

Certificado (Import/Export/Generate CSR) no RV160 e RV260 Series Router

Objetivo

O objetivo deste documento é mostrar como gerar uma Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request), bem como importar e exportar certificados nos RV160 e RV260 Series Routers.

Introduction

Os certificados digitais são importantes no processo de comunicação. Ele fornece identificação digital para autenticação. Um certificado digital inclui informações que identificam um dispositivo ou usuário, como nome, número de série, empresa, departamento ou endereço IP.

As Autoridades de Certificação (AC) são autoridades de confiança que "assinam" certificados para verificar a sua autenticidade, o que garante a identidade do dispositivo ou utilizador. Garante que o titular do certificado é realmente quem alega ser. Sem um certificado assinado confiável, os dados podem ser criptografados, mas a pessoa com quem você está se comunicando pode não ser a pessoa com quem você pensa. A CA usa PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) ao emitir certificados digitais, que usam a criptografia de chave pública ou privada para garantir a segurança. As ACs são responsáveis por gerenciar solicitações de certificado e emitir certificados digitais. Alguns exemplos de CA são: IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verisign e muito mais.

Os certificados são usados para conexões Secure Socket Layer (SSL), Transport Layer Security (TLS), Datagram TLS (DTLS), como o Hypertext Transfer Protocol (HTTPS) e Secure Lightweight Directory Access Protocol (LDAPS).

Dispositivos aplicáveis

- RV160
- RV260

Versão de software

- 1.0.00.15

Table Of Contents

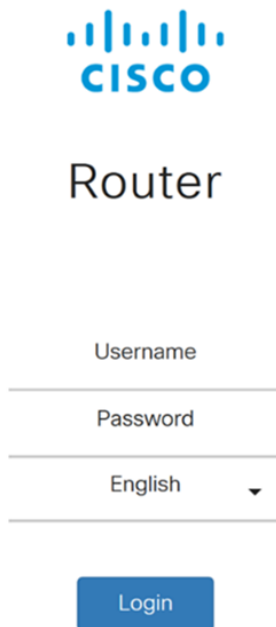
Por meio deste artigo, você:

1. [Gerar CSR/certificado](#)

2. [Exibição do certificado](#)
3. [Exportar certificado](#)
4. [Importar certificado](#)
5. [Conclusão](#)

Gerar CSR/certificado

Etapa 1. Faça login na página de configuração da Web.

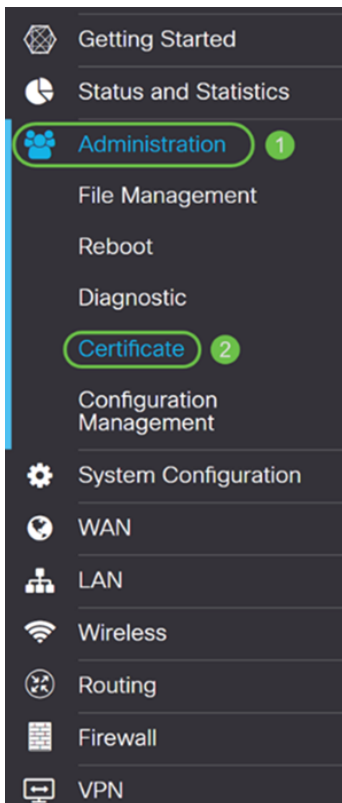


The image shows the Cisco Router login page. At the top is the Cisco logo, which consists of a stylized signal icon above the word "CISCO". Below the logo is the word "Router". Underneath, there are three input fields: "Username", "Password", and a language dropdown menu currently set to "English". At the bottom of the form is a blue "Login" button.

©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.

Etapa 2. Navegue até **Administração > Certificado**.



Etapa 3. Na página *Certificado*, clique no botão **Gerar CSR/Certificado...**

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...

Etapa 4. Selecione o tipo de certificado a gerar a partir de uma das seguintes opções na lista suspensa.

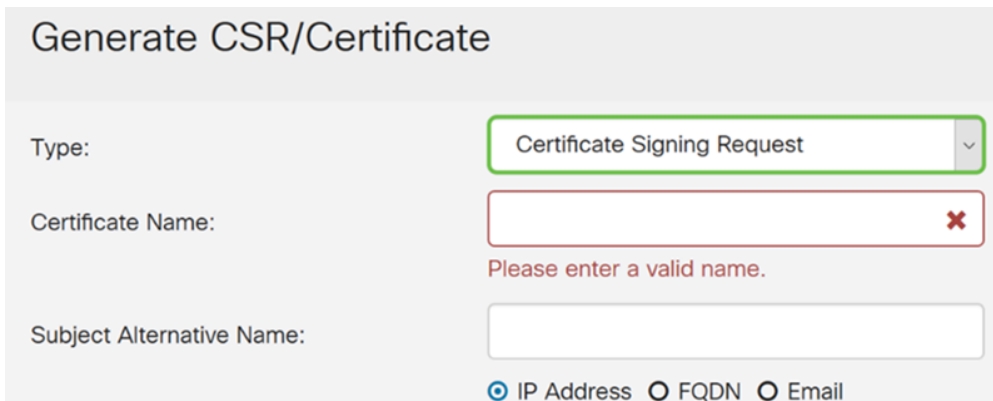
Certificado autoassinado - Este é um certificado SSL (Secure Socket Layer) assinado por seu próprio criador. Este certificado é menos confiável, pois não pode ser cancelado se a chave privada for comprometida de alguma forma por um invasor. Você deve fornecer a duração válida em dias.

• **Certificado CA** - Selecione este tipo de certificado para que o roteador funcione como uma autoridade de certificado interna e emita certificados. Em um ponto de vista de segurança, é semelhante a um certificado autoassinado. Isso pode ser usado para OpenVPN.

Solicitação de assinatura de certificado - Esta é uma infraestrutura de chave pública (PKI) que é enviada à autoridade de certificação para solicitar um certificado de identidade digital. É mais segura do que autoassinada, já que a chave privada é mantida em segredo. Essa opção é recomendada.

• **Certificado assinado por certificado CA** - Selecione este tipo de certificado e forneça detalhes relevantes para obter o certificado assinado pela sua autoridade de certificação interna.

Neste exemplo, selecionaremos **Solicitação de assinatura de certificado**.



Generate CSR/Certificate

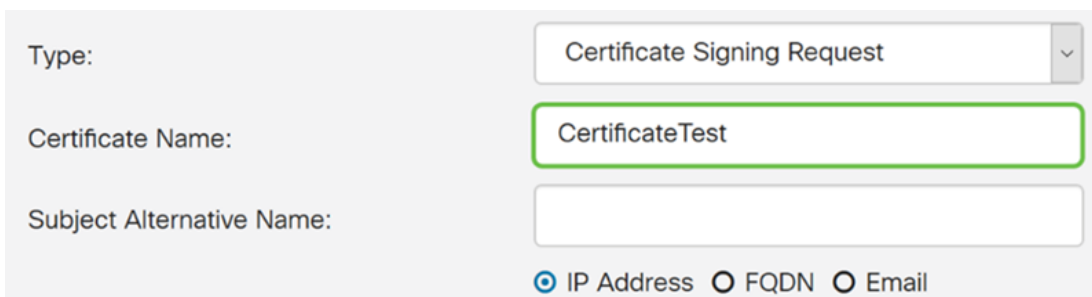
Type: Certificate Signing Request

Certificate Name: ✘
Please enter a valid name.

Subject Alternative Name:

IP Address FQDN Email

Etapa 5. Digite o *nome do certificado*. Neste exemplo, vamos inserir **CertificateTest**.



Type: Certificate Signing Request

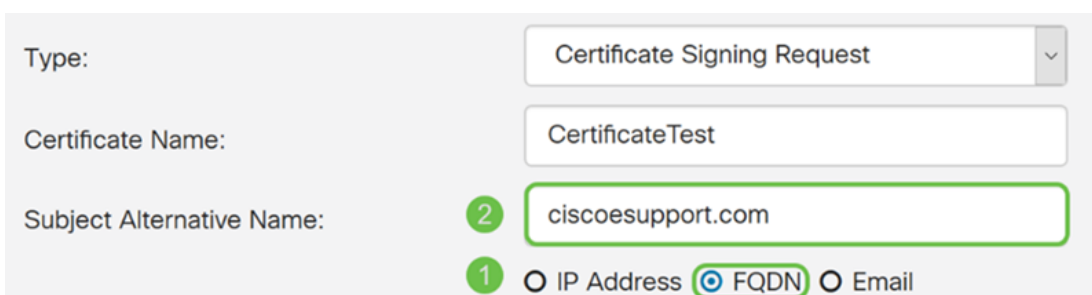
Certificate Name: CertificateTest

Subject Alternative Name:

IP Address FQDN Email

Etapa 6. No campo *Nome alternativo do assunto*, selecione uma das seguintes opções: **Endereço IP**, **FQDN** (Nome de domínio totalmente qualificado) ou **Email** e insira o nome apropriado do que você selecionou. Esse campo permite especificar nomes de host adicionais.

Neste exemplo, selecionaremos o **FQDN** e inseriremos **ciscoesupport.com**.



Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name: ciscoesupport.com

IP Address FQDN Email

Passo 7. Selecione um **país** na lista suspensa *Nome do 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"/>

Etapa 8. Insira um **nome de estado** ou **província** no campo *Estado ou Nome da Província*.

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"/>

Etapa 9. No *Locality Name*, digite um nome **da cidade**.

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"/>

Etapa 10. Digite o nome da **organização** no campo *Nome da organização*.

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"/>

Etapa 11. Digite o nome da **unidade organizacional** (por exemplo, Treinamento, Suporte, etc.).

Neste exemplo, vamos inserir o **eSupport** como o nome da unidade da nossa organização.

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

Etapa 12. Introduza um **nome comum**. É o FQDN do servidor Web que receberá esse certificado.

Neste exemplo, **ciscosmbsupport.com** foi usado como o nome comum.

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

Etapa 13. Introduza um **endereço de correio eletrônico**.

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

Etapa 14. Selecione **Key Encryption Length** no menu suspenso. As opções são: **512, 1024, ou 2048**. Quanto maior o tamanho da chave, mais seguro o certificado. Quanto maior o tamanho da chave, maior o tempo de processamento.

Prática recomendada: É recomendável escolher o comprimento de criptografia de chave mais alto, permitindo criptografia mais dura.

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

Etapa 15. Clique em **Gerar**.

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:

Etapa 16. Um pop-up *Information* aparecerá com um "Generate certificate successfully!" mensagem. Clique em OK para continuar.

Information ✕

Generate certificate successfully!

OK

Etapa 17. Exporte o CSR da *tabela 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...

Etapa 18. Uma janela *Exportar certificado* é exibida. Selecione **PC** para *Exportar para* e clique em **Exportar**.

Export Certificate



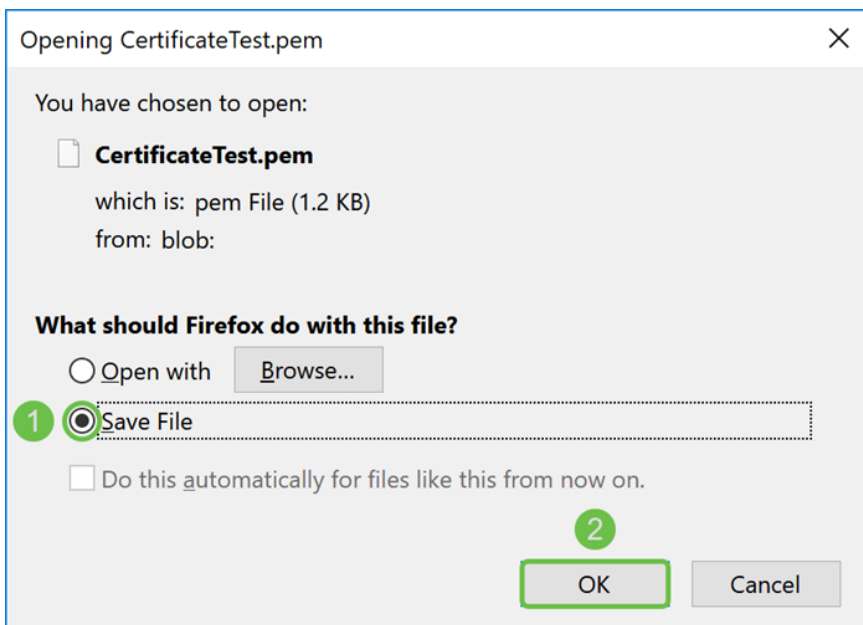
Export as PEM format

Export to:



Etapa 19. Outra janela deve ser exibida perguntando se o arquivo deve ser aberto ou salvo.

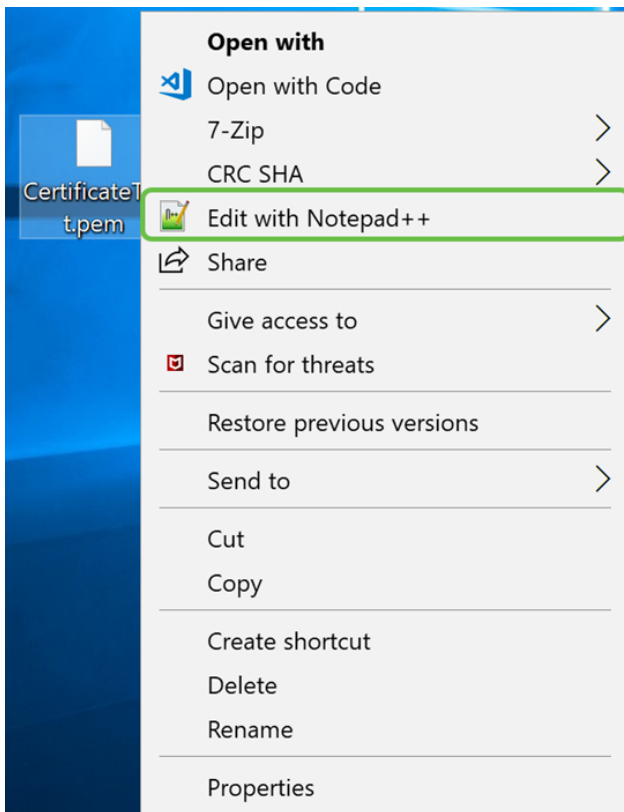
Neste exemplo, selecionaremos **Salvar arquivo** e clicaremos em **OK**.



Etapa 20. Localize o local onde o arquivo .pem foi salvo. **Clique com o botão direito** no arquivo .pem e abra-o com seu editor de texto favorito.

Neste exemplo, abriremos o arquivo .pem com o Notepad++.

Note: Fique à vontade para abri-lo com o Notepad.



Etapa 21. Certifique-se de que a **—BEGIN CERTIFICATE REQUEST—** e **—END CERTIFICATE REQUEST—** esteja em sua própria linha.



Note: Algumas partes do certificado estavam desfocadas.

```
CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 [blurred] VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwWIU2FuIEpvc2UxZjAMBgNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY21zY29zbWJzdXBwb3J0 [blurred]
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXp1u
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LAFoLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv [blurred]
9 soTqNBrYqR8h46NHh0J5fMXDsPY1j2LWmS1VbkskoiMdr5SZlwmhkrqgLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAaCBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BAIw [blurred].gXg
13 MCcGA1UdJQogMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY21zY29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAIL1UeIUy
15 TqFZ2wQx3r29E1SWOU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16
17
18
19
20
21 -----END CERTIFICATE REQUEST----- 2
22
```

Etapa 22. Quando você tiver seu CSR, precisaria ir para seus serviços de hospedagem ou para um site da autoridade de certificação (por exemplo, GoDaddy, Verisign etc.) e solicitar um certificado. Depois de enviar uma solicitação, ele se comunicará com o servidor de certificados para garantir que não haja motivo para não emitir o certificado.







Note: Entre em contato com o CA ou com o suporte do site de hospedagem se não souber onde está a solicitação de certificado no site.

Etapa 23. Baixe o certificado quando ele estiver concluído. Deve ser um arquivo **.cer** ou **.crt**. Neste exemplo, recebemos ambos os arquivos.

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

Etapa 24. Volte para a página *Certificado* no roteador e importe o arquivo de certificado clicando na **seta apontando para o ícone do 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	-	-		  

Etapa 25. No campo *Nome do certificado*, digite o **nome do certificado**. Não pode ser o mesmo nome que a solicitação de assinatura de certificado. Na seção *Carregar arquivo de certificado*, selecione **importar do PC** e clique em **Procurar...** para carregar seu arquivo de certificado.

Import Signed-Certificate

Type: Local Certificate

Certificate Name: 1

Upload Certificate file

2

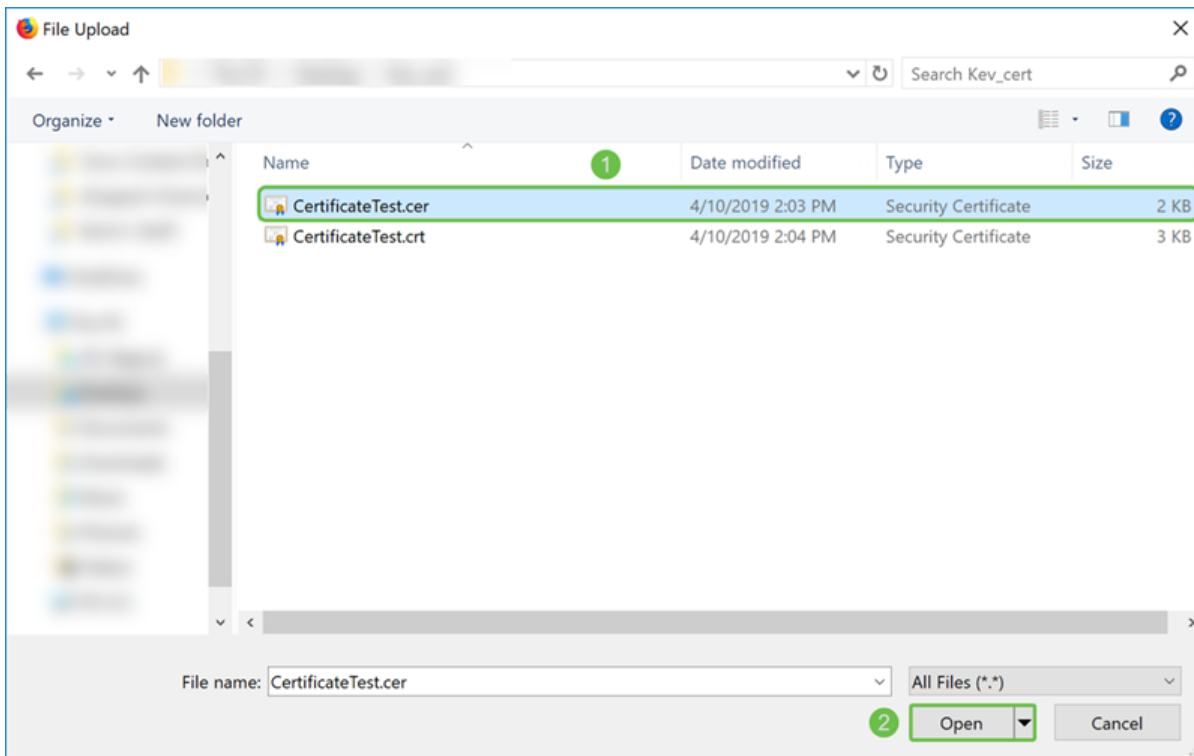
Import from PC

3 No file is selected

Import from USB 

No file is selected

Etapa 26. Uma janela *File Upload* é exibida. Navegue até o local de onde seu arquivo de certificado está. Selecione o arquivo de **certificado** que deseja carregar e clique em **Abrir**. Neste exemplo, **CertificateTest.cer** foi selecionado.



Etapa 27. Clique no botão **Upload** para começar a carregar seu certificado no roteador.

Note: Se você receber um erro no qual não pode carregar seu arquivo .cer, pode ser porque seu roteador exige que o certificado esteja em uma codificação pem. Você precisaria converter sua codificação de der (extensão de arquivo .cer) em uma codificação de pem (extensão de arquivo .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






Etapa 28. Se a importação tiver sido bem-sucedida, uma janela *de informações* será exibida informando que foi bem-sucedida. Clique em OK para continuar.

 Import certificate successfully!

OK

Etapa 29. O certificado deve ser atualizado com êxito. Você deve poder ver por quem seu certificado foi assinado. Neste exemplo, podemos ver que nosso certificado foi assinado pela *CiscoTest-DC1-CA*. Para tornar o certificado nosso certificado principal, selecione o certificado usando o botão de opção no lado esquerdo e clique no botão **Selecionar como certificado primário**....

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...**

Note: A alteração do certificado principal pode levá-lo de volta a uma página de aviso. Se estiver usando o Firefox e ele aparecer como uma página em branco cinza, você precisará ajustar alguma configuração no Firefox. Este documento no site Mozilla wiki dá algumas explicações sobre isso: [CA/AddRootToFirefox](#). Para poder ver a página de aviso novamente, [siga estas etapas encontradas na página de suporte da comunidade Mozilla](#).

Etapa 30. Na página de aviso do Firefox, clique em **Avançado...** e em **Aceitar o Risco e Continuar** para retornar ao roteador.

Note: Essas telas de avisos variam de navegador para navegador, mas executam as mesmas funções.



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

Etapa 31. Na Tabela de Certificados, você deve ver que o NETCONF, o *WebServer* e o *RESTCONF* foram trocados para o novo certificado em vez de usar o *Default*.

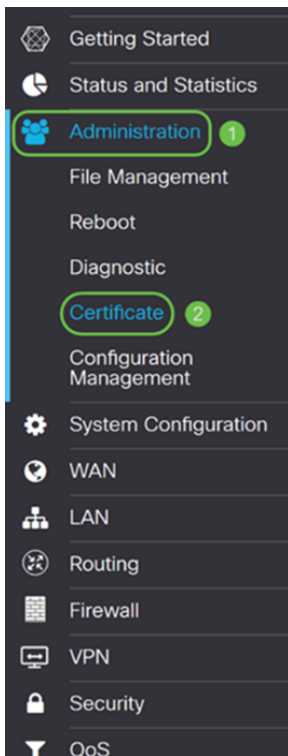
Certificate Table

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		

Agora você deve ter instalado com êxito um certificado no roteador.






Exibição do certificado

Etapa 1. Se você tiver saído da página *Certificado*, navegue para **Administração > Certificado**.



Etapa 2. Na *Tabela de certificados*, clique no ícone **Detalhes** localizado na seção *Detalhes*.

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		 

Etapa 3. A página *Detalhes do certificado* é exibida. Você deve poder ver todas as informações sobre seu 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

Etapa 4. Clique no ícone de bloqueio localizado no lado esquerdo da barra Uniform Resource Locator (URL).

Note: As etapas a seguir são usadas em um navegador Firefox.

Cisco RV160 VPN Router

https://192.168.2.1/#/certificate

RV160--router5680AA

cisco(admin) English

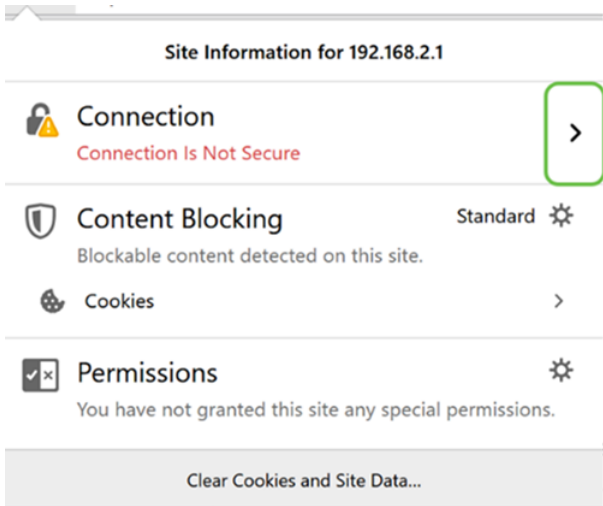
Certificate

Certificate Table

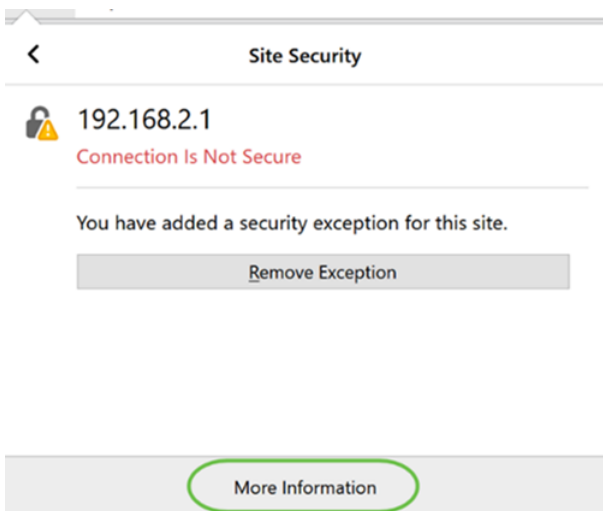
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

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

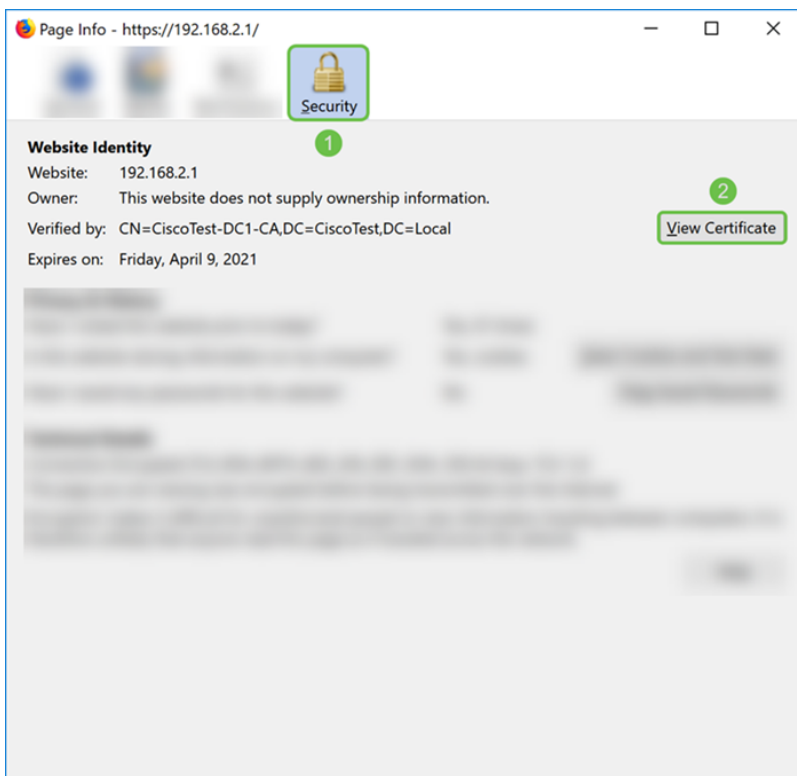
Etapa 5. Uma lista suspensa de opções é exibida. Clique no ícone **Seta** ao lado do campo **Conexão**.



Etapa 6. Clique em **Mais informações**.

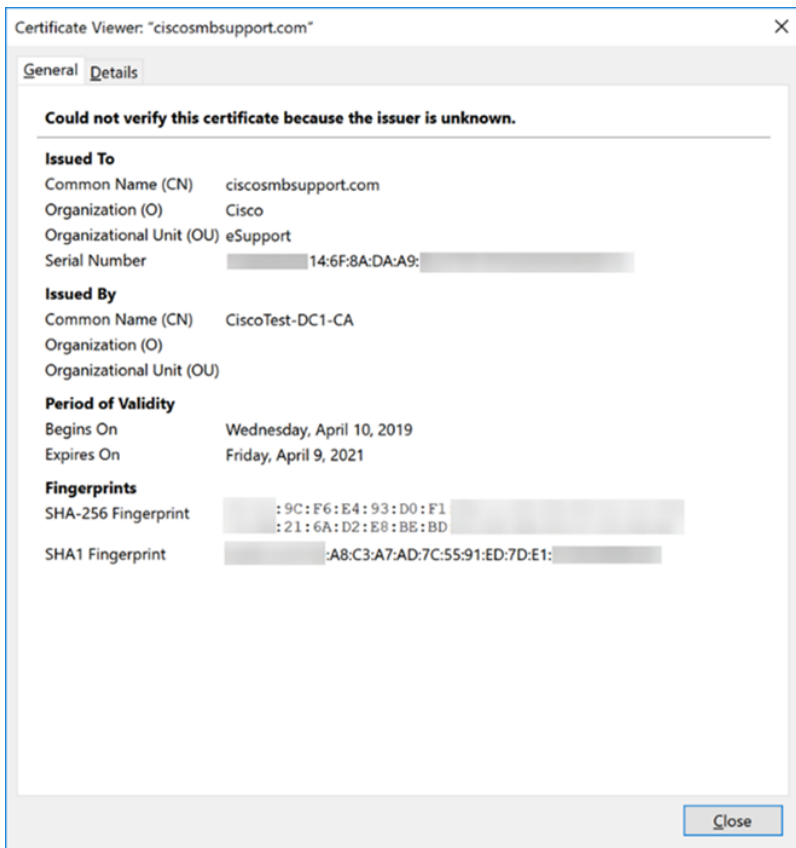


Passo 7. Na janela *Informações da página*, você poderá ver uma breve informação sobre seu certificado na seção *Identidade do site*. Certifique-se de estar na guia **Segurança** e, em seguida, clique em **Ver certificado** para ver mais informações sobre o certificado.



Etapa 8. A página *Certificate Viewer* deve ser exibida. Você deve poder ver todas as informações sobre seu certificado, período de validade, impressões digitais e por quem ele foi emitido.

Note: Como este certificado foi emitido pelo nosso servidor de certificados de teste, o emissor é desconhecido.



Exportando certificado

Para baixar seu certificado para importá-lo em outro roteador, siga as etapas abaixo.

Etapa 1. Na página *Certificado*, clique no ícone **exportar** ao lado do certificado que você deseja 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		

Etapa 2. Um *Certificado de exportação* é exibido. Selecione um formato para exportar o certificado. As opções são:

- **PKCS#12** - Public Key Cryptography Standards (PKCS) #12 é um certificado exportado que vem em uma extensão .p12. Será necessária uma senha para criptografar o arquivo

para protegê-lo à medida que for exportado, importado e excluído.

• **PEM** - O Privacy Enhanced Mail (PEM) é frequentemente usado para servidores Web para que eles possam ser facilmente traduzidos em dados legíveis usando um editor de texto simples, como o notepad.

Selecione **Exportar como formato PKCS#12** e insira uma **senha** e **confirme a senha**. Em seguida, selecione **PC** como *Exportar para:* campo. Clique em **Exportar** para iniciar a exportação do certificado para o computador.

Note: Lembre-se desta senha porque você a usará ao importá-la para um roteador.

Export Certificate



1

Export as PKCS#12 format

Enter Password:

2

Confirm Password:

Export as PEM format

Export to:

3

PC USB

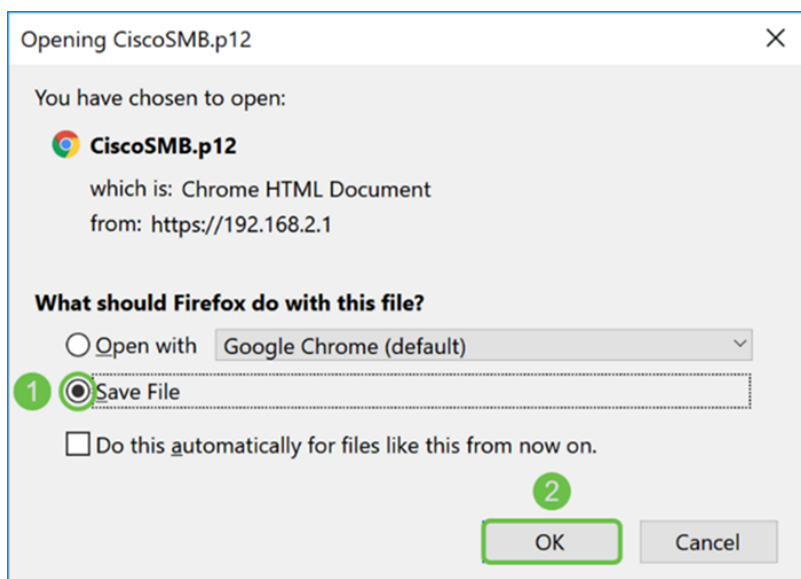


4

Export

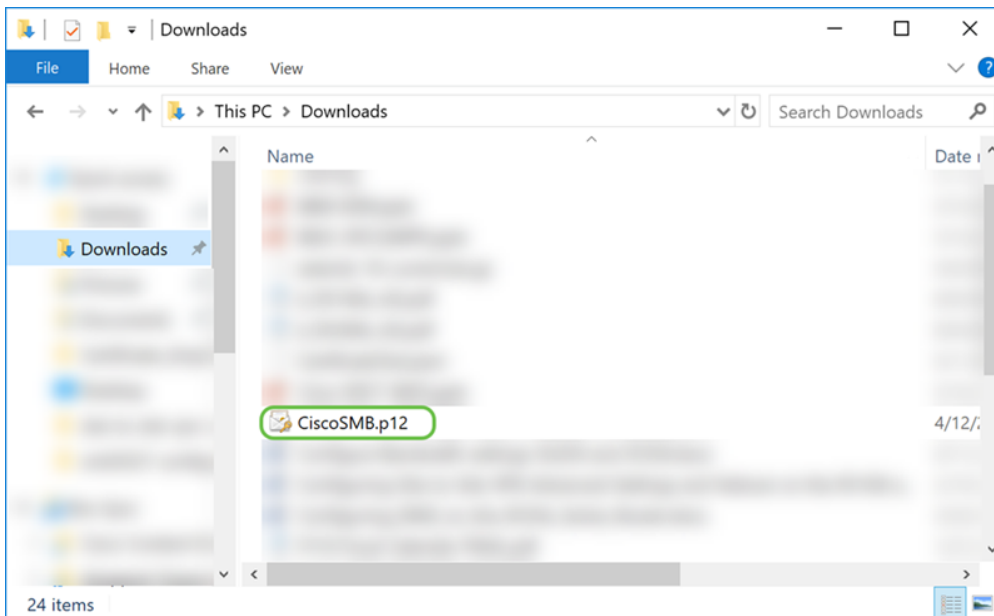
Cancel

Etapa 3. Será exibida uma janela perguntando o que você deve fazer com este arquivo. Neste exemplo, selecionaremos **Salvar arquivo** e clicaremos em **OK**.



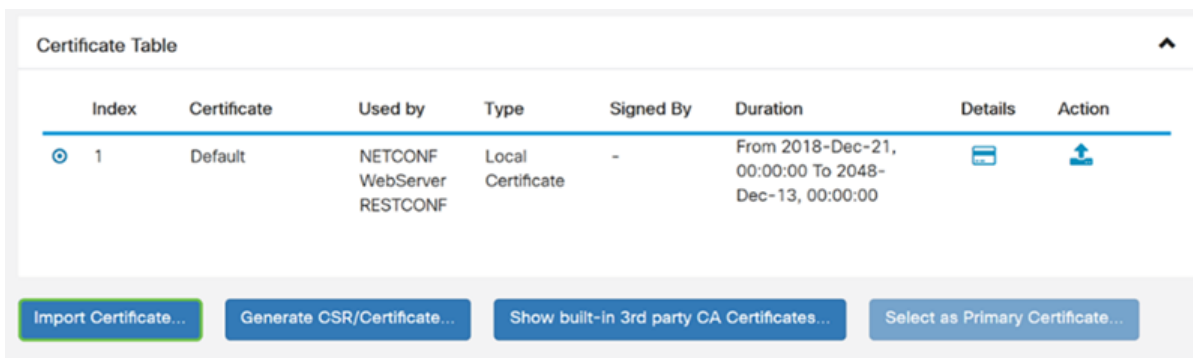
Etapa 4. O arquivo deve ser salvo no local de gravação padrão.

Em nosso exemplo, o arquivo foi salvo na pasta *Downloads* em nosso computador.



Importando certificado

Etapa 1. Na página *Certificado*, clique no botão **Importar certificado....**



Etapa 2. Selecione o **tipo** de certificado a importar da lista suspensa *Tipo* na seção *Importar certificado*. As opções são definidas como:

Certificado • CA - Um certificado certificado certificado por uma autoridade de terceiros confiável que confirmou a exatidão das informações contidas no certificado.

• **Certificado de Dispositivo Local** - Um certificado gerado no roteador.

• **Arquivo Codificado PKCS#12** - PKCS (Public Key Cryptography Standards) #12 é um certificado exportado que vem em uma extensão .p12.

Neste exemplo, **PKCS#12 Encoded File** foi selecionado como o tipo. Introduza um **nome** para o certificado e introduza a **senha** que foi utilizada.

Import Certificate

Type: 1


Certificate Name: 2

Import Password: 3

Upload Certificate file

Import from PC

No file is selected

Import from USB 

No file is selected

Etapa 3. Na seção *Carregar arquivo de certificado*, selecione **Importar do PC** ou **Importar do USB**. Neste exemplo, **Importar do PC** foi selecionado. Clique em **Procurar...** para escolher um arquivo para carregar.

Import Certificate

Type:


Certificate Name:

Import Password:

Upload Certificate file

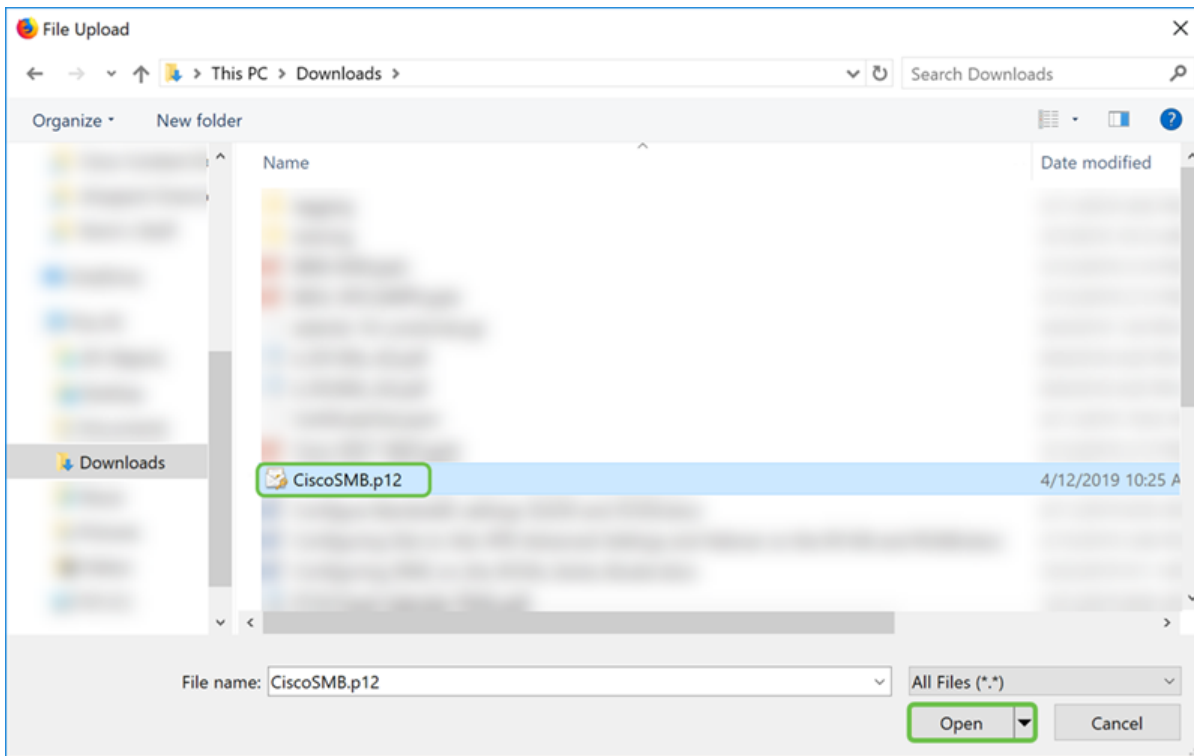
Import from PC

No file is selected

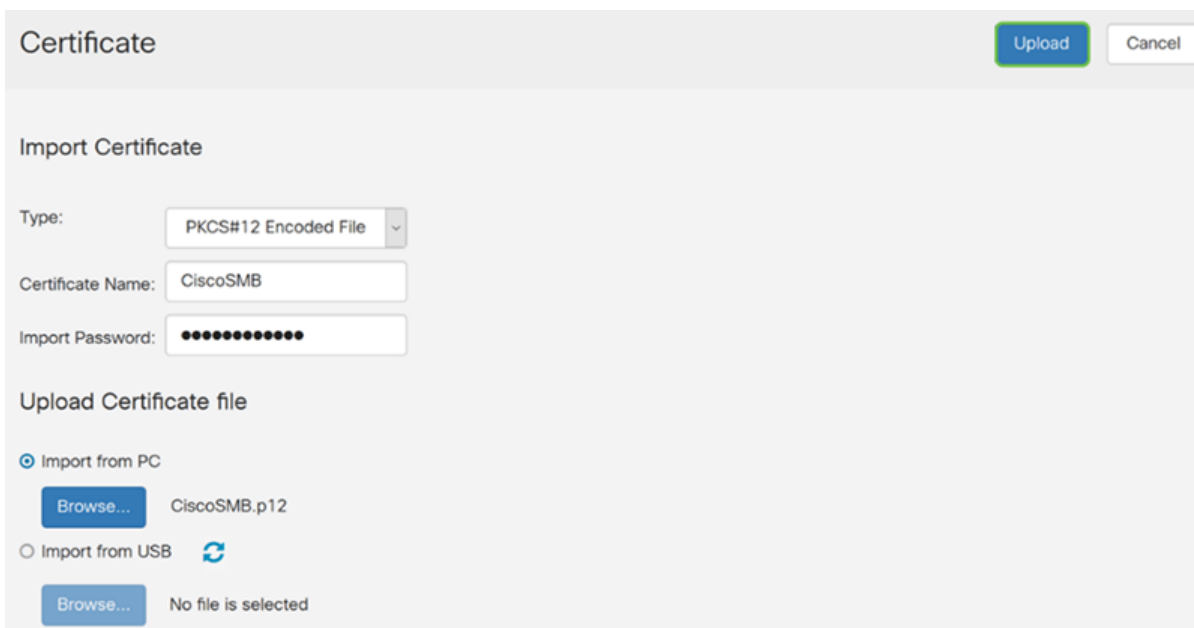
Import from USB 

No file is selected

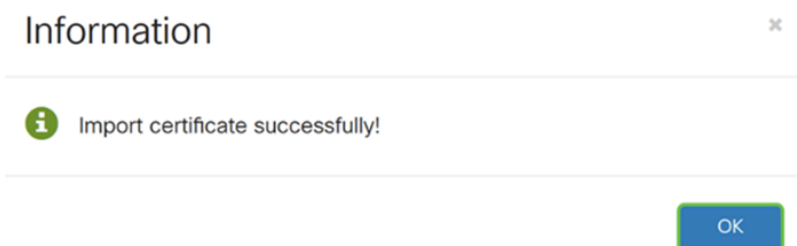
Etapa 4. Na janela *File Upload*, navegue até o local onde o arquivo codificado PKCS#12 (extensão de arquivo .p12) está localizado. Selecione o arquivo **.p12** e clique em **Abrir**.



Etapa 5. Clique em **Carregar** para iniciar o carregamento do certificado.





Etapa 6. Uma janela *Informações* será exibida informando que seu certificado foi importado com êxito. Clique em OK para continuar.



Passo 7. Você deve ver que seu certificado foi carregado.

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		 

Conclusão

Você deve ter aprendido com êxito como gerar um CSR, importar e baixar um certificado no RV160 e no RV260 Series Router.