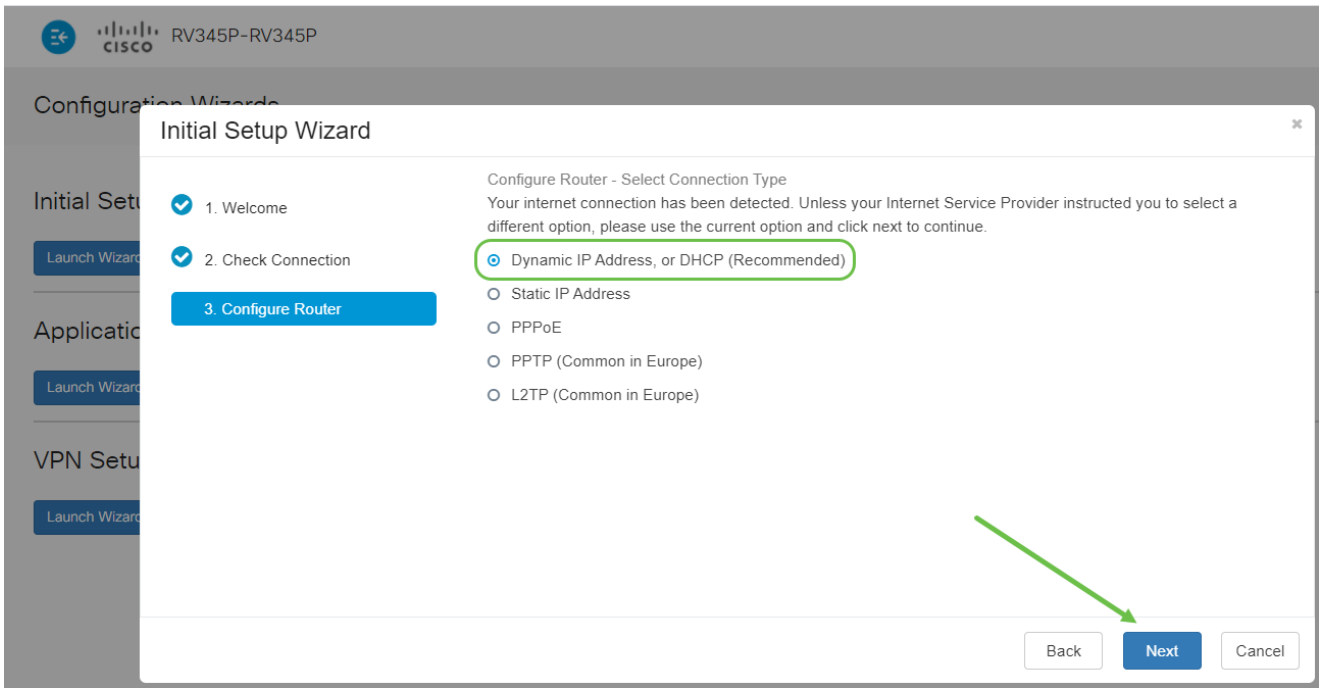
Paso 3

En este paso se explican los pasos básicos para asegurarse de que el router está conectado. Como ya lo ha confirmado, haga clic en Next.



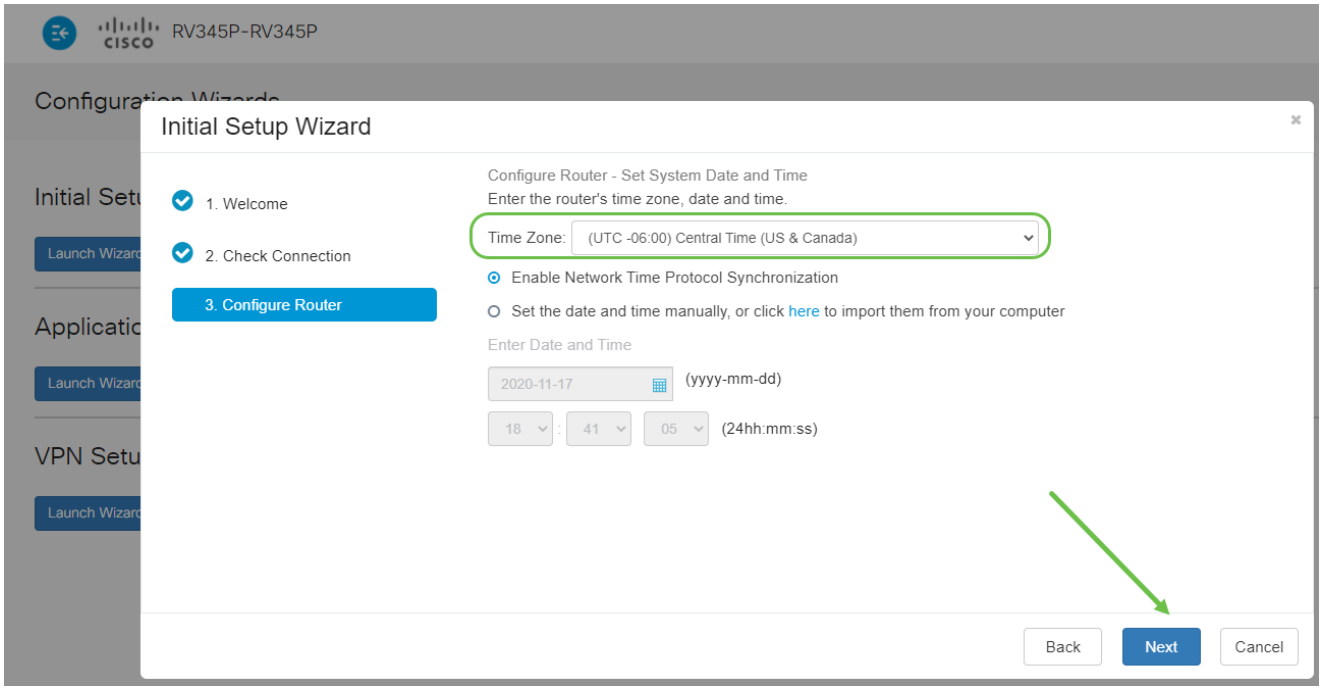
Paso 4

En la siguiente pantalla se muestran las opciones para asignar direcciones IP al router. En este escenario, debe seleccionar DHCP. Haga clic en Next (Siguiente).



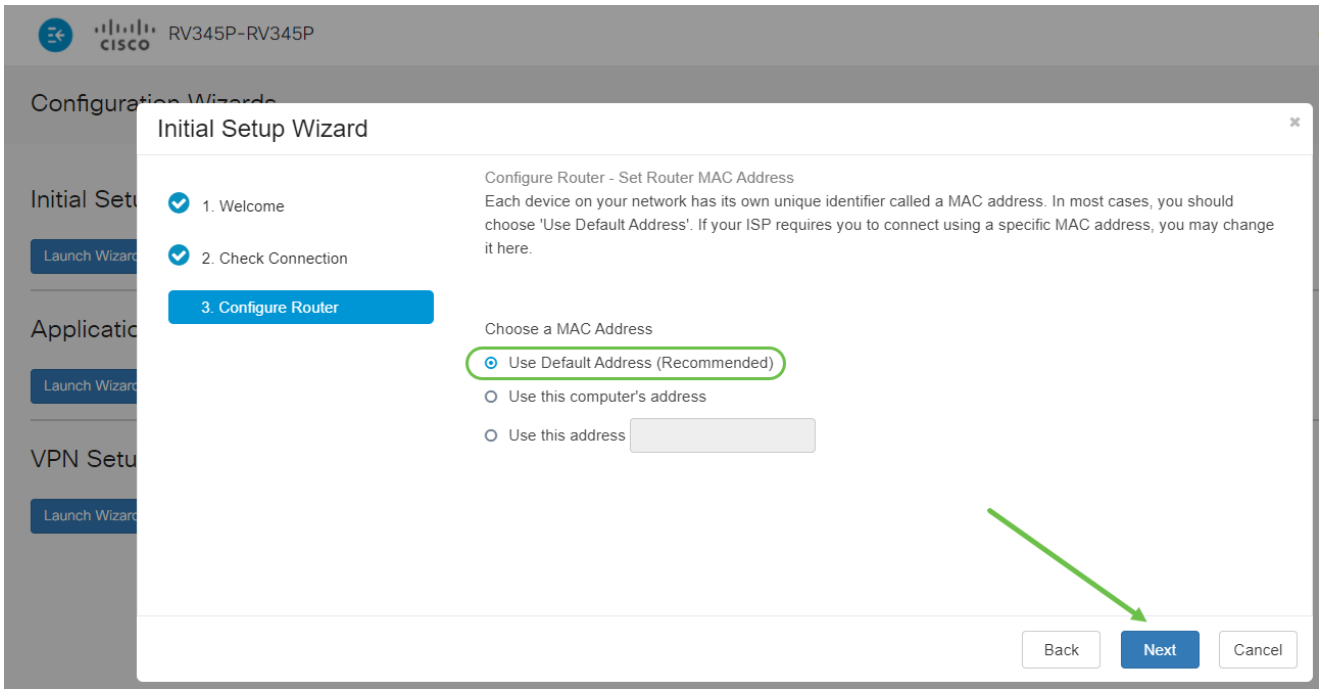
Paso 5

Se le solicitará que establezca los parámetros de hora del router. Esto es importante porque permite la precisión al revisar registros o solucionar problemas de eventos. Seleccione la zona horaria y haga clic en Next.



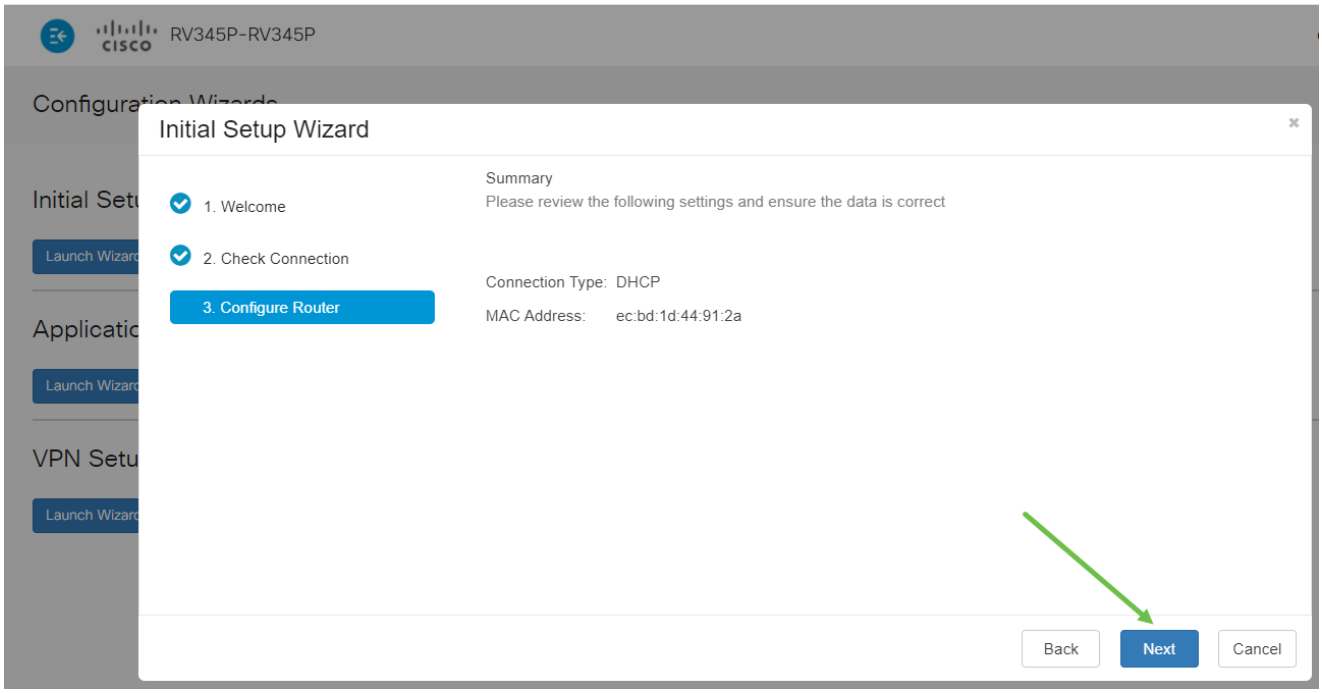
Paso 6

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



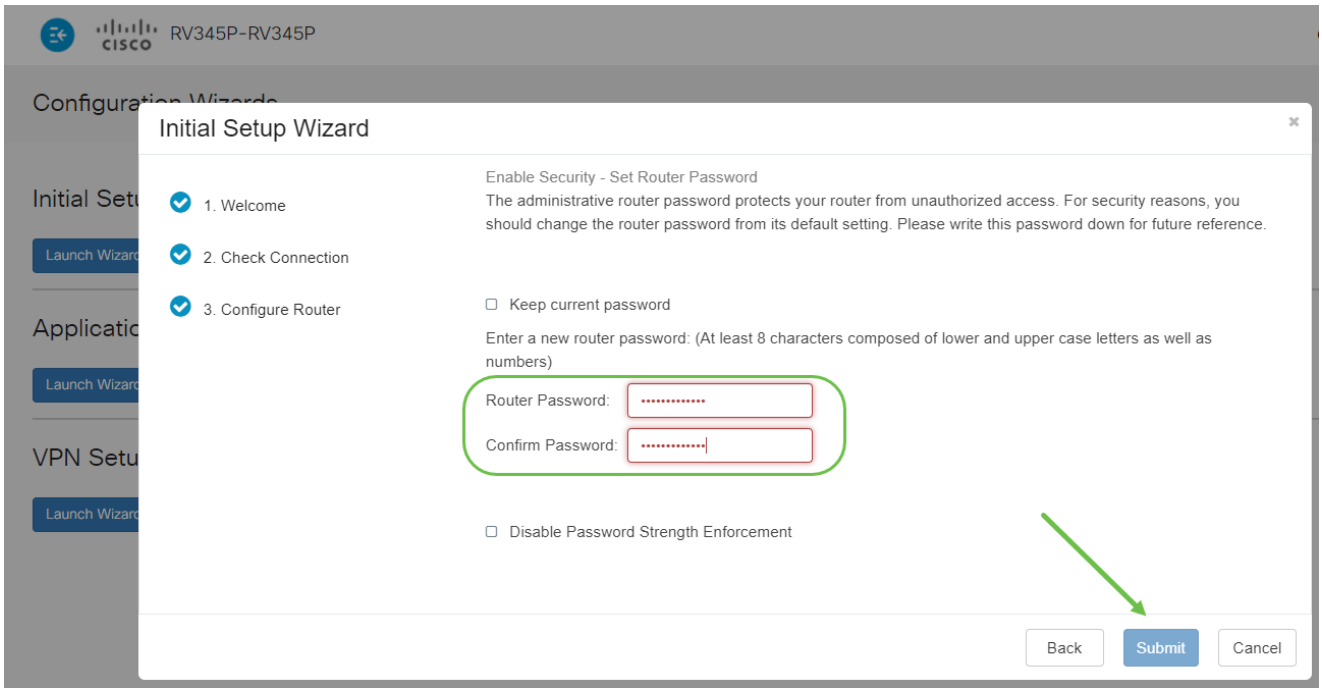
Paso 7

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



Paso 8

En el siguiente paso, seleccionará una contraseña que utilizará al iniciar sesión en el router. El estándar para las contraseñas es contener al menos 8 caracteres (mayúsculas y minúsculas) e incluir números. Introduzca una contraseña que cumpla los requisitos de seguridad. Haga clic en Next (Siguiente). Tome nota de su contraseña para futuros inicios de sesión.



No se recomienda que seleccione Desactivar aplicación de seguridad 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 la descifraran.

Paso 9

Haga clic en el icono de guardar.

Si desea obtener más información sobre estos parámetros, puede leer Configure DHCP WAN Settings (Configurar parámetros WAN DHCP) en el router RV34x.

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

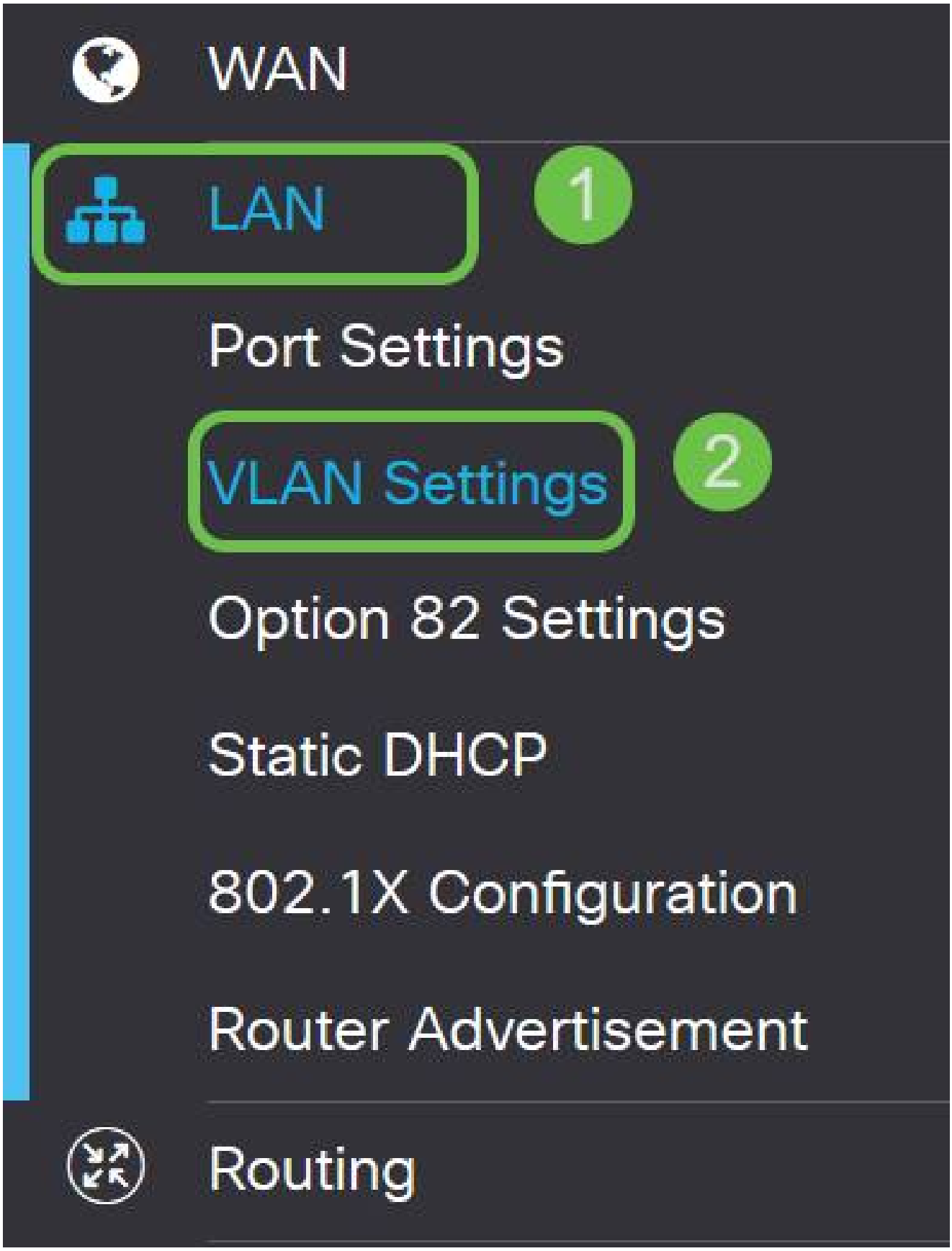
Edite una dirección IP si es necesario (opcional)

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

Este proceso solo es necesario si la dirección IP del router debe asignarse a una dirección específica de la red existente. Si no necesita editar una dirección IP, puede pasar a la siguiente sección de este artículo.

Paso 1

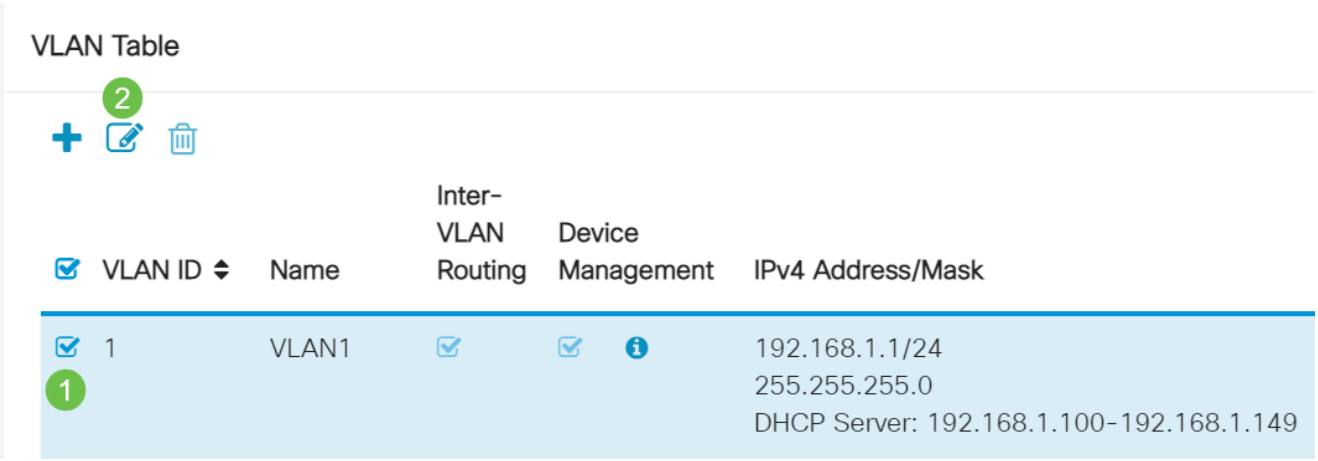
En el menú de la izquierda, haga clic en LAN > VLAN Settings.



Paso 2

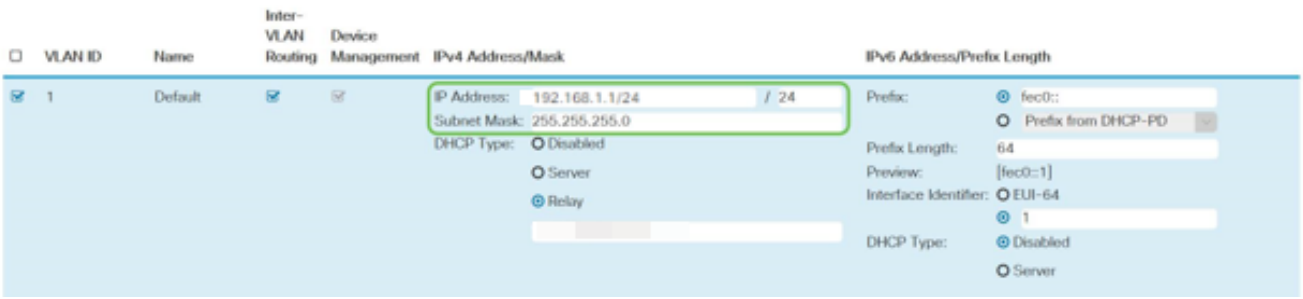
Seleccione la VLAN que contiene su dispositivo de ruteo, luego haga clic en el icono de

edición.



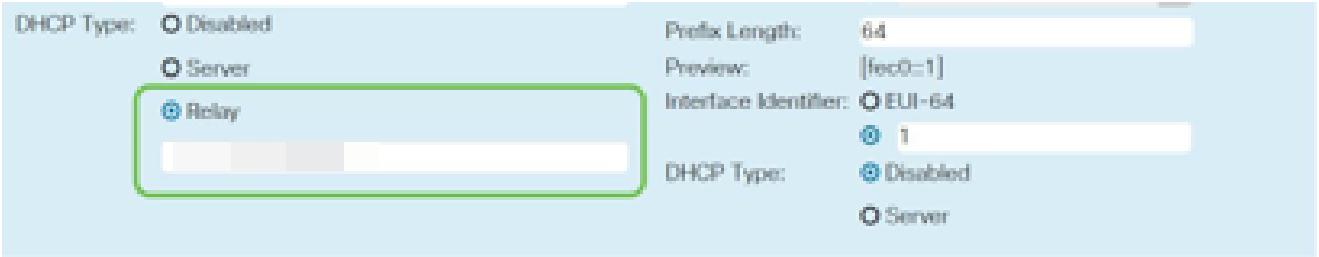
Paso 3

Ingrese la dirección IP estática que desee y haga clic en Apply 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 (Retransmisión DHCP) para dirigir las solicitudes DHCP a una dirección IP específica. Es probable que la dirección IP sea el router conectado a la WAN/Internet.

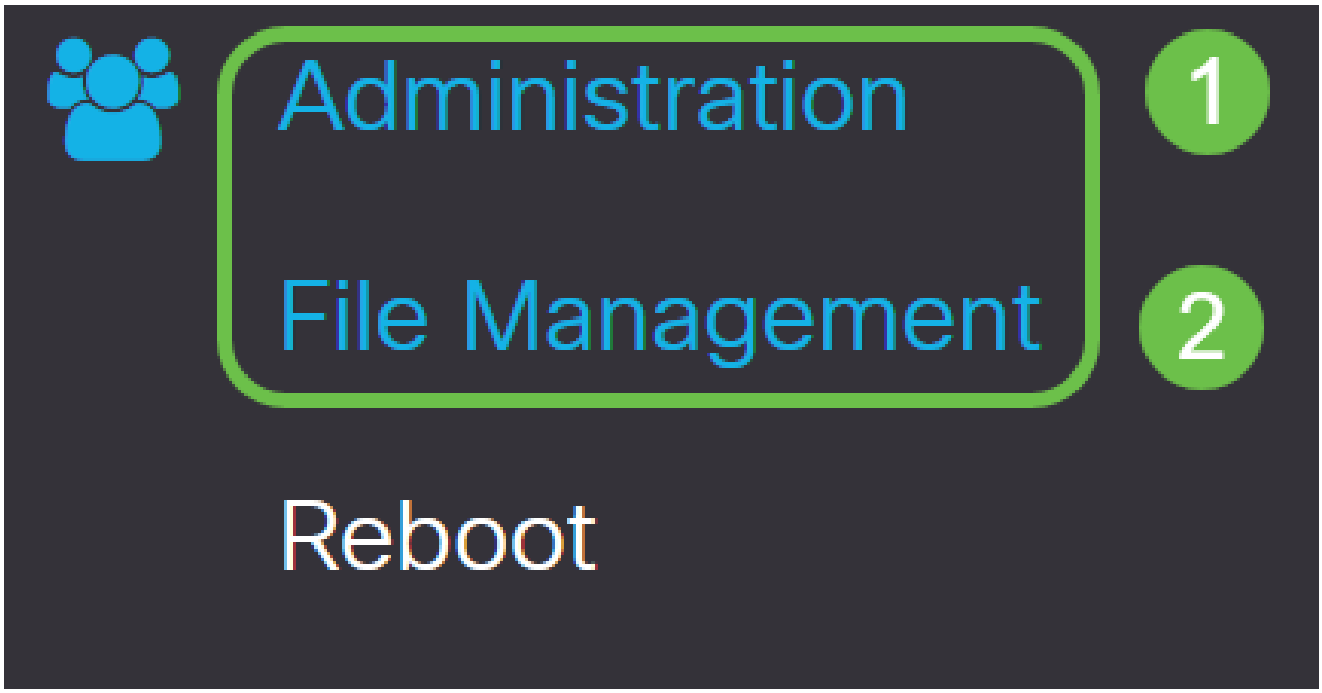


Actualice el firmware si es necesario

Se trata de un paso importante, ¡no se lo pierda!

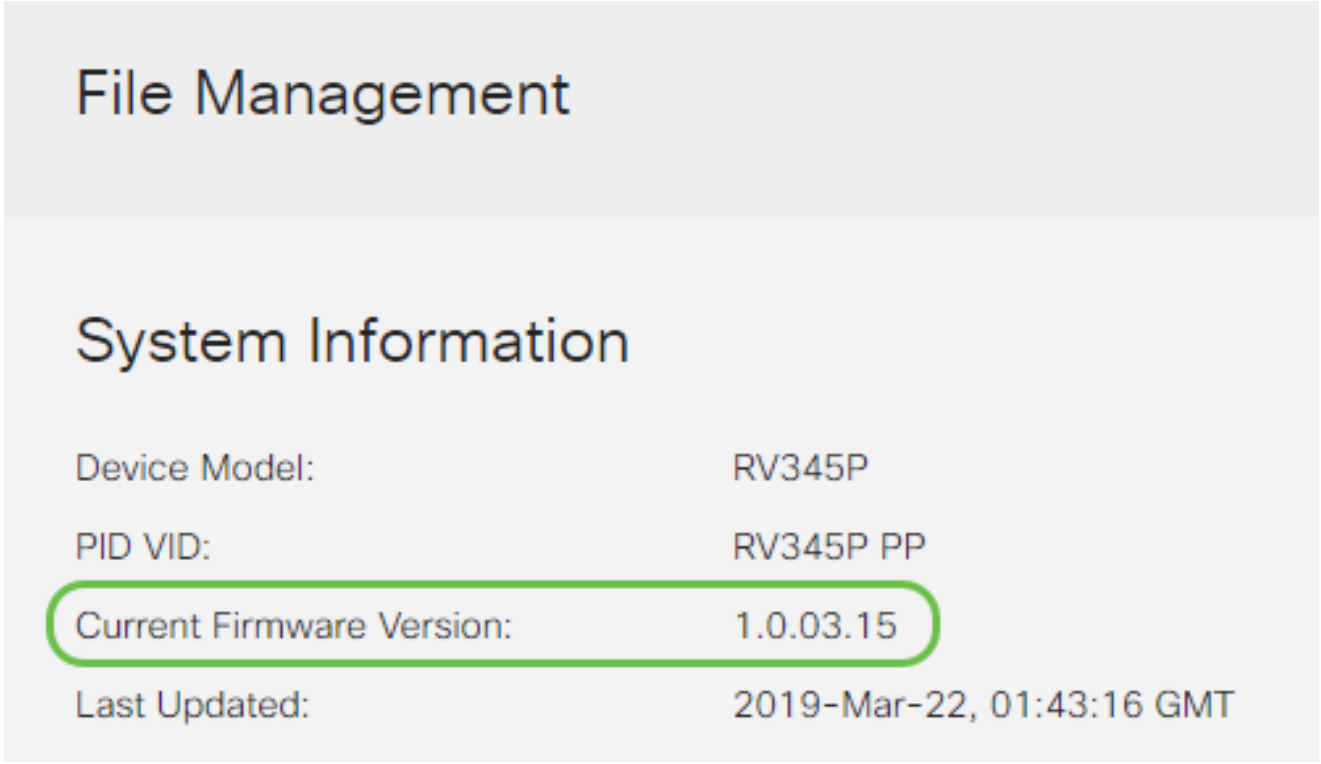
Paso 1

Elija Administration > File Management.



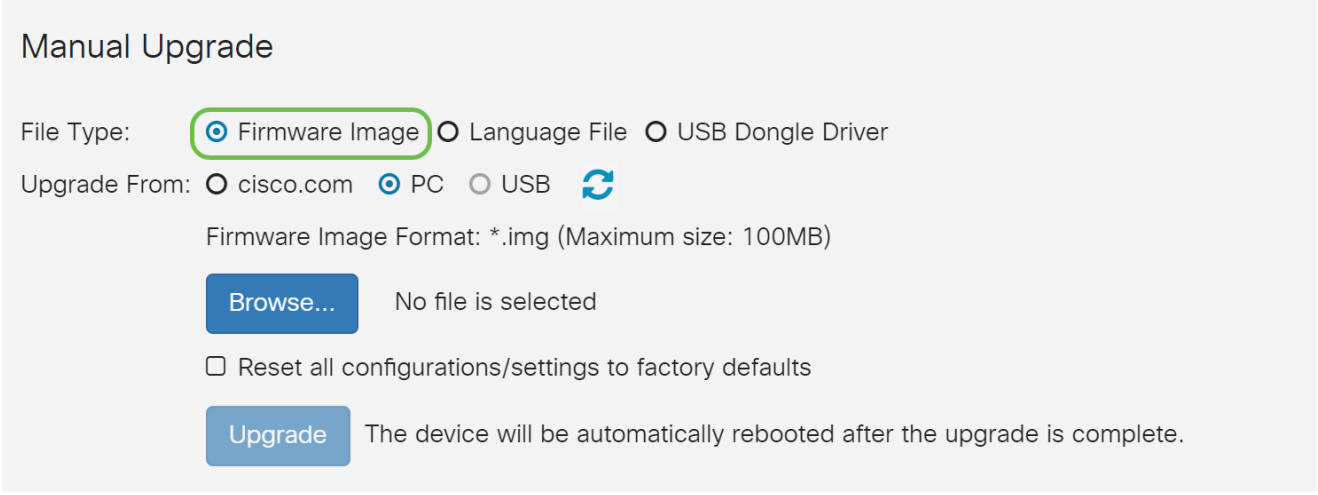
En el área Información del sistema, las siguientes subáreas describen lo siguiente:

- Device Model (Modelo de dispositivo): Muestra el modelo del dispositivo.
- PID VID: ID de producto e ID de proveedor del router.
- Versión de firmware actual: 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

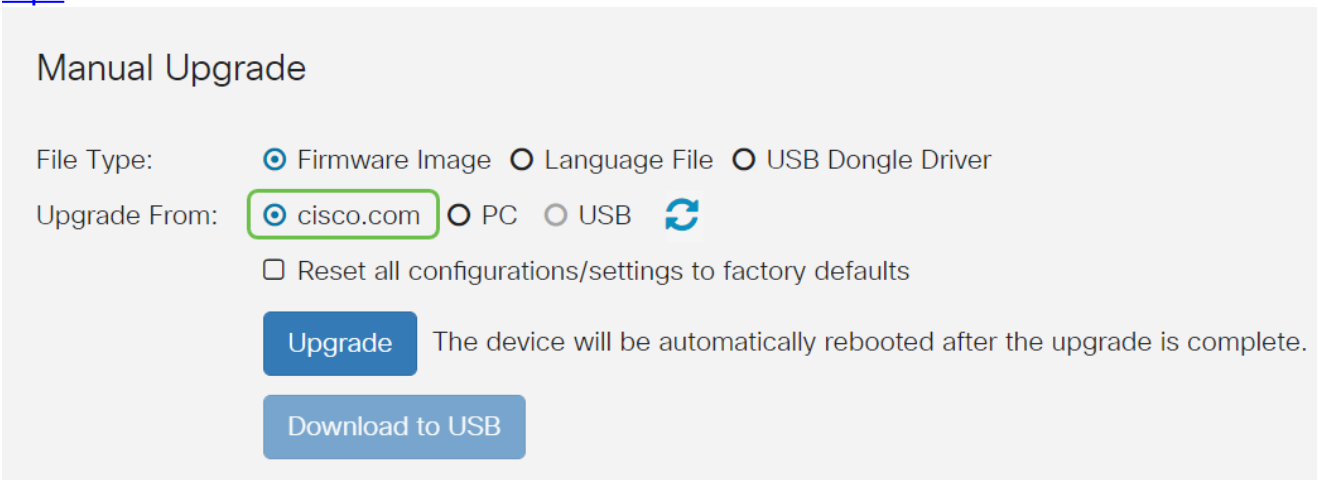
En la sección Actualización manual, haga clic en el botón de opción Imagen del firmware para Tipo de archivo.



Paso 3

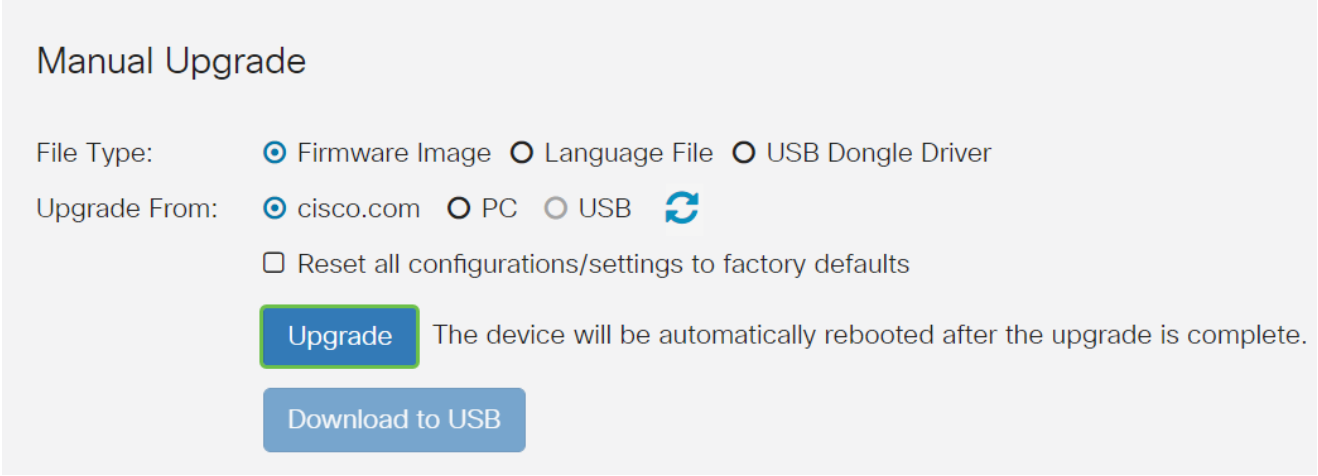
En la página Manual Upgrade, haga clic en el botón de opción para seleccionar cisco.com. Hay algunas otras opciones para esto, pero esta es la manera más fácil de hacer una actualización. Este proceso instala el archivo de actualización más reciente directamente desde la página web de descargas de software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

Si el dispositivo no está conectado a Internet o sufre desconexiones de Internet, no podrá actualizar desde cisco.com. Si esto le concierne, puede encontrar opciones alternativas aquí.



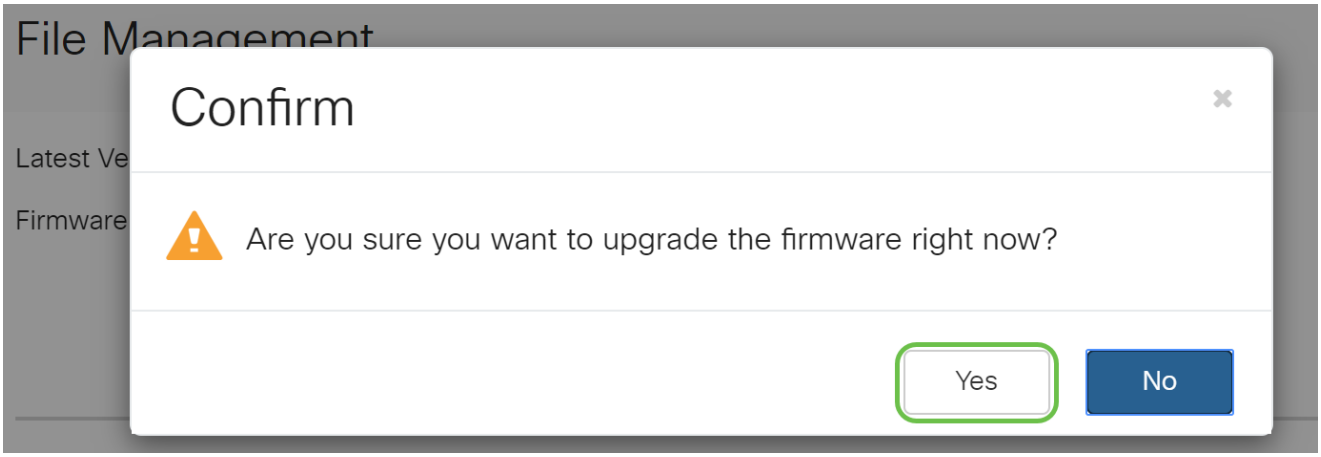
Paso 4

Haga clic en Upgrade.

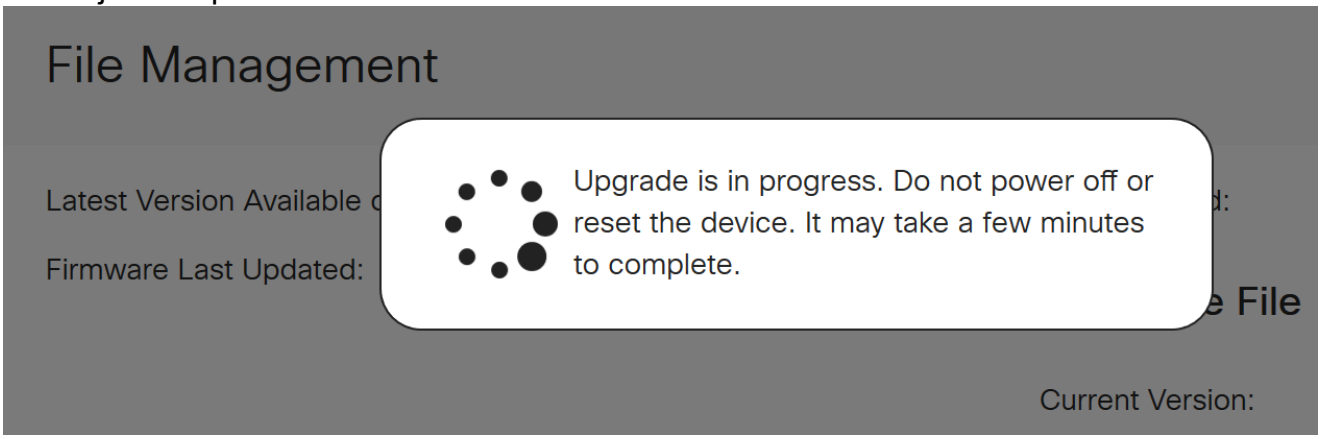


Paso 5

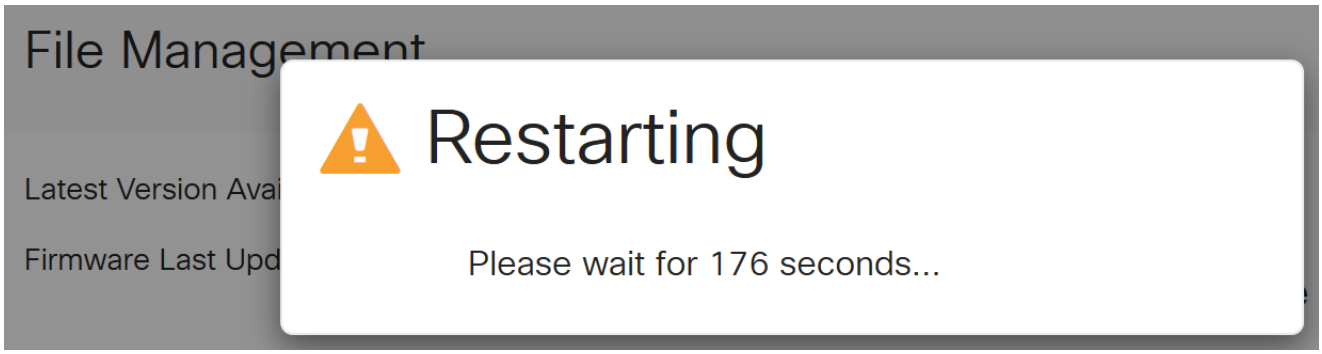
Haga clic en Yes en la ventana de confirmación para continuar.



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

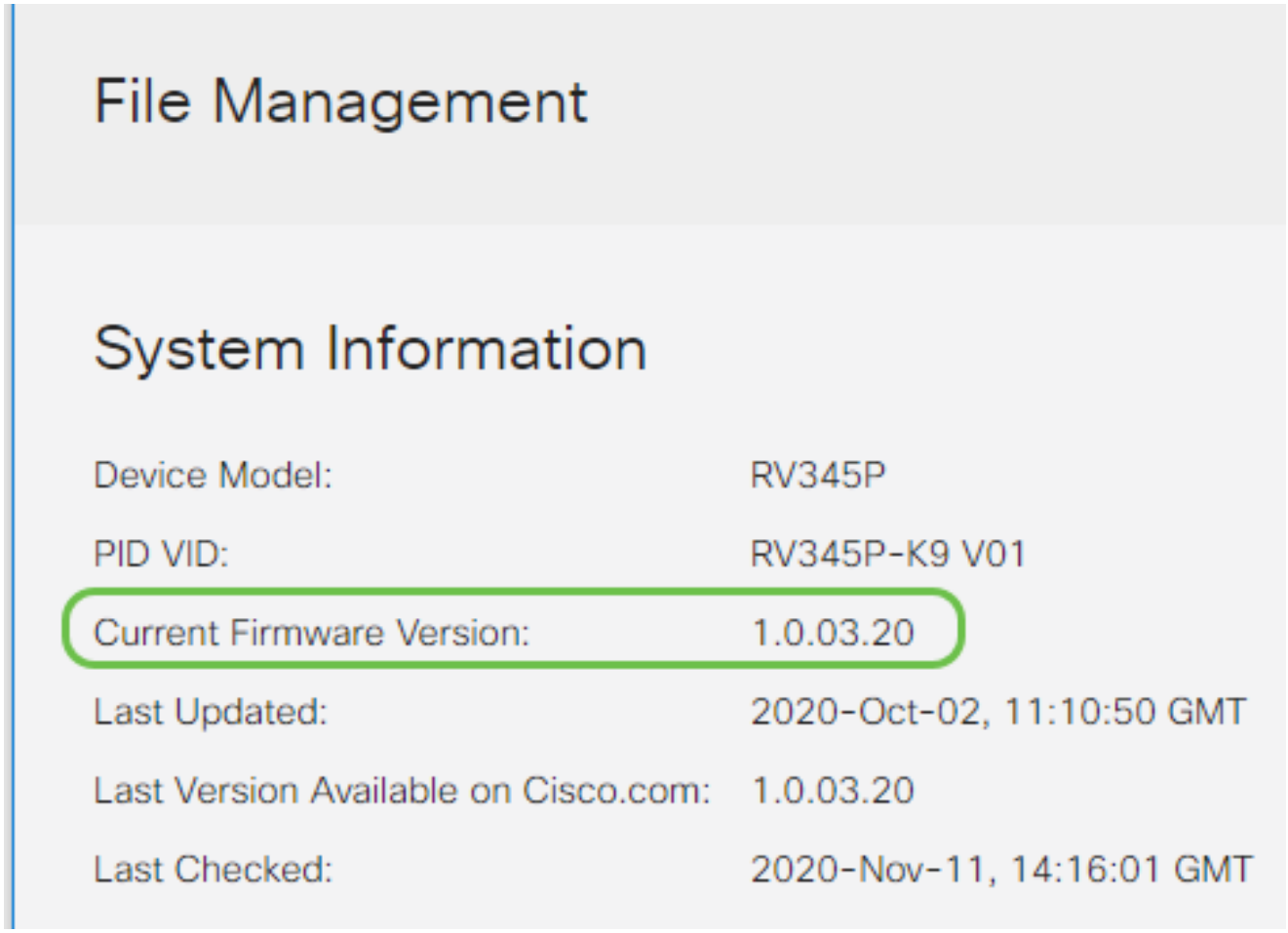


Una vez que se haya completado la actualización, aparecerá una ventana de notificación que le informará que el router se reiniciará con una cuenta atrás del tiempo estimado para que finalice el proceso. A continuación, se cerrará su sesión.



Paso 6

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



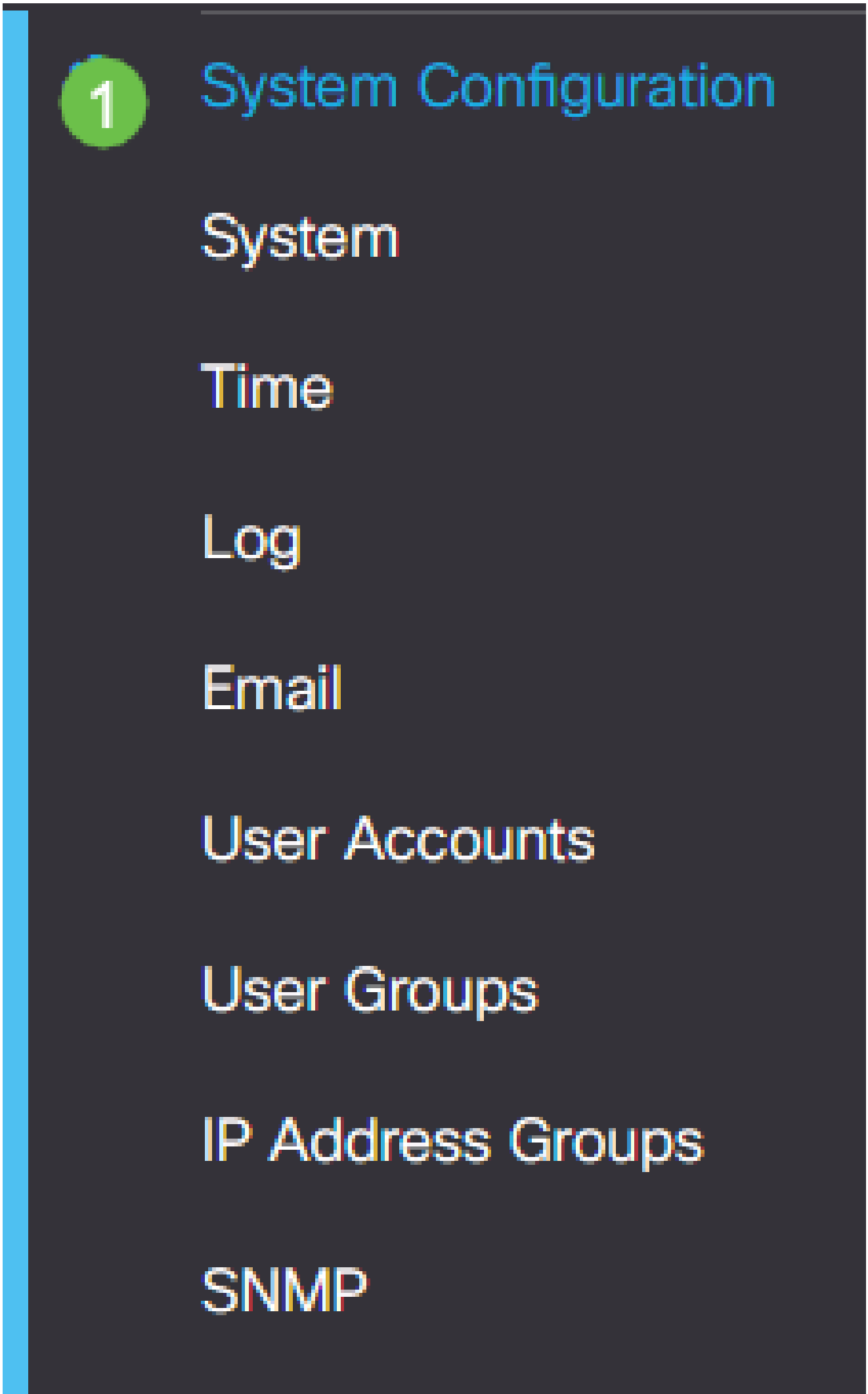
Configuración de actualizaciones automáticas en el router serie RV345P

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

Paso 1

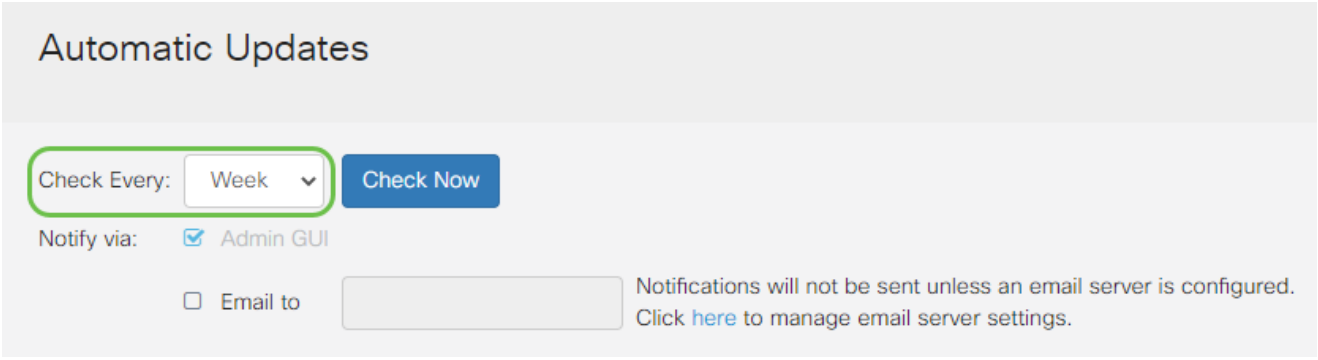
Inicie sesión en la utilidad basada en Web y seleccione System Configuration > Automatic

Updates.


1
System Configuration
System
Time
Log
Email
User Accounts
User Groups
IP Address Groups
SNMP

Paso 2

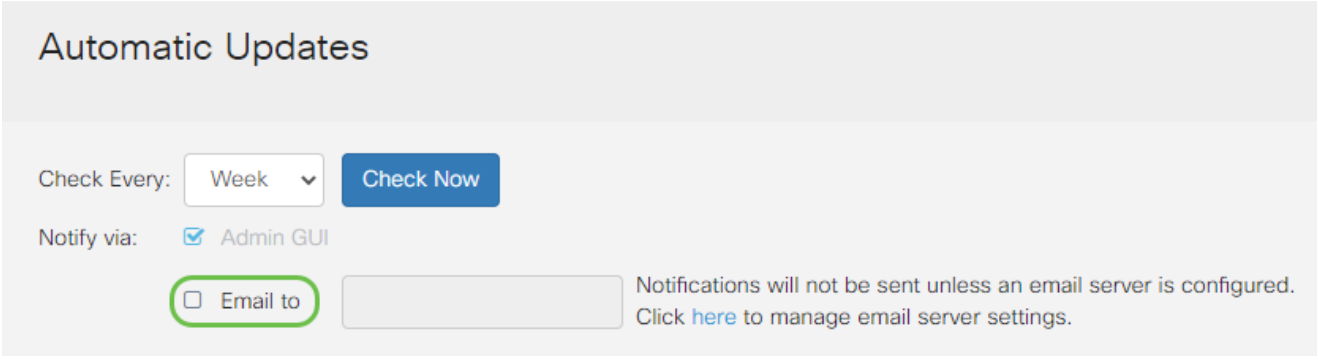
En la lista desplegable Comprobar cada, elija la frecuencia con la que el router debe buscar actualizaciones.



Paso 3

En el área Notificar vía, marque la casilla de verificación Enviar correo electrónico a para recibir actualizaciones por correo electrónico. La casilla de verificación Admin GUI está activada de forma predeterminada y no se puede desactivar. Una vez que haya una actualización disponible, aparecerá una notificación en la configuración basada en web.

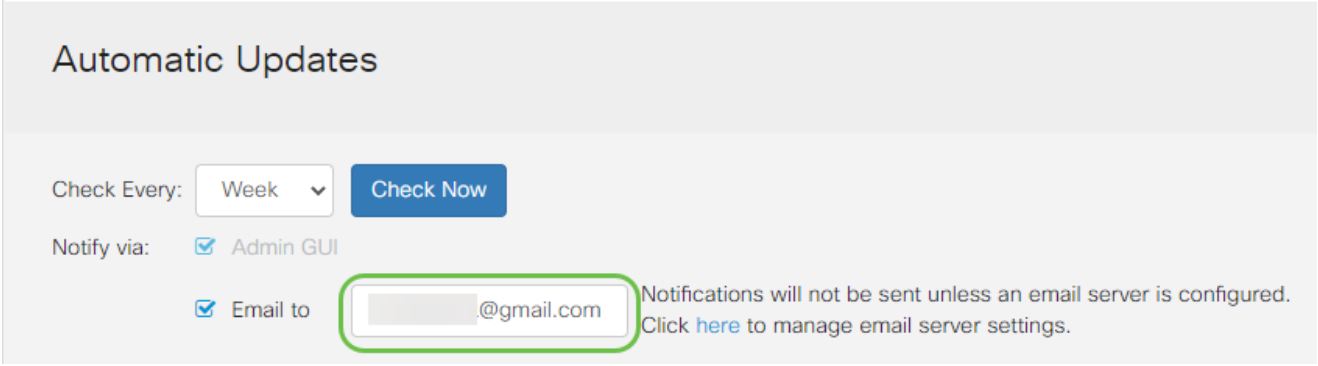
Si desea configurar los parámetros del servidor de correo electrónico, haga clic aquí para obtener más información.



Paso 4

Introduzca una dirección de correo electrónico en el campo Enviar correo electrónico a dirección.

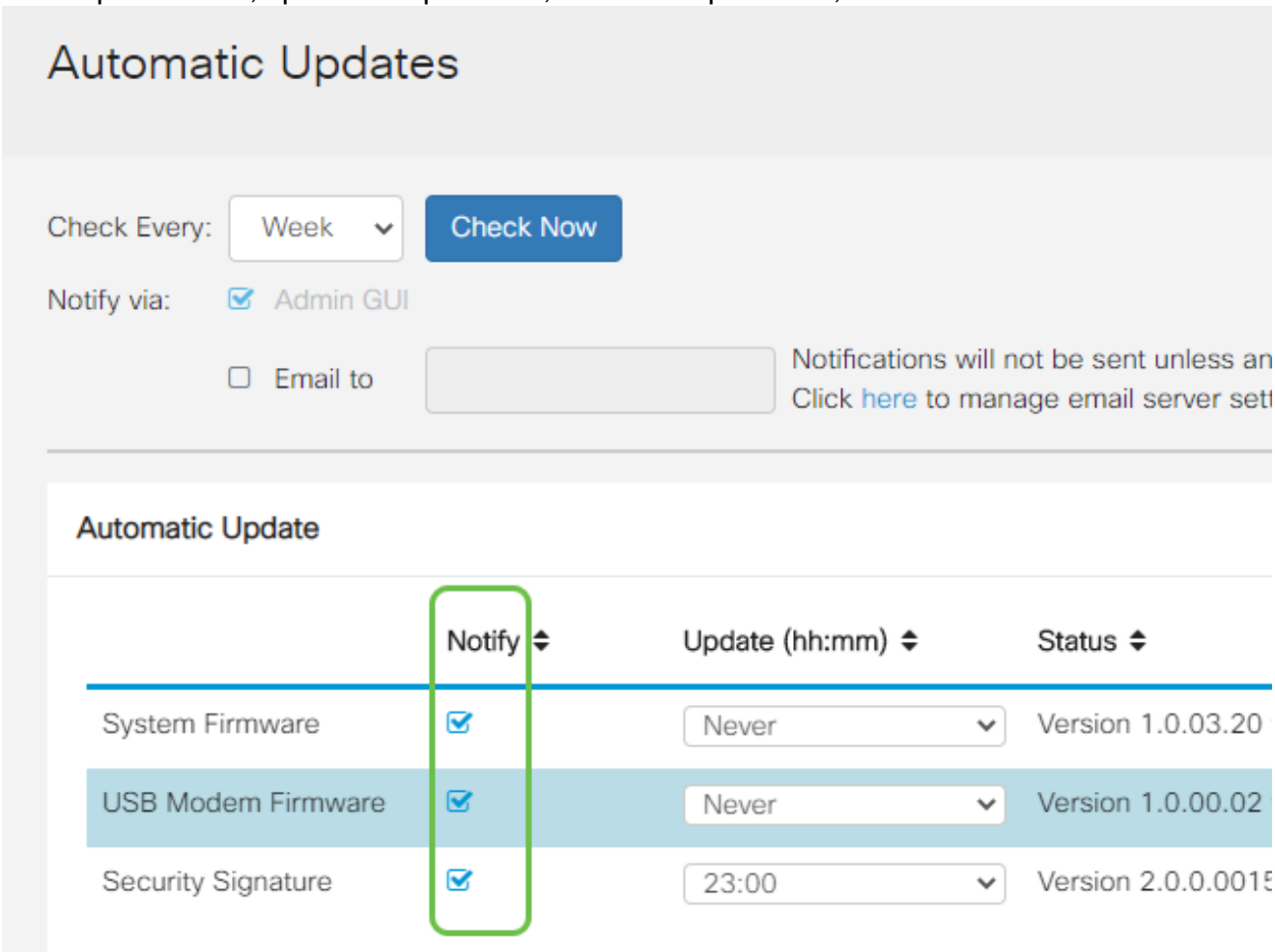
Se recomienda utilizar una cuenta de correo electrónico independiente en lugar de utilizar su correo electrónico personal para mantener la privacidad.



Paso 5

En el área Actualización automática, marque las casillas de verificación Notificar del tipo de actualizaciones sobre las que desea recibir notificaciones. Las opciones son:

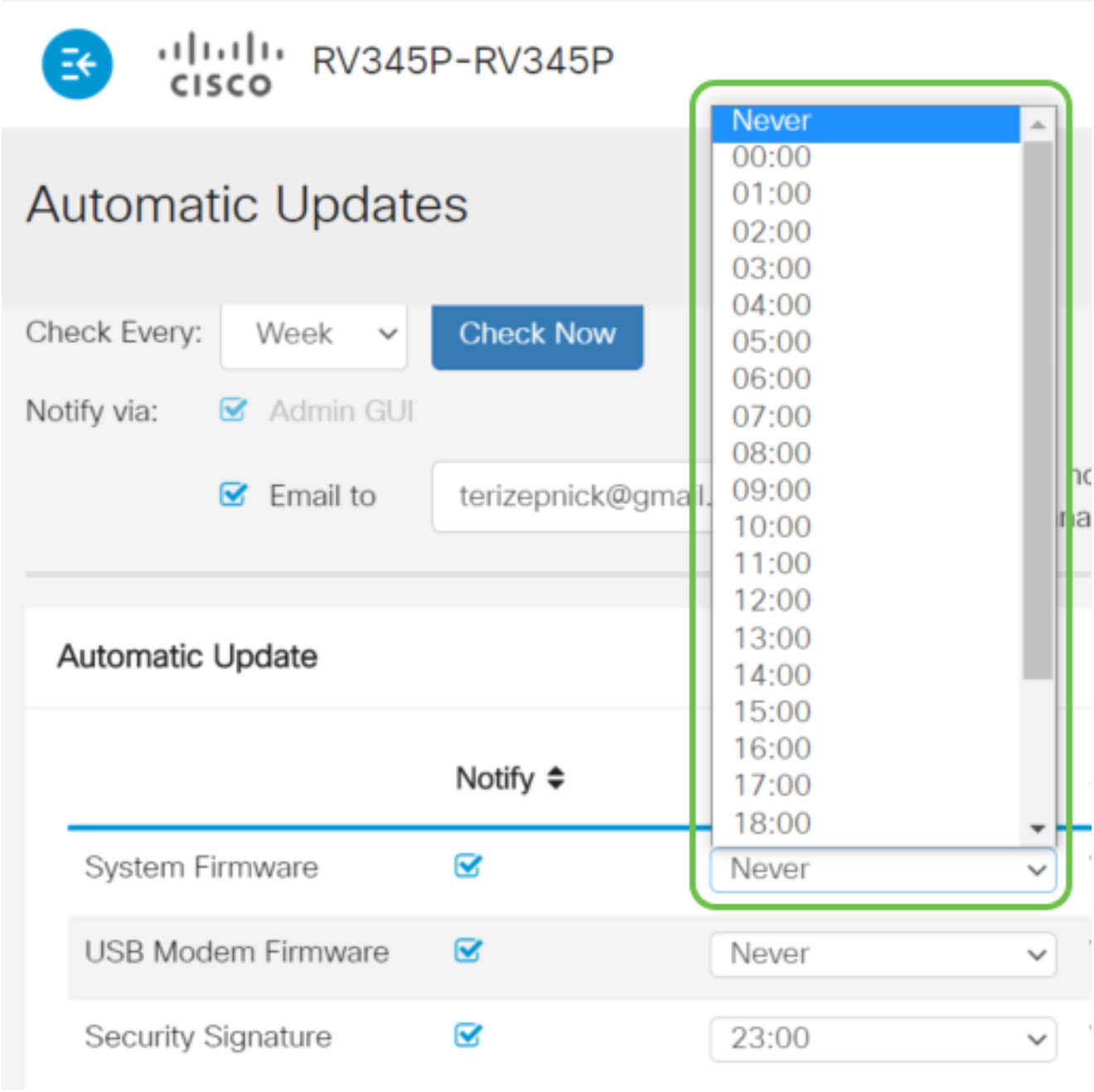
- Firmware del sistema: el programa de control principal del dispositivo.
- Firmware del módem USB: programa de control o controlador del puerto USB.
- Firma de seguridad: contendrá firmas para que el control de aplicaciones identifique aplicaciones, tipos de dispositivos, sistemas operativos, etc.



Paso 6

En la lista desplegable Actualización automática, elija la hora del día en la que desea que se

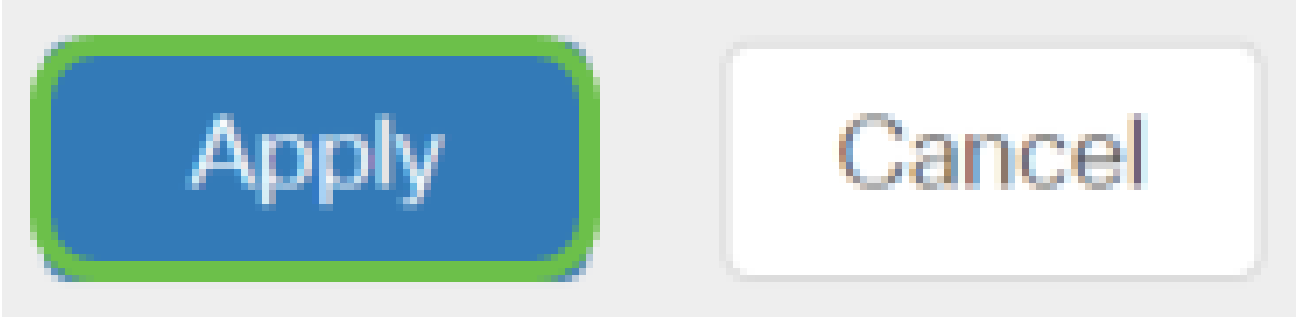
realice la actualización automática. Algunas opciones pueden variar según el tipo de actualización que haya elegido. La firma de seguridad es la única opción que dispone de una actualización inmediata. Se recomienda establecer una hora a la que la oficina esté cerrada para que el servicio no se interrumpa en un momento inconveniente.



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

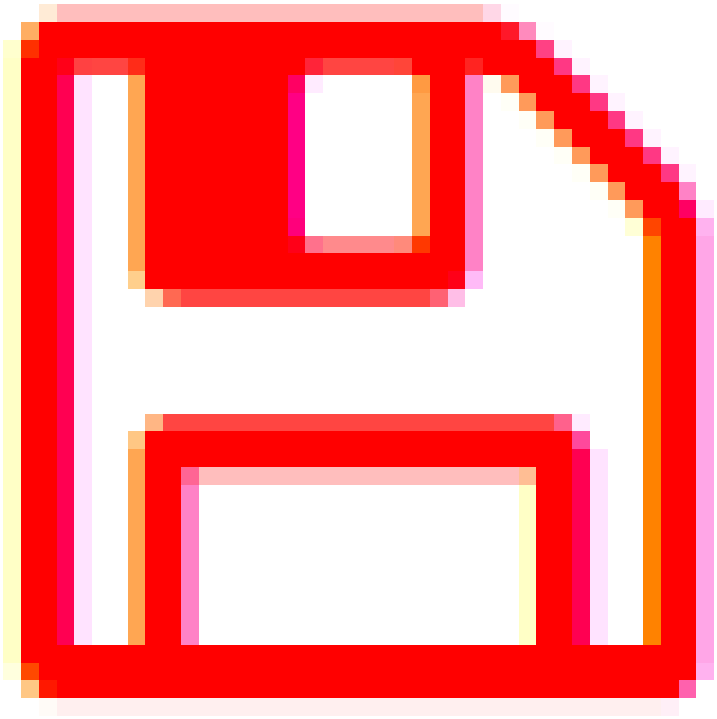
Paso 7

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 de guardar situado en la parte superior de la página.



Increíble, 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 protegida. Hay algunas opciones simples, como tener una contraseña compleja, pero si desea tomar medidas para una red aún más segura, consulte esta sección sobre seguridad.

Licencia de seguridad para autocaravanas (opcional)

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

- Sistema de prevención de intrusiones (IPS): inspecciona paquetes de red, registros o bloquea una amplia gama de ataques a la 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 en busca de varios protocolos, como HTTP, FTP, archivos adjuntos de correo electrónico SMTP, archivos adjuntos de correo electrónico POP3 y archivos adjuntos de correo electrónico IMAP que pasan a través del router.
- Seguridad web: aumenta la eficacia y la seguridad de la empresa mientras se conecta a Internet, permite políticas de acceso a Internet para dispositivos finales y aplicaciones de Internet para ayudar a garantizar el rendimiento y la seguridad. Está basado en la nube y contiene más de 80 categorías con más de 450 millones de dominios clasificados.
- Identificación de aplicaciones: identifique y asigne políticas a las aplicaciones de Internet. Se identifican automáticamente 500 aplicaciones únicas.
- Identificación de clientes: identifica y categoriza a los clientes de forma dinámica. Capacidad para asignar políticas basadas en la categoría del dispositivo final y el sistema operativo.

La licencia de seguridad RV proporciona filtrado web. El filtrado web es una función que permite administrar el acceso a sitios web inapropiados. Puede filtrar las solicitudes de acceso web de un cliente para determinar si permite o deniega dicho sitio web.

Las funciones de seguridad con licencia se pueden probar sin coste alguno durante 90 días. Si desea continuar utilizando las funciones de seguridad avanzada 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 ir directamente a la sección Umbrella.

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

Introducción a las cuentas inteligentes

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

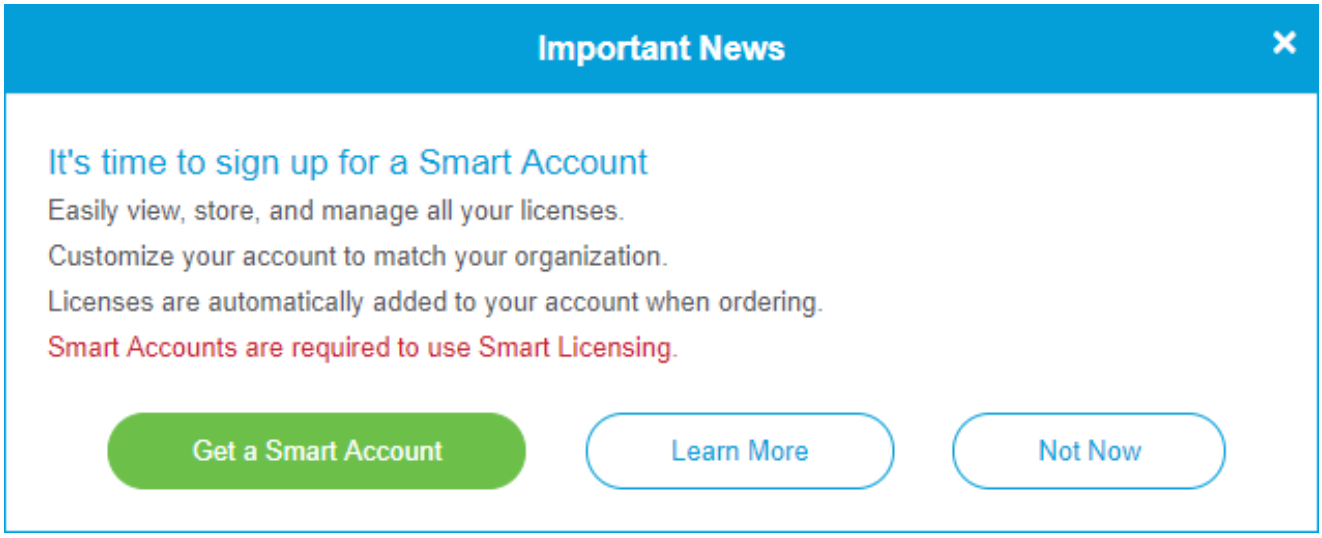
Al autorizar la activación de esta cuenta inteligente, acepta que está autorizado a crear cuentas y a administrar derechos de productos y servicios, acuerdos de licencia y acceso de usuario a cuentas en nombre de su organización. Los partners de Cisco no pueden autorizar

la creación de cuentas en nombre de los clientes.

La creación de una nueva cuenta inteligente es un evento único y la gestión a partir de ese momento se proporciona a través de la herramienta.

Crear una cuenta inteligente

Al acceder a su cuenta general de Cisco mediante su cuenta Cisco.com o ID de CCO (la que creó al principio de este documento), es posible que reciba un mensaje para crear una cuenta inteligente.



Si no ha visto esta ventana emergente, puede hacer clic para acceder a la página de creación de Smart Account. Es posible que deba iniciar sesión con sus credenciales de cuenta de Cisco.com.

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

Asegúrese de tomar nota del nombre de su cuenta junto con otros detalles de registro.

Consejo rápido: Si se le solicita que introduzca un dominio y no dispone de uno, puede introducir su dirección de correo electrónico en forma de name@domain.com. Los dominios comunes son gmail, yahoo, etc. dependiendo de su compañía 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 para autocaravanas.

Adquirir licencia de seguridad de RV

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

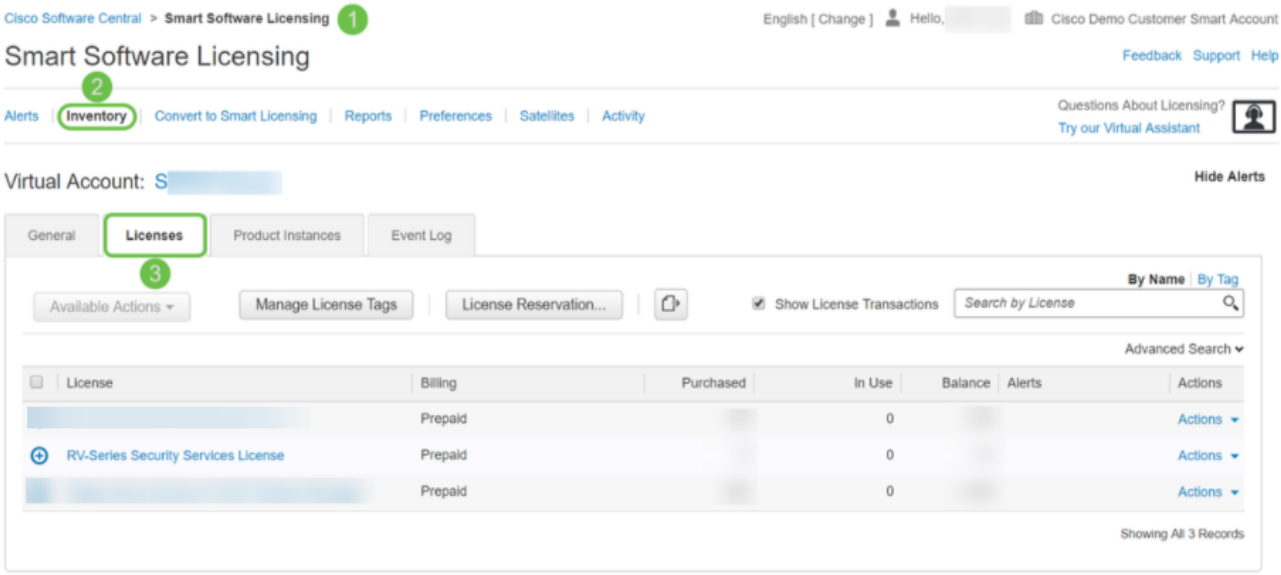
En la tabla siguiente se muestra el número de pieza de la licencia.

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

La clave de licencia no se introduce directamente en el router, sino que se asigna a la cuenta inteligente de Cisco después de solicitar la licencia. El tiempo que tarda la licencia en aparecer en su cuenta depende del momento en que el partner acepta el pedido y del momento en que el revendedor vincula las licencias a su cuenta, que suele ser de 24 a 48 horas.

Confirmar que la licencia está en la cuenta inteligente

Navegue hasta la página de su cuenta de Smart License y, a continuación, haga clic en Página de licencia de software inteligente > Inventario > Licencias.

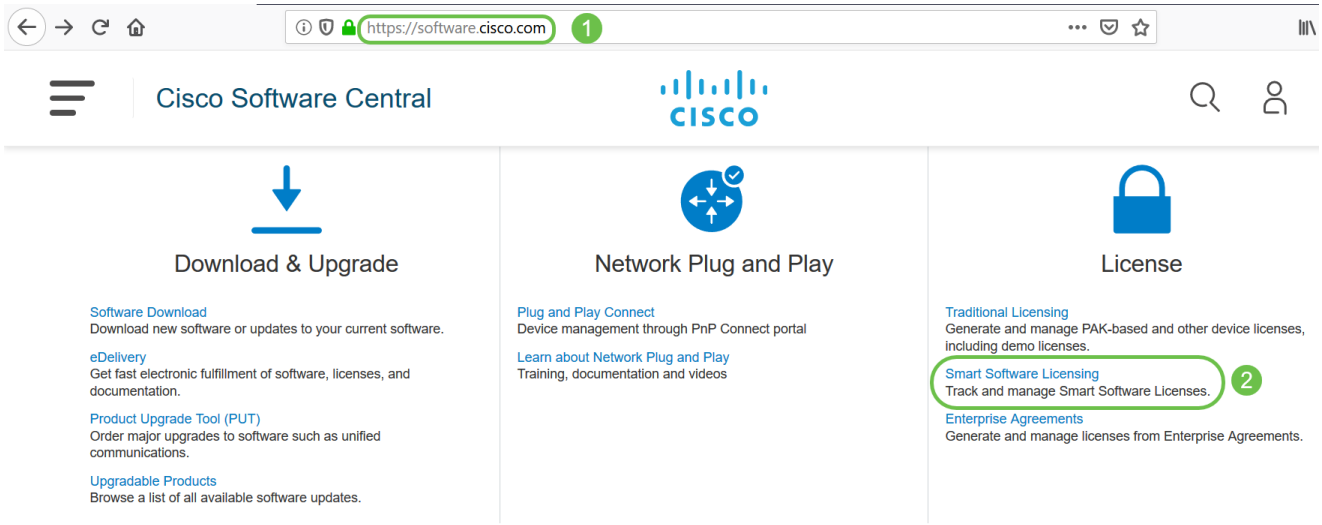


Si no ve su licencia en su cuenta Smart Account, póngase en contacto con su partner de Cisco.

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

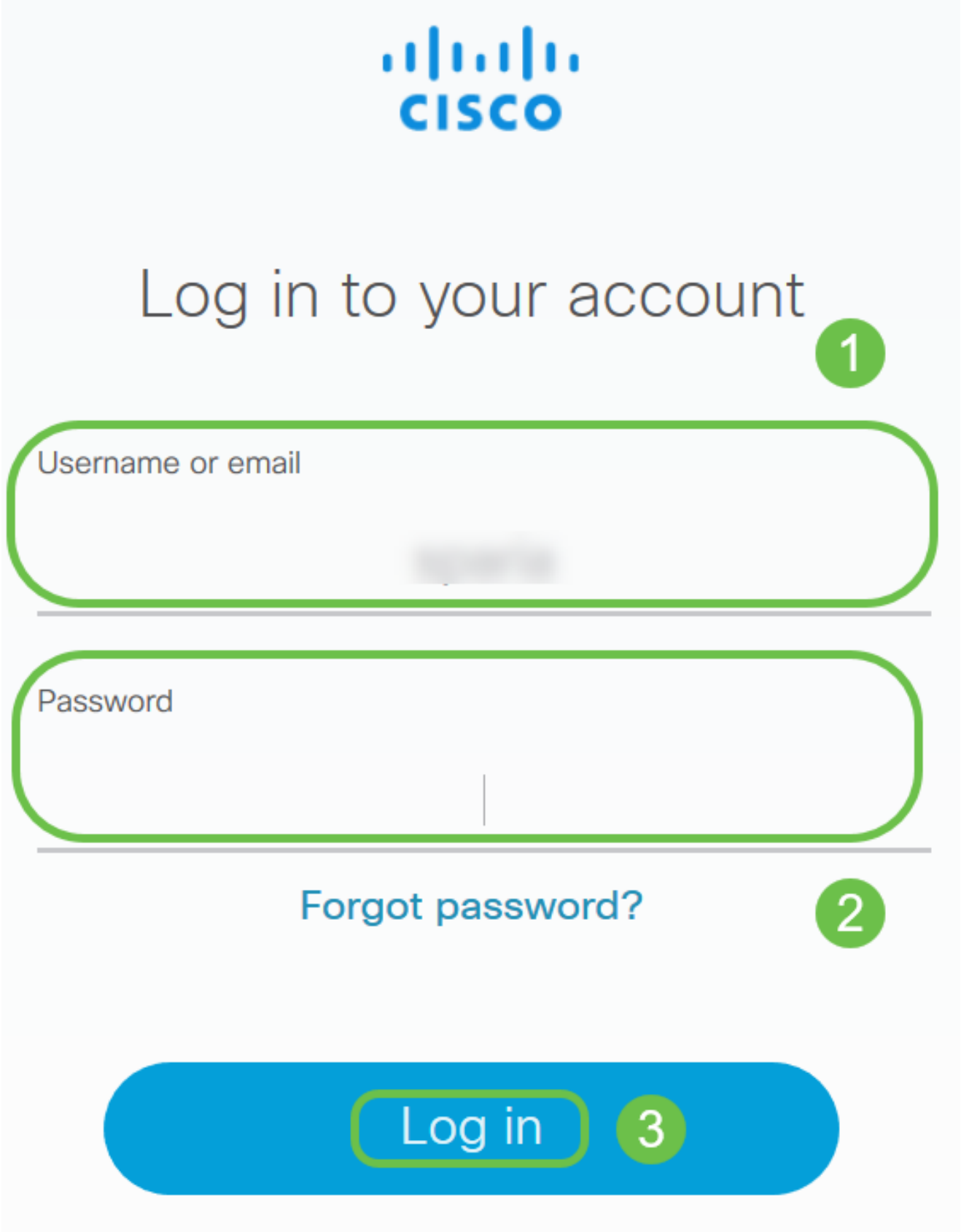
Paso 1

Acceda a Cisco Software y navegue hasta Smart Software Licensing.



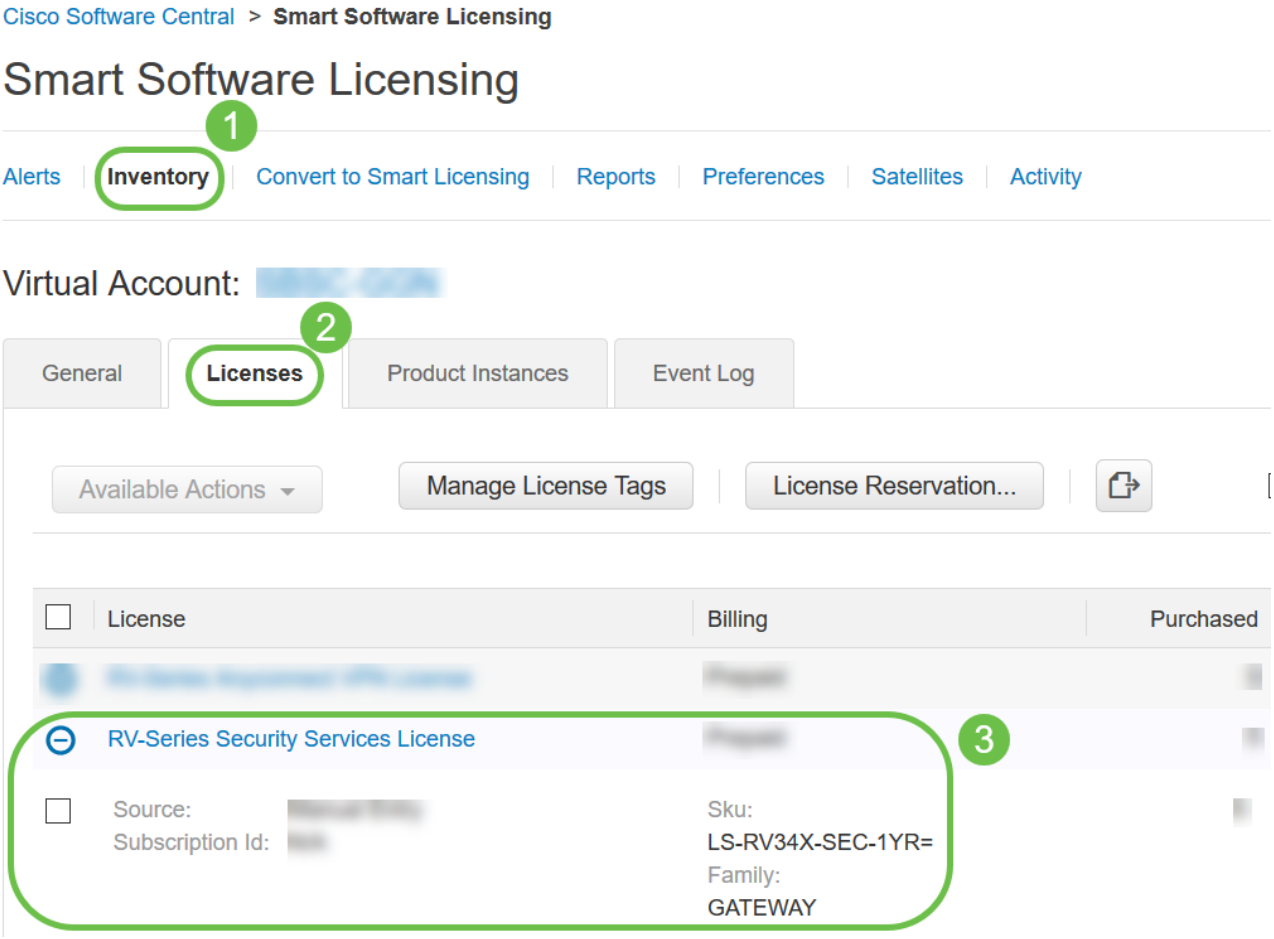
Paso 2

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



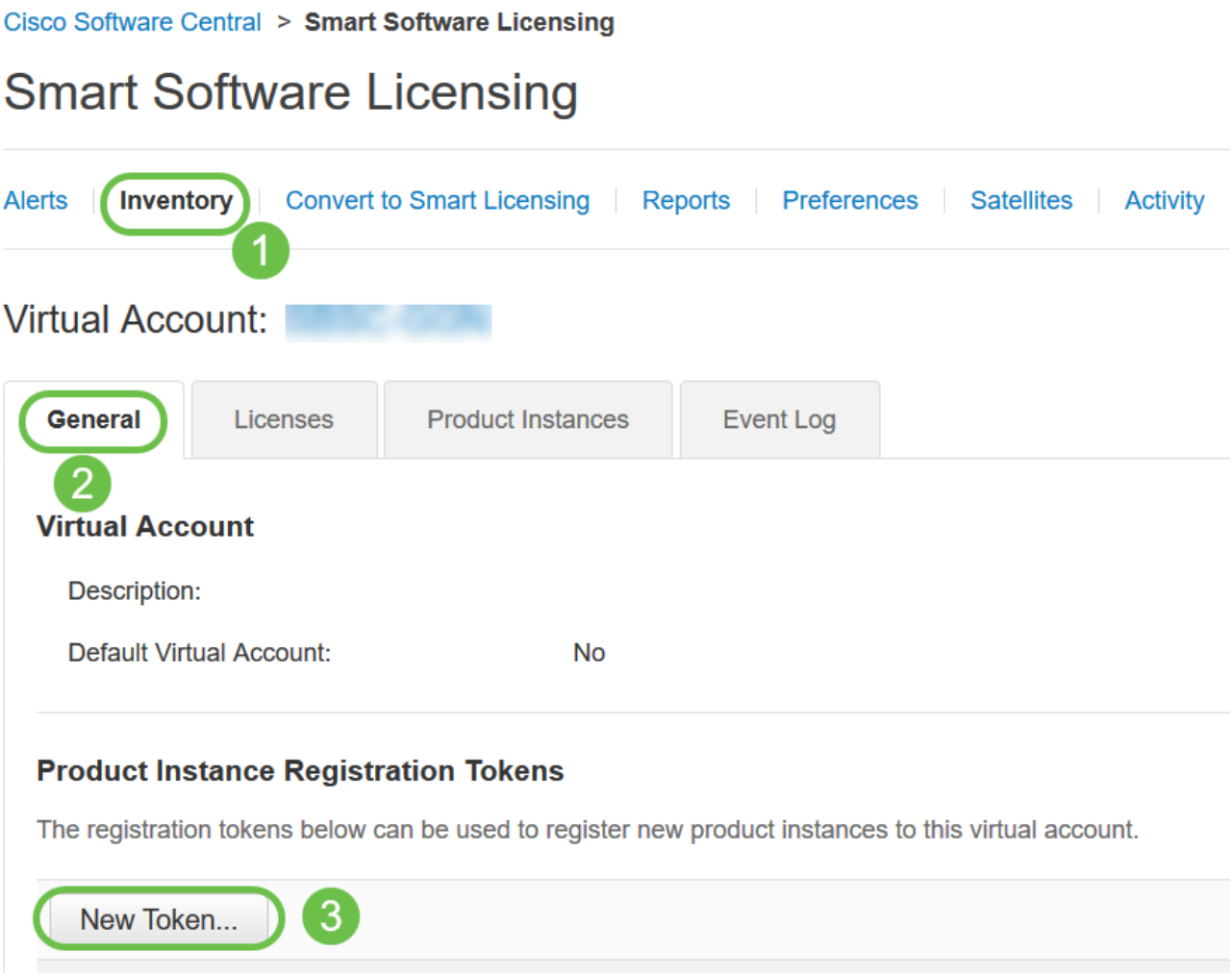
Paso 3

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 en la lista, póngase en contacto con su partner de Cisco.



Paso 4

Navegue hasta Inventario > General. En Product Instance Registration Tokens, haga clic en New Token.



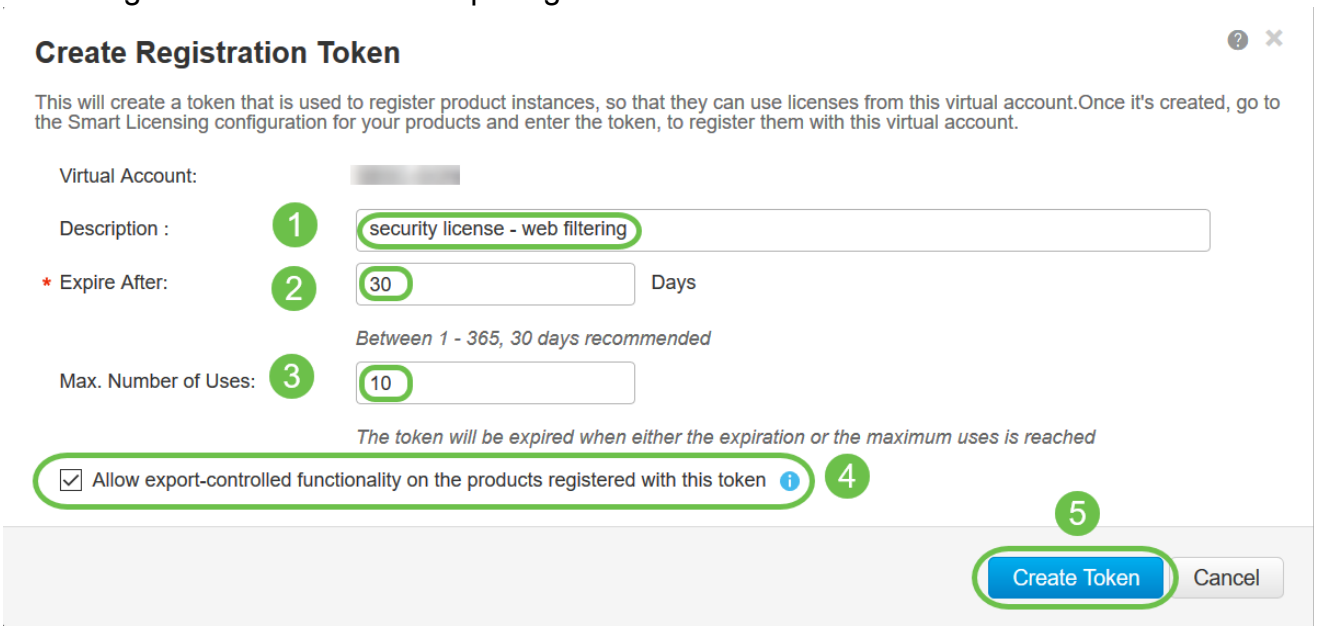
Paso 5

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

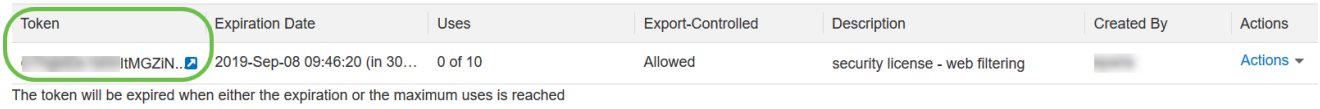
- En el campo Description (Descripción), introduzca una descripción única para el token. En este ejemplo, se introduce la licencia de seguridad: filtrado web.
- En el campo Caducar después de, introduzca un valor entre 1 y 365 días. Cisco recomienda el valor 30 días para este campo; sin embargo, puede editar el valor para que se ajuste a sus necesidades.
- En el campo Máx. Número de usuarios introduzca 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.
- Marque la casilla de verificación Permitir funcionalidad de exportación controlada en los productos registrados con este token para habilitar la funcionalidad de exportación controlada para los tokens de una instancia de producto en su cuenta virtual. Desmarque 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 de control de exportación. El Departamento de Comercio de los Estados Unidos restringe algunas funciones de exportación. Estas

funciones están restringidas para los productos registrados con este token cuando desmarque la casilla de verificación. Cualquier violación está sujeta a sanciones y cargos administrativos.

- Haga clic en Create Token para generar el token.

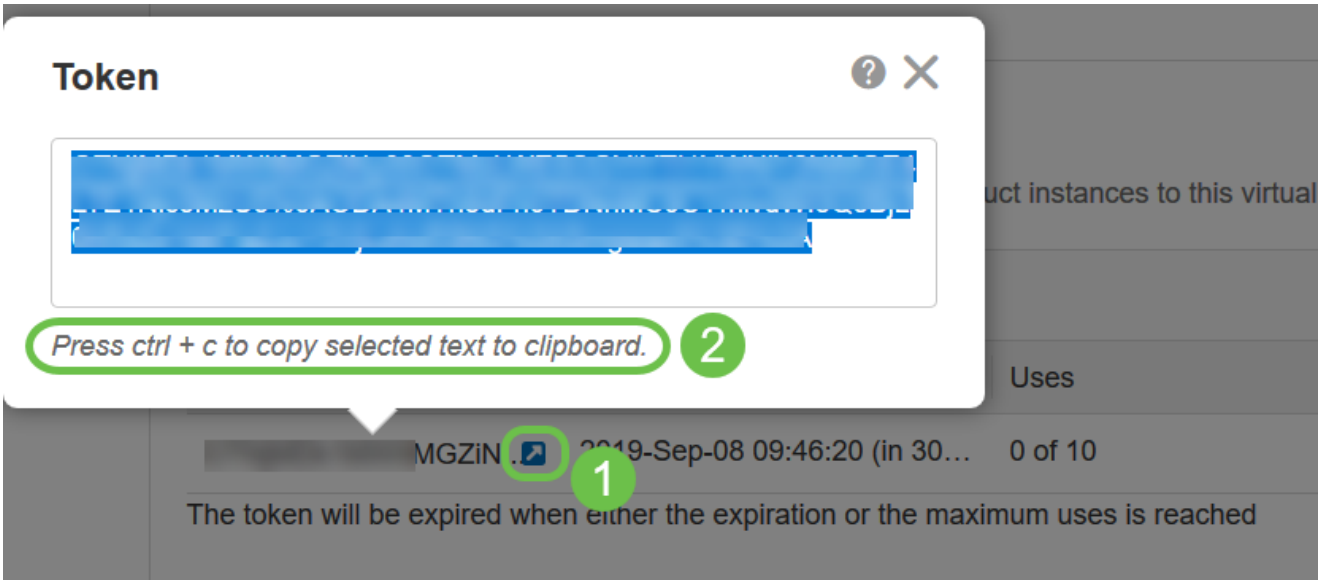


Ahora ha generado correctamente un token de registro de instancia de producto.



Paso 6

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

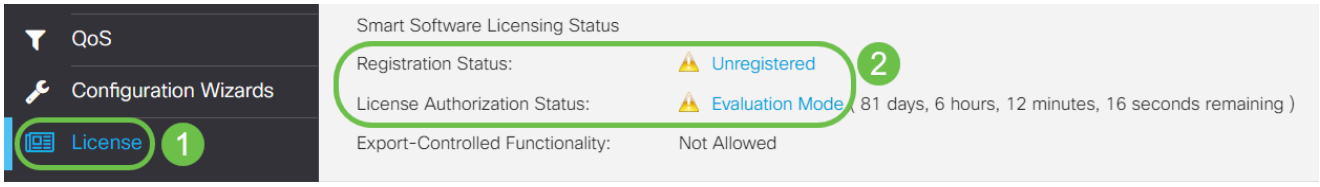


Paso 7 (opcional)

Haga clic en el menú desplegable Actions, elija Copy para copiar el token en el portapapeles o Download... para descargar una copia de archivo de texto del token desde el que puede copiar.

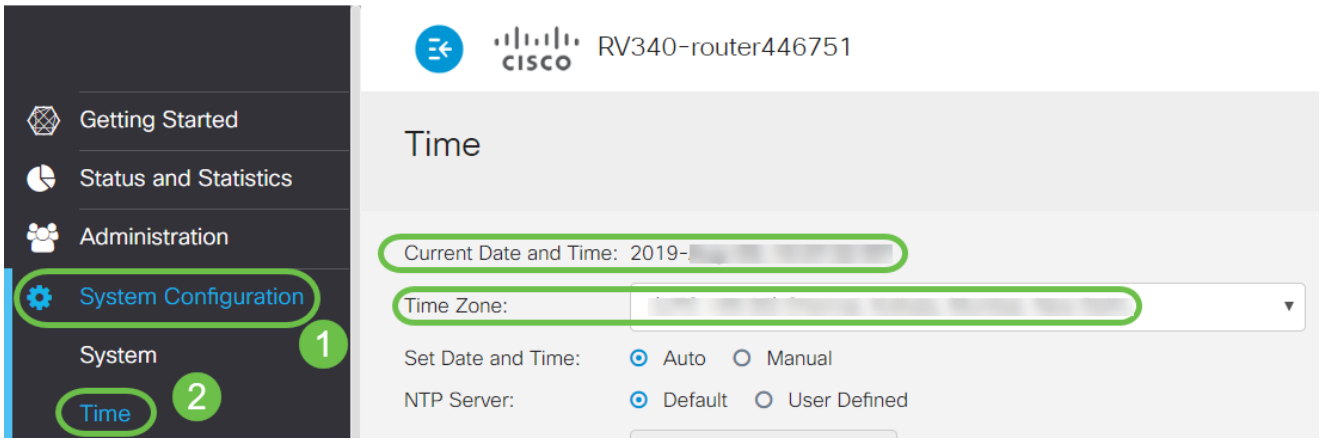
Paso 8

Desplácese hasta Licencia y verifique que Estado de registro aparece como No registrado y que Estado de autorización de licencia aparece como Modo de evaluación.



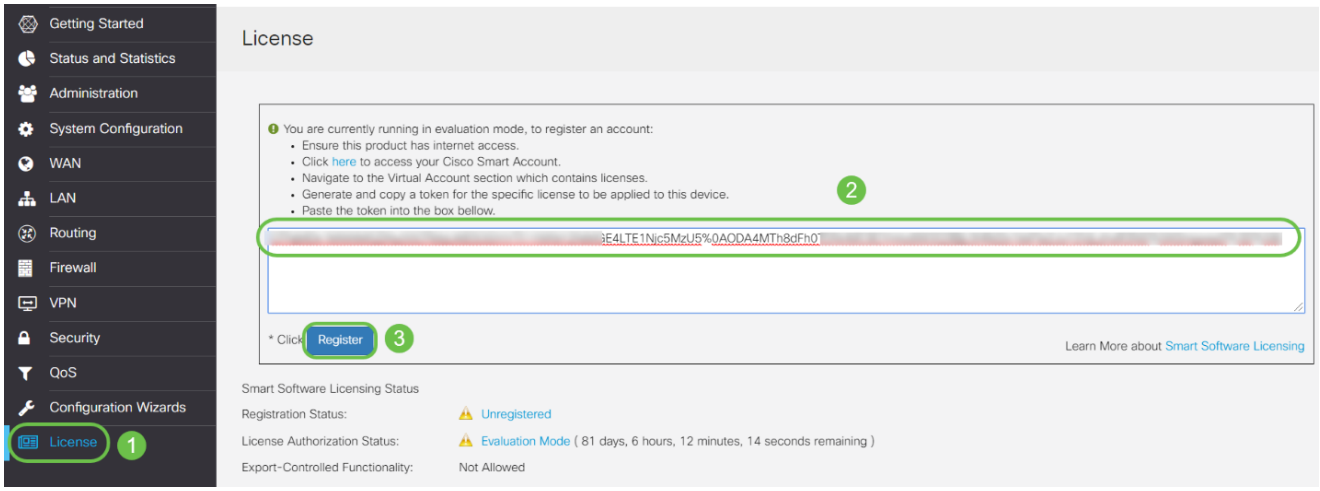
Paso 9

Navegue hasta System Configuration > Time y verifique que Current Date and Time y Time Zone se reflejen correctamente según su zona horaria.



Paso 10

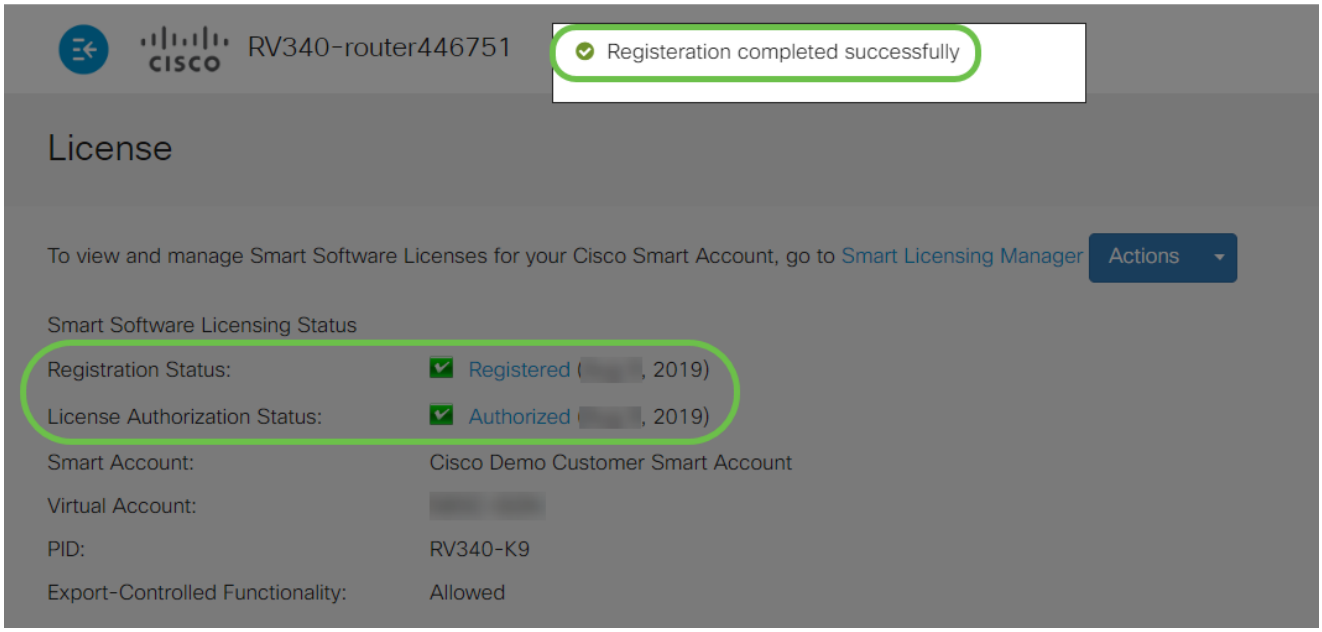
Vaya a Licencia. Pegue el token copiado en el paso 6 en el cuadro de texto debajo de la ficha Licencia seleccionando ctrl + v en el teclado. Haga clic en Register.



El registro puede tardar unos minutos. No salga de la página cuando el router intente ponerse en contacto con el servidor de licencias.

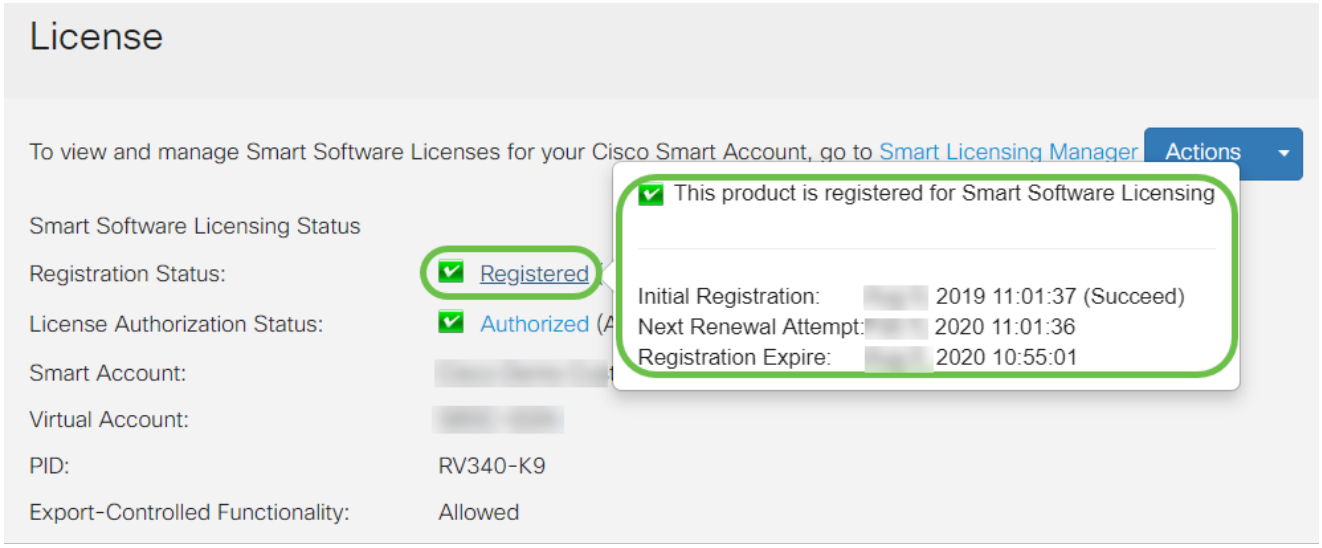
Paso 11

Ahora debería haber registrado y autorizado correctamente su 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 aparece como Registrado y el Estado de autorización de licencia aparece como Autorizado.



Paso 12 (opcional)

Para ver más detalles del estado de registro de la licencia, pase el puntero sobre el estado Registrado. Aparecerá un mensaje de diálogo con la siguiente información:

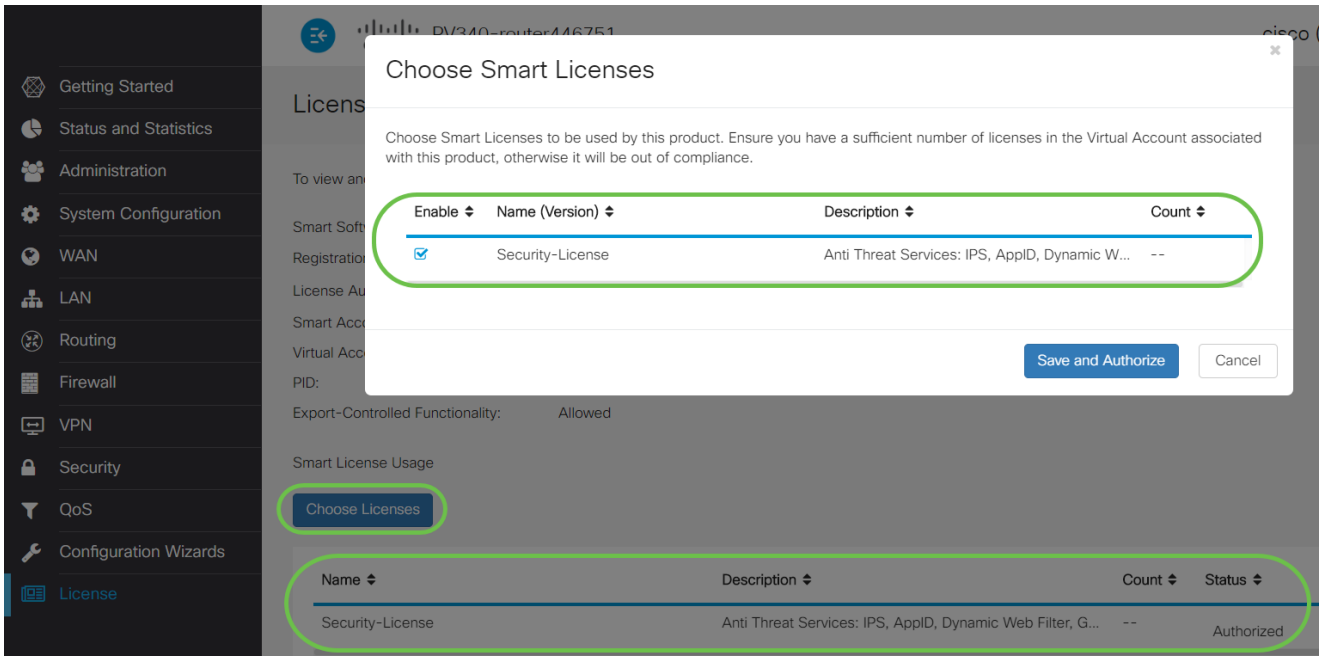


- Registro inicial: esta área indica la fecha y la hora en que se registró la licencia.
- Siguiente intento de renovación: esta área indica la fecha y la hora en que el router intentará renovar la licencia.
- Vencimiento del registro: esta área indica la fecha y la hora de vencimiento del registro.

Paso 13

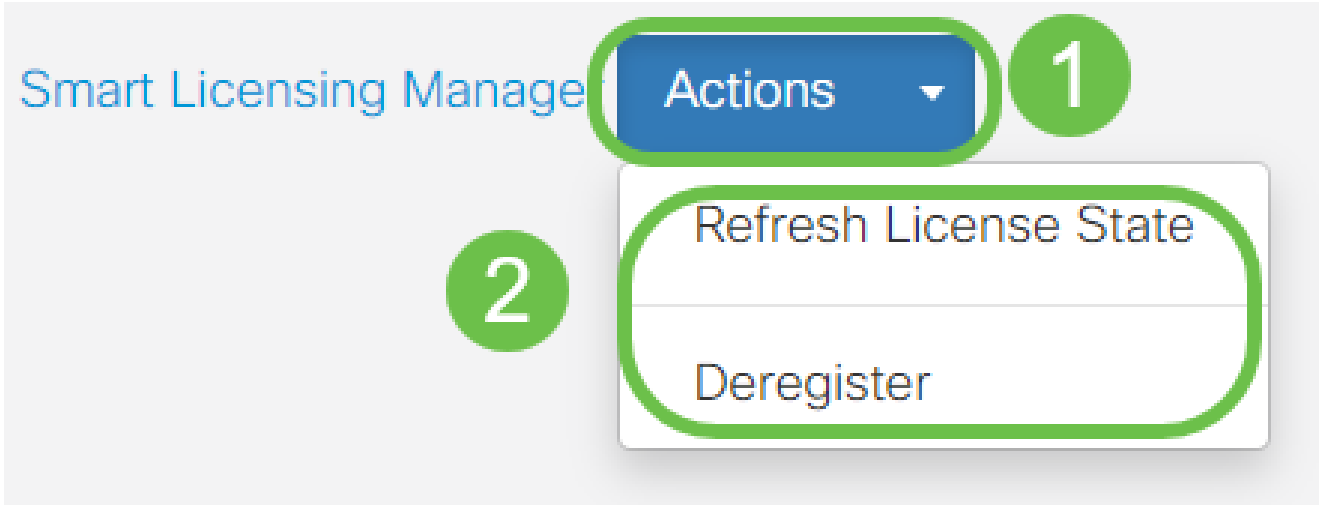
En la página License, verifique que el estado Security-License muestre Authorized. También puede hacer clic en el botón Choose License para verificar que Security-License esté habilitado.

Si tiene algún problema con este paso, es posible que tenga que reiniciar el router.



Paso 14 (opcional)

Para Actualizar el estado de licencia o Anular el registro de la licencia del router, haga clic en el menú desplegable Acciones del administrador de licencias inteligentes y seleccione un elemento de acción.



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

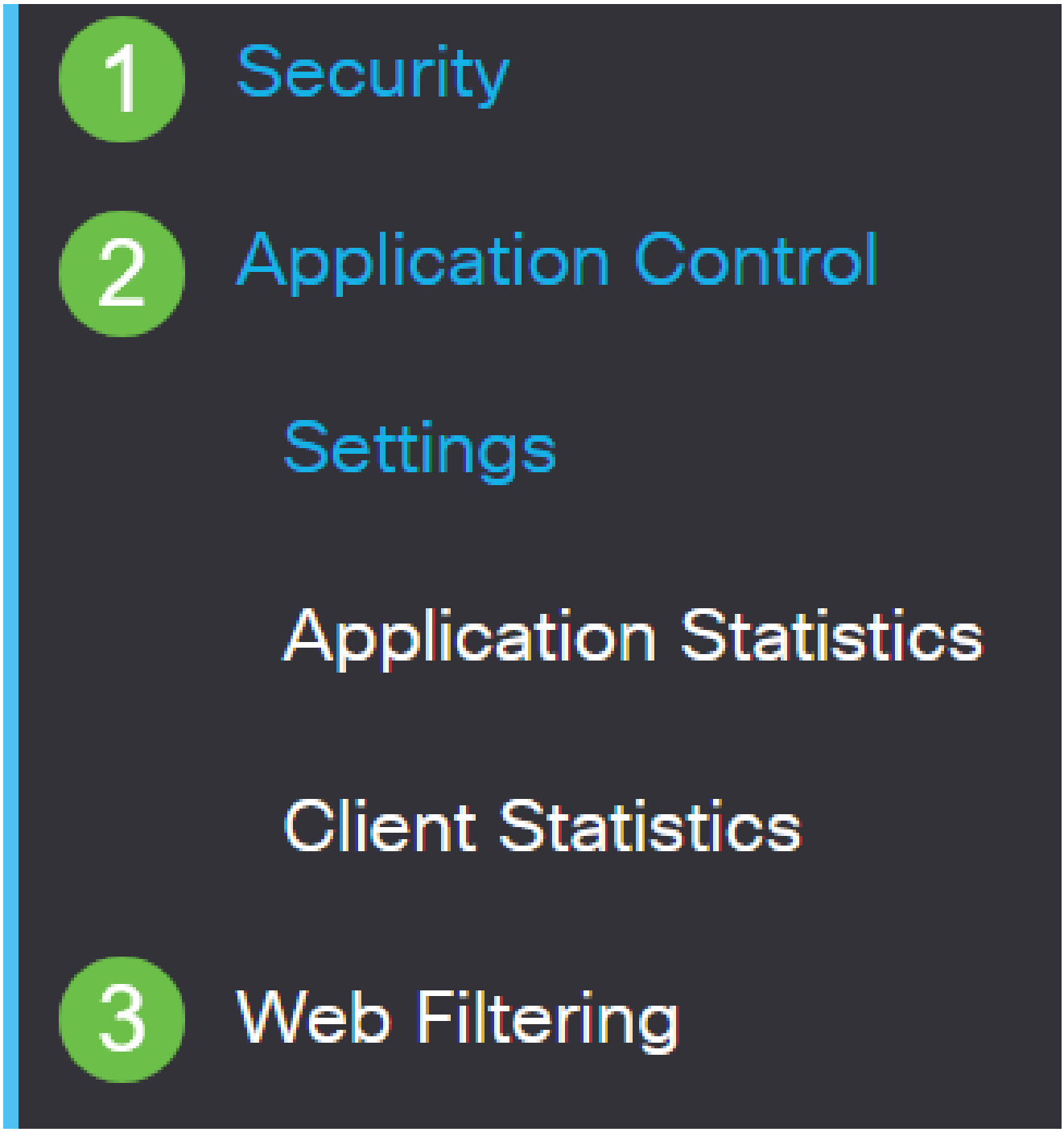
Filtrado web en el router RV345P

Dispone de 90 días tras 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

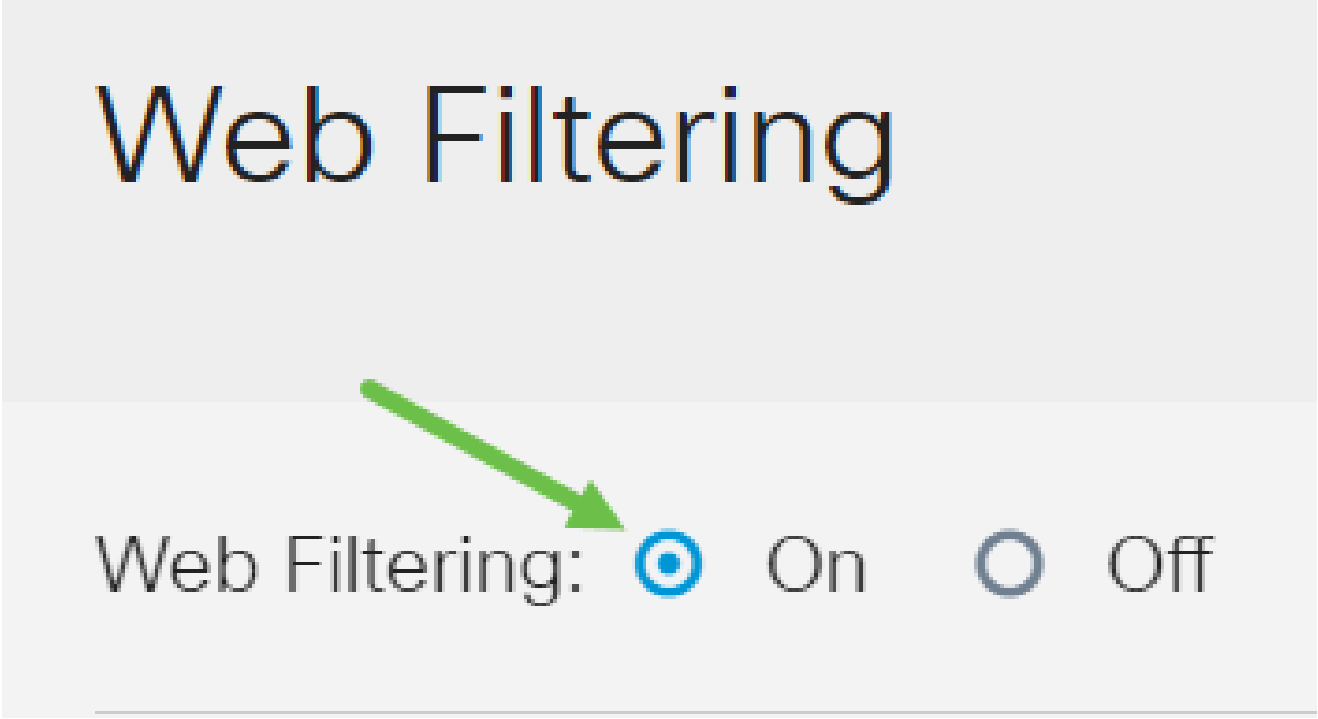
Inicie sesión en la utilidad basada en Web y seleccione Security > Application Control > Web

Filtering.



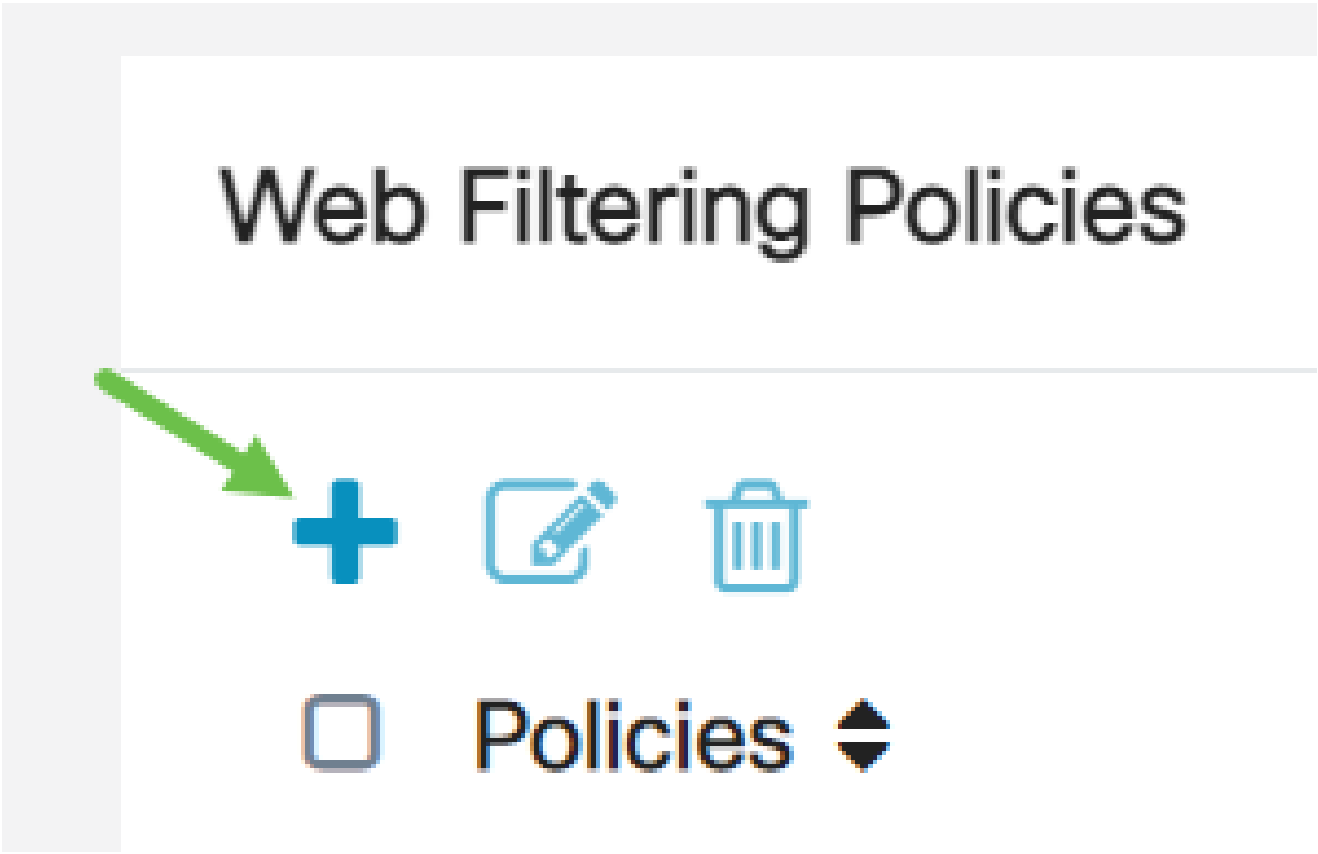
Paso 2

Seleccione el botón de opción On.



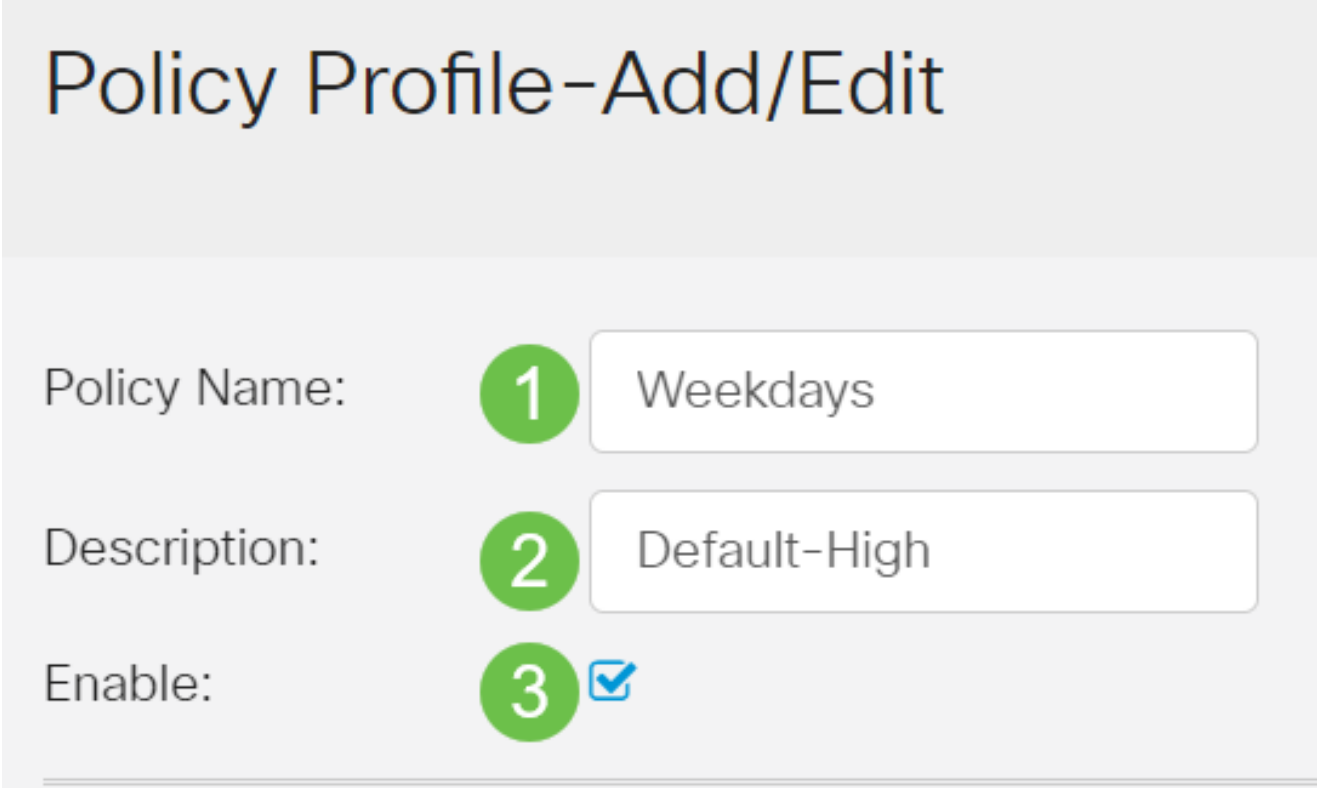
Paso 3

Haga clic en el icono de agregar.



Paso 4

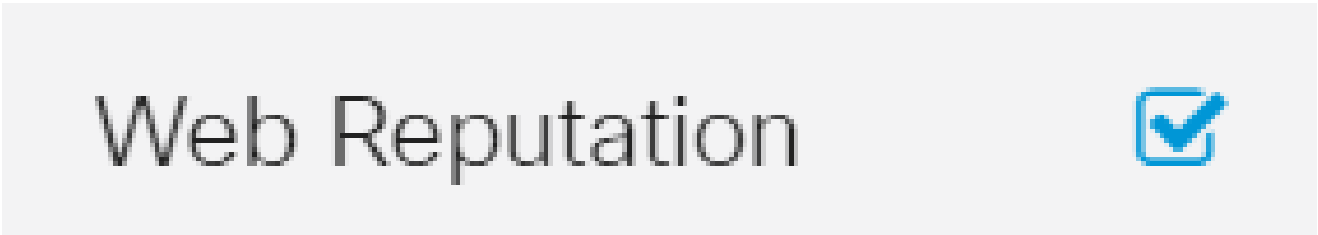
Ingrese un Nombre de Política, Descripción, y la casilla de verificación Enable.



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

Paso 5

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



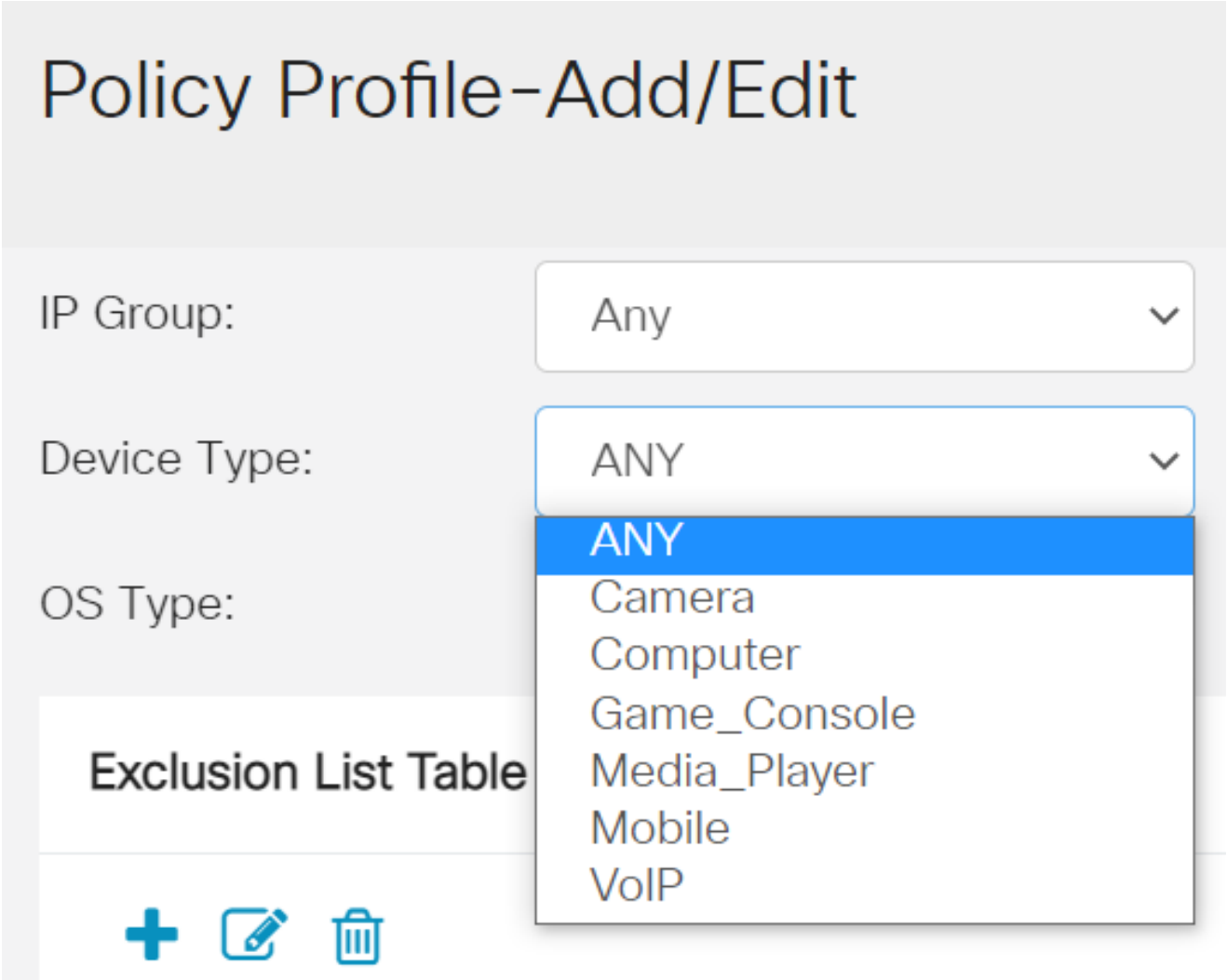
El contenido se filtrará según la notoriedad de un sitio web o URL según un índice de reputación web. Si la puntuación cae por debajo de 40, se bloqueará el sitio web. Para obtener más información sobre la tecnología de reputación web, haga clic aquí para obtener más información.

Paso 6

En la lista desplegable Tipo de dispositivo, seleccione el origen/destino de los paquetes que se van a filtrar. Sólo se puede elegir 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).

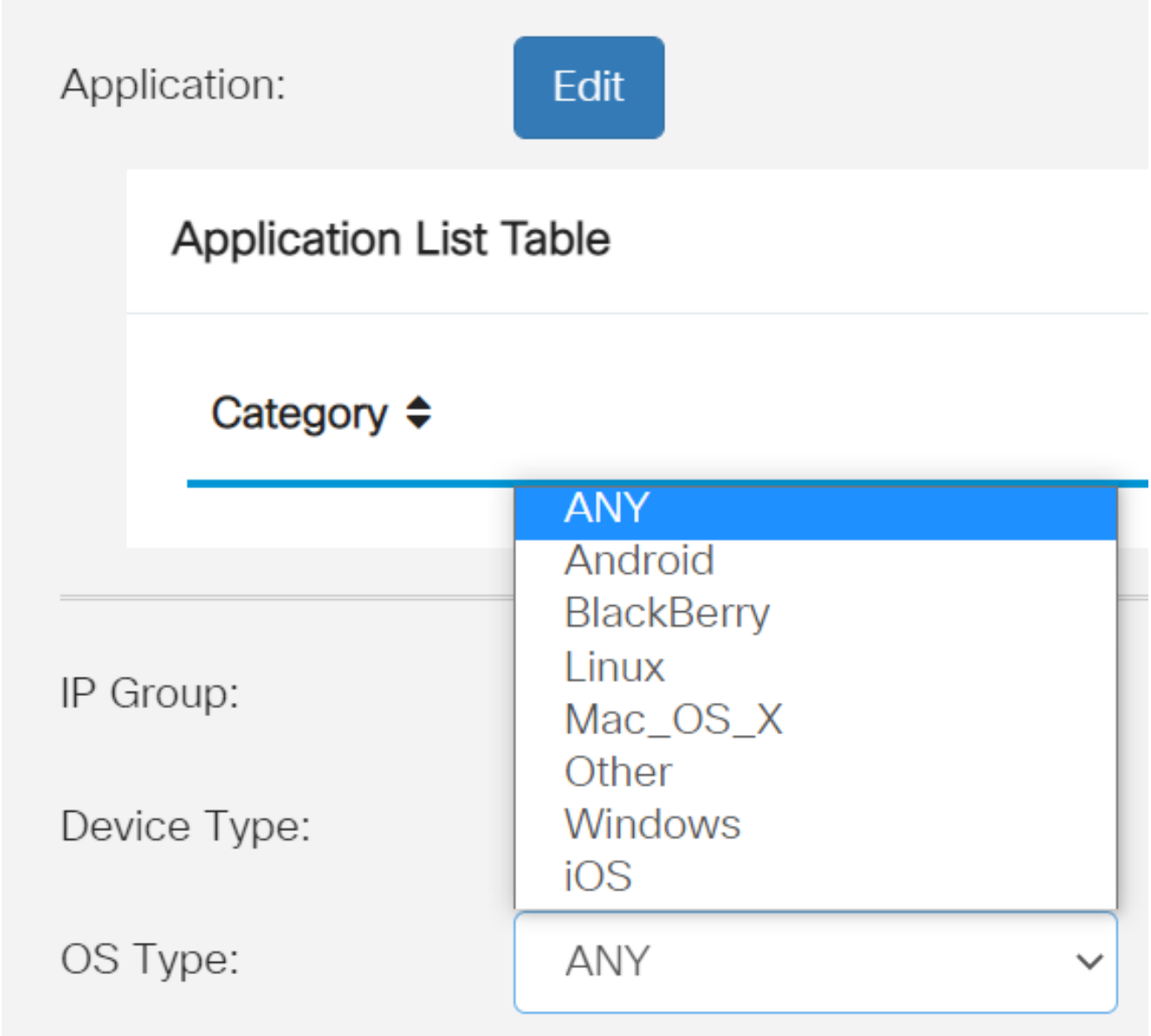
- Equipo: elija esta opción para aplicar la directiva a los equipos.
- Game_Console: elija esta opción para aplicar la política a las consolas de juegos.
- Media_Player: elija esta opción para aplicar la política a los reproductores multimedia.
- Móvil: elija esta opción para aplicar la política a los dispositivos móviles.
- VoIP: elija esta opción para aplicar la política a los dispositivos de voz sobre protocolo de Internet.



Paso 7

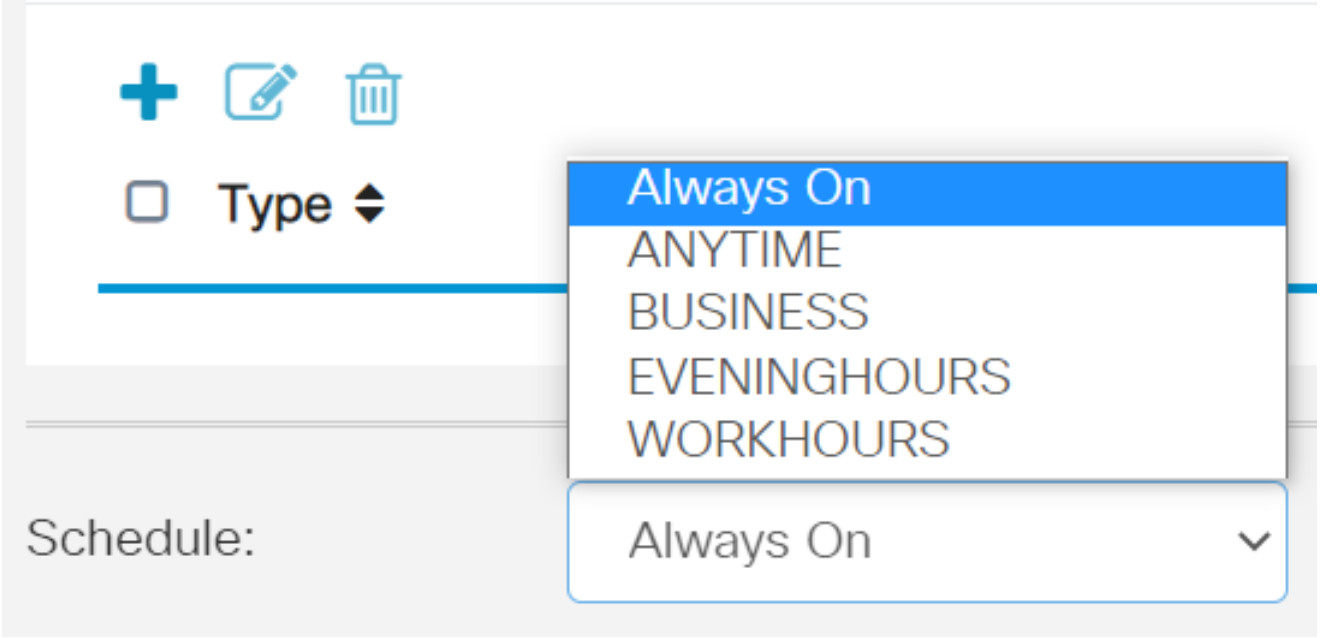
En la lista desplegable Tipo de SO, elija un sistema operativo (SO) al que debe aplicarse la política. Sólo se puede elegir una opción a la vez. Las opciones son:

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



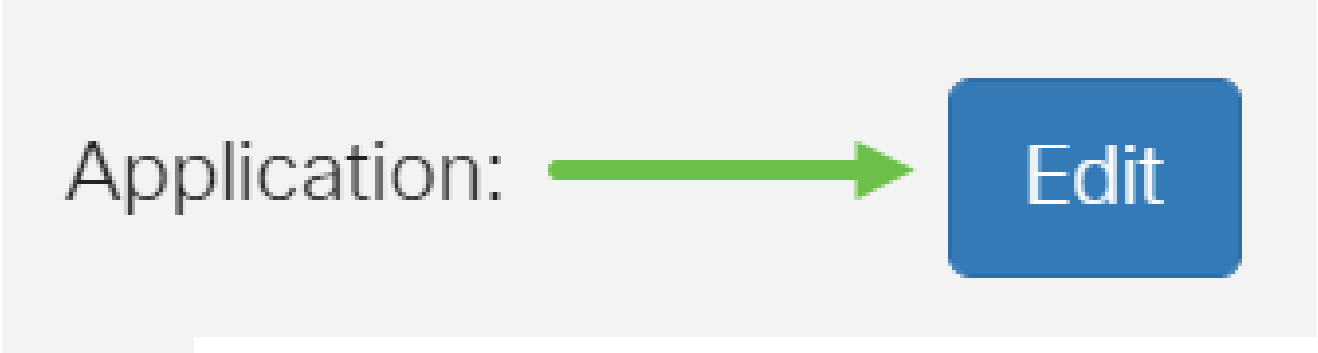
Paso 8

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



Paso 9

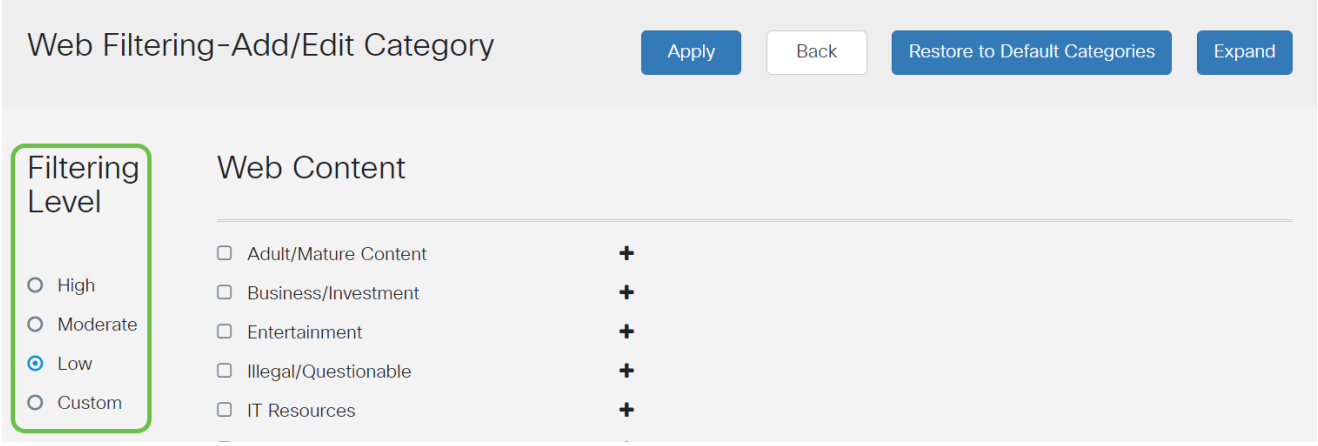
Haga clic en el icono de edición.



Paso 10

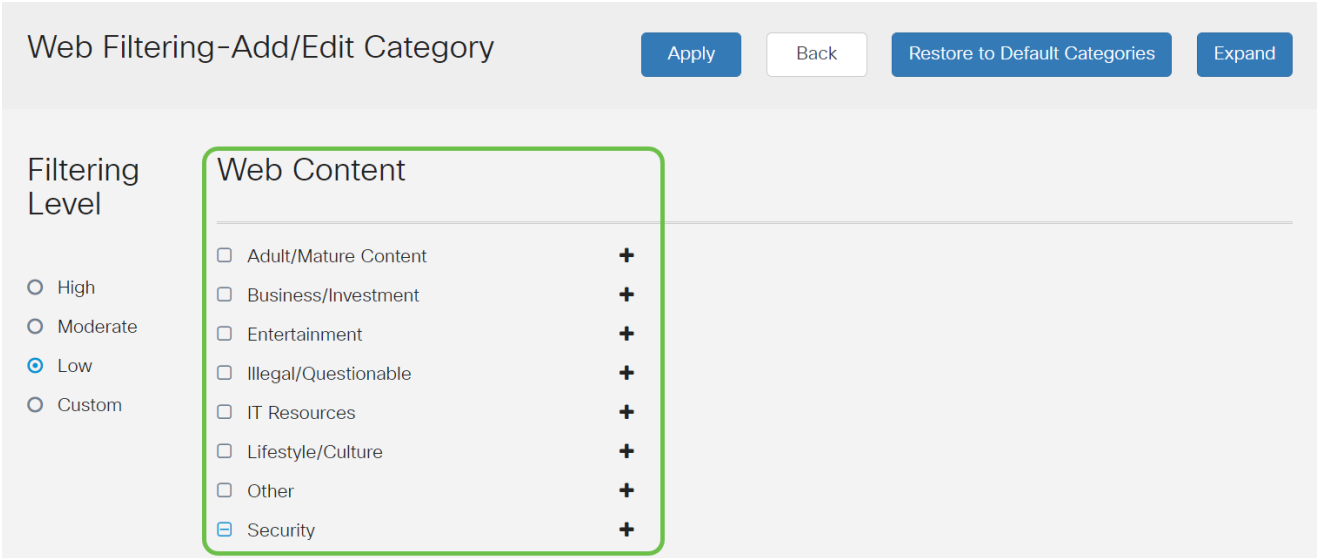
En la columna Nivel de filtrado, haga clic en un botón de opción para definir rápidamente el alcance de filtrado que mejor se adapte a las políticas de red. Las opciones disponibles son Alta, Moderada, Baja y Personalizada. Haga clic en cualquiera de los niveles de filtrado que aparecen a continuación para conocer las subcategorías predefinidas específicas filtradas en cada una de las categorías de contenido web habilitadas. Los filtros predefinidos no se pueden modificar más y están atenuados.

- Bajo: esta es la opción por defecto. La seguridad está activada con esta opción.
- Moderado: Contenido para adultos/adultos, ilegal/cuestionable y seguridad están habilitados con esta opción.
- Alto: contenido para adultos/adultos, empresa/inversión, ilegal/cuestionable, recursos de TI y seguridad están habilitados con esta opción.
- Personalizado: no se han definido valores predeterminados para permitir filtros definidos por el usuario.



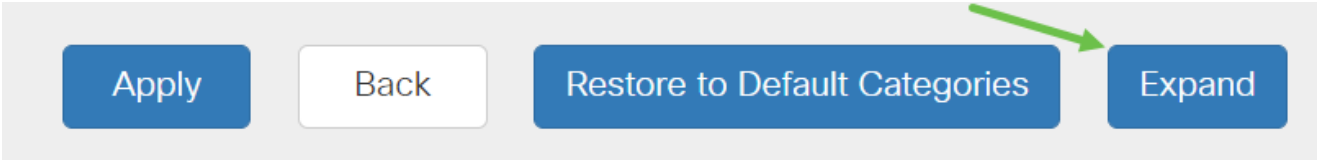
Paso 11

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



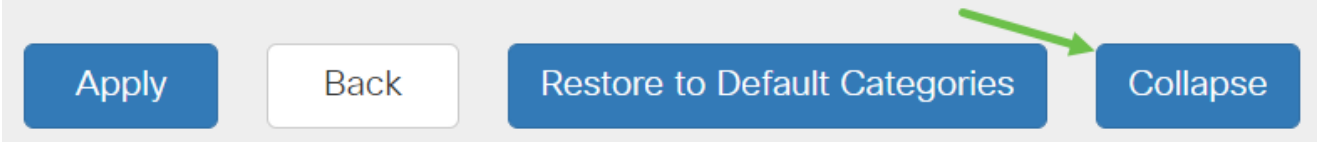
Paso 12 (opcional)

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



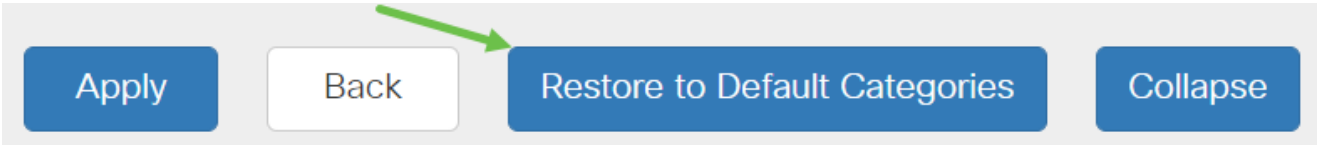
Paso 13 (opcional)

Haga clic en Contraer para contraer las subcategorías y descripciones.



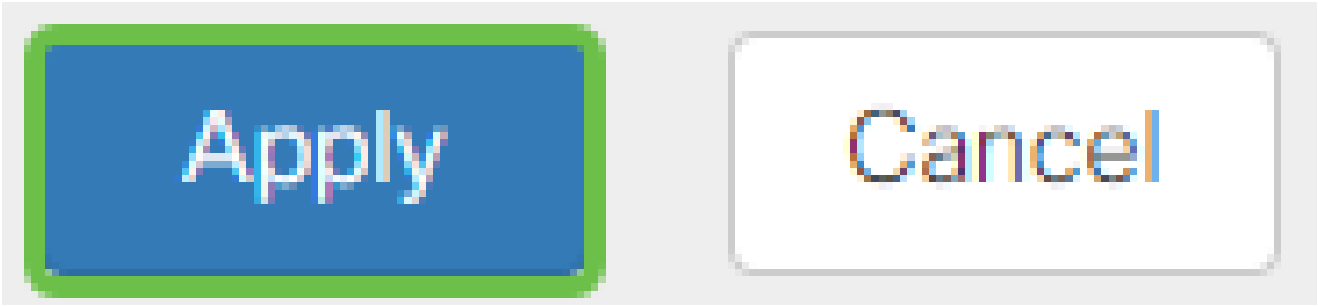
Paso 14 (opcional)

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



Paso 15

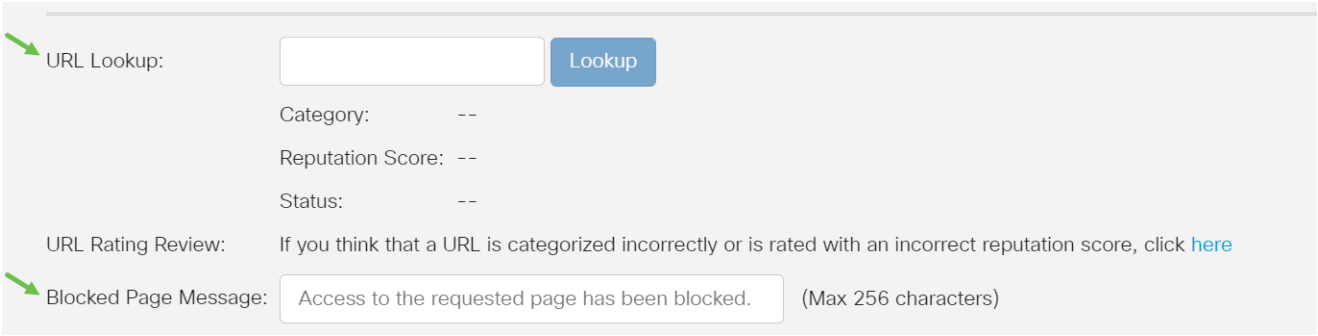
Haga clic en Apply para guardar la configuración y volver a la página Filter (Filtro) para continuar con la configuración.



En la tabla Lista de aplicaciones, se rellenarán las subcategorías correspondientes basadas en el nivel de filtrado seleccionado.

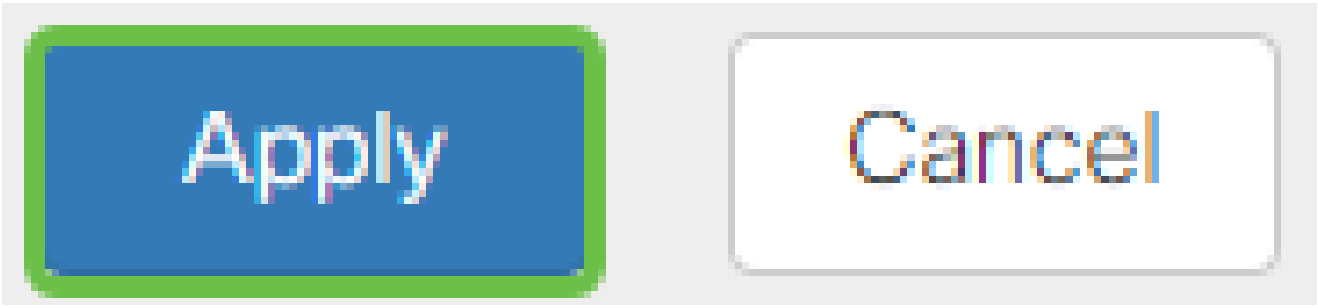
Paso 16 (opcional)

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



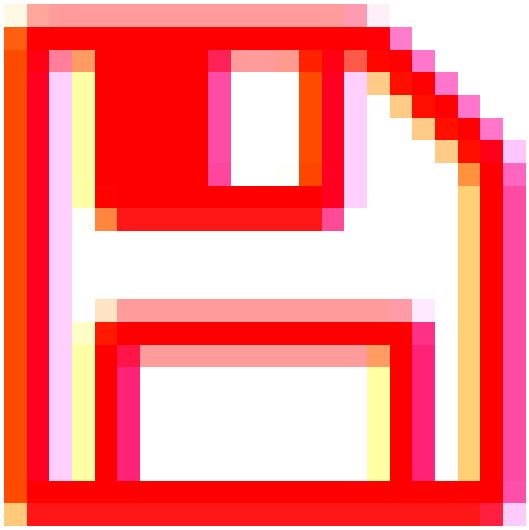
Paso 17 (opcional)

Haga clic en Apply (Aplicar).



Paso 18

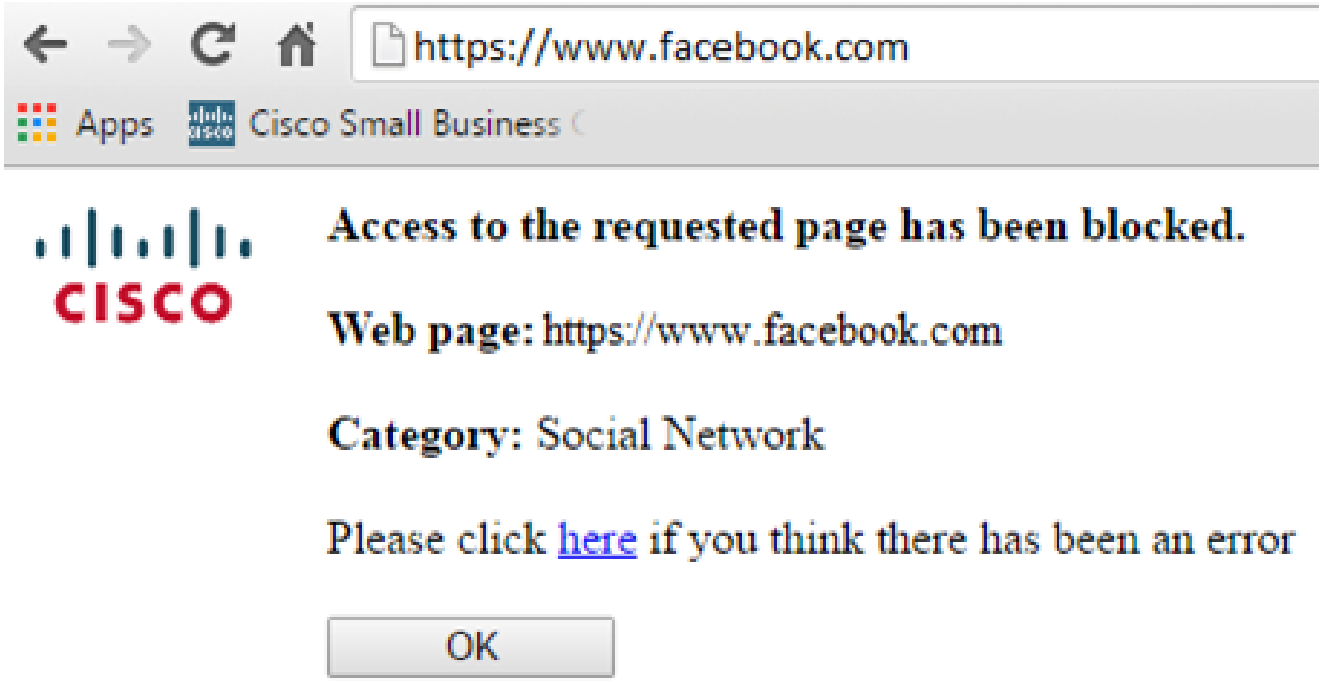
Para guardar la configuración de forma permanente, vaya a la página Copiar/Guardar configuración o haga clic en el icono Guardar en la parte superior de la página.



Paso 19 (opcional)

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

En este ejemplo, hemos utilizado www.facebook.com.



Ahora debería haber configurado correctamente el filtrado web en el router RV345P. Dado que está utilizando la licencia de seguridad de RV para el filtrado web, probablemente no necesite Umbrella. Si también desea utilizar Umbrella, haga clic aquí. Si dispone de suficiente seguridad, haga clic para pasar a la siguiente sección.

Resolución de problemas

Si ha adquirido una licencia pero no aparece en su cuenta virtual, tiene 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, estaremos encantados de ayudarle. Para que el proceso sea lo más expeditivo posible, necesitará las credenciales de la tabla anterior, así como las que se describen a continuación.

Información necesaria	Localización de la información
Factura de licencia	Se le enviará por correo electrónico una vez que haya completado la compra de las licencias.
Número de pedido de venta de Cisco	Es posible que tenga que volver al revendedor para obtener esta información.
Captura de pantalla de su	Al realizar una captura de pantalla, se captura el contenido de la

Información necesaria	Localización de la información
página de licencia de Smart Account	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 si está resolviendo problemas, se recomienda realizar 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 Umbrella RV Branch (opcional)

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

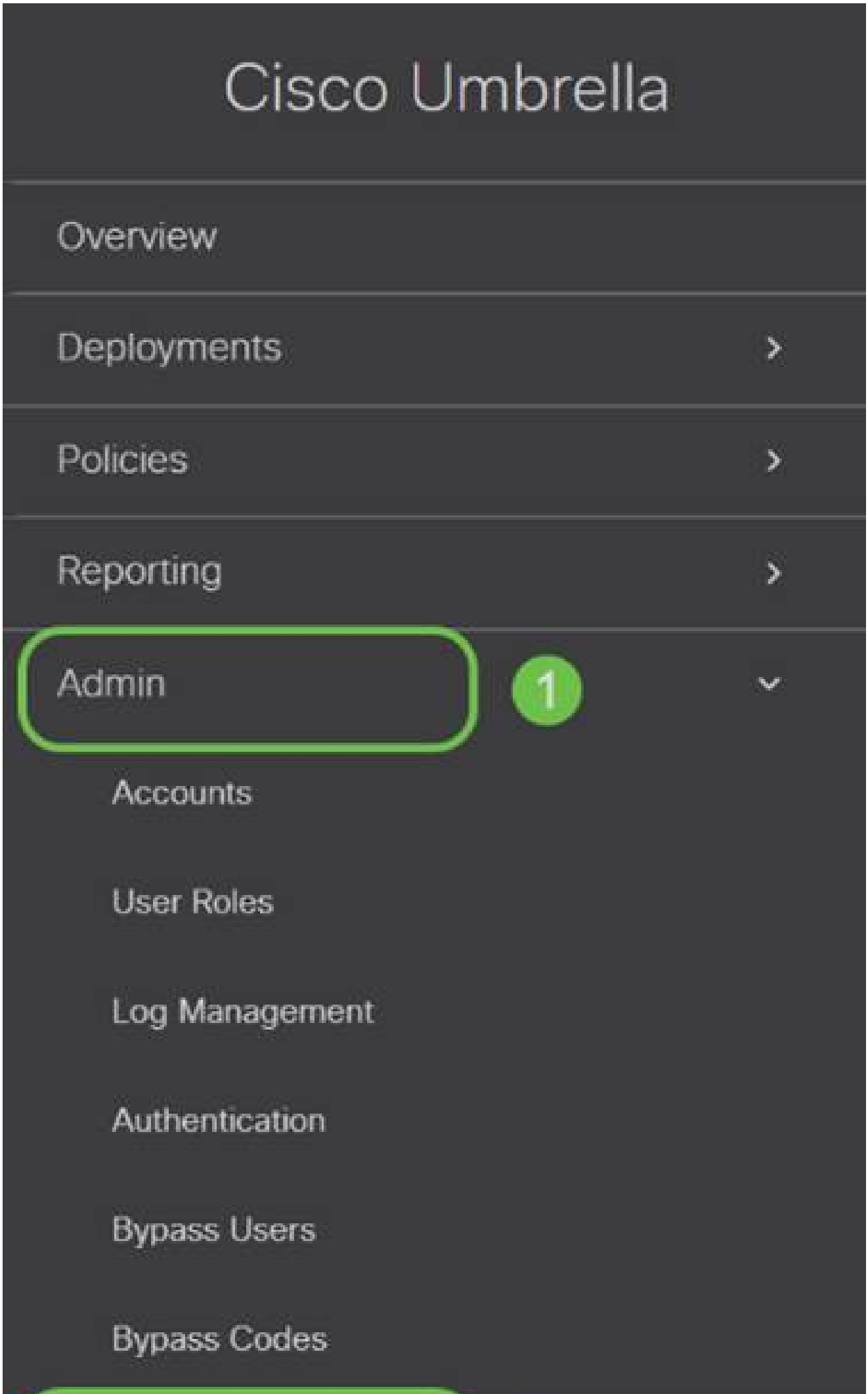
Umbrella funciona en la nube y presta muchos servicios relacionados con la seguridad. Desde la amenaza emergente hasta la investigación posterior al evento. Umbrella detecta y evita ataques en todos los puertos y protocolos.

Umbrella utiliza DNS como su principal vector de defensa. Cuando los usuarios introducen una URL en la barra del navegador y pulsan Intro, Umbrella participa en la transferencia. Esa URL pasa a la resolución de DNS de Umbrella y, si hay una advertencia de seguridad asociada al dominio, la solicitud se bloquea. Estos datos de telemetría se transfieren y analizan en microsegundos, lo que prácticamente no añade latencia. Los datos de telemetría utilizan registros e instrumentos que rastrean miles de millones de solicitudes de DNS en todo el mundo. Cuando estos datos son omnipresentes, su correlación en todo el mundo permite una respuesta rápida a los ataques a medida que estos 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 Umbrella Support.

Paso 1

Después de iniciar sesión en su cuenta de Umbrella, en la pantalla Dashboard, haga clic en Admin > API Keys.

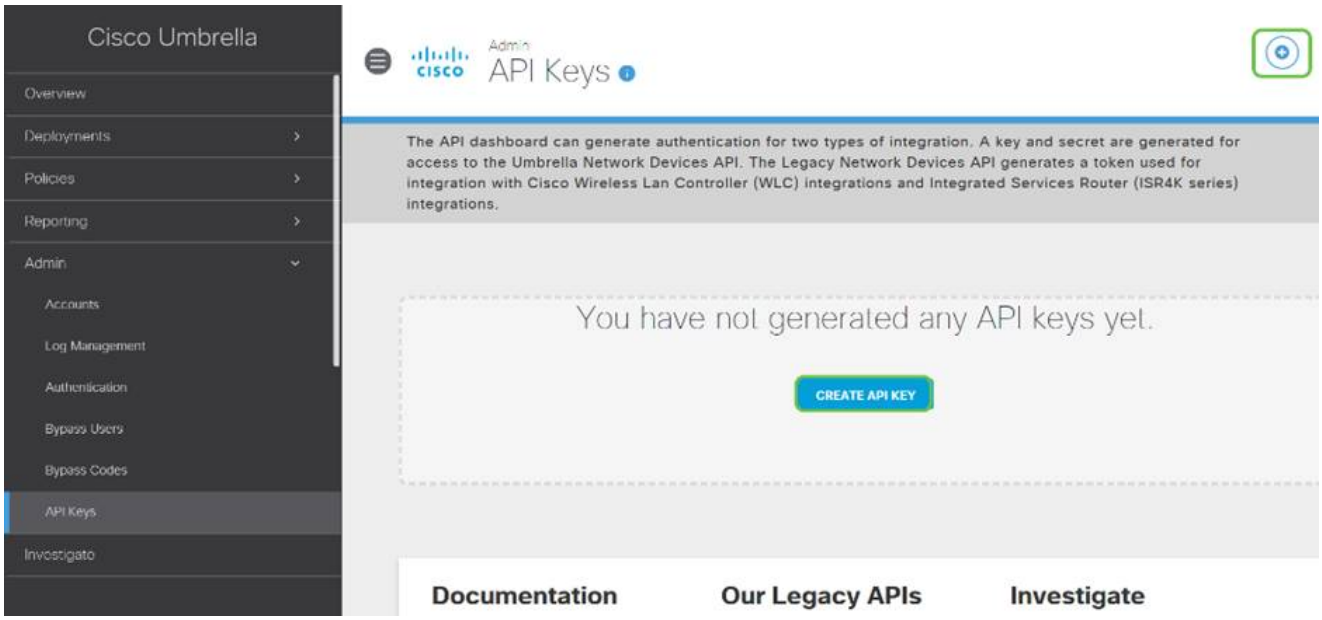

Cisco Umbrella
Overview
Deployments
Policies
Reporting
Admin
1
Accounts
User Roles
Log Management
Authentication
Bypass Users
Bypass Codes

Anatomía de la pantalla API Keys (Claves de API preexistentes)

1. Add API Key (Agregar clave de API): inicia la creación de una nueva clave para utilizarla con la API Umbrella.
2. Información adicional: se desliza hacia abajo/hacia arriba con una explicación para esta pantalla.
3. Token Well - Contiene todas las claves y tokens creados por esta cuenta. (Se rellena una vez que se ha creado una clave)
4. Documentos de soporte - Enlaces a la documentación del sitio de Umbrella relativa a los temas de cada sección.

Paso 2

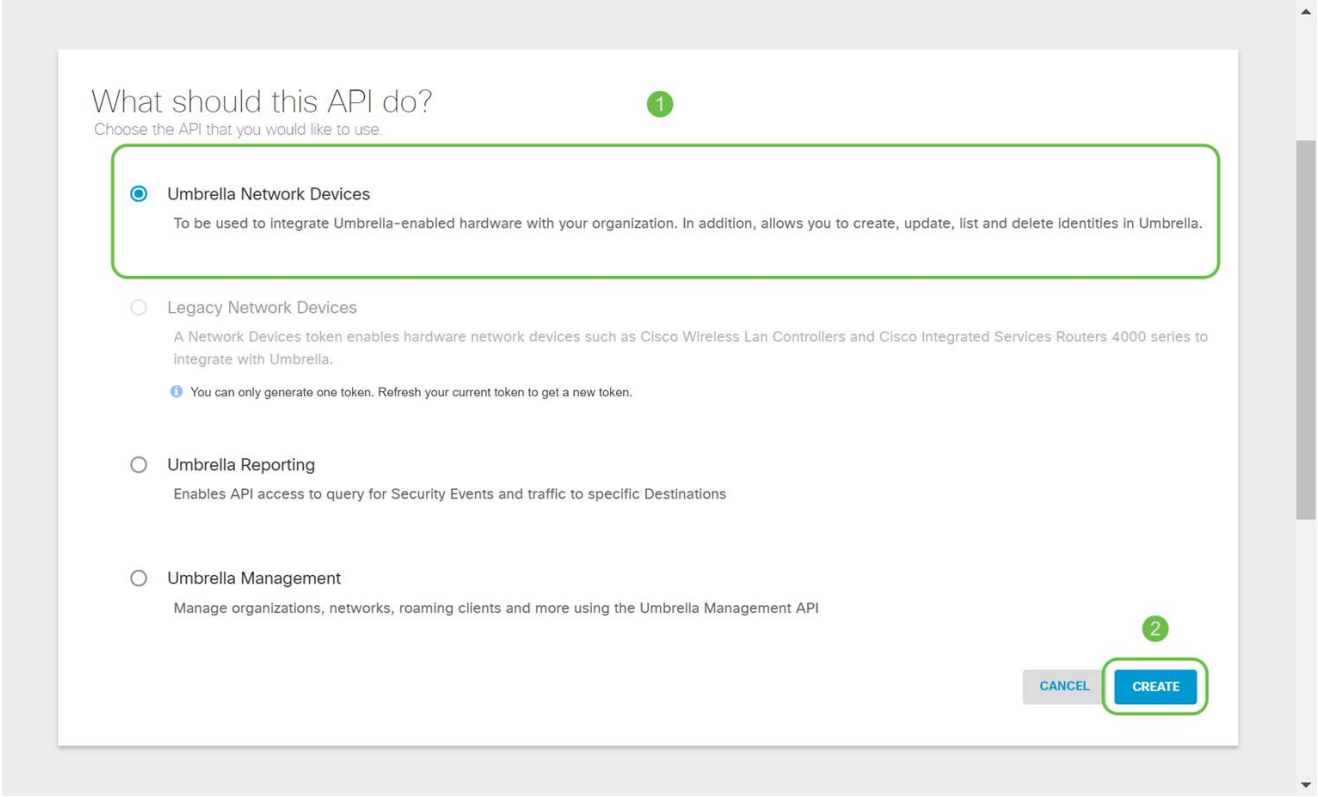
Haga clic en el botón Add API Key en la esquina superior derecha o haga clic en el botón Create API Key. Ambos funcionan de la misma manera.



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

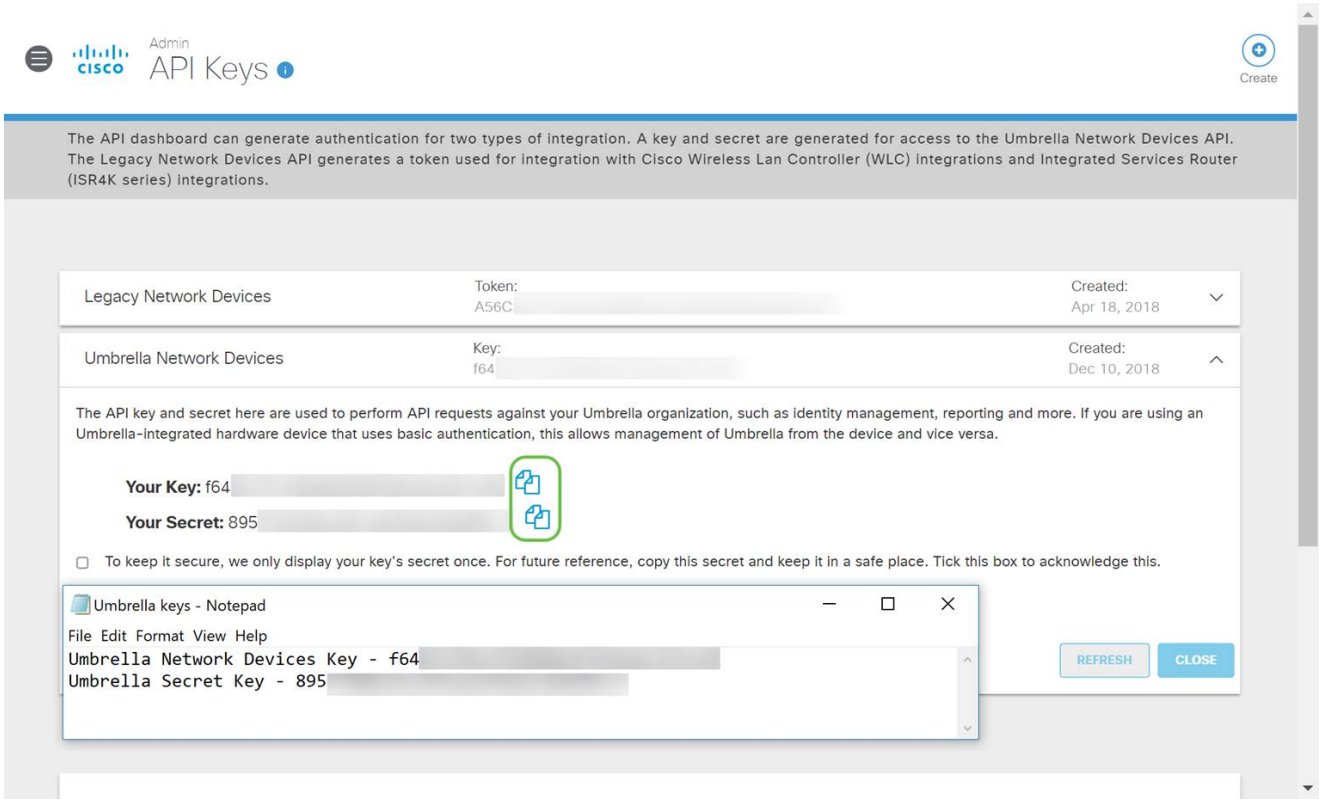
Paso 3

Seleccione Umbrella Network Devices y, a continuación, haga clic en el botón Create.



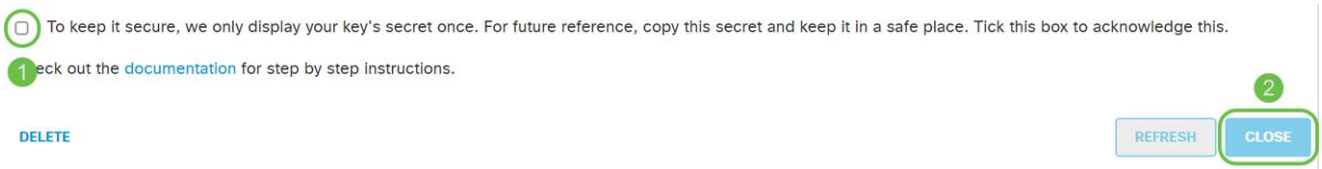
Paso 4

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 API Clave secreta, una notificación emergente confirmará que la clave se copia en el portapapeles. De uno en uno, pegue el secreto y la clave de API en el documento, etiquetándolos para futuras referencias. En este caso, su etiqueta es "Umbrella network devices key". A continuación, guarde el archivo de texto en una ubicación segura a la que pueda acceder fácilmente más adelante.



Paso 5

Una vez que haya copiado la clave y la clave secreta en una ubicación segura, en la pantalla Umbrella API, haga clic en la casilla de verificación para confirmar que se ha visto temporalmente la clave secreta y, a continuación, haga clic en el botón Close.



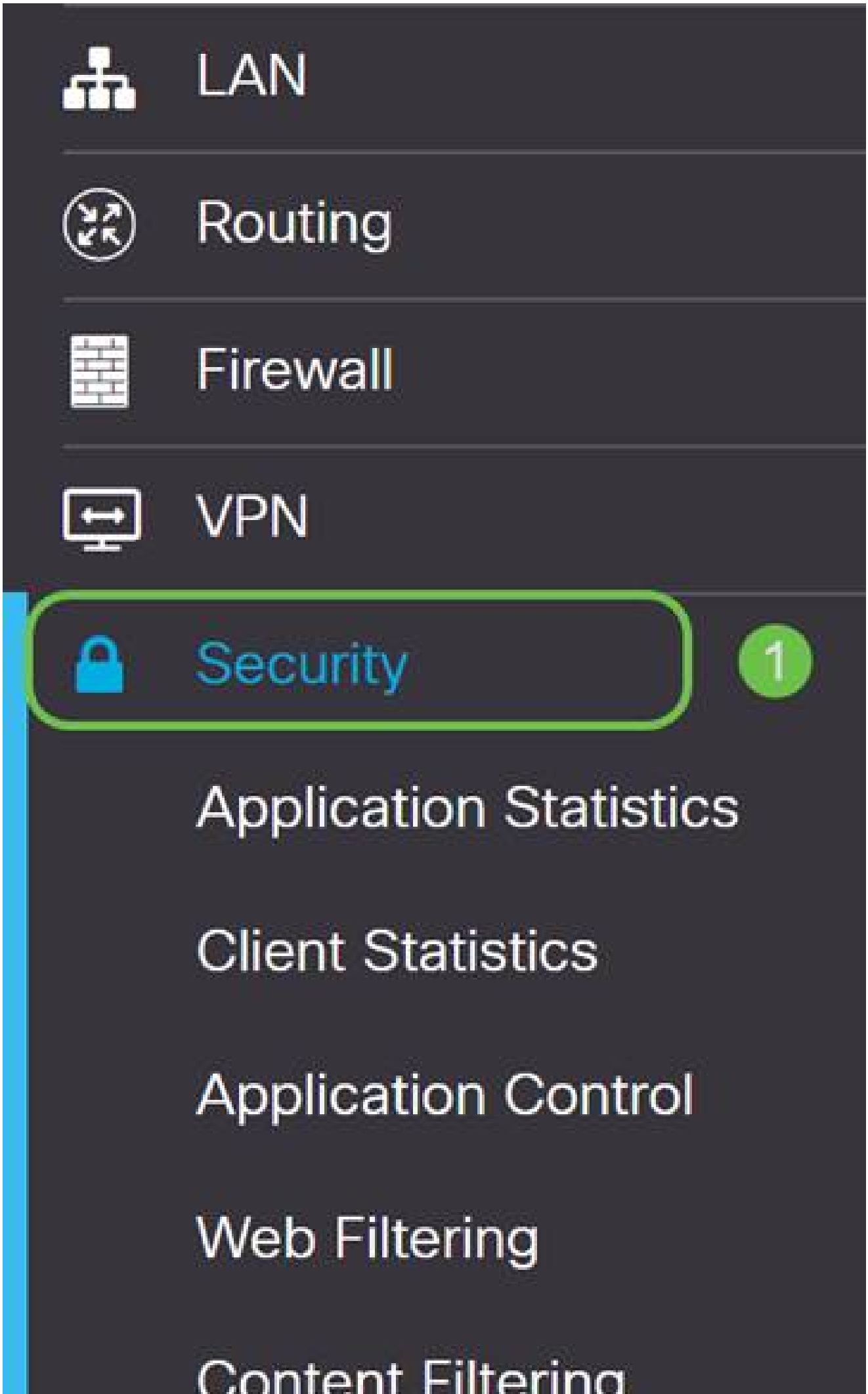
Si pierde o elimina accidentalmente la clave secreta, no hay ningún número de función o soporte al que llamar para recuperar esta clave. Si se pierde, tendrá que eliminar la clave y volver a autorizar la nueva clave API con cada dispositivo que desee proteger con Umbrella.

Configuración de Umbrella en el RV345P

Ahora que hemos creado claves de API en Umbrella, puede tomarlas e instalarlas en el RV345P.

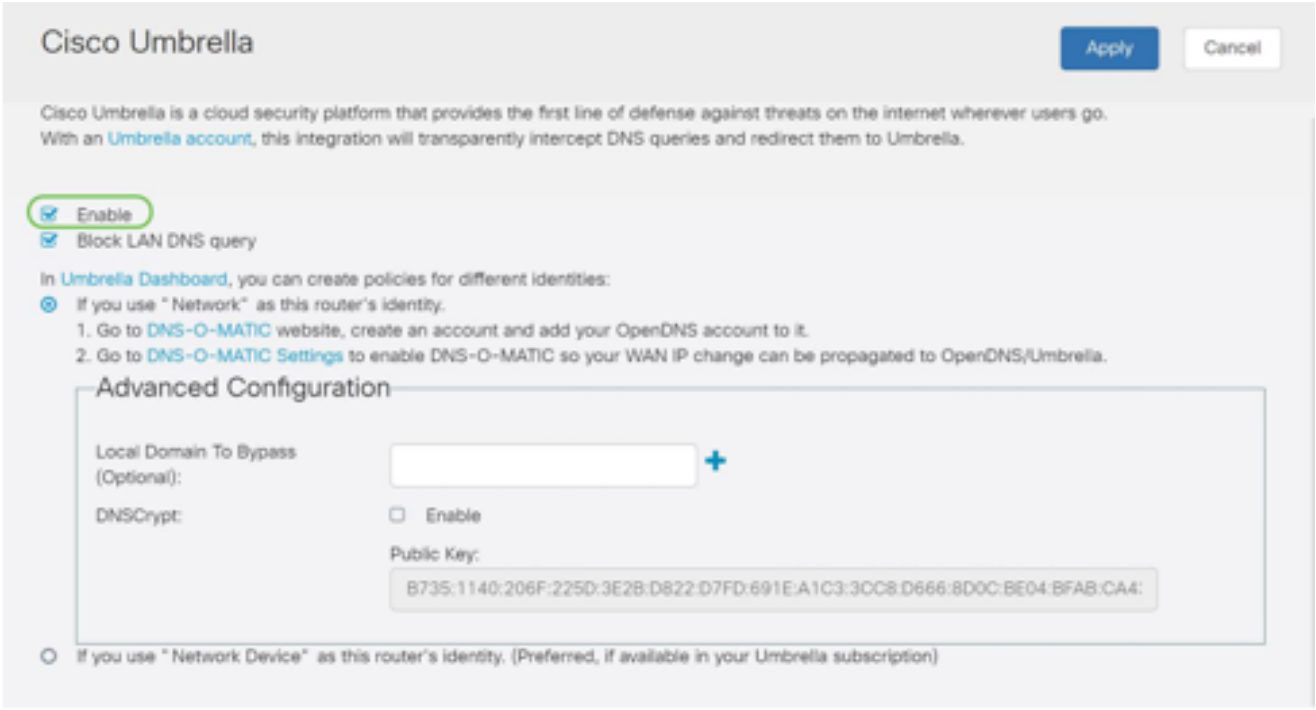
Paso 1

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


LAN
Routing
Firewall
VPN
Security
1
Application Statistics
Client Statistics
Application Control
Web Filtering
Content Filtering

Paso 2

La pantalla Umbrella API tiene varias opciones. Para empezar a activar Umbrella, haga clic en la casilla de verificación Enable.

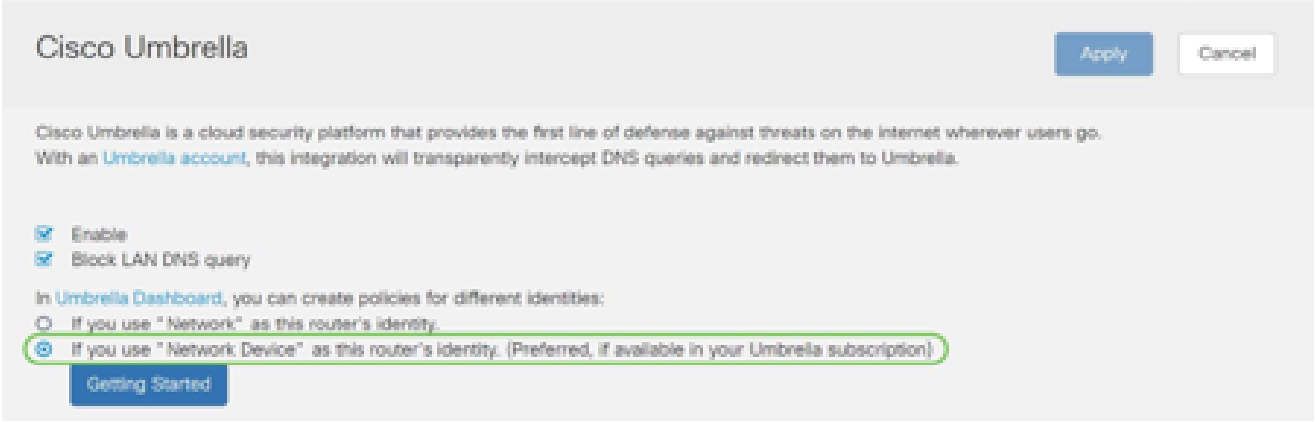


Paso 3 (opcional)

De forma predeterminada, la casilla Block LAN DNS Queries (Bloquear consultas DNS de LAN) está activada. Esta función limpia crea automáticamente listas de control de acceso en el router que evitarán que el tráfico DNS salga a Internet. Esta función obliga a dirigir todas las solicitudes de traducción de dominio a través del RV345P, lo que resulta una buena idea para la mayoría de los usuarios.

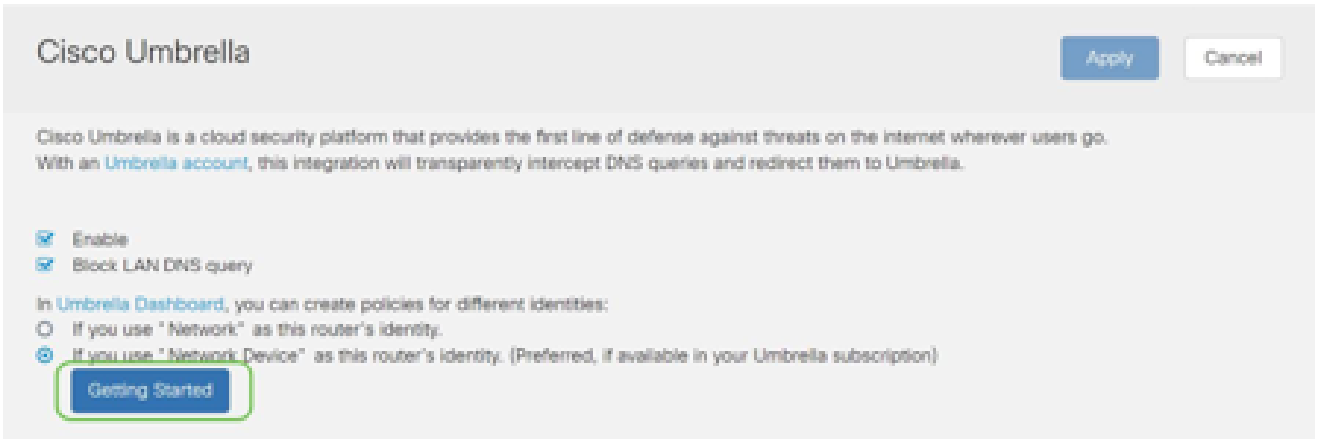
Paso 4

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". Tendrá que iniciar sesión en esas cuentas para garantizar que Umbrella interactúa con esos servicios, ya que proporciona protección. Para nuestros fines, confiamos en "Network Device" (Dispositivo de red), por lo que hacemos clic en el botón de radio inferior.



Paso 5

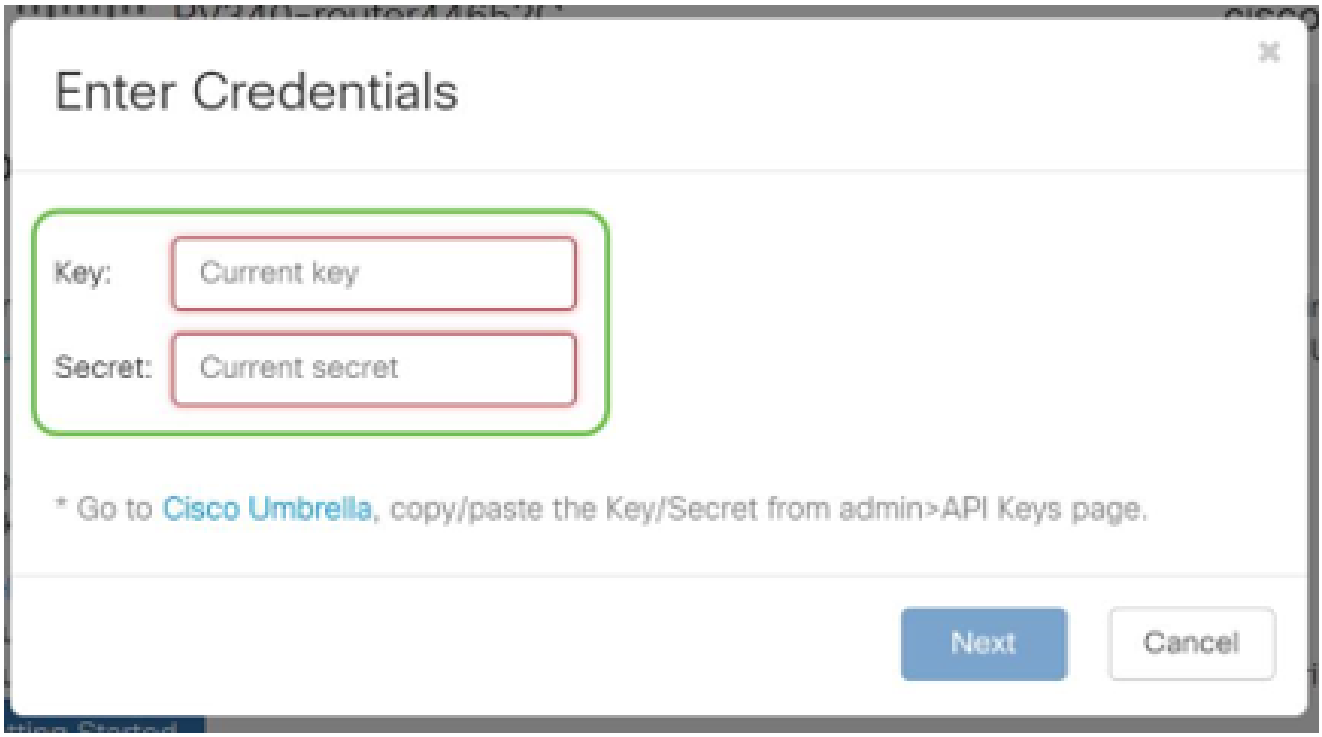
Haga clic en Getting Started.



Paso 6

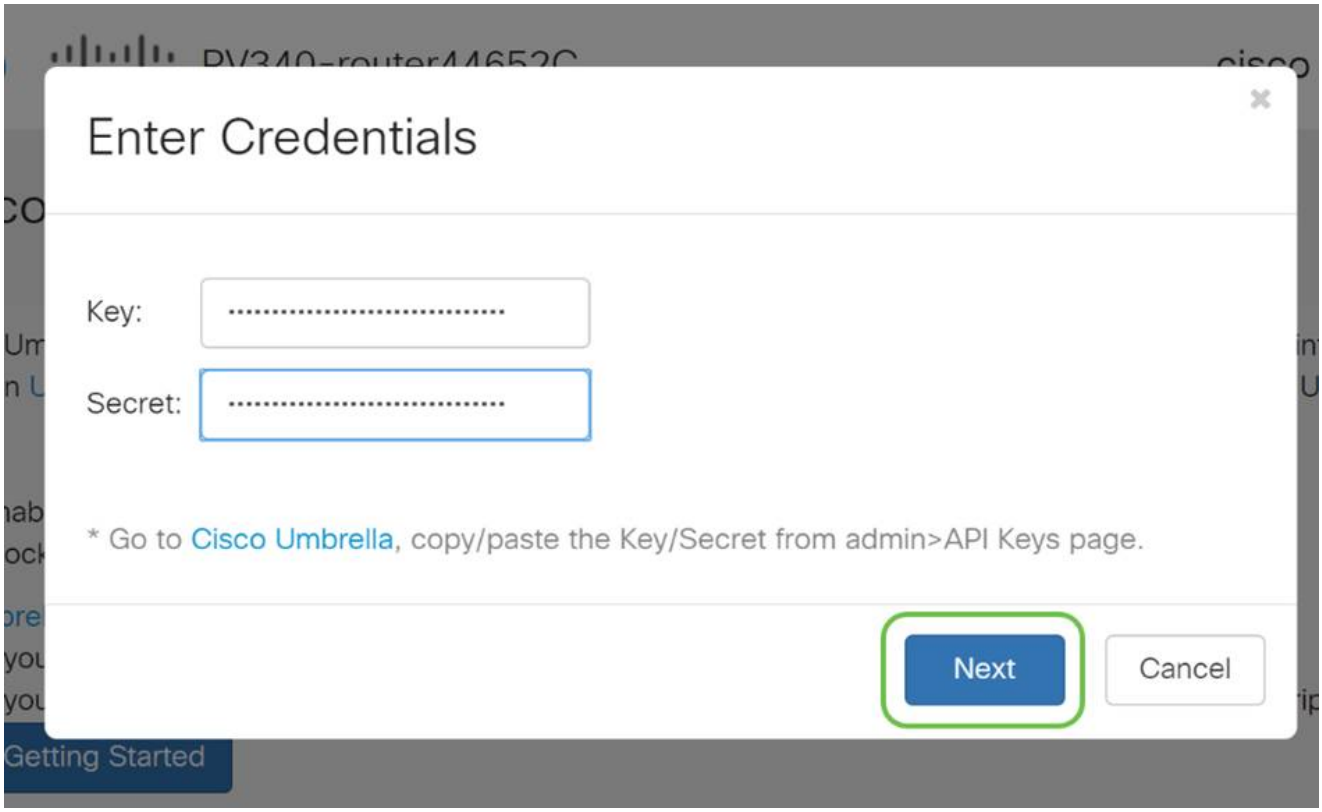
Ingrese la Clave API y la Clave Secreta en los cuadros de texto.

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



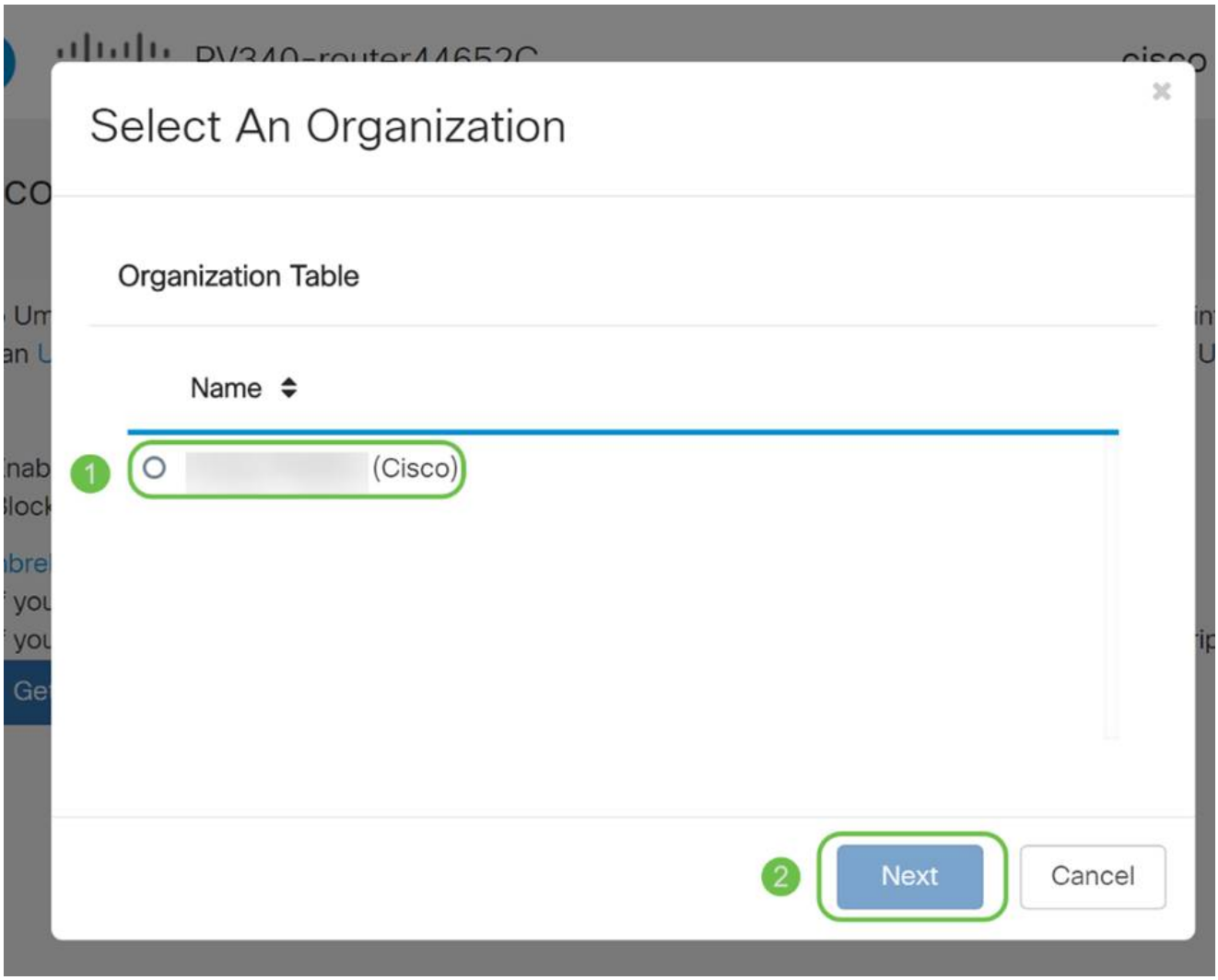
Paso 7

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



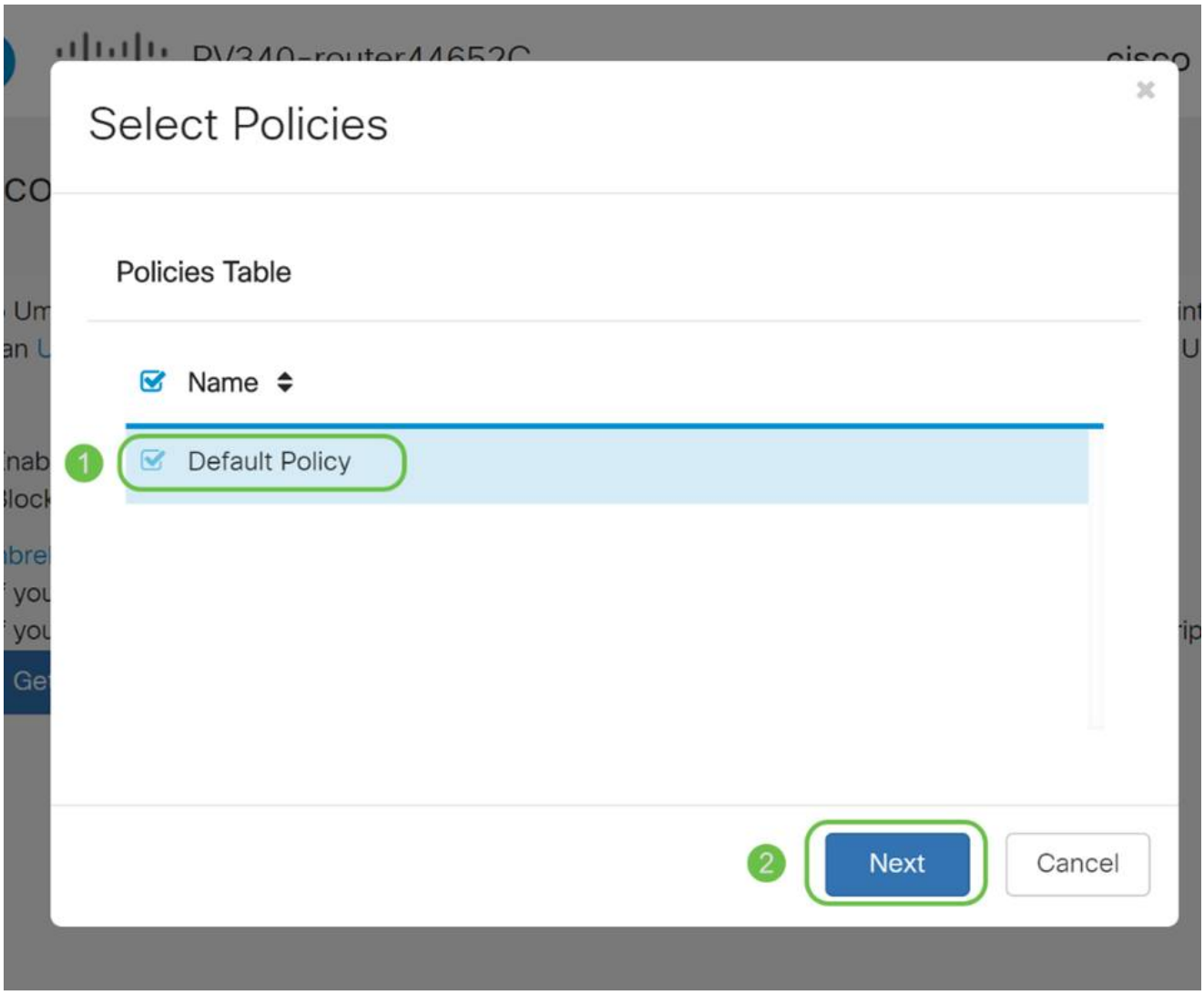
Paso 8

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



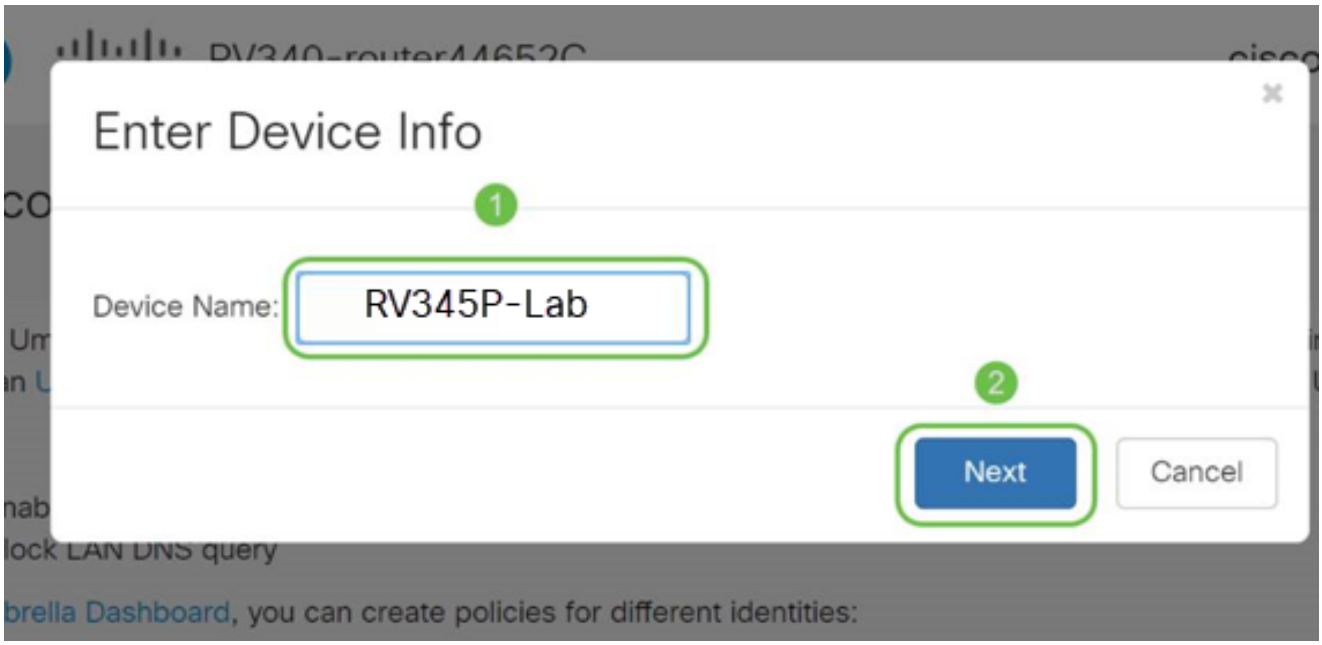
Paso 9

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



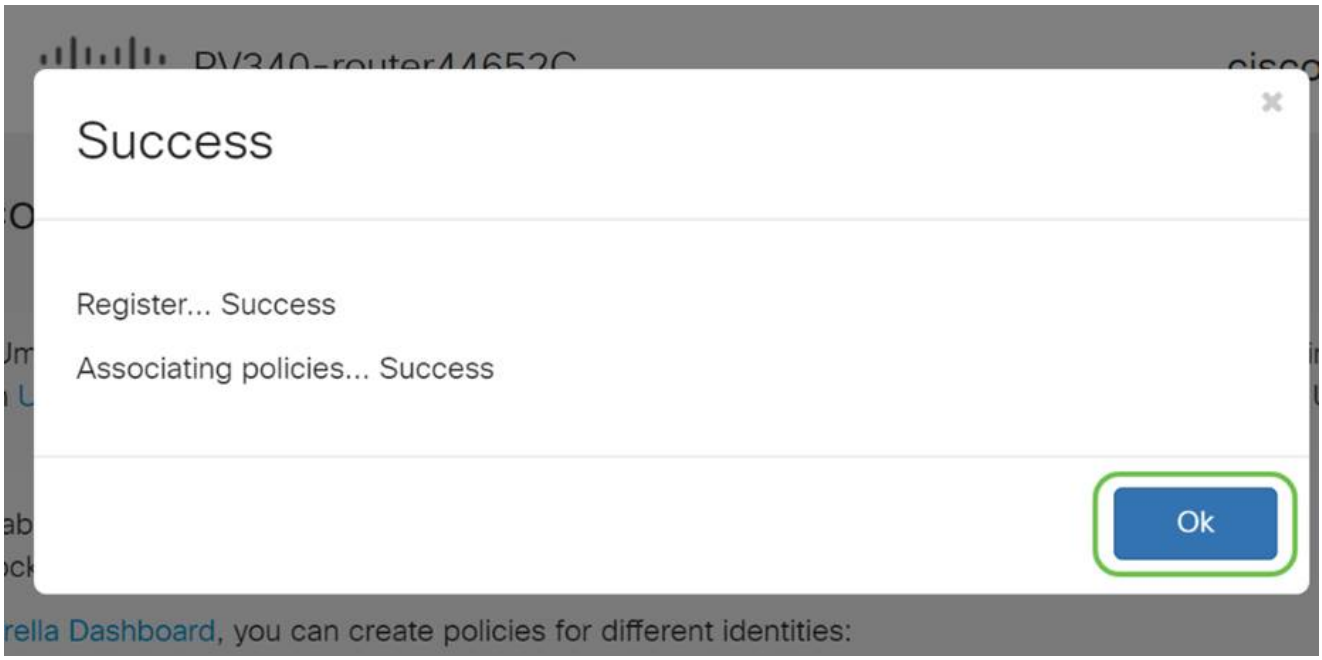
Paso 10

Asigne un nombre al dispositivo para que pueda designarse en los informes generales. En nuestra configuración, lo hemos denominado RV345P-Lab.



Paso 11

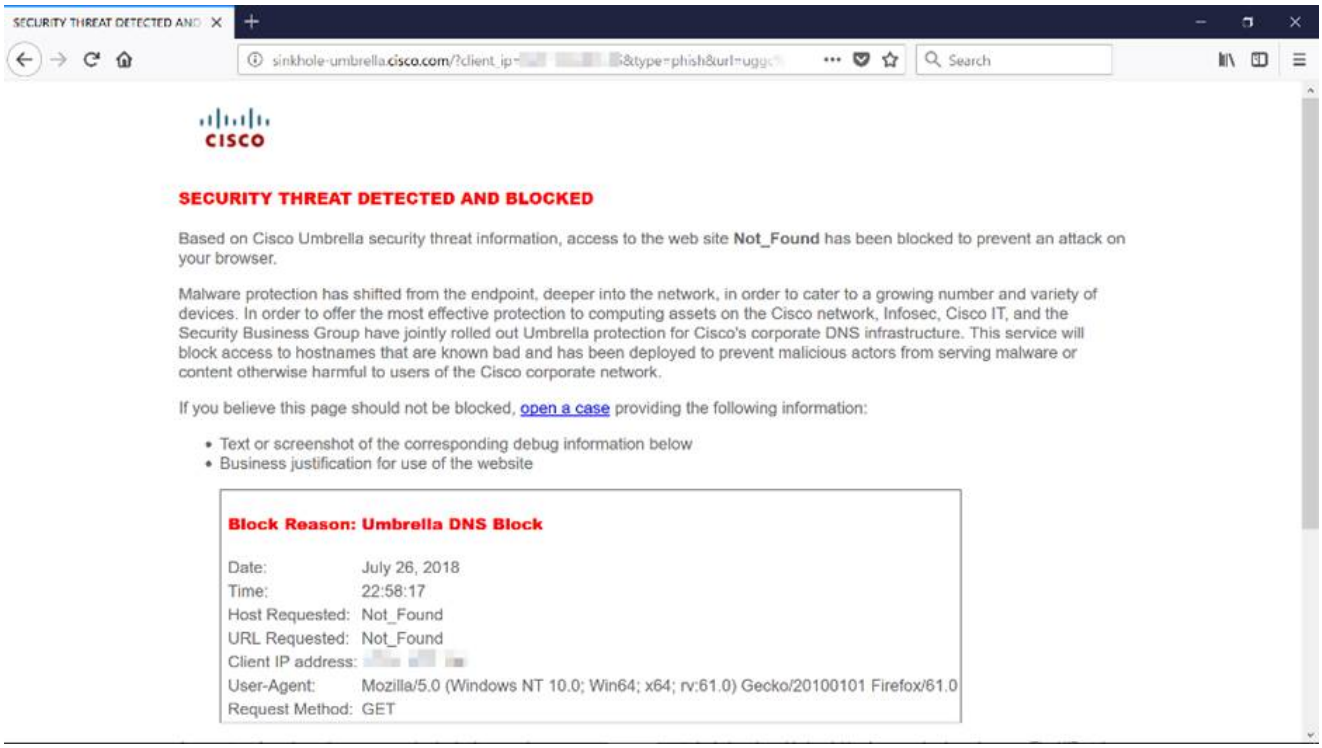
La siguiente pantalla validará los parámetros seleccionados y proporcionará una actualización cuando se haya asociado correctamente. Click OK.



Confirmación

Enhorabuena, ya está protegido por Cisco Umbrella. ¿O sí? No olvidemos que, al comprobar dos veces con un ejemplo en directo, Cisco ha creado un sitio web dedicado a determinar este aspecto 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, se le dará la bienvenida con una pantalla similar a esta.



Otras opciones de seguridad

¿Le preocupa que alguien intente acceder a la red sin autorización 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. Las instrucciones se pueden encontrar en el artículo Configure IP Source Guard on the 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 sigue garantizando 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 una conexión VPN, ya que es útil y necesario permitir a sus empleados tener acceso a su red privada incluso si se encuentran fuera de la oficina.

La VPN permite que un host remoto actúe como si estuviera ubicado 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 adapta mejor a sus necesidades, consulte Descripción general y prácticas recomendadas de Cisco Business VPN.

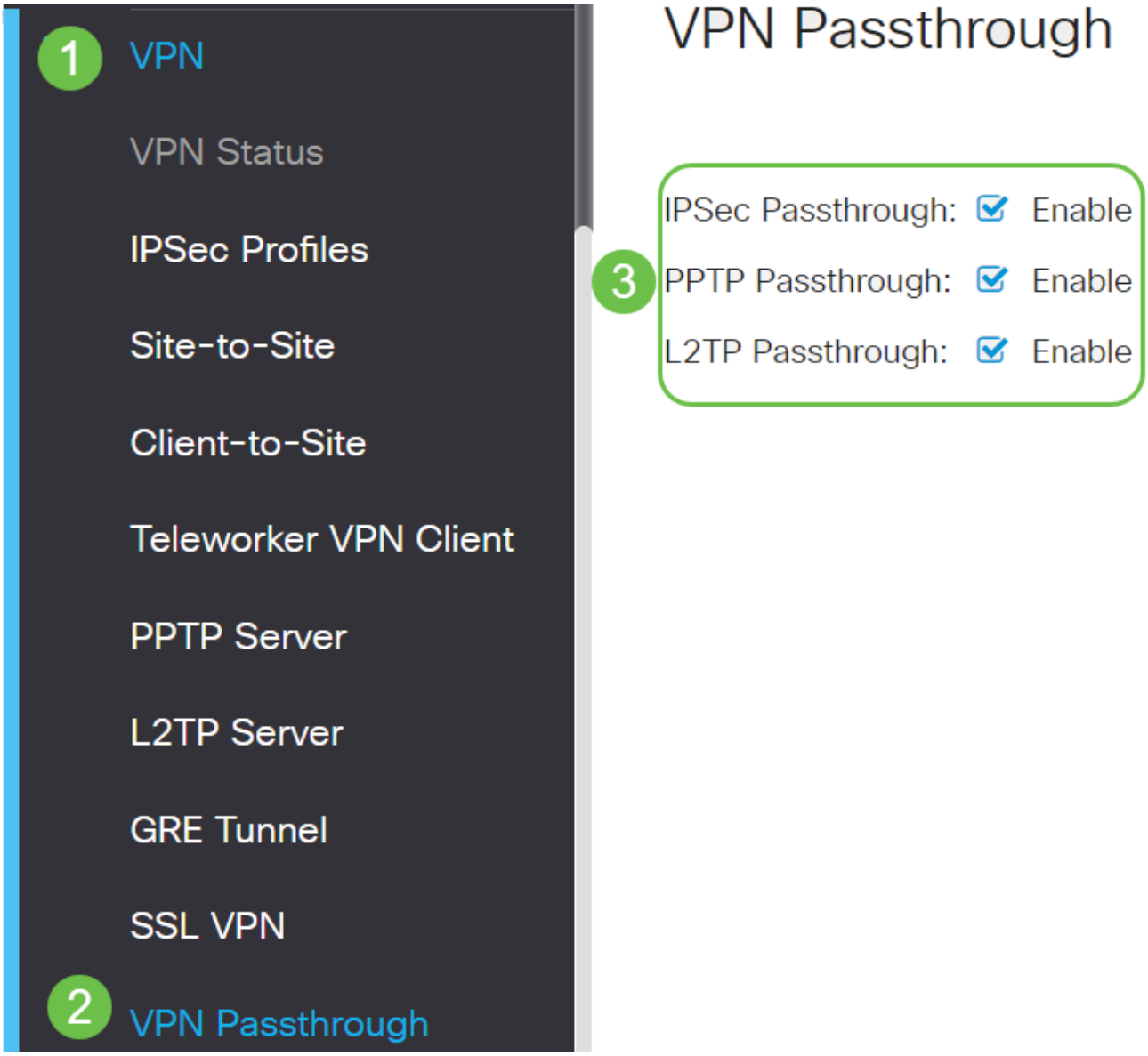
AnyConnect VPN es el único producto compatible con Cisco VPN que se muestra en esta guía de configuración. Cisco no admite productos de terceros que no sean de Cisco, como TheGreenBow y Shrew Soft. Se incluyen estrictamente con fines de orientación. Si necesita asistencia sobre estos temas más allá del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

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

Paso a través VPN

Por lo general, cada router admite la traducción de direcciones de red (NAT) para conservar las direcciones IP cuando desea admitir varios clientes con la misma conexión a Internet. Sin embargo, el protocolo de tunelación punto a punto (PPTP) y la VPN de seguridad de protocolo de Internet (IPsec) no admiten NAT. Aquí es donde entra en acción 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 los clientes VPN conectados a este router pase a través de este router y se conecte a un terminal VPN. El paso a través de VPN permite que PPTP y VPN IPsec sólo pasen a través de Internet, que se inicia desde un cliente VPN, y, a continuación, 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 (Paso a través de L2TP) están activados. Si desea ver o ajustar esta configuración, seleccione VPN > VPN Passthrough. Visualice o ajuste 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. Se puede implementar desde el dispositivo de seguridad adaptable (ASA) o desde los sistemas de implementación de software empresarial
4. Personalizable y traducible
5. Fácilmente configurado
6. Admite seguridad de protocolo de Internet (IPsec) y capa de sockets seguros (SSL)
7. Admite el protocolo Intercambio de claves de Internet 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 seleccione VPN > SSL VPN.

VPN 1

VPN Status

IPSec Profiles

Site-to-Site

Client-to-Site

Teleworker VPN Client

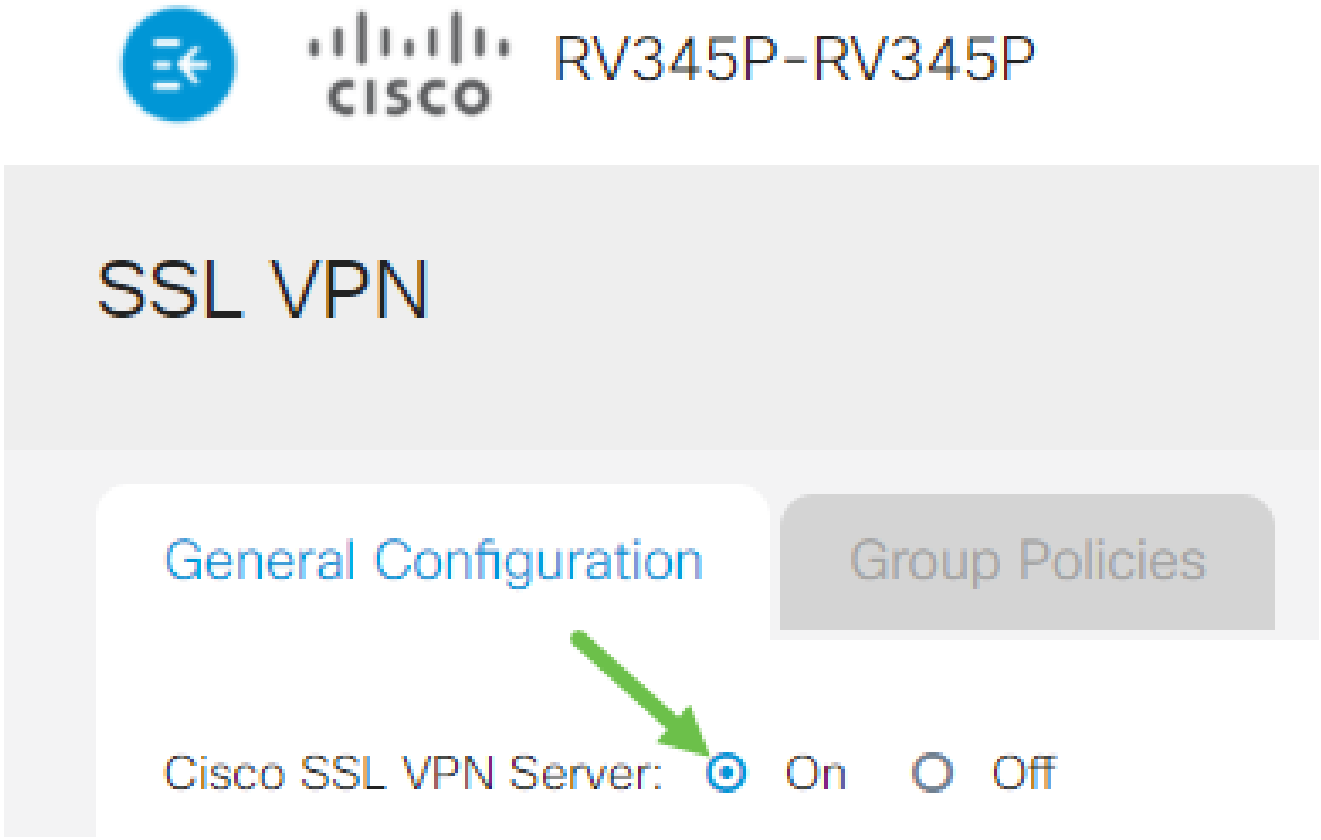
PPTP Server

L2TP Server

GRE Tunnel

Paso 2

Haga clic en el botón de radio On para habilitar el servidor Cisco SSL VPN.



Configuración de gateway obligatoria

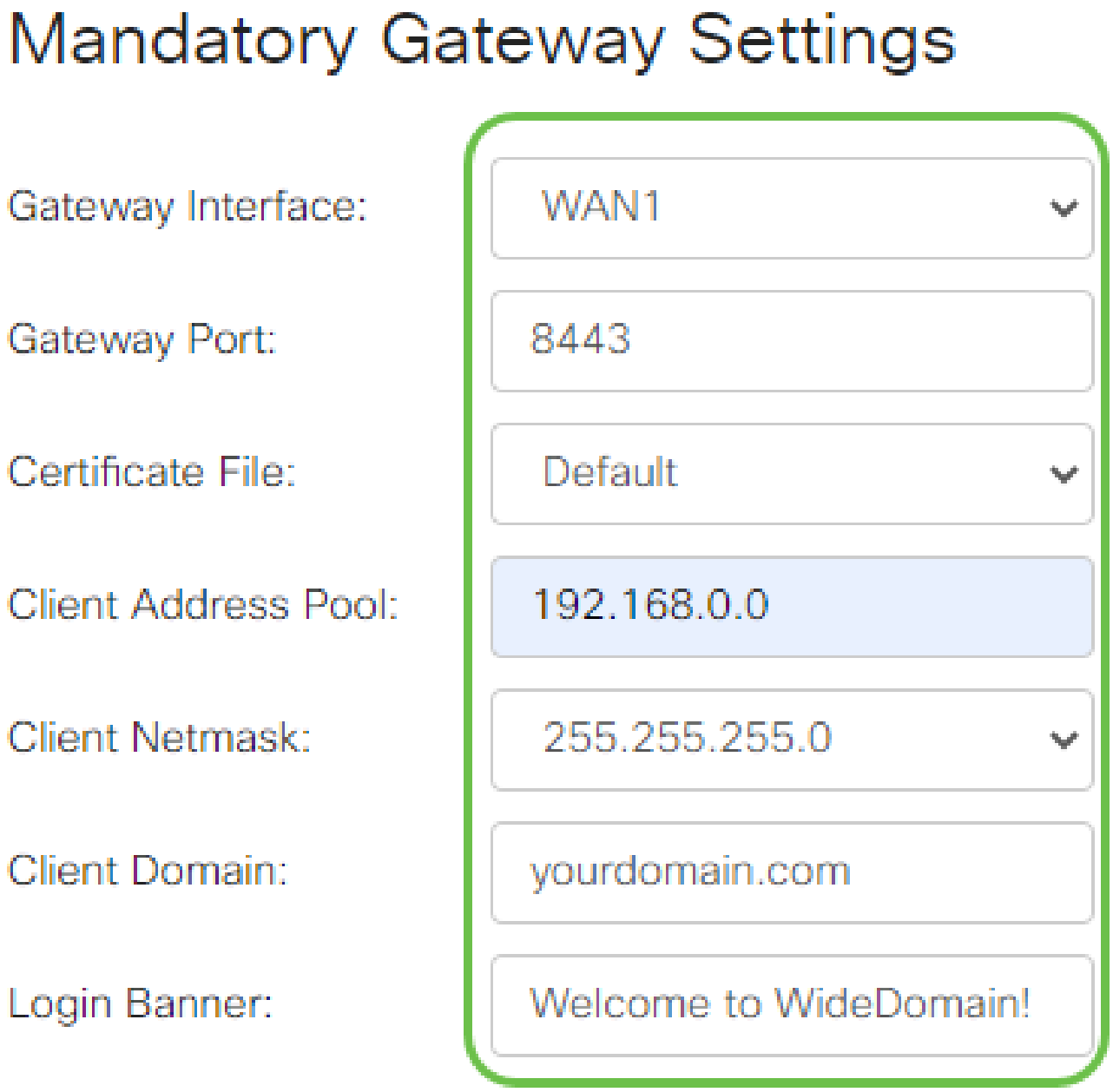
Paso 1

Los siguientes parámetros de configuración son obligatorios:

1. Seleccione la interfaz de la puerta de enlace en la lista desplegable. Este será el puerto que se utilizará para pasar el tráfico a través de los túneles VPN SSL. Las opciones 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 en la lista desplegable. Este certificado autentica a los usuarios que intentan acceder al recurso de red a través de los túneles VPN SSL. La lista desplegable contiene un certificado predeterminado y los certificados que se importan.
4. Ingrese la dirección IP del pool de direcciones del cliente en el campo Pool de Direcciones del Cliente. Este conjunto será el intervalo de direcciones IP que se asignarán a los clientes VPN remotos.

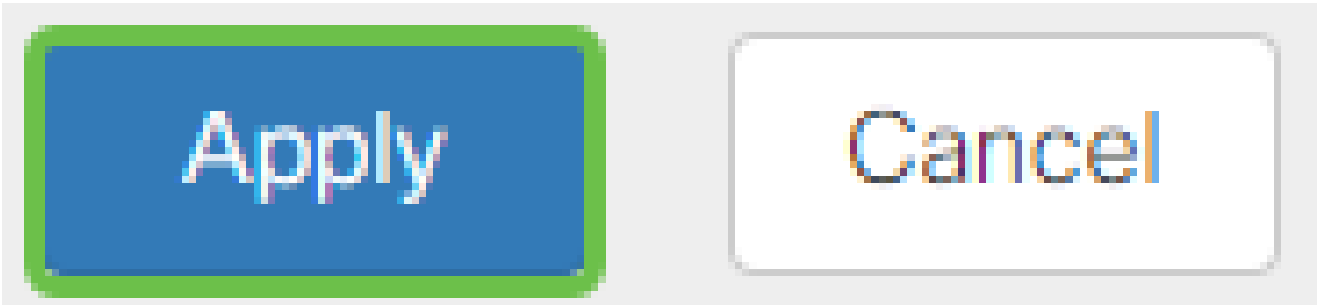
   Asegúrese de que el intervalo de direcciones IP no se superpone con ninguna de las direcciones IP de la red local.

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



Paso 2

Haga clic en Apply (Aplicar).

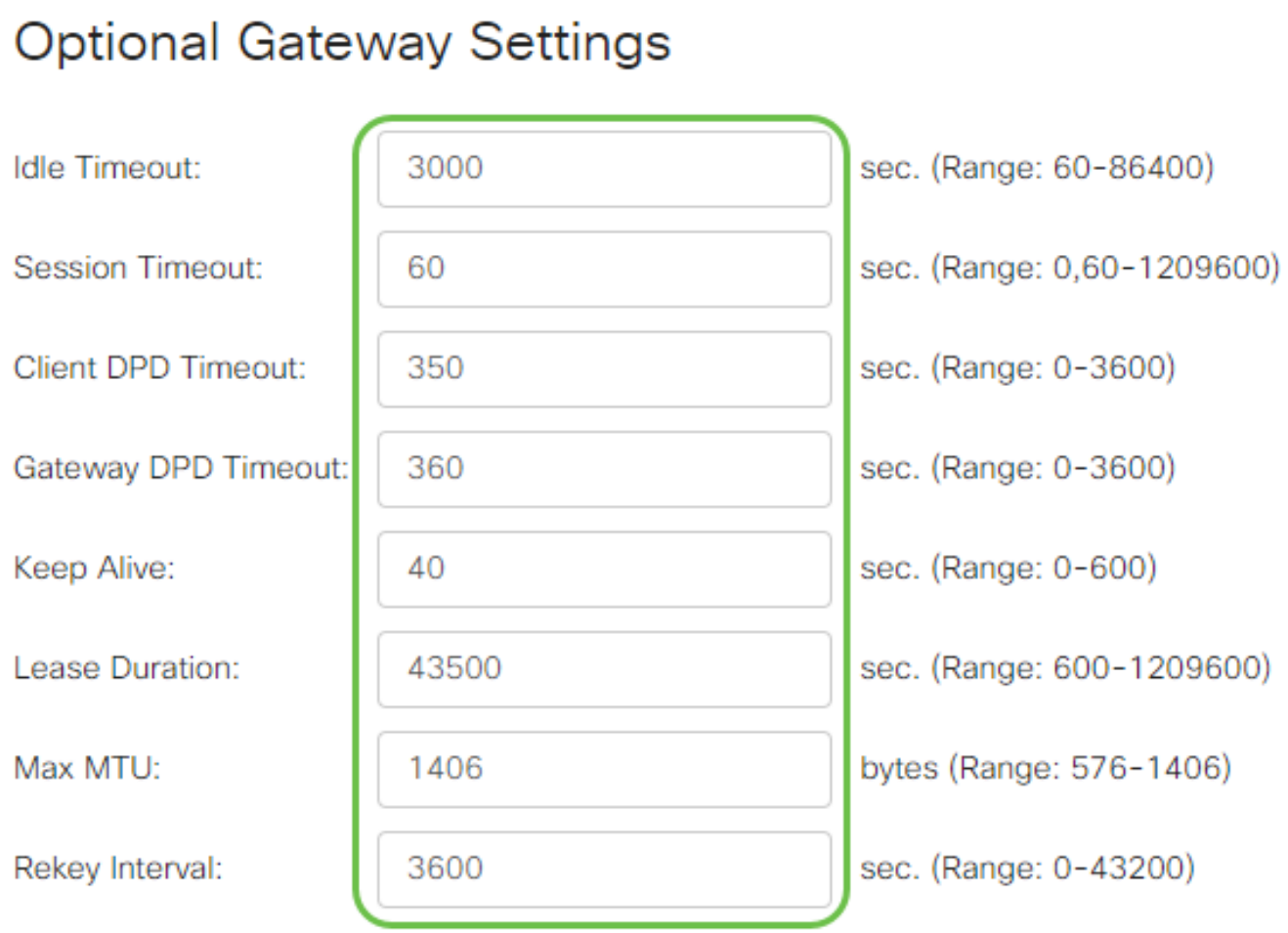


Configuración de gateway opcional

Paso 1

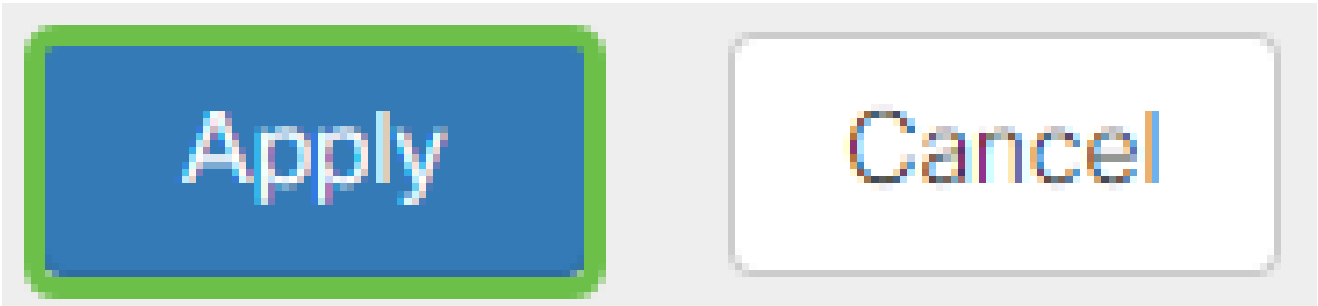
Los siguientes parámetros de configuración son opcionales:

1. Introduzca un valor en segundos para el tiempo de espera de inactividad comprendido entre 60 y 86400. Este será el tiempo que la sesión VPN SSL 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 de Protocolo de control de transmisión (TCP) o Protocolo de datagramas de usuario (UDP) en agotarse después del tiempo de inactividad especificado. El intervalo es de 60 a 1209600.
3. Introduzca un valor en segundos en el campo ClientDPD Timeout que va de 0 a 3600. Este valor especifica el envío periódico de mensajes HELLO/ACK para comprobar el estado del túnel VPN. Esta función debe estar activada en ambos extremos del túnel VPN.
4. Introduzca un valor en segundos en el campo GatewayDPD Timeout que va de 0 a 3600. Este valor especifica el envío periódico de mensajes HELLO/ACK para comprobar el estado del túnel VPN. Esta función debe estar activada en ambos extremos del túnel VPN.
5. Introduzca un valor en segundos en el campo Keep Alive que oscila entre 0 y 600. Esta función garantiza que el router esté siempre conectado a Internet. Si se interrumpe, intentará restablecer la conexión VPN.
6. Introduzca un valor en segundos para la duración del túnel que se va a conectar en el campo Duración del arrendamiento. El intervalo es de 600 a 1209600.
7. Introduzca el tamaño del paquete en bytes que se puede enviar a través de la red. El intervalo es de 576 a 1406.
8. Introduzca el tiempo del intervalo de retransmisión en el campo Rekey Interval. La función Rekey permite que las claves SSL se renegocien después de que se haya establecido la sesión. El intervalo es de 0 a 43200.



Paso 2

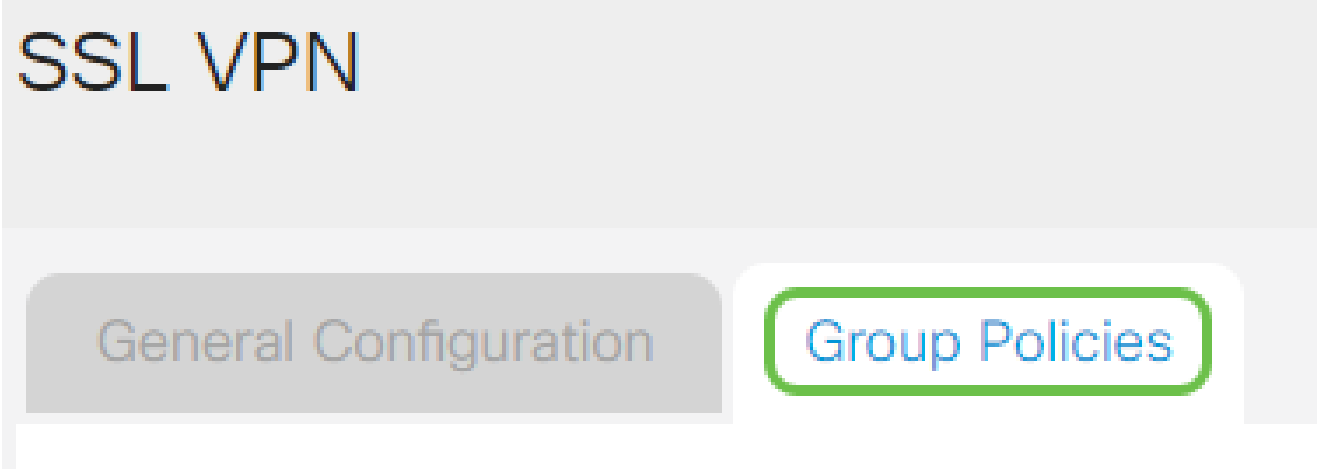
Haga clic en Apply (Aplicar).



Configurar directivas de grupo

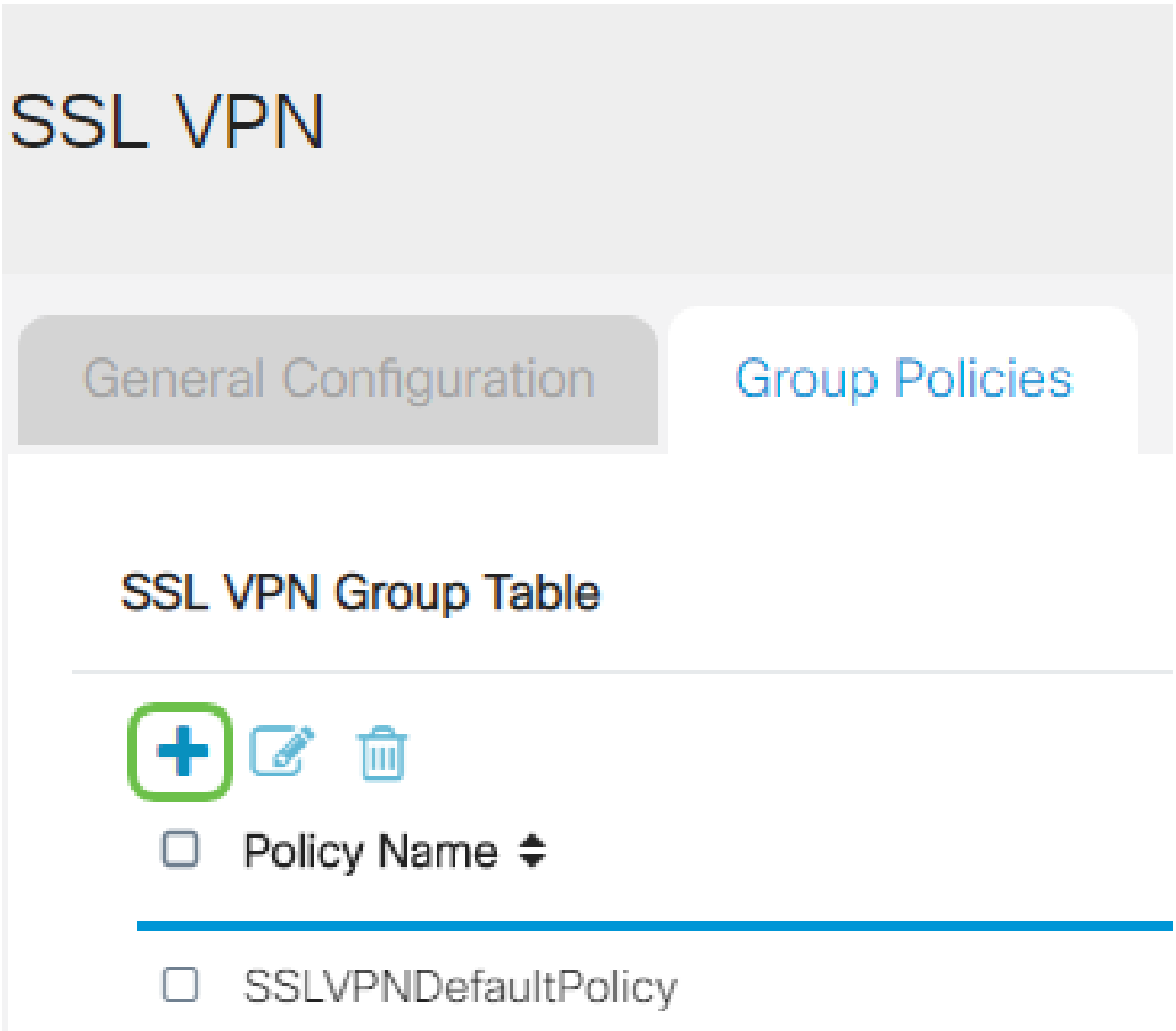
Paso 1

Haga clic en la ficha Directivas de grupo.



Paso 2

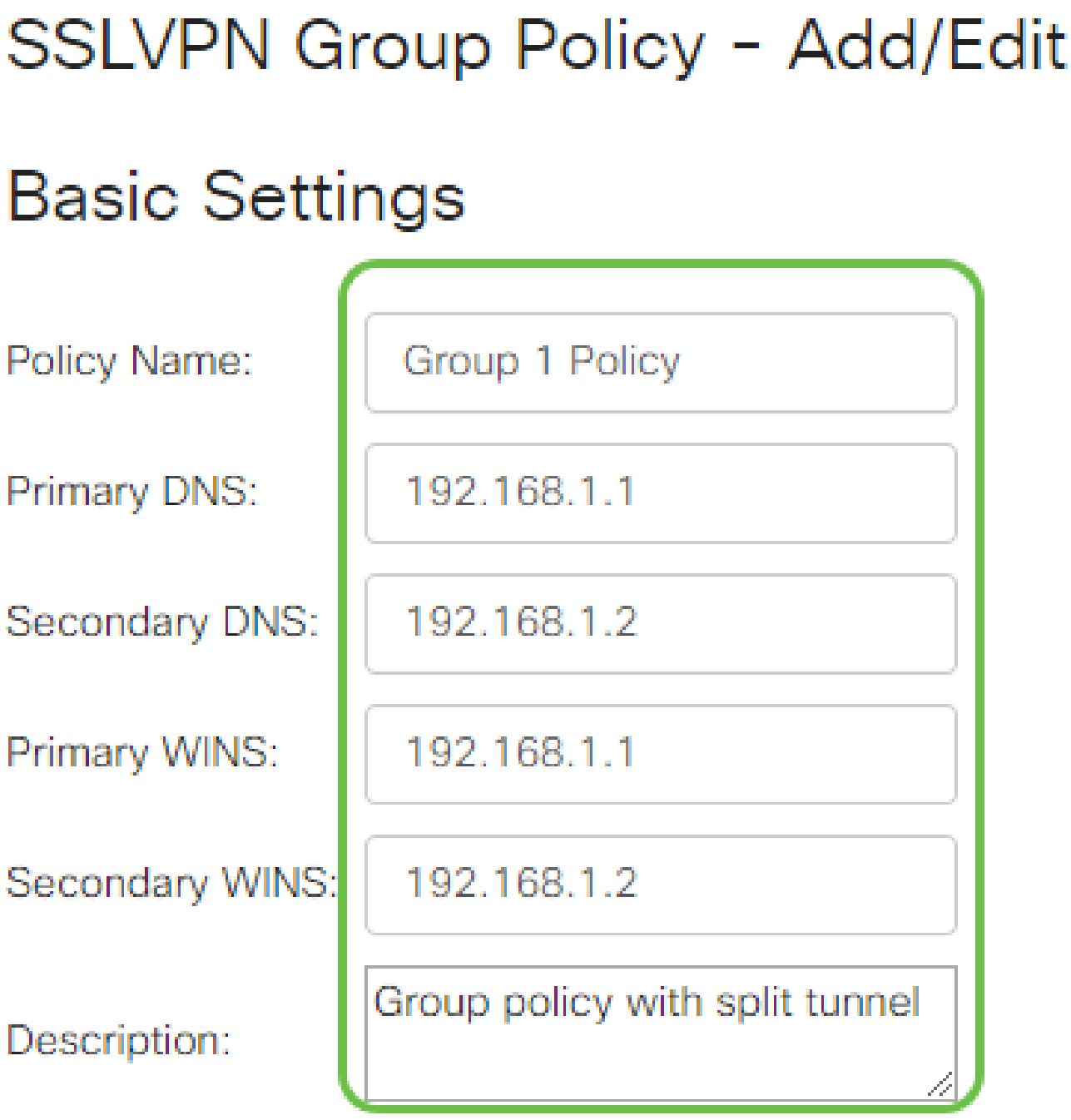
Haga clic en el icono add bajo la SSL VPN Group Table para agregar una política de grupo.



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

Paso 3

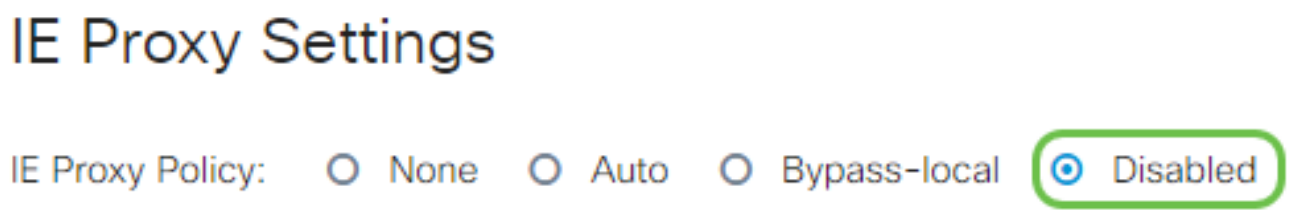
1. Introduzca el nombre de la política que prefiera en el campo Nombre de Política.
2. Introduzca la dirección IP del DNS principal en el campo proporcionado. De forma predeterminada, esta dirección IP ya se proporciona.
3. (Opcional) Introduzca la dirección IP del DNS secundario en el campo proporcionado. Esto servirá como respaldo 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 directiva de proxy de Internet Explorer (MSIE) que permitirá a la configuración de proxy de Microsoft Internet Explorer (MSIE) establecer el túnel VPN. Las opciones son:

- None (Ninguno): permite al explorador no utilizar ninguna configuración de proxy.
- Automático: permite al explorador detectar automáticamente los parámetros de proxy.
- Bypass-local: permite al explorador omitir los parámetros de proxy configurados en el usuario remoto.
- Deshabilitado: deshabilita la configuración de proxy de MSIE.



Paso 5 (opcional)

En el área Configuración de tunelización dividida, marque la casilla de verificación Habilitar tunelización dividida para permitir que el tráfico con destino a Internet se envíe directamente a Internet sin cifrar. La tunelización completa envía todo el tráfico al dispositivo final, donde 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 desea incluir o excluir el tráfico al aplicar la tunelización dividida.

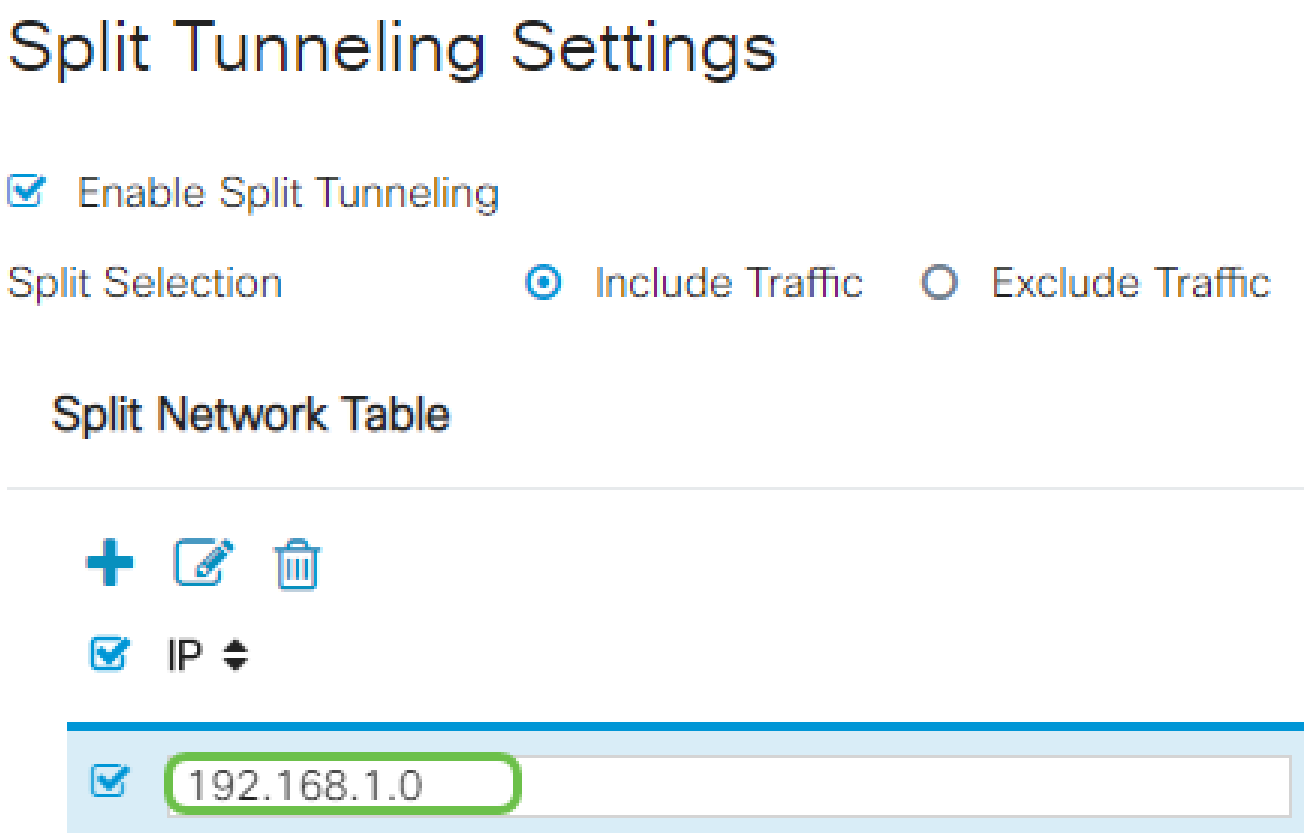
Paso 7

En la tabla de red dividida, haga clic en el icono add para agregar una excepción de red

dividida.

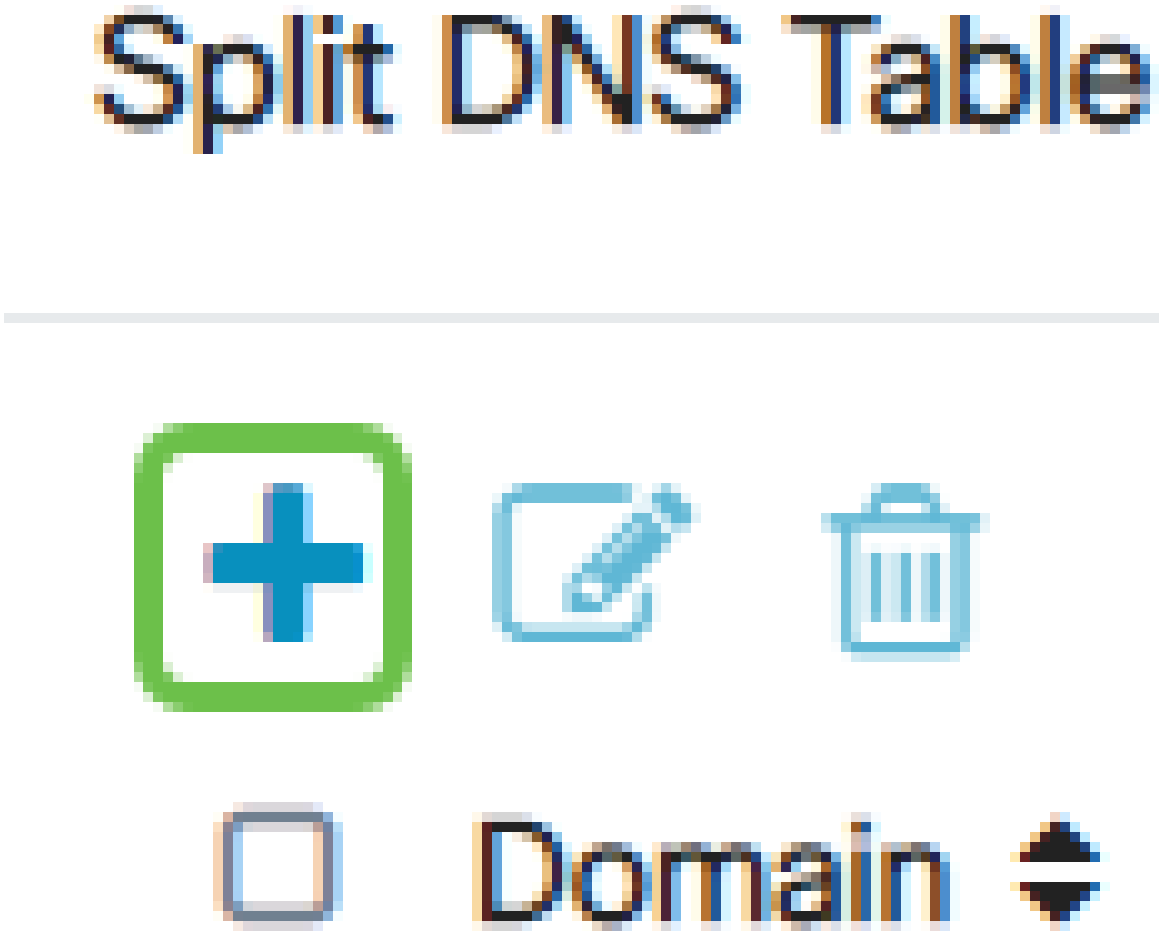
Paso 8

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



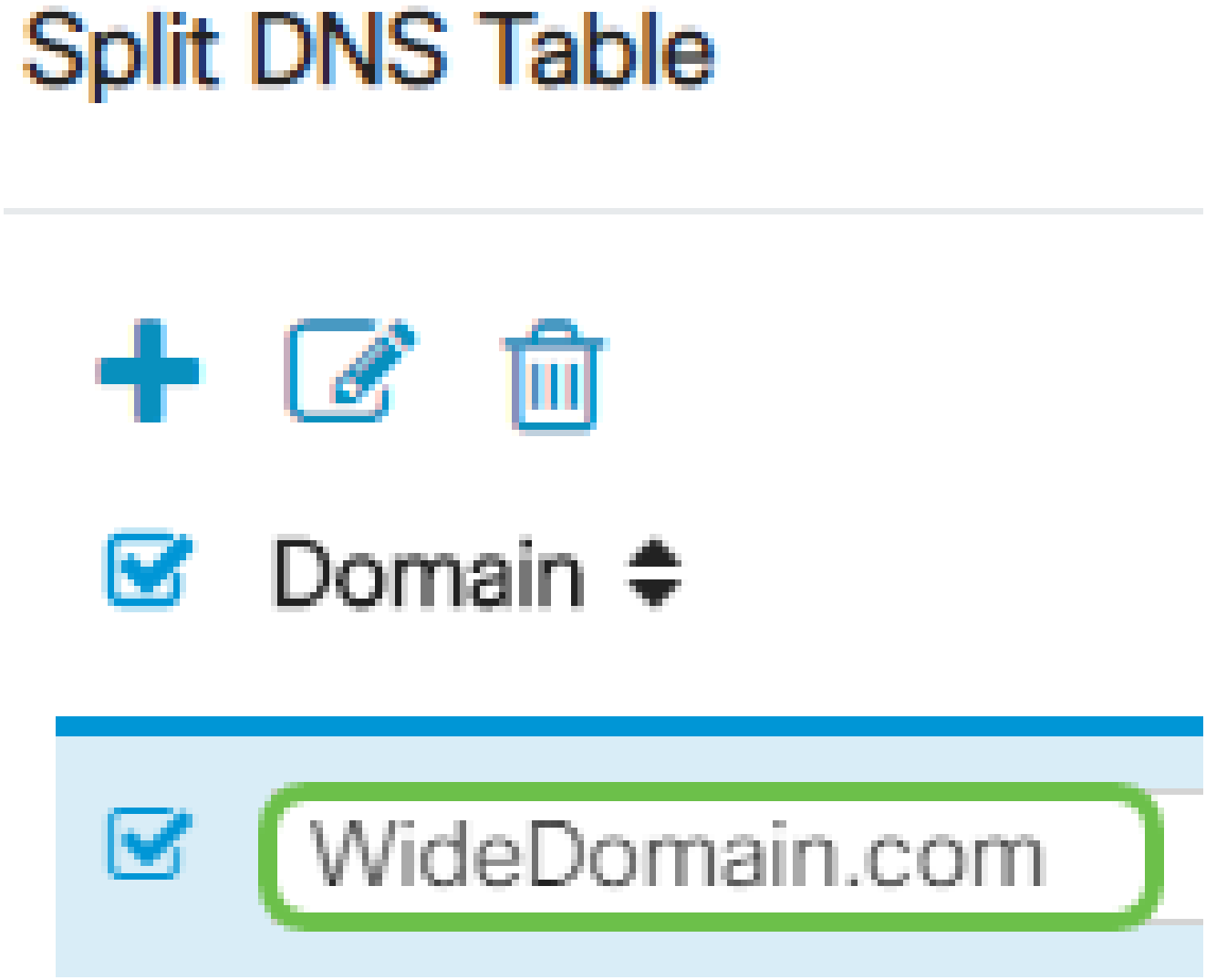
Paso 9

En la Tabla de DNS dividido, haga clic en el icono de agregar para agregar una excepción de DNS dividido.



Paso 10

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



El router viene con 2 licencias de servidor AnyConnect de forma predeterminada. Esto significa que una vez que tenga licencias de cliente 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 la siguiente sección se detalla cómo obtener licencias para sus clientes.

Cliente de movilidad AnyConnect

Un cliente VPN es un software que se instala y ejecuta 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 utilizarán para cifrar los datos. Según la ubicación física de las redes que se van a conectar, 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 independientes.

Cisco AnyConnect Secure Mobility Client es una aplicación de software para conectarse a una VPN que funciona en varios 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 disponibles 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 forma de name@domain.com.

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

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

Tenga en cuenta que la SKU del producto de la licencia de cliente AnyConnect que aparece 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 diferentes niveles de suscripción, como se indica a continuación:

- LS-AC-PLS-1Y-S1: licencia de cliente de Cisco AnyConnect Plus de 1 año
- LS-AC-PLS-3Y-S1: licencia de cliente de Cisco AnyConnect Plus de 3 años
- LS-AC-PLS-5Y-S1: licencia de cliente de Cisco AnyConnect Plus de 5 años
- LS-AC-PLS-P-25-S: paquete de 25 licencias de cliente perpetuas 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 el cliente configura una de las siguientes opciones, debe enviarles estos enlaces:

- Windows: AnyConnect en un ordenador con 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 sobre errores de Cisco AnyConnect Secure Mobility Client.

Verifique la conectividad VPN de AnyConnect

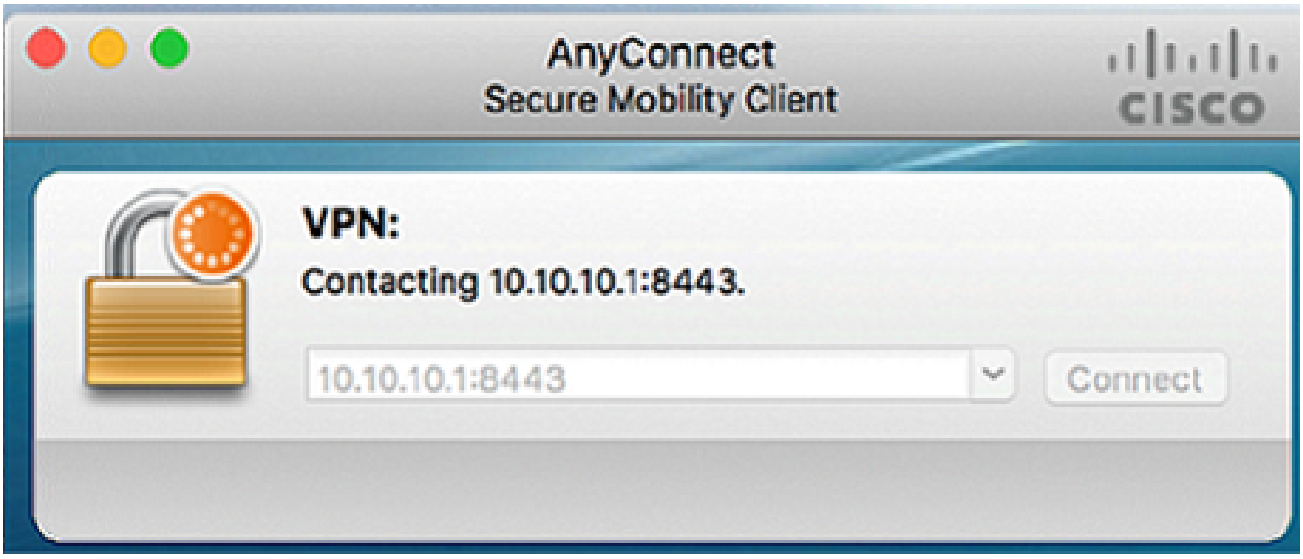
Paso 1

Haga clic en el icono de AnyConnect Secure Mobility Client.

Paso 2

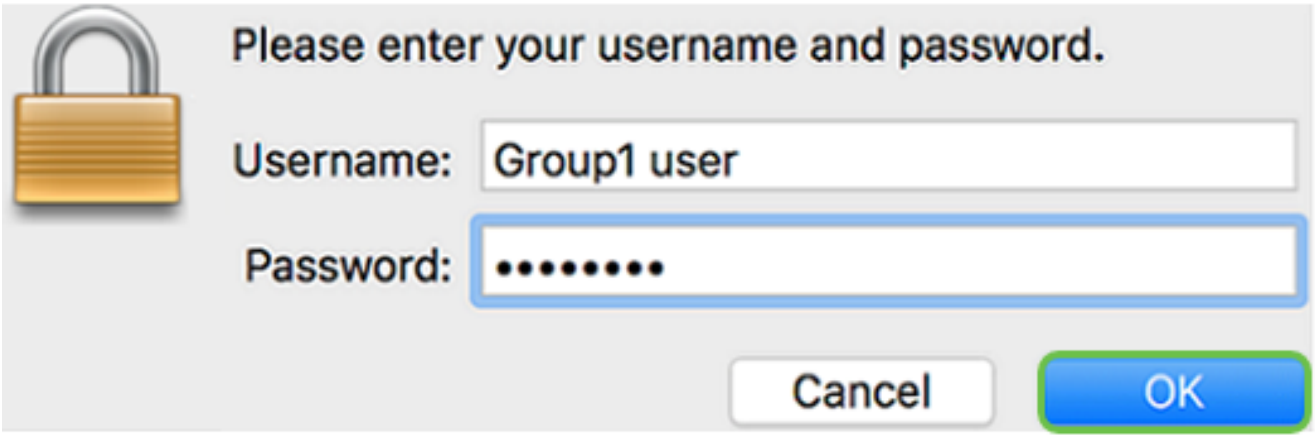
En la ventana AnyConnect Secure Mobility Client, introduzca la dirección IP y el número de puerto de la puerta de enlace separados por dos puntos (:) y, a continuación, haga clic en Connect.

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



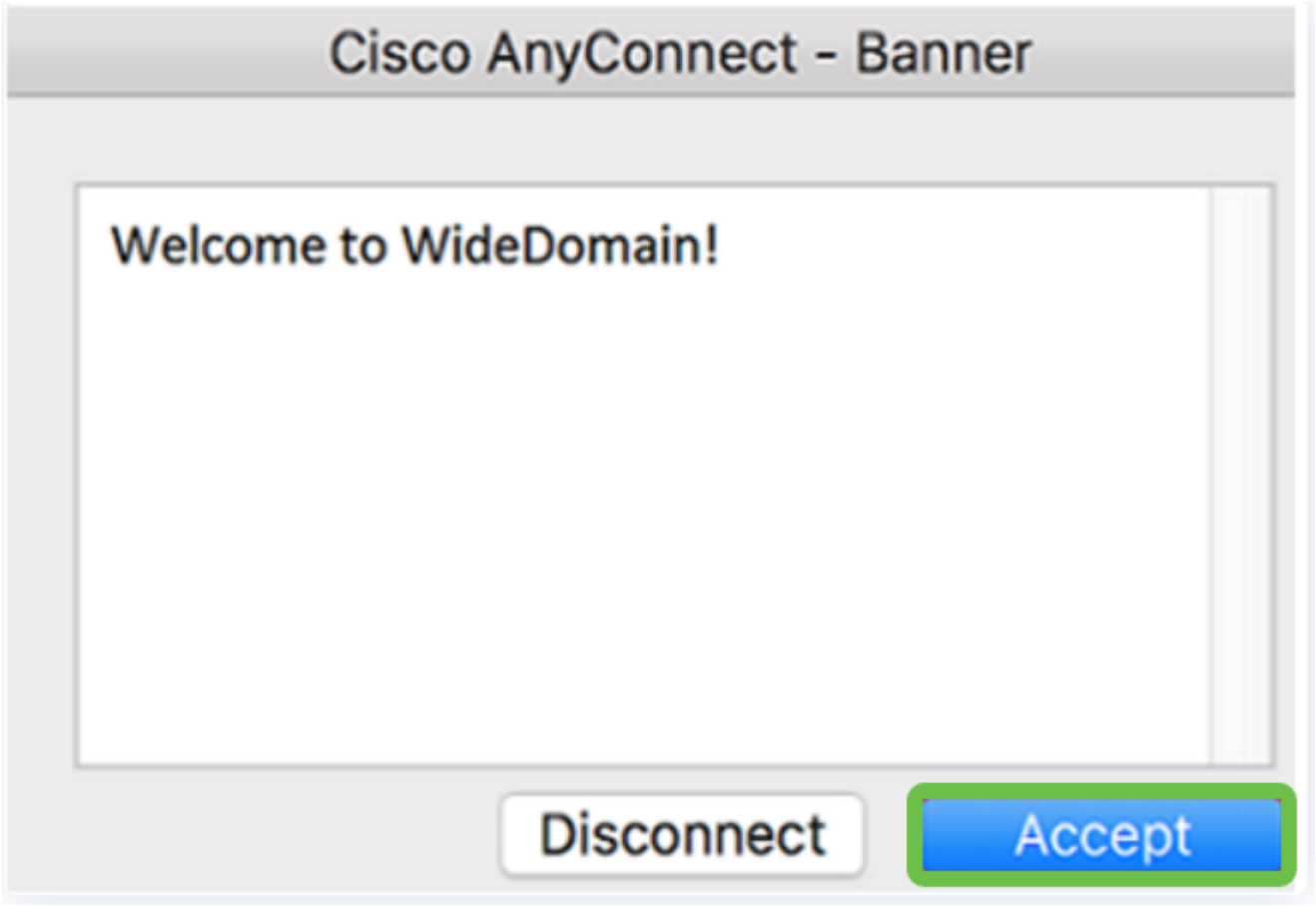
Paso 3

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

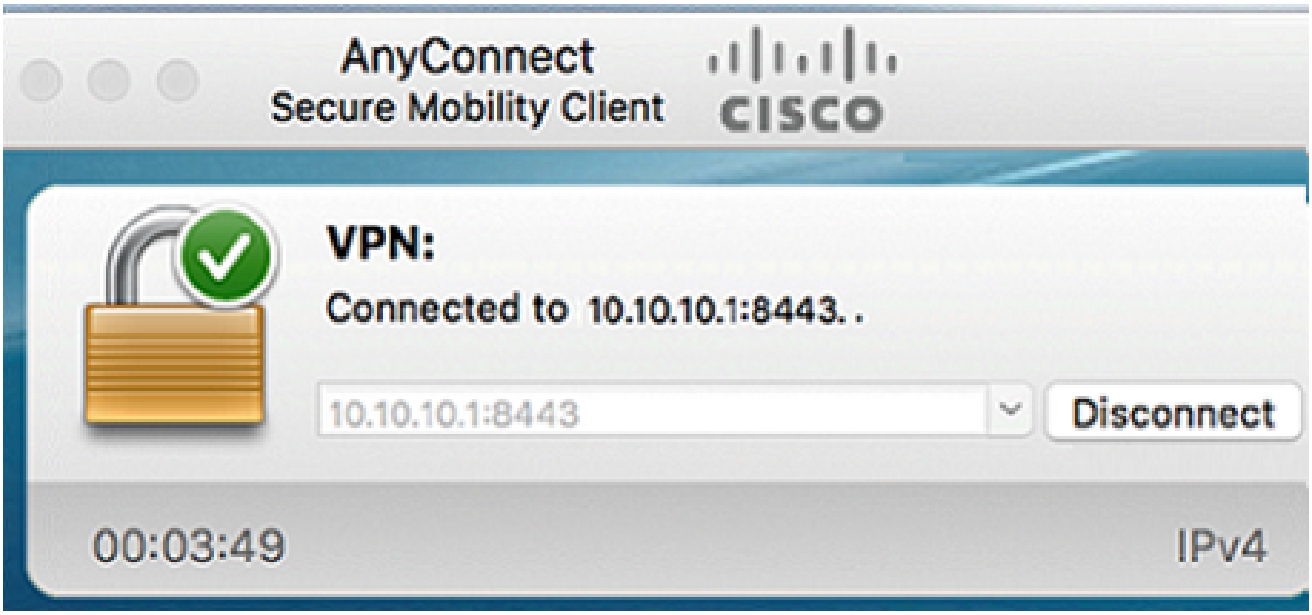


Paso 4

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 utiliza AnyConnect VPN, puede saltarse 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 cliente VPN Shrew Soft. Esta sección le mostrará cómo configurar su router y el cliente de software de Shrew para asegurar una conexión a una VPN.

Cisco no es compatible con Shrew Soft. Este ejemplo sólo se proporciona con fines de demostración. Si tiene problemas con Shrew Soft, por favor póngase en contacto con ellos para obtener ayuda.

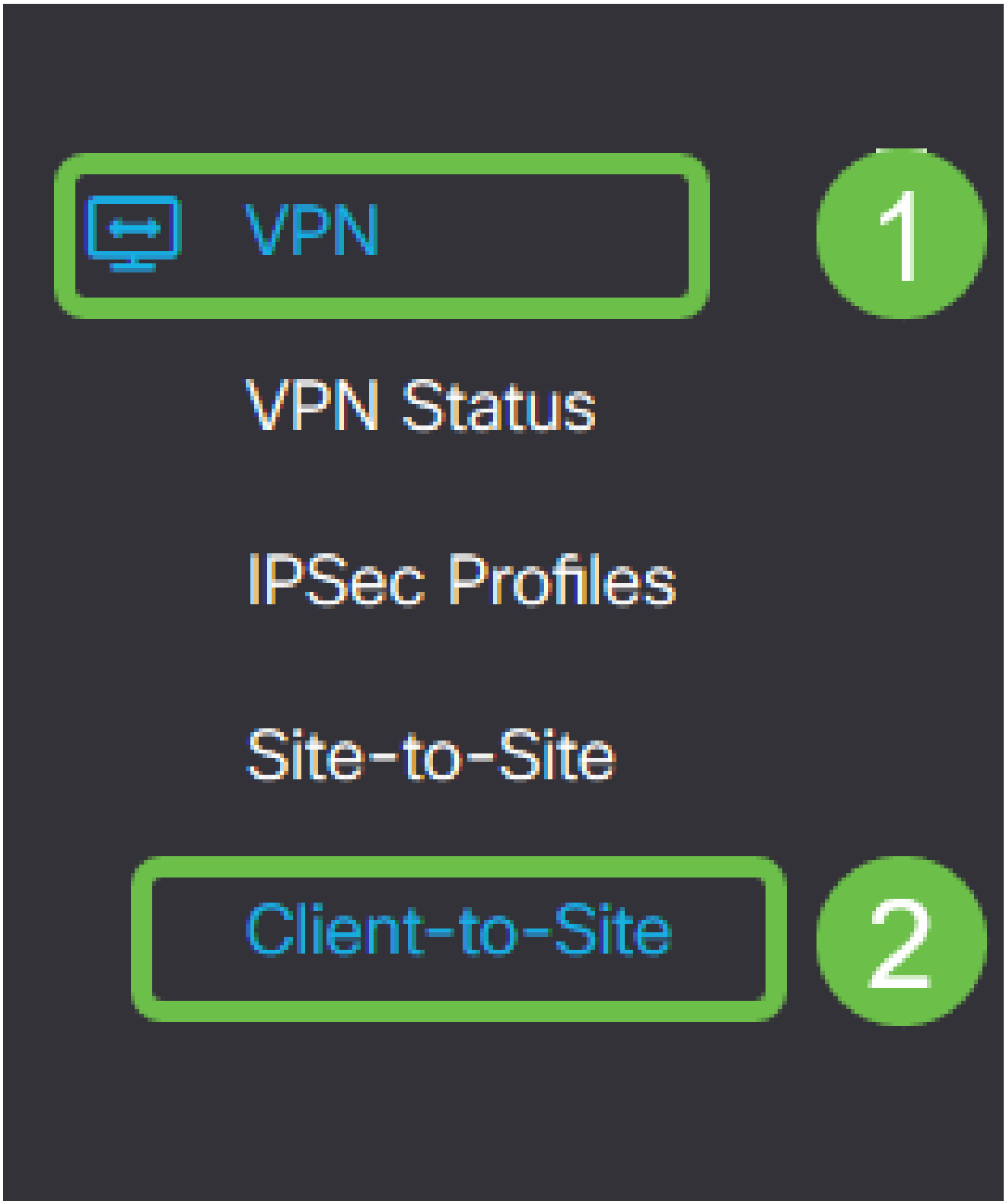
Puede descargar la última versión del software cliente Shrew Soft VPN aquí: https://www.shrew.net/download/vpn

Configuración de Shrew Soft en el router serie RV345P

Empezaremos configurando la VPN de cliente a sitio en el RV345P.

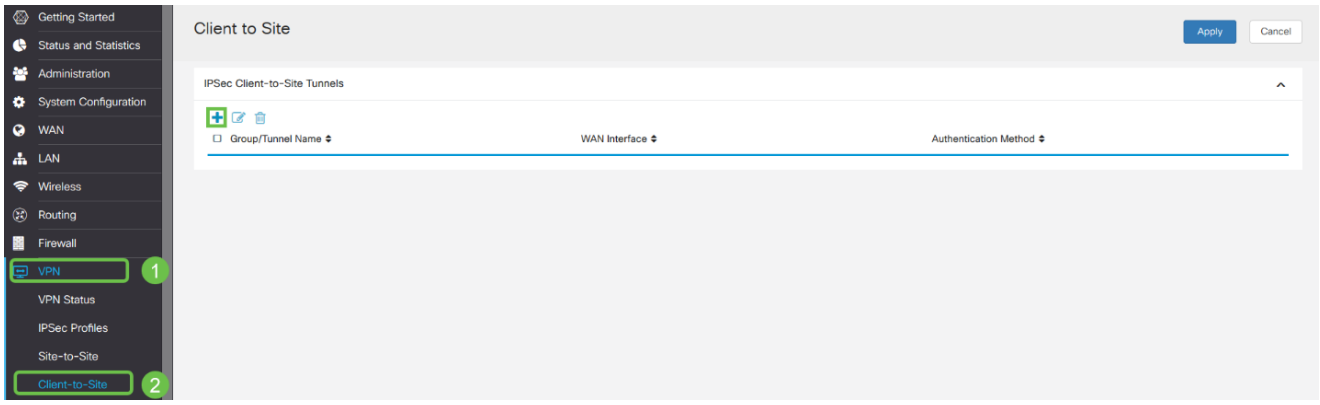
Paso 1

Vaya a VPN > Client-to-Site.



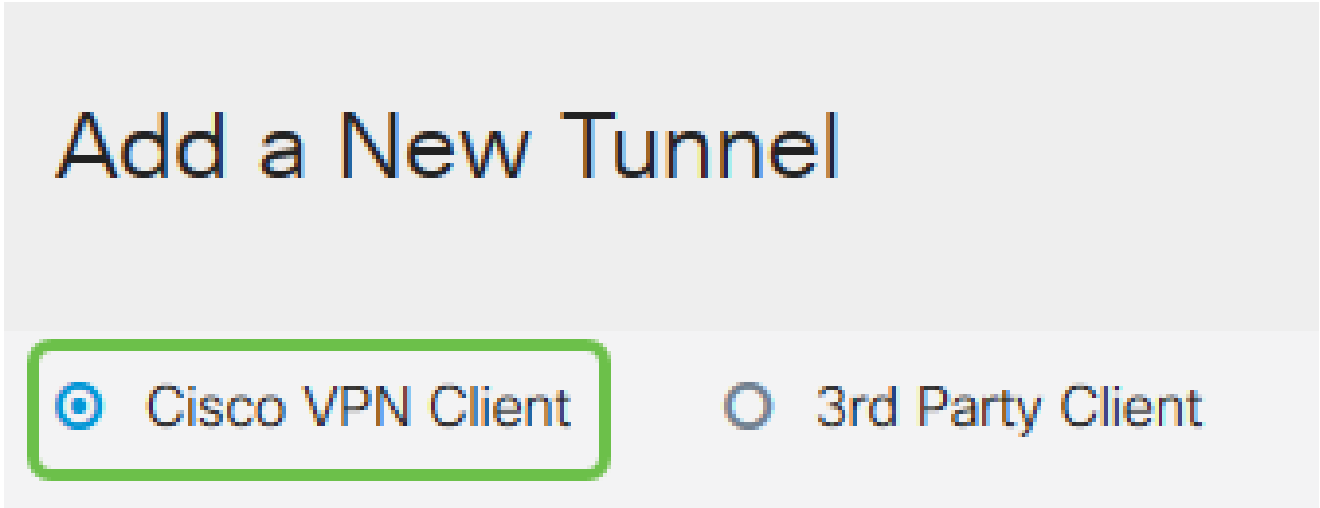
Paso 2

Agregue un perfil VPN de cliente a sitio.



Paso 3

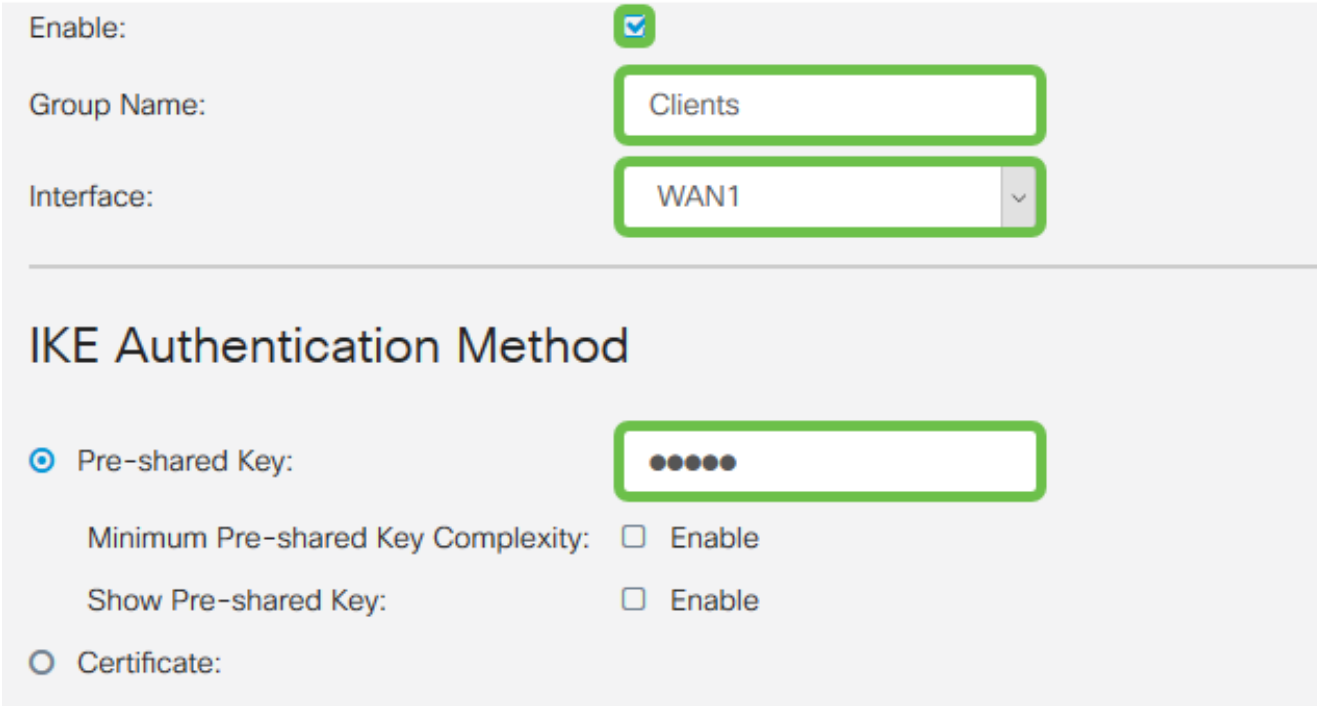
Seleccione la opción Cisco VPN Client.



Paso 4

Marque la casilla Enable para activar el perfil de cliente VPN. También configuraremos el nombre de grupo, seleccionaremos la interfaz WAN e ingresaremos una clave previamente compartida.

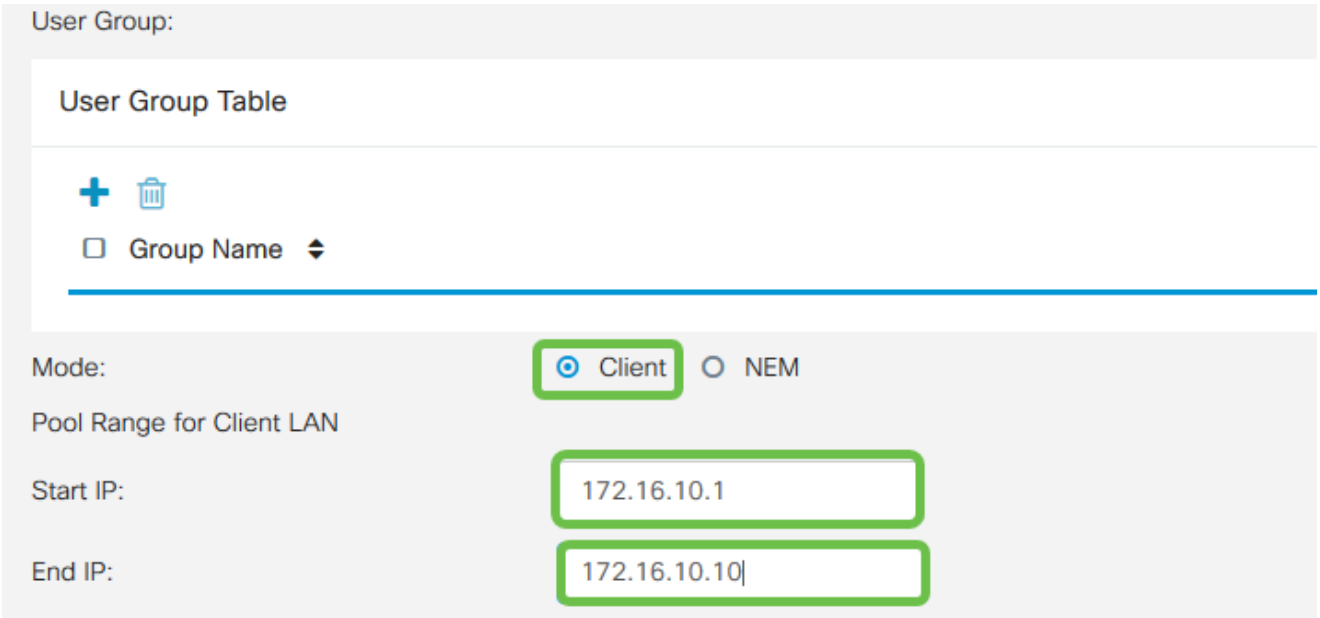
Tenga en cuenta el nombre de grupo y la clave precompartida, ya que se utilizarán más adelante al configurar el cliente.



Paso 5

Por el momento, deje la Tabla de Grupos de Usuarios en blanco. Esto es para el grupo de usuarios en el router, pero aún no lo hemos configurado. Asegúrese de que Mode esté configurado en Client. Ingrese el Rango de Conjunto para LAN Cliente. Utilizaremos desde 172.16.10.1 hasta 172.16.10.10.

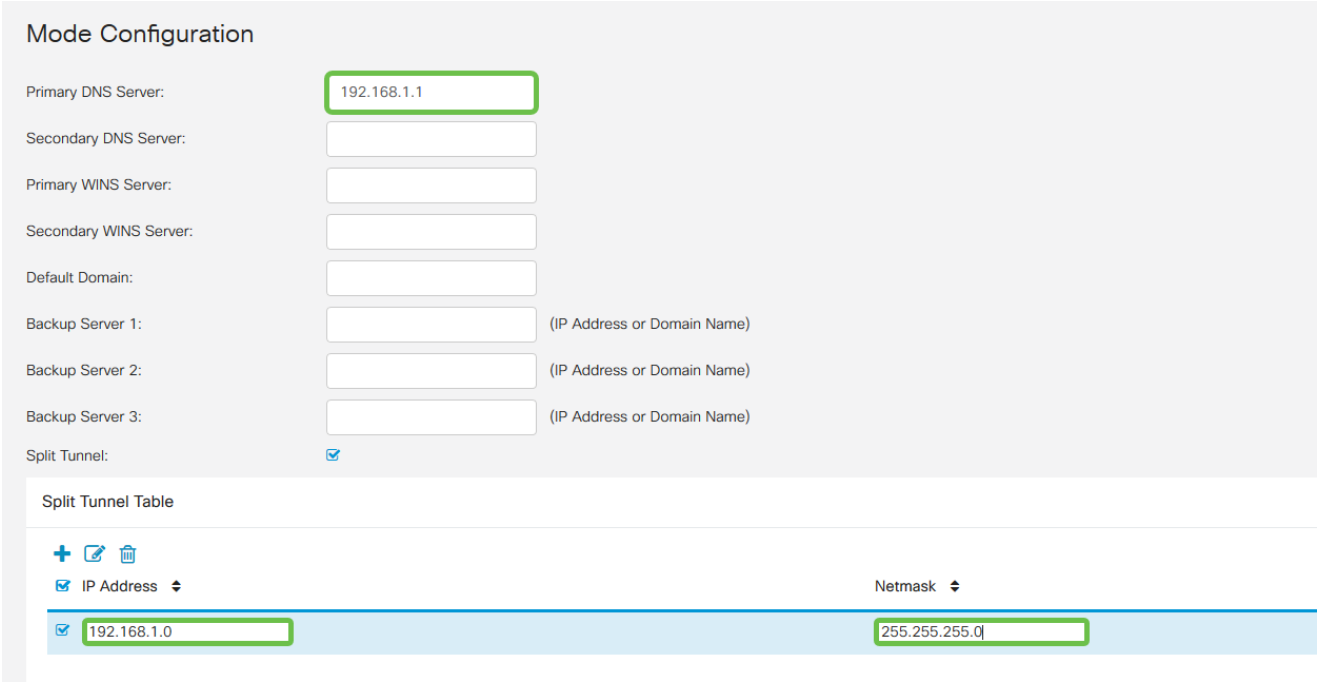
El rango de conjunto debe utilizar una subred única que no se utilice en ningún otro lugar de la red.



Paso 6

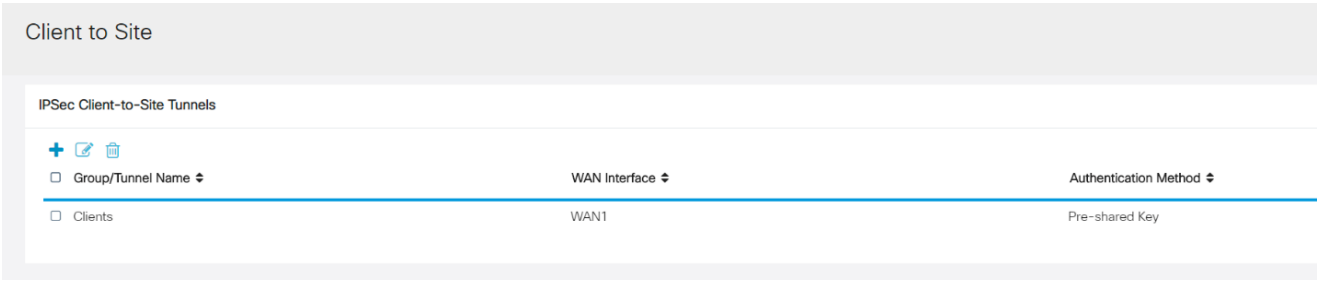
Aquí es donde configuramos los parámetros Mode Configuration. Estos son los parámetros que utilizaremos:

- Servidor DNS principal: 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 la LAN RV345P. Utilizaremos el valor predeterminado en nuestro ejemplo.
- Túnel dividido: active esta opción para activar el túnel dividido. 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. En este ejemplo se utiliza la red LAN RV345P.



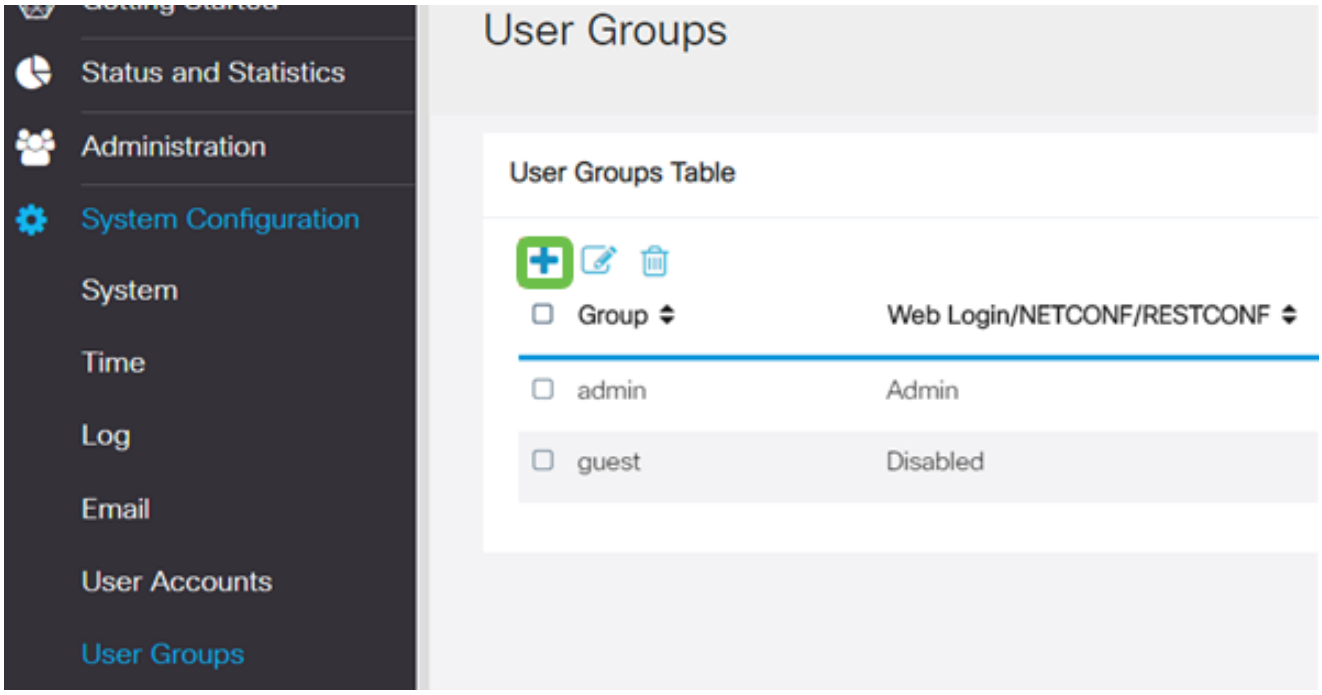
Paso 7

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



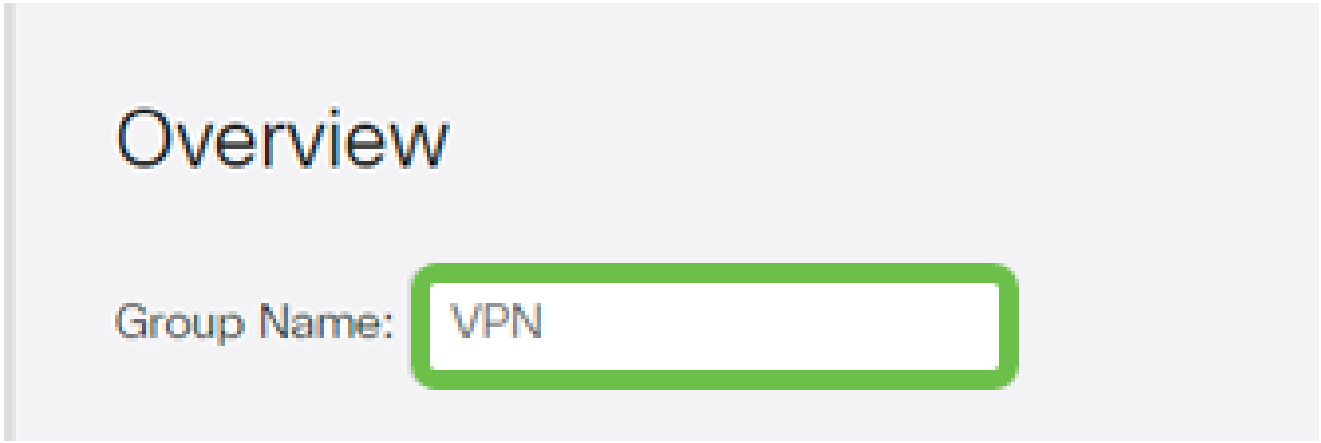
Paso 8

Configure un grupo de usuarios que se utilizará para autenticar usuarios de cliente VPN. En System Configuration > User Groups, haga clic en el icono más para agregar un grupo de usuarios.



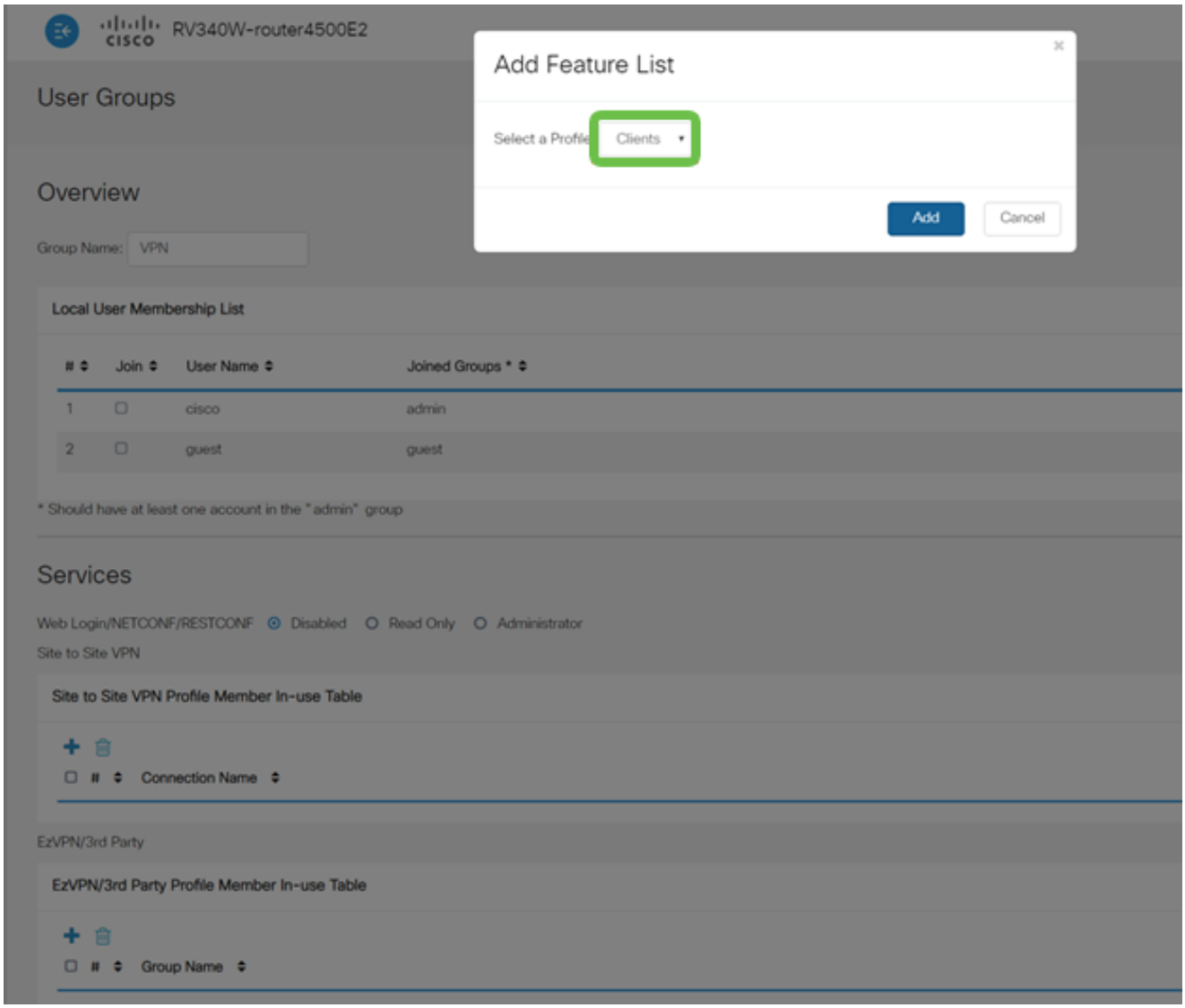
Paso 9

Introduzca un nombre de grupo.



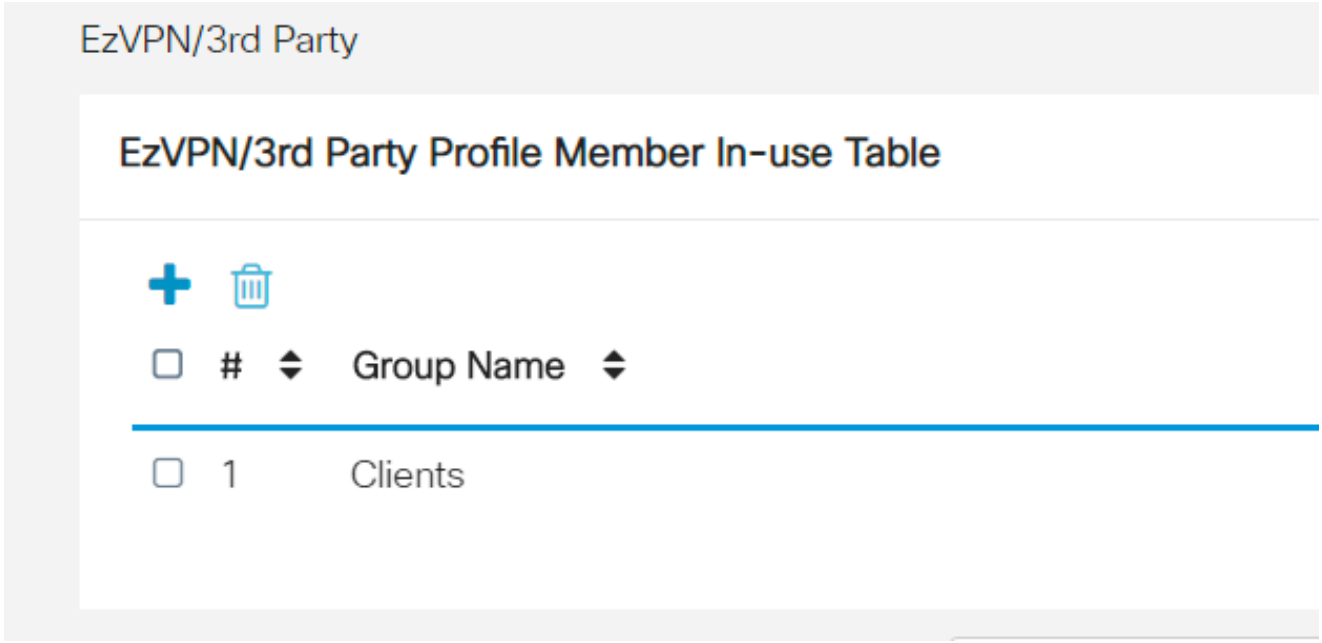
Paso 10

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.



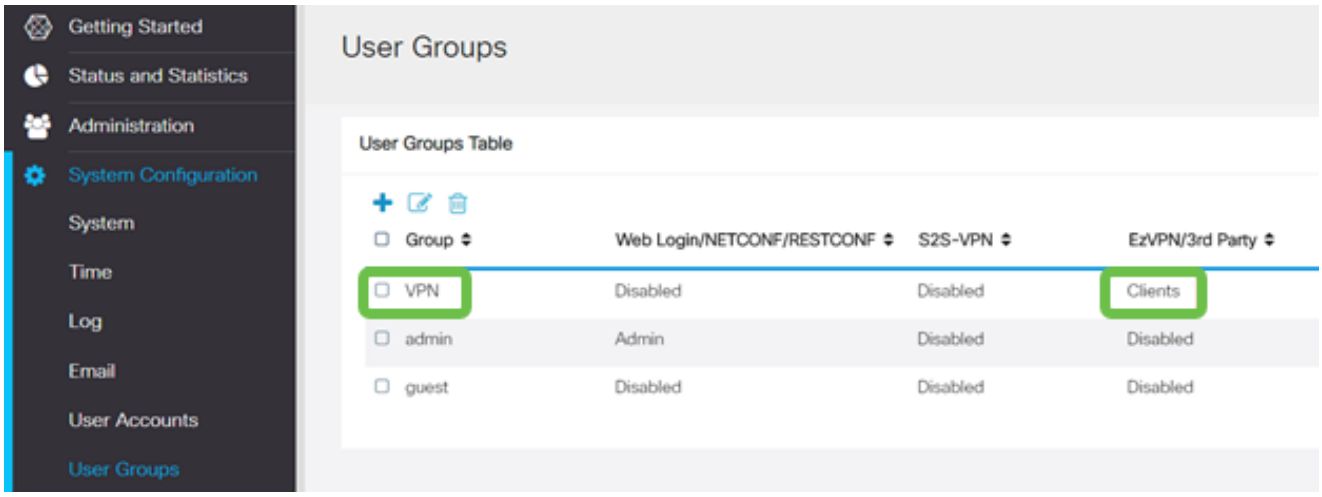
Paso 11

Ahora debería ver el nombre de grupo de cliente a sitio en la lista para EzVPN/3rd Party.



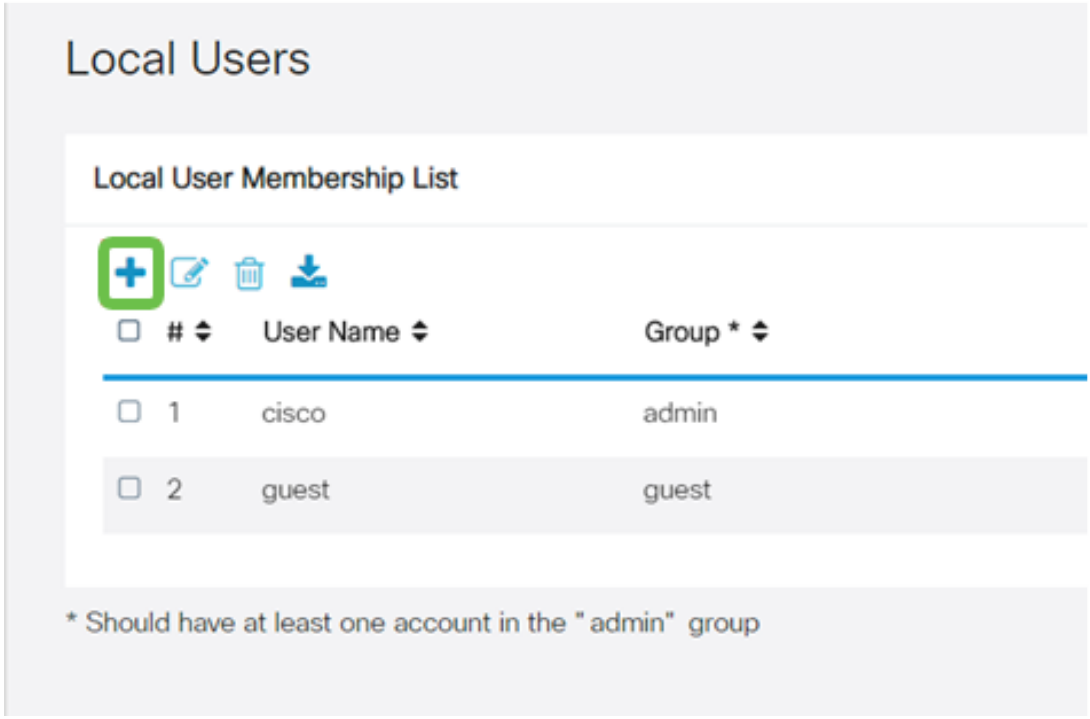
Paso 12

Después de Aplicar la configuración del 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

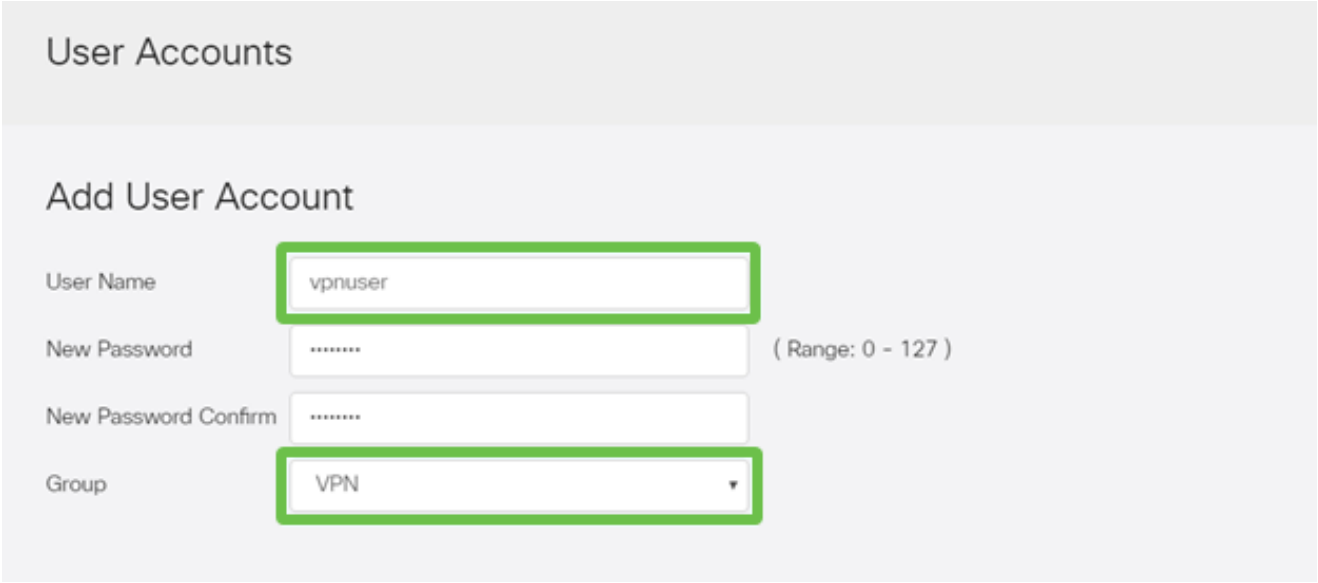
Configure un nuevo usuario en Configuración del sistema > Cuentas de usuario. Haga clic en el icono más para crear un nuevo usuario.



Paso 14

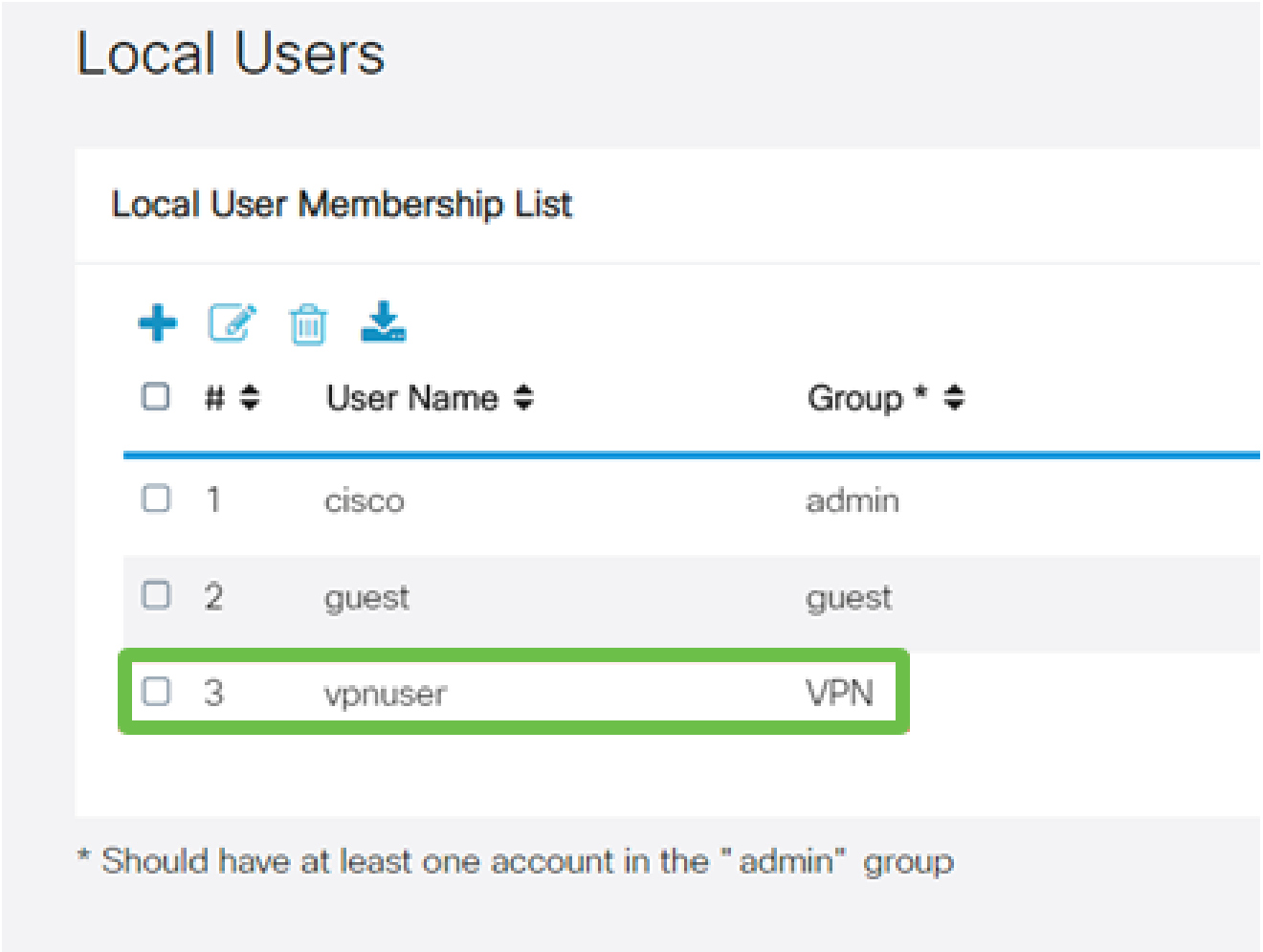
Introduzca el nuevo nombre de usuario junto con la nueva contraseña. Verifique que el

Grupo esté establecido en el nuevo Grupo de usuarios que acaba de configurar. Haga clic en Apply cuando termine.



Paso 15

El nuevo Usuario aparecerá en la lista de Usuarios locales.



Con esto finaliza la configuración del router de la serie RV345P. A continuación, configurará

el cliente VPN de Shrew Soft.

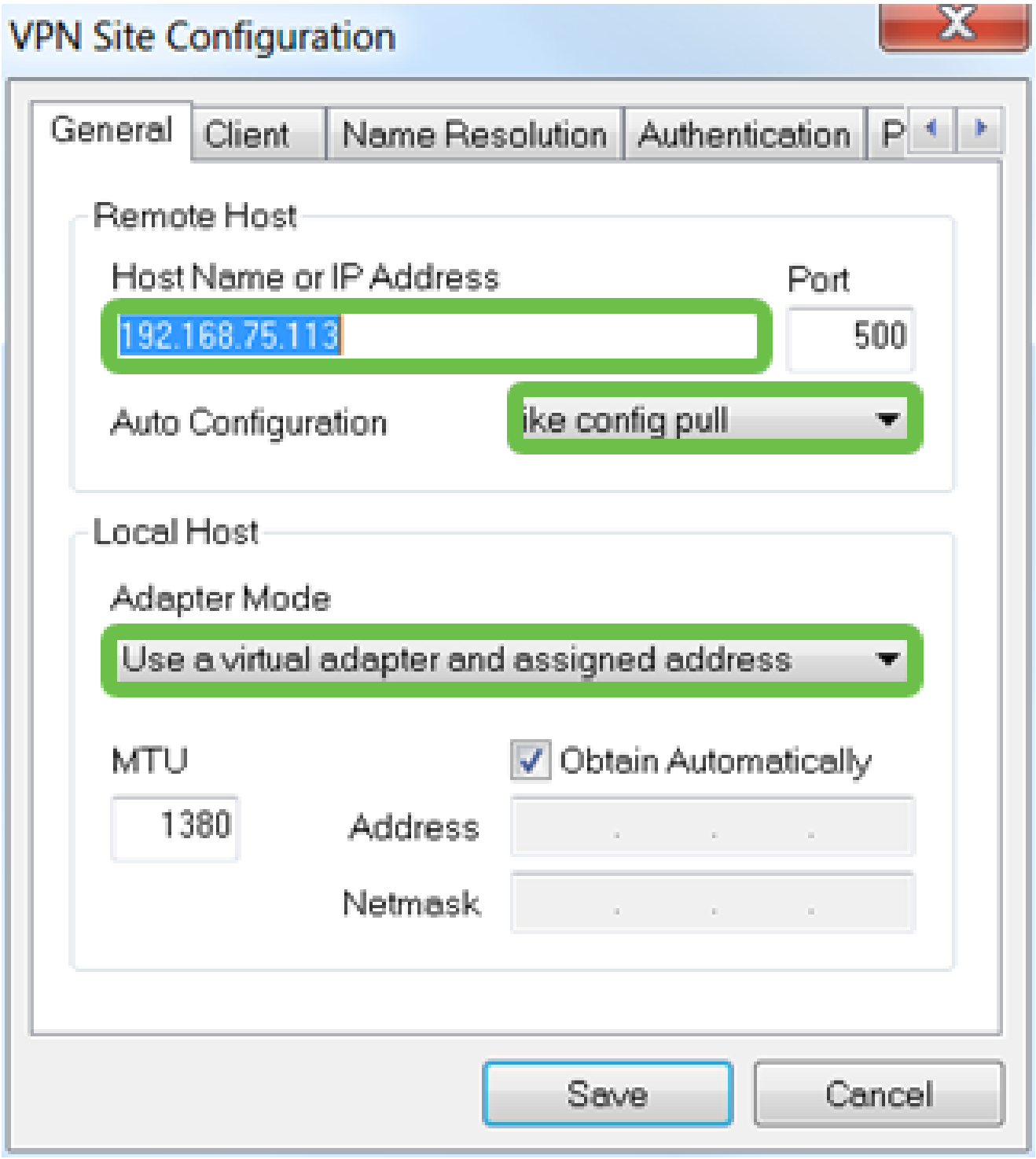
Configuración del cliente Shrew Soft VPN

Siga los pasos descriptos a continuación.

Paso 1

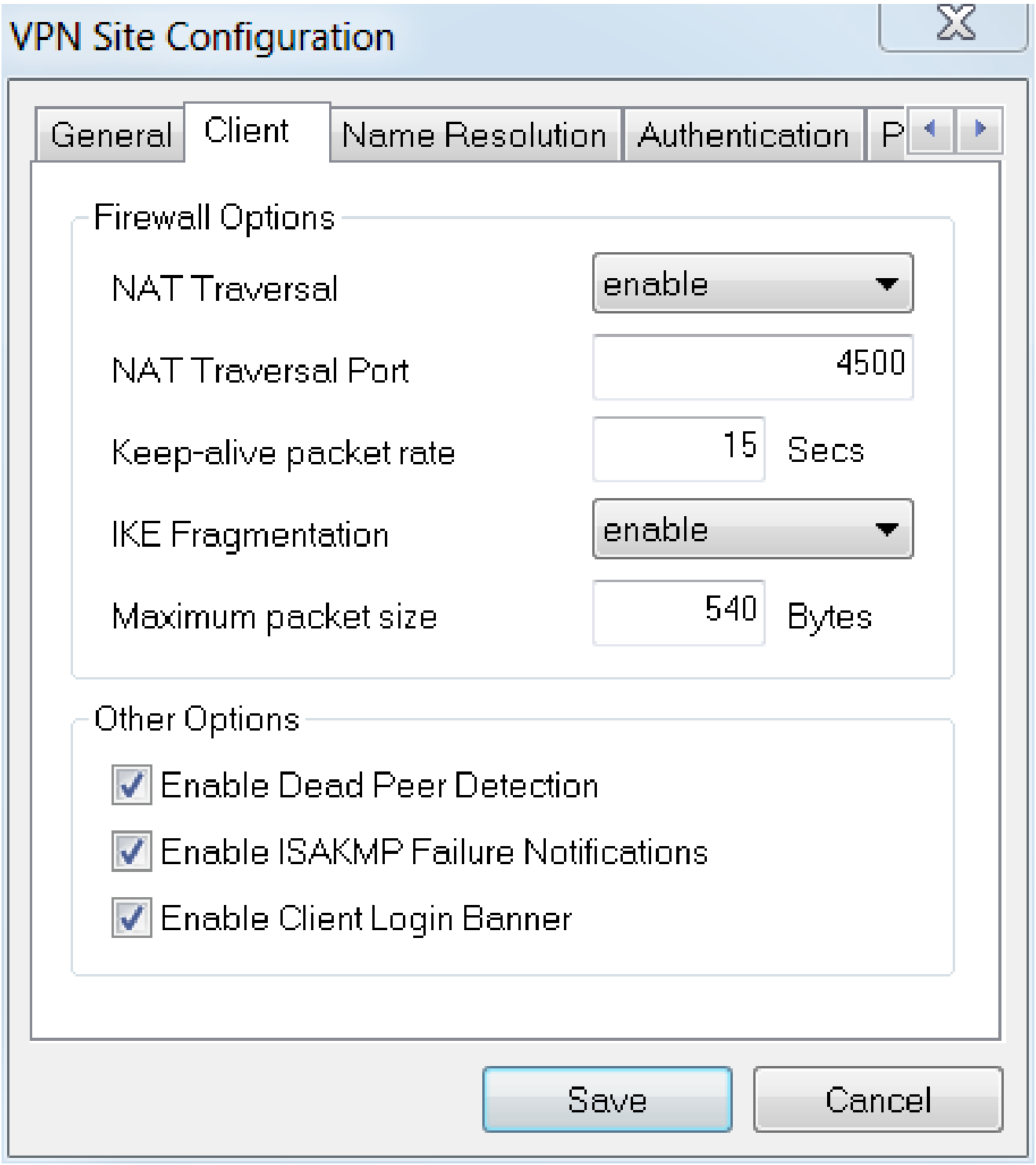
Abra el Administrador de acceso VPN de Shrew Soft y haga clic en Agregar para agregar un perfil. En la ventana VPN Site Configuration que aparece, configure la ficha General:

- 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 una dirección asignada



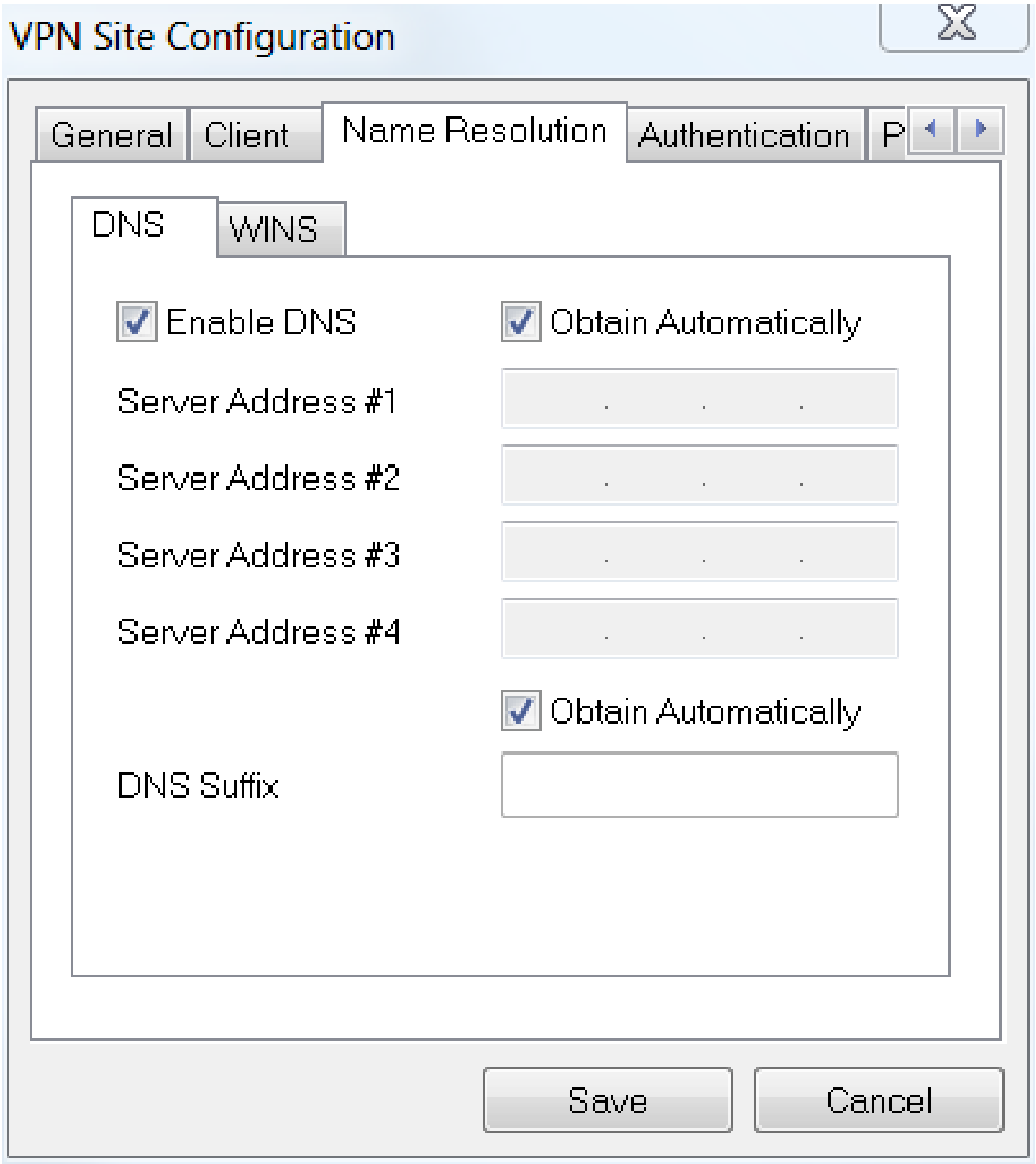
Paso 2

Configure la ficha Cliente. En este ejemplo, hemos mantenido la configuración predeterminada.



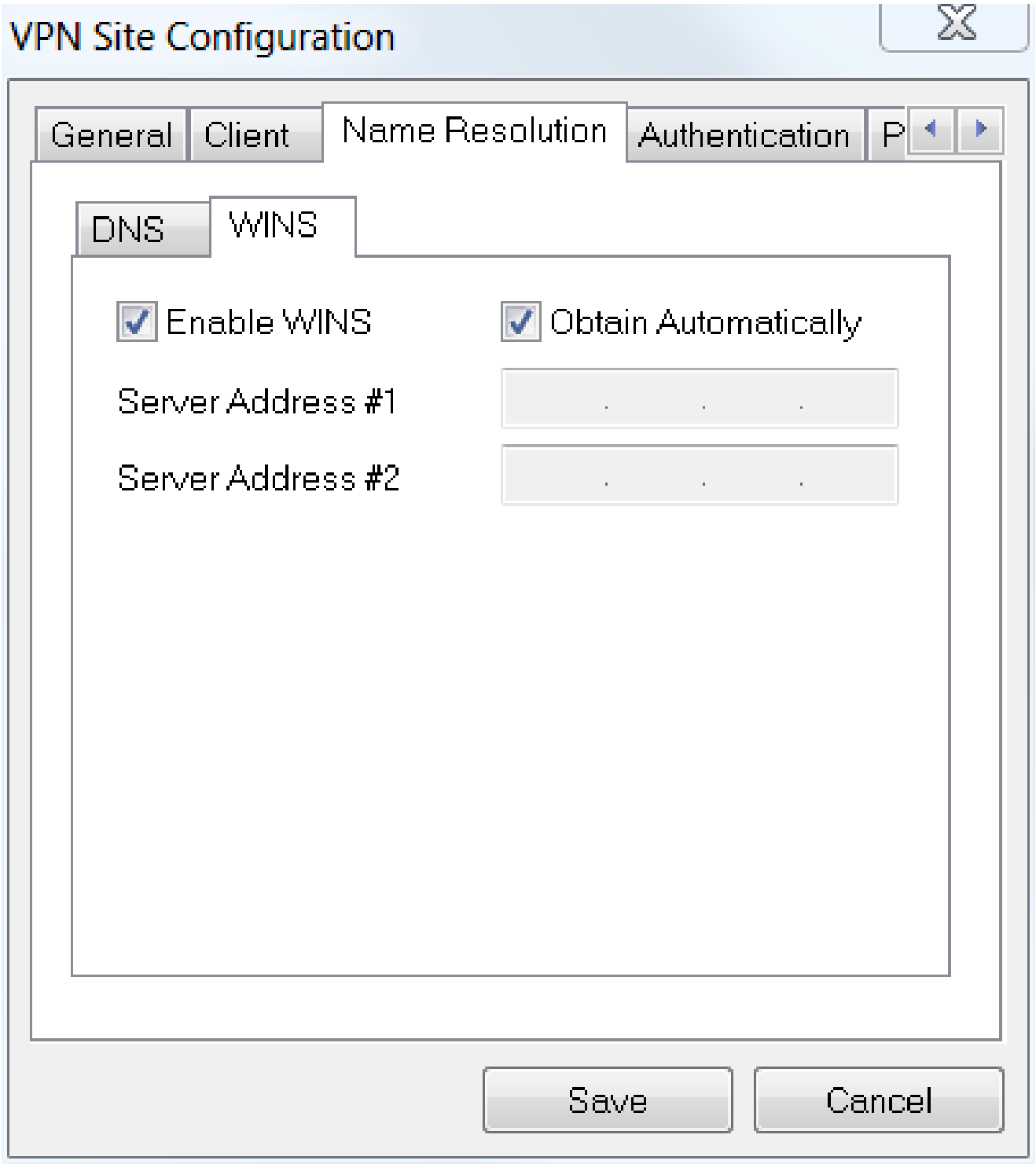
Paso 3

En Resolución de nombres > DNS, marque la casilla Enable DNS y deje las casillas Obtain Automatically marcadas.



Paso 4

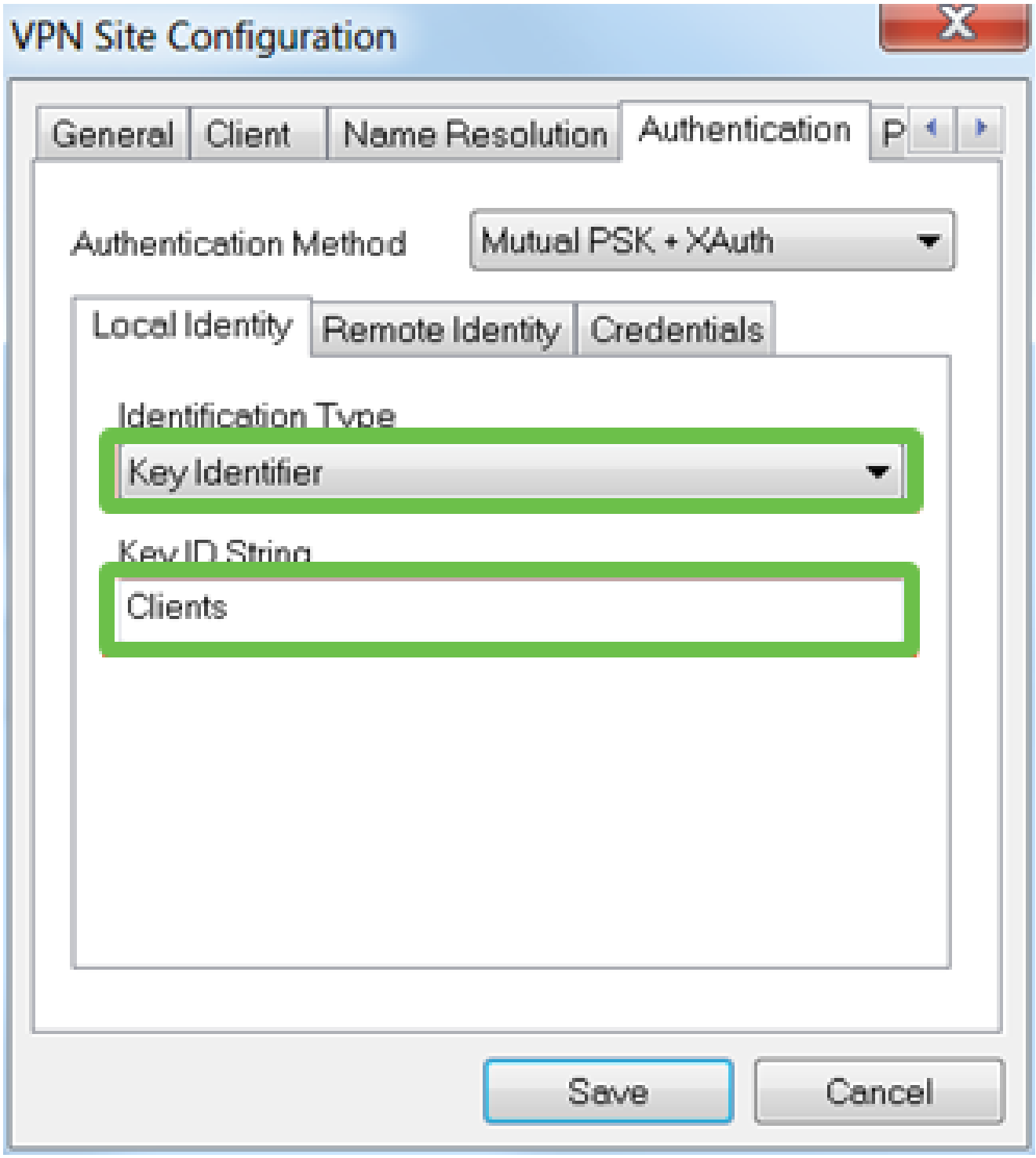
En la ficha Resolución de nombres > WINS, marque la casilla Habilitar WINS y deje marcada la casilla Obtener automáticamente.



Paso 5

Haga clic en Authentication > Local Identity.

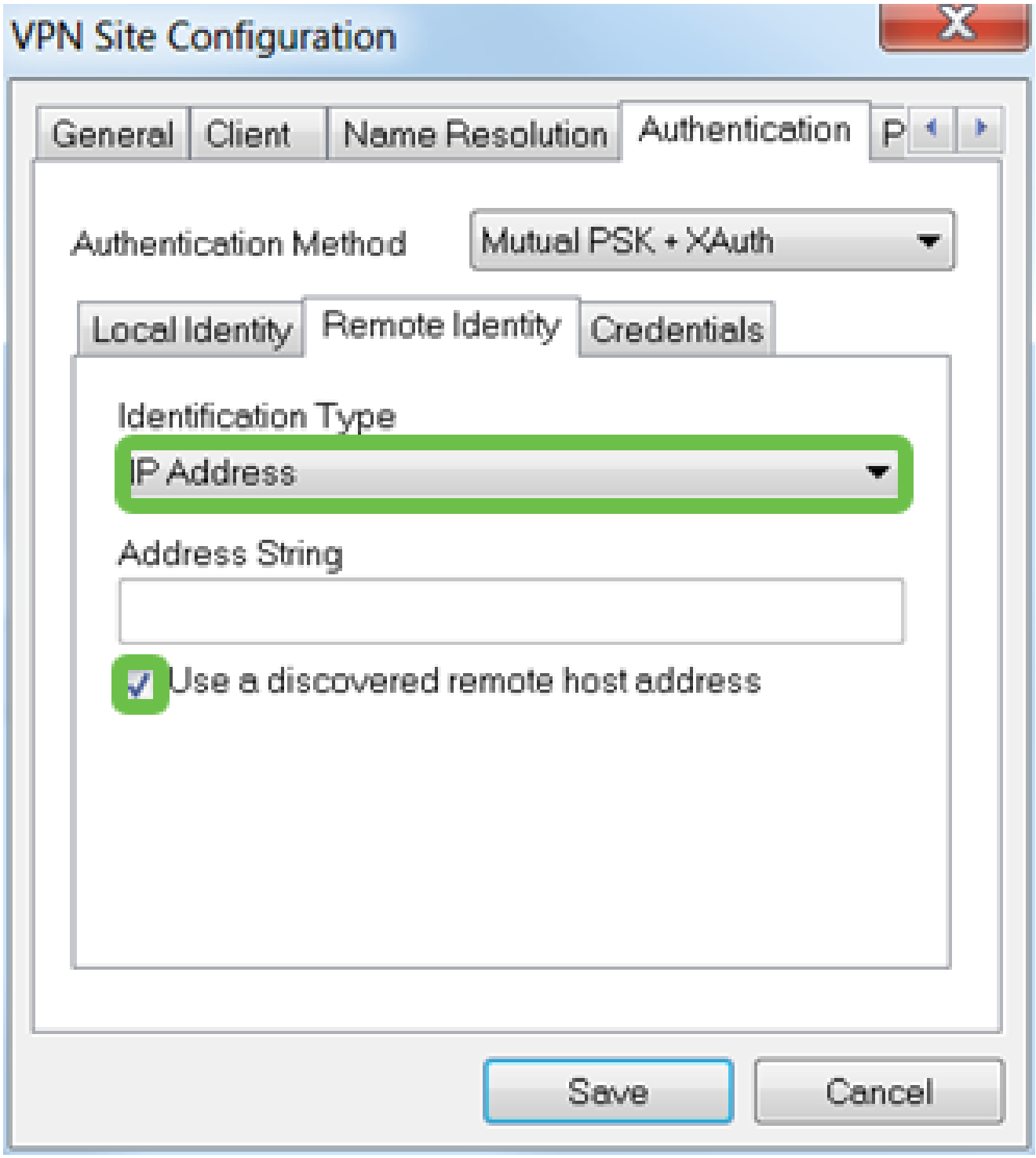
- Tipo de identificación: Seleccionar identificador de clave
- Cadena de ID de clave: introduzca el nombre de grupo configurado en el RV345P



Paso 6

En Autenticación > Identidad remota. En este ejemplo, hemos mantenido la configuración predeterminada.

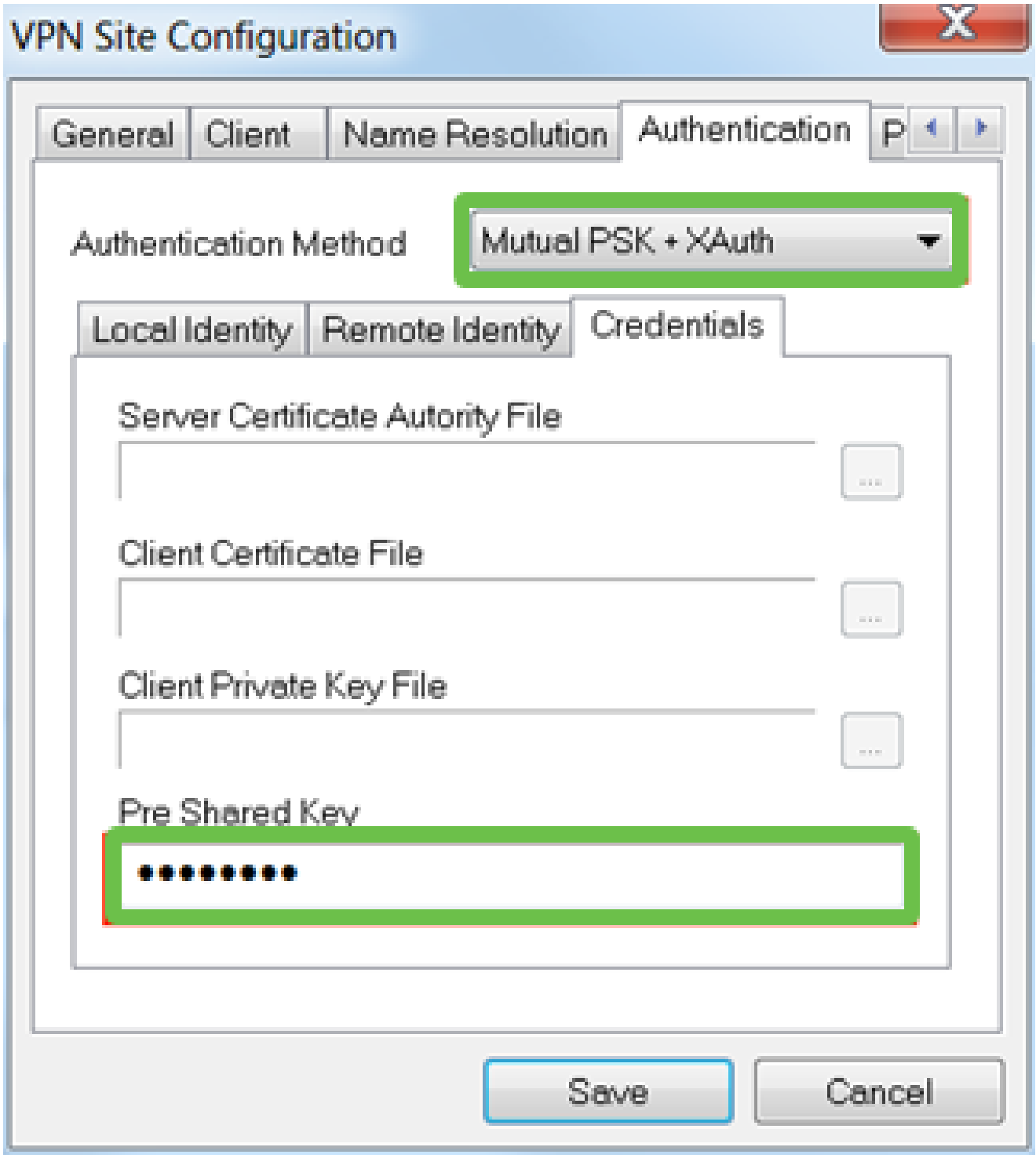
- Tipo de identificación: Dirección IP
- Cadena de dirección: <en blanco>
- Usar una casilla de dirección de host remoto detectada: activada



Paso 7

En Authentication > Credentials, configure lo siguiente:

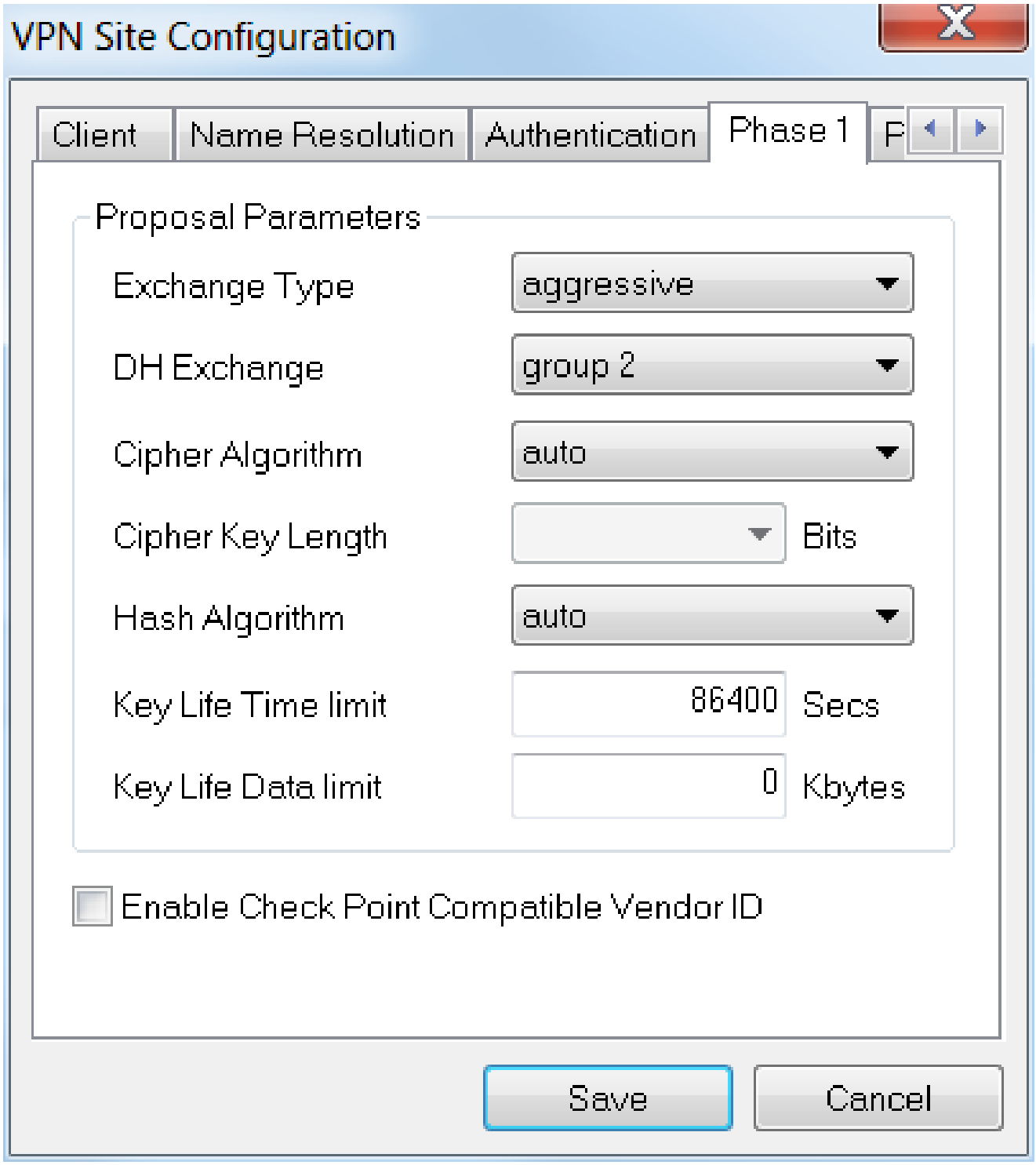
- Método de autenticación: seleccione Mutual PSK + XAuth
- Pre-Shared Key (Clave precompartida): Introduzca la clave precompartida configurada en el perfil de cliente RV345P



Paso 8

Para la pestaña Phase 1. En este ejemplo, se conservó la configuración predeterminada:

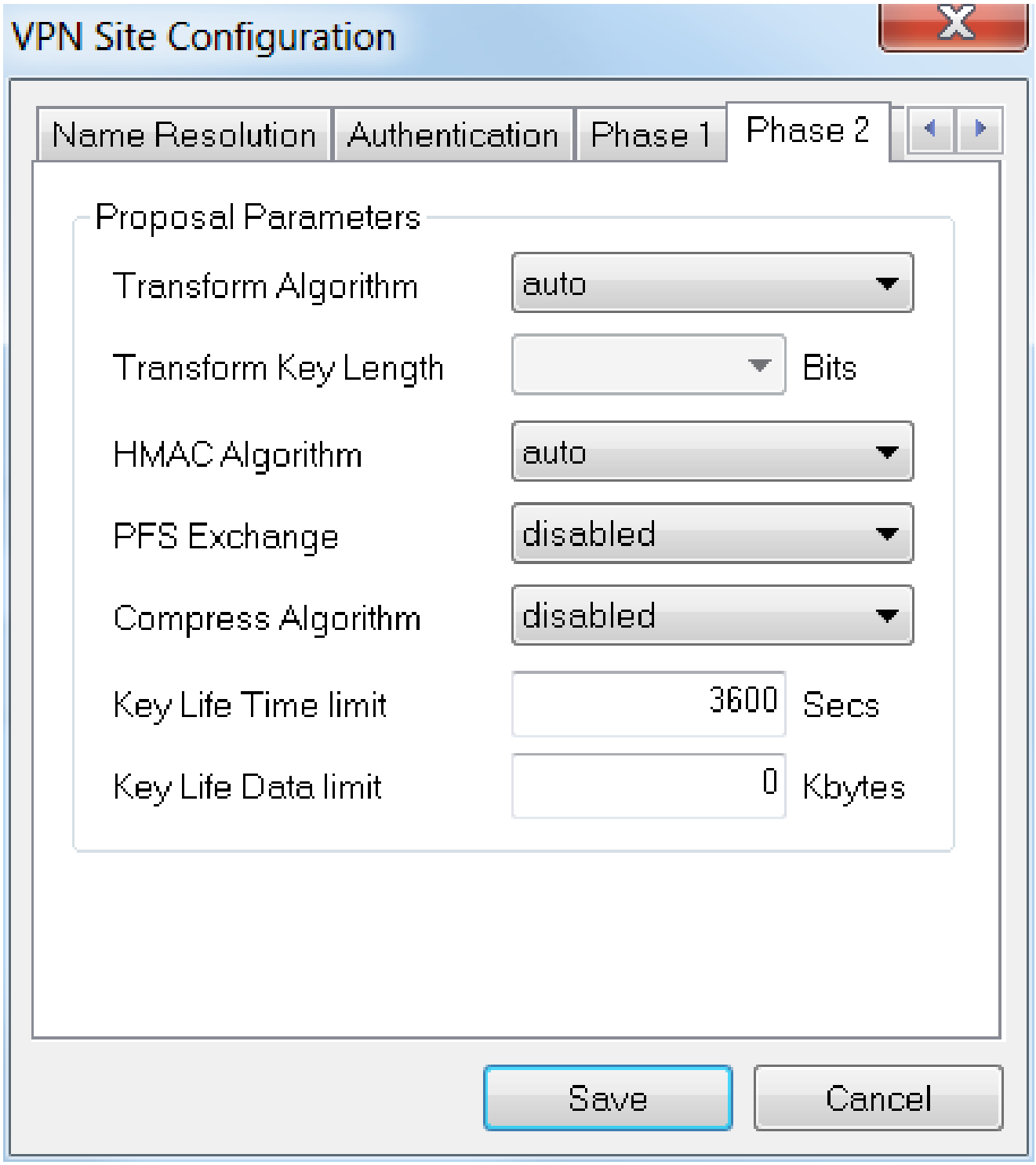
- Tipo de intercambio: agresivo
- Intercambio DH: grupo 2
- Algoritmo de cifrado: Automático
- Algoritmo de hash: Automático



Paso 9

En este ejemplo, los valores predeterminados para la pestaña Phase 2 se mantuvieron igual.

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

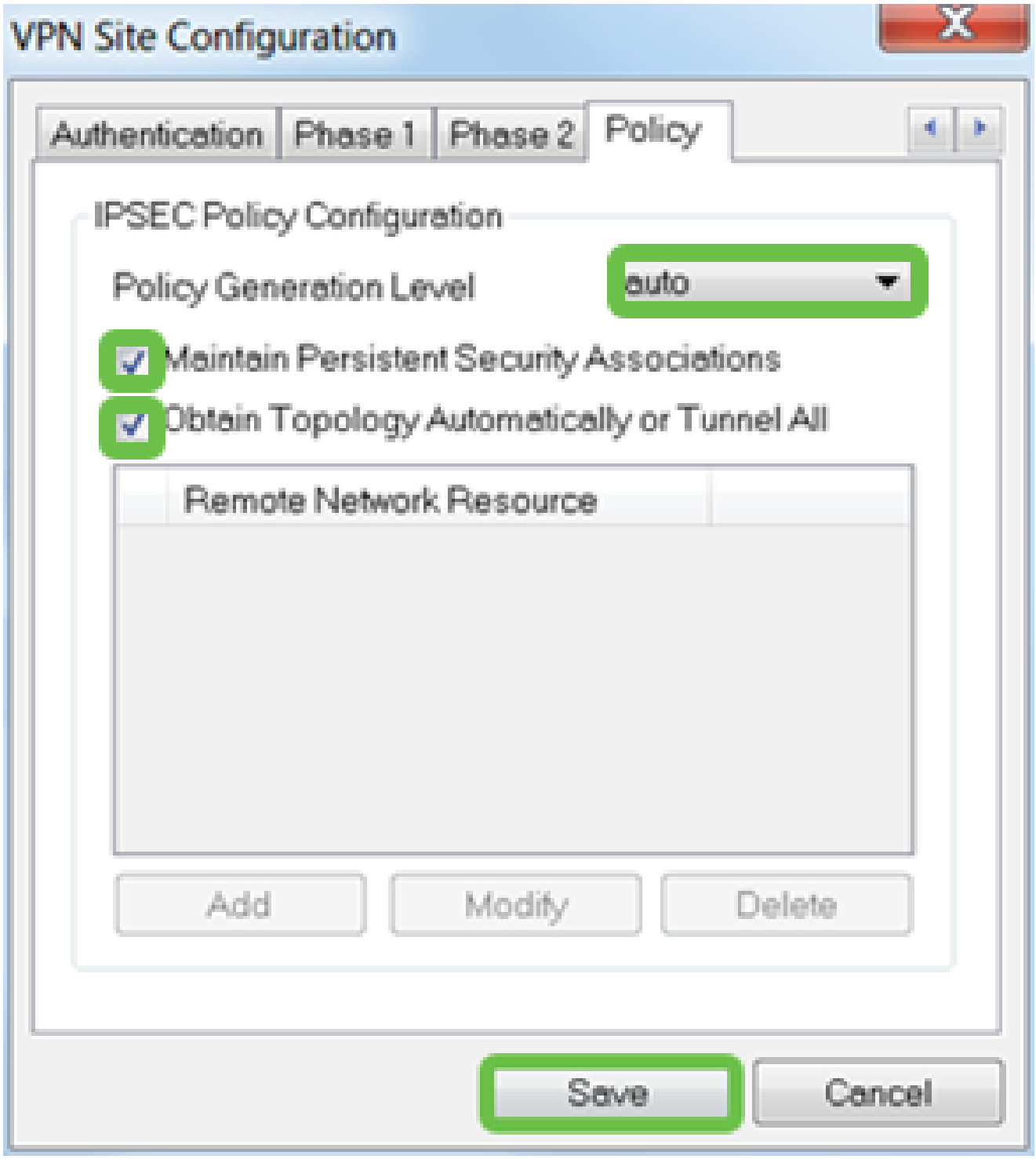


Paso 10

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 completo: activado

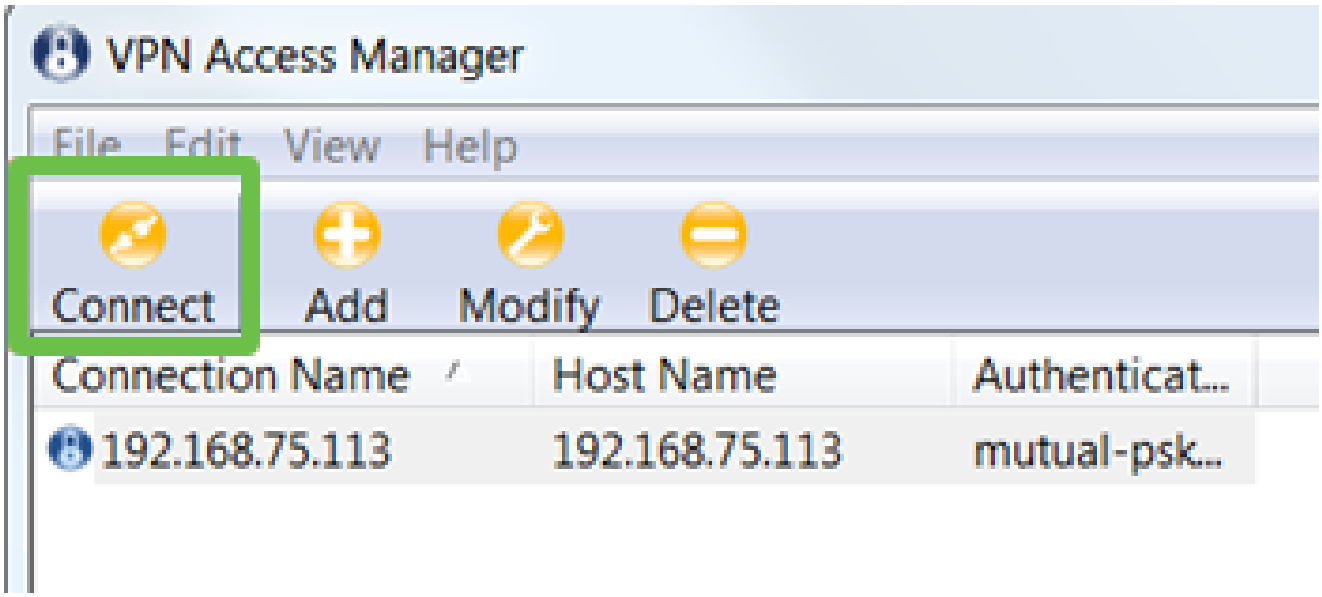
Como configuramos la tunelización dividida en el RV345P, no es necesario configurarla aquí.



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.

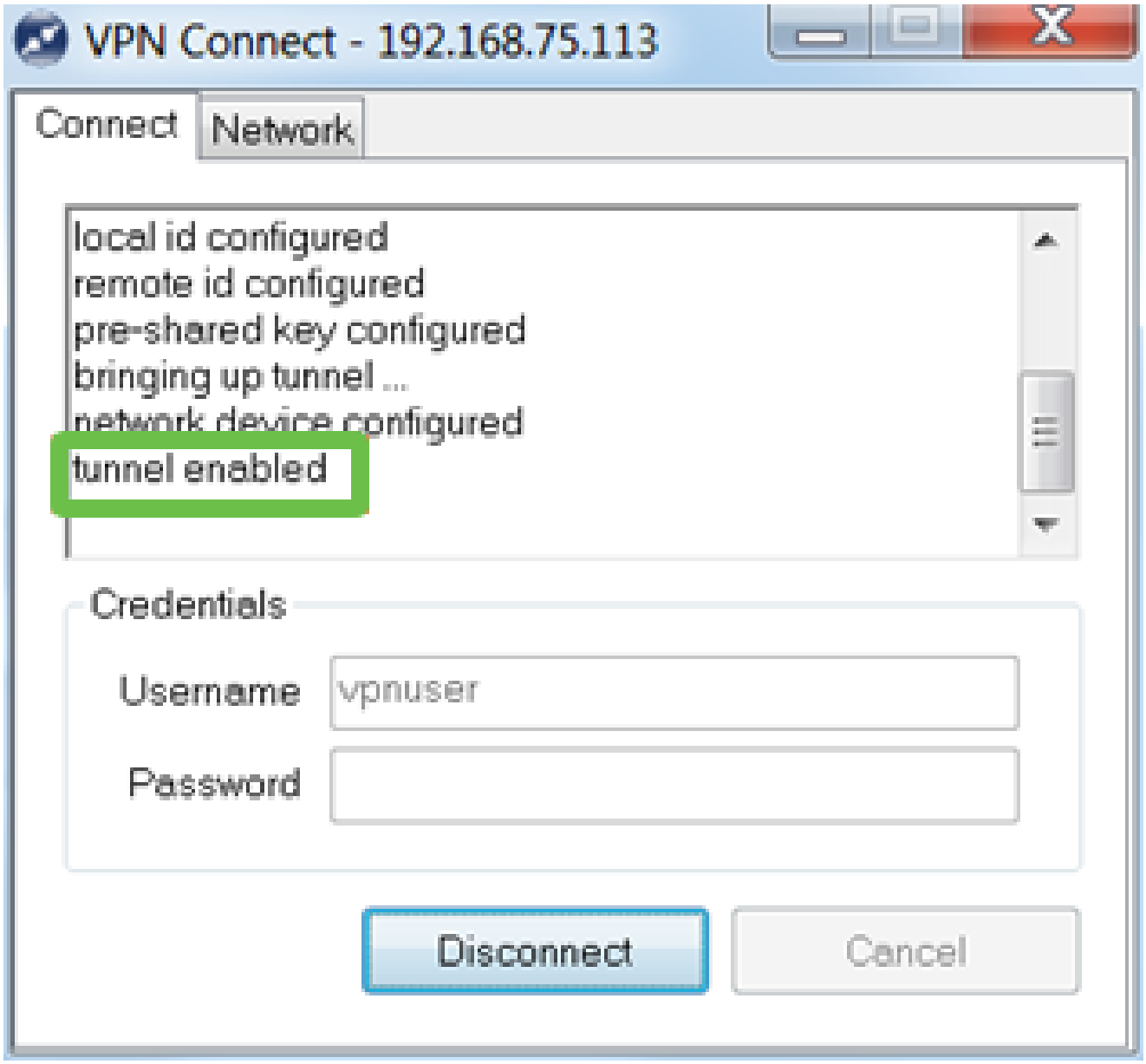


Paso 12

En la ventana VPN Connect que aparece, introduzca el nombre de usuario y la contraseña con las credenciales de la cuenta de usuario que ha creado en el RV345P (pasos 13 y 14). Cuando haya terminado, haga clic en Connect.

Paso 13

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



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

Otras opciones de VPN

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

- Uso del cliente VPN GreenBow para conectar con el router serie RV34x
- Configuración de un cliente VPN de teletrabajador en el router serie RV34x
- Configuración de un servidor de protocolo de tunelación 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 WAN L2TP en el router RV34x
- Configuración de VPN de sitio a sitio en el RV34x

Configuraciones adicionales del router RV345P

Configuración de VLAN (opcional)

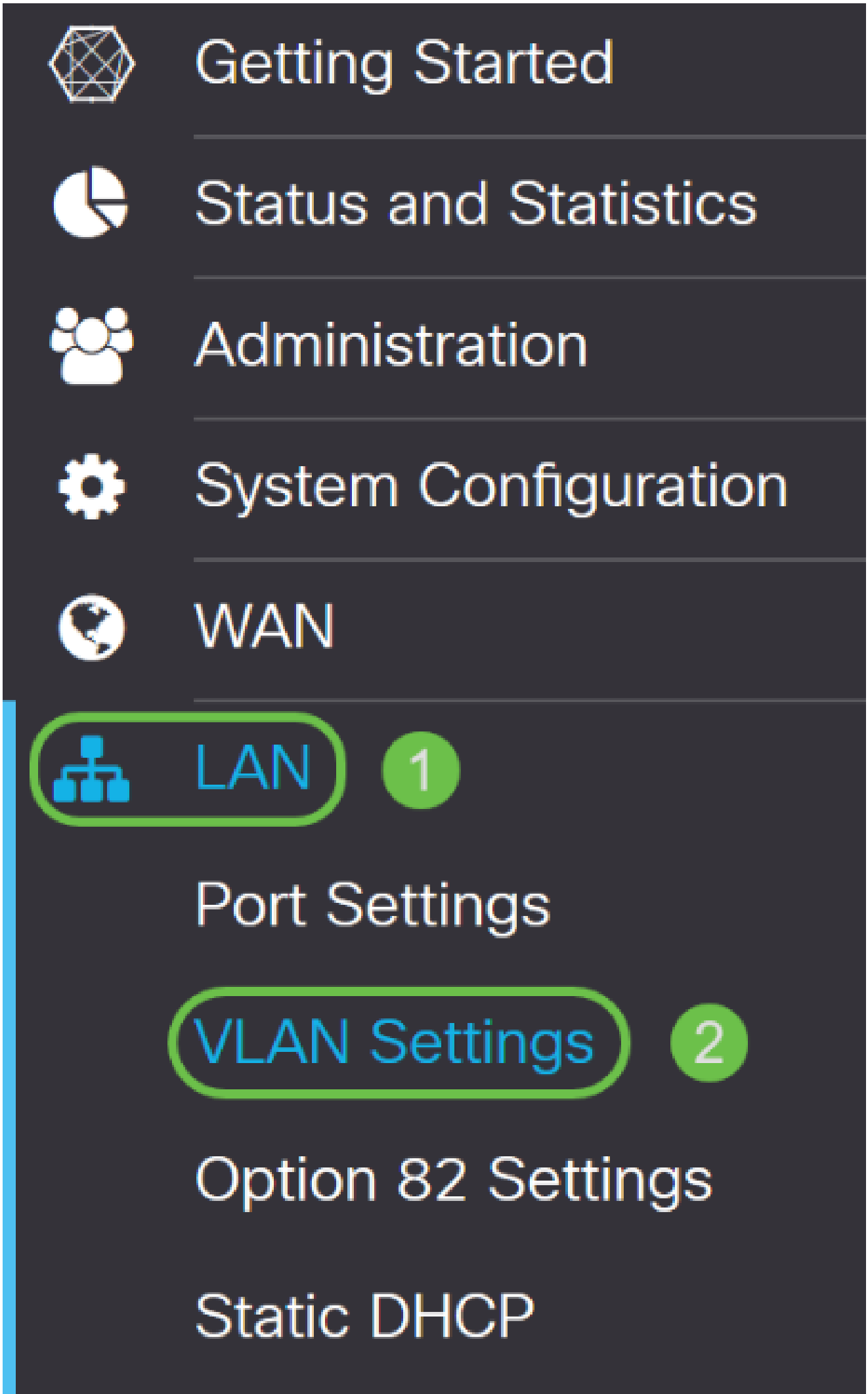
Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En situaciones en las que se pueden transmitir datos confidenciales en una red, se puede crear una VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Las VLAN también pueden utilizarse para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusiones a destinos innecesarios. Puede crear una VLAN, pero esto no tiene ningún 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.

Es posible que desee consultar Prácticas recomendadas de VLAN y Consejos de seguridad para obtener orientación adicional.

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

Paso 1

Vaya a LAN > VLAN Settings.

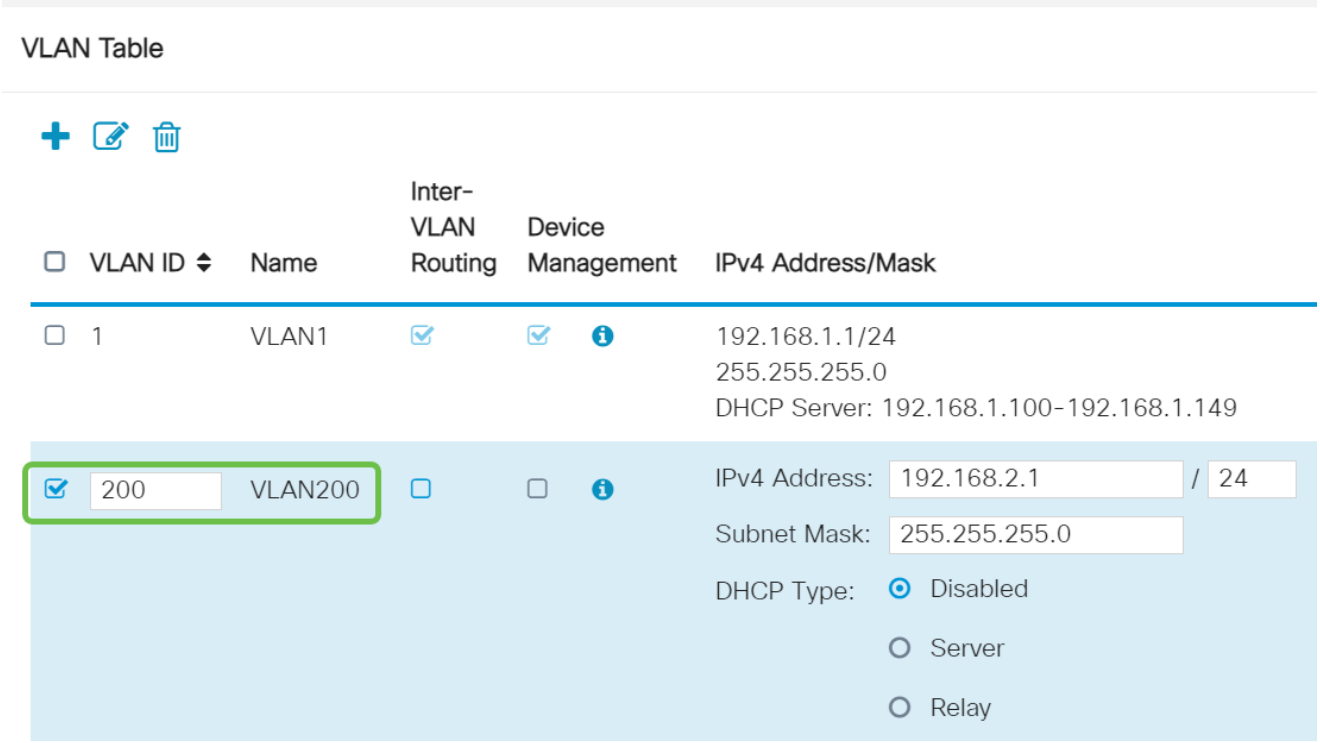

Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
1
Port Settings
VLAN Settings
2
Option 82 Settings
Static DHCP

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 está entre 1 y 4093.



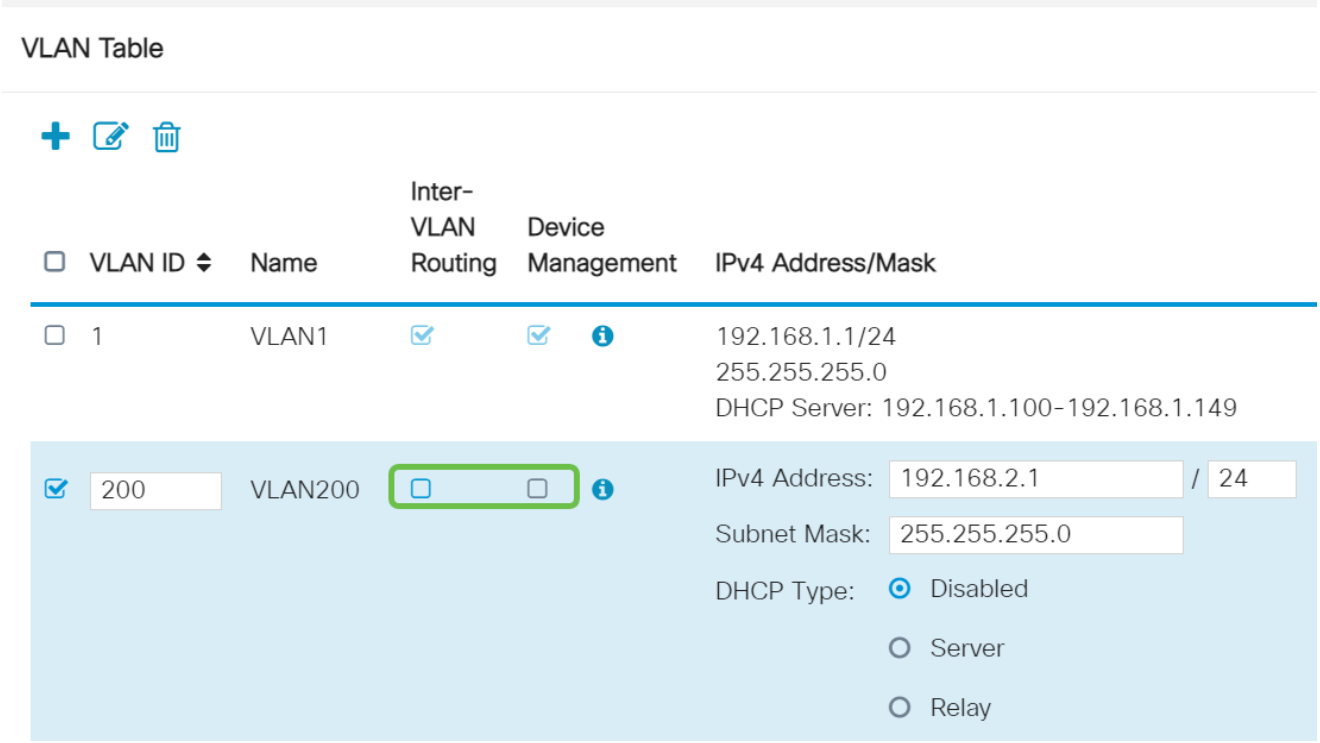
Paso 4

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 deseará aislar a los usuarios invitados, ya que deja las VLAN menos seguras. Hay momentos en los que puede ser necesario que las VLAN se enruten entre sí. Si este es el caso, verifique Inter-VLAN Routing en un Router RV34x con Restricciones de ACL de Destino para configurar el tráfico específico que permite entre las VLAN.

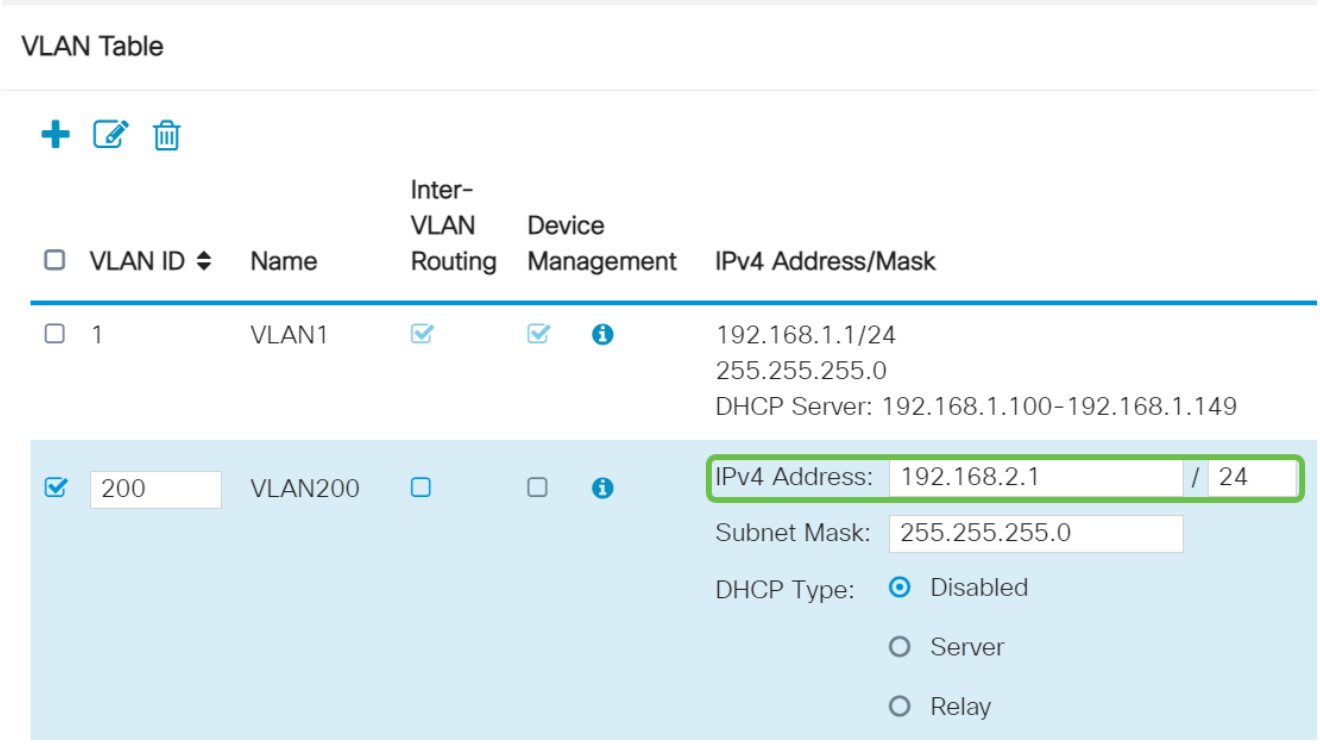
Device Management (Gestión de dispositivos) es el software que permite utilizar el explorador para iniciar sesión en la interfaz de usuario web del RV345P, desde la VLAN, y gestionar el RV345P. Esto también debe desactivarse en las redes de invitados.

En este ejemplo, no habilitamos el ruteo entre VLAN ni la administración de dispositivos para mantener la VLAN más segura.



Paso 5

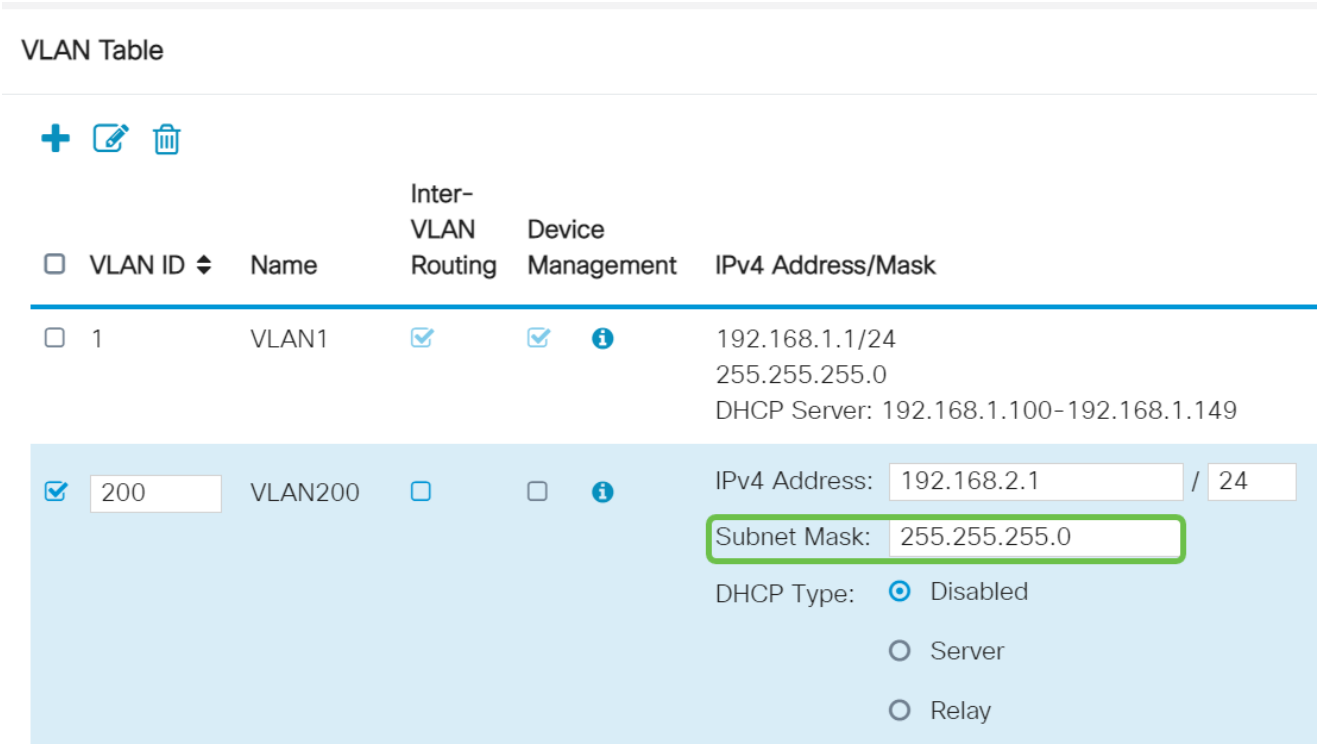
La dirección IPv4 privada se rellenará automáticamente en el campo IP Address. Puede ajustar esta opción si lo desea. En este ejemplo, la subred tiene direcciones IP 192.168.2.100-192.168.2.149 disponibles para DHCP. 192.168.2.1-192.168.2.99 y 192.168.2.150-192.168.2.254 están disponibles para direcciones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



Paso 6

La máscara de subred en 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

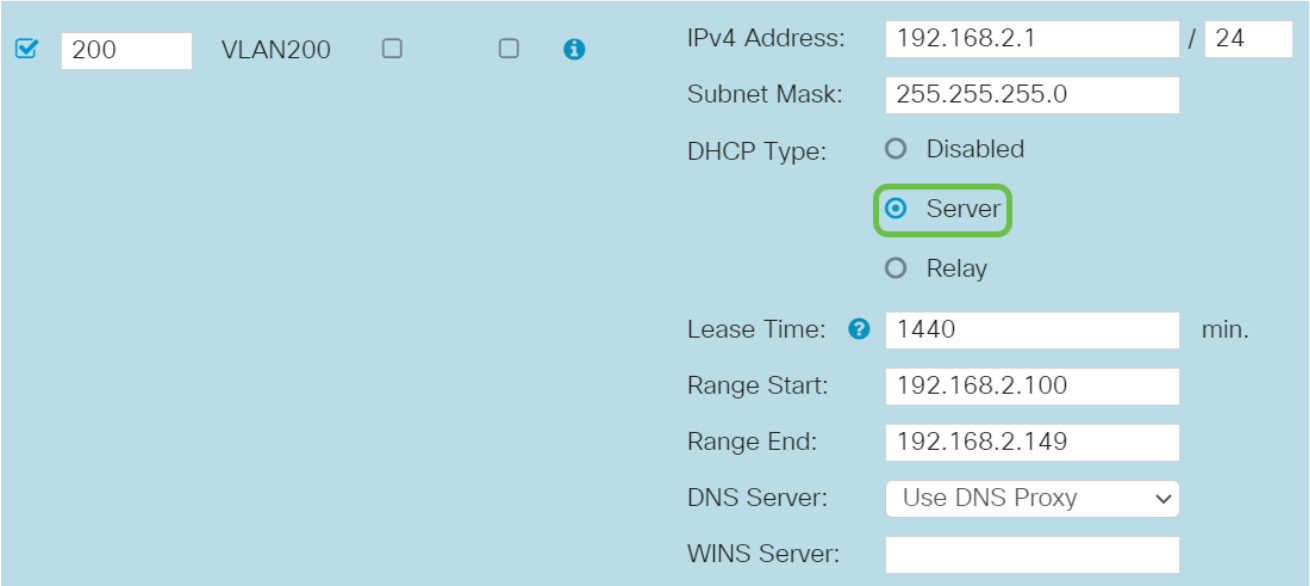
Seleccione un tipo de protocolo de configuración dinámica de host (DHCP). Las opciones siguientes son:

Disabled: desactiva el servidor DHCP IPv4 en la VLAN. Esto se recomienda en un entorno de prueba. En esta situación, todas las direcciones IP tendrían que configurarse manualmente y todas las comunicaciones serían internas.

Server (Servidor): Es la opción que se utiliza con más frecuencia.

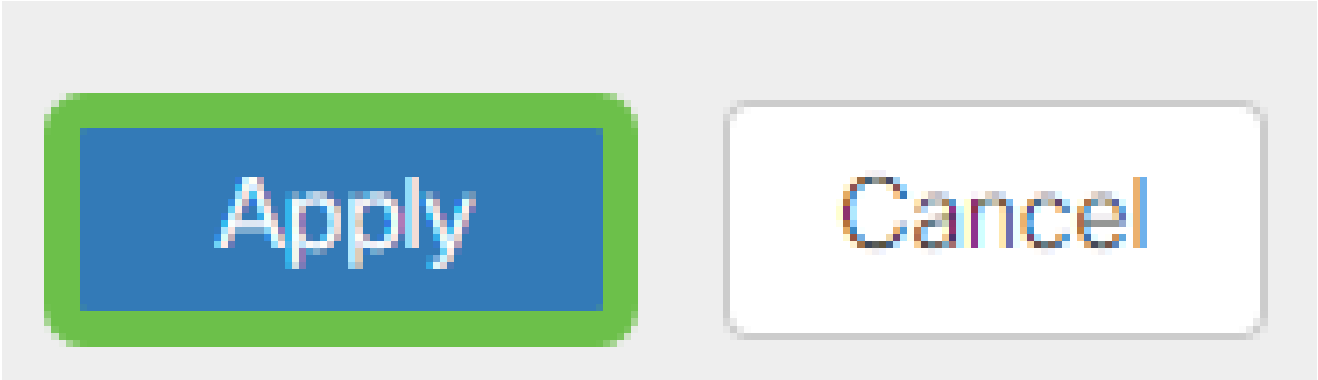
- Lease Time (Tiempo de concesión): Introduzca un valor de tiempo de 5 a 43.200 minutos. El valor predeterminado es 1440 minutos (es decir, 24 horas).
- Range Start and Range End (Inicio y fin del intervalo): Introduzca el inicio y el final del intervalo de las direcciones IP que se pueden asignar dinámicamente.
- DNS Server (Servidor DNS): Seleccione esta opción para utilizar el servidor DNS como proxy o ISP en la lista desplegable.
- WINS Server (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 de archivo de la configuración.
- Relay (Retransmisión): Introduzca la dirección IPv4 del servidor DHCP remoto para configurar el agente de retransmisión DHCP. Se trata de una configuración más

avanzada.



Paso 8

Haga clic en Apply para crear la nueva VLAN.



Asignar 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 que el usuario asignó específicamente. Se considera una práctica óptima.

Los puertos se pueden configurar para ser un puerto de acceso o un puerto troncal:

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

Una VLAN asignó su propio puerto:

- Se considera un puerto de acceso.

- La VLAN que se asigna a este puerto debe etiquetarse como Sin etiqueta.
- Todas las demás VLAN deben etiquetarse como Excluidas para ese puerto.

Dos o más VLAN que comparten un puerto:

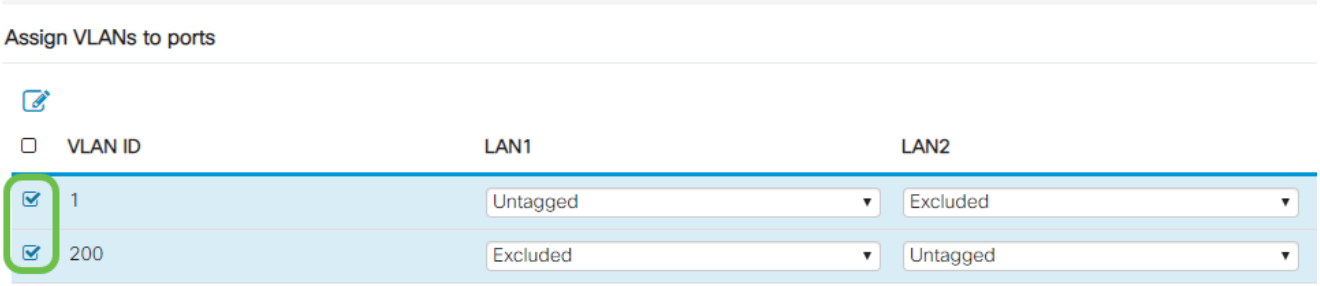
- Se considera un puerto troncal.
- Una de las VLAN se puede etiquetar como Sin etiqueta.
- El resto de las VLAN que forman parte del puerto troncal deben etiquetarse como Tagged (Etiquetado).
- Las VLAN que no forman parte del puerto troncal deben etiquetarse como Excluidas para ese puerto.

En este ejemplo, no hay trunks.

Paso 1

Seleccione los ID de VLAN que desea editar.

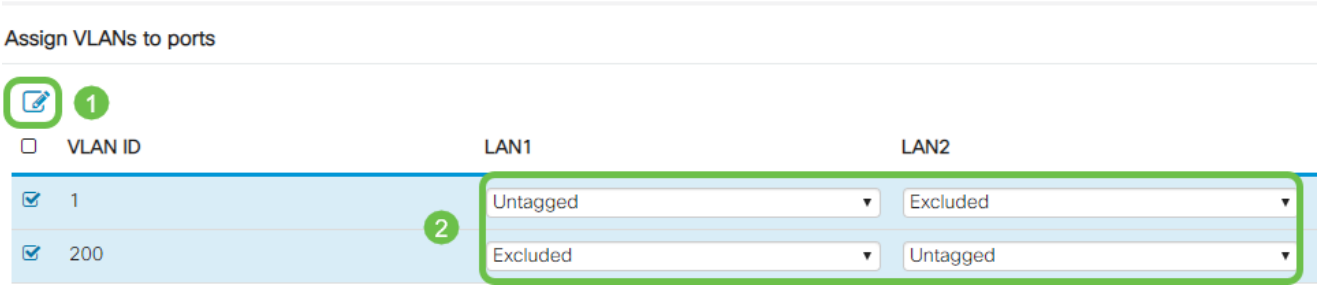
En este ejemplo, hemos seleccionado VLAN 1 y VLAN 200.



Paso 2

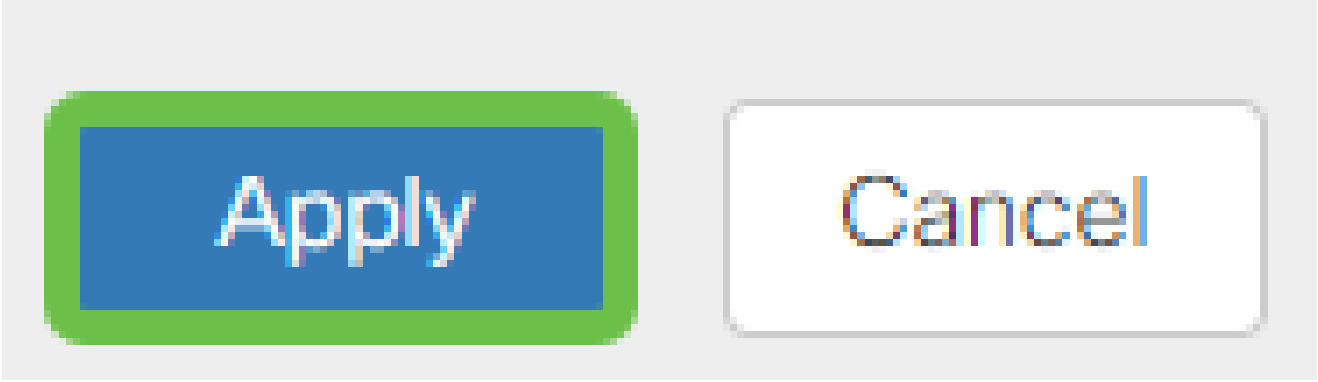
Haga clic en Edit para asignar una VLAN a un puerto LAN y especificar cada configuración como Tagged, Untagged o Excluded.

En este ejemplo, en LAN1 asignamos la VLAN 1 como Untagged y la VLAN 200 como Excluded. Para LAN2 asignamos VLAN 1 como Excluded y VLAN 200 como Untagged.



Paso 3

Haga clic en Apply para guardar la configuración.



Ahora debería haber creado correctamente una nueva VLAN y haber configurado las VLAN en los puertos del RV345P. Repita el proceso para crear las otras VLAN. Por ejemplo, VLAN300 se crearía para marketing con una subred de 192.168.3.x y VLAN400 se crearía para contabilidad con una subred de 192.168.4.x.

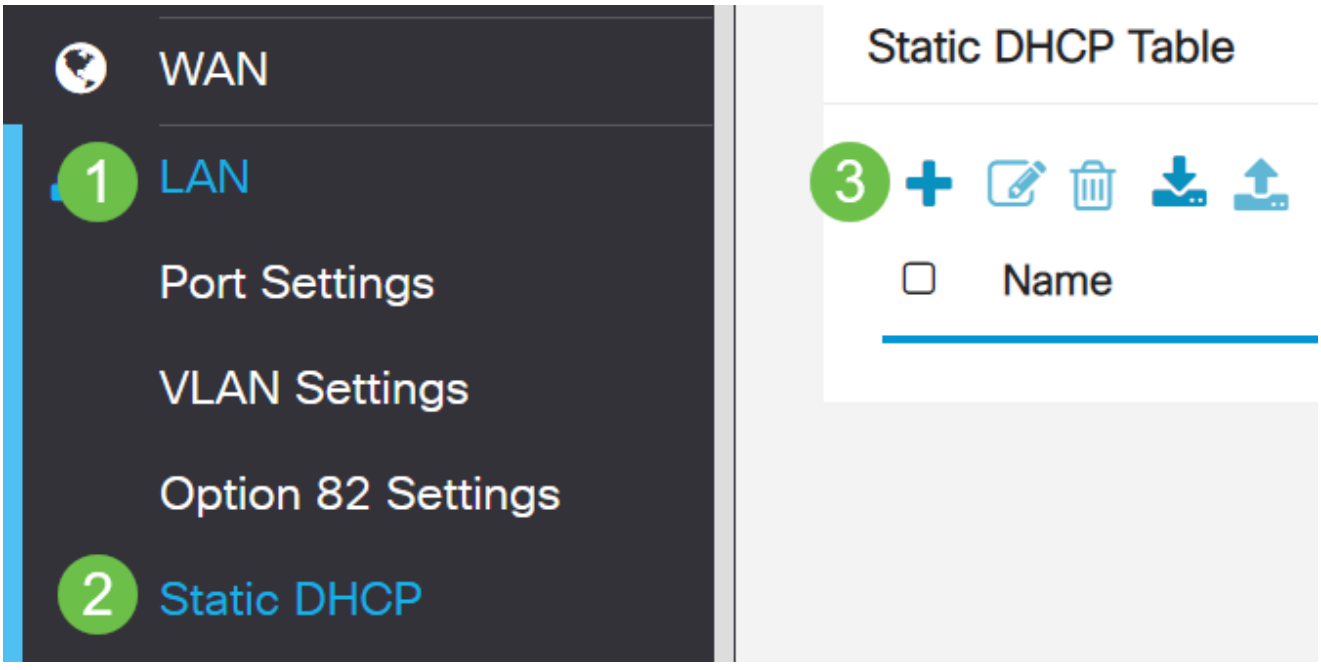
Agregar una IP estática (opcional)

Si desea que un determinado dispositivo sea accesible para otras VLAN, puede darle una dirección IP local estática y crear una regla de acceso para hacerlo accesible. Esto sólo funciona si el ruteo entre VLAN está habilitado. Hay otras situaciones en las que una IP estática puede ser útil. Para obtener más información sobre cómo establecer direcciones IP estáticas, consulte Prácticas recomendadas para establecer direcciones IP estáticas en el hardware empresarial de Cisco.

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

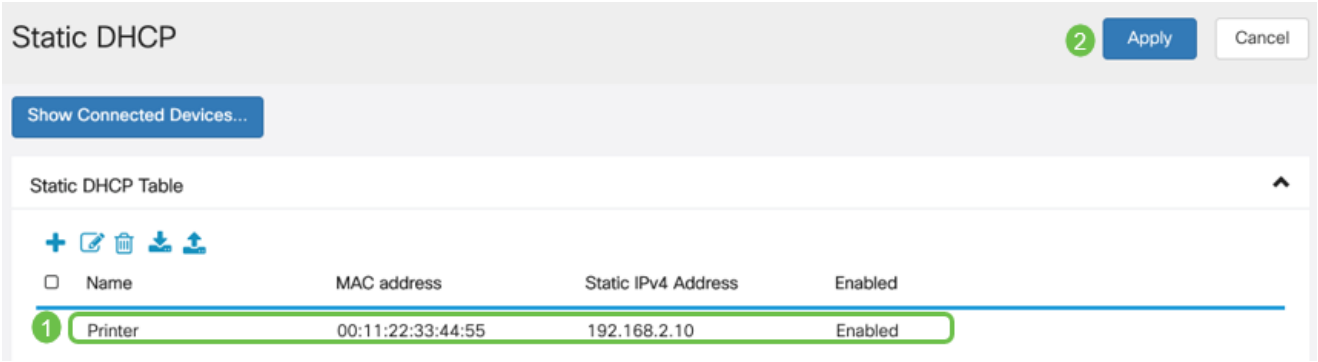
Paso 1

Vaya a LAN > Static DHCP . 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)

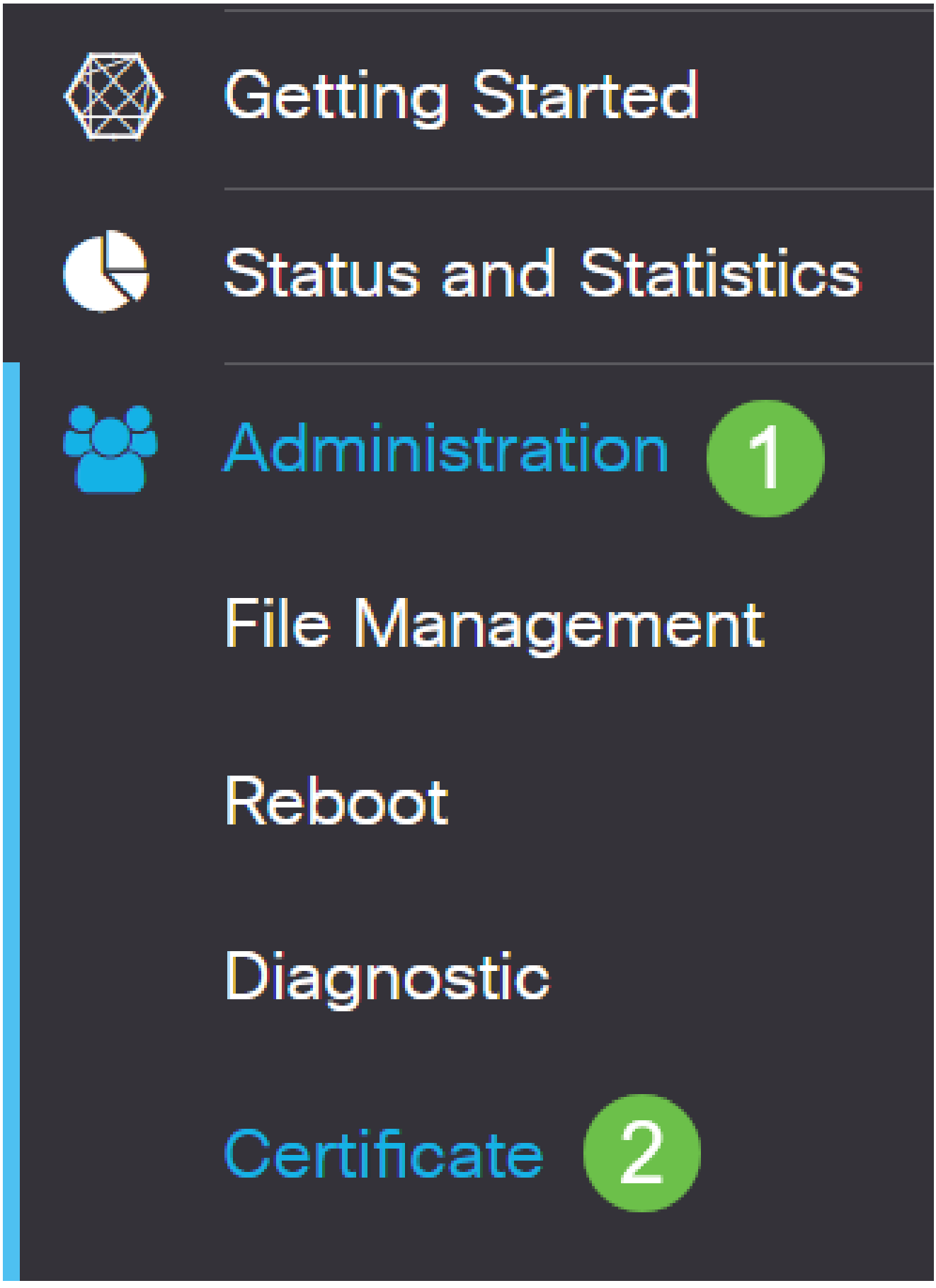
Un certificado digital certifica la propiedad de una clave pública por el sujeto designado del certificado. Esto permite a las partes que confían en la clave depender de firmas o afirmaciones realizadas por la clave privada que corresponde a la clave pública certificada. Un router puede generar un certificado 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 tener certificados legítimos de aplicaciones de terceros.

Para la autenticación se utiliza una autoridad de certificación (CA). 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 que se puede confiar en usted. Dependiendo de sus necesidades, un certificado a un costo mínimo. La CA lo desprotege y, una vez que verifique su información, le emitirán el certificado. Este certificado se puede descargar como un archivo en el equipo. A continuación, puede acceder al router (o servidor VPN) y cargarlo allí.

Generar CSR/certificado

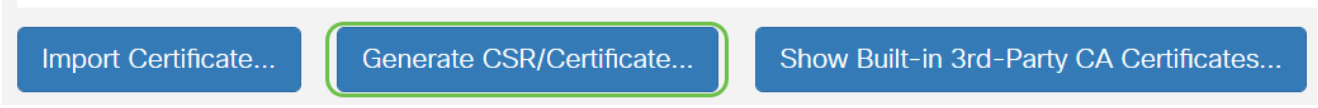
Paso 1

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.

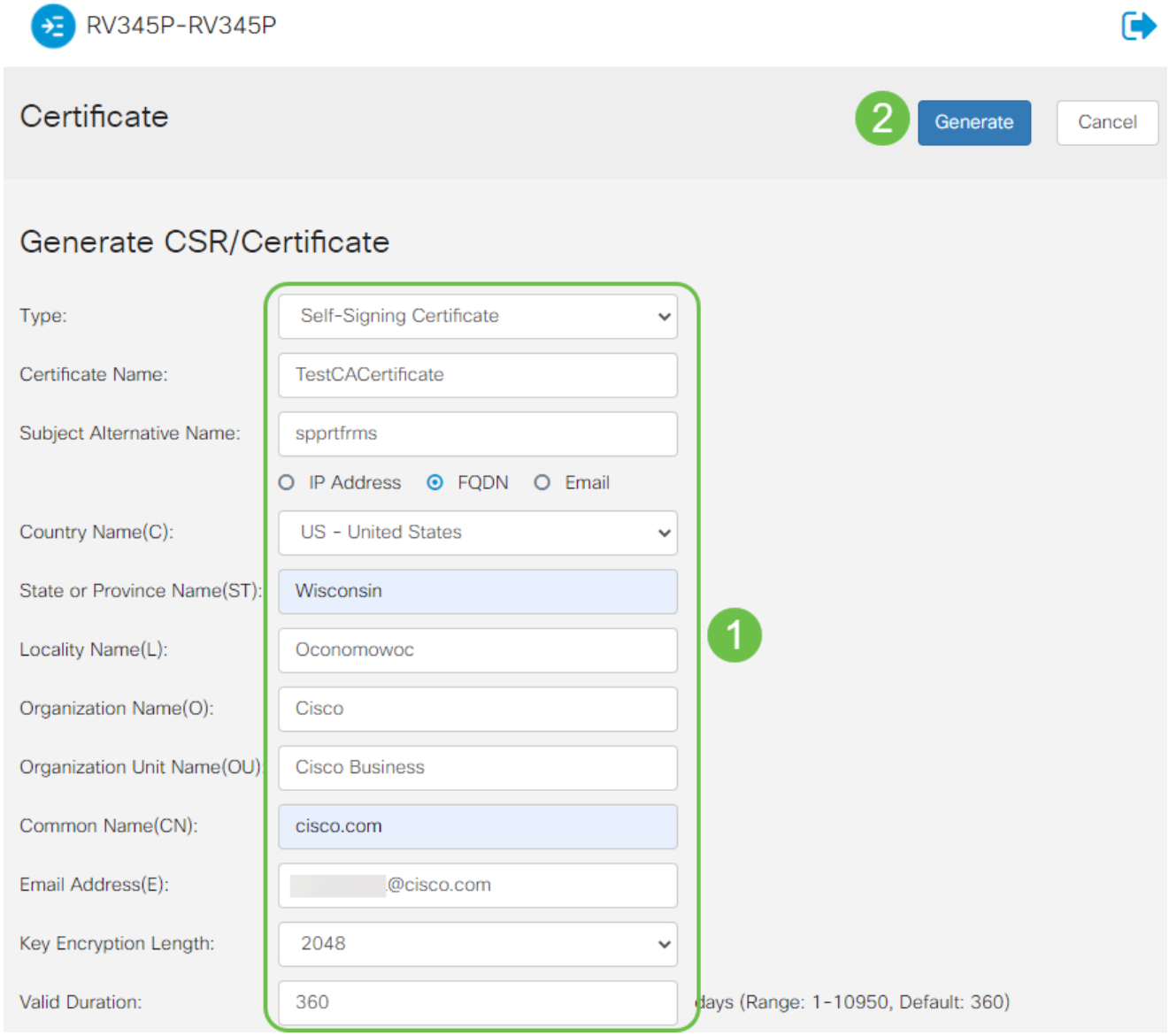


Paso 3

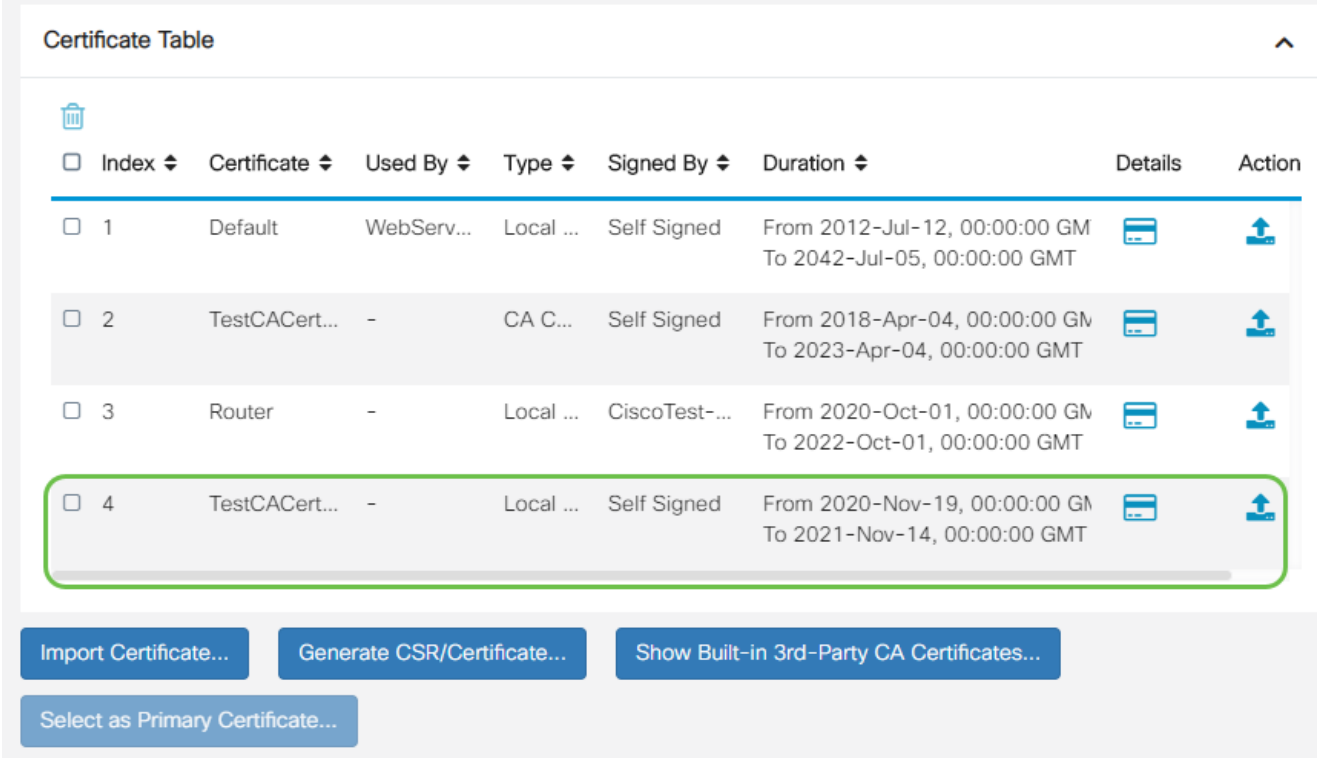
Rellene los recuadros con lo siguiente:

- Elija el tipo de certificado adecuado
  - Certificado de firma automática: se trata de un certificado de capa de socket seguro (SSL) firmado por su propio creador. Este certificado es menos fiable, 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 de certificación 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 del certificado para identificar la solicitud. Este campo no puede estar vacío 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 Nombre alternativo del sujeto, introduzca el FQDN.
- Elija un nombre de país en el que su organización esté registrada legalmente en la lista desplegable Nombre del país.
- Introduzca un nombre o abreviatura del estado, provincia, región o territorio en el que se encuentra la organización en el campo Estado o Nombre de provincia (ST).
- Introduzca un nombre para la localidad o ciudad en la que está registrada o ubicada la organización en el campo Nombre de la localidad.
- Introduzca un nombre con el que su empresa esté registrada legalmente. Si se está inscribiendo como pequeña empresa o propietario único, introduzca el nombre del solicitante del certificado en el campo Nombre de la organización. No se pueden utilizar caracteres especiales.
- Introduzca un nombre en el campo Nombre de Unidad de Organización para diferenciar entre las divisiones de una organización.
- Introduzca un nombre en el campo Common Name (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.
- Elija una longitud de clave en la lista desplegable Longitud de cifrado 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 durante los 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.

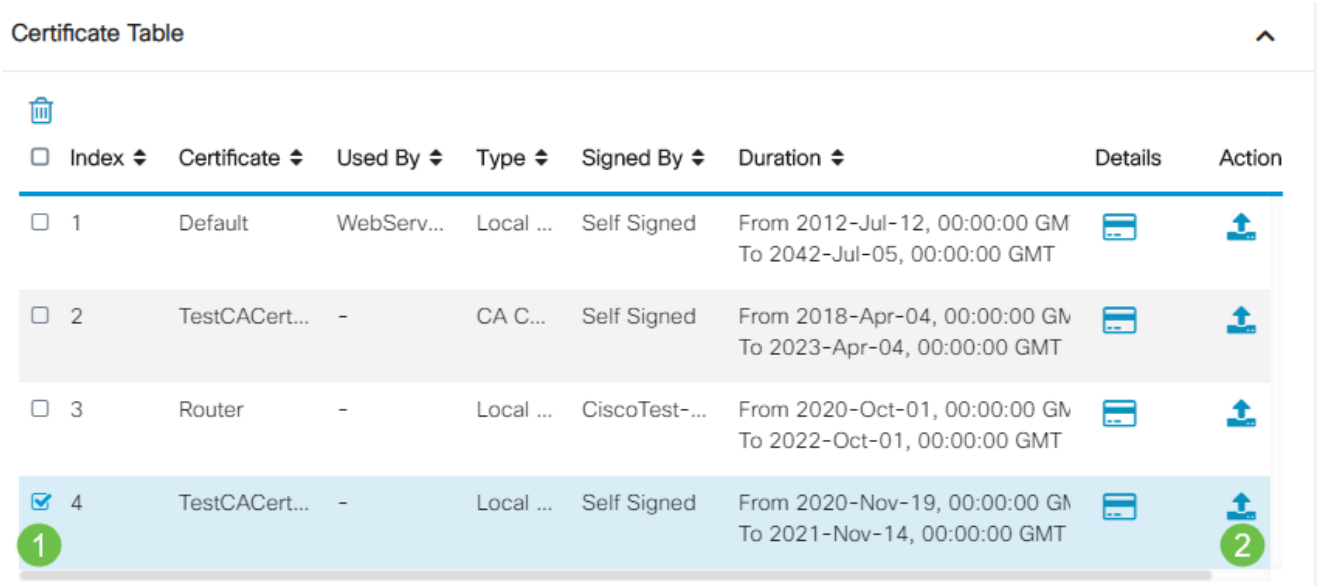


Ahora debería haber creado correctamente un certificado en el router RV345P.

Exportar un certificado

Paso 1

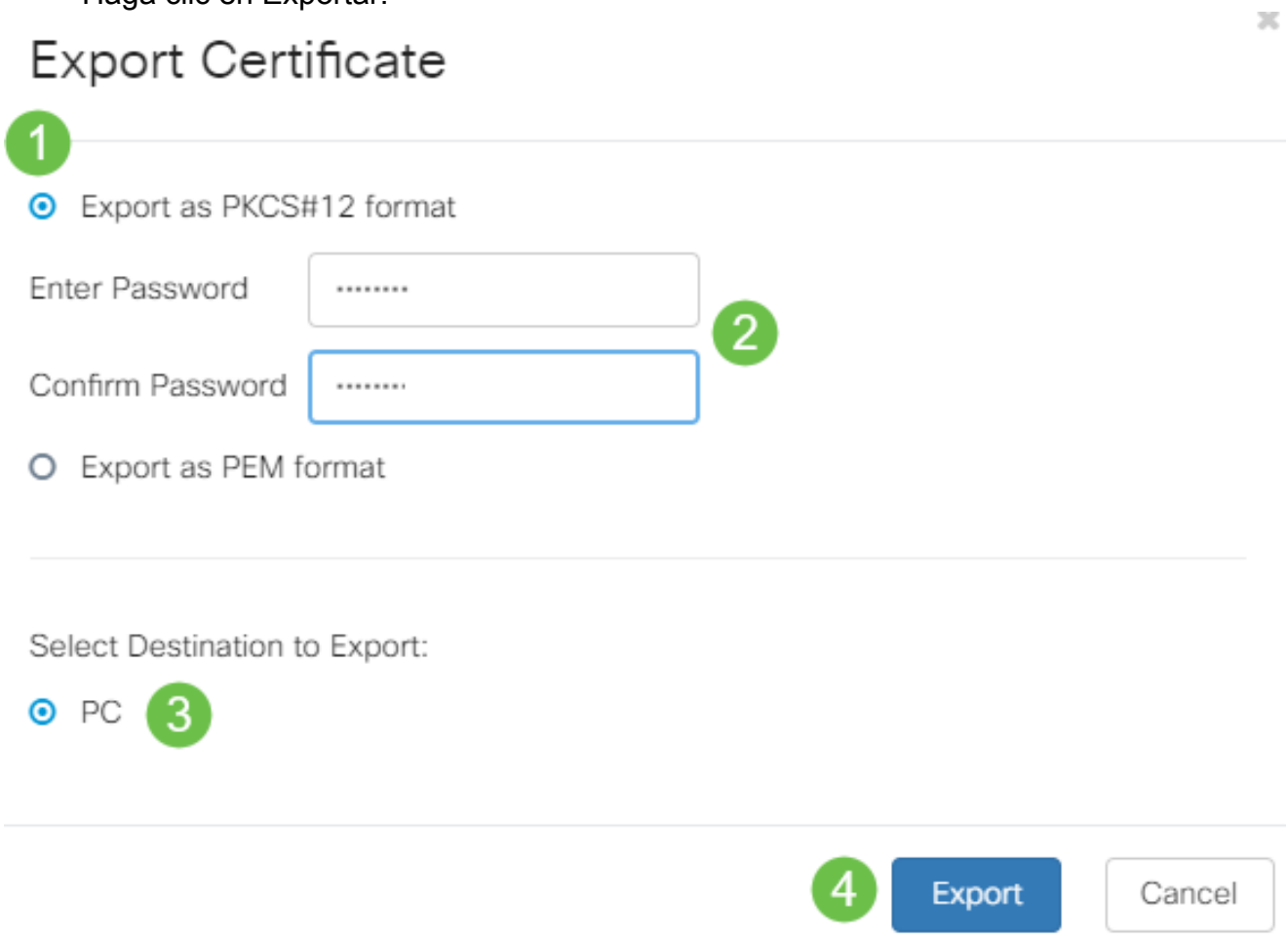
En la Tabla de certificados, marque la casilla del certificado que desea exportar y haga clic en el icono de exportación.



Paso 2

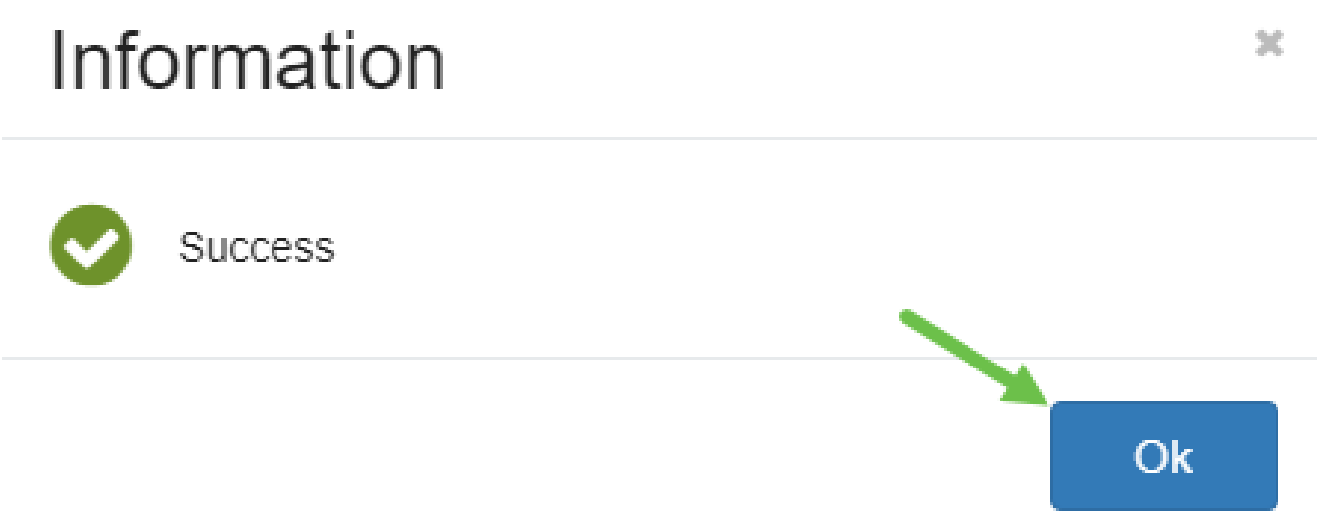
- Haga clic en un formato para exportar el certificado. Las opciones son:
  - PKCS #12: Public Key Cryptography Standards (PKCS) #12 es un certificado

exportado que viene en una extensión .p12. Se requerirá una contraseña para cifrar el archivo y protegerlo a medida que se exporta, importa y elimina.
    - PEM: Privacy Enhanced Mail (PEM) se utiliza a menudo para servidores web por su capacidad de traducirse fácilmente a datos legibles mediante el uso de un sencillo editor de texto 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 elegido PC, que es la única opción disponible actualmente.
- Haga clic en Exportar.



Paso 3

Debajo del botón Download (Descargar) aparecerá un mensaje que indica que la descarga se ha realizado correctamente. Se empezará a descargar un archivo en el explorador. Click OK.

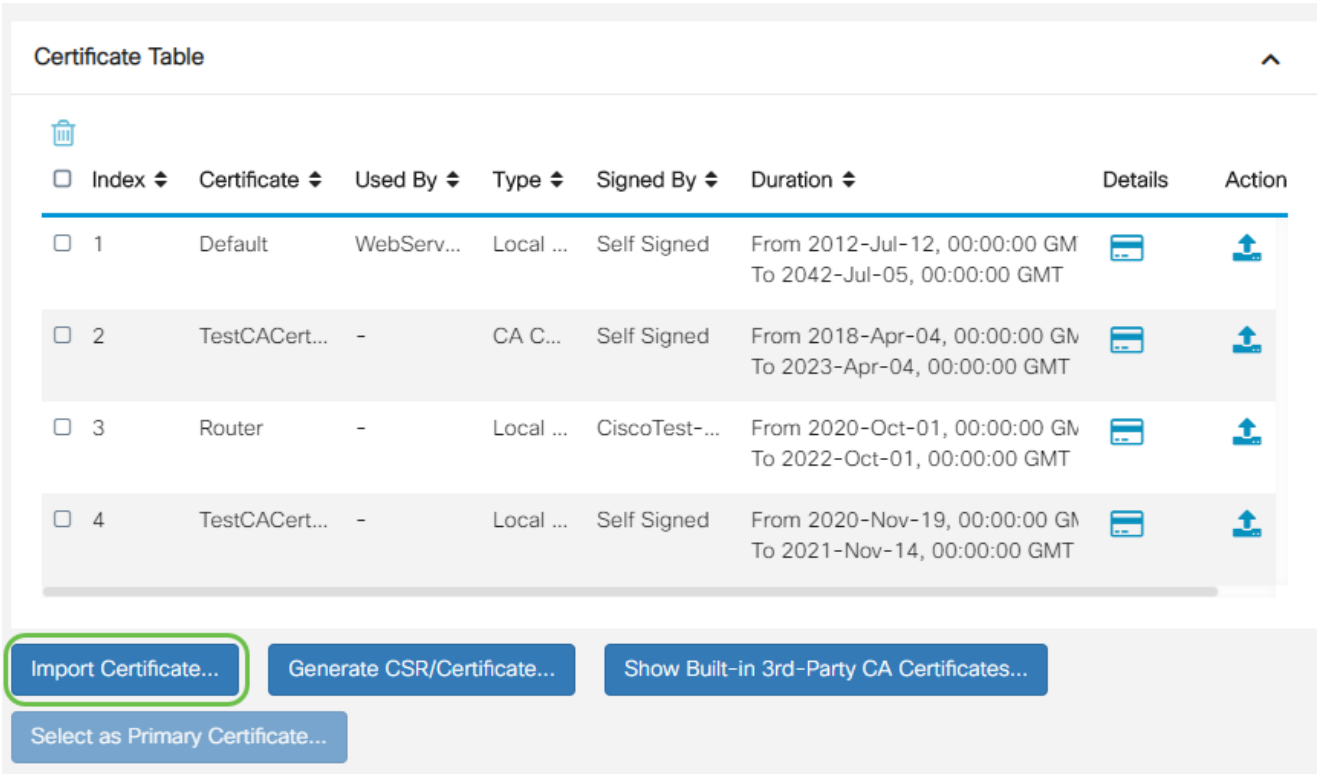


Ahora debería haber exportado correctamente un certificado en el router serie RV345P.

Importar un certificado

Paso 1

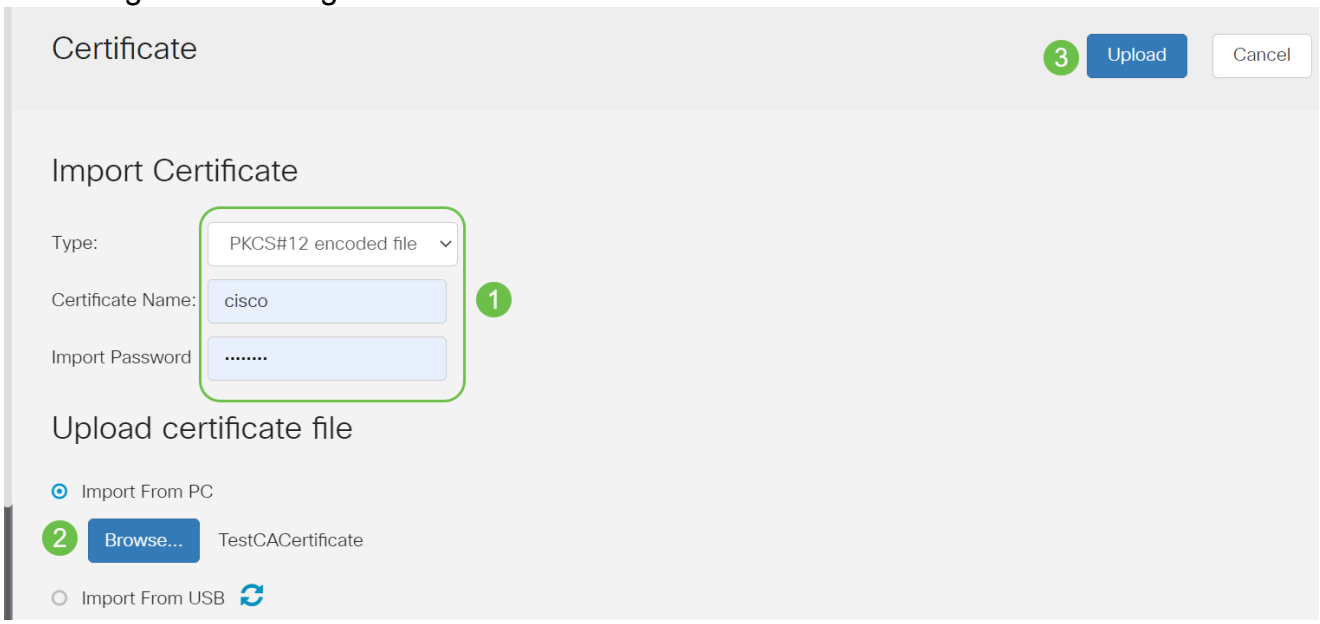
Haga clic en Importar certificado...



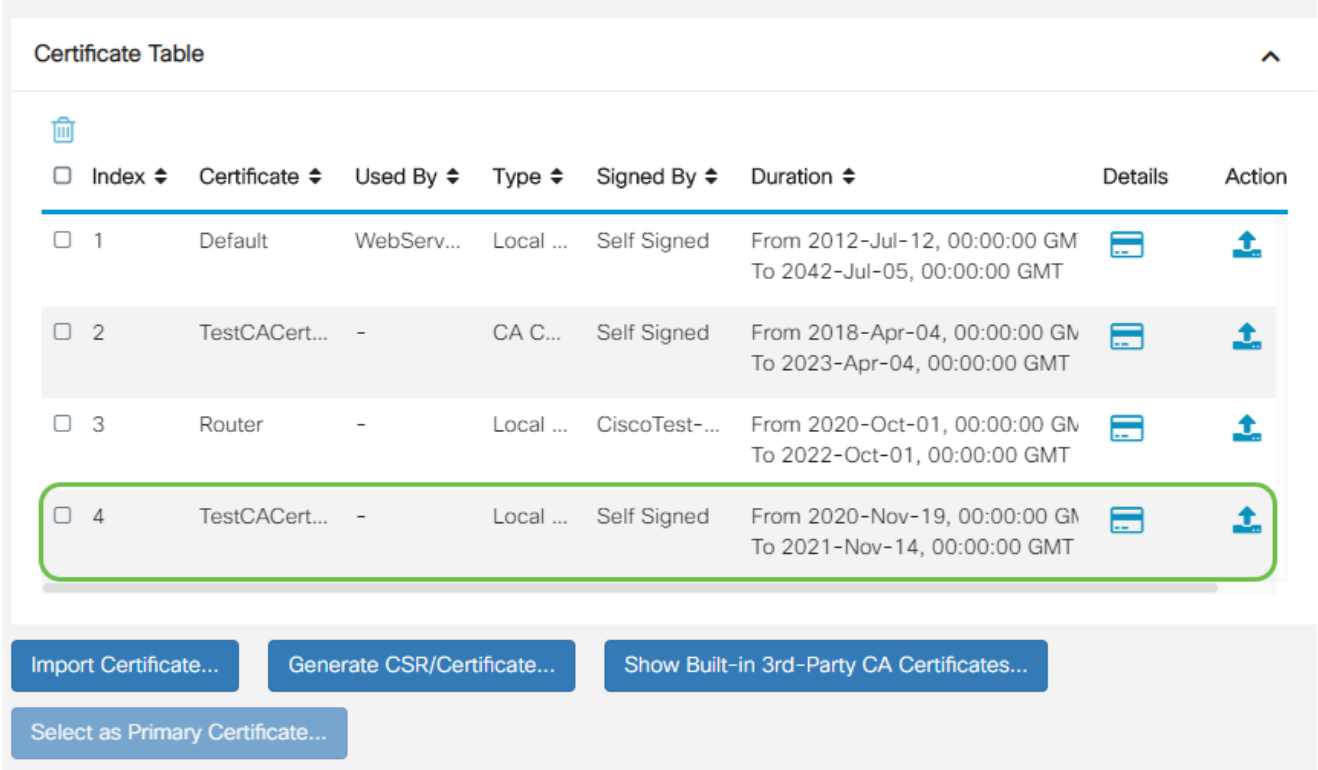
Paso 2

- Elija el tipo de certificado que desea importar en la lista desplegable. Las opciones son:
  - Certificado local: un certificado generado en el router.
  - Certificado de CA: certificado certificado certificado por una autoridad de terceros

de confianza que ha confirmado que la información contenida en el certificado es exacta.
    - PKCS #12 Archivo codificado: Public Key Cryptography Standards (PKCS) #12 es un formato de almacenamiento de un certificado de servidor.
- Introduzca un nombre para el certificado en el campo Nombre del certificado.
- Si ha elegido PKCS #12, introduzca una contraseña para el archivo en el campo Import Password (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 aparecerá atenuada.
- Si selecciona 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 correspondiente.
- Haga clic en Cargar.



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



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

Configuración de una red móvil mediante un dongle y un router de la serie RV345P (opcional)

Es posible que desee configurar una red móvil de reserva mediante un mecanismo de seguridad y el 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 de Cisco Business.

Configuración de la red de malla inalámbrica

CBW140AC Out of the Box

Comience conectando un cable Ethernet desde el puerto PoE del CBW140AC a un puerto PoE del RV345P. La mitad de los puertos del RV345P pueden proporcionar PoE, por lo que se puede utilizar cualquiera de ellos.

Compruebe el estado de las luces testigo. El arranque del punto de acceso tardará unos 10 minutos. El LED parpadeará en verde en varios patrones, alternando rápidamente entre verde, rojo y ámbar antes de volver a iluminarse en verde. Puede haber pequeñas variaciones en la intensidad y el tono del color del LED de una unidad a otra. Cuando la luz LED parpadee en verde, continúe con el siguiente paso.

El puerto de enlace ascendente Ethernet PoE del punto de acceso de la aplicación móvil

SOLO se puede utilizar para proporcionar un enlace ascendente a la LAN y NO para conectarse a ningún otro dispositivo con capacidad para aplicaciones móviles o de extensión de malla.

Si el punto de acceso no es nuevo, asegúrese de que se ha restablecido a los parámetros predeterminados de fábrica para que el SSID de Cisco Business-Setup aparezca en las opciones Wi-Fi. Para obtener ayuda sobre esto, consulte Cómo reiniciar y restablecer los parámetros predeterminados de fábrica en los routers RV345x.

Configuración del punto de acceso inalámbrico 140AC Mobile Application

En esta sección, utilizará la aplicación móvil para configurar el punto de acceso inalámbrico de la aplicación móvil.

Tenga en cuenta que la aplicación se actualiza con frecuencia y que el aspecto o el diseño pueden cambiar con el tiempo.

En la parte posterior del 140AC, conecte el cable que venía con el AP en el PoE amarillo y enchufe su 140 AC. Conecte el otro extremo a uno de los puertos LAN del RV345P.

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

Paso 1

Descargue la aplicación Cisco Business Wireless App disponible en Google Play o la App Store de Apple en su dispositivo móvil. Necesitará uno de los siguientes sistemas operativos:

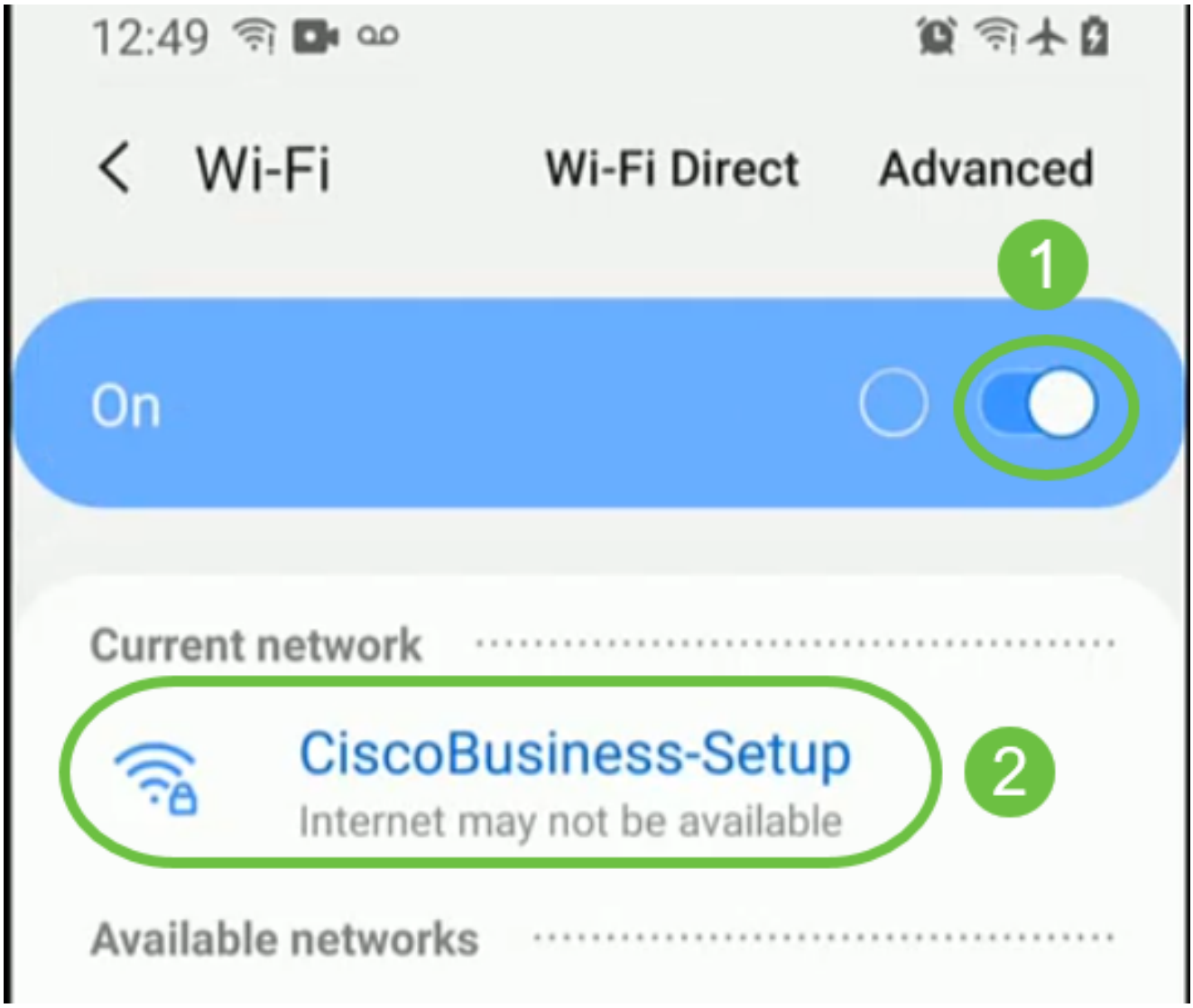
- Android versión 5.0 o superior
- versión 8.0 o superior de iOS

Paso 2

Abra la aplicación Cisco Business en su dispositivo móvil.

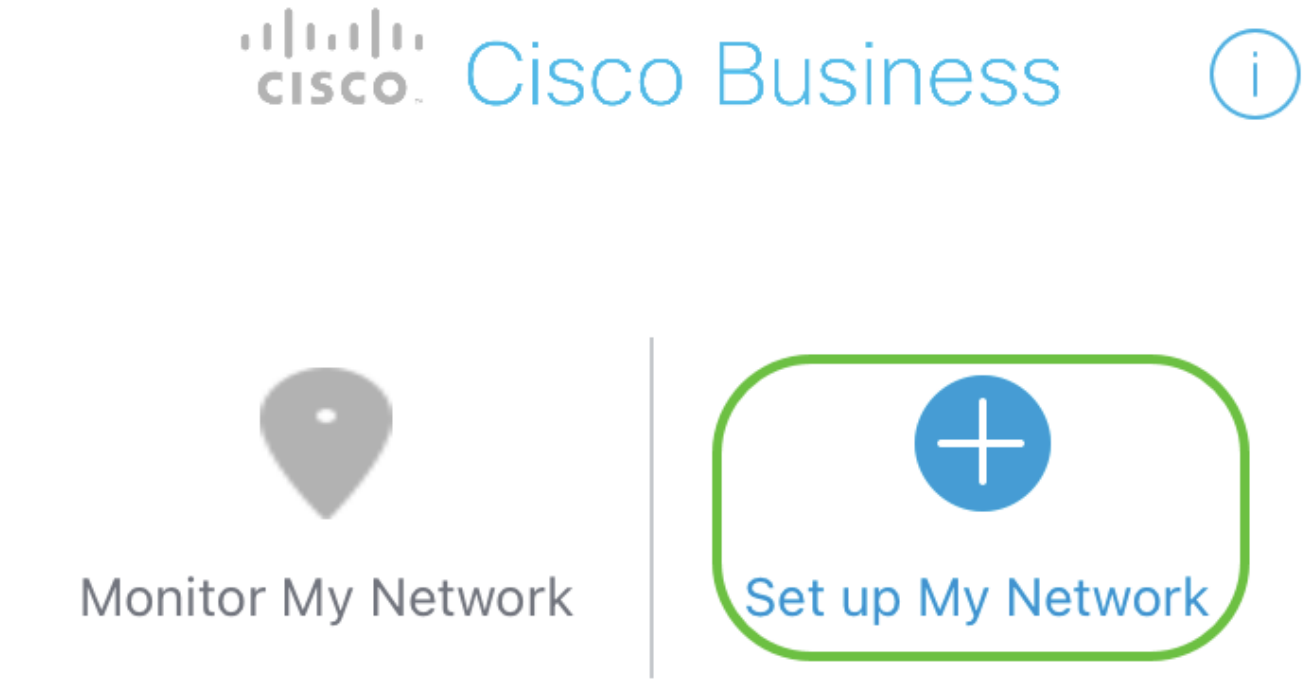
Paso 3

Conéctese a la red inalámbrica Cisco Business-Setup en su dispositivo móvil. La frase de contraseña es cisco123.



Paso 4

La aplicación detecta automáticamente la red móvil. Seleccione Configurar mi red.

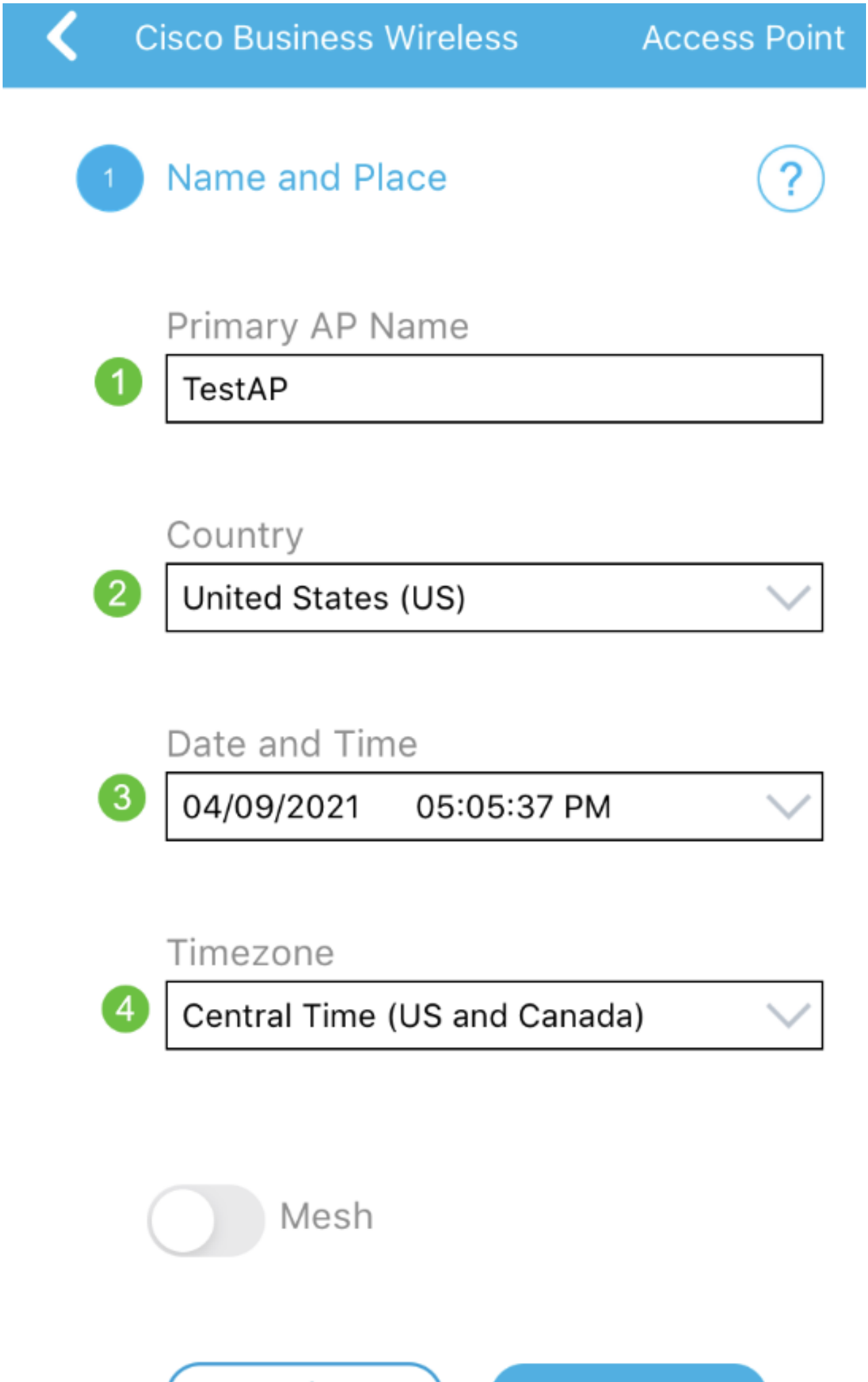


Paso 5

Para configurar la red, introduzca lo siguiente:

- Crear nombre de usuario de administrador
- Crear contraseña de administrador
- Confirme la contraseña de administrador volviéndola a introducir
- (Opcional) Active la casilla de verificación para Mostrar contraseña.

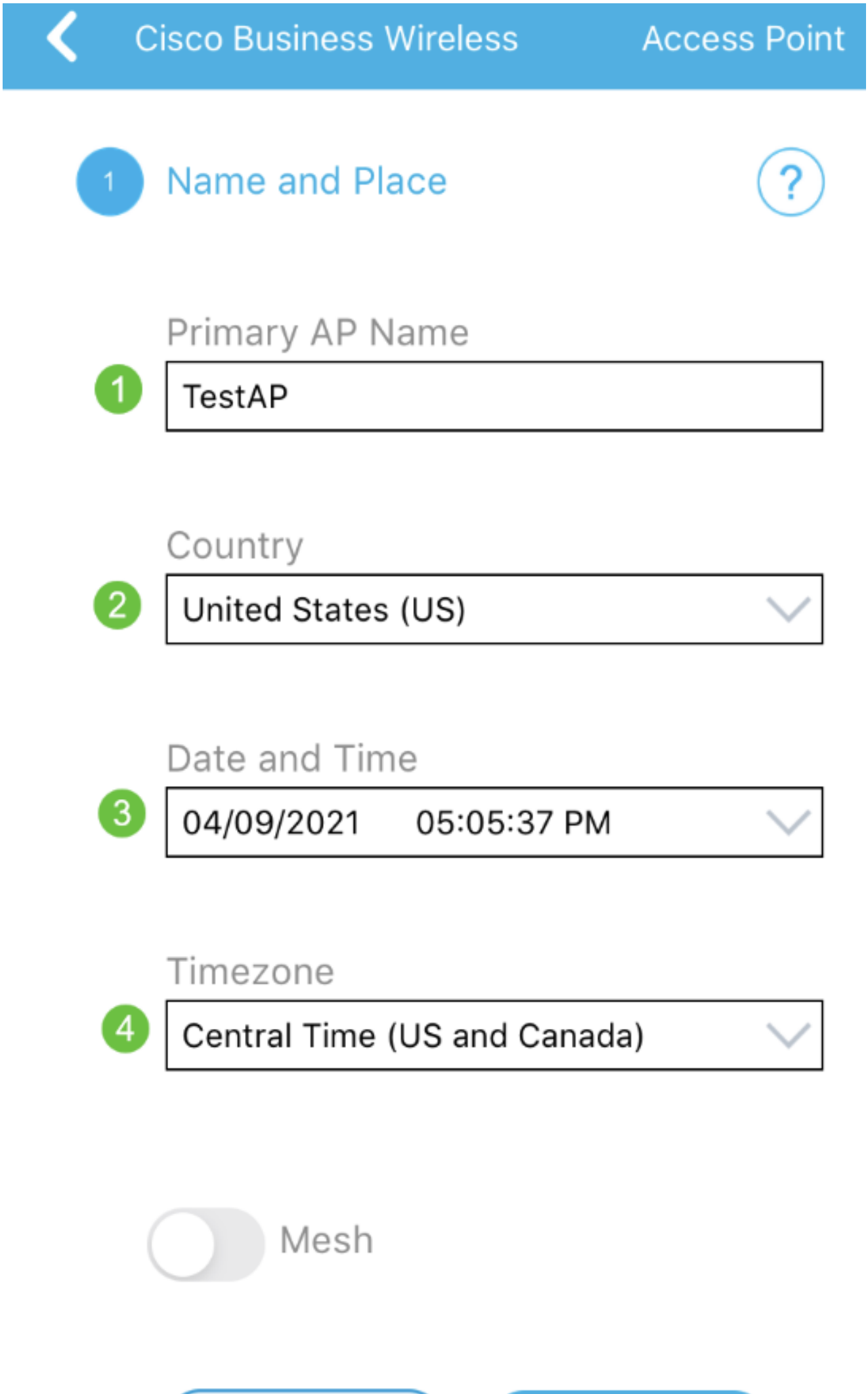
Seleccione Introducción.


Cisco Business Wireless
Access Point
1
Name and Place
?
Primary AP Name
1
TestAP
Country
2
United States (US)
Date and Time
3
04/09/2021 05:05:37 PM
Timezone
4
Central Time (US and Canada)
Mesh

Paso 6

Para configurar Name y Place, introduzca con precisión la siguiente información. Si introduce información conflictiva, puede provocar un comportamiento impredecible.

- Nombre del punto de acceso de la aplicación móvil para la red inalámbrica.
- País
- Fecha
- Hora
- Zona horaria


Cisco Business Wireless
Access Point
1
Name and Place
Primary AP Name
1
TestAP
Country
2
United States (US)
Date and Time
3
04/09/2021 05:05:37 PM
Timezone
4
Central Time (US and Canada)
Mesh

Paso 7

Encienda la palanca de malla. Haga clic en Next (Siguiente).

1 Name and Place

Primary AP Name

TestAP

Country

United States (US)

Date and Time

04/09/2021 05:05:37 PM

Timezone

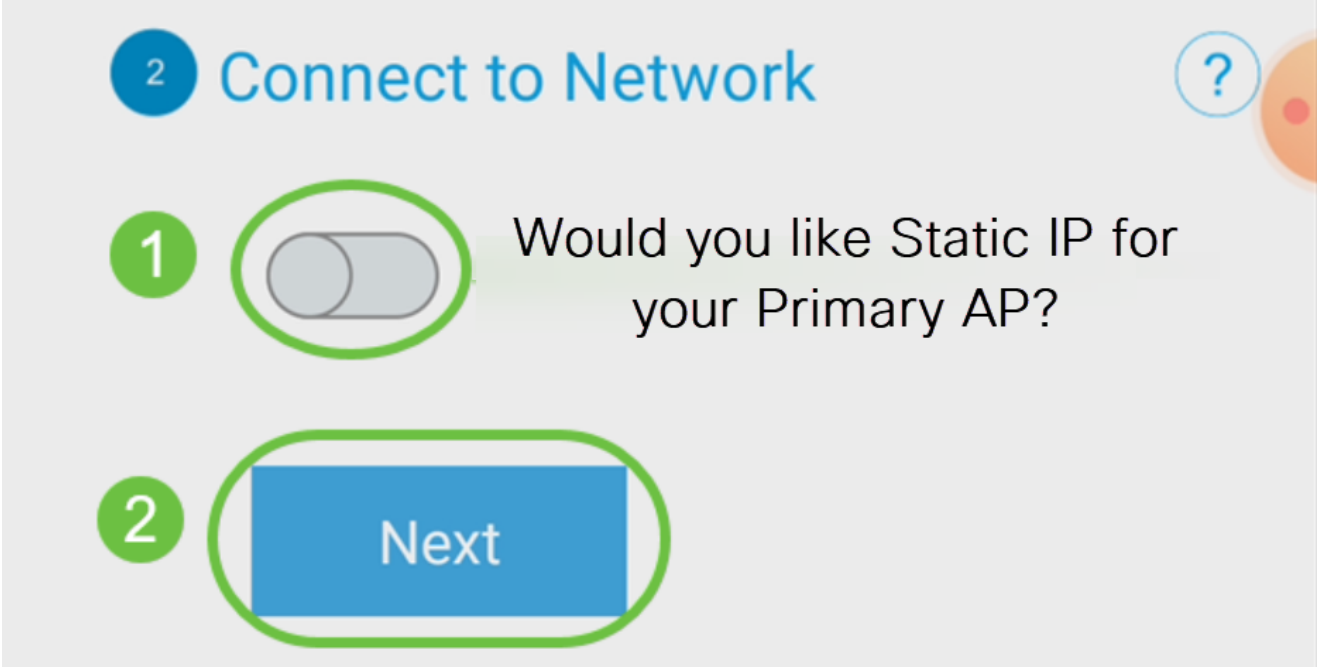
Central Time (US and Canada)

1

Mesh

Paso 8

(Opcional) Puede optar por habilitar la IP estática para el AP de la aplicación móvil para fines de administración. Si no es así, el servidor DHCP asignará una dirección IP. Si no desea configurar una IP estática para el punto de acceso, haga clic en Next.

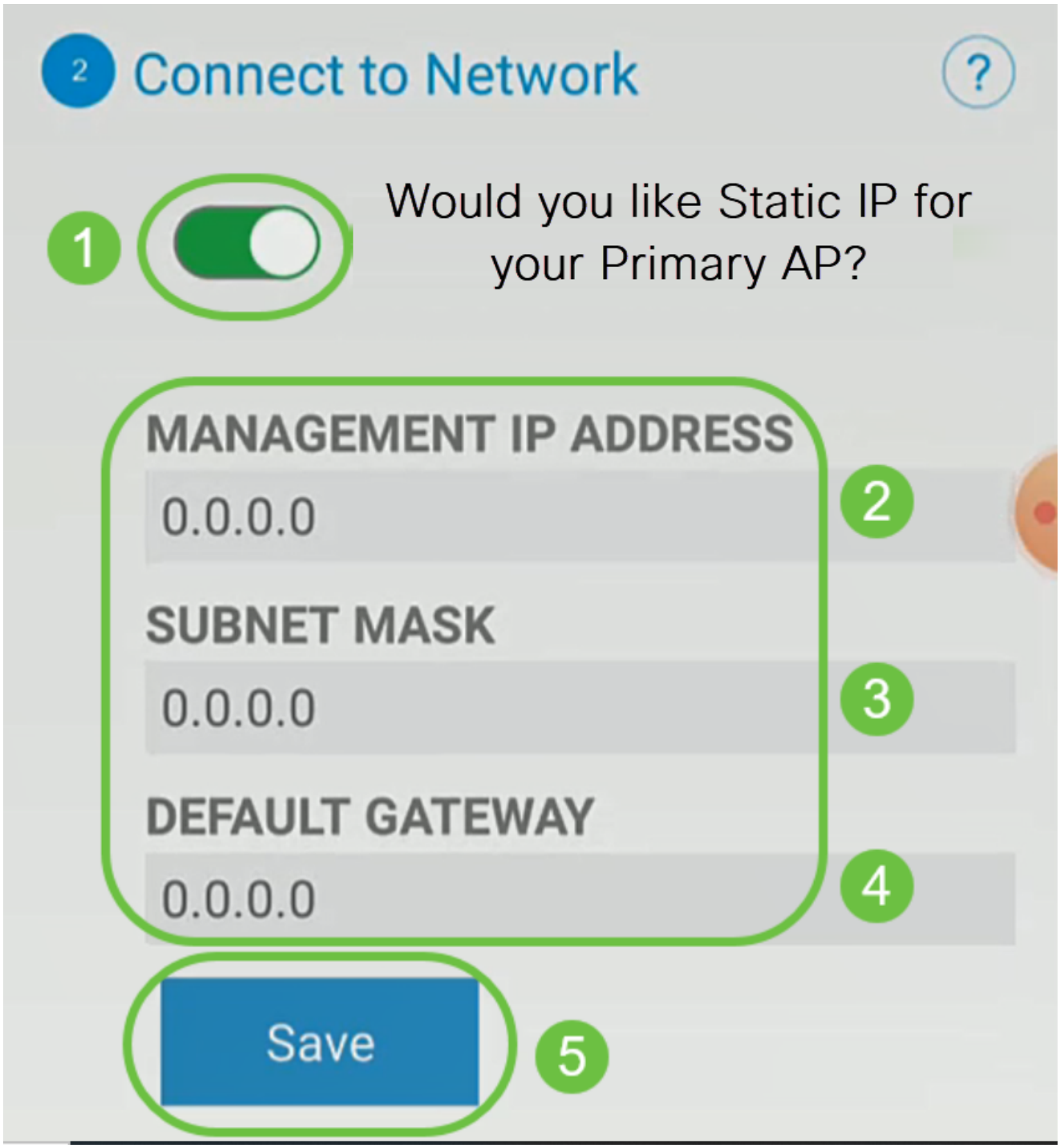


Como alternativa, para conectarse a la red:

Seleccione Static IP for your Mobile Application AP. De forma predeterminada, esta opción está desactivada.

- Introduzca la dirección IP de gestión
- Máscara de subnet
- Gateway predeterminado

Click Save.

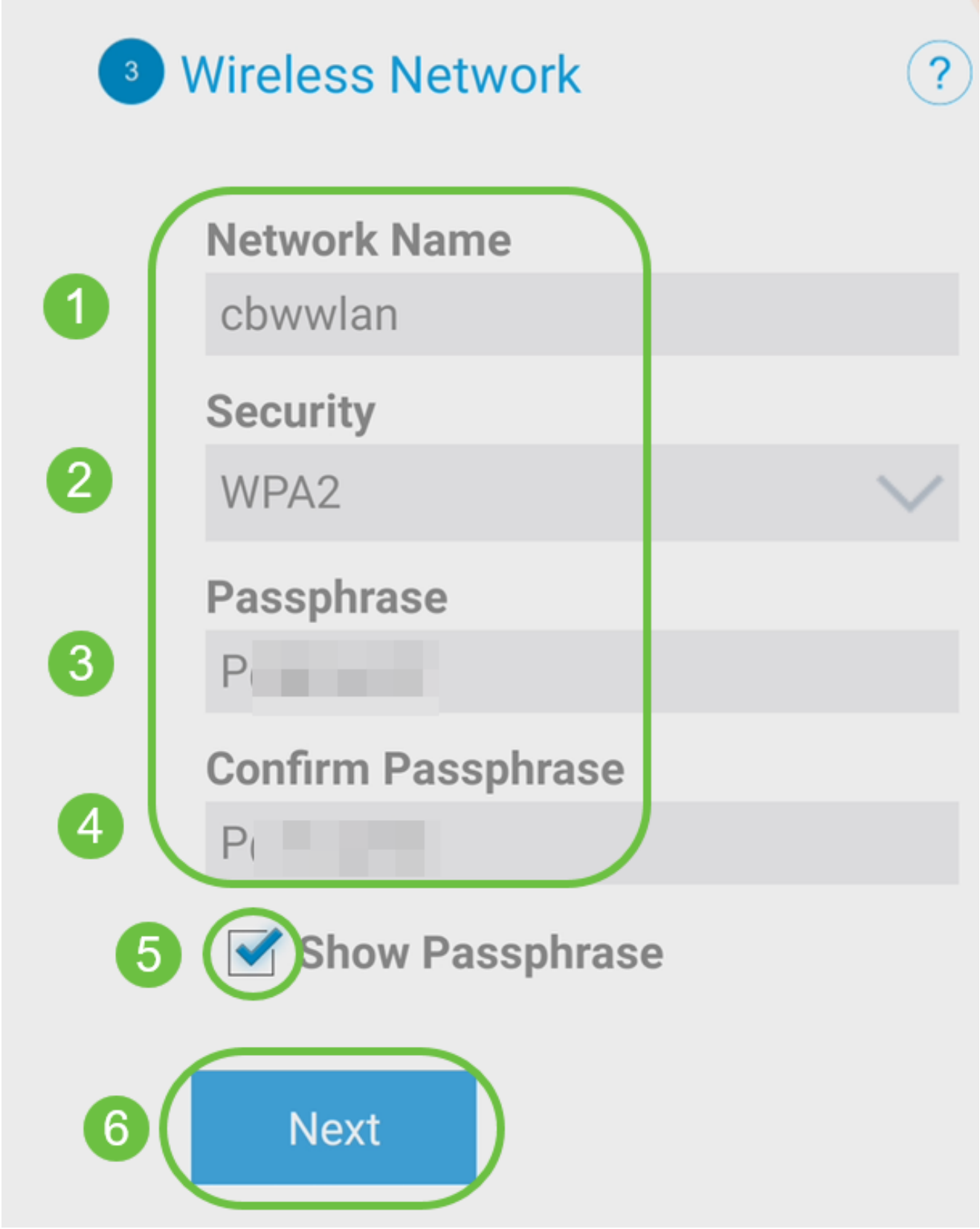


Paso 9

Configure la red inalámbrica introduciendo lo siguiente:

- Nombre de red/SSID
- Security
- Frase de contraseña
- Confirmar frase de contraseña
- (Opcional) Marque Mostrar frase de paso

Haga clic en Next (Siguiente).

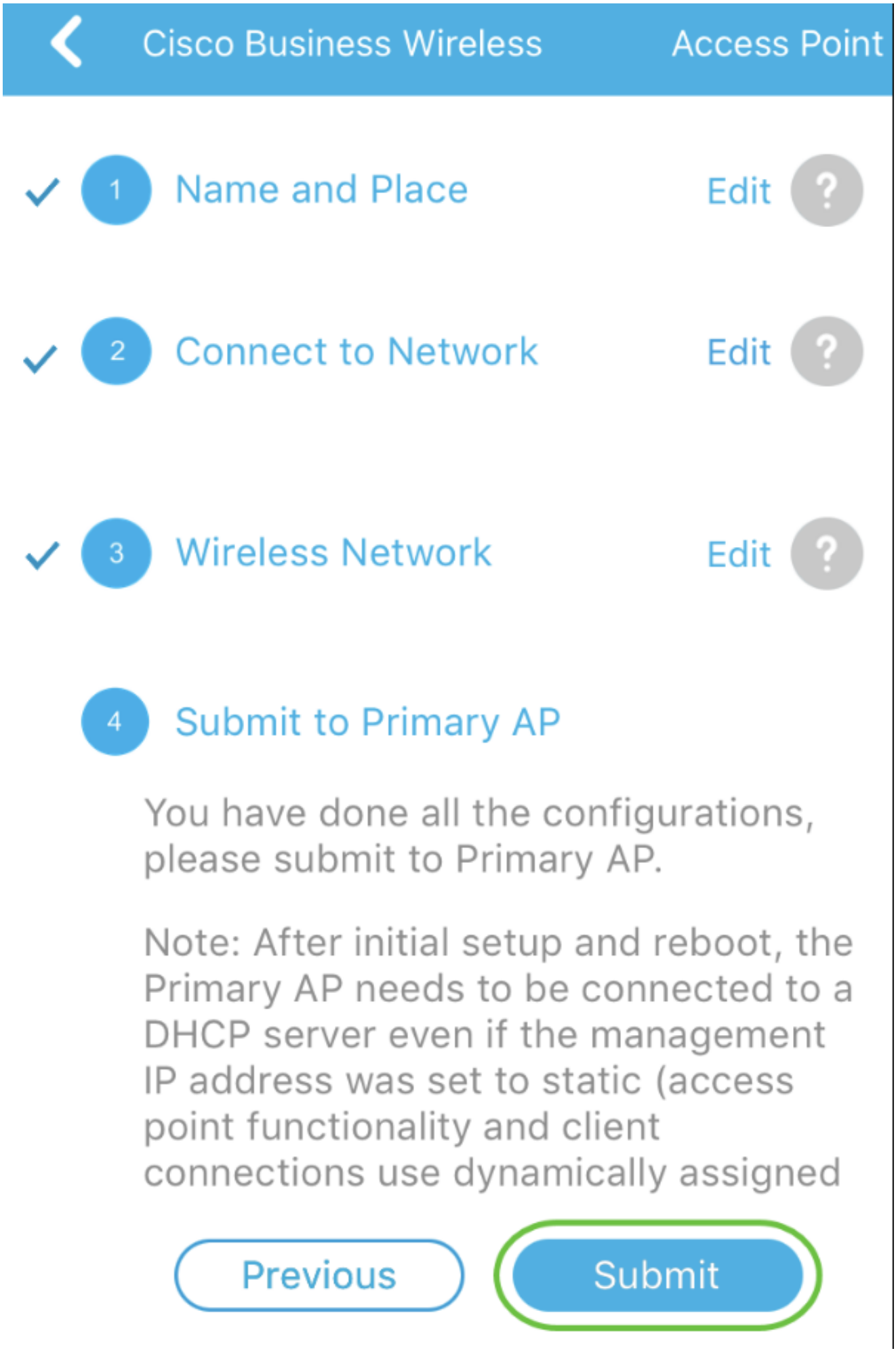


El acceso Wi-Fi protegido (WPA) versión 2 (WPA2) es el estándar actual de seguridad Wi-Fi.

Paso 10

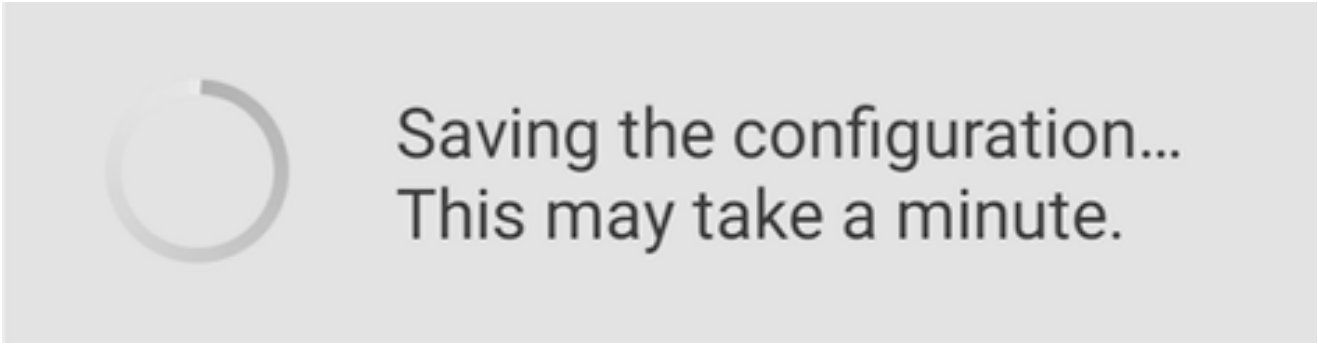
Para confirmar la configuración en la pantalla Enviar a AP de aplicación móvil, haga clic en

Enviar.


Cisco Business Wireless
Access Point
1
Name and Place
Edit
2
Connect to Network
Edit
3
Wireless Network
Edit
4
Submit to Primary AP
You have done all the configurations, please submit to Primary AP.
Note: After initial setup and reboot, the Primary AP needs to be connected to a DHCP server even if the management IP address was set to static (access point functionality and client connections use dynamically assigned
Previous
Submit

Paso 11

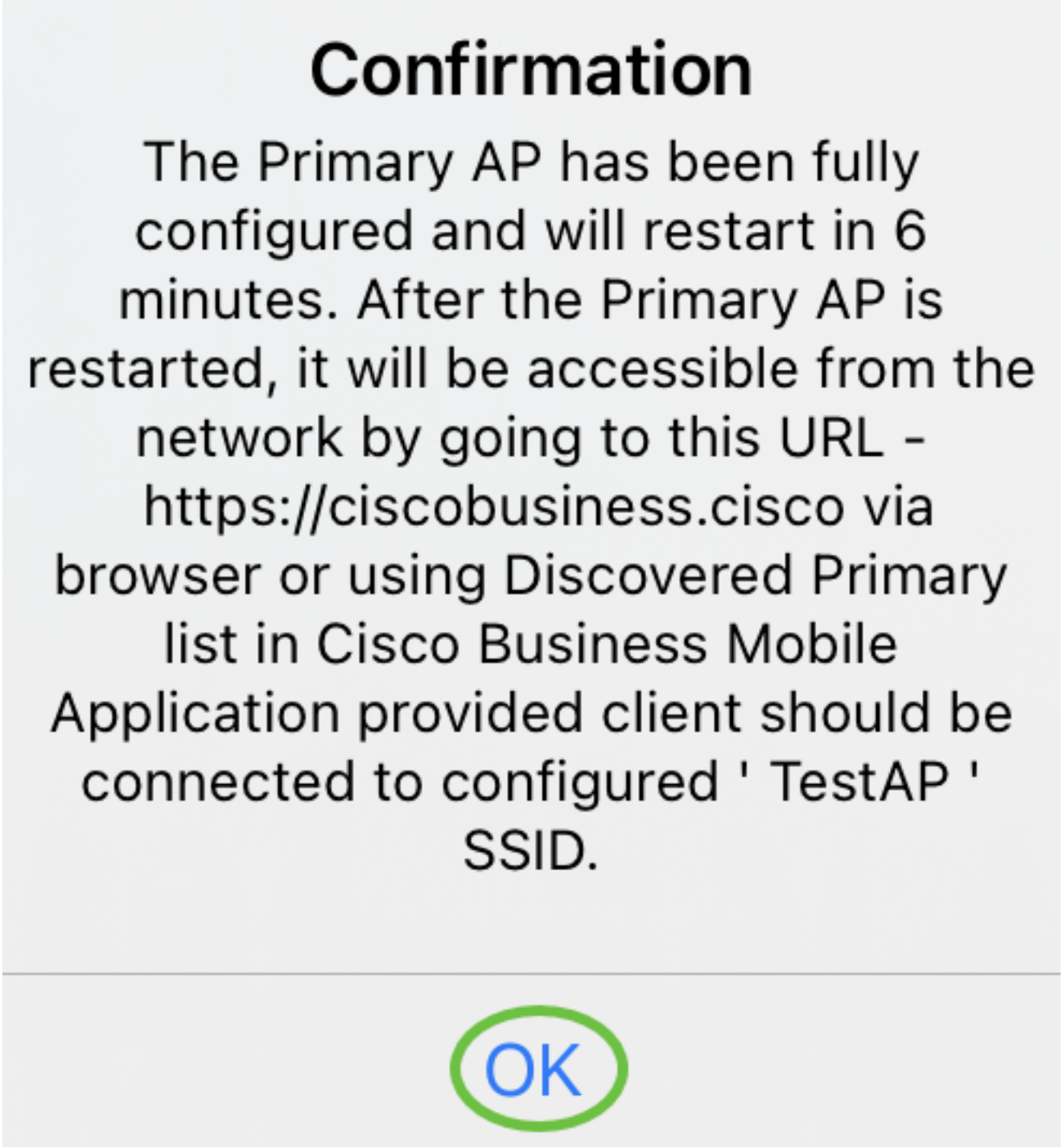
Espere a que se complete el reinicio.



El reinicio puede tardar hasta 10 minutos. Durante un reinicio, el LED del punto de acceso pasará por varios patrones de color. Cuando el LED parpadee en verde, vaya al paso siguiente. Si la luz no supera el patrón de parpadeo rojo, indica que la red no tiene servidor DHCP. Asegúrese de que el AP esté conectado a un switch o un router con un servidor DHCP.

Paso 12

Verá la siguiente pantalla Confirmation (Confirmación). Click OK.



Paso 13

Cierre la aplicación, conéctese a la red inalámbrica recién creada y vuelva a iniciarla para completar correctamente la primera parte de la red inalámbrica.

Consejos para Troubleshooting Inalámbrico

Si tiene algún problema, consulte los siguientes consejos:

- Asegúrese de que se ha seleccionado el identificador del conjunto de servicios (SSID) correcto. Este es el nombre que ha creado para la red inalámbrica.
- Desconecte cualquier VPN de la aplicación móvil o de un portátil. Es posible que

incluso esté conectado a una VPN que su proveedor de servicios móviles utiliza y que es posible que ni siquiera conozca. 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 debería ser inhabilitado para encontrar el AP de la aplicación móvil.

- Inicie sesión en el AP de aplicación móvil con https://<dirección IP del AP de aplicación móvil>.
- Una vez que haya realizado la configuración inicial, asegúrese de que https:// is se esté utilizando tanto si está iniciando sesión en ciscobusiness.cisco como si introduce la dirección IP en su navegador web. Según la configuración, es posible que el equipo se haya llenado automáticamente con http:// since, que es lo que utilizó la primera vez que inició sesión.
- 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 ampliadores de malla CBW142ACM

Se encuentra en la etapa inicial de la configuración de esta red, solo tiene que agregar sus extensores de malla!

Inicie sesión en la aplicación Cisco Business en su dispositivo móvil.

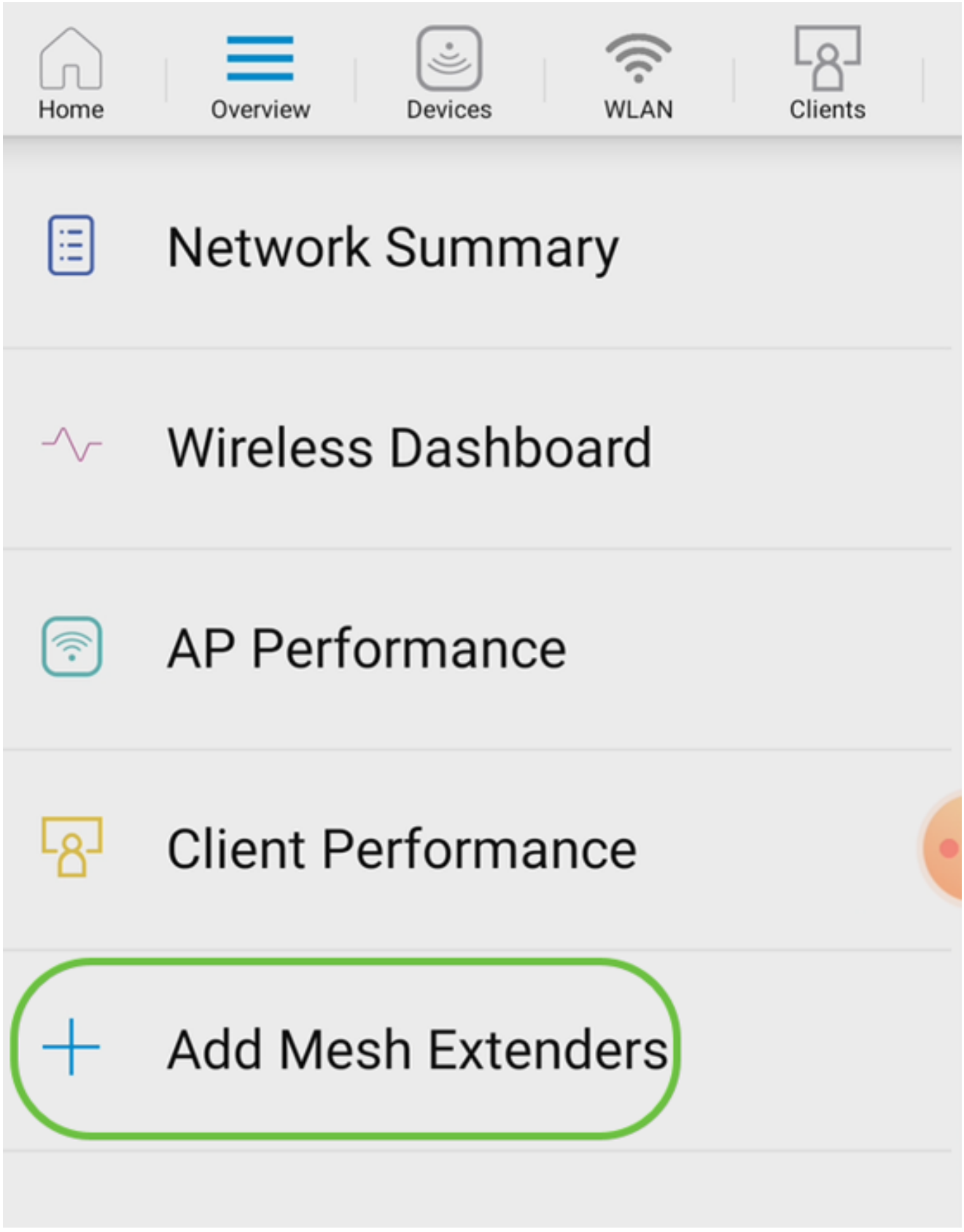
Paso 1

Vaya a Dispositivos. Vuelva a comprobar que la malla está activada.

Name	Clients	Usage
APA453.0E1E.2338*	0	0 Bytes
AP4CBC.48C0.74B8	0	0 Bytes
APA453.0E22.0A70	0	0 Bytes
AP68CA.E46E.1650	0	2 MB
AP68CA.E470.0500	0	11 MB

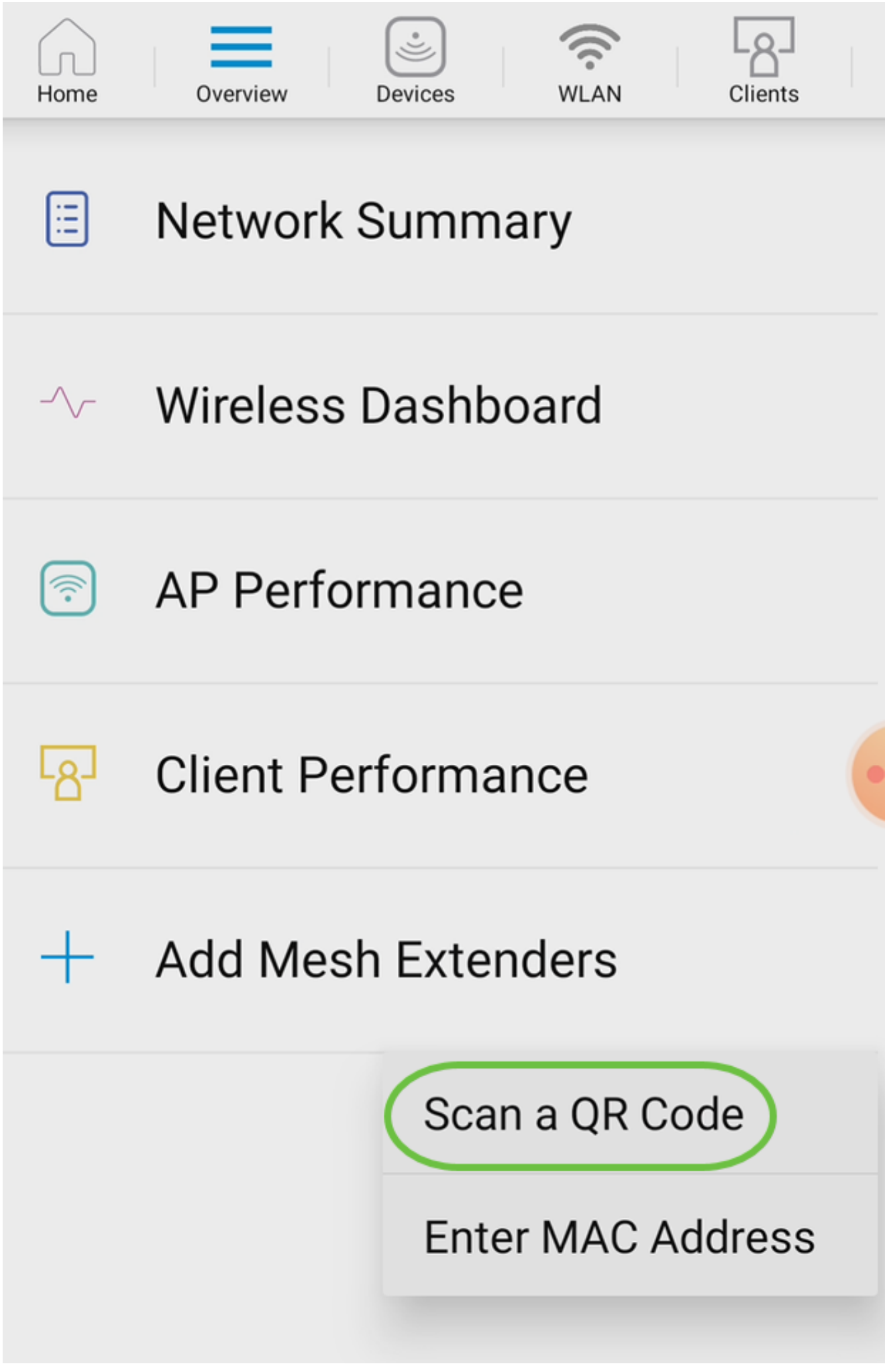
Paso 2

Debe ingresar la dirección MAC de todos los Mesh Extenders que desea utilizar en la red de malla con el Mobile Application AP. Para agregar la dirección MAC, haga clic en Add Mesh Extenders en el menú.



Paso 3

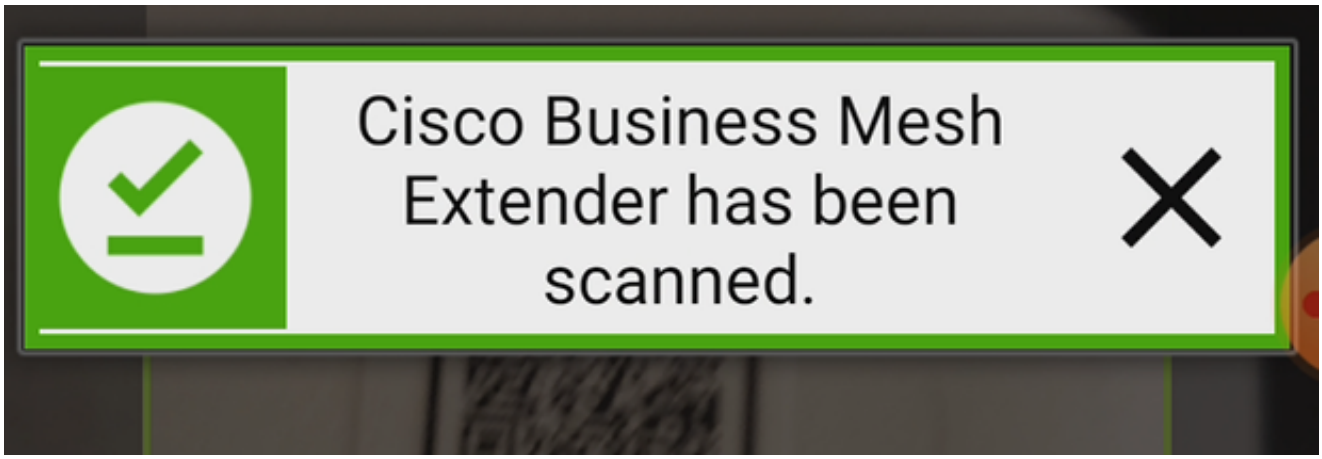
Puede agregar la dirección MAC escaneando un código QR o introduciendo manualmente la dirección MAC. En este ejemplo, se selecciona Scan a QR code.


Home
Overview
Devices
WLAN
Clients
Network Summary
Wireless Dashboard
AP Performance
Client Performance
Add Mesh Extenders
Scan a QR Code
Enter MAC Address

Paso 4

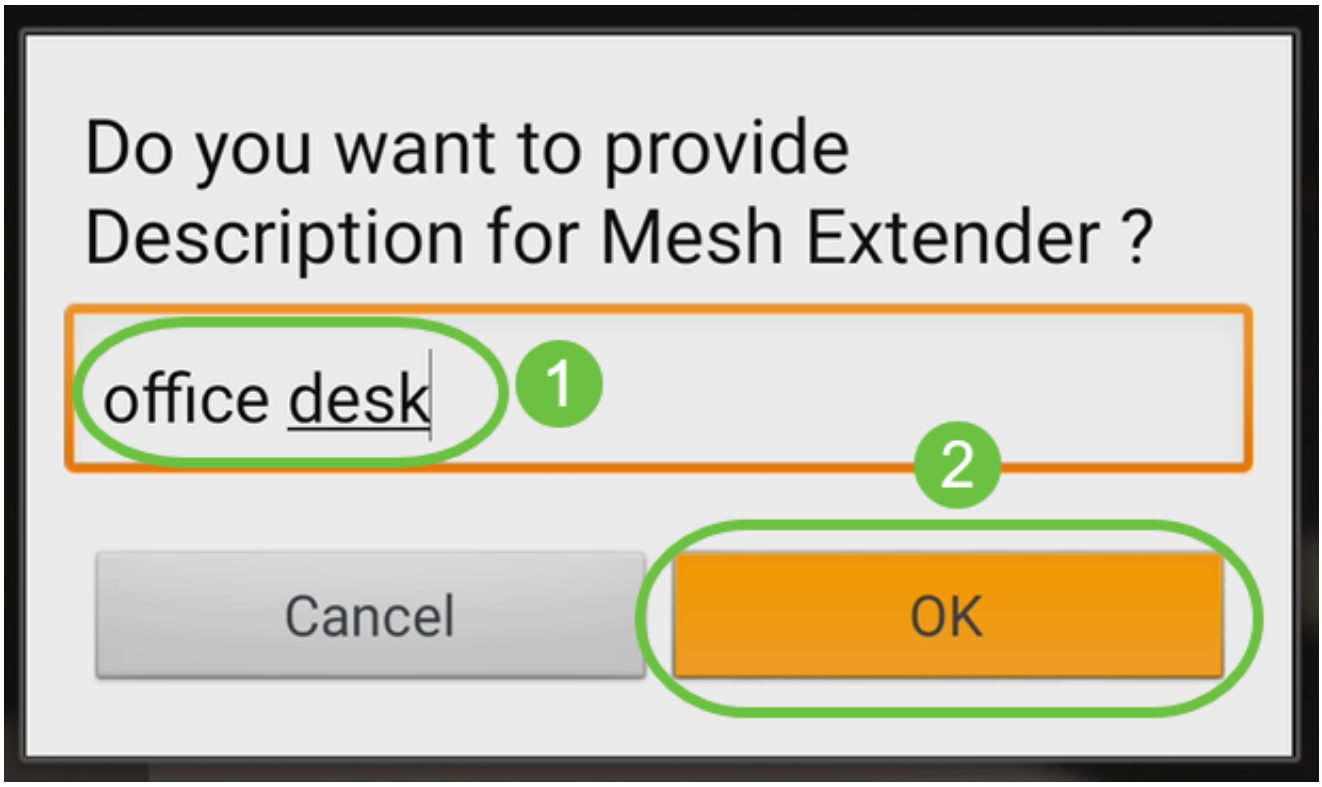
Aparecerá un lector de códigos QR para escanear el código QR.

Una vez escaneado el código QR del ampliador de malla, verá la siguiente pantalla.



Paso 5 (opcional)

Si lo prefiere, introduzca una descripción para el extensor de malla. Click OK.



Paso 6

Revise el resumen y haga clic en Enviar.

Summary

Almost done. The following Mesh Extenders will be added to your site. If you are done adding Mesh Extenders, click submit.

Mesh Extenders To Be Added

Scanned MAC Address

A4 0 office desk

Paso 7

Haga clic en Add More Mesh Extenders para agregar otros extensores de malla a su red. Una vez agregados todos los extensores de malla, haga clic en Finalizado.

Done! Your Mesh Extender has been added

Good News! You've successfully added your Mesh Extender

Mesh Extender Status

A4 0 SUCCESS

What's Next ?

Add More Mesh Extenders

Repita este procedimiento para cada extensor de malla.

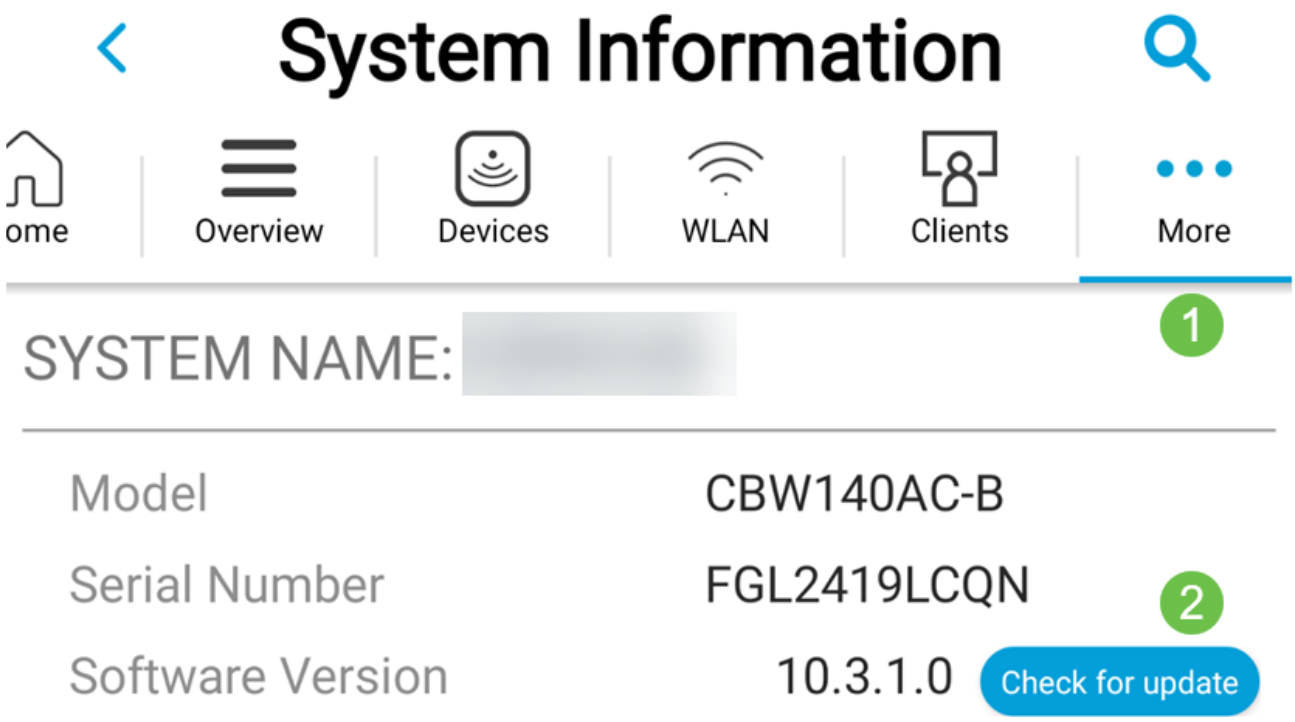
Ya tiene los parámetros básicos listos para la reversión. Antes de continuar, asegúrese de comprobar y actualizar el software si es necesario.

Comprobación y actualización de software en la aplicación móvil

La actualización del software es extremadamente importante, así que no se salte esta parte.

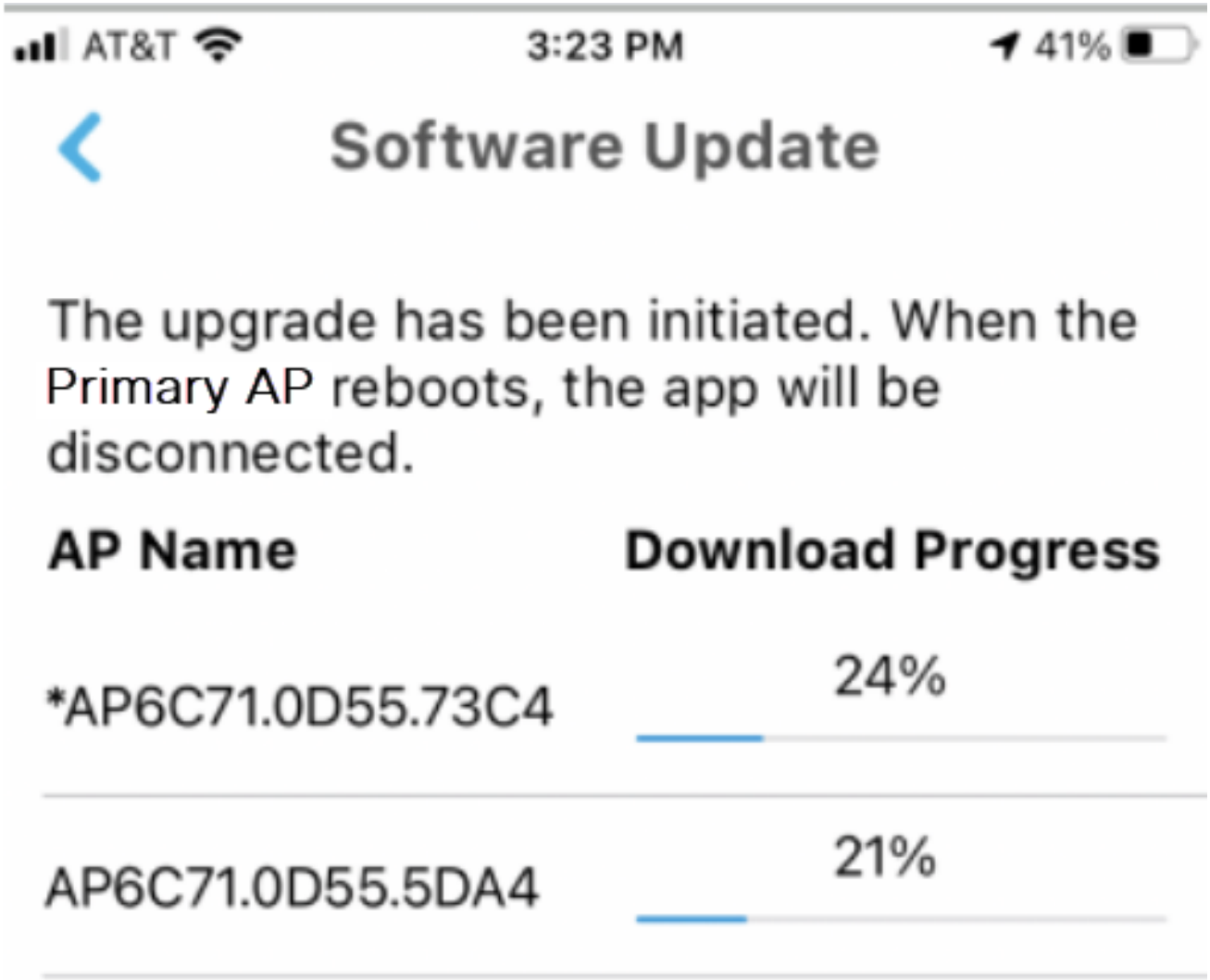
Paso 1

En la aplicación móvil, en la pestaña More, haga clic en el botón Check for update. Siga las indicaciones para actualizar el software a la última versión.



Paso 2

Verá el progreso de la descarga a medida que se carga.


AT&T
3:23 PM
41%
Software Update
The upgrade has been initiated. When the Primary AP reboots, the app will be disconnected.
AP Name
Download Progress
*AP6C71.0D55.73C4
24%
AP6C71.0D55.5DA4
21%

Paso 3

Una confirmación emergente le notificará la conclusión de la actualización del software. Click OK.

Creación de WLAN mediante la aplicación móvil

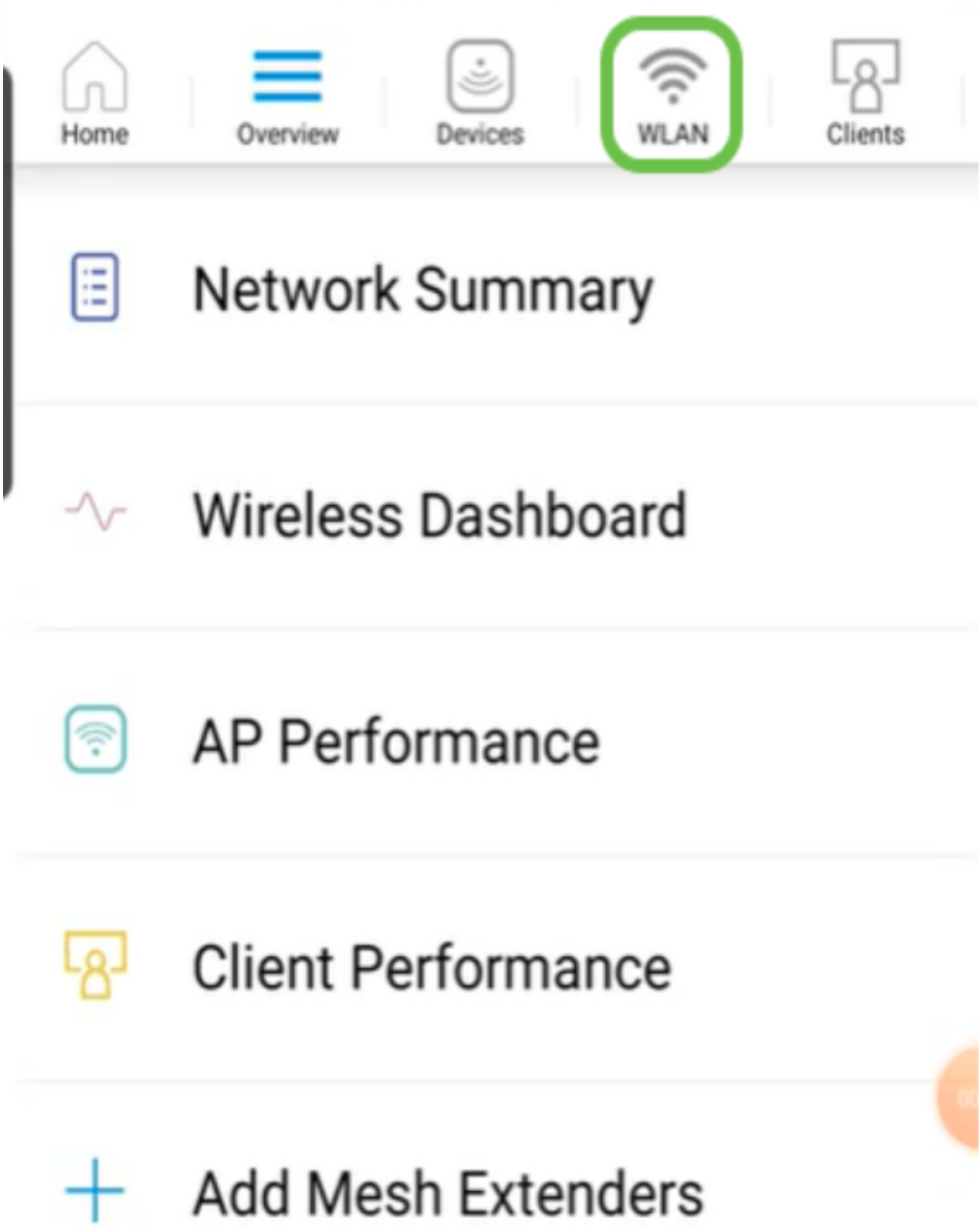
En esta sección puede crear redes de área local inalámbricas (WLAN).

Paso 1

Abra la aplicación Cisco Business Wireless.

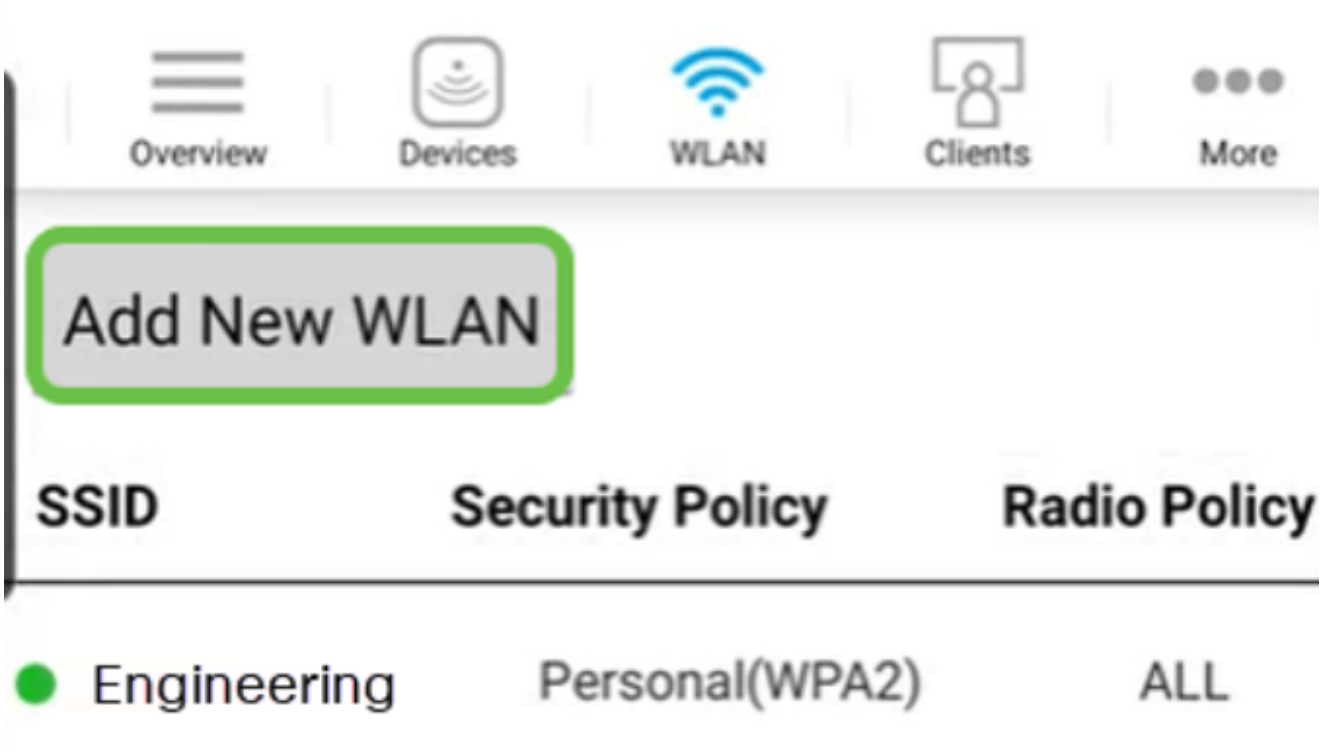
Paso 2

Conéctese a la red inalámbrica empresarial de Cisco desde su teléfono móvil. Inicie sesión en la aplicación. Haga clic en el icono WLAN en la parte superior de la página.



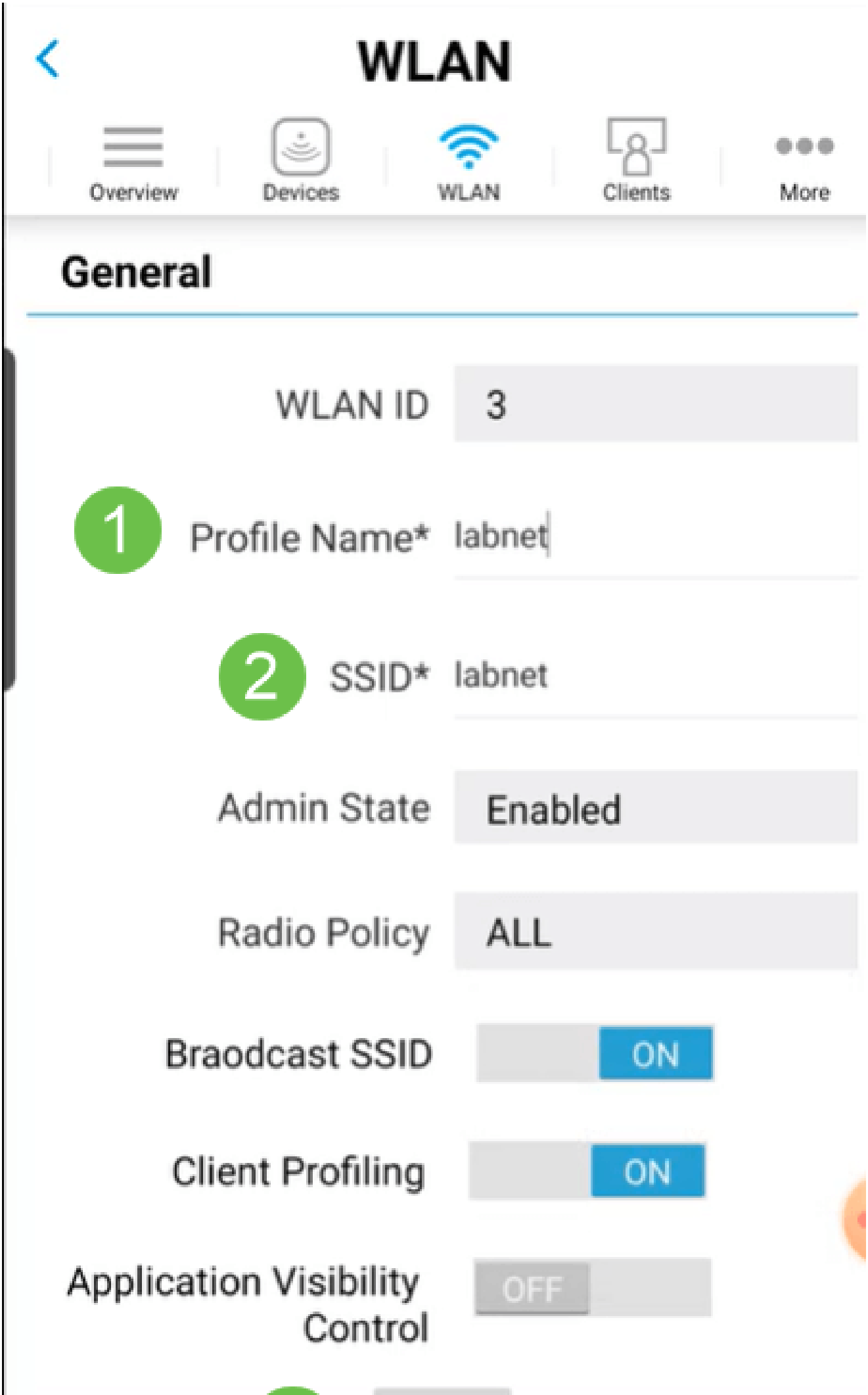
Paso 3

Se abre la pantalla Add New WLAN. Verá las WLAN existentes. Seleccione Add New WLAN.



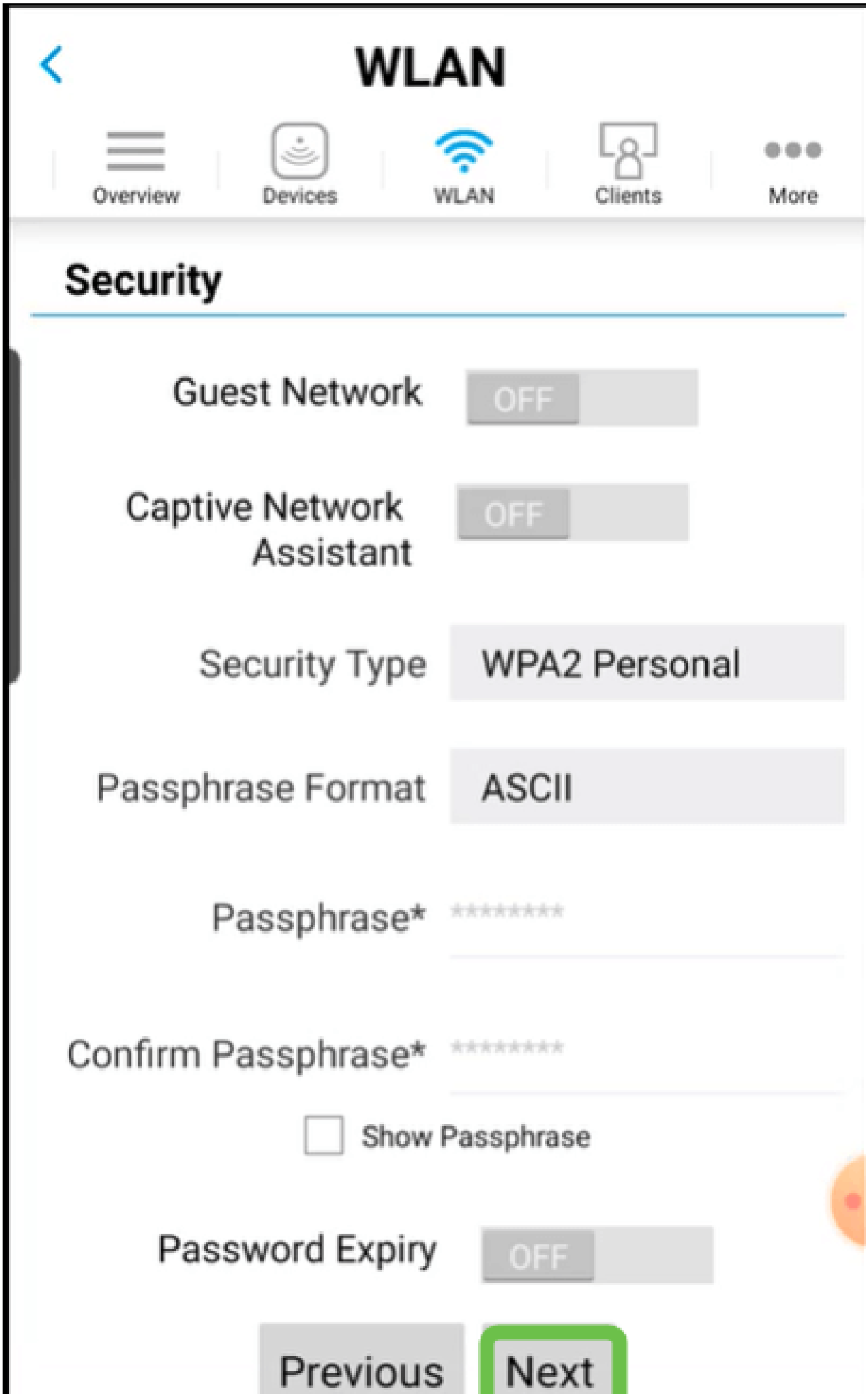
Paso 4

Introduzca un nombre de perfil y SSID. Rellene el resto de los campos o déjelos con la configuración predeterminada. Si ha activado el control de visibilidad de la aplicación, tendrá otras configuraciones explicadas en el paso 6. Haga clic en Next (Siguiente).


WLAN
Overview
Devices
WLAN
Clients
More
General
WLAN ID
3
1
Profile Name*
labnet
2
SSID*
labnet
Admin State
Enabled
Radio Policy
ALL
Braodcast SSID
ON
Client Profiling
ON
Application Visibility Control
OFF

Paso 5 (opcional)

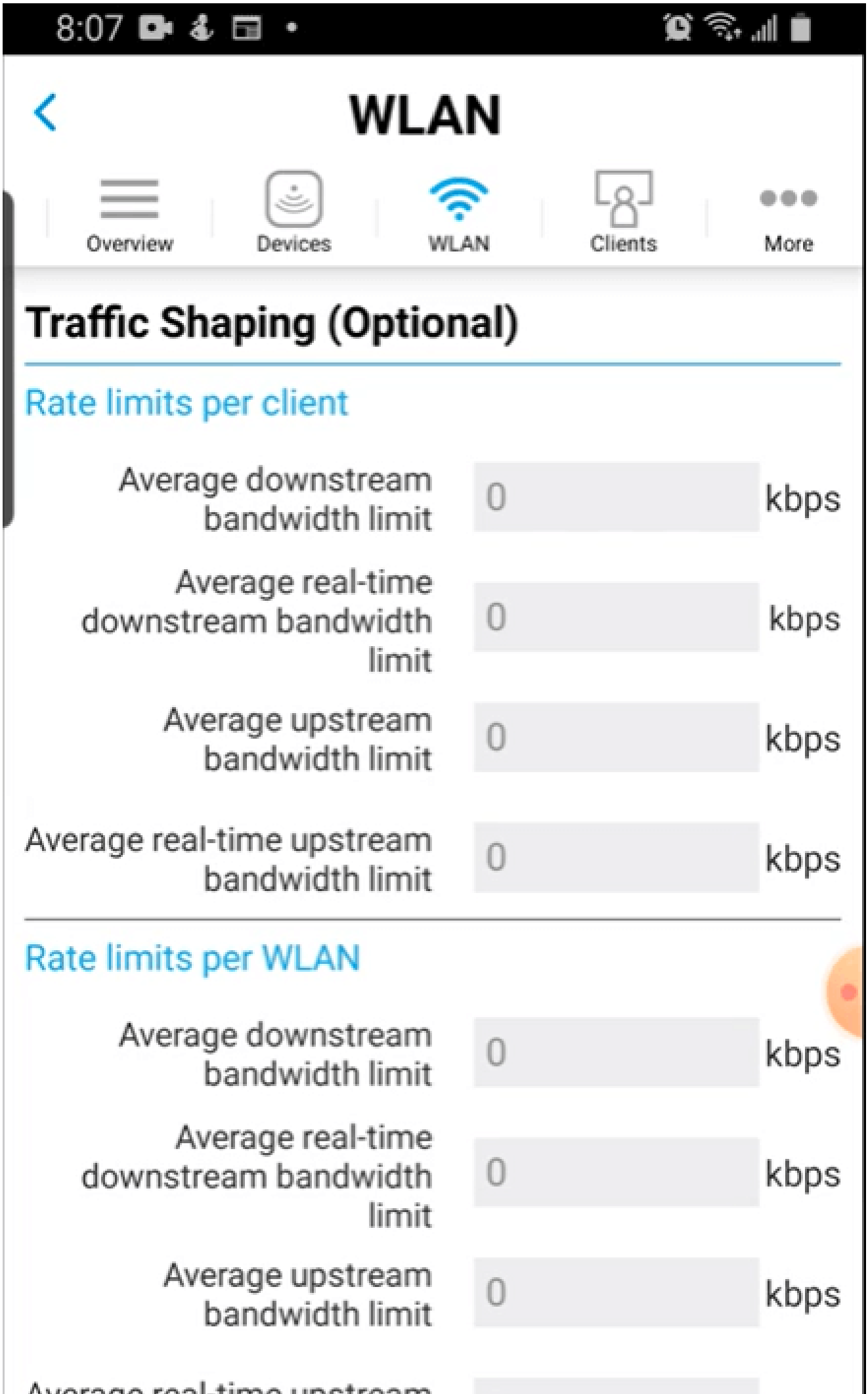
Si habilitó Application Visibility Control en el paso 4, puede configurar otros ajustes, incluida una red para invitados. Los detalles de esto se pueden encontrar en la siguiente sección. También se pueden agregar aquí Captive Network Assistant, Security Type, Passphrase y Password Expiry. Cuando haya agregado todas las configuraciones, haga clic en Next.


WLAN
Overview
Devices
WLAN
Clients
More
Security
Guest Network
OFF
Captive Network Assistant
OFF
Security Type
WPA2 Personal
Passphrase Format
ASCII
Passphrase*
Confirm Passphrase*
Show Passphrase
Password Expiry
OFF
Previous
Next

Cuando se utiliza la aplicación móvil, las únicas opciones para Security Type son Open o WPA2 Personal. Para obtener opciones más avanzadas, inicie sesión en la interfaz de usuario web del punto de acceso de la aplicación móvil.

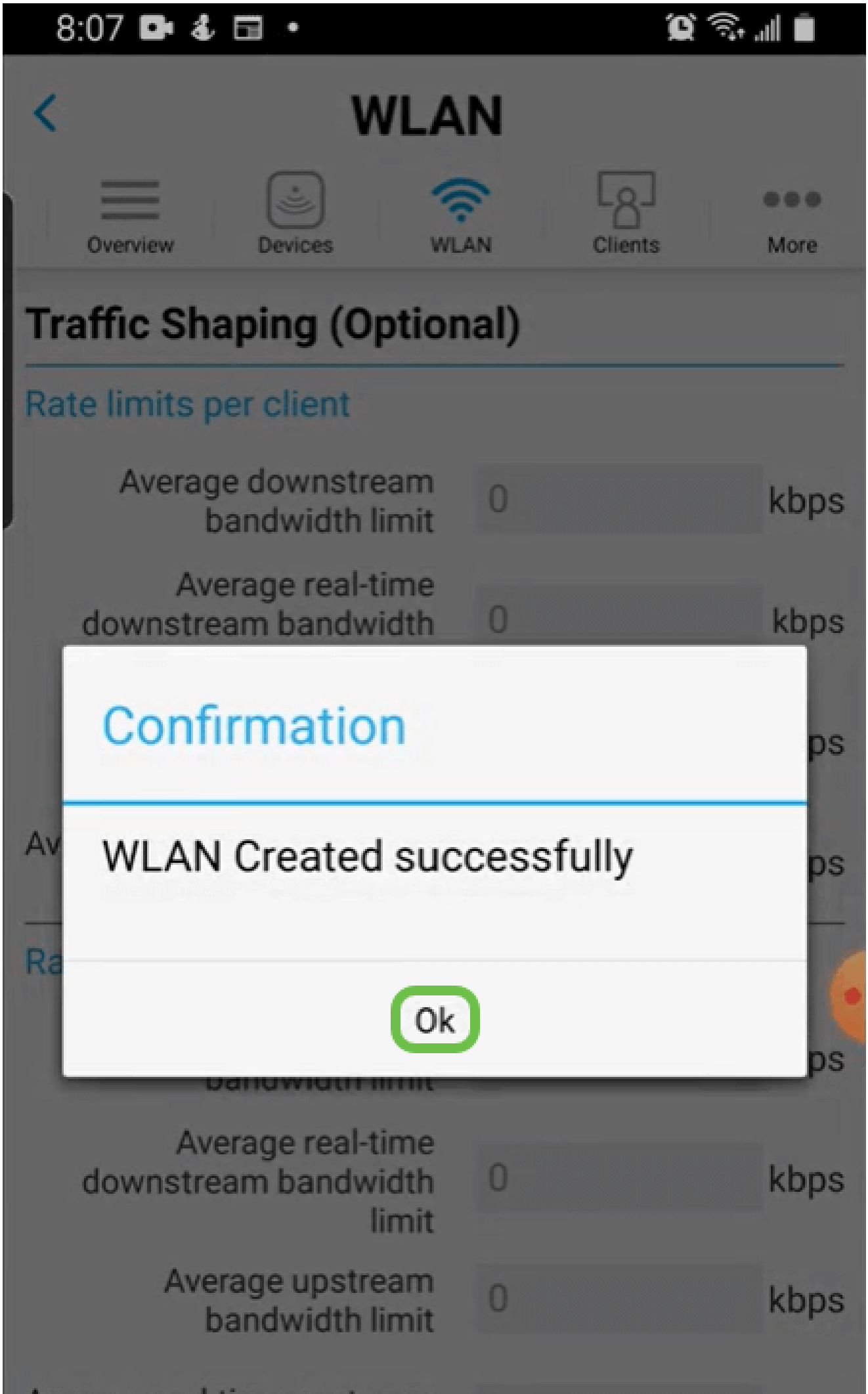
Paso 6 (opcional)

Esta pantalla ofrece las opciones para el modelado de tráfico. En este ejemplo, no se ha configurado ningún modelado de tráfico. Haga clic en Submit (Enviar).


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps
Average real-time upstream bandwidth limit
0
kbps
Rate limits per WLAN
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

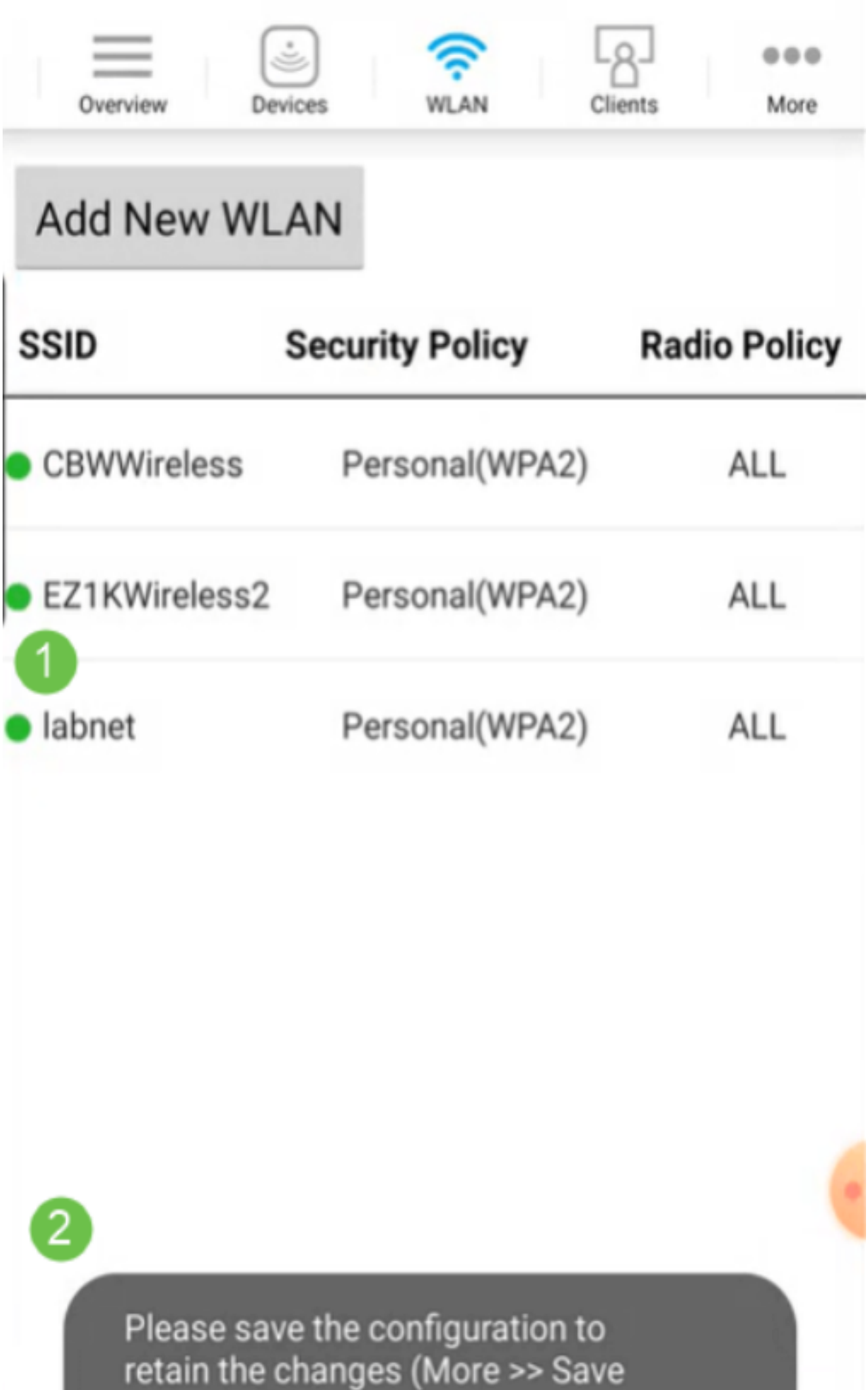
Paso 7

Verá una ventana emergente de confirmación. Click OK.


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth
0
kbps
Confirmation
WLAN Created successfully
Ok
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

Paso 8

Verá la nueva WLAN agregada a la red, así como un recordatorio para guardar la configuración.


Overview
Devices
WLAN
Clients
More
Add New WLAN
SSID
Security Policy
Radio Policy
CBWWireless
Personal(WPA2)
ALL
EZ1KWireless2
Personal(WPA2)
ALL
1
labnet
Personal(WPA2)
ALL
2
Please save the configuration to
retain the changes (More >> Save

Paso 9

Guarde su configuración haciendo clic en la pestaña More y luego seleccione Save Configuration en el menú desplegable.

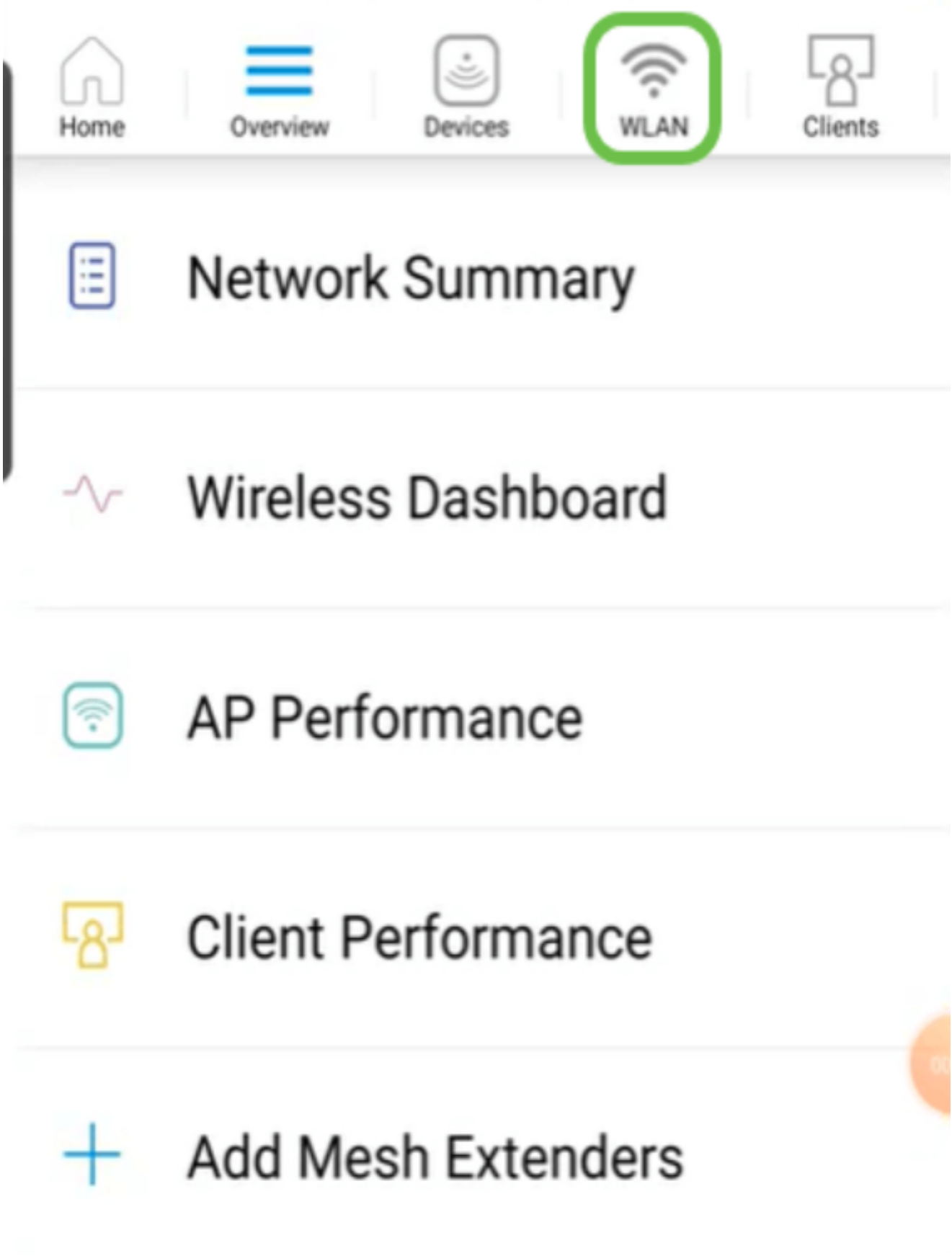
Creación de una WLAN de invitado mediante la aplicación móvil

Paso 1

Conéctese a la red inalámbrica empresarial de Cisco desde su dispositivo móvil. Inicie sesión en la aplicación.

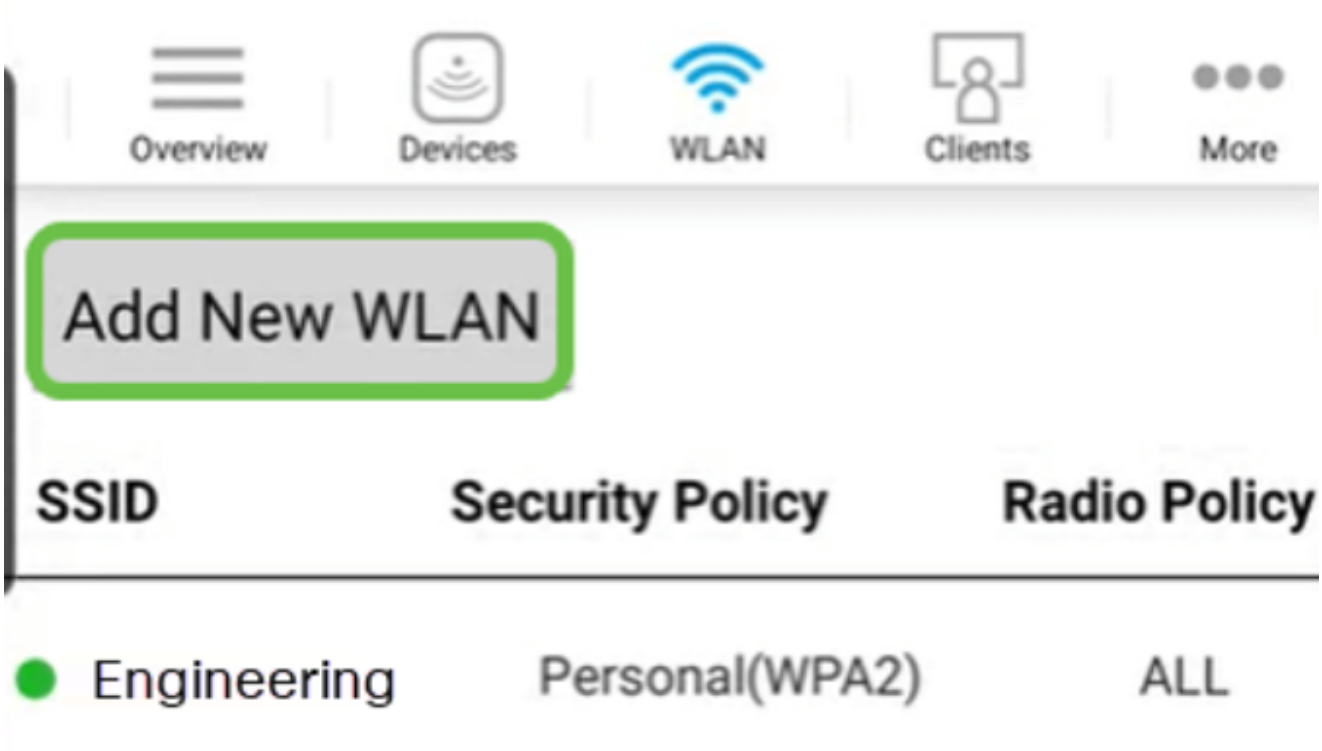
Paso 2

Haga clic en el icono WLAN en la parte superior de la página.



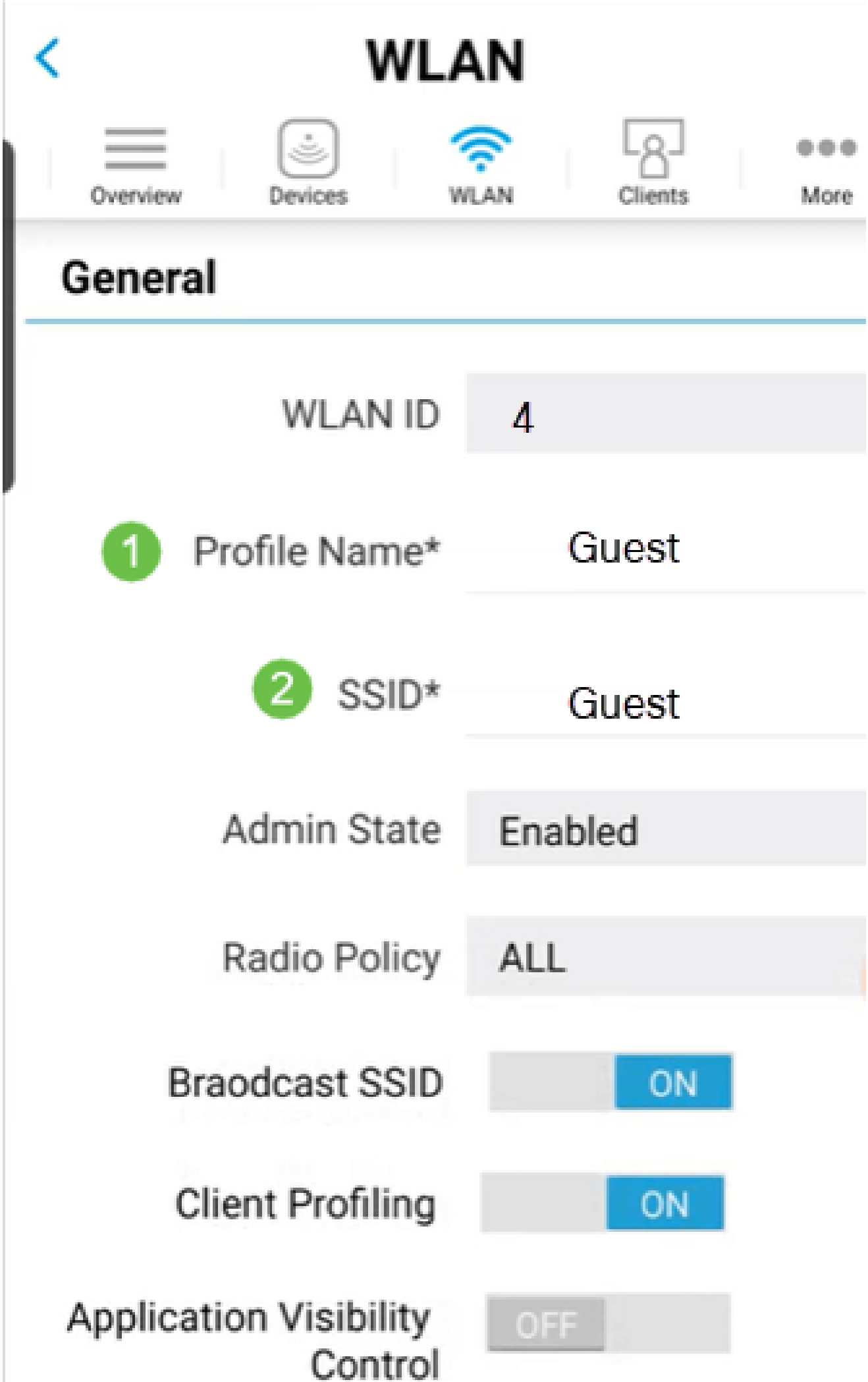
Paso 3

Se abre la pantalla Add New WLAN. Verá cualquier WLAN existente. Seleccione Add New WLAN.



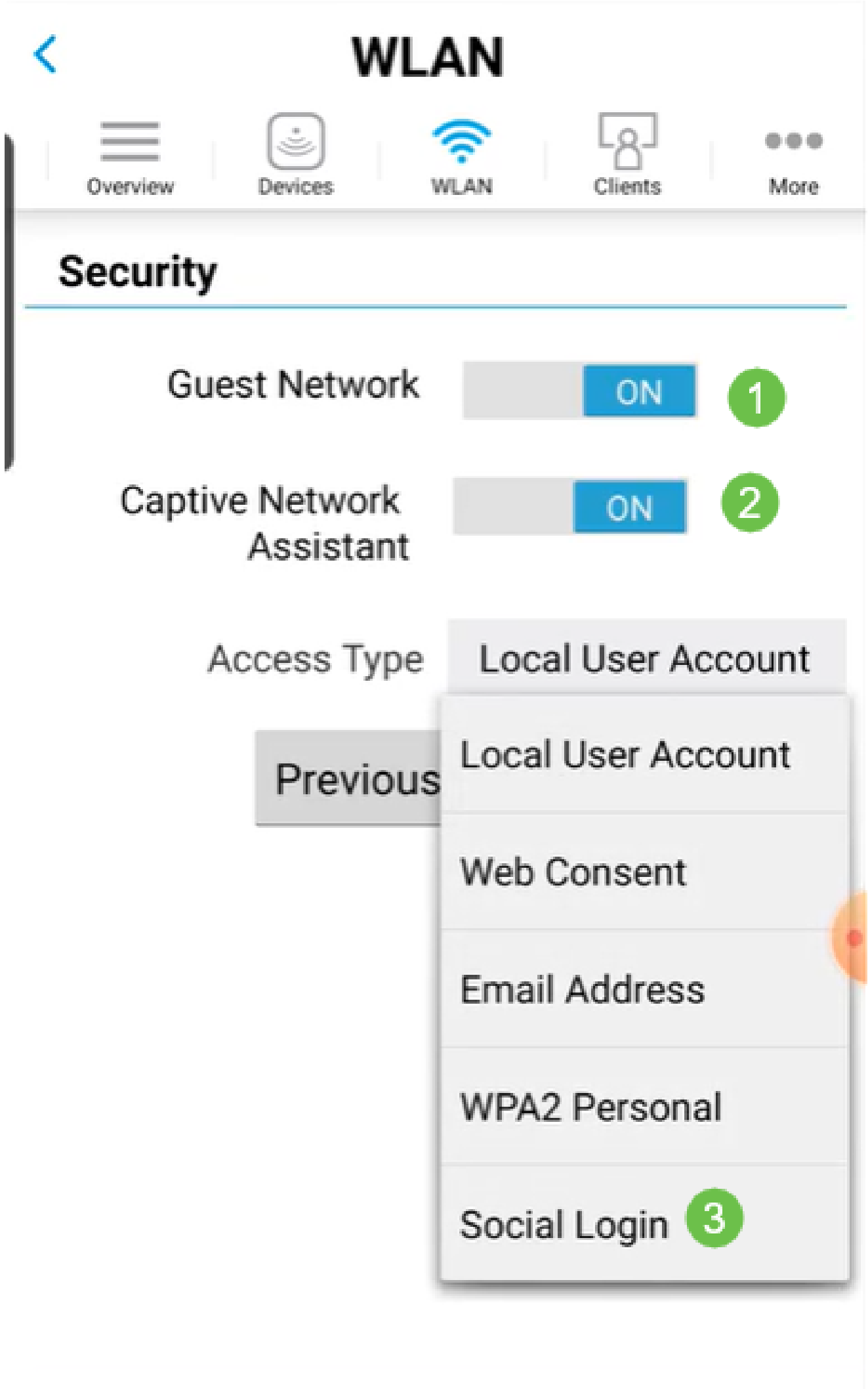
Paso 4

Introduzca un nombre de perfil y SSID. Rellene el resto de los campos o déjelos con la configuración predeterminada. Haga clic en Next (Siguiente).


WLAN
Overview
Devices
WLAN
Clients
More
General
WLAN ID
4
1
Profile Name*
Guest
2
SSID*
Guest
Admin State
Enabled
Radio Policy
ALL
Braodcast SSID
ON
Client Profiling
ON
Application Visibility Control
OFF

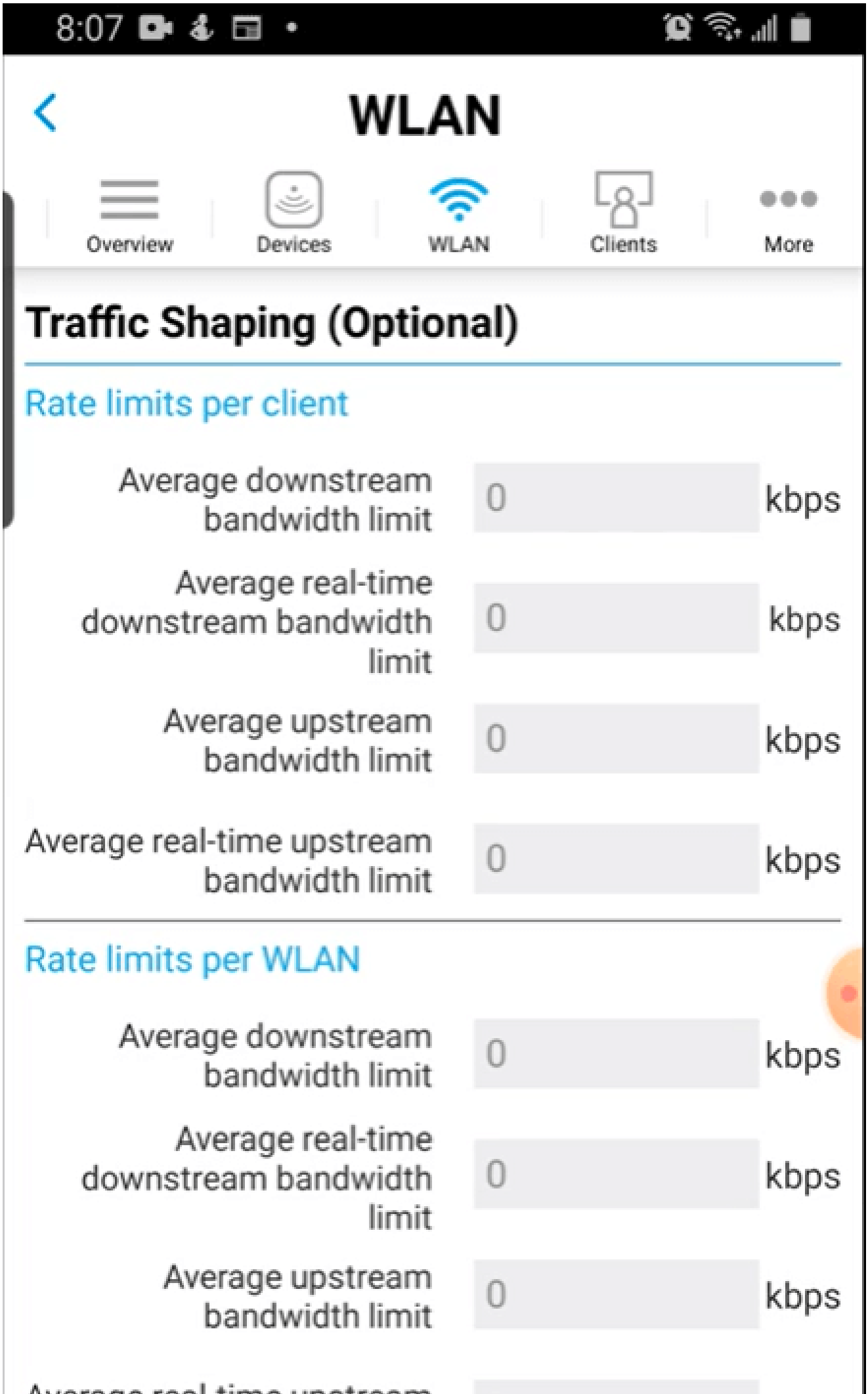
Paso 5

Active Red de invitado. En este ejemplo, Captive Network Assistant también está activado, pero es opcional. Tiene opciones para el tipo de acceso. En este caso, se selecciona Inicio de sesión social.


WLAN
Overview
Devices
WLAN
Clients
More
Security
Guest Network
ON
1
Captive Network Assistant
ON
2
Access Type
Local User Account
Previous
Local User Account
Web Consent
Email Address
WPA2 Personal
Social Login
3

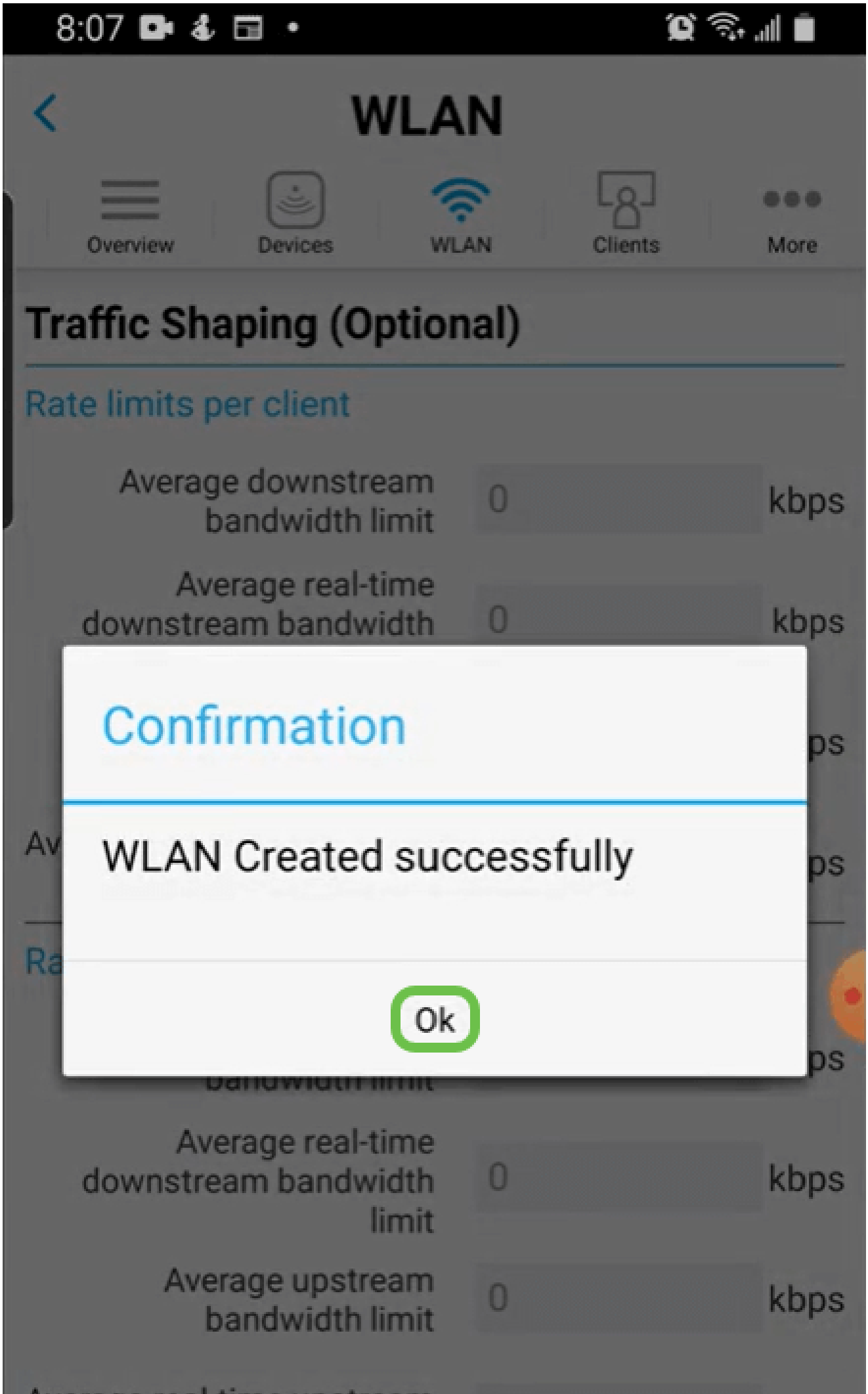
Paso 6

Esta pantalla ofrece las opciones para el modelado de tráfico (opcional). En este ejemplo, no se ha configurado ningún modelado de tráfico. Haga clic en Submit (Enviar).


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps
Average real-time upstream bandwidth limit
0
kbps
Rate limits per WLAN
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

Paso 7

Verá una ventana emergente de confirmación. Click OK.


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth
0
kbps
Confirmation
WLAN Created successfully
Ok
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

Paso 8

Guarde su configuración haciendo clic en la pestaña More y luego seleccione Save Configuration en el menú desplegable.

Conclusión

Ahora dispone de una configuración completa de la red. ¡Tómate un minuto para celebrar y luego ponte a trabajar!

Si desea agregar perfiles de aplicación o perfiles de cliente a la red de malla inalámbrica, deberá utilizar la interfaz de usuario (IU) web. Haga clic para configurar estas funciones.

Queremos lo mejor para nuestros clientes; si tiene comentarios o sugerencias sobre este tema, envíe un correo electrónico al equipo de contenido de Cisco.

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

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).