FTDでの複数RAVPN接続プロファイルのSAML認証の設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

コンフィギュレーション

- 設定の概要:
- 設定
  - Azure IdPの構成
  - FMCを介したFTDの設定

確認

- FTDコマンドラインでの設定
- Azureエントリ識別子からのサインインログ

トラブルシュート

はじめに

このドキュメントでは、FMCによって管理されるCisco FTDの複数の接続プロファイルに対するAzure IDプロバイダーを使用したSAML認証について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center(FMC)で管理される次世代ファイアウォール(NGFW)のセキュアクライアントの設定
- SAMLおよびmetatada.xml値

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Threat Defense(FTD)バージョン7.4.0
- FMCバージョン7.4.0
- SAML 2.0を使用したAzure Microsoft Entra ID
- Cisco Secureクライアント5.1.7.80

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この構成により、FTDはAzure idp上の2つの異なるSAMLアプリケーションと、FMC上で構成された1つのSAMLオブジェクトを使用して、セキュアなクライアントユーザーを認証できます。

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://

Microsoft Azure環境では、複数のアプリケーションが同じエンティティIDを共有できます。各アプリケーションは、通常、異なるトンネルグループにマッピングされ、一意の証明書を必要とし、単一のSAML IdPオブジェクトのFTD側のIdP設定内で複数の証明書を設定する必要があります。ただし、Cisco Bug ID CSCvi29084で説明されているように、Cisco FTDでは1つのSAML IdPオブジェクトに複数の証明書を設定することはできません。

この制限を克服するために、シスコはFTDバージョン7.1.0およびASAバージョン9.17.1から使用可能なIdP証明書オーバーライド機能を導入しました。この機能拡張は、この問題に対する恒久的な解決策となり、バグレポートに記載されている既存の回避策を補完します。

コンフィギュレーション

このセクションでは、Firepower Management Center(FMC)で管理されるCisco Firepower Threat Defense(FTD)の複数の接続プロファイルのIDプロバイダー(IdP)としてAzureを使用してSAML認証を設定するプロセスの概要について説明します。 IdP証明書の上書き機能を使用すると、この設定を効果的に行うことができます。

設定の概要:

2つの接続プロファイルをCisco FTDに設定します。

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

この設定例では、VPNゲートウェイURL(Cisco Secure Client FQDN)がnigarapa2.cisco.comに設定されています

設定

Azure IdPの構成

Cisco Secure ClientのSAMLエンタープライズアプリケーションを効果的に設定するには、次の手順を実行して、各トンネルグループのすべてのパラメータが正しく設定されていることを確認します。

SAMLエンタープライズアプリケーションへのアクセス：

エンタープライズアプリケーションがリストされているSAMLプロバイダーの管理コンソールに移動します。

適切なSAMLアプリケーションを選択します。

設定するCisco Secure Clientトンネルグループに対応するSAMLアプリケーションを特定して選択します。

識別子（エンティティID）を設定します。

各アプリケーションの識別子（エンティティID）を設定します。これは、ベースURLである必要があります。ベースURLは、Cisco Secure Clientの完全修飾ドメイン名(FQDN)です。

応答URL（アサーションコンシューマサービスURL）を設定します。

正しいベースURLを使用して、返信URL（アサーションコンシューマサービスURL）を設定します。Cisco Secure ClientのFQDNと一致していることを確認します。

接続プロファイルまたはトンネルグループ名をベースURLに追加して、特異性を確保します。

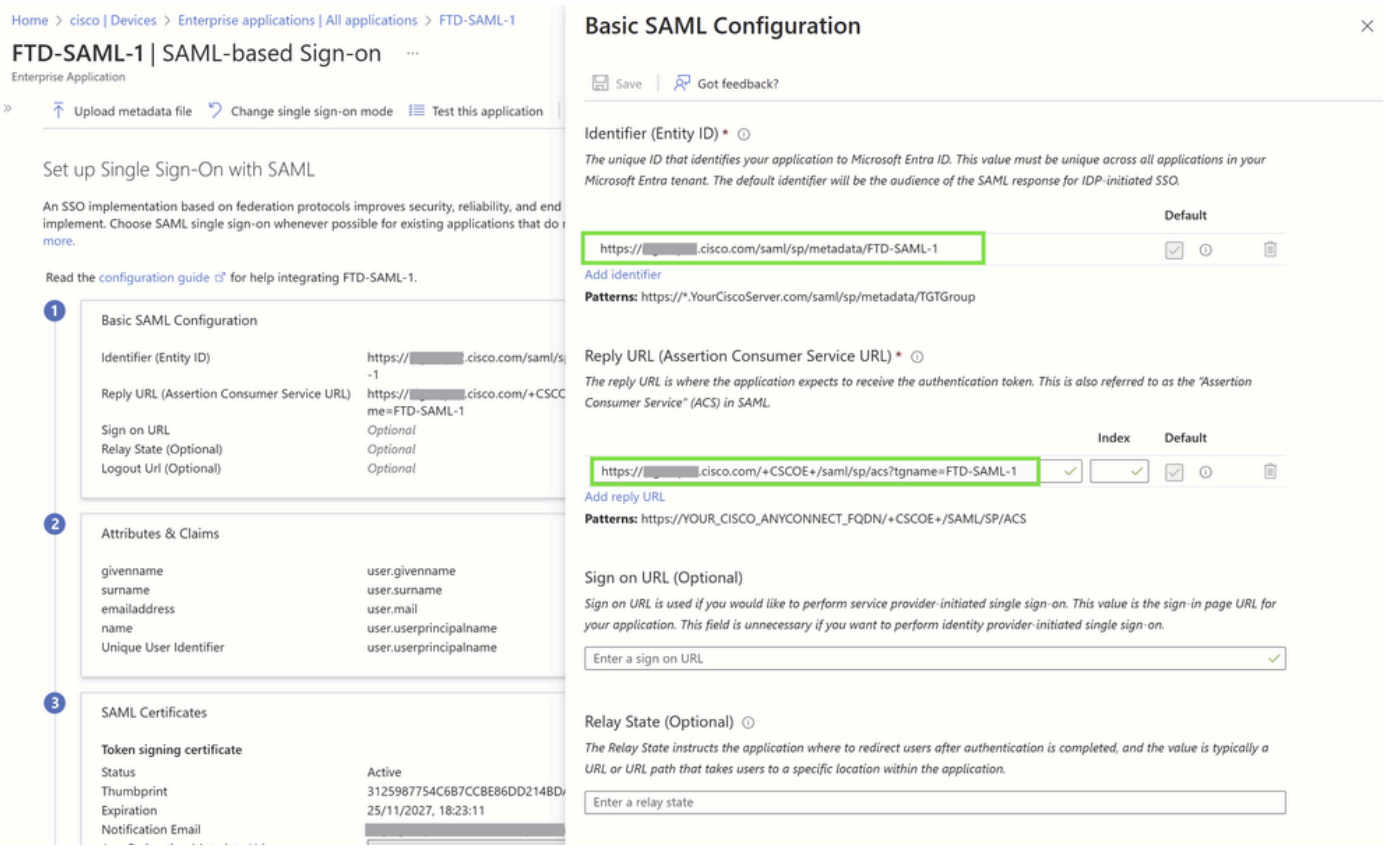
設定の確認:

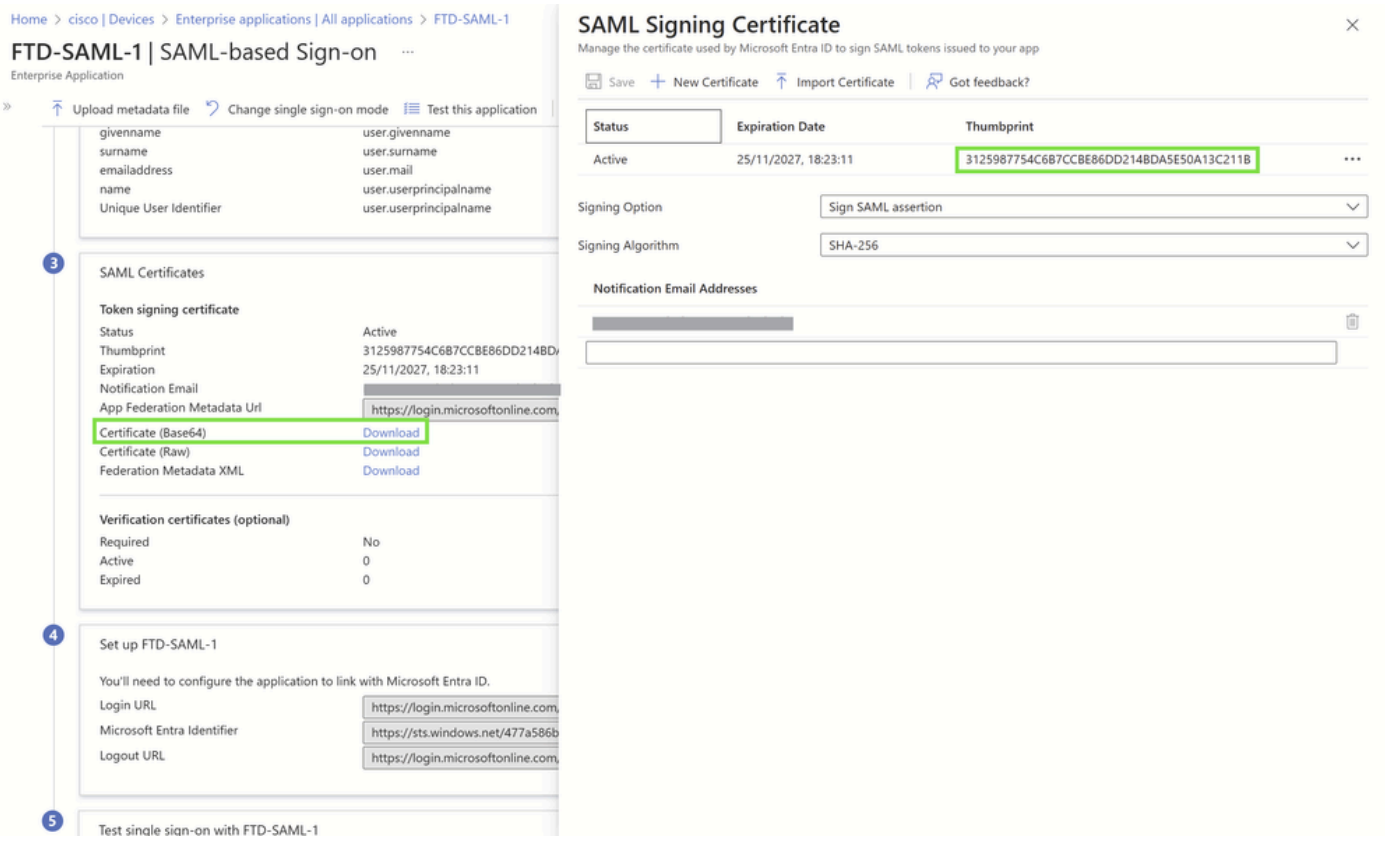
すべてのURLとパラメータが正しく入力され、対応するトンネルグループに対応していることを再確認します。

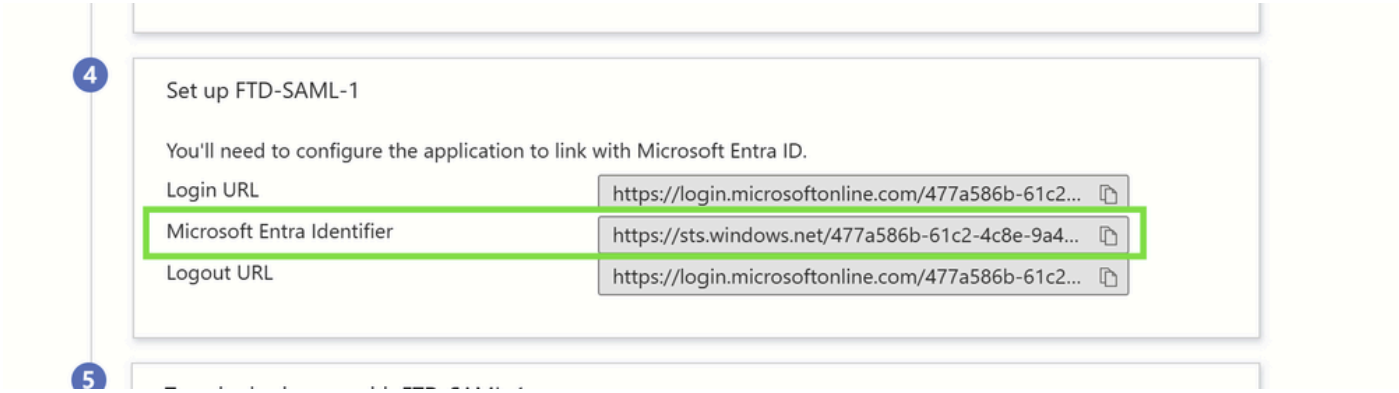
変更を保存し、可能であればテスト認証を実行して、設定が期待どおりに動作していることを確認します。

詳細なガイダンスについては、シスコのドキュメント「SAMLを使用したMicrosoft Azure MFAでのASAセキュアクライアントVPNの設定」の「Microsoft App GalleryからのCisco Secure Clientの追加」を参照してください。

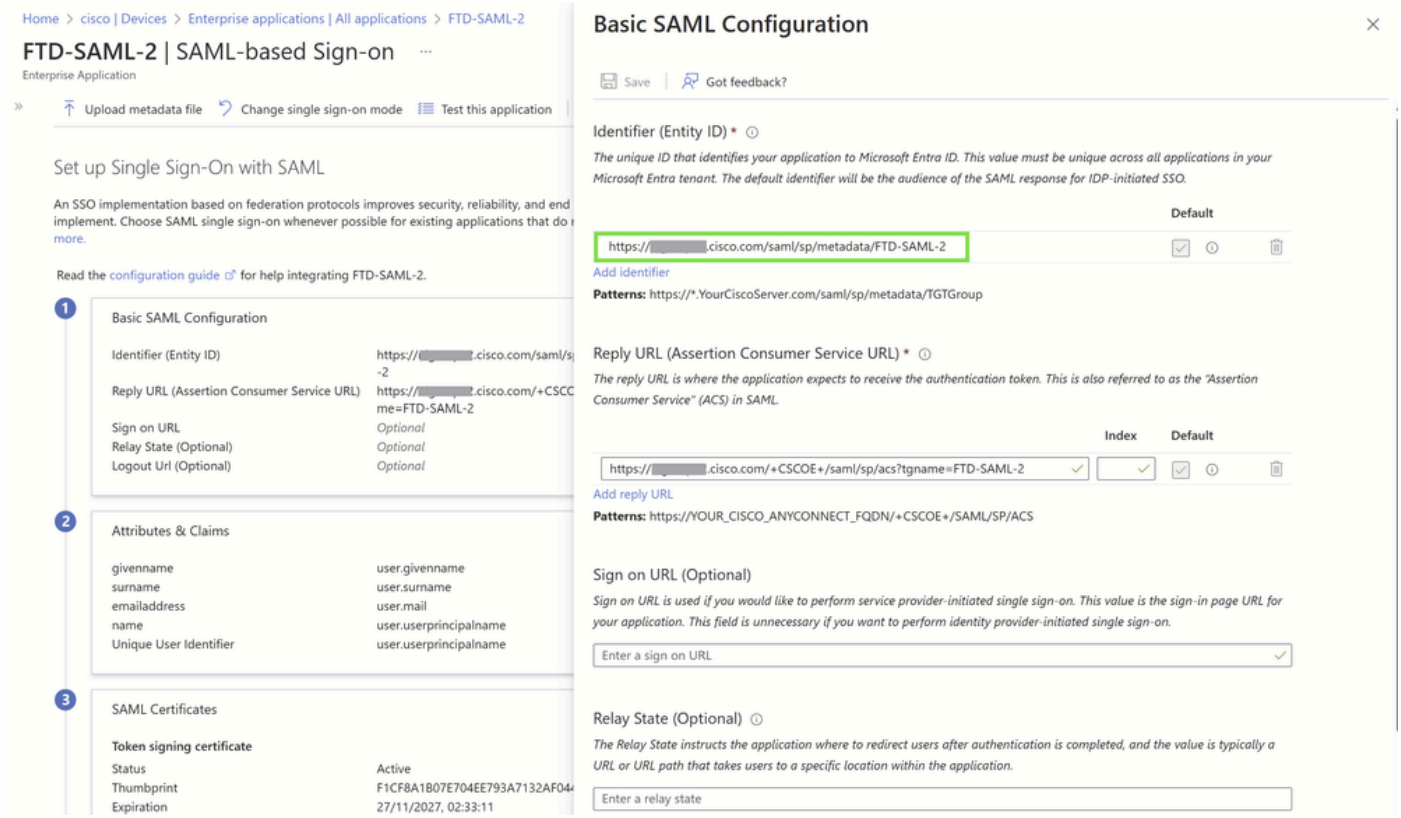
FTD-SAML-1

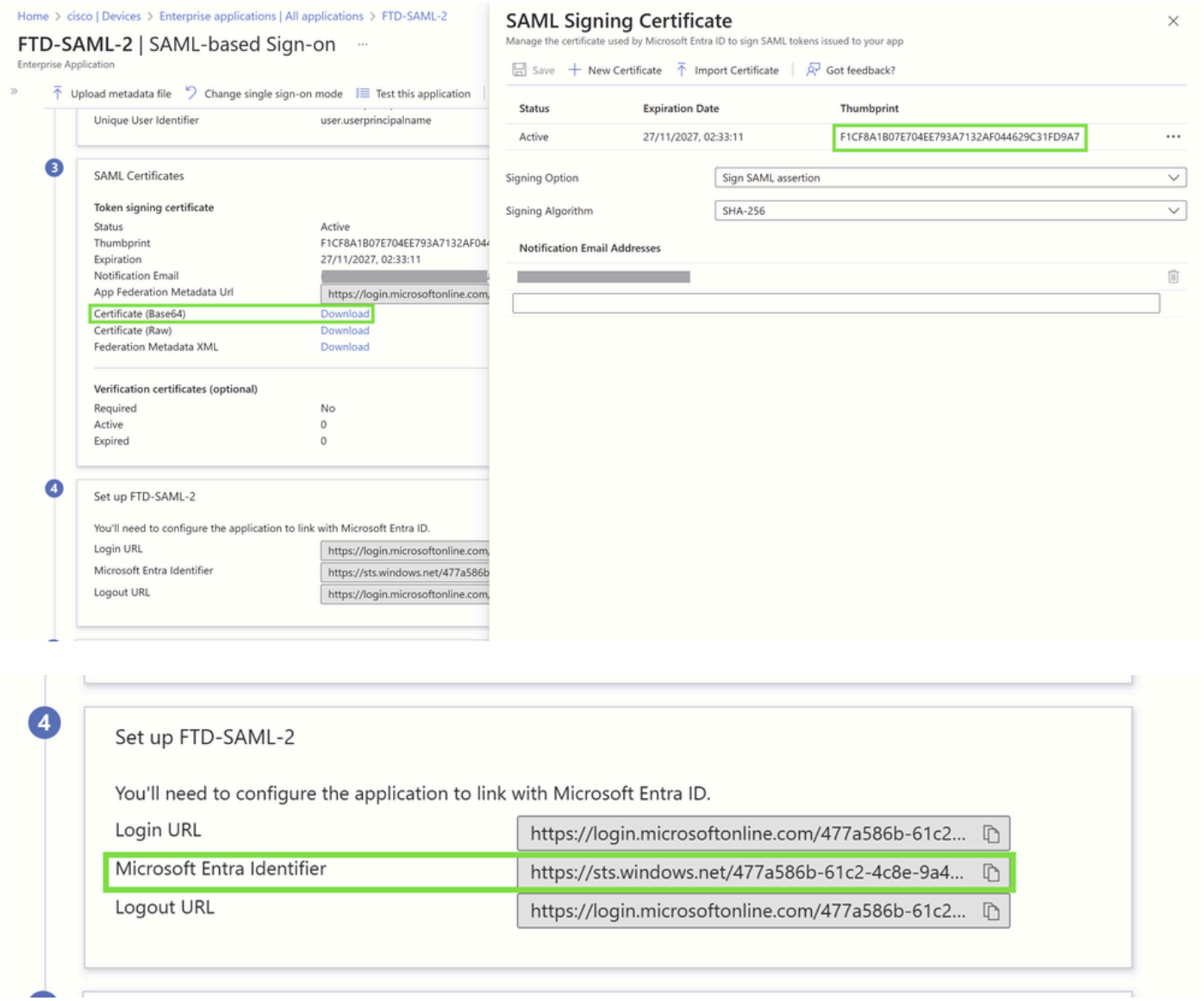

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security,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



IDプロバイダーとしてMicrosoft Entraを使用してSAML認証を設定するために必要な情報とファイルが揃っていることを確認してください。

Microsoft Entra Identifierを探します。

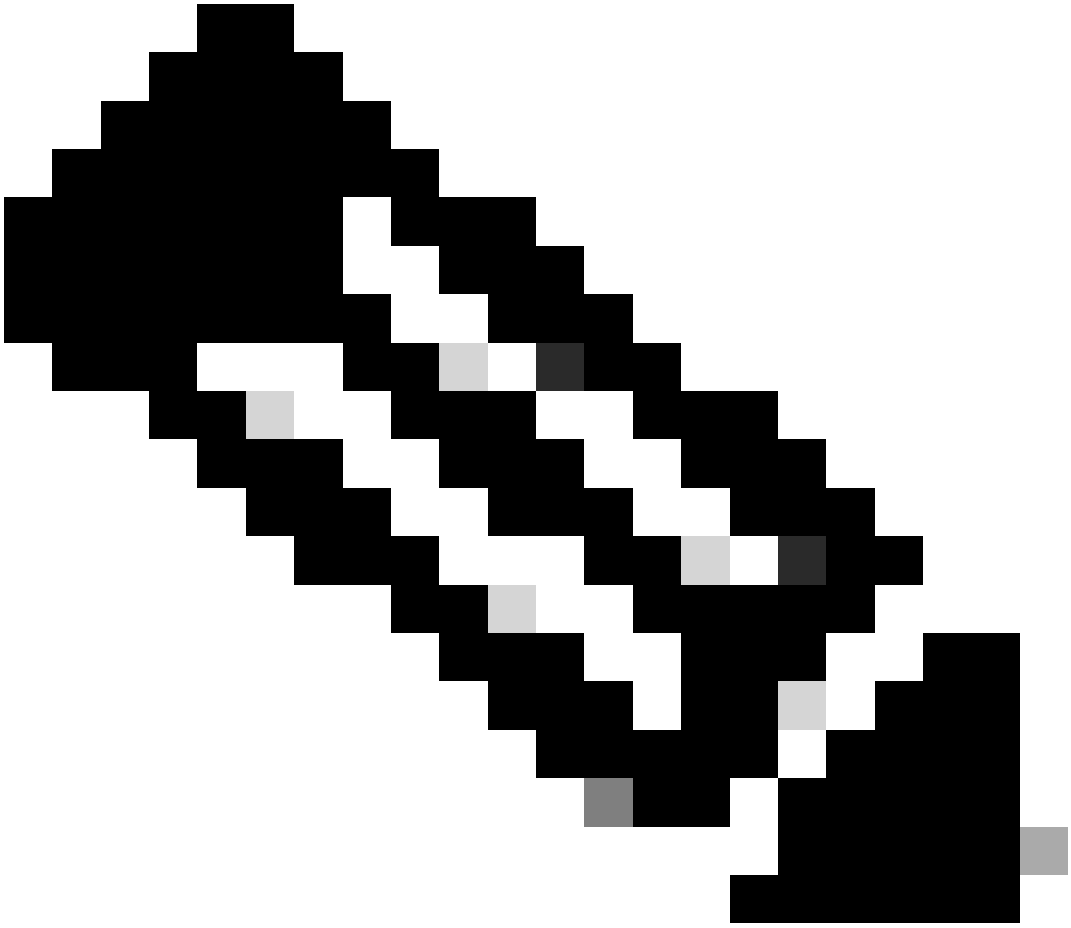
Microsoft Entraポータル内の両方のSAMLエンタープライズアプリケーションの設定にアクセスします。

Microsoft Entra Identifierは、両方のアプリケーションで一貫しており、SAML設定にとって重要です。

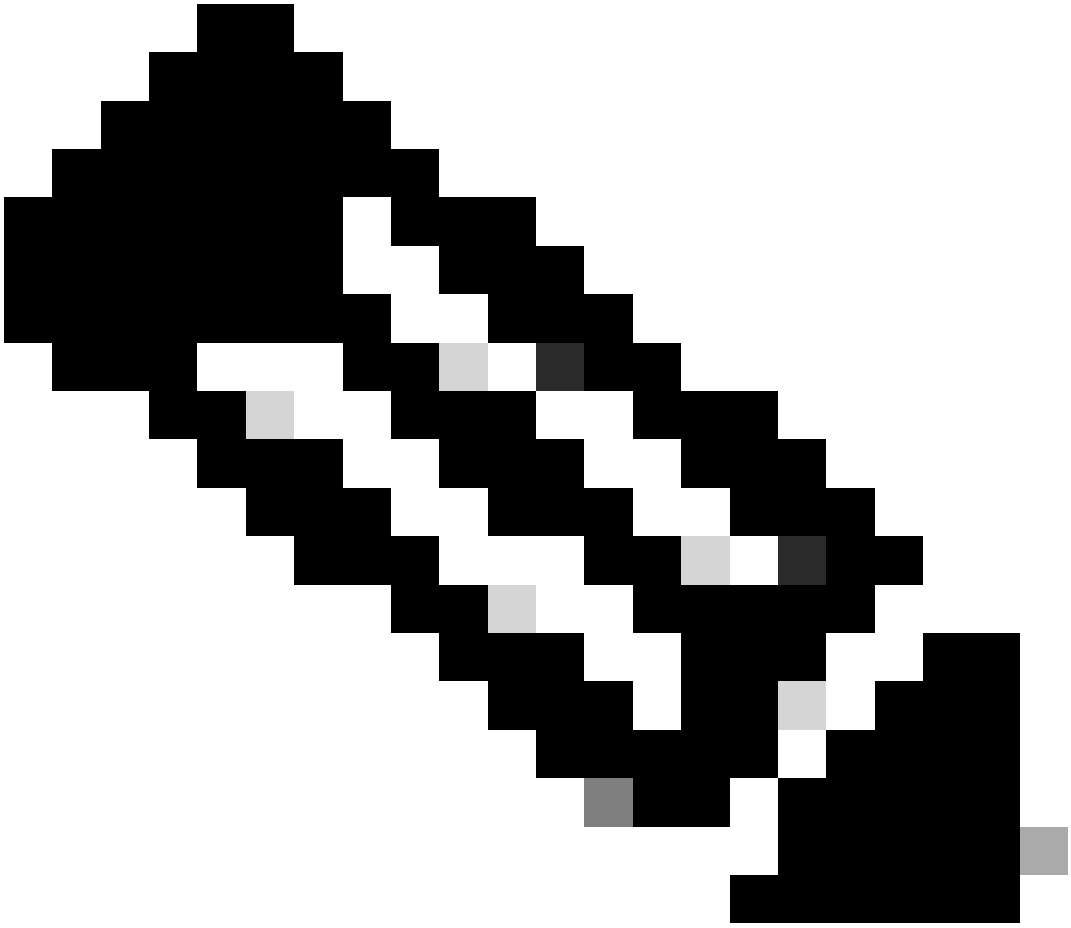
Base64 IdP証明書のダウンロード：

設定された各SAMLエンタープライズアプリケーションに移動します。

それぞれのBase64エンコードIdP証明書をダウンロードします。これらの証明書は、アイデンティティプロバイダーとCisco VPNの設定間の信頼を確立するために不可欠です。



注:FTD接続プロファイルに必要なSAML設定はすべて、各アプリケーション用のIdPから提供されるmetadata.xmlファイルから取得することもできます。



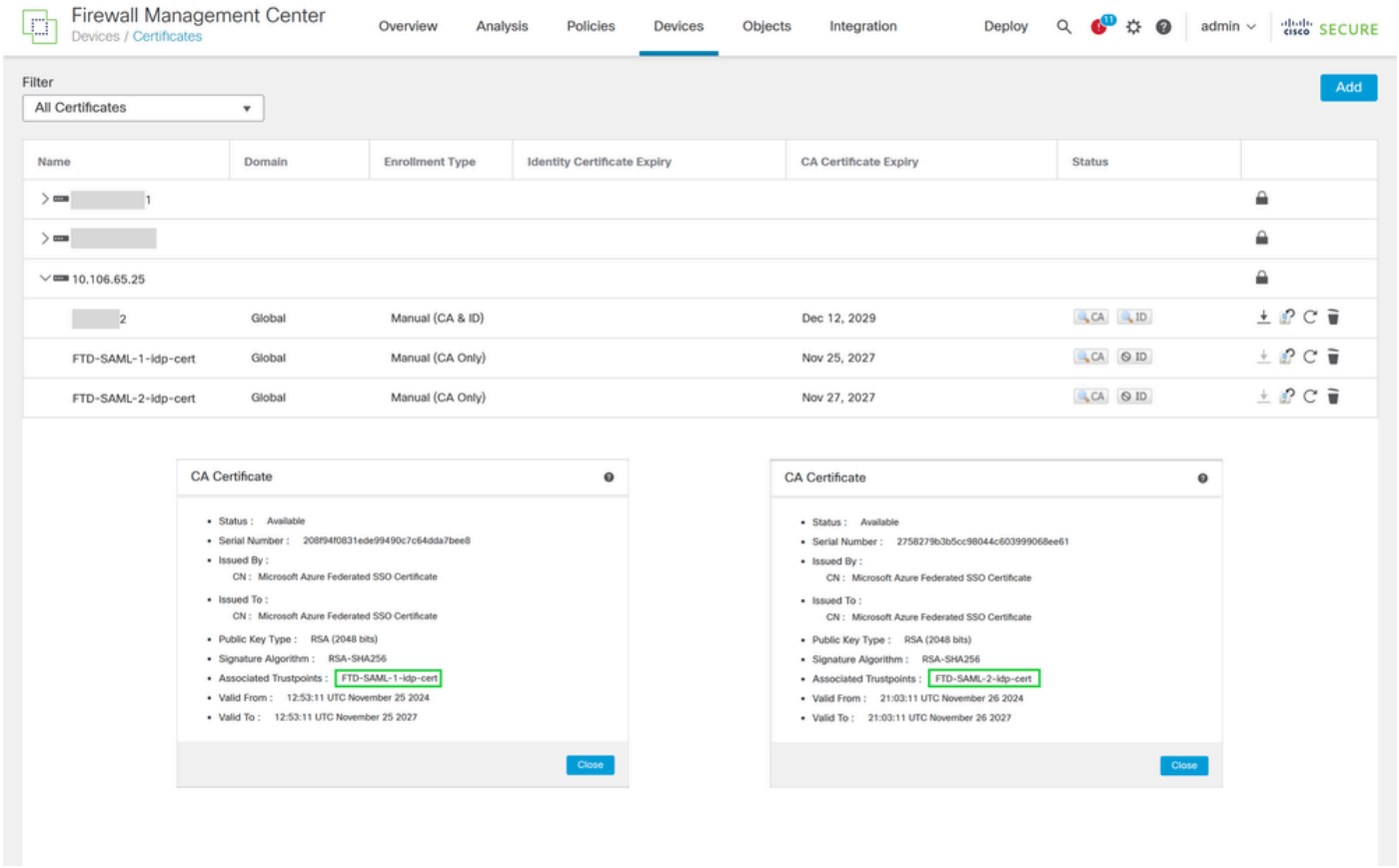
注：カスタムIdP証明書を使用するには、カスタム生成のIdP証明書をIdPとFMCの両方にアップロードする必要があります。Azure IdPの場合、証明書がPKCS#12形式であることを確認してください。FMCで、PKCS#12ファイルではなく、IdPからのID証明書のみをアップロードします。詳細な手順については、シスコのドキュメント「FDMでSAML認証を使用して複数のRAVPNプロファイルを設定する」の「AzureおよびFDMでのPKCS#12ファイルのアップロード」を参照してください。

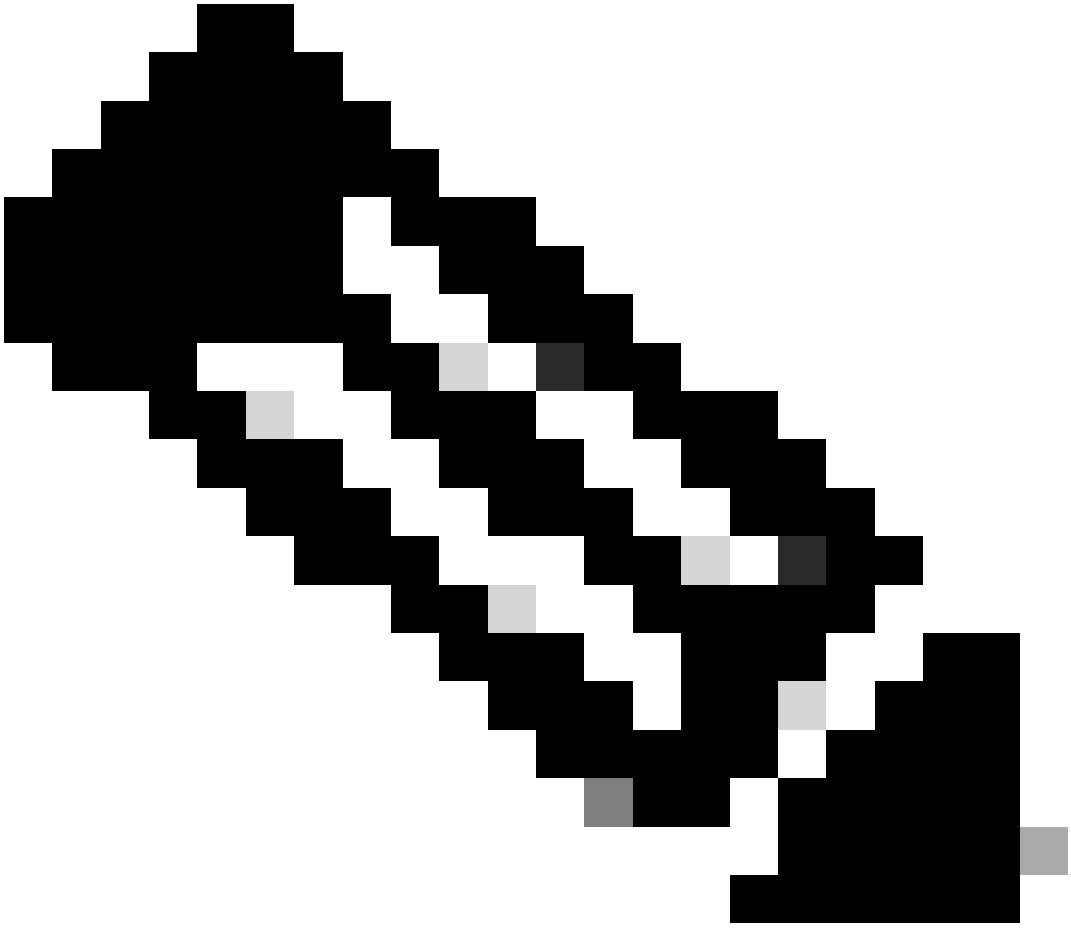
FMCを介したFTDの設定

IdP証明書の登録：

FMC内の証明書管理セクションに移動し、両方のSAMLアプリケーション用にダウンロードしたBase64でエンコードされたIdP証明書を登録します。これらの証明書は、信頼を確立し、SAML認証を有効にするために不可欠です。

詳細なガイダンスについては、シスコのドキュメント「FMCを介して管理されるFTDのSAML認証でセキュアクライアントを設定する」の最初の2つの手順を参照してください。


Firewall Management Center
Devices / Certificates
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Filter
All Certificates
Add
Name
Domain
Enrollment Type
Identity Certificate Expiry
CA Certificate Expiry
Status
10.106.65.25
Global
Manual (CA & ID)
Dec 12, 2029
FTD-SAML-1-idp-cert
Global
Manual (CA Only)
Nov 25, 2027
FTD-SAML-2-idp-cert
Global
Manual (CA Only)
Nov 27, 2027
CA Certificate
Status : Available
Serial Number : 208f94f0831ede99490c7c64dda7bee8
Issued By :
CN : Microsoft Azure Federated SSO Certificate
Issued To :
CN : Microsoft Azure Federated SSO Certificate
Public Key Type : RSA (2048 bits)
Signature Algorithm : RSA-SHA256
Associated Trustpoints : FTD-SAML-1-idp-cert
Valid From : 12:53:11 UTC November 25 2024
Valid To : 12:53:11 UTC November 25 2027
Close
CA Certificate
Status : Available
Serial Number : 2758279b3b5cc98044c603999068ee61
Issued By :
CN : Microsoft Azure Federated SSO Certificate
Issued To :
CN : Microsoft Azure Federated SSO Certificate
Public Key Type : RSA (2048 bits)
Signature Algorithm : RSA-SHA256
Associated Trustpoints : FTD-SAML-2-idp-cert
Valid From : 21:03:11 UTC November 26 2024
Valid To : 21:03:11 UTC November 26 2027
Close



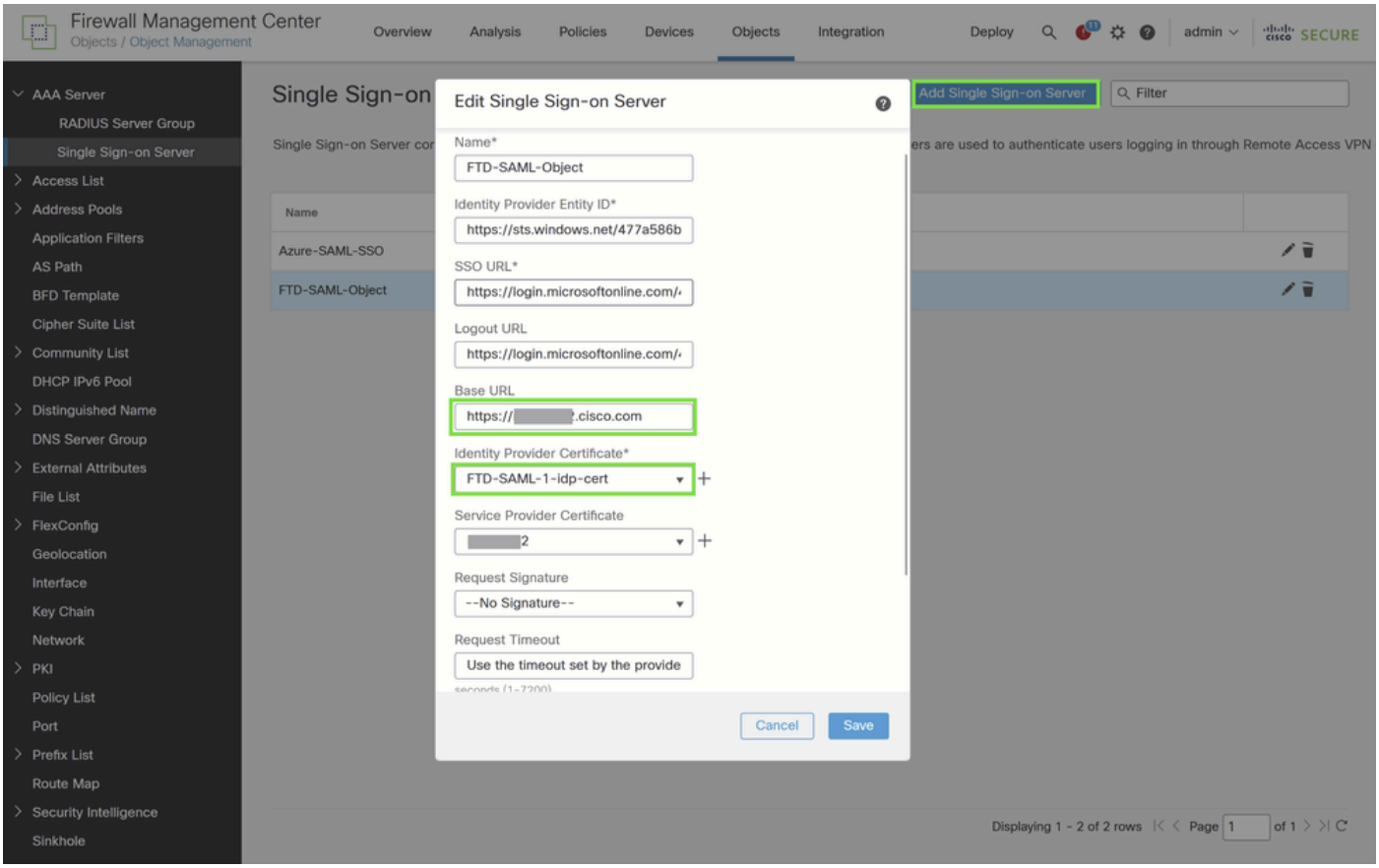
注：画像は、より見やすくするために、両方の証明書を同時に表示するように編集されています。FMCで両方の証明書を同時に開くことはできません。

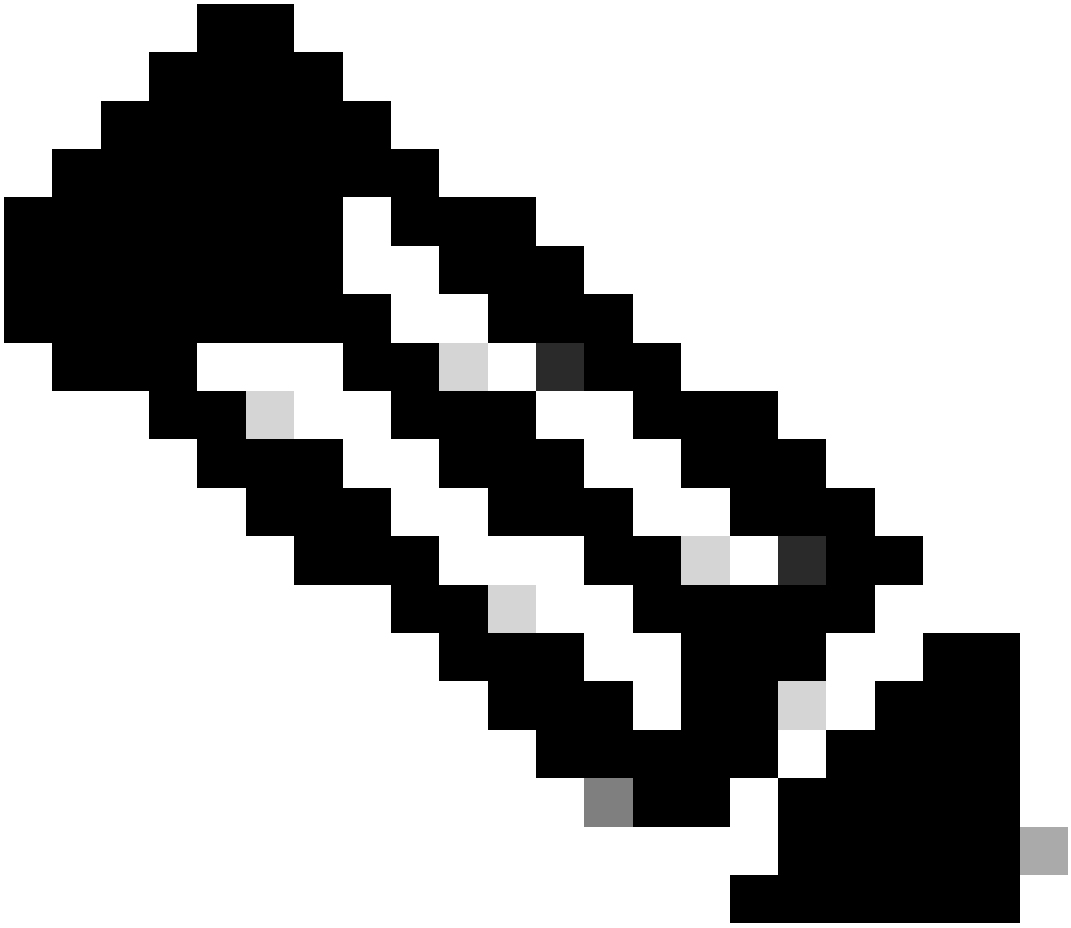
FMCを介したCisco FTDでのSAMLサーバ設定

Firepower Management Center(FMC)を使用してCisco Firepower Threat Defense(FTD)でSAMLサーバを設定するには、次の手順を実行します。

1. Single Sign-on Server Configurationの順に移動します。
   - Objects > Object Management > AAA Servers > Single Sign-on Serverの順に選択します。
   - Add Single Sign-on Serverをクリックして、新しいサーバの設定を開始します。
2. SAMLサーバの設定：
   - SAMLエンタープライズアプリケーションから収集したパラメータ、またはアイデンティティプロバイダー(IdP)からダウンロードしたmetadata.xmlファイルを使用して、New Single Sign-on Serverフォームに必要なSAML値を入力します。
   - 設定する主なパラメータは次のとおりです。

- SAMLプロバイダーエンティティID: metadata.xmlのentityID
- SSO URL: metadata.xmlのSingleSignOnService。
- ログアウトURL: metadata.xmlのSingleLogoutService。
- BASE URL:FTD SSL ID証明書のFQDN。
- アイデンティティプロバイダー証明書： IdP署名証明書。
  - Identity Provider Certificateセクションで、登録済みIdP証明書のいずれかを添付します
  - この使用例では、FTD-SAML-1アプリケーションからのIdP証明書を使用しています。
- サービスプロバイダー証明書：FTD署名証明書。



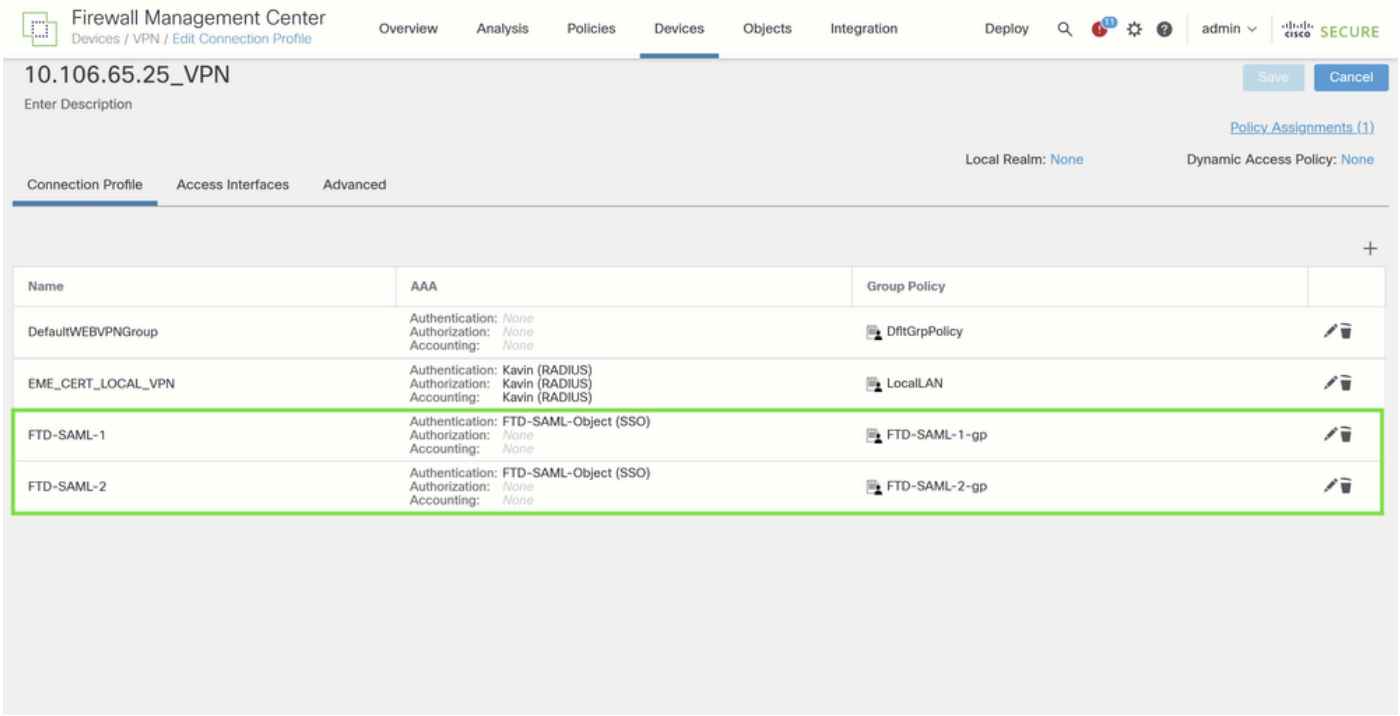


注：現在の設定では、接続プロファイル設定内のSAMLオブジェクトから上書きできるのは、アイデンティティプロバイダー証明書だけです。残念ながら、「ログイン時のIdP再認証の要求」や「内部ネットワークからアクセス可能なIdPのみを有効にする」などの機能は、各接続プロファイルに対して個別に有効または無効にすることはできません。

FMCによるCisco FTDの接続プロファイルの設定

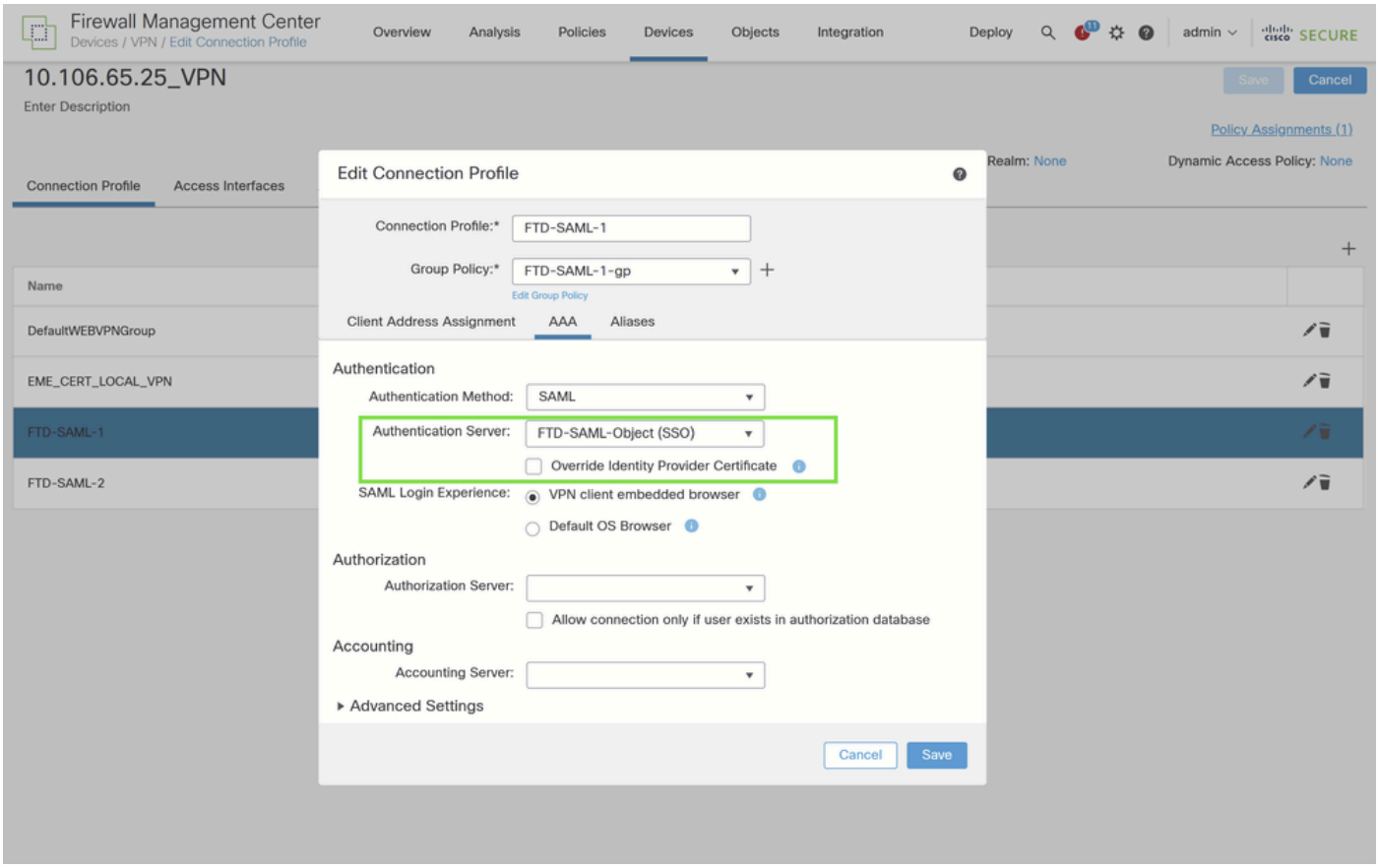
SAML認証の設定を完了するには、適切なパラメータを使用して接続プロファイルを設定し、以前に設定したSAMLサーバを使用してAAA認証をSAMLに設定する必要があります。

詳細なガイダンスについては、シスコのドキュメント「FMCを介して管理されるFTDでSAML認証を使用してセキュアクライアントを設定する」の5番目のステップを参照してください。



最初の接続プロファイル用のAAA設定の抽出

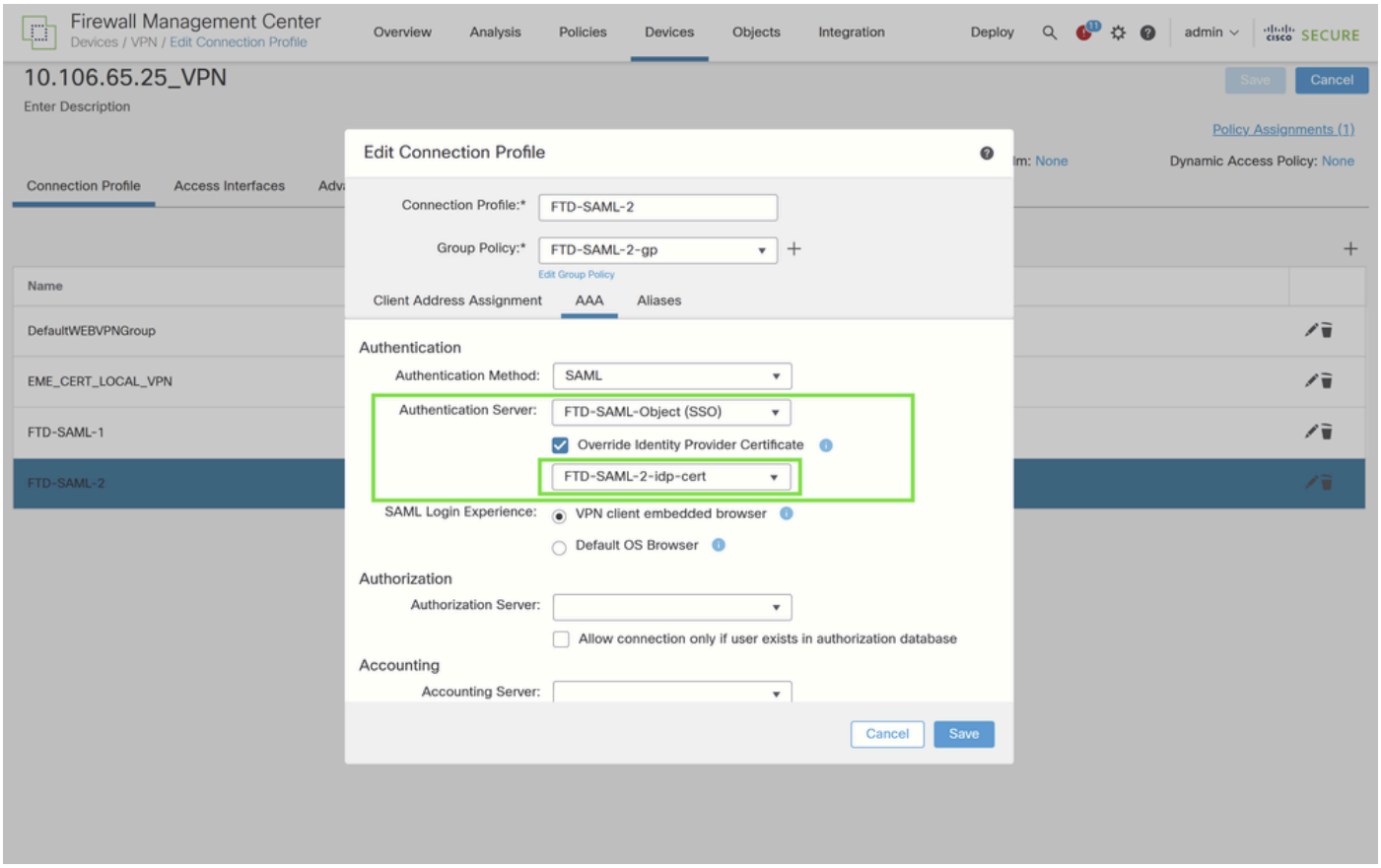
最初の接続プロファイルのAAA設定の概要を次に示します。



Cisco FTDの2番目の接続プロファイルのためのIdP証明書オーバーライドの設定
2番目の接続プロファイルに正しいアイデンティティプロバイダー(IdP)証明書が使用されるようにするには、次の手順を実行してIdP証明書のオーバーライドを有効にします。

接続プロファイル設定で、オプション「Override Identity Provider Certificate」を見つけて有効にし、SAMLサーバに設定されているものとは異なるIdP証明書の使用を許可します。

登録済みIdP証明書のリストから、FTD-SAML-2アプリケーション用に明示的に登録済みの証明書を選択します。この選択により、この接続プロファイルに対して認証要求が行われたときに、正しいIdP証明書が使用されることが保証されます。



設定の導入

SAML認証VPN**Deploy > Deployment**の変更を適用する適切なFTDに移動して選択します。

確認

FTDコマンドラインでの設定

<#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>

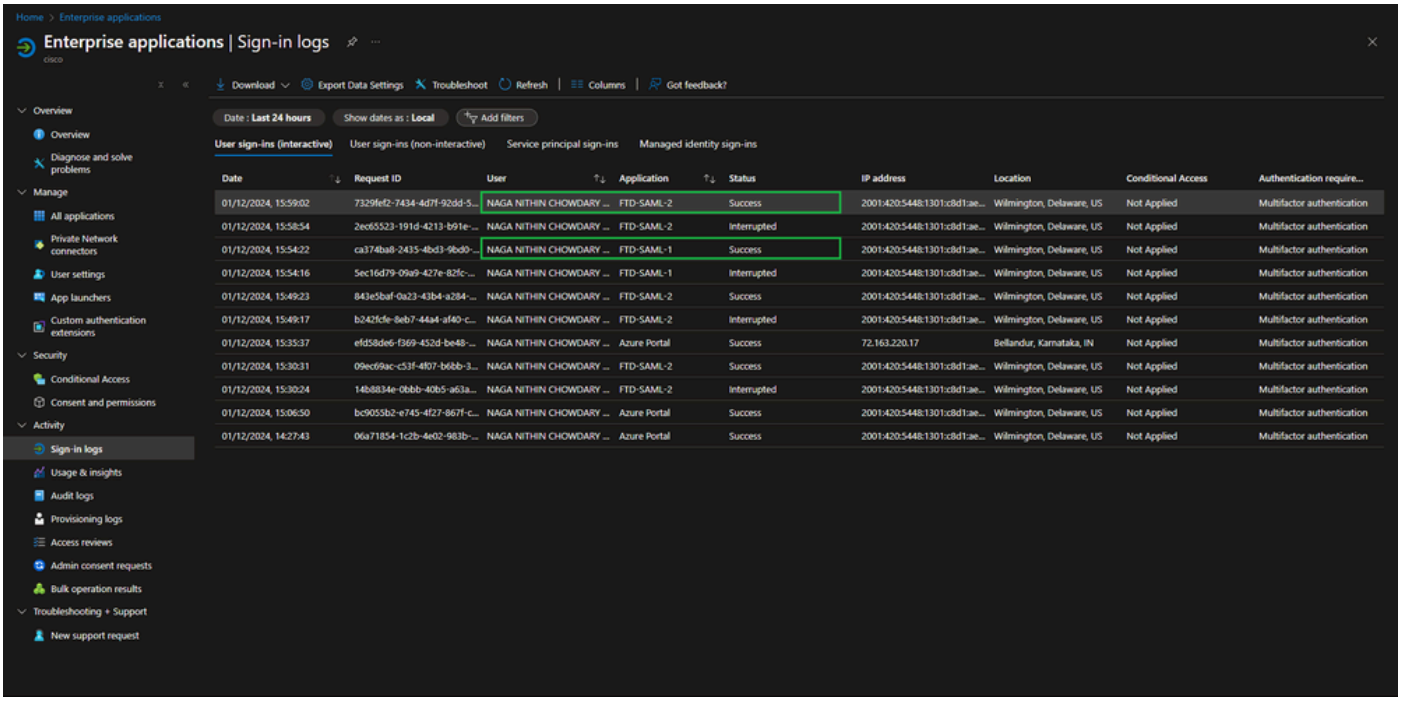
```
firepower# sh run tunnel-group FTD-SAML-2
tunnel-group FTD-SAML-2 type remote-access
tunnel-group FTD-SAML-2 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-2-gp
tunnel-group FTD-SAML-2 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-2 enable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


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


firepower#
```

Azureエントリ識別子からのサインインログ

エンタープライズアプリケーションのサインインログセクションにアクセスします。FTD-SAML-1やFTD-SAML-2などの特定の接続プロファイルに関連する認証要求を探します。ユーザが、各接続プロファイルに関連付けられたSAMLアプリケーションを介して正常に認証されていることを確認します。



Azure IdPのサインインログ

トラブルシュート

1. Secure ClientユーザPCからDARTを使用してトラブルシューティングを行うことができます。
2. SAML認証の問題をトラブルシューティングするには、次のデバッグを使用します。

<#root>

firepower#

debug webvpn saml 255

3. 前述のように、セキュアクライアントの設定を確認します。このコマンドは、証明書の確認に使用できます。

<#root>

firepower#

show crypto ca certificate

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。