

Mijn certificaat configureren op RV320 en RV325 VPN-routers

Doel

Er worden certificaten gebruikt om de identiteit van een persoon of apparaat te controleren, een service te authentifieren of bestanden te versleutelen. Op de RV320 kunt u maximaal 50 certificaten toevoegen door zelf-ondertekening of toestemming van derden. U kunt een certificaat voor een client of beheerder exporteren en opslaan op een USB-apparaat of een USB-apparaat, en het vervolgens importeren.

Dit document heeft als doel u te laten zien hoe u een primair certificaat kunt selecteren, een certificaat kunt exporteren en een certificaat kunt importeren op de RV32x Series VPN-routers.

Toepasselijke apparaten

- RV320 VPN-router met dubbel WAN
- RV325 Gigabit VPN-router met dubbel WAN

Softwareversie

- v1.1.0.09

Mijn certificaat

Stap 1. Meld u aan bij het web-configuratieprogramma en kies **het certificaatbeheer > Mijn certificaat**. De pagina *Mijn certificaat* wordt geopend:



The screenshot shows a web interface titled "My Certificate". Below the title is a table with the following columns: "Used", "Type", "Subject", "Duration", "Details", and "Export". There are three rows of certificates. The first row is highlighted in green and has a radio button selected. The second and third rows have radio buttons that are not selected. Below the table are three buttons: "Add", "Delete", and "Select as Primary Certificate".

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Er zijn twee soorten certificaten:

- Zelfgetekend — een Secure Socket Layer (SSL) certificaat dat is ondertekend door zijn eigen maker. Dit type is minder veilig aangezien het niet kan worden geannuleerd als de privé sleutel door een aanvalleur wordt gecompromitteerd.
- Aanvraag van certificatie — Een infrastructuur voor openbare sleutel (PKI) die naar de certificeringsinstantie wordt gestuurd om een digitaal identiteitsbewijs aan te vragen. Het is veiliger dan door zichzelf getekend, aangezien de privé-sleutel geheim gehouden wordt.

Stap 2. Klik het gewenste keuzerondje in de *tabel Mijn certificaat* aan om een certificaat te kiezen.

Stap 3. Klik op **Selecteren als Primair certificaat** om het geselecteerde certificaat als primair certificaat te maken.

Stap 4. (Optioneel) Klik op het pictogram **Details** om gedetailleerde informatie over het certificaat te bekijken.

My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Het venster *certificaatdetails* wordt geopend:

Certificate Details

Certificate Information

Version: 3
 Serial Number: D8 AF 62 26 26 36 5D D1

Subject Information

Subject: CN=6c:20:56:c6:16:52
 OU=RV320
 O=Cisco Systems, Inc.
 L=Irvine
 C=US
 ST=California

Public Key Algorithm: rsaEncryption -
 Subject Key Identifier: 2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63

Issuer Information

Issuer: CN=6c:20:56:c6:16:52
 OU=RV320
 O=Cisco Systems, Inc.
 L=Irvine
 C=US
 ST=California

Valid From: Apr 8 19:12:48 2013 GMT
 Valid Through: Apr 6 19:12:48 2023 GMT
 Signature Algorithm: sha1WithRSAEncryption
 Authority Key Identifier: 2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63
 Fingerprint: 33 C4 E6 40 7D DD 1F 44 32 57 18 A9 AA D1 66 FB 5A B2 CD 36

Stap 5. (Optioneel) Klik om een certificaat te verwijderen op de radioknop van het certificaat dat u wilt verwijderen en vervolgens op **Verwijderen**.

Stap 6. Klik op **Save** om de instellingen op te slaan.

Een zelfondertekend certificaat exporteren

Stap 1. Klik op de gewenste knop in de kolom *Exporteren* om een zelfondertekend certificaat te exporteren.

My Certificate

My Certificate Table

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

De beschikbare pictogram-knoppen zijn als volgt gedefinieerd:

- Exportcertificaat voor client — Exporteren van een client-certificaat dat wordt gebruikt om de client aan te sluiten op het Virtual Private Network (VPN).
- Exportcertificaat voor beheerder — Exporteren van een beheerder. Er wordt een privésleutel gegenereerd en er wordt een kopie bewaard voor back-up.
- Exporteren Private Key — Exporteren van een particuliere sleutel voor VPN-clientsoftware, die afzonderlijke aanmeldingsgegevens nodig heeft voor een VPN-verbinding.

Stap 2. Klik op **Open** om de toets te bekijken.

Stap 3. Klik op **Save** om de toets op te slaan.

Een certificaataanvraag exporteren

Stap 1. Klik op **CSR** (Exportwachtingsaanvraag).



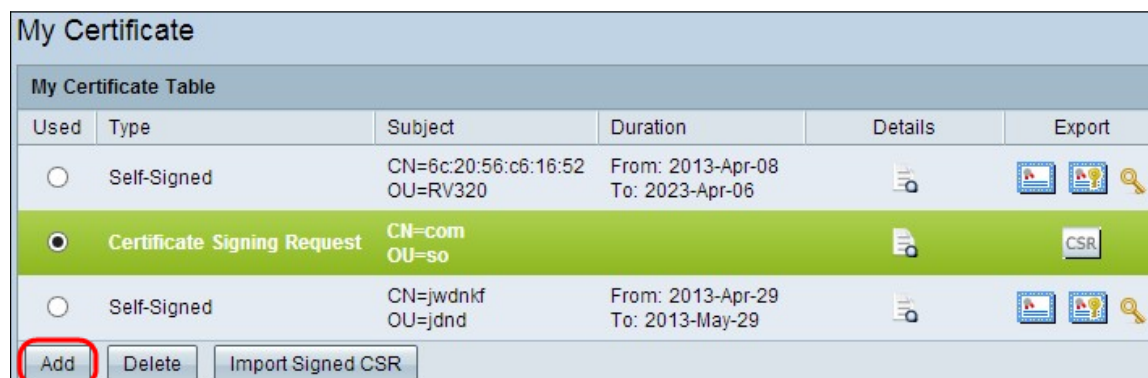
My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Stap 2. Klik op **Open** om deze te bekijken.

Stap 3. Klik op **Save** om de toets op uw PC of USB op te slaan.

Een certificaat importeren

Stap 1. Klik op **Add** om een certificaat te importeren.



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Het volgende venster verschijnt:

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: No file chosen (PEM format)

Certificate + Private Key: No file chosen (PEM format)

Import from USB Device

USB Device Status: No Device Attached

Stap 2. Klik op het gewenste keuzerondje om het type certificaat te definiëren dat u importeert.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: No file chosen (PEM format)

Certificate + Private Key: No file chosen (PEM format)

Import from USB Device

USB Device Status: No Device Attached

- Goedgekeurd door derden — een infrastructuur voor de openbare sleutel (PKI) waarin de certificeringsinstantie de digitale handtekening aanbiedt.
- Zelfgetekend — een Secure Socket Layer (SSL) certificaat dat is ondertekend door zijn eigen maker.

Stap 3. Klik op het gewenste keuzerondje om te kiezen hoe u het certificaat wilt importeren.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC
 CA Certificate: No file chosen (PEM format)
 Certificate + Private Key: No file chosen (PEM format)
 Import from USB Device

- Importeren vanaf een pc - Het certificaat wordt geïmporteerd vanaf uw pc waar u het hebt opgeslagen.
- Importeren vanuit USB — certificaatvoer vanuit uw USB-station.

Certificaat importeren vanaf een pc

Stap 1. Als u een geautoriseerd certificaat van derden importeert, klikt u op **Bestand** naast *CA-certificaat* om door te bladeren naar de locatie van het bestand en selecteert u dit.

Stap 2. Klik op **Kies bestand** naast *Certificaat + Private Key* om naar de locatie van het bestand te bladeren en selecteer dit.

Stap 3. Klik op **Save** om de instellingen op te slaan. Het geïmporteerde certificaat wordt weergegeven in de *tabel Mijn certificaat*.

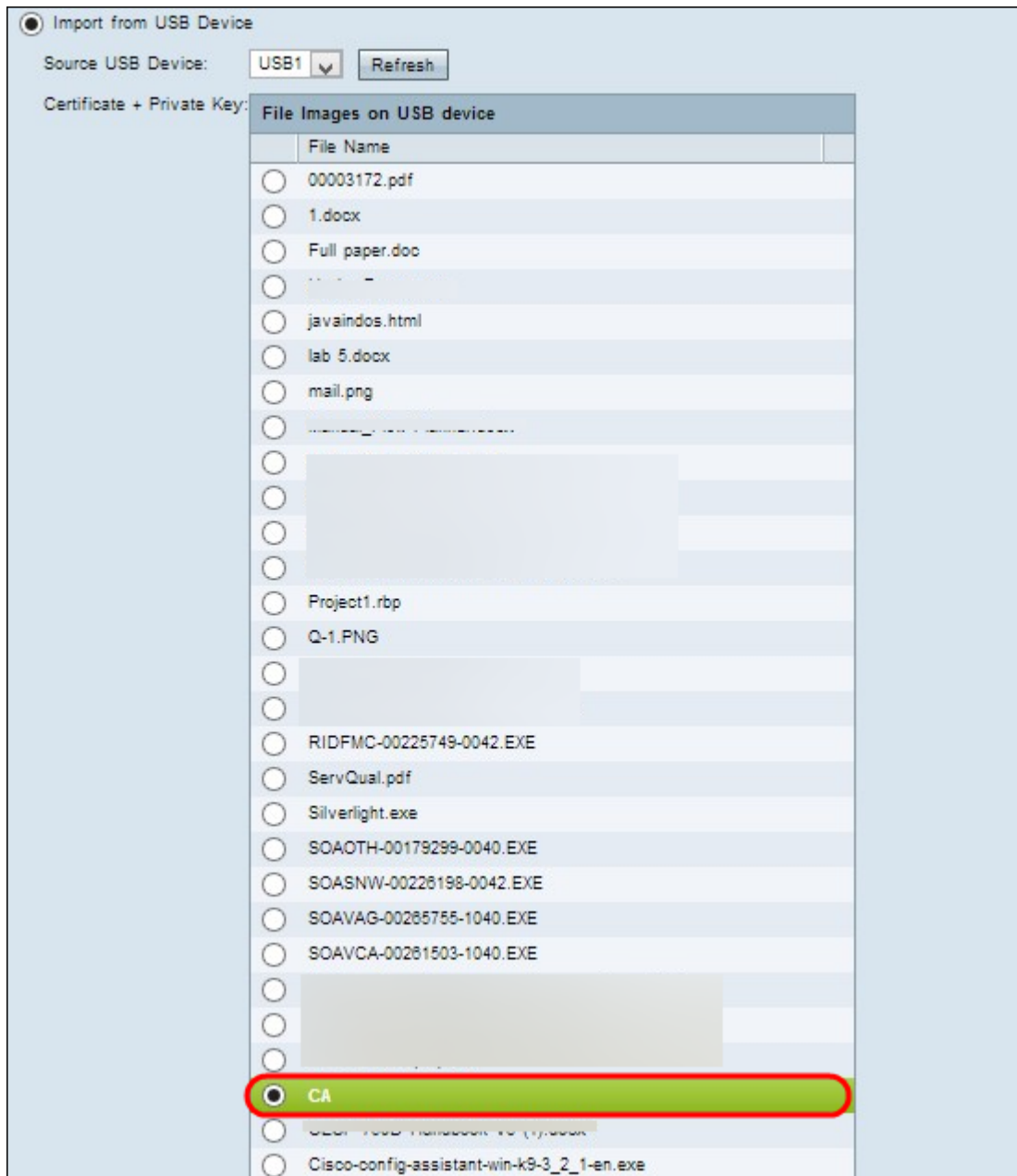
My Certificate

My Certificate Table

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		
<input type="radio"/>	Self-Signed	CN= OU=			

Certificaat importeren vanaf USB

Stap 1. Kies het juiste USB-apparaat in de vervolgkeuzelijst *Bron-USB* apparaat.













Stap 2. Als u een geautoriseerd certificaat van derden importeert, klikt u op de juiste radioknop om het CA-certificaat te importeren dat u op uw USB hebt opgeslagen.

Stap 3. Kies het juiste radioknop om het certificaat + de privésleutel te importeren die u op uw USB hebt opgeslagen.

Stap 4. Klik op **Opslaan** om de instellingen op te slaan. Het geïmporteerde certificaat wordt weergegeven in de *tabel Mijn certificaat*.

My Certificate

My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		  
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			 CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		  
<input type="radio"/>	Self-Signed	CN= OU=		