

# Meervoudige RAVPN-profielen configureren met SAML-verificatie op FDM

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Stap 1: Maak een zelfondertekend certificaat en PKCS#12 File met OpenSSL](#)

[Stap 2: Upload het PKCS#12-bestand op Azure en FDM](#)

[Stap 2.1. Certificaat uploaden naar Azure](#)

[Stap 2.2. Upload het certificaat naar de FDM](#)

[Verifiëren](#)

---

## Inleiding

In dit document wordt beschreven hoe u SAML-verificatie kunt configureren voor Meerdere verbindingsprofielen van externe toegang VPN met Azure als IdP op CSF via FDM.

## Voorwaarden

### Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- Secure Socket Layer (SSL)-certificaten
- OpenSSL
- Remote Access Virtual Private Network (RAVPN)
- Cisco Secure Firewall Device Manager (FDM)
- Security Assertion Markup Language (SAML)
- Microsoft Azure

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- OpenSSL
- Cisco Secure Firewall (CSF) versie 7.4.1
- Cisco Secure Firewall Device Manager versie 7.4.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

SAML, of Security Assertion Markup Language, is een open standaard voor het uitwisselen van verificatie- en autorisatiegegevens tussen partijen, met name een Identity Provider (IDP) en een Service Provider (SP). Het gebruik van SAML-verificatie voor RAVPN-verbindingen (Remote Access VPN) en diverse andere toepassingen is steeds populairder geworden vanwege de vele voordelen. In het Firepower Management Center (FMC) kunnen meerdere verbindingsprofielen worden geconfigureerd voor het gebruik van verschillende met IDP beschermde toepassingen, dankzij de optie Override Identity Provider Certificate die beschikbaar is in het configuratiemenu van het verbindingsprofiel. Met deze functie kunnen beheerders het primaire IDP-certificaat in het SSO-serverobject (Single Sign-On) overschrijven met een specifiek IDP-certificaat voor elk verbindingsprofiel. Deze functionaliteit is echter beperkt voor Firepower Device Manager (FDM) omdat deze geen vergelijkbare optie biedt. Als er een tweede SAML-object is geconfigureerd, resulteert een poging om verbinding te maken met het eerste verbindingsprofiel in een verificatiefout door de foutmelding weer te geven: "Verificatie mislukt vanwege een probleem bij het ophalen van de enkele aanmelding-cookie." Om deze beperking te omzeilen, kan een aangepast zelfondertekend certificaat worden gemaakt en geïmporteerd in Azure voor gebruik in alle toepassingen. Hierbij hoeft slechts één certificaat in de FDM te worden geïnstalleerd, waardoor een naadloze SAML-verificatie voor meerdere toepassingen mogelijk is.

## Configureren

### Stap 1: Maak een zelfondertekend certificaat en PKCS#12 File met OpenSSL

In deze sectie wordt beschreven hoe u het zelfondertekende certificaat maakt met OpenSSL

1. Meld u aan bij een eindpunt waarop de OpenSSL-bibliotheek is geïnstalleerd.



Opmerking: in dit document wordt een Linux-machine gebruikt, dus sommige opdrachten zijn specifiek voor een Linux-omgeving. De opdrachten voor OpenSSL zijn echter hetzelfde.

---

b. Maak een configuratiebestand met de opdracht `touch`

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

c. Bewerk het bestand met een teksteditor. In dit voorbeeld wordt Vim gebruikt en wordt de `vim`

**.conf**

opdracht uitgevoerd. U kunt elke andere teksteditor gebruiken.

**<#root>**

root@host#

**vim config.conf**

d. Voer de informatie in die in het zelfondertekende document moet worden opgenomen.

Verzeker u ervan dat u de waarden tussen < > en de informatie van uw organisatie vervangt.

[req]

distinguished\_name = req\_distinguished\_name

prompt = no

[req\_distinguished\_name]

C =

ST =

L =

O =

OU =

CN =

e. Met deze opdracht wordt een nieuwe 2048-bits RSA-privésleutel en een zelfondertekend certificaat gegenereerd met behulp van het SHA-256-algoritme, geldig voor 3650 dagen, op basis van de configuratie die in het

`.conf`

bestand is gespecificeerd. De persoonlijke sleutel wordt opgeslagen in

`.pem`

en het zelfondertekende certificaat wordt opgeslagen in

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

f. Na het maken van de privé-sleutel en het zelfondertekende certificaat, exporteert het deze naar een PKCS#12-bestand, dat een formaat is dat zowel de privé-sleutel als het certificaat kan bevatten.

<#root>

root@host#

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

.pem -in

.crt -name

-out

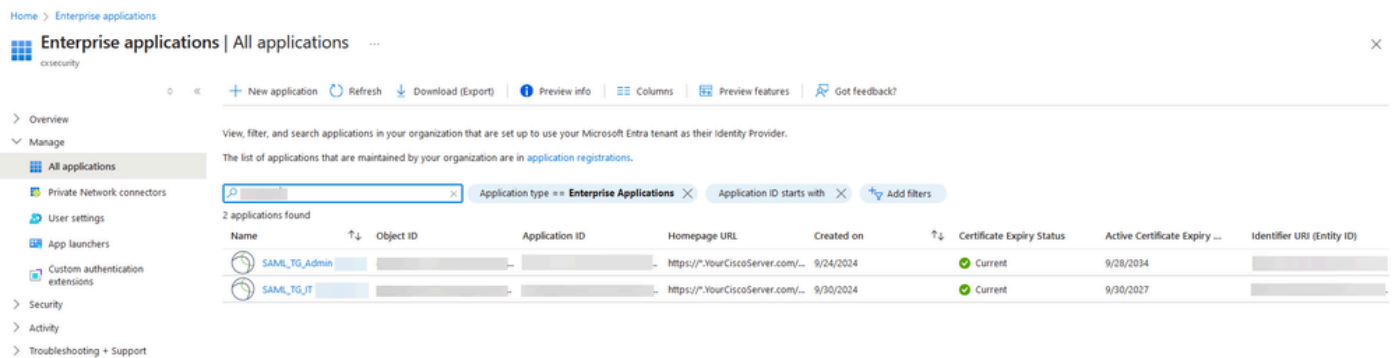
.pfx

```
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
```

Noteer het wachtwoord.

## Stap 2: Upload het PKCS#12-bestand op Azure en FDM

Zorg ervoor dat u op Azure een toepassing maakt voor elk verbindingsprofiel dat SAML-verificatie gebruikt op de 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:

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	

Zodra u het PKCS#12-bestand uit Stap 1 hebt: Maak een zelfondertekend certificaat en PKCS#12-bestand met OpenSSL, moet het worden geüpload naar Azure voor meerdere toepassingen en geconfigureerd in de FDM SSO-configuratie.


### Stap 2.1. Certificaat uploaden naar Azure

a. Log in op uw Azure-portal, navigeer naar de Enterprise-applicatie die u wilt beveiligen met

SAML-verificatie en selecteer Single Sign-On.

b. Blader naar beneden naar het gedeelte SAML-certificaten en selecteer de optie Meer opties > Bewerken.

### 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. Selecteer nu de optie Certificaat importeren.

## 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. Zoek het PKCS#12-bestand dat eerder is gemaakt en gebruik het wachtwoord dat u hebt ingevoerd toen u het PKCS#12-bestand hebt gemaakt.

### 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:  



e. Selecteer tot slot de optie Certificaat actief maken.

## 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



Opmerking: Zorg ervoor dat u Stap 2.1 uitvoert: Upload het certificaat naar Azure voor elke toepassing.

---

## Stap 2.2. Upload het certificaat naar de FDM

a. Navigeer naar **Objects > Certificates > Click Add Trusted CA certificate.**



# 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 Usage: ...)

Identity Provider Certificate

Azure\_SSO (Validation Usage: ...)

Request Signature

None

Request Timeout

*Range: 1 - 7200 (sec)*

d. Stel het SAML-object in op de verschillende verbindingsprofielen die SAML gebruiken als de verificatiemethode en waarvoor de toepassing is gemaakt in Azure. De wijzigingen implementeren

## 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



## Verifiëren

Voer de opdrachten `show running-config webvpn` en `show running-config tunnel-group` uit om de configuratie te bekijken en te controleren of dezelfde URL voor IDP is geconfigureerd op de verschillende verbindingsprofielen.

```
<#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#
```



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.