RV160和RV260系列路由器上的证书（导入/导出/生成CSR）

目标

本文档旨在向您展示如何生成证书签名请求(CSR)，以及如何在RV160和RV260系列路由器上导入和导出证书。

简介

数字证书在通信过程中非常重要。它提供数字身份验证。数字证书包括标识设备或用户的信息，如名称、序列号、公司、部门或IP地址。

证书颁发机构(CA)是“签署”证书以验证其真实性的受信任颁发机构，可保证设备或用户的身份。它确保证书持有者是他们真正声称的拥有者。如果没有受信任的签名证书，数据可能会被加密，但您与之通信的一方可能不是您认为的一方。CA在颁发数字证书时使用公钥基础设施(PKI)，数字证书使用公钥或私钥加密来确保安全。CA负责管理证书请求和颁发数字证书。CA的一些示例包括：IdenTrust、Comodo、GoDaddy、GlobalSign、GeoTrust、Verisign等。

证书用于安全套接字层(SSL)、传输层安全(TLS)、数据报TLS(DTLS)连接，例如超文本传输协议(HTTPS)和安全轻量级目录访问协议(LDAPS)。

适用设备

- RV160
- RV260

软件版本

- 1.0.00.15

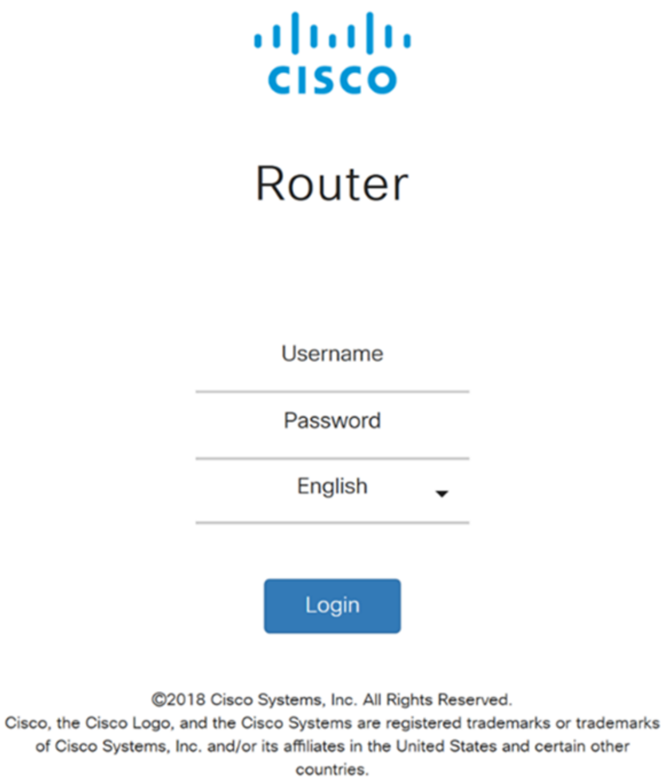
目录

通过本文，您将：

1. 生成CSR/证书
2. 查看证书
3. 导出证书
4. 导入证书
5. 结论

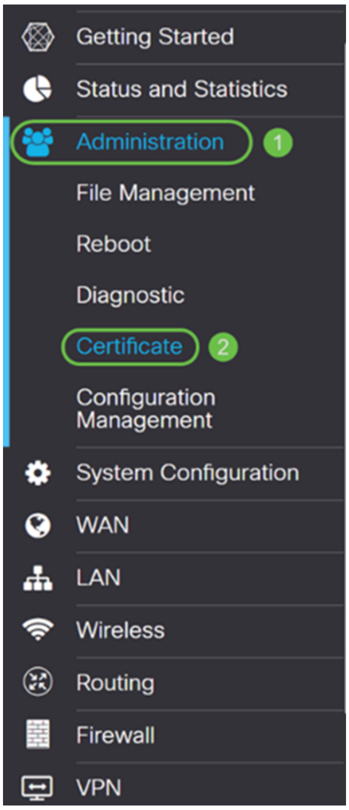
生成CSR/证书

步骤1.登录Web配置页面。

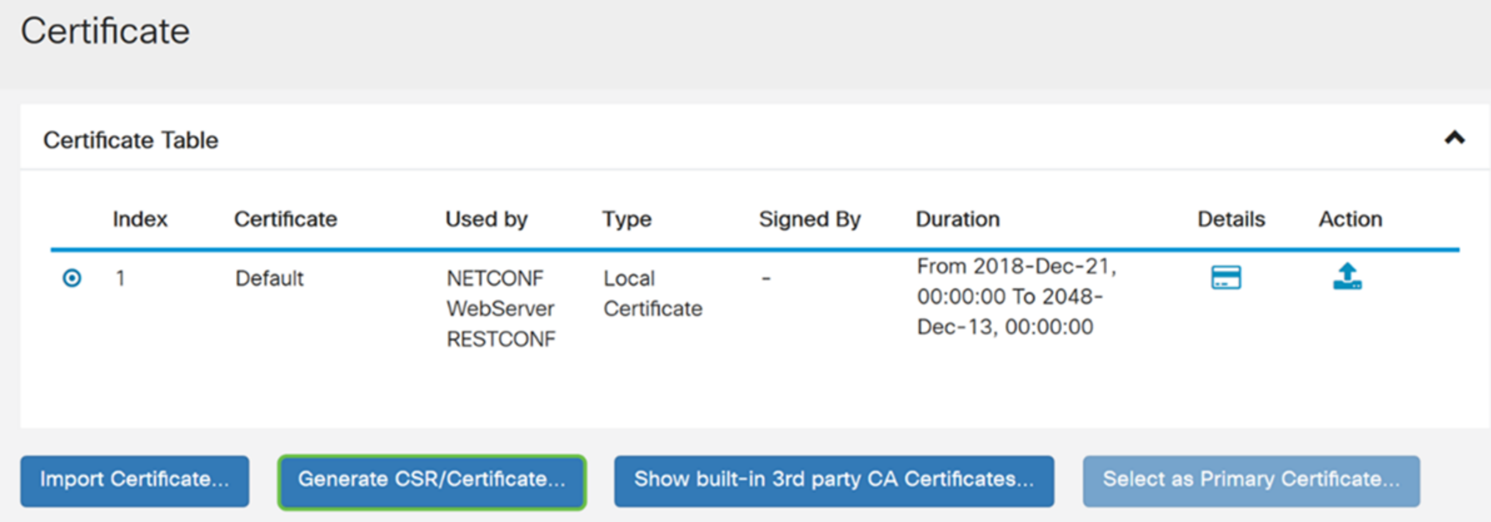


©2018 Cisco Systems, Inc. All Rights Reserved.
Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

步骤2.导航至**Administration > Certificate**。



步骤3.在“证书”页面中，单击**“生成CSR/证书......”**按钮。



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...

步骤4.从下拉列表中的以下选项之一选择要生成的证书类型。

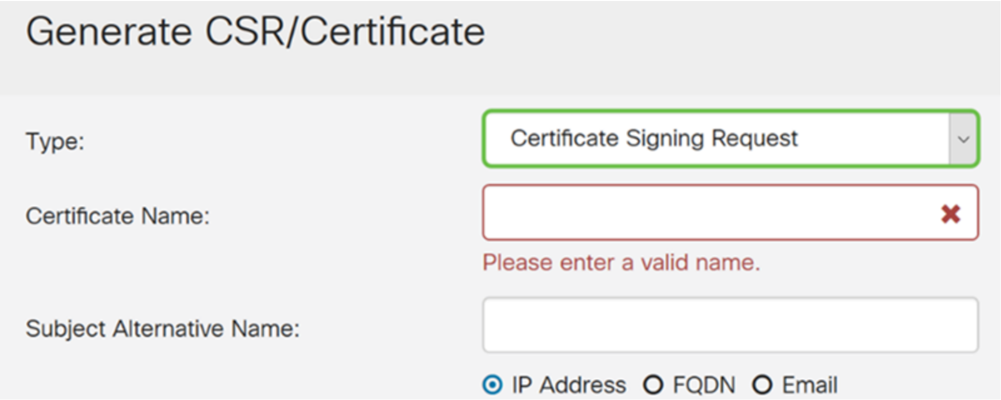
• **自签名证书** — 这是安全套接字层(SSL)证书，由其自己的创建者签名。此证书不太可信，因为如果私钥被攻击者以某种方式入侵，则无法取消该证书。您必须提供有效持续时间（以天为单位）。

·**CA Certificate** 在安全方面，它类似于自签名证书。这可用于OpenVPN。

·**证书签名请求** (ΠKI)它比自签名更安全，因为私钥是保密的。建议使用此选项。

• **Certificate Signed by CA Certificate** — 选择此证书类型并提供相关详细信息，以获取由内部证书颁发机构签名的证书。

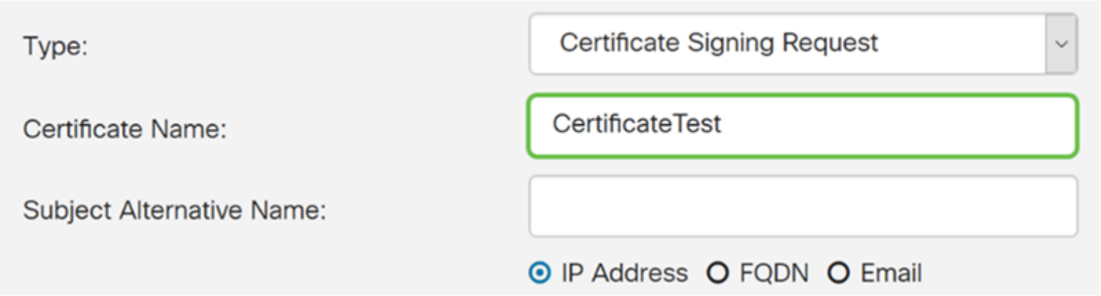
在本例中，我们将选择“证书签**名请求”**。



Generate CSR/Certificate

Type:	Certificate Signing Request
Certificate Name:	✖ Please enter a valid name.
Subject Alternative Name:	 ● IP Address ○ FQDN ○ Email

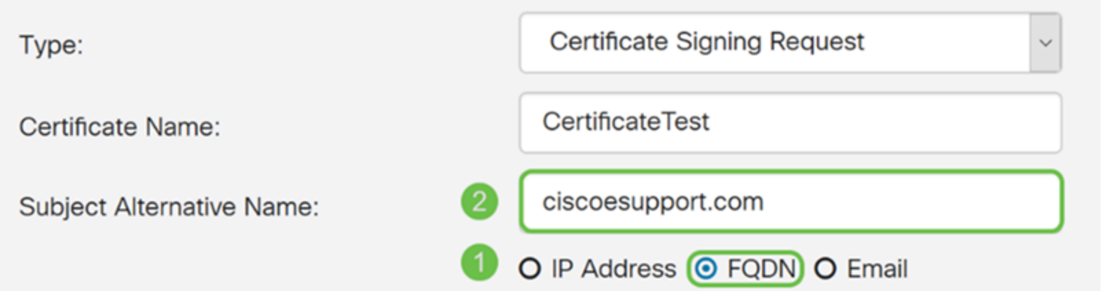
步骤5.输入证*书名称*。在本例中，我们将输入**CertificateTest**。



Type:	Certificate Signing Request
Certificate Name:	CertificateTest
Subject Alternative Name:	 ● IP Address ○ FQDN ○ Email

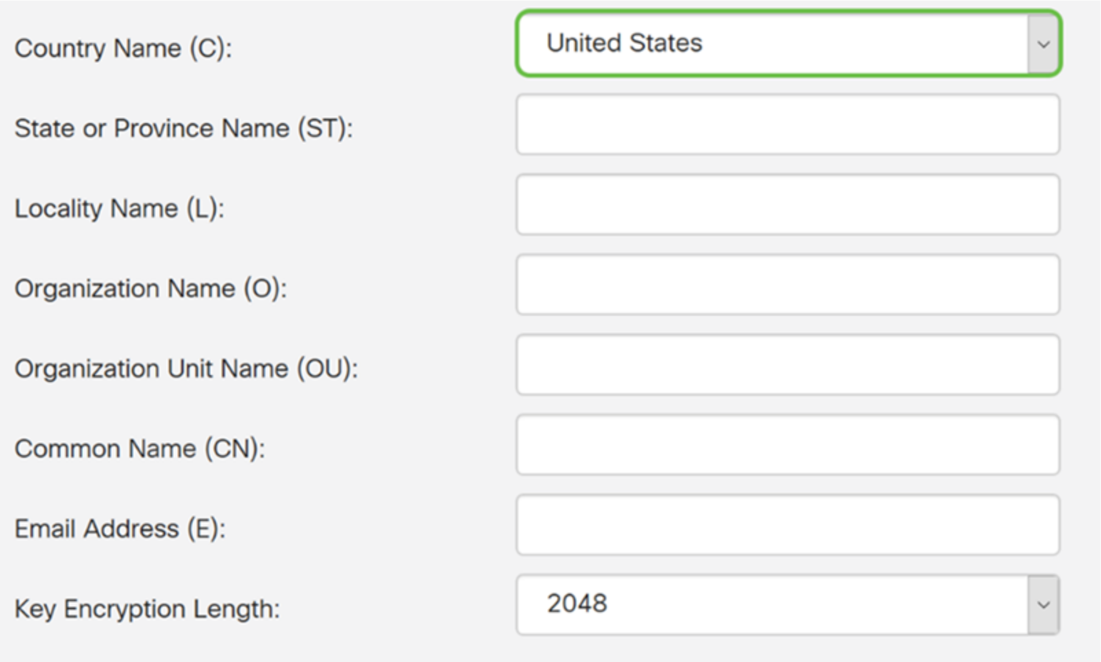
步骤6.在“主*题替代名称*”字段中，选择以下选项之一：**IP Address、FQDN（完全限定域名）或Email，然后输入您选择的相应名称。**此字段允许您指定其他主机名。

在本示例中，我们将选择**FQDN并**输入**ciscoesupport.com**。



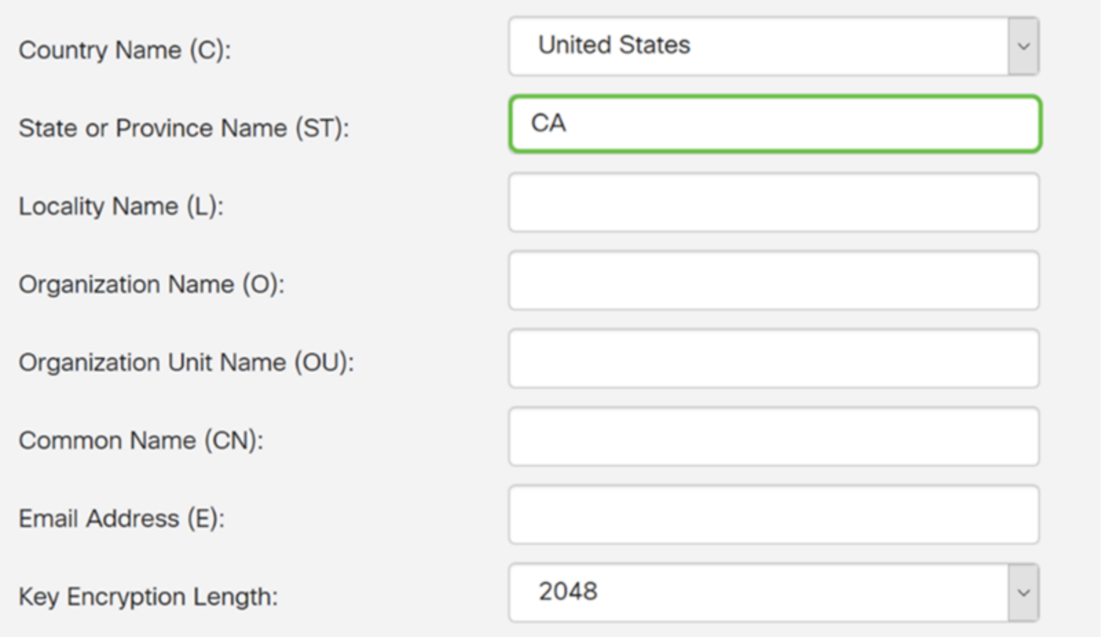
Type:	Certificate Signing Request
Certificate Name:	CertificateTest
Subject Alternative Name:	ciscoesupport.com
	○ IP Address ● FQDN ○ Email

步骤7.从Country Name**(C)**下*拉列表中选择*国家/地区。



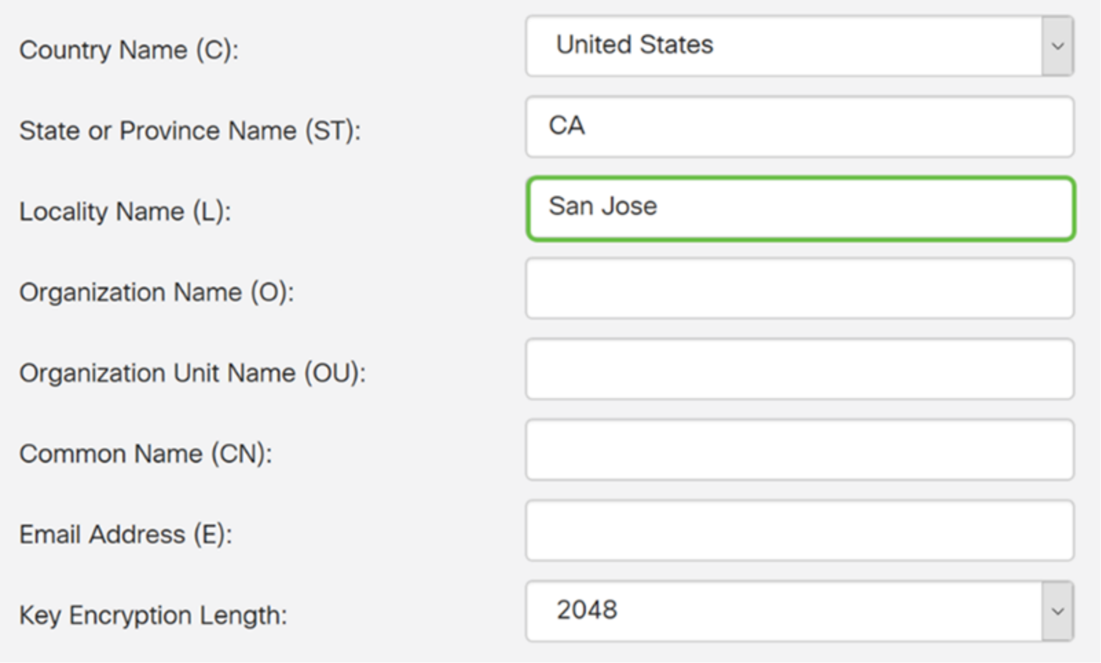
Country Name (C):	United States
State or Province Name (ST):	
Locality Name (L):	
Organization Name (O):	
Organization Unit Name (OU):	
Common Name (CN):	
Email Address (E):	
Key Encryption Length:	2048

步骤8.在“省**名”**或“**省名**”字*段中输入省名*称。



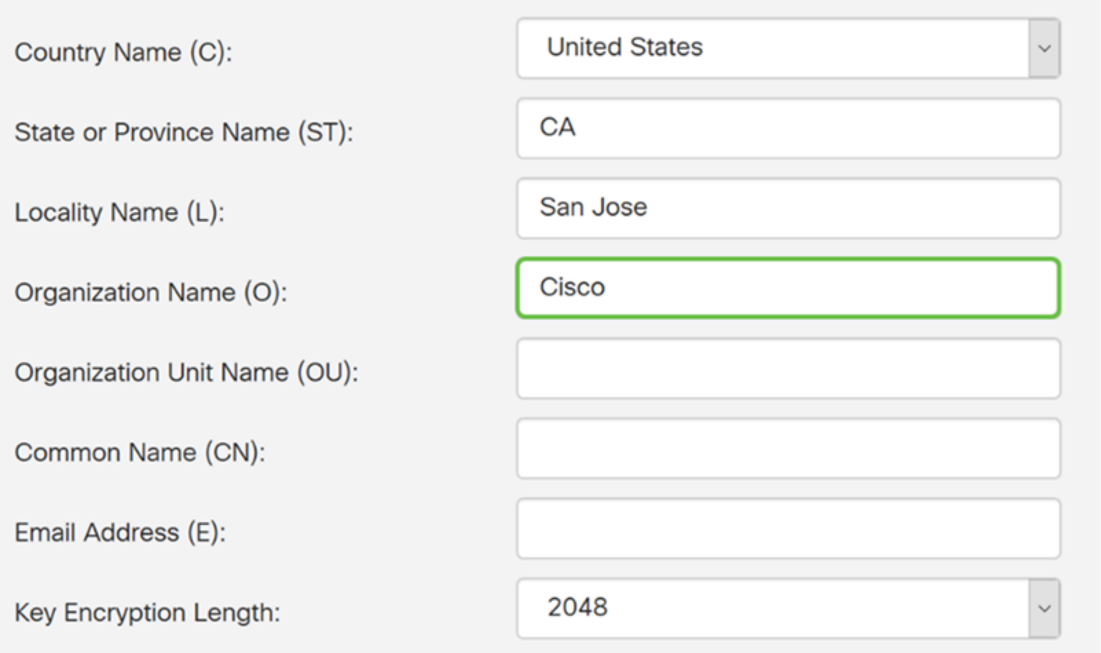
Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	
Organization Name (O):	
Organization Unit Name (OU):	
Common Name (CN):	
Email Address (E):	
Key Encryption Length:	2048

步骤9.在Locality Name*中*，输入**城市**名称。



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

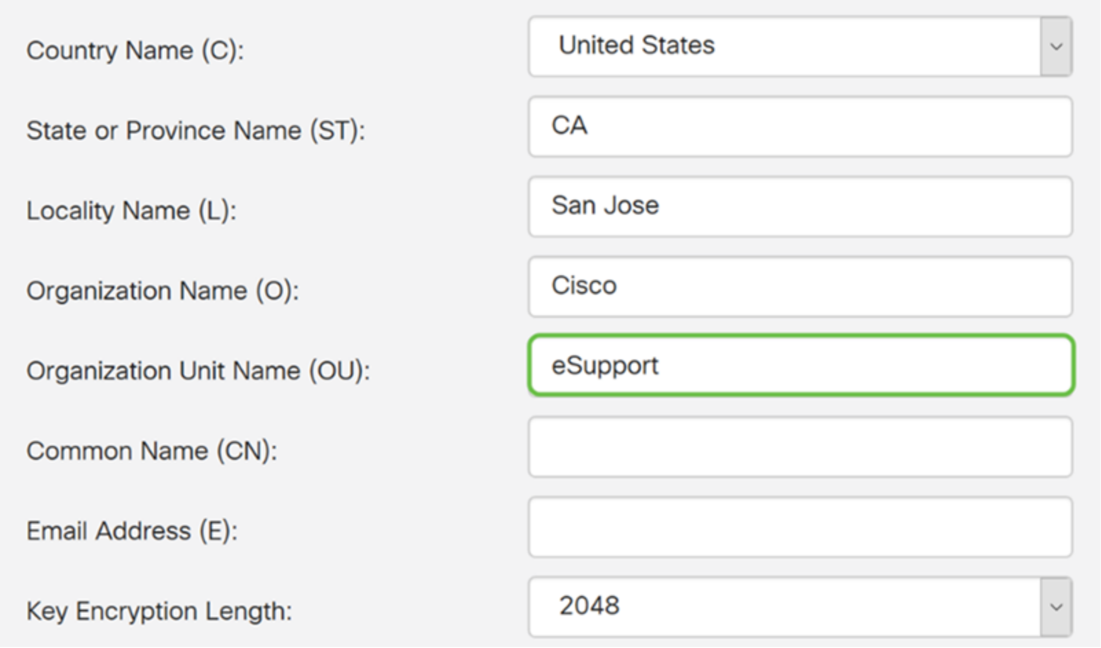
步骤10.在“组织名称”字**段中**输入组*织的*名称。



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

步骤11.输入组织单**位的**名称（如培训、支持等）。

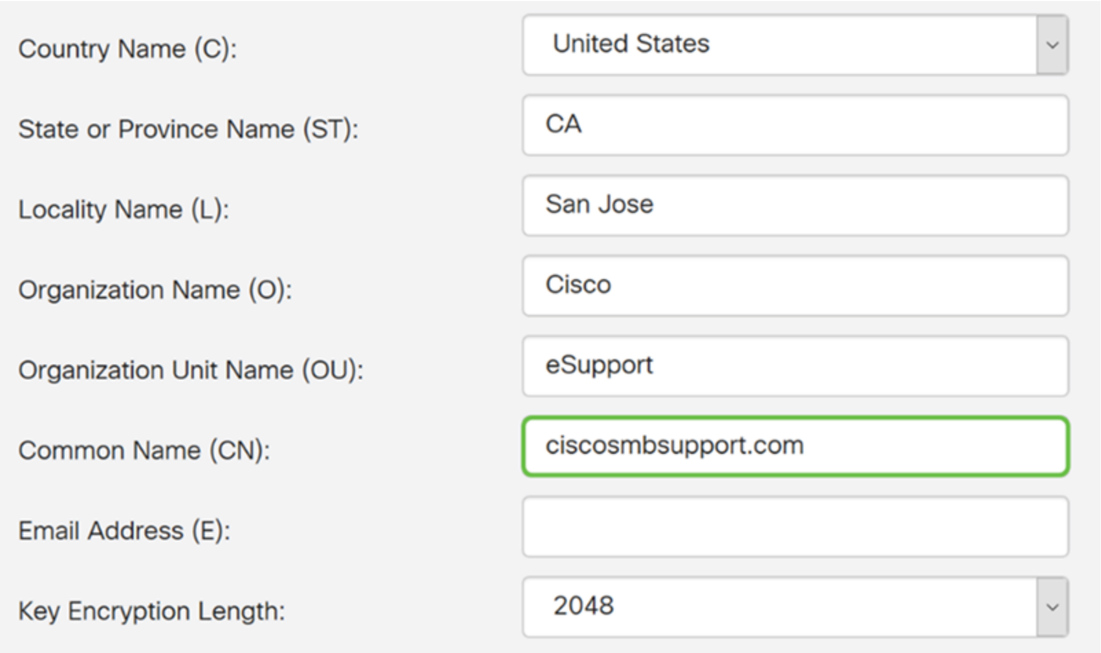
在本例中，我们将输入**eSupport**作为组织单位名称。



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

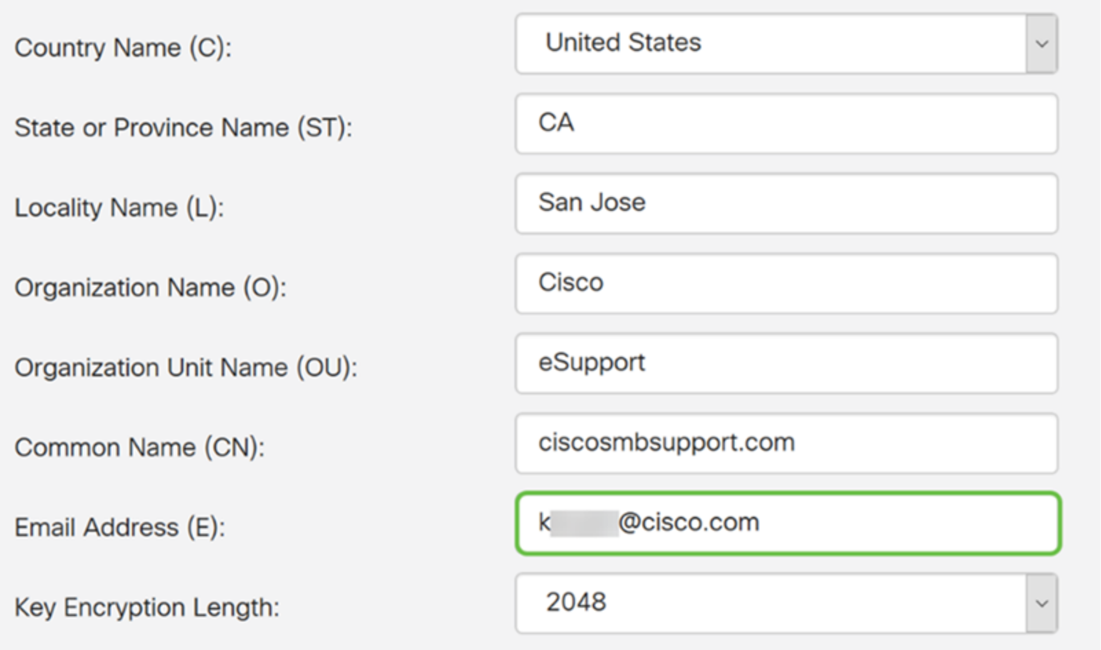
步骤12.输入公**用名**。接收此证书的是Web服务器的FQDN。

在本示例中，**ciscosmbsupport.com**用作通用名称。



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

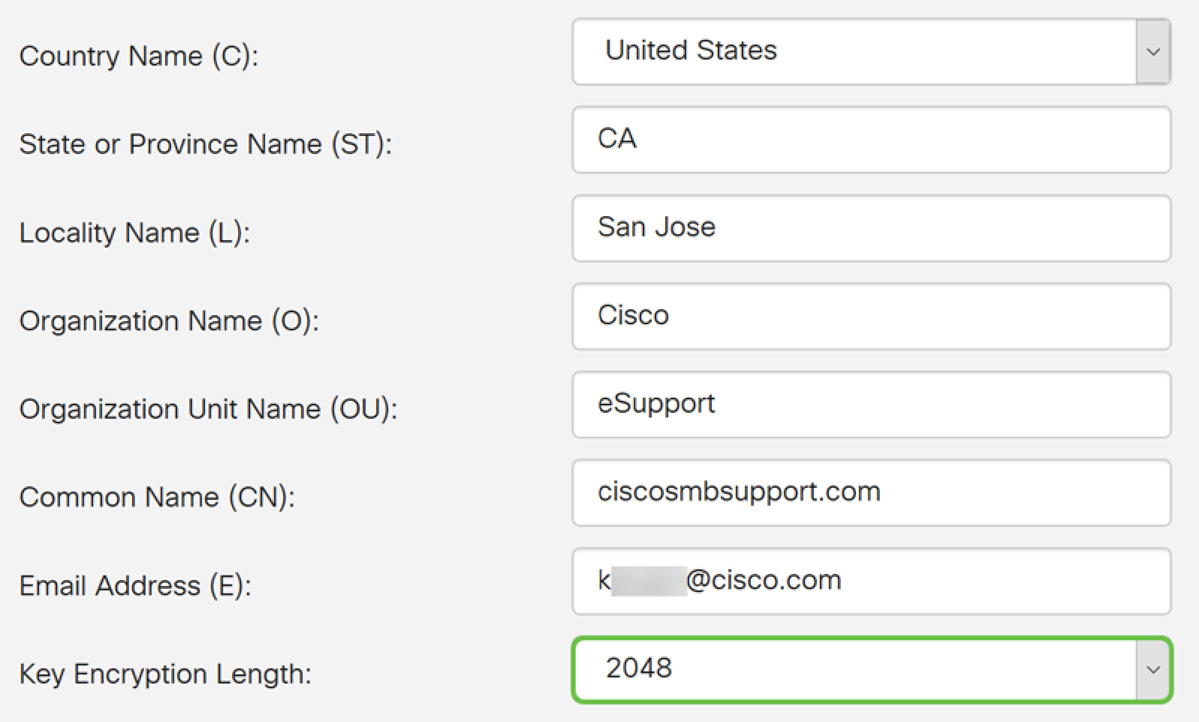
步骤13.输入电子邮**件地址**。



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

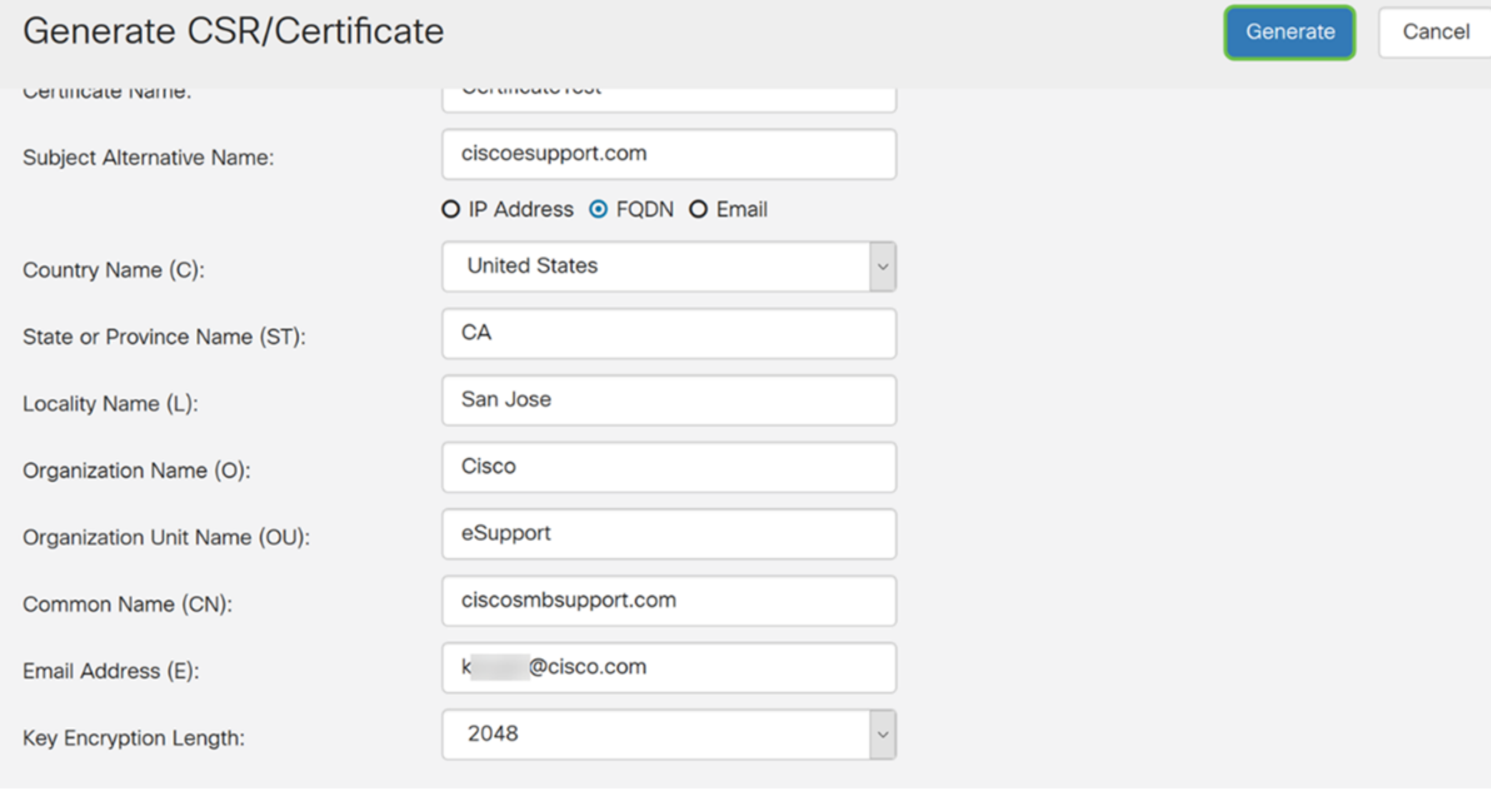
步骤14.从下拉菜**单中选**择Key Encryption Length。选项有：**512、1024 或 2048.**密钥大小越大，证书就越安全。密钥大小越大，处理时间越长。

最佳实践:建议选择最高密钥加密长度 — 启用更严格的加密。



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

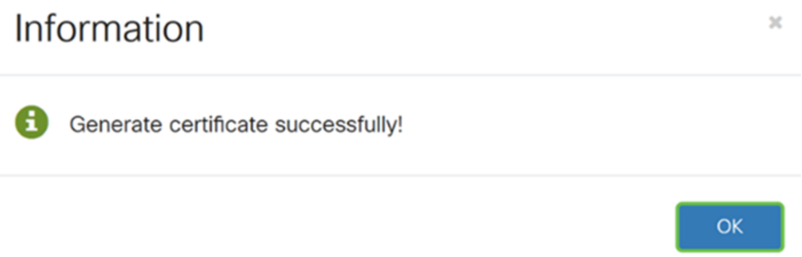
步骤15.单击“**生成”**。



Generate CSR/Certificate

Certificate Name:	CertificateTest
Subject Alternative Name:	ciscoesupport.com ○ IP Address ● FQDN ○ Email
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

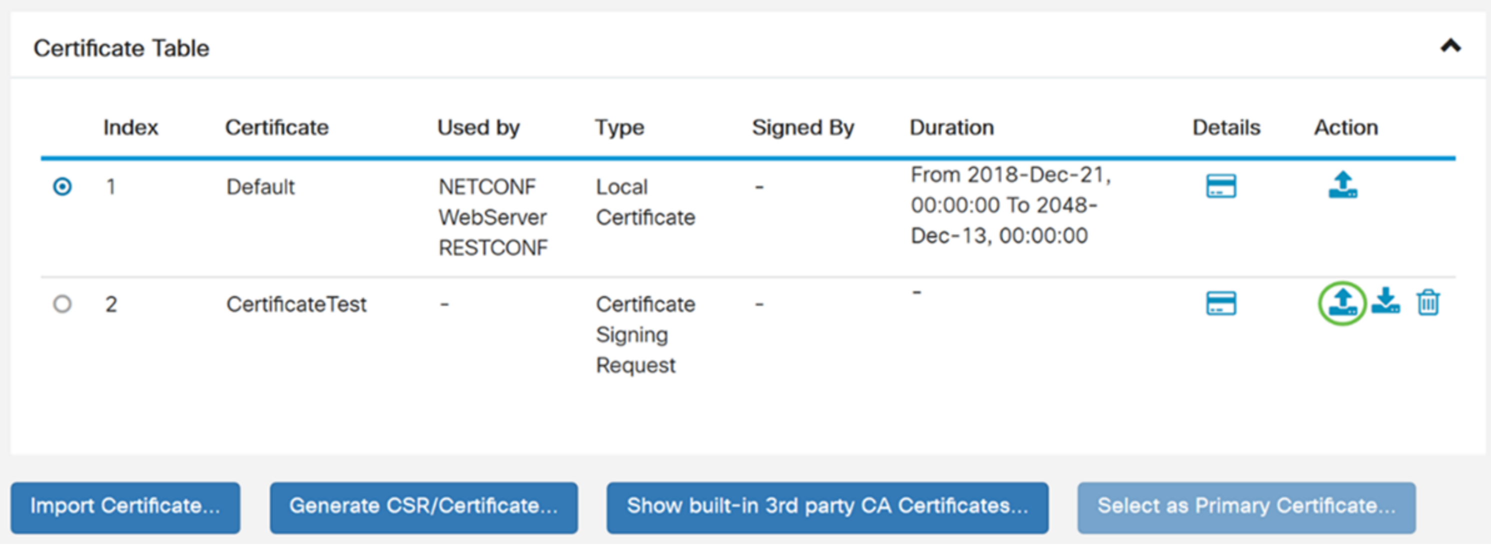
步骤16.系统将*显示*一个“信息”弹出窗口，其中显示“成功生成证书！” 邮件.单击 **OK** 继续。



Information

Generate certificate successfully!

步骤17.从证书表导出*CSR*。

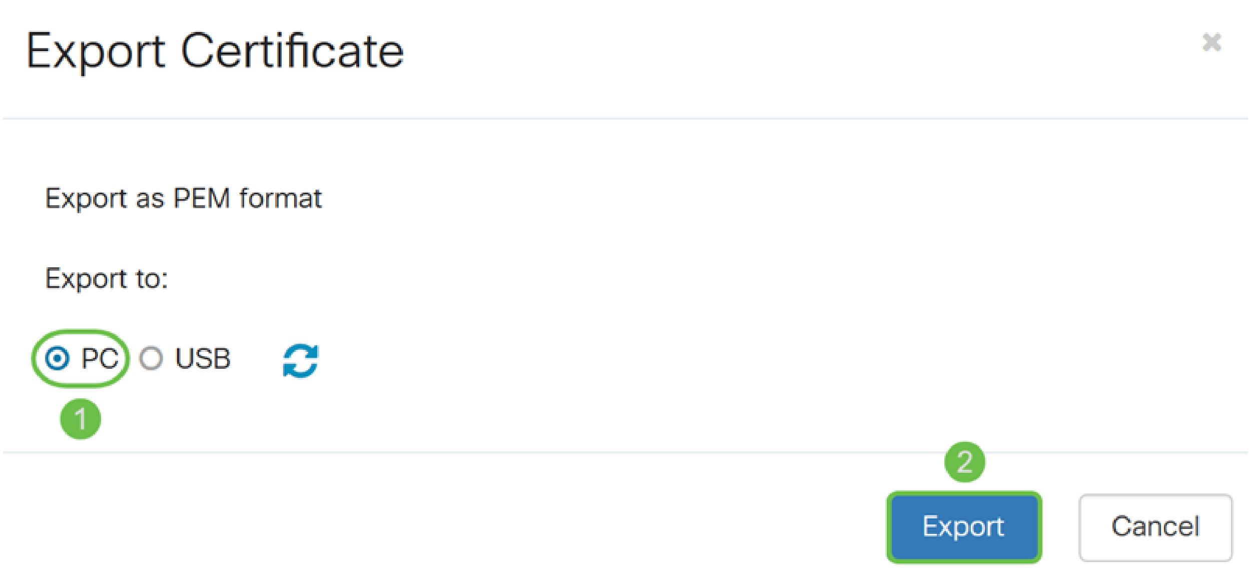


Certificate Table

	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	▭	⬆
○	2	CertificateTest	-	Certificate Signing Request	-	-	▭	⬆ ⬇ 🗑

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

步骤18.出现“*导出证书*”窗口。为“**导出**到”选*择PC*，然后单击**导出**。



Export Certificate

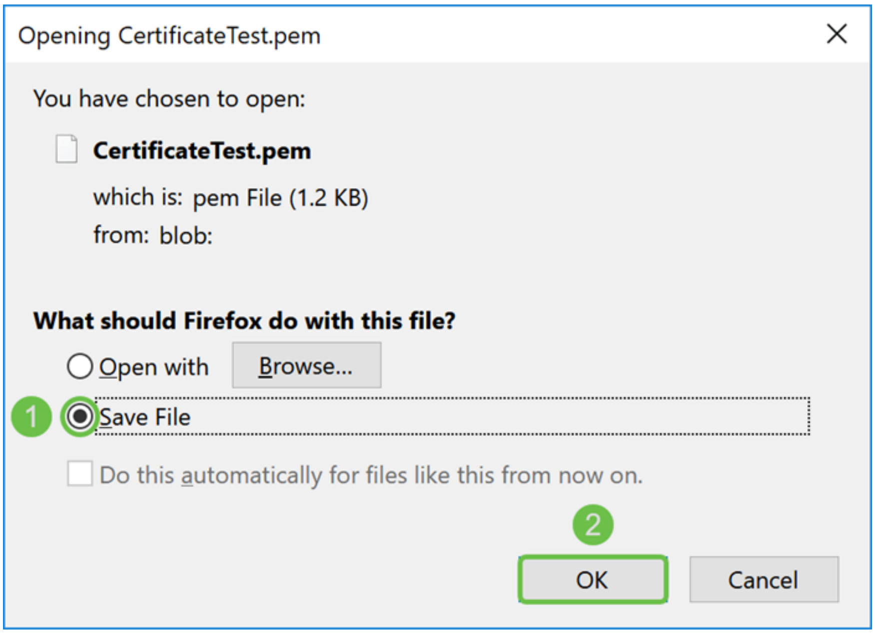
Export as PEM format

Export to:

● PC ○ USB

步骤19.应出现另一个窗口，询问是打开还是保存文件。

在本例中，我们将选择“保存文**件”**，然后单击“**确定”**。



Opening CertificateTest.pem

You have chosen to open:

CertificateTest.pem

which is: pem File (1.2 KB)

from: blob:

What should Firefox do with this file?

○ Open with

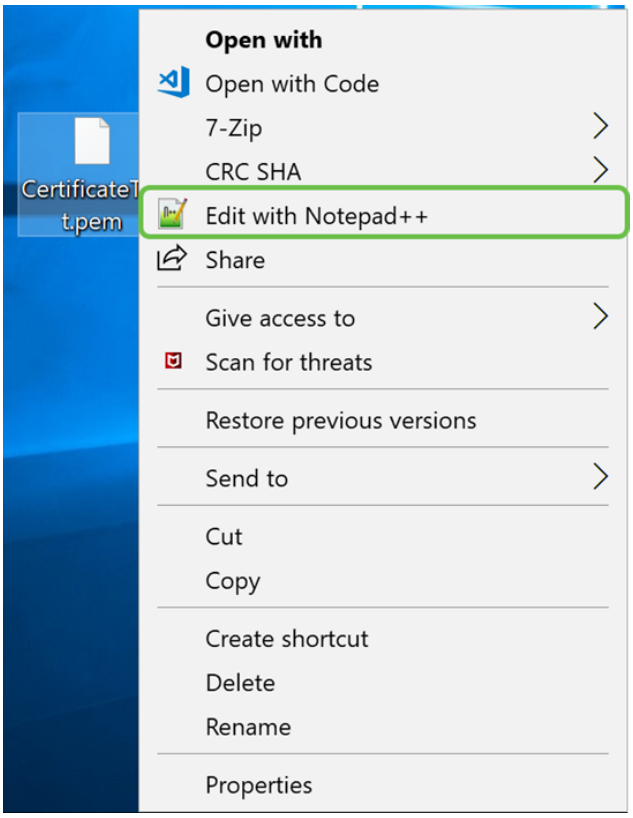
● Save File

□ Do this automatically for files like this from now on.

步骤20.查找.pem文件的保存位置。**右键单击**.pem文件，然后使用您最喜爱的文本编辑器将其打开。

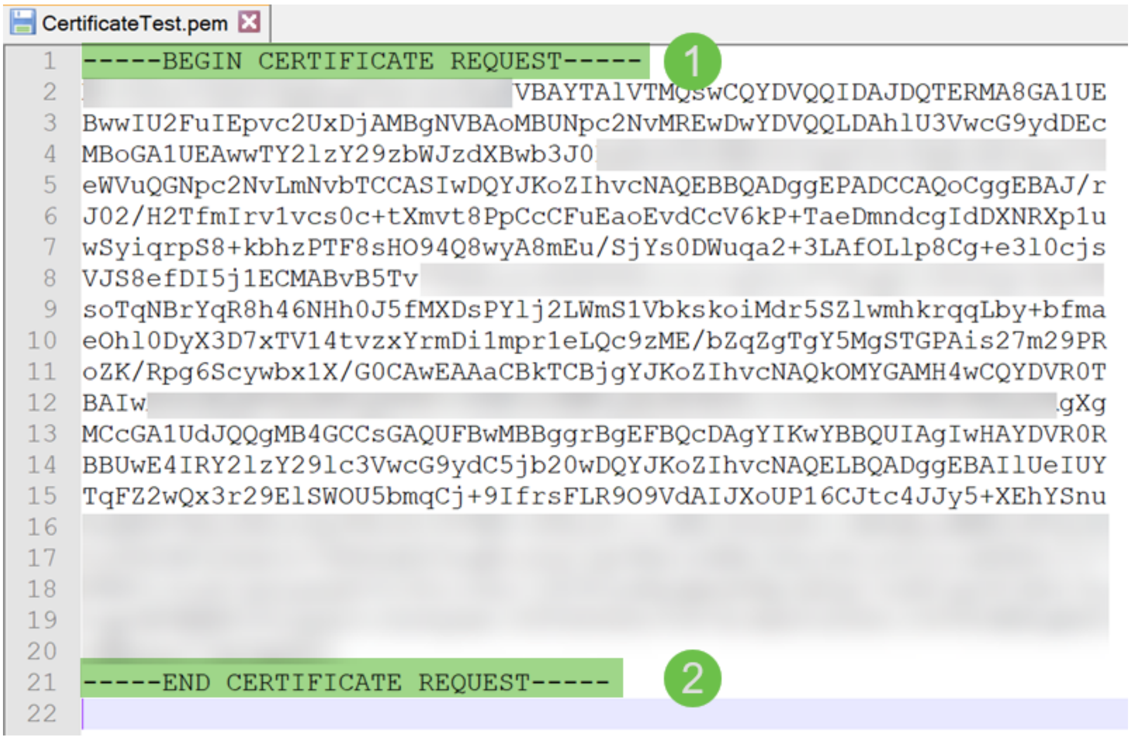
在本例中，我们将使用Notepad++打开.pem文件。

注意：使用记事本打开时，您可以随意打开。



步骤21.确保*—BEGIN CERTIFICATE REQUEST —*和*—END CERTIFICATE REQUEST —*在其自己的行上。

注意：证书的某些部分被模糊了。

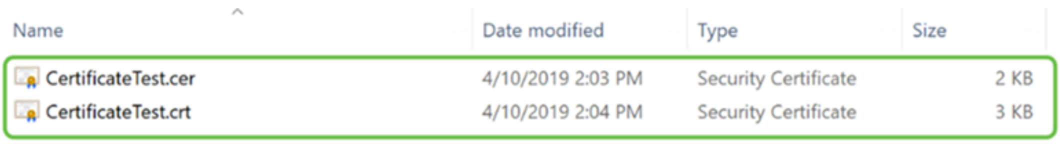


```
-----BEGIN CERTIFICATE REQUEST-----
[redacted]VBAYTAlVTMQswCQYDVQQIDAJDQTERMA8GA1UE
BwwIU2FuIEpvc2UxDjAMBgNVBAoMBUNpc2NvMREwDwYDVQQLDAhlU3VwcG9ydDEc
MBoGA1UEAwwTY2lzY29zbWJzdXBwb3J0[redacted]
eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXp1u
wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LAfOLlp8Cg+e310cjs
VJS8efDI5j1ECMABvB5Tv[redacted]
soTqNBrYqR8h46NHh0J5fMXDsPYlj2LWmS1VbkskoiMdr5SZlwmhkrqqLby+bfma
eOhl0DyX3D7xTV14tvzxYrmDi1mpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
oZK/Rpg6Scywbx1X/G0CAwEAAaCBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
BAIw[redacted]gXg
MCcGA1UdJQQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
BBUwE4IRY2lzY29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAIlUeIUY
TqFZ2wQx3r29ElSWOU5bmqCj+9IfrsFLR9O9VdAIJXoUP16CJtc4JJy5+XEhYSnu
[redacted]
-----END CERTIFICATE REQUEST-----
```

步骤22.当您拥有CSR时，您需要转到您的托管服务或证书颁发机构站点（如GoDaddy、Verisign等）并请求证书。提交请求后，它将与证书服务器通信，以确保没有任何理由不颁发证书。

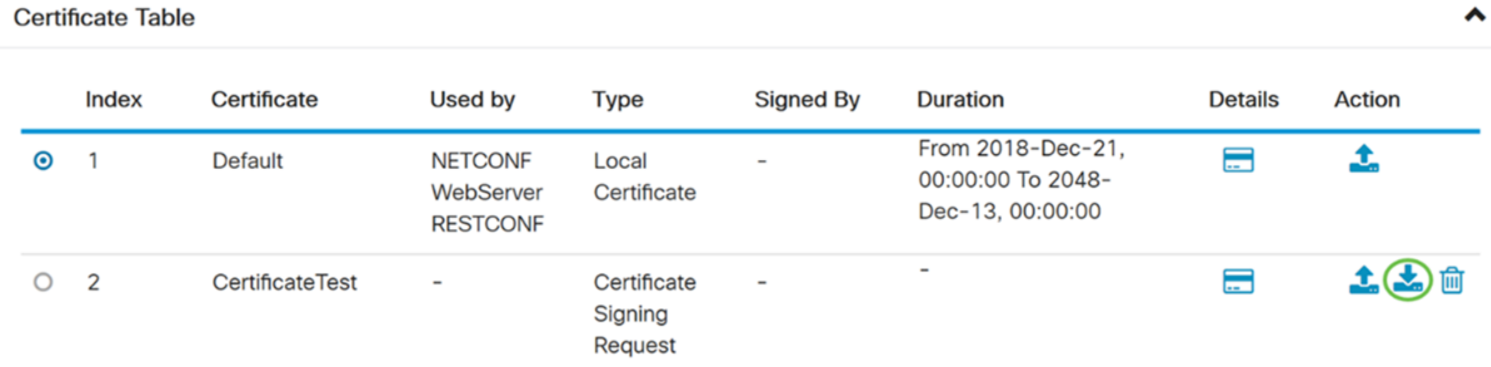
注意：如果您不知道证书请求在其站点上的位置，请联系CA或托管站点支持。

步骤23.完成证书后下载。它应该是.cer**或**.crt**文件**。在本例中，我们提供了两个文件。



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

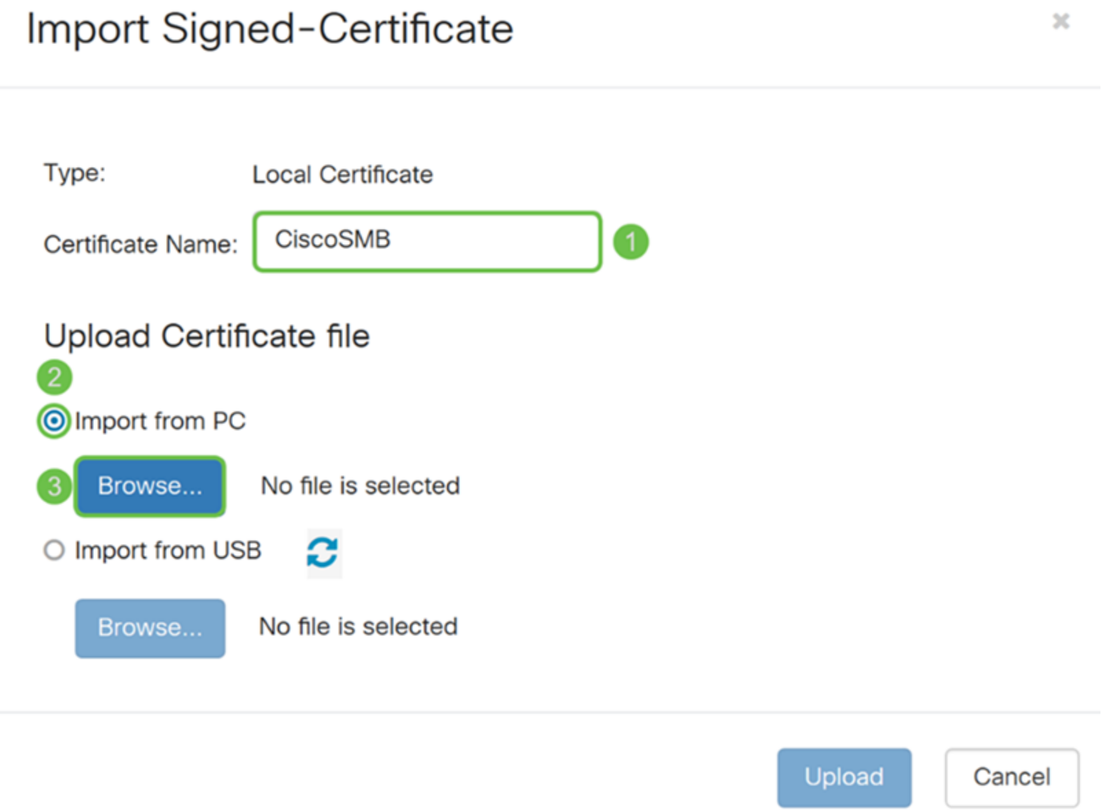
步骤24.返回路由器的*Certificate页*面，单击指向设备图标的**箭头导入证书**文件。



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		
○	2	CertificateTest	-	Certificate Signing Request	-	-		

步骤25.在Certificate Name字*段中*，输入证书**名称**。它不能与证书签名请求同名。在“上*载证书文件*”部分**，选择从PC**导入，**然后单击“浏览……**”上传证书文件。



Import Signed-Certificate

Type: Local Certificate

Certificate Name: CiscoSMB

Upload Certificate file

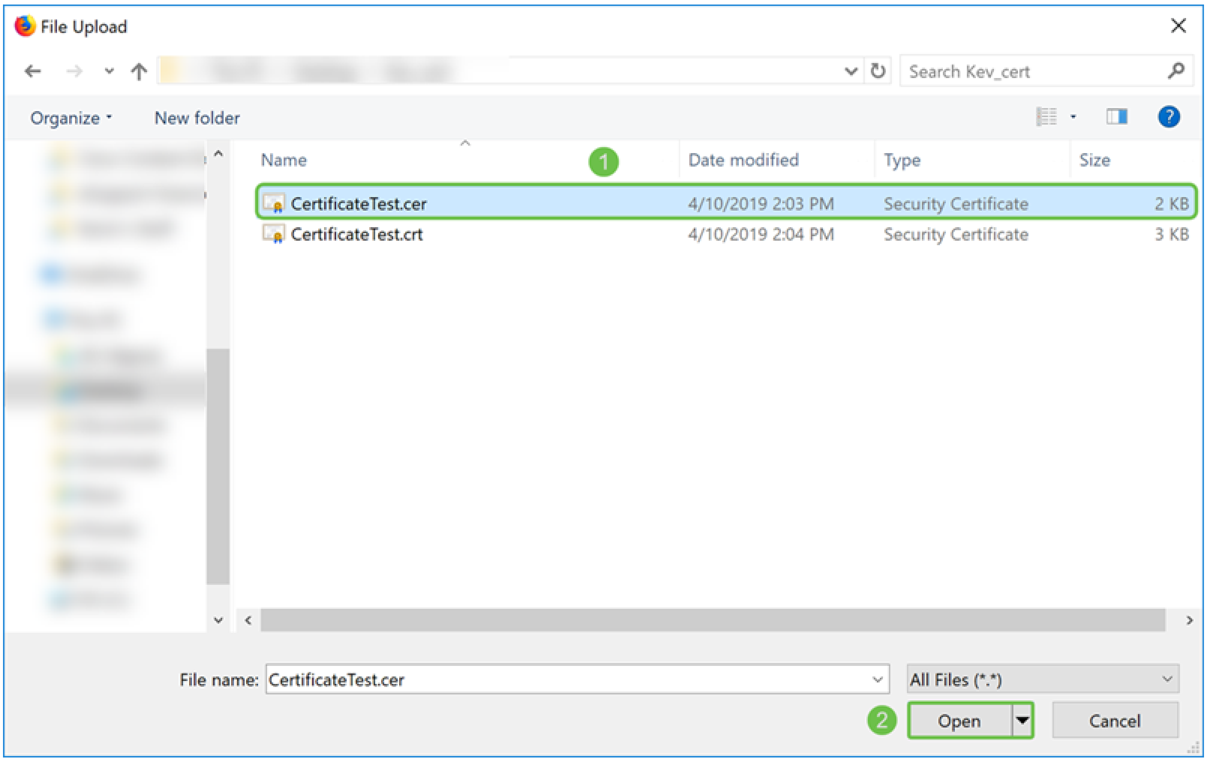
● Import from PC

Browse... No file is selected

○ Import from USB

Browse... No file is selected

步骤26.出现“文*件上传*”窗口。导航至证书文件所在的位置。选择要**上**载的证书文件，然后单击**Open**。在本示例中，选**择了CertificateTest.cer**。



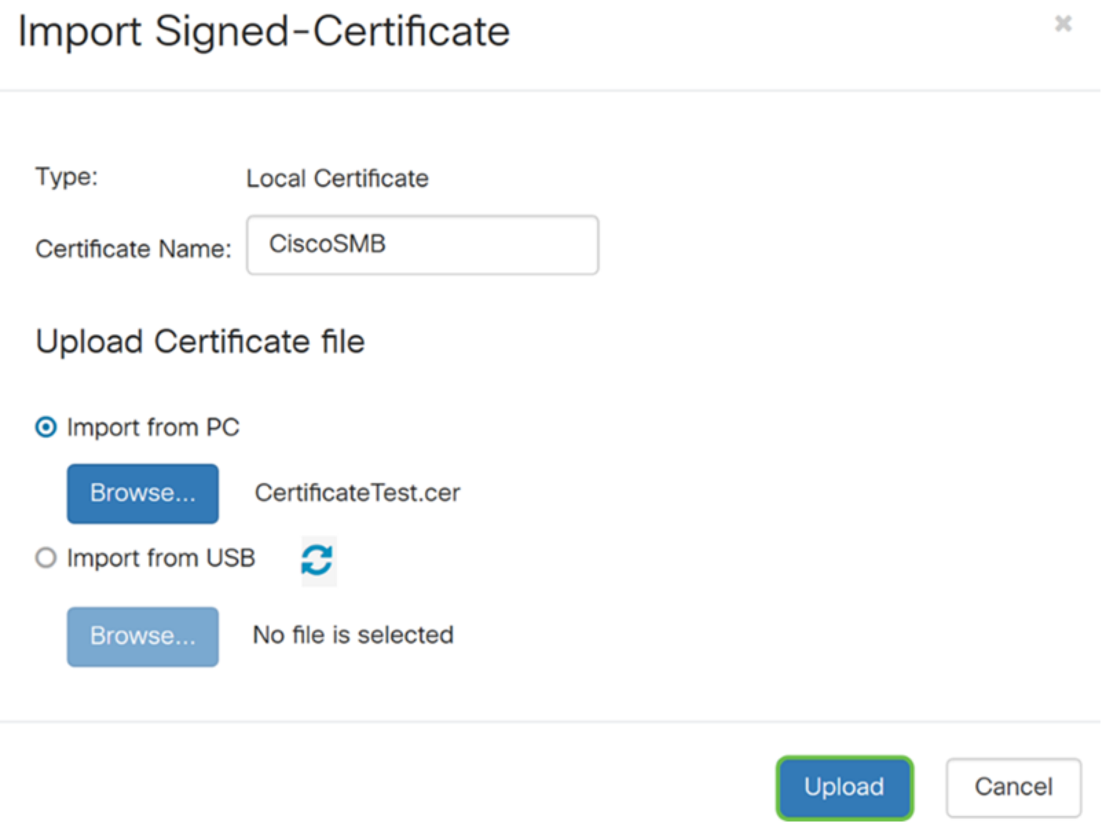
Name	Date modified	Type	Size
CertificateTest.cer	4/10/2019 2:03 PM	Security Certificate	2 KB
CertificateTest.crt	4/10/2019 2:04 PM	Security Certificate	3 KB

File name: CertificateTest.cer

All Files (*.*)

步骤27.单击“**上载**”按钮开始将证书上传到路由器。

注意：如果出现无法上传.cer文件的错误，可能是因为您的路由器要求证书采用pem编码。您需要将您的der编码（.cer文件扩展名）转换为pem编码（.crt文件扩展名）。



Type: Local Certificate

Certificate Name: CiscoSMB

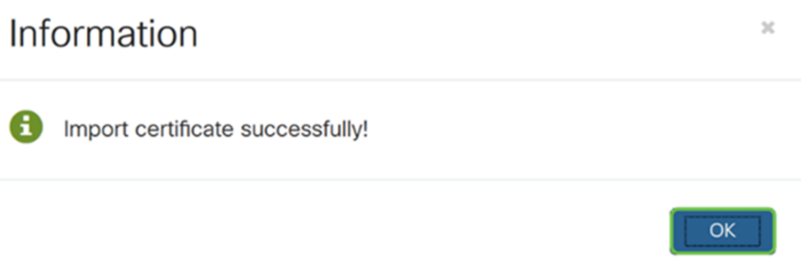
● Import from PC

CertificateTest.cer

○ Import from USB

No file is selected

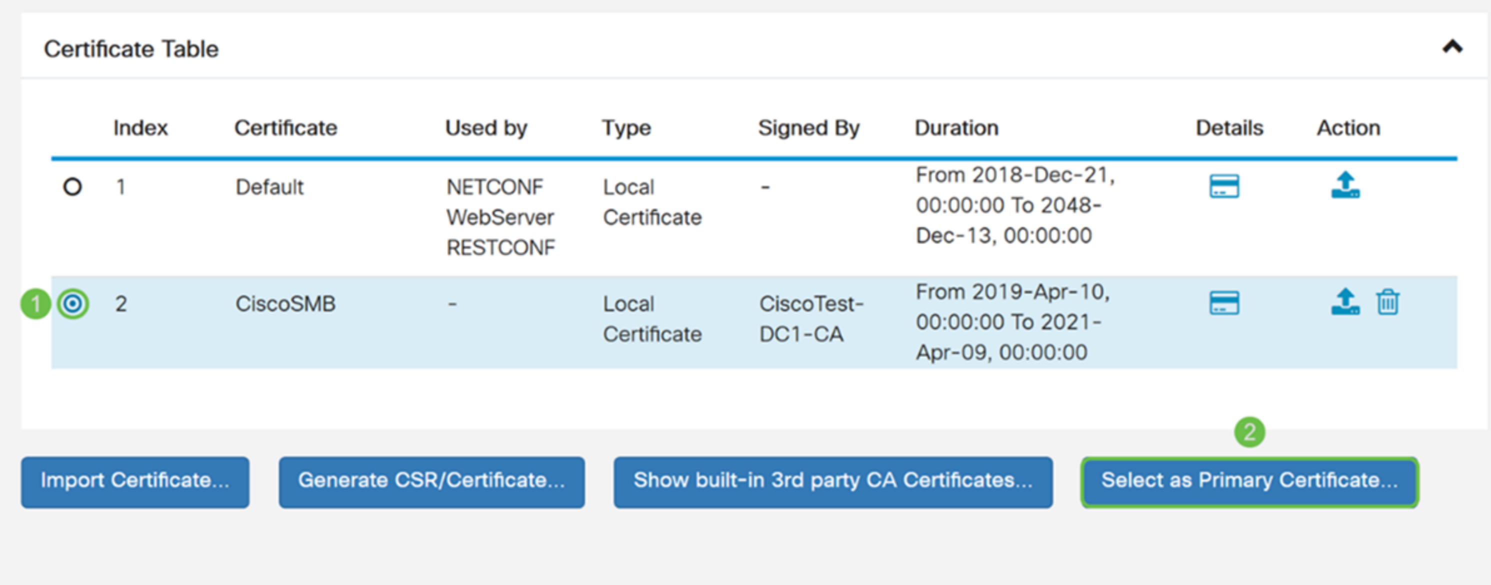
步骤28.如果导入成功，则应显示一个信息窗口，告知您导入成功。单击 **OK** 继续。



Information

Import certificate successfully!

步骤29.您的证书应成功更新。您应该能够查看证书的签名者。在本例中，我们可以看到我们的证书由*CiscoTest-DC1-CA*签名。要使证书成为我们的主证书，请使用左侧的单选按钮选择证书，然后单击**Select as Primary Certificate...按**钮。



Certificate Table

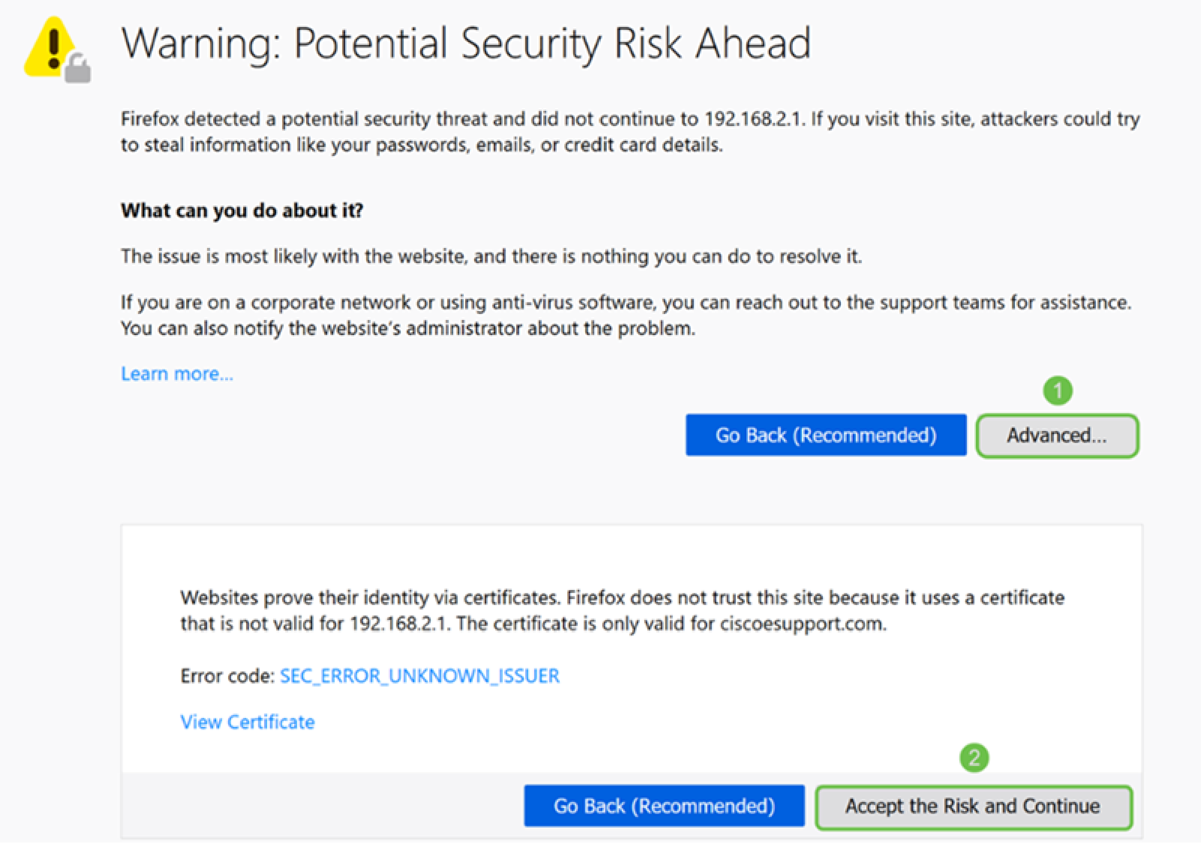
	Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
○	1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
●	2	CiscoSMB	-	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

1
2
Import Certificate...
Generate CSR/Certificate...
Show built-in 3rd party CA Certificates...
Select as Primary Certificate...

注意：更改主证书可能会返回到警告页面。如果您使用Firefox，并且它显示为灰色空白页面，则需要调整Firefox上的一些配置。Mozilla Wiki上的本文档对此进行了一些说明：CA/AddRootToFirefox。要再次看到警告页，请执行Mozilla社区支持页中的这些步骤。

步骤30.在Firefox警告页中，单击**Advanced...**，然**后单击Accept the Risk and Continue**以继续进入路由器。

注意：这些警告屏幕会因浏览器而异，但执行相同的功能。



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.

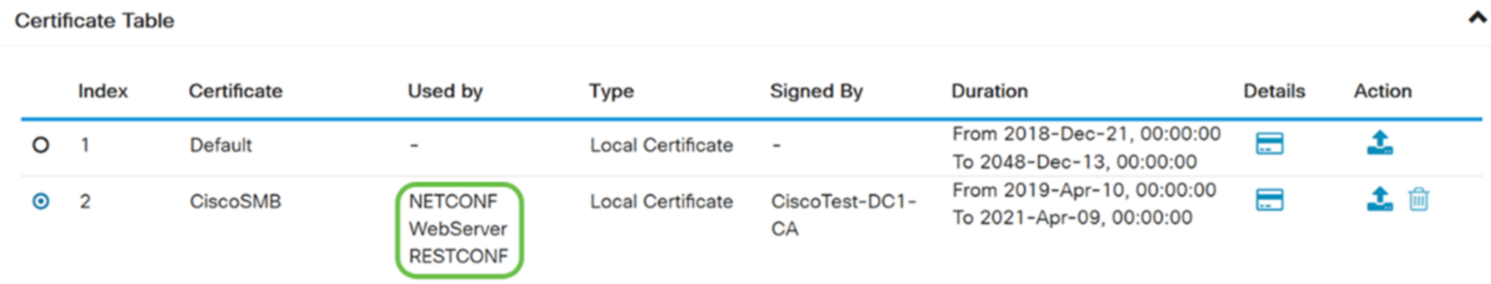
Learn more...

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

步骤31.在证书表中，您应该看到NETCONF、*WebServer*和RESTCONF已交换到您的新证书，而不是使用Default证书。



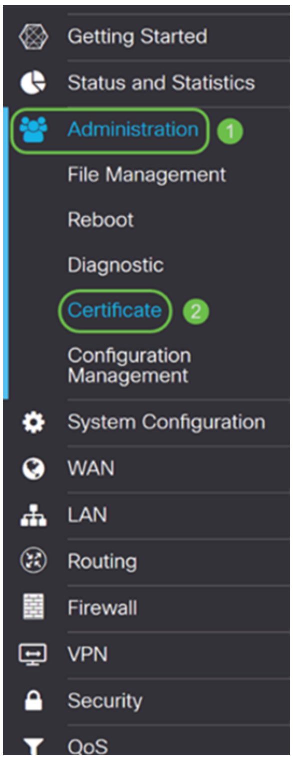
Certificate Table

	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		

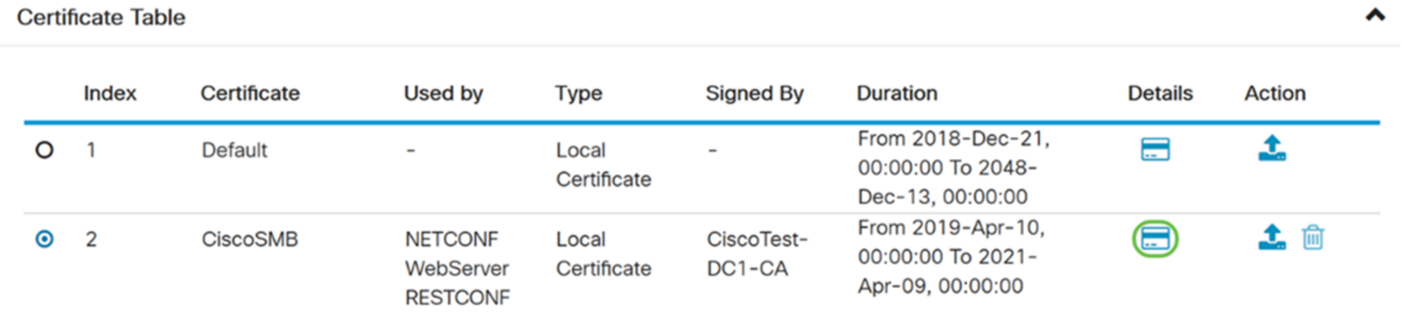
现在，您应该已成功将证书安装到您的路由器上。

查看证书

步骤1.如果已从“证书”页导航至“管理”>“**证书”**。



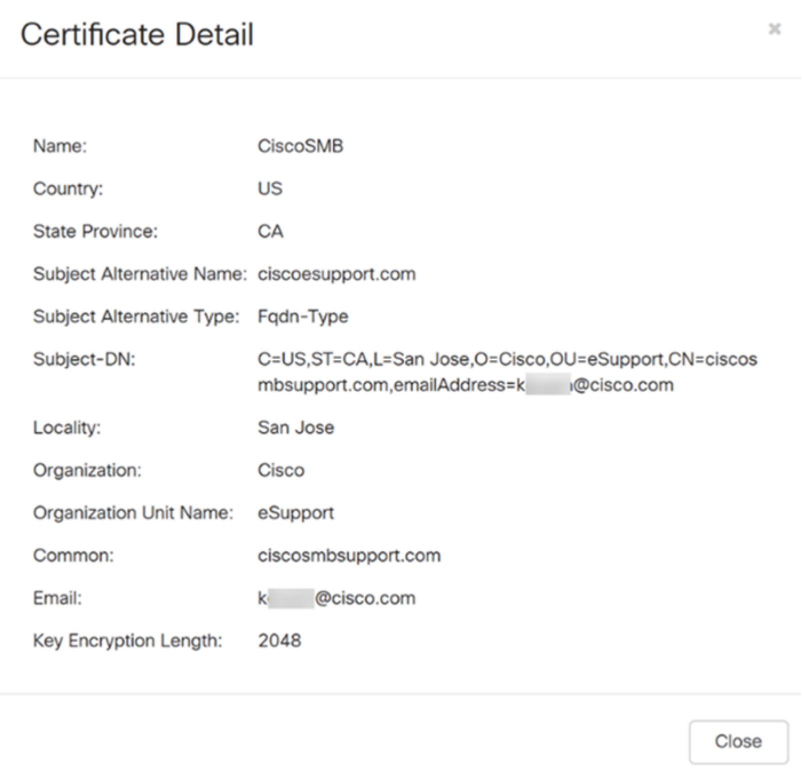
步骤2.在Certificate Table(*证书表*)中，单击Details(详细**信息)**部分下方的*Details(详细*信息)图标。



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		

步骤3.系统将显示*Certificate Detail*页面。您应该能够查看有关证书的所有信息。

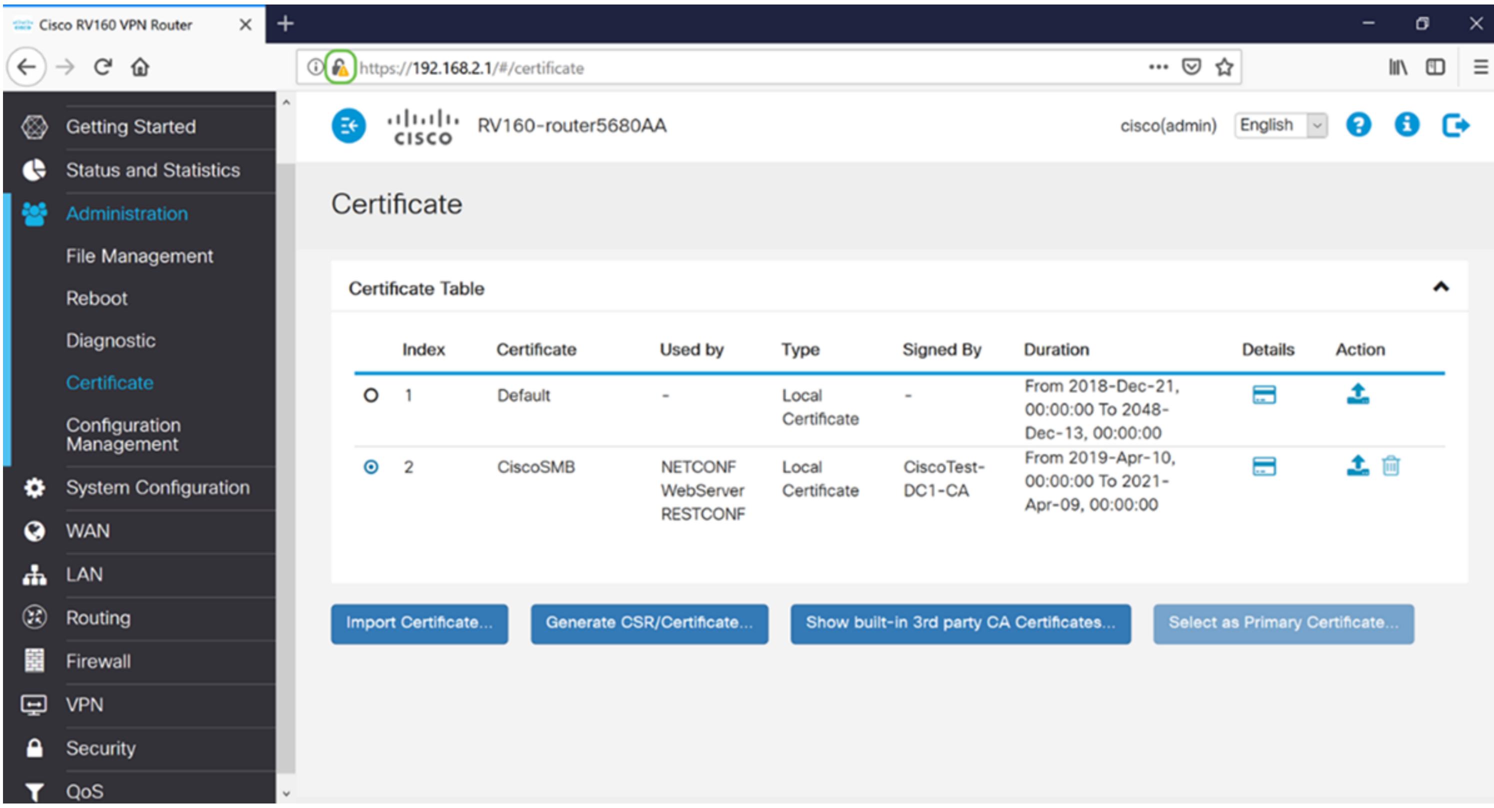


Certificate Detail

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

步骤4.单击**Uniform Resource Locator(URL)栏左侧的锁图标。**

注意：在Firefox浏览器中使用以下步骤。



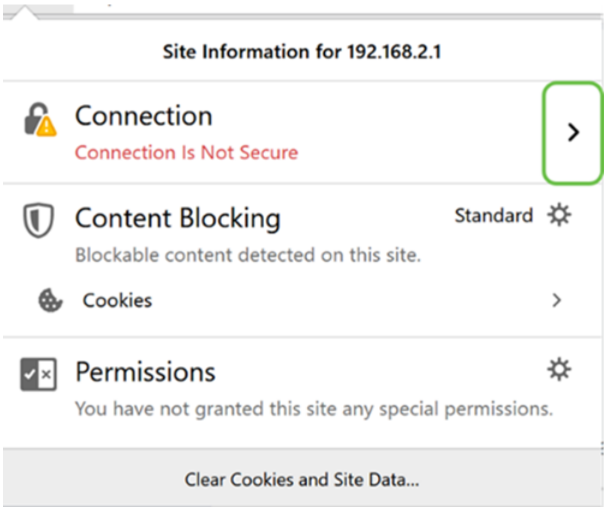
Certificate

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...

步骤5.系统将显示选项下拉列表。单击“Connection”字段旁的箭头图标。



Site Information for 192.168.2.1

Connection

Connection Is Not Secure

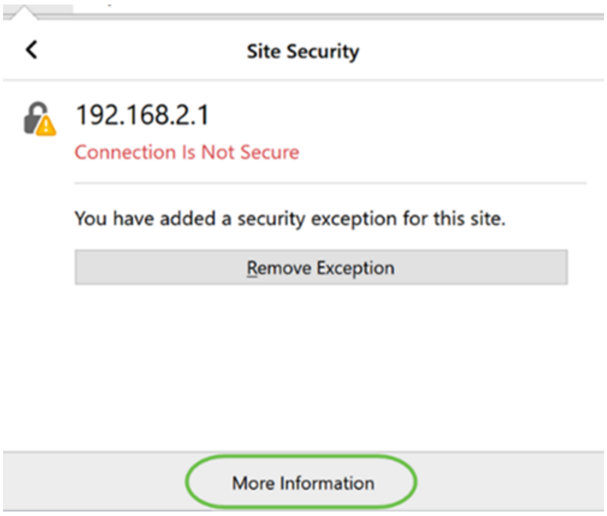
Content Blocking

Blockable content detected on this site.

Permissions

You have not granted this site any special permissions.

步骤6.单击“更**多信息”**。



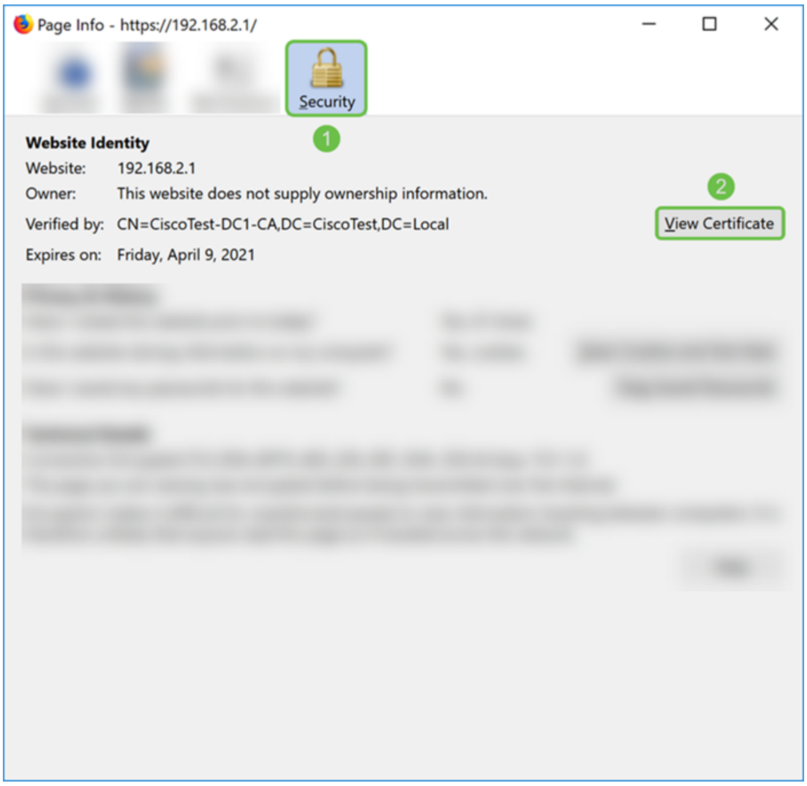
Site Security

192.168.2.1

Connection Is Not Secure

You have added a security exception for this site.

步骤7.在“页面*信息*”窗口中，您应能在“网站身份”部分下看到有关证*书的简*要信息。确保您处于“安全”选**项卡**中，然后单击“**查看证**书”以查看有关证书的详细信息。



Page Info - https://192.168.2.1/

Website Identity

Website: 192.168.2.1

Owner: This website does not supply ownership information.

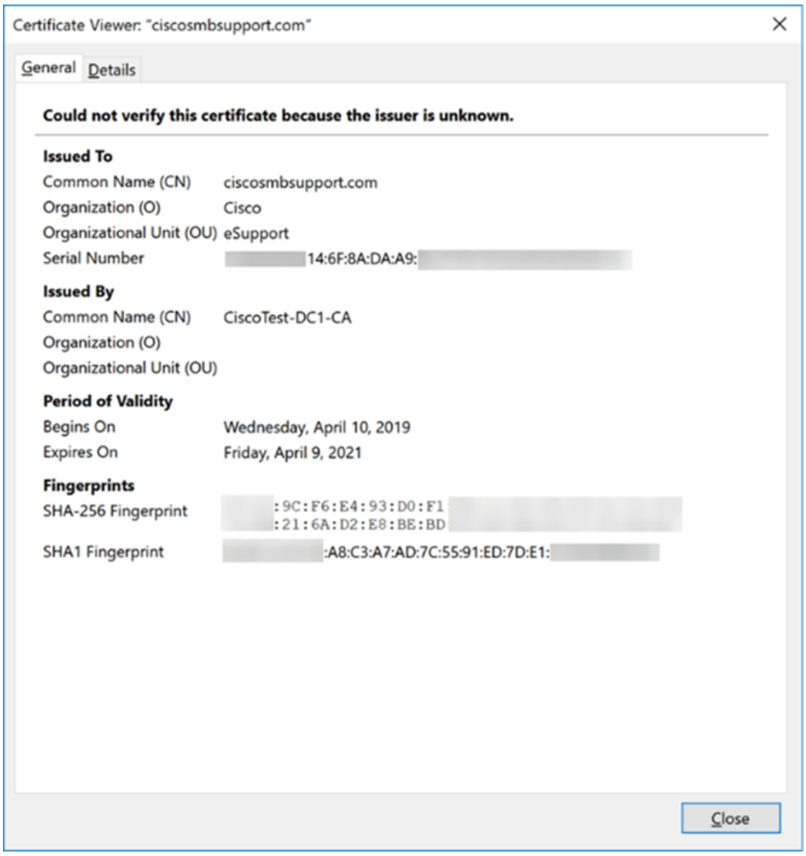
Verified by: CN=CiscoTest-DC1-CA,DC=CiscoTest,DC=Local

Expires on: Friday, April 9, 2021

步骤8.应显示*Certificate Viewer*页面。您应该能够查看有关证书、有效期、指纹以及颁发者的

所有信息。

注意：由于此证书由测试证书服务器颁发，因此颁发者未知。



Certificate Viewer: "ciscosmbsupport.com"

General Details

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	ciscosmbsupport.com
Organization (O)	Cisco
Organizational Unit (OU)	eSupport
Serial Number	[redacted]14:6F:8A:DA:A9:[redacted]

Issued By

Common Name (CN)	CiscoTest-DC1-CA
Organization (O)	
Organizational Unit (OU)	

Period of Validity

Begins On	Wednesday, April 10, 2019
Expires On	Friday, April 9, 2021

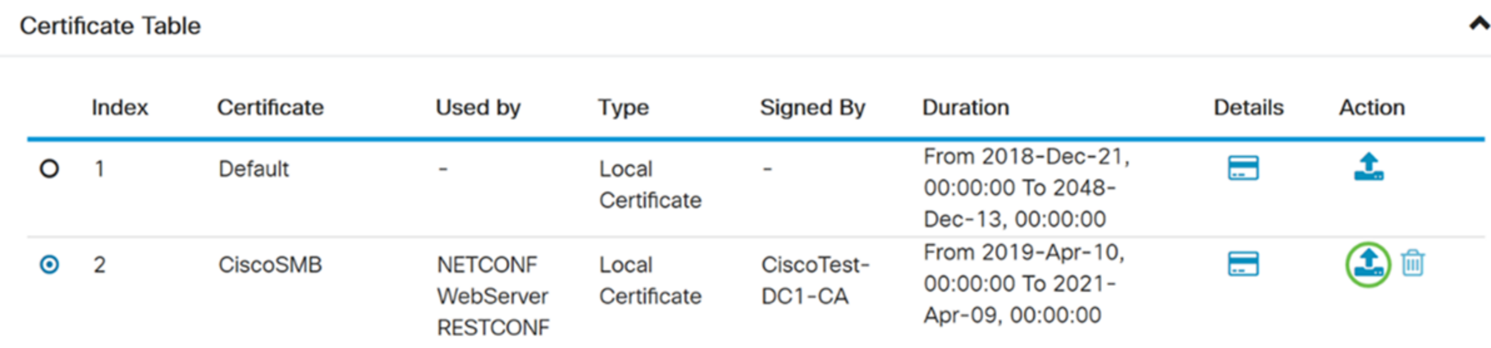
Fingerprints

SHA-256 Fingerprint	[redacted]:9C:F6:E4:93:D0:F1[redacted] :21:6A:D2:E8:BE:BD
SHA1 Fingerprint	[redacted]:A8:C3:A7:AD:7C:55:91:ED:7D:E1:[redacted]

导出证书

要下载证书以将其导入另一台路由器，请执行以下步骤。

步骤1.在“*证书*”页面中，单击**要导**出的证书旁边的导出图标。



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		

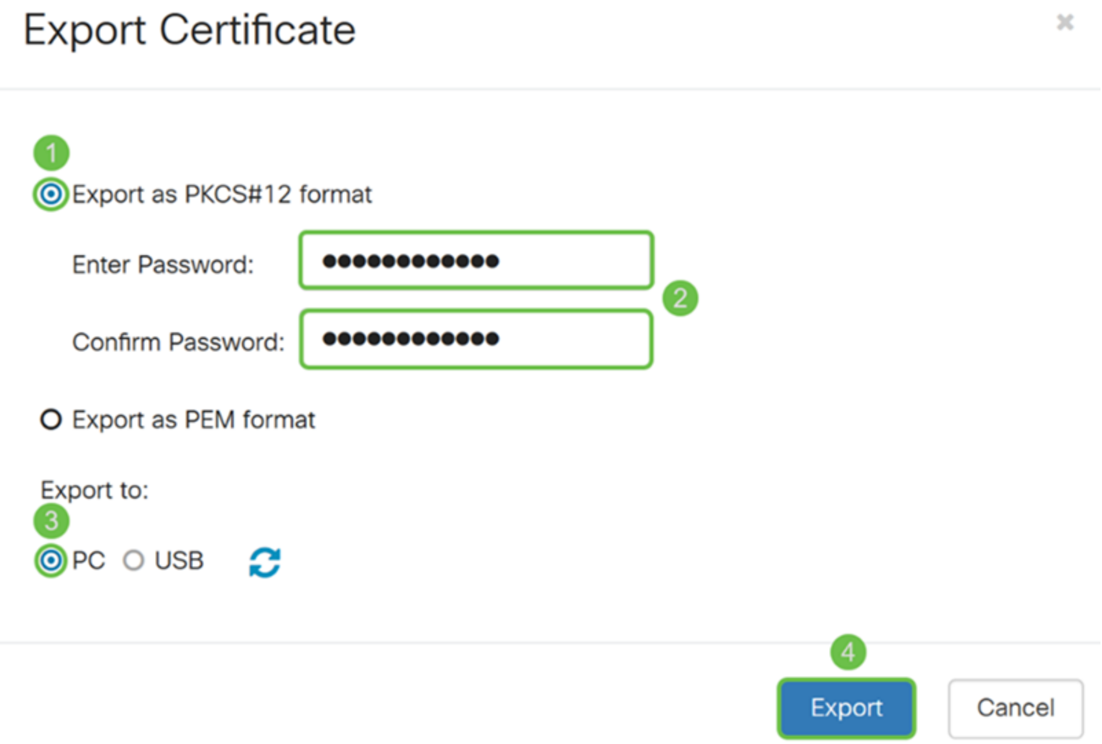
步骤2.出现*导出证*书。选择导出证书的格式。选项有：

·**PKCS#12** — 公钥加密标准(PKCS)#12是带有.p12扩展的导出证书。要加密文件以在文件导出、导入和删除时对其进行保护，需要密码。

·**PEM** – Πριϖαχψ Ενηανχεδ Μαιλ(ΠΕΜ)Ωεβ

选择**Export as PKCS#12 format并**输入密**码**和**确认密码**。然后选**择PC**作导*出到：*字段。单击**Export**开始将证书导出到计算机。

注意：请记住此密码，因为您将在将其导入路由器时使用它。



Export Certificate

1 ● Export as PKCS#12 format

Enter Password: ●●●●●●●●●●●●●

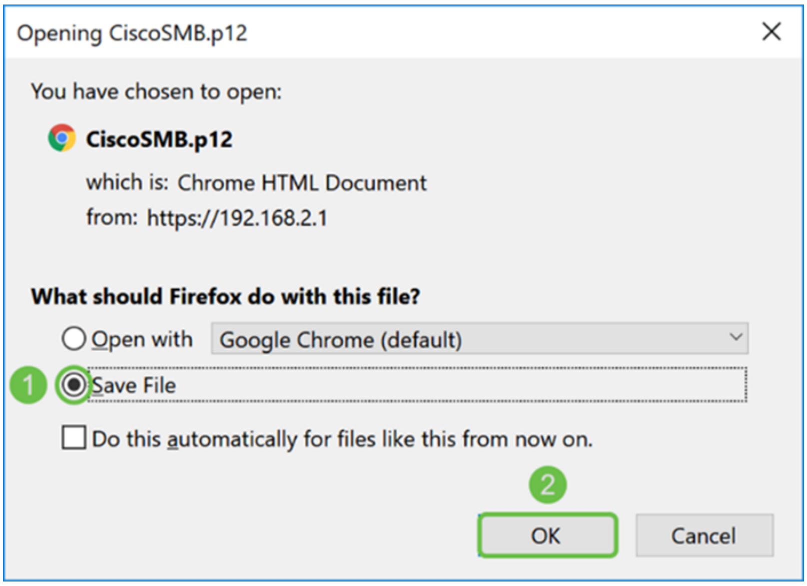
Confirm Password: ●●●●●●●●●●●●● 2

○ Export as PEM format

Export to:

3 ● PC ○ USB

步骤3.将出现一个窗口，询问您应如何处理此文件。在本例中，我们将选择“保存文**件”，**然后单击“**确定”**。



Opening CiscoSMB.p12

You have chosen to open:

CiscoSMB.p12

which is: Chrome HTML Document

from: https://192.168.2.1

What should Firefox do with this file?

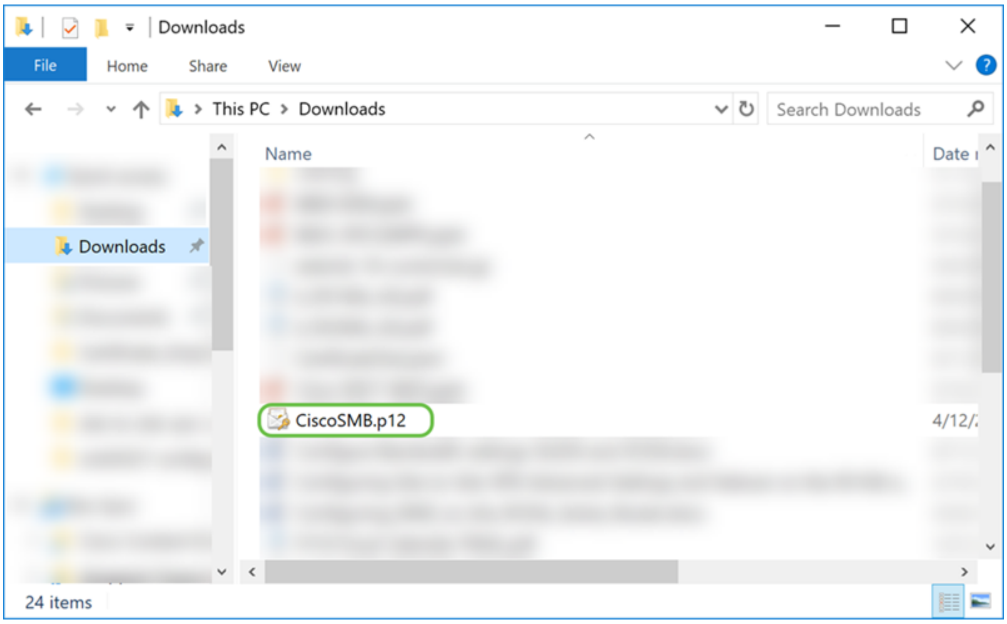
○ Open with Google Chrome (default)

1 ● Save File

□ Do this automatically for files like this from now on.

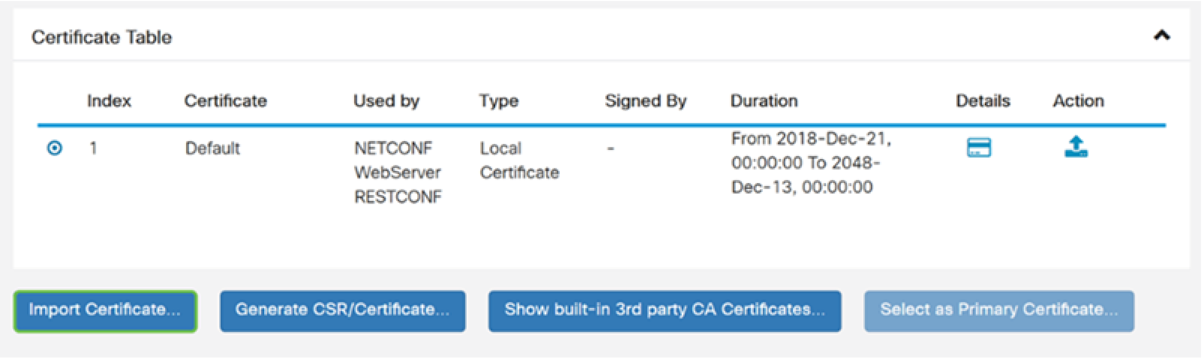
步骤4.文件应保存到默认保存位置。

在我们的示例中，该文件已保存到计算机*上的*“下载”文件夹中。



导入证书

步骤1.在“证*书*”页面中，单**击“导入证书.......**”按钮。


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...

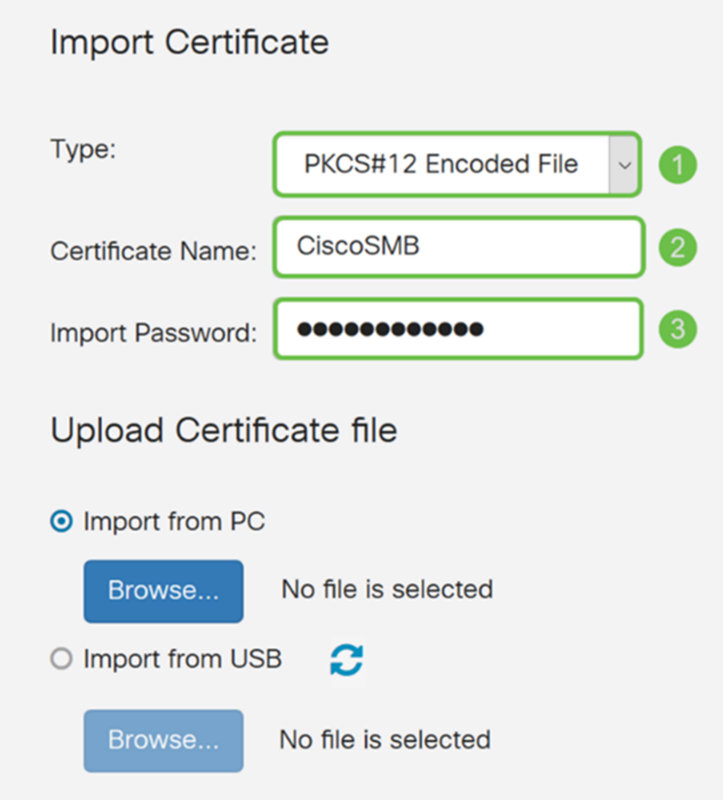
步骤2.从“导入证**书”**部分下的“类型”下*拉列*表中选择要导入的证*书类型*。选项定义为：

- **CA证书** — 由可信第三方机构认证的证书，其确认证书中包含的信息准确。

·**本地设备证书**

·**PKCS#12 Encoded File** - Public Key Cryptography Standards(PKCS)#12是带有.p12扩展的导出证书。

在本示例中，**选择PKCS#12 Encoded File**作为类型。输入证**书**的名称，然后输**入**使用的密码。



Import Certificate

Type: PKCS#12 Encoded File

Certificate Name: CiscoSMB

Import Password: ●●●●●●●●●●●●●

Upload Certificate file

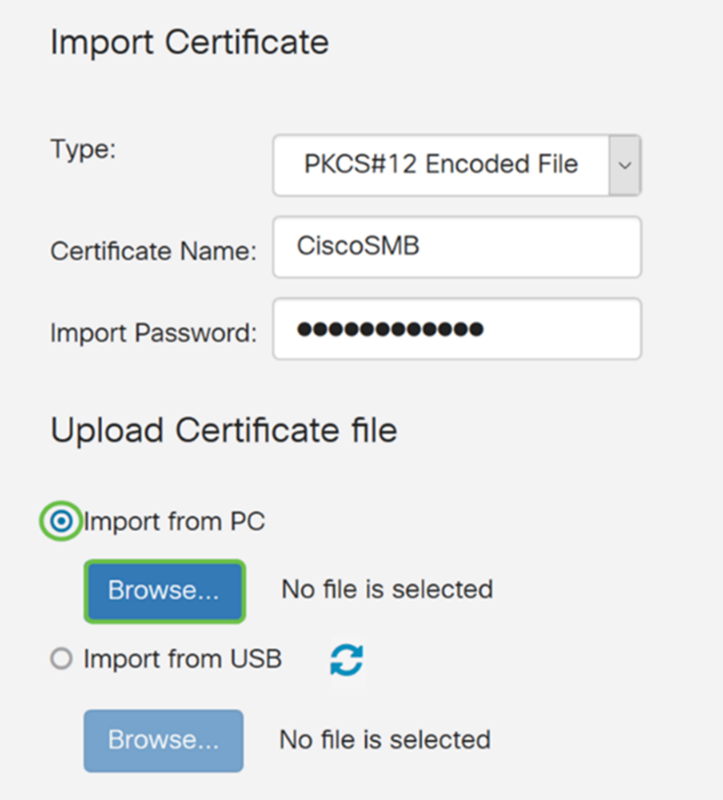
● Import from PC

Browse... No file is selected

○ Import from USB

Browse... No file is selected

步骤3.在Upload Certificate file部分下，选择Import from PC**或Import from USB**。在本示例中，选**择了从PC**导入。单击**Browse...**以选择要上传的文件。



Import Certificate

Type: PKCS#12 Encoded File

Certificate Name: CiscoSMB

Import Password: ●●●●●●●●●●●●●

Upload Certificate file

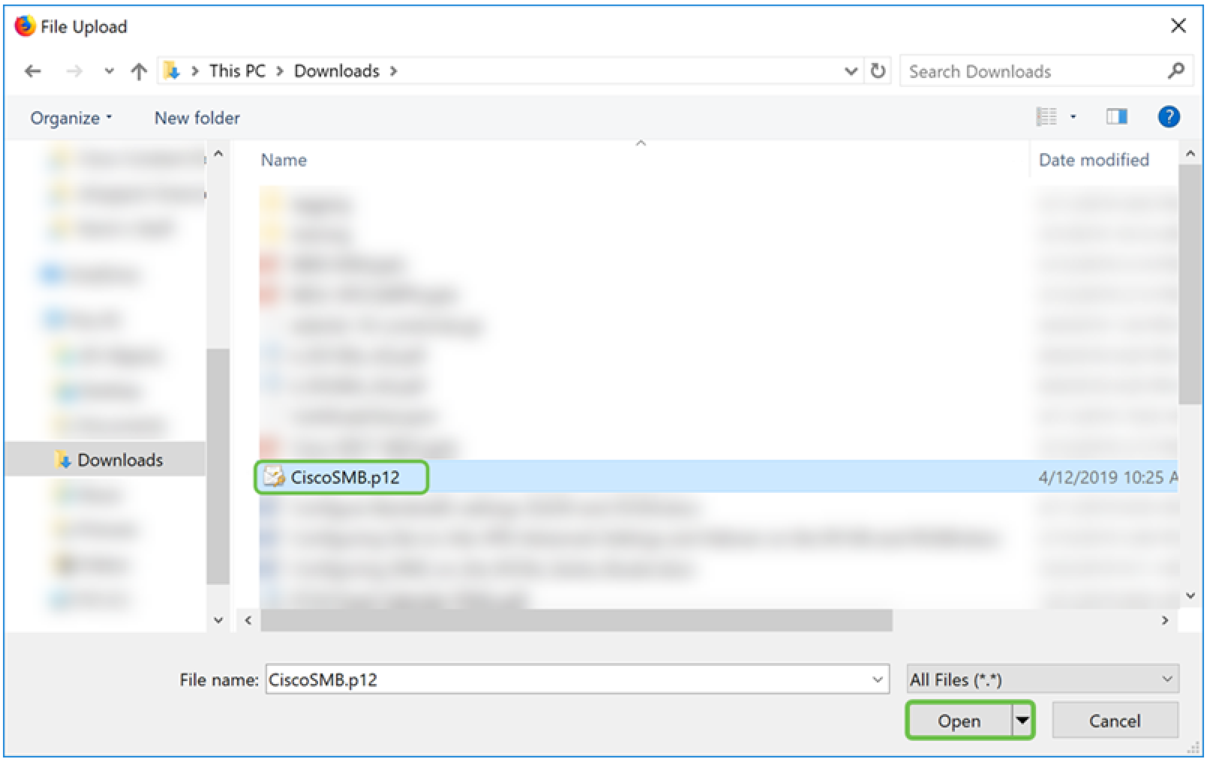
● Import from PC

Browse... No file is selected

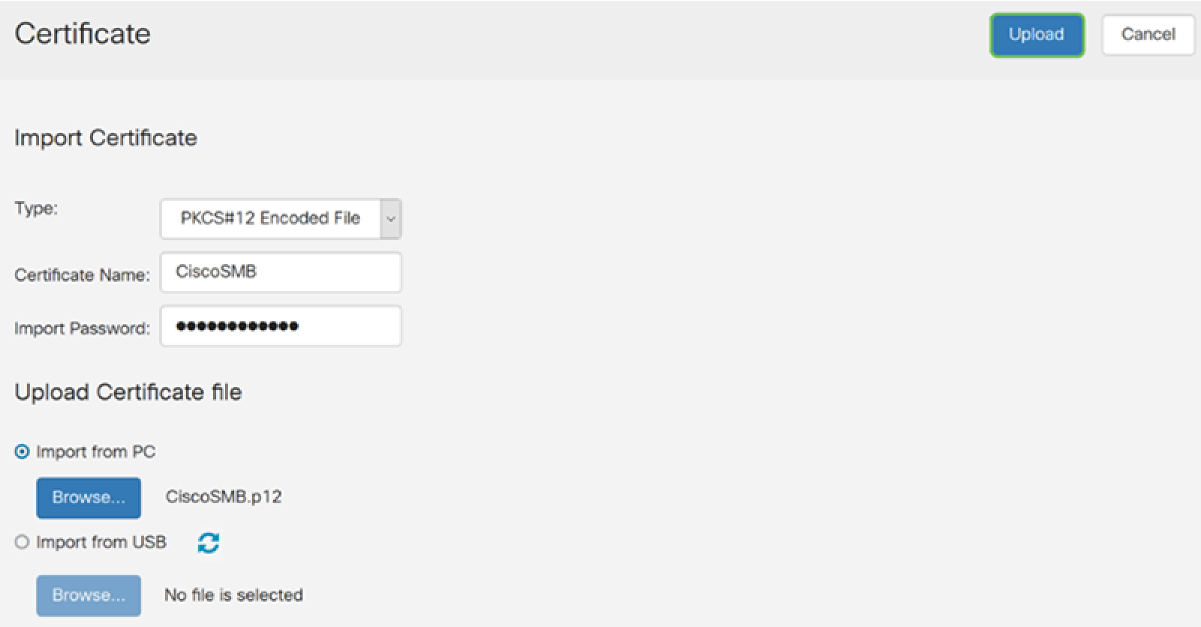
○ Import from USB

Browse... No file is selected

步骤4.在“文件*上传*”窗口中，导航至PKCS#12编码文件（.p12文件扩展名）所在的位置。选择。**p12文件**，然后单击“**打开”**。



步骤5.单击**Upload**开始上传证书。



Import Certificate

Type: PKCS#12 Encoded File

Certificate Name: CiscoSMB

Import Password: ●●●●●●●●●●●●●

Upload Certificate file

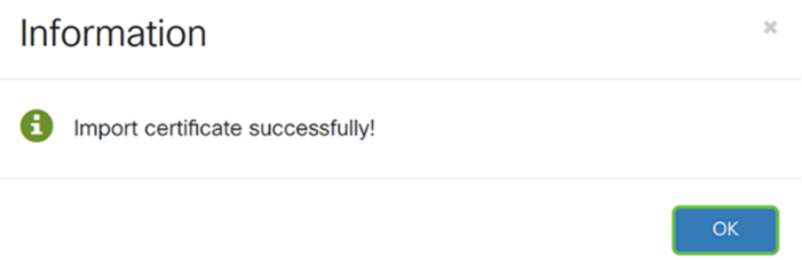
● Import from PC

Browse... CiscoSMB.p12

○ Import from USB

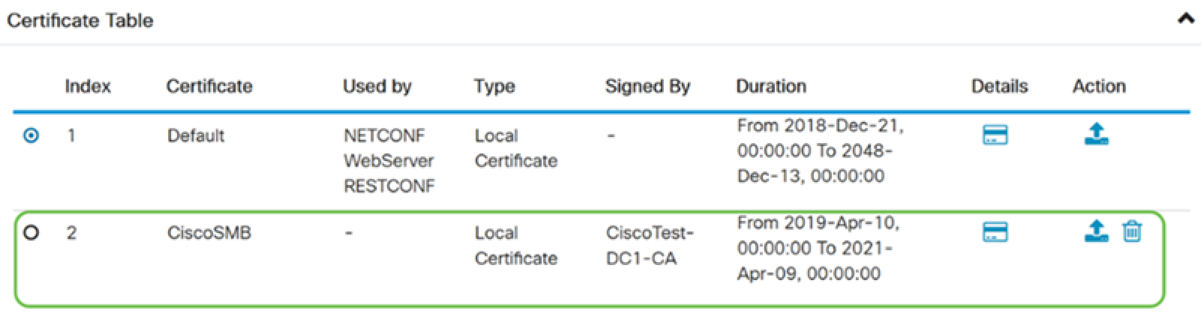
Browse... No file is selected

步骤6.将出现"信息"窗口，告知您证书已成功导入。单击 **OK 继续。**



Import certificate successfully!

步骤7.您应看到证书已上传。



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		
○	2	CiscoSMB	-	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

结论

您应该已成功学习如何在RV160和RV260系列路由器上生成CSR、导入和下载证书。