OpenVPN su un RV160 e RV260 Router

Obiettivo

L'obiettivo di questo articolo è di guidarvi nella configurazione di OpenVPN sul router RV160 o RV260 e nella configurazione del client VPN di OpenVPN sul computer.

Dispositivi interessati

- RV160
- RV260

Versione del software

- 1.0.00.15

Sommario

Introduzione

OpenVPN è un'applicazione open source gratuita che può essere configurata e utilizzata per una rete VPN (Virtual Private Network). Utilizza una connessione client-server per garantire comunicazioni protette tra un server e una posizione remota del client tramite Internet.

OpenVPN utilizza OpenSSL per la crittografia di UDP e TCP per la trasmissione del traffico. Una VPN offre un tunnel di protezione sicuro, meno vulnerabile agli hacker poiché crittografa i dati inviati dal computer tramite la connessione VPN. Ad esempio, se si utilizza WiFi in un luogo pubblico, come in un aeroporto, i dati, le transazioni e le query non vengono visualizzati da altri utenti. Analogamente al protocollo HTTPS, crittografa i dati inviati tra due endpoint.

Uno dei passaggi più importanti per la configurazione di OpenVPN è ottenere un certificato da un'Autorità di certificazione (CA). Utilizzato per l'autenticazione. 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. Per OpenVPN è sufficiente un certificato di livello inferiore 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. Nota: i client non hanno bisogno di un certificato per usare OpenVPN, è solo per la verifica tramite il router.

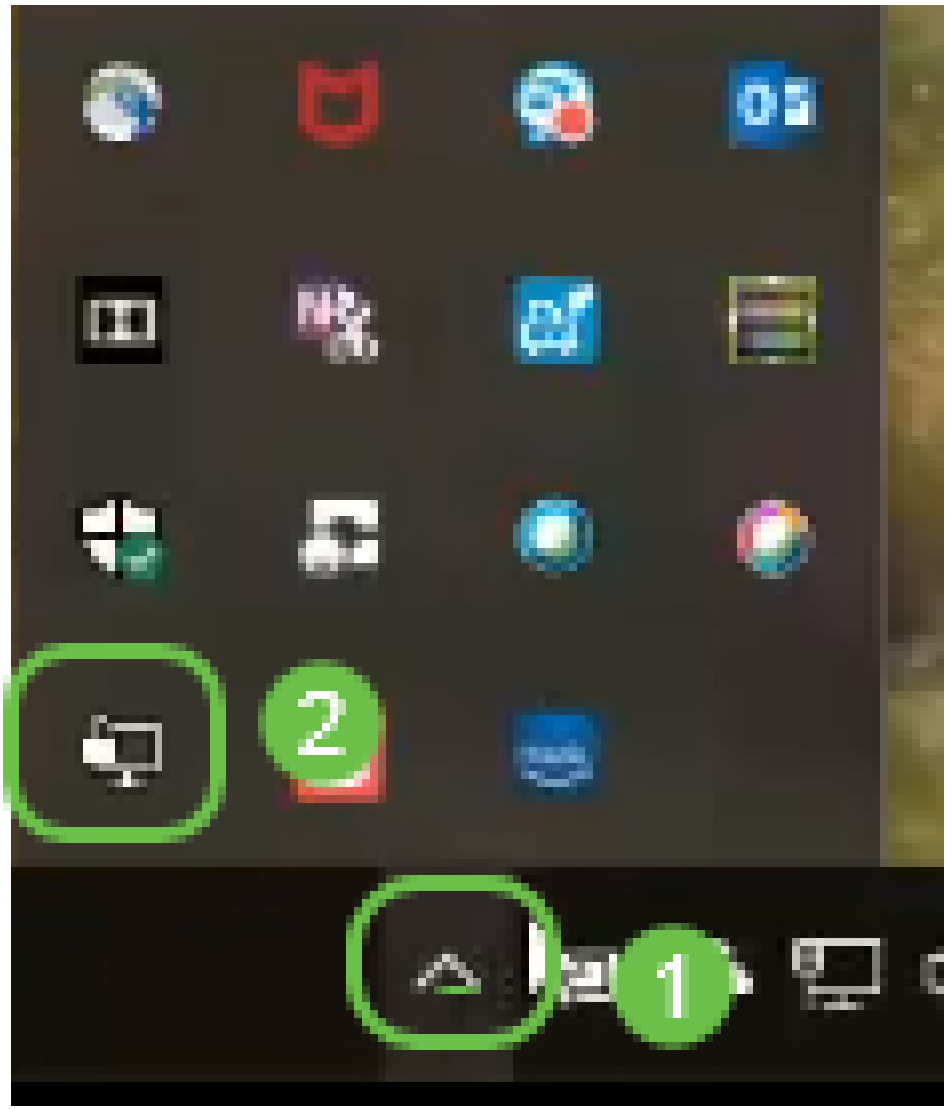
Prerequisiti

Installare l'applicazione OpenVPN nel sistema. Fare clic qui per accedere al sito Web OpenVPN.

Per ulteriori informazioni su OpenVPN e le risposte a molte domande che potresti avere, clicca qui .

Nota: Questa installazione è specifica di Windows 10.

Una volta installato OpenVPN, l'applicazione dovrebbe apparire sul desktop o come una piccola icona sul lato destro della barra delle applicazioni. Anche i client OpenVPN avranno bisogno di questa installazione.



Assicurarsi di aver impostato l'ora di sistema corretta su tutti i dispositivi. Prima di creare un

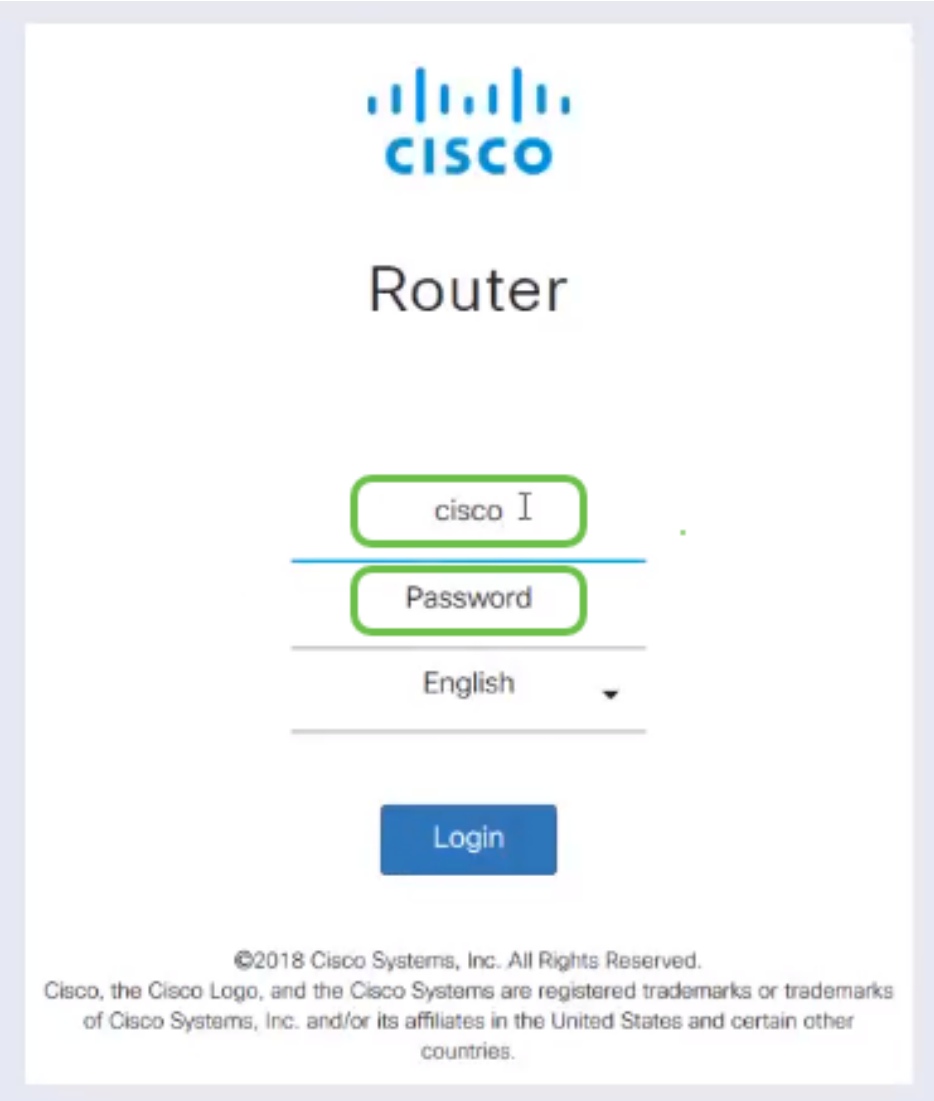
certificato, è necessario sincronizzare completamente l'ora di sistema corretta sul router. Questa operazione viene spesso eseguita automaticamente, ma se si verificano problemi, è consigliabile controllare in questa posizione.

Configurazione di una Demo OpenVPN su un router RV160/RV260

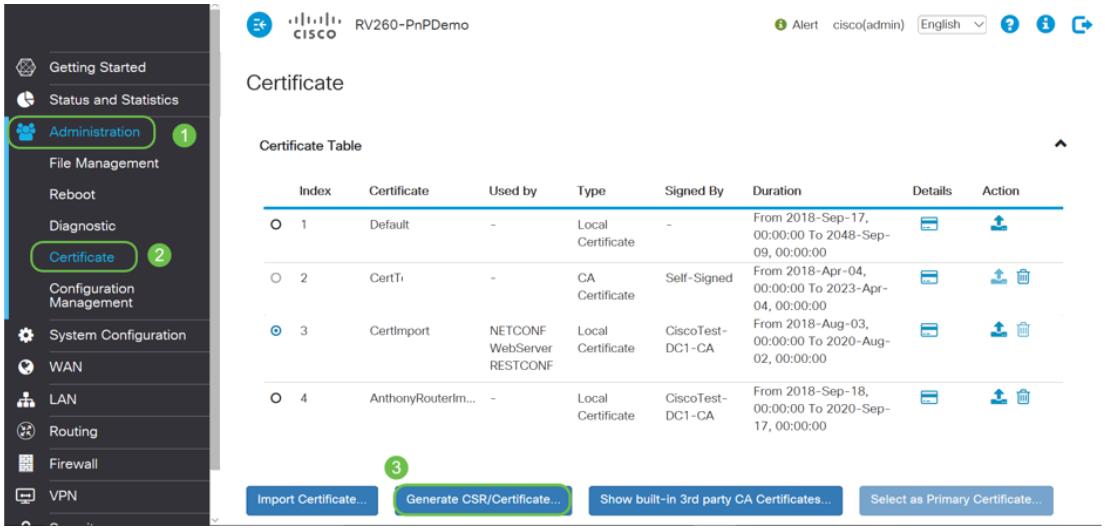
Se si desidera provare OpenVPN prima di pagare per una CA, è possibile creare un certificato autofirmato. Questo è un modo a costo zero per vedere se OpenVPN è qualcosa che si desidera installare per la vostra azienda. Se già si è certi di voler acquistare una CA, è possibile saltare questa sezione dell'articolo e andare direttamente a Configurazione di OpenVPN su un router RV160/RV260.

Passaggio 1. Accedere al router utilizzando le credenziali. Il nome utente e la password predefiniti sono *cisco*.

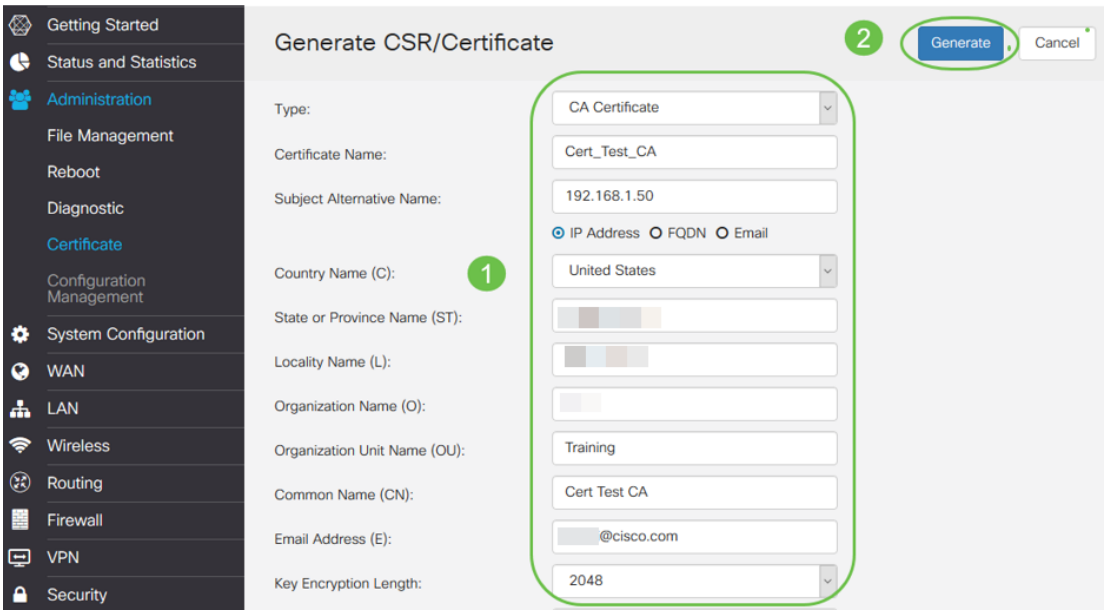
Nota: Si consiglia di modificare tutte le password in modo da renderle più complesse. Altrimenti, è come lasciare la chiave alla porta chiusa a chiave sulla soglia.



Passaggio 2. È necessario ottenere un certificato sul router. Passare a **Amministrazione > Certificato > Genera CSR/Certificato...** In questo modo viene creata la richiesta di un certificato.



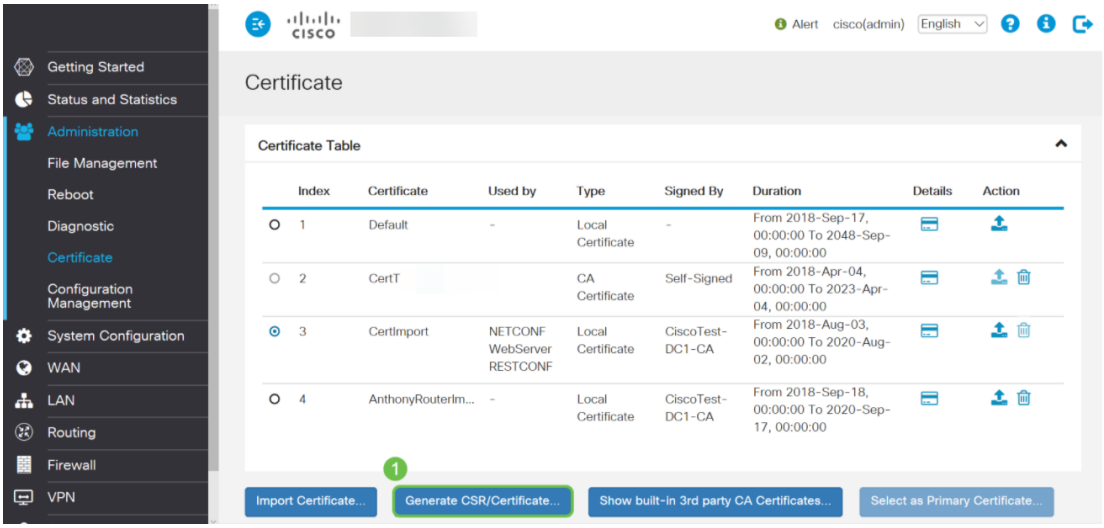
Passaggio 3. Richiedere un *certificato CA*.



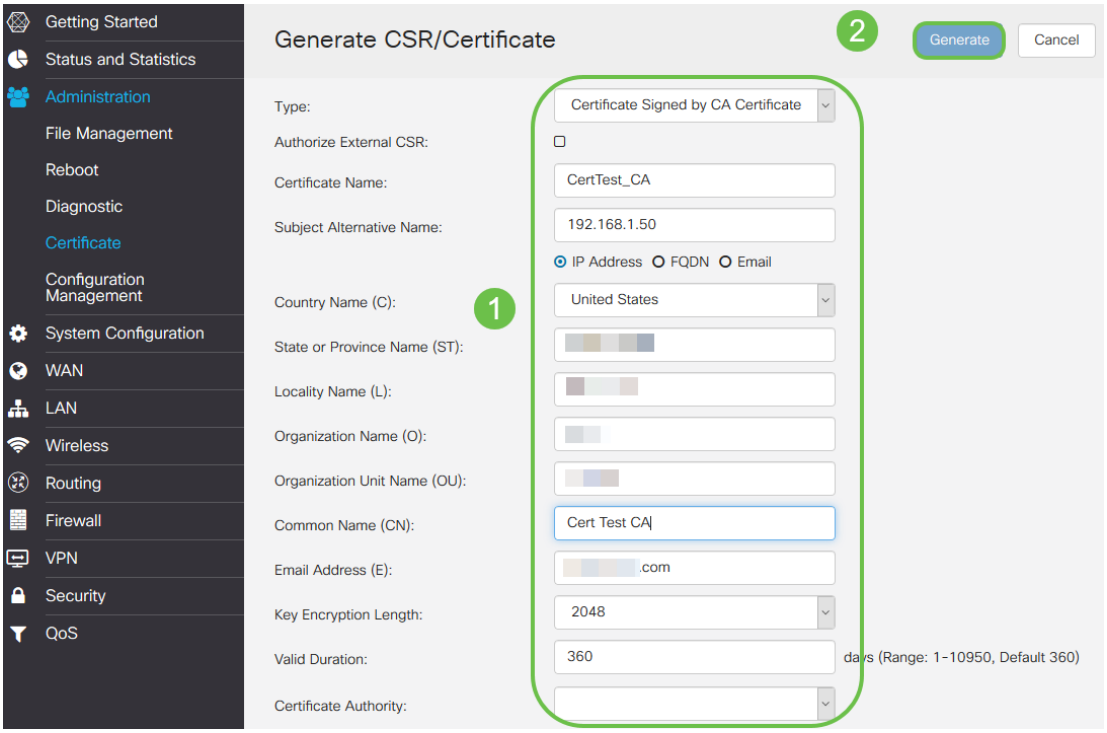
- Selezionare *Certificato CA* dal menu a discesa
- Immettere il nome di un certificato
- Immettere l'indirizzo IP, il nome di dominio completo (FQDN) o l'indirizzo di posta elettronica. L'immissione dell'indirizzo IP è la scelta più comune.
- Inserire il Paese
- Immettere lo stato
- Inserire il nome della località, in genere la città
- Inserire il nome dell'organizzazione
- Inserire il nome dell'unità organizzativa
- Immetti il tuo indirizzo e-mail
- Immettere la lunghezza di crittografia della chiave, si consiglia 2048

Fare clic sul pulsante **Genera in** alto a destra.

Passaggio 4. È inoltre necessario un certificato server. Questo *certificato firmato da CA* verrà firmato dal certificato CA appena creato.



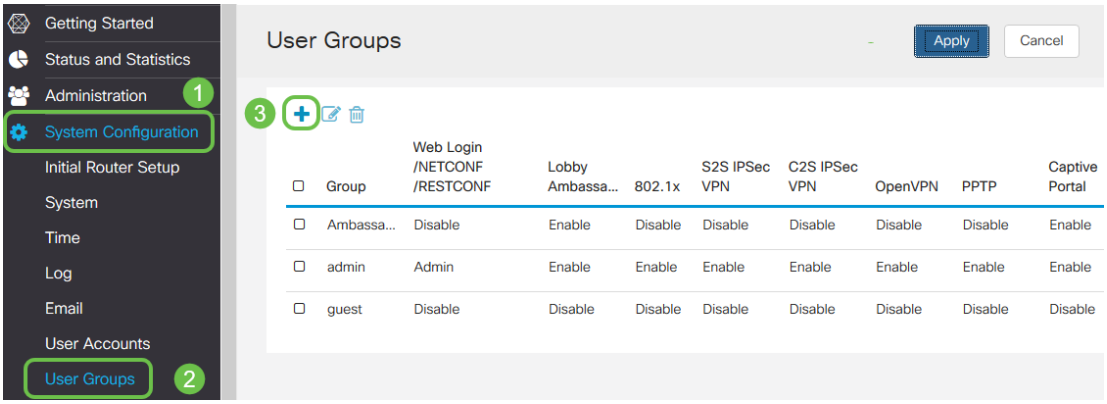
Passaggio 5. Richiedere un *certificato firmato da un certificato CA*.



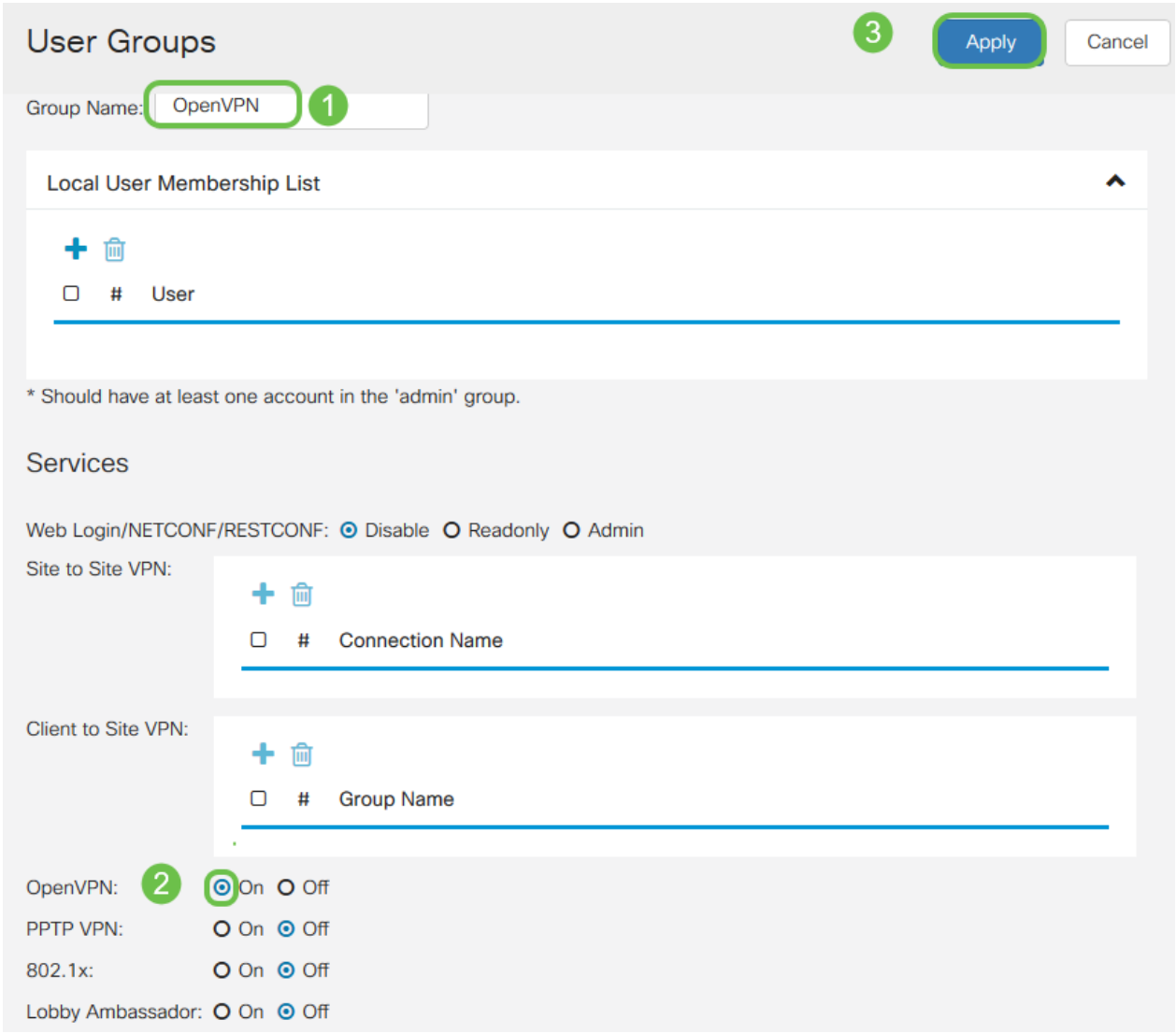
- Selezionare *Richiesta firma certificato* dal menu a discesa
- Immettere il nome di un certificato
- Immettere l'indirizzo IP, il nome di dominio completo (FQDN) o l'indirizzo di posta elettronica. L'immissione dell'indirizzo IP è la scelta più comune.
- Inserire il Paese
- Immettere lo stato
- Inserire il nome della località, in genere la città
- Inserire il nome dell'organizzazione
- Inserire il nome dell'unità organizzativa
- Immetti il tuo indirizzo e-mail
- Immettere la lunghezza di crittografia della chiave, si consiglia 2048
- Scegliere l'autorità di certificazione appropriata dal menu a discesa

Fare clic sul pulsante **Genera in** alto a destra.

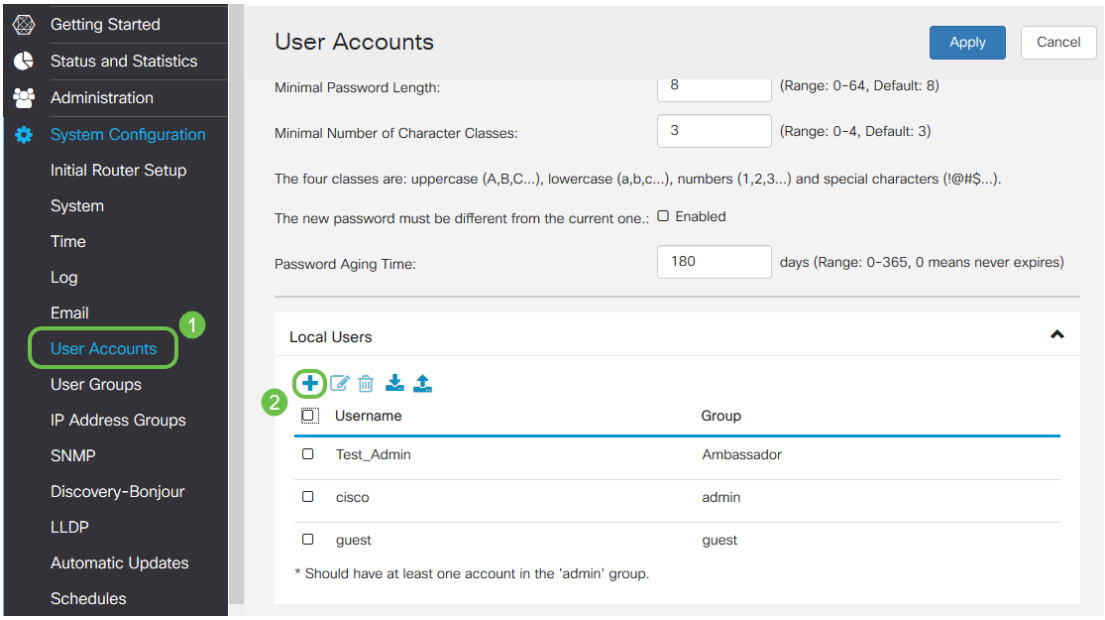
Passaggio 6. Passare a **Configurazione di sistema > Gruppi di utenti**. Selezionare l'icona **più** per aggiungere il nuovo gruppo.



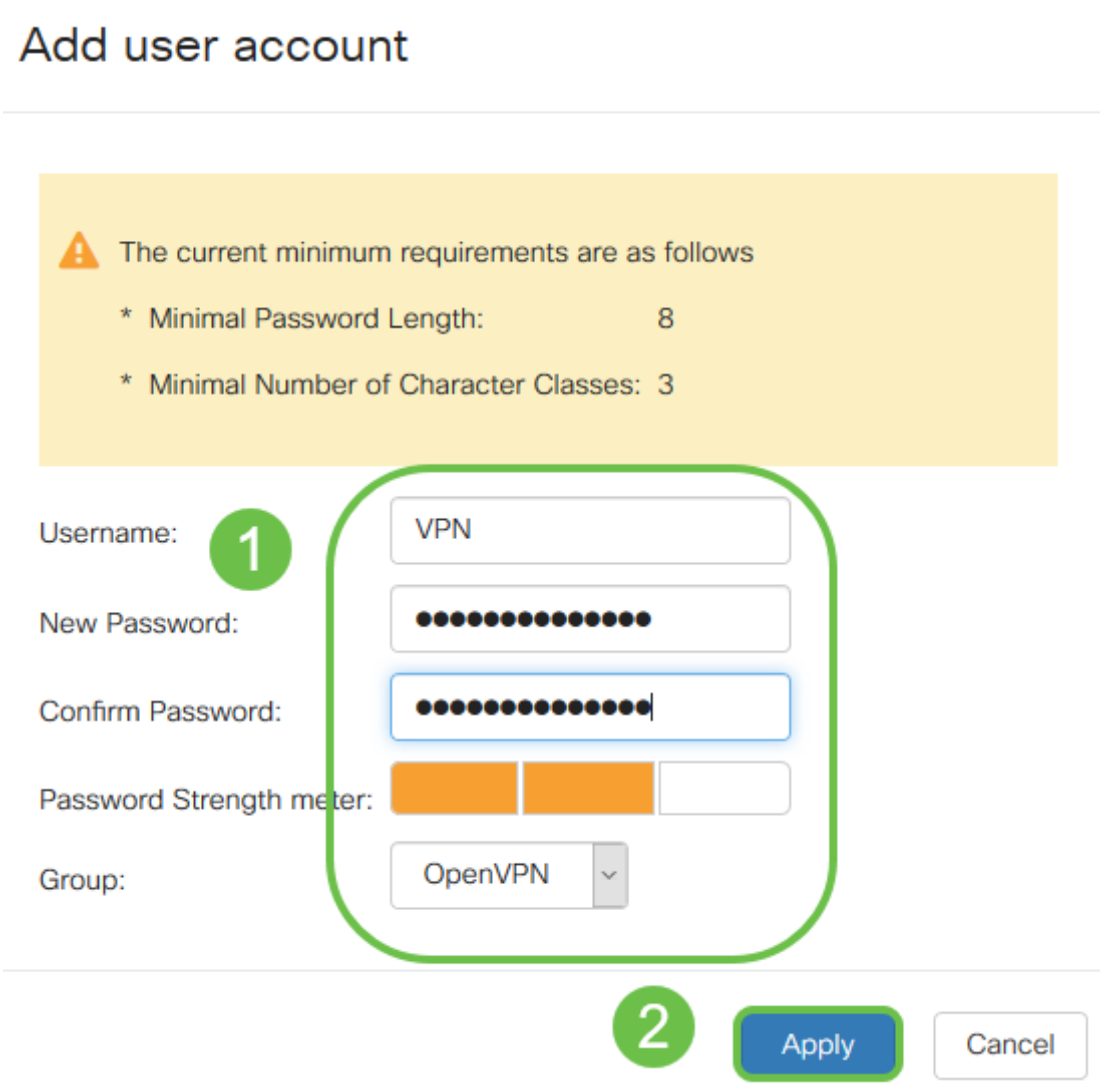
Passaggio 7. Immettere il nome del gruppo e fare clic su *On* per attivare OpenVPN. Fare clic su **Apply** (Applica).



Passaggio 8. Passare al menu Configurazione di sistema e fare clic su **Account utente**. In Utenti locali, fare clic sull'icona **più**.

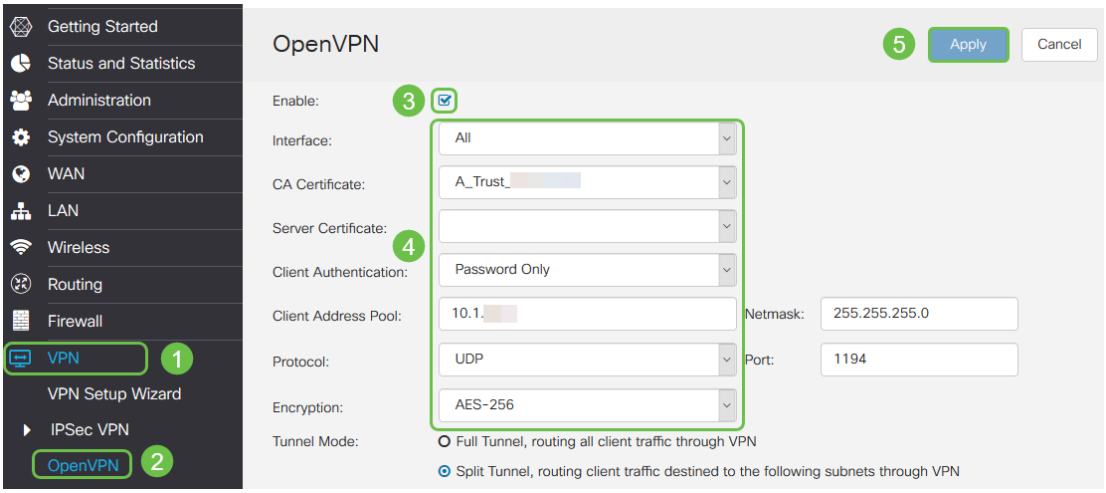


Passaggio 9. Inserire le informazioni richieste di seguito. Assicurarsi di selezionare OpenVPN dal menu a discesa. Fare clic su **Apply** (Applica).



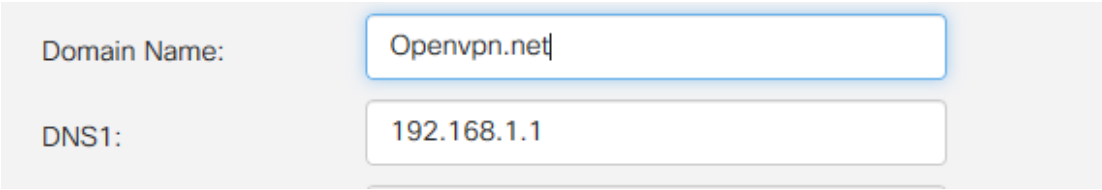
Tutte le dipendenze sono complete e il router può ora essere configurato per OpenVPN.

Passaggio 10. Passare a **VPN > OpenVPN**. Viene visualizzata la pagina OpenVPN. Completare ogni casella della pagina, assicurandosi di selezionare i certificati creati in precedenza dal menu a discesa.



- Selezionare la casella *Attiva*. Selezionare l'interfaccia che verrà consentita nel traffico. In questo caso, una rete WAN (Wide Area Network) e selezionare un certificato CA (Certification Authority).
- Selezionare il *certificato CA* dal menu a discesa
- Selezionare il certificato server scaricato dal menu a discesa
- Selezionare *Autenticazione client*. Se si seleziona Password, è necessario eseguire l'autenticazione con una password. Se si seleziona Password + Certificato, anche il client deve disporre di un certificato. Ciò è più sicuro, ma aumenta il costo della VPN in quanto dovrebbe acquistare una CA separata.
- Immettere il *pool di indirizzi client*. Scegliere un indirizzo IP in una subnet di rete che non venga utilizzato in altre posizioni della società. È possibile selezionare un intervallo tra quelli riservati e scegliere un intervallo non utilizzato altrove.
- Scegliere il tipo di *crittografia*. Assicurarsi che la crittografia sia la stessa del client. DES e 3DES non sono consigliati e devono essere utilizzati solo per compatibilità con le versioni precedenti.
- Scegliere Dividi tunnel se si desidera solo specificare il traffico che attraversa la VPN. Per una VPN, è necessario un tunnel suddiviso. La *modalità tunnel completo* è selezionata in altre situazioni quando si desidera che tutto il traffico client passi attraverso la VPN.

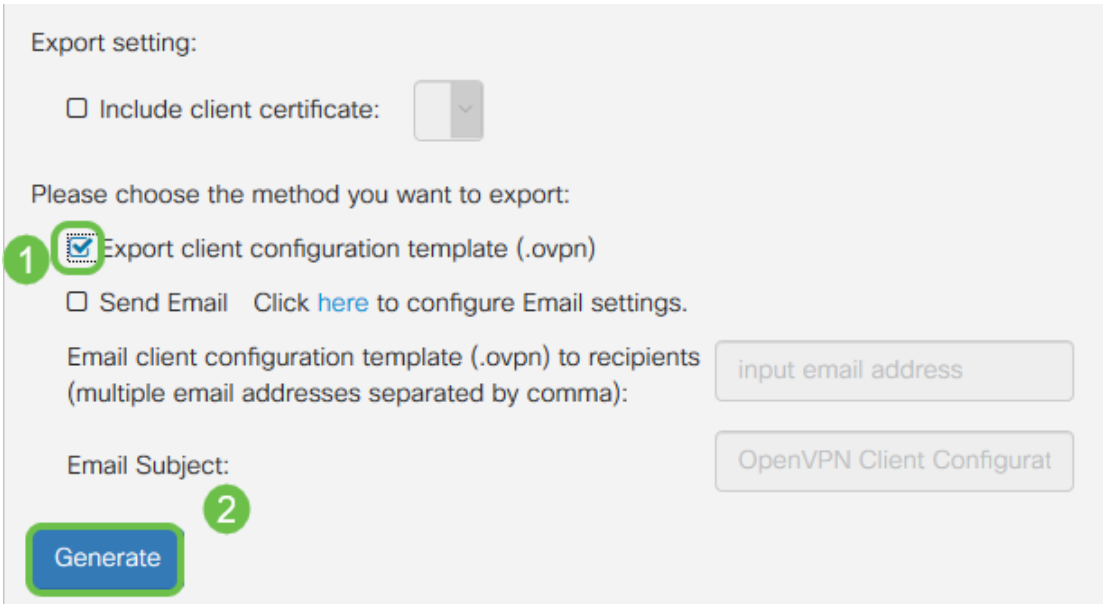
Passaggio 11. Scorrere la pagina verso il basso e compilare i campi *Domain Name* e *DNS1*.



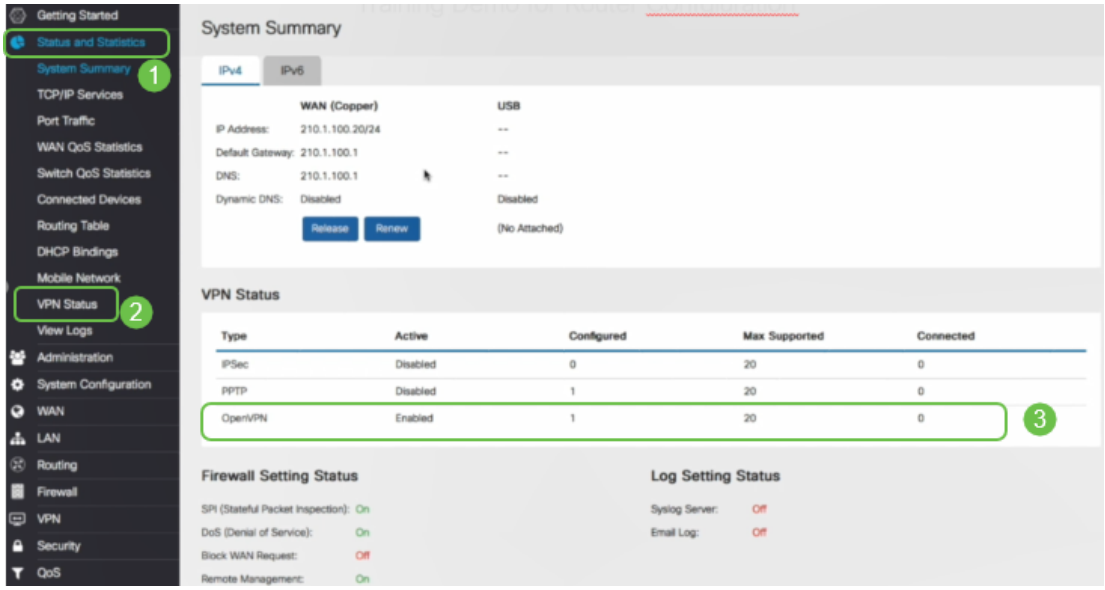
Nota: l'indirizzo IP DNS1 potrebbe essere un server DNS interno dedicato, lo stesso indirizzo IP del gateway predefinito fornito dal provider di servizi Internet (ISP), in una macchina virtuale o un server DNS trusted in Internet.

Passaggio 12. Fare clic su **Apply** per salvare la configurazione sul router.

Passaggio 13. Rimanere sulla stessa pagina e scorrere ulteriormente. Generare il modello di configurazione da installare sul client OpenVPN. Questo file ha estensione *.ovpn* e verrà utilizzato dal client OpenVPN. Selezionare la casella per *Esportare* il *modello di configurazione client (ovpn)* e fare clic su **Genera**. Il file verrà scaricato nel computer.



Passaggio 14. Passare a **Stato e statistiche** > **Stato VPN**. È possibile scorrere verso il basso per ottenere informazioni più dettagliate.



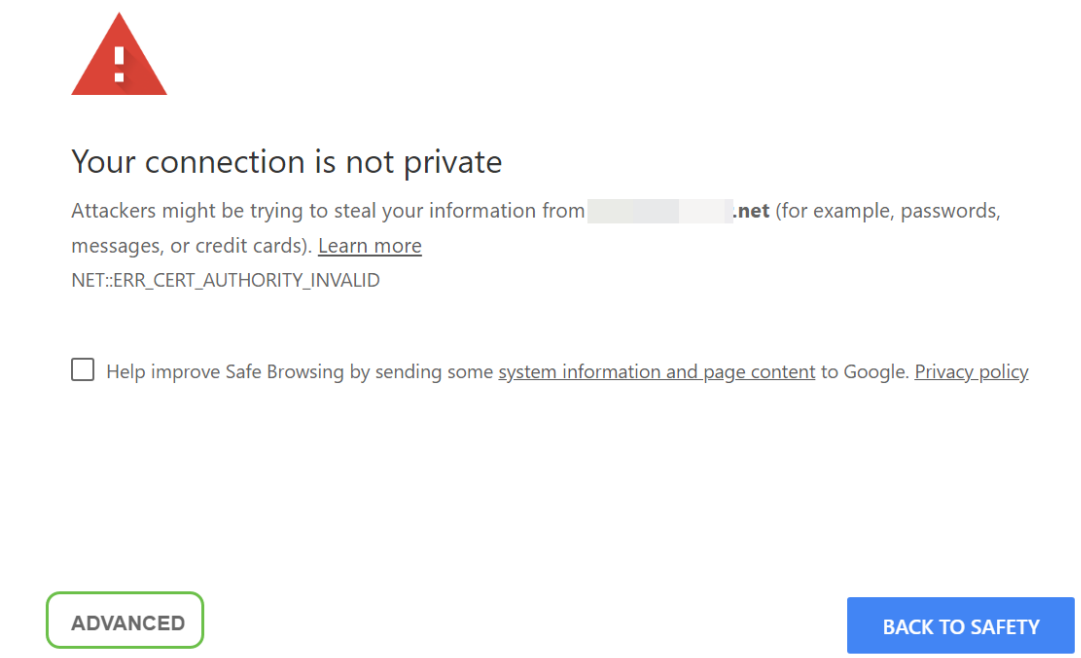
La sezione successiva di questo articolo è importante da rivedere, in quanto spiega come accedere con un certificato autofirmato.

Accesso con certificato autofirmato dopo la configurazione di Demo OpenVPN

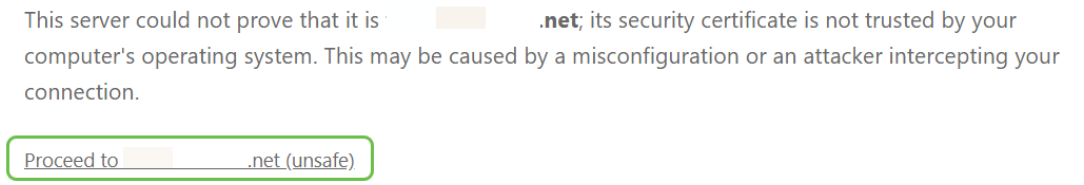
Quando si accede con un certificato autofirmato, è possibile che venga visualizzato un messaggio di avviso popup quando si tenta di eseguire l'accesso. Per continuare, è necessario fare clic su Avanzate, Procedi, Considera attendibile o su un'altra opzione a seconda del browser Web utilizzato.

A questo punto è possibile che venga visualizzato un messaggio di avviso per segnalare che non è sicuro. È possibile scegliere di continuare, aggiungere un'eccezione o avanzate. Questo può variare a seconda del browser.

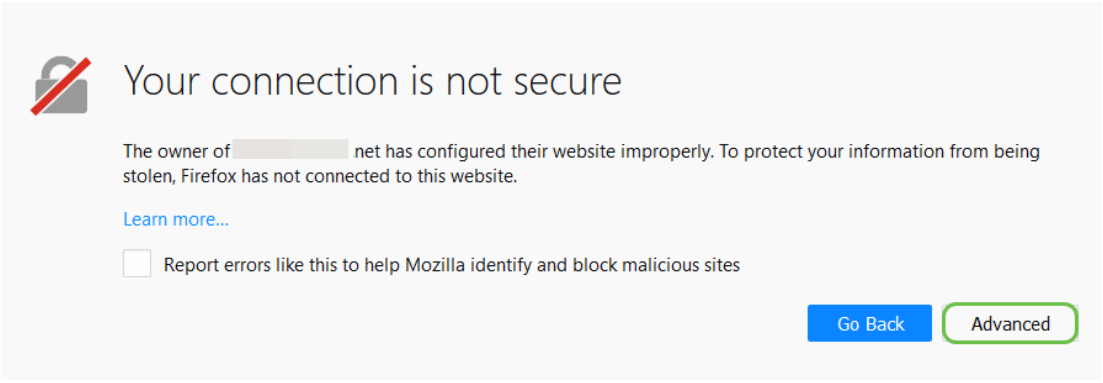
In questo esempio, Chrome è stato utilizzato per un browser Web. Viene visualizzato questo messaggio. Fare clic su **Avanzate**.



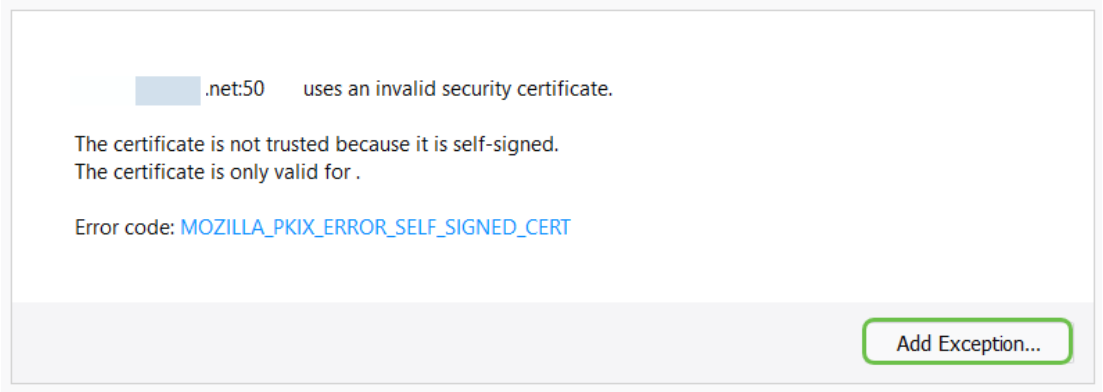
Verrà visualizzata una nuova schermata e sarà necessario fare clic su **Procedi a yourwebsite.net (unsafe)**



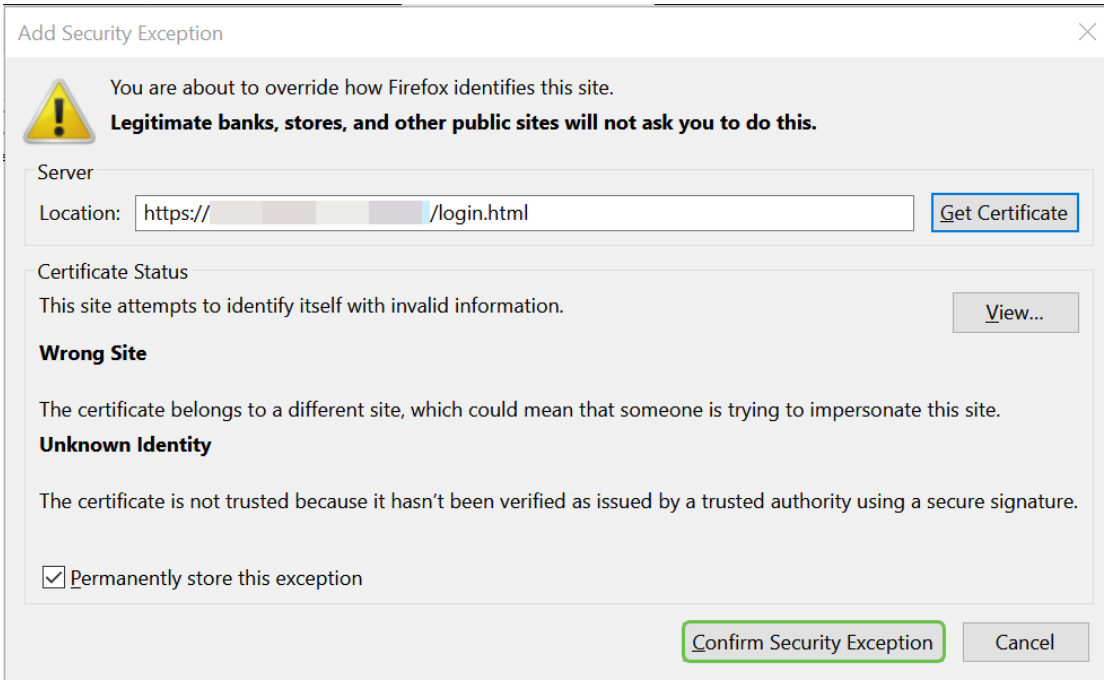
Di seguito è riportato un esempio di accesso all'avviso del dispositivo quando si utilizza Firefox come browser Web. Fare clic su **Advanced** (Avanzate).



Fare clic su **Aggiungi eccezione....**



Infine, fare clic su **Conferma eccezione di protezione.**



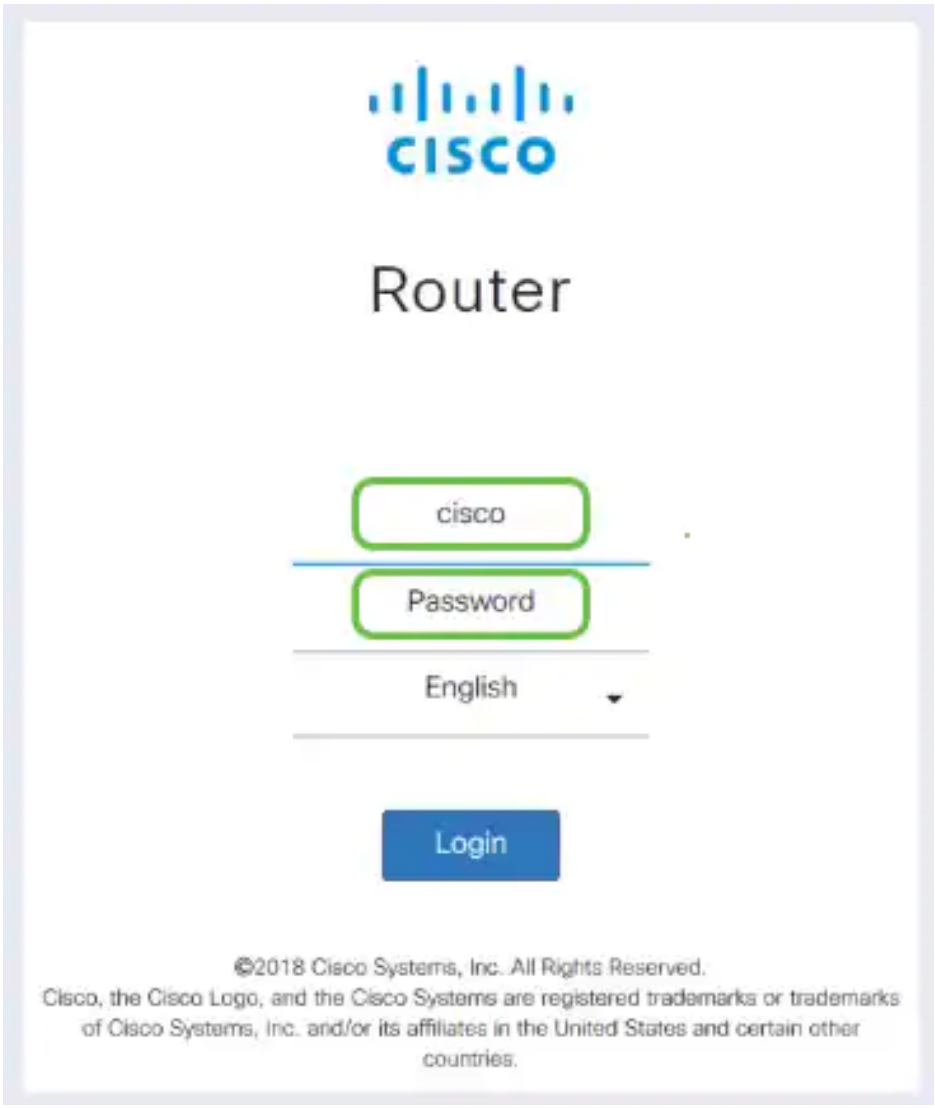
Il router è ora configurato con tutti i parametri necessari per supportare una connessione client OpenVPN. Poiché il modello di configurazione client è già stato scaricato nel dispositivo, quello che termina con *.ovpn*, è possibile passare alla sezione Installazione client OpenVPN nel computer. Se si decide di distribuire OpenVPN per la propria azienda, è possibile seguire i passaggi descritti in questa sezione successiva.

Configurazione di OpenVPN su un router RV160/RV260

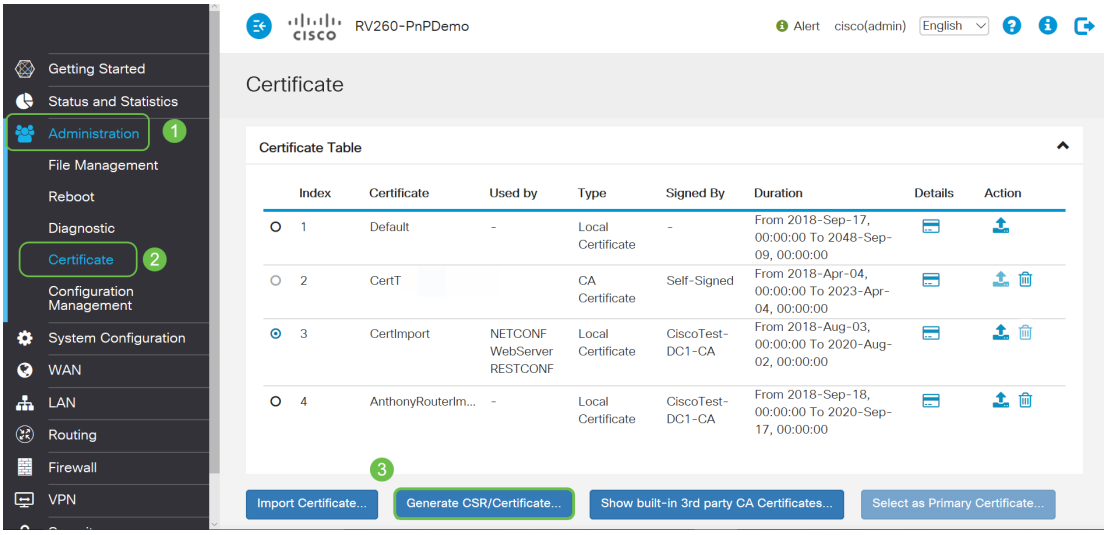
Si tratta di un processo più complicato in quanto comporta l'ottenimento di un'autorizzazione da parte di terzi, che comporta costi elevati. È inoltre necessario inviare il modello di configurazione del client VPN, che termina con *.ovpn*, a tutti i client in modo che possano eseguire la configurazione nel dispositivo. Affinché i client possano comunicare, hanno bisogno di diverse impostazioni uguali a quelle del router. La parte migliore è che, a un costo minimo, tu e i tuoi dipendenti potete usare Internet e condurre gli affari in modo più sicuro.

Passaggio 1. Accedere al router utilizzando le credenziali. Il nome utente e la password predefiniti sono *cisco*.

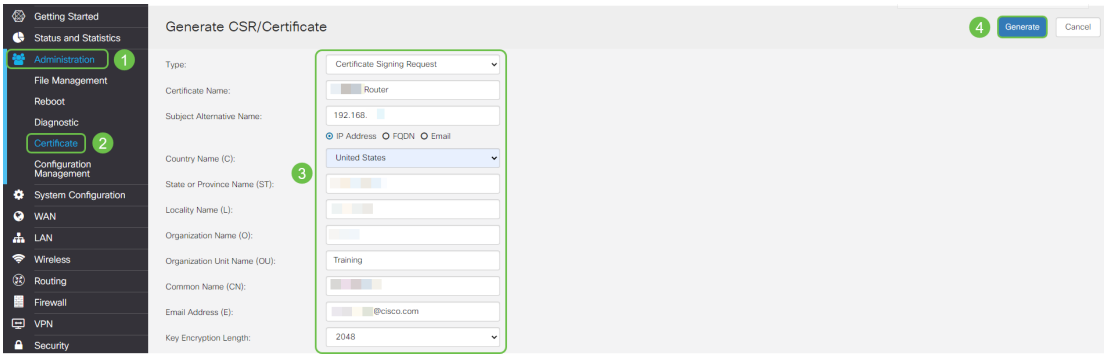
Nota: Si consiglia di modificare tutte le password in modo da renderle più complesse. Altrimenti, è come lasciare la chiave alla porta chiusa a chiave sulla soglia.



Passaggio 2. È necessario ottenere un certificato. Passare a **Amministrazione > Certificato > Genera CSR/Certificato...** In questo modo viene creata la richiesta di un certificato.



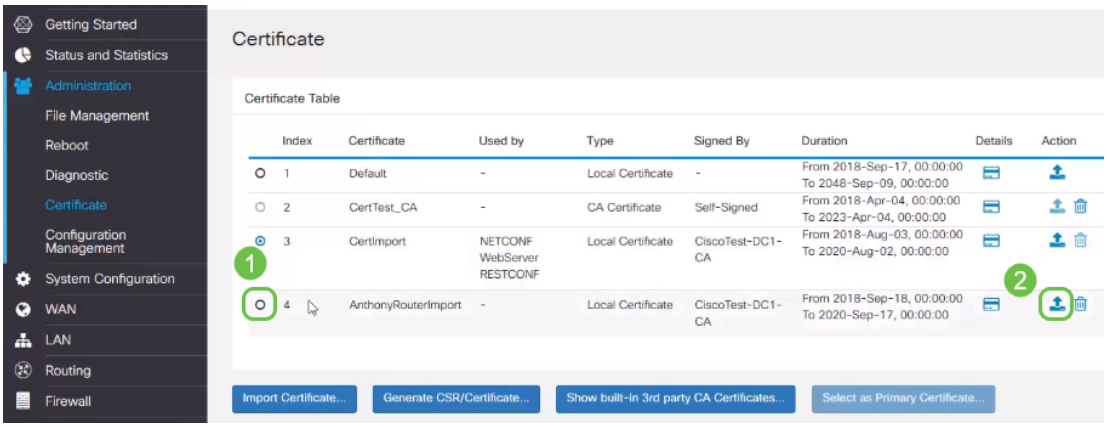
Passaggio 3. Richiedere un *certificato firmato da un certificato CA*. Per ulteriori informazioni, selezionare **Amministrazione > Certificato**.



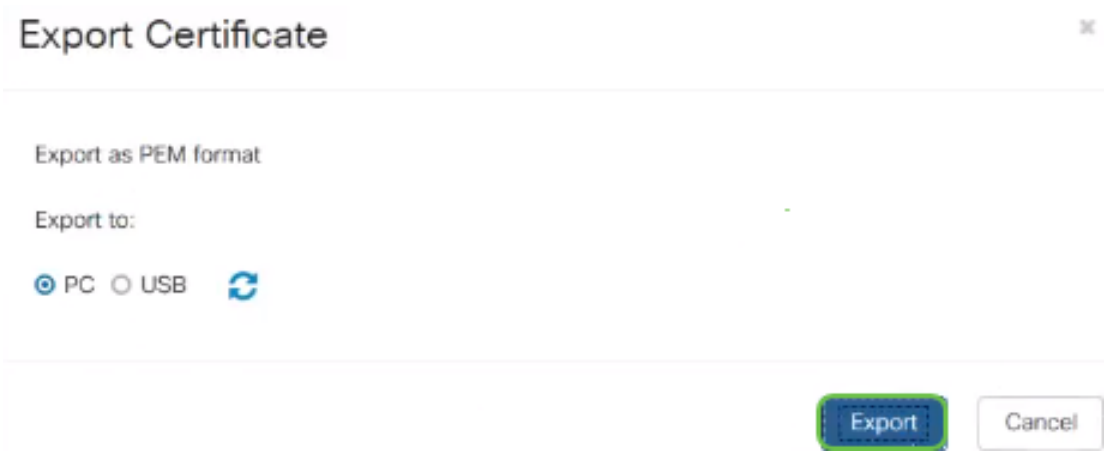
- Selezionare *Richiesta firma certificato* dal menu a discesa
- Immettere il nome di un certificato
- Immettere l'indirizzo IP, il nome di dominio completo (FQDN) o l'indirizzo di posta elettronica. L'immissione dell'indirizzo IP è la scelta più comune.
- Inserire il Paese
- Immettere lo stato
- Inserire il nome della località, in genere la città
- Inserire il nome dell'organizzazione
- Inserire il nome dell'unità organizzativa
- Immetti il tuo indirizzo e-mail
- Immettere la lunghezza di crittografia della chiave, si consiglia 2048

Fare clic sul pulsante **Genera in** alto a destra

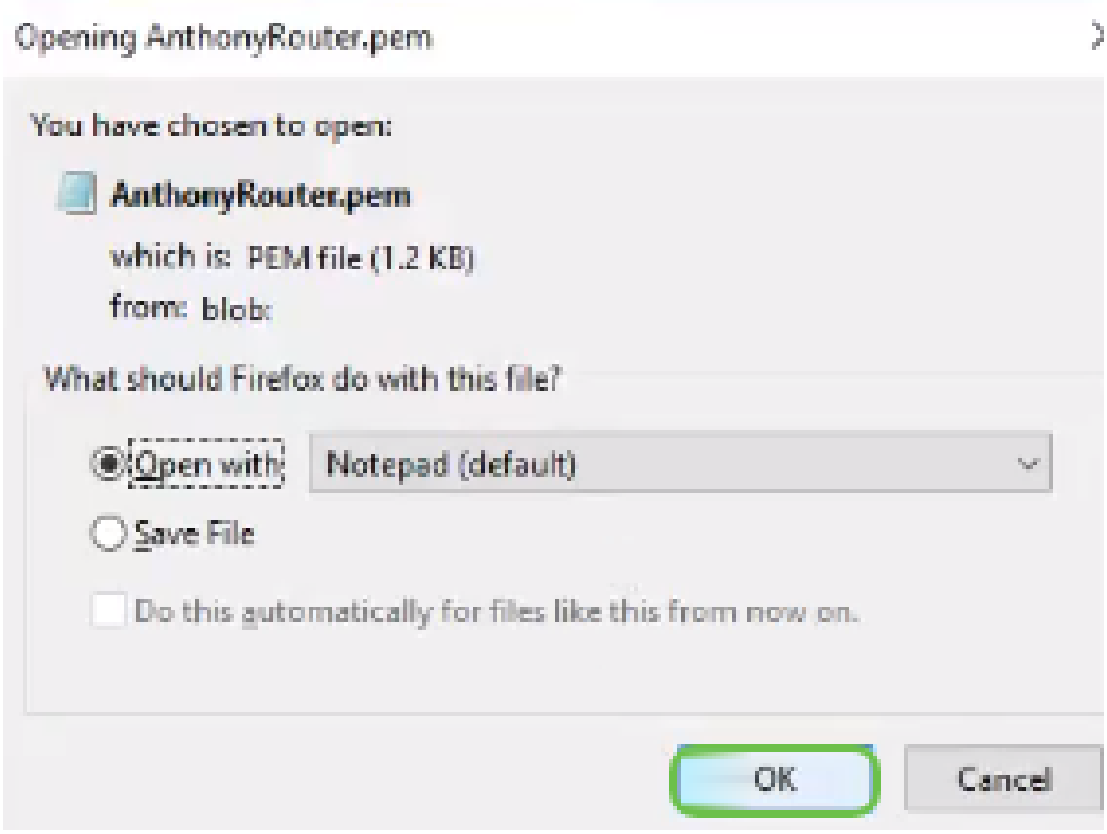
Passaggio 4. Selezionare Esporta facendo clic sulla freccia su in Azione.



Passaggio 5. Viene visualizzata questa schermata. Fare clic su **Esporta**.



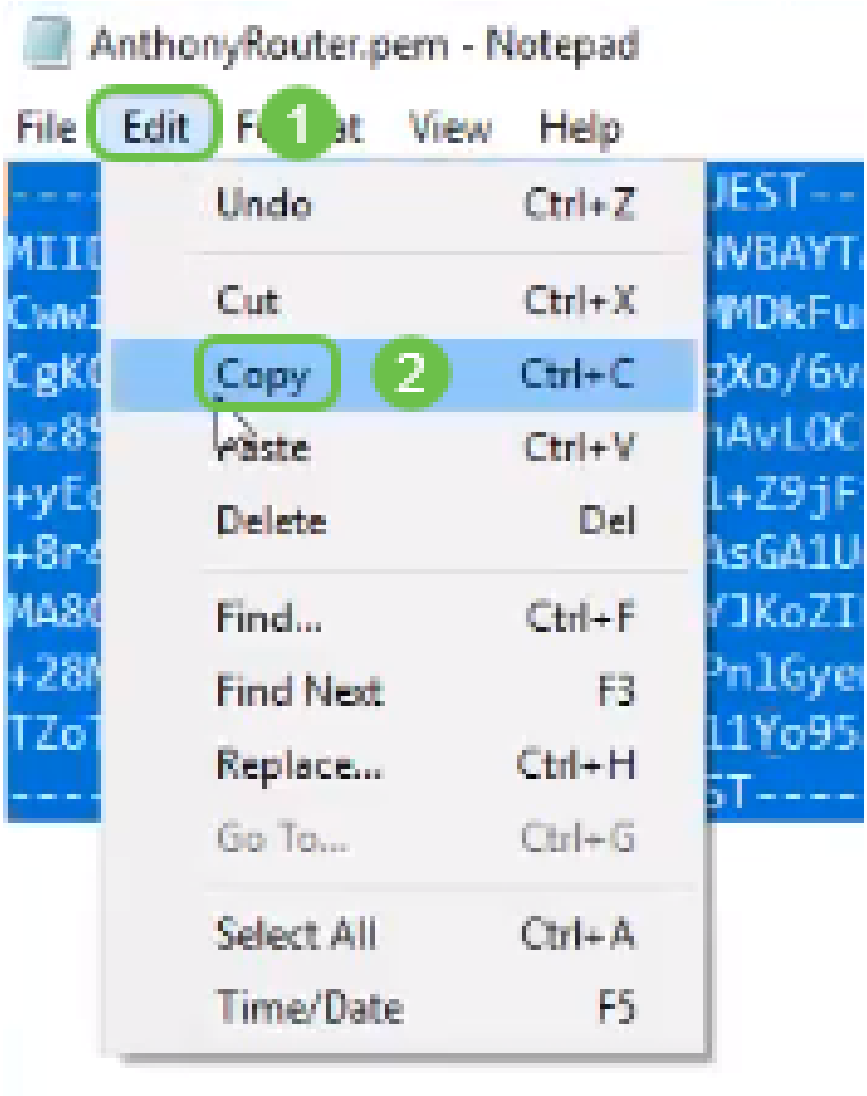
Passaggio 6. Selezionare *Apri con e Blocco note* (impostazione predefinita) dal menu a discesa. Fare clic su **OK**.



Passaggio 7. Verrà aperto un file XML.

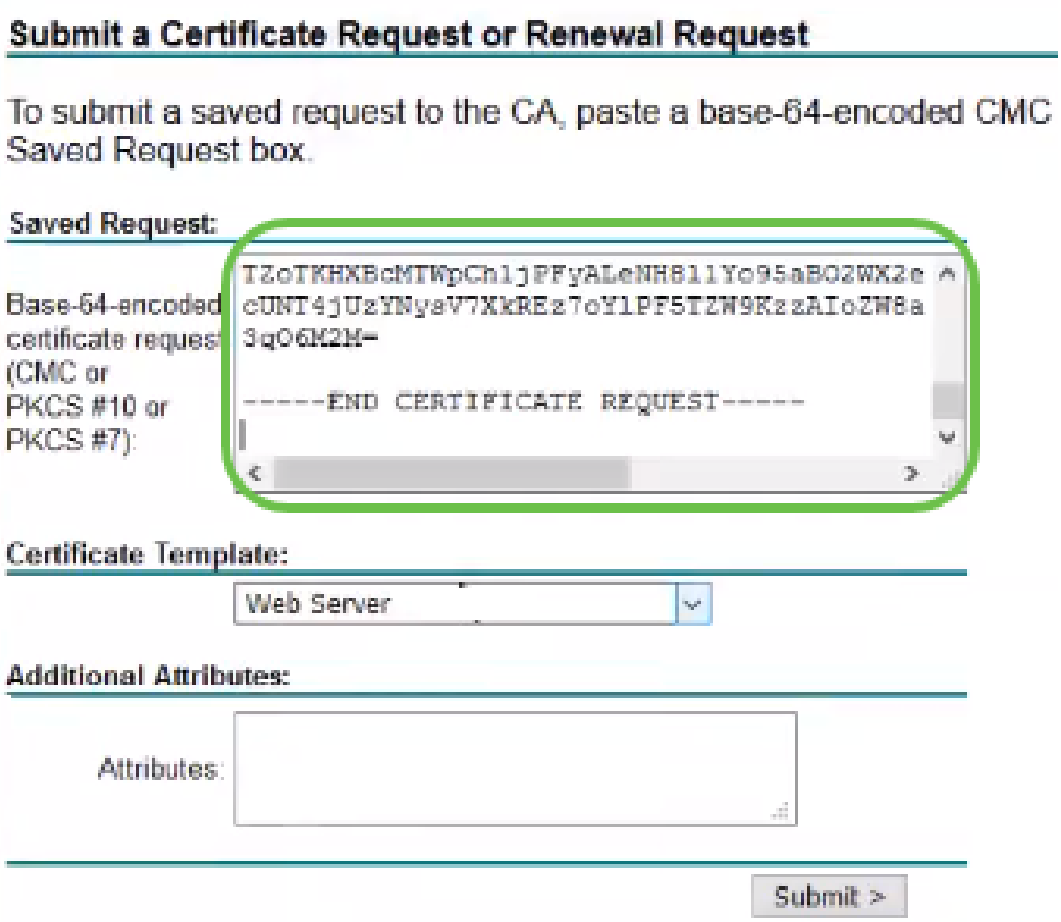
Nota: Assicurarsi che le righe BEGIN CERTIFICATE REQUEST e END CERTIFICATE REQUEST siano separate, come illustrato sopra.

Passaggio 8. Nella parte superiore dello schermo, fare clic su **Modifica** e selezionare **Copia** dal menu a discesa.

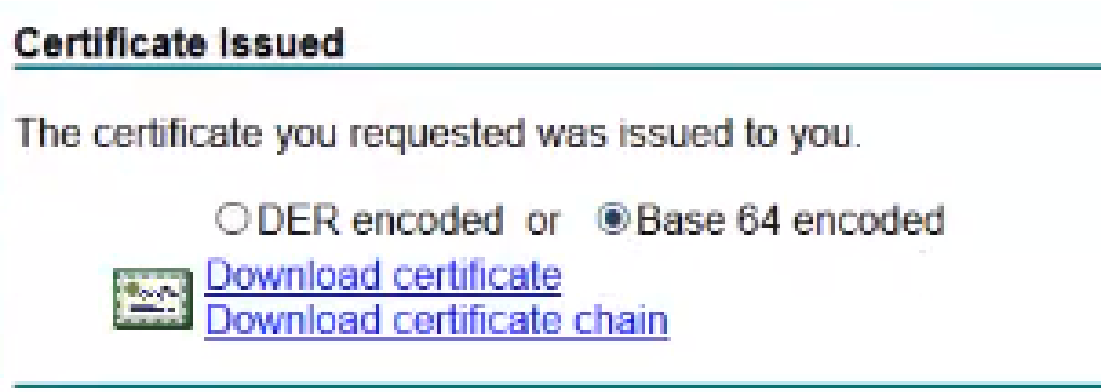


Passaggio 9. Scegliere una sede di terze parti attendibile per eseguire la richiesta di certificato. È necessario incollare il file XML copiato come parte della richiesta.

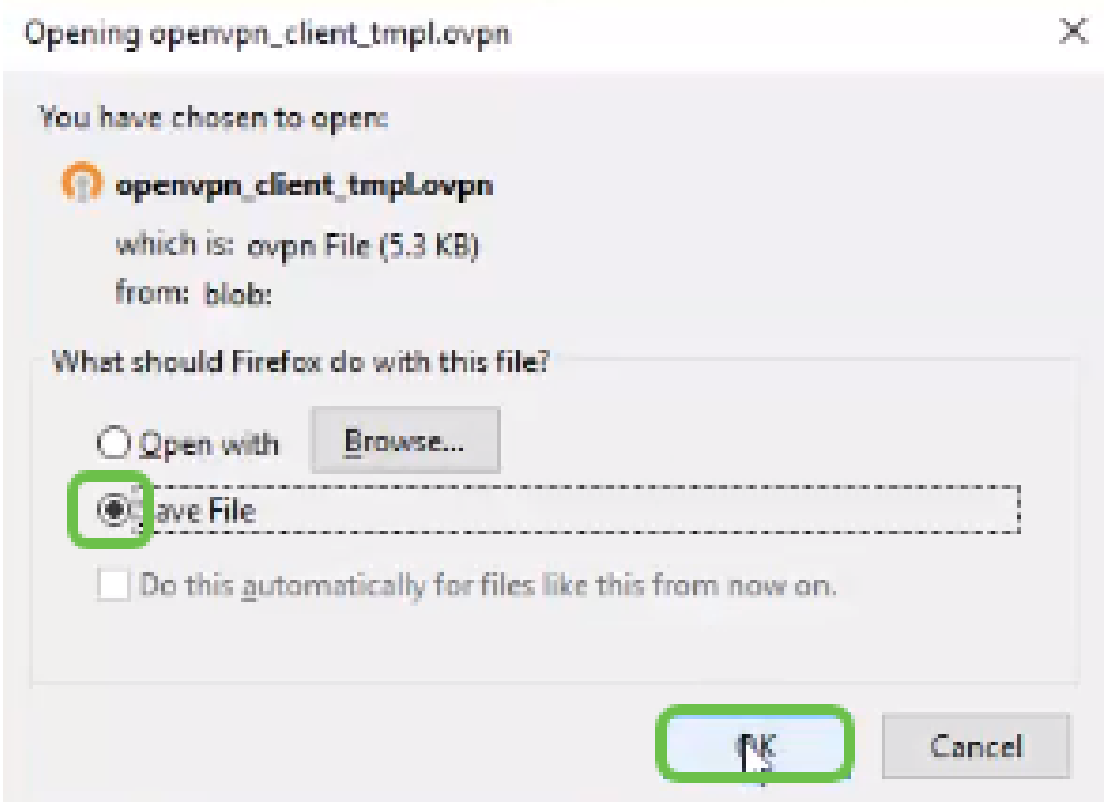
Nota: Se nella rete è presente un server di certificati interno, è possibile utilizzarlo in alternativa, anche se questa condizione non è comune.



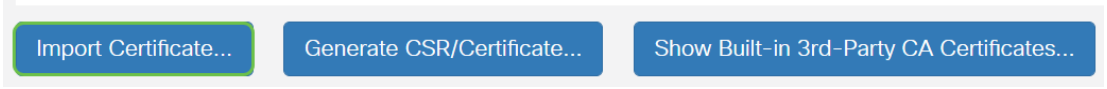
Passaggio 10. Dopo la verifica, è possibile scegliere *Scarica certificato*.



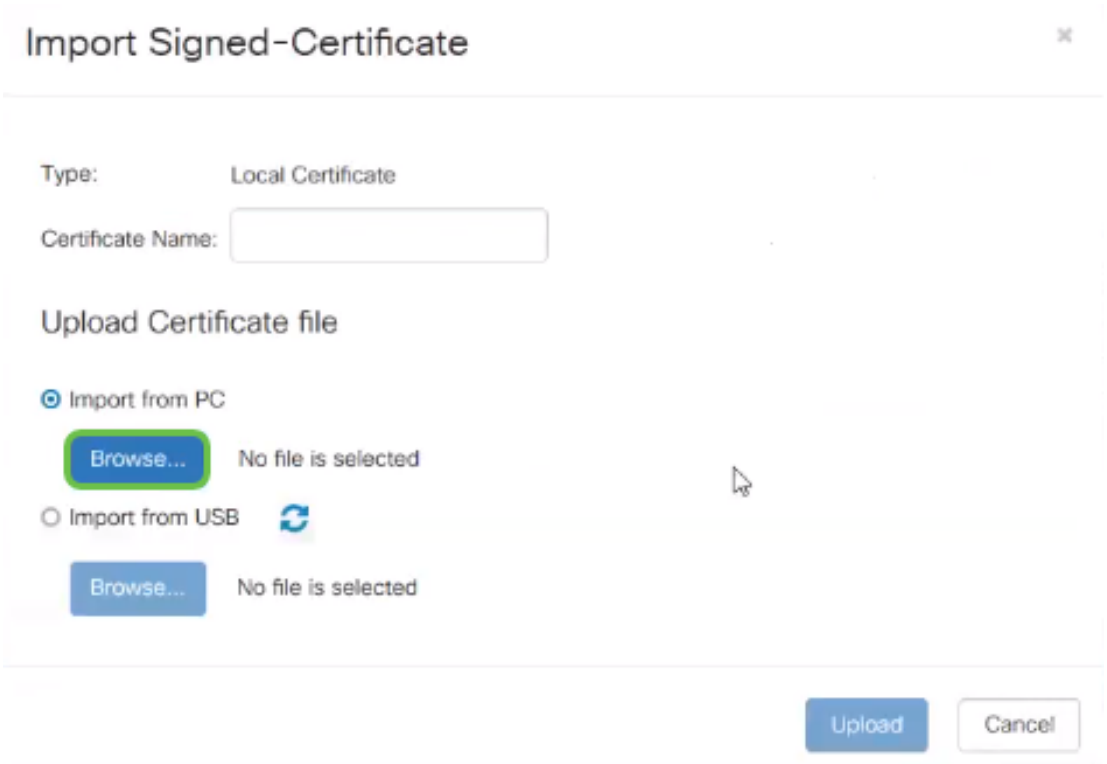
Passaggio 11. Fare clic sul pulsante di opzione per *salvare il file* e fare clic su **OK**.



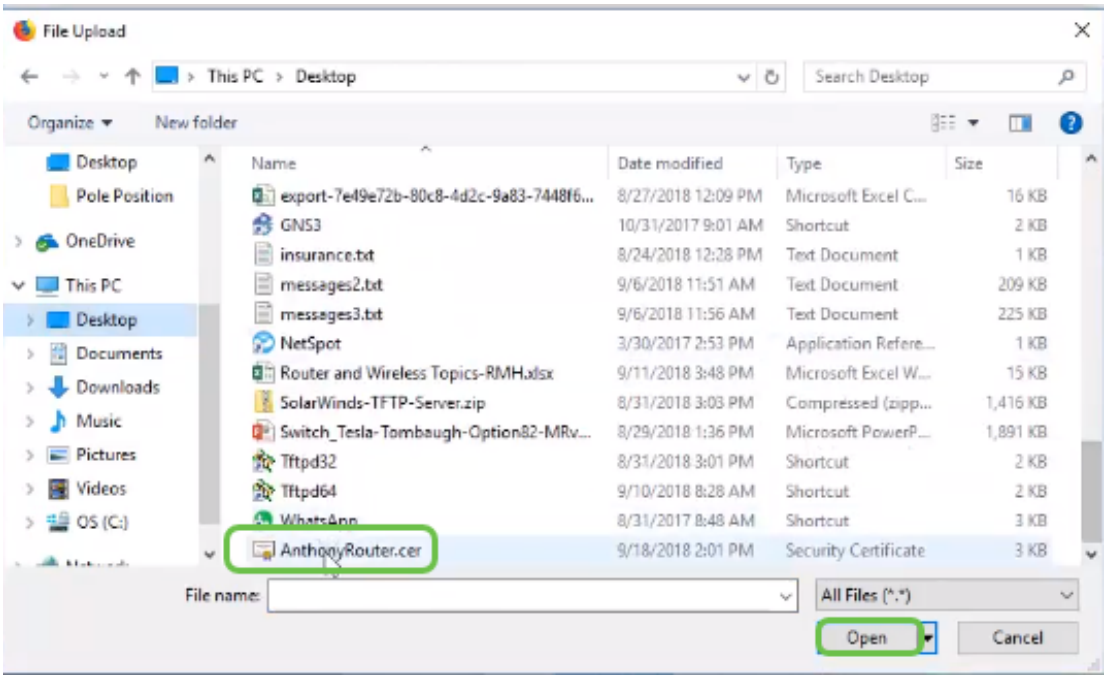
Passaggio 12. Una volta salvato, selezionare il pulsante di opzione per il certificato e fare clic sull'icona **freccia giù**.



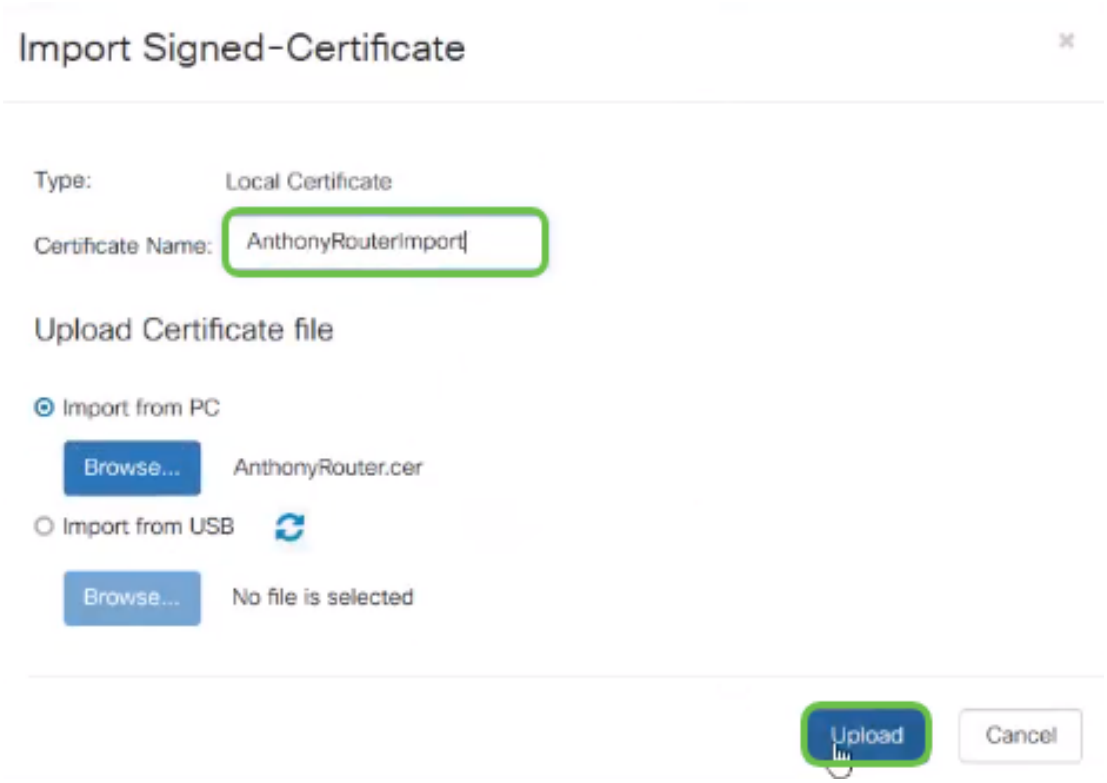
Passaggio 13. Verrà visualizzata questa schermata. Seleziona **Sfoglia....**



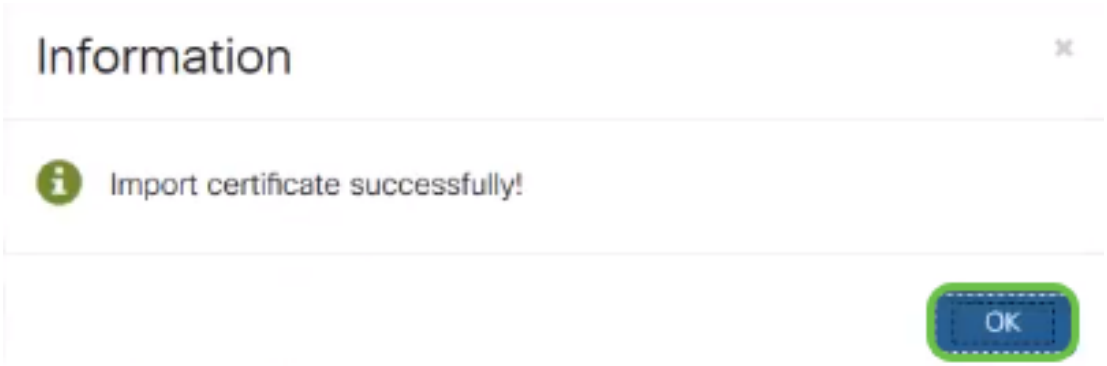
Passaggio 14. Scegliere il file del certificato e fare clic su **Apri**.



Passaggio 15. Immettere il *nome* del *certificato* da importare e fare clic su **Carica**.

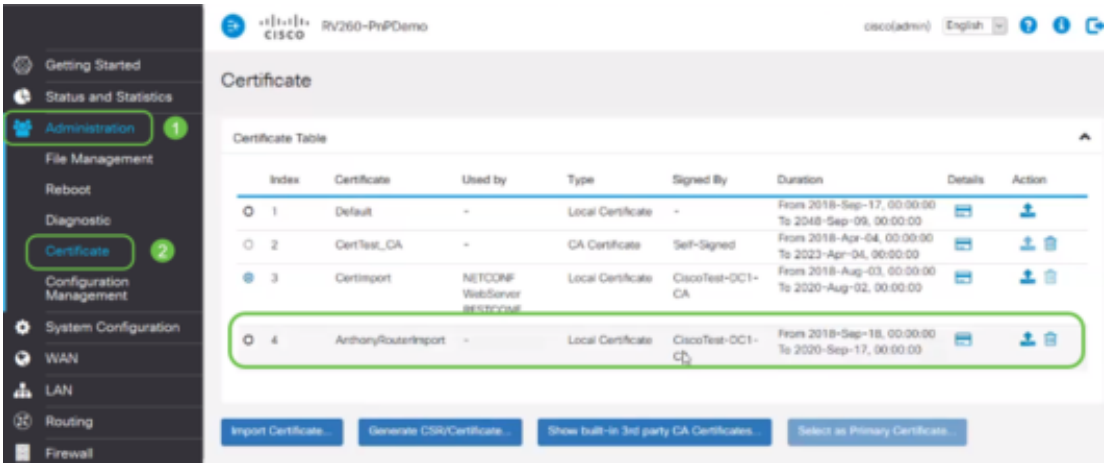


Passaggio 16. L'importazione del certificato verrà notificata. Fare clic su **OK**.

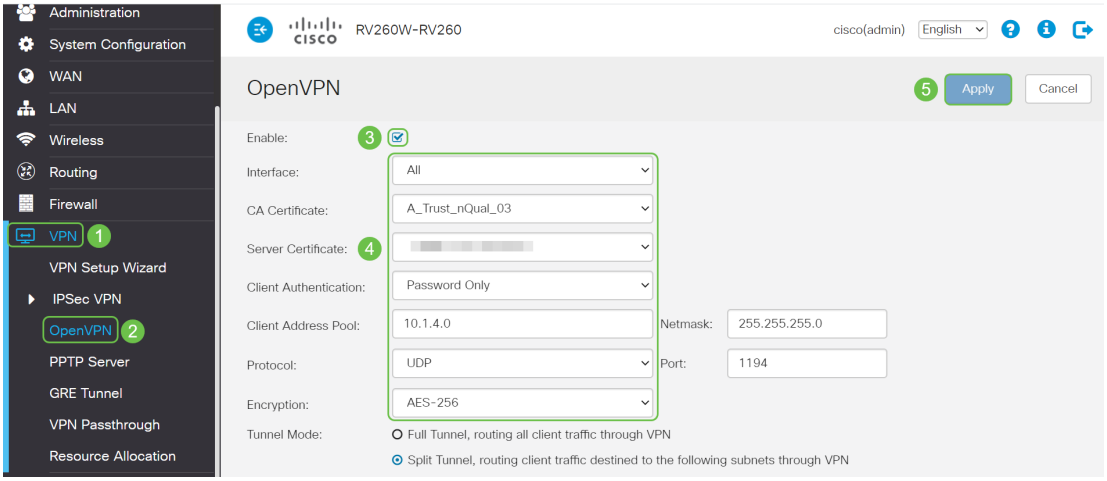


Passaggio 17. Passare a **Amministrazione > Certificato**. Il certificato è stato caricato.

Nota: In questo esempio è stato utilizzato un server dei certificati locale.



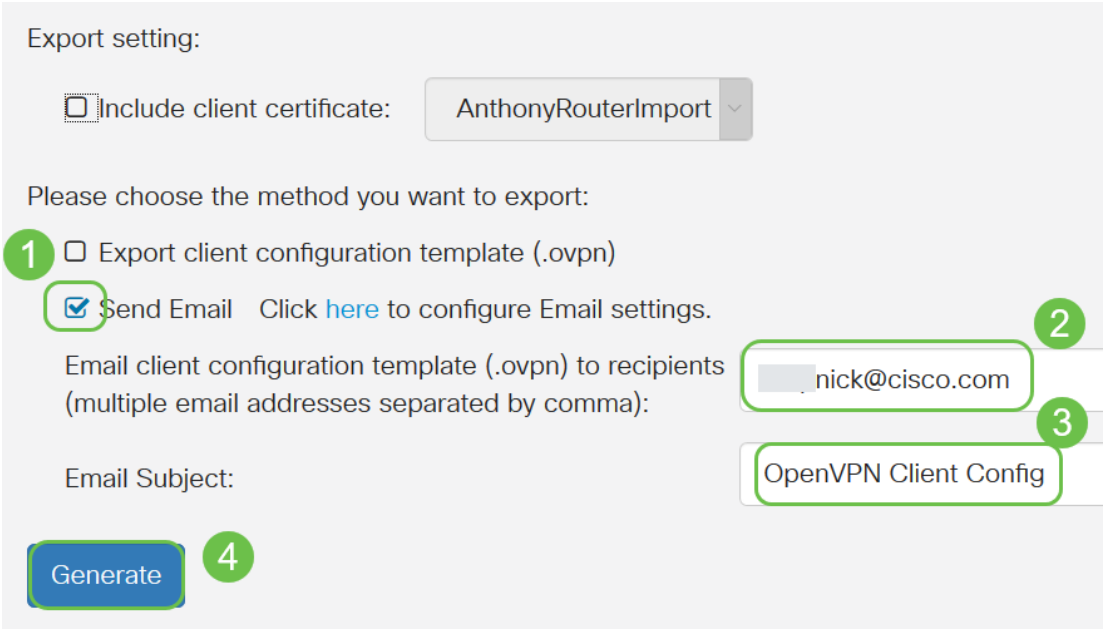
Passaggio 18. Passare a **VPN > OpenVPN**. Viene visualizzata la pagina OpenVPN. Completare le informazioni seguenti.



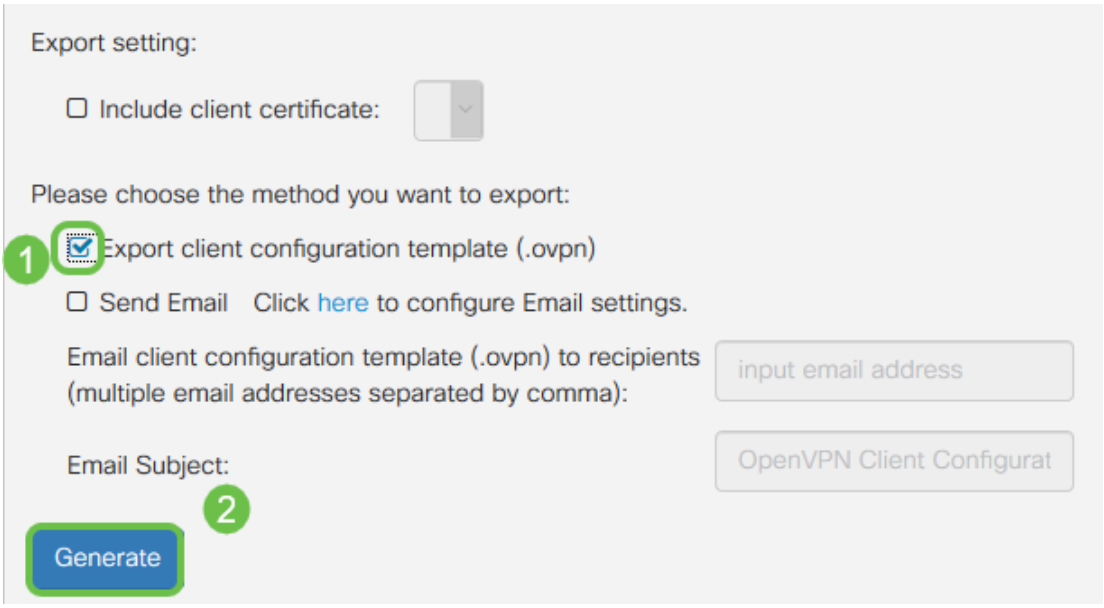
- Selezionare la casella *Attiva*. Selezionare l'interfaccia che verrà consentita nel traffico. In questo caso, una rete WAN (Wide Area Network) e selezionare un certificato CA (Certification Authority)
- Selezionare il *certificato CA* dal menu a discesa
- Selezionare il *certificato server* scaricato dal menu a discesa
- Selezionare *Autenticazione client*. Se si seleziona Password, è necessario eseguire l'autenticazione con una password. Se si seleziona Password + Certificato, anche il client deve disporre di un certificato. Ciò è più sicuro, ma aumenta il costo della VPN in quanto dovrebbe acquistare una CA separata.
- Immettere il *pool di indirizzi client*. Scegliere un indirizzo IP in una subnet di rete che non venga utilizzato in altre posizioni della società. È possibile selezionare un intervallo tra quelli riservati e scegliere un intervallo non utilizzato altrove.
- Scegliere il tipo di *crittografia*. Assicurarsi che la crittografia sia la stessa del client. DES e 3DES non sono consigliati e devono essere utilizzati solo per compatibilità con le versioni precedenti.
- Scegliere *Modalità tunnel completo* se si desidera che tutto il traffico del client passi attraverso la VPN o il tunnel diviso se si desidera solo specificare il traffico che attraversa la VPN
- L'indirizzo IP *DNS1* potrebbe essere un server DNS interno dedicato, lo stesso indirizzo IP del gateway predefinito fornito dal provider di servizi Internet (ISP), in una macchina virtuale o un server DNS trusted in Internet.

Fare clic su **Apply** (Applica) per salvare la configurazione.

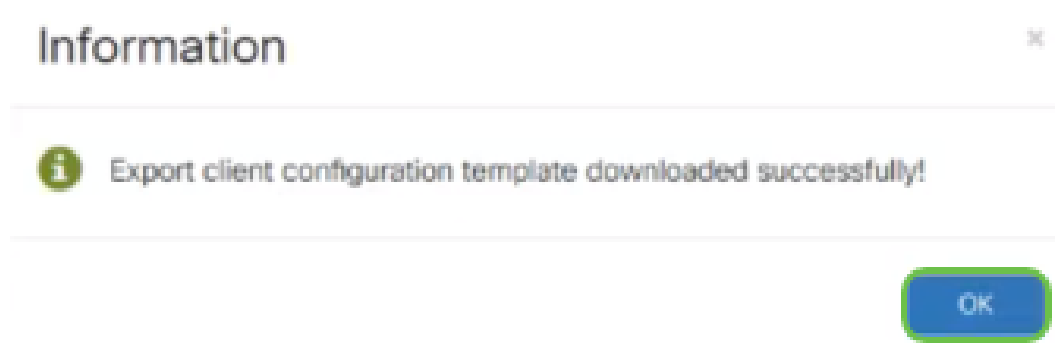
Passaggio 19 (opzione 1). È possibile inviare questa configurazione per e-mail al client. Selezionare la casella *Send Email*. Immettere un indirizzo di posta elettronica. Aggiungere un titolo Oggetto per l'e-mail. Fare clic su **Genera**.



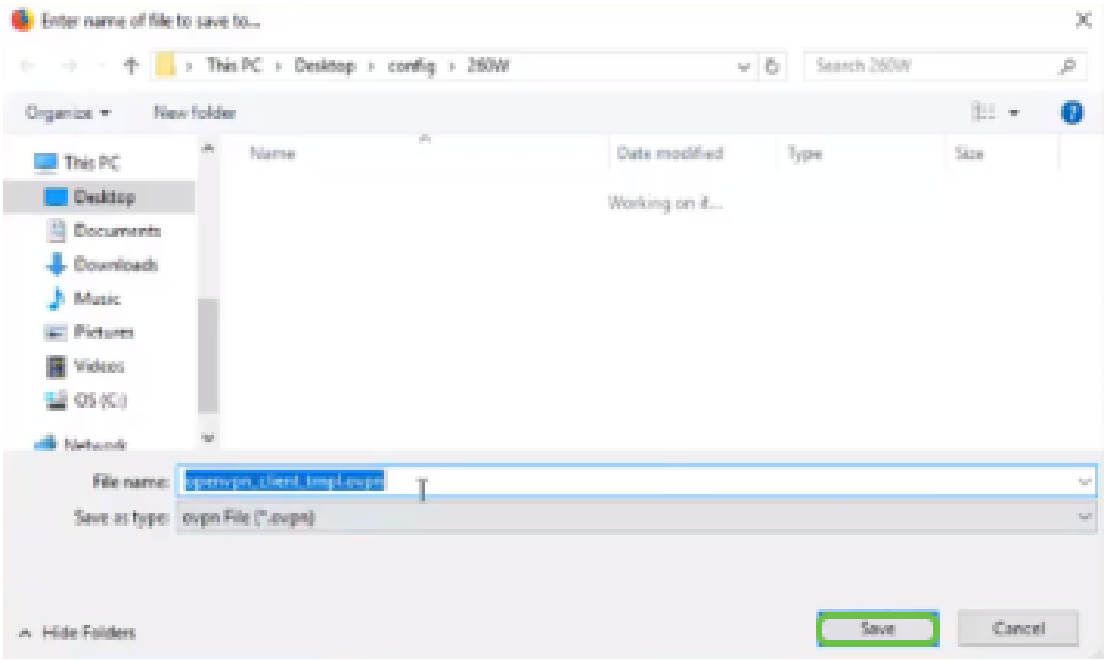
Passaggio 20. (Opzione 2). Selezionare *Esporta modello di configurazione client (.ovpn)* e fare clic su **Genera**.



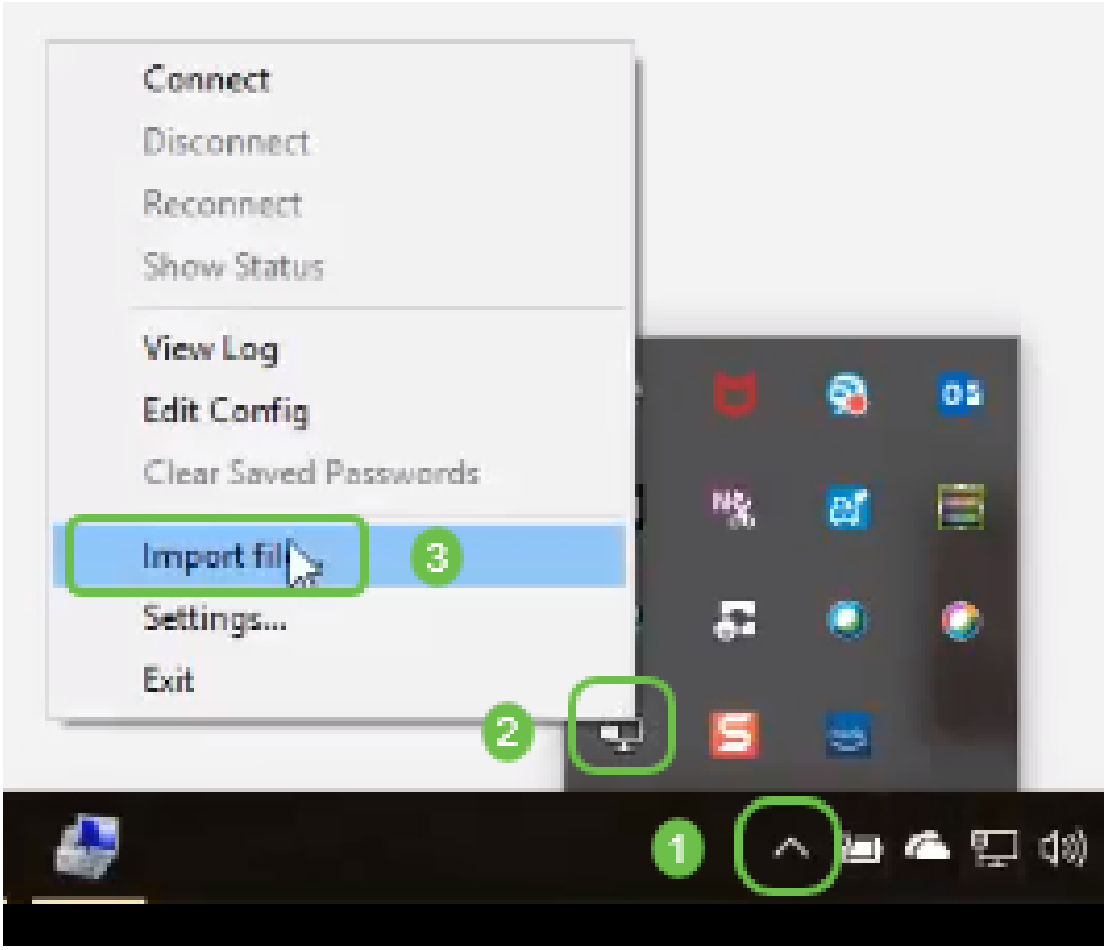
Passaggio 21. Si riceverà conferma dell'esito positivo. Fare clic su **OK**.



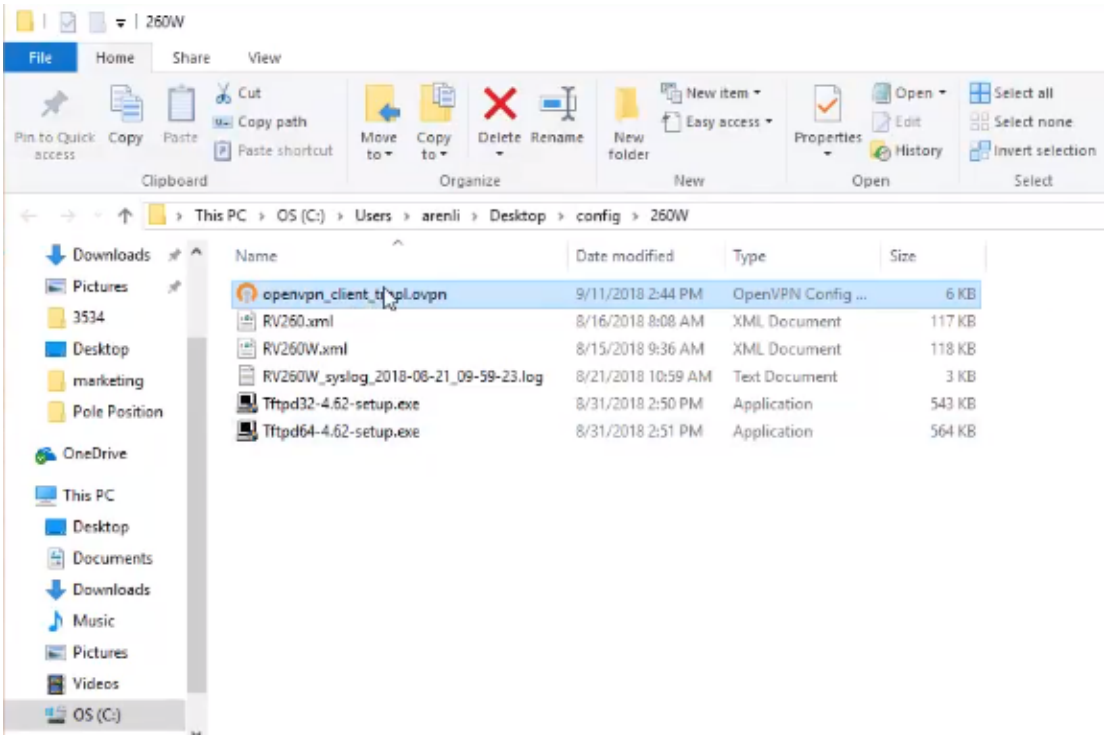
Passaggio 2. Fare clic su **Salva**.



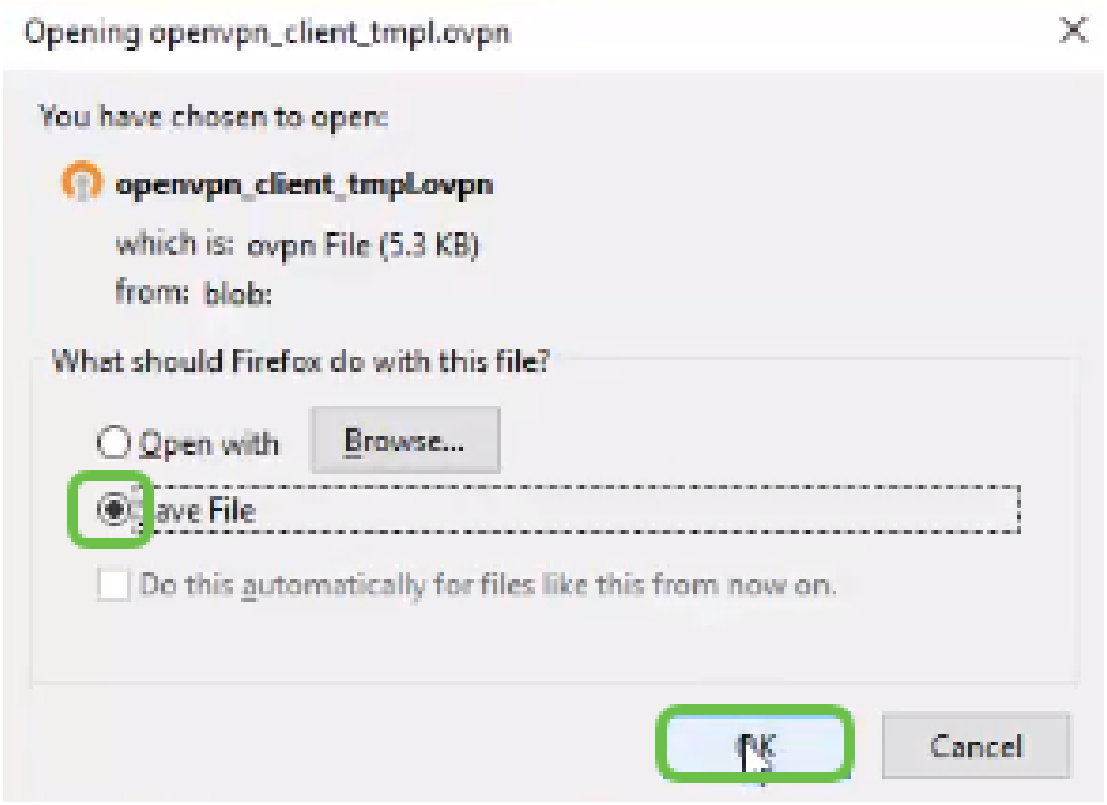
Passaggio 23. Nella parte inferiore destra del desktop e fare clic per aprire OpenVPN. Fare clic con il pulsante destro del mouse per aprire il menu a discesa. Fare clic su *Importa file*.



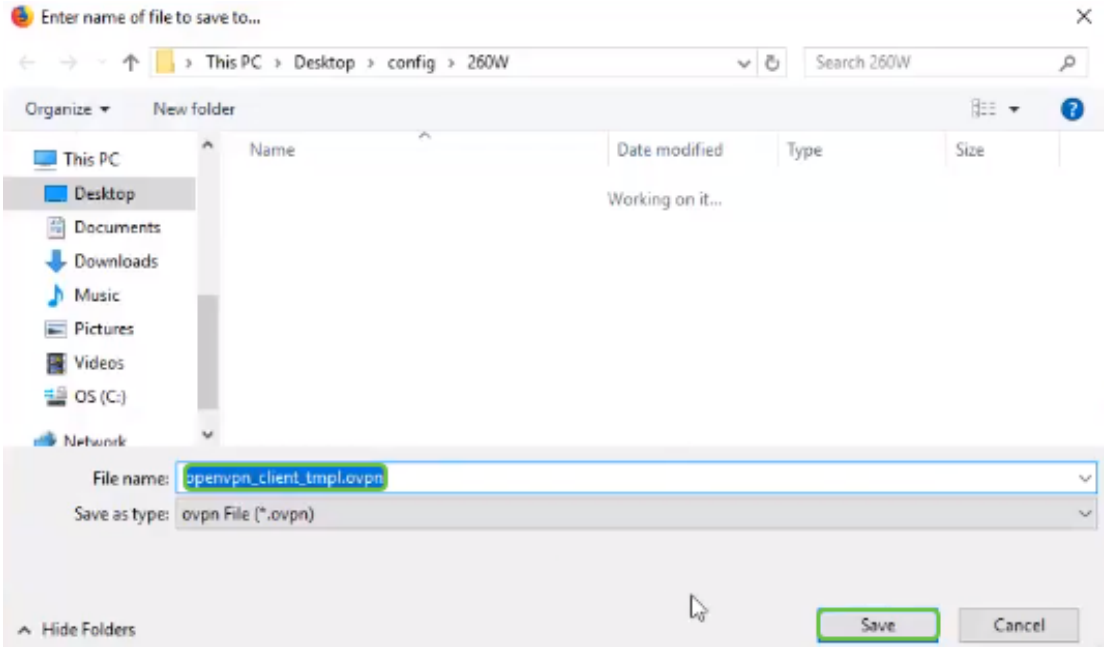
Passaggio 24. Selezionare il file OpenVPN che termina con *.ovpn*.



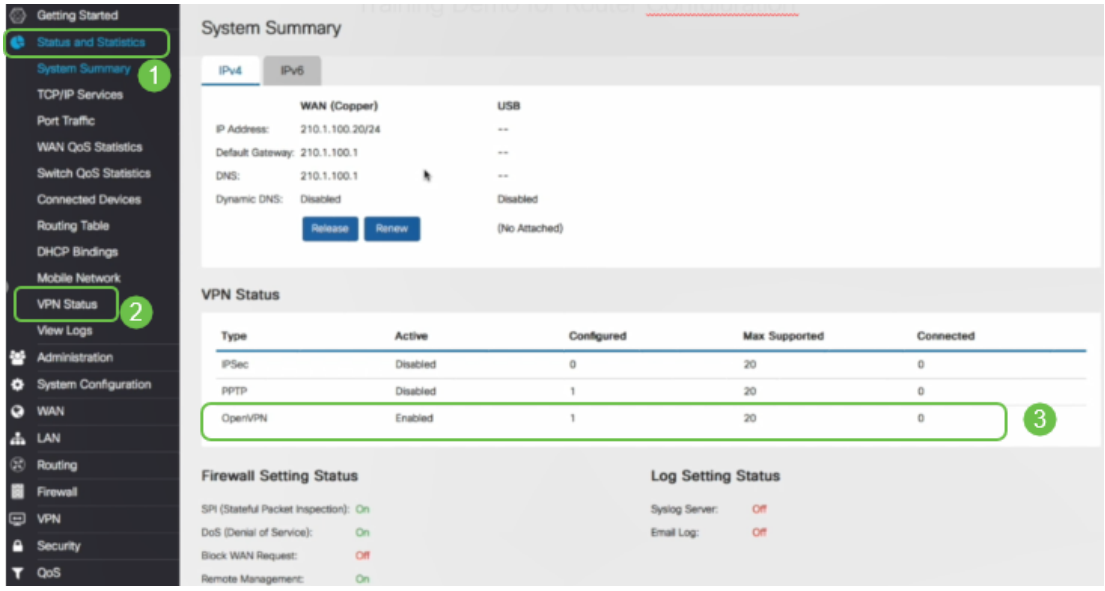
Passaggio 25. Fare clic sul pulsante di opzione *Salva file* e fare clic su **OK**.



Passaggio 26. Se si sceglie di modificare il nome del file, lasciare *.ovpn* alla fine del nome del file. Fare clic su **Salva**.



Passaggio 27. Passare a **Stato e statistiche > Stato VPN**. È possibile scorrere verso il basso per ottenere informazioni più dettagliate.



Il router è ora configurato con tutti i parametri necessari per supportare una connessione client OpenVPN per la versione di valutazione personale.

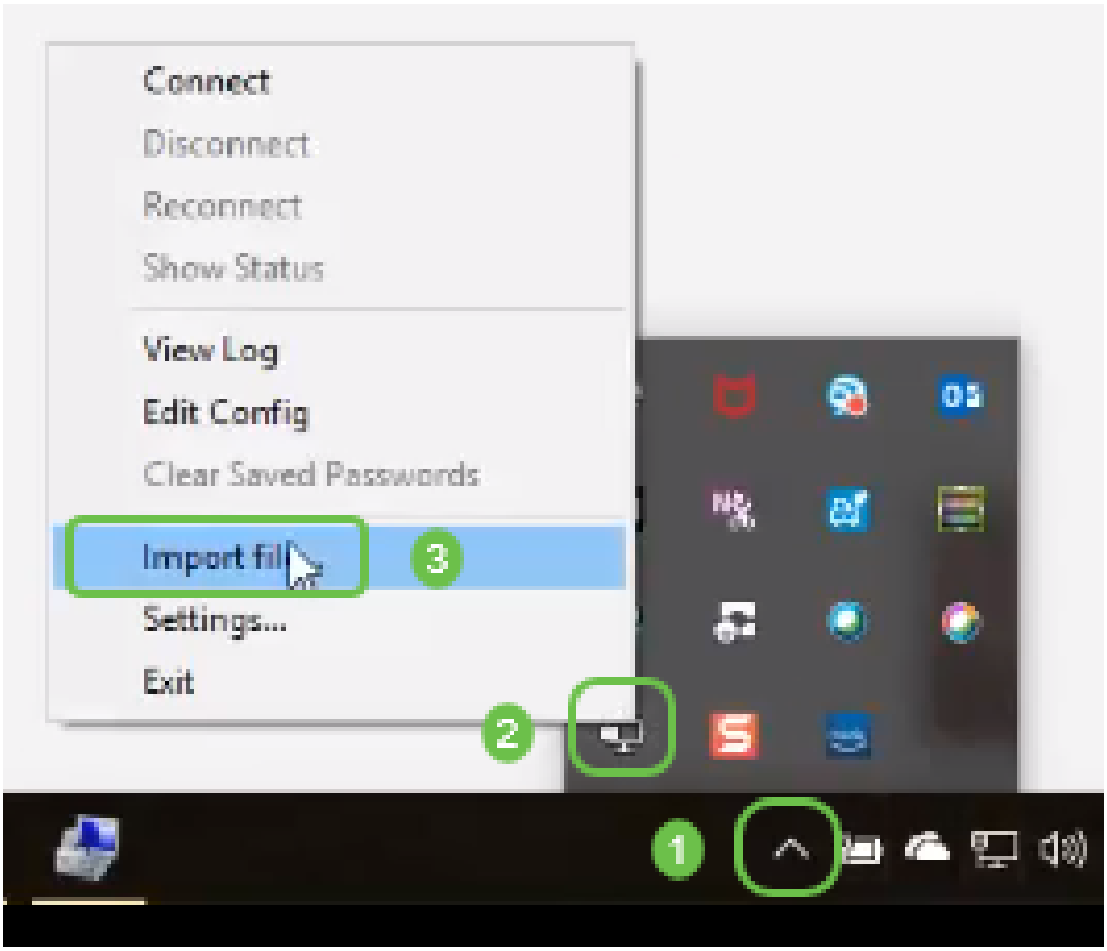
Installazione di OpenVPN Client sul computer

Ogni client OpenVPN deve eseguire le seguenti attività come prerequisito:

- Scaricare l'applicazione OpenVPN sul dispositivo.
- Aprire e salvare il file di configurazione inviato nei passaggi 19-22 della sezione precedente. Il file di configurazione termina in *.ovpn*.

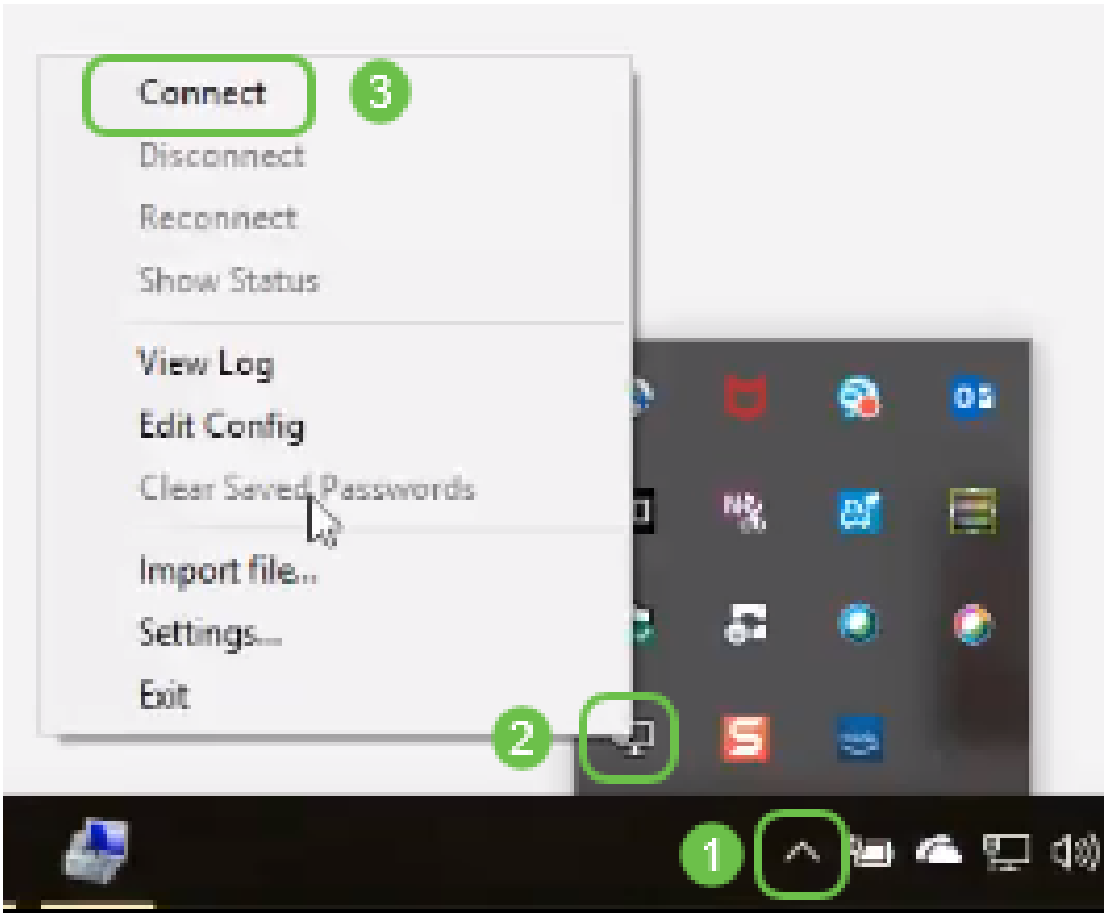
Nota: Questa installazione è specifica per Windows 10.

Passaggio 1. Passare all'icona a forma di freccia nella parte inferiore destra del desktop e fare clic per aprire l'icona OpenVPN. Fare clic con il pulsante destro del mouse e selezionare *Importa file*.

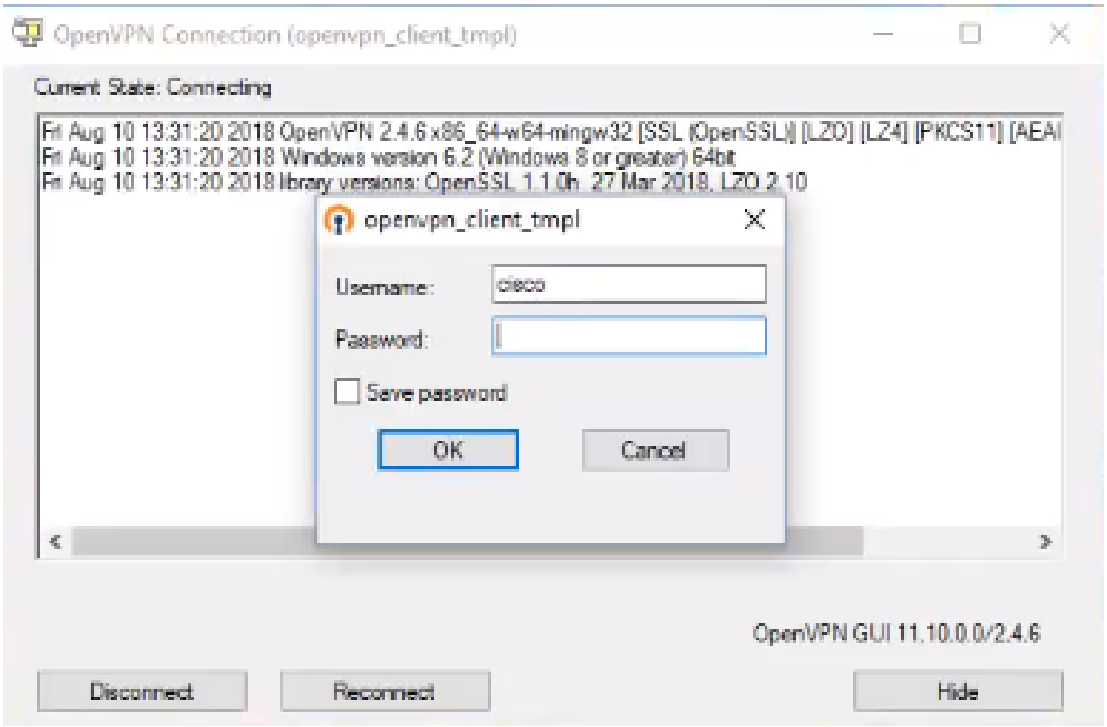


Nota: L'icona è in bianco e nero, a indicare che non è in esecuzione. Una volta eseguita, l'icona viene visualizzata a colori.

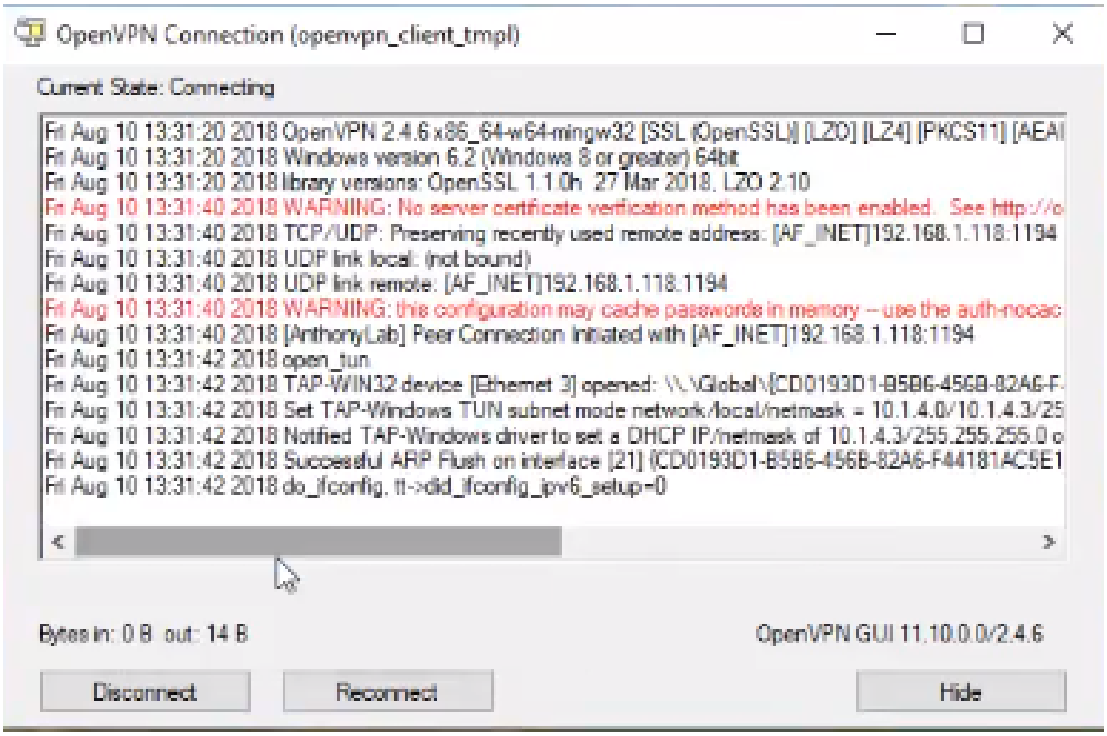
Passaggio 2. Fare clic sulla *freccia su*. Fare clic sull'icona OpenVPN. Fare clic con il pulsante destro del mouse e selezionare *Connetti* dal menu a discesa.



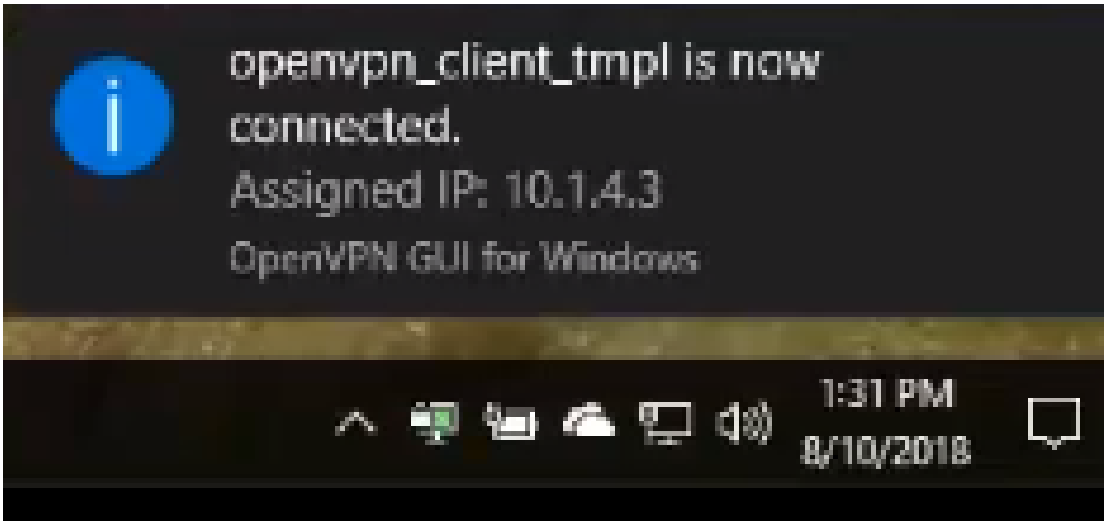
Passaggio 3. Inserire il *nome utente* e la *password*.



Passaggio 4. La finestra mostrerà la connessione OpenVPN con alcuni dati di log.

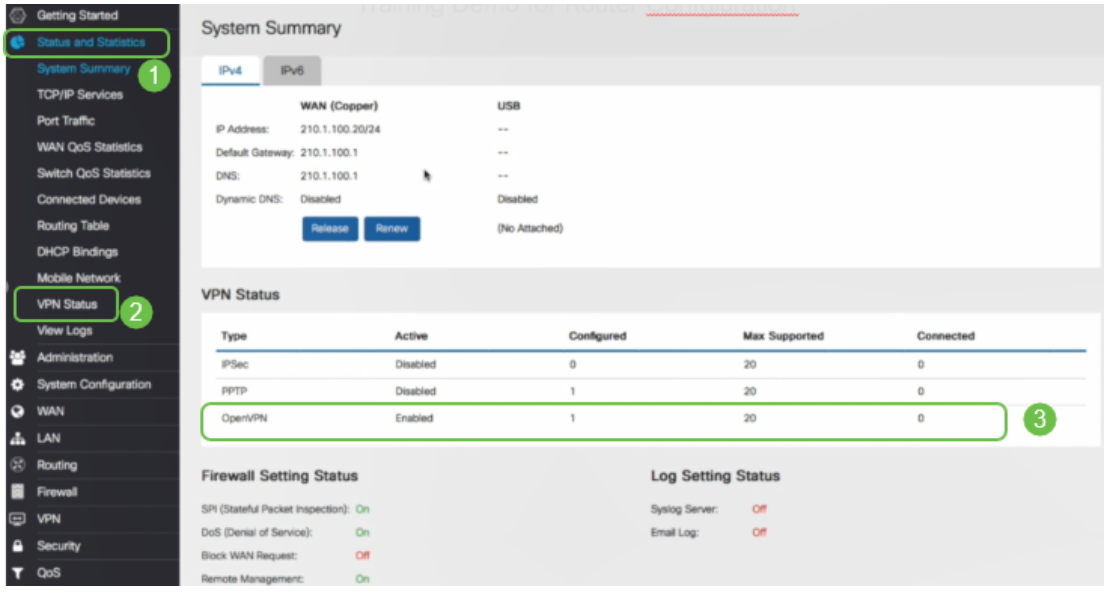


Passaggio 5. Un registro eventi di sistema deve segnalare che è presente una connessione.



Passaggio 6. Il client VPN deve essere in grado di eseguire il tunnel delle informazioni in entrata e in uscita tramite OpenVPN. È possibile impostare la connessione automatica nelle impostazioni OpenVPN.

Passaggio 7. L'amministratore può confermare lo stato della VPN passando a **Stato e statistiche** > **Stato VPN** sul router.



Conclusioni

A questo punto, OpenVPN dovrebbe essere installato correttamente sul router RV160 o RV260 e sul sito del client VPN.

Per le discussioni della community su OpenVPN, fare clic qui ed eseguire una ricerca di OpenVPN.

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco