

Certificado (Importar/Exportar/Generar CSR) en el router serie RV160 y RV260

Objetivo

El objetivo de este documento es mostrarle cómo generar una solicitud de firma de certificado (CSR), así como importar y exportar certificados en los routers serie RV160 y RV260.

Introducción

Los certificados digitales son importantes en el proceso de comunicación. Proporciona identificación digital para la autenticación. Un certificado digital incluye información que identifica un dispositivo o usuario, como el nombre, número de serie, empresa, departamento o dirección IP.

Las autoridades de certificación (CA) son autoridades de confianza que firman certificados para verificar su autenticidad, lo que garantiza la identidad del dispositivo o usuario. Garantiza que el titular del certificado es realmente quien afirma ser. Sin un certificado firmado de confianza, los datos se pueden cifrar, pero es posible que la persona con la que se comunica no sea la persona con la que piensa. CA utiliza la infraestructura de clave pública (PKI) al emitir certificados digitales, que utiliza cifrado de clave pública o privada para garantizar la seguridad. Las CA son responsables de administrar las solicitudes de certificados y emitir certificados digitales. Algunos ejemplos de CA son: IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verisign y muchos más.

Los certificados se utilizan para conexiones Secure Socket Layer (SSL), Transport Layer Security (TLS), Datagram TLS (DTLS), como el protocolo de transferencia de hipertexto (HTTPS) y el protocolo de acceso a directorios ligeros seguros (LDAPS).

Dispositivos aplicables

- RV160
- RV260

Versión del software

- 1.0.00.15

Table Of Contents

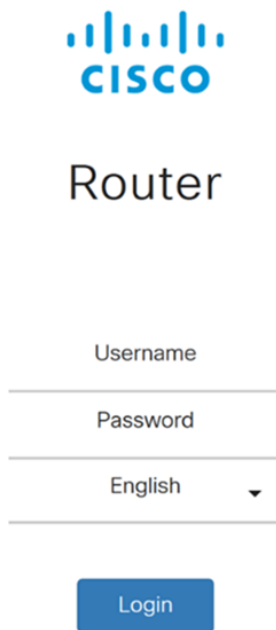
A través de este artículo:

1. [Generar CSR/Certificado](#)
2. [Visualización de certificado](#)

3. [Exportar certificado](#)
4. [Importar certificado](#)
5. [Conclusión](#)

Generar CSR/Certificado

Paso 1. Inicie sesión en la página de configuración web.

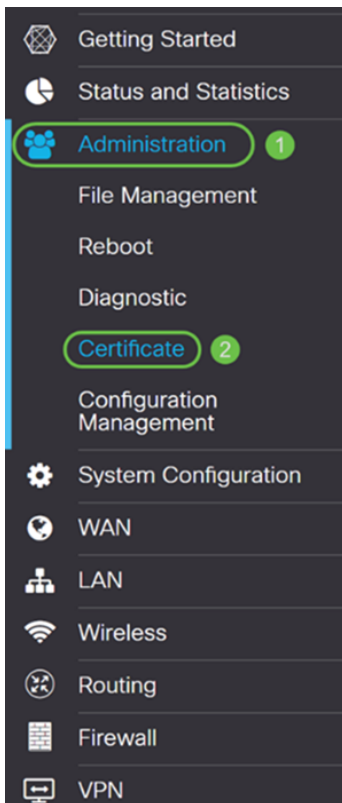


The image shows the Cisco Router login page. At the top is the Cisco logo, followed by the word "Router". Below this are three input fields: "Username", "Password", and a language dropdown menu currently set to "English". A blue "Login" button is positioned below the language dropdown.

©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. Vaya a **Administración > Certificado**.



Paso 3. En la página *Certificate*, haga clic en el botón **Generate CSR/Certificate....**

Certificate

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		

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

Paso 4. Seleccione el tipo de certificado que desea generar a partir de una de las opciones siguientes de la lista desplegable.

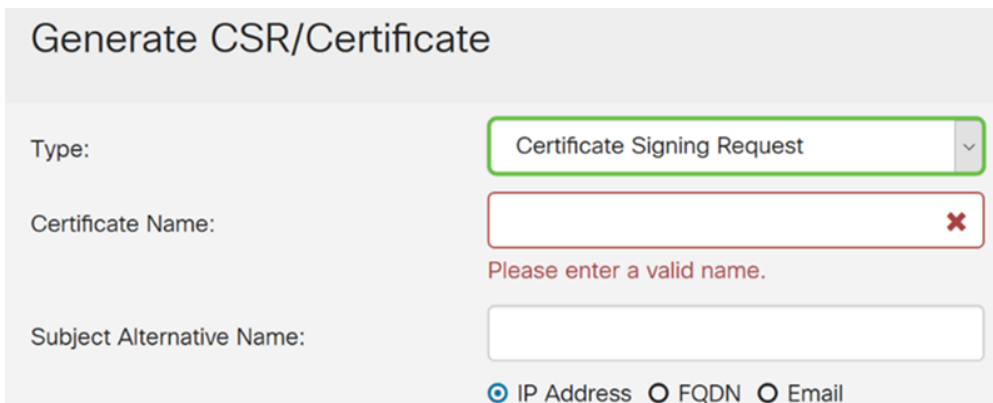
- **Certificado firmado automáticamente:** σε τρατα δε υν χειρτιφιχαδο δε χαπα δε σοχκετ σεγυρο (ΣΣΛ) φιρμαδο πορ συ προπιο χρεαδορ. Este certificado es menos confiable, ya que no se puede cancelar si la clave privada está comprometida de alguna manera por un atacante. Debe proporcionar la duración válida en días.

- **Certificado CA:** σελεχχιονε εστε τιπο δε χειρτιφιχαδο παρα θυε ελ ρουτερ αχτ λε χομο υνα αυτοριδαδ δε χειρτιφιχαδοσ υντερνα ψ εμιτα χειρτιφιχαδοσ. Desde el punto de vista de la seguridad, es similar a un certificado autofirmado. Esto se puede utilizar para OpenVPN.

- **Solicitud de firma de certificado:** se trata de una infraestructura de clave pública (PKI) que se envía a la autoridad de certificación para solicitar un certificado de identidad digital. Es más seguro que autofirmado, ya que la clave privada se mantiene en secreto. Se recomienda esta opción.

• **Certificado firmado por certificado de CA:** σελεγχιونه εστε τιπο δε χερτιφιχαδο ψ προπορχιونه λος δεταλλεσ ρελεπωντες παρα θυε ελ χερτιφιχαδο σεα φιρμαδο πορ συ αυτοριδαδ δε χερτιφιχαχι (ν ιντερνα.

En este ejemplo, seleccionaremos **Solicitud de firma de certificado**.



Generate CSR/Certificate

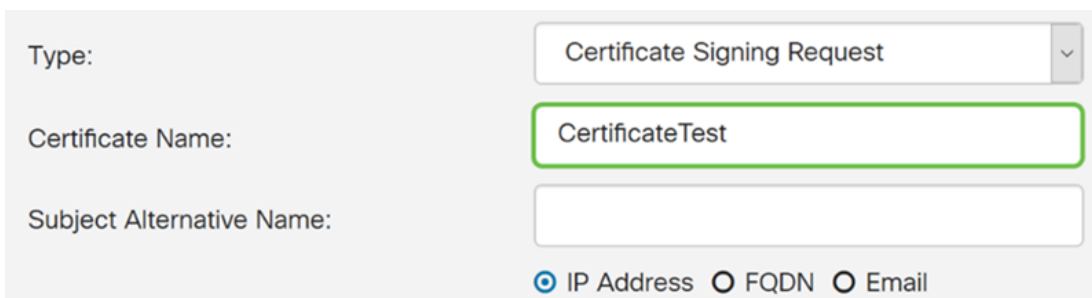
Type: Certificate Signing Request

Certificate Name: ✘
Please enter a valid name.

Subject Alternative Name:

IP Address FQDN Email

Paso 5. Introduzca el *nombre del certificado*. En este ejemplo, ingresaremos **CertificateTest**.



Type: Certificate Signing Request

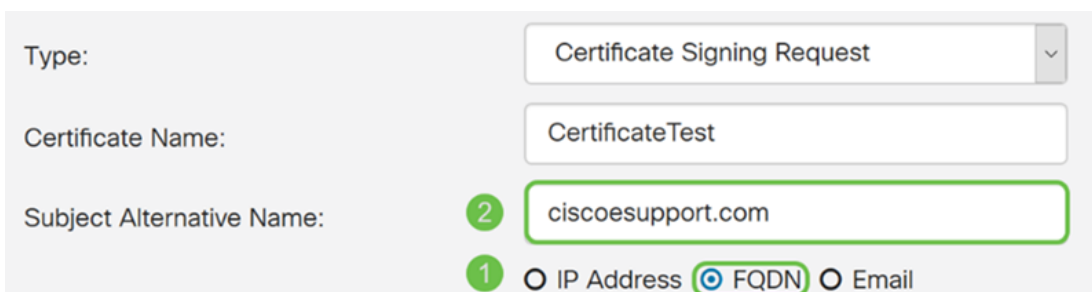
Certificate Name: CertificateTest

Subject Alternative Name:

IP Address FQDN Email

Paso 6. En el campo *Nombre alternativo del sujeto*, seleccione una de las siguientes opciones: **Dirección IP**, **FQDN** (Nombre de dominio completamente calificado) o **Correo electrónico y, a continuación, introduzca el nombre adecuado de lo que ha seleccionado**. Este campo permite especificar nombres de host adicionales.

En este ejemplo, seleccionaremos **FQDN** e introduciremos **ciscoesupport.com**.



Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name: ciscoesupport.com 2

1 IP Address FQDN Email

Paso 7. Seleccione un **país** en la lista desplegable *Nombre del país (C)*.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text"/>
Locality Name (L):	<input type="text"/>
Organization Name (O):	<input type="text"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Paso 8. Ingrese un **estado** o **nombre de provincia** en el campo *Nombre de estado o provincia*.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text"/>
Organization Name (O):	<input type="text"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Paso 9. En el *nombre de localidad*, introduzca un **nombre de ciudad**.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text" value="San Jose"/>
Organization Name (O):	<input type="text"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Paso 10. Introduzca el nombre de la **organización** en el campo *Organization Name*.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text" value="San Jose"/>
Organization Name (O):	<input type="text" value="Cisco"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Paso 11. Introduzca el nombre de la **unidad de organización** (formación, soporte, etc.).

En este ejemplo, entraremos en **eSupport** como nombre de unidad de nuestra organización.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	
Email Address (E):	
Key Encryption Length:	2048

Paso 12. Introduzca un **nombre común**. Es el FQDN del servidor web el que recibirá este certificado.

En este ejemplo, **ciscosmbsupport.com** se utilizó como nombre común.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	
Key Encryption Length:	2048

Paso 13. Introduzca una **dirección de correo electrónico**.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	k[redacted]@cisco.com
Key Encryption Length:	2048

Paso 14. Seleccione **Key Encryption Length** en el menú desplegable. Las opciones son: **512, 1024, o 2048**. Cuanto mayor sea el tamaño de la clave, más seguro será el certificado. Cuanto mayor sea el tamaño de la clave, mayor será el tiempo de procesamiento.

Práctica recomendada: Se recomienda elegir la longitud de cifrado de clave más alta, lo que permite una encriptación más estricta.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	k[redacted]@cisco.com
Key Encryption Length:	2048

Paso 15. Haga clic en **Generar**.

Generate CSR/Certificate Generate Cancel

Certificate Name:

Subject Alternative Name:
 IP Address FQDN Email

Country Name (C):

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length:

Paso 16. Aparecerá una ventana emergente *Information* con un mensaje "¡Generar certificado correctamente!" mensaje. Para continuar, haga clic en OK (Aceptar).

Information ✕

Generate certificate successfully!

OK

Paso 17. Exportar la CSR desde la *Tabla de Certificados*.

Certificate Table ▲							
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CertificateTest	-	Certificate Signing Request	-	-		

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

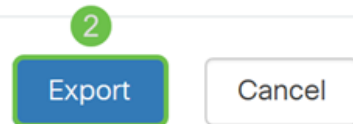
Paso 18. Aparecerá una ventana *Exportar certificado*. Seleccione **PC** para *Export to* y luego haga clic en **Export**.

Export Certificate



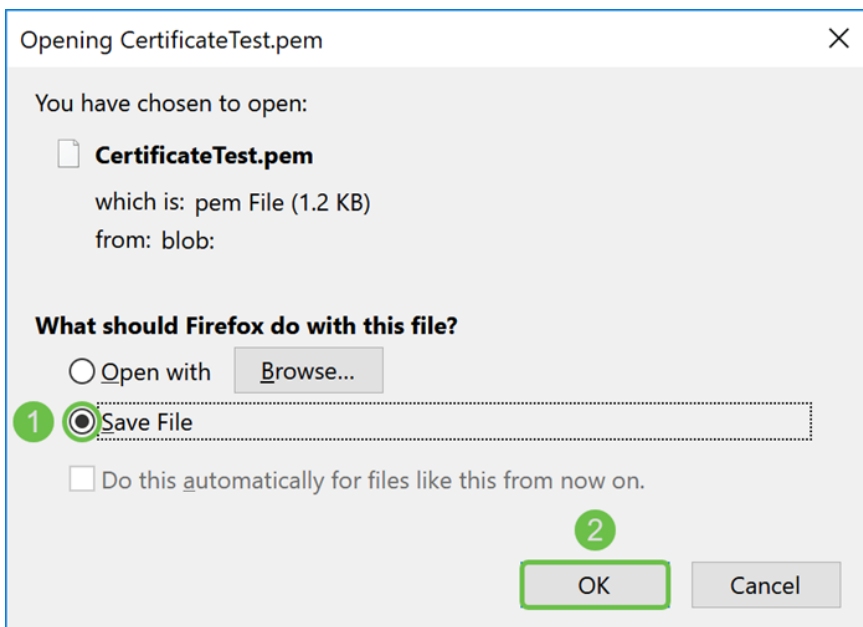
Export as PEM format

Export to:



Paso 19. Aparecerá otra ventana en la que se le preguntará si desea abrir o guardar el archivo.

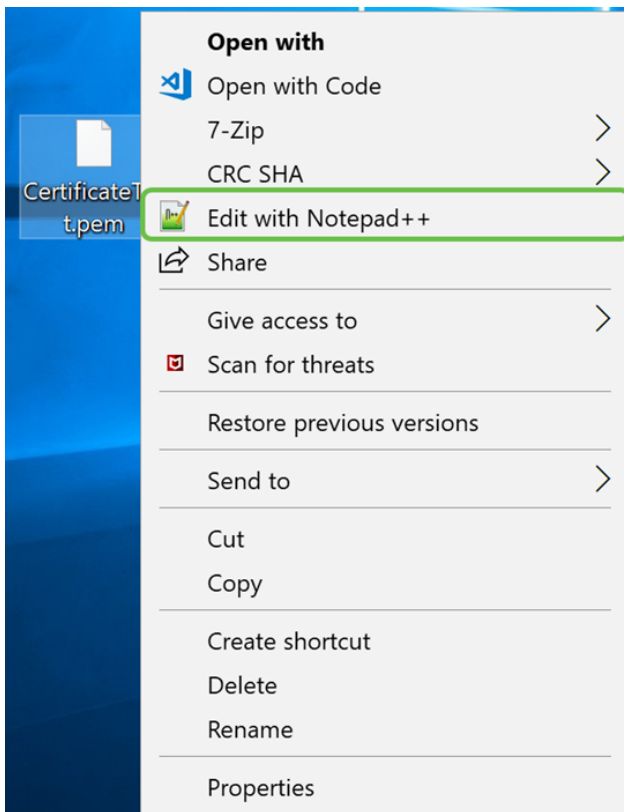
En este ejemplo, seleccionaremos **Guardar archivo** y luego haremos clic en **Aceptar**.



Paso 20. Busque la ubicación en la que se guardó el archivo .pem. **Haga clic con el botón derecho del ratón en el archivo .pem** y ábralo con su editor de texto favorito.

En este ejemplo, abriremos el archivo .pem con Notepad++.

Nota: No dude en abrirlo con el Bloc de notas.



Paso 21. Asegúrese de que la **—INICIAR SOLICITUD DE CERTIFICADO—** y **—FINALIZAR SOLICITUD DE CERTIFICADO—** se encuentre en su propia línea.



Nota: Algunas partes del certificado fueron borradas.

```
CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 [REDACTED] VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwwIU2FuIEpvc2UxDjAMBgNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY21zY29zbWJzdXBwb3J0 [REDACTED]
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXplu
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LAFoLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv [REDACTED]
9 soTqNBrYqR8h46NHh0J5fMXDsPY1j2LWmS1VbkskoiMdr5SZlwmhkrqgLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAaCBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BAIw [REDACTED].gXg
13 MCcGA1UdJQogMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY21zY29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAILUeIUy
15 TqFZ2wQx3r29E1SWOU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16
17
18
19
20
21 -----END CERTIFICATE REQUEST----- 2
22
```

Paso 22. Cuando tenga su CSR, deberá ir a sus servicios de alojamiento o a un sitio de la autoridad certificadora (es decir, GoDaddy, Verisign, etc.) y solicitar un certificado. Una vez que haya enviado una solicitud, se comunicará con el servidor de certificados para asegurarse de que no hay ningún motivo para no emitir el certificado.







Nota: Póngase en contacto con la CA o el soporte del sitio de alojamiento si no sabe dónde se encuentra la solicitud de certificado en su sitio.

Paso 23. Descargue el certificado una vez que se haya completado. Debe ser un archivo **.cer** o **.crt**. En este ejemplo, se nos proporcionaron ambos archivos.

Name	Date modified	Type	Size
 CertificateTest.cer	4/10/2019 2:03 PM	Security Certificate	2 KB
 CertificateTest.crt	4/10/2019 2:04 PM	Security Certificate	3 KB

Paso 24. Vuelva a la página *Certificate* del router e importe el archivo de certificado haciendo clic en la **flecha que apunta al icono del dispositivo**.

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CertificateTest	-	Certificate Signing Request	-	-		  

Paso 25. En el campo *Nombre del certificado*, ingrese el **nombre del certificado**. No puede tener el mismo nombre que la solicitud de firma de certificado. En la sección *Cargar archivo de certificado*, seleccione **importar desde PC** y haga clic en **Examinar...** para cargar su archivo de certificado.

Import Signed-Certificate

Type: Local Certificate

Certificate Name: 1

Upload Certificate file

2

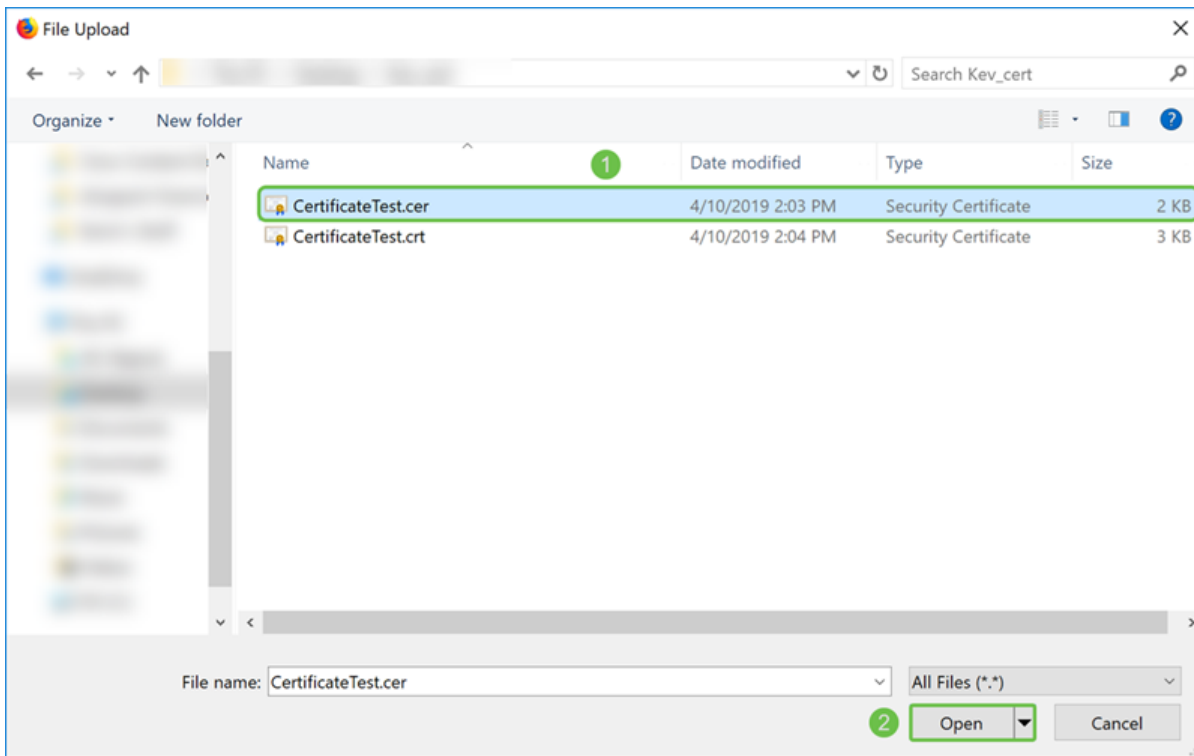
Import from PC

3 No file is selected

Import from USB 

No file is selected

Paso 26. Aparecerá una ventana *Carga de archivos*. Desplácese hasta la ubicación en la que se encuentra el archivo de certificado. Seleccione el archivo **de certificado** que desea cargar y haga clic en **Abrir**. En este ejemplo, se seleccionó **CertificateTest.cer**.



Paso 27. Haga clic en el botón **Cargar** para comenzar a cargar el certificado en el router.

Nota: Si se produce un error en el que no se puede cargar el archivo .cer, es posible que se deba a que el router requiere que el certificado esté en una codificación pem. Tendría que convertir la codificación der (extensión de archivo .cer) en una codificación pem (extensión de archivo .crt).

Import Signed-Certificate



Type: Local Certificate

Certificate Name: CiscoSMB

Upload Certificate file

Import from PC

Browse...

CertificateTest.cer

Import from USB



Browse...

No file is selected

Upload

Cancel






Paso 28. Si la importación se ha realizado correctamente, debería aparecer una ventana de *información* que le haga saber que se ha realizado correctamente. Para continuar, haga clic en OK (Aceptar).

 Import certificate successfully!

OK

Paso 29. El certificado debe actualizarse correctamente. Debe poder ver quién ha firmado el certificado. En este ejemplo, podemos ver que nuestro certificado fue firmado por *CiscoTest-DC1-CA*. Para convertir el certificado en nuestro certificado primario, selecciónelo usando el botón de opción de la izquierda y haga clic en el botón **Seleccionar como certificado primario**....

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action	
<input type="radio"/>	1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input checked="" type="radio"/>	2	CiscoSMB	-	Local Certificate	CiscoTest- DC1-CA	From 2019-Apr-10, 00:00:00 To 2021- Apr-09, 00:00:00		 

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

Nota: Si cambia el certificado primario, puede volver a una página de advertencia. Si utiliza Firefox y aparece como una página en blanco gris, tendría que ajustar alguna configuración en Firefox. Este documento en Mozilla wiki da alguna explicación al respecto: [CA/AddRootToFirefox](#). Para poder ver la página de advertencia de nuevo, [siga estos pasos que se encontraron en la página de soporte comunitario de Mozilla](#).

Paso 30. En la página de advertencia de Firefox, haga clic en **Avanzado...** y luego **Aceptar el Riesgo y Continuar** para volver al router.

Nota: Esta pantalla de advertencias varía de un navegador a otro, pero realiza las mismas funciones.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.2.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

Go Back (Recommended)

Advanced...

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.2.1. The certificate is only valid for ciscoesupport.com.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

[View Certificate](#)

Go Back (Recommended)

Accept the Risk and Continue

Paso 31. En la Tabla de Certificados, debe ver que NETCONF, *WebServer*, y RESTCONF se ha cambiado a su nuevo certificado en lugar de utilizar el certificado Default.

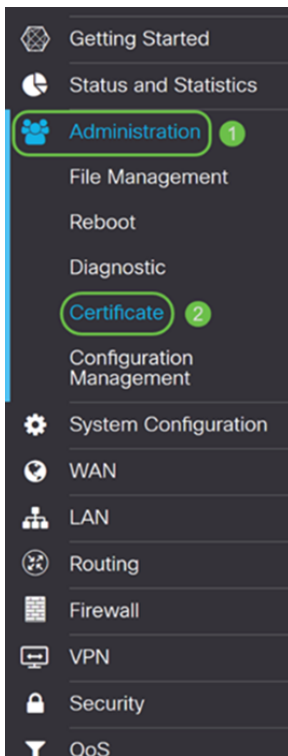
Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Ahora debería haber instalado correctamente un certificado en el router.

Visualización de certificado

Paso 1. Si se ha desplazado fuera de la página *Certificate*, navegue hasta **Administration > Certificate**.



Paso 2. En la *Tabla de Certificados*, haga clic en el icono **Detalles** ubicado bajo la sección *Detalles*.

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Paso 3. Aparece la página *Detalles del certificado*. Debe poder ver toda la información sobre su certificado.

Certificate Detail

✕

Name: CiscoSMB
Country: US
State Province: CA
Subject Alternative Name: ciscoesupport.com
Subject Alternative Type: Fqdn-Type
Subject-DN: C=US,ST=CA,L=San Jose,O=Cisco,OU=eSupport,CN=ciscosmbsupport.com,emailAddress=k[redacted]@cisco.com
Locality: San Jose
Organization: Cisco
Organization Unit Name: eSupport
Common: ciscosmbsupport.com
Email: k[redacted]@cisco.com
Key Encryption Length: 2048

Close

Paso 4. Haga clic en el icono de **bloqueo** situado en el lado izquierdo de la barra de localizador uniforme de recursos (URL).

Nota: Los siguientes pasos se utilizan en un navegador Firefox.

Cisco RV160 VPN Router

https://192.168.2.1/#/certificate

RV160--router5680AA

cisco(admin) English

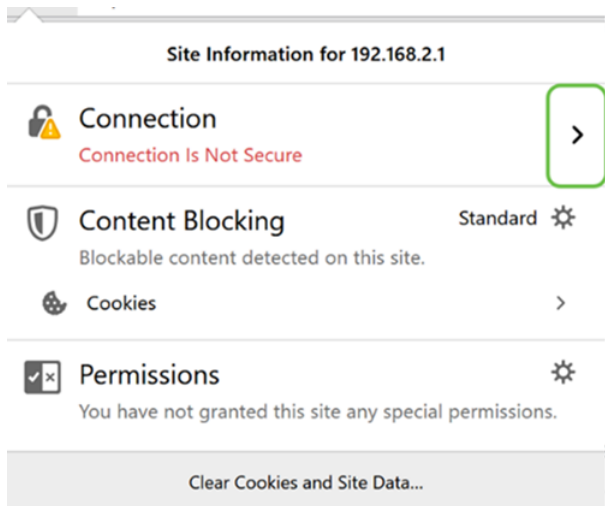
Certificate

Certificate Table

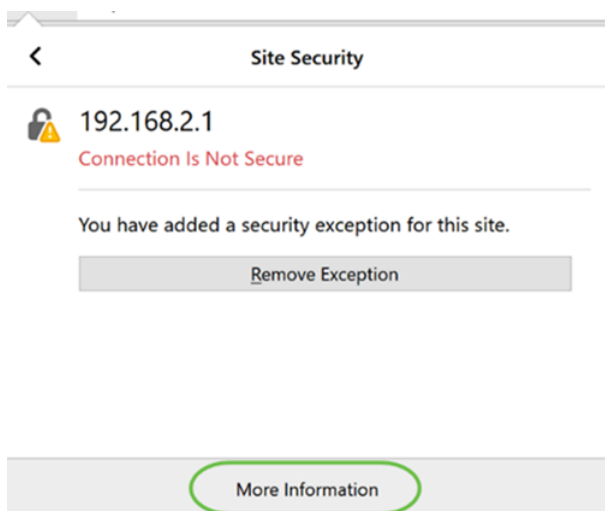
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

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

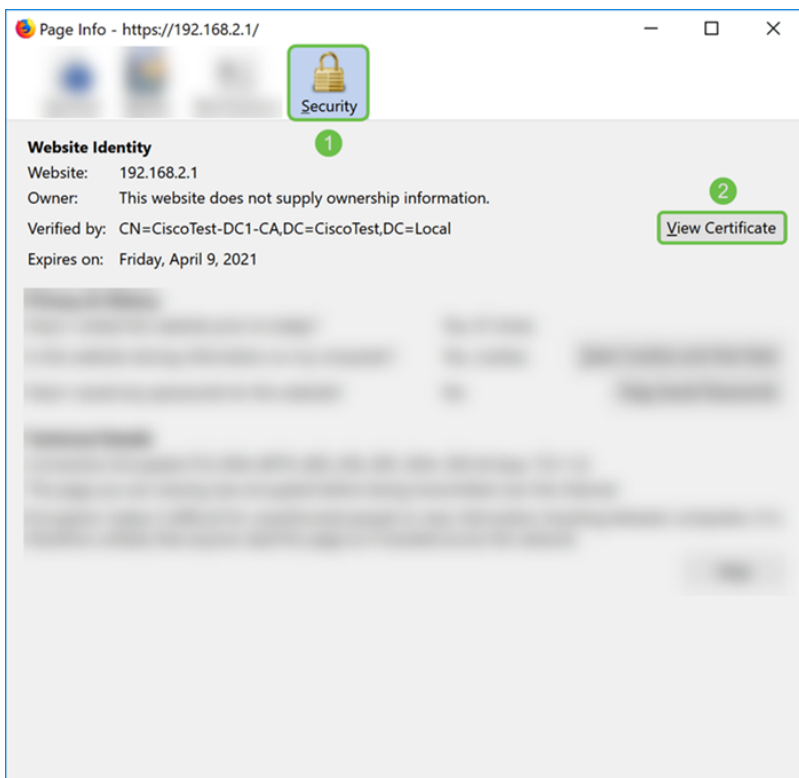
Paso 5. Aparece una lista desplegable de opciones. Haga clic en el icono de **flecha** junto al campo *Connection*.



Paso 6. Haga clic en **Más información**.

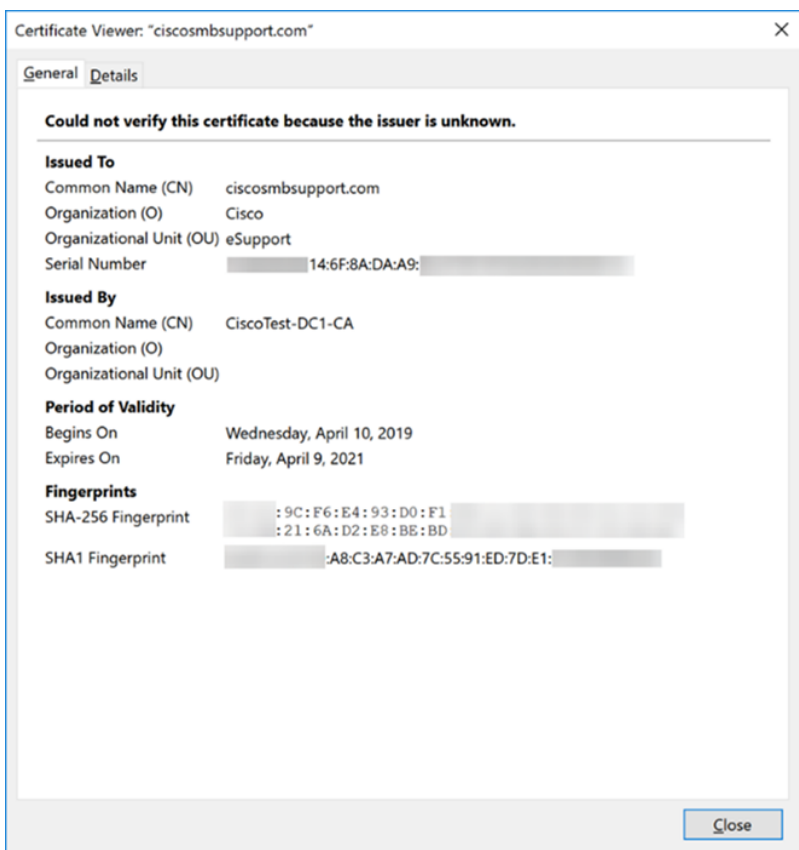


Paso 7. En la ventana *Información de la página*, debería poder ver una breve información sobre su certificado en la sección *Identidad del sitio web*. Asegúrese de que se encuentra en la ficha **Seguridad** y, a continuación, haga clic en **Ver certificado** para ver más información sobre su certificado.



Paso 8. Debería aparecer la página *Visor de certificados*. Debe poder ver toda la información sobre su certificado, período de validez, huellas dactilares y por quién fue emitido.

Nota: Dado que este certificado fue emitido por nuestro servidor de certificados de prueba, el emisor es desconocido.



Exportación de certificado

Para descargar el certificado para importarlo en otro router, siga estos pasos.

Paso 1. En la página *Certificate*, haga clic en el **icono export** junto al certificado que desea exportar.

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
○ 1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
⦿ 2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Paso 2. Aparece un *certificado de exportación*. Seleccione un formato para exportar el certificado. Las opciones son:

• **PKCS#12** – Πύβλιχ Κεψ Χρηπτογραπτηψ Στανδαρδσ (ΠΚΧΣ) #12 εσ υν χερτιφιχαδο εζπορταδο θνε σε ινχλυψε εν υνα εζτενσι (ν .π12. Se requerirá una contraseña para cifrar el archivo para protegerlo a medida que se exporta, importa y elimina.

• **PEM** - Privacy Enhanced Mail (PEM) se utiliza a menudo en servidores web para que puedan traducirse fácilmente a datos legibles mediante un editor de texto simple, como el bloc de notas.

Seleccione **Export as PKCS#12 format** e ingrese una **contraseña** y **confirm password**. A continuación, seleccione **PC** como *Exportar a:* campo. Haga clic en **Exportar** para comenzar a exportar el certificado a su equipo.

Nota: Recuerde esta contraseña porque la utilizará al importarla a un router.

Export Certificate

1
 Export as PKCS#12 format

Enter Password:

Confirm Password:

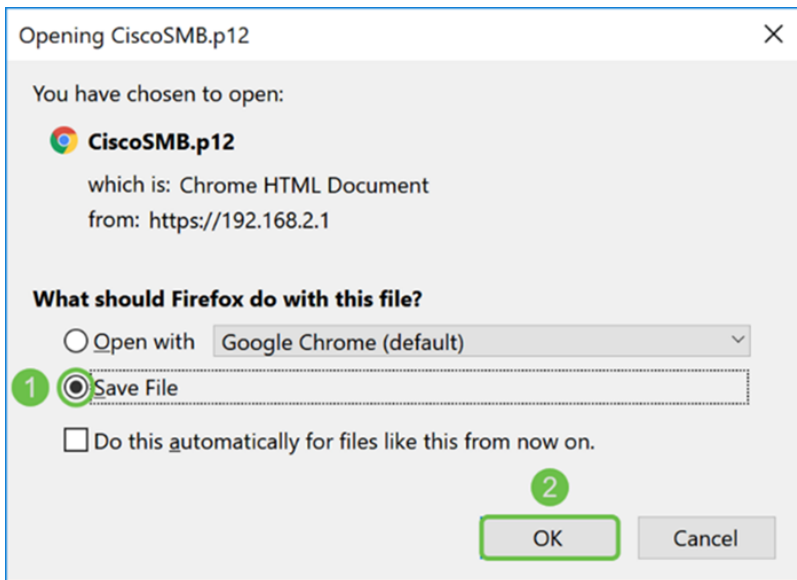
Export as PEM format

Export to:

3
 PC USB

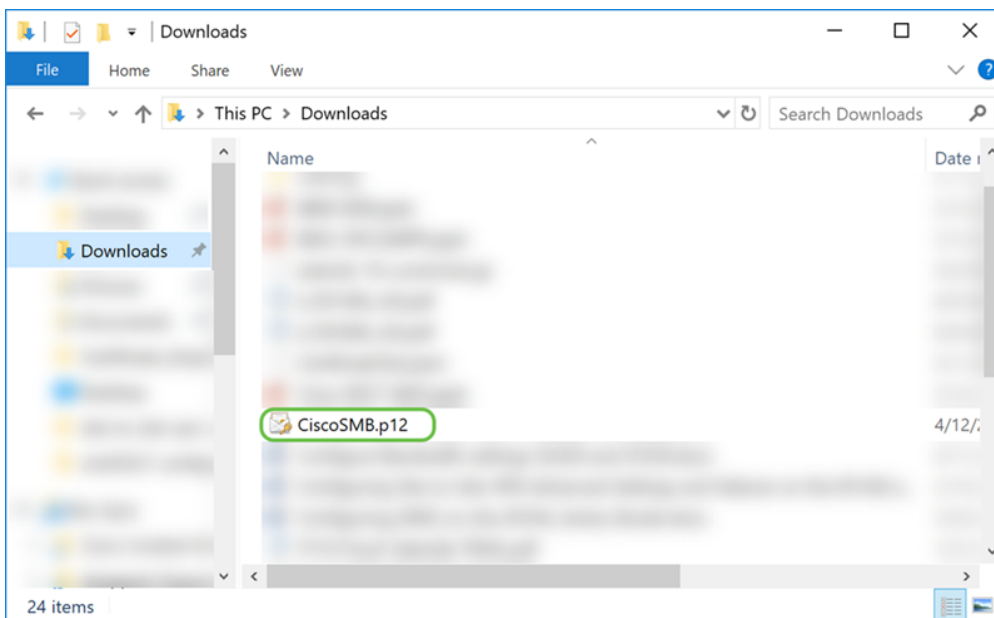
4

Paso 3. Aparecerá una ventana en la que se le preguntará qué debe hacer con este archivo. En este ejemplo, seleccionaremos **Guardar archivo** y luego haremos clic en **Aceptar**.



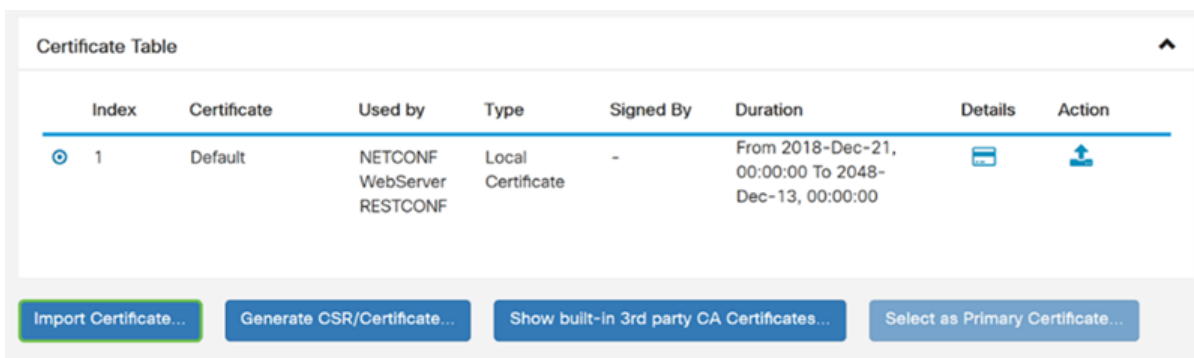
Paso 4. El archivo debe guardarse en la ubicación de almacenamiento predeterminada.

En nuestro ejemplo, el archivo se guardó en nuestra carpeta *Descargas* en nuestro equipo.



Importación de certificado

Paso 1. En la página *Certificado*, haga clic en el botón **Importar certificado....**



Paso 2. Seleccione el **tipo** de certificado que desea importar de la lista desplegable *Tipo* bajo la sección *Importar certificado*. Las opciones se definen de la siguiente manera:

Certificado CA - Certificado certificado certificado por una autoridad de terceros de

confianza que ha confirmado que la información contenida en el certificado es exacta.

· **Certificado de dispositivo local:** χερτιφιαδο γενεραδο εν ελ ρουτερ.

· **PKCS#12 Archivo codificado** - Public Key Cryptography Standards (PKCS) #12 es un certificado exportado que se incluye en una extensión .p12.

En este ejemplo, el **archivo codificado PKCS#12** se seleccionó como tipo. Ingrese un **nombre** para el certificado y luego ingrese la **contraseña** que se usó.

Import Certificate

Type: PKCS#12 Encoded File 1

Certificate Name: CiscoSMB 2

Import Password: ●●●●●●●●●● 3

Upload Certificate file

Import from PC

Import from USB

Browse... No file is selected

Browse... No file is selected

Paso 3. En la sección *Cargar archivo de certificado*, seleccione **Importar desde PC** o **Importar desde USB**. En este ejemplo, se seleccionó **Importar desde PC**. Haga clic en **Examinar...** para elegir un archivo para cargar.

Import Certificate

Type:


Certificate Name:

Import Password:

Upload Certificate file

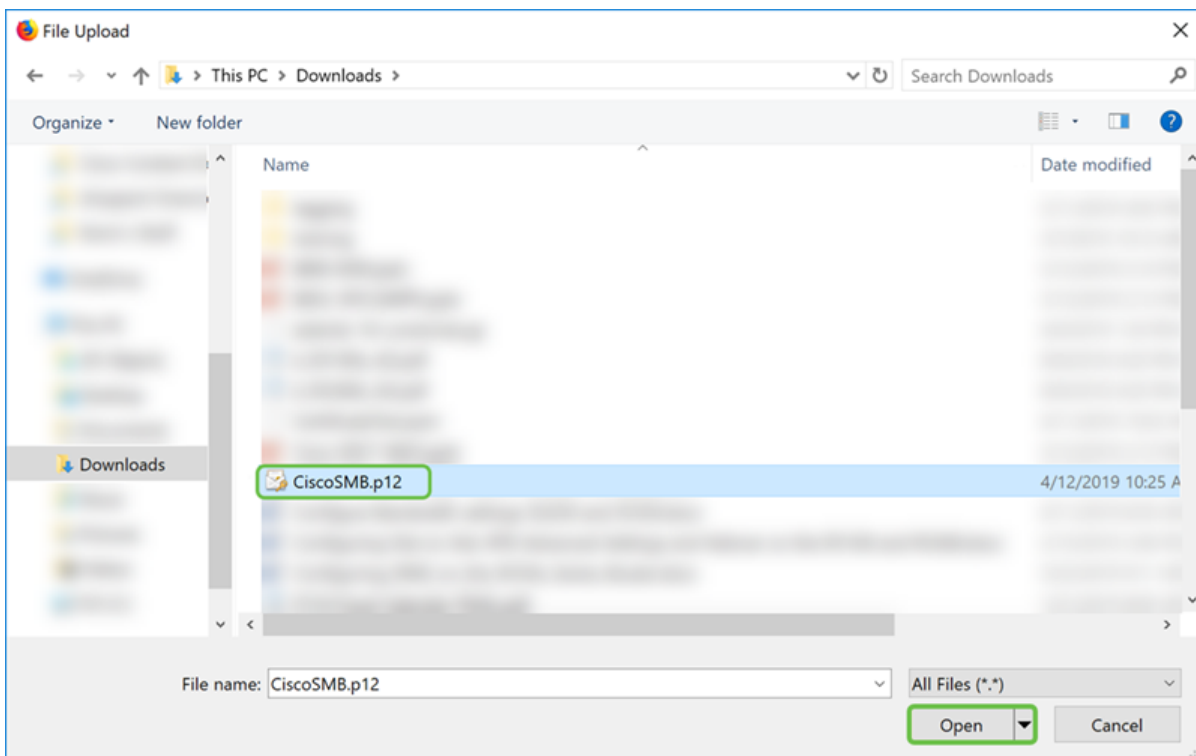
Import from PC

No file is selected

Import from USB 

No file is selected

Paso 4. En la ventana *Carga de archivos*, navegue hasta la ubicación en la que se encuentra el archivo codificado PKCS#12 (extensión de archivo .p12). Seleccione el archivo **.p12** y luego haga clic en **Abrir**.



Paso 5. Haga clic en **Cargar** para comenzar a cargar el certificado.

Certificate

Upload
Cancel

Import Certificate

Type: PKCS#12 Encoded File

Certificate Name: CiscoSMB

Import Password: ●●●●●●●●

Upload Certificate file

Import from PC

Browse... CiscoSMB.p12

Import from USB ↻

Browse... No file is selected

Paso 6. Aparecerá una ventana *Information* que le informará de que el certificado se ha importado correctamente. Para continuar, haga clic en OK (Aceptar).

Information
✕

i
Import certificate successfully!

OK

Paso 7. Debe ver que se ha cargado el certificado.

Certificate Table ^

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CiscoSMB	-	Local Certificate	CiscoTest- DC1-CA	From 2019-Apr-10, 00:00:00 To 2021- Apr-09, 00:00:00		

Conclusión

Debería haber aprendido con éxito cómo generar una CSR, importar y descargar un certificado en los routers de las series RV160 y RV260.