FDM에서 SAML 인증을 사용하여 여러 RAVPN 프로파일 구성

목차

소개

이 문서에서는 FDM을 통해 CSF에서 Azure를 IdP로 사용하여 원격 액세스 VPN의 다중 연결 프로파일에 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
- RAVPN(Remote Access Virtual Private Network)
- Cisco FDM(Secure Firewall Device Manager)
- SAML(Security Assertion Markup Language)
- Microsoft Azure

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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

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

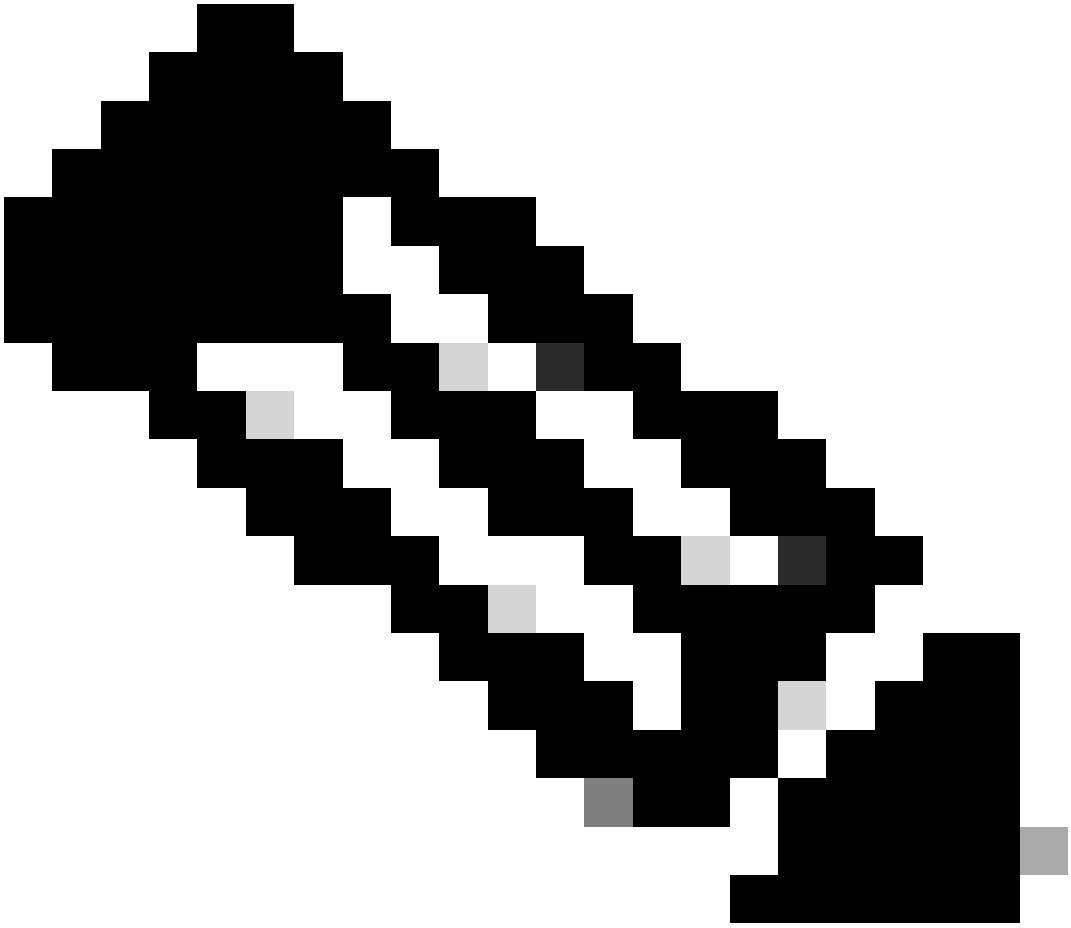
SAML(Security Assertion Markup Language)은 당사자 간에 인증 및 권한 부여 정보를 교환하기 위한 개방형 표준으로, 특히 IdP(Identity Provider)와 SP(Service Provider)입니다. RAVPN(Remote Access VPN) 연결 및 다양한 기타 애플리케이션에 SAML 인증을 사용하는 것은 여러 가지 이점 때문에 점점 더 널리 사용되고 있습니다. FMC(Firepower 관리 센터)에서는 연결 프로파일 구성 메뉴에서 사용할 수 있는 ID 공급자 인증서 재정의 옵션 때문에 여러 연결 프로파일이 서로 다른 IdP 보호 응용 프로그램을 사용하도록 구성할 수 있습니다. 이 기능을 사용하면 관리자가 SSO(Single Sign-On) 서버 개체의 기본 IdP 인증서를 각 연결 프로파일에 대한 특정 IdP 인증서로 재정의할 수 있습니다. 그러나 이 기능은 유사한 옵션을 제공하지 않으므로 FDM(Firepower 장치 관리자)에서 제한됩니다. 두 번째 SAML 객체가 구성된 경우 첫 번째 연결 프로파일에 연결을 시도하면 인증이 실패하고 "Single Sign-on 쿠키 검색 문제로 인해 인증에 실패했습니다."라는 오류 메시지가 표시됩니다. 이 제한을 해결하기 위해 모든 응용 프로그램에서 사용할 수 있도록 사용자 지정 자체 서명 인증서를 만들고 Azure로 가져올 수 있습니다. 이렇게 하면 FDM에 인증서를 하나만 설치해야 하므로 여러 응용 프로그램에 대해 원활한 SAML 인증이 가능합니다.

구성

1단계: OpenSSL을 사용하여 자체 서명 인증서 및 PKCS#12 파일 생성

이 섹션에서는 OpenSSL을 사용하여 자체 서명 인증서를 생성하는 방법에 대해 설명합니다

1. OpenSSL 라이브러리가 설치된 엔드포인트에 로그인합니다.



참고: 이 문서에서는 Linux 시스템을 사용하므로 일부 명령은 Linux 환경에 따라 달라집니다. 그러나 OpenSSL 명령은 동일합니다.

---

b. 명령을 사용하여 컨피그레이션 파일을touch

.conf
생성합니다.

<#root>

root@host#

touch config.conf

c. 텍스트 편집기로 파일을 편집합니다. 이 예에서는 Vim이 사용되고 명령**vim**

.conf

이 실행됩니다. 다른 텍스트 편집기를 사용할 수 있습니다.

<#root>

root@host#

vim config.conf

d. 자체 서명에 포함할 정보를 입력합니다.

< > 사이의 값을 조직의 정보로 대체해야 합니다.

[req]
distinguished_name = req_distinguished_name
prompt = no

[req_distinguished_name]
C =

ST =

L =

O =

OU =

CN =

e. 이 명령을 사용하면 파일에 지정된 컨피그레이션에 따라 3650일 동안 유효한 SHA-256 알고리즘을 사용하여 새 2048비트 RSA 개인 키 및 자체 서명 인증서를

.conf

생성합니다. 개인 키는에

.pem

저장되고 자체 서명 인증서는에

.crt

저장됩니다.

<#root>

root@host#

openssl req -newkey rsa:2048 -nodes -keyout

.pem -x509 -sha256 -days 3650 -config

.conf -out

.crt

f. 개인 키 및 자체 서명 인증서를 생성한 후 이를 PKCS#12 파일로 내보냅니다. 이 파일은 개인 키와 인증서를 모두 포함할 수 있는 형식입니다.

<#root>

root@host#

openssl pkcs12 -export -inkey

.pem -in

.crt -name

-out

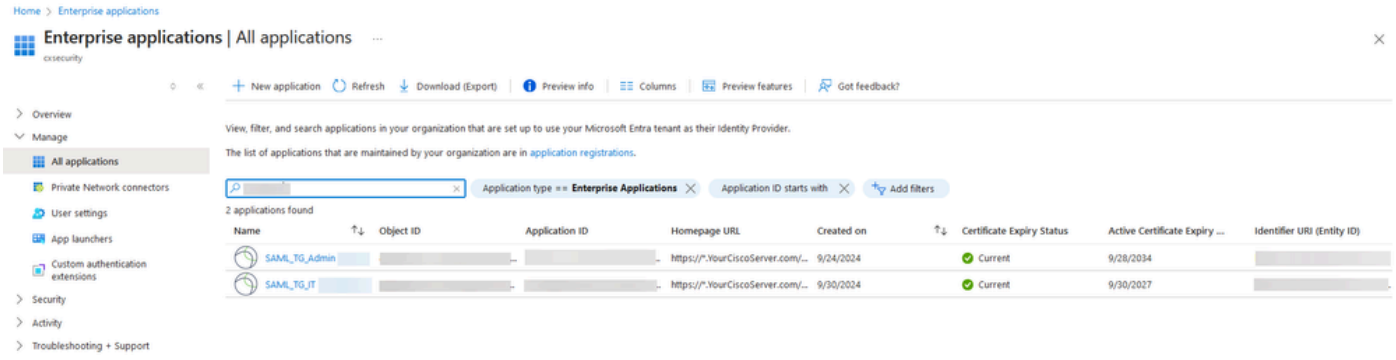
`.pfx`

```
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
```

비밀번호를 기록해 둡니다.

2단계: Azure 및 FDM에 PKCS#12 파일 업로드

FDM에서 SAML 인증을 사용하는 각 연결 프로파일에 대해 Azure에서 응용 프로그램을 만들어야 합니다.

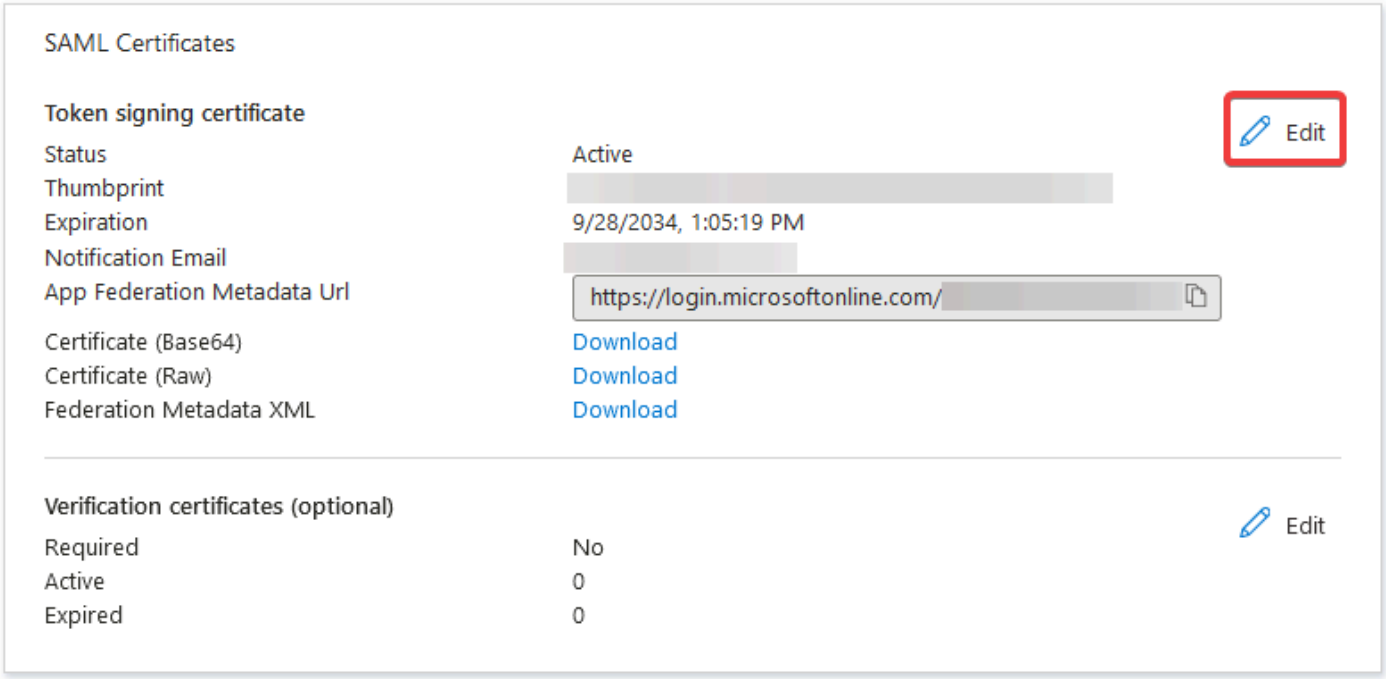


1단계: OpenSSL을 사용하여 자체 서명된 인증서 및 PKCS#12 파일 생성에서 PKCS#12 파일을 갖게 되면 여러 응용 프로그램에 대해 Azure에 업로드하고 FDM SSO 컨피그레이션에 구성해야 합니다.

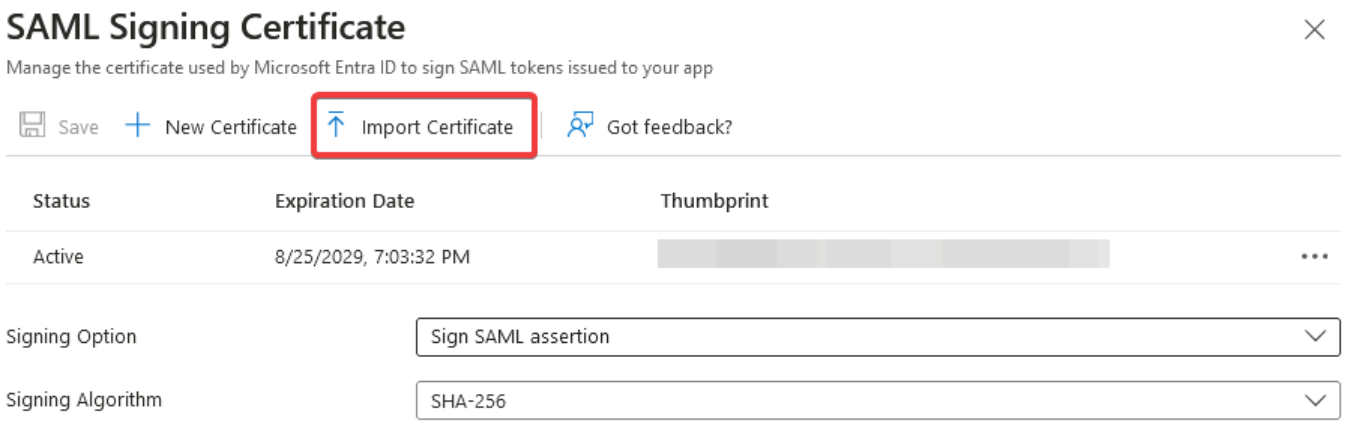
2.1단계. Azure에 인증서 업로드

a. Azure 포털에 로그인하여 SAML 인증으로 보호할 엔터프라이즈 응용 프로그램으로 이동한 후 Single Sign-On을 선택합니다.

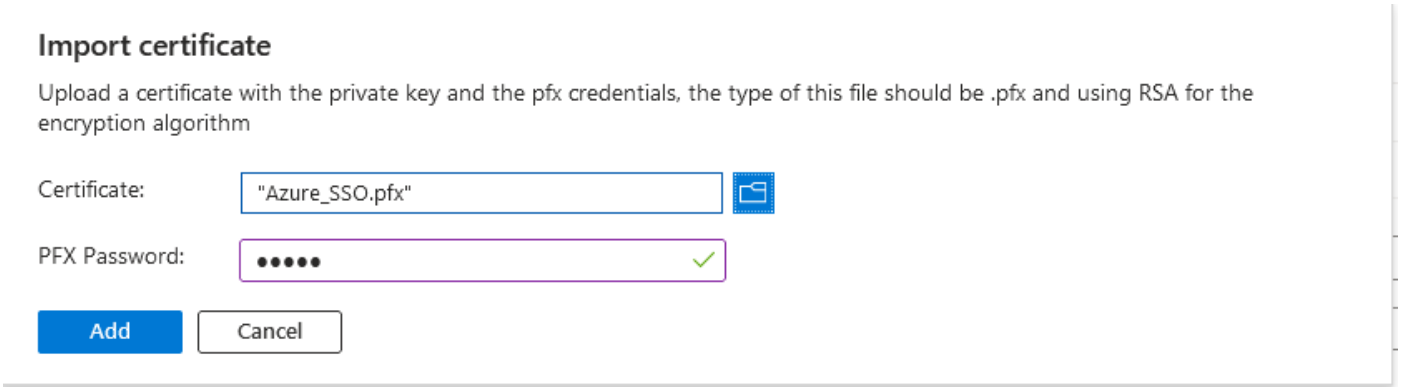
b. 아래로 스크롤하여 SAML Certificates(SAML 인증서) 섹션으로 이동하고 More Options(추가 옵션) > Edit(수정)를 선택합니다.



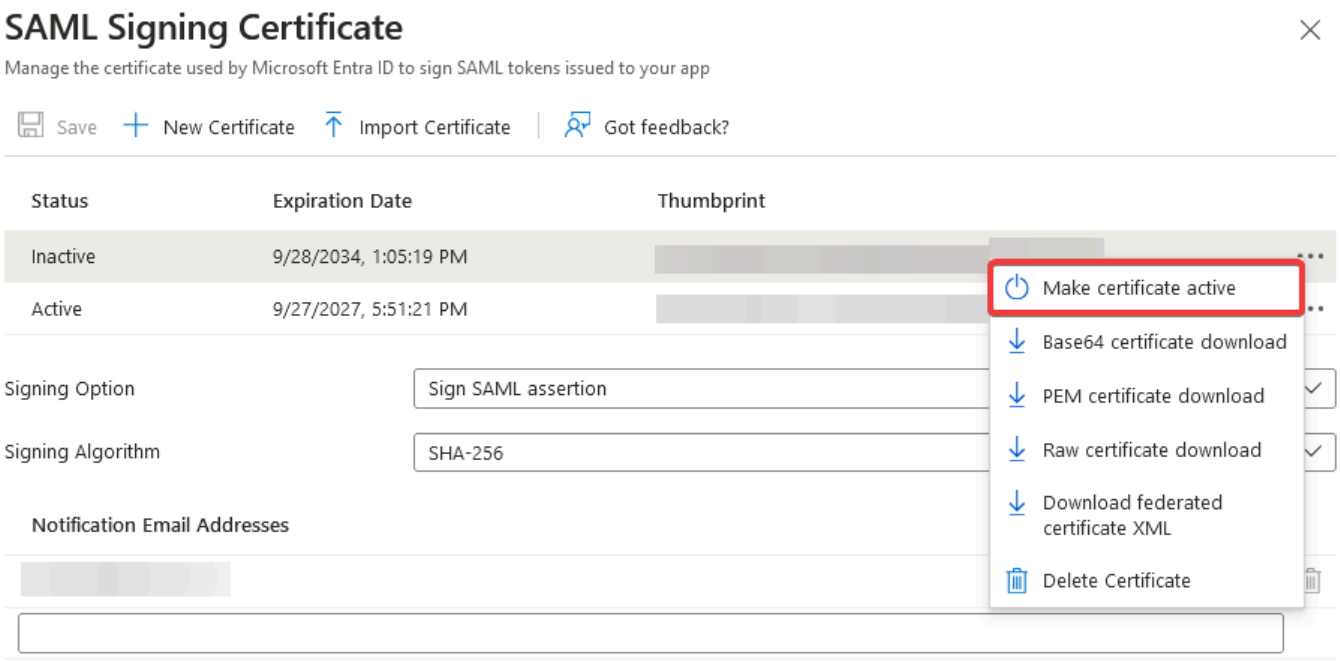
c. 이제 Import certificate(인증서 가져오기) 옵션을 선택합니다.

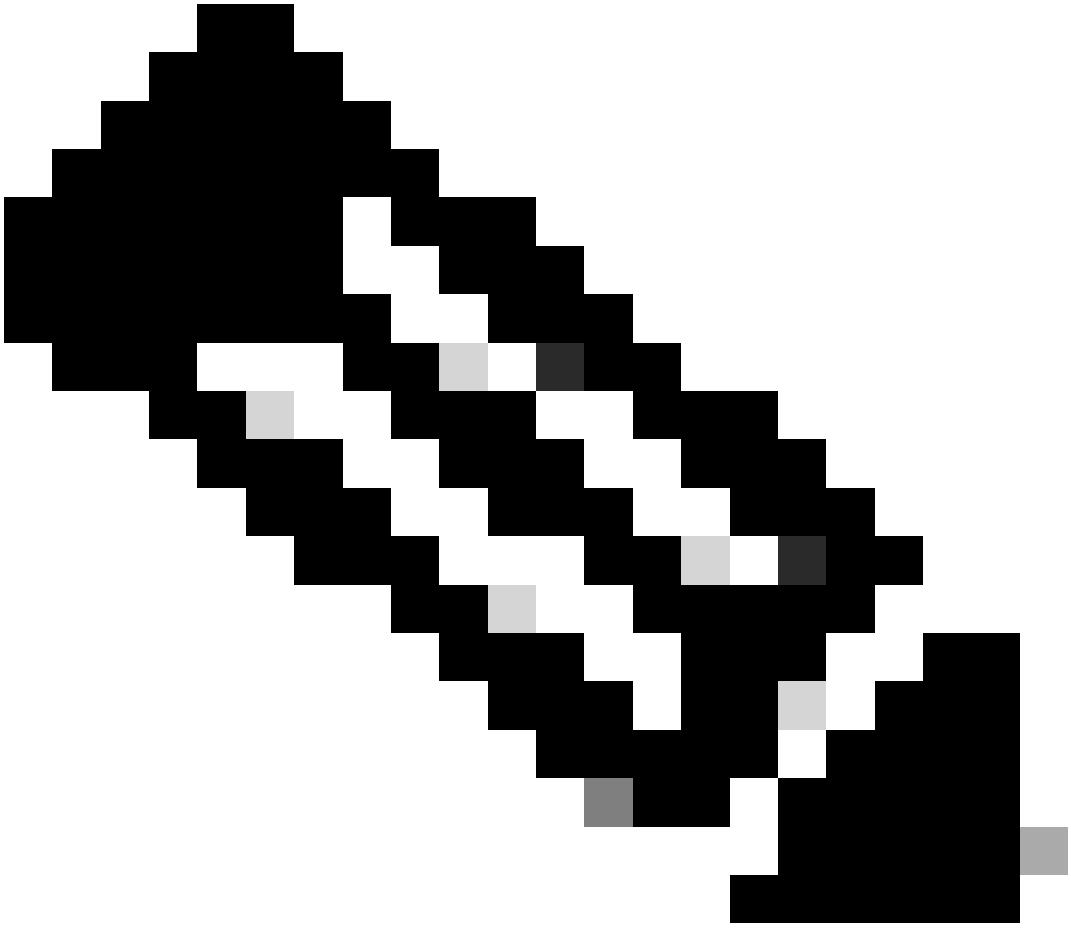


d. 이전에 생성한 PKCS#12 파일을 찾아 PKCS#12 파일을 생성할 때 입력한 비밀번호를 사용합니다.



e. 마지막으로, Make Certificate Active 옵션을 선택합니다.

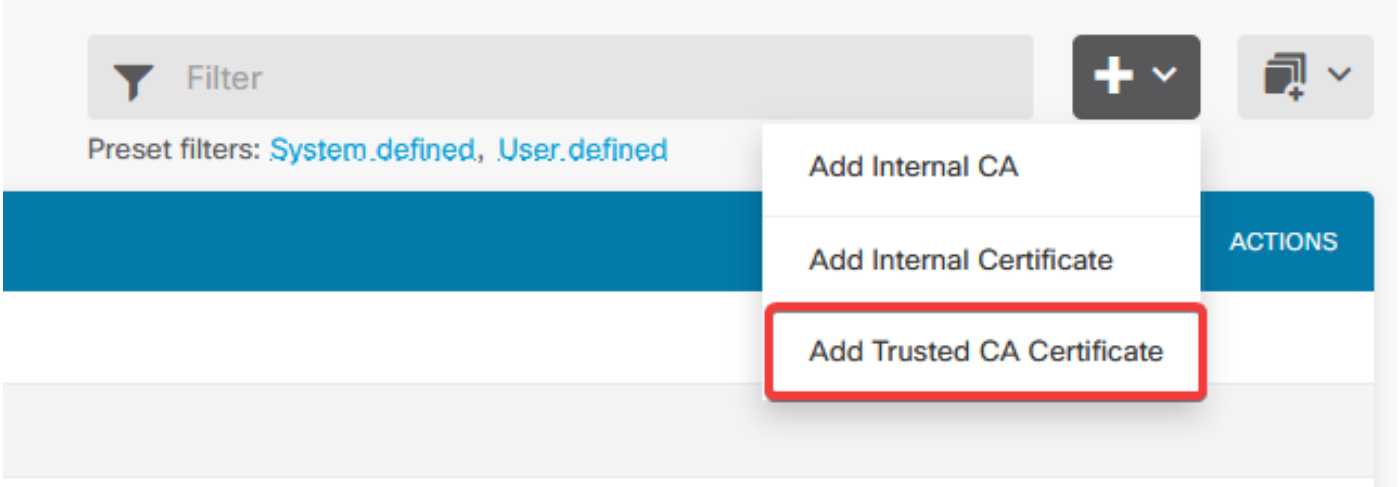




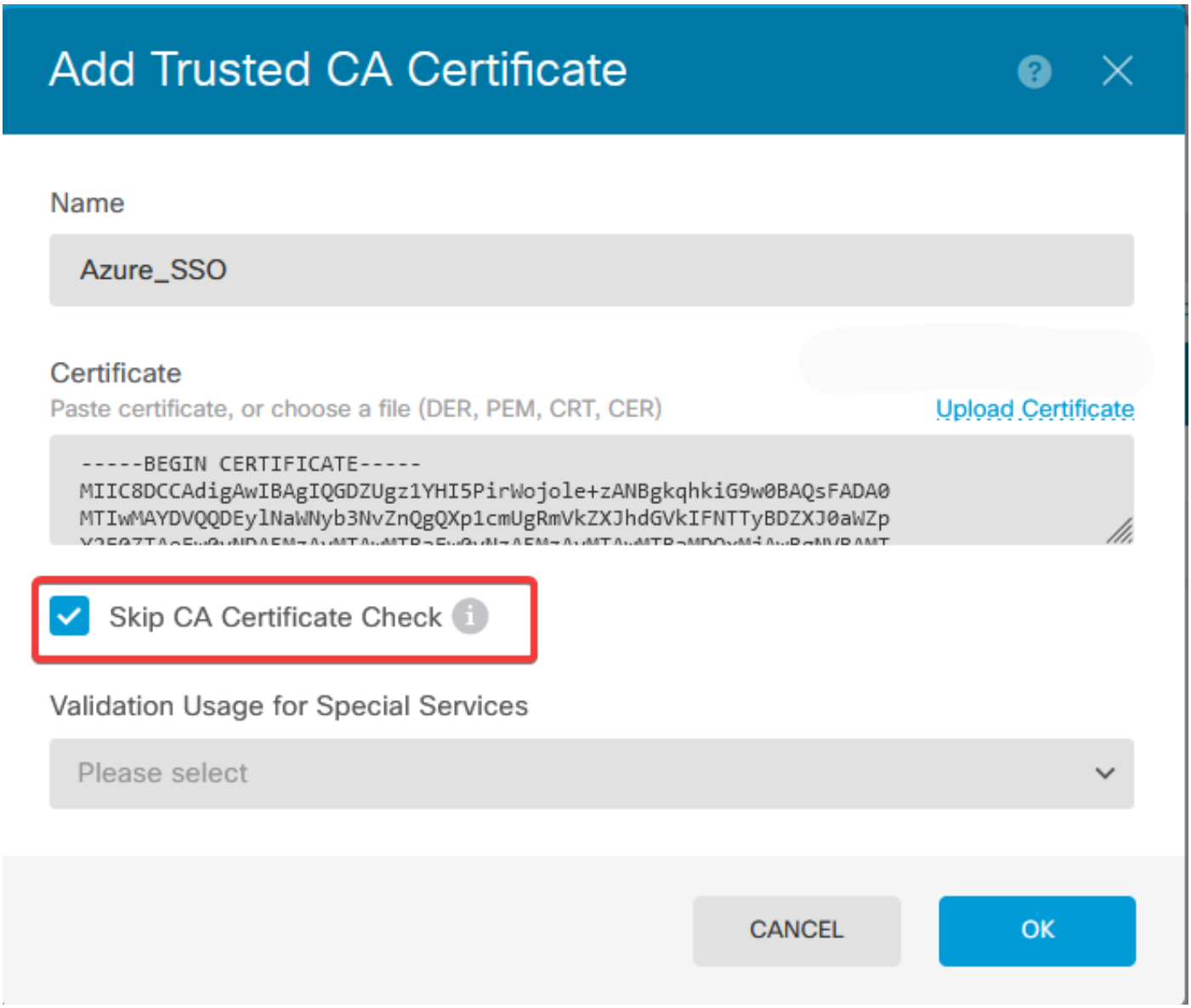
참고: 2.1단계를 수행해야 합니다. 각 애플리케이션에 대해 Azure에 인증서를 업로드하십시오.

2.2단계. FDM에 인증서 업로드

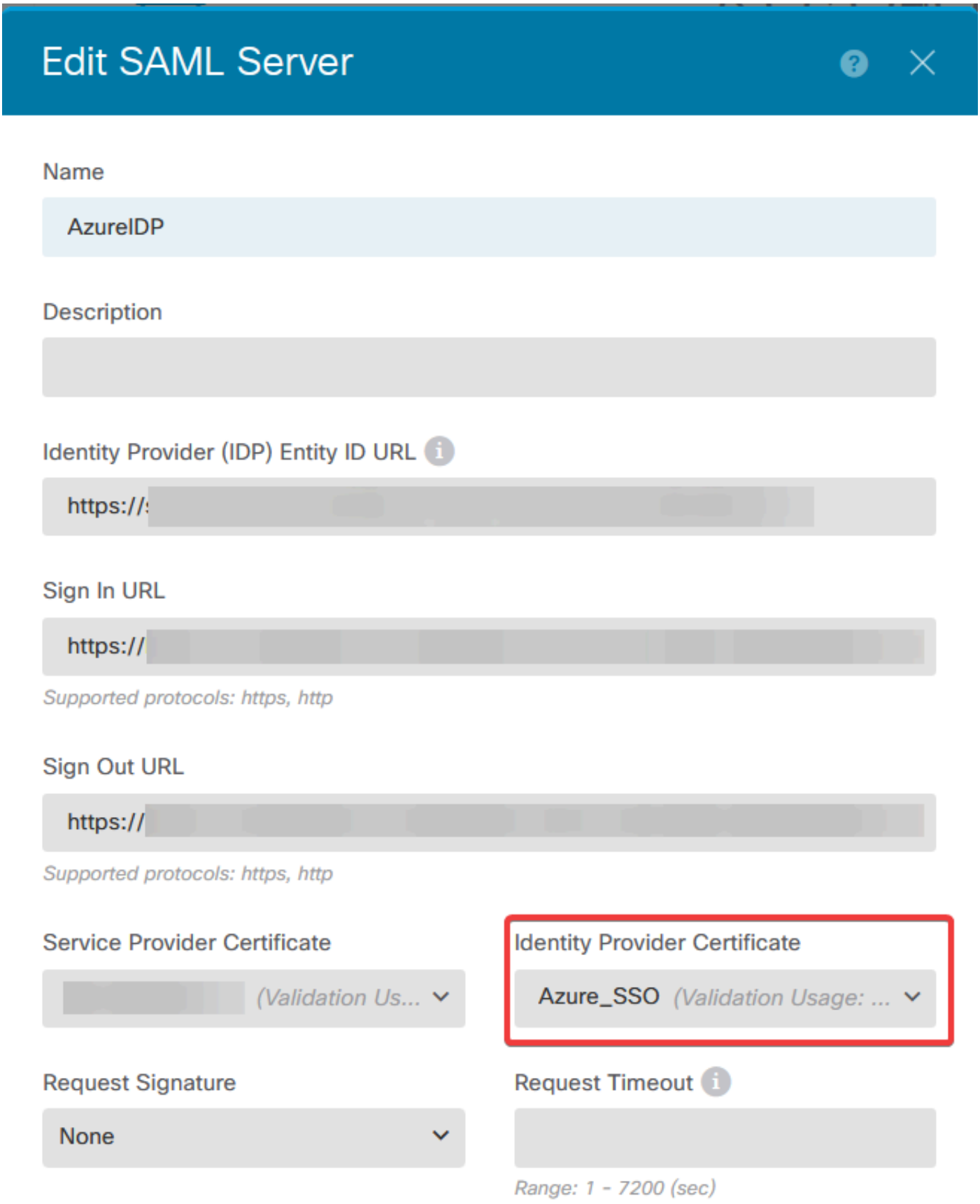
a. 로 **Objects** > **Certificates** > **Click Add Trusted CA certificate** 이동합니다.



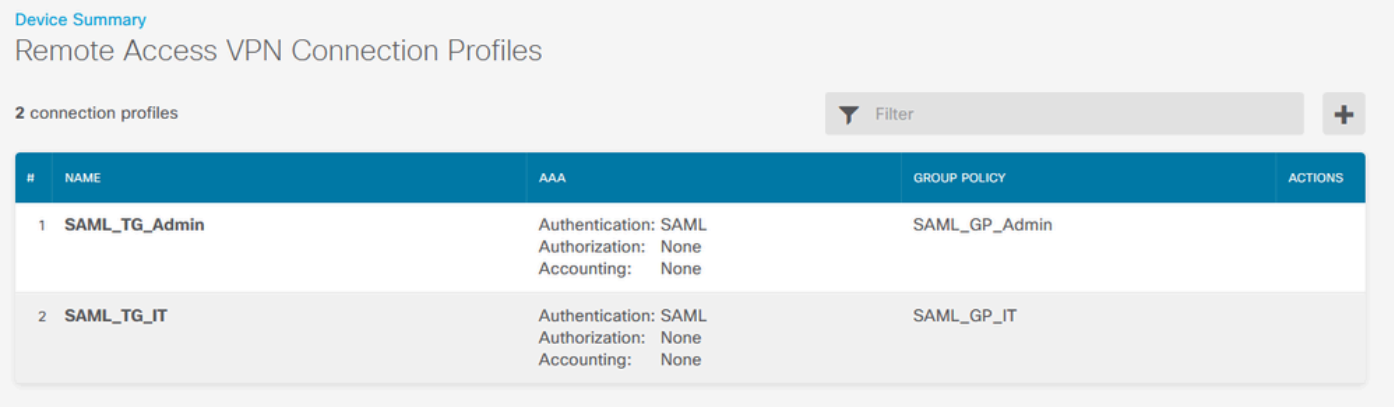
b. 원하는 신뢰 지점 이름을 입력하고 IdP(PKCS#12 파일 아님)의 ID 인증서만 업로드한 다음 를 **Skip CA Certificate Check**확인합니다.

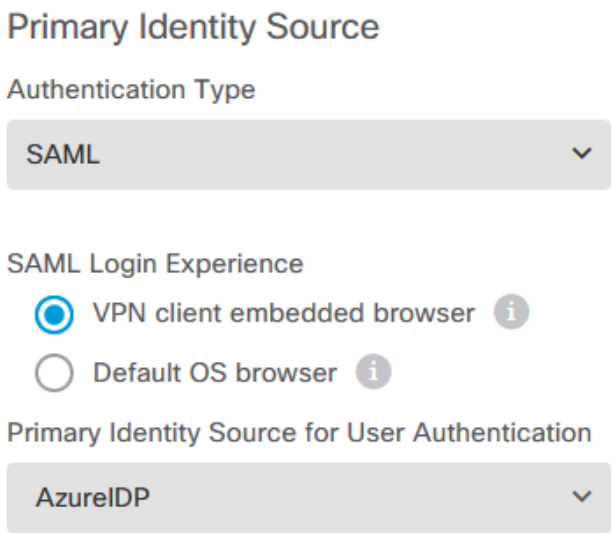


c. SAML 객체에서 새 인증서를 설정합니다.



d. SAML을 인증 방법으로 사용하고 Azure에서 응용 프로그램을 만든 다른 연결 프로필에 SAML 개체를 설정합니다. 변경 사항 배포





다음을 확인합니다.

webvpn 및show running-config명령을show running-config tunnel-group실행하여 구성을 검토하고 동일한 IDP URL이 다른 연결 프로파일에 구성되어 있는지 확인합니다.

<#root>

```
firepower#

show running-confuting 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:/anyconncprofs/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#
```

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.