

FDM 7.2以下で管理されるFTDでAzure as IdPを使用してSAML認証を使用するRAVPNを設定する

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](#)

[設定](#)

[ステップ 1: 「Basic Constraints: CA:TRUE」拡張を使用した証明書署名要求\(CSR\)の作成](#)

[ステップ 2: PKCS12ファイルの作成](#)

[ステップ 3: PKCS#12証明書をAzureとFDMにアップロードします](#)

[Azureへの証明書のアップロード](#)

[証明書のFDMへのアップロード](#)

[確認](#)

はじめに

このドキュメントでは、FDMバージョン7.2以下で管理されるFTDでAzure as IdPを使用してリモートアクセスVPNのSAML認証を設定する方法について説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- Secure Socket Layer(SSL)証明書
- OpenSSL
- Linuxコマンド
- リモートアクセス仮想プライベートネットワーク(RAVPN)
- Secure Firewall Device Manager(FDM)
- Security Assertion Markup Language(SAML)
- Microsoft Azure

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- OpenSSLバージョンCiscoSSL 1.1.1j.7.2sp.230
- Secure Firewall Threat Defense(FTD)バージョン7.2.0
- Secure Firewall Device Managerバージョン7.2.0
- 内部認証局(CA)


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

RAVPN接続およびその他の多くのアプリケーションに対するSAML認証の使用は、その利点のために最近ますます普及しています。SAMLは、認証および許可情報をパーティ、特にアイデンティティプロバイダー(IdP)とサービスプロバイダー(SP)の間で交換するためのオープンスタンダードです。

SAML認証用にサポートされているIdPがDuoのみである場合、FDMバージョン7.2.x以下で管理されるFTDには制限があります。これらのバージョンでは、SAML認証に使用する証明書をFDMにアップロードする際に、Basic Constraints: CA:TRUEという拡張子を付ける必要があります。

このため、SAML認証用のMicrosoft Azureなどの他のIdPs(必要な拡張子を持たない)によって提供された証明書はこれらのバージョンでネイティブにサポートされていないため、SAML認証が失敗する原因になります。

 注:FDMバージョン7.3.x以降では、新しい証明書をアップロードするときに「CAチェックをスキップする」オプションを有効にできます。これにより、このドキュメントで説明されている制限が解決されます。

Basic Constraints: CA:TRUE拡張がないAzureから提供される証明書を使用してSAML認証でRAVPNを設定する場合、`show saml metadata <trustpoint name>`コマンドを実行してFTDコマンドラインインターフェイス(CLI)からメタデータを取得すると、出力は空白になります。次に出力を示します。

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

```
SP Metadata
```

```
-----
```

```
IdP Metadata
```

設定

この制限を解決するために推奨されるプランは、セキュアファイアウォールをバージョン7.3以降にアップグレードすることです。ただし、ファイアウォールでバージョン7.2以下を実行する必要がある場合は、Basic Constraints: CA:TRUE拡張を含むカスタム証明書を作成することで、この制限を回避できます。証明書がカスタムCAによって署名された後、このカスタム証明書を代わりに使用するには、Azure SAML構成ポータル構成を変更する必要があります。

ステップ 1 : 「Basic Constraints: CA:TRUE」拡張を使用した証明書署名要求 (CSR)の作成

このセクションでは、OpenSSLを使用してCSRを作成し、Basic Constraints: CA:TRUE Extensionを含める方法について説明します。

1. OpenSSLライブラリがインストールされているエンドポイントにログインします。
2. (オプション) mkdir <folder name>コマンドを使用して、この証明書に必要なファイルを配置できるディレクトリを作成します。

```
<#root>
```

```
root@host1:/home/admin#
```


```
mkdir certificate
```

- 3.新しいディレクトリを作成した場合は、ディレクトリをそのディレクトリに変更し、openssl genrsa -out <key_name>.key 4096コマンドを実行して新しい秘密キーを生成します。

```
<#root>
```

```
root@host1:/home/admin/certificate#
```

```
openssl genrsa -out privatekey.key 4096
```

 注:4096ビットは、この設定例のキー長を表します。必要に応じて、長いキーを指定できます。

4. touch <config_name>.confコマンドを使用して、コンフィギュレーションファイルを作成します。

- 5.テキストエディタでファイルを編集します。この例では、Vimが使用され、vim

<config_name>.confコマンドが実行されます。その他のテキストエディタを使用できます。

<#root>

```
vim config.conf
```

6.証明書署名要求(CSR)に含める情報を入力します。次に示すように、ファイルにbasicConstraints = CA:true拡張子を追加します。

<#root>

```
[ req ]
```

```
default_bits = 4096
```

```
default_md = sha256
```

```
prompt = no
```

```
encrypt_key = no
```

```
distinguished_name = req_distinguished_name
```

```
req_extensions = v3_req
```

```
[ req_distinguished_name ]
```

```
countryName =
```

```
stateOrProvinceName =
```

localityName =


organizationName =

organizationalUnitName =

commonName =

[v3_req]

basicConstraints = CA:true

 注:basicConstraints = CA:trueは、FTDが証明書を正常にインストールするために証明書に必要な内線番号です。

7.前の手順で作成したキーとコンフィギュレーションファイルを使用して、`openssl req -new <key_name>.key -config <conf_name>.conf -out <CSR_Name>.csr`コマンドでCSRを作成できます。

<#root>


```
openssl req -new -key privatekey.key -config config.conf -out CSR.csr
```

8.このコマンドの実行後、フォルダに<CSR_name>.csrファイルが表示されます。このファイルは、署名するCAサーバに送信する必要があるCSRファイルです。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDbXR5
MRQwEgYDVQQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITckD5VJa6KRssDJ8
[...]

Output Omitted

[...]
1RZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JsPkvJmRpKSi1c7w
3rKfTXe1ewT1IJdCmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLgJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

 注:Azureの要件により、SHA-256またはSHA-1が設定されたCAでCSRに署名する必要があります。そうしないと、アップロード時にAzure IdPが証明書を拒否します。詳細については、次のリンクを参照してください。[SAMLトークンの高度な証明書署名オプション](#)

9.このCSRファイルをCAに送信して、署名付き証明書を取得します。

ステップ 2 : PKCS12ファイルの作成

ID証明書が署名されたら、次の3つのファイルを使用してPublic-Key Cryptography Standards(PKCS#12)ファイルを作成する必要があります。

- 署名付きID証明書
- 秘密キー (前の手順で定義)
- CA証明書チェーン

ID証明書とCA証明書チェーンは、秘密キーとCSRファイルを作成したのと同じデバイスにコピーできます。3つのファイルが作成されたら、`openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx`コマンドを実行して、証明書をPKCS#12に変換します。

<#root>

```
openssl pkcs12 -export -in id.cer -certfile ca_chain.cer -inkey privatekey.key -out cert.pfx
```

コマンドを実行すると、パスワードの入力を求められます。このパスワードは、証明書をインストールするときに必要です。

コマンドが正常に実行されると、「<pkcs12_name>.pfx」という名前の新しいファイルが現在のディレクトリに作成されます。これが新しいPKCS#12証明書です。

ステップ 3 : PKCS#12証明書をAzureとFDMにアップロードします

PKCS#12ファイルを作成したら、AzureとFDMにアップロードする必要があります。

Azureへの証明書のアップロード

1. Azureポータルにログインし、SAML認証で保護するエンタープライズアプリケーションに移動して、[シングルサインオン]を選択します。
2. SAML Certificatesセクションまでスクロールし、More Optionsアイコン> Editを選択します。

3

SAML Certificates

Token signing certificate ...

Status	Active
Thumbprint	99 [redacted]
Expiration	12/19/2026, 1:25:53 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted] ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) ...

Required	No
Active	0
Expired	0

3.次に、Import certificateオプションを選択します。

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	12/19/2026, 1:25:53 PM	99 [redacted]	...

4.以前に作成したPKCS12ファイルを検索し、PKCS#12ファイルの作成時に入力したパスワードを使用します。


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?

Import certificate

Upload a certificate with the private key and the pfx credentials, the type of this file should be .pfx and using RSA for the encryption algorithm

Certificate: 

PFX Password:  

Add

Cancel

5.最後に、Make Certificate Activeオプションを選択します。

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	12/19/2026, 1:25:53 PM	99...	...
Inactive	12/13/2026, 2:43:39 PM	E6...	...
Inactive	12/21/2026, 5:58:45 PM	9E...	...

Signing Option

Signing Algorithm


Notification Email Addresses

 Make certificate active

 Base64 certificate download

 PEM certificate download

 Raw certificate download

 Download federated certificate XML

 Delete Certificate

証明書のFDMへのアップロード

1. Objects > Certificatesの順に移動し、Add Trusted CA certificateをクリックします。

https://login.microsoftonline.com/

Supported protocols: https, http

Sign Out URL

https://login.microsoftonline.com/

Supported protocols: https, http

Service Provider Certificate

ftdSAML

Identity Provider Certificate

azureIDP

Request Signature

None

Request Timeout ⓘ

Range: 1 - 7200 (sec)

This SAML identity provider (IDP) is on an internal network

Request IDP re-authentication at login ⓘ

CANCEL

OK

確認

show saml metadata <trustpoint name>コマンドを実行して、FTD CLIからメタデータを使用できることを確認します。

```
<#root>
```

```
firepower#
```

```
show saml metadata azure
```

```
SP Metadata
```

```
-----
```

xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

MIIDbzCCA1egAwIBAgIBDDANBgkqhkiG9w0BAQwFADBbMQwwCgYDVQQLEwN2cG4x

...omitted...

HGaq+/IfNKKqkhgT6q4egqMHiA==

Location="https://[...omitted...]/+CSCOE+/saml/sp/logout"/>

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://[...omitted...]/+CSCOE+/saml/sp/logout"/>

IdP Metadata

xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

MIIEcjCCA1qgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBbMQwwCgYDVQQLEwN2cG4x

[...omitted...]

3Zmzsc5faZ8dMX0+1ofQVvMaPifcZZFoM7oB09RK2PaMwIAV+Mw=

Location="https://login.microsoftonline.com/[...omitted...]/saml2" />

Location="https://login.microsoftonline.com/[...omitted...]/saml2" />

```
Location="https://login.microsoftonline.com/[...omitted...]/saml2" />
```


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。