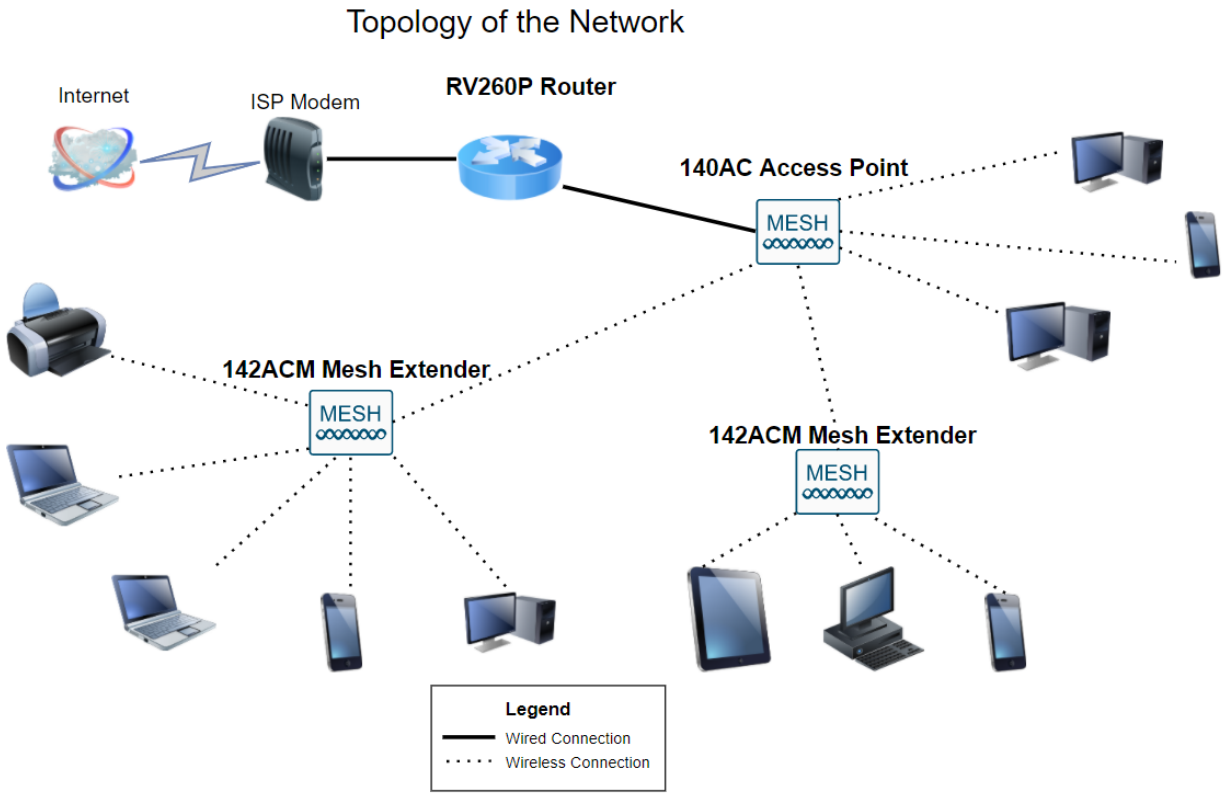
Totale netwerkconfiguratie: RV260P met Cisco Business Wireless en Web UI

Doel:

Deze gids zal u tonen hoe u een draadloos netwerk met een router RV260P, een access point CBW140AC en twee extenders van het ACM-netwerk kunt configureren.

Dit artikel gebruikt het Web User Interface (UI) om het netwerk voor draadloze netwerken in te stellen. Als u liever de mobiele toepassing gebruikt, die voor eenvoudige draadloze installatie wordt aanbevolen, klikt u op om naar het artikel te springen dat de mobiele toepassing gebruikt. Als je het web UI wilt gebruiken, blijf lezen!

Topologie:



Inleiding

Hier ben je klaar om je nieuwe netwerk op te zetten. Het is een opwindende dag! In dit scenario gebruiken we een RV260P router. Deze router biedt Power over Ethernet (PoE) waardoor u CBW140AC in de router kunt aansluiten in plaats van een switch. De CBW140AC en de CBW142ACM mesh-extenders zullen worden gebruikt om een draadloos netwerk te maken.

Als u niet bekend bent met een aantal bepalingen die in dit document voorkomen of meer informatie wilt over netwerken in mesh, dan dient u de volgende artikelen te

controleren:

- Cisco Business: Lijst van termen
- Welkom in Cisco Business Wireless mesh-netwerken
- Vaak gestelde vragen (FAQ) voor een Cisco Business Wireless Network

Ben je klaar? Laten we daar aan werken!

Toepasselijke apparaten | Software versie

- RV260P-switch | 1.0.0.17
- CBW140 AC | 10.3.1.0
- CBW142ACM | 10.3.1.0 (voor het net van mazen is ten minste één extender nodig)

Inhoud

Voordat u start

1. Zorg ervoor dat u een huidige internetverbinding hebt voor installatie.
2. Neem contact op met uw ISP om eventuele speciale instructies te ontdekken die u hebt wanneer u uw RV260-router gebruikt. Sommige ISPs bieden gateways met ingebouwde routers aan. Als u een gateway met een geïntegreerde router hebt, kunt u de router uitschakelen en het WAN-adres (Wide Area Network) (het unieke Internet-protocoladres dat de Internet-provider aan uw account toekent) en al het netwerkverkeer naar uw nieuwe router doorgeven.
3. Bepaal waar u de router wilt plaatsen. U wilt indien mogelijk een open gebied. Dit kan

niet makkelijk zijn, omdat u de router aan de breedbandgateway (modem) van uw Internet Service Provider (ISP) moet verbinden.

Het configureren van de RV260P router

Een router is essentieel in een netwerk omdat het pakketten vervoert. Het stelt een computer in om met andere computers te communiceren die niet op hetzelfde netwerk of net zijn. Een router heeft toegang tot een routingtabel om te bepalen waar pakketten moeten worden verzonden. De routingtabel toont doeladressen. De statische en dynamische configuraties kunnen beiden op de routingtabel worden vermeld om pakketten naar hun specifieke bestemming te krijgen.

Uw RV260P wordt geleverd met standaardinstellingen die voor veel kleine bedrijven zijn geoptimaliseerd. Uw netwerkvereisten voor Internet Service Provider (ISP) vereisen echter dat u een aantal van deze instellingen wijzigt. Nadat u voor de vereisten contact hebt opgenomen met uw ISP, kunt u wijzigingen aanbrengen met behulp van de Web User Interface (UI).

RV260P uit het vakje

Stap 1

Sluit de Ethernet-kabel van een van de RV260P LAN (Ethernet)-poorten aan op de Ethernet-poort op de computer. U hebt een adapter nodig als uw computer geen Ethernet poort heeft. De terminal moet in hetzelfde bekabelde subnetwerk zijn als de RV260P om de eerste configuratie uit te voeren.

Stap 2

Gebruik de voedingsadapter die bij de RV260P is geleverd. Een andere voedingsadapter gebruiken kan de RV260P beschadigen of kan ervoor zorgen dat USB-dongels niet werken. De switch is standaard ingeschakeld.

Sluit de voedingsadapter aan op de 12VDC-poort van de RV260P, maar stop deze nog niet in het stopcontact.

Stap 3

Controleer of de modem is uitgeschakeld.

Stap 4

Gebruik een Ethernet-kabel om uw kabel of DSL-modem aan te sluiten op de WAN-poort op de RV260P.

Stap 5

Sluit het andere uiteinde van de RV260P-adapter aan op een stopcontact. Dit schakelt de RV260 in. Steek de modem opnieuw in zodat deze ook kan inschakelen. Het stroomlicht op het voorpaneel is stevig groen wanneer de voedingsadapter goed is aangesloten en de RV260P is klaar met starten.

Stel de router in

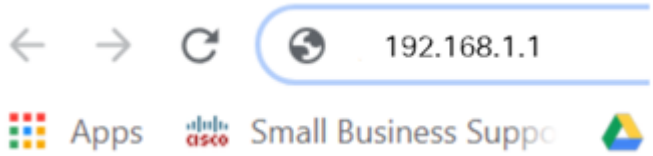
Het voorbereidend werk is gedaan, nu is het tijd om wat formaties te doen! U kunt het web UI starten door deze stappen te volgen:

Stap 1

Als uw computer is ingesteld op een DHCP-client (Dynamic Host Configuration Protocol), wordt een IP-adres in het bereik 192.1.x aan de PC toegewezen. DHCP automatiseert het proces om IP adressen, SUBNET maskers, standaardgateways, en andere instellingen aan computers toe te wijzen. Computers moeten worden ingesteld om aan het DHCP-proces deel te nemen om een adres te verkrijgen. Dit gebeurt door te selecteren om automatisch een IP-adres te verkrijgen in de eigenschappen van TCP/IP op de computer.

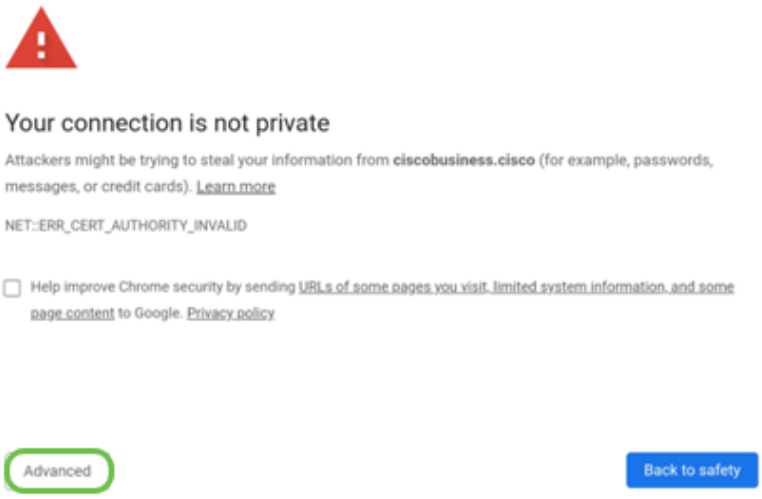
Stap 2

Open een webbrowser zoals Safari, Internet Explorer of Firefox. Voer in de adresbalk het standaard IP-adres van de RV260P in dat 192.168.1.1 is.



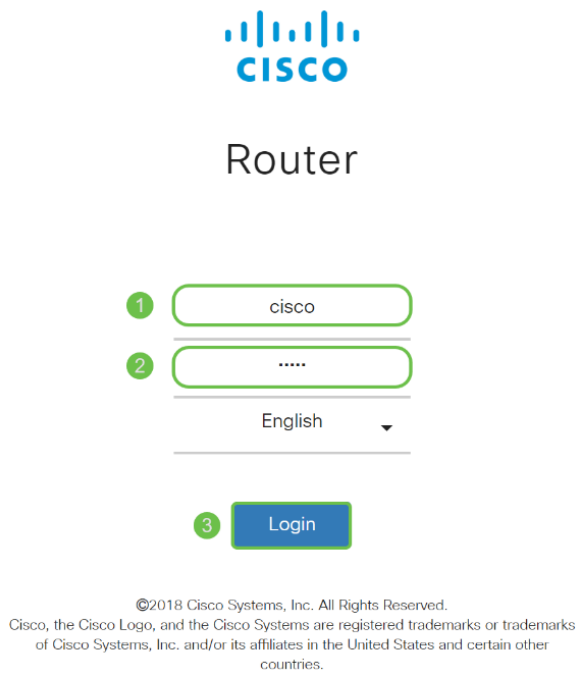
Stap 3

De browser waarschuwt dat de website onbetrouwbaar is. Ga verder naar de website. Als u geen verbinding hebt, keert u terug naar Problemen oplossen bij de internetverbinding.



Stap 4

Wanneer de inlogpagina verschijnt, voert u de standaard gebruikersnaam cisco in en *cisco* met het standaardwachtwoord. Zowel de gebruikersnaam als het wachtwoord zijn hoofdlettergevoelig.



Stap 5

Klik op **Aanmelden**. De pagina *Introductie* verschijnt. Nu u de verbinding hebt bevestigd en op de router hebt inlogd, springt u naar het gedeelte Initiële configuratie van dit artikel.

Probleemoplossing voor de internetverbinding

Als je dit leest, heb je waarschijnlijk moeite om verbinding te maken met het internet of de web UI. Eén van deze oplossingen moet helpen.

In uw aangesloten Windows OS kunt u de netwerkverbinding testen door de opdrachtmelding te openen. Voer 192.168.1.1 in (het standaard IP-adres van de router). Als het verzoek uit is, kunt u niet met de router communiceren.

Als er geen connectiviteit plaatsvindt, kunt u Problemen oplossen bij RV160 en RV260 routers controleren.

Nog een paar dingen om te proberen:

1. Controleer dat uw webbrowser niet is ingesteld op Werk Offline.
2. Controleer de lokale verbindingsinstellingen voor uw Ethernet-adapter. De PC zou een IP adres via DHCP moeten verkrijgen. U kunt ook een statisch IP-adres in het bereik 192.168.1.x hebben als de standaardgateway wordt ingesteld op 192.168.1.1 (het standaard IP-adres van de RV260P). Om verbinding te kunnen maken, moet u mogelijk de netwerkinstellingen van RV260P wijzigen. Als u Windows 10 gebruikt, raadpleegt u

Windows 10-instructies om de netwerkinstellingen te wijzigen.

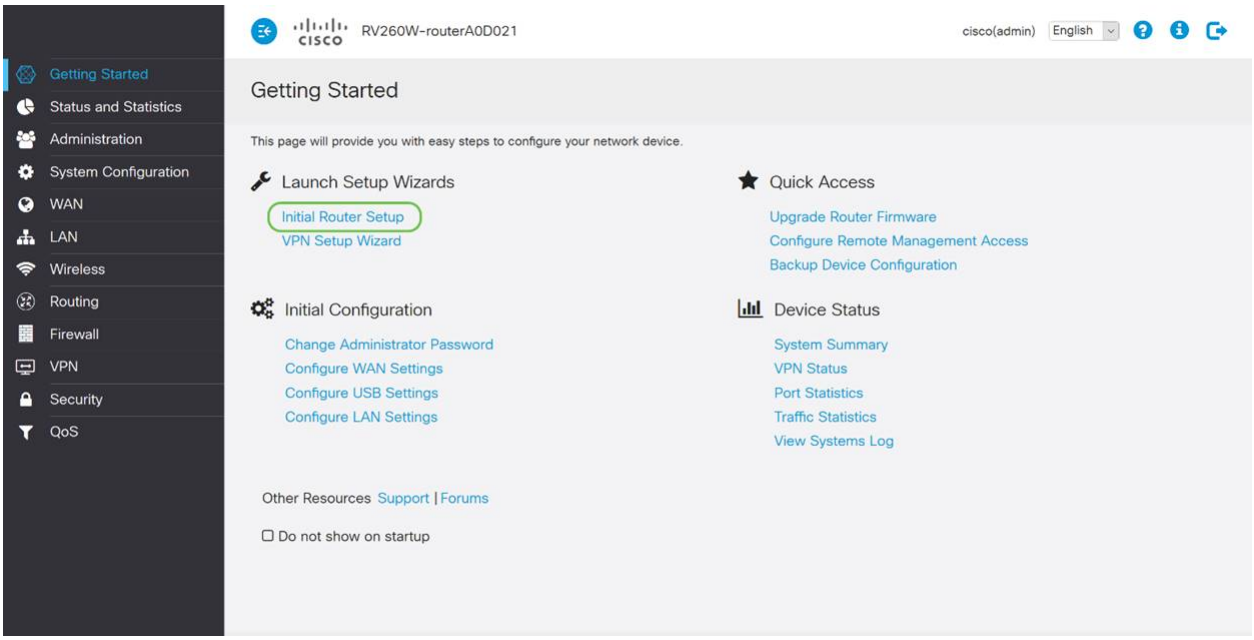
3. Als u bestaand apparaat hebt dat het 192.168.1.1 IP-adres bezet houdt, zult u dit conflict moeten oplossen zodat het netwerk kan functioneren. Klik hier aan het einde van dit gedeelte of klik hier om direct te worden ingenomen.
4. Reset de modem en de RV260P door beide apparaten uit te schakelen. Zet de modem vervolgens aan en laat het ongeveer 2 minuten niets doen. Schakel de RV260P in. U dient nu een WAN IP-adres te ontvangen.
5. Als u een DSL-modem hebt, vraag uw ISP om de DSL-modem in de brugmodus te zetten.

Eerste configuratie

We raden u aan om de stappen van de wizard voor eerste installatie uit te voeren die in deze sectie zijn vermeld. U kunt deze instellingen op elk moment wijzigen.

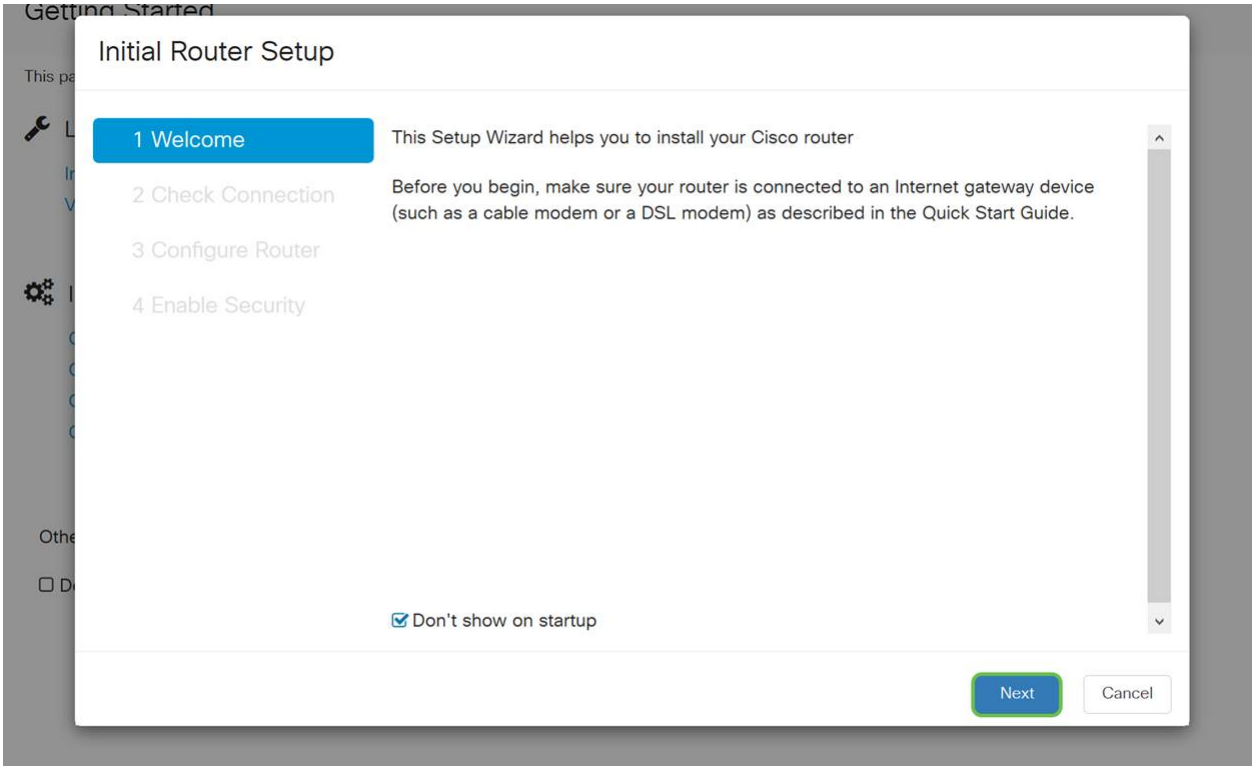
Stap 1

Klik op de **Wizard Setup** op de pagina *Introductie*.



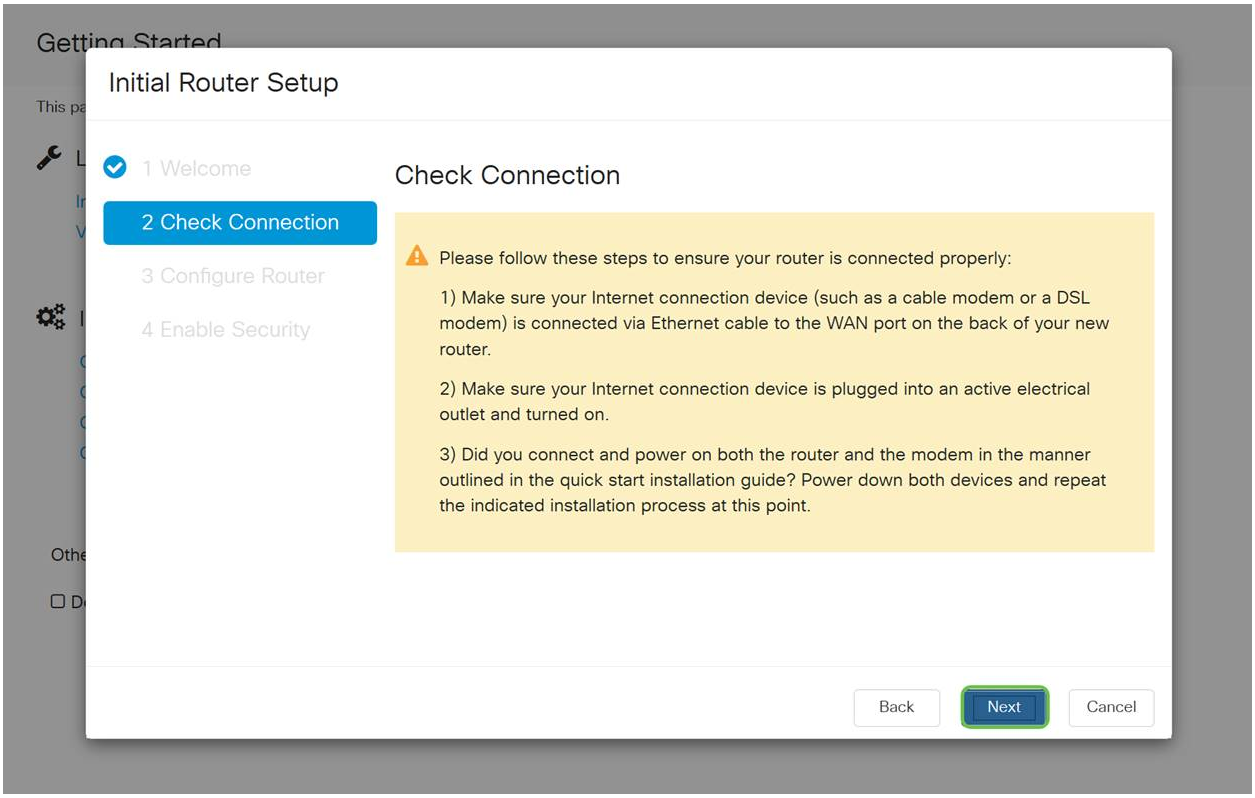
Stap 2

Deze stap bevestigt dat de kabels zijn aangesloten. Aangezien u dit al hebt bevestigd, klikt u op **Volgende**.



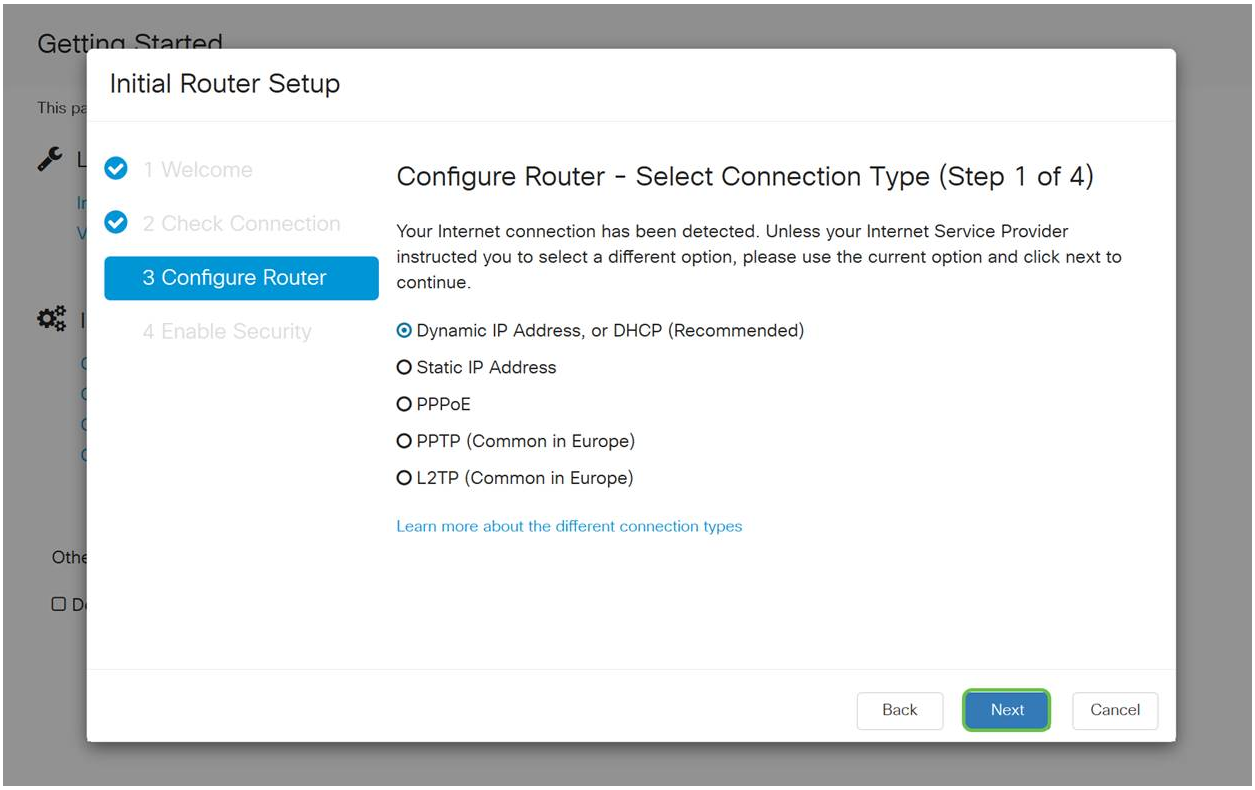
Stap 3

Deze stap bestrijkt basisstappen om er zeker van te zijn dat uw router is aangesloten. Aangezien u dit al hebt bevestigd, klikt u op **Volgende**.



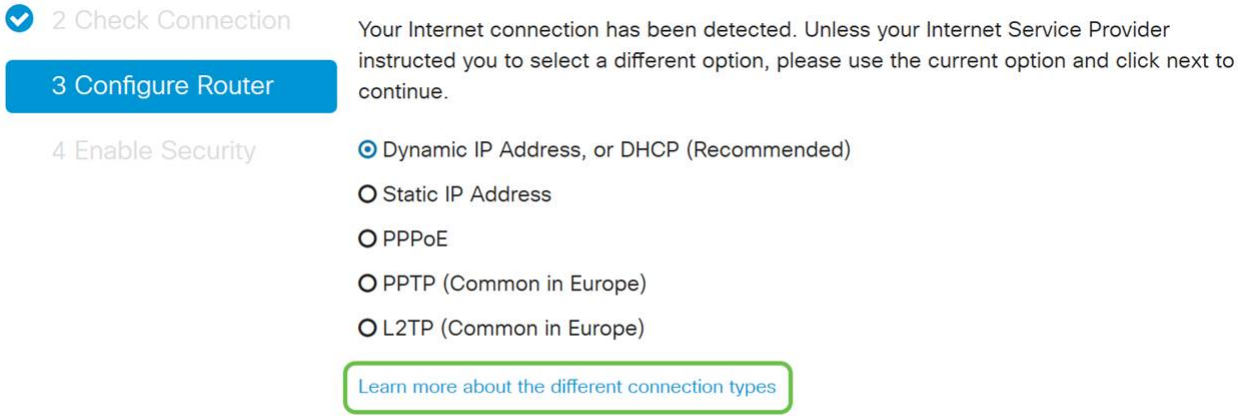
Stap 4

Het volgende scherm toont uw opties om IP adressen aan uw router toe te wijzen. U moet DHCP in dit scenario selecteren. Klik op **Volgende**.



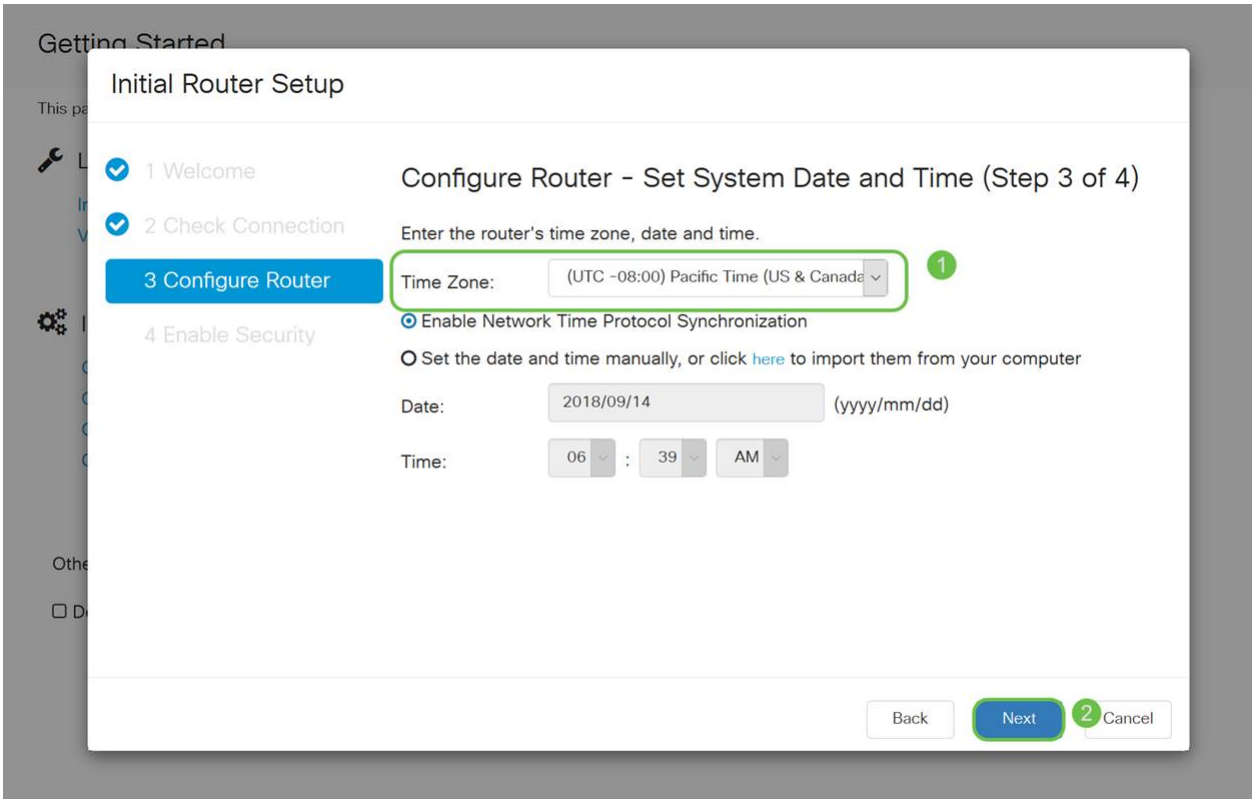
Hoewel u DHCP voor deze eerste instelling moet gebruiken, kunt u instellen om *meer* te *weten* te *komen over de verschillende soorten verbindingen* naar de onderkant van uw scherm en naar de referentie voor de toekomst. Bekijk de volgende artikelen voor meer informatie hierover:

- WAN-configuratie op RV160x en RV260x-apparaten
- Statische routing configureren op de RV160 en RV260



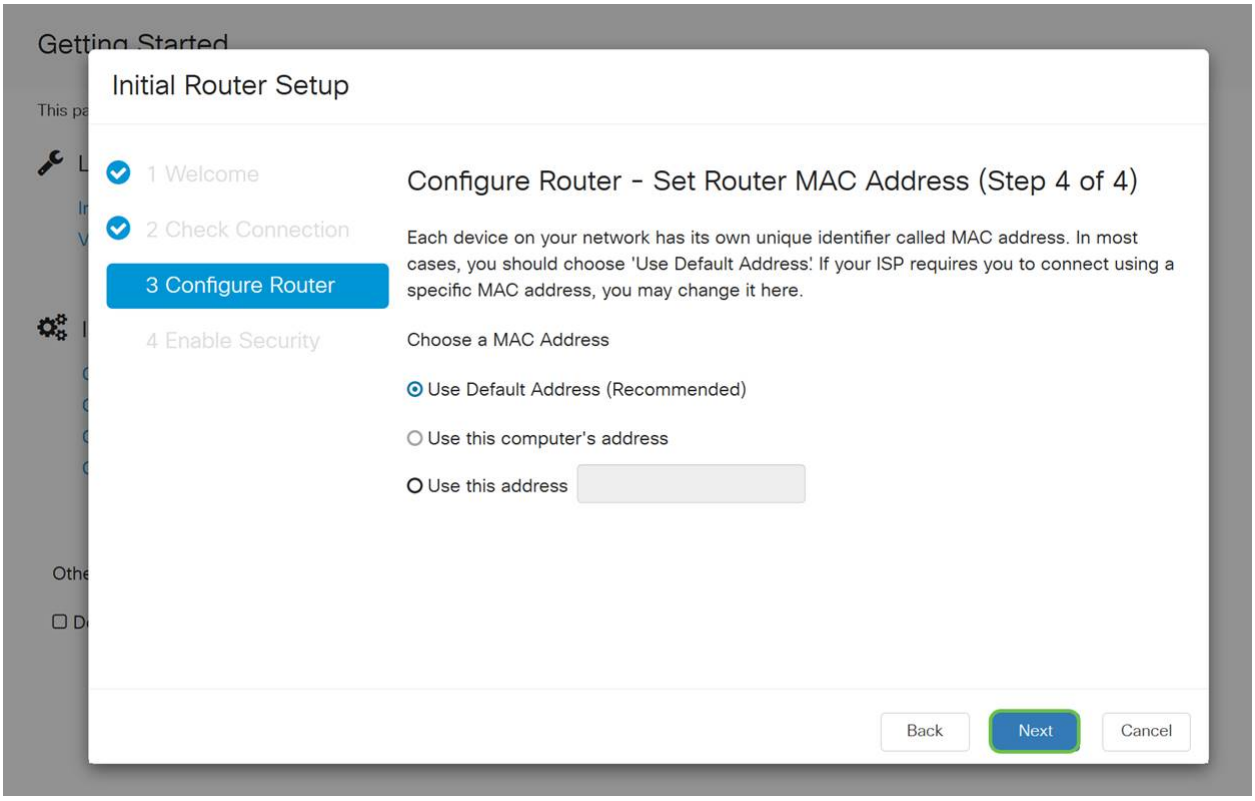
Stap 5

Hier wordt u gevraagd de instellingen van de routertijd in te stellen. Dit is belangrijk omdat het precisie in staat stelt bij het bekijken van logbestanden of het oplossen van gebeurtenissen. Selecteer uw **tijdzone** en klik vervolgens op **Volgende**.



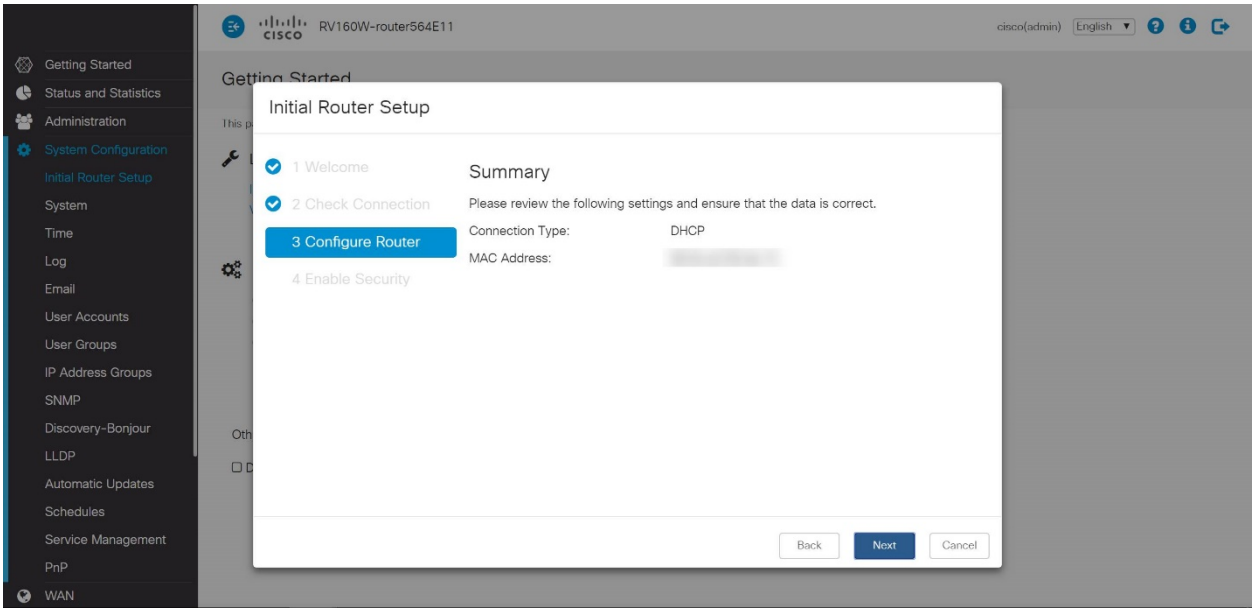
Stap 6

Op dit scherm, zult u selecteren welke MAC adressen aan apparaten toe te wijzen. Meestal gebruikt u het standaardadres. Klik op **Volgende**.



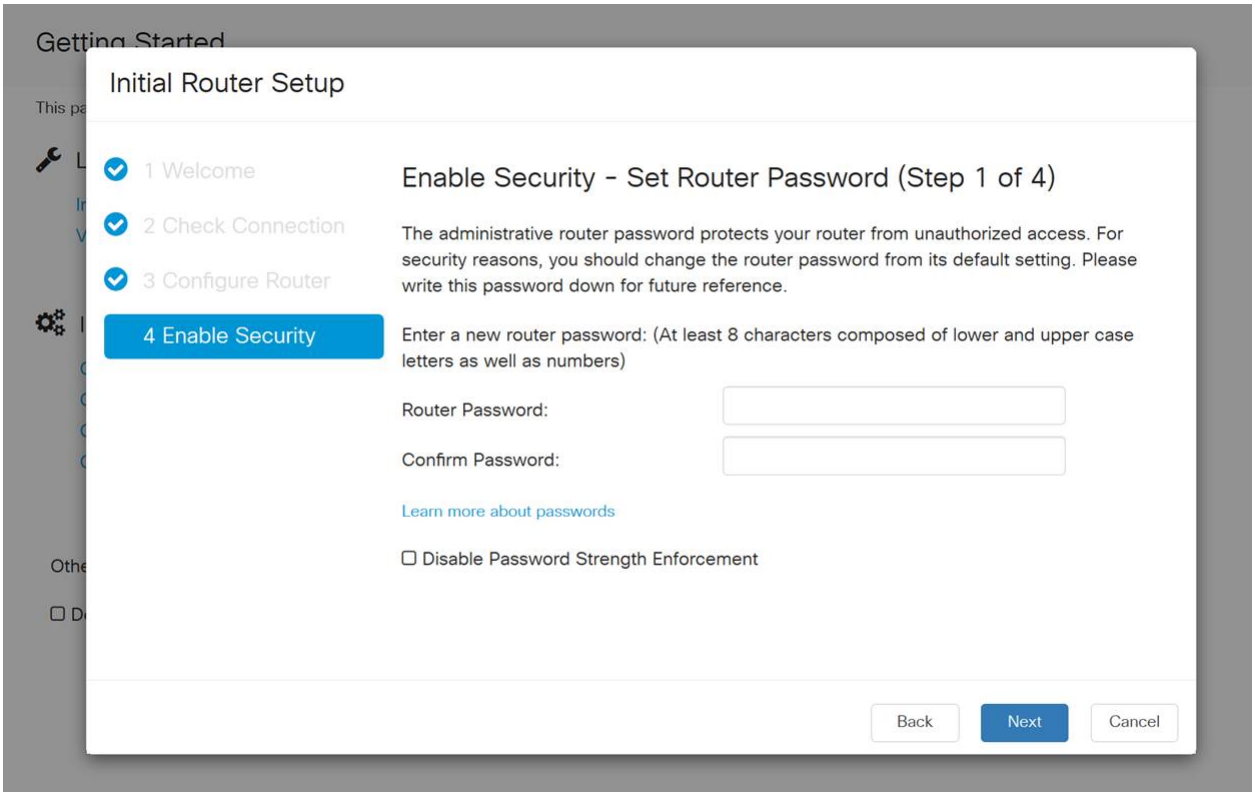
Stap 7

De volgende pagina is een samenvatting van de geselecteerde opties. Bekijk dit en klik op **Volgende** als u tevreden bent.



Stap 8

Voor de volgende stap selecteert u een wachtwoord dat u wilt gebruiken wanneer u in de router logt. De standaard voor wachtwoorden is dat minimaal 8 tekens (zowel hoofdletters als kleine letters) moeten bevatten. **Voer een wachtwoord in** dat aan de vereisten voor de sterkte voldoet. Klik op **Volgende**. Neem nota van uw wachtwoord voor toekomstige logins.



Het wordt *niet* aanbevolen om de optie *Wachtwoordsterkte* uitschakelen te selecteren. Met deze optie kunt u een wachtwoord selecteren dat zo eenvoudig is als 123, wat net zo makkelijk is als 1-2-3 voor kwaadaardige acteurs om te breken.

Stap 9

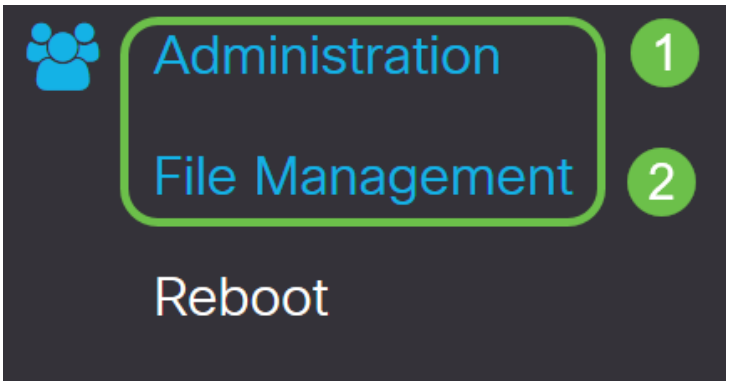
Klik op het **pictogram Opslaan**.

Upgradefirmware indien nodig

Dit is een belangrijk deel, sla het dan niet over!

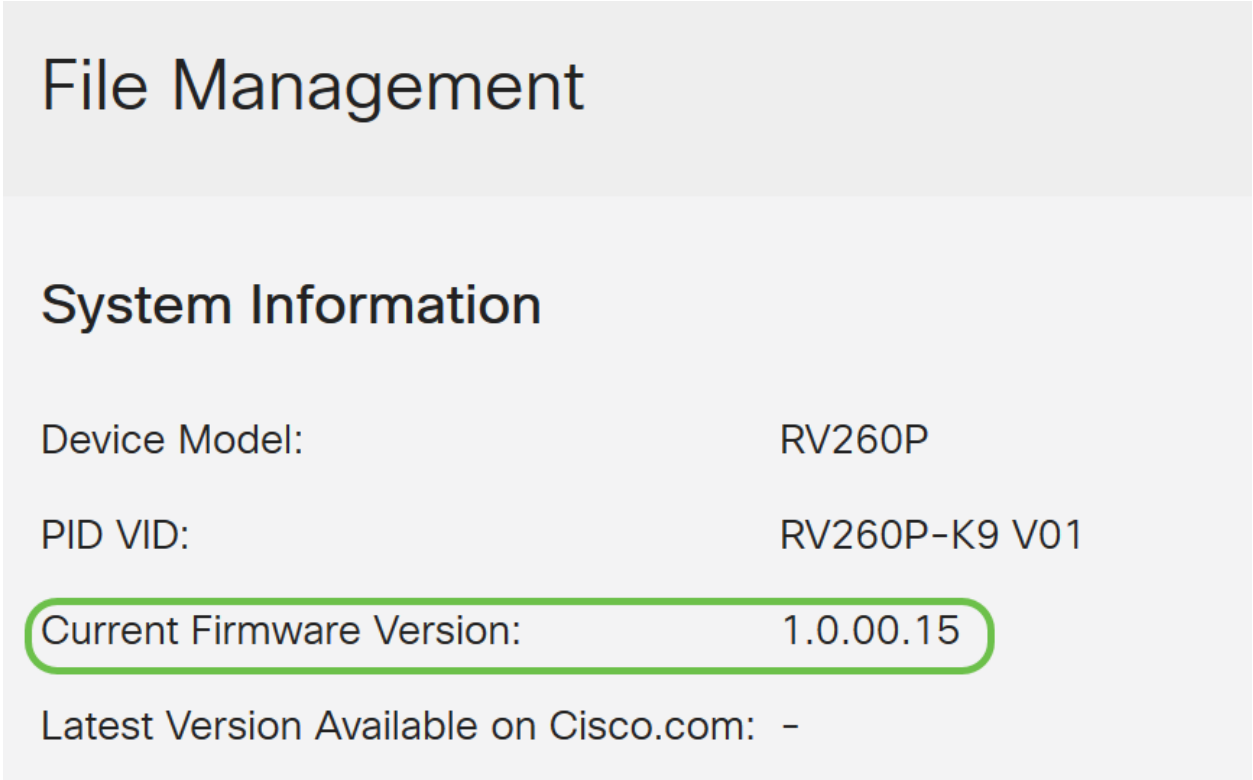
Stap 1

Kies **Beheer > Bestandsbeheer**.



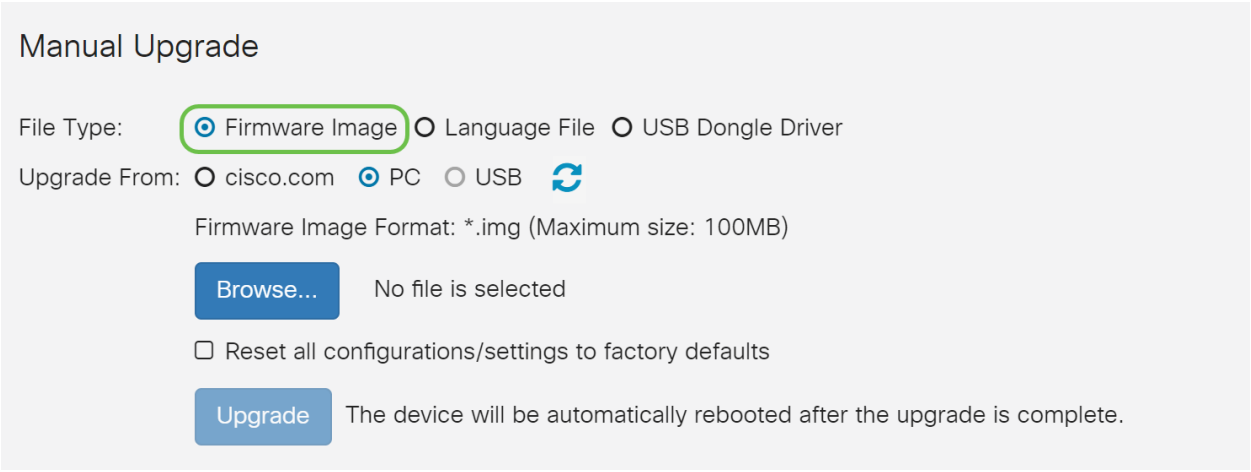
In het gebied *systeeminformatie* beschrijven de volgende subgebieden het volgende:

- Apparaatmodel - hiermee wordt het model van uw apparaat weergegeven.
- PID VID - Product-ID en ID van verkoper van de router.
- Huidige versie van firmware - firmware die momenteel op het apparaat actief is.
- Nieuwste versie beschikbaar op Cisco.com - De laatste versie van de software is beschikbaar op de Cisco-website.
- Firmware laatste bijgewerkt - Datum en tijd van de laatste firmware-update die op de router gemaakt is.



Stap 2

Klik onder het gedeelte *Handmatige upgrade* op de knop **Afbeelding firmware** voor *bestandstype*.



Stap 3

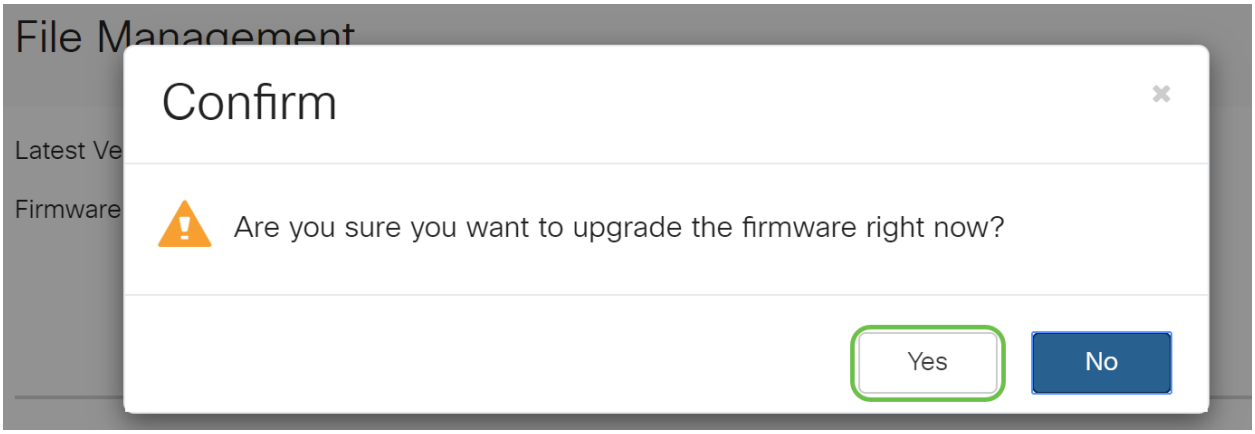
Klik op een radioknop op de pagina *Handmatige upgrade* om cisco.com te selecteren. Er zijn nog een paar andere opties voor, maar dit is de eenvoudigste manier om een upgrade uit te voeren. Dit proces installeert het laatste upgradebestand rechtstreeks vanaf de website Cisco-softwaredownloads.

Stap 4

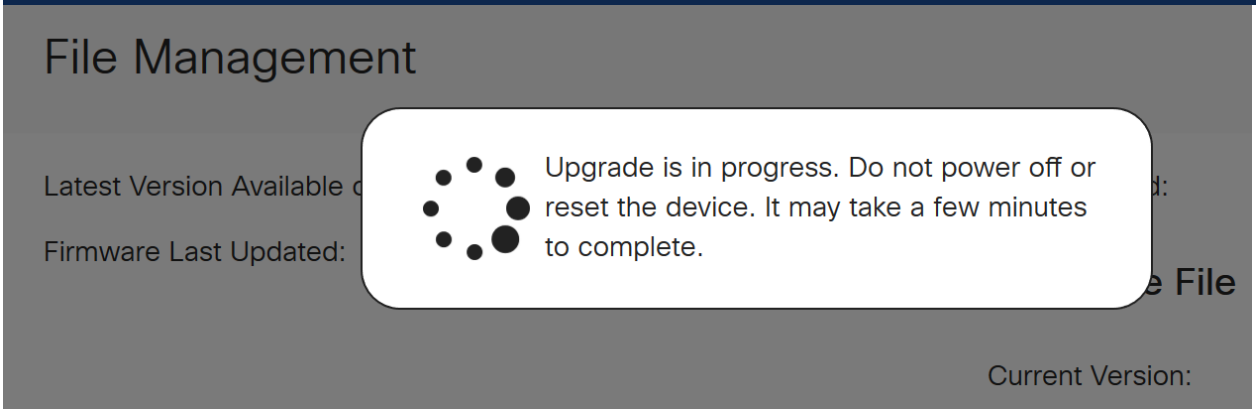
Klik op **upgrade**.

Stap 5

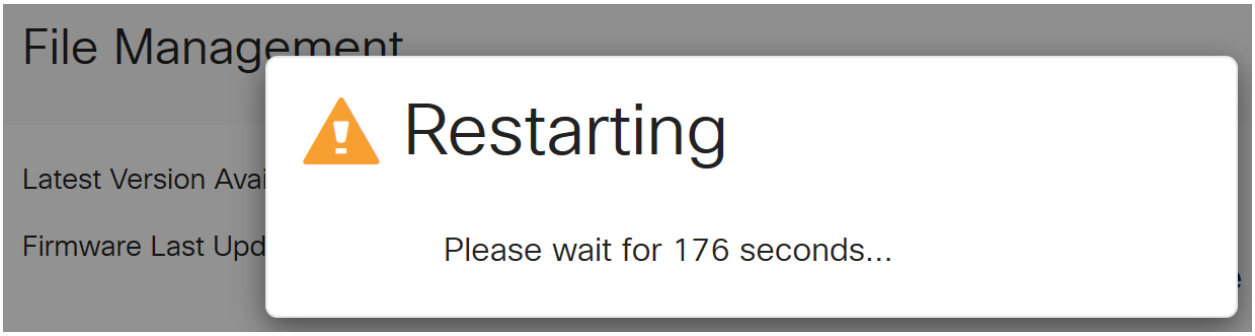
Klik op **Ja** in het bevestigingsvenster om verder te gaan.



Het moderniseringsproces moet zonder problemen verlopen. Tijdens de upgrade krijgt u het volgende bericht op het scherm.

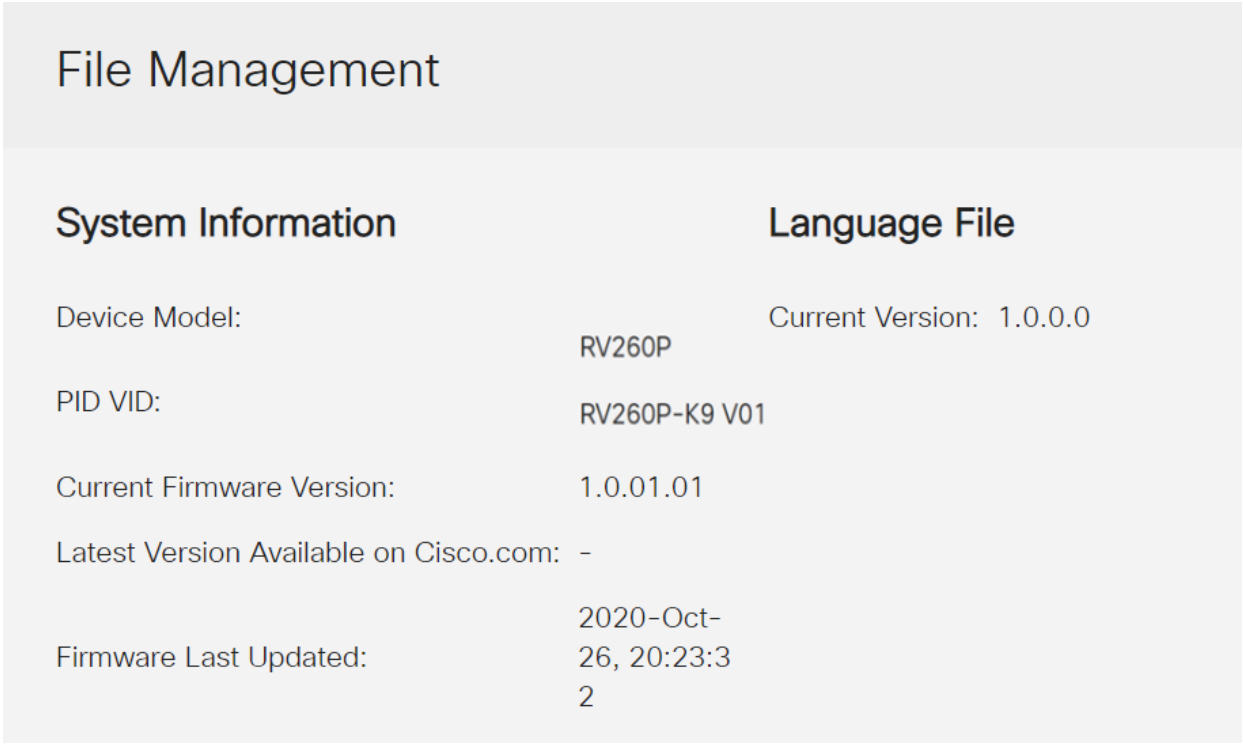


Nadat de upgrade is voltooid, verschijnt er een melding-venster om u te laten weten dat de router *opnieuw start* met een aftelsom van de geschatte tijd die u nodig hebt om het proces te voltooien. Daarna wordt je uitgelogd.



Stap 6

Log terug in het op web gebaseerde hulpprogramma om te controleren of de routerfirmware is bijgewerkt, scrollen naar de *systeeminformatie*. Het gebied *Huidige versie* van de *firmware* moet nu de aangepaste versie weergeven.



Gefeliciteerd, uw basisinstellingen op uw router zijn volledig! U hebt een aantal configuratieopties die vooruit gaan.

Ik moedig u aan door het artikel te bladeren om meer te weten te komen over deze opties en, indien ze op u van toepassing zijn, over deze opties. Als u dat liever wilt, kunt u op een van de hyperlinks klikken om in plaats daarvan naar een sectie te springen.

- VLAN's configureren (optioneel)
- IP-adres bewerken (optioneel)
- statische IP-adressen toevoegen (optioneel)
- Ik ben klaar om het mesh draadloze deel van mijn netwerk te configureren!

VLAN's configureren (optioneel)

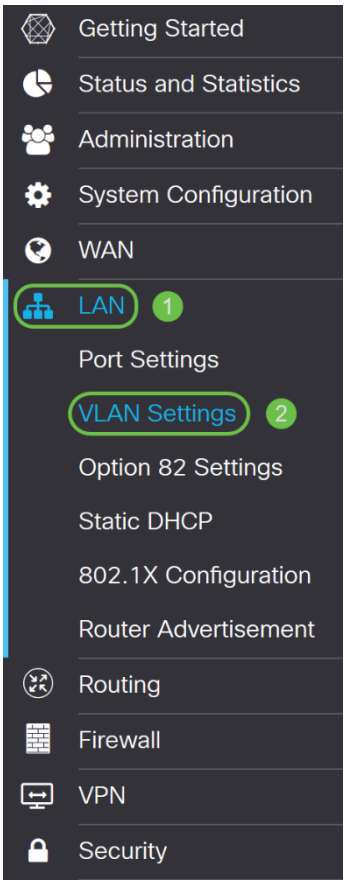
Met een Virtual Local Area Network (VLAN) kunt u een Local Area Network (LAN) logisch segmenteren in verschillende broadcastdomeinen. In scenario's waarbij

gevoelige gegevens via een netwerk kunnen worden doorgegeven, kunnen VLAN's worden opgezet om data beter te beveiligen door een broadcast aan een specifiek VLAN toe te wijzen. VLAN's kunnen ook worden gebruikt om prestaties te verbeteren door de behoefte te verminderen om broadcast en multicast pakketten naar onnodige bestemmingen te verzenden. U kunt een VLAN maken, maar dit heeft geen effect tot het VLAN aan minstens één poort is verbonden, handmatig of dynamisch. Poorten moeten altijd aan één of meer VLAN's behoren.

Als u geen VLAN's wilt maken, kunt u naar de volgende sectie overslaan.

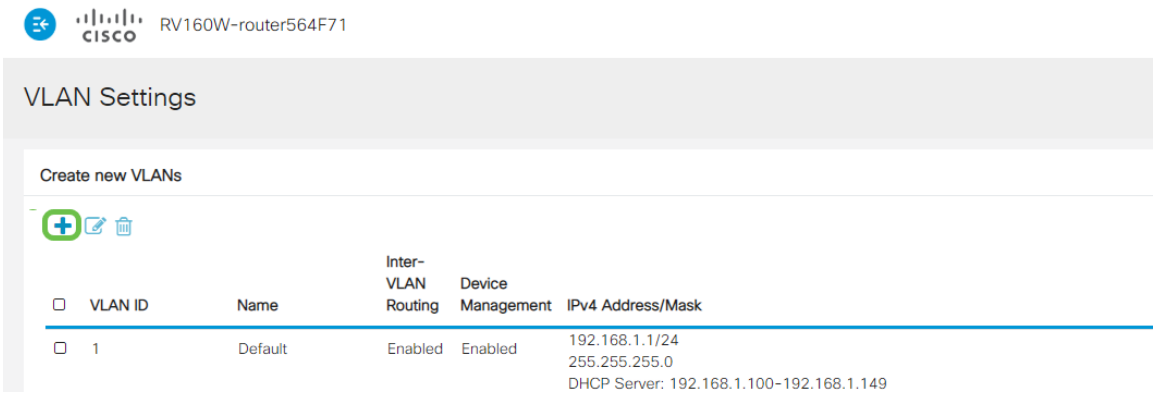
Stap 1

Navigeer naar **LAN > VLAN-instellingen**.



Stap 2

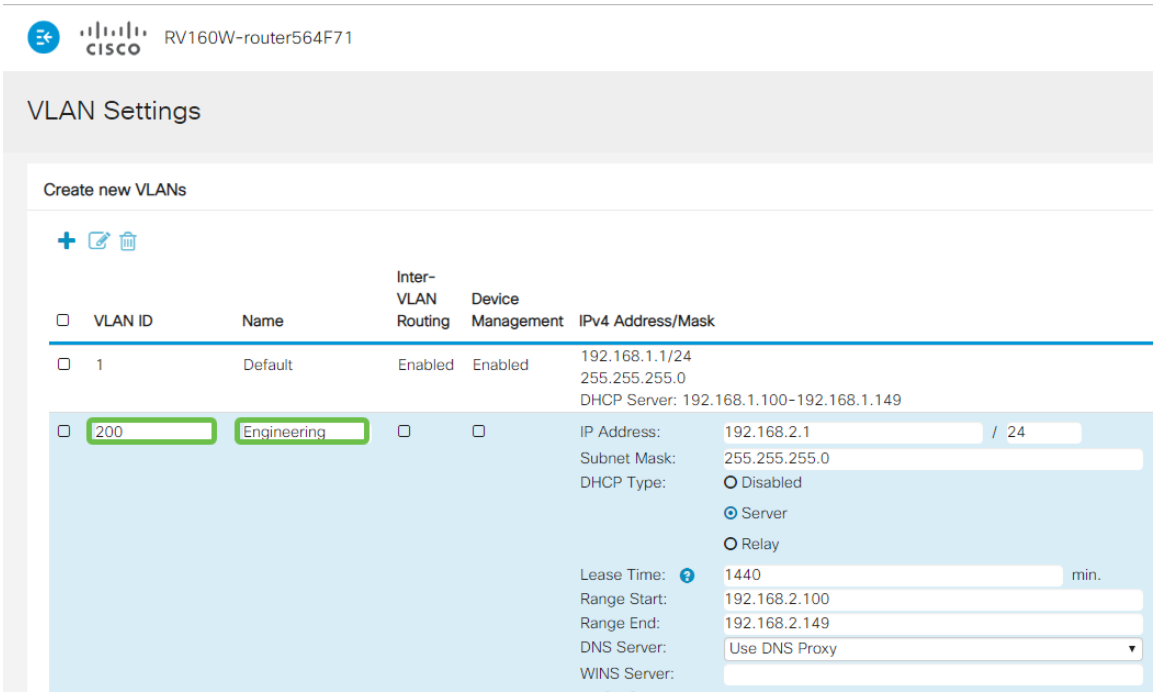
Klik op **Add** om een nieuw VLAN te maken.



Stap 3

Voer de *VLAN-id in* die u wilt maken en een *naam*. Het *VLAN ID* bereik loopt van 1-4093.

We zijn **200** ingevoerd als onze *VLAN-id* en **techniek** als *naam* voor VLAN.



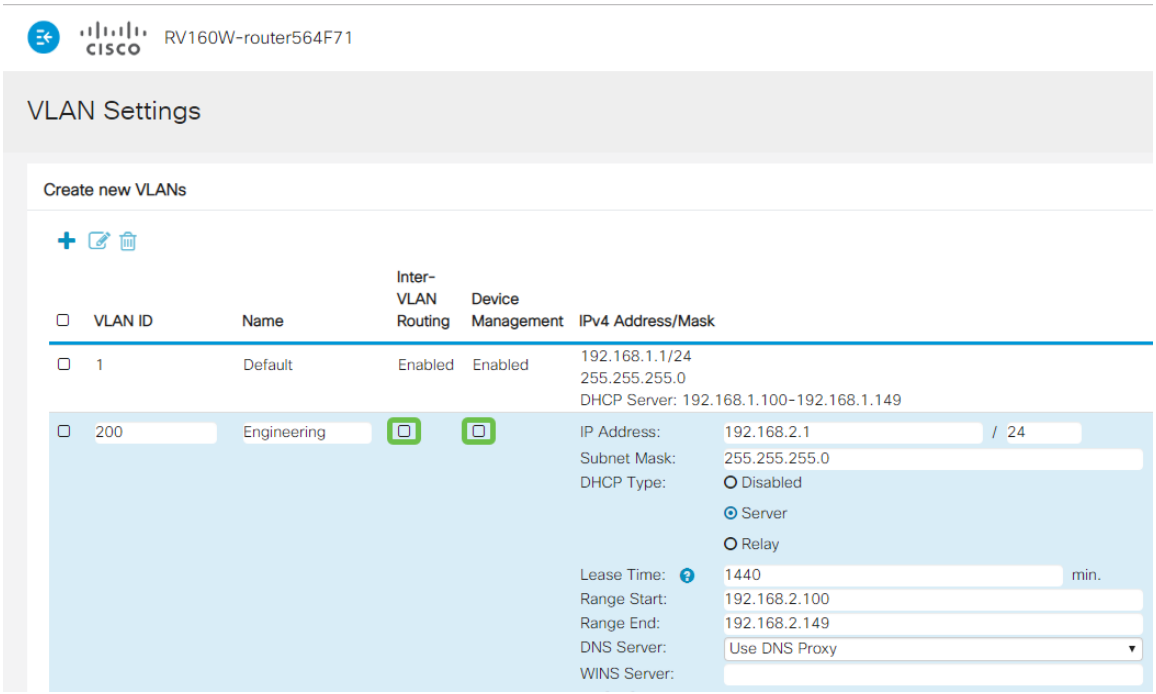
Stap 4

Schakel het vakje *Enabled* uit voor zowel *Inter-VLAN-routing* en *apparaatbeheer* indien gewenst.

De routing tussen VLAN's wordt gebruikt om pakketten van één VLAN naar een ander VLAN te verzenden. In het algemeen, wordt dit niet aanbevolen voor gastnetwerken aangezien u gastgebruikers zult willen isoleren het VLANs minder veilig verlaat. Er zijn tijden wanneer het voor VLAN's nodig kan zijn om tussen elkaar te leiden. Als dit het geval is, moet u de routing tussen VLAN's op een RV34x-router met gerichte ACL-beperkingen controleren om specifiek verkeer te configureren dat u tussen VLAN's toestaat.

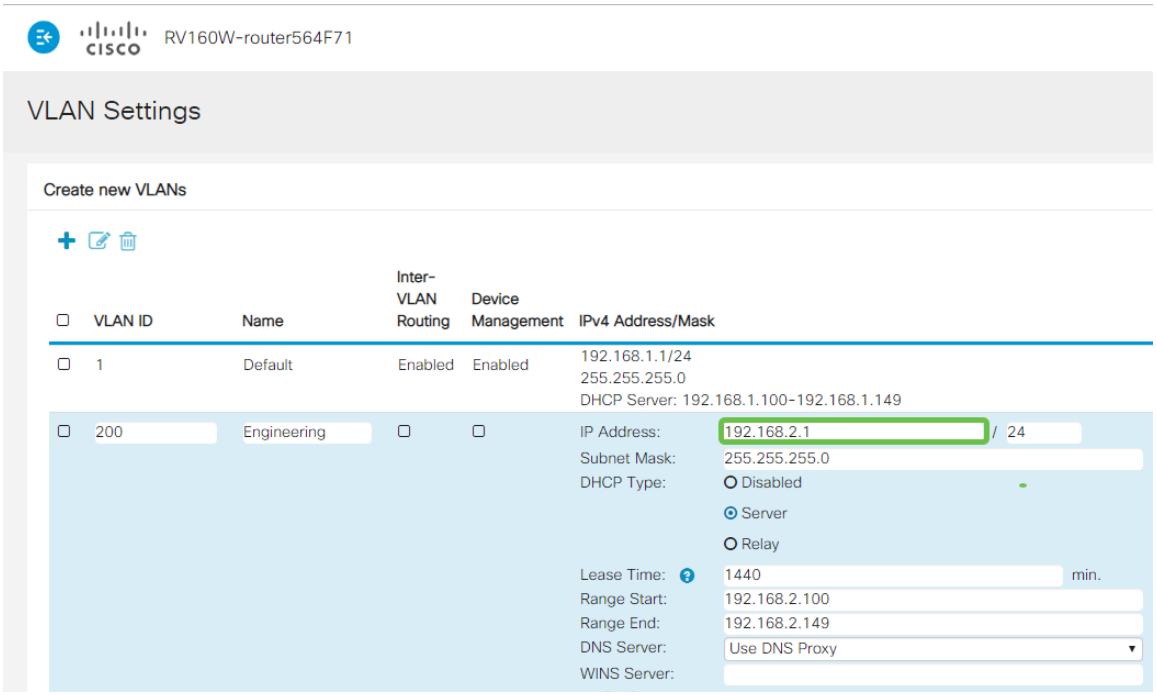
Apparaatbeheer is de software waarmee u uw browser kunt gebruiken om in de Web UI van de RV260P, van het VLAN te loggen en de RV260P te beheren. Dit moet ook worden uitgeschakeld op Guest-netwerken.

In dit voorbeeld, maakten we noch de *Inter-VLAN routing* of het *apparaatbeheer* mogelijk om het VLAN veiliger te houden.



Stap 5

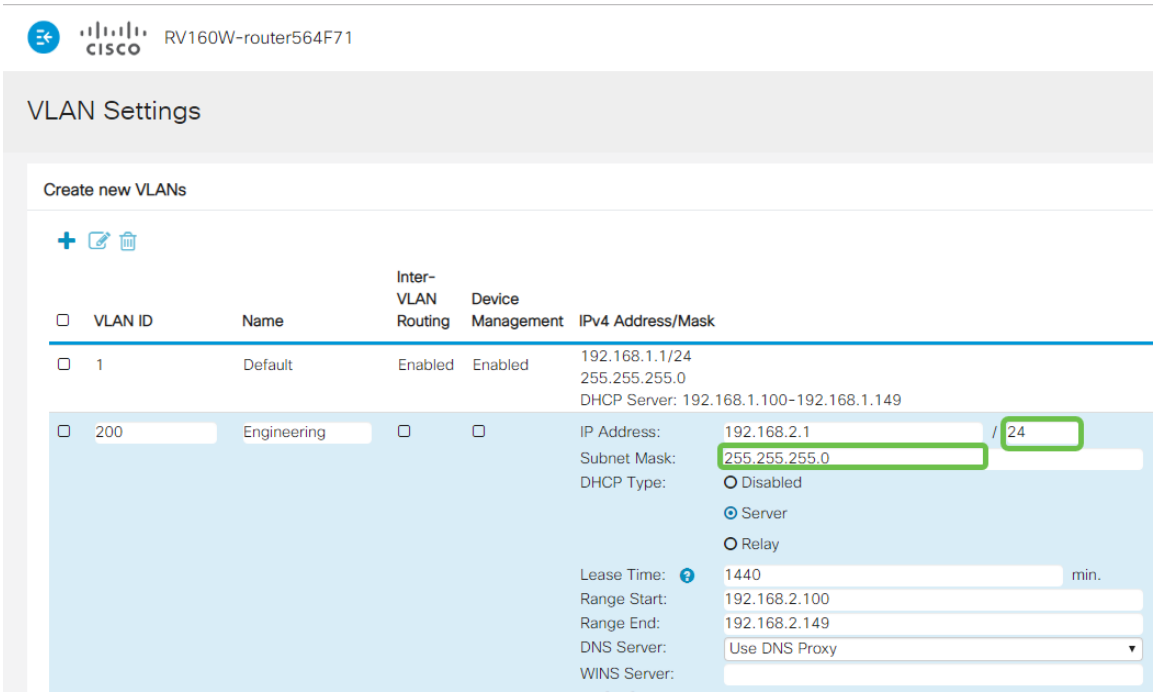
Het particuliere IPv4-adres wordt automatisch ingevuld in het veld *IP-adres*. U kunt dit aanpassen als u kiest. In dit voorbeeld, heeft Subnet 192.168.2.100-192.168.2.149 IP adressen beschikbaar voor DHCP. 192.168.2.1-192.168.2.99 en 192.168.2.150-192.168.2.254 zijn beschikbaar voor statische IP-adressen.



Stap 6

Het subnetmasker onder *Subnet Mask* zal automatisch bevolken. Als u wijzigingen aanbrengt, wordt het veld automatisch aangepast.

Voor deze demonstratie verlaten we het *Subnetmasker* als **255.255.255.0** of **/24**.



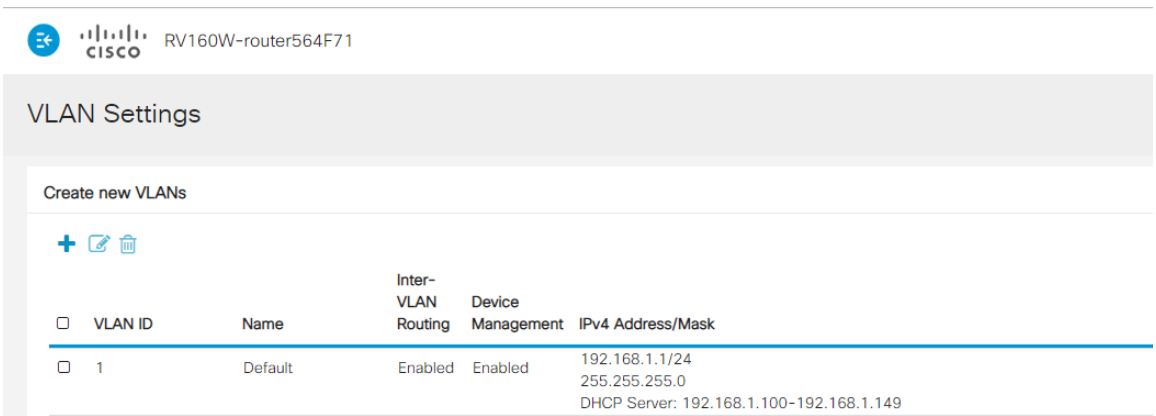
Stap 7

Selecteer een *type Dynamic Host Configuration Protocol (DHCP)*. De volgende opties zijn:

Uitgeschakeld - Hiermee wordt de DHCP IPv4 server op VLAN uitgeschakeld. Dit wordt aanbevolen in een testomgeving. In dit scenario zouden alle IP-adressen handmatig moeten worden geconfigureerd en alle communicatie zou intern zijn.

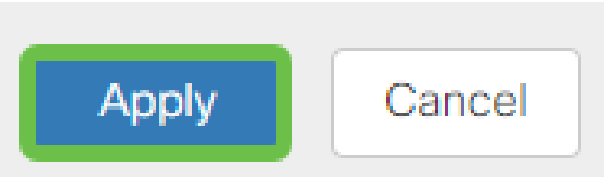
Server - Dit is de meest gebruikte optie.

- Begintijd - Voer een tijdwaarde van 5 tot 43.200 minuten in. De standaardinstelling is 1440 minuten (gelijk aan 24 uur).
- Einde bereik en bereik - Voer het begin en einde van IP-adressen in die dynamisch kunnen worden toegewezen.
- DNS-server - Selecteer deze optie om de DNS-server als proxy of ISP te gebruiken in de vervolgkeuzelijst.
- WINS Server - Voer de naam van de WINS-server in.
- DHCP-opties:
    - Optie 66 - Voer het IP-adres van de TFTP-server in.
    - Optie 150 - Voer het IP-adres in van een lijst met TFTP-servers.
    - Optie 67 - Voer de configuratiebestandsnaam in.
- Relay - Voer het IPv4-adres van de externe DHCP-server in om de DHCP-relais te configureren. Dit is een geavanceerdere configuratie.



Stap 8

Klik op **Toepassen** om het nieuwe VLAN te maken.



VLAN's aan poorten toewijzen

16 VLAN's kunnen op RV260 worden geconfigureerd, met één VLAN voor het WAN (Wide Area Network). VLAN's die niet op een poort staan, moeten worden *uitgesloten*. Dit houdt het verkeer op die haven uitsluitend voor VLAN/VLANs aan de specifiek toegewezen gebruiker. Het wordt als een goede praktijk beschouwd.

Poorten kunnen worden ingesteld als een Access Port of een Trunk-poort:

- Access Port - toegewezen één VLAN. Niet-gelabelde frames worden doorgegeven.
- Trunk-poort - Kan meer dan één VLAN dragen. 802,1q. Trunking maakt het mogelijk om een inheems VLAN niet te labelen. VLAN's die u niet op de Trunk wilt gebruiken, moeten worden uitgesloten.

Eén VLAN heeft zijn eigen poort toegewezen:

- Wordt beschouwd als een toegangspoort.
- Het VLAN dat aan deze poort wordt toegewezen moet worden geëtiketteerd Untagged.
- Alle andere VLAN's moeten voor die poort zijn uitgesloten.

Twee of meer VLAN's die één poort delen:

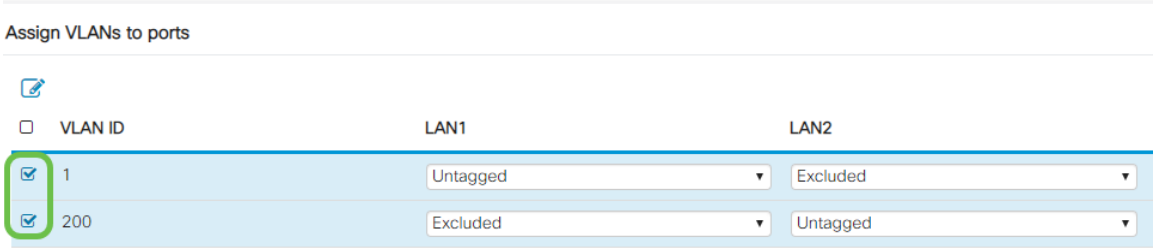
- Wordt beschouwd als een Trunk-poort.
- Eén van de VLAN's kan worden aangeduid als Untagged.
- De rest van de VLAN's die deel uitmaken van de Trunk-poort moet van een label zijn voorzien.
- VLAN's die geen deel uitmaken van de Trunk-poort moeten van een etiket worden voorzien dat voor die poort is uitgesloten.

Opmerking: In dit voorbeeld zijn er geen stammen.

Stap 9

Selecteer de *VLAN-ID's* die u wilt bewerken. Klik op Edit (Bewerken).

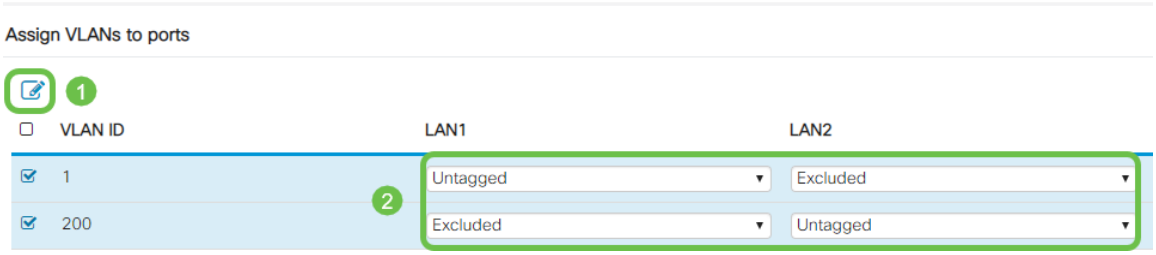
In dit voorbeeld, hebben we *VLAN 1* en *VLAN 200* geselecteerd.



Stap 10

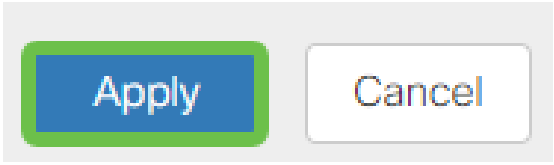
Klik op **Bewerken** om een VLAN aan een LAN poort toe te wijzen en specificeer elke instelling als *Bijgesneden*, *niet gelabeld* of *uitgesloten*.

In dit voorbeeld, op LAN1 hebben we VLAN 1 als **Untagged** en VLAN 200 toegewezen als **Uitgesloten**. Voor LAN2 hebben we VLAN 1 als **Uitgesloten** en VLAN 200 als **Untagged** toegewezen.



Stap 11

Klik op **Toepassen** om de configuratie op te slaan.



U zou nu met succes een nieuw VLAN moeten hebben gemaakt en geconfigureerd VLAN's in poorten op RV260. Herhaal het proces om de andere VLAN's te maken. Bijvoorbeeld, VLAN300 zou voor het op de markt brengen met een netto van 192.168.3.x en VLAN400 worden gemaakt voor Boekhouding met een netto van 192.168.4.x.

Dat is de basis van VLAN's. Klik op de hyperlink om meer over de beste praktijken van VLAN en de Tips van de Beveiliging voor het Zaken van Cisco Routers te leren.

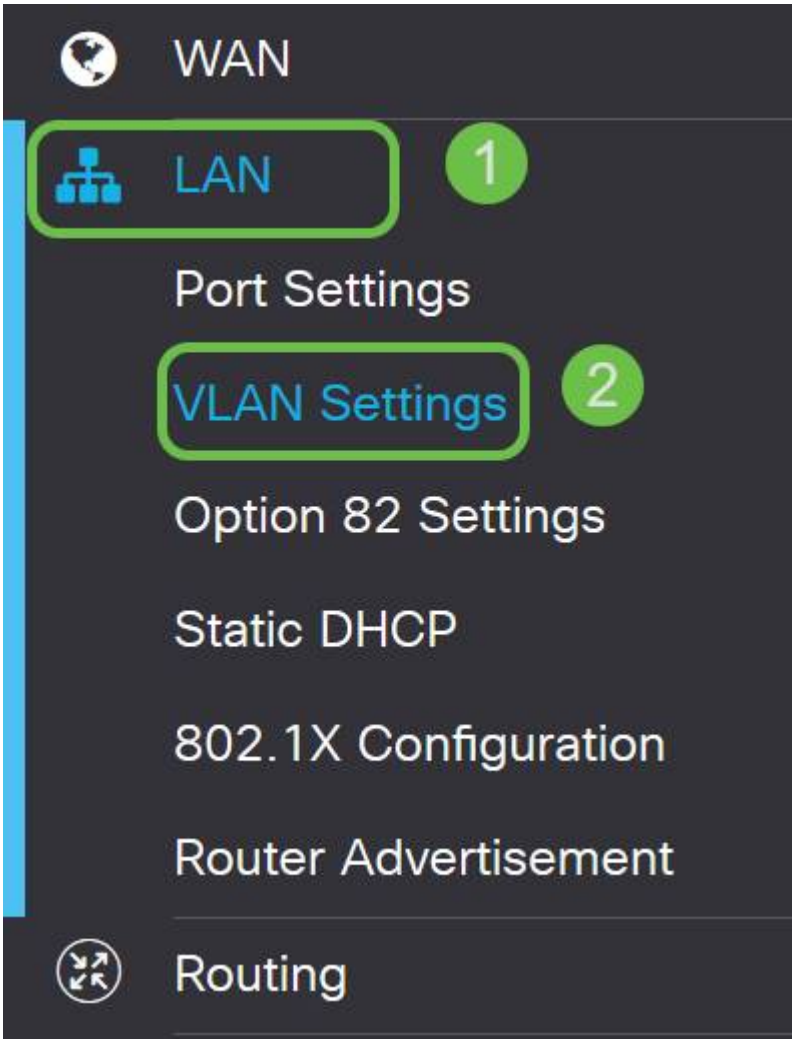
Een IP-adres bewerken (optioneel)

Na het voltooien van de *wizard* van de *Eerste installatie* kunt u een statisch IP-adres op de router instellen door de VLAN-instellingen te bewerken. Als u de wizard voor de eerste installatie opnieuw wilt uitvoeren, volgt u de onderstaande stappen om deze wijziging uit te voeren.

Als u geen IP-adres hoeft te bewerken, kunt u naar de volgende sectie van dit artikel gaan.

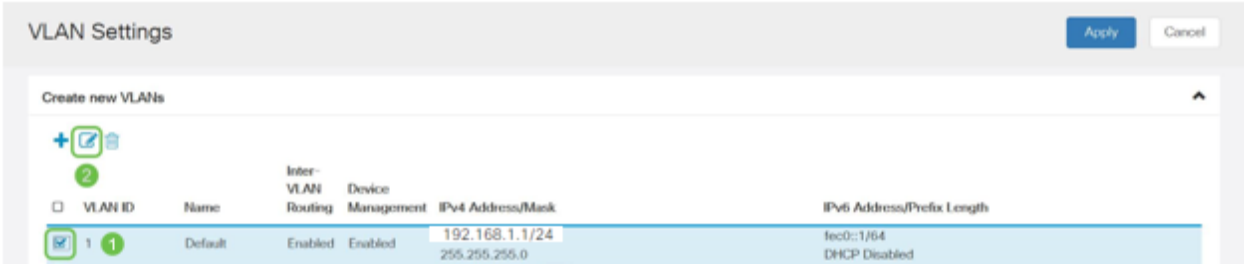
Stap 1

Klik in de linker menu-balk op **LAN > VLAN-instellingen**.



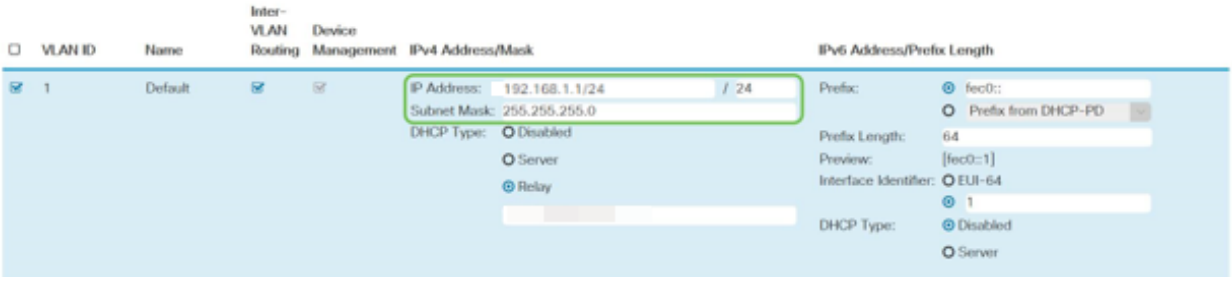
Stap 2

Selecteer vervolgens het **VLAN** dat uw routeringsapparaat bevat, en klik vervolgens op het **pictogram bewerken**.



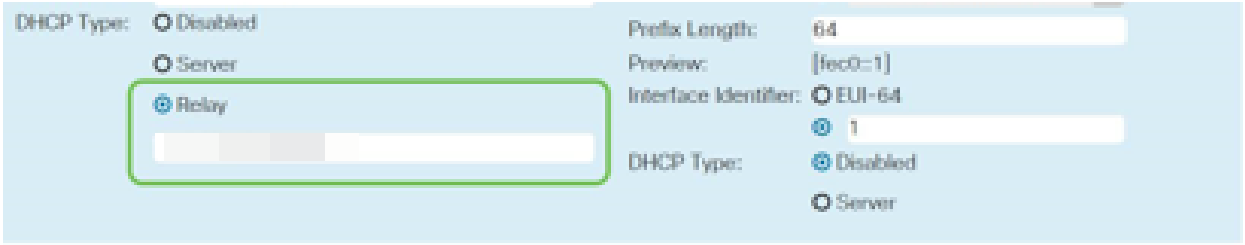
Stap 3

Voer uw gewenste **statische IP-adres in** en klik op **Toepassen** in de rechterbovenhoek.



Stap 4 (optioneel)

Als uw router niet de server/het apparaat van DHCP is die IP adressen toewijst, kunt u de eigenschap van DHCP Relay gebruiken om DHCP-verzoeken aan een specifiek IP adres te richten. Het IP-adres is waarschijnlijk de router die is aangesloten op WAN/Internet.



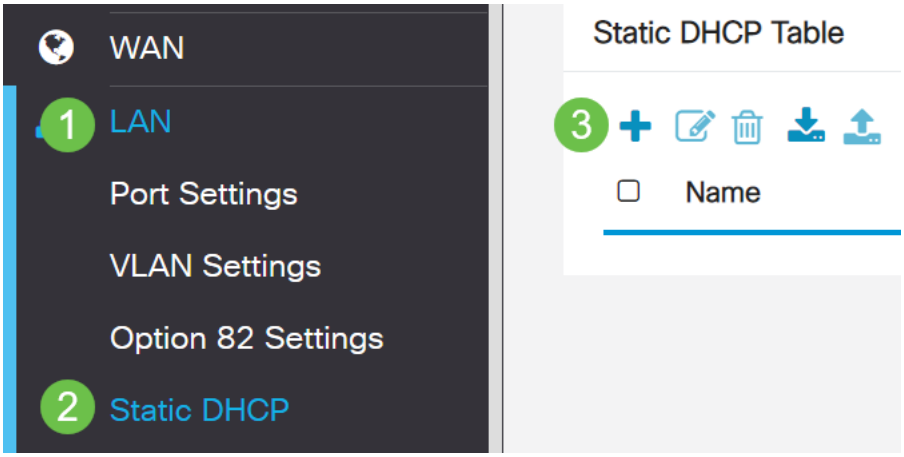
Een statische IP toevoegen

Als u wilt dat een bepaald apparaat bereikbaar is voor andere VLAN's, kunt u dat apparaat een statisch lokaal IP-adres geven en een toegangsregel maken om het toegankelijk te maken. Dit werkt alleen als de routing tussen VLAN's is ingeschakeld. Er zijn andere situaties waarin een statische IP nuttig kan zijn. Voor meer informatie over het instellen van statische IP-adressen, controleer beste praktijken voor het instellen van statische IP-adressen op Cisco Business Hardware.

Als u geen statisch IP-adres hoeft toe te voegen, kunt u naar de volgende sectie van dit artikel bewegen om de Access Point te configureren.

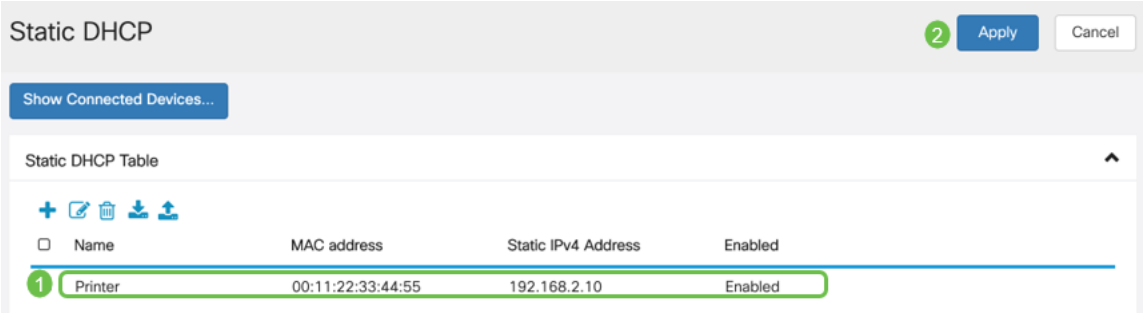
Stap 1

Navigeer naar **LAN > Statische DHCP.** Klik op het **pictogram plus**.



Stap 2

Voeg de **Statische DHCP-**informatie voor het apparaat toe. In dit voorbeeld is het apparaat een printer.



Gefeliciteerd, hebt u de configuratie van uw RV260P router voltooid. We zullen nu uw Cisco Business Wireless-apparaten configureren.

CBW140AC configureren

CBW140AC uit het vak

Start door een Ethernet-kabel van de PoE-poort op uw CBW140AC te aansluiten op een PoE-poort op de RV260P. De eerste 4 poorten op de RV260P kunnen PoE leveren, zodat alle poorten ook gebruikt kunnen worden.

Controleer de status van het indicatielampje. Het toegangspunt duurt ongeveer 10 minuten om te beginnen. De LED knippert groen in meerdere patronen, wisselend snel door groen, rood en amber voordat hij weer groen wordt. Er kunnen kleine verschillen zijn in de LED-kleurintensiteit en -tint, van eenheid tot eenheid. Wanneer het LED-licht groen knippert, gaat u naar de volgende stap.

De PoE Ethernet uplink-poort op de Primaire AP kan ALLEEN worden gebruikt om een uplinks op het LAN te bieden en NIET om verbinding te maken met andere Primaire geschikt of booster-extenders.

Als uw toegangspunt niet nieuw is, uit het vak, zorg er dan voor dat deze is teruggezet op de standaardinstellingen van de fabriek voor de SSID *van Cisco Business Setup* om in uw Wi-Fi-opties te tonen. Kijk voor assistentie hierbij hoe u de software opnieuw kunt opstarten en terugzetten op fabrieksinstellingen op RV260-routers.

Stel het 140AC primaire draadloze access point in op de web UI

U kunt het access point instellen met behulp van de mobiele toepassing of de web UI. Dit artikel gebruikt het Web UI voor opstelling, wat meer opties voor configuratie geeft maar wat gecompliceerder is. Als u de mobiele applicatie voor de volgende secties wilt gebruiken, klikt u op de mobiele applicatie instructies.

Als u problemen hebt met het aansluiten, raadpleegt u het gedeelte Tips voor draadloze probleemoplossing van dit artikel.

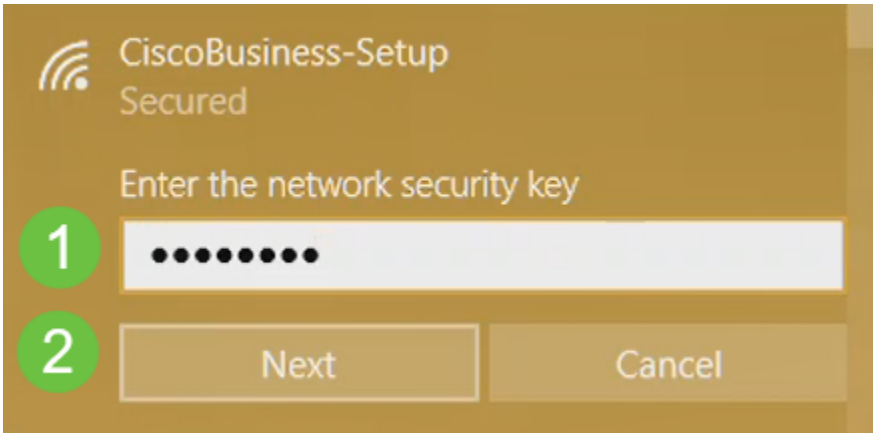
Stap 1

Klik op uw pc op het **Wi-Fi-pictogram** en kies *Cisco Business-Setup* draadloze netwerken. Klik op Connect.

Als uw toegangspunt niet nieuw is, uit het vak, zorg er dan voor dat deze is teruggezet op de standaardinstellingen van de fabriek voor de SSID *van Cisco Business Setup* om in uw Wi-Fi-opties te tonen.

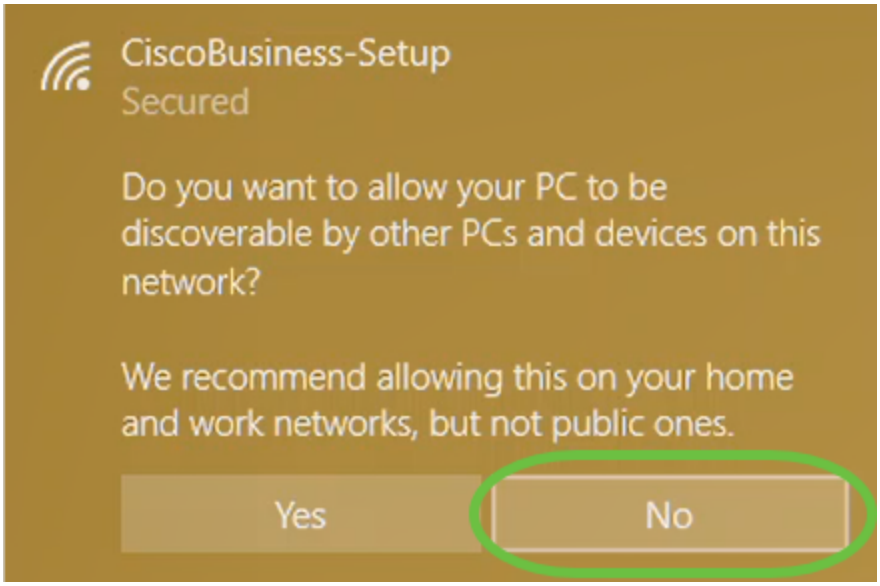
Stap 2

Typ het wachtwoord **cisco123** en klik op **Volgende**.



Stap 3

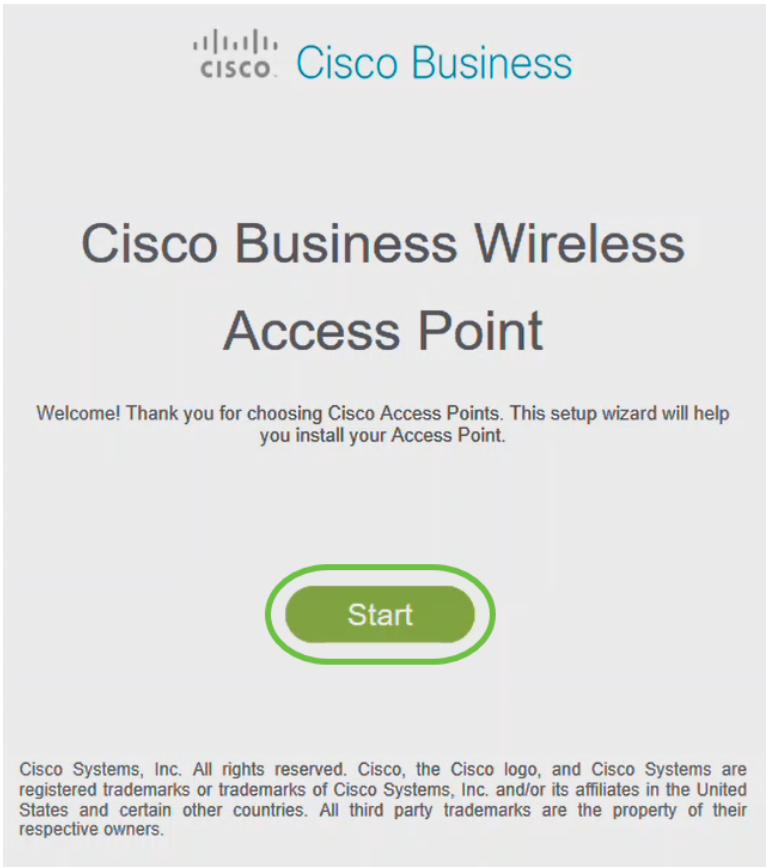
U krijgt het volgende scherm. Aangezien u slechts één apparaat tegelijkertijd kunt configureren klikt u op **Nee**.



Slechts één apparaat kan met de SSID *van Cisco Business Setup* worden verbonden. Als een tweede apparaat probeert verbinding te maken, kan dit niet. Als u geen verbinding kunt maken met SSID en het wachtwoord hebt gevalideerd, kan een ander apparaat de verbinding hebben gemaakt. Start het AP opnieuw en probeer het opnieuw.

Stap 4

Nadat het netwerk is aangesloten, dient de webbrowser automatisch te richten naar de setup-wizard van CBW AP. Als dit niet het geval is, opent u een webbrowser, zoals Internet Explorer, Firefox, Chrome of Safari. Typ in de adresbalk **http://ciscobusiness.cisco** en druk op **ENTER**. Klik op **Start** op de webpagina.



Als de webpagina niet wordt weergegeven, wacht dan nog een paar minuten of laad de

pagina opnieuw. Na deze eerste instelling gebruikt u https://ciscobusiness.cisco om in te loggen. Als uw webbrowser automatisch met *http://* vult, moet u handmatig typen in de *https://* om toegang te krijgen.

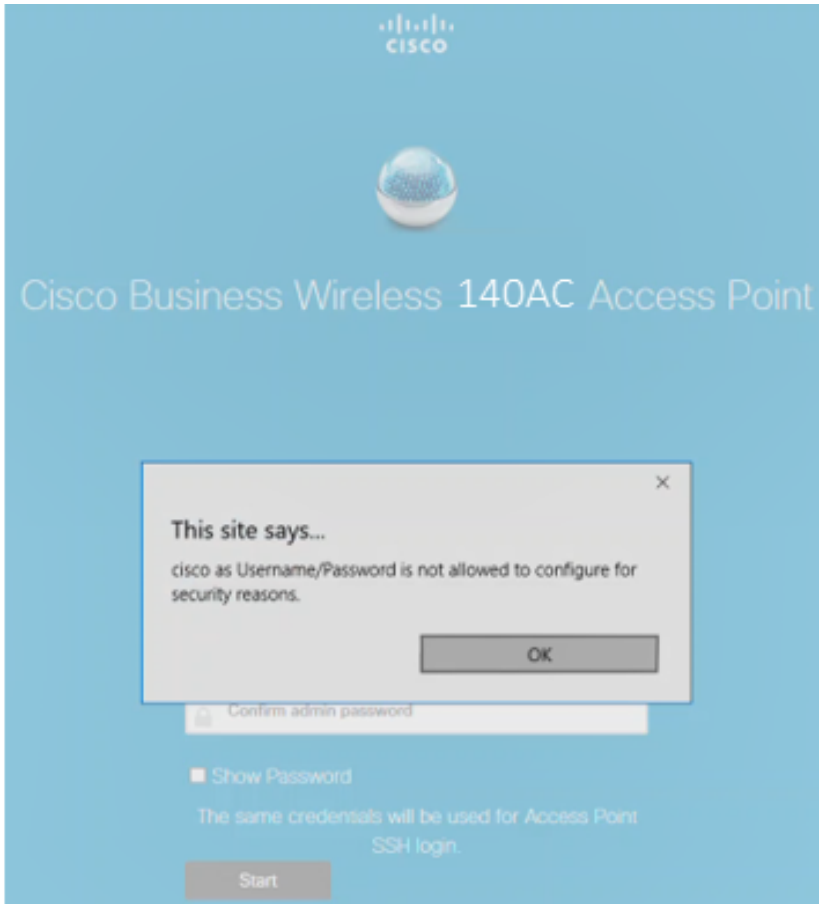
Stap 5

Maak een *admin-account* door het volgende in te voeren:

- Gebruikersnaam beheren (maximaal 24 tekens)
- Wachtwoord beheren
- Wachtwoord voor beheerder bevestigen

U kunt ervoor kiezen het wachtwoord weer te geven door het vakje naast *Wachtwoord* te controleren. Klik op **Start**.

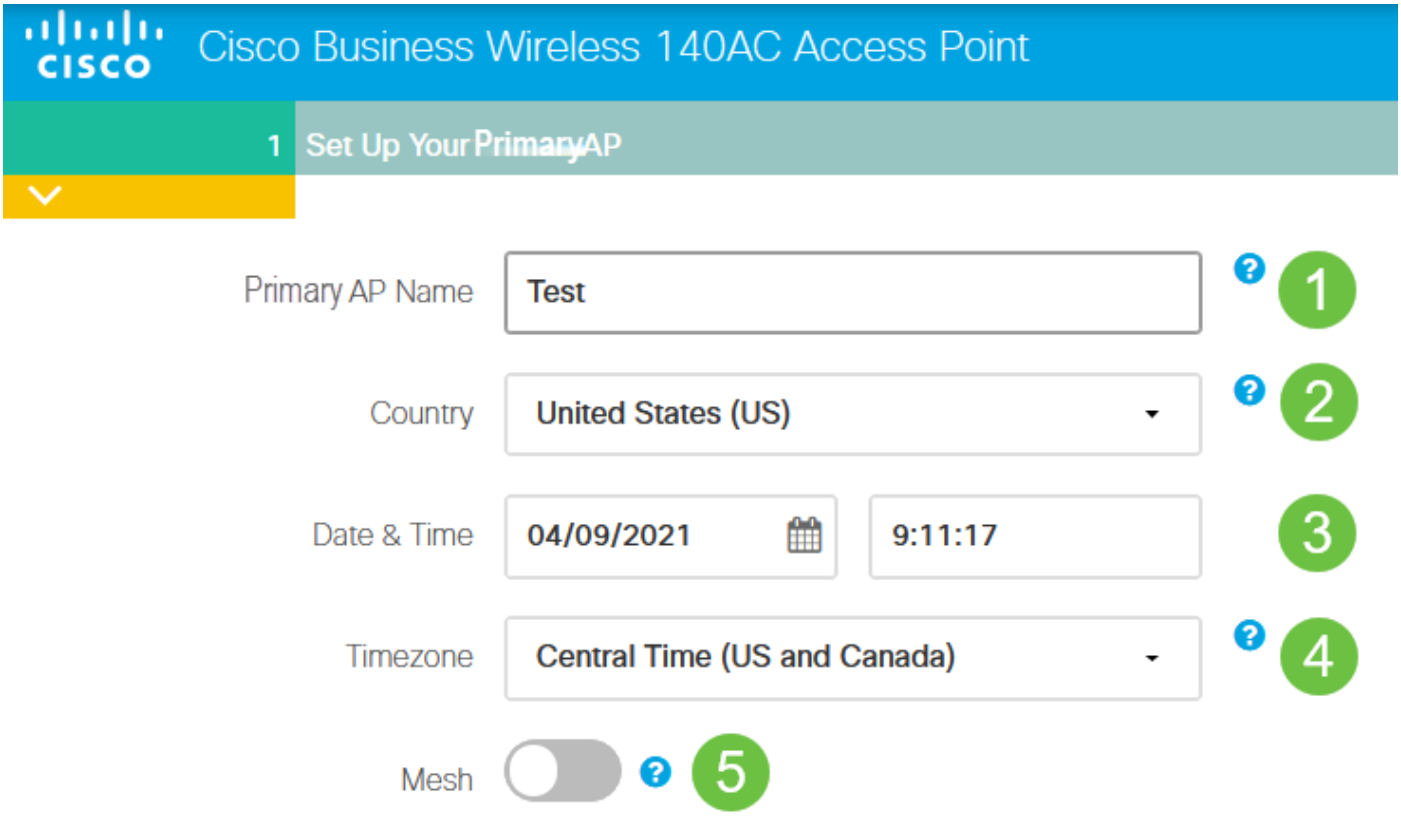
Gebruik *cisco* niet, of variaties ervan in de gebruikers- of wachtwoordvelden. Als u dit wel doet, ontvangt u een foutmelding zoals hieronder wordt weergegeven.



Stap 6

Stel uw primaire AP in door het volgende in te voeren:

- Primaire AP-naam
- Land
- Datum en tijd
- Tijdzone
- mesh



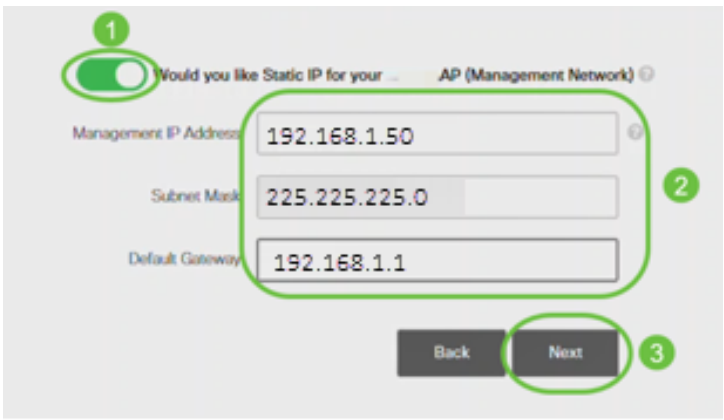
mesh zou alleen ingeschakeld moeten worden als u een netwerk wilt maken. Standaard is het uitgeschakeld.

Stap 7

(Optioneel) U kunt *Static IP* inschakelen *voor uw* CBW140AC-beheerdoeleinden. Als niet, krijgt de interface een IP adres van uw DHCP-server. U kunt statische IP als volgt configureren:

- IP-adres beheer
- Subnetmasker
- Standaard gateway

Klik op **Volgende**.



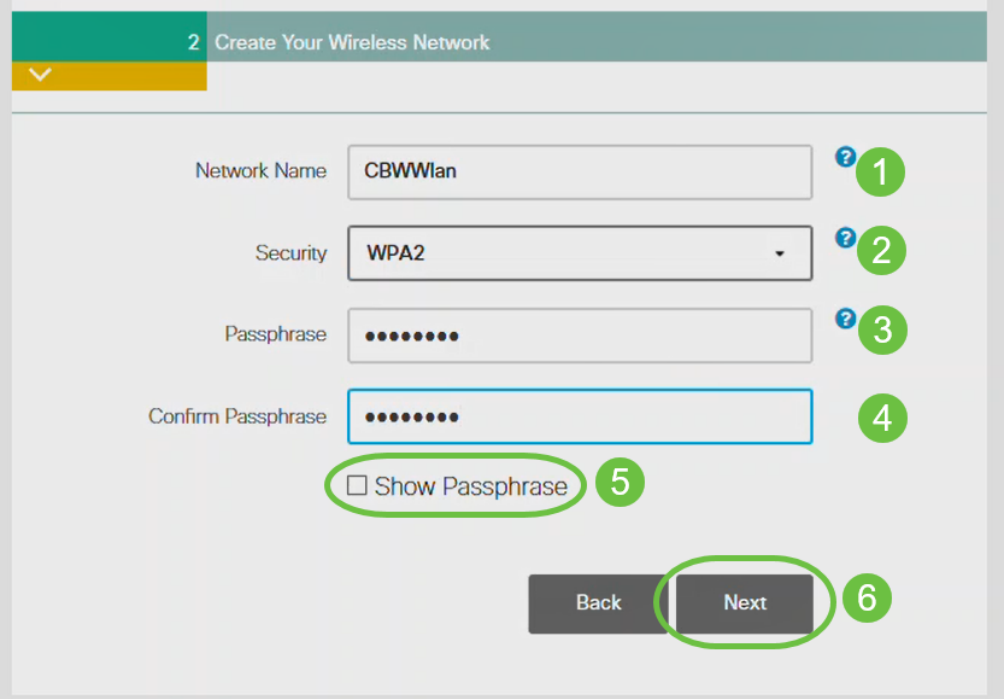
Deze optie is standaard uitgeschakeld.

Stap 8

Maak uw draadloze netwerken door het volgende in te voeren:

- Netwerknaam
- Kies veiligheid
- Wachtwoord
- Wachtwoord bevestigen
- (Optioneel) Controleer het selectieteken om wachtwoord weer te geven.

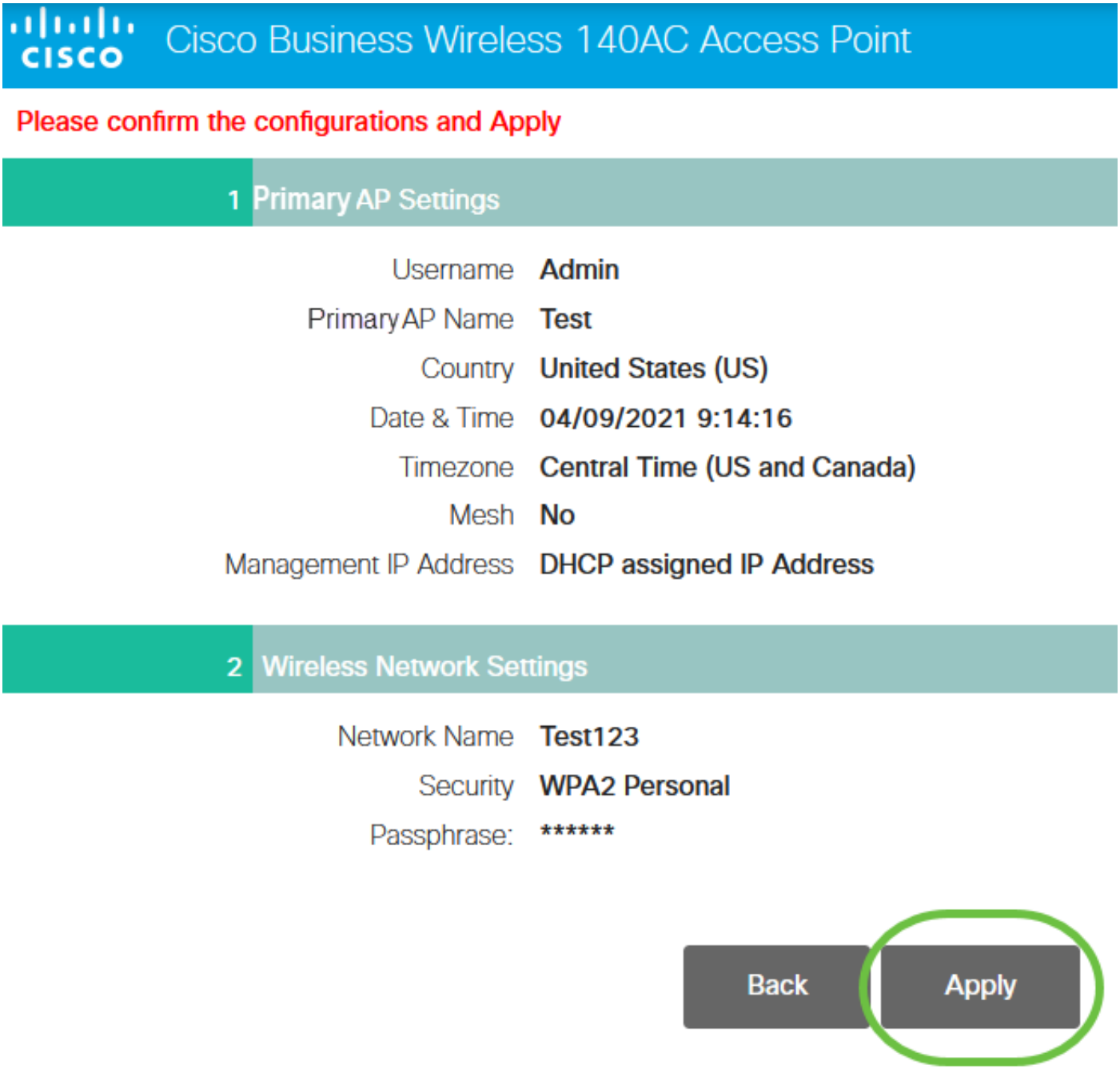
Klik op **Volgende**.



Wi-Fi Secure Access (WAP) versie 2 (WAP2) is de huidige standaard voor Wi-Fi-beveiliging.

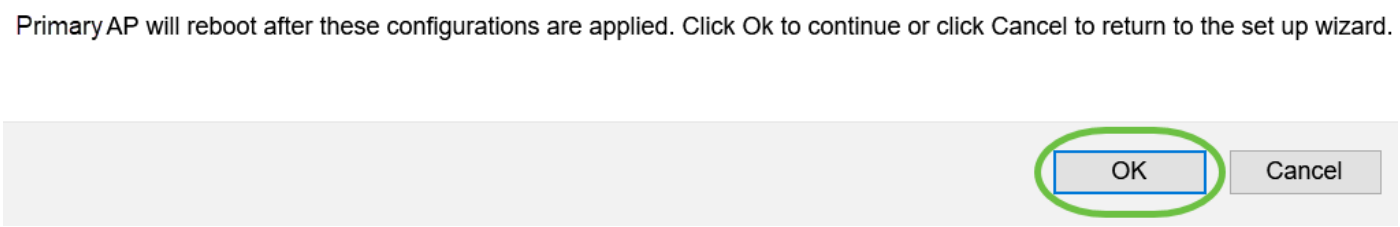
Stap 9

Bevestig de instellingen en klik op **Toepassen**.

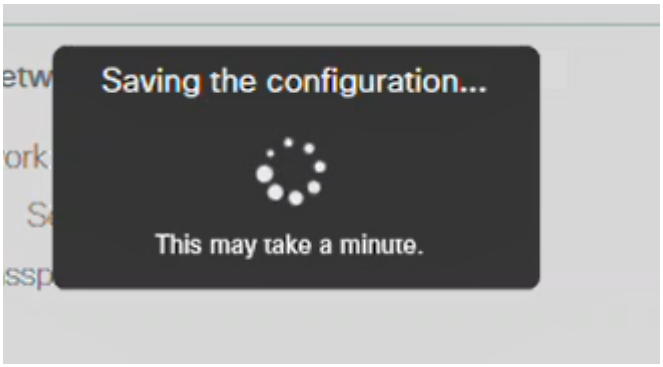


Stap 10

Klik op **OK** om de instellingen toe te passen.



U ziet het volgende scherm terwijl de configuraties worden opgeslagen en het systeem wordt herstart. Dit kan 10 minuten duren.

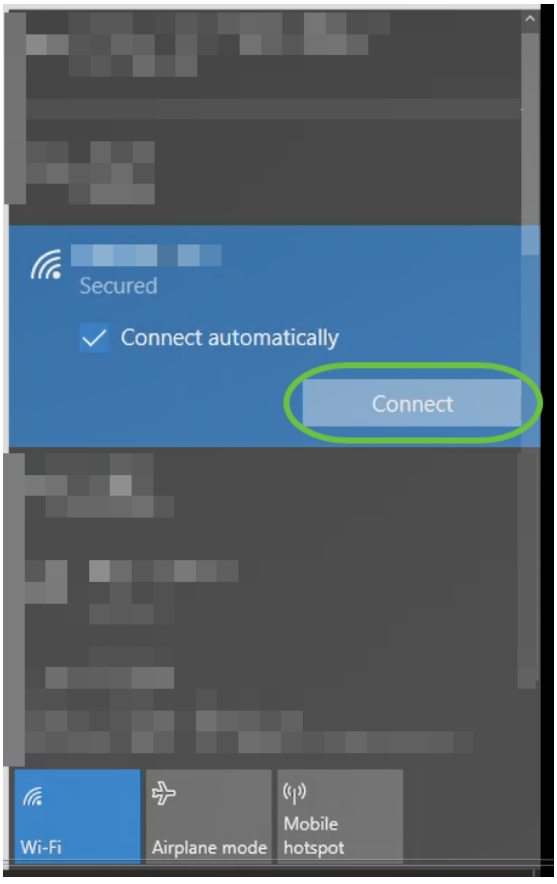


Tijdens het opnieuw opstarten, gaat de LED in het access point door meerdere kleurpatronen. Wanneer de LED groen knippert, gaat u naar de volgende stap. Als de LED niet voorbij het rode knipperpatroon komt, geeft dit aan dat er geen DHCP-server in uw netwerk is. Zorg ervoor dat AP op een switch of een router met een DHCP server wordt aangesloten.

Stap 11

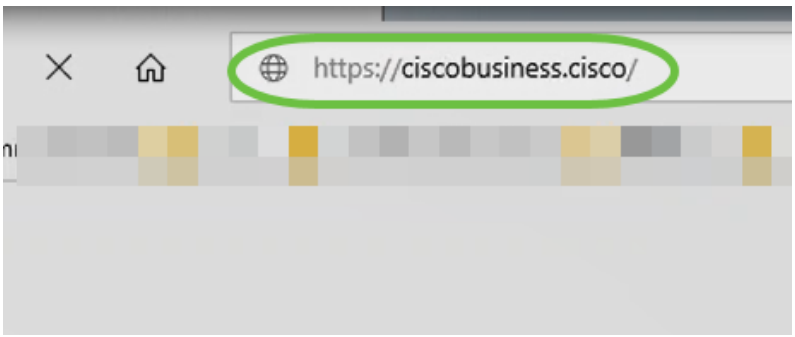
Ga naar de draadloze opties op uw pc en kies het netwerk dat u hebt ingesteld. Klik op **Connect**.

De SSID *van Cisco Business Setup* wordt na de herstart verdwijnt.



Stap 12

Open een webbrowser en type in *https://[IP-adres van het CBW AP]*. In plaats hiervan kunt u ook *https://ciscobusiness.cisco* typen in de adresbalk en op ingedrukt houden.



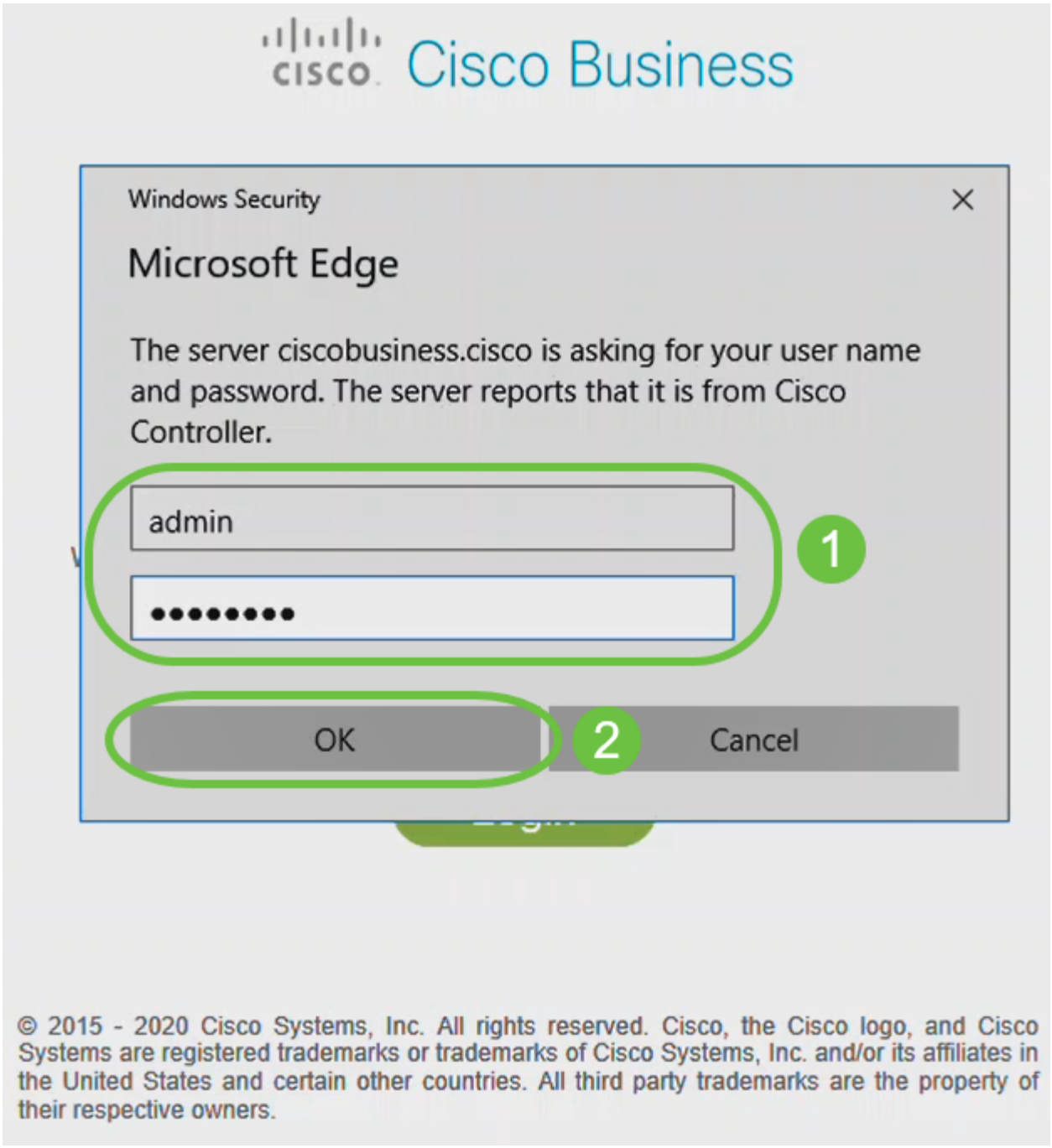
Zorg ervoor dat u *https* typt en niet *http* bij deze stap.

Stap 13

Klik op **Aanmelden**.

Stap 14

Meld u aan met behulp van de ingestelde aanmeldingsgegevens. Klik op OK.



Stap 15

U hebt toegang tot de webpagina UI van het AP.

Tips voor draadloze probleemoplossing

Als u problemen hebt, raadpleegt u de volgende tips:

- Zorg ervoor dat de juiste Service Set-id (SSID) is geselecteerd. Dit is de naam die je maakte voor het draadloze netwerk.
- Koppel VPN los van de app of op een laptop. Mogelijk bent u zelfs verbonden met een VPN dat uw mobiele serviceprovider gebruikt en dat u misschien niet eens weet. Een Android-telefoon (Pixel 3) met Google Fi als serviceprovider is er bijvoorbeeld een ingebouwde VPN die automatisch verbonden is zonder kennisgeving. Dit moet worden uitgeschakeld om de primaire AP te vinden.
- Log in op de primaire AP met https://<IP adres van de primaire AP>.
- Zodra u de eerste instelling hebt uitgevoerd, dient u zeker te zijn dat https:// is wordt gebruikt of u zich in *ciscobusiness.cisco* vastlegt of door het IP-adres in uw webbrowser in te voeren. Afhankelijk van uw instellingen is het mogelijk dat de computer automatisch gevuld is met http:// since dat is wat u de eerste keer dat u inlogde hebt gebruikt.
- Om te helpen met problemen die te maken hebben met de toegang tot Web UI of browser problemen tijdens het gebruik van het AP, klik in de web browser (in dit geval Firefox) op het Open menu, ga naar Help > Informatie voor probleemoplossing en klik op Vernieuwen Firefox.

Configuratie van CBW142ACM mesh-extenders met behulp van de WebUI

U bevindt zich in het beginpunt van het opzetten van dit netwerk, u hoeft alleen de extenders van het netwerk toe te voegen!

Stap 1

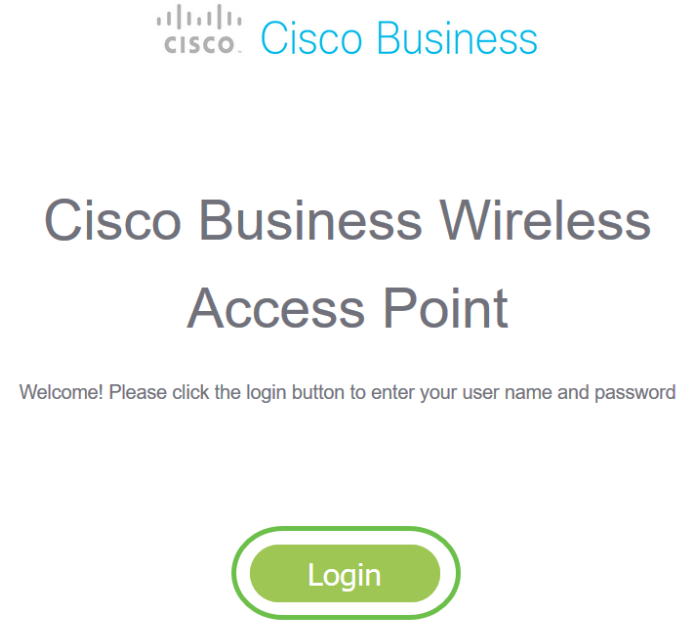
Steek de twee mesh-extenders in de muur op de geselecteerde locaties. Schrijf het MAC-adres van elke mesh-extender op.

Stap 2

Wacht ongeveer 10 minuten voordat de mesh-extenders beginnen.

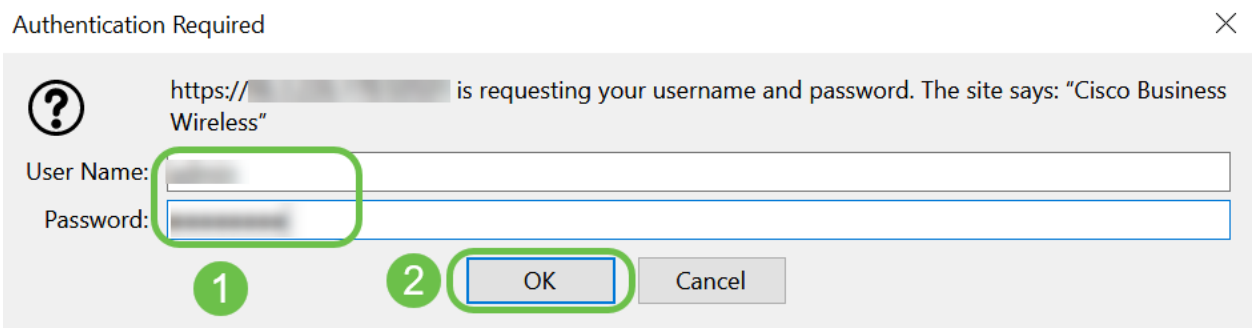
Stap 3

Voer het IP-adres van Primaire Access Point (AP's) in op de webbrowser. Klik op **Aanmelden** om toegang te krijgen tot de primaire AP.



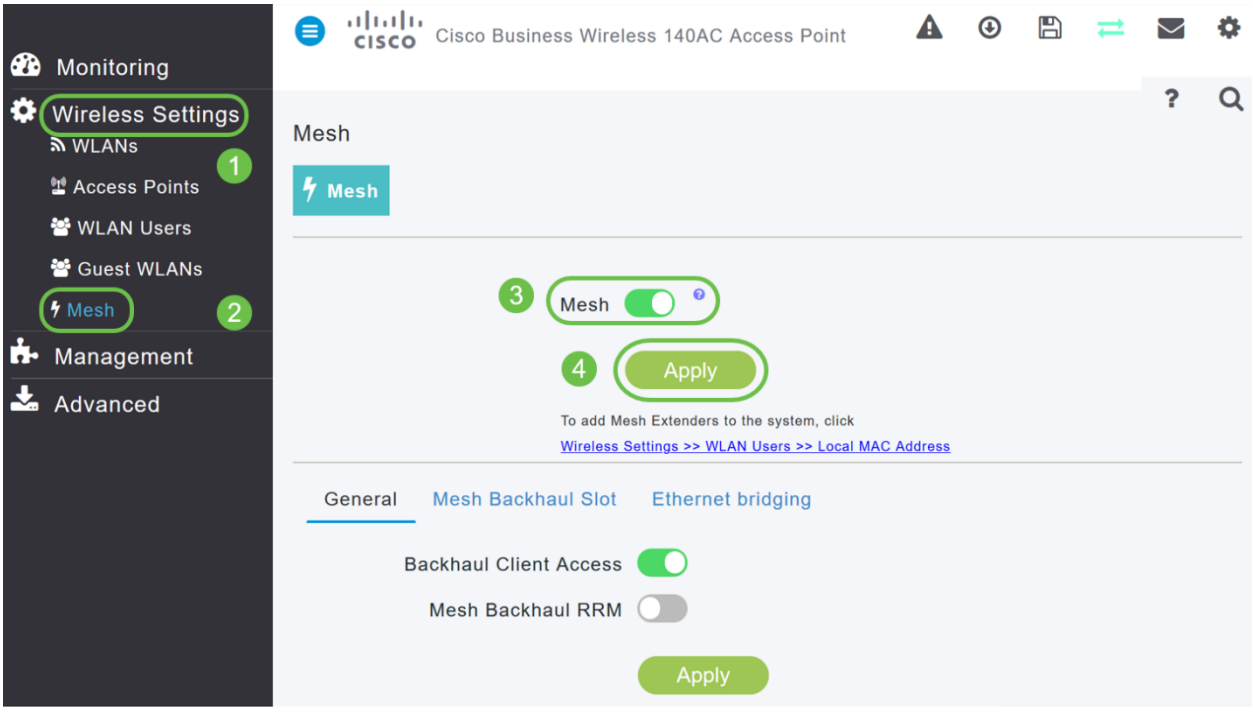
Stap 4

Voer uw gebruikersnaam en *wachtwoord in* om toegang tot de primaire AP te krijgen. Klik op OK.



Stap 5

Navigeer naar **draadloze instellingen > mesh**. Controleer of het *mesh* is ingeschakeld. Klik op Apply (Toepassen).

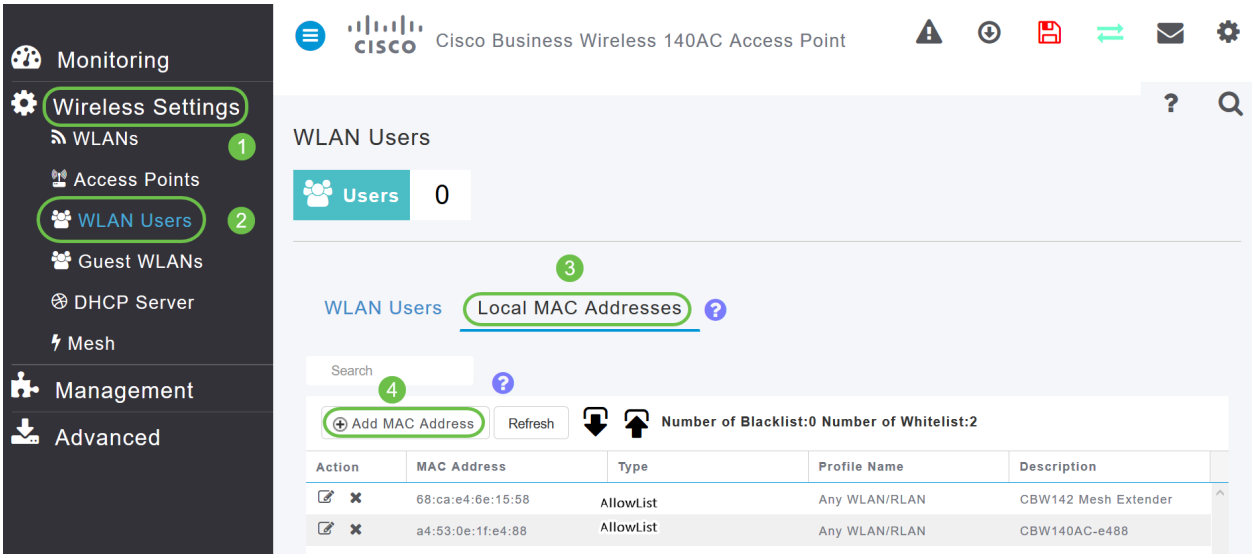


Stap 6

Als Mesh nog niet is ingeschakeld, moet WAP misschien opnieuw worden opgestart. Er verschijnt een pop-up die de computer opnieuw opstart. Bevestig. Dit duurt ongeveer 10 minuten. Tijdens een herstart knippert de LED groen in meerdere patronen, waarbij deze snel groen, rood en amber doorgaat voordat u weer groen wordt. Er kunnen kleine verschillen zijn in de LED-kleurintensiteit en -tint, van eenheid tot eenheid.

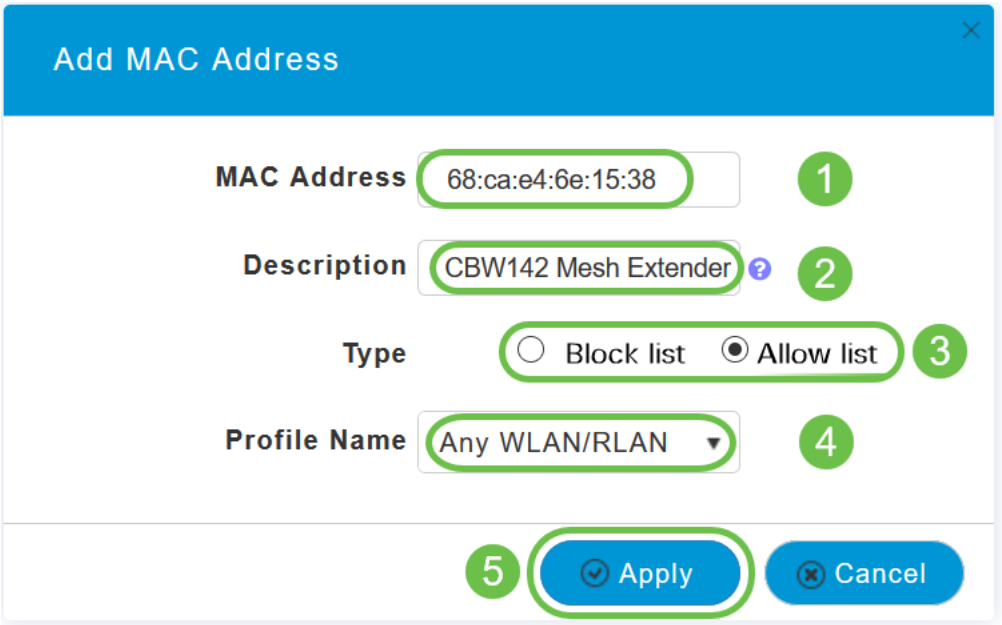
Stap 7

navigeren naar **draadloze instellingen > WLAN-gebruikers > lokale MAC-adressen**. Klik op **MAC-adres toevoegen**.



Stap 8

Voer het MAC-adres en de beschrijving van de mesh-extender in. Selecteer het *Type* zoals toestaan in de lijst. Selecteer de *profielnaam* in het vervolgkeuzemenu. Klik op Apply (Toepassen).



Stap 9

Vergeet niet alle configuraties op te slaan door op het **pictogram** op het rechter bovenpaneel van het scherm te drukken.

Herhaal voor elke vertakte extender.

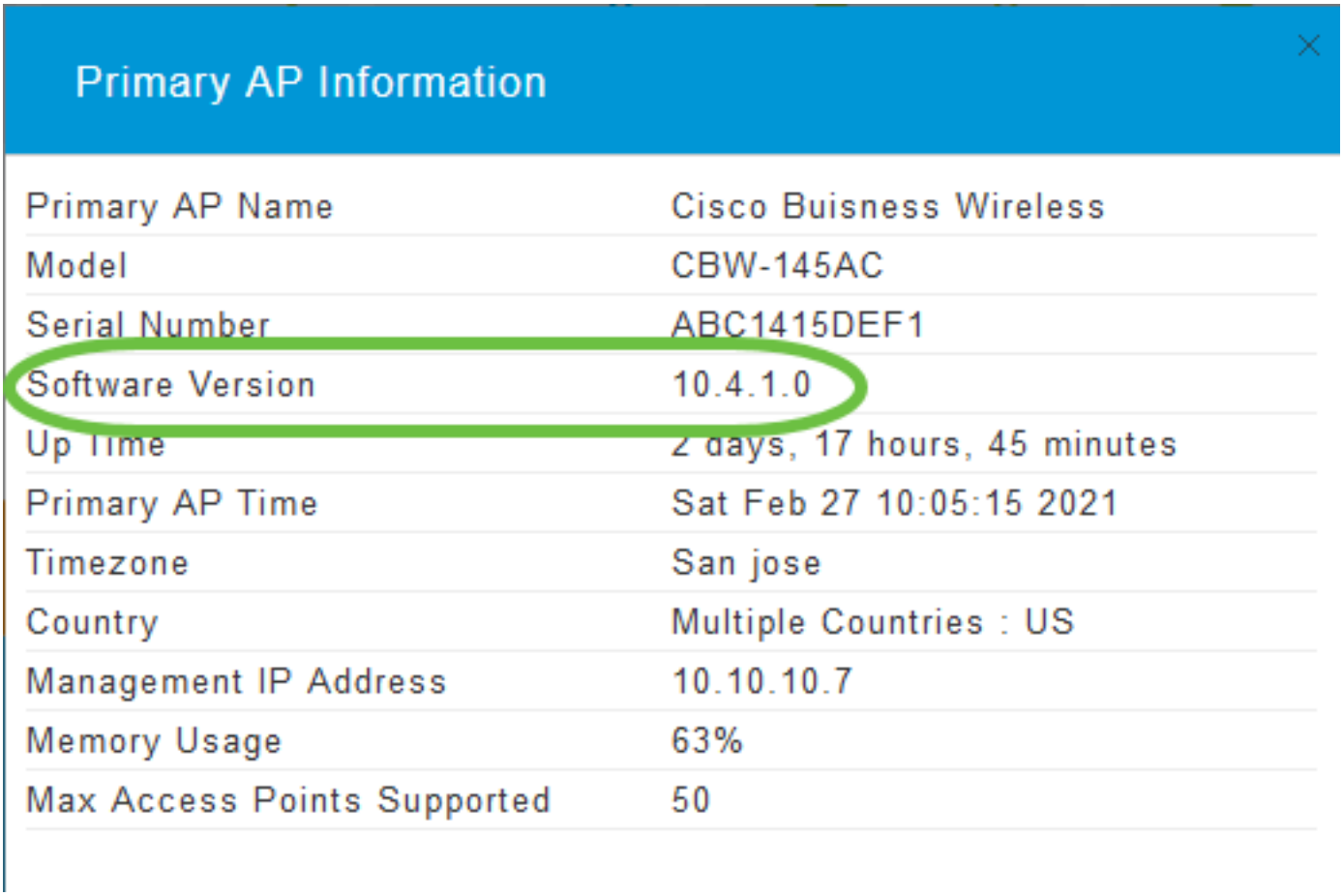
Software controleren en bijwerken met WebUI

Sla deze belangrijke stap niet over! Er zijn een paar manieren om software bij te werken, maar de stappen hieronder worden aanbevolen als het makkelijkst om uit te voeren wanneer u Web UI gebruikt.

Voer de volgende stappen uit om de huidige softwareversie van uw primaire AP te bekijken en bij te werken.

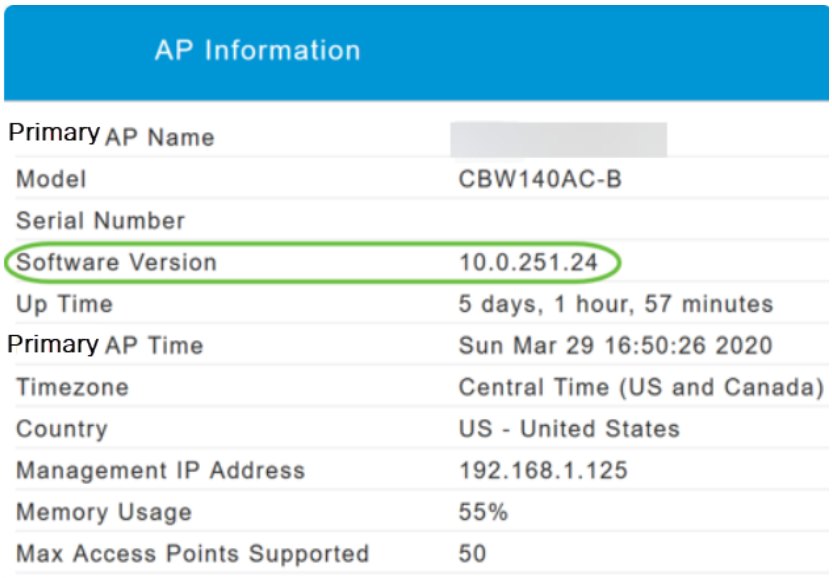
Stap 1

Klik op het **pictogram** boven in de rechthoek van de web interface en klik vervolgens op **Primaire AP-informatie**.



Stap 2

Vergelijk de versie die draait met de nieuwste softwareversie. Sluit het venster zodra u weet of u de software moet bijwerken.



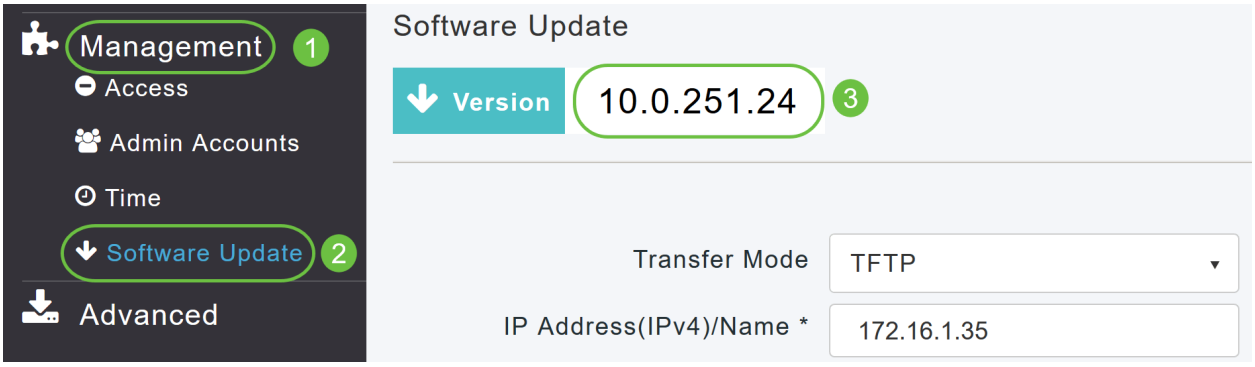
Als u de nieuwste versie van de software draait, kunt u naar het gedeelte WLAN's maken.

Stap 3

Kies **Management > Software Update** in het menu.

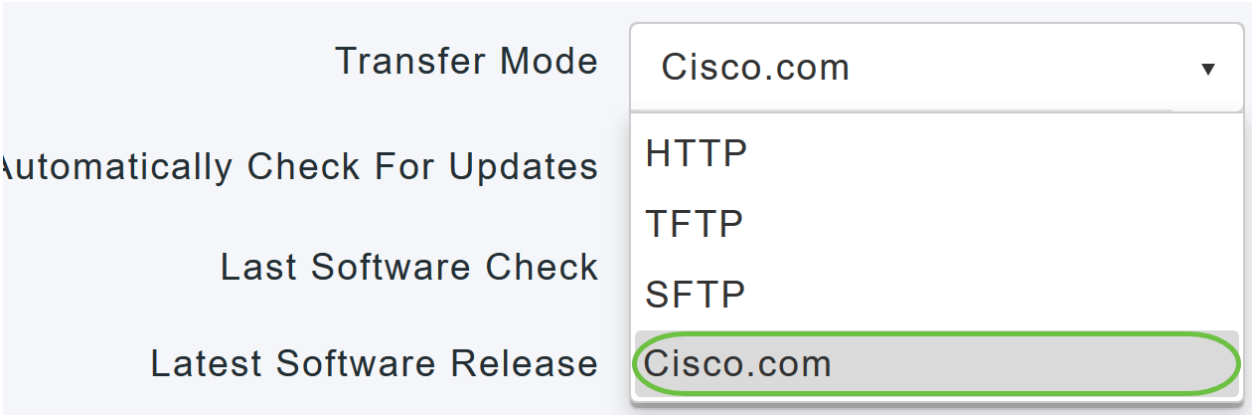
Het venster *Software Update* wordt weergegeven met het huidige versienummer van

de software dat bovenaan wordt weergegeven.



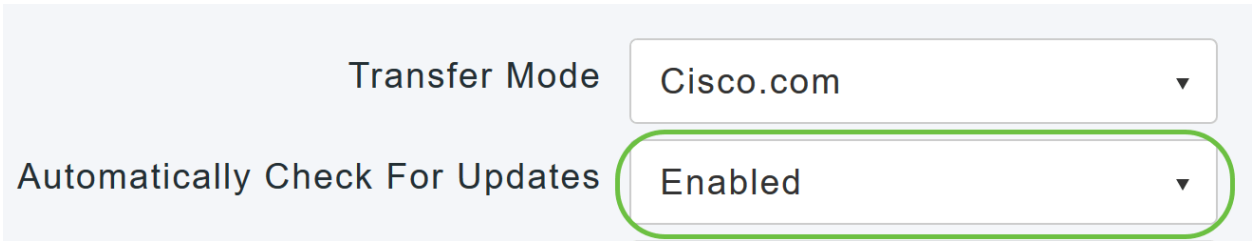
U kunt de CBW AP-software bijwerken en de huidige configuraties op de Primaire AP worden niet verwijderd.

Kies **Cisco.com** in de vervolgkeuzelijst *Vervoermodus*.



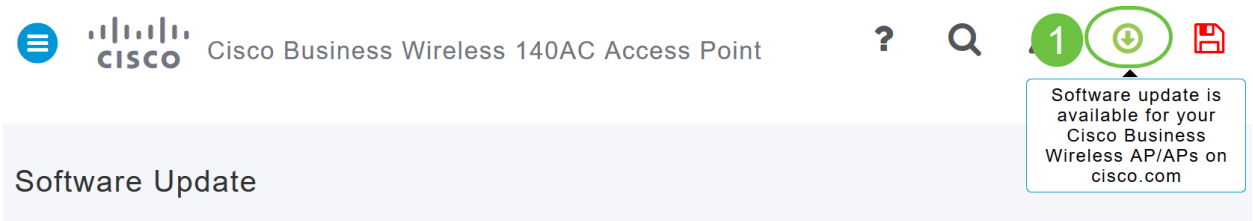
Stap 4

Als u de primaire AP wilt instellen om automatisch te controleren op software updates, kiest u **Ingeschakeld** in de vervolgkeuzelijst *Automatisch controleren op updates*. Dit is standaard ingeschakeld.



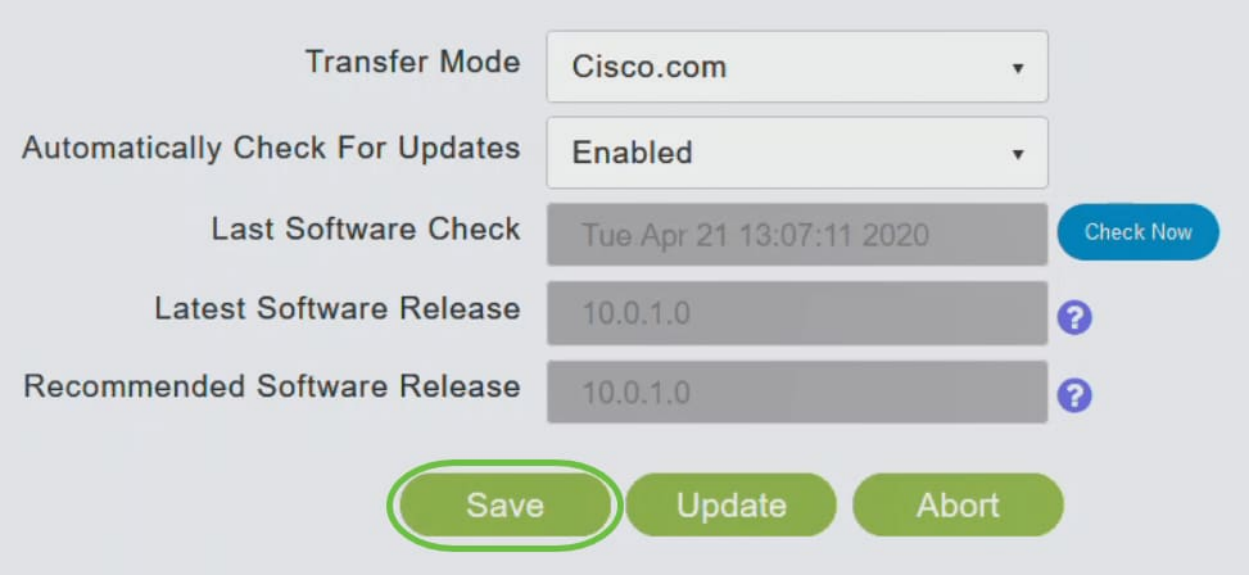
Wanneer een softwarecontrole wordt uitgevoerd en als er een nieuwere, laatste of aanbevolen softwareupdate beschikbaar is op Cisco.com, dan:

- Het **pictogram Software Update** op de rechterbovenhoek van het web UI is groen in kleur (of grijs). Wanneer u op het pictogram klikt, wordt u naar de pagina Software Update gebracht.
- De knop Update onder op de pagina *Software Update* is ingeschakeld.

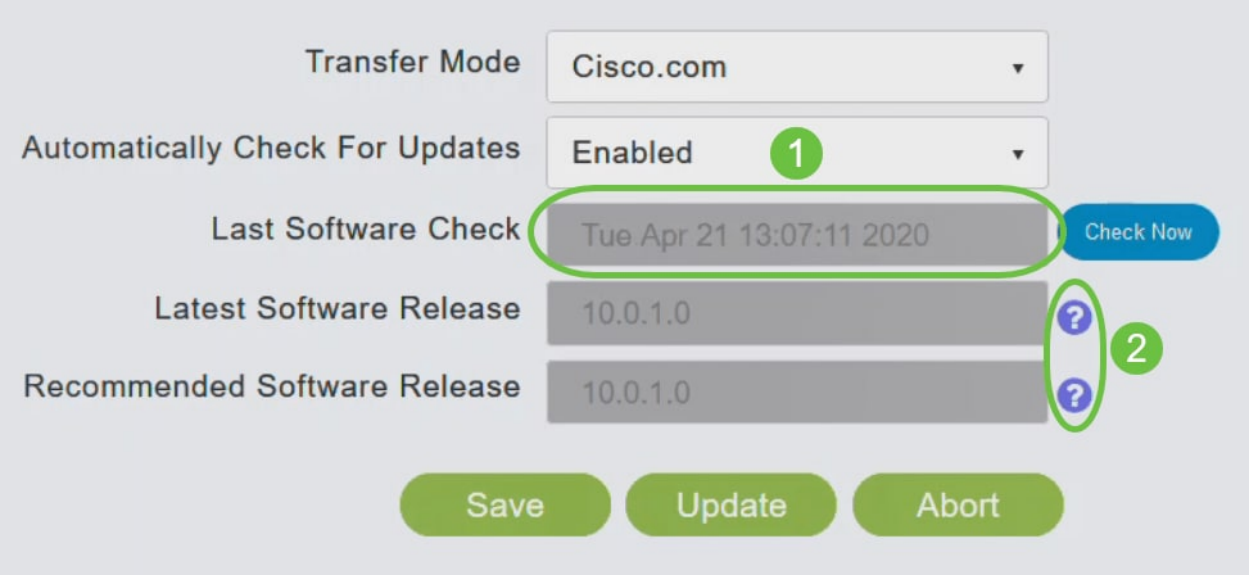


Stap 5

Klik op **Opslaan**. Hiermee slaat u de items die u in zowel de *overdrachtmodus* als de wijzigingen hebt aangebracht, op en *automatisch controleren op updates*.

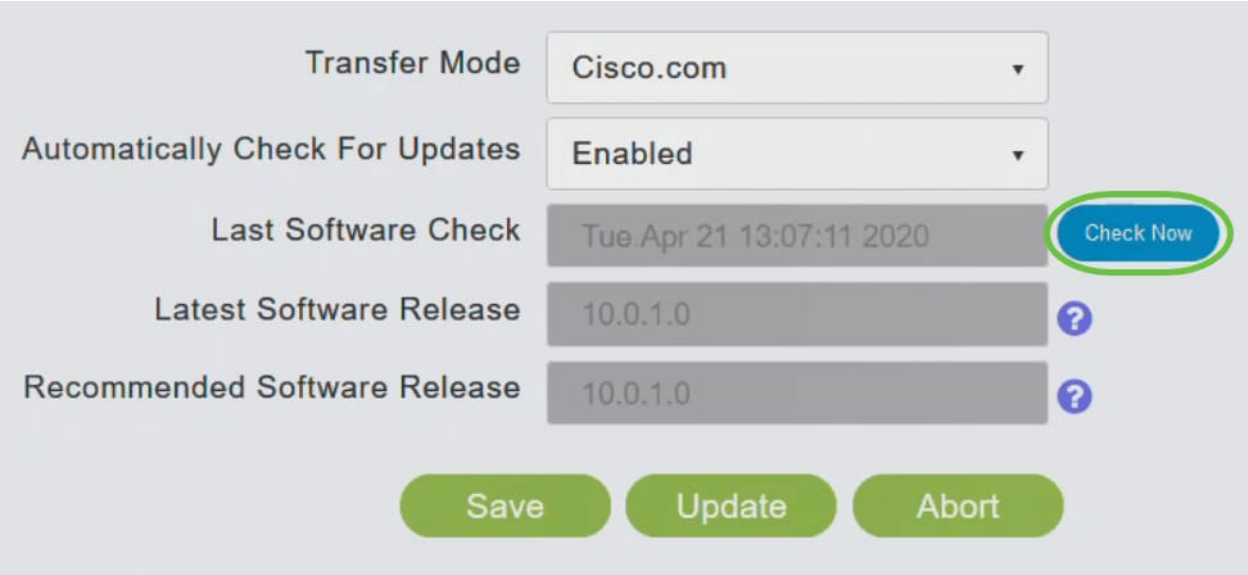


Het veld *Laatste controle op de software* geeft de tijdstempel van de laatste automatische of handmatige controle van de software weer. U kunt de opmerkingen van weergegeven releases bekijken door op het **pictogram** van het **vraagteken** naast deze te klikken.



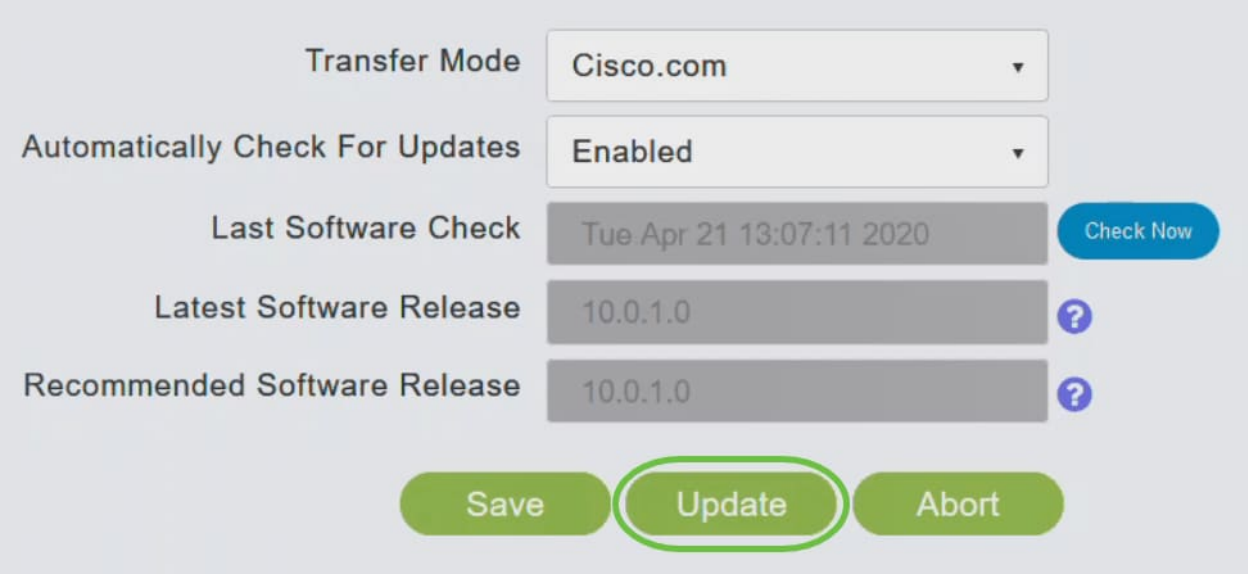
Stap 6

U kunt de software altijd handmatig starten door op *Nu controleren* te klikken.



Stap 7

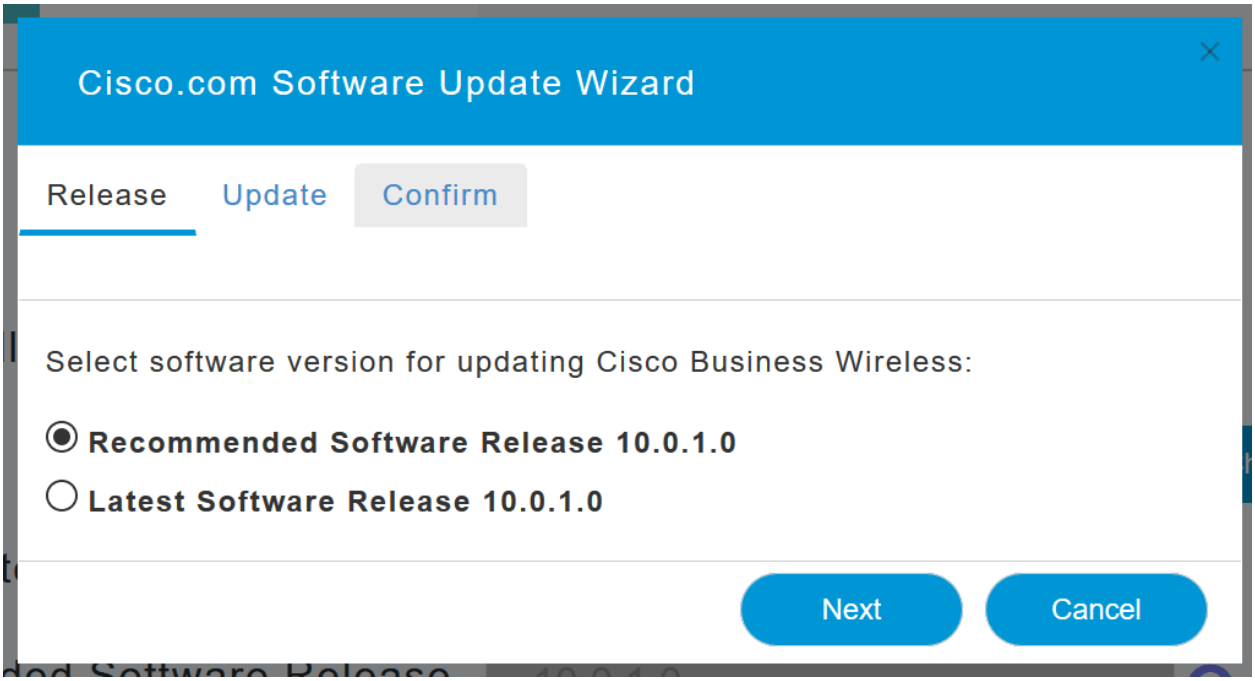
Klik op **Update** om verder te gaan met de softwareupdate.



De *Wizard Software bijwerken* verschijnt. De tovenaar neemt u door de volgende drie tabbladen na elkaar:

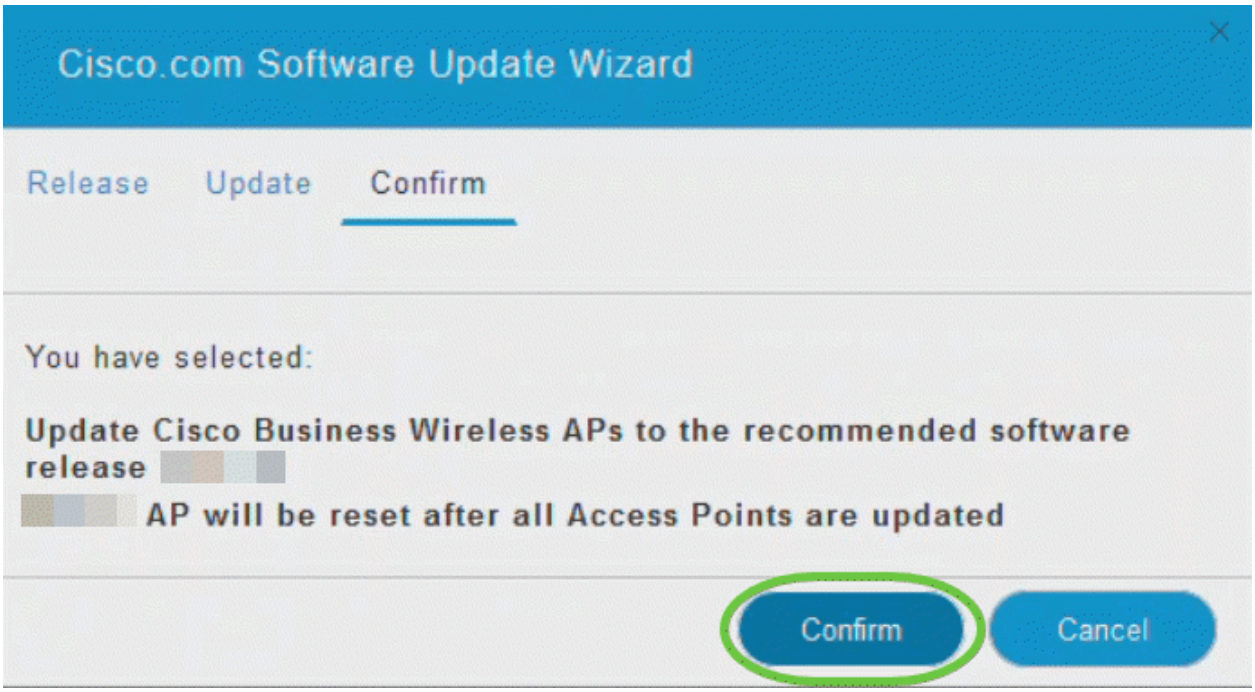
- Release tab - Specificeer of u wilt bijwerken naar de aanbevolen softwarerelease of de nieuwste softwarerelease.
- Tabblad bijwerken - Specificeer wanneer de AP's opnieuw ingesteld moeten worden. U kunt ervoor kiezen het onmiddellijk te laten doen of het voor een later tijdstip te laten plannen. Als u de primaire AP wilt instellen om automatisch opnieuw te starten nadat de afbeelding al is gedownload, schakelt u het selectieknop Auto Restart in.
- Bevestig tabblad - Bevestig de geselecteerde opties.

Volg de instructies in de wizard. U kunt op elk gewenst moment terugkeren naar een ander tabblad voordat u op *Bevestiging* klikt.



Stap 8

Klik op **Bevestig**.

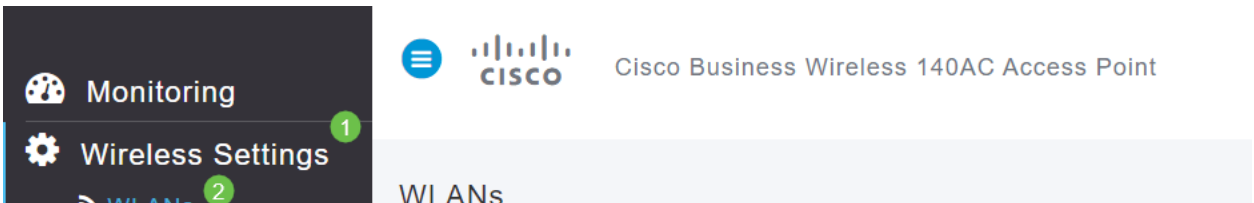


WLAN's maken op de web-UI

In deze sectie kunt u Wireless Local Area Networks (WLAN's) maken.

Stap 1

Een WLAN kan worden gecreëerd door te navigeren naar **draadloze instellingen > WLAN's**. Selecteer vervolgens **Nieuwe WLAN/LAN toevoegen**.



Stap 2

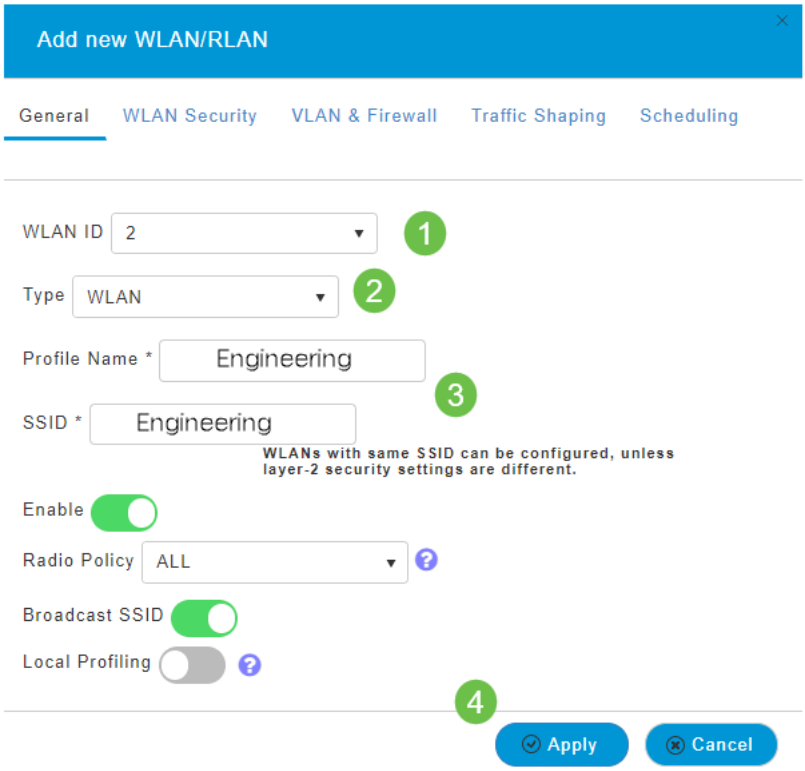
Voer onder het tabblad *Algemeen* de volgende informatie in:

- WLAN-id - selecteer een nummer voor WLAN
- Type - selecteer **WLAN**
- Profielnaam - Wanneer u een naam invoert, vult SSID met dezelfde naam automatisch op. De naam moet uniek zijn en mag niet meer dan 31 tekens bevatten.

De volgende velden werden standaard gelaten in dit voorbeeld, maar de toelichtingen zijn vermeld voor het geval u ze anders wilt configureren.

- SSID - De profielnaam fungeert ook als de SSID. Je kunt dit veranderen als je wilt. De naam moet uniek zijn en mag niet meer dan 31 tekens bevatten.
- Inschakelen - Dit moet worden bewaard zodat het WLAN kan werken.
- Radiobeleid - Meestal wil je dit als **alles** laten, zodat klanten van 2,4 GHz en 5 GHz toegang hebben tot het netwerk.
- Broadcast SSID - Gewoonlijk wilt u dat de SSID wordt ontdekt, zodat u deze als Enabled wilt laten.
- Local Profiles - U wilt alleen deze optie in staat stellen om het besturingssysteem dat op de client actief is te bekijken of de naam van de gebruiker te zien.

Klik op Apply (Toepassen).



Stap 3

U wordt naar het tabblad *WLAN-beveiliging* gebracht.

In dit voorbeeld bleven de volgende opties standaard over:

- Guest Network, Captive Network Assistant en MAC Filtering zijn uitgeschakeld. Nadere details voor het opzetten van een gastnetwerk zijn te vinden in de volgende paragraaf.
- WAP2 Mobile - Wi-Fi beschermde access point 2 met Voorgedeeld sleutel (PSK) Wachtwoordformaat - ASCII. Deze optie staat voor Wi-Fi Protected Access 2 met Vooraf gedeelde sleutel (PSK).

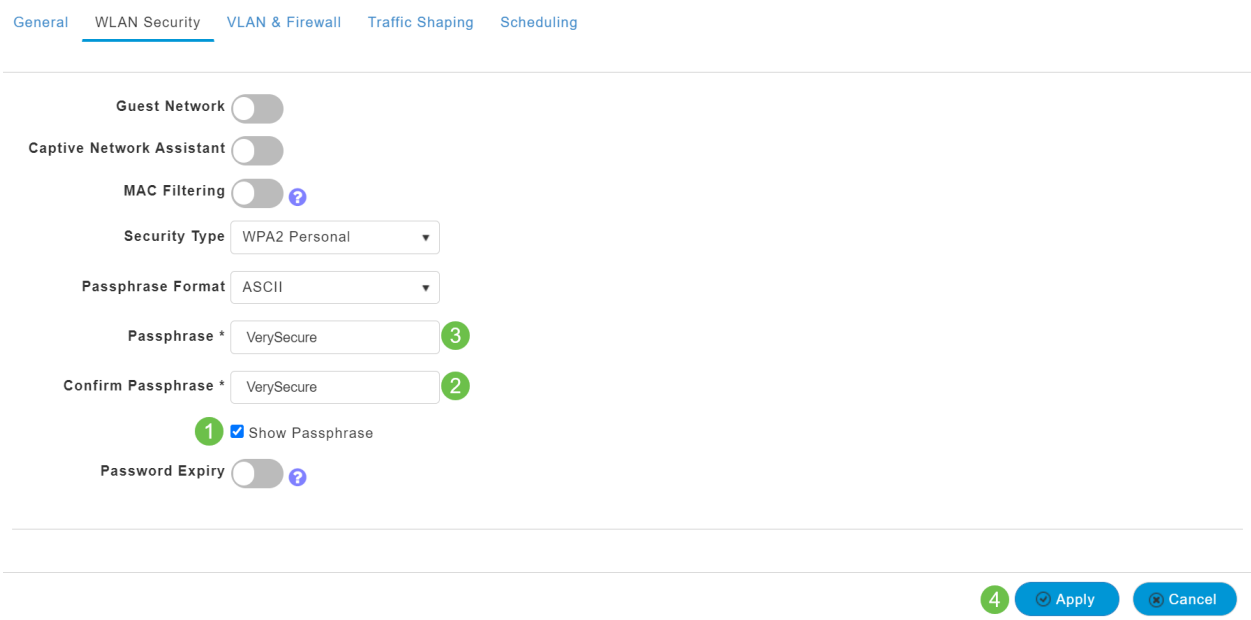
WAP2 Mobile is een methode die gebruikt wordt om uw netwerk te beveiligen met het gebruik van een PSK-verificatie. De PSK wordt afzonderlijk ingesteld, zowel op de Primaire AP, onder het WLAN-beveiligingsbeleid als op de client. WAP2 Persoonlijk baseert zich niet op een authenticatieserver op uw netwerk.

- Wachtwoordformaat - **ASCII blijft standaard ingeschakeld.**

In dit scenario zijn de volgende velden ingevoerd:

- Wachtwoord tonen - klik op het selectieteken om het wachtwoord te kunnen zien dat u invoert.
- Wachtwoord - Voer een naam in voor het wachtwoord (wachtwoord).
- Wachtwoord bevestigen - Voer het wachtwoord nogmaals in om het te bevestigen.

Klik op Apply (Toepassen). Dit zal automatisch het nieuwe WLAN activeren.



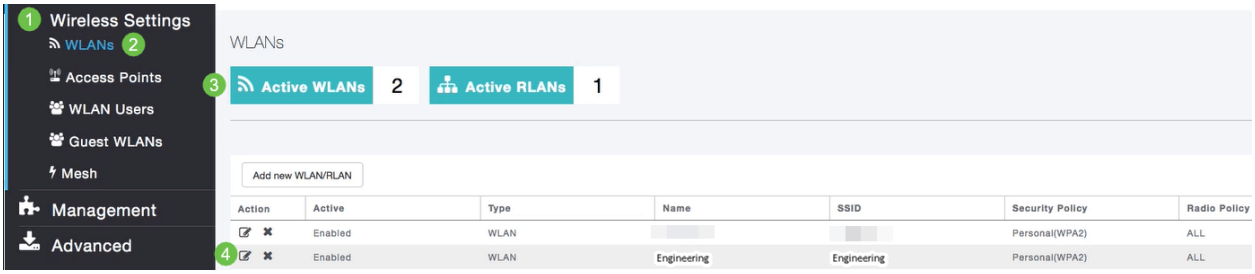
Stap 4

Zorg ervoor dat u uw configuraties opslaat door op het **pictogram** opslaan op het rechter bovenpaneel van het Web UI-scherm te klikken.

Stap 5

Als u de WLAN's wilt bekijken die u hebt gemaakt, selecteert u **Draadloze instellingen > WLAN's**. U ziet het aantal actieve WLAN's dat naar 2 wordt verhoogd, en het nieuwe

WLAN wordt weergegeven.



Herhaal deze stappen voor andere WLAN's die u wilt maken.

Optionele draadloze configuraties

U hebt nu alle basisconfiguraties ingesteld en bent klaar om te rollen. U hebt een aantal opties, dus kunt u in de volgende fasen springen:

- Maak een Guest WLAN met behulp van de Web UI (optioneel)
- Toepassingsprofielen (optioneel)
- Clientprofielen (optioneel)
- Ik ben bereid om dit op te maken en mijn netwerk te gebruiken!

Maak een Guest WLAN met behulp van de Web UI (optioneel)

Een gast WLAN geeft gasttoegang tot uw netwerk van Cisco Business Wireless.

Stap 1

Log in op de web UI van de primaire AP. Open een webbrowser en voer www.https://ciscobusiness.cisco in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer je geloofsbrieven in. U kunt deze ook benaderen door het IP-adres van de primaire AP in te voeren.

Stap 2

Een Wireless Local Area Network (WLAN) kan worden gecreëerd door te navigeren naar **draadloze instellingen > WLAN's**. Selecteer vervolgens **Nieuwe WLAN/LAN toevoegen**.

Stap 3

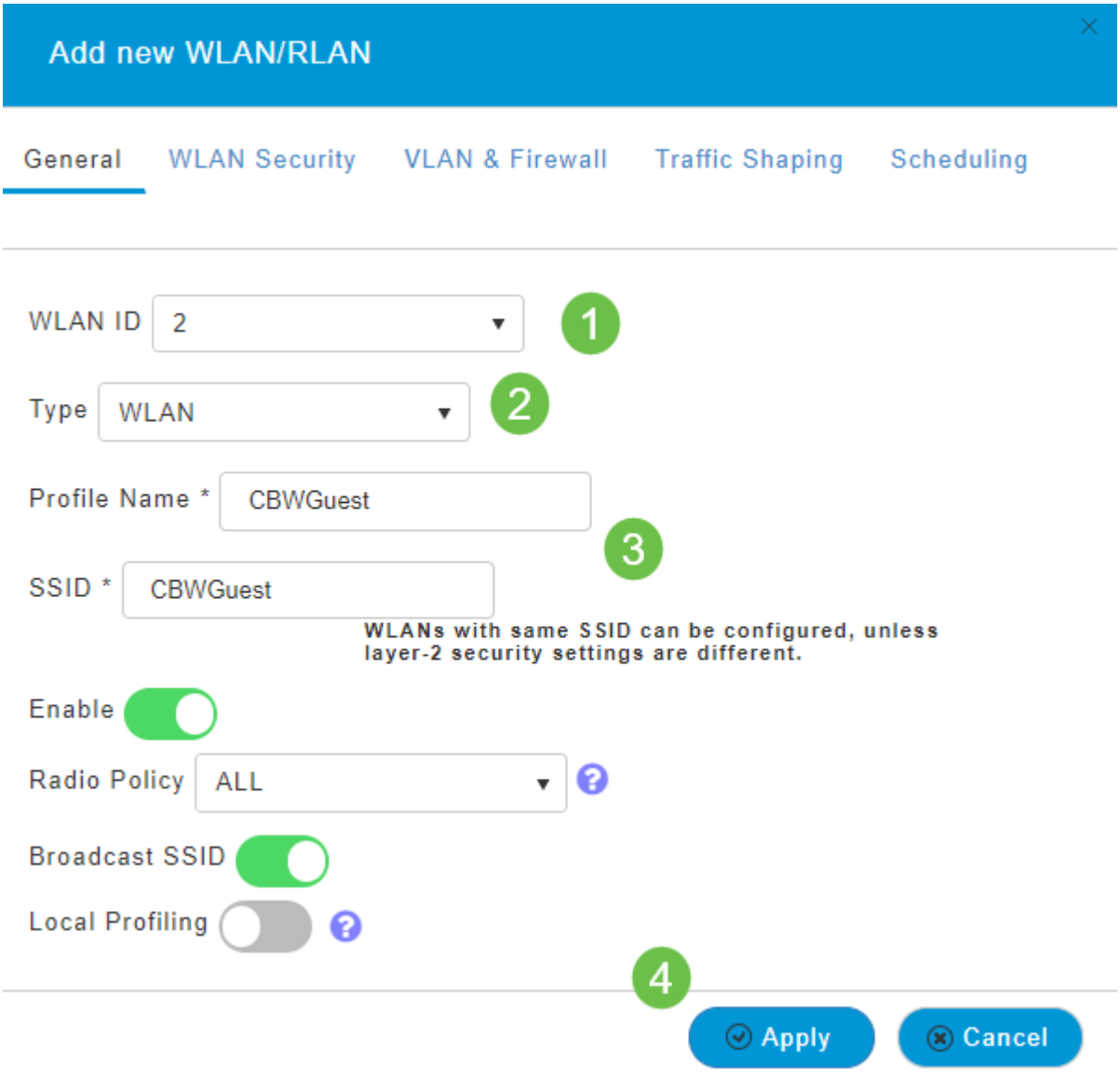
Voer onder het tabblad *Algemeen* de volgende informatie in:

WLAN-id - selecteer een nummer voor de WLAN-functie
Type - selecteer **WLAN**
Profielnaam - Wanneer u een naam invoert, wordt SSID met dezelfde naam automatisch ingevuld. De naam moet uniek zijn en mag niet meer dan 31 tekens bevatten.

De volgende velden werden standaard gelaten in dit voorbeeld, maar de toelichtingen zijn vermeld voor het geval u ze anders wilt configureren.

SSID - De profielnaam fungeert ook als SSID. Je kunt dit veranderen als je wilt. De naam moet uniek zijn en mag niet meer dan 31 tekens bevatten.
Inschakelen - Dit moet worden bewaard zodat het WLAN kan werken.
Radio Policy - Meestal wil u dit als **All** laten, zodat klanten van 2,4 GHz en 5 GHz toegang hebben tot het netwerk.
Uitzenden van SSID - Meestal wil u dat de SSID wordt ontdekt, zodat u dit als Enabled wilt laten.
Lokale profilering - u kunt deze optie alleen activeren om het besturingssysteem dat op de client wordt uitgevoerd te bekijken of de gebruikersnaam te zien.

Klik op Apply (Toepassen).

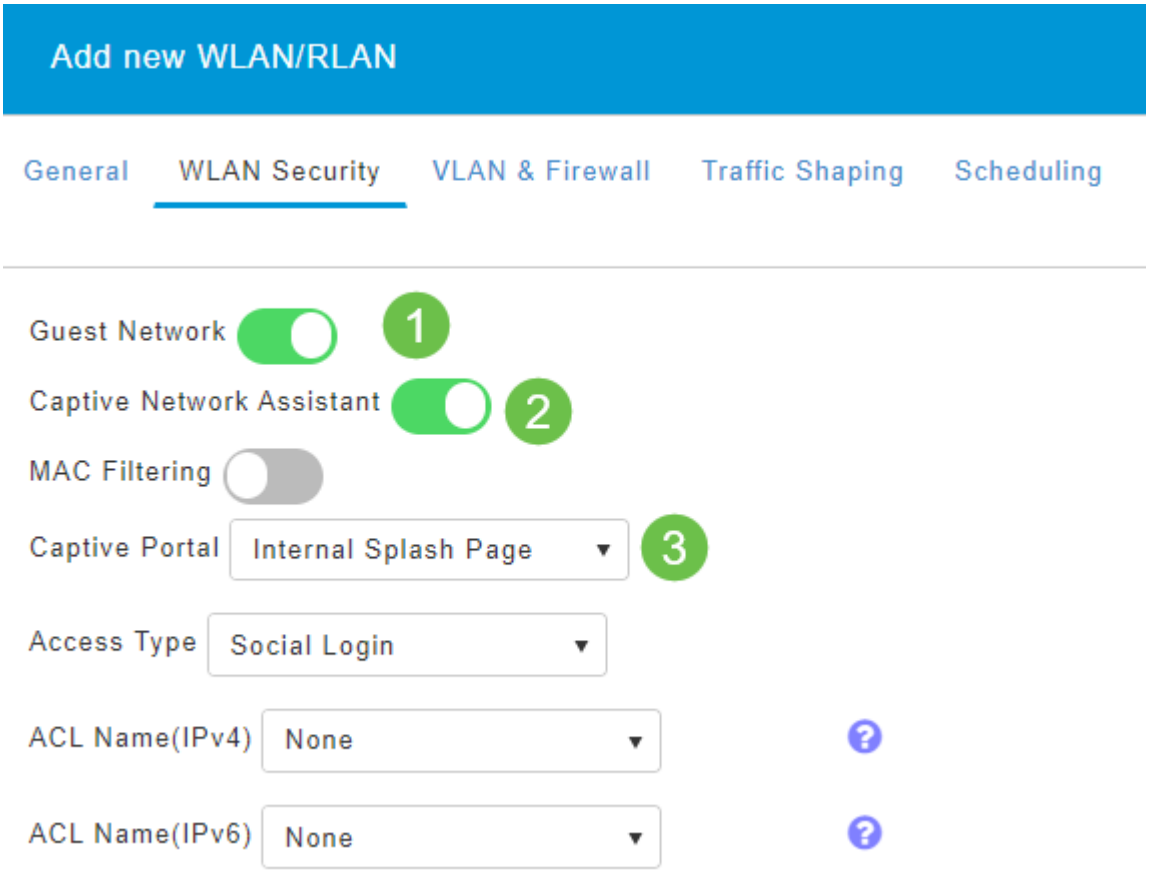


Stap 4

U wordt naar het tabblad *WLAN-beveiliging* gebracht. In dit voorbeeld werden de volgende opties geselecteerd.

- Guest Network - activeren
- Captive Network Assistant - Als u Mac of IOS gebruikt, zult u dit waarschijnlijk willen inschakelen. Deze optie detecteert de aanwezigheid van een portal door een webaanvraag te verzenden voor een verbinding met een draadloos netwerk. Dit verzoek is gericht op een Unified Resource Locator (URL) voor iPhone-modellen en als een reactie wordt ontvangen, is de internettoegang beschikbaar en is geen verdere interactie vereist. Als er geen respons wordt ontvangen, wordt de internettoegang verondersteld geblokkeerd te zijn door het gevangen portaal en wordt de automatische start van Apple's Captive Network Assistant (CNA) gestart met de pseudo-browser om inloggen in een gecontroleerd venster aan te vragen. De CNA kan breken wanneer hij wordt omgeleid naar een portal voor Identity Services Engine (ISE). Primaire AP voorkomt dat deze pseudo-browser opduikt.
- Captive Portal - Dit veld is alleen zichtbaar wanneer de optie Gast Network is ingeschakeld. Dit wordt gebruikt om het type webportaal te specificeren dat kan worden gebruikt voor authenticatiedoeleinden. Selecteer Interne startpagina voor het gebruik van de standaard Cisco webportal-gebaseerde verificatie. Kies een externe pagina voor

spons als u een interne authenticatie van het portaal hebt, met behulp van een webserver buiten uw netwerk. Specificeer ook de URL van de server in het veld Site URL.



In dit voorbeeld wordt het Guest WLAN met een ingeschakeld type sociale inlogtoegang gecreëerd. Wanneer de gebruiker zich op deze gastWLAN aansluit, worden ze opnieuw naar de standaardlogpagina van Cisco verwezen, waar de inlogknoppen van Google en Facebook worden gevonden. De gebruiker kan zich aanmelden om gebruik te maken van zijn Google- of Facebook-account voor toegang tot het internet.

Stap 5

Selecteer in dit tabblad een *toegangstype* in het vervolgkeuzemenu. In dit voorbeeld werd *Social Login* geselecteerd. Dit is de optie die gasten in staat stelt om hun Google of Facebook geloofsbrieven te gebruiken om te authentiseren en toegang tot het netwerk te krijgen.

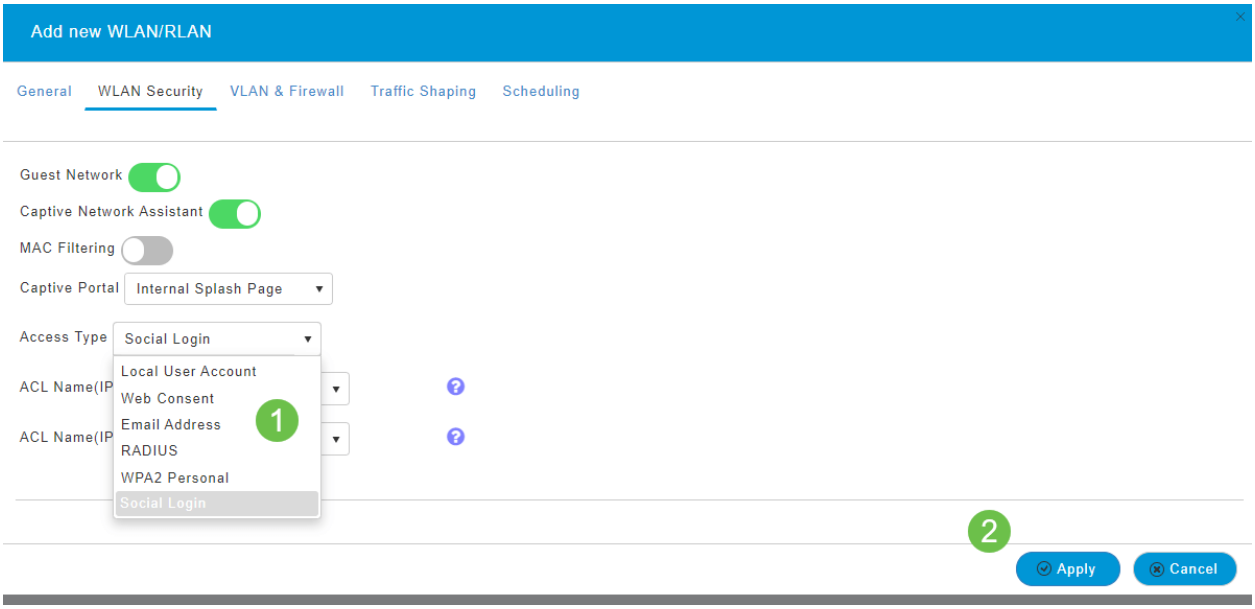
Andere opties voor *Type toegang* omvatten:

Lokale gebruikersaccount - de standaardoptie. Kies deze optie om gasten te authentiseren met de gebruikersnaam en het wachtwoord die u voor gastgebruikers van dit WLAN kunt specificeren, onder **Draadloze Instellingen > WLAN-gebruikers**. Dit is een voorbeeld van de standaard interne pagina van de spiegel.

U kunt dit aanpassen door naar **draadloze instellingen** te navigeren **> Gast WLAN's**. Vanaf hier kunt u een *paginanumlijn* en een *paginabereik* invoeren. Klik op Apply (Toepassen). Klik op **Voorbeeld**.

Webex - Hiermee kunnen gasten toegang krijgen tot het WLAN bij aanvaarding van weergegeven bepalingen en voorwaarden. Guest-gebruikers kunnen de WLAN's benaderen zonder een gebruikersnaam en wachtwoord in te voeren.
E-mailadres - Gastgebruikers moeten hun e-mailadres invoeren om toegang te krijgen tot het netwerk.
RADIUS - Gebruik dit met een externe verificatieserver.
Persoonlijk WAP2 - Wi-Fi beschermde access point 2 met voorgedeelde sleutel (PSK)

Klik op Apply (Toepassen).



Stap 6

Zorg ervoor dat u uw configuraties opslaat door op het **pictogram** opslaan op het rechter bovenpaneel van het Web UI-scherm te klikken.

U hebt nu een gastnetwerk gemaakt dat op uw netwerk van CBW beschikbaar is. Uw gasten zullen het gemak waarderen.

Toepassingsprofielen met behulp van Web UI (optioneel)

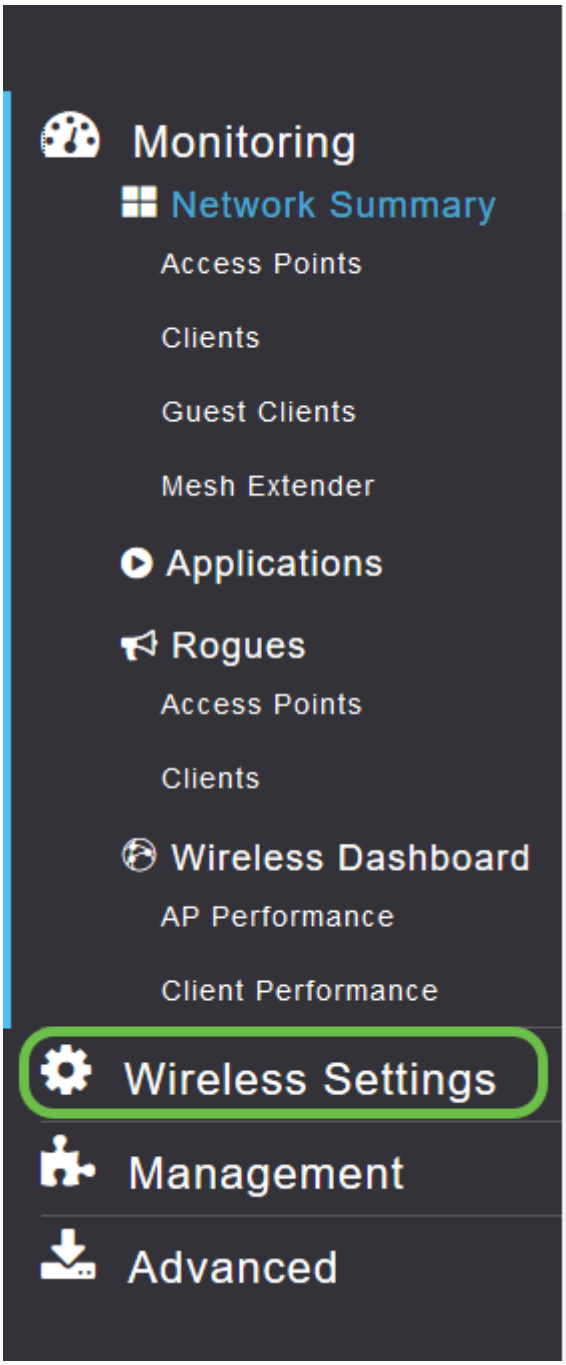
Profileren is een deelgroep van functies die het voeren van een organisatorisch beleid mogelijk maken. Hiermee kunt u verkeerstypen koppelen en prioriteren. Zoals regels beslissen over hoe je het verkeer rangschikt of laat vallen. Het Cisco Business mesh draadloze systeem is voorzien van client- en toepassingsprofielen. De toegang tot een netwerk als gebruiker begint met veel uitwisseling van informatie, waaronder het type verkeer. Het beleid onderbreekt verkeersstromen om het pad te sturen, net zoals een stroomschema. Andere soorten beleidsfuncties zijn onder andere - toegang voor gasten, toegangscontrolelijsten en QoS.

Stap 1

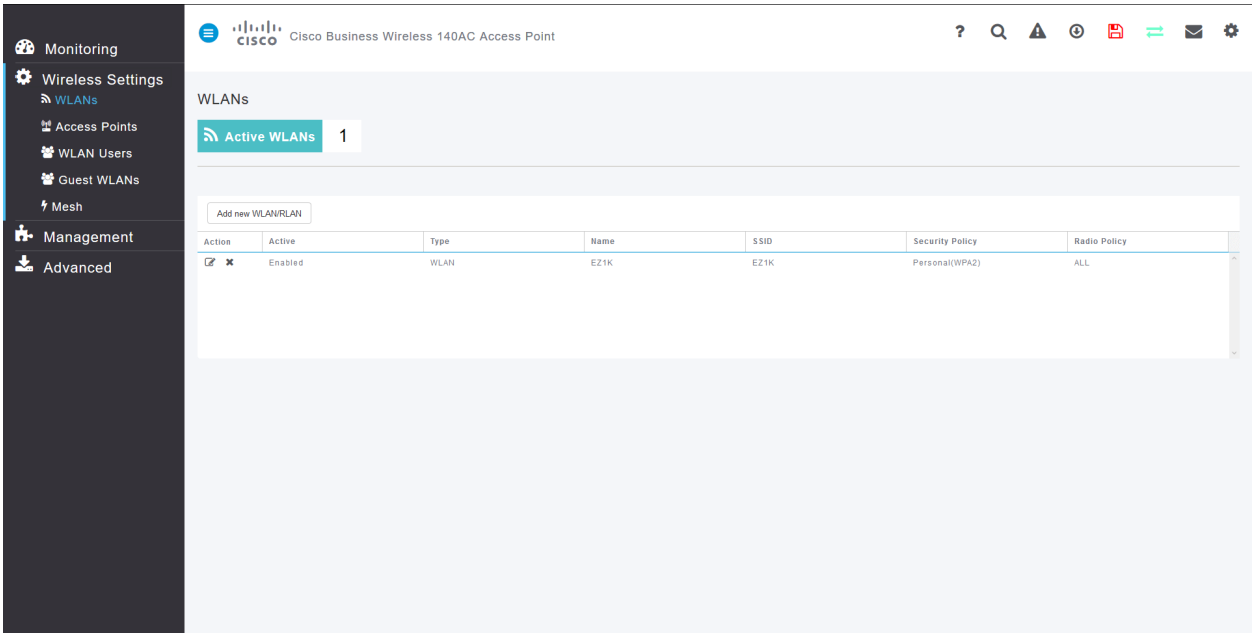
Navigeer naar het menu aan de linkerkant van het scherm als u de linker menubalk niet ziet.

Stap 2

Het bewakingsmenu wordt standaard geladen wanneer u in het apparaat tekent. U moet op **Draadloze instellingen** klikken.

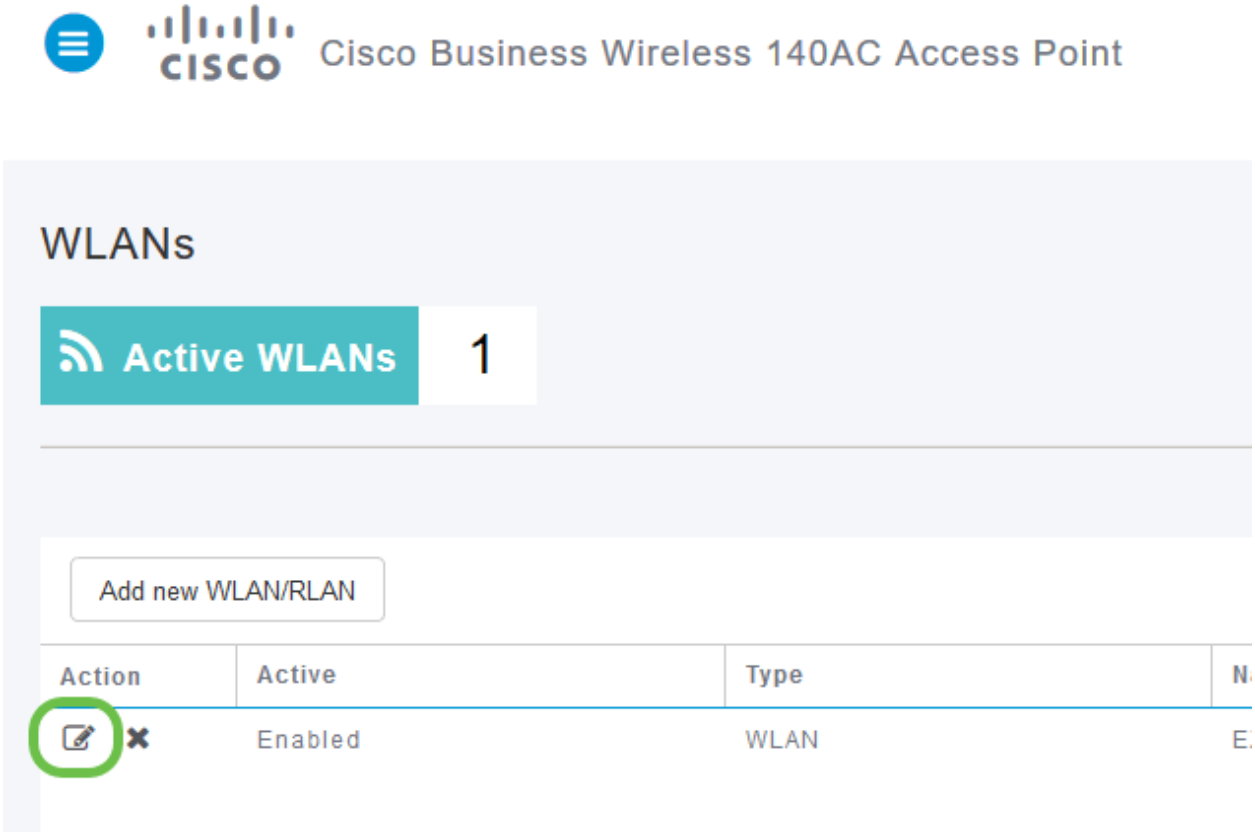


De afbeelding hieronder is gelijk aan de afbeelding die u ziet wanneer u op de link Draadloze instellingen klikt.

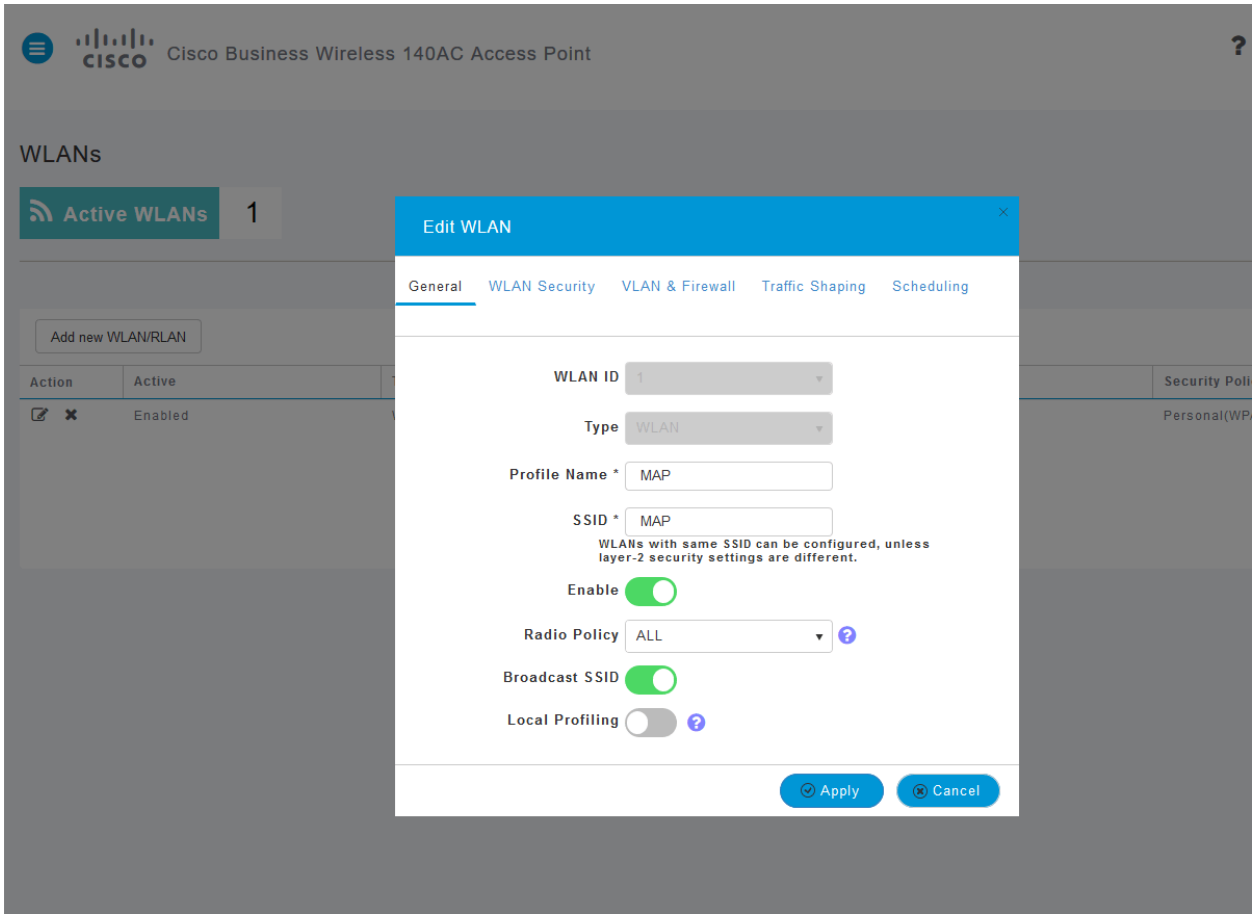


Stap 3

Klik op het **pictogram** bewerken links van het Wireless Local Area Network dat u wilt inschakelen.

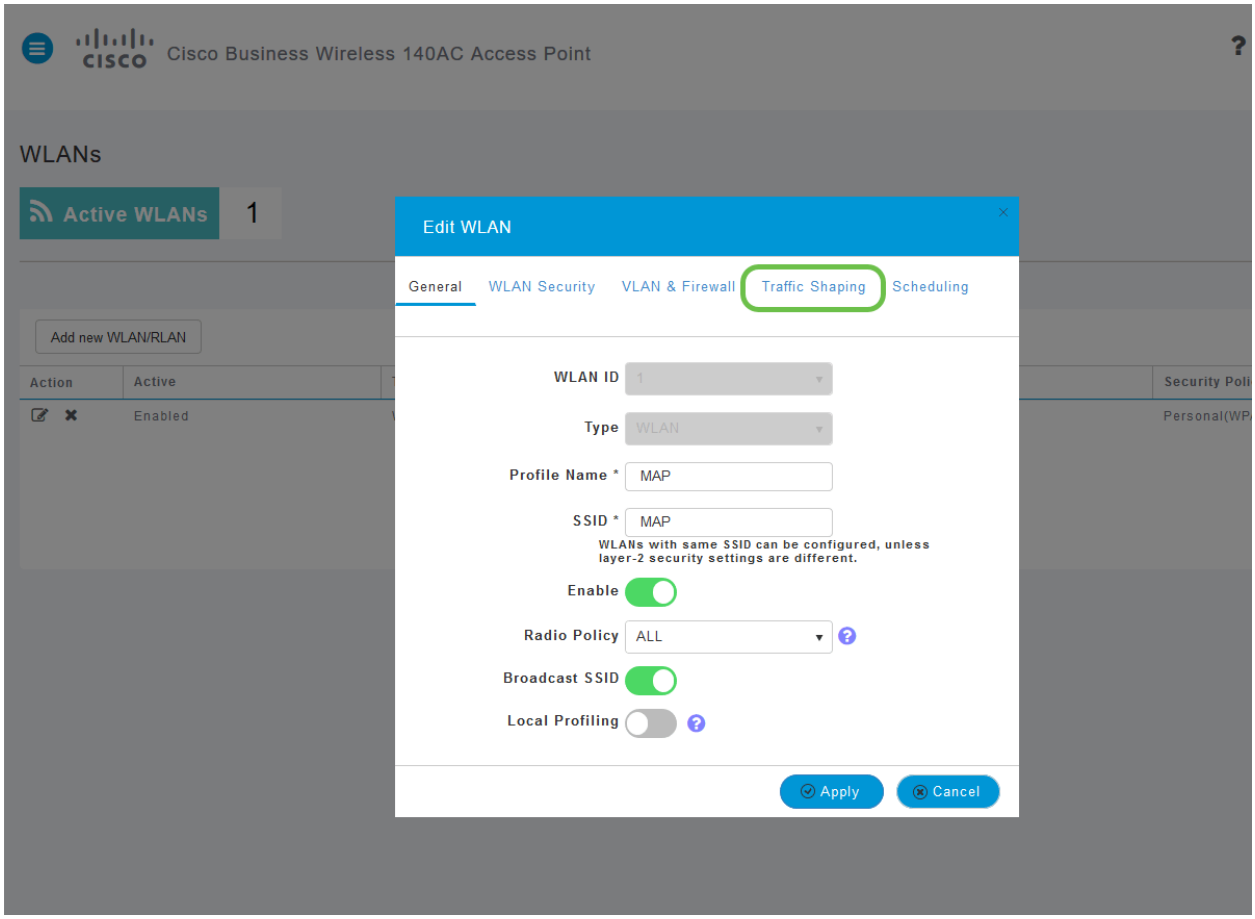


Aangezien u onlangs de WLAN-pagina hebt toegevoegd, kan uw *WLAN*-pagina *bewerken* vergelijkbaar met de onderstaande pagina worden weergegeven:

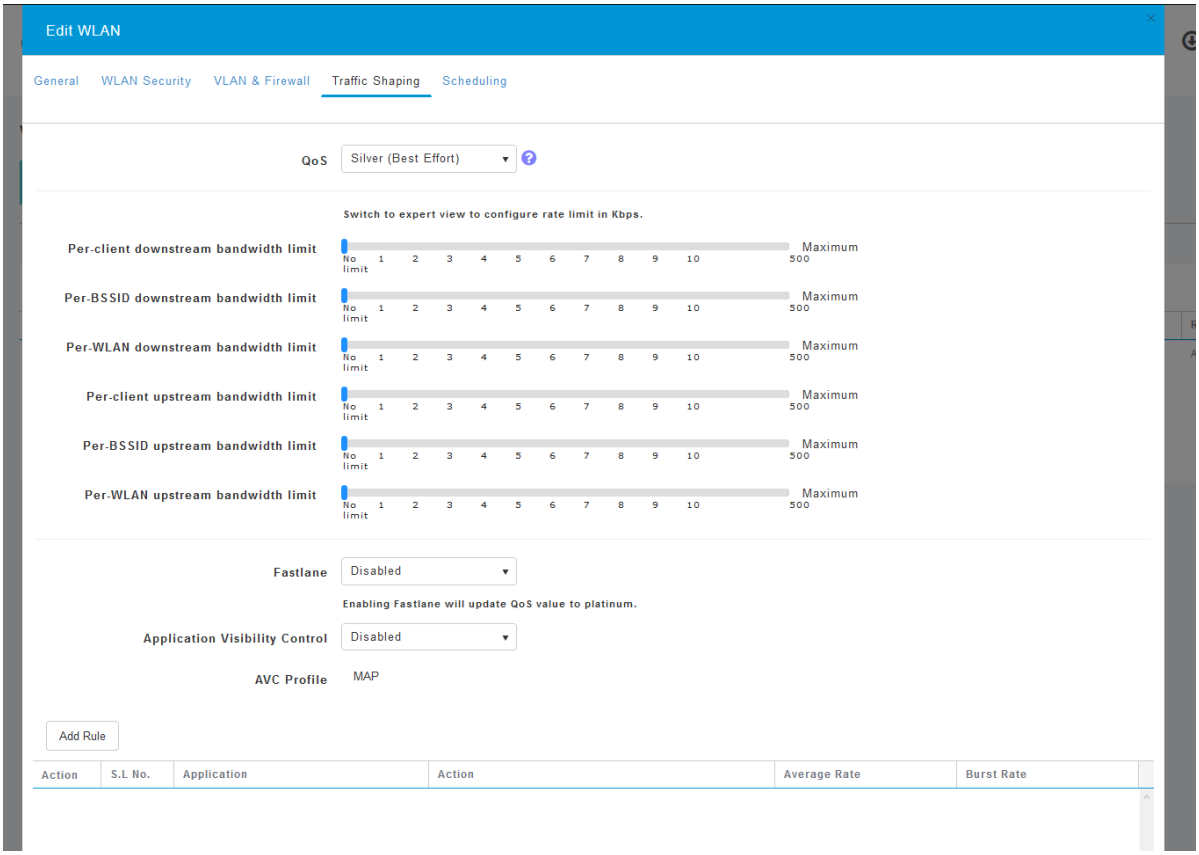


Stap 4

Navigeer naar het tabblad **Traffic Shaping** door op het tabblad te klikken.

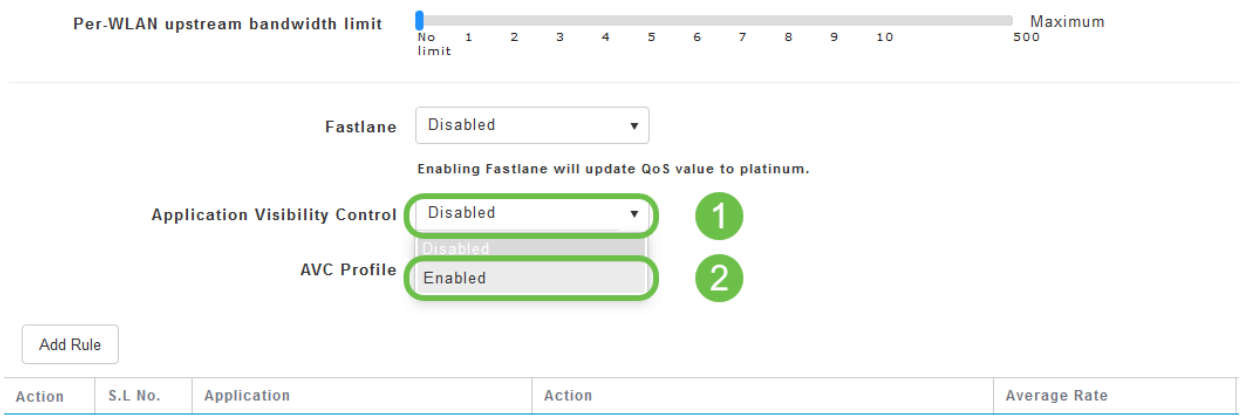


Uw scherm kan als volgt verschijnen:



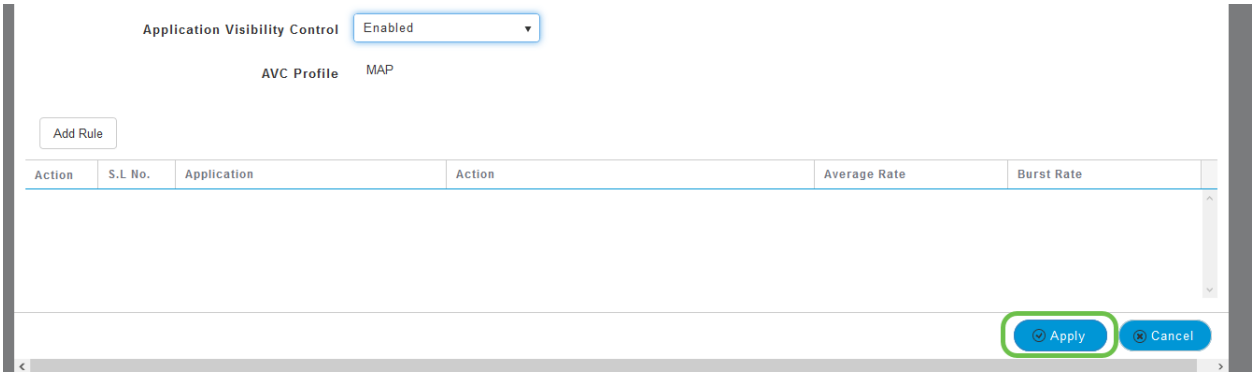
Stap 5

Naar de onderkant van de pagina vindt u de optie *Application Visibility and Control*. Dit wordt standaard uitgeschakeld. Klik op de vervolgkeuzelijst en selecteer **Ingeschakeld**.



Stap 6

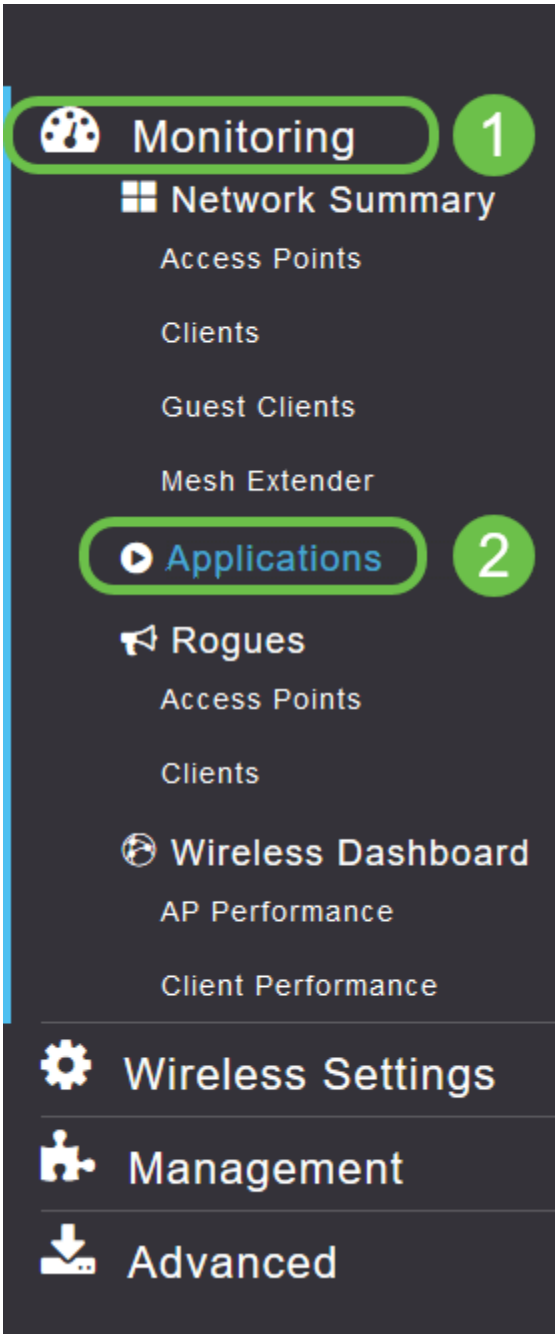
Klik op de knop **Toepassen**.



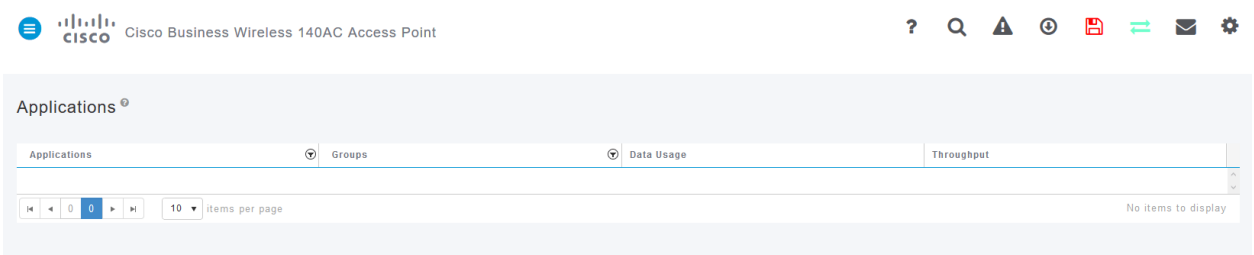
Deze instelling moet worden ingeschakeld, anders werkt deze functie niet.

Stap 7

Klik op de knop annuleren om het WLAN-submenu te sluiten. Klik vervolgens op het menu **Monitoring** in de linker menubalk. Zodra u in staat bent, klikt u op de menuoptie **Toepassingen**.



Als u geen verkeer naar een bron hebt gehad, wordt uw pagina leeg zoals hieronder wordt weergegeven.



Op deze pagina wordt de volgende informatie weergegeven:

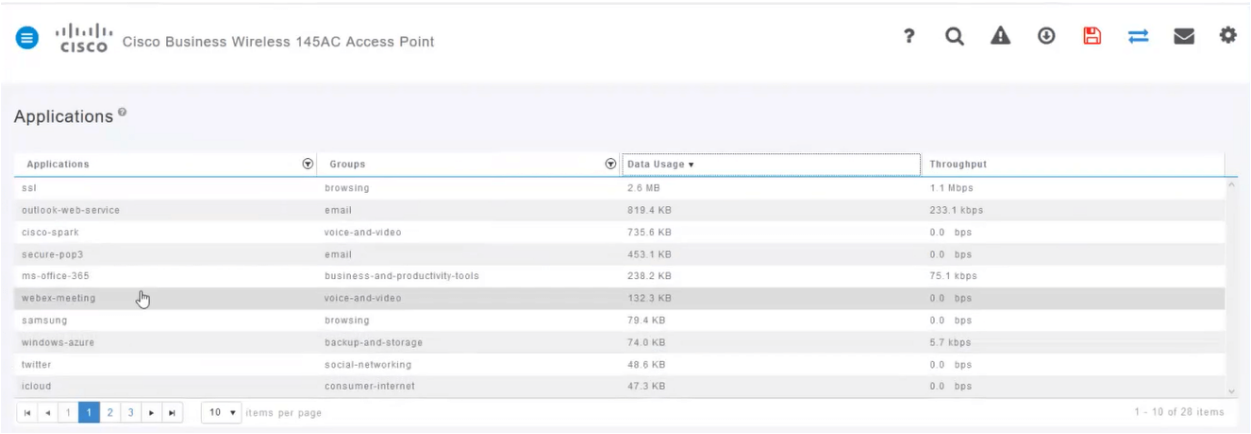
- Toepassing - omvat vele verschillende typen
- Groepen - Geeft het type toepassingsgroep aan zodat het gemakkelijker te sorteren is
- Gebruik van gegevens - de hoeveelheid gegevens die door deze dienst in het algemeen wordt gebruikt
- Doorvoersnelheid - de hoeveelheid bandbreedte die door de toepassing wordt gebruikt

U kunt op de tabbladen klikken om van het grootste naar het kleinste te sorteren, wat kan helpen de grootste consumenten van netwerkmiddelen te identificeren.

Deze functie is zeer krachtig voor het beheer van uw WLAN-bronnen op granulair niveau. Hieronder vind je een aantal meest voorkomende groepen en applicatietypen. Uw lijst bevat waarschijnlijk nog veel meer, waaronder de volgende groepen en voorbeelden:

- kabelen
    - EX: Clientspecifiek, SSL
- Email
    - EX: Outlook, Secure-pop3
- Spraak-en-video
    - EX: Webex, Cisco Spark
- Tools voor zakelijk gebruik en productiviteit
    - EX: Microsoft Office 365,
- Reserve-en-opslag
    - EX: Windows-uurs,
- Consumenteninternet
    - Cloud-, Google Drive
- Sociale netwerken
    - EX: Twitter, Facebook
- Software updates
    - EX: Google Play, IOS
- Instant Messaging
    - EX: Hangouts, berichten

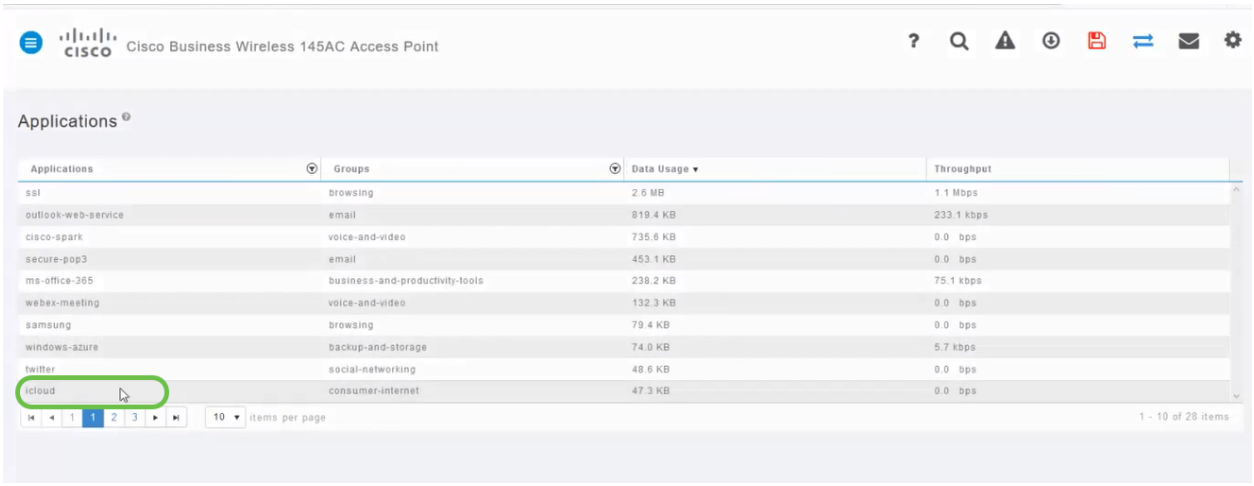
Hier wordt een voorbeeld getoond van hoe de pagina eruit zal zien wanneer gevuld.



Elke tabelrubriek is klikbaar voor sortering wat met name nuttig is voor *gegevensgebruik* en *doorvoervelden*.

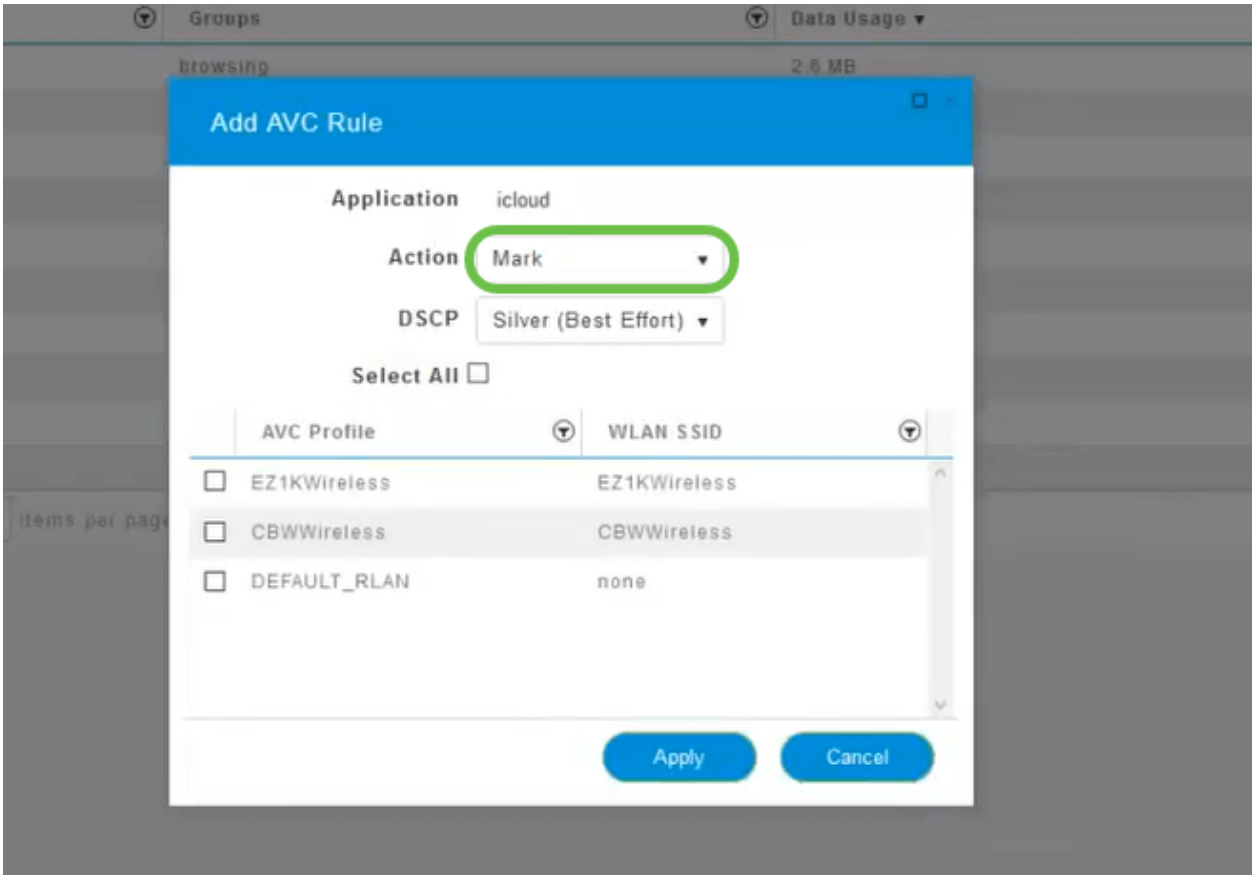
Stap 8

Klik op de rij voor het type verkeer dat u wilt beheren.



Stap 9

Klik op de vervolgkeuzelijst **Action** om te selecteren hoe u dat type verkeer wilt behandelen.



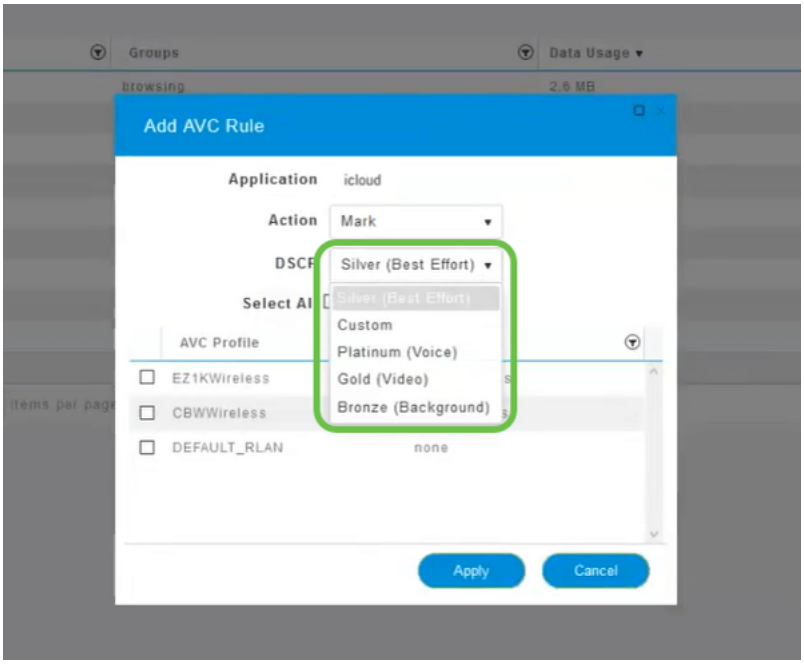
Dit voorbeeld laten we deze optie bij *Mark* achter.

Maatregelen om het verkeer te bevorderen

- Mark - Plaatst het type verkeer in een van de lagen van de Gedifferentieerde Servicescode Point (DSCP) 3 - voor het bepalen van het aantal beschikbare bronnen voor het applicatietype
- Drop - niets anders dan weggooien
- Snelheidsbeperking - Hiermee kunt u het gemiddelde tarief, het Burst Rate in Kbps instellen

Stap 10

Klik het vervolgkeuzevenster in het veld **DSCP** aan om uit de volgende opties te selecteren.



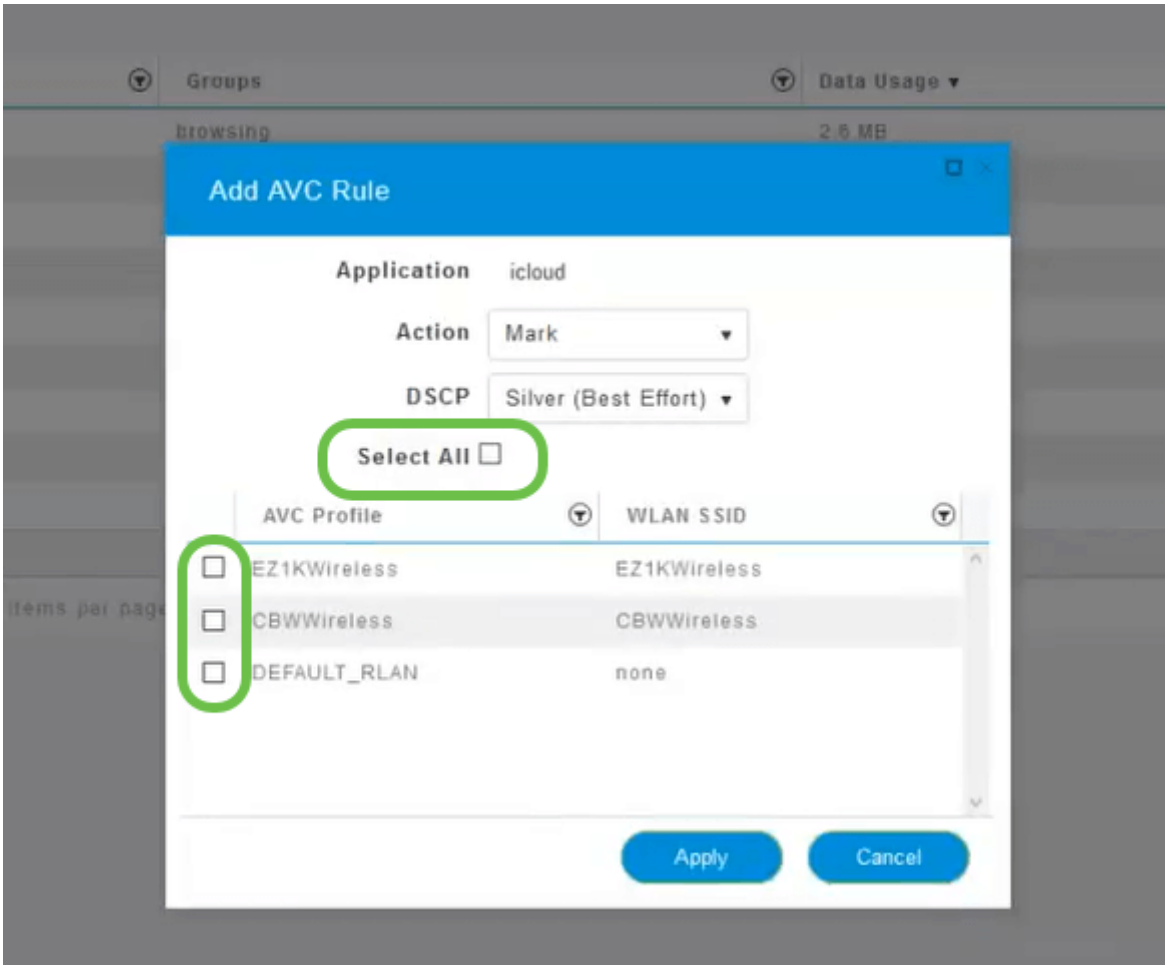
Hieronder staan de DSCP-opties voor het te markeren verkeer. Deze opties gaan van minder bronnen naar meer bronnen beschikbaar voor het type verkeer dat u bewerkt.

- Bronze (Achtergrond) - Minder
- Silver (beste inspanning)
- Goud (video)
- Platinum (spraak) meer
- Aangepaste - Gebruiker ingesteld

Als een web conventie is het verkeer naar SSL browsing gemigreerd, wat u ervan weerhoudt om te zien wat er in de pakketten zit terwijl ze van uw netwerk naar WAN bewegen. Als zodanig zal een groot deel van het webverkeer gebruik maken van SSL. Het instellen van SSL-verkeer voor een lagere prioriteit kan uw browservaring beïnvloeden.

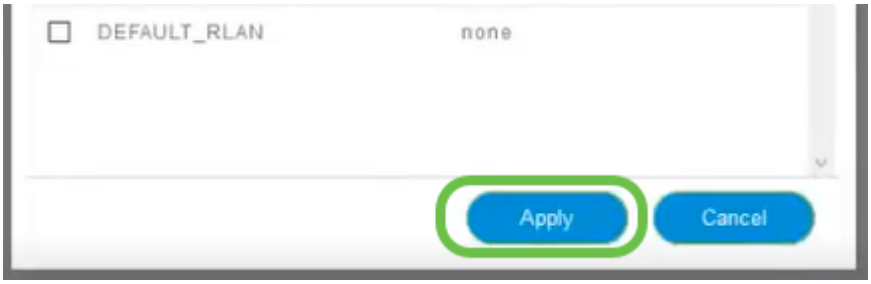
Stap 11

Selecteer nu de afzonderlijke SSID die u wilt dat dit beleid wordt uitgevoerd of klik op **Alles selecteren**.



Stap 12

Klik nu op **Toepassen** om dit beleid te starten.



Twee gevallen waarin dit zou kunnen gelden:

- De gasten/gebruikers streamen een grote hoeveelheid verkeer die het missie-kritieke verkeer verhindert door te komen. U kunt de prioriteit voor Voice verhogen en de prioriteit van Netflix-verkeer verlagen om dingen te verbeteren.
- Grote software-updates die tijdens kantooruren worden gedownload, kunnen worden weggelaten of de frequentie ervan kan worden beperkt.

Je hebt het gedaan. Toepassingsprofilering is een zeer krachtig instrument dat verder mogelijk kan worden gemaakt door ook clientprofilering mogelijk te maken, zoals in de volgende sectie wordt beschreven.

Clientprofilering met behulp van de WebUI (optioneel)

Bij verbinding met een netwerk wisselen apparaten client profileringsinformatie uit. Standaard is *het maken van clientprofielen* uitgeschakeld. Deze informatie kan het volgende omvatten:

- Host Name - of de naam van het apparaat
- Besturingssysteem - de kernsoftware van het apparaat
- IOS-versie - De herhaling van de van toepassing zijnde software

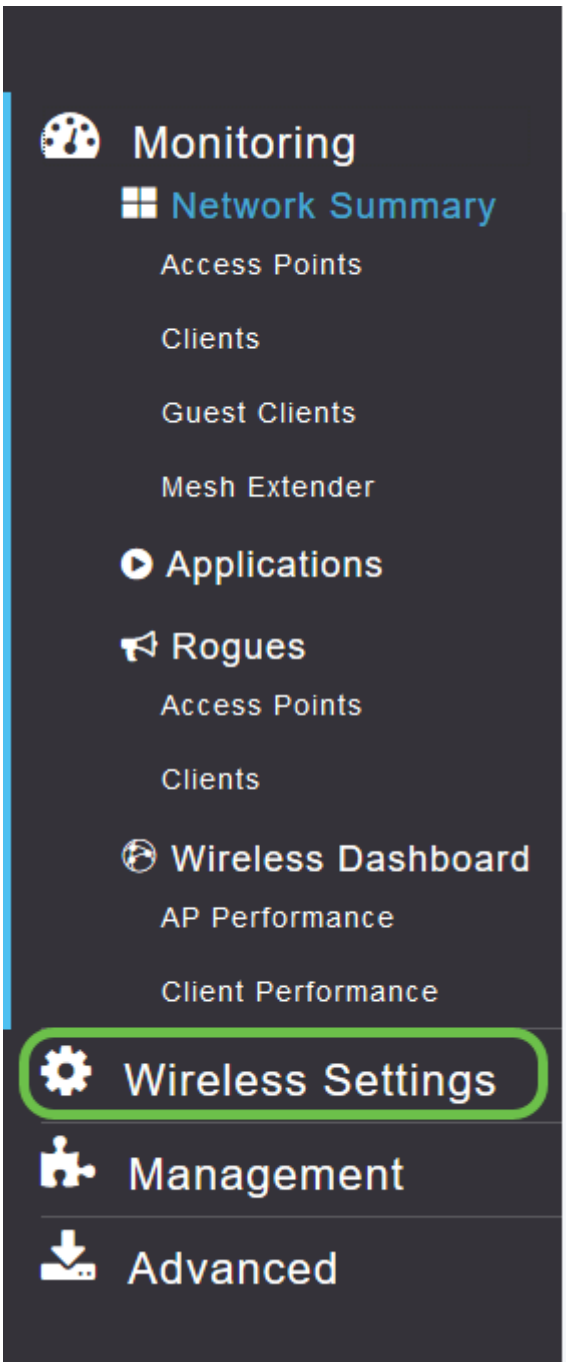
Statistieken over deze klanten omvatten de gebruikte hoeveelheid gegevens en de doorvoersnelheid.

Het volgen van clientprofielen maakt een grotere controle mogelijk over het draadloze lokale netwerk. Of je zou het kunnen gebruiken als functie van een andere functie. Bijvoorbeeld het gebruik van applicatie-throttling apparaten die geen missie-kritieke gegevens voor uw bedrijf dragen.

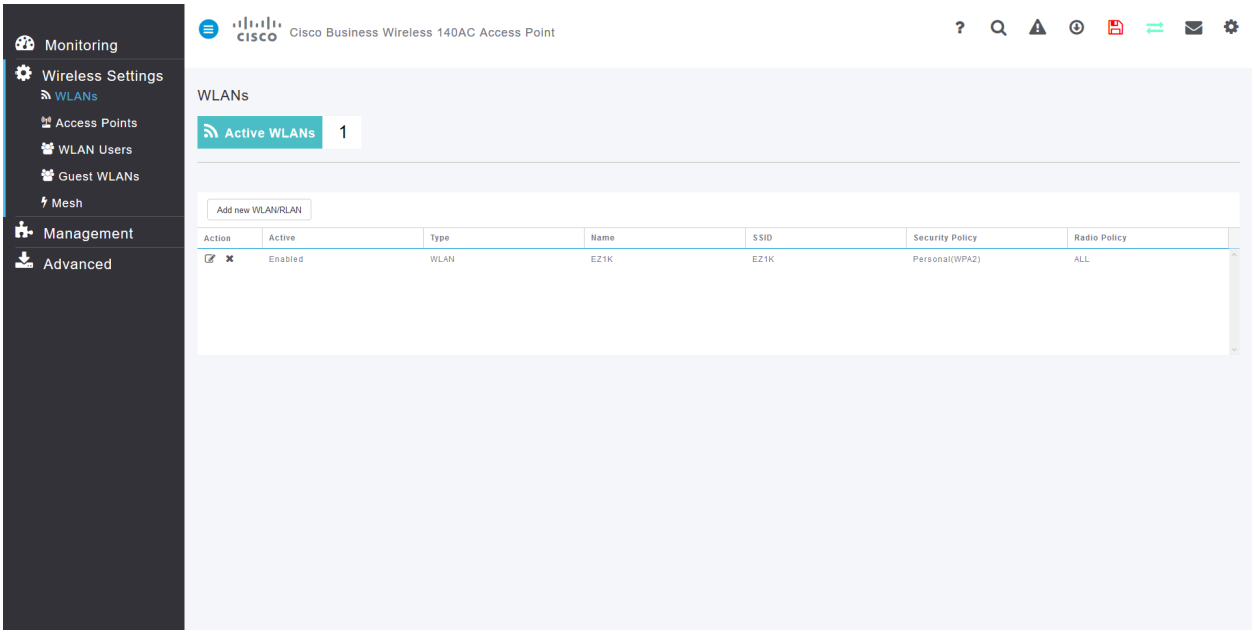
Als deze functie is ingeschakeld, zijn clientgegevens voor uw netwerk te vinden in het gedeelte Monitoring van het web UI.

Stap 1

Klik op **Draadloze instellingen**.

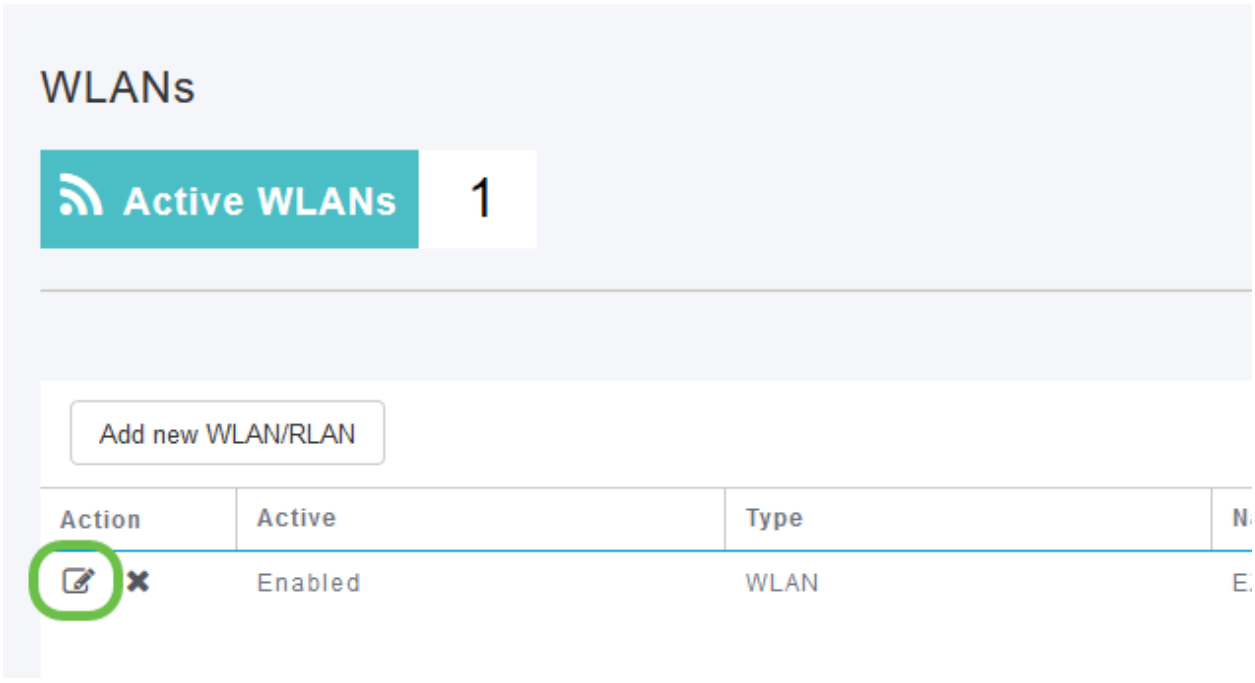


Het onderstaande is gelijk aan wat u ziet wanneer u op de link Draadloze instellingen klikt:



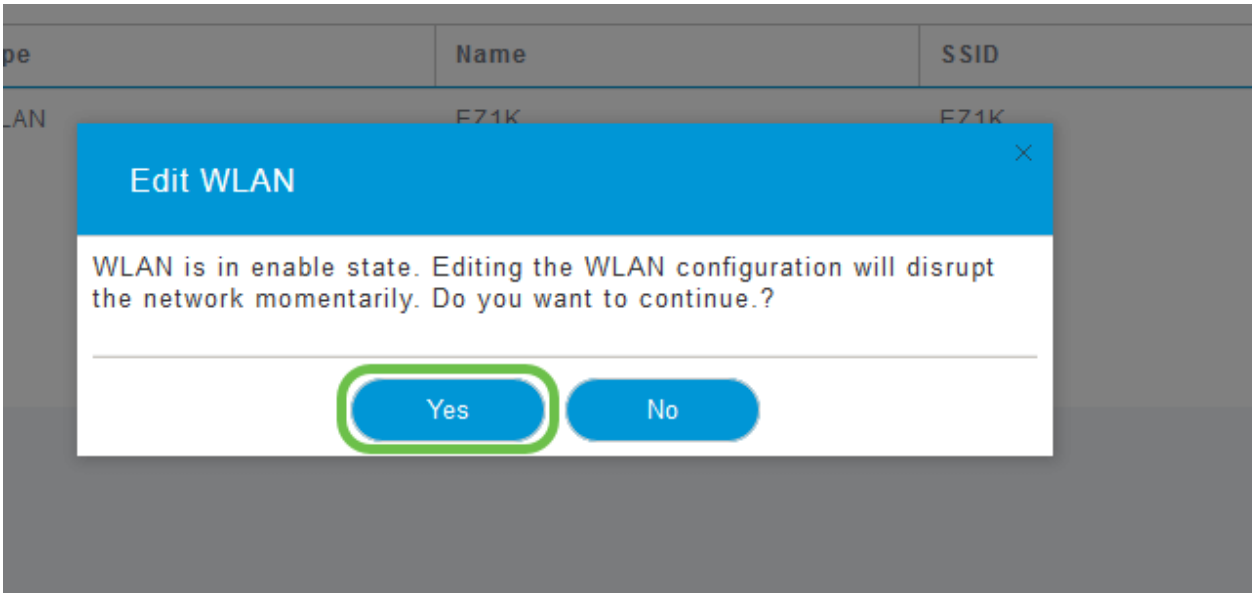
Stap 2

Kies welke WLAN u voor de toepassing wilt gebruiken en klik op het **pictogram** bewerken links van het scherm.



Stap 3

Een pop-up-menu kan op de onderstaande lijst lijken. Dit belangrijke bericht kan de service op uw netwerk tijdelijk beïnvloeden. Klik op **Ja** om verder te gaan.

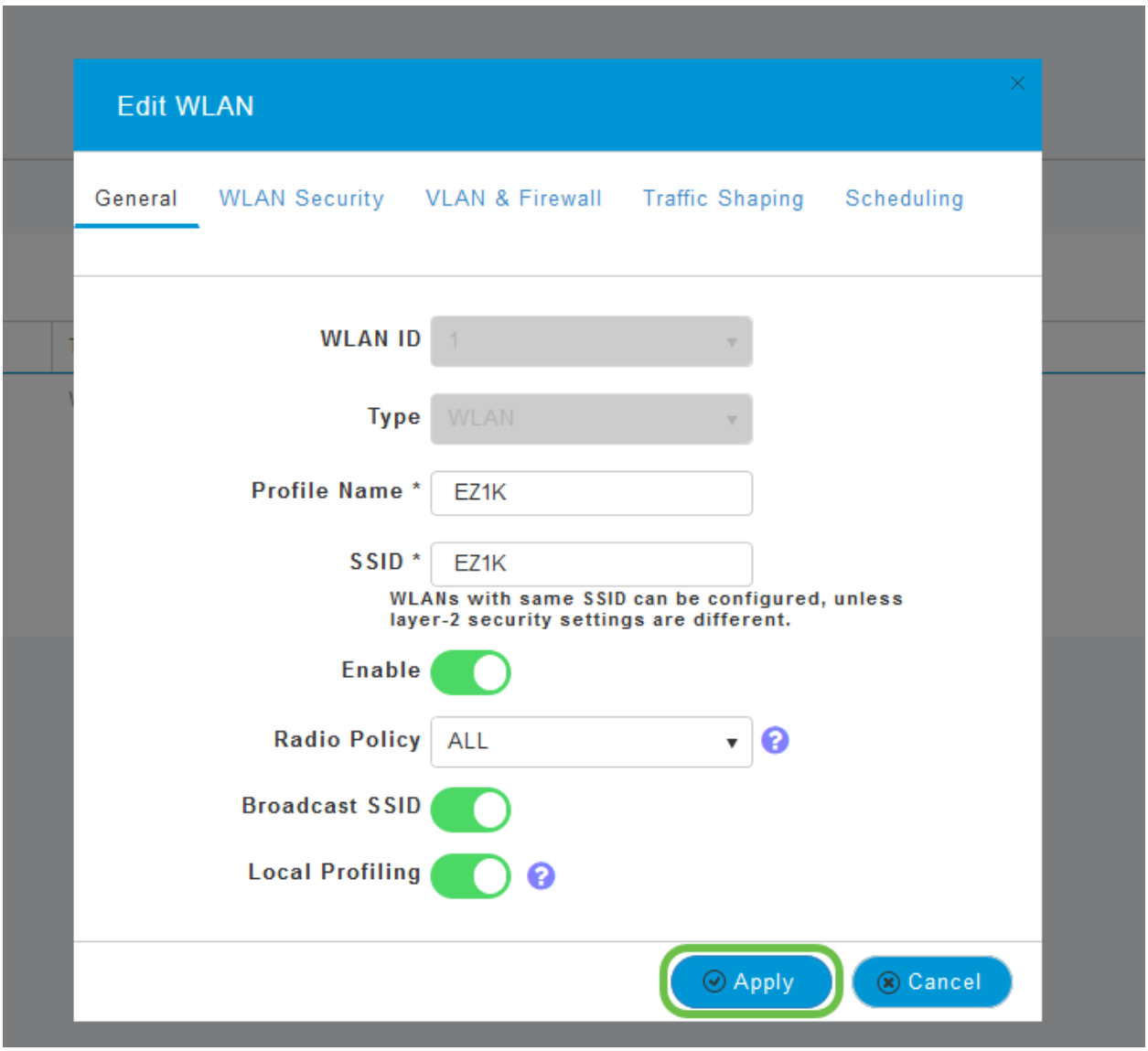


Stap 4

Keer client profileren door op de knop **Local Profilering** te klikken.

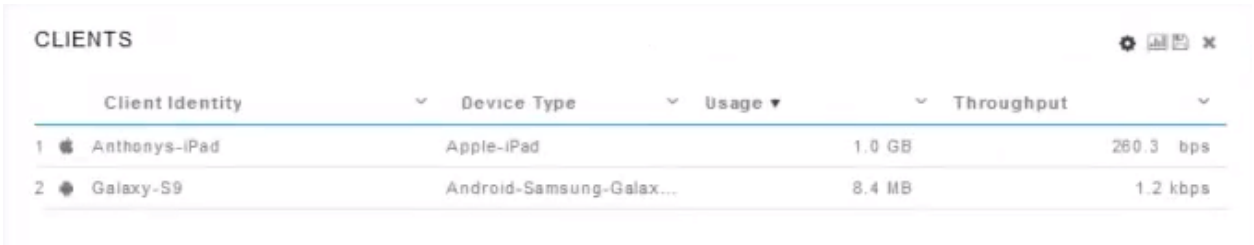
Stap 5

Klik op Apply (Toepassen).



Stap 6

Klik aan de linkerkant op de **optie** in het menu **Monitoring**. U ziet de clientgegevens verschijnen in het Dashboard van het tabblad *Monitoring*.



Conclusie

U hebt nu de instellingen van uw beveiligde netwerk voltooid. Wat een geweldig gevoel, neem nu even een minuut om feest te vieren en aan het werk te gaan!

We willen het beste voor onze klanten, zodat u opmerkingen of suggesties met betrekking tot dit onderwerp hebt. Stuur ons een e-mail naar het Cisco Content Team.

Als u andere artikelen en documentatie wilt lezen, raadpleegt u de ondersteuningspagina's voor uw hardware:

- Cisco RV260P VPN-router met PoE
- Cisco Business 140 AC access point
- Cisco Business 142ACM mesh-extender