

OpenVPN en un router RV160 y RV260

Objetivo

El objetivo de este artículo es guiarle a través de la configuración de OpenVPN en su router RV160 o RV260, así como la configuración del cliente VPN de OpenVPN en su equipo.

Dispositivos aplicables

- RV160
- RV260

Versión del software

- 1.0.00.15

Table Of Contents

[Configuración de una demostración OpenVPN en un router RV160/RV260](#)

[Configuración de OpenVPN en un Router RV160/RV260](#)

[Inicio de sesión con un certificado autofirmado después de configurar Demo OpenVPN](#)

[Configuración de OpenVPN Client en el equipo](#)

Introducción

OpenVPN es una aplicación gratuita de código abierto que se puede configurar y utilizar para una red privada virtual (VPN). Utiliza una conexión cliente-servidor para proporcionar comunicaciones seguras entre un servidor y una ubicación de cliente remoto a través de Internet.

OpenVPN utiliza OpenSSL para el cifrado de UDP y TCP para la transmisión del tráfico. Una VPN proporciona un túnel de protección seguro, que es menos vulnerable a los hackers, ya que cifra los datos enviados desde su equipo a través de la conexión VPN. Por ejemplo, si utiliza WiFi en un lugar público, como en un aeropuerto, evita que otros usuarios vean sus datos, transacciones y consultas. Al igual que HTTPS, cifra los datos enviados entre dos puntos finales.

Uno de los pasos más importantes en la configuración de OpenVPN es la obtención de un certificado de una autoridad certificadora (CA). Esto se utiliza para la autenticación. Los certificados se compran en cualquier número de sitios de terceros. Es una manera oficial de probar que su sitio es seguro. Básicamente, la CA es una fuente de confianza que verifica que usted es una empresa legítima y de confianza. Para OpenVPN sólo necesita un certificado de nivel inferior a un costo mínimo. La CA le desprotege y, una vez que verifiquen su información, le emitirán el certificado. Este certificado se puede descargar como un archivo en su equipo. A continuación, puede ir al router (o al servidor VPN) y cargarlo allí. Tenga en cuenta que los clientes no necesitan un certificado para utilizar OpenVPN, solo para la verificación a través del router.

Prerequisites

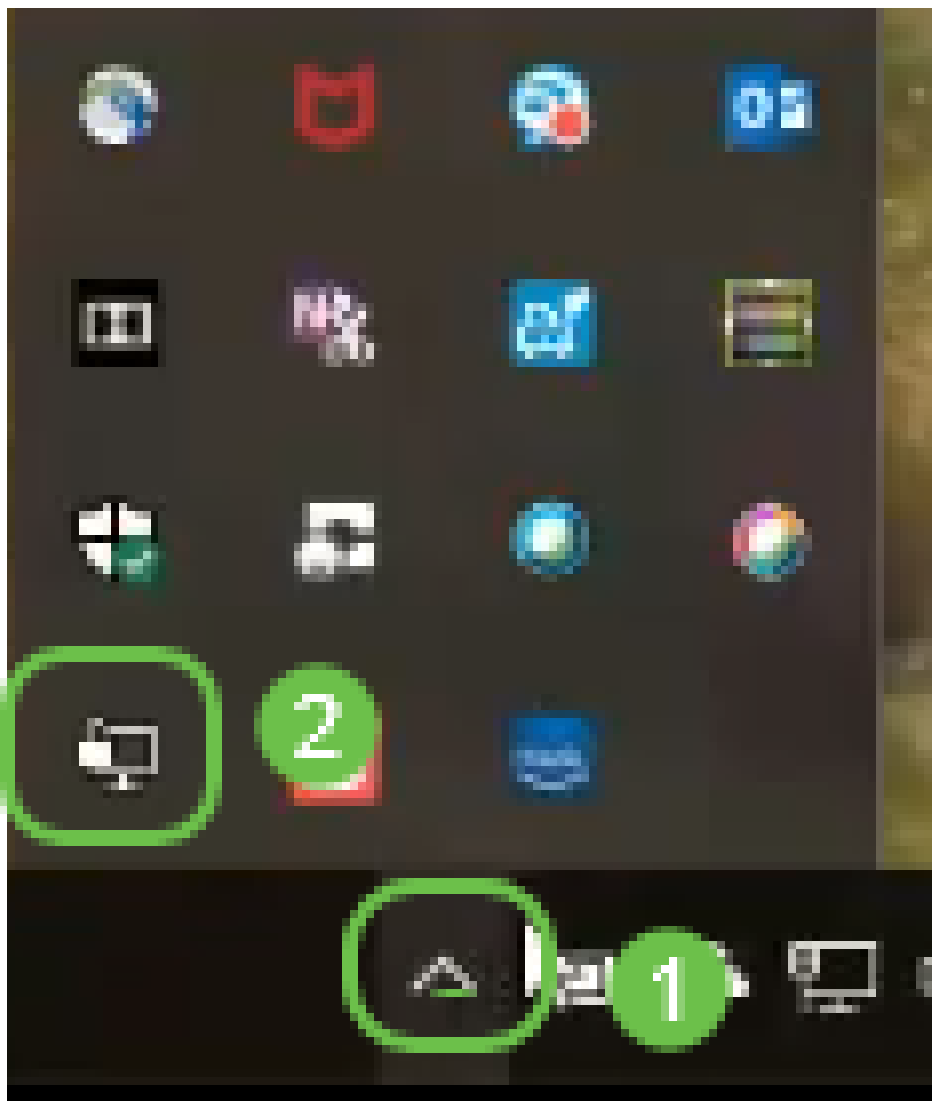
Instale la aplicación OpenVPN en el sistema. Haga clic [aquí](#) para ir al sitio web OpenVPN.

Para obtener más información sobre OpenVPN y respuestas a muchas preguntas que pueda tener, haga clic [aquí](#).

Nota: Esta configuración es específica para Windows 10.



Una vez que haya instalado OpenVPN, la aplicación debe aparecer en el escritorio o como un pequeño icono en el lado derecho de la barra de tareas. Los clientes OpenVPN también necesitarán esto instalado.



Asegúrese de que dispone del tiempo adecuado del sistema en todos los dispositivos. La hora

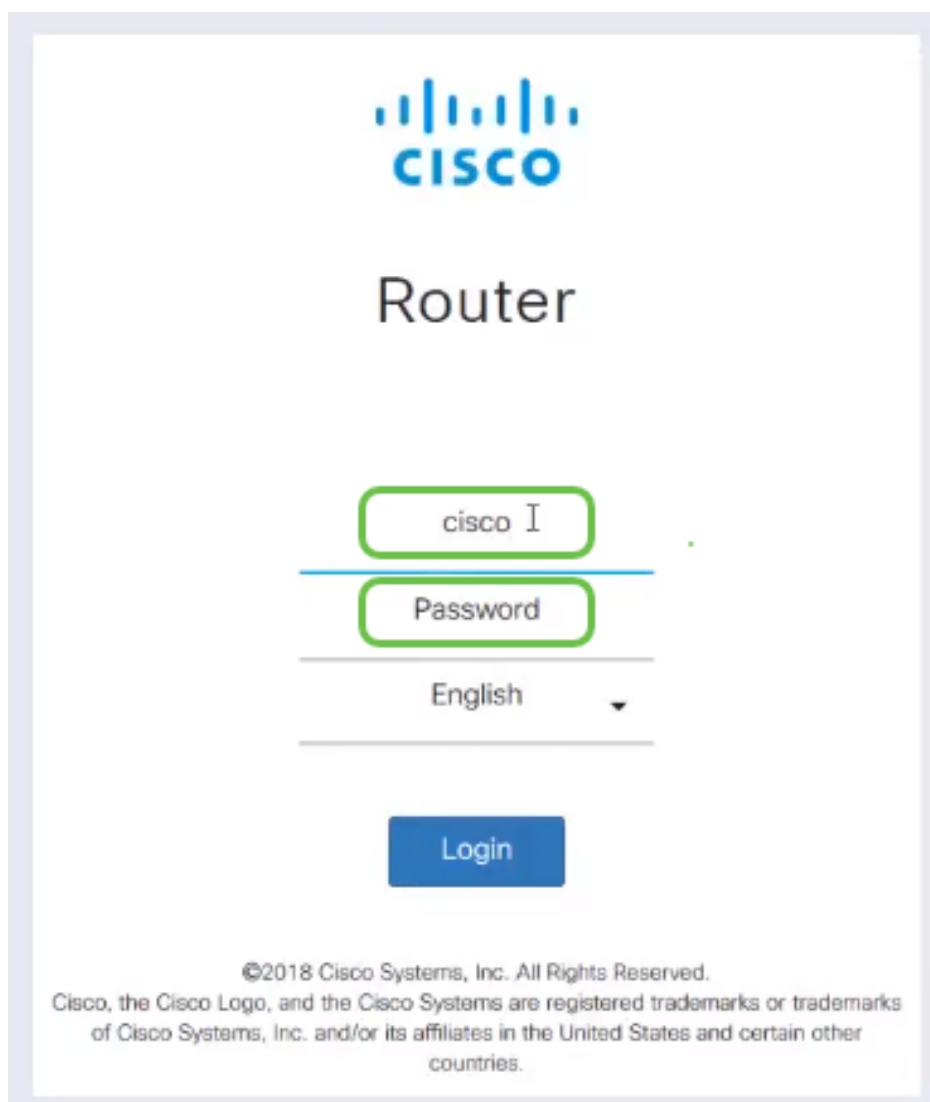
correcta del sistema se debe sincronizar completamente en el router antes de la creación de un certificado. A menudo esto se realiza automáticamente, pero si se encuentra con problemas, este es un buen lugar para verificar.

Configuración de una demostración OpenVPN en un router RV160/RV260

Si desea probar OpenVPN antes de pagar el dinero por una CA, puede crear un certificado autofirmado. Se trata de una forma gratuita de comprobar si OpenVPN es algo que le gustaría implementar para su empresa. Si ya sabe que desea adquirir una CA, puede saltarse esta sección del artículo y ir directamente a [Configuración de OpenVPN en un RV160/RV260 Router](#).

Paso 1. Inicie sesión en el router con sus credenciales. El nombre de usuario y la contraseña predeterminados son *cisco*.

Nota: Se recomienda encarecidamente cambiar todas las contraseñas a algo más complejo. De lo contrario, es como dejar la llave en la puerta cerrada en la puerta.



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 contains "cisco I", the second is labeled "Password", and the third is labeled "English" with a dropdown arrow. A blue "Login" button is centered below these fields. At the bottom, 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."

Paso 2. Es un requisito obtener un certificado en el router. Navegue hasta **Administración > Certificado > Generar CSR/Certificado...** Esto es cómo crear la solicitud de un certificado.

Alert cisco(admin) English ? i

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		

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

Paso 3. Realice una solicitud de un *certificado de CA*.

Generate CSR/Certificate

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):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU): Training

Common Name (CN): Cert Test CA

Email Address (E): @cisco.com

Key Encryption Length: 2048

- Seleccione *CA Certificate* en el menú desplegable
- Introduzca un nombre de certificado
- Introduzca la dirección IP, el nombre de dominio completo (FQDN) o el correo electrónico. La elección más común es ingresar la dirección IP.
- Introduzca su país
- Introduzca su estado
- Introduzca su nombre de localidad, normalmente su ciudad
- Introduzca su nombre de organización
- Introduzca el nombre de la unidad de la organización
- Introduzca su dirección de correo electrónico
- Introduzca la longitud de cifrado de la clave; se recomienda 2048

Haga clic en el botón **Generar** arriba a la derecha.

Paso 4. También necesita un certificado de servidor. Este *certificado firmado por el certificado de CA* será firmado por el certificado de CA que acaba de crear.

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		

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

Paso 5. Realice una solicitud de un *certificado firmado por el certificado de CA*.

Generate CSR/Certificate

Type: Certificate Signed by CA Certificate

Authorize External CSR:

Certificate Name: CertTest_CA

Subject Alternative Name: 192.168.1.50

Country Name (C): United States

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU):

Common Name (CN): Cert Test CA

Email Address (E): .com

Key Encryption Length: 2048

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

Certificate Authority:

Buttons: Generate, Cancel

- Seleccione *Solicitud de firma de certificado* en el menú desplegable
- Introduzca un nombre de certificado
- Introduzca la dirección IP, el nombre de dominio completo (FQDN) o el correo electrónico. La elección más común es ingresar la dirección IP.
- Introduzca su país
- Introduzca su estado
- Introduzca su nombre de localidad, normalmente su ciudad
- Introduzca su nombre de organización
- Introduzca el nombre de la unidad de la organización
- Introduzca su dirección de correo electrónico
- Introduzca la longitud de cifrado de la clave; se recomienda 2048
- Elija la autoridad de certificación adecuada en el menú desplegable

Haga clic en el botón **Generar** arriba a la derecha.

Paso 6. Vaya a **Configuración del sistema > Grupos de usuarios**. Seleccione el icono **más** para agregar el nuevo grupo.

Getting Started
Status and Statistics
Administration 1
System Configuration
Initial Router Setup
System
Time
Log
Email
User Accounts
User Groups 2

User Groups

Apply Cancel

3 + - trash

<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

Paso 7. Introduzca el nombre del grupo, haga clic en *On* para que el botón de opción active OpenVPN. Haga clic en Apply (Aplicar).

User Groups

3 Apply Cancel

Group Name: OpenVPN 1

Local User Membership List

+ trash

User

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

Services

Web Login/NETCONF/RESTCONF: Disable Readonly Admin

Site to Site VPN:

+ trash

Connection Name

Client to Site VPN:

+ trash

Group Name

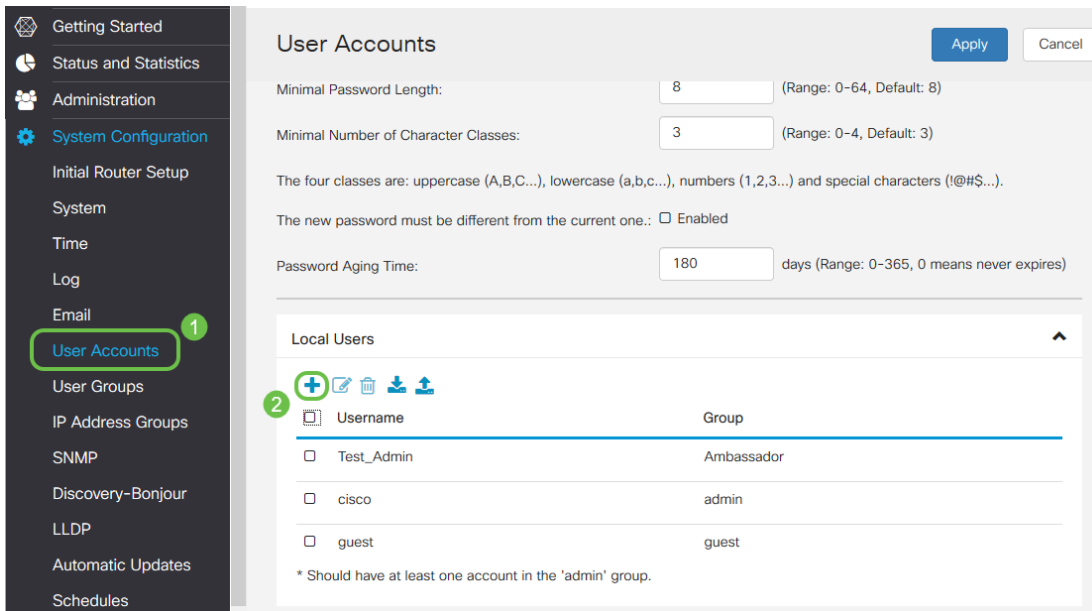
OpenVPN: 2 On Off

PPTP VPN: On Off

802.1x: On Off


Lobby Ambassador: On Off

Paso 8. Navegue dentro del menú System Configuration y haga clic en **User Accounts**. En Usuarios locales, haga clic en el icono **más**.



Paso 9. Complete la siguiente información. Asegúrese de seleccionar OpenVPN en el menú desplegable. Haga clic en Apply (Aplicar).

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:

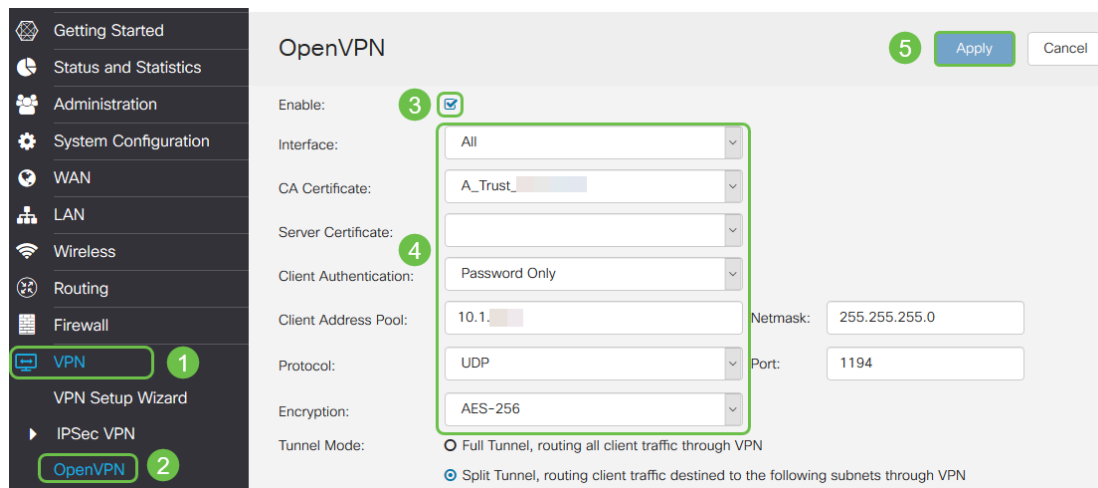
Password Strength meter: 

Group: 

2

Todas las dependencias están completas y el router ahora se puede configurar para OpenVPN.

Paso 10. Navegue hasta VPN > OpenVPN. Se abre la página OpenVPN. Complete cada cuadro de la página y asegúrese de seleccionar los certificados creados anteriormente en el menú desplegable.



- Marque la casilla *Enable* (Activar). Seleccione la interfaz que se permitirá en el tráfico. En este caso, una red de área extensa (WAN) y seleccione un certificado de autoridad certificadora (CA).
- Seleccione el *certificado de CA* en el menú desplegable
- Seleccione el certificado de servidor que ha descargado en el menú desplegable
- Seleccione *Autenticación de cliente*. Si selecciona Contraseña, deberán autenticarse con una contraseña. Si selecciona Contraseña + Certificado, el cliente también debe tener un certificado. Esto es más seguro, pero aumenta el coste de la VPN, ya que necesitarían comprar una CA independiente.
- Ingrese el *Conjunto de Direcciones de Cliente*. Elija una dirección IP en una subred de red que no se utilice en ningún otro lugar de la empresa. Seleccione uno de los intervalos reservados y elija un intervalo que no se utilice en ningún otro lugar.
- Elija la forma de *Cifrado*. Asegúrese de que el cifrado es el mismo que el cliente. No se recomiendan DES y 3DES y sólo se deben utilizar para la compatibilidad con versiones anteriores.
- Elija Dividir túnel si sólo desea especificar qué tráfico pasa a través de la VPN. Para una VPN, se necesita un túnel dividido. *El modo de túnel completo* se selecciona en otras situaciones cuando desea que todo el tráfico del cliente pase a través de la VPN.

Paso 11. Desplácese hacia abajo por la página y rellene los campos *Domain Name* y *DNS1*.

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

Nota: La dirección IP DNS1 puede ser un servidor DNS interno dedicado, la misma dirección IP de la gateway predeterminada proporcionada por el distribuidor de servicios de Internet (ISP), en una máquina virtual o un servidor DNS de confianza en Internet.

Paso 12. Haga clic en **Apply** para guardar la configuración en el router.

Paso 13. Permanezca en la misma página y desplácese más allá. Genere la plantilla de configuración que se instalará en el cliente OpenVPN. Este archivo tiene una extensión *.ovpn* y será utilizado por el cliente OpenVPN. Marque la casilla para *Exportar plantilla de configuración de cliente (.ovpn)* y haga clic en **Generar**. Esto descarga el archivo en el equipo.

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

Paso 14. Navegue hasta **Estado y estadísticas > Estado de VPN**. Puede desplazarse hacia abajo para obtener información más detallada.

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

La siguiente sección de este artículo es importante para revisar, ya que explica cómo iniciar sesión con un certificado autofirmado.

Inicio de sesión con un certificado autofirmado después de configurar Demo OpenVPN

Cuando inicie sesión con un certificado autofirmado, puede que aparezca una ventana emergente de advertencia cuando intente iniciar sesión. Para continuar, deberá hacer clic en Advanced (Avanzado), Proceed (Proceder), Trust (Confiar) u otra opción en función del navegador web.

En este momento, puede recibir una advertencia de que no es seguro. Puede optar por continuar, agregar excepción o avanzada. Esto variará según el navegador web.

En este ejemplo, Chrome se utilizó para un navegador web. Aparece este mensaje, haga clic en **Avanzadas**.



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

Se abrirá una nueva pantalla y tendrá que hacer clic en **Proceed to your website.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)

A continuación se muestra un ejemplo de cómo acceder a la advertencia del dispositivo cuando se utiliza Firefox como navegador web. Haga clic en **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](#)

Haga clic en **Agregar excepción....**

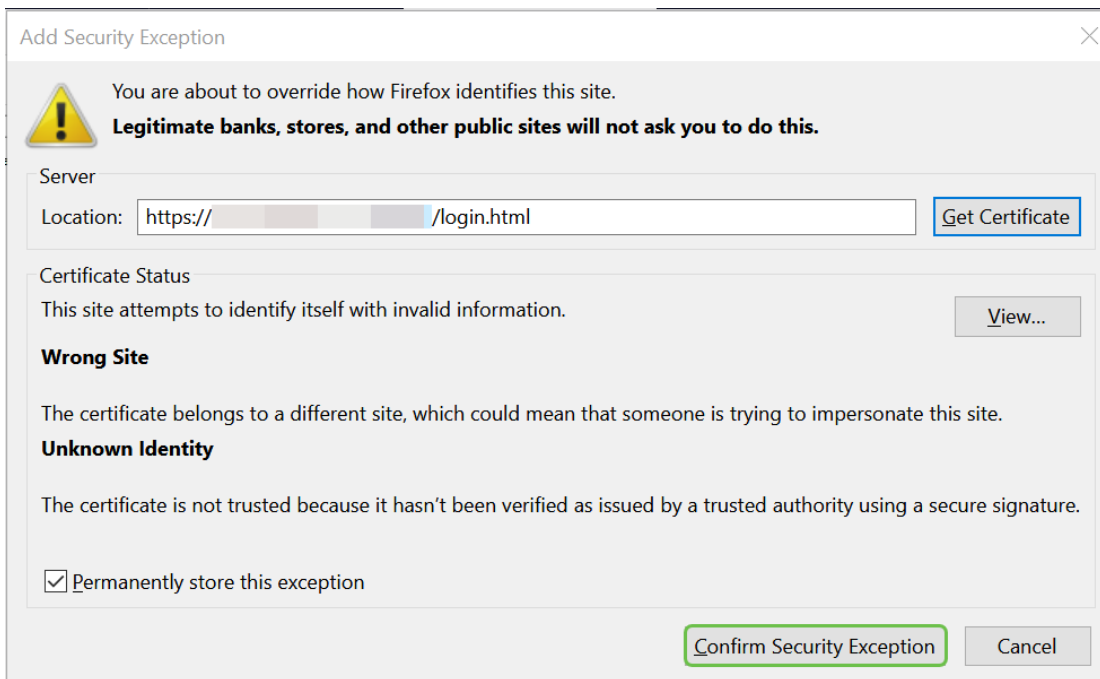
[redacted].net:50 uses an invalid security certificate.

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...](#)

Por último, tendrá que hacer clic en **Confirmar excepción de seguridad**.



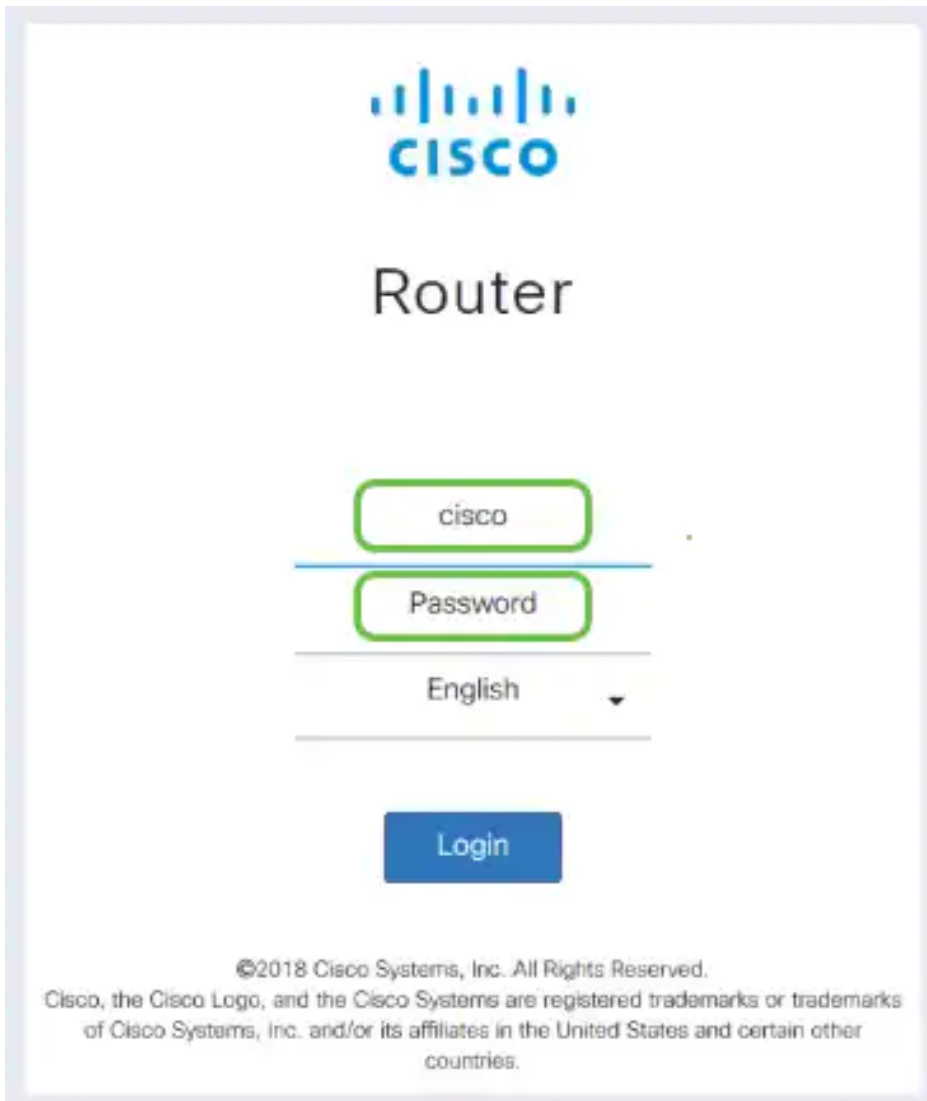
El router ahora está configurado con todos los parámetros necesarios para soportar una conexión OpenVPN Client. Dado que ya ha descargado la plantilla de configuración del cliente en su dispositivo, la que finaliza en `.ovpn`, puede pasar a la sección [Configuración del cliente OpenVPN en el equipo](#). Si decide implementar OpenVPN para su empresa, puede seguir los pasos de esta siguiente sección.

Configuración de OpenVPN en un Router RV160/RV260

Este es un proceso más complicado ya que implica obtener una CA de un tercero, lo que cuesta dinero. También debe enviar la plantilla de configuración del cliente VPN, que finaliza en `.ovpn`, a todos los clientes para que puedan configurarla en su dispositivo. Los clientes necesitan varias configuraciones iguales que el router para que se comuniquen. La mejor parte es que, por un coste mínimo, usted y sus empleados pueden utilizar Internet y realizar negocios de forma más segura.

Paso 1. Inicie sesión en el router con sus credenciales. El nombre de usuario y la contraseña predeterminados son `cisco`.

Nota: Se recomienda encarecidamente cambiar todas las contraseñas a algo más complejo. De lo contrario, es como dejar la llave en la puerta cerrada en la puerta.



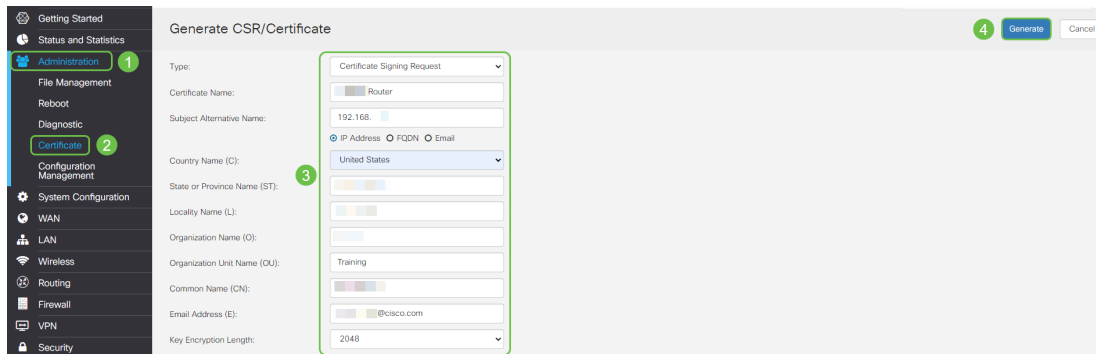
Paso 2. Es un requisito obtener un certificado. Navegue hasta **Administración > Certificado > Generar CSR/Certificado...** Esto es cómo crear la solicitud de un certificado.

The screenshot shows the Cisco Router Administration interface. 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 table, there are four buttons: "Import Certificate...", "Generate CSR/Certificate..." (3), "Show built-in 3rd party CA Certificates...", and "Select as Primary Certificate...".

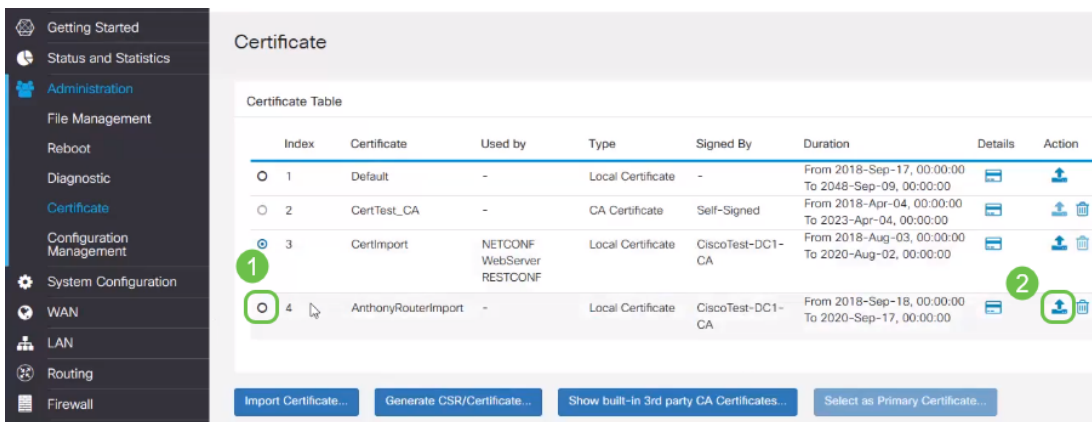
Paso 3. Realice una solicitud de un *certificado firmado por el certificado de CA*. Esto se puede encontrar navegando a **Administration > Certificate**.



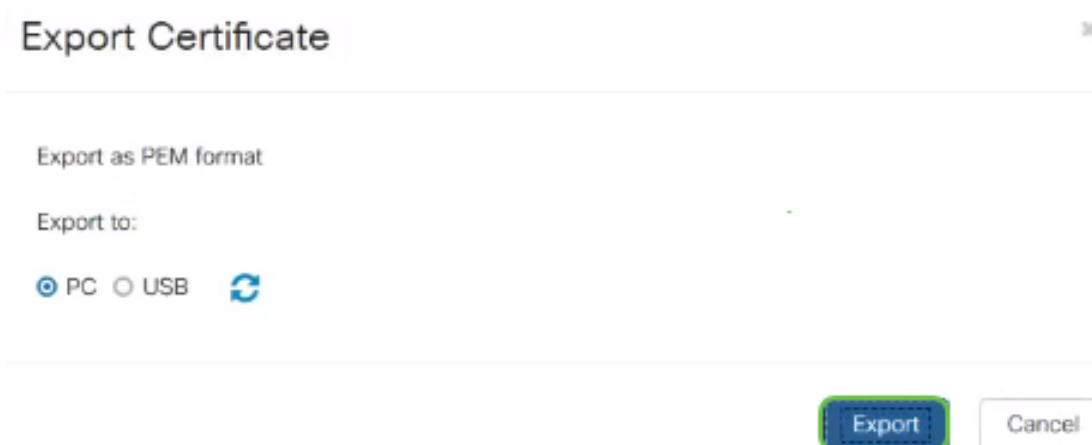
- Seleccione *Solicitud de firma de certificado* en el menú desplegable
- Introduzca un nombre de certificado
- Introduzca la dirección IP, el nombre de dominio completo (FQDN) o el correo electrónico. La elección más común es ingresar la dirección IP.
- Introduzca su país
- Introduzca su estado
- Introduzca su nombre de localidad, normalmente su ciudad
- Introduzca su nombre de organización
- Introduzca el nombre de la unidad de la organización
- Introduzca su dirección de correo electrónico
- Introduzca la longitud de cifrado de la clave; se recomienda 2048

Haga clic en el botón **Generar** arriba a la derecha

Paso 4. Seleccione Exportar haciendo clic en la flecha hacia arriba de Acción.

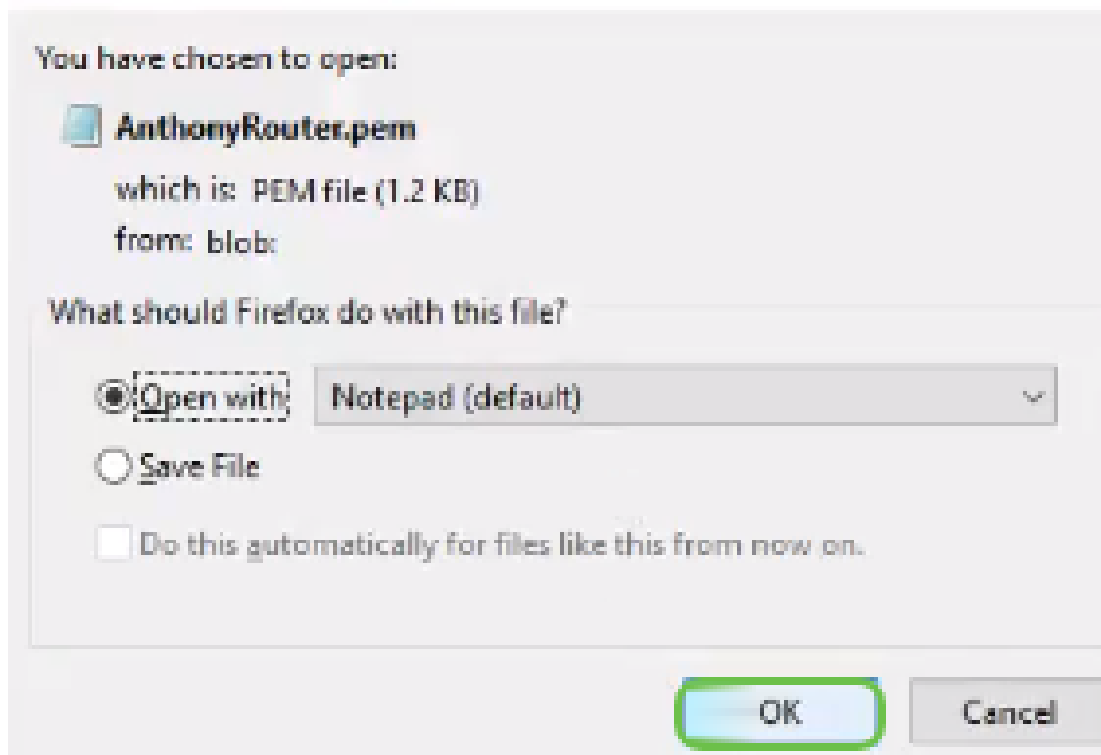


Paso 5. Aparecerá esta pantalla. Haga clic en **Exportar**.



Paso 6. Seleccione *Abrir con y Bloc de notas* (valor predeterminado) en el menú desplegable. Click OK.

Opening AnthonyRouter.pem

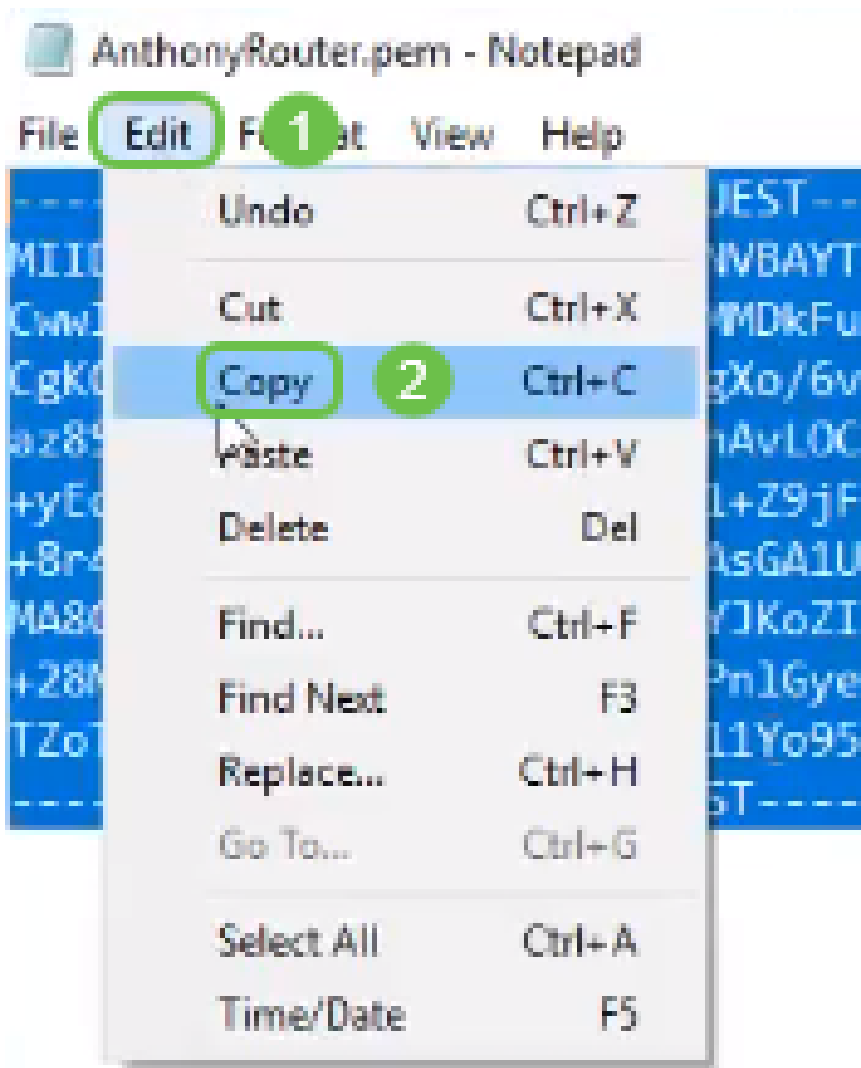


Paso 7. Se abrirá un archivo XML.



Nota: Asegúrese de que la SOLICITUD DE CERTIFICADO DE INICIO y LA SOLICITUD DE CERTIFICADO FINAL se encuentran en sus propias líneas, como se muestra anteriormente.

Paso 8. En la parte superior de la pantalla, haga clic en **Editar** y seleccione **Copiar** en el menú desplegable.



Paso 9. Elija un sitio de terceros de confianza para realizar la solicitud de certificado. Deberá pegar el archivo XML copiado como parte de la solicitud.

Nota: Si tiene un servidor de certificados interno en la red, puede usarlo en su lugar, pero esto no es común.

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):

```
TZoTKHXBcMTWpCh1jPFy8LeNH811Yo95aBO2WX2e  
cUNT4jUzYNyaV7XkREz7oY1PF5TZW9KzzAIo2W8a  
3qO6K2M=  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

Paso 10. Una vez verificado, puede elegir *Descargar certificado*.

Certificate Issued

The certificate you requested was issued to you.

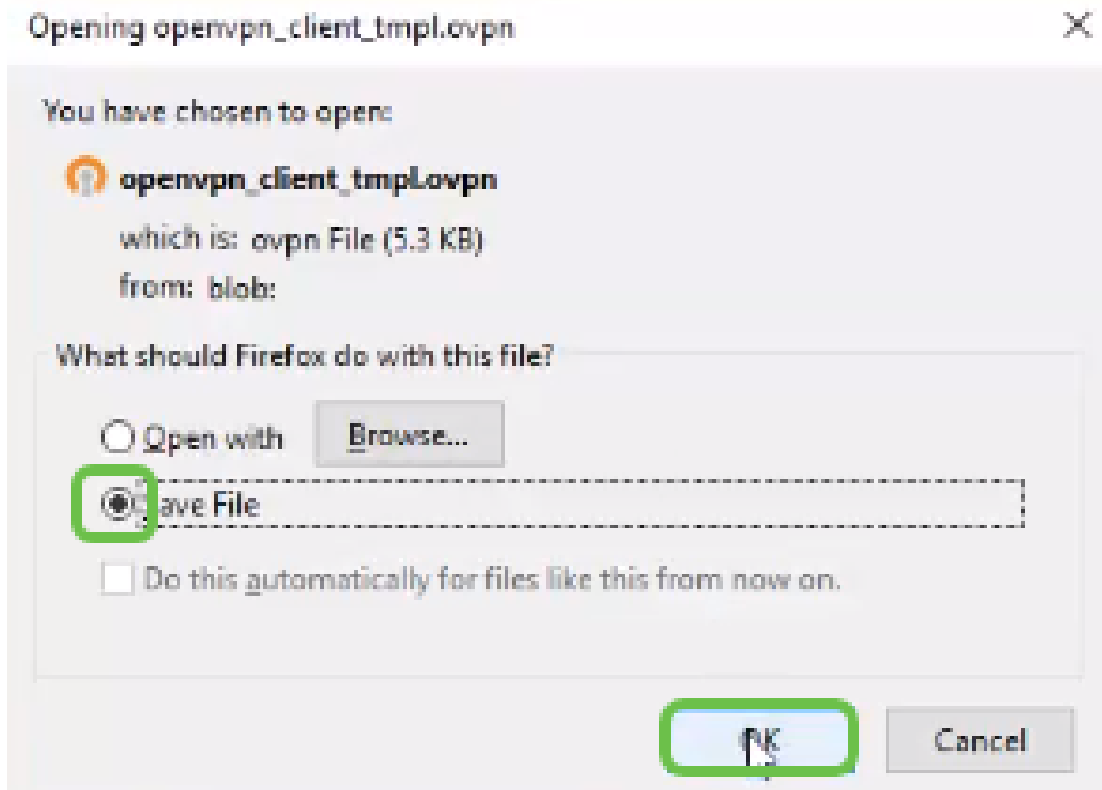
DER encoded or Base 64 encoded



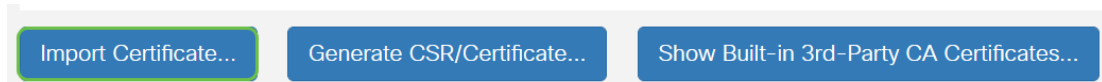
[Download certificate](#)

[Download certificate chain](#)

Paso 11. Haga clic en el botón de opción para *Guardar archivo* y haga clic en **Aceptar**.



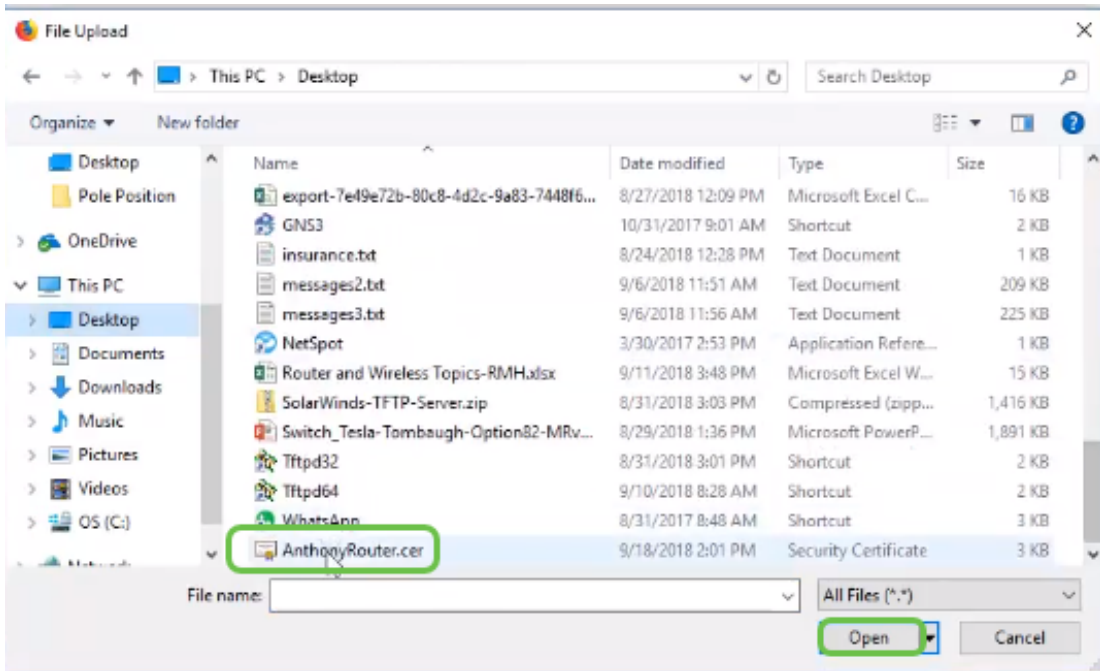
Paso 12. Una vez guardado, seleccione el botón de opción de ese certificado y haga clic en el icono de **flecha hacia abajo**.



Paso 13. Se abrirá esta pantalla. Seleccione **Examinar....**



Paso 14. Elija el archivo del certificado y haga clic en **Abrir**.



Paso 15. Ingrese el *Nombre del Certificado* para importar y haga clic en **Cargar**.

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

Paso 16. Recibirá una notificación de que el certificado se ha importado correctamente. Click OK.

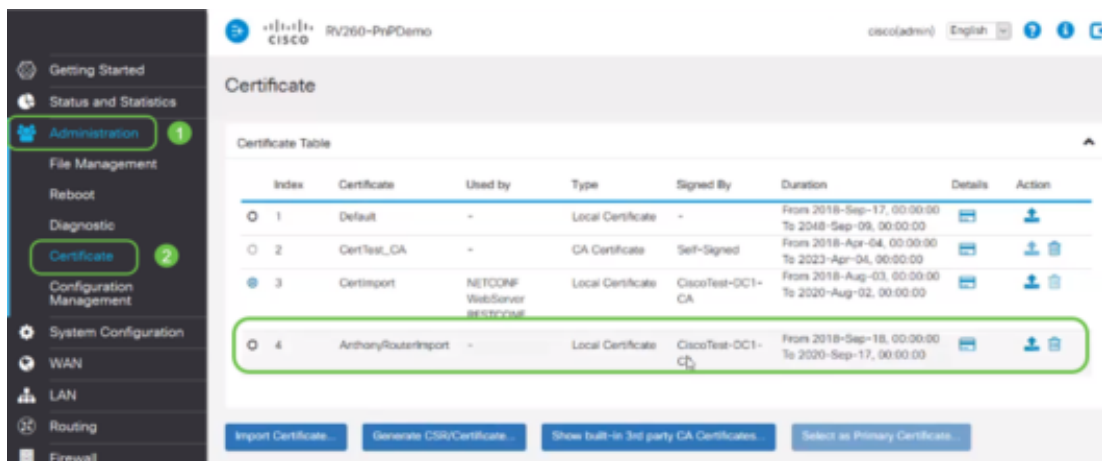
Information

Import certificate successfully!

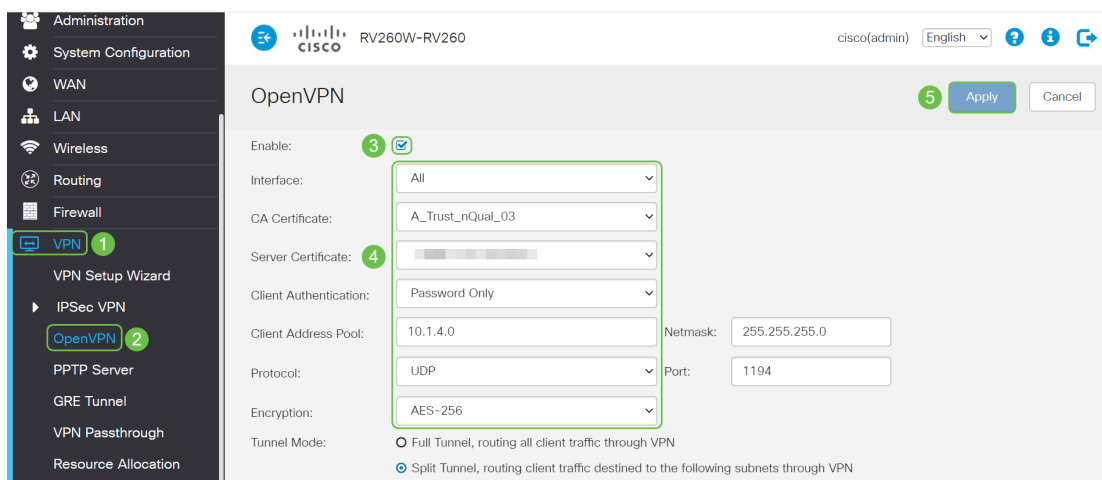
OK

Paso 17. Vaya a **Administración > Certificado**. El certificado se ha cargado.

Nota: En este ejemplo, se utilizó un servidor de certificados local.



Paso 18. Navegue hasta **VPN > OpenVPN**. Se abre la página OpenVPN. Complete lo siguiente con su información.



- Marque la casilla *Enable (Activar)*. Seleccione la interfaz que se permitirá en el tráfico. En este caso, una red de área extensa (WAN) y seleccione un certificado de autoridad certificadora (CA)
- Seleccione el *certificado de CA* en el menú desplegable
- Seleccione el *certificado de servidor* que descargó en el menú desplegable
- Seleccione *Autenticación de cliente*. Si selecciona Contraseña, deberán autenticarse con una contraseña. Si selecciona Contraseña + Certificado, el cliente también debe tener un certificado. Esto es más seguro, pero aumenta el coste de la VPN, ya que necesitarían comprar una CA independiente.
- Ingrese el *Conjunto de Direcciones de Cliente*. Elija una dirección IP en una subred de red que no se utilice en ningún otro lugar de la empresa. Seleccione uno de los intervalos reservados y elija un intervalo que no se utilice en ningún otro lugar.
- Elija la forma de *Cifrado*. Asegúrese de que el cifrado es el mismo que el cliente. No se recomiendan DES y 3DES y sólo se deben utilizar para la compatibilidad con versiones anteriores.
- Elija *Modo de túnel completo* si desea que todo el tráfico del cliente pase a través del túnel VPN o *Split* si sólo desea especificar qué tráfico pasa a través de la VPN
- La dirección IP *DNS1* puede ser un servidor DNS interno dedicado, la misma dirección IP de la gateway predeterminada proporcionada por el distribuidor de servicios de Internet (ISP), en una máquina virtual o un servidor DNS de confianza en Internet.

Haga clic en **Aplicar** para guardar la configuración.

Paso 19 (opción 1). Puede enviar esta configuración por correo electrónico al cliente. Marque la casilla *Enviar correo electrónico*. Introduzca una dirección de correo electrónico. Agregue un título de asunto para el correo electrónico. Haga clic en **Generar**.

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. 2

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): nick@cisco.com 3

Email Subject: OpenVPN Client Config

4 **Generate**

Paso 20. (Opción 2). Seleccione *Exportar plantilla de configuración de cliente (.ovpn)* y haga clic en **Generar**.

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 **Generate**

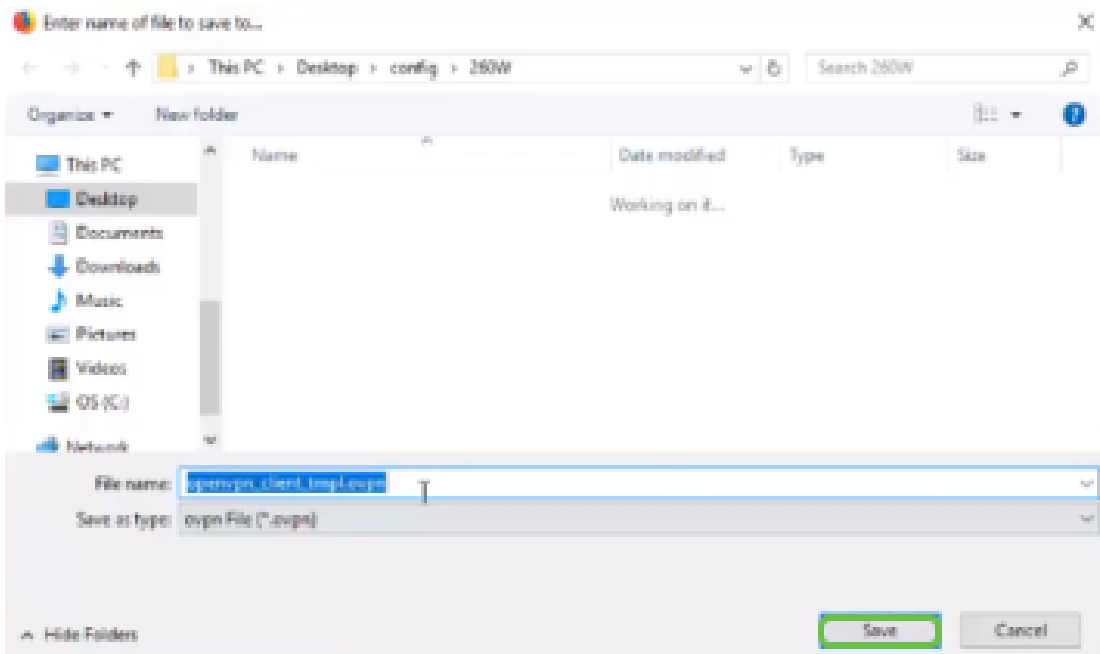
Paso 21. Recibirá una confirmación de que se ha realizado correctamente. Click OK.

Information

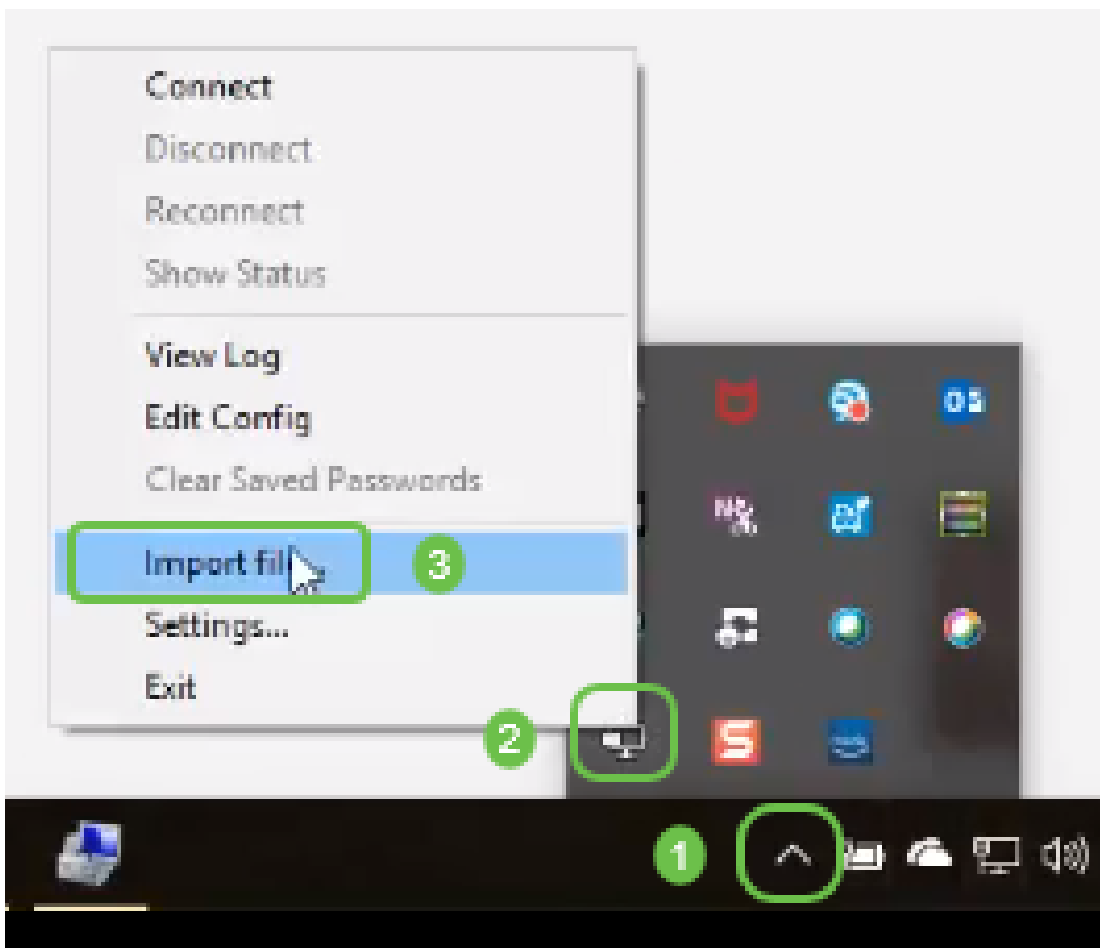
 Export client configuration template downloaded successfully!

OK

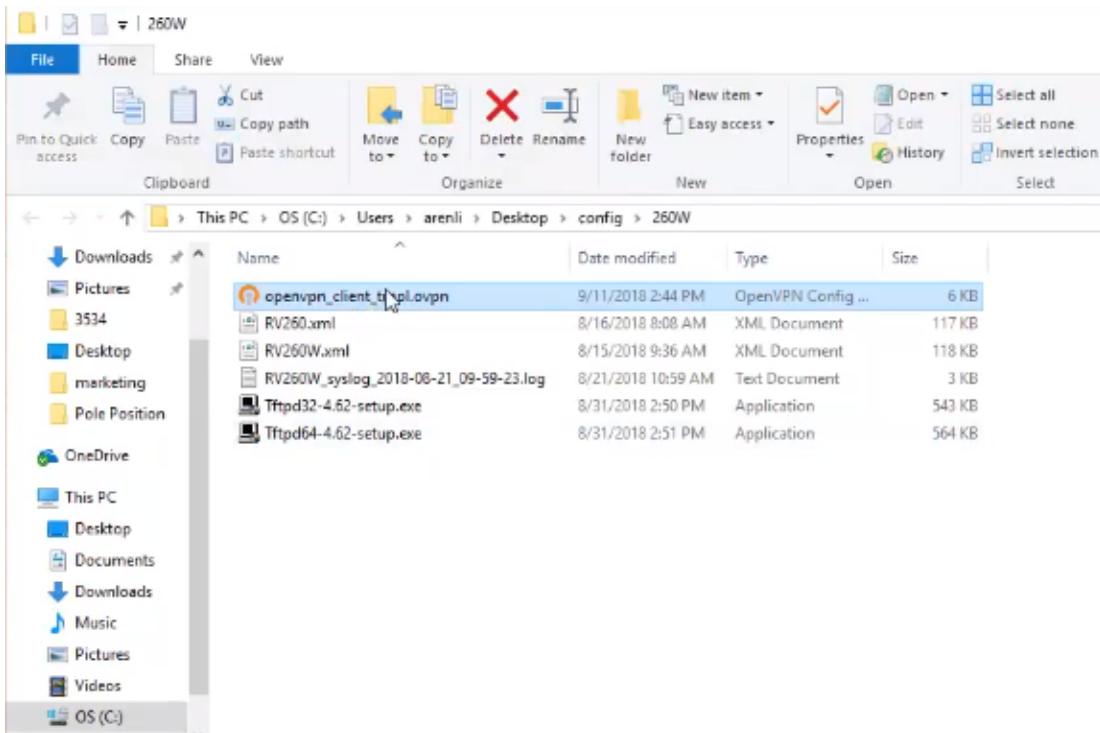
Paso 22. Click **Save**.



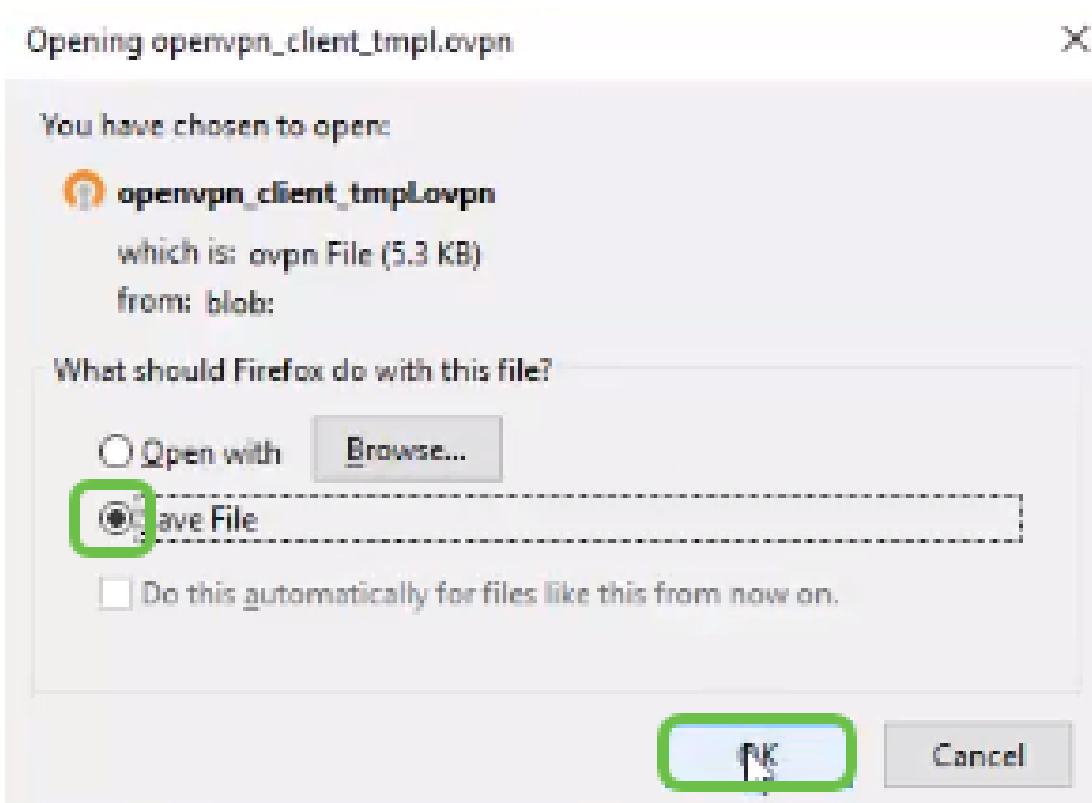
Paso 23. En la parte inferior derecha del escritorio y haga clic para abrir OpenVPN. Haga clic con el botón derecho del ratón para abrir el menú desplegable. Haga clic en *Importar archivo*.



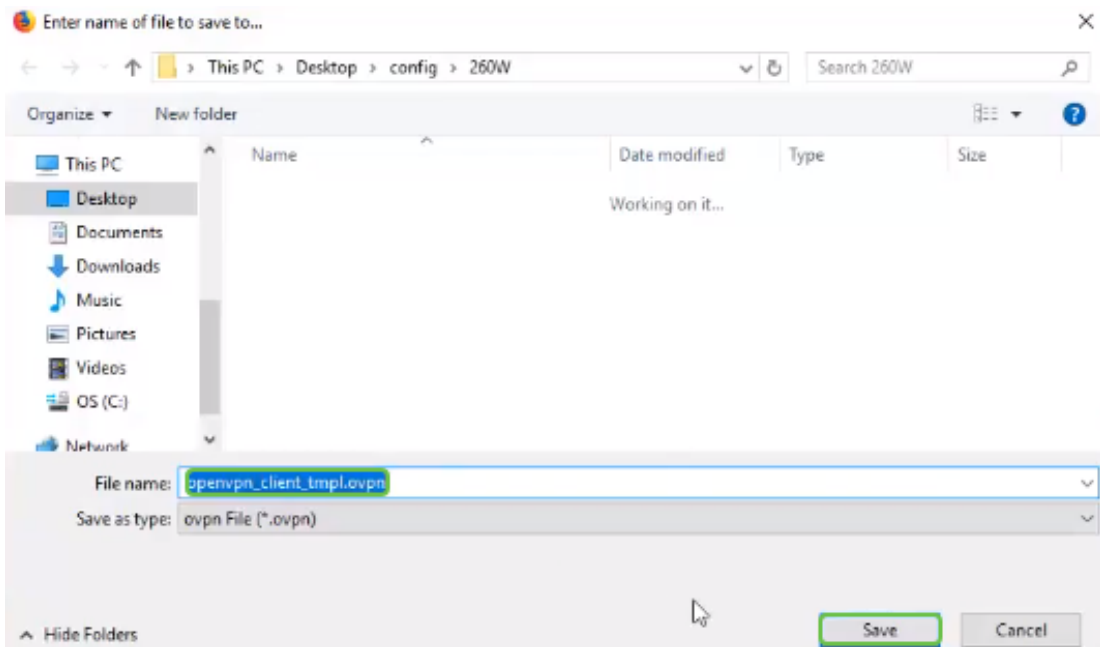
Paso 24. Seleccione el archivo OpenVPN que finaliza en *.ovpn*.



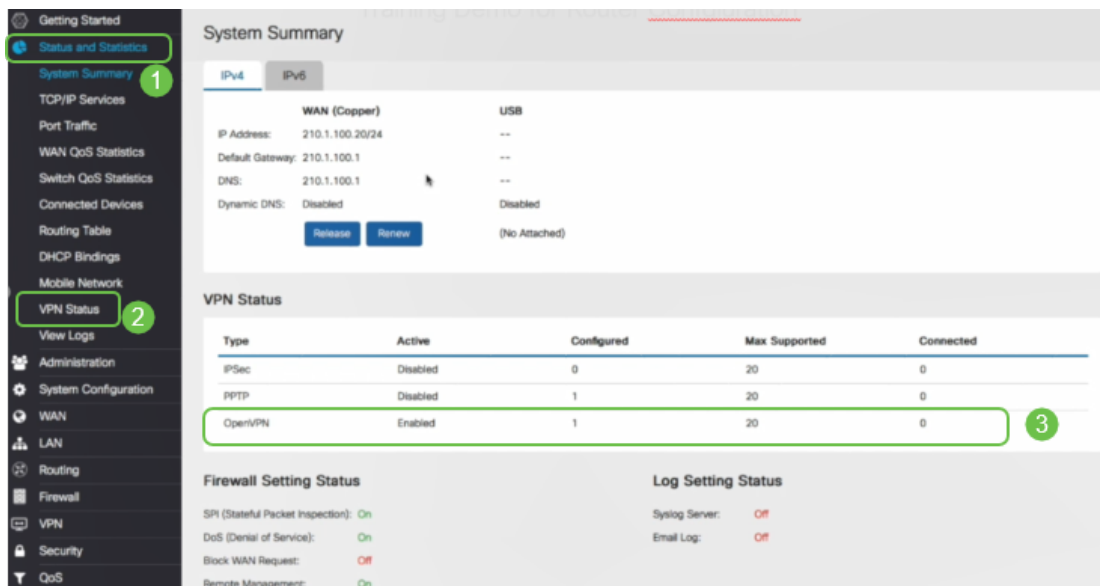
Paso 25. Haga clic en el botón de opción *Guardar archivo* y haga clic en **Aceptar**.



Paso 26. Cambie el nombre del archivo si lo desea, pero deje *.ovpn* al final del nombre del archivo. Click **Save**.



Paso 27. Navegue hasta **Estado y estadísticas > Estado de VPN**. Puede desplazarse hacia abajo para obtener información más detallada.



El router ahora está configurado con todos los parámetros necesarios para soportar una conexión OpenVPN Client para su prueba personal.

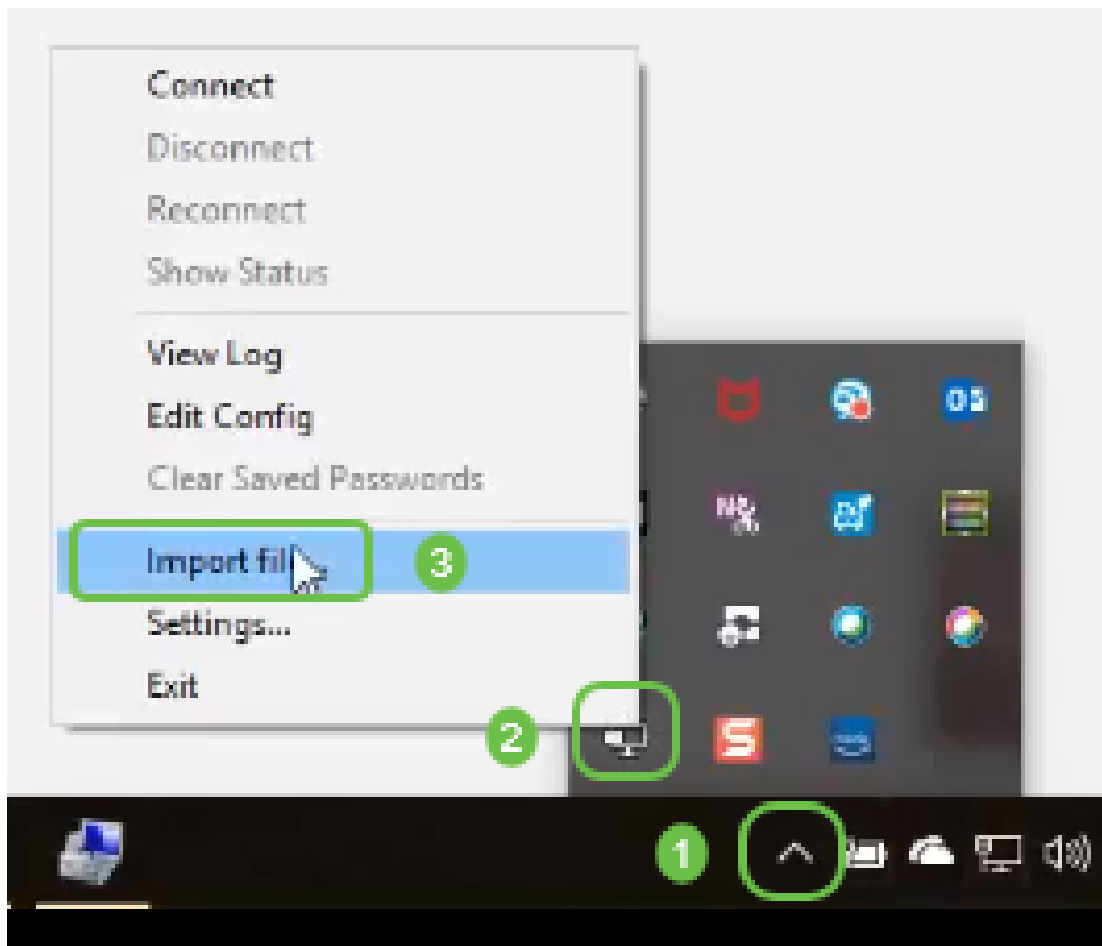
Configuración de OpenVPN Client en el equipo

Cada cliente OpenVPN debe realizar las siguientes tareas como requisito previo:

- Descargue la aplicación OpenVPN en su dispositivo.
- Abra y guarde el archivo de configuración que se envió en los pasos 19-22 de la sección anterior. El archivo de configuración finaliza en *.ovpn*.

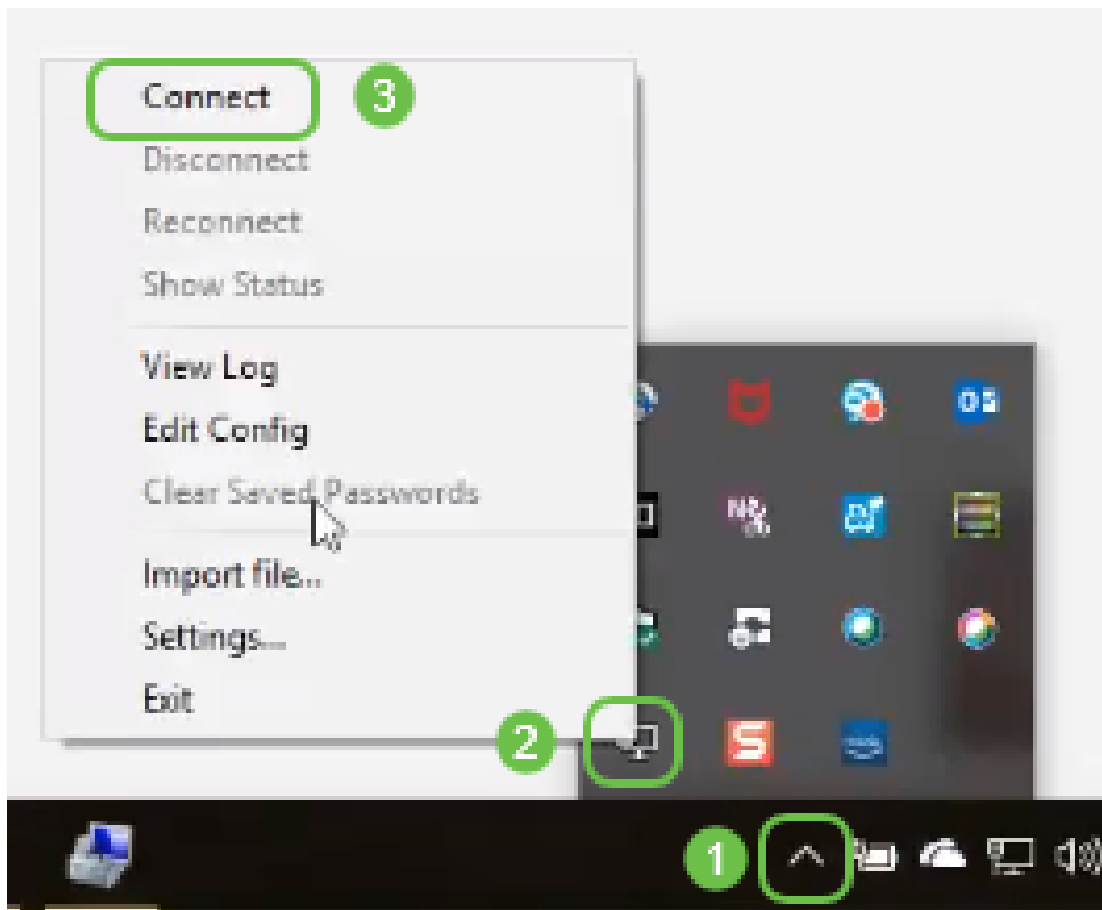
Nota: Esta configuración es específica para Windows 10.

Paso 1. Desplácese hasta el icono de flecha situado en la parte inferior derecha del escritorio y haga clic para abrir el icono OpenVPN. Haga clic con el botón derecho del ratón y seleccione *Importar archivo*.

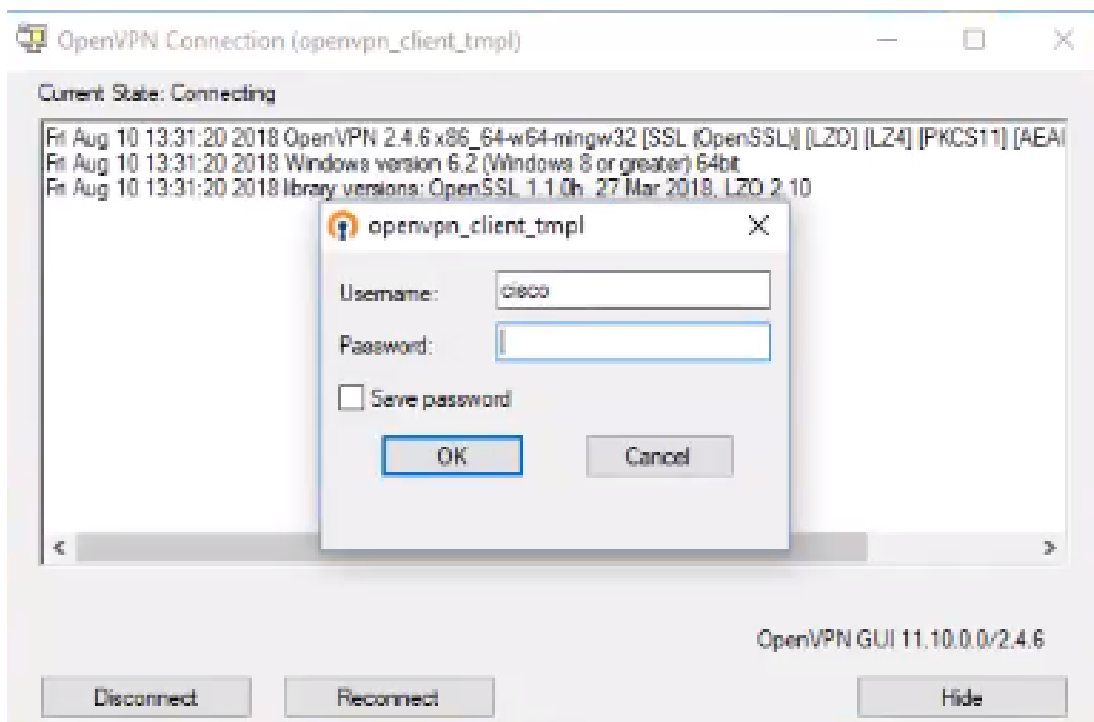


Nota: El icono es blanco y negro, lo que indica que no se está ejecutando actualmente. Una vez que se ejecute, el icono se mostrará en color.

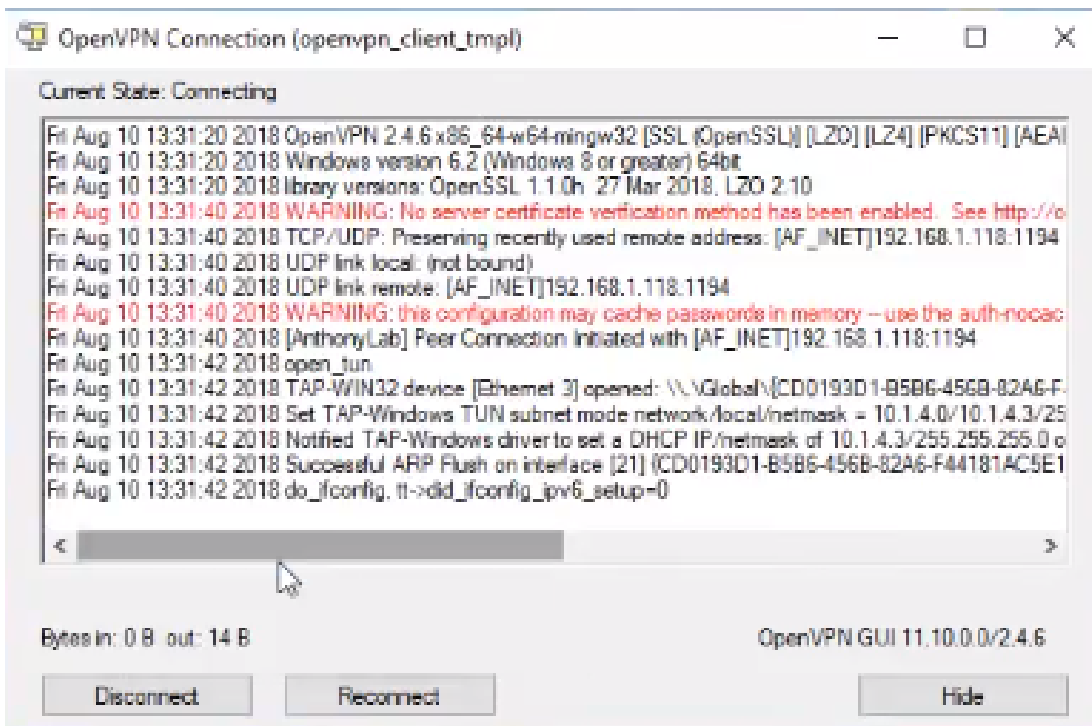
Paso 2. Haga clic en la *flecha hacia arriba*. Haga clic en el icono OpenVPN. Haga clic con el botón derecho del ratón y seleccione *Connect* en el menú desplegable.



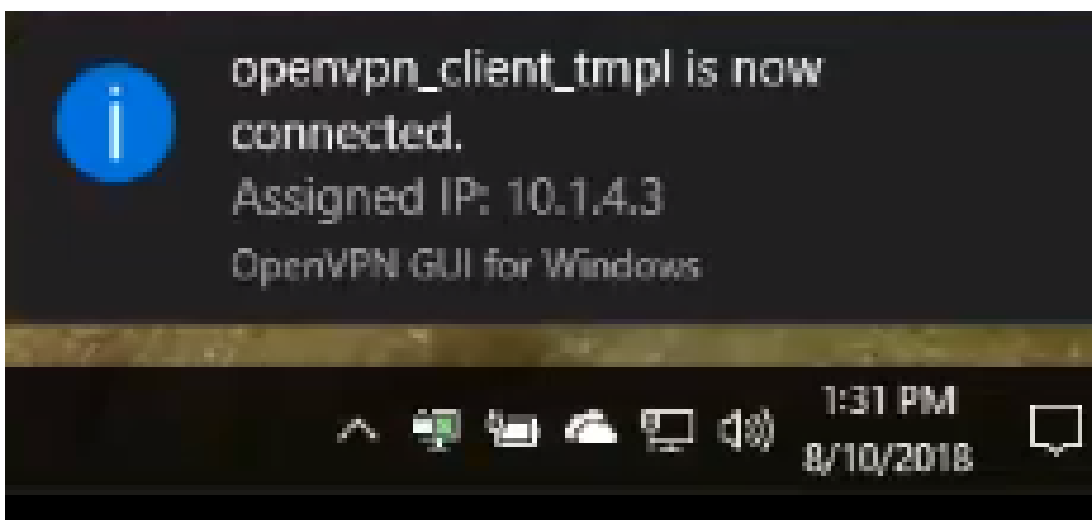
Paso 3. Ingrese el nombre de usuario y la contraseña.



Paso 4. La ventana mostrará la conexión OpenVPN junto con algunos datos de registro.

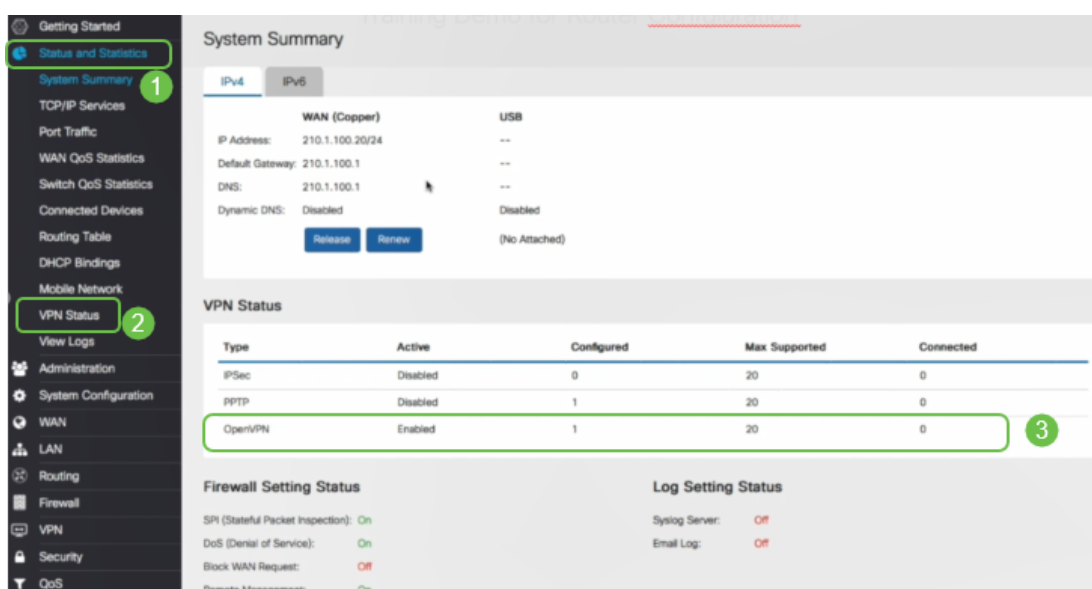


Paso 5. Un registro del sistema debe advertir que hay una conexión.



Paso 6. El cliente VPN debe ser capaz de tunelizar la información entrante y saliente a través de OpenVPN. Esto se puede configurar para que se conecte automáticamente en los parámetros de OpenVPN.

Paso 7. El administrador puede confirmar el estado de VPN navegando hasta **Estado y estadísticas > estado de VPN** en el router.



Conclusión

Ahora debería haber instalado correctamente OpenVPN en su router RV160 o RV260 y en el sitio cliente VPN.

Para los debates de la comunidad sobre OpenVPN, haga clic [aquí](#) y busque OpenVPN.

Ver un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras charlas técnicas de Cisco](#)