OpenVPN auf einem RV160- und RV260-Router

Ziel

In diesem Artikel erfahren Sie, wie Sie OpenVPN auf Ihrem RV160- oder RV260-Router einrichten und OpenVPN-Clients auf Ihrem Computer einrichten.

Anwendbare Geräte

- RV160
- RV260

Softwareversion

- 1,0 00,15

Inhaltsverzeichnis

Einführung

OpenVPN ist eine kostenlose Open-Source-Anwendung, die für ein Virtual Private Network (VPN) eingerichtet und verwendet werden kann. Sie verwendet eine Client-Server-Verbindung, um eine sichere Kommunikation zwischen einem Server und einem Remote-Client-Standort über das Internet bereitzustellen.

OpenVPN verwendet OpenSSL für die Verschlüsselung von UDP und TCP für die Datenverkehrsübertragung. Ein VPN bietet einen sicheren Sicherheitstunnel, der weniger anfällig für Hacker ist, da er Daten verschlüsselt, die von Ihrem Computer über die VPN-Verbindung gesendet werden. Wenn Sie beispielsweise Wi-Fi an einem öffentlichen Ort, z. B. in einem Flughafen, verwenden, werden Ihre Daten, Transaktionen und Abfragen nicht von anderen Benutzern erkannt. Ähnlich wie HTTPS verschlüsselt es Daten, die zwischen zwei Endpunkten gesendet werden.

Einer der wichtigsten Schritte bei der Einrichtung von OpenVPN ist der Erhalt eines Zertifikats einer Zertifizierungsstelle (Certificate Authority, CA). Diese 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. Für OpenVPN benötigen Sie nur ein Zertifikat der unteren Ebene zu einem minimalen Preis. 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. Bitte beachten Sie, dass die Clients kein Zertifikat für die Verwendung von OpenVPN benötigen, sondern nur zur Verifizierung über den Router.

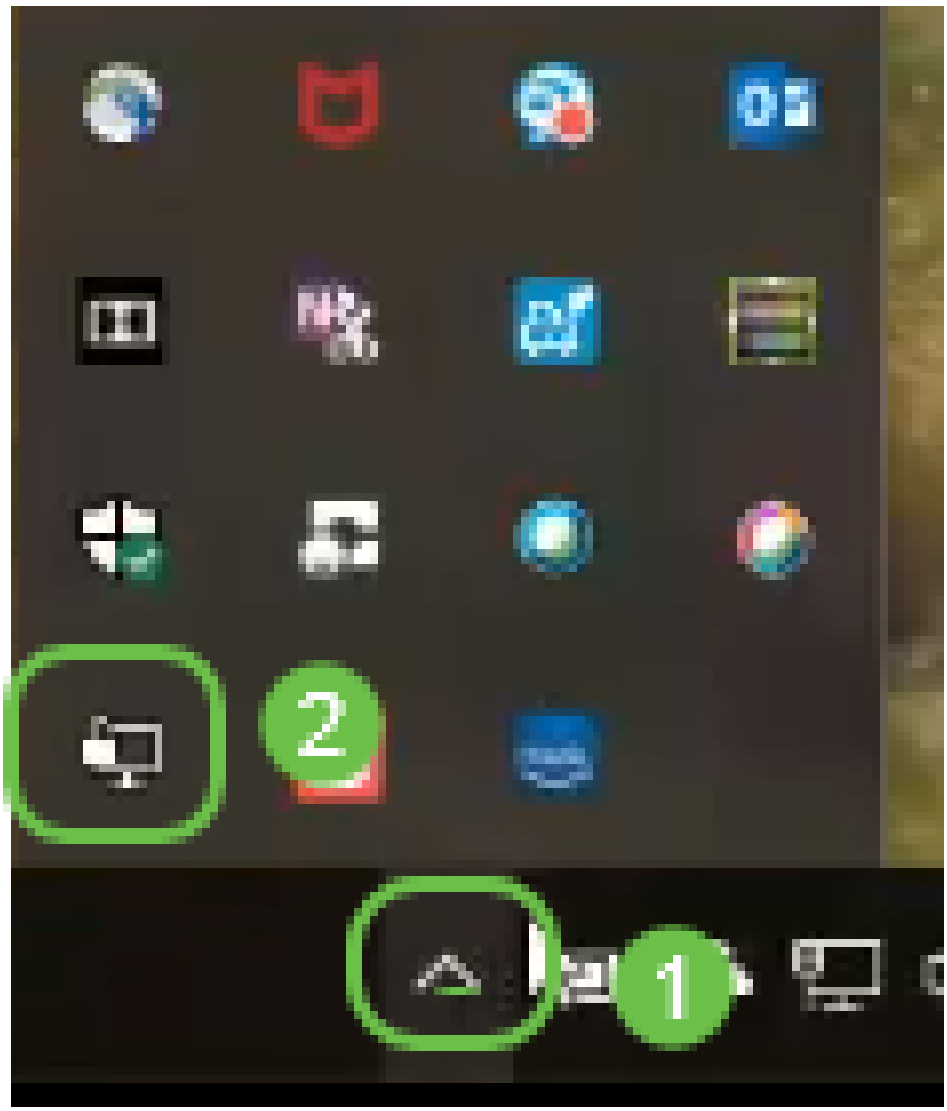
Voraussetzungen

Installieren Sie die OpenVPN-Anwendung auf Ihrem System. Klicken Sie hier, um zur OpenVPN-Website zu gelangen.

Für weitere Informationen zu OpenVPN und Antworten auf viele Fragen, die Sie haben, klicken Sie hier.

Hinweis: Diese Konfiguration ist speziell für Windows 10 bestimmt.

Sobald Sie OpenVPN installiert haben, sollte die Anwendung auf Ihrem Desktop oder als kleines Symbol auf der rechten Seite der Taskleiste angezeigt werden. OpenVPN-Clients benötigen diese ebenfalls.



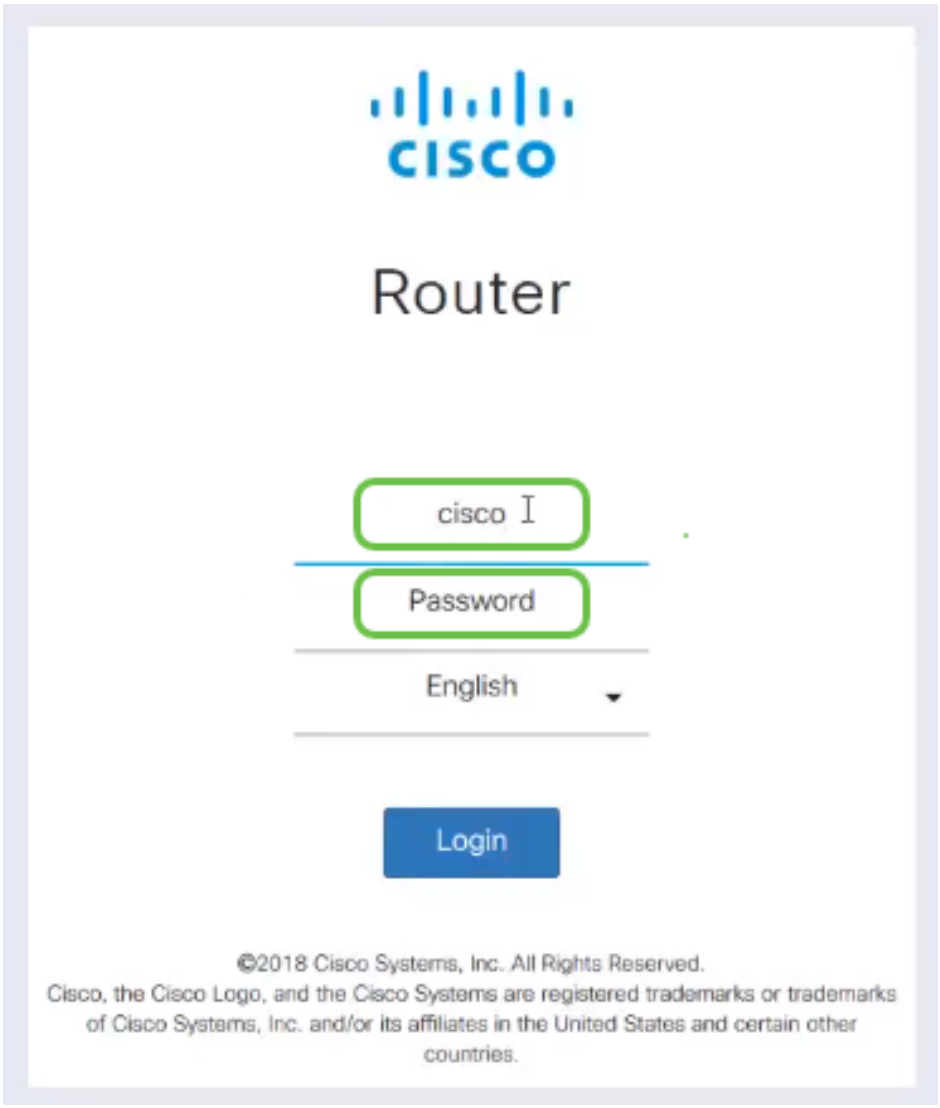
Stellen Sie sicher, dass auf allen Geräten die korrekte Systemzeit eingerichtet ist. Die korrekte Systemzeit muss vor der Erstellung eines Zertifikats am Router vollständig synchronisiert werden. Oft wird dies automatisch durchgeführt, aber wenn Sie auf Probleme stoßen, ist dies ein guter Ort zu überprüfen.

Einrichten einer OpenVPN-Demo auf einem RV160/RV260-Router

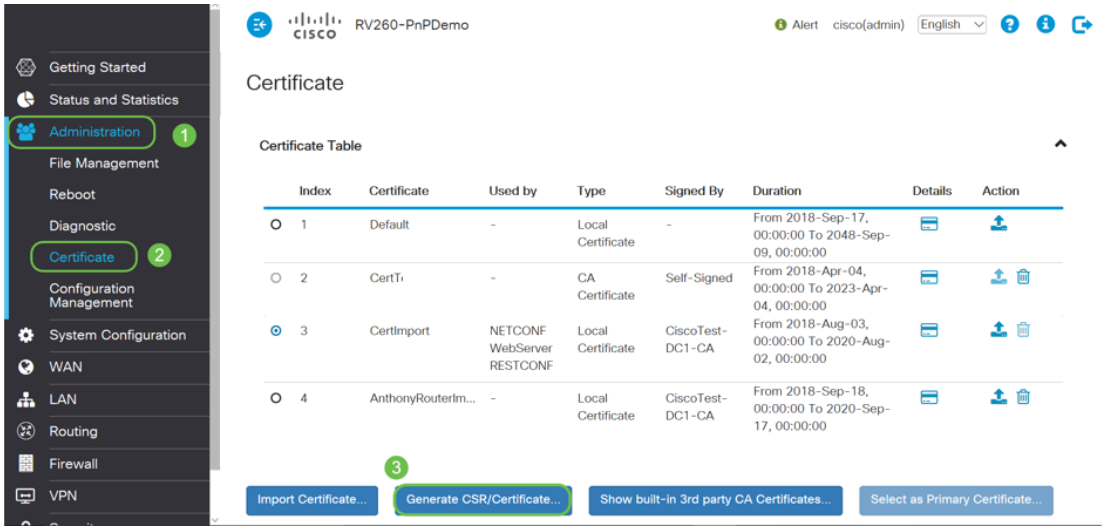
Wenn Sie OpenVPN ausprobieren möchten, bevor Sie Geld für eine CA bezahlen, können Sie ein selbstsigniertes Zertifikat erstellen. Auf diese Weise können Sie kostenfrei prüfen, ob Sie OpenVPN für Ihr Unternehmen bereitstellen möchten. Wenn Sie bereits wissen, dass Sie eine CA erwerben möchten, können Sie diesen Abschnitt des Artikels überspringen und direkt zu OpenVPN auf einem RV160/RV260 Router einrichten.

Schritt 1: Melden Sie sich mit Ihren Anmeldeinformationen beim Router an. Der Standardbenutzername und das Standardkennwort sind *cisco*.

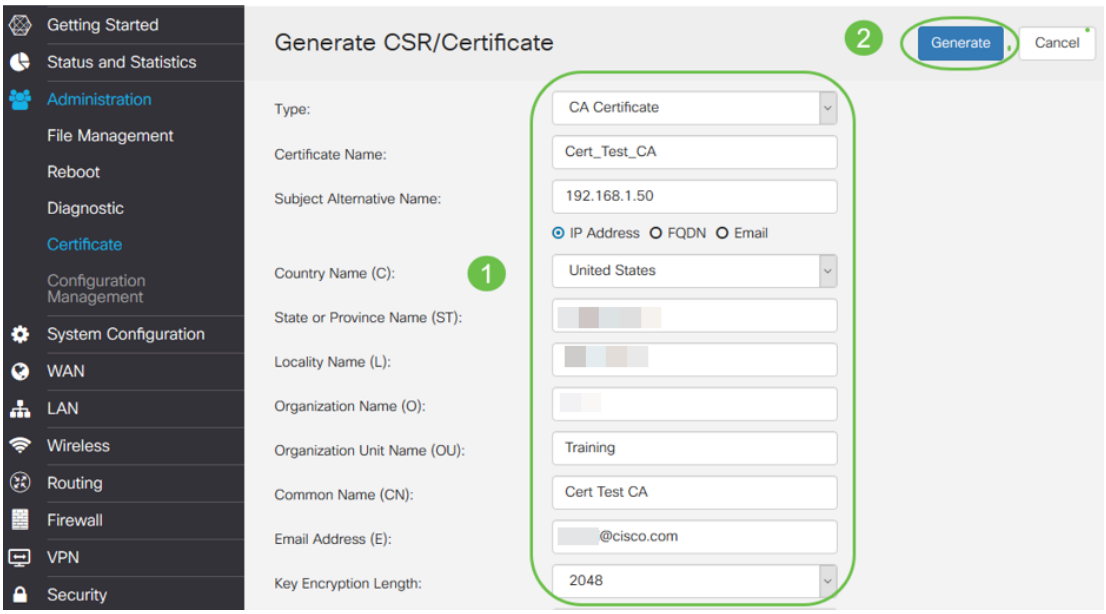
Hinweis: Es wird dringend empfohlen, alle Kennwörter in etwas Komplexeres zu ändern. Ansonsten ist es so, als ob man den Schlüssel an der Türschwelle hinter der verschlossenen Tür lassen würde.



Schritt 2: Es ist erforderlich, dass Sie ein Zertifikat auf dem Router erhalten. Navigieren Sie zu **Administration > Certificate > Generate CSR/Certificate...** So erstellen Sie die Anforderung für ein Zertifikat.



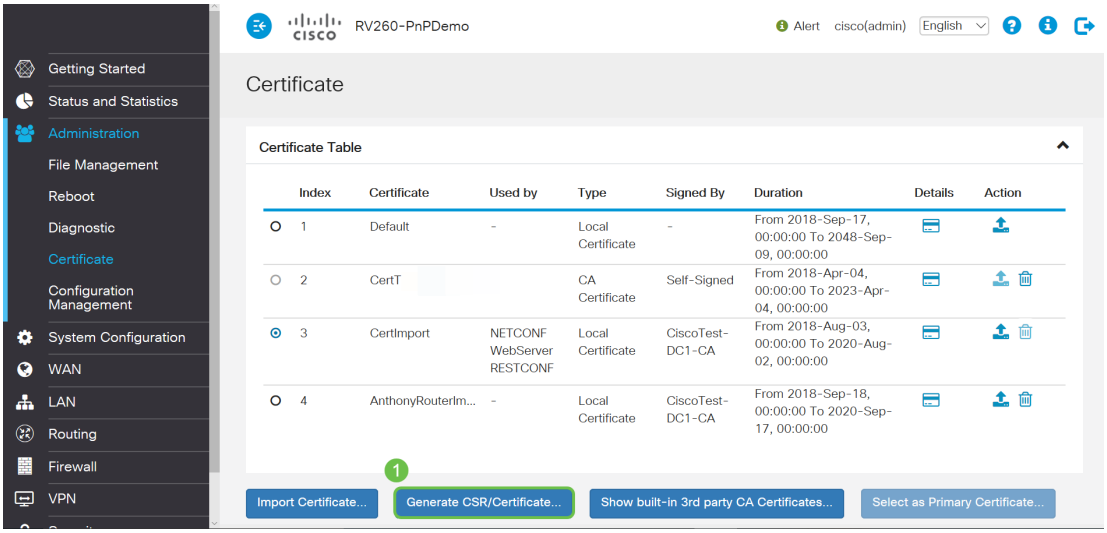
Schritt 3: Stellen Sie eine Anforderung für ein *Zertifizierungsstellenzertifikat*.



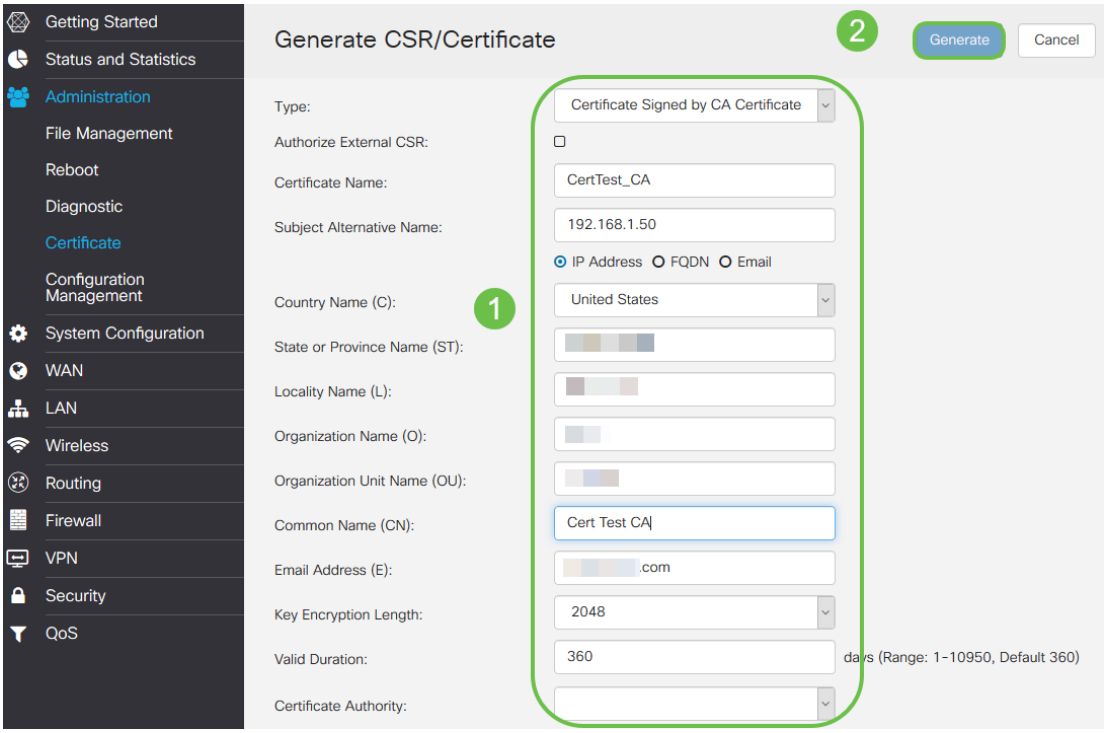
- Wählen Sie *CA Certificate* aus dem Dropdown-Menü aus.
- Zertifikatsname eingeben
- Geben Sie die IP-Adresse, den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die E-Mail-Adresse ein. Die Eingabe der IP-Adresse ist die häufigste Wahl.
- Land eingeben
- Geben Sie Ihren Bundesstaat ein.
- Geben Sie Ihren Ortsnamen ein, in der Regel Ihre Stadt.
- Geben Sie Ihren Firmennamen ein.
- Geben Sie den Namen der Organisationseinheit ein.
- Geben Sie Ihre E-Mail-Adresse ein.
- Geben Sie die Schlüssellänge ein. Es wird empfohlen, 2048 einzugeben.

Klicken Sie auf die Schaltfläche **Generieren** oben rechts.

Schritt 4: Sie benötigen auch ein Serverzertifikat. Dieses *Zertifikat, das vom Zertifizierungsstellenzertifikat signiert* wird, wird vom Zertifizierungsstellenzertifikat signiert, das Sie gerade erstellt haben.



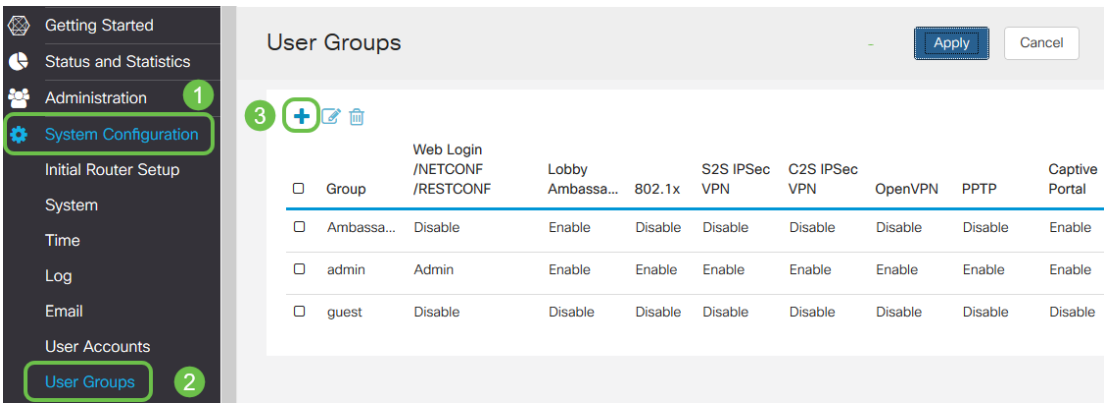
Schritt 5: Anforderung eines *Zertifikats, das vom Zertifizierungsstellenzertifikat signiert wurde*.



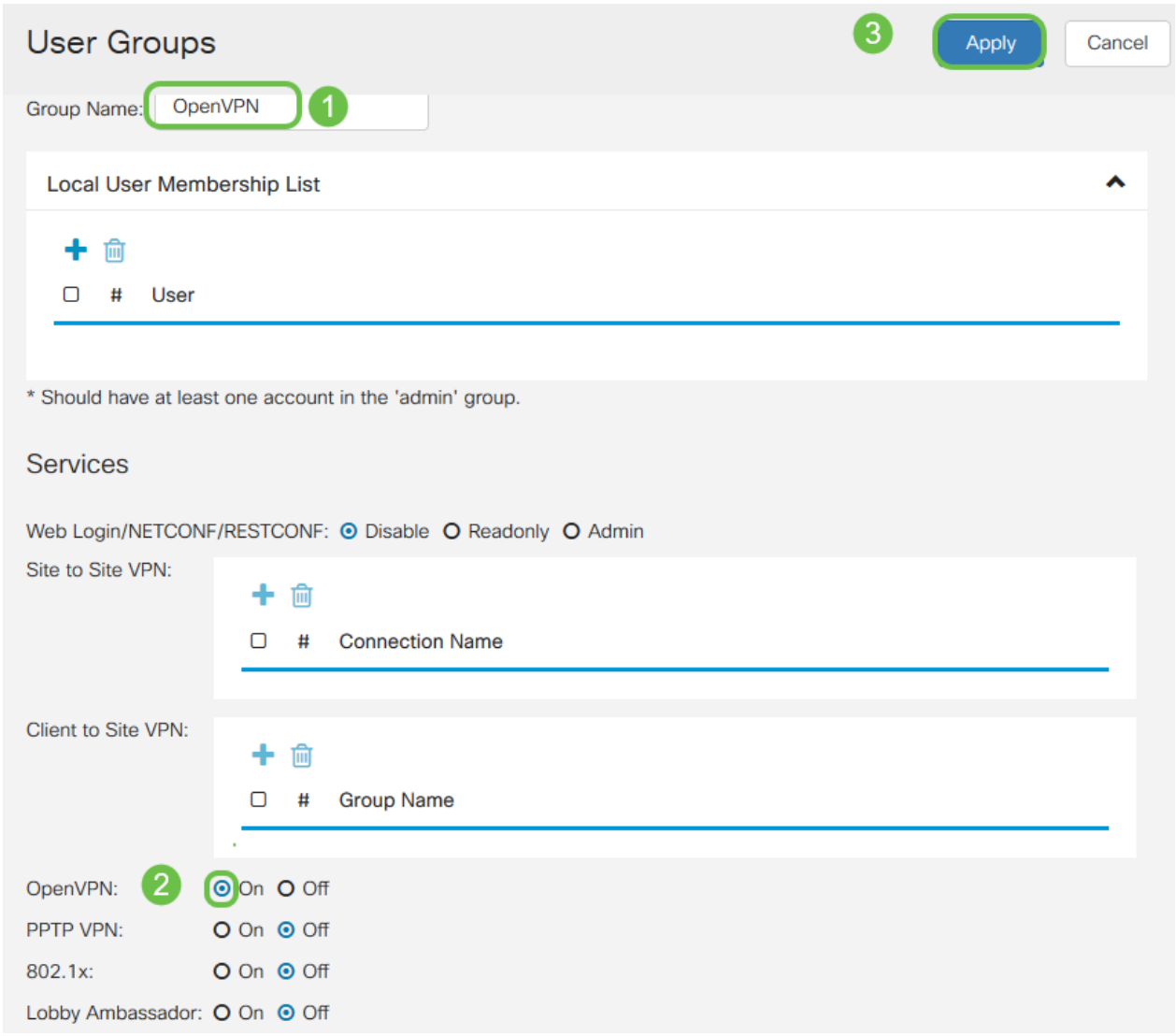
- Wählen Sie *Zertifikatssignaturanforderung* aus dem Dropdown-Menü aus.
- Zertifikatsname eingeben
- Geben Sie die IP-Adresse, den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die E-Mail-Adresse ein. Die Eingabe der IP-Adresse ist die häufigste Wahl.
- Land eingeben
- Geben Sie Ihren Bundesstaat ein.
- Geben Sie Ihren Ortsnamen ein, in der Regel Ihre Stadt.
- Geben Sie Ihren Firmennamen ein.
- Geben Sie den Namen der Organisationseinheit ein.
- Geben Sie Ihre E-Mail-Adresse ein.
- Geben Sie die Schlüssellänge ein. Es wird empfohlen, 2048 einzugeben.
- Wählen Sie im Dropdown-Menü die entsprechende Zertifizierungsstelle aus.

Klicken Sie auf die Schaltfläche **Generieren** oben rechts.

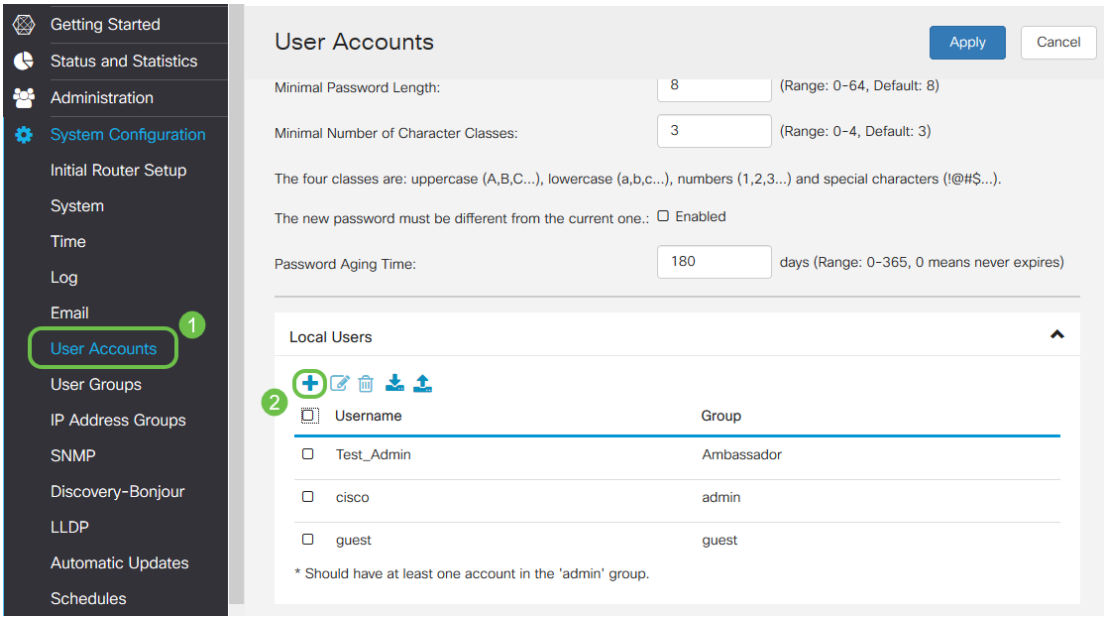
Schritt 6: Navigieren Sie zu **Systemkonfiguration > Benutzergruppen**. Wählen Sie das **Plus-**Symbol, um die neue Gruppe hinzuzufügen.



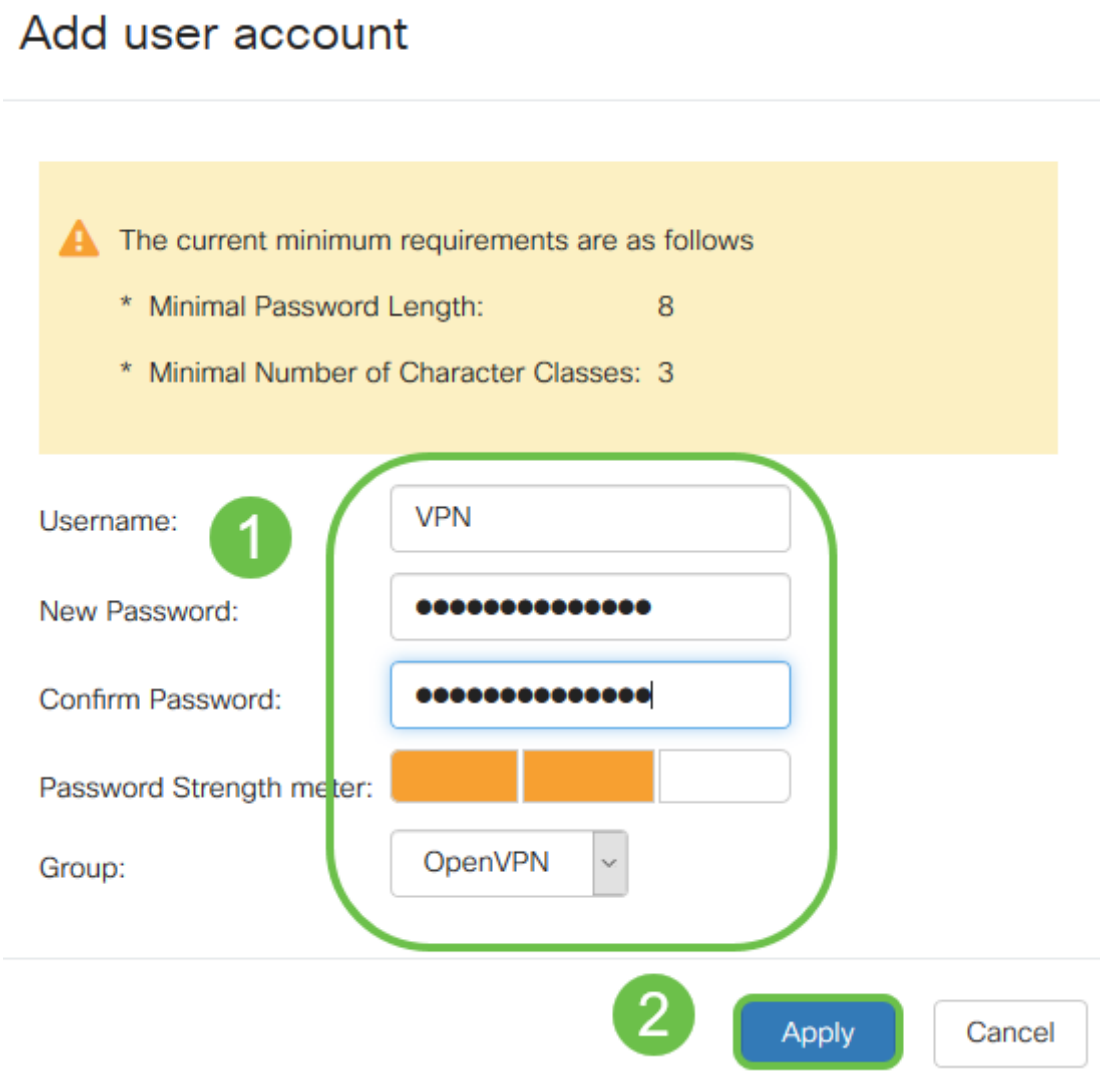
Schritt 7: Geben Sie den Namen der Gruppe ein, und klicken Sie auf *Ein*, damit das Optionsfeld OpenVPN aktiviert. Klicken Sie auf **Übernehmen**.



Schritt 8: Navigieren Sie im Menü Systemkonfiguration, und klicken Sie auf **Benutzerkonten**. Klicken Sie unter Lokale Benutzer auf das **Pluszeichen**.

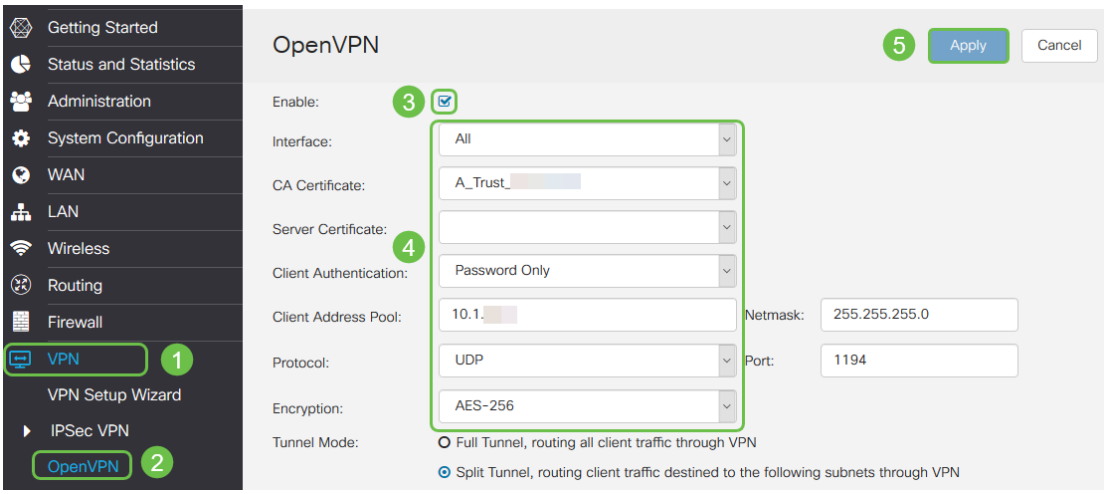


Schritt 9: Füllen Sie die unten stehenden Informationen aus. Wählen Sie im Dropdown-Menü OpenVPN aus. Klicken Sie auf **Übernehmen**.



Alle Abhängigkeiten sind abgeschlossen, und der Router kann jetzt für OpenVPN konfiguriert werden.

Schritt 10: Navigieren Sie zu **VPN > OpenVPN**. Die Seite OpenVPN wird geöffnet. Füllen Sie alle Felder auf der Seite aus, und wählen Sie im Dropdown-Menü die zuvor erstellten Zertifikate aus.

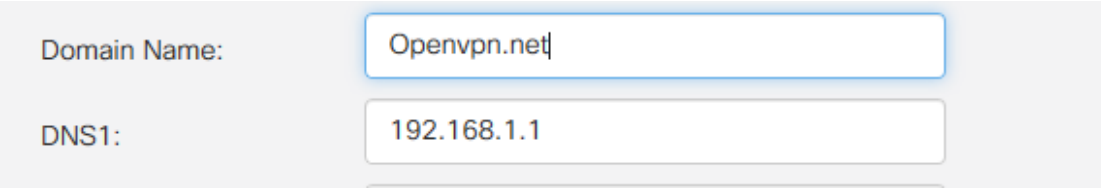


- Aktivieren Sie das Kontrollkästchen *Aktivieren*. Wählen Sie die Schnittstelle aus, die im Datenverkehr zugelassen werden soll. In diesem Fall ein Wide Area Network (WAN), und wählen Sie ein Certificate Authority (CA)-Zertifikat aus.
- Wählen Sie das *CA Certificate* aus dem Dropdown-Menü aus.
- Wählen Sie das vom Dropdown-Menü heruntergeladene Serverzertifikat aus.
- Wählen Sie *Client Authentication aus*. Wenn Sie Passwort auswählen, müssen sie sich

mit einem Passwort authentifizieren. Wenn Sie Password + Certificate auswählen, muss der Client auch über ein Zertifikat verfügen. Dies ist sicherer, erhöht jedoch die Kosten für das VPN, da eine separate CA erworben werden muss.

- Geben Sie den *Client-Adresspool ein*. Wählen Sie eine IP-Adresse in einem Netzwerk-Subnetz aus, die nirgendwo anders im Unternehmen verwendet wird. Sie wählen aus den reservierten Bereichen einen Bereich aus, der nirgendwo anders verwendet wird.
- Wählen Sie die Form der *Verschlüsselung aus*. Stellen Sie sicher, dass die Verschlüsselung mit dem Client übereinstimmt. DES und 3DES werden nicht empfohlen und sollten nur zur Abwärtskompatibilität verwendet werden.
- Wählen Sie Split Tunnel (Tunnel teilen), wenn Sie nur angeben möchten, welcher Datenverkehr das VPN durchläuft. Für ein VPN ist ein Split-Tunnel erforderlich. In anderen Situationen wird der *Full-Tunnel-Modus* ausgewählt, wenn der gesamte Client-Datenverkehr das VPN durchlaufen soll.

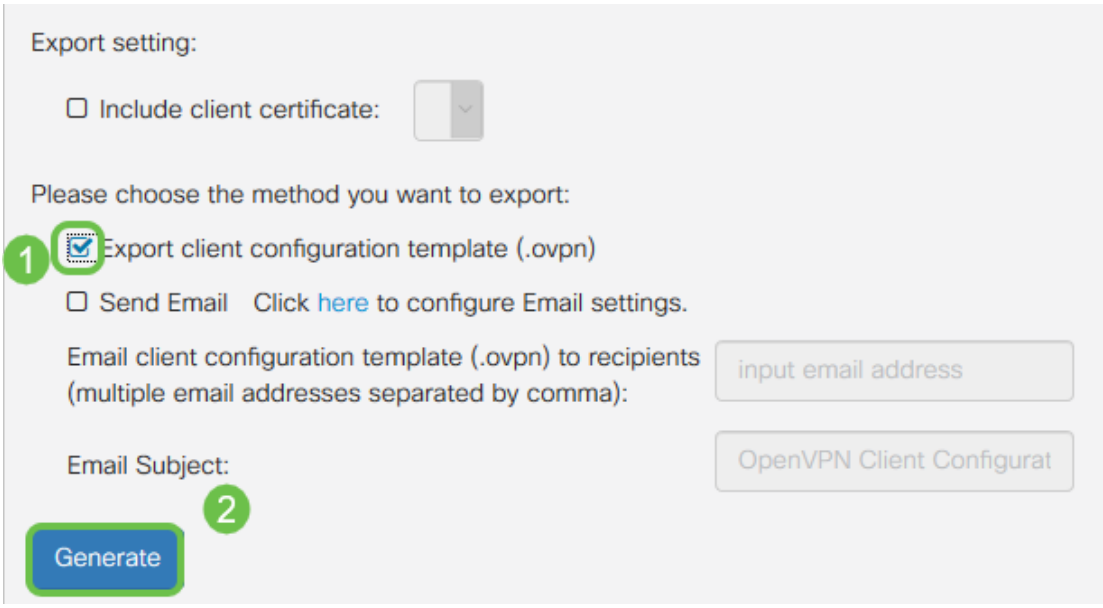
Schritt 11: Blättern Sie auf der Seite nach unten, und füllen Sie den *Domänennamen* und *DNS1 aus*.



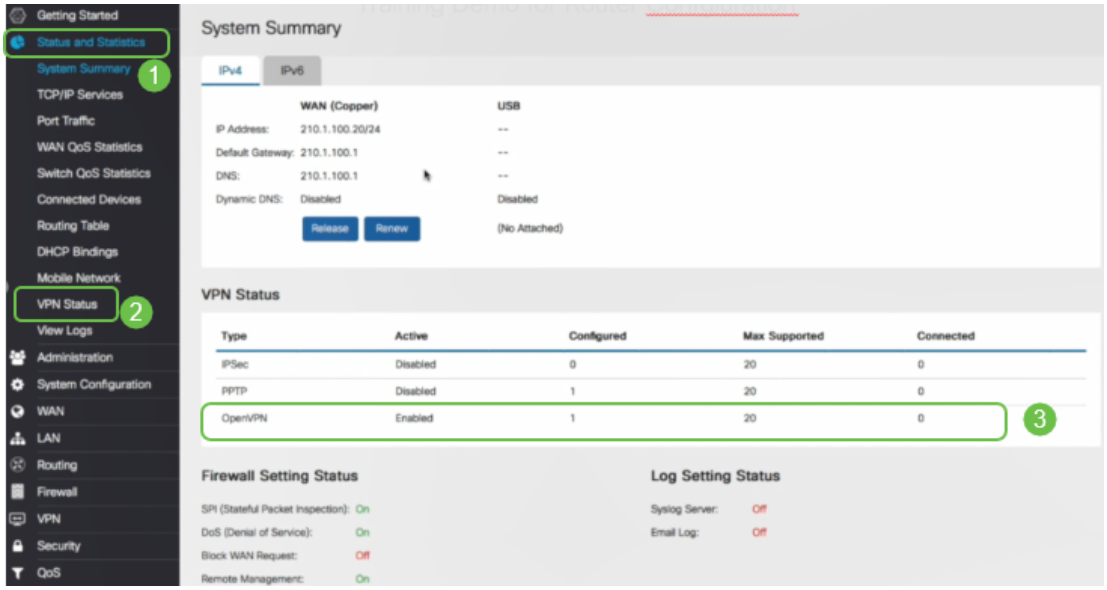
Hinweis: Bei der DNS1-IP-Adresse kann es sich um einen dedizierten internen DNS-Server, die gleiche IP-Adresse des Standard-Gateways handeln, die von Ihrem Internetdienstanbieter (ISP), auf einem virtuellen System oder einen vertrauenswürdigen DNS-Server im Internet bereitgestellt wird.

Schritt 12: Klicken Sie auf **Apply**, um die Konfiguration auf dem Router zu speichern.

Schritt 13: Bleiben Sie auf derselben Seite und scrollen Sie weiter. Erstellen Sie die Konfigurationsvorlage, die auf dem OpenVPN-Client installiert werden soll. Diese Datei hat eine Erweiterung *.ovpn* und wird vom OpenVPN-Client verwendet. Aktivieren Sie das Kontrollkästchen *Client-Konfigurationsvorlage exportieren (.ovpn)*, und klicken Sie auf **Generieren**. Dadurch wird die Datei auf Ihren Computer heruntergeladen.



Schritt 14: Navigieren Sie zu **Status und Statistik > VPN Status**. Sie haben die Möglichkeit, nach unten zu scrollen, um detailliertere Informationen zu erhalten.



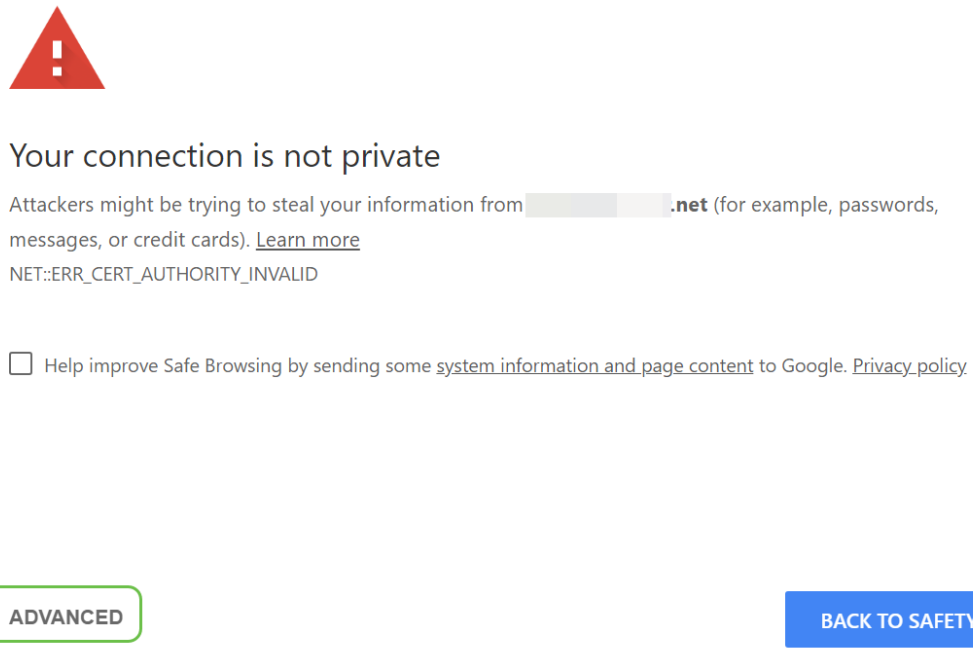
Der nächste Abschnitt dieses Artikels ist sehr wichtig, da darin erläutert wird, wie Sie sich mit einem selbstsignierten Zertifikat anmelden.

Anmelden mit einem selbst signierten Zertifikat nach der Einrichtung von Demo OpenVPN

Wenn Sie sich mit einem selbstsignierten Zertifikat anmelden, wird bei der Anmeldung möglicherweise ein Warnmeldungsfenster angezeigt. Sie müssen abhängig von Ihrem Webbrowser auf Erweitert, Weiter, Vertrauenswürdig oder eine andere Option klicken, um fortzufahren.

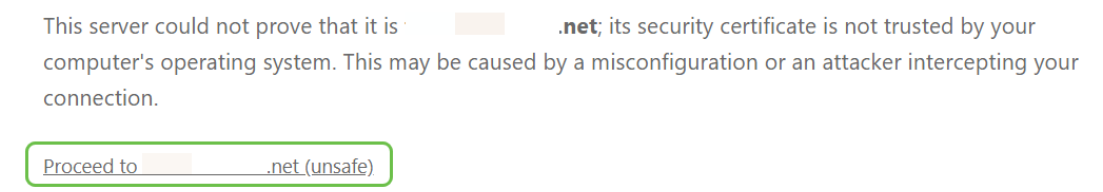
An dieser Stelle erhalten Sie möglicherweise eine Warnung, dass es unsicher ist. Sie können fortfahren, eine Ausnahme hinzufügen oder eine erweiterte Option auswählen. Dies variiert je nach Webbrowser.

In diesem Beispiel wurde Chrome für einen Webbrowser verwendet. Diese Meldung wird angezeigt, klicken Sie auf **Erweitert**.

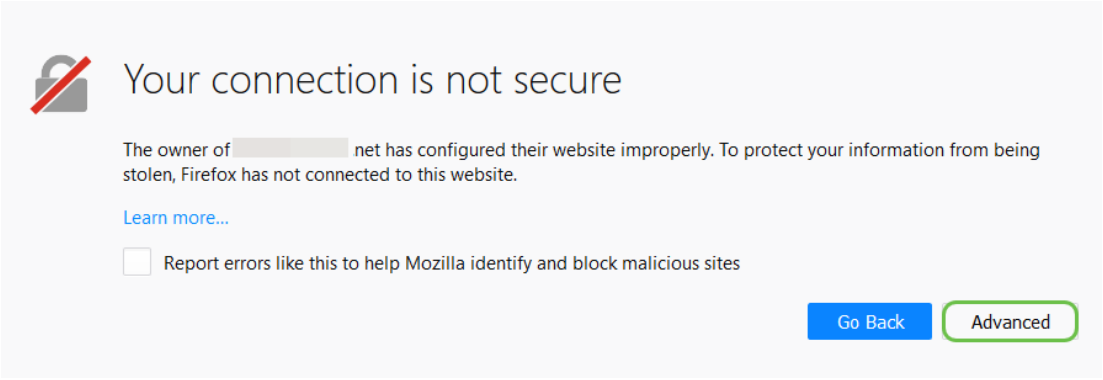


Ein neuer Bildschirm wird geöffnet, und Sie müssen auf **Weiter zu Ihrer Website.net** klicken

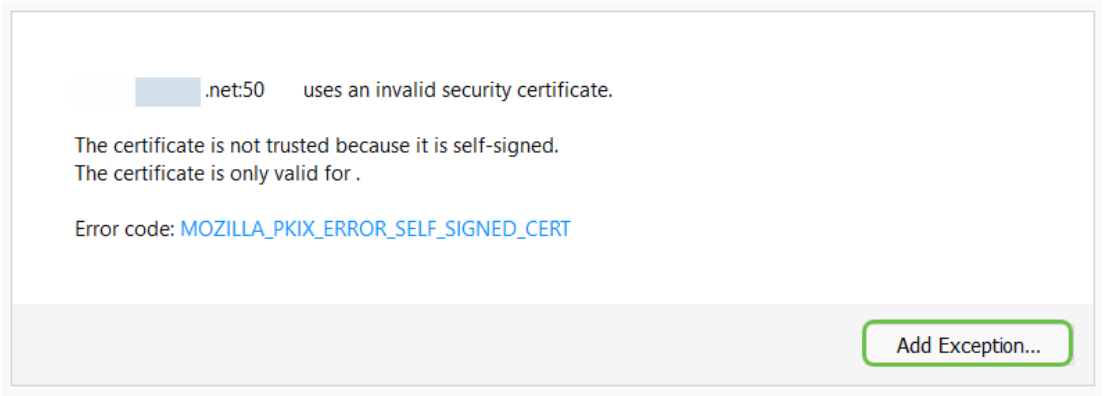
(unsafe).



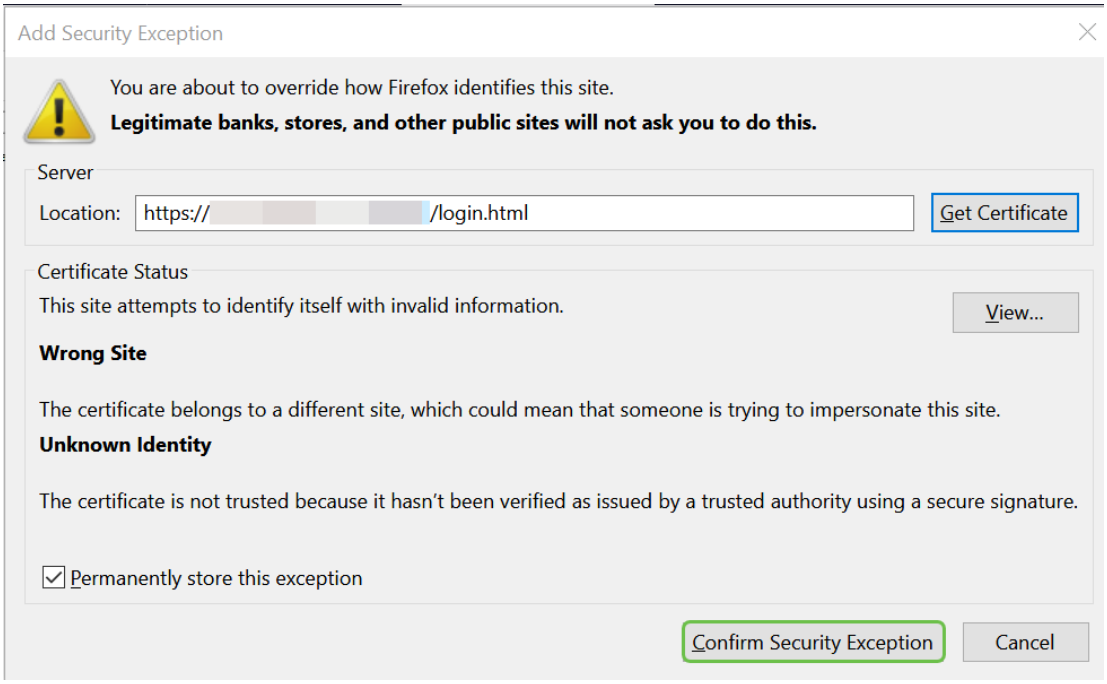
Im Folgenden finden Sie ein Beispiel für den Zugriff auf die Gerätewarnung, wenn Firefox als Webbrowser verwendet wird. Klicken Sie auf **Erweitert**.



Klicken Sie auf **Ausnahme hinzufügen...**



Schließlich müssen Sie auf **Sicherheitsausnahme bestätigen** klicken.



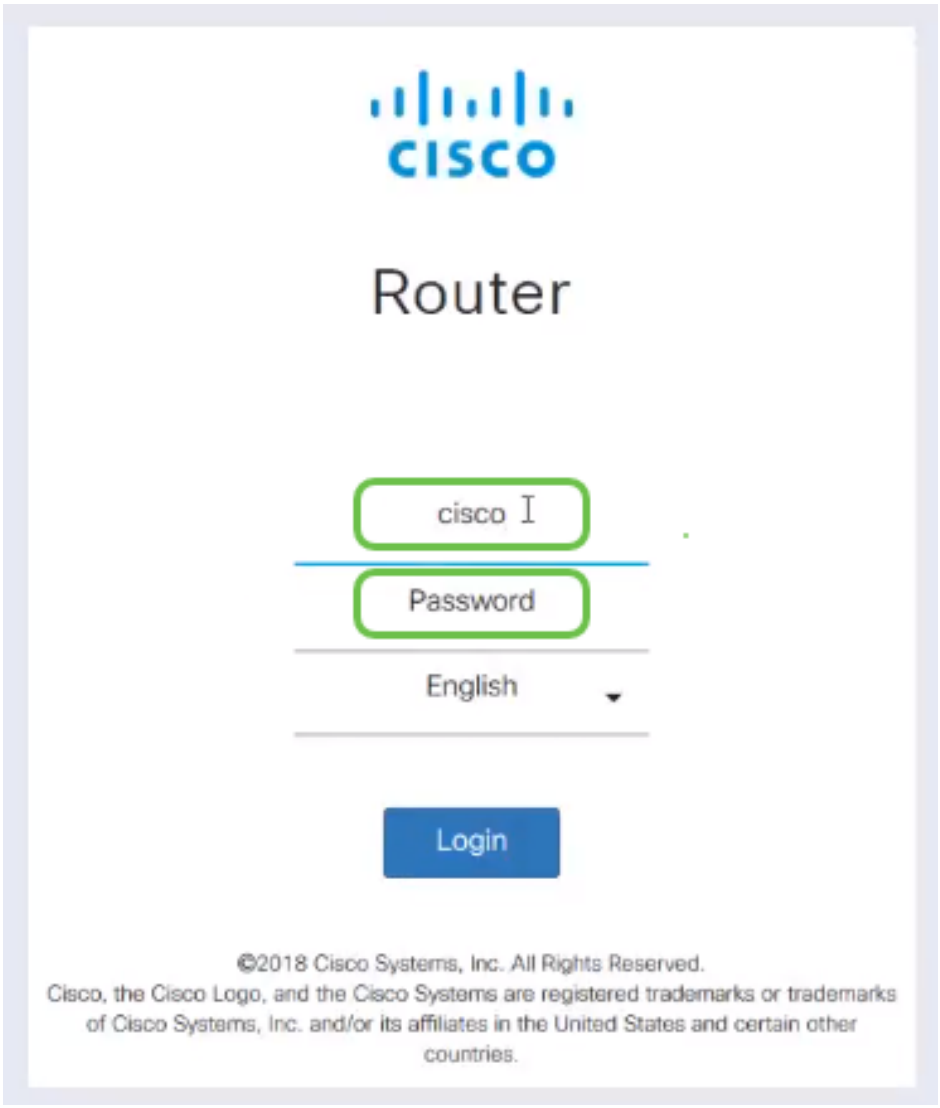
Der Router ist nun mit allen Parametern konfiguriert, die zur Unterstützung einer OpenVPN-Client-Verbindung erforderlich sind. Da Sie die Client-Konfigurationsvorlage bereits auf Ihr Gerät heruntergeladen haben, das in *.ovpn endet*, können Sie mit dem Abschnitt OpenVPN Client Setup on Computer fortfahren. Wenn Sie sich für die Bereitstellung von OpenVPN für Ihr Unternehmen entscheiden, können Sie die Schritte in diesem nächsten Abschnitt befolgen.

Einrichten von OpenVPN auf einem RV160/RV260-Router

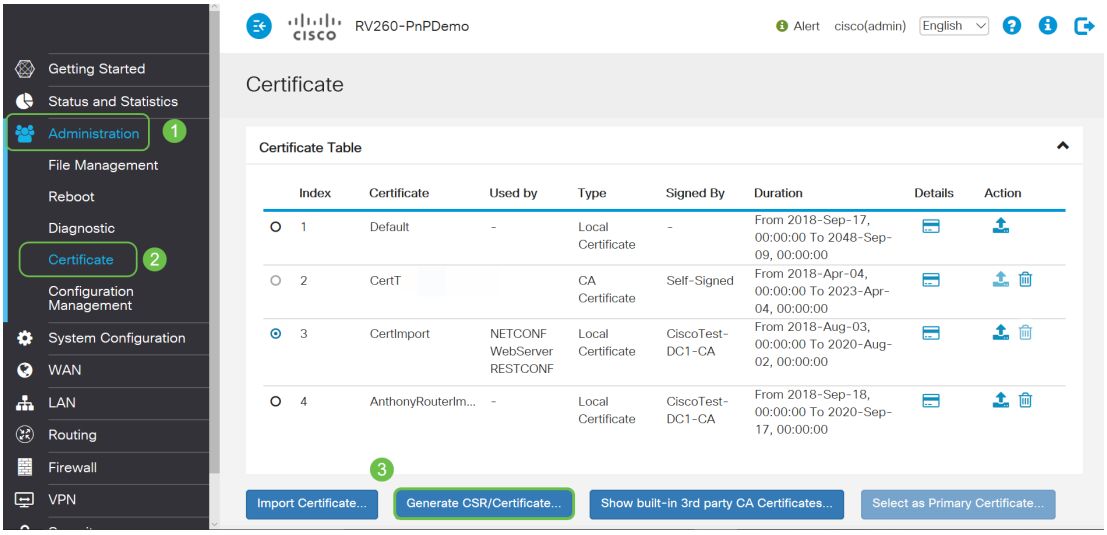
Dies ist ein komplizierterer Prozess, da es darum geht, eine CA von einem Drittanbieter zu bekommen, was Geld kostet. Sie müssen außerdem die VPN-Client-Konfigurationsvorlage, die in *.ovpn* endet, an alle Clients senden, damit diese auf ihrem Gerät eingerichtet werden können. Clients benötigen mehrere Einstellungen, die mit dem Router übereinstimmen, damit sie kommunizieren können. Das Beste daran ist, dass Sie und Ihre Mitarbeiter bei minimalen Kosten das Internet nutzen und Geschäfte sicherer abwickeln können.

Schritt 1: Melden Sie sich mit Ihren Anmeldeinformationen beim Router an. Der Standardbenutzername und das Standardkennwort sind *cisco*.

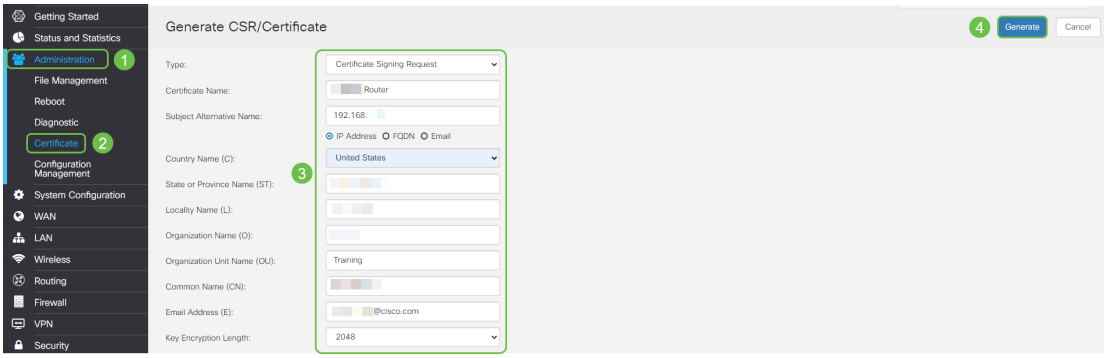
Hinweis: Es wird dringend empfohlen, alle Kennwörter in etwas Komplexeres zu ändern. Ansonsten ist es so, als ob man den Schlüssel an der Türschwelle hinter der verschlossenen Tür lassen würde.



Schritt 2: Sie müssen ein Zertifikat erwerben. Navigieren Sie zu **Administration > Certificate > Generate CSR/Certificate...** So erstellen Sie die Anforderung für ein Zertifikat.



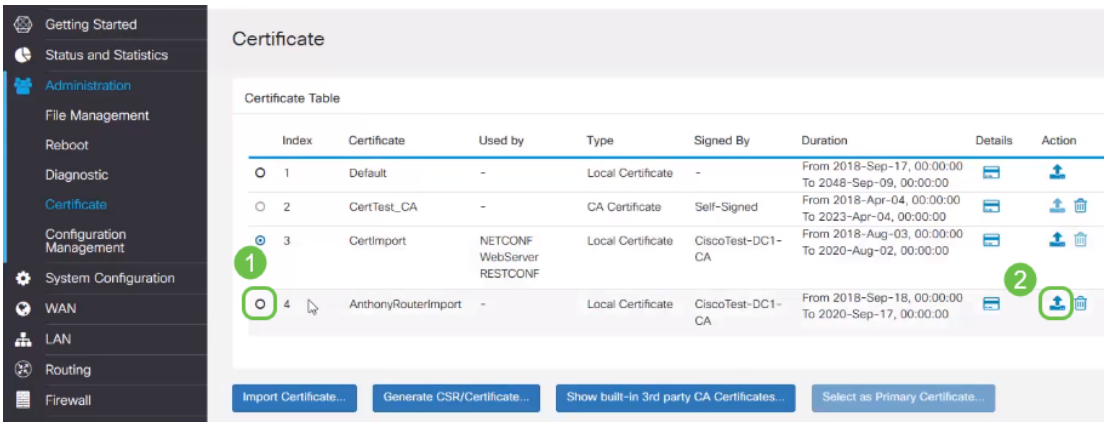
Schritt 3: Anforderung eines *Zertifikats, das vom Zertifizierungsstellenzertifikat signiert wurde*. Navigieren Sie dazu zu **Administration > Certificate**.



- Wählen Sie *Zertifikatssignaturanforderung* aus dem Dropdown-Menü aus.
- Zertifikatsname eingeben
- Geben Sie die IP-Adresse, den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die E-Mail-Adresse ein. Die Eingabe der IP-Adresse ist die häufigste Wahl.
- Land eingeben
- Geben Sie Ihren Bundesstaat ein.
- Geben Sie Ihren Ortsnamen ein, in der Regel Ihre Stadt.
- Geben Sie Ihren Firmennamen ein.
- Geben Sie den Namen der Organisationseinheit ein.
- Geben Sie Ihre E-Mail-Adresse ein.
- Geben Sie die Schlüssellänge ein. Es wird empfohlen, 2048 einzugeben.

  Klicken Sie auf die Schaltfläche **Generieren** oben rechts

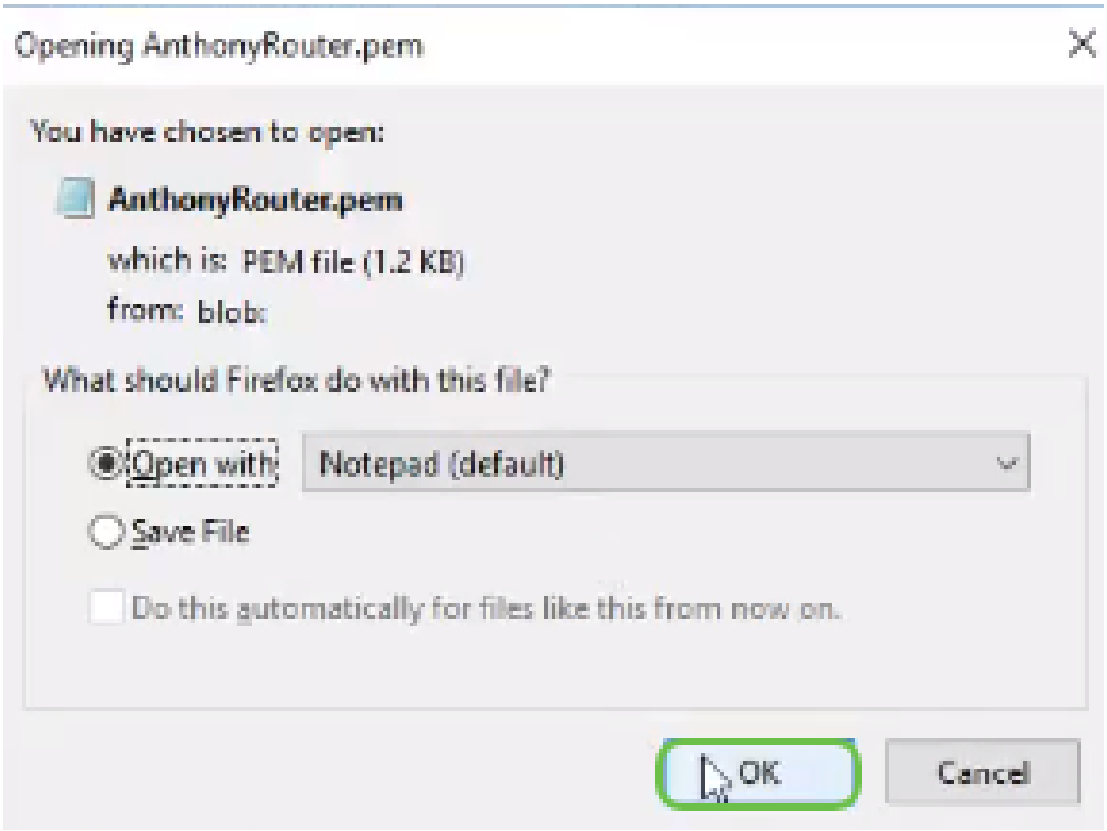
Schritt 4: Wählen Sie diese Option aus, indem Sie unter Aktion auf den Pfeil nach oben klicken.



Schritt 5: Dieser Bildschirm wird angezeigt. Klicken Sie auf **Exportieren**.

Schritt 6: Wählen Sie *Öffnen mit und Editor* (Standard) aus dem Dropdown-Menü aus. Klicken Sie

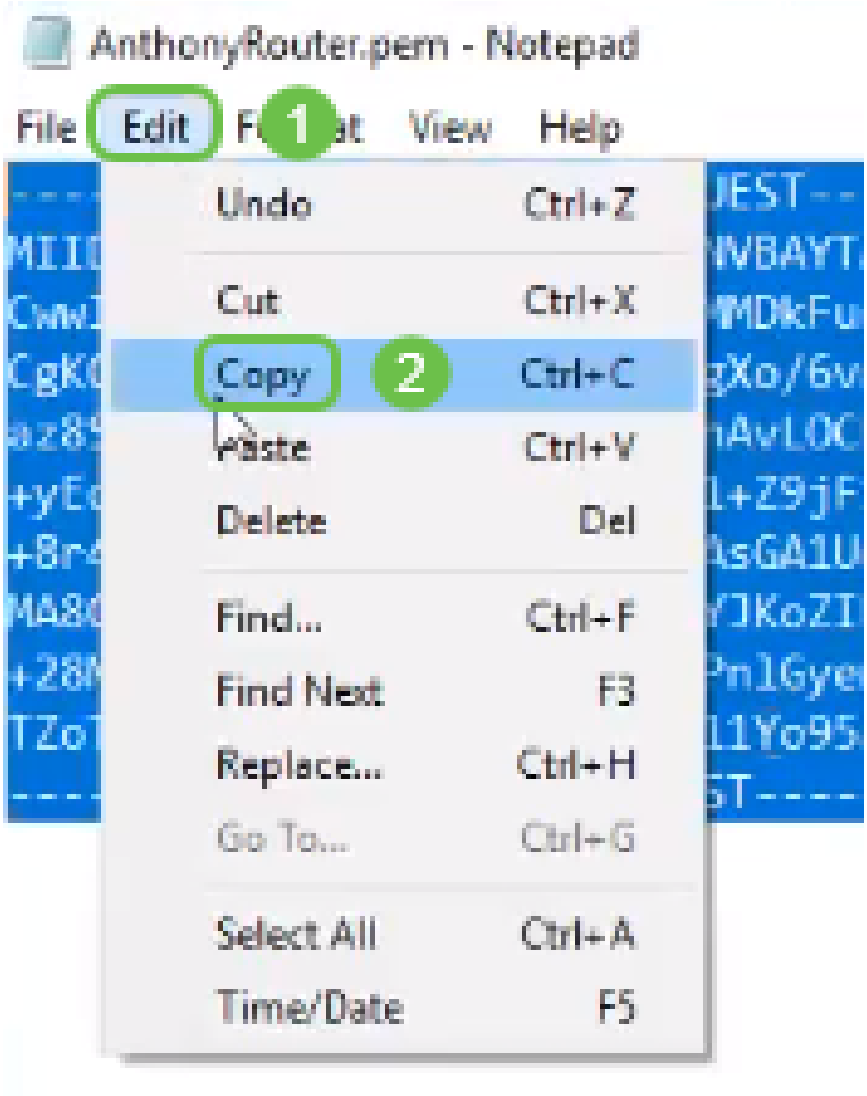
auf **OK**.



Schritt 7: Eine XML-Datei wird geöffnet.

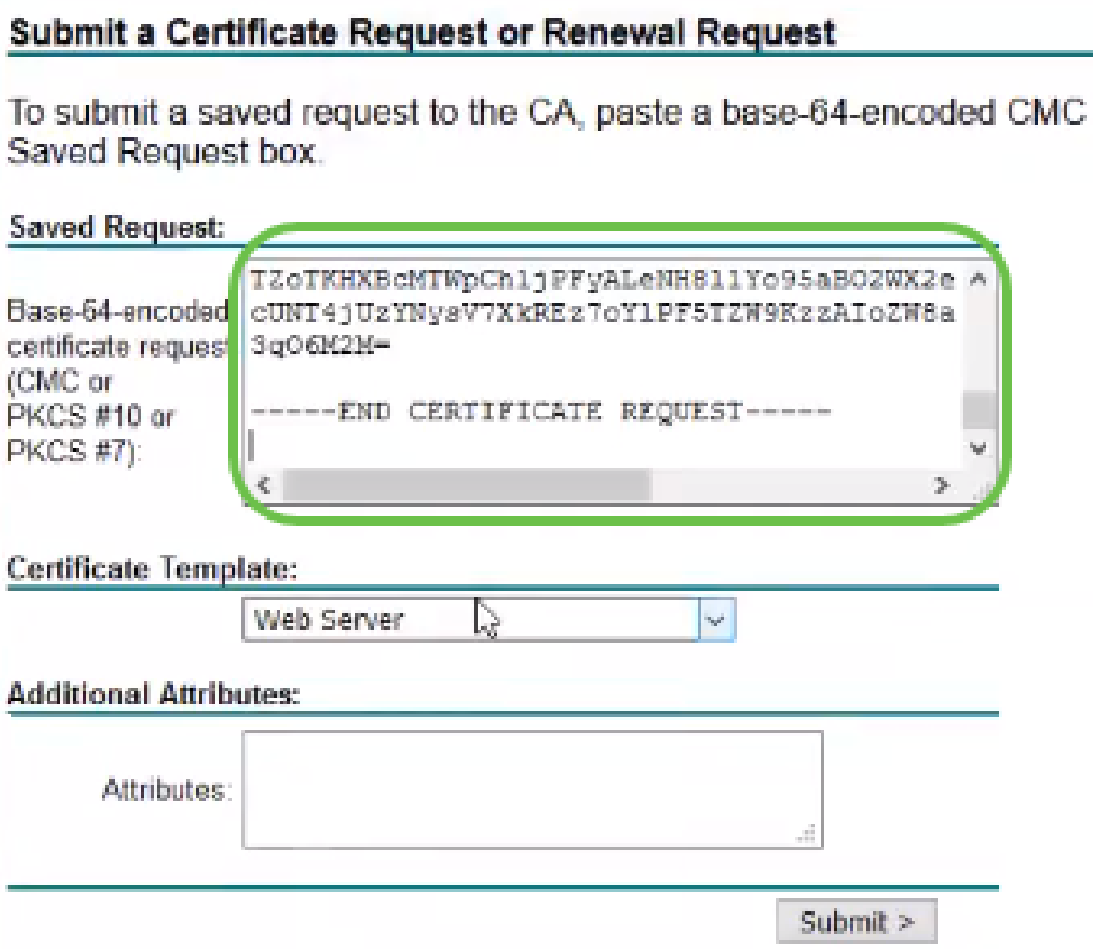
Hinweis: Stellen Sie sicher, dass die BEGIN-ZERTIFIKATANFORDERUNG und die ENDZERTIFIKATANFORDERUNG wie oben gezeigt in den jeweiligen Zeilen aufgeführt sind.

Schritt 8: Klicken Sie oben im Bildschirm auf **Bearbeiten**, und wählen Sie aus dem Dropdown-Menü **Kopieren** aus.

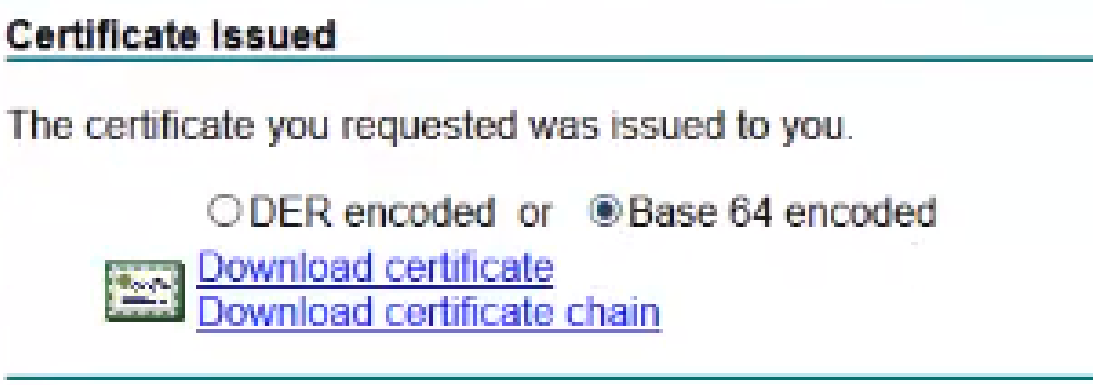


Schritt 9: Wählen Sie eine renommierte Drittanbieter-Website aus, um die Zertifikatsanforderung anzufordern. Sie müssen die kopierte XML-Datei als Teil der Anforderung einfügen.

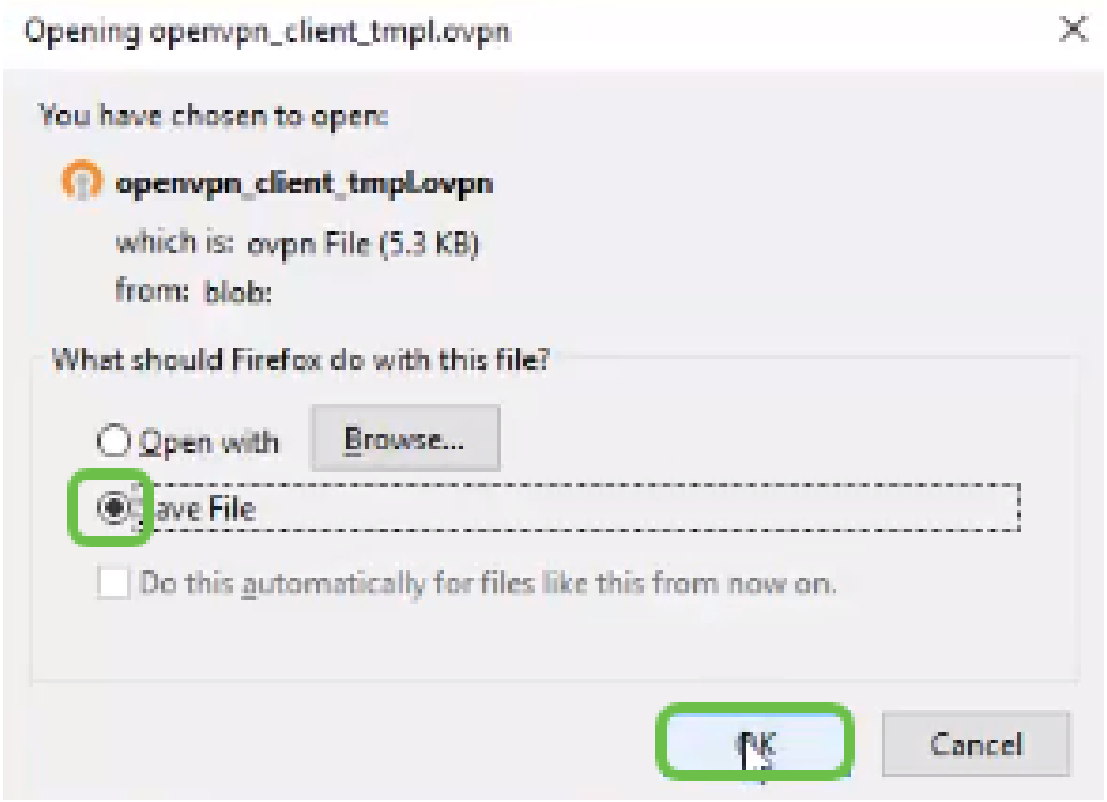
Hinweis: Wenn Sie über einen internen Zertifikatsserver in Ihrem Netzwerk verfügen, können Sie diesen stattdessen verwenden, dies ist jedoch nicht üblich.



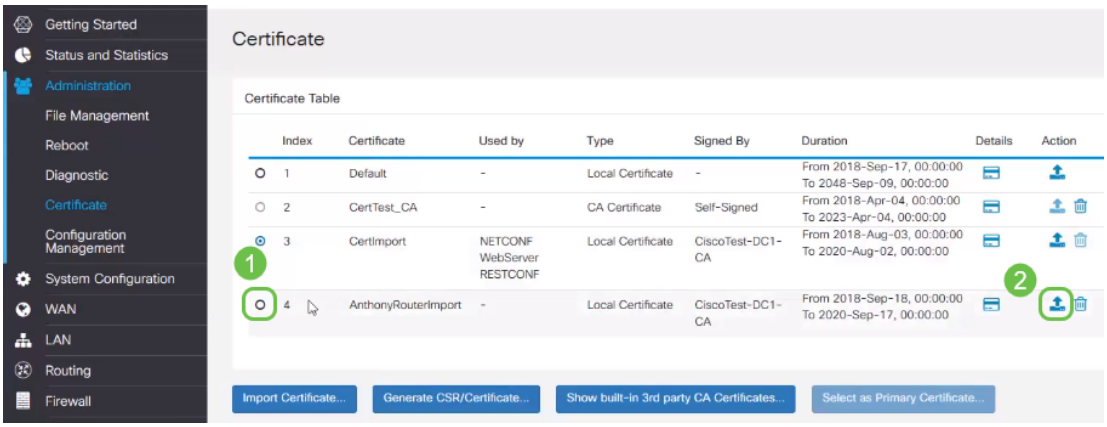
Schritt 10: Nach der Überprüfung können Sie *Zertifikat herunterladen* auswählen.



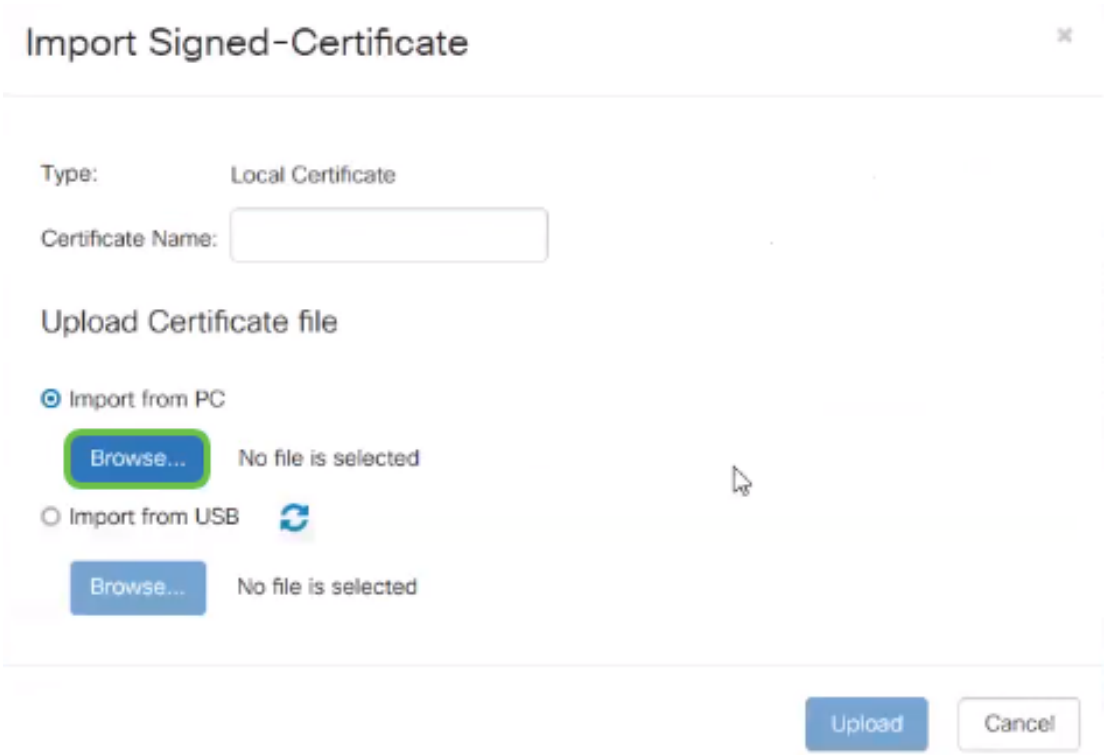
Schritt 11: Klicken Sie auf das Optionsfeld *Datei speichern* und dann auf **OK**.



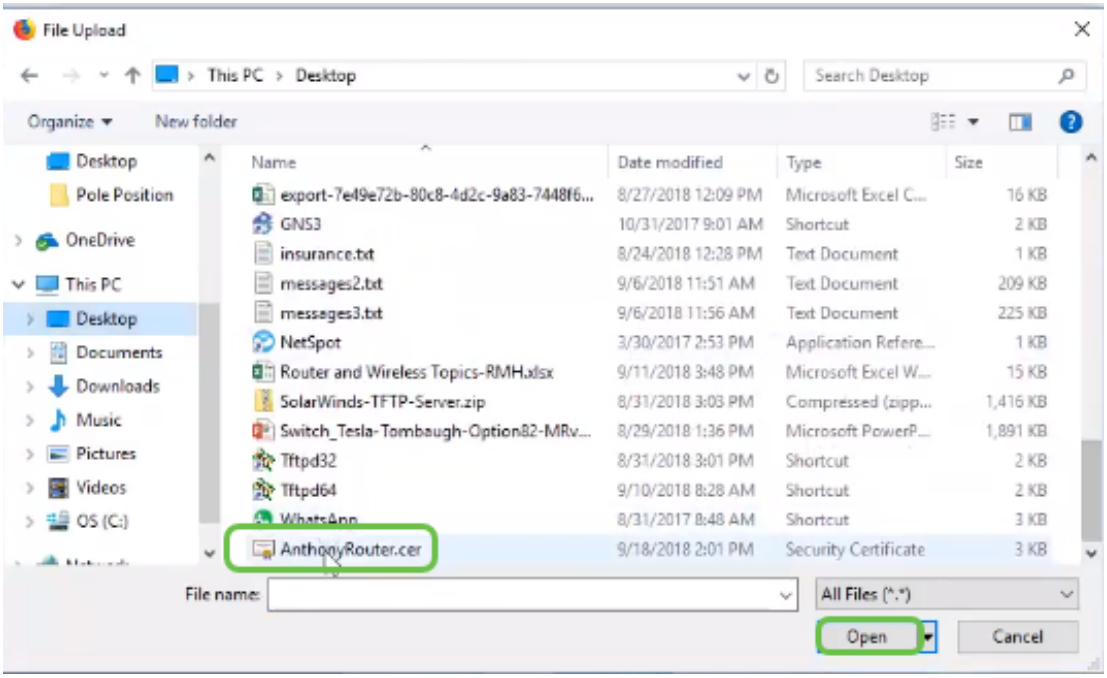
Schritt 12: Wählen Sie nach dem Speichern das Optionsfeld für dieses Zertifikat aus, und klicken Sie auf das Symbol **mit dem Pfeil nach unten**.



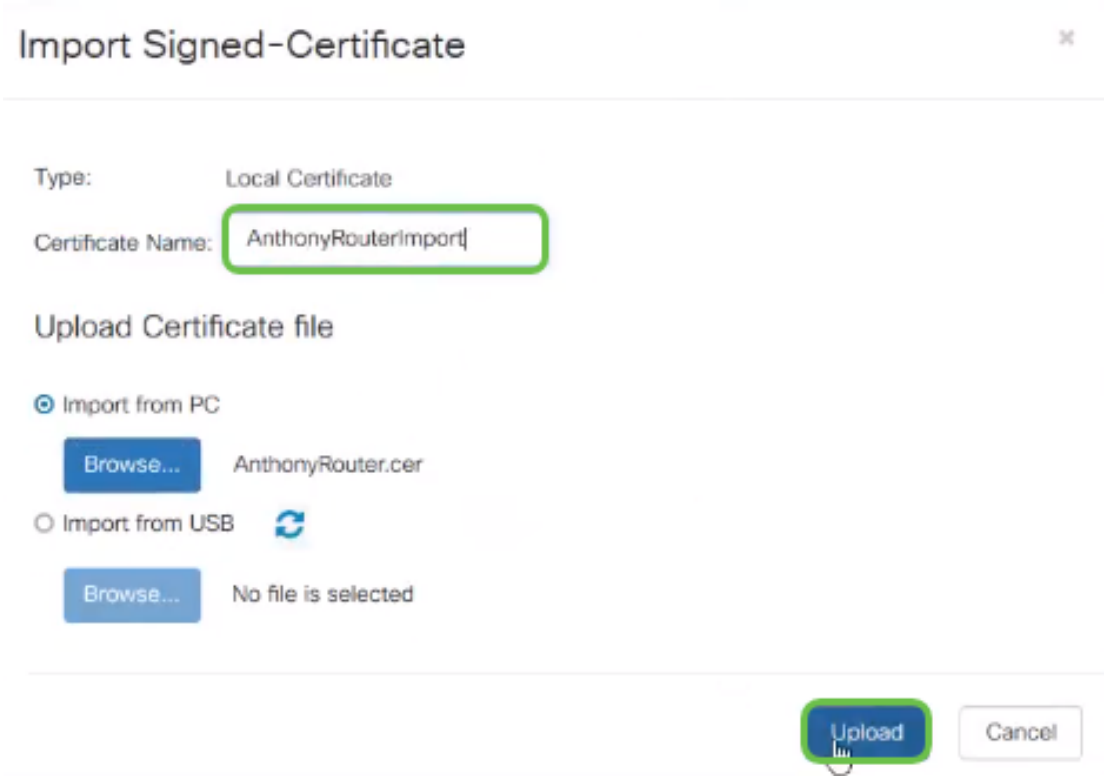
Schritt 13: Dieser Bildschirm wird geöffnet. Wählen Sie **Durchsuchen aus....**



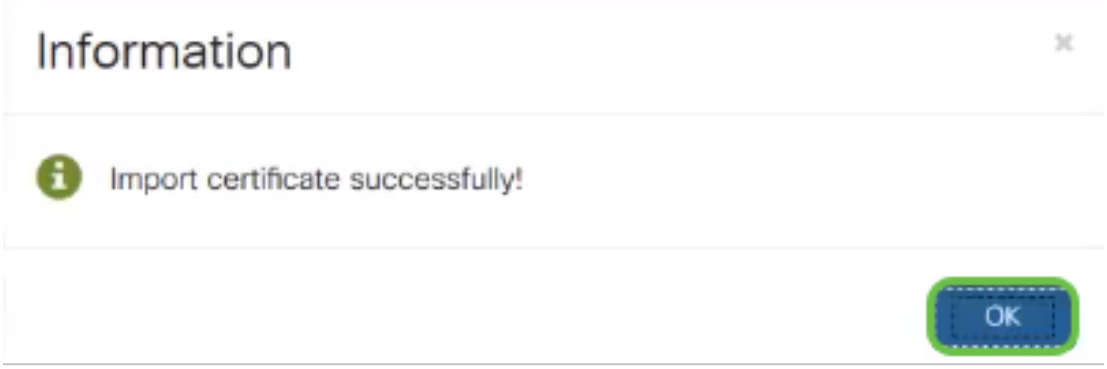
Schritt 14: Wählen Sie die Datei des Zertifikats aus, und klicken Sie auf **Öffnen**.



Schritt 15: Geben Sie den *Zertifikatsnamen* für den Import ein, und klicken Sie auf **Hochladen**.

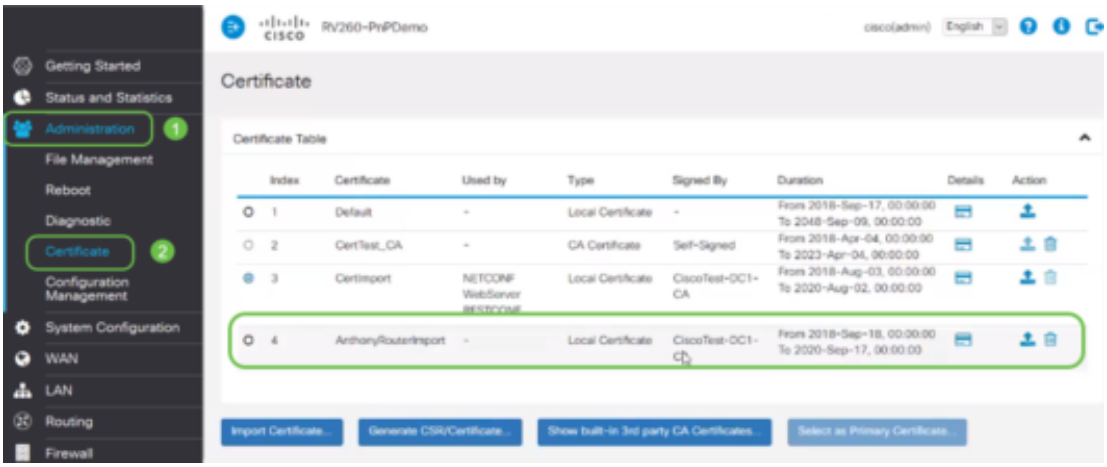


Schritt 16: Sie erhalten eine Benachrichtigung, dass das Zertifikat erfolgreich importiert wurde. Klicken Sie auf **OK**.

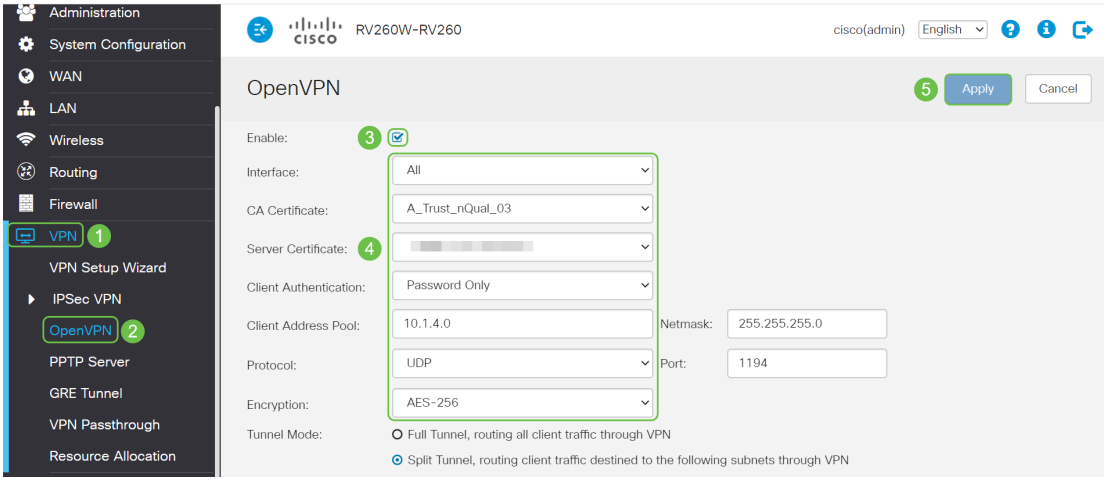


Schritt 17: Navigieren Sie zu **Administration > Certificate**. Das Zertifikat wurde geladen.

Hinweis: In diesem Beispiel wurde ein lokaler Zertifikatsserver verwendet.



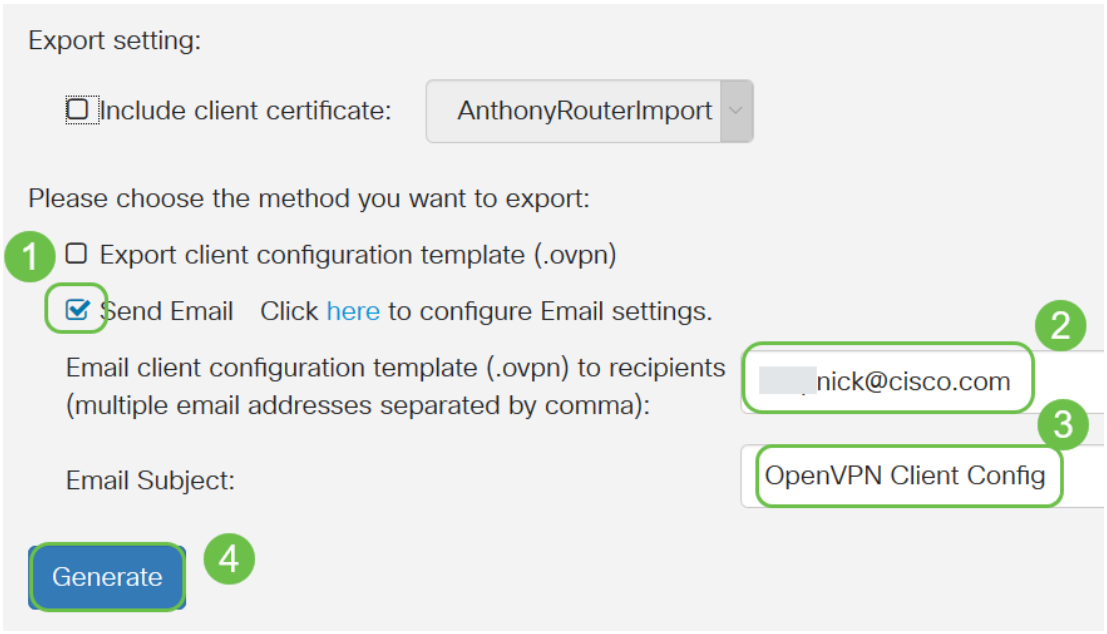
Schritt 18: Navigieren Sie zu **VPN > OpenVPN**. Die Seite OpenVPN wird geöffnet. Füllen Sie die folgenden Felder mit Ihren Informationen aus.



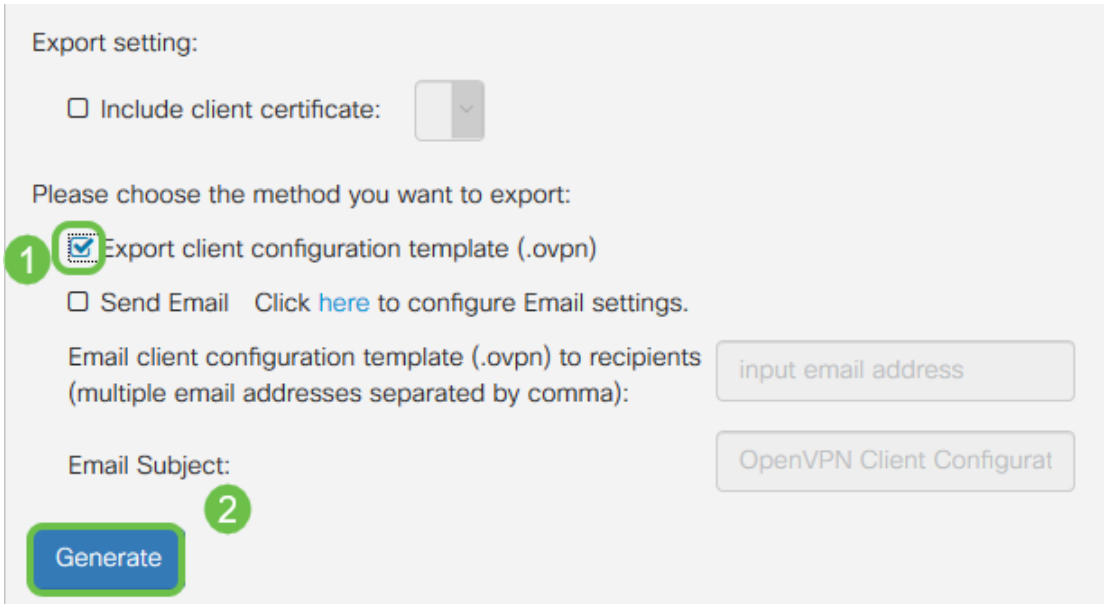
- Aktivieren Sie das Kontrollkästchen *Aktivieren*. Wählen Sie die Schnittstelle aus, die im Datenverkehr zugelassen werden soll. In diesem Fall ein Wide Area Network (WAN), und wählen Sie ein Certificate Authority (CA)-Zertifikat aus.
- Wählen Sie das *CA Certificate* aus dem Dropdown-Menü aus.
- Wählen Sie aus dem Dropdown-Menü das *Serverzertifikat* aus, das Sie heruntergeladen haben.
- Wählen Sie *Client Authentication aus*. Wenn Sie Passwort auswählen, müssen sie sich mit einem Passwort authentifizieren. Wenn Sie Password + Certificate auswählen, muss der Client auch über ein Zertifikat verfügen. Dies ist sicherer, erhöht jedoch die Kosten für das VPN, da eine separate CA erworben werden muss.
- Geben Sie den *Client-Adresspool ein*. Wählen Sie eine IP-Adresse in einem Netzwerk-Subnetz aus, die nirgendwo anders im Unternehmen verwendet wird. Sie wählen aus den reservierten Bereichen einen Bereich aus, der nirgendwo anders verwendet wird.
- Wählen Sie die Form der *Verschlüsselung aus*. Stellen Sie sicher, dass die Verschlüsselung mit dem Client übereinstimmt. DES und 3DES werden nicht empfohlen und sollten nur zur Abwärtskompatibilität verwendet werden.
- Wählen Sie den *Full-Tunnel-Modus aus*, wenn der gesamte Client-Datenverkehr über den VPN- oder Split-Tunnel geleitet werden soll, wenn Sie nur angeben möchten, welcher Datenverkehr über das VPN läuft.
- Bei der *DNS1*-IP-Adresse kann es sich um einen dedizierten internen DNS-Server, die gleiche IP-Adresse des Standard-Gateways handeln, das vom Internet Service Provider (ISP), auf einem virtuellen System oder einen vertrauenswürdigen DNS-Server im Internet bereitgestellt wird.

Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

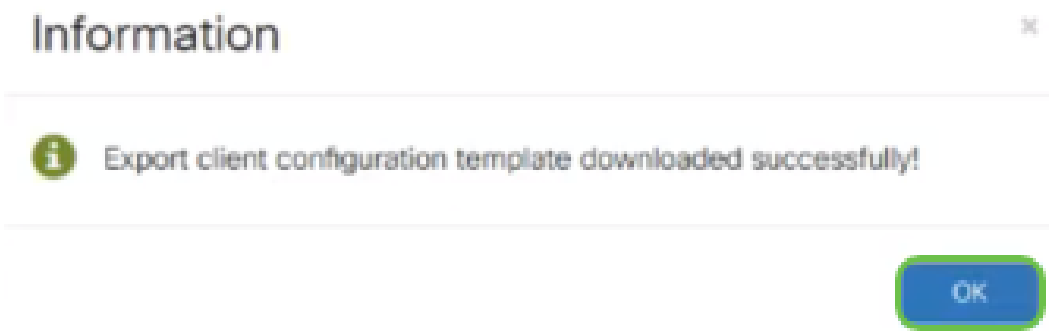
Schritt 19 (Option 1): Sie können diese Konfiguration per E-Mail an den Client senden. Aktivieren Sie das Kontrollkästchen *E-Mail senden*. Geben Sie eine E-Mail-Adresse ein. Fügen Sie einen Betreff-Titel für die E-Mail hinzu. Klicken Sie auf **Generieren**.



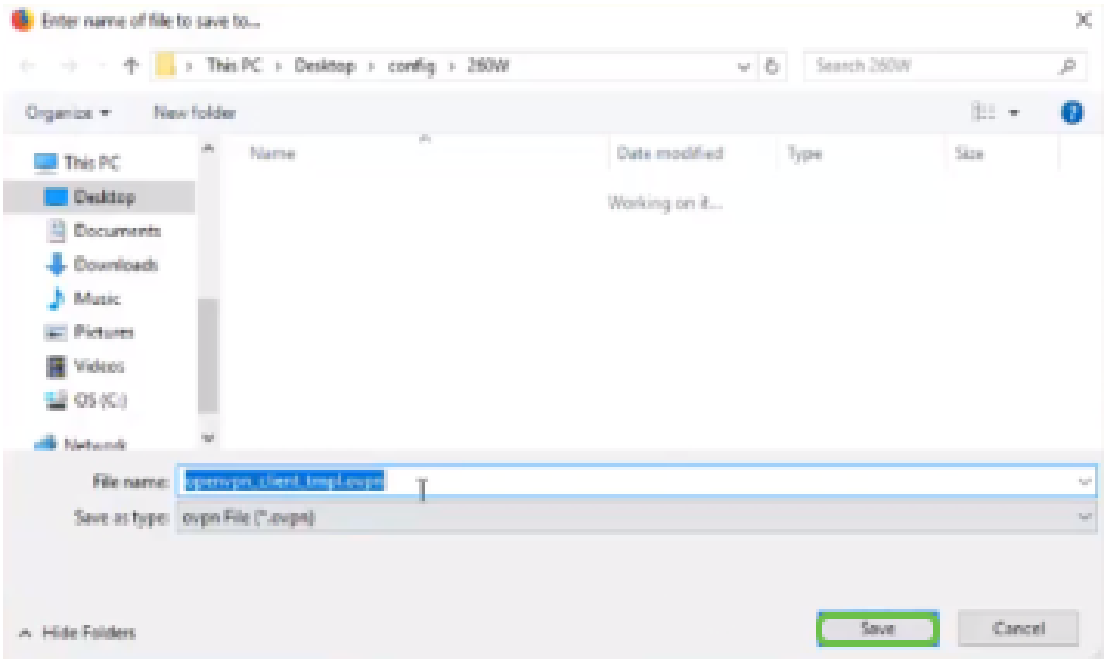
Schritt 20: (Option 2) Wählen Sie *Vorlage für die Client-Konfiguration exportieren (.ovpn)* aus, und klicken Sie auf **Generieren**.



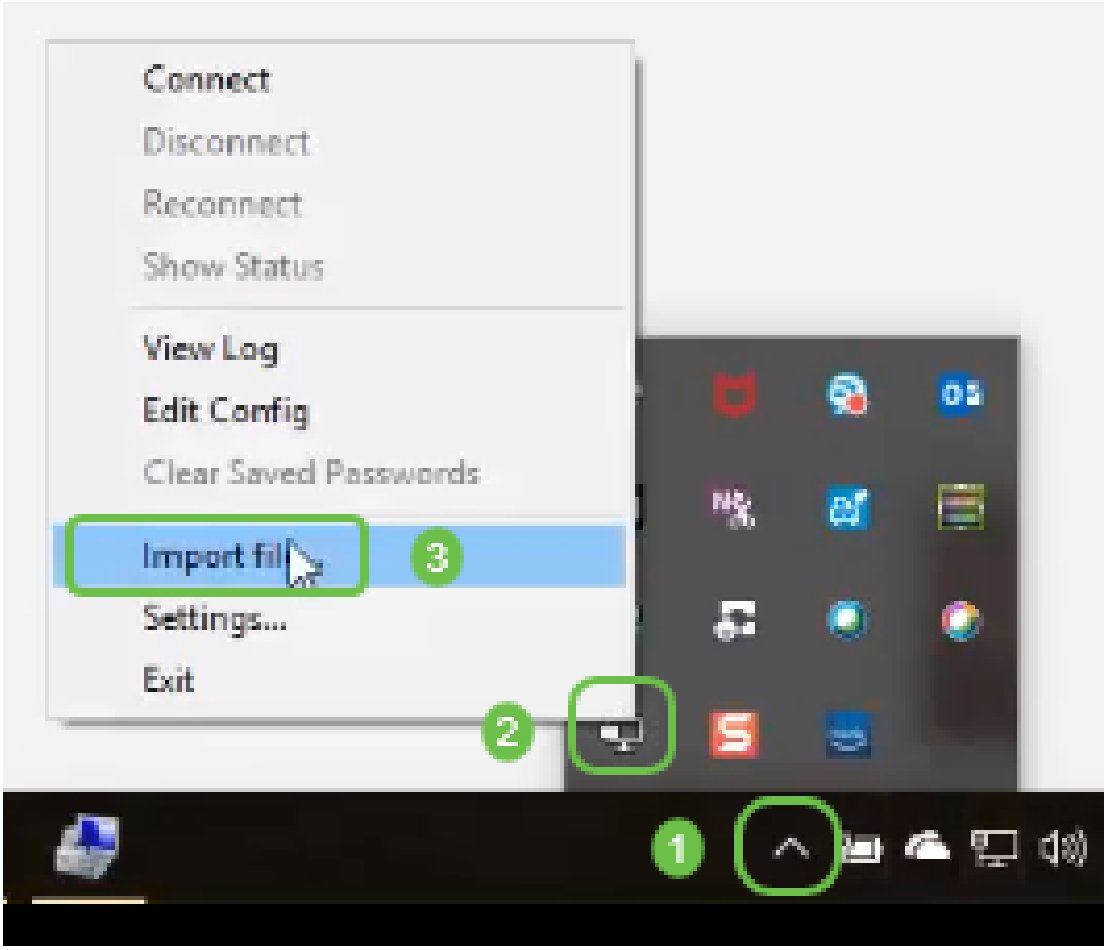
Schritt 21: Sie erhalten eine Bestätigung, dass erfolgreich war. Klicken Sie auf **OK**.



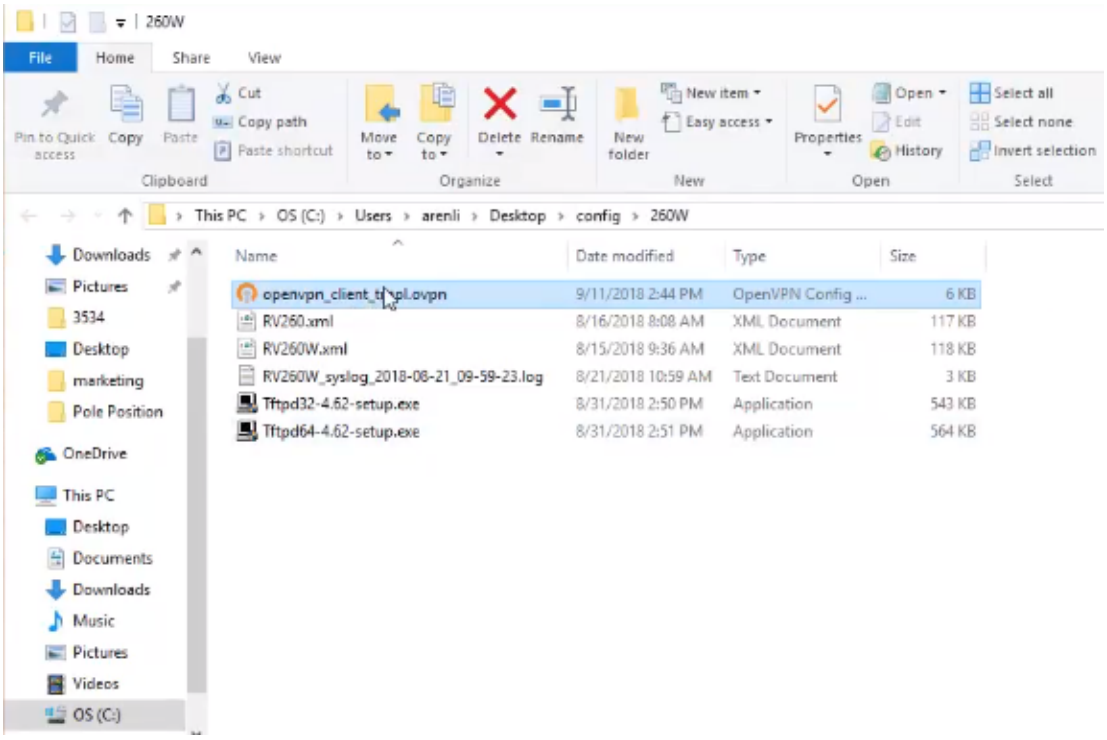
Schritt 22: Klicken Sie auf **Speichern**.



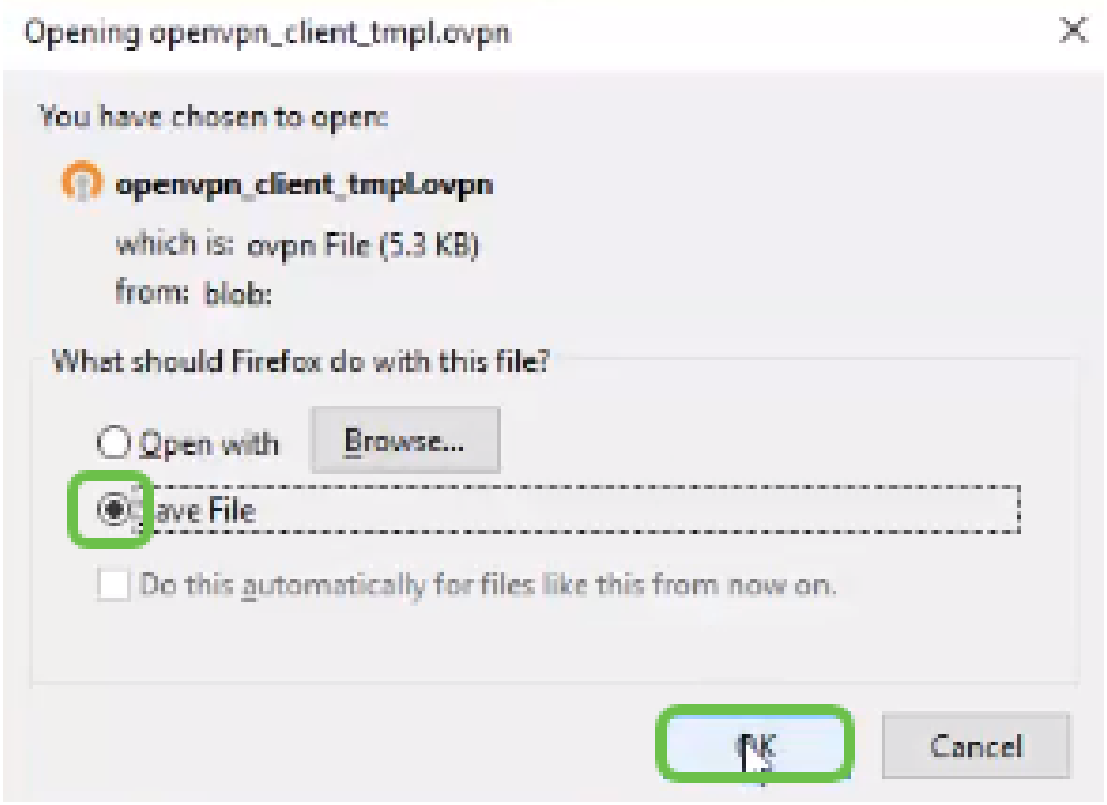
Schritt 23: Klicken Sie unten rechts auf Ihrem Desktop, um OpenVPN zu öffnen. Klicken Sie mit der rechten Maustaste, um das Dropdown-Menü zu öffnen. Klicken Sie auf *Datei importieren*.



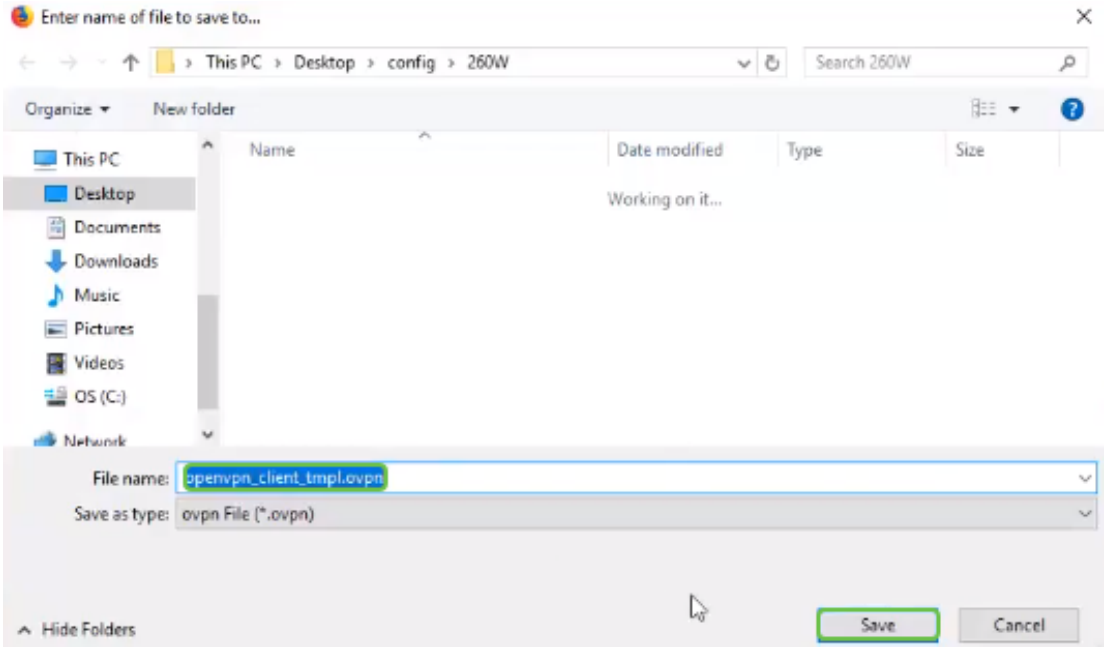
Schritt 24: Wählen Sie die OpenVPN-Datei aus, die in *.ovpn endet*.



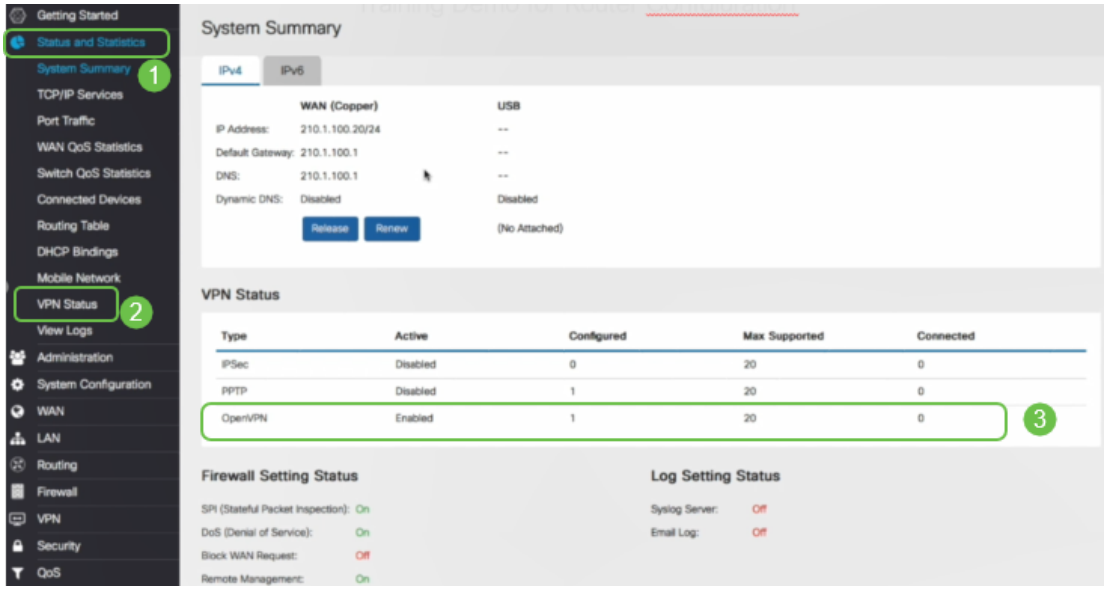
Schritt 25: Klicken Sie auf das Optionsfeld *Datei speichern* und dann auf **OK**.



Schritt 26: Ändern Sie den Namen der Datei, wenn Sie wählen, aber lassen Sie *.ovpn* am Ende des Dateinamens. Klicken Sie auf **Speichern**.



Schritt 27: Navigieren Sie zu **Status und Statistik > VPN Status**. Sie haben die Möglichkeit, nach unten zu scrollen, um detailliertere Informationen zu erhalten.



Der Router ist nun mit allen Parametern konfiguriert, die zur Unterstützung einer OpenVPN-Client-Verbindung für Ihre persönliche Testversion erforderlich sind.

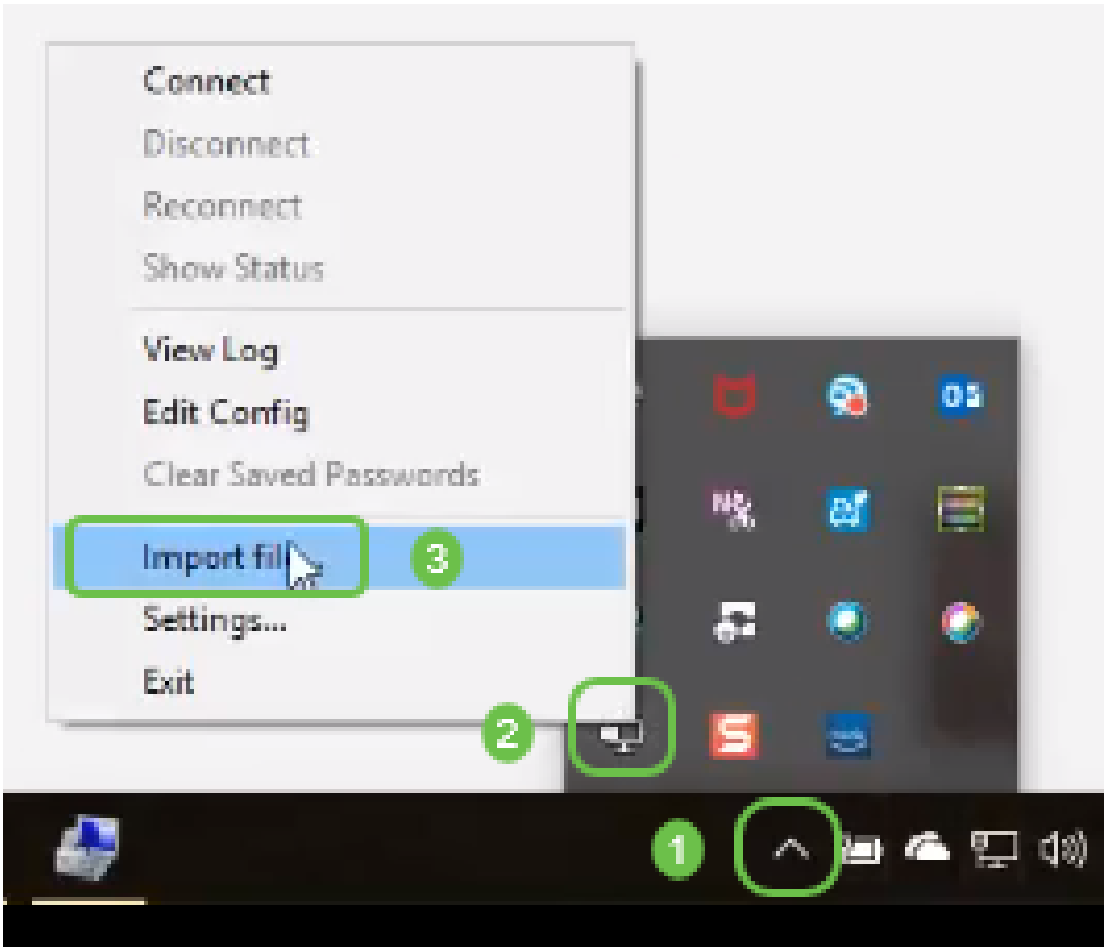
OpenVPN-Client-Setup auf einem Computer

Voraussetzung hierfür ist, dass jeder OpenVPN-Client die folgenden Aufgaben ausführt:

- Laden Sie die OpenVPN-Anwendung auf Ihr Gerät herunter.
- Öffnen und speichern Sie die Konfigurationsdatei, die in den Schritten 19-22 im vorherigen Abschnitt gesendet wurde. Die Konfigurationsdatei endet in *.ovpn*.

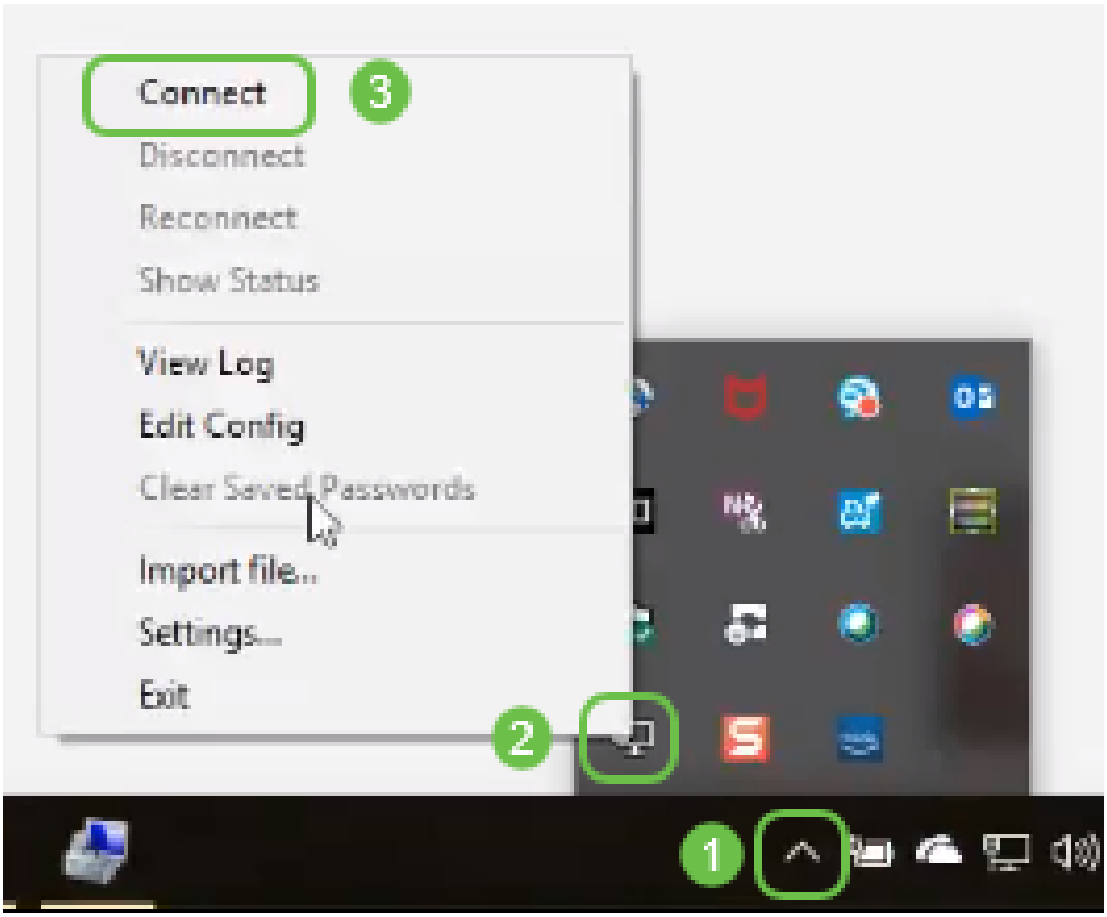
Hinweis: Diese Konfiguration ist speziell für Windows 10 bestimmt.

Schritt 1: Navigieren Sie zum Pfeilsymbol unten rechts auf dem Desktop, und klicken Sie, um das OpenVPN-Symbol zu öffnen. Klicken Sie mit der rechten Maustaste, und wählen Sie *Datei importieren aus*.

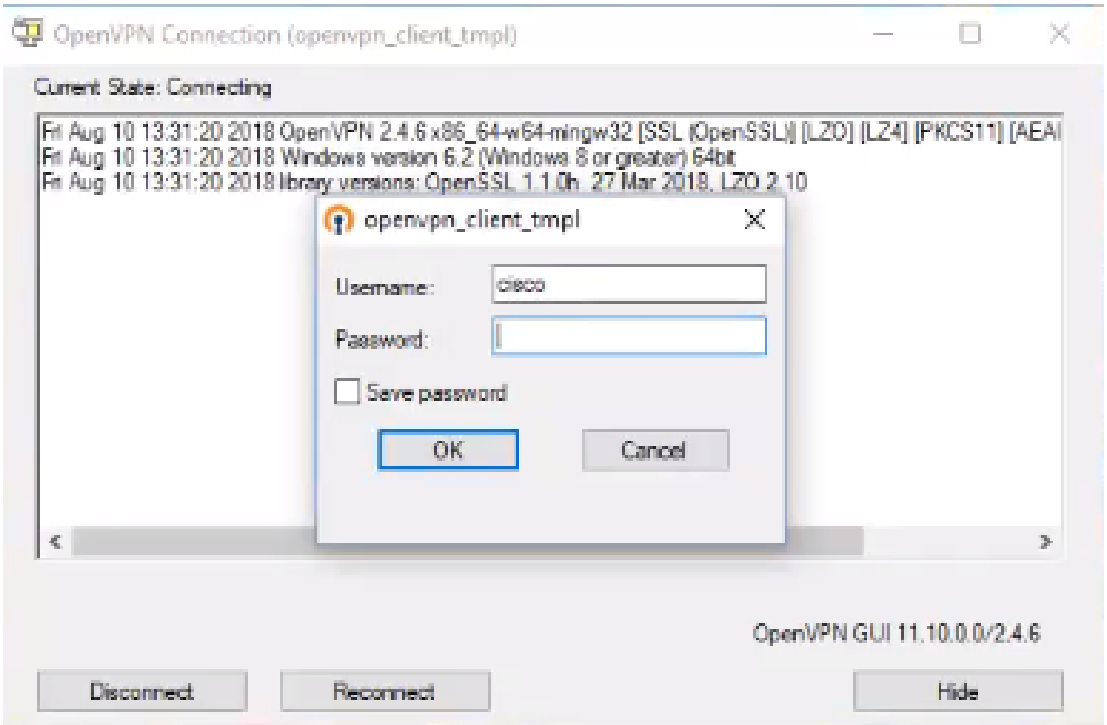


Hinweis: Das Symbol ist schwarz-weiß und zeigt an, dass es derzeit nicht ausgeführt wird. Sobald das Symbol ausgeführt wird, wird es farbig angezeigt.

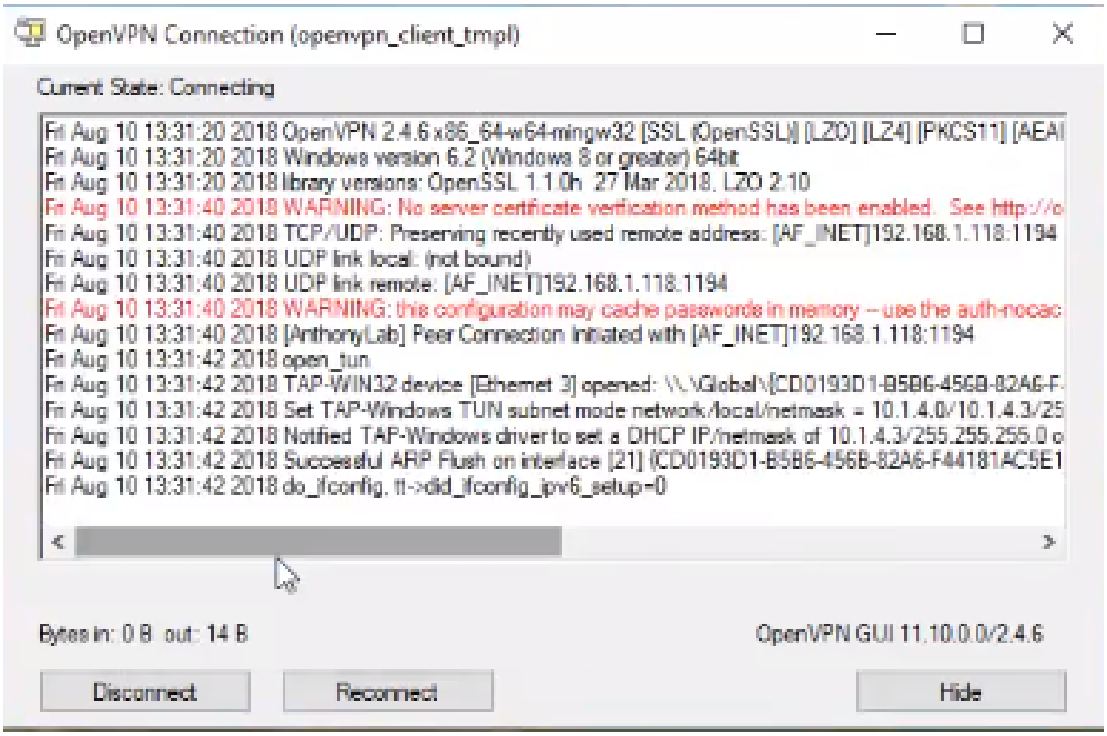
Schritt 2: Klicken Sie auf den *Pfeil nach oben*. Klicken Sie auf das Symbol OpenVPN. Klicken Sie mit der rechten Maustaste, und wählen Sie *Connect* aus dem Dropdown-Menü aus.



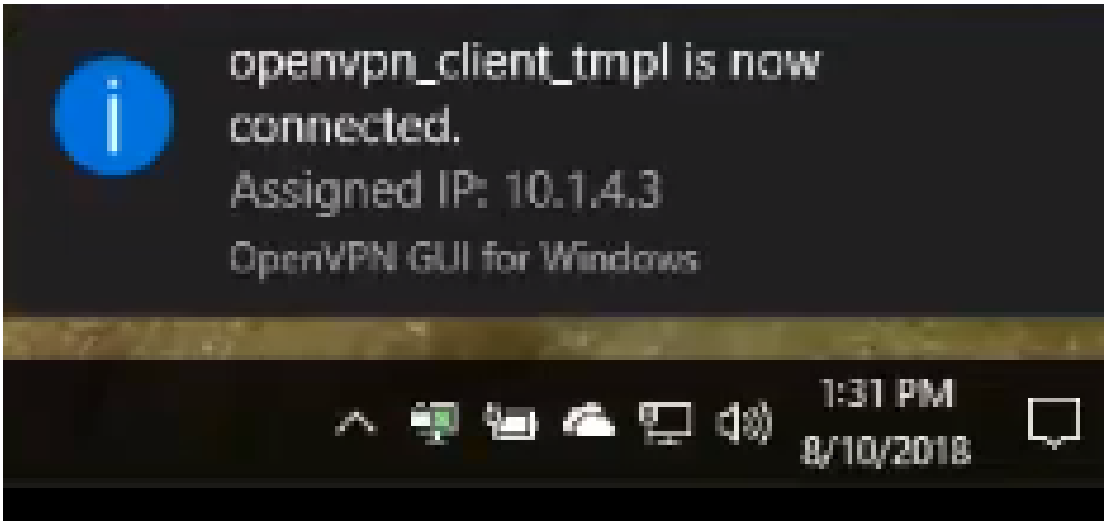
Schritt 3: Geben Sie den *Benutzernamen* und das *Kennwort ein*.



Schritt 4: Das Fenster zeigt die OpenVPN-Verbindung mit einigen Protokolldaten an.

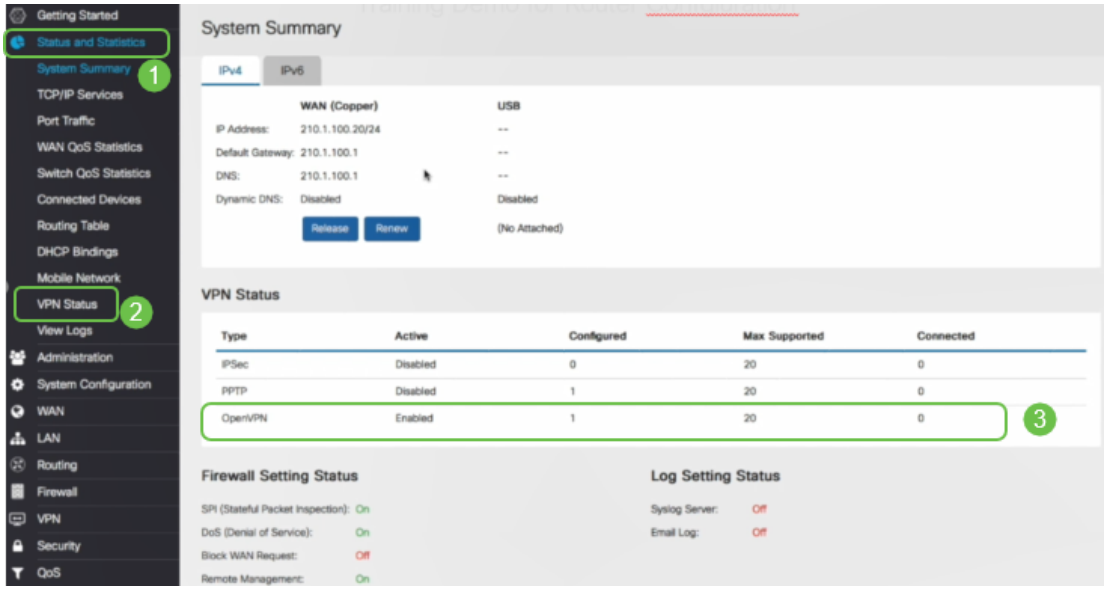


Schritt 5: Ein Systemprotokoll sollte eine Warnmeldung ausgeben, dass eine Verbindung besteht.



Schritt 6: Der VPN-Client sollte in der Lage sein, eingehende und ausgehende Informationen sicher über OpenVPN zu tunneln. Dies kann so eingestellt werden, dass eine automatische Verbindung in den OpenVPN-Einstellungen hergestellt wird.

Schritt 7: Der Administrator kann den VPN-Status bestätigen, indem er auf dem Router zu **Status und Statistics > VPN Status** navigiert.



Schlussfolgerung

Sie sollten OpenVPN jetzt erfolgreich auf Ihrem RV160- oder RV260-Router und am VPN-Client-Standort installiert haben.

Für Community-Diskussionen über OpenVPN klicken Sie hier und suchen Sie nach OpenVPN.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.