تكوين RAPN باستخدام مصادقة SAML باستخدام Azure ك IDp على FTD الذي تتم إدارته بواسطة FDM 7.2 أو أقل

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة SAML للوصول عن بعد إلى VPN باستخدام Azure ك IDp على FTD الذي تتم إدارته بواسطة الإصدار 7.2 من FDM أو أقل.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- شهادات طبقة مأخذ التوصيل الآمنة (SSL)
- OpenSSL
- أوامر Linux
- شبكة الوصول عن بعد الخاصة الظاهرية (RAVPN)
- مدير أجهزة جدار الحماية الآمن (FDM)
- لغة ترميز تأكيد الأمان (SAML)
- Microsoft Azure

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- OpenSSL الإصدار Cisco SSL 1.1.1j.7.2sp.230
- الدفاع ضد تهديد جدار الحماية الآمن (FTD)، الإصدار 7.2.0
- Secure Firewall Device Manager، الإصدار 7.2.0
- جهة منح الشهادة الداخلية (CA)

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

أصبح إستخدام مصادقة SAML لاتصالات RAPN والعديد من التطبيقات الأخرى أكثر شيوعا في الآونة الأخيرة بسبب مزاياها. SAML هو معيار مفتوح لتبادل معلومات المصادقة والتفويض بين الأطراف، وتحديدا موفر الهوية (IDp) ومزود الخدمة (SP).

يوجد تقييد في FTD تتم إدارته بواسطة إصدارات FDM 7.2.x وأقل حيث يكون معرف P الوحيد المعتمد لمصادقة SAML هو Duo. في هذه الإصدارات، يجب أن تحتوي الشهادات التي سيتم إستخدامها لمصادقة SAML على قيود الملحق الأساسية: ca:TRUE عند تحميلها إلى FDM.

ولهذا السبب، ال يتم اعتماد الشهادات المقدمة من معرفات أخرى (التي ال تحتوي على الملحق المطلوب) مثل Microsoft Azure لمصادقة SAML بشكل طبيعي في هذه الإصدارات، مما يتسبب في فشل مصادقة SAML.

ملاحظة: تتيح إصدارات FDM 7.3.x والإصدارات الأحدث تمكين خيار تخطي فحص المرجع المصدق عند تحميل شهادة جديدة. هذا يحل التقييد الموضح في هذا المستند.

في حالة تكوين RAPN باستخدام مصادقة SAML باستخدام الشهادة المقدمة من Azure والتي ال تحتوي على القيود الأساسية: CA:TRUE extension، عند تشغيل الأمر show saml metadata <trustPoint name> لاستيراد بيانات التعريف من واجهة سطر الأوامر (CLI) في FTD، يكون الإخراج فارغا كما هو معروض التالي:

```
<#root>

firepower#

show saml metadata



SP Metadata
-----------

IdP Metadata
-----------
```

التكوين

تتمثل الخطوة المقترحة لحل هذه القيود في ترقية جدار الحماية الآمن إلى الإصدار 7.3 أو أعلى، على الرغم من ذلك، إذا كنت تحتاج لأي سبب من الأسباب إلى جدار الحماية لتشغيل الإصدار 7.2 أو أقل، فيمكنك العمل حول هذه التحديد من خلال إنشاء شهادة مخصصة تتضمن الامتداد الأساسي: CA:TRUE. بمجرد توقيع الشهادة من مرجع مصدق مخصص، تحتاج إلى تغيير التكوين في مدخل تكوين Azure SAML الذي يستخدم هذه الشهادة المخصصة بدلاً من ذلك.

الخطوة 1. إنشاء طلب توقيع شهادة (CSR) باستخدام ملحق القيود الأساسية: CA:TRUE

يصف هذا القسم كيفية إنشاء CSR باستخدام OpenSSL له لتضمين القيود الأساسية: CA:TRUE Extension.

1. سجل الدخول إلى نقطة نهاية تم تثبيت مكتبة OpenSSL عليها.

2. (إختياري) قم بإنشاء دليل حيث يمكنك تحديد موقع الملفات المطلوبة لهذه الشهادة (إذا قمت بإنشاء دليل جديد، فقم بتغيير الدليل إليه وإنشاء مفتاح خاص جديد يشغل الأمر mkdir <folder name>.

<#root>

root@host1:/home/admin#

mkdir certificate

3. إذا قمت بإنشاء دليل جديد، فقم بتغيير الدليل إليه وإنشاء مفتاح خاص جديد يشغل الأمر openssl genrsa -out <key_name>.key 4096.

<#root>

root@host1:/home/admin/certificate#

openssl genrsa -out privatekey.key 4096

ملاحظة: تمثل 4096 حد بت طول المفتاح لمثال التكوين هذا. يمكنك تحديد مفتاح أطول إذا لزم الأمر.

---

4. قم بإنشاء ملف تكوين باستخدام الأمر touch <config_name>.conf.

5. قم بتحرير الملف باستخدام محرر نصي. في هذا المثال، تم استخدام Vim وتم تشغيل الأمر vim <config_name>.conf. يمكنك استخدام أي محرر نصوص آخر.

<#root>

```
vim config.conf
```

6. أدخل المعلومات التي سيتم تضمينها في طلب توقيع الشهادة (CSR). تأكد من إضافة basicConstraints = ca:true extension في الملف كما هو معروض بعد ذلك:

<#root>

```
[ req ]

default_bits = 4096

default_md = sha256

prompt = no

encrypt_key = no

distinguished_name = req_distinguished_name

req_extensions = v3_req

[ req_distinguished_name ]

countryName =

stateOrProvinceName =

localityName =
```

```
organizationName =

organizationalUnitName =

commonName =

[ v3_req ]

basicConstraints = CA:true
```

> ملاحظة: BasicConstraints = CA:True وه الملحق الذي يجب أن تحتوي عليه الشهادة لكي يتمكن FTD من تثبيت الشهادة بنجاح.

7. باستخدام ملف التكوين والمفاتيح الذي تم إنشاؤه في الخطوات السابقة، يمكنك إنشاء

CSR باستخدام الأمر openssl req -new <key_name>.key -config <conf_name>.conf -out <csr_name>.csr:

<#root>

```
openssl req -new -key privatekey.key -config config.conf -out CSR.csr
```

8. بعد هذا الأمر، يمكنك أن ترى ملف <CSR_name>.csr الخاص بك المدرج في المجلد، وهو ملف CSR الذي يجب إرساله إلى خادم CA للتوقيع.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC01laXhjbyBDaXR5
MRQwEgYDVQQHDAtNZW14Y28gQ2l0eTEOMAwGA1UECgwFQ2lzY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQDRWH+ij26HuF/Y6NvITCkD5VJa6KRssDJ8
[...]

Output Omitted

[...]
lRZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTw1Q5h23JsPkvJmRpKSilc7w
3rKfTXelewT1IJdCmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

ملاحظة: انظر لمتطلبات Azure، من الضروري توقيع CSR بنقطة وصول CA مكونة من SHA-1، وإلا، فإن معرف Azure يرفض الشهادة عند تحميلها. يمكن العثور على مزيد من المعلومات على الارتباط التالي: خيارات توقيع الشهادات المتقدمة في رمز SAML المميز

---

9. أرسل ملف CSR هذا مع المرجع المصدق للحصول على الشهادة الموقعة.

الخطوة 2. إنشاء ملف PKCS12

بمجرد أن تقوم بتوقيع شهادة الهوية، فإنك تحتاج لإنشاء ملف معايير تشفير المفاتيح العام (PKCS#12) مع الملفات الثلاثة التالية:

- شهادة هوية موقعة
- مفتاح خاص (معرف في الخطوات السابقة)
- سلسلة شهادات CA

يمكنك نسخ شهادة الهوية وسلسلة شهادة المرجع المصدق إلى نفس الجهاز حيث قمت بإنشاء المفاتيح الخاص وملف CSR. بمجرد أن يكون لديك الملفات الثلاثة التي تقوم بتشغيل الأمر openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_series>.cer -

inkey <private_key_name>.key -out <pkcs12_name>.pfx الأمر لتحويل الشهادة إلى PKCS#12.

<#root>

```
openssl pkcs12 -export -in id.cer -certfile ca_chain.cer -inkey privatekey.key -out cert.pfx
```

بعد تشغيل الأمر، يطلب منك إدخال كلمة مرور. كلمة المرور هذه مطلوبة عند تثبيت الشهادة.

إذا نجح الأمر، يتم إنشاء ملف جديد باسم "<pkcs12_name>.pfx" في الدليل الحالي. هذه هي شهادة PKCS#12 الجديدة.

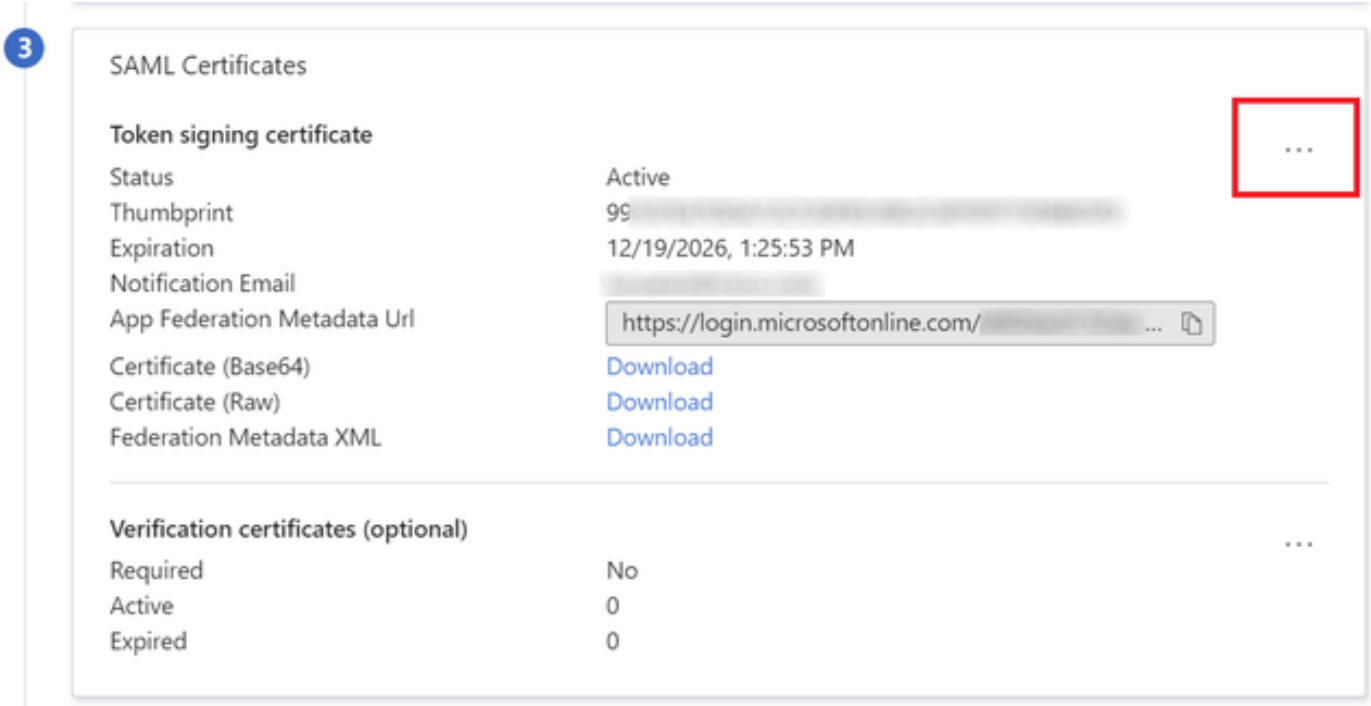
الخطوة 3. تحميل شهادة PKCS#12 إلى Azure و FDM

بمجرد أن يكون لديك ملف PKCS#12، تحتاج إلى تحميله إلى Azure و FDM.

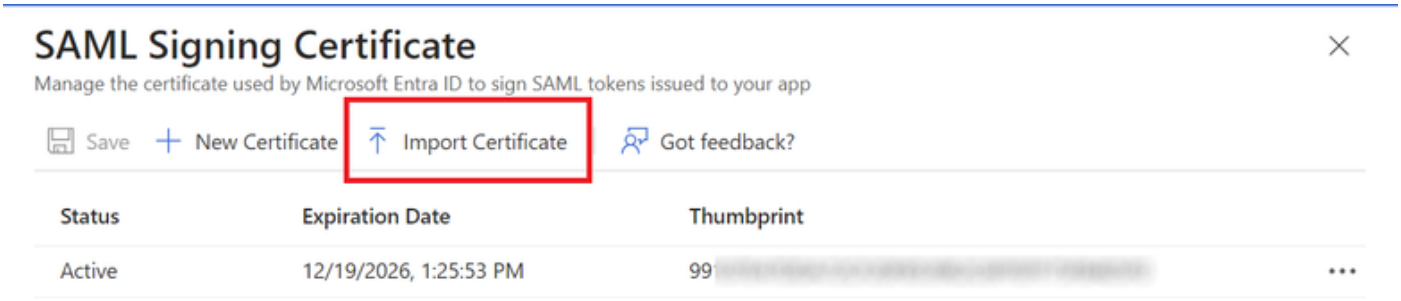
تحميل الشهادة إلى Azure

1. سجل الدخول إلى مدخل Azure، انتقل إلى تطبيق Enterprise الذي تريد حمايته بمصادقة SAML وحدد تسجيل الدخول الأحادي.

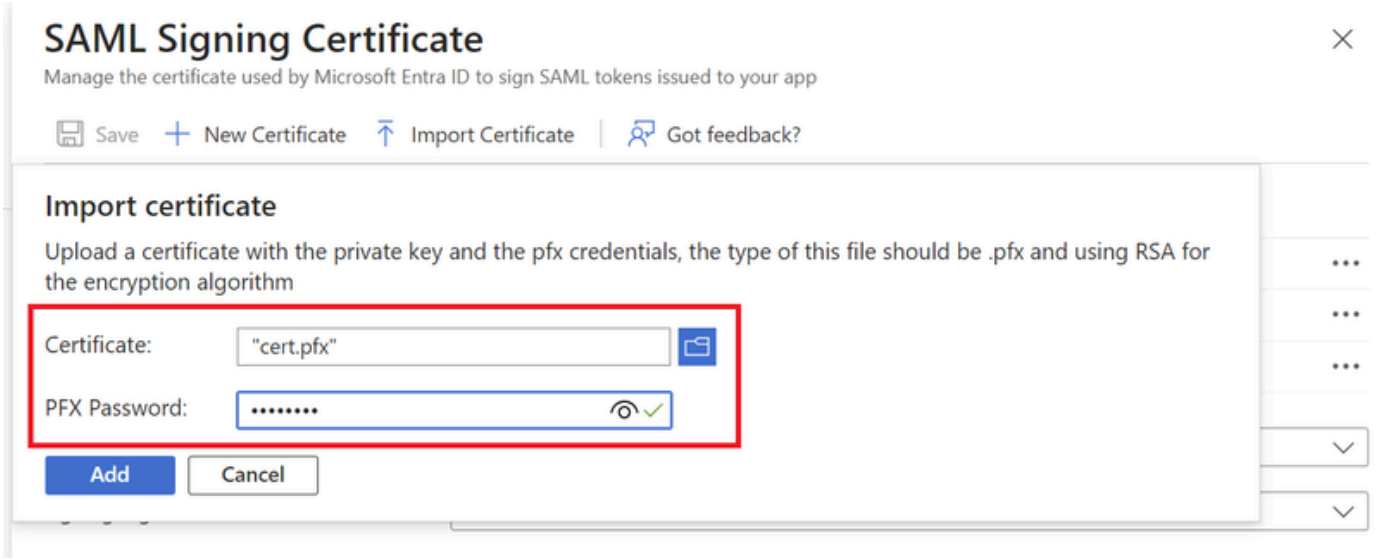
2. قم بالتمرير لأسفل إلى قسم شهادات SAML" وحدد أيقونة المزيد من الخيارات > تحرير.



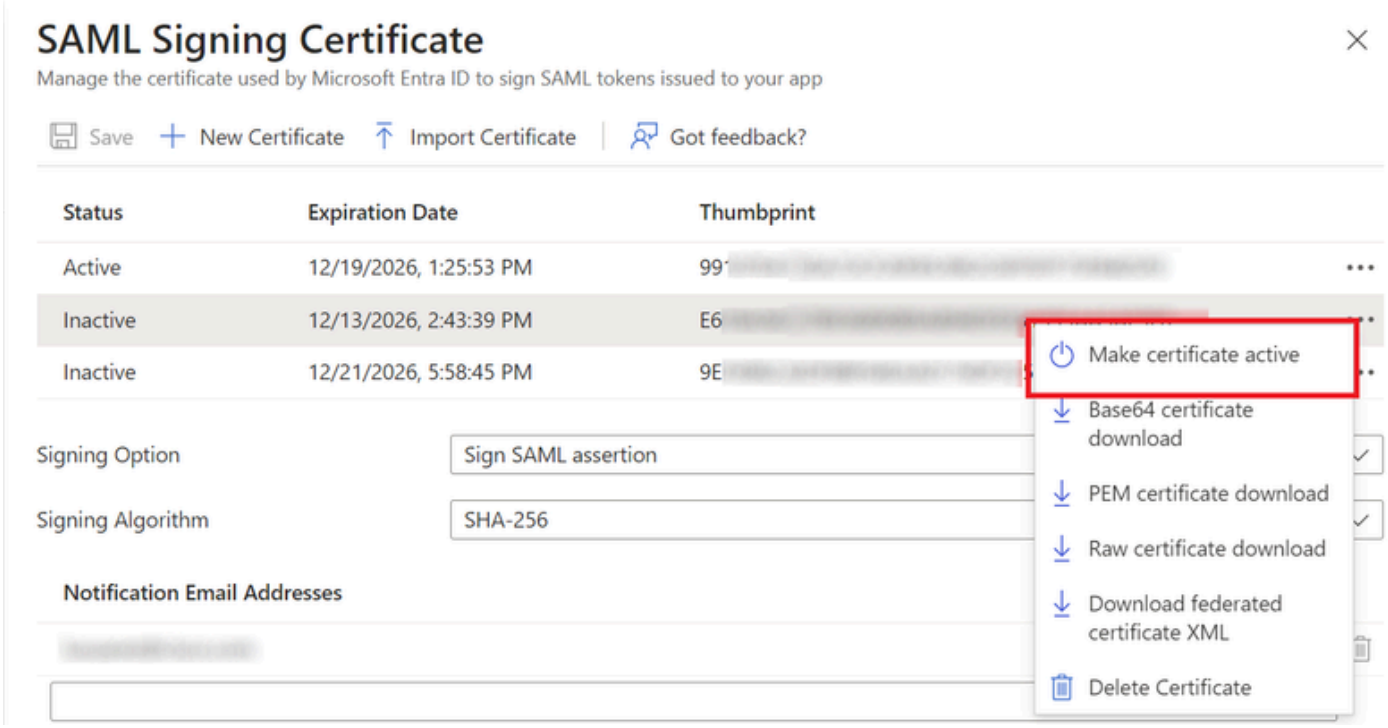
3. حدد الآن خيار إستيراد شهادة.



4. ابحث عن ملف PKCS12 الذي تم إنشاؤه مسبقا واستخدم كلمة المرور التي أدخلتها عندما قمت بإنشاء ملف PKCS#12.

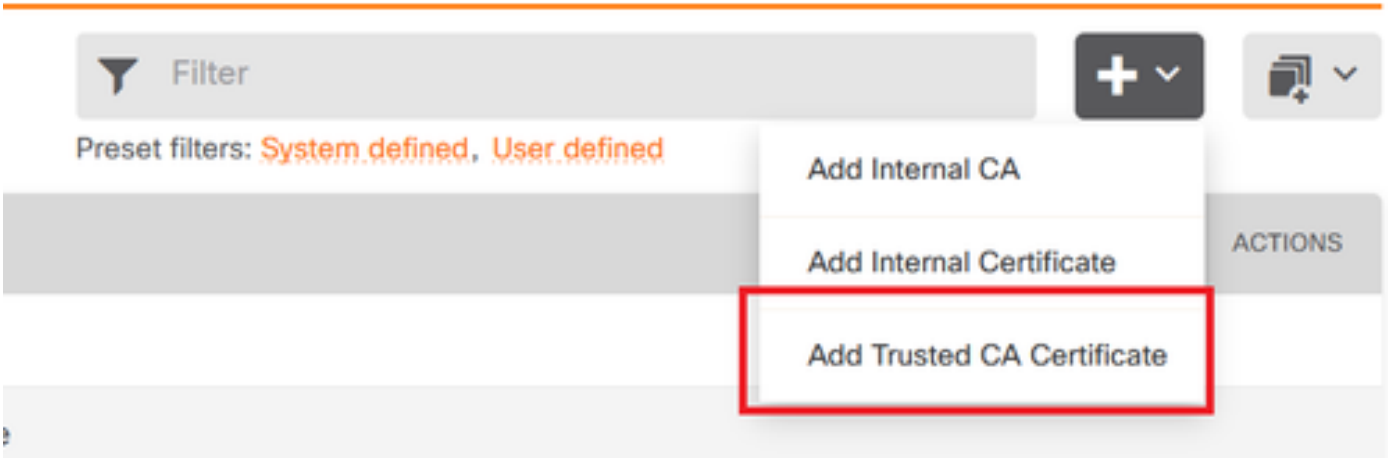


5. أخيرا، حدد خيار جعل الشهادة نشطة.

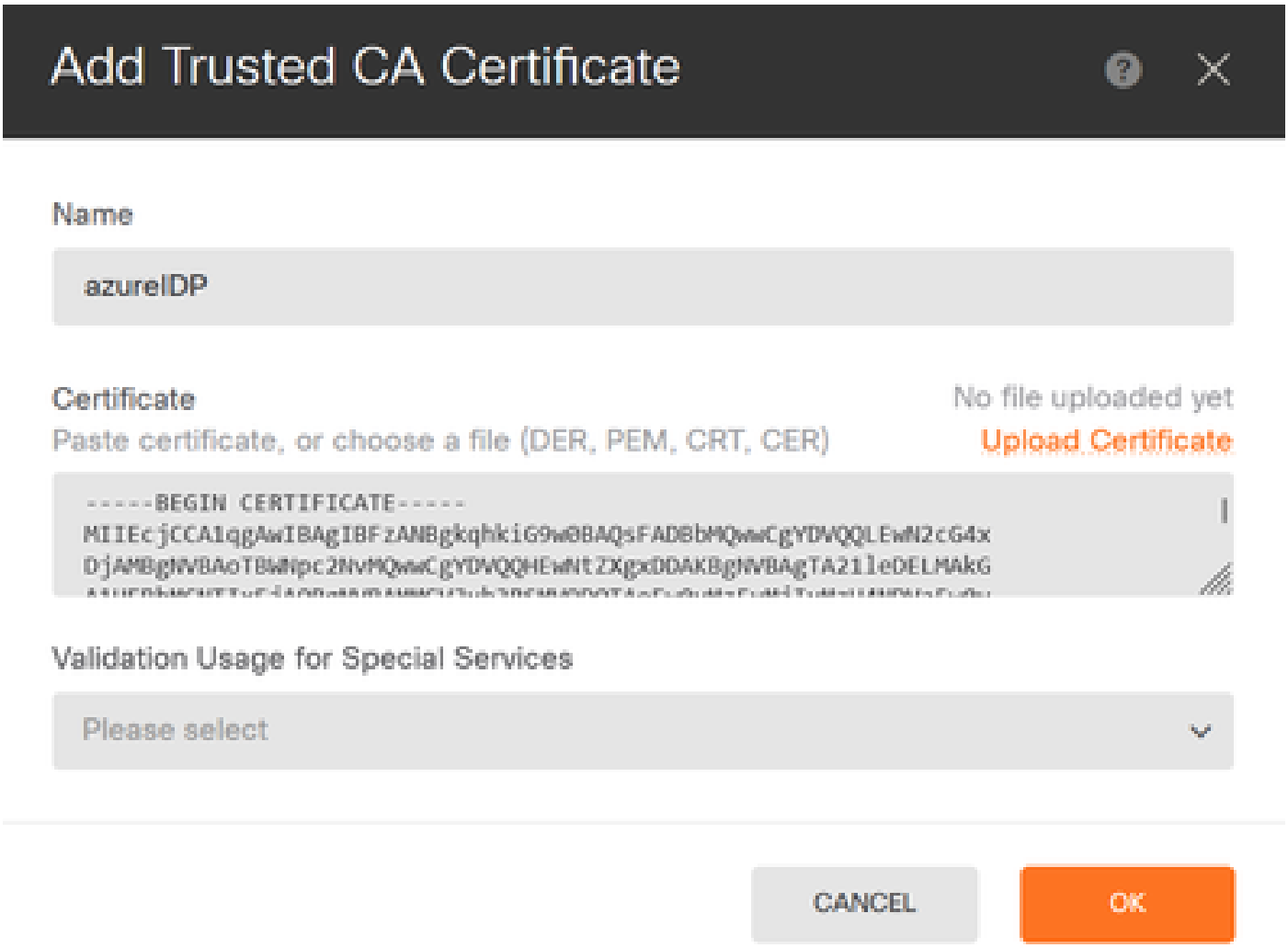


تحميل الشهادة إلى FDM

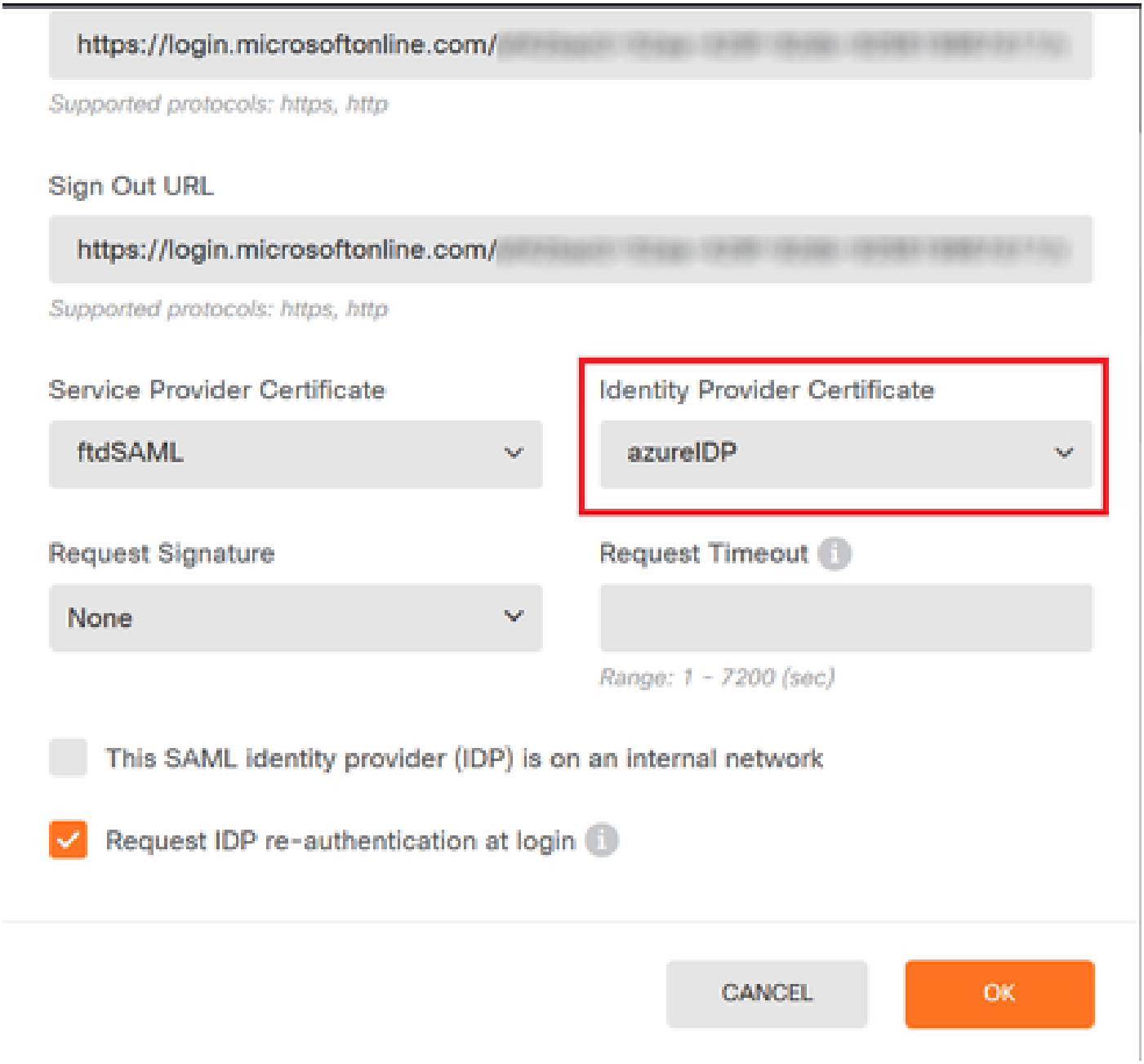
1. انتقل إلى كائنات > شهادات > انقر على إضافة شهادة مرجع مصدق ثقة.



2. أدخل اسم TrustPoint الذي تفضله وتحميل شهادة الهوية فقط من IdP (ليس ملف PKCS#12)



3. قم بتعيين الشهادة الجديدة في كائن SAML ونشر التغييرات.



التحقق من الصحة

قم بتشغيل الأمر show saml metadata <trustPoint name> لضمان توفر بيانات التعريف من واجهة سطر الأوامر (CLI) الخاصة ب FTD:

```
<#root>

firepower#

show saml metadata azure


SP Metadata
-----------
```

xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

MIIDbzCCAlegAwIBAgIBDDANBgkqhkiG9w0BAQwFADBbMQwwCgYDVQQLEwN2cG4x

...omitted...

HGaq+/IfNKKqkhgT6q4egqMHiA==

Location="https://[...omitted...]/+CSCOE+/saml/sp/logout"/>

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://[...omitted...]/+CSCOE+/saml/sp/logout"/>

IdP Metadata
----

xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

MIIEcjCCA1qgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBbMQwwCgYDVQQLEwN2cG4x

[...omitted...]

3Zmzsc5faZ8dMXO+1ofQVvMaPifcZZFoM7oBO9RK2PaMwIAV+Mw=

Location="https://login.microsoftonline.com/[...omitted...]/saml2" />

Location="https://login.microsoftonline.com/[...omitted...]/saml2" />

```
Location="https://login.microsoftonline.com/[...omitted...]/saml2" />
```

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).