FTD에서 여러 RAVPN 연결 프로파일에 대한 SAML 인증 구성

목차

소개

이 문서에서는 FMC에서 관리하는 Cisco FTD의 여러 연결 프로파일에 대한 Azure ID 공급자와의 SAML 인증에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- FMC(Firepower 관리 센터)에서 관리하는 NGFW(Next Generation Firewall)의 보안 클라이언트 구성
- SAML 및 metatada.xml 값

사용되는 구성 요소

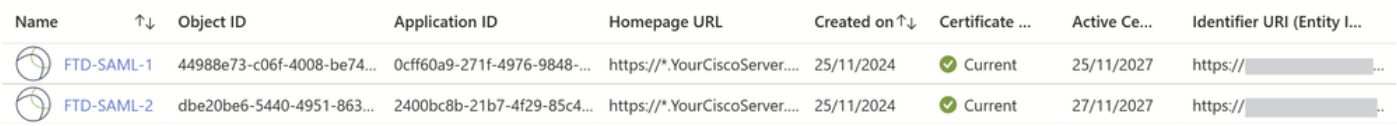
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD(firepower Threat Defense) 버전 7.4.0
- FMC 버전 7.4.0
- SAML 2.0의 Azure Microsoft Entra ID
- Cisco Secure Client 5.1.7.80

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

이 구성을 사용하면 FTD가 FMC에 구성된 단일 SAML 개체를 사용하여 Azure idp에서 서로 다른 두 SAML 응용 프로그램을 사용하여 보안 클라이언트 사용자를 인증할 수 있습니다.



Name	Object ID	Application ID	Homepage URL	Created on	Certificate ...	Active Ce...	Identifier URI (Entity I...
FTD-SAML-1	44988e73-c06f-4008-be74...	0cff60a9-271f-4976-9848-...	https://*.YourCiscoServer....	25/11/2024	Current	25/11/2027	https://
FTD-SAML-2	dbe20be6-5440-4951-863...	2400bc8b-21b7-4f29-85c4...	https://*.YourCiscoServer....	25/11/2024	Current	27/11/2027	https://

Microsoft Azure 환경에서 여러 응용 프로그램이 동일한 엔터티 ID를 공유할 수 있습니다. 일반적으로 서로 다른 터널 그룹에 매핑된 각 애플리케이션에는 고유한 인증서가 필요하므로, 단일 SAML IdP 객체 아래에서 FTD 측의 IdP 컨피그레이션 내에 여러 인증서를 구성해야 합니다. 그러나 Cisco FTD는 Cisco 버그 ID CSCvi29084에 설명된 대로 하나의 SAML IdP 개체에서 여러 인증서의 컨피그레이션을 지원하지 않습니다.

이러한 한계를 극복하기 위해 Cisco는 FTD 버전 7.1.0 및 ASA 버전 9.17.1에서 사용할 수 있는 IdP 인증서 재정의 기능을 도입했습니다. 이러한 기능 향상은 문제에 대한 영구적인 해결책을 제공하며 버그 보고서에 설명된 기존 해결 방법을 보완합니다.

설정

이 섹션에서는 FMC(Firepower 관리 센터)에서 관리하는 Cisco FTD(Firepower Threat Defense)의 여러 연결 프로파일에 대해 IdP(ID 공급자)로서 Azure를 사용하는 SAML 인증을 구성하는 프로세스에 대해 설명합니다. IdP 인증서 재정의 기능은 이를 효과적으로 설정하는 데 사용됩니다.

구성 개요:

Cisco FTD에서 2개의 연결 프로파일을 구성해야 합니다.

- FTD-SAML-1
- FTD-SAML-2

이 컨피그레이션 샘플에서는 VPN 게이트웨이 URL(Cisco Secure Client FQDN)이 nigarapa2.cisco.com으로 설정됩니다

구성

Azure IdP에 대한 구성

Cisco Secure Client용 SAML 엔터프라이즈 애플리케이션을 효율적으로 구성하려면 다음 단계를 완료하여 모든 매개변수가 각 터널 그룹에 대해 올바르게 설정되었는지 확인합니다.

SAML 엔터프라이즈 애플리케이션에 액세스:

엔터프라이즈 애플리케이션이 나열된 SAML 공급자의 관리 콘솔로 이동합니다.

적절한 SAML 애플리케이션을 선택합니다.

구성할 Cisco Secure Client 터널 그룹에 해당하는 SAML 애플리케이션을 식별하고 선택합니다.

식별자(엔티티 ID)를 구성합니다.

각 응용 프로그램의 식별자(엔터티 ID)를 설정합니다. 이 URL은 Cisco Secure Client FQDN(Fully Qualified Domain Name)인 기본 URL이어야 합니다.

회신 URL(어설션 소비자 서비스 URL)을 설정합니다.

올바른 기준 URL을 사용하여 회신 URL(Assertion Consumer Service URL)을 구성합니다. Cisco Secure Client FQDN과 일치하는지 확인합니다.

기본 URL에 연결 프로파일 또는 터널 그룹 이름을 추가하여 구체성을 확인합니다.

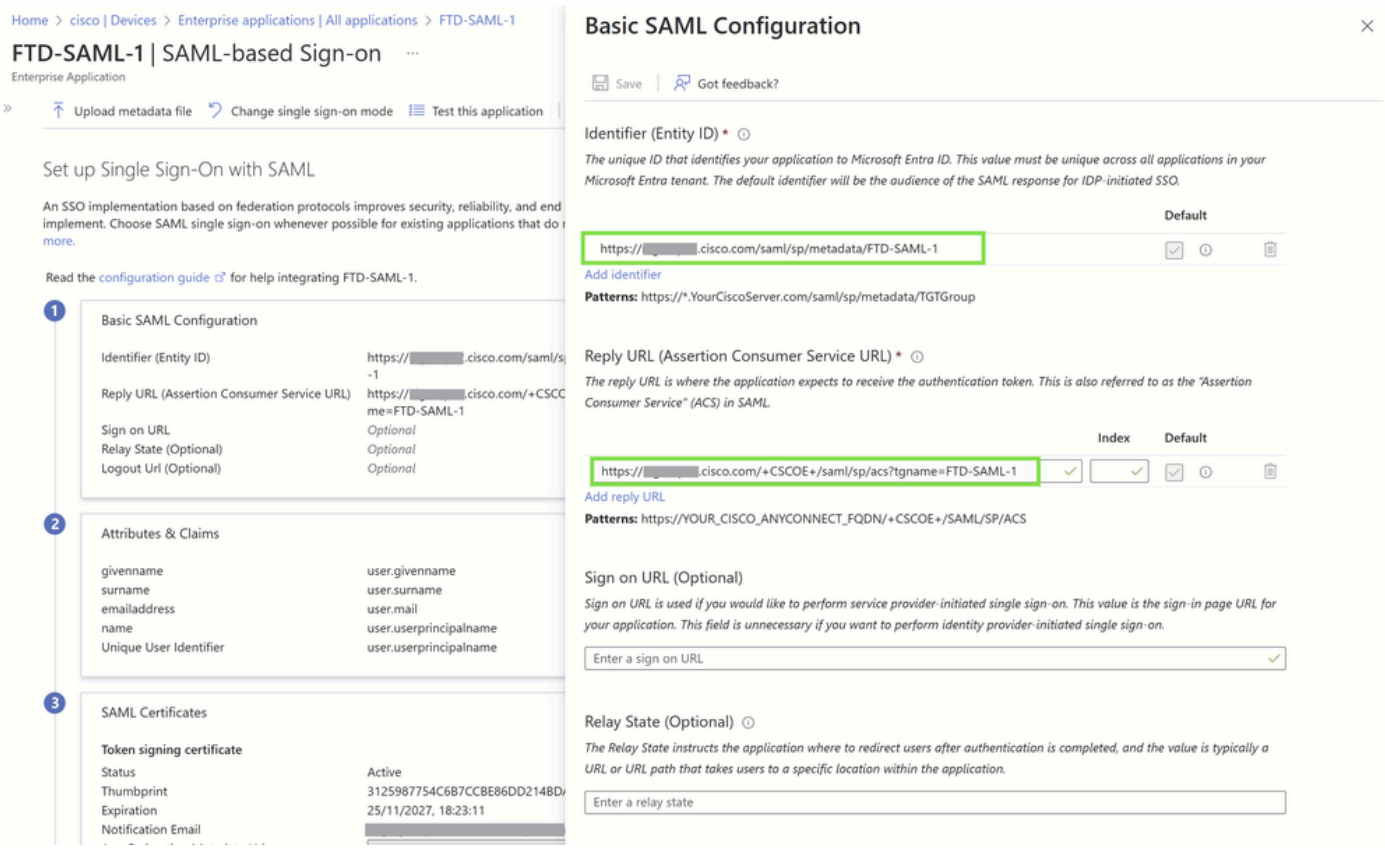
컨피그레이션 확인:

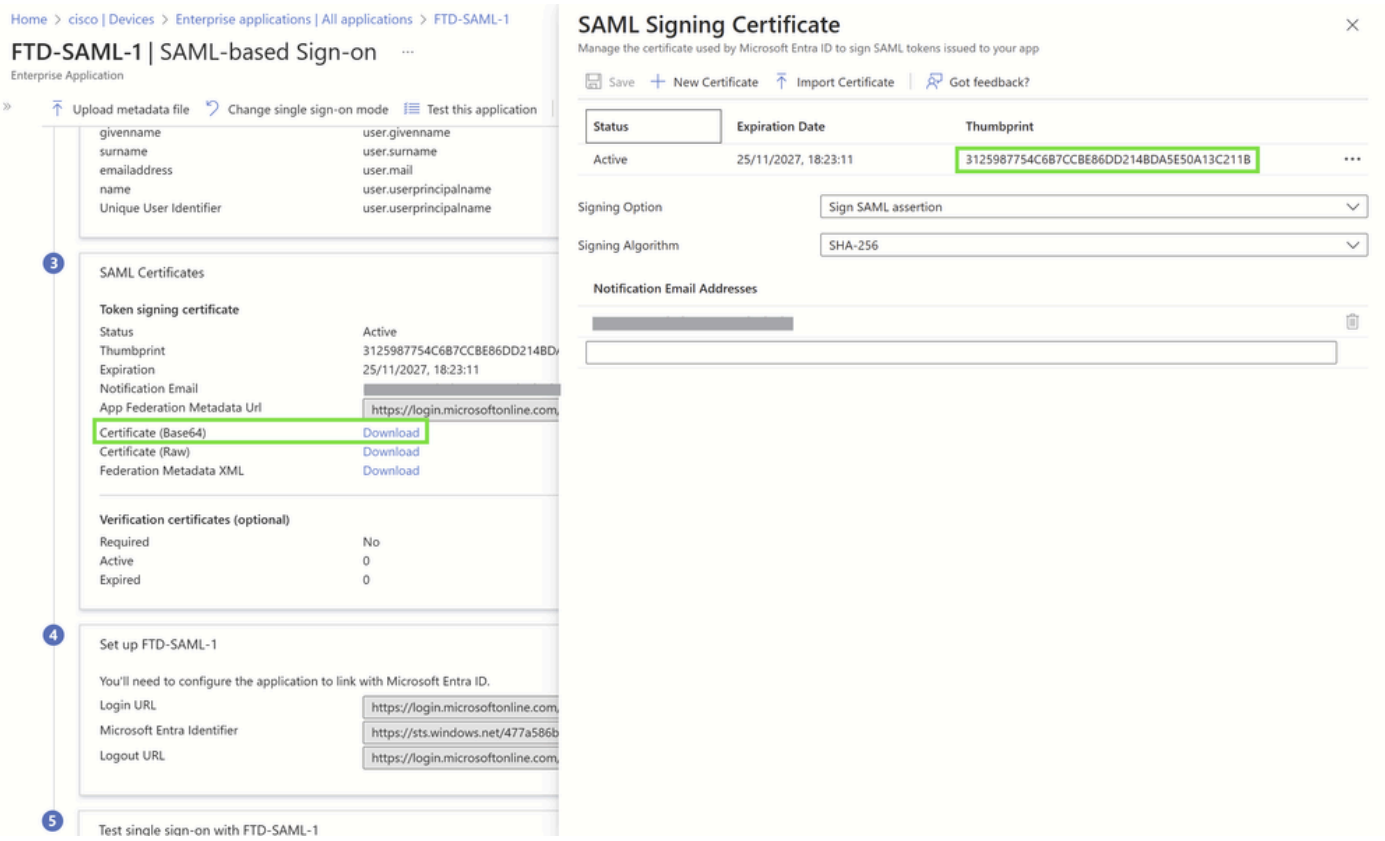
모든 URL 및 매개변수가 정확하게 입력되었고 각 터널 그룹에 해당하는지 다시 확인합니다.

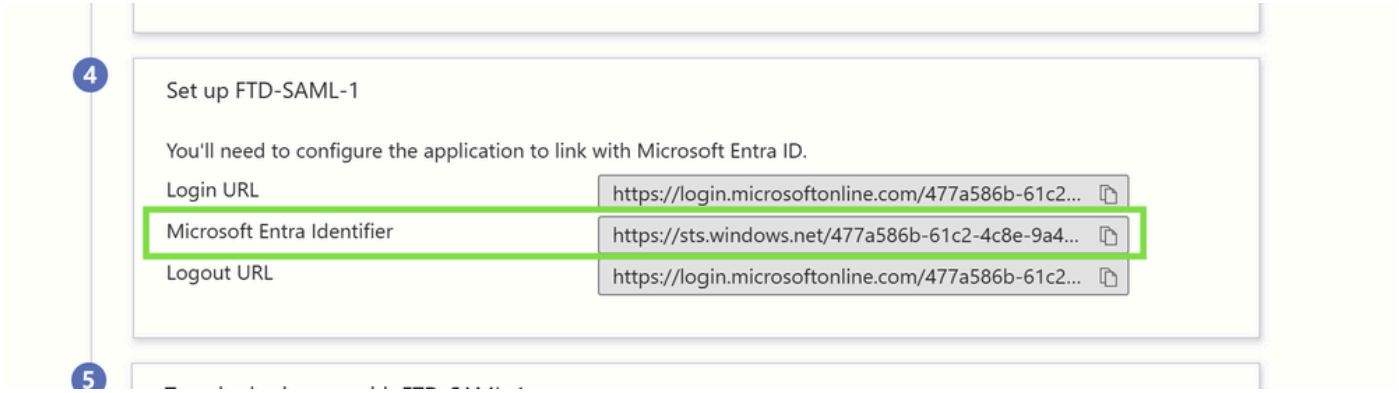
변경 사항을 저장하고 가능한 경우 테스트 인증을 수행하여 컨피그레이션이 예상대로 작동하는지 확인합니다.

자세한 지침은 Cisco 설명서의 "Microsoft App Gallery에서 Cisco Secure Client 추가"를 참조하십시오. SAML을 통해 Microsoft Azure MFA로 ASA Secure Client VPN 구성

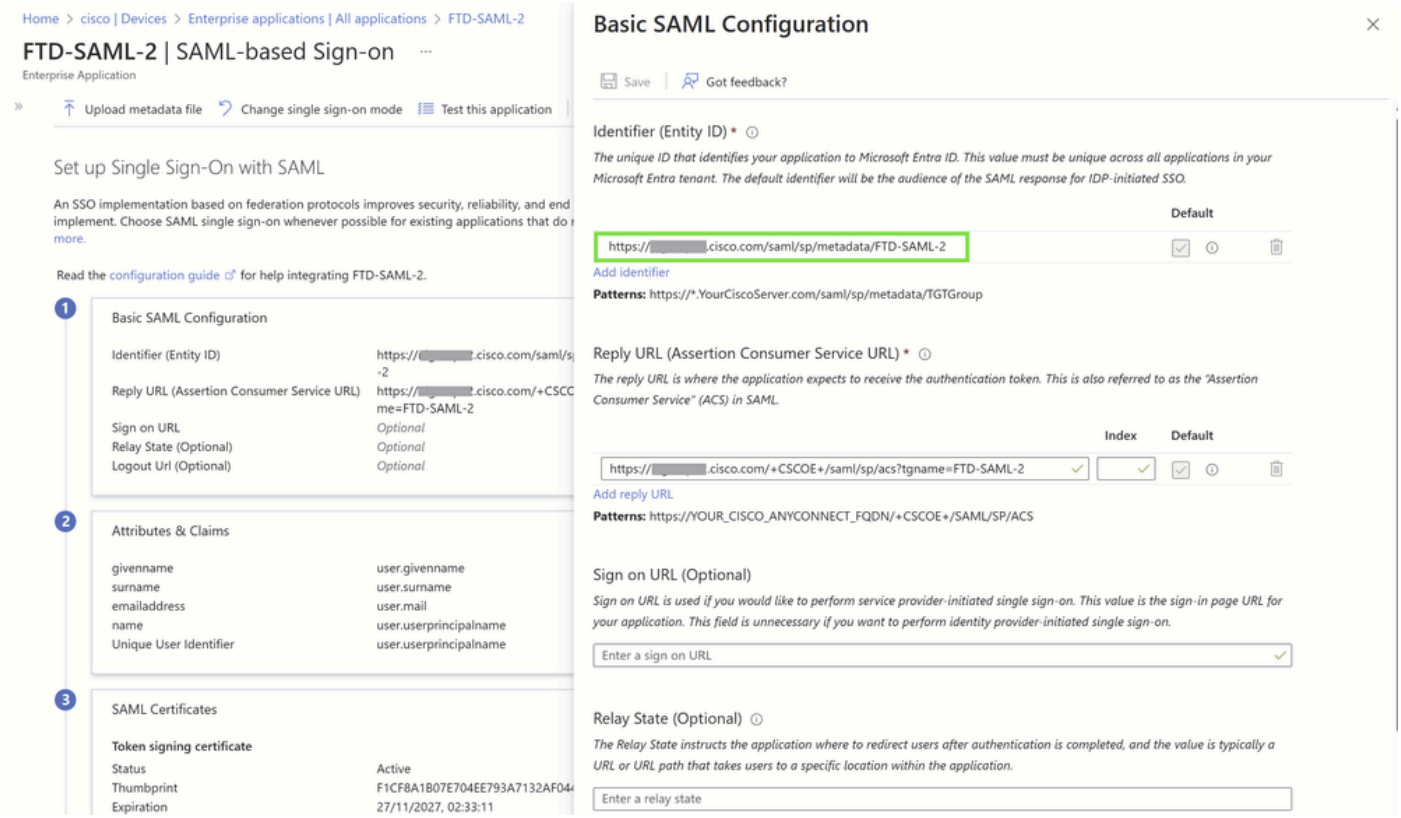
FTD-SAML-1

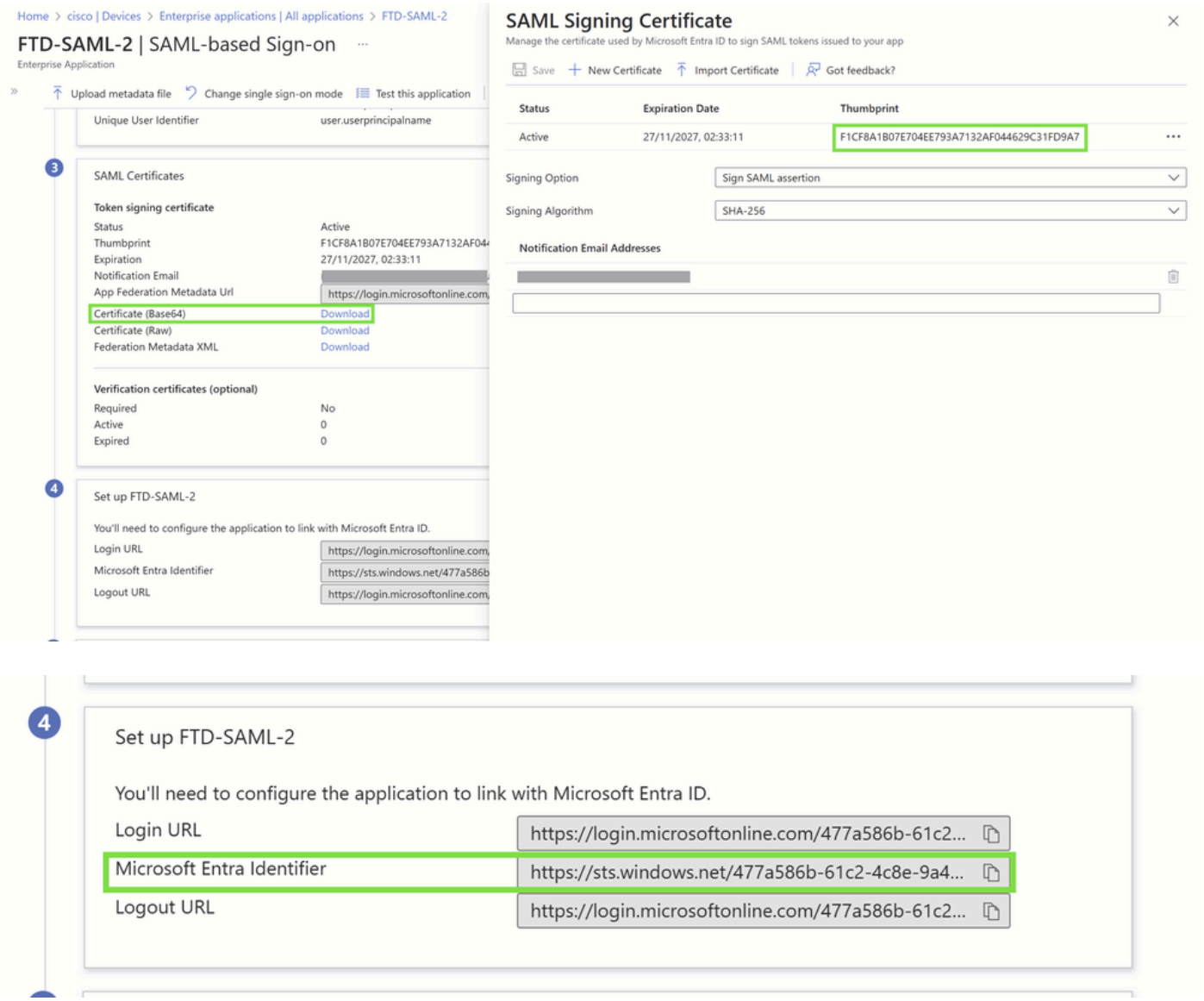

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end
implement. Choose SAML single sign-on whenever possible for existing applications that do
more.
Read the configuration guide for help integrating FTD-SAML-1.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
Optional
Optional
Optional
2
Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
Basic SAML Configuration
Save
Got feedback?
Identifier (Entity ID) *
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
Default
https://.cisco.com/saml/sp/metadata/FTD-SAML-1
Add identifier
Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup
Reply URL (Assertion Consumer Service URL) *
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.
Index
Default
https://.cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-1
Add reply URL
Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS
Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.
Enter a sign on URL
Relay State (Optional)
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
Enter a relay state


Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
App Federation Metadata Url
https://login.microsoftonline.com/
Certificate (Base64)
Download
Certificate (Raw)
Download
Federation Metadata XML
Download
Verification certificates (optional)
Required
No
Active
0
Expired
0
4
Set up FTD-SAML-1
You'll need to configure the application to link with Microsoft Entra ID.
Login URL
https://login.microsoftonline.com/
Microsoft Entra Identifier
https://sts.windows.net/477a586b
Logout URL
https://login.microsoftonline.com/
5
Test single sign-on with FTD-SAML-1
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
25/11/2027, 18:23:11
3125987754C6B7CCBE86DD214BDA5E50A13C211B
Signing Option
Sign SAML assertion
Signing Algorithm
SHA-256
Notification Email Addresses


4
Set up FTD-SAML-1
You'll need to configure the application to link with Microsoft Entra ID.
Login URL
https://login.microsoftonline.com/477a586b-61c2...
Microsoft Entra Identifier
https://sts.windows.net/477a586b-61c2-4c8e-9a4...
Logout URL
https://login.microsoftonline.com/477a586b-61c2...
5

FTD-SAML-2


Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-2
FTD-SAML-2 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end
implement. Choose SAML single sign-on whenever possible for existing applications that do
more.
Read the configuration guide for help integrating FTD-SAML-2.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
Optional
Optional
Optional
2
Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Thumbprint
Expiration
Active
27/11/2027, 02:33:11
Basic SAML Configuration
Save
Got feedback?
Identifier (Entity ID) *
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
Default
.cisco.com/saml/sp/metadata/FTD-SAML-2
Add identifier
Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup
Reply URL (Assertion Consumer Service URL) *
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.
Index
Default
.cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-2
Add reply URL
Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS
Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.
Enter a sign on URL
Relay State (Optional)
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
Enter a relay state



이제 Microsoft Entra를 ID 공급자로 사용하여 SAML 인증을 구성하는 데 필요한 정보와 파일이 있는지 확인하십시오.

Microsoft Entra Identifier를 찾습니다.

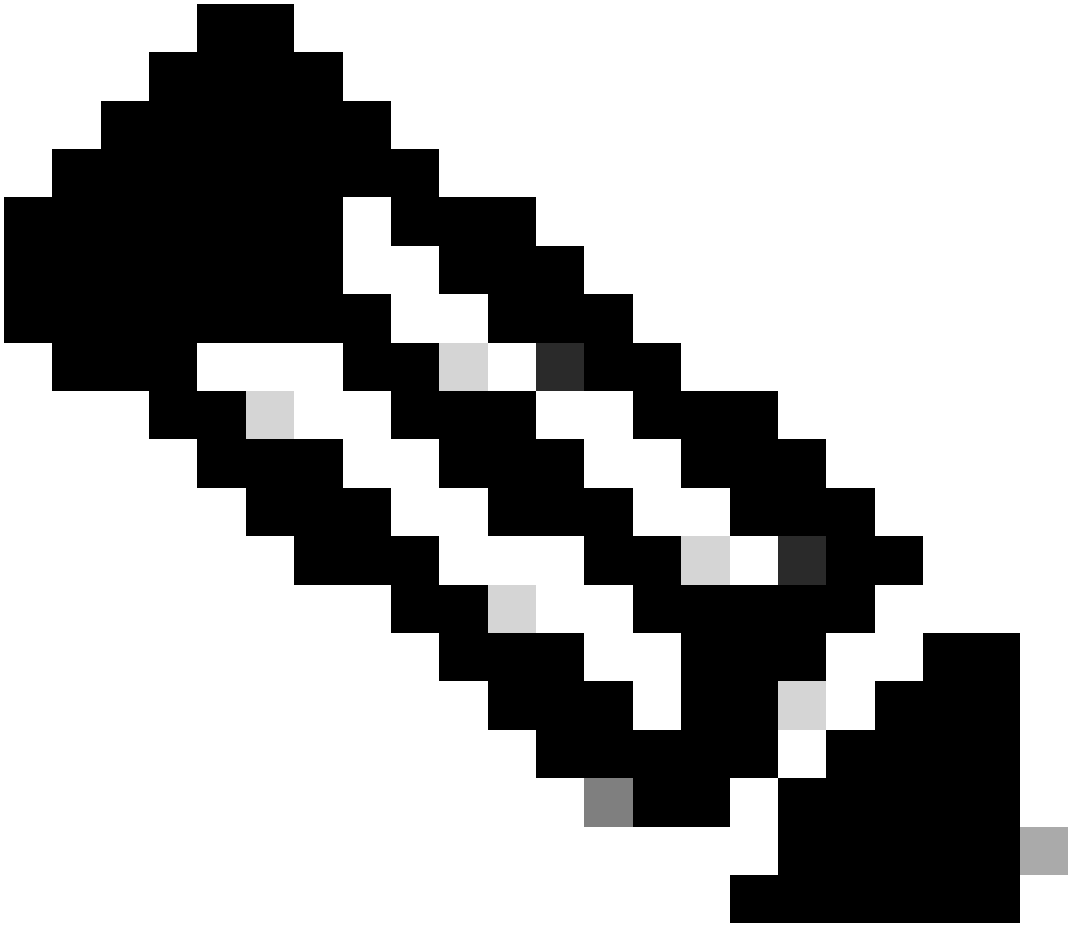
Microsoft Entra 포털에서 두 SAML 엔터프라이즈 애플리케이션에 대한 설정에 액세스합니다.

두 애플리케이션 모두에서 일관되게 유지되며 SAML 컨피그레이션에 중요한 Microsoft Entra Identifier를 확인합니다.

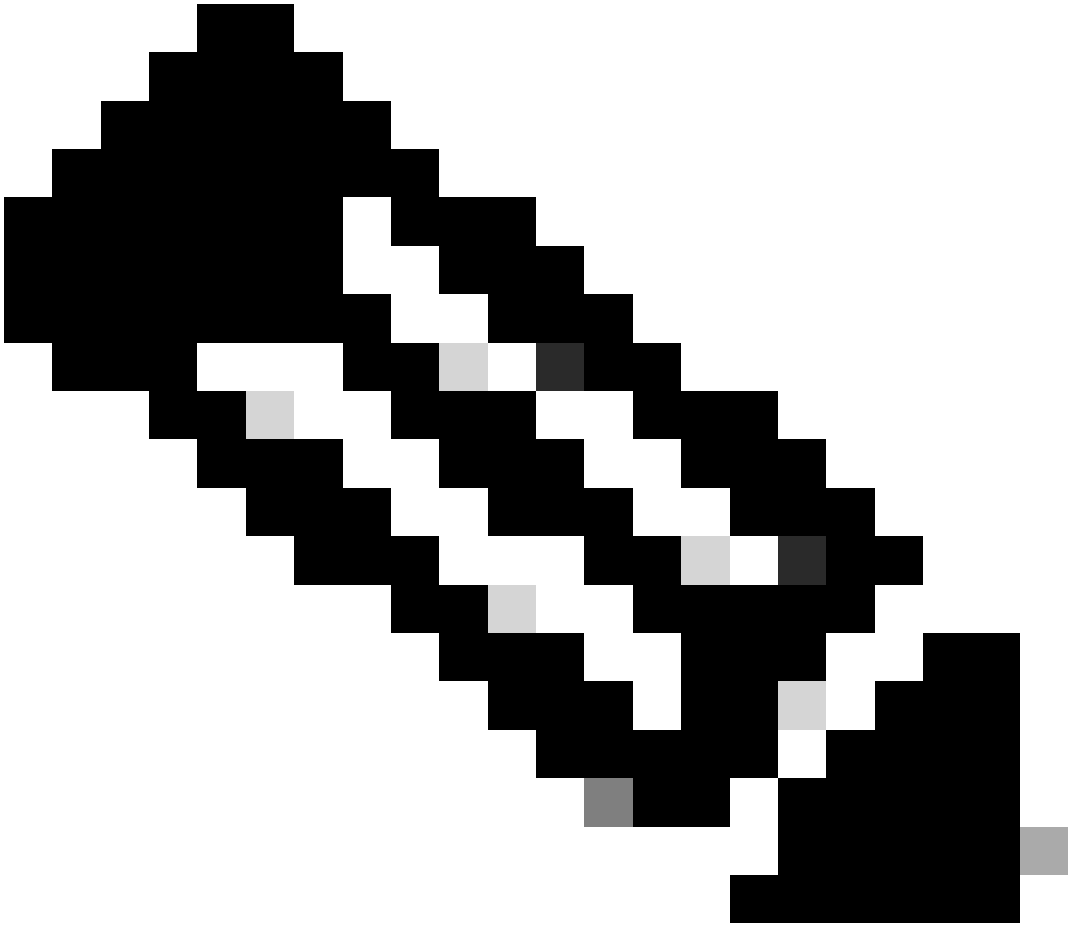
Base64 IdP 인증서 다운로드:

구성된 각 SAML 엔터프라이즈 애플리케이션으로 이동합니다.

각 Base64 인코딩 IdP 인증서를 다운로드합니다. 이러한 인증서는 ID 제공자와 Cisco VPN 설정 간의 신뢰를 구축하는 데 필수적입니다.



참고: FTD 연결 프로파일에 필요한 이러한 모든 SAML 컨피그레이션은 각 애플리케이션의 IdP에서 제공하는 metadata.xml 파일에서도 소싱할 수 있습니다.



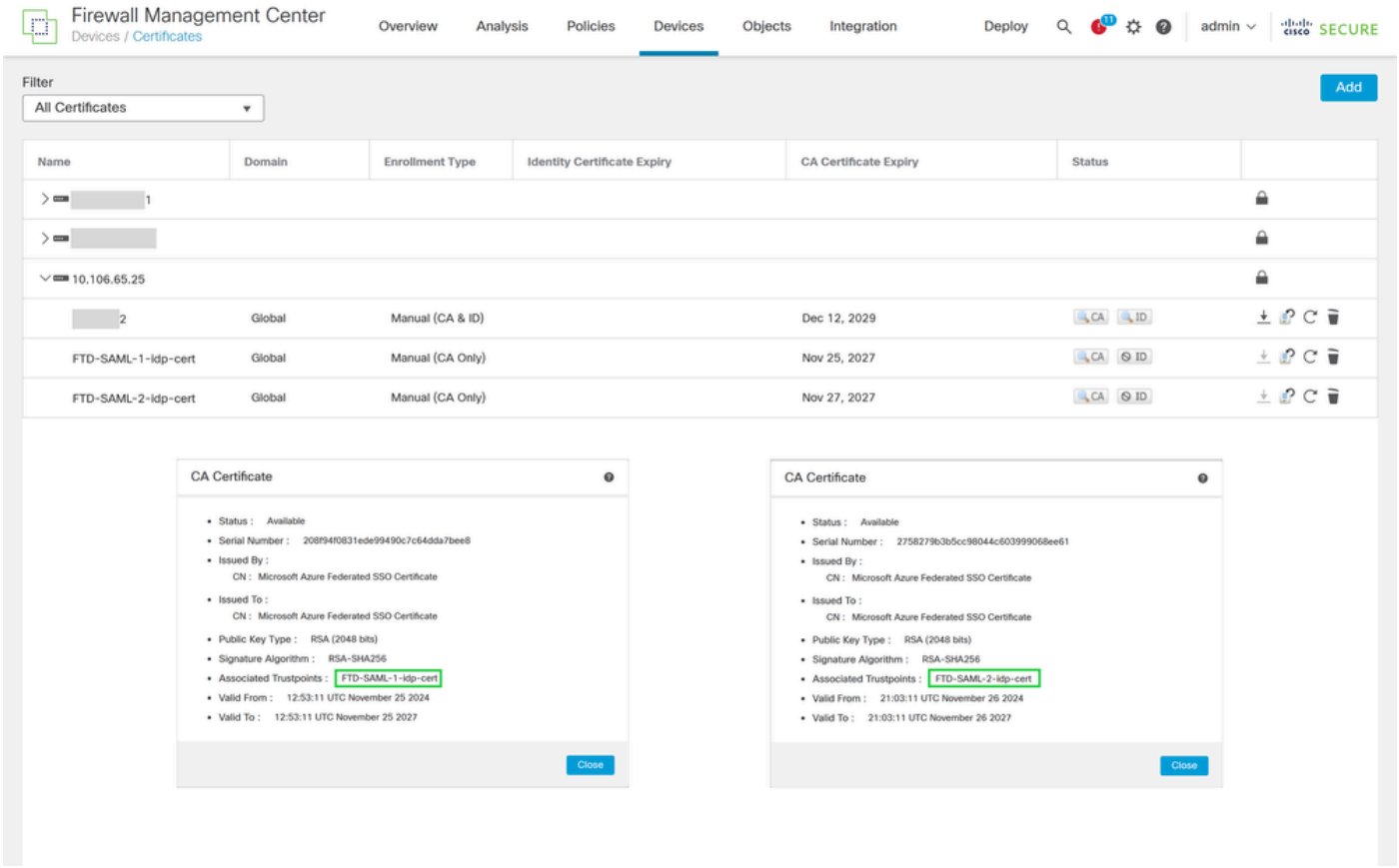
참고: 사용자 지정 IdP 인증서를 사용하려면 사용자 지정 생성 IdP 인증서를 IdP 및 FMC 모두에 업로드해야 합니다. Azure IdP의 경우 인증서가 PKCS#12 형식인지 확인합니다. FMC에서 PKCS#12 파일이 아닌 IdP의 ID 인증서만 업로드합니다. 자세한 지침은 Cisco 설명서의 "Azure 및 FDM에 PKCS#12 파일 업로드" 섹션을 참조하십시오. FDM에서 SAML 인증을 사용하여 여러 RAVPN 프로파일 구성

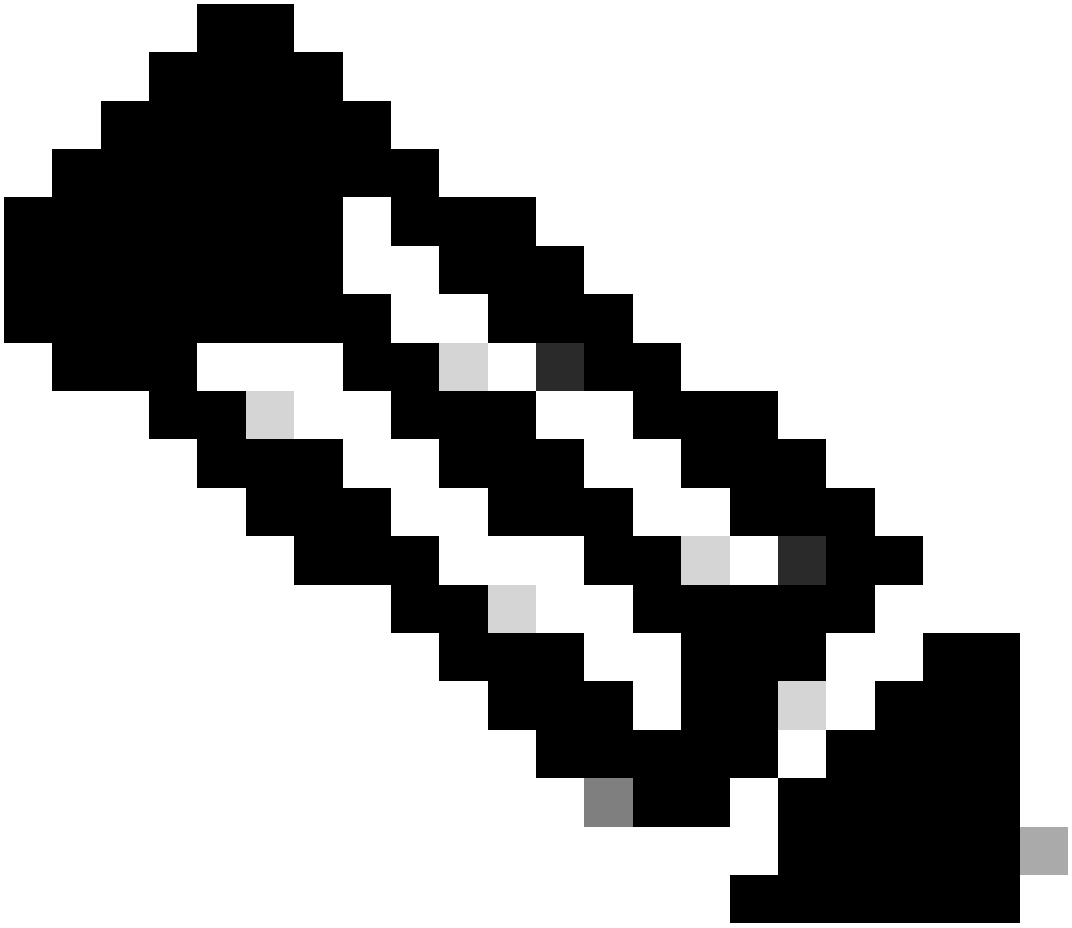
FMC를 통한 FTD 컨피그레이션

IdP 인증서 등록:

FMC 내의 인증서 관리 섹션으로 이동하여 두 SAML 애플리케이션에 대해 다운로드된 Base64 인코딩 IdP 인증서를 등록합니다. 이러한 인증서는 신뢰를 설정하고 SAML 인증을 활성화하는 데 매우 중요합니다.

자세한 지침은 다음 Cisco 문서에서 "FMC를 통한 FTD 구성"의 처음 두 단계를 참조하십시오. FMC를 통해 관리되는 FTD에서 SAML 인증을 사용하여 보안 클라이언트를 구성합니다.


Firewall Management Center
Devices / Certificates
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Filter
All Certificates
Add
Name
Domain
Enrollment Type
Identity Certificate Expiry
CA Certificate Expiry
Status
10.106.65.25
Global
Manual (CA & ID)
Dec 12, 2029
FTD-SAML-1-idp-cert
Global
Manual (CA Only)
Nov 25, 2027
FTD-SAML-2-idp-cert
Global
Manual (CA Only)
Nov 27, 2027
CA Certificate
Status : Available
Serial Number : 208f94f0831ede99490c7c64dda7bee8
Issued By :
CN : Microsoft Azure Federated SSO Certificate
Issued To :
CN : Microsoft Azure Federated SSO Certificate
Public Key Type : RSA (2048 bits)
Signature Algorithm : RSA-SHA256
Associated Trustpoints : FTD-SAML-1-idp-cert
Valid From : 12:53:11 UTC November 25 2024
Valid To : 12:53:11 UTC November 25 2027
Close
CA Certificate
Status : Available
Serial Number : 2758279b3b5cc98044c603999068ee61
Issued By :
CN : Microsoft Azure Federated SSO Certificate
Issued To :
CN : Microsoft Azure Federated SSO Certificate
Public Key Type : RSA (2048 bits)
Signature Algorithm : RSA-SHA256
Associated Trustpoints : FTD-SAML-2-idp-cert
Valid From : 21:03:11 UTC November 26 2024
Valid To : 21:03:11 UTC November 26 2027
Close



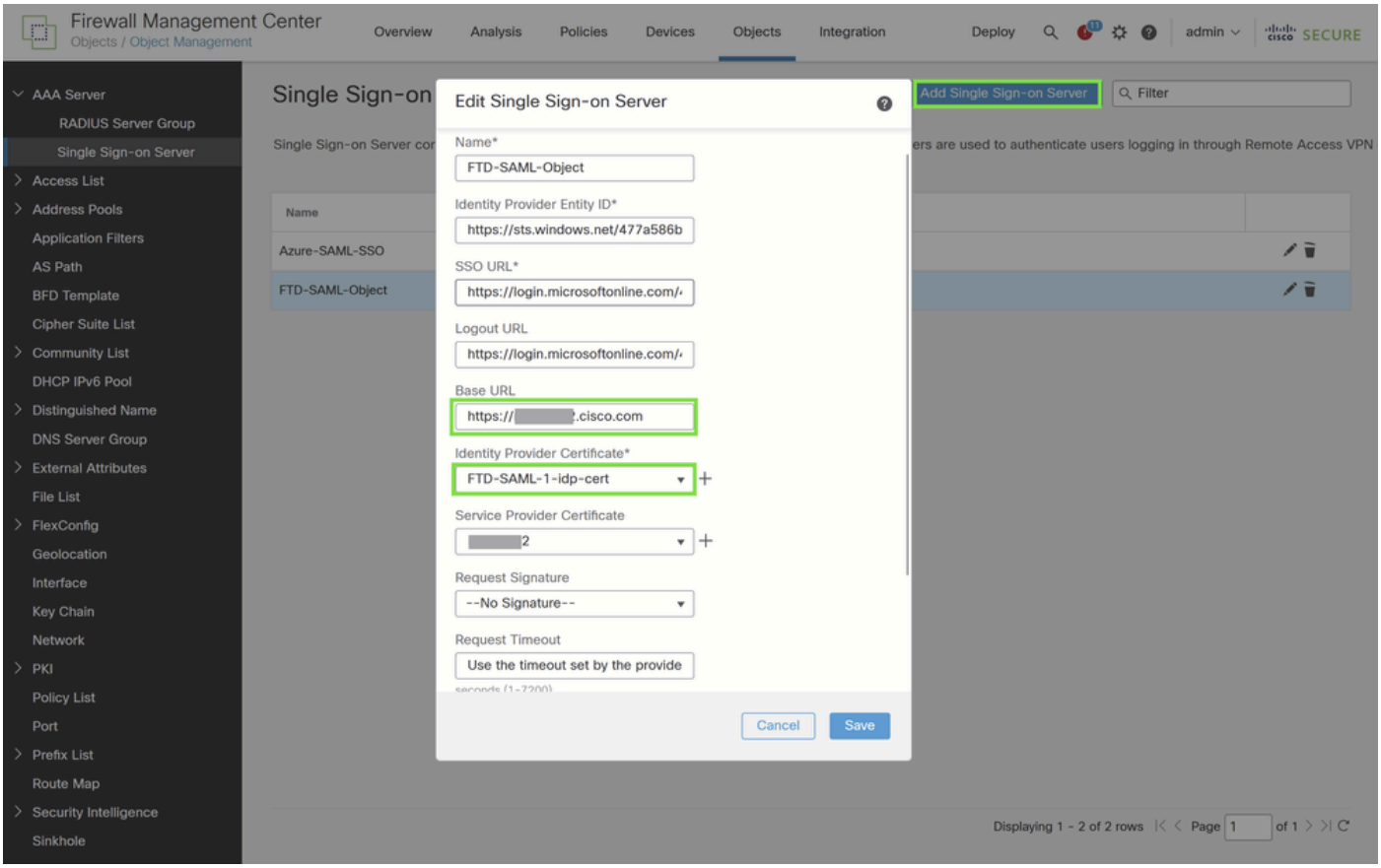
참고: 더 나은 보기를 위해 두 인증서를 동시에 표시하도록 이미지가 편집되었습니다. FMC에서는 두 인증서를 동시에 열 수 없습니다.

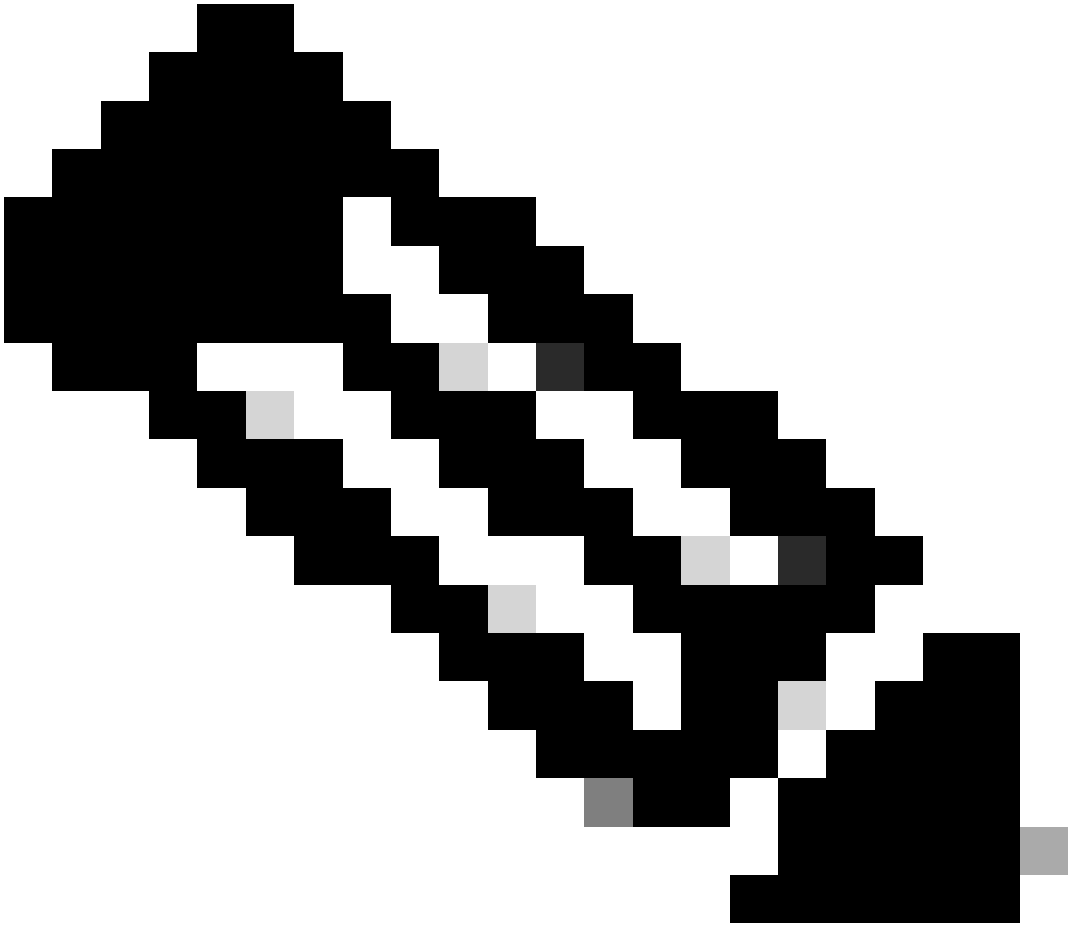
FMC를 통해 Cisco FTD에서 SAML 서버 설정 구성

FMC(Firepower Management Center)를 사용하여 Cisco FTD(Firepower Threat Defense)에서 SAML 서버 설정을 구성하려면 다음 단계를 구현합니다.

1. Single Sign-on Server Configuration(단일 로그인 서버 컨피그레이션)으로 이동합니다.
   - Objects(개체) > Object Management(개체 관리) > AAA Servers(AAA 서버) > Single Sign-on Server(단일 로그인 서버)로 이동합니다.
   - Add Single Sign-on Server(단일 로그인 서버 추가)를 클릭하여 새 서버 구성을 시작합니다.
2. SAML 서버 설정을 구성합니다.
   - SAML 엔터프라이즈 응용 프로그램에서 수집되거나 IdP(ID 공급자)에서 다운로드한 metadata.xml 파일에서 수집된 매개변수를 사용하여 New Single Sign-on Server 양식에 필요한 SAML 값을 입력합니다.

- 구성할 주요 매개변수는 다음과 같습니다.
  - SAML 공급자 엔티티 ID: metadata.xml의 entityID
  - SSO URL: metadata.xml의 SingleSignOnService
  - 로그아웃 URL: metadata.xml의 SingleLogoutService.
  - 기본 URL: FTD SSL ID 인증서의 FQDN.
  - ID 공급자 인증서: IdP 서명 인증서
    - Identity Provider Certificate(ID 제공자 인증서) 섹션에서 등록된 IdP 인증서 중 하나를 연결합니다
    - 이 활용 사례에서는 FTD-SAML-1 애플리케이션의 IdP 인증서를 사용합니다 .
  - 서비스 공급자 인증서: FTD 서명 인증서



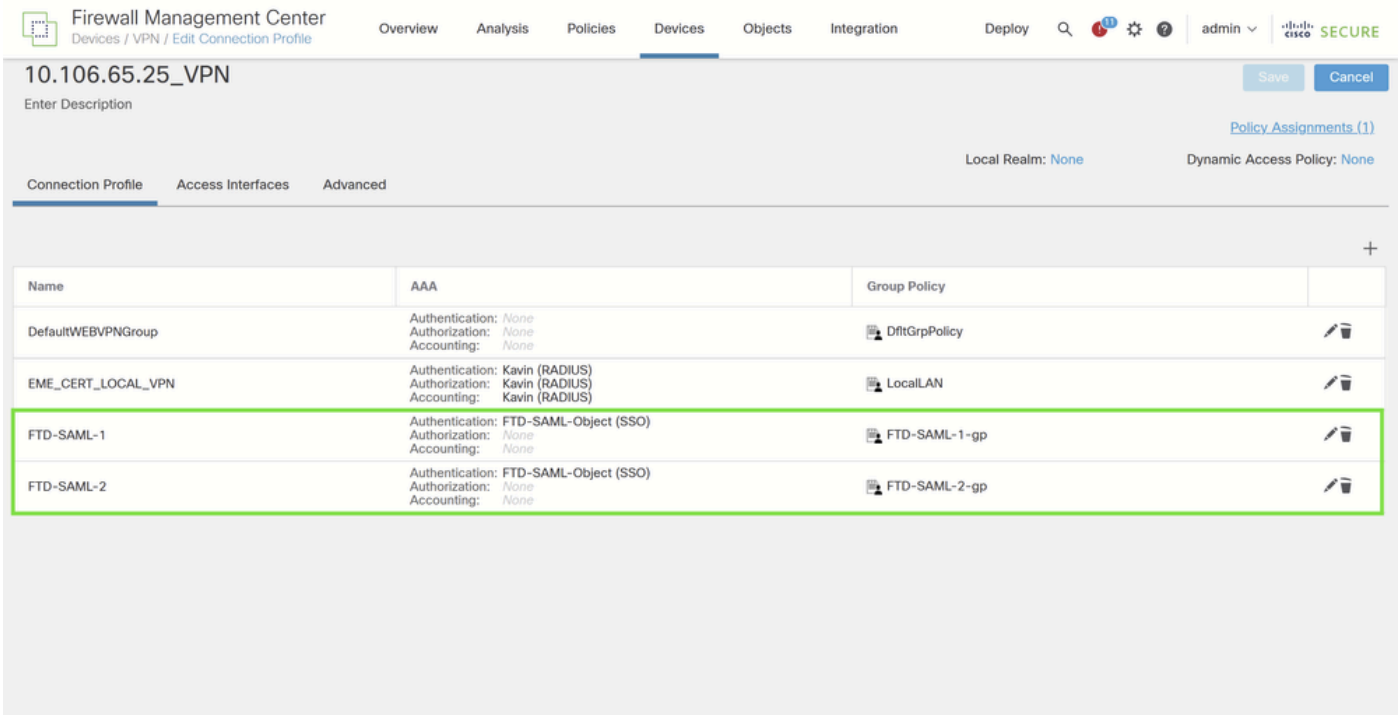


참고: 현재 컨피그레이션에서는 연결 프로파일 설정 내의 SAML 객체에서 ID 제공자 인증서만 재정의할 수 있습니다. 안타깝게도 "로그인 시 IdP 재인증 요청" 및 "내부 네트워크에서만 액세스 가능한 IdP 활성화"와 같은 기능은 각 연결 프로파일에 대해 개별적으로 활성화하거나 비활성화할 수 없습니다.

FMC를 통해 Cisco FTD에서 연결 프로파일 구성

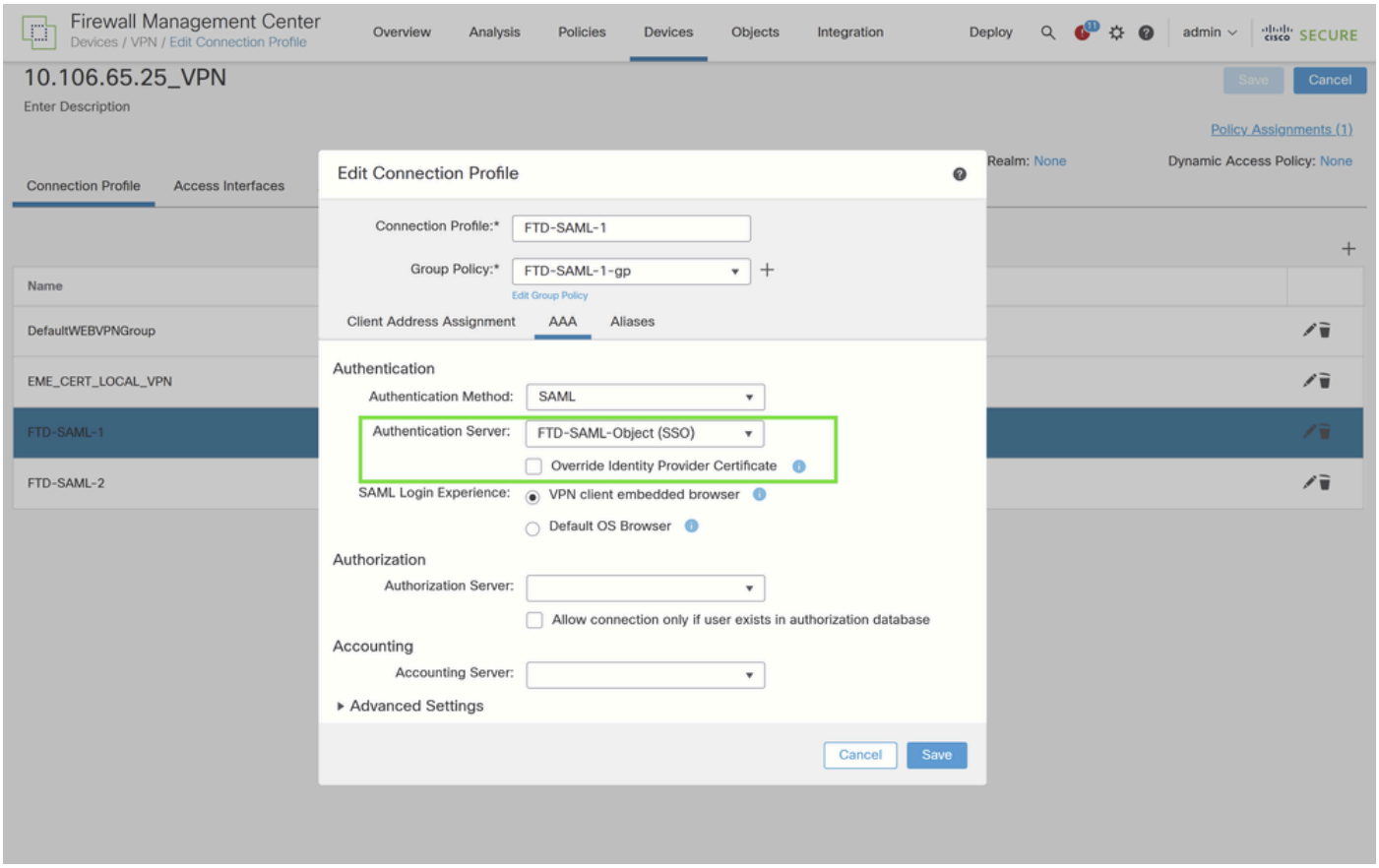
SAML 인증 설정을 완료하려면 적절한 매개변수로 연결 프로파일을 구성하고 이전에 구성된 SAML 서버를 사용하여 AAA 인증을 SAML로 설정해야 합니다.

자세한 지침은 Cisco 설명서의 "FMC를 통한 FTD 구성"에서 다섯 번째 단계를 참조하십시오. FMC를 통해 관리되는 FTD에서 SAML 인증을 사용하여 보안 클라이언트를 구성합니다.



첫 번째 연결 프로파일에 대한 AAA 컨피그레이션 추출

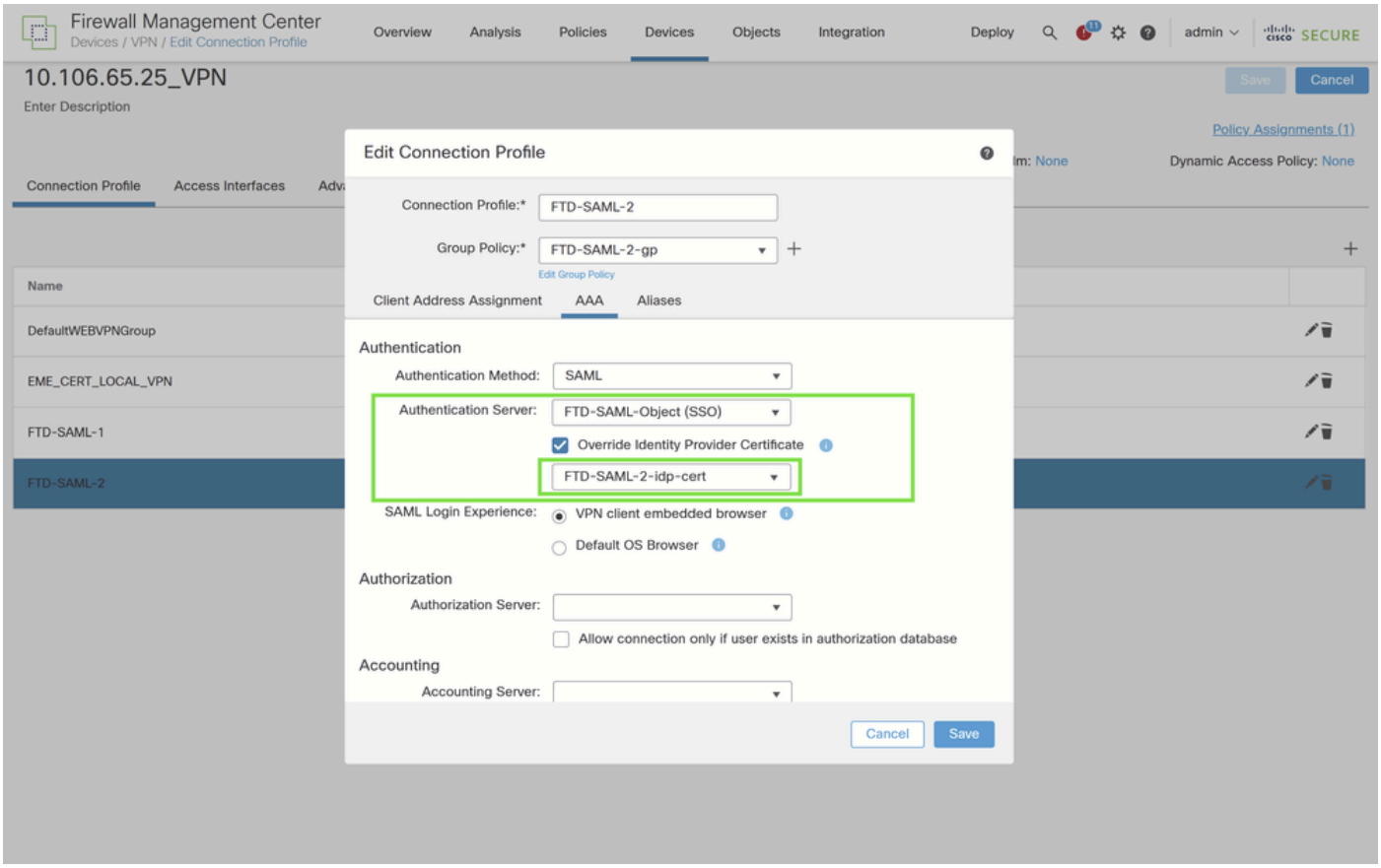
첫 번째 연결 프로파일에 대한 AAA 컨피그레이션 설정의 개요는 다음과 같습니다.



Cisco FTD에서 두 번째 연결 프로파일에 대한 IdP 인증서 재정의 구성
올바른 IdP(Identity Provider) 인증서가 두 번째 연결 프로파일에 사용되도록 하려면 다음 단계를 완료하여 IdP 인증서 재정의를 활성화합니다.

연결 프로파일 설정에서 "Override Identity Provider Certificate(ID 공급자 인증서 재정의)" 옵션을 찾아 활성화하여 SAML 서버에 구성된 것과 다른 IdP 인증서를 사용하도록 허용합니다.

등록된 IdP 인증서 목록에서 FTD-SAML-2 애플리케이션에 대해 특별히 등록된 인증서를 선택합니다. 이렇게 선택하면 이 연결 프로파일에 대한 인증 요청이 이루어질 때 올바른 IdP 인증서가 사용됩니다.



컨피그레이션 구축

SAML**Deploy** > **Deployment**인증 VPN 변경 사항을 적용할 적절한 FTD를 탐색하고 선택합니다.

다음을 확인합니다.

FTD 명령줄의 컨피그레이션

<#root>

```
firepower# sh run 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
    Secure Client image disk0:/csm/Secure Client-win-4.10.08025-webdeploy.pkg 1 regex "Windows"
    Secure Client enable


 saml idp https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/


        url sign-in https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2


        url sign-out https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2


        base-url https://nigarapa2.cisco.com


        trustpoint idp FTD-SAML-1-idp-cert


        trustpoint sp nigarapa2


        no signature


        force re-authentication


    tunnel-group-list enable
    cache
        disable
    error-recovery disable
firepower#
```

<#root>

```
firepower# sh run tunnel-group FTD-SAML-1
tunnel-group FTD-SAML-1 type remote-access
tunnel-group FTD-SAML-1 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-1-gp
tunnel-group FTD-SAML-1 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-1 enable


saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/


firepower#
```

<#root>

```
firepower# sh run tunnel-group FTD-SAML-2
tunnel-group FTD-SAML-2 type remote-access
tunnel-group FTD-SAML-2 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-2-gp
tunnel-group FTD-SAML-2 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-2 enable
```

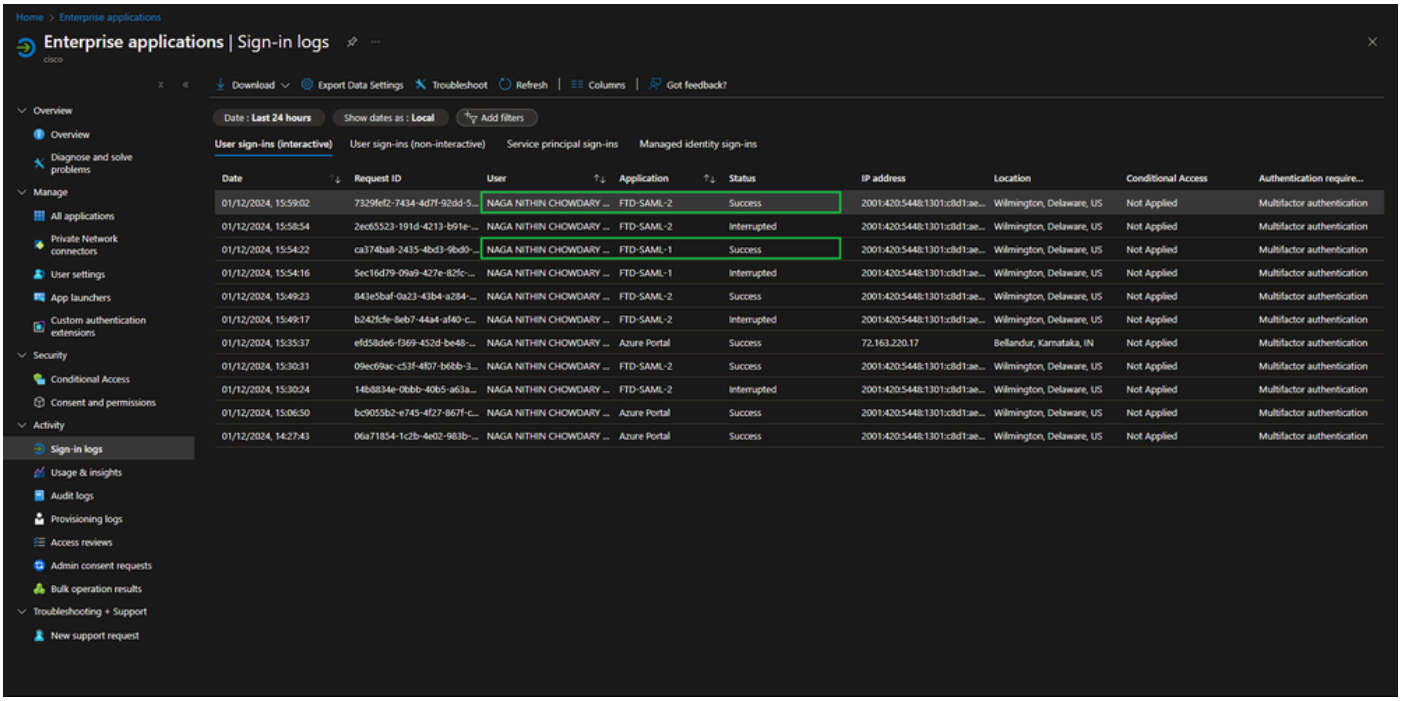
saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/

saml idp-trustpoint FTD-SAML-2-idp-cert

```
firepower#
```

Azure Entra 식별자의 로그인 로그

엔터프라이즈 애플리케이션 아래의 로그인 로그 섹션에 액세스합니다. FTD-SAML-1 및 FTD-SAML-2와 같은 특정 연결 프로파일과 관련된 인증 요청을 찾습니다. 각 연결 프로파일과 연결된 SAML 응용 프로그램을 통해 사용자가 성공적으로 인증되고 있는지 확인하십시오.



Azure IdP의 로그인 로그

문제 해결

1. 보안 클라이언트 사용자 PC에서 DART를 사용하여 문제를 해결할 수 있습니다.
2. SAML 인증 문제를 해결하려면 다음 디버그를 활용하십시오.

<#root>

```
firepower#
 debug webvpn saml 255
```

3. 위에서 설명한 대로 보안 클라이언트 컨피그레이션을 확인합니다. 이 명령을 사용하여 인증서를 확인할 수 있습니다.

<#root>

```
firepower#
 show crypto ca certificate
```

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.