

RAVPN met SAML-verificatie configureren met Azure als IDP op FTD beheerde via FDM 7.2 en lager

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Stap 1. Maak een Certificate Signing Verzoek \(CSR\) met "Basic Constraints: CA:TRUE" Extension](#)

[Stap 2. PKCS12-bestand maken](#)

[Stap 3. Upload het PKCS#12-certificaat naar Azure en de FDM](#)

[Certificaat uploaden naar Azure](#)

[Upload het certificaat naar de FDM](#)

[Verifiëren](#)

Inleiding

In dit document wordt beschreven hoe u SAML-verificatie voor externe toegang VPN kunt configureren met Azure als IdP op FTD die wordt beheerd door FDM versie 7.2 of hieronder.

Voorwaarden

Vereisten

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

- Secure Socket Layer (SSL)-certificaten
- OpenSSL
- Linux-opdrachten
- Remote Access Virtual Private Network (RAVPN)
- 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 versie Cisco SSL 1.1.1j.7.2sp.230
- Secure Firewall Threat Defence (FTD) versie 7.2.0
- Secure Firewall Device Manager versie 7.2.0
- Interne certificeringsinstantie (CA)


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

Het gebruik van SAML-verificatie voor RAVPN-verbindingen en veel andere toepassingen is de laatste tijd populairder geworden door de voordelen ervan. SAML is een open standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen partijen, met name een Identity Provider (IDP) en een Service Provider (SP).

Er is een beperking in FTD beheerd door FDM versies 7.2.x of hieronder waar de enige ondersteunde IDP voor SAML authenticatie Duo is. In deze versies moeten de certificaten die gebruikt worden voor SAML-verificatie de extensie Basic Constraints: CA:TRUE hebben bij het uploaden ervan naar de FDM.

Om deze reden worden certificaten die door andere ID's worden geleverd (die niet de vereiste extensie hebben) zoals Microsoft Azure voor SAML-verificatie, niet ondersteund in deze versies, waardoor de SAML-verificatie mislukt.

 **Opmerking:** FDM-versies 7.3.x en nieuwer maken het mogelijk om de optie Skip CA Check in te schakelen bij het uploaden van een nieuw certificaat. Dit lost de in dit document beschreven beperking op.

In het geval dat u RAVPN met SAML-verificatie configureren met behulp van het certificaat dat door Azure wordt verstrekt en dat niet de basisbeperkingen heeft: CA:TRUE-extensie, wanneer u de opdracht `show saml metadata <trustpoint name>` uitvoert om de metagegevens terug te halen van de FTD Command Line Interface (CLI), is de uitvoer leeg zoals hierna weergegeven:

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

```
SP Metadata
```

```
-----
```

Configureren

Het voorgestelde plan om deze beperking op te lossen is om de Secure Firewall te upgraden naar versie 7.3 of hoger, maar als u om welke reden dan ook de Firewall nodig hebt om versie 7.2 uit te voeren of lager kunt u rond deze beperking werken door een aangepast certificaat te creëren dat de Basisbeperkingen bevat: CA:TRUE extensie. Zodra het certificaat is ondertekend door een aangepaste CA, moet u de configuratie wijzigen in het Azure SAML-configuratieportal, zodat het dit aangepaste certificaat kan gebruiken.

Stap 1. Een aanvraag voor certificaatondertekening (CSR) aanmaken met de extensie "Basic Constraints: CA:TRUE"

In deze paragraaf wordt beschreven hoe u een CSR kunt maken met OpenSSL zodat deze de Basic Constraints: CA:TRUE Extension bevat.

1. Log in op een eindpunt waarop de OpenSSL-bibliotheek is geïnstalleerd.
2. (Optioneel) Maak een map waarin u de bestanden die nodig zijn voor dit certificaat kunt vinden met de opdracht `mkdir <folder name>`.

```
<#root>
```

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


```
mkdir certificate
```

3. Als u een nieuwe directory aanmaakt, wijzigt u de directory naar deze directory en genereert u een nieuwe privé-sleutel met de opdracht `openssl genrsa -out <key_name>.key 4096`.

```
<#root>
```

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

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

 **Opmerking:** 4096 bits vertegenwoordigt de sleutellengte voor dit configuratievoorbeeld. U kunt indien nodig een langere toets opgeven.

4. Maak een configuratiebestand met de opdracht `<configuratie_name>.conf`.

5. Bewerk het bestand met een teksteditor. In dit voorbeeld wordt Vim gebruikt en wordt de opdracht `vim <config_name>.conf` uitgevoerd. U kunt elke andere teksteditor gebruiken.

```
<#root>
```

```
vim config.conf
```

6. Voer in de informatie die in het verzoek tot ondertekening van het certificaat moet worden opgenomen, de gegevens in. Zorg ervoor dat u de `basicConstraints = CA:true` extension in het bestand toevoegt zoals hieronder weergegeven:

```
<#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

 Opmerking: basicConstraints = CA:true is de extensie die het certificaat nodig heeft om het FTD succesvol te kunnen installeren.

7. Met behulp van de sleutel en het configuratiebestand dat in de vorige stappen is gemaakt, kunt u de CSR maken met de opdracht `openssl -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. Na deze opdracht ziet u het bestand <CSR_name>.csr in de map, het CSR-bestand dat naar de CA-server moet worden verzonden voor ondertekening.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDbXR5
MRQwEgYDVQQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQDRWH+ij26HuF/Y6NvITckD5VJa6KRssDJ8
[...]
```

Output Omitted

```
[...]
1RZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JsPkvJmRpKSi7c7w
3rKfTXe1ewT1IJdCmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

 Opmerking: vanwege Azure-vereisten is het nodig om de CSR te ondertekenen met een CA die SHA-256 of SHA-1 heeft geconfigureerd, anders wijst de Azure IDP het certificaat af wanneer u het uploadt. Meer informatie vindt u op de volgende link: [Geavanceerde opties voor het ondertekenen van certificaten in een SAML-token](#)

9. Verzend dit CSR-bestand met uw CA om het ondertekende certificaat te ontvangen.

Stap 2. PKCS12-bestand maken

Zodra u het identiteitsbewijs hebt ondertekend, moet u het Public-Key Cryptography Standards (PKCS#12) bestand met de volgende 3 bestanden maken:

- Ondertekend identiteitsbewijs
- Private sleutel (gedefinieerd in de vorige stappen)

- CA certificaatketen

U kunt het identiteitsbewijs en de CA-certificaatketen kopiëren naar hetzelfde apparaat waar u de privé-sleutel en het CSR-bestand hebt gemaakt. Zodra u de 3 bestanden hebt uitgevoerd, voert u de opdracht `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx` uit om het certificaat te converteren naar PKCS#12.

<#root>

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

Nadat u de opdracht hebt uitgevoerd, wordt u gevraagd een wachtwoord in te voeren. Dit wachtwoord is nodig wanneer u het certificaat installeert.

Als de opdracht succesvol was, wordt er een nieuw bestand met de naam "<pkcs12_name>.pfx" gemaakt in de huidige map. Dit is je nieuwe PKCS#12 certificaat.

Stap 3. Upload het PKCS#12-certificaat naar Azure en de FDM

Zodra u het PKCS#12-bestand hebt, moet u het uploaden naar Azure en de FDM.

Certificaat uploaden naar Azure

1. Log in op uw Azure-portal, navigeer naar de Enterprise-applicatie die u wilt beveiligen met SAML-verificatie en selecteer Single Sign-On.
2. Blader naar beneden naar het gedeelte SAML Certificates en selecteer het pictogram Meer opties > Bewerken.

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

4. Zoek het PKCS12-bestand dat eerder is gemaakt en gebruik het wachtwoord dat u hebt ingevoerd toen u het PKCS#12-bestand hebt gemaakt.

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. 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 | |
|----------|------------------------|------------|-----|
| 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

Upload het certificaat naar de FDM

1. Navigeer naar objecten > Certificaten > Klik op Add Trusted CA-certificaat.

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

Verifiëren

Voer de opdracht `show saml metadata <trustpoint name>` uit om er zeker van te zijn dat de metadata beschikbaar zijn via de FTD CLI:

```
<#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" />
```


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.