تشكيل توصيفات WAPN متعددة بمصادقة SAML على FDM

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين مصادقة SAML لملفات تعريف توصيل متعددة لـ Remote Access VPN باستخدام Azure AS IDp على CSF عبر FDM.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

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

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- OpenSSL
- Cisco Secure Firewall (CSF)، الإصدار 7.4.1
- Cisco Secure Firewall Device Manager، الإصدار 7.4.1

.تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

معلومات أساسية

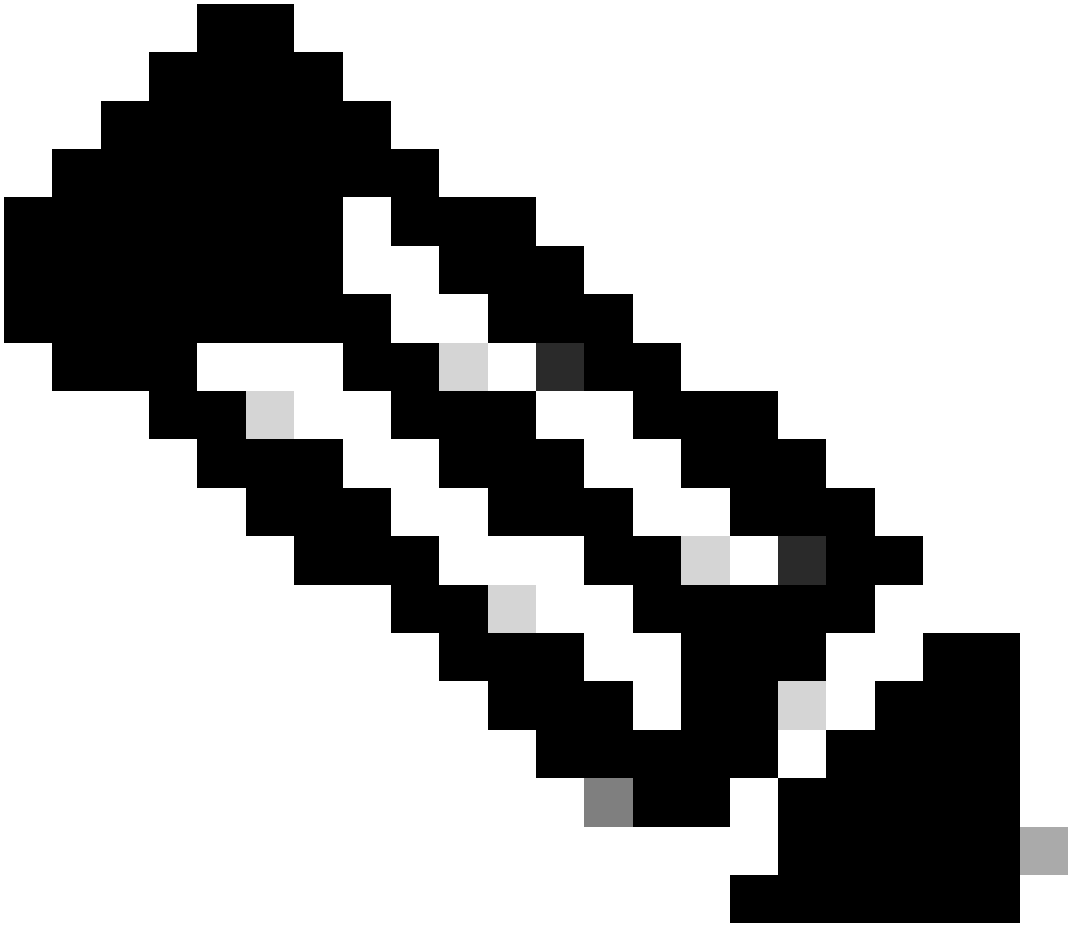
SAML أو لغة تمييز تأكيد الأمان هي معيار مفتوح لتبادل معلومات المصادقة والتفويض بين الأطراف، وعلى وجه التحديد موفر الهوية (IDp) ومزود الخدمة (SP). أصبح إستخدام مصادقة SAML لاتصالات Remote Access VPN (RAVPN) والتطبيقات الأخرى المختلفة شائعة بشكل متزايد بسبب مزاياها المتعددة. في مركز إدارة Firepower (FMC)، يمكن تكوين توصيفات توصيل متعددة لاستخدام تطبيقات محمية بمعرف P مختلفة بسبب خيار شهادة تجاوز مزود الهوية المتوفر في قائمة تكوين ملف تعريف الاتصال. تسمح هذه الميزة للمسؤولين بتجاوز شهادة IdP الأساسية في كائن خادم تسجيل الدخول الأحادي (SSO) بشهادة IdP معينة لكل ملف تعريف اتصال. ومع ذلك، فإن هذه الوظيفة محدودة على "مدير أجهزة FirePOWER (FDM)" الذي لا يوفر خيارا مماثلا. في حالة تكوين كائن SAML ثان، ويعرض المصادقة، يتم إنتاج رسالة الخطأ: "فشلت المصادقة بسبب مشكلة في إسترداد ملف تعريف الارتباط التسجيل الدخول الأحادي." للعمل على هذا القيد، يمكن إنشاء شهادة مخصصة ذاتية التوقيع واستيرادها في Azure لاستخدام عبر كل التطبيقات. ومن خلال القيام بذلك، يزيل متطلبات تثبيت شهادة واحدة فقط في إدارة قاعدة بيانات المحول (FDM)، مما يتيح إمكانية مصادقة SAML بسلاسة للتطبيقات المتعددة.

التكوين

الخطوة 1: إنشاء شهادة موقعة ذاتيا وملف PKCS#12 باستخدام OpenSSL

يوضح هذا القسم كيفية إنشاء الشهادة الموقعة ذاتيا باستخدام OpenSSL

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



ملاحظة: في هذا المستند، يتم إستخدام جهاز Linux، لذلك فإن بعض الأوامر خاصة ببيئة Linux. ومع ذلك، فإن أوامر OpenSSL هي نفسها.

ب. إنشاء ملف تكوين باستخدامtouch

.conf
الأمر.

<#root>

root@host#

touch config.conf

ج. تحرير الملف باستخدام محرر نصي. في هذا المثال، يتم إستخدام VIM ويتم تشغيل الأمرvim

.conf

. يمكنك إستخدام أي محرر نصوص آخر.

<#root>

root@host#

vim config.conf

د. أدخل المعلومات لتضمينها في التوقيع الذاتي.

تأكد من إستبدال القيم بين < > بمعلومات المؤسسة الخاصة بك.

[req]
distinguished_name = req_distinguished_name
prompt = no

[req_distinguished_name]
C =

ST =

L =

O =

OU =

CN =

ه. باستخدام هذا الأمر، يتم إنشاء مفتاح RSA خاص جديد إصدار 2048 بت وشهادة موقعة ذاتيا باستخدام خوارزمية SHA-256، صالحة لمدة 3650 يوما، استنادا إلى التكوين المحدد في

.conf

الملف. يتم حفظ المفتاح الخاص عليه

.pem

ويتم حفظ الشهادة الموقعة ذاتيا عليه

.crt

.

<#root>

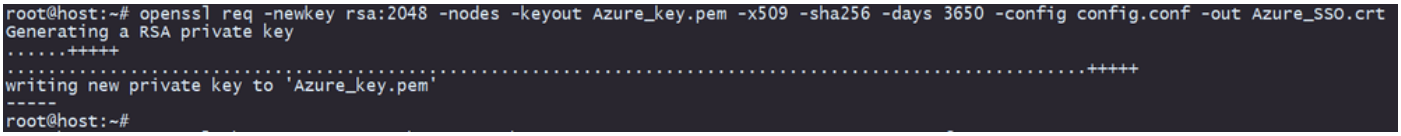
root@host#

openssl req -newkey rsa:2048 -nodes -keyout

.pem -x509 -sha256 -days 3650 -config

.conf -out

.crt



و. بعد إنشاء المفتاح الخاص والشهادة الموقعة ذاتيا، يقوم بتصديرهم إلى ملف PKCS#12، وهو تنسيق يمكن أن يتضمن كل من المفتاح الخاص والشهادة.

<#root>

root@host#

openssl pkcs12 -export -inkey

.pem -in

.crt -name

-out

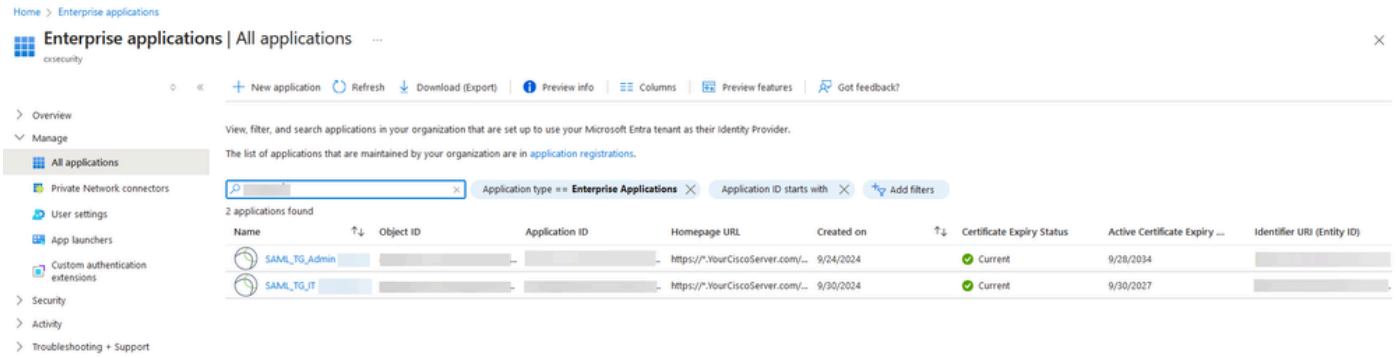
`.pfx`

```
root@host:~# openssl pkcs12 -export -inkey Azure_key.pem -in Azure_SSO.crt -out Azure_SSO.pfx
Enter Export Password:
Verifying - Enter Export Password:
root@host:~#
root@host:~# ls
Azure_SSO.crt  Azure_SSO.pfx  Azure_key.pem  config.conf
```

انتبه إلى كلمة المرور.

الخطوة 2: تحميل ملف PKCS#12 على Azure و FDM

تأكد من إنشاء تطبيق على Azure لكل توصيف توصيل يستخدم مصادقة SAML على FDM.

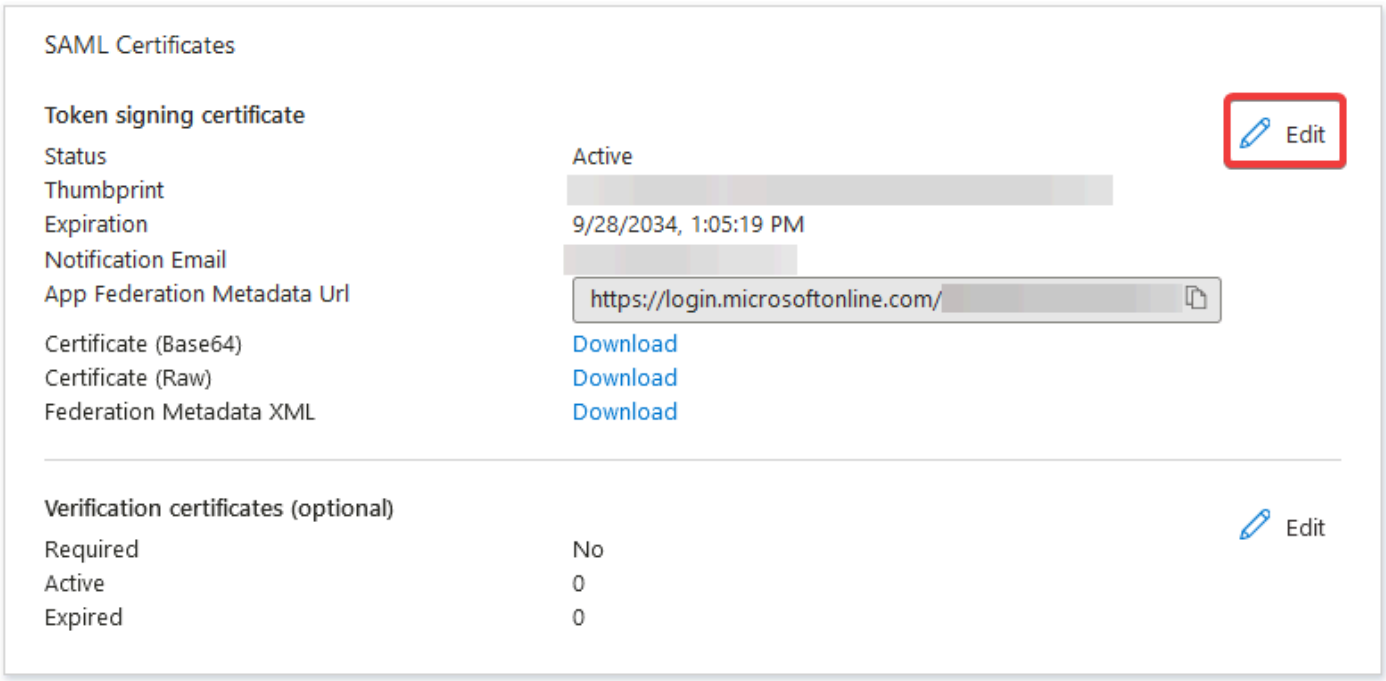


بمجرد حصولك على ملف PKCS#12 من الخطوة 1: إنشاء شهادة موقعة ذاتيا وملف PKCS#12 باستخدام OpenSSL، يجب تحميله إلى Azure للعديد من التطبيقات وتكوينه في تكوين FDM SSO.

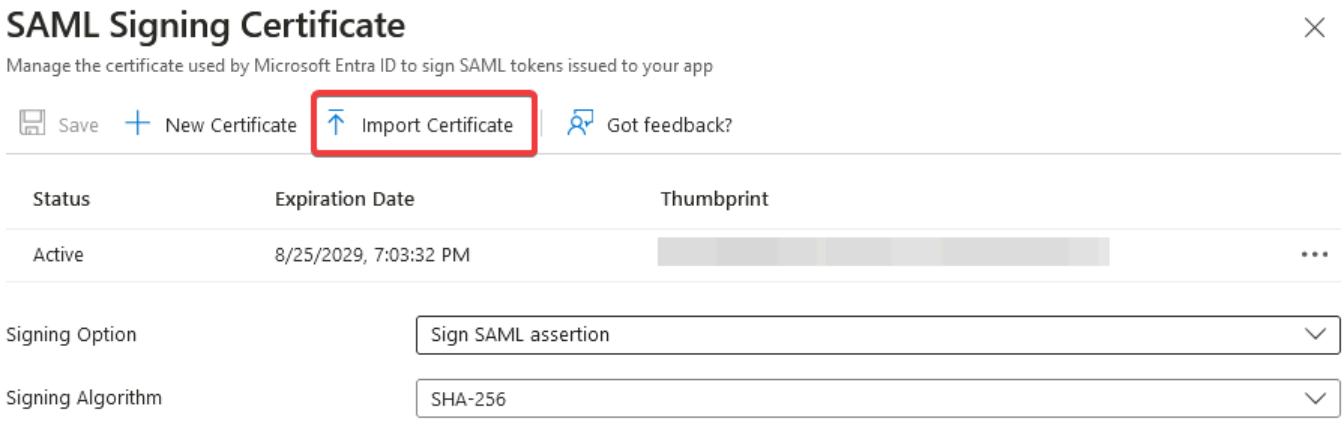
الخطوة 2.1. تحميل الشهادة إلى Azure

أ. سجل الدخول إلى مدخل Azure الخاص بك، وانتقل إلى تطبيق المؤسسة الذي تريد حمايته بمصادقة SAML، وحدد تسجيل الدخول الأحادي.

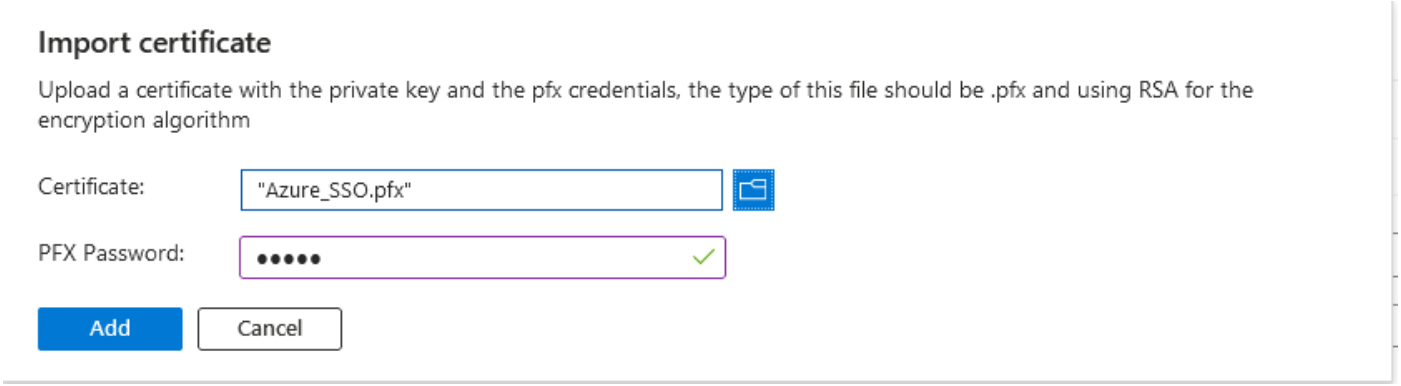
ب. قم بالتمرير لأسفل إلى قسم شهادات SAML وحدد المزيد من الخيارات > تحرير.



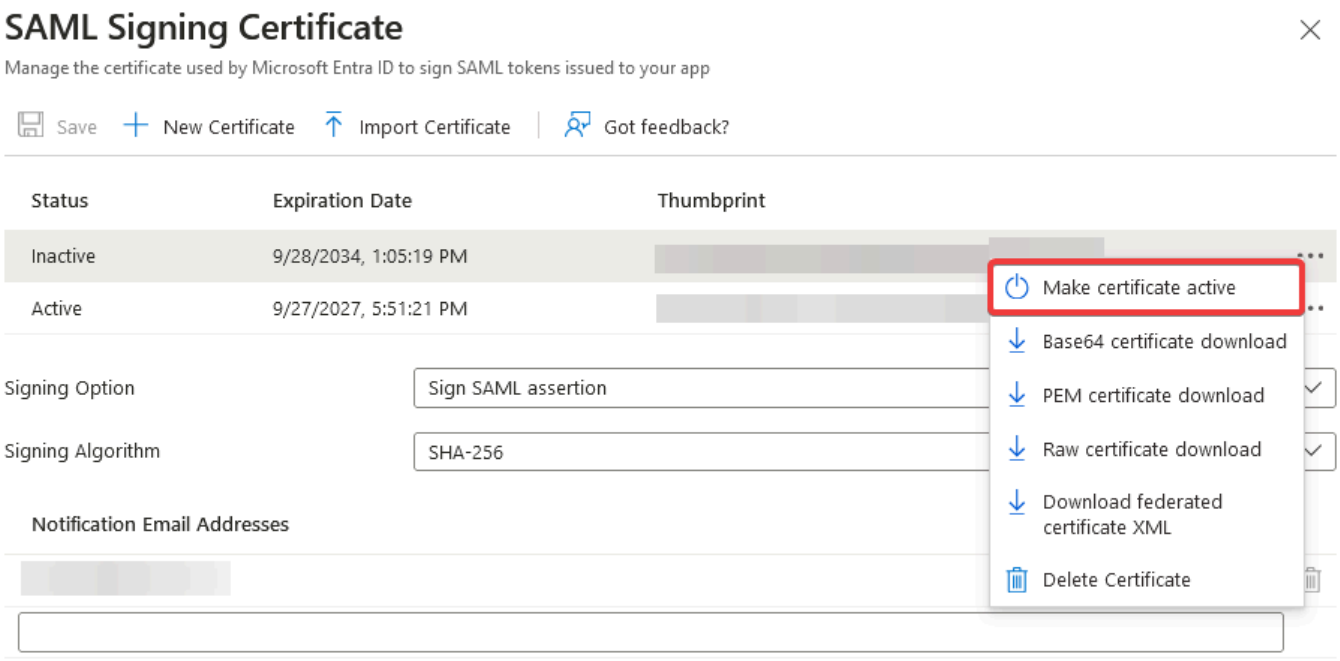
ج. الآن، حدد خيار إستيراد شهادة.

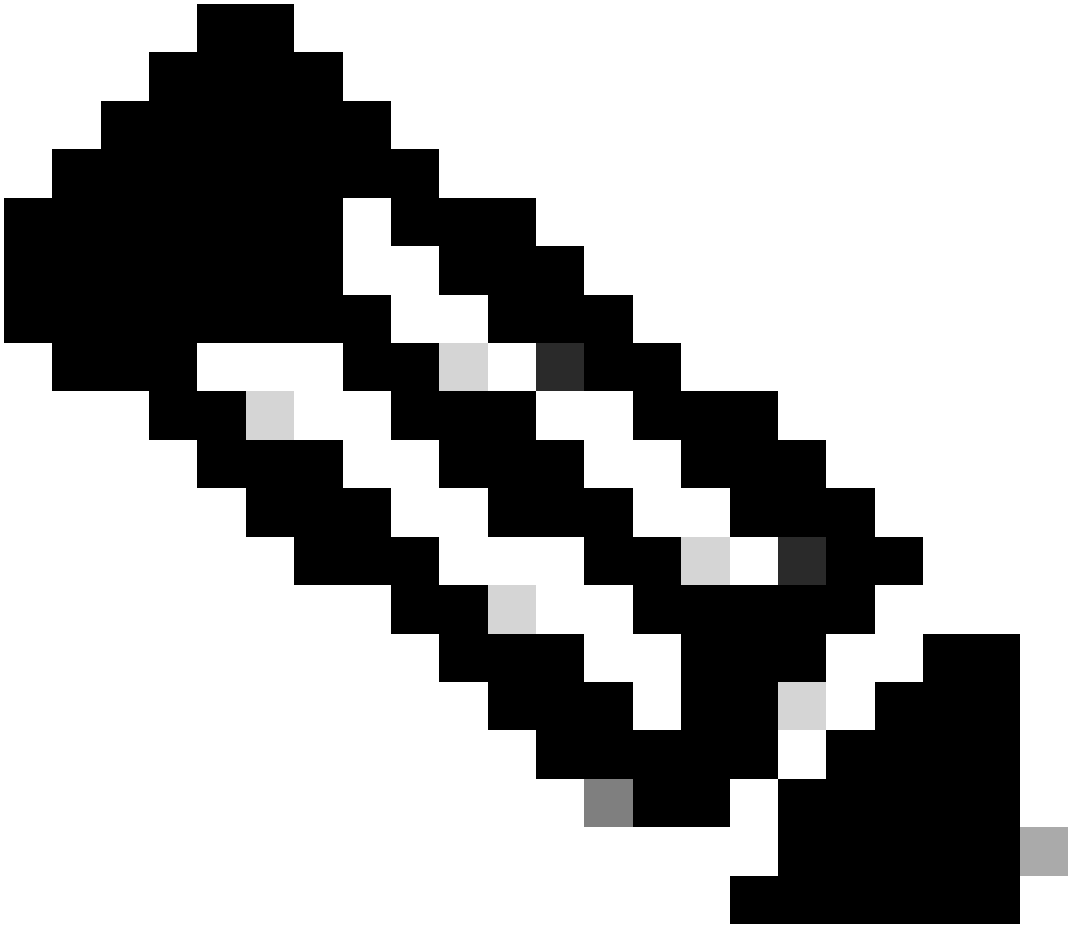


د. ابحث عن الـ PKCS#12 مبرد خلقت سابقا واستخدم الكلمة دخلت عندما خلقت الـ PKCS#12 مبرد.



ه. أخيرا، حدد خيار جعل الشهادة نشطة.

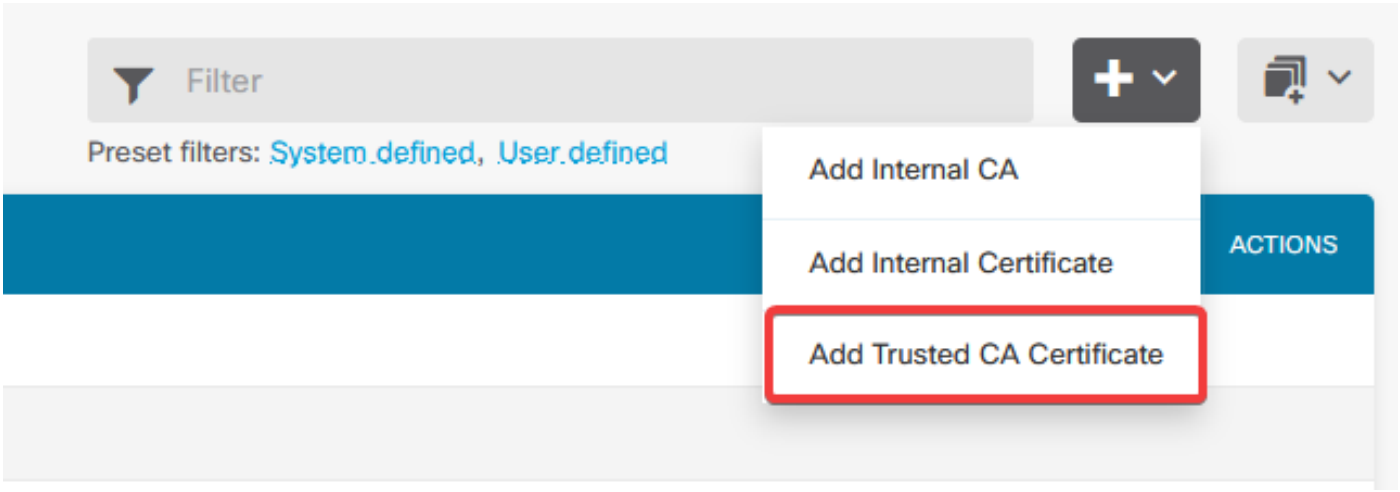




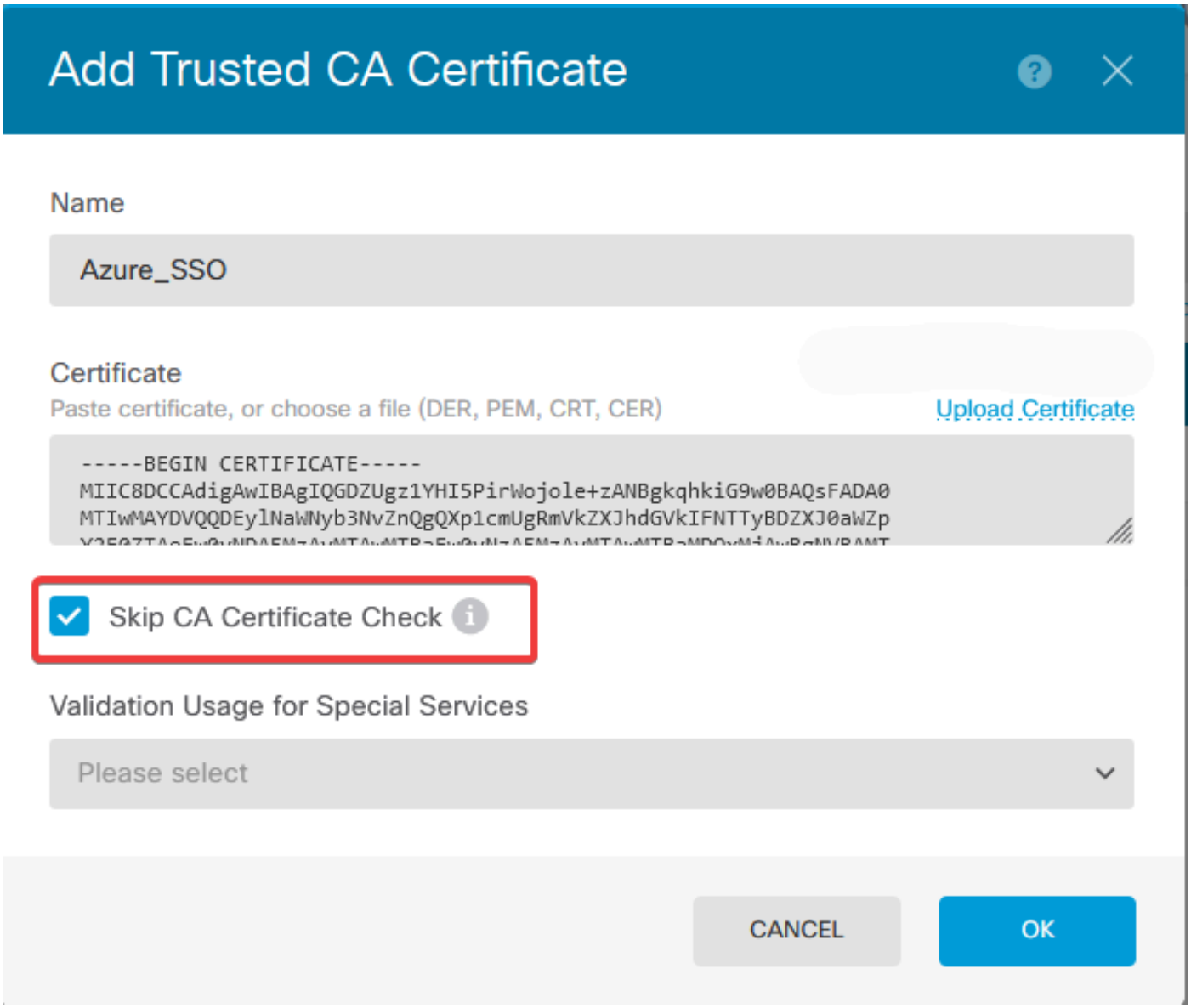
ملاحظة: تأكد من تنفيذ الخطوة 2.1: تحميل الشهادة إلى Azure لكل تطبيق.

الخطوة 2.2. تحميل الشهادة إلى FDM

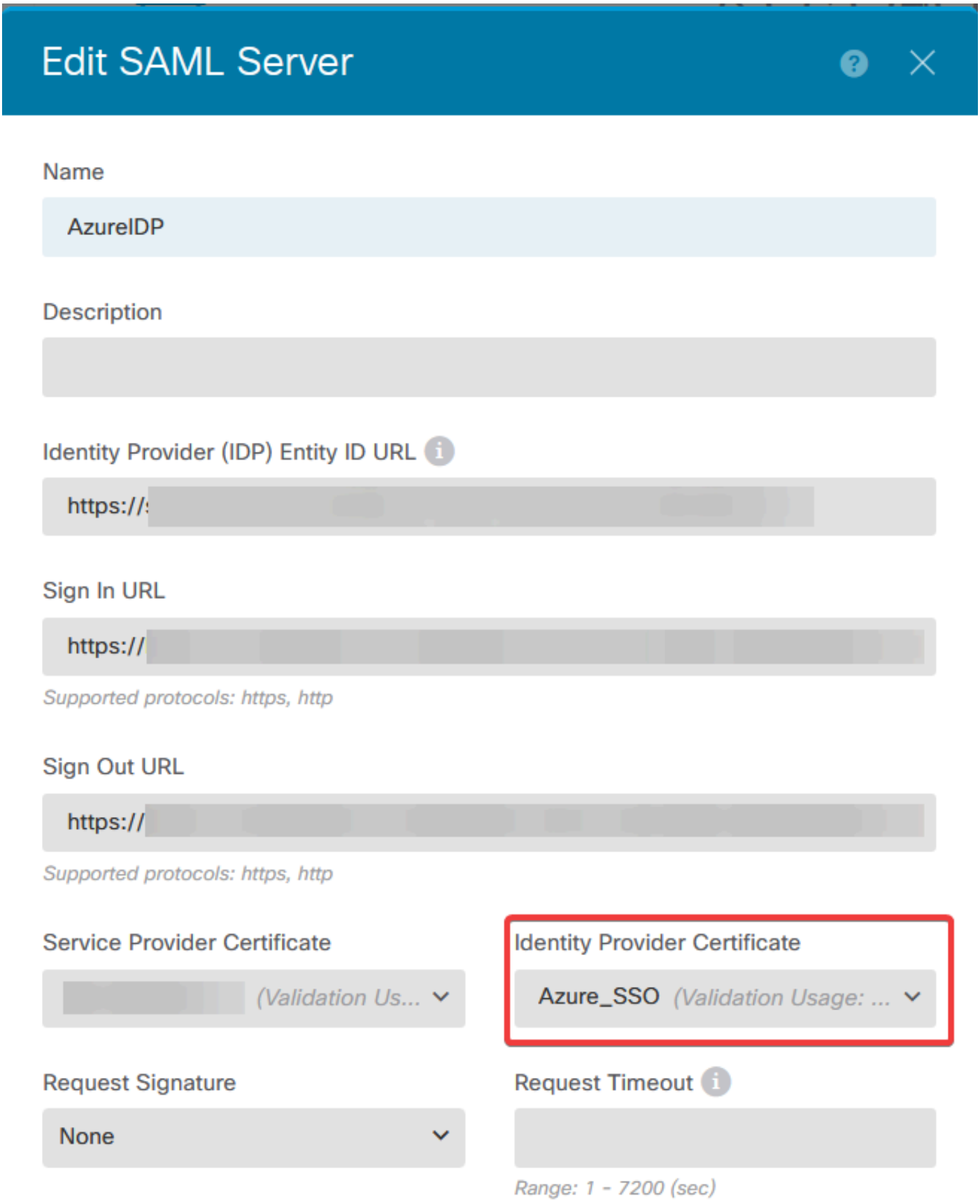
أ. انتقل إلى **Objects > Certificates > Click Add Trusted CA certificate.**



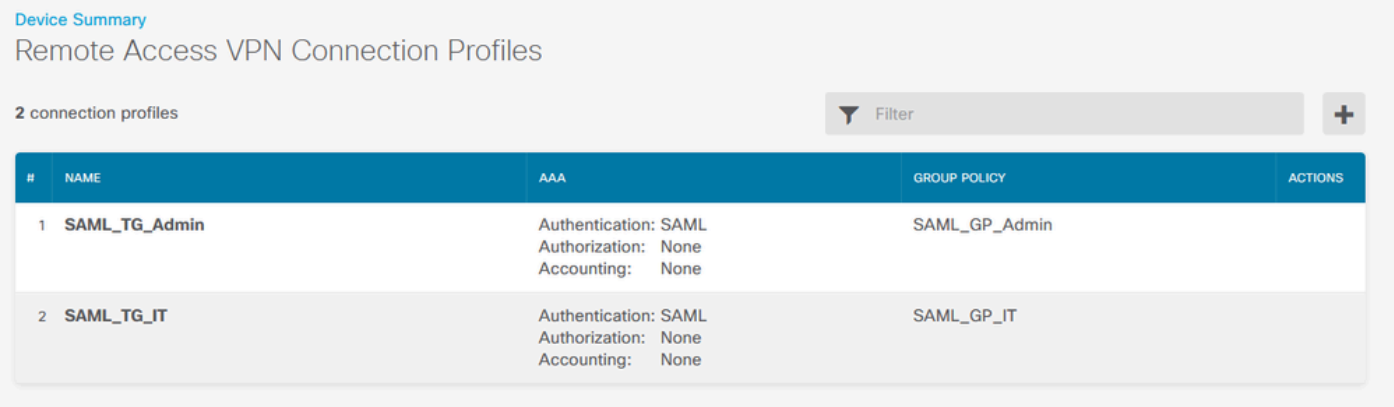
ب. أدخل اسم TrustPoint الذي تفضله وقم بتحميل شهادة الهوية فقط من IdP (ليس ملف PKCS#12)، وتحقق من **Skip CA Certificate Check.**

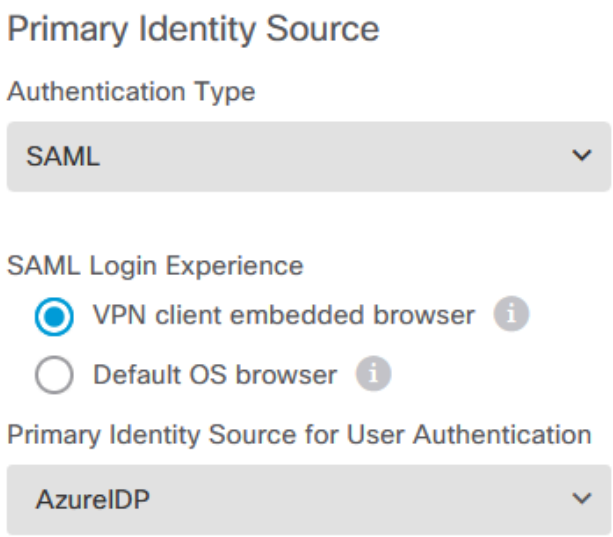


ج. تعيين الشهادة الجديدة في كائن SAML.



د. قم بتعيين كائن SAML على ملفات تعريف التوصيل المختلفة التي تستخدم SAML كطريقة مصادقة والتي تم إنشاء التطبيق لها في Azure. نشر التغييرات





التحقق من الصحة

قم بتشغيل show running-configWebVPN وshow running-config tunnel-groupالأمر لمراجعة التكوين والتحقق من تكوين نفس URL الخاص بالنازحين على ملفات تعريف الاتصال المختلفة.

<#root>

firepower#

show running-confuting webvpn

```
webvpn
 enable outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
   x-content-type-options
   x-xss-protection
   content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.10.08029-webdeploy-k9.pkg 2
```

```
 anyconnect profiles defaultClientProfile disk0:/anyconncprofs/defaultClientProfile.xml
 anyconnect enable

saml idp https://saml.lab.local/af42bac0

       /

  url sign-in https://login.saml.lab.local/af42bac0

      /saml2

 url sign-out https://login.saml.lab.local/af42bac0

       /saml2

 base-url https://Server.cisco.com

 trustpoint idp

Azure_SSO
```

```
 trustpoint sp FWCertificate

 no signature

 force re-authentication

 tunnel-group-list enable

 cache

 disable

 error-recovery disable

firepower#
```

<#root>

```
firepower#

show running-config tunnel-group


tunnel-group SAML_TG_Admin type remote-access
tunnel-group SAML_TG_Admin general-attributes
 address-pool Admin_Pool
 default-group-policy SAML_GP_Admin
tunnel-group SAML_TG_Admin webvpn-attributes

 authentication saml


 group-alias SAML_TG_Admin enable

 saml identity-provider https://saml.lab.local/af42bac0
```

```
       /

tunnel-group SAML_TG_IT type remote-access
tunnel-group SAML_TG_IT general-attributes
 address-pool IT_Pool
 default-group-policy SAML_GP_IT
tunnel-group SAML_TG_IT webvpn-attributes
 authentication saml

 group-alias SAML_TG_IT enable
 saml identity-provider https://saml.lab.local/af42bac0

       /

firepower#
```

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).