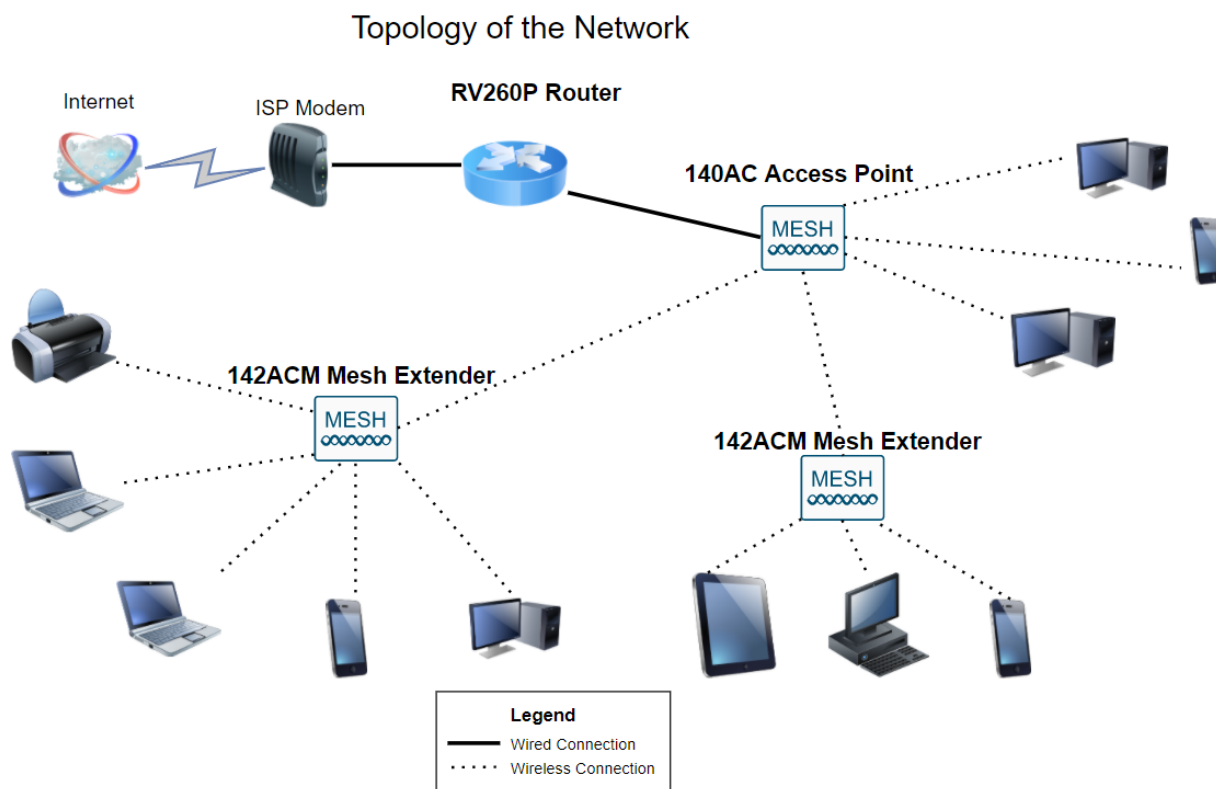


Configuración de red total: RV260P con CBW y la aplicación Cisco Business Mobile

Objetivo:

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

Topología:



Introducción

Aquí está, listo para configurar su nueva red. ¡Es un día emocionante! En esta situación, estamos utilizando un router RV260P. Este router proporciona alimentación a través de Ethernet (PoE), lo que le permite conectar un Cisco Business Wireless (CBW) 140AC al router en lugar de un switch. El punto de acceso CBW140AC y los extensores de malla CBW142ACM se utilizarán para crear una red de malla inalámbrica.

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

- [Bienvenido a Cisco Business Wireless Mesh Networking](#)

- [Preguntas frecuentes \(FAQ\) sobre una red inalámbrica empresarial de Cisco](#)

La aplicación móvil se recomienda como la forma más sencilla de establecer configuraciones básicas en CBW; sin embargo, no todas las funciones se pueden configurar en la aplicación. Si es nuevo en la aplicación Cisco Business Wireless, consulte los siguientes artículos:

- [Familiarícese con la aplicación Cisco Business CB-Wireless-Mesh](#)
- [Cisco Business Wireless: Aplicaciones de CBW vs Funciones de interfaz de usuario web](#)

Si prefiere utilizar la interfaz de usuario web al configurar la red inalámbrica de malla, haga clic para ver la versión que [sólo utiliza la interfaz de usuario web](#).

¿Estás listo? ¡Vamos a ello!

Dispositivos aplicables | Versión de software

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

Table Of Contents

- [Configuración del router RV260P](#)
- [Configuración del CBW140AC](#)
- [Configurar los ampliadores de malla CBW142ACM](#)

Antes de empezar

1. Asegúrese de que dispone de una conexión a Internet actual para la configuración.
2. Póngase en contacto con el ISP para obtener información sobre las instrucciones especiales que tenga al utilizar el router RV260. Algunos ISP ofrecen puertas de enlace con routers integrados. Si dispone de una puerta de enlace con un router integrado, es posible que tenga que desactivar el router y pasar la dirección IP de la red de área extensa (WAN) (la dirección de protocolo de Internet única que el proveedor de Internet asigna a su cuenta) y todo el tráfico de red a través del nuevo router.
3. Decida dónde colocar el router. Si es posible, querrá un área abierta. Esto puede no ser fácil porque debe conectar el router al gateway de banda ancha (módem) desde el ISP.

Configuración del router RV260P

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

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

RV260P fuera de la caja

Paso 1

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

Paso 2

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

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

Paso 3

Asegúrese de que el módem también está apagado.

Paso 4

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

Paso 5

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

Configuración del router

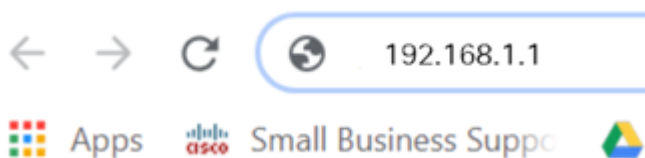
El trabajo preparatorio se ha realizado, ahora es el momento de realizar algunas configuraciones. Para iniciar la interfaz de usuario Web, siga estos pasos:

Paso 1

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

Paso 2

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



Paso 3

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



Your connection is not private

Attackers might be trying to steal your information from [ciscobusiness.cisco](#) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety

Paso 4

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



Router

1

2

English ▾

3

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Paso 5

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

Resolución de problemas de la conexión a Internet

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

En el sistema operativo Windows conectado, puede probar la conexión de red abriendo el símbolo del sistema. Introduzca ping 192.168.1.1 (la dirección IP predeterminada del router). Si se agota el tiempo de espera de la solicitud, no podrá comunicarse con el router. Si recibe una respuesta, tiene conectividad y puede pasar a la sección [Configuración inicial](#) de este artículo.

Si no se produce la conectividad, puede desproteger [la resolución de problemas en los routers RV160 y RV260](#).

Otras cosas que se deben intentar:

1. Compruebe que el explorador Web no está configurado en Trabajar sin conexión.
2. Compruebe los parámetros de conexión de red de área local del adaptador Ethernet. El PC debe obtener una dirección IP a través de DHCP. Alternativamente, el PC puede tener una dirección IP estática en el rango 192.168.1.x con el gateway predeterminado establecido en 192.168.1.1 (la dirección IP predeterminada del RV260P). Para conectarse, es posible que deba modificar los parámetros de red del RV260P. Si utiliza Windows 10, consulte [las instrucciones de Windows 10 para modificar los parámetros de red del RV260P](#).

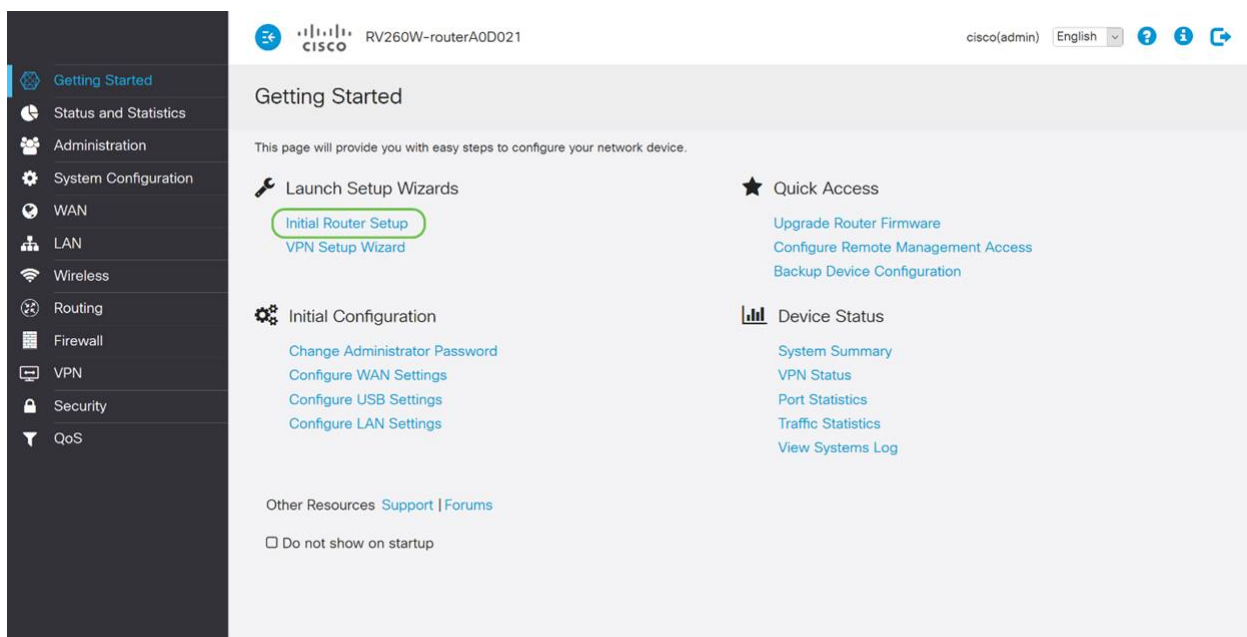
3. Si tiene equipos existentes ocupando la dirección IP 192.168.1.1, necesitará resolver este conflicto para que la red funcione. Más sobre esto al final de esta sección, o [haga clic aquí para tomarlo directamente](#).
4. Reinicie el módem y el RV260P apagando ambos dispositivos. A continuación, encienda el módem y déjelo inactivo durante unos 2 minutos. A continuación, encienda el RV260P. Ahora debe recibir una dirección IP de WAN.
5. Si tiene un módem DSL, pida al ISP que ponga el módem DSL en modo de puente.

Configuración inicial

Le recomendamos que siga los pasos del Asistente de configuración inicial que se enumeran en esta sección. Puede cambiar estos parámetros en cualquier momento. Si hay artículos para una configuración específica, se mostrarán al final del paso.

Paso 1

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



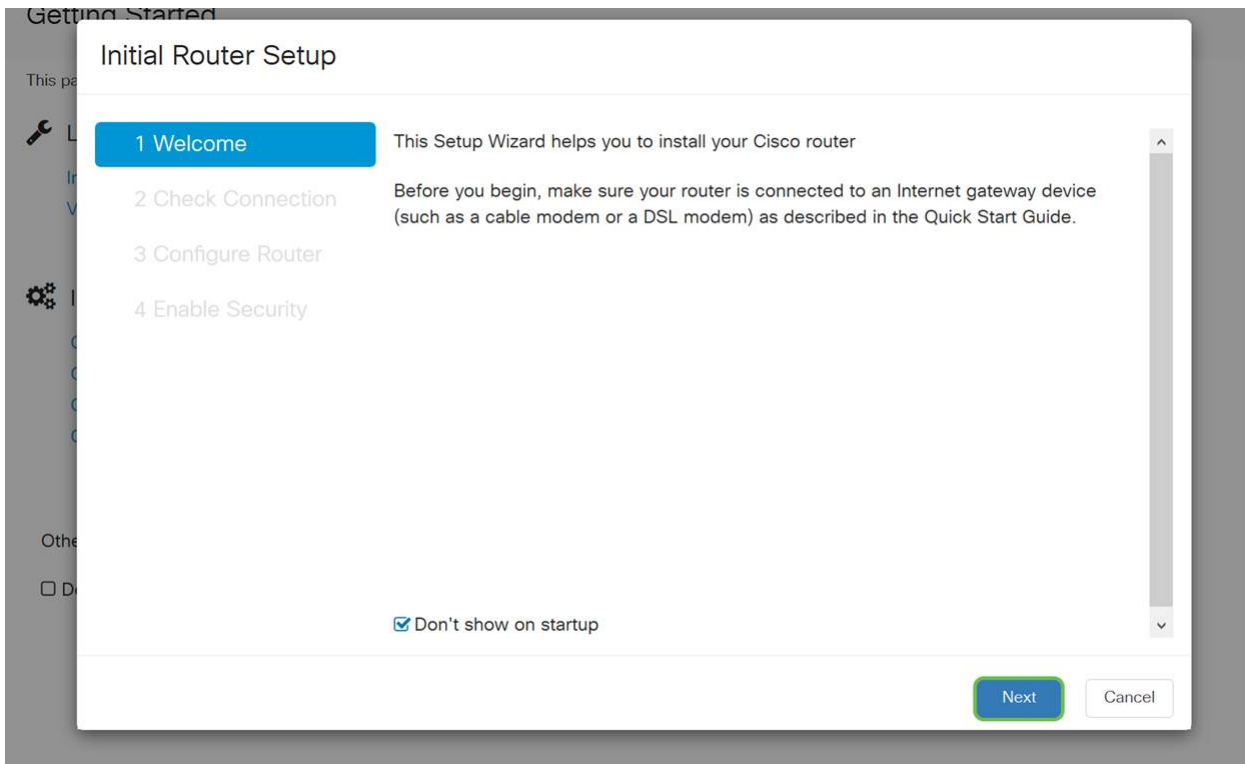
The screenshot shows the Cisco RV260W router configuration interface. The top navigation bar includes the Cisco logo, the device ID 'RV260W-routerA0D021', and the user 'cisco(admin)' with a language dropdown set to 'English'. The left sidebar contains a menu with options: Getting Started (selected), Status and Statistics, Administration, System Configuration, WAN, LAN, Wireless, Routing, Firewall, VPN, Security, and QoS. The main content area is titled 'Getting Started' and contains the following sections:

- Launch Setup Wizards:** Includes 'Initial Router Setup' (highlighted with a green circle) and 'VPN Setup Wizard'.
- Initial Configuration:** Includes links for 'Change Administrator Password', 'Configure WAN Settings', 'Configure USB Settings', and 'Configure LAN Settings'.
- Quick Access:** Includes links for 'Upgrade Router Firmware', 'Configure Remote Management Access', and 'Backup Device Configuration'.
- Device Status:** Includes links for 'System Summary', 'VPN Status', 'Port Statistics', 'Traffic Statistics', and 'View Systems Log'.

At the bottom, there are links for 'Other Resources Support | Forums' and a checkbox labeled 'Do not show on startup'.

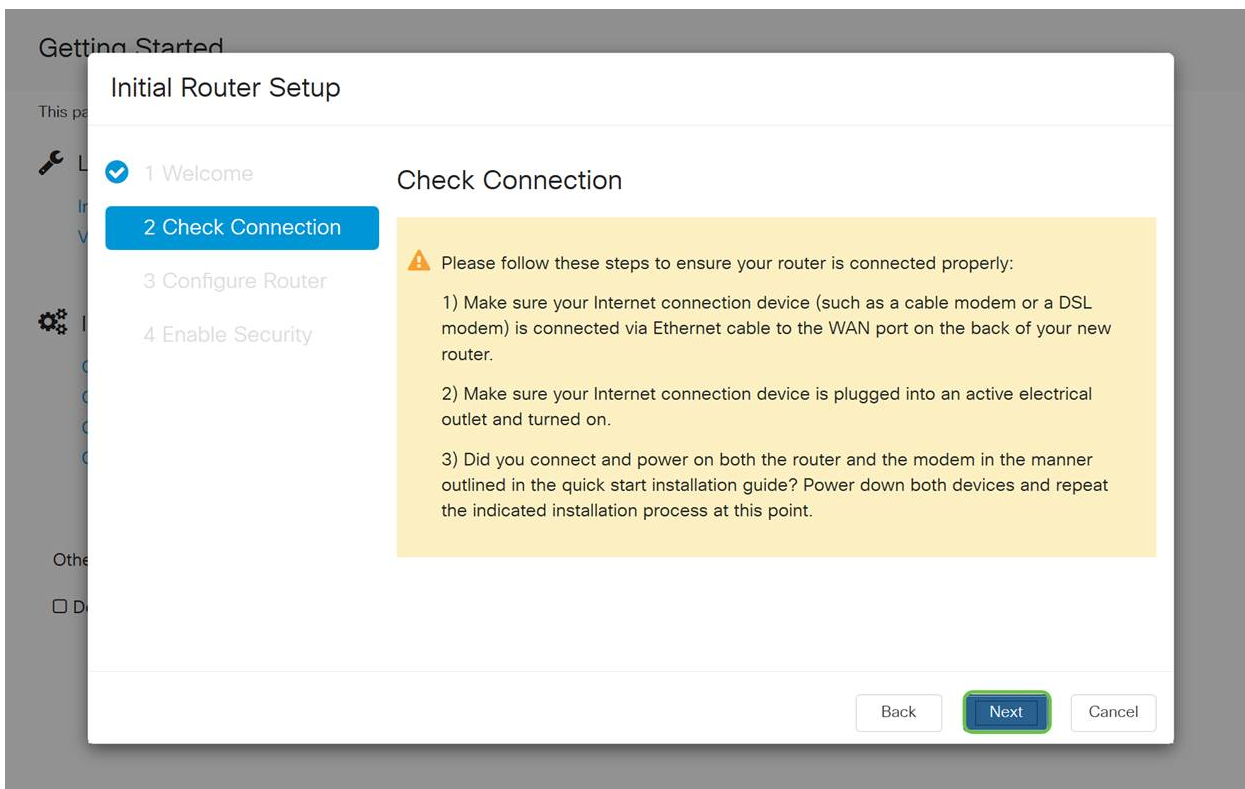
Paso 2

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



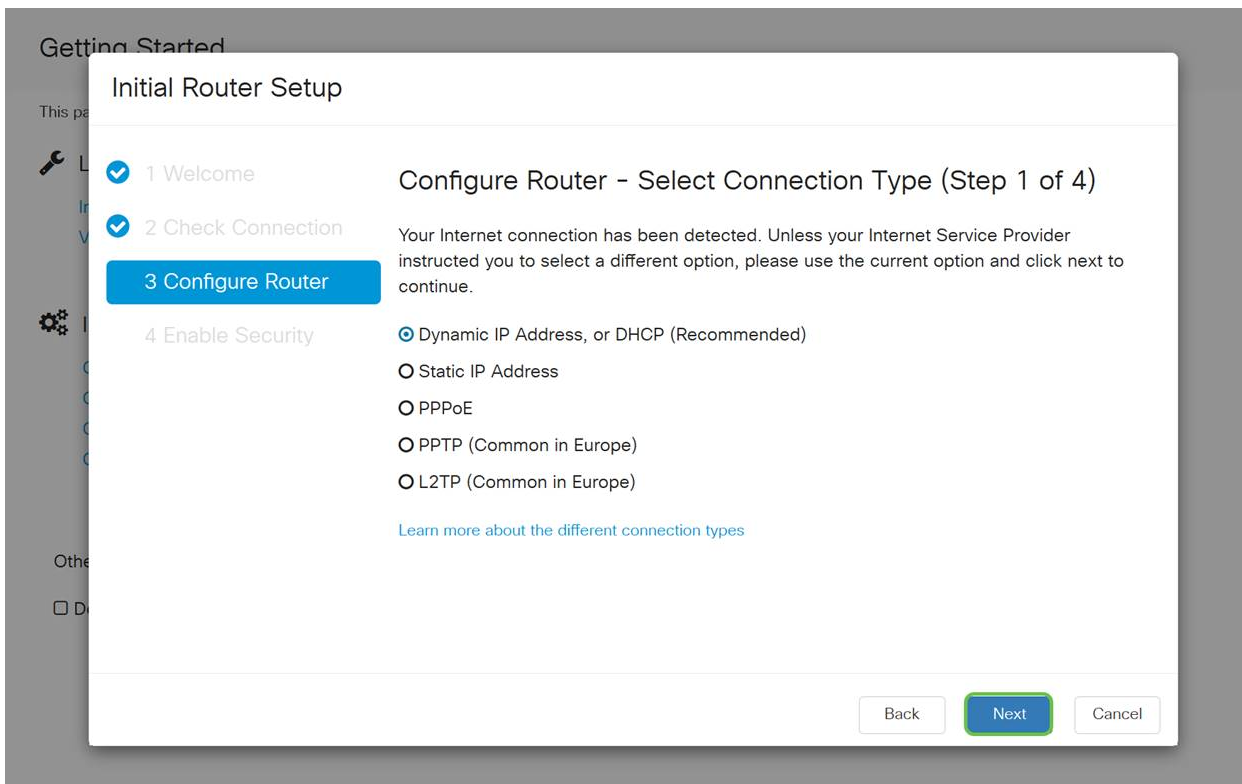
Paso 3

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



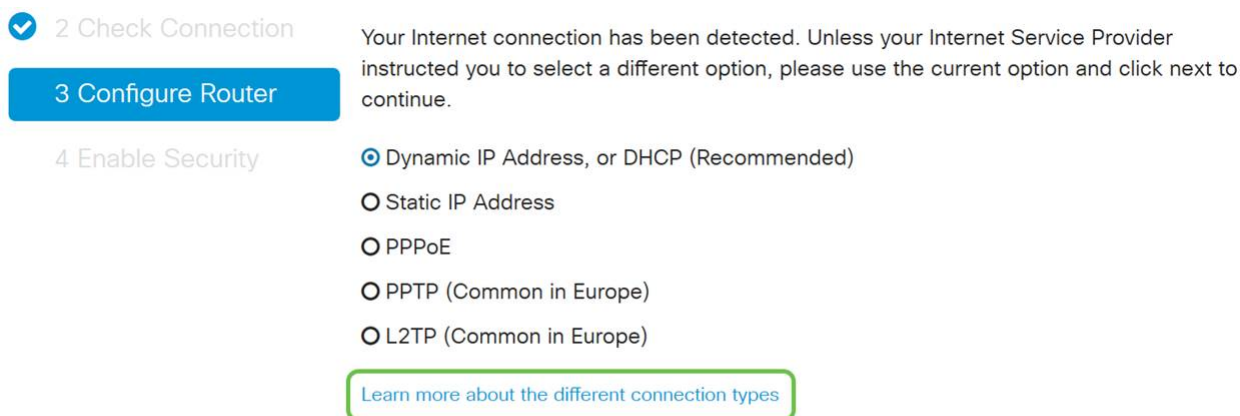
Paso 4

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



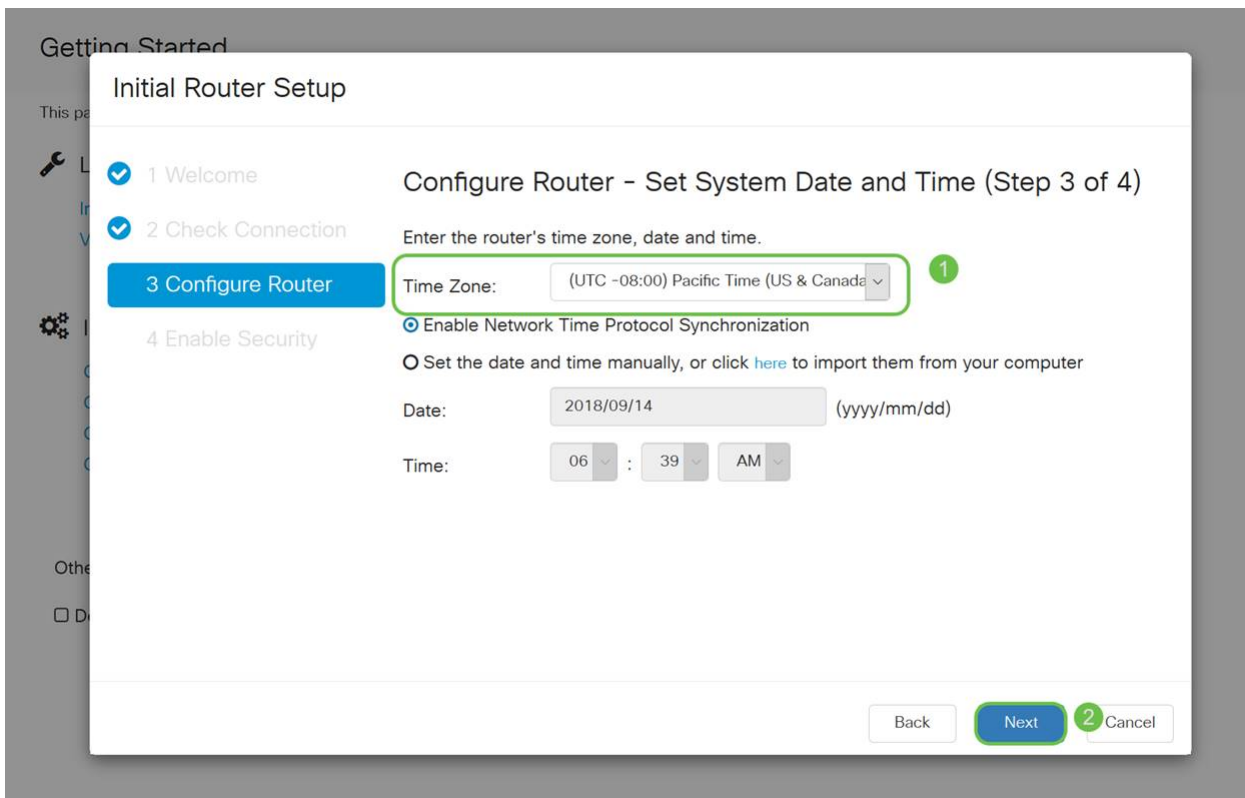
Aunque debe utilizar DHCP para esta configuración inicial, puede seleccionar para **obtener más información sobre los diferentes tipos de conexión** hacia la parte inferior de la pantalla y la referencia futura. Para obtener más información al respecto, consulte:

- [Configuración de WAN en dispositivos RV160x y RV260x](#)
- [Configuración del Ruteo Estático en RV160 y RV260](#)



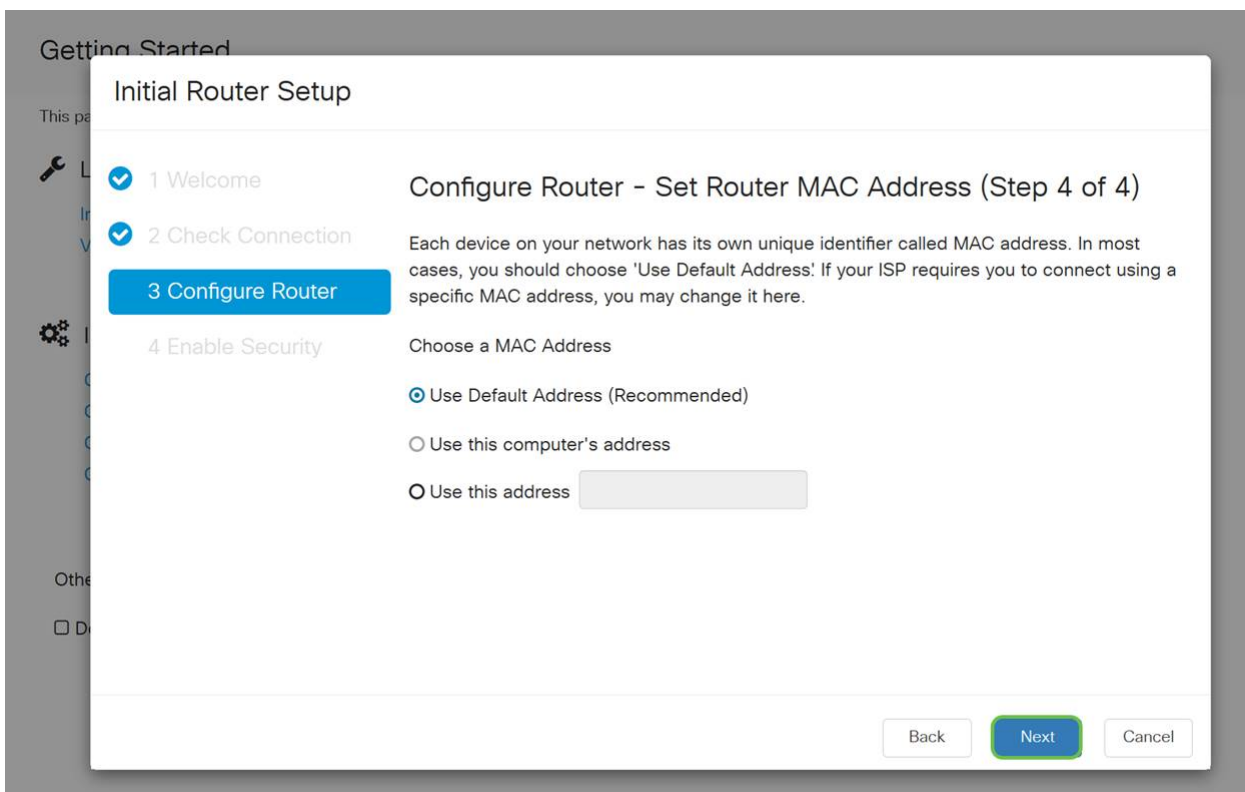
Paso 5

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



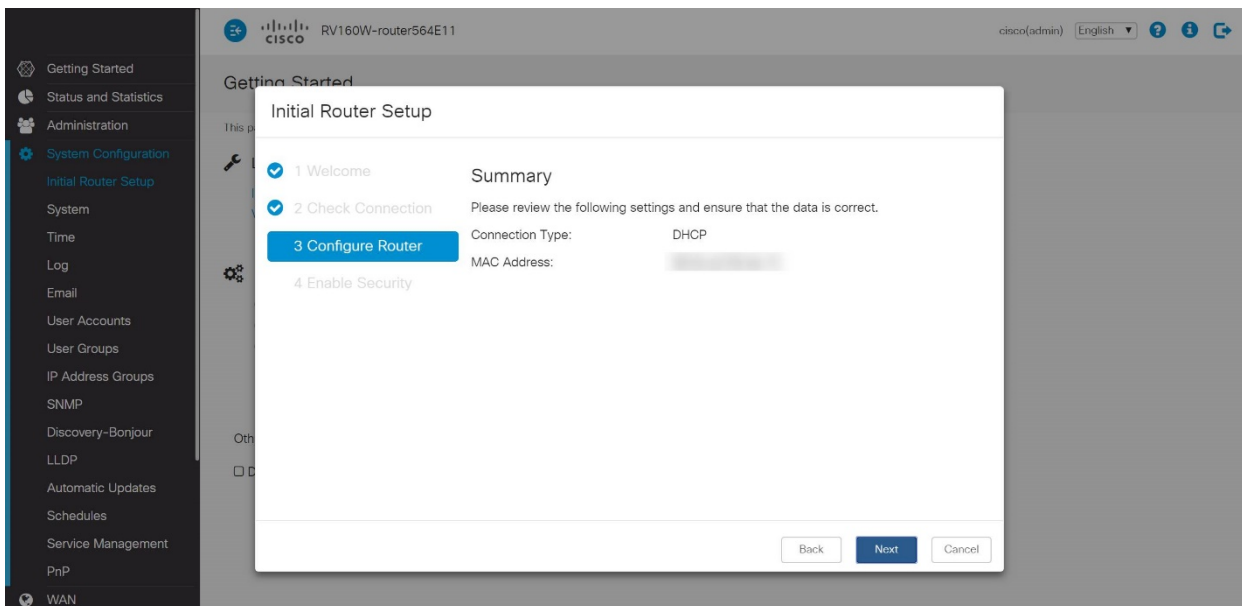
Paso 6

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



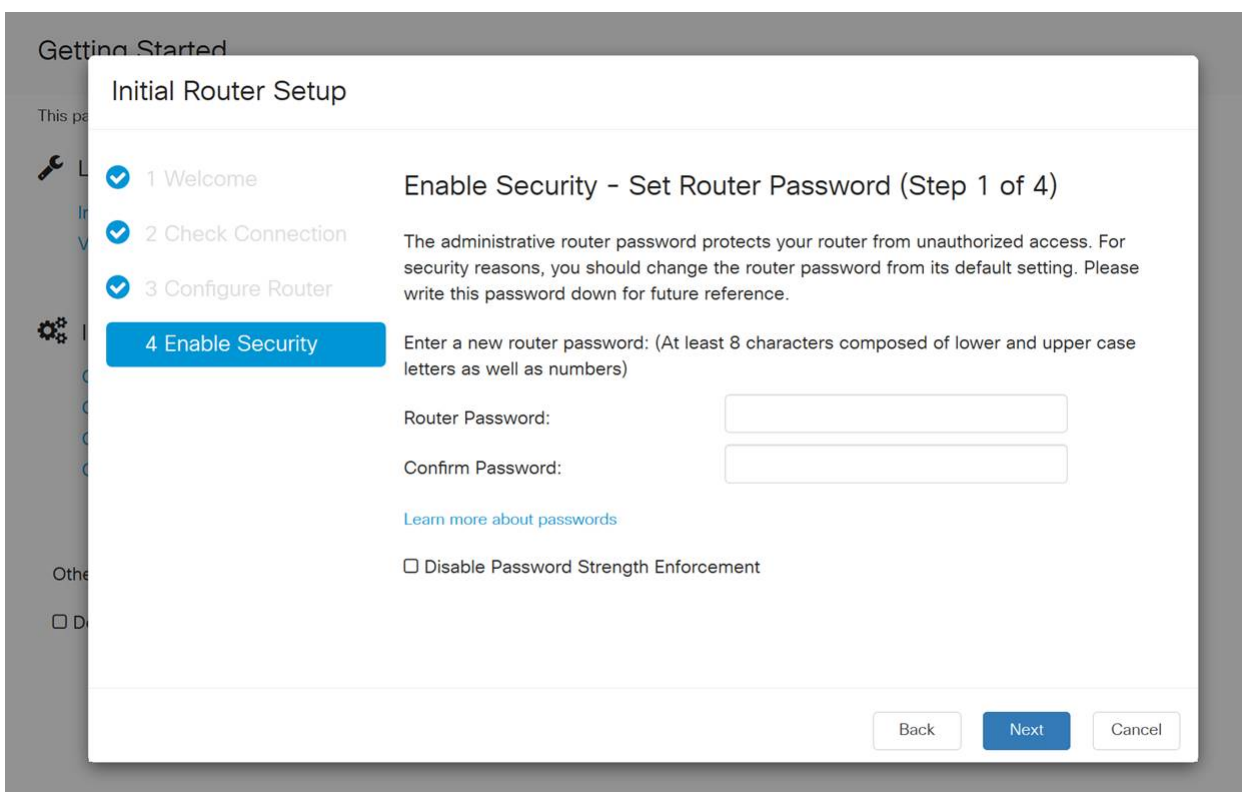
Paso 7

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



Paso 8

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



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

Paso 9

Haga clic en el icono **Guardar**.

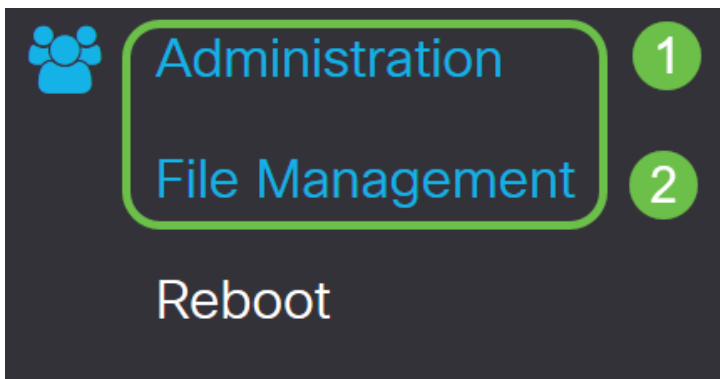


Actualización del firmware si es necesario

Esto es importante, ¡no lo omita!

Paso 1

Elija **Administration > File Management**.



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

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

File Management

System Information


Device Model:	RV260P
PID VID:	RV260P-K9 V01
Current Firmware Version:	1.0.00.15
Latest Version Available on Cisco.com:	-
Firmware Last Updated:	2019-Apr-17, 18:28:12

Paso 2

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

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Firmware Image Format: *.img (Maximum size: 100MB)

No file is selected

Reset all configurations/settings to factory defaults


The device will be automatically rebooted after the upgrade is complete.

Paso 3

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

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Reset all configurations/settings to factory defaults

The device will be automatically rebooted after the upgrade is complete.

Paso 4

Haga clic en **Upgrade**.

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Reset all configurations/settings to factory defaults

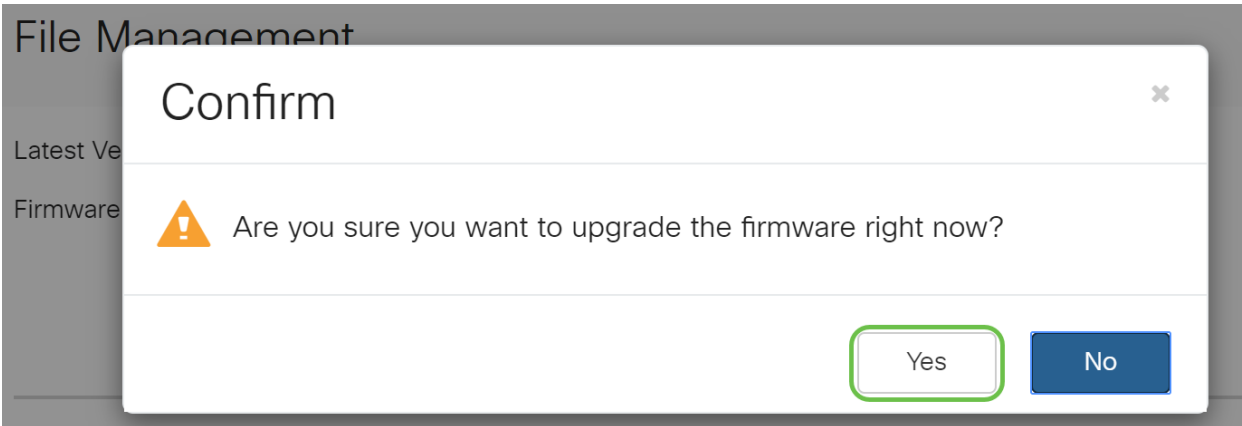
Upgrade

The device will be automatically rebooted after the upgrade is complete.

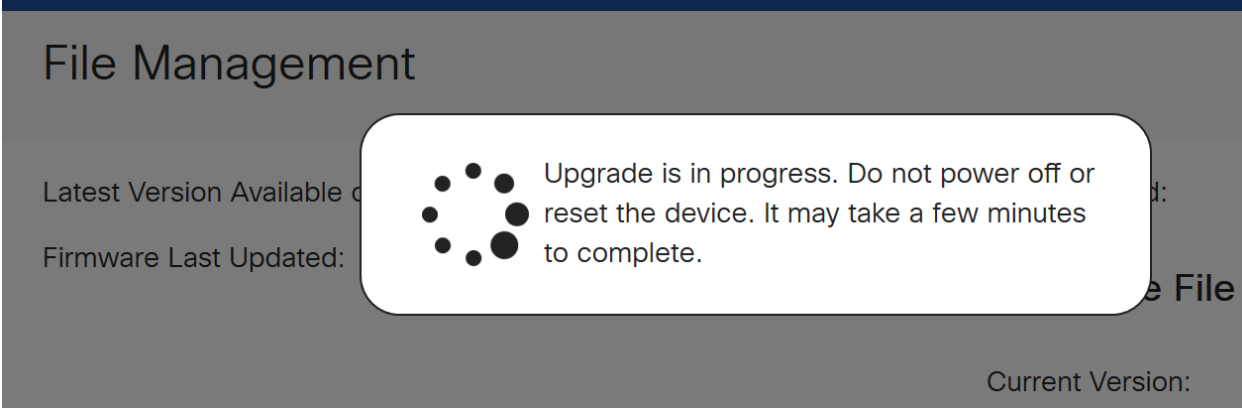
Download to USB

Paso 5

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



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



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

File Management

Latest Version Available

Firmware Last Updated



Restarting

Please wait for 176 seconds...

Paso 6

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

File Management

System Information

Device Model:	RV260P
PID VID:	RV260P-K9 V01
Current Firmware Version:	1.0.00.15
Latest Version Available on Cisco.com:	-
Firmware Last Updated:	2019-Apr-17, 18:28:12

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

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

- [Redes de área local virtuales \(VLAN\)](#)
- [Editar dirección IP](#)
- [Agregar direcciones IP estáticas](#)
- [Estoy preparado para configurar la parte de red inalámbrica de malla de mi red](#)

Configuración de VLAN (opcional)

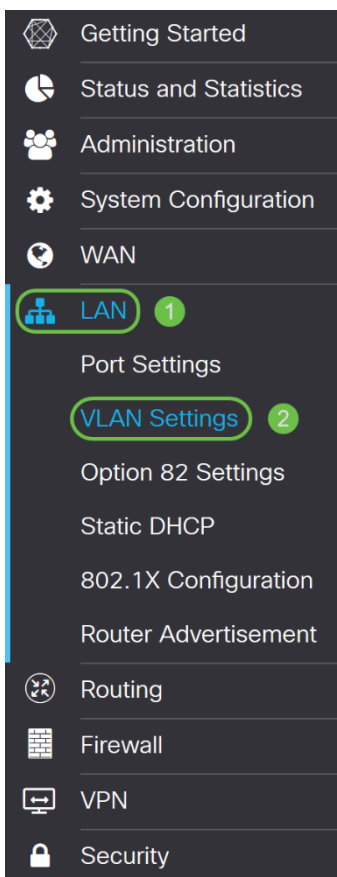
Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En los escenarios donde los datos

confidenciales se pueden difundir en una red, se pueden crear VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Las VLAN también se pueden utilizar para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusión a destinos innecesarios. Puede crear una VLAN, pero esto no tendrá efecto hasta que la VLAN esté conectada al menos a un puerto, ya sea manual o dinámicamente. Los puertos siempre deben pertenecer a una o más VLAN.

Si no desea crear VLAN, puede saltar a la [siguiente sección](#).

Paso 1

Vaya a **LAN > VLAN Settings**.



Paso 2

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

VLAN Settings

Create new VLANs



<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149

Paso 3

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

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

VLAN Settings

Create new VLANs



<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/>	200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

Paso 4

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

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

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

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

The screenshot shows the 'VLAN Settings' page for a Cisco RV160W-router564F71. Under 'Create new VLANs', there is a table with columns: VLAN ID, Name, Inter-VLAN Routing, Device Management, and IPv4 Address/Mask. The table lists two VLANs: 'Default' (VLAN 1) and 'Engineering' (VLAN 200). The 'Engineering' VLAN configuration is expanded, showing fields for IP Address (192.168.2.1 / 24), Subnet Mask (255.255.255.0), DHCP Type (Server), Lease Time (1440 min), Range Start (192.168.2.100), Range End (192.168.2.149), DNS Server (Use DNS Proxy), and WINS Server.

Paso 5

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

This screenshot is similar to the previous one, but the 'Inter-VLAN Routing' and 'Device Management' checkboxes for the 'Engineering' VLAN are now unchecked. The 'IP Address' field in the expanded configuration for VLAN 200 is highlighted with a green box, showing the value '192.168.2.1 / 24'.

Paso 6

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

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

VLAN Settings

Create new VLANs



VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	
<input type="checkbox"/>	1	Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/>	200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

Paso 7

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

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

Servidor: esta es la opción más utilizada.

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

VLAN Settings

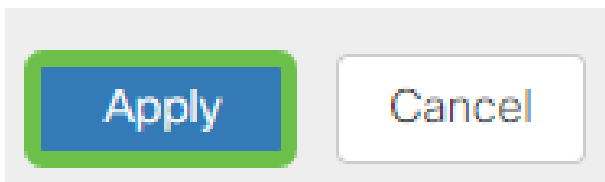
Create new VLANs



VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	
<input type="checkbox"/>	1	Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149

Paso 8

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



Asignar VLAN a puertos

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

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

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

Una VLAN asignó su propio puerto:

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

Dos o más VLAN que comparten un puerto:

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

Nota: En este ejemplo, no hay trunks.

Paso 9

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

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

Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

Paso 10

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

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

Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

Paso 11

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

Apply Cancel

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

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

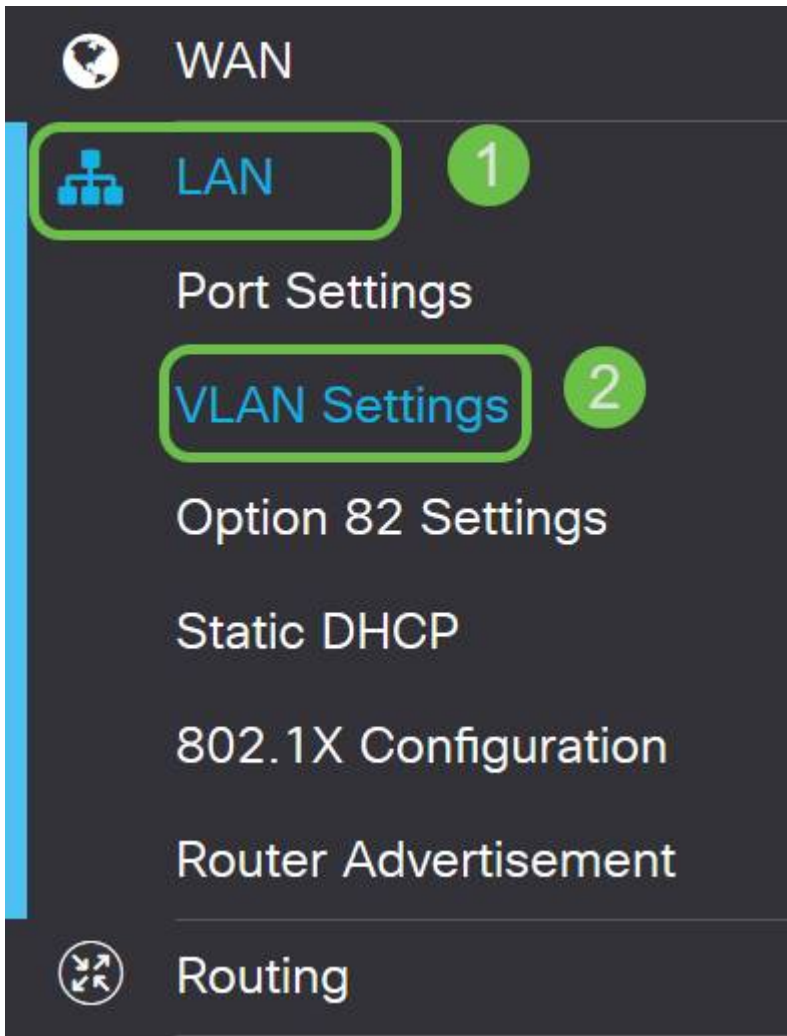
Editar una dirección IP (opcional)

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

Si no necesita editar una dirección IP, puede pasar a la [siguiente sección](#) de este artículo.

Paso 1

En la barra de menús izquierda, haga clic en el botón **LAN** y luego haga clic en **VLAN Settings**.



Paso 2

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



Paso 3

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

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
1	Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IP Address: 192.168.1.1/24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input type="radio"/> Server <input checked="" type="radio"/> Relay	Prefix: <input checked="" type="radio"/> fec0: <input type="radio"/> Prefix from DHCP-PD Prefix Length: 64 Preview: [fec0::1] Interface Identifier: <input type="radio"/> EUI-64 <input checked="" type="radio"/> 1 DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server

Paso 4 (opcional)

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

DHCP Type: Disabled
 Server
 Relay

Prefix Length: 64
 Preview: [fec0::1]
 Interface Identifier: EUI-64
 1
 DHCP Type: Disabled
 Server

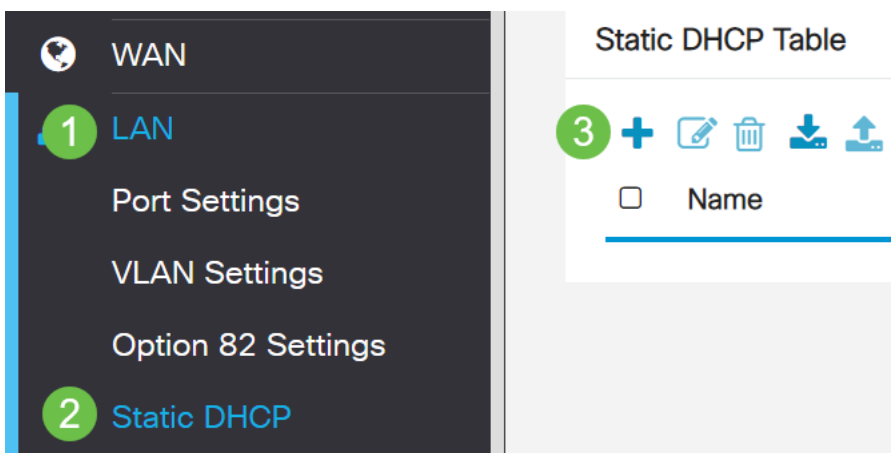
Agregar una IP estática (opcional)

Si desea que un dispositivo determinado sea accesible a otras VLAN, puede darle una dirección IP estática a ese dispositivo y crear una regla de acceso para que sea accesible. Esto sólo funciona si se habilita el ruteo entre VLAN.

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

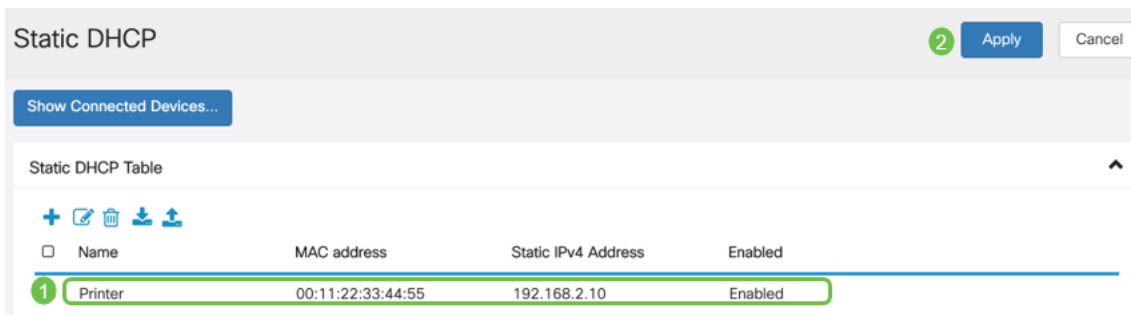
Paso 1

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



Paso 2

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



Si necesita más información sobre la configuración de direcciones IP estáticas, consulte [Prácticas Recomendadas para Establecer Direcciones IP Estáticas en Cisco Business Hardware](#).

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

Configuración del CBW140AC

CBW140AC fuera de la caja

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

Compruebe el estado de las luces indicadoras. El punto de acceso tardará unos 10 minutos en iniciarse. La luz parpadeará en verde en varios patrones, alternando rápidamente entre verde, rojo y ámbar antes de volver a girar en verde. Puede haber pequeñas variaciones en la intensidad de color del LED y el color de la unidad a la unidad. Cuando la luz LED parpadee en verde, vaya al siguiente paso.

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

Si el punto de acceso no es nuevo, asegúrese de que se restablece a los parámetros predeterminados de fábrica para que el SSID *CiscoBusiness-Setup* aparezca en las opciones Wi-Fi. Para obtener ayuda con esto, consulte [Cómo Reiniciar y Restablecer los Parámetros Predeterminados de Fábrica en Routers RV160 y RV260](#).

Configuración del punto de acceso inalámbrico para aplicaciones móviles 140AC

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

Tenga en cuenta que la aplicación tiene frecuentes actualizaciones y que el aspecto/diseño puede cambiar con el tiempo.

En la parte posterior del 140AC, enchufe el cable que viene con el AP en el conector

PoE amarillo de su 140 AC. Conecte el otro extremo a uno de los puertos RV260P LAN.

Si tiene problemas para conectarse, consulte la sección [Consejos para la resolución de problemas inalámbricos](#) de este artículo.

Paso 1

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

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

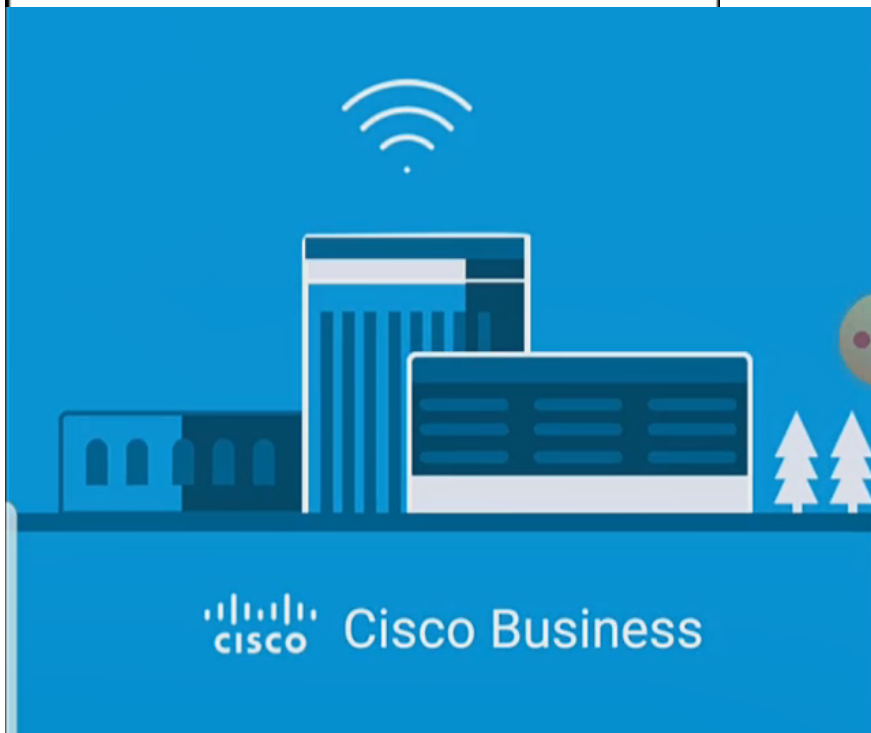
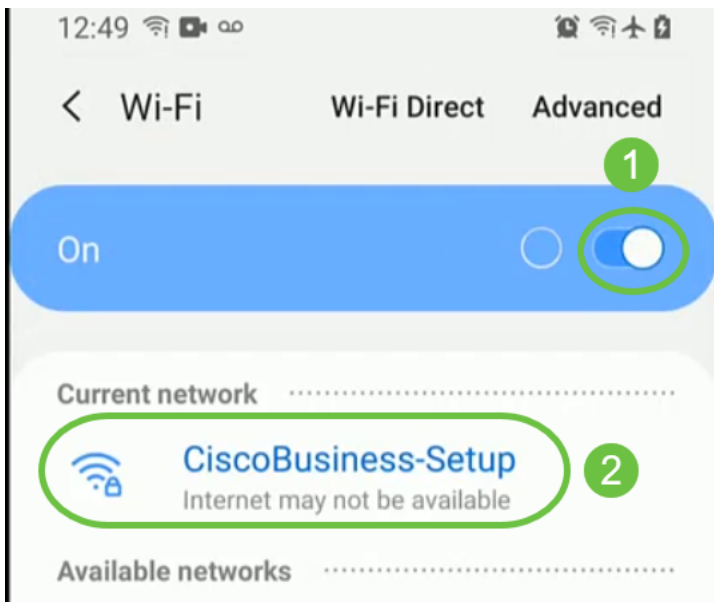
Paso 2

Abra la aplicación **Cisco Business Wireless** en su dispositivo móvil.



Paso 3

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



Paso 4

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



Monitor My Network



Set up My Network



Enter the name of the Primary AP / IP

Discovered Primary

Paso 5

Para configurar la red, introduzca lo siguiente:

- *Crear nombre de usuario de administrador*
- *Crear contraseña de administrador*
- *Confirme la contraseña de administrador volviendo a introducirla*
- (Opcional) Marque la casilla de verificación para *Mostrar contraseña*.

Seleccione **Introducción**.




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 en conflicto, puede dar lugar a un comportamiento impredecible.

- *Mobile Application AP Name* para su red inalámbrica.
- *País*
- *Fecha*
- *Hora*
- *Zona horaria*

< Cisco Business Wireless 140AC 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

Previous Next

Paso 7

Enciende la barra de *mall*a. Haga clic en Next (Siguiete).



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)



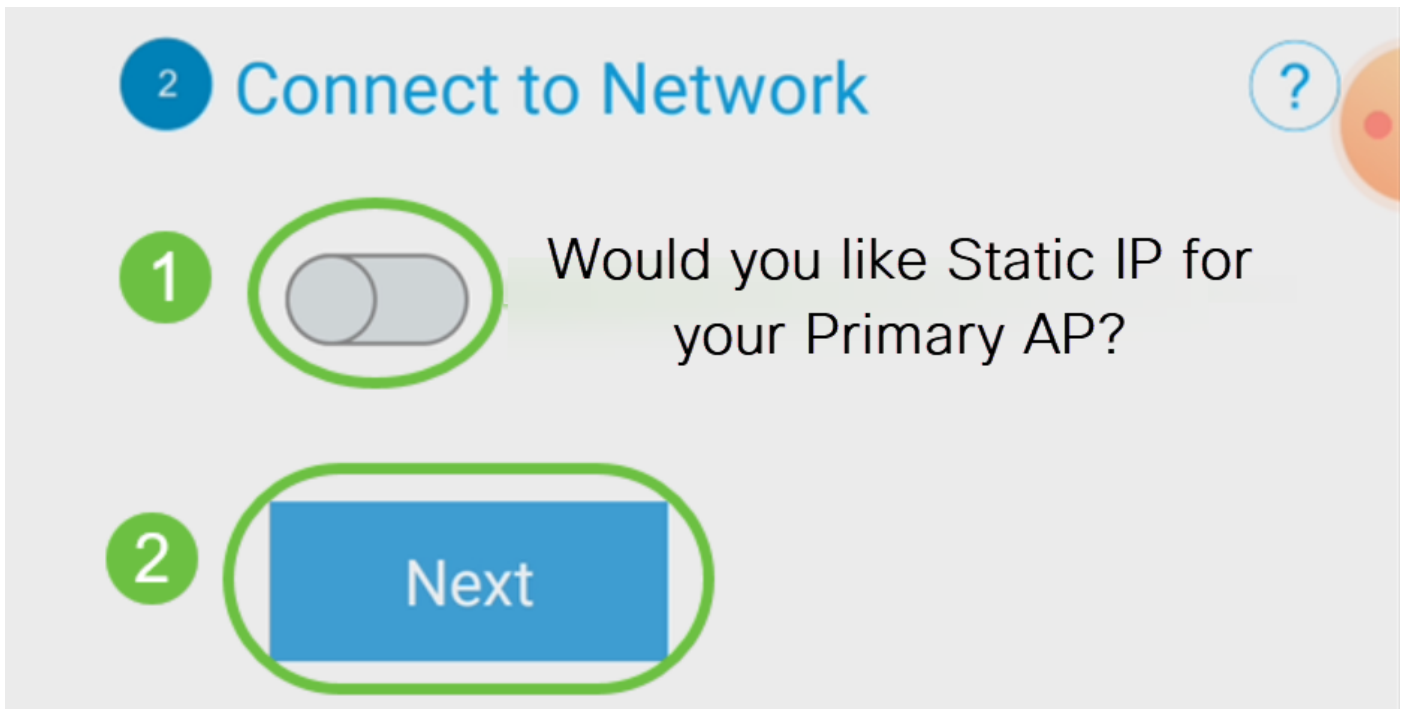
1



Mesh

Paso 8

(Opcional) Puede elegir habilitar *Static IP para su Mobile Application AP* para fines de administración. Si no es así, el servidor DHCP asignará una dirección IP. Si no desea configurar la IP estática para el punto de acceso, haga clic en **Siguiente**.



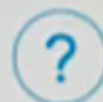
Alternativamente, para *conectarse a la red*:

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

- Introduzca la *dirección IP de administración*
- *Máscara de subnet*
- *Gateway predeterminado*

Click Save.

2 Connect to Network



Would you like Static IP for your Primary AP?

MANAGEMENT IP ADDRESS

0.0.0.0

2

SUBNET MASK

0.0.0.0

3

DEFAULT GATEWAY

0.0.0.0

4

Save

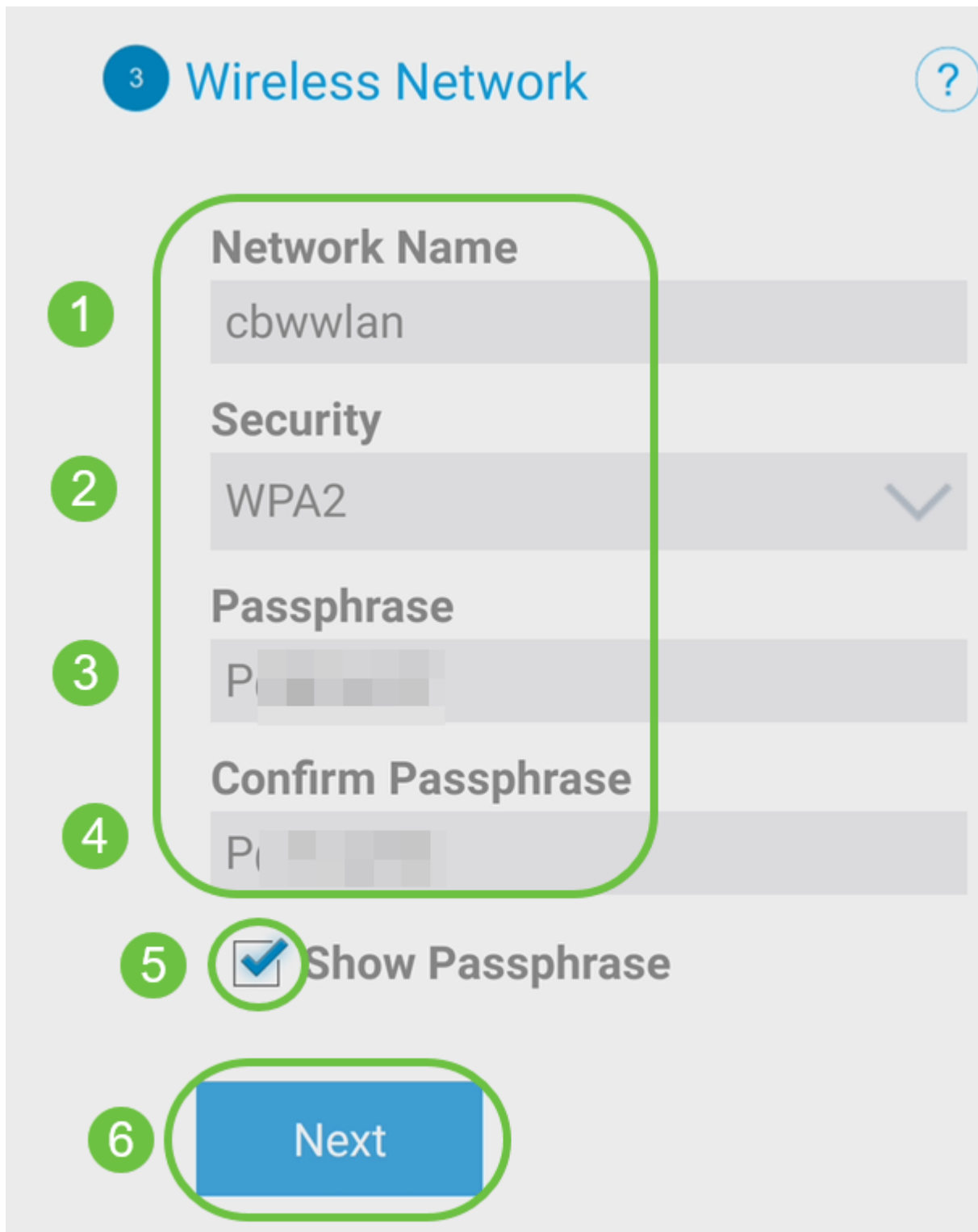
5

Paso 9

Configure la *red inalámbrica* introduciendo lo siguiente:

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

Haga clic en Next (Siguiente).



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

Paso 10

Para confirmar la configuración en la pantalla *Enviar al AP de la aplicación móvil*, haga clic en **Enviar**.



Cisco Business Wireless 140AC 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.

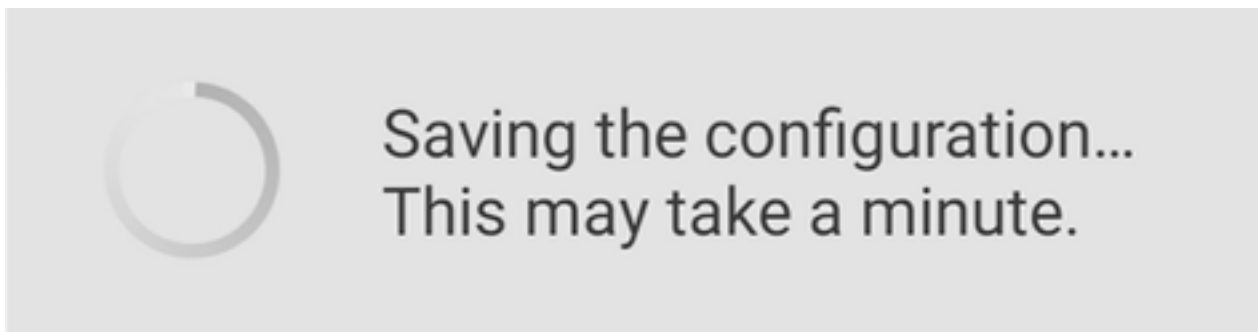
Note: After initial setup and reboot, the Primary AP needs to be connected to a DHCP server even if the management IP address was set to static (access point functionality and client connections use dynamically assigned

[Previous](#)

[Submit](#)

Paso 11

Espere a que se complete el reinicio.



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

Paso 12

Verá la siguiente pantalla *Confirmation*. Click OK.

Confirmation

The Primary AP has been fully configured and will restart in 6 minutes. After the Primary AP is restarted, it will be accessible from the network by going to this URL - <https://ciscobusiness.cisco> via browser or using Discovered Primary list in Cisco Business Mobile Application provided client should be connected to configured ' TestAP ' SSID.



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 la resolución de problemas inalámbricos

Si tiene algún problema, consulte los siguientes consejos:

- Asegúrese de que está seleccionado el identificador del conjunto de servicios (SSID) correcto. Este es el nombre que ha creado para la red inalámbrica.
- Desconecte cualquier VPN para la aplicación móvil o en un portátil. Es posible que incluso esté conectado a una VPN que su proveedor de servicios móviles utilice que puede que ni siquiera sepa. Por ejemplo, un teléfono Android (Pixel 3) con Google Fi

como proveedor de servicios, hay una VPN integrada que se conecta automáticamente sin notificación. Esto tendría que ser inhabilitado para encontrar el AP de la aplicación móvil.

- Inicie sesión en Mobile Application AP con `https://<IP address of the Mobile Application AP>`.
- Una vez que realice la configuración inicial, asegúrese de que `https://` se utiliza tanto si inicia sesión en `ciscobusiness.cisco` como si introduce la dirección IP en su navegador web. En función de la configuración, es posible que el ordenador se haya rellenado automáticamente con `http://` since que es lo que utilizó la primera vez que se conectó.
- Para ayudar con los 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*.

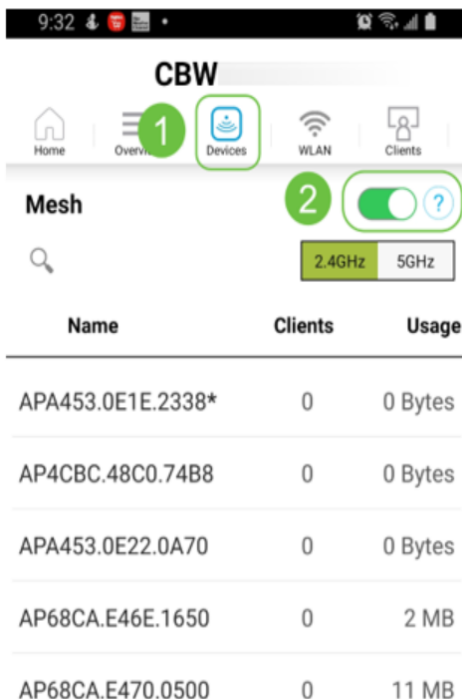
Configurar los ampliadores de malla CBW142ACM

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

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

Paso 1

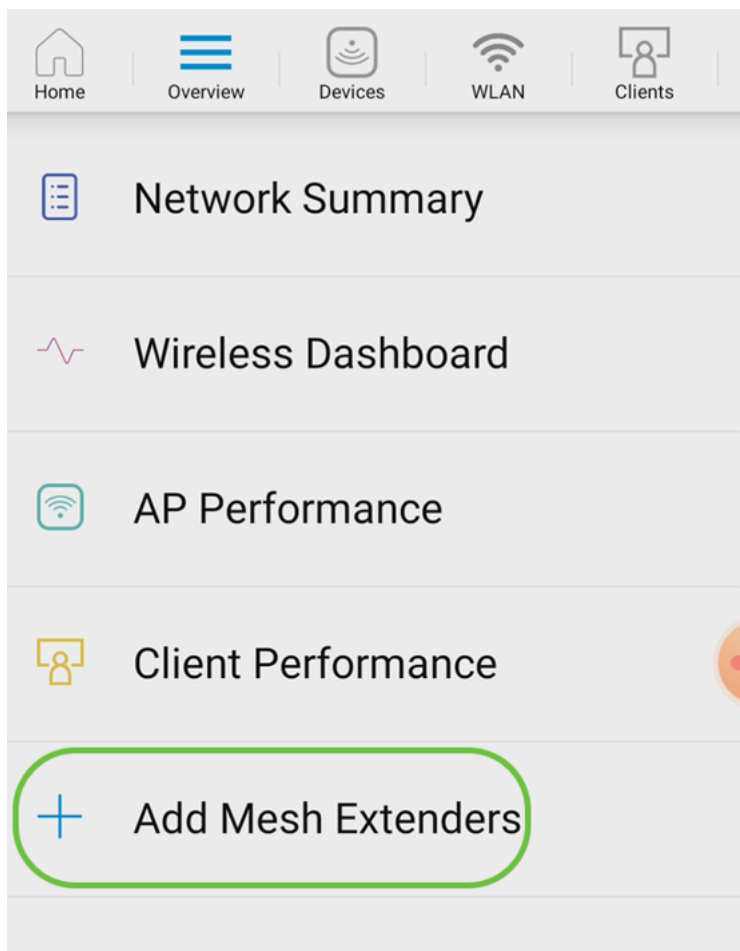
Vaya a **Dispositivos**. Verifique que *Mesh* esté habilitado.



Paso 2

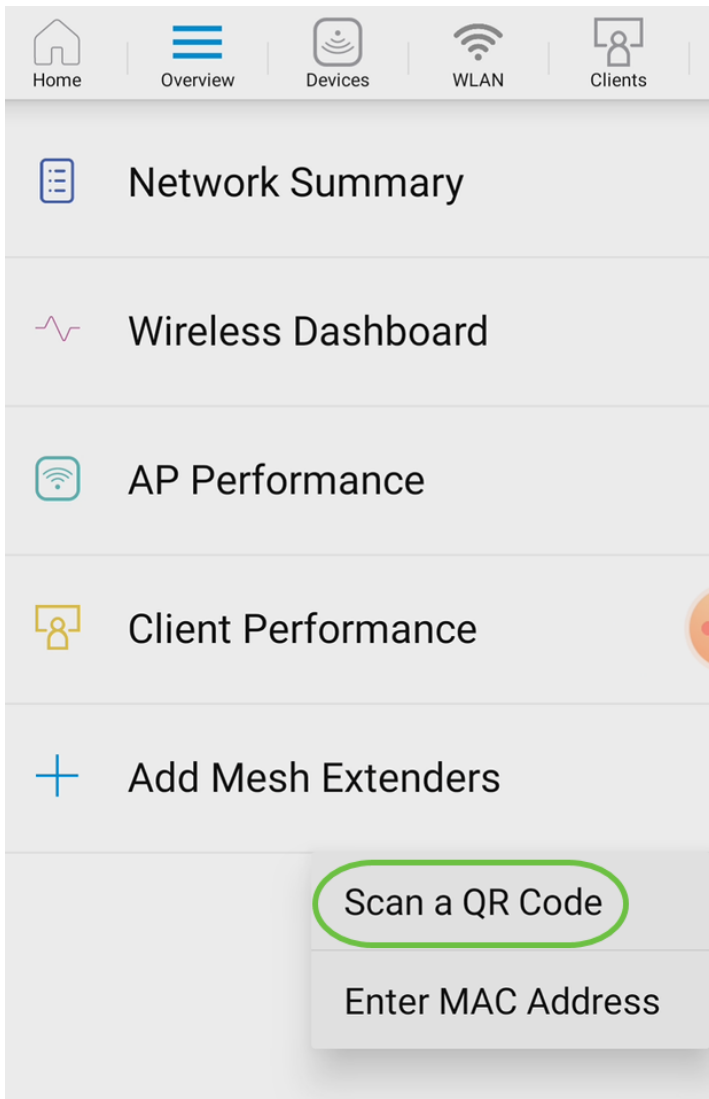
Debe ingresar la dirección MAC de todos los Extensores de malla que desea utilizar en la red de malla con el AP de aplicación móvil. Para agregar la dirección MAC, haga

clic en **Agregar extensores de malla** del menú.



Paso 3

Puede agregar la dirección MAC mediante el escaneo de un código QR o introduciendo manualmente la dirección MAC. En este ejemplo, se selecciona **Escanear un código QR**.

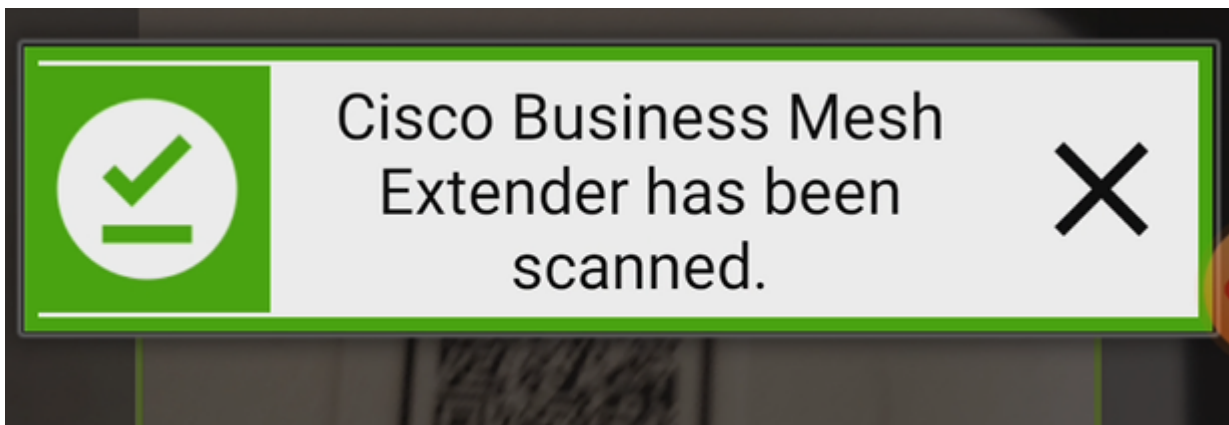


Paso 4

Aparecerá un lector de código QR para analizar el código QR.

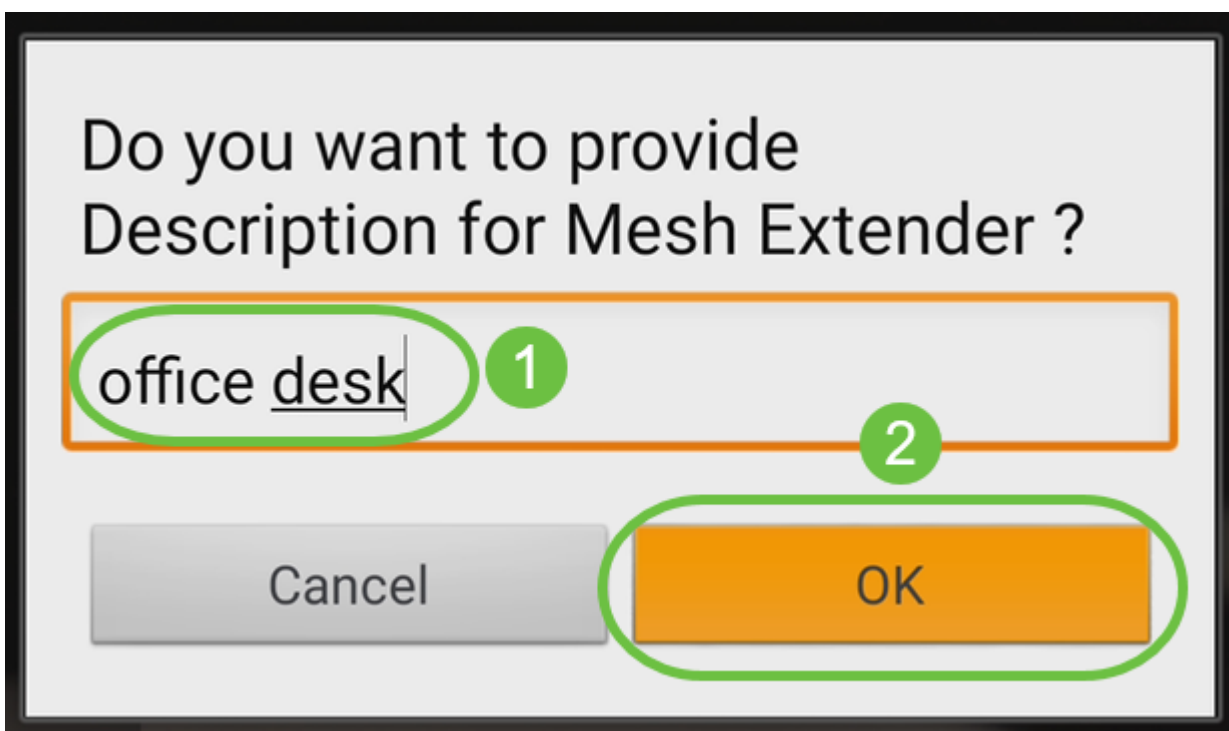


Verá la siguiente pantalla una vez que se haya analizado el código QR del amplificador de malla.



Paso 5 (opcional)

Si lo prefiere, introduzca una *descripción para Mesh Extender*. 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 [redacted] 0

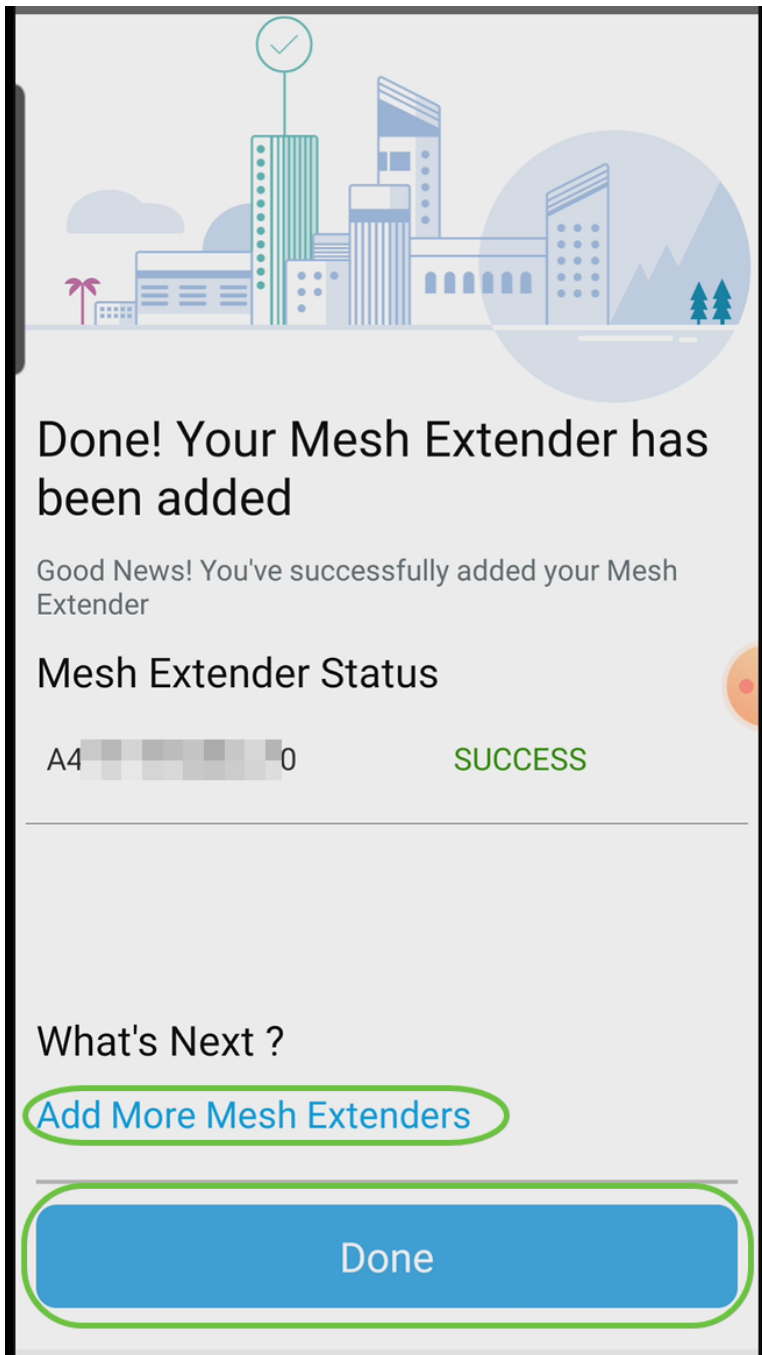
office desk



Submit

Paso 7

Haga clic en *Agregar más extensores de malla* para agregar otros extensores de malla a su red. Una vez que se hayan agregado todos los extensores de malla, haga clic en **Finalizado**.



Repita este procedimiento para cada extensor de malla.

Ahora tiene la configuración básica lista para su lanzamiento. Antes de continuar, asegúrese de comprobar y actualizar el software si es necesario.

Comprobar y actualizar software en la aplicación móvil

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

Paso 1

En su aplicación móvil, bajo la pestaña **Más**, haga clic en el **botón Buscar actualización**. Siga las indicaciones para actualizar el software a la última versión.



System Information



Home



Overview



Devices



WLAN



Clients



More

SYSTEM NAME:



1

Model

CBW140AC-B

Serial Number

FGL2419LCQN

2

Software Version

10.3.1.0

[Check for update](#)

Paso 2

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



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.

Crear WLAN mediante la aplicación móvil

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

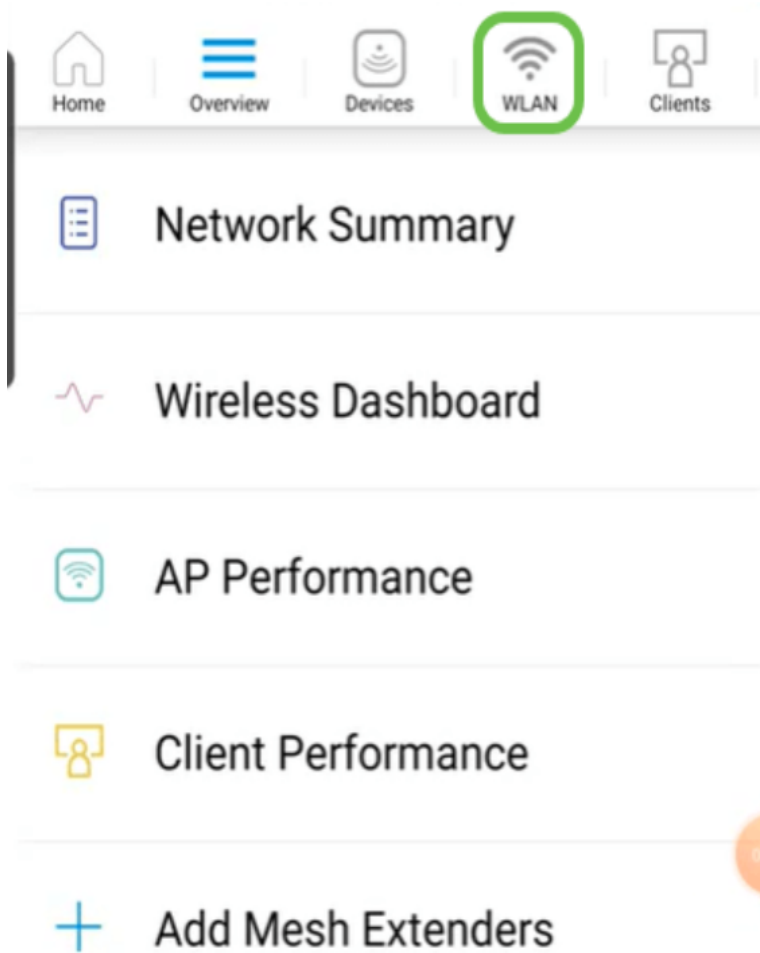
Paso 1

Abra la aplicación Cisco Business Wireless App. _



Paso 2

Conéctese a la red inalámbrica de Cisco Business en su 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

Ingrese un **Nombre de Perfil** y **SSID**. Rellene el resto de los campos o déjelos en la configuración predeterminada. Si ha activado el control de visibilidad de la aplicación, se explicarán otras configuraciones en el paso 6. Haga clic en Next (Siguiete).

The screenshot shows the 'WLAN' configuration page in a mobile application. At the top, there is a navigation bar with a back arrow, the title 'WLAN', and five menu items: Overview, Devices, WLAN (selected), Clients, and More. Below the navigation bar is the 'General' section. The configuration fields are as follows:

- WLAN ID: 3
- Profile Name*: labnet (marked with a green circle '1')
- SSID*: labnet (marked with a green circle '2')
- Admin State: Enabled
- Radio Policy: ALL
- Broadcast SSID: ON (toggle switch)
- Client Profiling: ON (toggle switch)
- Application Visibility Control: OFF (toggle switch)
- Next button (marked with a green circle '3')

Paso 5 (opcional)

Si ha activado *Control de visibilidad de la aplicación* en el paso 4, puede configurar otros parámetros, incluida una red de invitado. Los detalles de esto se pueden encontrar en la siguiente sección. También puede agregar *Network Assistant cautivo*, *tipo de seguridad*, *frase de paso* y *caducidad de contraseña*. Cuando haya agregado todas las configuraciones, haga clic en **Siguiete**.

The screenshot displays the WLAN Security configuration interface. At the top, there is a navigation bar with a back arrow, the title 'WLAN', and five menu items: Overview, Devices, WLAN (selected), Clients, and More. Below the navigation bar is a section titled 'Security'. The settings are as follows:

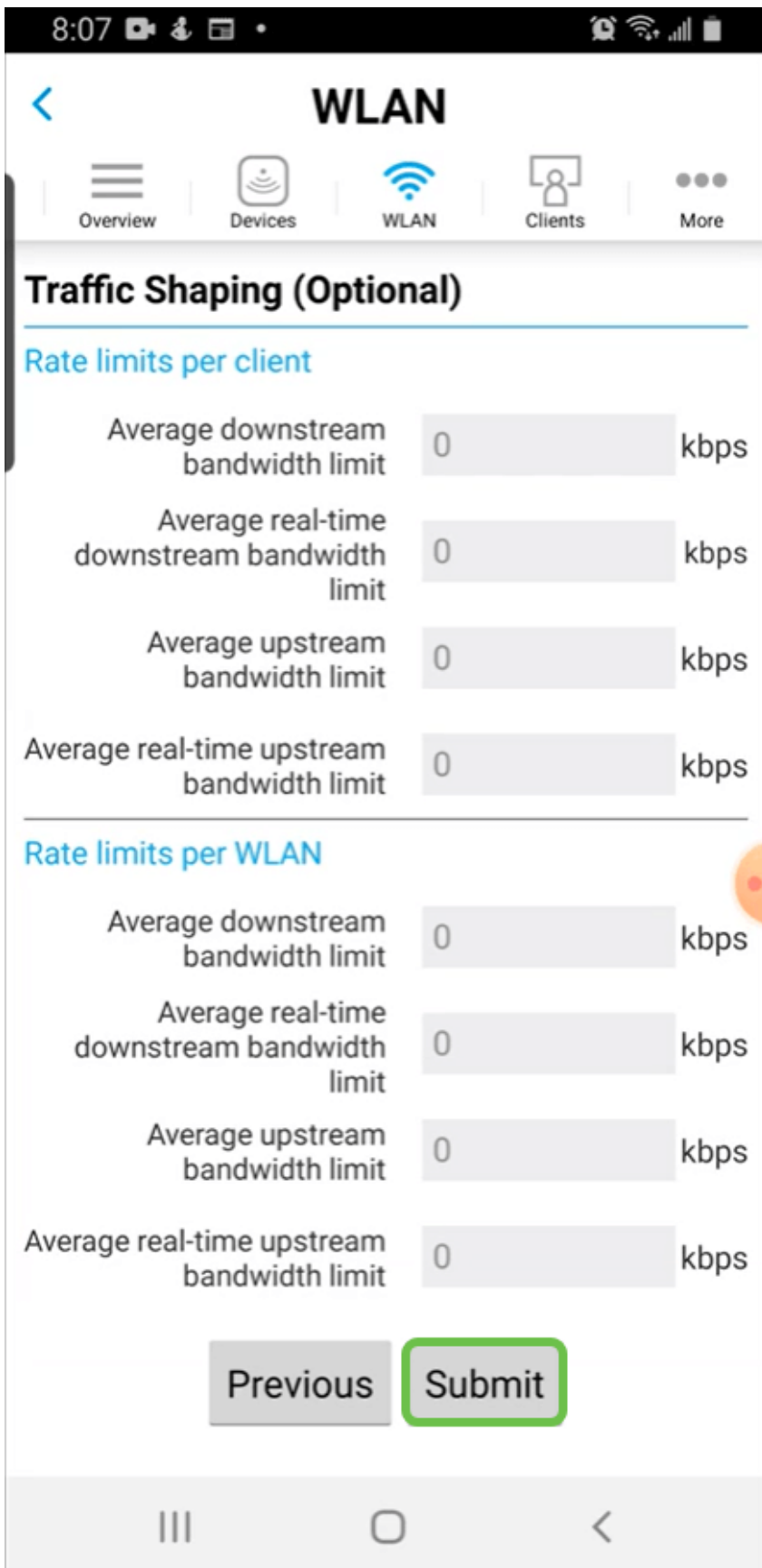
- Guest Network: OFF
- Captive Network Assistant: OFF
- Security Type: WPA2 Personal
- Passphrase Format: ASCII
- Passphrase*: [Redacted]
- Confirm Passphrase*: [Redacted]
- Show Passphrase:
- Password Expiry: OFF

At the bottom of the form, there are two buttons: 'Previous' and 'Next'. The 'Next' button is highlighted with a green border.

Cuando se utiliza la aplicación móvil, las únicas opciones para *Tipo de seguridad* son *Open* o *WPA2 Personal*. Para opciones más avanzadas, inicie sesión en la interfaz de usuario web del punto de acceso de la aplicación móvil en su lugar.

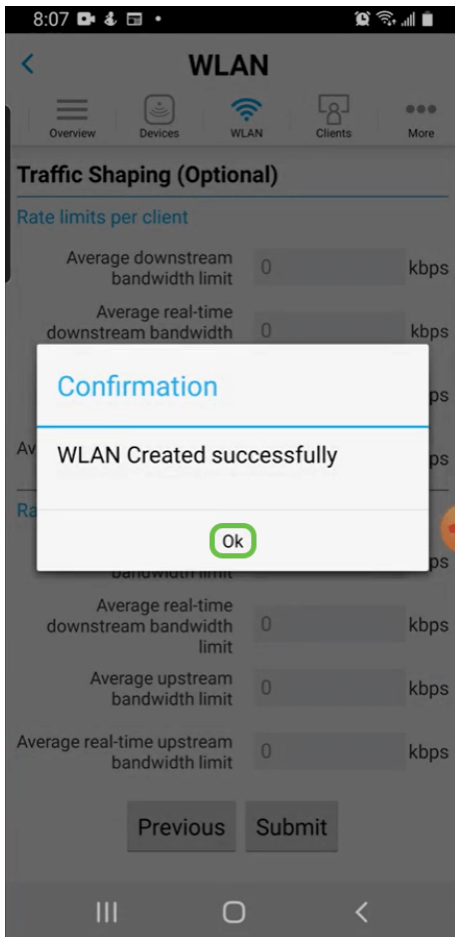
Paso 6 (opcional)

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



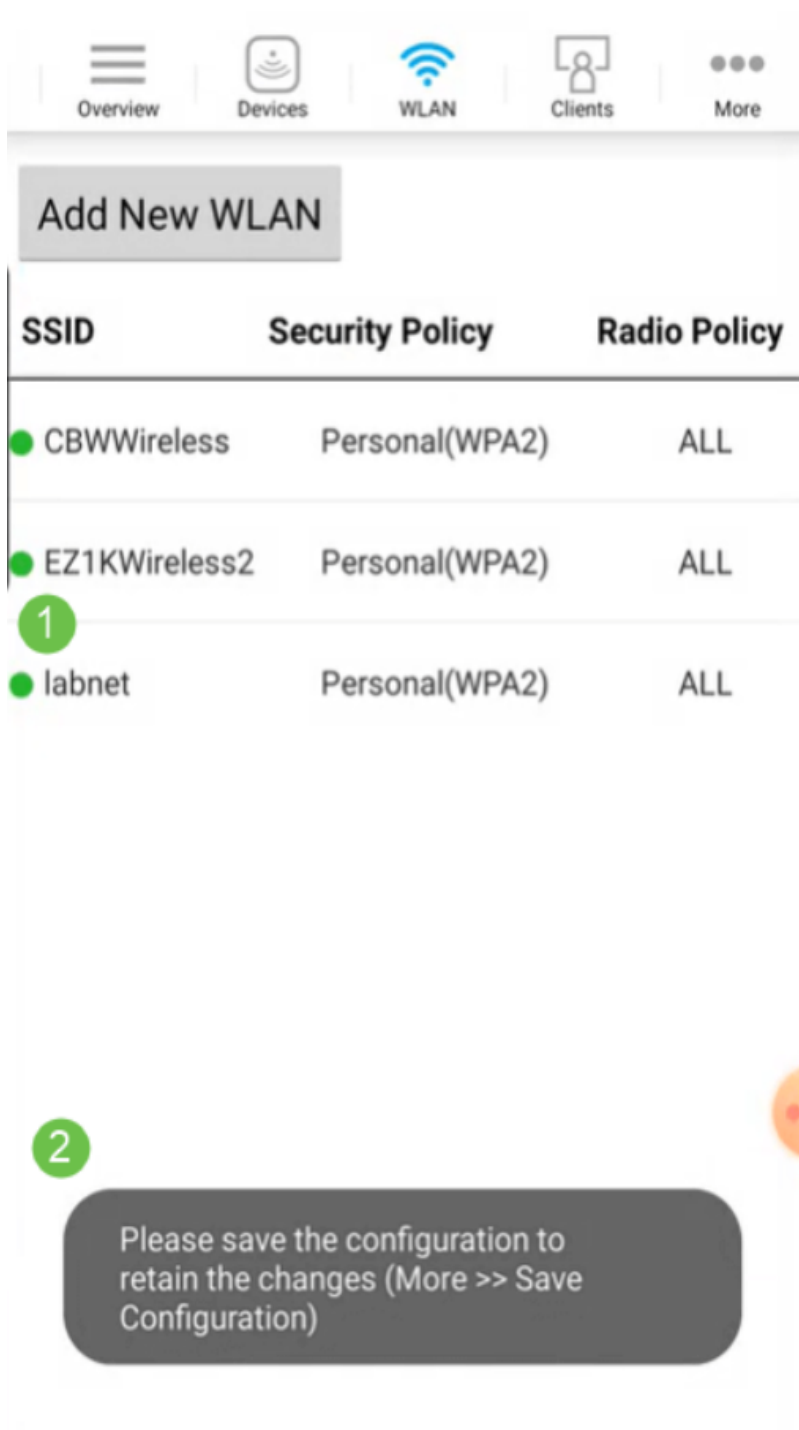
Paso 7

Verá una ventana emergente de confirmación. Click OK.



Paso 8

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



Paso 9

Para guardar la configuración, haga clic en la ficha **Más** y, a continuación, seleccione **Guardar configuración** en el menú desplegable.



Cree una WLAN de invitado mediante la aplicación móvil

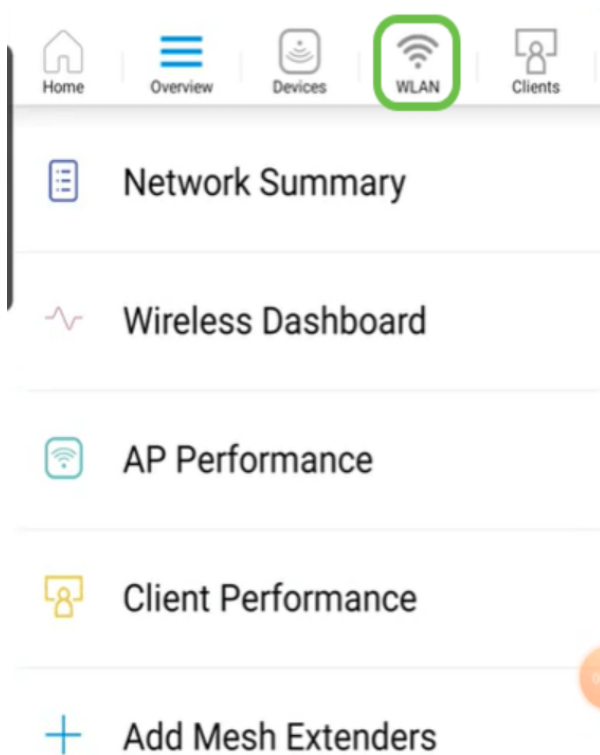
Paso 1

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



Paso 2

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



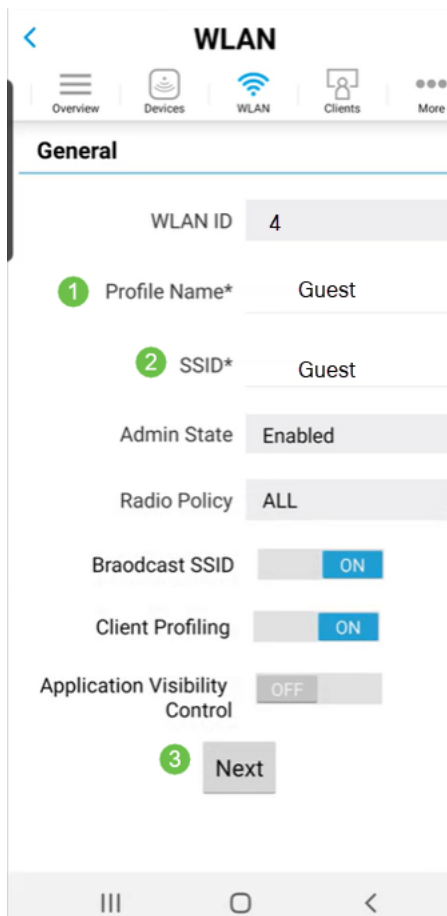
Paso 3

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



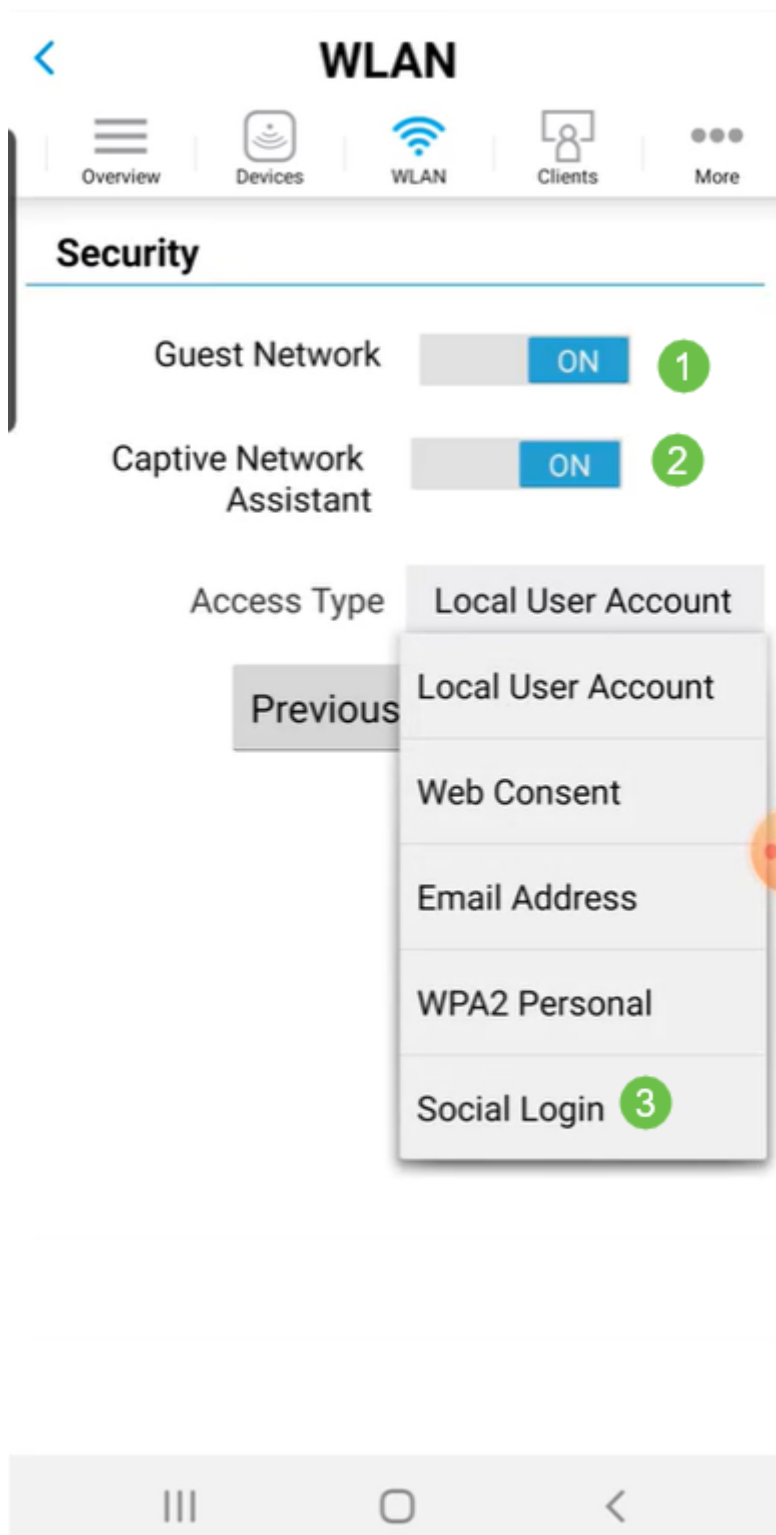
Paso 4

Ingrese un **Nombre de Perfil** y **SSID**. Rellene el resto de los campos o déjelos en la configuración predeterminada. Haga clic en Next (Siguiente).



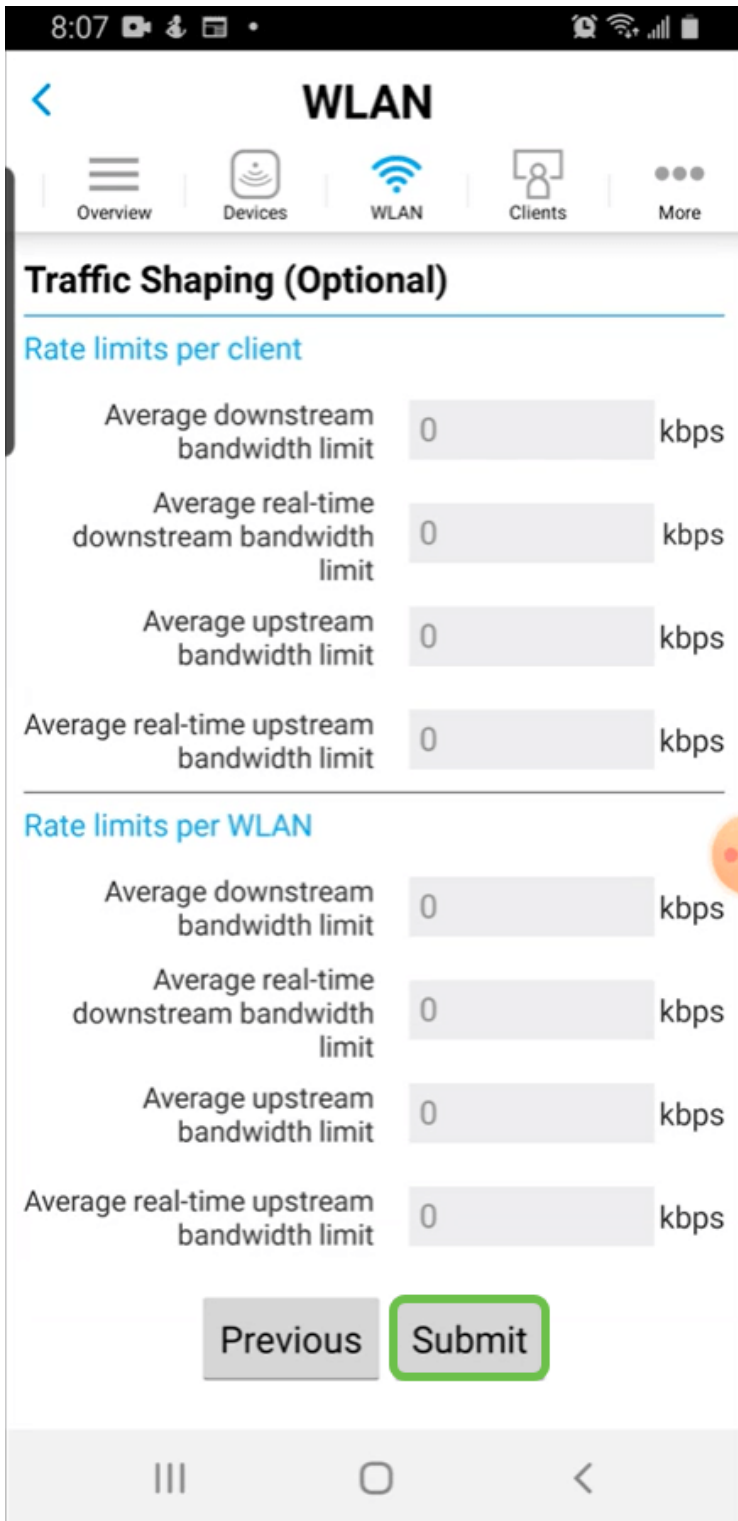
Paso 5

Active *Red de invitado*. En este ejemplo, *Captive Network Assistant* también se activa, pero esto es opcional. Tiene opciones para *Tipo de acceso*. En este caso, se selecciona *Inicio de sesión social*.



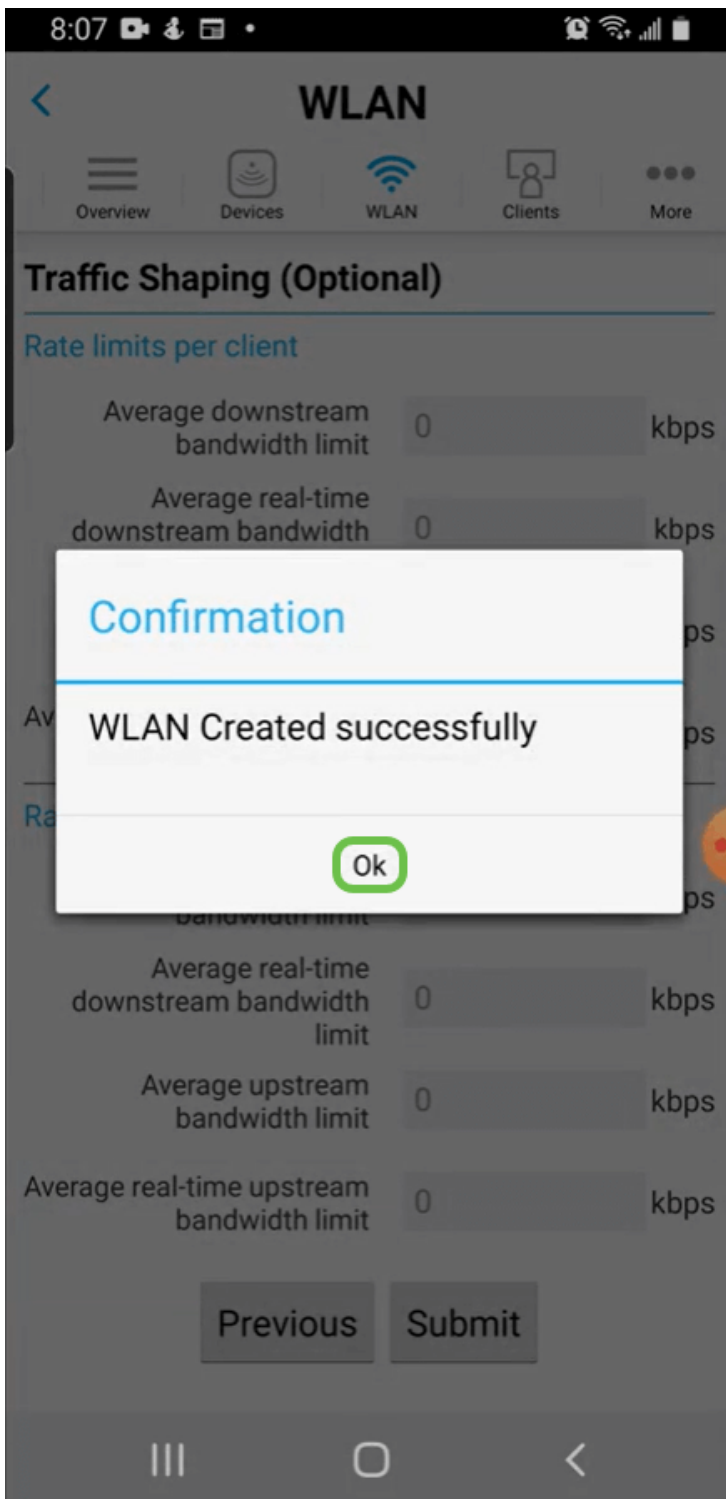
Paso 6

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



Paso 7

Verá una ventana emergente de confirmación. Click OK.



Paso 8

Para guardar la configuración, haga clic en la ficha **Más** y, a continuación, seleccione **Guardar configuración** en el menú desplegable.



Conclusión

Ahora tiene una configuración completa para su red. ¡Tómate un minuto para celebrar

y luego ponte a trabajar!

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

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

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

- [Router VPN Cisco RV260P con PoE](#)
- [Punto de acceso Cisco Business 140AC](#)
- [Cisco Business 142ACM Mesh Extender](#)