

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

[Einrichten einer OpenVPN-Demo auf einem RV160/RV260-Router](#)

[Einrichten von OpenVPN auf einem RV160/RV260-Router](#)

[Anmelden mit einem selbst signierten Zertifikat nach dem Einrichten von OpenVPN-Demos](#)

[OpenVPN-Client-Setup auf einem Computer](#)

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

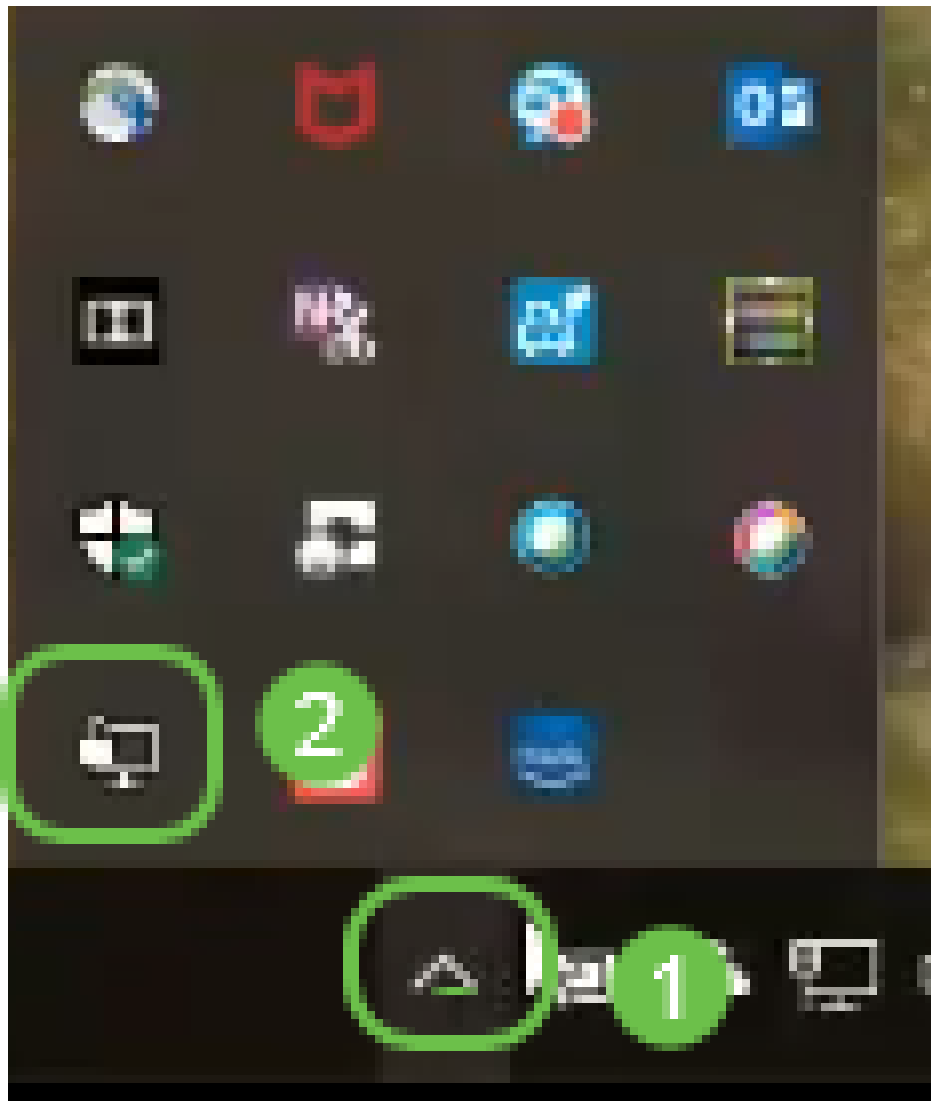
Installieren Sie die OpenVPN-Anwendung auf Ihrem System. Klicken Sie [hier](#), um zur OpenVPN-Website zu gelangen.

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.



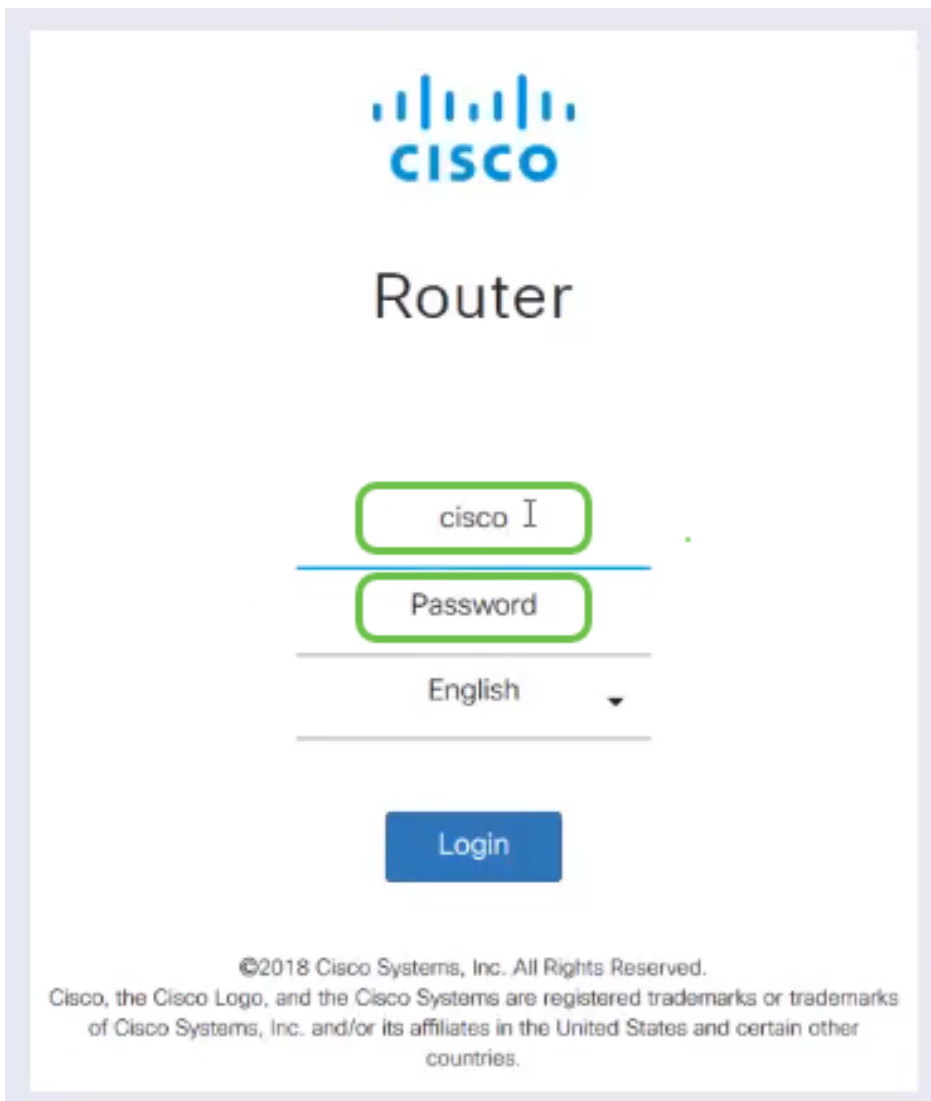
Stellen Sie sicher, dass auf allen Geräten die korrekte Systemzeit eingerichtet ist. Die korrekte Systemzeit muss vor der Erstellung eines Zertifikats am Router vollständig synchronisiert werden. Oft wird dies automatisch durchgeführt, aber wenn Sie auf Probleme stoßen, ist dies ein guter Ort zu überprüfen.

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.

RV260-PnP Demo

Alert cisco(admin) English

Certificate

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		
2	CertT...	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterIm...	-	Local Certificate	CiscoTest-DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

[Import Certificate...](#)
[Generate CSR/Certificate...](#)
[Show built-in 3rd party CA Certificates...](#)
[Select as Primary Certificate...](#)

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 Domännennamen (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.

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		
2	CertT	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterIm...	-	Local Certificate	CiscoTest-DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

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 Domännennamen (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.

Group	Web Login /NETCONF /RESTCONF	Lobby Ambassa...	802.1x	S2S IPSec VPN	G2S IPSec VPN	OpenVPN	PPTP	Captive Portal
<input type="checkbox"/>	Ambassa...	Disable	Enable	Disable	Disable	Disable	Disable	Enable
<input type="checkbox"/>	admin	Admin	Enable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	guest	Disable	Disable	Disable	Disable	Disable	Disable	Disable

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

User Groups

3 Apply Cancel

Group Name: OpenVPN 1

Local User Membership List

+

<input type="checkbox"/>	#	User

* Should have at least one account in the 'admin' group.

Services

Web Login/NETCONF/RESTCONF: Disable Readonly Admin

Site to Site VPN:

+

<input type="checkbox"/>	#	Connection Name

Client to Site VPN:

+

<input type="checkbox"/>	#	Group Name

OpenVPN: 2 On Off

PPTP VPN: On Off

802.1x: On Off

Lobby Ambassador: On Off

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

- Getting Started
- Status and Statistics
- Administration
- System Configuration
- Initial Router Setup
- System
- Time
- Log
- Email
- User Accounts 1
- User Groups
- IP Address Groups
- SNMP
- Discovery-Bonjour
- LLDP
- Automatic Updates
- Schedules

User Accounts

Apply Cancel

Minimal Password Length: (Range: 0-64, Default: 8)

Minimal Number of Character Classes: (Range: 0-4, Default: 3)

The four classes are: uppercase (A,B,C...), lowercase (a,b,c...), numbers (1,2,3...) and special characters (!@#\$...).

The new password must be different from the current one.: Enabled

Password Aging Time: days (Range: 0-365, 0 means never expires)

Local Users


+

<input type="checkbox"/>	Username	Group
<input type="checkbox"/>	Test_Admin	Ambassador
<input type="checkbox"/>	cisco	admin
<input type="checkbox"/>	guest	guest

* Should have at least one account in the 'admin' group.

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

Add user account

 The current minimum requirements are as follows

* Minimal Password Length: 8

* Minimal Number of Character Classes: 3

Username:

1

VPN

New Password:

●●●●●●●●

Confirm Password:

●●●●●●●●

Password Strength meter:



Group:

OpenVPN

2

Apply

Cancel

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.

Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
Wireless
Routing
Firewall
VPN 1
VPN Setup Wizard
IPSec VPN
OpenVPN 2

OpenVPN 5 Apply Cancel

Enable: 3

Interface: 4 All

CA Certificate: 4 A_Trust_...

Server Certificate:

Client Authentication: Password Only

Client Address Pool: 10.1... Netmask: 255.255.255.0

Protocol: UDP Port: 1194

Encryption: AES-256

Tunnel Mode:
 Full Tunnel, routing all client traffic through VPN
 Split Tunnel, routing client traffic destined to the following subnets through VPN

- 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 *Domännennamen* und *DNS1* aus.

Domain Name:	<input type="text" value="Openvpn.net"/>
DNS1:	<input type="text" value="192.168.1.1"/>

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.

Export setting:

Include client certificate:

Please choose the method you want to export:

1 Export client configuration template (.ovpn)

Send Email [Click here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma):

Email Subject:

2

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

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, 'System Summary' is highlighted with a green circle containing the number '1', and 'VPN Status' is highlighted with a green circle containing the number '2'. The main content area is titled 'System Summary' and has tabs for 'IPv4' and 'IPv6'. Under 'WAN (Copper)', it shows IP Address: 210.1.100.20/24, Default Gateway: 210.1.100.1, and DNS: 210.1.100.1. There are 'Release' and 'Renew' buttons. Under 'VPN Status', there is a table with columns: Type, Active, Configured, Max Supported, and Connected. The 'OpenVPN' row is highlighted with a green border and has a green circle with the number '3' next to it. Below the table are sections for 'Firewall Setting Status' and 'Log Setting Status'.

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**.



Your connection is not private

Attackers might be trying to steal your information from [redacted].net (for example, passwords, messages, or credit cards). [Learn more](#)
NET::ERR_CERT_AUTHORITY_INVALID

Help improve Safe Browsing by sending some [system information and page content](#) to Google. [Privacy policy](#)

ADVANCED

BACK TO SAFETY

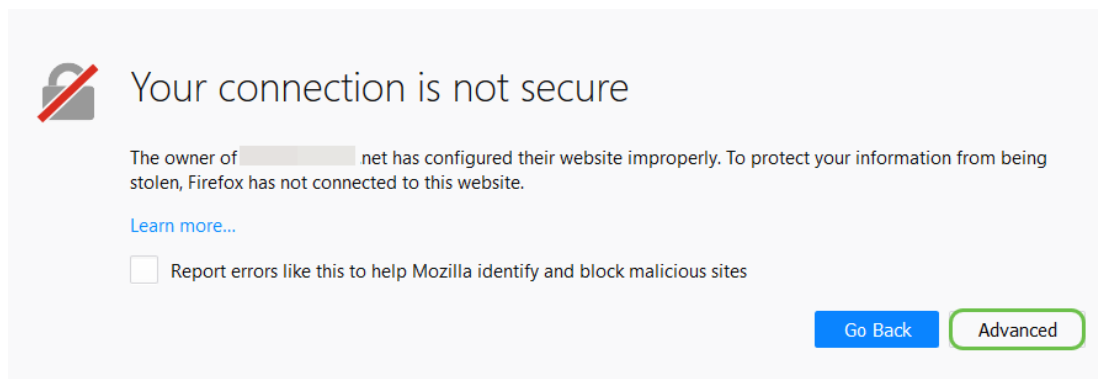
Ein neuer Bildschirm wird geöffnet, und Sie müssen auf **Weiter zu Ihrer Website.net** klicken

(unsafe).

This server could not prove that it is **net**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

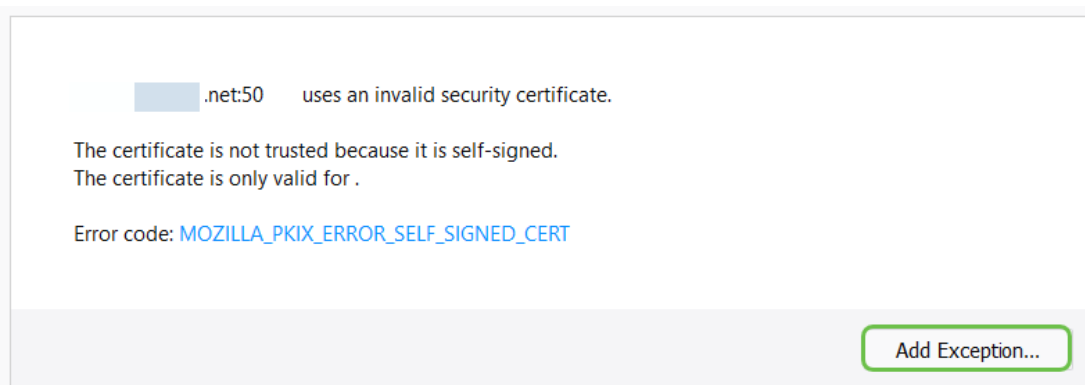
Proceed to **net** (unsafe)

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



The screenshot shows a security warning dialog box. At the top left is a red padlock icon with a diagonal slash. The main heading is "Your connection is not secure". Below this, a paragraph explains that the website owner has configured the site improperly, and Firefox has not connected to protect information. A "Learn more..." link is provided. There is a checkbox labeled "Report errors like this to help Mozilla identify and block malicious sites". At the bottom right, there are two buttons: "Go Back" (blue) and "Advanced" (green).


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



The screenshot shows a detailed security error dialog box. It states that ".net:50" uses an invalid security certificate. It explains that the certificate is not trusted because it is self-signed and only valid for ".net:50". The error code is "MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT". At the bottom right, there is a green button labeled "Add Exception...".

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

Add Security Exception ✕

 You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location:

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

Permanently store this exception

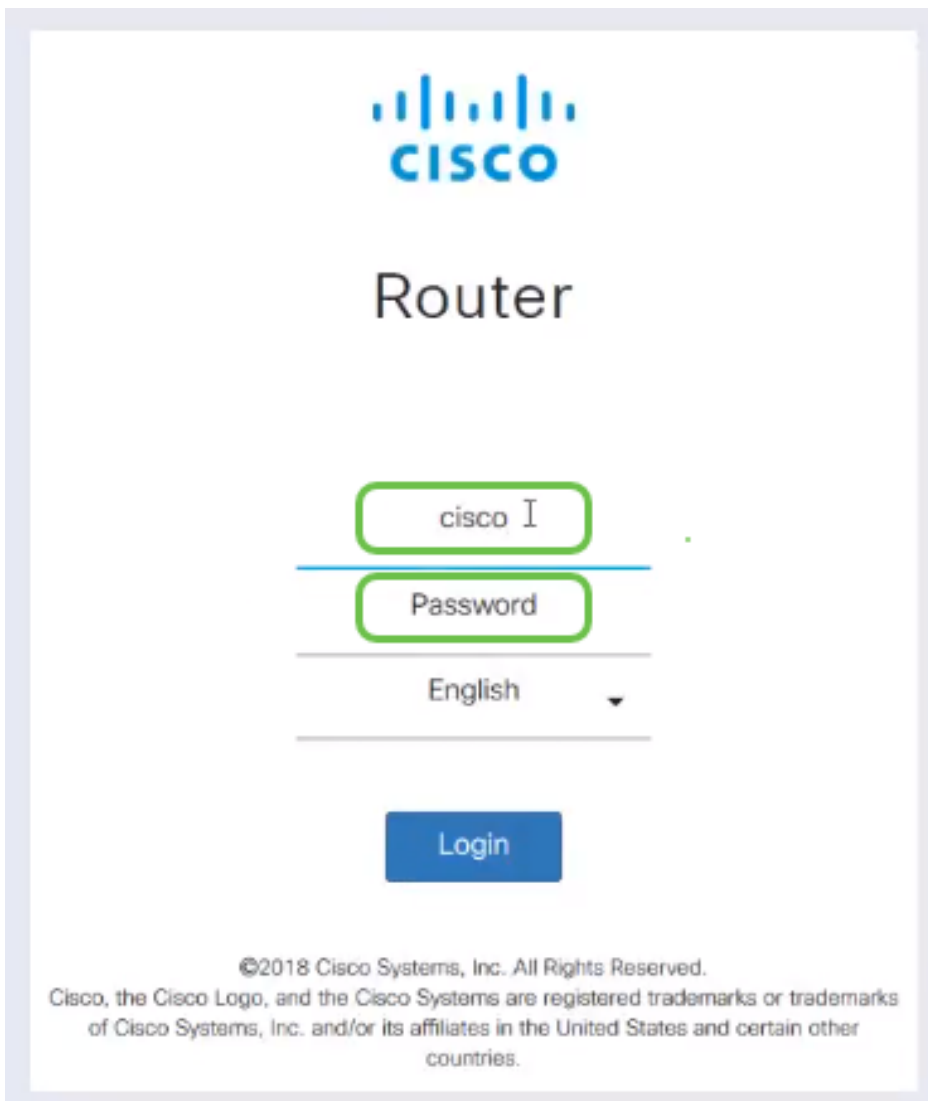
Der Router ist nun mit allen Parametern konfiguriert, die zur Unterstützung einer OpenVPN-Client-Verbindung erforderlich sind. Da Sie die Client-Konfigurationsvorlage bereits auf Ihr Gerät heruntergeladen haben, das in `.ovpn endet`, können Sie mit dem Abschnitt [OpenVPN Client Setup on Computer](#) 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.

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		
2	CertT		CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterIm...	-	Local Certificate	CiscoTest-DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

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 Domännennamen (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

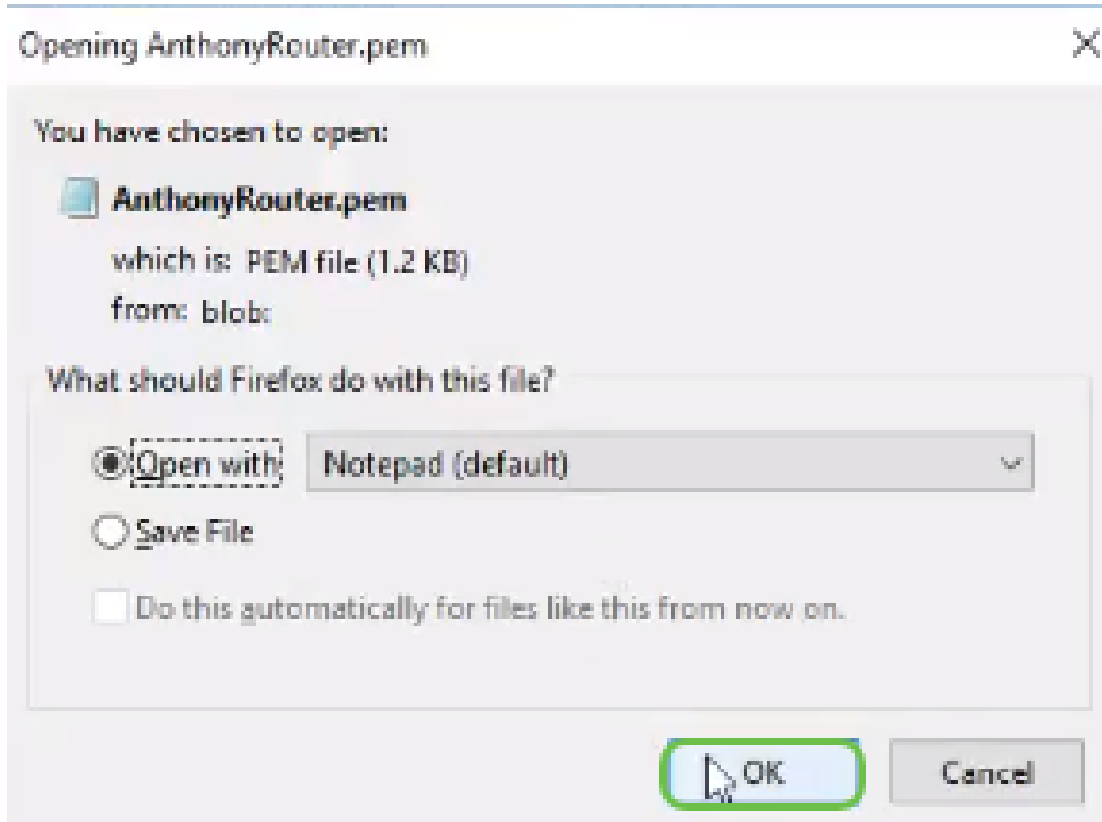
Schritt 4: Wählen Sie diese Option aus, indem Sie unter Aktion auf den Pfeil nach oben klicken.

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		
2	CertTest_CA	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterImport	-	Local Certificate	CiscoTest-DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

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.

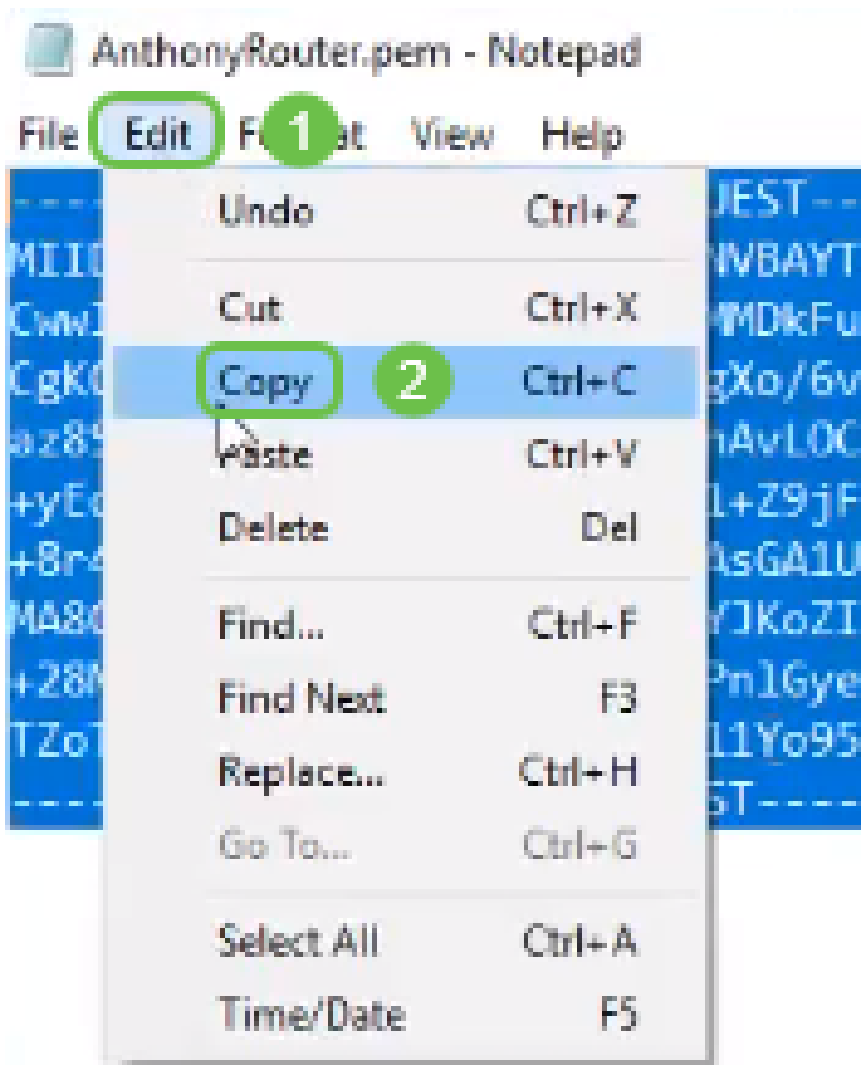


Schritt 7: Eine XML-Datei wird geöffnet.



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.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
TZoTKHXBcMTWpCh1jPFyALeNH811Yo95aBO2WX2e  
cUNT4jUzYNYaV7XkREz7oY1PF5TZW9KzzAIoZW8a  
3qO6K2H=  
  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

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

Certificate Issued

The certificate you requested was issued to you.

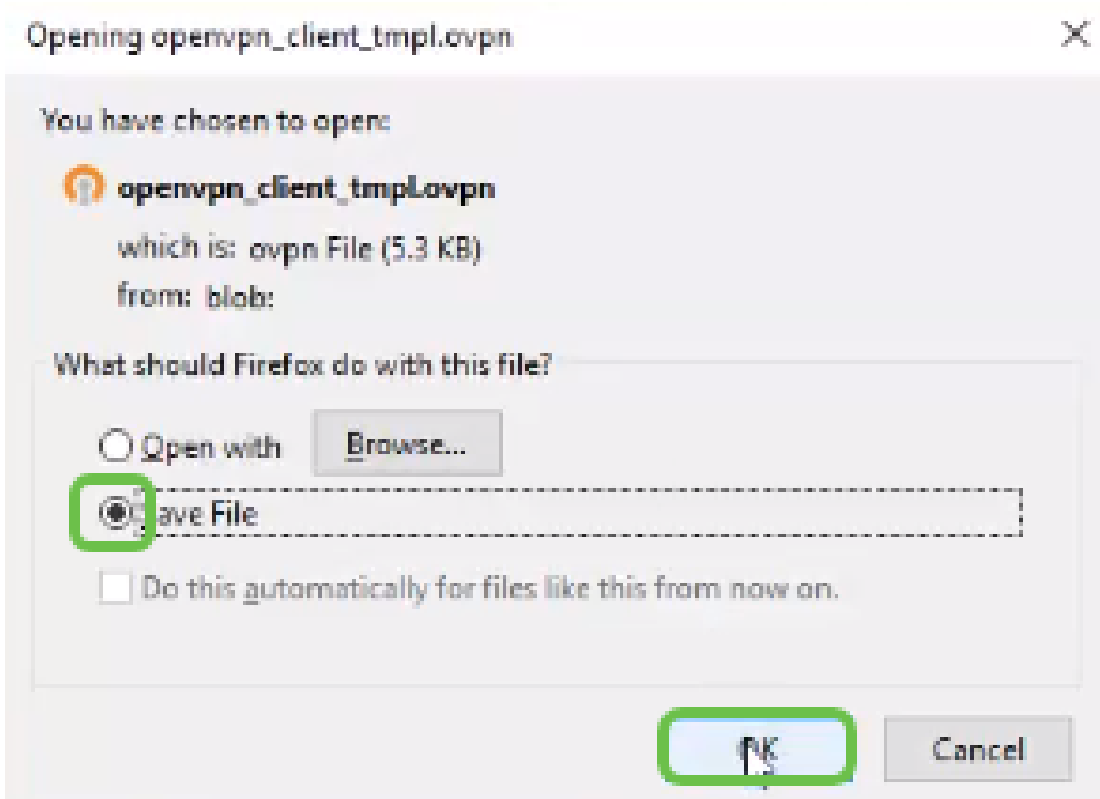
DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

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.

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		
2	CertTest_CA	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	Certimport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterimport	-	Local Certificate	CiscoTest-DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

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

Import Signed-Certificate


Type: Local Certificate

Certificate Name:

Upload Certificate file

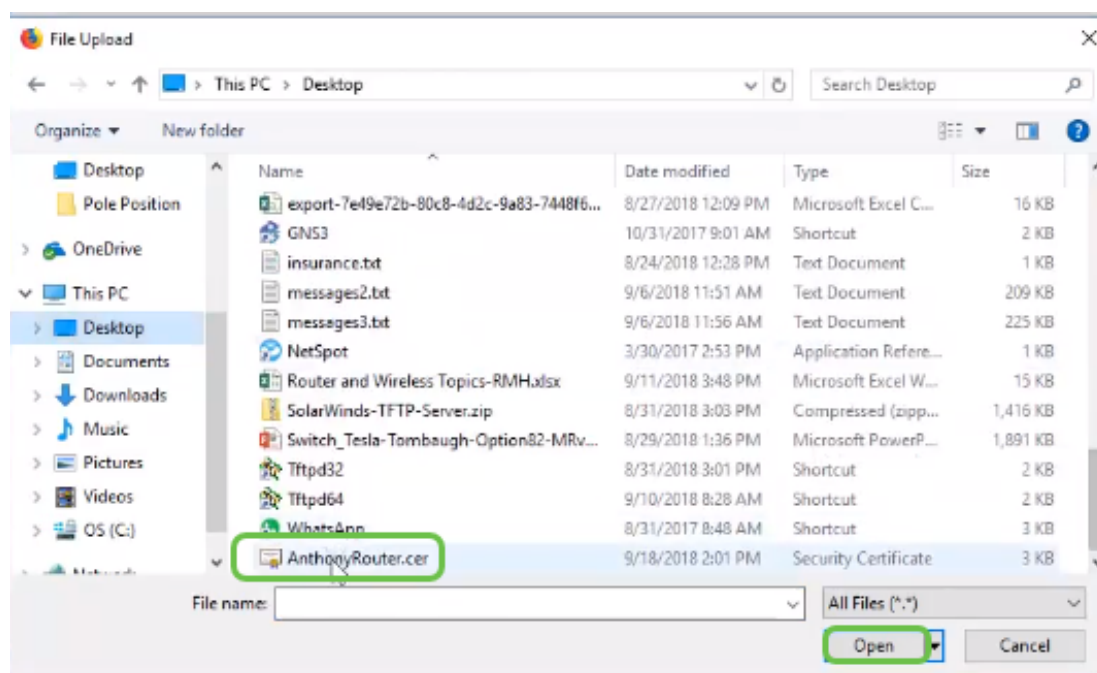
Import from PC

No file is selected

Import from USB 

No file is selected

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**.

Import Signed-Certificate



Type: Local Certificate

Certificate Name: AnthonyRouterImport

Upload Certificate file

Import from PC

Browse...

AnthonyRouter.cer

Import from USB



Browse...

No file is selected

Upload

Cancel

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

Information



Import certificate successfully!

OK

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

Hinweis: In diesem Beispiel wurde ein lokaler Zertifikatsserver verwendet.

The screenshot shows the Cisco configuration interface for a device (RV260-PrPDemo). The left sidebar shows the navigation menu with 'Administration' selected. The main content area displays the 'Certificate' configuration page. A table titled 'Certificate Table' lists the following certificates:

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		
2	CertTest_CA	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-OC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterImport	-	Local Certificate	CiscoTest-OC1-CP	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

At the bottom of the page, there are four buttons: 'Import Certificate', 'Generate CSR/Certificate', 'Show built-in 3rd party CA Certificates', and 'Select as Primary Certificate'.

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

The screenshot shows the 'OpenVPN' configuration page on a Cisco RV260W-RV260 router. The left sidebar contains navigation options: Administration, System Configuration, WAN, LAN, Wireless, Routing, Firewall, VPN (1), VPN Setup Wizard, IPsec VPN, OpenVPN (2), PPTP Server, GRE Tunnel, VPN Passthrough, and Resource Allocation. The main configuration area includes:

- Enable:** Checked (3)
- Interface:** All
- CA Certificate:** A_Trust_nQual_03
- Server Certificate:** (4)
- Client Authentication:** Password Only
- Client Address Pool:** 10.1.4.0, **Netmask:** 255.255.255.0
- Protocol:** UDP, **Port:** 1194
- Encryption:** AES-256
- Tunnel Mode:**
 - Full Tunnel, routing all client traffic through VPN
 - Split Tunnel, routing client traffic destined to the following subnets through VPN

 Buttons for 'Apply' and 'Cancel' are visible at the top right, with a '5' next to 'Apply'.

- 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 Passwort + 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**.

Export setting:

Include client certificate: AnthonyRouterImport

Please choose the method you want to export:

1 Export client configuration template (.ovpn)

Send Email Click [here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): nick@cisco.com

Email Subject: OpenVPN Client Config

4

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

Export setting:

Include client certificate:

Please choose the method you want to export:

1 Export client configuration template (.ovpn)

Send Email Click [here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): input email address

Email Subject: OpenVPN Client Configurat

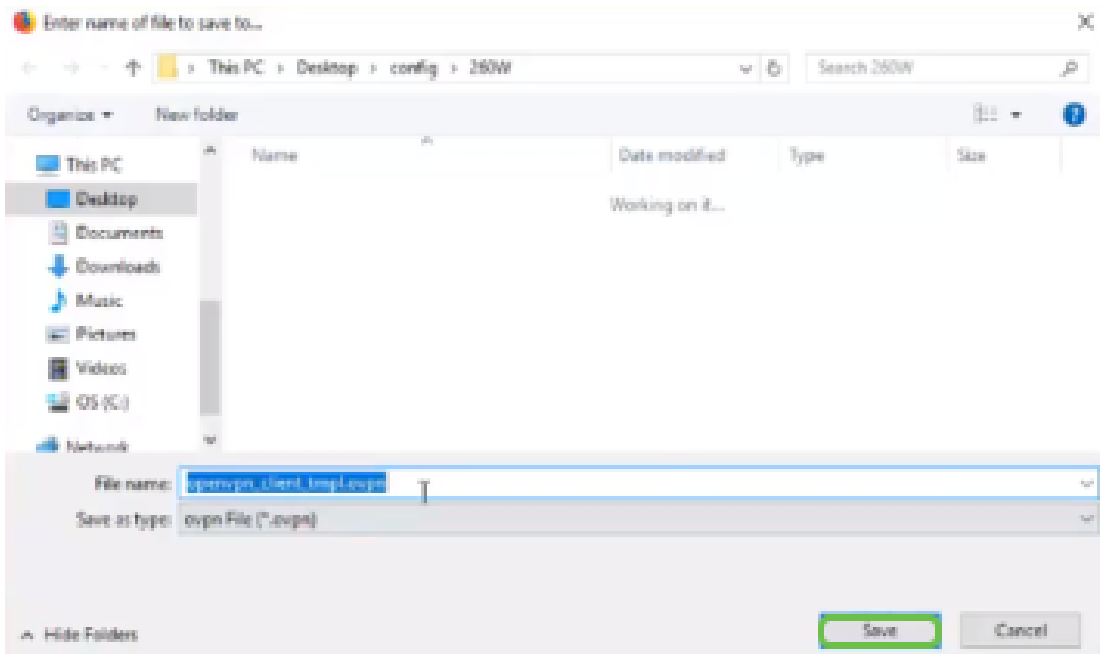
2

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

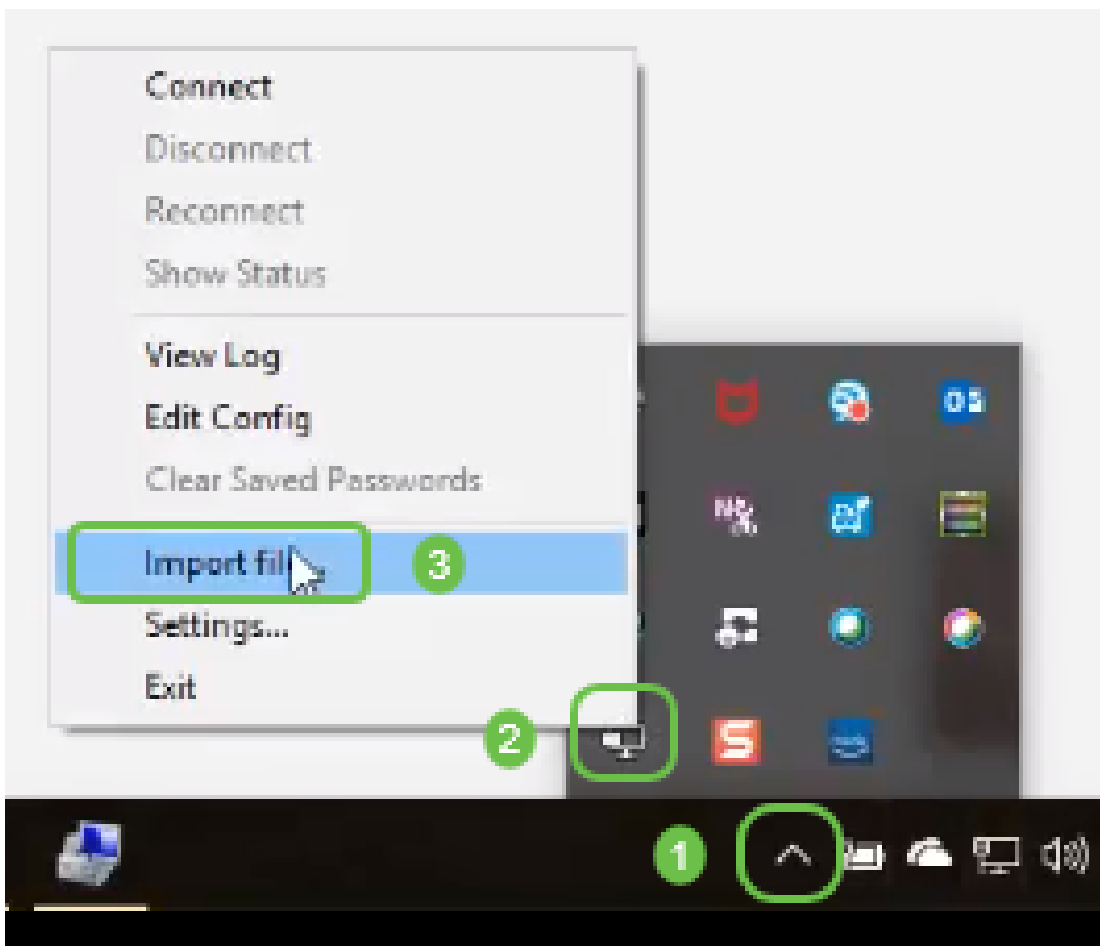
Information

 Export client configuration template downloaded successfully!

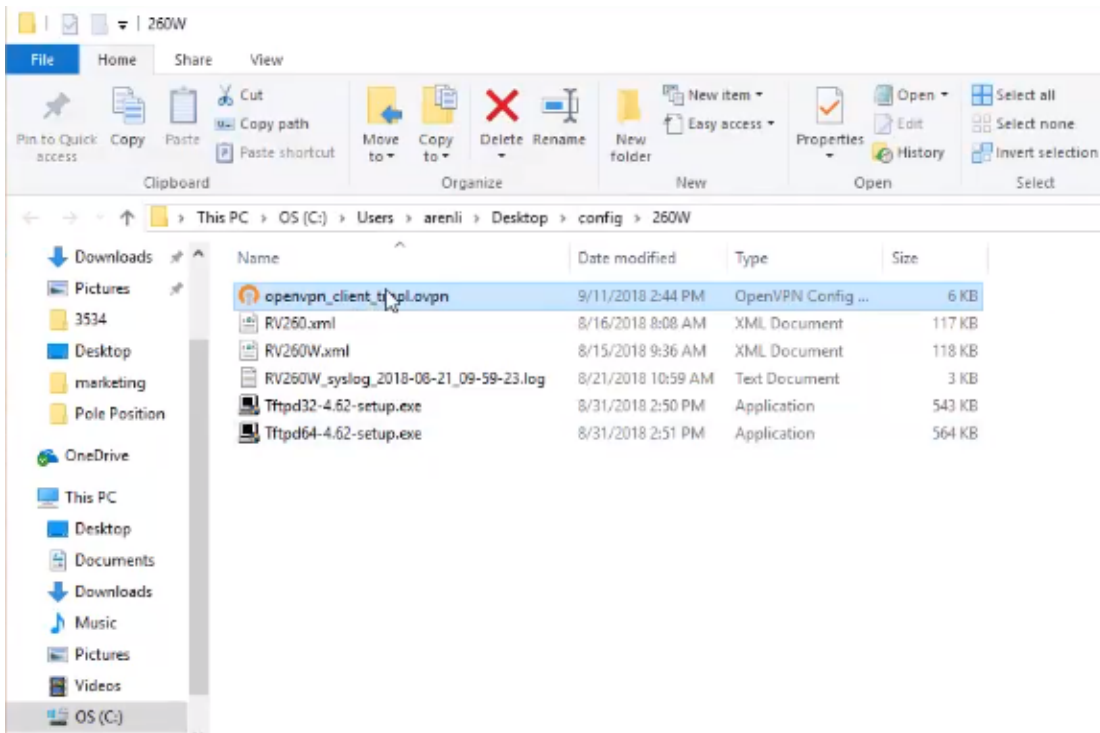
Schritt 22: Klicken Sie auf **Speichern**.



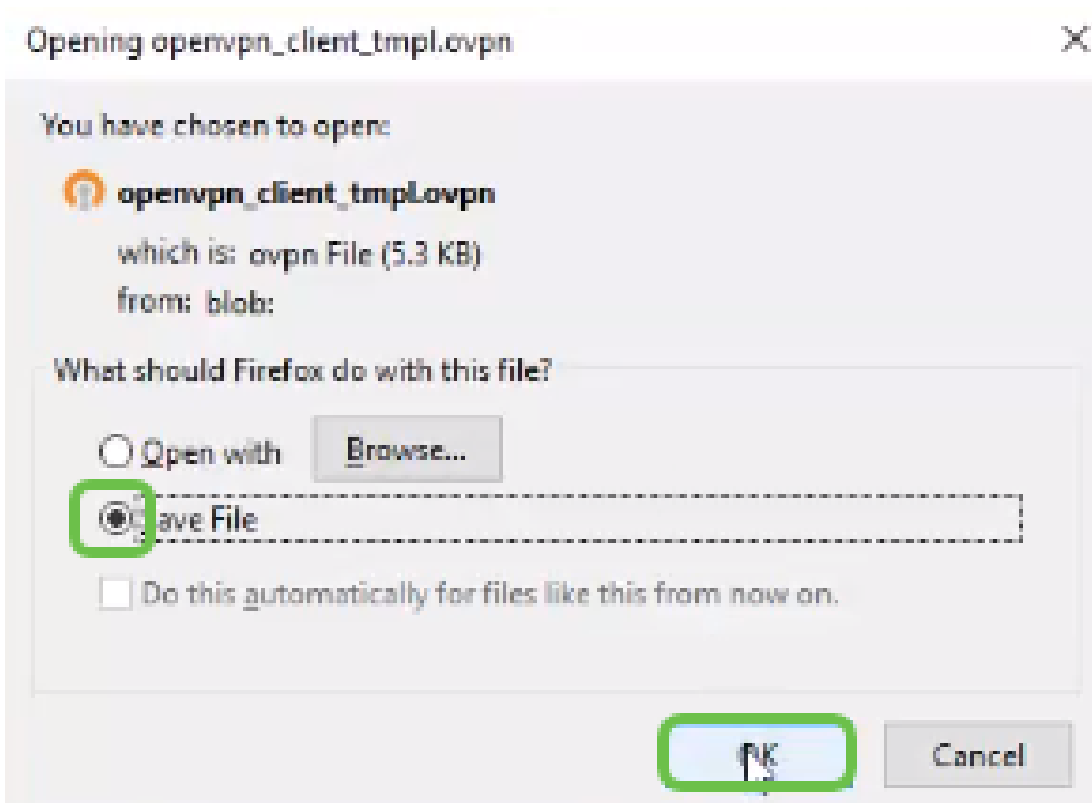
Schritt 23: Klicken Sie unten rechts auf Ihrem Desktop, um OpenVPN zu öffnen. Klicken Sie mit der rechten Maustaste, um das Dropdown-Menü zu öffnen. Klicken Sie auf *Datei importieren*.



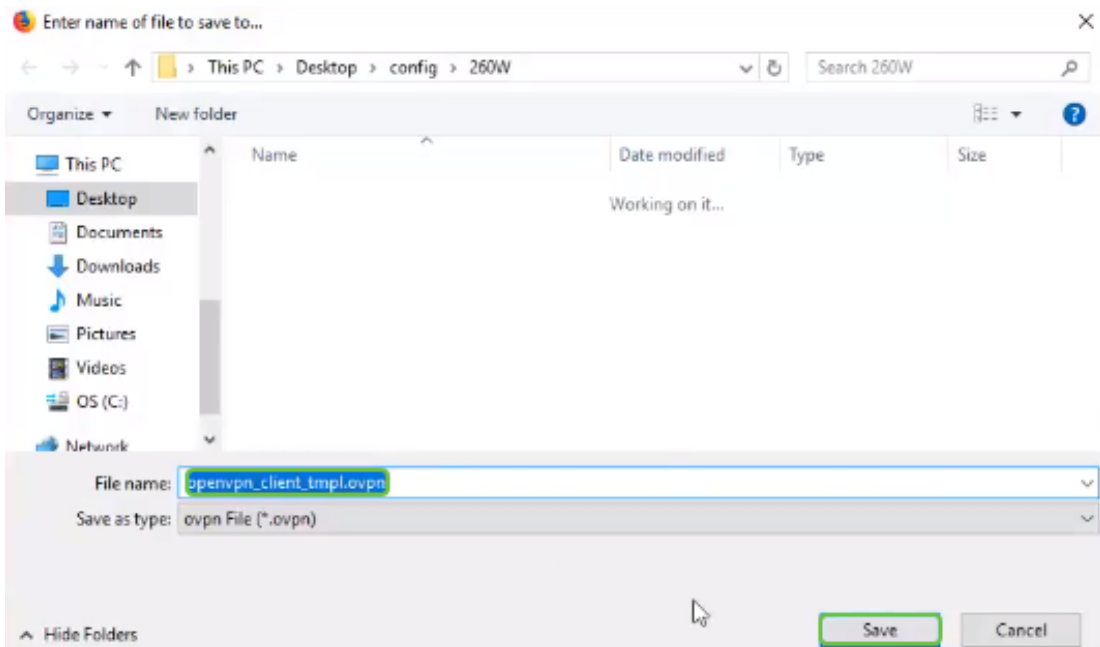
Schritt 24: Wählen Sie die OpenVPN-Datei aus, die in *.ovpn endet*.



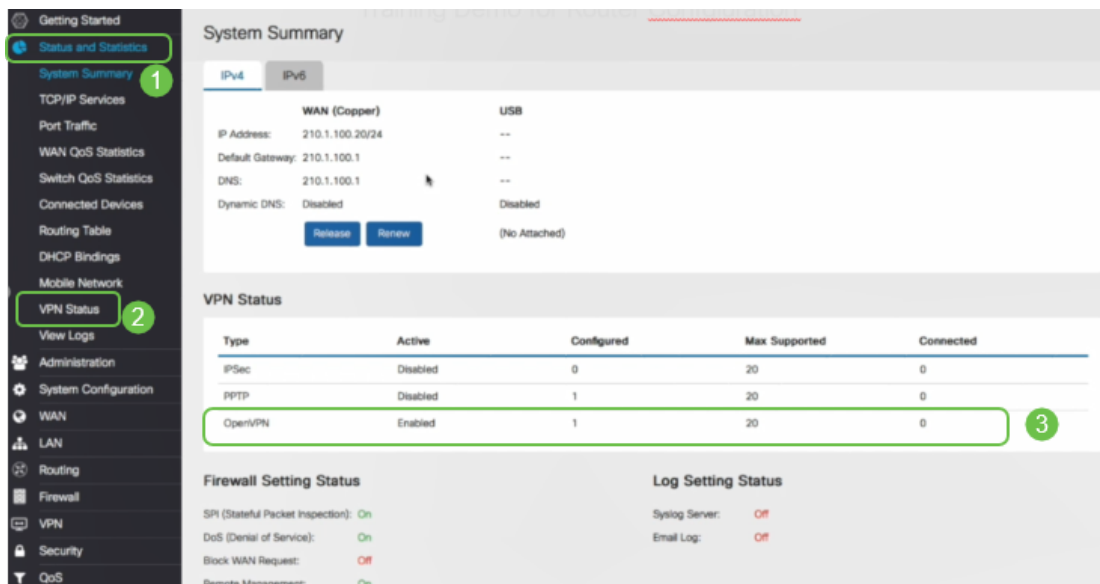
Schritt 25: Klicken Sie auf das Optionsfeld *Datei speichern* und dann auf **OK**.



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.

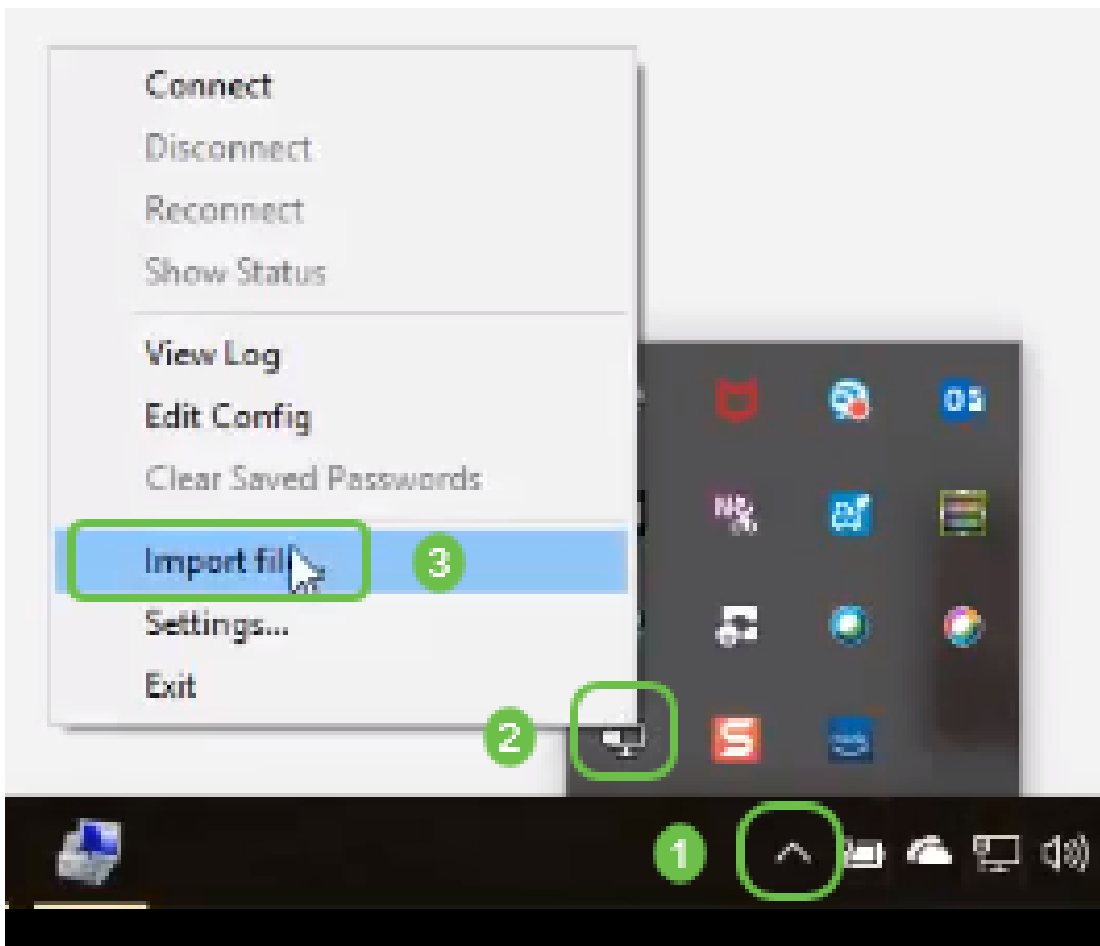
OpenVPN-Client-Setup auf einem Computer

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*.

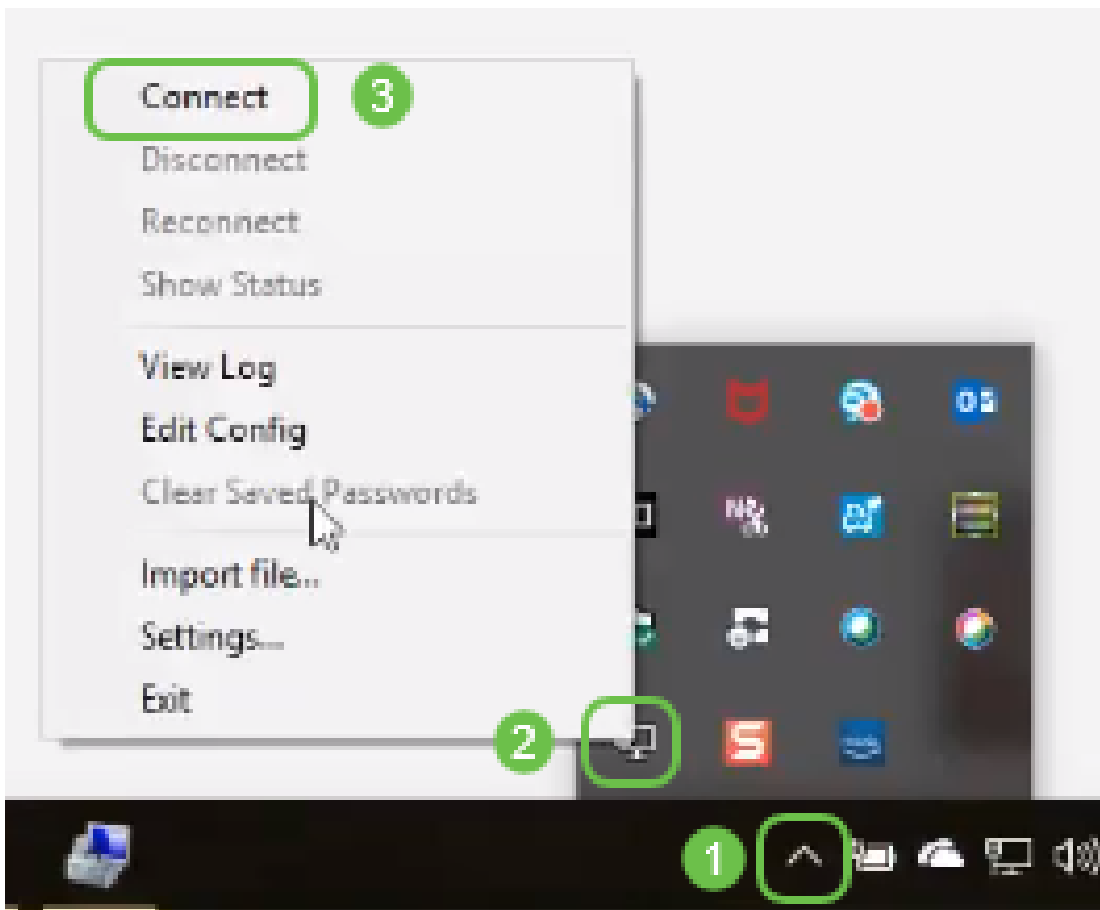
Hinweis: Diese Konfiguration ist speziell für Windows 10 bestimmt.

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*.

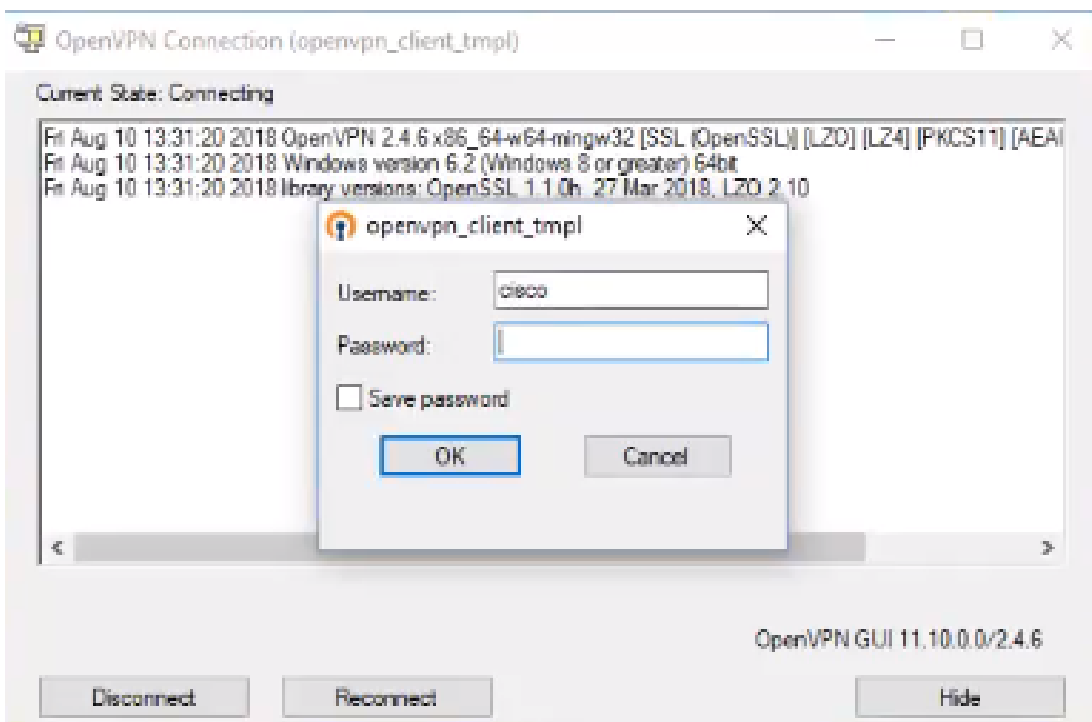


Hinweis: Das Symbol ist schwarz-weiß und zeigt an, dass es derzeit nicht ausgeführt wird. Sobald das Symbol ausgeführt wird, wird es farbig angezeigt.

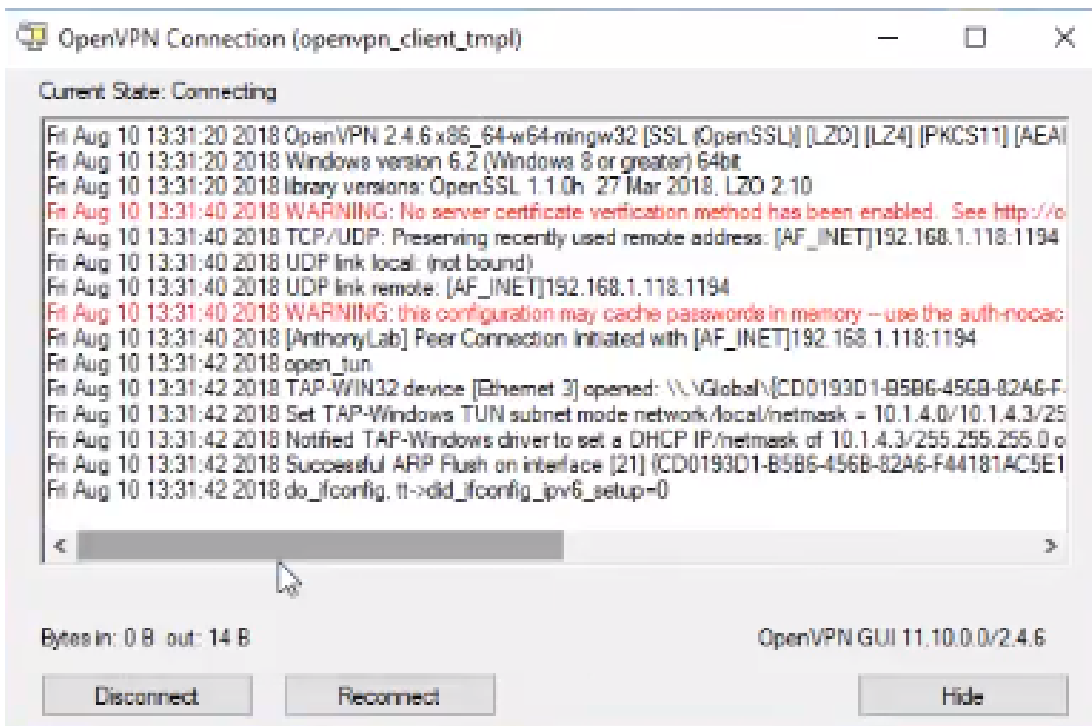
Schritt 2: Klicken Sie auf den *Pfeil nach oben*. Klicken Sie auf das Symbol OpenVPN. Klicken Sie mit der rechten Maustaste, und wählen Sie *Connect* aus dem Dropdown-Menü aus.



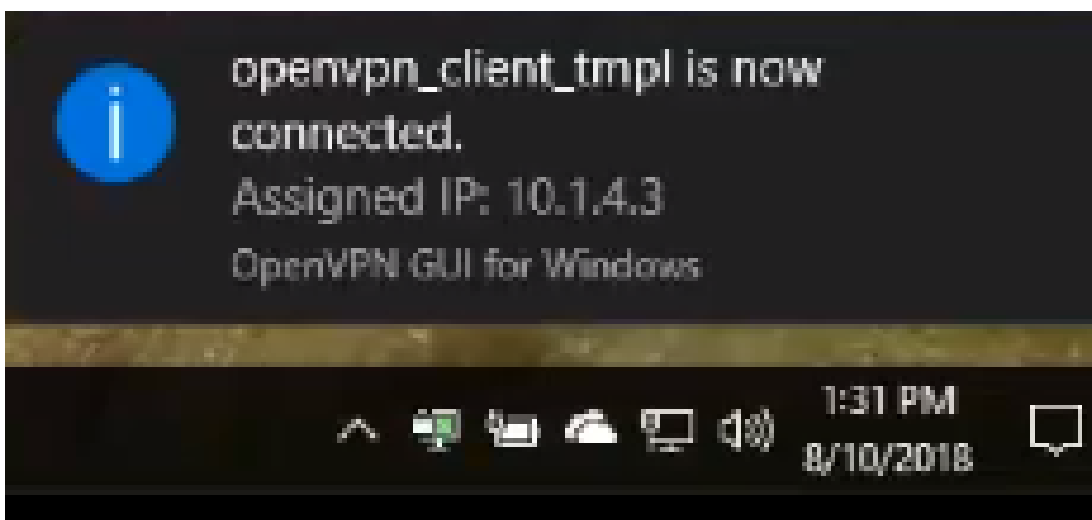
Schritt 3: Geben Sie den *Benutzernamen* und das *Kennwort* ein.



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

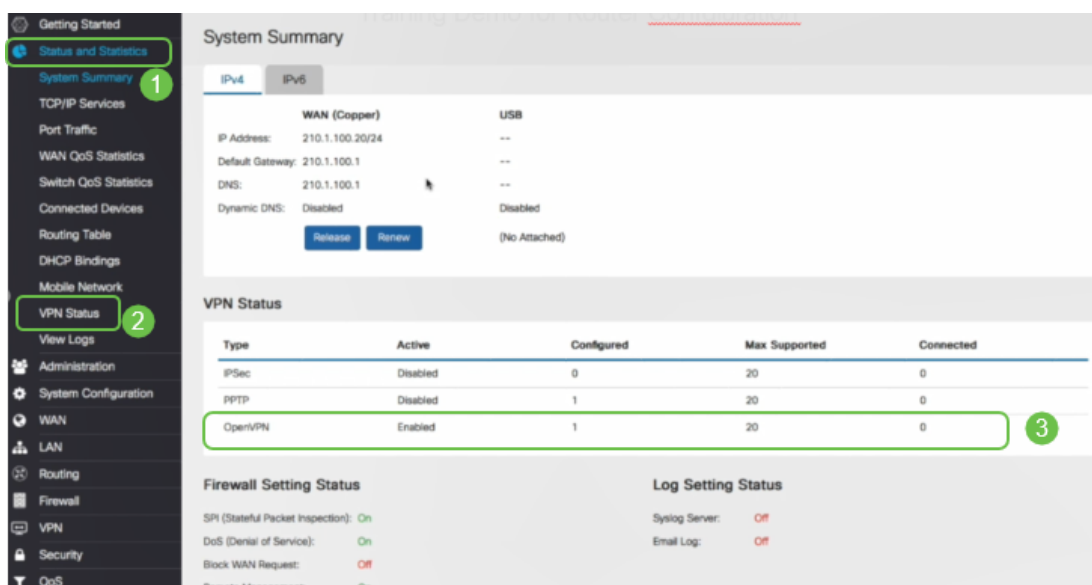


Schritt 5: Ein Systemprotokoll sollte eine Warnmeldung ausgeben, dass eine Verbindung besteht.



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.](#)