View/Add Trusted SSL Certificate on RV320 and RV325 VPN Routers

Objective

Certificates are used to verify the user identity on a computer or Internet and to enhance a private or secured conversation. On the RV320, you can add a maximum of 50 certificates through self-signing or third-party authorization. You can export a certificate for a client or for an administrator, save that in a PC or USB and then import that. Secure Sockets Layer (SSL) is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remains private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. To be able to generate an SSL link, a web server requires a SSL Certificate.

This article explains how to View and Add Trusted SSL Certificate on the RV32x VPN Router Series.

Applicable Devices

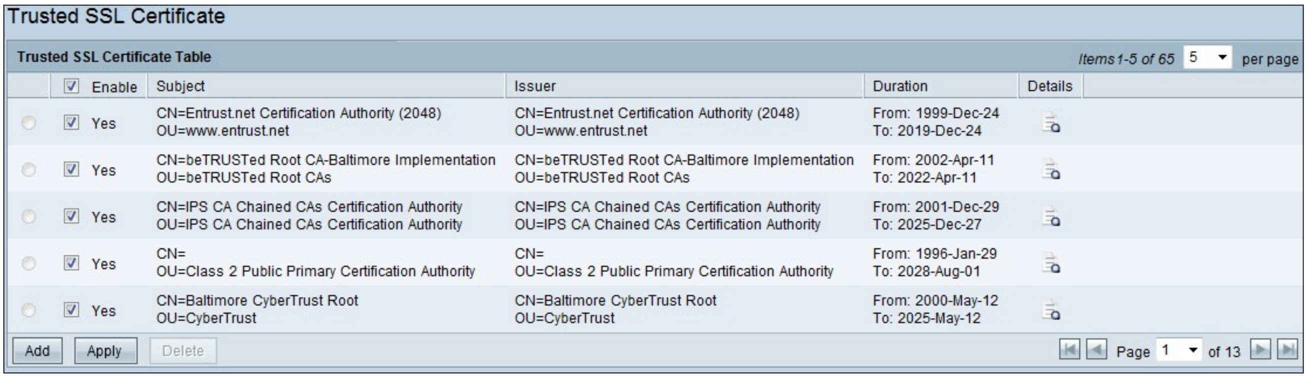
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

Software Version

- v1.0.1.17

Trusted SSL Certificate

Step 1. Log in to the web configuration utility and choose **Certificate Management > Trusted SSL Certificate**. The *Trusted SSL* page opens:



Trusted SSL Certificate

Trusted SSL Certificate Table — *Items 1-5 of 65* 5 per page

	☑ Enable	Subject	Issuer	Duration	Details
○	☑ Yes	CN=Entrust.net Certification Authority (2048) OU=www.entrust.net	CN=Entrust.net Certification Authority (2048) OU=www.entrust.net	From: 1999-Dec-24 To: 2019-Dec-24	
○	☑ Yes	CN=beTRUSTed Root CA-Baltimore Implementation OU=beTRUSTed Root CAs	CN=beTRUSTed Root CA-Baltimore Implementation OU=beTRUSTed Root CAs	From: 2002-Apr-11 To: 2022-Apr-11	
○	☑ Yes	CN=IPS CA Chained CAs Certification Authority OU=IPS CA Chained CAs Certification Authority	CN=IPS CA Chained CAs Certification Authority OU=IPS CA Chained CAs Certification Authority	From: 2001-Dec-29 To: 2025-Dec-27	
○	☑ Yes	CN= OU=Class 2 Public Primary Certification Authority	CN= OU=Class 2 Public Primary Certification Authority	From: 1996-Jan-29 To: 2028-Aug-01	
○	☑ Yes	CN=Baltimore CyberTrust Root OU=CyberTrust	CN=Baltimore CyberTrust Root OU=CyberTrust	From: 2000-May-12 To: 2025-May-12	

The *Trusted SSL Certificate* Page Contains the following fields:

- Enable — It shows whether a certificate is Enabled or Disabled.

- Issuer — It provides the Information about the Issuer who Issues the certificate

- Subject — It shows to whom the certificate is issued.

- Duration — It shows the date the certificate expires. The security of the Web site cannot be guaranteed if this date has been exceeded.

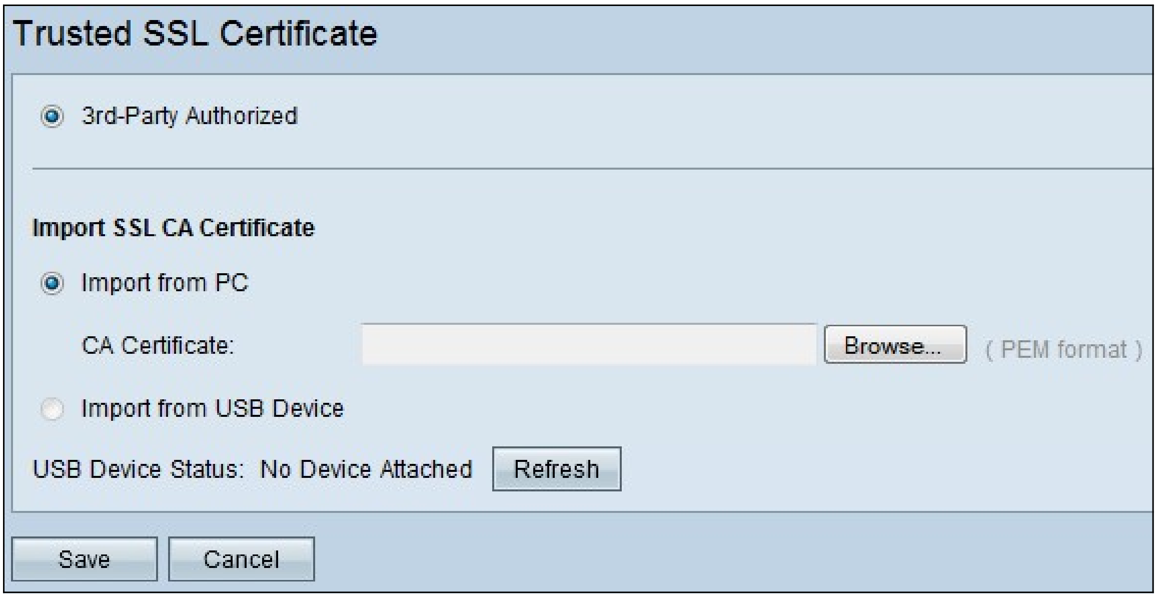
- Details — It shows all the details about the Certificate Issuer, Certificate Serial Number, and the Expiration Date are generated by the CA service. The information is used when a Generate Certificate Signing Request is created and sent to your CA service for validation

Step 2. Click the **Enable** Check-box to enable a particular SSL certificate.

Step 3. Click **Add** to get a new certificate from the PC or from USB.

- Import From PC — From the PC you can locate the Certificate and import to the device

- Import From USB — From the USB which is attached to the device you can also import the certificate.



Trusted SSL Certificate

● 3rd-Party Authorized

Import SSL CA Certificate

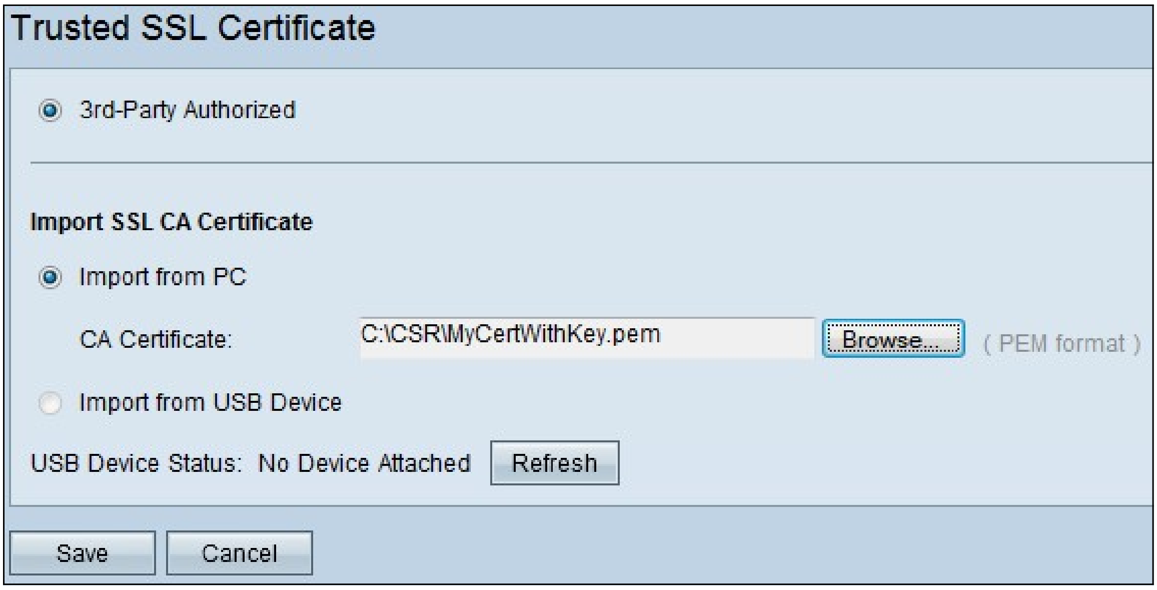
● Import from PC

CA Certificate:

○ Import from USB Device

USB Device Status: No Device Attached

Step 3. Click on **Browse** to locate the CA Certificate from the PC.



Trusted SSL Certificate

● 3rd-Party Authorized

Import SSL CA Certificate

● Import from PC

CA Certificate: C:\CSR\MyCertWithKey.pem

○ Import from USB Device

USB Device Status: No Device Attached

Step 4. Click **Save** to add the certificate to the trusted SSL Certificate Table.