تكوين مصادقة SAML لملفات تعريف اتصال WAPN متعددة على FTD

المحتويات

المقدمة

يصف هذا المستند مصادقة SAML مع موفر هوية Azure لملفات تعريف توصيل متعددة على Cisco FTD المدارة بواسطة FMC.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- تكوين العميل الآمن على جدار الحماية من الجيل التالي (NGFW) المدار بواسطة مركز إدارة Firepower (FMC)
- قيم SAML و metadata.xml

المكونات المستخدمة

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

- الدفاع ضد تهديد Firepower (FTD)، الإصدار 7.4.0
- FMC، الإصدار 7.4.0
- Azure Microsoft Entra ID مع SAML 2.0
- Cisco Secure Client 5.1.7.80

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

يسمح هذا التكوين لـ FTD بمصادقة مستخدمي العميل الآمن باستخدام تطبيق SAML مختلف على Azure idp مع كائن SAML واحد تم تكوينه على FMC.

Name	Object ID	Application ID	Homepage URL	Created on	Certificate ...	Active Ce...	Identifier URI (Entity I...
FTD-SAML-1	44988e73-c06f-4008-be74...	0cff60a9-271f-4976-9848-...	https://*.YourCiscoServer....	25/11/2024	Current	25/11/2027	https://
FTD-SAML-2	dbe20be6-5440-4951-863...	2400bc8b-21b7-4f29-85c4...	https://*.YourCiscoServer....	25/11/2024	Current	27/11/2027	https://

في بيئة Microsoft Azure، يمكن للعديد من التطبيقات مشاركة نفس معرف الكيان. يتطلب كل تطبيق، يتم تعيينه بشكل نموذجي على مجموعة نفق مختلفة، شهادة فريدة، تتطلب تكوين شهادات متعددة ضمن تكوين معرف P على جانب FTD ضمن كائن SAML IdP واحد. ومع ذلك، الدعم بروتوكول FTD من Cisco تكوين شهادات متعددة ضمن كائن SAML IdP واحد، كما هو موضح في معرف تصحيح الأخطاء من Cisco CSCvi29084.

للتغلب على هذا التحدي، أدخلت Cisco ميزة تجاوز شهادة IdP، المتاحة من FTD الإصدار 7.1.0 و ASA الإصدار 9.17.1. يوفر هذه التحسين الحل دائما للمسألة ويكمل الحلول الموجودة الموضحة في تقرير الخطأ.

التكوينات

يوضح هذا القسم عملية تكوين مصادقة SAML باستخدام Azure كمزود الهوية (IDp) لملفات تعريف إتصالات متعددة على Cisco Firepower Threat Defense (FTD) الذي تتم إدارته بواسطة مركز إدارة FirePOWER (FMC). يتم إستخدام ميزة تجاوز شهادة IdP لإعداد هذا بشكل فعال.

نظرة عامة على التكوين:

يجب تكوين إثنين من ملفات تعريف الاتصال على FTD من Cisco:

- FTD-SAML-1
- FTD-SAML-2

في عينة التكوين هذه، يتم تعيين عنوان URL لعبارة VPN (Cisco Secure Client FQDN) على nigarapa2.cisco.com

التكوين

التكوين على Azure IDp

لتكوين تطبيقات SAML الخاصة بالمؤسسة ل Cisco Secure Client بشكل فعال، تأكد من تعيين جميع المعلمات بشكل صحيح لكل مجموعة نفق عن طريق إكمال الخطوات التالية:

الوصول إلى تطبيقات SAML الخاصة بالمؤسسات:

انتقل إلى وحدة التحكم الإدارية لمورد SAML حيث يتم سرد تطبيقات المؤسسة.

حدد تطبيق SAML المناسب:

حدد تطبيقات SAML المطابقة لمجموعات نفق العميل الآمن من Cisco التي ترغب في تكوينها.

تكوين المعرف (معرف الكيان):

قم بتعيين المعرف (معرف الكيان) لكل تطبيق. يجب أن يكون هذا عنوان URL الأساسي، وهو اسم المجال المؤهل بالكامل (FQDN) لـ Cisco Secure Client.

تعيين عنوان URL الخاص بالرد (عنوان URL لخدمة المستهلك للتأكيد):

قم بتكوين عنوان URL الخاص بالرد (عنوان URL الخاص بخدمة المستهلك للتأكيد) باستخدام عنوان URL الأساسي الصحيح. تأكد من أنها تتوافق مع FQDN الخاص بالعميل الآمن من Cisco.

قم بإلحاق ملف تعريف الاتصال أو اسم مجموعة النفق بعنوان URL الأساسي لضمان التحديد.

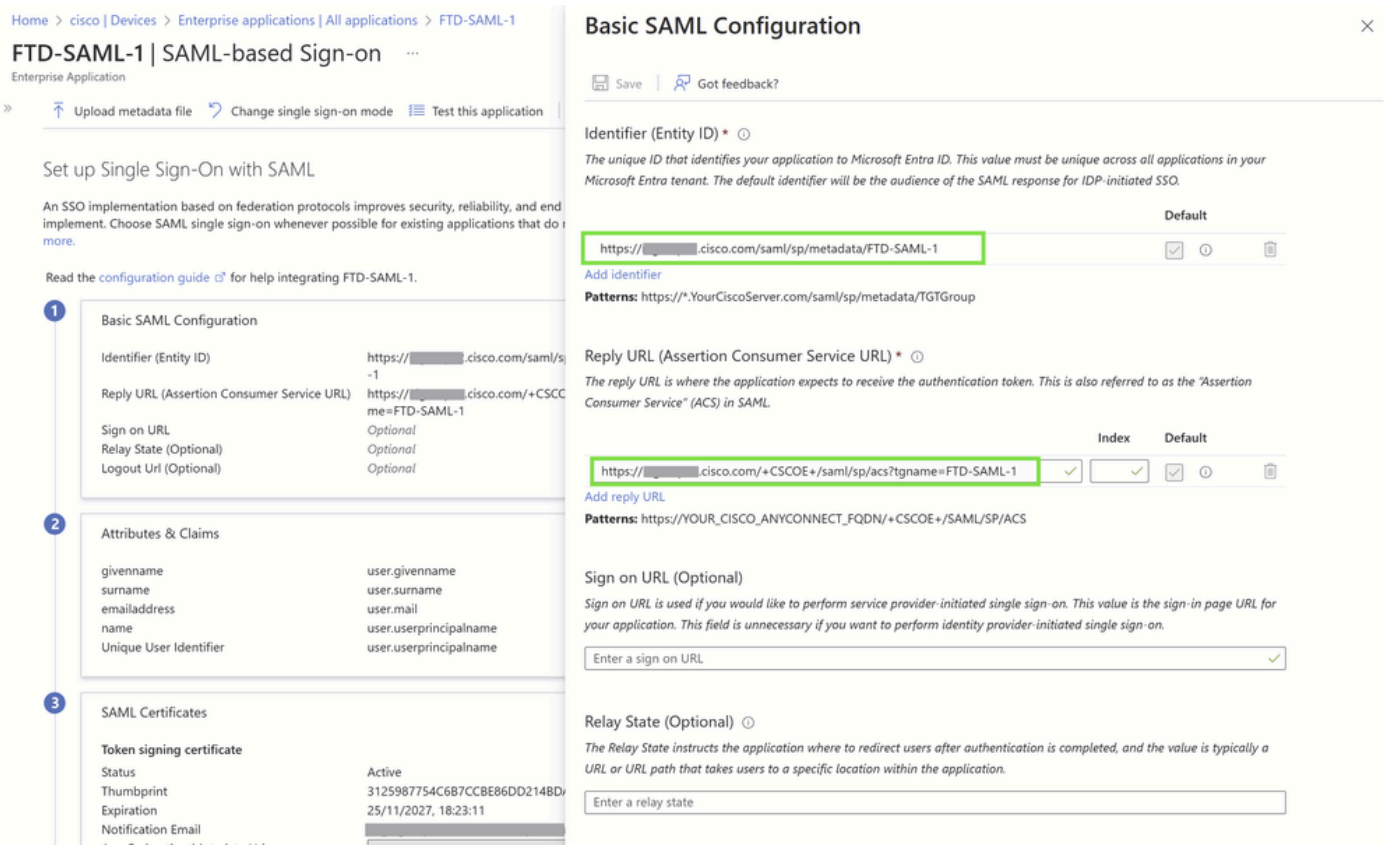
التحقق من التكوين:

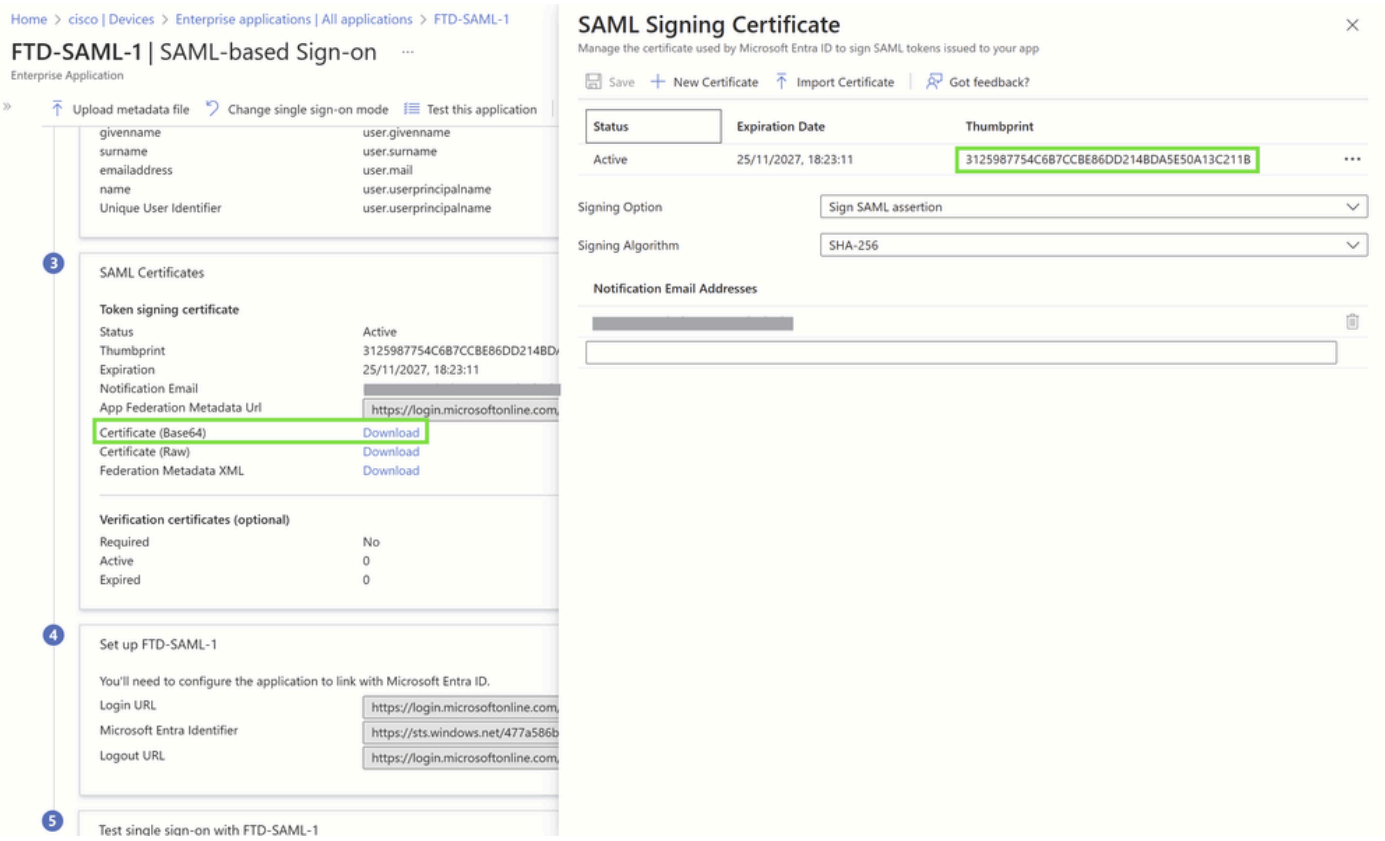
تحقق من إدخال كافة عناوين URL والمعلمات بشكل صحيح ومن مطابقتها لمجموعات النفق الخاصة.

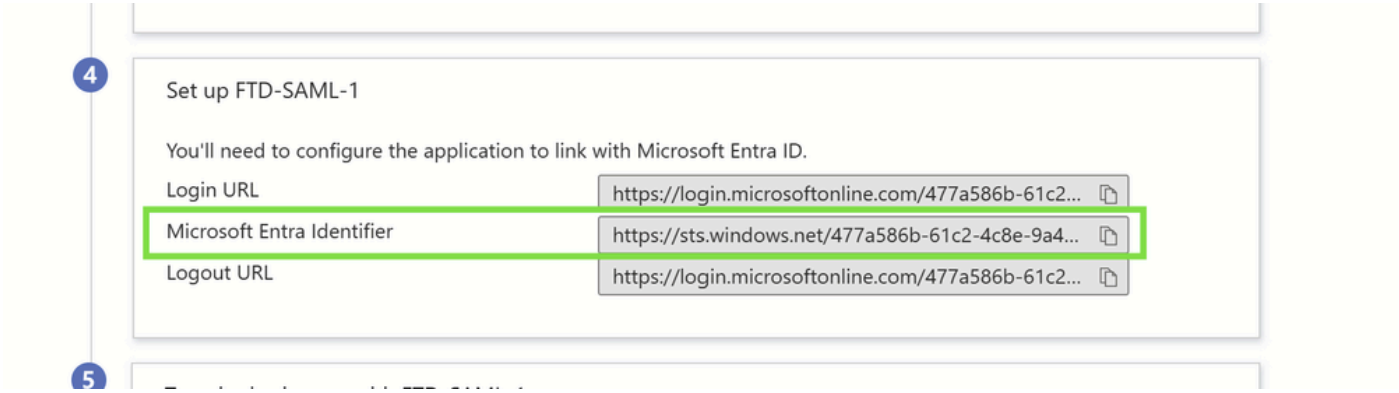
قم بحفظ التغييرات، وإذا أمكن، قم بإجراء اختبار المصادقة لضمان عمل التكوين كما هو متوقع.

للحصول على إرشادات أكثر تفصيلاً، راجع "إضافة عميل Cisco الآمن من مزود تطبيقات Microsoft" في وثائق Cisco: [تكوين ASA Secure Client VPN مع Microsoft Azure MFA من خلال SAML]

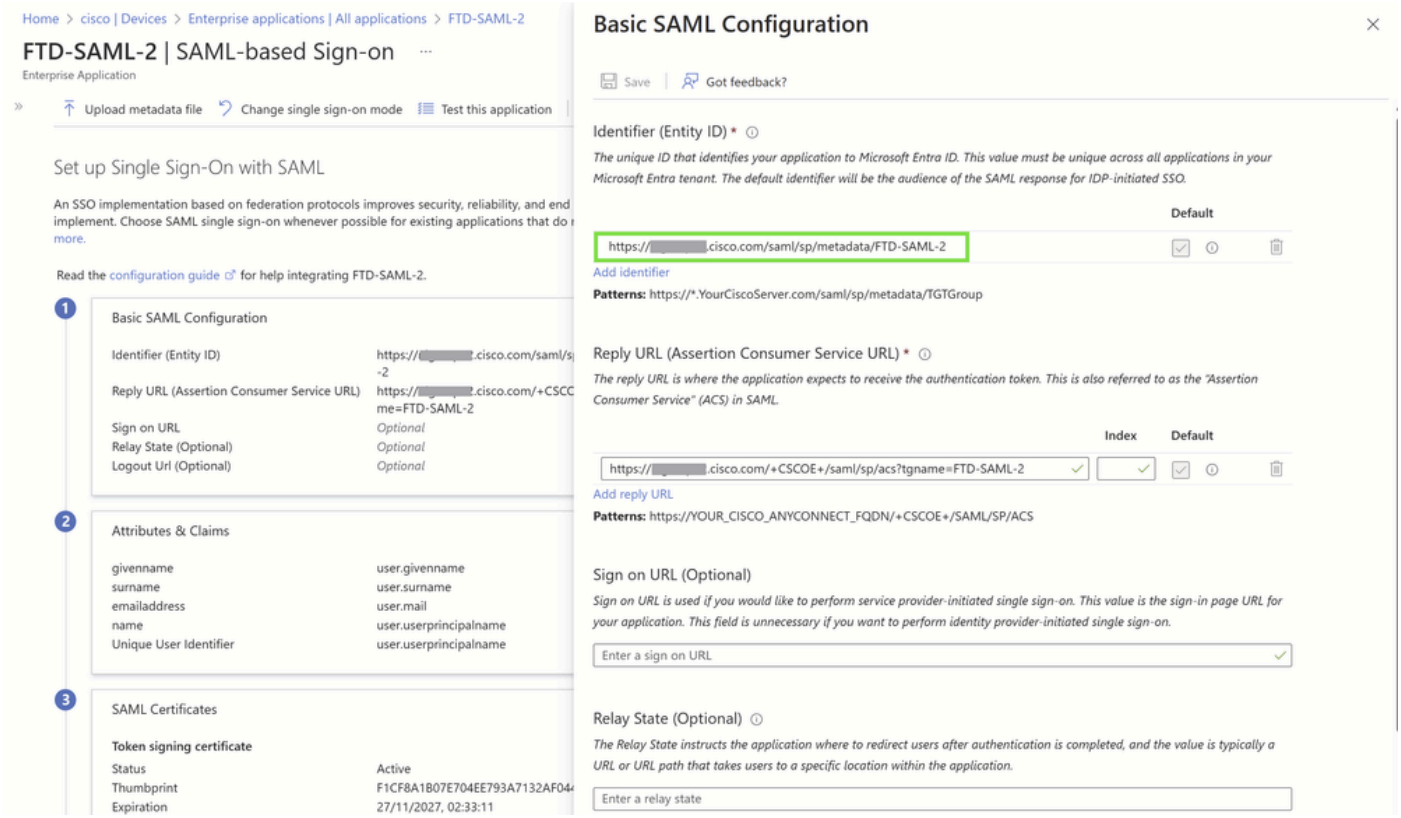
FTD-SAML-1

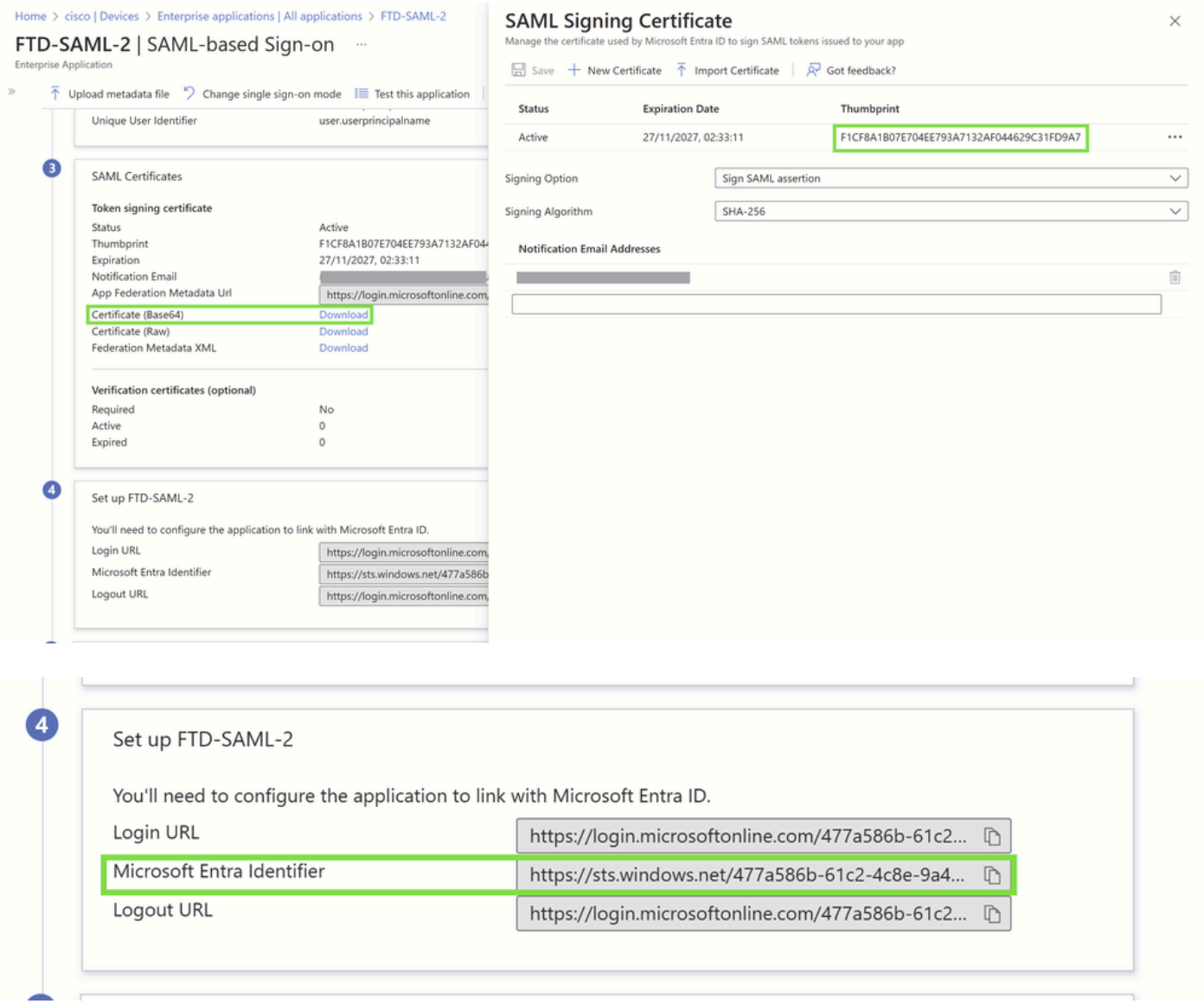

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end
implement. Choose SAML single sign-on whenever possible for existing applications that do
more.
Read the configuration guide for help integrating FTD-SAML-1.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
Optional
Optional
Optional
2
Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
Basic SAML Configuration
Save
Got feedback?
Identifier (Entity ID) *
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
Default
https://.cisco.com/saml/sp/metadata/FTD-SAML-1
Add identifier
Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup
Reply URL (Assertion Consumer Service URL) *
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.
Index
Default
https://.cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-1
Add reply URL
Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS
Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.
Enter a sign on URL
Relay State (Optional)
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
Enter a relay state


Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
App Federation Metadata Url
https://login.microsoftonline.com/
Certificate (Base64)
Download
Certificate (Raw)
Download
Federation Metadata XML
Download
Verification certificates (optional)
Required
No
Active
0
Expired
0
4
Set up FTD-SAML-1
You'll need to configure the application to link with Microsoft Entra ID.
Login URL
https://login.microsoftonline.com/
Microsoft Entra Identifier
https://sts.windows.net/477a586b
Logout URL
https://login.microsoftonline.com/
5
Test single sign-on with FTD-SAML-1
SAML Signing Certificate
Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app
Save
New Certificate
Import Certificate
Got feedback?
Status
Expiration Date
Thumbprint
Active
25/11/2027, 18:23:11
3125987754C6B7CCBE86DD214BDA5E50A13C211B
Signing Option
Sign SAML assertion
Signing Algorithm
SHA-256
Notification Email Addresses


4
Set up FTD-SAML-1
You'll need to configure the application to link with Microsoft Entra ID.
Login URL
https://login.microsoftonline.com/477a586b-61c2...
Microsoft Entra Identifier
https://sts.windows.net/477a586b-61c2-4c8e-9a4...
Logout URL
https://login.microsoftonline.com/477a586b-61c2...
5

FTD-SAML-2


Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-2
FTD-SAML-2 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end
implement. Choose SAML single sign-on whenever possible for existing applications that do
more.
Read the configuration guide for help integrating FTD-SAML-2.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
Optional
Optional
Optional
2
Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Thumbprint
Expiration
Active
27/11/2027, 02:33:11
Basic SAML Configuration
Save
Got feedback?
Identifier (Entity ID) *
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
Default
.cisco.com/saml/sp/metadata/FTD-SAML-2
Add identifier
Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup
Reply URL (Assertion Consumer Service URL) *
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.
Index
Default
.cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-2
Add reply URL
Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS
Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.
Enter a sign on URL
Relay State (Optional)
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
Enter a relay state



الآن يرجى التأكد من أن لديك المعلومات والملفات اللازمة لتكوين مصادقة SAML مع Microsoft Entra كموفر الهوية الخاص بك:

حدد موقع معرف Microsoft Entra:

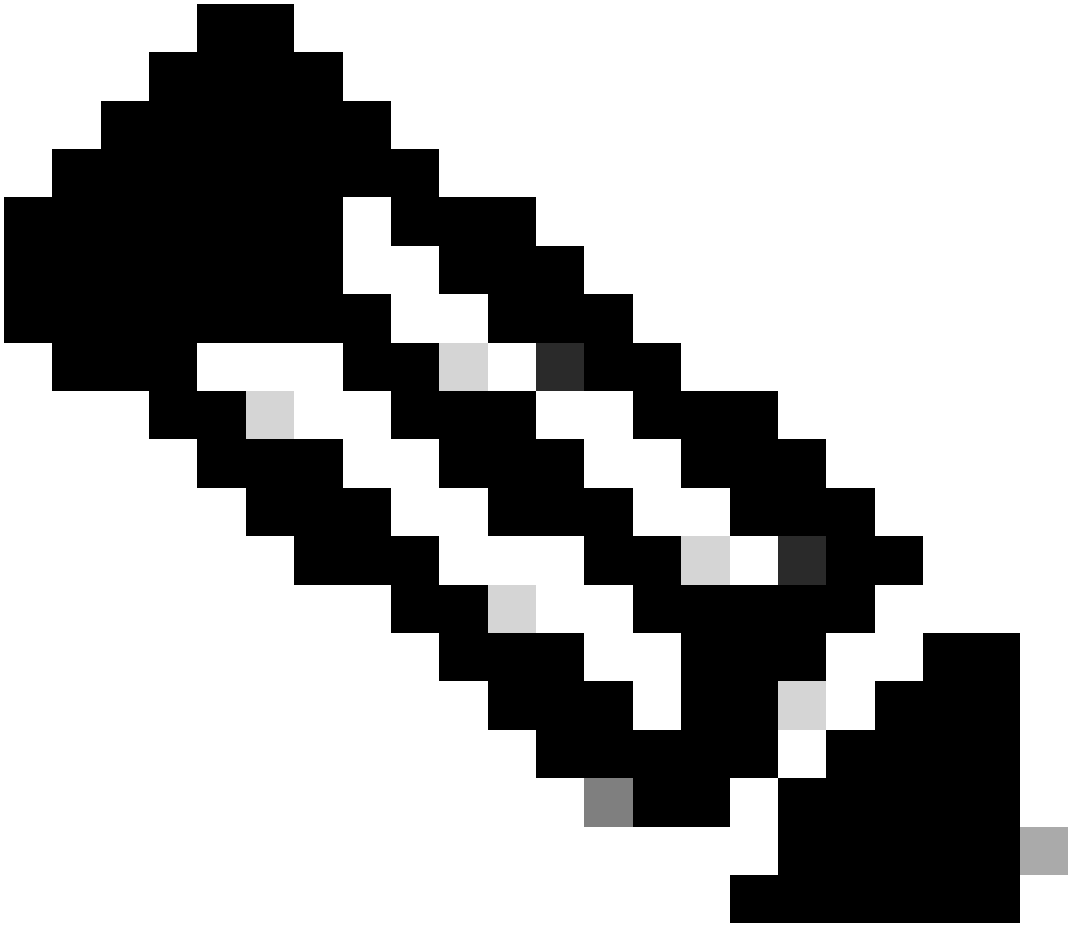
قم بالوصول إلى إعدادات كل من تطبيقات SAML Enterprise داخل مدخل Microsoft Entra.

لاحظ معرف Microsoft Entra، الذي يظل متسقا عبر كل التطبيقين وهو مهم لتكوين SAML.

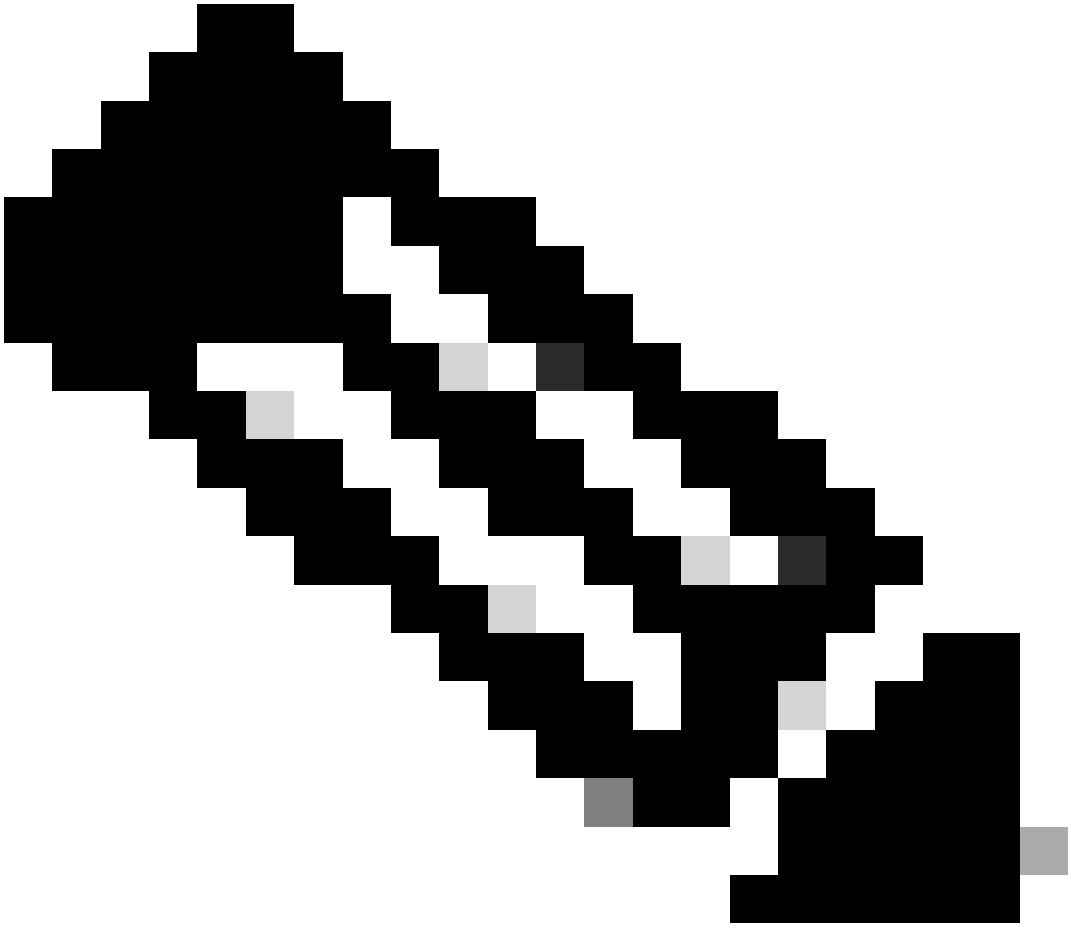
تنزيل شهادات Base64 IDp:

انتقل إلى كل تطبيق مكون من تطبيقات SAML Enterprise.

قم بتنزيل شهادات IdP الخاصة التي تم ترميزها بواسطة Base64. هذه الشهادات ضرورية لإنشاء الثقة بين موفر الهوية الخاص بك وإعداد Cisco VPN الخاص بك.



ملاحظة: كل تكوينات SAML هذه المطلوبة لملفات تعريف اتصال FTD يمكن أيضا الحصول عليها من ملفات التعريف.xml التي توفرها IdP الخاصة بك للتطبيقات المعنية.



ملاحظة: لاستخدام شهادة IdP مخصصة، تحتاج إلى تحميل شهادة IdP المنشأة خصيصا إلى كل من IdP و FMC. بالنسبة لمعرف Azure، تأكد من أن الشهادة بتنسيق PKCS#12. في FMC، قم بتحميل شهادة الهوية من IdP فقط، وليس ملف PKCS#12. للحصول على تعليمات تفصيلية، راجع القسم "تحميل ملف PKCS#12 على Azure و FDM" في وثائق Cisco: تشكيل توصيفات WAPN متعددة بمصادقة SAML على FDM

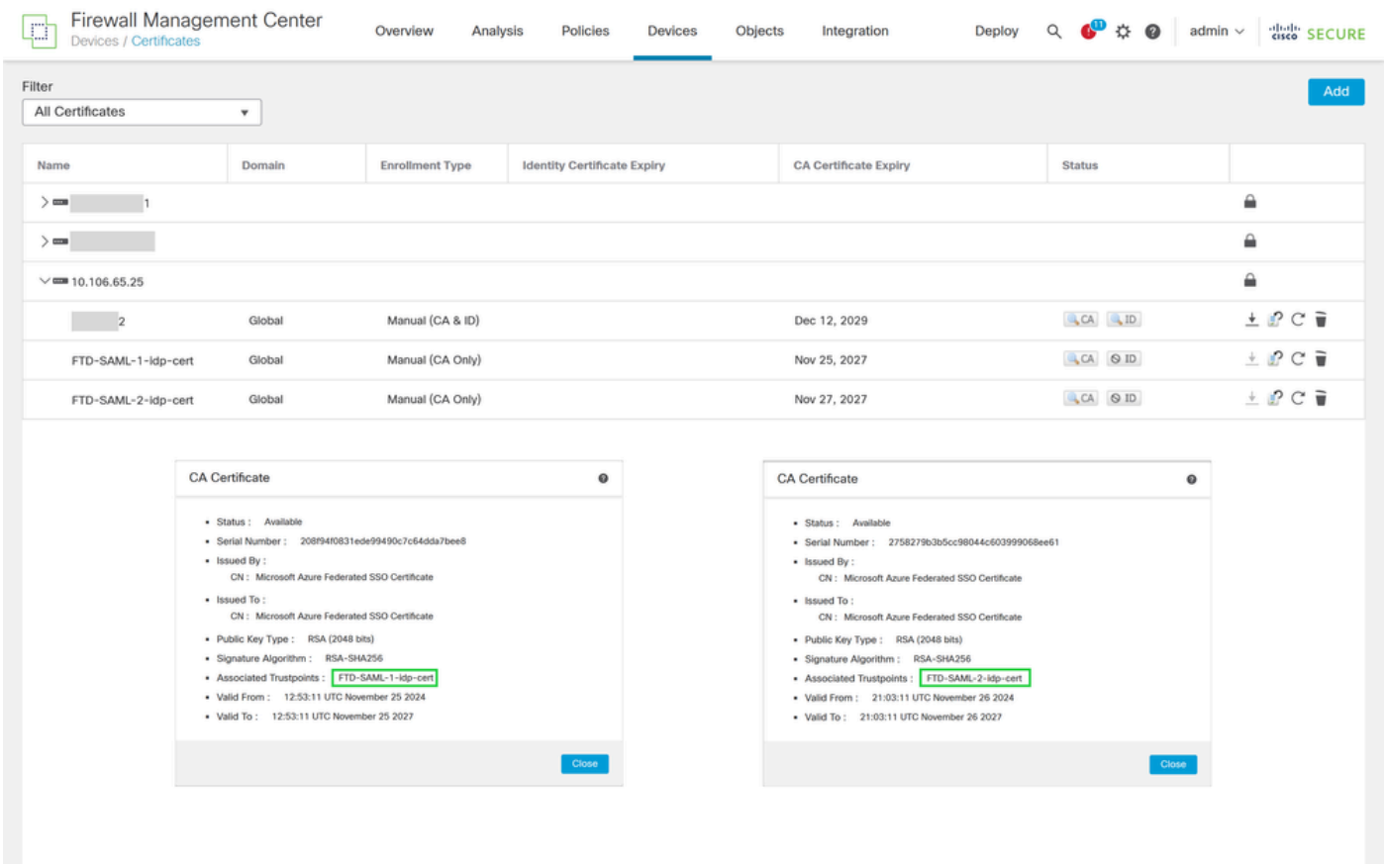
التكوين على FTD عبر FMC

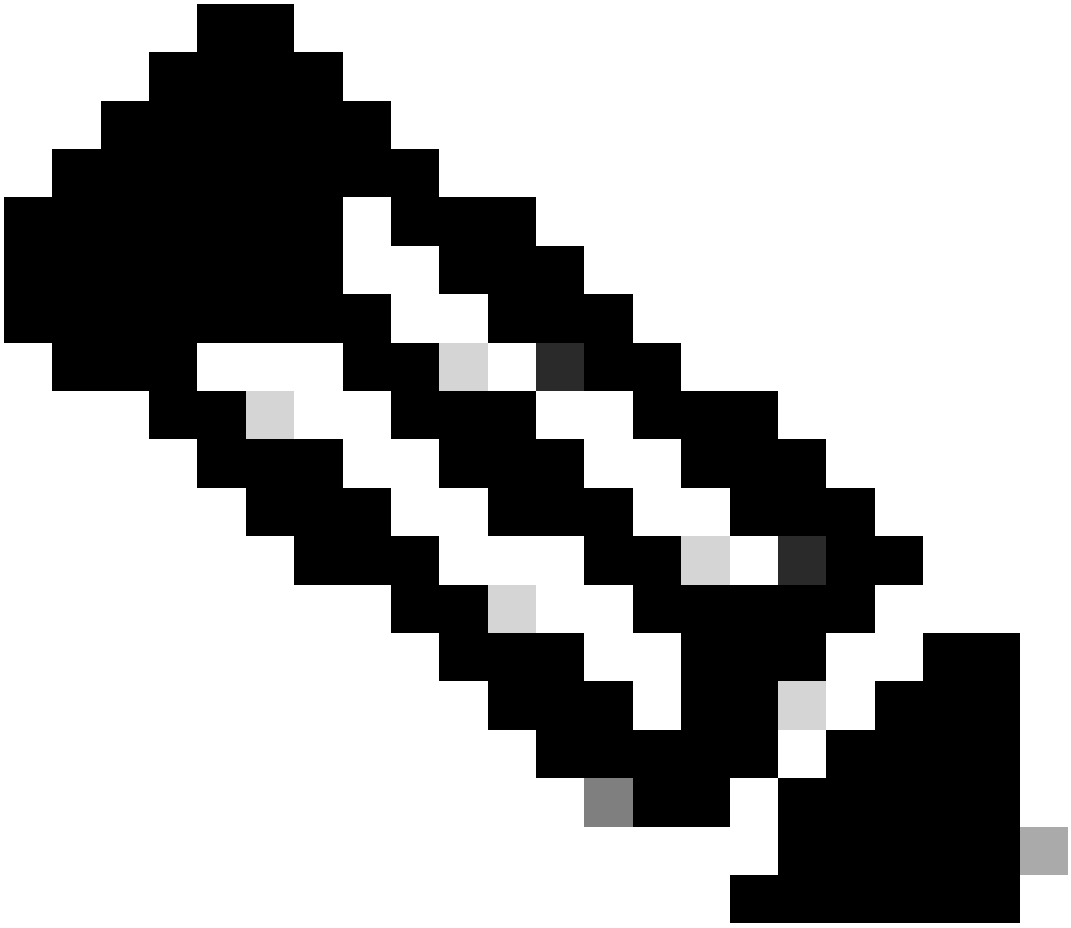
تسجيل شهادات IDp:

انتقل إلى قسم إدارة الشهادات داخل FMC وأدخل شهادات IdP التي تم تنزيلها والتي تم ترميزها بواسطة Base64 لكل من تطبيقي SAML. هذه الشهادات حيوية لإنشاء الثقة وتمكين مصادقة SAML.

للحصول على إرشادات تفصيلية، يرجى الرجوع إلى الخطوتين الأوليين ضمن "التكوين على FTD عبر FMC" في وثائق Cisco المتوفرة على: تكوين Secure Client باستخدام

مصادقة SAML على FTD المدار عبر FMC.





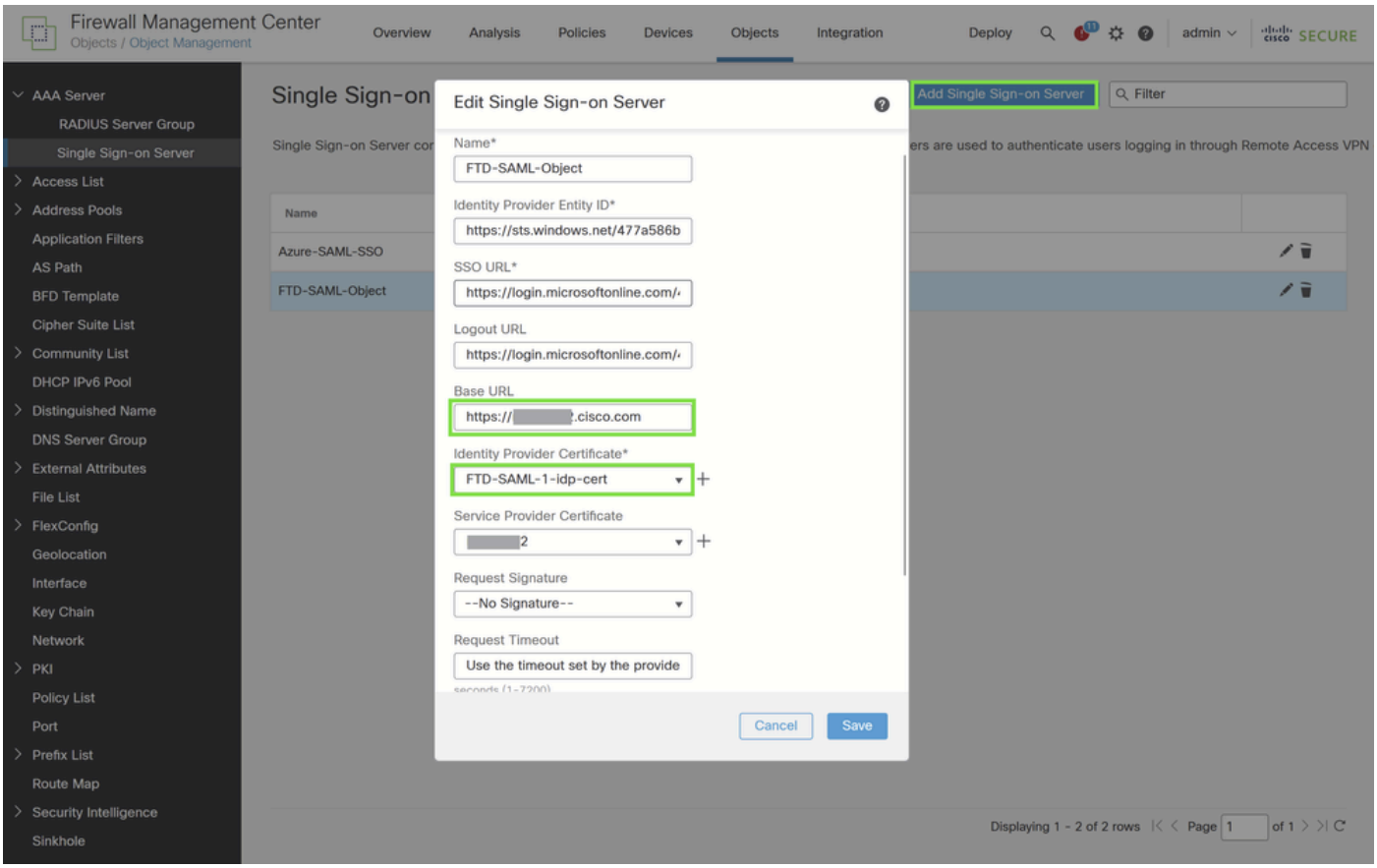
ملاحظة: تم تحرير الصورة لعرض كل الشاشتين في نفس الوقت من أجل عرض أفضل. لا يمكن فتح كل الشاشتين في نفس الوقت على FMC.

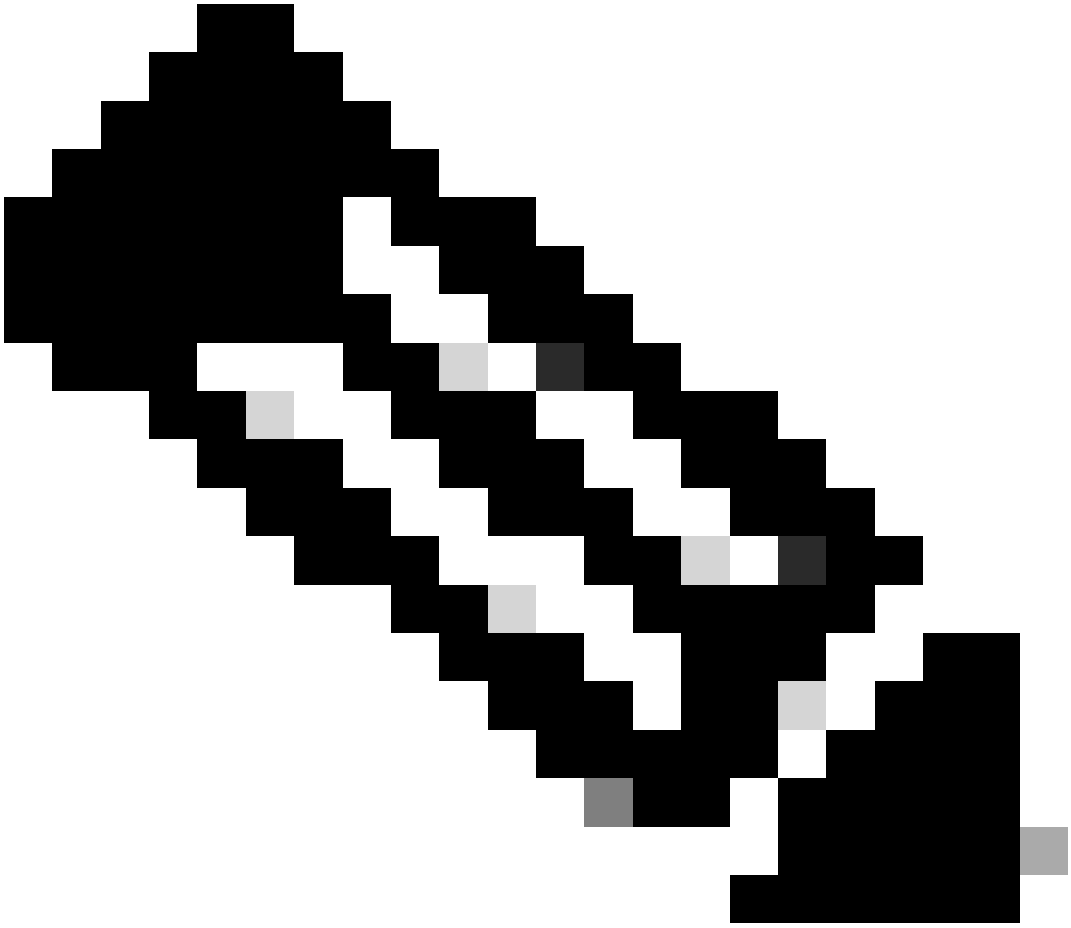
تكوين إعدادات خادم SAML على Cisco FTD من خلال FMC

لتكوين إعدادات خادم SAML على الدفاع عن تهديد FirePOWER (FTD) من Cisco باستخدام مركز إدارة FirePOWER (FMC)، قم بتنفيذ الخطوات التالية:

1. انتقل إلى تكوين خادم تسجيل الدخول الأحادي:
   - انتقل إلى كائنات > إدارة الكائن > خوادم AAA > خادم تسجيل الدخول الأحادي.
   - انقر فوق إضافة خادم تسجيل دخول أحادي لبدء تكوين خادم جديد.
2. تكوين إعدادات خادم SAML:
   - باستخدام المعلومات التي تم تجميعها من تطبيقات SAML الخاصة بالمؤسسة أو من ملف Metadata.xml الذي تم تنزيله من موفر الهوية (IdP)، قم بتعبئة قيم SAML الضرورية في نموذج خادم تسجيل الدخول الأحادي الجديد.
   - تتضمن المعلومات الرئيسية التي سيتم تكوينها ما يلي:
     - معرف كيان موفر SAML: ENTITYid من metadata.xml

- عنوان URL الخاص بالموجه الخاص بالموجه: SingleSignOnService من metadata.xml.
- عنوان URL لتسجيل الخروج: SingleLogoutService من metadata.xml.
- عنوان URL الأساسي: FQDN لشهادة معرف SSL ل FTD الخاصة بك.
- شهادة موفر الهوية: شهادة توقيع IDp.
  - تحت قسم شهادة مزود الهوية، قم بإرفاق إحدى شهادات IdP المسجلة
  - في حالة الاستخدام هذه، نستخدم شهادة IdP من تطبيق FTD-SAML-1.
- شهادة موفر الخدمة: شهادة توقيع FTD.



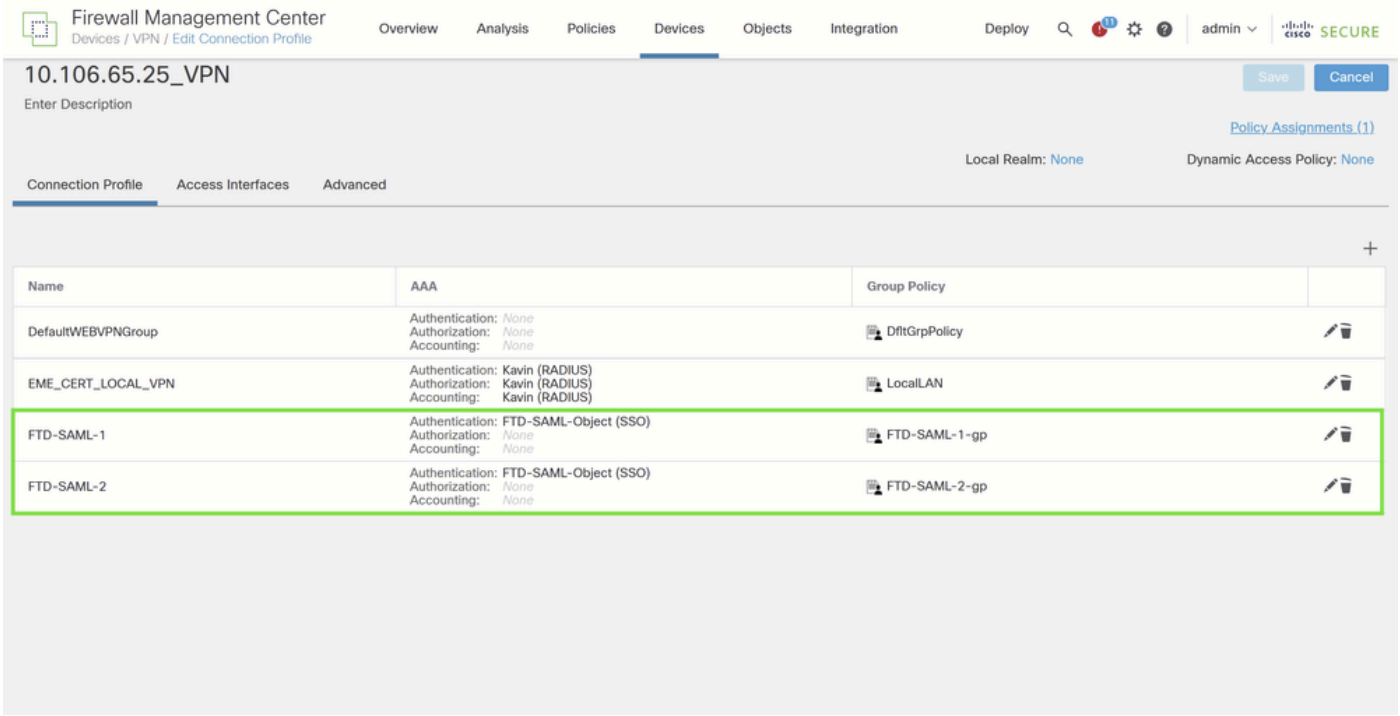


ملاحظة: في التكوين الحالي، يمكن فقط إستبدال شهادة موفر الهوية من كائن SAML ضمن إعدادات ملف تعريف الاتصال. لسوء الحظ، لا يمكن تمكين الميزات مثل "تمكين معرف P الذي يمكن" و"طلب إعادة مصادقة معرف P عند تسجيل الدخول" بشكل فردي أو تعطيلها لكل ملف تعريف اتصال.

تكوين ملفات تعريف الاتصال على Cisco FTD عبر FMC

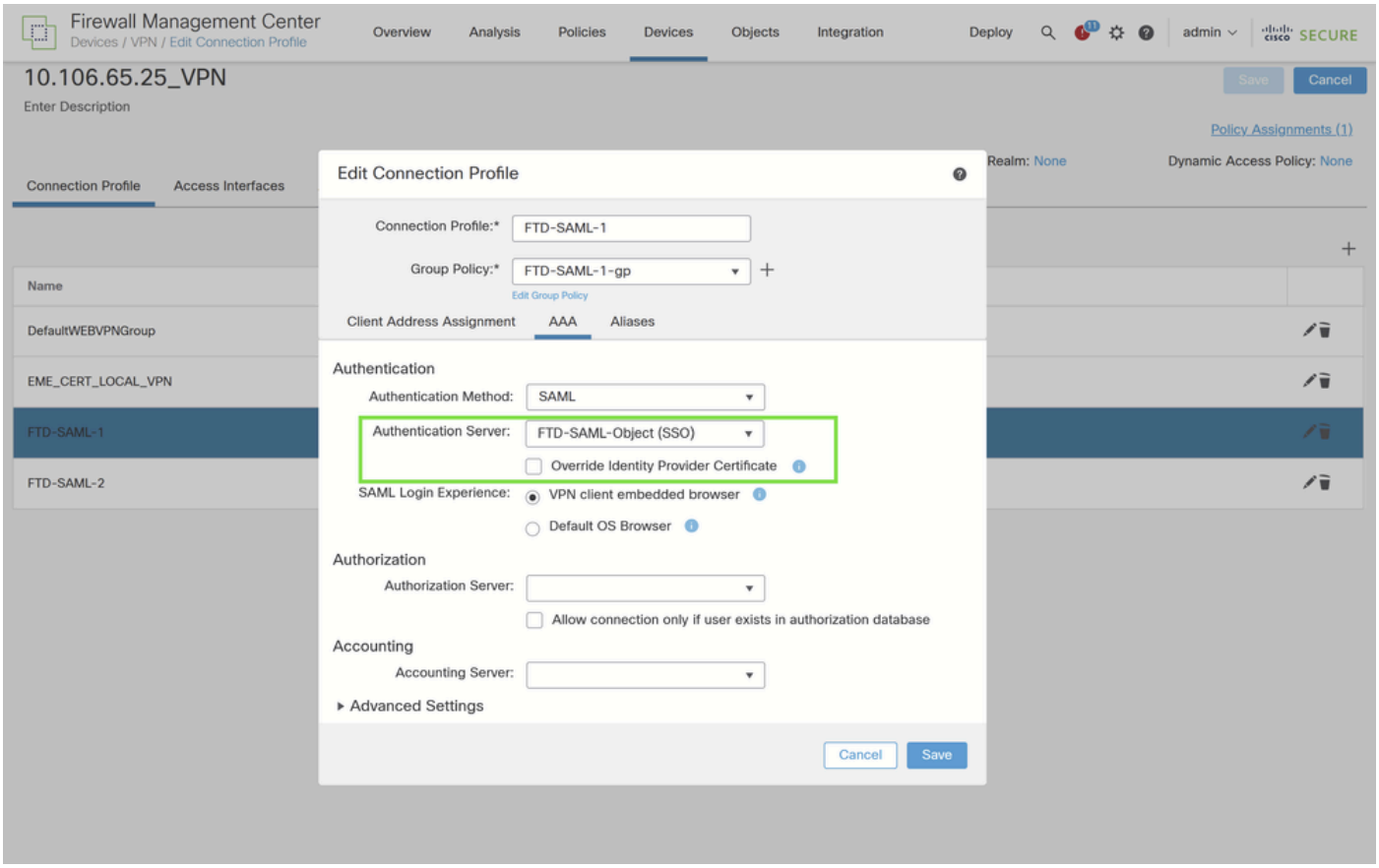
لإنهاء إعداد مصادقة SAML، يلزمك تكوين توصيفات التوصيل بالمعلومات المناسبة وتعيين مصادقة AAA على SAML باستخدام خادم SAML الذي تم تكوينه مسبقا.

للحصول على إرشادات أكثر تفصيلا، ارجع إلى الخطوة الخامسة ضمن "التكوين في FTD عبر FMC" في وثائق Cisco: تكوين Secure Client باستخدام مصادقة SAML على FTD المدار عبر FMC.



إستخراج تكوين AAA لملف تعريف الاتصال الأول

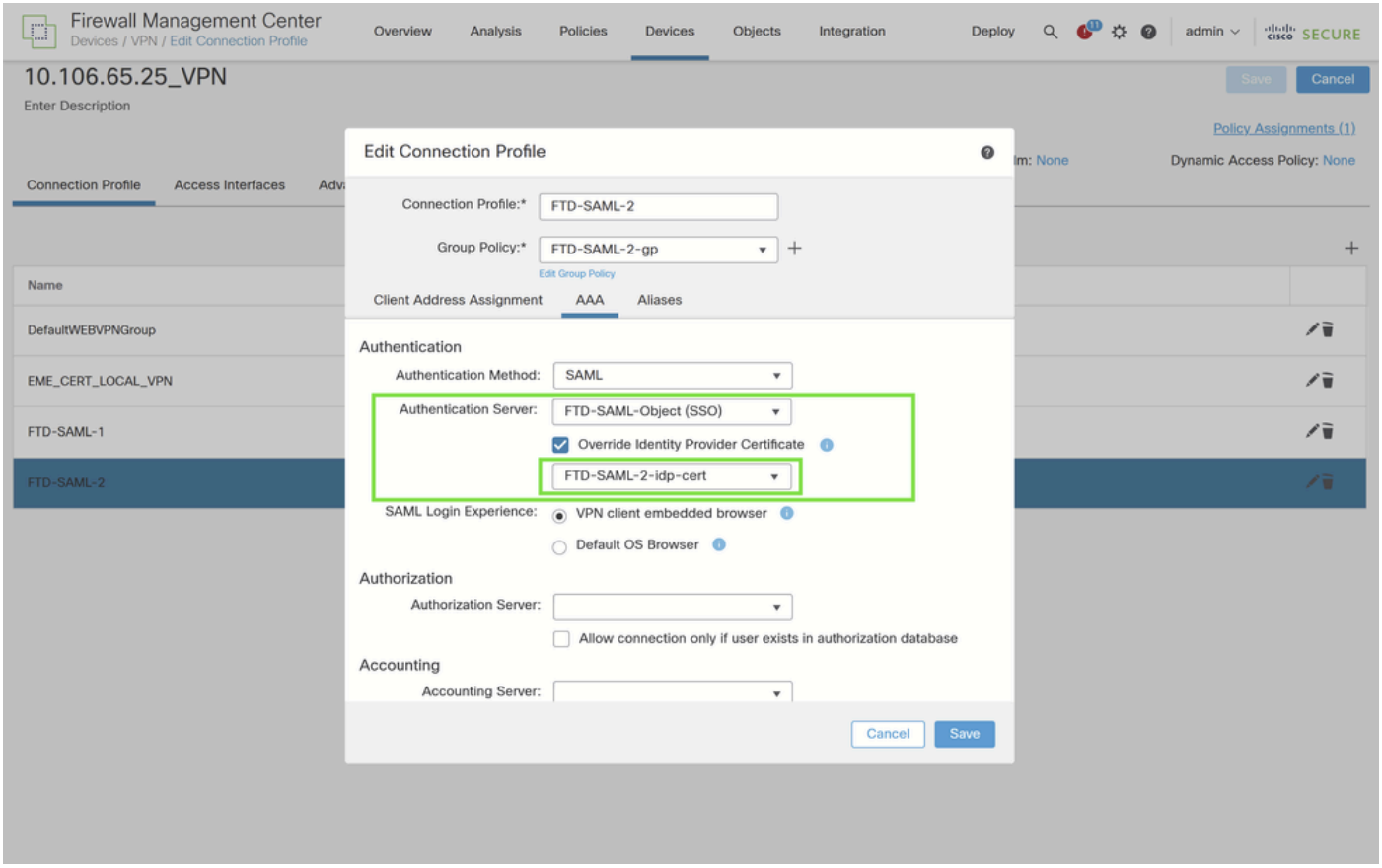
فيما يلي نظرة عامة على إعدادات تكوين AAA لتوصيف الاتصال الأول:



تكوين تجاوز شهادة IDp لملف تعريف الاتصال الثاني في Cisco FTD
للتأكد من إستخدام شهادة موفر الهوية (IdP) الصحيحة لملف تعريف الاتصال الثاني، قم بتمكين تجاوز شهادة IdP بإكمال الخطوات التالية:

ضمن إعدادات توصيف التوصيل، حدد مكان خيار "تخطي شهادة مزود الهوية" وقم بتمكينه للسماح باستخدام شهادة IdP مختلفة عن تلك التي تم تكوينها لخادم SAML.

من قائمة شهادات IdP المسجلة، حدد الشهادة المسجلة خصيصا لتطبيق FTD-SAML-2. يضمن هذا التحديد إستخدام شهادة IDp الصحيحة عند إجراء طلب مصادقة لملف تعريف الاتصال هذا.



نشر التكوين

انتقلDeploy > Deploymentإلى تحديد FTD المناسب لتطبيق تغييرات VPN لمصادقة SAML.

التحقق من الصحة

التكوين على سطر أوامر FTD

<#root>

```
firepower# sh run 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
    Secure Client image disk0:/csm/Secure Client-win-4.10.08025-webdeploy.pkg 1 regex "Windows"
    Secure Client enable


 saml idp https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/


        url sign-in https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2


        url sign-out https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2


        base-url https://nigarapa2.cisco.com


        trustpoint idp FTD-SAML-1-idp-cert


        trustpoint sp nigarapa2


        no signature


        force re-authentication


    tunnel-group-list enable
    cache
        disable
    error-recovery disable
firepower#
```

<#root>

```
firepower# sh run tunnel-group FTD-SAML-1
tunnel-group FTD-SAML-1 type remote-access
tunnel-group FTD-SAML-1 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-1-gp
tunnel-group FTD-SAML-1 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-1 enable


saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/


firepower#
```

<#root>

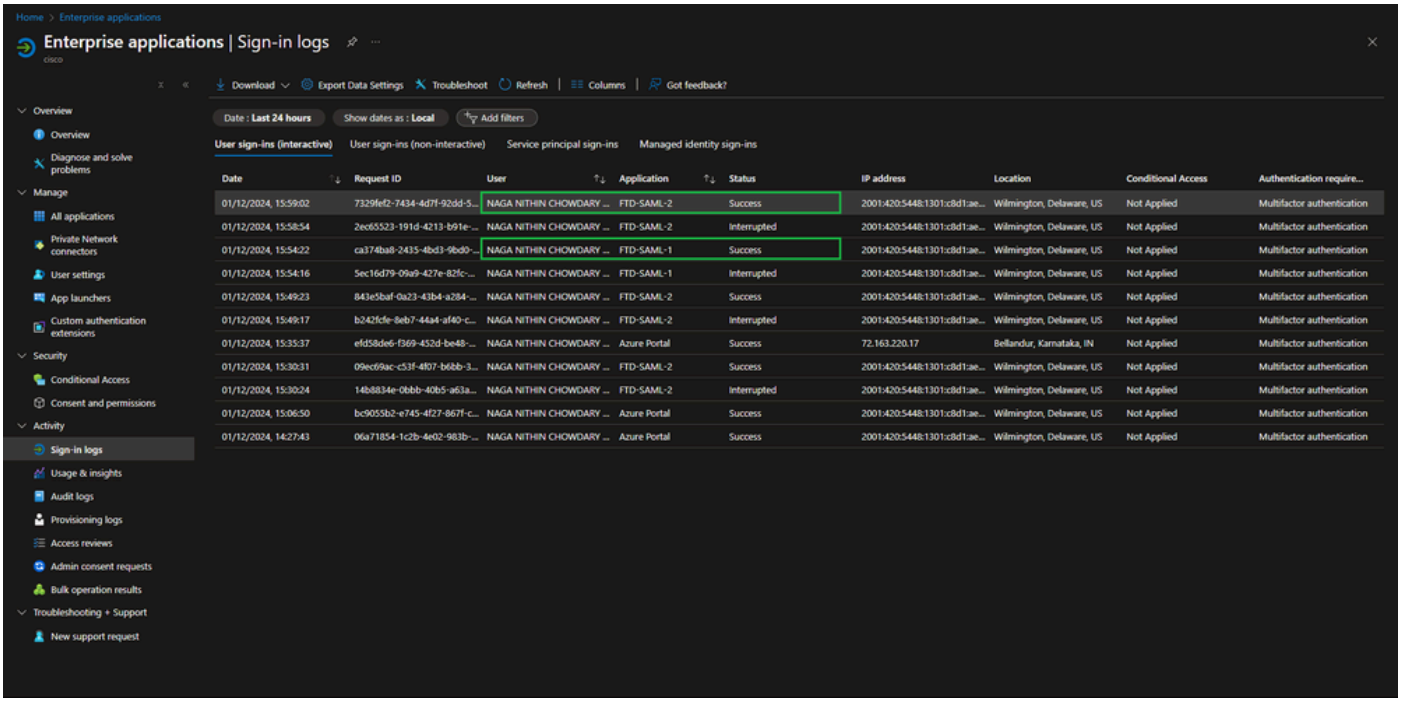
```
firepower# sh run tunnel-group FTD-SAML-2
tunnel-group FTD-SAML-2 type remote-access
tunnel-group FTD-SAML-2 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-2-gp
tunnel-group FTD-SAML-2 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-2 enable
    saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/


    saml idp-trustpoint FTD-SAML-2-idp-cert

firepower#
```

سجل تسجيل الدخول من معرف معرف معرف معرف بطاقة Azure

قم بالوصول إلى قسم سجلات تسجيل الدخول ضمن تطبيق المؤسسة. ابحث عن طلبات المصادقة المتعلقة بتوصيفات التوصيل المحددة، مثل FTD-SAML-1 وFTD-SAML-2. تحقق من أن المستخدمين يقومون بالمصادقة بنجاح من خلال تطبيقات SAML المقترنة بكل ملف تعريف اتصال.



سجلات تسجيل الدخول على Azure IdP

استكشاف الأخطاء وإصلاحها

1. يمكنك أستكشاف الأخطاء وإصلاحها باستخدام DART من كمبيوتر المستخدم العميل الآمن.

2. لاستكشاف أخطاء مصادقة SAML وإصلاحها، أستخدم تصحيح الأخطاء هذا:

```
<#root>

firepower#

 debug webvpn saml 255
```

3. تحقق من تكوين "العميل الآمن" كما هو موضح أعلاه؛ يمكن إستخدام هذا الأمر للتحقق من الشهادة.

```
<#root>

firepower#

 show crypto ca certificate
```

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).