Ersetzen Sie das Standard-selbstsignierte Zertifikat durch ein SSL-Zertifikat eines Drittanbieters auf dem Router der Serie RV34x.

Einführung

Ein digitales Zertifikat bescheinigt das Eigentum an einem öffentlichen Schlüssel durch den benannten Subjekt des Zertifikats. Dadurch können sich die Parteien auf Signaturen oder Behauptungen des privaten Schlüssels verlassen, der dem öffentlichen Schlüssel entspricht, der zertifiziert ist. Ein Router kann ein selbstsigniertes Zertifikat generieren, ein Zertifikat, das von einem Netzwerkadministrator erstellt wurde. Sie kann auch Anfragen an Zertifizierungsstellen (Certificate Authority, CA) senden, um ein digitales Identitätszertifikat zu beantragen. Es ist wichtig, legitime Zertifikate von Drittanbieteranwendungen zu erhalten.

CA signiert die Zertifikate auf zwei Arten:

1. CA signiert das Zertifikat mit privaten Schlüsseln.

2. CA signiert die Zertifikate mithilfe der vom RV34x generierten Zertifikatsanforderung (Certificate Signing Request, CSR).

Die meisten Anbieter von gewerblichen Zertifikaten verwenden Zwischenzertifikate. Da das Zwischenzertifikat von der Vertrauenswürdigen Stammzertifizierungsstelle ausgestellt wird, erbt jedes vom Zwischenzertifikat ausgestellte Zertifikat das Vertrauen der Trusted Root, wie eine Vertrauenszertifizierungskette.

Ziel

Dieser Artikel zeigt, wie ein von einer Zertifizierungsstelle ausgestelltes Secure Sockets Layer (SSL)-Zertifikat eines Drittanbieters angefordert und hochgeladen wird, um das selbstsignierte Zertifikat des RV34x-Routers zu ersetzen.

Anwendbare Geräte

- RV340
- RV340 W
- RV345
- RV345P

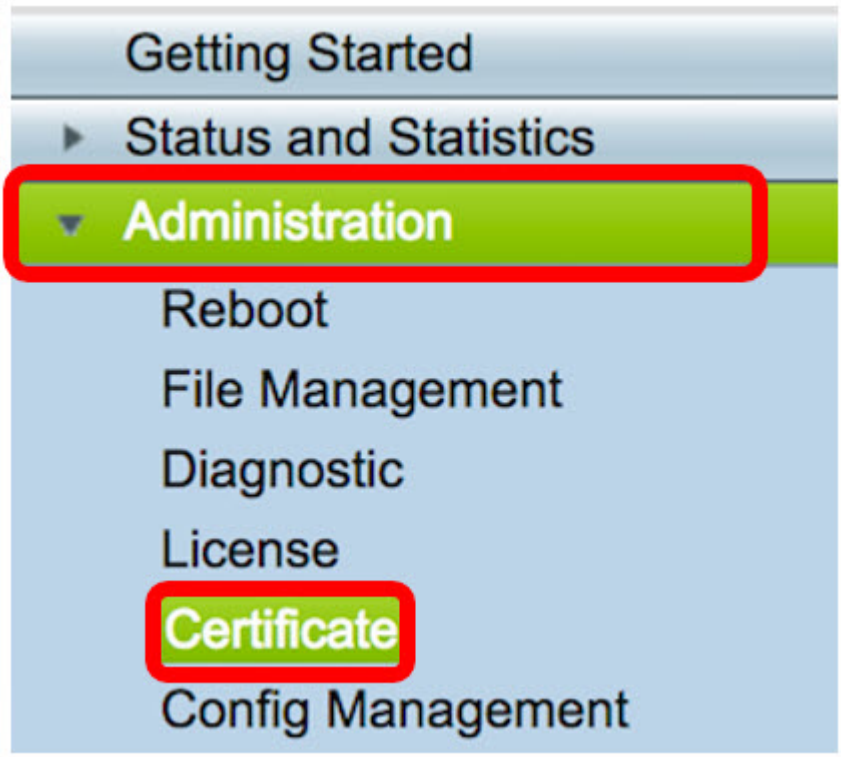
Softwareversion

- 1.0.01.17

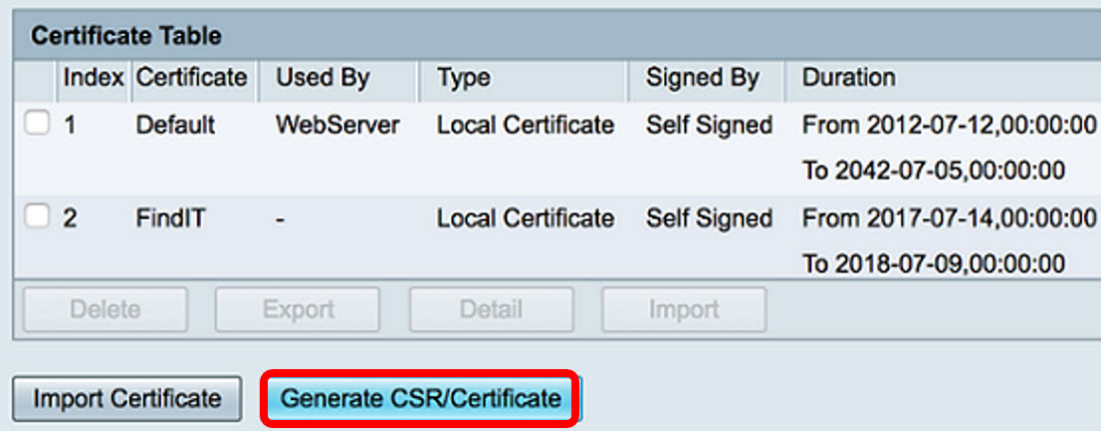
Ersetzen Sie das Standard-selbstsignierte Zertifikat durch ein SSL-Zertifikat eines Drittanbieters.

CSR erstellen

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Administration > Certificate aus**.



Schritt 2: Klicken Sie in der Zertifikatstabelle auf die Schaltfläche **CSR/Zertifikat generieren**.

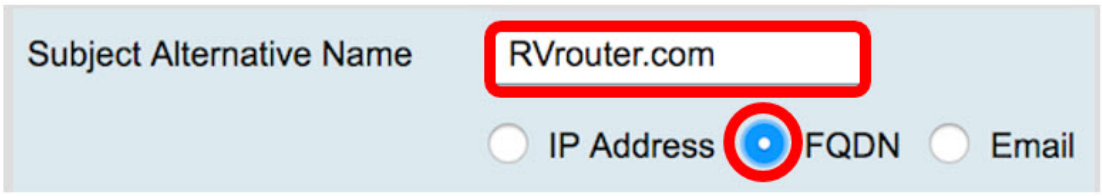


Schritt 3: Klicken Sie im Fenster *CSR/Zertifikat generieren* auf den Dropdown-Pfeil *Typ*, und wählen Sie **Zertifikatsanforderung** aus.

Schritt 4: Geben Sie im Feld *Zertifikatsname* einen Namen für das Zertifikat ein.

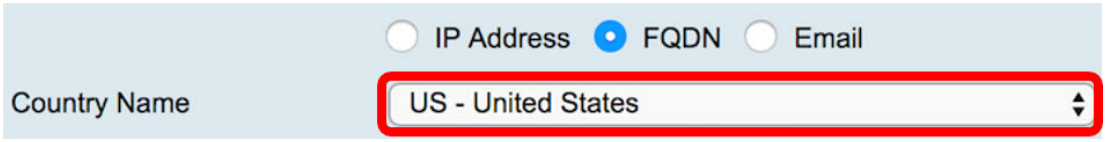
Hinweis: In diesem Beispiel wird der 34xrouter verwendet.

Schritt 5: Geben Sie einen alternativen Namen in das Feld *Subject Alternative Name (Subject Alternative Name*) ein, und klicken Sie dann auf das Optionsfeld **FQDN** darunter, um eine Übereinstimmung zu erhalten. Der alternative Name ist der Domänenname, der für den Zugriff auf den Router verwendet werden kann.



Hinweis: In diesem Beispiel wird RVrouter.com verwendet.

Schritt 6: Klicken Sie auf den Pfeil des Dropdown-Menüs *Ländername*, um das Land Ihres Standorts auszuwählen.

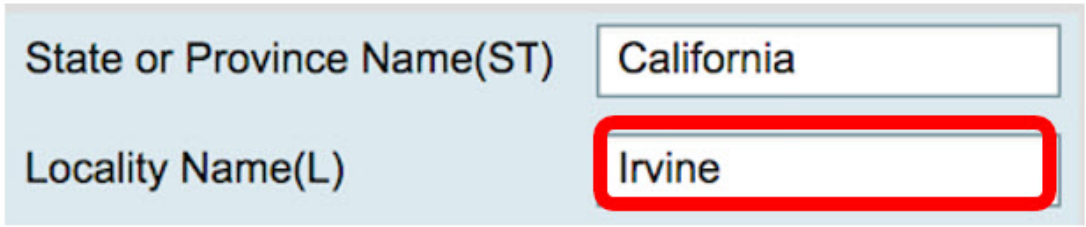


Hinweis: In diesem Beispiel wird US - Vereinigte Staaten ausgewählt.

Schritt 7: Geben Sie im Feld *Bundesland* oder *Bundesland den* Namen *(ST)* ein.

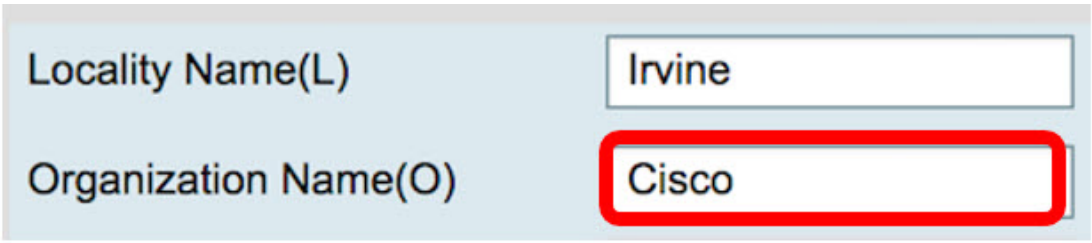
Hinweis: In diesem Beispiel wird Kalifornien verwendet.

Schritt 8: Geben Sie im Feld *Locality Name(L)* den Ort ein.



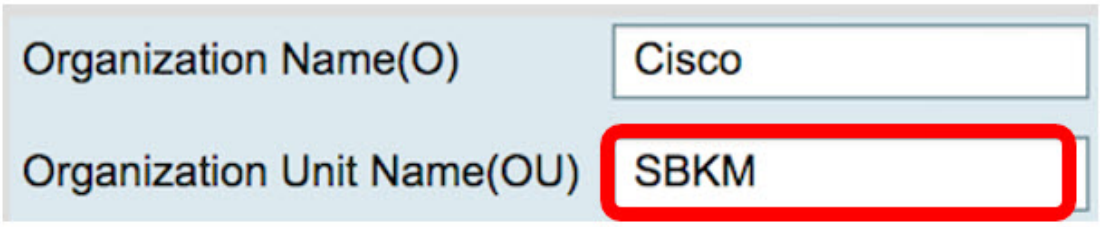
Hinweis: In diesem Beispiel wird Irvine verwendet.

Schritt 9: Geben Sie in das Feld den Organisationsnamen (O) ein.



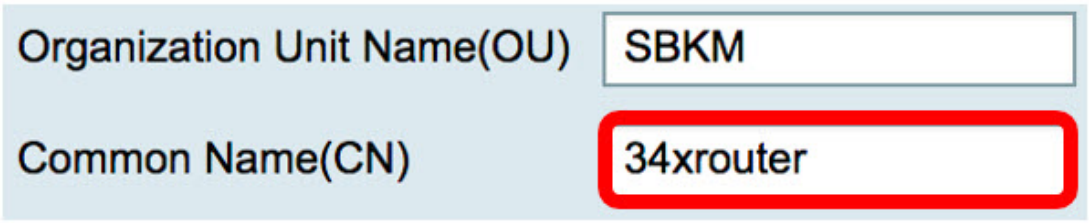
Hinweis: In diesem Beispiel wird Cisco verwendet.

Schritt 10: Geben Sie in das Feld den Namen der Organisationseinheit (OU) ein.



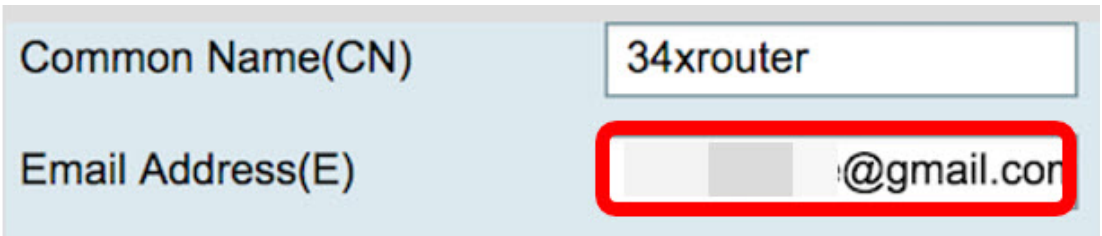
Hinweis: In diesem Beispiel wird SBKM verwendet.

Schritt 11: Geben Sie im Feld *Common Name(CN)* einen Namen ein.



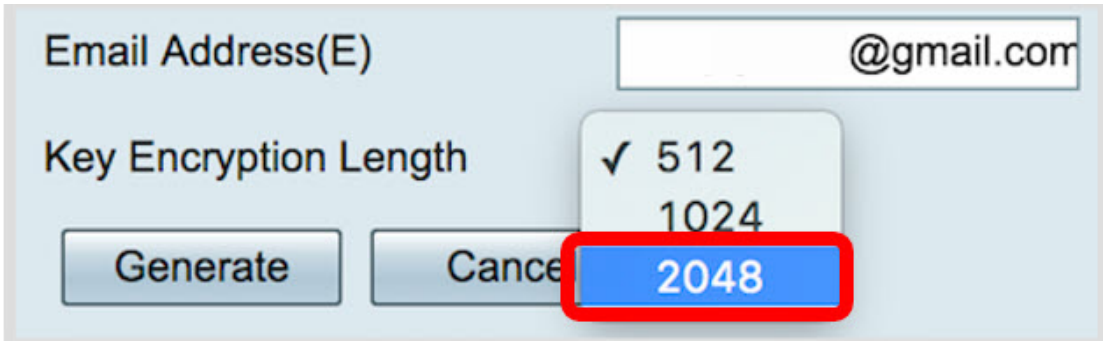
Hinweis: In diesem Beispiel wird der 34xrouter verwendet.

Schritt 12: Geben Sie Ihre E-Mail-Adresse oder eine beliebige E-Mail-Adresse ein, an die das Zertifikat gesendet werden soll.



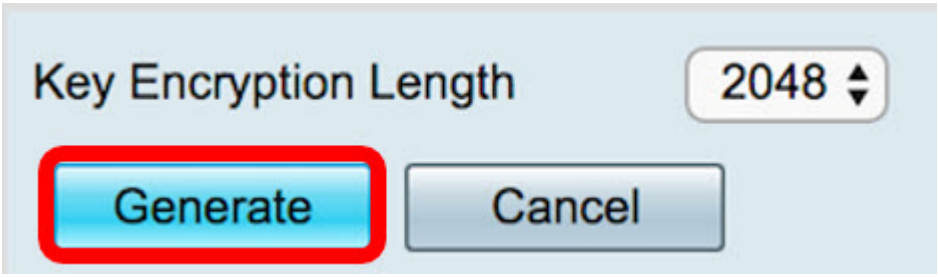
Hinweis: In diesem Beispiel wird eine gmail.com-E-Mail-Adresse verwendet.

Schritt 13: Wählen Sie eine *Schlüssellänge* aus dem Dropdown-Menü aus, um die Anzahl der Bits in Ihrem Schlüssel festzulegen. Die Standardlänge ist 512.



Hinweis: In diesem Beispiel wird 2048 verwendet. Dies wird dringend empfohlen, da eine längere Verschlüsselung schwerer zu entschlüsseln ist als kürzere Schlüssel, sodass sie sicherer.

Schritt 14: Klicken Sie auf **Generieren**.

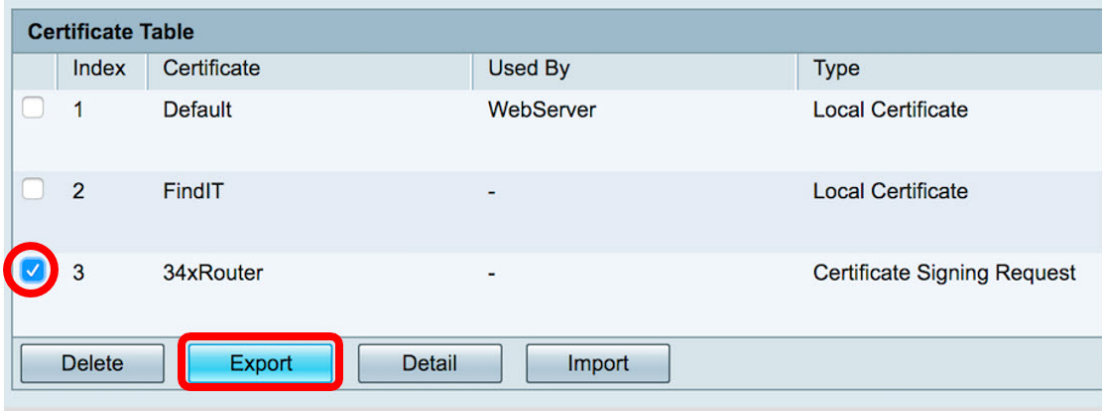


Die von Ihnen erstellte Zertifikatsanforderung wird jetzt in der Zertifikatstabelle angezeigt.

Sie haben jetzt erfolgreich eine CSR-Anfrage erstellt.

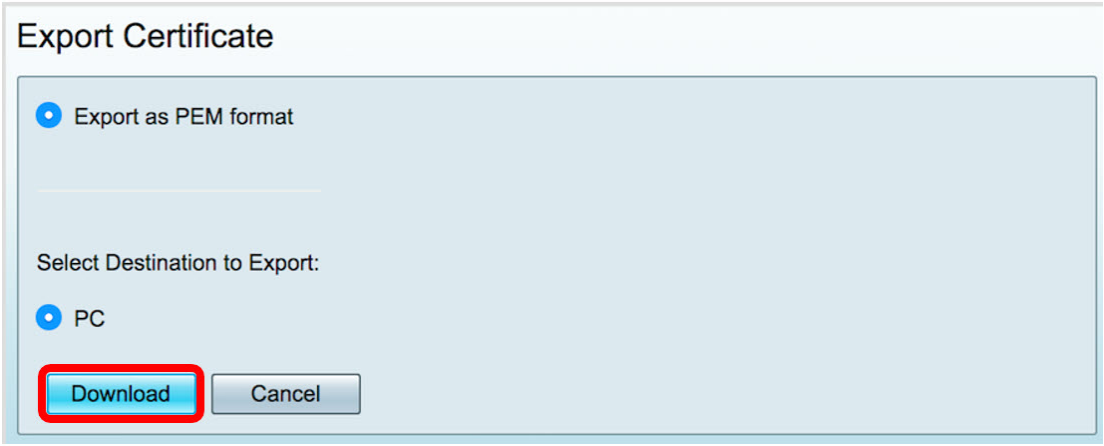
CSR exportieren

Schritt 1: Aktivieren Sie in der Zertifikatstabelle das Kontrollkästchen neben der Zertifikatsanforderung, und klicken Sie auf **Exportieren**.



Schritt 2: Klicken Sie im Fenster *Exportzertifikat auf* **Herunterladen**, um die Datei im PEM-

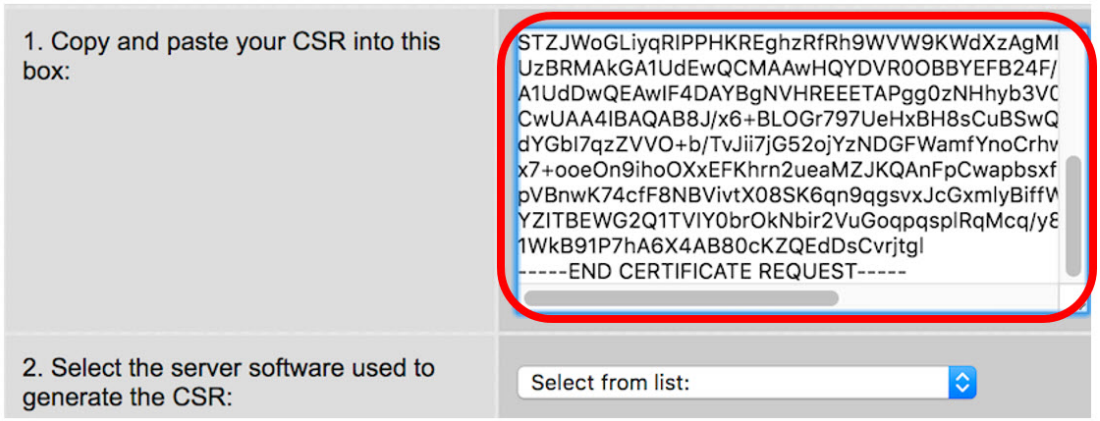
Format auf Ihren Computer herunterzuladen.



Sie haben die CSR-Datei jetzt erfolgreich in Ihren Computer exportiert.

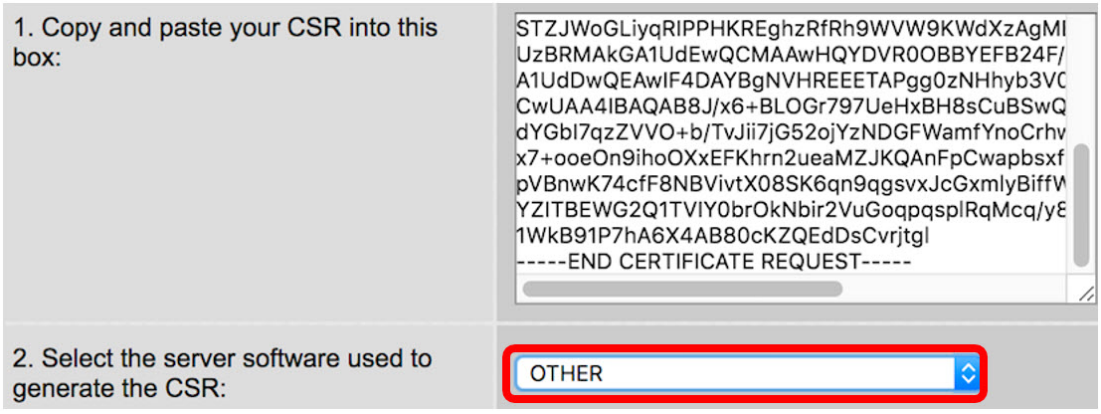
Laden Sie den CSR in den Zertifikatanbieter hoch.

Schritt 1: Öffnen Sie die heruntergeladene Datei mit einem Notizblock, kopieren Sie die CSR-Datei, und fügen Sie sie in das Feld ein, das auf der Website des SSL-Zertifikatsanbieters eines Drittanbieters bereitgestellt wird.



Hinweis: In diesem Beispiel wird Comodo.com als Zertifikatanbieter verwendet.

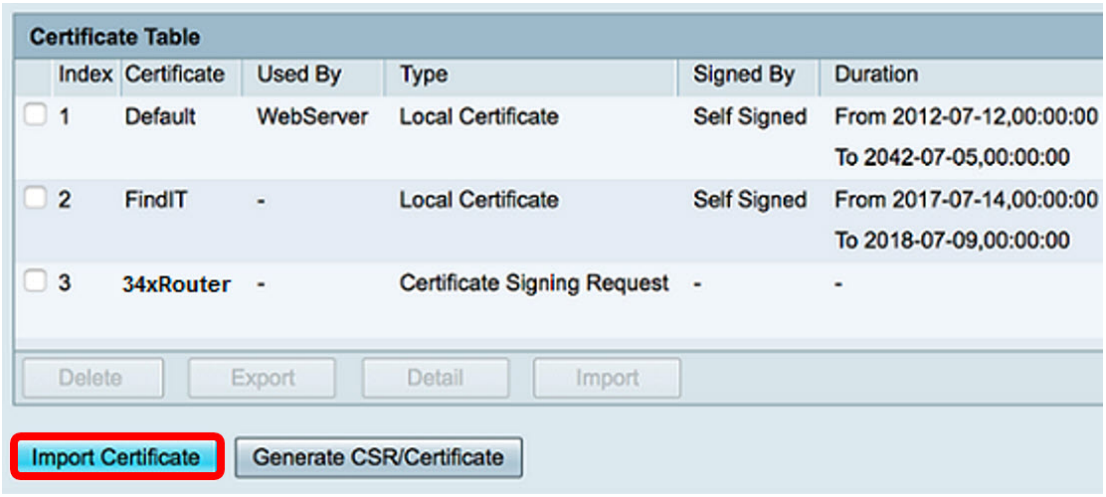
Schritt 2: Wählen Sie die Serversoftware aus, die zum Generieren des CSR verwendet wird. Da der RV34x-Router nicht in der Liste enthalten ist, wird in diesem Fall "ANDERE" ausgewählt.



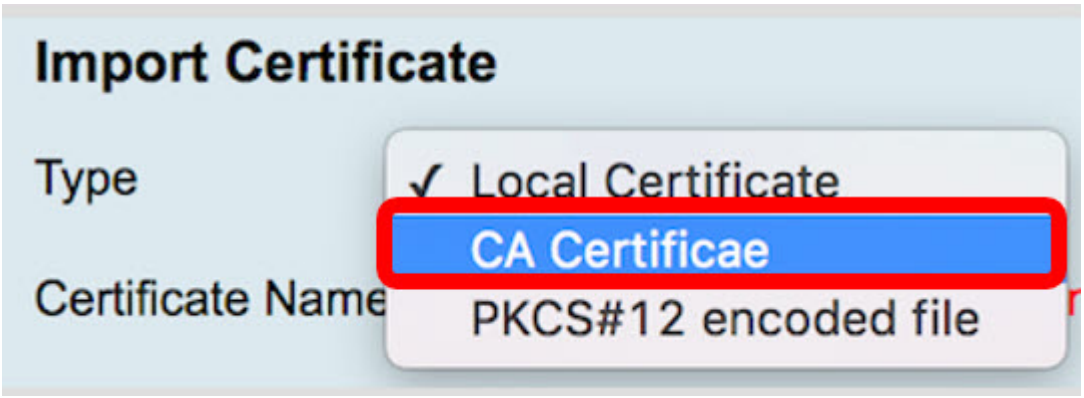
Schritt 3: Laden Sie Ihr Zertifikat auf Ihren Computer herunter.

Hochladen des Zertifikats von Drittanbietern

Schritt 1: Klicken Sie im webbasierten Dienstprogramm des Routers unter der Zertifikatstabelle auf die Schaltfläche **Zertifikat importieren**.



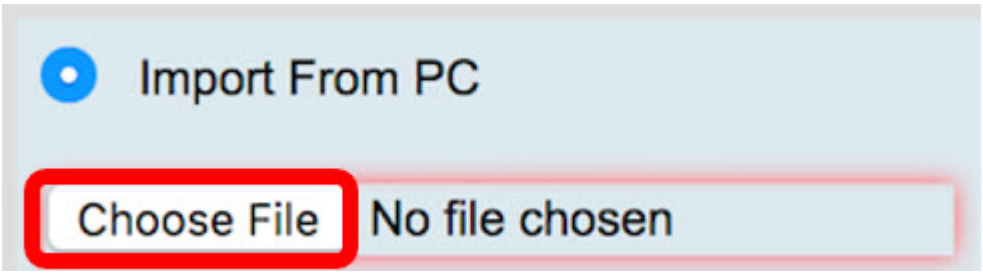
Schritt 2: Klicken Sie im Fenster *Zertifikat importieren* auf das Dropdown-Menü *Typ*, und wählen Sie **Zertifizierungsstellenzertifikat aus**.



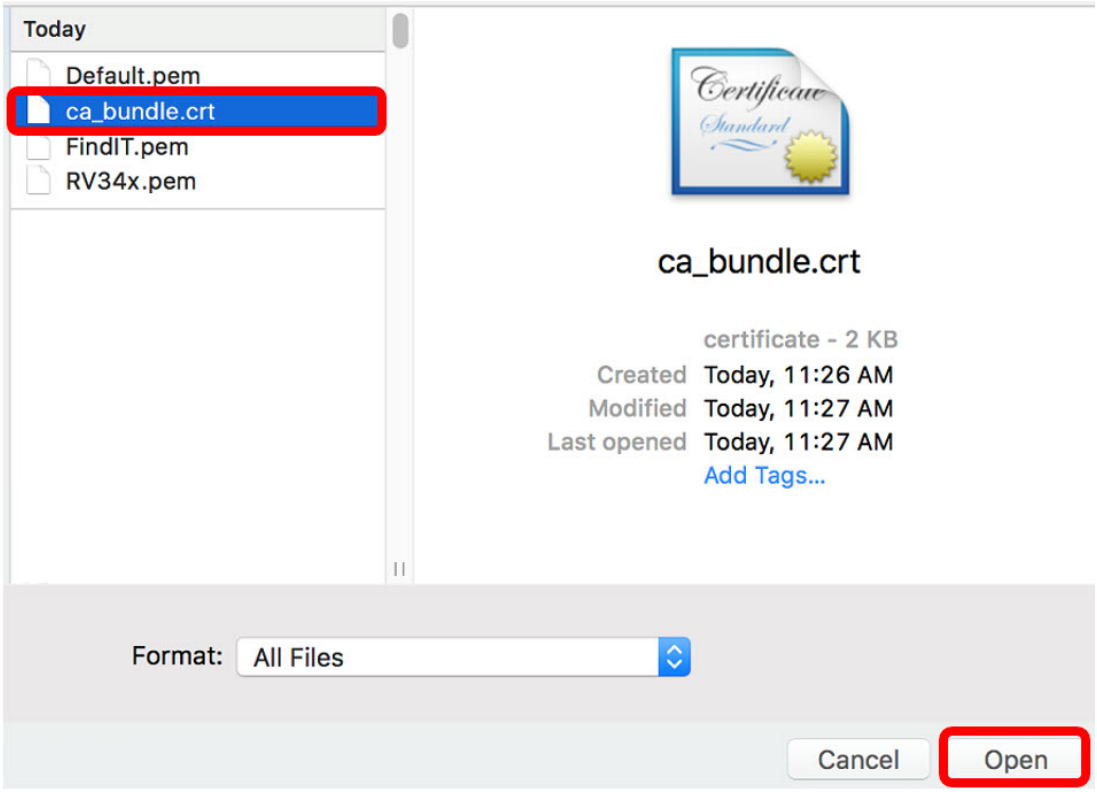
Schritt 3: Geben Sie in das Feld einen Zertifikatsnamen ein.

Hinweis: In diesem Beispiel wird RV34xCert verwendet.

Schritt 4: Klicken Sie auf die Schaltfläche **Choose File (Datei auswählen)**, und suchen Sie die Zertifikatsdatei, die Sie von der CA heruntergeladen haben.

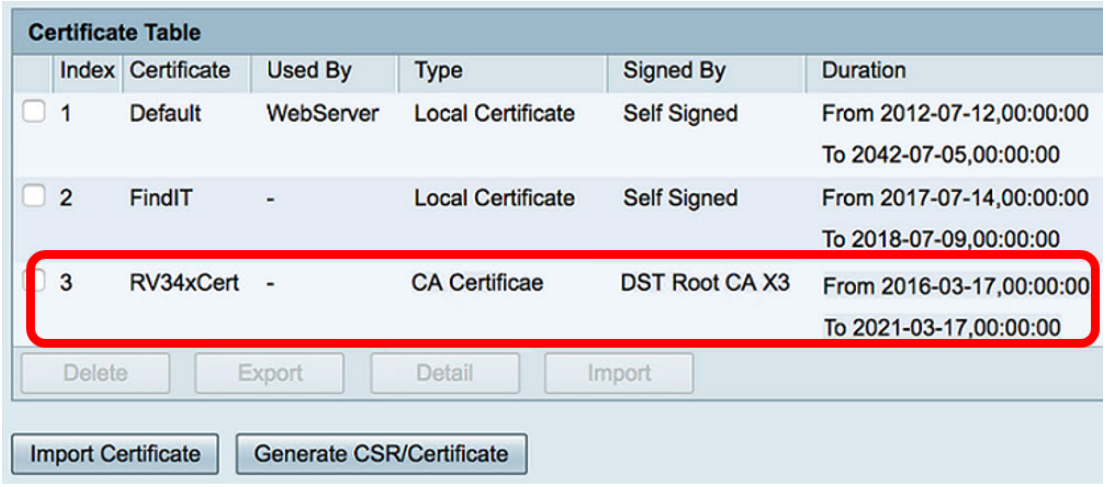


Schritt 5: Klicken Sie auf die Datei und anschließend auf **Öffnen**.



Schritt 6: Klicken Sie auf **Hochladen**.

In der Zertifikatstabelle wird nun der neue Zertifikatsname angezeigt, und der Typ wird nun durch das Zertifizierungsstellenzertifikat ersetzt, das durch das von der Zertifizierungsstelle eines Drittanbieters signierte Label ersetzt wurde.

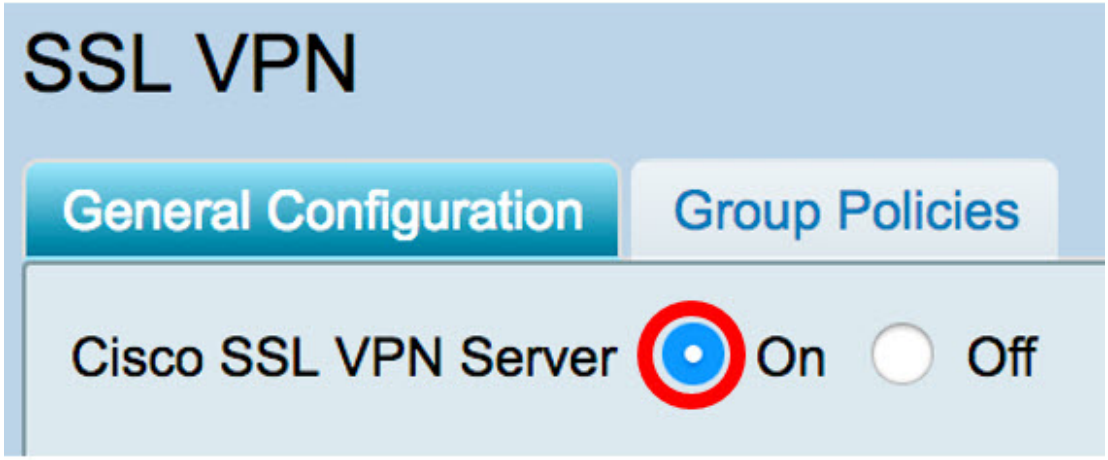


Sie haben nun erfolgreich ein SSL-Zertifikat eines Drittanbieters auf den RV34x-Router hochgeladen.

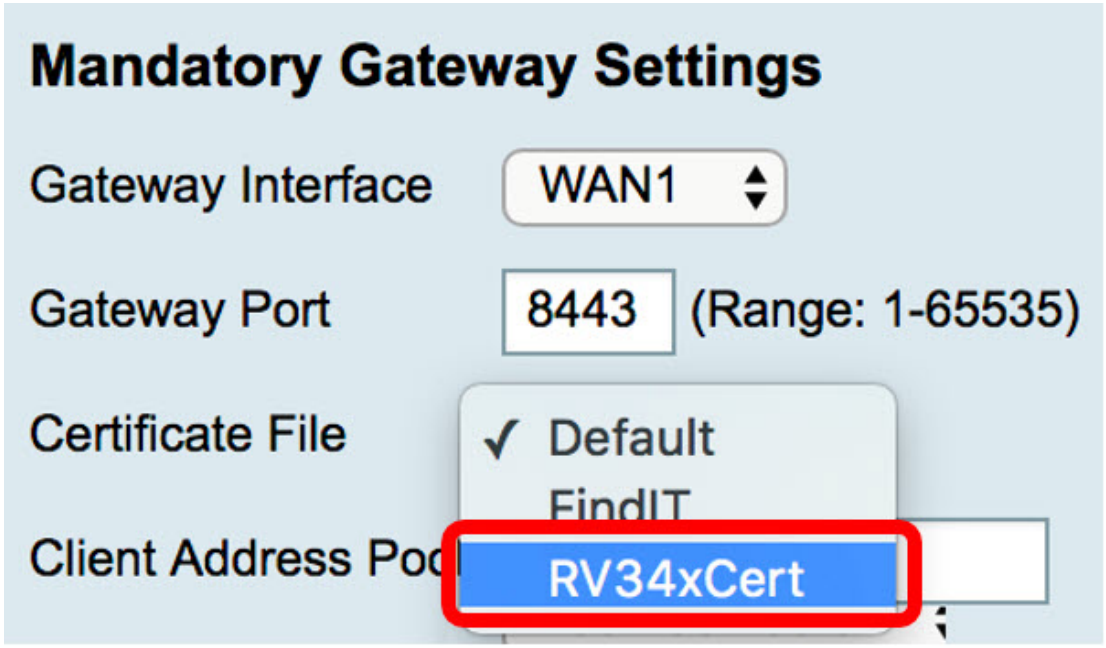
Ersetzen Sie das selbst signierte Standardzertifikat.

Schritt 1: Wählen Sie im webbasierten Dienstprogramm **VPN > SSL VPN aus**.

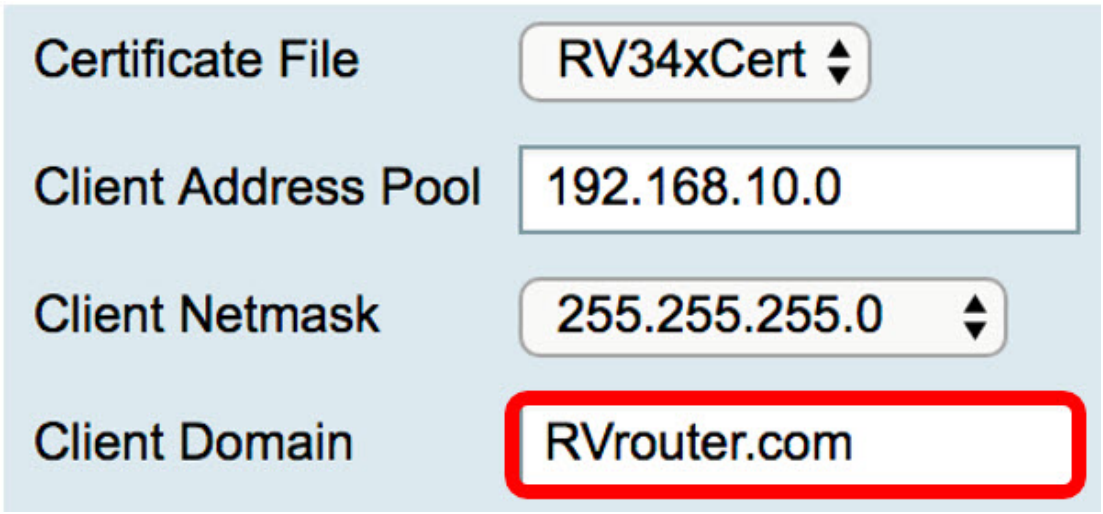
Schritt 2: Klicken Sie auf das Optionsfeld **Ein**, um den Cisco SSL VPN Server zu aktivieren.



Schritt 3: Klicken Sie unter Obligatorische Gateway-Einstellungen auf das Dropdown-Menü *Zertifikatsdatei*, und ersetzen Sie das Standardzertifikat, indem Sie das neu hochgeladene SSL-Zertifikat auswählen.

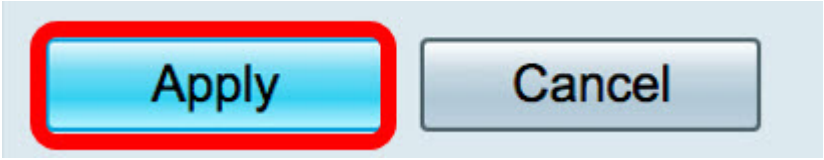


Schritt 4: Geben Sie die erforderliche Client-Domäne in das entsprechende Feld ein.



Hinweis: In diesem Beispiel wird RVrouter.com verwendet.

Schritt 5: Klicken Sie auf **Übernehmen**.



Sie haben jetzt das selbstsignierte Standardzertifikat erfolgreich durch das SSL-Zertifikat eines Drittanbieters ersetzt.

Dieser Artikel enthält außerdem hilfreiche Informationen: Häufig gestellte Fragen (FAQs) zu Routern der Serie RV34x

Diese Seite bietet mehrere Links zu anderen Artikeln, die Sie vielleicht interessant finden: Produktseite für Router der Serie RV34x