

Configurer RAVPN avec authentification SAML en utilisant Azure comme IdP sur FTD géré par FDM 7.2 et versions antérieures

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Étape 1. Créer une demande de signature de certificat \(CSR\) avec l'extension « Contraintes de base : CA : TRUE »](#)

[Étape 2. Créer un fichier PKCS12](#)

[Étape 3. Téléchargez le certificat PKCS#12 sur Azure et sur FDM](#)

[Télécharger le certificat sur Azure](#)

[Télécharger le certificat sur le FDM](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer l'authentification SAML pour le VPN d'accès à distance en utilisant Azure comme IdP sur FTD géré par FDM version 7.2 ou inférieure.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats SSL (Secure Socket Layer)
- OpenSSL
- Commandes Linux
- Réseau privé virtuel d'accès à distance (RAVPN)
- Gestionnaire de périphériques de pare-feu sécurisé (FDM)
- SAML (Security Assertion Markup Language)
- Microsoft Azure

Composants utilisés

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

- OpenSSL Version CiscoSSL 1.1.1j.7.2sp.230
- Protection pare-feu contre les menaces (FTD) version 7.2.0
- Gestionnaire de périphériques Secure Firewall Version 7.2.0
- Autorité de certification interne (CA)


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

L'utilisation de l'authentification SAML pour les connexions RAVPN et de nombreuses autres applications est devenue plus populaire ces derniers temps en raison de ses avantages. SAML est une norme ouverte d'échange d'informations d'authentification et d'autorisation entre des parties, en particulier un fournisseur d'identité (IdP) et un fournisseur de services (SP).

Il y a une limitation dans FTD géré par FDM versions 7.2.x ou inférieures où le seul IdP pris en charge pour l'authentification SAML est Duo. Dans ces versions, les certificats à utiliser pour l'authentification SAML doivent avoir l'extension Basic Constraints: CA:TRUE lors de leur téléchargement vers le FDM.

Pour cette raison, les certificats fournis par d'autres IdP (qui n'ont pas l'extension requise) comme Microsoft Azure pour l'authentification SAML ne sont nativement pas pris en charge dans ces versions, ce qui entraîne l'échec de l'authentification SAML.

 Remarque : les versions 7.3.x et ultérieures de FDM permettent d'activer l'option Ignorer la vérification de l'autorité de certification lors du téléchargement d'un nouveau certificat. Ceci résout la limitation décrite dans ce document.

Si vous configurez RAVPN avec l'authentification SAML à l'aide du certificat fourni par Azure et qui n'a pas l'extension Basic Constraints: CA:TRUE, lorsque vous exécutez la commande `show saml metadata <trustpoint name>` pour récupérer les métadonnées à partir de l'interface de ligne de commande FTD (CLI), le résultat est vide comme indiqué ci-dessous :

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

```
SP Metadata
```

```
-----
```

```
IdP Metadata
```

Configurer

Le plan suggéré pour résoudre cette limitation est de mettre à niveau le pare-feu sécurisé vers la version 7.3 ou supérieure, cependant, si pour une raison quelconque vous avez besoin du pare-feu pour exécuter la version 7.2 ou inférieure, vous pouvez contourner cette limitation en créant un certificat personnalisé qui inclut l'extension Contraintes de base : CA:TRUE. Une fois le certificat signé par une autorité de certification personnalisée, vous devez modifier la configuration dans le portail de configuration Azure SAML pour qu'il utilise ce certificat personnalisé à la place.

Étape 1. Créer une demande de signature de certificat (CSR) avec l'extension « Contraintes de base : CA : TRUE »

Cette section décrit comment créer un CSR à l'aide d'OpenSSL pour qu'il inclue les contraintes de base : CA:TRUE Extension.

1. Connectez-vous à un terminal sur lequel la bibliothèque OpenSSL est installée.
2. (Facultatif) Créez un répertoire dans lequel vous pouvez localiser les fichiers nécessaires à ce certificat à l'aide de la commande `mkdir <nom du dossier>`.

<#root>

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

```
mkdir certificate
```

3. Si vous avez créé un nouveau répertoire, accédez-y et générez une nouvelle clé privée en exécutant la commande `openssl genrsa -out <key_name>.key 4096`.

<#root>

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

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



Remarque : 4 096 bits représente la longueur de clé pour cet exemple de configuration. Vous pouvez spécifier une clé plus longue si nécessaire.

4. Créez un fichier de configuration à l'aide de la commande `touch <config_name>.conf`.
5. Modifiez le fichier avec un éditeur de texte. Dans cet exemple, Vim est utilisé et la commande

vim <config_name>.conf est exécutée. Vous pouvez utiliser tout autre éditeur de texte.

```
<#root>
```

```
vim config.conf
```

6. Saisissez les informations à inclure dans la demande de signature de certificat (CSR). Assurez-vous d'ajouter l'extension basicConstraints = CA : true dans le fichier comme indiqué ci-dessous :

```
<#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

 Remarque : basicConstraints = CA:true est l'extension que le certificat doit avoir pour que le FTD puisse installer le certificat.

7. À l'aide de la clé et du fichier de configuration créés lors des étapes précédentes, vous pouvez créer le CSR à l'aide de la commande `openssl req -new <key_name>.key -config <conf_name>.conf -out <CSR_Name>.csr` :

<#root>


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

8. Après cette commande, vous pouvez voir votre fichier <CSR_name>.csr répertorié dans le dossier, qui est le fichier CSR qui doit être envoyé au serveur AC pour être signé.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDaXR5
MRQwEgYDVQQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITckD5VJa6KRssDJ8
[...]
```

Output Omitted

```
[...]
1RZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JsPkvJmRpKSi1c7w
3rKfTXe1ewT1IJdCmgrp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

 Remarque : en raison des conditions requises Azure, il est nécessaire de signer le CSR avec une autorité de certification dont SHA-256 ou SHA-1 est configuré. Dans le cas contraire, l'IdP Azure rejette le certificat lorsque vous le téléchargez. Pour plus d'informations, consultez le lien suivant : [Options avancées de signature de certificat dans un jeton SAML](#)

9. Envoyez ce fichier CSR à votre autorité de certification pour obtenir le certificat signé.

Étape 2. Créer un fichier PKCS12

Une fois le certificat d'identité signé, vous devez créer le fichier Public-Key Cryptography Standards (PKCS#12) avec les 3 fichiers suivants :

- Certificat d'identité signé

- Clé privée (définie dans les étapes précédentes)
- Chaîne de certificats CA

Vous pouvez copier le certificat d'identité et la chaîne de certificats d'autorité de certification sur le même périphérique que celui sur lequel vous avez créé la clé privée et le fichier CSR. Une fois que vous avez les 3 fichiers, exécutez la commande `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx` pour convertir le certificat en PKCS#12.

<#root>

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

Après avoir exécuté la commande, vous êtes invité à saisir un mot de passe. Ce mot de passe est nécessaire lorsque vous installez le certificat.

Si la commande a réussi, un nouveau fichier nommé « <pkcs12_name>.pfx » est créé dans le répertoire actif. Ceci est votre nouveau certificat PKCS#12.

Étape 3. Téléchargez le certificat PKCS#12 sur Azure et sur FDM

Une fois que vous avez le fichier PKCS#12, vous devez le télécharger sur Azure et sur le FDM.

Télécharger le certificat sur Azure

1. Connectez-vous à votre portail Azure, accédez à l'application Entreprise que vous souhaitez protéger avec l'authentification SAML et sélectionnez Authentification unique.
2. Faites défiler jusqu'à la section Certificats SAML et sélectionnez l'icône Plus d'options > Modifier.

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. Sélectionnez maintenant l'option Importer un certificat.

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. Recherchez le fichier PKCS12 précédemment créé et utilisez le mot de passe que vous avez entré lors de la création du fichier PKCS#12.

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. Enfin, sélectionnez l'option Make Certificate Active.

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

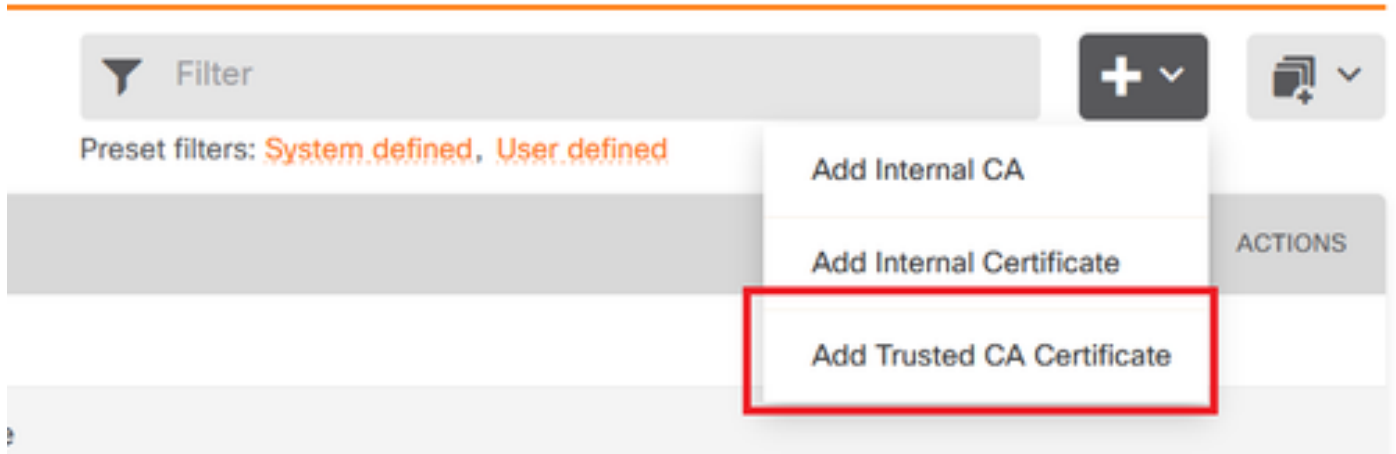
 Raw certificate download

 Download federated certificate XML

 Delete Certificate

Télécharger le certificat sur le FDM

1. Accédez à Objets > Certificats > Cliquez sur Ajouter un certificat CA de confiance.



2. Entrez le nom du point de confiance que vous préférez et téléchargez uniquement le certificat d'identité à partir du fournisseur d'identité (et non le fichier PKCS#12)

Add Trusted CA Certificate

Name

azureIDP

Certificate No file uploaded yet

Paste certificate, or choose a file (DER, PEM, CRT, CER) [Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----
MIIEcjCCA1ggAwIBAgIBFzANBgkqhkiG9w0BAQsFADBBMQwwCgYDVQQLEwN2cG4x
DjAMBgNVBAoTBWVpc2NvMQwwCgYDVQQHEwNtZXApc000AKBghNVBAgTA21leDELMAkG
A1UdEw0wCgYDVQQLAQ0wCgYDVQQLAQ0wCgYDVQQLAQ0wCgYDVQQLAQ0wCgYDVQQLAQ0w
-----
```

Validation Usage for Special Services

Please select

CANCEL OK

3. Définissez le nouveau certificat dans l'objet SAML et déployez les modifications.

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

Vérifier

Exécutez la commande `show saml metadata <trustpoint name>` pour vous assurer que les métadonnées sont disponibles à partir de l'interface de ligne de commande FTD :

```
<#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...]/sam12" />

Location="https://login.microsoftonline.com/[...omitted...]/sam12" />

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


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.