

FDMでのSAML認証による複数のRAVPNプロファイルの設定

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](#)

[設定](#)

[ステップ1:OpenSSLを使用した自己署名証明書およびPKCS#12ファイルの作成](#)

[手順2: AzureとFDMにPKCS#12ファイルをアップロードします](#)

[ステップ 2.1 : Azureへの証明書のアップロード](#)

[ステップ 2.2 : 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を介してCSFでAzure as IdPを使用して、リモートアクセスVPNの複数の接続プロファイルに対して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
- リモートアクセス仮想プライベートネットワーク(RAVPN)
- Cisco 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
- Cisco Secure Firewall(CSF)バージョン7.4.1
- Cisco Secure Firewall Device Managerバージョン7.4.1

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

SAML(Security Assertion Markup Language)は、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))間で認証および認可情報を交換するためのオープンスタンダードです。リモートアクセスVPN(RAVPN)接続およびその他のさまざまなアプリケーションに対するSAML認証の使用は、数多くの利点があるため、ますます普及しています。Firepower Management Center(FMC)では、複数の接続プロファイルで異なるIdPで保護されたアプリケーションを使用するように設定できます。これは、接続プロファイルの設定メニューにあるOverride Identity Provider Certificateオプションが有効なためです。この機能を使用すると、管理者は、接続プロファイルごとに特定のIdP証明書を使用して、シングルサインオン(SSO)サーバオブジェクトのプライマリIdP証明書を上書きできます。ただし、Firepower Device Manager(FDM)では同様のオプションが提供されないため、この機能は制限されます。2つ目のSAMLオブジェクトが設定されている場合、最初の接続プロファイルに接続しようとするすると認証エラーが発生し、「シングルサインオンCookieの取得中に問題が発生したため、認証に失敗しました。」というエラーメッセージが表示されます。この制限を回避するために、カスタムの自己署名証明書を作成してAzureにインポートし、すべてのアプリケーションで使用できます。これにより、FDMにインストールする必要がある証明書は1つだけになり、複数のアプリケーションに対するシームレスなSAML認証が可能になります。

設定

ステップ1:OpenSSLを使用した自己署名証明書およびPKCS#12ファイルの作成

ここでは、OpenSSLを使用して自己署名証明書を作成す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。

注：このドキュメントでは、Linuxマシンが使用されているため、一部のコマンドはLinux環境に固有です。ただし、OpenSSLコマンドは同じです。

b. touch

.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。

<#root>

root@host#

```
touch config.conf
```

c. 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

.conf

コマンドが実行されます。他のテキストエディタも使用できます。

<#root>

root@host#

vim config.conf

d.自己署名に含める情報を入力します。

< >の間の値は、必ず組織の情報で置き換えてください。

[req]

distinguished_name = req_distinguished_name

prompt = no

[req_distinguished_name]

C =

ST =

L =

O =

OU =

CN =

e.このコマンドを使用すると、

.conf

ファイルで指定された設定に基づいて、3650日間有効なSHA-256アルゴリズムを使用する、新しい2048ビットRSA秘密キーと自己署名証明書が生成されます。秘密キーは

.pem

に保存され、自己署名証明書は

.cert

に保存されます。

<#root>

root@host#

```
openssl req -newkey rsa:2048 -nodes -keyout
```

```
.pem -x509 -sha256 -days 3650 -config
```

```
.conf -out
```

.crt

```
root@host:~# openssl req -newkey rsa:2048 -nodes -keyout Azure_key.pem -x509 -sha256 -days 3650 -config config.conf -out Azure_SSO.crt
Generating a RSA private key
.....+++++
writing new private key to 'Azure_key.pem'
.....+++++
root@host:~#
```

f.秘密キーと自己署名証明書を作成した後、それらをPKCS#12ファイルにエクスポートします。
これは、秘密キーと証明書の両方を含めることができる形式です。

<#root>

root@host#

openssl pkcs12 -export -inkey

.pem -in

.crt -name

-out

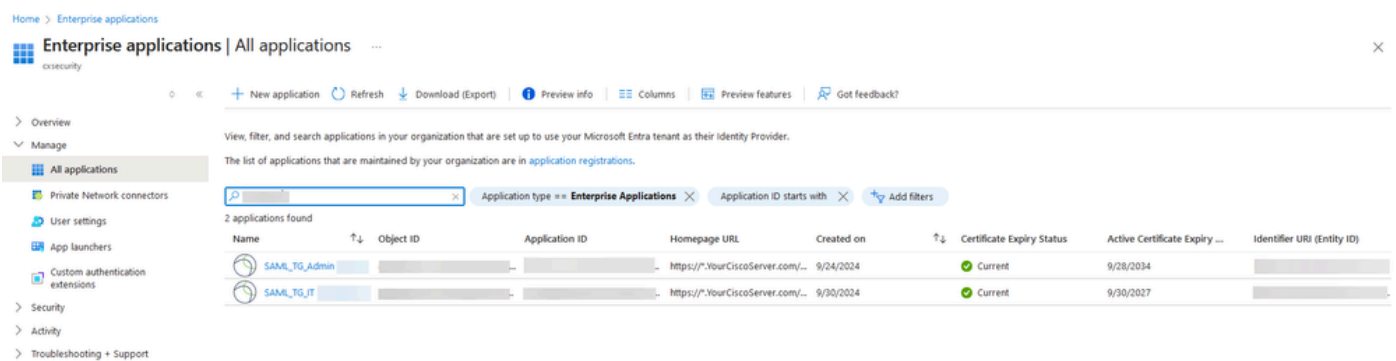
.pfx

```
root@host:~# openssl pkcs12 -export -inkey Azure_key.pem -in Azure_SSO.crt -out Azure_SSO.pfx
Enter Export Password:
Verifying - Enter Export Password:
root@host:~#
root@host:~# ls
Azure_SSO.crt Azure_SSO.pfx Azure_key.pem config.conf
```

パスワードを書き留めます。

手順2: AzureとFDMにPKCS#12ファイルをアップロードします

FDMでSAML認証を使用する接続プロファイルごとに、Azureにアプリケーションを作成してください。



The screenshot shows the Azure Enterprise Applications management console. The page title is "Enterprise applications | All applications". The left sidebar contains navigation options: Overview, Manage, All applications (selected), Private Network connectors, User settings, App launchers, Custom authentication extensions, Security, Activity, and Troubleshooting + Support. The main content area displays a table of applications with the following columns: Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expiry Status, Active Certificate Expiry, and Identifier URI (Entity ID). Two applications are listed:

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry	Identifier URI (Entity ID)
SAML_TG_Admin			https://*.YourCiscoServer.com/...	9/24/2024	Current	9/28/2034	
SAML_TG_IT			https://*.YourCiscoServer.com/...	9/30/2024	Current	9/30/2027	


「手順1:OpenSSLを使用して自己署名証明書とPKCS#12ファイルを作成する」からのPKCS#12ファイルを取得したら、複数のアプリケーション用にAzureにアップロードし、FDM SSO構成で設定する必要があります。


ステップ 2.1 : Azureへの証明書のアップロード


a. 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。

b. SAML Certificates セクションまでスクロールダウンして、More Options > Editの順に選択します。

SAML Certificates

Token signing certificate  Edit

Status	Active
Thumbprint	[Redacted]
Expiration	9/28/2034, 1:05:19 PM
Notification Email	[Redacted]
App Federation Metadata Url	https://login.microsoftonline.com/ 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)  Edit

Required	No
Active	0
Expired	0

c.ここで、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	8/25/2029, 7:03:32 PM	[Redacted]	...


Signing Option Sign SAML assertion ▼

Signing Algorithm SHA-256 ▼

d.以前に作成したPKCS#12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。

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

e.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?

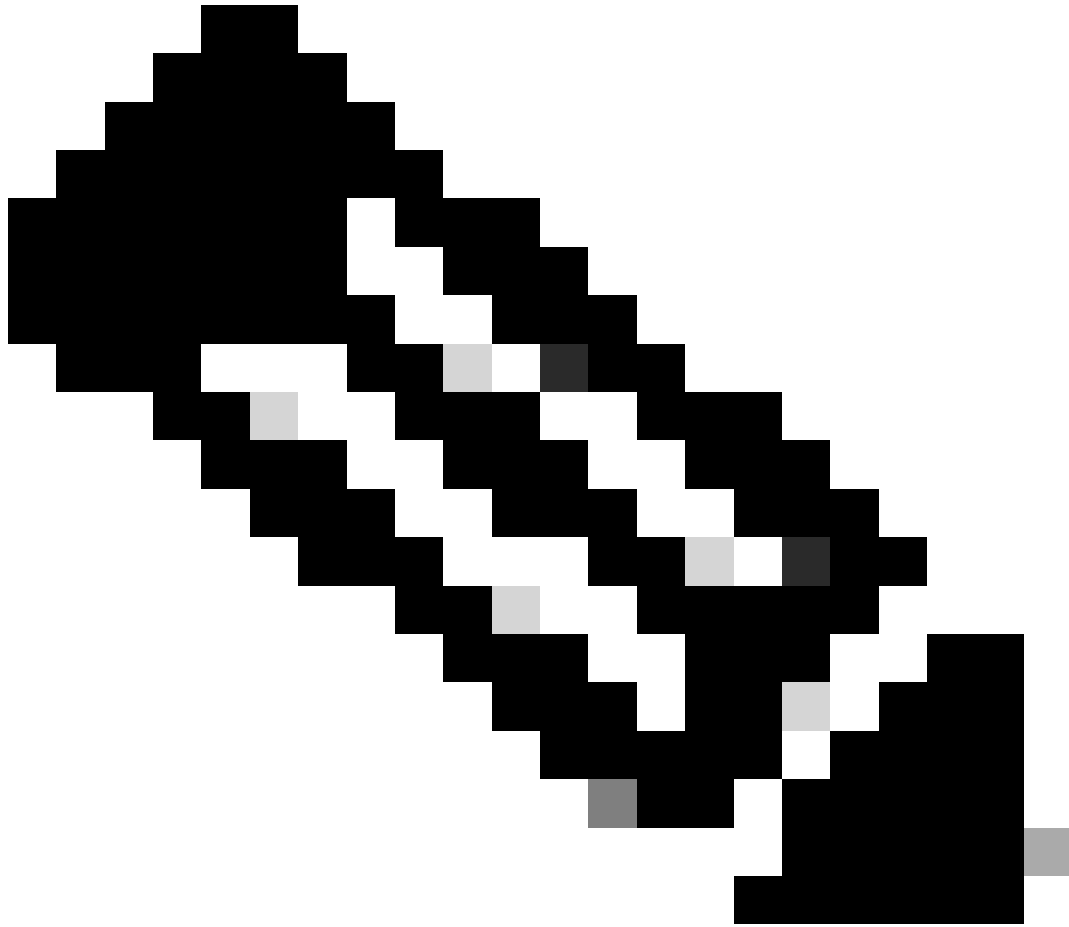
Status	Expiration Date	Thumbprint	
Inactive	9/28/2034, 1:05:19 PM	[Redacted]	⋮
Active	9/27/2027, 5:51:21 PM	[Redacted]	⋮

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



注:各アプリケーションに対して、「ステップ2.1：証明書をAzureにアップロードする」を必ず実行してください。

ステップ 2.2 : 証明書のFDMへのアップロード

a. **Objects > Certificates > Click Add Trusted CA certificate**に移動します。

Edit SAML Server



Name

AzureIDP

Description

Identity Provider (IDP) Entity ID URL

https://

Sign In URL

https://

Supported protocols: https, http

Sign Out URL

https://

Supported protocols: https, http

Service Provider Certificate

(Validation Us...

Identity Provider Certificate

Azure_SSO (Validation Usage: ...

Request Signature

None

Request Timeout

Range: 1 - 7200 (sec)

d. SAMLオブジェクトを、SAMLを認証方法として使用し、Azureでアプリケーションが作成された別の接続プロファイルに設定します。変更を展開します

Device Summary

Remote Access VPN Connection Profiles

2 connection profiles

Filter



#	NAME	AAA	GROUP POLICY	ACTIONS
1	SAML_TG_Admin	Authentication: SAML Authorization: None Accounting: None	SAML_GP_Admin	
2	SAML_TG_IT	Authentication: SAML Authorization: None Accounting: None	SAML_GP_IT	

Primary Identity Source

Authentication Type

SAML



SAML Login Experience

VPN client embedded browser

Default OS browser

Primary Identity Source for User Authentication

AzureIDP



確認

show running-config webvpnコマンドと show running-config tunnel-groupコマンドを実行して設定をレビューし、同じIDP URLが異なる接続プロファイルで設定されていることを確認します。

```
<#root>
```

```
firepower#
```

```
show running-confuting 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
```

```
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.10.08029-webdeploy-k9.pkg 2
```

anyconnect profiles defaultClientProfile disk0:/anyconncprofs/defaultClientProfile.xml
anyconnect enable

saml idp https://saml.lab.local/af42bac0

/

url sign-in https://login.saml.lab.local/af42bac0

/saml2

url sign-out https://login.saml.lab.local/af42bac0

/saml2

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

trustpoint idp

Azure_SSO

```
trustpoint sp FWCertificate
```

```
no signature
```

```
force re-authentication
```

```
tunnel-group-list enable
```

```
cache
```

```
disable
```

```
error-recovery disable
```

```
firepower#
```

```
<#root>
```

```
firepower#
```

```
show running-config tunnel-group
```

```
tunnel-group SAML_TG_Admin type remote-access
```

```
tunnel-group SAML_TG_Admin general-attributes
```

```
address-pool Admin_Pool
```

```
default-group-policy SAML_GP_Admin
```

```
tunnel-group SAML_TG_Admin webvpn-attributes
```

```
authentication saml
```

```
group-alias SAML_TG_Admin enable
```

```
saml identity-provider https://saml.lab.local/af42bac0
```

/

```
tunnel-group SAML_TG_IT type remote-access
tunnel-group SAML_TG_IT general-attributes
  address-pool IT_Pool
  default-group-policy SAML_GP_IT
tunnel-group SAML_TG_IT webvpn-attributes
```

```
  authentication saml
```

```
group-alias SAML_TG_IT enable
```

```
saml identity-provider https://saml.lab.local/af42bac0
```

/

```
firepower#
```


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。