

# FDM 7.2 이하에서 관리되는 FTD에서 Azure를 IdP로 사용하여 SAML 인증으로 RAVPN 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. "Basic Constraints: CA:TRUE" 확장명으로 CSR\(Certificate Signing Request\) 생성](#)

[2단계. PKCS12 파일 만들기](#)

[3단계. Azure 및 FDM에 PKCS#12 인증서 업로드](#)

[Azure에 인증서 업로드](#)

[FDM에 인증서 업로드](#)

[다음을 확인합니다.](#)

---

## 소개

이 문서에서는 FDM 버전 7.2 이하에서 관리되는 FTD에서 Azure를 IdP로 사용하여 원격 액세스 VPN에 대한 SAML 인증을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- SSL(Secure Socket Layer) 인증서
- OpenSSL
- Linux 명령
- RAVPN(Remote Access Virtual Private Network)
- 보안 방화벽 장치 관리자(FDM)
- SAML(Security Assertion Markup Language)
- Microsoft Azure

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- OpenSSL 버전 CiscoSSL 1.1.1j.7.2sp.230
- FTD(Secure Firewall Threat Defense) 버전 7.2.0

- Secure Firewall Device Manager 버전 7.2.0
- 내부 CA(인증 기관)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.


## 배경 정보

RAVPN 연결 및 기타 여러 애플리케이션에 SAML 인증을 사용하는 것이 장점으로 인해 최근에 더 많이 사용되고 있습니다. SAML은 당사자 간, 특히 IdP(Identity Provider)와 SP(Service Provider) 간에 인증 및 권한 부여 정보를 교환하기 위한 개방형 표준입니다.

FDM 버전 7.2.x 이하에서 관리되는 FTD에서는 SAML 인증에 지원되는 유일한 IdP가 Duo인 데 한계가 있습니다. 이러한 버전에서 SAML 인증에 사용할 인증서는 FDM에 업로드할 때 Basic Constraints: CA:TRUE라는 확장명을 가져야 합니다.

이러한 이유로 SAML 인증을 위한 Microsoft Azure와 같은 다른 IdP(필요한 확장명이 없음)에서 제공하는 인증서는 이러한 버전에서 기본적으로 지원되지 않으므로 SAML 인증이 실패합니다.

---

 참고: FDM 버전 7.3.x 이상에서는 새 인증서를 업로드할 때 [CA 확인 건너뛰기] 옵션을 활성화할 수 있습니다. 이는 이 문서에 설명된 제한을 해결합니다.

---

기본 제약 조건이 없는 Azure에서 제공하는 인증서를 사용하여 SAML 인증으로 RAVPN을 구성하는 경우: CA:TRUE 확장 show saml metadata <trustpoint name> 명령을 실행하여 FTD CLI(Command Line Interface)에서 메타데이터를 검색하면 다음과 같이 출력이 비어 있습니다.

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

```
SP Metadata
```

```
-----
```

```
IdP Metadata
```

```
-----
```

## 구성

이 제한을 해결하기 위해 제안된 계획은 보안 방화벽을 버전 7.3 이상으로 업그레이드하는 것입니

다. 그러나 방화벽에서 버전 7.2 이하를 실행해야 하는 경우에는 Basic Constraints: CA:TRUE extension이 포함된 사용자 지정 인증서를 생성하여 이 제한을 해결할 수 있습니다. 사용자 지정 CA에서 인증서를 서명한 경우 Azure SAML 구성 포털에서 구성을 변경하여 이 사용자 지정 인증서를 대신 사용해야 합니다.

1단계. "Basic Constraints: CA:TRUE" 확장명으로 CSR(Certificate Signing Request)을 생성합니다.

이 섹션에서는 OpenSSL을 사용하여 CSR을 생성하여 기본 제약 조건(CA:TRUE Extension)을 포함하는 방법에 대해 설명합니다.

1. OpenSSL 라이브러리가 설치된 엔드포인트에 로그인합니다.

2. (선택 사항) mkdir <folder name> 명령을 사용하여 이 인증서에 필요한 파일을 찾을 수 있는 디렉토리를 만듭니다.

```
<#root>
```

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

```
mkdir certificate
```


3. 새 디렉토리를 생성한 경우 디렉토리를 해당 디렉토리로 변경하고 openssl genrsa -out <key\_name>.key 4096 명령을 실행하는 새 개인 키를 생성합니다.

```
<#root>
```

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

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

---

 참고: 4096비트는 이 컨피그레이션 예의 키 길이를 나타냅니다. 필요한 경우 더 긴 키를 지정할 수 있습니다.

---

4. touch <config\_name>.conf 명령을 사용하여 구성 파일을 만듭니다.

5. 텍스트 편집기로 파일을 편집합니다. 이 예에서는 Vim이 사용되고 vim <config\_name>.conf 명령이 실행됩니다. 다른 텍스트 편집기를 사용할 수 있습니다.

```
<#root>
```

```
vim config.conf
```

6. CSR(Certificate Signing Request)에 포함할 정보를 입력합니다. 다음에 표시된 대로 파일에 basicConstraints = CA:true 확장을 추가해야 합니다.

```
<#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
```

---

 참고: basicConstraints = CA:true는 FTD가 인증서를 성공적으로 설치하기 위해 인증서에 필요한 확장입니다.

---

7. 이전 단계에서 생성한 키 및 구성 파일을 사용하여 `openssl req -new <key_name>.key -config <conf_name>.conf -out <CSR_Name>.csr` 명령으로 CSR을 생성할 수 있습니다.

```
<#root>
```

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


8. 이 명령을 실행하면 폴더에 나열된 <CSR\_name>.csr 파일을 볼 수 있습니다. 이 파일은 서명을 위해 CA 서버로 전송해야 하는 CSR 파일입니다.

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIErTCCApUCAQAwwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDaXR5  
MRQwEgYDVQQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG  
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITCkD5VJa6KRssDJ8  
[...]
```

Output Omitted

```
[...]  
1RZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JSPkvJmRpKSi1c7w  
3rKFTXe1ewT1IJdCmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG  
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm  
RA==  
-----END CERTIFICATE REQUEST-----
```

---

 참고: Azure 요구 사항으로 인해 SHA-256 또는 SHA-1이 구성된 CA로 CSR에 서명해야 합니다. 그렇지 않으면 Azure IdP에서 인증서를 업로드할 때 인증서를 거부합니다. 자세한 내용은 다음 링크에서 확인할 수 있습니다. [SAML 토큰의 고급 인증서 서명 옵션](#)

---

9. 이 CSR 파일을 CA와 함께 보내 서명된 인증서를 가져옵니다.

## 2단계. PKCS12 파일 만들기

ID 인증서에 서명을 한 후에는 다음 3개 파일로 PKCS#12(Public-Key Cryptography Standards) 파일을 만들어야 합니다.

- 서명된 ID 인증서
- 개인 키(이전 단계에서 정의)
- CA 인증서 체인

개인 키 및 CSR 파일을 생성한 동일한 디바이스에 ID 인증서 및 CA 인증서 체인을 복사할 수 있습니다. 3개의 파일이 있는 경우 `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx` 명령을 실행하여 인증서를 PKCS#12로 변환합니다.

<#root>

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

명령을 실행한 후 비밀번호를 입력하라는 메시지가 표시됩니다. 이 비밀번호는 인증서를 설치할 때 필요합니다.

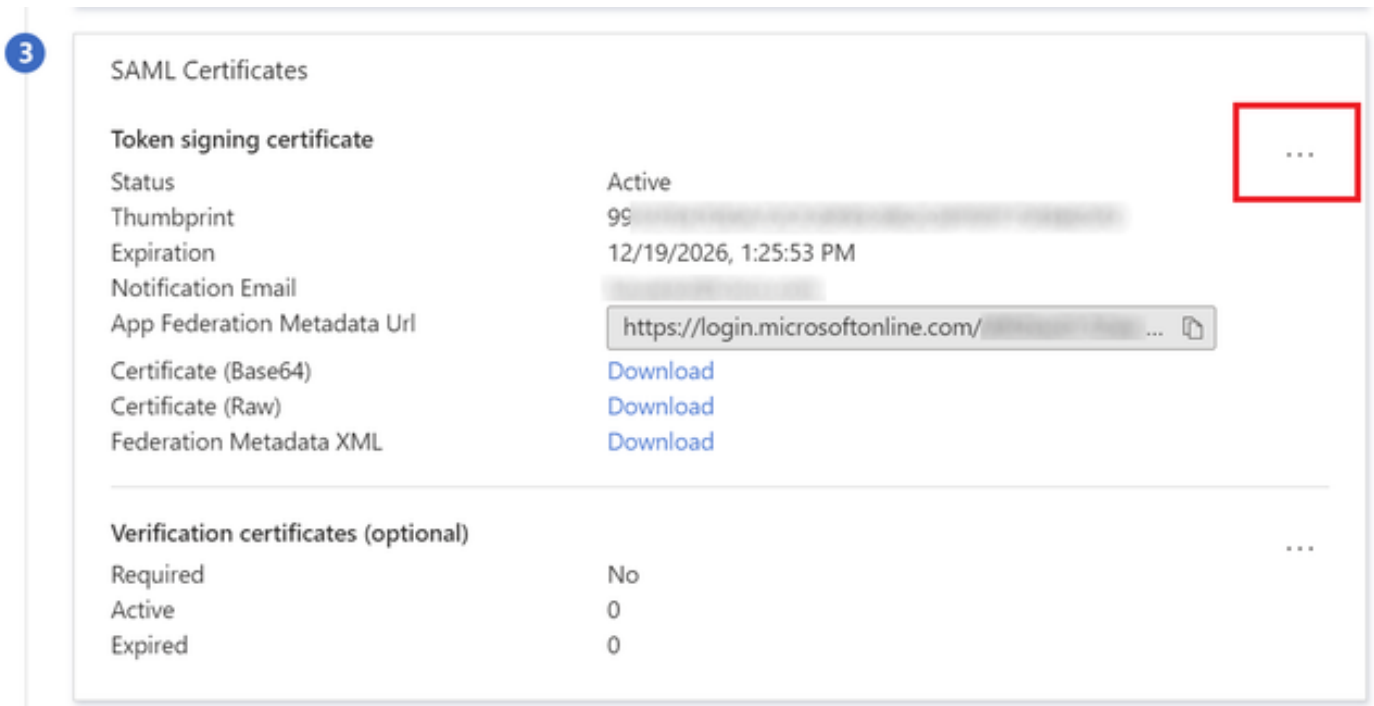
명령이 성공하면 현재 디렉터리에 "<pkcs12\_name>.pfx"라는 새 파일이 만들어집니다. 이것이 새로운 PKCS#12 인증서입니다.

### 3단계. Azure 및 FDM에 PKCS#12 인증서 업로드

PKCS#12 파일이 있는 경우 Azure 및 FDM에 업로드해야 합니다.

#### Azure에 인증서 업로드

1. Azure 포털에 로그인하여 SAML 인증으로 보호할 엔터프라이즈 응용 프로그램으로 이동한 후 Single Sign-On을 선택합니다.
2. 아래로 스크롤하여 "SAML 인증서" 섹션으로 이동한 다음 추가 옵션 아이콘 > 편집을 선택합니다



3. 이제 인증서 가져오기 옵션을 선택합니다.

## 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. 이전에 생성한 PKCS12 파일을 찾고 PKCS#12 파일을 생성할 때 입력한 비밀번호를 사용합니다


## 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: "cert.pfx"   
PFX Password: .....  

Add

Cancel

5. 마지막으로, 인증서 활성 설정 옵션을 선택합니다.



# 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: Sign SAML assertion

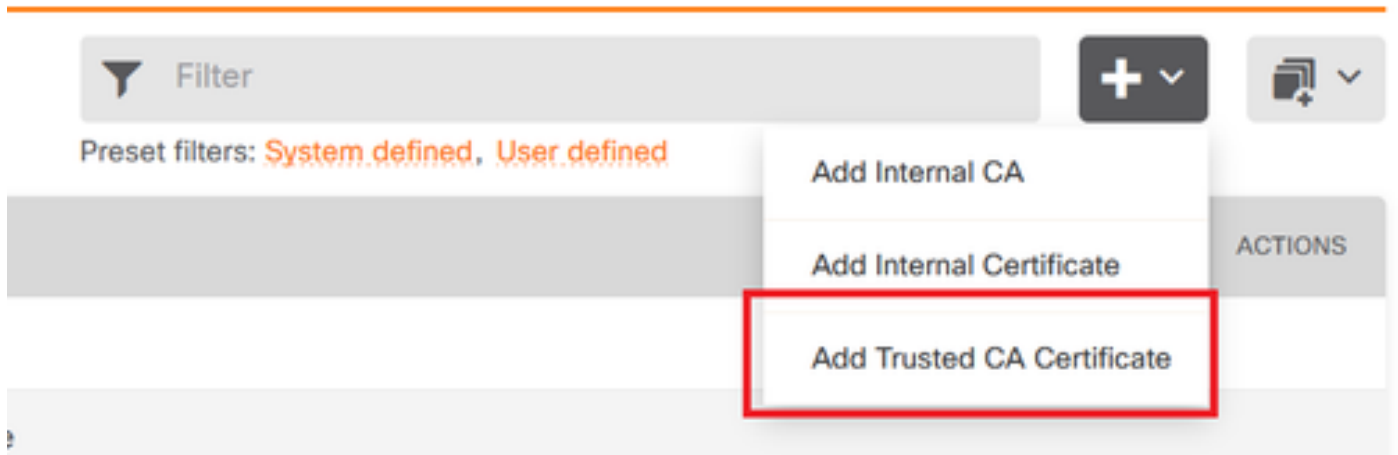
Signing Algorithm: SHA-256

Notification Email Addresses: [Empty field]

- Make certificate active
- Base64 certificate download
- PEM certificate download
- Raw certificate download
- Download federated certificate XML
- Delete Certificate

## FDM에 인증서 업로드

1. Objects(개체) > Certificates(인증서) > Add Trusted CA certificate(신뢰할 수 있는 CA 인증서 추가)를 클릭하여 이동합니다.



2. 원하는 신뢰 지점 이름을 입력하고 IdP(PKCS#12 파일 아님)의 ID 인증서만 업로드합니다.



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

다음을 확인합니다.

show saml metadata <trustpoint name> 명령을 실행하여 FTD CLI에서 메타데이터를 사용할 수 있는지 확인합니다.

```
<#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...]/saml2" />

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

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



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.