

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

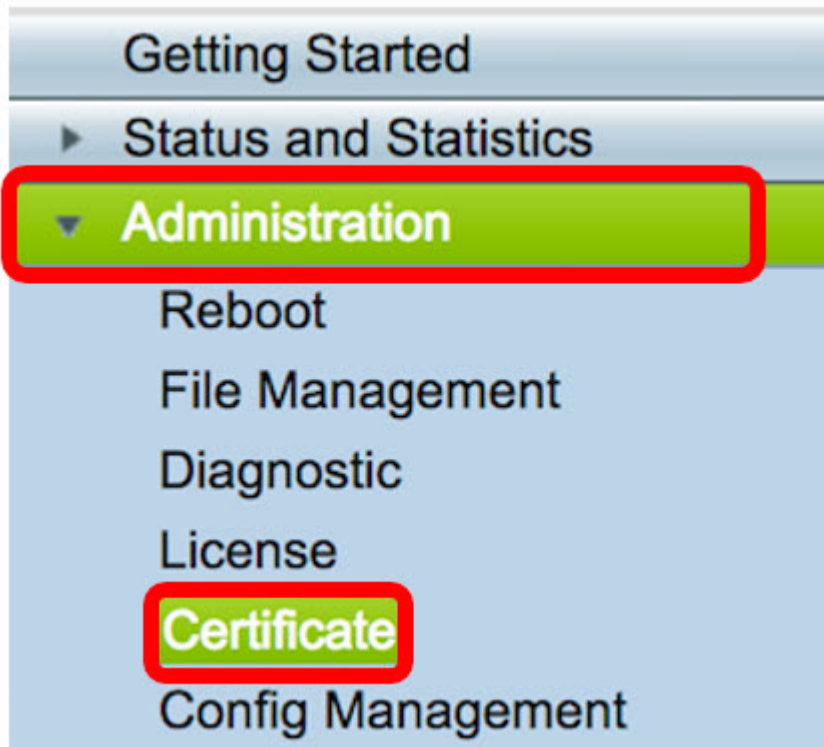
Softwareversie

- 1.0.01.17

Vervang het standaard zelfgetekende certificaat door een SSL-certificaat van 3^e 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**.

Certificate Table						
	Index	Certificate	Used By	Type	Signed By	Duration
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00

Delete Export Detail Import

Import Certificate **Generate CSR/Certificate**

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

Generate CSR/Certificate

Type
✓ Self-Signing Certificate
Certificate Signing Request

Certificate Name

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

Generate CSR/Certificate

Type

Certificate Signing Request ▾

Certificate Name

34xrouter

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.

Subject Alternative Name

RVrouter.com

IP Address FQDN Email

Opmerking: In dit voorbeeld wordt RVrouter.com gebruikt.

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

IP Address FQDN Email

Country Name

US - United States

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)*.

Country Name

US - United States

State or Province Name(ST)

California

Opmerking: In dit voorbeeld wordt Californië gebruikt.

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

State or Province Name(ST)

California

Locality Name(L)

Irvine

Opmerking: In dit voorbeeld wordt Irvine gebruikt.

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

Locality Name(L)	Irvine
Organization Name(O)	Cisco

Opmerking: In dit voorbeeld wordt Cisco gebruikt.

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

Organization Name(O)	Cisco
Organization Unit Name(OU)	SBKM

Opmerking: In dit voorbeeld wordt SBKM gebruikt.

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

Organization Unit Name(OU)	SBKM
Common Name(CN)	34xrouter

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.

Common Name(CN)	34xrouter
Email Address(E)	@gmail.com

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.

Email Address(E)

Key Encryption Length

512
 1024
 2048

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**.

Key Encryption Length

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

Certificate Table					
	Index	Certificate	Used By	Type	Signed By
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed
<input checked="" type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-

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**.

Certificate Table				
	Index	Certificate	Used By	Type
<input type="checkbox"/>	1	Default	WebServer	Local Certificate
<input type="checkbox"/>	2	FindIT	-	Local Certificate
<input checked="" type="checkbox"/>	3	34xRouter	-	Certificate Signing Request

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.

1. Copy and paste your CSR into this box:	<pre>STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI UzBRMAkGA1UdEwQCMAAwHQYDVR0OBByEFB24F/ A1UdDwQEAWIF4DAYBgNVHREETAPgg0zNHhyb3VC CwUAA4IBAQAB8J/x6+BLOGr797UeHxBH8sCuBSwQ dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE 1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI -----END CERTIFICATE REQUEST-----</pre>
2. Select the server software used to generate the CSR:	Select from list: <input type="button" value="v"/>

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.

1. Copy and paste your CSR into this box:	<pre>STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI UzBRMAkGA1UdEwQCMAAwHQYDVR0OBByEFB24F/ A1UdDwQEAWIF4DAYBgNVHREETAPgg0zNHhyb3VC CwUAA4IBAQAB8J/x6+BLOGr797UeHxBH8sCuBSwQ dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE 1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI -----END CERTIFICATE REQUEST-----</pre>
2. Select the server software used to generate the CSR:	<input type="button" value="OTHER"/> <input type="button" value="v"/>

Stap 3. Download uw certificaat in uw computer.

Het certificaat van de 3^e SSL-partij uploaden

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

Certificate Table						
	Index	Certificate	Used By	Type	Signed By	Duration
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00
<input type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-	-

Buttons: Delete, Export, Detail, Import

Buttons: **Import Certificate**, Generate CSR/Certificate

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

Import Certificate

Type

✓ Local Certificate

CA Certificae

Certificate Name

PKCS#12 encoded file

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

Import Certificate

Type

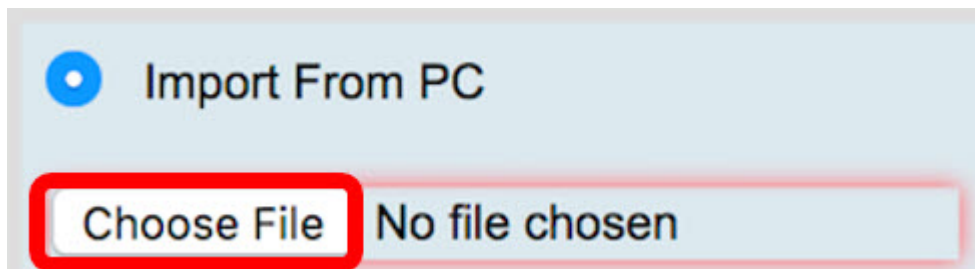
CA Certificae

Certificate Name

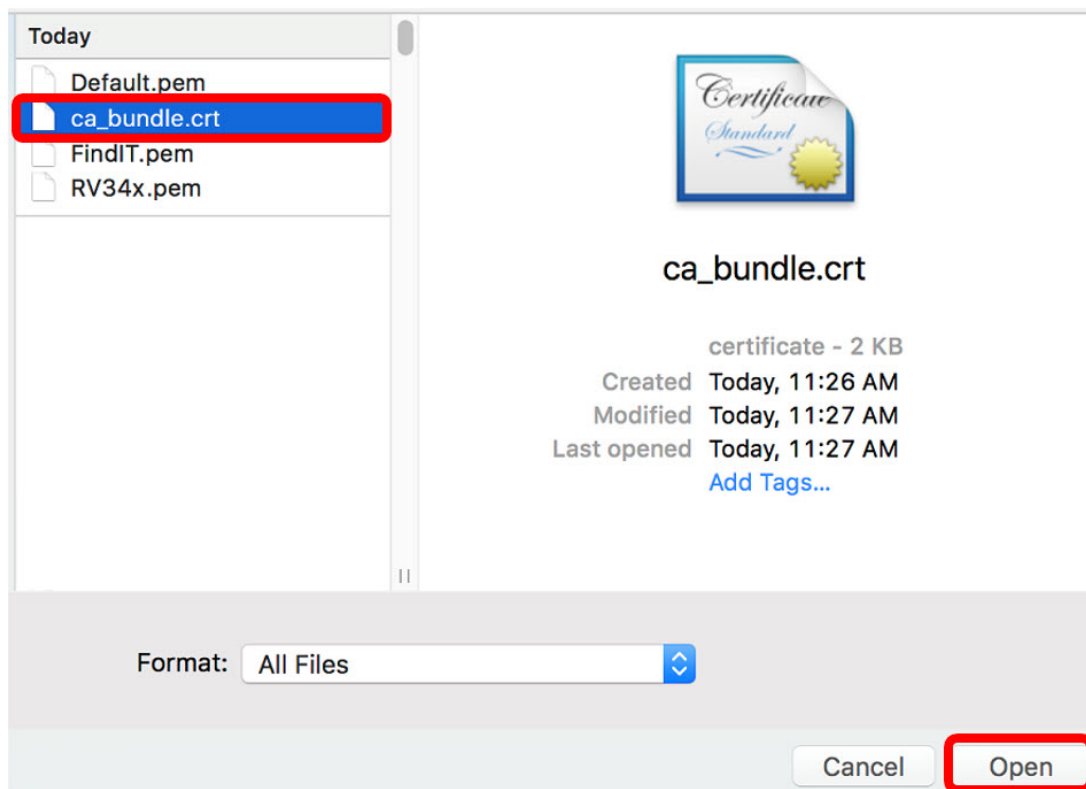
RV34xCert

Opmerking: In dit voorbeeld wordt RV34xCert gebruikt.

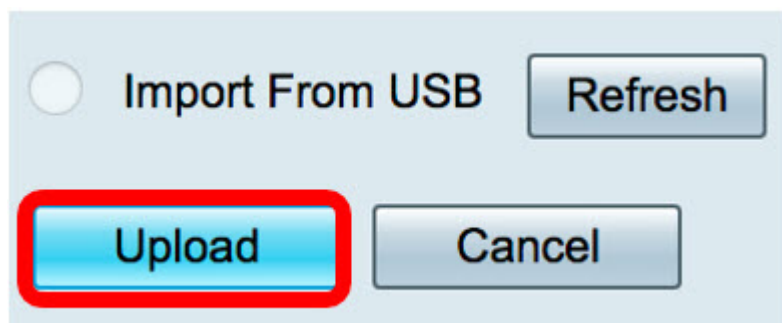
Stap 4. Klik op de knop **Bestand kiezen** en plaats het certificeringsbestand dat u hebt gedownload van de CA.



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.

Certificate Table						
Index	Certificate	Used By	Type	Signed By	Duration	
<input type="checkbox"/> 1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00	
<input type="checkbox"/> 2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00	
<input type="checkbox"/> 3	RV34xCert	-	CA Certificate	DST Root CA X3	From 2016-03-17,00:00:00 To 2021-03-17,00:00:00	

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.

SSL VPN

General Configuration

Group Policies

Cisco SSL VPN Server On Off

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

Mandatory Gateway Settings

Gateway Interface

WAN1

Gateway Port

8443

(Range: 1-65535)

Certificate File

✓ Default
FindIT

Client Address Pool

RV34xCert

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

Certificate File

RV34xCert

Client Address Pool

192.168.10.0

Client Netmask

255.255.255.0

Client Domain

RVrouter.com

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](#)