Configurer l'authentification SAML pour plusieurs profils de connexion RAVPN sur FTD

Table des matières

Introduction

Ce document décrit l'authentification SAML avec le fournisseur d'identité Azure pour plusieurs profils de connexion sur Cisco FTD géré par FMC.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Configuration sécurisée du client sur le pare-feu de nouvelle génération (NGFW) géré par Firepower Management Center (FMC)
- Valeurs SAML et metatada.xml

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Threat Defense (FTD) version 7.4.0
- FMC version 7.4.0
- Azure Microsoft Entra ID avec SAML 2.0

- Cisco Secure Client 5.1.7.80

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cette configuration permet à FTD d'authentifier les utilisateurs clients sécurisés à l'aide de deux applications SAML différentes sur Azure IDP avec un seul objet SAML configuré sur 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://

Dans un environnement Microsoft Azure, plusieurs applications peuvent partager le même ID d'entité. Chaque application, généralement mappée à un groupe de tunnels différent, nécessite un certificat unique, nécessitant la configuration de plusieurs certificats dans la configuration IdP du côté FTD sous un seul objet IdP SAML. Cependant, Cisco FTD ne prend pas en charge la configuration de plusieurs certificats sous un seul objet IDP SAML, comme détaillé dans l'ID de bogue Cisco CSCvi29084.

Pour surmonter cette limitation, Cisco a introduit la fonctionnalité de remplacement de certificat IdP, disponible à partir des versions FTD 7.1.0 et ASA 9.17.1. Cette amélioration offre une solution permanente au problème et complète les solutions de contournement existantes décrites dans le rapport de bogue.

Configurations

Cette section décrit le processus de configuration de l'authentification SAML avec Azure comme fournisseur d'identité (IdP) pour plusieurs profils de connexion sur Cisco Firepower Threat Defense (FTD) géré par Firepower Management Center (FMC). La fonction de remplacement de certificat IdP est utilisée pour configurer cette option de manière efficace.

Présentation de la configuration :

Deux profils de connexion doivent être configurés sur Cisco FTD :

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

Dans cet exemple de configuration, l'URL de la passerelle VPN (FQDN du client sécurisé Cisco) est définie sur nigarapa2.cisco.com

Configurer

Configuration sur Azure IdP

Pour configurer efficacement vos applications d'entreprise SAML pour Cisco Secure Client, assurez-vous que tous les paramètres sont définis correctement pour chaque groupe de tunnels en procédant comme suit :

Accéder aux applications SAML Enterprise :

Accédez à la console d'administration de votre fournisseur SAML où sont répertoriées vos applications d'entreprise.

Sélectionnez l'application SAML appropriée :

Identifiez et sélectionnez les applications SAML correspondant aux groupes de tunnels Cisco Secure Client que vous souhaitez configurer.

Configurez l'identificateur (ID d'entité) :

Définissez l'identificateur (ID d'entité) de chaque application. Il doit s'agir de l'URL de base, qui est votre nom de domaine complet (FQDN) du client sécurisé Cisco.

Définissez l'URL de réponse (Assertion Consumer Service URL) :

Configurez l'URL de réponse (Assertion Consumer Service URL) à l'aide de l'URL de base correcte. Assurez-vous qu'il est conforme au nom de domaine complet du client sécurisé Cisco.

Ajoutez le nom du profil de connexion ou du groupe de tunnels à l'URL de base pour garantir la spécificité.

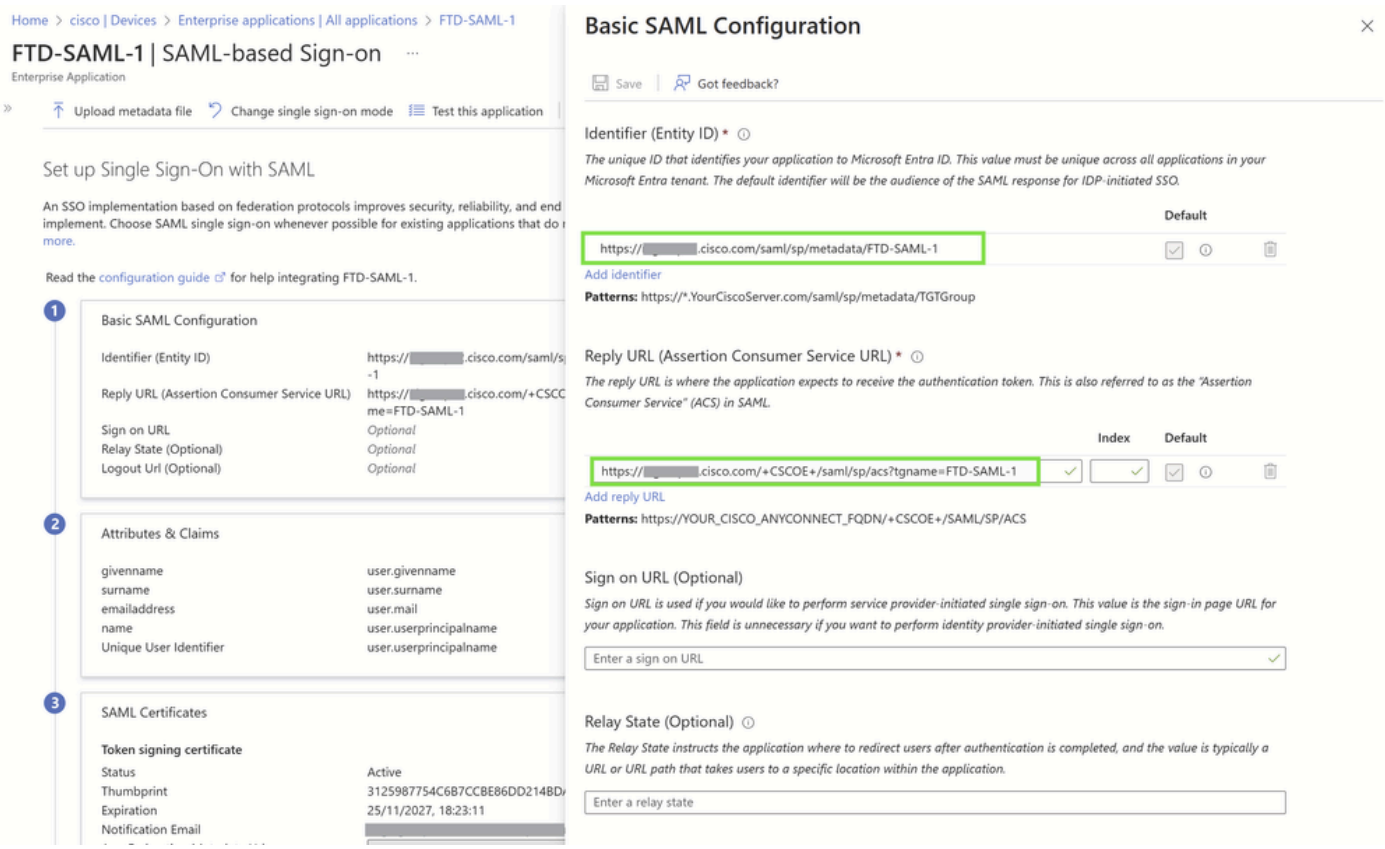
Vérifier la configuration:

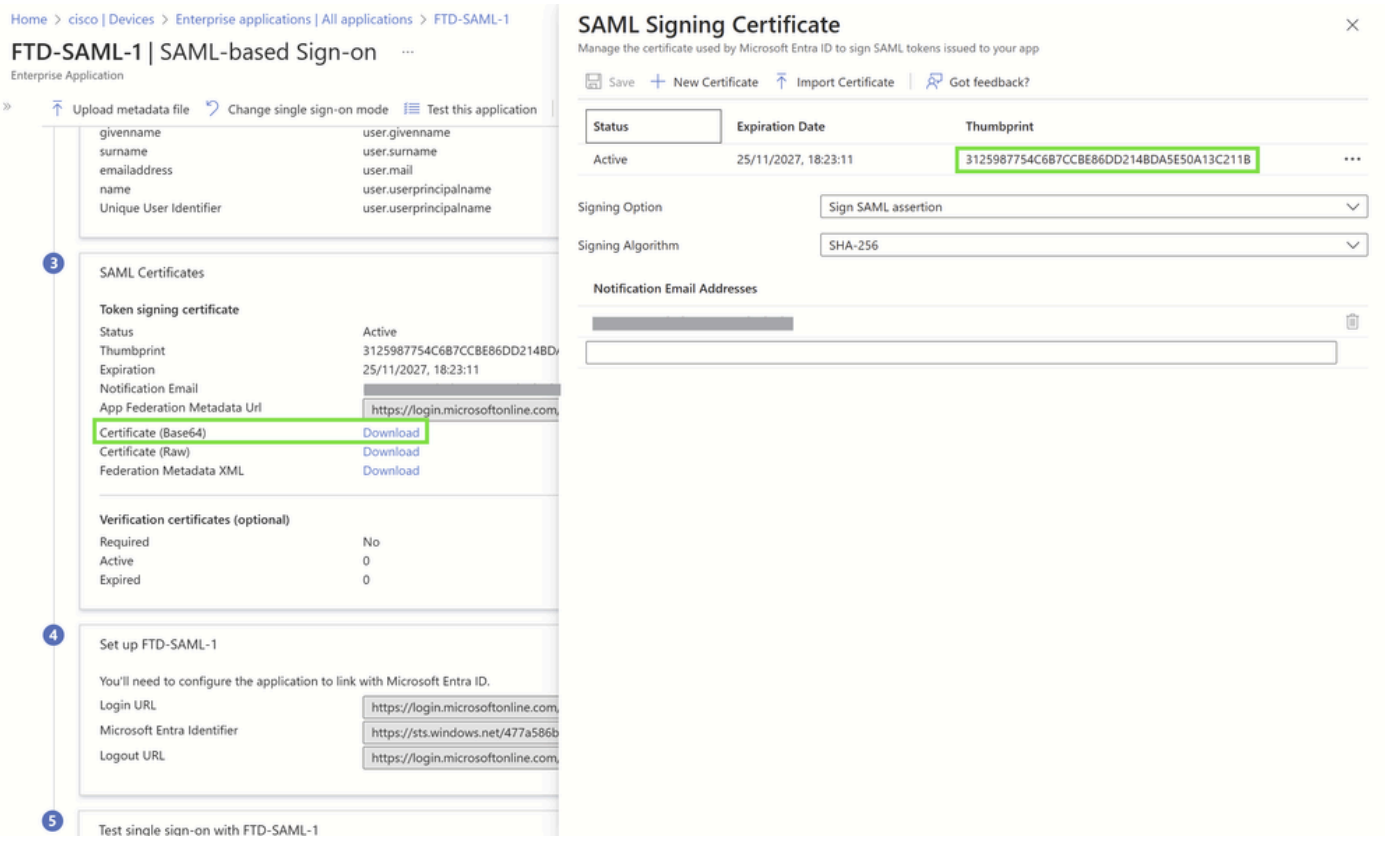
Vérifiez à nouveau que toutes les URL et tous les paramètres sont correctement entrés et correspondent aux groupes de tunnels respectifs.

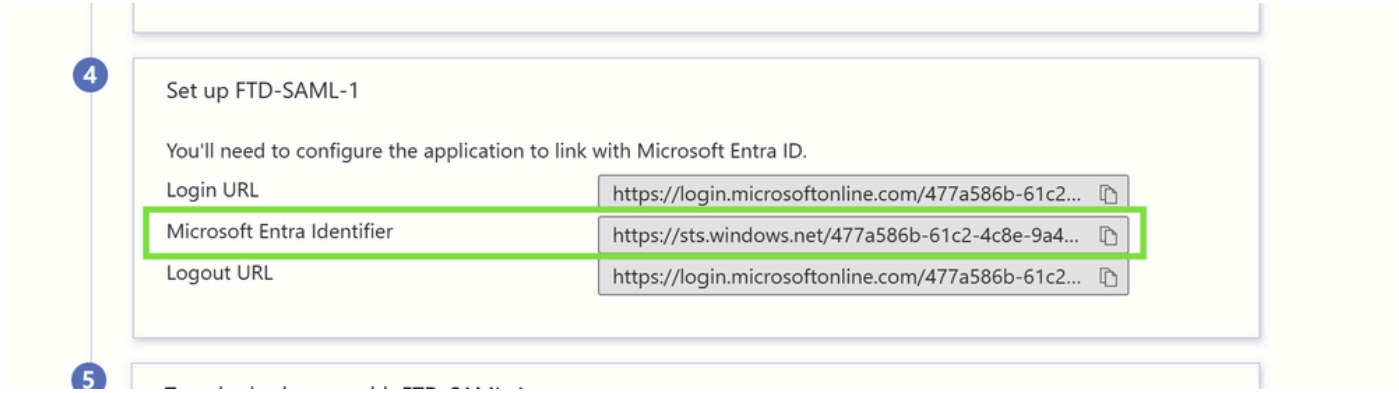
Enregistrez les modifications et, si possible, effectuez un test d'authentification pour vous assurer que la configuration fonctionne comme prévu.

Pour obtenir des conseils plus détaillés, reportez-vous à la section « Add Cisco Secure Client from the Microsoft App Gallery » de la documentation Cisco : Configurer le VPN ASA Secure Client avec Microsoft Azure MFA via SAML

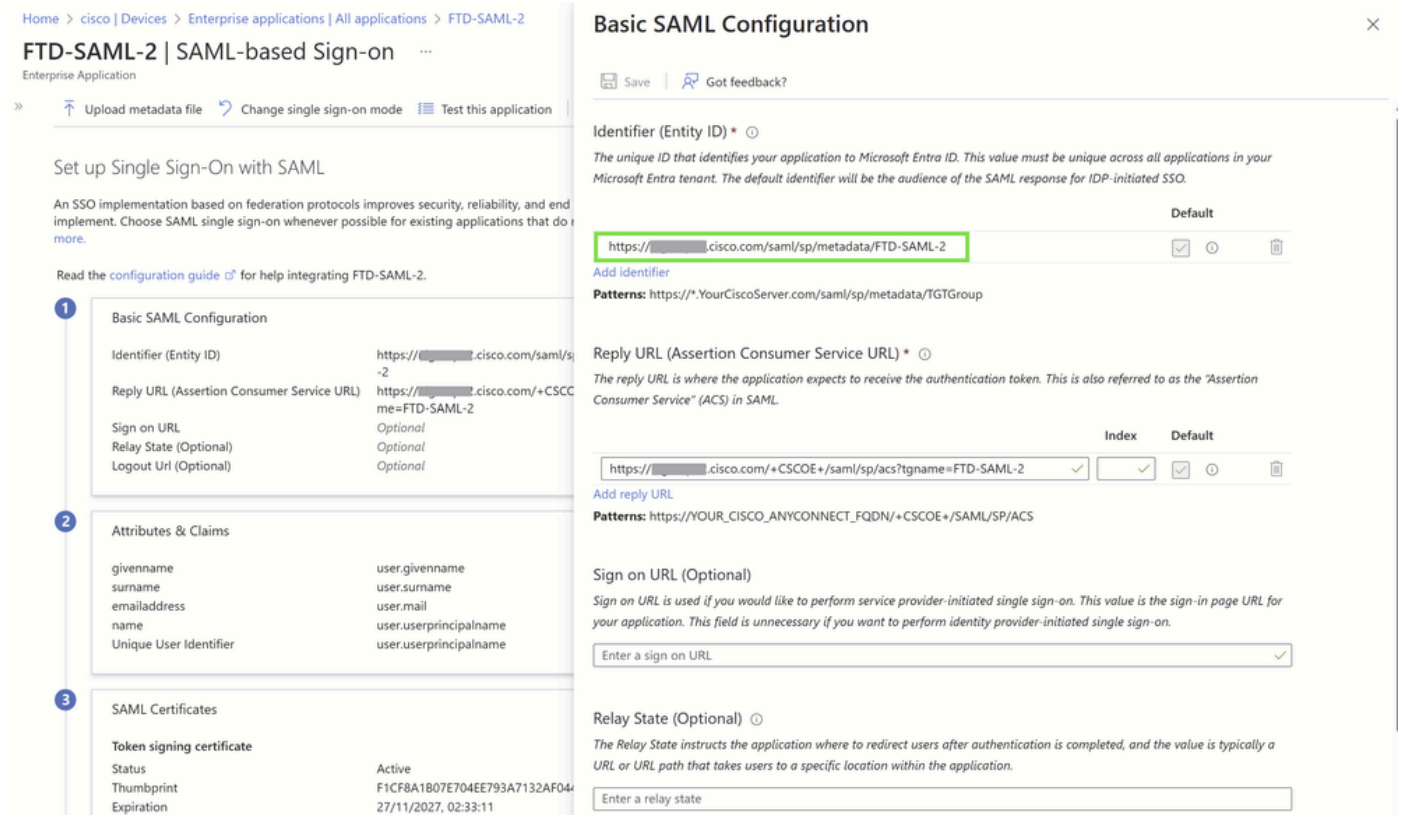
FTD-SAML-1

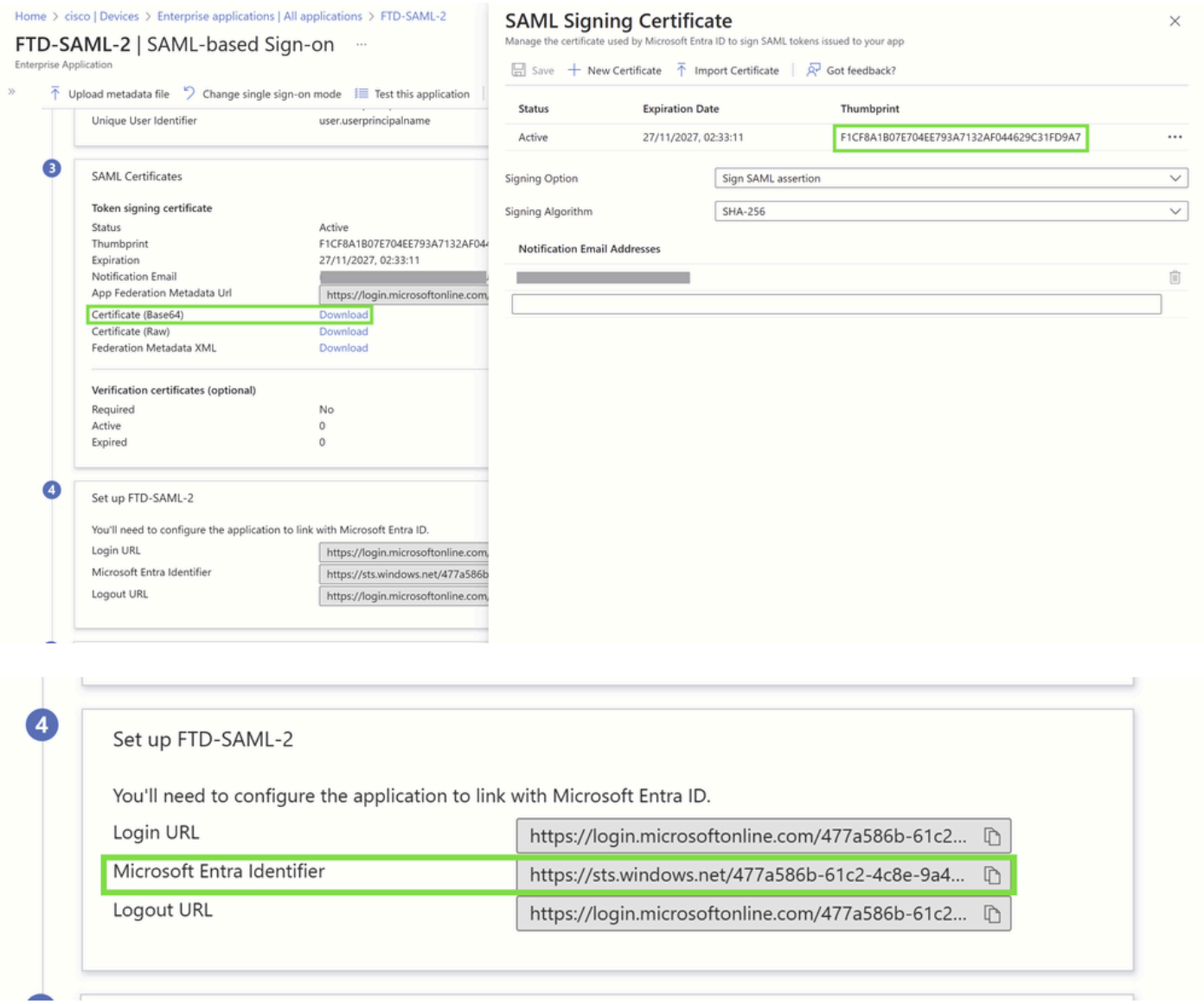

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security,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



Vérifiez que vous disposez des informations et des fichiers nécessaires pour configurer l'authentification SAML avec Microsoft Entra comme fournisseur d'identité :

Localisez l'identificateur Microsoft Entra :

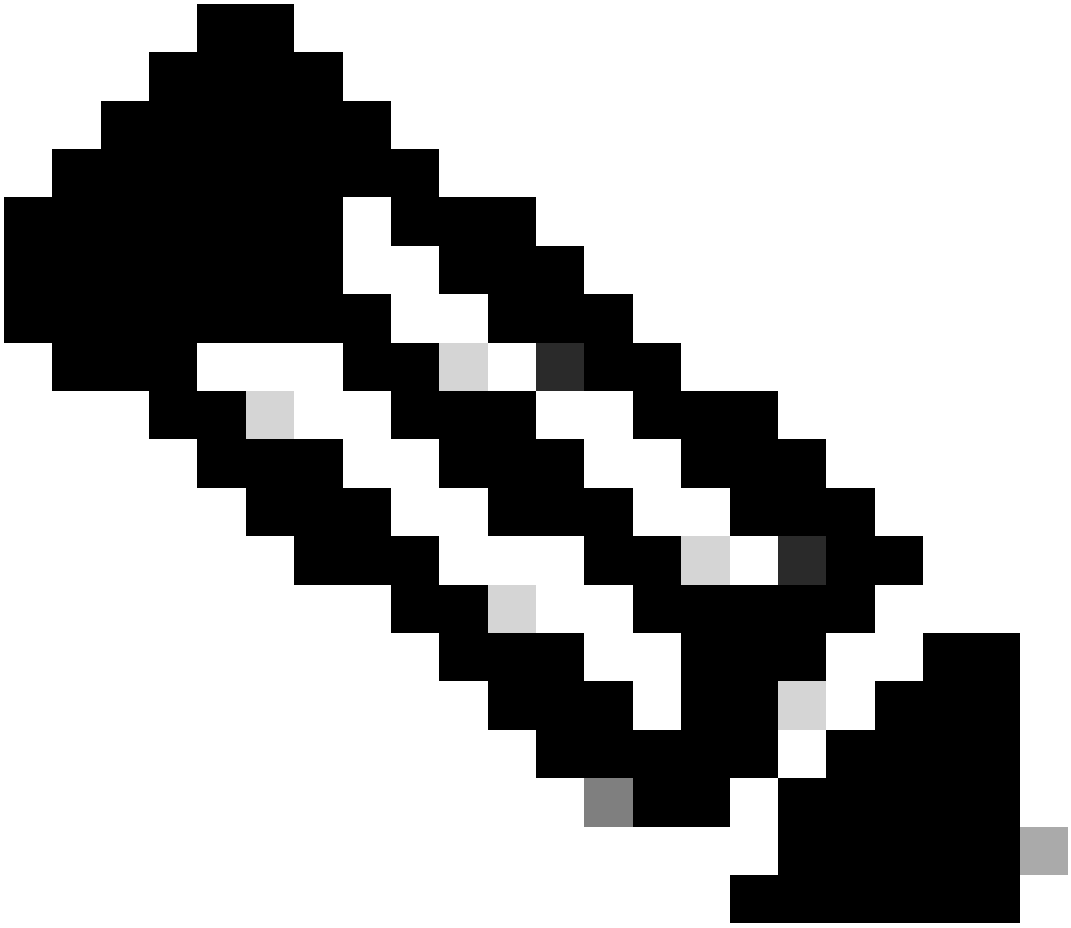
Accédez aux paramètres des deux applications d'entreprise SAML dans votre portail Microsoft Entra.

Notez l'identificateur Microsoft Entra, qui reste cohérent entre les deux applications et est essentiel pour votre configuration SAML.

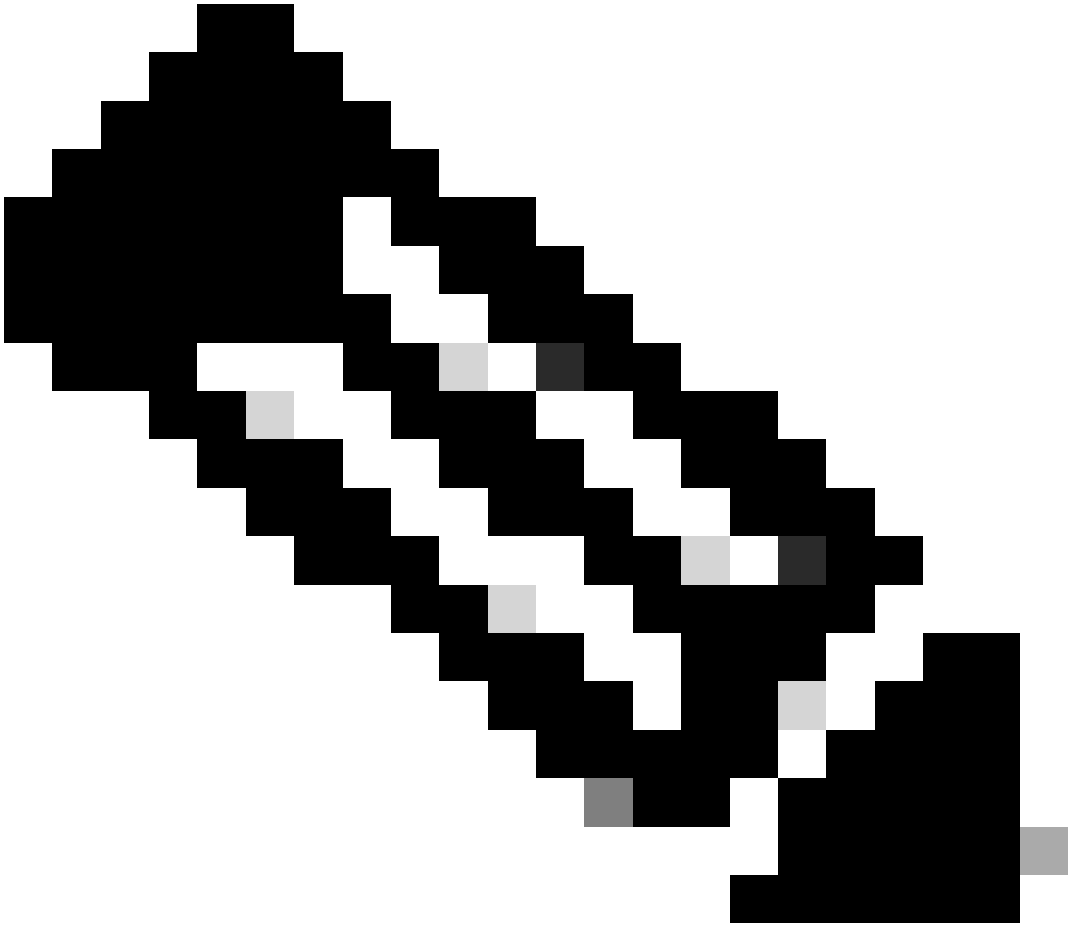
Télécharger les certificats IdP Base64 :

Accédez à chaque application d'entreprise SAML configurée.

Téléchargez les certificats IdP codés en Base64 respectifs. Ces certificats sont essentiels pour établir la confiance entre votre fournisseur d'identité et votre configuration VPN Cisco.



Remarque : Toutes ces configurations SAML requises pour les profils de connexion FTD peuvent également provenir des fichiers metadata.xml fournis par votre fournisseur d'accès pour les applications respectives.



> Remarque : Pour utiliser un certificat de fournisseur d'identité personnalisé, vous devez télécharger le certificat de fournisseur d'identité généré sur le fournisseur d'identité et le FMC. Pour Azure IdP, assurez-vous que le certificat est au format PKCS#12. Sur le FMC, téléchargez uniquement le certificat d'identité à partir du fournisseur d'identité, et non le fichier PKCS#12. Pour obtenir des instructions détaillées, reportez-vous à la section « Upload the PKCS#12 File on Azure and FDM » de la documentation Cisco : Configuration de plusieurs profils RAVPN avec authentification SAML sur FDM

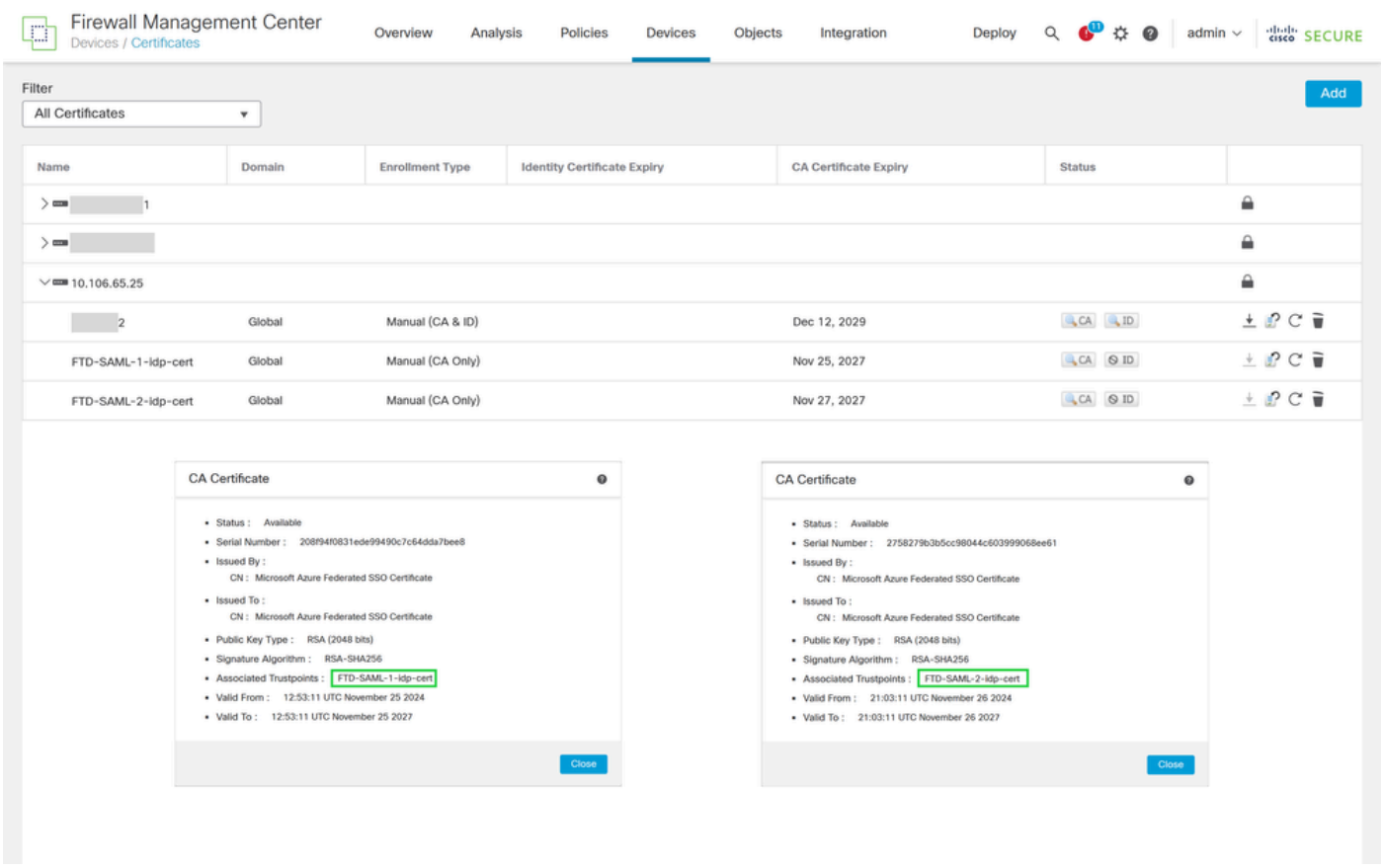
Configuration sur le FTD via FMC

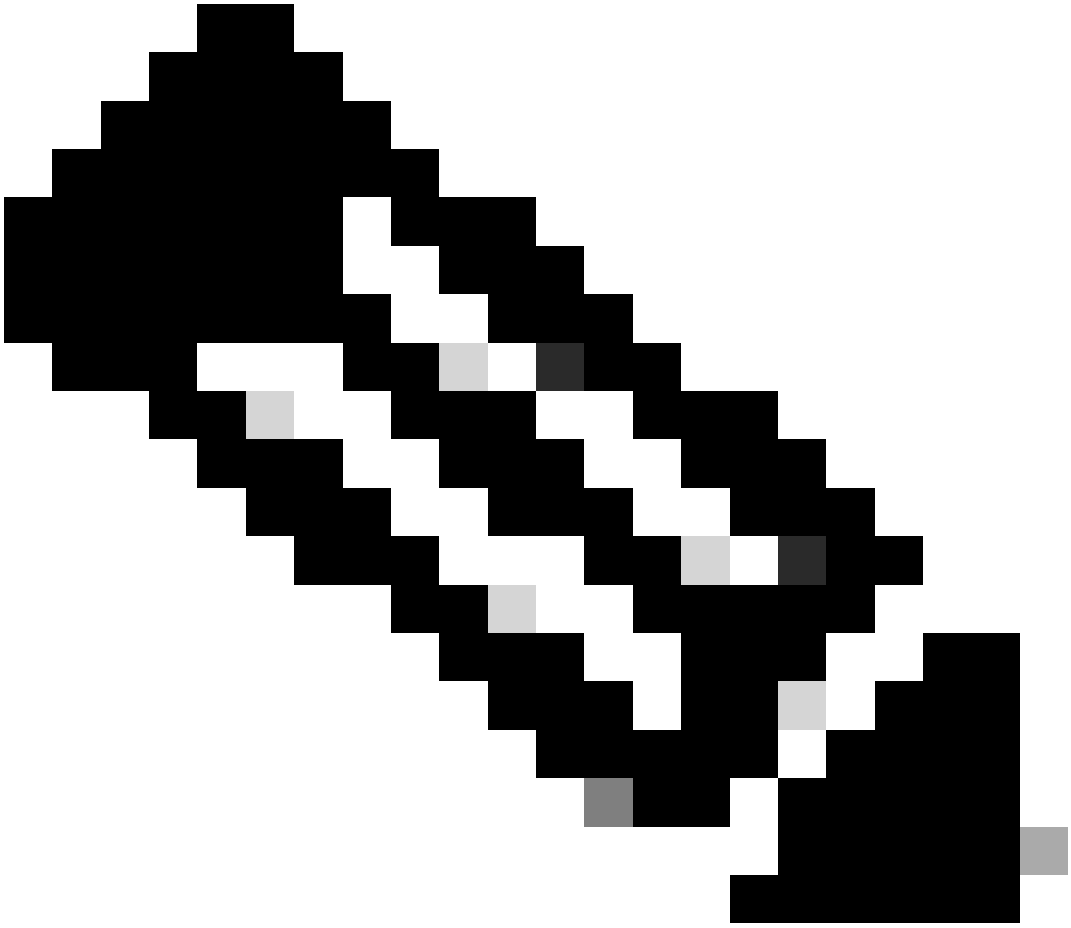
Inscrire des certificats IdP :

Accédez à la section de gestion des certificats dans FMC et inscrivez les certificats IdP codés en Base64 téléchargés pour les deux applications SAML. Ces certificats sont essentiels pour établir la confiance et activer l'authentification SAML.

Pour obtenir des instructions détaillées, reportez-vous aux deux premières étapes sous «

Configuration sur le FTD via FMC » dans la documentation Cisco disponible à l'adresse : [Configurez le client sécurisé avec l'authentification SAML sur FTD géré via FMC](#).





Remarque : L'image a été modifiée pour afficher les deux certificats simultanément pour une meilleure visualisation. Il n’est pas possible d’ouvrir les deux certificats en même temps sur FMC.

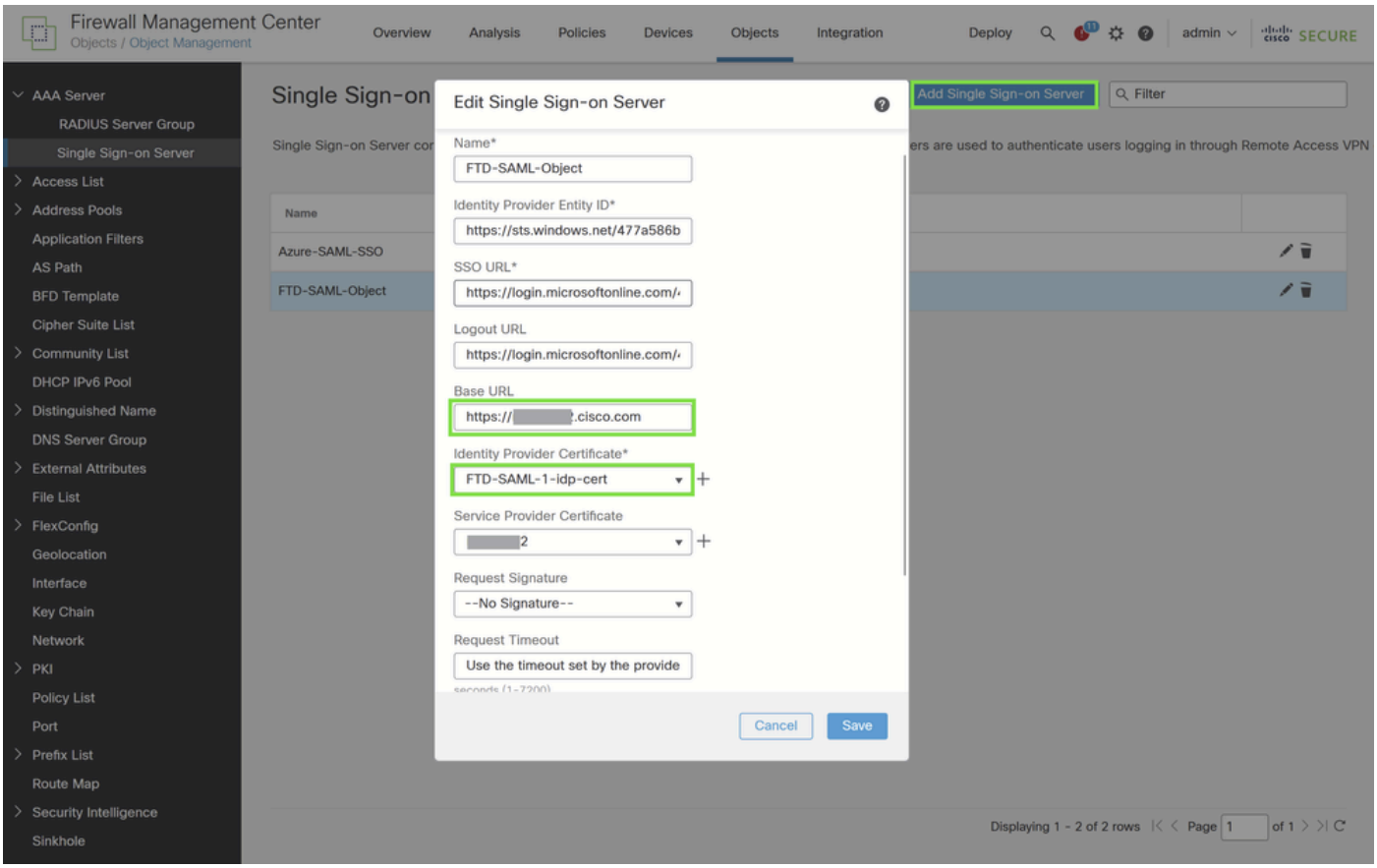
Configuration des paramètres du serveur SAML sur Cisco FTD via FMC

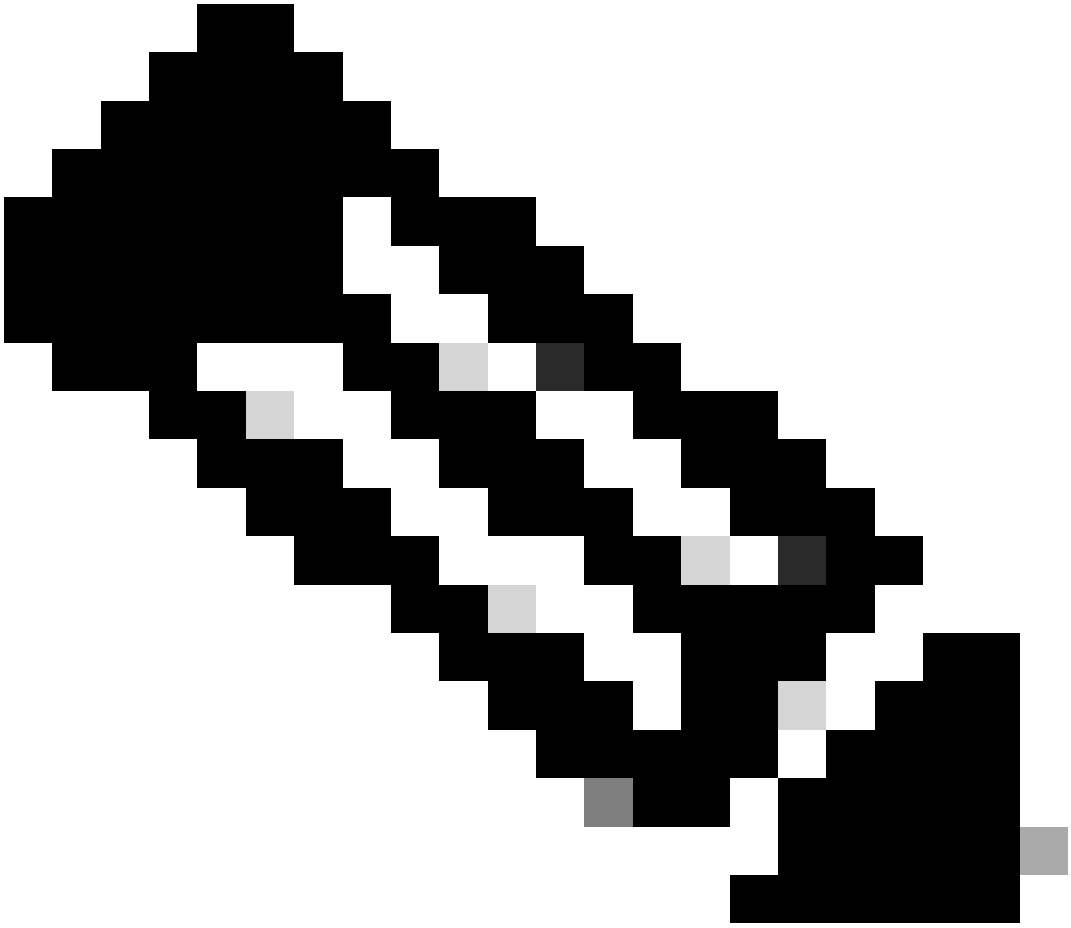
Pour configurer les paramètres du serveur SAML sur votre système Cisco Firepower Threat Defense (FTD) à l'aide de Firepower Management Center (FMC), procédez comme suit :

1. Accédez à Single Sign-on Server Configuration :
    - Accédez à Objets > Gestion des objets > Serveurs AAA > Serveur SSO.
    - Cliquez sur Add Single Sign-on Server pour commencer à configurer un nouveau serveur.
2. Configurer les paramètres du serveur SAML :
    - À l'aide des paramètres collectés à partir de vos applications d'entreprise SAML ou du fichier metadata.xml téléchargé à partir de votre fournisseur d'identité (IdP), remplissez les valeurs SAML nécessaires dans le formulaire Nouveau serveur d'authentification

unique.

- Les paramètres clés à configurer sont les suivants :
  - ID entité du fournisseur SAML : entityID de metadata.xml
  - URL SSO : SingleSignOnService de metadata.xml.
  - URL de déconnexion : SingleLogoutService de metadata.xml.
  - URL DE BASE : FQDN de votre certificat d'ID SSL FTD.
  - Certificat du fournisseur d'identité : Certificat de signature IdP.
    - Dans la section Certificat de fournisseur d'identité, joignez l'un des certificats IdP inscrits
    - Pour ce cas d'utilisation, nous utilisons le certificat IdP de l'application FTD-SAML-1.
  - Certificat du fournisseur de services : Certificat de signature FTD.



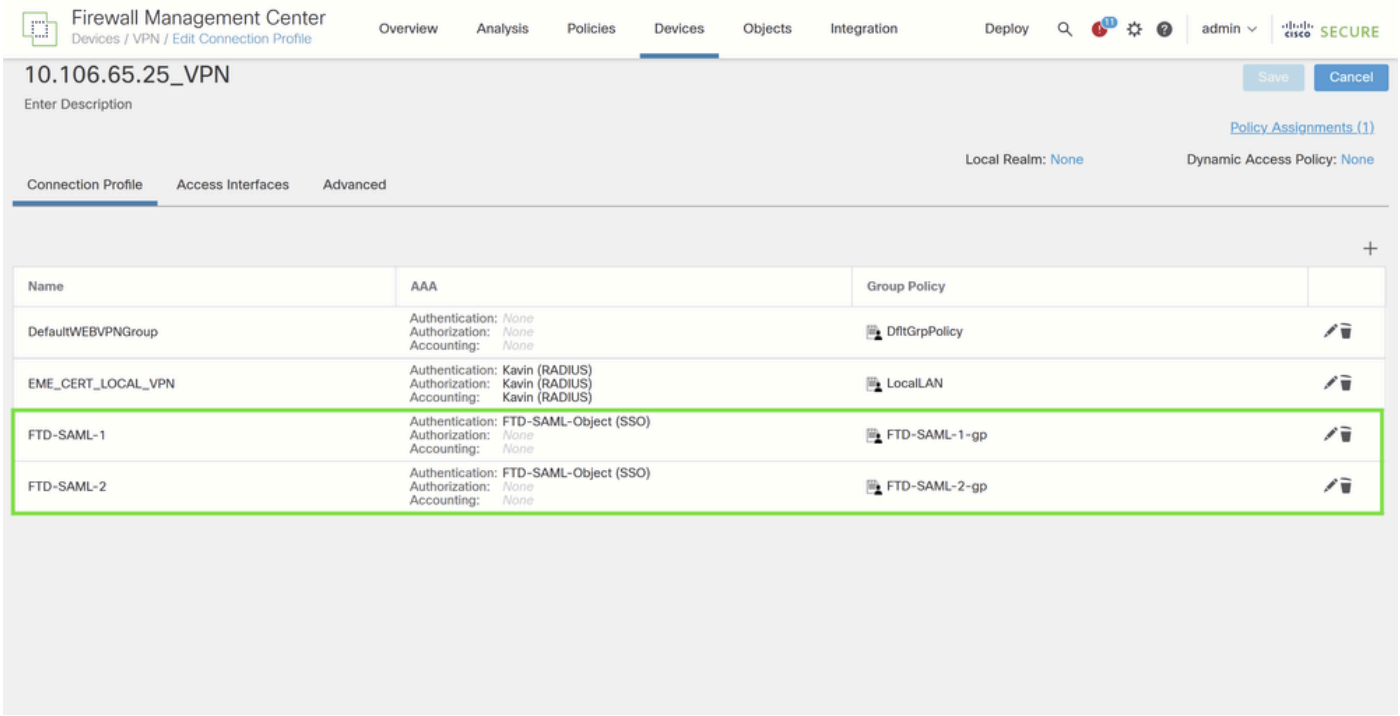


Remarque : Dans la configuration actuelle, seul le certificat du fournisseur d'identité peut être remplacé à partir de l'objet SAML dans les paramètres du profil de connexion. Malheureusement, les fonctionnalités telles que « Demander une nouvelle authentification IdP à la connexion » et « Activer l'authentification IdP uniquement accessible sur le réseau interne » ne peuvent pas être activées ou désactivées individuellement pour chaque profil de connexion.

Configuration des profils de connexion sur Cisco FTD via FMC

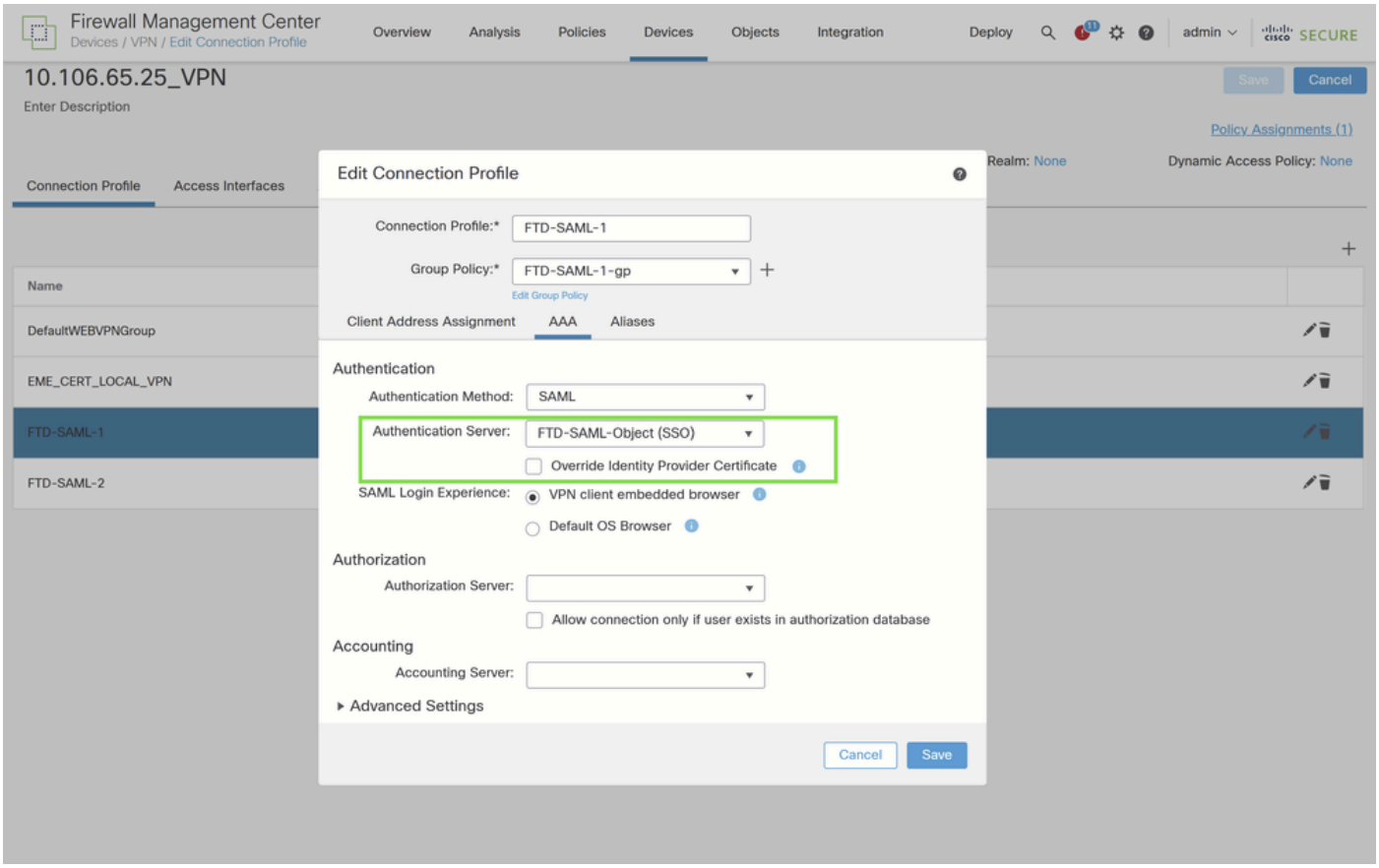
Pour finaliser la configuration de l'authentification SAML, vous devez configurer les profils de connexion avec les paramètres appropriés et définir l'authentification AAA sur SAML à l'aide du serveur SAML précédemment configuré.

Pour obtenir des conseils plus détaillés, reportez-vous à la cinquième étape sous « Configuration sur le FTD via FMC » dans la documentation Cisco : Configurez le client sécurisé avec l'authentification SAML sur FTD géré via FMC.



Extrait de la configuration AAA pour le premier profil de connexion

Voici un aperçu des paramètres de configuration AAA pour le premier profil de connexion :

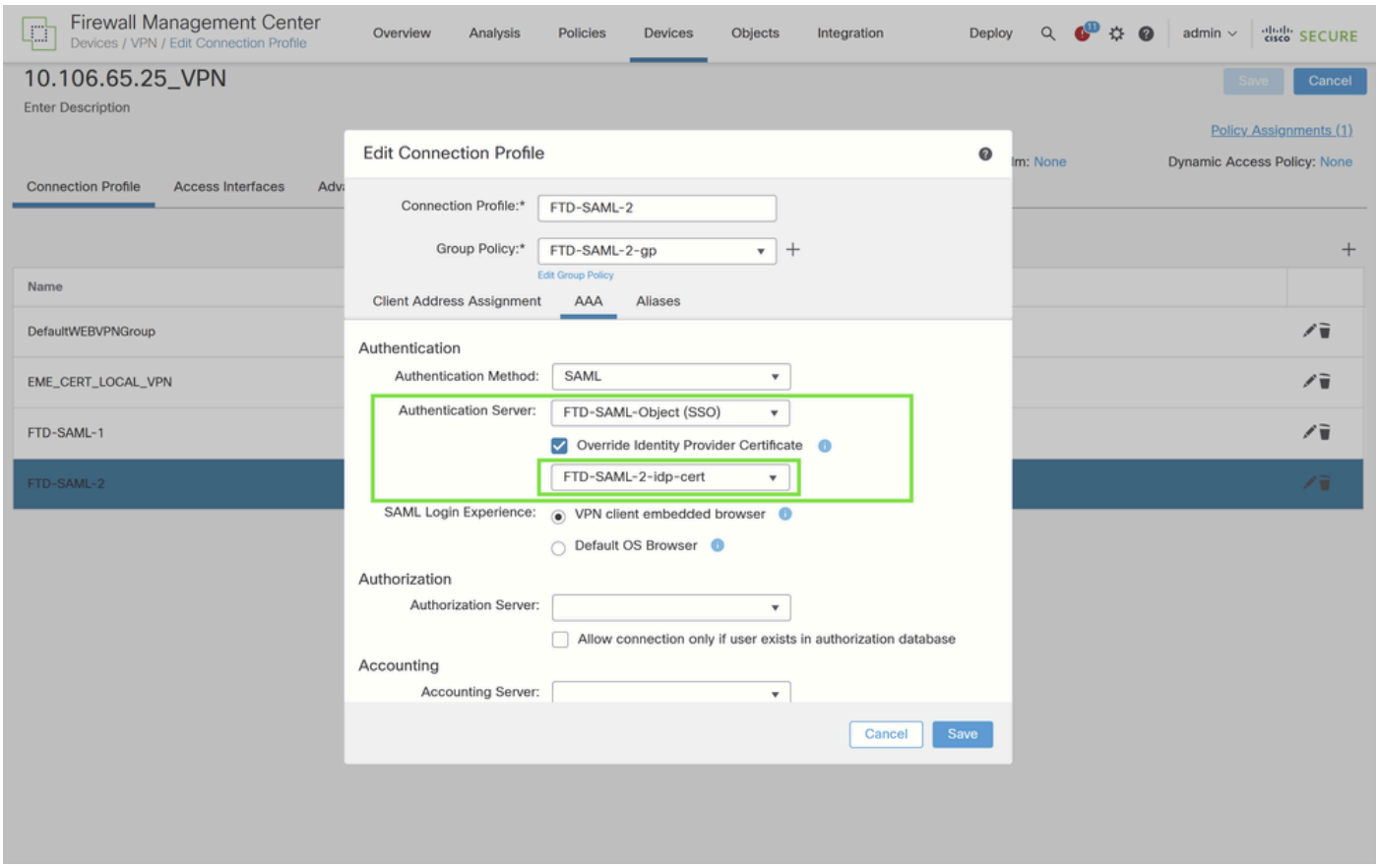


Configuration du remplacement du certificat IdP pour le deuxième profil de connexion sur Cisco FTD

Pour vous assurer que le certificat du fournisseur d'identité (IdP) correct est utilisé pour le second profil de connexion, activez le remplacement du certificat IdP en procédant comme suit :

Dans les paramètres du profil de connexion, localisez et activez l'option « Remplacer le certificat du fournisseur d'identité » pour autoriser l'utilisation d'un certificat de fournisseur d'identité différent de celui configuré pour le serveur SAML.

Dans la liste des certificats IdP inscrits, sélectionnez le certificat spécifiquement inscrit pour l'application FTD-SAML-2. Cette sélection garantit que lorsqu'une demande d'authentification est effectuée pour ce profil de connexion, le certificat IdP correct est utilisé.



Déploiement de la configuration

Naviguez jusqu'**Deploy** > **Deployment**au FTD approprié et sélectionnez-le pour appliquer les modifications SAML Authentication VPN.

Vérifier

Configuration sur la ligne de commande 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
```

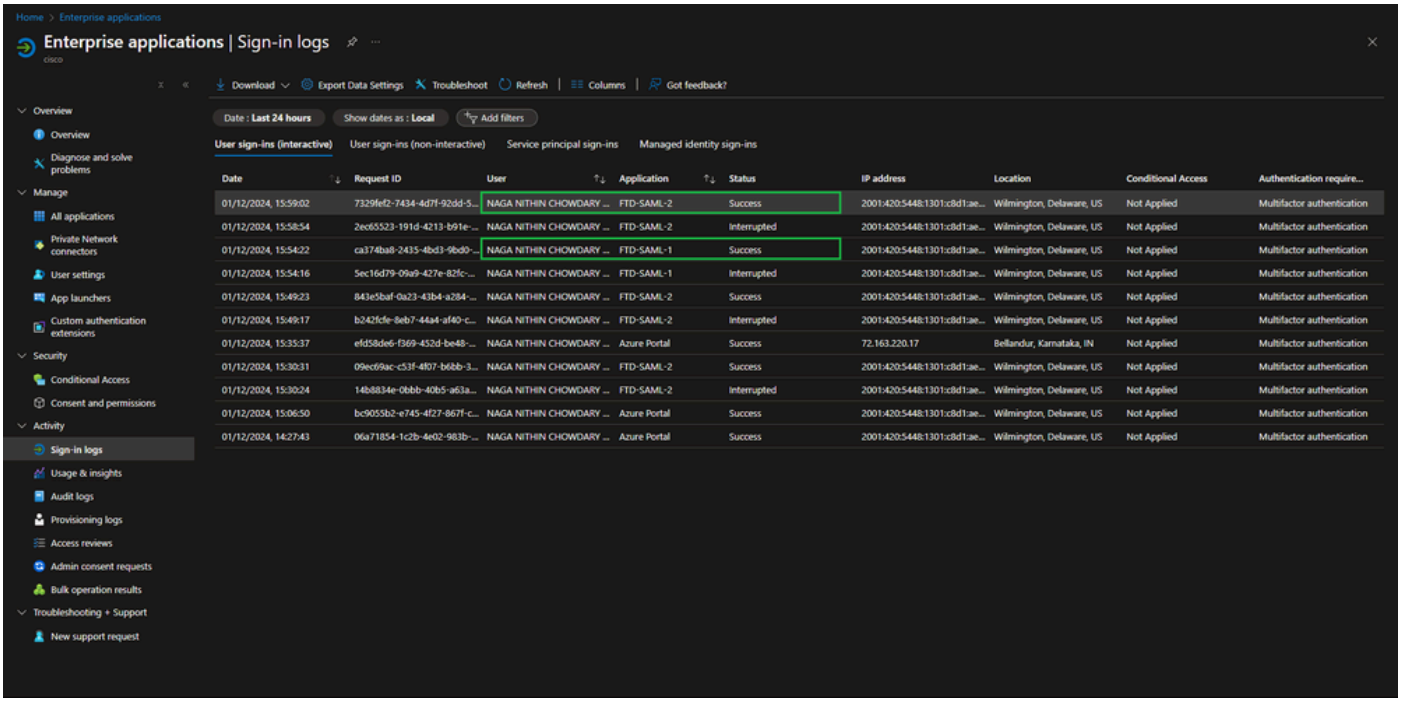
saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/

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

```
firepower#
```

Journaux de connexion à partir de l'identificateur d'entrée Azure

Accédez à la section Logs de connexion sous application d'entreprise. Recherchez les demandes d'authentification liées aux profils de connexion spécifiques, tels que FTD-SAML-1 et FTD-SAML-2. Vérifiez que les utilisateurs s'authentifient correctement via les applications SAML associées à chaque profil de connexion.



Journaux de connexion sur Azure IdP

Dépannage

1. Vous pouvez effectuer un dépannage à l'aide du DART à partir du PC utilisateur Secure Client.

2. Pour dépanner un problème d'authentification SAML, utilisez ce débogage :

```
<#root>

firepower#

 debug webvpn saml 255
```

3. Vérifiez la configuration du client sécurisé comme expliqué ci-dessus ; cette commande peut être utilisée pour vérifier le certificat.

```
<#root>

firepower#

 show crypto ca certificate
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.