

# OpenVPN on an RV160 and RV260 Router

## Objective

The objective of this article is to guide you through setting up OpenVPN on your RV160 or RV260 router as well as the VPN client setup of OpenVPN on your computer.

## Applicable Devices

- RV160
- RV260

## Software Version

- 1.0.00.15

## Table of Contents

[Setting up a Demo OpenVPN on an RV160/RV260 Router](#)

[Setting up OpenVPN on an RV160/RV260 Router](#)

[Logging in With a Self-signed Certificate after Setting up Demo OpenVPN](#)

[OpenVPN Client Setup on Computer](#)

## Introduction

OpenVPN is a free, open-source application that can be set up and used for a Virtual Private Network (VPN). It uses a client-server connection to provide secure communications between a server and a remote client location over the internet.

OpenVPN uses OpenSSL for encryption of UDP and TCP for traffic transmission. A VPN provides a secure tunnel of protection, which is less vulnerable to hackers since it encrypts data sent from your computer through the VPN connection. For example, if you are using WiFi in a public place, such as in an airport, it keeps your data, transactions, and queries from being seen by other users. Much like HTTPS, it encrypts data sent between two end points.

One of the most important steps in setting up OpenVPN is obtaining a Certificate from a Certificate Authority (CA). This is used for authentication. Certificates are purchased from any number of third party sites. It is an official way to prove that your site is secure. Essentially, the CA is a trusted source that verifies that you are a legitimate business and can be trusted. For OpenVPN you only need a lower level certificate at a minimal cost. You get checked out by the CA, and once they verify your information, they will issue the certificate to you. This certificate can be downloaded as a file on your computer. You can then go into your router (or VPN server) and upload it there. Please note, clients don't need a Certificate to use OpenVPN, it is just for verification through the router.

## Prerequisites

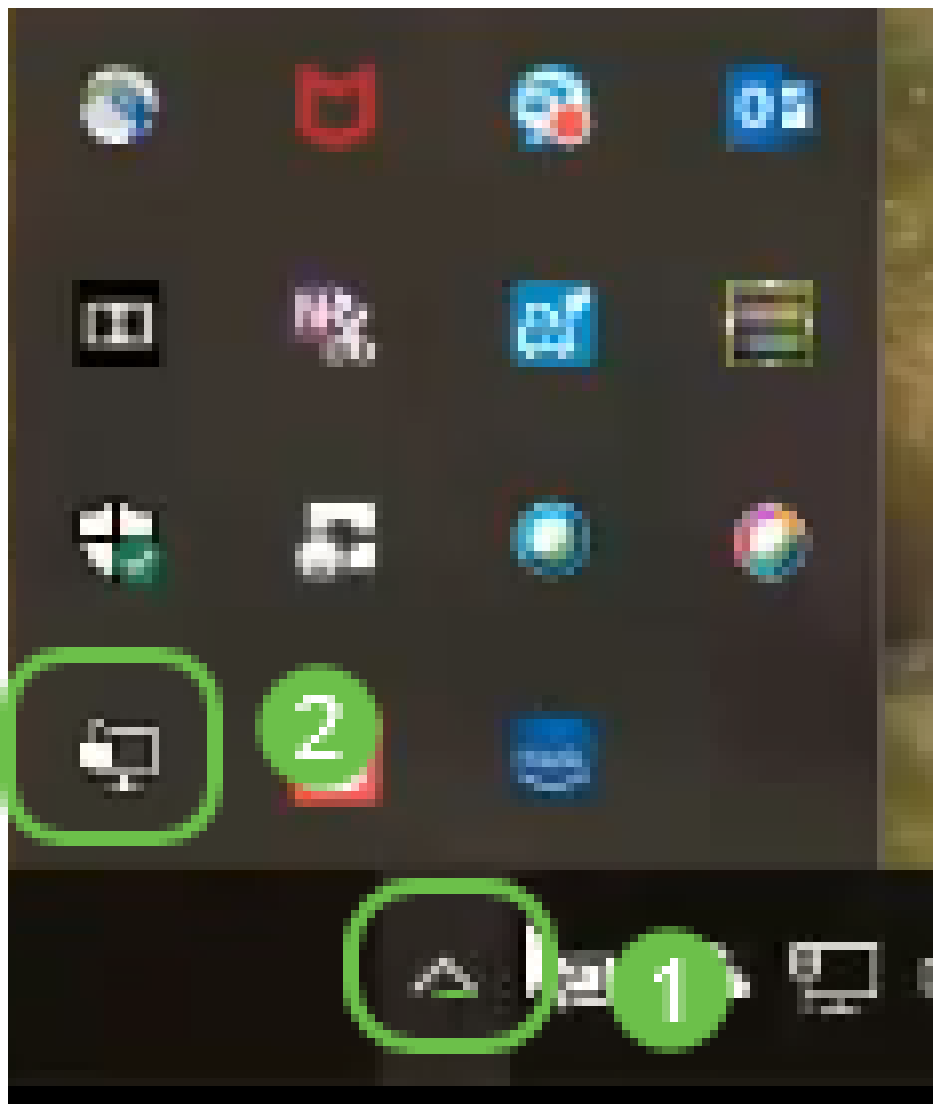
Install the OpenVPN application onto your system. Click [here](#) to go to the OpenVPN Website.

For more information on OpenVPN and answers to many questions you may have, click [here](#).

**Note:** This setup is specific to Windows 10.



Once you have OpenVPN installed, the application should appear on your desktop or as a small icon on the right side of the task bar. OpenVPN clients will also need this installed.



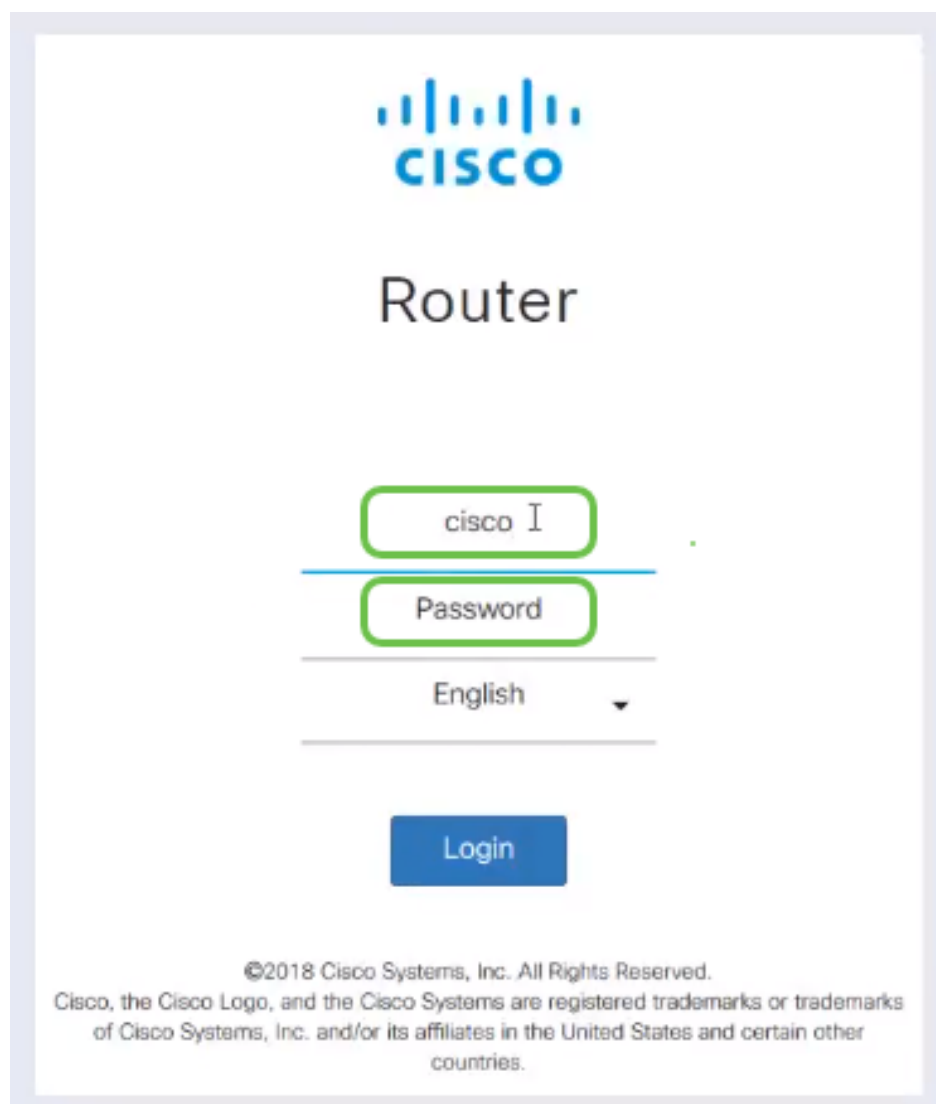
Ensure you have the proper system time set up on all devices. The proper system time must be completely synced at the router before the creation of a certificate. This is often done automatically, but if you run into issues, this is a good place to check.

## Setting up a Demo OpenVPN on an RV160/RV260 Router

If you want to try out OpenVPN before you pay money for a CA, you can create a self-signed certificate. This is a no-cost way to see if OpenVPN is something you would like to deploy for your business. If you already know you would like to purchase a CA, you can skip this section of the article and go directly to [Setting up OpenVPN on a RV160/RV260 Router](#).

Step 1. Log into the router using your credentials. The default user name and password are *cisco*.

**Note:** It is highly recommended that you change all passwords to something more complex. Otherwise, it is like leaving the key to your locked door on the doorstep.



The image shows the Cisco Router login interface. At the top is the Cisco logo. Below it, the word "Router" is displayed. There are three input fields: the first is labeled "Username" and contains the text "cisco"; the second is labeled "Password"; and the third is a language dropdown menu currently set to "English". Below these fields is a blue "Login" button. At the bottom of the page, there is a copyright notice: "©2018 Cisco Systems, Inc. All Rights Reserved. Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries."

Step 2. It is a requirement that you obtain a certificate on the router. Navigate to **Administration > Certificate > Generate CSR/Certificate...** This is how to create the request for a certificate.

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	CertTr	-	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		

Buttons: Import Certificate..., Generate CSR/Certificate..., Show built-in 3rd party CA Certificates..., Select as Primary Certificate...

Step 3. Make a request for a *CA Certificate*.

Generate CSR/Certificate

Buttons: Generate, Cancel

Type: CA Certificate

Certificate Name: Cert\_Test\_CA

Subject Alternative Name: 192.168.1.50

IP Address  FQDN  Email

Country Name (C): United States

State or Province Name (ST): South Dakota

Locality Name (L): Sioux Falls

Organization Name (O): Cisco

Organization Unit Name (OU): Training

Common Name (CN): Cert Test CA

Email Address (E): arenli@cisco.com

Key Encryption Length: 2048

- Select *CA Certificate* from the dropdown menu
- Enter a Certificate Name
- Enter the IP address, Fully Qualified Domain Name (FQDN), or Email. Entering the IP address is the most common choice.
- Enter your Country
- Enter your State
- Enter your Locality Name, usually your city
- Enter your Organization Name
- Enter your Organization Unit Name
- Enter your email address
- Enter Key Encryption Length, 2048 is recommended

Click the top right **Generate** button.

Step 4. You also need a server certificate. This *Certificate Signed by CA Certificate* will be signed by the CA certificate you just created.

RV260-PnP Demo

Alert cisco(admin) English

### Certificate

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		

1

Import Certificate... Generate CSR/Certificate... Show built-in 3rd party CA Certificates... Select as Primary Certificate...

Step 5. Make a request for a *Certificate Signed by CA Certificate*.

### Generate CSR/Certificate

2

Generate Cancel

Type: Certificate Signed by CA Certificate

Authorize External CSR:

Certificate Name: CertTest\_CA

Subject Alternative Name: 192.168.1.50

Country Name (C): 1 United States

State or Province Name (ST): South Dakota

Locality Name (L): Sioux Falls

Organization Name (O): Cisco

Organization Unit Name (OU): Training

Common Name (CN): Cert Test CA

Email Address (E): test@cisco.com

Key Encryption Length: 2048

Valid Duration: 360 days (Range: 1-10950, Default 360)

Certificate Authority:

- Select *Certificate Signing Request* from the dropdown menu
- Enter a Certificate Name
- Enter the IP address, Fully Qualified Domain Name (FQDN), or Email. Entering the IP address is the most common choice.
- Enter your Country
- Enter your State
- Enter your Locality Name, usually your city
- Enter your Organization Name
- Enter your Organization Unit Name
- Enter your email address
- Enter Key Encryption Length, 2048 is recommended
- Choose the proper Certificate Authority from the dropdown menu

Click the top right **Generate** button.

Step 6. Navigate to **System Configuration > User Groups**. Select the **plus** icon to add the new group.

**User Groups** [Apply] [Cancel]

<input type="checkbox"/> Group	Web Login /NETCONF /RESTCONF	Lobby Ambassa...	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP	Captive Portal
<input type="checkbox"/> Ambassa...	Disable	Enable	Disable	Disable	Disable	Disable	Disable	Enable
<input type="checkbox"/> admin	Admin	Enable	Enable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/> guest	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable

Step 7. Enter the name of the Group, click *On* for the radio button to turn on OpenVPN. Click **Apply**.

**User Groups** [Apply] [Cancel]

Group Name:  [1]

Local User Membership List

+ [trash icon]

# User

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

Services

Web Login/NETCONF/RESTCONF:  Disable  Readonly  Admin

Site to Site VPN:

+ [trash icon]

# Connection Name

Client to Site VPN:

+ [trash icon]

# Group Name

OpenVPN: [2]  On  Off

PPTP VPN:  On  Off

802.1x:  On  Off

Lobby Ambassador:  On  Off

Step 8. Navigate within the System Configuration menu and click on **User Accounts**. Under Local Users, Click on the **plus** icon.

**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 ▲

+ ✎ 🗑️ 📄 ⬇️ ⬆️

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.

Step 9. Fill out the information below. Make sure to select OpenVPN from the dropdown menu. Click **Apply**.

## Add user account

The current minimum requirements are as follows

- \* Minimal Password Length: 8
- \* Minimal Number of Character Classes: 3

Username: 1

New Password:

Confirm Password:

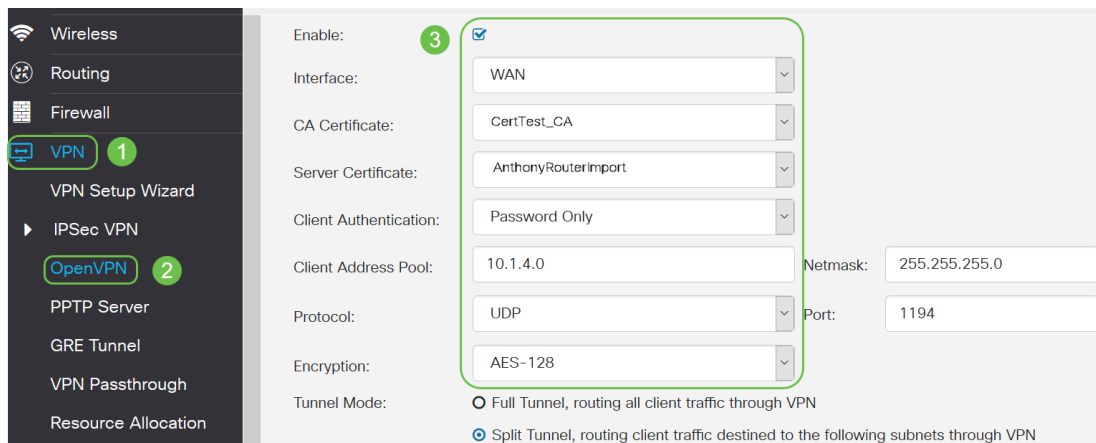
Password Strength meter:

Group:  ▼

2 Apply Cancel

All of the dependencies are complete and the router can now be configured for OpenVPN.

Step 10. Navigate to **VPN > OpenVPN**. The OpenVPN page opens. Complete each box on the page, making sure to select the previously created certificates from the dropdown menu.



- Check the *Enable* box. Select the Interface that is going to allow in traffic. In this case a Wide Area Network (WAN), and select a Certificate Authority (CA) Certificate.
- Select the *CA Certificate* from the dropdown menu
- Select the *Server Certificate* you downloaded from the dropdown menu
- Select *Client Authentication*. If you select Password they need to authenticate with a password. If you select Password + Certificate, the client must also have a certificate. This is more secure but adds to the cost of the VPN as they would need to purchase a separate CA.
- Enter the *Client Address Pool*. Choose an IP address on a Network subnet that isn't used anywhere else in the company. You select out of the reserved ranges and choose a range not used anywhere else.
- Choose the form of *Encryption*. Make sure the encryption is the same as the client. DES and 3DES are not recommended and should only be used for backwards compatibility.
- Choose Split tunnel if you only want to specify which traffic goes through the VPN. For a VPN, a split tunnel is necessary. *Full Tunnel Mode* is selected in other situations when you want all client traffic to go through the VPN.

Step 11. Scroll down the page and fill out the the *Domain Name* and *DNS1*.

Domain Name:	Openvpn.net
DNS1:	192.168.1.1

**Note:**The DNS1 IP address could be a dedicated internal DNS server, the same IP address of your default gateway provided by your Internet Service Provider (ISP), on a virtual machine, or a trusted DNS server out on the internet.

Step 12. Click **Apply** to save the configuration at the router.

Step 13. Stay on the same page and scroll further. Generate the configuration template that is to be installed on the OpenVPN client. This file has an *.ovpn* extension and will be used by the OpenVPN client. Check the box to *Export client configuration template (.ovpn)* and click **Generate**. This downloads the file onto your computer.



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

Step 14. Navigate to **Status and Statistics > VPN Status**. You have the ability to scroll down for more detailed information.

**System Summary**

IPv4 | IPv6

WAN (Copper) | USB

IP Address: 210.1.100.20/24 | --

Default Gateway: 210.1.100.1 | --

DNS: 210.1.100.1 | --

Dynamic DNS: Disabled | Disabled

(No Attached)

**VPN Status**

Type	Active	Configured	Max Supported	Connected
IPSec	Disabled	0	20	0
PPTP	Disabled	1	20	0
OpenVPN	Enabled	1	20	0

**Firewall Setting Status**

SPI (Stateful Packet Inspection): On

DoS (Denial of Service): On

Block WAN Request: Off

Remote Management: On

**Log Setting Status**

Syslog Server: Off

Email Log: Off

The next section of this article is important to review, as it explains how to log in with a self-signed certificate.

## Logging in With a Self-signed Certificate after setting up Demo OpenVPN

When you log in with a self-signed certificate, you may see a warning popup when you attempt to log in. You will need to click Advanced, Proceed, Trust, or another option depending on your web browser in order to proceed.

At this point you may receive a warning that it is unsafe. You can choose to proceed, add exception, or advanced. This will vary by web browser.

In this example, Chrome was used for a web browser. This message appears, click **Advanced**.



## 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

A new screen will open and you need to click on **Proceed to yourwebsite.net (unsafe)**

This server could not prove that it is [redacted].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 [redacted].net (unsafe)

Here is an example of accessing the device warning when using Firefox as a web browser. Click on **Advanced**.

 Your connection is not secure

The owner of [redacted].net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

Go Back Advanced

Click **Add Exception....**

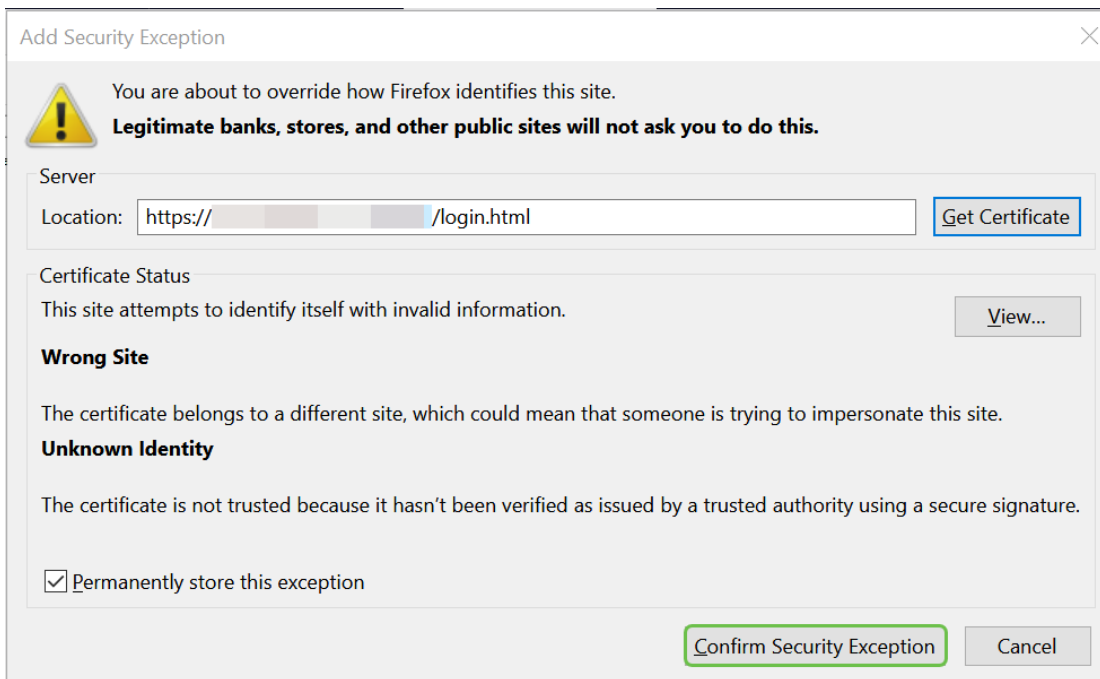
[redacted].net:50 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.  
The certificate is only valid for .

Error code: [MOZILLA\\_PKIX\\_ERROR\\_SELF\\_SIGNED\\_CERT](#)

Add Exception...

Finally, you will have to click on **Confirm Security Exception**.



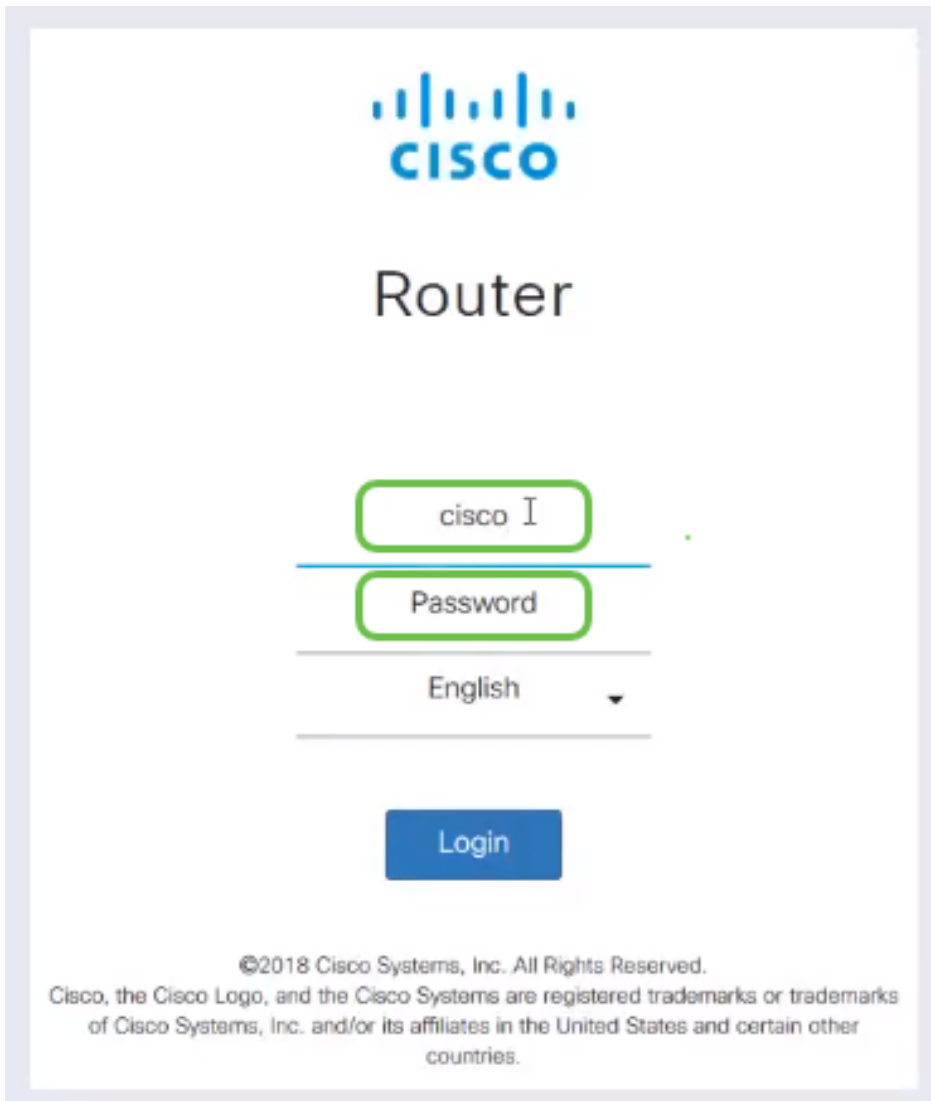
The router is now configured with all the parameters necessary to support an OpenVPN Client connection. Since you have already downloaded the client configuration template to your device, the one that ends in `.ovpn`, you can move on to the section [OpenVPN Client Setup on Computer](#). If you decide to deploy OpenVPN for your company, you can follow the steps in this next section.

## Setting up OpenVPN on an RV160/RV260 Router

This is a more complicated process as it involves getting a CA from a third party, which costs money. You also need to send the VPN client configuration template, ending in `.ovpn`, to all clients so they can set up on their device. Clients need several settings the same as the router in order for them to communicate. The best part is that for minimal cost, you and your employees can use the internet and conduct business more securely.

Step 1. Log into the router using your credentials. The default user name and password are `cisco`.

**Note:** It is highly recommended that you change all passwords to something more complex. Otherwise, it is like leaving the key to your locked door on the doorstep.



Step 2. It is a requirement that you obtain a certificate. Navigate to **Administration > Certificate > Generate CSR/Certificate...** This is how to create the request for a certificate.

The screenshot shows the Cisco configuration interface for a RV260-PnP Demo. The left sidebar has a menu with "Administration" (1) and "Certificate" (2) highlighted. The main content area is titled "Certificate" and contains a "Certificate Table" with the following data:

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		

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

Step 3. Make a request for a *Certificate Signed by CA Certificate*. This can be found by navigating to **Administration > Certificate**.

- Select *Certificate Signing Request* from the dropdown menu
- Enter a Certificate Name
- Enter the IP address, Fully Qualified Domain Name (FQDN), or Email. Entering the IP address is the most common choice.
- Enter your Country
- Enter your State
- Enter your Locality Name, usually your city
- Enter your Organization Name
- Enter your Organization Unit Name
- Enter your email address
- Enter Key Encryption Length, 2048 is recommended

Click the top right **Generate** button

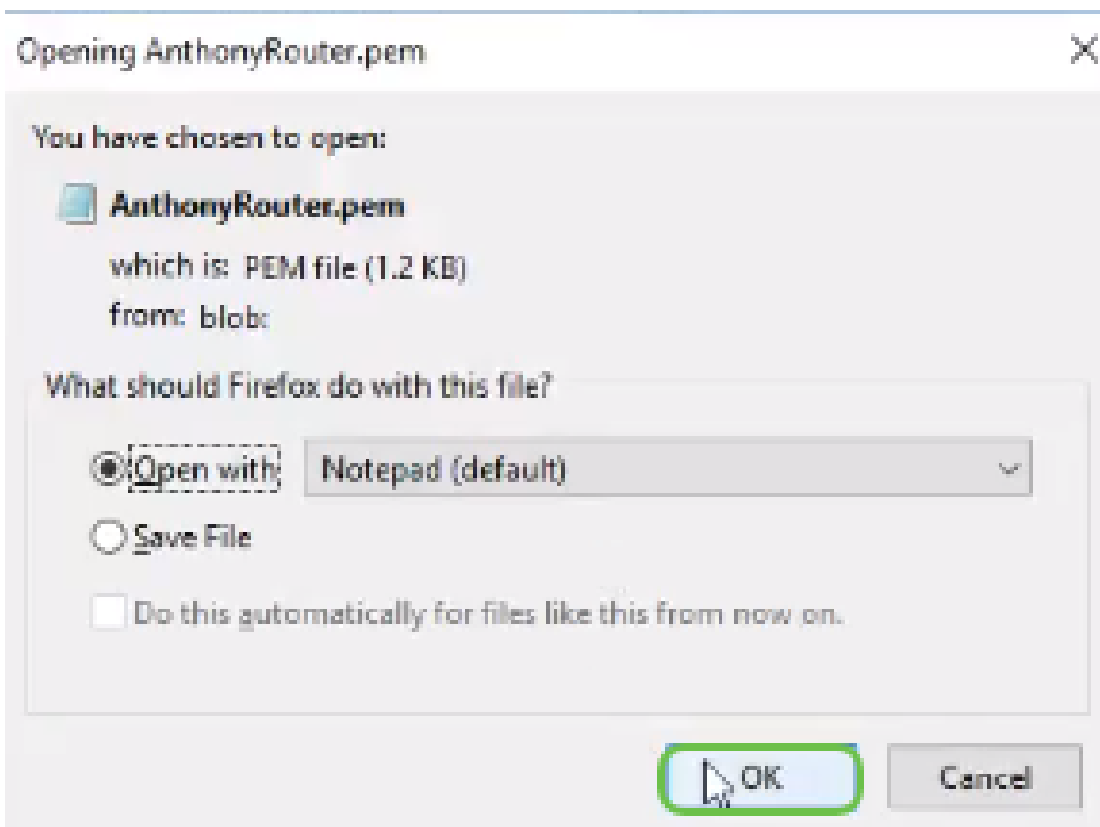
Step 4. Select to Export it by clicking the up arrow under Action.

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		

Step 5. This screen will appear. Click **Export**.



Step 6. Select *Open with and Notepad* (default) from the dropdown menu. Click **OK**.

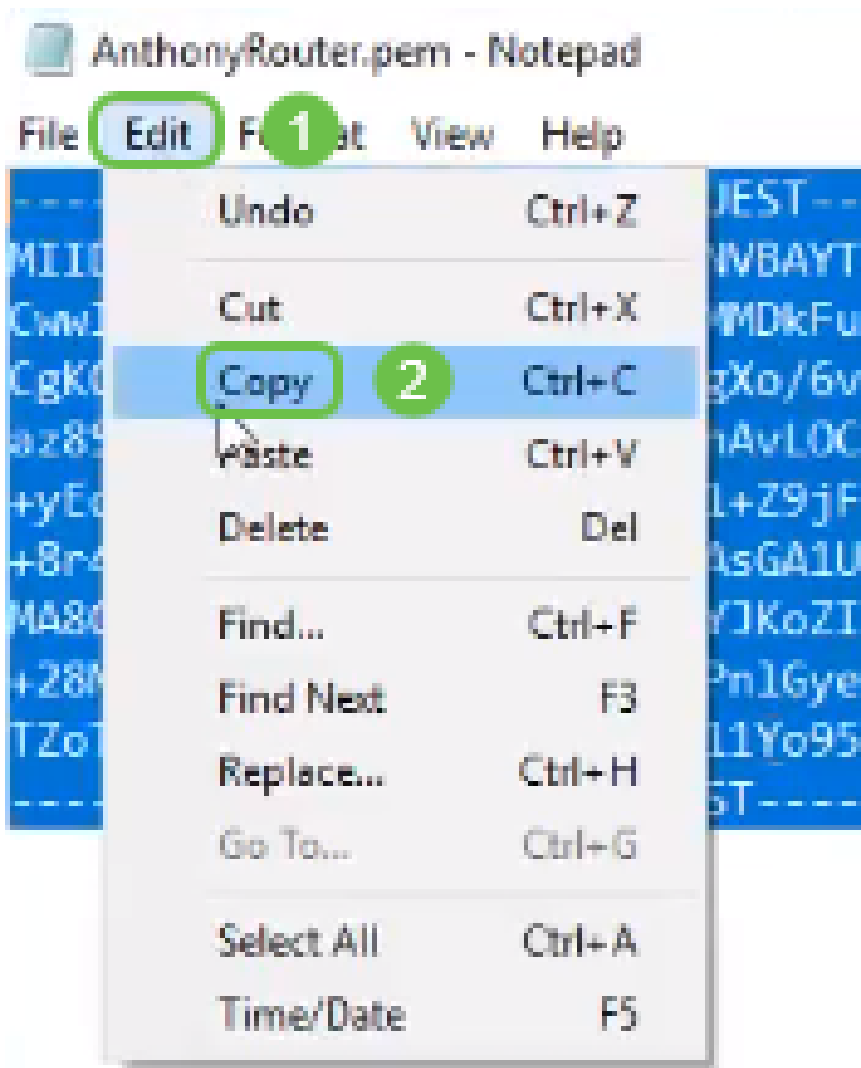


Step 7. An XML File will open.



**Note:** Make sure the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST are each on their own lines as shown above.

Step 8. At the top of the screen click **Edit** and select **Copy** from the dropdown menu.



Step 9. Choose a reputable third party site to make the certificate request. You will need to paste the copied XML file as part of the request.

**Note:** If you have an internal certificate server on your network you can use that instead, however this is not common.

## 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 >

Step 10. Once you have been verified, you can choose *Download certificate*.

## Certificate Issued

---

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

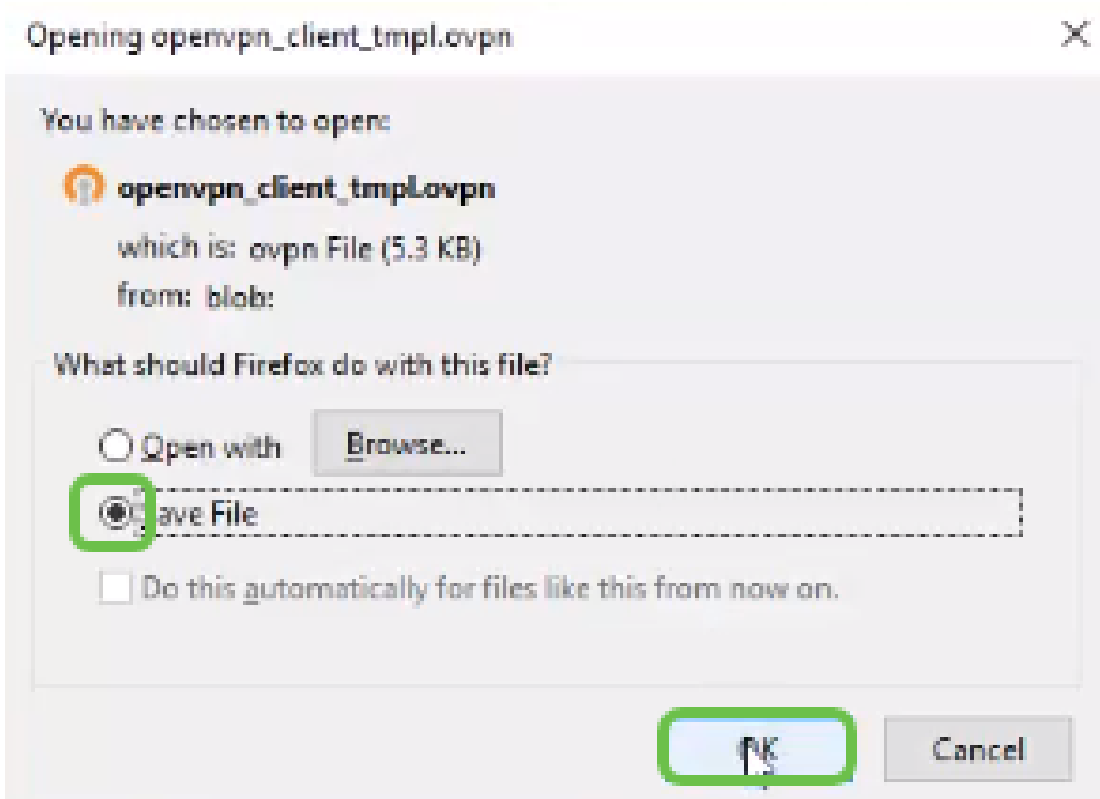


[Download certificate](#)

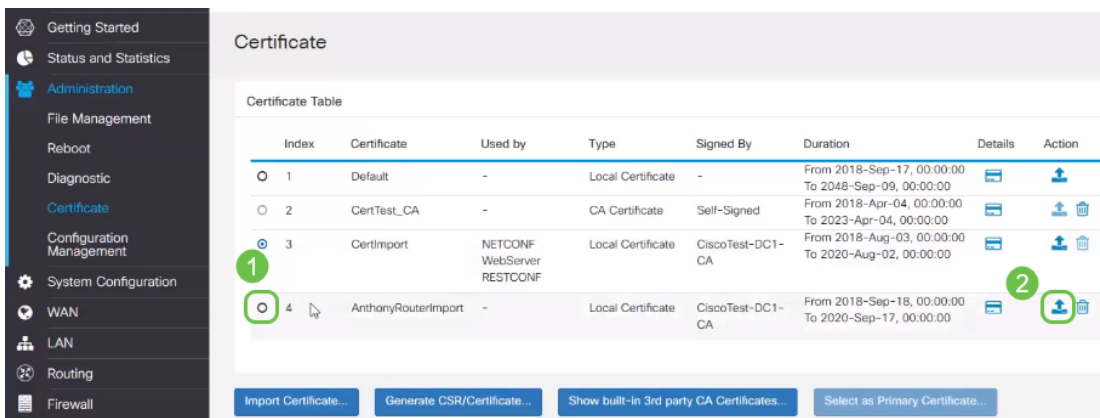
[Download certificate chain](#)

Step 11. Click the radio button to *Save File* and Click **OK**.





Step 12. Once it has been saved, select the radio button for that certificate and click on the **down arrow** icon.



Step 13. This screen will open. Select **Browse...**

# Import Signed-Certificate

Type: Local Certificate

Certificate Name:

## Upload Certificate file

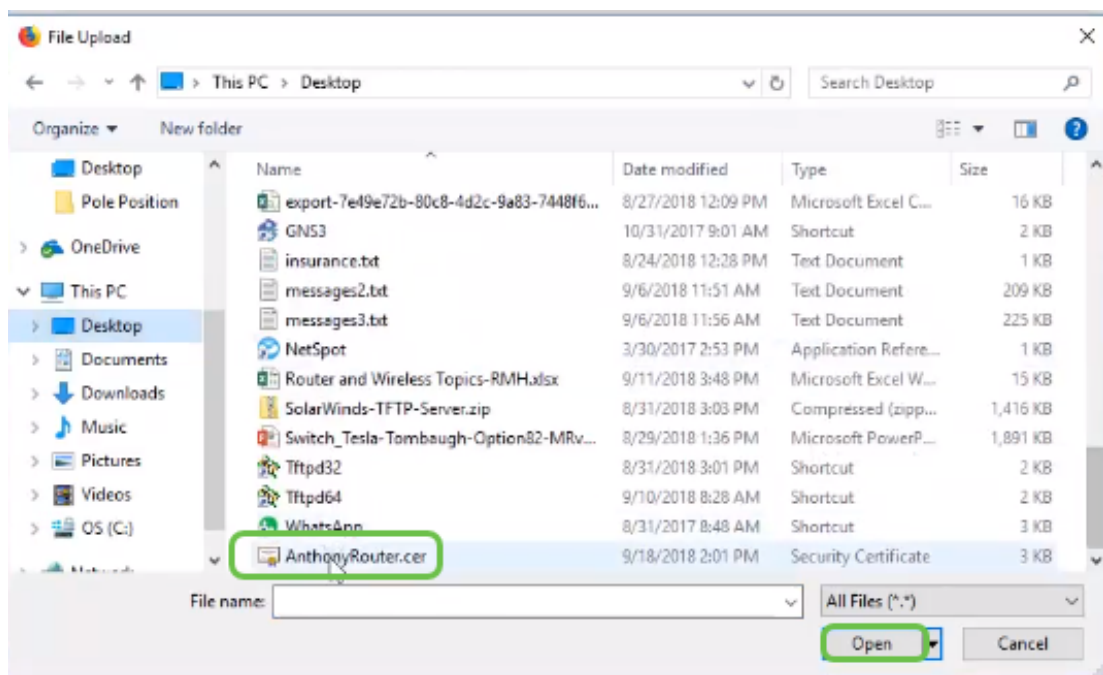
Import from PC

No file is selected

Import from USB

No file is selected

Step 14. Choose the file of the certificate and click **Open**.



Step 15. Enter the *Certificate Name* to import and click **Upload**.

## 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

Step 16. You will receive a notification that the certificate successfully imported. Click **OK**.

## Information



Import certificate successfully!

OK

Step 17. Navigate to **Administration > Certificate**. The certificate has been loaded.

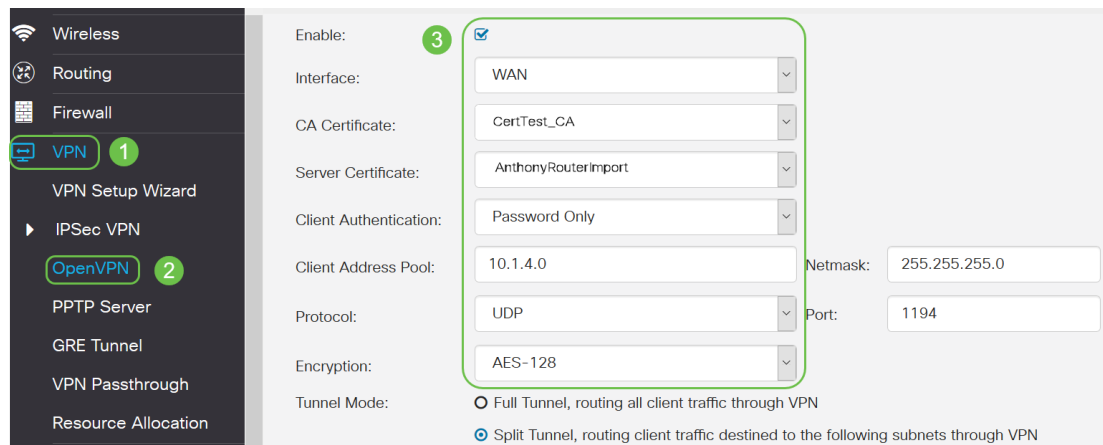
**Note:** In this example, a local certificate server was used.

The screenshot shows the Cisco IOS Administration interface for a Cisco RV260-PrPDemo router. The left sidebar shows the navigation menu with 'Administration' selected and 'Certificate' highlighted. The main content area displays the 'Certificate' configuration page, which includes a 'Certificate Table' with the following data:

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	NETCOM WebServer (823000)	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-CA	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'.

Step 18. Navigate to **VPN > OpenVPN**. The OpenVPN page opens. Complete the following with your information.



- Check the *Enable* box. Select the Interface that is going to allow in traffic. In this case a Wide Area Network (WAN), and select a Certificate Authority (CA) Certificate
- Select the *CA Certificate* from the dropdown menu
- Select the *Server Certificate* you downloaded from the dropdown menu
- Select *Client Authentication*. If you select Password they need to authenticate with a password. If you select Password + Certificate, the client must also have a certificate. This is more secure but adds to the cost of the VPN as they would need to purchase a separate CA.
- Enter the *Client Address Pool*. Choose an IP address on a Network subnet that isn't used anywhere else in the company. You select out of the reserved ranges and choose a range not used anywhere else.
- Choose the form of *Encryption*. Make sure the encryption is the same as the client. DES and 3DES are not recommended and should only be used for backwards compatibility.
- Choose *Full Tunnel Mode* if you want all client traffic to go through the VPN or *Split tunnel* if you only want to specify which traffic goes through the VPN
- The *DNS1* IP address could be a dedicated internal DNS server, the same IP address of your default gateway provided by your Internet Service Provider (ISP), on a virtual machine, or a trusted DNS server out on the internet.

Click **Apply** to save the configuration.

Step 19 (Option 1). You can email this configuration to the client. Check the box *Send Email*. Enter an email address. Add a Subject title for the email. Click **Generate**.

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):

Email Subject:

Step 20. (Option 2). Select *Export client configuration template (.ovpn)* and click **Generate**.

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):

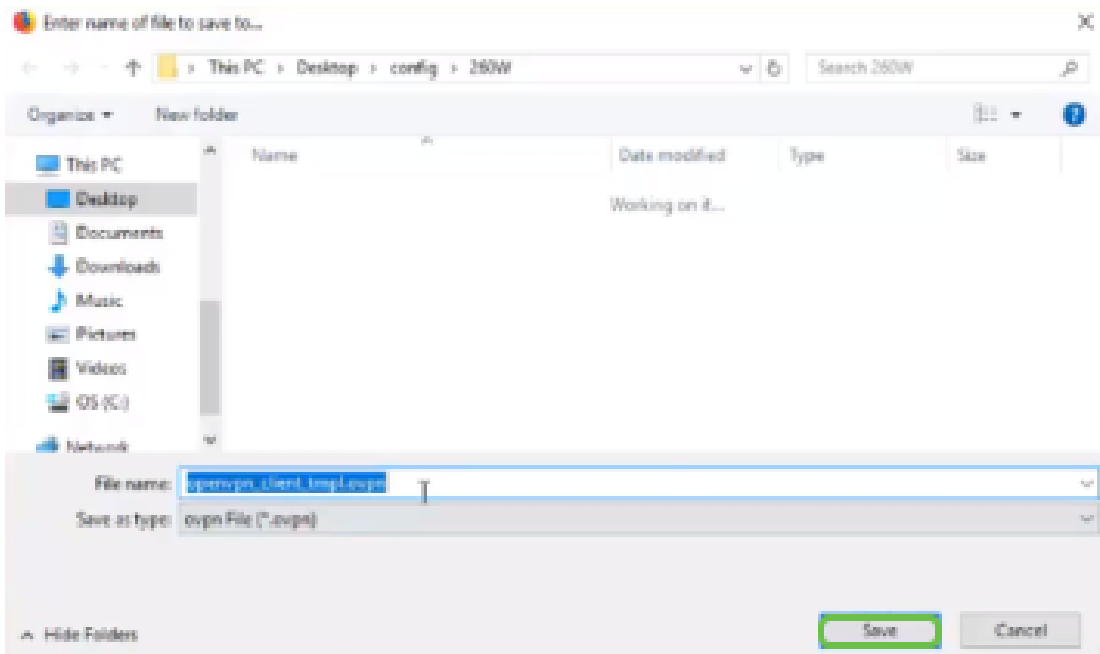
Email Subject:

Step 21. You will receive confirmation that is was successful. Click **OK**.

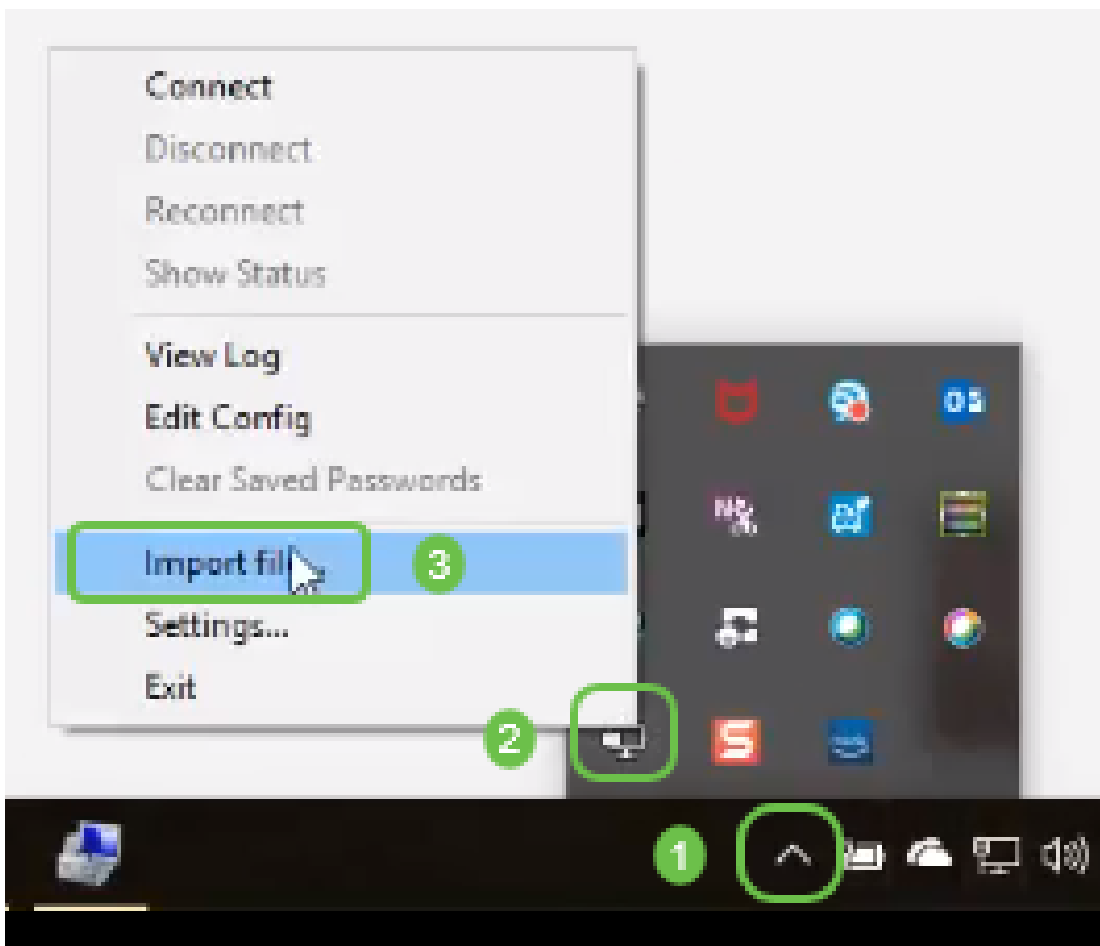
## Information

 Export client configuration template downloaded successfully!

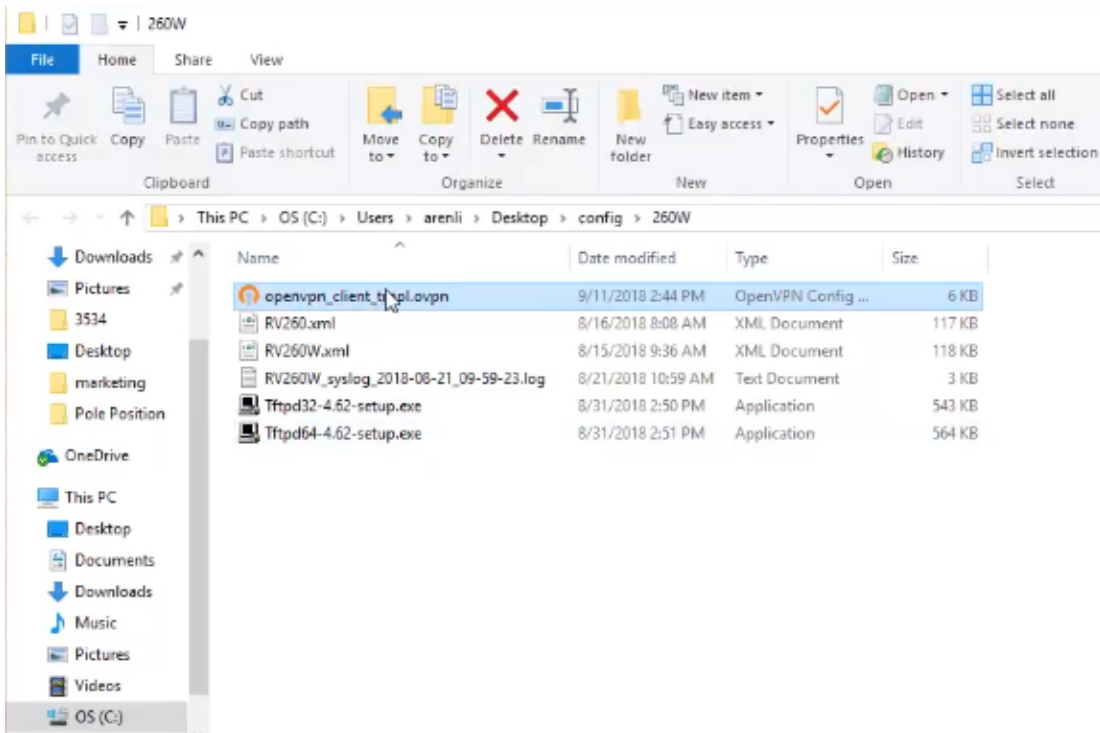
Step 22. Click **Save**.



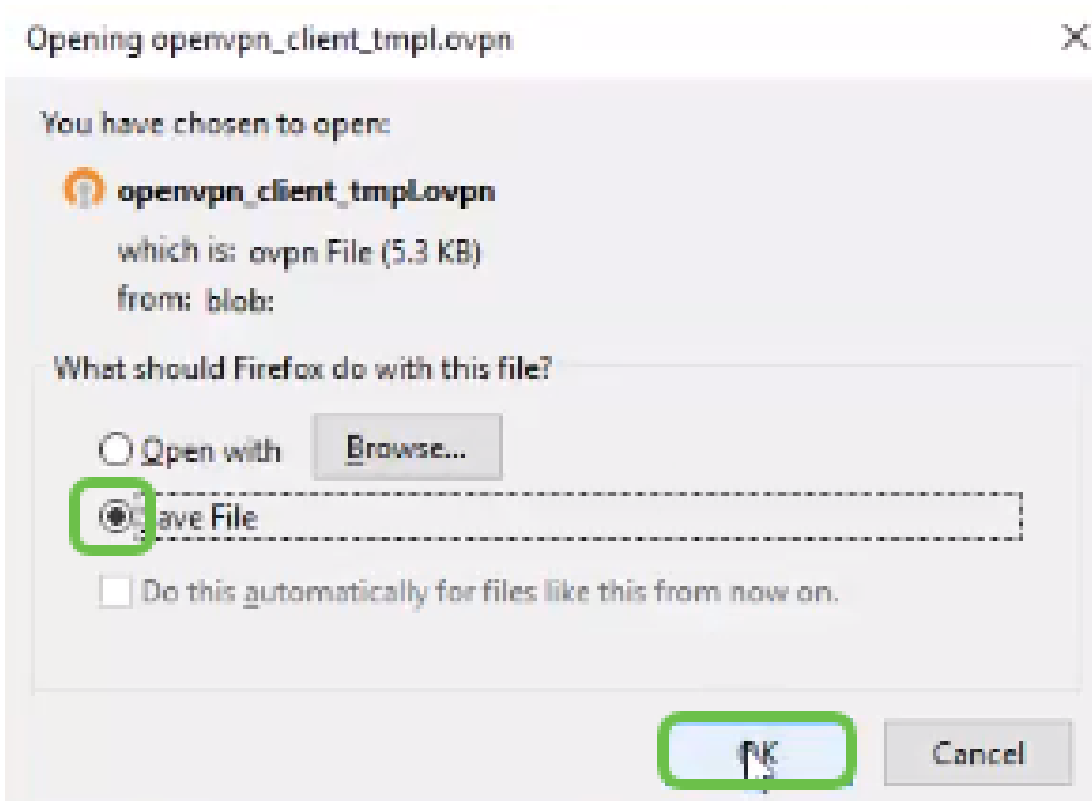
Step 23. At the bottom right of your desktop and click to open OpenVPN. Right click to open up dropdown menu. Click *Import File*.



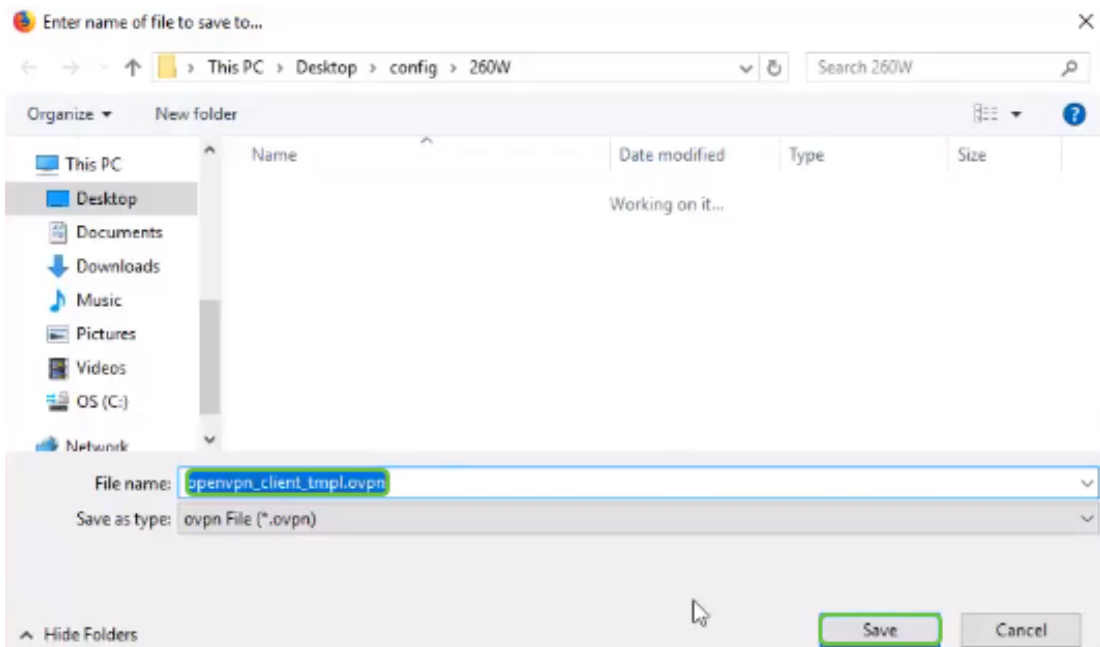
Step 24. Select the OpenVPN file that ends in *.ovpn*.



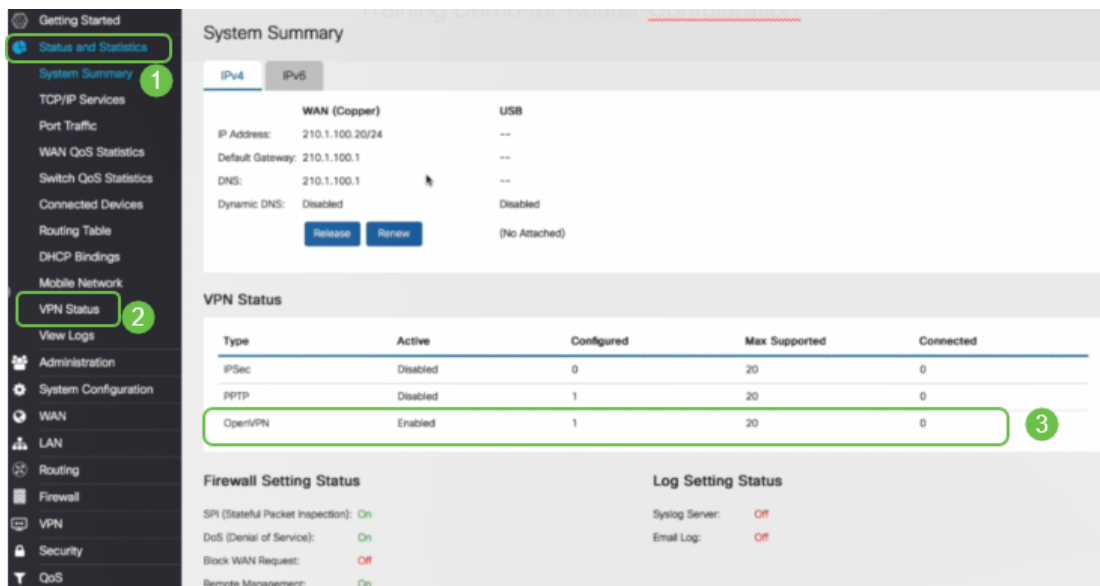
Step 25. Click on the radio button *Save File* and click **OK**.



Step 26. Change the name of the file if you choose, but leave *.ovpn* at the end of the file name. Click **Save**.



Step 27. Navigate to **Status and Statistics > VPN Status**. You have the ability to scroll down for more detailed information.



The router is now configured with all the parameters necessary to support an OpenVPN Client connection for your personal trial.

## OpenVPN Client Setup on Computer

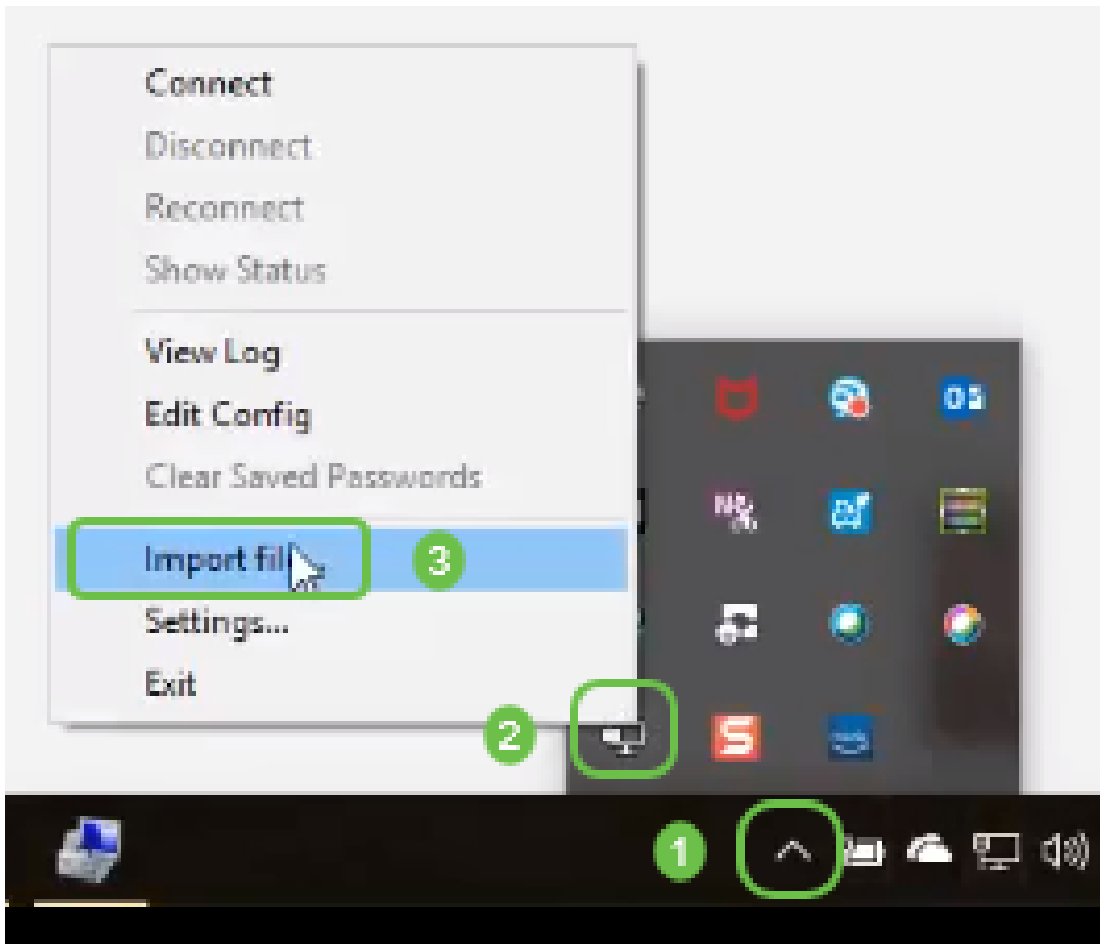
Each OpenVPN client needs to perform the following tasks as a prerequisite:

- Download the OpenVPN application on your device.
- Open and save the configuration file that was sent in steps 19-22 in the previous section. The configuration file ends in *.ovpn*.

**Note:** This setup is specifically for Windows 10.

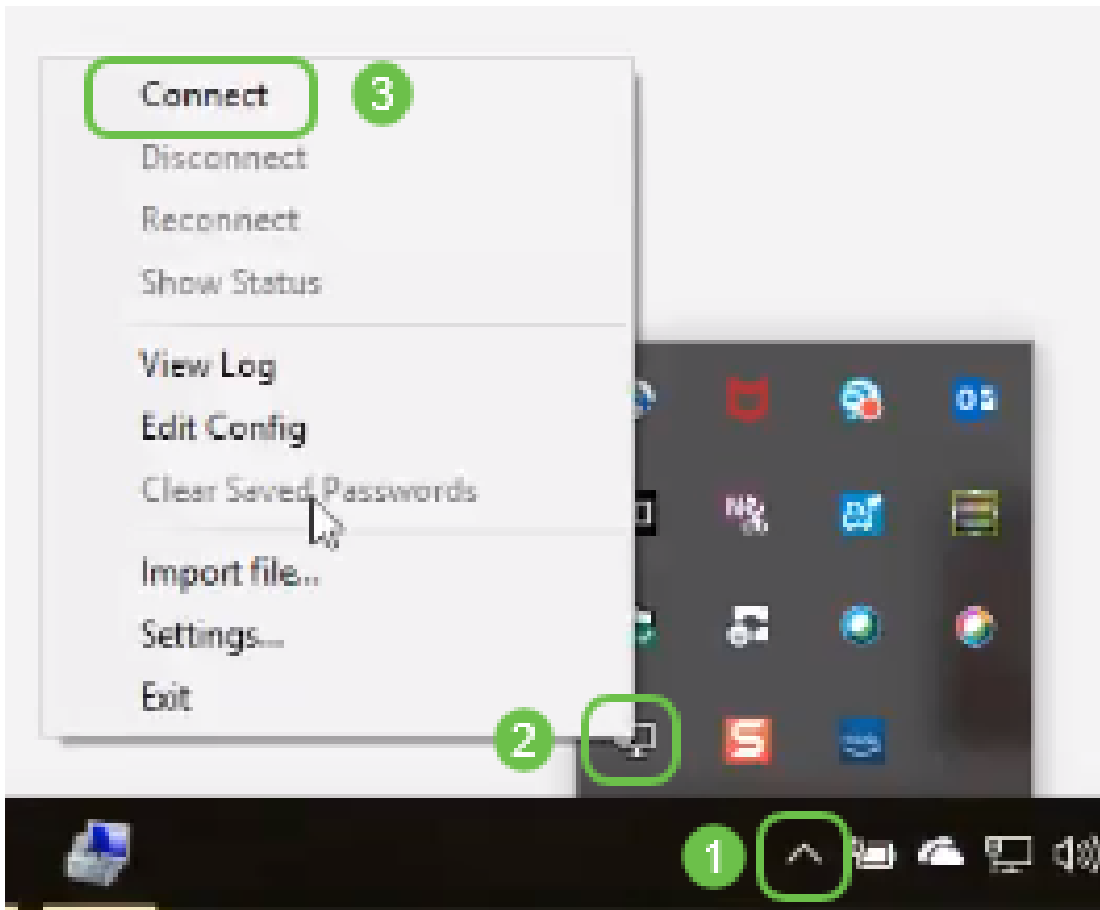
Step 1. Navigate to the arrow icon on the bottom right of the desktop and click to open the OpenVPN icon. Right click and select *Import File*.



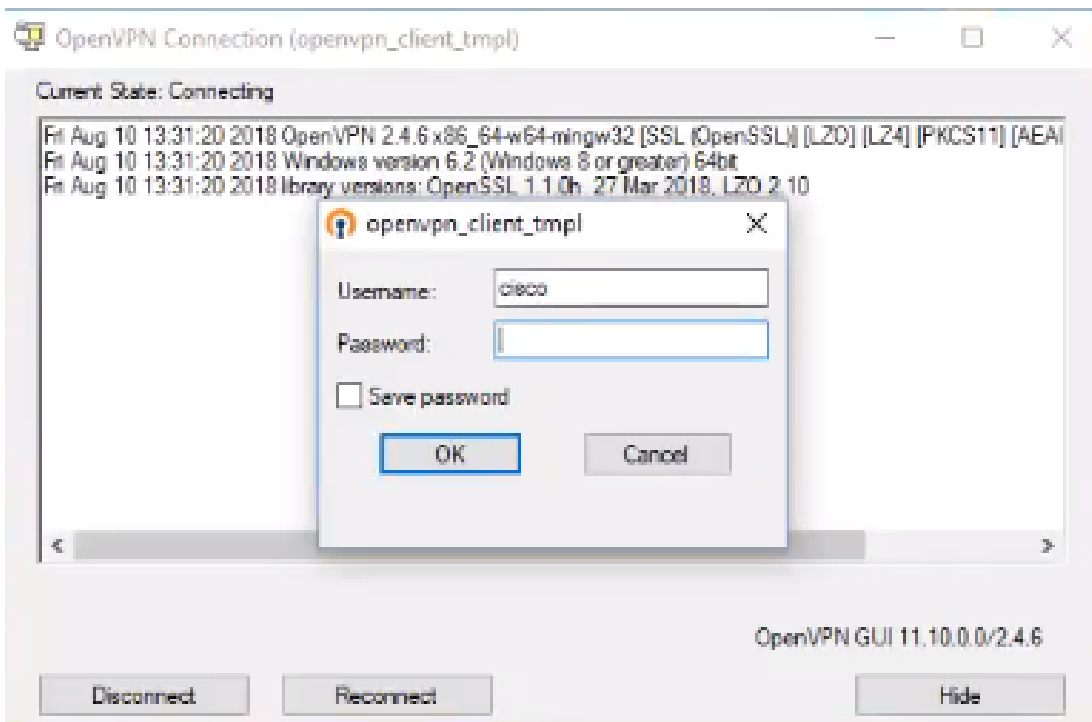


**Note:** The icon is black and white, indicating that it is not currently running. Once it is running the icon will show in color.

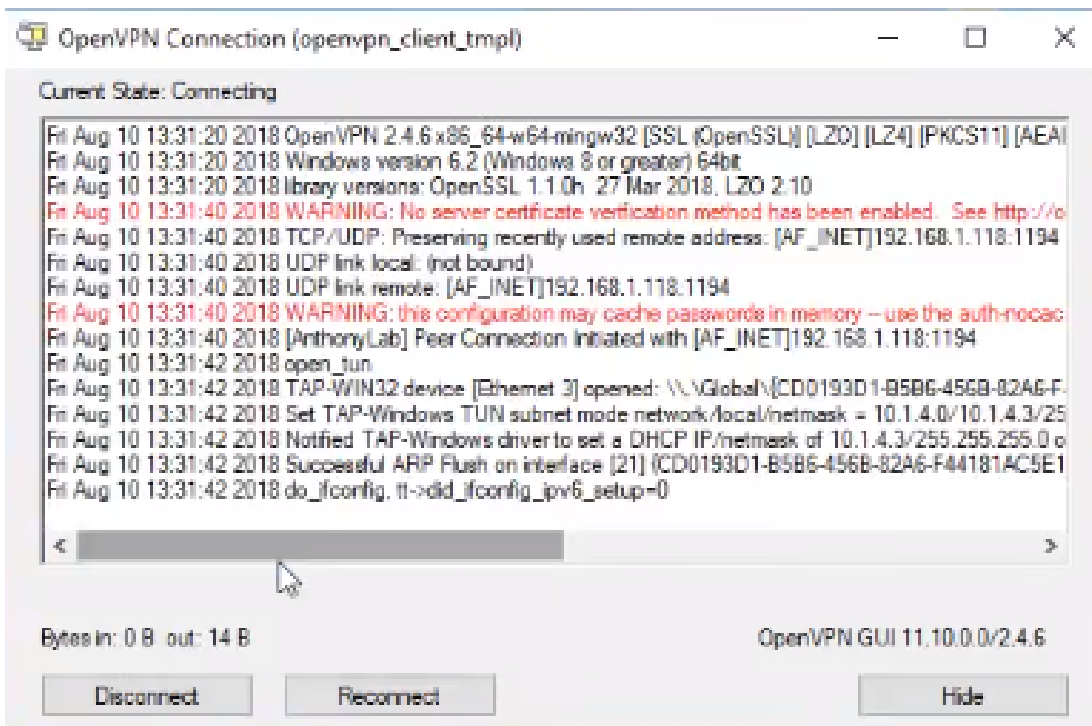
Step 2. Click on the *up arrow*. Click on the OpenVPN icon. Right click and select *Connect* from the dropdown menu.



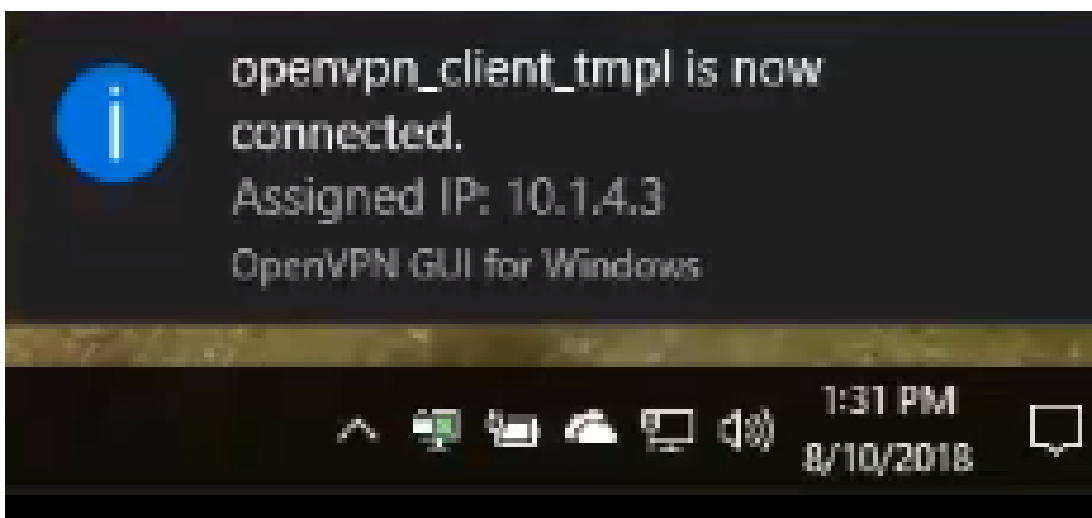
Step 3. Enter the *Username* and *Password*.



Step 4. The window will show the OpenVPN connecting along with some log data.

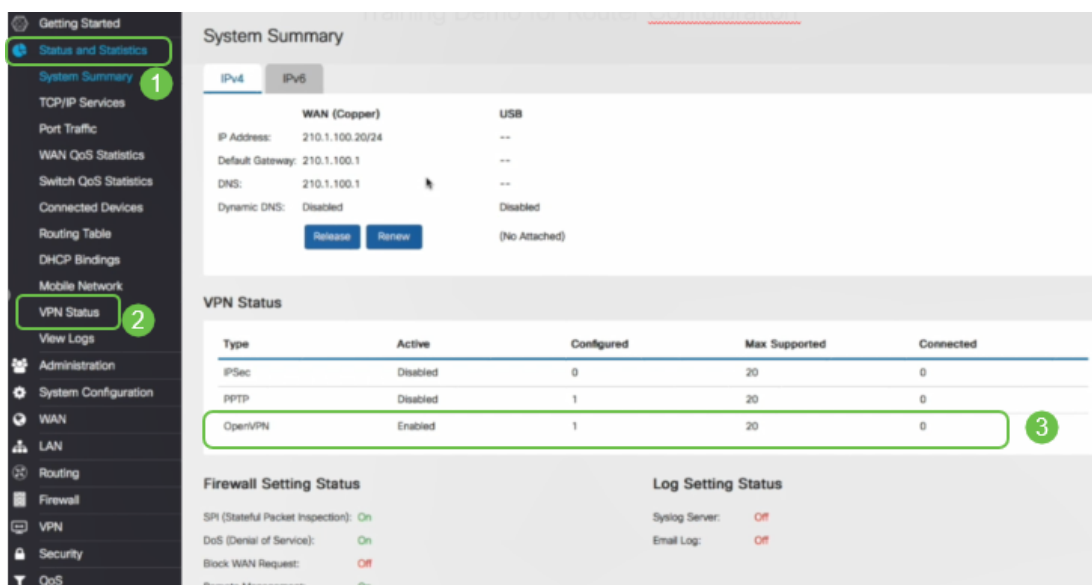


Step 5. A system log should alert that there is a connection.



Step 6. The VPN client should safely be able to tunnel incoming and outgoing information through OpenVPN. This can be set to automatically connect in the OpenVPN settings.

Step 7. The administrator can confirm the VPN Status by navigating to **Status and Statistics > VPN Status** on the router.



## Conclusion

You should now have successfully installed OpenVPN on your RV160 or RV260 router and at the VPN client site.

For community discussions on OpenVPN, click [here](#) and do a search for OpenVPN.

**[View a video related to this article...](#)**

**[Click here to view other Tech Talks from Cisco](#)**