Totale netwerkconfiguratie: RV345P en Cisco Business Wireless-N met Web-UI

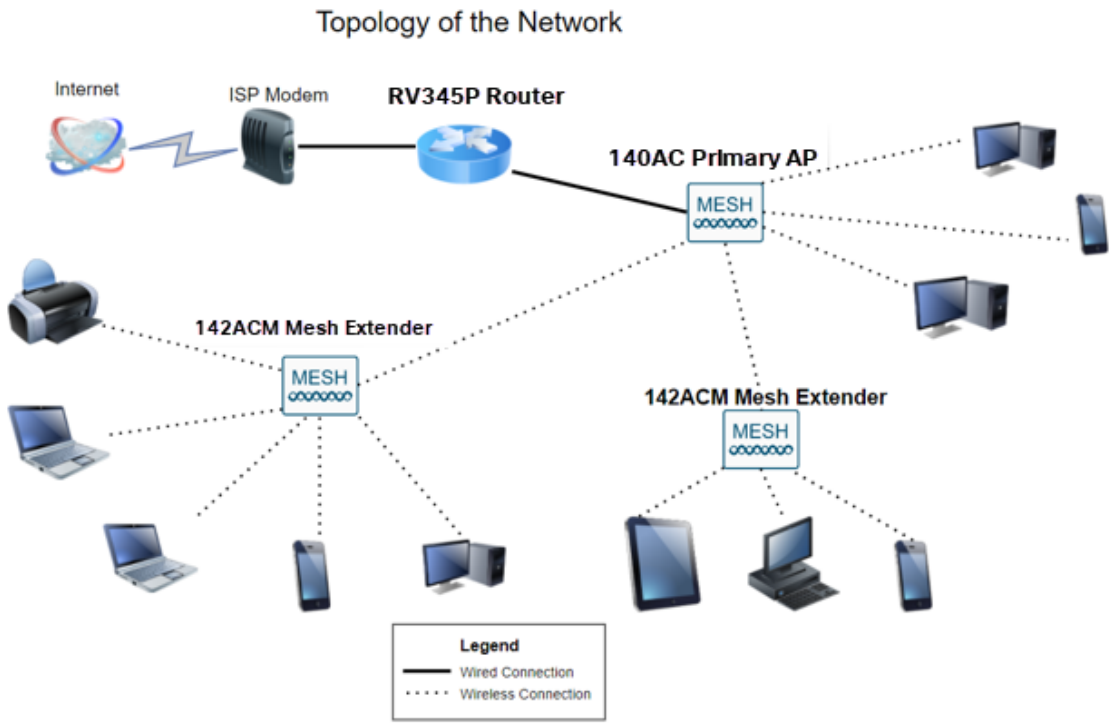
Doel

Deze gids zal u tonen hoe u een draadloos netwerk kunt configureren met behulp van een RV345P router, een CBW140AC access point en twee CBW142ACM mesh extenders.

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.

Inhoud

Topologie



Inleiding

Al uw onderzoek is bij elkaar gekomen en u hebt uw Cisco-apparatuur aangeschaft, hoe opwindend! In dit scenario gebruiken we een RV345P 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.

Deze geavanceerde router biedt ook de optie voor extra functies.

1. Met toepassingscontrole kunt u verkeer besturen. Deze optie kan worden ingesteld om verkeer toe te staan maar te loggen, verkeer te blokkeren en te loggen, of om verkeer te blokkeren.
2. Webfiltering wordt gebruikt om internetverkeer te voorkomen tegen onveilige of ongeschikte websites. Er is geen houtkap met deze functie.
3. AnyConnect is een Secure Socket Layer (SSL) Virtual Private Network (VPN) die

beschikbaar is in Cisco. VPN's maken externe gebruikers en sites in staat om verbinding te maken met uw kantoor of datacenter door een beveiligde tunnel te maken via het internet.

Als u deze functies wilt gebruiken, moet u een licentie aanschaffen. Routers en licenties zijn online geregistreerd, en worden in deze handleiding besproken.

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

Toepasselijke apparaten | Software versie

- RV345P router | 1.0.03.21
- CBW140 AC | 10.4.1.0
- CBW142ACM | 10.4.1.0 (voor het net van mazen is ten minste één extender nodig)

Voorwaarden

Bereid de router voor

1. Zorg ervoor dat u een huidige internetverbinding hebt voor installatie.
2. Neem contact op met uw Internet Service Provider (ISP) om eventuele speciale instructies te vinden die u hebt bij het gebruik van uw RV345P-router. 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.

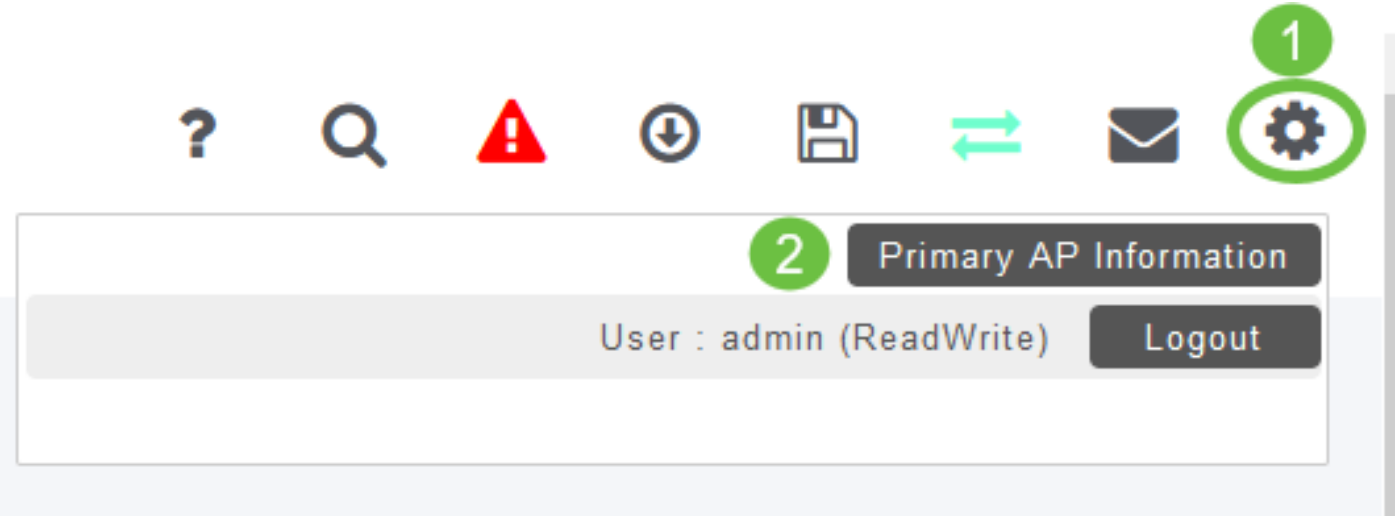
Een Cisco.com-account verkrijgen

Nu u Cisco-apparatuur bezit, moet u een Cisco.com-account krijgen, ook wel Cisco Connection Online Identification (CCO-id) genoemd. Er is geen rekening in rekening gebracht.

Als je al een account hebt, kun je naar de volgende sectie van dit artikel springen.

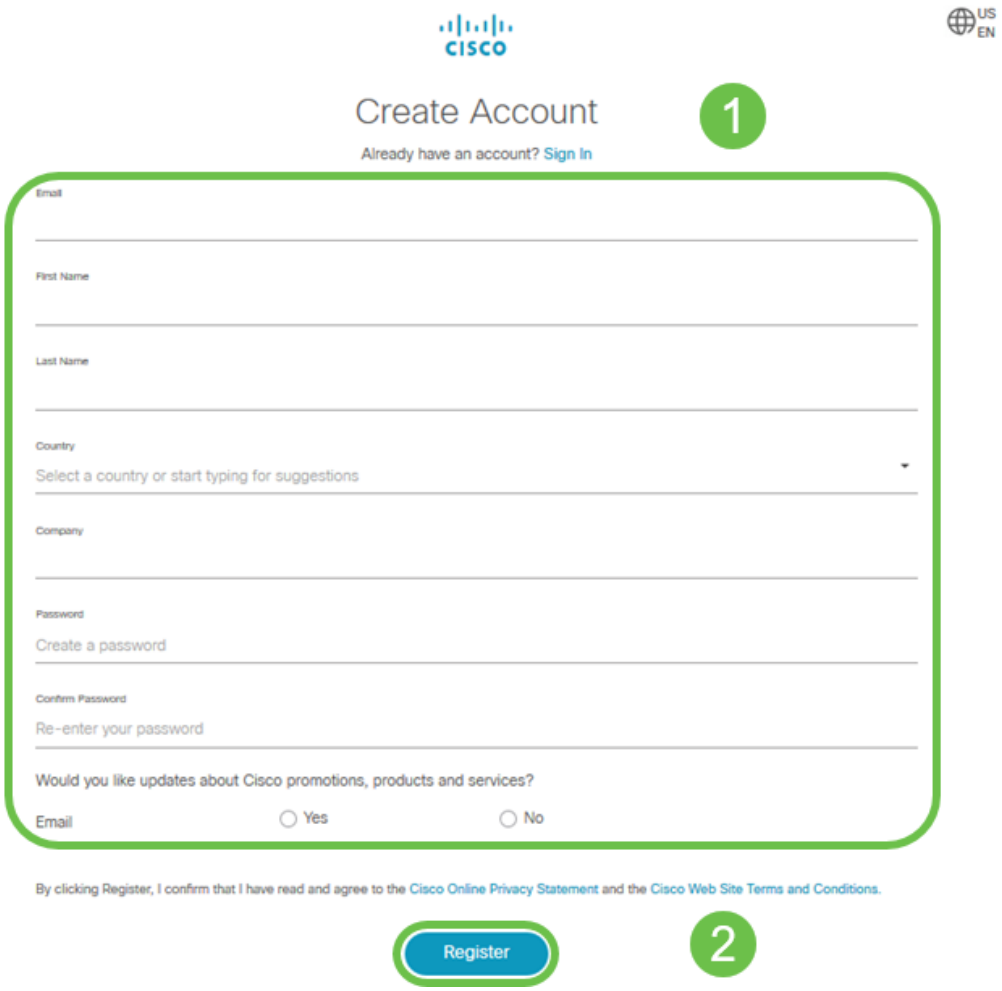
Stap 1

Ga naar Cisco.com. Klik op het **persoonlijke pictogram** en **maak** vervolgens **een account**.



Stap 2

Voer de gewenste gegevens in om de account te maken en klik op **Registreren**. Volg de instructies om het registratieproces te voltooien.



Als u problemen hebt, klikt u op om naar de Help-pagina voor accountregistratie van Cisco.com te springen.

RV345P router configureren

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 RV345P 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).

Ben je klaar? Laten we daar aan werken!

RV345P uit het vakje

Stap 1

Sluit de Ethernet-kabel van een van de RV345P LAN (Ethernet)-poorten aan op de Ethernet-poort van de computer. U hebt een adapter nodig als uw computer geen Ethernet poort heeft. De terminal moet in hetzelfde bekabelde subnetwerk zijn als de RV345P om de eerste configuratie uit te voeren.

Stap 2

Gebruik de voedingsadapter die bij de RV345P is geleverd. Een andere voedingsadapter gebruiken kan de RV345P 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 RV345P, 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 RV345P.

Stap 5

Sluit het andere uiteinde van de RV345P-adapter aan op een stopcontact. Hierdoor wordt de RV345P ingeschakeld. Steek de modem terug in de machine zodat deze ook aan kan. Het stroomlicht op het voorpaneel is stevig groen wanneer de voedingsadapter goed is aangesloten en de RV345P is klaar met starten.

Stel de router in

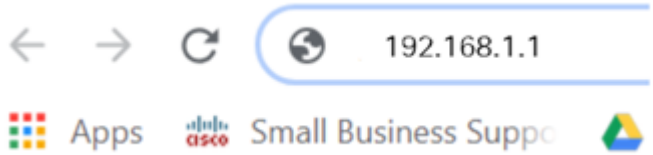
Het voorbereidend werk is gedaan, nu is het tijd om in sommige formaties te geraken! Om het Web UI te lanceren, volg deze stappen.

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.

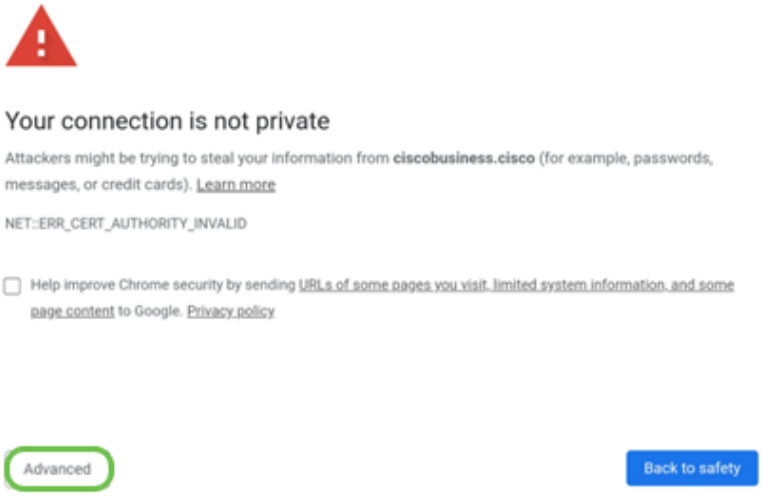
Stap 2

Open een webbrowser zoals Safari, Internet Explorer of Firefox. Voer in de adresbalk het standaard IP-adres van de RV345P, 192.168.1.1 in.



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.

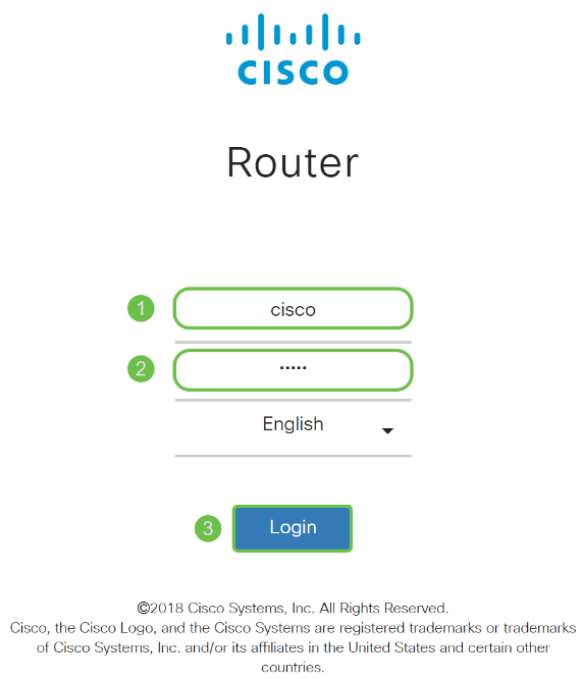


Stap 4

Wanneer de inlogpagina verschijnt, voert u de standaard gebruikersnaam *cisco* in en *cisco* van het defaultwachtwoord.

Klik op **Aanmelden**.

Klik voor gedetailleerde informatie op Hoe u toegang hebt tot de webgebaseerde setup-pagina van Cisco RV340 Series VPN-routers.



Stap 5

Klik op **Aanmelden**. De pagina *Introductie* verschijnt. Als het navigatiedeelvenster niet is geopend, kunt u dit openen door op het **menupictogram** te klikken.

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 **ping 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 dit artikel van Problemen oplossen 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 RV345P). Om verbinding te maken, moet u mogelijk de netwerkinstellingen van RV345P wijzigen. Als u Windows 10 gebruikt, raadpleegt u Windows 10-aanwijzingen om de netwerkinstellingen te wijzigen.

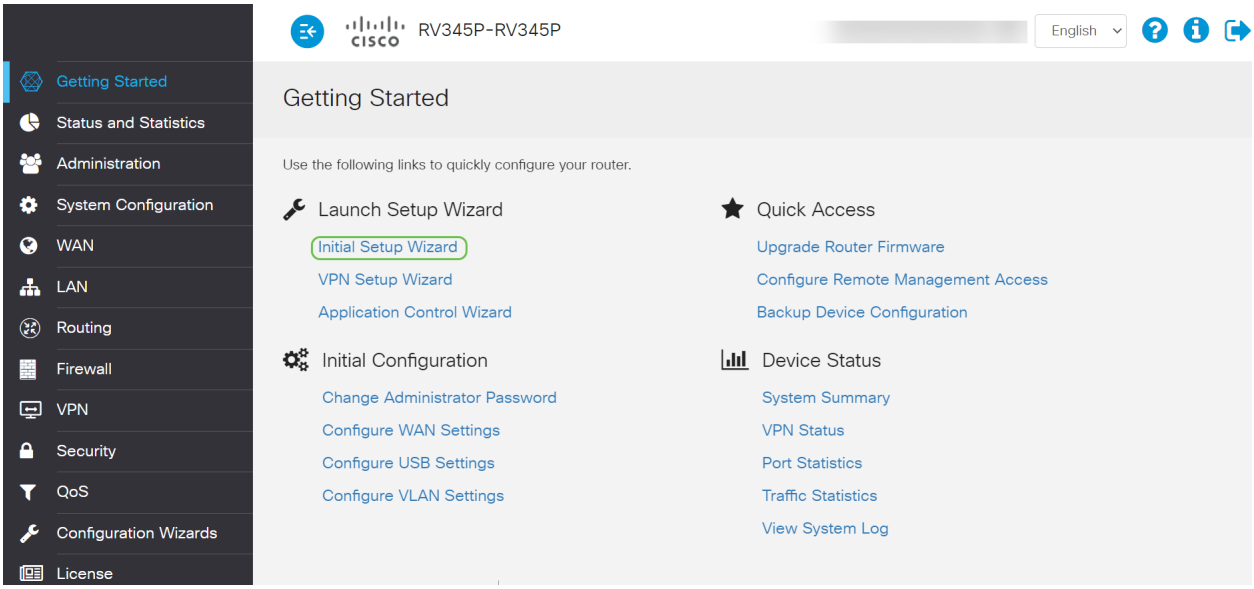
3. Als u bestaand apparaat hebt dat het 192.168.1.1 IP-adres bezet houdt, zult u dit conflict moeten oplossen zodat het netwerk kan functioneren. Klik hier aan het einde van dit gedeelte of klik hier om direct te worden ingenomen.
4. Reset de modem en de RV345P door beide apparaten uit te schakelen. Zet de modem vervolgens aan en laat het ongeveer 2 minuten niets doen. Zet de RV345P vervolgens aan. 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 *met de* wizard *Initiële installatie uit* te voeren die in deze sectie zijn beschreven. U kunt deze instellingen op elk moment wijzigen.

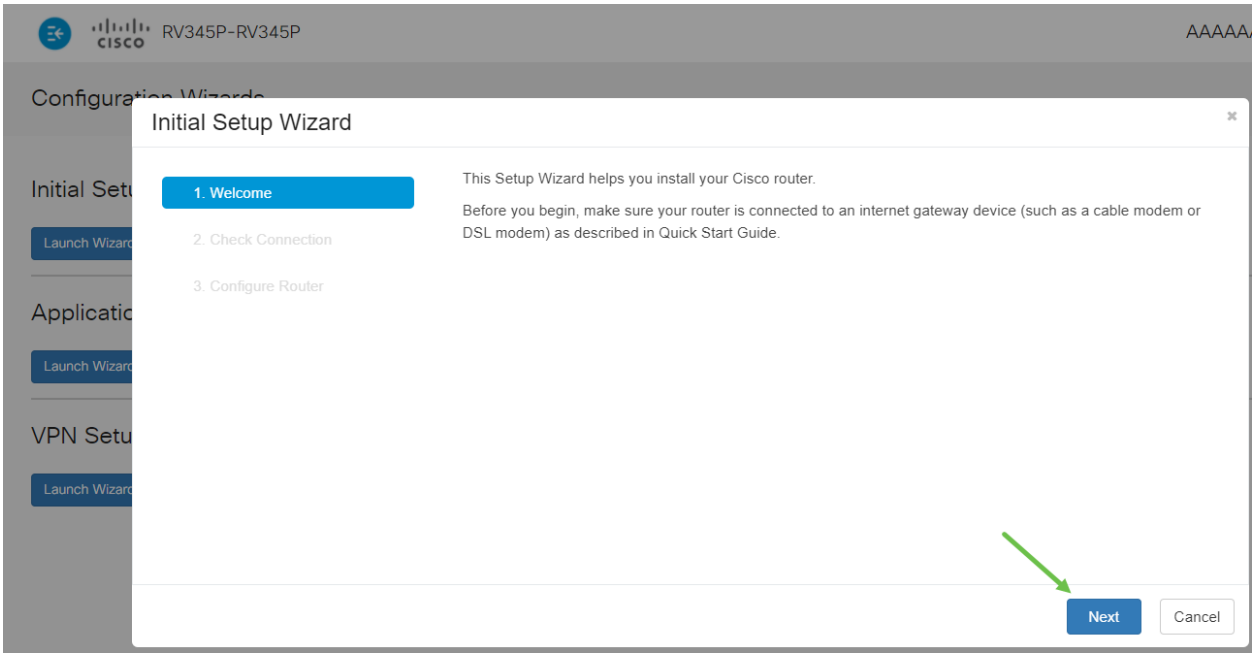
Stap 1

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



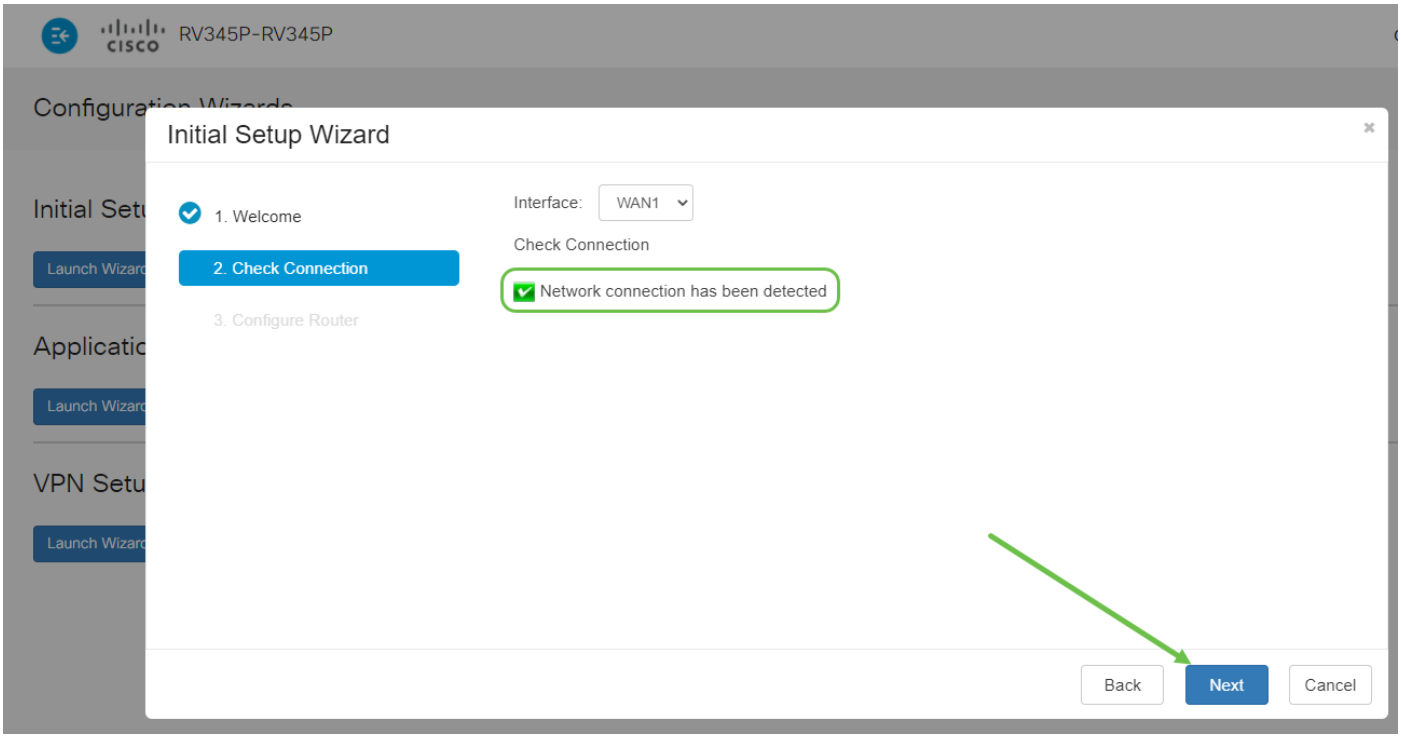
Stap 2

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



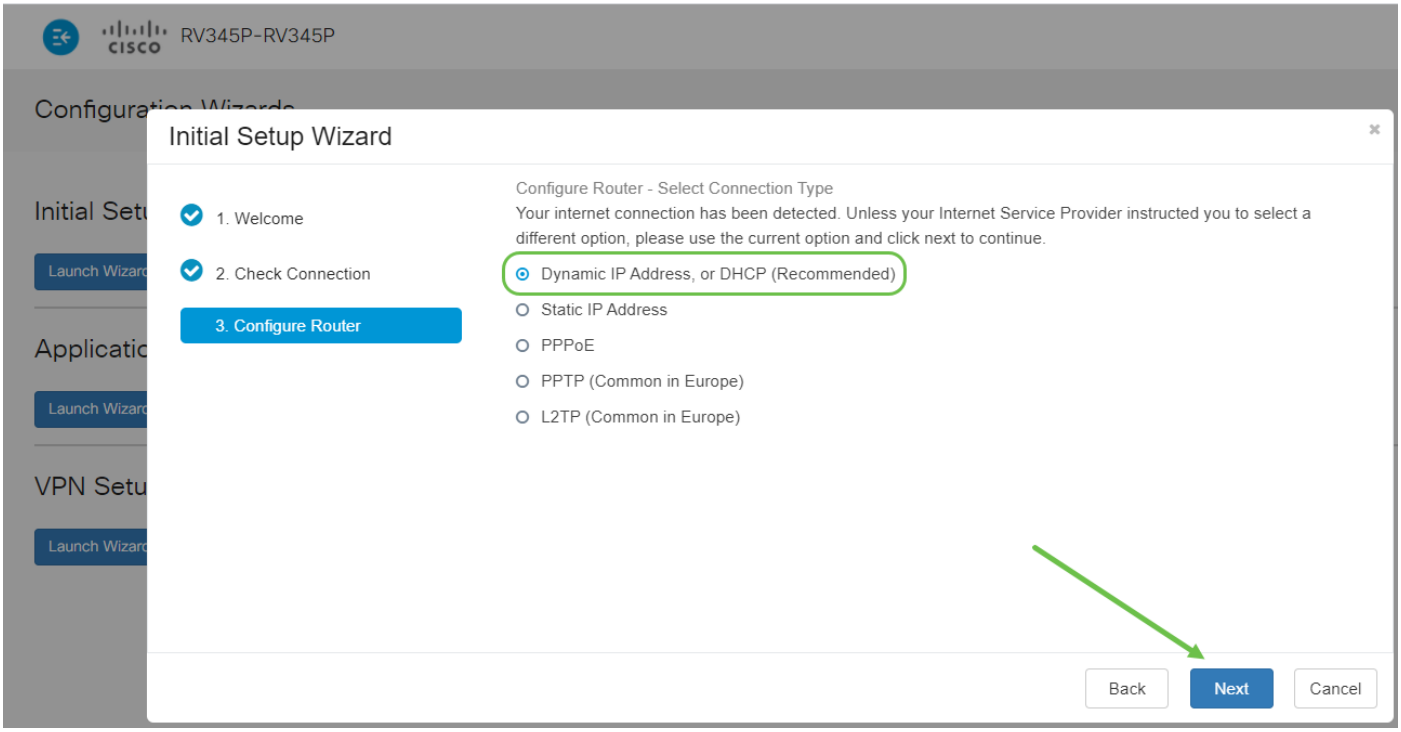
Stap 3

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**.



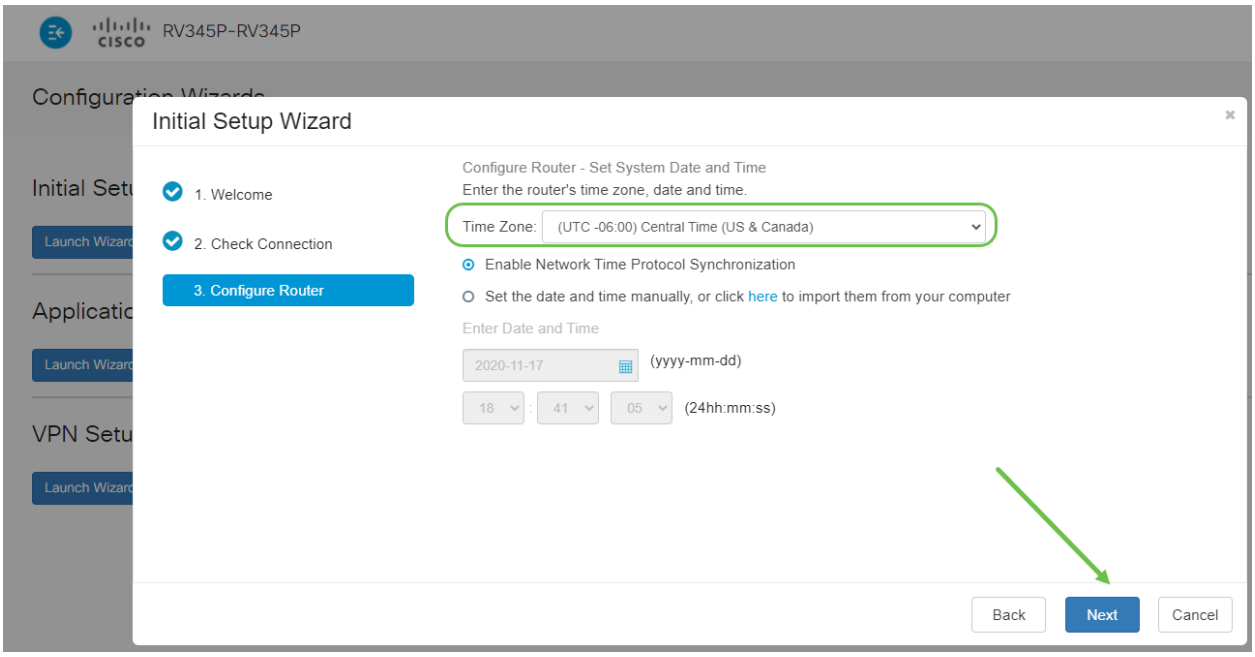
Stap 4

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**.



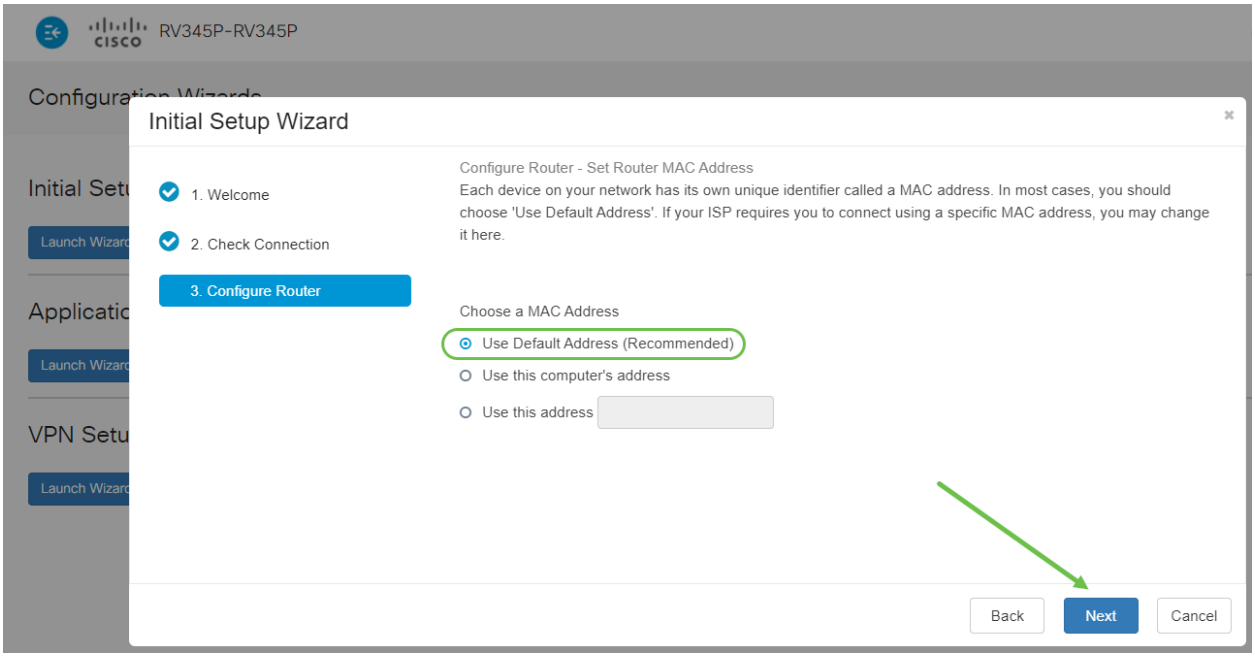
Stap 5

U wordt 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**.



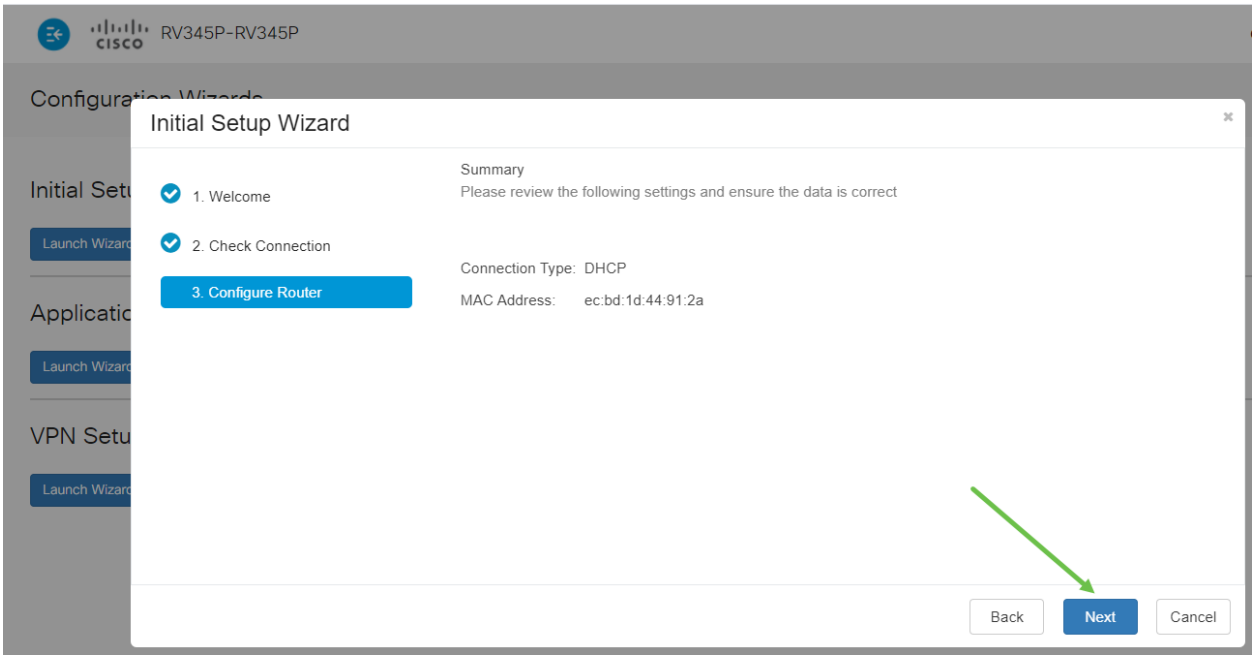
Stap 6

U selecteert welke MAC-adressen aan apparaten moeten worden toegewezen. Meestal gebruikt u het standaardadres. Klik op **Volgende**.



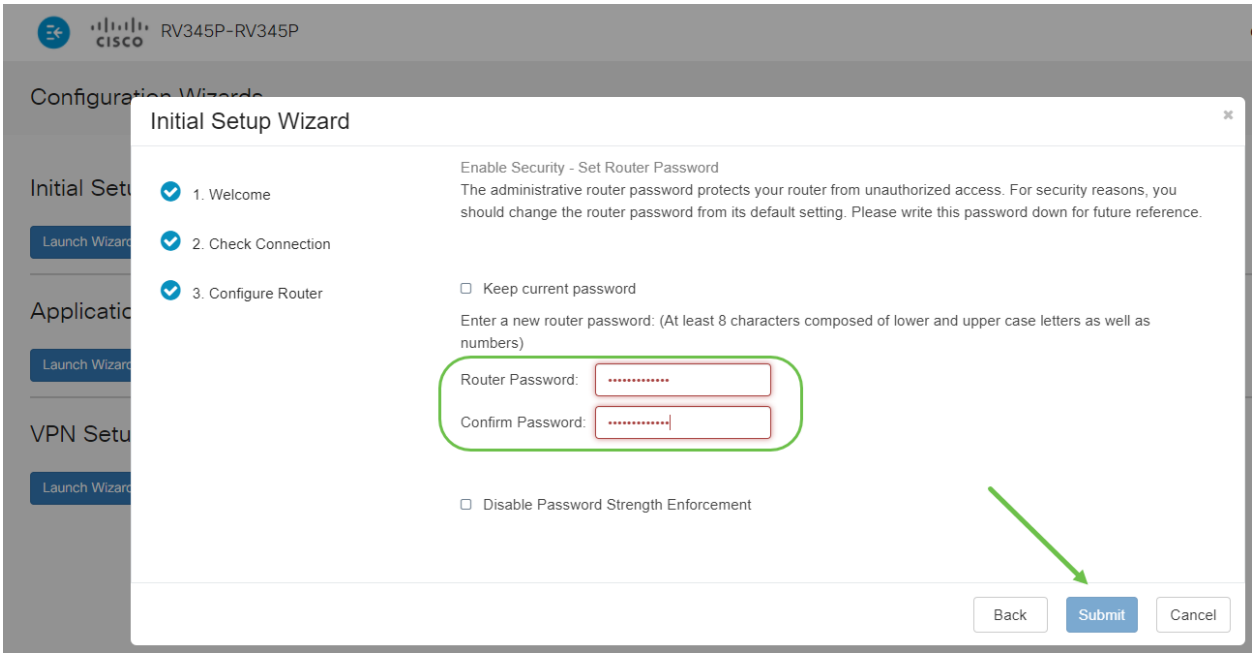
Stap 7

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**.

Als u meer informatie over deze instellingen wilt, kunt u DHCP-instellingen configureren op de RV34x-router.

Uw RV345P heeft Power over Ethernet (PoE) ingeschakeld door standaard, maar u kunt er een aantal aanpassingen aan aanbrengen. Als u de instellingen wilt aanpassen, controleert u instellingen voor Power over Ethernet (PoE) op de RV345P router.

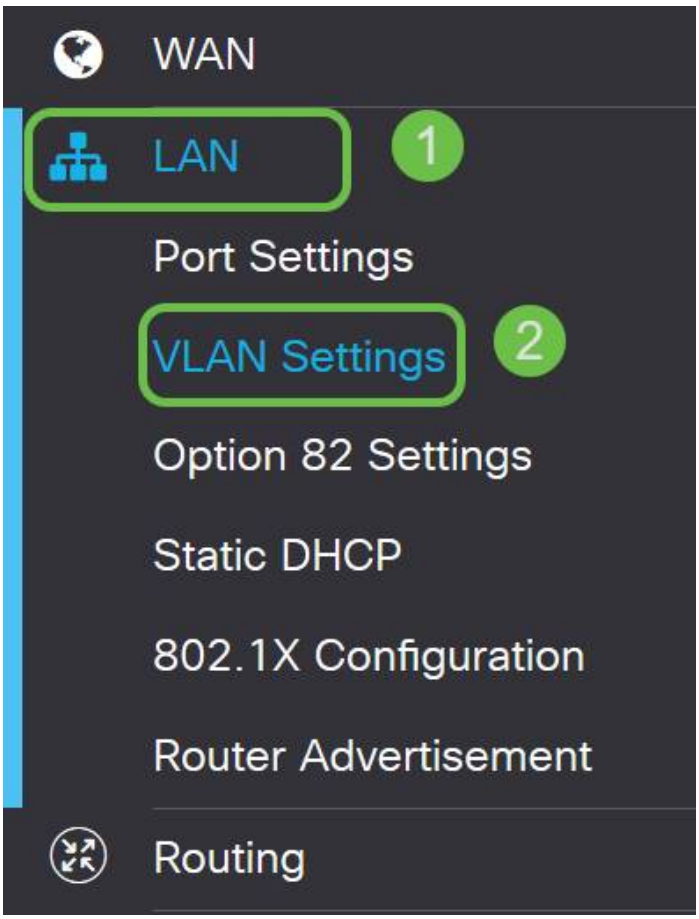
Indien nodig een IP-adres bewerken (optioneel)

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.

Dit proces is alleen nodig als uw IP-adres van de router een specifiek adres in uw bestaande netwerk moet worden toegewezen. Als u geen IP-adres hoeft te bewerken, kunt u naar de volgende sectie van dit artikel gaan.

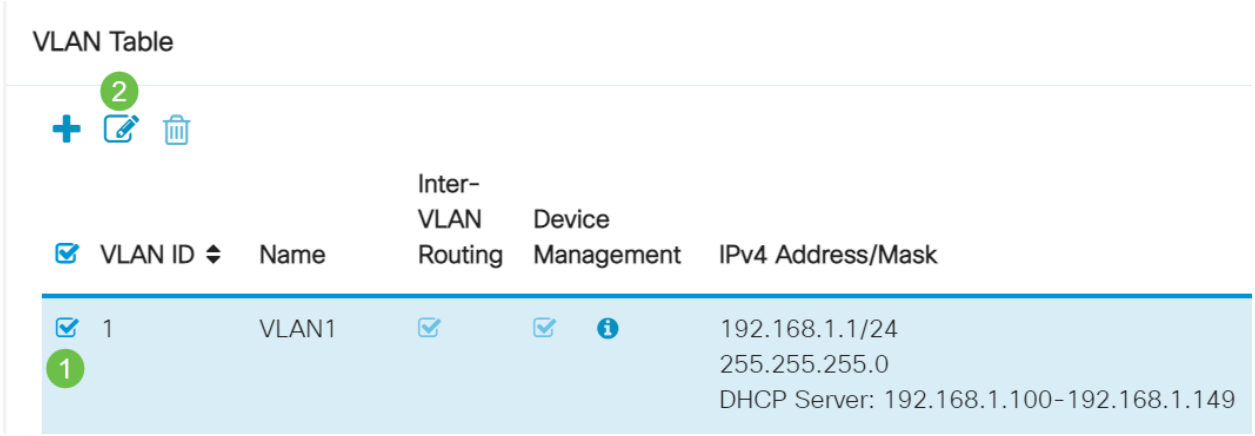
Stap 1

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



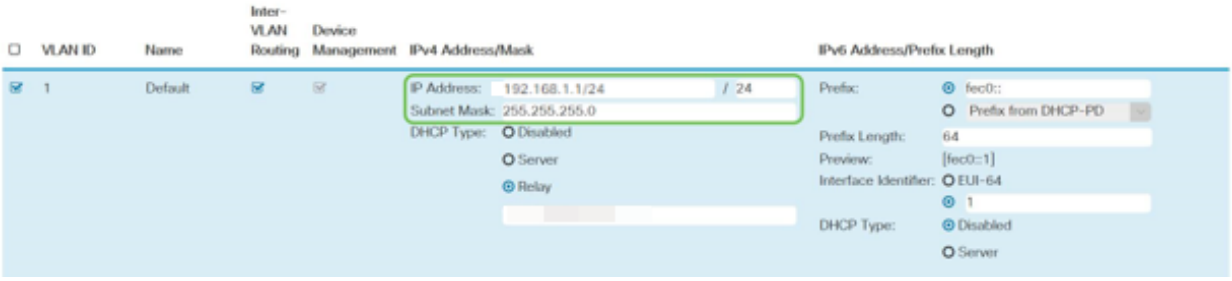
Stap 2

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



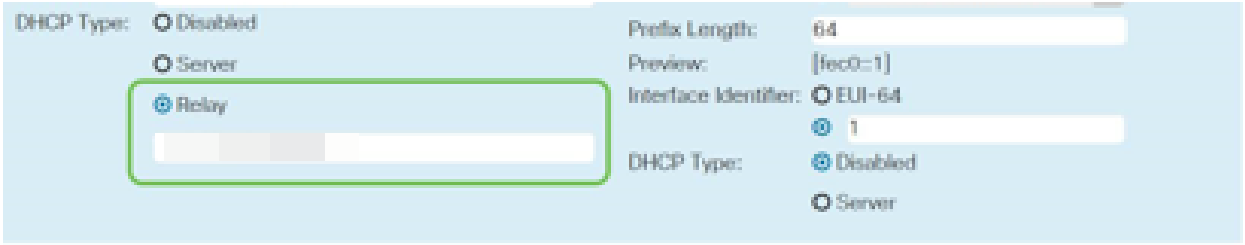
Stap 3

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.

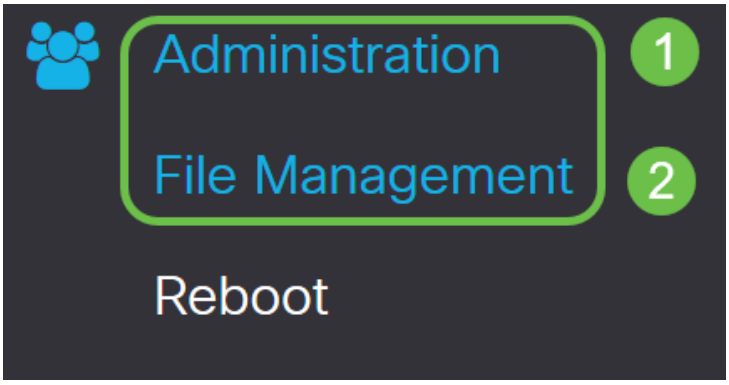


Upgradefirmware indien nodig

Dit is een belangrijke stap, sla het niet over!

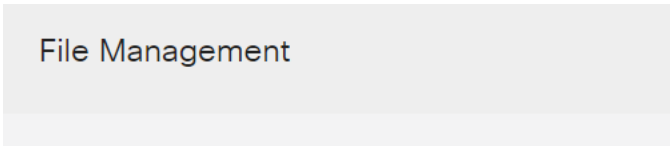
Stap 1

Kies **Beheer > Bestandsbeheer**.



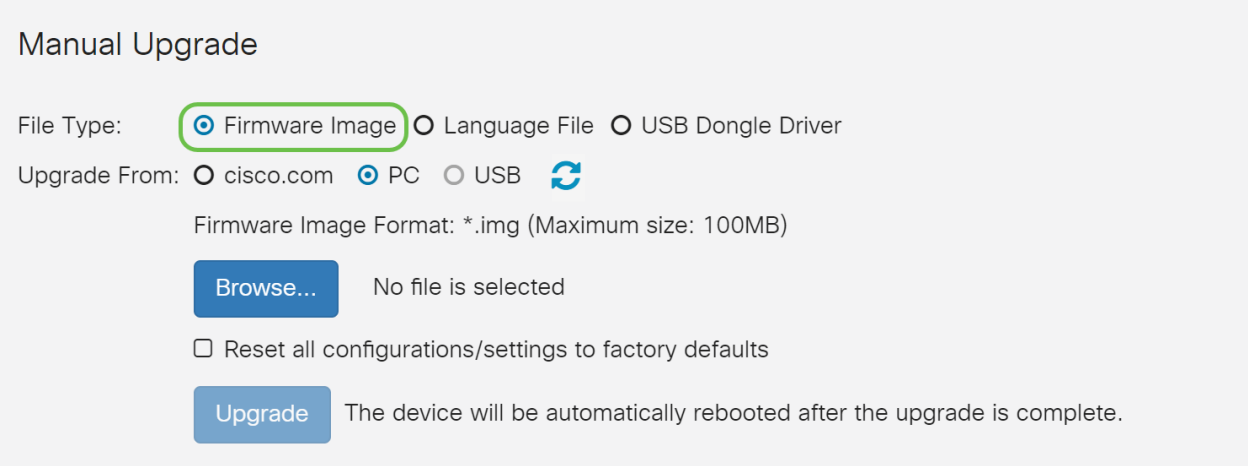
In het gebied *systeeminformatie* beschrijven de volgende subgebieden het volgende:

- 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

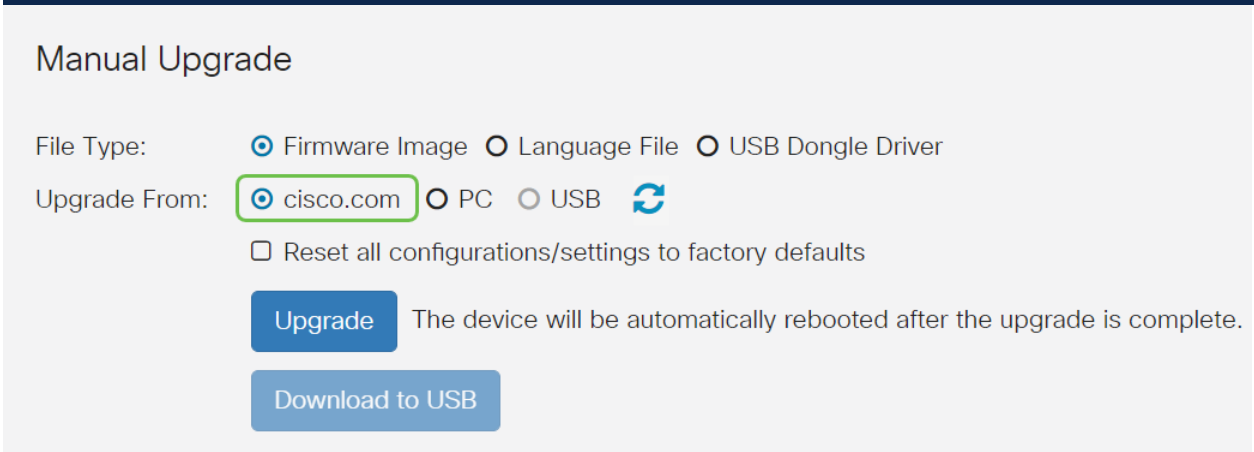
Klik onder het gedeelte *Handmatige upgrade* op de knop **Afbeelding firmware** voor *bestandstype*.



Stap 3

Klik op de pagina *Handmatige upgrade* op de radioknop 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.

Als uw apparaat niet op het internet is aangesloten of lijdt aan internetverbindingen kunt u geen upgrade vanaf cisco.com uitvoeren. Als dit voor u geldt, zijn hier alternatieve opties te vinden.

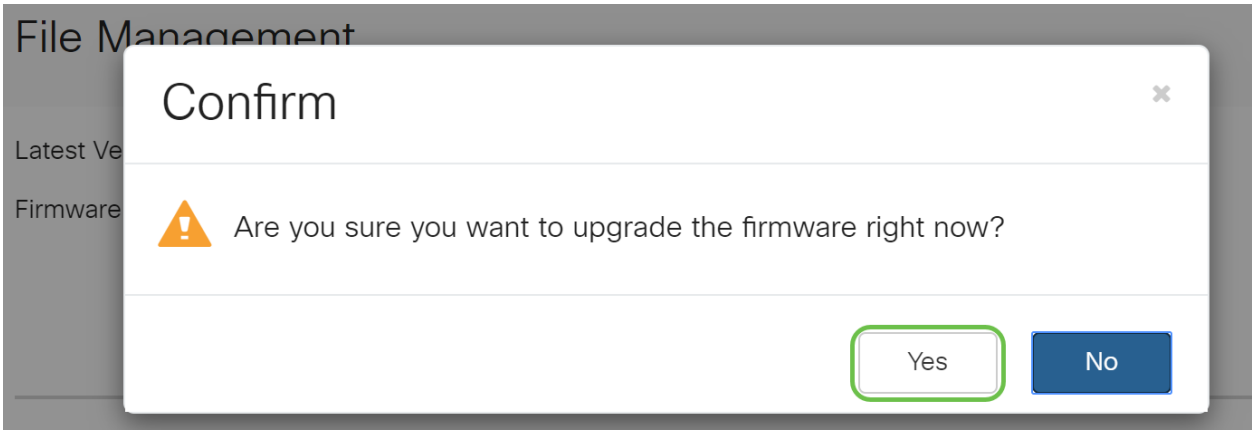


Stap 4

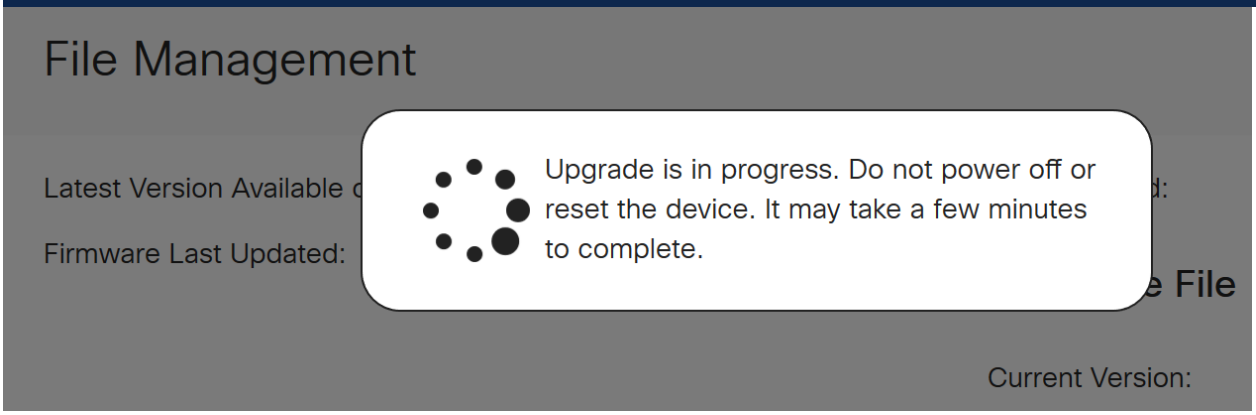
Klik op **upgrade**.

Stap 5

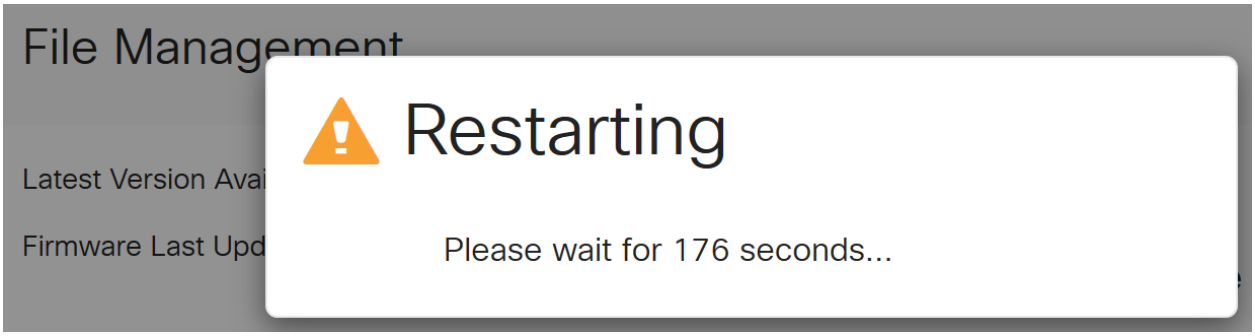
Klik op **Ja** in het bevestigingsvenster om verder te gaan.



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

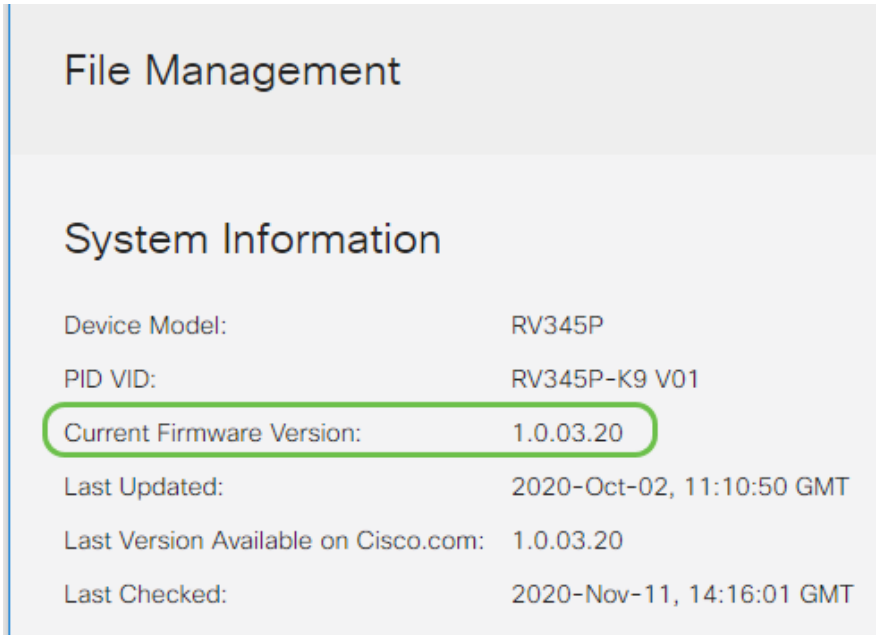


Nadat de upgrade is voltooid, verschijnt er een melding-venster om u te laten weten dat de router *opnieuw start* met een aftelsom van de geschatte tijd die u nodig hebt om het proces te voltooien. Daarna wordt je uitgelogd.



Stap 6

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

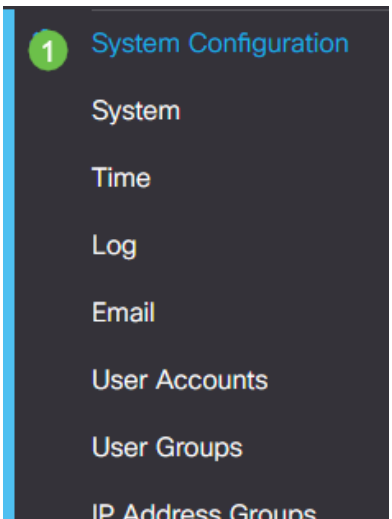


Configureer automatische updates met de RV345P Series router

Aangezien updates zo belangrijk zijn en u een druk persoon bent, is het verstandig om automatische updates vanuit hier buiten te configureren!

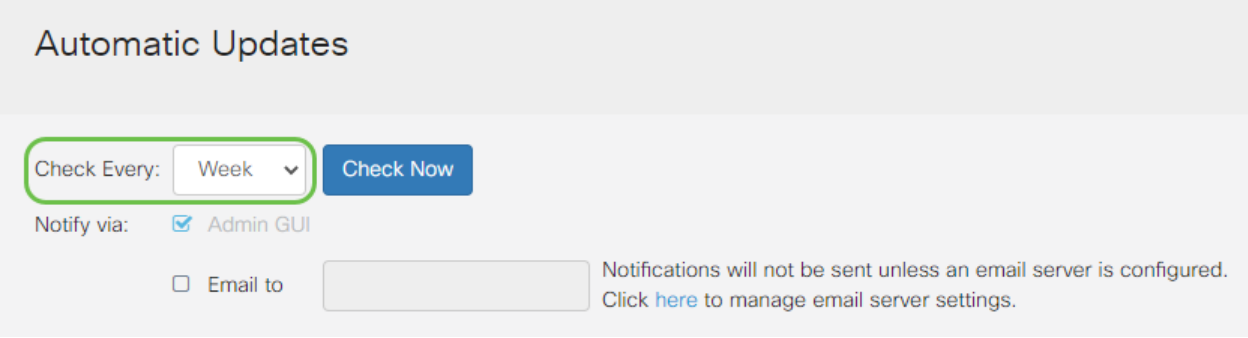
Stap 1

Meld u aan bij het webgebaseerde hulpprogramma en kiest u **systeemconfiguratie > Automatische updates**.



Stap 2

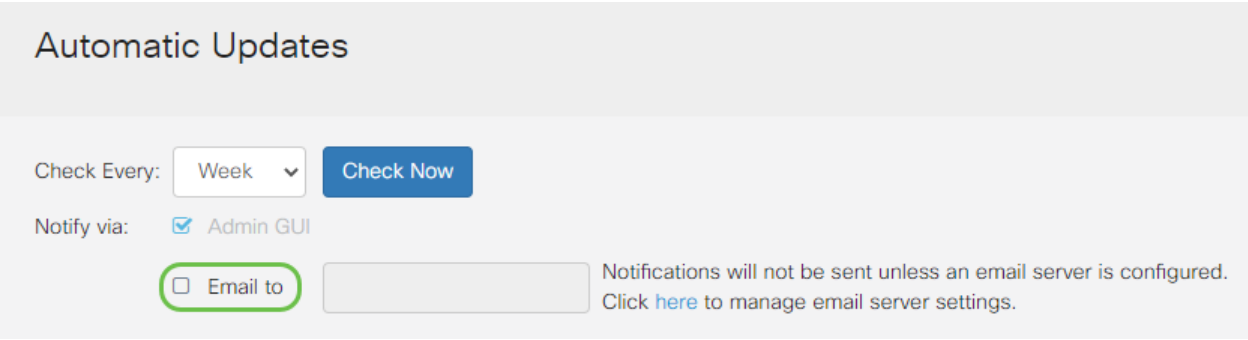
Kies in de vervolgkeuzelijst *Elk* controleren hoe vaak de router moet controleren op updates.



Stap 3

Schakel in het *gedeelte* Melden *via* het vakje **E-mail naar** selectieteken in om updates via e-mail te ontvangen. Het selectieteken *Admin GUI* zijn standaard ingeschakeld en kunnen niet worden uitgeschakeld. Zodra een update beschikbaar is, verschijnt er een bericht in de webconfiguratie.

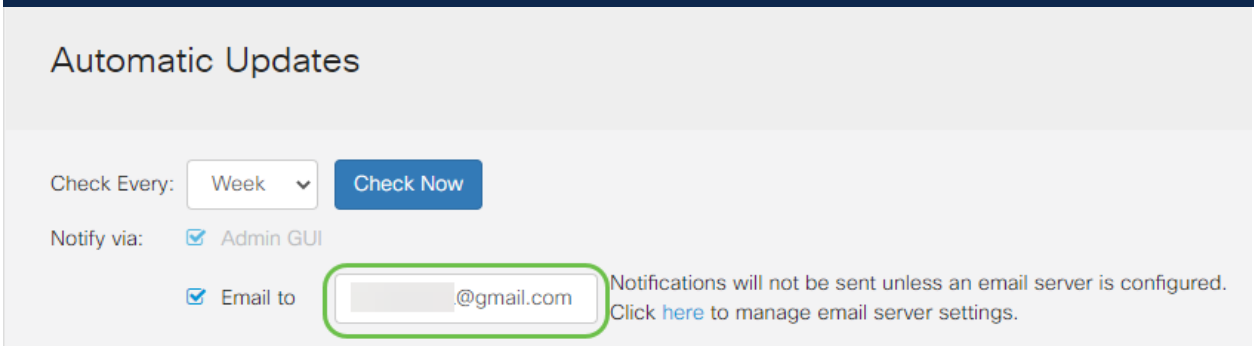
Als u instellingen voor e-mailservers wilt instellen, klikt u hier om te weten hoe.



Stap 4

Voer in het veld *E-mail* een e-mailadres in.

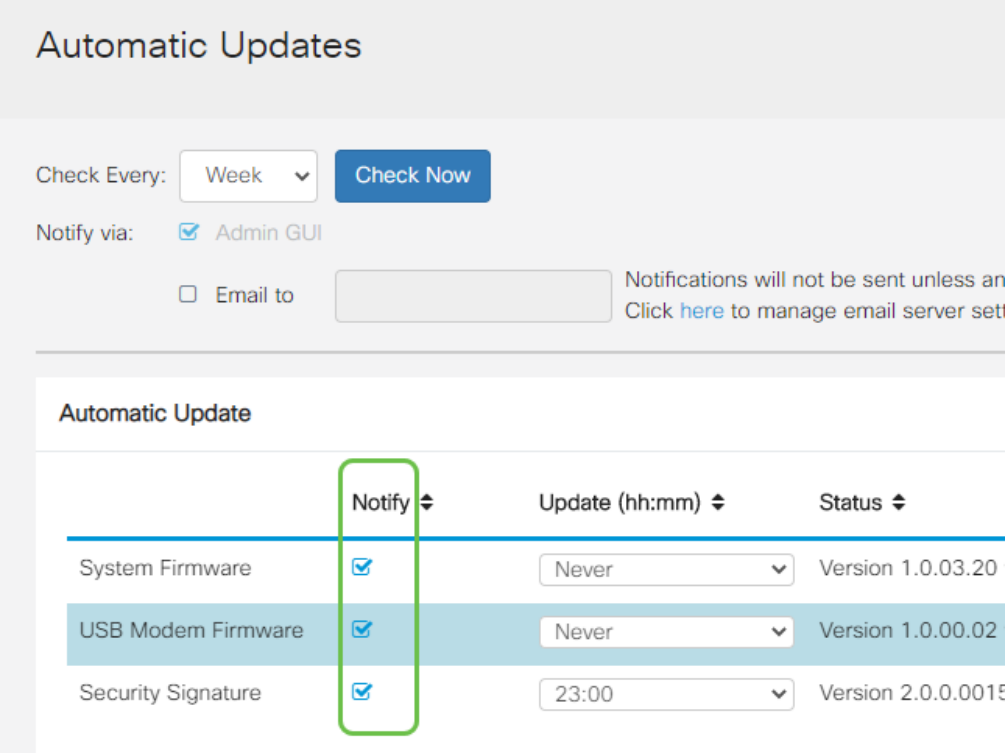
Het is sterk aanbevolen om een aparte e-mailaccount te gebruiken in plaats van je persoonlijke e-mail om privacy te behouden.



Stap 5

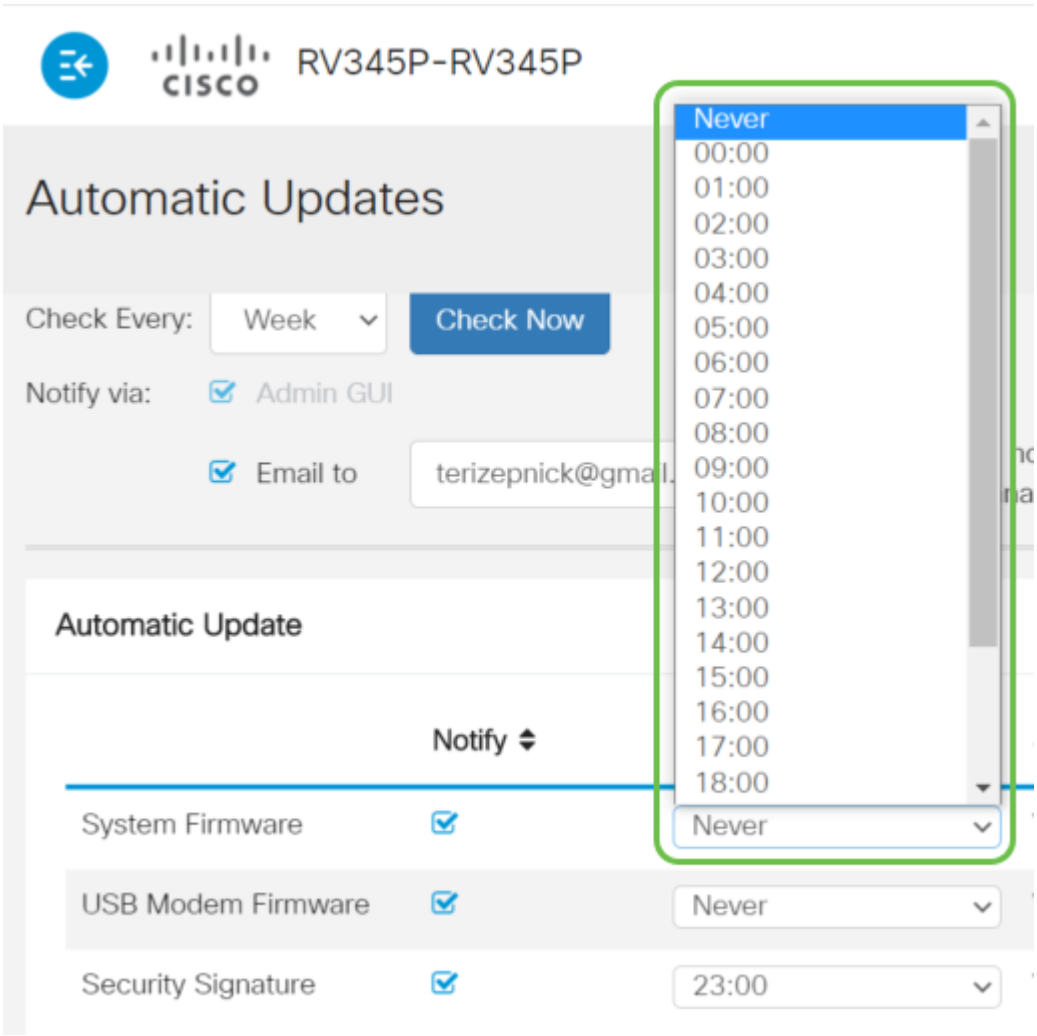
Selecteer onder het gebied *Automatisch bijwerken* de selectieteksten van het soort updates waarover u wilt worden geïnformeerd. De opties zijn:

- System Firmware — het hoofdprogramma voor de besturing van het apparaat.
- USB-modemfirmware — Het controleprogramma of stuurprogramma voor de USB-poort.
- Security Signature - Dit zal handtekeningen bevatten voor Application Control om toepassingen, typen apparaten, besturingssystemen enzovoort te identificeren.



Stap 6

Kies in de vervolgkeuzelijst *Automatische update* een tijdstip van de dag waarop u de automatische update wilt uitvoeren. Sommige opties kunnen variëren afhankelijk van het gekozen type update. Security Signature is de enige optie voor een onmiddellijke bijwerking. Aanbevolen wordt om een tijdstip in te stellen waarop uw kantoor is gesloten zodat de service niet op een ongelegen tijdstip wordt onderbroken.



De status geeft de huidige versie van de firmware of de veiligheidshandtekening weer.

Stap 7

Klik op Apply (Toepassen).

Stap 8

Als u de configuratie permanent wilt opslaan, gaat u naar de pagina Configuration kopiëren/opslaan of klikt u op het **pictogram** voor het **opslaan** in het bovenste gedeelte van de pagina.

Dit geldt ook voor uw basisinstellingen op uw router! Nu heb je een aantal configuratieopties om te verkennen.

Beveiligingsopties

Natuurlijk wil je dat je netwerk veilig is. Er zijn een aantal eenvoudige opties, zoals het hebben van een complex wachtwoord, maar als u stappen voor een nog veiliger netwerk wilt ondernemen, controleer dan deze sectie over veiligheid.

RV-beveiligingslicentie (optioneel)

Met deze RV Security Licentiefuncties beschermt u uw netwerk tegen aanvallen op het internet:

- Inbraakpreventiesysteem (IPS): Inspecteert netwerkpakketten, logs en/of blokken een brede reeks netwerkaanvallen. Het biedt meer netwerkbeschikbaarheid, sneller herstel en uitgebreide bedreigingsbescherming.
- Antivirus: Bescherming tegen virussen door de toepassingen te scannen voor verschillende protocollen zoals HTTP, FTP, e-mailbijlagen, POP3 e-mailbijlagen en IMAP e-mail bijlagen die door de router gaan.
- Web security Maakt bedrijfsefficiëntie en beveiliging mogelijk terwijl u verbinding maakt met het internet, maakt internettoegangsbeleid mogelijk voor eindapparaten en internettoepassingen om prestaties en beveiliging te garanderen. Het is op de cloud gebaseerd en bevat meer dan 80 categorieën met meer dan 450 miljoen geclassificeerde domeinen.
- Identificatie van de toepassing: Vastleggen en toewijzen van beleid aan internettoepassingen. 500 unieke toepassingen worden automatisch geïdentificeerd.
- Clientidentificatie: Klanten dynamisch identificeren en categoriseren. De mogelijkheid om beleid toe te wijzen op basis van de categorie eindapparatuur en het besturingssysteem.

De RV Security-licentie biedt webfiltering. Webfiltering is een functie waarmee u de toegang tot ongeschikte websites kunt beheren. Zij kan de verzoeken om toegang tot het web van een cliënt onderzoeken om te bepalen of zij die website al dan niet toestaan of ontkennen.

De gelicentieerde beveiligingsfuncties kunnen gedurende 90 dagen zonder kosten worden getest. Als u na de evaluatieperiode de geavanceerde beveiligingsfuncties op uw router wilt blijven gebruiken, moet u een licentie verkrijgen en activeren.

Een andere beveiligingsoptie is Cisco Umbrella. Klik hier als u in plaats daarvan naar de Umbrella-sectie wilt springen.

Als u geen van beide beveiligingslicenties wilt gebruiken, klikt u op om naar het VPN-gedeelte van dit document te springen.

Inleiding tot slimme rekeningen

Om de RV Security Licentie te kunnen aanschaffen, hebt u een Smart Account nodig.

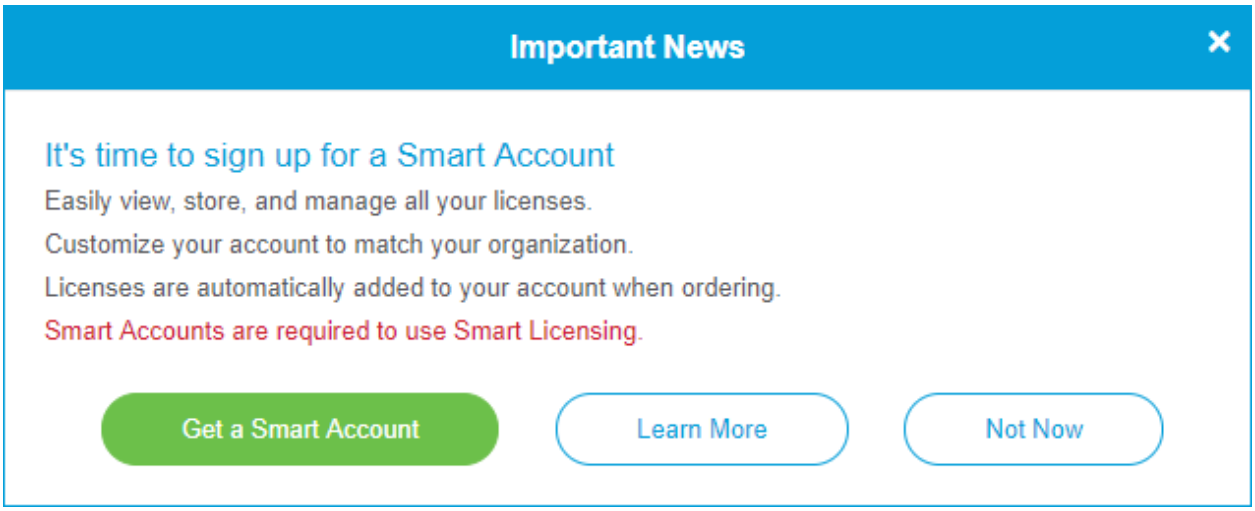
Door toestemming te geven voor het activeren van deze Smart-account, stemt u ermee

in dat u namens uw organisatie rekeningen kunt maken en product- en servicerechten, licentieovereenkomsten en toegang van gebruikers tot rekeningen kunt beheren. Cisco-partners kunnen geen toestemming geven voor het maken van account namens klanten.

Het creëren van een nieuwe Smart Account is een eenmalige gebeurtenis en vanaf dat moment wordt het beheer door het instrument geboden.

Een slimme account maken

Wanneer u toegang hebt tot uw algemene Cisco-account met uw Cisco.com-account of CCO-id (de account die u aan het begin van dit document hebt gemaakt), kunt u met een bericht worden begroet om een slimme account te maken.



Als u deze pop-up niet hebt gezien, kunt u klikken om aan de pagina voor het maken van een slimme account te worden gehouden. U moet mogelijk met uw Cisco.com-accountreferenties inloggen.

Klik hier voor meer informatie over de stappen die betrokken zijn bij het aanvragen van uw slimme account.

Let erop dat u nota neemt van uw rekeningnaam en andere registratiegegevens.

Snelle Tip: Als u een domein moet invoeren en u geen domein hebt, kunt u uw e-mailadres in de vorm van *name@domain.com* invoeren. Gewoonlijk zijn e-mail, yahoo, enz., afhankelijk van uw bedrijf of leverancier.

Het is heel belangrijk dat u een Cisco.com (CCO ID)-account en een Cisco Smart-account hebt voordat u de RV-beveiligingslicentie aanschaft.

RV-beveiligingslicentie kopen

U moet een licentie aanschaffen bij uw Cisco-distributeur of uw Cisco-partner. Om een partner van Cisco te vinden, klik hier.

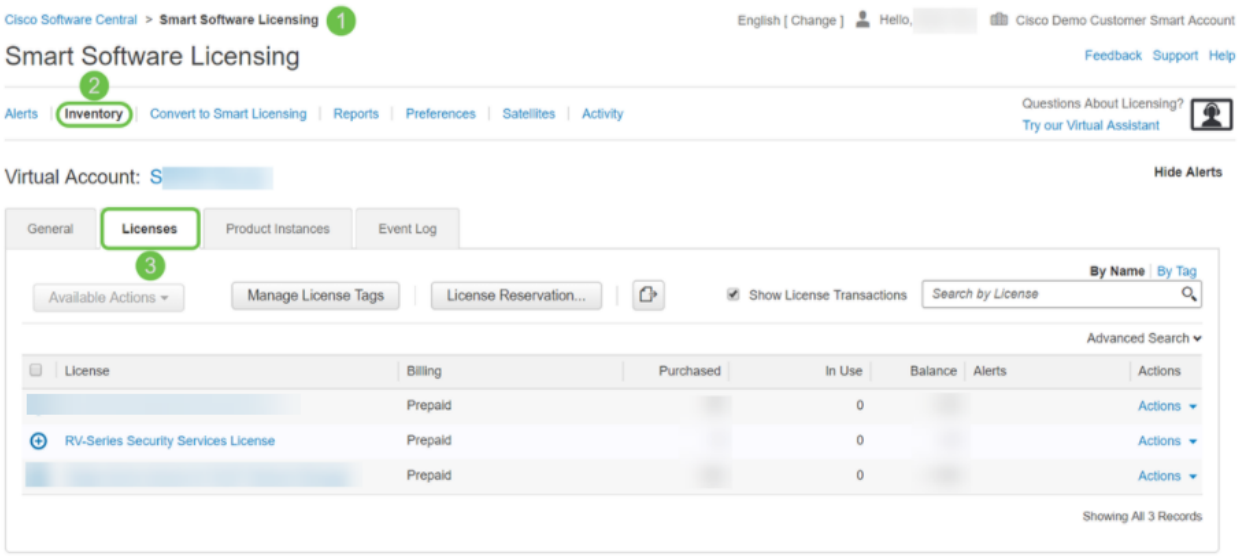
In de onderstaande tabel wordt het onderdeelnummer voor de licentie weergegeven.

Type	Product-ID	Beschrijving
Licentie voor RV-beveiliging	LS-RV34X-SEC-1YR=	RV-beveiliging: 1 jaar: Dynamisch webfilter, Application Visibility and Identification and Statistics, Gateway Antivirus en Inbraakpreventiesysteem IPS.

De licentiesleutel wordt niet rechtstreeks in uw router ingevoerd, maar zal aan uw Cisco Smart-account worden toegewezen nadat u de licentie hebt besteld. Welke tijd het kost om de licentie op je account te laten verschijnen, is mede afhankelijk van het moment dat de partner de opdracht accepteert en wanneer de wederverkoper de licenties aan je account koppelt, doorgaans 24-48 uur.

Licentie bevestigen in Smart-account

navigeren naar uw pagina Smart Licentie-account en vervolgens klikt u op **de licentiepagina voor slimme software > inventaris > Licenties**.

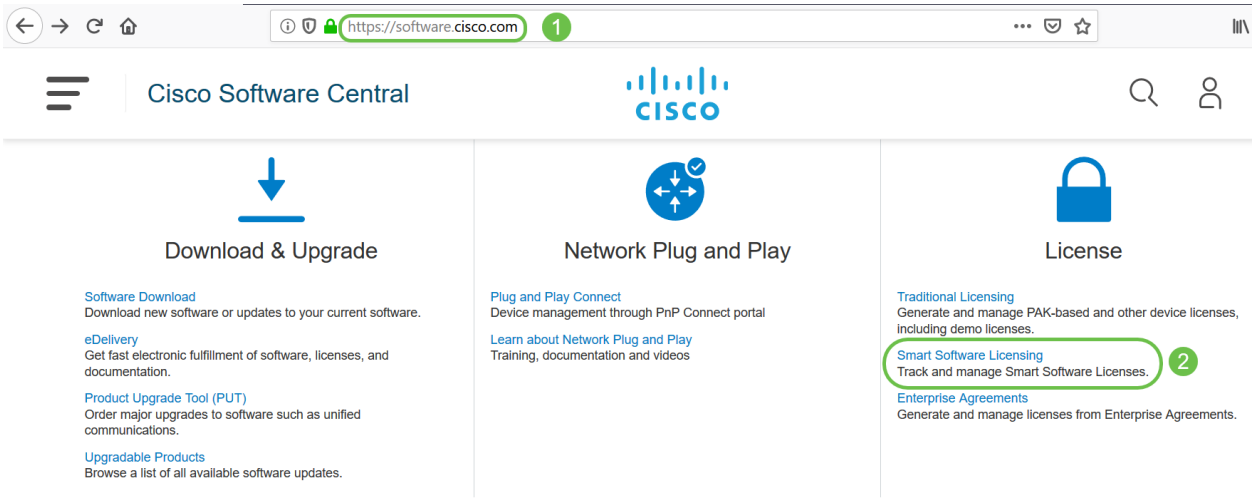


Als u uw licentie niet in uw Smart-account ziet, neemt u contact op met uw Cisco-partner.

Configuratie van de RV Security Licentie op de RV345P Series router

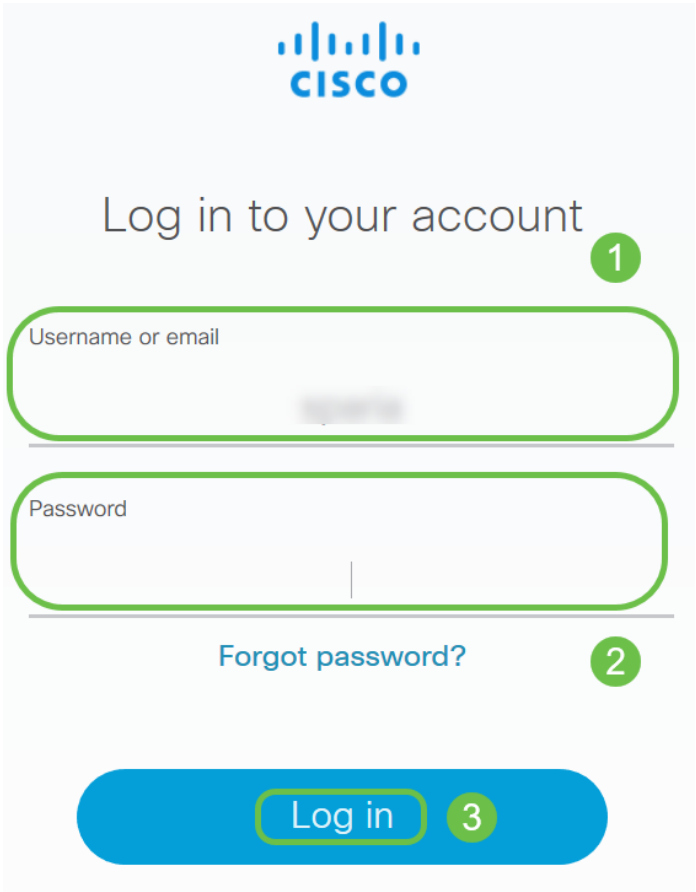
Stap 1

Toegang tot Cisco-software en navigeer naar **Smart Software Licensing**.



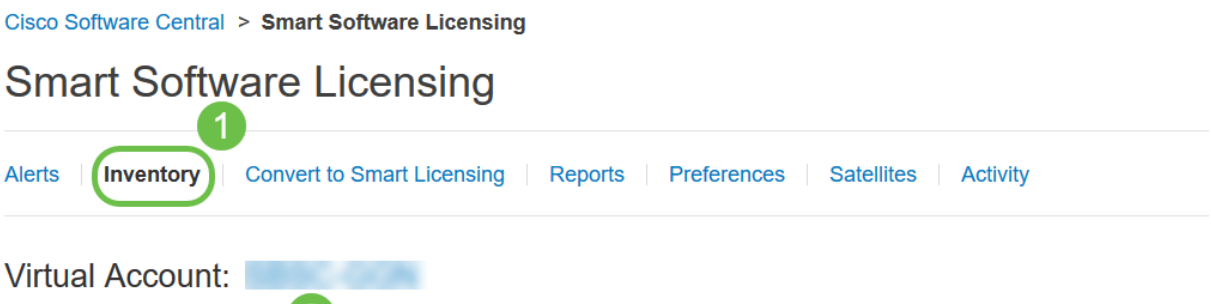
Stap 2

Voer uw *gebruikersnaam of e-mail* en *wachtwoord in* om in uw slimme account te loggen. Klik op **Inloggen**.



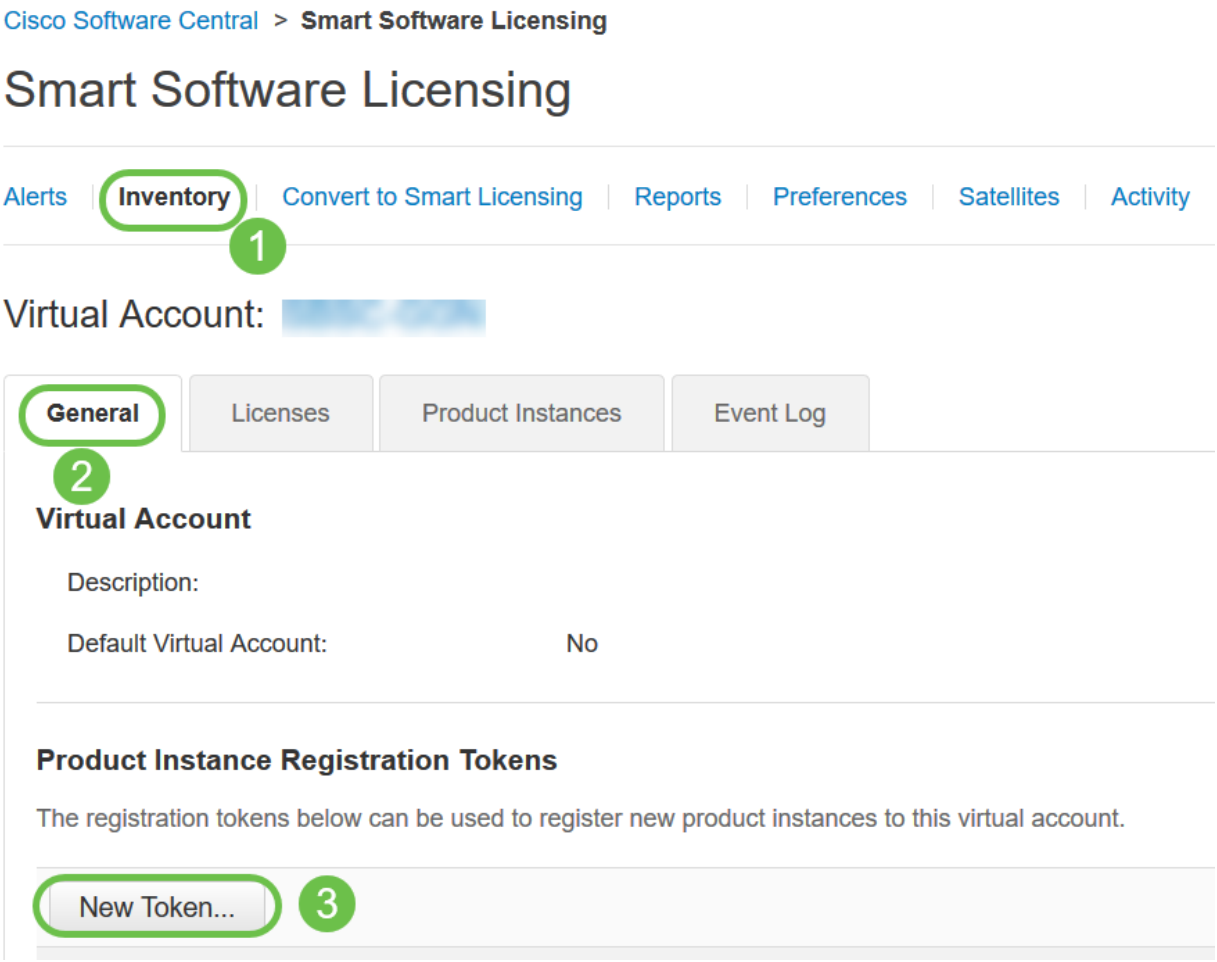
Stap 3

Navigeer naar **inventaris > Licenties** en controleer of de *RV-Series Licentie voor security services* op uw slimme account staat. Als u de licentie niet ziet, neemt u contact op met uw Cisco-partner.



Stap 4

Navigeer naar **inventaris > Algemeen**. Klik onder *Product Instance Registration Tokens* op **New Token**.



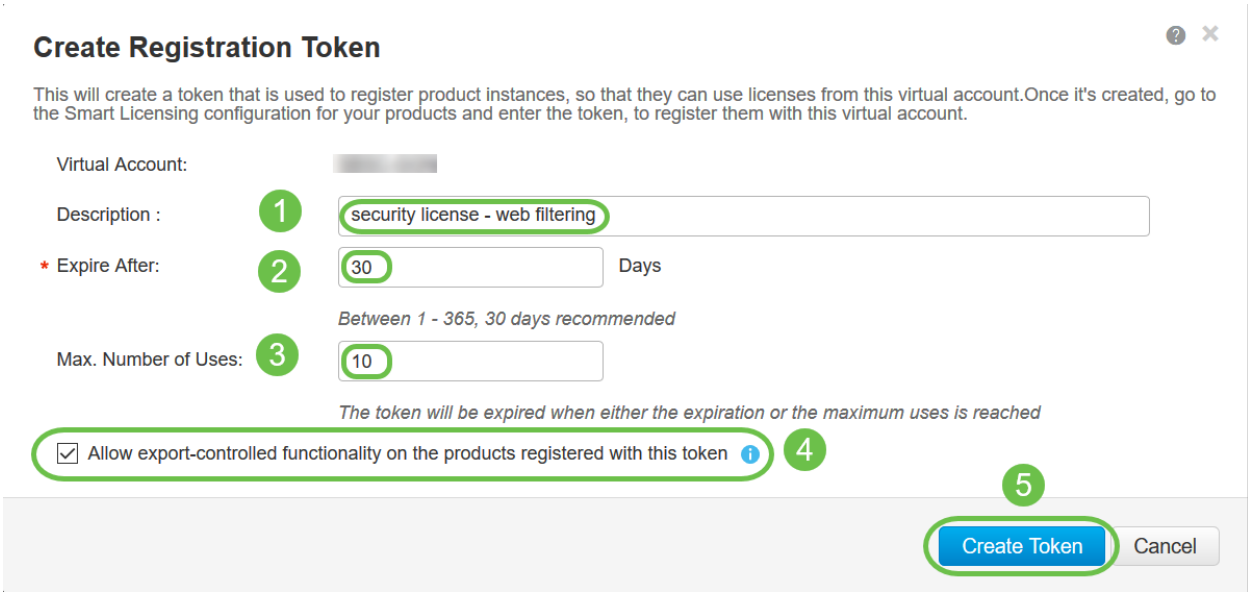
Stap 5

Er verschijnt een venster Registratie-token maken. Het gebied *Virtuele account* geeft de virtuele account weer waaronder het registrtoken wordt aangemaakt. Vul op de pagina *Registratie*-token *maken* het volgende in:

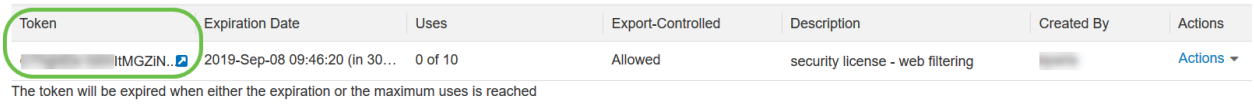
- Typ in het veld Description een unieke omschrijving van de token. In dit voorbeeld wordt de security licentie - webfiltering ingevoerd.
- Voer in het veld Verlopen na een waarde in van 1 tot 365 dagen. Cisco raadt de waarde 30 dagen voor dit veld aan. u kunt de waarde echter bewerken om aan uw behoeften te voldoen.
- In de Max. Het veld Aantal gebruiken voert een waarde in om het aantal keren te definiëren dat u dat token wilt gebruiken. Het token vervalt wanneer het aantal dagen of het maximale aantal toepassingen is bereikt.
- Controleer de door export gecontroleerde functionaliteit toestaan op de producten die bij dit symbolische selectieteken zijn geregistreerd om de door export gecontroleerde functionaliteit mogelijk te maken voor penningen van een product in uw virtuele account. Schakel het selectieteken uit als u niet wilt dat de door export gecontroleerde functionaliteit beschikbaar is voor gebruik met deze token. Gebruik deze optie alleen als

u voldoet aan de door export gecontroleerde functionaliteit. Sommige door export gecontroleerde kenmerken zijn beperkt door het Amerikaanse ministerie van Handel. Deze functies zijn beperkt voor producten die met dit token zijn geregistreerd wanneer u het selectieteken uit het keuzerondje wilt halen. Schendingen worden bestraft met straffen en administratieve heffingen.

- Klik op **Token maken** om het token op te halen.

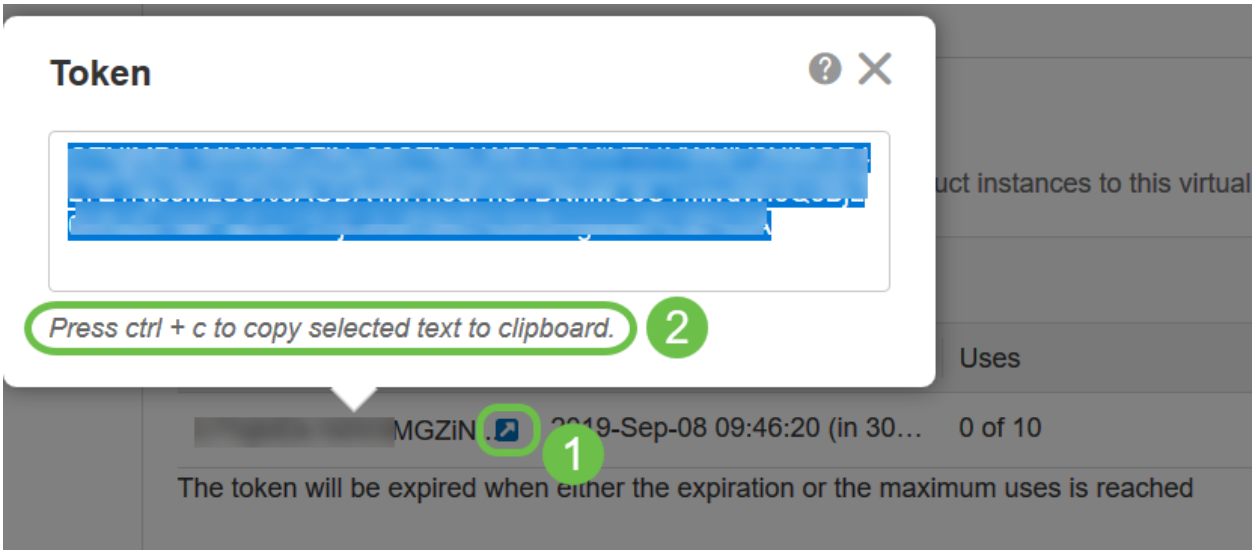


U hebt nu met succes een registratieteken voor producten gegenereerd.



Stap 6

Klik op het **pictogram pijl** in de *Token*-kolom om het token naar het klembord te kopiëren en druk op **Ctrl + c** op het toetsenbord.

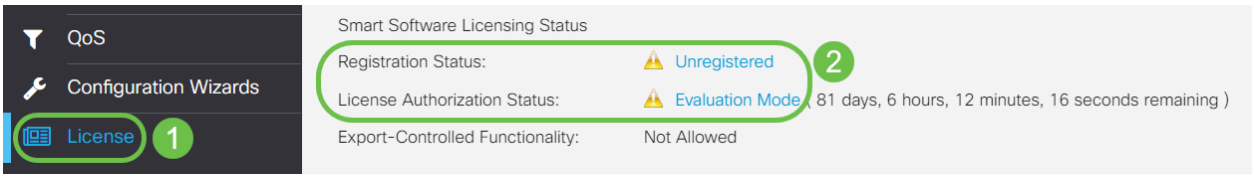


Stap 7 (optioneel)

Klik op het vervolgkeuzemenu **Handelingen**, kies **Kopieer** om het token naar het klembord te kopiëren of Downloaden... om een tekstbestand te downloaden van het token waarvan u kunt kopiëren.

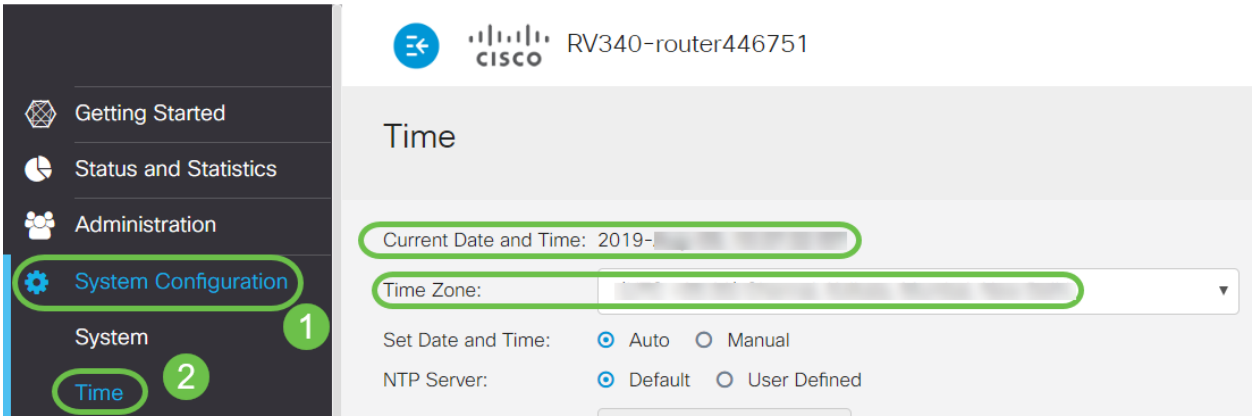
Stap 8

Navigeer in op **Licentie** en controleer of de *Registratiestatus* wordt weergegeven zoals *Niet-geregistreerd* en *de licentiestatus* van de *Licentie* weergegeven als *evaluatiemodus.*



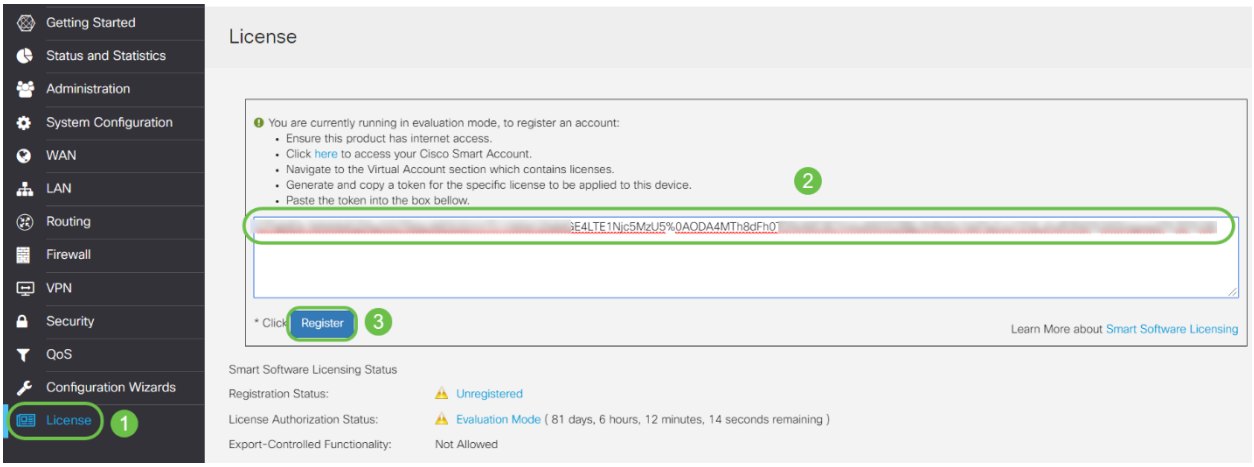
Stap 9

Blader naar **systeemconfiguratie > Tijd** en controleer of de *huidige datum en tijd* en *tijdzone* correct reflecteren zoals in uw tijdzone.



Stap 10

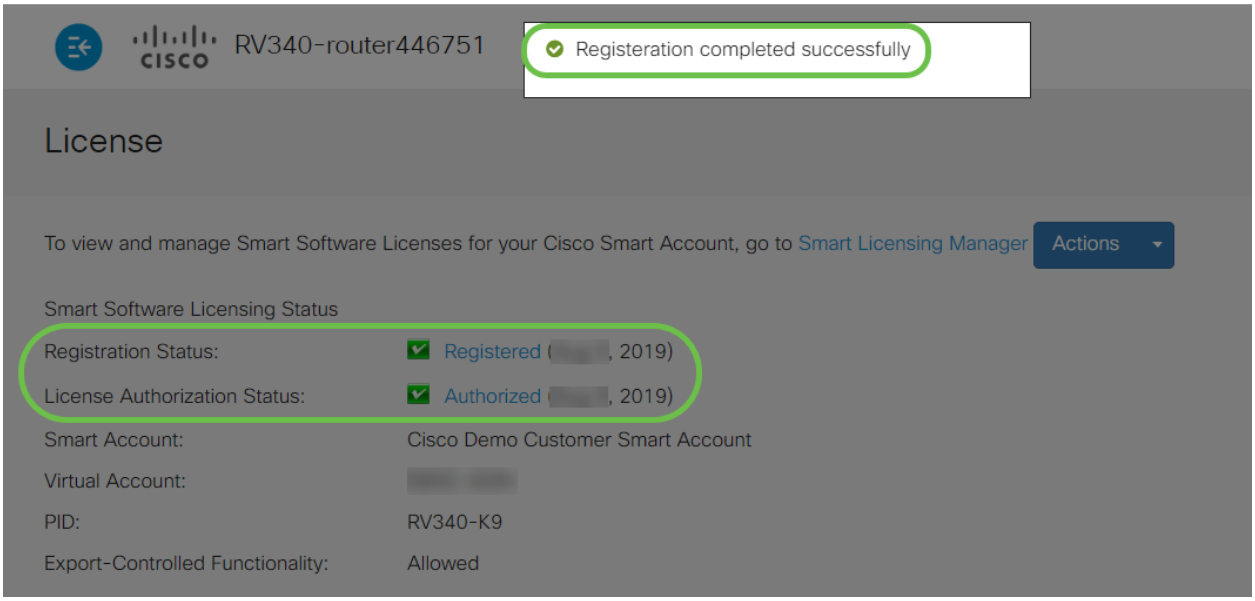
Blader naar **Licentie**. Plakt het gekopieerde token in stap 6 in het tekstvak onder het tabblad *Licentie* door **Ctrl + v** op uw toetsenbord te selecteren. Klik op **Registreren**.



De registratie kan een paar minuten duren. Laat de pagina niet staan als de router probeert contact op te nemen met de licentieserver.

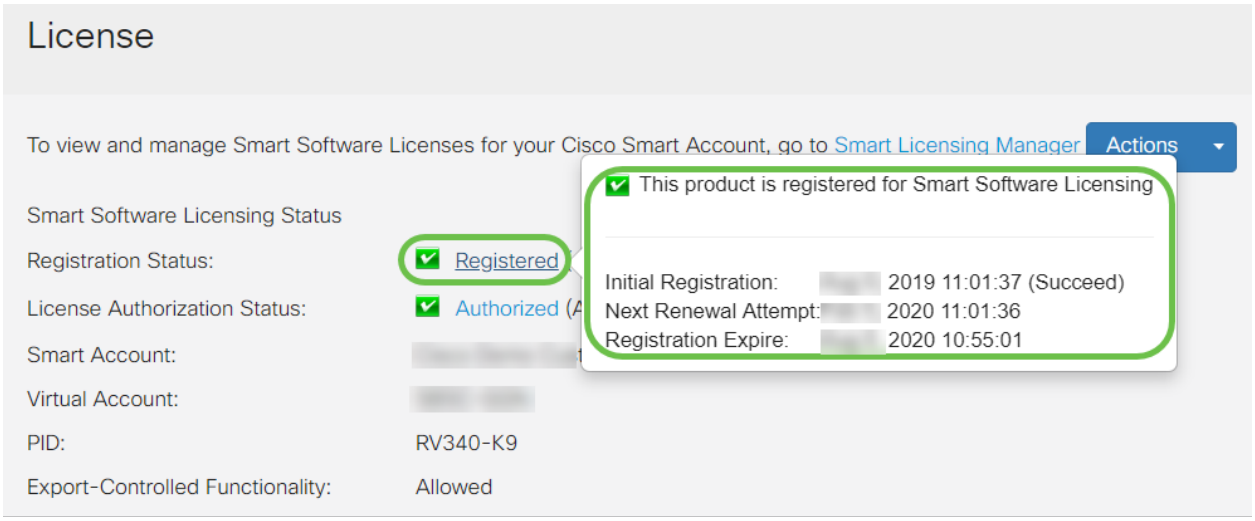
Stap 11

U hebt uw RV345P Series router nu geregistreerd en geautoriseerd met een Smart Licentie. U krijgt een melding op het scherm *Registratie voltooid*. Tevens kunt u zien dat de *Registratiestatus* van de *Registratiestatus* wordt weergegeven als *geregistreerd* en dat de *licentiestatus* van de *Licentie* wordt weergegeven *als geautoriseerd*.



Stap 12 (optioneel)

Als u meer informatie wilt over de *Registratiestatus* van de licentie, beweegt u de muisaanwijzer boven de *geregistreerde* status. Er verschijnt een dialoogvenster met de volgende informatie:

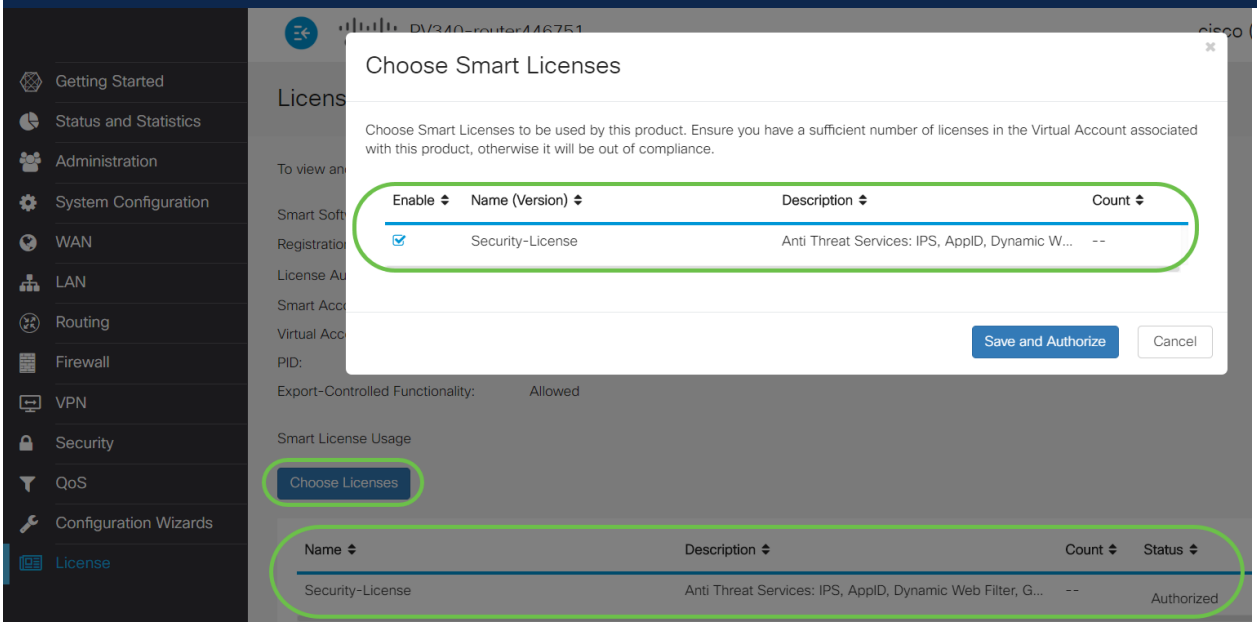


- Initiële registratie — Dit gebied geeft de datum en het tijdstip aan waarop de licentie is geregistreerd.
- Next Renewal Promint - Dit gebied geeft de datum en het tijdstip aan dat de router zal proberen de licentie te verlengen.
- Registratie verlopen — Dit gebied geeft de datum en het tijdstip aan waarop de registratie verloopt.

Stap 13

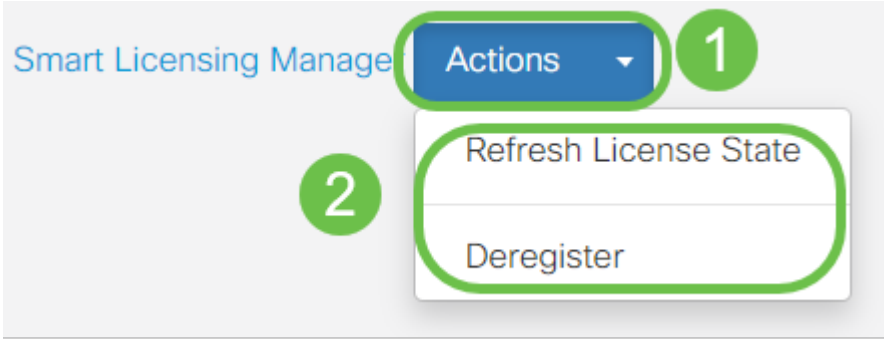
Controleer op de pagina *Licentie of* de *Security-Licentiestatus* wordt weergegeven *op* de *Authorized*. U kunt ook op de knop **Licentie kiezen** klikken om te controleren of de *Security-Licentie* is ingeschakeld.

Als u problemen bij deze stap hebt, moet u de router mogelijk opnieuw opstarten.



Stap 14 (optioneel)

Als u de *licentiestatus* wilt *verversen* of de *licentie* van de router wilt *registreren*, klikt u in het vervolgkeuzemenu *Smart Licensing Manager* en vervolgens selecteert u een actieitem.



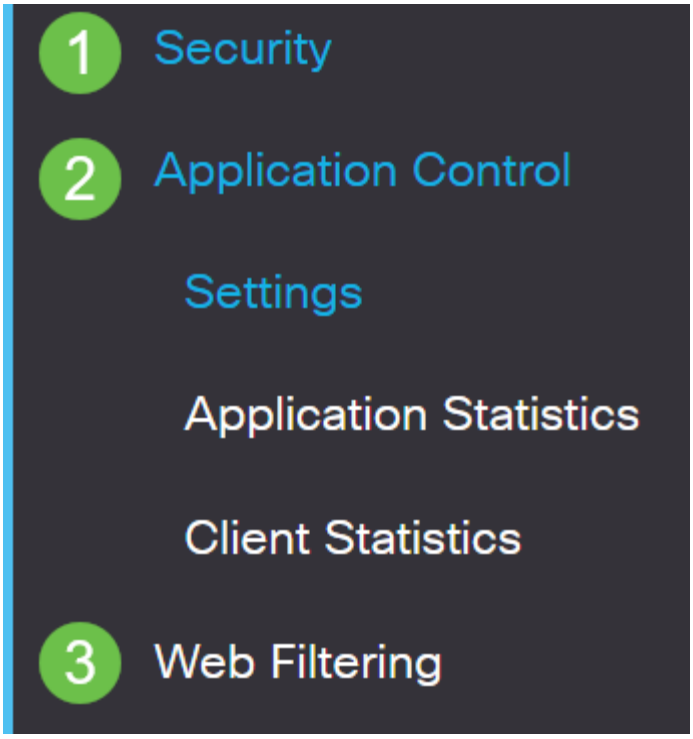
Nu u uw licentie op de router hebt, moet u de stappen in de volgende sectie voltooien.

Webfiltering op de RV345P router

U hebt 90 dagen na activering de tijd om gratis webfiltering te gebruiken. Als u deze functie wilt blijven gebruiken, moet u na het gratis proces een licentie aanschaffen. Klik om terug te gaan naar die sectie.

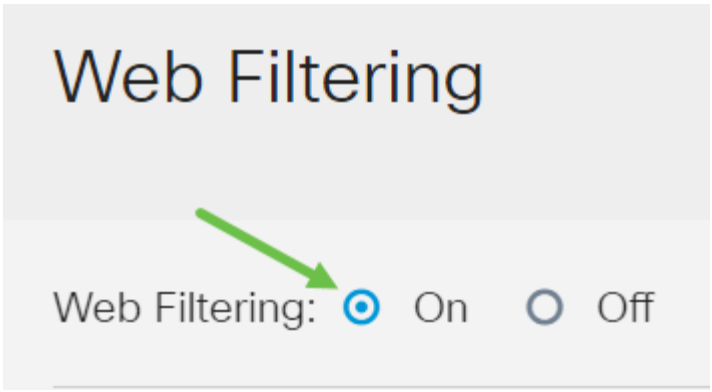
Stap 1

Meld u aan bij het webgebaseerde programma en kies **Security > Application Control > webfiltering**.



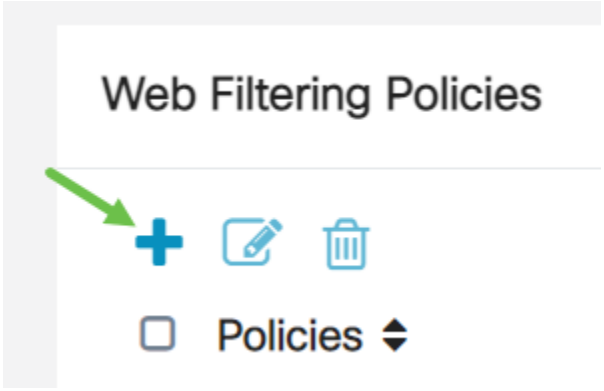
Stap 2

Selecteer de selectieknop **Aan**.



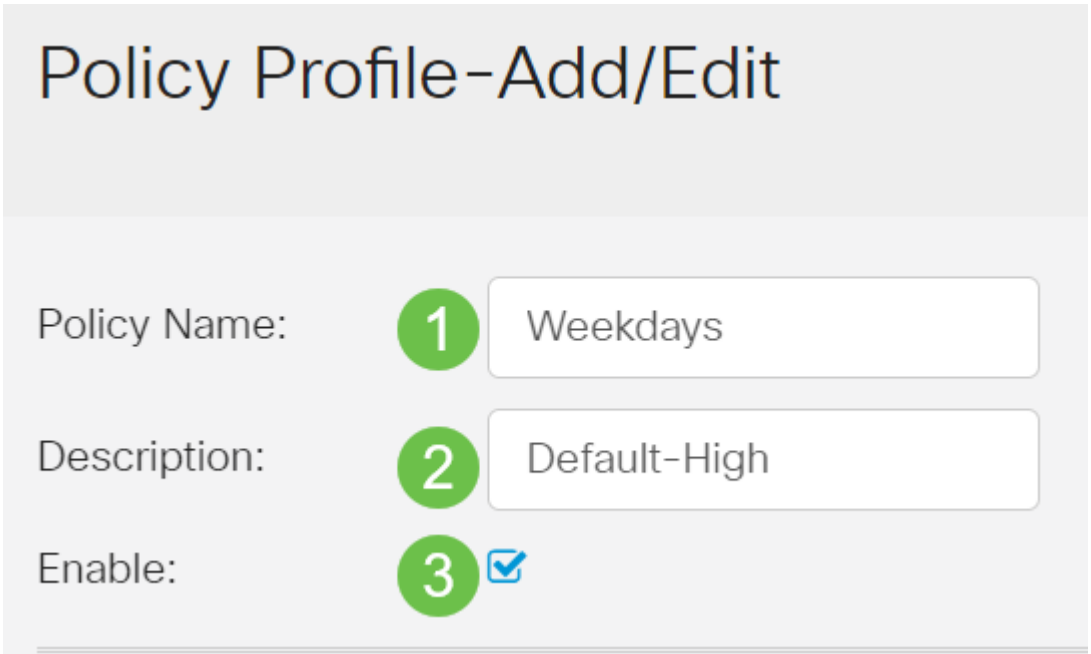
Stap 3

Klik op het **pictogram toevoegen**.



Stap 4

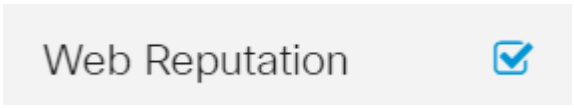
Typ een *beleidsnaam*, *Beschrijving* en het selectieteken *Inschakelen*.



Als Content Filtering op uw router is ingeschakeld, verschijnt een waarschuwing om u te laten weten dat Content Filtering is uitgeschakeld en dat de twee functies niet tegelijkertijd kunnen worden ingeschakeld. Klik op **Toepassen** om verder te gaan met de configuratie.

Stap 5

Controleer het selectieteken van het Web Reputation om het filteren toe te staan op basis van een web reputatie index.

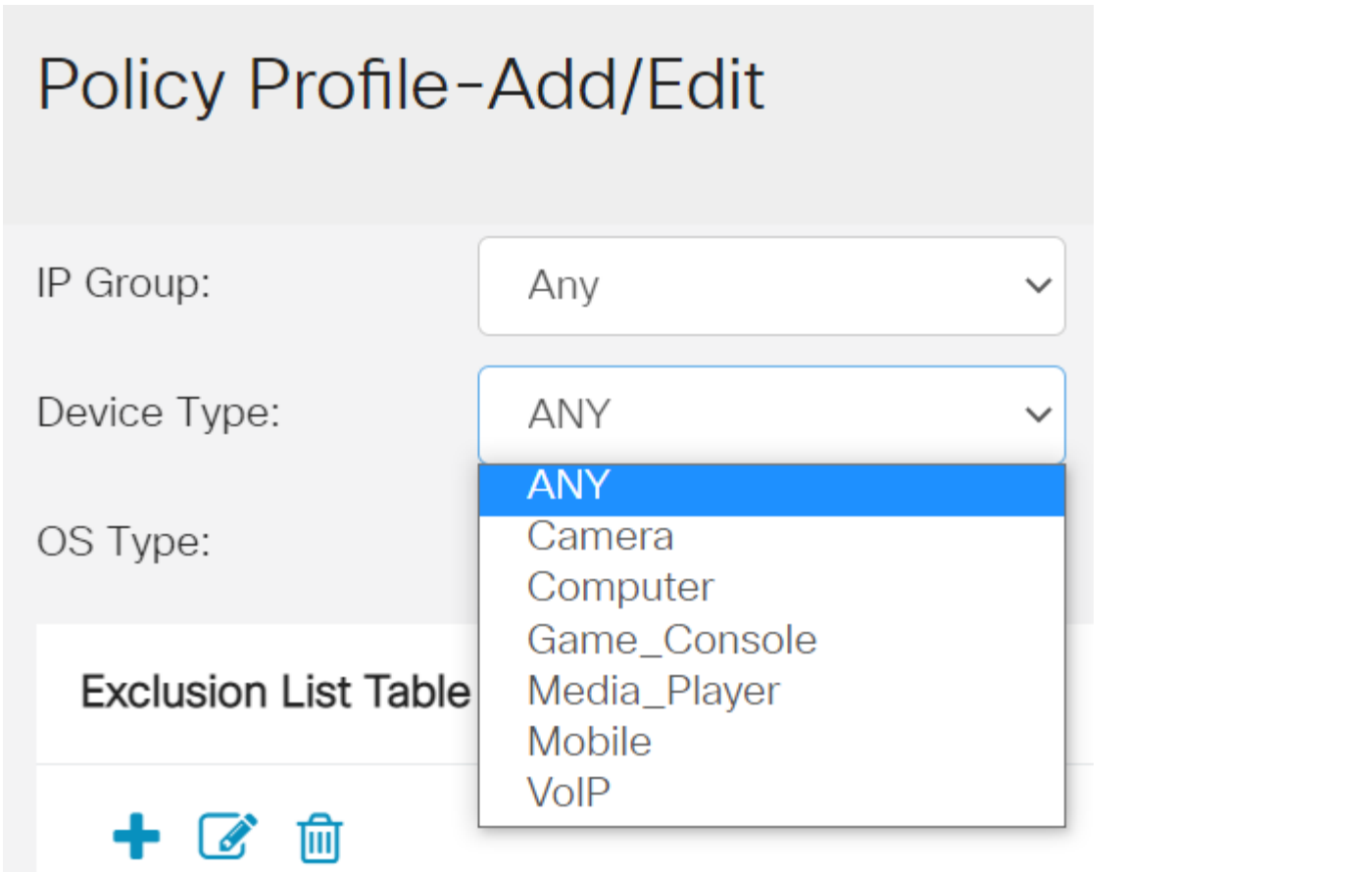


De inhoud wordt gefilterd volgens de bekendheid van een website of URL op basis van een webreputatie-index. Als de score onder de 40 ligt, wordt de website geblokkeerd. Om meer te lezen over de web reputatie technologie, klik hier voor meer informatie.

Stap 6

Selecteer in de vervolgkeuzelijst *Type apparaat* de bron/bestemming van de pakketten die moeten worden gefilterd. U kunt slechts één optie tegelijkertijd selecteren. De opties zijn:

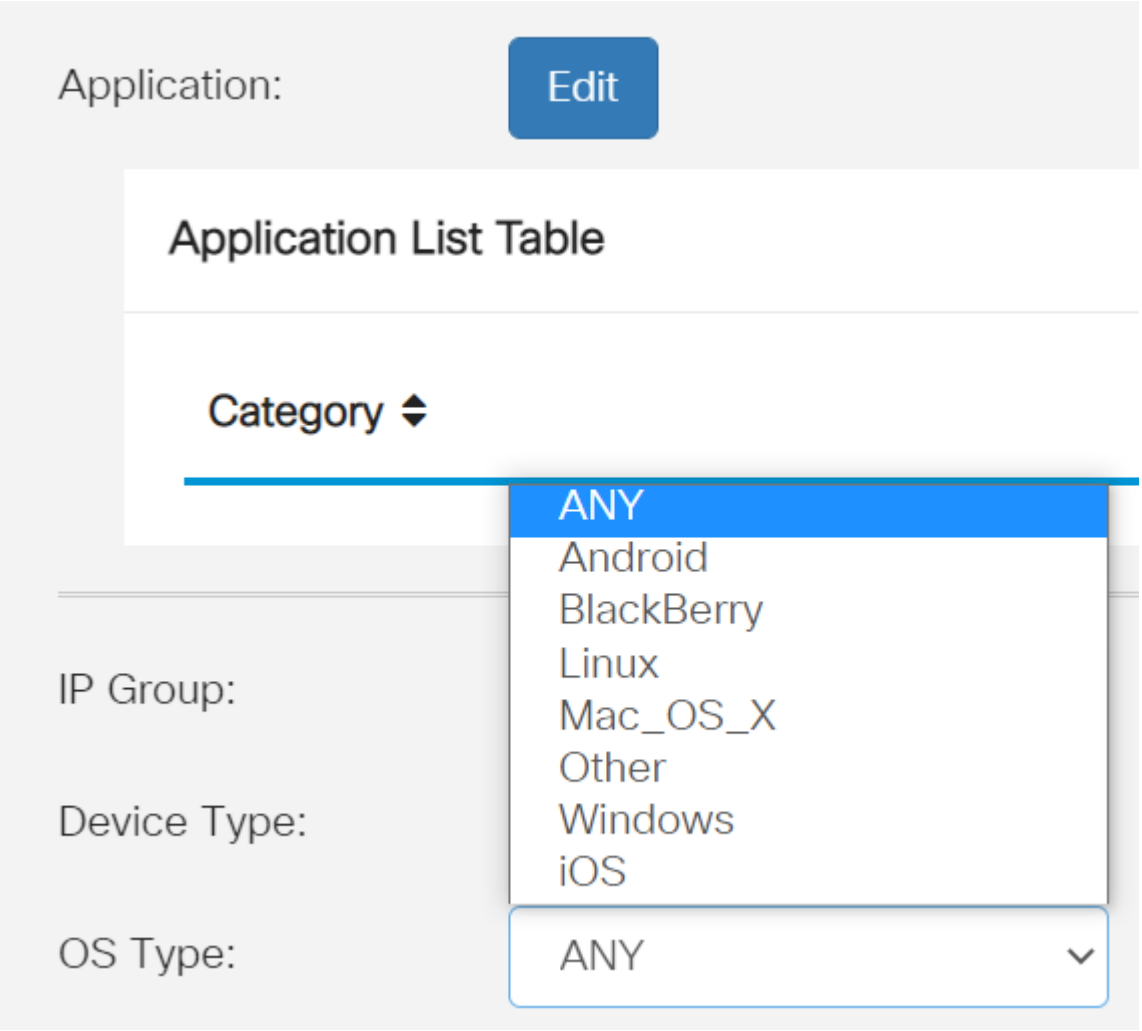
- ALLE — Kies dit om het beleid op elk apparaat toe te passen.
- Camera — Kies dit om het beleid op camera's toe te passen (zoals IP veiligheidscamera's).
- Computer — Kies dit om het beleid op computers toe te passen.
- Game_Console — Kies dit om het beleid toe te passen op Gaming Consoles.
- Media_Player — Kies dit om het beleid op mediaspelers toe te passen.
- Mobiel — Kies dit om het beleid toe te passen op mobiele apparaten.
- VoIP — Kies dit om het beleid toe te passen op Voice over Internet Protocol apparaten.



Stap 7

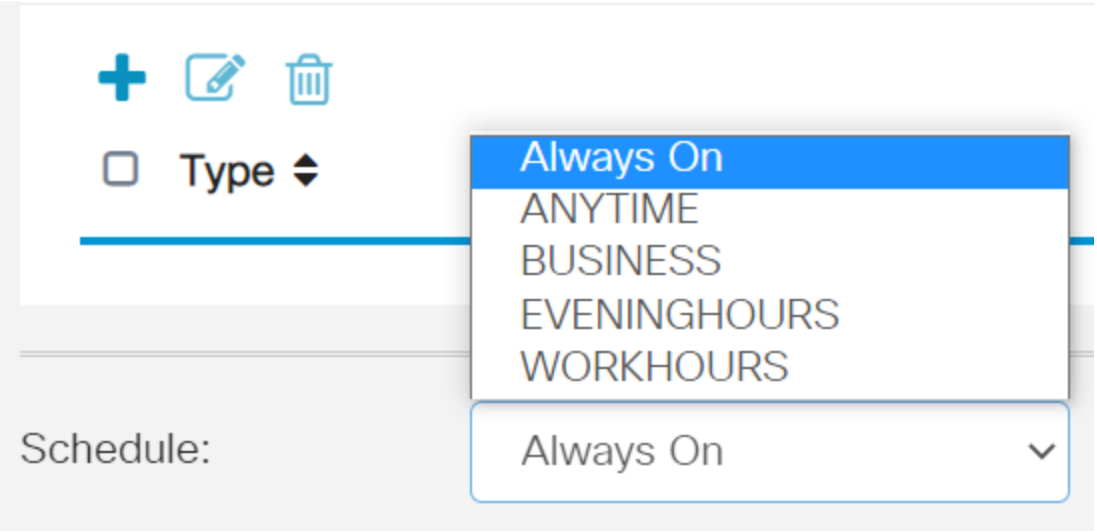
Kies in de vervolgkeuzelijst *OS-type* een besturingssysteem waarop het beleid van toepassing moet zijn. U kunt slechts één optie tegelijkertijd selecteren. De opties zijn:

- ALLE — past het beleid toe op elk type besturingssysteem. Dit is de standaard.
- Android — past het beleid alleen op Android OS toe.
- BlackBerry — past het beleid alleen toe op Blackberry OS.
- Linux — is alleen van toepassing op Linux OS.
- Mac_OS_X — Past het beleid alleen op Mac OS toe.
- Overige — past het beleid toe op een niet in de lijst opgenomen besturingssysteem.
- Windows — past het beleid op Windows OS toe.
- iOS — Past het beleid alleen op iOS toe.



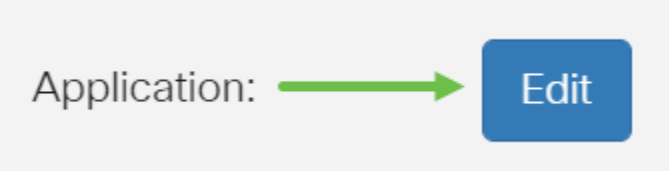
Stap 8

Scrolt naar het gedeelte *Schedule* en selecteer de optie die het best op uw behoeften aansluit.



Stap 9

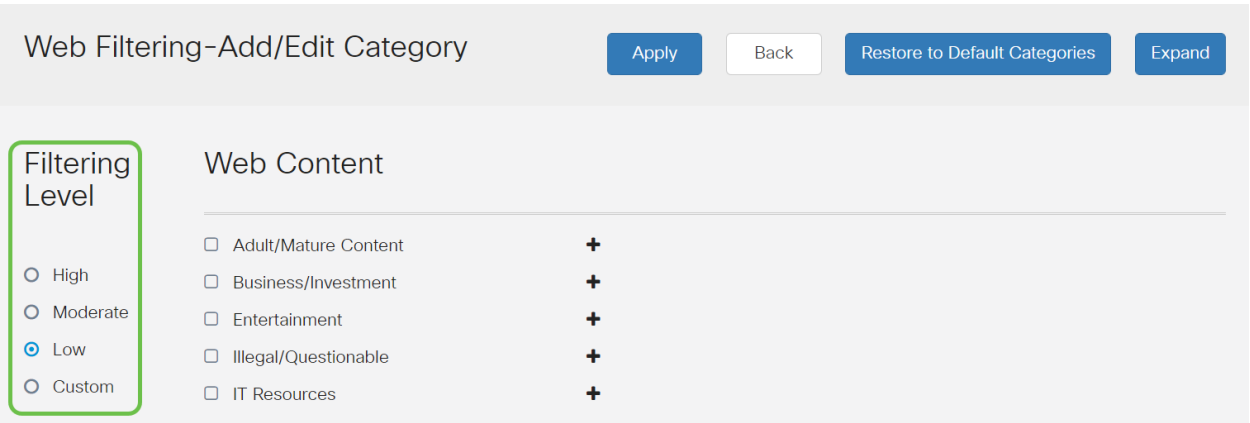
Klik op het **pictogram Bewerken**.



Stap 10

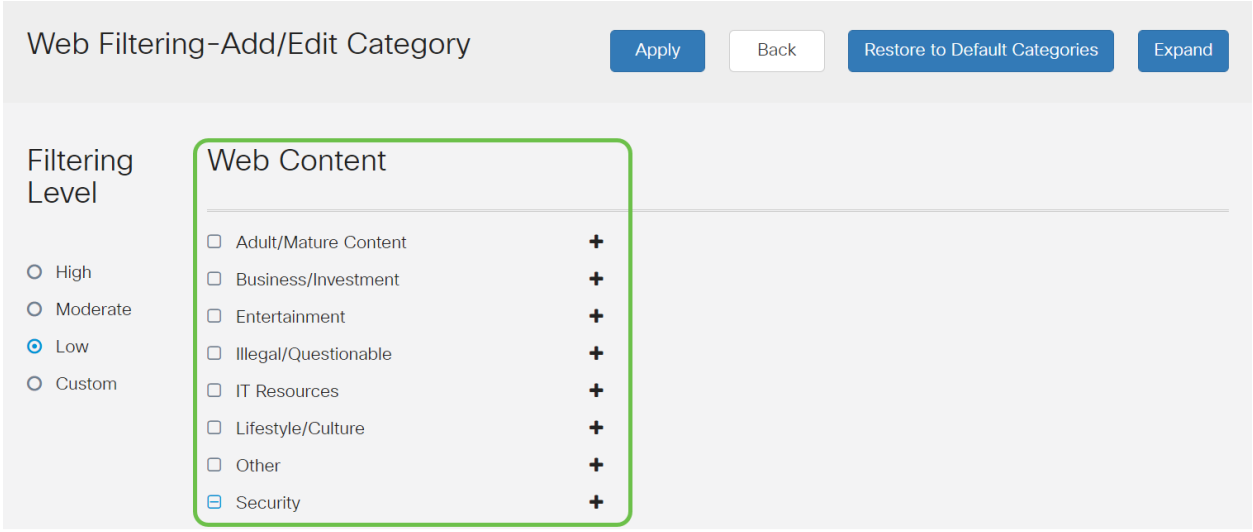
In de kolom Filtering Level klikt u op een radioknop om de filtermate snel te definiëren die het best op het netwerkbeleid past. De opties zijn Hoog, Matig, Laag en Aangepast. Klik op een van de onderstaande filterniveaus om de specifieke vooraf gedefinieerde subcategorieën te kennen die zijn gefilterd naar elk van de toegestane webcontentcategorie. Vooraf gedefinieerde filters kunnen niet verder worden gewijzigd en worden grijswaarden weergegeven.

- Laag — Dit is de standaardoptie. Beveiliging is ingeschakeld met deze optie.
- Matig — Content bij volwassen/mannelijke dieren, illegaal/twijfelachtig, en Beveiliging zijn ingeschakeld met deze optie.
- High — Adult/Mature Content, Business/Investment, Illegaal/Questionable, IT Resources en Security worden met deze optie ingeschakeld.
- Aangepast - de standaardinstellingen worden niet ingesteld om door de gebruiker gedefinieerde filters toe te staan.



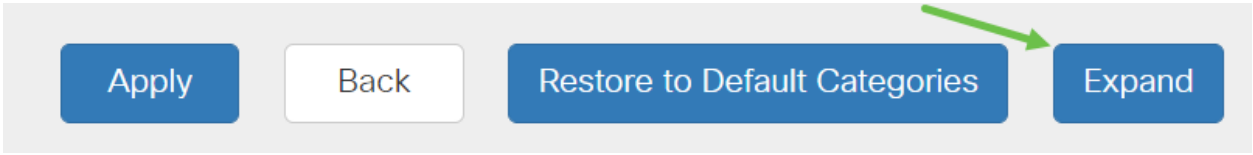
Stap 11

Voer de webinhoud in die u wilt filteren. Klik op het **pictogram plus** als u meer details wilt over één sectie.



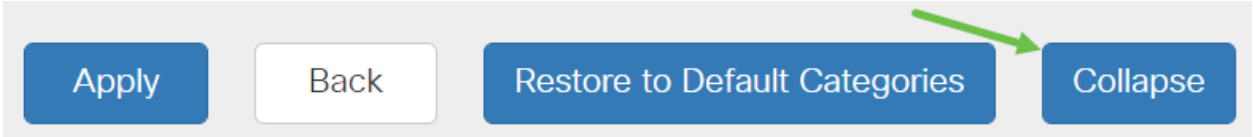
Stap 12 (optioneel)

U kunt alle subcategorieën en beschrijvingen van webcontent bekijken door op de knop **Uitvouwen** te klikken.



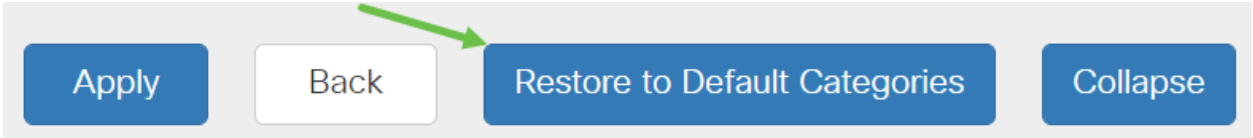
Stap 13 (optioneel)

Klik op **Invouwen** om de subcategorieën en beschrijvingen in elkaar te zetten.



Stap 14 (optioneel)

Als u wilt terugkeren naar de standaardcategorieën, klikt u op **Standaardcategorieën herstellen**.



Stap 15

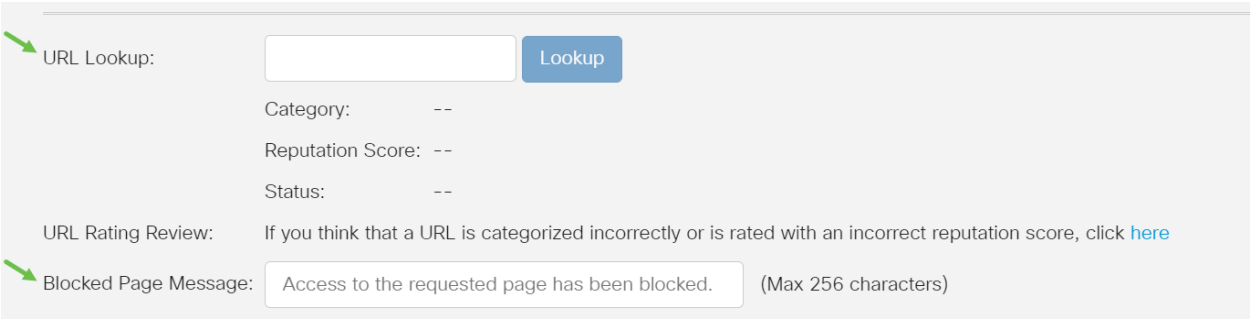
Klik op **Toepassen** om de configuratie op te slaan en naar de pagina Filter terug te keren om de instelling voort te zetten.

In de tabel op de toepassingslijst worden de overeenkomstige subcategorieën op basis van

het gekozen filterniveau ingevuld.

Stap 16 (optioneel)

Andere opties omvatten URL Lookup en het bericht dat toont wanneer een gevraagde pagina is geblokkeerd.



Stap 17 (optioneel)

Klik op Apply (Toepassen).

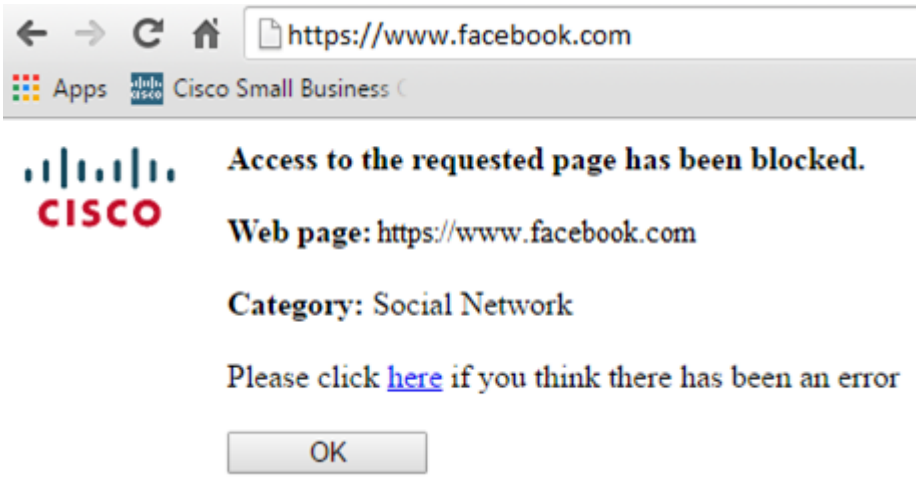
Stap 18

Ga naar de pagina *Configuration* kopiëren*/opslaan* om de configuratie permanent op te slaan of klik op het **pictogram** op het bovenste gedeelte van de pagina.

Stap 19 (optioneel)

Om te verifiëren dat een website of URL is gefilterd of geblokkeerd, lanceert u een webbrowser of opent u een nieuw tabblad in uw browser. Voer de domeinnaam in die u hebt geblokkeerd of gefilterd om geblokkeerd of ontkend te worden.

In dit voorbeeld gebruikten we www.facebook.com.



U had nu met succes een webfiltering op uw RV345P router moeten hebben ingesteld. Aangezien u de RV Security Licentie voor webfiltering gebruikt, hebt u Umbrella waarschijnlijk niet nodig. Als je ook Umbrella wilt, klik dan hier. Als u voldoende beveiliging hebt, klikt u op om naar de volgende sectie te overslaan.

Probleemoplossing

Als u een licentie hebt aangeschaft maar deze niet op uw virtuele account voorkomt, hebt u twee opties:

1. Volg het bericht op met de wederverkoper om te vragen dat hij de overdracht uitvoert.
2. Neem contact met ons op en we nemen contact op met de wederverkoper.

Idealiter zou je ook niet hoeven te doen, maar als je op dit kruispunt aankomt zijn we blij dat je helpt! Om het proces zo snel mogelijk te maken, hebt u de geloofsbrieven in de tabel hierboven nodig evenals de hieronder geschetste.

Vereiste informatie	De informatie lokaliseren
Licentievorm	U dient dit e-mailadres in te schakelen nadat u de licenties hebt aangeschaft.
Cisco-verkooporder nummer	Misschien moet je terug naar de wederverkoper om dit te krijgen.
Schermafbeelding van uw Smart Account-licentiepagina	Een screenshot maken van de inhoud van het scherm om met ons team te delen. Als u niet bekend bent met screenshots kunt u de onderstaande methoden gebruiken.

Screenshots

Als u een token hebt of als u een oplossing wilt vinden, wordt aanbevolen een screenshot te maken om de inhoud van het scherm op te nemen.

Gezien de verschillen in de procedure die vereist zijn om een screenshot op te nemen, zie hieronder voor koppelingen specifiek voor uw besturingssysteem.

- Windows

- MAC
- iPhone/iPad
- Android

Licentie voor Umbrella RV-tak (optioneel)

Umbrella is een eenvoudig, maar zeer effectief cloudbeveiligingsplatform van Cisco.

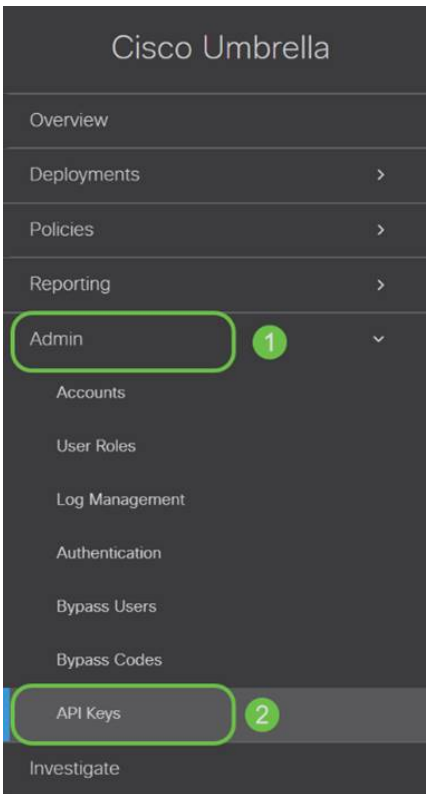
Umbrella is in de wolk actief en voert veel aan veiligheid gerelateerde diensten uit. Van opkomende dreiging tot onderzoek na de gebeurtenis. Umbrella ontdekt en voorkomt aanvallen in alle havens en protocollen.

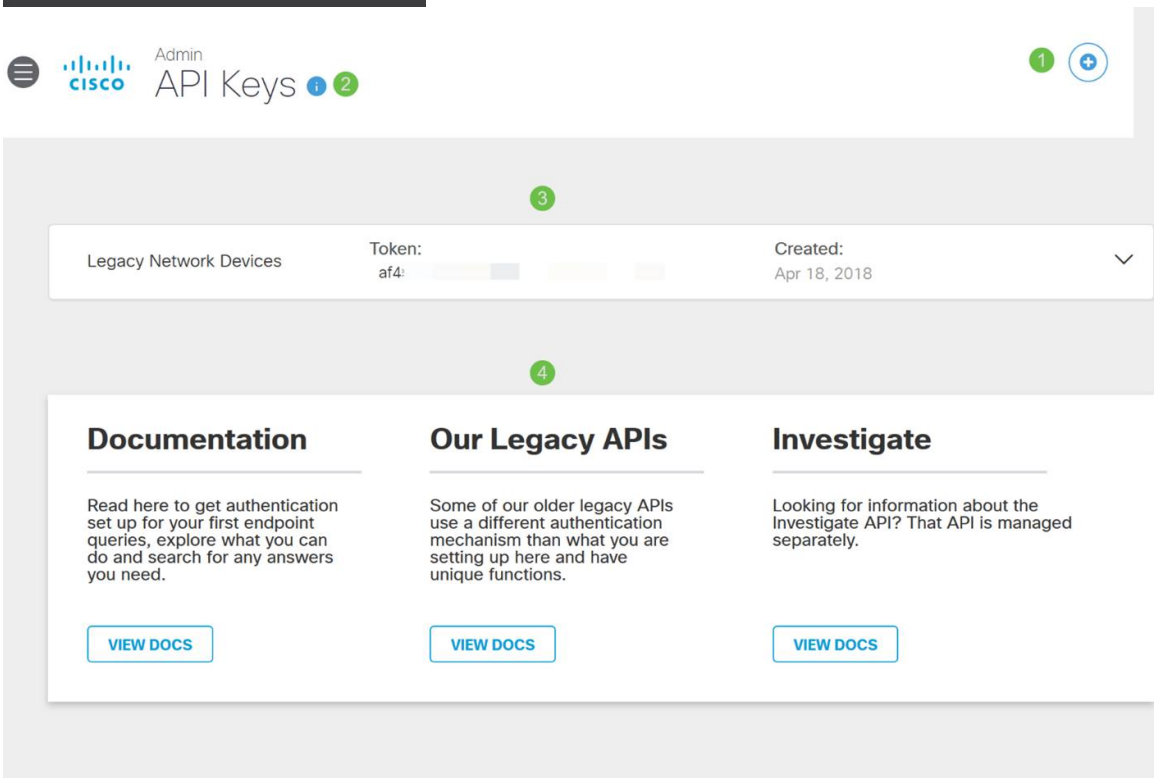
Umbrella gebruikt DNS als hoofdvector voor defensie. Wanneer gebruikers een URL in hun adresbalk invoeren en op *ENTER* klikken, neemt Umbrella deel aan de overdracht. Die URL gaat over naar de DNS-oplossing van Umbrella en als een veiligheidswaarschuwing aan het domein gekoppeld is, wordt het verzoek geblokkeerd. Deze telemetrie gegevensoverdracht en wordt geanalyseerd in microseconden, wat bijna geen latentie toevoegt. Telemetrie-gegevens gebruiken logbestanden en instrumenten om miljarden DNS-verzoeken overal ter wereld te volgen. Als deze gegevens alomtegenwoordig zijn, kan correlatie ermee over de hele wereld een snelle reactie op aanvallen mogelijk maken vanaf het moment dat ze beginnen. Zie het privacybeleid van Cisco hier voor meer informatie: het volledige beleid, samenvattende versie. Denk aan telemetrie data als data afgeleid van tools en logs.

Bezoek Cisco Umbrella om meer te leren en een account te maken. Als u problemen hebt, controleert u hier op documentatie en hier op de opties voor Umbrella Support.

Stap 1

Nadat u hebt gelogd in uw Umbrella-account, klikt u op in het *Dashboard* op **Admin > API-toetsen**.





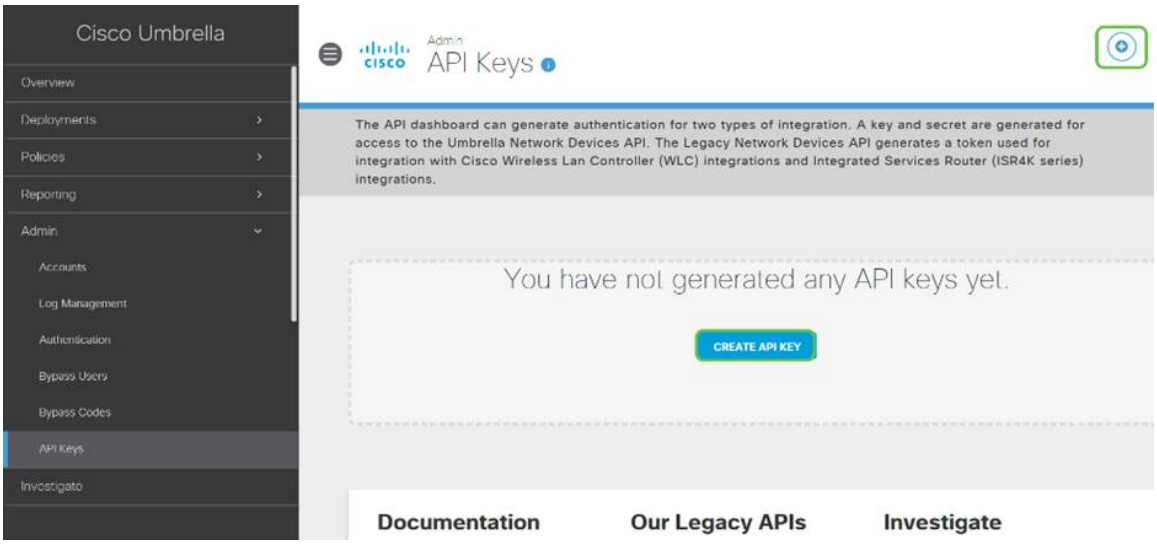
Anatomie van het API-toetsenbord (met een reeds bestaande API-toets)

1. Voeg API-toets toe - hiermee wordt de creatie van een nieuwe toets gestart voor gebruik met de Umbrella API.
2. Aanvullende informatie - Dielt neer/omhoog met een toelichting voor dit scherm.
3. Token Well - Bevat alle sleutels en penningen die door deze account zijn gemaakt. (Populaten zodra een sleutel is gecreëerd)
4. Ondersteunende documenten - links naar documentatie op de Umbrella-site over de

onderwerpen in elke sectie.

Stap 2

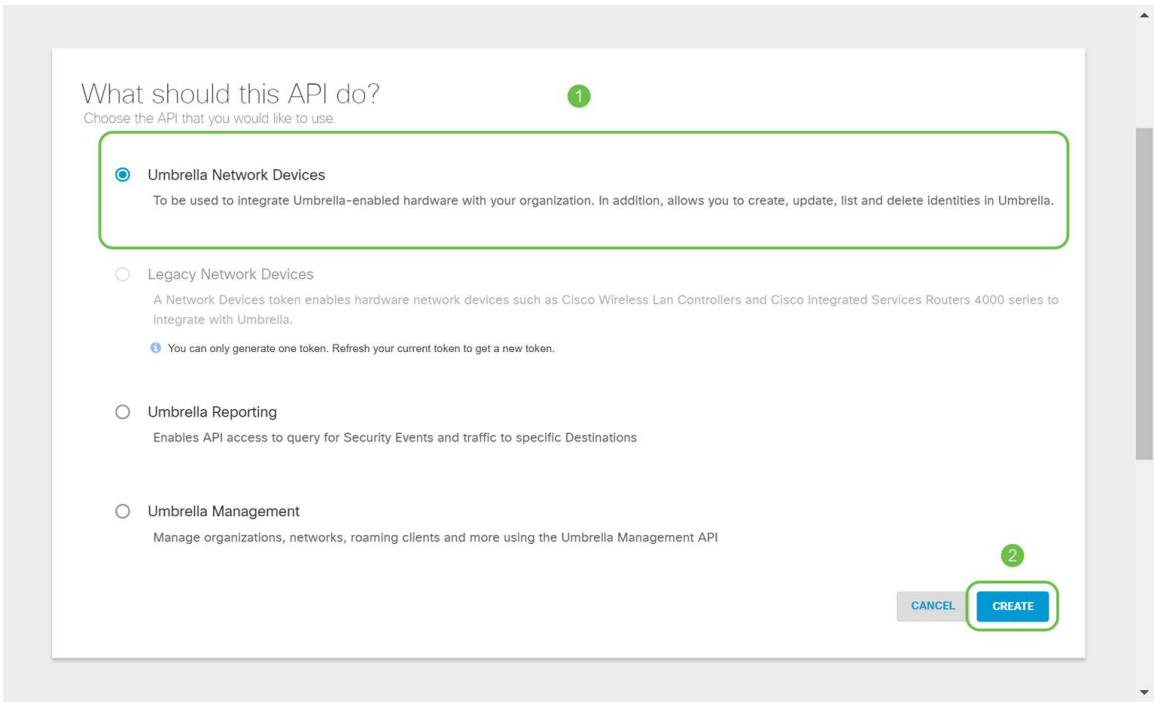
Klik op de knop **API-sleutel toevoegen** in de rechterbovenhoek of klik op de knop **API-toets maken**. Ze functioneren allebei hetzelfde.



De bovenstaande screenshot is vergelijkbaar met wat u ziet wanneer u dit menu voor het eerst opent.

Stap 3

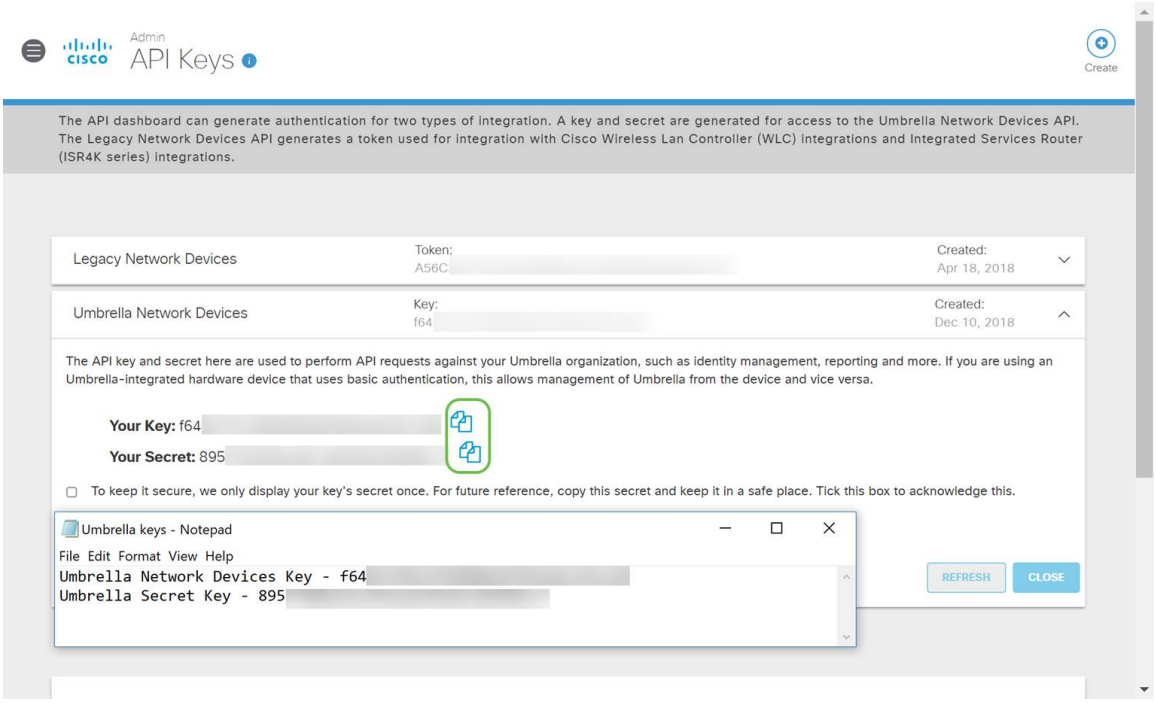
Selecteer **Umbrella Network Devices** en klik vervolgens op de knop **Maken**.



Stap 4

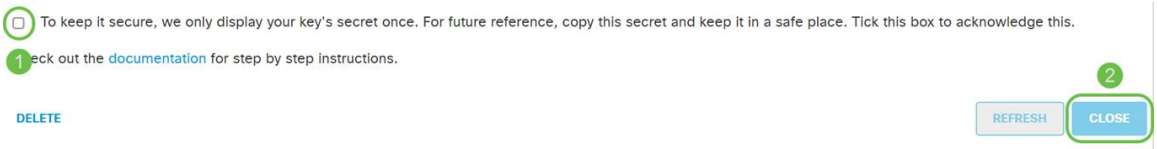
Open een teksteditor zoals een notebook en klik vervolgens op het **kopiëren-pictogram**

rechts van uw API en API-*beveiligingssleutel.* Een pop-up-melding bevestigt dat de toets naar uw klembord is gekopieerd. Plaats één voor één uw geheime en API-toets in het document en etiketteer ze voor toekomstig gebruik. In dit geval is het label "Umbrella network devices key". Sla het tekstbestand vervolgens op een beveiligde locatie waar u later makkelijk toegang toe kunt krijgen.



Stap 5

Nadat u de sleutel en de geheime sleutel naar een veilige plaats hebt gekopieerd, klik van het *scherm* van *Umbrella API* op het **selectieteken** om te bevestigen dat de tijdelijke weergave van de geheime sleutel is voltooid, en klik vervolgens op de knop **Close.**



Als u de geheime toets kwijtraakt of per ongeluk verwijdert, is er geen functie of ondersteuningsnummer om deze toets te bellen. Indien verloren, moet u de toets verwijderen en de nieuwe API-toets opnieuw autoriseren met elk apparaat dat u wilt beveiligen met Umbrella.

Umbrella configureren op uw RV345P

Nu we API-toetsen hebben gemaakt binnen Umbrella, kunt u deze toetsen gebruiken en op uw RV345P installeren.

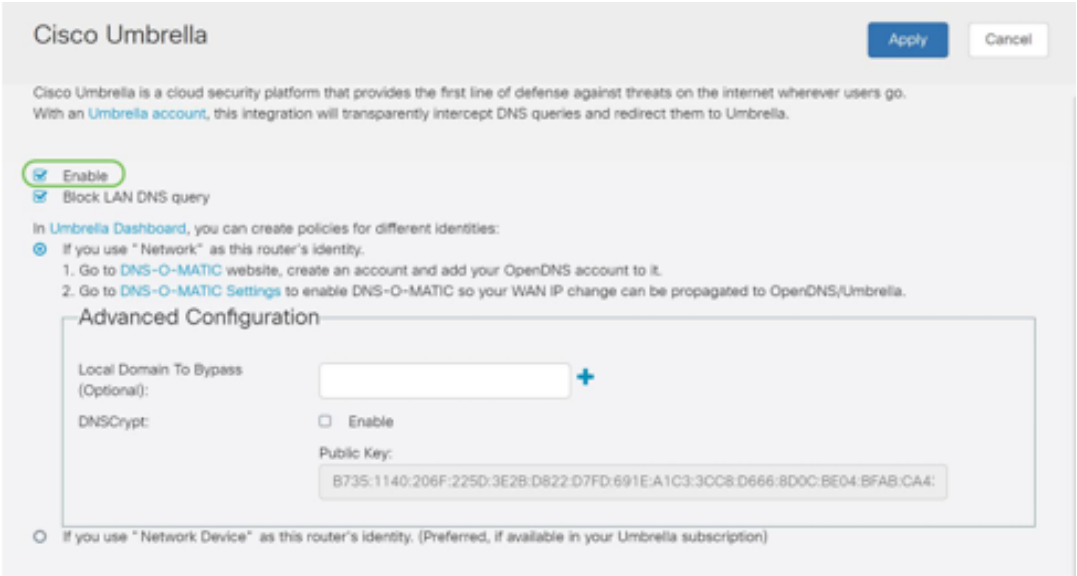
Stap 1

Nadat u in de RV345P-router hebt gelogd, klikt u op **Security >** Umbrella in het menu

Sidebar.

Stap 2

Het Umbrella API-scherm heeft een scala aan opties, begin Umbrella in te schakelen door op het selectieteken **Enable**.



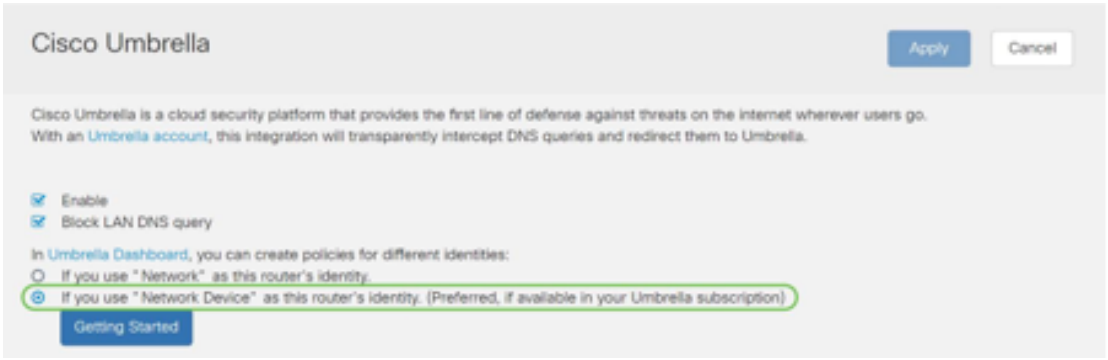
Stap 3 (optioneel)

Standaard wordt het vakje *LAN DNS-reeks blokkeren* geselecteerd. Deze duidelijke optie maakt automatisch toegangscontrolelijsten op uw router die DNS-verkeer niet naar het internet kunnen uitvoeren. Deze eigenschap dwingt alle

domeinvertaalverzoeken om door RV345P te worden gericht en is een goed idee voor de meeste gebruikers.

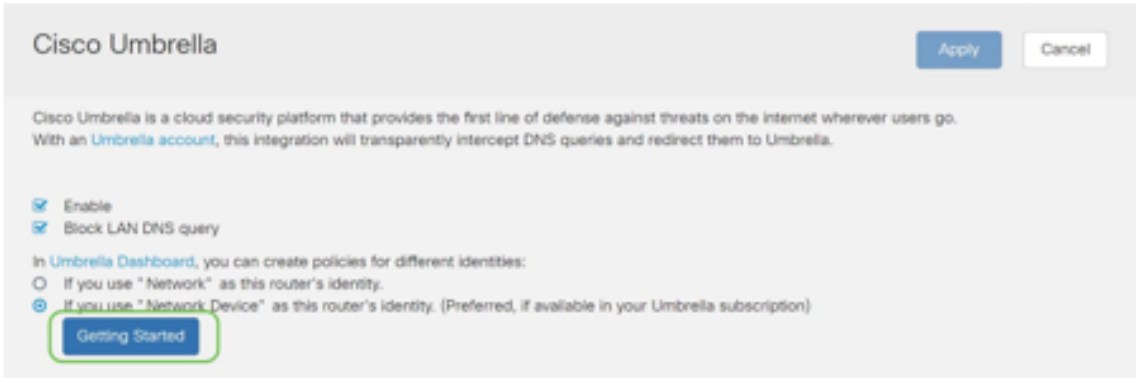
Stap 4

De volgende stap speelt zich op twee verschillende manieren af. Ze zijn allebei afhankelijk van de installatie van uw netwerk. Als u een service zoals DynDNS of NoIP gebruikt, laat u het standaard naamschema van "Netwerk" achter. U moet deze accounts registreren om Umbrella-interfaces met deze services te garanderen. We vertrouwen alleen op "Netwerkapparaat" en klik dus op de onderste radioknop.



Stap 5

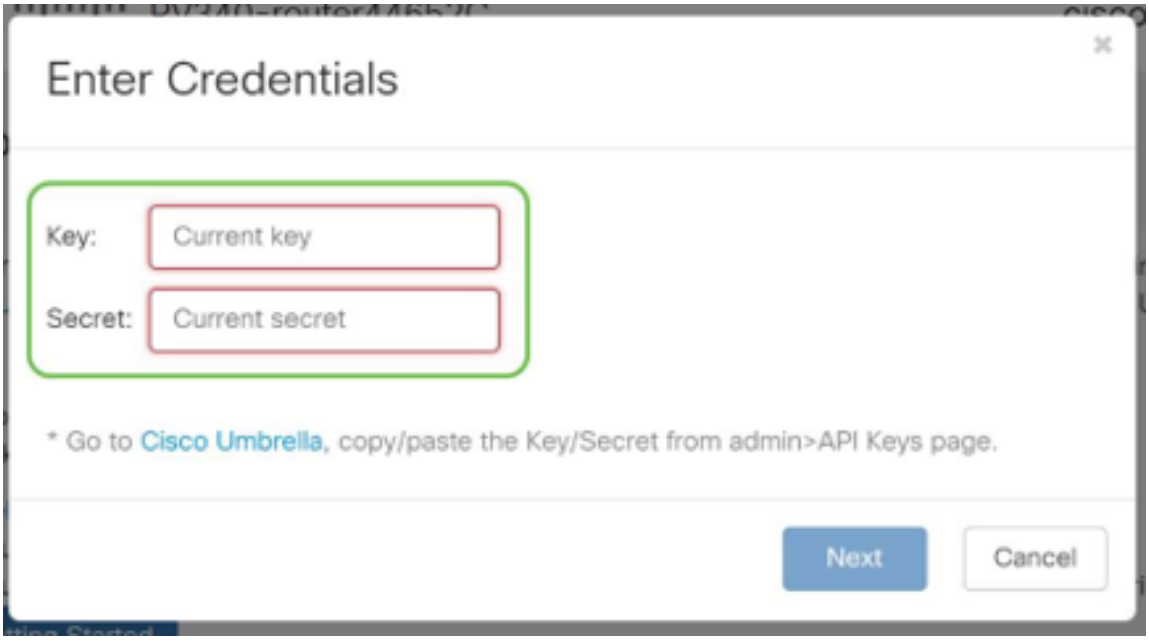
Klik op **Introductie**.



Stap 6

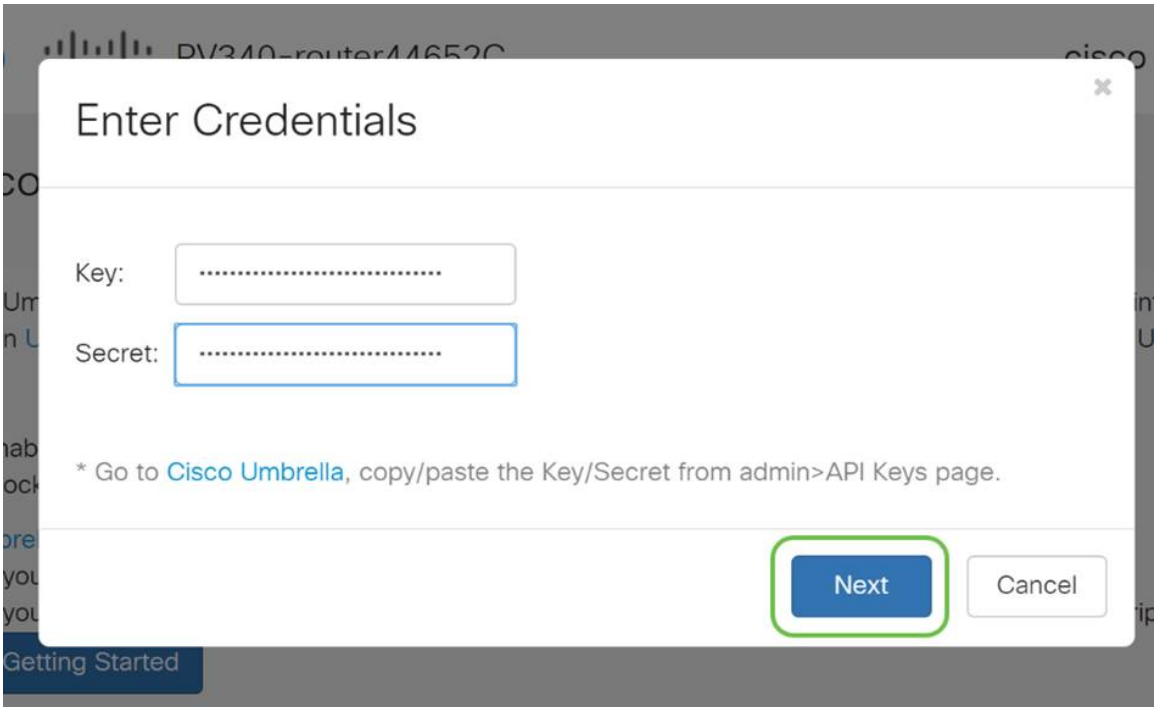
Voer de **API-toets** en de **geheime sleutel in** voor de tekstvakjes.

Twee keer uitbellen zodat je weet dat het belangrijk is! Als u de geheime toets kwijtraakt of per ongeluk verwijdert, is er geen functie of ondersteuningsnummer om deze toets te bellen. Houd deze geheim en veilig. Indien verloren, moet u de toets verwijderen en de nieuwe API-toets opnieuw autoriseren met elk apparaat dat u wilt beveiligen met Umbrella.



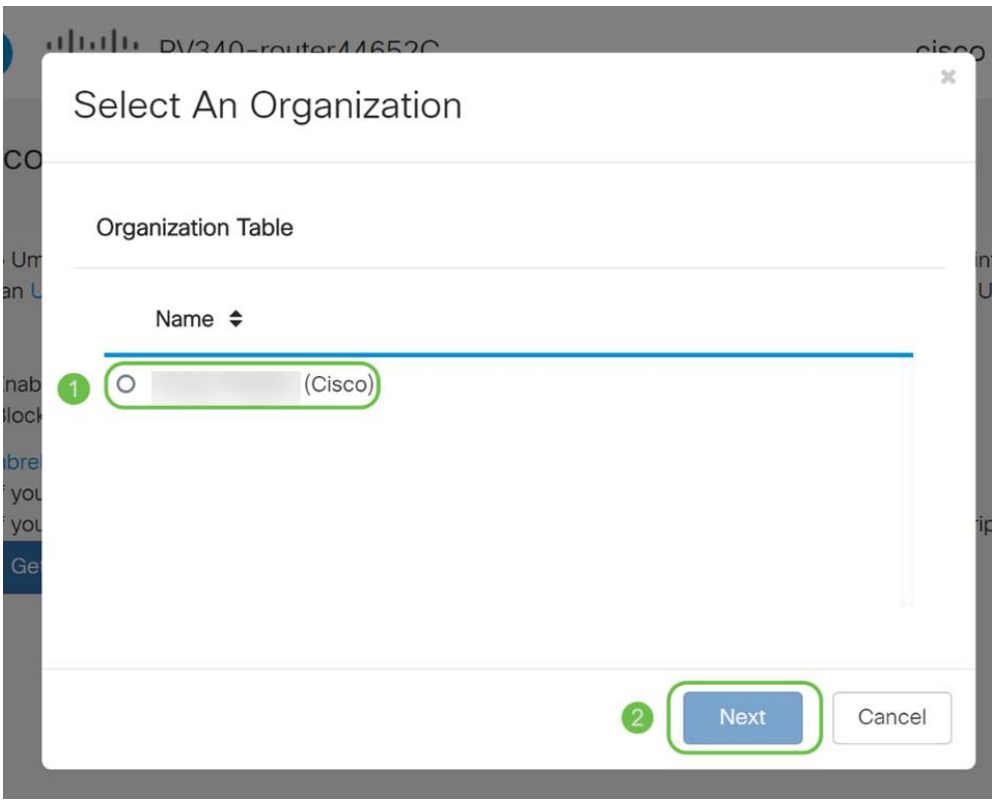
Stap 7

Klik na het invoeren van uw API- en geheime sleutel op de **volgende** knop.



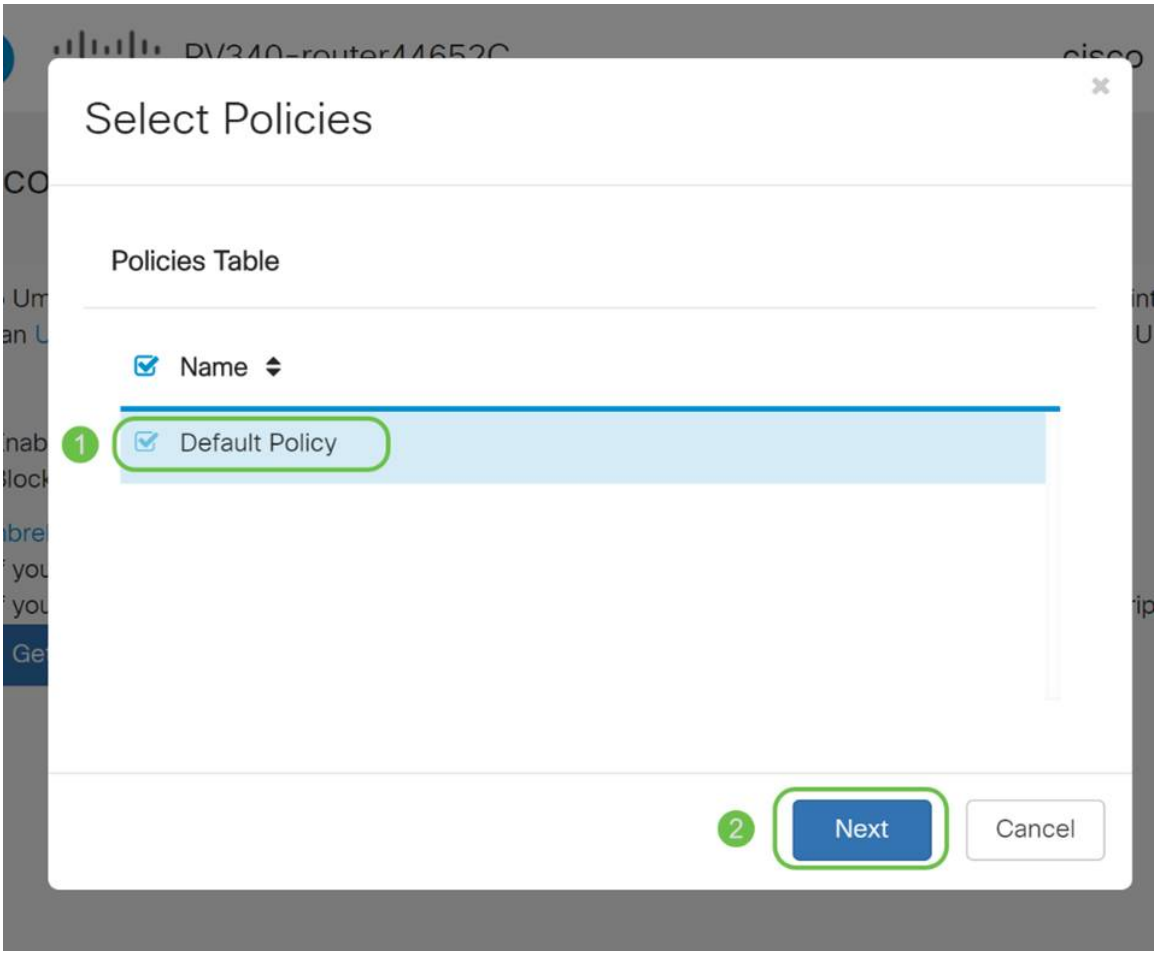
Stap 8

Selecteer in het volgende scherm de **organisatie** die u met de router wilt associëren. Klik op **Volgende**.



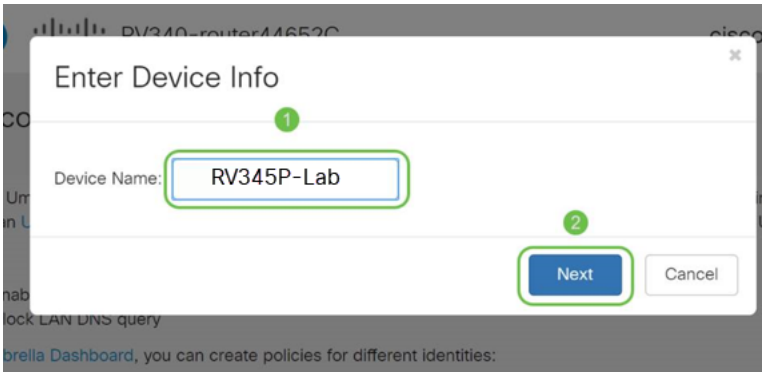
Stap 9

Selecteer het beleid dat moet worden toegepast op verkeer dat door de RV345P wordt routeerd. Voor de meeste gebruikers zal het standaardbeleid genoeg dekking bieden.



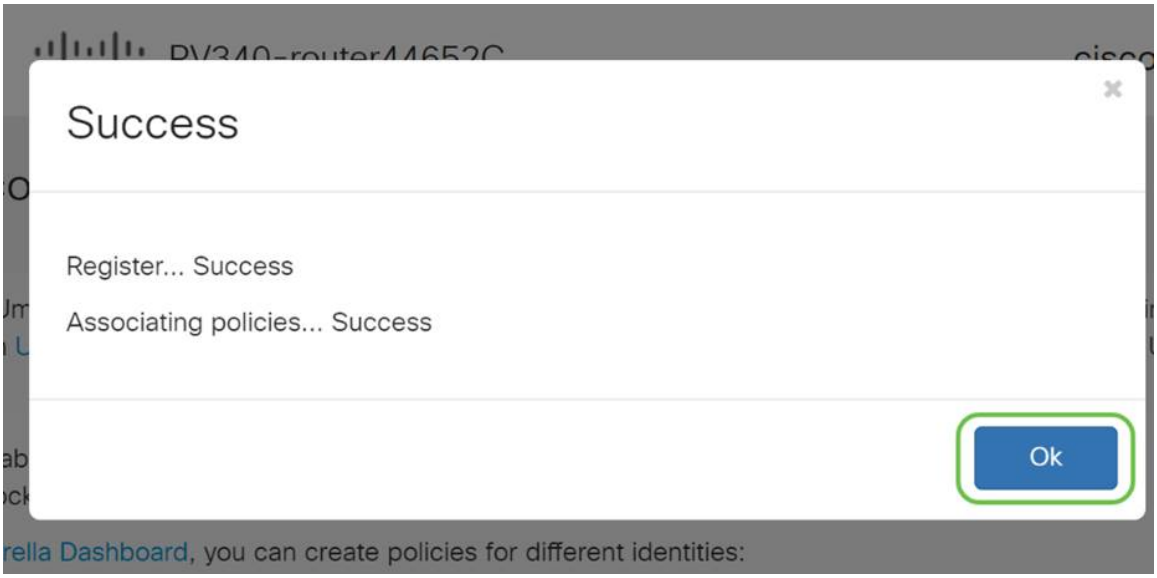
Stap 10

Wijs een naam aan het apparaat toe zodat deze kan worden aangewezen in Umbrella rapportage. We hebben hem *RV345P-Lab* genoemd.



Stap 11

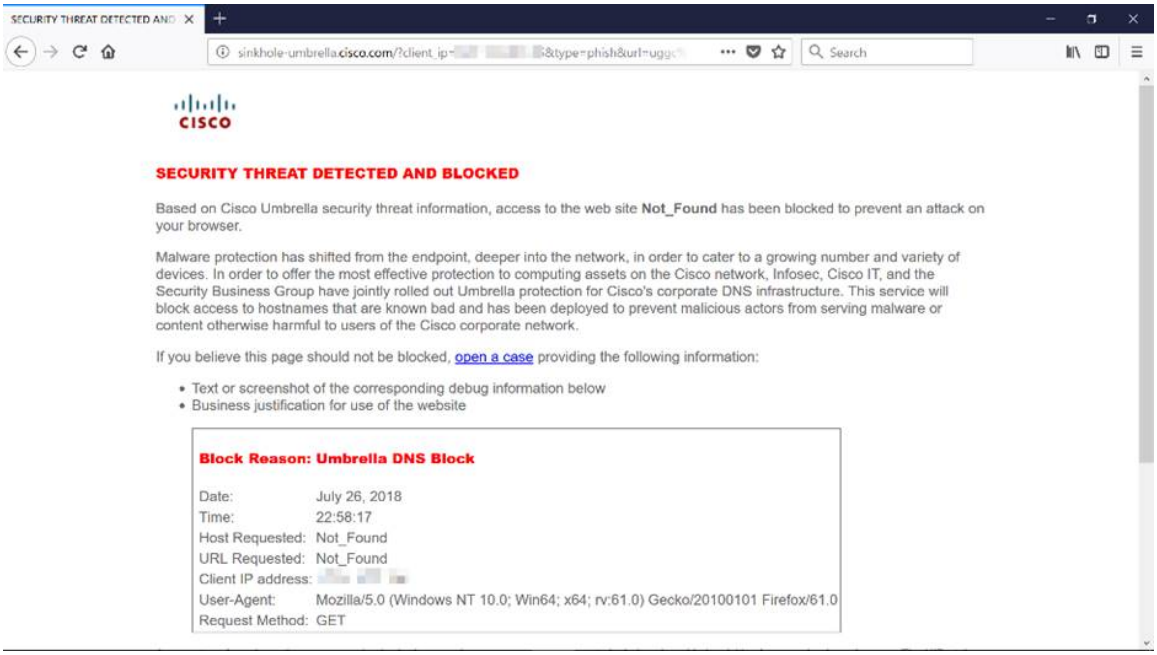
Het volgende scherm zal uw gekozen instellingen valideren en een update verstrekken wanneer geassocieerd met succes. Klik op OK.



bevestiging

Gefeliciteerd, u wordt nu beschermd door Cisco Umbrella. Of ben jij? Laten we zeker zijn door te dubbelcontroleren met een bewegend voorbeeld, heeft Cisco een website gemaakt die zich richt op het bepalen van dit snel als de pagina-ladingen. Klik hier of type https://InternetBadGuys.com in de browser bar.

Als Umbrella correct is ingesteld, wordt u begroet door een scherm dat hierop lijkt.



Overige beveiligingsopties

Bent u bezorgd dat iemand onbevoegde toegang tot het netwerk zou proberen door een Ethernet kabel van een netwerkapparaat uit te trekken en op het te verbinden? In dit geval, is het belangrijk om een lijst van toegestane hosts te registreren om direct met de router te verbinden met hun respectieve IP- en MAC-adressen. De instructies kunnen in het artikel Configuration IP Source Guard op de RV34x Series router gevonden worden.

VPN-opties

Een Virtual Private Network (VPN)-verbinding stelt gebruikers in staat om toegang te krijgen tot, gegevens te verzenden en te ontvangen van en naar een privaat netwerk door middel van een openbaar of gedeeld netwerk zoals het internet, maar toch een beveiligde verbinding met een onderliggende netwerkinfrastructuur te waarborgen om het particuliere netwerk en de bijbehorende bronnen te beschermen.

Een VPN-tunnel stelt een privaat netwerk in dat gegevens veilig kan verzenden met behulp van encryptie en verificatie. Bedrijven maken gebruik vooral van VPN-verbinding omdat het zowel nuttig als noodzakelijk is om hun werknemers toegang te geven tot hun privénetwerk, zelfs als ze zich niet binnen het kantoor bevinden.

VPN staat een externe host toe te handelen alsof ze zich op hetzelfde lokale netwerk bevonden. De router ondersteunt maximaal 50 tunnels. Een VPN-verbinding kan tussen de router en een eindpunt worden ingesteld nadat de router voor internetverbinding is geconfigureerd. De VPN-client is volledig afhankelijk van de instellingen van de VPN-router om een verbinding op te zetten.

Als u niet zeker weet welke VPN het beste bij uw behoeften past, dan uitkijken op Cisco Business VPN - Overzicht en Best Practices.

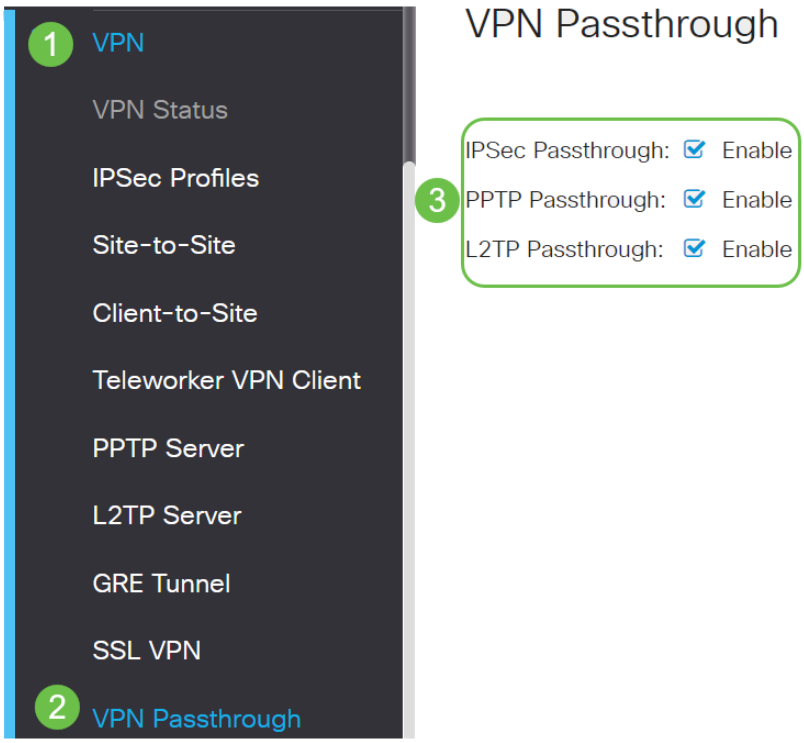
AnyConnect VPN is het enige door Cisco VPN ondersteunde product dat in deze configuratiehandleiding wordt vermeld. Producten die niet afkomstig zijn van derden, zoals The GreenBow en Shrew Soft, worden niet ondersteund door Cisco. Zij worden uitsluitend ter begeleiding opgenomen. Als u deze buiten het artikel wilt ondersteunen, kunt u contact opnemen met die derde partij voor ondersteuning.

Als u niet van plan bent een VPN op te zetten, kunt u klikken om naar de volgende sectie te springen.

VPN-doorgifte

Over het algemeen ondersteunt elke router Network Address Translation (NAT) om IP-adressen te besparen wanneer u meerdere clients met dezelfde internetverbinding wilt ondersteunen. Point-to-Point Tunneling Protocol (PPTP) en Internet Protocol Security (IPsec) VPN ondersteunen NAT niet. Dit is waar de VPN-doorgifte binnenkomt. Een VPN-passthrough is een functie waarmee VPN-verkeer dat gegenereerd is vanuit VPN-clients die op deze router zijn aangesloten, door deze router kan gaan en op een VPN-eindpunt kan worden aangesloten. De Wachtwoord van VPN staat PPTP en IPsec VPN toe om door te gaan naar het internet dat vanaf een VPN-client wordt geïnitieerd en vervolgens de externe VPN-gateway te bereiken. Deze optie wordt vaak aangetroffen op thuisrouters die NAT ondersteunen.

Standaard wordt IPsec, PPTP en L2TP-passthrough ingeschakeld. Als u deze instellingen wilt bekijken of aanpassen, selecteert u **VPN > VPN-doorloop**. Bekijk of pas indien nodig aan.



AnyConnect VPN

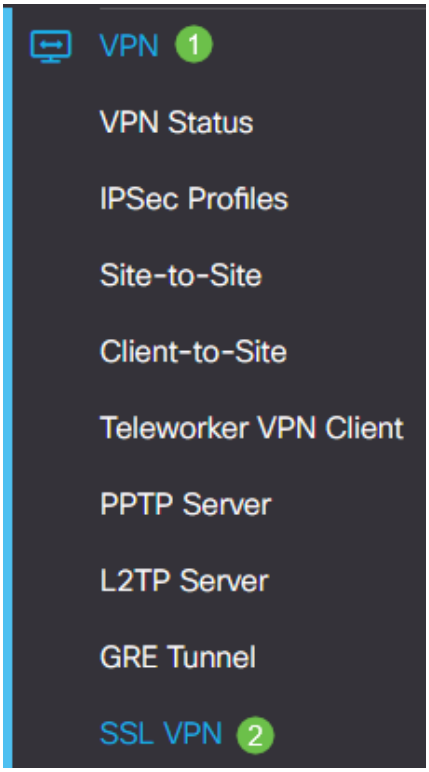
Er zijn verschillende voordelen aan het gebruik van Cisco AnyConnect:

1. Beveiligde en persistente connectiviteit
2. Aanhoudende veiligheid en handhaving van het beleid
3. Invoerbaar van de adaptieve security applicatie (ASA) of van Enterprise Software Deployment Systems
4. Aanpasbaar en vertaalbaar
5. Eenvoudig ingesteld
6. Ondersteunt zowel Internet Protocol Security (IPsec) als Secure Socket Layer (SSL)
7. Ondersteunt het protocol Internet Key Exchange versie 2.0 (IKEv2.0)

AnyConnect SSL VPN configureren op RV345P

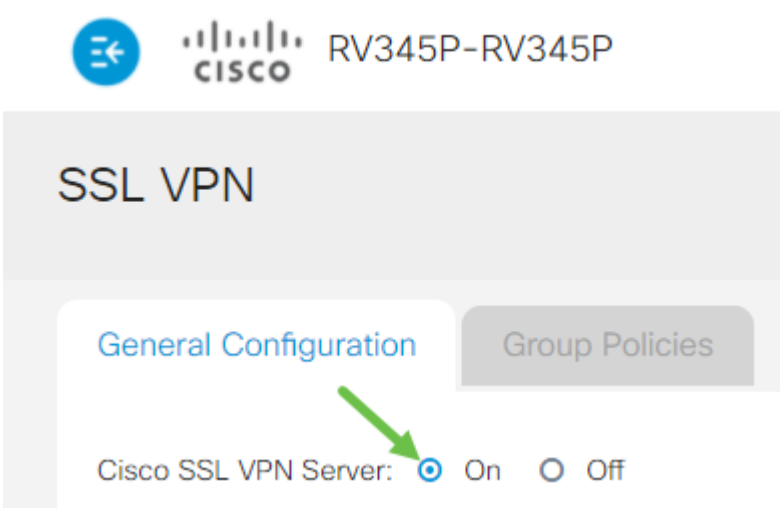
Stap 1

Toegang tot de router op web-gebaseerde voorziening en kies **VPN > SSL VPN**.



Stap 2

Klik op het radioknop Aan om Cisco SSL VPN-server in te schakelen.



Instellingen verplichte gateway

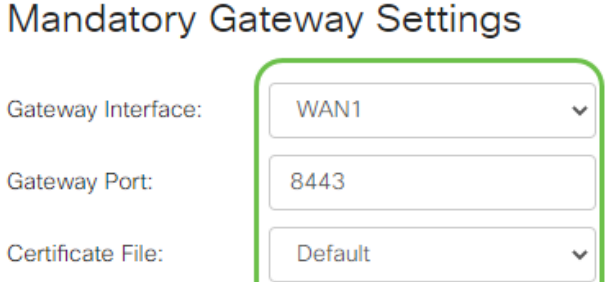
Stap 1

De volgende configuratie-instellingen zijn verplicht:

1. Kies de Gateway-interface in de vervolgkeuzelijst. Dit is de poort die wordt gebruikt voor het doorgeven van verkeer door de SSL VPN-tunnels. De opties omvatten: WAN1, WAN2, USB1, USB2
2. Voer het poortnummer in dat voor de SSL VPN-poort wordt gebruikt in het veld Gateway-poort tussen 1 en 65535.
3. Selecteer het certificaatbestand in de vervolgkeuzelijst. Dit certificaat verklaart gebruikers die proberen om tot de netwerkbron door de SSL VPN-tunnels te toegang te krijgen, authentiek. De vervolgkeuzelijst bevat een standaardcertificaat en de geïmporteerde certificaten.
4. Voer het IP-adres in van de pool van het clientadres in het veld *Clientadres*. Deze pool zal het bereik van IP-adressen zijn dat aan externe VPN-clients wordt toegewezen.

   Zorg dat het IP-adresbereik geen overlap is met de IP-adressen op het lokale netwerk.

6. Kies het clientnetwerkmasker in de vervolgkeuzelijst.
7. Voer de client-domeinnaam in in het veld *Clientdomein*. Dit zal de domeinnaam zijn die aan SSL VPN cliënten moet worden geduwd.
8. Voer de tekst in die als een inlogbanner wordt weergegeven in het veld *Login Banner*. Dit is de banner die wordt weergegeven telkens wanneer een client inlogt.



Stap 2

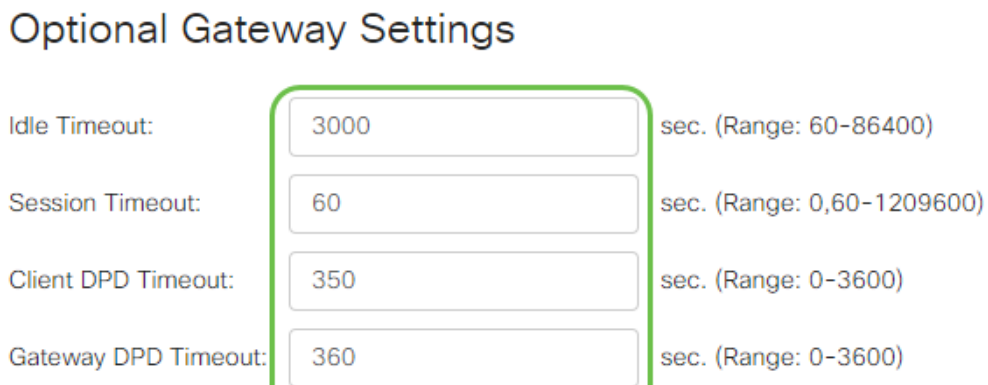
Klik op Apply (Toepassen).

Optionele gateway-instellingen

Stap 1

De volgende configuratie-instellingen zijn optioneel:

1. Geef een waarde in seconden op voor de tijdelijke oplossing van inactiviteitstimer die varieert van 60 tot 86400. Dit is de tijdsduur waarop de SSL VPN-sessie ongebruikt kan blijven.
2. Voer in het veld Time-out van *sessie* een waarde in seconden in. Dit is de tijd die het nodig heeft voor de TCP- of UDP-sessie (Transmission Control Protocol) of User Datagram Protocol (UDP) om na de opgegeven stationaire tijd uit te schakelen. Het bereik loopt van 60 tot 1209600.
3. Voer in seconden een waarde in in het veld *Time-out bij ClientDPD* tussen 0 en 3600. Deze waarde specificeert het periodiek verzenden van HELLO/ACK berichten om de status van de VPN-tunnel te controleren. Deze optie moet aan beide uiteinden van de VPN-tunnel zijn ingeschakeld.
4. Voer een waarde in seconden in het veld *Time-out* bij *GatewayDPD* tussen 0 en 3600 in. Deze waarde specificeert het periodiek verzenden van HELLO/ACK berichten om de status van de VPN-tunnel te controleren. Deze optie moet aan beide uiteinden van de VPN-tunnel zijn ingeschakeld.
5. Voer een waarde in seconden in het veld *Levend houden* in variërend van 0 tot 600. Deze functie garandeert dat uw router altijd met internet verbonden is. De VPN-verbinding wordt hersteld als deze wordt verbroken.
6. Voer in seconden een waarde in voor de duur van de tunnel die wordt aangesloten in het veld *Lease Duration*. Het bereik loopt van 600 tot 1209600.
7. Geef de pakketgrootte in bytes op die via het netwerk kunnen worden verzonden. Het bereik loopt van 576 tot 1406.
8. Voer de tussenliggende tijd in in het veld *Rekey Interval*. De Rekey-functie stelt de SSL-toetsen in staat om opnieuw te onderhandelen nadat de sessie is ingesteld. Het bereik loopt van 0 tot 43200.



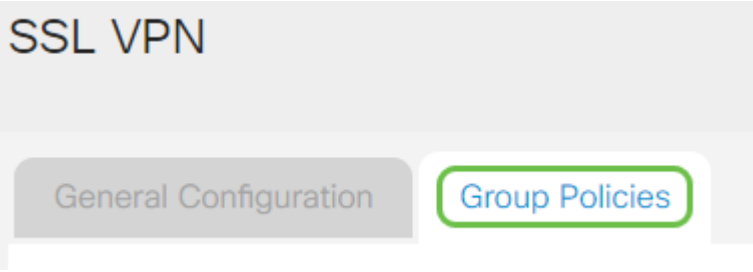
Stap 2

Klik op Apply (Toepassen).

Groepsbeleid configureren

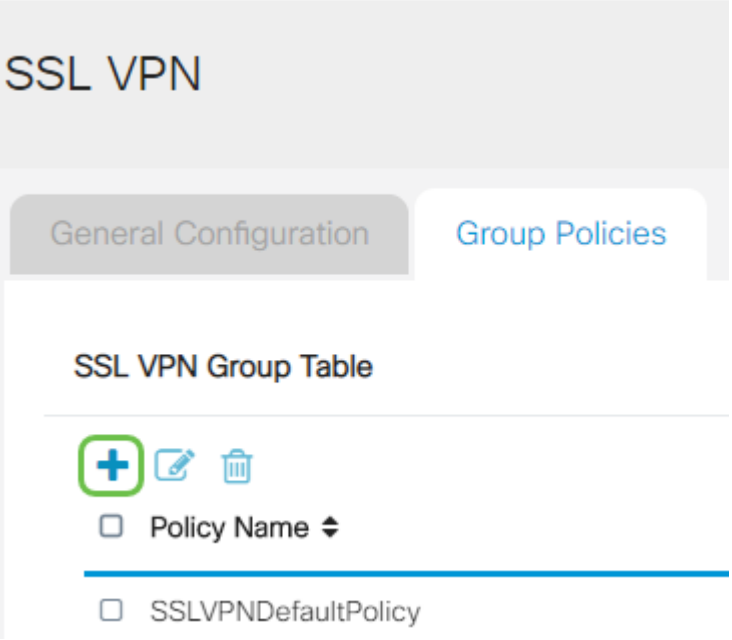
Stap 1

Klik op het tabblad **Groepsbeleid**.



Stap 2

Klik op het **pictogram toevoegen** onder de SSL VPN Group Tabel om een groepsbeleid toe te voegen.

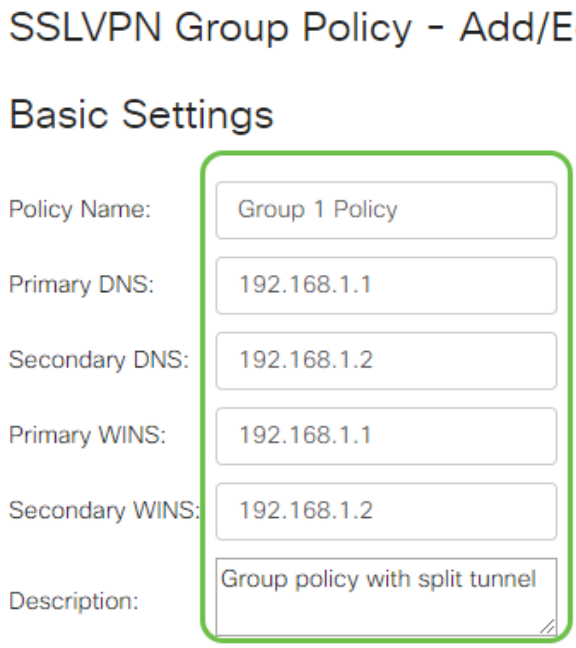


De SSL VPN Group tabel toont de lijst met groepsbeleid op het apparaat. U kunt ook het eerste groepsbeleid in de lijst bewerken, dat SSLVPNefaultPolicy wordt genoemd. Dit is het standaardbeleid dat door het apparaat wordt geleverd.

Stap 3

1. Voer de gewenste beleidsnaam in het veld *Beleidsnaam* in.

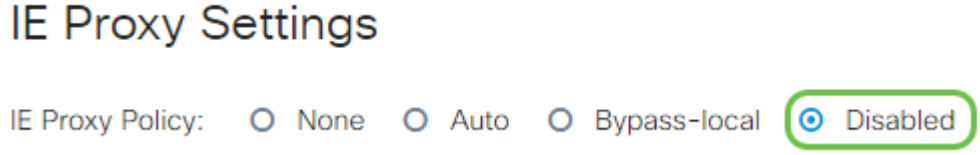
2. Voer het IP-adres van de primaire DNS in het veld in. Standaard wordt dit IP-adres al meegeleverd.
3. *(Optioneel) Voer in het daarvoor bestemde veld het IP-adres van de secundaire DNS in. Dit zal als back-up dienen voor het geval dat de primaire DNS niet werkt.*
4. (Optioneel) Voer het IP-adres van de primaire WINS in het daarvoor bestemde veld in.
5. (Optioneel) Voer het IP-adres van de secundaire WINS in het veld in dat wordt opgegeven.
6. (Optioneel) Typ een beschrijving van het beleid in het veld *Description*.



Stap 4 (optioneel)

Klik op een radioknop om het beleid van de Proxy te kiezen om de volmachtinstellingen van Microsoft Internet Explorer (MSIE) toe te staan om een VPN-tunnel op te zetten. De opties zijn:

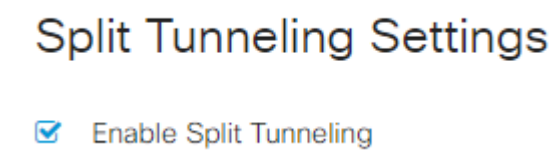
- Geen - Hiermee kan de browser geen proxy instellingen gebruiken.
- Auto - Hiermee kan de browser de proxy-instellingen automatisch detecteren.
- Bypass-local - Hiermee kan de browser de proxy-instellingen omzeilen die zijn ingesteld op de externe gebruiker.
- Uitgeschakeld - schakelt de MSIE proxy-instellingen uit.



Stap 5 (optioneel)

In het gebied Instellingen gesplitste tunneling controleert u het selectieknop **Split-tunneling inschakelen** om het voor Internet bestemde verkeer ongeversleuteld via Internet te laten versturen. Full Tunneling stuurt al verkeer naar het eindapparaat waar

het dan naar bestemmingsmiddelen wordt routeerd, die het bedrijfsnetwerk van het pad voor web toegang elimineert.

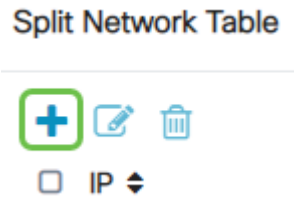


Stap 6 (optioneel)

Klik op een radioknop om te kiezen of u verkeer wilt opnemen of uitsluiten bij het toepassen van de gesplitste tunneling.

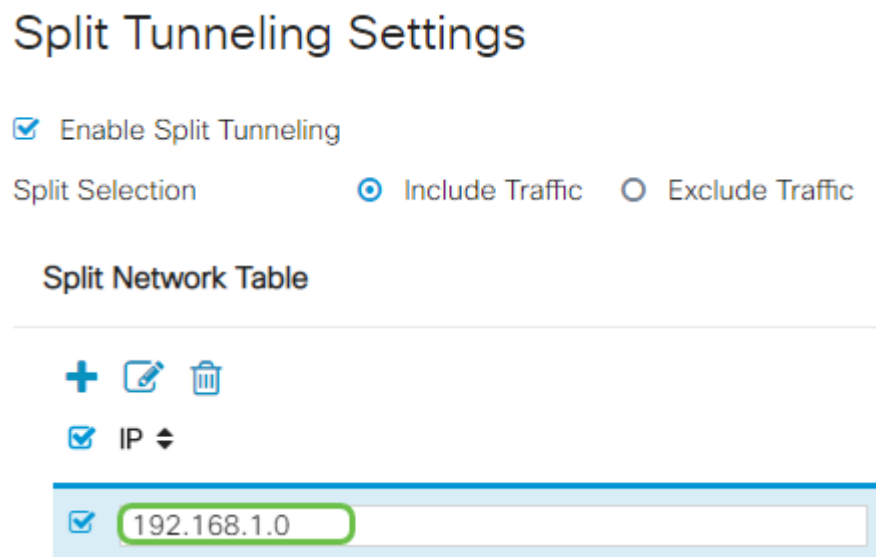
Stap 7

In de tabel Netwerk splitsen klikt u op het **pictogram toevoegen** om een uitzondering op netwerk toe te voegen.



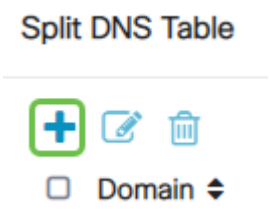
Stap 8

Voer in het daarvoor bestemde veld het IP-adres van het netwerk in.



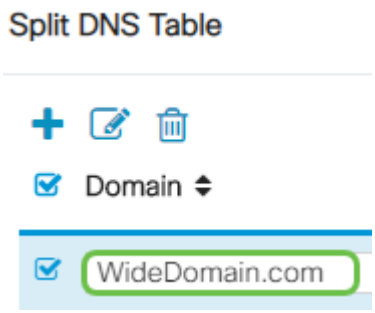
Stap 9

Klik in de DNS-tabel splitsen op het **pictogram toevoegen** om een gesplitste DNS-uitzondering toe te voegen.



Stap 10

Voer de naam van het domein in in het daarvoor bestemde veld en klik vervolgens op **Toepassen**.



De router heeft standaard 2 AnyConnect-serverlicenties. Dit betekent dat als u AnyConnect-clientlicenties hebt, u 2 VPN-tunnels tegelijkertijd kunt instellen met een andere RV340-seriemurouter.

Kortom, de RV345P-router heeft geen licentie nodig, maar alle klanten hebben er een nodig. AnyConnect-clientlicenties bieden desktop en mobiele klanten externe toegang tot het VPN-netwerk.

In dit volgende gedeelte wordt beschreven hoe u licenties voor uw klanten kunt krijgen.

AnyConnect Mobility-client

Een VPN-client is software die op een computer is geïnstalleerd en uitgevoerd om verbinding te maken met het externe netwerk. Deze clientsoftware moet worden ingesteld met dezelfde configuratie als de VPN-server, zoals het IP-adres en de verificatieinformatie. Deze authenticatie-informatie bevat de gebruikersnaam en de vooraf gedeelde sleutel die gebruikt zal worden om de gegevens te versleutelen. Afhankelijk van de fysieke locatie van de netwerken die moeten worden aangesloten, kan een VPN-client ook een hardwareapparaat zijn. Dit gebeurt meestal als de VPN-verbinding wordt gebruikt om twee netwerken aan te sluiten die op verschillende locaties liggen.

De Cisco AnyConnect Secure Mobility Client is een softwaretoepassing voor de aansluiting op een VPN dat werkt op verschillende besturingssystemen en hardwareconfiguraties. Deze softwaretoepassing maakt het mogelijk om middelen op afstand van een ander netwerk toegankelijk te maken alsof de gebruiker direct op zijn netwerk is aangesloten, maar op een veilige manier.

Nadat de router is geregistreerd en geconfigureerd met AnyConnect, kan de client licenties op de router installeren vanuit uw beschikbare pool van licenties die u hebt aangeschaft, hetgeen in de volgende sectie gedetailleerd is.

Licentie kopen

U moet een licentie aanschaffen bij uw Cisco-distributeur of uw Cisco-partner. Wanneer u een licentie bestelt, moet u uw Cisco Smart Account-ID of Domain ID in de vorm van *name@domain.com* verstrekken.

Als u geen distributeur of partner van Cisco hebt, kunt u hier één plaatsen.

Op het moment van schrijven kunnen de volgende product-SKU's worden gebruikt om extra licenties in bundels van 25 aan te schaffen. Merk op dat er andere opties zijn voor de AnyConnect-clientlicenties zoals uiteengezet in de Cisco AnyConnect-bestelgids, maar de product-ID die in de lijst staat, is het minimumvereiste voor volledige functionaliteit.

Let op, het product SKU van de AnyConnect-clientlicentie dat eerst wordt vermeld, geeft licenties voor een periode van 1 jaar en vereist een minimale aankoop van 25 licenties. Andere SKU's die van toepassing zijn op de RV340-Series routers zijn ook beschikbaar met verschillende abonnementsniveaus, en wel als volgt:

- **LS-AC-PLS-1Y-S1** — 1 jaar Cisco AnyConnect Plus-licentie
- **LS-AC-PLS-3Y-S1** — 3-jarig Cisco AnyConnect Plus-licentie
- **LS-AC-PLS-5Y-S1** — 5 jaar Cisco AnyConnect Plus-licentie
- **LS-AC-PLS-P-25-S** — 25-poorts Cisco AnyConnect Plus permanente client-licentie
- **LS-AC-PLS-P-50-S** — 50-poorts Cisco AnyConnect Plus permanente client-licentie

Clientinformatie

Wanneer uw client een van de volgende instellingen instelt, dient u deze links te verzenden:

- Windows: AnyConnect op een Windows-computer
- Mac: Installeer AnyConnect op Mac.
- Ubuntu-desktop: AnyConnect installeren en gebruiken op een Ubuntu-desktop
- Als u problemen hebt, kunt u informatie voor fundamentele probleemoplossing gaan verzamelen op Cisco AnyConnect Secure Mobility Client-fouten.

Controleer de AnyConnect VPN-connectiviteit

Stap 1

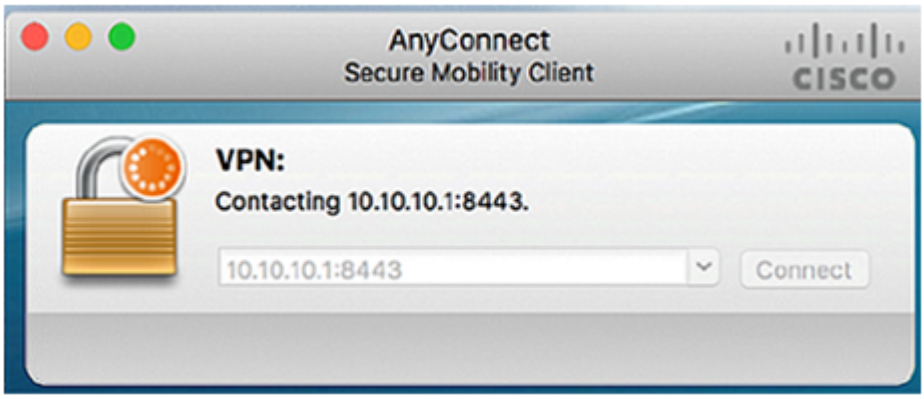
Klik op het **pictogram AnyConnect Secure Mobility Client**.

Stap 2

Voer in het venster AnyConnect Secure Mobility Client het IP-adres van de gateway en het poortnummer in dat door een kolom wordt gescheiden (:) en klik vervolgens op

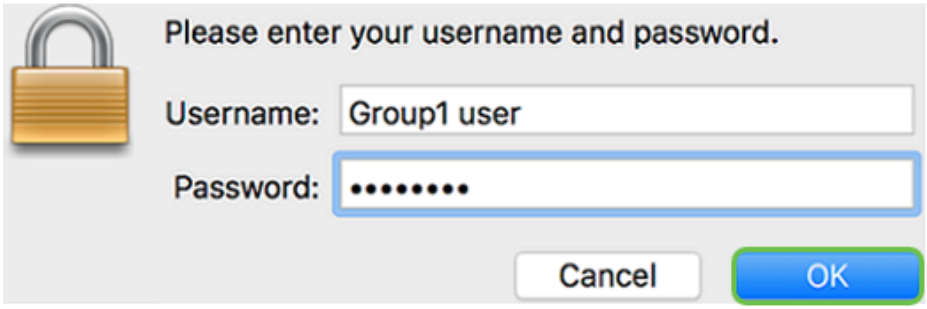
Connect.

De software zal nu laten zien dat hij contact opneemt met het externe netwerk.



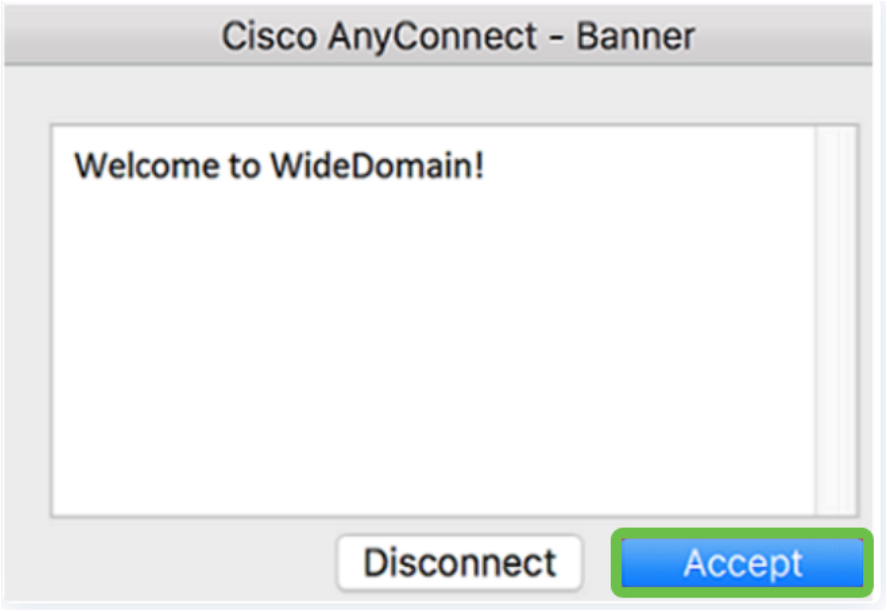
Stap 3

Voer in de betreffende velden uw gebruikersnaam en wachtwoord in en klik vervolgens op OK.

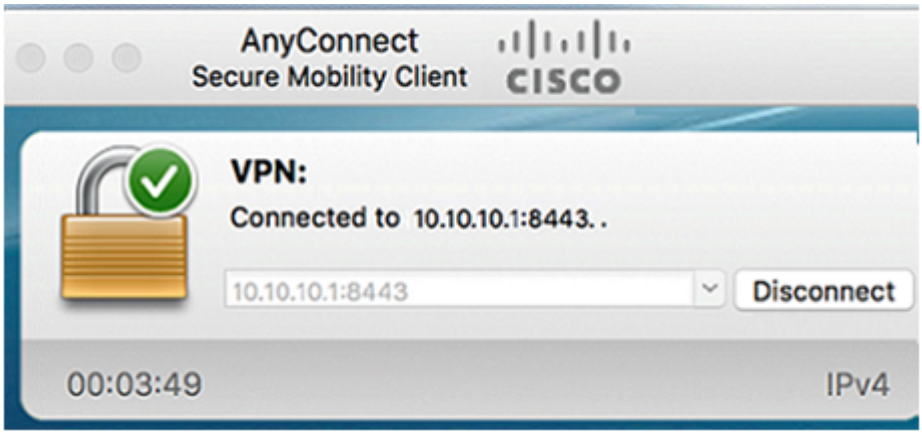


Stap 4

Zodra de verbinding wordt tot stand gebracht, wordt de Login Banner weergegeven. Klik op Aanvaarden.



Het AnyConnect-venster dient nu de succesvolle VPN-verbinding met het netwerk aan te geven.



Als u nu AnyConnect VPN gebruikt, kunt u voorbij de andere VPN-opties overslaan en naar de volgende sectie verdergaan.

Zachte VPN weergeven

Een IPsec VPN stelt u in staat om externe bronnen veilig te verkrijgen door het instellen van een versleutelde tunnel over het internet. De RV34X Series-routers werken als IPsec VPN-servers en ondersteunen de Shrew Soft VPN-client. Deze sectie zal u tonen hoe u uw router en de Zachte client van de Rij kunt configureren om een verbinding met een VPN te maken.

Cisco ondersteunt Shrew Soft niet. Dit voorbeeld wordt uitsluitend voor demonstratiedoeleinden verstrekt. Als u problemen hebt met Shrew Soft, neemt u contact op met deze organisaties voor ondersteuning.

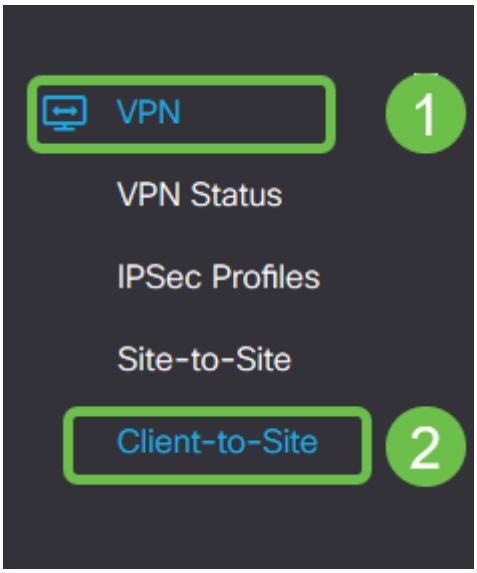
U kunt de nieuwste versie van de software van de Shrew Soft VPN-client hier downloaden: https://www.shrew.net/download/vpn

Zachte tonen op de RV345P Series router

We beginnen met het configureren van het **client-naar-site VPN** op de RV345P.

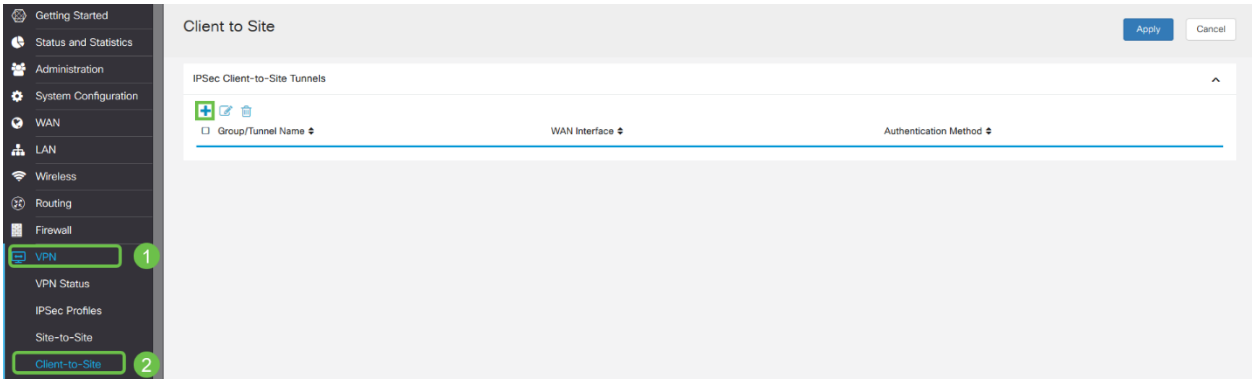
Stap 1

Navigeer naar **VPN > Client-to-Site.**



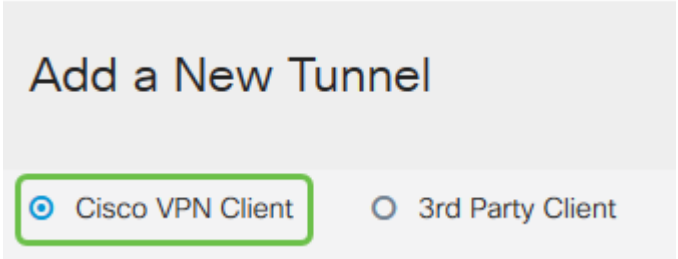
Stap 2

Voeg een **client-to-Site** VPN-profiel toe.



Stap 3

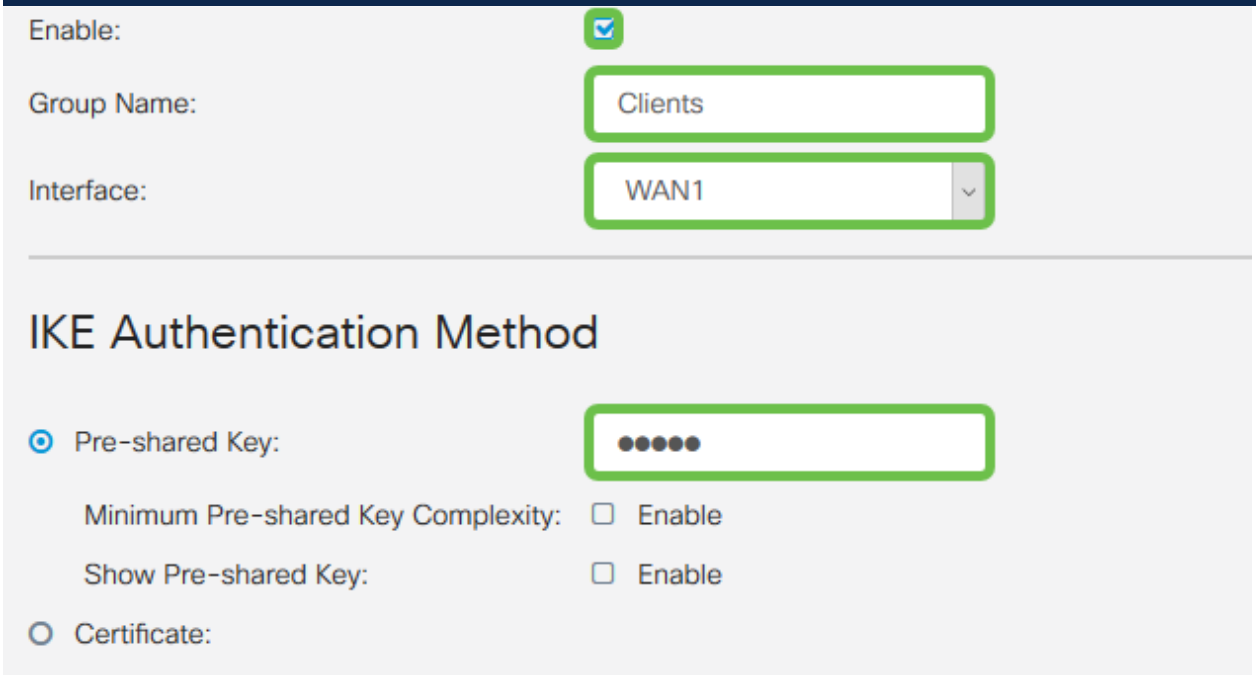
Selecteer de optie **Cisco VPN-client**.



Stap 4

Controleer het vakje Inschakelen om het VPN-clientprofiel actief te maken. We zullen ook de *groepsnaam* configureren, de **WAN-interface** selecteren en een **vooraf gedeelde sleutel** invoeren.

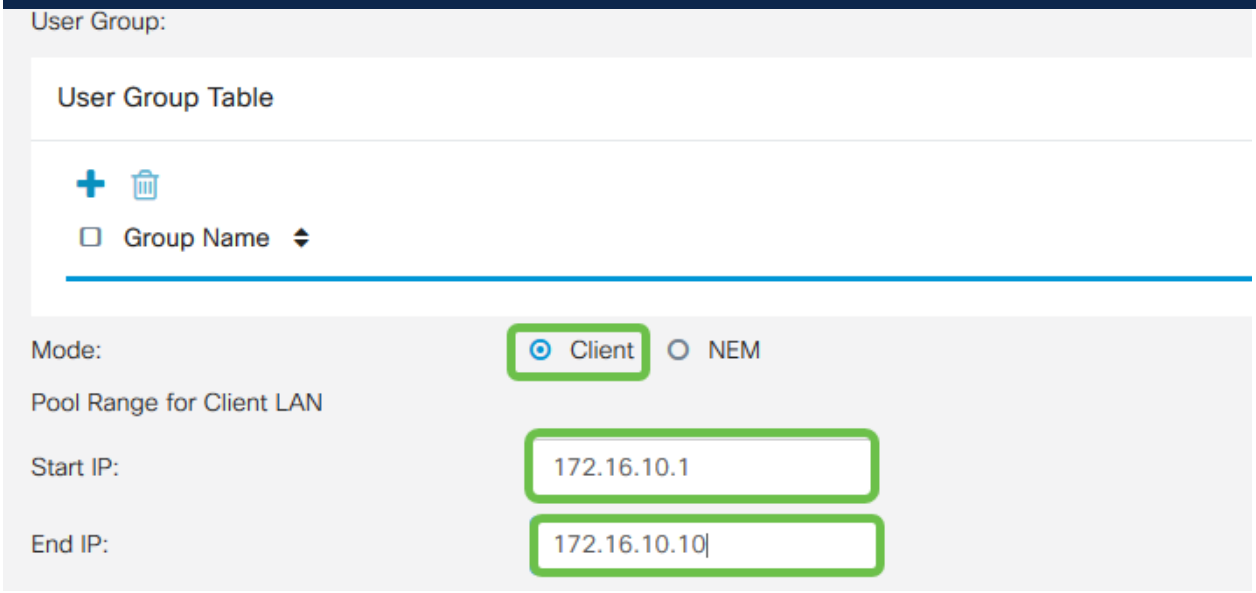
Let op de *groepsnaam* en *Voorgedeelde sleutel* omdat deze later bij het configureren van de client gebruikt zal worden.



Stap 5

Laat de lege **gebruikersgroep** voorlopig achter. Dit is voor de *Gebruikersgroep* op de router, maar we hebben deze nog niet ingesteld. Zorg ervoor dat de **modus** is ingesteld op **client**. Geef het **wolbereik voor clientadaptertools op**. We gebruiken 172.16.10.1 tot en met 172.16.10.10.

Het bereik van de pool zou een uniek Subnet moeten gebruiken dat niet elders op het netwerk gebruikt wordt.

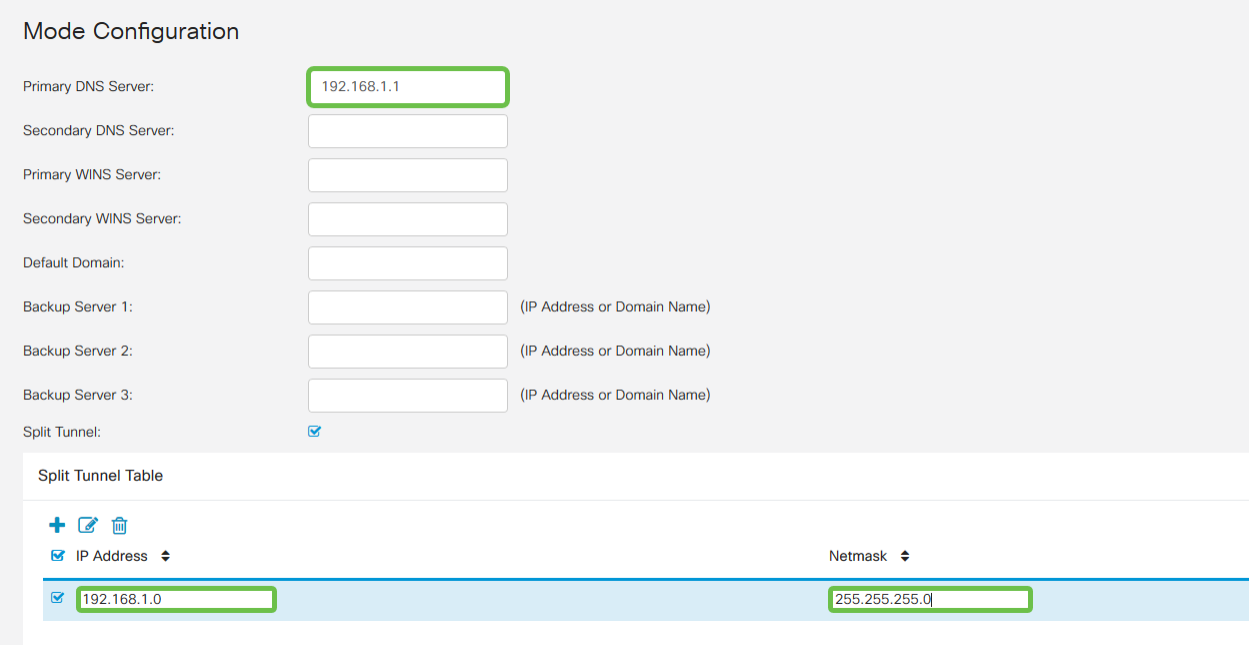


Stap 6

Hier configureren we de instellingen van de **Mode Configuration**. Hier zijn de

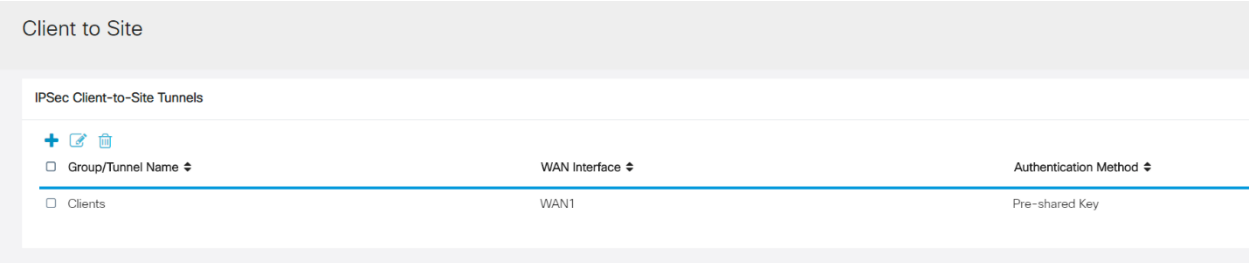
instellingen die we zullen gebruiken:

- **Primaire DNS-server**: Als u een interne DNS-server hebt of een externe DNS-server wilt gebruiken, kunt u deze hier invoeren. Anders wordt de standaard ingesteld op het RV345P LAN IP-adres. We zullen het standaard gebruiken in ons voorbeeld.
- **Split Tunnel:** controleer of Split Tunneling mogelijk is. Dit wordt gebruikt om te specificeren welk verkeer via de VPN-tunnel gaat. In ons voorbeeld zullen we Split Tunnel gebruiken.
- **Tabel voor splitsingen:** Voer de netwerken in waarop de VPN-client toegang moet hebben via VPN. Dit voorbeeld gebruikt het RV345P LAN-netwerk.



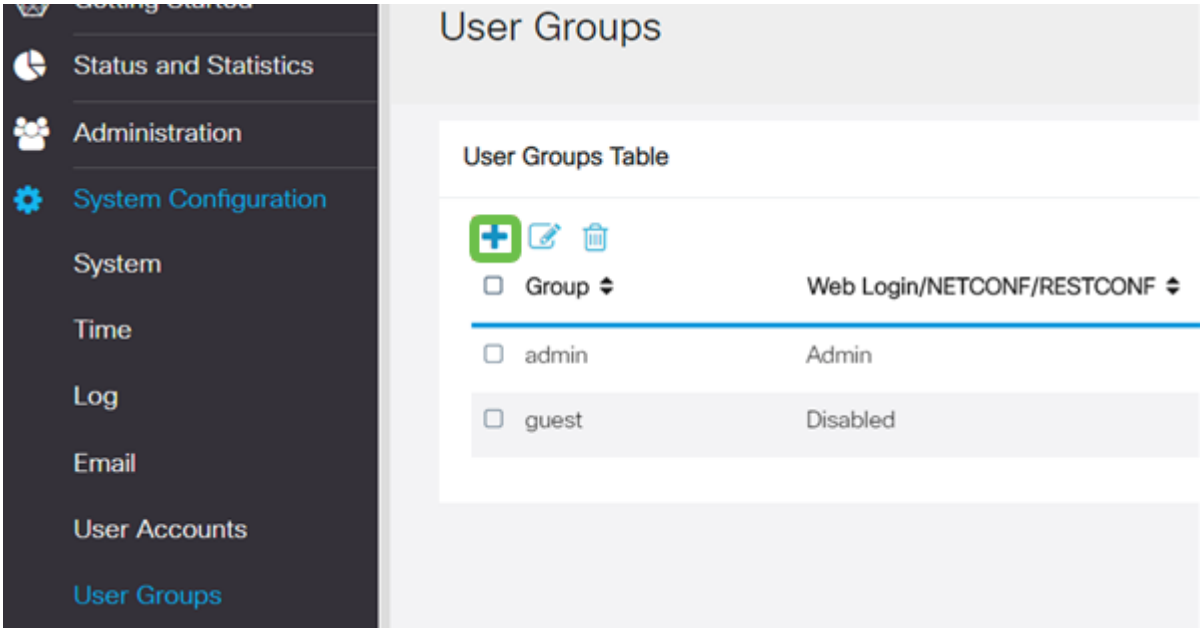
Stap 7

Nadat u op **Opslaan** hebt geklikt, kunt u het profiel zien in de lijst **IPsec Client-to-Site Group**.



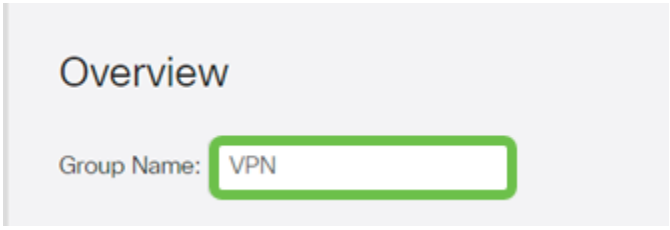
Stap 8

Het configureren van een **gebruikersgroep** voor het controleren van VPN-clientgebruikers. Klik onder **Systeemconfiguratie > Gebruikersgroepen** op het **pictogram plus** om een gebruikersgroep toe te voegen.



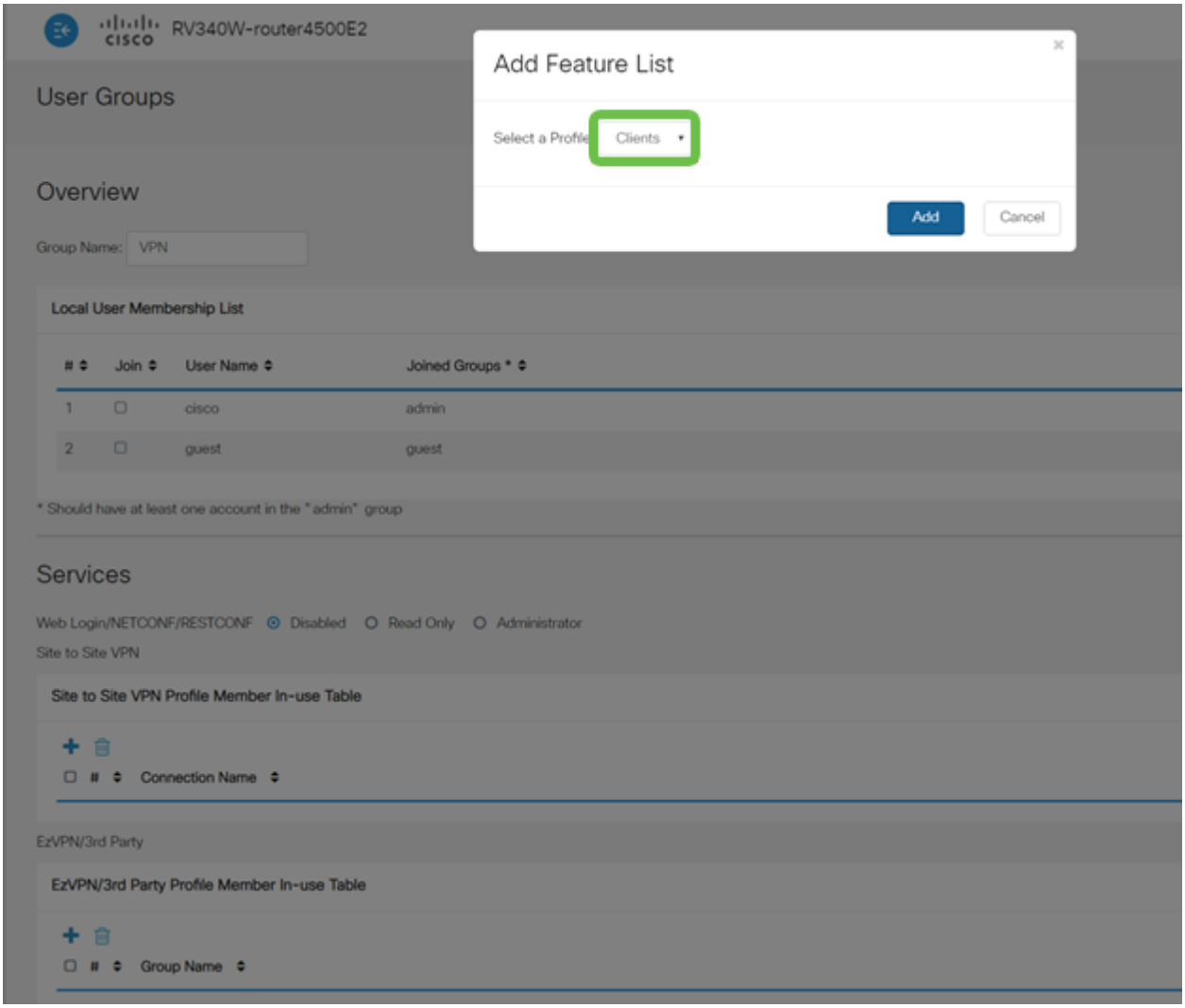
Stap 9

Voer een **groepsnaam in**.



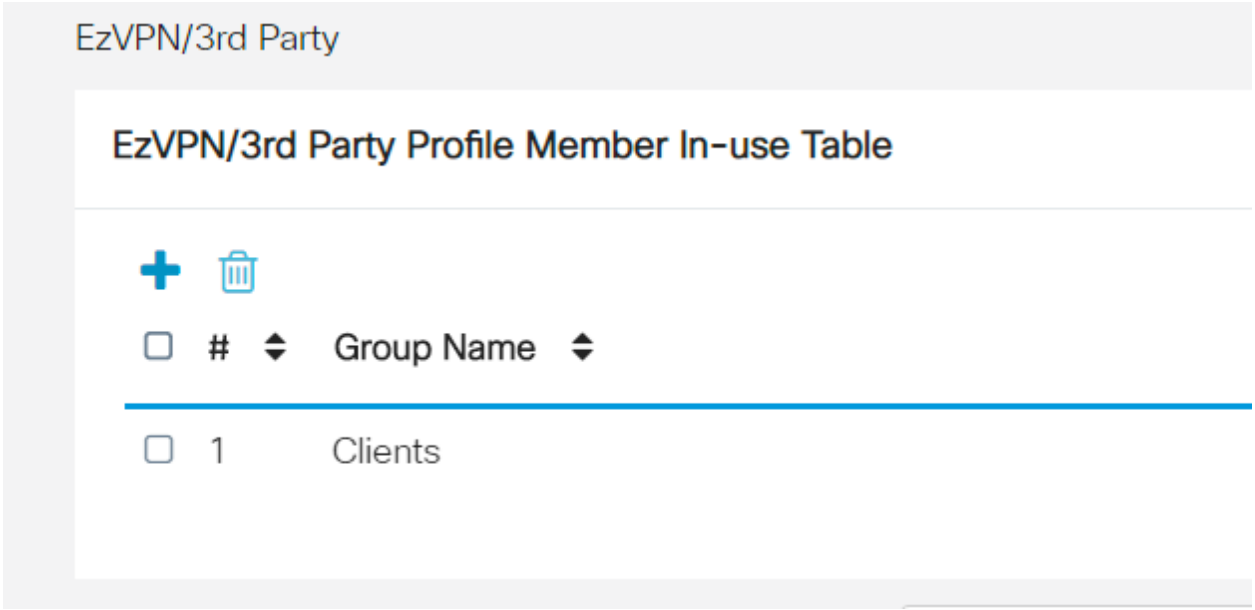
Stap 10

Klik onder **Services > EzVPN/3rd Party** op **Add** om deze gebruikersgroep te koppelen aan het **client-to-site** profiel dat eerder was geconfigureerd.



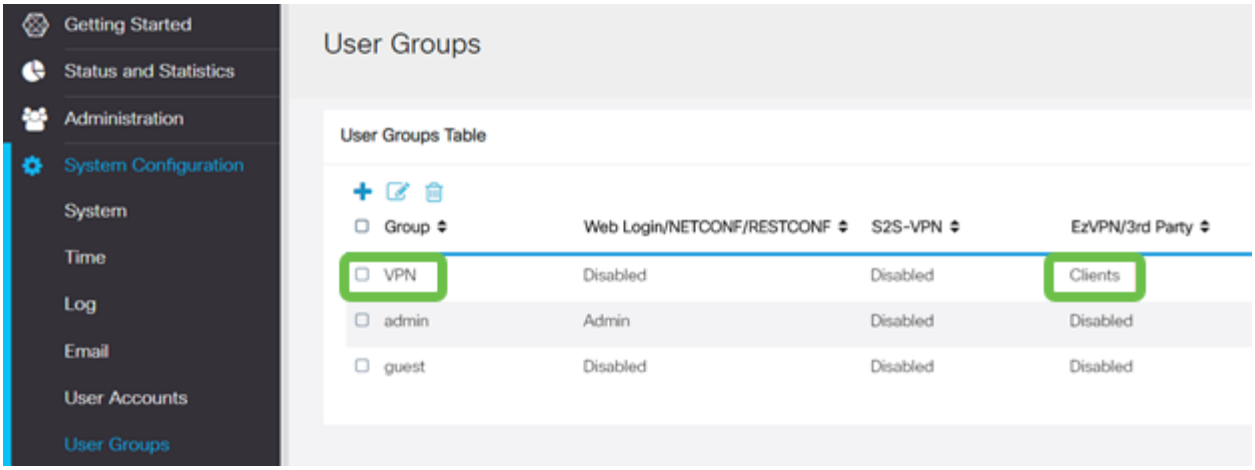
Stap 11

U dient nu de naam **van de client-to-Site** groep in de lijst voor **EzVPN/3rd** te zien.



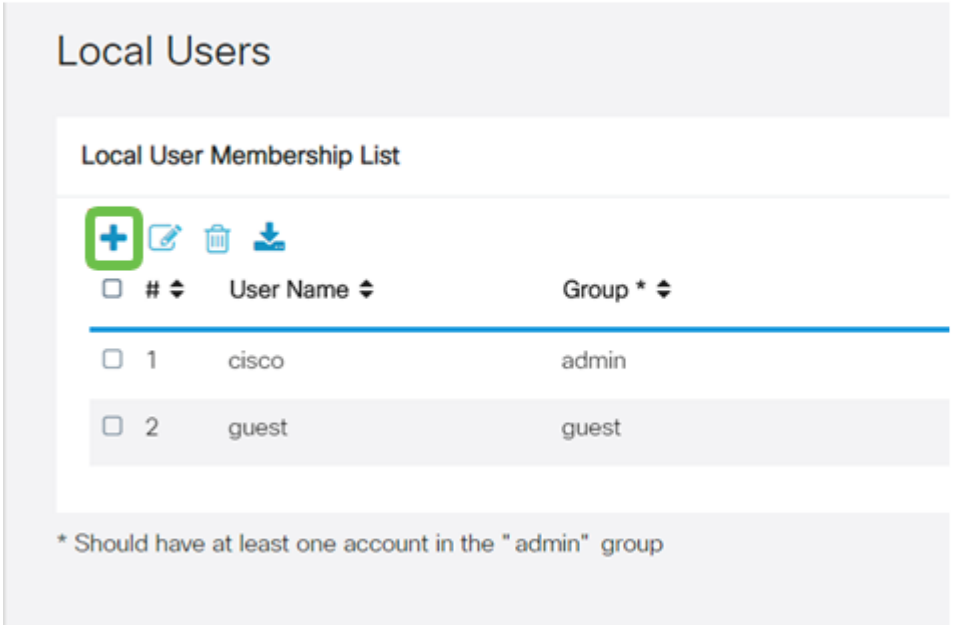
Stap 12

Nadat u de configuratie van de gebruikersgroep **toepast**, ziet u het in de lijst **Gebruikersgroepen** en de nieuwe gebruikersgroep wordt gebruikt met het client-naar-site profiel dat u eerder hebt gemaakt.



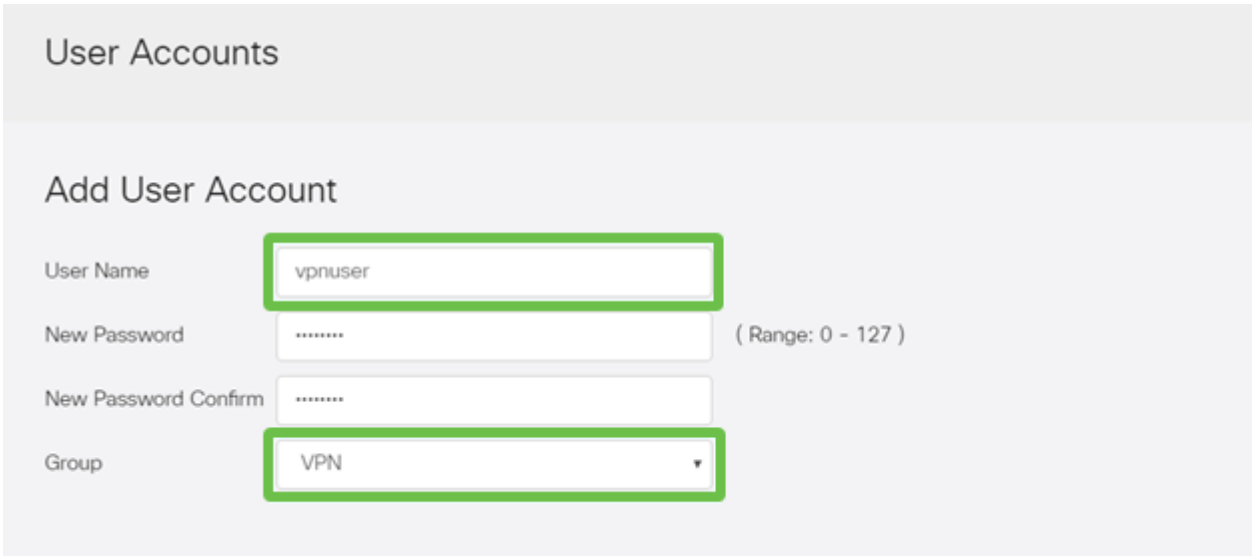
Stap 13

Configureer een nieuwe gebruiker in **systeemconfiguratie > gebruikersrekeningen**. Klik op het **pictogram plus** om een nieuwe gebruiker te maken.



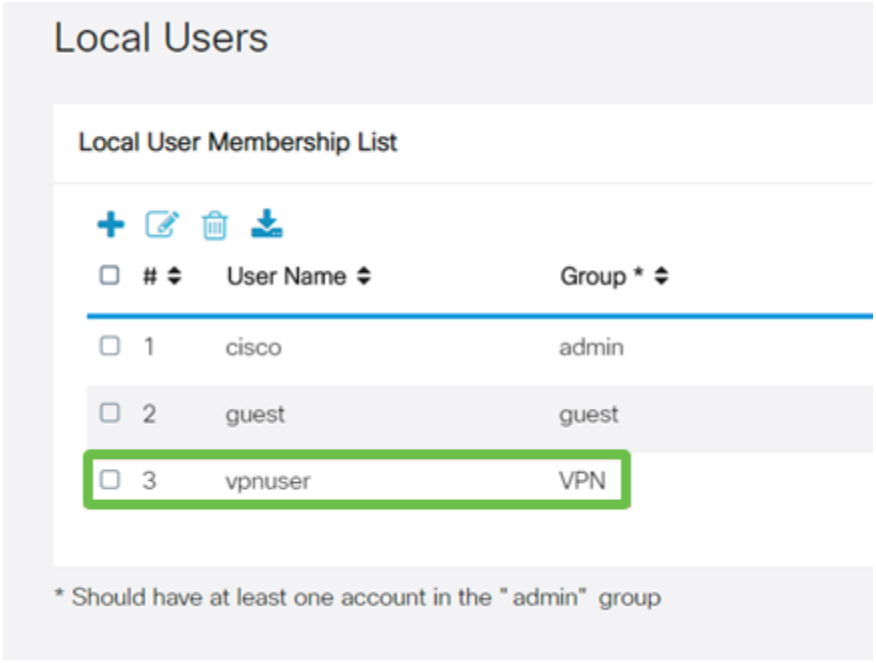
Stap 14

Voer de nieuwe **gebruikersnaam** in samen met het **nieuwe wachtwoord**. Controleer dat de **groep** is ingesteld op de nieuwe **gebruikersgroep** die u zojuist hebt ingesteld. Klik op **Toepassen** na voltooiing.



Stap 15

De nieuwe **gebruiker** verschijnt in de lijst met **lokale gebruikers**.



Dit voltooit de configuratie op de RV345P Series router. Daarna zult u de Shrew Soft VPN client configureren.

De zachte VPN-client tonen

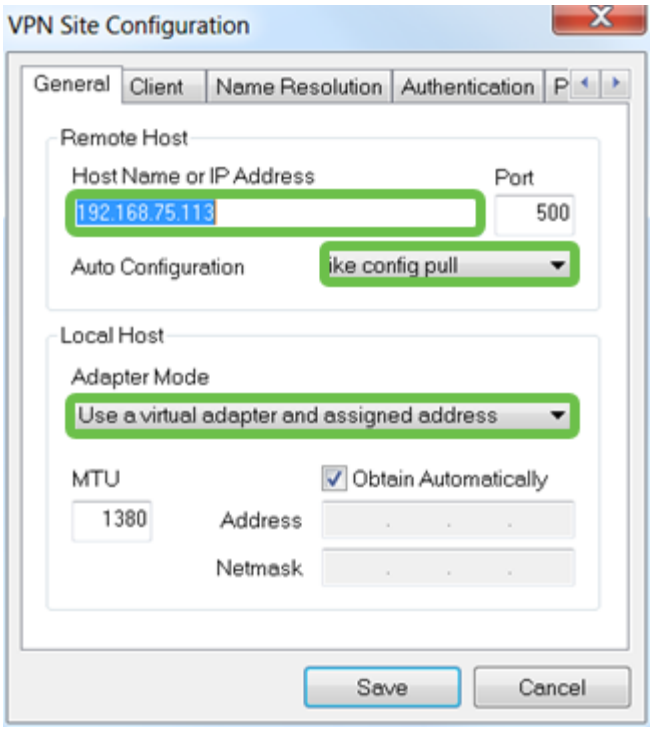
Volg de volgende stappen.

Stap 1

Open de Shrew *Soft VPN Access Manager* en klik op **Add** om een profiel toe te voegen. In het venster *VPN Site Configuration* dat nu wordt weergegeven, configureren u het **tabblad General**:

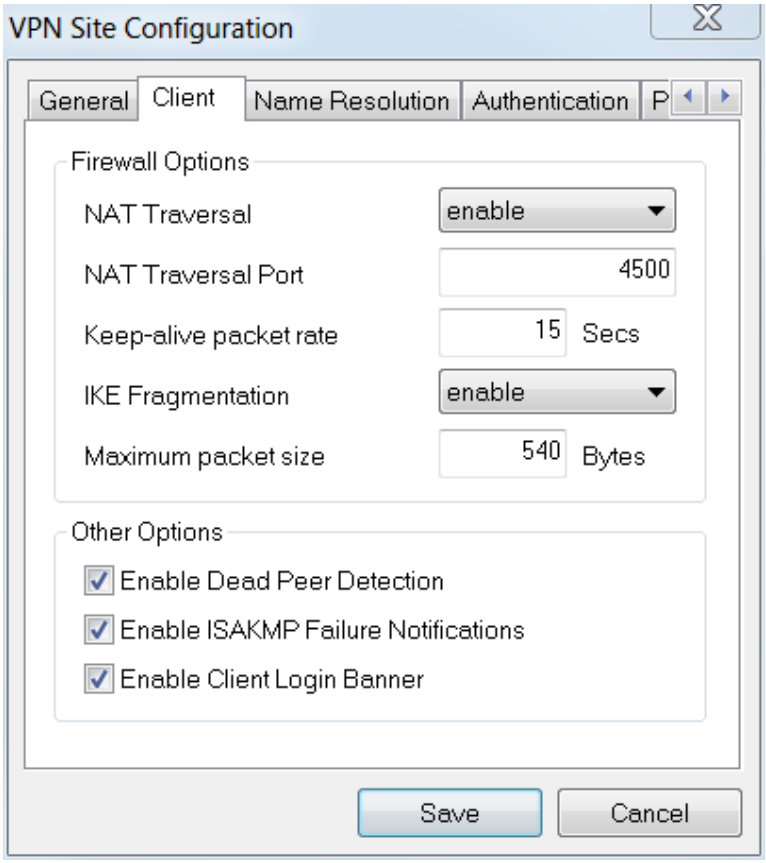
- **Hostnaam of IP-adres**: Gebruik het WAN IP-adres (of hostname van RV345P)
- **Automatische configuratie**: Selecteren **bestand bestand bestand**

- **Adapter-modus**: Selecteer **Gebruik een virtuele adapter en toegewezen adres**



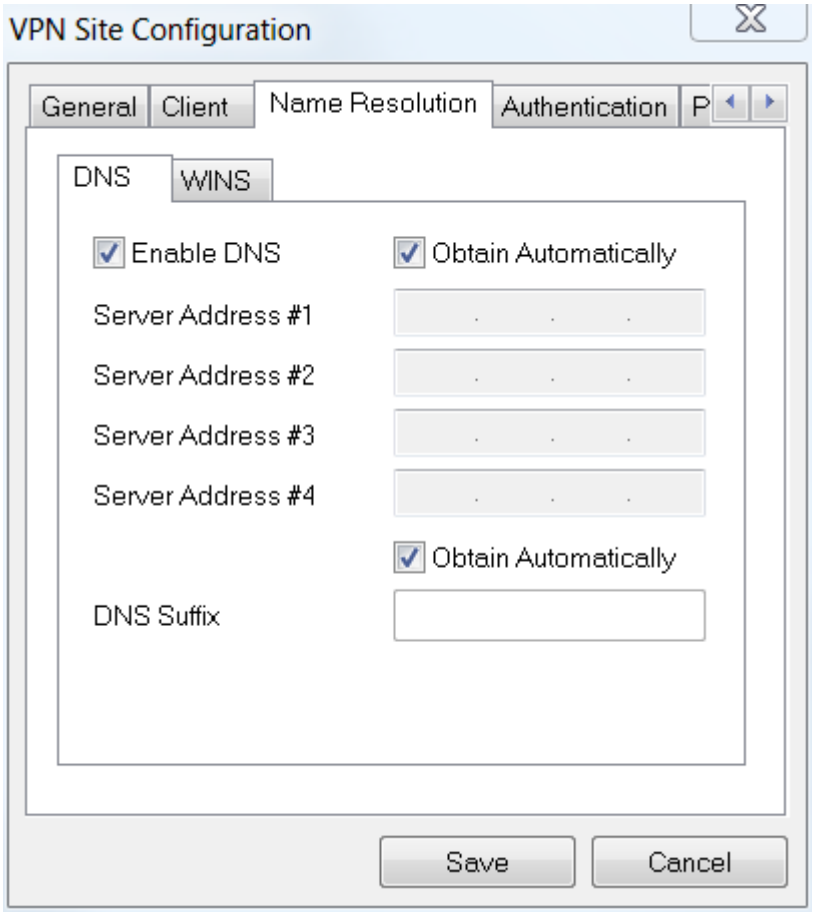
Stap 2

Configuratie van het tabblad **Client** In dit voorbeeld hielden we de standaardinstellingen.



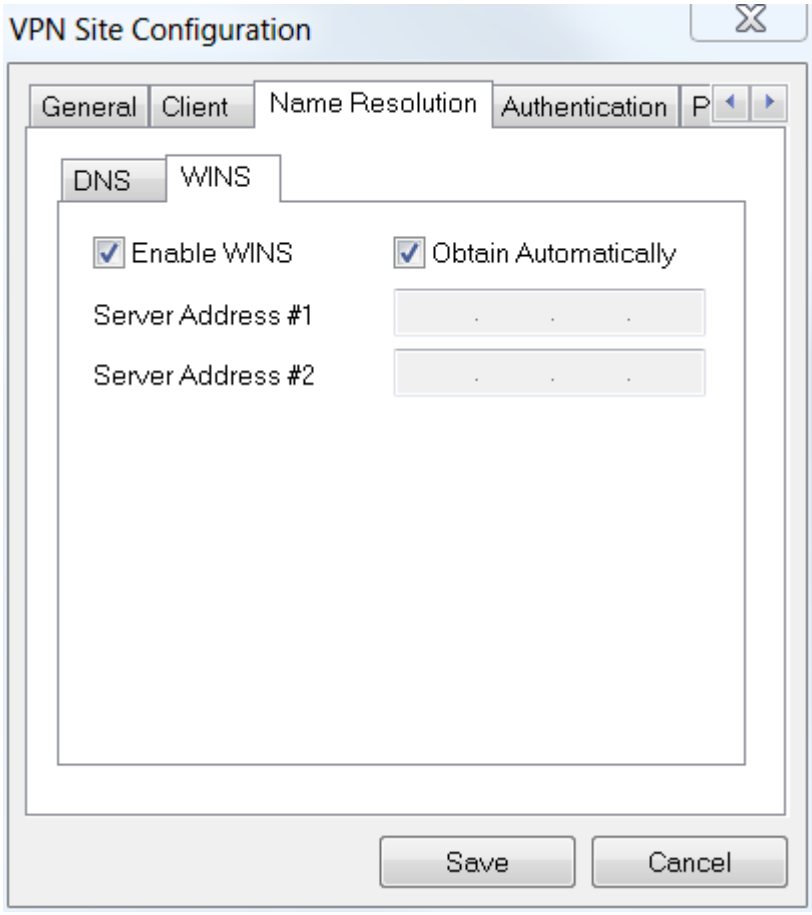
Stap 3

Onder **Name Solutions > DNS**, controleer het **DNS-**vakje **inschakelen** en laat de vakjes **Automatisch** verkrijgen controleren.



Stap 4

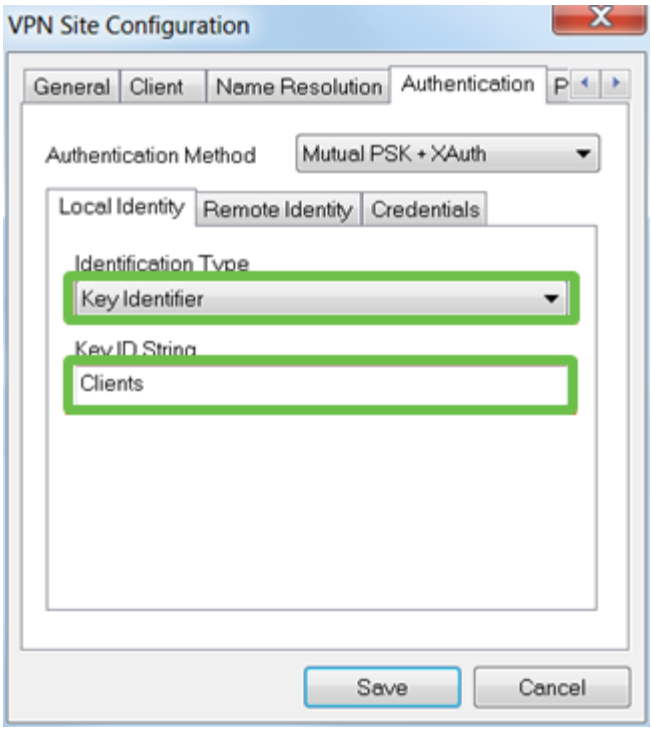
Schakel in het tabblad **Naam** > **WINS** het vakje **WINS** inschakelen in en laat **automatisch** het vakje **Obtain** ingeschakeld.



Stap 5

Klik op **Verificatie > Lokale identiteit**.

- **Identificatietype**: Selecteer **Key Identifier**
- **Belangrijkste ID-string**: Voer de **groepsnaam in** die op de RV345P is ingesteld

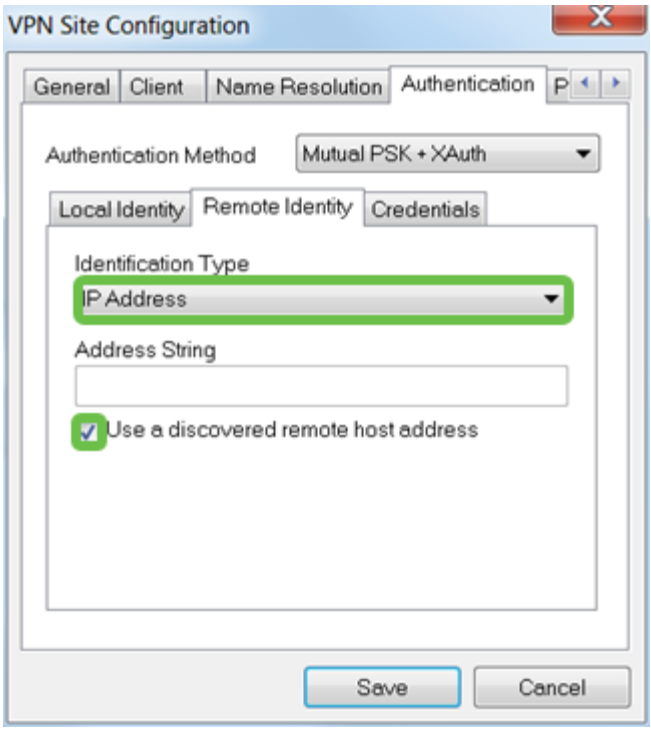


Stap 6

Onder **Verificatie > Remote Identity**. In dit voorbeeld hielden we de

standaardinstellingen.

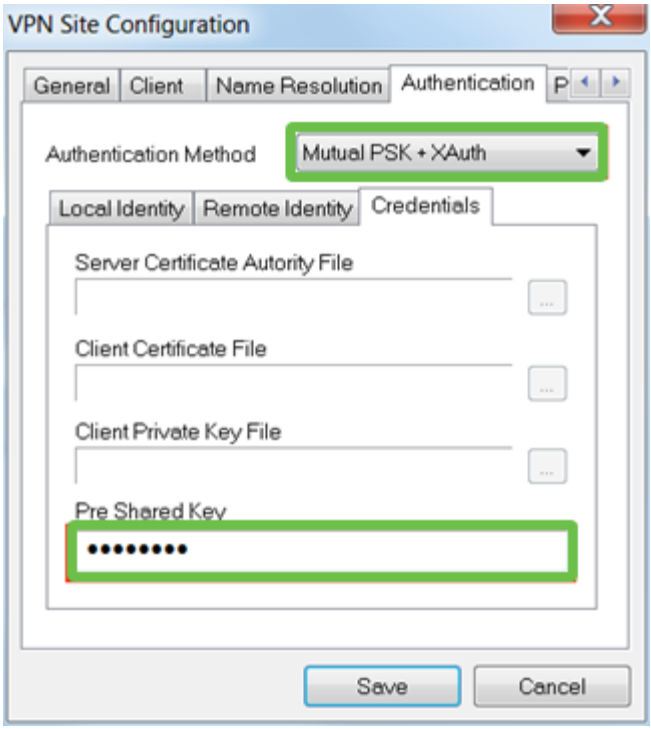
- **Identificatietype**: IP-adres
- **Adres**: <blanco>
- **Gebruik een ontdekt** veld **adres op afstand**: gecontroleerd



Stap 7

Onder **Verificatie > Credentials**, moet u het volgende configureren:

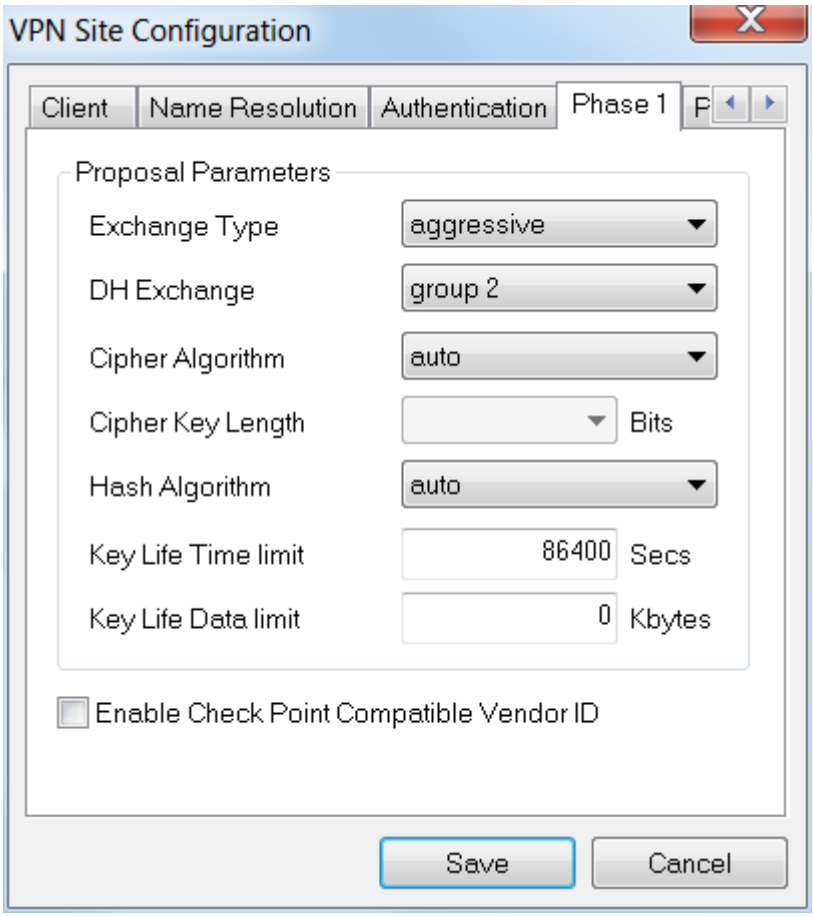
- **Verificatiemethode**: Selecteer **Wederom PSK + XAuth**
- **Vooraf gedeelde sleutel**: Voer de **vooraf gedeelde sleutel in** die is ingesteld in het RV345P-clientprofiel



Stap 8

Zie voor het tabblad **Fase 1**. In dit voorbeeld werden de standaardinstellingen bewaard:

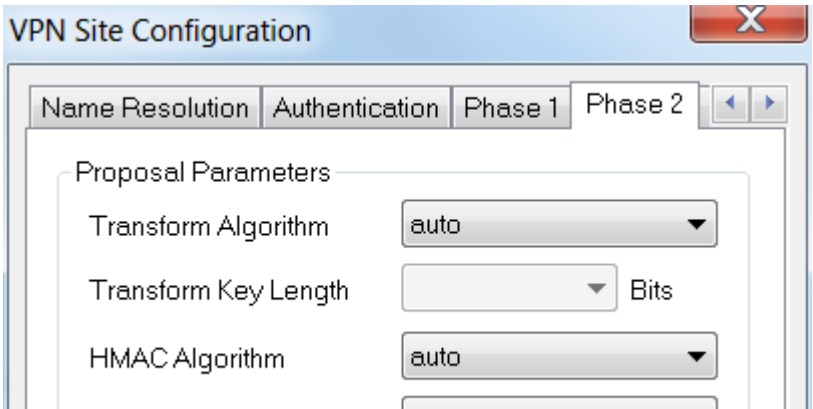
- **Wisseltype:** agressief
- **DH Exchange:** groep 2
- **algoritme gebruiken:** auto
- **Hash Algorithm:** Auto



Stap 9

In dit voorbeeld werden de standaardinstellingen voor het tabblad **Fase 2** gelijk gehouden.

- **Algoritme omzetten:** auto
- **HMAC-algoritme:** Auto
- **PFS exchange:** uitgeschakeld
- **Comprimeer-algoritme:** Uitgeschakeld

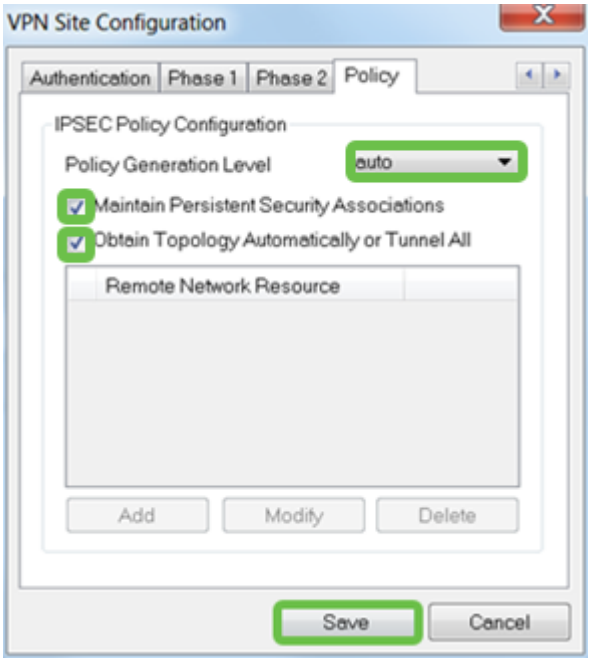


Stap 10

In het voorbeeld Beleidsbeleid hebben we de volgende instellingen gebruikt:

- **Beleidsgeneratieniveau:** Auto
- **Blijvende beveiligingsassociaties behouden:** ingeschakeld
- **Zorg dat de topologie automatisch wordt aangepast of tunneleffect heeft:** ingeschakeld

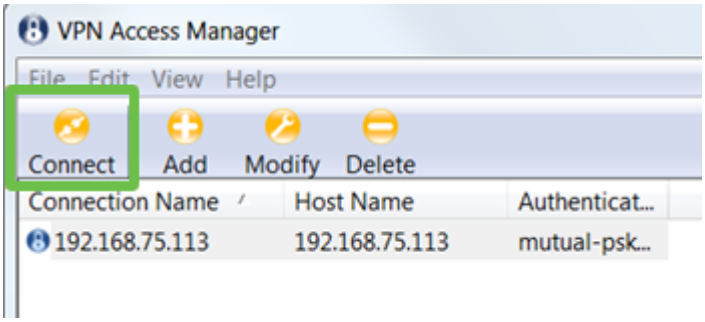
Aangezien we het **Split-Tunneling** hebben ingesteld op de RV345P, hoeven we het hier niet te configureren.



Klik na voltooiing op **Opslaan**.

Stap 11

U bent nu klaar om de verbinding te testen. In *VPN Access Manager* kunt u het verbindingsprofiel markeren en op de knop **Connect** klikken.

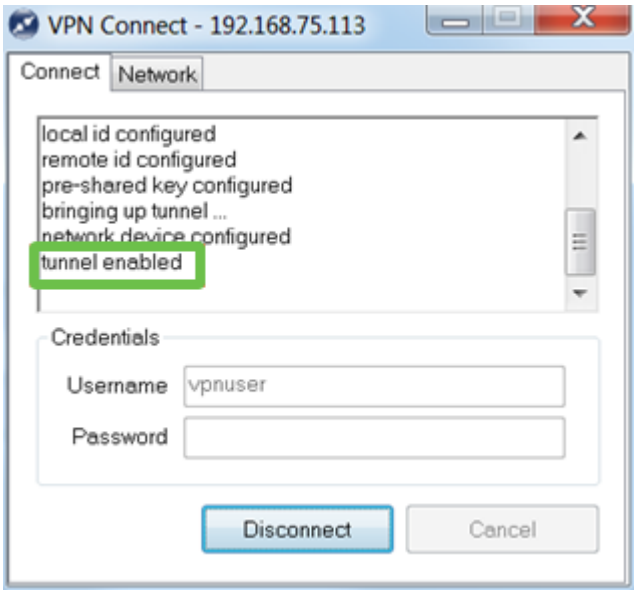


Stap 12

Voer in het venster **VPN Connect** dat nu verschijnt de **gebruikersnaam** en het **wachtwoord in** met behulp van de **gebruikersaccount** die u op RV345P hebt gemaakt (stap 13 en 14). Klik na voltooiing op **Connect**.

Stap 13

Controleer of de tunnel is aangesloten. Je zou **tunnel** moeten zien **ingeschakeld**.



Shrew Soft werd in deze configuratie als voorbeeld gebruikt. Aangezien Shrew Soft geen product van Cisco is, kunt u contact opnemen met deze derde als u technische assistentie nodig hebt.

Andere VPN-opties

Er zijn andere opties voor het gebruik van een VPN. Klik op de volgende koppelingen voor meer informatie:

- Gebruik de GreenBow VPN-client voor een verbinding met RV34x Series router
- Een VPN-client voor Teleworker configureren op de RV34x Series router
- Configuratie van een Point-to-Point Tunneling Protocol (PPTP) Server op de RV34x Series router
- Een IPsec-profiel (Internet Protocol Security) configureren op een RV34x Series router

- L2TP WAN-instellingen configureren op de RV34x-router
- Site-to-Site VPN configureren op de RV34x

Aanvullende configuraties met de RV345P router

VLAN's configureren (optioneel)

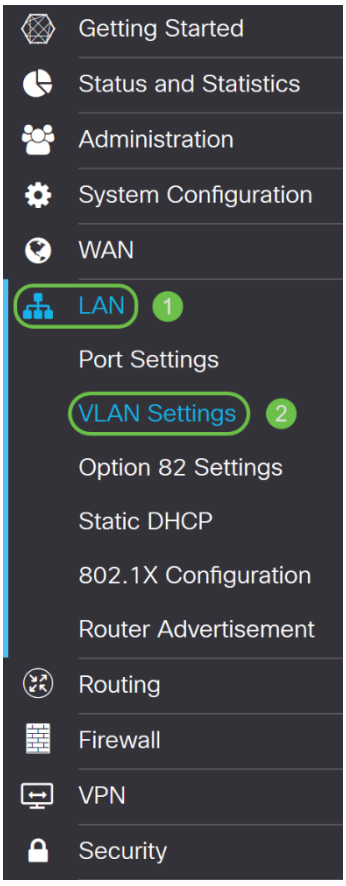
Met een Virtual Local Area Network (VLAN) kunt u een Local Area Network (LAN) logisch segmenteren in verschillende broadcastdomeinen. In scenario's waarbij gevoelige gegevens via een netwerk kunnen worden doorgegeven, kunnen VLAN's worden opgezet om data beter te beveiligen door een broadcast aan een 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.

U kunt naar VLAN-beste praktijken en -tips verwijzen voor extra richtlijnen.

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

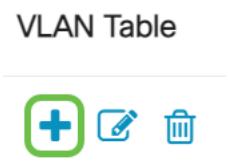
Stap 1

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



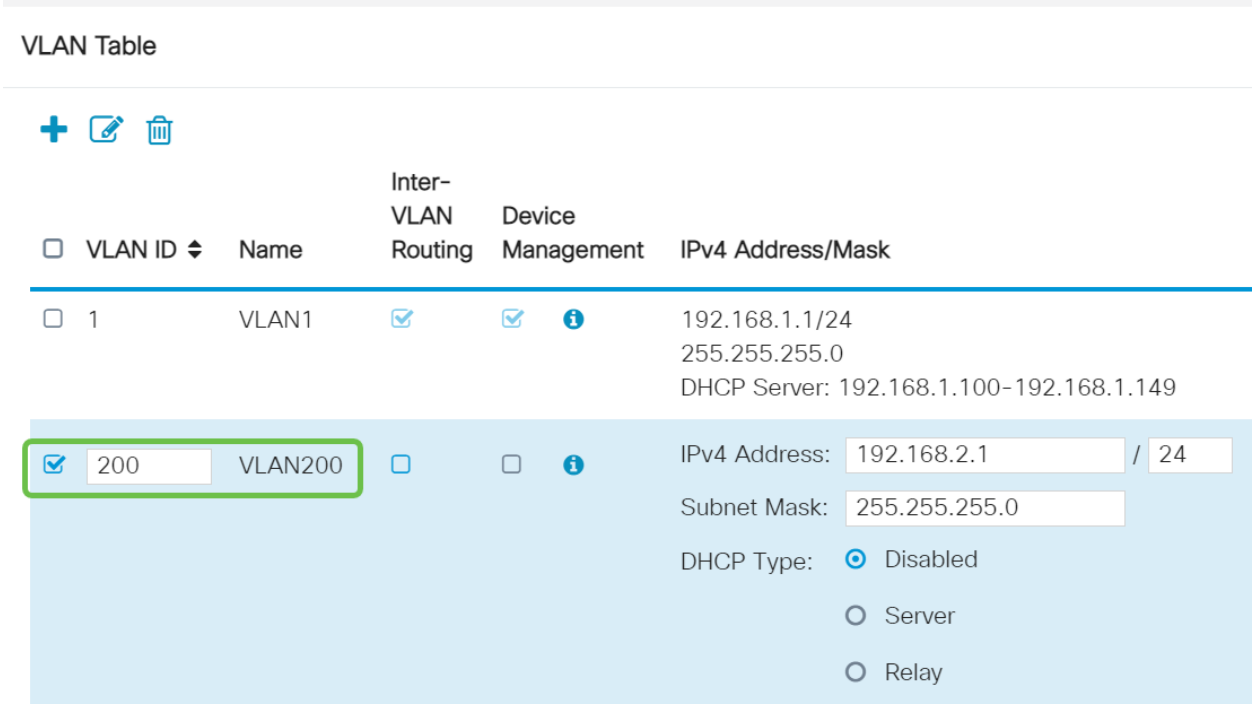
Stap 2

Klik op het **pictogram toevoegen** 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.



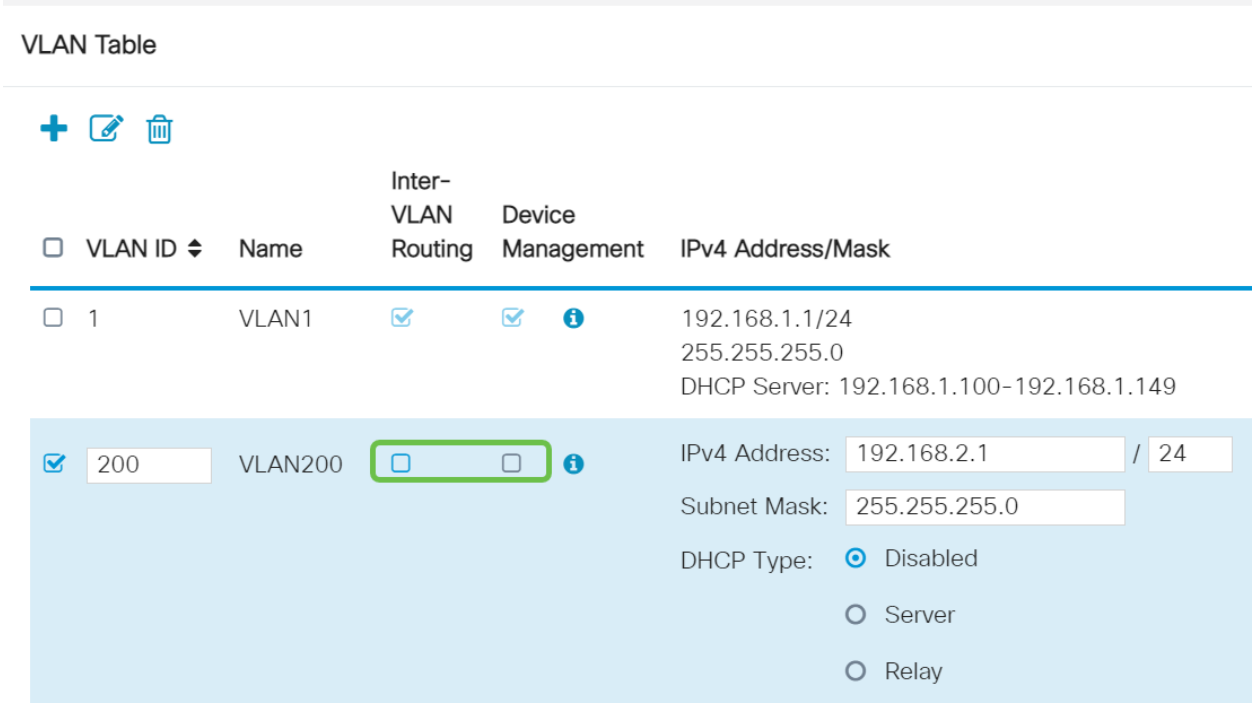
Stap 4

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.

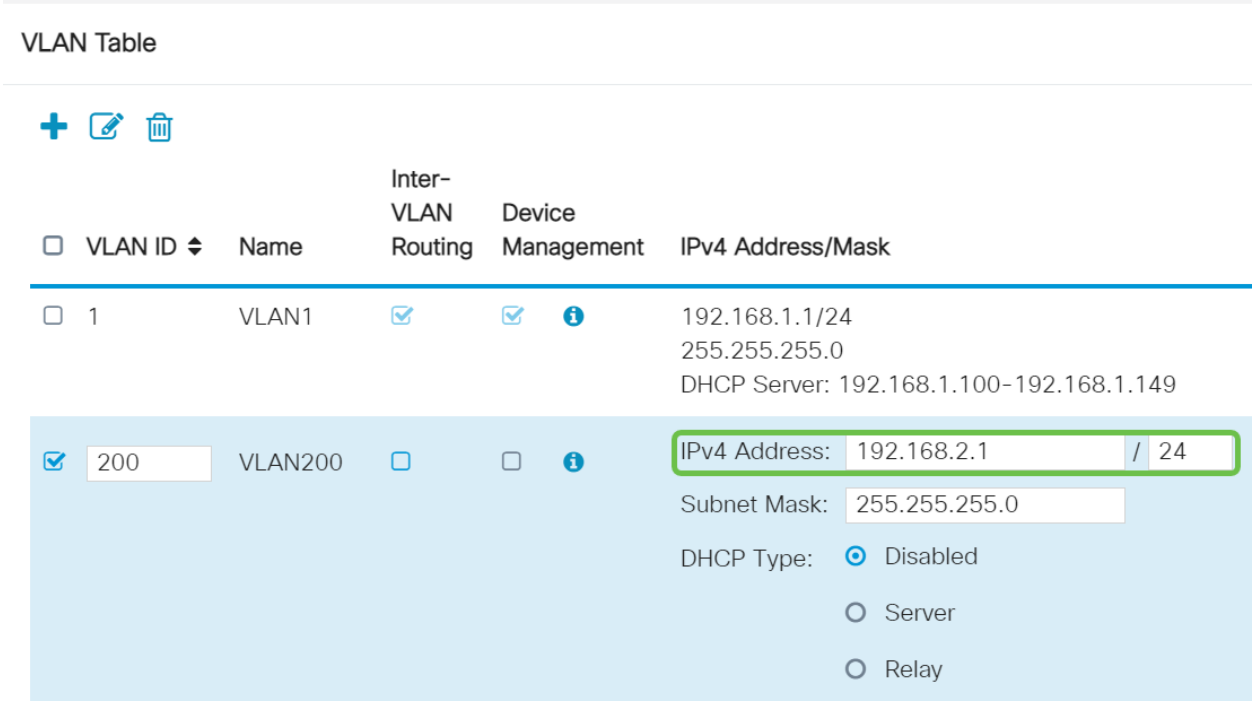
Apparaatbeheer is de software waarmee u uw browser kunt gebruiken om in de Web UI van RV345P van het VLAN te loggen en de RV345P te beheren. Dit moet ook worden uitgeschakeld op Guest-netwerken.

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



Stap 5

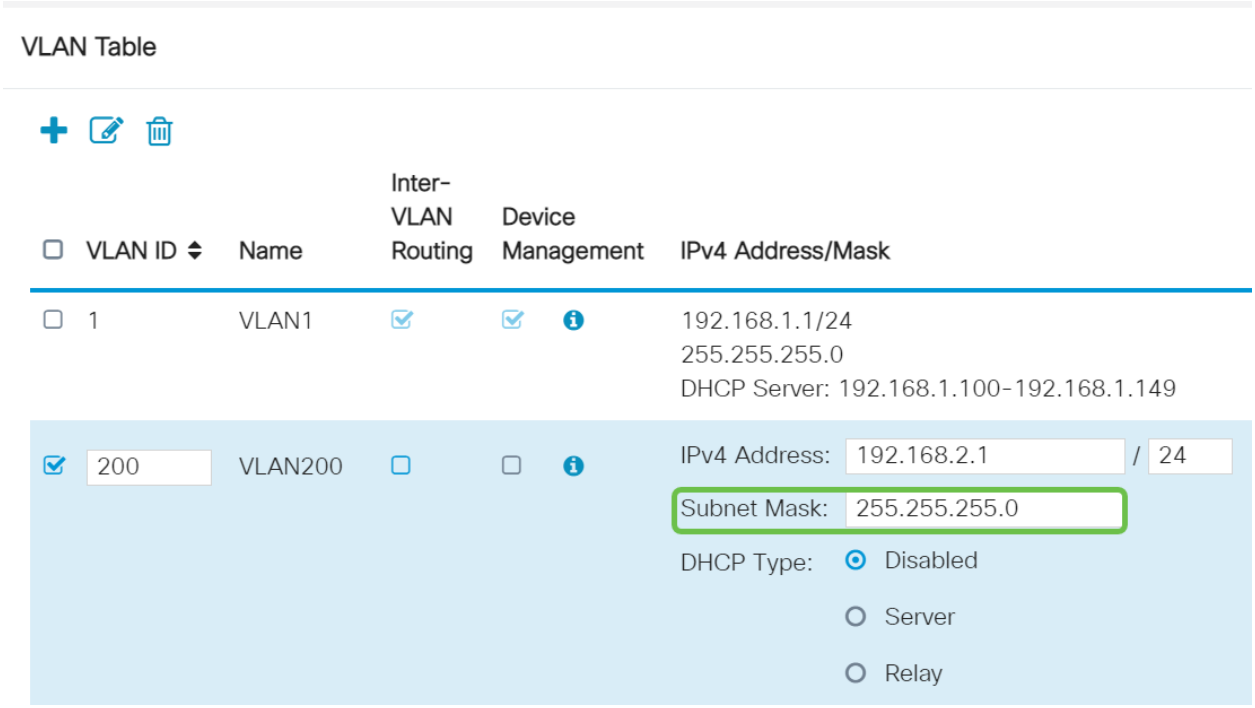
Het particuliere IPv4-adres wordt automatisch ingevuld in het veld *IP-adres*. U kunt dit aanpassen als u kiest. In dit voorbeeld, heeft Subnet 192.168.2.100-192.168.2.149 IP adressen beschikbaar voor DHCP. 192.168.2.1-192.168.2.99 en 192.168.2.150-192.168.2.254 zijn beschikbaar voor statische IP-adressen.



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**.



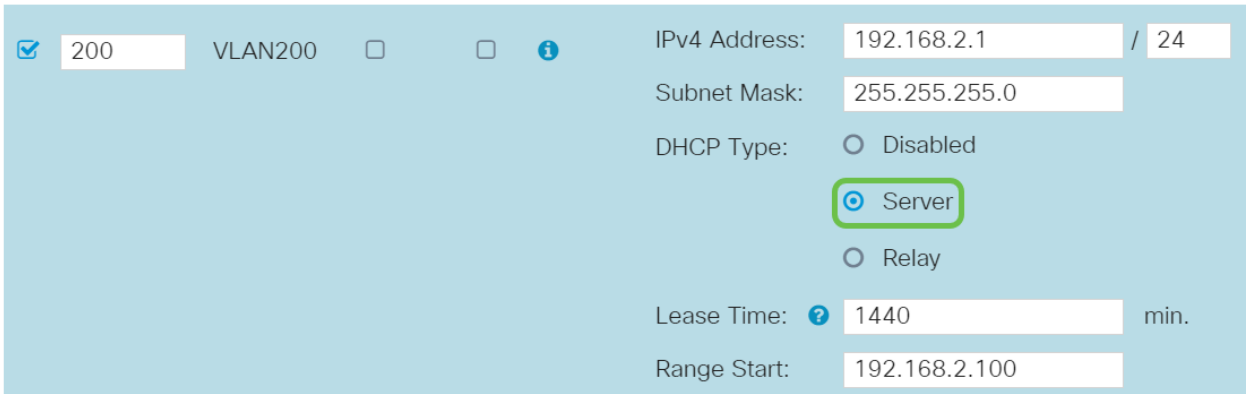
Stap 7

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.

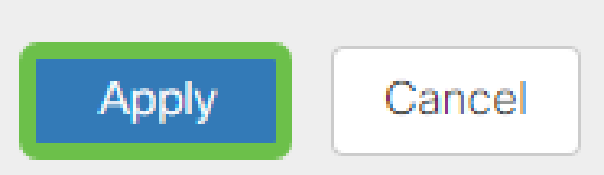
Server - Dit is de meest gebruikte optie.

- 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.



Toewijzen VLAN's aan poorten (optioneel)

16 VLAN's kunnen op RV345P 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 dat een inheems VLAN wordt gelokt. VLAN's die u niet op de romp wilt hebben, moeten worden uitgesloten.

Eén VLAN heeft zijn eigen poort toegewezen:

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

Twee of meer VLAN's die één poort delen:

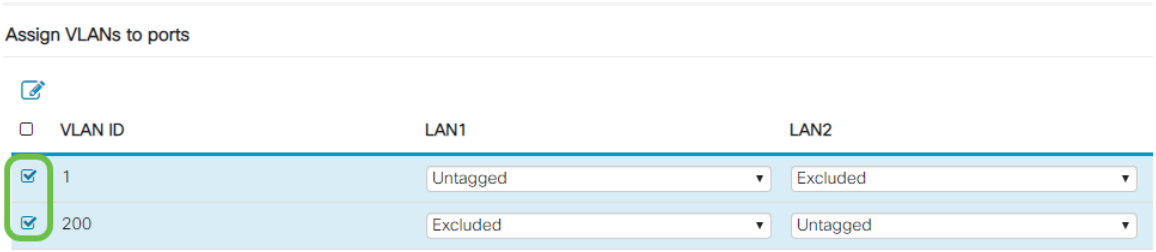
- Wordt beschouwd als een Trunk-poort.
- Eén van de VLAN's kan worden aangeduid als Untagged.
- De rest van de VLAN's die deel uitmaken van de Trunk-poort moet van een label zijn voorzien.
- VLAN's die geen deel uitmaken van de Trunk-poort moeten van een etiket worden voorzien dat voor die poort is uitgesloten.

In dit voorbeeld zijn er geen stammen.

Stap 1

Selecteer de *VLAN-ID's* die u wilt bewerken.

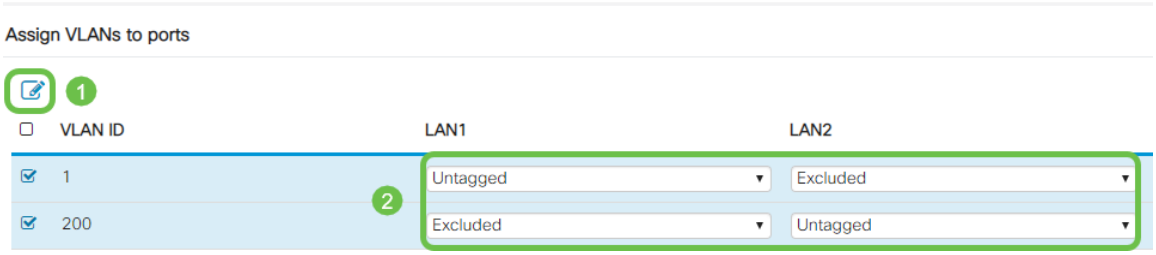
In dit voorbeeld, hebben we *VLAN 1* en *VLAN 200* geselecteerd.



Stap 2

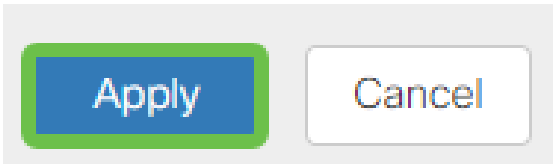
Klik op **Bewerken** om een VLAN aan een LAN poort toe te wijzen en specificeer elke instelling als *Bijgesneden*, *niet gelabeld* of *uitgesloten*.

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 3

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



U moet nu met succes een nieuw VLAN en geconfigureerd VLAN's in poorten op RV345P hebben gemaakt. 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.

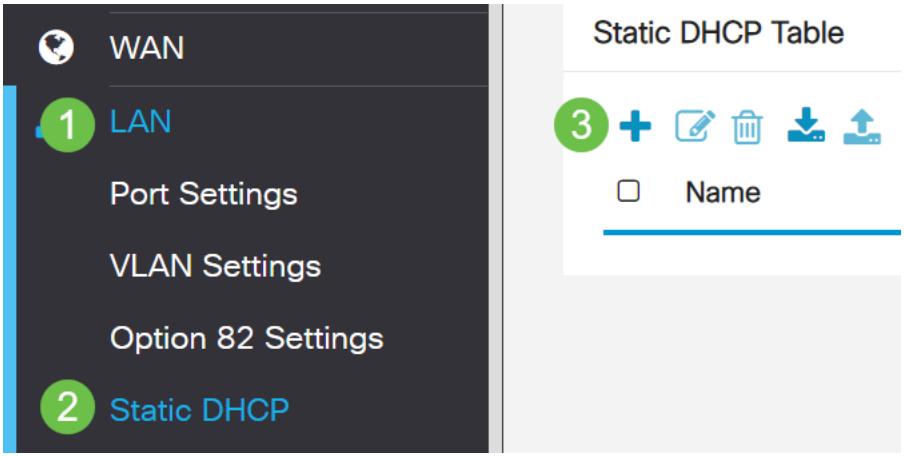
Voeg een statische IP toe (optioneel)

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.

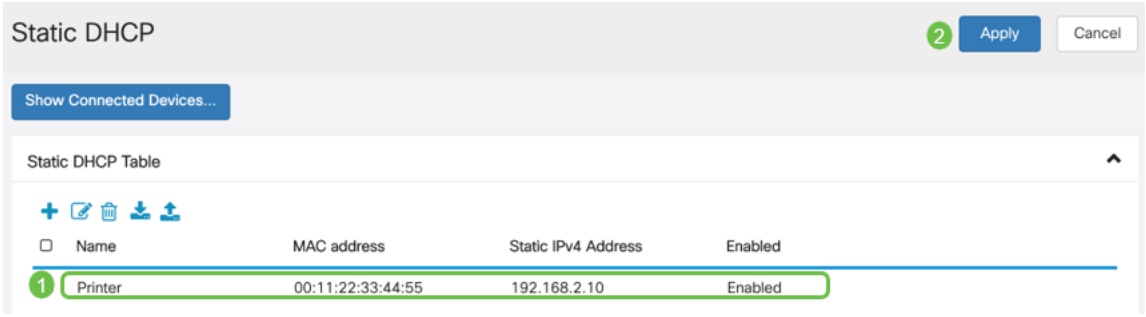
Stap 1

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.



Certificaten beheren (optioneel)

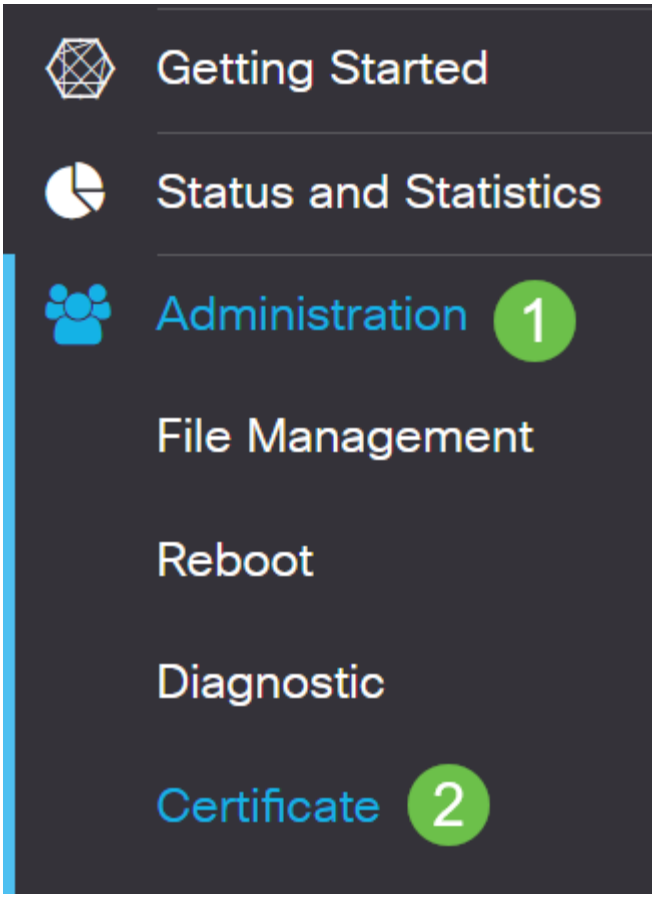
Een digitaal certificaat certificeert de eigendom van een openbare sleutel door het genoemde onderwerp van het certificaat. Dit stelt betrouwbare partijen in staat om afhankelijk te zijn van handtekeningen of beweringen van de privé-sleutel die overeenkomt met de openbare sleutel die gecertificeerd is. Een router kan een zichzelf ondertekend certificaat, een certificaat produceren dat door een netwerkbeheerder wordt gemaakt. Het kan ook verzoeken aan de certificaatautoriteiten (CA) zenden om een digitaal identiteitsbewijs aan te vragen. Het is belangrijk dat er een rechtmatig certificaat is van een verzoek van derden.

Voor de echtheidscontrole wordt een certificeringsinstantie (CA) gebruikt. Certificaten kunnen worden aangeschaft op elk aantal locaties van derden. Het is een officiële manier om te bewijzen dat je site veilig is. De CA is in wezen een vertrouwde bron die verifieert dat u een legitiem bedrijf bent en kan worden vertrouwd. Afhankelijk van uw behoeften, een certificaat tegen minimale kosten. U wordt uitgecheckt door de CA en zodra ze uw informatie hebben geverifieerd, geven ze het certificaat aan u af. Dit certificaat kan als bestand op uw computer worden gedownload. U kunt dan naar uw router (of VPN-server) gaan en het daar uploaden.

CSR/certificaat genereren

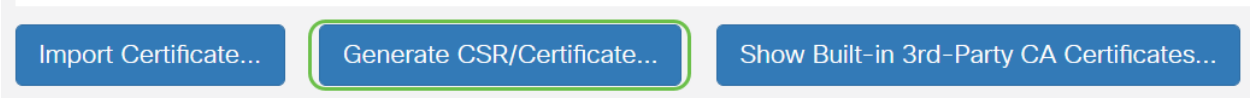
Stap 1

Meld u aan bij het webgebaseerde hulpprogramma van de router en kies **Beheer > Certificaat**.



Stap 2

Klik op **Generate CSR/certificaat**. U wordt naar de pagina Generate CSR/certificaatpagina gebracht.



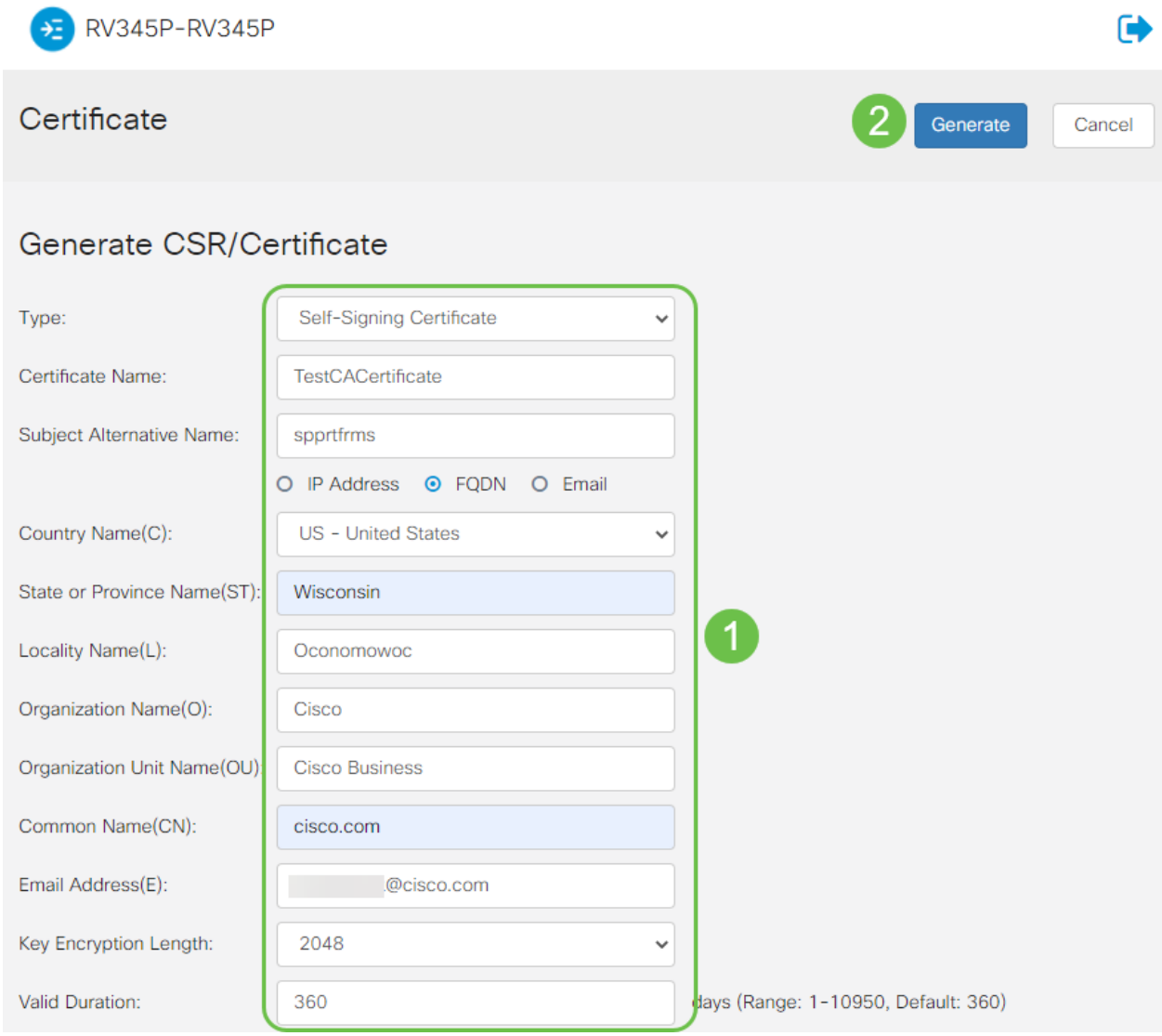
Stap 3

Vul de vakjes in met het volgende:

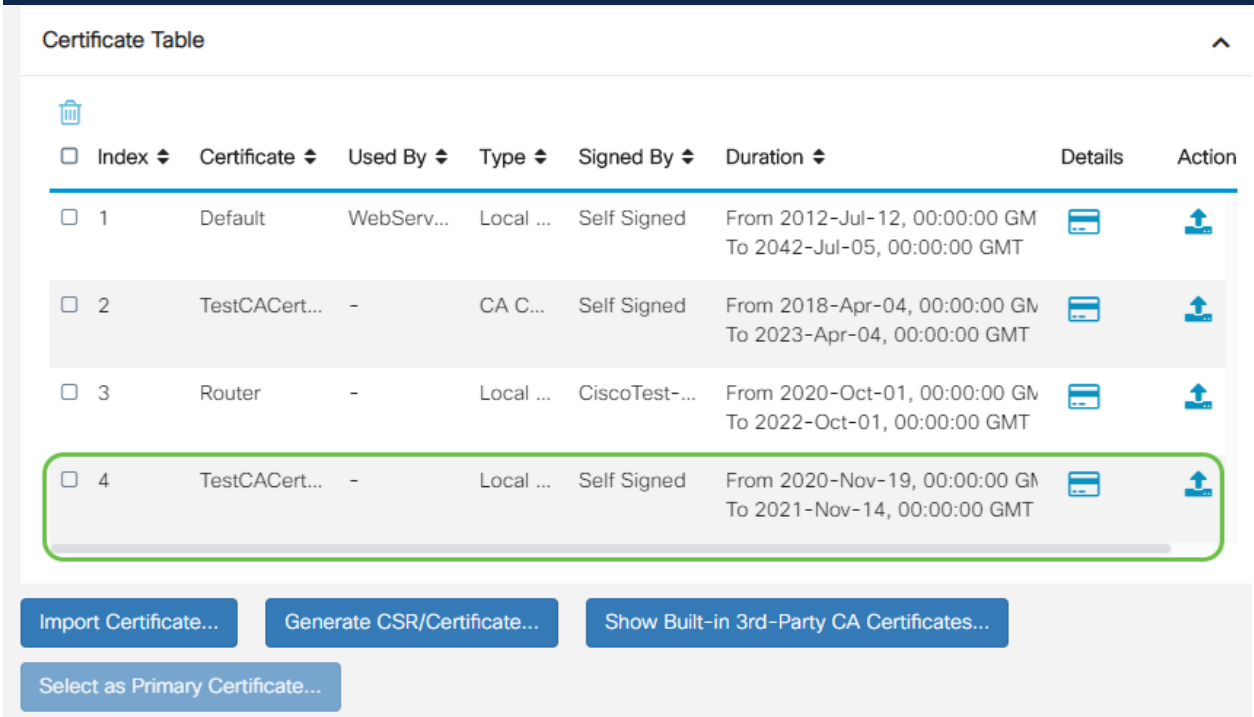
- Kies het juiste type certificaat
  - Zelfvormend certificaat — Dit is een Secure Socket Layer (SSL) certificaat dat door zijn eigen schepper is ondertekend. Dit certificaat is minder betrouwbaar, omdat het niet kan worden geannuleerd als de privétoets op een of andere manier door een aanvaller wordt gecompromitteerd.
  - Aanvraag van gecertificeerde handtekening — Dit is een openbare sleutelinfrastructuur (PKI) die naar de certificeringsinstantie wordt gestuurd om een digitaal identiteitsbewijs aan te vragen. Het is veiliger dan door zichzelf getekend te worden, omdat de privé-sleutel geheim gehouden wordt.
- Voer in het veld Naam van het certificaat een naam in voor uw certificaat om het verzoek te identificeren. Dit veld kan niet leeg zijn en geen spaties en speciale tekens bevatten.

- (Optioneel) Klik onder het gebied Onderwerp Alternative Name op een radioknop. De opties zijn:
    - IP-adres — Voer een IP-adres (Internet Protocol) in
    - FQDN - Voer een volledig gekwalificeerde domeinnaam in (FQDN)
    - E-mail — Voer een e-mailadres in

- Voer in het veld Alternatieve naam in.
- Kies een landennaam waarin uw organisatie wettelijk is geregistreerd in de vervolgkeuzelijst Landnaam.
- Voer een naam of afkorting in van de staat, provincie, regio of gebied waar uw organisatie zich bevindt in het veld Naam of provincie (ST).
- Voer een naam in van de locatie of de stad waarin uw organisatie is geregistreerd of zich in het veld Naam van de locatie bevindt.
- Voer een naam in waaronder uw bedrijf wettelijk is geregistreerd. Als u zich inschrijft als een klein bedrijf of eenmansbedrijf, specificeert u de naam van de certificaataanvrager in het veld Naam van de organisatie. Speciale tekens kunnen niet worden gebruikt.
- Voer een naam in het veld Naam van de organisatie in om onderscheid te maken tussen splitsingen binnen een organisatie.
- Voer een naam in het veld Naam in. Deze naam moet de volledig gekwalificeerde domeinnaam zijn van de website waarvoor u het certificaat gebruikt.
- Voer het e-mailadres in van de persoon die het certificaat wil genereren.
- Kies een belangrijke lengte in de vervolgkeuzelijst Lengte versleutelen. De opties zijn 512, 1024 en 2048. Hoe groter de sleutellengte, hoe veiliger het certificaat.
- Voer in het veld Geldige duur het aantal dagen in dat het certificaat geldig is. De standaard is 360.
- Klik op **Generate**.



Het gegenereerde certificaat moet nu in de certificaattabel worden weergegeven.

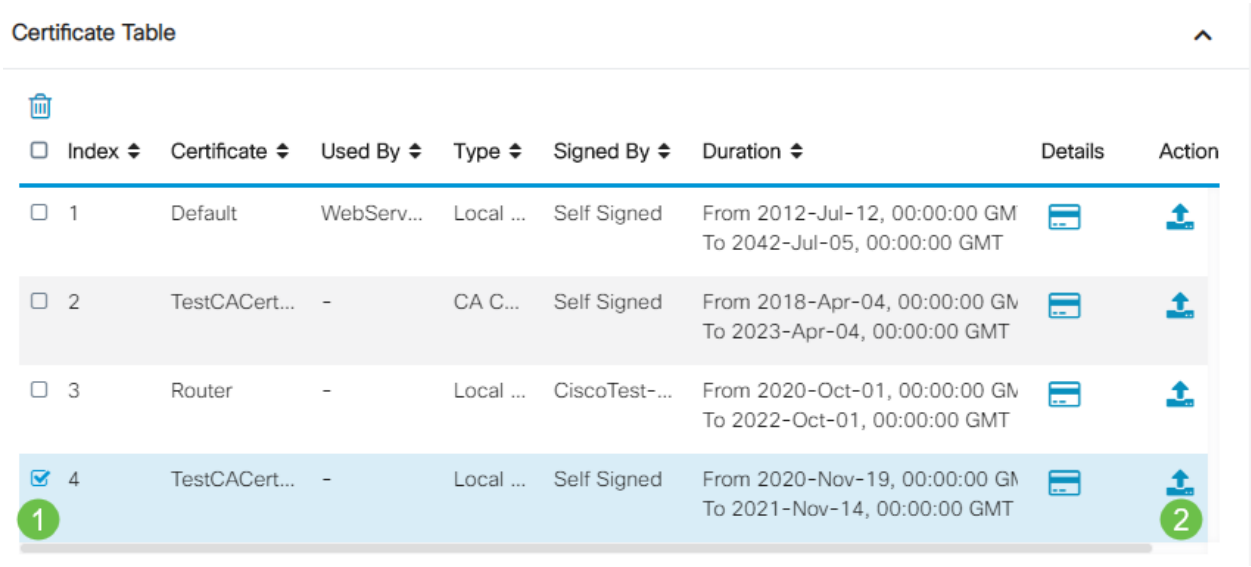


U moet nu met succes een certificaat op de RV345P router hebben gemaakt.

Een certificaat exporteren

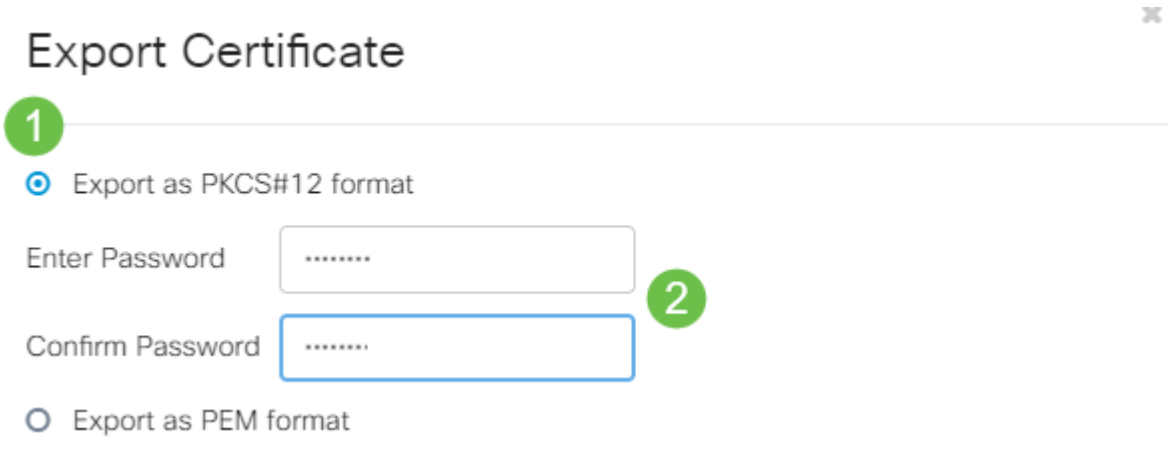
Stap 1

In de tabel Certificaat controleert u het vakje van het certificaat dat u wilt exporteren en klikt u op het **pictogram Exporteren**.



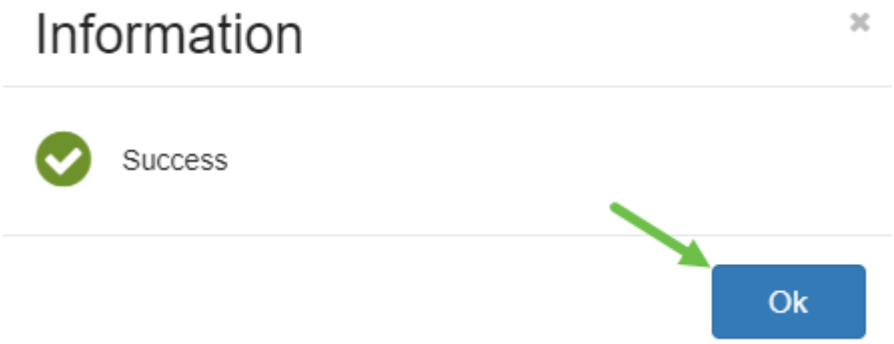
Stap 2

- Klik op een bestandsindeling voor het exporteren van het certificaat. De opties zijn:
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 is een geëxporteerd certificaat dat een .p12-extensie bevat. Er wordt een wachtwoord vereist om het bestand te versleutelen om het te beveiligen wanneer het wordt geëxporteerd, geïmporteerd en verwijderd.
  - PEM — Privacy Enhanced Mail (PEM) wordt vaak gebruikt voor webservers om gemakkelijk te kunnen worden vertaald in leesbare gegevens door gebruik te maken van een eenvoudige teksteditor zoals notedop.
- Als u PEM hebt gekozen, klikt u op **Exporteren**.
- Typ een wachtwoord om het bestand te beveiligen dat moet worden geëxporteerd in het veld Wachtwoord invoeren.
- Voer het wachtwoord opnieuw in het veld Wachtwoord bevestigen.
- In het gedeelte Bestemming selecteren is de PC geselecteerd en is de enige optie die momenteel beschikbaar is.
- Klik op **Exporteren**.



Stap 3

Onder de knop Downloaden verschijnt een bericht met het succes van de download. Er wordt een bestand in uw browser gedownload. Klik op OK.

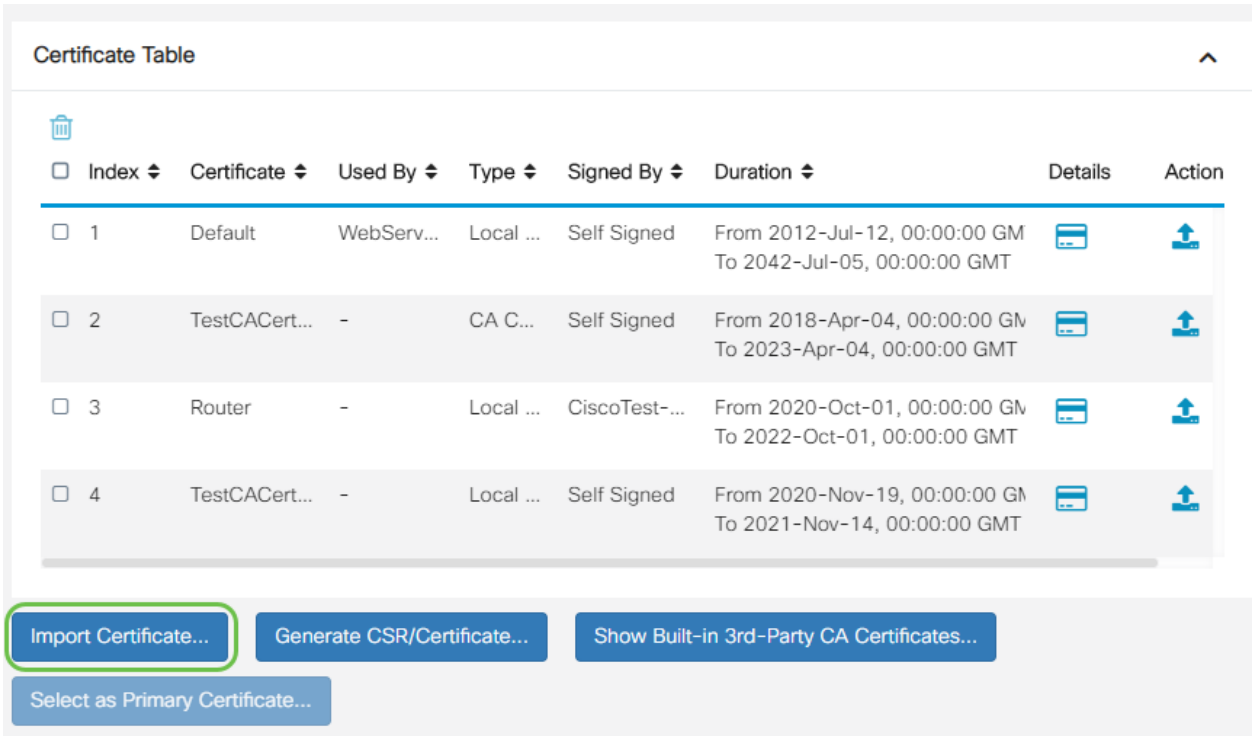


U dient nu een certificaat voor de RV345P Series router te hebben geëxporteerd.

Een certificaat importeren

Stap 1

Klik op **importcertificaat...**.

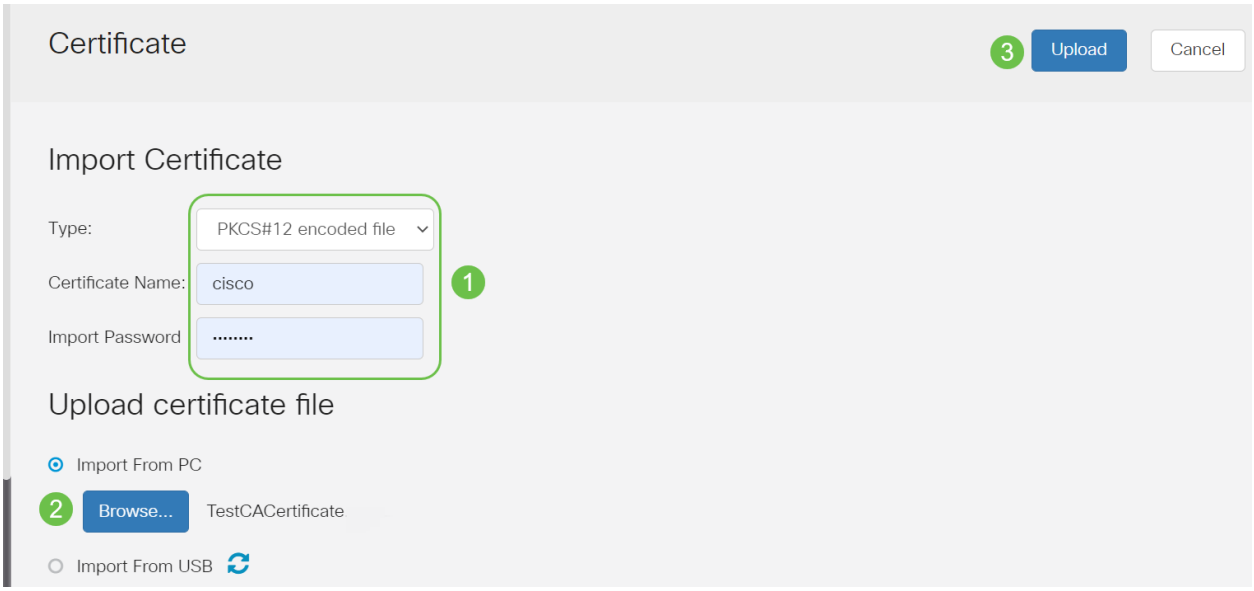


Stap 2

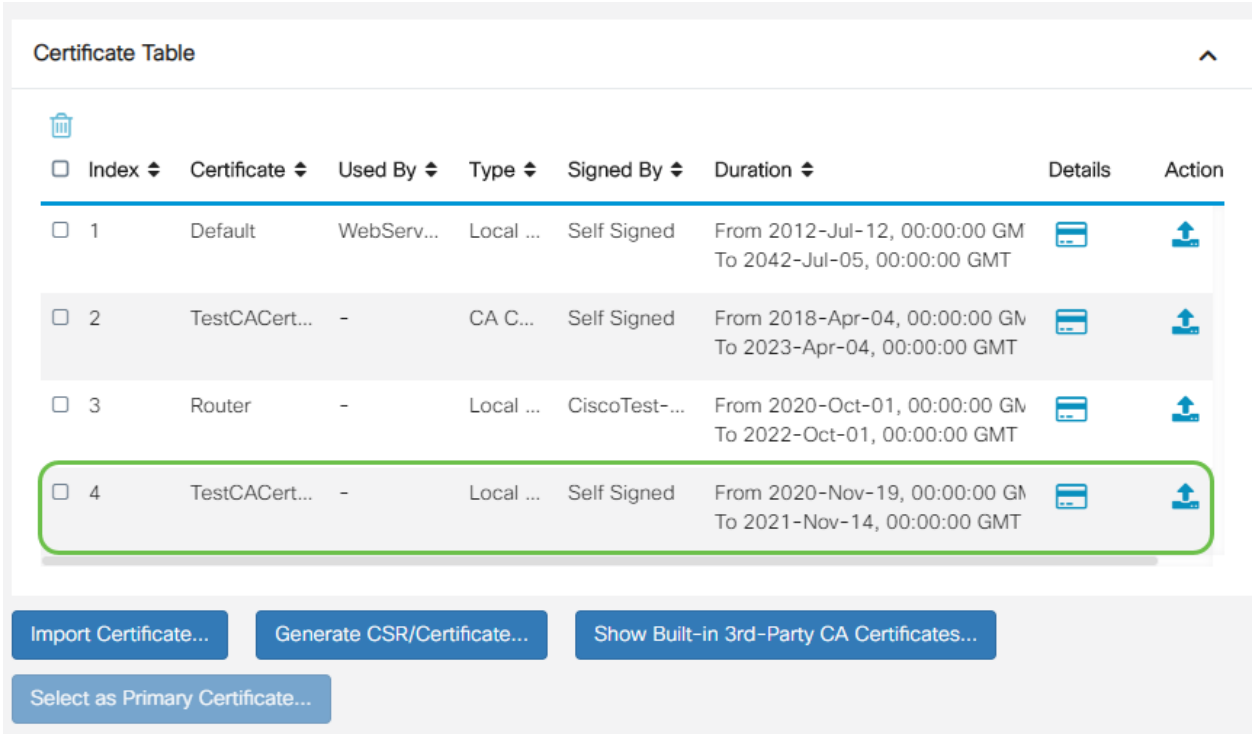
- Selecteer het type certificaat dat u wilt importeren in de vervolgkeuzelijst. De opties zijn:
  - Lokaal certificaat — een certificaat dat op de router gegenereerd is.
  - CA-certificaat — een certificaat dat is gecertificeerd door een betrouwbare derde die heeft bevestigd dat de informatie in het certificaat juist is.
  - PKCS #12 Encoded file — Public Key Cryptography Standards (PKCS) #12 is een formaat voor het opslaan van een servercertificaat.
- Typ een naam voor het certificaat in het veld Naam certificaat.

- Als PKCS #12 is geselecteerd, typt u een wachtwoord voor het bestand in het veld Wachtwoord voor importeren. Anders overslaan naar Stap 3.
- Klik op een bron om het certificaat te importeren. De opties zijn:
    - Importeren op PC
    - Importeren op USB

- Als de router een USB-station niet detecteert, wordt de optie Importeren uit USB-camera uitgevoerd.
- Als u Importeren uit USB hebt geselecteerd en uw USB-apparaat niet door de router wordt herkend, klikt u op Vernieuwen.
- Klik op de knop Bestand kiezen en kies het gewenste bestand.
- Klik op **Upload**.



Nadat dit is gelukt, wordt u automatisch naar de hoofdpagina van het certificaat verwezen. De certificaattabel wordt ingevuld met het onlangs ingevoerde certificaat.



U moet nu met succes een certificaat op uw RV345P router hebben geïmporteerd.

Een mobiel netwerk configureren met behulp van een dongle en een RV345P Series router (optioneel)

Misschien wilt u een back-upnetwerk configureren met behulp van een dongle en uw RV345P-router. Als dit probleem zich voordoet, kunt u lezen Een mobiel netwerk configureren met behulp van een ongle en een RV34x Series router.

Gefeliciteerd, hebt u de configuratie van uw RV345P router voltooid! U zult 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 RV345P. De eerste 4 poorten op de RV345P 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 RV345x-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.

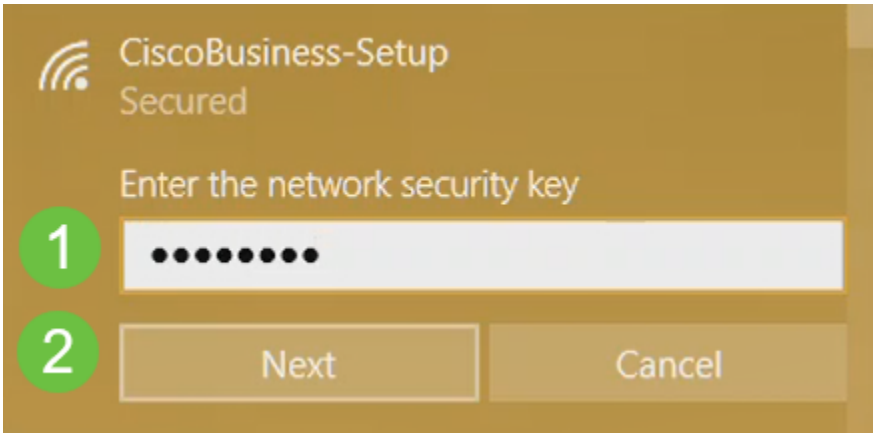
Stap 1

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.

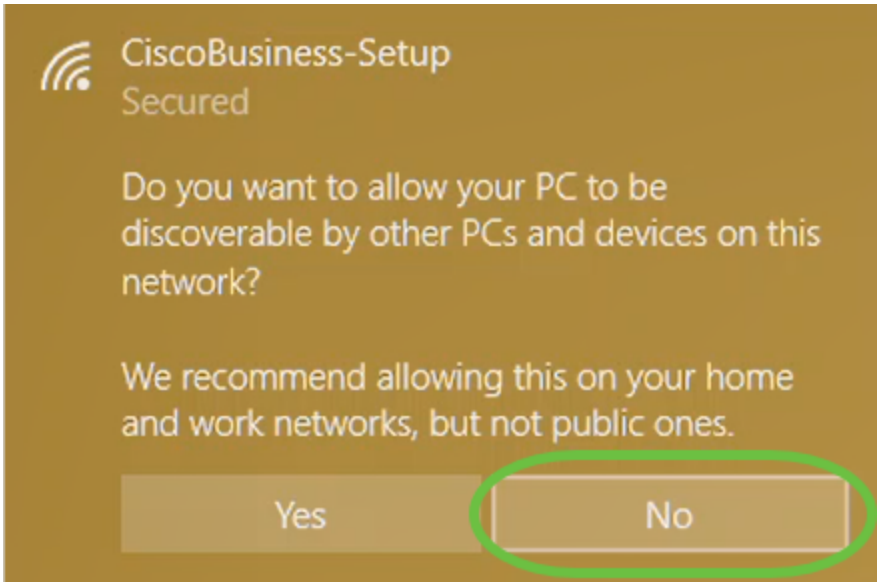
Stap 2

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



Stap 3

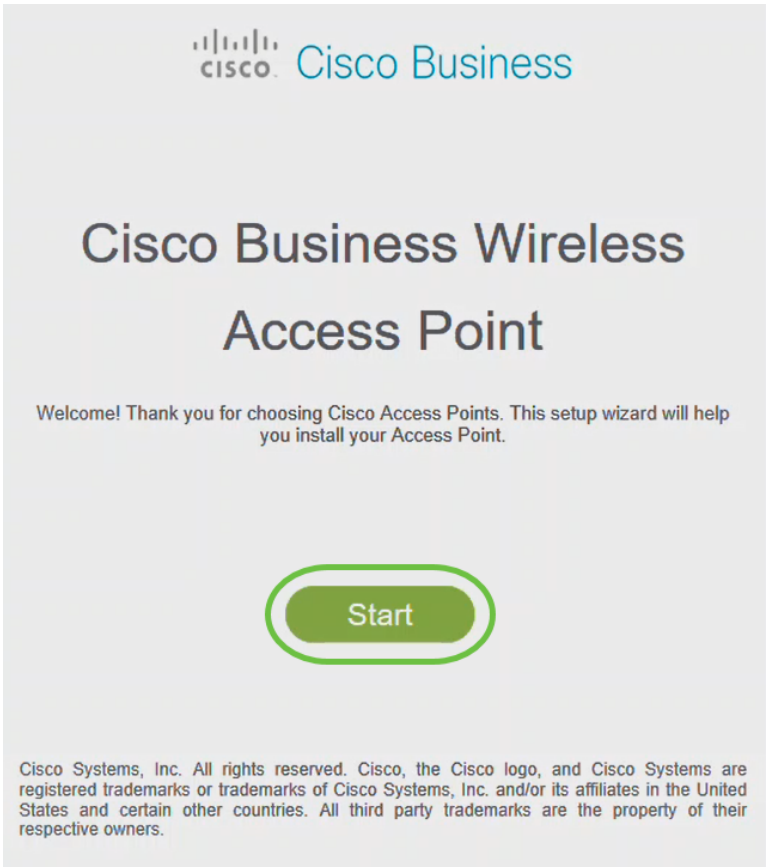
U krijgt het volgende scherm. Aangezien u slechts één apparaat tegelijkertijd kunt configureren klikt u op **Nee**.



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.

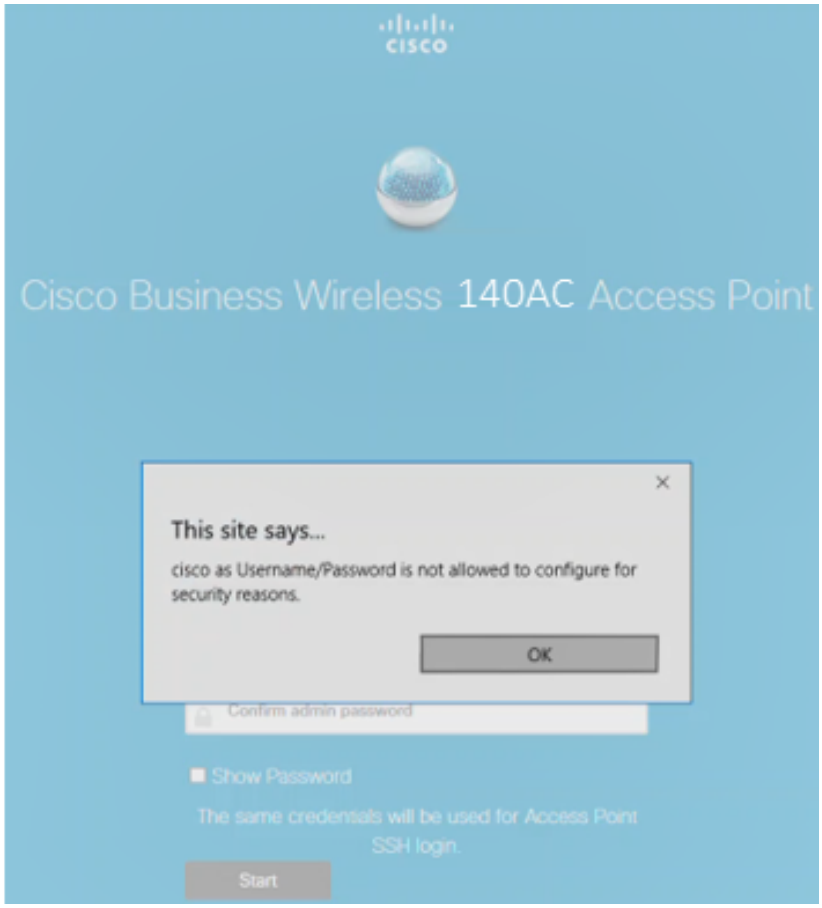
Stap 5

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**.

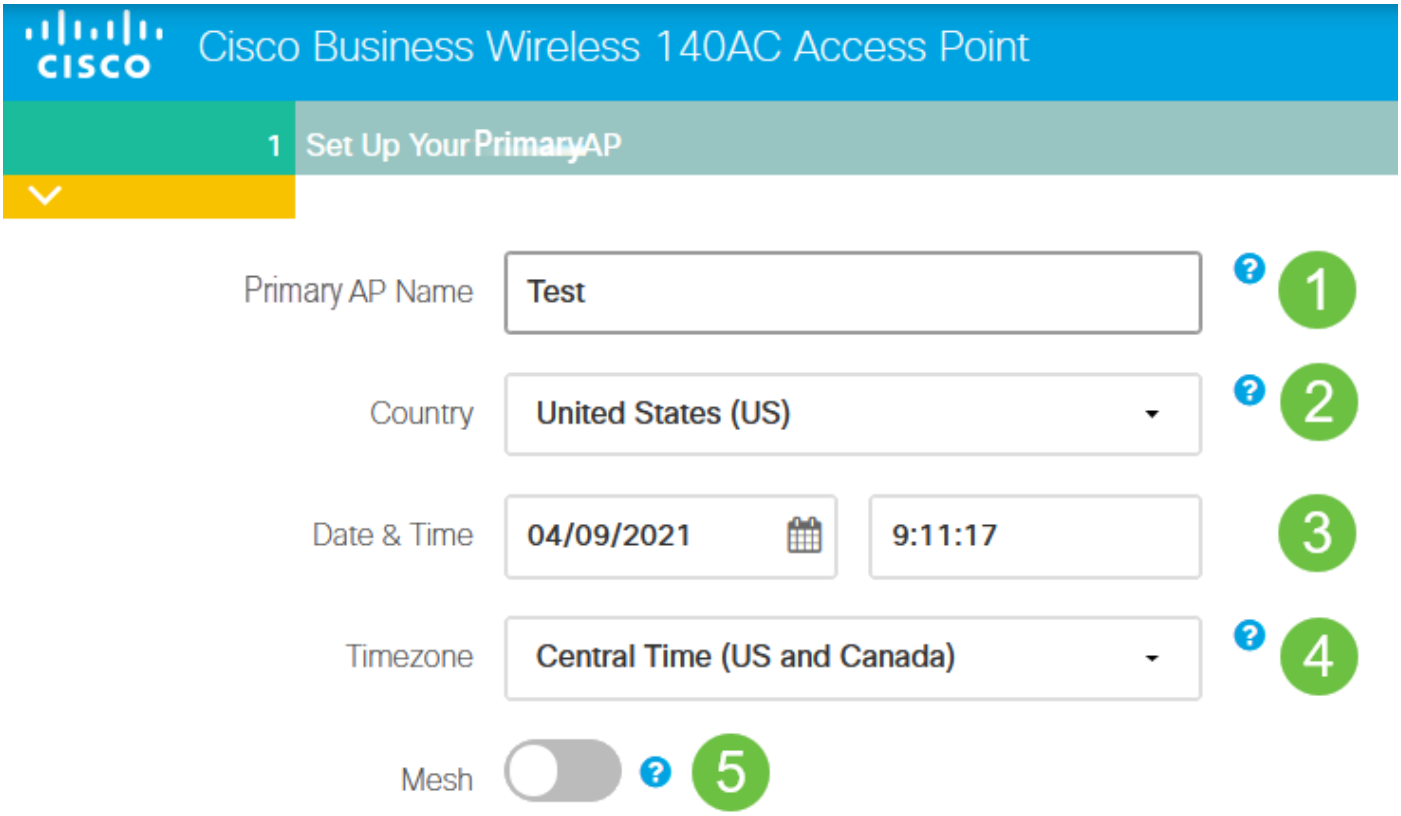
Gebruik *cisco* niet, of variaties ervan in de gebruikers- of wachtwoordvelden. Als u dit wel doet, ontvangt u een foutmelding zoals hieronder wordt weergegeven.



Stap 6

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

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



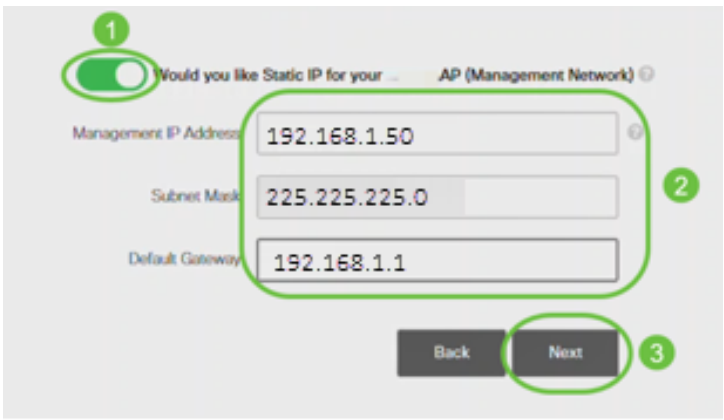
mesh zou alleen ingeschakeld moeten worden als u een netwerk wilt maken. Standaard is het uitgeschakeld.

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**.



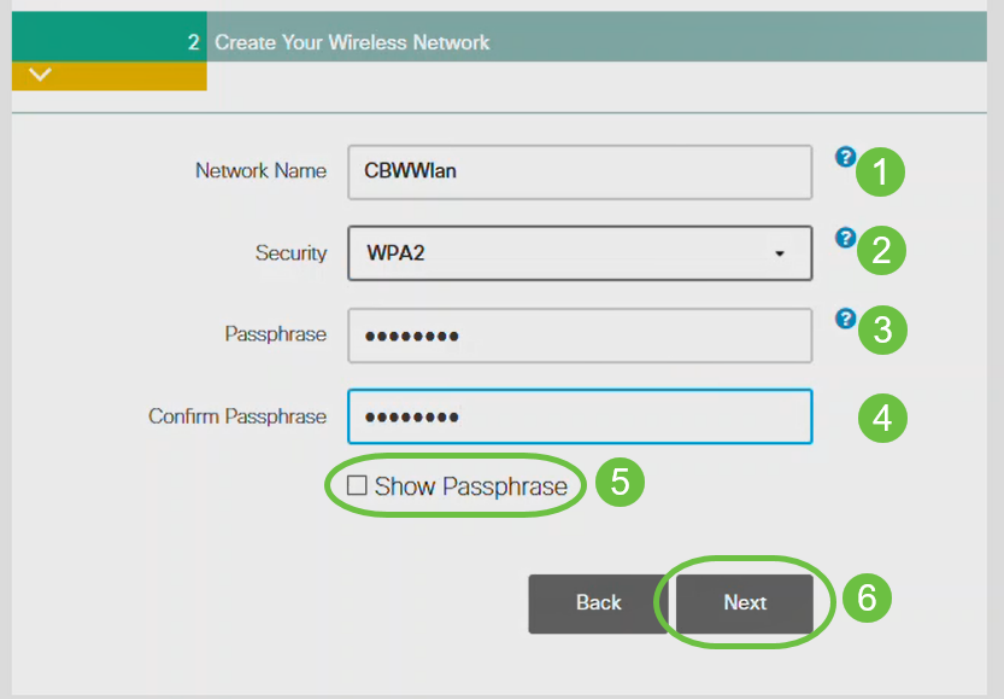
Deze optie is standaard uitgeschakeld.

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.

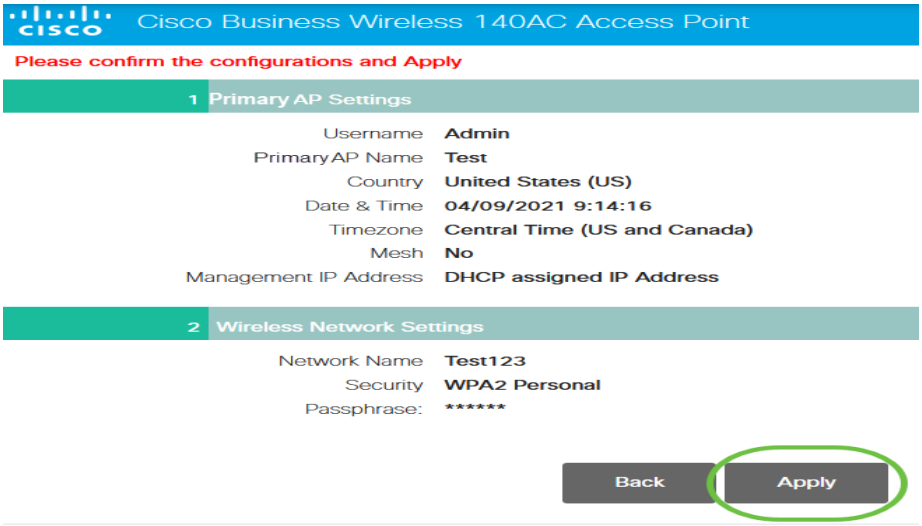
Klik op **Volgende**.



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

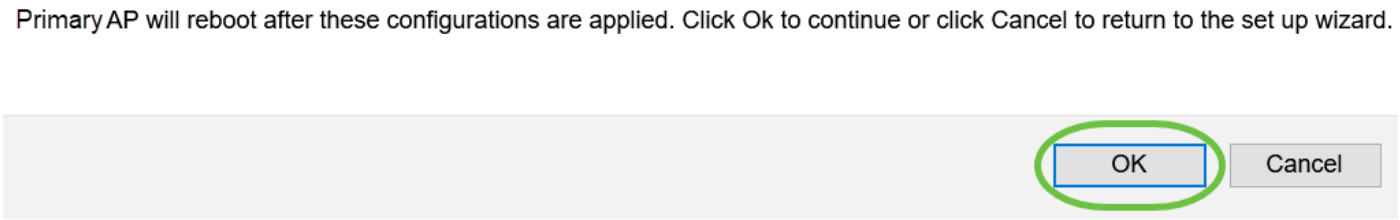
Stap 9

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

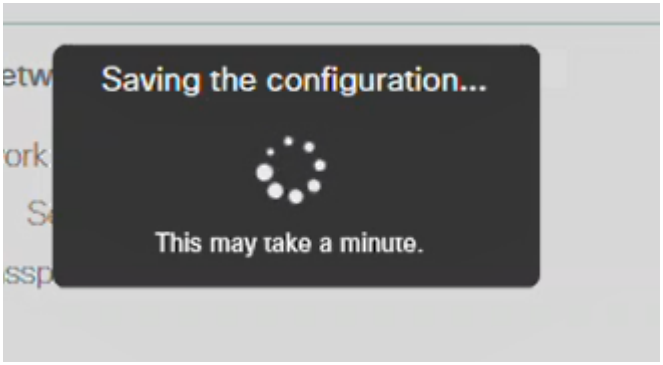


Stap 10

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.

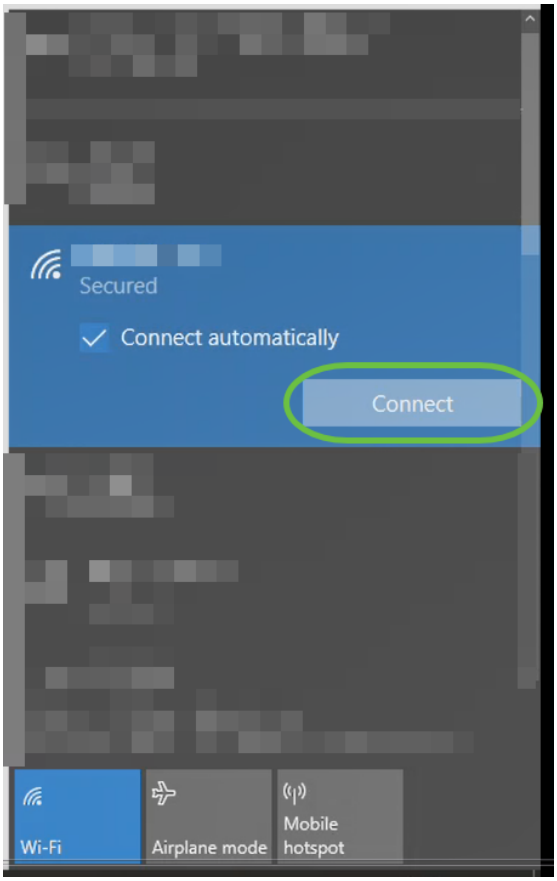


Tijdens het opnieuw opstarten, gaat de LED in het access point door meerdere kleurpatronen. Wanneer de LED groen knippert, gaat u naar de volgende stap. Als de LED niet voorbij het rode knipperpatroon komt, geeft dit aan dat er geen DHCP-server in uw netwerk is. Zorg ervoor dat AP op een switch of een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

Stap 11

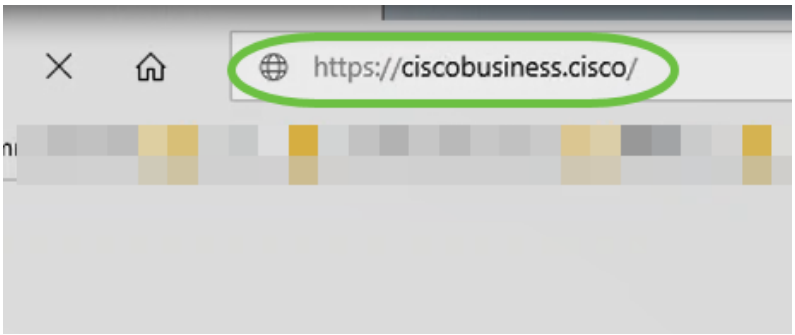
Ga naar de draadloze opties op uw pc en kies het netwerk dat u hebt ingesteld. Klik op **Connect**.

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.



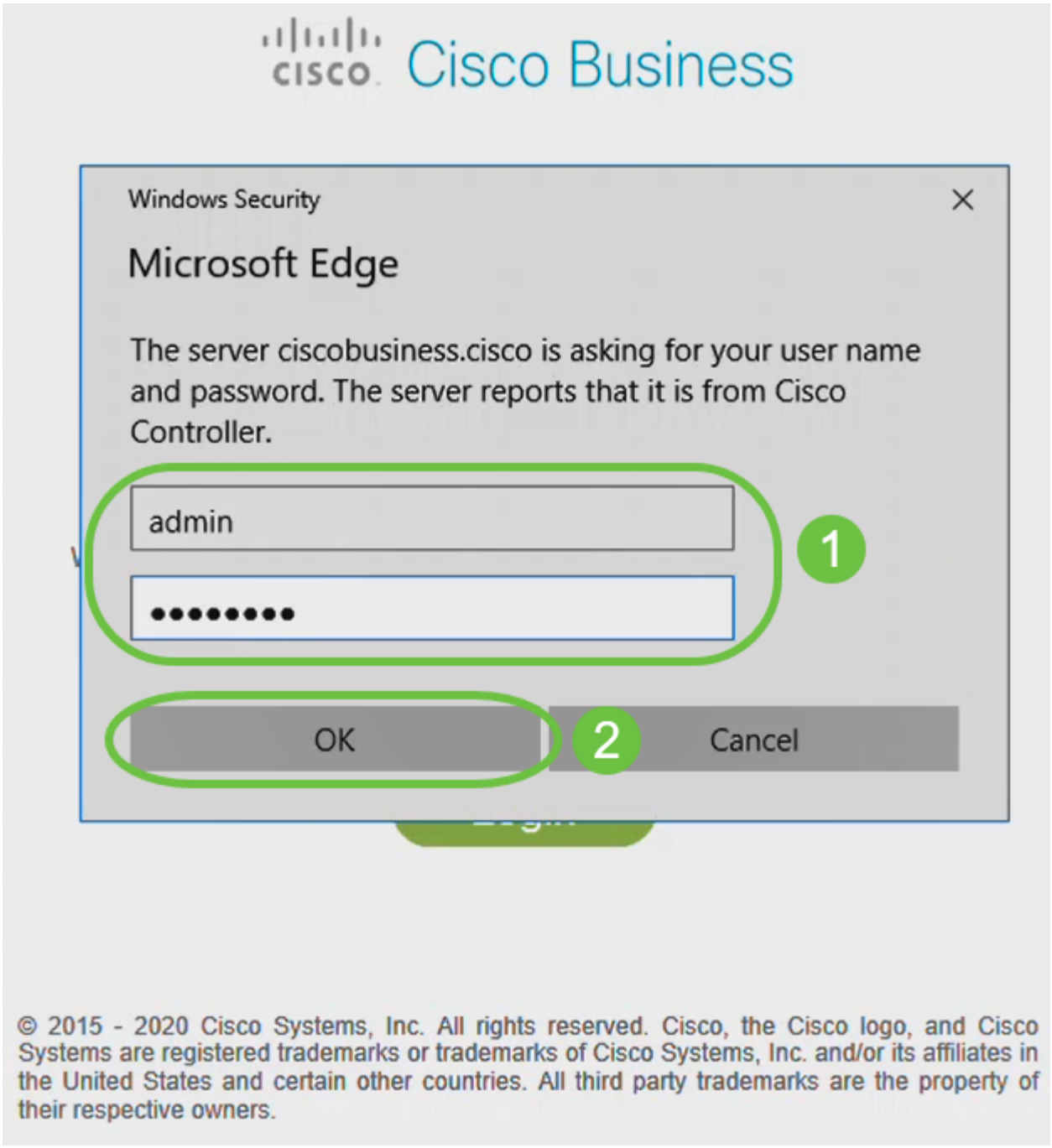
Zorg ervoor dat u *https* typt en niet *http* bij deze stap.

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

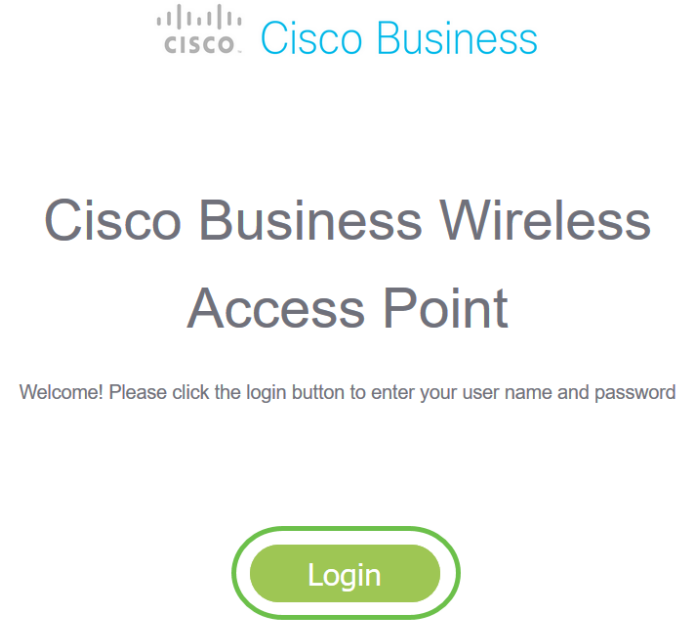
Steek de twee mesh-extenders in de muur op de geselecteerde locaties. Schrijf het MAC-adres van elke mesh-extender op.

Stap 2

Wacht ongeveer 10 minuten voordat de mesh-extenders beginnen.

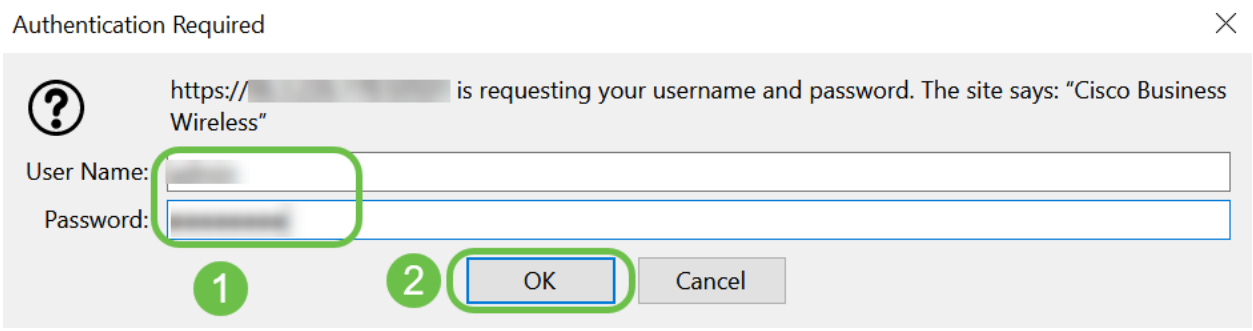
Stap 3

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.



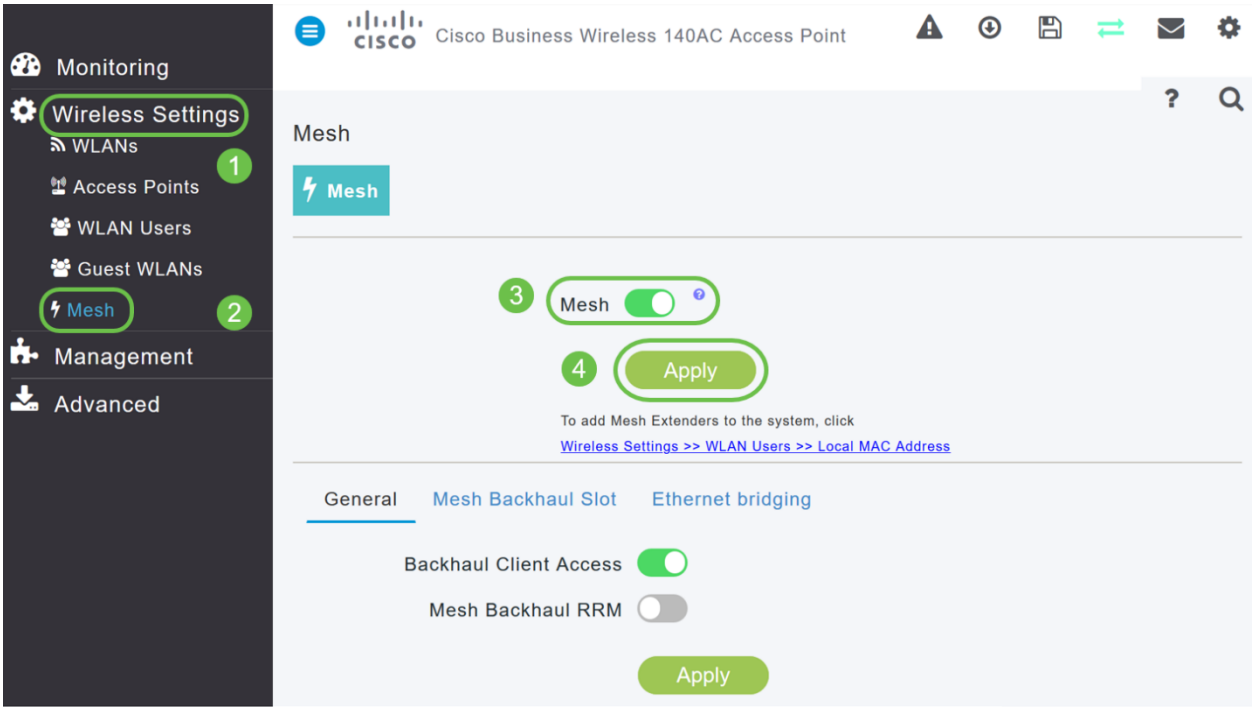
Stap 4

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).

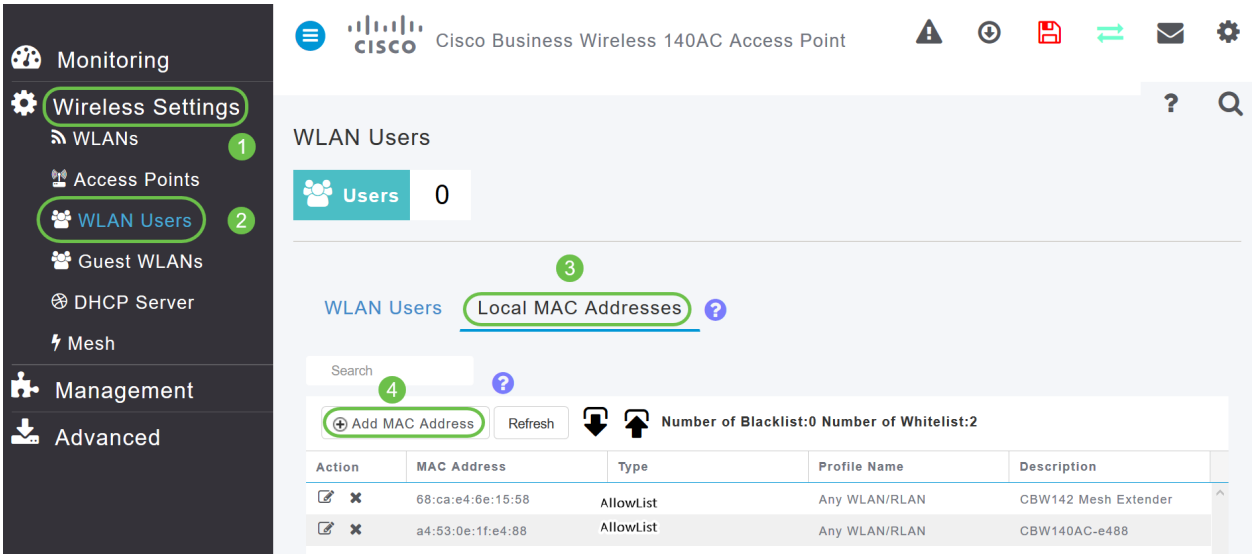


Stap 6

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.

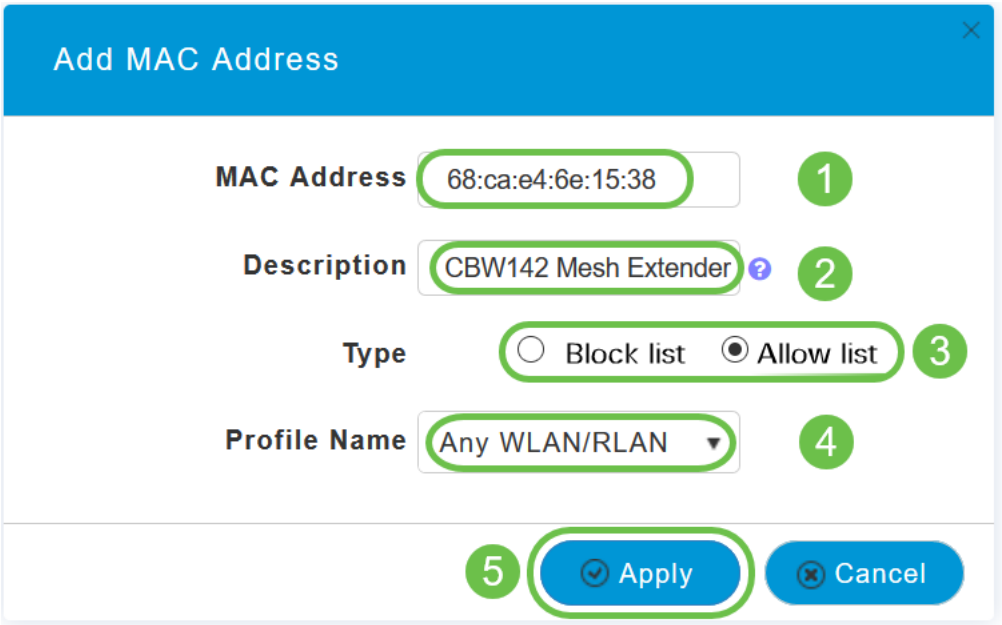
Stap 7

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.

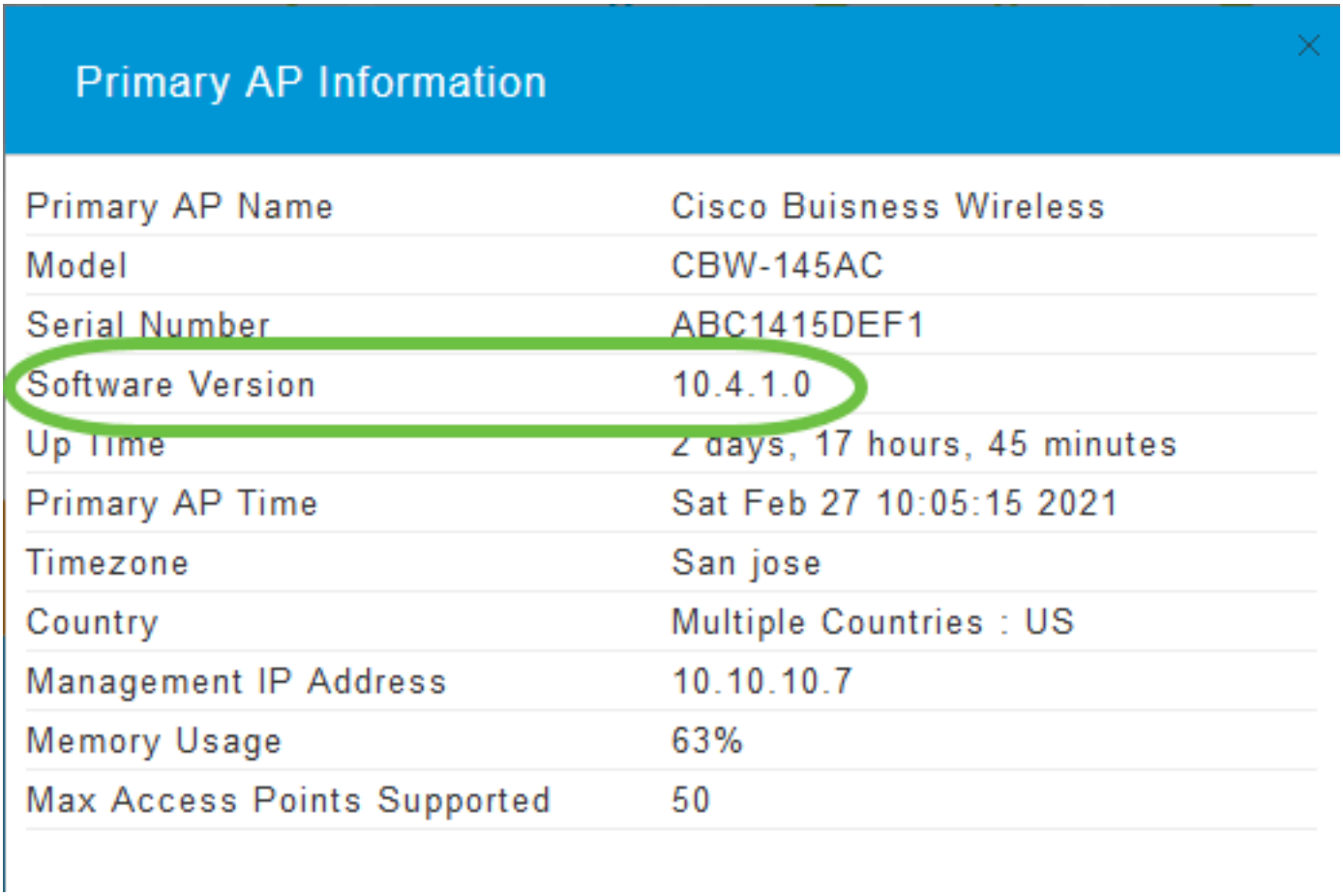
Software controleren en bijwerken met WebUI

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.

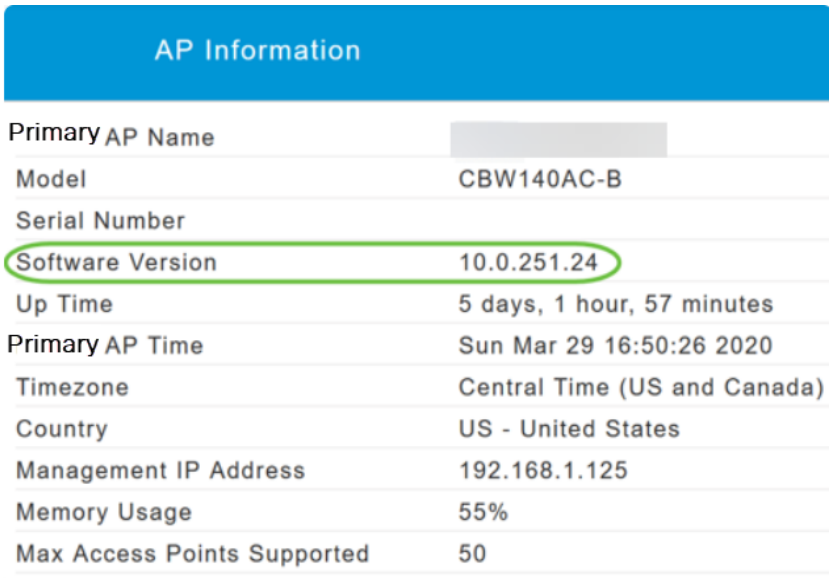
Stap 1

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.



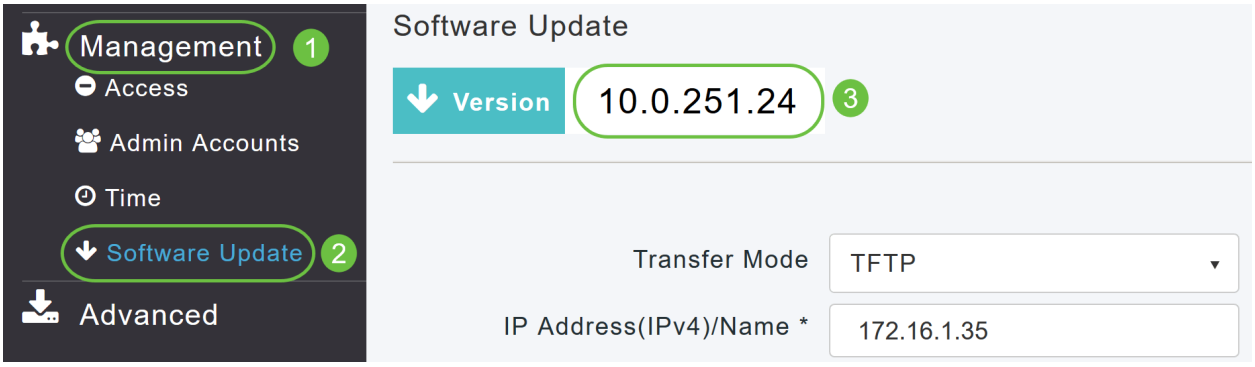
Als u de nieuwste versie van de software draait, kunt u naar het gedeelte WLAN's maken.

Stap 3

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

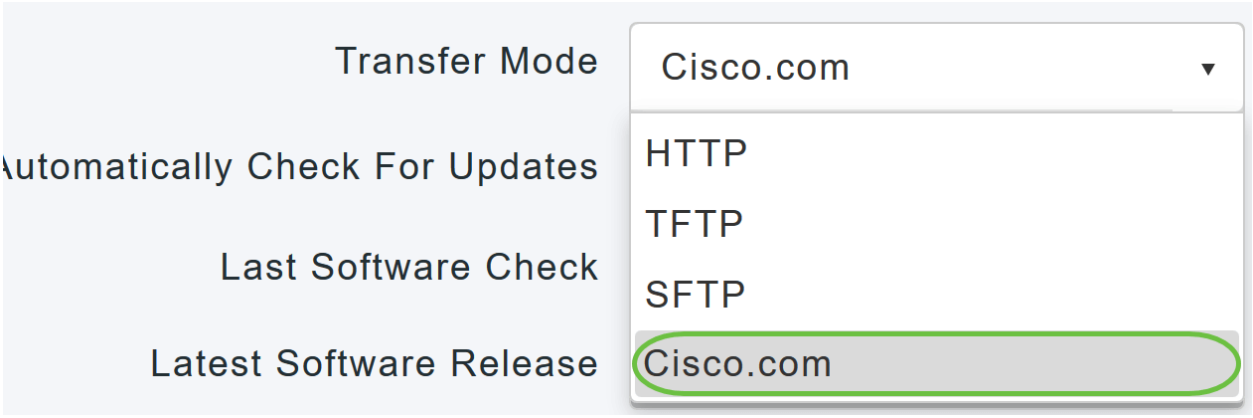
Het venster *Software Update* wordt weergegeven met het huidige versienummer van

de software dat bovenaan wordt weergegeven.



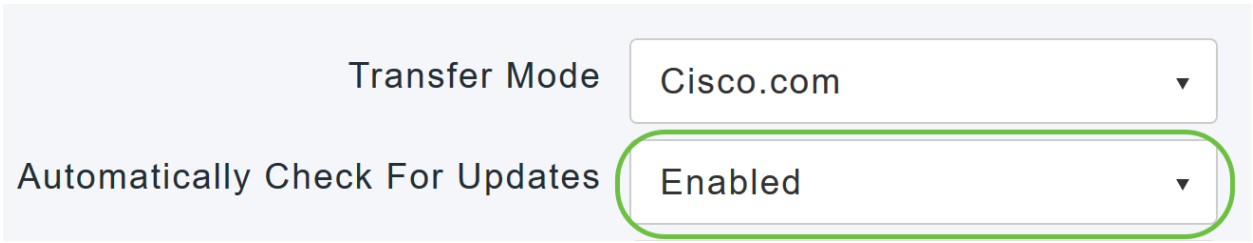
U kunt de CBW AP-software bijwerken en de huidige configuraties op de Primaire AP worden niet verwijderd.

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



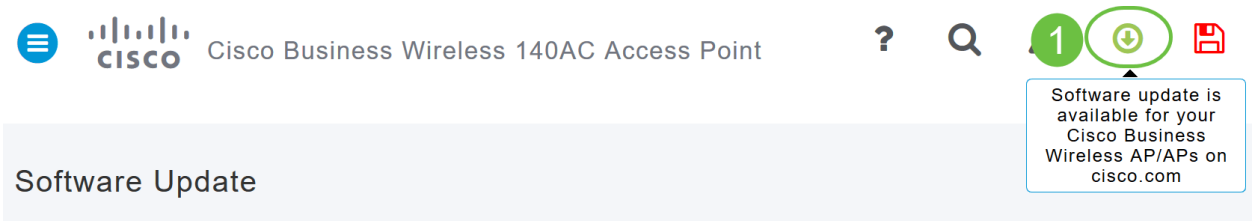
Stap 4

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.



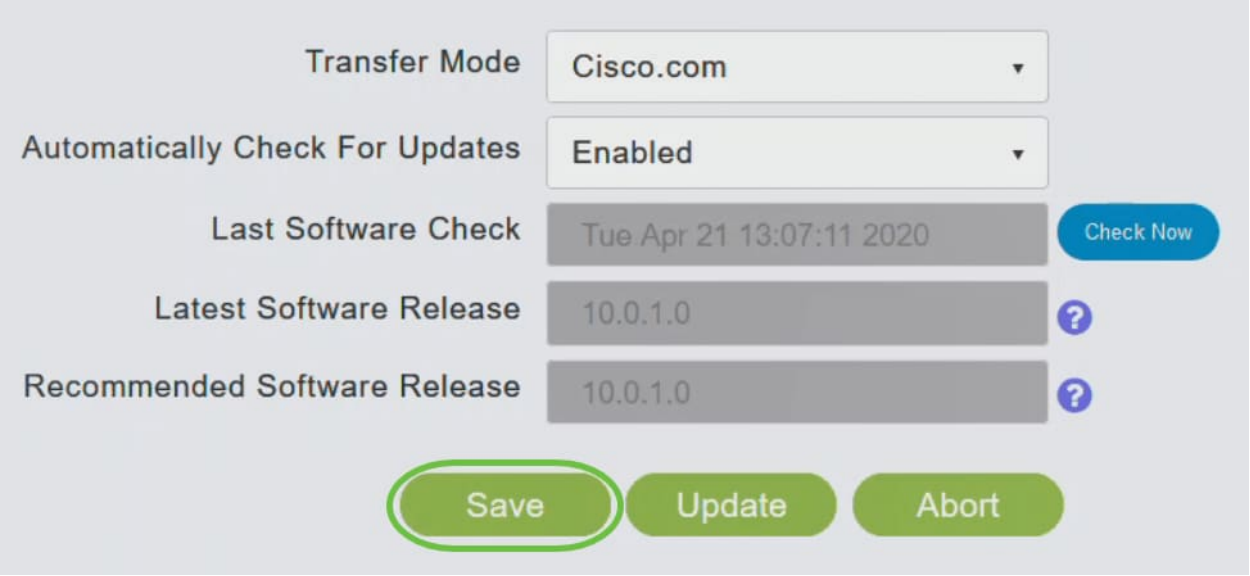
Wanneer een softwarecontrole wordt uitgevoerd en als er een nieuwere, laatste of aanbevolen softwareupdate beschikbaar is op Cisco.com, dan:

- 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.

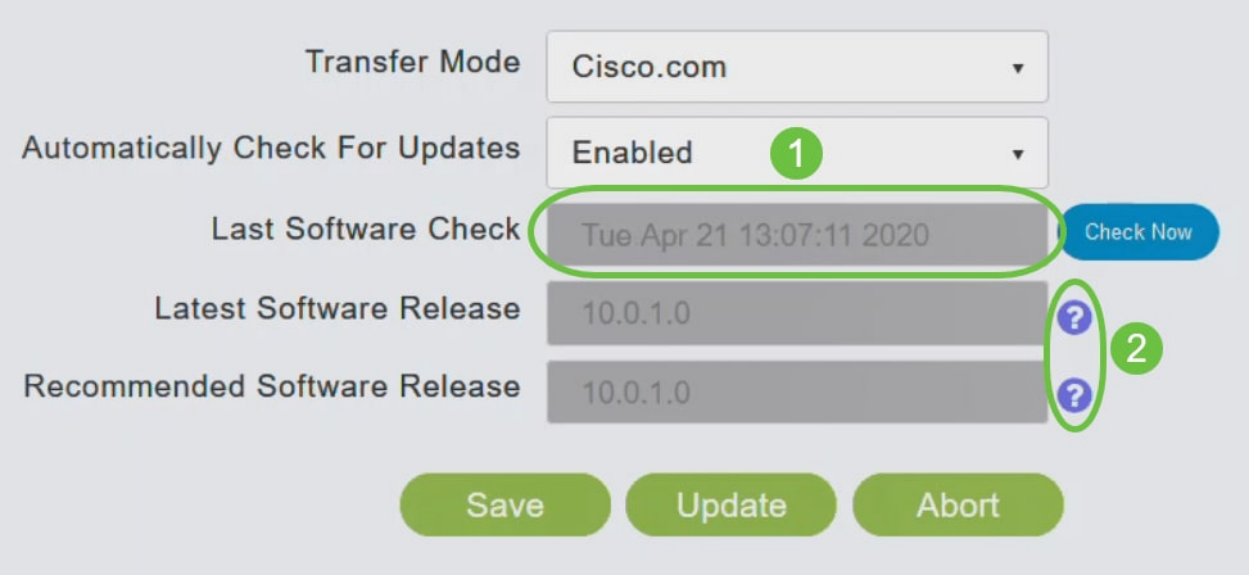


Stap 5

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*.

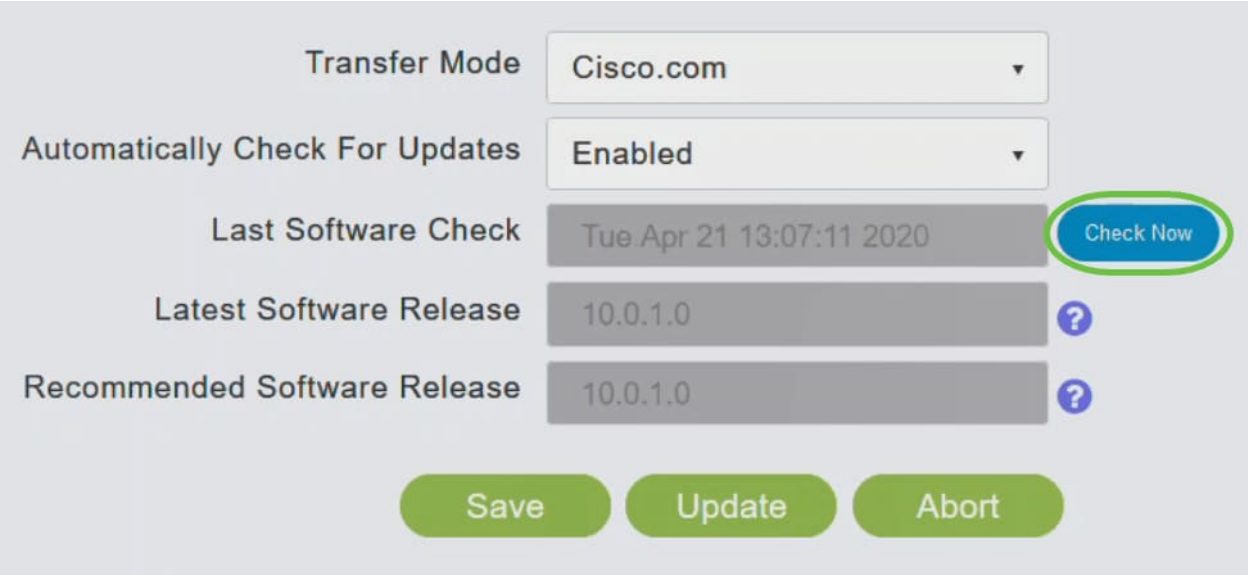


Het veld *Laatste controle op de software* geeft de tijdstempel van de laatste automatische of handmatige controle van de software weer. U kunt de opmerkingen van weergegeven releases bekijken door op het **pictogram** van het **vraagteken** naast deze te klikken.



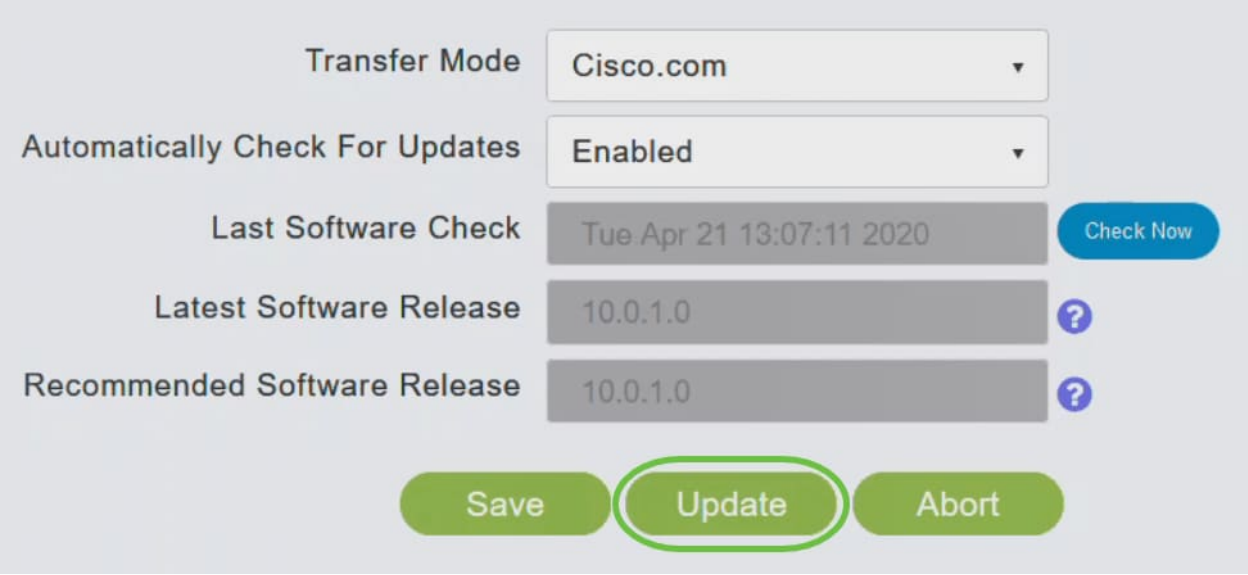
Stap 6

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



Stap 7

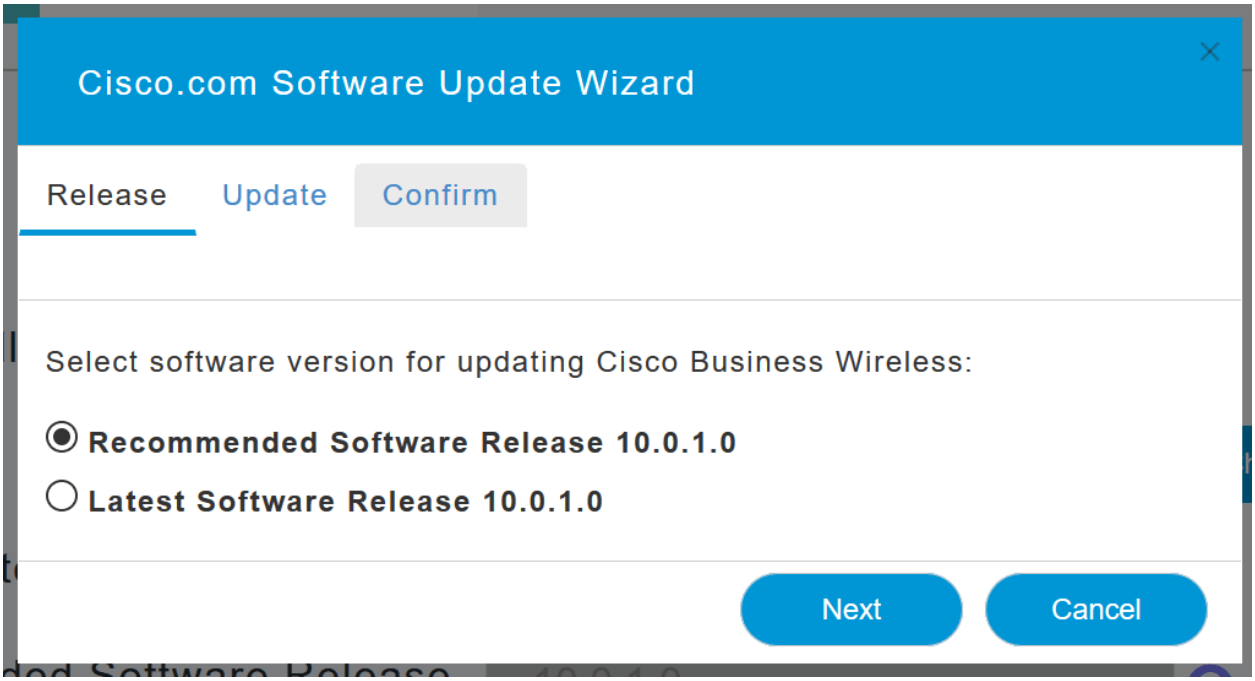
Klik op **Update** om verder te gaan met de softwareupdate.



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

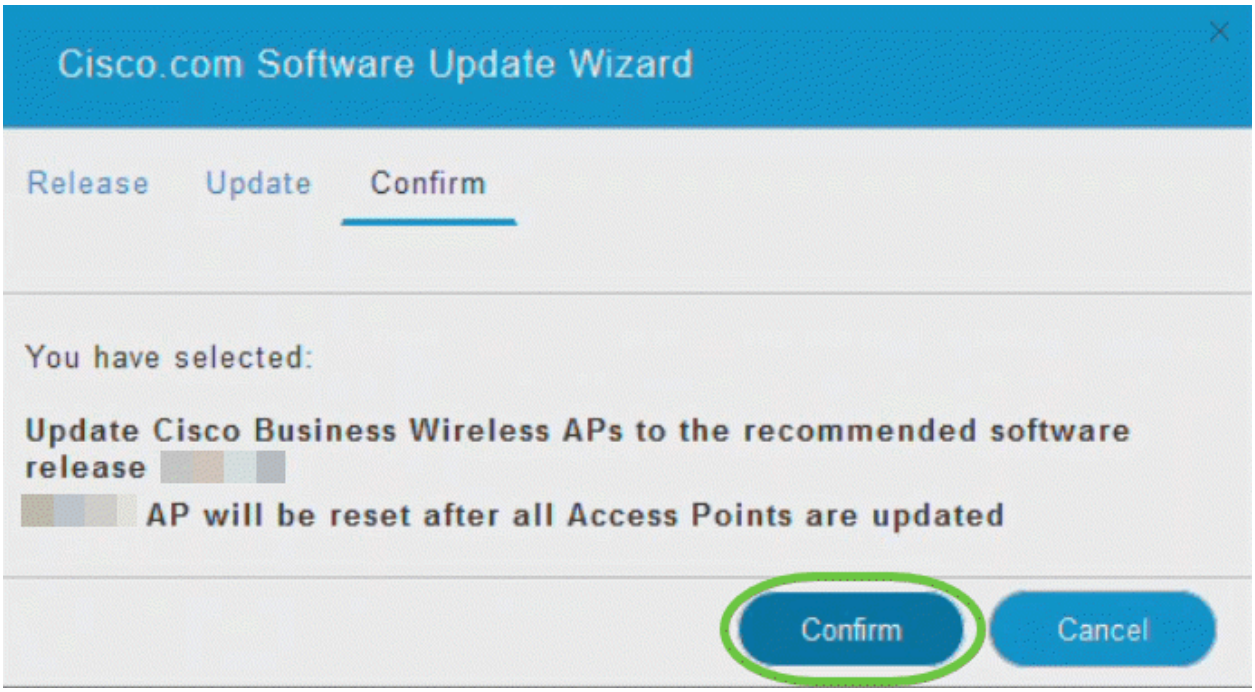
- Release tab - Specificeer of u wilt bijwerken naar de aanbevolen softwarerelease of de nieuwste softwarerelease.
- Tabblad bijwerken - Specificeer wanneer de AP's opnieuw ingesteld moeten worden. U kunt ervoor kiezen het onmiddellijk te laten doen of het voor een later tijdstip te laten plannen. Als 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**.

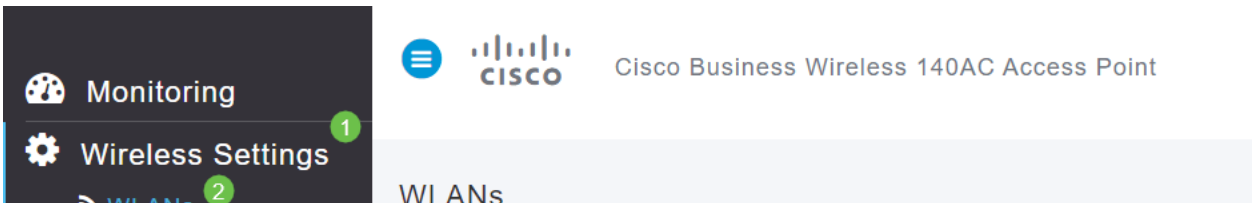


WLAN's maken op de web-UI

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

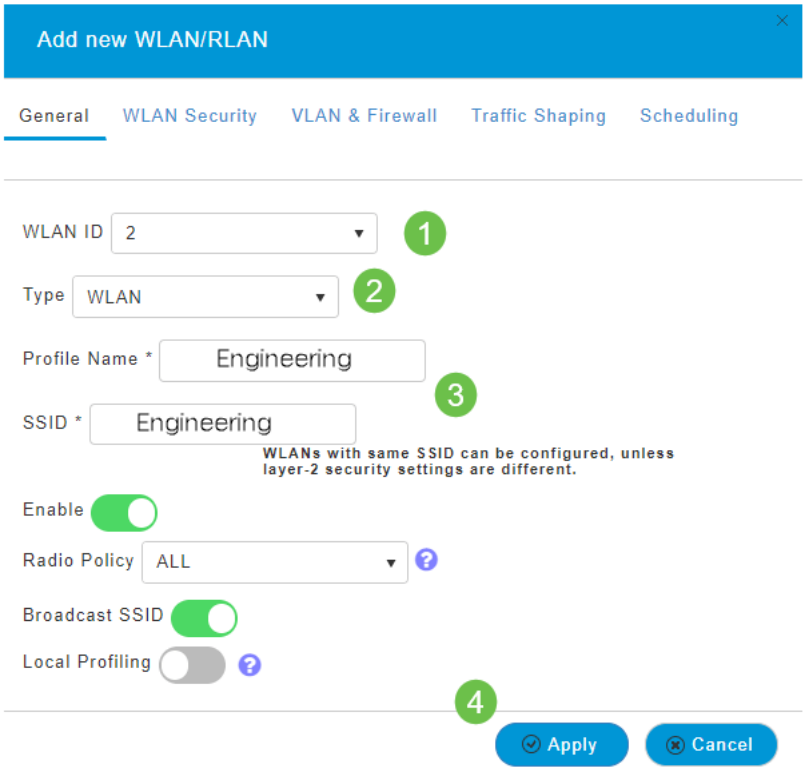
Voer onder het tabblad *Algemeen* de volgende informatie in:

- 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).

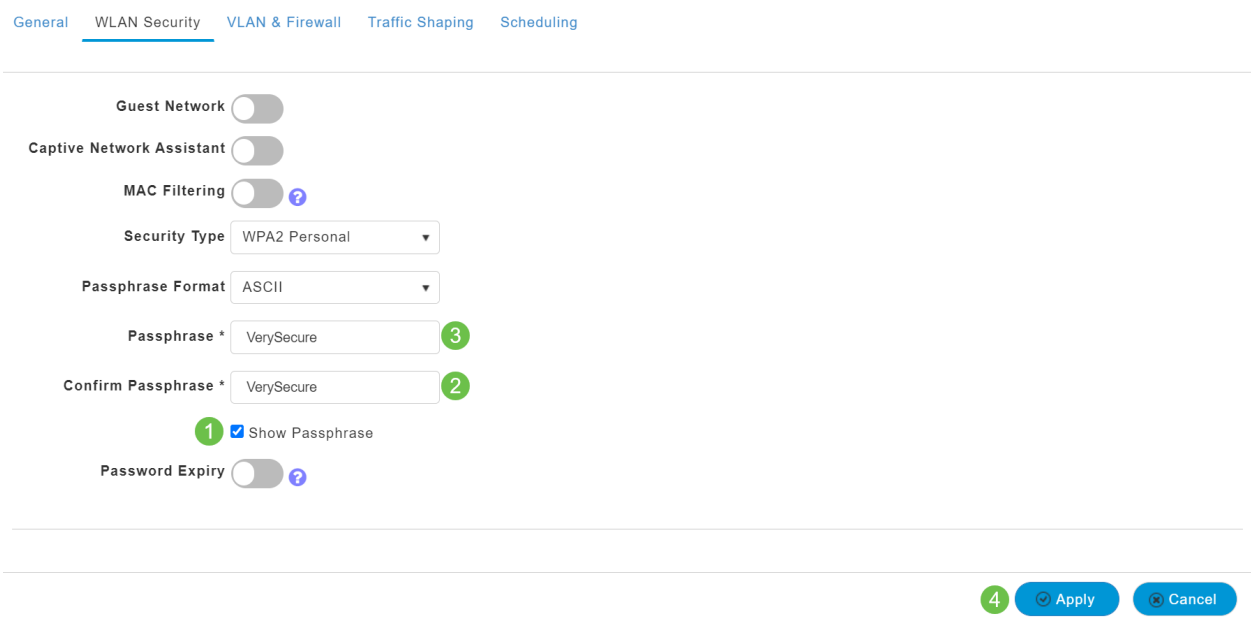
WAP2 Mobile is een methode die gebruikt wordt om uw netwerk te beveiligen met het gebruik van een PSK-verificatie. De PSK wordt afzonderlijk ingesteld, zowel op de Primaire AP, onder het WLAN-beveiligingsbeleid als op de client. WAP2 Persoonlijk baseert zich niet op een authenticatieserver op uw netwerk.

- 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.



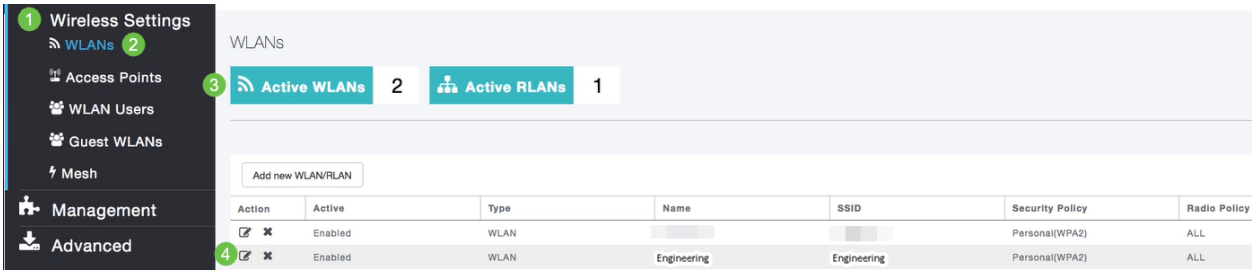
Stap 4

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

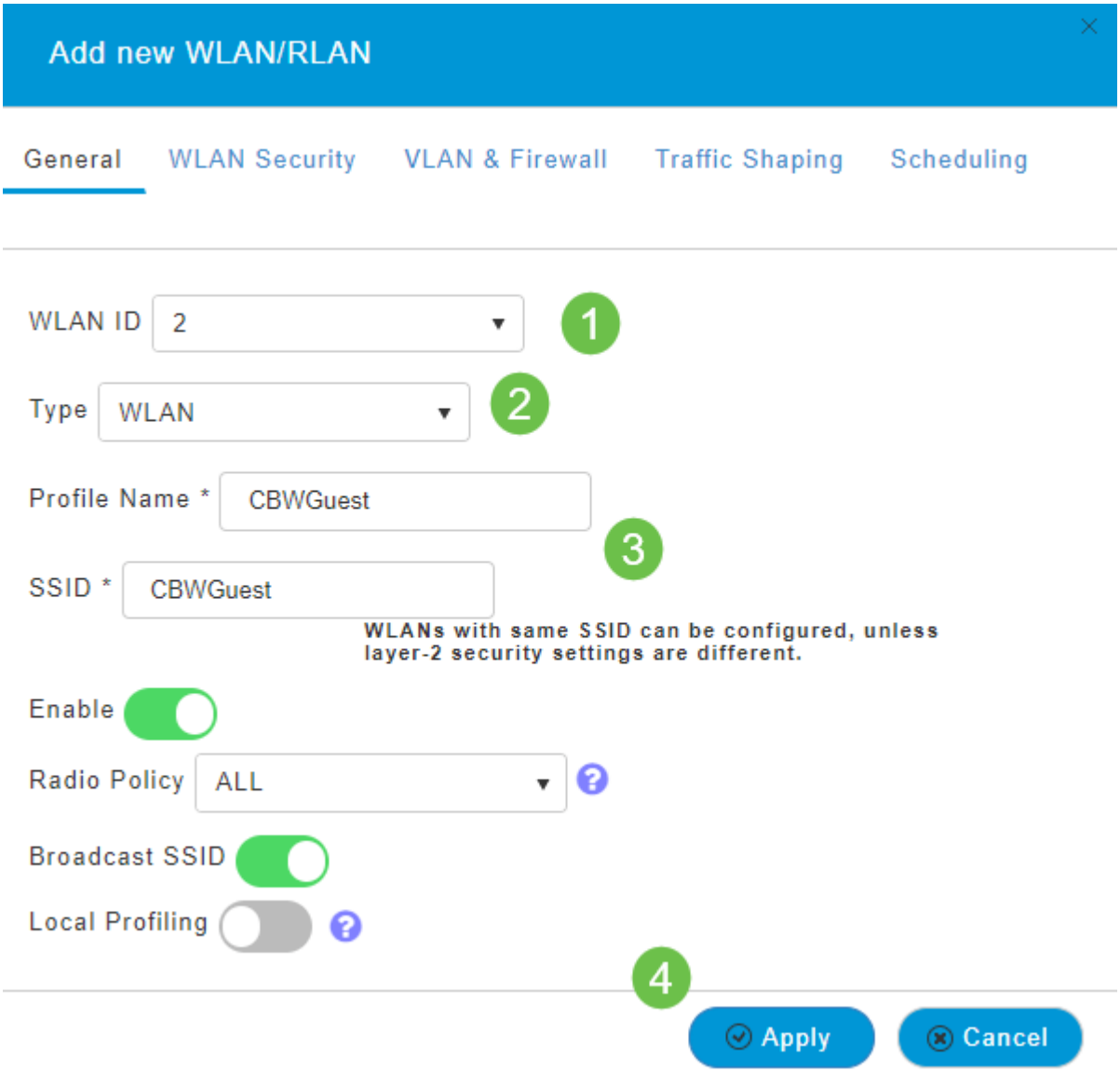
Voer onder het tabblad *Algemeen* de volgende informatie in:

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).

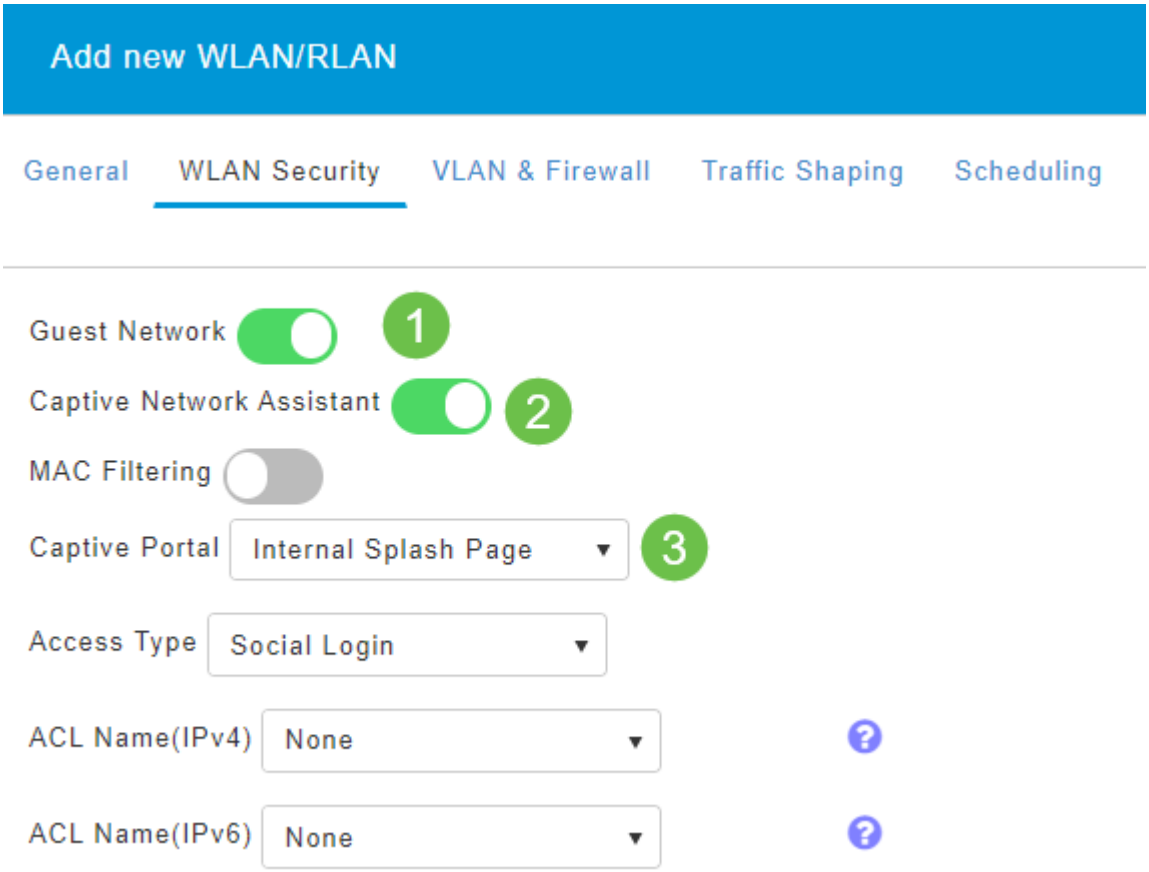


Stap 4

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.

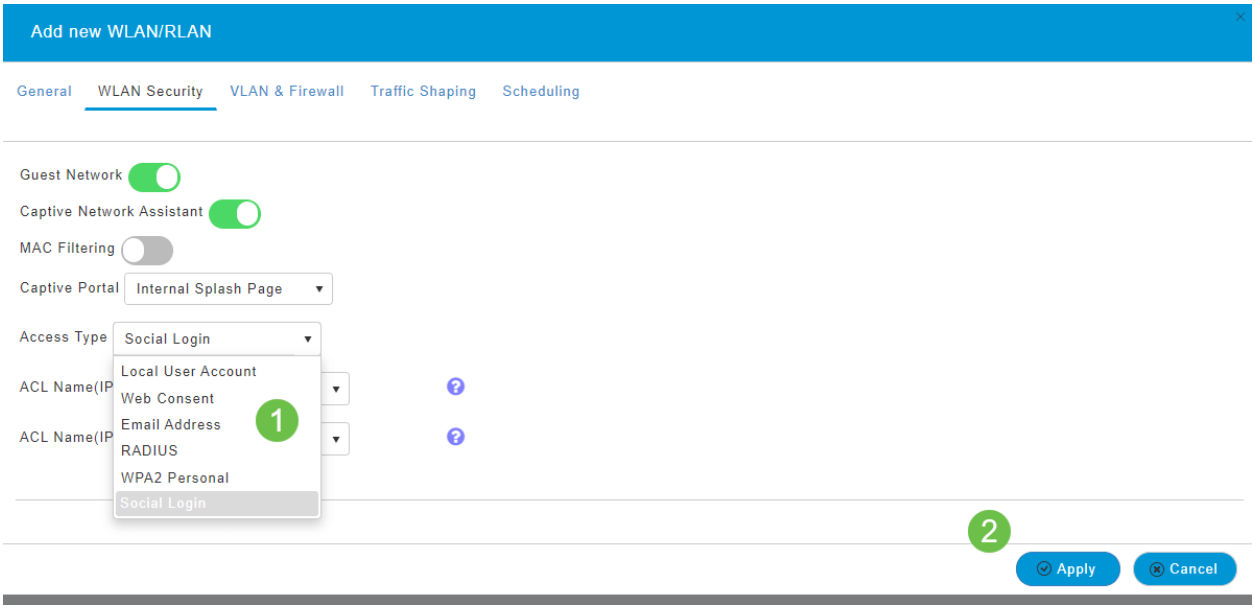
Andere opties voor *Type toegang* omvatten:

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)

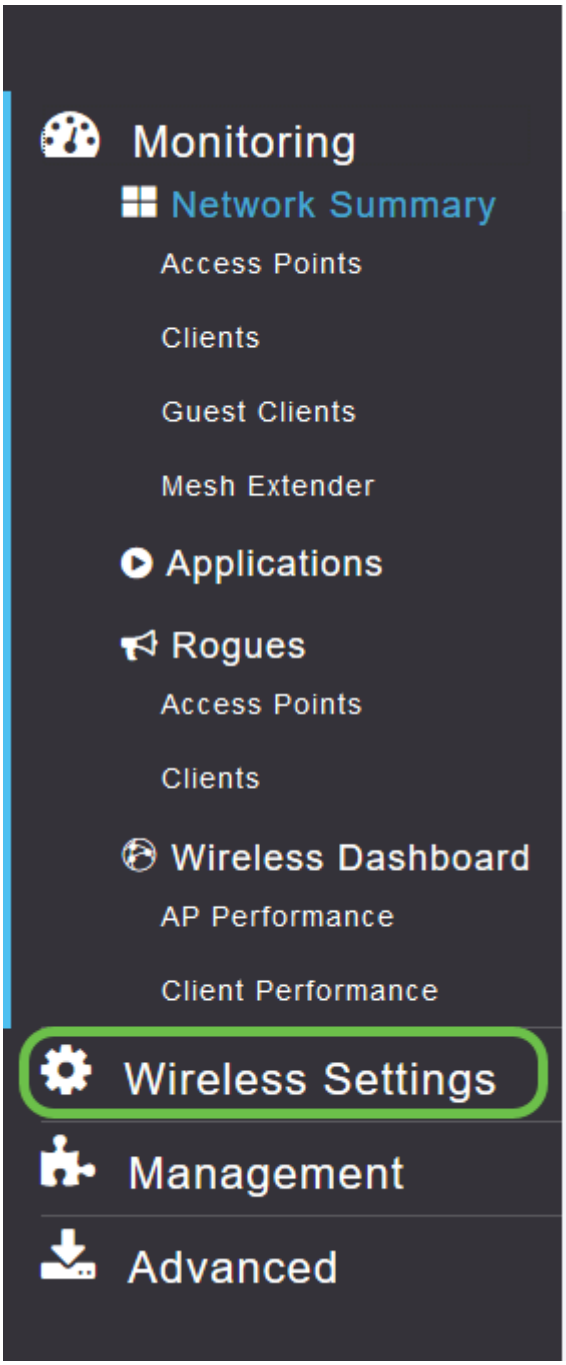
Profileren is een deelgroep van functies die het voeren van een organisatorisch beleid mogelijk maken. Hiermee kunt u verkeerstypen koppelen en prioriteren. Zoals regels beslissen over hoe je het verkeer rangschikt of laat vallen. Het Cisco Business mesh draadloze systeem is voorzien van client- en toepassingsprofielen. 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

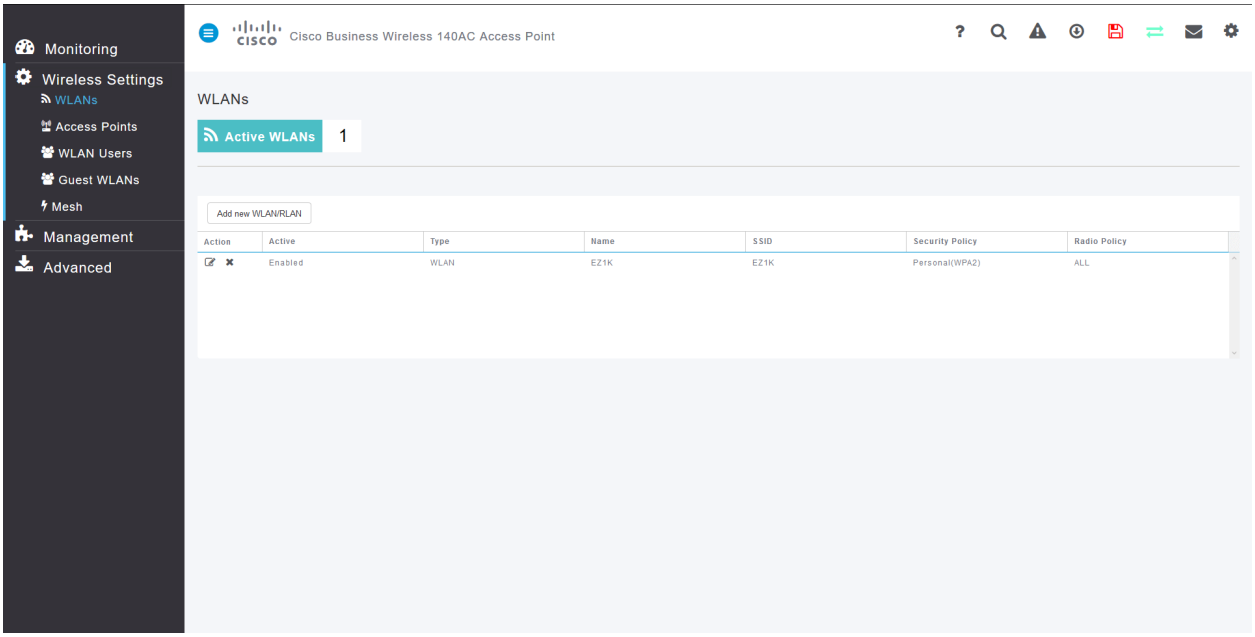
Navigeer naar het menu aan de linkerkant van het scherm als u de linker menubalk niet ziet.

Stap 2

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

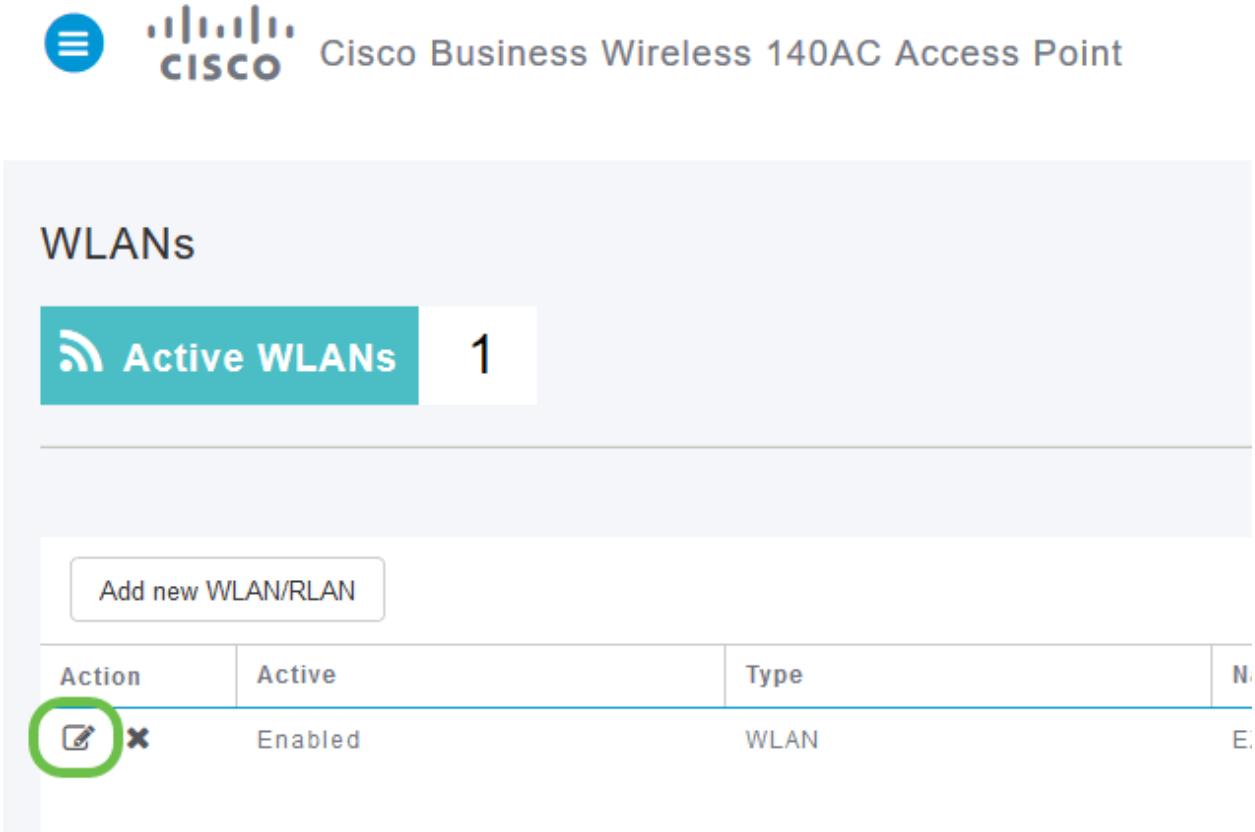


De afbeelding hieronder is gelijk aan de afbeelding die u ziet wanneer u op de link Draadloze instellingen klikt.

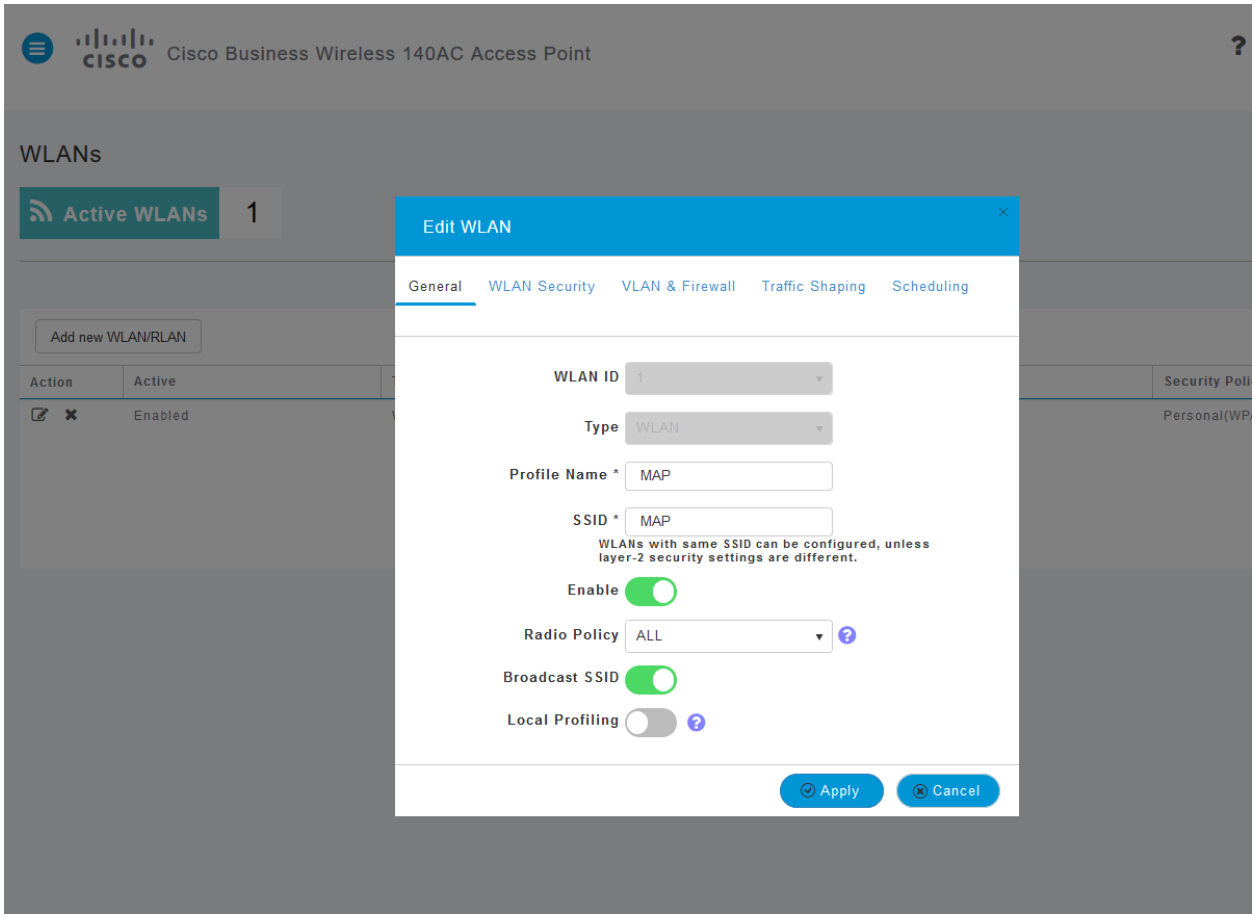


Stap 3

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

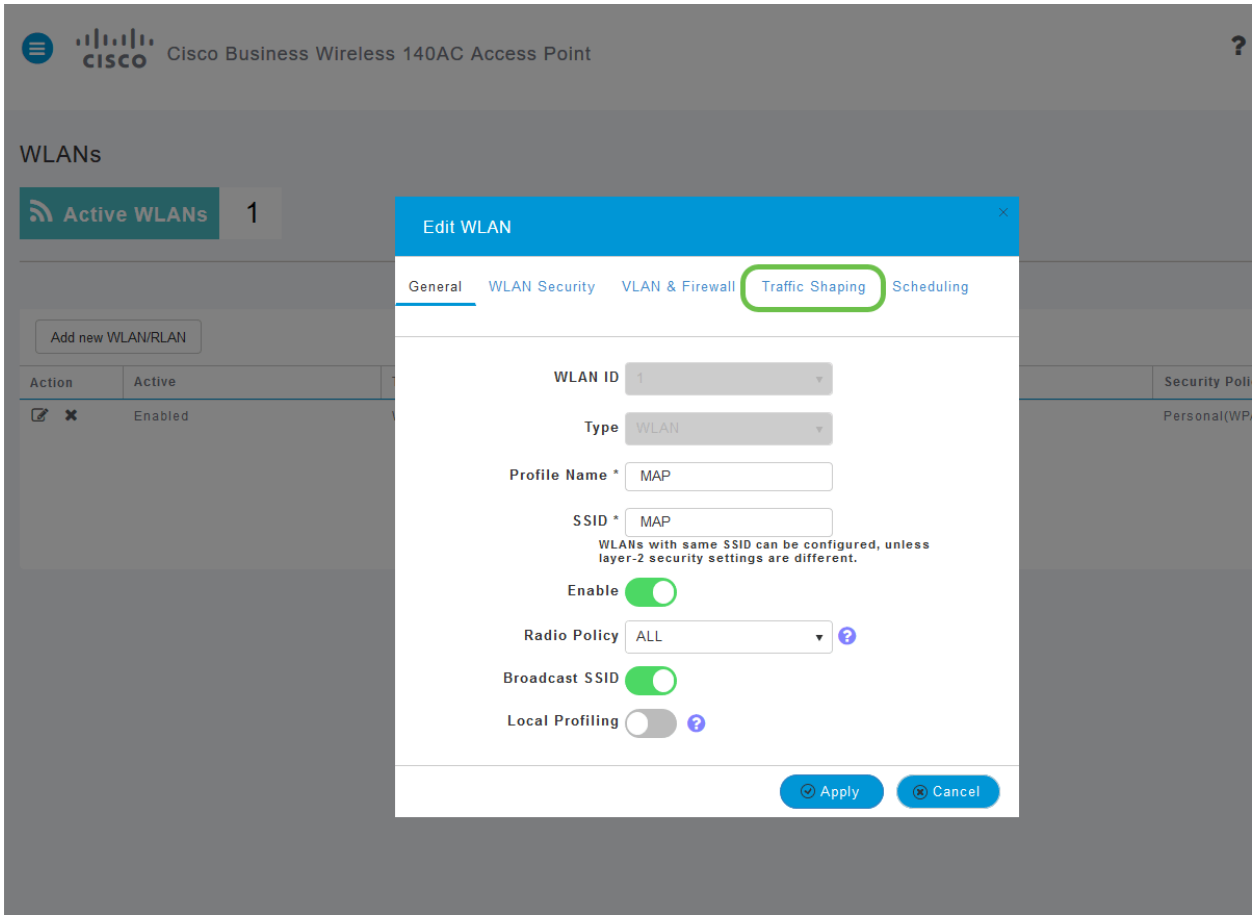


Aangezien u onlangs de WLAN-pagina hebt toegevoegd, kan uw *WLAN*-pagina *bewerken* vergelijkbaar met de onderstaande pagina worden weergegeven:

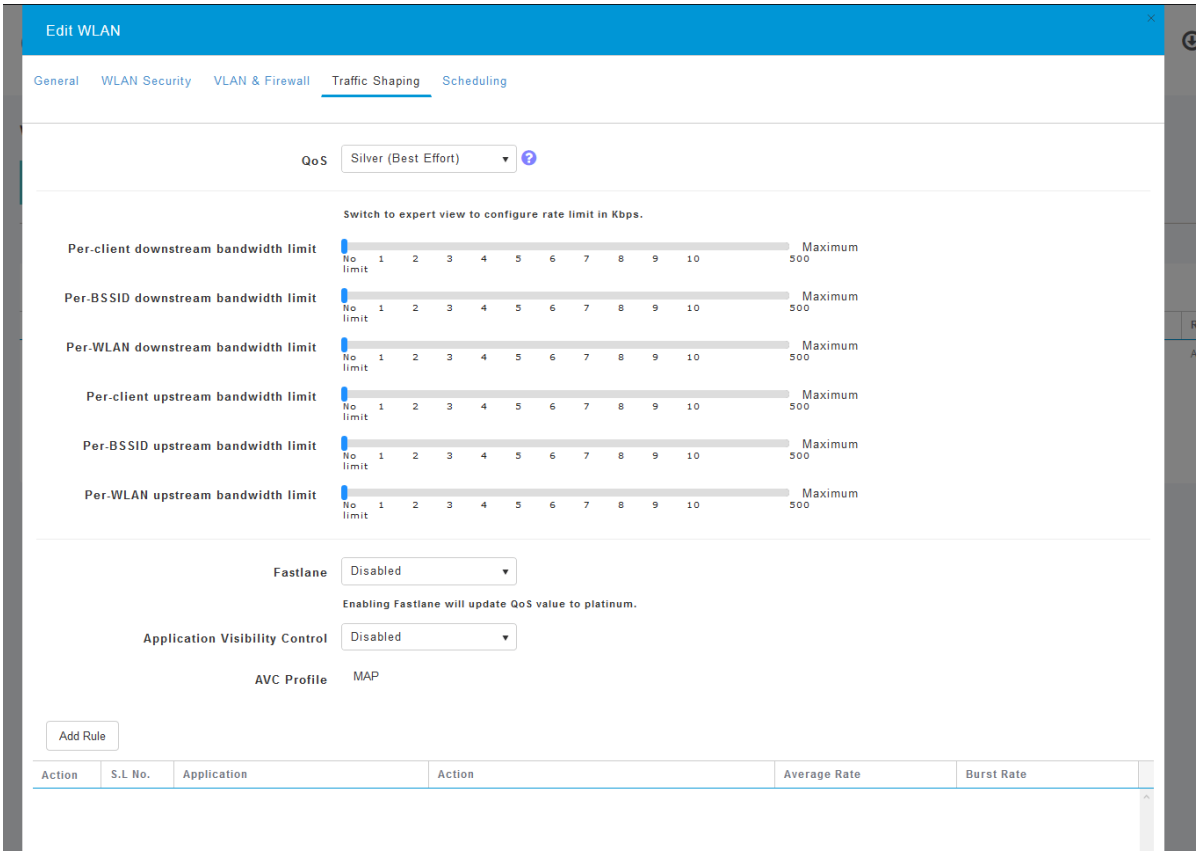


Stap 4

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

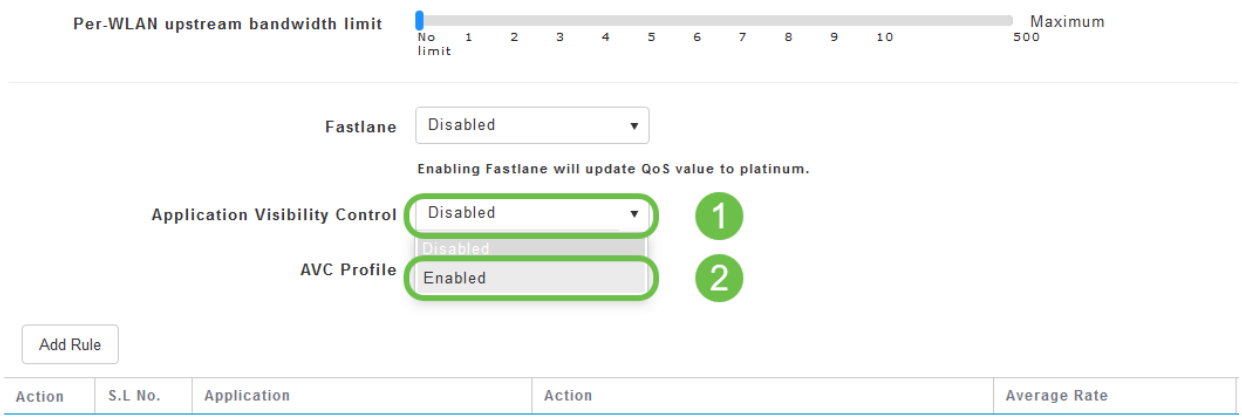


Uw scherm kan als volgt verschijnen:



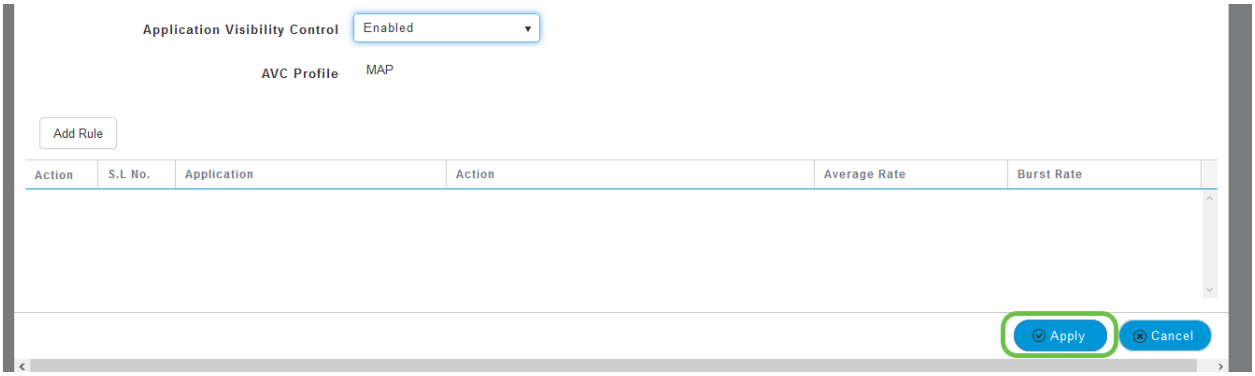
Stap 5

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

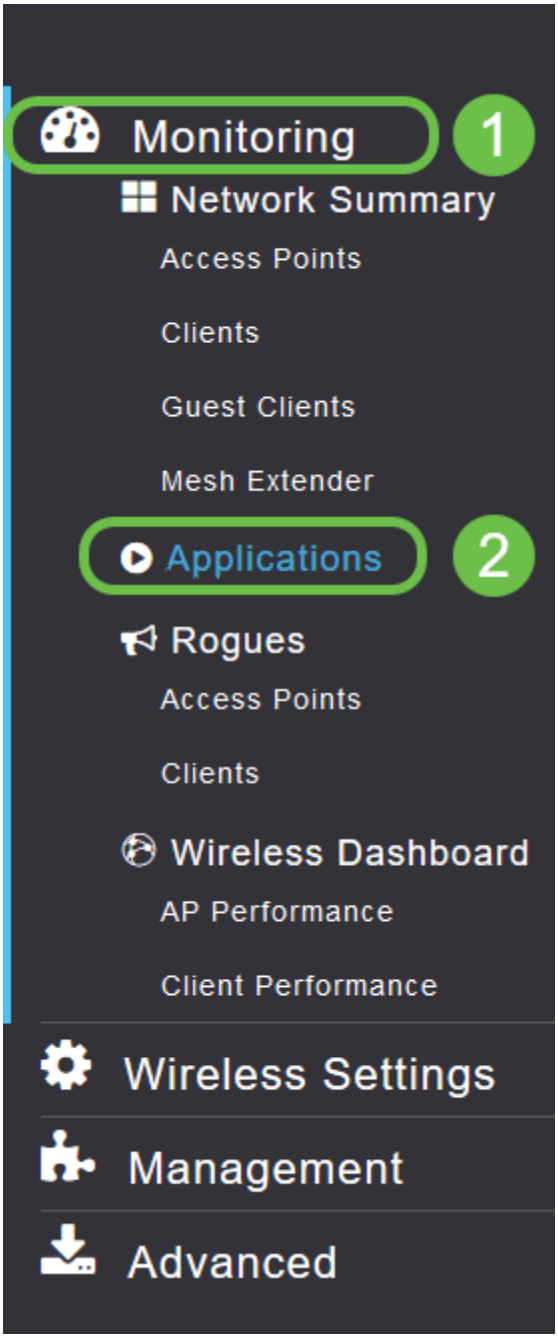
Klik op de knop **Toepassen**.



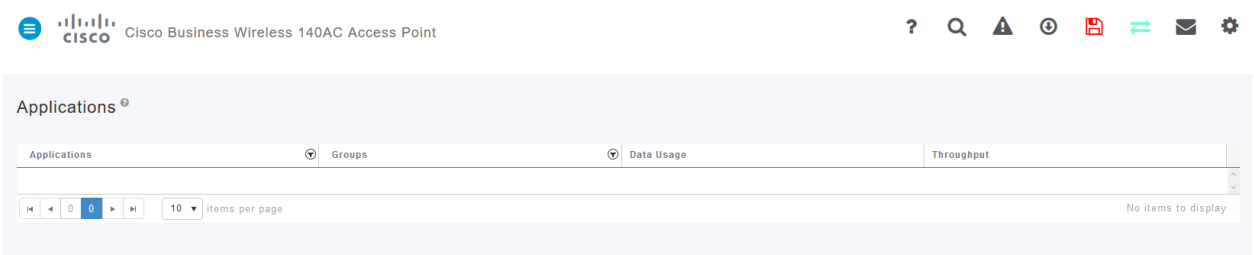
Deze instelling moet worden ingeschakeld, anders werkt deze functie niet.

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:

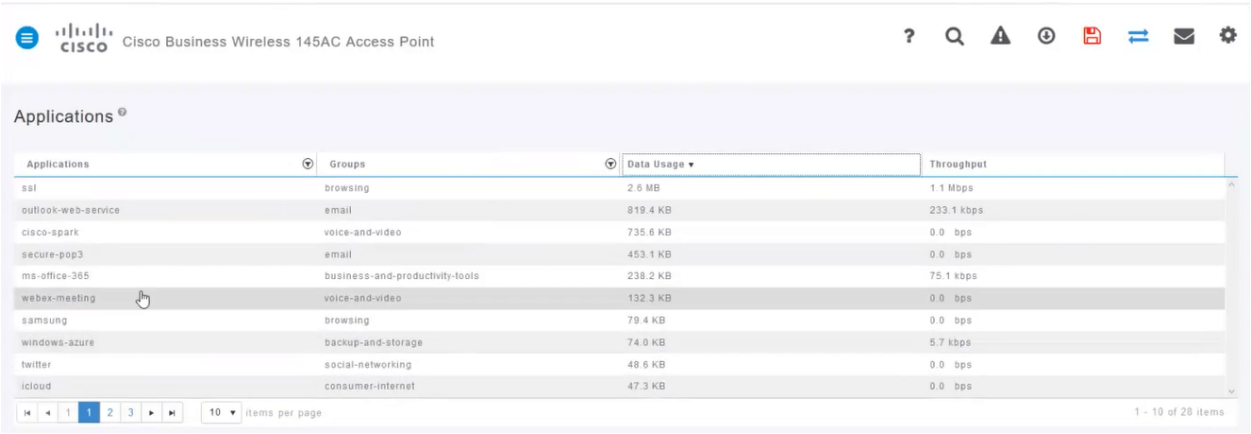
- Toepassing - omvat vele verschillende typen
- Groepen - Geeft het type toepassingsgroep aan zodat het gemakkelijker te sorteren is
- Gebruik van gegevens - de hoeveelheid gegevens die door deze dienst in het algemeen wordt gebruikt
- Doorvoersnelheid - de hoeveelheid bandbreedte die door de toepassing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

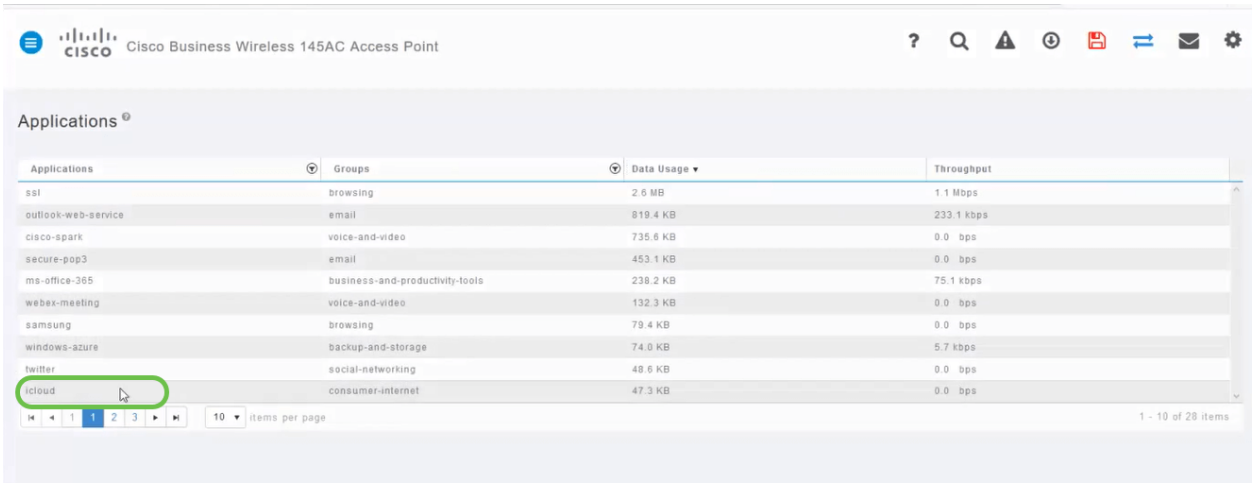
Hier wordt een voorbeeld getoond van hoe de pagina eruit zal zien wanneer gevuld.



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

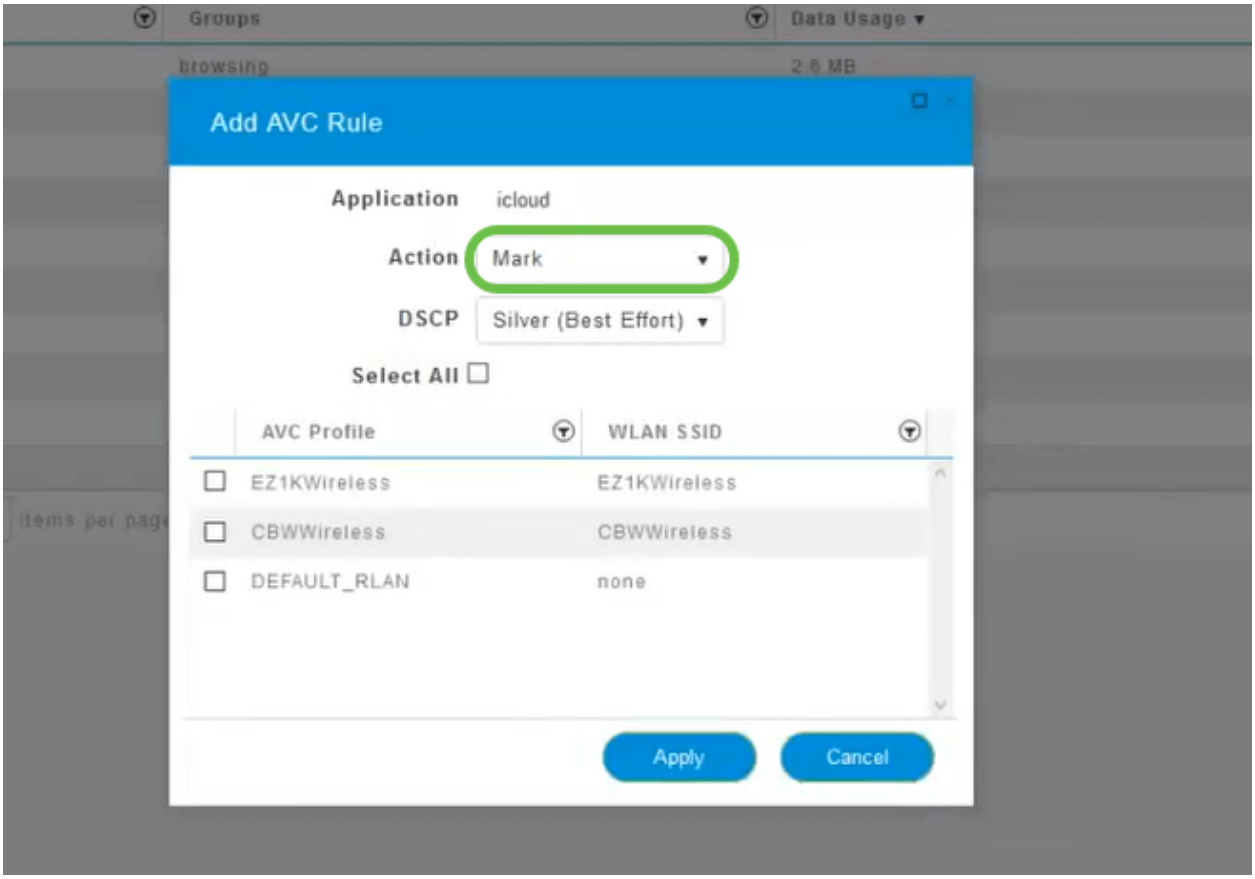
Stap 8

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.



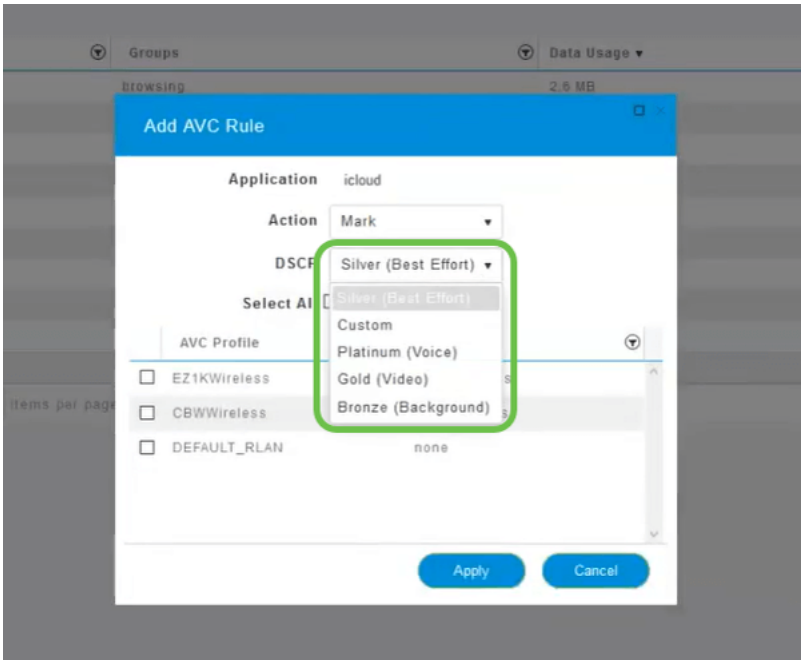
Dit voorbeeld laten we deze optie bij *Mark* achter.

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.



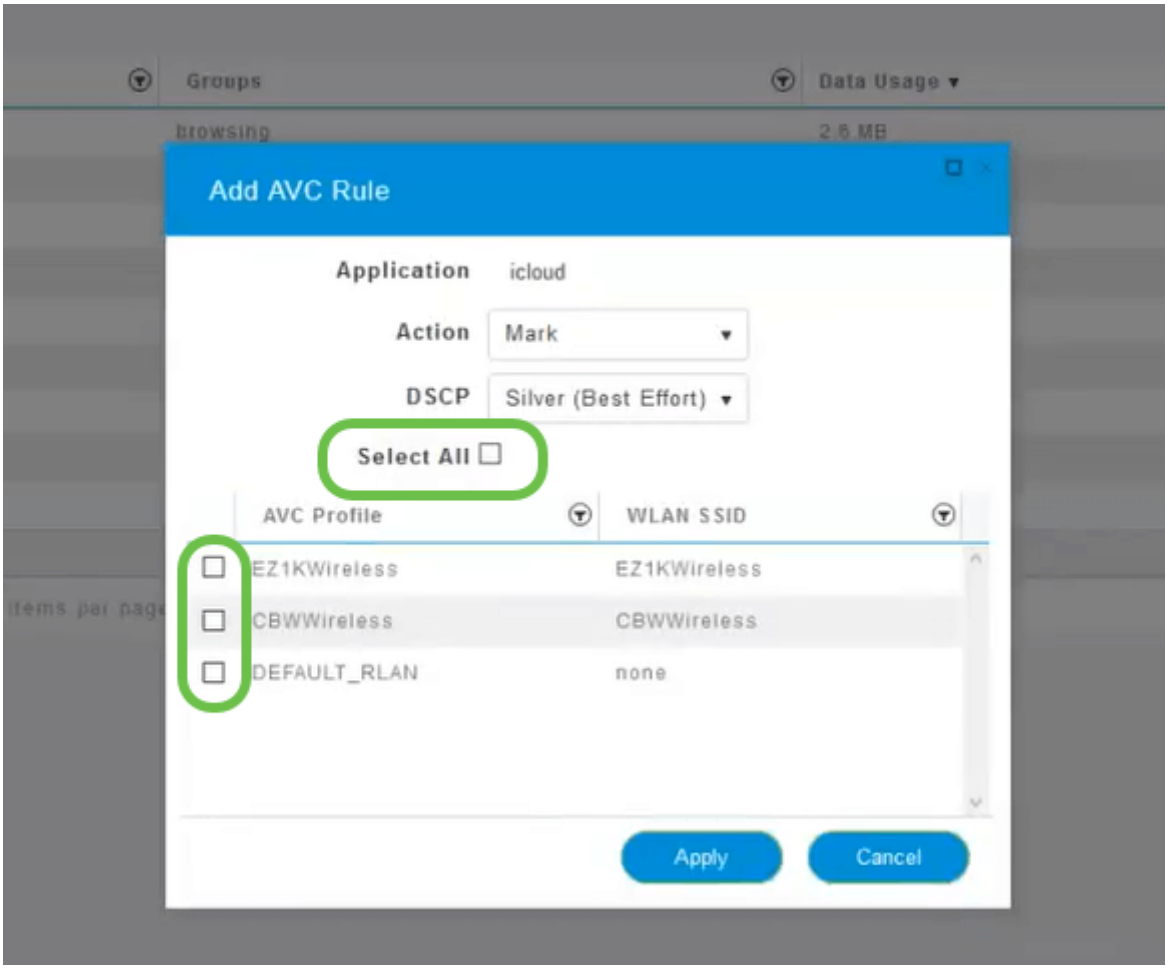
Hieronder staan de DSCP-opties voor het te markeren verkeer. Deze opties gaan van minder bronnen naar meer bronnen beschikbaar voor het type verkeer dat u bewerkt.

- 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.

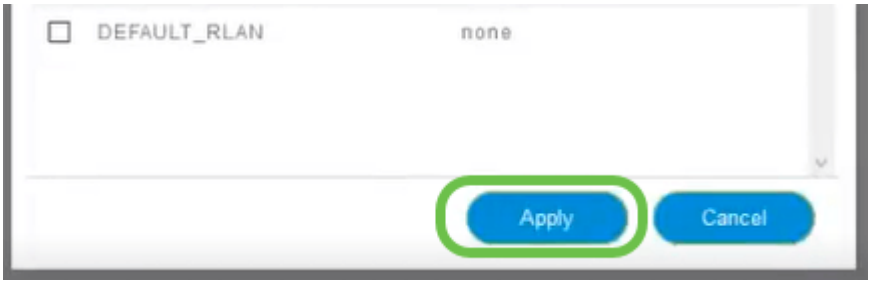
Stap 11

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

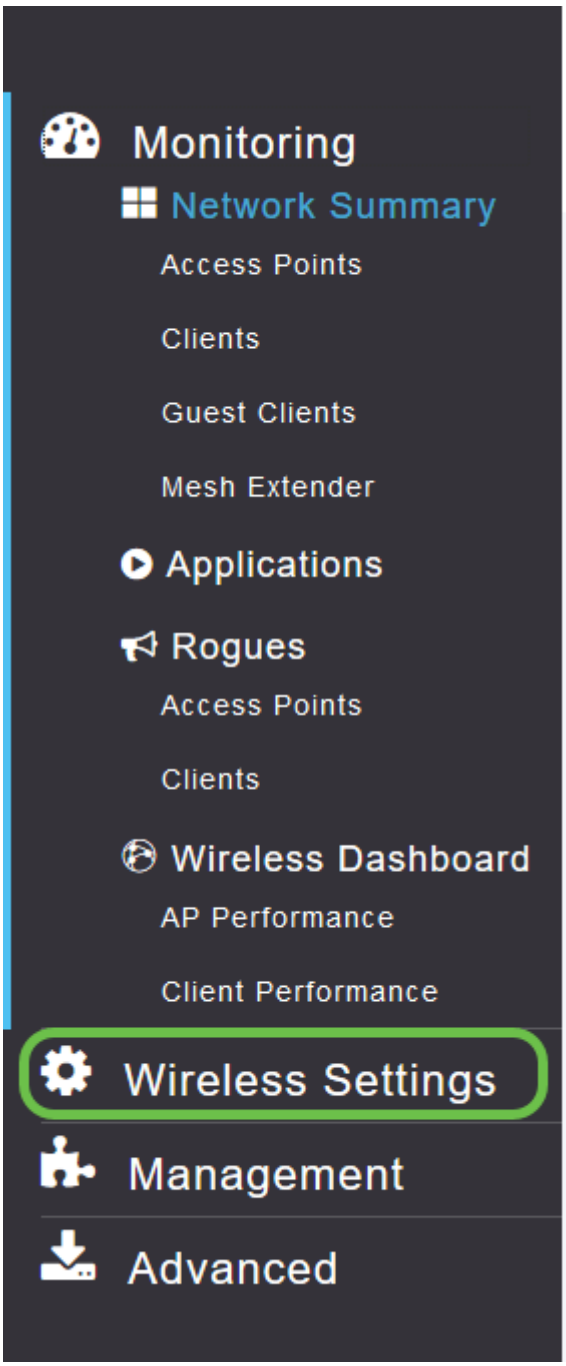
Statistieken over deze klanten omvatten de gebruikte hoeveelheid gegevens en de doorvoersnelheid.

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.

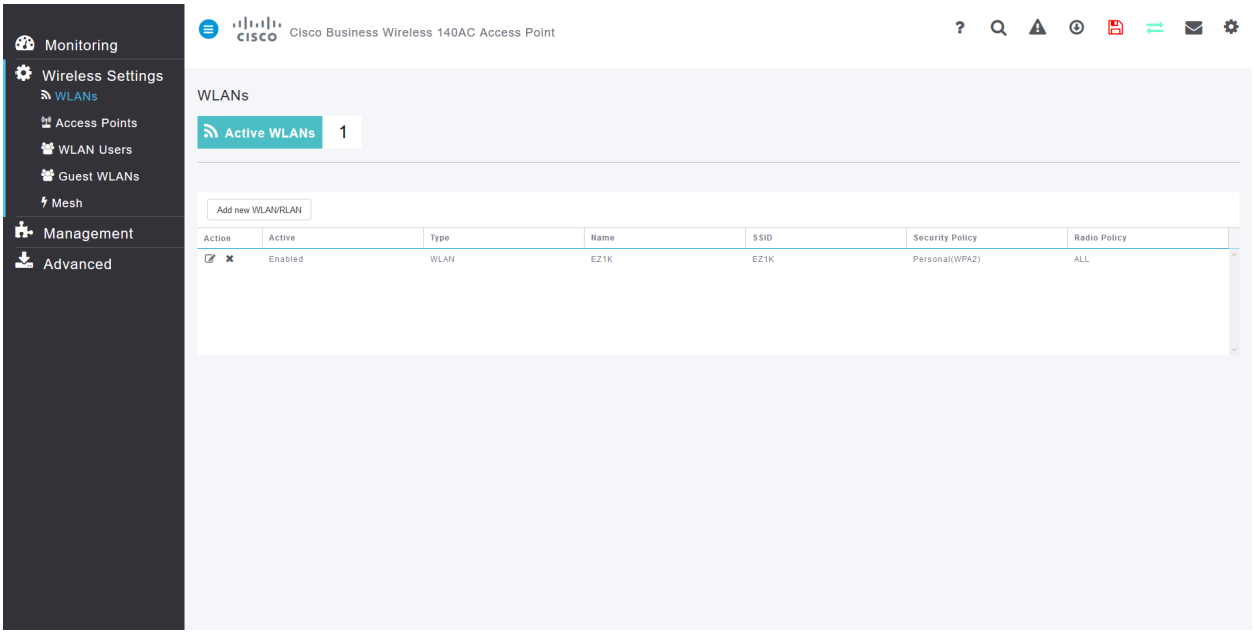
Als deze functie is ingeschakeld, zijn clientgegevens voor uw netwerk te vinden in het gedeelte Monitoring van het web UI.

Stap 1

Klik op **Draadloze instellingen**.

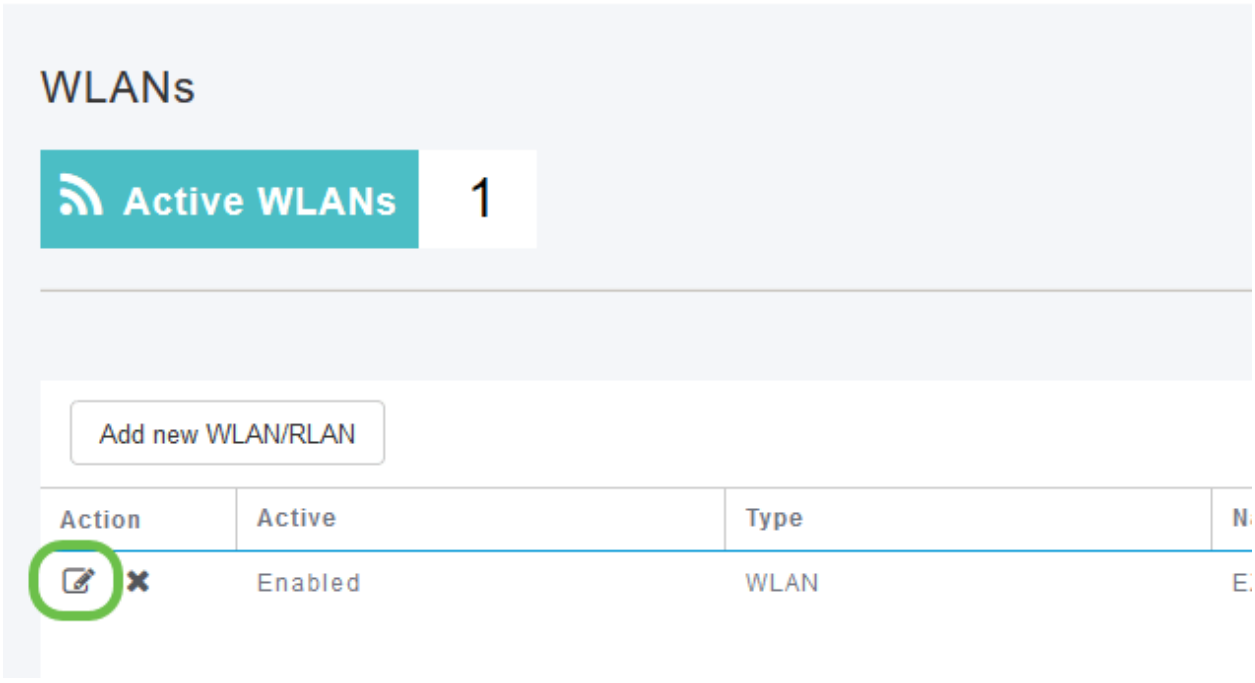


Het onderstaande is gelijk aan wat u ziet wanneer u op de link Draadloze instellingen klikt:



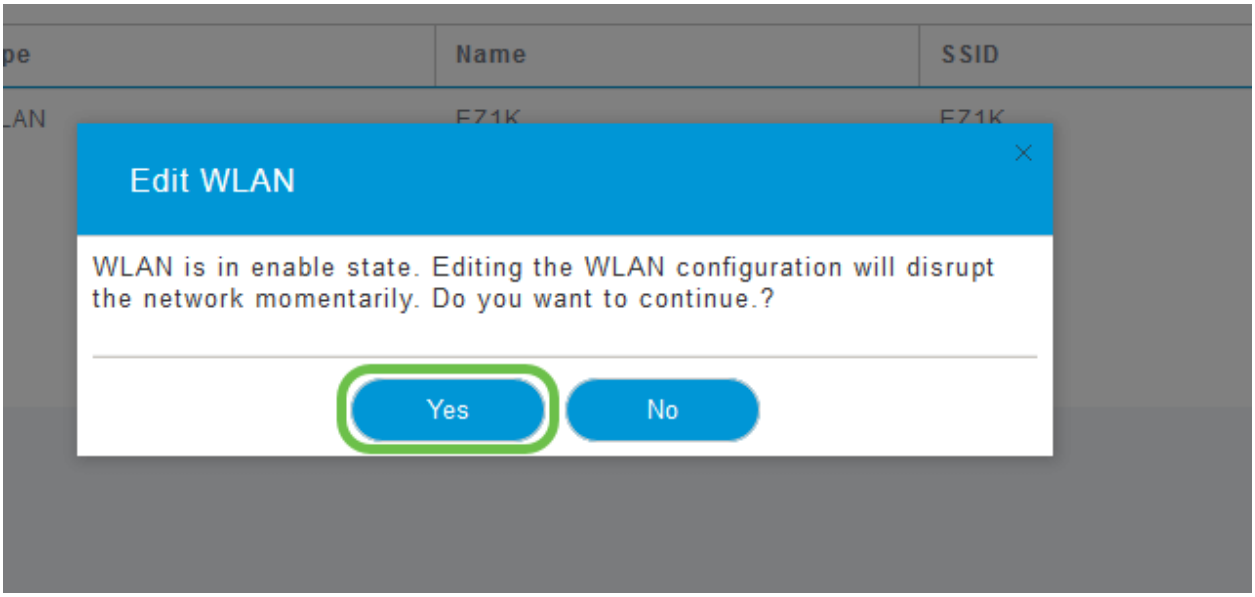
Stap 2

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.

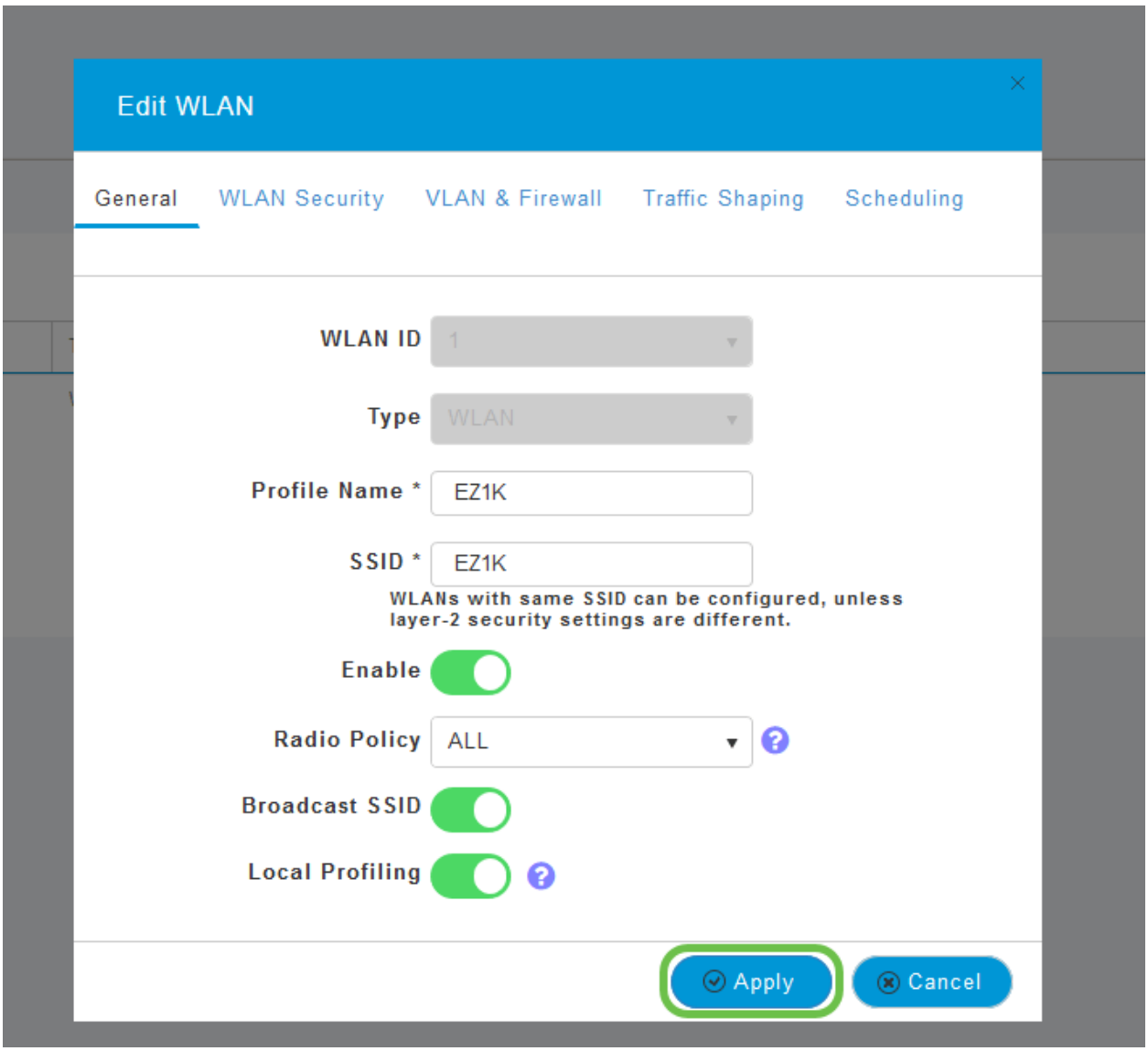


Stap 4

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

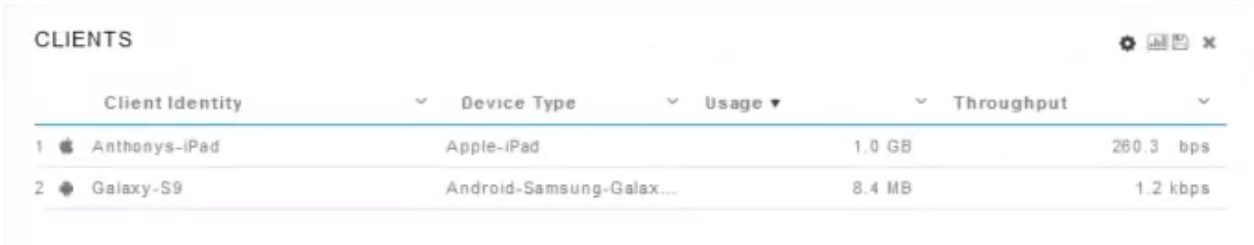
Stap 5

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 RV345P VPN-router met PoE
- Cisco Business 140 AC access point
- Cisco Business 142ACM mesh-extender