

# Zertifikat (Import/Export/CSR erstellen) für Router der Serien RV160 und RV260

## Ziel

In diesem Dokument erfahren Sie, wie Sie eine CSR-Anfrage (Certificate Signing Request) erstellen und Zertifikate auf den Routern der Serien RV160 und RV260 importieren und exportieren.

## Einleitung

Digitale Zertifikate sind im Kommunikationsprozess wichtig. Sie ermöglicht die digitale Identifikation für die Authentifizierung. Ein digitales Zertifikat enthält Informationen zur Identifizierung eines Geräts oder Benutzers, z. B. Name, Seriennummer, Firma, Abteilung oder IP-Adresse.

Zertifizierungsstellen (Certificate Authority, CA) sind vertrauenswürdige Behörden, die Zertifikate zur Überprüfung ihrer Authentizität "signieren", was die Identität des Geräts oder Benutzers garantiert. Sie stellt sicher, dass der Zertifikatsinhaber wirklich der ist, der er sein will. Ohne ein vertrauenswürdiges signiertes Zertifikat können Daten verschlüsselt werden, aber die Partei, mit der Sie kommunizieren, ist möglicherweise nicht die, mit der Sie denken. CA verwendet Public Key Infrastructure (PKI) bei der Ausgabe von digitalen Zertifikaten, die die Sicherheit durch Verschlüsselung von öffentlichen oder privaten Schlüsseln gewährleisten. Zertifizierungsstellen sind für die Verwaltung von Zertifikatsanfragen und die Ausstellung digitaler Zertifikate zuständig. Beispiele für CA: IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verisign und vieles mehr.

Zertifikate werden für SSL- (Secure Socket Layer), TLS- (Transport Layer Security), DTLS- (Datagram TLS)-Verbindungen (z. B. Hypertext Transfer Protocol (HTTPS) und LDAPS (Secure Lightweight Directory Access Protocol) verwendet.

## Unterstützte Geräte

- RV160
- RV260

## Software-Version

- 1.0.00.15

## Inhalt

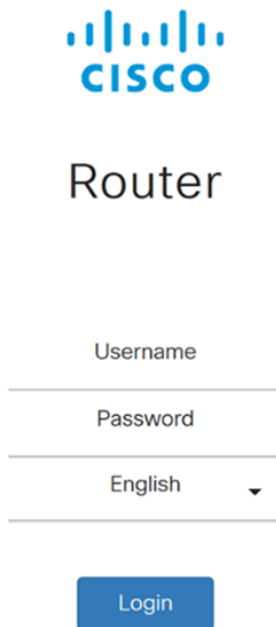
Dieser Artikel enthält folgende Informationen:

1. [CSR/Zertifikat erstellen](#)

2. [Zertifikat anzeigen](#)
3. [Zertifikat exportieren](#)
4. [Zertifikat importieren](#)
5. [Schlussfolgerung](#)

## CSR/Zertifikat erstellen

Schritt 1: Melden Sie sich bei der Webseite für die Konfiguration an.

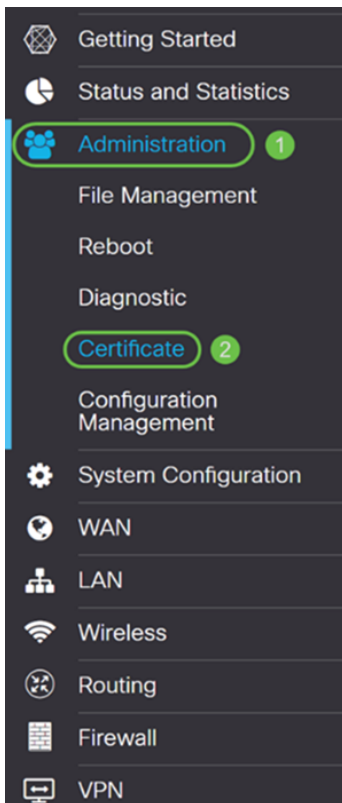


The image shows the Cisco Router login interface. At the top is the Cisco logo, consisting of a stylized bridge icon above the word "CISCO". Below the logo is the word "Router". There are three input fields: "Username", "Password", and "English" (with a dropdown arrow). Below the input fields is a blue "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.

Schritt 2: Navigieren Sie zu **Administration > Certificate**.



Schritt 3: Klicken Sie auf der Seite *Zertifikat* auf die Schaltfläche **CSR/Zertifikat generieren...**

## 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...

Schritt 4: Wählen Sie aus einer der folgenden Optionen in der Dropdown-Liste den zu generierenden Zertifikatstyp aus.

- **Selbstsigniertes Zertifikat** - Dies ist ein SSL-Zertifikat (Secure Socket Layer), das von einem eigenen Ersteller signiert wird. Dieses Zertifikat ist weniger vertrauenswürdig, da es nicht abgebrochen werden kann, wenn der private Schlüssel durch einen Angreifer kompromittiert wird. Sie müssen die gültige Dauer in Tagen angeben.
- **Zertifizierungsstellenzertifikat**: Wählen Sie diesen Zertifikatstyp aus, damit Ihr Router wie eine interne Zertifizierungsstelle fungiert und Zertifikate ausstellt. Im Hinblick auf die Sicherheit ähnelt es einem selbstsignierten Zertifikat. Dies kann für OpenVPN verwendet werden.
- **Certificate Signing Request** - Dies ist eine Public Key Infrastructure (PKI), die an die Zertifizierungsstelle gesendet wird, um ein digitales Identitätszertifikat zu beantragen. Sie ist sicherer als selbstsignierte Schlüssel, da der private Schlüssel geheim gehalten wird. Diese Option wird empfohlen.

• **Zertifikat signiert durch Zertifizierungsstellenzertifikat** - Wählen Sie diesen Zertifikatstyp aus, und geben Sie die entsprechenden Details an, um das Zertifikat von Ihrer internen Zertifizierungsstelle zu signieren.

In diesem Beispiel wählen Sie **Zertifikatssignierungsanfrage**.

Generate CSR/Certificate

Type:

Certificate Name:  ✘  
Please enter a valid name.

Subject Alternative Name:

IP Address  FQDN  Email

Schritt 5: Geben Sie den *Zertifikatsnamen ein*. In diesem Beispiel geben Sie **CertificateTest ein**.

Type:

Certificate Name:

Subject Alternative Name:

IP Address  FQDN  Email

Schritt 6: Wählen Sie im Feld *Subject Alternative Name (Subject Alternative Name)* eine der folgenden Optionen aus: **IP-Adresse**, **FQDN** (Fully Qualified Domain Name) oder **E-Mail** und geben Sie dann den gewünschten Namen aus dem, was Sie ausgewählt haben, ein. In diesem Feld können Sie zusätzliche Hostnamen angeben.

In diesem Beispiel wählen wir **FQDN** und geben **ciscoesupport.com ein**.

Type:

Certificate Name:

Subject Alternative Name:

2  IP Address 1  FQDN  Email

Schritt 7: Wählen Sie ein **Land** aus der Dropdown-Liste *Ländername (C)* aus.

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"/>

Schritt 8: Geben Sie einen **Bundesland-** oder **Provinznamen** in das Feld *Bundesland oder Bundesland* ein.

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"/>

Schritt 9: Geben Sie im *Ortsnamen* einen Ortsnamen ein.

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"/>

Schritt 10: Geben Sie den Namen der **Organisation** im Feld *Organisationsname* ein.

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"/>

Schritt 11: Geben Sie den Namen der **Organisationseinheit** ein (z. B. Schulung, Support usw.).

In diesem Beispiel geben wir **eSupport** als Namen unserer Organisationseinheit ein.

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

Schritt 12: Geben Sie einen **allgemeinen Namen ein**. Der FQDN des Webservers, der dieses Zertifikat empfängt.

In diesem Beispiel wurde **ciscosmbssupport.com** als allgemeiner Name verwendet.

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):	ciscosmbssupport.com
Email Address (E):	
Key Encryption Length:	2048

Schritt 13: Geben Sie eine **E-Mail-Adresse ein**.

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

Schritt 14: Wählen Sie im Dropdown-Menü die **Schlüssellänge für die Verschlüsselung** aus. Folgende Optionen sind verfügbar: **512**, **1024** oder **2048**. Je größer die Schlüssellänge, desto sicherer ist das Zertifikat. Je größer die Schlüssellänge, desto länger dauert die Verarbeitung.

**Best Practice:** Es wird empfohlen, die maximale Schlüssellänge auszuwählen, um eine strengere Verschlüsselung zu ermöglichen.

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

Schritt 15: Klicken Sie auf **Generieren**.



## 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:

Schritt 16: Ein *Information*-Popup wird mit dem Text "Zertifikat erfolgreich generieren!" angezeigt. Nachricht. Klicken Sie auf **OK**, um fortzufahren.

### Information ✕

Generate certificate successfully!

**OK**

Schritt 17: Exportieren Sie die CSR aus der *Zertifikatstabelle*.

Certificate Table <span style="float: right;">▲</span>							
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...

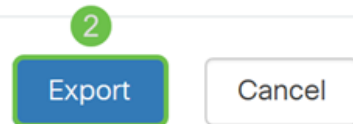
Schritt 18: Ein Fenster *Zertifikat exportieren* wird angezeigt. Wählen Sie **PC** für den *Export in aus* und klicken Sie anschließend auf **Exportieren**.

# Export Certificate



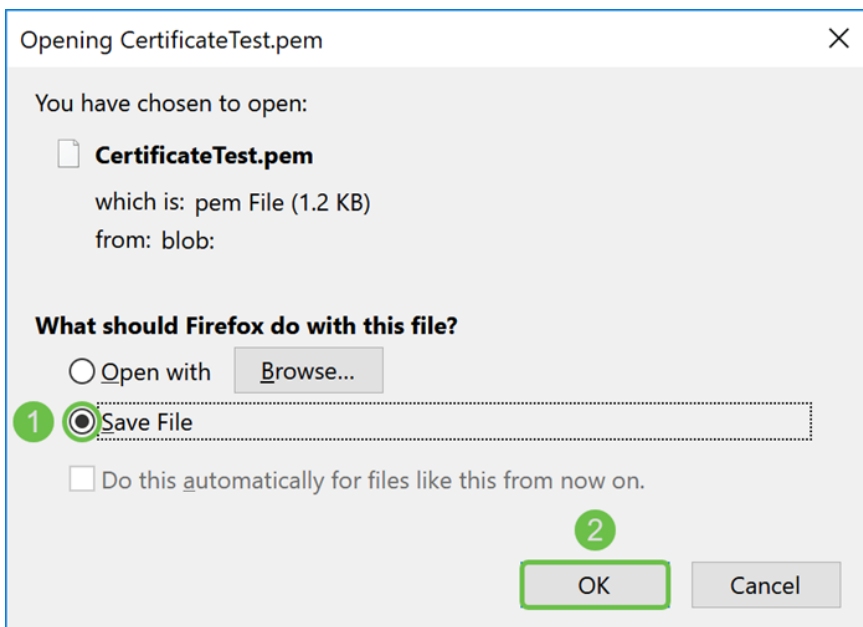
Export as PEM format

Export to:



Schritt 19: Es sollte ein anderes Fenster angezeigt werden, in dem Sie gefragt werden, ob die Datei geöffnet oder gespeichert werden soll.

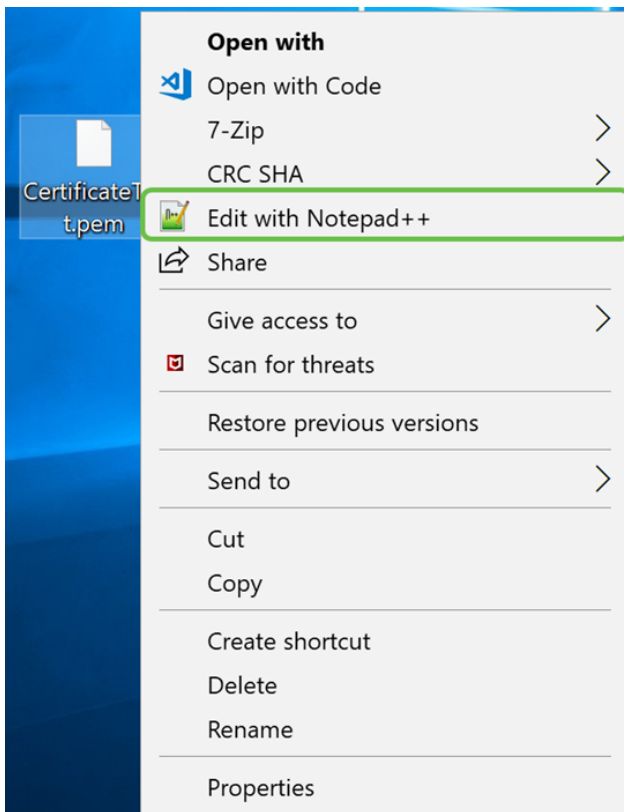
In diesem Beispiel wählen wir **Datei speichern** und klicken dann auf **OK**.



Schritt 20: Suchen Sie den Speicherort der .pem-Datei. Klicken Sie mit der **rechten Maustaste** auf die .pem-Datei, und öffnen Sie sie mit dem bevorzugten Text-Editor.

In diesem Beispiel öffnen wir die .pem-Datei mit Notepad++.

**Anmerkung:** Sie können es auch mit Notepad öffnen.



Schritt 21: Stellen Sie sicher, dass die - **BEGINNUNGSZERTIFIKATANFORDERUNG** und - **ENDZERTIFIKATANFORDERUNG** - sich in der eigenen Zeile befindet.

**Anmerkung:** Einige Teile des Zertifikats waren verschwommen.

```



CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwWIU2FuIEpvc2UxDjAMBGNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY2lzY29zbWJzdXBwb3J0
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXplu
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LAFOLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv
9 soTqNBrYqR8h46NHh0J5fMXDsPY1j2LWmS1VbkskoiMdr5SZlwmhkrqgLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAACBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BAIw
13 MCcGA1UdJQogMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY21zY29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAILUeIUy
15 TqFZ2wQx3r29E1SWOU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16
17
18
19
20
21 -----END CERTIFICATE REQUEST----- 2
22

```

Schritt 22: Wenn Sie Ihren CSR haben, müssten Sie zu Ihren Hosting-Diensten oder einer Zertifizierungsstelle-Website (z. B. GoDaddy, Verisign usw.) gehen und ein Zertifikat anfordern. Sobald Sie eine Anfrage gesendet haben, wird diese mit dem Zertifikatsserver kommunizieren, um sicherzustellen, dass kein Grund besteht, das Zertifikat nicht auszustellen.







**Anmerkung:** Wenn Sie nicht wissen, wo sich die Zertifikatsanforderung auf der Website befindet, wenden Sie sich an die Zertifizierungsstelle oder den Support für die Hosting-Site.

Schritt 23: Laden Sie das Zertifikat herunter, sobald es abgeschlossen ist. Es sollte sich um eine **.cer**- oder **.crt**-Datei handeln. In diesem Beispiel wurden beide Dateien bereitgestellt.

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

Schritt 24: Gehen Sie zurück zur Seite *Zertifikat* Ihres Routers, und importieren Sie die Zertifikatsdatei, indem Sie auf den **Pfeil** klicken, **der auf das Symbol Gerät zeigt**.

#### 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	-	-		  

Schritt 25: Geben Sie im Feld *Zertifikatsname* den **Zertifikatsnamen ein**. Der Name darf nicht mit dem Namen der Zertifikatssignierungsanfrage übereinstimmen. Wählen Sie im Abschnitt *Zertifikatsdatei hochladen* die Option **Importieren aus PC aus**, und klicken Sie auf **Durchsuchen...**, um die Zertifikatsdatei hochzuladen.

### Import Signed-Certificate

Type: Local Certificate

Certificate Name:  1

#### Upload Certificate file

2

Import from PC

3

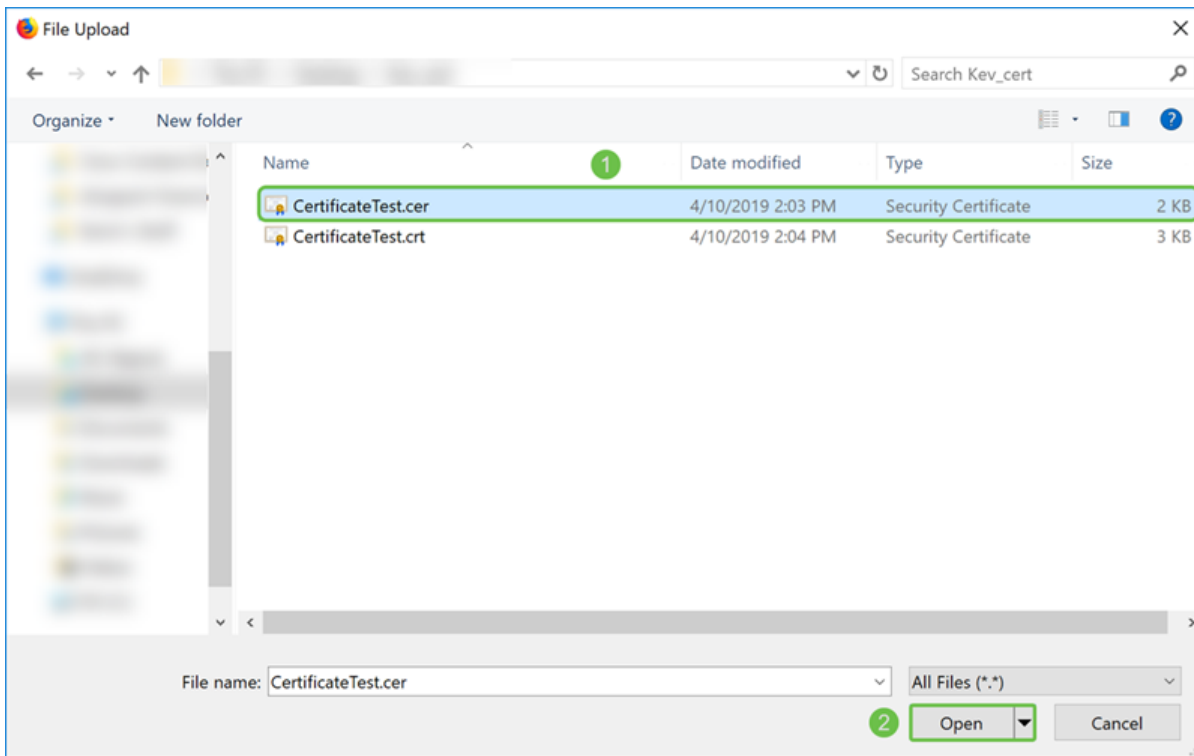
No file is selected

Import from USB



No file is selected

Schritt 26: Ein Fenster *Datei-Upload* wird angezeigt. Navigieren Sie zum Speicherort der Zertifikatsdatei. Wählen Sie die **Zertifikatsdatei**, die Sie hochladen möchten, und klicken Sie auf **Öffnen**. In diesem Beispiel wurde **CertificateTest.cer** ausgewählt.



Schritt 27: Klicken Sie auf die Schaltfläche **Hochladen**, um das Hochladen Ihres Zertifikats zum Router zu starten.

**Anmerkung:** Wenn Sie eine Fehlermeldung erhalten, bei der Sie Ihre .cer-Datei nicht hochladen können, kann dies daran liegen, dass Ihr Router das Zertifikat als Spam-Kodierung benötigt. Sie müssen die Codierung (.cer Dateierweiterung) in eine Paketcodierung (.crt Dateierweiterung) konvertieren.

## Import Signed-Certificate ✕

Type: Local Certificate

Certificate Name:

### Upload Certificate file

Import from PC

CertificateTest.cer

Import from USB



No file is selected






Schritt 28: Wenn der Import erfolgreich war, sollte ein *Informationsfenster* angezeigt werden, das Sie darüber informiert, dass der Import erfolgreich war. Klicken Sie auf **OK**, um fortzufahren.

 Import certificate successfully!

OK

Schritt 29: Ihr Zertifikat sollte erfolgreich aktualisiert werden. Sie sollten sehen können, von wem Ihr Zertifikat signiert wurde. In diesem Beispiel sehen wir, dass unser Zertifikat von *CiscoTest-DC1-CA* signiert wurde. Wenn Sie das Zertifikat als unser primäres Zertifikat festlegen möchten, wählen Sie das Zertifikat mithilfe des Optionsfelds links aus, und klicken Sie auf die Schaltfläche **Als primäres Zertifikat auswählen...**

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		 

**1**  **2**

**2**

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

**Anmerkung:** Wenn Sie das primäre Zertifikat ändern, gelangen Sie zurück zu einer Warnseite. Wenn Sie Firefox verwenden und es als graue leere Seite angezeigt wird, müssten Sie die Konfiguration auf Ihrem Firefox anpassen. Dieses Dokument über das Mozilla Wiki bietet einige Erläuterungen dazu: [CA/AddRootToFirefox](#). Um die Warnungsseite erneut sehen zu können, [folgen](#) Sie [diesen Schritten, die auf der Support-Seite der Mozilla-Community gefunden wurden](#).

Schritt 30: Klicken Sie auf der Firefox-Warnseite auf **Erweitert ...** und **akzeptieren Sie das Risiko und fahren Sie fort**, um zum Router zurückzukehren.

**Anmerkung:** Diese Warnbildschirme unterscheiden sich je nach Browser, führen aber die gleichen Funktionen aus.



## 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

Schritt 31: In der Zertifikatstabelle sollten Sie sehen, dass NETCONF, *WebServer* und *RESTCONF* auf das neue Zertifikat ausgetauscht wurden, anstatt das *Default*-Zertifikat zu verwenden.

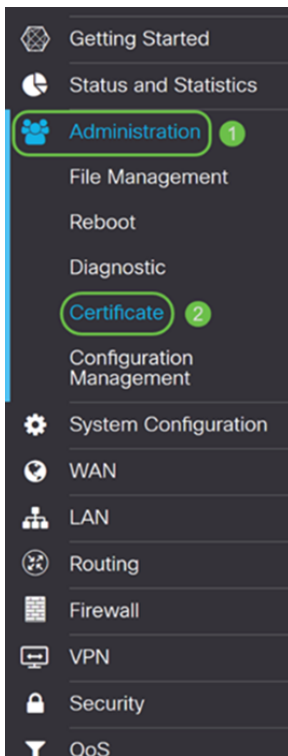
Certificate Table

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		

Sie sollten jetzt erfolgreich ein Zertifikat auf Ihrem Router installiert haben.






## Zertifikat anzeigen

Schritt 1: Wenn Sie von der Seite *Zertifikat* weg navigiert haben, wechseln Sie zu **Administration > Certificate**.



Schritt 2: Klicken Sie in der *Zertifikatstabelle* auf das **Details**-Symbol im Abschnitt *Details*.

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		 

Schritt 3: Die Seite *Zertifikatdetails* wird angezeigt. Sie sollten alle Informationen zu Ihrem Zertifikat anzeigen können.



## 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

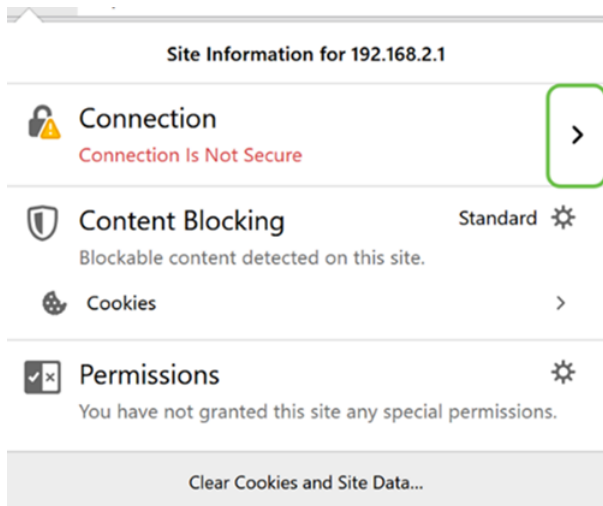
Close

Schritt 4: Klicken Sie auf das **Sperrsymbol** auf der linken Seite der Leiste Uniform Resource Locator (URL).

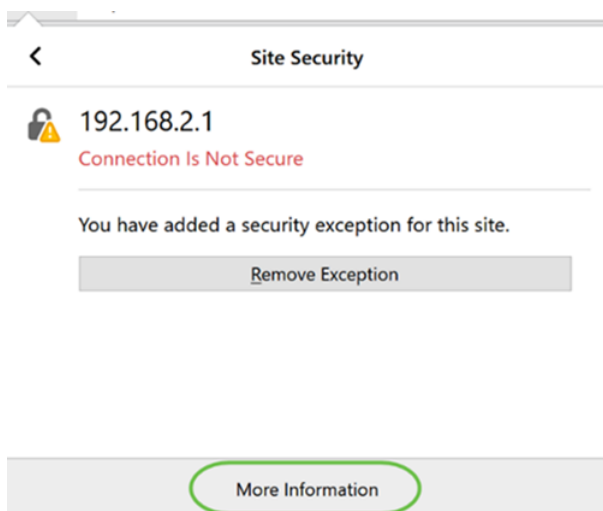
**Anmerkung:** Die folgenden Schritte werden in einem Firefox-Browser verwendet.

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		

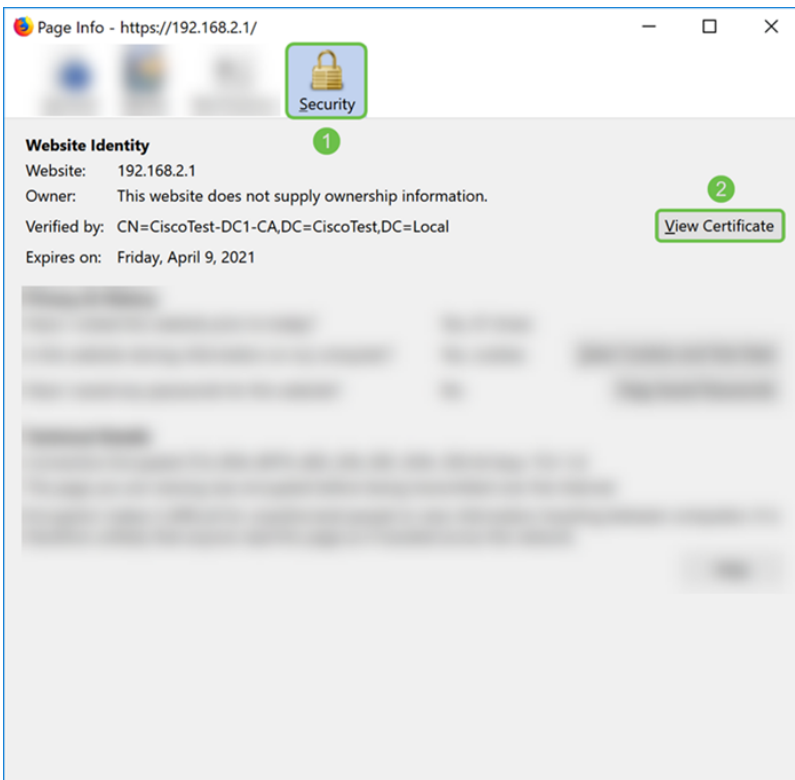
Schritt 5: Eine Dropdown-Liste mit Auswahlmöglichkeiten wird angezeigt. Klicken Sie auf das **Pfeilsymbol** neben dem Feld *Verbindung*.



Schritt 6: Klicken Sie auf **Weitere Informationen**.

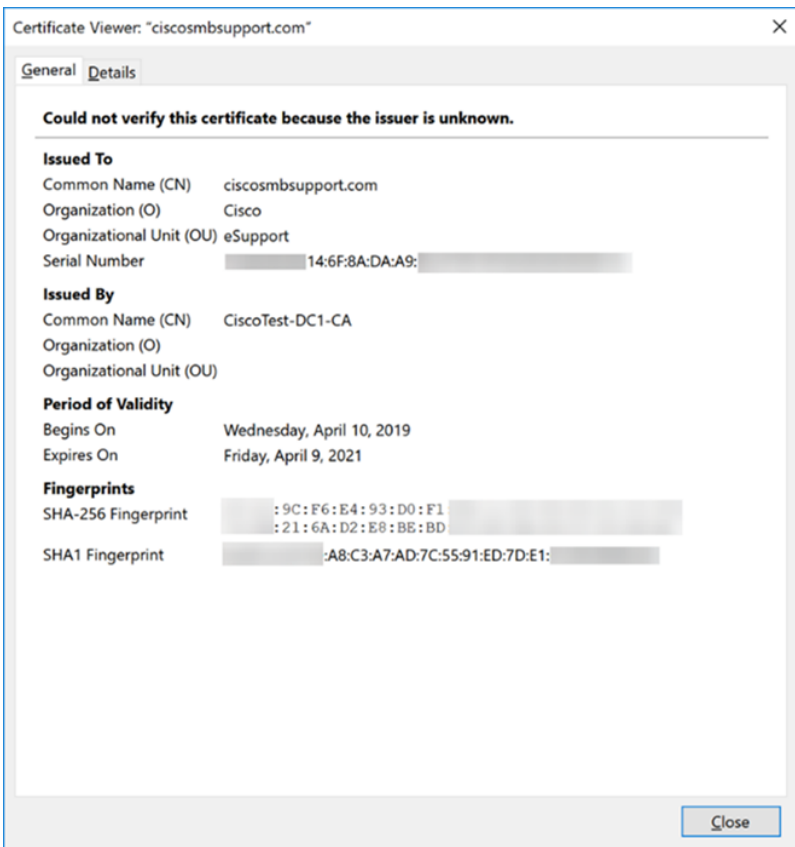


Schritt 7: Im Bereich *Seiteninfo* sollten Sie im Abschnitt *Website-Identität* kurze Informationen zu Ihrem Zertifikat sehen können. Vergewissern Sie sich, dass Sie sich auf der Registerkarte **Sicherheit** befinden, und klicken Sie dann auf **Zertifikat anzeigen**, um weitere Informationen zu Ihrem Zertifikat anzuzeigen.



Schritt 8: Die Seite *Certificate Viewer* sollte angezeigt werden. Sie sollten alle Informationen über Ihr Zertifikat, die Gültigkeitsdauer, die Fingerabdrücke und die Person, von der es ausgestellt wurde, einsehen können.

**Anmerkung:** Da dieses Zertifikat von unserem Testzertifikatserver ausgestellt wurde, ist der Aussteller unbekannt.



## Zertifikat exportieren

So laden Sie Ihr Zertifikat herunter, um es auf einen anderen Router zu importieren:

Schritt 1: Klicken Sie auf der Seite *Zertifikat* auf das **Exportsymbol** neben dem Zertifikat, das Sie exportieren möchten.

#### 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		

Schritt 2: Ein *Exportzertifikat* wird angezeigt. Wählen Sie ein Format für den Export des Zertifikats aus. Folgende Optionen sind verfügbar:

- **PKCS#12** - Public Key Cryptography Standards (PKCS) #12 ist ein exportiertes Zertifikat, das in der Erweiterung .p12 enthalten ist. Um die Datei zu verschlüsseln, wird ein Kennwort benötigt, um sie beim Exportieren, Importieren und Löschen zu schützen.
- **PEM** - Privacy Enhanced Mail (PEM) wird häufig für Webserver verwendet, damit diese mithilfe eines einfachen Texteditors wie Notepad leicht in lesbare Daten übersetzt werden können.

Wählen Sie **Als PKCS#12-Format exportieren aus**, geben Sie ein **Kennwort ein** und **bestätigen Sie das Kennwort**. Wählen Sie anschließend **PC** als *Exportieren in:* feld. Klicken Sie auf **Exportieren**, um das Zertifikat auf Ihren Computer zu exportieren.

**Anmerkung:** Denken Sie daran, dass dieses Kennwort beim Importieren in einen Router verwendet wird.

## Export Certificate

1

Export as PKCS#12 format

Enter Password:

2

Confirm Password:

Export as PEM format

Export to:

3

PC  USB



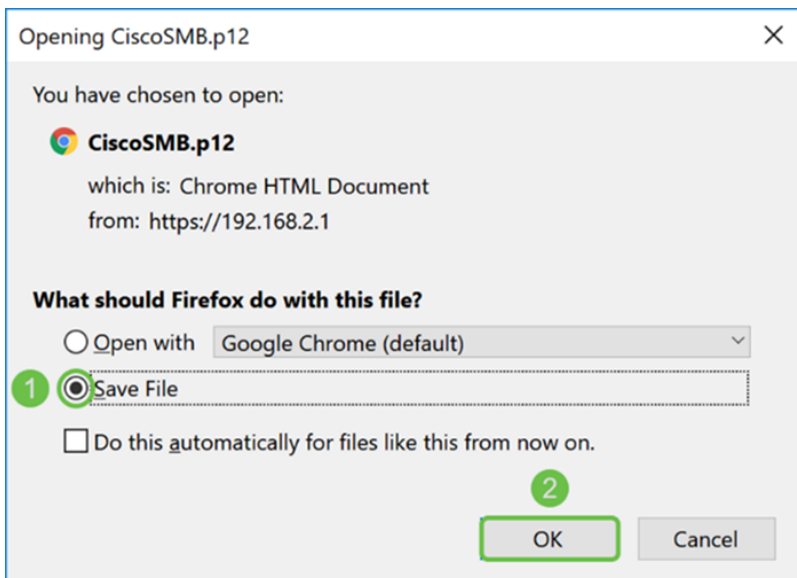
4

Export

Cancel

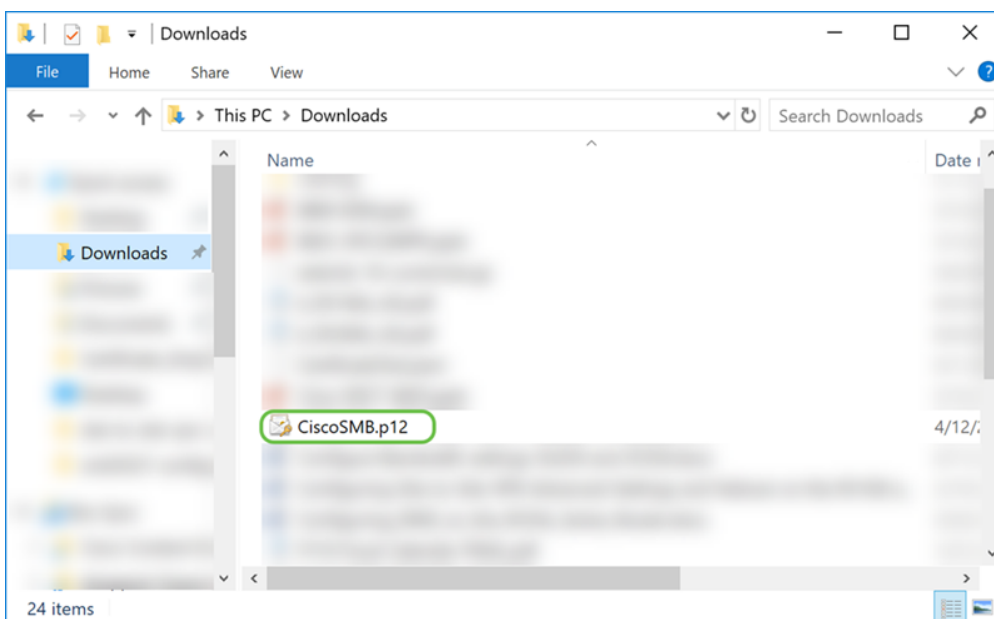
Schritt 3: Es erscheint ein Fenster mit der Frage, was Sie mit dieser Datei machen sollten. In

diesem Beispiel wählen wir **Datei speichern** und klicken dann auf **OK**.



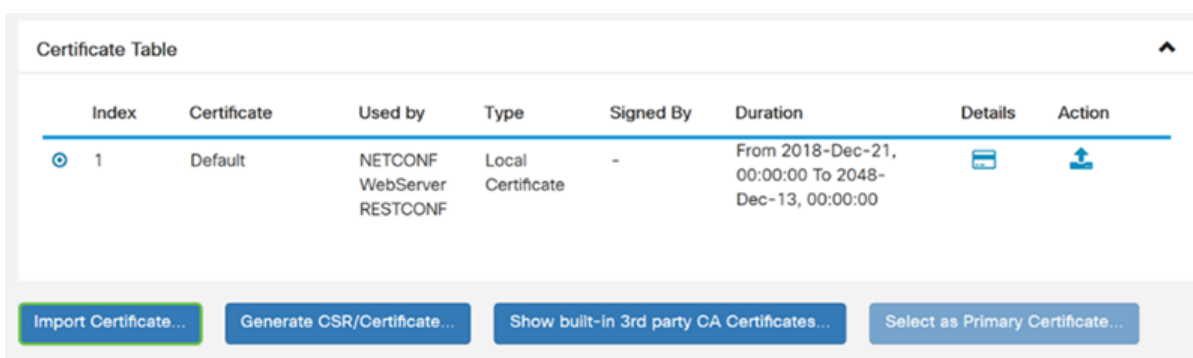
Schritt 4: Die Datei sollte im Standardspeicherort gespeichert werden.

In unserem Beispiel wurde die Datei im Ordner *Downloads* auf unserem Computer gespeichert.



## Zertifikat importieren

Schritt 1: Klicken Sie auf der Seite *Zertifikat* auf die Schaltfläche **Zertifikat importieren...**



Schritt 2: Wählen Sie den **Zertifikatstyp** aus der Dropdown-Liste *Typ* im Abschnitt *Zertifikat*

*importieren aus*. Die Optionen sind wie folgt definiert:

• **Zertifizierungsstellenzertifikat** - Ein Zertifikat, das von einer vertrauenswürdigen Behörde eines Drittanbieters zertifiziert wurde, die bestätigt hat, dass die im Zertifikat enthaltenen Informationen korrekt sind.

**Zertifikat für lokales Gerät** - Ein auf dem Router generiertes Zertifikat.

• **PKCS#12 Encoded File** - Public Key Cryptography Standards (PKCS) #12 ist ein exportiertes Zertifikat, das in der Erweiterung .p12 enthalten ist.

In diesem Beispiel wurde **PKCS#12 Encoded File** als Typ ausgewählt. Geben Sie einen **Namen** für das Zertifikat ein, und geben Sie dann das **Kennwort** ein, das verwendet wurde.

Import Certificate

Type: PKCS#12 Encoded File 1


Certificate Name: CiscoSMB 2

Import Password: ●●●●●●●●●● 3

Upload Certificate file

Import from PC

Browse... No file is selected

Import from USB 

Browse... No file is selected

Schritt 3: Wählen Sie im Abschnitt *Zertifikatsdatei hochladen* entweder **Importieren vom PC** oder **Importieren aus USB**. In diesem Beispiel wurde **Import von PC** ausgewählt. Klicken Sie auf **Durchsuchen...**, um eine Datei zum Hochladen auszuwählen.

### Import Certificate

Type:


Certificate Name:

Import Password:

### Upload Certificate file

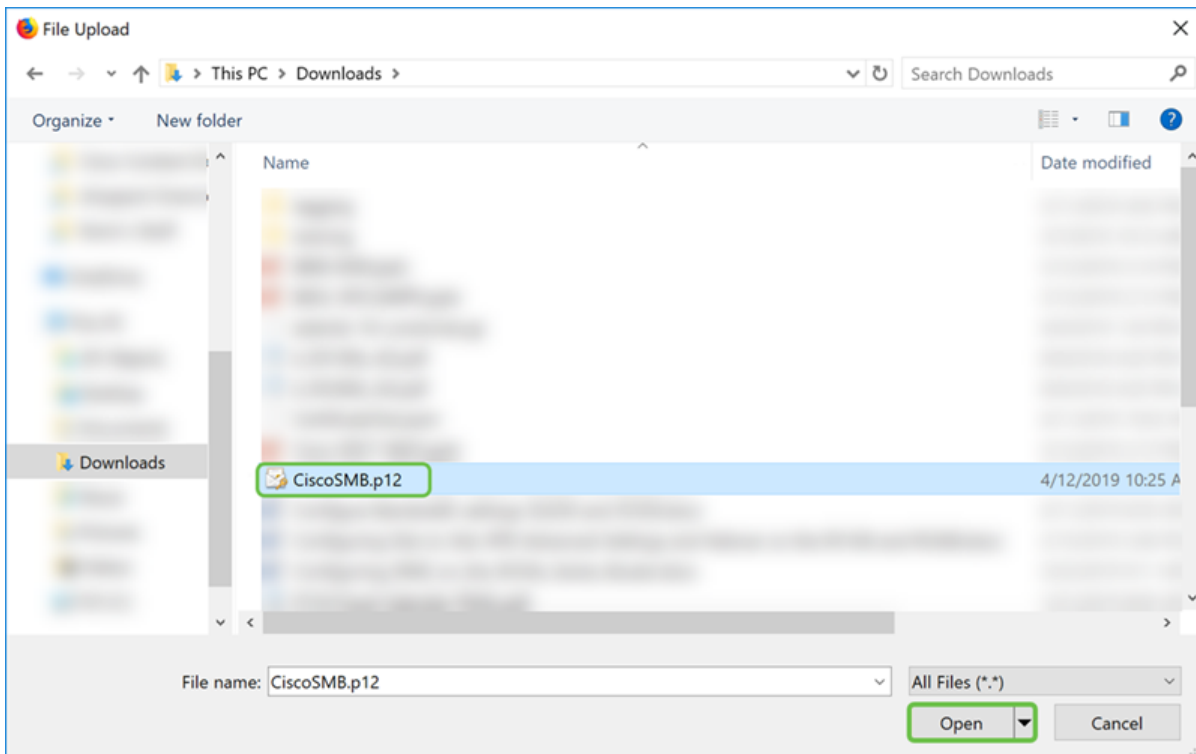
Import from PC

No file is selected

Import from USB 

No file is selected

Schritt 4: Navigieren Sie im Fenster *File Upload* (Datei hochladen) zu dem Speicherort, an dem sich die PKCS#12 Encoded File (Dateierweiterung .p12) befindet. Wählen Sie die Datei **.p12** aus und klicken Sie dann auf **Öffnen**.



Schritt 5: Klicken Sie auf **Hochladen**, um das Hochladen des Zertifikats zu starten.

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

Schritt 6: Ein *Informationsfenster* wird angezeigt, in dem Sie wissen, dass das Zertifikat erfolgreich importiert wurde. Klicken Sie auf **OK**, um fortzufahren.

Information
✕

---

i
Import certificate successfully!

OK

Schritt 7: Sie sollten sehen, dass Ihr Zertifikat hochgeladen wurde.

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		

## Schlussfolgerung

Sie sollten gelernt haben, wie Sie ein CSR-Zertifikat generieren, importieren und ein Zertifikat auf den Routern der Serien RV160 und RV260 herunterladen.