# Erstellen von Zertifikaten für RV320- und RV325-VPN-Router

## Ziel

Eine der gängigsten Formen der Kryptografie ist heute die Verschlüsselung mit öffentlichen Schlüsseln. Bei der Verschlüsselung mit öffentlichem Schlüssel werden ein öffentlicher Schlüssel und ein privater Schlüssel verwendet. Das System verschlüsselt Daten zuerst mithilfe des öffentlichen Schlüssels. Die Informationen können dann nur mithilfe des privaten Schlüssels entschlüsselt werden. Eine häufige Verwendung bei der Verschlüsselung von öffentlichen Schlüsseln ist die Verschlüsselung des Anwendungsdatenverkehrs mithilfe einer SSL- (Secure Socket Layer)- oder TLS-Verbindung (Transport Layer Security). Ein Zertifikat ist eine Methode zur Verteilung eines öffentlichen Schlüssels und anderer Informationen über einen Server und die Organisation, die für diesen Schlüssel verantwortlich ist. Zertifikate können durch eine Zertifizierungsstelle (Certificate Authority, CA) digital signiert werden. Eine Zertifizierungsstelle ist ein vertrauenswürdiger Drittanbieter, der bestätigt hat, dass die im Zertifikat enthaltenen Informationen korrekt sind.

In diesem Artikel wird erläutert, wie Zertifikate auf einer RV32x VPN Router-Serie generiert werden.

## Anwendbare Geräte

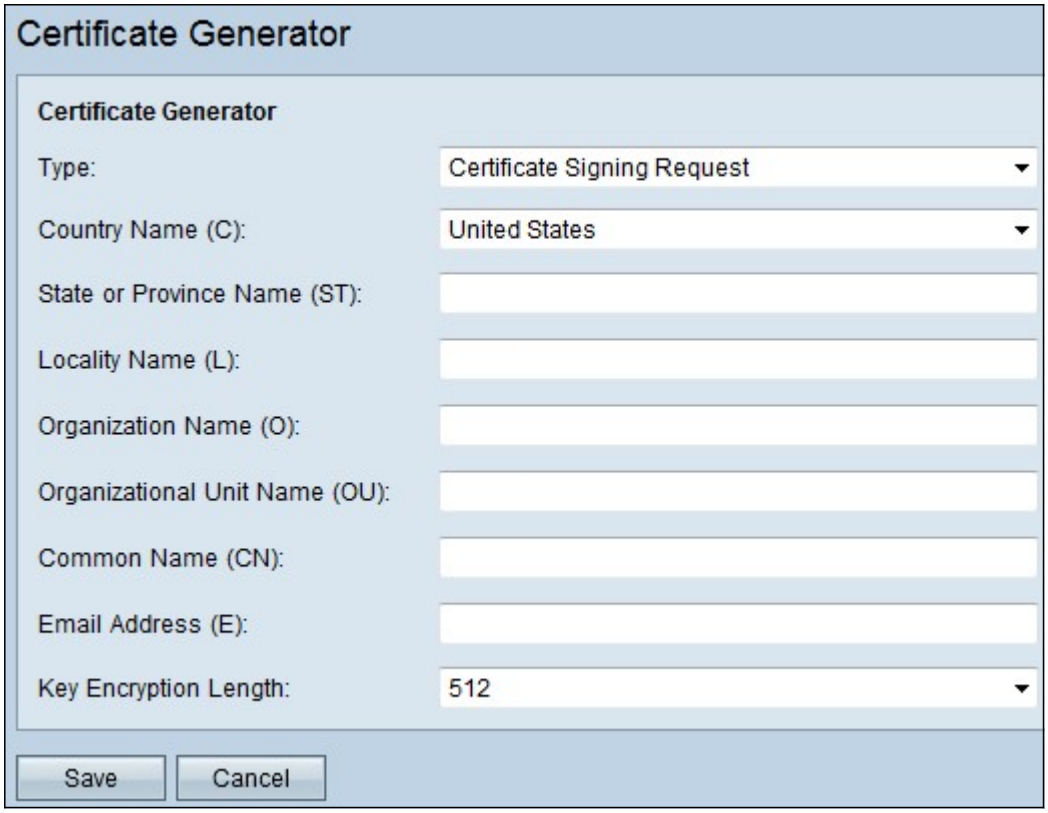
·RV320 Dual-WAN VPN-Router
· RV325 Gigabit Dual-WAN VPN-Router

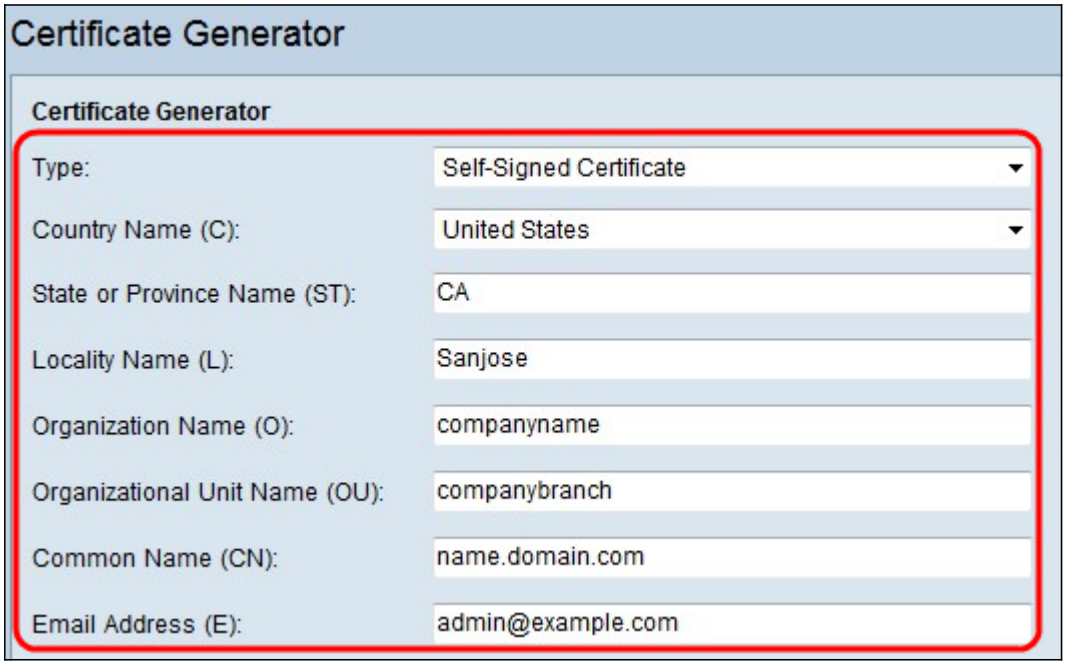
## Softwareversion

·v1.1.0.09

## Zertifikat generieren

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Certificate Management > Certificate Generator aus**. Die Seite *Certificate Generator* wird geöffnet:




Schritt 2: Wählen Sie in der Dropdown-Liste Type (Typ) den entsprechenden Zertifikatstyp aus:

·Selbstsigniertes Zertifikat - Dies ist ein SSL-Zertifikat (Secure Socket Layer), das vom eigenen Ersteller signiert wird. Dieses Zertifikat ist weniger vertrauenswürdig, da es nicht abgebrochen werden kann, wenn der private Schlüssel vom Angreifer irgendwie kompromittiert wird.

·Certified Signing Request - Dies ist eine Public Key Infrastructure (PKI), die an die Zertifizierungsstelle gesendet wird, um ein digitales Identitätszertifikat zu beantragen. Sie ist sicherer als selbstsignierte Schlüssel, da der private Schlüssel geheim gehalten wird.

Schritt 3: Wählen Sie im Dropdown-Menü "Ländername" einen Ländernamen aus, in dem Ihre Organisation legal registriert ist.

Schritt 4: Geben Sie einen Namen oder eine Abkürzung für das Bundesland, die Provinz, die Region oder das Gebiet ein, in dem sich Ihr Unternehmen im Feld "Bundesland/Region" befindet.

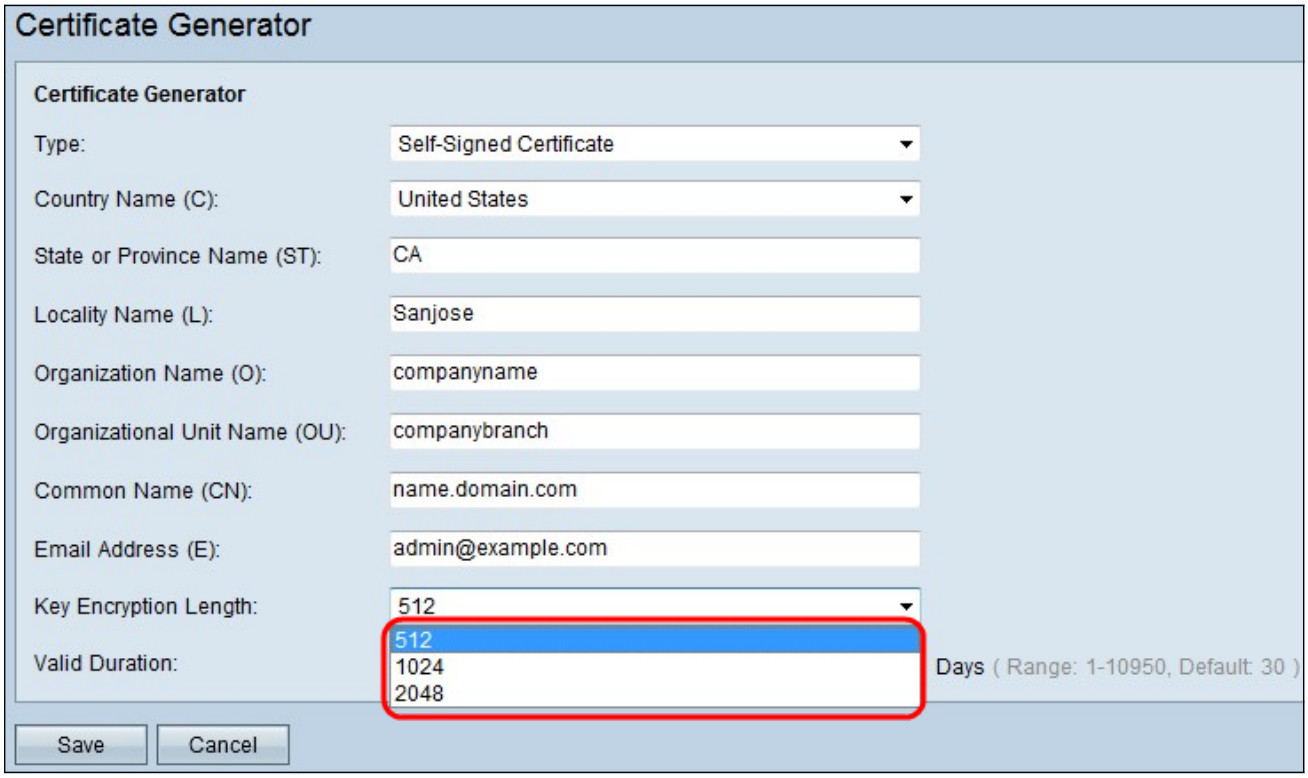
Schritt 5: Geben Sie im Feld "Locality Name" (Ortsname) den Namen der Stadt bzw. des Ortes ein, in der/dem Ihre Organisation registriert ist/sich befindet.

Schritt 6: Geben Sie einen Namen ein, unter dem Ihr Unternehmen rechtlich registriert ist. Wenn Sie sich als kleines Unternehmen/Einzelunternehmer anmelden, geben Sie den Namen des Zertifikatsanforderers in das Feld Organisationsname ein.

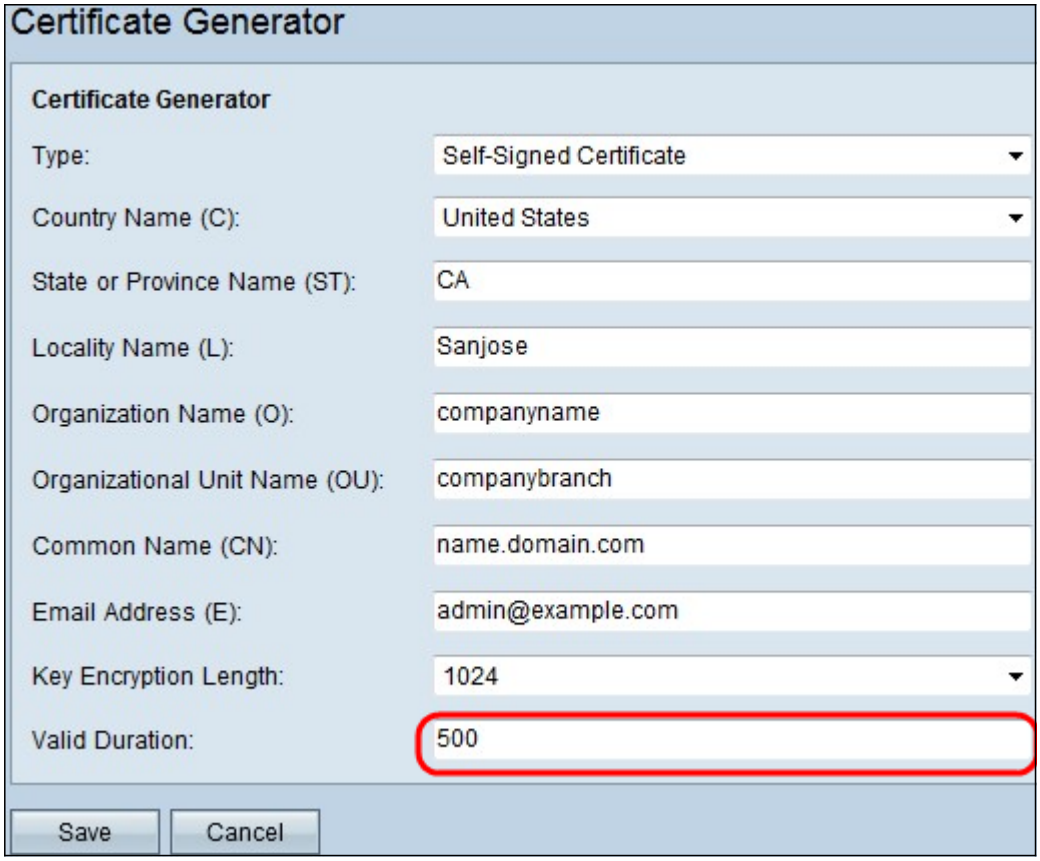
Schritt 7: Geben Sie im Feld Name der Organisationseinheit einen Namen ein, um zwischen den Abteilungen innerhalb einer Organisation zu unterscheiden.

Schritt 8: Geben Sie im Feld "Allgemeiner Name" einen Namen ein. Dieser Name muss der vollqualifizierte Domänenname der Website sein, für die Sie das Zertifikat verwenden.

Schritt 9: Geben Sie die E-Mail-Adresse der Person ein, die das Zertifikat generieren möchte.




Schritt 10: Wählen Sie im Dropdown-Menü Key Encryption Length (Schlüssellänge) eine Schlüssellänge aus. Je größer die Schlüssellänge, desto sicherer ist das Zertifikat. Je größer die Schlüssellänge, desto länger dauert die Verarbeitung.




**Hinweis:** Wenn Sie den Zertifikatstyp als Zertifikatssignierungsanfrage ausgewählt haben, überspringen Sie Schritt 11 und fahren Sie fort.

Schritt 11: Geben Sie die Anzahl der Tage ein, für die das Zertifikat gültig ist.

Schritt 12: Klicken Sie auf **Speichern**, um das Zertifikat zu generieren. Das generierte Zertifikat wird auf der Seite *Mein Zertifikat* angezeigt. Um die Seite *Mein Zertifikat* anzuzeigen, wählen Sie **Zertifikatsverwaltung > Zertifikat aus**.