تثبيت وتجديد الشهادات على ASA المدارة من قبل ASDM

المحتويات

الأسئلة المتكررة

المقدمة

يوضح هذا المستند كيفية طلب أنواع معينة من الشهادات على برنامج Cisco ASA المدار باستخدام ASDM وتثبيتها وتوثيقها وتجديدها.

المتطلبات الأساسية

المتطلبات

- قبل البدء في التحقق من أن جهاز الأمان القابل للتكيف (ASA) يتوفر عليه وقت الساعة والتاريخ والمنطقة الزمنية الصحيحة. مع مصادقة الشهادة، يوصى باستخدام خادم بروتوكول وقت الشبكة (NTP) لمزامنة الوقت على ASA. تحقق من المعلومات ذات الصلة للمرجع.
- لطلب شهادة تستخدم طلب توقيع الشهادة (CSR)، يلزم أن يكون لها وصول إلى مرجع مصدق داخلي أو جهة خارجية موثوق بها. تشمل أمثلة بائعي CA التابعين لجهة خارجية، على سبيل المثال لا الحصر، Entrust و Geotrust و GoDaddy و Thawte و VeriSign.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASAv 9.18.1
- لإنشاء PKCS12، يتم إستخدام OpenSSL.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

نوع الشهادات التي عنونين هذا المستند هي:

- شهادات موقعة ذاتيا
- الشهادات الموقعة من قبل هيئة شهادة تابعة لجهة خارجية أو مرجع مصدق داخلي

يشترط خادم طبقة مأخذ التوصيل الآمنة (SSL) وأمان طبقة النقل (TLS) و IKEv2 RFC7296 لبروتوكولات مصادقة EAP أن يوفر العميل شهادة خادم ليقوم العميل بمصادقة الخادم. يوصى باستخدام CAs التابعة لجهة خارجية موثوق بها لإصدار شهادات SSL إلى ASA لهذا الغرض.

لا توصي Cisco باستخدام شهادة موقعة ذاتيا بسبب احتمال أن يقوم المستخدم بتكوين مستعرض عن غير قصد ليثق في شهادة من خادم مخادع. هناك أيضا إزعاج للمستخدمين للإستجابة إلى تحذير أمان عند إتصاله بالبوابة الآمنة.

طلب شهادة هوية جديدة مع ASDM وتثبيتها

يمكن طلب شهادة من مرجع مصدق وتثبيتها على ASA بطريقتين:

- إستخدام طلب توقيع الشهادة (CSR). قم بإنشاء زوج مفاتيح، وطلب شهادة هوية من CA باستخدام CSR، وتثبيت شهادة الهوية الموقعة التي تم الحصول عليها من CA.
- أستخدم ملف PKCS12 الذي تم الحصول عليه من CA، أو تم تصديره من جهاز مختلف. يحتوي ملف PKCS12 على زوج مفاتيح، شهادة هوية، شهادة (شهادات) CA.

طلب وتثبيت شهادة هوية جديدة مع طلب توقيع الشهادة (CSR)

يتم إنشاء CSR على الجهاز الذي يحتاج إلى شهادة هوية، أستخدم زوج مفاتيح تم إنشاؤه على الجهاز.

يحتوي CSR على:

- معلومات طلب الشهادة - الموضوع المطلوب والسمات الأخرى، المفتاح العام من زوج المفاتيح،
- معلومات خوارزمية التوقيع،
- التوقيع الرقمي لمعلومات طلب الترخيص، الموقع بالمفتاح الخاص من زوج المفاتيح.

يتم تمرير CSR إلى المرجع المصدق (CA)، حتى يتم توقيعه، في نموذج PKCS#10.

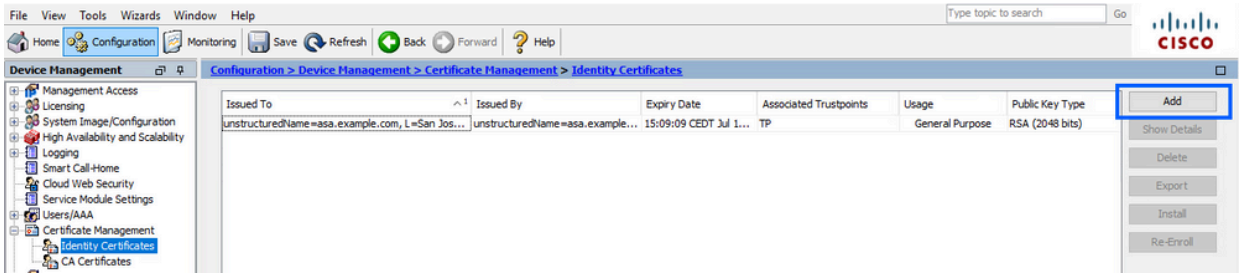
يتم إرجاع الشهادة الموقعة من CA في نموذج PEM.

ملاحظة: يمكن ل CA تغيير معلمات FQDN واسم الموضوع المحددة في TrustPoint عند توقيعها على CSR وإنشاء شهادة هوية موقعة.

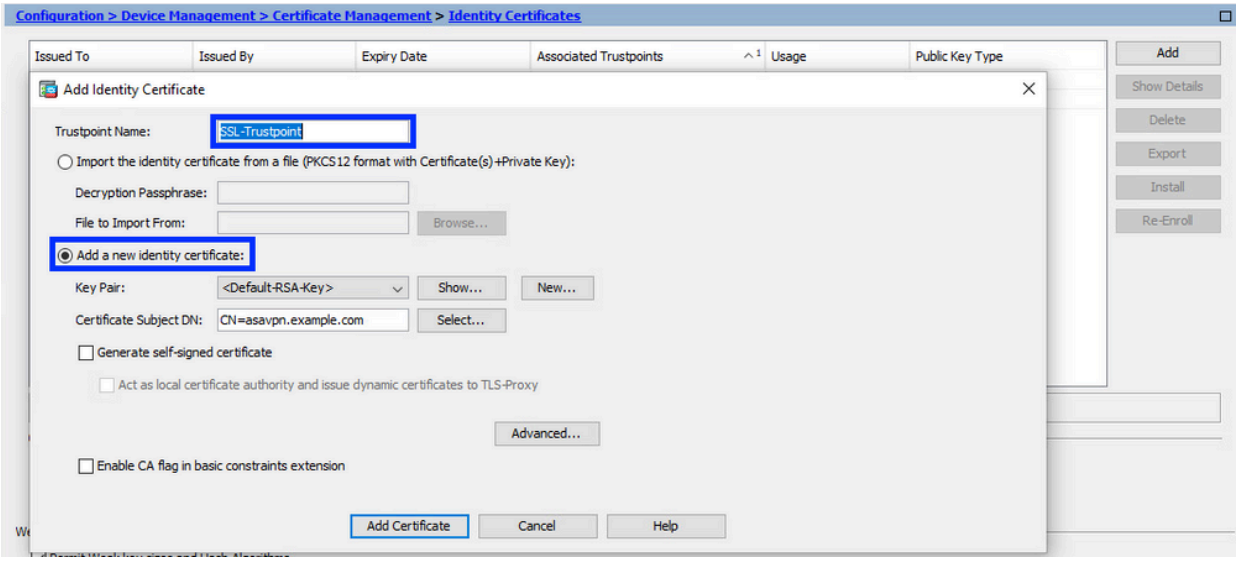
إنشاء CSR باستخدام ASDM

1. إنشاء TrustPoint باسم محدد

   a. انتقل إلى التكوين > إدارة الأجهزة >إدارة الشهادات > شهادات الهوية.



   b. انقر فوق إضافة (Add).
   c. قم بتحديد اسم TrustPoint.



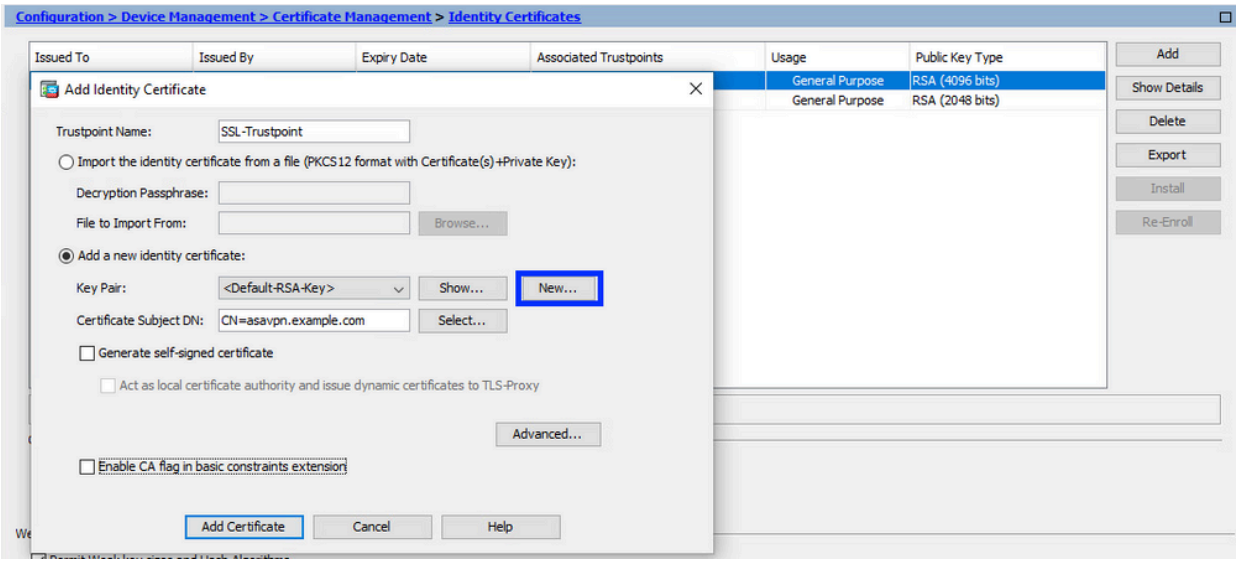
d. انقر على زر إضافة شهادة هوية جديدة.

2. (إختياري) قم بإنشاء زوج مفاتيح جديد

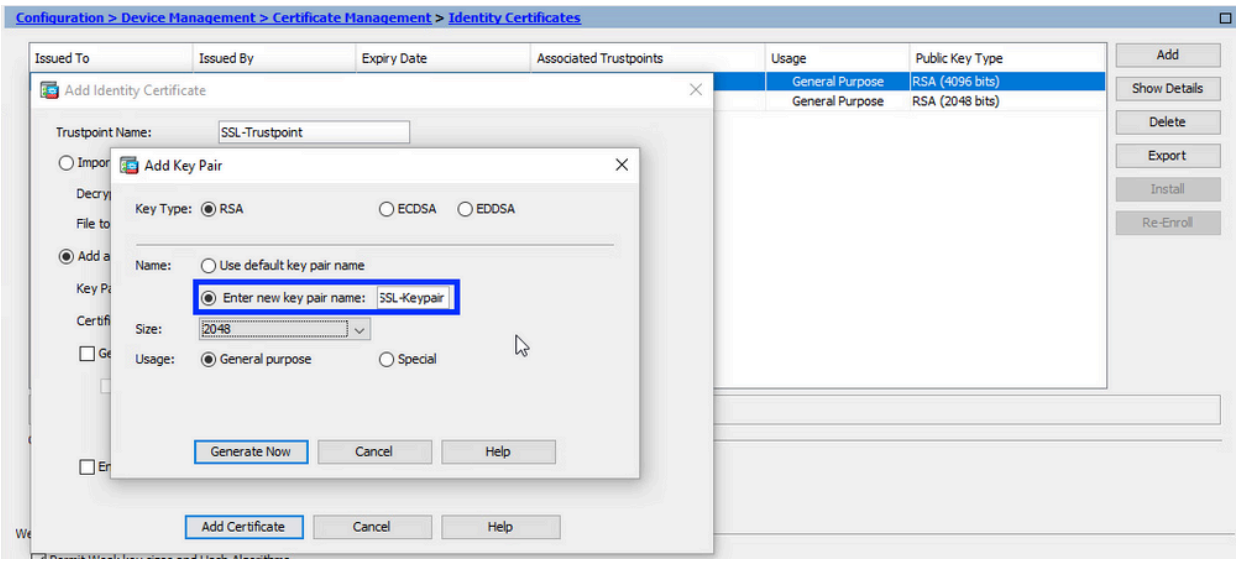
ملاحظة: يتم إستخدام مفتاح RSA باسم Default-RSA-Key وحجم 2048 بشكل افتراضي، ومع ذلك، يوصى باستخدام زوج مفاتيح خاص/عام فريد لكل شهادة هوية.

---

a. انقر فوق جديد لإنشاء زوج مفاتيح جديد.

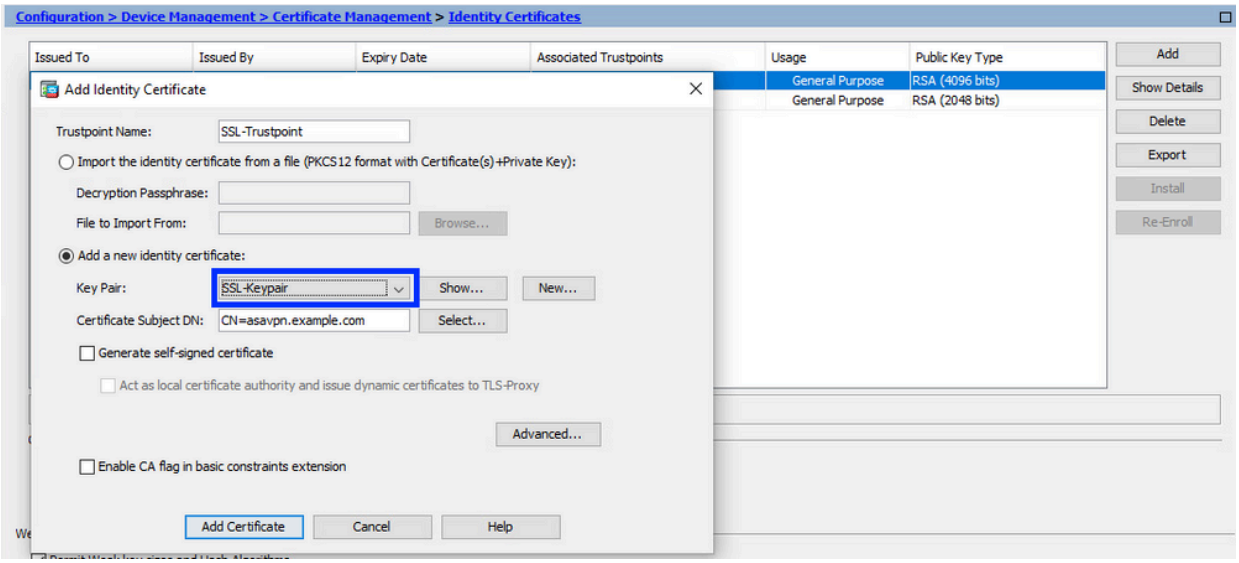


b. أختر الخيار إدخال اسم زوج مفاتيح جديد وأدخل اسم لزوج المفاتيح الجديد.
c. أختر نوع المفتاح - RSA أو ECDSA.
d. أختر حجم المفتاح؛ ل RSA، أختر الغرض العام للاستخدام.
e. انقر فوق إنشاء الآن. يتم الآن إنشاء زوج المفاتيح.



3. أختر اسم زوج المفاتيح

أختر زوج المفاتيح لتوقيع CSR به، وليتم ربطه بالشهادة الجديدة.

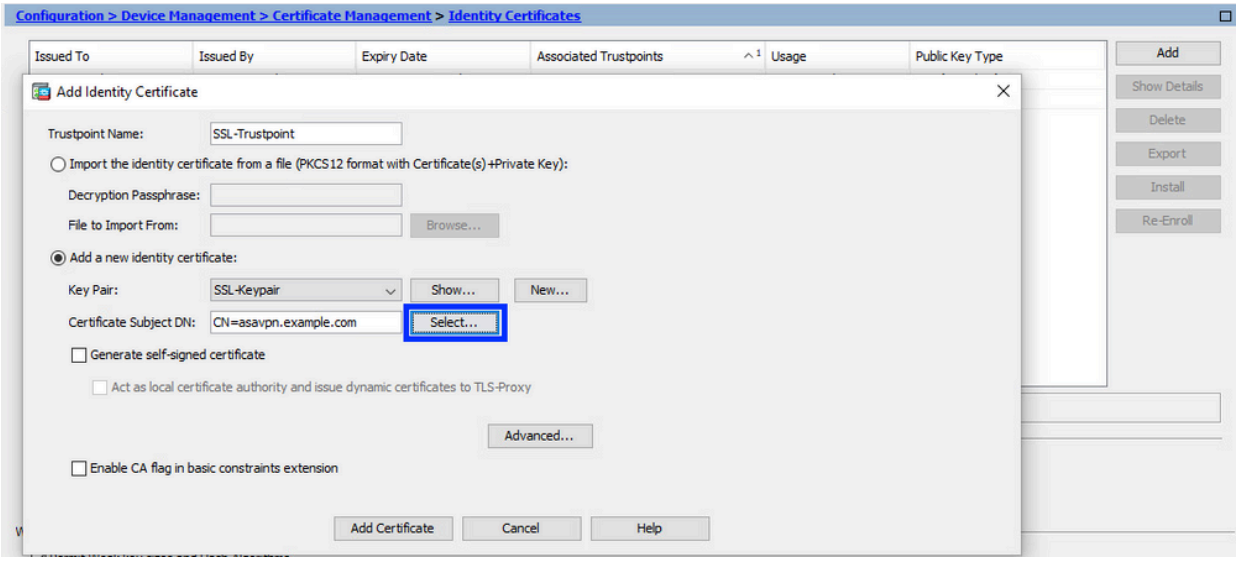


4. تكوين موضوع الشهادة واسم المجال المؤهل بالكامل (FQDN)

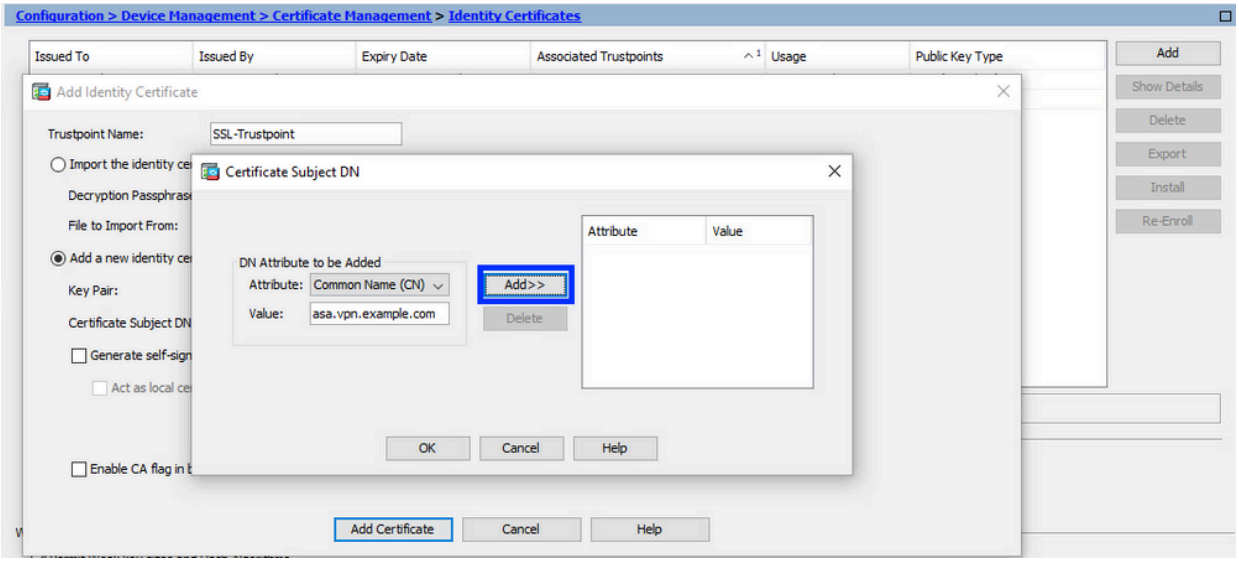
تحذير: يجب أن تطابق معلمة FQDN FQDN أو عنوان IP الخاص بواجهة ASA التي يتم إستخدام شهادة الهوية لها. تقوم هذه المعلمة بتعيين ملحق "الاسم البديل للموضوع" (SAN) المطلوب لشهادة الهوية. يتم إستخدام ملحق شبكة التخزين (SAN) من قبل عميل SSL/TLS/IKEv2 للتحقق مما إذا كانت الشهادة تطابق FQDN الذي تتصل به.

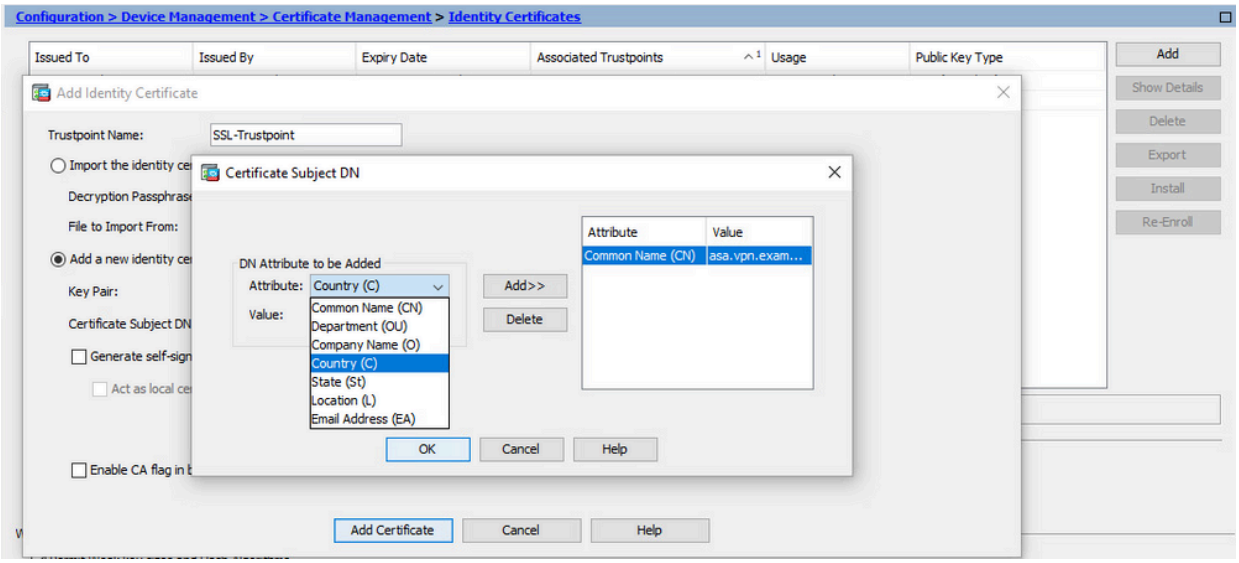
---

a. انقر فوق تحديد.



b. في نافذة عنوان الشهادة DN، قم بتكوين سمات الشهادة - أختر سمة من القائمة المنسدلة، أدخل القيمة، انقر على إضافة.



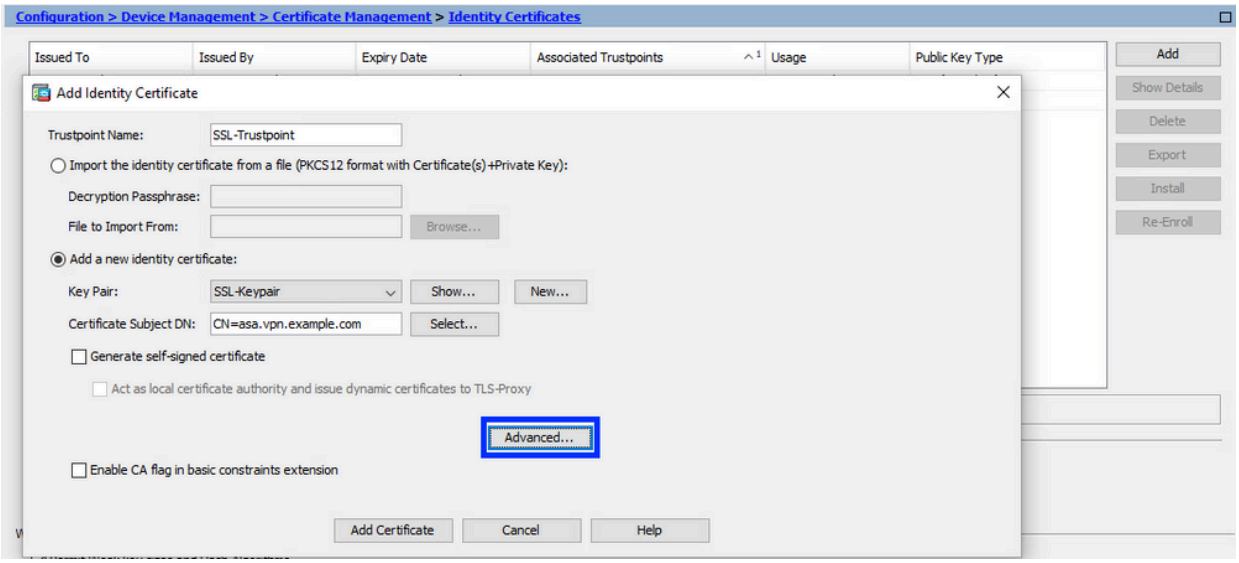


سمة	الوصف
سي إن	الاسم الذي يمكن الوصول من خلاله إلى جدار الحماية (عادة اسم المجال المؤهل بالكامل، على سبيل المثال، vpn.example.com).
أو	اسم القسم الخاص بك داخل المؤسسة
O	الاسم المسجل قانونيا لمؤسستك/شركتك
C	رمز البلد (رمز حرف بدون علامة ترقيم)
سانت	الحالة التي توجد فيها مؤسستك.
L	المدينة التي تقع فيها مؤسستك.
آي إيه	عنوان البريد الإلكتروني

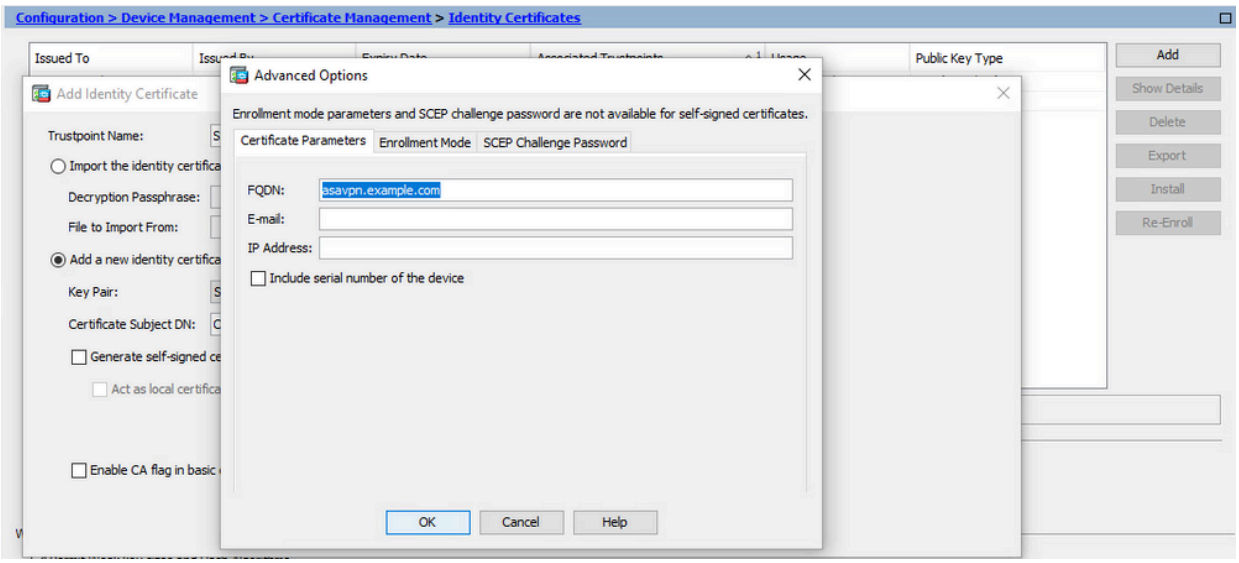
ملاحظة: لا يمكن لأي من قيم الحقول السابقة أن تتجاوز حد 64 حرفا. قد تتسبب القيمة الأطول في حدوث مشاكل في تثبيت شهادة الهوية. أيضا، ليس من الضروري أن تقوم بتعريف كل سمات DN.

انقر فوق موافق بعد إضافة كافة السمات.

c. قم بتكوين FQDN للجهاز - انقر فوق خيارات متقدمة.

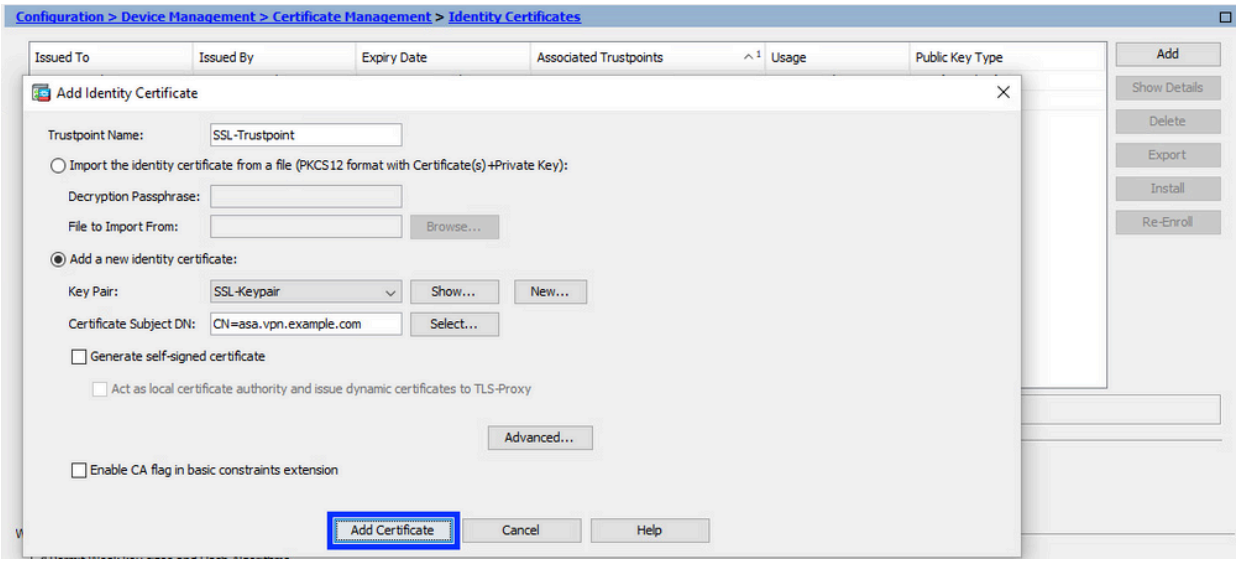


d. في حقل FQDN، أدخل اسم المجال المؤهل بالكامل الذي يمكن من خلاله الوصول إلى الجهاز من الإنترنت. وانقر فوق OK.

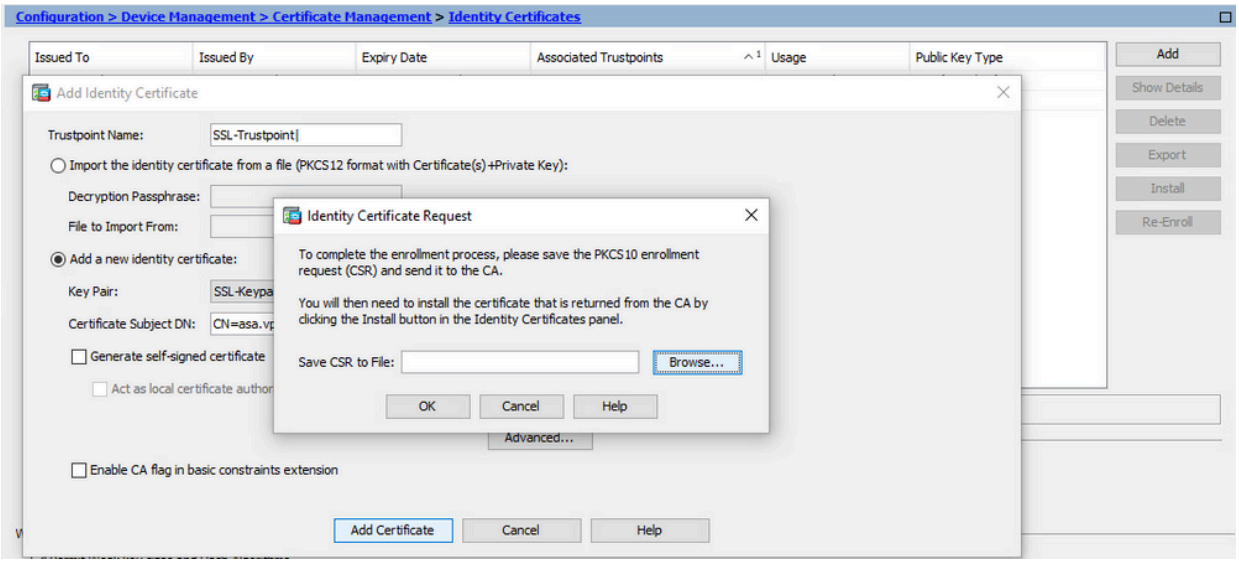


5. إنشاء CSR وحفظه

a. انقر على إضافة شهادة.



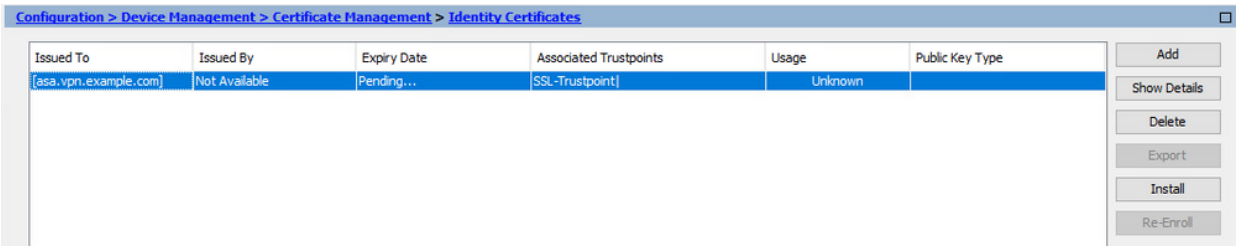
b. تظهر نافذة مطالبة لحفظ CSR إلى ملف على الجهاز المحلي.



انقر فوق إستعراض، أختر موقعا لحفظ CSR فيه، ثم احفظ الملف بامتداد .txt.

> ملاحظة: عند حفظ الملف بامتداد .txt، يمكن فتح طلب PKCS#10 وعرضه باستخدام محرر نصوص (مثل Notepad).

c. يتم الآن عرض TrustPoint الجديد في حالة معلق.

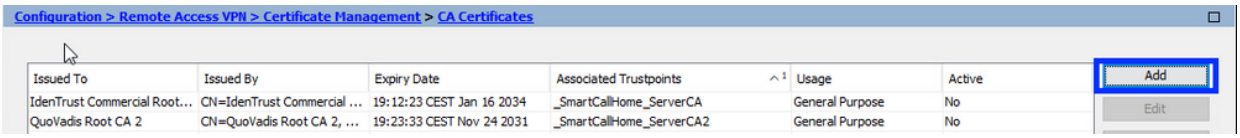


تثبيت شهادة الهوية بتنسيق PEM باستخدام ASDM

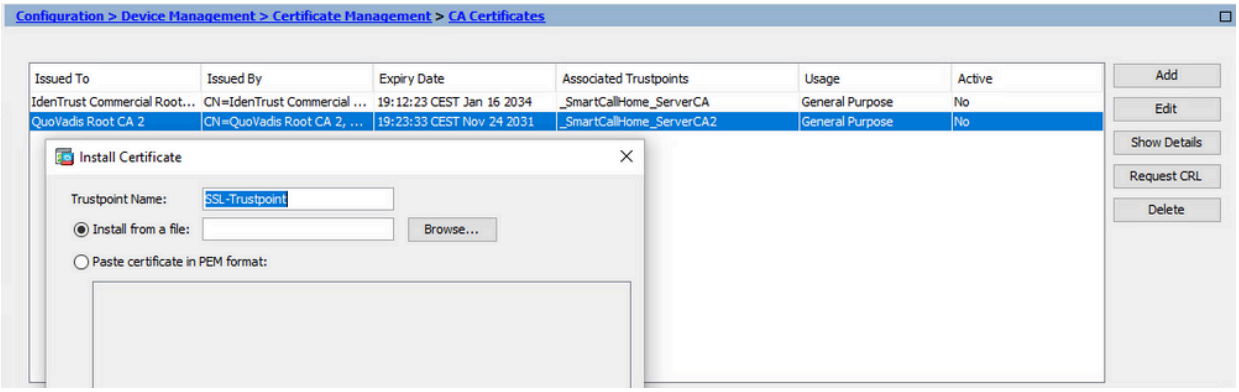
يفترض خطوات التثبيت أن CA وقع على CSR، وقدم شهادة هوية مرمزة بترميز PEM (.pem، .cer، .crt) وحزمة شهادة CA.

1. تثبيت شهادة CA التي وقعت على CSR

a. انتقل إلى التكوين > إدارة الأجهزة >إدارة الشهادات >، واختر شهادات CA. انقر فوق إضافة (Add).

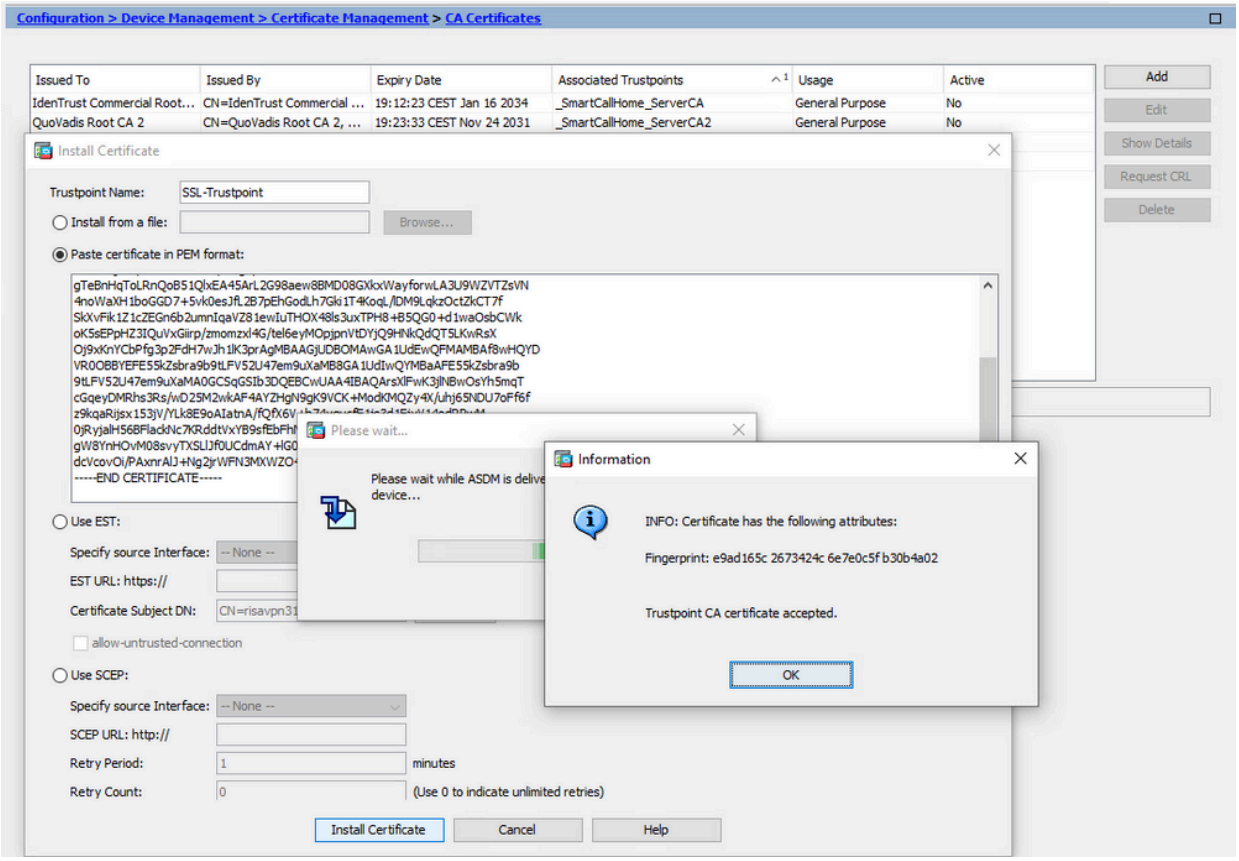


b. أدخل اسم TrustPoint وحدد تثبيت من ملف، وانقر على زر إستعراض، وحدد الشهادة الوسيطة. بدلا من ذلك، قم بلصق شهادة مرجع مصدق (CA) مرمزة بترميز PEM من ملف نصي في حقل النص.



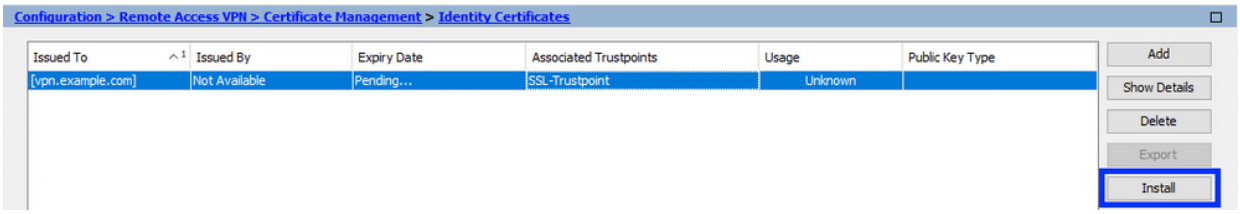
> ملاحظة: قم بتثبيت شهادة CA التي وقعت على CSR، واستخدم نفس اسم نقطة الثقة مثل شهادة الهوية. يمكن تثبيت شهادات المرجع المصدق الأخرى الأعلى في التدرج الهرمي ل PKI في نقاط الثقة المنفصلة.

c. انقر على تثبيت الشهادة.



2. تثبيت شهادة الهوية

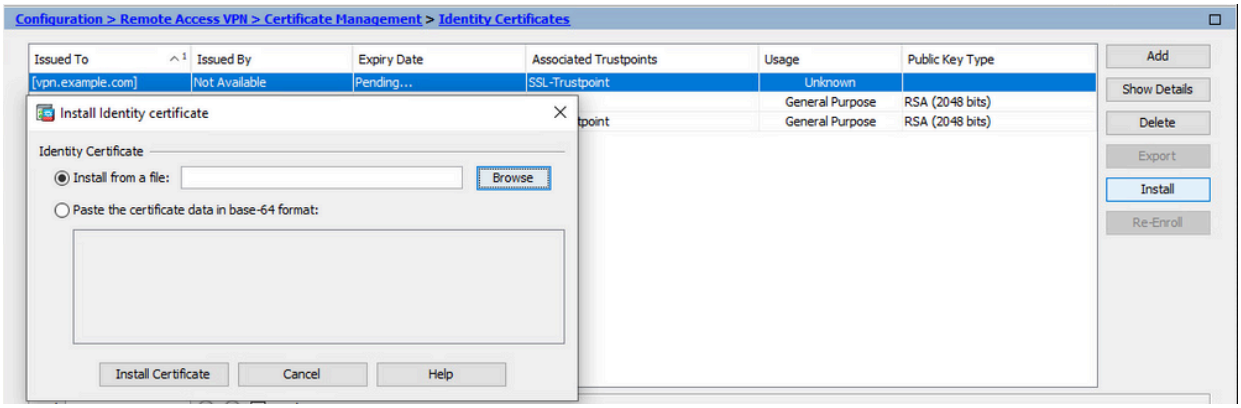
a. أختر شهادة الهوية التي تم إنشاؤها مسبقا أثناء إنشاء CSR. انقر على تثبيت.



ملاحظة: يمكن أن تكون شهادة الهوية قد تم إصدارها بواسطة الحقل غير متوفر وحقل تاريخ انتهاء الصلاحية كحقل معلق.

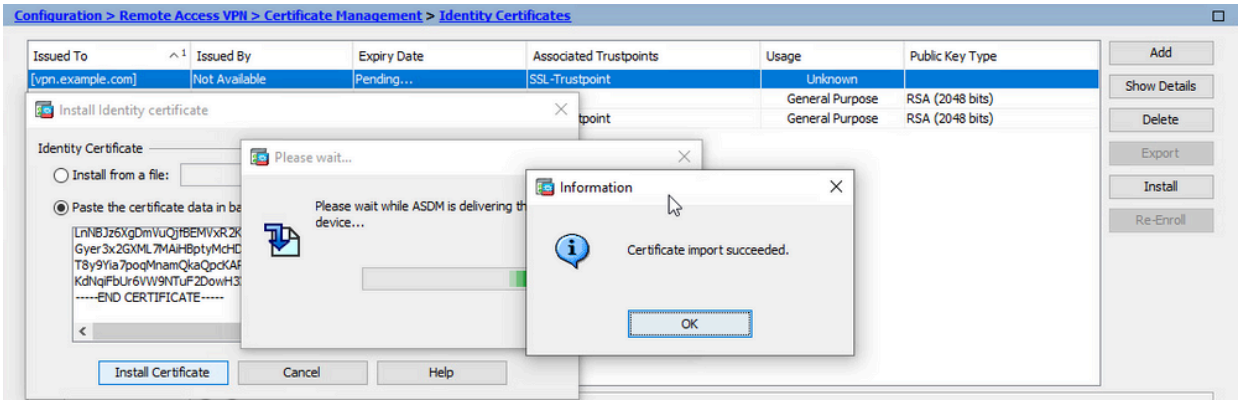
---

b. أختر ملف يحتوي على شهادة تعريف PEM المرمزة المستلمة من المرجع المصدق، أو افتح شهادة PEM المرمزة في محرر نص وانسخ/لصق شهادة الهوية المقدمة من المرجع المصدق في حقل النص.



ملاحظة: يمكن أن تكون شهادة الهوية بتنسيق .pem، .cer، .crt للتثبيت.

c. انقر على تثبيت الشهادة.



3. ربط الشهادة الجديدة بالواجهة باستخدام ASDM

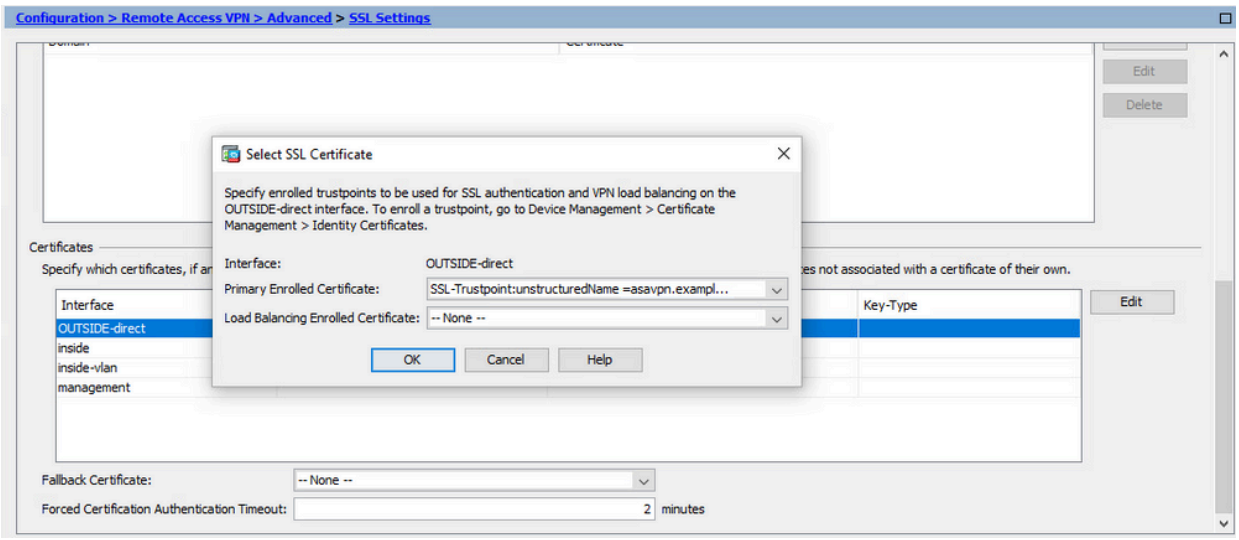
يجب تكوين ASA لاستخدام شهادة الهوية الجديدة لجلسات عمل WebVPN التي تنتهي على الواجهة المحددة.

a. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > Advanced (خيارات متقدمة) > إعدادات SSL.

b. تحت شهادات، أختر الواجهة التي يتم إستخدامها لإنهاء جلسات عمل WebVPN. في هذا المثال، يتم إستخدام الواجهة الخارجية.

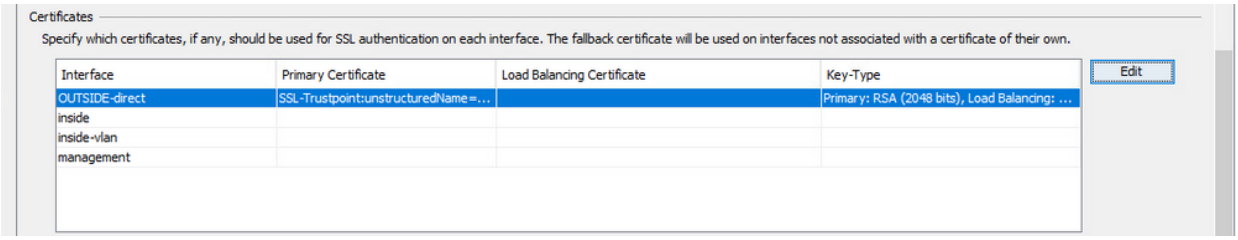
انقر فوق تحرير.

c. في القائمة المنسدلة ترخيص، أختر الشهادة المثبتة حديثا.



d. وانقر فوق OK.

e. طقطقة يطبق.



شهادة الهوية الجديدة قيد الاستخدام الآن.

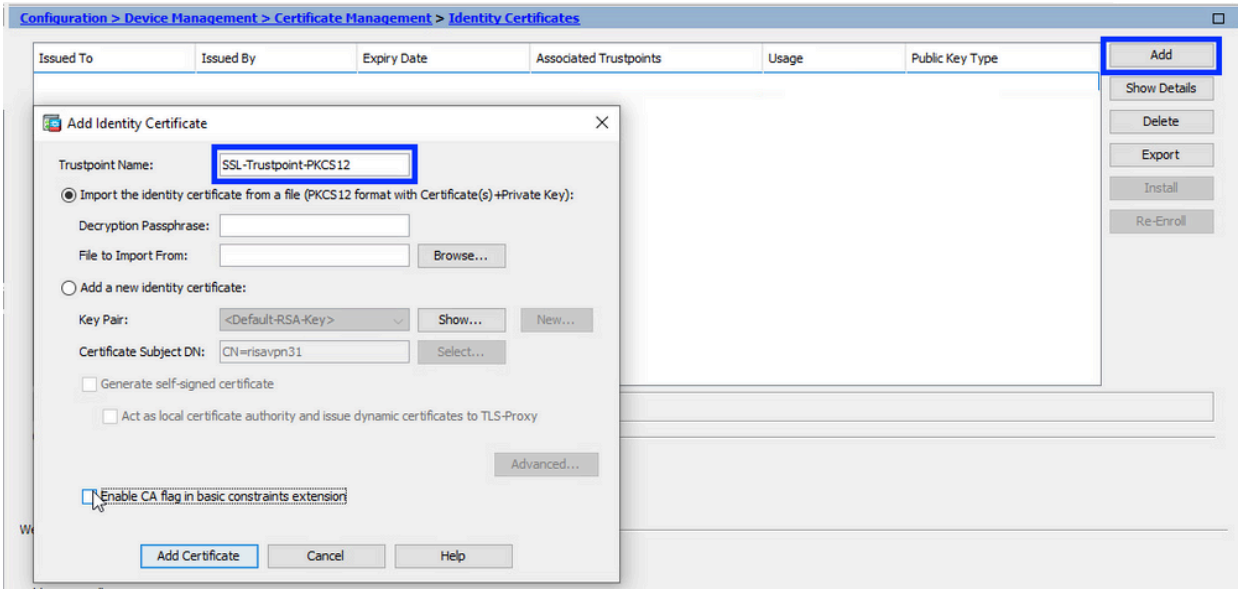
تثبيت شهادة هوية مستلمة بتنسيق PKCS12 باستخدام ASDM

يحتوي ملف PKCS12 (.p12 أو .pfx) على شهادة هوية، زوج مفاتيح، وشهادة (شهادات) CA. يتم إنشاؤها بواسطة المرجع المصدق، على سبيل المثال في حالة شهادة حرف البدل، أو تصديرها من جهاز مختلف. وه ملف ثنائي، لا يمكن عرضه باستخدام محرر نص.

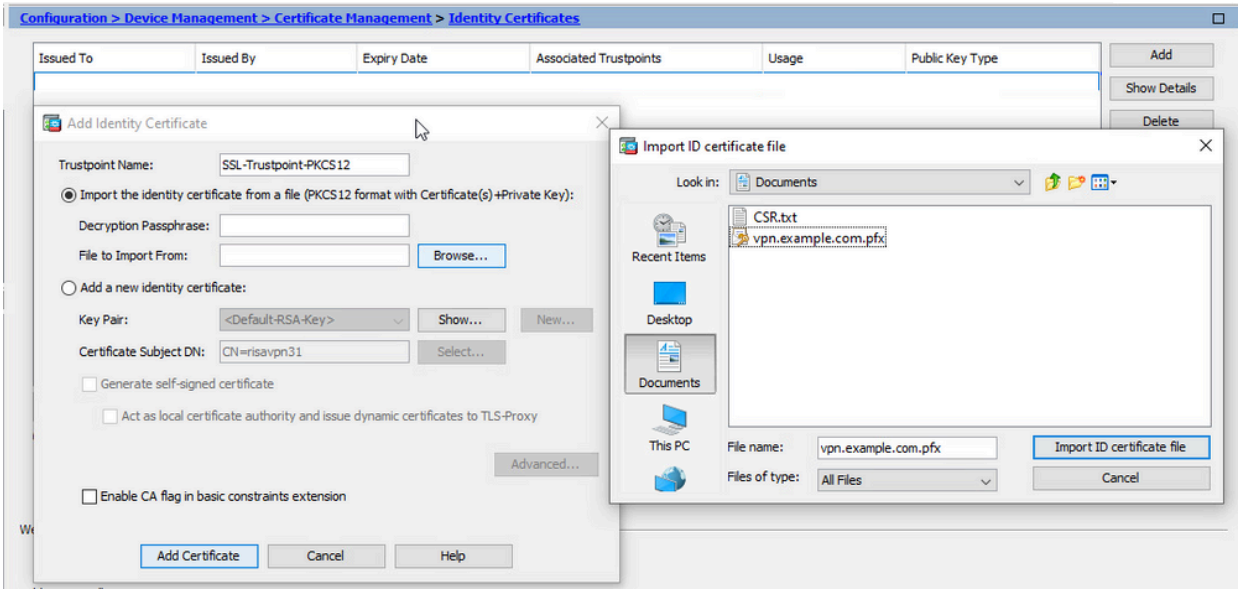
1. ثبت الهوية وشهادات المرجع المصدق من ملف PKCS12

يلزم تجميع شهادة الهوية وشهادة (شهادات) المرجع المصدق (CA) وزوج المفاتيح في ملف PKCS12 واحد.

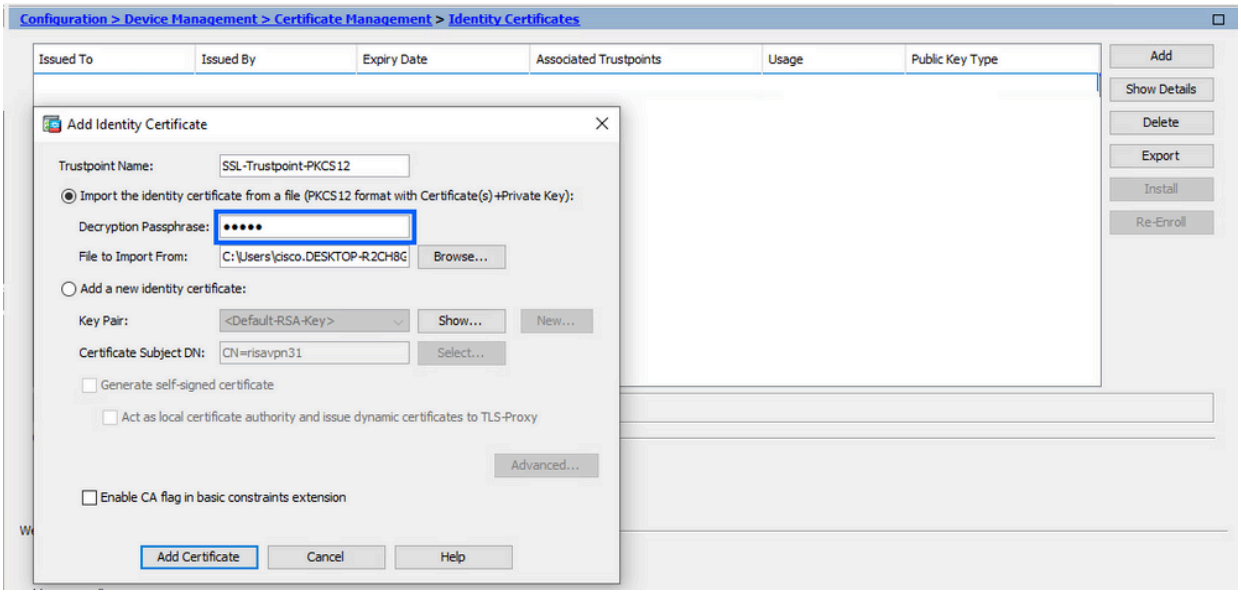
a. انتقل إلى التكوين > إدارة الأجهزة > إدارة الشهادات، واختر شهادات الهوية.
b. انقر فوق إضافة (Add).
c. حدد اسم TrustPoint.



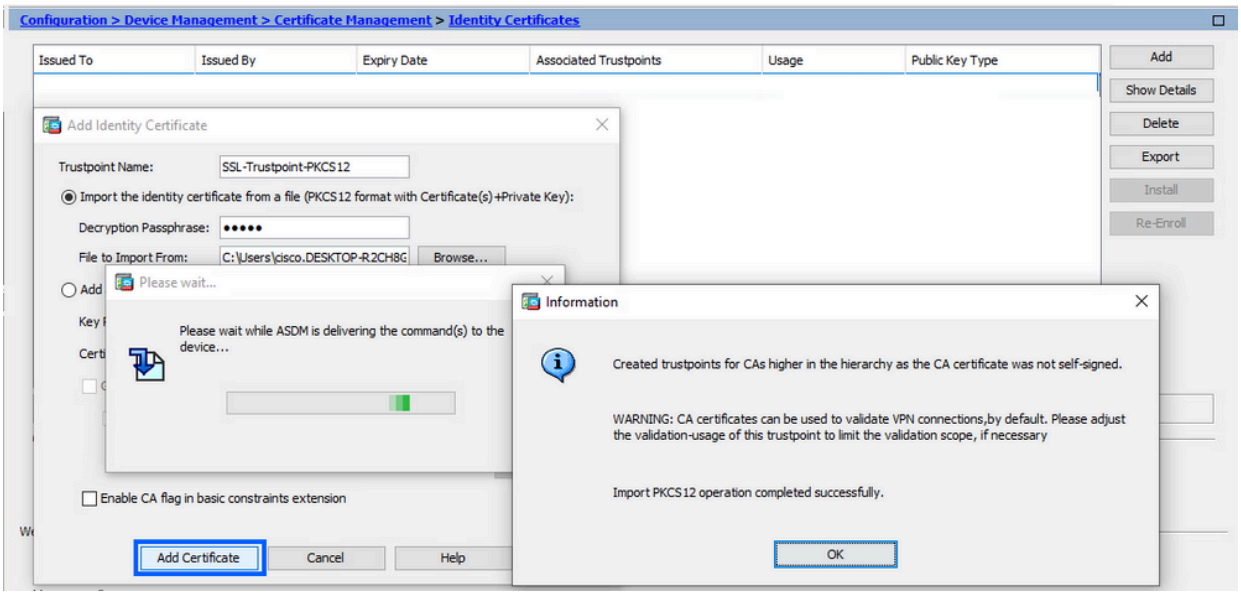
d. انقر على زر إدراج شهادة الهوية من مرجع ملف.



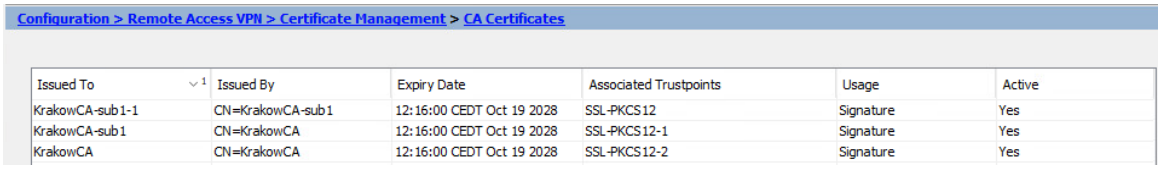
e. أدخل عبارة المرور المستخدمة لإنشاء ملف PKCS12.



f. انقر على إضافة شهادة.



ملاحظة: عندما تقوم باستيراد PKCS12 مع سلسلة شهادات CA، يقوم ASDM بإنشاء نقاط ثقة CA للتدفق تلقائيا مع أسماء ذات لاحقة مضافة -number.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. ربط الشهادة الجديدة بالواجهة باستخدام ASDM

يجب تكوين ASA لاستخدام شهادة الهوية الجديدة لجلسات عمل WebVPN التي تنتهي على الواجهة المحددة.

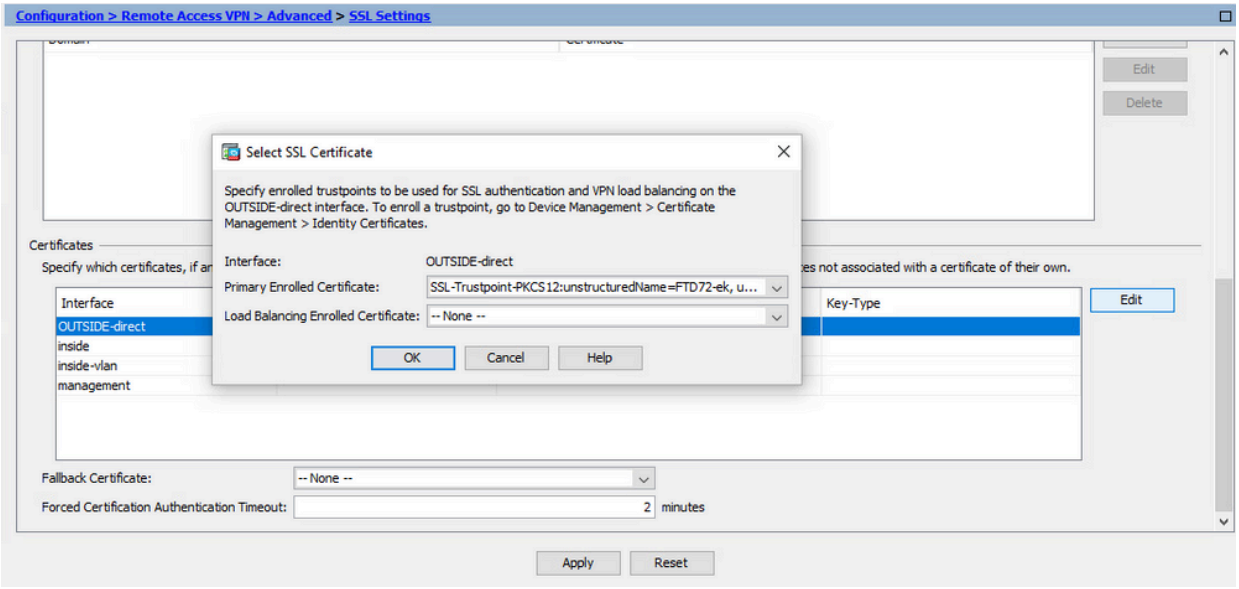
a. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > Advanced (خيارات

متقدمة) > إعدادات SSL.

b. تحت شهادات، حدد الواجهة التي يتم إستخدامها لإنهاء جلسات عمل WebVPN. في هذا المثال، يتم إستخدام الواجهة الخارجية.

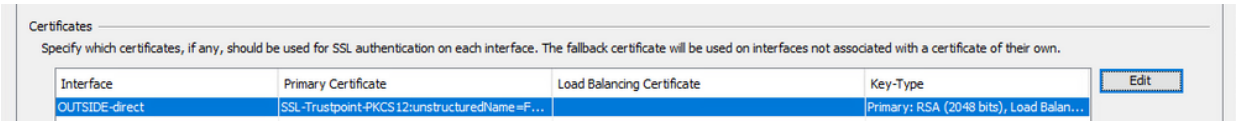
انقر فوق تحرير.

c. في القائمة المنسدلة ترخيص، أختر الشهادة المثبتة حديثا.



d. وانقر فوق OK.

e. طقطقة يطبق.



شهادة الهوية الجديدة قيد الاستخدام الآن.

تجديد الشهادة

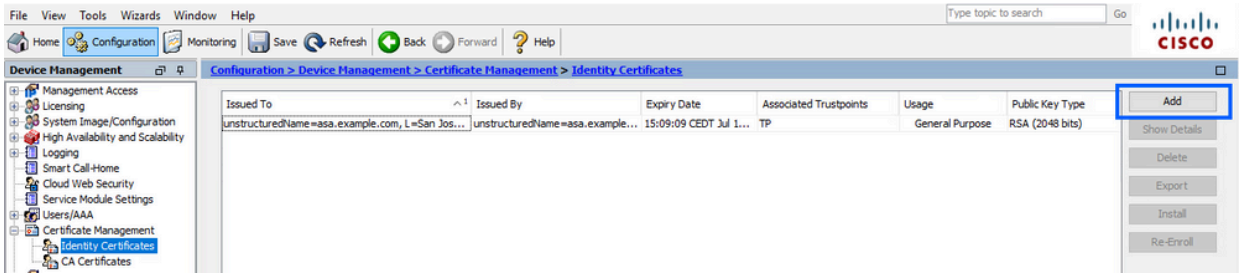
تجديد شهادة مسجلة مع طلب توقيع الشهادة (CSR) باستخدام ASDM

يتطلب تجديد الشهادة المسجلة في CSR إنشاء TrustPoint جديد وتسجيله. يجب أن يكون له اسم مختلف (على سبيل المثال، الاسم القديم مع لاحقة سنة التسجيل). يمكن أن يستخدم نفس المعلمات وزوج المفاتيح مثل الشهادة القديمة، أو يمكن أن يستخدم أخرى مختلفة.

إنشاء CSR باستخدام ASDM

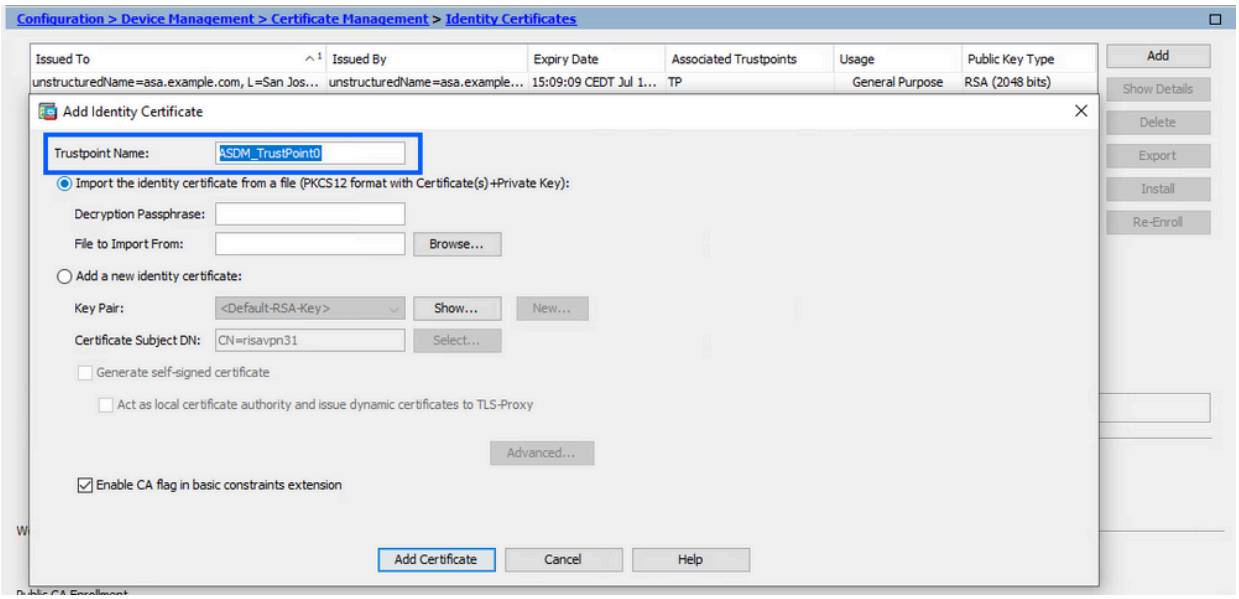
1. إنشاء TrustPoint جديد باسم محدد.

a. انتقل إلى التكوين > إدارة الأجهزة >إدارة الشهادات > شهادات الهوية.



b. انقر فوق إضافة (Add).

c. قم بتحديد اسم TrustPoint.



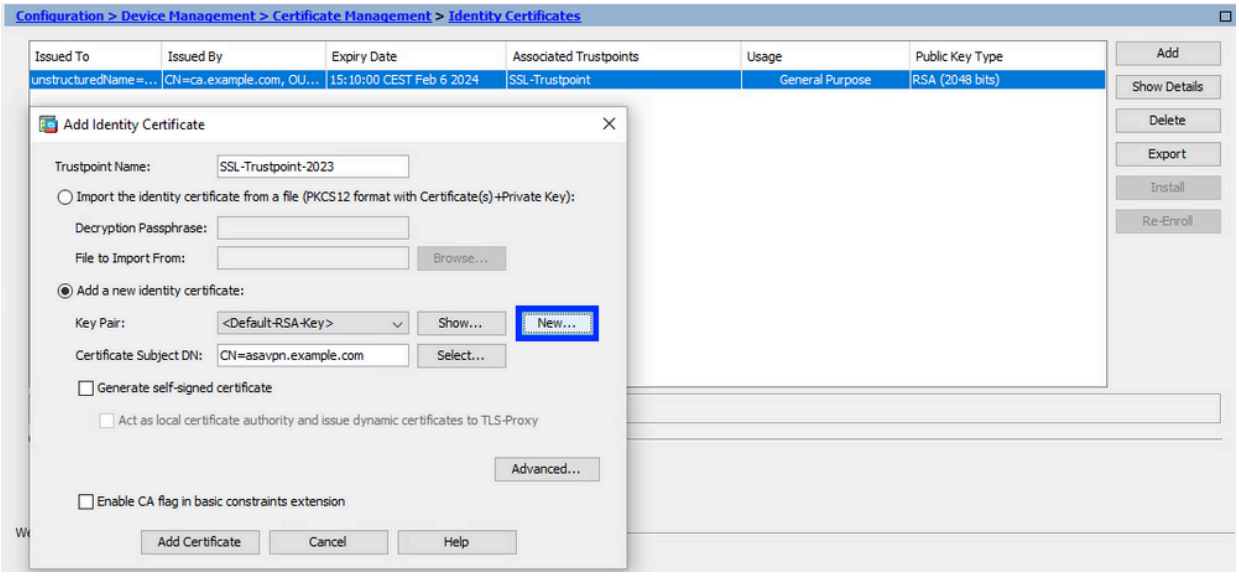
d. انقر على زر إضافة شهادة هوية جديدة.

2. (إختياري) قم بإنشاء زوج مفاتيح جديد

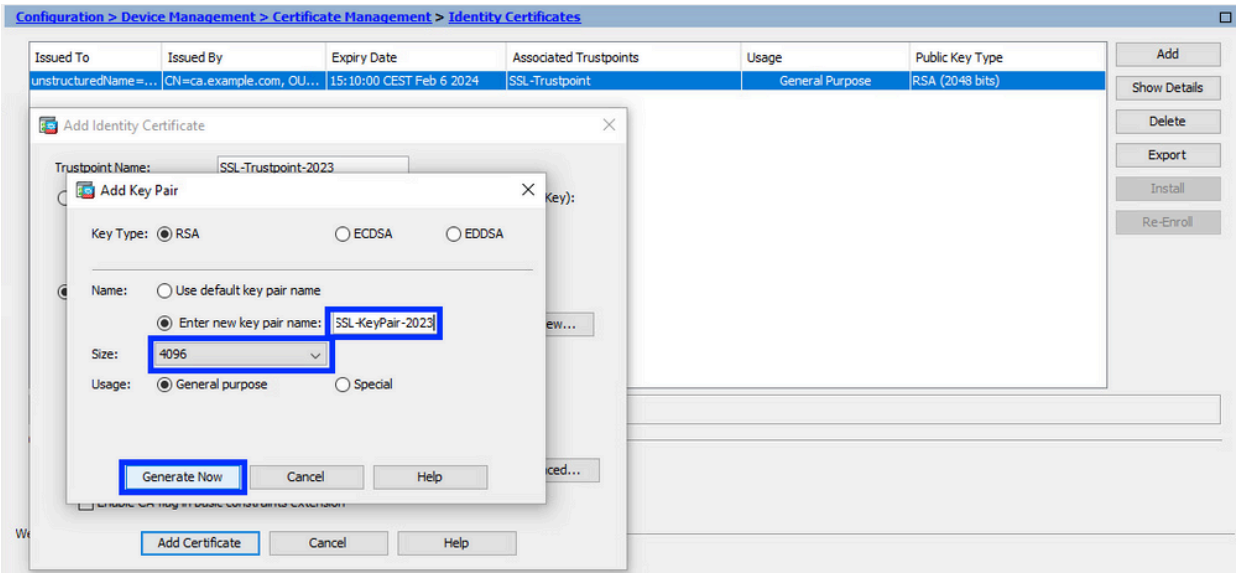
ملاحظة: يتم إستخدام مفتاح RSA باسم Default-RSA-Key وحجم 2048 بشكل افتراضي، ومع ذلك، يوصى باستخدام زوج مفاتيح خاص/عام فريد لكل شهادة هوية.

---

a. انقر فوق جديد لإنشاء زوج مفاتيح جديد.

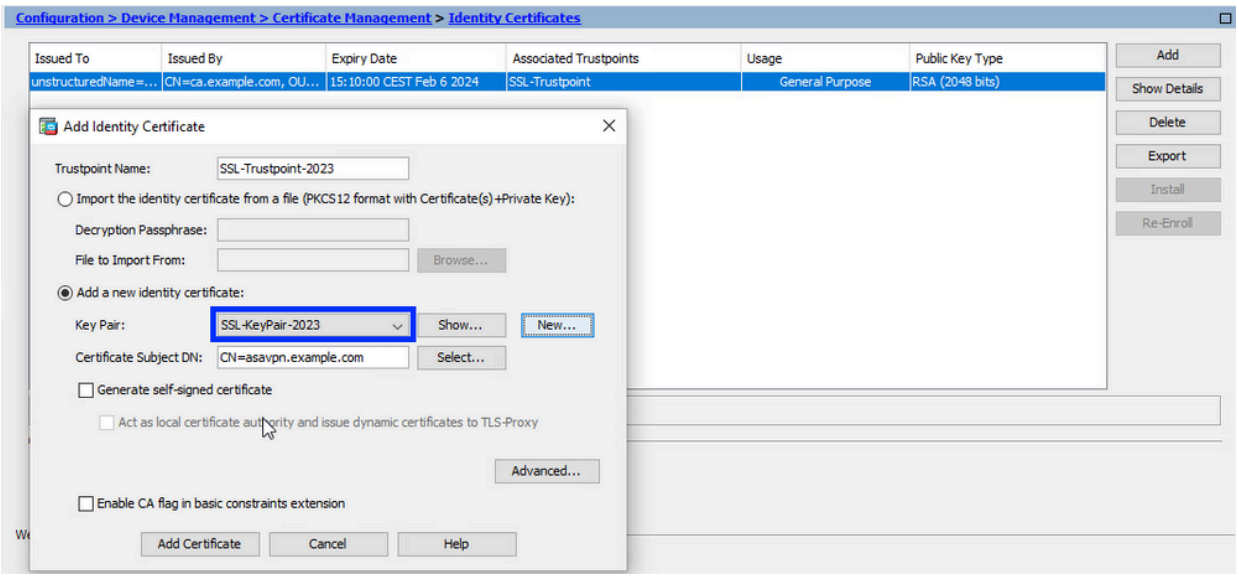


b. أختر الخيار إدخال اسم زوج مفاتيح جديد وإدخال اسم لزوج المفاتيح الجديد.
c. أختر نوع المفتاح - RSA أو ECDSA.
d. أختر حجم المفتاح؛ ل RSA، أختر الغرض العام للاستخدام.
e. انقر فوق إنشاء الآن. يتم الآن إنشاء زوج المفاتيح.



3. حدد اسم زوج المفاتيح

أختر زوج المفاتيح لتوقيع CSR به، وليتم ربطه بالشهادة الجديدة.

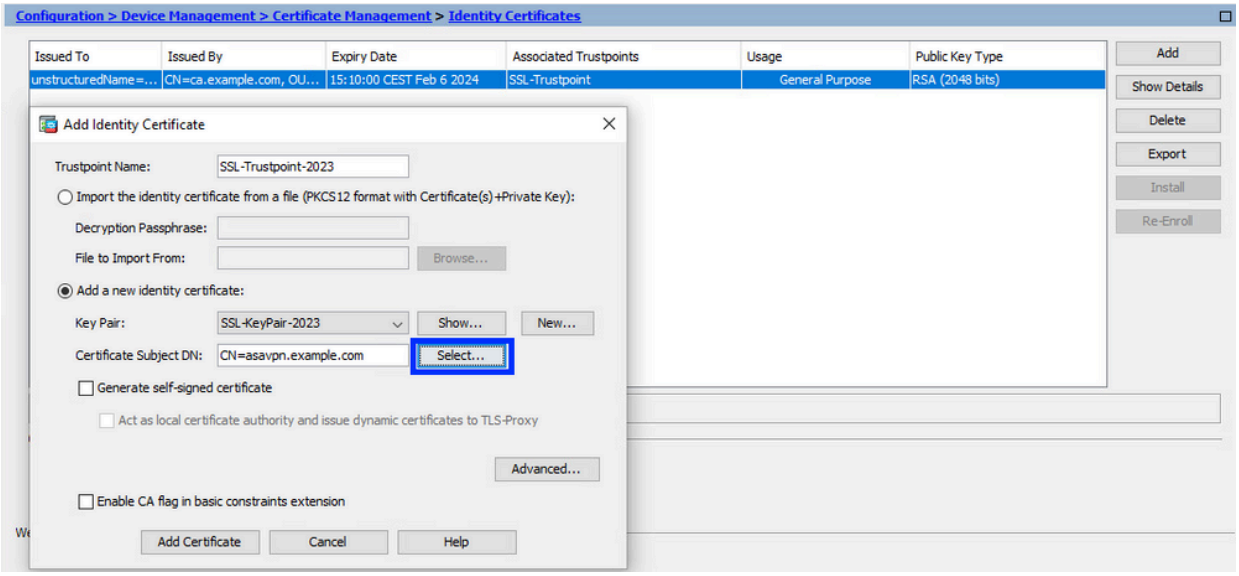


4. تكوين موضوع الشهادة واسم المجال المؤهل بالكامل (FQDN)

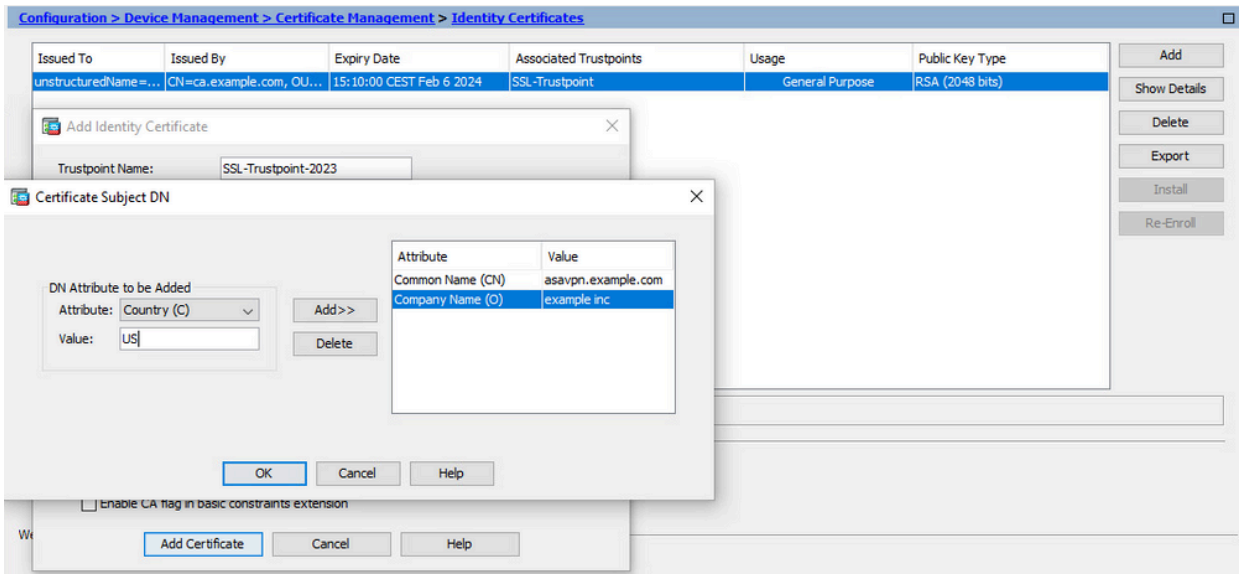
تحذير: يجب أن تطابق معلمة FQDN FQDN أو عنوان IP الخاص بواجهة ASA التي يتم إستخدام الشهادة لها. تقوم هذه المعلمة بتعيين اسم الموضوع البديل (SAN) للشهادة. يتم إستخدام حقل شبكة التخزين (SAN) من قبل عميل SSL/TLS/IKEv2 للتحقق من تطابق الشهادة مع FQDN الذي يتصل به.

ملاحظة: يمكن ل CA تغيير معلمات FQDN و Subject Name المحددة في TrustPoint عند توقيعها على CSR وإنشاء شهادة هوية موقعة.

a. انقر فوق تحديد.



b. في نافذة عنوان الشهادة DN، قم بتكوين سمات الشهادة - حدد سمة من القائمة المنسدلة، أدخل القيمة، انقر فوق إضافة.

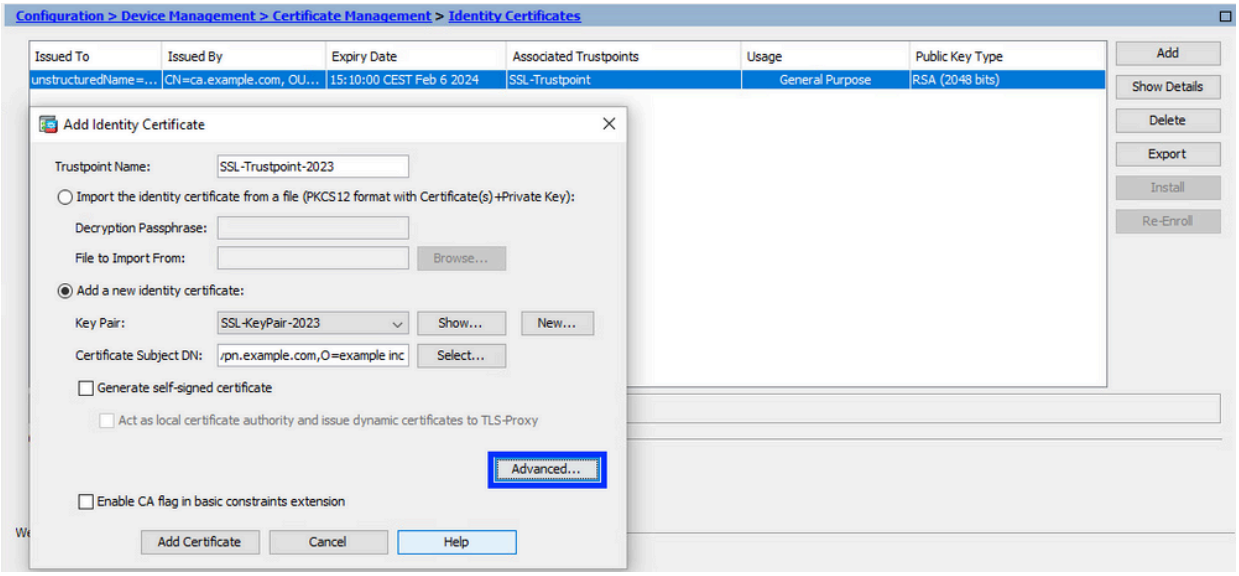


سمة	الوصف
سي إن	الاسم الذي يمكن الوصول من خلاله إلى جدار الحماية (عادة اسم المجال المؤهل بالكامل، على سبيل المثال، vpn.example.com).
أو	اسم القسم الخاص بك داخل المؤسسة
O	الاسم المسجل قانونيا لمؤسستك/شركتك
C	رمز البلد (رمز حرف ثنائي عالمي)
سانت	الولاية التي توجد فيها مؤسستك.
L	المدينة التي تقع فيها مؤسستك.
آي إيه	عنوان البريد الإلكتروني

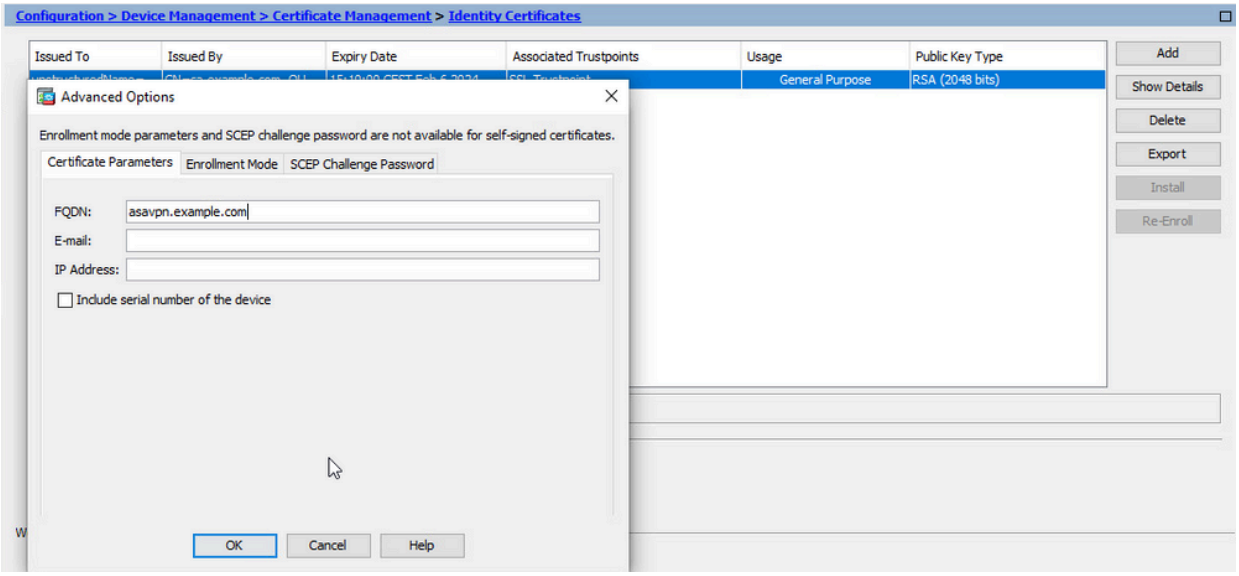
ملاحظة: لا يمكن لأي من الحقول السابقة أن تتجاوز حد الـ 64 حرفا. قد تتسبب القيمة الأطول في حدوث مشاكل في تثبيت شهادة الهوية. أيضا، ليس من الضروري أن تقوم بتعريف كل سمات DN.

انقر فوق موافق بعد إضافة كافة السمات.

c. لتكوين FQDN للجهاز، انقر فوق خيارات متقدمة.

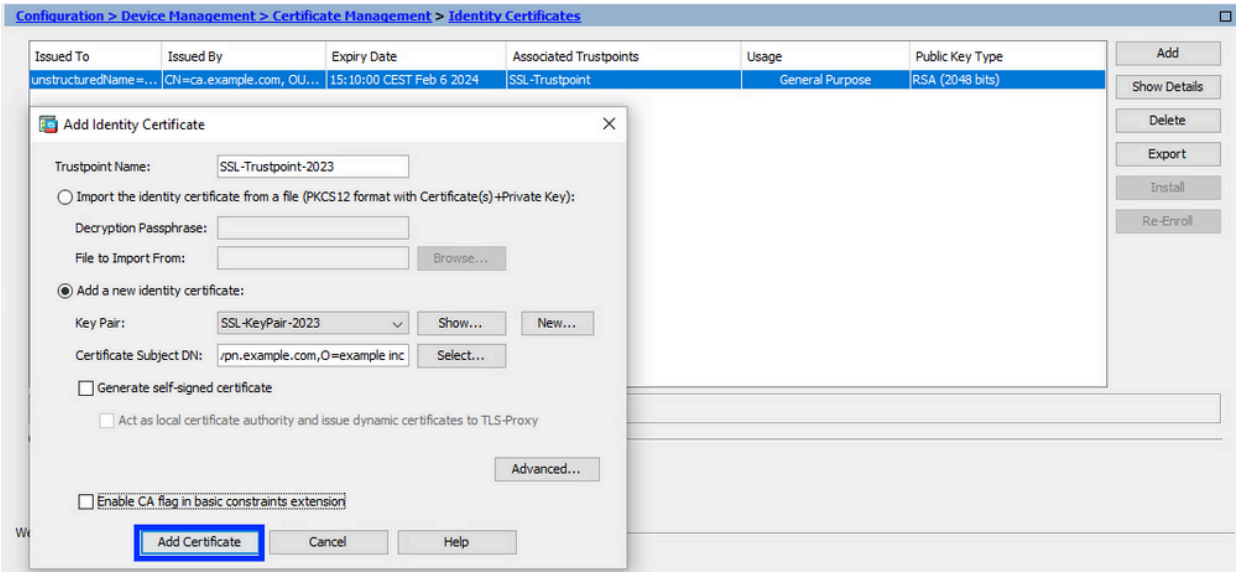


d. في حقل FQDN، أدخل اسم المجال المؤهل بالكامل الذي يمكن من خلاله الوصول إلى الجهاز من الإنترنت. وانقر فوق OK.

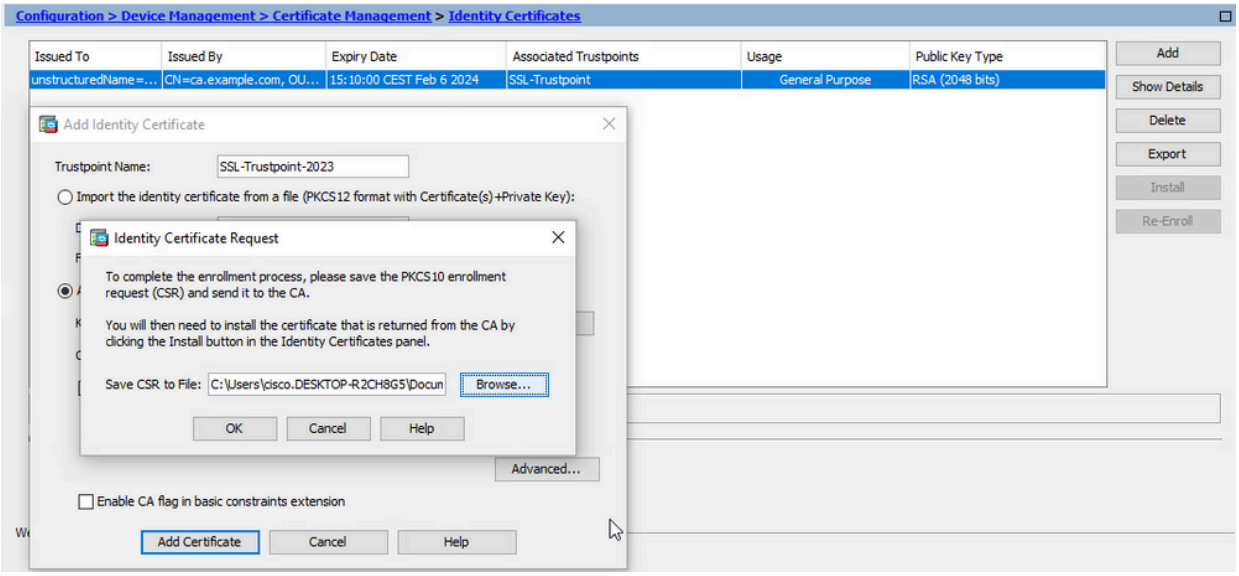


5. إنشاء CSR وحفظه

a. انقر على إضافة شهادة.



b. يعرض موجه الأمر لحفظ CSR إلى ملف على الجهاز المحلي.

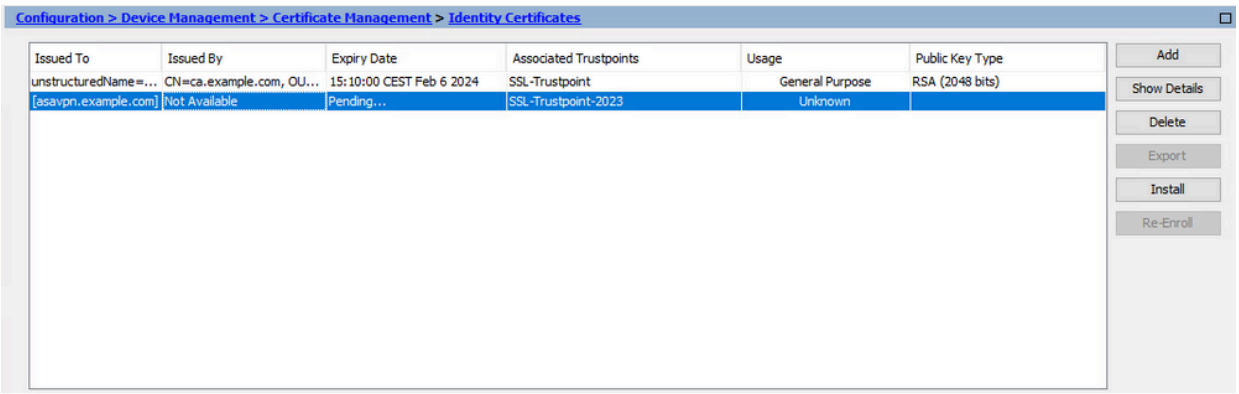


انقر على إستعراض. أختر المكان الذي تريد حفظ CSR فيه، ثم احفظ الملف بامتداد .txt.

ملاحظة: عند حفظ الملف بامتداد .txt، يمكن فتح طلب PKCS#10 وعرضه باستخدام محرر نصوص (مثل Notepad).

---

c. يتم الآن عرض TrustPoint الجديد في حالة معلق.



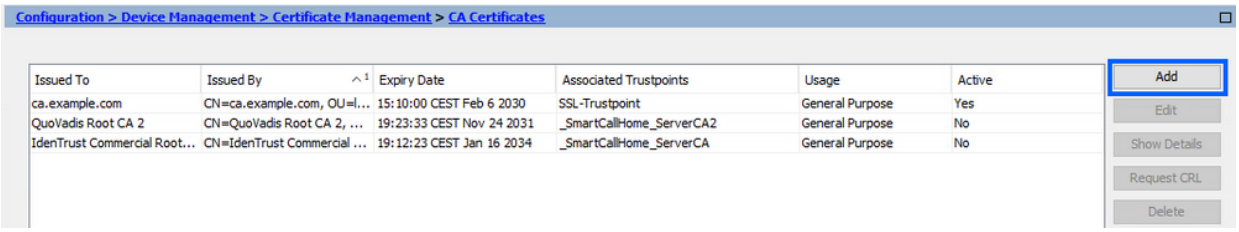
تثبيت شهادة الهوية بتنسيق PEM باستخدام ASDM

يفترض خطوات التثبيت أن CA وقع على CSR، وقدم شهادة هوية جديدة مرمزة وفقا لمعيار PEM (.pem و.cer.crt) وحزمة شهادة CA.

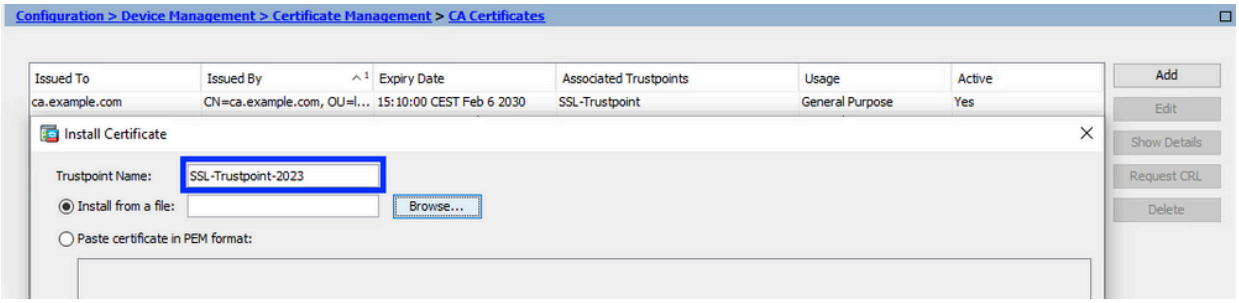
1. تثبيت شهادة CA التي وقعت على CSR

   يمكن تثبيت شهادة المرجع المصدق الموقعة على شهادة الهوية في TrustPoint التي تم إنشاؤها لشهادة الهوية. إذا كانت شهادة الهوية موقعة بواسطة المرجع المصدق الوسيط، يمكن تثبيت شهادة المرجع المصدق هذه في Identity Certificate TrustPoint. يمكن تثبيت جميع شهادات CA في الجزء العلوي من التدرج الهرمي في نقاط ثقة CA المنفصلة.

   a. انتقل إلى التكوين > إدارة الأجهزة >إدارة الشهادات >، واختر شهادات CA. انقر فوق إضافة (Add).



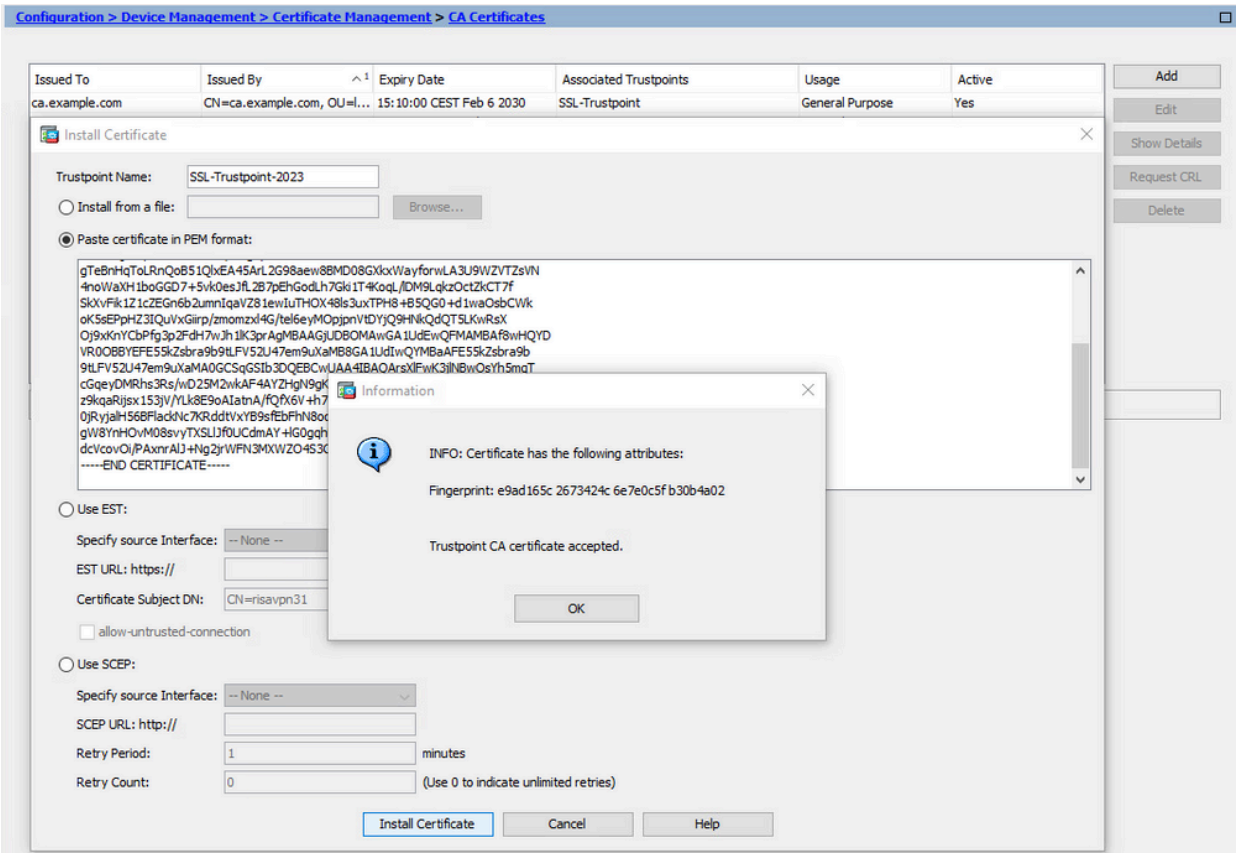
   b. أدخل اسم TrustPoint واختر تثبيت من ملف، وانقر زر إستعراض، واختر الشهادة الوسيطة. بدلا من ذلك، قم بلصق شهادة مرجع مصدق (CA) مرمزة بترميز PEM من ملف نصي في حقل النص.



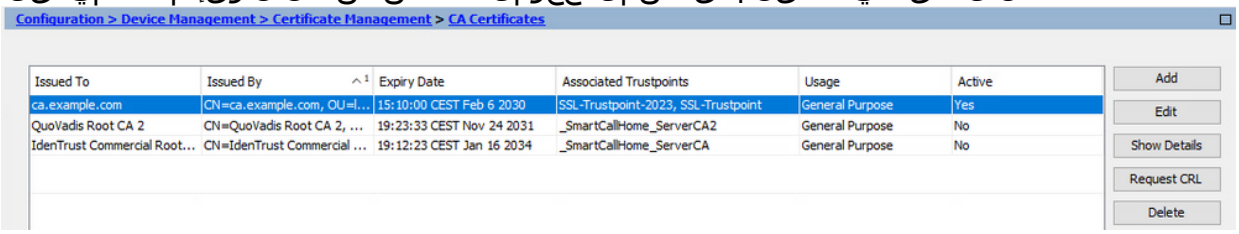
ملاحظة: تثبيت الشهادة الوسيطة بنفس اسم نقطة الثقة مثل اسم نقطة ثقة شهادة الهوية، إذا كانت شهادة الهوية موقعة بشهادة CA

الوسيطة.

c. انقر على تثبيت الشهادة.

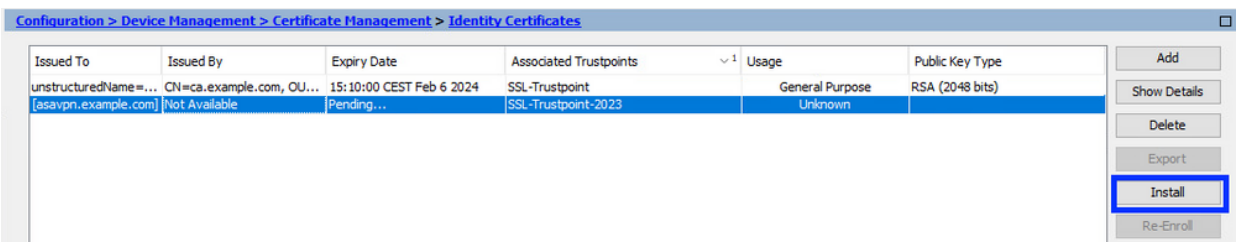


في المثال، يتم توقيع الشهادة الجديدة بنفس شهادة CA مثل الشهادة القديمة. تم إقران نفس شهادة المرجع المصدق بنقطتي ثقة الآن.



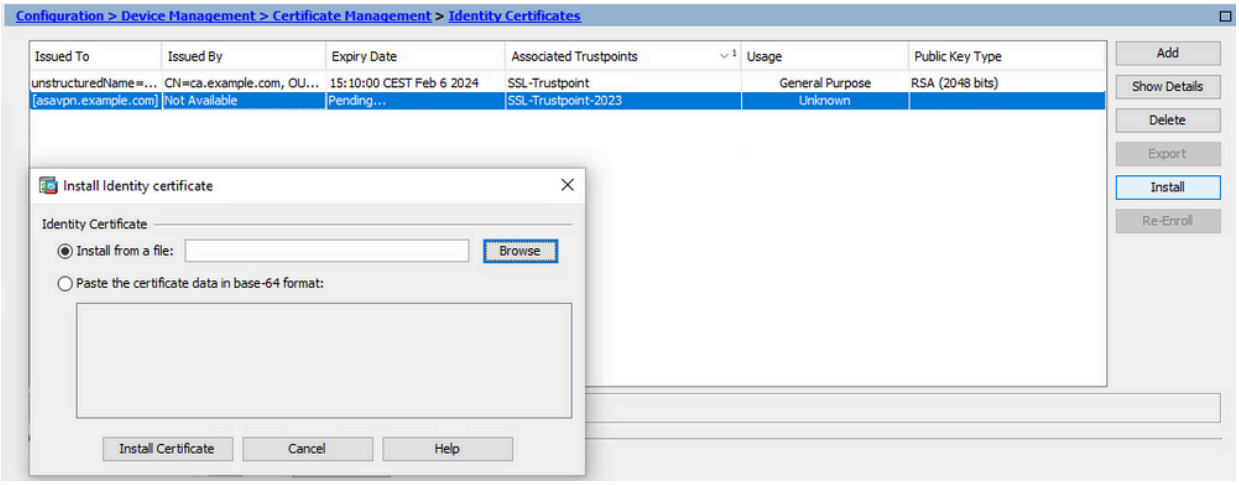
2. تثبيت شهادة الهوية

a. أختر شهادة الهوية التي تم إنشاؤها مسبقا باستخدام إنشاء CSR. انقر على تثبيت.



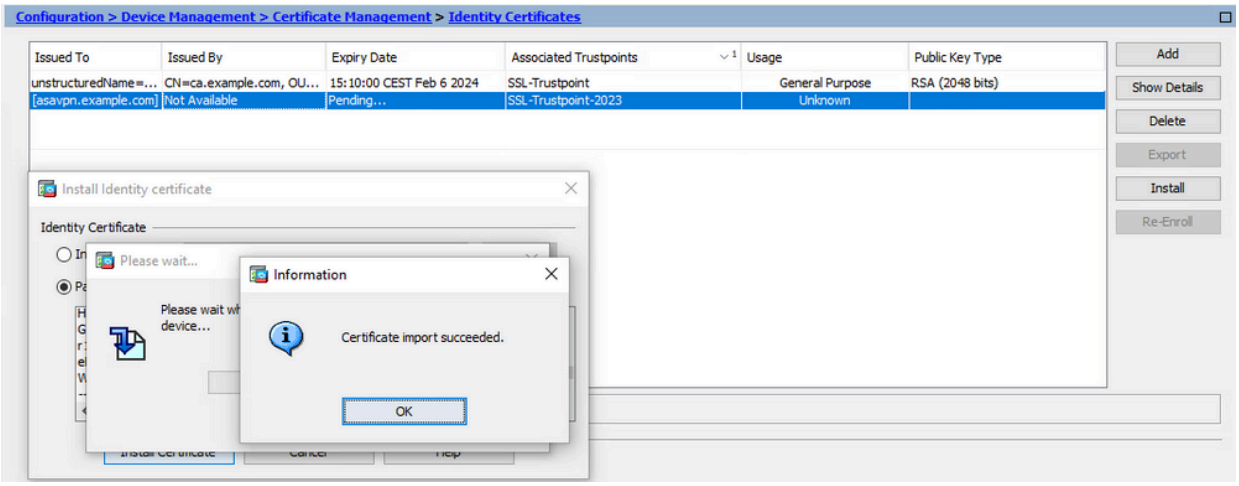
ملاحظة: يمكن أن تكون شهادة الهوية قد تم إصدارها بواسطة الحقل غير متوفر، وحقل تاريخ انتهاء الصلاحية ك معلق.

b. أختر ملف يحتوي على شهادة تعريف PEM المرمزة المستلمة من المرجع المصدق، أو افتح شهادة PEM المرمزة في محرر نص، وقم بنسخ ولصق شهادة الهوية المقدمة من المرجع المصدق في حقل النص.

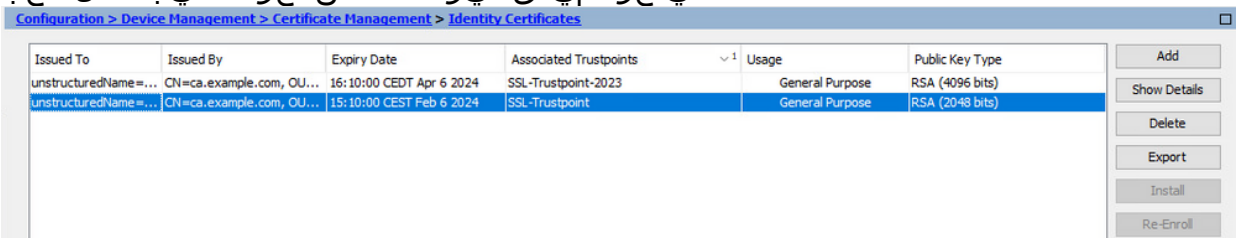


ملاحظة: يمكن أن تكون شهادة الهوية بتنسيق .pem، .cer، .crt للتثبيت.

c. انقر على تثبيت الشهادة.



بعد التثبيت، توجد شهادات هوية قديمة وجديدة.



3. ربط الشهادة الجديدة بالواجهة باستخدام ASDM

يجب تكوين ASA لاستخدام شهادة الهوية الجديدة لجلسات عمل WebVPN التي تنتهي

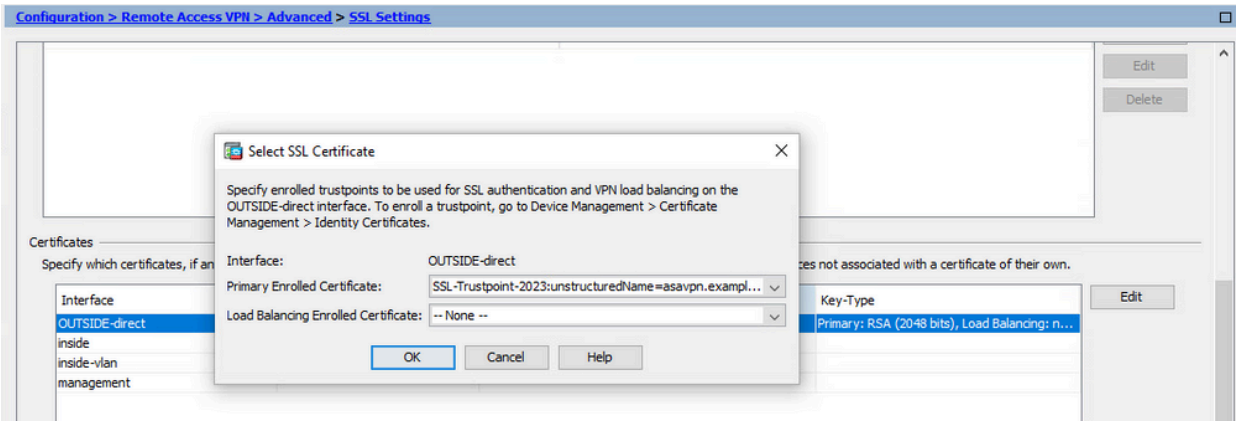
على الواجهة المحددة.

a. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > Advanced (خيارات متقدمة) > إعدادات SSL.

b. تحت شهادات، أختر الواجهة التي يتم إستخدامها لإنهاء جلسات عمل WebVPN. في هذا المثال، يتم إستخدام الواجهة الخارجية.

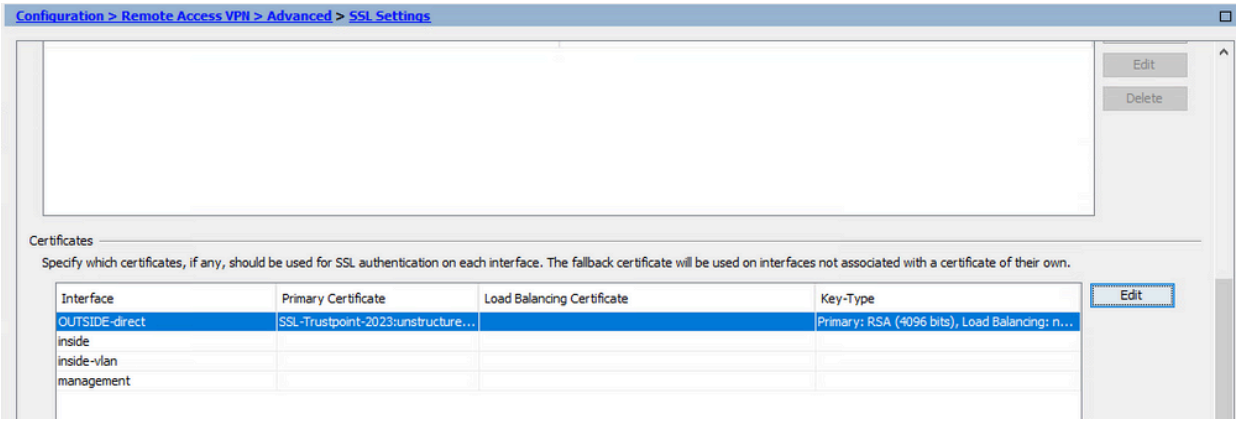
انقر فوق تحرير.

c. في القائمة المنسدلة ترخيص، أختر الشهادة المثبتة حديثا.



d. وانقر فوق OK.

e. طقطقة يطبق. شهادة الهوية الجديدة قيد الاستخدام الآن.



تجديد شهادة مسجلة في ملف PKCS12 مع ASDM

يتطلب تجديد الشهادة ل PKCS12 REGISTERED إنشاء TrustPoint جديد وتسجيله. يجب أن يكون له اسم مختلف (على سبيل المثال، الاسم القديم مع لاحقة سنة التسجيل).

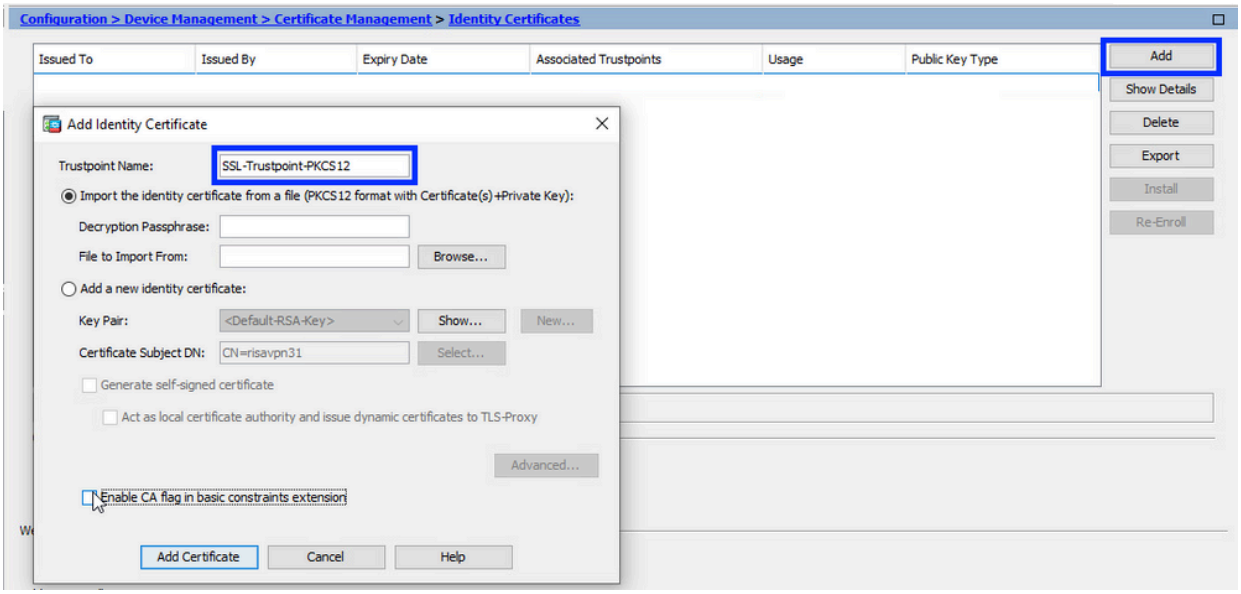
يحتوي ملف PKCS12 (.p12 أو .pfx) على شهادة هوية، زوج مفاتيح، وشهادة (شهادات) CA. يتم إنشاؤها بواسطة المرجع المصدق، على سبيل المثال، في حالة شهادة حرف البدل، أو تصديرها من جهاز مختلف. وهو ملف ثنائي، ولا يمكن عرضه باستخدام محرر النص.

1. قم بتثبيت شهادة الهوية المتجددة وشهادات المرجع المصدق من ملف

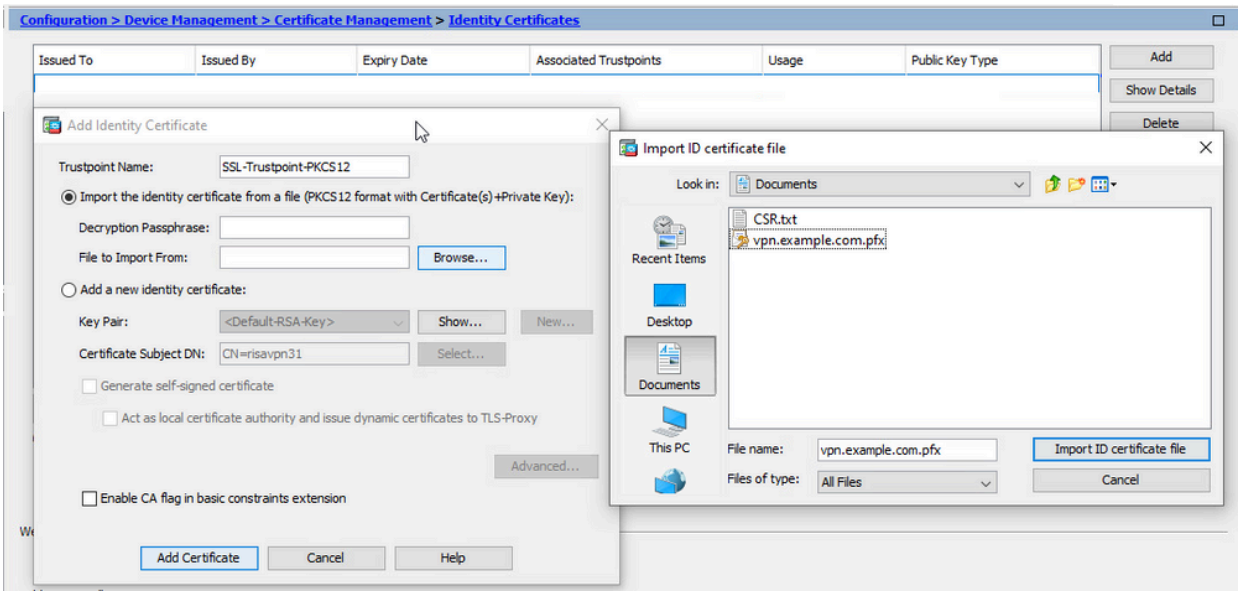
PKCS12

يلزم تجميع شهادة الهوية وشهادة (شهادات) المرجع المصدق (CA) وزوج المفاتيح في ملف PKCS12 واحد.

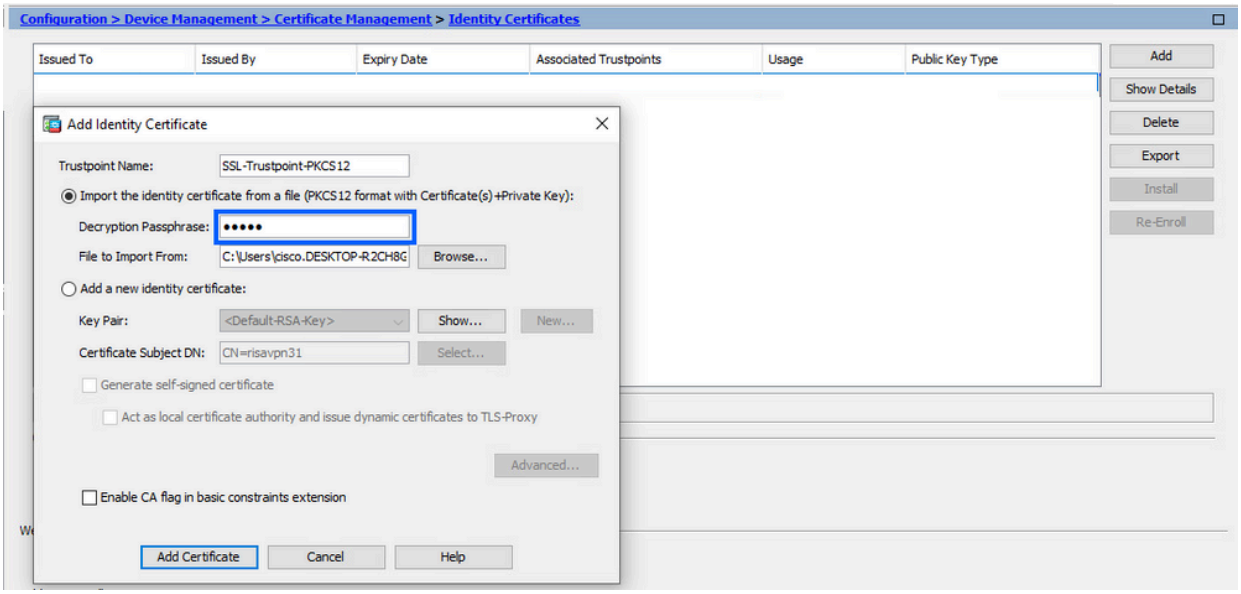
a. انتقل إلى التكوين > إدارة الأجهزة > إدارة الشهادات، واختر شهادات الهوية.
b. انقر فوق إضافة (Add).
c. حدد اسم TrustPoint جديد.



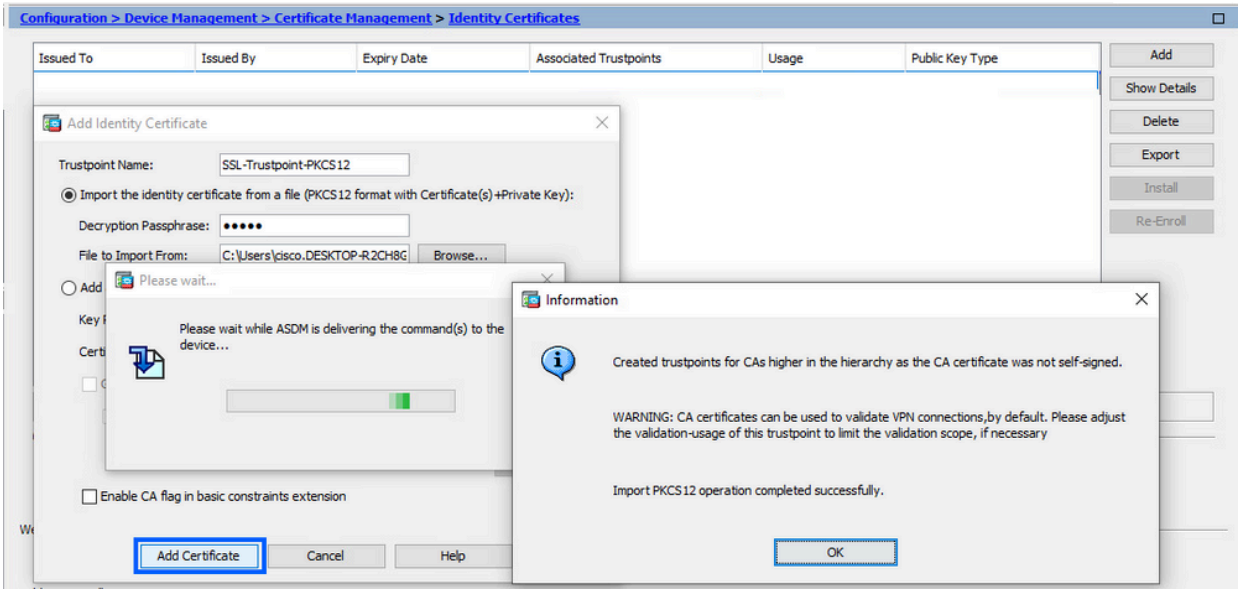
d. انقر على زر إدراج شهادة الهوية من مرجع ملف.



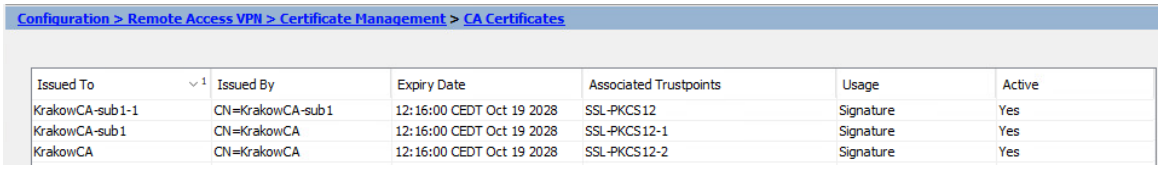
e. أدخل عبارة المرور المستخدمة لإنشاء ملف PKCS12.



f. انقر على إضافة شهادة.



ملاحظة: عند إستيراد PKCS12 مع سلسلة شهادات CAs، يقوم ASDM بإنشاء نقاط الثقة ل CAs للتحميل تلقائيا مع أسماء ذات لاحقة إضافية -number.



2. ربط الشهادة الجديدة بالواجهة باستخدام ASDM

يجب تكوين ASA لاستخدام شهادة الهوية الجديدة لجلسات عمل WebVPN التي تنتهي على الواجهة المحددة.

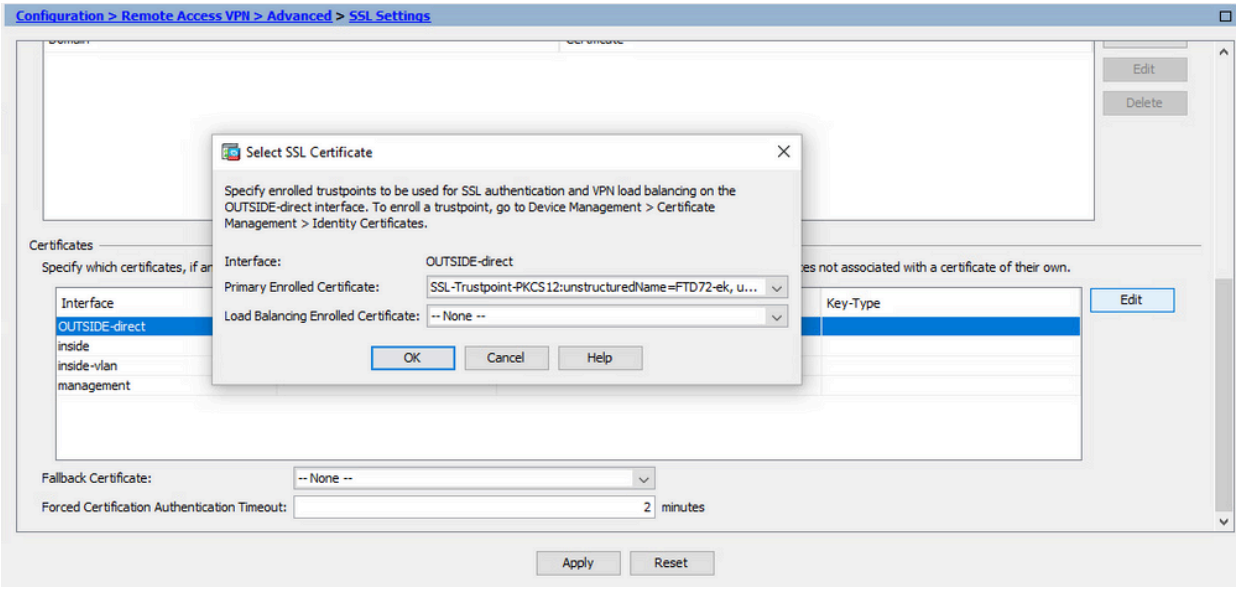
a. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > Advanced (خيارات

متقدمة) > إعدادات SSL.

b. تحت شهادات، أختر الواجهة التي يتم إستخدامها لإنهاء جلسات عمل WebVPN. في هذا المثال، يتم إستخدام الواجهة الخارجية.

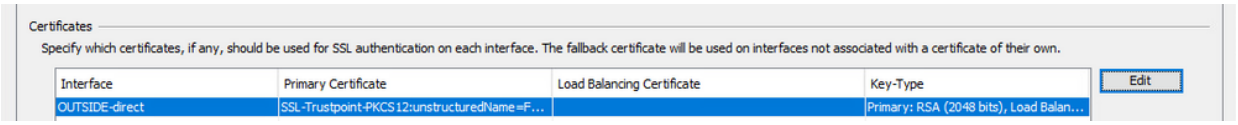
انقر فوق تحرير.

c. في القائمة المنسدلة ترخيص، أختر الشهادة المثبتة حديثا.



d. وانقر فوق OK.

e. طقطقة يطبق.



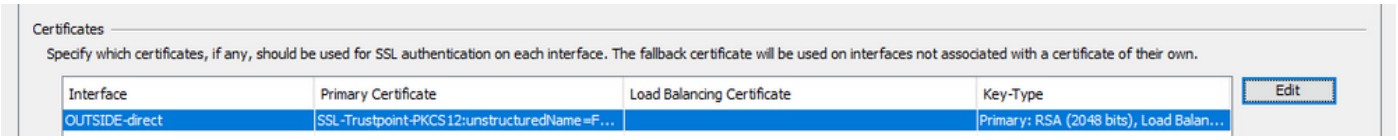
شهادة الهوية الجديدة قيد الاستخدام الآن.

التحقق من الصحة

أستخدم هذه الخطوات للتحقق من التثبيت الناجح لشهادة مورد الجهة الخارجية واستخدامها لاتصالات SSL VPN.

عرض الشهادات المثبتة عبر ASDM

1. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > إدارة الشهادات، واختر شهادات الهوية.
2. يمكن أن تظهر شهادة الهوية التي تم إصدارها من قبل مورد الطرف الثالث.



استكشاف الأخطاء وإصلاحها

يجب تجميع أمر تصحيح الأخطاء هذا على واجهة سطر الأوامر في حالة فشل تثبيت شهادة SSL.

- debug crypto ca 14

الأسئلة المتكررة

س. ما هو PKCS12؟
A. في التشفير، يعرف PKCS12 تنسيق ملف أرشيف تم إنشاؤه لتخزين العديد من كائنات التشفير كملف واحد. وعادة ما يتم إستخدامه لتجميع مفتاح خاص بشهادة X.509 وأ لتجميع كافة أعضاء سلسلة الثقة.

س. ما هي CSR؟
أ/ف - في نظم الهياكل الأساسية للمفتاح العام (PKI)، يمثل طلب توقيع الشهادة (أيضا طلب الاعتماد CSR) رسالة مرسلة من مقدم الطلب إلى سلطة تسجيل للبنية الأساسية للمفتاح العام من أجل التقدم بطلب للحصول على شهادة هوية رقمية. عادة ما يحتوي على المفتاح العام الذي من أجله يمكن إصدار الشهادة، المعلومات التي يتم إستخدامها لتعريف الشهادة المووقعة (مثل اسم المجال في الموضوع) وحماية التكامل (على سبيل المثال، التوقيع الرقمي).

Q.أين كلمة المرور ل PKCS12؟
a.عندما يتم تصدير الشهادات وأزواج المفاتيح إلى ملف PKCS12، يتم إعطاء كلمة المرور بواسطة مالك خادم CA في أمر التصدير. لا يستيراد ملف PKCS12 يجب تسليم كلمة المرور إلى مسؤول آخر من جهاز آخر أو الشخص الذي قام بتصدير PKCS12.

س. ما هو الفرق بين الجذر والهوية؟
أ/ف - في التشفير وأمان الكمبيوتر، تكون الشهادة الجذر شهادة مفتاح عام تعرف مرجع شهادات جذر (CA). تكون الشهادات الجذر موقعة ذاتيا (ومن الممكن أن يكون للشهادة مسارات تكون مختلفة، ولنقل إذا كانت الشهادة صادرة عن جذر موقع تابع لي) وتشكل الأساس لبنية أساسية للمفتاح العام (PKI) مستندة إلى X.509. وشهادة المفتاح العام، المعروفة أيضا بشهادة رقمية أو شهادة هوية، هي وثيقة إلكترونية تستخدم لإثبات ملكية مفتاح عام. تتضمن الشهادة معلومات حول المفتاح، ومعلومات حول هوية مالكها (تسمى الموضوع)، والتوقيع الرقمي للكيان الذي تحقق من محتويات الشهادة (يسمى المصدر). إذا كان المصدر، فيمكن إستخدام التوقيع صحيحا، وكان البرنامج الذي يفحص الشهادة يثق في المصدر، وتوافق اسم الموضوع الشهادة.

Q.لقد ركبت الصندوق، لماذا لا يعمل؟
أ/ف - قد يرجع ذلك إلى أسباب عديدة، منها على سبيل المثال:

1. تم تكوين الشهادة ونقطة الثقة، ولكن لم يتم ربطها بالعملية التي يجب إستخدامها. على سبيل المثال، لا يتم ربط TrustPoint التي سيتم إستخدامها بالواجهة الخارجية التي تقوم بإنهاء عملاء AnyConnect.

2. يتم تثبيت ملف PKCS12، لكنه يعطي أخطاء بسبب شهادة CA الوسيطة المفقودة في

ملف PKCS12. يتعذر على العملاء الذين لديهم شهادة CA الوسيطة كموثوق بها، ولكن ليس لديهم شهادة CA الجذر كموثوق بها، التحقق من سلسلة الشهادات بأكملها والإبلاغ عن شهادة هوية الخادم كغير موثوق بها.

3. قد تتسبب الشهادة التي تم ملؤها بسمات غير صحيحة في فشل التثبيت، أو أخطاء من جانب العميل. على سبيل المثال، قد يتم تشفير بعض السمات باستخدام تنسيق خاطئ. سبب آخر هو أن شهادة الهوية تفتقد للاسم البديل للموضوع (SAN)، أو أن اسم المجال المستخدم للوصول إلى الخادم غير موجود كشبكة منطقة تخزين (SAN).

س. هل يتطلب تثبيت وحدة جديدة إطار صيانة أم أنه يتسبب في وقت التوقف عن العمل؟
أ. تثبيت شهادة جديدة (الهوية أو المرجع المصدق) ليس متطفلا والو الو يجب أن يتسبب في وقت توقف عن العمل أو يطلب نافذة صيانة. لتمكين شهادة جديدة ليتم إستخدامها لخدمة موجودة هو تغيير وقد يتطلب طلب تغيير / إطار صيانة.

Q.هل يمكن أن تؤدي إضافة شهادة أو تغييرها إلى قطع اتصال المستخدمين المتصلين؟
A.No، يظل المستخدمون المتصلون حاليا على اتصال. يتم إستخدام الشهادة عند إنشاء الاتصال. بمجرد إعادة اتصال المستخدمين، يتم إستخدام الشهادة الجديدة.

Q.كيف يمكنني إنشاء CSR بحرف بدل؟ أو اسم بديل للموضوع (SAN)؟
حاليا، ال يمكن أن يقوم ASA/FTD بإنشاء CSR بحرف البدل؛ ومع ذلك، يمكن القيام بهذه العملية باستخدام OpenSSL. in order to خلق ال CSR ومعرف مفتاح، أنت يستطيع ركض الأمر:

openssl genrsa -out id.key 2048

openssl req -out id.csr -key id.key - جديد

عند تكوين نقطة ثقة باستخدام سمة "اسم المجال المؤهل بالكامل (FQDN)"، تحتوي CSR على اسم المجال المؤهل بالكامل (FQDN) لواجهة ASA/FTD التي تم إنشاؤها وبواسطة شبكة منطقة التخزين (SAN) بهذه القيمة. يمكن إضافة المزيد من سمات شبكة التخزين (SAN) بواسطة المرجع المصدق عندما يوقع على CSR، أو يمكن إنشاء CSR باستخدام OpenSSL

س. هل يسري مفعول إستبدال الشهادة فورا؟

أ. تستخدم شهادة هوية الخادم الجديدة فقط للاتصالات الجديدة. تكون الشهادة الجديدة جاهزة للاستخدام بعد التغيير مباشرة، ولكنها تستخدم بالفعل مع الاتصالات الجديدة.

س. كيف يمكن التحقق من تشغيل التثبيت؟
a.ال CLI أمر أن يدقق: أبدي crypto ca cert <trustPointName>

Q.كيف أن يخلق PKCS12 من شهادة الهوية، شهادة CA، والمفاتح الخاص؟
يمكن إنشاء A. PKCS12 باستخدام OpenSSL، باستخدام الأمر:

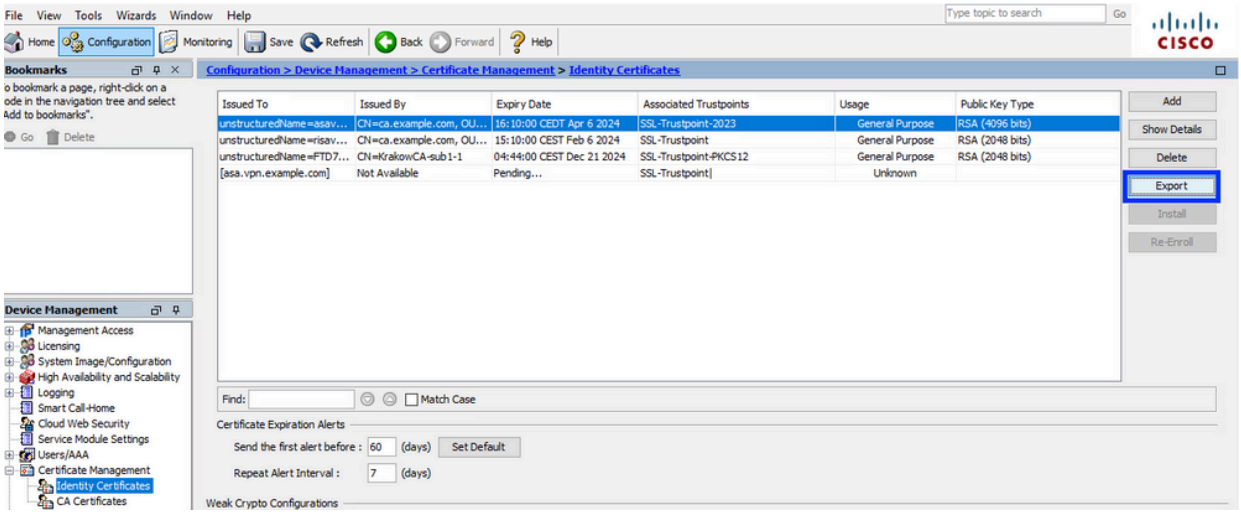
openssl pkcs12 -export -out12.pfx -inkey id.key -in id.crt -certfile ca.crt

Q. كيف يمكنك تصدير شهادة لتثبيتها في ASA جديد؟
ج.

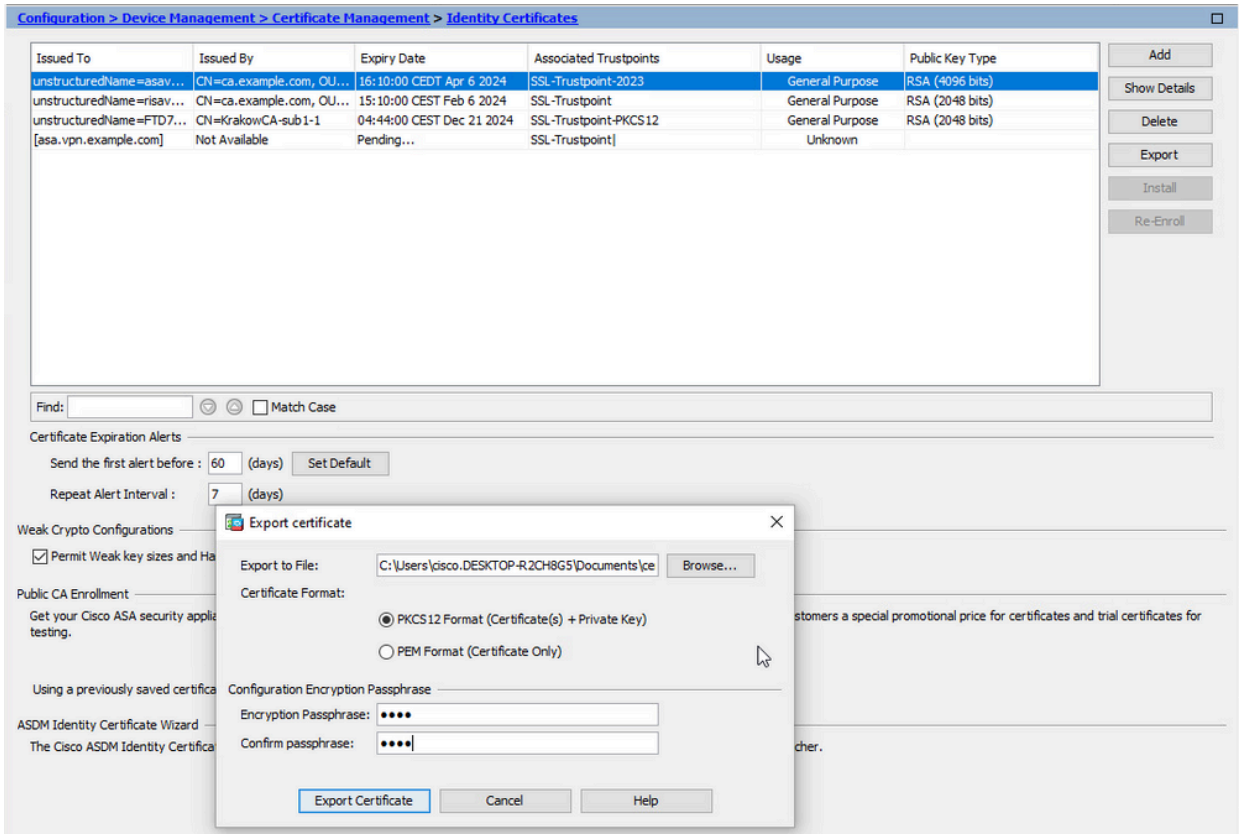
- مع CLI: أستخدم الأمر: crypto ca export <trustPointName> pkcs12 <password>

- مع ASDM:

a. انتقل إلى التكوين > إدارة الأجهزة > إدارة الشهادات > شهادات الهوية واختر شهادة الهوية. طقطقة يصدر.



b. أختر أين تريد تصدير الملف، حدد كلمة مرور التصدير، انقر تصدير الترخيص.



يمكن أن تكون الشهادة المصدرة على قرص الكمبيوتر. من فضلك لاحظ عبارة المرور في مكان آمن، فلا فائدة من الملف بدونها.

Q. إذا كانت مفاتيح ECDSA مستخدمة، هل تختلف عملية إنشاء شهادة SSL؟
a. الاختلاف الوحيد في التكوين هو خطوة إنشاء زوج المفاتيح، حيث يمكن إنشاء زوج مفاتيح ECDSA بدلا من زوج مفاتيح RSA. أما باقي الخطوات فبقيت كما هي.

Q.هل مطلوب دائما إنشاء زوج مفاتيح جديد؟
a.خطوة إنشاء زوج المفاتيح إختيارية. يمكن إستخدام زوج المفاتيح الموجود، أو في حالة PKCS12 يتم إستيراد زوج المفاتيح مع الشهادة. الرجاء مراجعة القسم تحديد اسم زوج المفاتيح لنوع التسجيل / إعادة التسجيل ذي الصلة.

Q.هل من الآمن إنشاء زوج مفاتيح جديد لشهادة هوية جديدة؟
A. العملية آمنة طالما يتم إستخدام اسم زوج مفاتيح جديد. في مثل هذه الحالة، ال يتم تغيير أزواج المفاتيح القديمة.

Q.هل يلزم إنشاء المفاتح مرة أخرى عند إستبدال جدار حماية (مثل RMA)؟
ألف - ال يتضمن الجدار النار الجديد حسب التصميم أزواج المفاتيح الموجودة على جدار الحماية القديم.
ال يحتوي النسخ الاحتياطي ل running-configuration على أزواج المفاتيح.
يمكن أن يحتوي النسخ الاحتياطي الكامل الذي تم إجراؤه مع ASDM على أزواج المفاتيح.
يمكن تصدير شهادات الهوية من ASA مع ASDM أو CLI، قبل فشلها.
في حالة زوج تجاوز الفشل، تتم مزامنة الشهادات وأزواج المفاتيح مع وحدة إحتياطية باستخدام أمر كتابة في وضع الاستعداد. في حالة إستبدال عقدة واحدة من زوج تجاوز الفشل، يكفي تكوين تجاوز الفشل الأساسي ودفع التكوين إلى الجهاز الجديد.
في حالة فقد زوج مفاتيح مع الجهاز وعدم وجود نسخة إحتياطية، يلزم توقيع شهادة جديدة مع زوج مفاتيح موجود على الجهاز الجديد.

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).