Gestione dei certificati sui router serie RV34x

Obiettivo

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 provenienti da applicazioni di terze parti.

In questa sezione verrà illustrato come ottenere un certificato da un'Autorità di certificazione (CA). Per l'autenticazione viene utilizzata una CA. I certificati possono essere acquistati da diversi siti di terze parti. È un modo ufficiale per dimostrare che il tuo sito è sicuro. Essenzialmente, la CA è una fonte attendibile che verifica che l'azienda sia legittima e che possa essere considerata attendibile. A seconda delle esigenze, un certificato a un costo minimo. L'utente viene estratto dall'autorità di certificazione e, una volta verificate le informazioni, il certificato verrà rilasciato all'utente. Il certificato può essere scaricato come file nel computer. È quindi possibile accedere al router (o al server VPN) e caricarlo in tale posizione.

Lo scopo di questo articolo è quello di illustrare come generare, esportare e importare certificati sul router serie RV34x.

Dispositivi interessati | Versione software

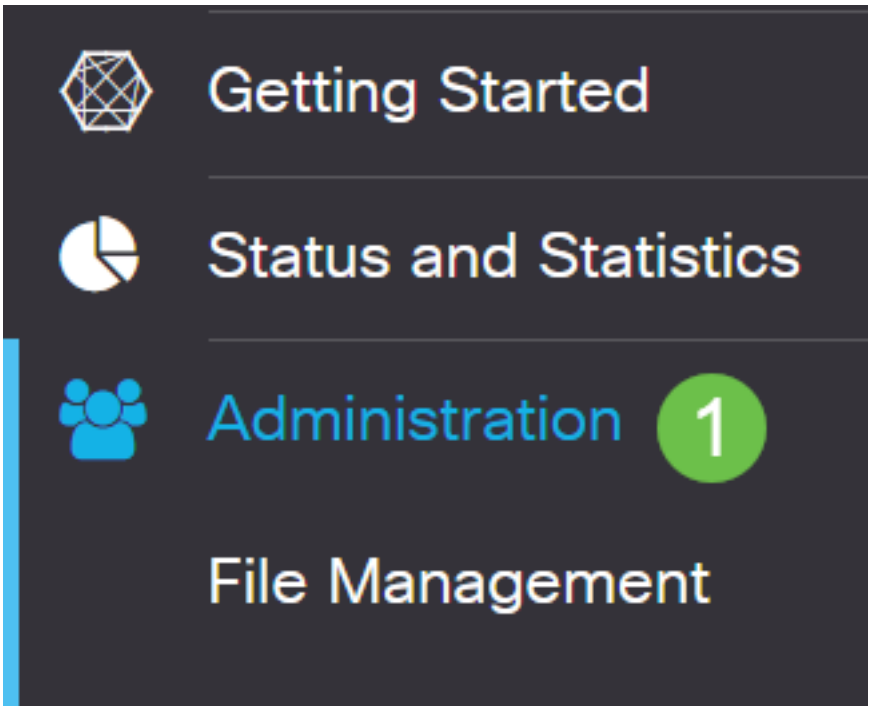
- Serie RV34x | 1.0.03.20

Gestisci certificati sul router

Genera CSR/certificato

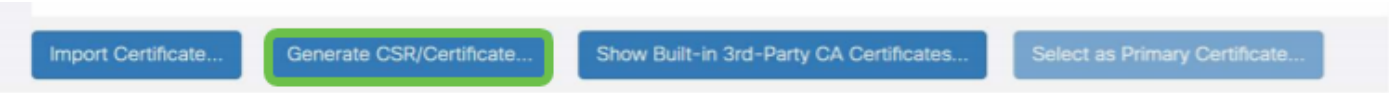
Passaggio 1

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



Passaggio 2

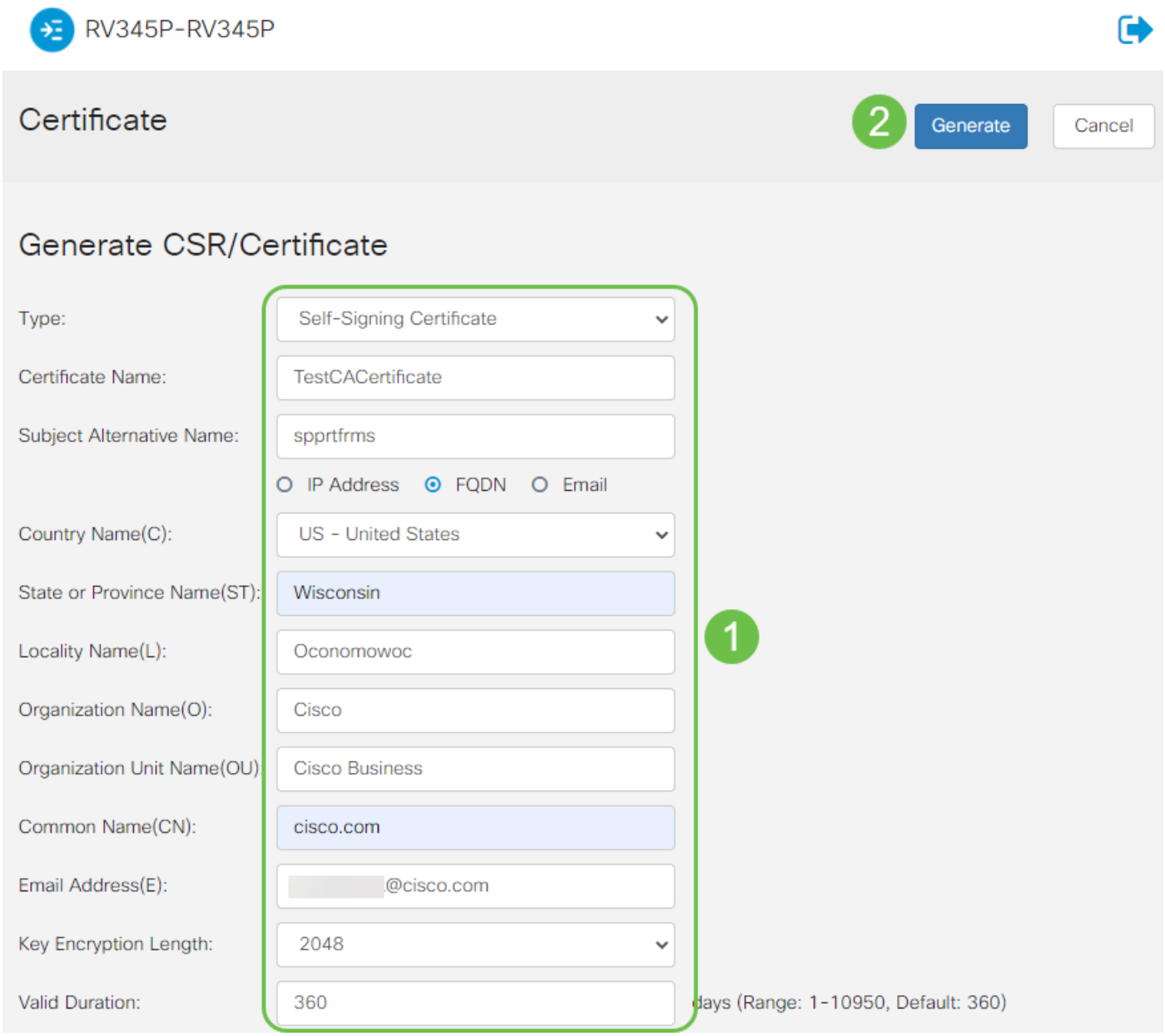
Fare clic su **Genera CSR/Certificato**. Verrà visualizzata la pagina Genera CSR/certificato.



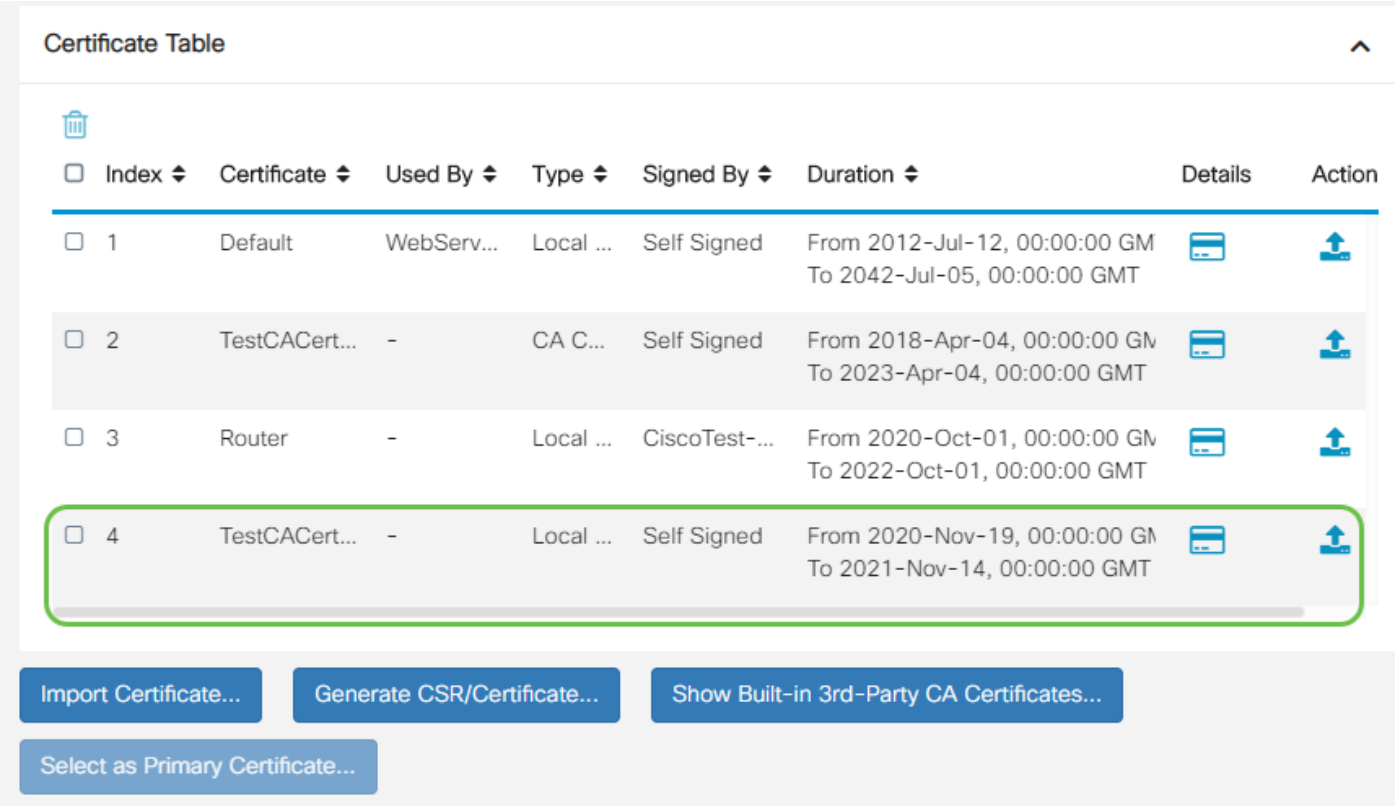
Passaggio 3

Compilare le caselle con quanto segue:

- Scegliere il tipo di certificato appropriato
  - Certificato autofirmato: certificato SSL (Secure Socket Layer) firmato dal proprio creatore. Il certificato è meno attendibile, in quanto non può essere annullato se la chiave privata è compromessa da un utente non autorizzato.
  - Richiesta di firma certificata - Infrastruttura a chiave pubblica (PKI) inviata all'autorità di certificazione per richiedere un certificato di identità digitale. È più sicuro della firma automatica in quanto la chiave privata viene mantenuta segreta.
- Immettere un nome per il certificato nel campo *Nome certificato* per identificare la richiesta. Il campo non può essere vuoto né contenere spazi e caratteri speciali.
- (Facoltativo) Nell'area Nome alternativo soggetto fare clic su un pulsante di opzione. Le opzioni sono:
  - Indirizzo IP — Immettere un indirizzo IP (Internet Protocol)
  - FQDN — immettere un nome di dominio completo (FQDN)
  - Email - Inserisci un indirizzo email
- Nel campo *Nome alternativo soggetto*, immettere il nome di dominio completo.
- Dall'elenco a discesa Country Name (Nome paese), selezionare il paese in cui l'organizzazione è legalmente registrata.
- Inserire il nome o l'abbreviazione dello stato, della provincia, della regione o del territorio in cui si trova l'organizzazione nel campo *Stato o Nome provincia(ST)*.
- Nel campo *Nome località* immettere il nome della località o della città in cui l'organizzazione è registrata o si trova.
- Immettere un nome con il quale l'azienda è legalmente registrata. Se ci si iscrive come piccola impresa o come proprietario unico, immettere il nome del richiedente del certificato nel campo *Nome organizzazione*. Non è possibile utilizzare caratteri speciali.
- Inserire un nome nel campo *Nome unità organizzazione* per distinguere le divisioni all'interno di un'organizzazione.
- Immettere un nome nel campo *Nome comune*. Questo nome deve essere il nome di dominio completo del sito Web per il quale si utilizza il certificato.
- Immettere l'indirizzo di posta elettronica della persona che desidera generare il certificato.
- Dall'elenco a discesa Lunghezza crittografia chiave, scegliere la lunghezza della chiave. Le opzioni sono 512, 1024 e 2048. Maggiore è la lunghezza della chiave, più sicuro sarà il certificato.
- Nel campo *Durata valida* immettere il numero di giorni di validità del certificato. Il valore predefinito è 360.
- Fare clic su **Genera**.



Nota: Il certificato generato verrà visualizzato nella tabella Certificati.

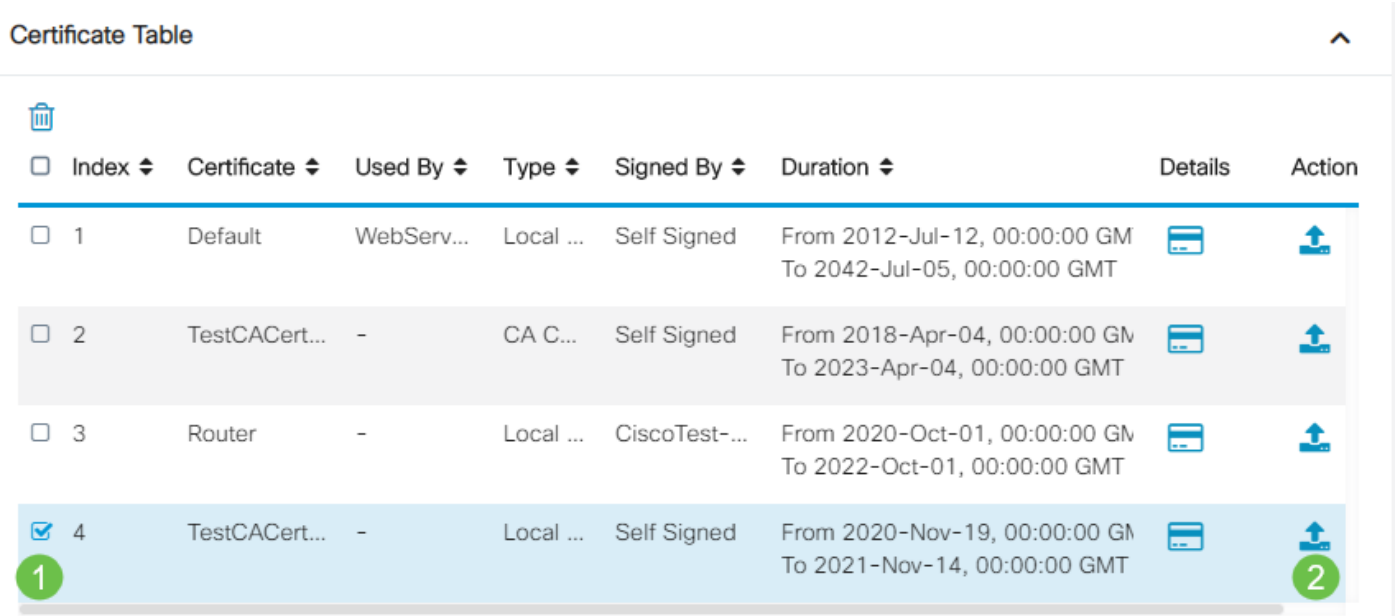


A questo punto, è necessario creare un certificato sul router RV345P.

Esporta certificato

Passaggio 1

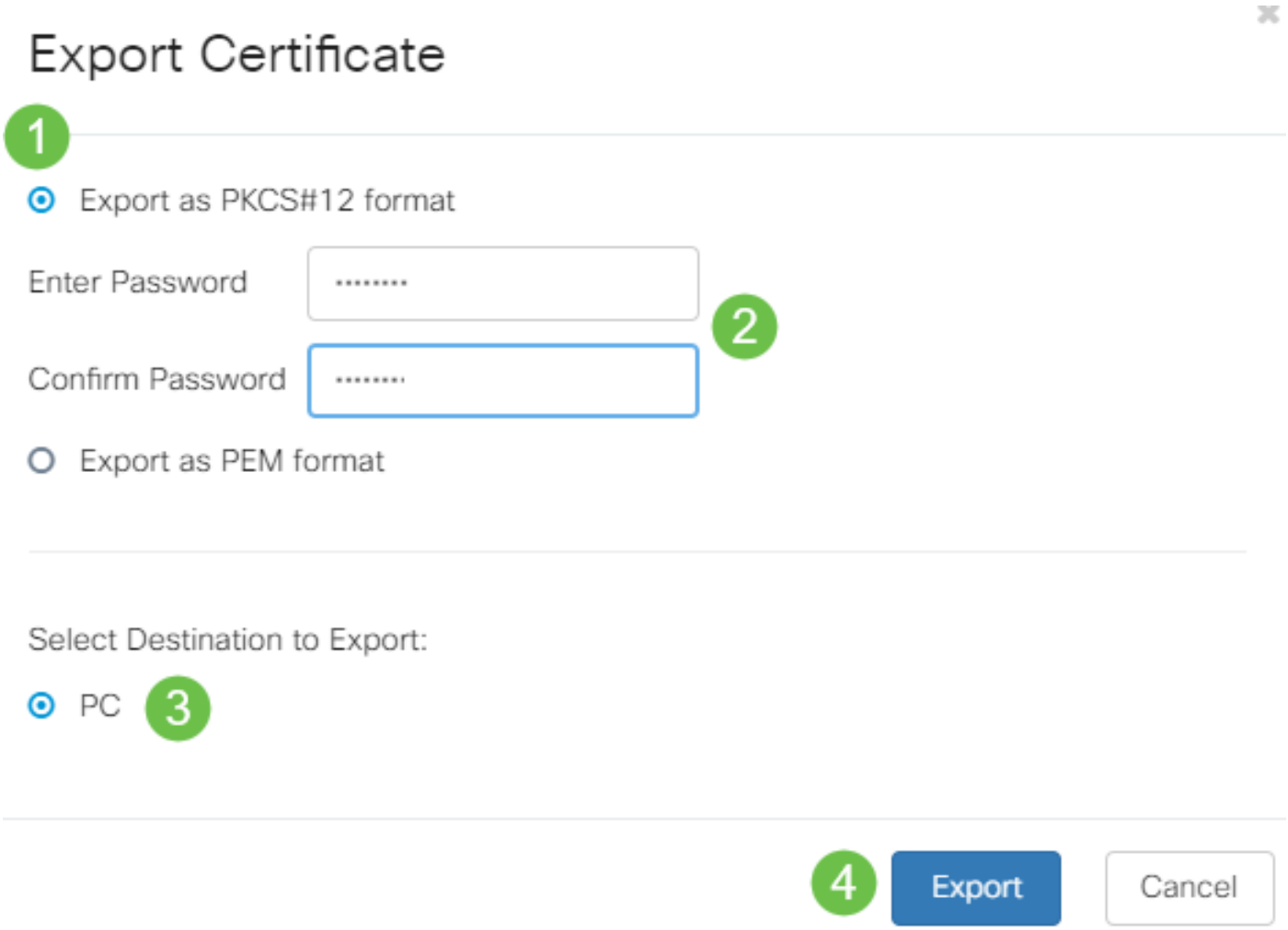
Nella tabella Certificati selezionare la casella di controllo del certificato che si desidera esportare e fare clic sull'**icona Esporta**.



Passaggio 2

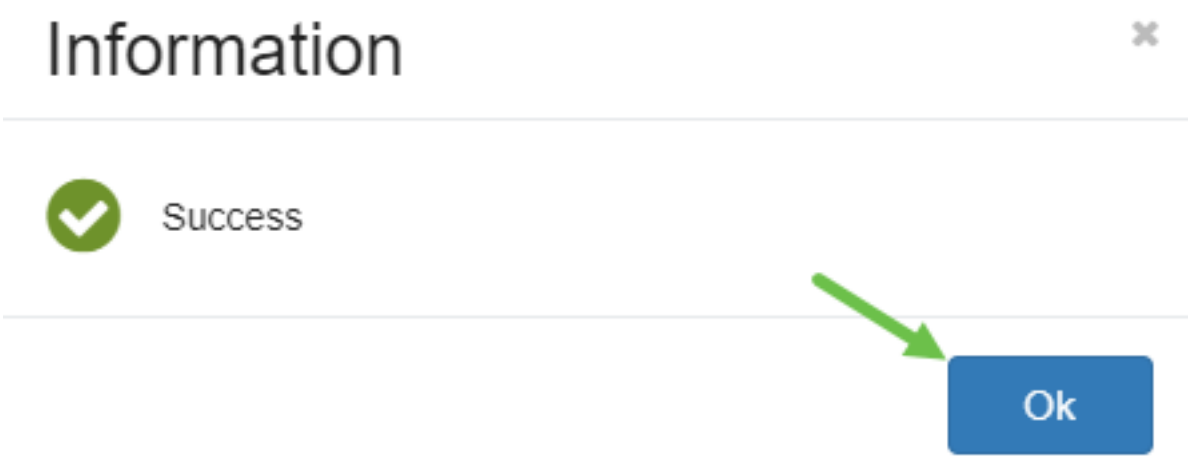
- Fare clic su un formato per esportare il certificato. Le opzioni sono:
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 è un certificato esportato con estensione .p12. Per crittografare il file e proteggerlo durante l'esportazione, l'importazione e l'eliminazione è necessaria una password.

    - PEM — Privacy Enhanced Mail (PEM) è spesso utilizzato per i server Web per la loro capacità di essere facilmente tradotti in dati leggibili utilizzando un semplice editor di testo come il Blocco note.
- Se si sceglie PEM, fare clic su **Esporta**.
- Immettere una password per proteggere il file da esportare nel campo *Immettere password*.
- Immettere nuovamente la password nel campo *Conferma password*.
- Nell'area Seleziona destinazione è stato scelto PC, l'unica opzione attualmente disponibile.
- Fare clic su **Esporta**.



Passaggio 3

Sotto il pulsante Download viene visualizzato un messaggio che indica che il download è riuscito. Verrà avviato il download di un file nel browser. Fare clic su **OK**.

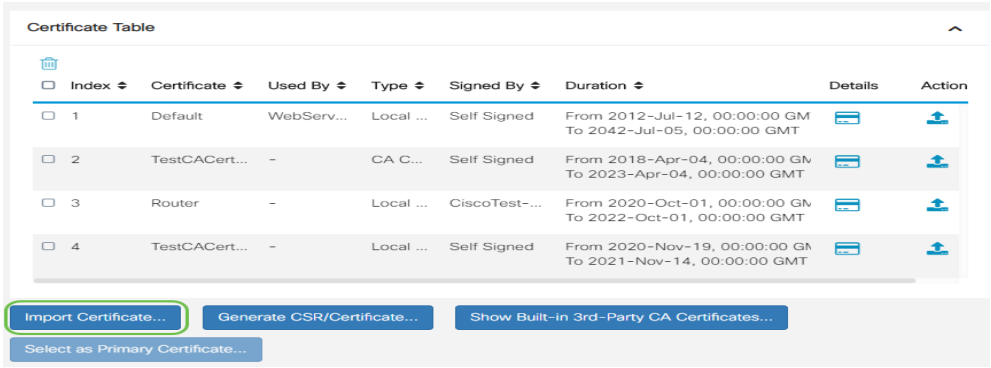


A questo punto, il certificato sul router serie Rv34x dovrebbe essere stato esportato correttamente.

Importa certificato

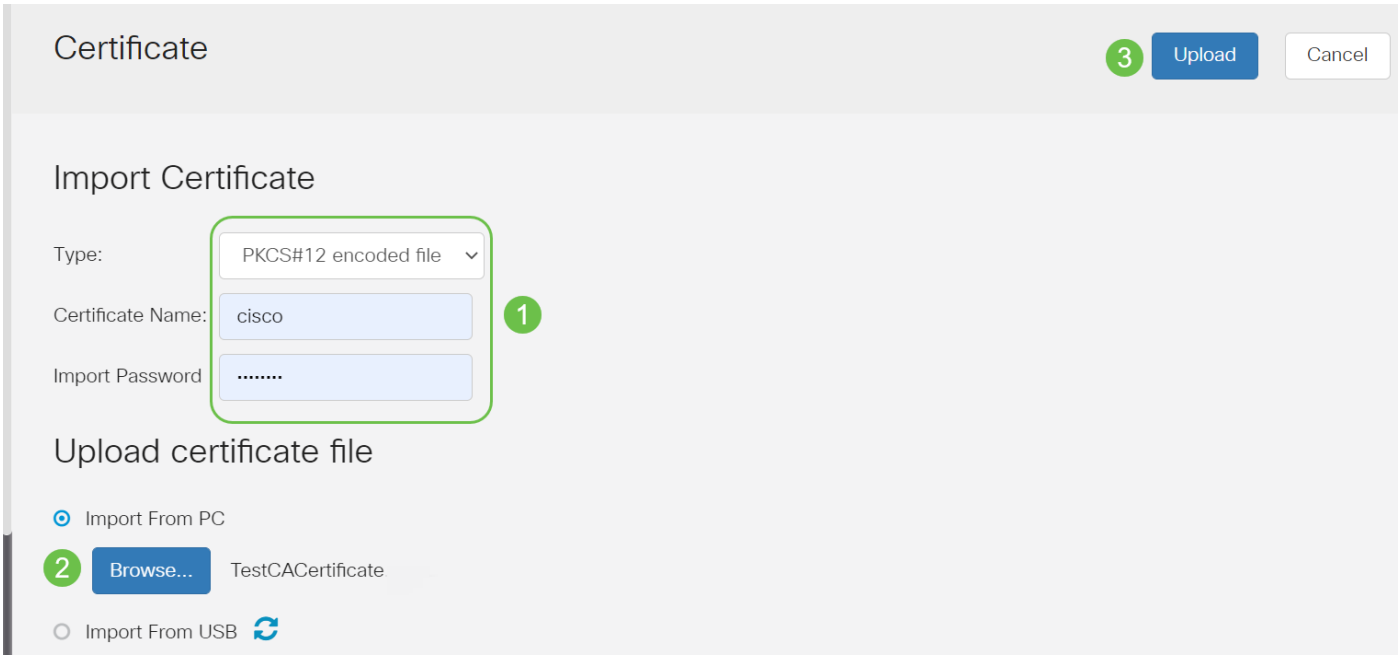
Passaggio 1

Fare clic su **Importa certificato...**.

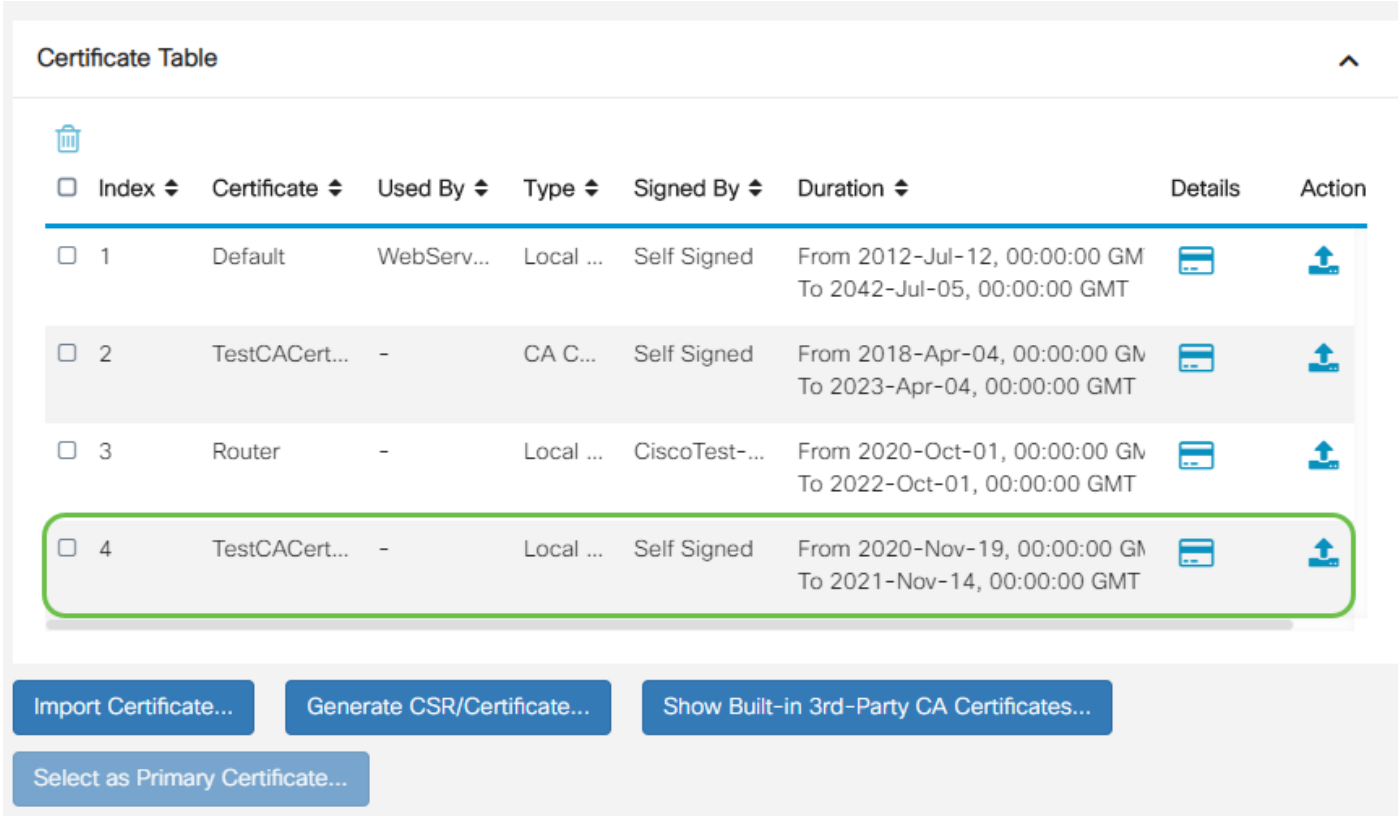


Passaggio 2

- Selezionare dall'elenco a discesa il tipo di certificato da importare. Le opzioni sono:
  - Certificato locale — Un certificato generato sul router.
  - Certificato CA - Certificato certificato da un'autorità di terze parti attendibile che ha confermato l'accuratezza delle informazioni contenute nel certificato.
  - File codificato PKCS #12 — PKCS (Public Key Cryptography Standards) #12 è un formato di archiviazione di un certificato server.
- Immettere un nome per il certificato nel campo *Nome certificato*.
- Se è stato scelto PKCS #12, immettere una password per il file nel campo *Importa password*. In caso contrario, andare al passaggio 3.
- Fare clic su un'origine per importare il certificato. Le opzioni sono:
  - Importa da PC
  - Importa da USB
- Se il router non rileva un'unità USB, l'opzione Importa da USB non è disponibile.
- Se si sceglie Importa da USB e il dispositivo USB non viene riconosciuto dal router, fare clic su Aggiorna.
- Fare clic sul pulsante Scegli file e scegliere il file appropriato.
- Fare clic su **Upload**.



Se l'operazione ha esito positivo, verrà visualizzata automaticamente la pagina principale del certificato. Nella tabella dei certificati verrà inserito il certificato importato di recente.



A questo punto, il certificato sul router serie RV34x dovrebbe essere stato importato correttamente.