الشهادة (إستيراد/تصدير/إنشاء CSR) على RV260 و RV160 السلسلة من الموجه

الهدف

الهدف من هذا المستند هو توضيح كيفية إنشاء طلب توقيع شهادة (CSR) بالإضافة إلى إستيراد وتصدير الشهادات على موجهات 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: Verisign، GeoTrust، GlobalSign، GoDaddy، Comodo، IdenTrust 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

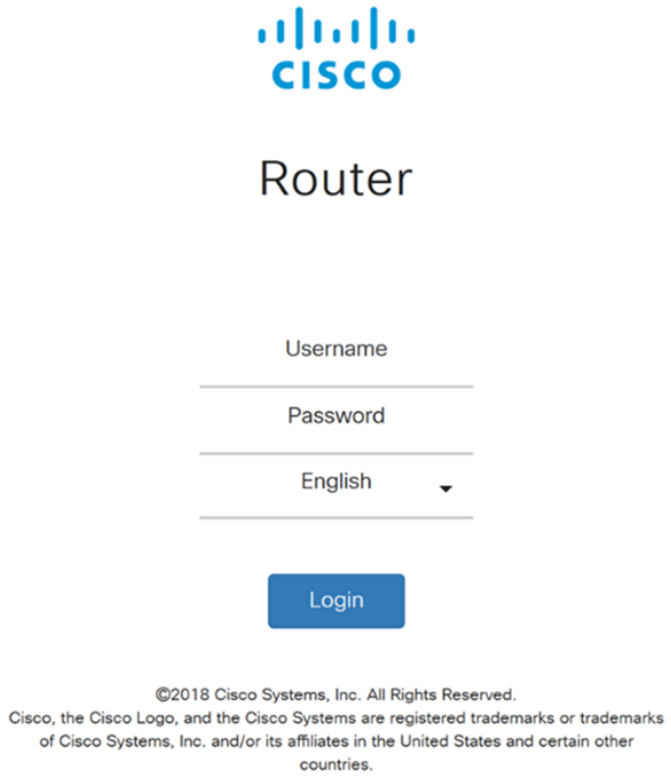
من خلال هذه المقالة، سوف:

1. إنشاء CSR/شهادة
2. عرض الشهادة
3. تصدير الشهادة
4. إستيراد الشهادة

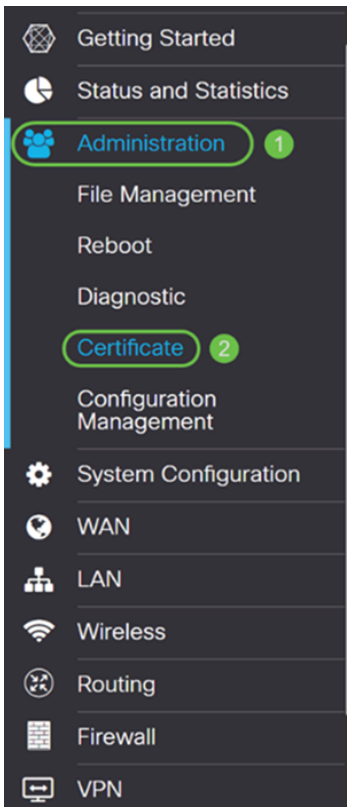
5. القرار

إنشاء CSR/شهادة

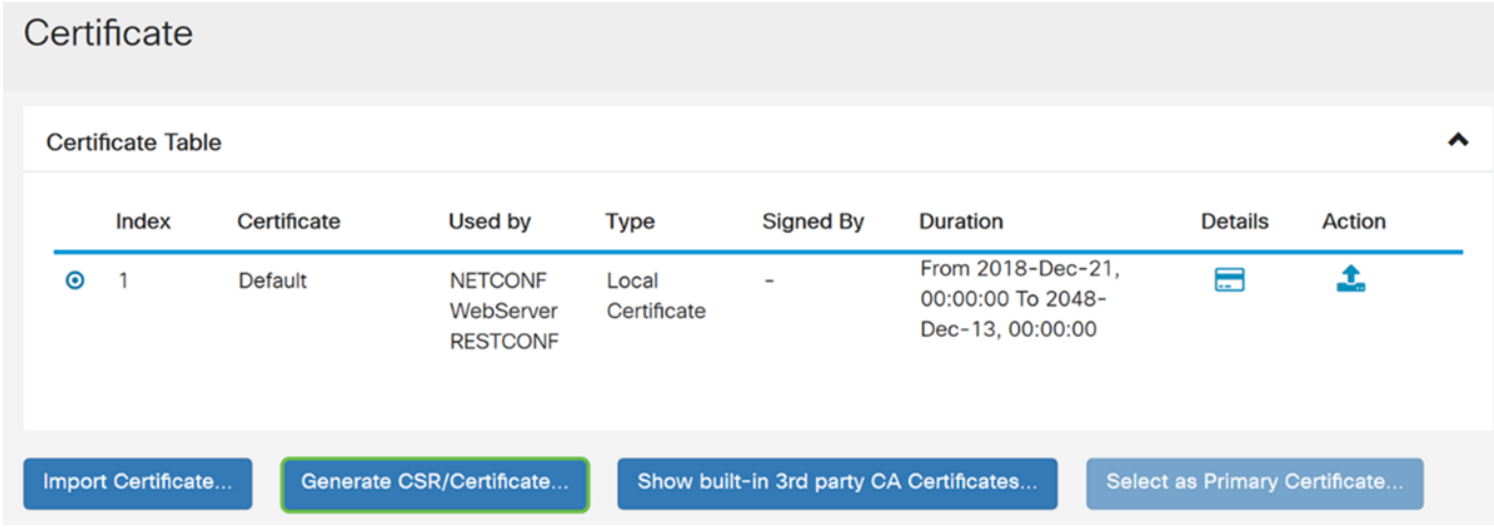
الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب.



الخطوة 2. انتقل إلى **إدارة > شهادة**.



الخطوة 3. في صفحة *الشهادة*، انقر على **زر إنشاء CSR/Certificate...**



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

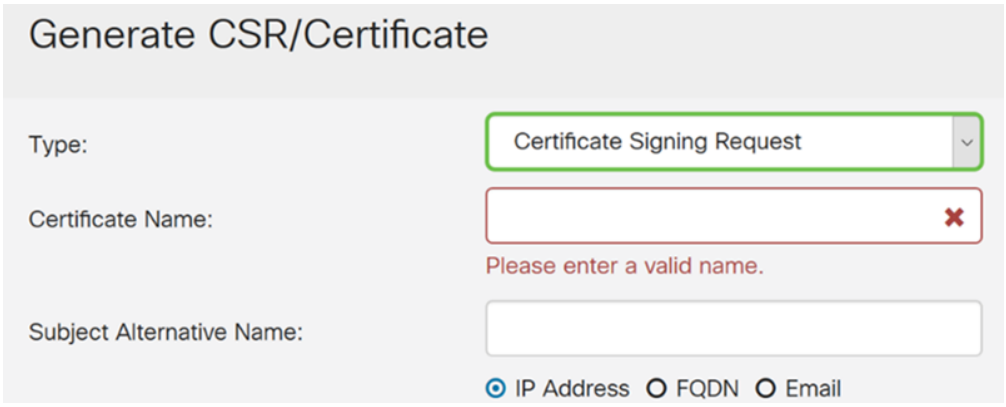
- **شهادة موقعة ذاتيا** - هذه هي شهادة طبقة مأخذ التوصيل الآمنة (SSL) الموقعة من قبل منشئها. تكون هذه الشهادة أقل ثقة، حيث لا يمكن إلغاؤها إذا تم أختراق المفتاح الخاص بطريقة ما من قبل المهاجم. يجب توفير المدة الصحيحة بالأيام.

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

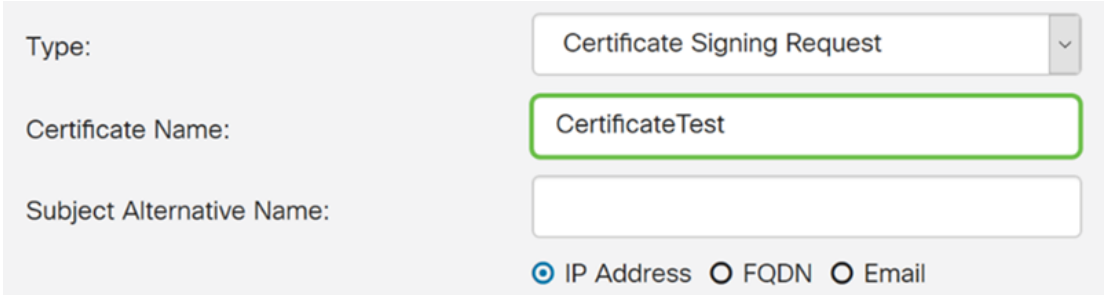
- **طلب توقيع الشهادة** - هذه هي البنية الأساسية للمفتاح العام (PKI) التي يتم إرسالها إلى المرجع المصدق لتقديم طلب لشهادة الهوية الرقمية. إنه أكثر أمانا من التوقيع الذاتي نظرا لأنه يتم الاحتفاظ بالمفتاح الخاص سرا. يوصى بهذا الخيار.

- **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**.



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

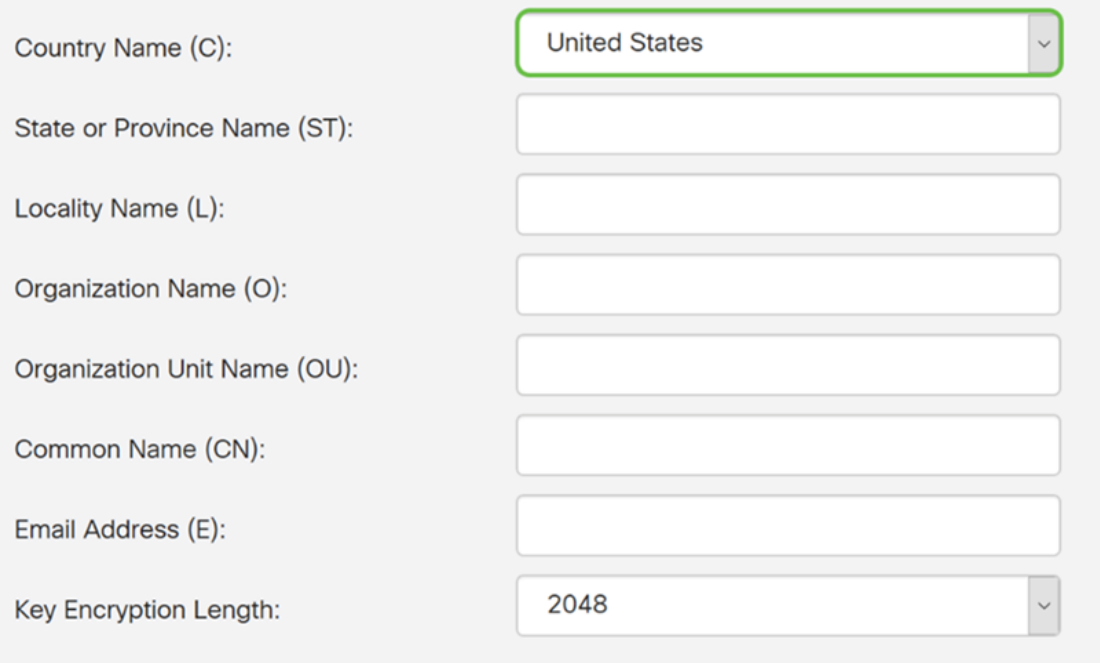


الخطوة 6. في حقل *الاسم البديل للموضوع*، حدد واحدا مما يلي: **عنوان IP**، أو **FQDN** (اسم المجال المؤهل

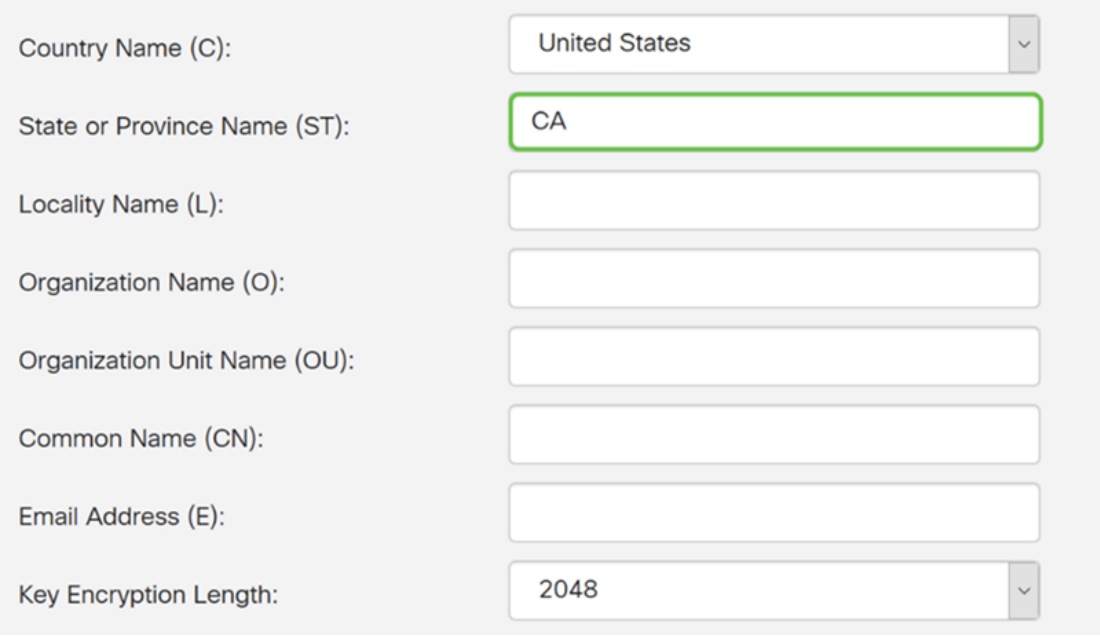
بالكامل)، **أو** البريد الإلكتروني **ثم أدخل الاسم المناسب من ما قمت بتحديده.** يتيح لك هذا الحقل تحديد أسماء مضيف إضافية.

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

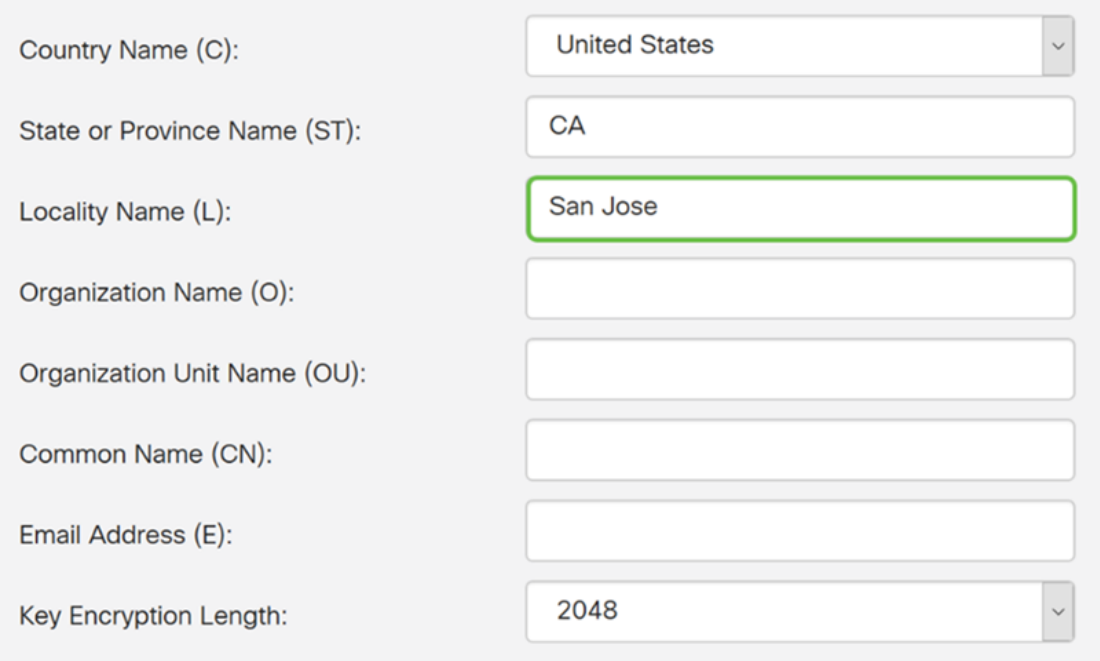
الخطوة 7. حدد **دولة** من القائمة المنسدلة *اسم البلد (C)*.



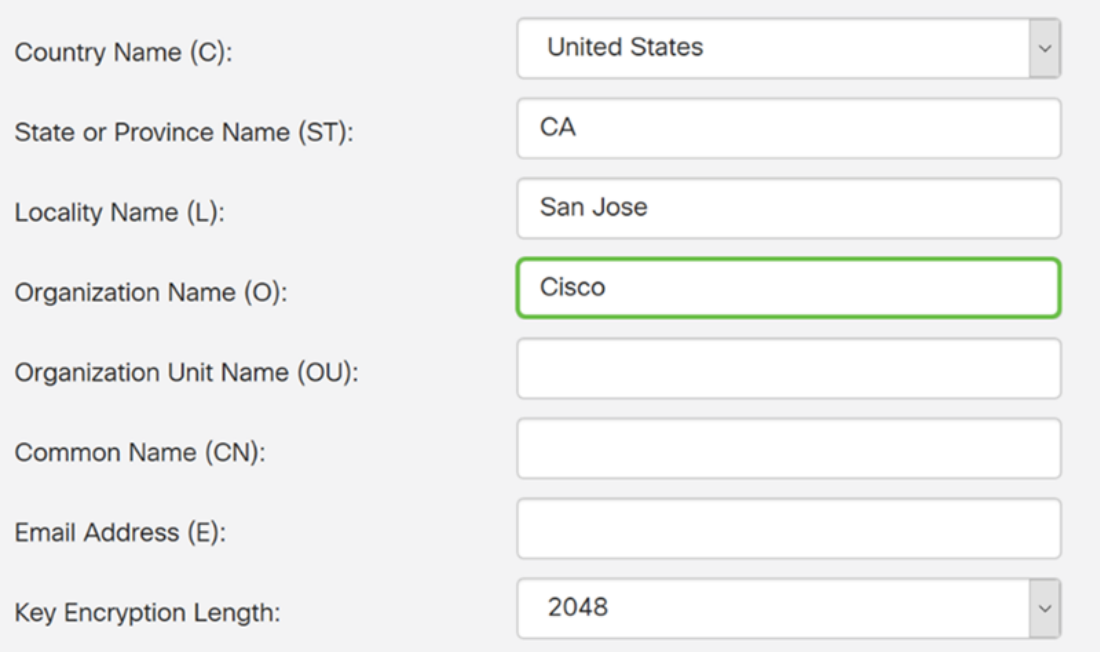
الخطوة 8. أدخل **اسم ولاية** أو **مقاطعة** في حقل *اسم الولاية أو المقاطعة*.



الخطوة 9. دخلت في *المحلي إسم*، **مدينة** إسم.

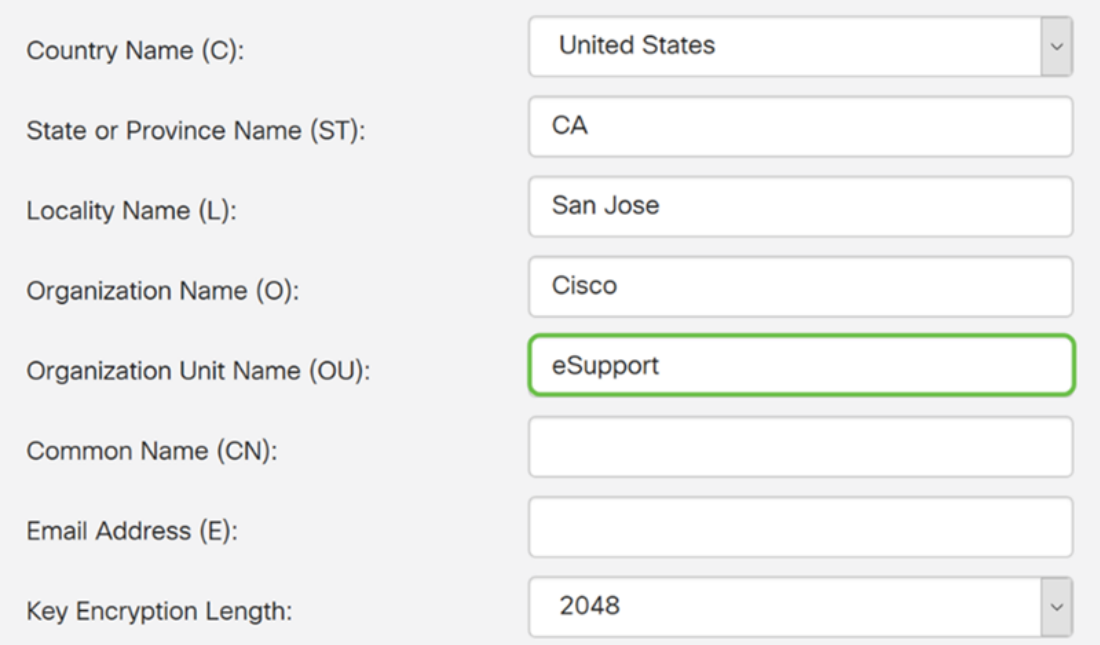


الخطوة 10. أدخل اسم **المؤسسة** في حقل *اسم المؤسسة*.



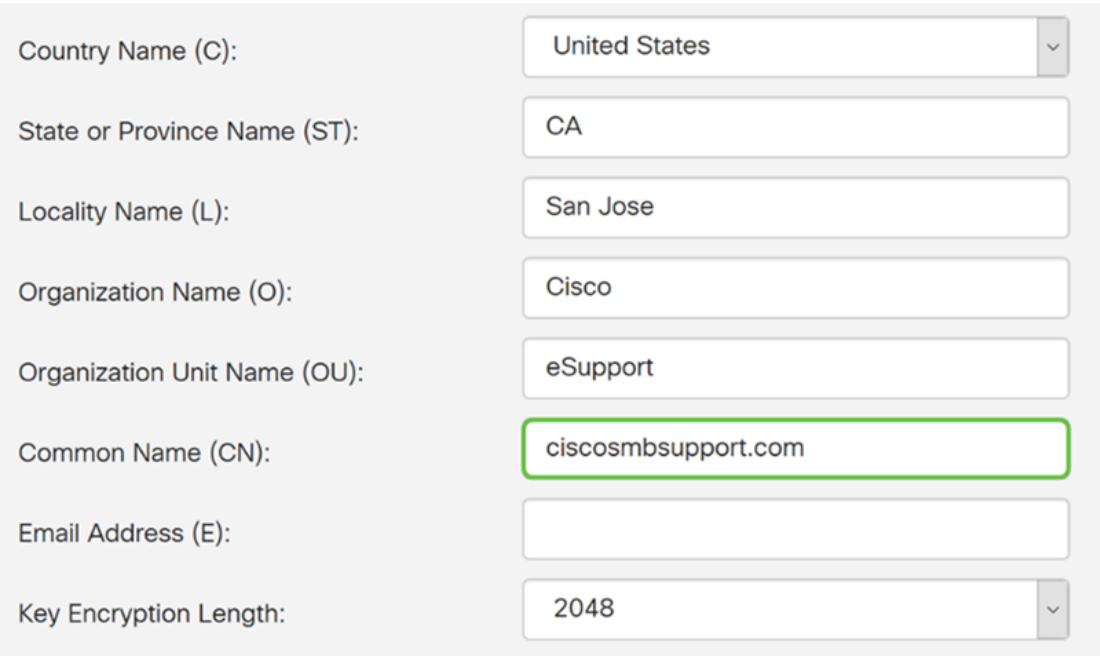
الخطوة 11. أدخل اسم **الوحدة التنظيمية** (أي التدريب والدعم، وما إلى ذلك).

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

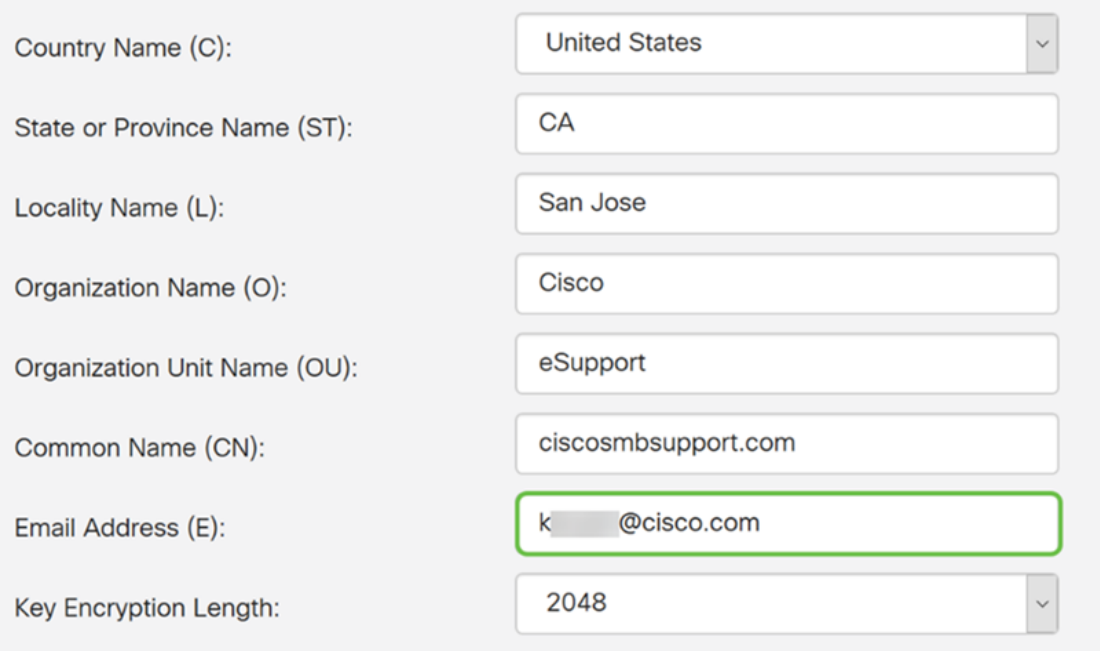


الخطوة 12. أدخل **اسما عاما**. إن FQDN الخاص بخادم ويب هو الذي سيتلقى هذه الشهادة.

في هذا المثال، تم إستخدام **ciscosmbsupport.com** كاسم عام.

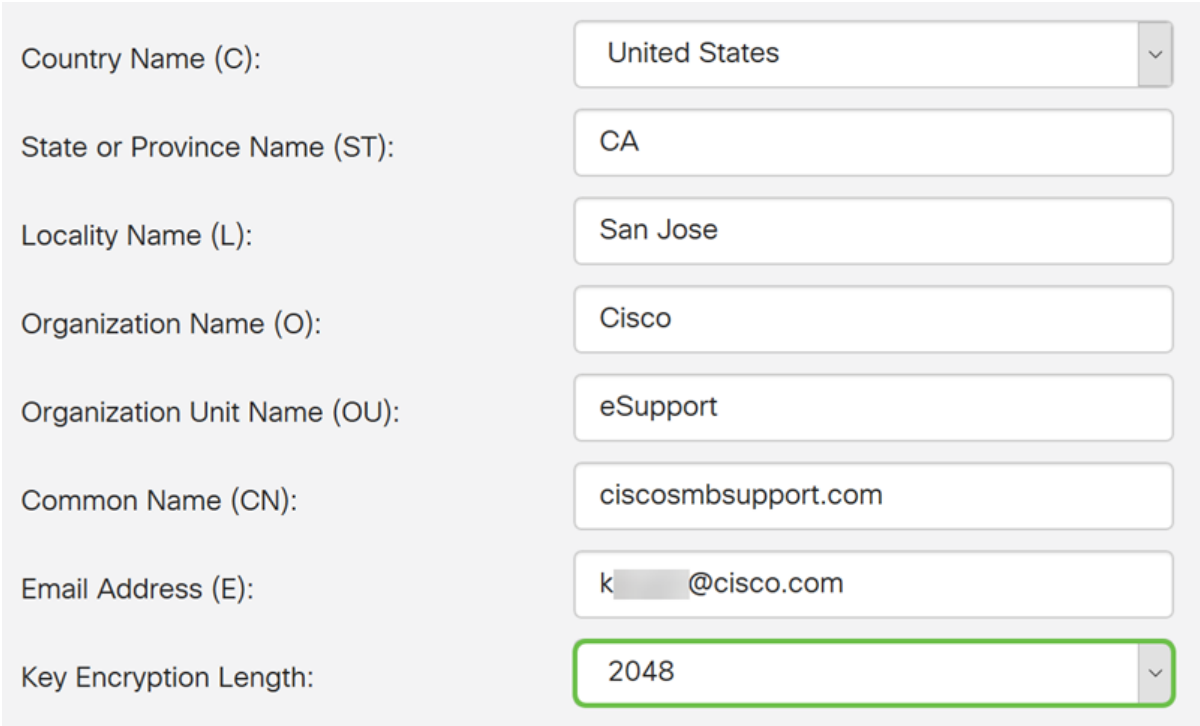


الخطوة 13. أدخل **عنوان بريد إلكتروني**.

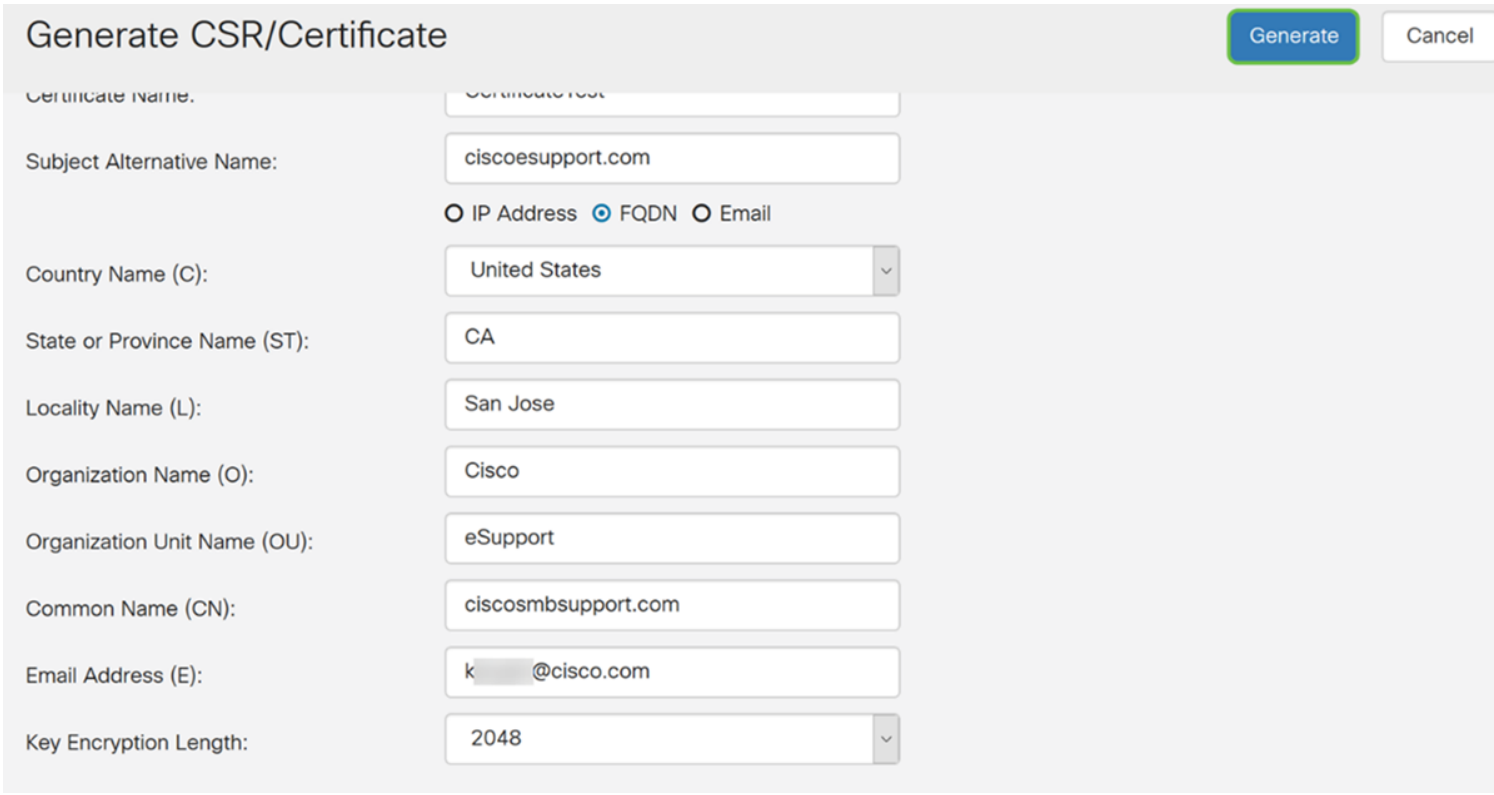


الخطوة 14. حدد **طول تشفير المفاتيح** من القائمة المنسدلة. الخيارات هي: **512**، **1024**، أو **2048**. كلما زاد حجم المفتاح، زاد تأمين الشهادة. كلما كبر حجم المفتاح، كلما زاد وقت المعالجة.

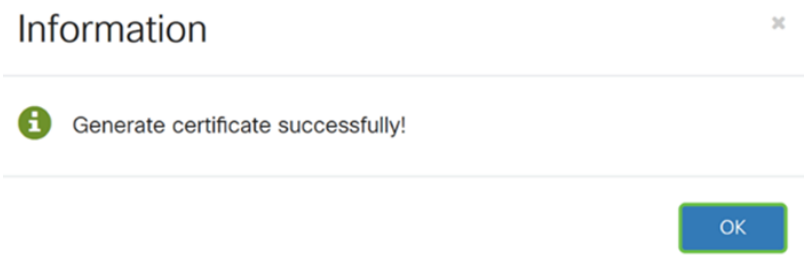
أفضل الممارسات: يوصى باختيار أعلى طول تشفير للمفتاح - مما يتيح تشفيرا أكثر صرامة.



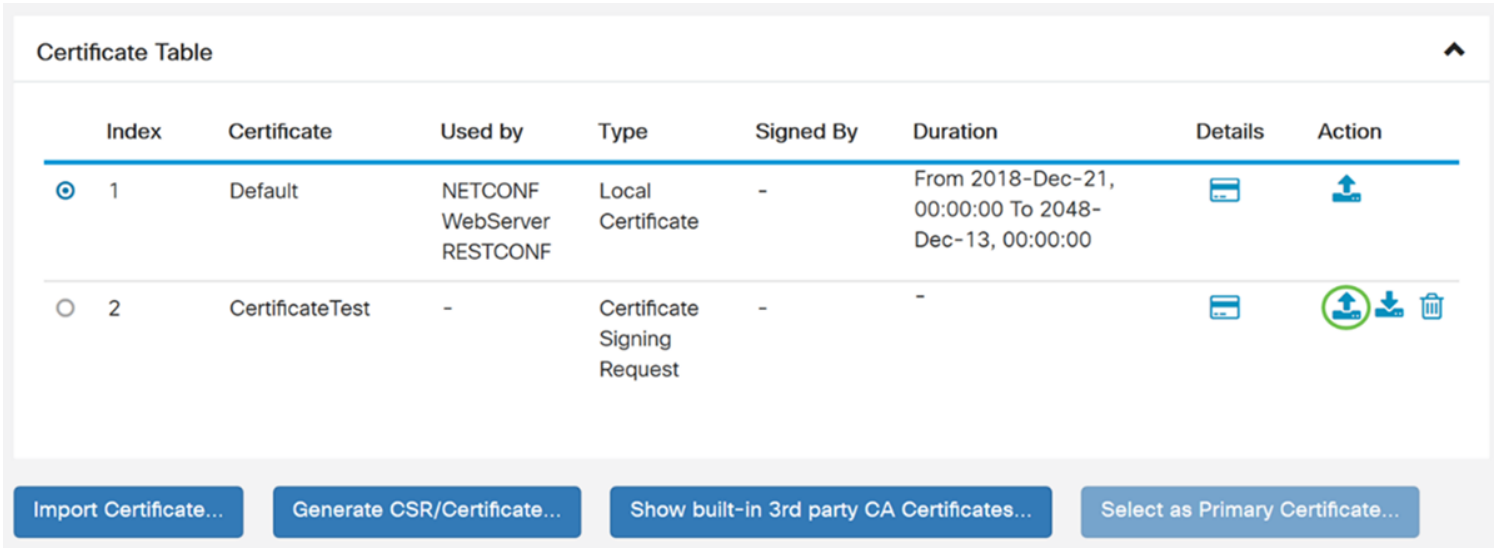
الخطوة 15. طقطقة **يلد**.



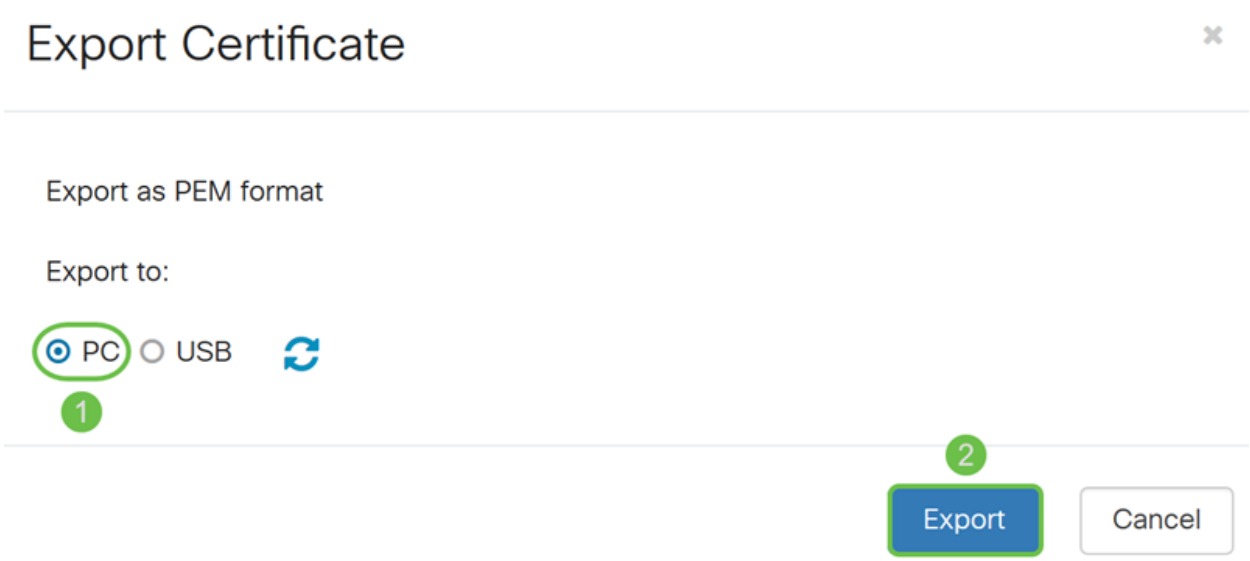
الخطوة 16. ستظهر قائمة *معلومات* منبثقة مع رسالة "إنشاء شهادة بنجاح!". انقر فوق **موافق** للمتابعة.



الخطوة 17. تصدير CSR من *جدول الشهادات*.

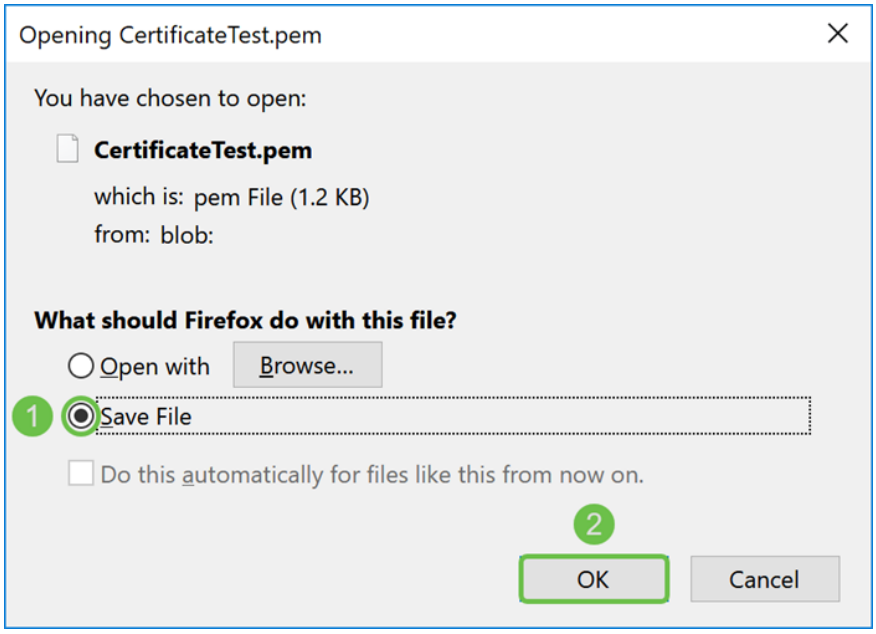


الخطوة 18. تظهر نافذة *تصدير شهادات*. حدد **كمبيوتر شخصي** ل *التصدير إلى* ثم انقر فوق **تصدير**.



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

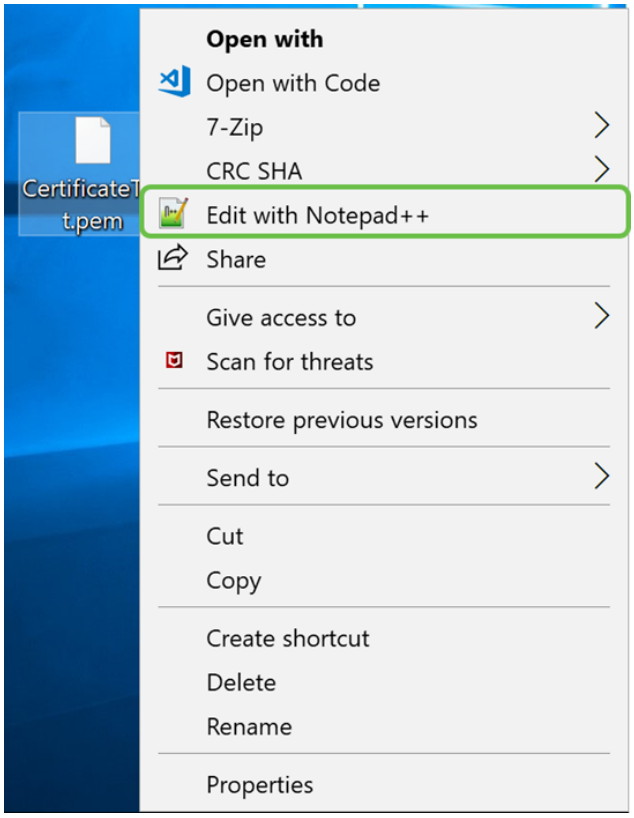
في هذا المثال، سنقوم بتحديد **حفظ الملف** ثم انقر فوق **موافق**.



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.



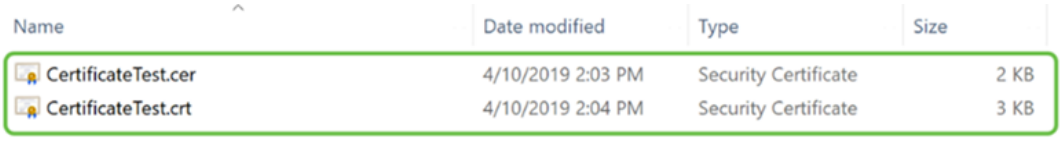
الخطوة 21. تأكد من أن ***بدء طلب الشهادة*** —و— ***نهاية طلب الشهادة*** — في السطر الخاص به.

ملاحظة: كانت بعض أجزاء الشهادة غير واضحة.

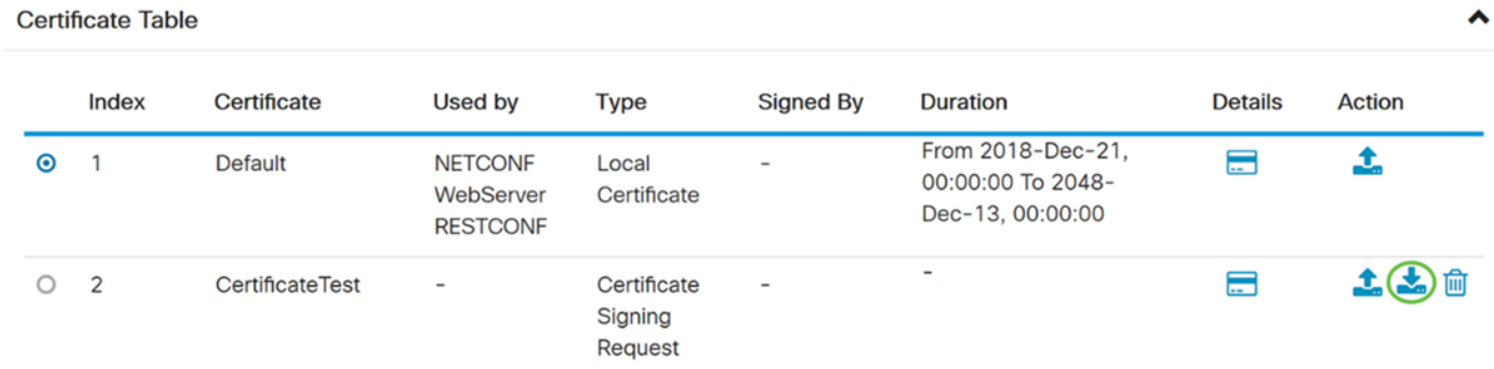
الخطوة 22. عندما يكون لديك CSR الخاص بك، ستحتاج إلى الانتقال إلى خدمات الاستضافة الخاصة بك أو إلى موقع مرجع شهادات (مثل GoDaddy و Verisign وما إلى ذلك) وطلب شهادة. بمجرد أن تقوم بإرسال طلب، فإنه يتصل بخادم الشهادات للتأكد من عدم وجود أي سبب لعدم إصدار الشهادة.

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

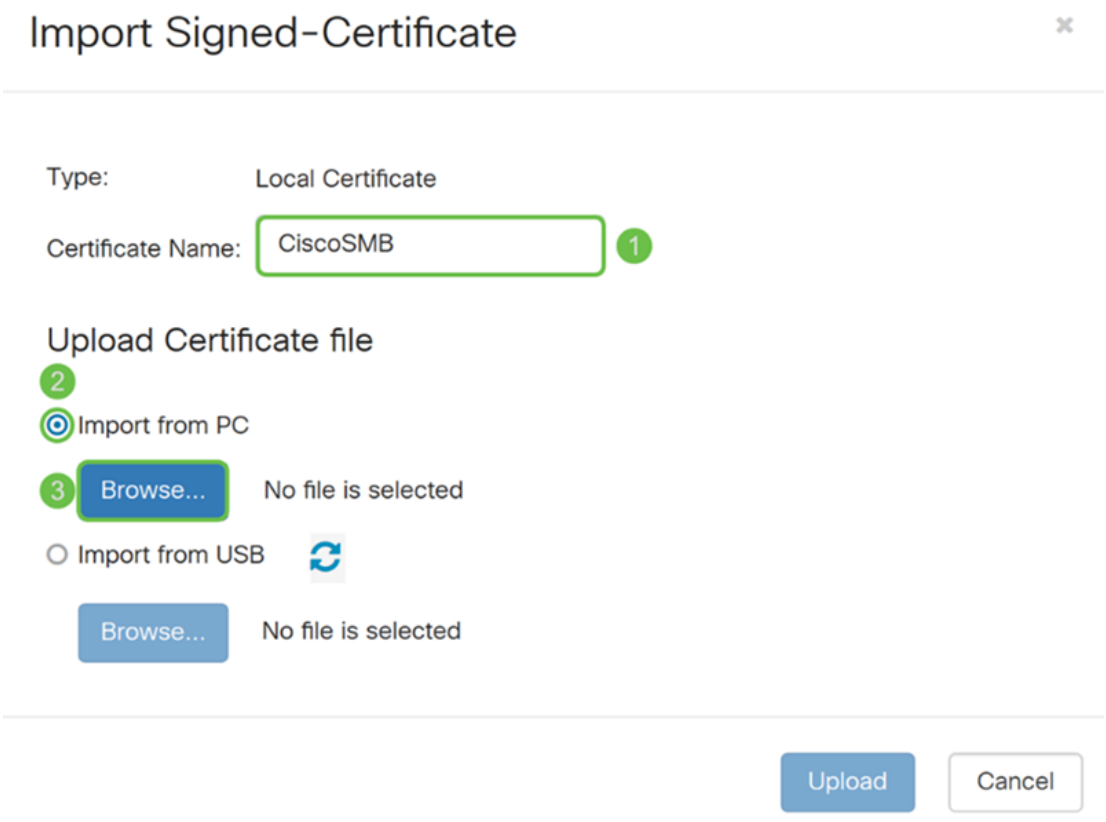
الخطوة 23. قم بتنزيل الشهادة بمجرد اكتمالها. يجب أن يكون إما **.cer** أو **.crt** مبرد. في هذا المثال، تم تزويدنا بكلا الملفين.



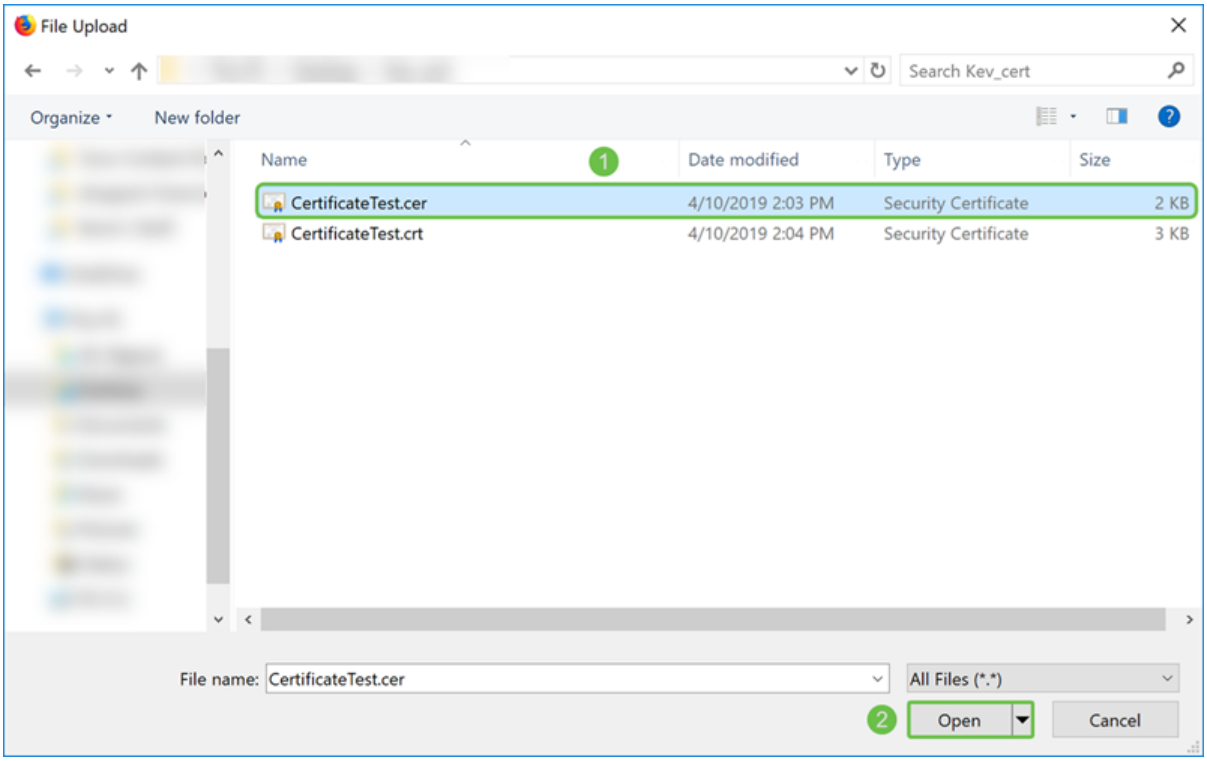
الخطوة 24. عد إلى صفحة *الشهادة* في الموجه الخاص بك واستورد ملف الترخيص بالنقر على **السهم المشير إلى** أيقونة **الجهاز**.



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.

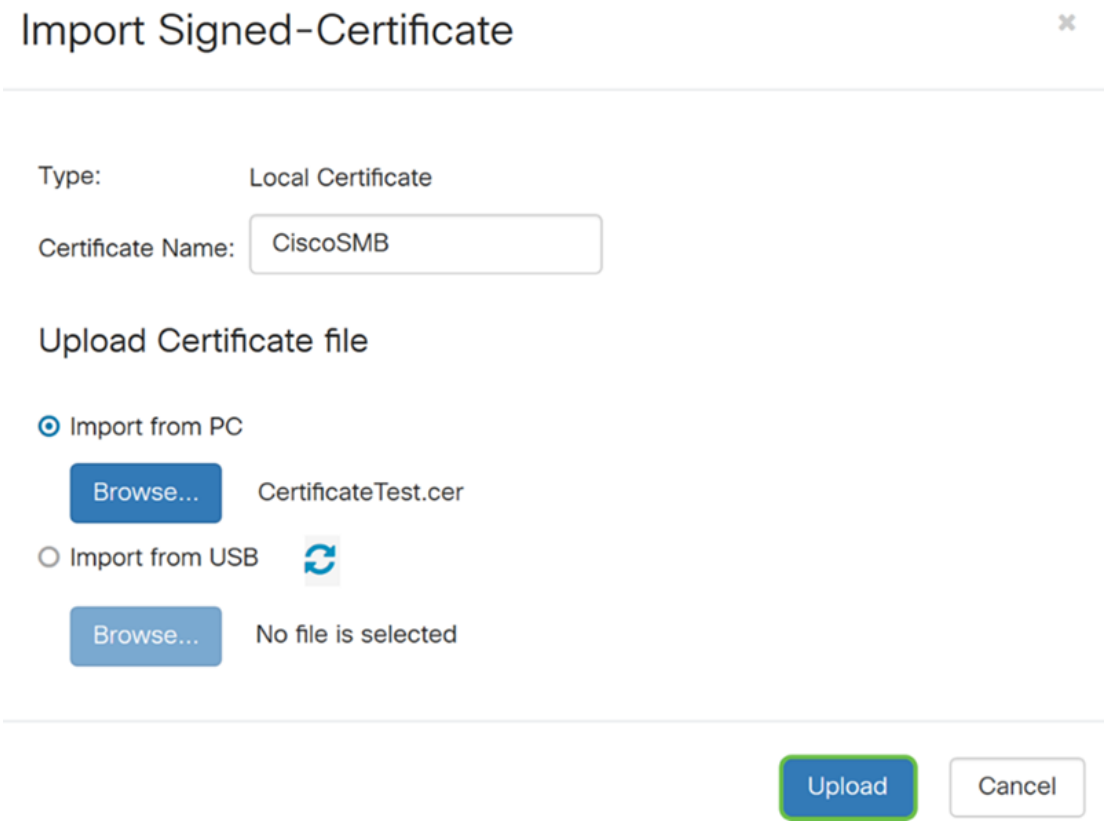


الخطوة 26. تظهر نافذة *تحميل ملف*. انتقل إلى موقع ملف الشهادة الخاص بك. حدد ملف **الشهادة** الذي تريد تحميله وانقر فوق **فتح**. في هذا المثال، تم تحديد **CertificateTest.cer**.

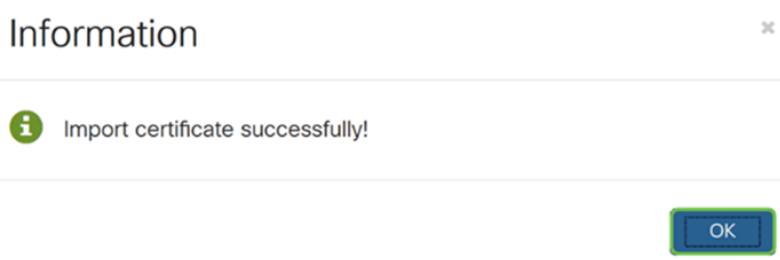


الخطوة 27. انقر على زر **التحميل** لبدء تحميل شهادتك إلى الموجه.

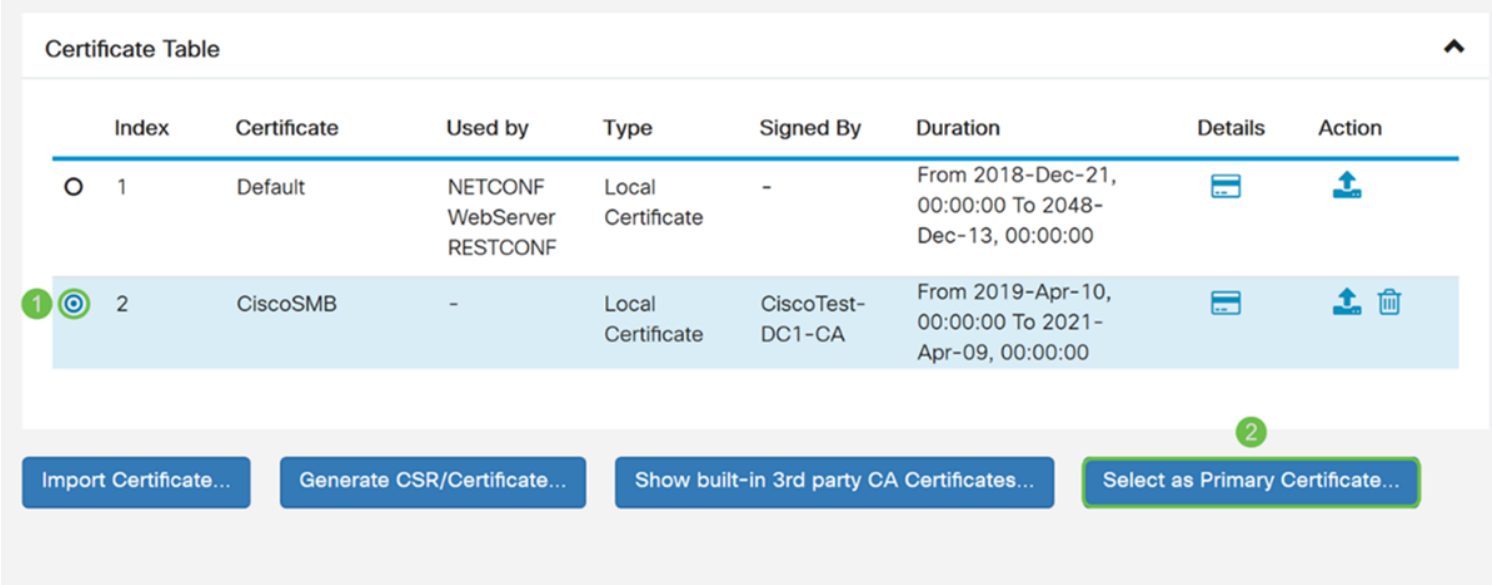
ملاحظة: إذا حدث خطأ لا يمكنك من خلاله تحميل ملف .cer الخاص بك، فقد يحدث ذلك لأن الموجه الخاص بك يطلب أن تكون الشهادة في ترميز PEM. ستحتاج إلى تحويل ترميز جهاز التشفير الخاص بك (.cer file extension)، إلى ترميز بيم (.crt file extension).



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



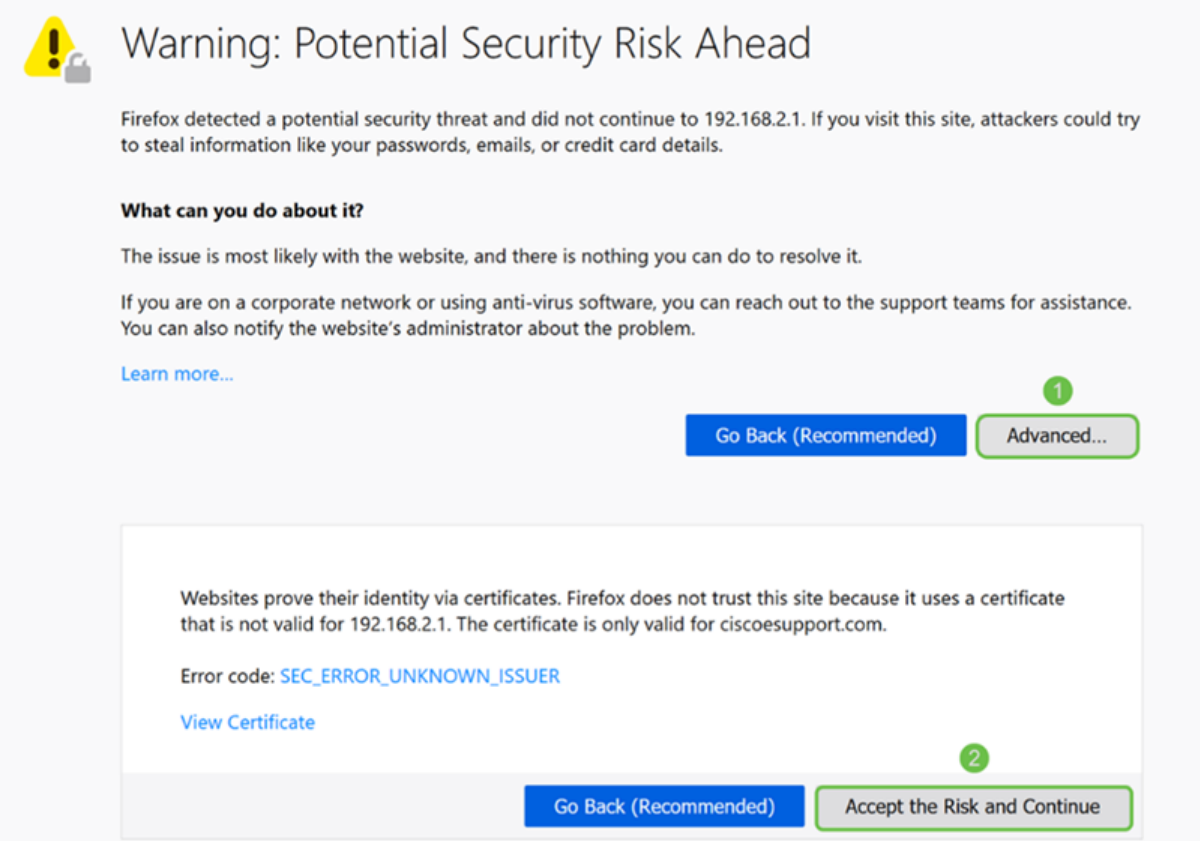
الخطوة 29. يجب تحديث شهادتك بنجاح. يجب أن تكون قادرا على معرفة من تم توقيع شهادتك. في هذا المثال، يمكننا أن نرى أن شهادتنا تم توقيعها بواسطة *CiscoTest-DC1-CA*. لجعل الشهادة الشهادة الأساسية، حدد الشهادة باستخدام زر الخيار الموجود على الجانب الأيسر وانقر على **زر تحديد كشهادة أساسية...**



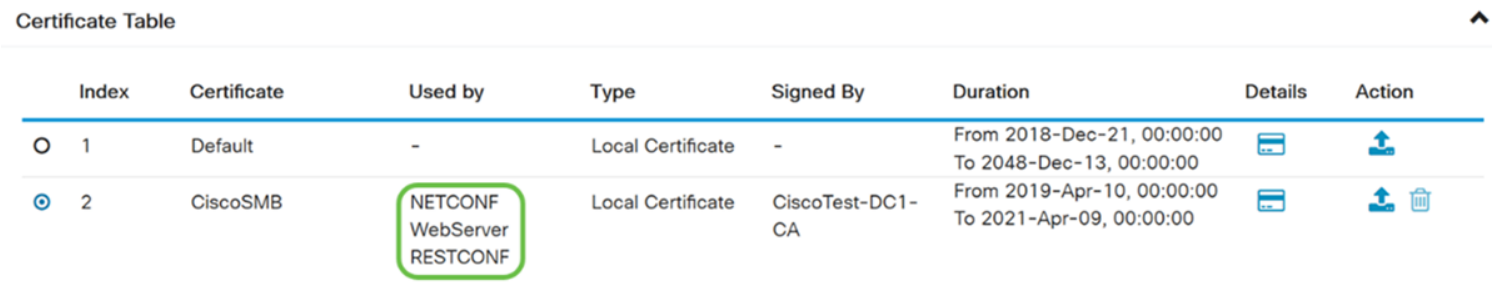
ملاحظة: قد يؤدي تغيير الشهادة الأساسية إلى إعادتك إلى صفحة التحذير. إذا كنت تستخدم Firefox وتظهر كصفحة فارغة رمادية، ستحتاج إلى ضبط بعض التهيئة على Firefox لديك. هذه الوثيقة على موقع موزيلا تعطي بعض الإيضاحات عنها: CA/AddRootToFirefox. لكي تتمكن من رؤية صفحة التحذير مرة أخرى، اتبع هذه الخطوات التي تم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



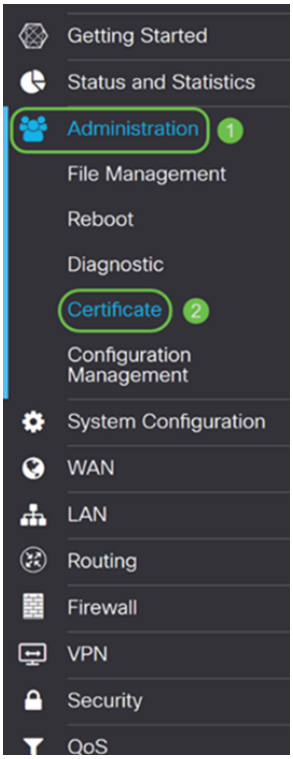
الخطوة 31. في جدول الشهادات، يجب أن ترى أن *WebServer*، NetConf، و*RESTCONF* قد استبدلت شهادتك الجديدة بدلا من إستخدام *الشهادة* الافتراضية.



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

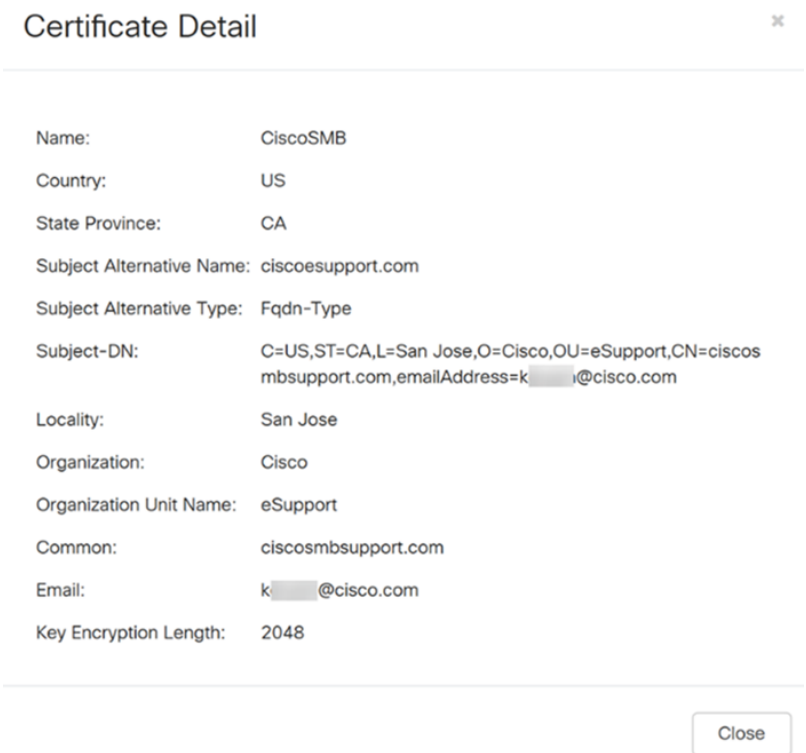
عرض الشهادة

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



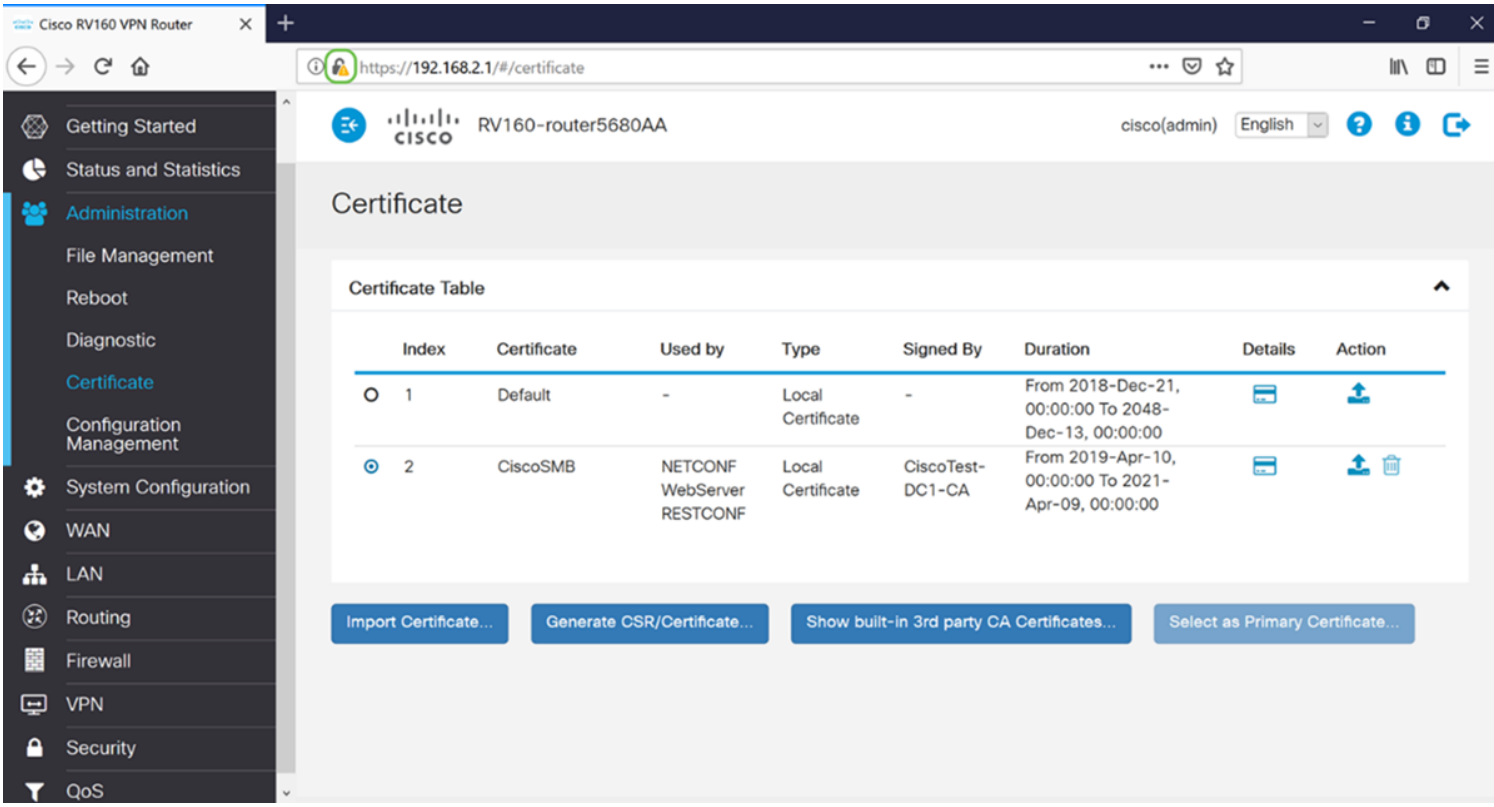
الخطوة 2. في *جدول الترخيص*، انقر على أيقونة **التفاصيل** الموجودة تحت قسم *التفاصيل*.

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

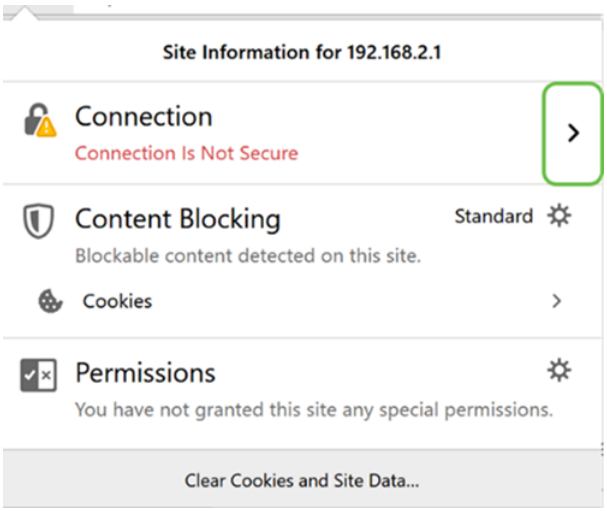


الخطوة 4. انقر فوق رمز **القفل** الموجود على الجانب الأيسر من شريط محدد موقع الموارد الموحد (URL).

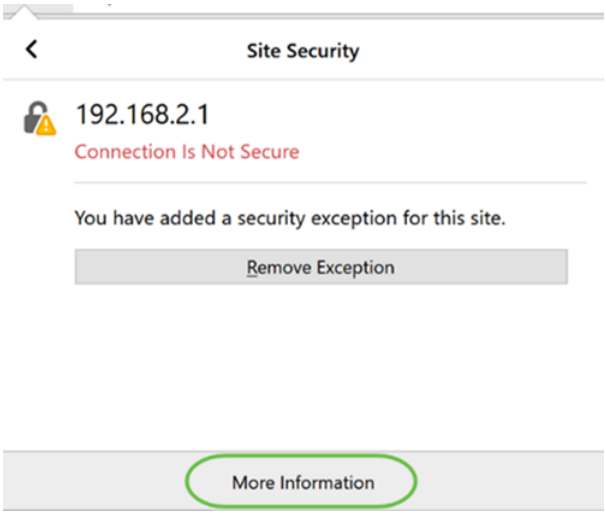
ملاحظة: يتم إستخدام الخطوات التالية في متصفح Firefox.



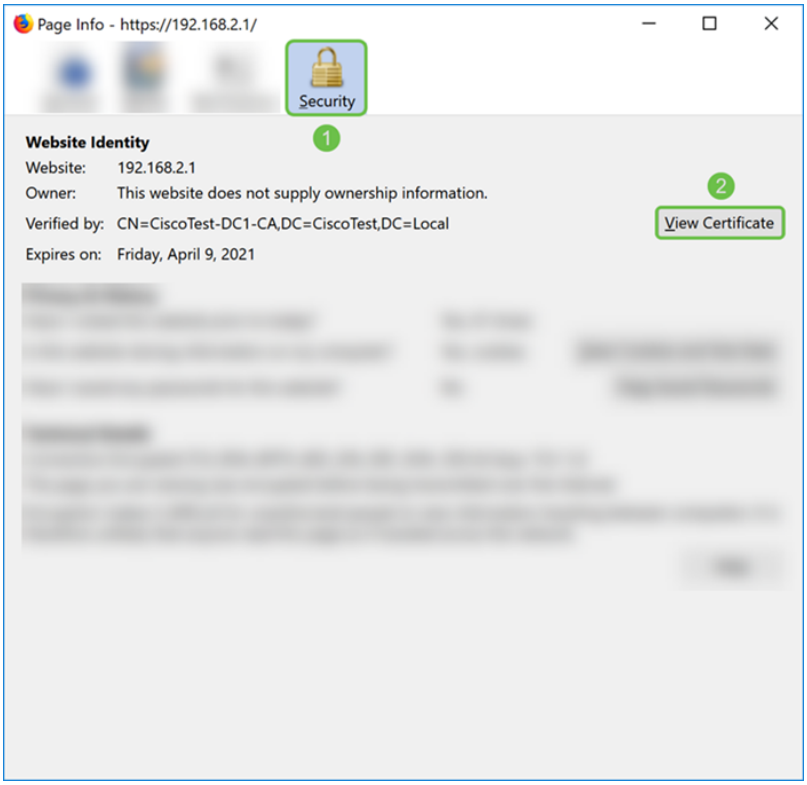
الخطوة 5. تظهر قائمة منسدلة من الخيارات. انقر على رمز **السهم** الموجود بجوار حقل *الاتصال*.



الخطوة 6. انقر فوق **مزيد من المعلومات**.

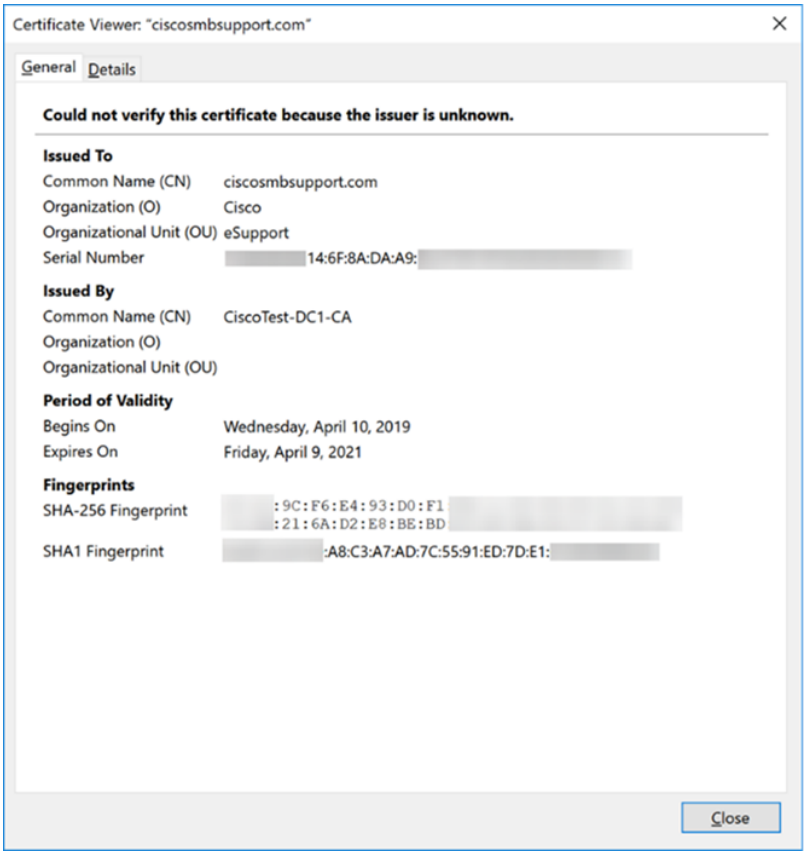


الخطوة 7. في نافذة *معلومات الصفحة*، يجب أن تكون قادرا على رؤية معلومات مختصرة عن شهادتك تحت قسم *هوية موقع الويب*. تأكد من أنك في علامة تبويب **التأمين** ثم انقر على **عرض الترخيص** للاطلاع على مزيد من المعلومات حول ترخيصك.



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.

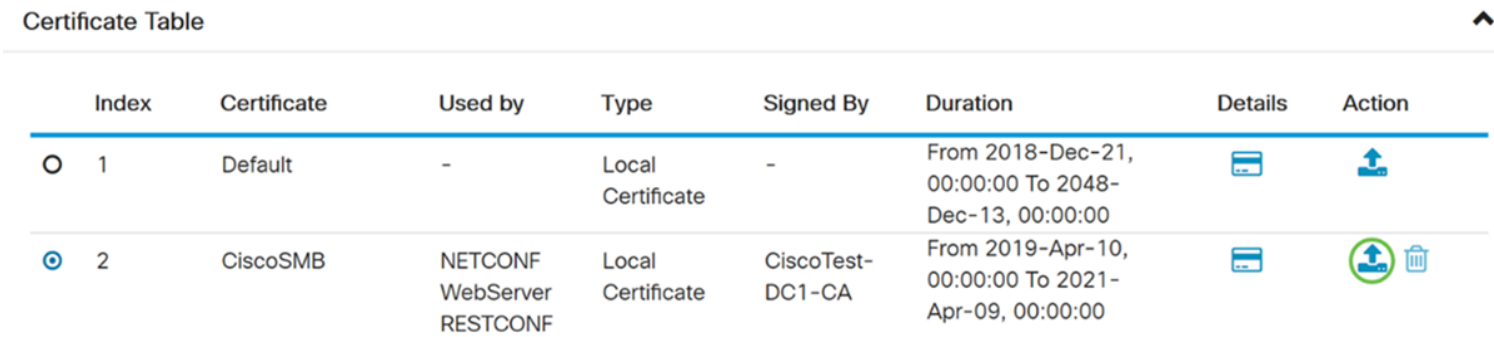
ملاحظة: بما أن هذه الشهادة تم إصدارها بواسطة خادم شهادات الاختبار، فإن المصدر غير معروف.



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.



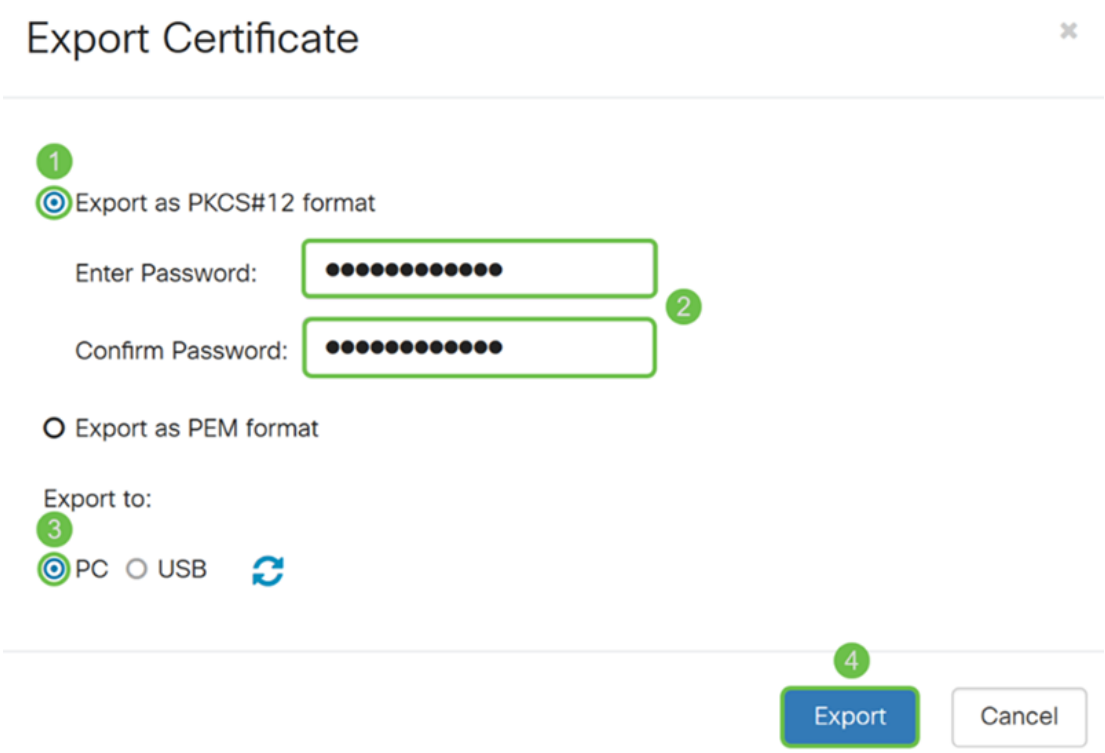
الخطوة 2. تظهر *شهادة تصدير*. حدد تنسيقا لتصدير الشهادة. الخيارات هي:

- **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.

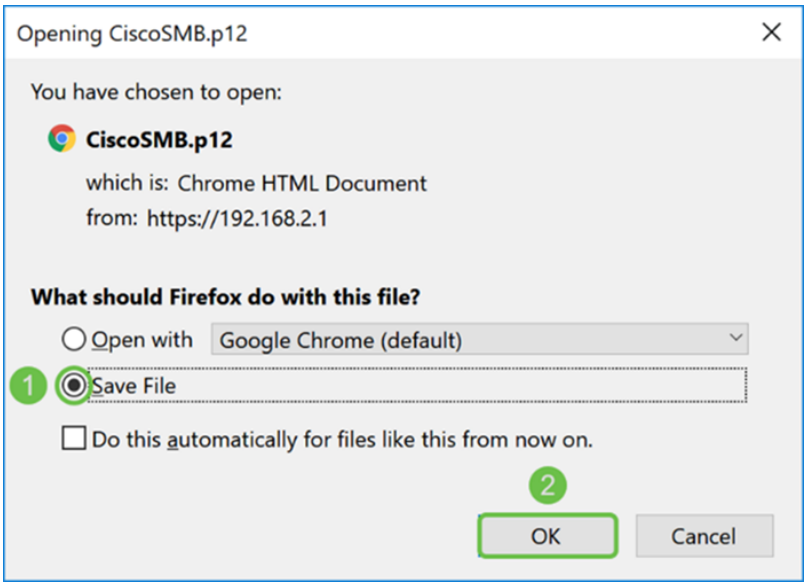
- **PEM** - غالبا ما يتم إستخدام البريد المحسن للخصوصية (PEM) لخوادم الويب لقدرتها على الترجمة بسهولة إلى بيانات قابلة للقراءة باستخدام محرر نصوص بسيط مثل Notepad.

حدد **تصدير بتنسيق PKCS#12** وأدخل **كلمة مرور** و**تأكيد 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 إستيرادها إلى الموجه.

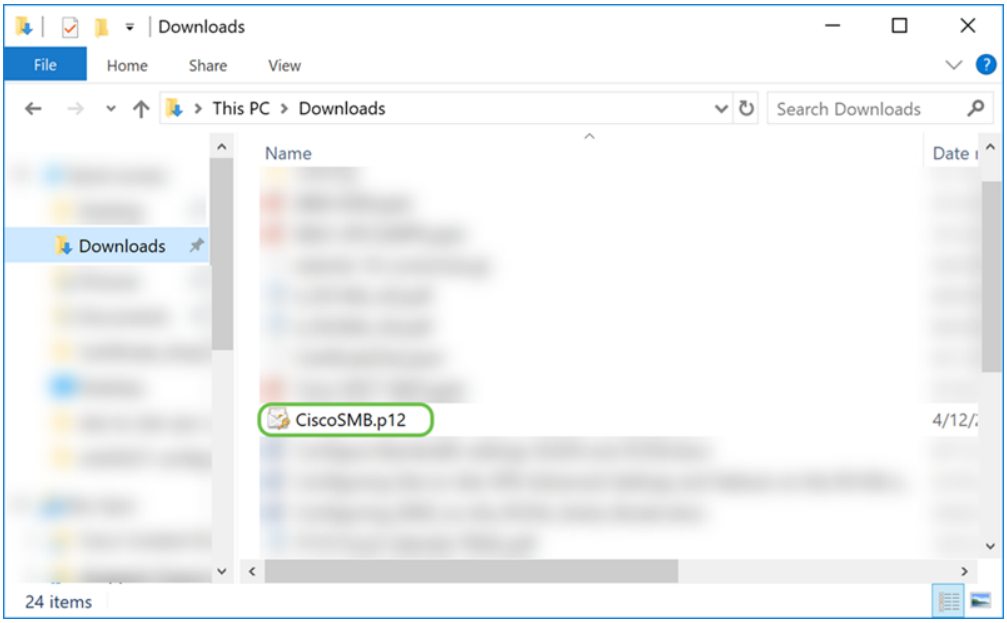


الخطوة 3. سوف يظهر إطار يطلب ما يجب القيام به مع هذا الملف. في هذا المثال، سنقوم بتحديد **حفظ الملف** ثم انقر فوق **موافق**.



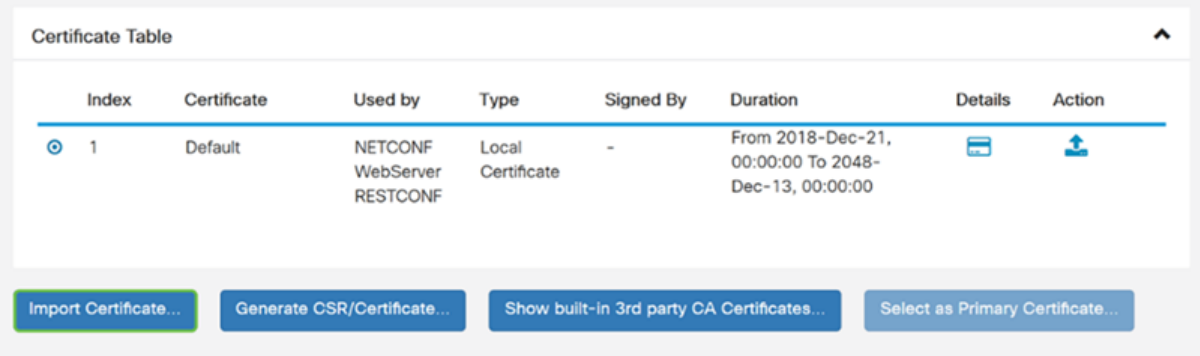
الخطوة 4. يجب حفظ الملف في موقع الحفظ الافتراضي الخاص بك.

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



إستيراد الشهادة

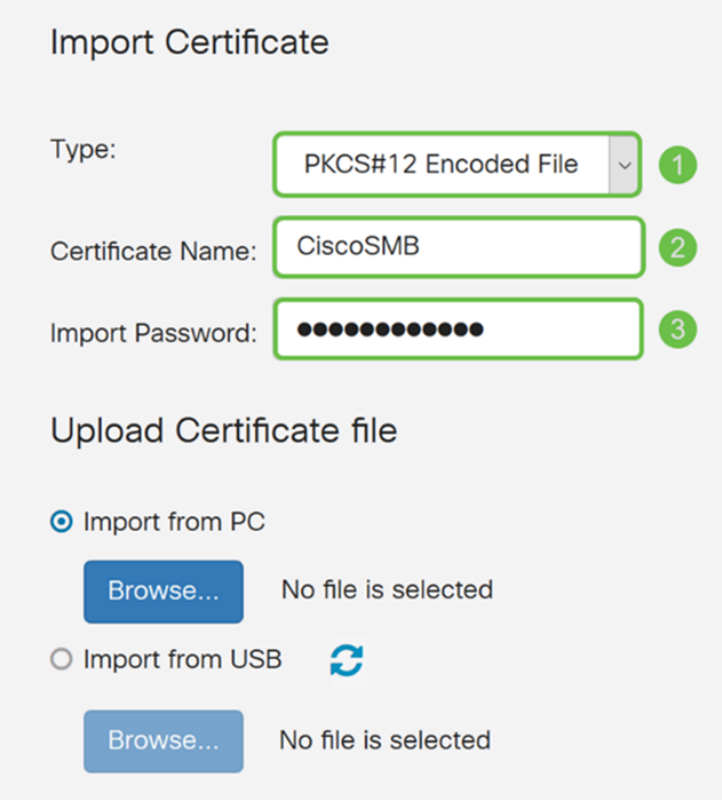
الخطوة 1. في صفحة *الترخيص*، انقر على **زر إستيراد شهادة...**



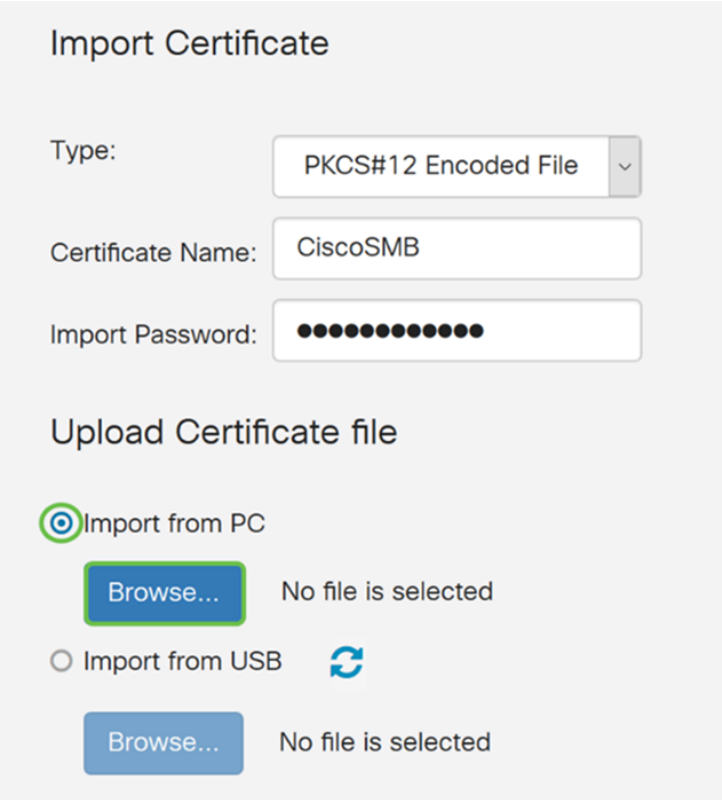
الخطوة 2. حدد **نوع** الشهادة التي سيتم إستيرادها من القائمة المنسدلة *النوع* أسفل قسم *إستيراد شهادة*. يتم تعريف الخيارات على أنها:

- **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.

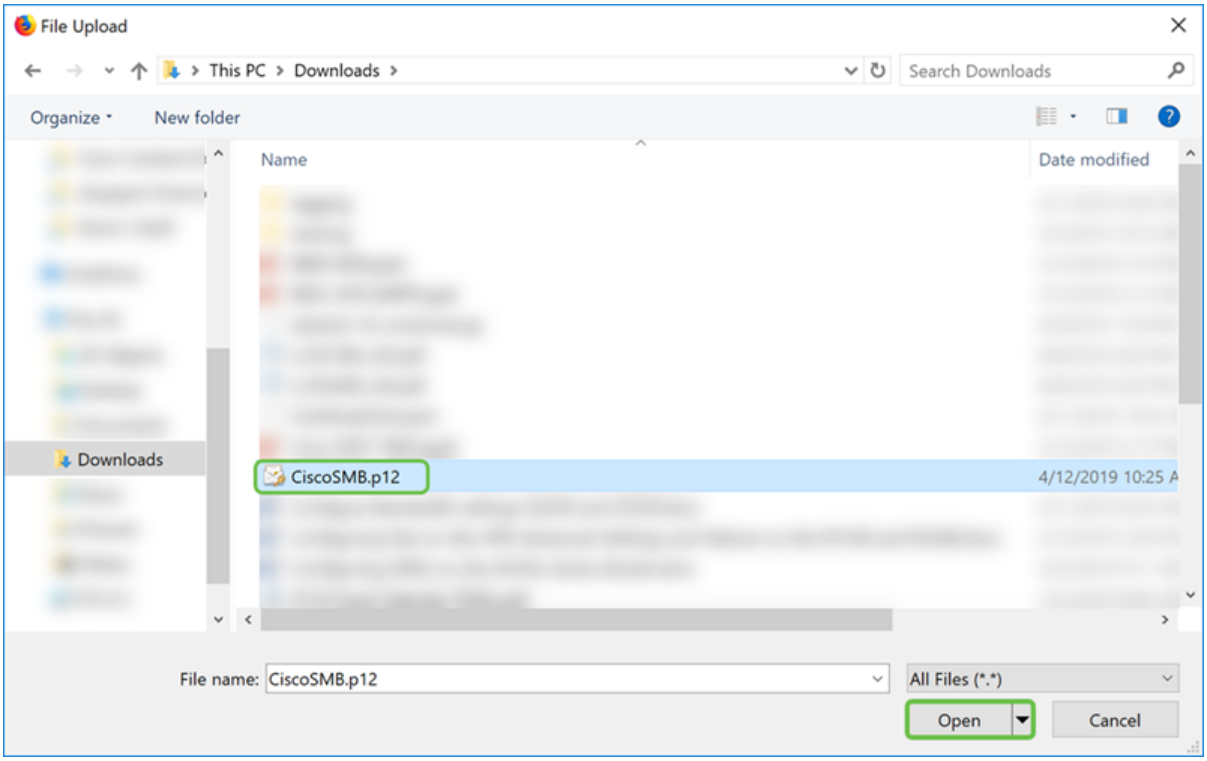
في هذا المثال، تم تحديد **ملف PKCS#12 المشفر** كنوع. أدخل **اسما** للشهادة ثم أدخل **كلمة المرور** التي تم إستخدامها.



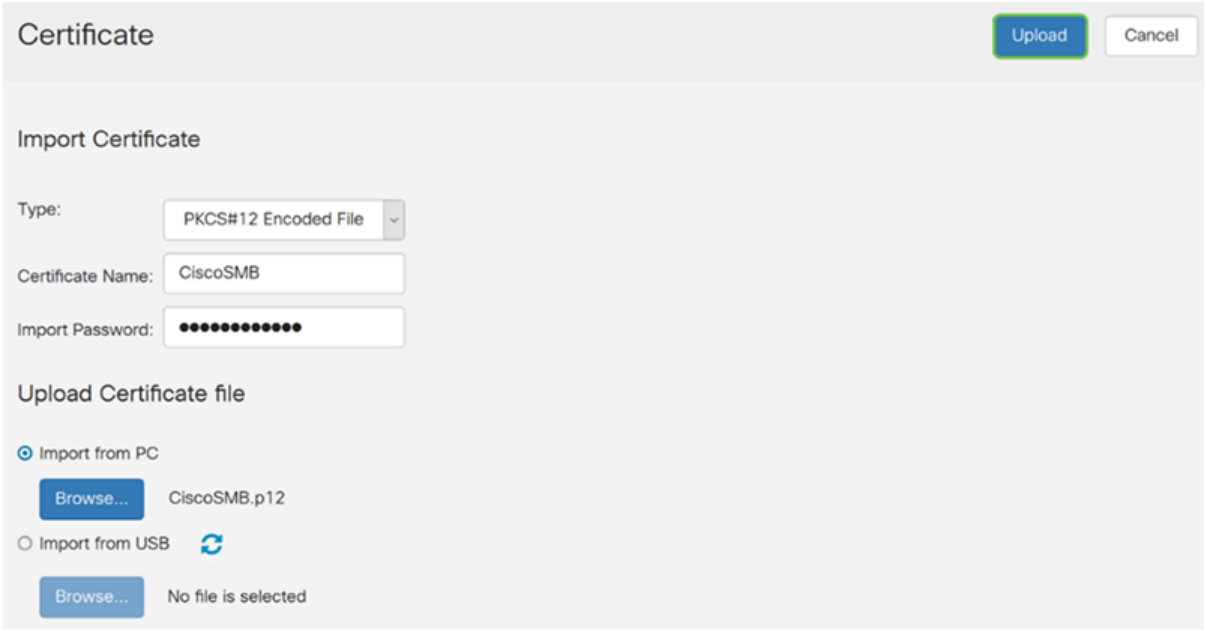
الخطوة 3. تحت قسم *تحميل ملف الشهادة*، حدد إما **إستيراد من الكمبيوتر الشخصي** أو **إستيراد من USB**. في هذا المثال، تم تحديد **إستيراد من الكمبيوتر الشخصي**. انقر فوق **إستعراض..** لاختيار ملف لتحميله.



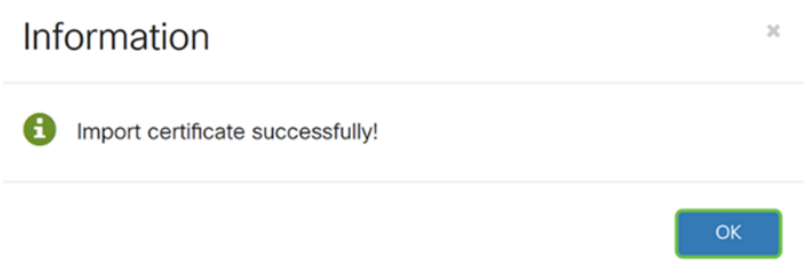
الخطوة 4. في نافذة *تحميل الملف*، انتقل إلى موقع موقع موقع ملف PKCS#12 المشفر (.p12). حدد ملف **p12.** ثم انقر **فتح**.



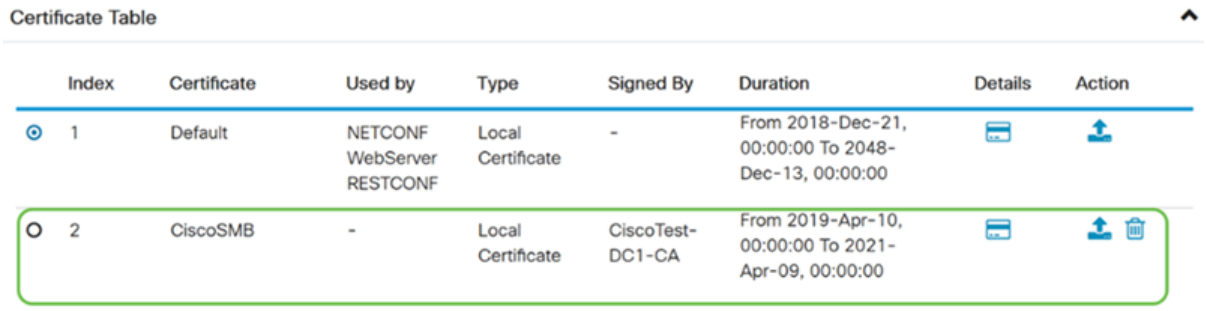
الخطوة 5. انقر على **تحميل** لبدء تحميل الشهادة.



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



الخطوة 7. يجب أن ترى أن شهادتك تم تحميلها.



القرار

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).