

# دليل (CSR) عاشن إاري دصت/داري ت سا) ة داهش ل ا RV260 و RV160 ة لس لس ل ا ن م ه ج و م

## الهدف

الهدف من هذا المستند هو توضيح كيفية إنشاء طلب توقيع شهادة (CSR) بالإضافة إلى إستيراد وتصدير الشهادات على موجّهات السلسلتين RV160 و RV260.

## المقدمة

إن الشهادات الرقمية مهمة في عملية التواصل. وهو يوفر الهوية الرقمية للمصادقة. تحتوي الشهادة الرقمية على معلومات تعرف جهازا أو مستخدما، مثل الاسم أو الرقم التسلسلي أو الشركة أو القسم أو عنوان IP.

المراجع المصدقة (CA) هي سلطات موثوق بها "توقع" شهادات للتحقق من أصالتها، مما يضمن هوية الجهاز أو المستخدم. فهي تضمن أن صاحب الشهادة هو فعلا من يدعون أنه هو. بدون شهادة موقعة موثوق بها، قد يتم تشفير البيانات، ولكن الطرف الذي تتواصل معه قد لا يكون الشخص الذي تعتقد. يستخدم CA البنية الأساسية للمفتاح العام (PKI) عند إصدار الشهادات الرقمية، والتي تستخدم تشفير المفتاح العام أو المفتاح الخاص لضمان الأمان. يكون CAs مسؤولا عن إدارة طلبات الشهادات وإصدار الشهادات الرقمية. بعض الأمثلة ل CA هي: IdenTrust، Comodo، GoDaddy، GlobalSign، GeoTrust، Verisign وغيرها الكثير.

يتم إستخدام الشهادات لطبقة مأخذ التوصيل الآمنة (SSL) وأمان طبقة النقل (TLS) واتصالات TLS لمخطط البيانات (DTLS)، مثل بروتوكول نقل النص التشعبي (HTTPS) وبروتوكول الوصول الآمن الخفيف للدليل (LDAP).

## الأجهزة القابلة للتطبيق

RV160 .

RV260 .

## إصدار البرامج

1.0.00.15•

## جدول المحتويات

من خلال هذه المقالة، سوف:

1. [إنشاء CSR/شهادة](#)

2. [عرض الشهادة](#)

3. [تصدير الشهادة](#)

4. [إستيراد الشهادة](#)

## إنشاء CSR/شهادة

الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب.



### Router

Username

Password

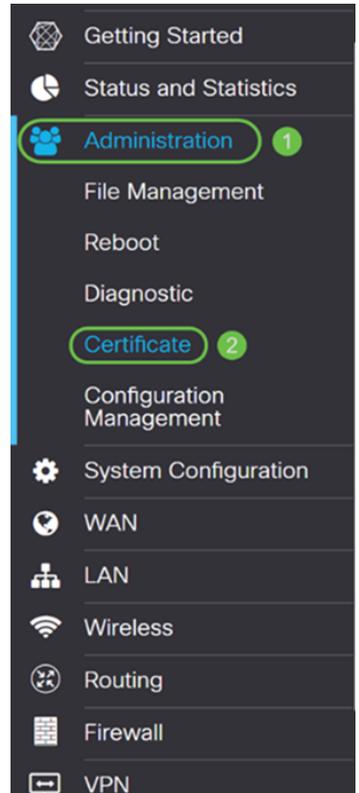
English

Login

©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.

الخطوة 2. انتقل إلى إدارة < شهادة.



الخطوة 3. في صفحة الشهادة، انقر على زر إنشاء 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...

الخطوة 4. حدد نوع الشهادة التي سيتم إنشاؤها من أحد الخيارات التالية في القائمة المنسدلة.

• **شهادة موقعة ذاتيا** - هذه هي شهادة طبقة مأخذ التوصيل الآمنة (SSL) الموقعة من قبل منشئها. تكون هذه الشهادة أقل ثقة، حيث لا يمكن إلغاؤها إذا تم اختراق المفتاح الخاص بطريقة ما من قبل المهاجم. يجب توفير المدة الصحيحة بالأيام.

• **شهادة CA** - حدد نوع الشهادة هذا لتجعل الموجه يعمل كمرجع شهادات داخلي وبصدر الشهادات. من وجهة نظر أمنية، فإنه يشبه الشهادة الموقعة ذاتيا. يمكن استخدام هذا ل OpenVPN.

• **طلب توقيع الشهادة** - هذه هي البنية الأساسية للمفتاح العام (PKI) التي يتم إرسالها إلى المرجع المصدق لتقديم طلب لشهادة الهوية الرقمية. إنه أكثر أمانا من التوقيع الذاتي نظرا لأنه يتم الاحتفاظ بالمفتاح الخاص سرا. يوصى بهذا الخيار.

• **الشهادة الموقعة من قبل شهادة CA** - حدد نوع الشهادة هذا وقدم التفاصيل ذات الصلة للحصول على الشهادة الموقعة من قبل مرجع الشهادة الداخلي الخاص بك.

في هذا المثال، سنقوم بتحديد **طلب توقيع الشهادة**.

### Generate CSR/Certificate

Type:

Certificate Name:  ✘  
Please enter a valid name.

Subject Alternative Name:

IP Address  FQDN  Email

الخطوة 5. أدخل اسم الشهادة. في هذا المثال، سنقوم بإدخال **CertificateTest**.

Type:

Certificate Name:

Subject Alternative Name:

IP Address  FQDN  Email

الخطوة 6. في حقل الاسم البديل للموضوع، حدد واحدا مما يلي: **عنوان IP**، أو **FQDN** (اسم المجال المؤهل

بالكامل)، أو البريد الإلكتروني ثم أدخل الاسم المناسب من ما قمت بتحديدته. يتيح لك هذا الحقل تحديد أسماء مضيف إضافية.

في هذا المثال، سنقوم بتحديد FQDN وإدخال CiscoSupportPort.com.

Type:	<input type="text" value="Certificate Signing Request"/>
Certificate Name:	<input type="text" value="CertificateTest"/>
Subject Alternative Name:	<input type="text" value="ciscoesupport.com"/>
	<input type="radio"/> IP Address <input checked="" type="radio"/> FQDN <input type="radio"/> Email

الخطوة 7. حدد دولة من القائمة المنسدلة اسم البلد (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"/>

الخطوة 8. أدخل اسم ولاية أو مقاطعة في حقل اسم الولاية أو المقاطعة.

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"/>

الخطوة 9. دخلت في المحلي إسم، مدينة إسم.

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"/>

الخطوة 10. أدخل اسم المؤسسة في حقل اسم المؤسسة.

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"/>

الخطوة 11. أدخل اسم الوحدة التنظيمية (أي التدريب والدعم، وما إلى ذلك).

في هذا المثال، سنقوم بإدخال خدمة الدعم الإلكتروني كاسم لوحدة المؤسسة.

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

الخطوة 12. أدخل اسما عاما. إن FQDN الخاص بخادم ويب هو الذي سيتلقى هذه الشهادة.

في هذا المثال، تم استخدام ciscosmbsupport.com كاسم عام.

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

الخطوة 13. أدخل عنوان بريد إلكتروني.

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

الخطوة 14. حدد طول تشفير المفاتيح من القائمة المنسدلة. الخيارات هي: 512، 1024، أو 2048. كلما زاد حجم المفتاح، زاد تأمين الشهادة. كلما كبر حجم المفتاح، كلما زاد وقت المعالجة.

أفضل الممارسات: يوصى باختيار أعلى طول تشفير للمفتاح - مما يتيح تشفيراً أكثر صرامة.

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

الخطوة 15. طقطقة يلد.

## 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:

الخطوة 16. ستظهر قائمة معلومات منبثقة مع رسالة "إنشاء شهادة بنجاح!". انقر فوق موافق للمتابعة.

### Information

 Generate certificate successfully!

[OK](#)

الخطوة 17. تصدير CSR من جدول الشهادات.

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...](#)

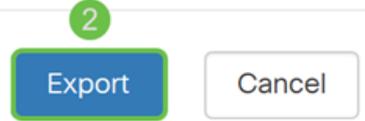
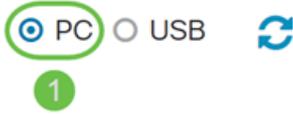
الخطوة 18. تظهر نافذة تصدير الشهادات. حدد كمبيوتر شخصي ل التصدير إلى ثم انقر فوق تصدير.

# Export Certificate



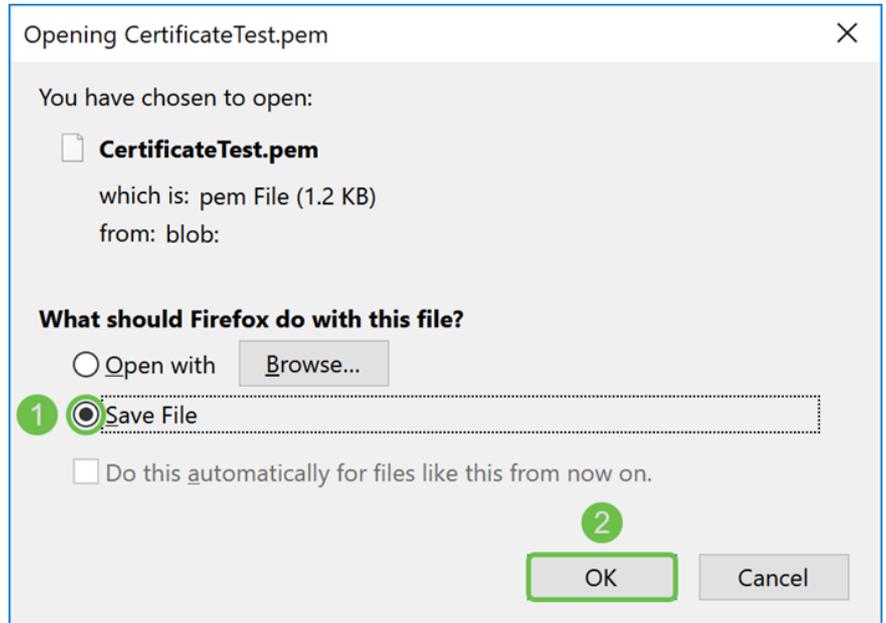
Export as PEM format

Export to:



الخطوة 19. يجب أن تظهر نافذة أخرى تسأل ما إذا كان سيتم فتح الملف أو حفظه.

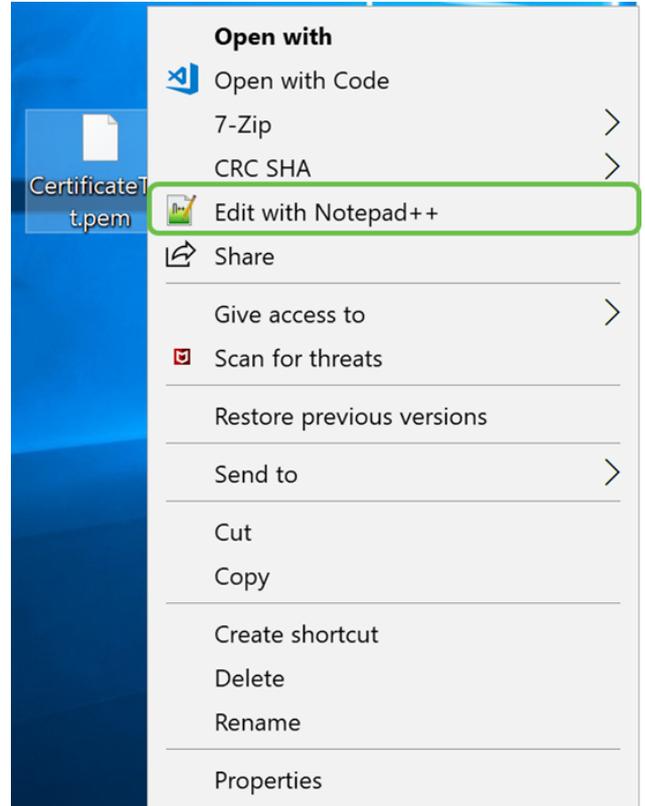
في هذا المثال، سنقوم بتحديد **حفظ الملف** ثم انقر فوق **موافق**.



الخطوة 20. العثور على موقع حفظ ملف pem. انقر بزر الماوس الأيمن على ملف pem. وافتحه باستخدام محرر النصوص المفضل لديك.

في هذا المثال، سنقوم بفتح ملف pem باستخدام Notepad++.

**ملاحظة:** لا تتردد في فتحه باستخدام Notepad.



الخطوة 21. تأكد من أن **بدء طلب الشهادة** — و**نهاية طلب الشهادة** — في السطر الخاص به.

**ملاحظة:** كانت بعض أجزاء الشهادة غير واضحة.

```

CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 VBAYTA1VTMQswCQYDVQQIDAJDQTERMA8GA1UE
3 BwwIU2FuIEpvc2UxDjAMBgNVBAoMBUNpc2NvMREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwwTY21zY29zbWJzdXBwb3J0
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXp1u
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LafOLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv
9 soTqNBrYqR8h46NHh0J5fMXDsPY1j2LWmS1VbkskoiMdr5SZlwmhkrqqLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDi1mpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAaCBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BAIw.gXg
13 MCcGA1UdJQqgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY21zY29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAI1UeIUy
15 TqFZ2wQx3r29E1SWOU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16
17
18
19
20
21 -----END CERTIFICATE REQUEST----- 2
22

```

الخطوة 22. عندما يكون لديك CSR الخاص بك، ستحتاج إلى الانتقال إلى خدمات الاستضافة الخاصة بك أو إلى موقع مرجع شهادات (مثل GoDaddy و Verisign وما إلى ذلك) وطلب شهادة. بمجرد أن تقوم بإرسال طلب، فإنه يتصل بخادم الشهادات للتأكد من عدم وجود أي سبب لعدم إصدار الشهادة.

**ملاحظة:** اتصل ب CA أو دعم الموقع المضيف إذا لم تكن تعرف أين طلب الشهادة في موقعهم.

الخطوة 23. قم بتنزيل الشهادة بمجرد اكتمالها. يجب أن يكون إما **cer** أو **crt** مبرد. في هذا المثال، تم تزويدنا بكلا الملفين.

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

الخطوة 24. عد إلى صفحة الشهادة في الموجه الخاص بك واستورد ملف الترخيص بالنقر على السهم المشير إلى أيقونة الجهاز.

#### 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	-	-		

الخطوة 25. في حقل اسم الشهادة، أدخل اسم الشهادة. لا يمكن أن يكون نفس اسم طلب توقيع الشهادة. في قسم تحميل ملف الشهادة، حدد إستيراد من الكمبيوتر الشخصي وانقر فوق إستعراض... لتحميل ملف شهادتك.

#### Import Signed-Certificate

Type: Local Certificate

Certificate Name: CiscoSMB

#### Upload Certificate file

2

Import from PC

3

Browse...

No file is selected

Import from USB



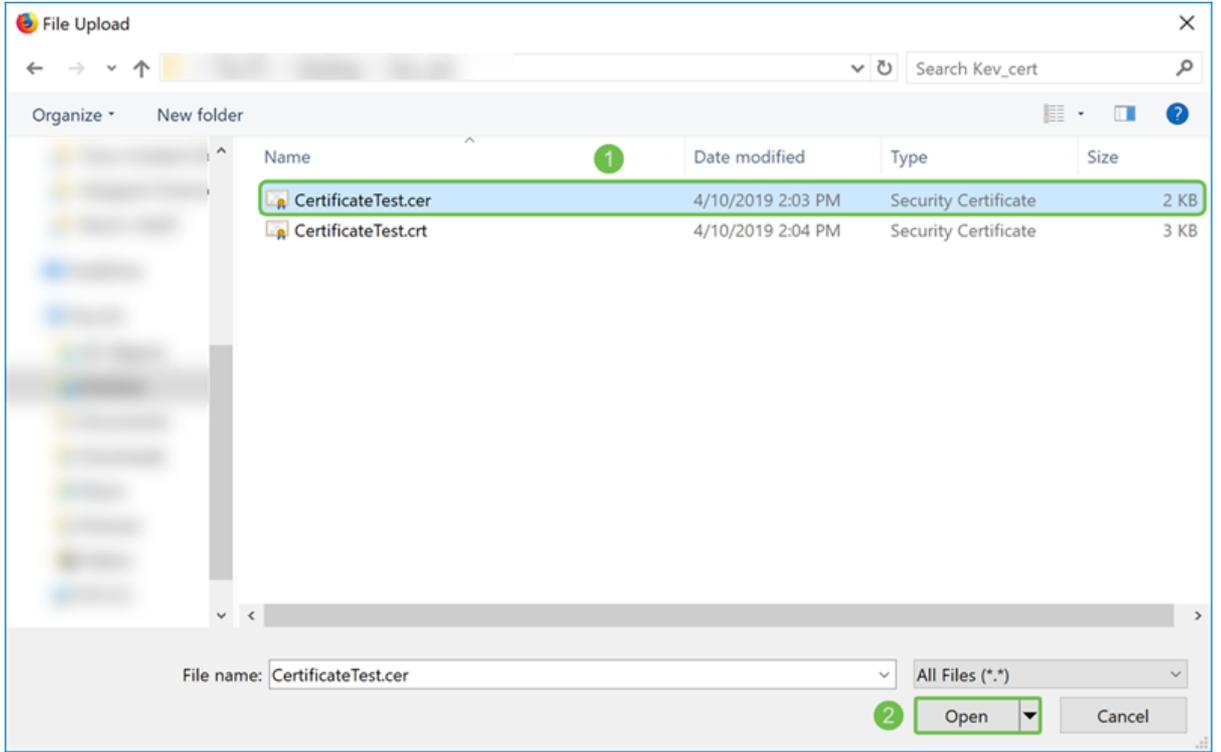
Browse...

No file is selected

Upload

Cancel

الخطوة 26. تظهر نافذة تحميل ملف. انتقل إلى موقع ملف الشهادة الخاص بك. حدد ملف الشهادة الذي تريد تحميله وانقر فوق فتح. في هذا المثال، تم تحديد CertificateTest.cer.



الخطوة 27. انقر على زر التحميل لبدء تحميل شهادتك إلى الموجه.

**ملاحظة:** إذا حدث خطأ لا يمكنك من خلاله تحميل ملف cer الخاص بك، فقد يحدث ذلك لأن الموجه الخاص بك يطلب أن تكون الشهادة في ترميز PEM. ستحتاج إلى تحويل ترميز جهاز التشفير الخاص بك (cer file extension)، إلى ترميز بيم (crt file extension).

## 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

الخطوة 28. في حالة نجاح عملية الاستيراد، يجب أن تظهر نافذة معلومات تسمح لك بإعلامك بأنها ناجحة. انقر فوق موافق للمتابعة.

## Information

 Import certificate successfully!

OK

الخطوة 29. يجب تحديث شهادتك بنجاح. يجب أن تكون قادرا على معرفة من تم توقيع شهادتك. في هذا المثال، يمكننا أن نرى أن شهادتنا تم توقيعها بواسطة *CiscoTest-DC1-CA*. لجعل الشهادة الشهادة الأساسية، حدد الشهادة باستخدام زر الخيار الموجود على الجانب الأيسر وانقر على زر تحديد كشهادة أساسية...

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		 

Import Certificate...

Generate CSR/Certificate...

Show built-in 3rd party CA Certificates...

Select as Primary Certificate...

**ملاحظة:** قد يؤدي تغيير الشهادة الأساسية إلى إعادتك إلى صفحة التحذير. إذا كنت تستخدم Firefox وتظهر كصفحة فارغة رمادية، ستحتاج إلى ضبط بعض التهيئة على Firefox لديك. هذه الوثيقة على موقع موزيلا تعطي بعض الإيضاحات عنها: [CA/AddRootToFirefox](#). لكي تتمكن من رؤية صفحة التحذير مرة أخرى، [اتبع هذه الخطوات التي تم العثور عليها في صفحة دعم مجتمع موزيلا](#).

الخطوة 30. في صفحة التحذير الخاصة ب Firefox، انقر فوق خيارات متقدمة... ثم اقبل المخاطرة واستمر في الرجوع إلى الموجه.

**ملاحظة:** تختلف شاشة التحذيرات تلك من متصفح إلى متصفح إلى آخر ولكنها تقوم بنفس الوظائف.



## 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

الخطوة 31. في جدول الشهادات، يجب أن ترى أن *WebServer*، *NetConf*، و *RESTCONF* قد استبدلت شهادتك الجديدة بدلا من استخدام الشهادة الافتراضية.

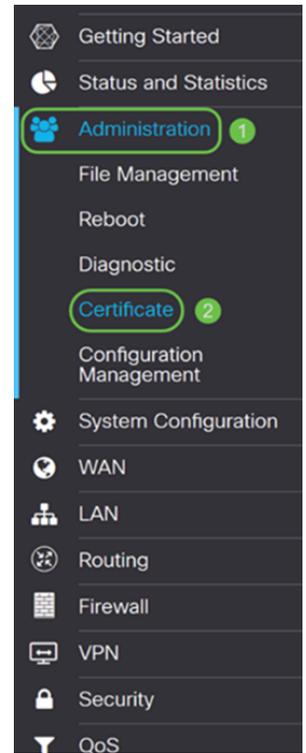
Certificate Table

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		

يجب أن تكون قد انتهيت الآن من تثبيت شهادة بنجاح على الموجه الخاص بك.

## عرض الشهادة

الخطوة 1. إذا كنت قد انتقلت من صفحة الترخيص، انتقل إلى إدارة < ترخيص.



الخطوة 2. في جدول الترخيص، انقر على أيقونة التفاصيل الموجودة تحت قسم التفاصيل.

#### 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		

الخطوة 3. سوف تظهر صفحة تفاصيل الشهادة. يجب أن تكون قادرا على رؤية كافة المعلومات حول شهادتك.

#### 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

الخطوة 4. انقر فوق رمز القفل الموجود على الجانب الأيسر من شريط محدد موقع الموارد الموحد (URL).

ملاحظة: يتم استخدام الخطوات التالية في متصفح Firefox.

The screenshot shows the Cisco RV160 VPN Router web interface. The left sidebar contains navigation options: Getting Started, Status and Statistics, Administration (highlighted), File Management, Reboot, Diagnostic, Certificate (highlighted), Configuration Management, System Configuration, WAN, LAN, Routing, Firewall, VPN, Security, and QoS. The main content area is titled 'Certificate' and features a 'Certificate Table' with the following data:

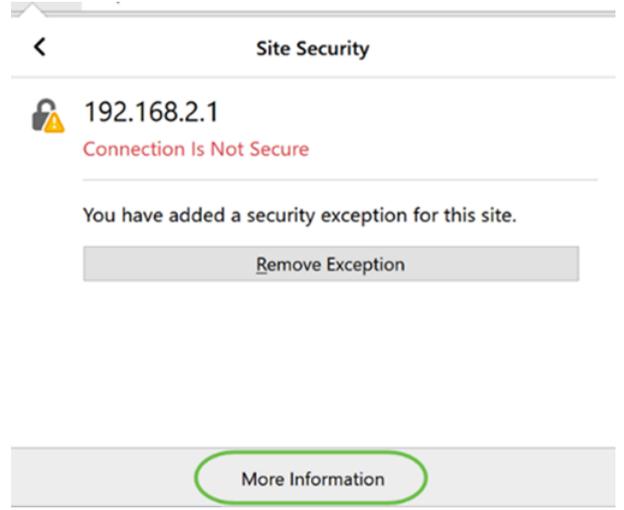
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Below the table are four buttons: 'Import Certificate...', 'Generate CSR/Certificate...', 'Show built-in 3rd party CA Certificates...', and 'Select as Primary Certificate...'.

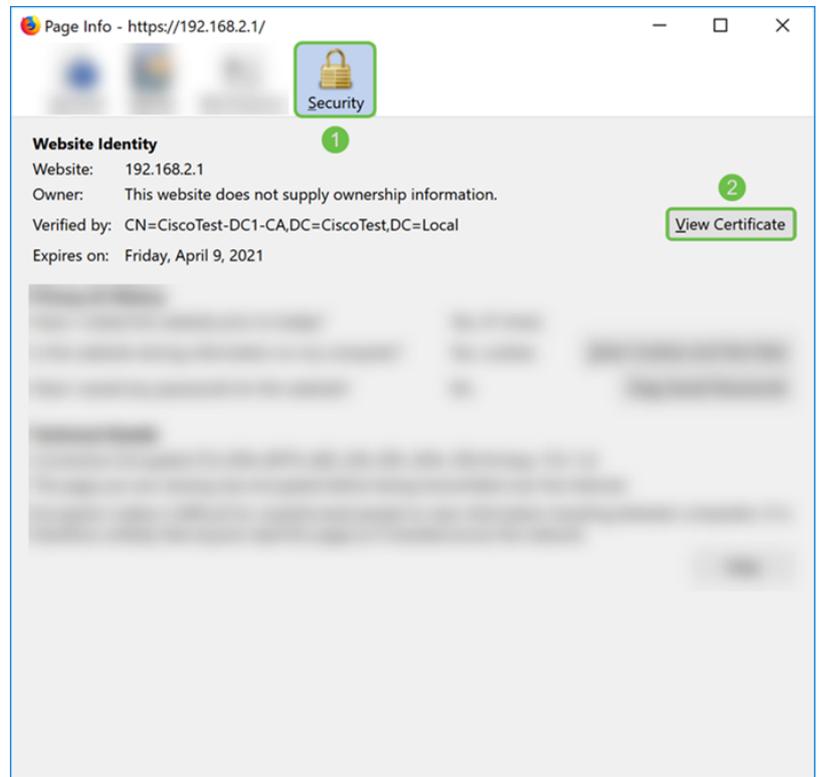
الخطوة 5. تظهر قائمة منسدلة من الخيارات. انقر على رمز السهم الموجود بجوار حقل الاتصال.

The screenshot shows the 'Site Information for 192.168.2.1' page. The 'Connection' section is highlighted with a green box and contains a warning icon and the text 'Connection Is Not Secure'. Other sections include 'Content Blocking' (Standard), 'Cookies', and 'Permissions'.

الخطوة 6. انقر فوق مزيد من المعلومات.

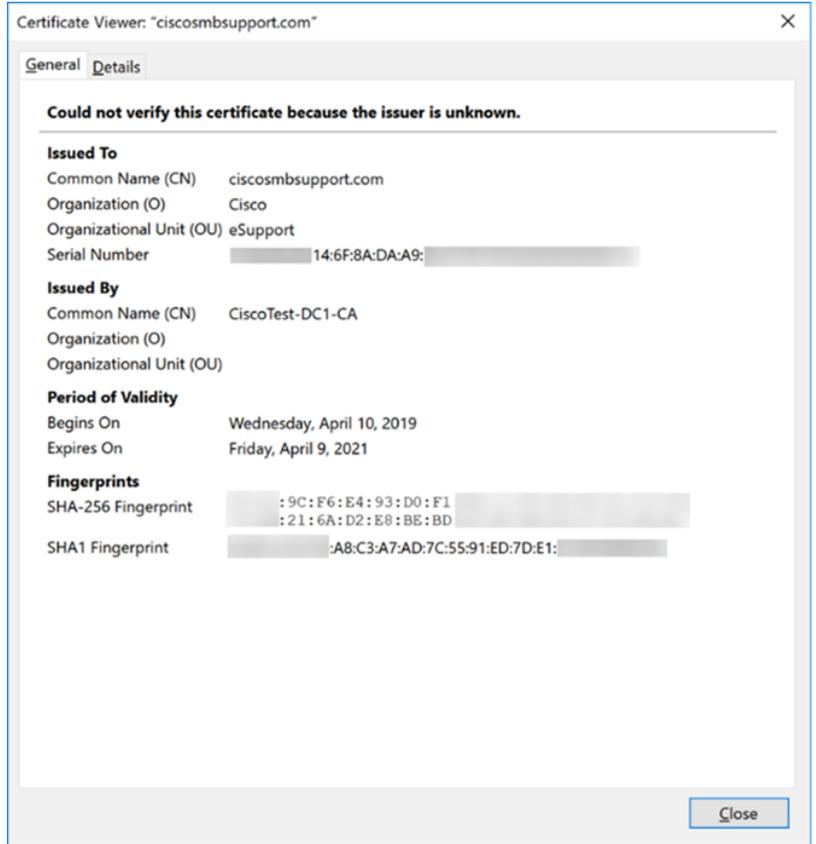


الخطوة 7. في نافذة معلومات الصفحة، يجب أن تكون قادرا على رؤية معلومات مختصرة عن شهادتك تحت قسم هوية موقع الويب. تأكد من أنك في علامة تبويب التأمين ثم انقر على عرض الترخيص للاطلاع على مزيد من المعلومات حول ترخيصك.



الخطوة 8. يجب أن تظهر صفحة عارض الشهادات. يجب أن تكون قادرا على رؤية جميع المعلومات المتعلقة بشهادتك ومدة صلاحيتها وبصماتها ومن تم إصدارها من قبل.

ملاحظة: بما أن هذه الشهادة تم إصدارها بواسطة خادم شهادات الاختبار، فإن المصدر غير معروف.



## تصدير الشهادة

لتنزيل شهادتك لاستيرادها على موجه آخر، اتبع الخطوات التالية.

الخطوة 1. في صفحة الترخيص، انقر أيقونة التصدير الموجودة بجوار الشهادة التي تريد تصديرها.

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		

الخطوة 2. تظهر شهادة تصدير. حدد تنسيقًا لتصدير الشهادة. الخيارات هي:

- **PKCS#12** - معايير تشفير المفتاح العام (PKCS) #12 هي شهادة مصدرة تأتي في امتداد .p12. سوف تكون كلمة المرور مطلوبة لتشفير الملف لحمايته كما هو صادر ومستورد ومحذوف.
- **PEM** - غالبًا ما يتم استخدام البريد المحسن للخصوصية (PEM) لخوادم الويب لقدرتها على الترجمة بسهولة إلى بيانات قابلة للقراءة باستخدام محرر نصوص بسيط مثل Notepad.

حدد تصدير بتنسيق PKCS#12 وأدخل كلمة مرور وتأكد كلمة المرور. ثم حدد الكمبيوتر الشخصي كحقل تصدير إلى:.. انقر على تصدير لبدء تصدير الشهادة إلى الكمبيوتر.

ملاحظة: تذكر كلمة المرور هذه لأنك ستستخدمها عند استيرادها إلى الموجه.

## Export Certificate



1

Export as PKCS#12 format

Enter Password:

2

Confirm Password:

Export as PEM format

Export to:

3

PC  USB

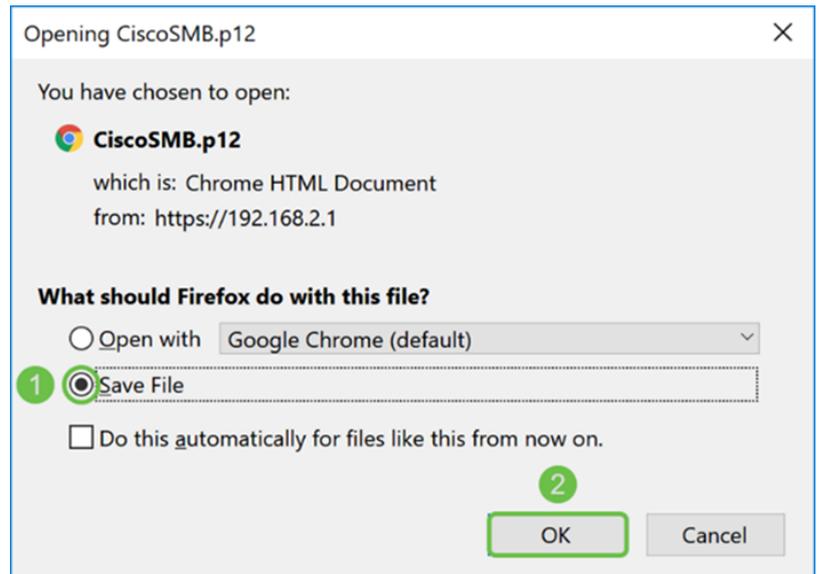


4

Export

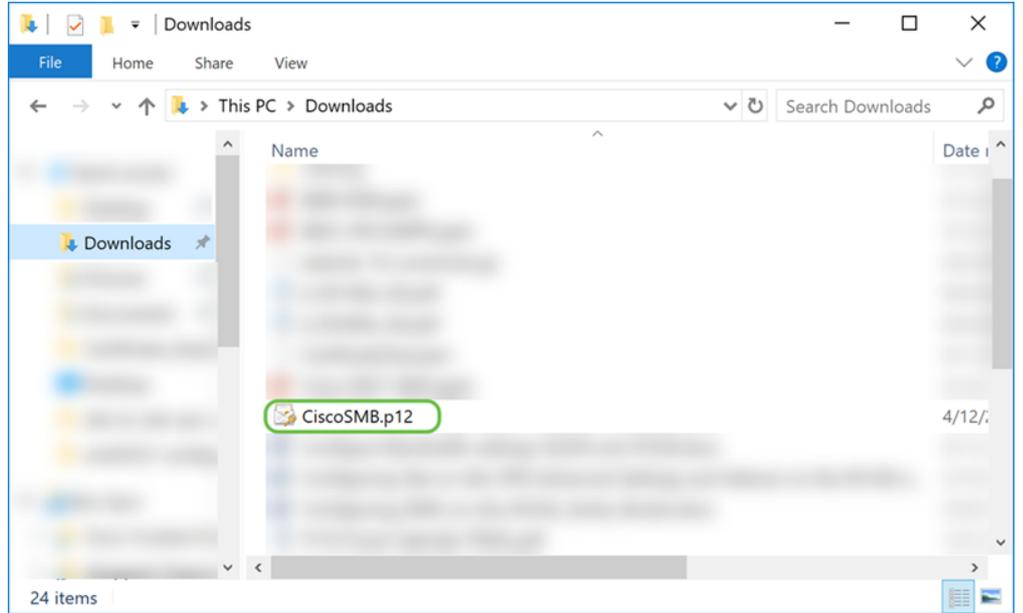
Cancel

الخطوة 3. سوف يظهر إطار يطلب ما يجب القيام به مع هذا الملف. في هذا المثال، سنقوم بتحديد حفظ الملف ثم انقر فوق موافق.



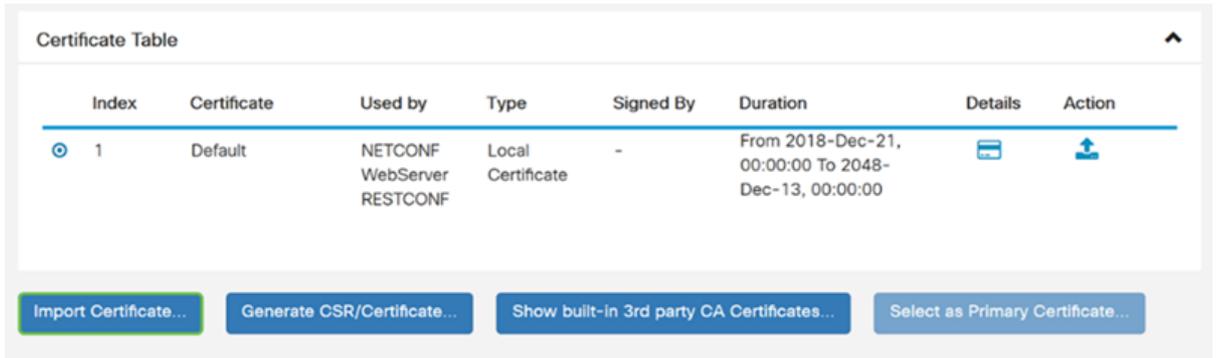
الخطوة 4. يجب حفظ الملف في موقع الحفظ الافتراضي الخاص بك.

في المثال الذي ضربناه، تم حفظ الملف في مجلد التنزيلات على جهاز الكمبيوتر الخاص بنا.



## إستيراد الشهادة

الخطوة 1. في صفحة الترخيص، انقر على زر إستيراد شهادة...



الخطوة 2. حدد نوع الشهادة التي سيتم إستيرادها من القائمة المنسدلة النوع أسفل قسم إستيراد شهادة. يتم تعريف الخيارات على أنها:

- شهادة CA - شهادة معتمدة من قبل هيئة خارجية موثوق بها تؤكد دقة المعلومات الواردة في الشهادة.
  - شهادة الجهاز المحلي - شهادة تم إنشاؤها على الموجه.
  - PKCS#12 المرمز الملف - معايير تشفير المفتاح العام (PKCS) #12 هي شهادة مصدرة تأتي في امتداد .p12.
- في هذا المثال، تم تحديد ملف PKCS#12 المشفر كنوع. أدخل اسما للشهادة ثم أدخل كلمة المرور التي تم إستخدامها.

### 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

الخطوة 3. تحت قسم تحميل ملف الشهادة، حدد إما إستيراد من الكمبيوتر الشخصي أو إستيراد من USB. في هذا المثال، تم تحديد إستيراد من الكمبيوتر الشخصي. انقر فوق إستعراض.. لاختيار ملف لتحميله.

### Import Certificate

Type:

Certificate Name:

Import Password:

### Upload Certificate file

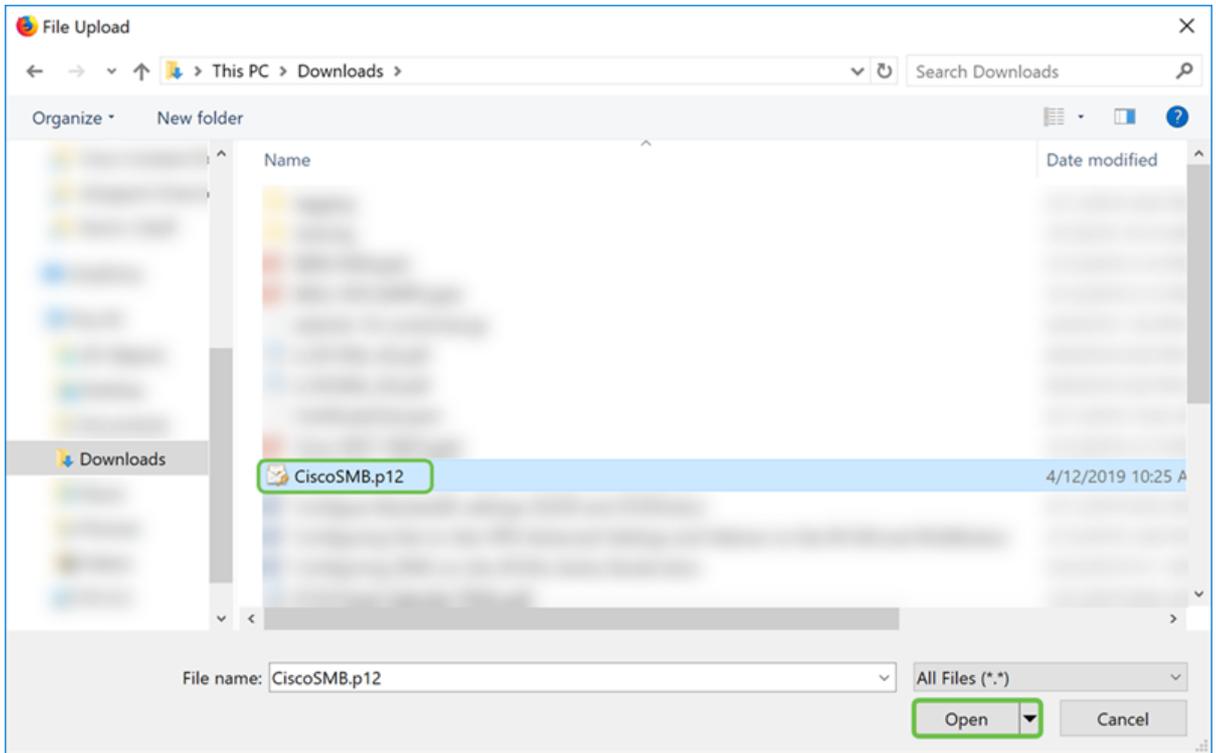
Import from PC

No file is selected

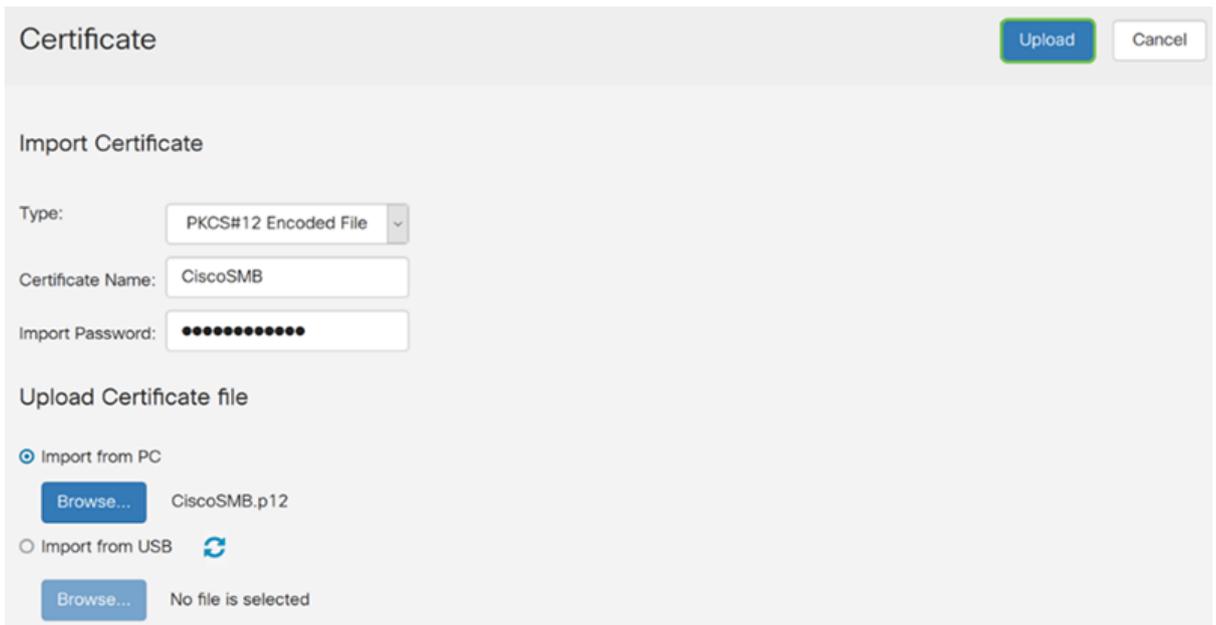
Import from USB 

No file is selected

الخطوة 4. في نافذة تحميل الملف، انتقل إلى موقع موقع موقع ملف PKCS#12 المشفر (.p12). حدد ملف p12. ثم انقر فتح.



الخطوة 5. انقر على تحميل لبدء تحميل الشهادة.



الخطوة 6. سوف يظهر إطار معلومات ليخبرك أن شهادتك تم إستيرادها بنجاح. انقر فوق موافق" للمتابعة.

## Information

**i** Import certificate successfully!

OK

الخطوة 7. يجب أن ترى أن شهادتك تم تحميلها.

## 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		 

## القرار

يجب أن تكون قد تعلمت بنجاح كيفية إنشاء شهادة CSR واستيرادها وتنزيلها على موجه من السلسلة RV160 و RV260.

