Replace the Default Self-Signed Certificate with a 3rd Party SSL Certificate on the RV34x Series Router

Introduction

A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows relying parties to depend upon signatures or assertions made by the private key that corresponds to the public key that is certified. A router can generate a self-signed certificate, a certificate created by a network administrator. It can also send out requests to Certificate Authorities (CAs) to apply for a digital identity certificate. It is important to have legitimate certificates from third-party applications.

There are two ways that CA signs the certificates:

1. CA signs the certificate with private keys.

2. CA signs the certificates using Certificate Signing Request (CSR) generated by the RV34x.

Most commercial certificate vendors use intermediate certificates. As the intermediate certificate is issued by the Trusted Root CA, any certificate issued by the intermediate certificate inherits the trust of the Trusted Root, like a certification chain of trust.

Objective

This article aims to show how to request and upload a 3rd party Secure Sockets Layer (SSL) certificate issued by a CA to replace the self-signed certificate on the RV34x Router.

Applicable Devices

- RV340
- RV340W
- RV345
- RV345P

Software Version

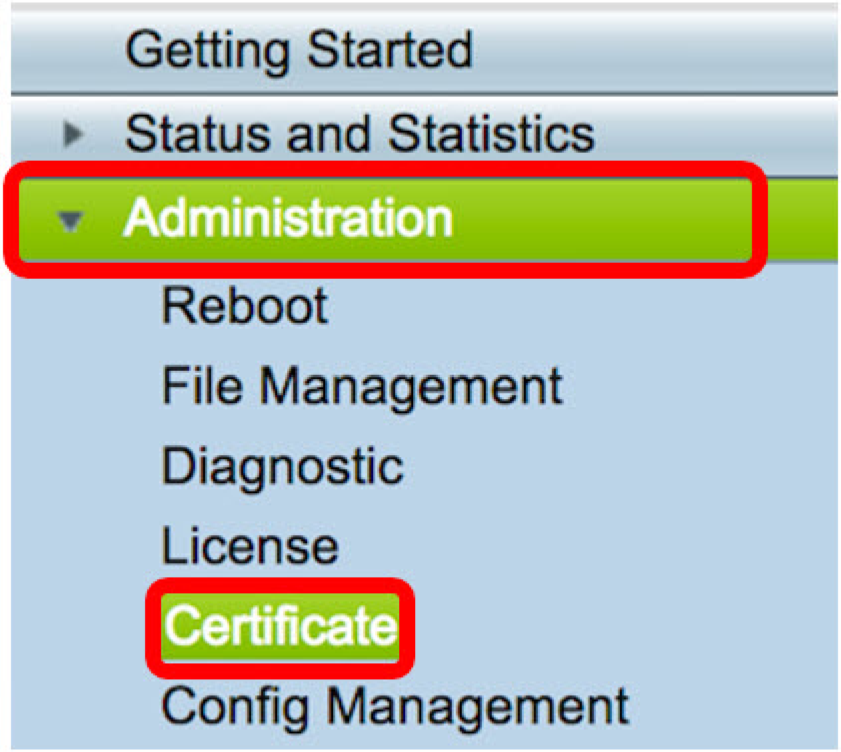
- 1.0.01.17

Replace the Default Self-Signed Certificate with a 3rd Party SSL Certificate

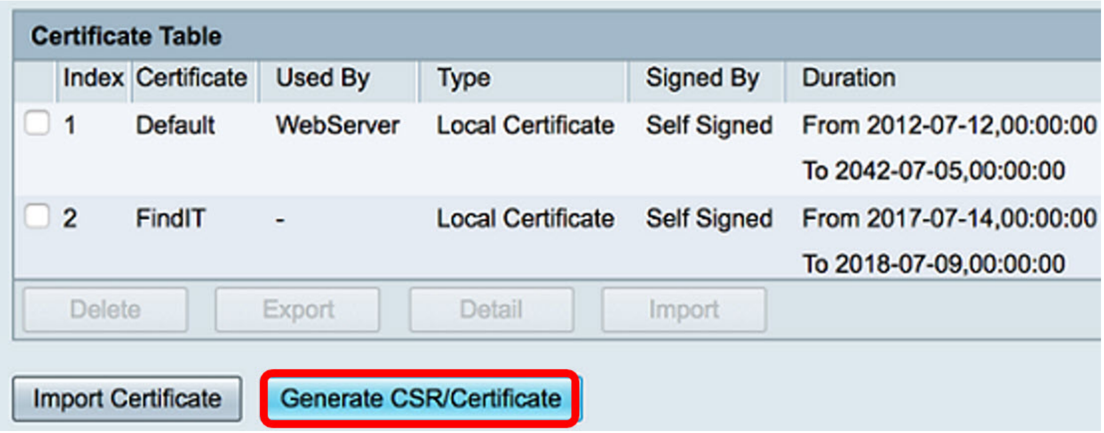
Generate a CSR

Step 1. Log in to the web-based utility of the router and choose **Administration >**

Certificate.



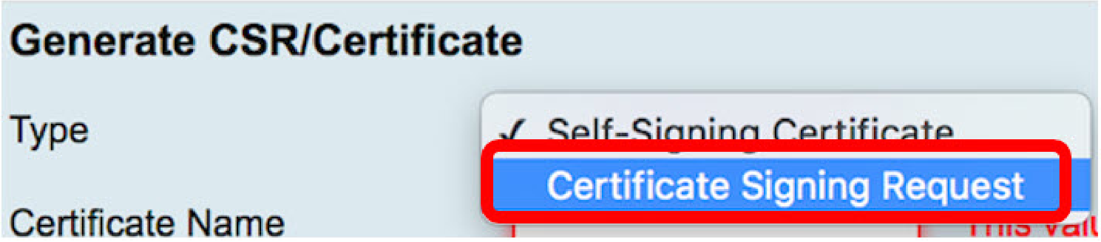
Step 2. Under the Certificate Table, click the **Generate CSR/Certificate** button.



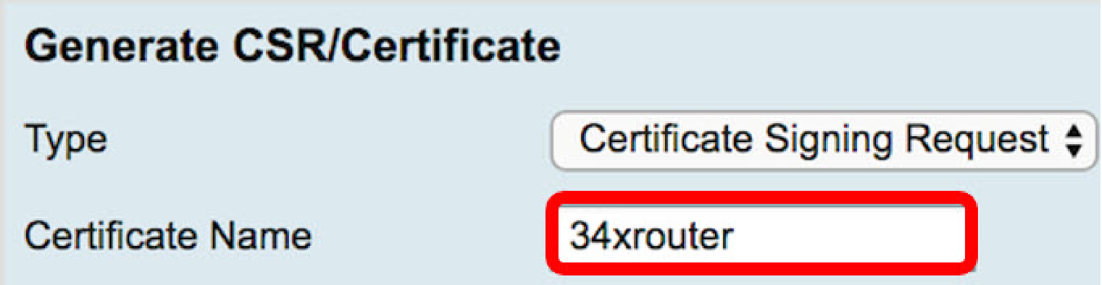
Certificate Table

	Index	Certificate	Used By	Type	Signed By	Duration
□	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
□	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00

Step 3. In the *Generate CSR/Certificate* window,click the *Type* drop-down arrow and choose **Certificate Signing Request**.



Step 4. Enter a name for the certificate in the *Certificate Name* field.



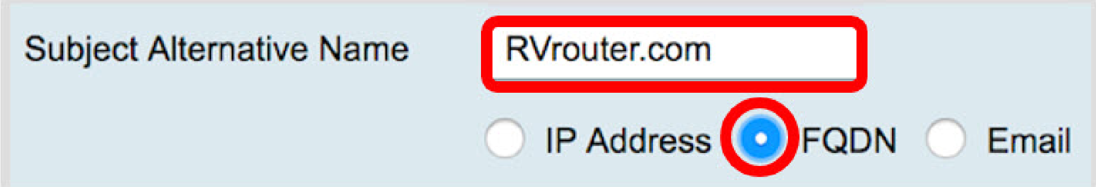
Generate CSR/Certificate

Type: Certificate Signing Request

Certificate Name: 34xrouter

Note: In this example, 34xrouter is used.

Step 5. Enter an alternative name in the *Subject Alternative Name* field and then click the **FQDN** radio button below it to match. The alternative name will be the domain name that can be used to access the router.

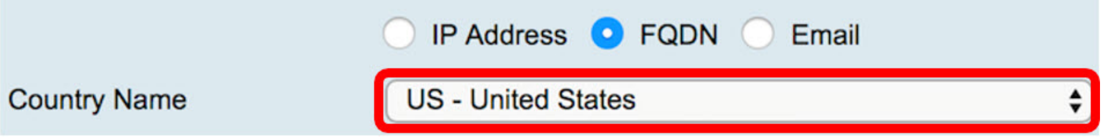


Subject Alternative Name: RVrouter.com

○ IP Address ● FQDN ○ Email

Note: In this example, RVrouter.com is used.

Step 6. Click the *Country Name* drop-down arrow to choose the country of your location.

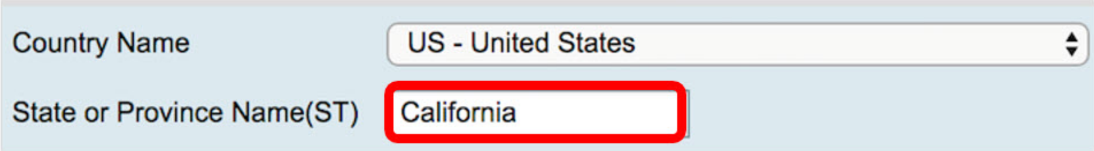


○ IP Address ● FQDN ○ Email

Country Name: US - United States

Note: In this example, US - United States is chosen.

Step 7. Enter the name of the state or province in the *State or Province Name(ST)* field.

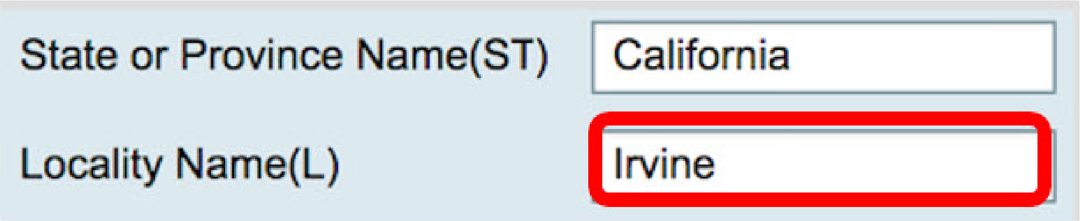


Country Name: US - United States

State or Province Name(ST): California

Note: In this example, California is used.

Step 8. Enter the locality in the *Locality Name(L)* field.

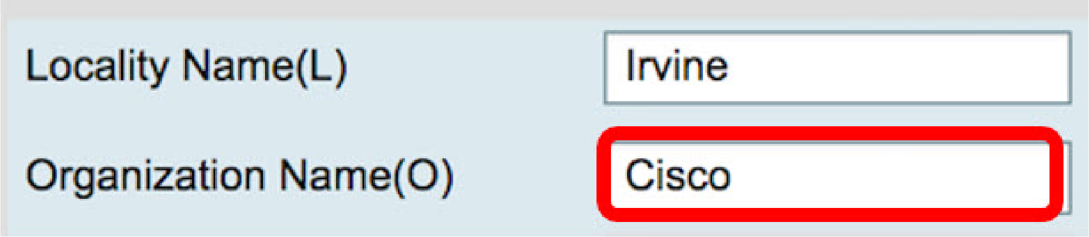


State or Province Name(ST): California

Locality Name(L): Irvine

Note: In this example, Irvine is used.

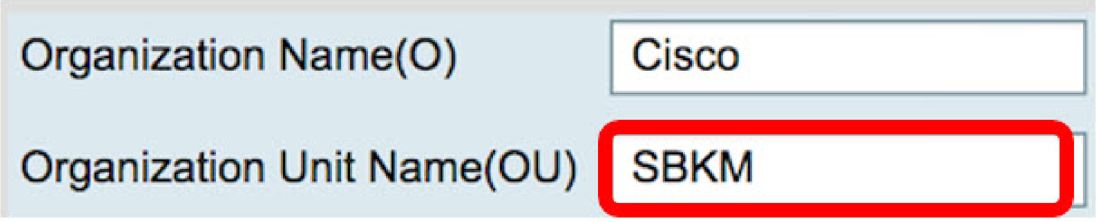
Step 9. Enter the Organization Name(O) in the field provided.



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

Note: In this example, Cisco is used.

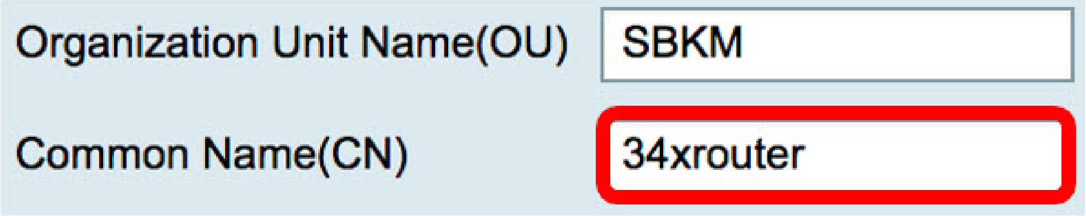
Step 10. Enter the Organization Unit Name(OU) in the field provided.



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

Note: In this example, SBKM is used.

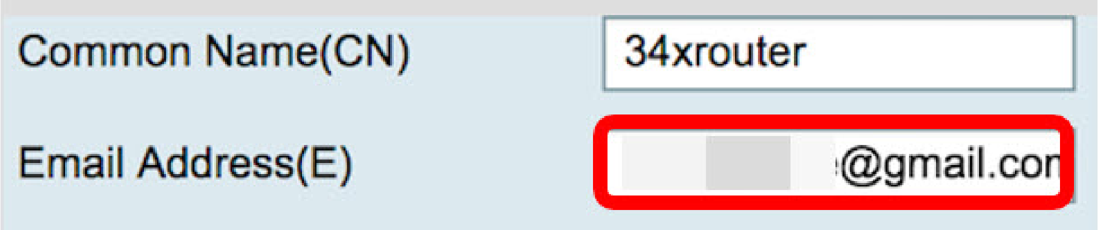
Step 11. Enter a name in the *Common Name(CN)* field.



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

Note: In this example, 34xrouter is used.

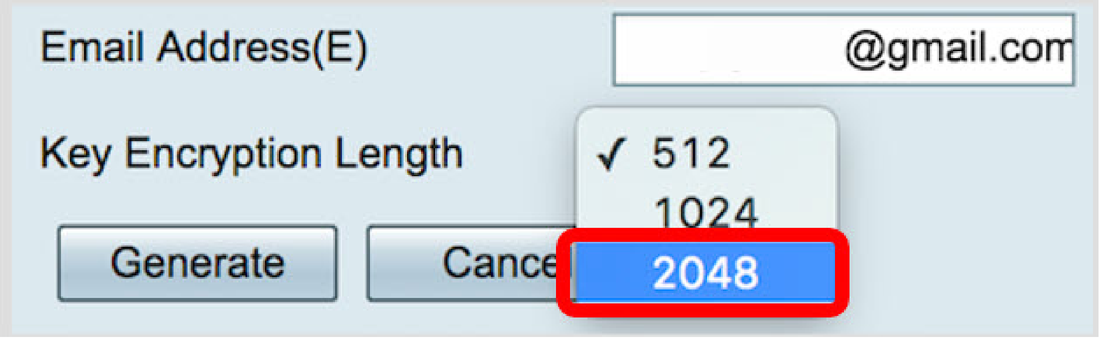
Step 12. Enter your email address or any email address where you want the certificate to be sent.



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

Note: In this example, a gmail.com email address is used.

Step 13. Choose a *Key Encryption Length* from the drop-down menu to set the number of bits in your key. The default length is 512.

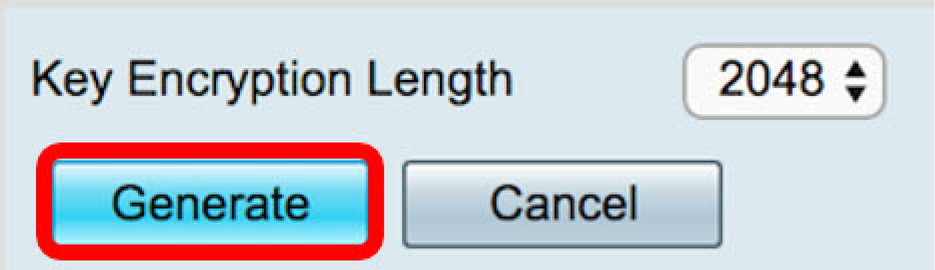


Email Address(E): @gmail.com

Key Encryption Length: ✓ 512 / 1024 / 2048

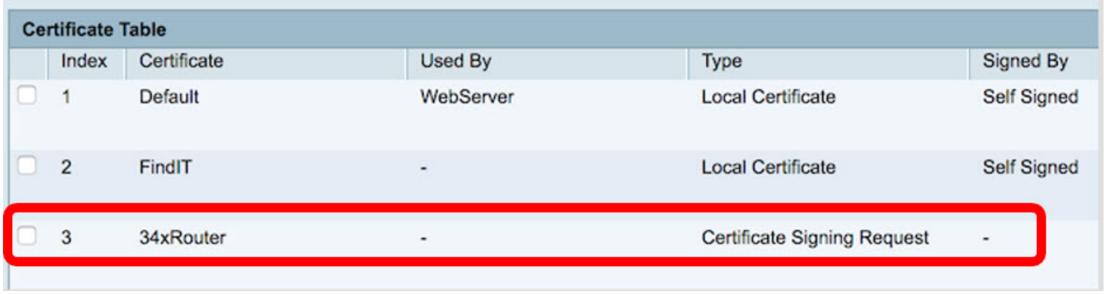
Note: In this example, 2048 is used. This is highly recommended since a longer encryption is more difficult to decode compared to shorter keys, thus, making it more secure.

Step 14. Click **Generate**.



Key Encryption Length: 2048

The certificate request you have created will now appear in the Certificate Table.



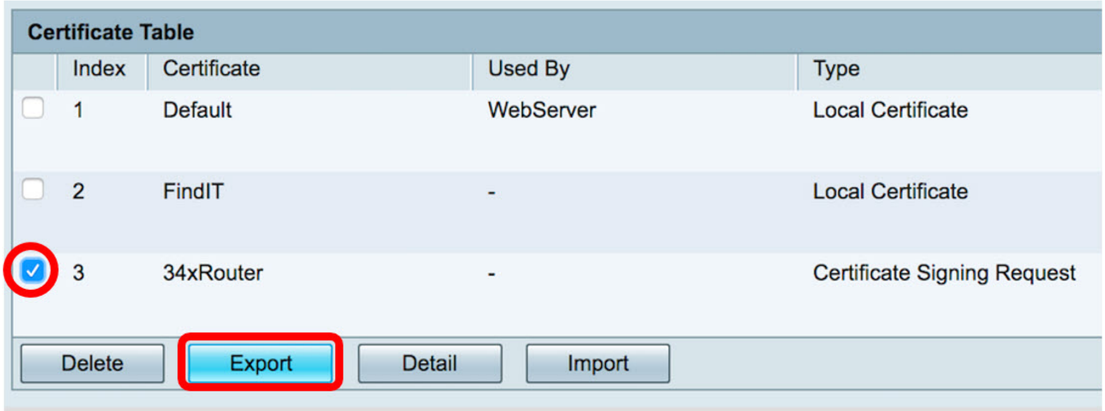
Certificate Table

	Index	Certificate	Used By	Type	Signed By
□	1	Default	WebServer	Local Certificate	Self Signed
□	2	FindIT	-	Local Certificate	Self Signed
□	3	34xRouter	-	Certificate Signing Request	-

You now have successfully generated a CSR.

Export the CSR

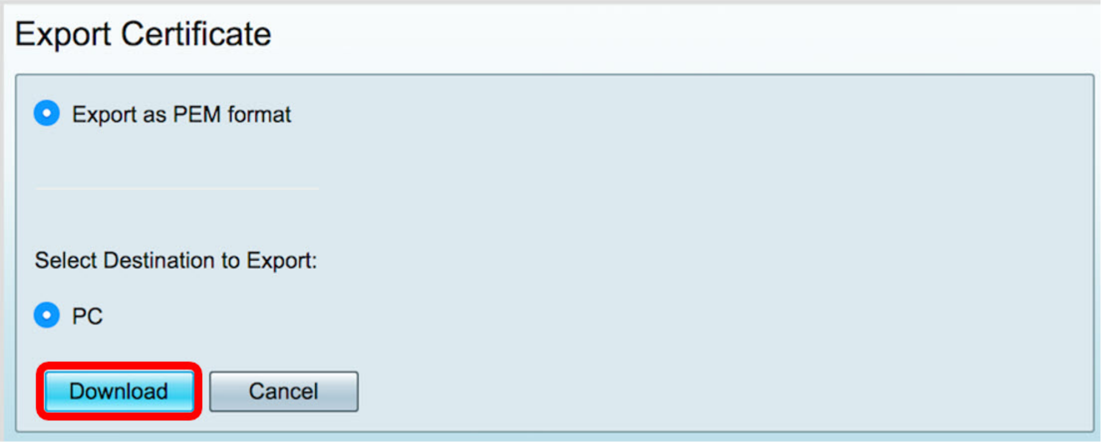
Step 1. Check the box beside the certificate request in the Certificate Table and click **Export**.



Certificate Table

	Index	Certificate	Used By	Type
□	1	Default	WebServer	Local Certificate
□	2	FindIT	-	Local Certificate
☑	3	34xRouter	-	Certificate Signing Request

Step 2. Click **Download** in the *Export Certificate* window to download the file into your computer in PEM format.



Export Certificate

● Export as PEM format

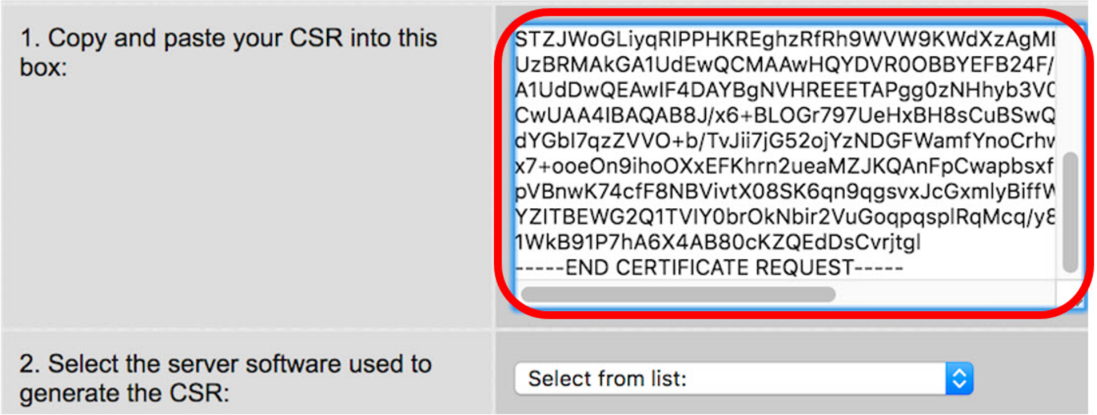
Select Destination to Export:

● PC

You now have successfully exported the CSR into your computer.

Upload the CSR to the Certificate Provider

Step 1. Open the downloaded file using a notepad and copy the CSR then paste it into the field provided in the 3rd party SSL certificate provider site.



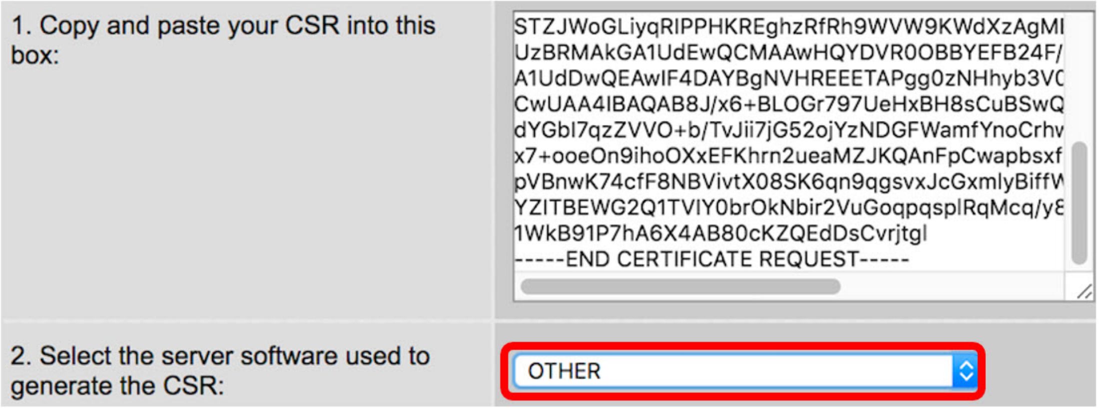
1. Copy and paste your CSR into this box:

```
STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI
UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/
A1UdDwQEAwIF4DAYBgNVHREEETAPgg0zNHhyb3V(
CwUAA4IBAQAB8J/x6+BLOGr797UeHxBH8sCuBSwQ
dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv
x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf
pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffW
YZITBEWG2Q1TVIY0brOkNbir2VuGoqpqsplRqMcq/y8
1WkB91P7hA6X4AB80cKZQEdDsCvrjtgl
-----END CERTIFICATE REQUEST-----
```

2. Select the server software used to generate the CSR: Select from list:

Note: In this example, Comodo.com is used as the certificate provider.

Step 2. Select the server software used to generate the CSR. In this case, since the RV34x router is not on the list, OTHER is chosen.



1. Copy and paste your CSR into this box:

```
STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI
UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/
A1UdDwQEAwIF4DAYBgNVHREEETAPgg0zNHhyb3V(
CwUAA4IBAQAB8J/x6+BLOGr797UeHxBH8sCuBSwQ
dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv
x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf
pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffW
YZITBEWG2Q1TVIY0brOkNbir2VuGoqpqsplRqMcq/y8
1WkB91P7hA6X4AB80cKZQEdDsCvrjtgl
-----END CERTIFICATE REQUEST-----
```

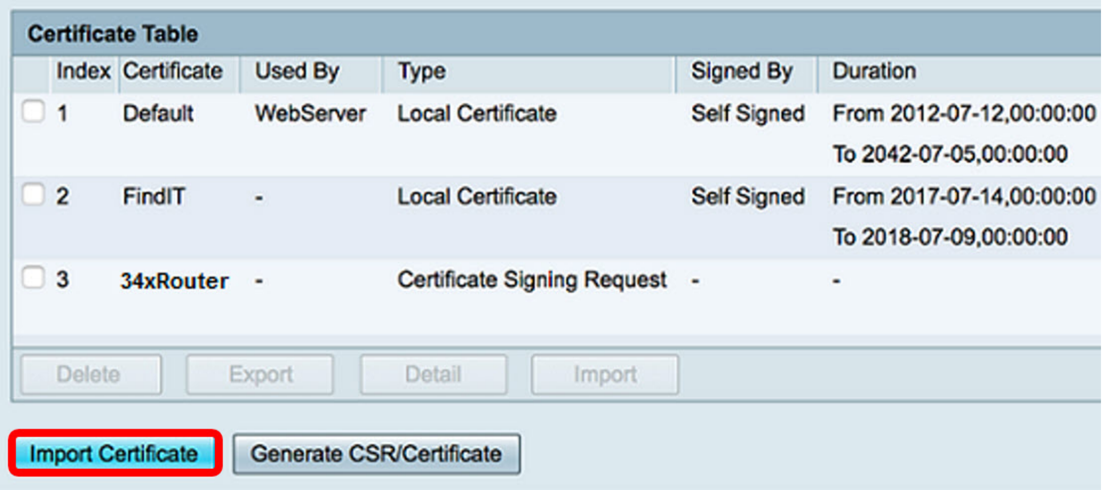
2. Select the server software used to generate the CSR: OTHER

Step 3. Download your certificate into your computer.

Upload the 3rd SSL Party Certificate

Step 1. In the web-based utility of the router, click the **Import Certificate** button under the

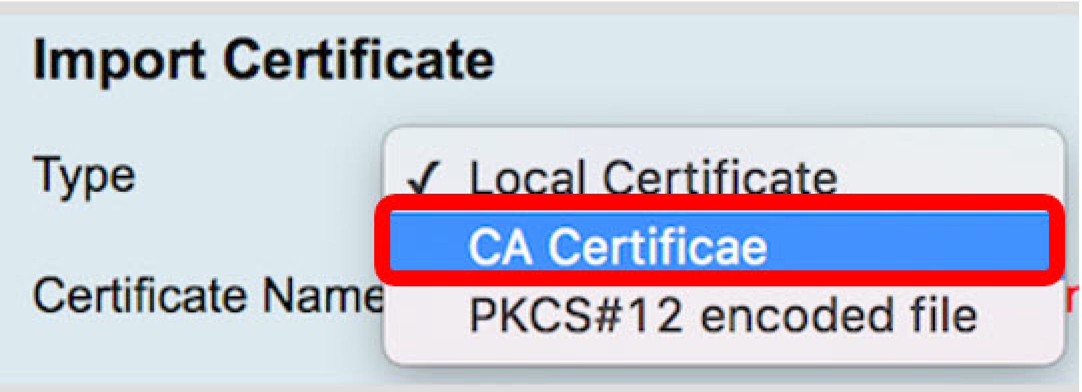
Certificate Table.



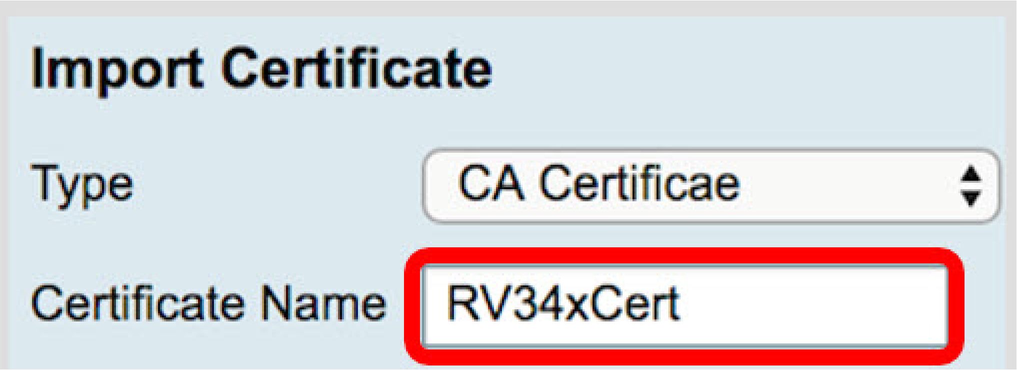
Certificate Table

	Index	Certificate	Used By	Type	Signed By	Duration
□	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
□	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00
□	3	34xRouter	-	Certificate Signing Request	-	-

Step 2. In the *Import Certificate* window, click the *Type* drop-down menu and choose **CA Certificate**.



Step 3. Enter a Certificate Name in the field provided.



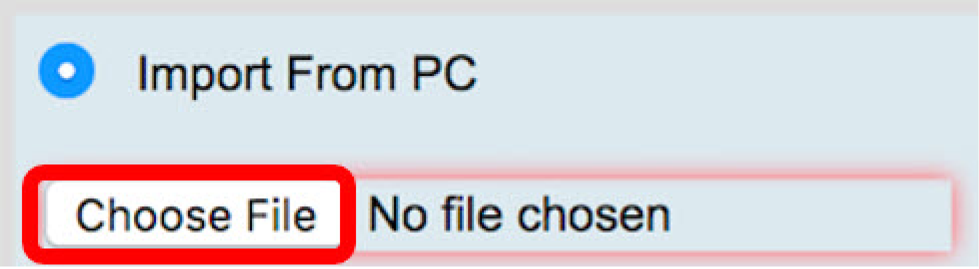
Import Certificate

Type: CA Certificae

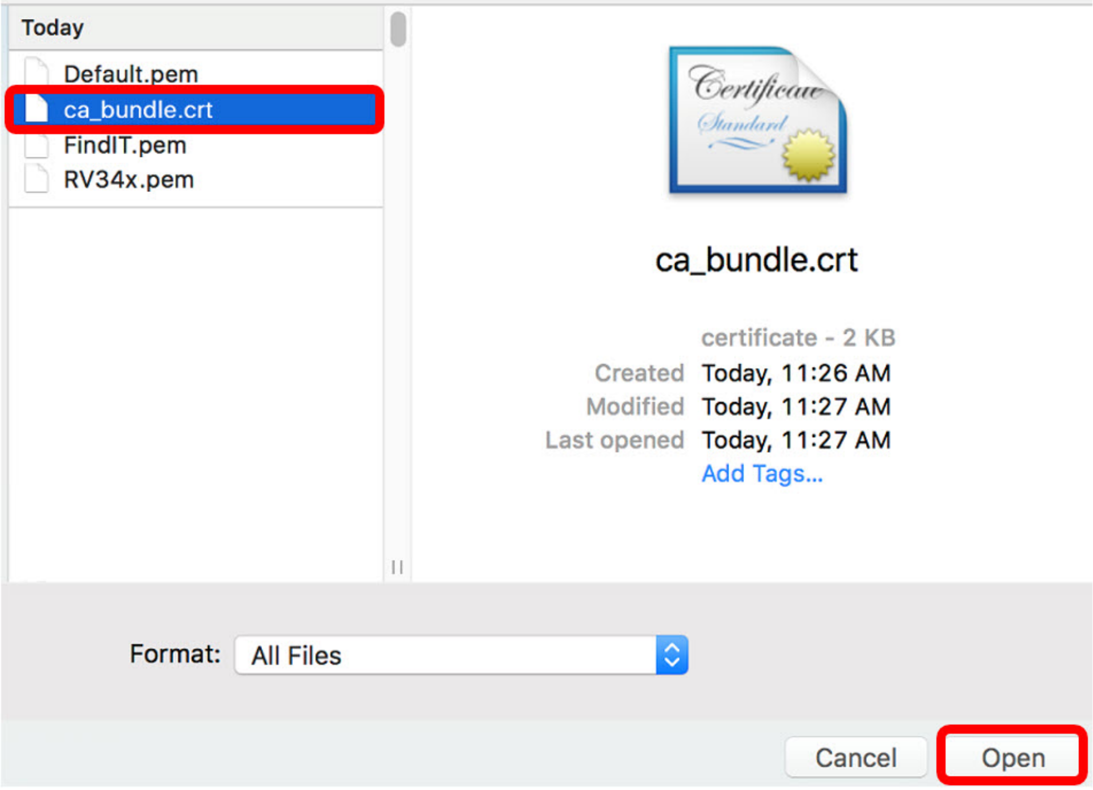
Certificate Name: RV34xCert

Note: In this example, RV34xCert is used.

Step 4. Click the **Choose File** button and locate the certificate file you have downloaded from the CA.



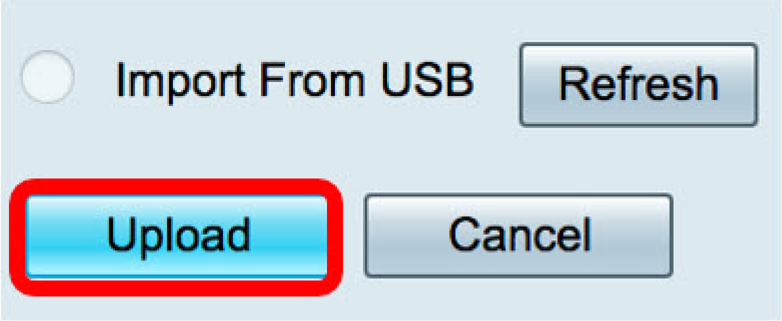
Step 5. Click on the file and then click **Open**.



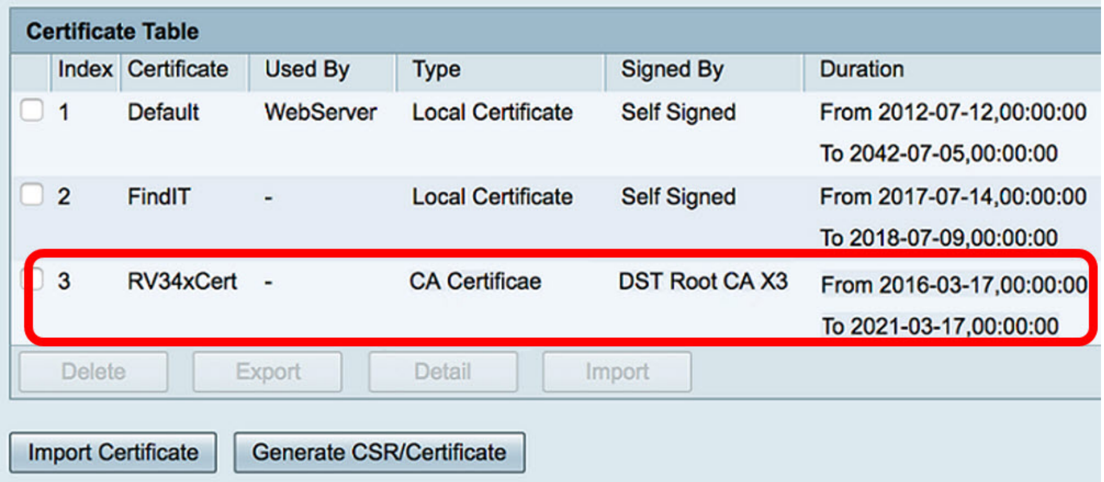
certificate - 2 KB
Created Today, 11:26 AM
Modified Today, 11:27 AM
Last opened Today, 11:27 AM

Format: All Files

Step 6. Click **Upload**.



The Certificate Table will now show the new certificate name and the type is now replaced with CA certificate with the label that it has been signed by the 3rd party CA.



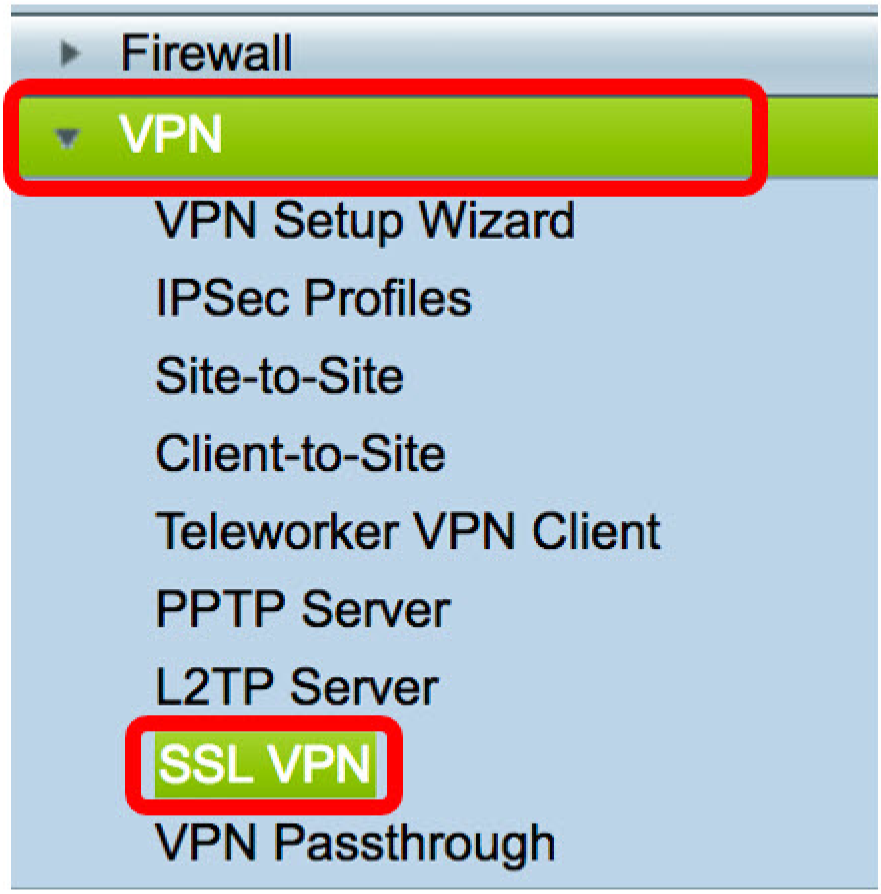
Certificate Table

	Index	Certificate	Used By	Type	Signed By	Duration
□	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
□	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00
□	3	RV34xCert	-	CA Certificae	DST Root CA X3	From 2016-03-17,00:00:00 To 2021-03-17,00:00:00

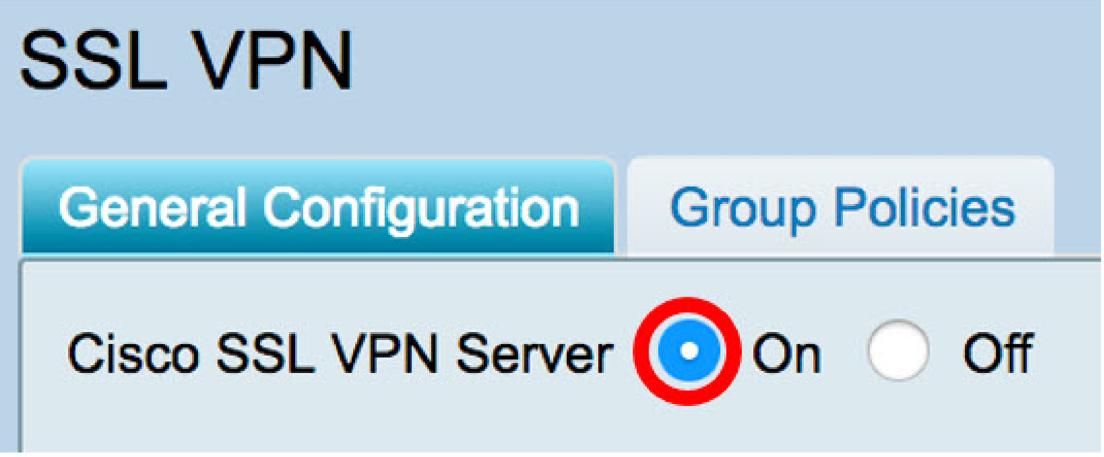
You now have successfully uploaded a 3rd party SSL certificate on the RV34x Router.

Replace the Default Self-Signed Certificate

Step 1. In the web-based utility, choose **VPN > SSL VPN**.



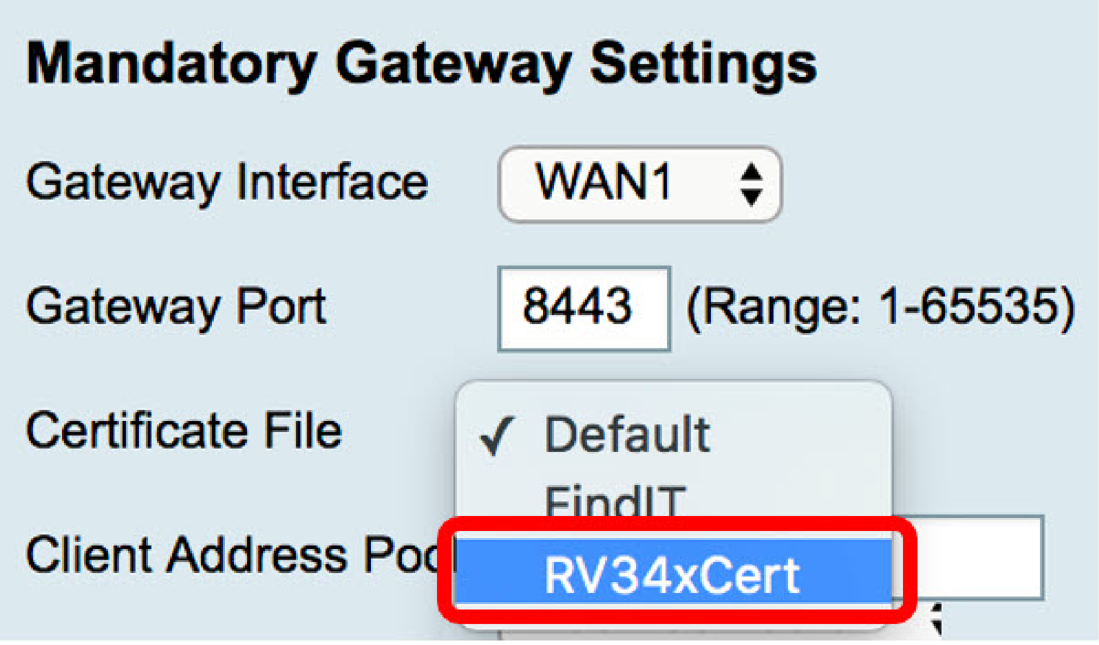
Step 2. Click the **On** radio button to enable the Cisco SSL VPN Server.



SSL VPN

Cisco SSL VPN Server ● On ○ Off

Step 3. Under Mandatory Gateway Settings, click the *Certificate File* drop-down menu and replace the default certificate by choosing the newly uploaded SSL certificate.



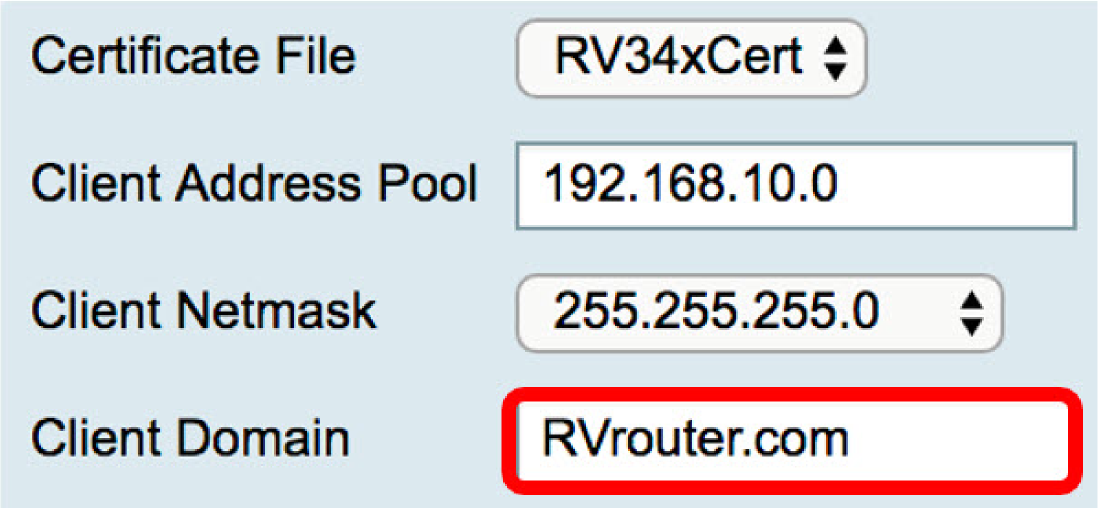
Mandatory Gateway Settings

Gateway Interface: WAN1

Gateway Port: 8443 (Range: 1-65535)

Certificate File

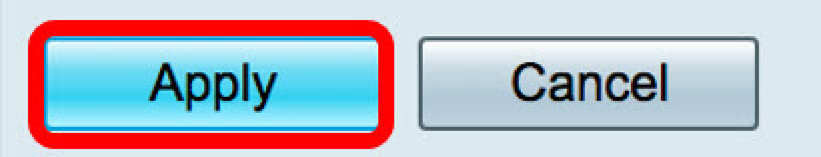
Step 4. Enter the required Client Domain in the field provided.



Certificate File	RV34xCert
Client Address Pool	192.168.10.0
Client Netmask	255.255.255.0
Client Domain	RVrouter.com

Note: In this example, RVrouter.com is used.

Step 5. Click **Apply**.



You now have successfully replaced the default self-signed certificate with the 3rd party SSL certificate.

You might find also this article informative: RV34x Series Router Frequently Asked Questions (FAQs)

This site offers several links to other articles you might find interesting: RV34x Series Router Product Page