Vervang het standaard zelfgetekende certificaat met een SSL-certificaat van een derde partij op de RV34x Series router

Inleiding

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. Zij kan ook verzoeken aan de certificaatinstanties (CA's) zenden om een digitaal identiteitsbewijs aan te vragen. Het is belangrijk om te beschikken over rechtmatige certificaten uit aanvragen van derden.

Er zijn twee manieren waarop CA de certificaten tekent:

1. CA tekent het certificaat met privé-toetsen.

2. CA-tekens in de certificaten met certificaataanvraag (CSR) die door RV34x zijn gegenereerd.

De meeste verkopers van handelscertificaten gebruiken intermediaire certificaten. Aangezien het intermediaire certificaat is afgegeven door de Trusted Root CA, erft elk certificaat dat is afgegeven door het intermediaire certificaat het vertrouwen van de Trusted Root, zoals een certificeringsketen van vertrouwen.

Doel

Dit artikel is bedoeld om te laten zien hoe u een door een CA afgegeven 3rd party Secure Socket Layer (SSL) certificaat kunt aanvragen en uploaden om het zelf-ondertekende certificaat op de RV34x Router te vervangen.

Toepasselijke apparaten

- RV340
- RV340 W
- RV345
- RV345P router

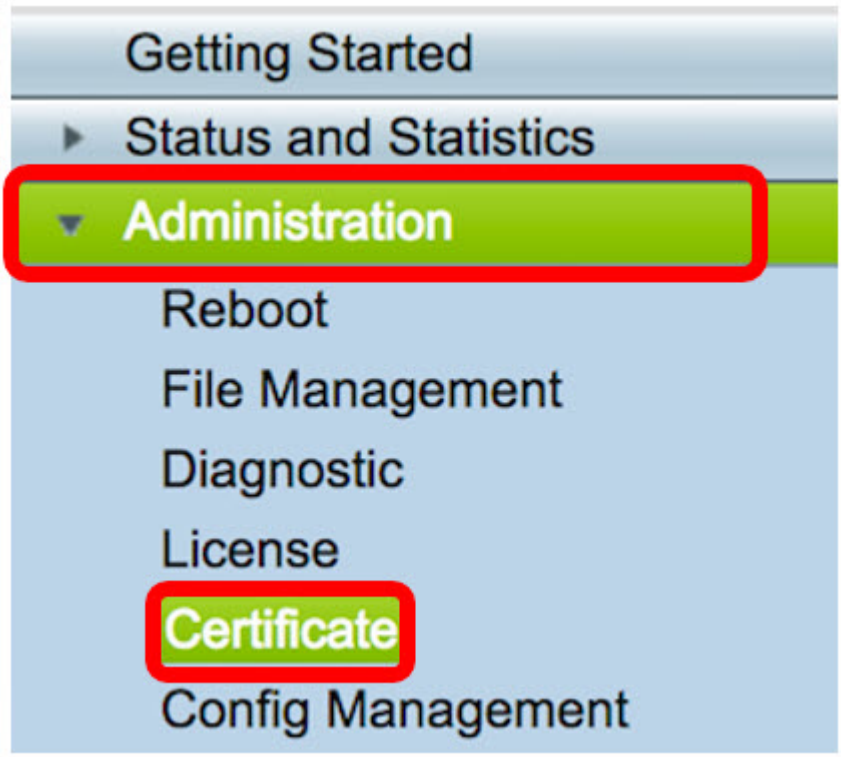
Softwareversie

- 1.0.01.17

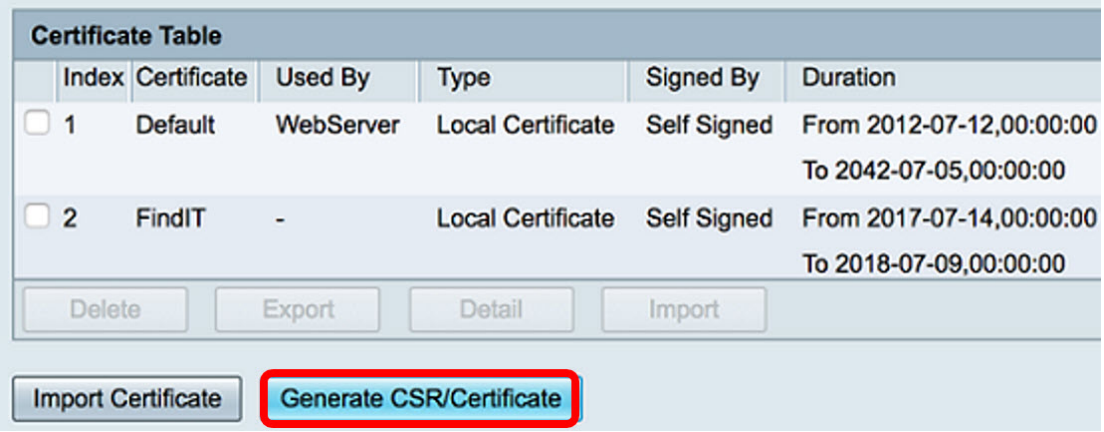
Vervang het standaard zelfgetekende certificaat door een SSL-certificaat van 3e partijen

Een CSR genereren

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de router en kies **Administratie > Certificaat**.



Stap 2. Klik onder de knop Certificaat **genereren** op de knop **CSR/certificaat**.

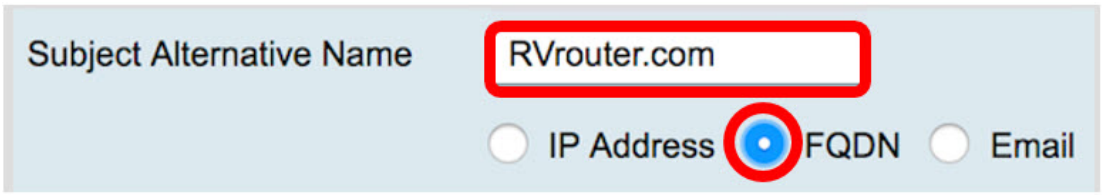


Stap 3. Klik in het venster *Generate CSR/certificaat* op de vervolgkeuzelijst *Type* en kies **de optie certificaatsignalering**.

Stap 4. Voer een naam voor het certificaat in het veld *certificaatnaam*.

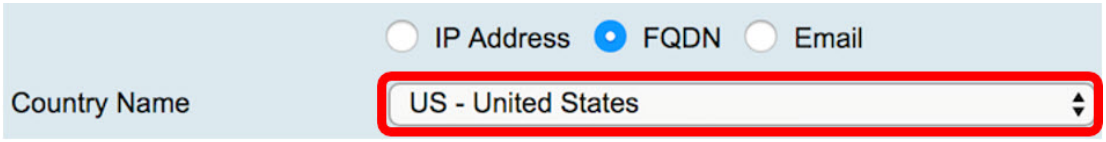
Opmerking: In dit voorbeeld wordt 34xrouter gebruikt.

Stap 5. Voer een alternatieve naam in het veld *Alternatieve naam* in *Onderwerp* en klik vervolgens op de radioknop **FQDN** hieronder om aan te passen. De alternatieve naam zal de domeinnaam zijn die kan worden gebruikt om tot de router toegang te krijgen.



Opmerking: In dit voorbeeld wordt RVrouter.com gebruikt.

Stap 6. Klik op de vervolgkeuzelijst *Landnaam* om het land van uw locatie te kiezen.

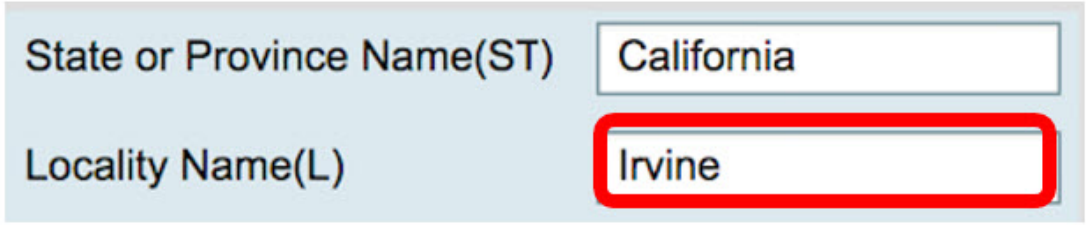


Opmerking: In dit voorbeeld worden de Verenigde Staten en de Verenigde Staten gekozen.

Stap 7. Voer de naam van de staat of provincie in het veld *Naam of provincie (ST)*.

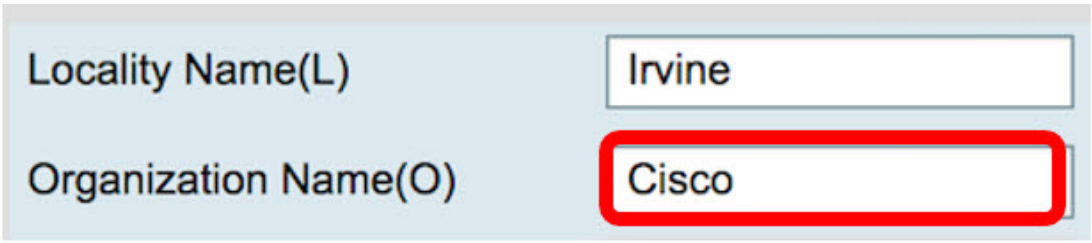
Opmerking: In dit voorbeeld wordt Californië gebruikt.

Stap 8. Voer de localiteit in het veld *Locality Name(L)*.



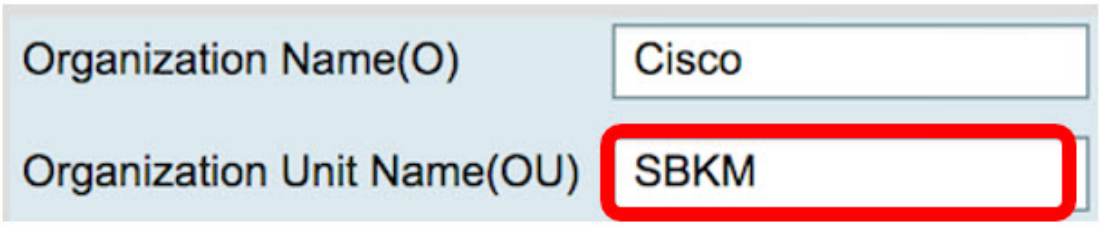
Opmerking: In dit voorbeeld wordt Irvine gebruikt.

Stap 9. Voer in het daarvoor bestemde veld de naam van de organisatie in.



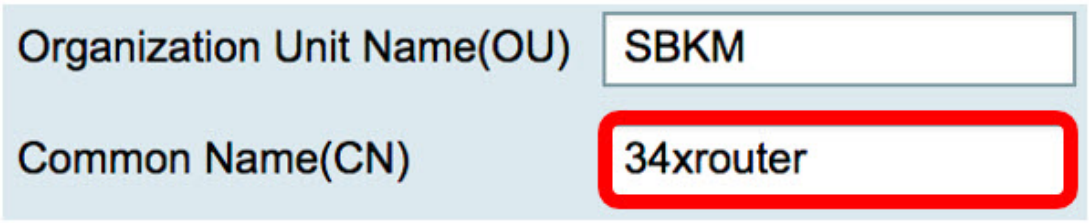
Opmerking: In dit voorbeeld wordt Cisco gebruikt.

Stap 10. Voer in het daarvoor bestemde veld de naam van de organisatie-eenheid in.



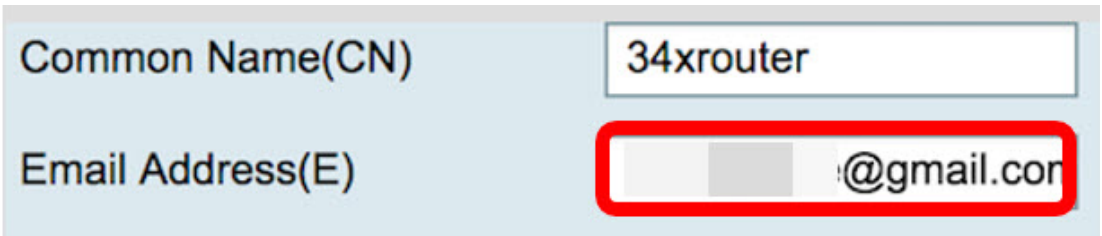
Opmerking: In dit voorbeeld wordt SBKM gebruikt.

Stap 1. Voer een naam in het veld *Gemeenschappelijke naam (GN)* in.



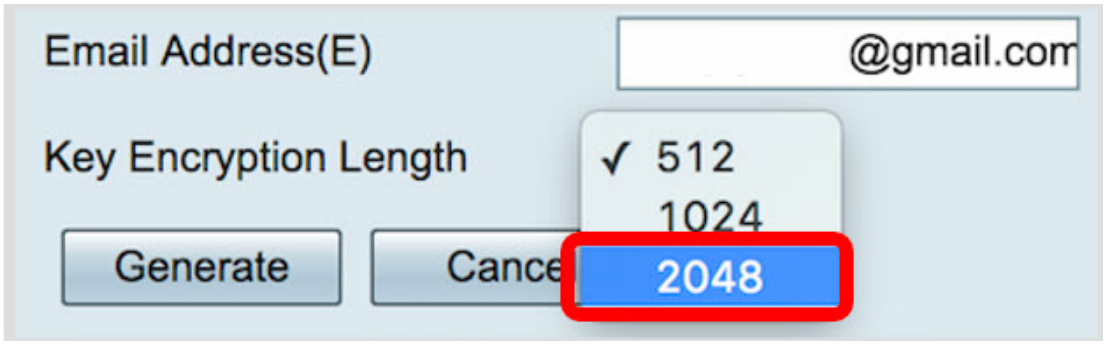
Opmerking: In dit voorbeeld wordt 34xrouter gebruikt.

Stap 12. Voer uw e-mailadres of een e-mailadres in waar u wilt dat het certificaat wordt verzonden.



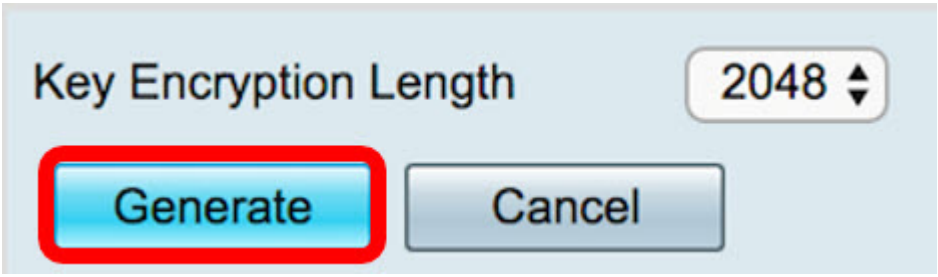
Opmerking: In dit voorbeeld wordt een e-mailadres gmail.com gebruikt.

Stap 13. Kies een *toetstitel* met *encryptie* uit het vervolgkeuzemenu om het aantal bits in uw sleutel in te stellen. De standaardlengte is 512.



Opmerking: In dit voorbeeld wordt 2048 gebruikt. Dit wordt ten zeerste aanbevolen, omdat een langere encryptie moeilijker te decoderen is dan kortere sleutels, waardoor deze veiliger is.

Stap 14. Klik op **Generate**.

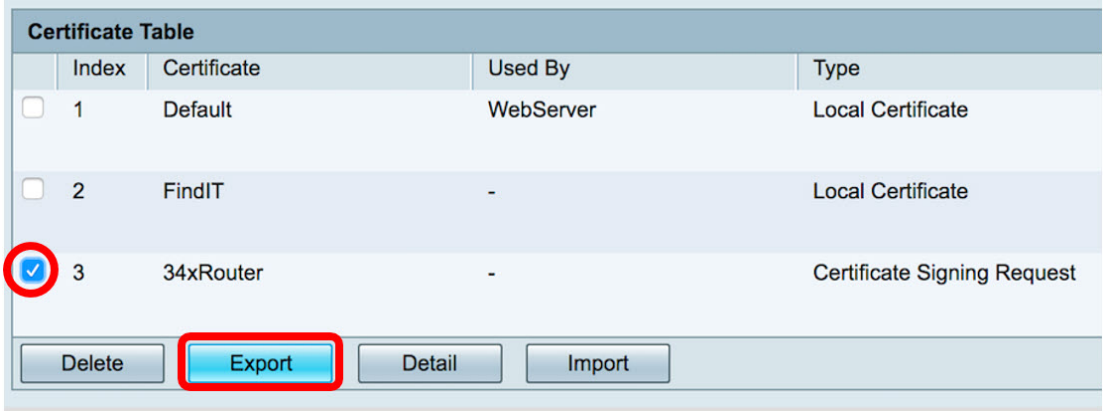


Het certificaatverzoek dat u hebt gemaakt, wordt nu in de certificaattabel weergegeven.

U hebt nu met succes een CSR gegenereerd.

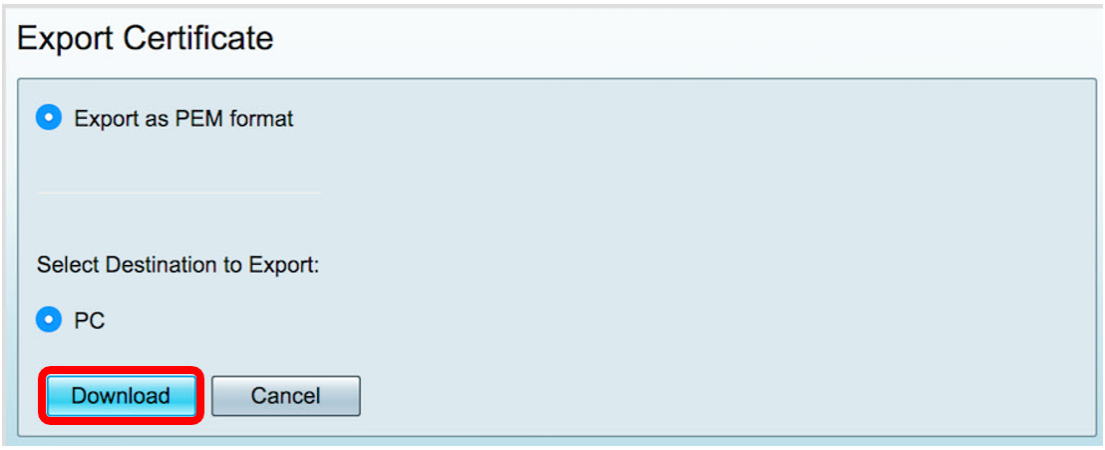
CSR exporteren

Stap 1. Controleer het vakje naast het certificaatverzoek in de certificaattabel en klik op **Exporteren**.



Stap 2. Klik op **Downloaden** in het venster *Exportcertificaat* om het bestand in uw computer

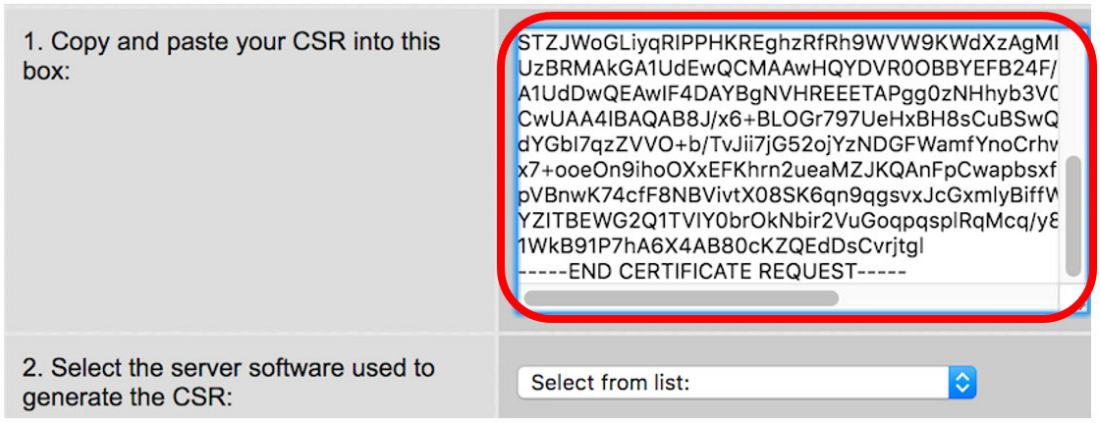
in PEM-indeling te downloaden.



U hebt de CSR nu naar uw computer geëxporteerd.

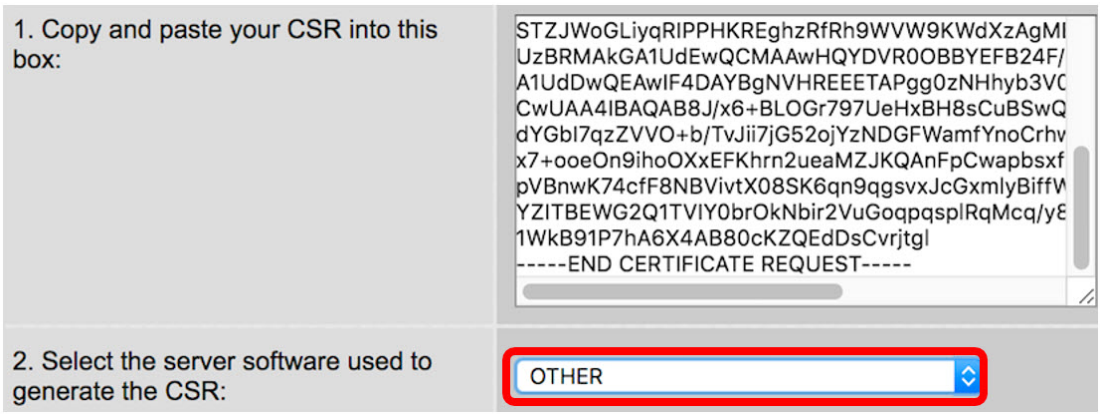
CSR uploaden naar de certificaatprovider

Stap 1. Open het gedownload bestand met een notebook, en kopieer de CSR vervolgens door het op te plakken in het veld dat op de website van de derde partij SSL-certificatieprovider is meegeleverd.



Opmerking: In dit voorbeeld wordt Comodo.com gebruikt als verstrekker van het certificaat.

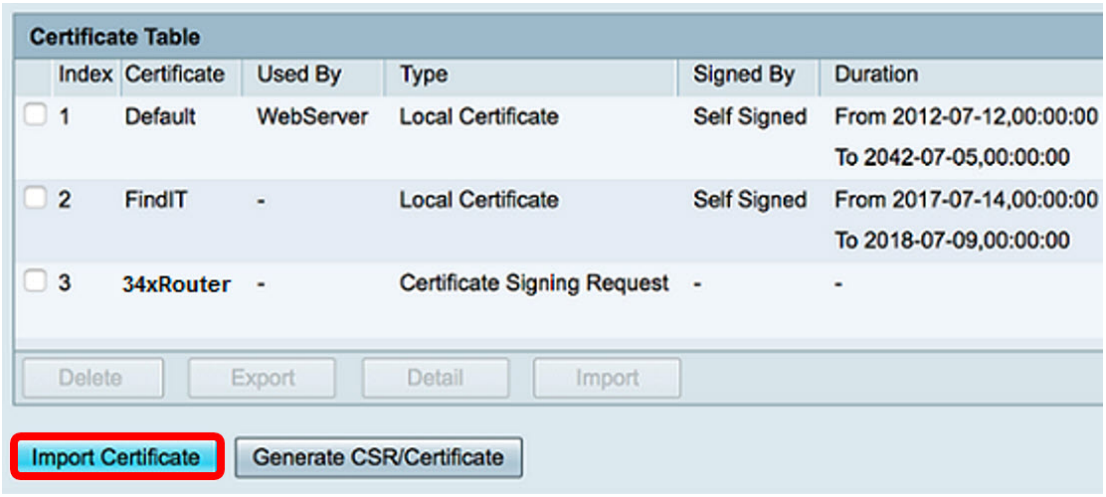
Stap 2. Selecteer de serversoftware die wordt gebruikt om de CSR te genereren. In dit geval, omdat de RV34x-router niet in de lijst staat, wordt er een andere gekozen.



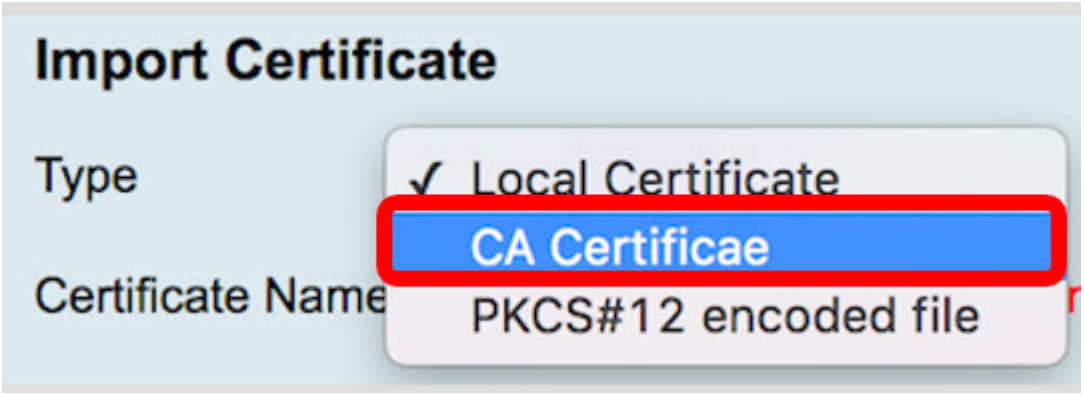
Stap 3. Download uw certificaat in uw computer.

Het certificaat van de 3e SSL-partij uploaden

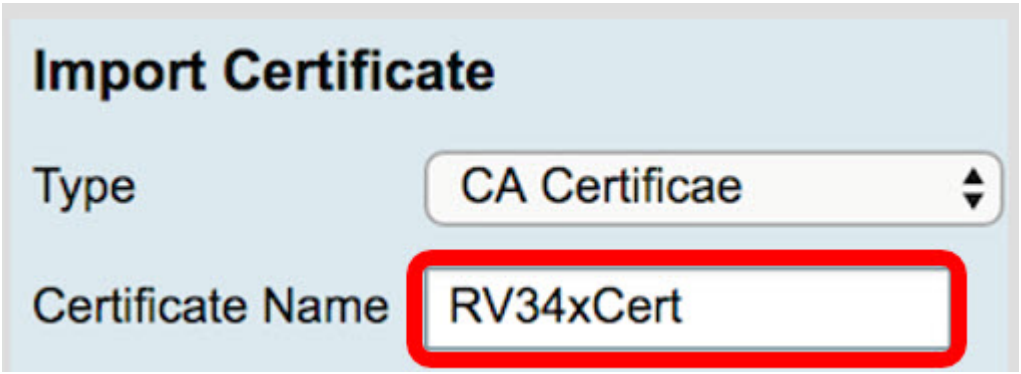
Stap 1. Klik in het op web gebaseerde hulpprogramma van de router op de knop **Importeren** onder de **knop** Certificaat.



Stap 2. Klik in het venster *Importeren* op het vervolgkeuzemenu *Type* en kies **CA-certificaat**.

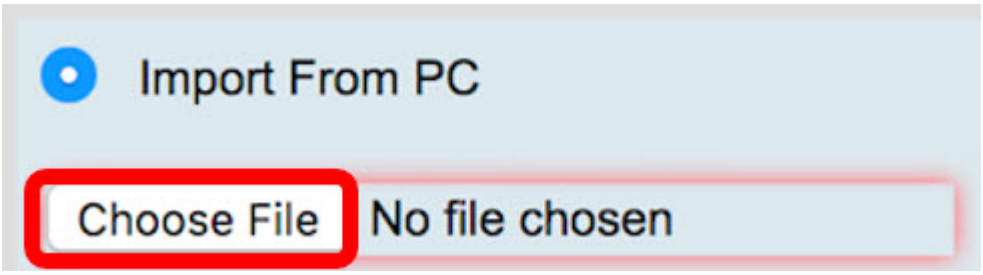


Stap 3. Voer in het daarvoor bestemde veld een certificaatnaam in.

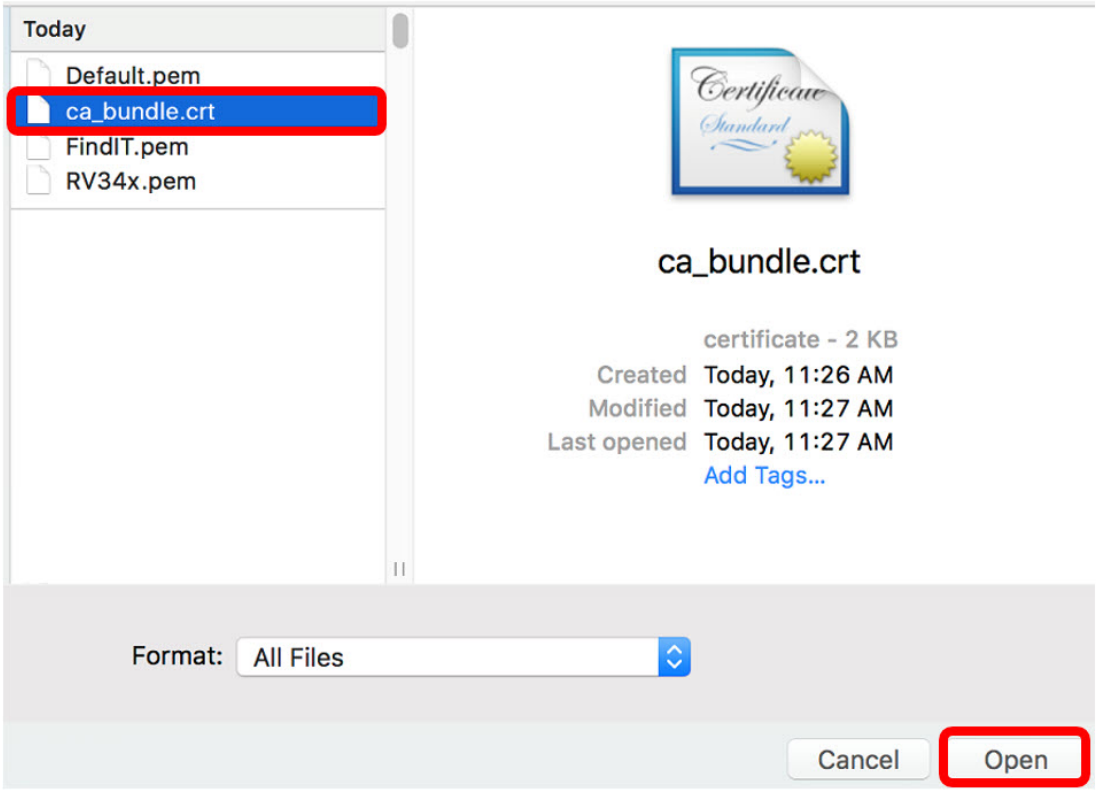


Opmerking: In dit voorbeeld wordt RV34xCert gebruikt.

Stap 4. Klik op de knop **Bestand kiezen** en plaats het certificeringsbestand dat u hebt gedownload van de CA.

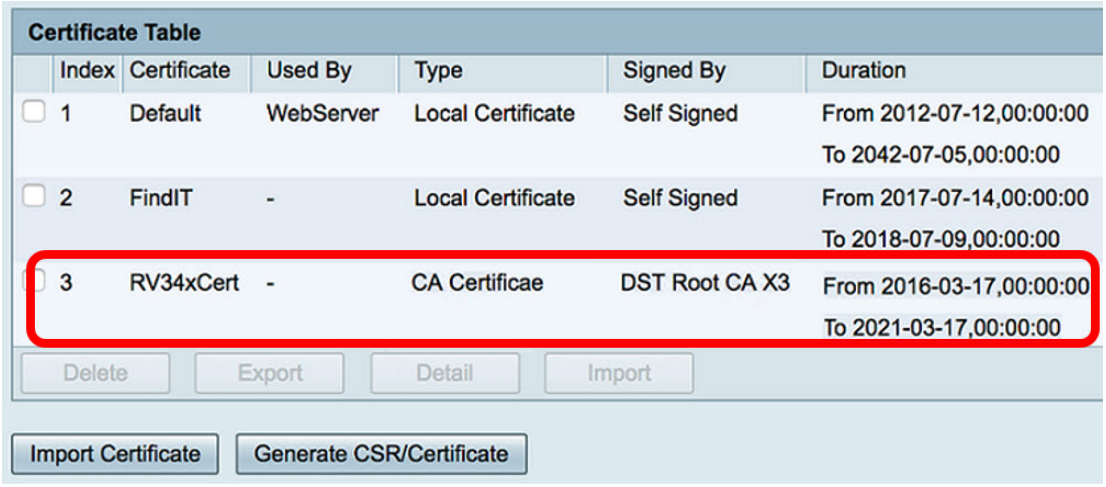


Stap 5. Klik op het bestand en vervolgens op **Openen**.



Stap 6. Klik op **Upload**.

De certificaattabel toont nu de nieuwe certificaatnaam en het type wordt nu vervangen door een CA-certificaat met het label dat door de CA van de derde partij is ondertekend.

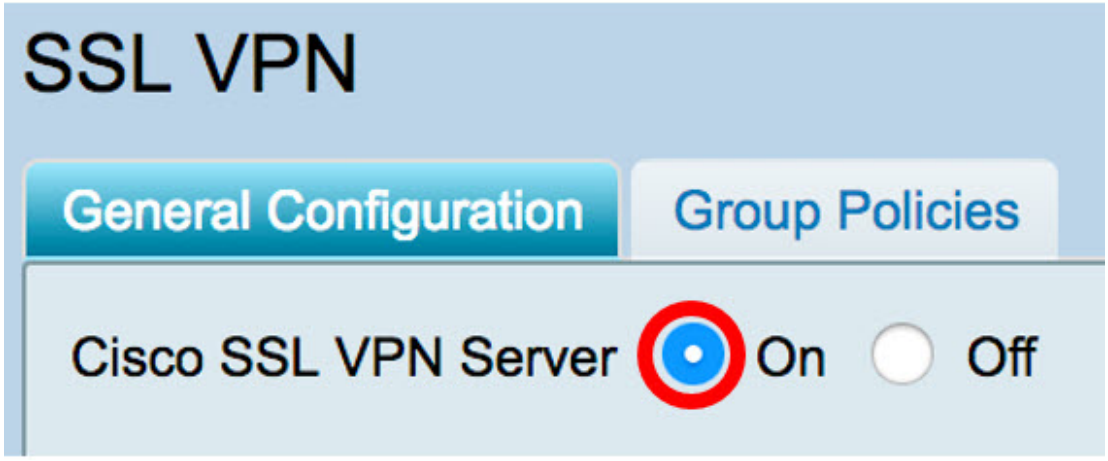


U hebt nu met succes een 3rd party SSL-certificaat op de RV34x-router geüpload.

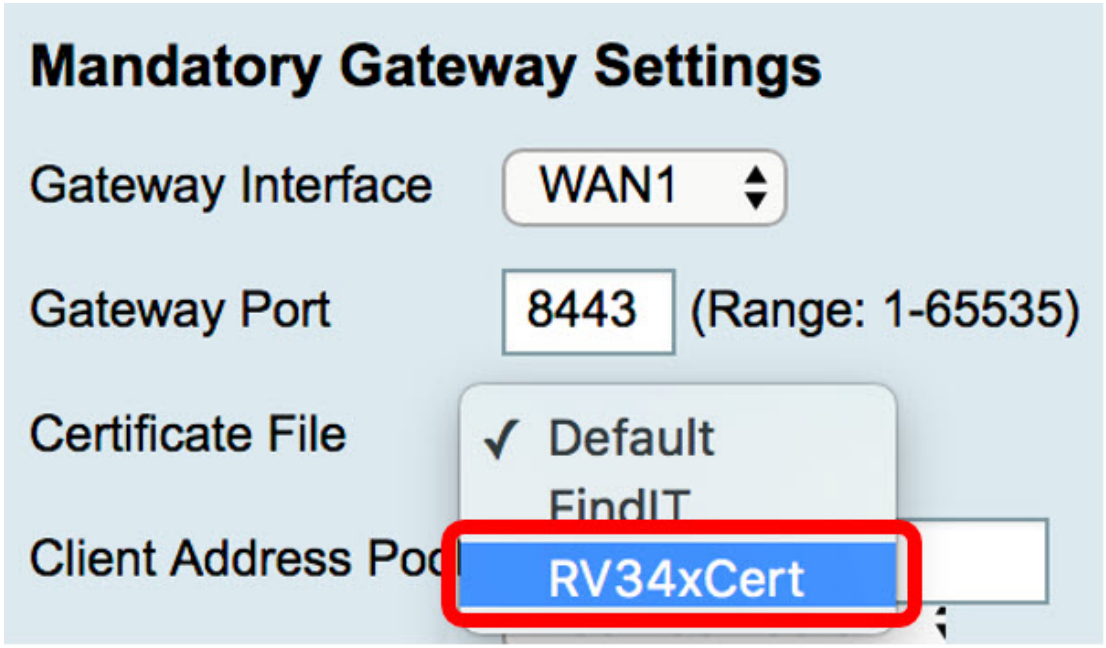
Vervang het standaard zelfgetekende certificaat

Stap 1. Kies in het web-gebaseerde hulpprogramma **VPN > SSL VPN**.

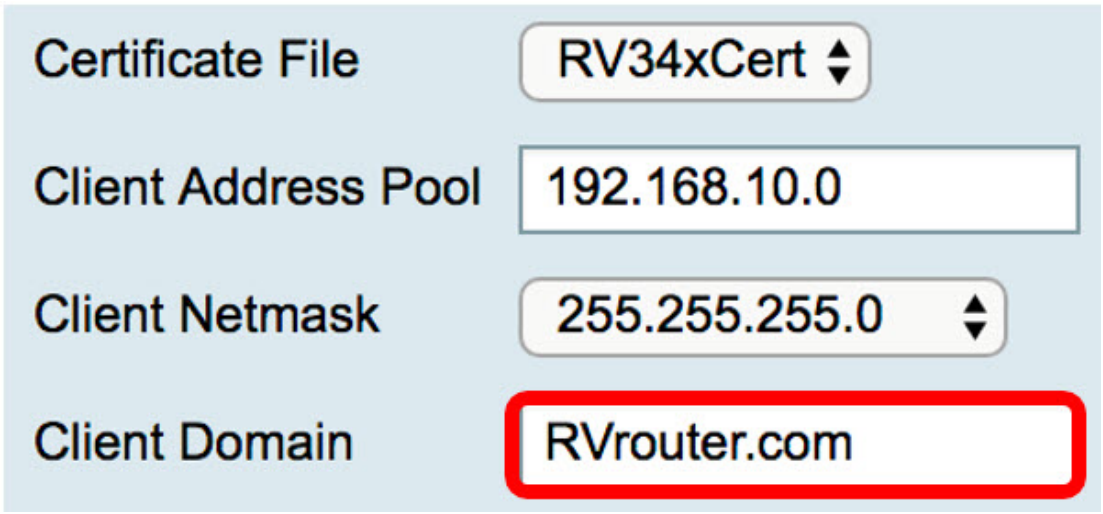
Stap 2. Klik op het radioknop **On** om de Cisco SSL VPN-server in te schakelen.



Stap 3. Klik onder Verplicht naar Gateway-instellingen op het vervolgkeuzemenu *certificaatbestand* en vervang het standaardcertificaat door het nieuwe geüploade SSL-certificaat te kiezen.

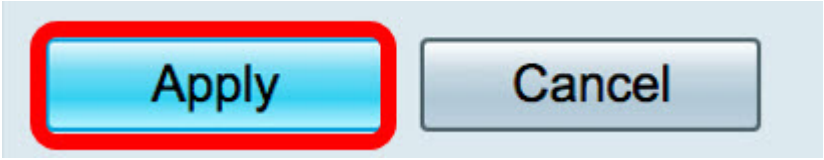


Stap 4. Voer in het daarvoor bestemde veld het gewenste clientdomein in.



Opmerking: In dit voorbeeld wordt RVrouter.com gebruikt.

Stap 5. Klik op **Toepassen**.



U hebt nu met succes het standaard zelfgetekende certificaat vervangen door het 3rd party SSL-certificaat.

Mogelijk vindt u dit artikel ook informatief: RV34x Series router vaak gestelde vragen (FAQ's)

Deze site biedt verschillende links naar andere artikelen die u interessant kunt vinden: RV34x Series routerpagina