Certificaat (Importeren/Exporteren/Generate CSR) op RV160 en RV260 Series router

Doel

Dit document heeft tot doel u te laten zien hoe u een certificaataanvraag (CSR) kunt genereren, evenals certificaten te importeren en uitvoeren op de RV160- en RV260-Series routers.

Inleiding

Digitale certificaten zijn belangrijk in het communicatieproces. Het biedt digitale identificatie voor authenticatie. Een digitaal certificaat bevat informatie die een apparaat of gebruiker identificeert, zoals de naam, het serienummer, het bedrijf, de afdeling of het IP-adres.

Certificeringsinstanties (CA) zijn vertrouwde instanties die "tekenen" van certificaten om de authenticiteit ervan te controleren, hetgeen de identiteit van de machine of gebruiker garandeert. Het zorgt ervoor dat de certificaathouder werkelijk is wie hij beweert te zijn. Zonder een betrouwbaar ondertekend certificaat kunnen gegevens worden versleuteld, maar het onderwerp waarmee u communiceert is niet degene die u denkt. CA gebruikt PKI (Public Key Infrastructure) bij de uitgifte van digitale certificaten, die gebruik maakt van openbare sleutel of privé-sleutelencryptie om beveiliging te waarborgen. CA's zijn verantwoordelijk voor het beheer van certificaataanvragen en de afgifte van digitale certificaten. Een paar voorbeelden van CA zijn: IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verising en nog veel meer.

Certificaten worden gebruikt voor Secure Socket Layer (SSL), Transport Layer Security (TLS), Datagram TLS (DTLS)-verbindingen, zoals Hypertext Transfer Protocol (HTTPS) en Secure Lichtgewicht Directory Access Protocol (LDAPS).

Toepasselijke apparaten

RV160

RV260

Softwareversie

•1.0.00.15

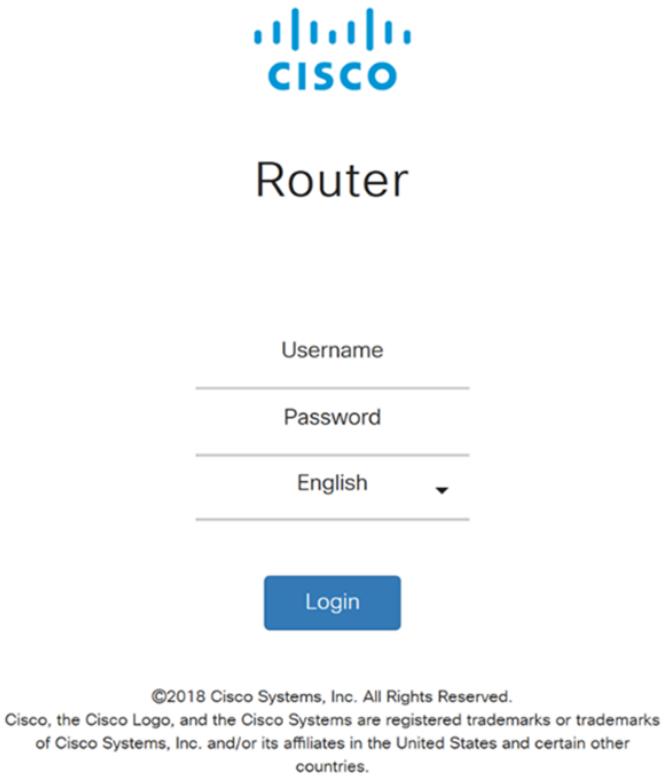
Inhoud

Via dit artikel zult u:

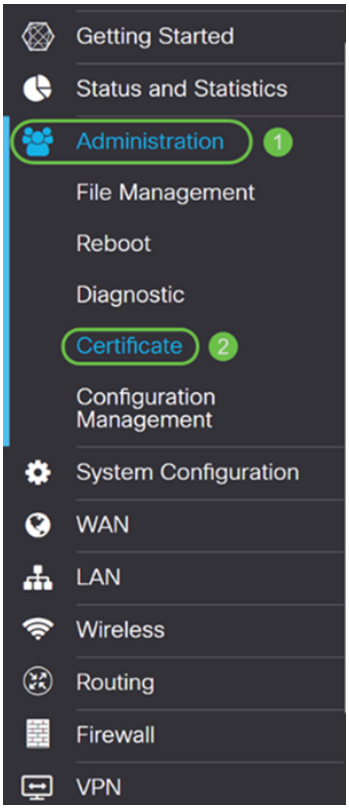
1. CSR/certificaat genereren
2. Certificaat bekijken

CSR/certificaat genereren

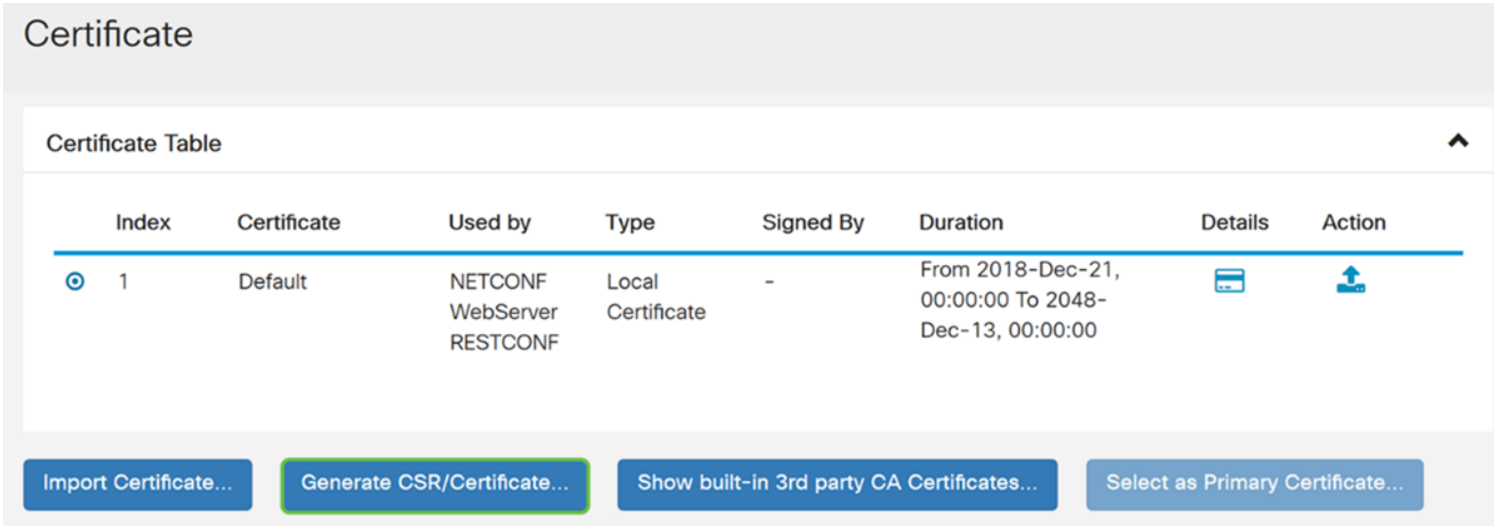
Stap 1. Meld u aan bij de webconfiguratie.



Stap 2. Navigeer naar **Administratie > Certificaat**.



Stap 3. Klik op de knop **CSR/certificaat genereren**..



Stap 4. Selecteer het type certificaat dat u wilt genereren uit een van de volgende opties in de vervolgkeuzelijst.

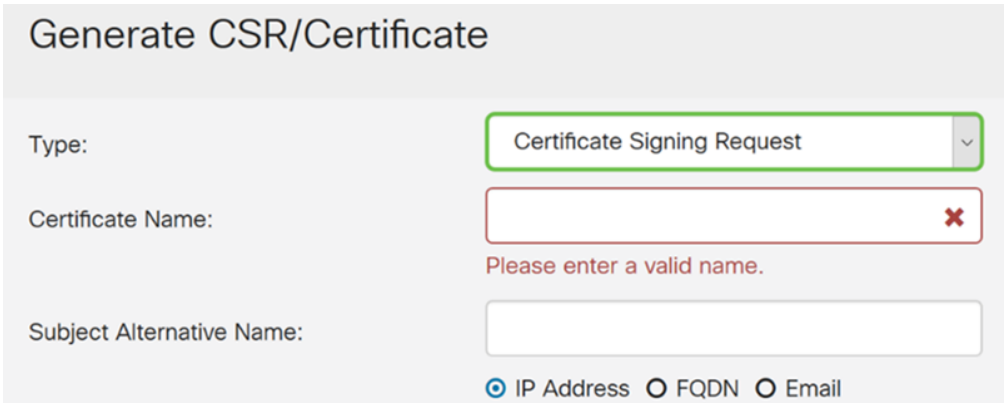
Zelfondertekend certificaat - Dit is een Secure Socket Layer (SSL) certificaat dat door zijn eigen maker wordt ondertekend. Dit certificaat is minder betrouwbaar, omdat het niet kan worden geannuleerd als de privétoets op een of andere manier door een aanvaller wordt gecompromitteerd. U moet de geldige duur in dagen opgeven.

CA-certificaat - Selecteer dit certificeringstype om uw router op dezelfde manier te laten werken als een interne certificeringsinstantie en certificaten af te geven. In veiligheidsopzicht is het vergelijkbaar met een zelfondertekend certificaat. Dit kan worden gebruikt voor OpenVPN.

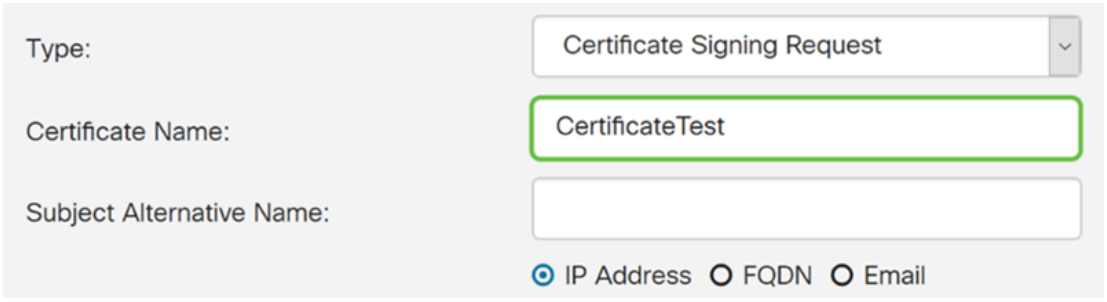
certificaataanvraag - Dit is een PKI-infrastructuur (Public Key Infrastructure) die naar de certificeringsinstantie wordt gestuurd om een digitaal identiteitsbewijs aan te vragen. Het is veiliger dan door zichzelf getekend te worden, omdat de privé-sleutel geheim gehouden wordt. Deze optie wordt aanbevolen.

Certificaat ondertekend door CA-certificaat - Selecteer dit certificeringstype en vermeld de relevante gegevens om het certificaat te laten ondertekenen door uw interne certificeringsinstantie.

In dit voorbeeld selecteren we **certificaataanvraag**.

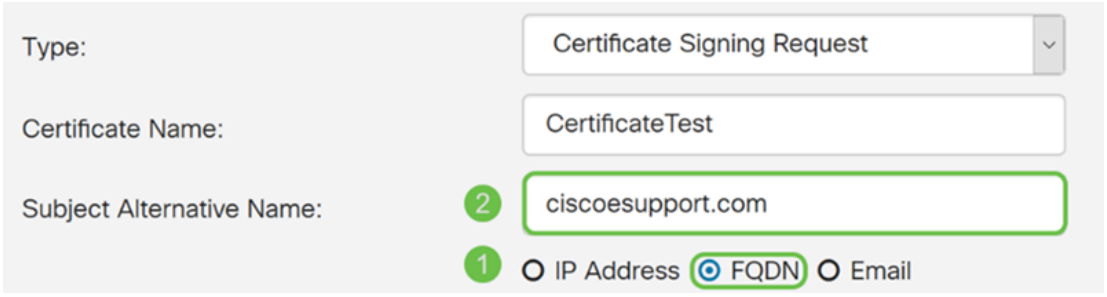


Stap 5. Voer de *certificaatnaam in*. In dit voorbeeld gaan we **certificaattest** in.

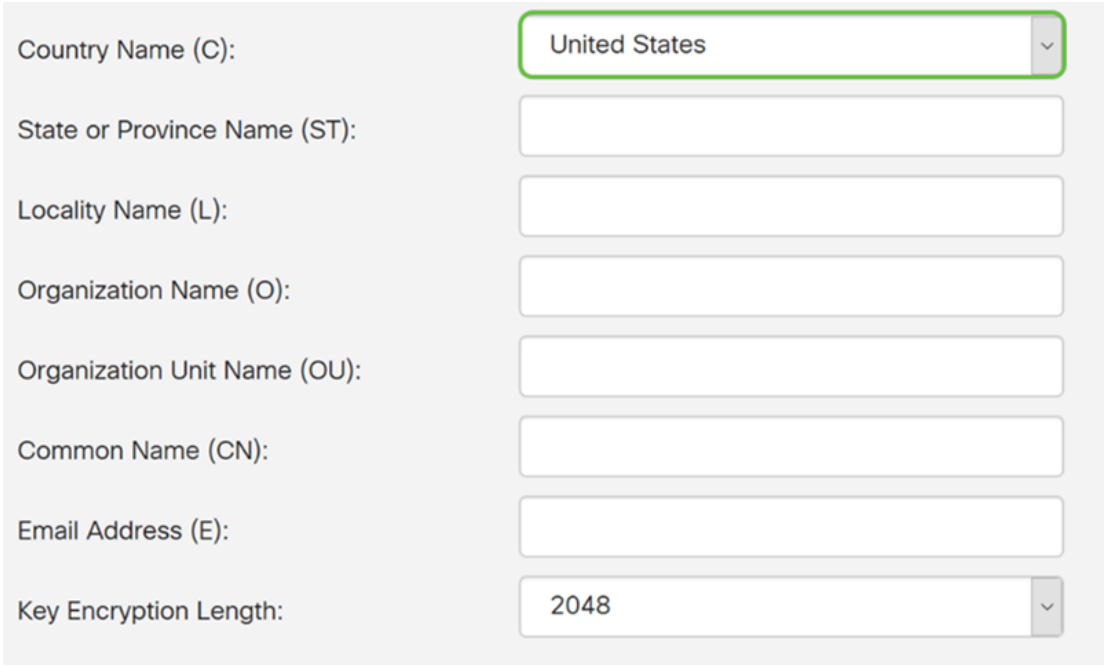


Stap 6. Selecteer in het veld *Alternatieve naam* voor onderwerp een van de volgende opties: **IP-Address**, **FQDN** (Full Qualified Domain Name) of **Email** en Voer vervolgens de juiste naam in van wat u hebt geselecteerd. In dit veld kunt u aanvullende hostnamen instellen.

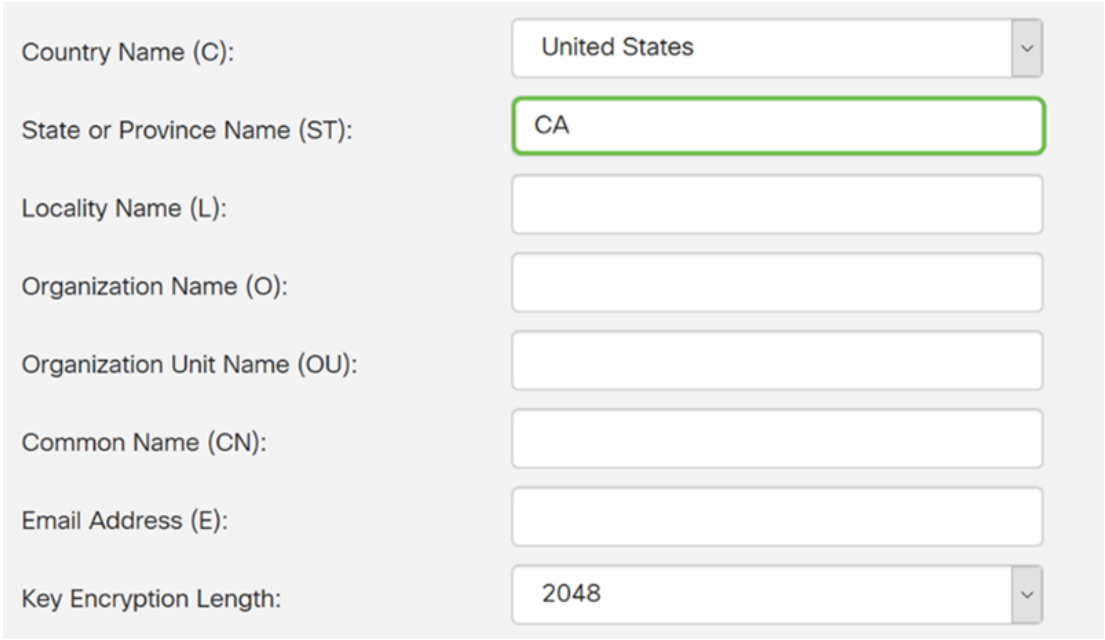
In dit voorbeeld zullen we **FQDN** selecteren en **ciscoessupport.com** invoeren.



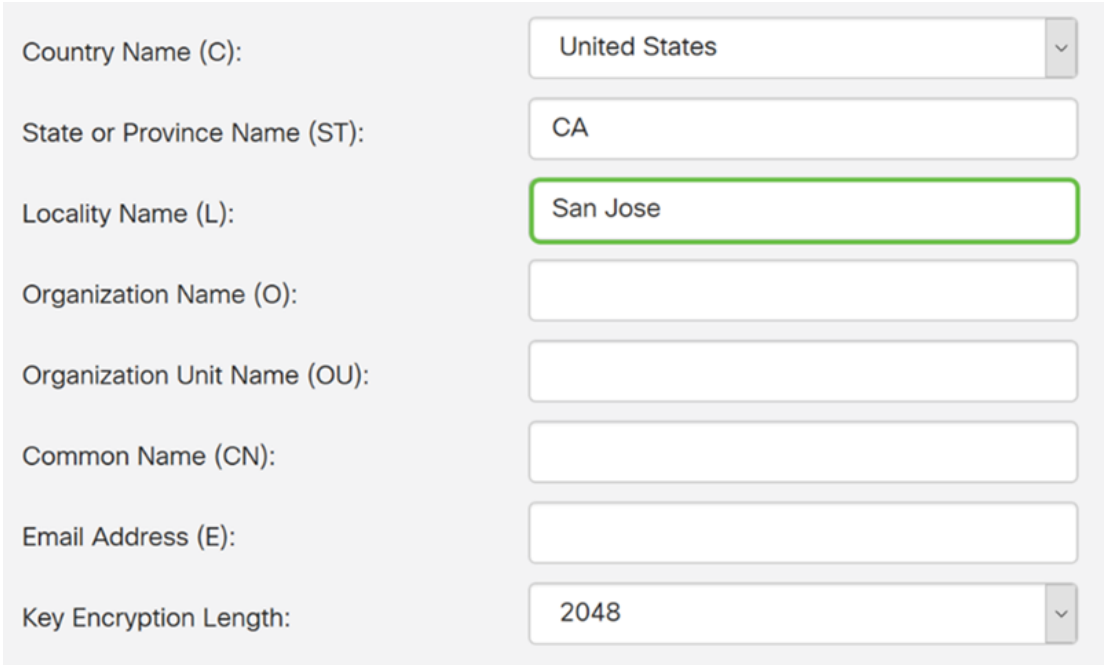
Stap 7. Selecteer een **land** in de vervolgkeuzelijst *Landnaam (C)*.



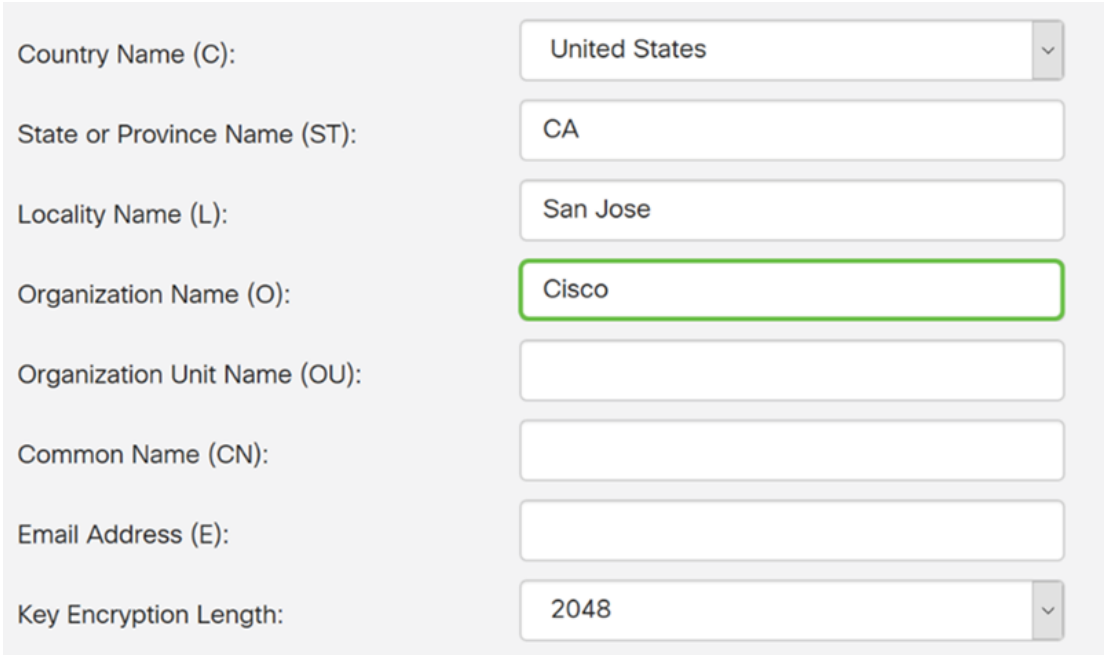
Stap 8. Voer een **naam** van de **staat** of **provincie** in het veld *Naam of provincie*.



Stap 9. Voer in de *naam Locality* een naam van een **stad in**.

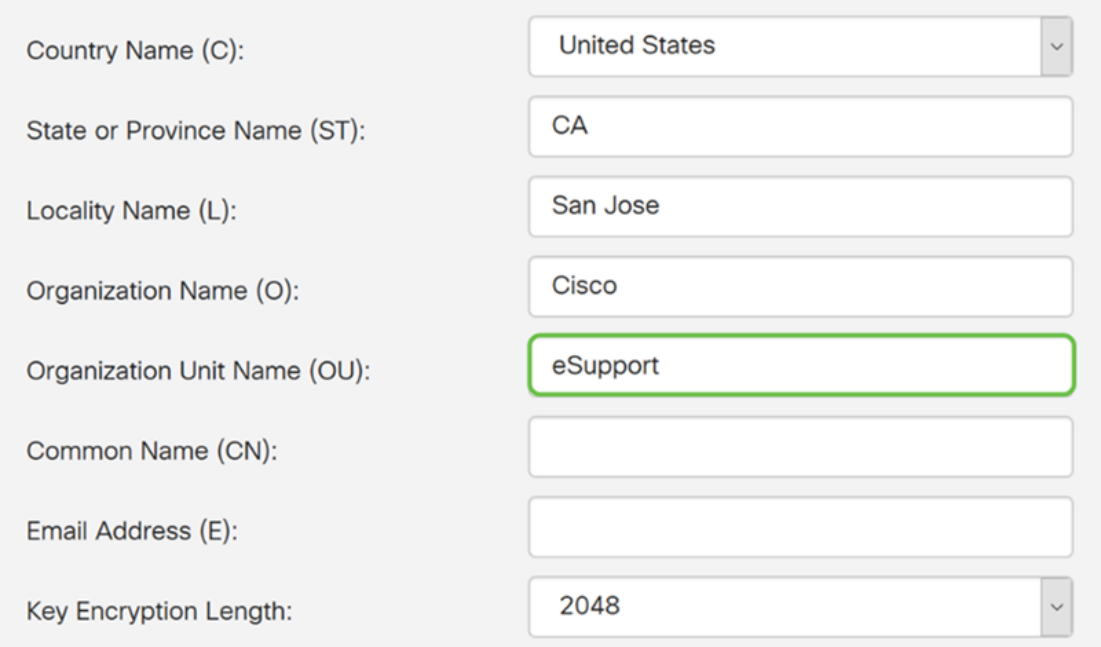


Stap 10. Voer de naam van de **organisatie** in het veld *Naam van* de *organisatie*.



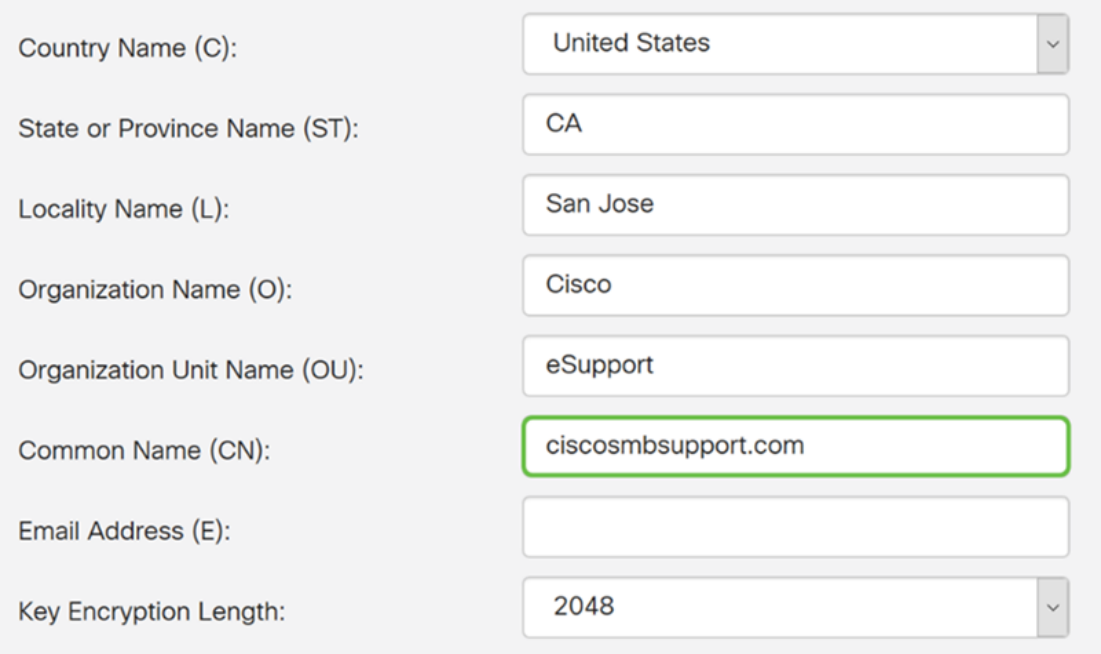
Stap 1. Voer de naam van de **organisatie-eenheid in** (bijv. training, ondersteuning, enz.).

In dit voorbeeld voeren we **eSupport** in als de naam van onze organisatie-eenheid.

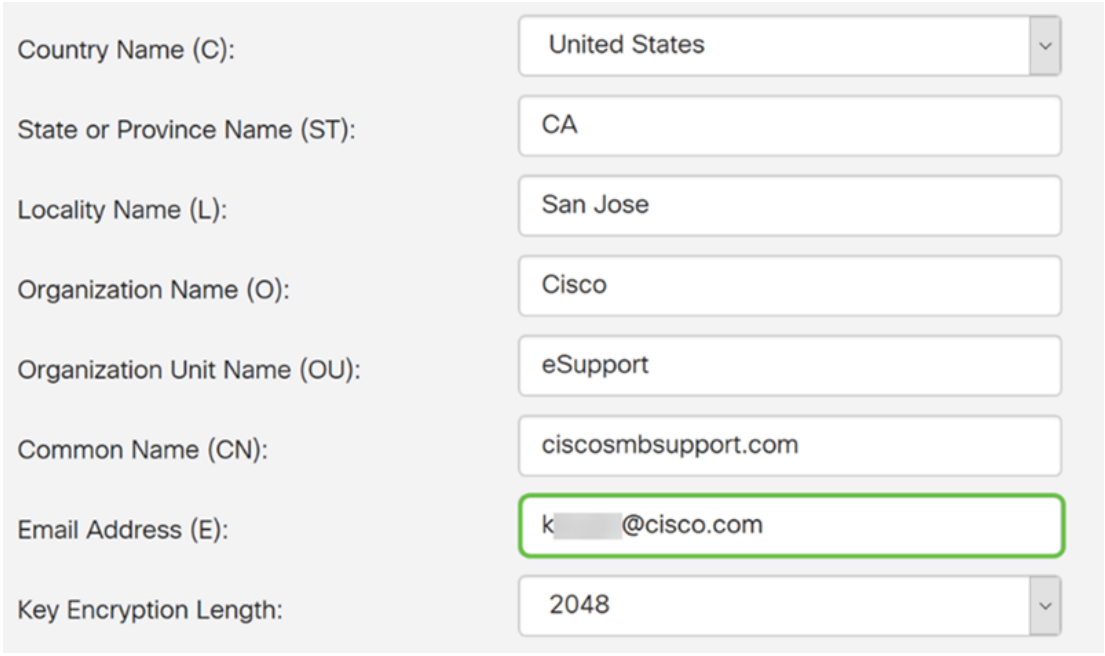


Stap 12. Voer een **gemeenschappelijke naam in**. Het is de FQDN van de webserver die dit certificaat zal ontvangen.

In dit voorbeeld werd **ciscosmbsupport.com** gebruikt als de gezamenlijke naam.

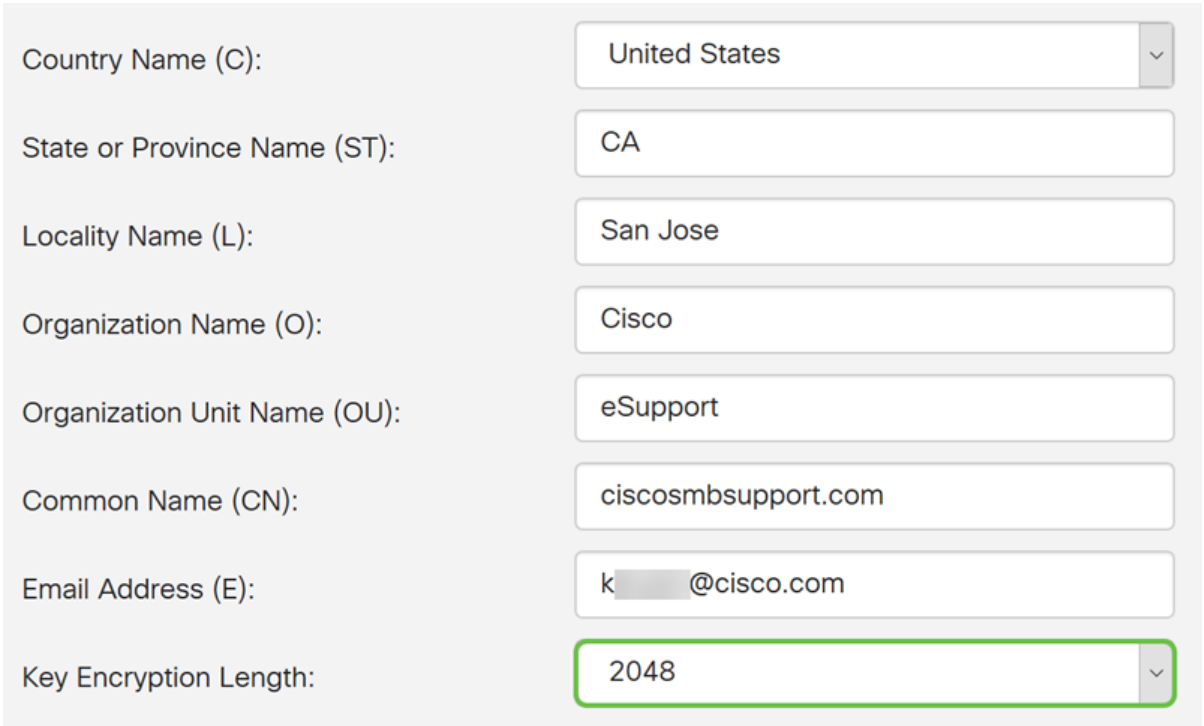


Stap 13. Voer een **e-mailadres in**.

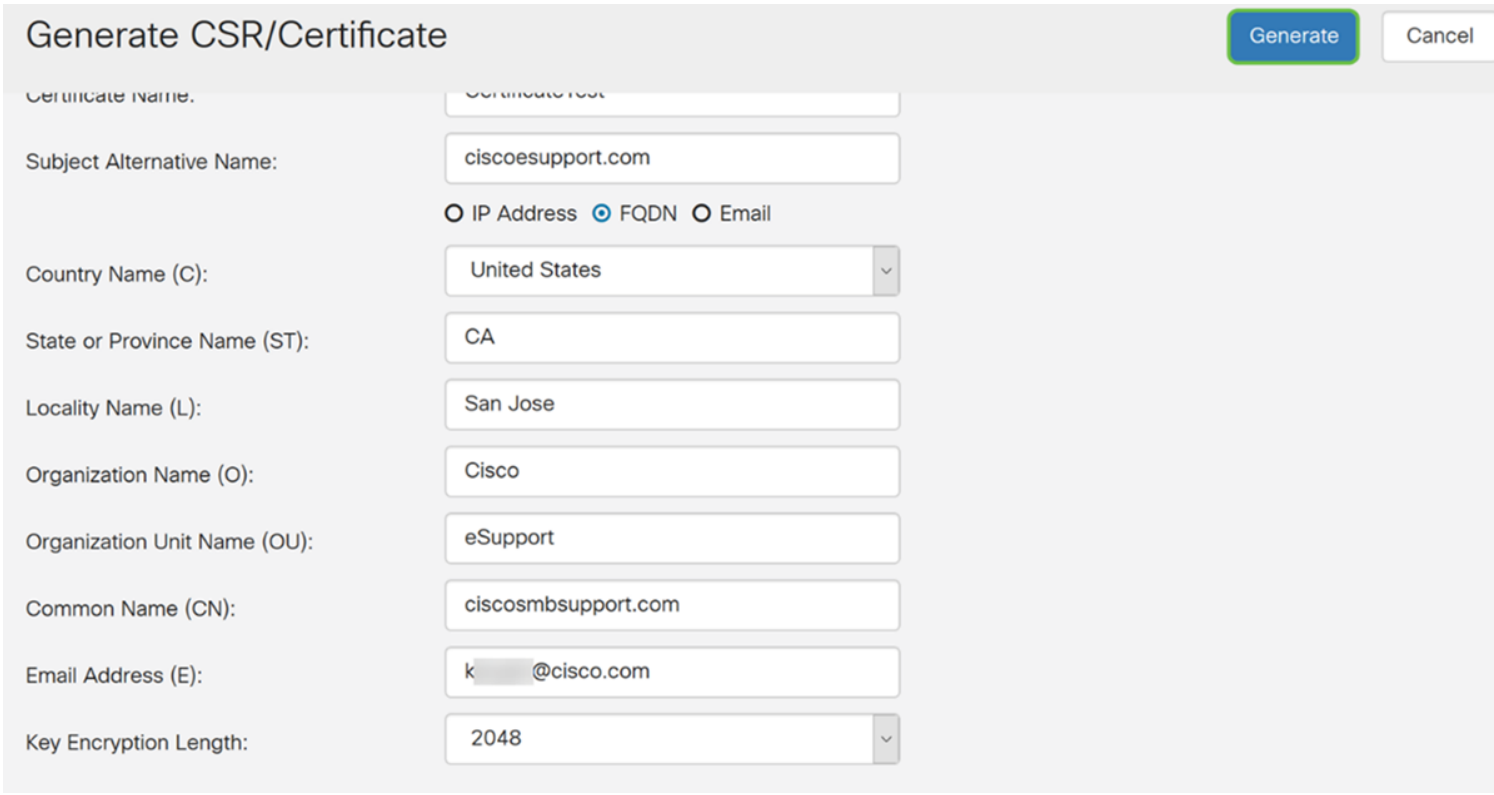


Stap 14. Selecteer de **toetstitel** tot **de encryptie-lengte** in het vervolgkeuzemenu. De opties zijn: **512**, **1024**, of **2048**. Hoe groter de sleutelgrootte, hoe veiliger het certificaat. Hoe groter de sleutelgrootte, hoe groter de verwerkingstijd.

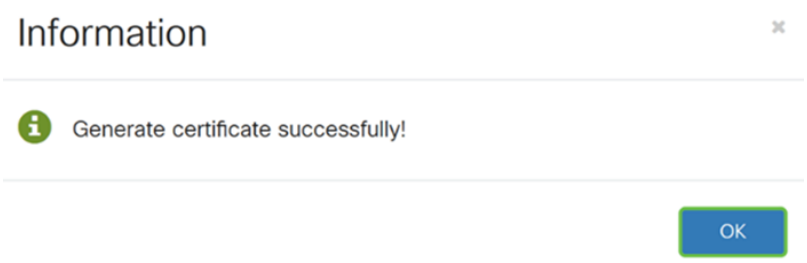
Best Practice: Het wordt aanbevolen de hoogste sleutelencryptie lengte te kiezen, wat een betere encryptie mogelijk maakt.



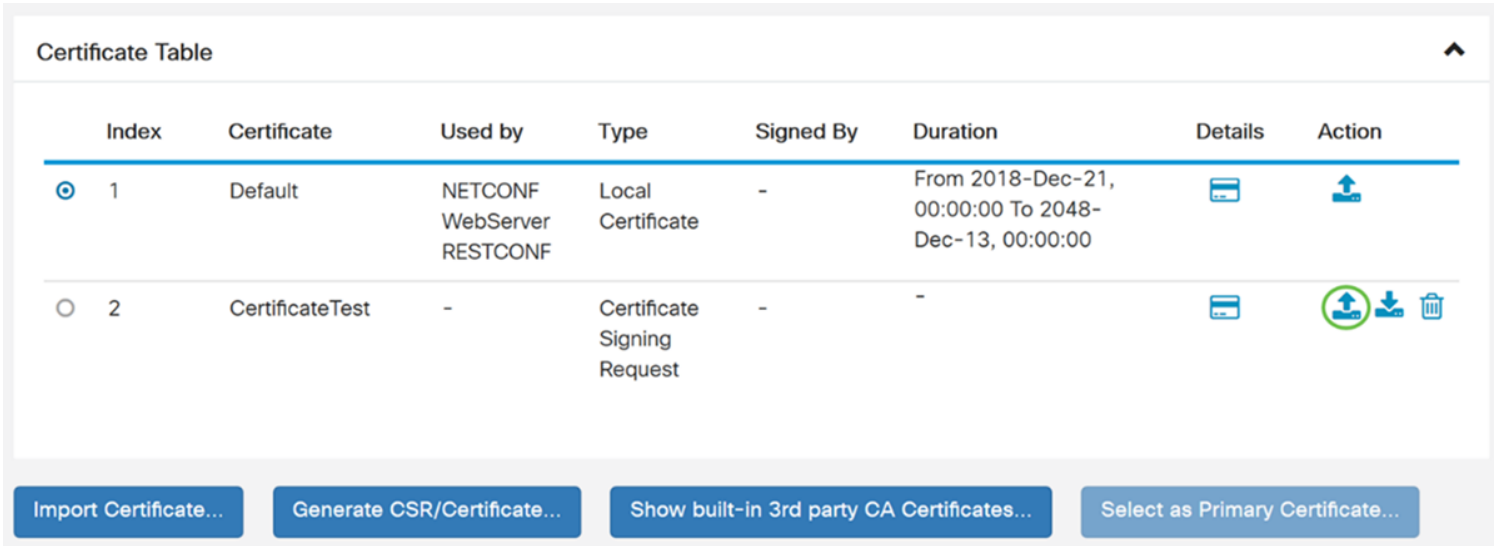
Stap 15. Klik op **Generate**.



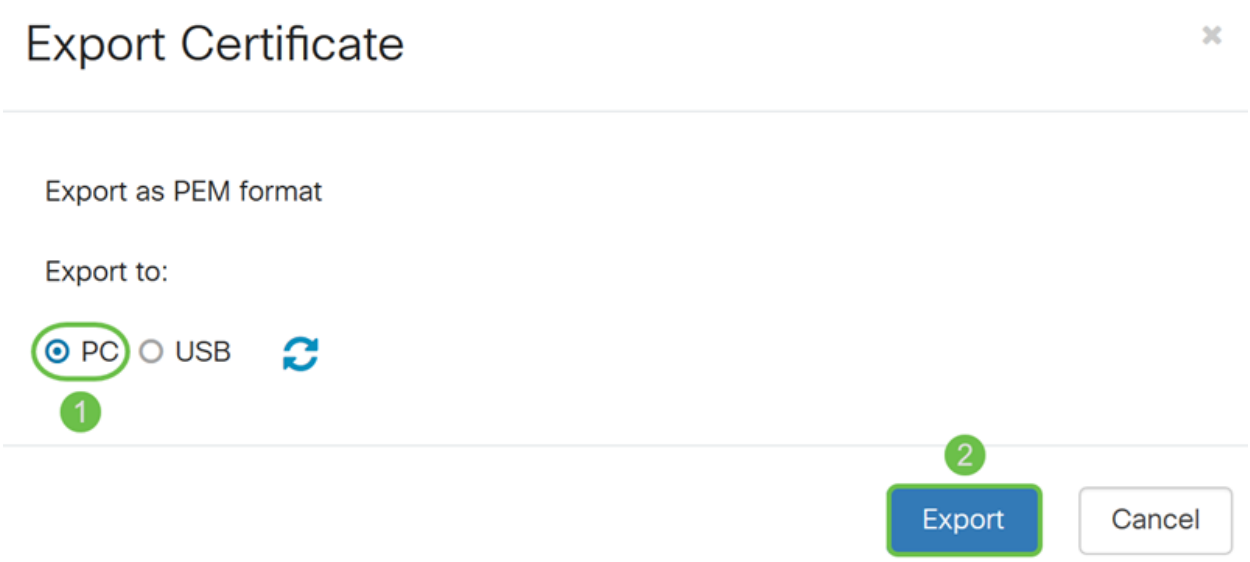
Stap 16. Er wordt *informatie* toegevoegd met een 'Generate certificaat!' bericht. Klik op **OK** om verder te gaan.



Stap 17. Exporteren van de CSR uit de *certificaattabel*.

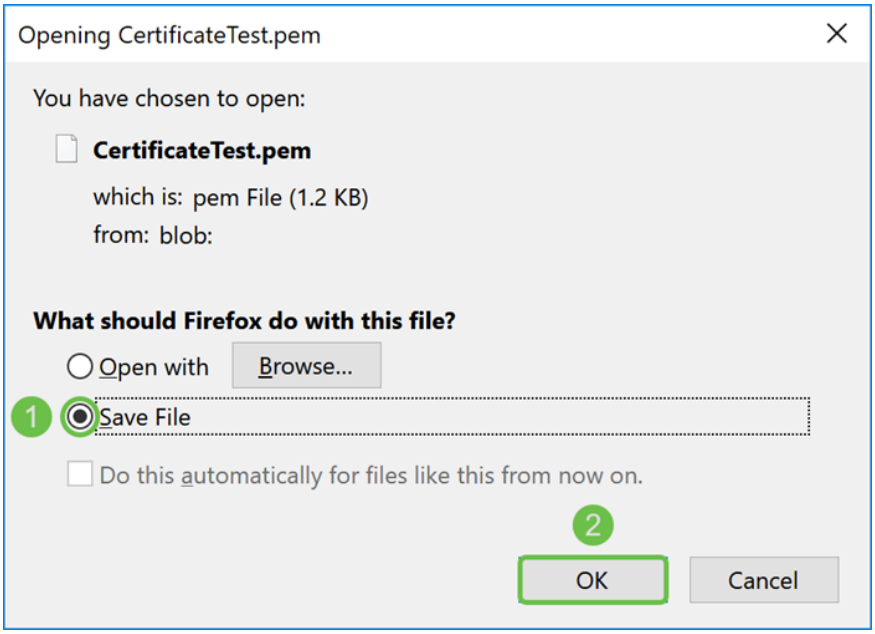


Stap 18. Er verschijnt een venster *voor* een *exportcertificaat*. Selecteer **PC** voor de *Exporteren naar* en klik vervolgens op **Exporteren**.



Stap 19. Er moet een ander venster verschijnen om te vragen of u het bestand wilt openen of opslaan.

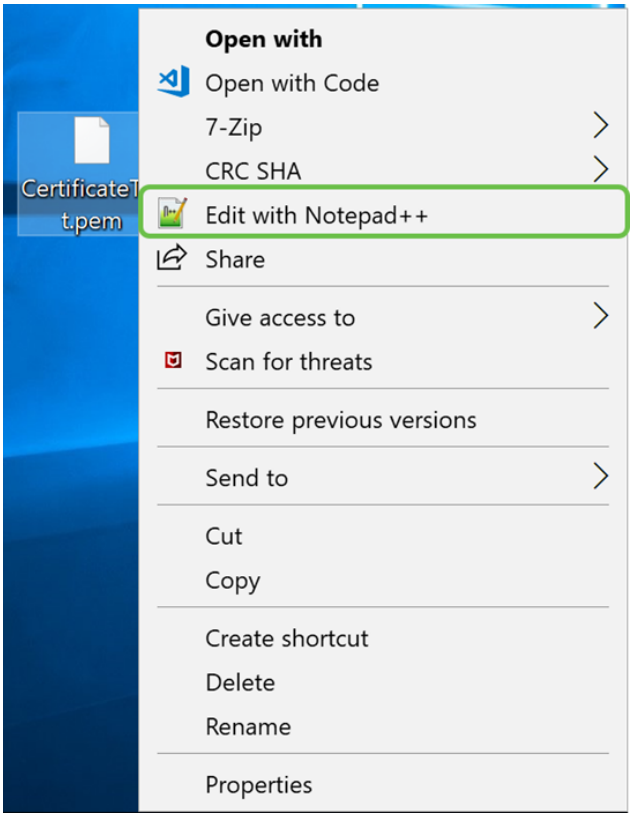
In dit voorbeeld selecteren we **Save File** en vervolgens klikt u op **OK**.



Stap 20. Zoek de locatie van waar het .pem-bestand is opgeslagen. Klik met de **rechtermuisknop op** het .pem-bestand en open het met uw favoriete teksteditor.

In dit voorbeeld openen we het .pem-bestand met Kladblok+.

Opmerking: Voel je vrij om het met Kladblok te openen.



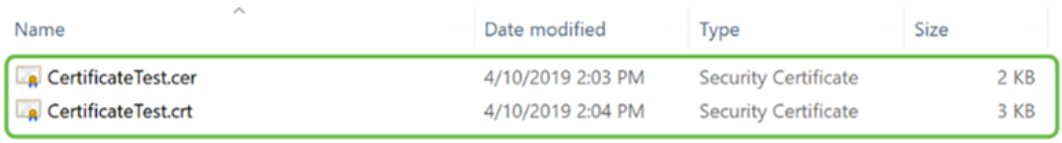
Stap 21. Zorg ervoor dat het *—BEGIN CERTIFICAATVERZOEK—* en *—EINDCERTIFICAATVERZOEK—* op de eigen regel staat.

Opmerking: Sommige onderdelen van het certificaat waren onvolledig.

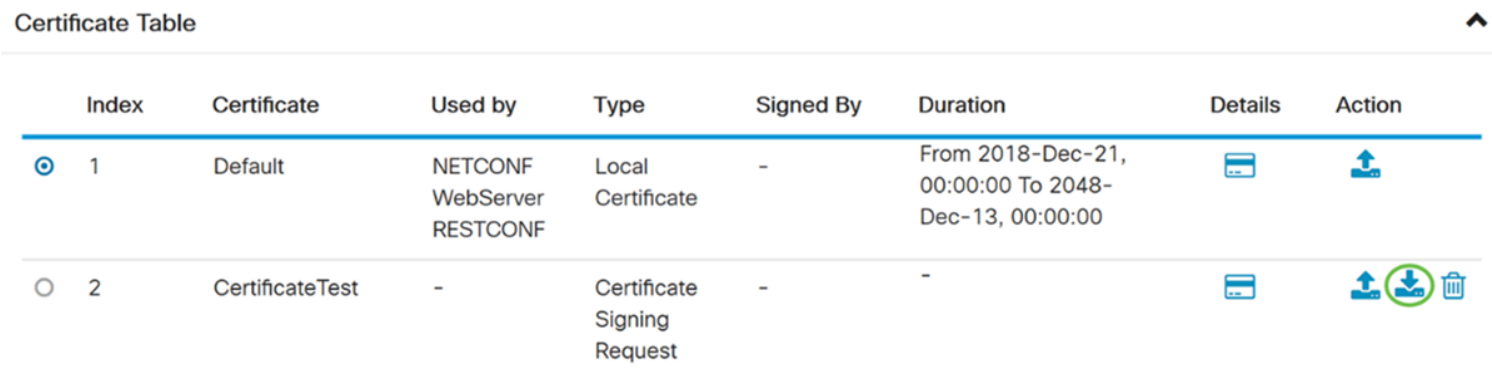
Stap 2. Wanneer u uw CSR hebt, moet u naar de ontvangende services of een certificeringsinstantie (bijvoorbeeld GoDaddy, Versiding, enz.) gaan en een certificaat aanvragen. Zodra u een verzoek hebt ingediend, zal het met de certificatenserver communiceren om te verzekeren dat er geen reden is om het certificaat niet af te geven.

Opmerking: Neem contact op met de CA- of hostinglocatie als u niet weet waar het certificaatverzoek op hun website staat.

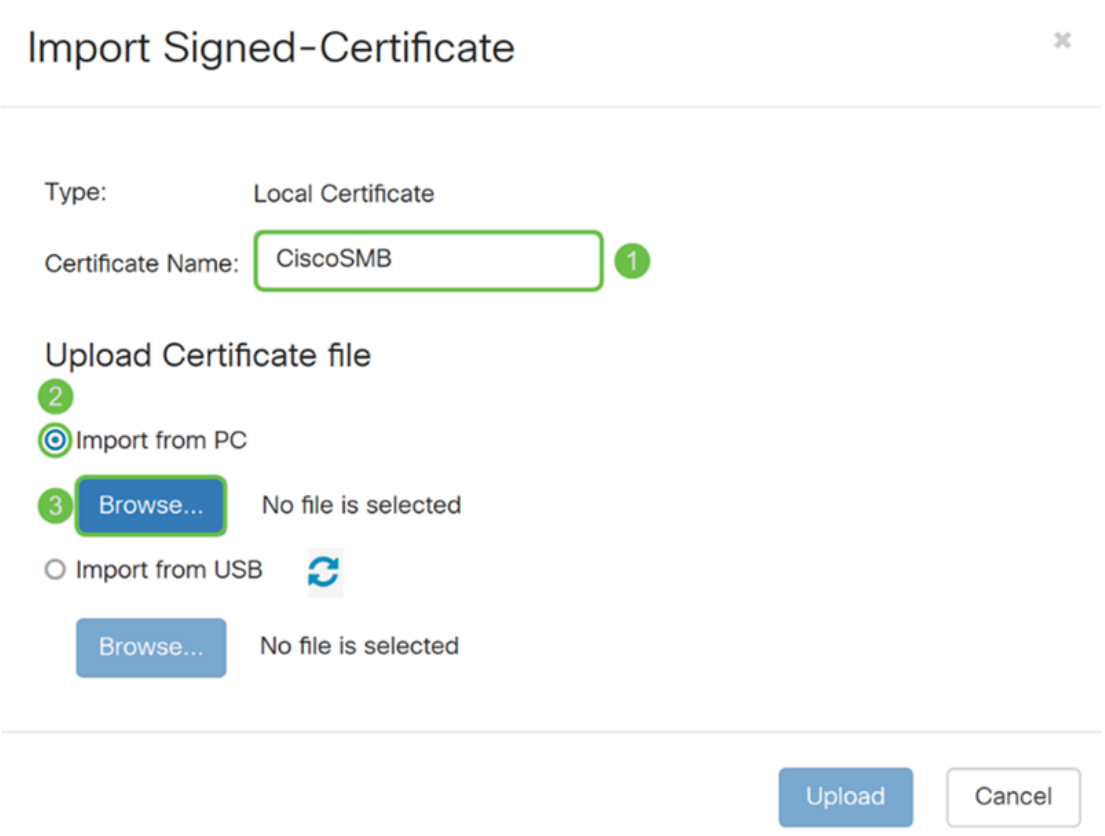
Stap 23. Download het certificaat zodra het is ingevuld. Het moet een **.cer** of **.crt** bestand zijn. In dit voorbeeld kregen we beide dossiers.



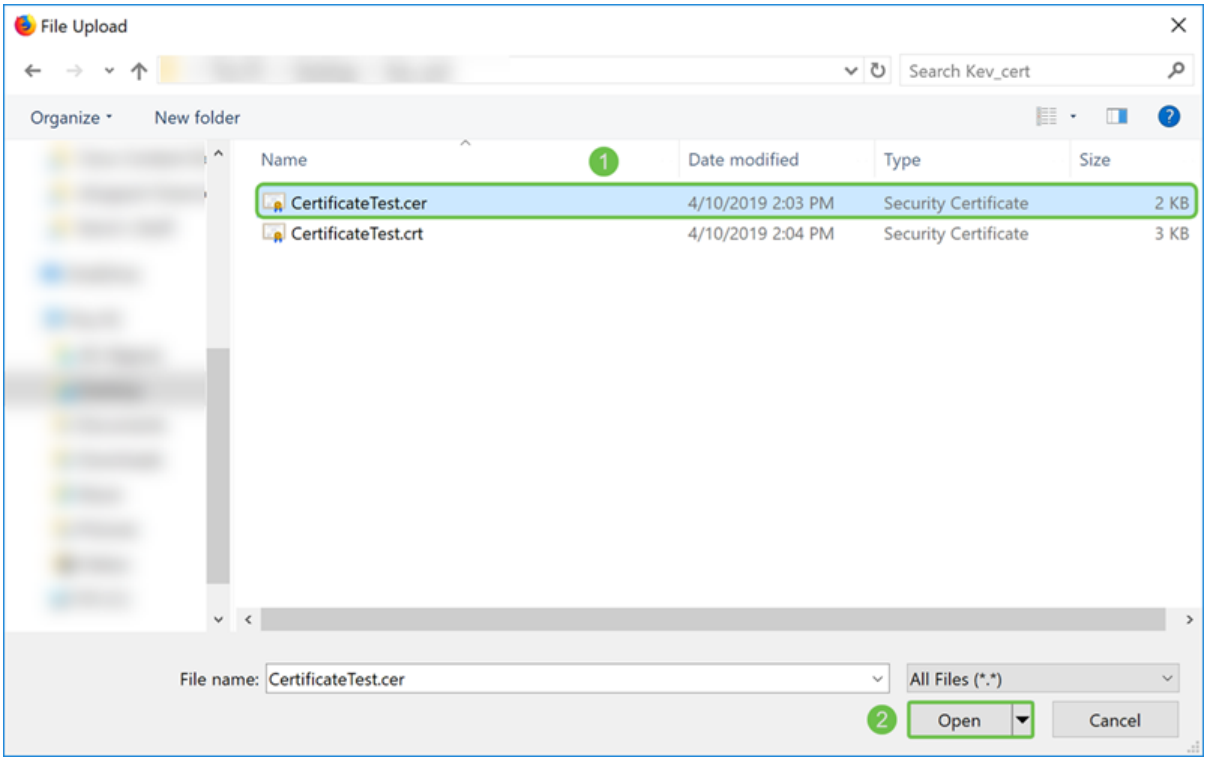
Stap 24. Ga terug naar de pagina *Certificaat* in uw router en voer het certificaatbestand in door op het **pijltje naar het** pictogram **van het apparaat te klikken**.



Stap 25. Voer in het veld *certificaatnaam* in van de **certificaatnaam**. Het kan niet dezelfde naam zijn als het certificaatgebarentekenverzoek. Selecteer in het gedeelte *Certificaat uploaden* de optie **importeren van een pc** en klik op **Bladeren...** om uw certificaatbestand te uploaden.

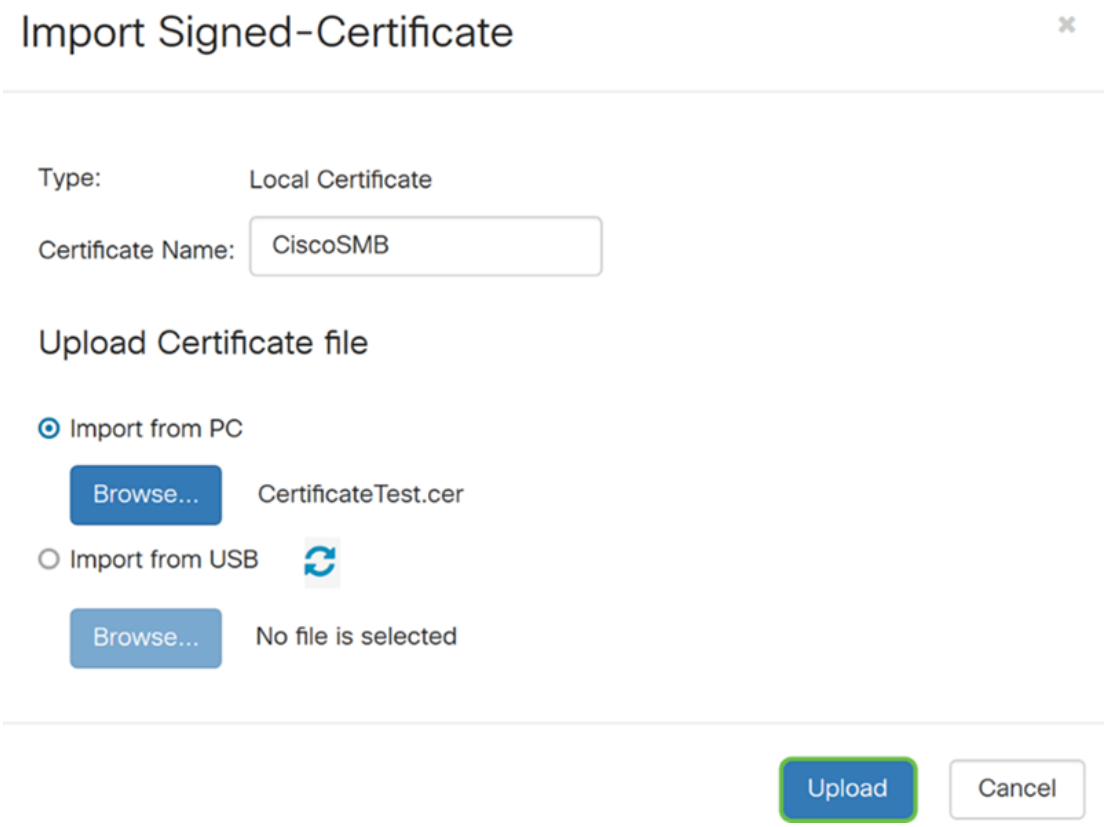


Stap 26. Er verschijnt een venster voor *het uploaden van bestanden*. Navigeer naar de locatie van uw certificaatbestand. Selecteer het certificaatbestand dat u wilt uploaden en klik op **Openen**. In dit voorbeeld werd **certificaattest.cer** geselecteerd.

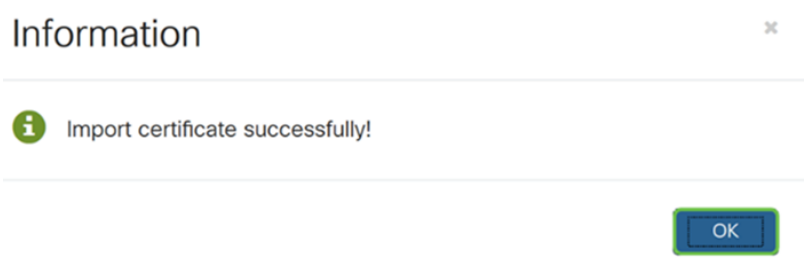


Stap 27. Klik op de knop **Upload** om het certificaat aan de router te uploaden.

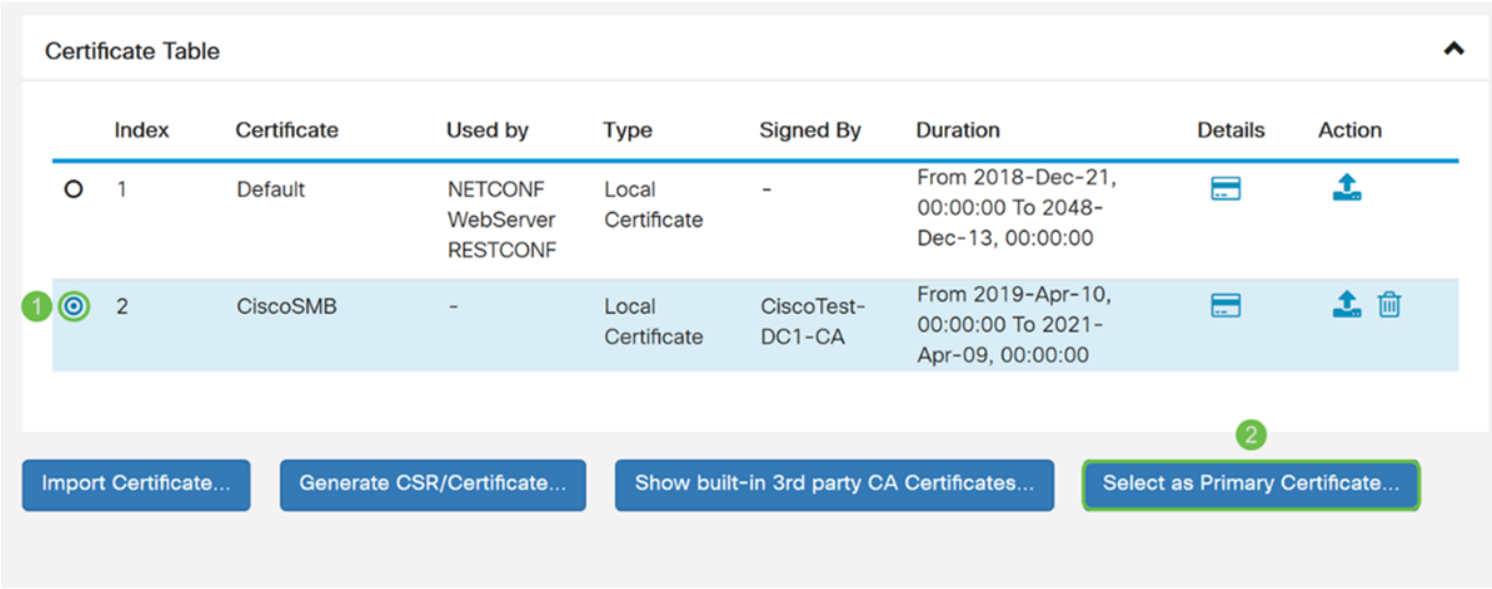
Opmerking: Als u een fout krijgt waar u uw .cer-bestand niet kunt uploaden, kan dit zijn omdat uw router vereist dat het certificaat in een pem-codering zit. U moet de bestandsextensie .cer converteren naar een pem-codering (.crt-bestandsextensie).



Stap 28. Als de invoer geslaagd is, moet *een* informatievenster verschijnen om u te laten weten dat de invoer geslaagd is. Klik op **OK** om verder te gaan.



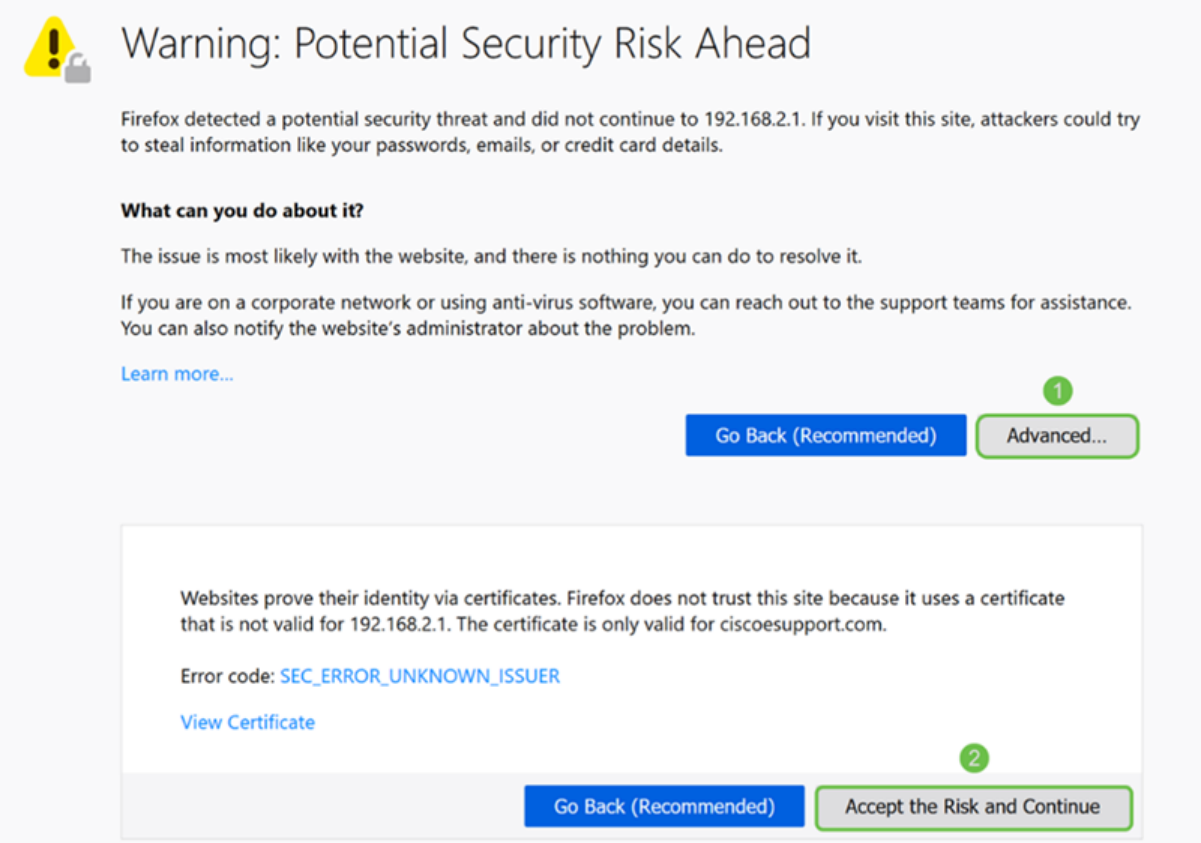
Stap 29. Uw certificaat moet met succes worden bijgewerkt. U dient te kunnen zien door wie uw certificaat is ondertekend. In dit voorbeeld, kunnen we zien dat ons certificaat door *CiscoTest-DC1-CA* is ondertekend. Als u het certificaat als ons primaire certificaat wilt maken, selecteert u het certificaat met de linkerknop en vervolgens klikt u op **de** knop **Primair certificaat selecteren...**.



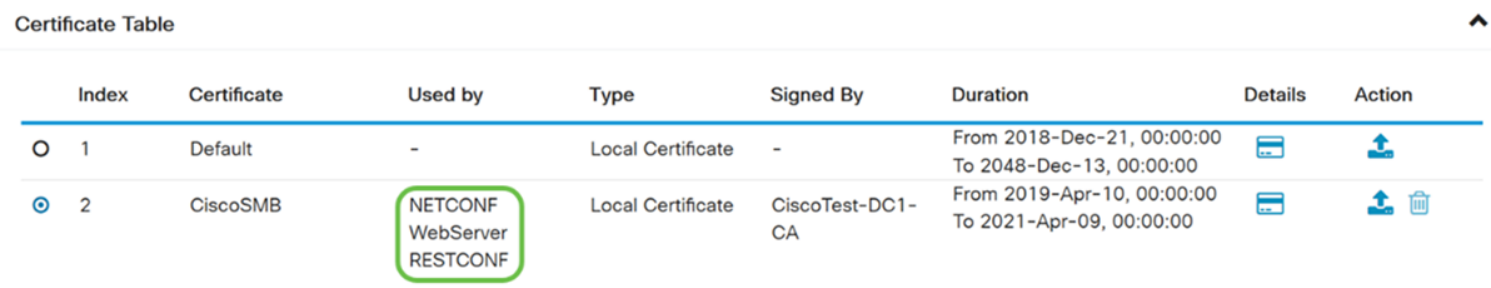
Opmerking: Door het primaire certificaat te wijzigen kunt u terugkeren naar een waarschuwingspagina. Als u Firefox gebruikt en het verschijnt als een grijze blanco pagina, moet u de configuratie van uw Firefox aanpassen. In dit document op Mozilla wiki wordt uitleg gegeven: CA/AddRootToFirefox. Om de waarschuwingspagina opnieuw te kunnen zien volgt u deze stappen op de pagina met Mozilla-ondersteuning.

Stap 30. In de pagina met de waarschuwing voor Firefox, klik op **Geavanceerd...** en **accepteer vervolgens het risico en ga door** met de router.

Opmerking: Deze waarschuwingen variëren van browser tot browser maar vervullen dezelfde functies.



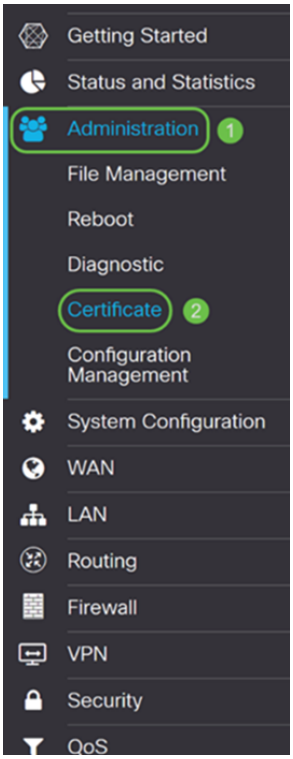
Stap 31. In de Tabel Certificaat ziet u dat het NETCONF, *WebServer* en *RESTCONF* naar uw nieuwe certificaat is veranderd in plaats van het *Standaardcertificaat* te gebruiken.



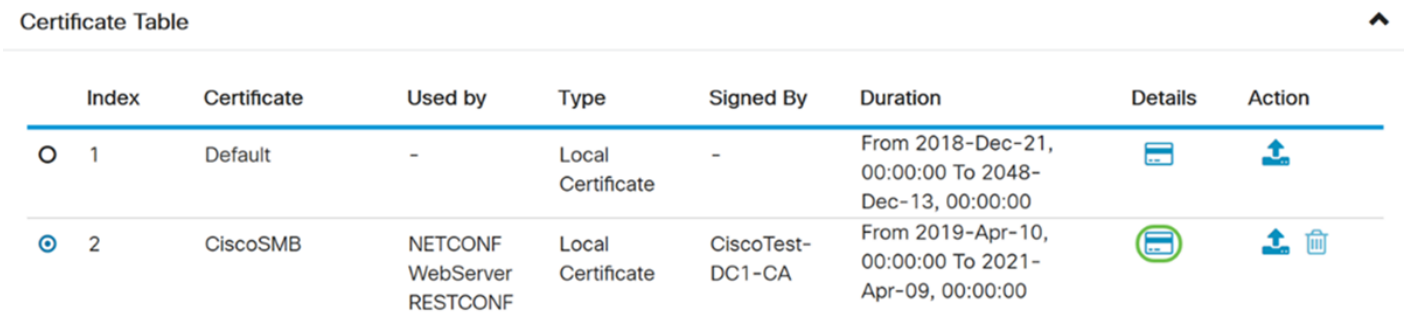
U moet nu een certificaat op uw router hebben geïnstalleerd.

Certificaat bekijken

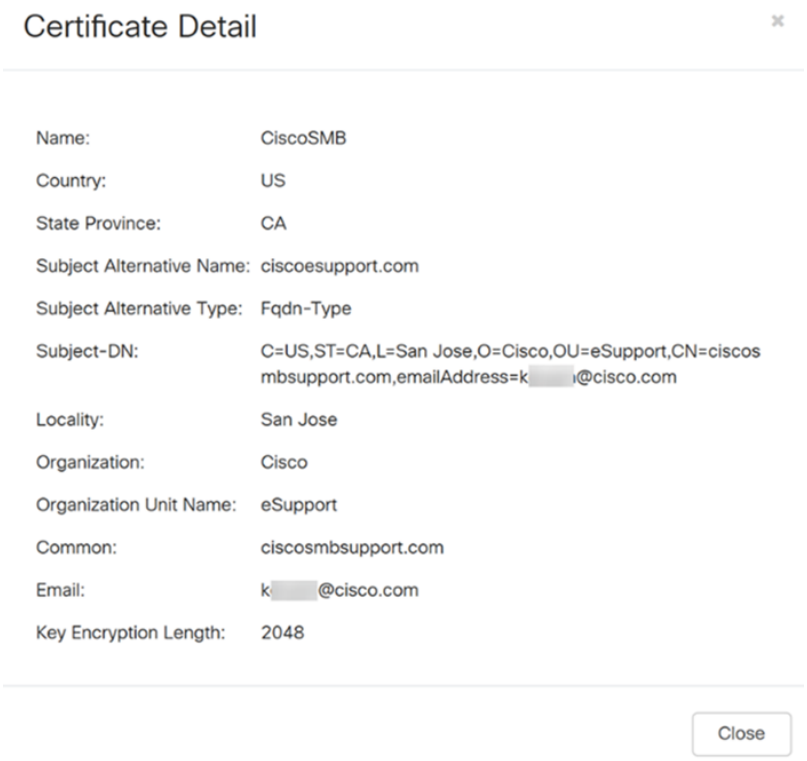
Stap 1. Als u niet op de certificaatpagina hebt navigeerd, navigeer dan naar **Administratie > Certificaat**.



Stap 2. Klik in de *certificaattabel* op het pictogram **Details** onder het kopje *Details* .

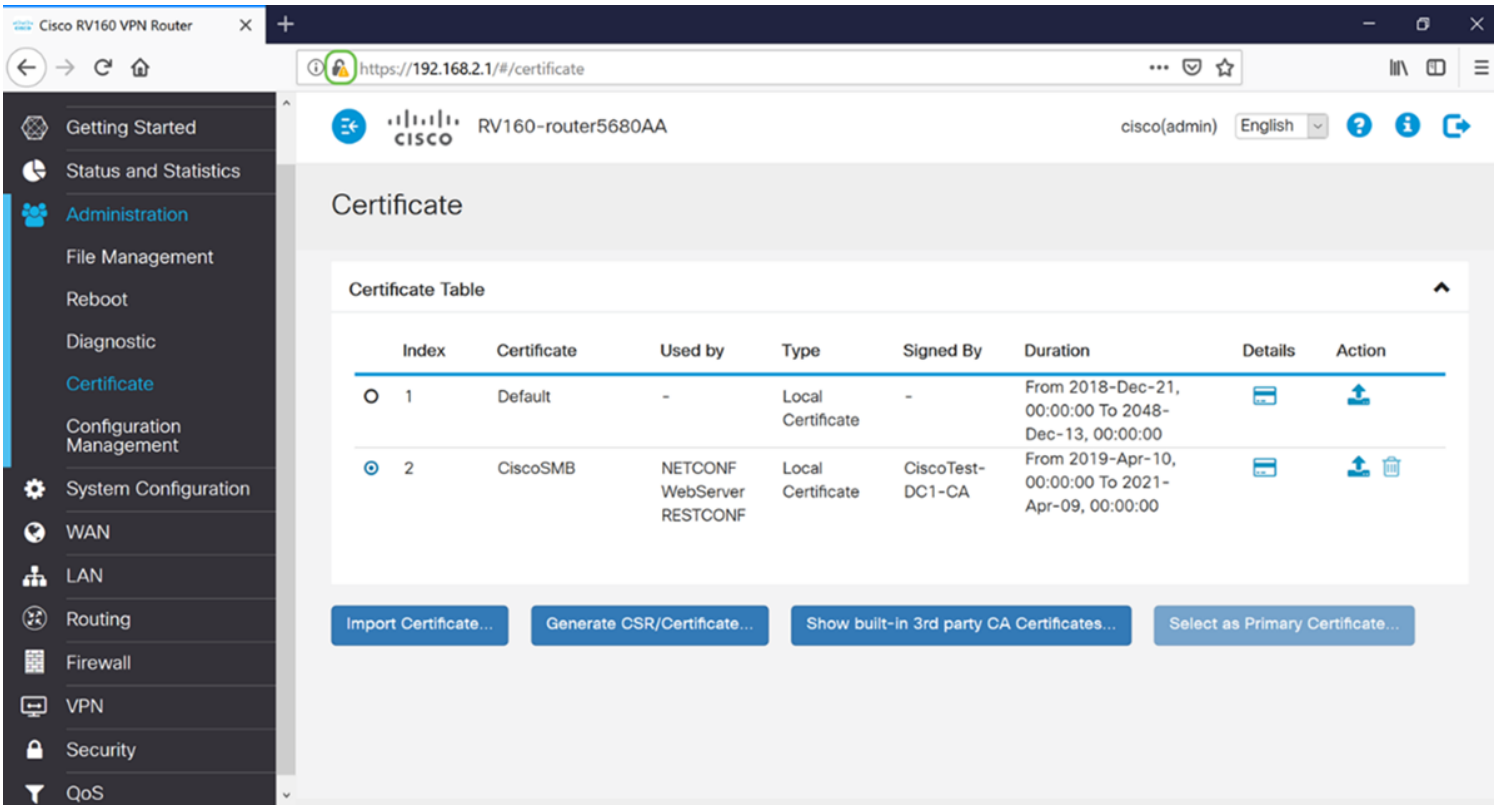


Stap 3. De pagina *met* certificaatgegevens wordt weergegeven. U dient alle informatie over uw certificaat te kunnen zien.

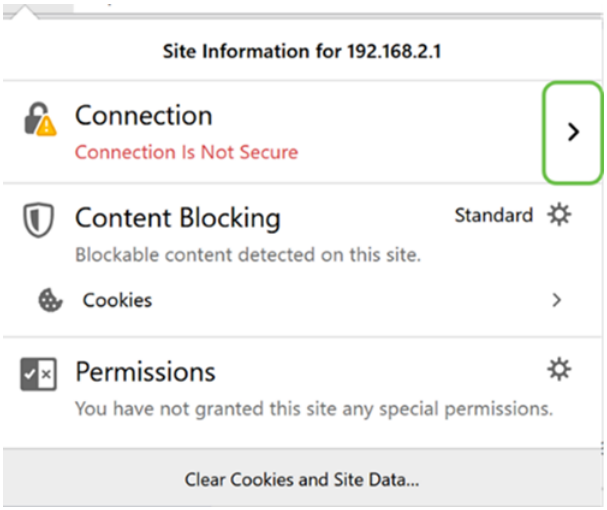


Stap 4. Klik op het pictogram **Lock** aan de linkerkant van de URL-balk (Uniform Resource Locator).

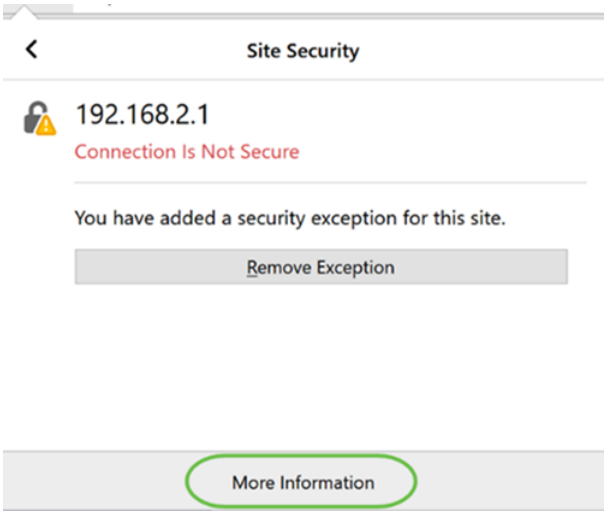
Opmerking: De volgende stappen worden gebruikt in een browser Firefox.



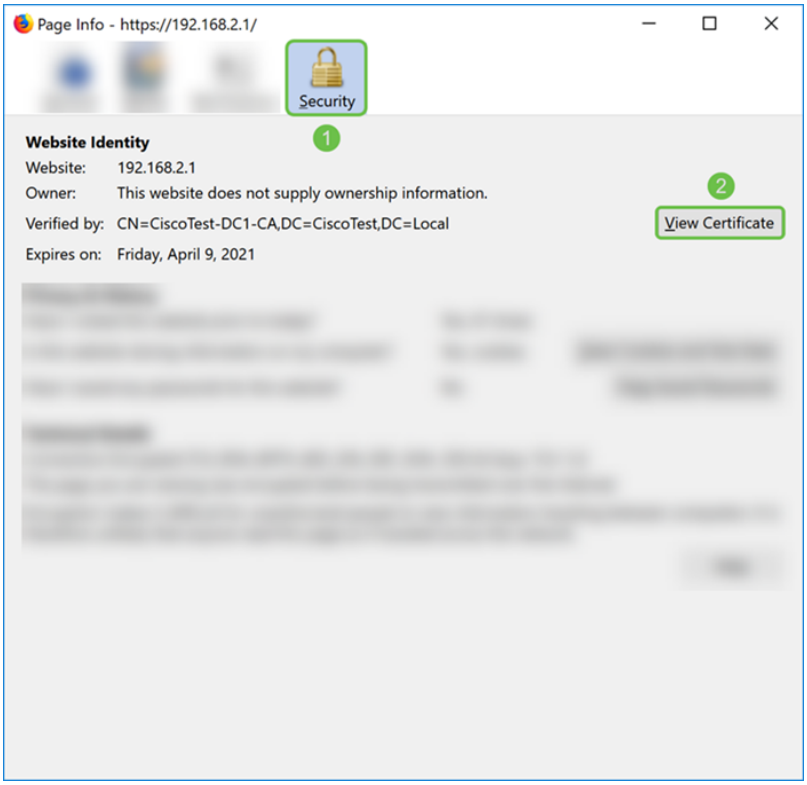
Stap 5. Er verschijnt een vervolgkeuzelijst met keuzes. Klik op het pictogram **Arrow** naast het veld *Connection*.



Stap 6. Klik op **Meer informatie**.

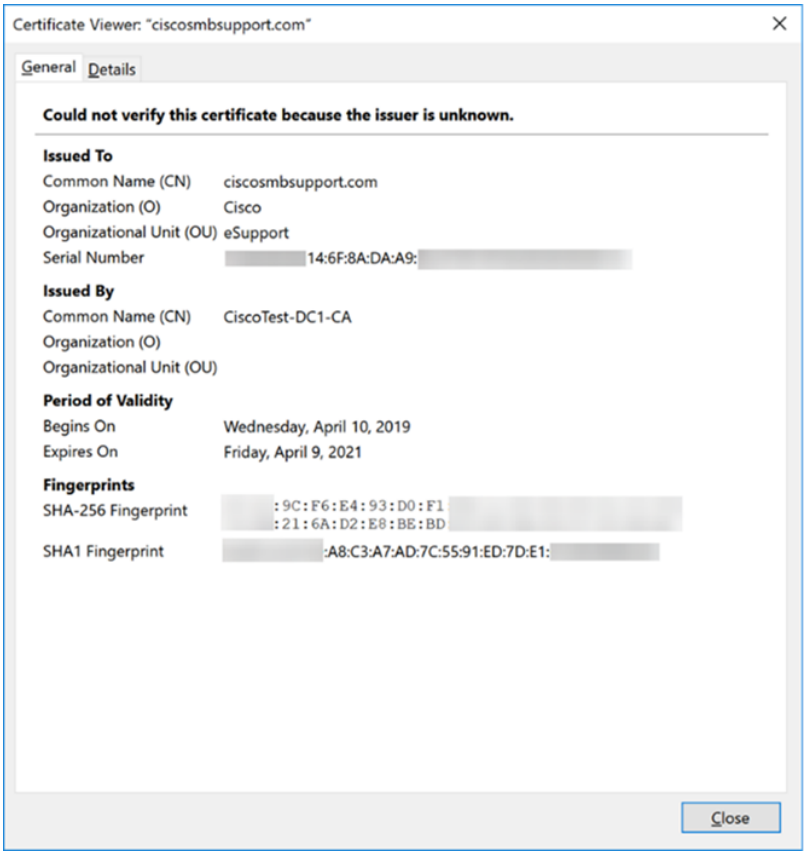


Stap 7. In het venster *Pagina-informatie* kunt u een korte informatie over uw certificaat zien onder het gedeelte *Website Identity*. Zorg ervoor dat u in het tabblad **Security** bent en klik vervolgens op **Certificaat bekijken** om meer informatie over uw certificaat te zien.



Stap 8. Het venster van het *certificaatvenster* moet worden weergegeven. U dient alle informatie te kunnen zien over uw certificaat, de geldigheidstermijn, de vingerafdrukken en wie het is afgegeven door.

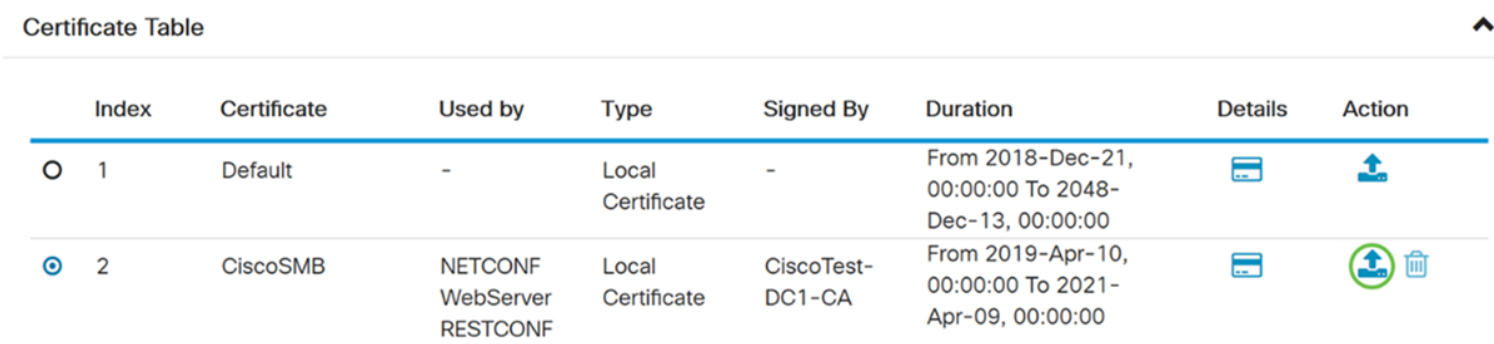
Opmerking: Aangezien dit certificaat is afgegeven door onze server van het testcertificaat, is de emittent onbekend.



Uitvoercertificaat

Om uw certificaat te downloaden om het op een andere router te importeren, volgt u de onderstaande stappen.

Stap 1. Klik in de pagina *Certificaat* op het pictogram **exporteren** naast het certificaat dat u wilt exporteren.



Stap 2. Er verschijnt een *uitvoercertificaat*. Selecteer een bestandsindeling voor het uitvoercertificaat. De opties zijn:

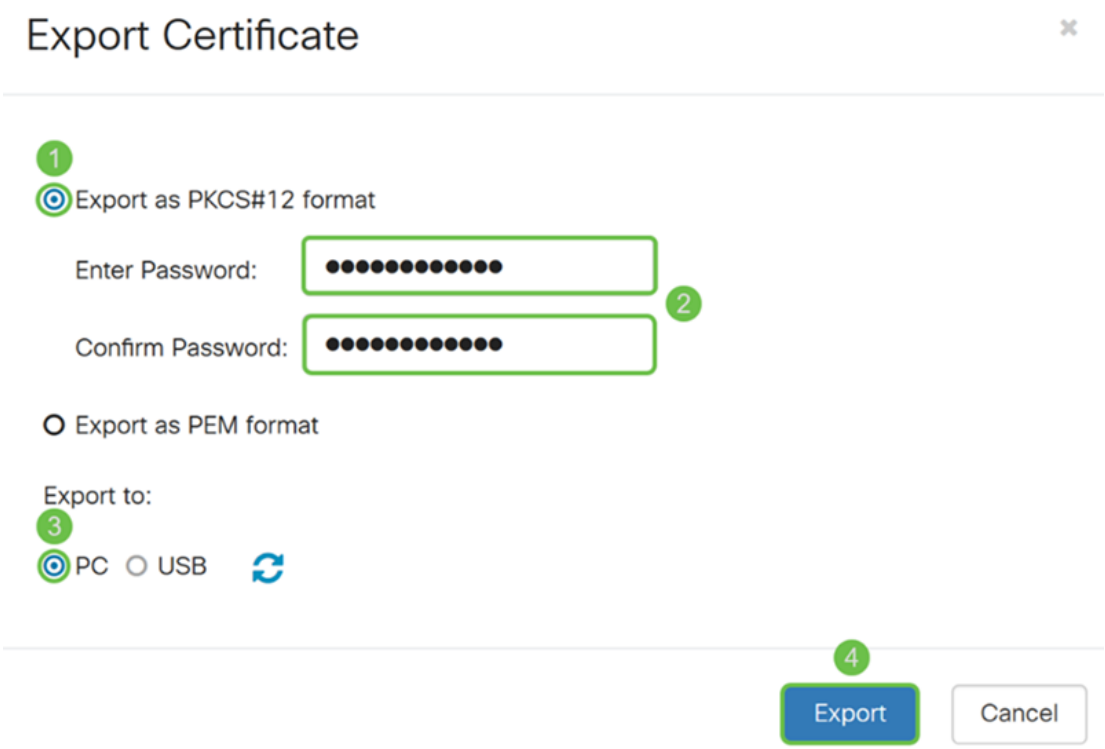
PKCS#12 - Public Key Cryptography Standards (PKCS) #12 is een geëxporteerd certificaat

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.

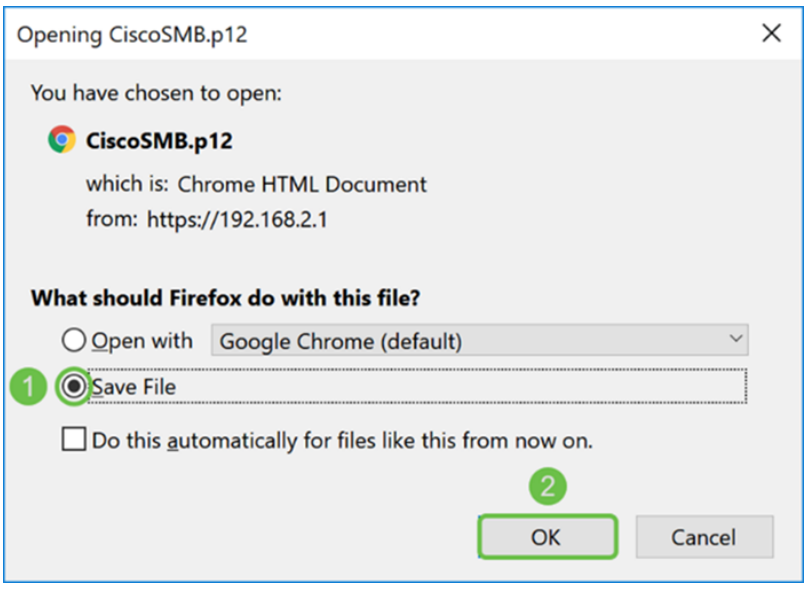
PEM - Privacy Enhanced Mail (PEM) wordt vaak gebruikt voor webservers zodat deze gemakkelijk kunnen worden vertaald in leesbare gegevens door gebruik te maken van een eenvoudige teksteditor zoals een notebook.

Selecteer **Exporteren als PKCS#12-indeling** en voer een **wachtwoord in** en **bevestig het wachtwoord**. Selecteer vervolgens **PC** als de *Exporteren naar:* veld. Klik op **Exporteren** om het certificaat naar uw computer te starten.

Opmerking: Vergeet dit wachtwoord niet omdat u het gebruikt bij het importeren naar een router.

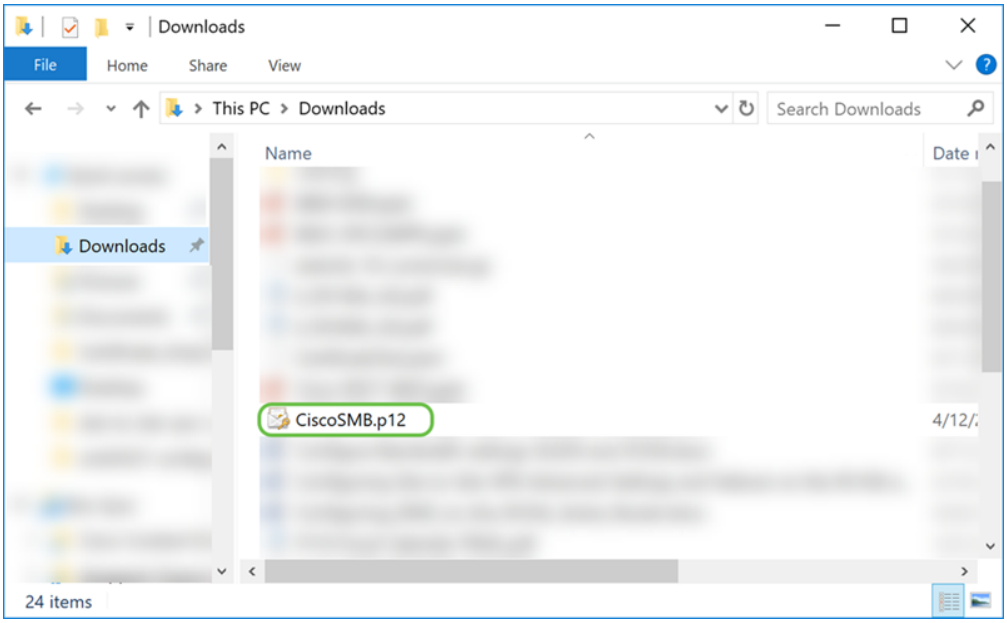


Stap 3. Er verschijnt een venster waarin u wordt gevraagd wat u met dit bestand moet doen. In dit voorbeeld selecteren we **Save File** en vervolgens klikt u op **OK**.



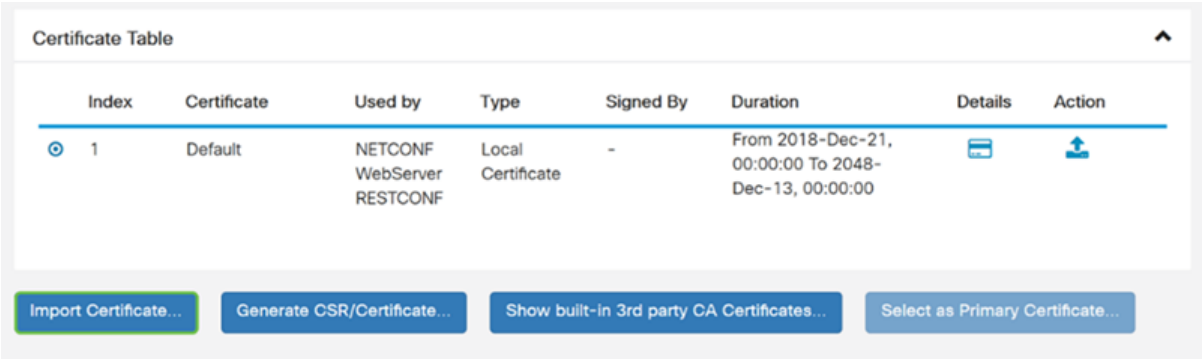
Stap 4. Het bestand moet op de standaard opslaglocatie worden opgeslagen.

In ons voorbeeld is het bestand op onze computer opgeslagen in onze map *Downloads*.



Invoercertificaat

Stap 1. Klik op de knop **Importeren** op de pagina *Certificaat*..



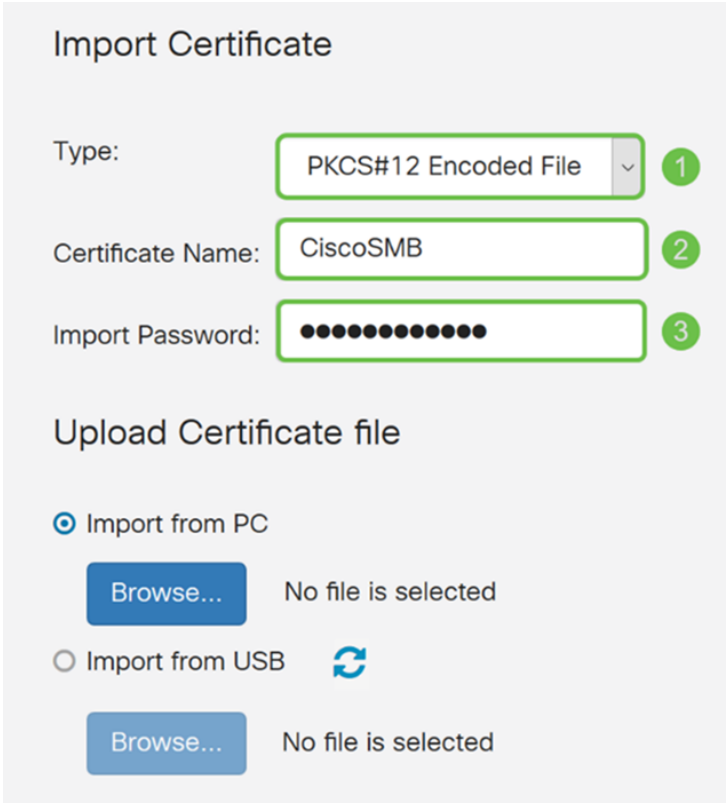
Stap 2. Selecteer het **type** certificaat dat u wilt importeren in de vervolgkeuzelijst *Type* onder *Importwoord*. De opties zijn gedefinieerd als:

CA-certificaat - Een certificaat dat is gecertificeerd door een vertrouwde autoriteit van een derde die heeft bevestigd dat de informatie in het certificaat juist is.

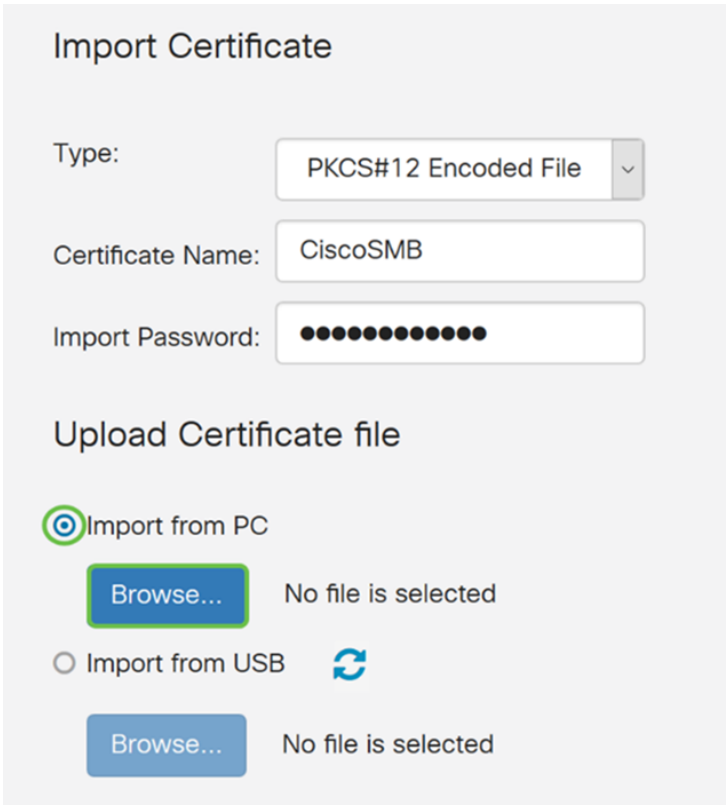
Lokaal apparaatcertificaat - een certificaat dat op de router is gegenereerd.

PKCS#12 Encoded File - Public Key Cryptography Standards (PKCS) #12 is een geëxporteerd certificaat dat in een .p12-extensie wordt geleverd.

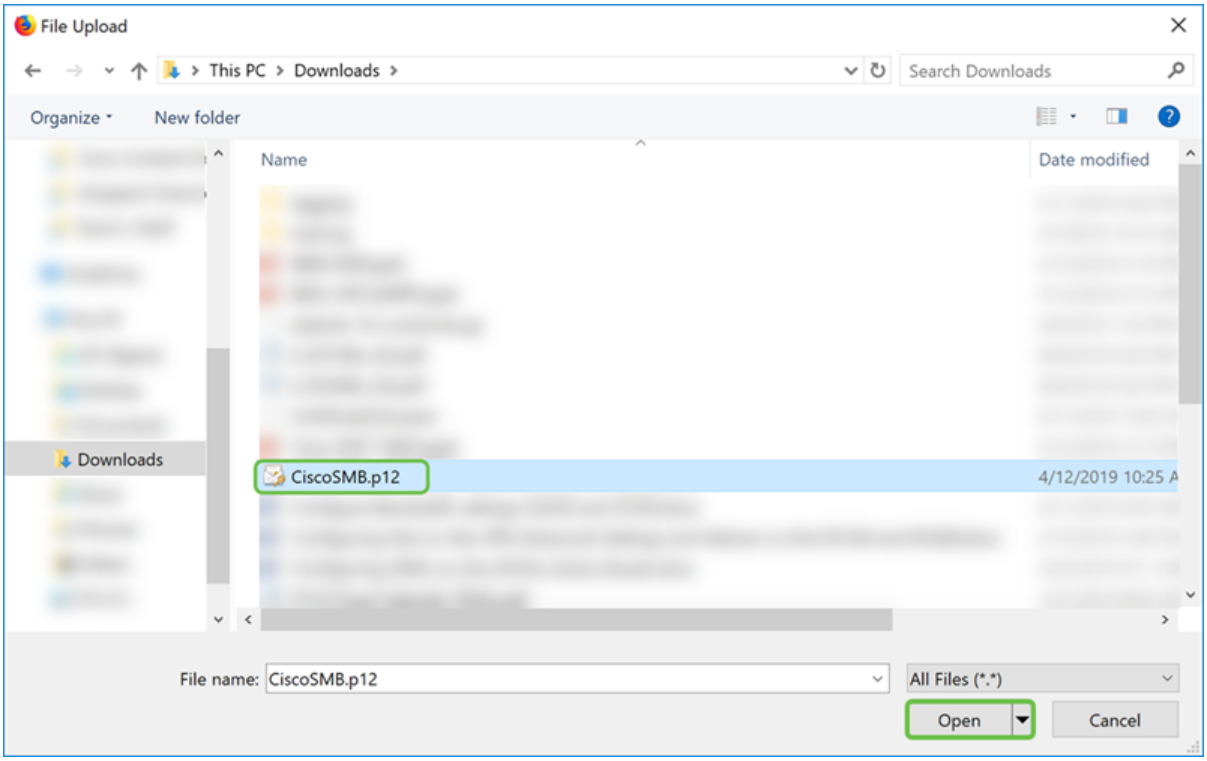
In dit voorbeeld is **PKCS#12 Encoded File** geselecteerd als het type. Voer een **naam** voor het certificaat in en voer vervolgens het **wachtwoord** in dat is gebruikt.



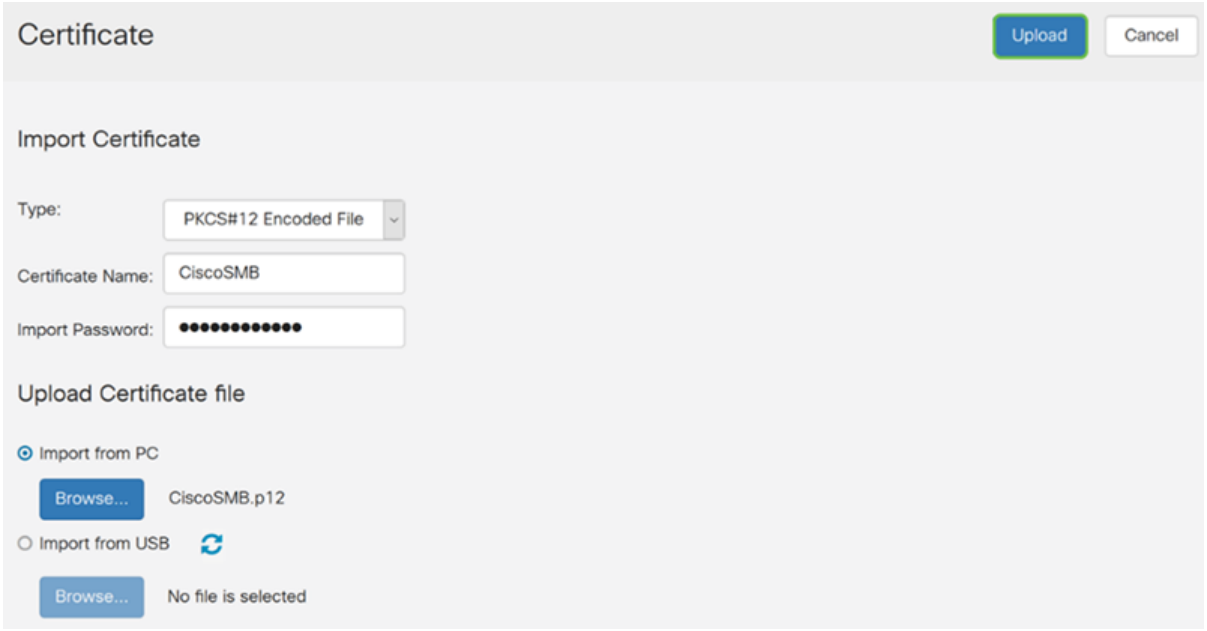
Stap 3. Selecteer onder het gedeelte *Upload certificaatbestand* de optie **Importeren uit PC** of **Importeren uit USB**. In dit voorbeeld werd **Importeren vanaf een pc** geselecteerd. Klik op **Bladeren...** om een bestand te kiezen om te uploaden.



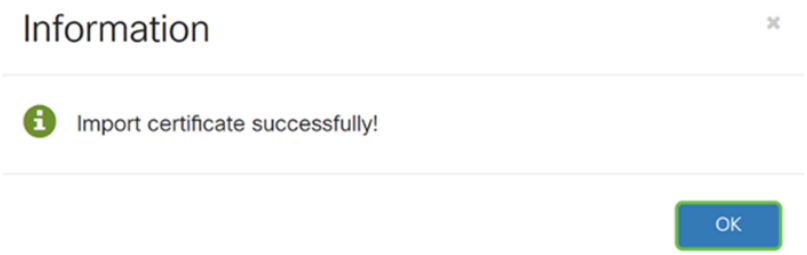
Stap 4. In het venster *File Upload* navigeren naar de locatie van het gecodeerde PKCS#12-bestand (1.p12-bestandsextensie). Selecteer het **.p12-**bestand en klik vervolgens op **Openen**.



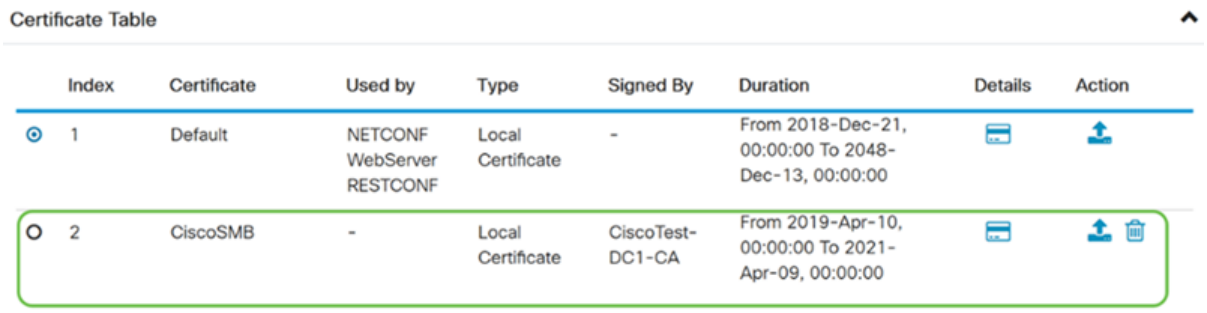
Stap 5. Klik op **Upload** om het certificaat te uploaden.



Stap 6. Het venster met *informatie* verschijnt waar u weet dat het certificaat is geïmporteerd. Klik op **OK** om verder te gaan.



Stap 7. Controleer dat uw certificaat is geüpload.



Conclusie

U hebt geleerd hoe u een CSR kunt genereren, importeren en downloaden van een certificaat op de RV160 en RV260 Series router.