ASA에서 SAML을 사용하여 여러 터널 그룹 구성

목차

소개

이 문서에서는 Cisco ASA의 여러 터널 그룹에 대한 Azure Identity Provider를 사용한 SAML 인증에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- ASA(Adaptive Security Appliance)
- SAML(Security Assertion Markup Language)
- SSL(Secure Socket Layer) 인증서
- Microsoft Azure

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 9.22(1)1
- SAML 2.0의 Microsoft Azure Entra ID
- Cisco Secure Client 5.1.7.80

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Microsoft Azure는 동일한 엔터티 ID에 대해 여러 응용 프로그램을 지원할 수 있습니다. 각 애플리케이션(다른 터널 그룹에 매핑됨)에는 고유한 인증서가 필요합니다. ASA에서는 IdP 인증서 기능 때문에 여러 터널 그룹이 서로 다른 IdP(Override Identity Provider) 보호 애플리케이션을 사용하도록 구성할 수 있습니다. 이 기능을 사용하면 관리자가 SSO(Single Sign-On) 서버 개체의 기본 IdP 인증서를 각 터널 그룹에 대한 특정 IdP 인증서로 재정의할 수 있습니다. 이 기능은 ASA에서 9.17.1 버전 이후에 도입되었습니다.

SAML SP에서 시작한 SSO

최종 사용자가 ASA에 액세스하여 로그인을 시작하면 다음과 같이 로그인 동작이 진행됩니다.

1. VPN 사용자가 SAML 사용 터널 그룹에 액세스하거나 선택하는 경우 최종 사용자는 인증을 위해 SAML IdP로 리디렉션됩니다. 사용자가 그룹 URL에 직접 액세스하지 않으면 메시지가 표시됩니다. 이 경우 리디렉션이 무음입니다.

2. ASA에서 SAML 인증 요청을 생성하며, 브라우저가 SAML IdP로 리디렉션합니다.

3. IdP가 최종 사용자에게 자격 증명에 대한 챌린지를 요청하고 최종 사용자가 로그인합니다. 입력한 자격 증명은 IdP 인증 컨피그레이션을 충족해야 합니다.

4. IdP 응답이 브라우저로 다시 전송되어 ASA 로그인 URL에 게시됩니다. ASA는 로그인을 완료하기 위해 응답을 확인합니다.

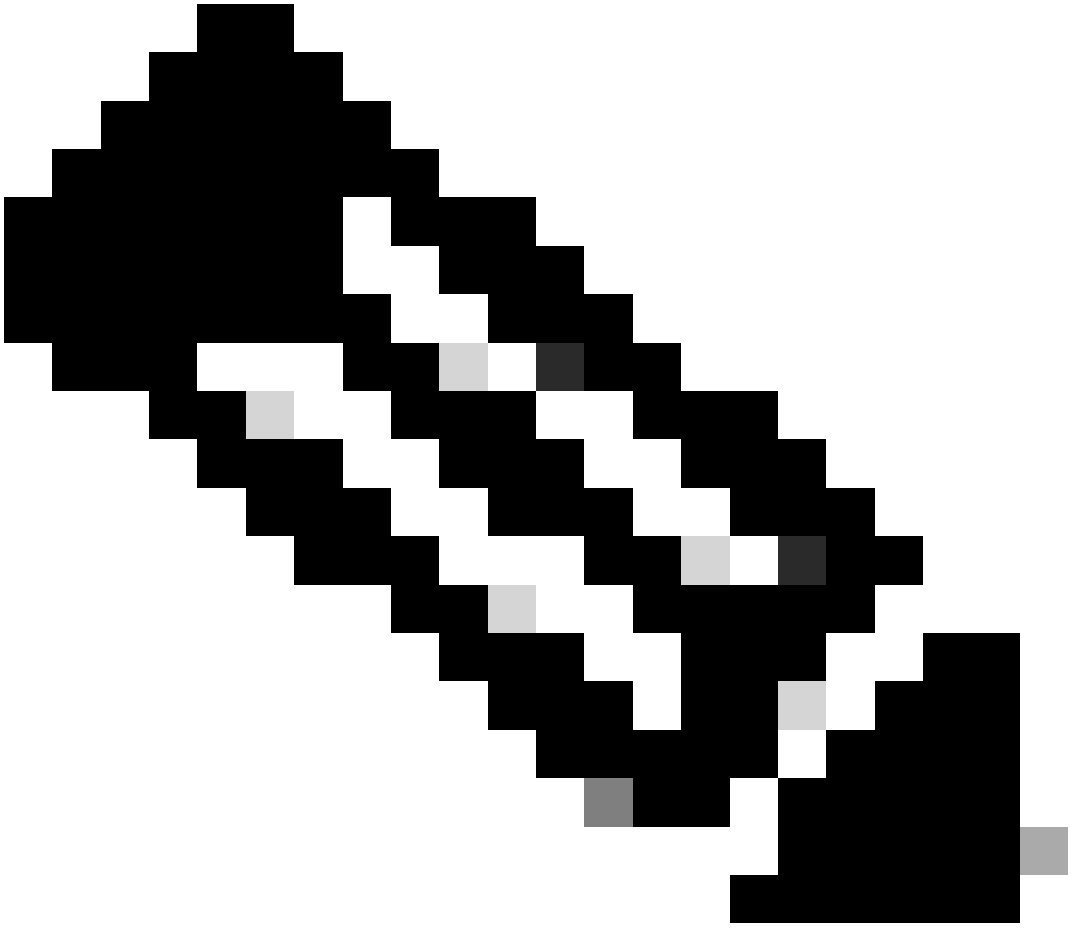
설정

갤러리에서 Cisco Secure Firewall - Secure Client 추가

이 예에서는 Microsoft Entra SSO와 Cisco Secure Firewall - Secure Client on Azure가 ASA에 구성된 두 개의 터널 그룹에 대해 추가됩니다.

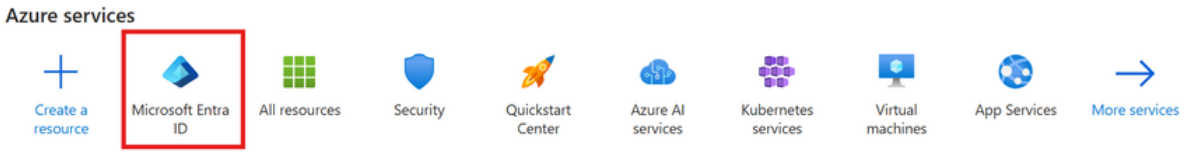
- SAML1
- SAML2

Cisco Secure Firewall - Secure Client를 Microsoft Centera ID에 통합하려면 갤러리의 Cisco Secure Firewall - Secure Client를 관리되는 SaaS 앱 목록에 추가해야 합니다.



참고: 이 단계는 첫 번째 터널 그룹인 SAML1의 갤러리에 Cisco Secure Firewall - Secure Client를 추가하는 단계입니다.

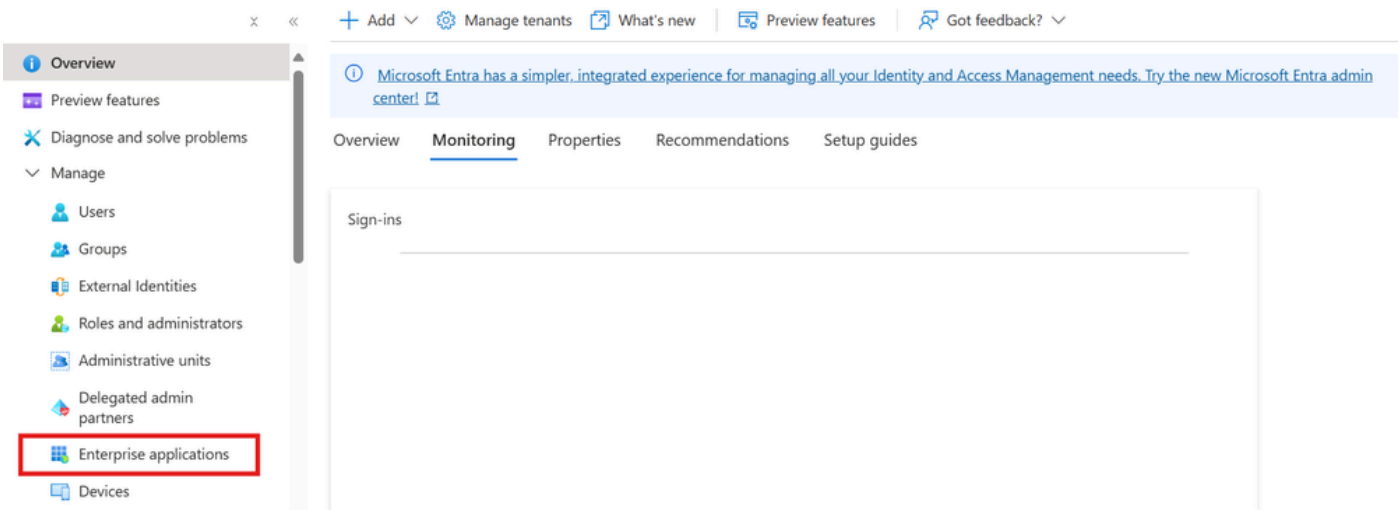
1단계. Azure Portal에 로그인하고 Microsoft Entra ID를 선택합니다.



Microsoft Entra ID

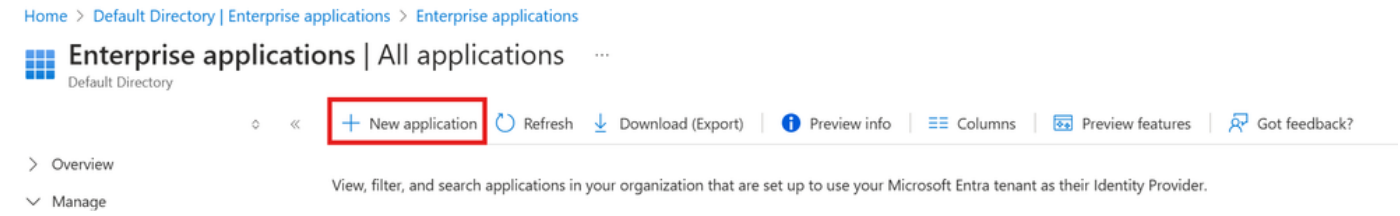
2단계. 이 이미지에 표시된 대로 Enterprise Applications(엔터프라이즈 애플리케이션)를 선택합니

다.



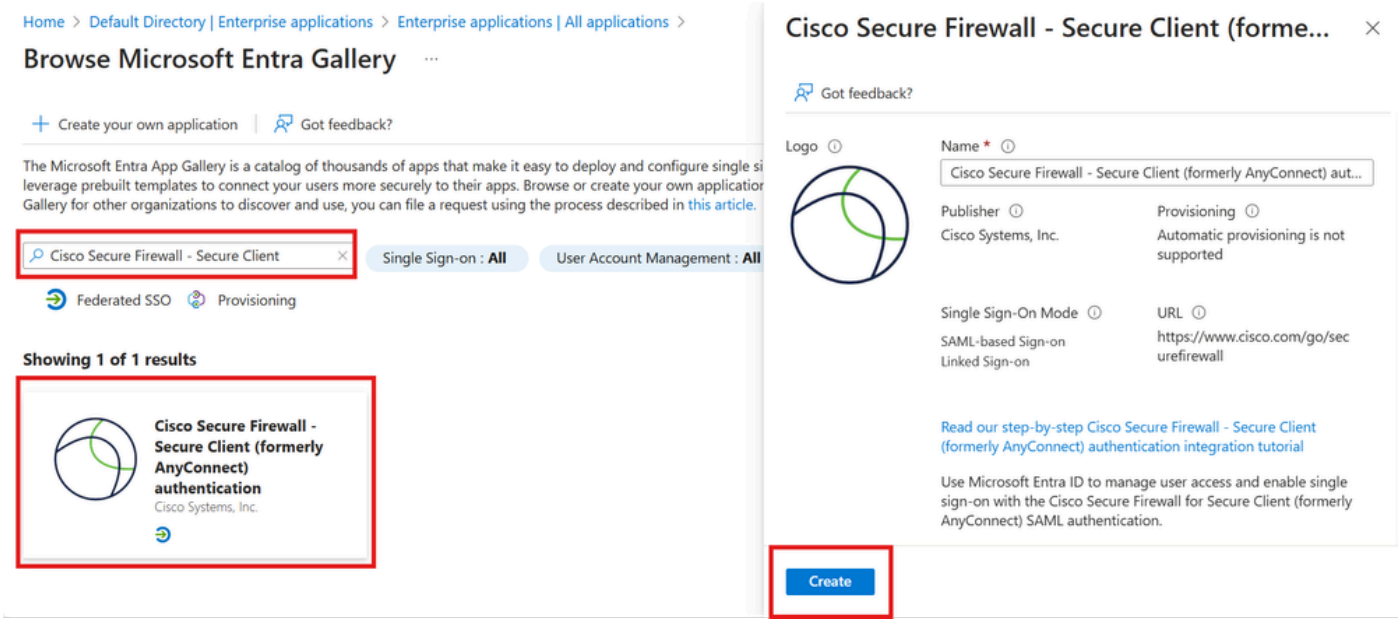
엔터프라이즈 애플리케이션

3단계. 이제 이 이미지에 표시된 대로 New Application(새 애플리케이션)을 선택합니다.



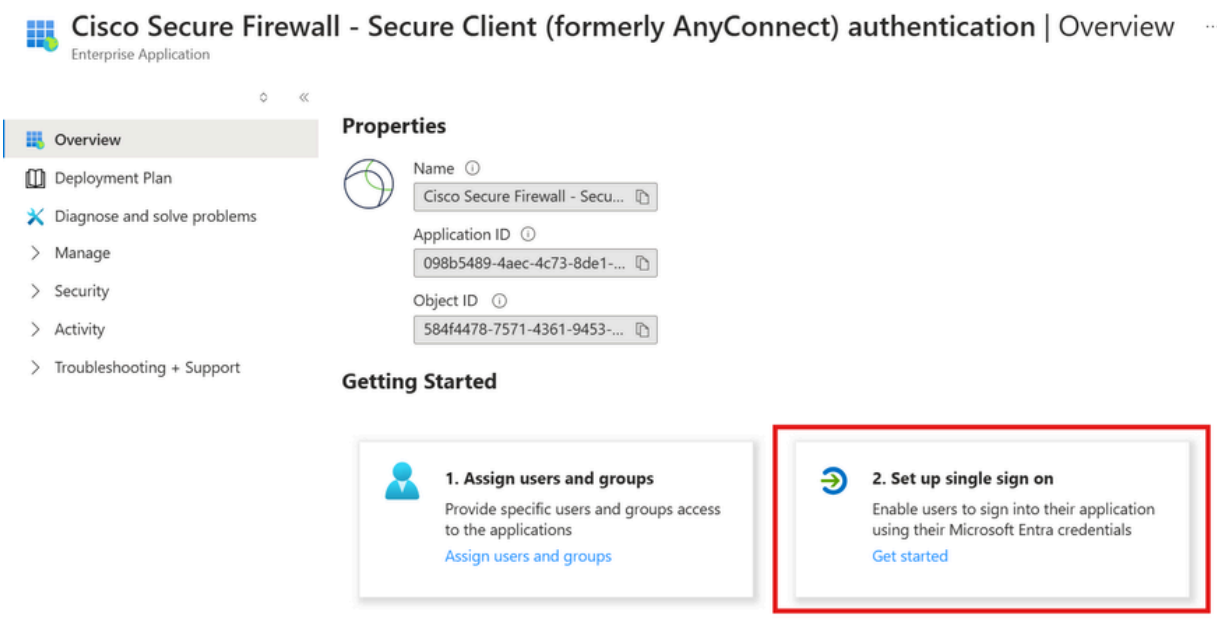
새 응용 프로그램

4단계. Add from the gallery(갤러리의 추가) 섹션에서 검색 상자에 Cisco Secure Firewall - Secure Client를 입력하고 결과 패널에서 Cisco Secure Firewall - Secure Client를 선택한 다음 앱을 추가합니다.



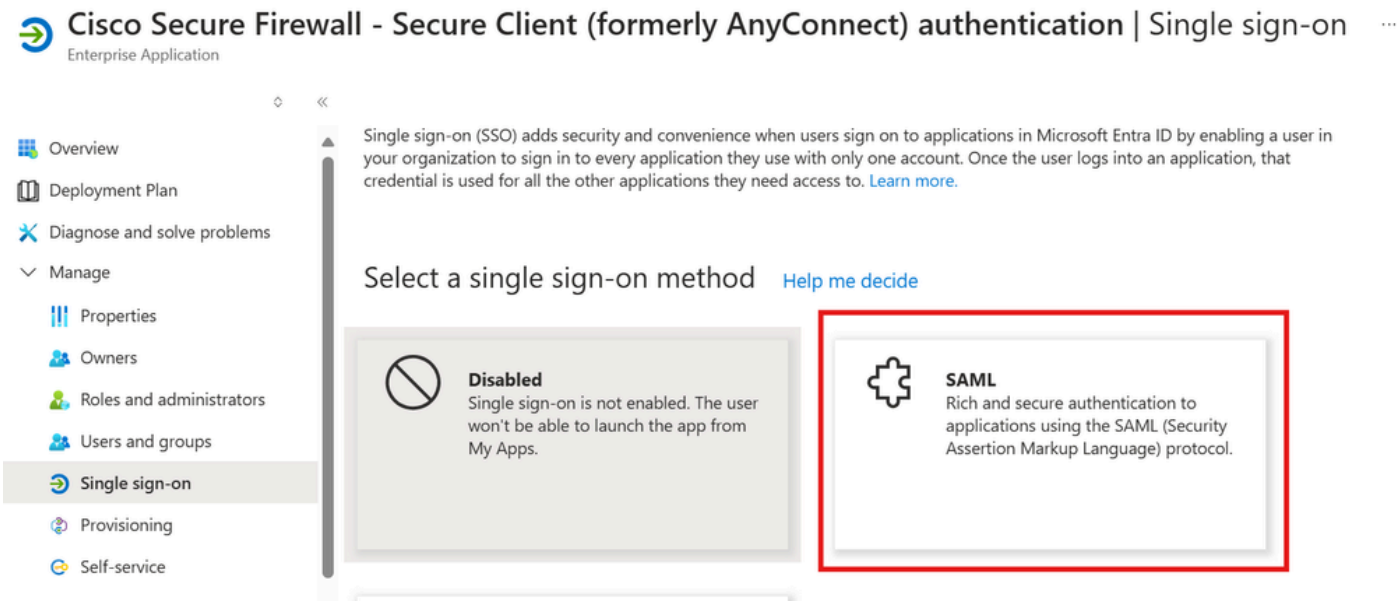
Cisco Secure Firewall - 보안 클라이언트

5단계. 이 이미지에 표시된 대로 Single Sign-on 메뉴 항목을 선택합니다.



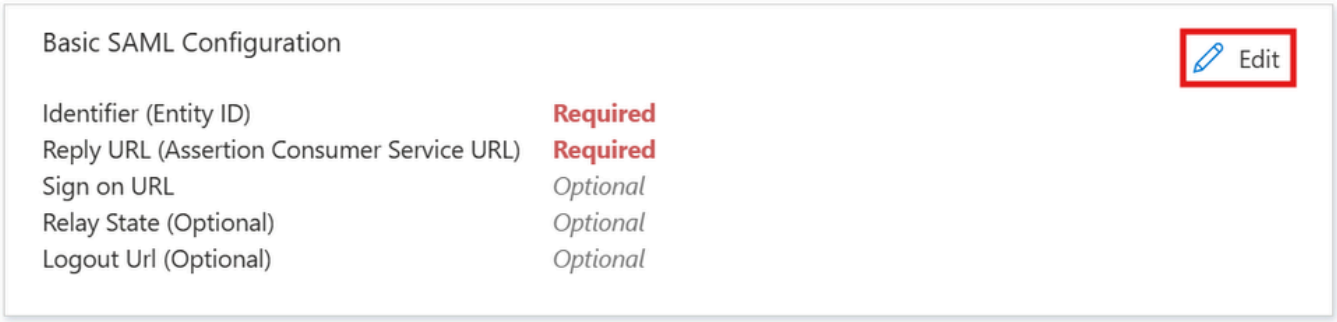
단일 로그인 설정

6단계. Select a single sign-on method(SSO 방식 선택) 페이지에서 SAML을 선택합니다.



SAML

7단계. 설정을 편집하려면 Set up single sign-on with SAML(SAML을 사용하여 단일 로그인 설정) 페이지에서 Basic SAML Configuration(기본 SAML 컨피그레이션)의 편집/펜 아이콘을 클릭합니다.



기본 Saml 컨피그레이션

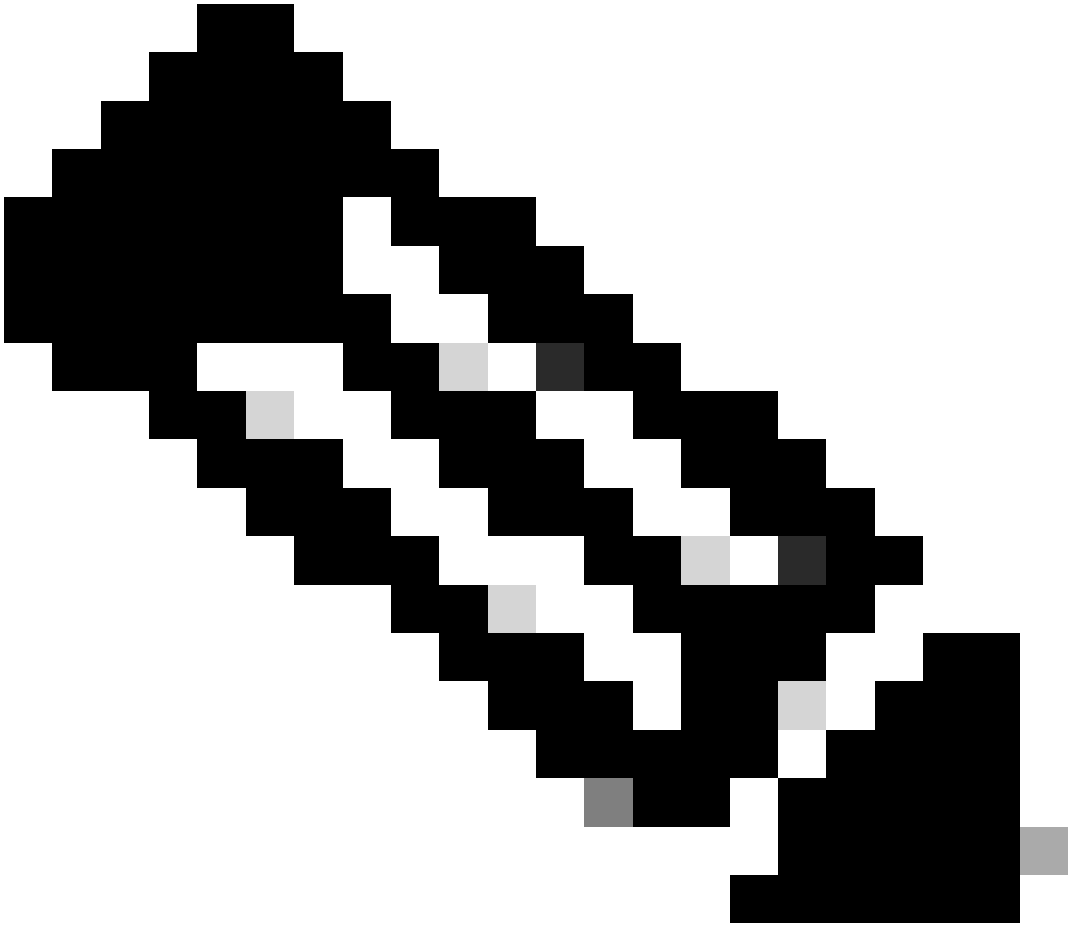
8단계. SAML을 사용하여 SSO 설정 페이지에서 다음 필드의 값을 입력합니다.

a. 식별자 텍스트 상자에 다음 패턴을 사용하여 URL을 입력합니다.

https://<VPN URL>/saml/sp/metadata/<Tunnel_Group_Name>

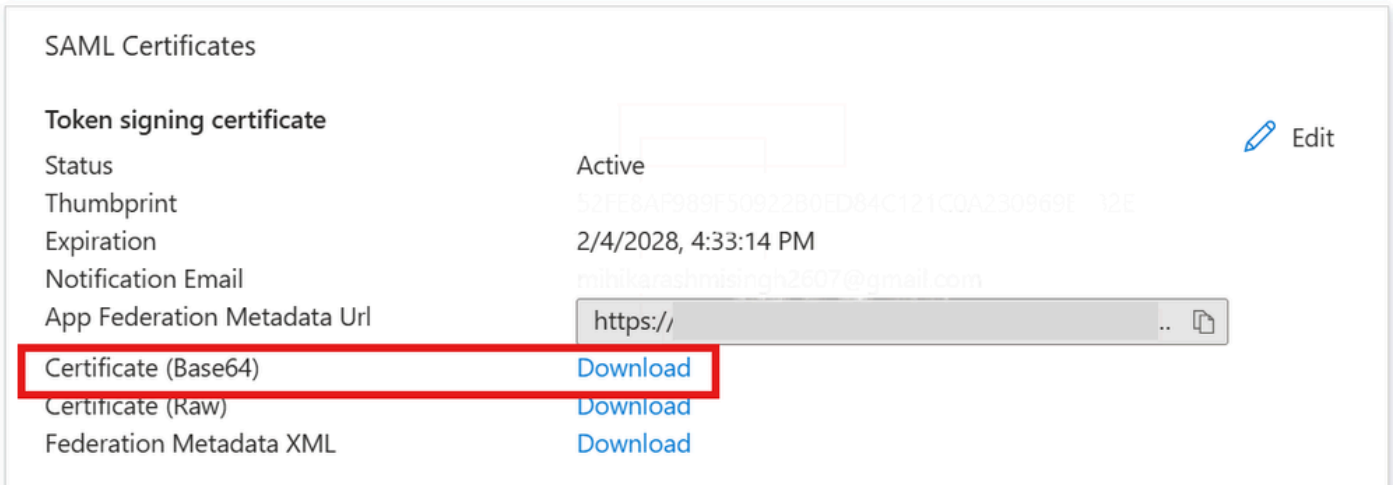
b. Reply URL(회신 URL) 텍스트 상자에 다음 패턴을 사용하여 URL을 입력합니다.

https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<Tunnel_Group_Name>
[Tunnel_Group_Name = SAML1]

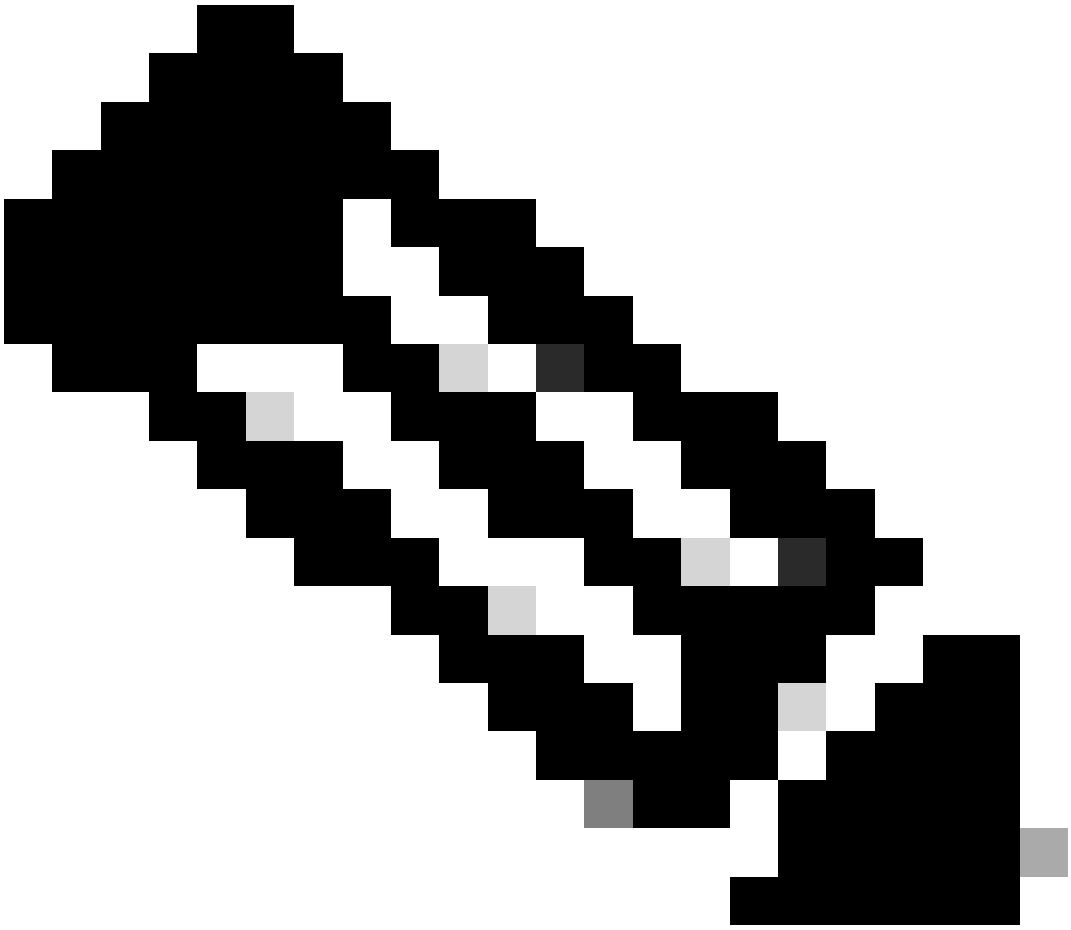


참고: Tunnel_Group_Name은 대/소문자를 구분하며 값에 점 '.'을 포함해서는 안 됩니다. 및 슬래시 '/'.

9단계. Set up single sign-on with SAML(SAML을 사용하여 단일 로그인 설정) 페이지의 SAML Signing Certificate(SAML 서명 인증서) 섹션에서 Certificate(Base64)를 찾고 Download(다운로드)를 선택하여 인증서 파일을 다운로드하고 컴퓨터에 저장합니다.



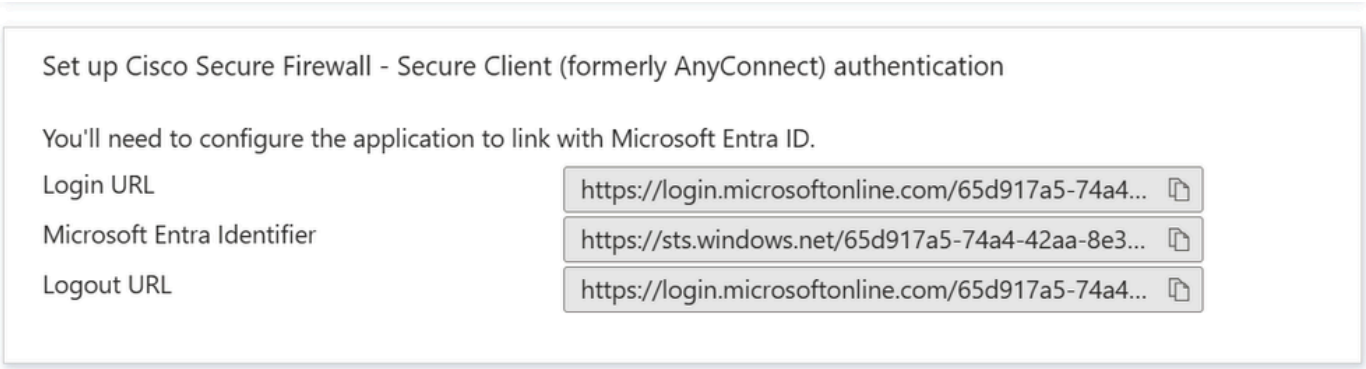
인증서(Base64) 다운로드



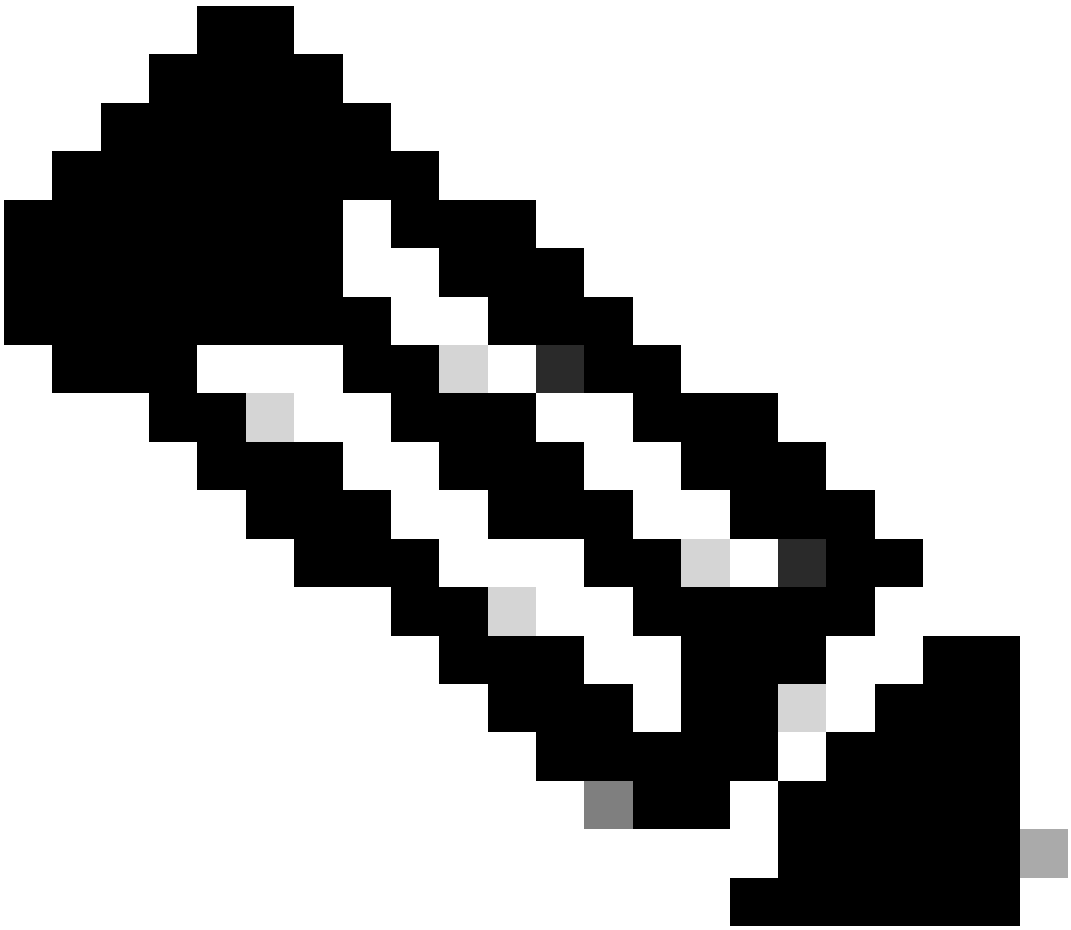
참고: 다운로드한 이 인증서는 ASA 신뢰 지점 AzureAD-AC-SAML1로 가져옵니다. 자세한 내용은 ASA 구성 섹션을 참조하십시오.

10단계. Cisco Secure Firewall 설정 - 보안 클라이언트 섹션에서 요구 사항에 따라 적절한 URL을 복사합니다. 이러한 URL은 ASA에서 SSO 서버 개체를 구성하는 데 사용됩니다.

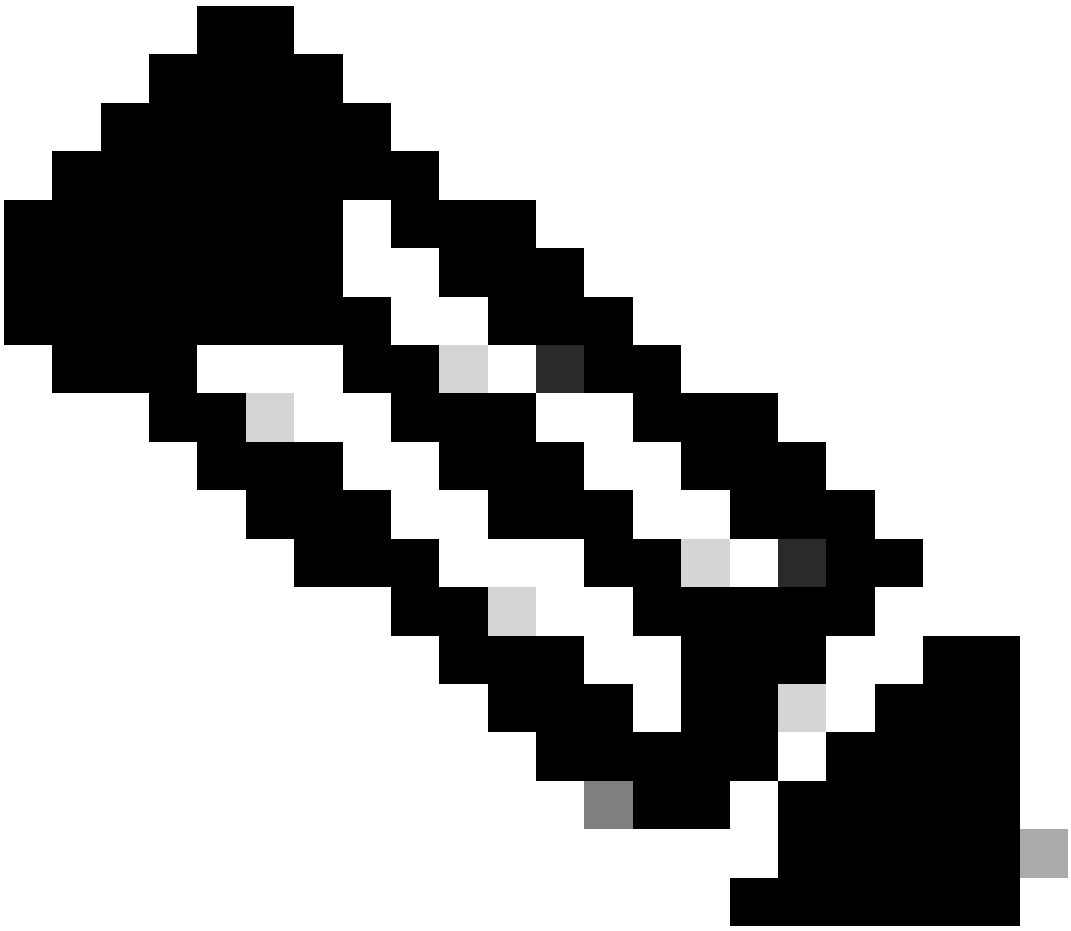
- Microsoft Entra Identifier - VPN 컨피그레이션의 SAML IDP입니다.
- Login URL(로그인 URL) - URL 로그인입니다.
- Logout URL(로그아웃 URL) - URL 로그아웃입니다.



SSO URL



참고: 갤러리에서 두 번째 터널 그룹에 대해 Cisco Secure Firewall - Secure Client 앱을 추가하려면 이전 컨피그레이션 단계를 반복합니다. 이 경우 두 번째 터널 그룹 이름은 SAML2입니다.



참고: 두 번째 터널 그룹(SAML 2)에 Cisco Secure Firewall - Secure Client 앱을 추가하는 동안 8단계에서 다운로드된 Azure 인증서가 ASA 신뢰 지점 AzureAD-AC-SAML2로 가져오기됩니다.

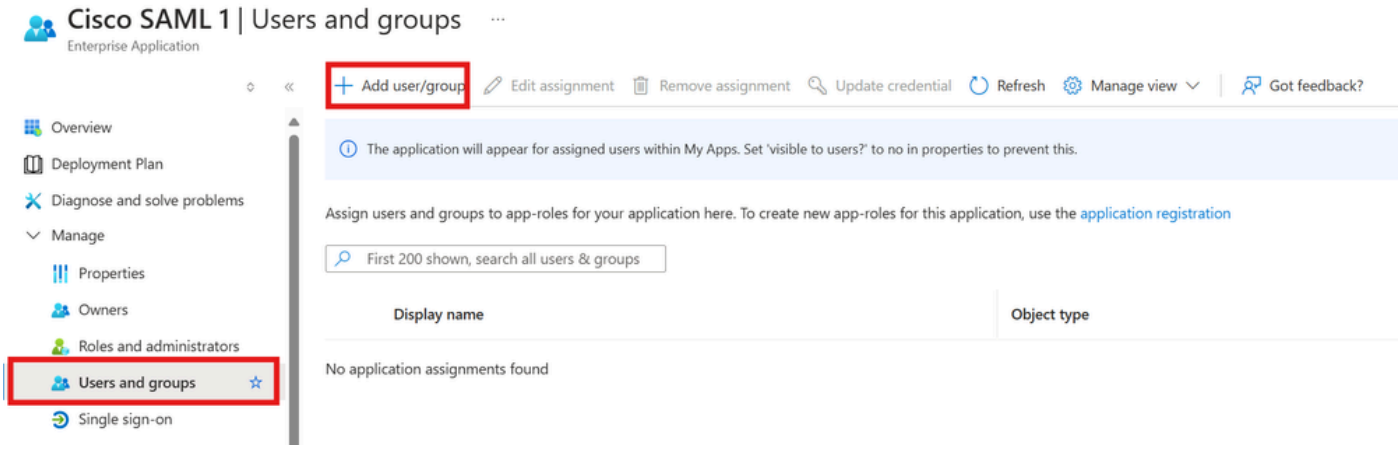
앱에 Azure AD 사용자 할당

이 섹션에서는 Cisco Secure Client 앱에 대한 액세스 권한을 부여하므로 Test1 및 Test2가 Azure SSO를 사용하도록 설정됩니다.

첫 번째 IdP 애플리케이션의 경우:

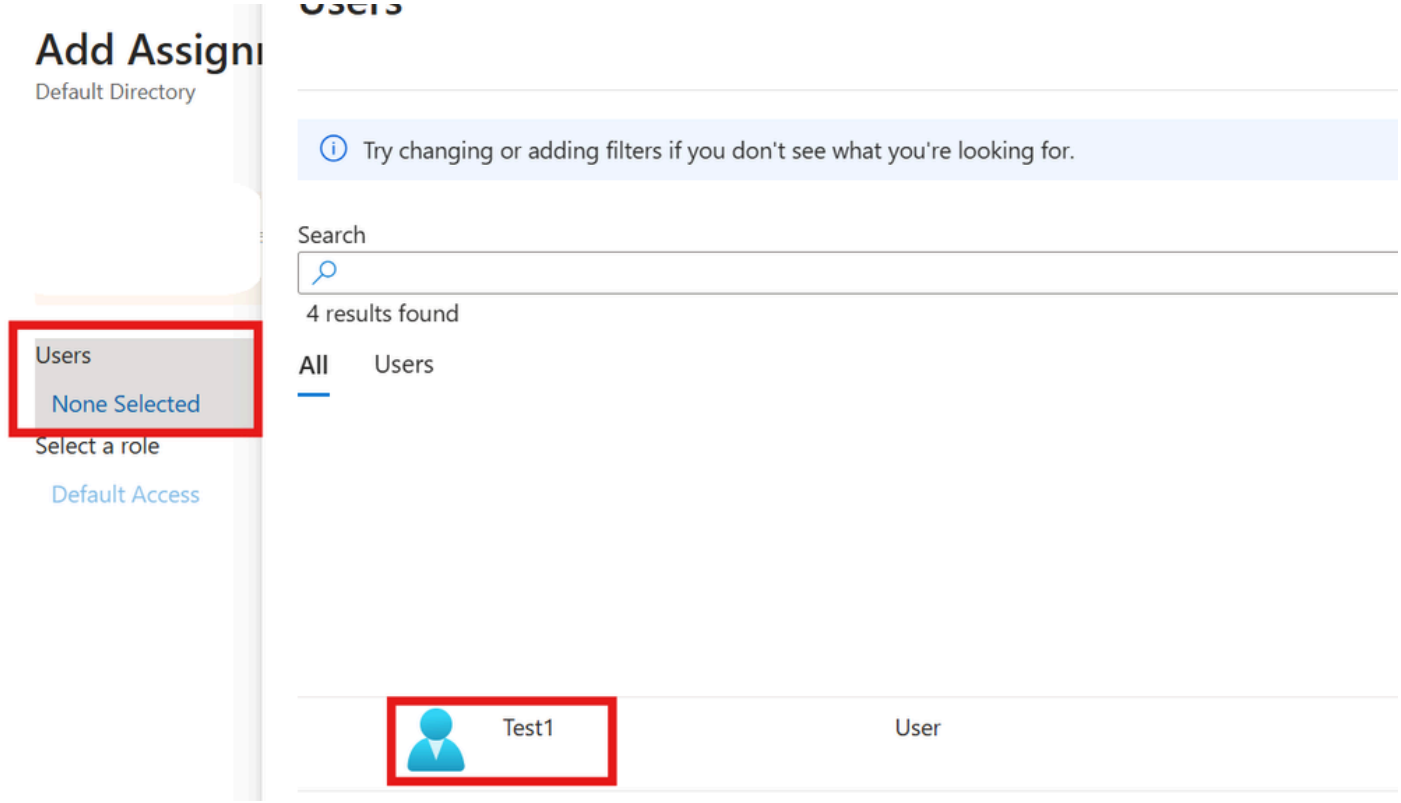
1단계. 첫 번째 IdP 애플리케이션 개요 페이지에서 Users and groups(사용자 및 그룹), Add user(사

용자 추가)를 선택합니다.



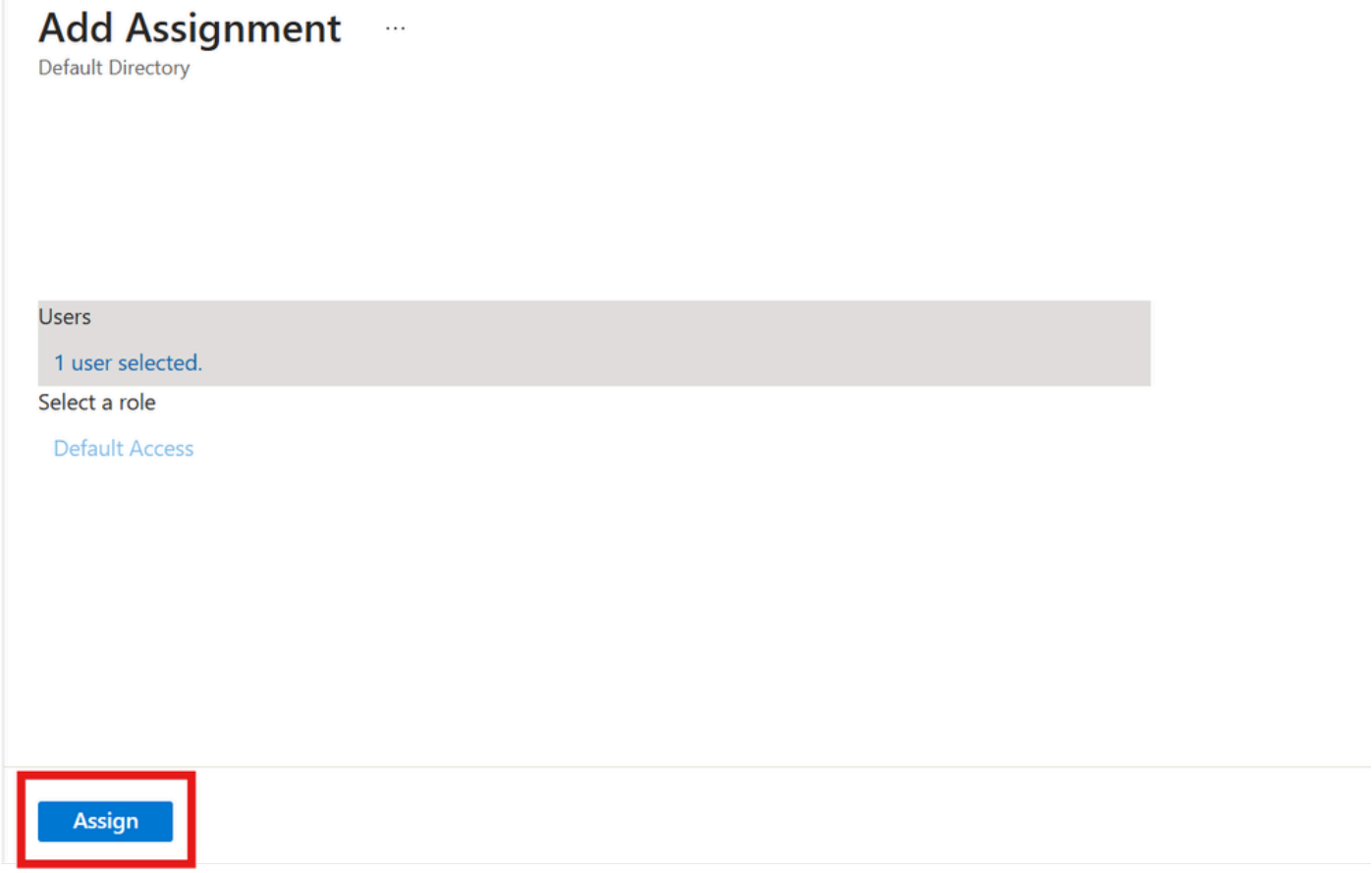
사용자 및 그룹

2단계. [할당 추가] 대화 상자에서 [사용자] 또는 [그룹]을 선택합니다.



배정 1 추가

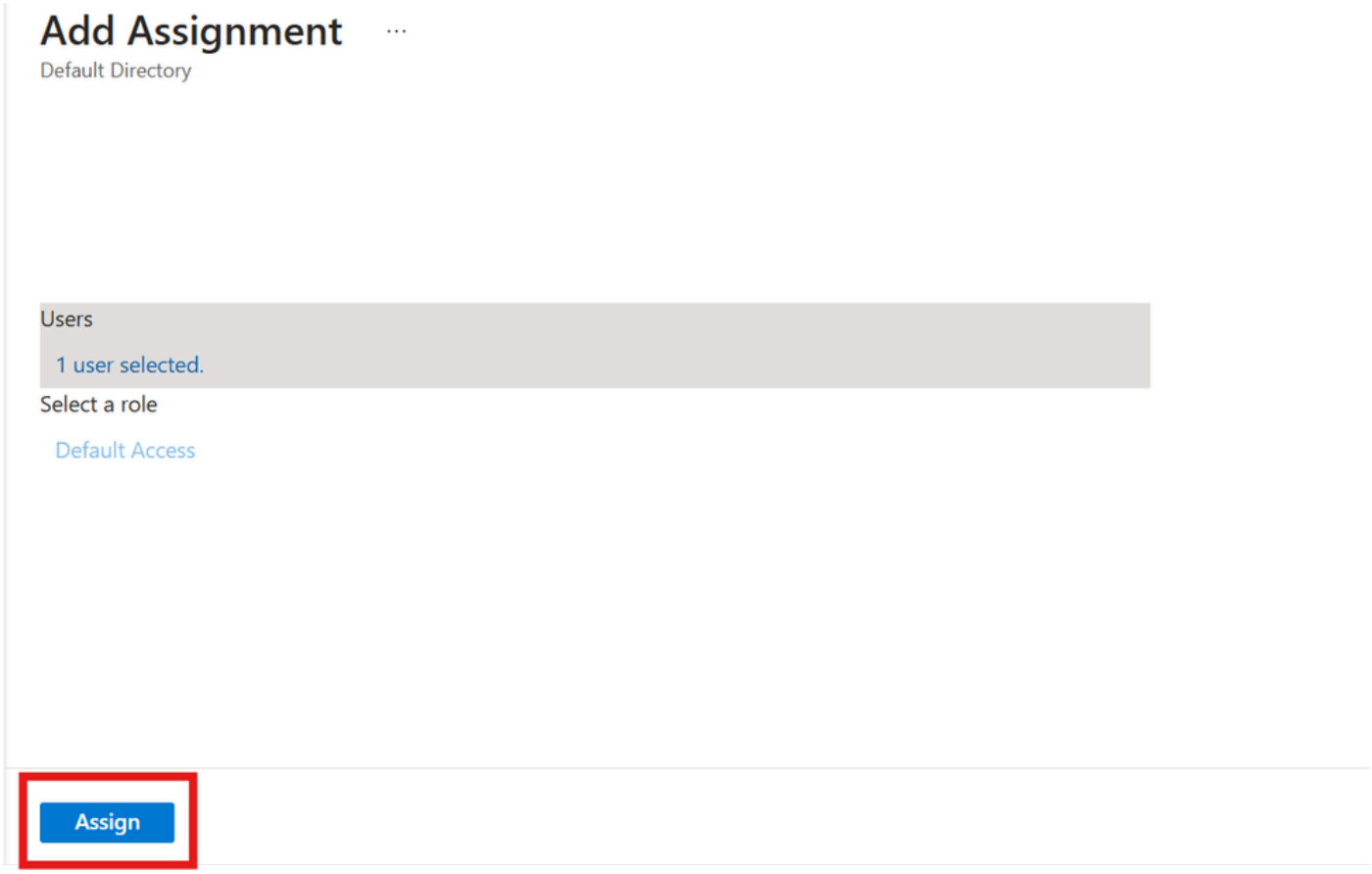
3단계. [할당 추가] 대화 상자에서 [할당] 단추를 클릭합니다.



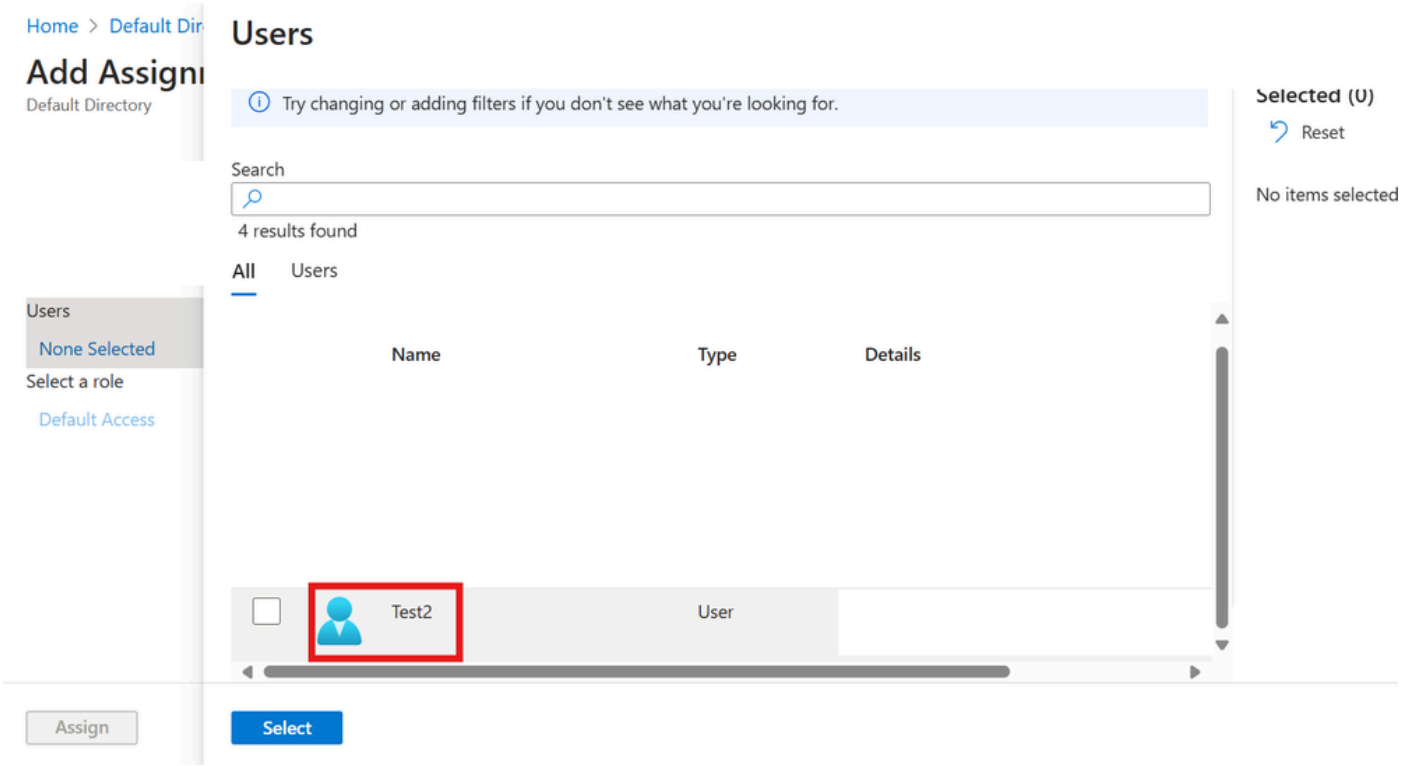
테스트1 사용자 할당

두 번째 IdP 애플리케이션의 경우:

두 번째 Idp 응용 프로그램에 대해 이 이미지에 표시된 대로 이전 단계를 반복합니다.

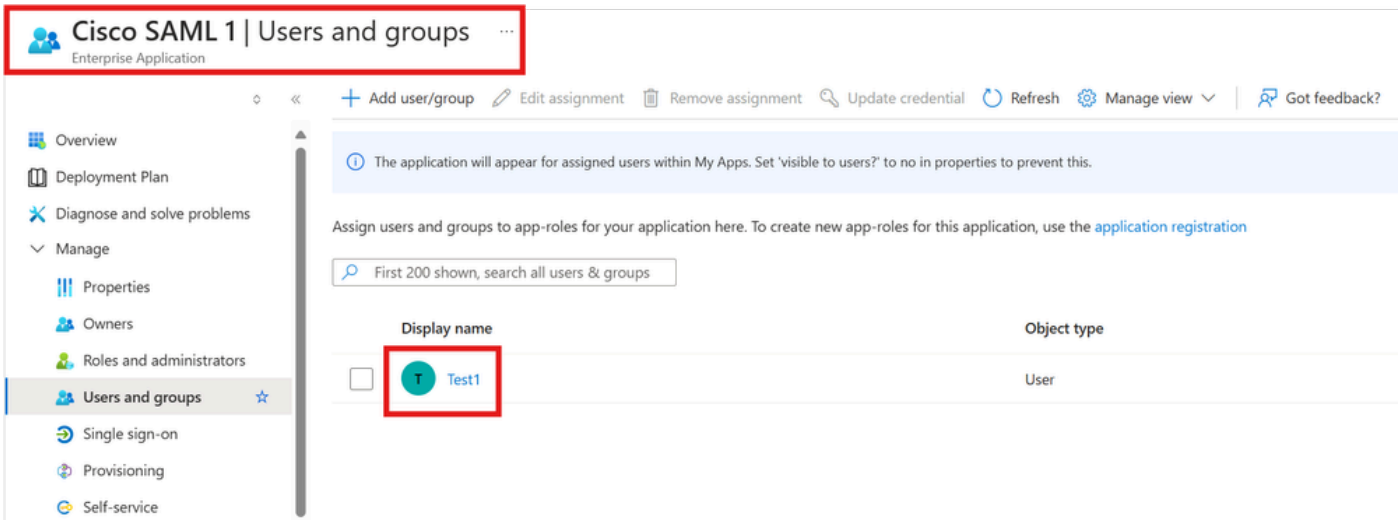


과제 2 추가



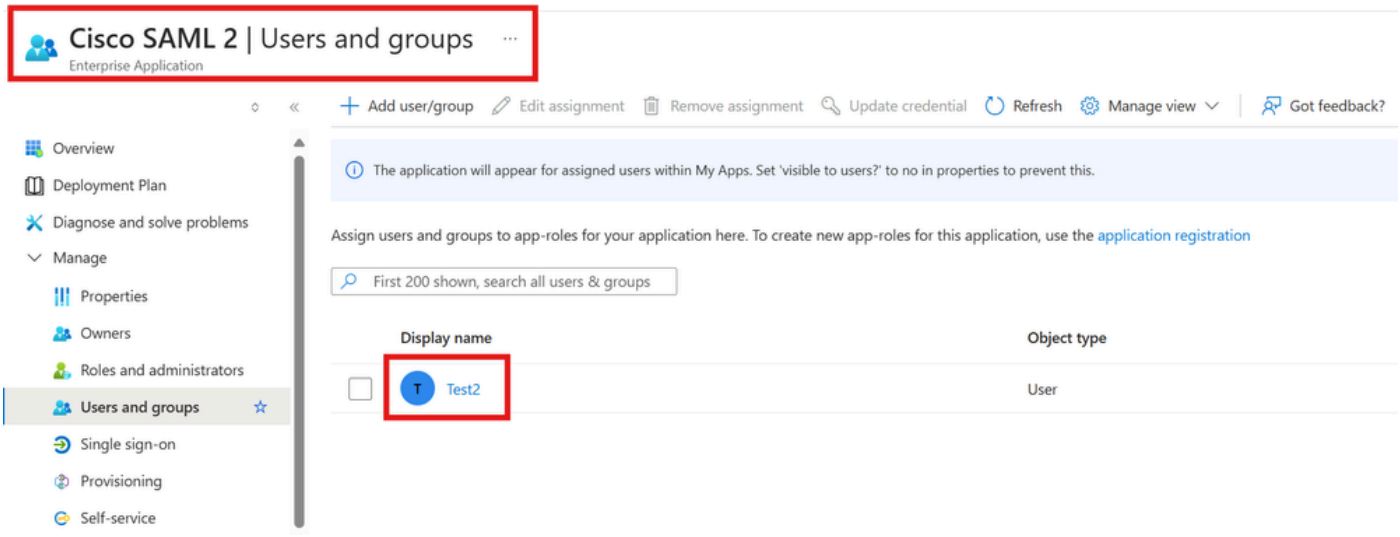
테스트2 사용자 할당

테스트1 사용자 할당:



테스트 1 사용자 지정

Test2 사용자 할당:



테스트 2 사용자 지정

CLI를 통한 ASA 컨피그레이션

1단계. 신뢰 지점을 생성하고 SAML 인증서를 가져옵니다.

두 개의 신뢰 지점을 구성하고 각 터널 그룹에 대한 각 SAML 인증서를 가져옵니다.

<#root>

```
config t

 crypto ca trustpoint
```

AzureAD-AC-SAML1

```
   revocation-check none
   no id-usage
   enrollment terminal
```

```
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML1

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit

!
!

crypto ca trustpoint
```

AzureAD-AC-SAML2

```
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML2

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit
```

2단계. SAML IdP를 구성합니다.

SAML IdP 설정을 프로비저닝하려면 다음 명령을 사용합니다.

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2  - [Logout URL]
 trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

3단계. 첫 번째 VPN 터널 그룹에 SAML 인증을 적용합니다.

AzureAD-AC-SAML1 IdP 신뢰 지점을 사용하여 SAML1 터널 그룹을 구성합니다.

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (

4단계. 두 번째 VPN 터널 그룹에 SAML 인증을 적용합니다.

AzureAD-AC-SAML2 IdP 신뢰 지점을 사용하여 SAML2 터널 그룹을 구성합니다.

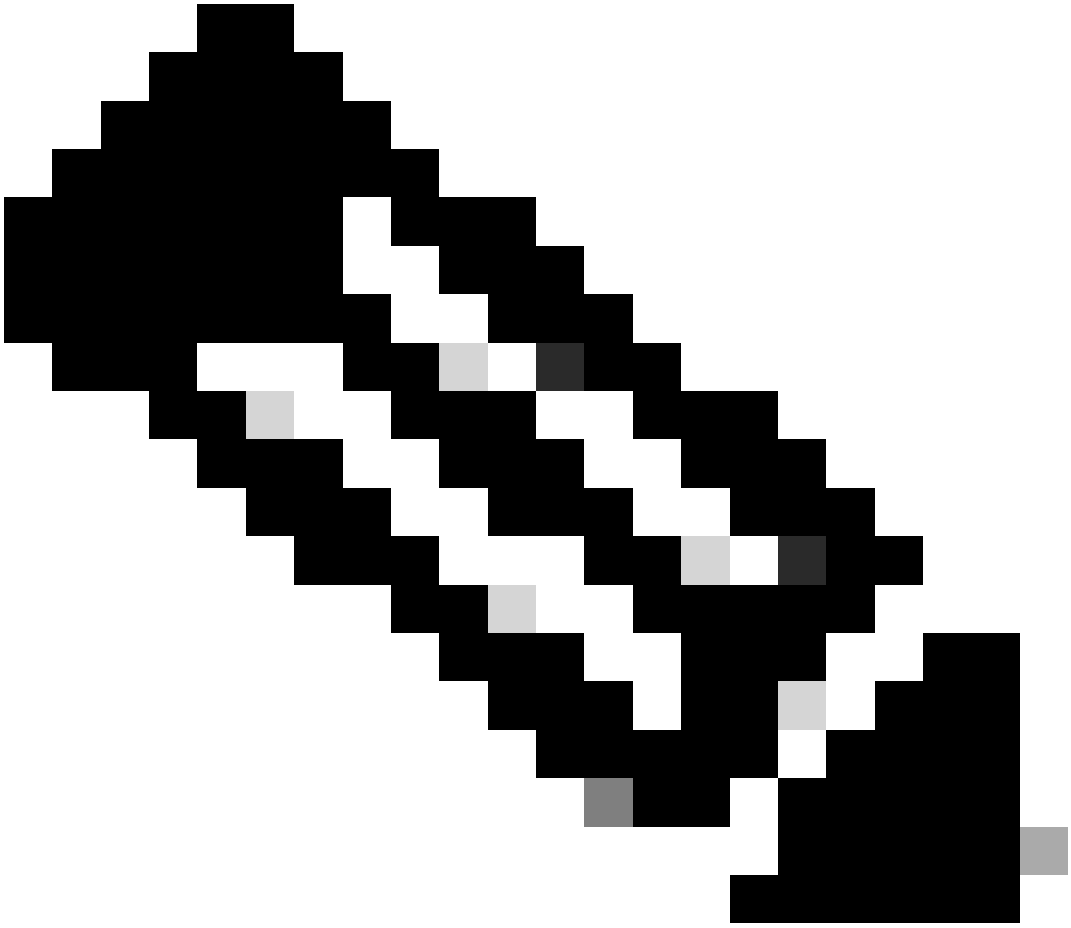
<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (

5단계: 설정 저장.

```
write memory
```



참고: IdP 컨피그레이션을 변경하는 경우 터널 그룹에서 SAML ID 제공자 컨피그레이션을 제거하고 다시 적용해야 변경 사항이 적용됩니다.

다음을 확인합니다.

SAML 인증으로 AnyConnect를 테스트합니다.

1단계. VPN URL에 연결하고 Azure AD 세부 정보에 로그를 입력합니다.

2단계. (선택 사항) 로그인 요청을 승인합니다.

3단계. AnyConnect가 연결되었습니다.

문제 해결

대부분의 SAML 문제 해결에는 SAML 컨피그레이션이 확인되거나 디버그가 실행될 때 찾을 수 있는 잘못된 컨피그레이션이 포함됩니다. debug webvpn saml 255를 사용하여 대부분의 문제를 해결할 수 있지만 이 디버그가 유용한 정보를 제공하지 않는 경우 추가 디버그를 실행할 수 있습니다.

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

관련 정보

- SAML을 통해 Microsoft Azure MFA를 사용하여 ASA AnyConnect VPN 구성
- 기술 지원 및 문서 – Cisco Systems

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.