Generate Certificates on RV320 and RV325 VPN Routers

Objective

One of the most common forms of cryptography today is public-key cryptography. Public-key cryptography utilizes a public key and a private key. The system first encrypts information through the use of the public key. The information can then only be decrypted through the use of the private key. A common use for public-key cryptography is the encryption of application traffic through the use of a Secure Socket Layer (SSL) or Transport Layer Security (TLS) connection. A Certificate is a method used to distribute a public key and other information about a server and the organization who is responsible for it. Certificates can be digitally signed by a Certificate Authority (CA). A CA is a trusted third party that has confirmed that the information contained in the certificate is accurate.

This article explains how to Generate Certificates on a RV32x VPN Router Series.

Applicable Devices

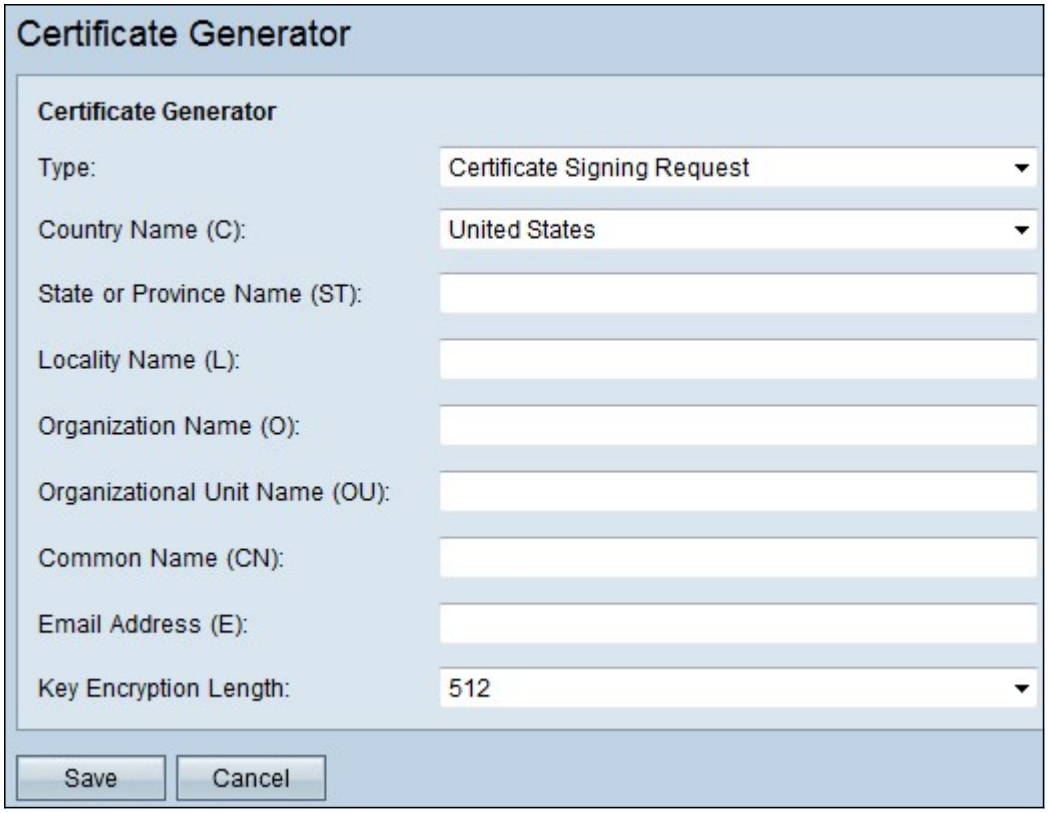
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

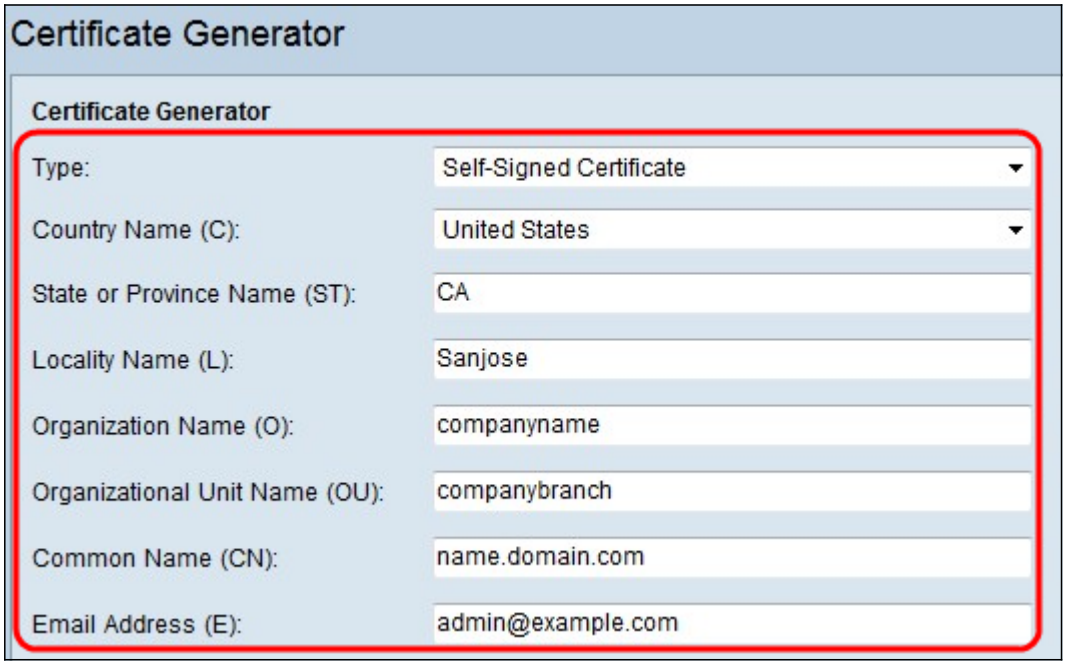
Software Version

- v1.1.0.09

Generate Certificate

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





Step 2. Choose the appropriate certificate type from the Type drop-down list:

- Self-Signed Certificate — This is a Secure Socket Layer (SSL) certificate which is signed by its own creator. This certificate is less trusty, as it can not be cancelled if the private key is compromised somehow by the attacker.

- Certified Signing Request — This is a public key infrastructure (PKI) which is sent to the certificate authority to apply for a digital identity certificate. It is more secure than self-signed as the private key is kept secret.

Step 3. Choose a country name in which your organization is legally registered from the Country Name Drop-down.

Step 4. Enter a name or abbreviation of the state, province, region or territory where your

organization is located in the State or Province Name field.

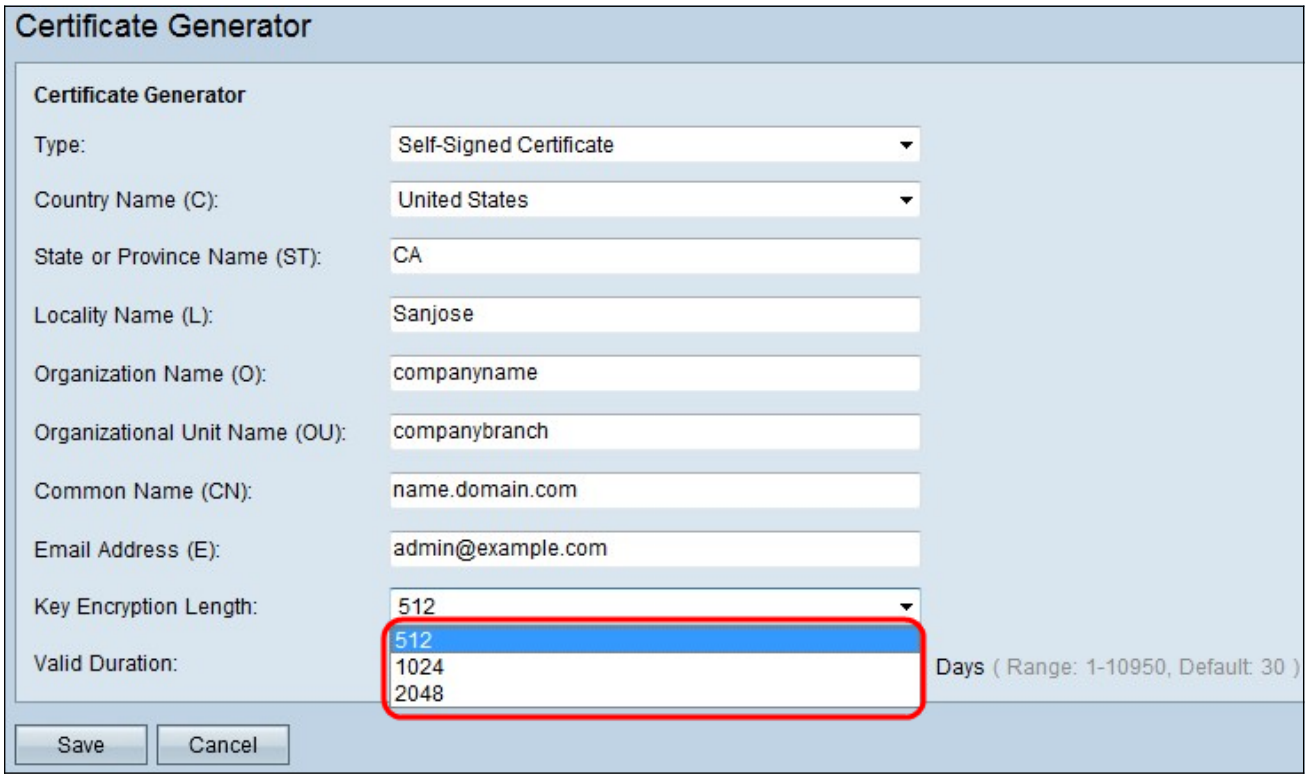
Step 5. Enter a name of the city/locality in which your organization is registered/located in the Locality Name field .

Step 6. Enter a name under which your business is legally registered, If you are enrolling as a small business/sole proprietor, enter the name of the certificate requester in the Organization Name field.

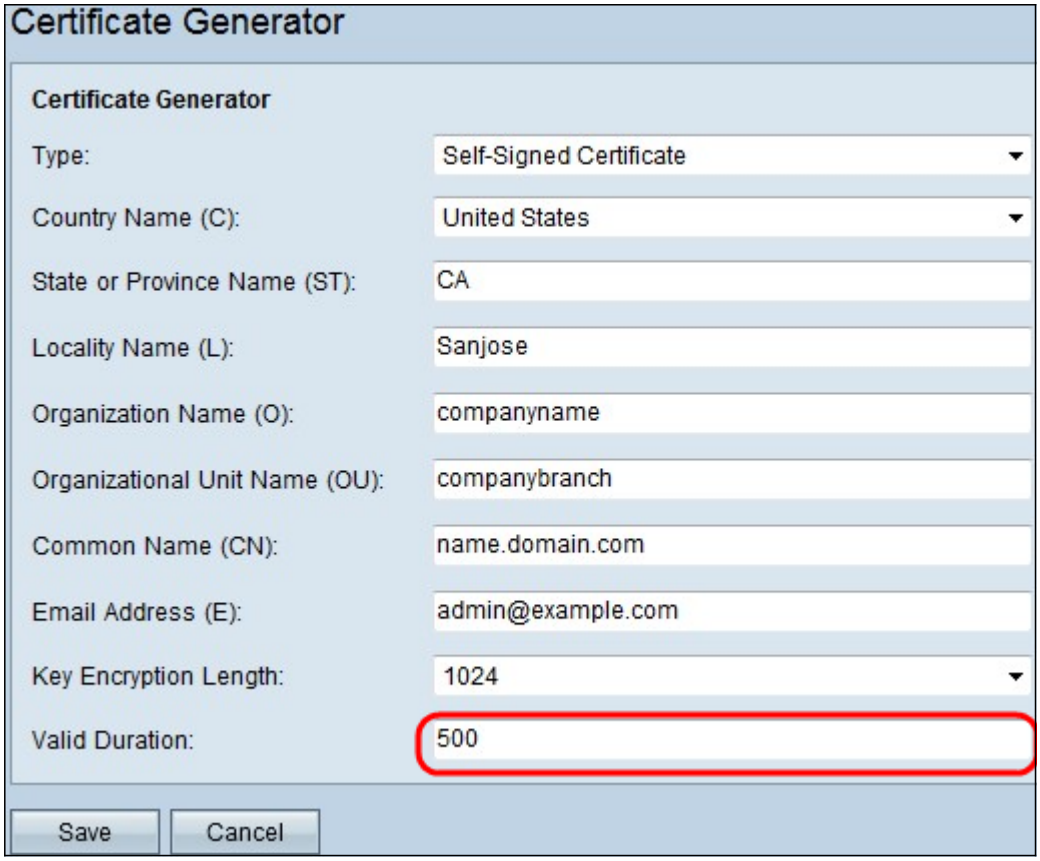
Step 7. Enter a name in the Organization Unit Name field to differentiate between divisions within an organization.

Step 8. Enter a name in the Common Name field. This name must be the fully-qualified domain name of the website for which you use the certificate for.

Step 9. Enter the Email Address of person who wants to generate the certificate.



Step 10. Choose a Key length from the Key Encryption Length drop-down, the larger the key size, the more secure the certificate. The larger the key size, the greater the processing time.



Note: If you chose the certificate type as certificate signing request, then skip Step 11 and proceed.

Step 11. Enter the number of days that the certificate is valid for.

Step 12. Click **Save** to Generate the Certificate. The generated certificate is shown on the *My Certificate* page. To view *My Certificate* page, choose **Certificate Management > My Certificate**.