SAML Auth configureren voor meerdere RAVPN-verbindingsprofielen op FTD

Inhoud

Inleiding

Dit document beschrijft SAML-verificatie met Azure Identity Provider voor meerdere verbindingsprofielen op Cisco FTD die worden beheerd door FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Beveiligde clientconfiguratie op Next Generation Firewall (NGFW), beheerd door Firepower Management Center (FMC)
- SAML- en metatada.xml-waarden

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Threat Defence (FTD) versie 7.4.0
- FMC versie 7.4.0
- Azure Microsoft Entra ID met SAML 2.0
- Cisco Secure-client 5.1.7.80

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Met deze configuratie kan FTD beveiligde clientgebruikers authenticeren met twee verschillende SAML-applicaties op Azure idp met één SAML-object geconfigureerd op 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://

In een Microsoft Azure-omgeving kunnen meerdere toepassingen dezelfde entiteit-id delen. Elke toepassing, meestal in kaart gebracht aan een verschillende tunnelgroep, vereist een uniek certificaat, dat de configuratie van meerdere certificaten vereist binnen de configuratie van IDP van de FTD-kant onder één enkel voorwerp van SAML IdP. Cisco FTD ondersteunt echter niet de configuratie van meerdere certificaten onder één SAML IDp-object, zoals gedetailleerd in Cisco bug ID CSCvi29084.

Om deze beperking te overwinnen, heeft Cisco de functie voor het negeren van IDP-certificaten geïntroduceerd die beschikbaar is via FTD versie 7.1.0 en ASA versie 9.17.1. Deze verbetering biedt een permanente oplossing voor het probleem en vormt een aanvulling op de bestaande tijdelijke oplossingen die in het bugrapport worden beschreven.

Configuraties

In dit gedeelte wordt het proces beschreven voor het configureren van SAML-verificatie met Azure als Identity Provider (IDP) voor meerdere verbindingsprofielen op Cisco Firepower Threat Defence (FTD), beheerd door Firepower Management Center (FMC). De functie voor het negeren van het IDP-certificaat wordt gebruikt om dit effectief in te stellen.

Overzicht van configuratie:

Er moeten twee verbindingsprofielen worden geconfigureerd op Cisco FTD:

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

In deze configuratiesteekproef, wordt de VPN gateway-URL (Cisco Secure Client FQDN) ingesteld op nigarapa2.cisco.com

Configureren

Configuratie op Azure IDP

Zorg ervoor dat alle parameters correct zijn ingesteld voor elke tunnelgroep door deze stappen te

voltooien om uw SAML enterprise applicaties voor Cisco Secure Client effectief te configureren:

Toegang tot SAML Enterprise-toepassingen:

Navigeer naar de beheerconsole van uw SAML-provider waar uw bedrijfstoepassingen worden vermeld.

Selecteer de juiste SAML-toepassing:

Identificeer en selecteer de SAML-toepassingen die overeenkomen met de groepen in de Cisco Secure-clienttunnel die u wilt configureren.

Configureer de identificator (entiteit-ID):

Stel de identificatiecode (entiteit-ID) voor elke toepassing in. Dit moet de Base URL zijn, die uw Cisco Secure Client Full Qualified Domain Name (FQDN) is.

Stel de antwoord-URL (Assertion Consumer Service URL) in:

Configureer de antwoord-URL (Assertion Consumer Service URL) met de juiste basis-URL. Zorg ervoor dat deze is afgestemd op de Cisco Secure Client FQDN.

Voeg het verbindingsprofiel of de naam van de tunnelgroep toe aan de basis-URL om de specificiteit te garanderen.

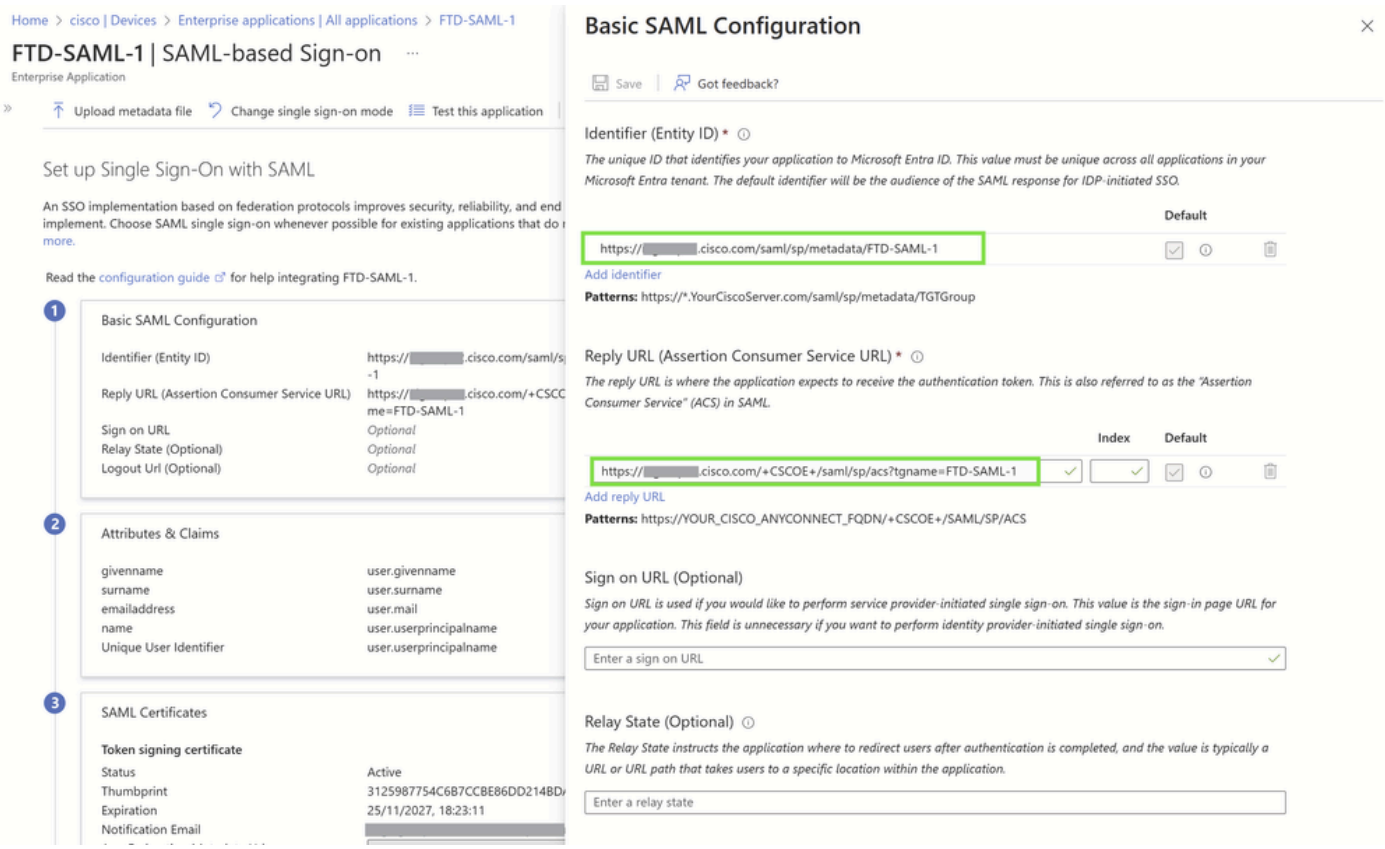
De configuratie verifiëren:

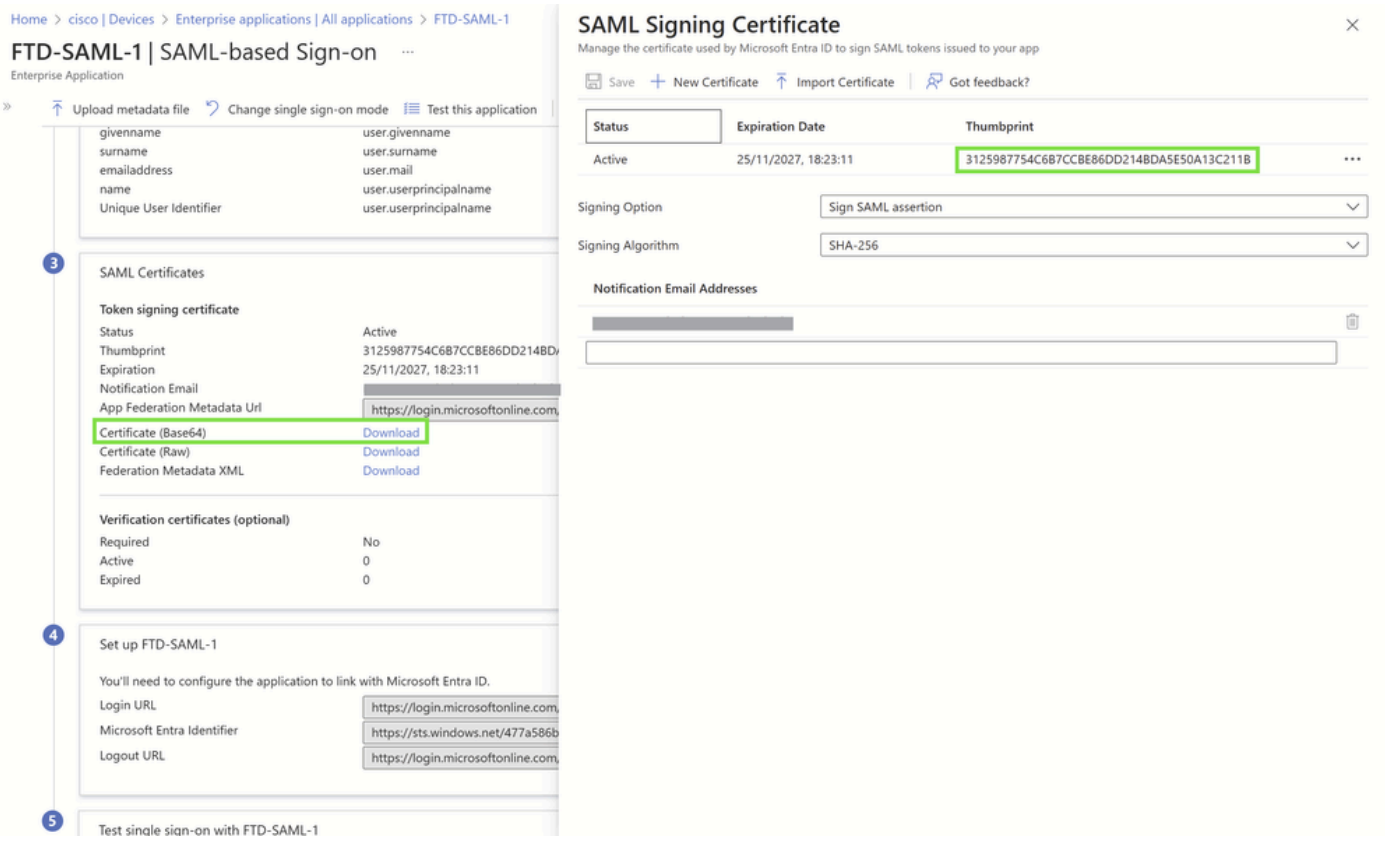
Dubbelcontroleer of alle URL's en parameters correct zijn ingevoerd en overeenkomen met de respectieve tunnelgroepen.

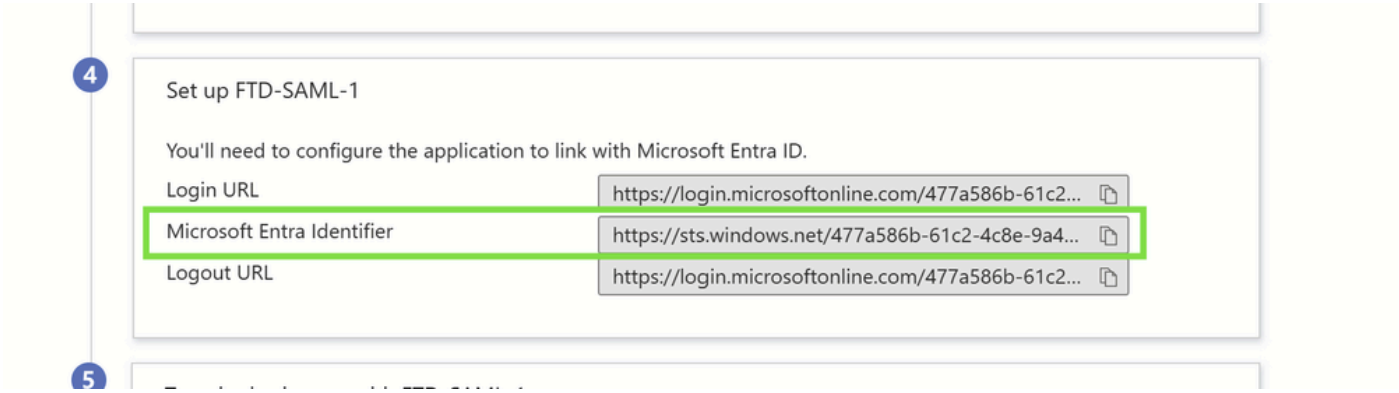
Wijzigingen opslaan en, indien mogelijk, een testverificatie uitvoeren om er zeker van te zijn dat de configuratie werkt zoals verwacht.

Raadpleeg voor meer informatie de "Add Cisco Secure Client from the Microsoft App Gallery" in de Cisco-documentatie: ASA Secure Client VPN configureren met Microsoft Azure MFA via SAML

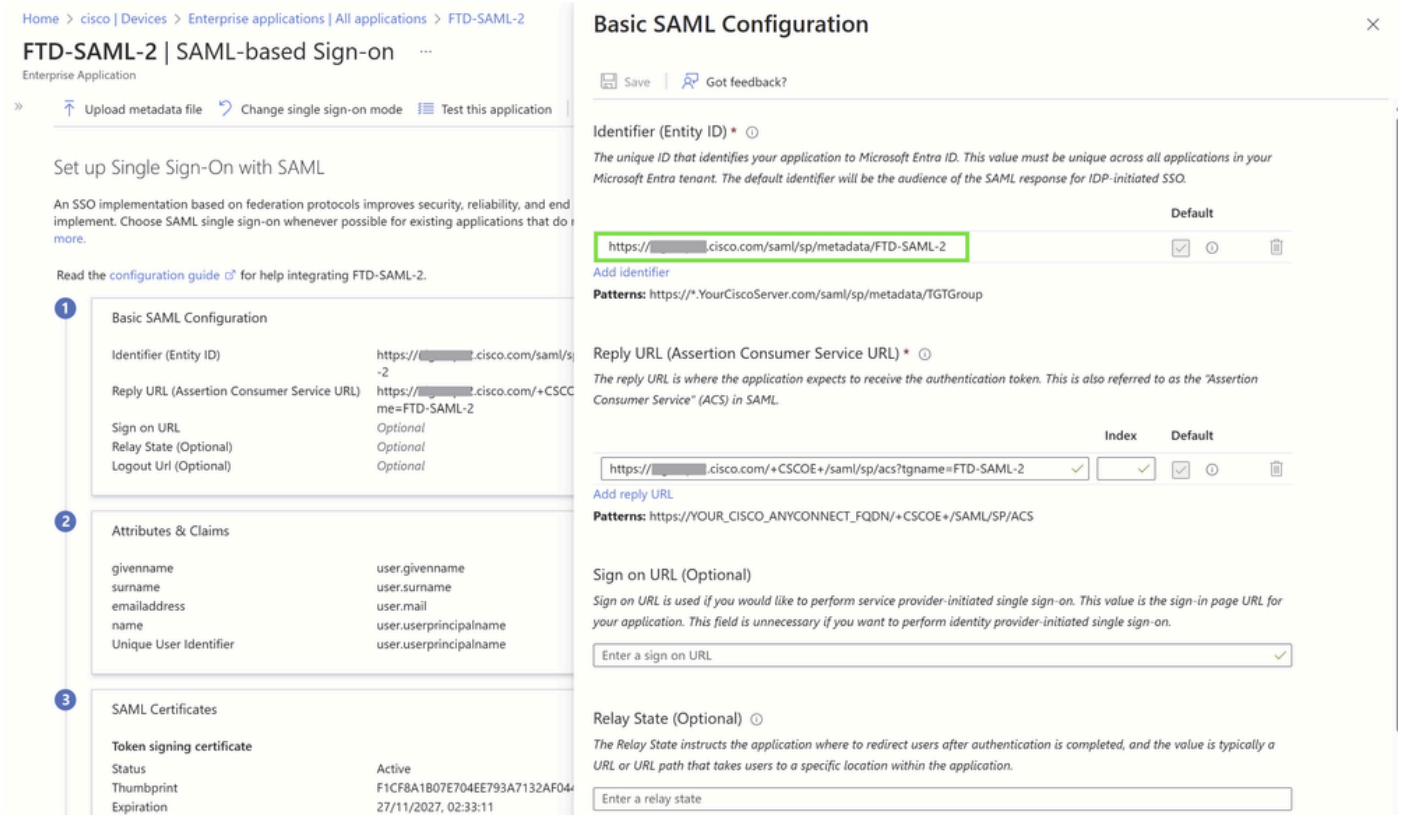
FTD-SAML-1

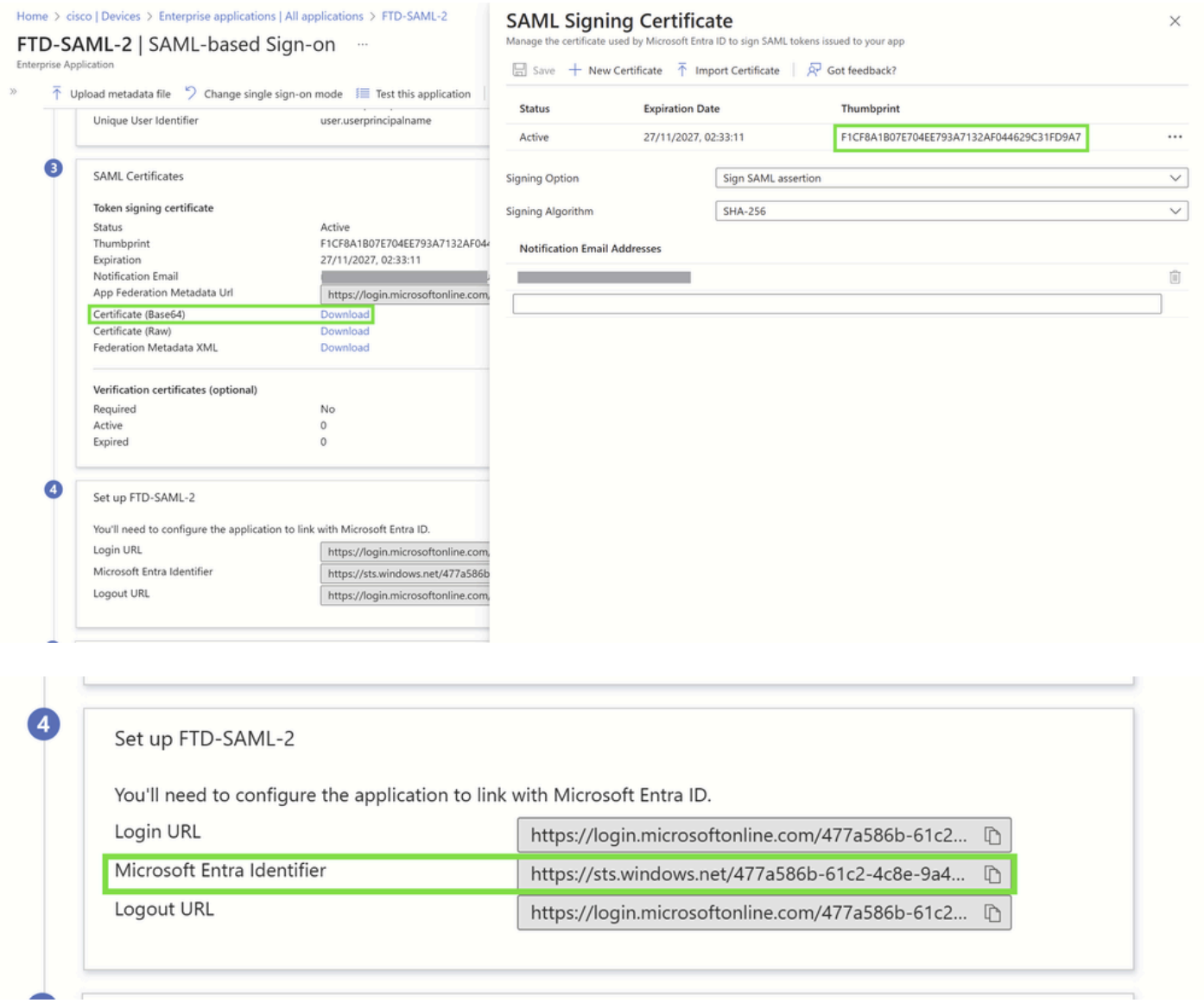

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, 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



Zorg er nu voor dat u over de benodigde informatie en bestanden beschikt om SAML-verificatie te configureren met Microsoft Entra als uw identiteitsprovider:

Zoek de Microsoft Entra Identifier:

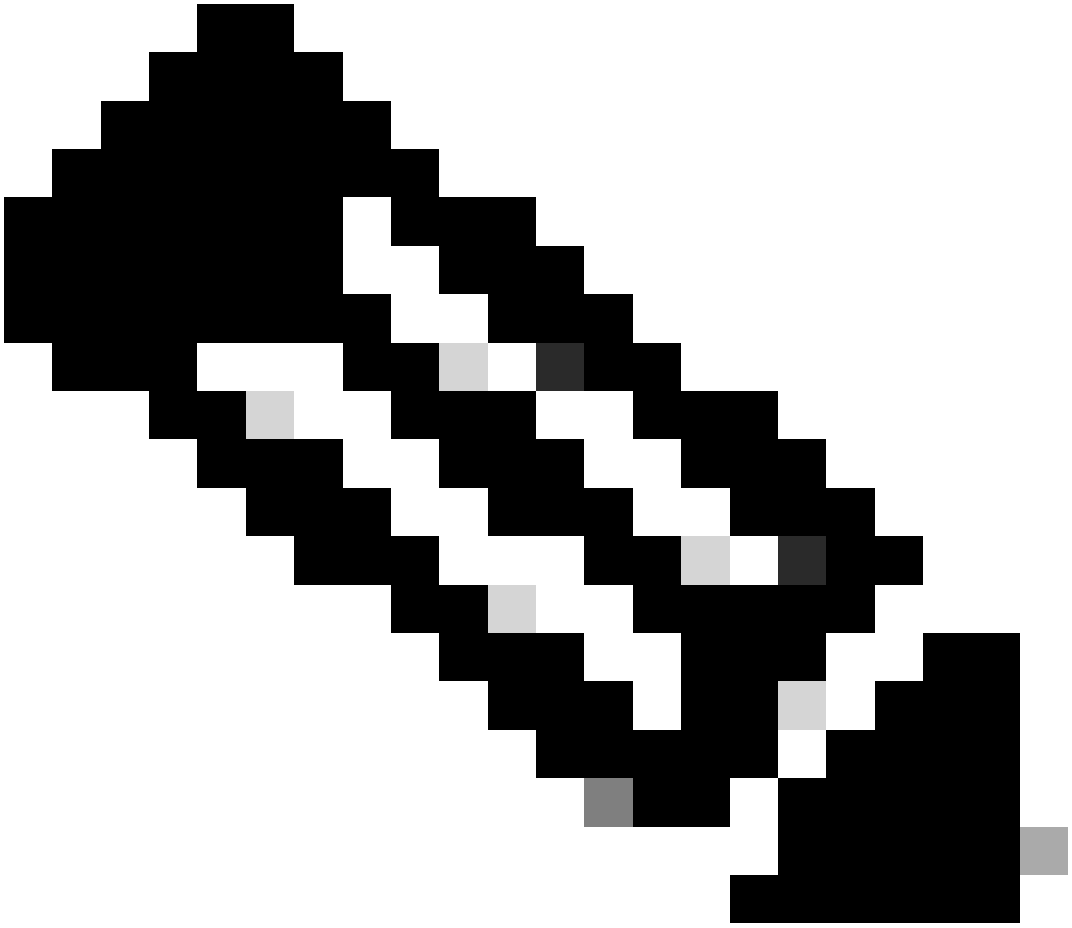
Toegang tot de instellingen voor beide SAML-bedrijfstoepassingen binnen uw Microsoft Entra-portal.

Let op de Microsoft Entra Identifier, die consistent blijft voor beide toepassingen en van cruciaal belang is voor uw SAML-configuratie.

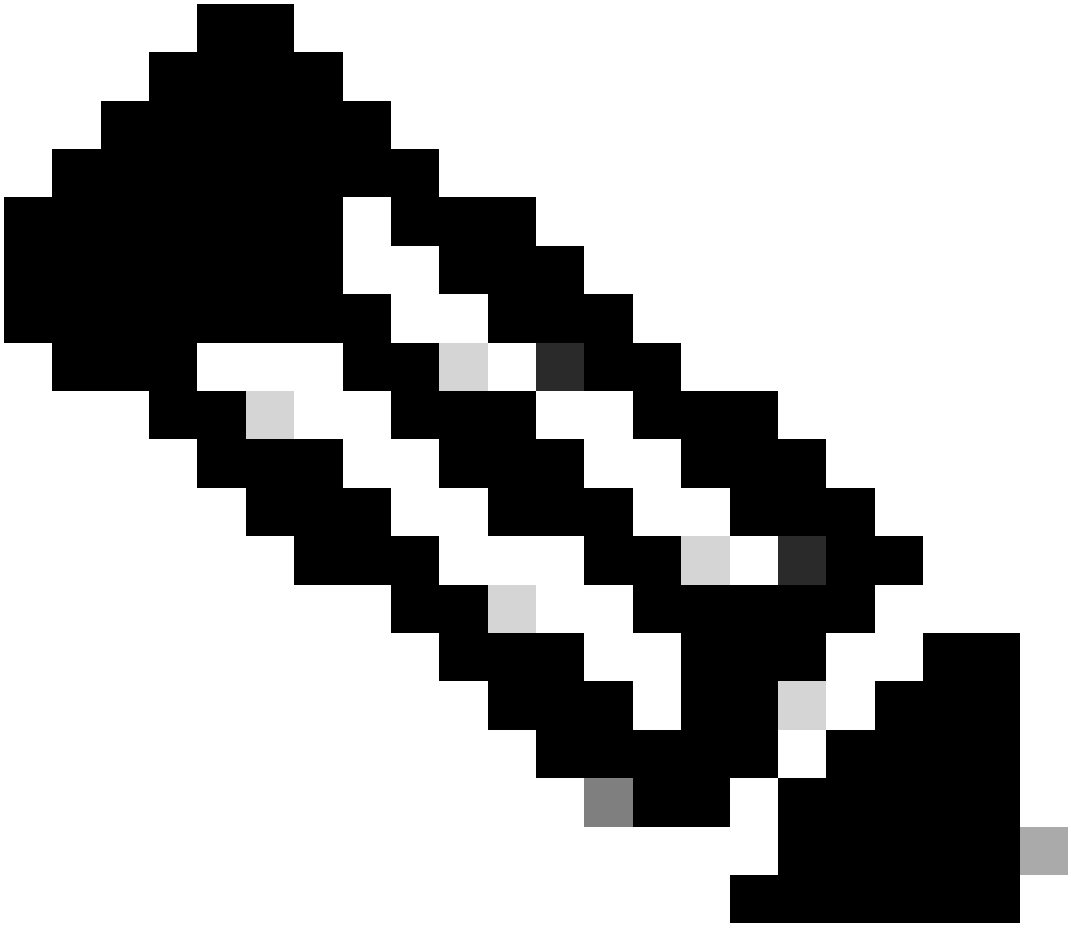
Base64 IDp-certificaten downloaden:

Navigeer naar elke geconfigureerde SAML-ondernemingstoepassing.

Download de respectievelijke Base64-encoded IDP-certificaten. Deze certificaten zijn essentieel voor het instellen van vertrouwen tussen uw identiteitsprovider en uw Cisco VPN-installatie.



Opmerking: Al deze SAML-configuraties die vereist zijn voor de FTD-verbindingsprofielen kunnen ook worden afgeleid van de metadata.xml-bestanden die door uw IDp worden geleverd voor de betreffende toepassingen.



Opmerking: Om een aangepast IDp-certificaat te gebruiken, moet u het op maat gemaakte IDp-certificaat uploaden naar zowel de IDp als de FMC. Zorg er voor dat het certificaat in PKCS#12-formaat is voor Azure IDP. Upload in het VCC alleen het identiteitsbewijs van de IDp en niet het PKCS#12-bestand. Raadpleeg voor gedetailleerde instructies de sectie "Upload the PKCS#12 File on Azure en FDM" in de Cisco-documentatie: Meervoudige RAVPN-profielen configureren met SAML-verificatie op FDM

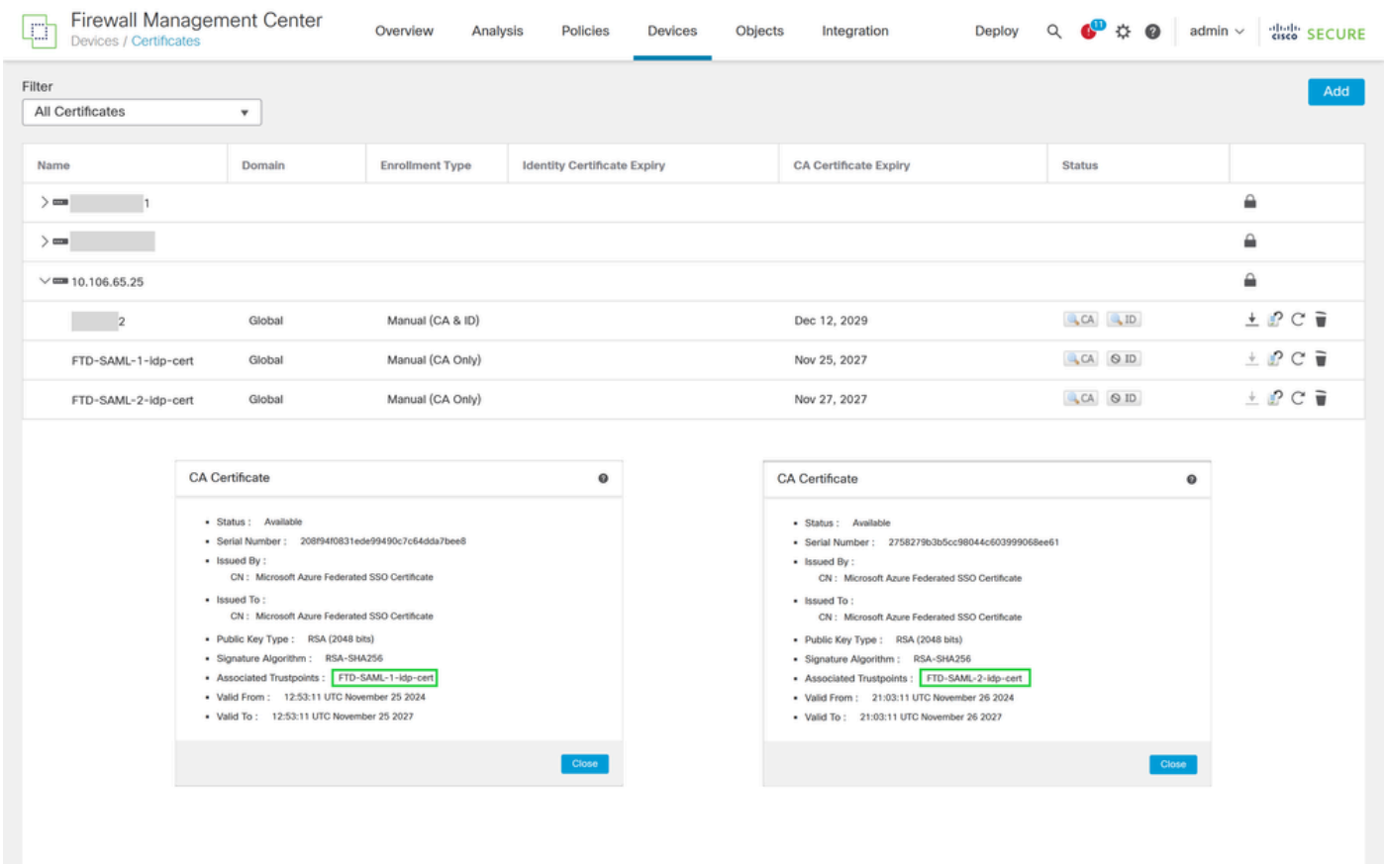
Configuratie op het FTD via het VCC

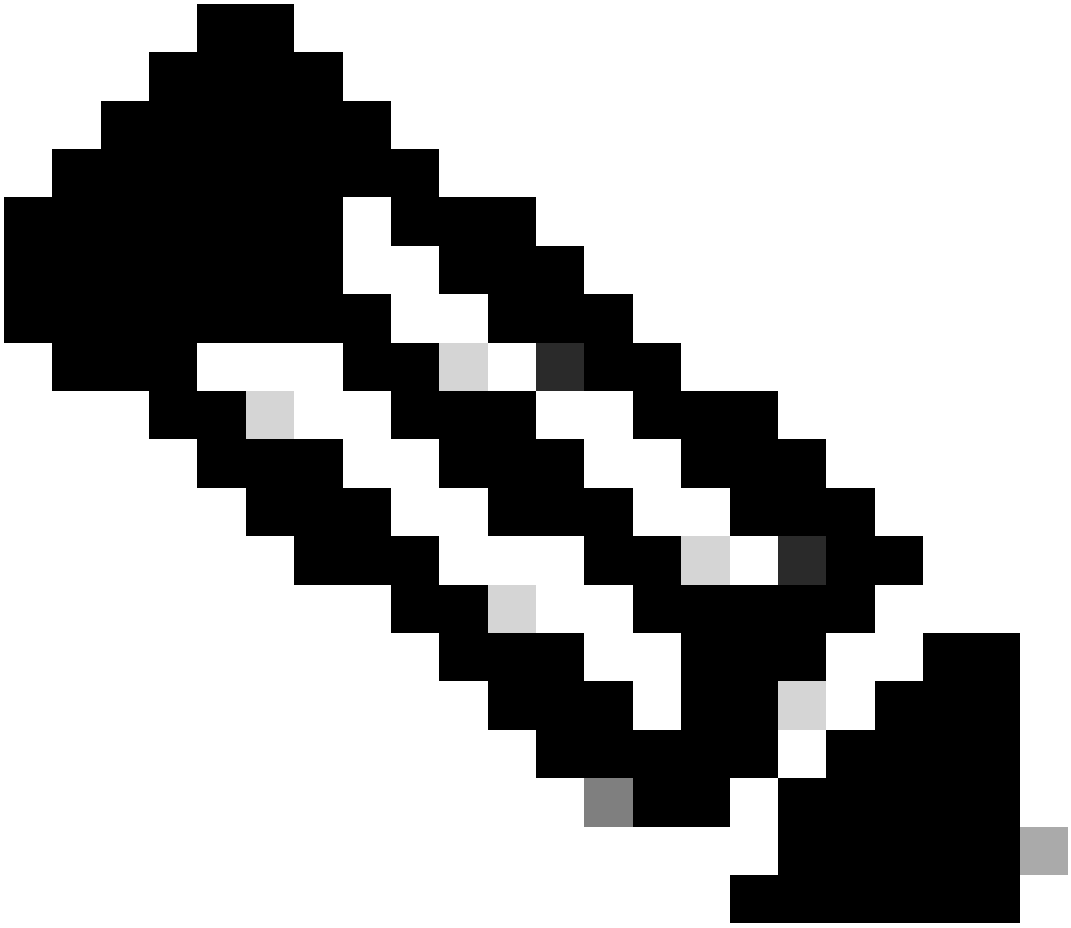
IDp-certificaten inschrijven:

Navigeer naar de sectie Certificaatbeheer binnen het VCC en schrijf de gedownloade Base64-encoded IDP-certificaten in voor beide SAML-toepassingen. Deze certificaten zijn essentieel voor het vestigen van vertrouwen en het toelaten van de authentificatie van SAML.

Raadpleeg voor uitgebreide informatie de eerste twee stappen onder "Configuration on the FTD via FMC" in de Cisco-documentatie die beschikbaar is op: Configureer beveiligde client met

[SAML-verificatie op FTD die via FMC wordt beheerd](#).





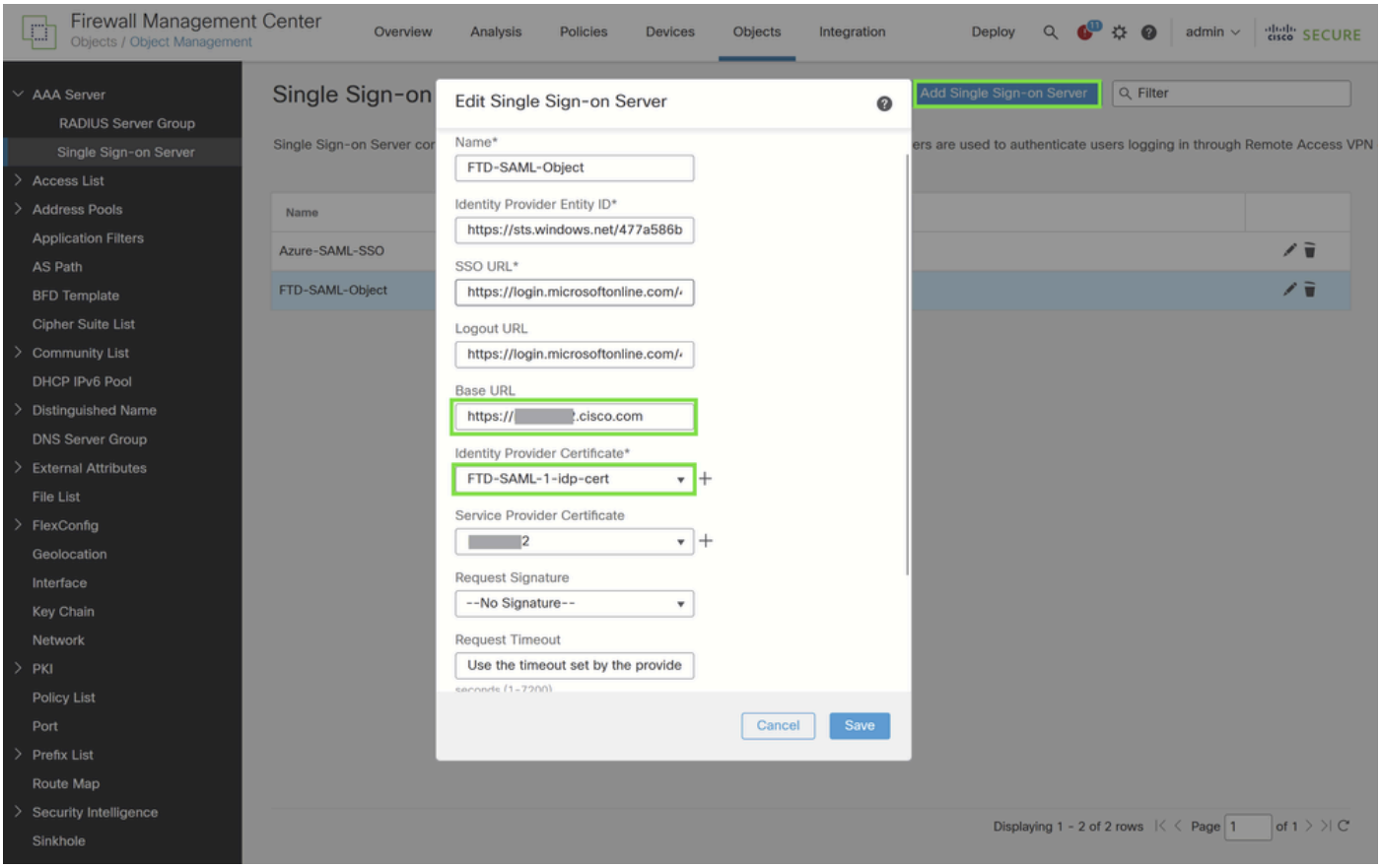
Opmerking: Het beeld is bewerkt om beide certificaten tegelijk weer te geven voor een betere weergave. Het is niet mogelijk beide certificaten tegelijkertijd op het VCC te openen.

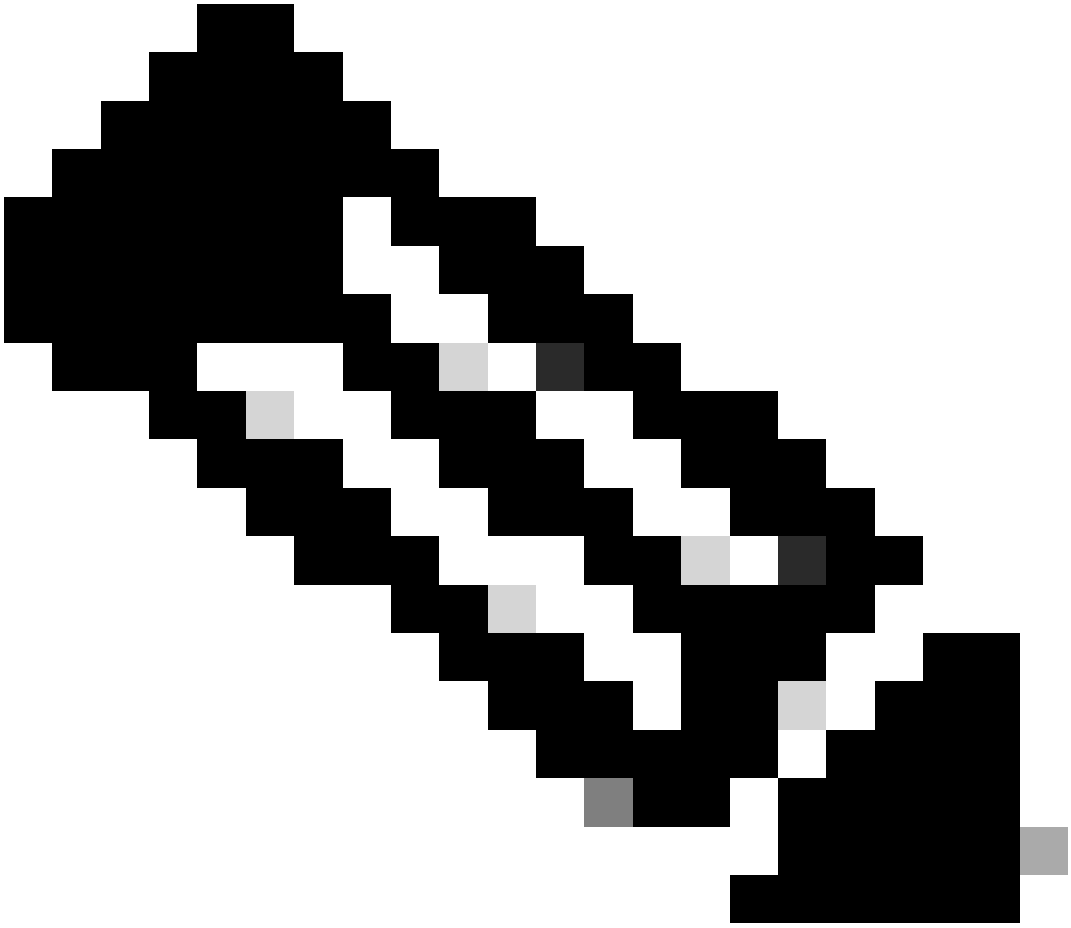
SAML Server-instellingen configureren op Cisco FTD via FMC

Voer de volgende stappen uit om de SAML-serverinstellingen op uw Cisco Firepower Threat Defence (FTD) te configureren met behulp van het Firepower Management Center (FMC):

1. Navigeren naar configuratie van één aanmelding bij server:
    - Navigeer naar Objecten > Objectbeheer > AAA-servers > Single Sign-on Server.
    - Klik op Add Single Sign-on Server om te beginnen met het configureren van een nieuwe server.
2. Instellingen SAML-server configureren:
    - Met behulp van de parameters die zijn verzameld uit uw SAML enterprise applicaties of uit het metadata.xml bestand dat is gedownload van uw Identity Provider (IDP), vult u de benodigde SAML-waarden in het formulier New Single Sign-on Server in.

- De volgende belangrijke parameters moeten worden geconfigureerd:
  - Entiteit-ID van SAML Provider: entityID van metadata.xml
  - URL VOOR DERGELIJKE OPTIE: SingleSignOnService van metadata.xml.
  - Uitloggen URL: SingleLogoutService van metadata.xml.
  - BASIS-URL: FQDN van uw FTD SSL ID-certificaat.
  - Certificaat van identiteitsverstrekker: IDp-ondertekeningscertificaat.
    - Voeg onder het gedeelte Identity Provider Certificate een van de ingeschreven IDP-certificaten bij
    - Voor dit gebruiksgeval gebruiken we het IDP-certificaat van de FTD-SAML-1 applicatie.
  - Certificaat voor serviceproviders: FTD Signing Certificate.



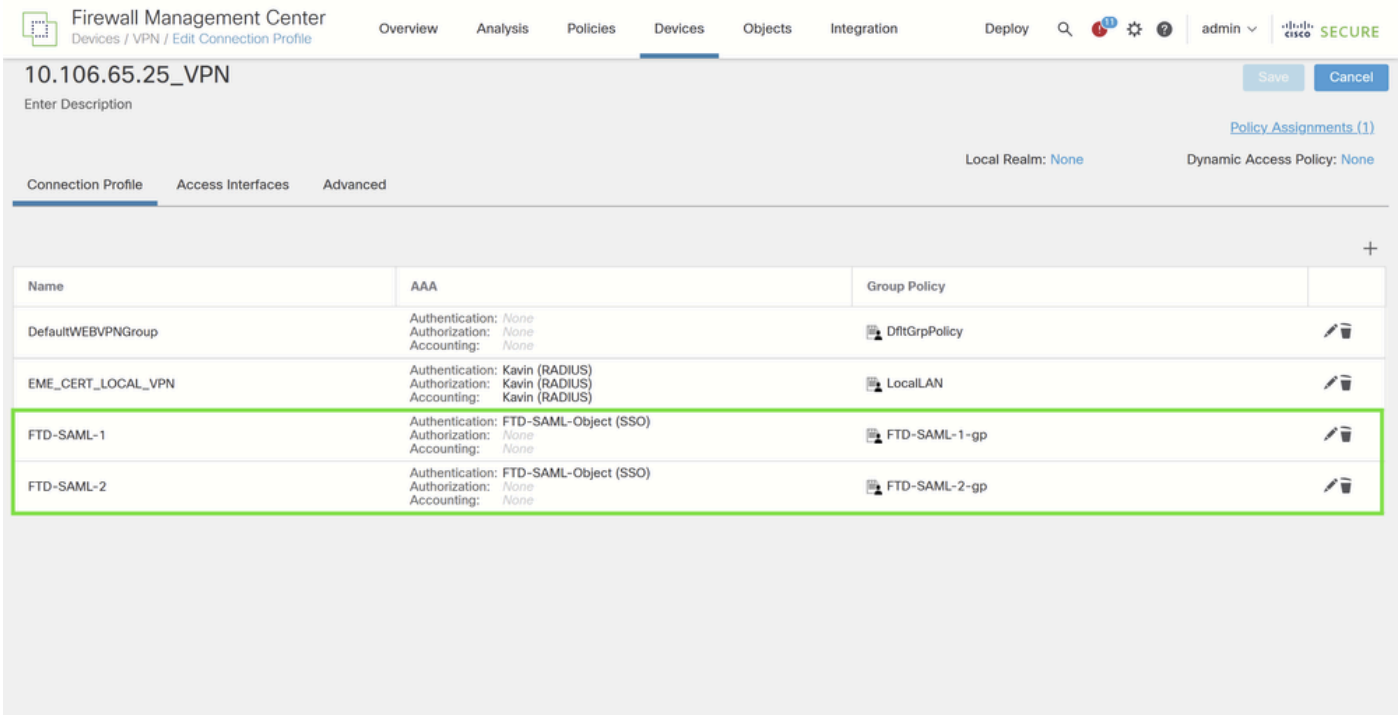


Opmerking: In de huidige configuratie kan alleen het Identity Provider-certificaat worden overschreven van het SAML-object binnen de instellingen van het verbindingsprofiel. Helaas kunnen functies zoals "Aanvraag-IDp opnieuw-verificatie bij aanmelding" en "Alleen toegankelijke IDp inschakelen op intern netwerk" niet afzonderlijk worden ingeschakeld of uitgeschakeld voor elk verbindingsprofiel.

Verbindingsprofielen configureren op Cisco FTD via FMC

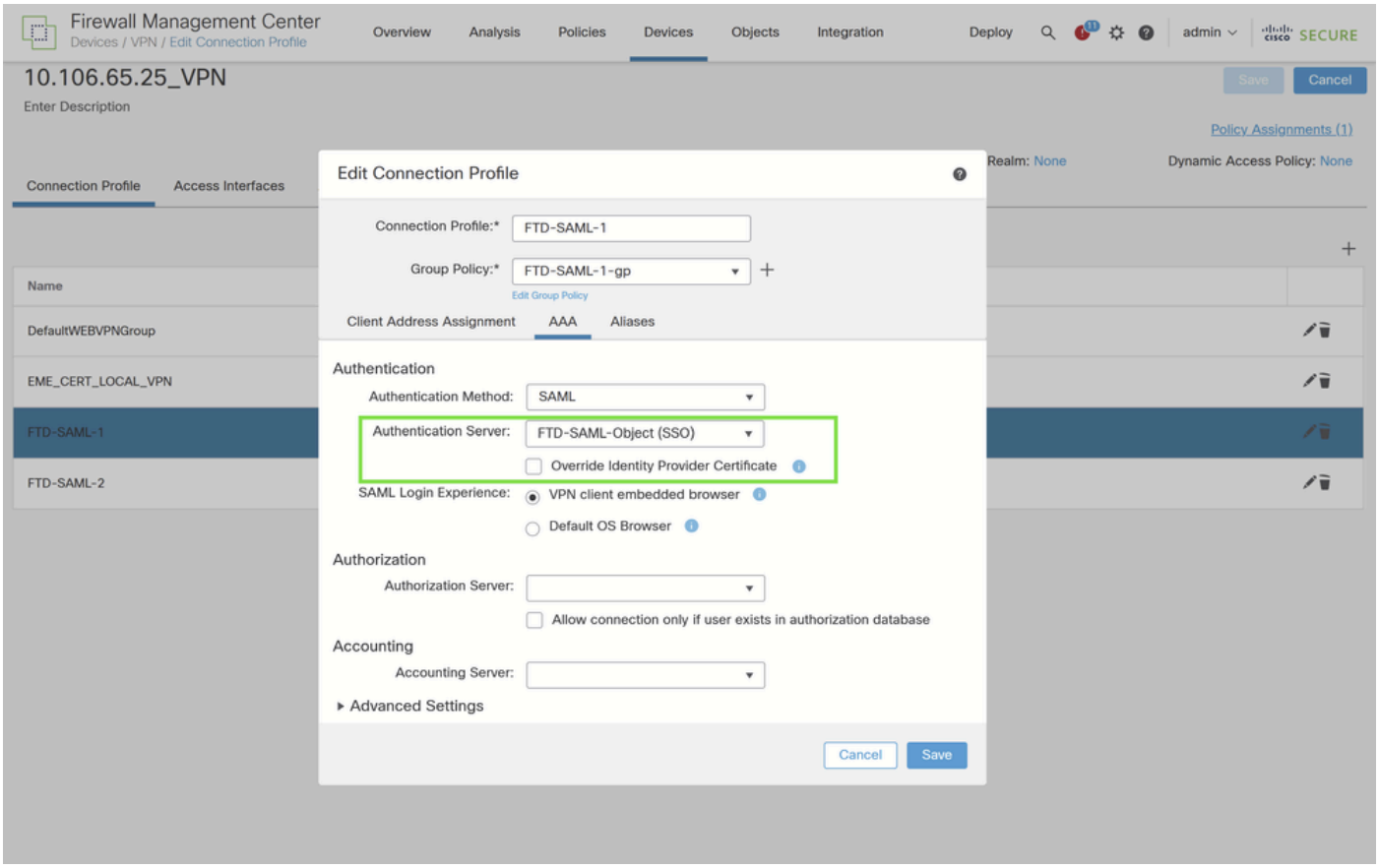
Om de instelling van de SAML-verificatie te voltooien, moet u de verbindingsprofielen met de juiste parameters configureren en de AAA-verificatie op SAML instellen met behulp van de eerder geconfigureerde SAML-server.

Raadpleeg voor meer informatie de vijfde stap onder "Configuration on the FTD via FMC" in de Cisco-documentatie: Configureer beveiligde client met SAML-verificatie op FTD die via FMC wordt beheerd.



Uittreksel van AAA-configuratie voor eerste verbindingsprofiel

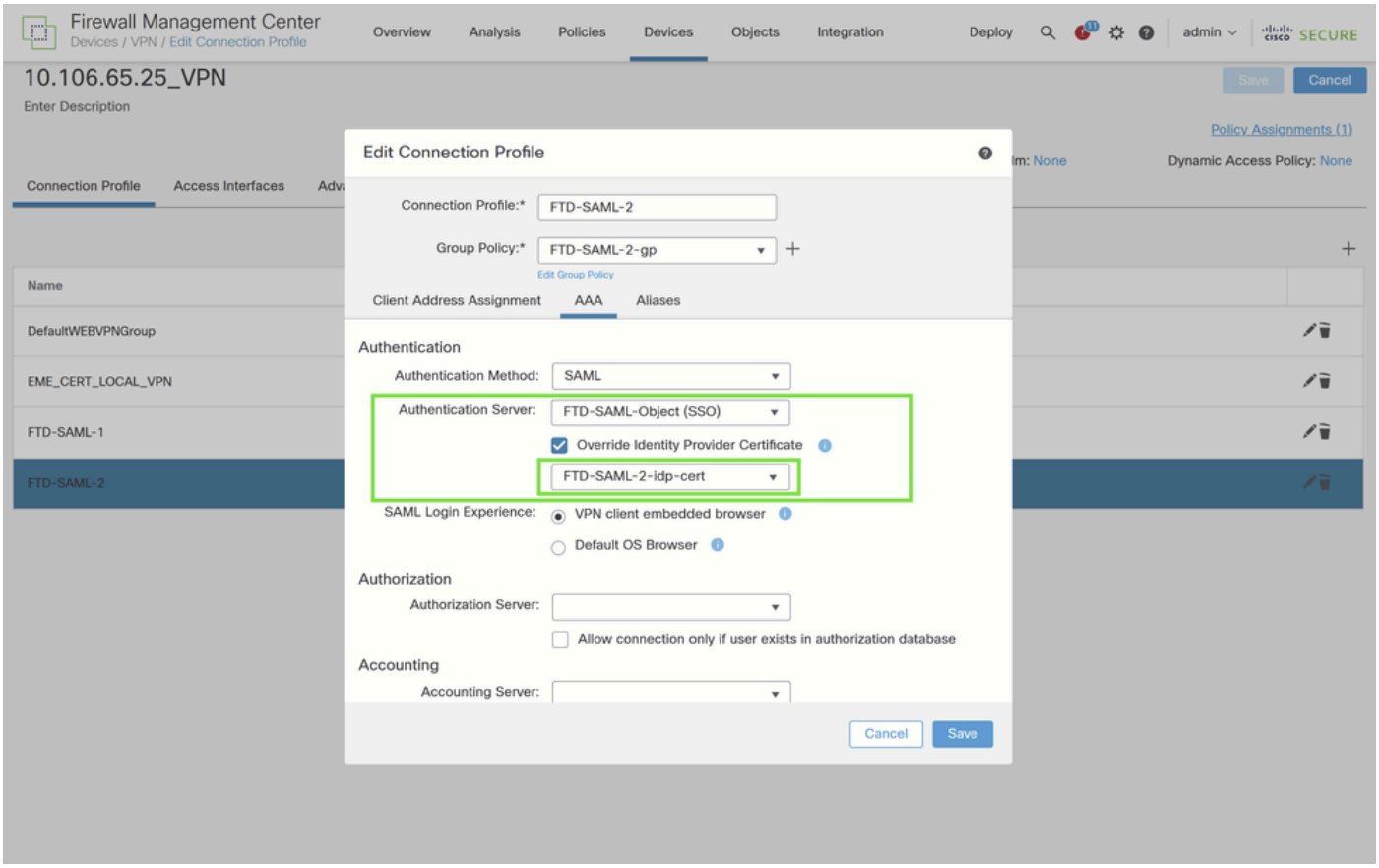
Hier volgt een overzicht van de AAA-configuratie-instellingen voor het eerste verbindingsprofiel:



Het configureren van het IDp-certificaat negeren voor het tweede verbindingsprofiel op Cisco FTD
Om er zeker van te zijn dat het juiste Identity Provider-certificaat (IDP) wordt gebruikt voor het tweede verbindingsprofiel, schakelt u de override van het IDP-certificaat in door de volgende stappen uit te voeren:

Zoek en schakel binnen de instellingen van het verbindingsprofiel de optie "Override Identity Provider Certificate" in om het gebruik van een ander IDP-certificaat toe te staan dan het certificaat dat is geconfigureerd voor de SAML-server.

Selecteer in de lijst met ingeschreven IDp-certificaten het certificaat dat specifiek is ingeschreven voor de FTD-SAML-2-toepassing. Deze selectie zorgt ervoor dat wanneer een verificatieaanvraag voor dit verbindingsprofiel wordt ingediend, het juiste IDp-certificaat wordt gebruikt.



Implementatie van configuratie

Navigeer**Deploy** > **Deployment**naar en selecteer de juiste FTD om de wijzigingen in SAML Verification VPN toe te passen.

Verifiëren

Configuratie op de FTD-opdrachtregel

<#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/
```

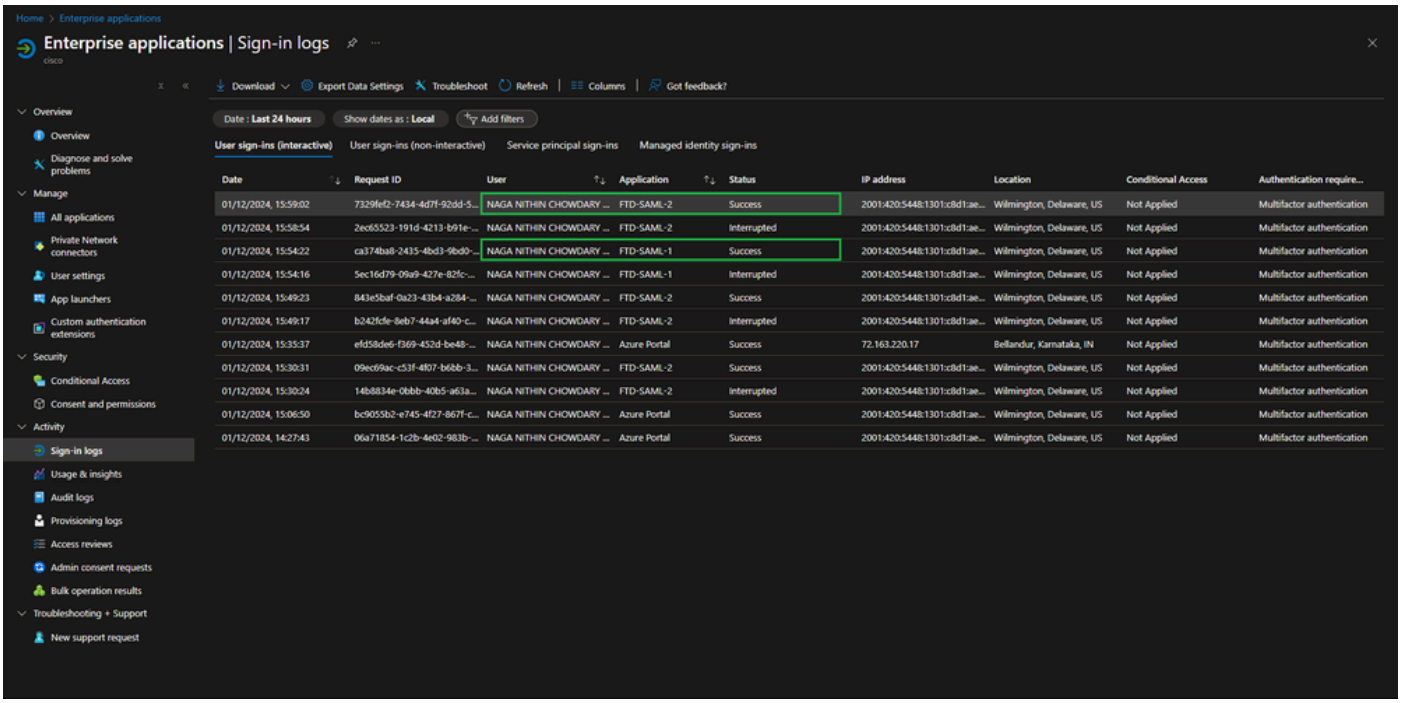
```
firepower#
```

<#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#
```

Inloggen vanaf Azure Boven-ID

Open de sectie Aanmeldingslogboeken onder Enterprise Application. Zoek naar verificatieverzoeken met betrekking tot specifieke verbindingsprofielen, zoals FTD-SAML-1 en FTD-SAML-2. Controleer of de gebruikers met succes verificatie uitvoeren via de SAML-toepassingen die aan elk verbindingsprofiel zijn gekoppeld.



Inloggen op Azure IDP

Problemen oplossen

1. U kunt problemen oplossen met DART vanaf de Secure Client-gebruiker-pc.
2. Om een probleem met SAML-verificatie op te lossen, gebruikt u deze debug:

```
<#root>

firepower#

 debug webvpn saml 255
```

3. Controleer de configuratie van de beveiligde client zoals hierboven uiteengezet; Deze opdracht kan worden gebruikt om het certificaat te controleren.

```
<#root>

firepower#

 show crypto ca certificate
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.