Sostituire il certificato autofirmato predefinito con un certificato SSL di terze parti sul router serie RV34x

Introduzione

Un certificato digitale certifica la proprietà di una chiave pubblica da parte del soggetto specificato del certificato. In questo modo le relying party possono dipendere da firme o asserzioni effettuate dalla chiave privata corrispondente alla chiave pubblica certificata. Un router può generare un certificato autofirmato, ovvero un certificato creato da un amministratore di rete. Può inoltre inviare richieste alle Autorità di certificazione (CA) per richiedere un certificato di identità digitale. È importante disporre di certificati legittimi di applicazioni di terze parti.

I certificati possono essere firmati da CA in due modi:

1. La CA firma il certificato con chiavi private.

2. CA firma i certificati utilizzando la richiesta di firma del certificato (CSR) generata dalla RV34x.

La maggior parte dei fornitori di certificati commerciali utilizza certificati intermedi. Poiché il certificato intermedio viene rilasciato dalla CA radice attendibile, qualsiasi certificato emesso dal certificato intermedio eredita l'attendibilità della radice attendibile, come una catena di certificati di attendibilità.

Obiettivo

In questo articolo viene spiegato come richiedere e caricare un certificato SSL (Secure Sockets Layer) di terze parti rilasciato da una CA per sostituire il certificato autofirmato sul router RV34x.

Dispositivi interessati

- RV340
- RV340W
- RV345
- RV345P

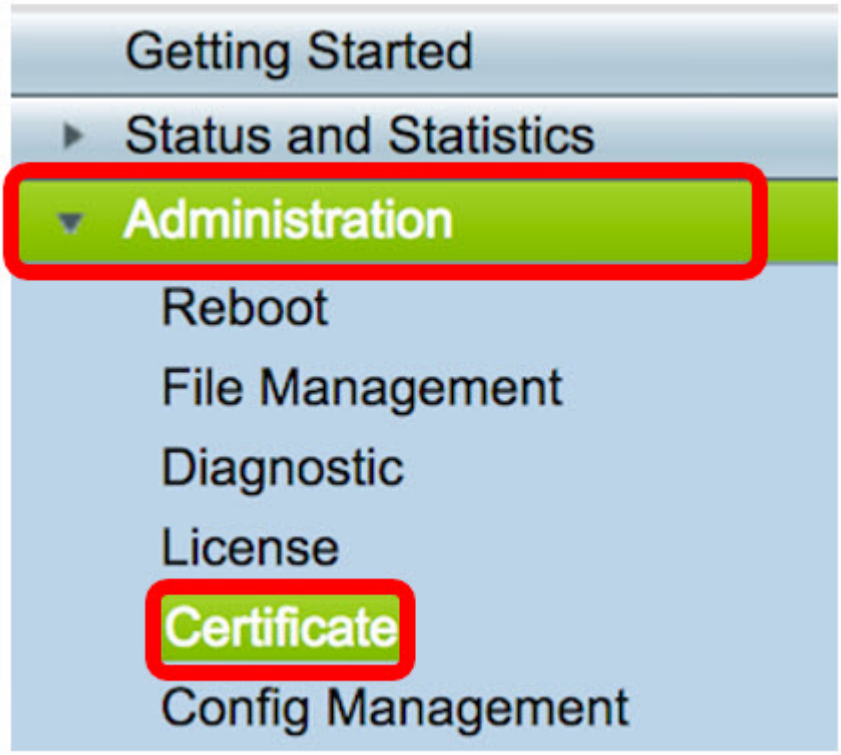
Versione del software

- 1.0.01.17

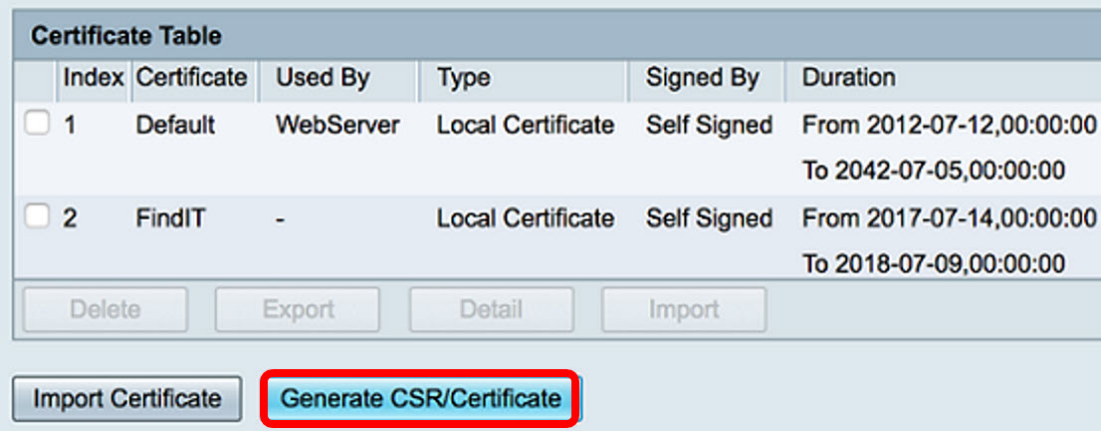
Sostituire il certificato autofirmato predefinito con un certificato SSL di terze parti

Genera un CSR

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Amministrazione > Certificato**.



Passaggio 2. Nella tabella Certificati, fare clic sul pulsante **Genera CSR/Certificato**.

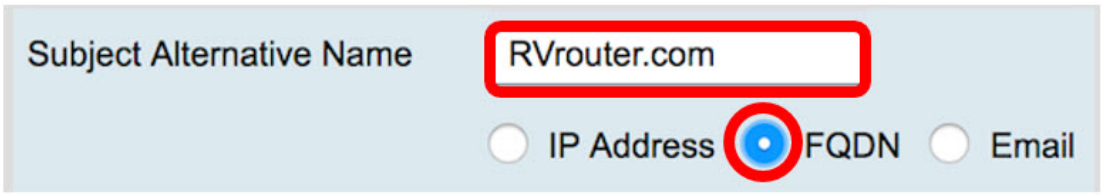


Passaggio 3. Nella finestra *Genera CSR/certificato*, fare clic sulla freccia a discesa *Tipo* e scegliere **Richiesta firma certificato**.

Passaggio 4. Immettere un nome per il certificato nel campo *Nome certificato*.

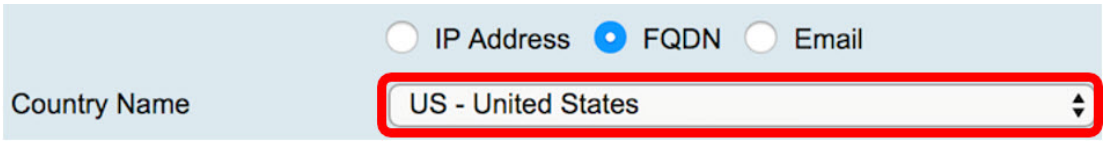
Nota: nell'esempio, viene usato un router 34x.

Passaggio 5. Immettere un nome alternativo nel campo *Nome alternativo soggetto*, quindi fare clic sul pulsante di opzione **FQDN** sottostante per trovare una corrispondenza. Il nome alternativo sarà il nome di dominio utilizzabile per accedere al router.



Nota: Nell'esempio viene utilizzato RVrouter.com.

Passaggio 6. Fare clic sulla freccia a discesa *Country Name* (Nome paese) per scegliere il paese in cui ci si trova.

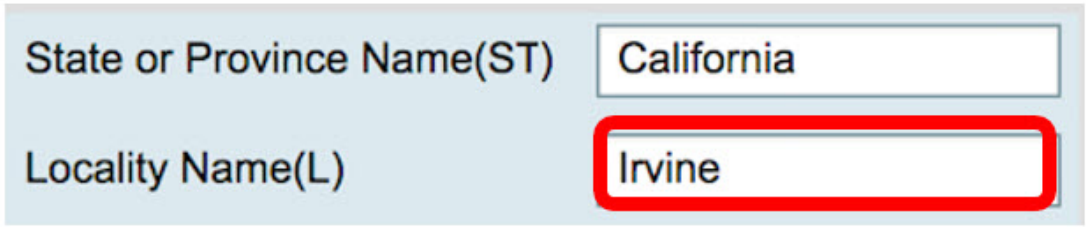


Nota: In questo esempio si scelgono gli Stati Uniti - USA.

Passaggio 7. Immettere il nome dello stato o della provincia nel campo *Stato o Nome provincia(ST)*.

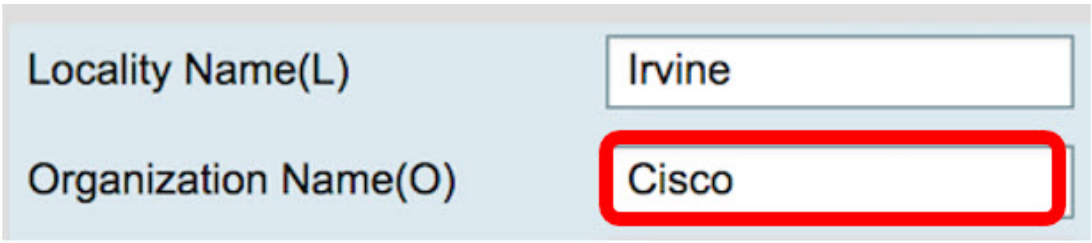
Nota: Nell'esempio viene utilizzata la California.

Passaggio 8. Inserire la località nel campo *Nome località (L)*.



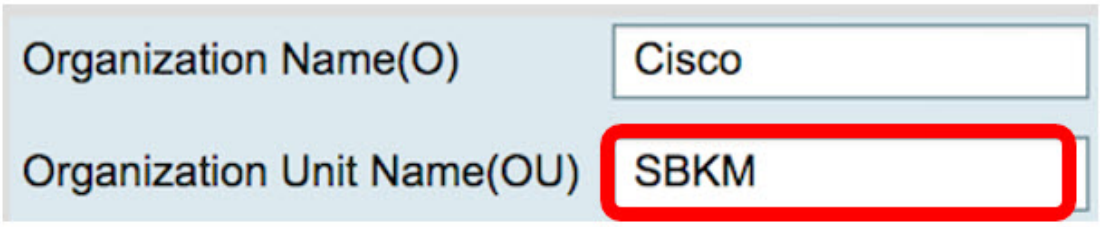
Nota: Nell'esempio viene utilizzato Irvine.

Passo 9: inserire il nome dell'organizzazione (O) nel campo fornito.



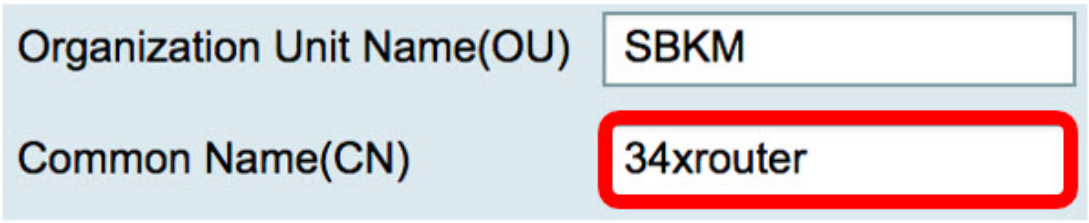
Nota: Nell'esempio, viene usato Cisco.

Passaggio 10. Inserire il nome dell'unità organizzativa nell'apposito campo.



Nota: Nell'esempio viene utilizzato il formato SBKM.

Passaggio 11. Inserire un nome nel campo *Nome comune (CN)*.

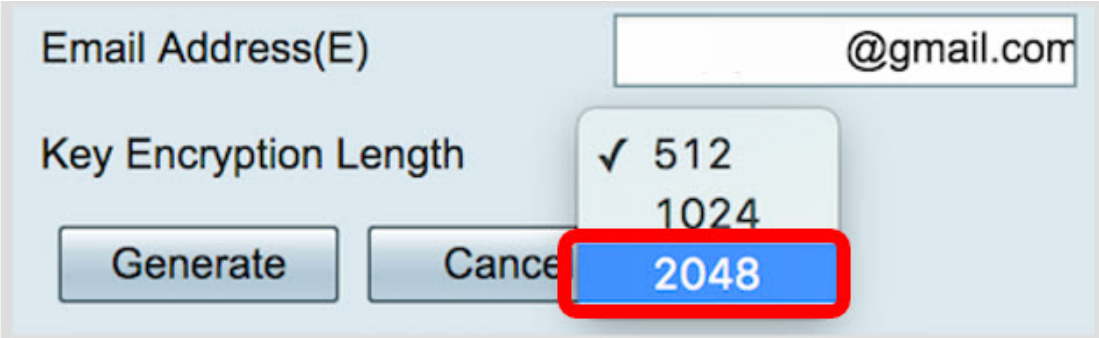


Nota: nell'esempio, viene usato un router 34x.

Passaggio 12. Immettere l'indirizzo di posta elettronica o qualsiasi indirizzo di posta elettronica a cui si desidera inviare il certificato.

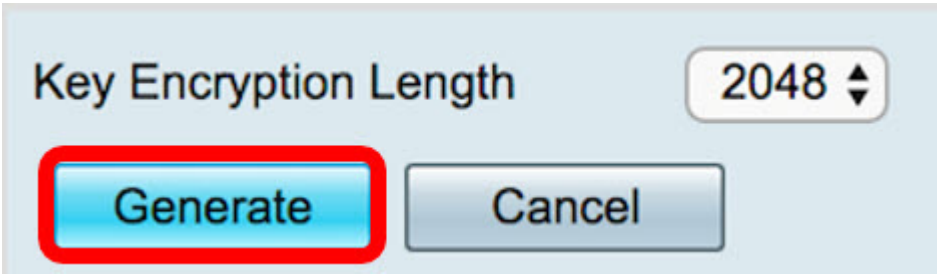
Nota: Nell'esempio viene utilizzato un indirizzo di posta elettronica gmail.com.

Passaggio 13. Scegliere una *Lunghezza crittografia chiave* dal menu a discesa per impostare il numero di bit nella chiave. La lunghezza predefinita è 512.



Nota: Nell'esempio viene utilizzato 2048. Si tratta di un'opzione consigliata, in quanto una crittografia più lunga è più difficile da decodificare rispetto a chiavi più corte, rendendola quindi più sicura.

Passaggio 14. Fare clic su **Genera**.



La richiesta di certificato creata verrà visualizzata nella tabella Certificati.

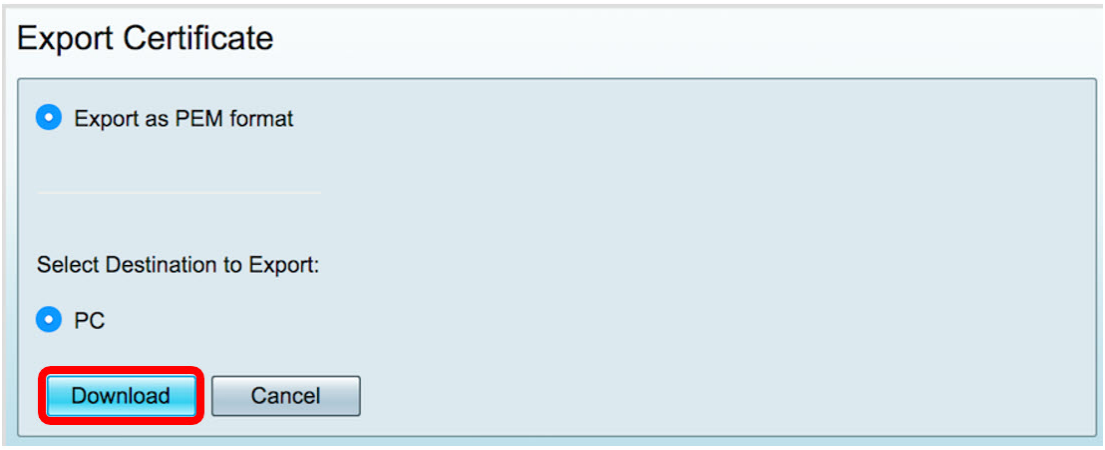
Creazione di un CSR completata.

Esportare il CSR

Passaggio 1. Selezionare la casella accanto alla richiesta di certificato nella tabella Certificati e fare clic su **Esporta**.

Passaggio 2. Fare clic su **Download** nella finestra *Esporta certificato* per scaricare il file nel

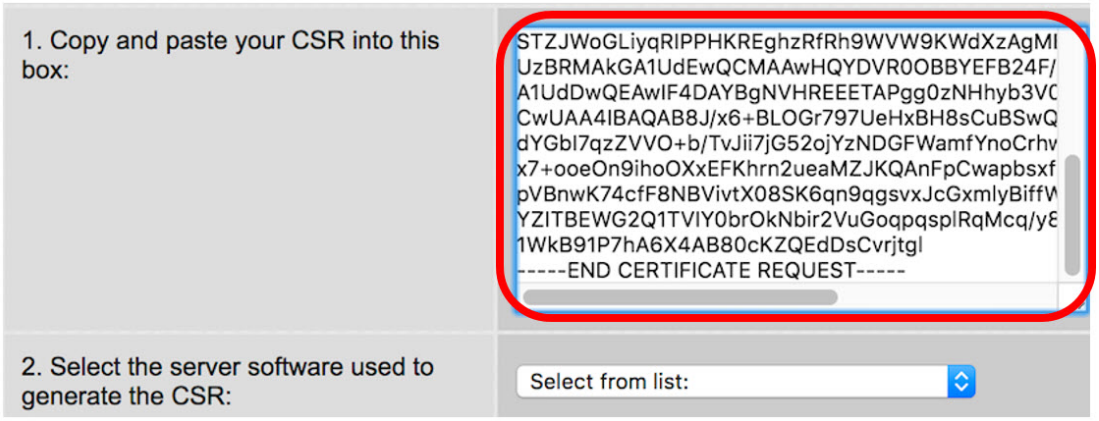
computer in formato PEM.



Esportazione del CSR nel computer completata.

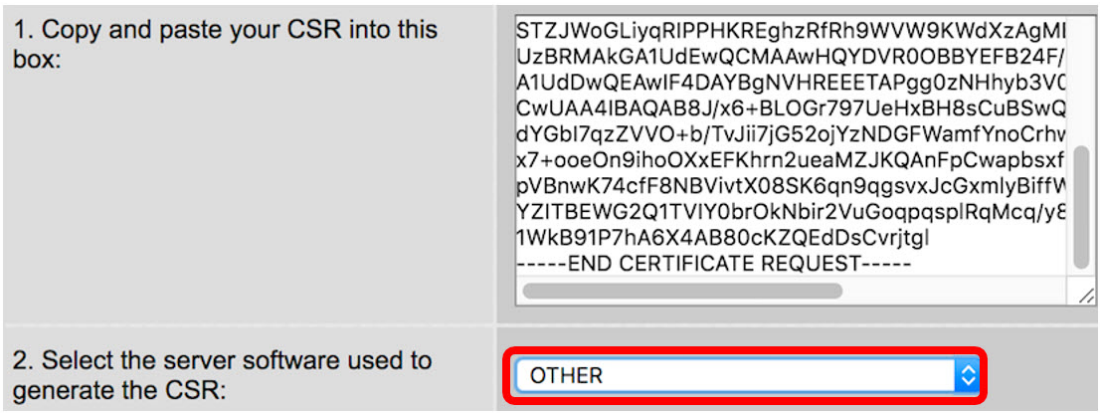
Carica CSR nel provider di certificati

Passaggio 1. Aprire il file scaricato utilizzando un blocco note e copiare il CSR, quindi incollarlo nel campo disponibile nel sito del provider di certificati SSL di terze parti.



Nota: In questo esempio, Comodo.com viene utilizzato come provider di certificati.

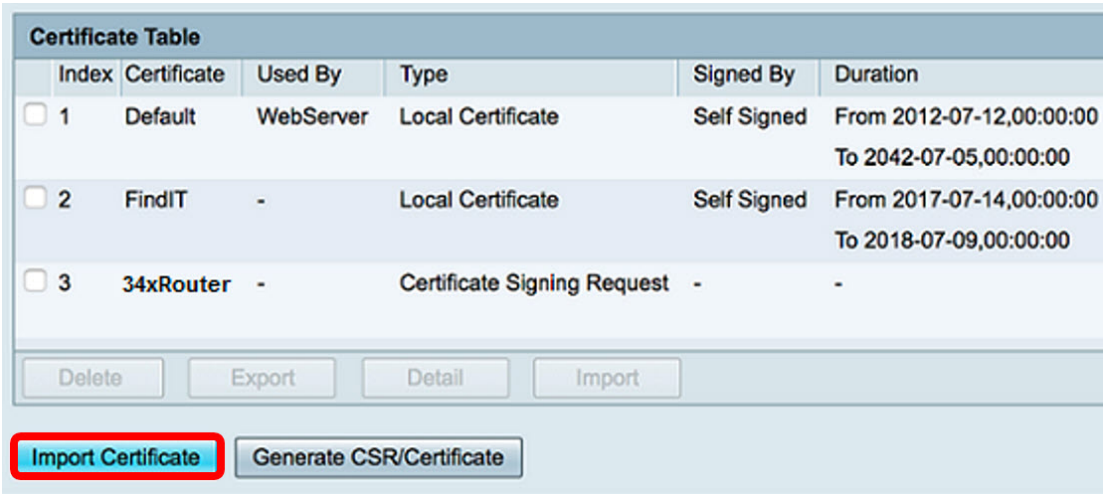
Passaggio 2. Selezionare il software server utilizzato per generare il CSR. In questo caso, poiché il router RV34x non è presente nell'elenco, si sceglie ALTRO.



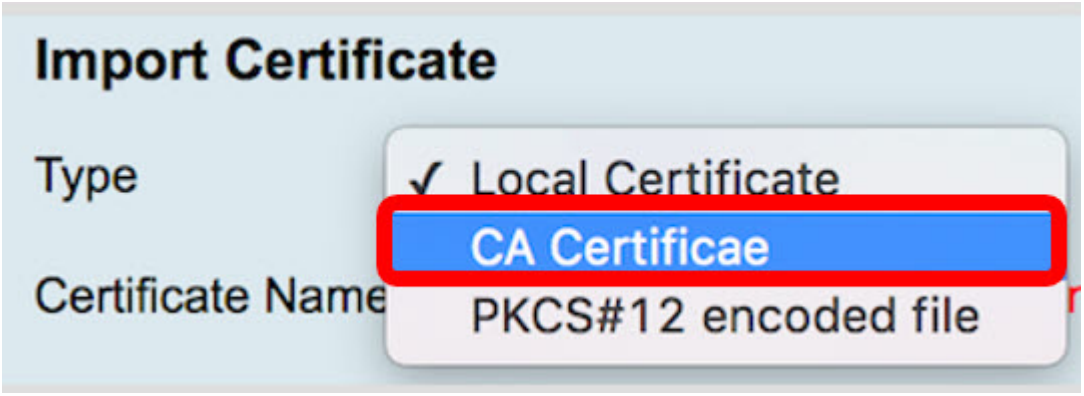
Passaggio 3. Scaricare il certificato nel computer.

Carica il certificato di terze parti SSL

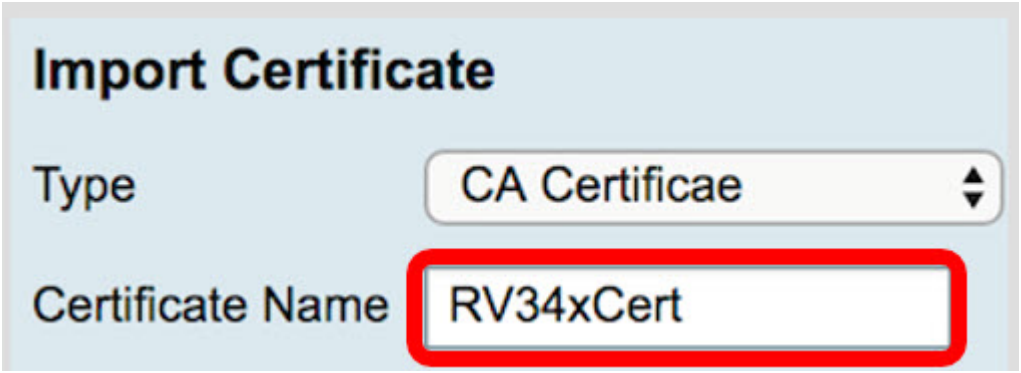
Passaggio 1. Nell'utility basata sul Web del router, fare clic sul pulsante **Importa certificato** sotto la tabella Certificati.



Passaggio 2. Nella finestra *Importa certificato*, fare clic sul menu a discesa *Tipo* e scegliere **Certificato CA**.

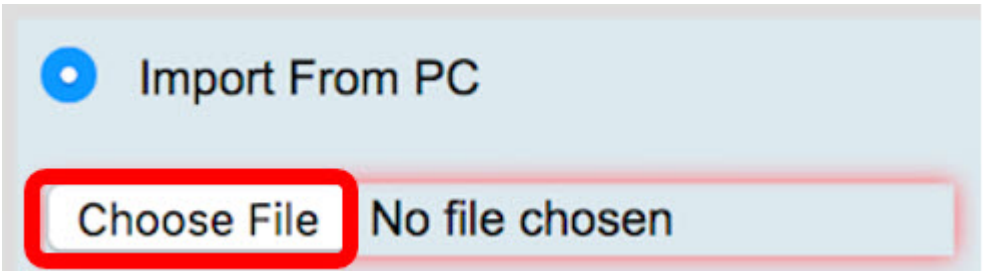


Passaggio 3. Inserire un nome di certificato nel campo fornito.

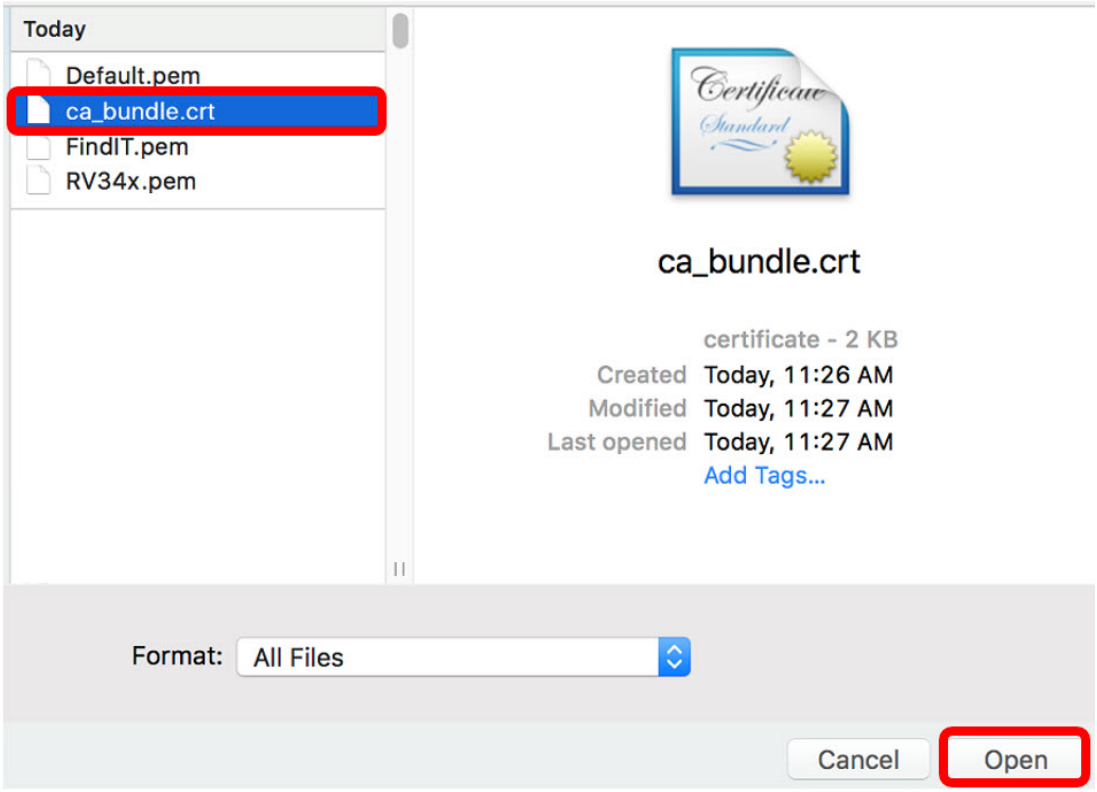


Nota: Nell'esempio viene utilizzato RV34xCert.

Passaggio 4. Fare clic sul pulsante **Scegli file** e individuare il file del certificato scaricato dalla CA.

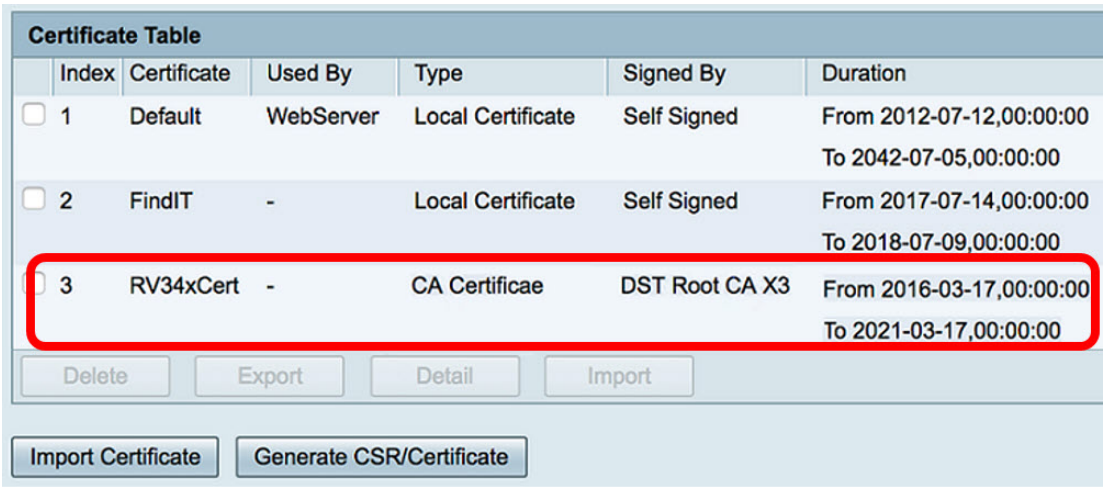


Passaggio 5. Fare clic sul file e quindi su **Apri**.



Passaggio 6. Fare clic su **Upload**.

Nella tabella Certificati verrà visualizzato il nuovo nome del certificato e il tipo verrà sostituito con un certificato CA con l'etichetta che indica che è stato firmato dall'autorità di certificazione di terze parti.

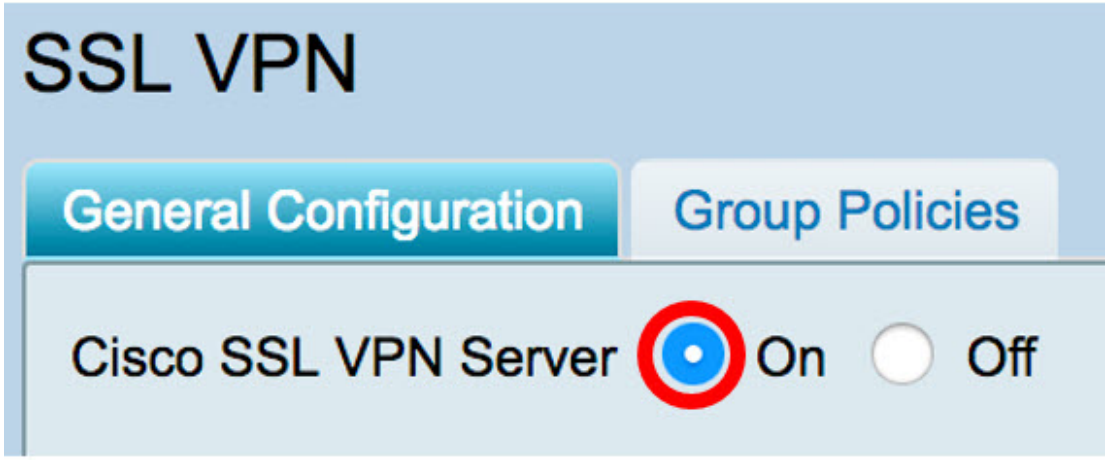


A questo punto, è stato caricato un certificato SSL di terze parti sul router RV34x.

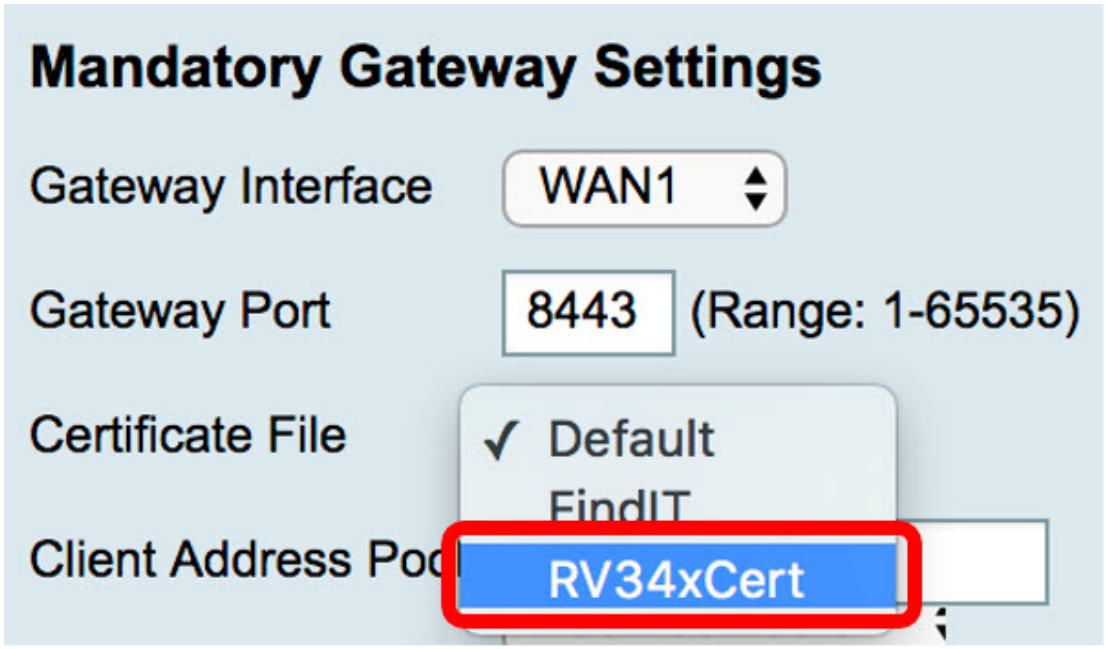
Sostituire il certificato autofirmato predefinito

Passaggio 1. Nell'utility basata sul Web, scegliere **VPN > SSL VPN**.

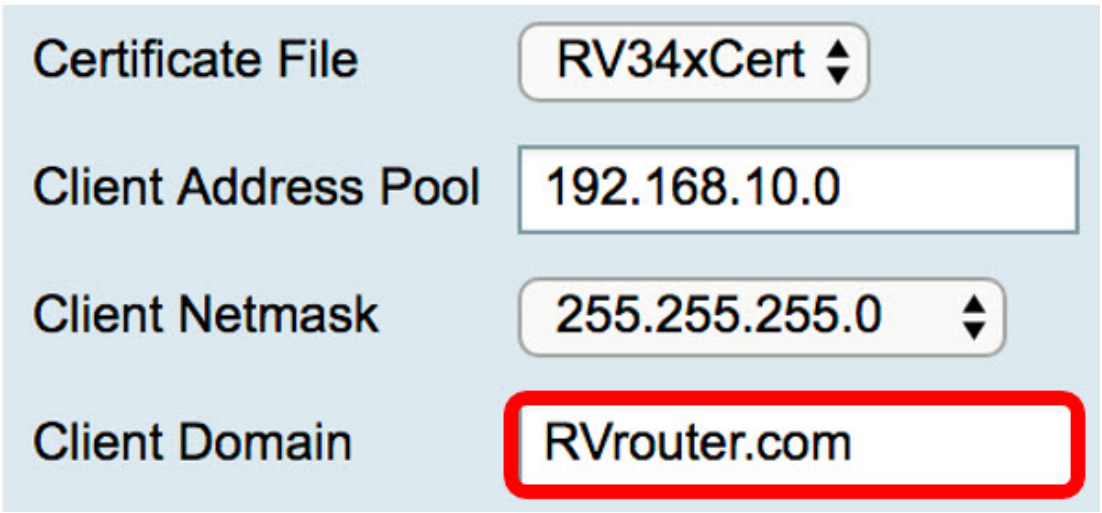
Passaggio 2. Fare clic sul pulsante di opzione **On** per abilitare il server VPN Cisco SSL.



Passaggio 3. In Impostazioni gateway obbligatorie fare clic sul menu a discesa *File certificato* e sostituire il certificato predefinito scegliendo il certificato SSL appena caricato.

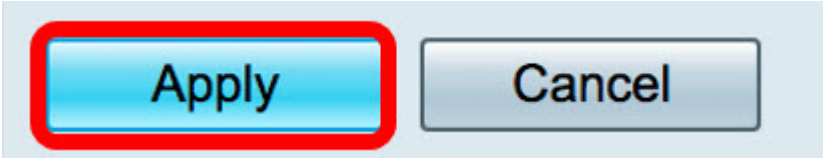


Passaggio 4. Inserire il dominio client richiesto nel campo fornito.



Nota: Nell'esempio viene utilizzato RVrouter.com.

Passaggio 5. Fare clic su **Applica**.



Il certificato autofirmato predefinito è stato sostituito con il certificato SSL di terze parti.

Potresti trovare anche questo articolo informativo: Domande frequenti (FAQ) sui router serie RV34x

Questo sito offre diversi collegamenti ad altri articoli che potrebbero essere interessanti: Serie RV34x Router - Pagina del prodotto