

Configuration de plusieurs profils RAVPN avec authentification SAML sur FDM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Étape 1 : Créez un certificat auto-signé et un fichier PKCS#12 à l'aide d'OpenSSL](#)

[Étape 2 : Téléchargez le fichier PKCS#12 sur Azure et FDM](#)

[Étape 2.1. Télécharger le certificat sur Azure](#)

[Étape 2.2. Télécharger le certificat sur le FDM](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer l'authentification SAML pour plusieurs profils de connexion de VPN d'accès à distance en utilisant Azure comme IdP sur CSF via FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats SSL (Secure Socket Layer)
- OpenSSL
- Réseau privé virtuel d'accès à distance (RAVPN)
- Cisco Secure Firewall Device Manager (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
- Cisco Secure Firewall (CSF) version 7.4.1
- Gestionnaire de périphériques Cisco Secure Firewall Version 7.4.1

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

Le langage SAML (Security Assertion Markup Language) est une norme ouverte d'échange d'informations d'authentification et d'autorisation entre les parties, en particulier un fournisseur d'identité (IdP) et un fournisseur de services (SP). L'utilisation de l'authentification SAML pour les connexions VPN d'accès à distance (RAVPN) et diverses autres applications est devenue de plus en plus populaire en raison de ses nombreux avantages. Sur le Centre de gestion Firepower (FMC), plusieurs profils de connexion peuvent être configurés pour utiliser différentes applications protégées par un fournisseur d'identité en raison de l'option Remplacer le certificat du fournisseur d'identité disponible dans le menu de configuration Profil de connexion. Cette fonctionnalité permet aux administrateurs de remplacer le certificat du fournisseur d'identité principal dans l'objet de serveur SSO (Single Sign-On) par un certificat de fournisseur d'identité spécifique pour chaque profil de connexion. Cependant, cette fonctionnalité est limitée sur le Gestionnaire de périphériques Firepower (FDM), car elle ne fournit pas d'option similaire. Si un deuxième objet SAML est configuré, toute tentative de connexion au premier profil de connexion entraîne un échec d'authentification et affiche le message d'erreur suivant : "L'authentification a échoué en raison d'un problème de récupération du cookie d'authentification unique." Pour contourner cette limitation, un certificat auto-signé personnalisé peut être créé et importé dans Azure pour être utilisé dans toutes les applications. Ainsi, un seul certificat doit être installé dans le FDM, ce qui permet une authentification SAML transparente pour plusieurs applications.

Configurer

Étape 1 : Créez un certificat auto-signé et un fichier PKCS#12 à l'aide d'OpenSSL

Cette section décrit comment créer le certificat auto-signé à l'aide d'OpenSSL

1. Connectez-vous à un terminal sur lequel la bibliothèque OpenSSL est installée.



Remarque : dans ce document, une machine Linux est utilisée, de sorte que certaines commandes sont spécifiques à un environnement Linux. Cependant, les commandes OpenSSL sont identiques.

b. Créez un fichier de configuration à l'aide de la commande `touch`

```
.conf
.  
  
<#root>  
root@host#  
touch config.conf
```

c. Modifiez le fichier avec un éditeur de texte. Dans cet exemple, Vim est utilisé et la `vim`

.conf

commande est exécutée. Vous pouvez utiliser tout autre éditeur de texte.

<#root>

root@host#

vim config.conf

d. Saisissez les informations à inclure dans l'auto-signature.

Veillez à remplacer les valeurs entre < > par les informations de votre organisation.

[req]

distinguished_name = req_distinguished_name

prompt = no

[req_distinguished_name]

C =

ST =

L =

O =

OU =

CN =

e. L'utilisation de cette commande génère une nouvelle clé privée RSA 2 048 bits et un certificat auto-signé à l'aide de l'algorithme SHA-256, valide pendant 3 650 jours, en fonction de la configuration spécifiée dans le

`.conf`

fichier. La clé privée est enregistrée dans

`.pem`

et le certificat auto-signé dans

`.cert`

.

<#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_ss0.crt
Generating a RSA private key
.....+++++
writing new private key to 'Azure_key.pem'
-----
root@host:~#
```

f. Après avoir créé la clé privée et le certificat auto-signé, il les exporte dans un fichier PKCS#12, qui est un format pouvant inclure à la fois la clé privée et le certificat.

<#root>

root@host#

```
openssl pkcs12 -export -inkey
```

.pem -in

.crt -name

-out

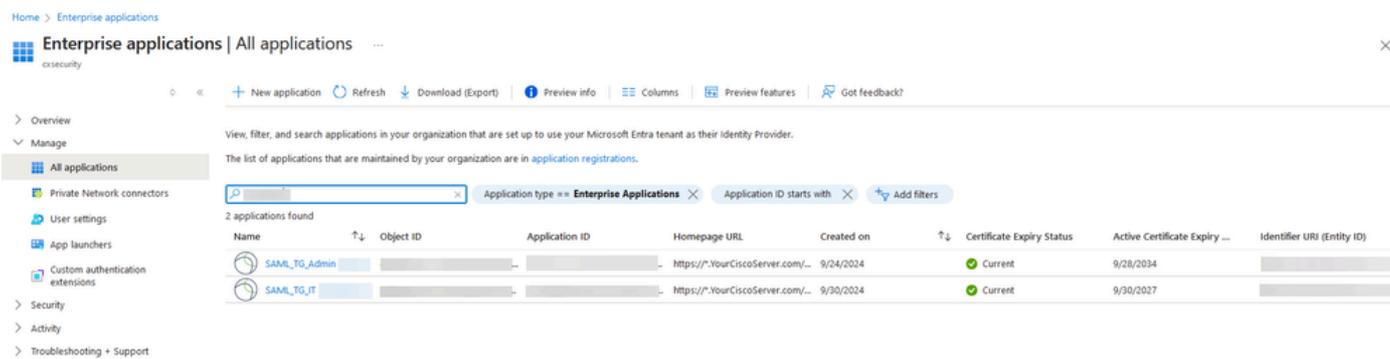
.pfx

```
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
```

Prenez note du mot de passe.

Étape 2 : Téléchargez le fichier PKCS#12 sur Azure et FDM

Assurez-vous de créer une application sur Azure pour chaque profil de connexion qui utilise l'authentification SAML sur FDM.



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: SAML_TG_Admin and SAML_TG_IT, both with a status of "Current".

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	

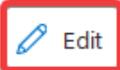
Une fois que vous avez le fichier PKCS#12 de l'étape 1 : Créer un certificat auto-signé et le fichier PKCS#12 à l'aide d'OpenSSL, il doit être téléchargé vers Azure pour plusieurs applications et configuré dans la configuration FDM SSO.

Étape 2.1. Télécharger le certificat sur Azure

a. Connectez-vous à votre portail Azure, accédez à l'application Entreprise que vous souhaitez protéger avec l'authentification SAML et sélectionnez Authentification unique.

b. Faites défiler jusqu'à la section Certificats SAML et sélectionnez Plus d'options > Modifier.

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/\[Redacted\]](https://login.microsoftonline.com/[Redacted]) 

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Verification certificates (optional)  Edit

Required: No

Active: 0

Expired: 0

c. Sélectionnez maintenant l'option Importer le 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	8/25/2029, 7:03:32 PM	[Redacted]	...

Signing Option:

Signing Algorithm:

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

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. 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?

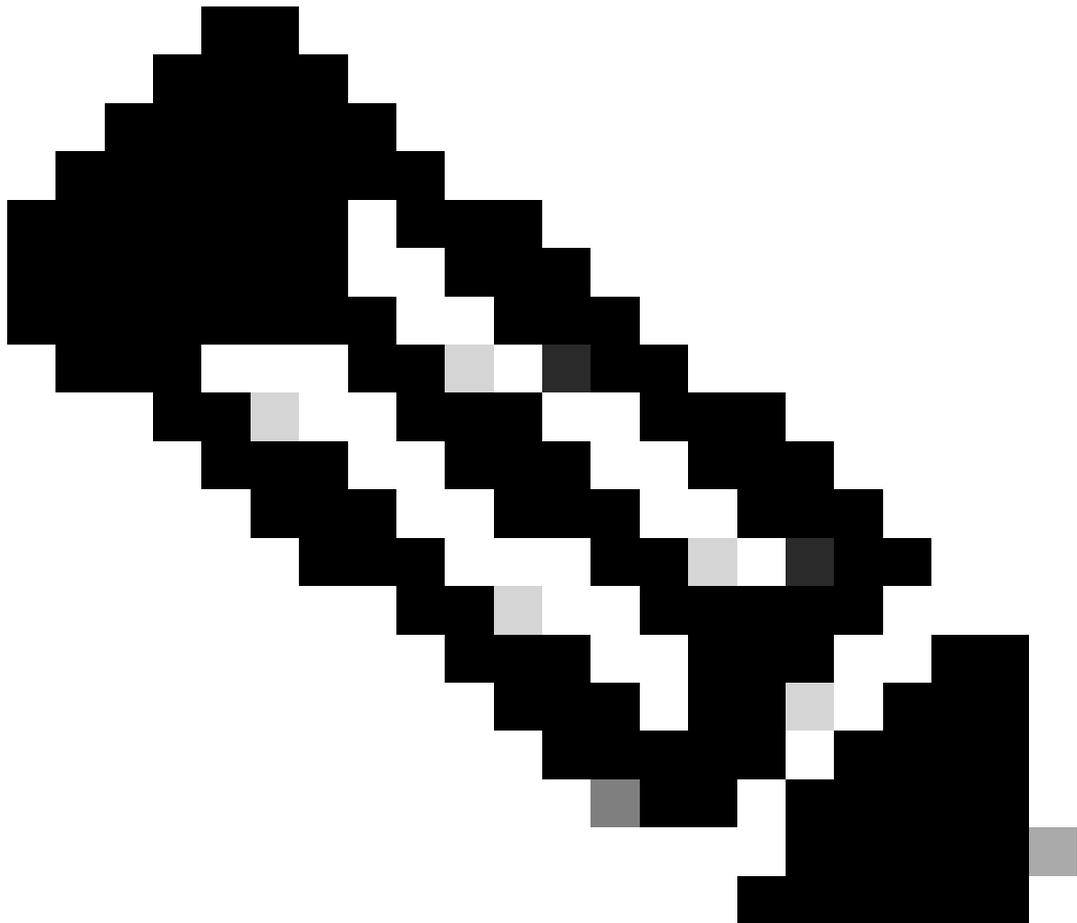
Status	Expiration Date	Thumbprint	
Inactive	9/28/2034, 1:05:19 PM	[Redacted]	⋮
Active	9/27/2027, 5:51:21 PM	[Redacted]	⋮

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

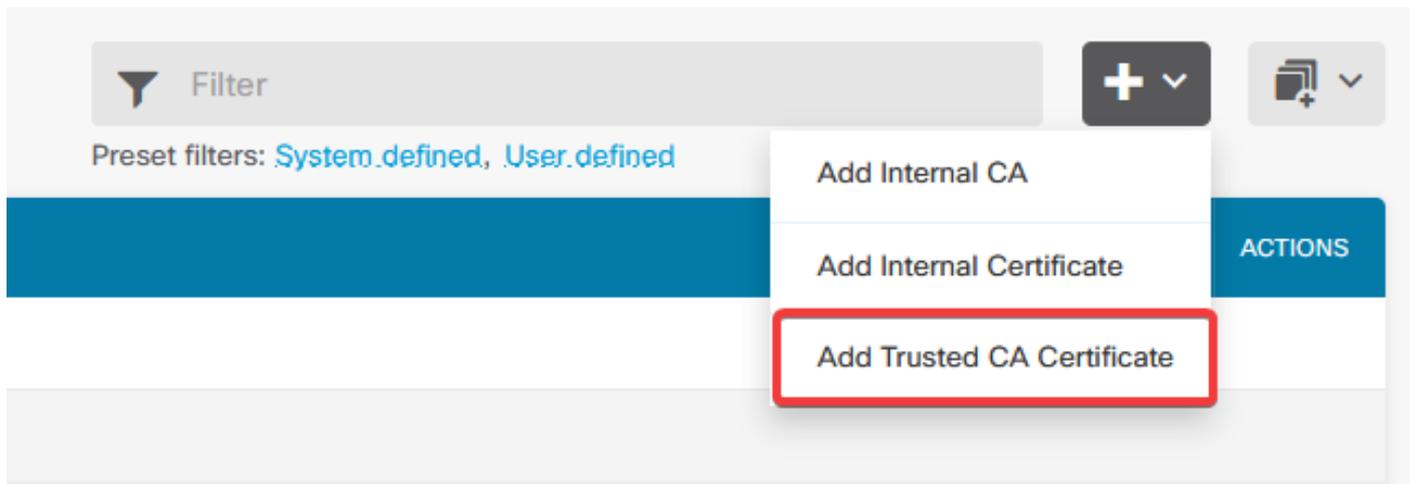


Remarque : assurez-vous d'effectuer l'étape 2.1 : Téléchargez le certificat vers Azure pour

chaque application.

Étape 2.2. Télécharger le certificat sur le FDM

a. Accédez à **Objects > Certificates > Click Add Trusted CA certificate.**



b. 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), puis vérifiez la `skip CA Certificate Check`.

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. Définissez l'objet SAML sur les différents profils de connexion qui utilisent SAML comme méthode d'authentification et pour lesquels l'application a été créée dans Azure. Déployer les modifications

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



Vérifier

Exécutez les commandes `show running-config webvpn` et `show running-config tunnel-group` pour vérifier la configuration et vérifier que la même URL IDP est configurée sur les différents profils de connexion.

```
<#root>
```

```
firepower#
```

```
show running-config 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:/anyconnprofs/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#
```

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.