Verwalten von Zertifikaten auf dem Router der Serie RV34x

Ziel

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.

Lassen Sie uns über den Erhalt eines Zertifikats einer Zertifizierungsstelle (Certificate Authority, CA) sprechen. Eine CA wird für die Authentifizierung verwendet. Zertifikate werden von einer beliebigen Anzahl von Websites Dritter erworben. Es ist eine offizielle Methode, zu beweisen, dass Ihre Website sicher ist. Im Wesentlichen ist die CA eine vertrauenswürdige Quelle, die sicherstellt, dass Sie ein legitimes Unternehmen sind und vertrauenswürdig sind. Je nach Ihren Bedürfnissen, ein Zertifikat zu minimalen Kosten. Sie werden von der Zertifizierungsstelle ausgecheckt, und sobald diese Ihre Informationen überprüft hat, wird Ihnen das Zertifikat ausgestellt. Dieses Zertifikat kann als Datei auf Ihren Computer heruntergeladen werden. Sie können dann zu Ihrem Router (oder VPN-Server) gehen und ihn dort hochladen.

In diesem Artikel erfahren Sie, wie Sie Zertifikate und Zertifikate auf dem Router der Serie RV34x generieren, exportieren und importieren.

Unterstützte Geräte | Softwareversion

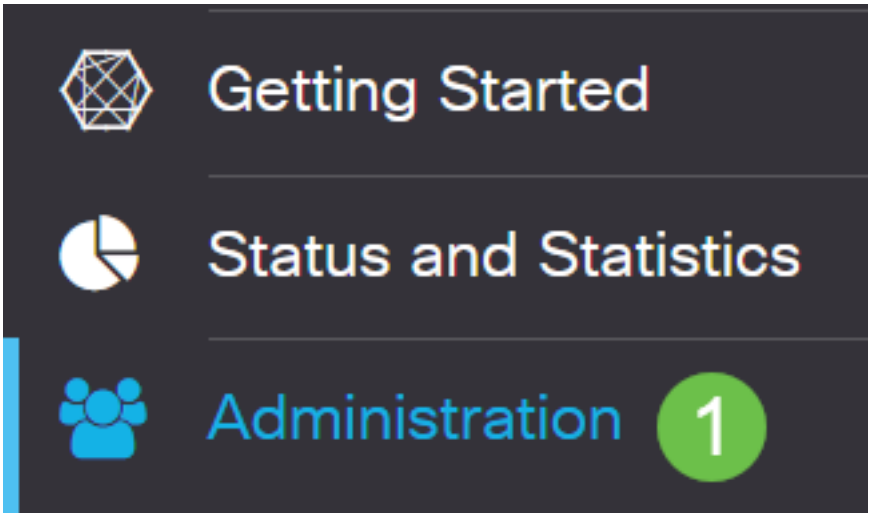
- Serie RV34x | 1.0.03.20

Verwalten von Zertifikaten auf dem Router

CSR/Zertifikat erstellen

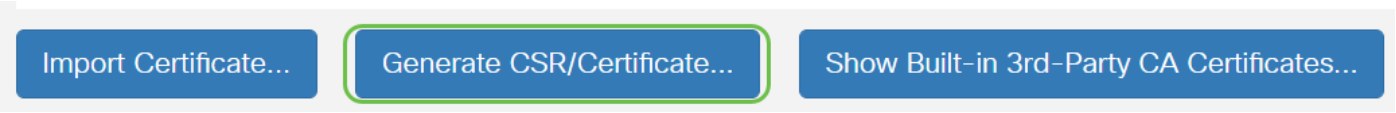
Schritt 1

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



Schritt 2

Klicken Sie auf **CSR/Zertifikat generieren**. Sie werden zur Seite "CSR/Zertifikat generieren" weitergeleitet.



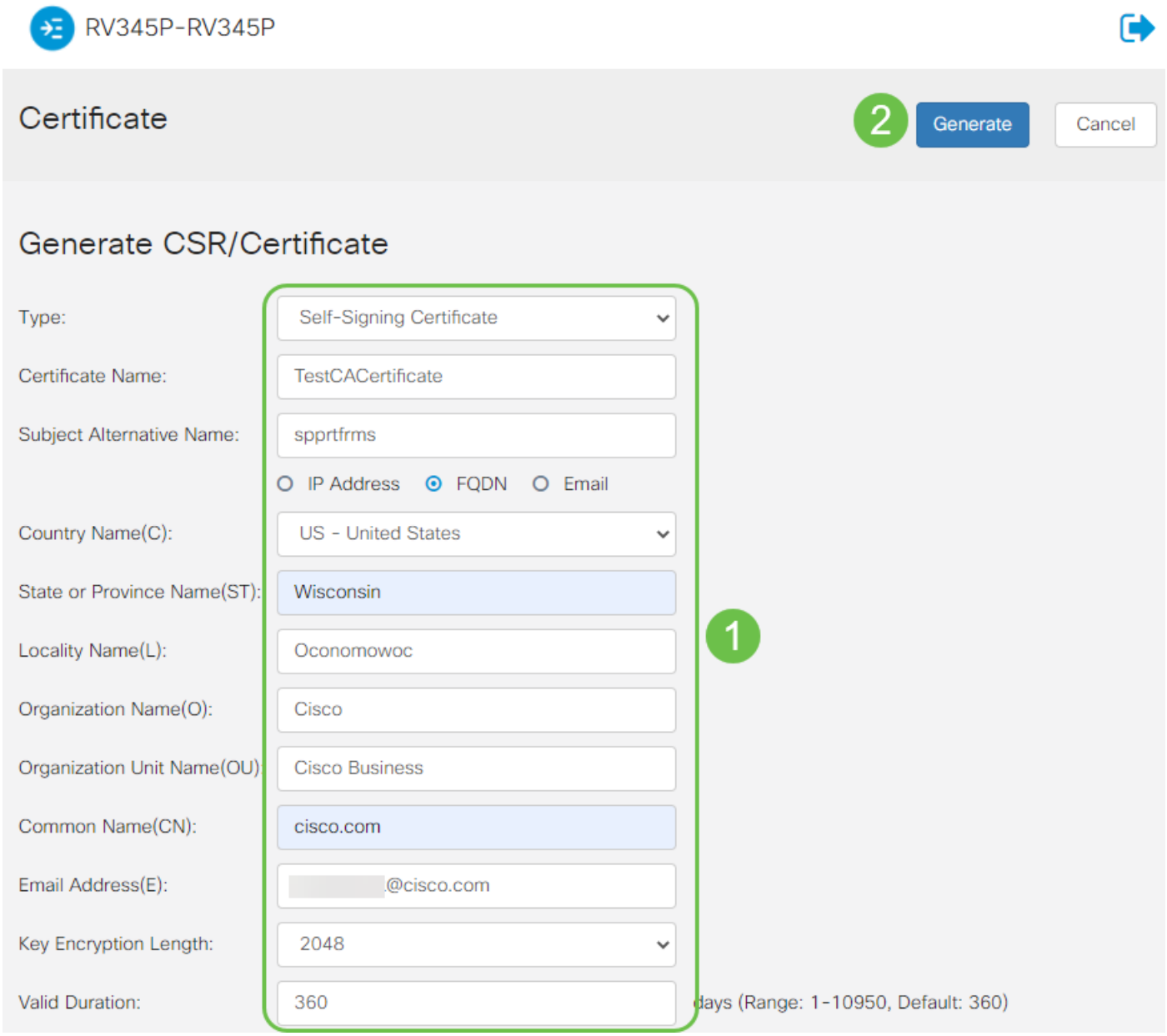
Schritt 3

Füllen Sie die Felder mit folgenden Angaben aus:

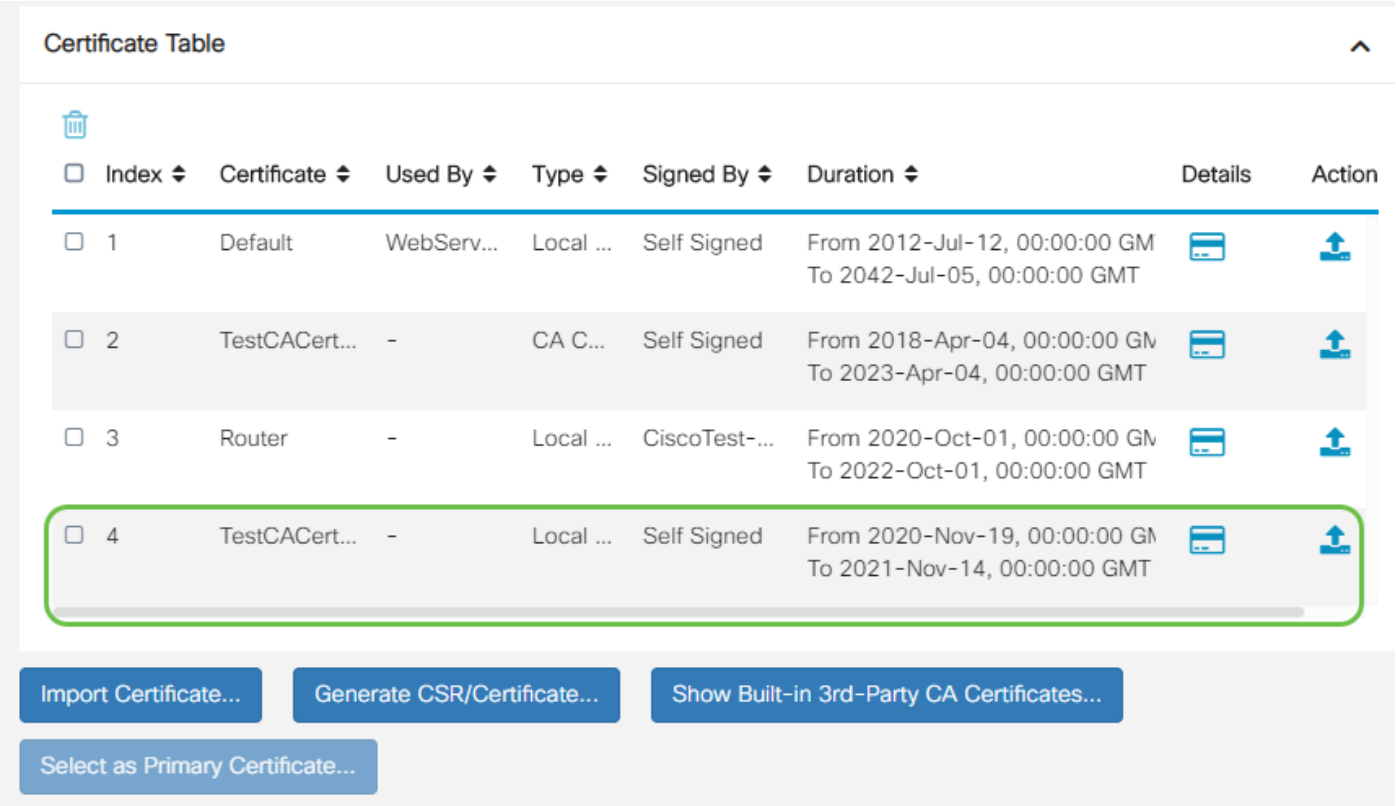
- Wählen Sie den entsprechenden Zertifikatstyp aus.
  - Self-Signing Certificate - Dies ist ein SSL-Zertifikat (Secure Socket Layer), das vom eigenen Ersteller signiert wird. Dieses Zertifikat ist weniger vertrauenswürdig, da es nicht abgebrochen werden kann, wenn der private Schlüssel durch einen Angreifer 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.
- Geben Sie im Feld *Zertifikatsname* einen Namen für das Zertifikat ein, um die Anforderung zu identifizieren. Dieses Feld darf nicht leer sein und keine Leerzeichen und Sonderzeichen enthalten.
- (Optional) Klicken Sie im Bereich "Betreff-Alternative Name" auf ein Optionsfeld. Folgende Optionen sind verfügbar:
  - IP-Adresse - Geben Sie eine IP-Adresse (Internet Protocol) ein.
  - FQDN - Geben Sie einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) ein.
  - E-Mail - E-Mail-Adresse eingeben
- Geben Sie im Feld *Subject Alternative Name (Betreffalternative Name*) den FQDN ein.
- Wählen Sie in der Dropdown-Liste Ländername einen Ländernamen aus, in dem Ihre Organisation legal registriert ist.
- 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 (ST)* befindet.
- Geben Sie im Feld *Locality Name* (*Lokalisierungsname)* den Namen der Stadt ein, in der Ihre Organisation registriert ist oder sich befindet.
- Geben Sie einen Namen ein, unter dem Ihr Unternehmen rechtlich registriert ist. Wenn Sie sich als kleines Unternehmen oder alleiniger Eigentümer anmelden, geben Sie den Namen des Zertifikatsanforderers in das Feld *Organisationsname ein*. Sonderzeichen können nicht verwendet werden.
- Geben Sie im Feld *Name* der *Organisationseinheit* einen Namen ein, um zwischen den Abteilungen innerhalb einer Organisation zu unterscheiden.
- Geben Sie einen Namen in das Feld *Allgemeiner Name ein*. Dieser Name muss der vollqualifizierte Domänenname der Website sein, für die Sie das Zertifikat verwenden.
- Geben Sie die E-Mail-Adresse der Person ein, die das Zertifikat generieren möchte.
- Wählen Sie aus der Dropdown-Liste Key Encryption Length (Schlüssellänge) eine Schlüssellänge aus. Die Optionen sind 512, 1024 und 2048. Je größer die Schlüssellänge, desto sicherer ist das Zertifikat.
- Geben Sie im Feld *Gültige Dauer* die Anzahl der Tage ein, für die das Zertifikat gültig ist. Der

Standardwert ist 360.

- Klicken Sie auf **Generieren**.



Hinweis: Das generierte Zertifikat sollte nun in der Zertifikatstabelle angezeigt werden.

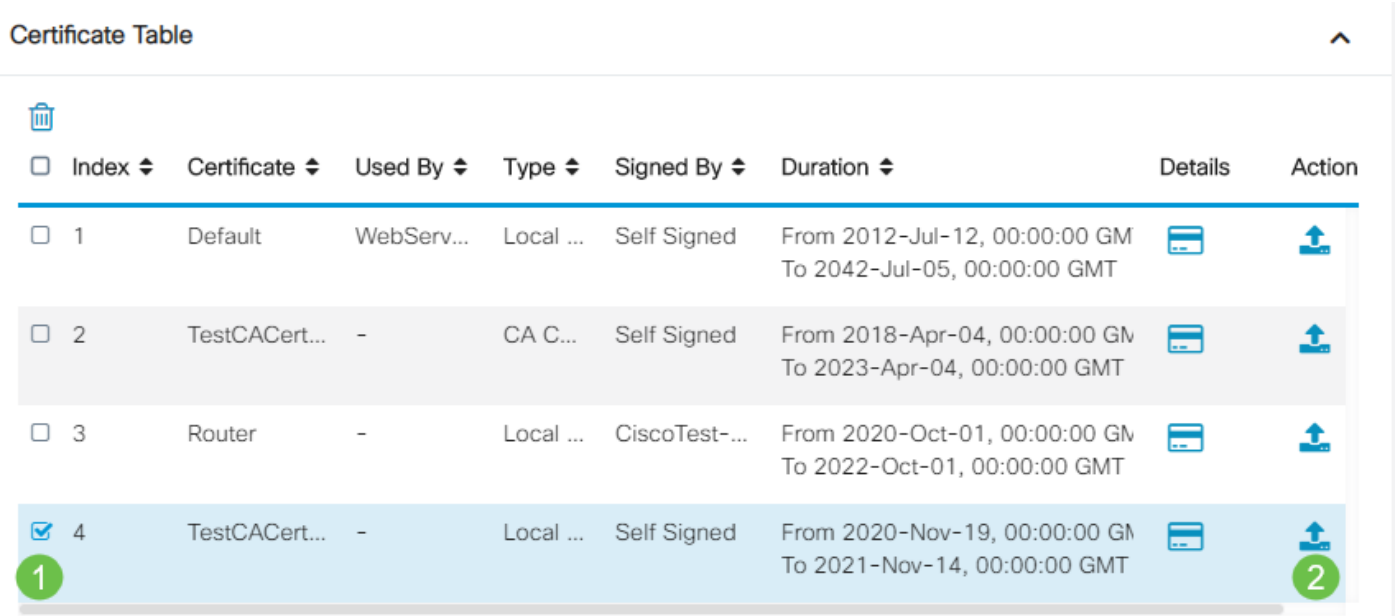


Sie sollten jetzt erfolgreich ein Zertifikat auf dem RV345P-Router erstellt haben.

Zertifikat exportieren

Schritt 1

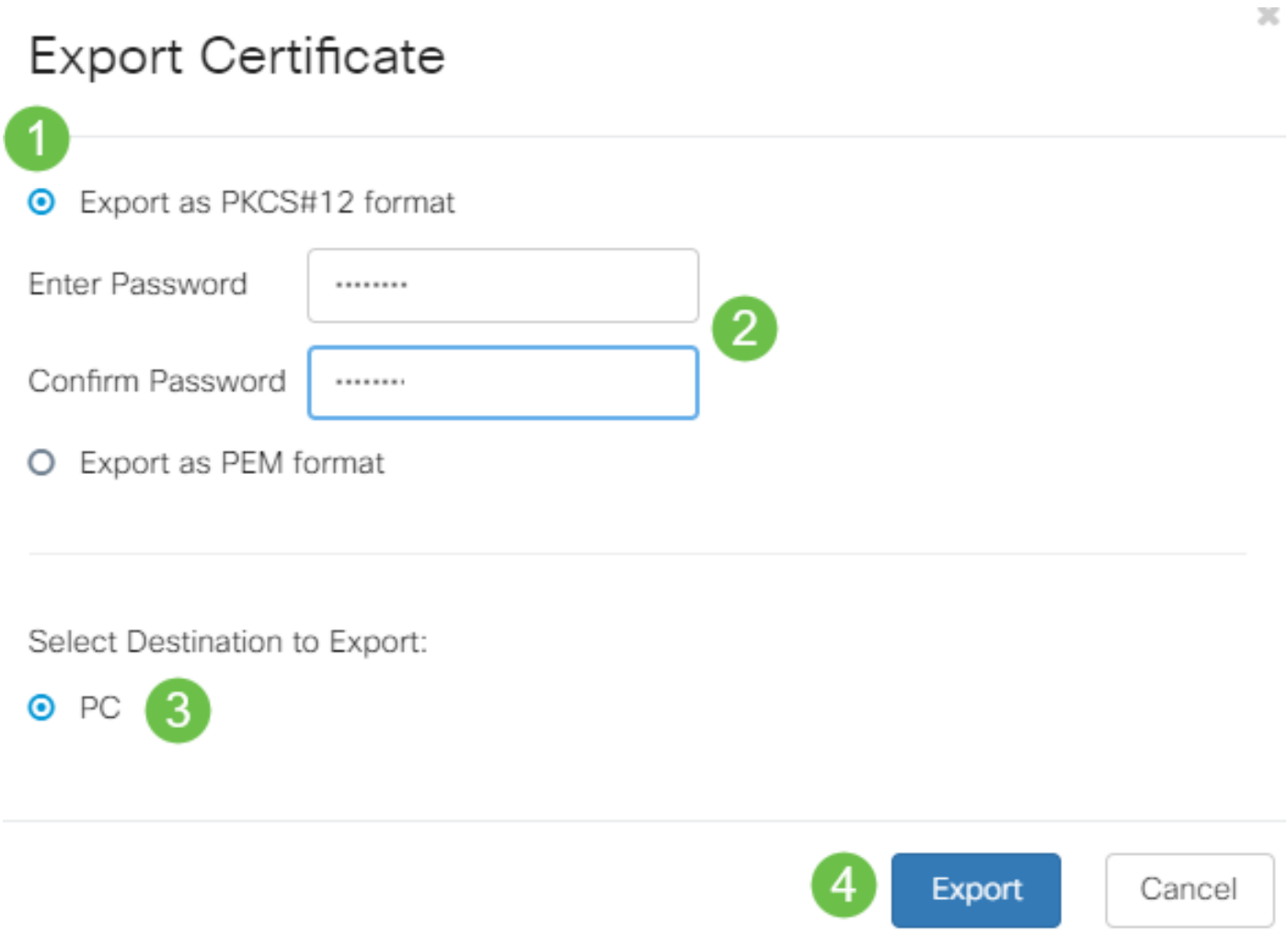
Aktivieren Sie in der Zertifikatstabelle das Kontrollkästchen des zu exportierenden Zertifikats, und klicken Sie auf das **Exportsymbol**.



Schritt 2

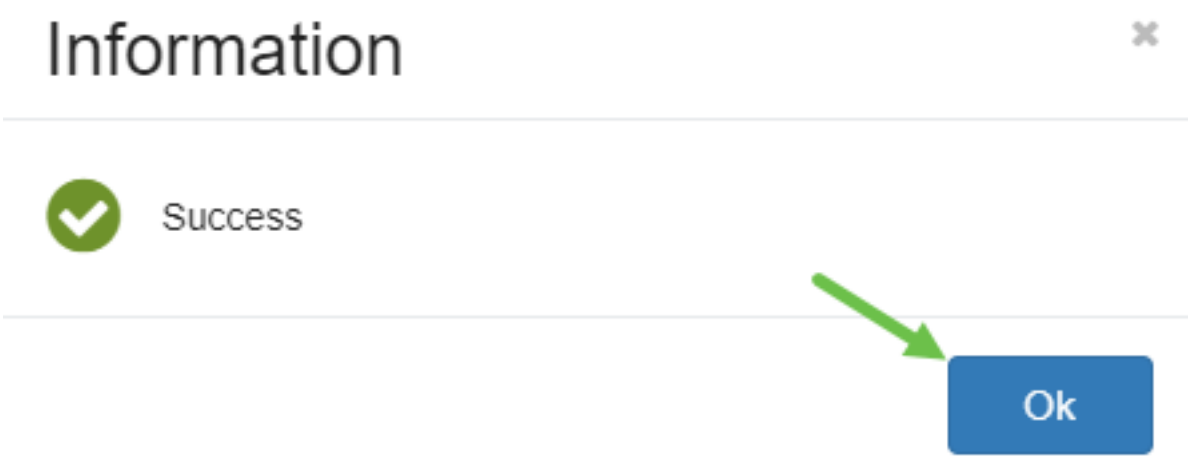
- Klicken Sie auf ein Format, um das Zertifikat zu exportieren. Folgende Optionen sind verfügbar:
  - PKCS #12 - Public Key Cryptography Standards (PKCS) #12 ist ein exportiertes Zertifikat, das in der Erweiterung .p12 enthalten ist. Um die Datei zu verschlüsseln, ist ein Kennwort

erforderlich, um sie beim Exportieren, Importieren und Löschen zu schützen.
    - PEM — Privacy Enhanced Mail (PEM) wird häufig für Webserver verwendet, um mithilfe eines einfachen Texteditors wie Notepad leicht in lesbare Daten übersetzt werden zu können.
- Wenn Sie PEM ausgewählt haben, klicken Sie einfach auf **Exportieren**.
- Geben Sie ein Kennwort ein, um die zu exportierende Datei im Feld *Kennwort eingeben* zu sichern.
- Geben Sie das Kennwort erneut im Feld *Kennwort bestätigen* ein.
- Im Bereich "Select Destination" (Ziel auswählen) wurde PC ausgewählt und ist die einzige derzeit verfügbare Option.
- Klicken Sie auf **Exportieren**.



Schritt 3

Unter der Schaltfläche Download wird eine Meldung angezeigt, die den Erfolg des Downloads anzeigt. Eine Datei wird in Ihrem Browser heruntergeladen. Klicken Sie auf **OK**.

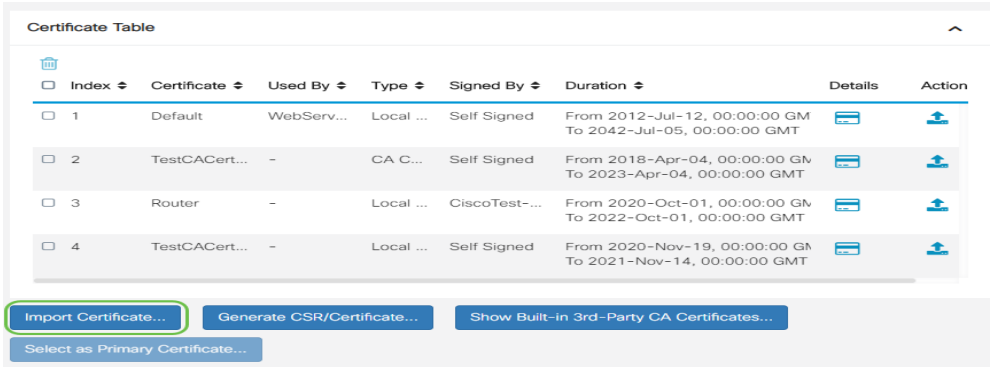


Sie sollten jetzt ein Zertifikat erfolgreich auf dem Router der Rv34x-Serie exportiert haben.

Importieren eines Zertifikats

Schritt 1

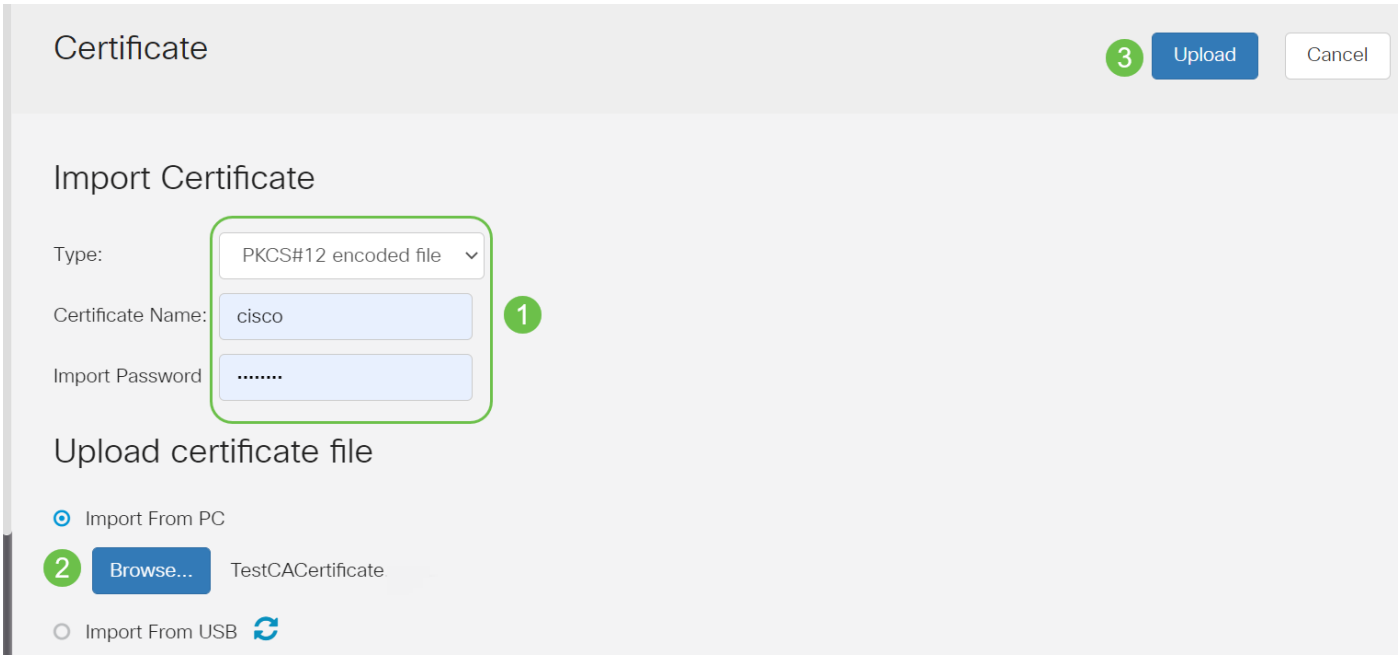
Klicken Sie auf **Zertifikat importieren...**.



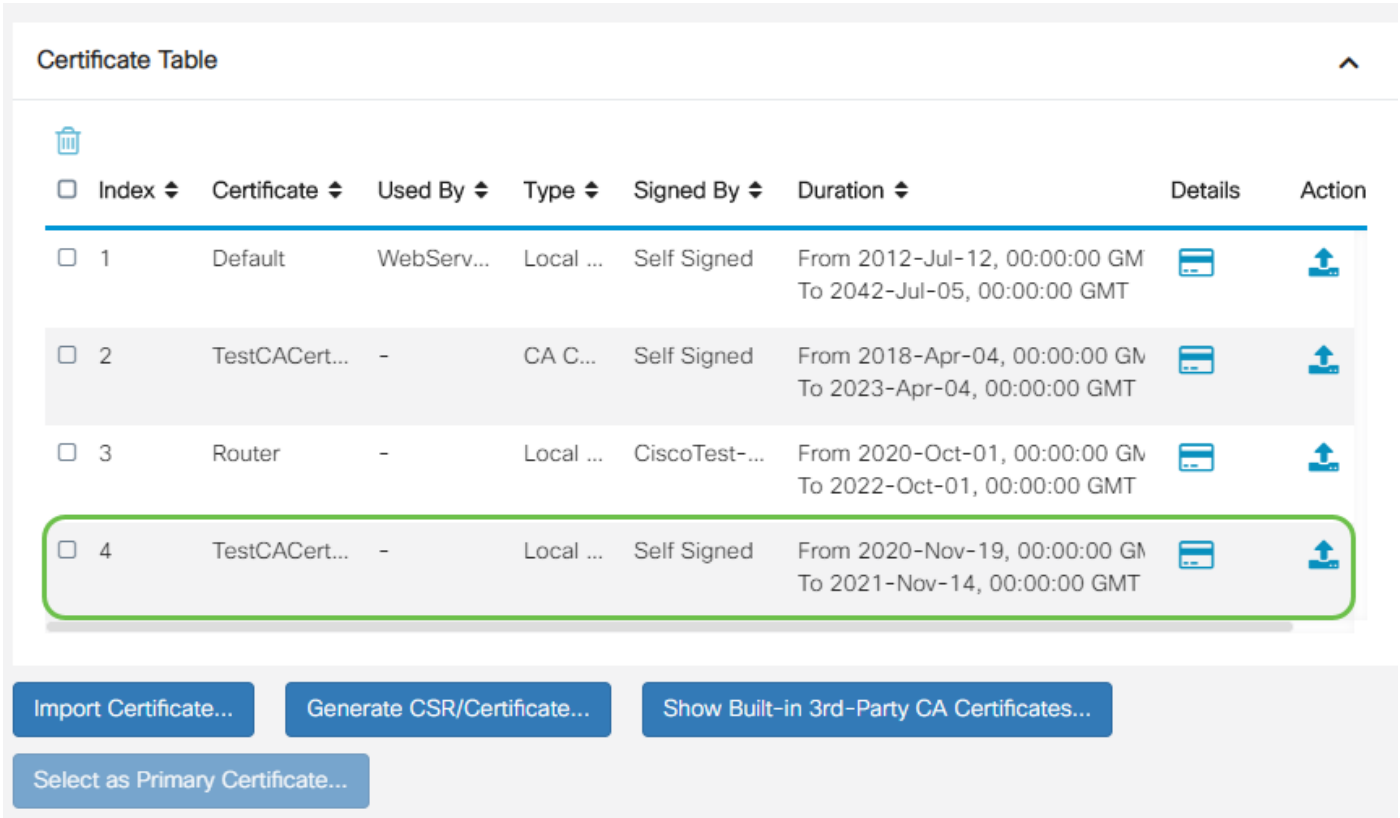
Schritt 2

- Wählen Sie aus der Dropdown-Liste den zu importierenden Zertifikattyp aus. Folgende Optionen sind verfügbar:
  - Local Certificate (Lokales Zertifikat): Ein auf dem Router generiertes Zertifikat.
  - Zertifizierungsstellenzertifikat - Ein Zertifikat, das von einer vertrauenswürdigen Drittbehörde zertifiziert wurde und bestätigt hat, dass die im Zertifikat enthaltenen Informationen korrekt sind.
  - PKCS #12 Encoded file — Public Key Cryptography Standards (PKCS) #12 ist ein Format zum Speichern eines Serverzertifikats.
- Geben Sie im Feld *Zertifikatsname* einen Namen für das Zertifikat ein.
- Wenn PKCS #12 ausgewählt wurde, geben Sie im Feld *Importpasswort* ein Kennwort für die Datei ein. Fahren Sie andernfalls mit Schritt 3 fort.
- Klicken Sie auf eine Quelle, um das Zertifikat zu importieren. Folgende Optionen sind verfügbar:
  - Importieren aus PC
  - Importieren über USB
- Wenn der Router kein USB-Laufwerk erkennt, wird die Option Import from USB (Von USB importieren) deaktiviert.
- Wenn Sie Import From USB (Aus USB importieren) ausgewählt haben und Ihr USB vom Router nicht erkannt wird, klicken Sie auf Refresh (Aktualisieren).

- Klicken Sie auf die Schaltfläche Choose File (Datei auswählen), und wählen Sie die entsprechende Datei aus.
- Klicken Sie auf **Hochladen**.



Nach dem erfolgreichen Abschluss werden Sie automatisch zur Hauptseite für Zertifikate weitergeleitet. Die Zertifikatstabelle wird mit dem kürzlich importierten Zertifikat gefüllt.



Sie sollten jetzt erfolgreich ein Zertifikat auf Ihren Router der Serie RV34x importiert haben.