# Azure에서 FMC SSO를 ID 공급자로 구성

## 목차



## 소개

이 문서에서는 Azure를 idP(Identity Provider)로 사용하는 FMC(Firepower Management Center) SSO(Single Sign-On)를 구성하는 방법에 대해 설명합니다.

SAML(Security Assertion Markup Language)은 SSO를 가능하게 하는 기본 프로토콜입니다.기업은 단일 로그인 페이지를 유지 관리하며 그 뒤에는 ID 저장소와 다양한 인증 규칙이 있습니다.SAML을 지원하는 모든 웹 앱을 쉽게 구성할 수 있으며, 모든 웹 애플리케이션에 로그인할 수 있습니다.또한 사용자가 액세스해야 하는 모든 웹 앱에 대해 비밀번호를 유지 관리(그리고 잠재적으로 재사용)하거나 이러한 웹 앱에 비밀번호를 노출시키지 않아도 보안 이점이 있습니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower Management Center에 대한 기본 이해
- Single Sign-On에 대한 기본 이해

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco FMC(Firepower Management Center) 버전 6.7.0
- Azure - IdP

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

# 배경 정보

### SAML 용어

SAML에 대한 컨피그레이션은 다음 두 곳에서 수행해야 합니다.SP에 있습니다사용자가 특정 SP에 로그인할 때 어디로 어떻게 전송할지 알 수 있도록 IdP를 구성해야 합니다.  IdP에서 서명한 SAML 어설션을 신뢰할 수 있도록 SP를 구성해야 합니다.

SAML의 핵심 용어 정의:

- IdP(Identity Provider) - 인증을 수행하는 소프트웨어 툴 또는 서비스(로그인 페이지 및/또는 대시보드로 시각화되는 경우가 많음)사용자 이름과 비밀번호를 확인하고, 계정 상태를 확인하고, 2단계 요소 등을 호출합니다.

- SP(서비스 공급자) - 사용자가 액세스를 시도하는 웹 애플리케이션입니다.

- SAML Assertion - 사용자의 ID 및 기타 특성을 주장하는 메시지로, 브라우저 리디렉션을 통해 HTTP를 통해 전송됩니다.

## IdP 구성

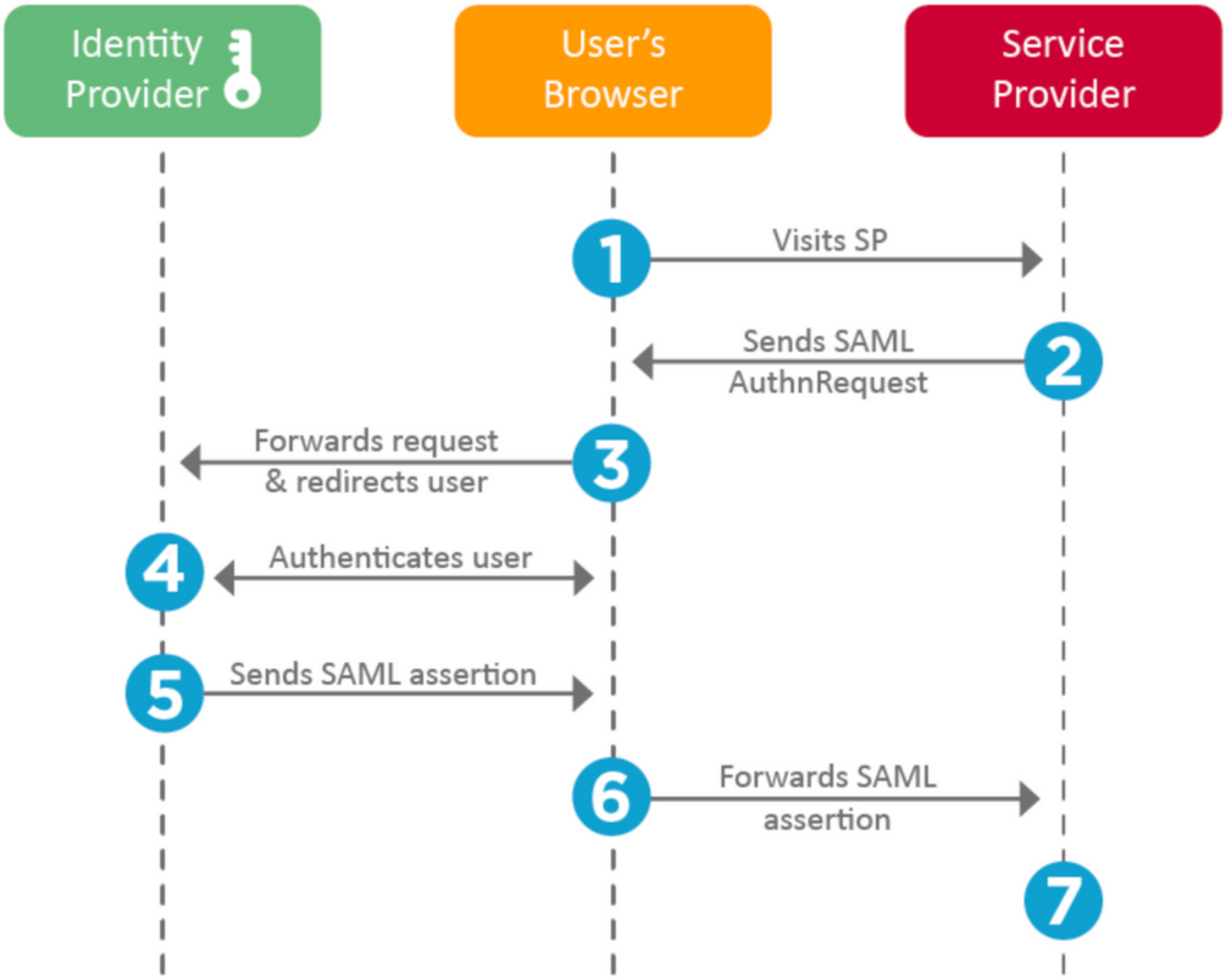
SAML assertion에 대한 사양, 포함해야 할 내용 및 형식 지정 방법은 SP에서 제공하고 IdP에서 설정합니다.

- EntityID - SP의 전역적으로 고유한 이름입니다.형식은 다양하지만 URL로 서식이 지정된 이 값을 보는 것이 일반적입니다.
  예:  <https://<FQDN 또는 IPaddress>/saml/metadata>

- ACS(Assertion Consumer Service) Validator - SAML assertion이 올바른 ACS로 전송되도록 하는 정규식(regex) 형식의 보안 측정값입니다.SAML 요청에 ACS 위치가 포함되어 있는 SP가 시작한 로그인 중에만 이 작업이 수행되므로 이 ACS 검사기는 SAML 요청 제공 ACS 위치가 올바른지 확인합니다.
  예: **https://<FQDN-or-IPaddress>/saml/acs**

- 속성 - 속성의 수와 형식은 크게 다를 수 있습니다.일반적으로 로그인하려는 사용자의 사용자 이름인 nameID라는 특성이 하나 이상 있습니다.

- SAML 서명 알고리즘 - SHA-1 또는 SHA-256. 일반적으로 SHA-384 또는 SHA-512. 이 알고리즘은 X.509 인증서와 함께 사용됩니다.




## SP 구성

위 섹션의 반대편에 있는 이 섹션에서는 IdP가 제공하고 SP에서 설정한 정보를 설명합니다.

- 발급자 URL - IdP의 고유 식별자입니다.SP에서 수신한 SAML 어설션이 올바른 IdP에서 발급되었는지 확인할 수 있도록 IdP에 대한 정보가 포함된 URL로 포맷되었습니다.
  예: <saml:Issuer https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/ >

- SAML SSO Endpoint/Service Provider Login URL - SAML 요청을 사용하여 SP에서 리디렉션할 때 인증을 시작하는 IdP 엔드포인트입니다.
  예: https://login.microsoftonline.com/023480840129412-824812/saml2

- SAML SLO(Single Log-out) Endpoint - SP에서 리디렉션하면 IdP 세션을 닫는 IdP 엔드포인트입니다(일반적으로 **로그아웃**을 클릭한 후).
  예: `https://access.wristbandtent.com/logout`

## FMC의 SAML

FMC의 SSO 기능은 6.7에서 도입되었습니다. 새로운 기능은 FMC 역할에 존재하는 정보를 매핑하므로 RBAC(FMC Authorization)를 간소화합니다.모든 FMC UI 사용자 및 FMC 역할에 적용됩니다.현재는 SAML 2.0 Specification과 지원되는 IDP를 지원합니다.

- 옥타
- OneLogin
- PingID
- Azure AD
- 기타(SAML 2.0을 준수하는 모든 IDP)

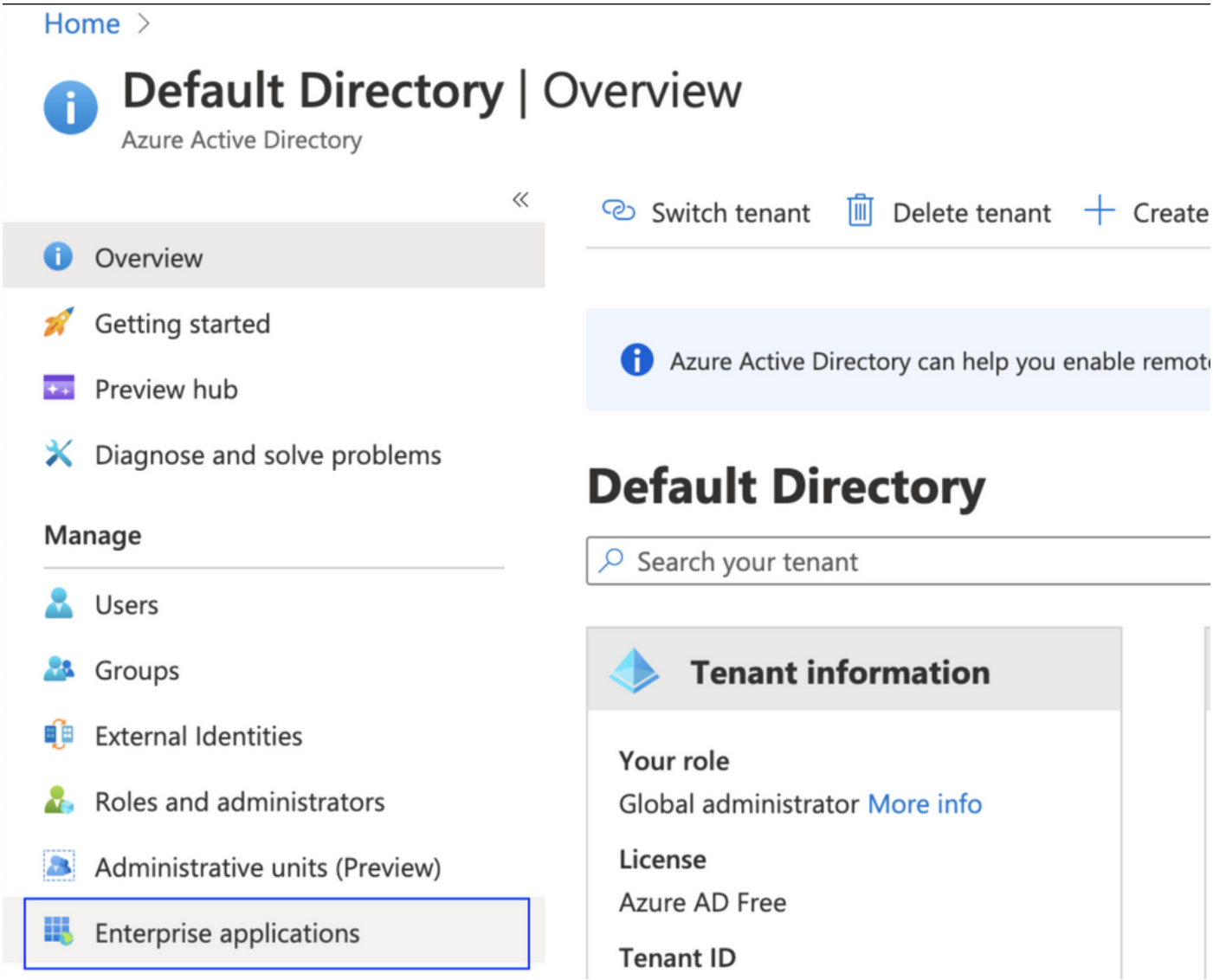
### 제한 사항 및 주의 사항

- SSO는 전역 도메인에 대해서만 구성할 수 있습니다.
- HA 쌍의 FMC에는 개별 컨피그레이션이 필요합니다.
- 로컬/AD 관리자만 단일 로그인을 구성할 수 있습니다.
- IDP에서 시작된 SSO는 지원되지 않습니다.

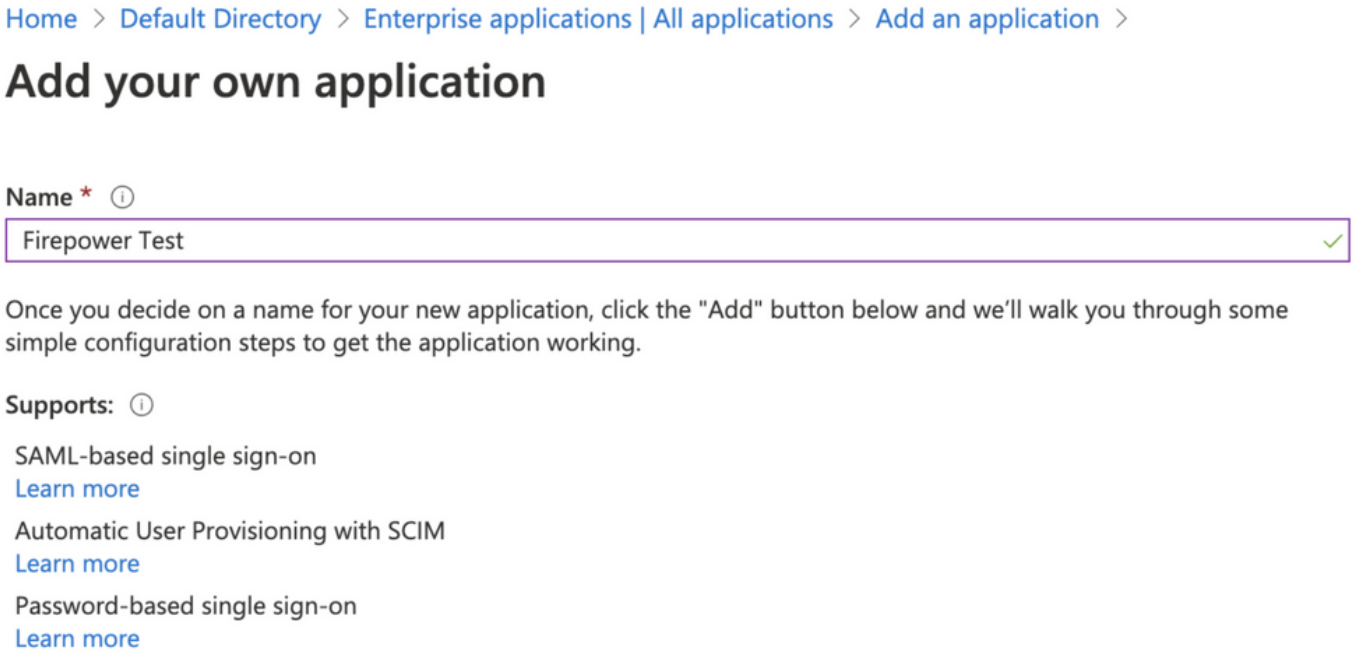
## 구성

### ID 공급자 구성

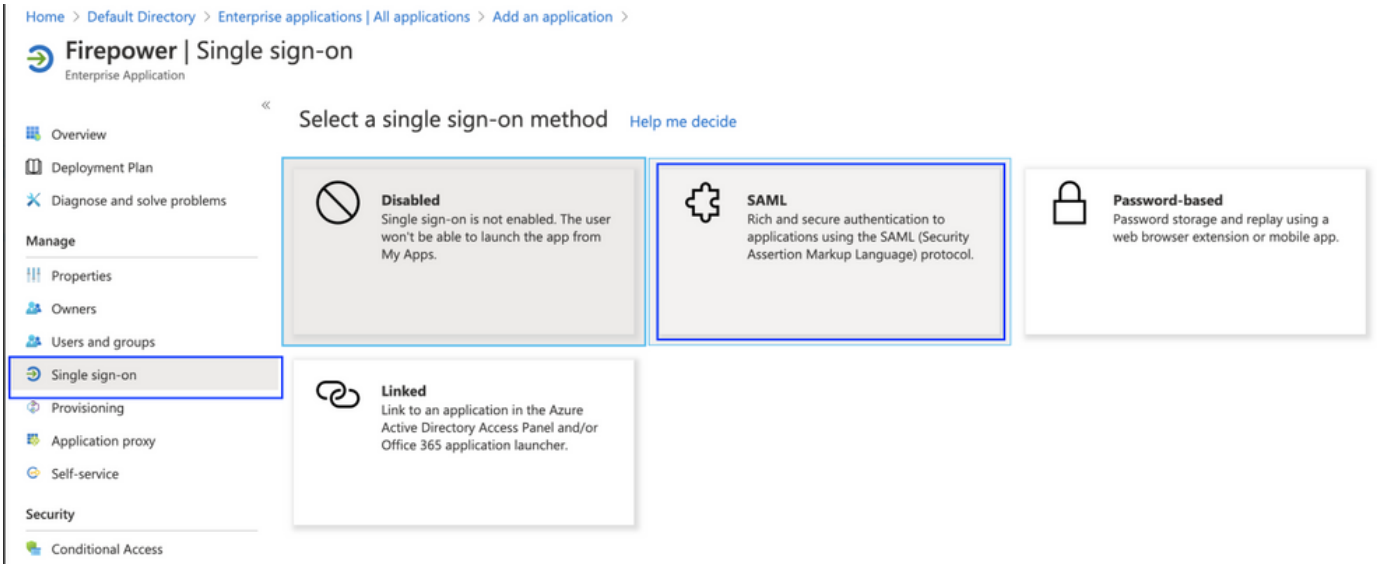
1단계. Microsoft Azure에 로그인합니다.Azure **Active Directory > 엔터프라이즈 응용 프로그램으로 이동합니다**.



- 2단계. 이 이미지에 표시된 대로 Non-Gallery Application 아래에서 새 응용 프로그램을 만듭니다.

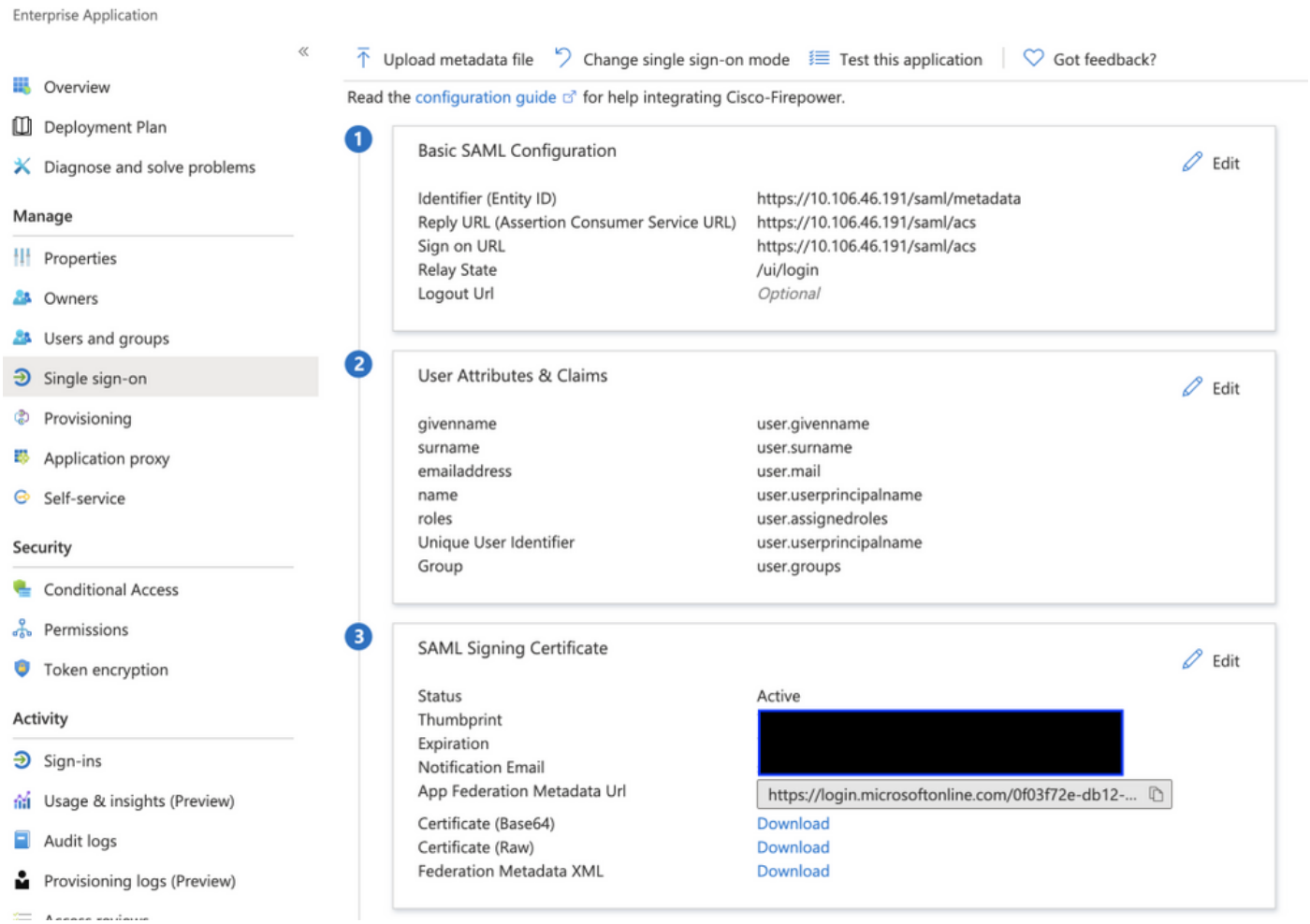



3단계. 생성된 애플리케이션을 편집하고 이 이미지에 표시된 대로 **Set up single sign on > SAML**로 이동합니다.




4단계. 기본 SAML 컨피그레이션을 수정하고 FMC 세부 정보를 제공합니다.

- FMC URL: https://<FMC-FQDN 또는 IPaddress>
- 식별자(엔터티 ID): https://<FMC-FQDN 또는 IPaddress>/saml/metadata
- 회신 URL: https://<FMC-FQDN 또는 IPaddress>/saml/acs
- 로그인 URL: **/https://<FMC-QDN 또는-IPaddress>/saml/acs**
- RelayState:**/ui/login**

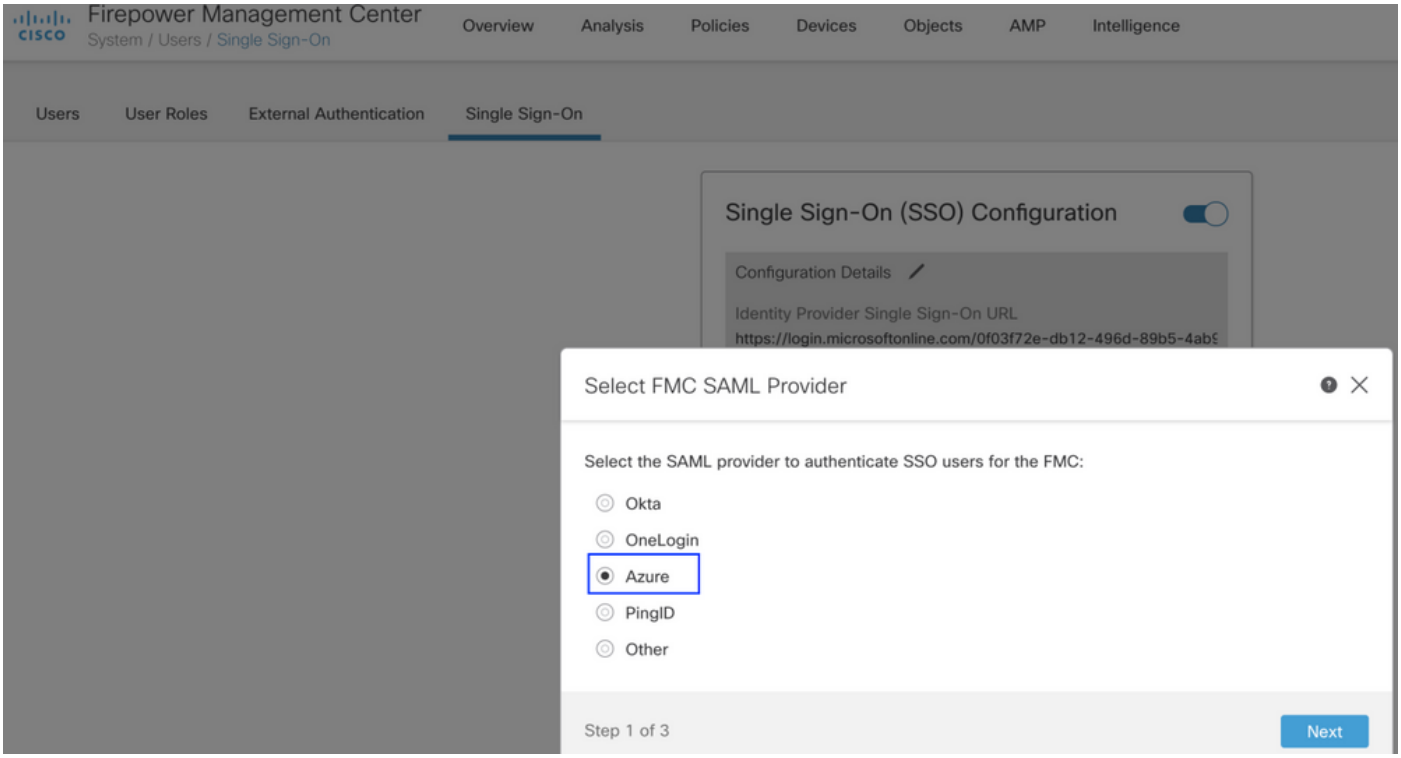



나머지는 기본값으로 유지 - 역할 기반 액세스에 대해 자세히 설명합니다.

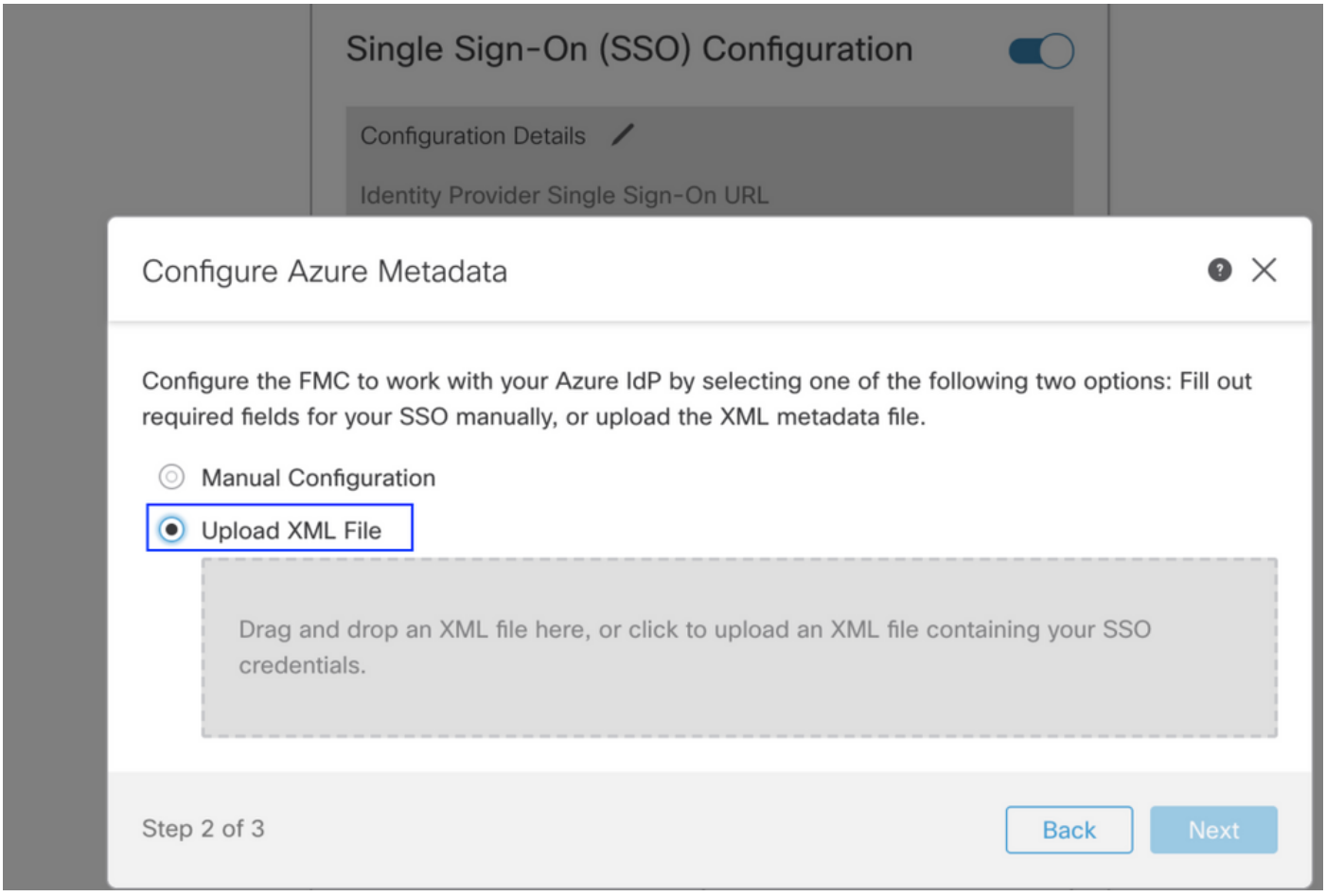
ID 공급자 구성의 끝을 표시합니다.FMC 구성에 사용할 페더레이션 메타데이터 XML을 다운로드합니다.

## Firepower Management Center의 컨피그레이션

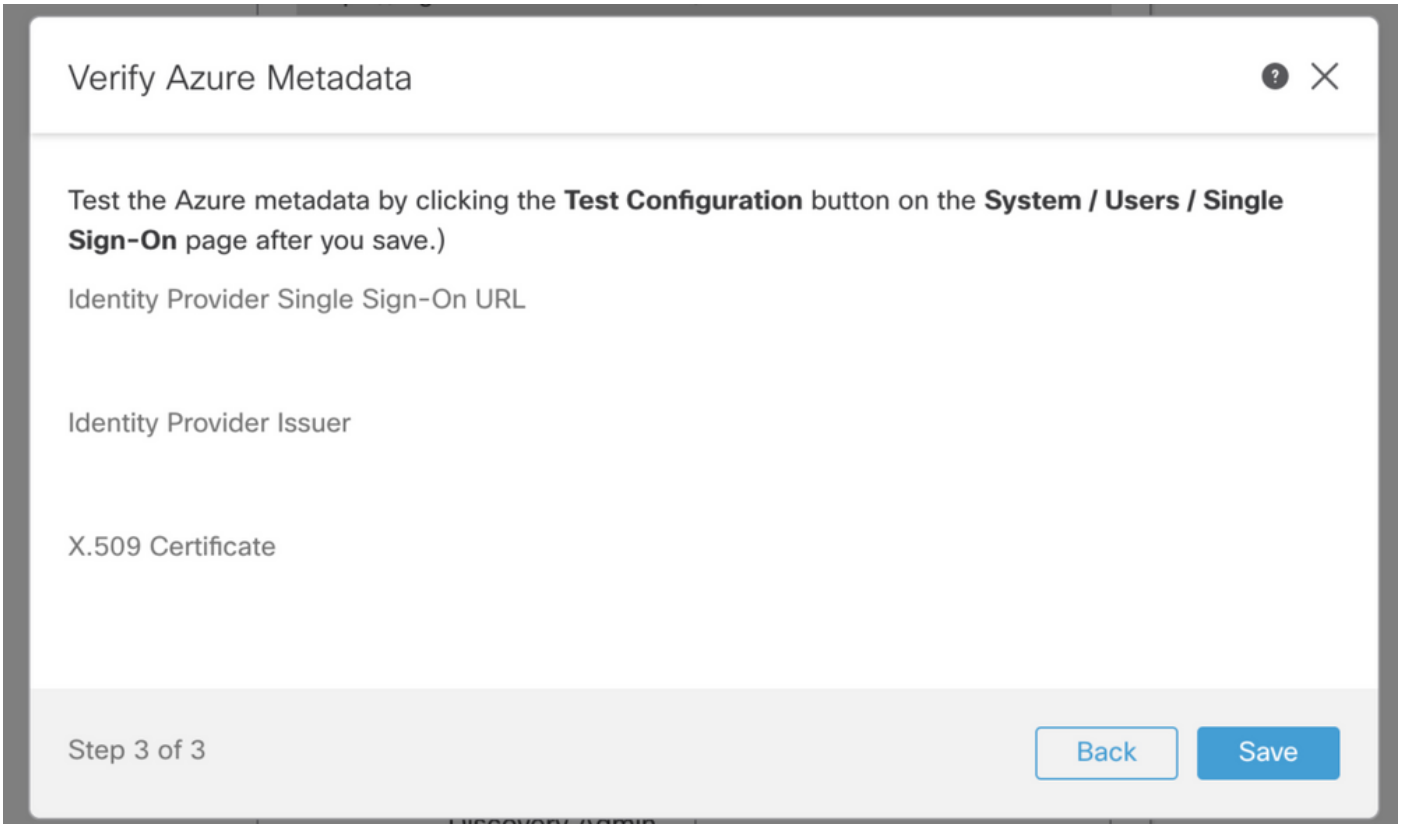
1단계. FMC에 로그인하고 **Settings(설정) > Users(사용자) > Single Sign-On** 및 Enable SSO(SSO 활성화)로 이동합니다.Azure를 공급자로 선택합니다.




2단계. Azure에서 다운로드한 XML 파일을 여기에 업로드합니다.필요한 모든 세부 정보가 자동으로 입력됩니다.



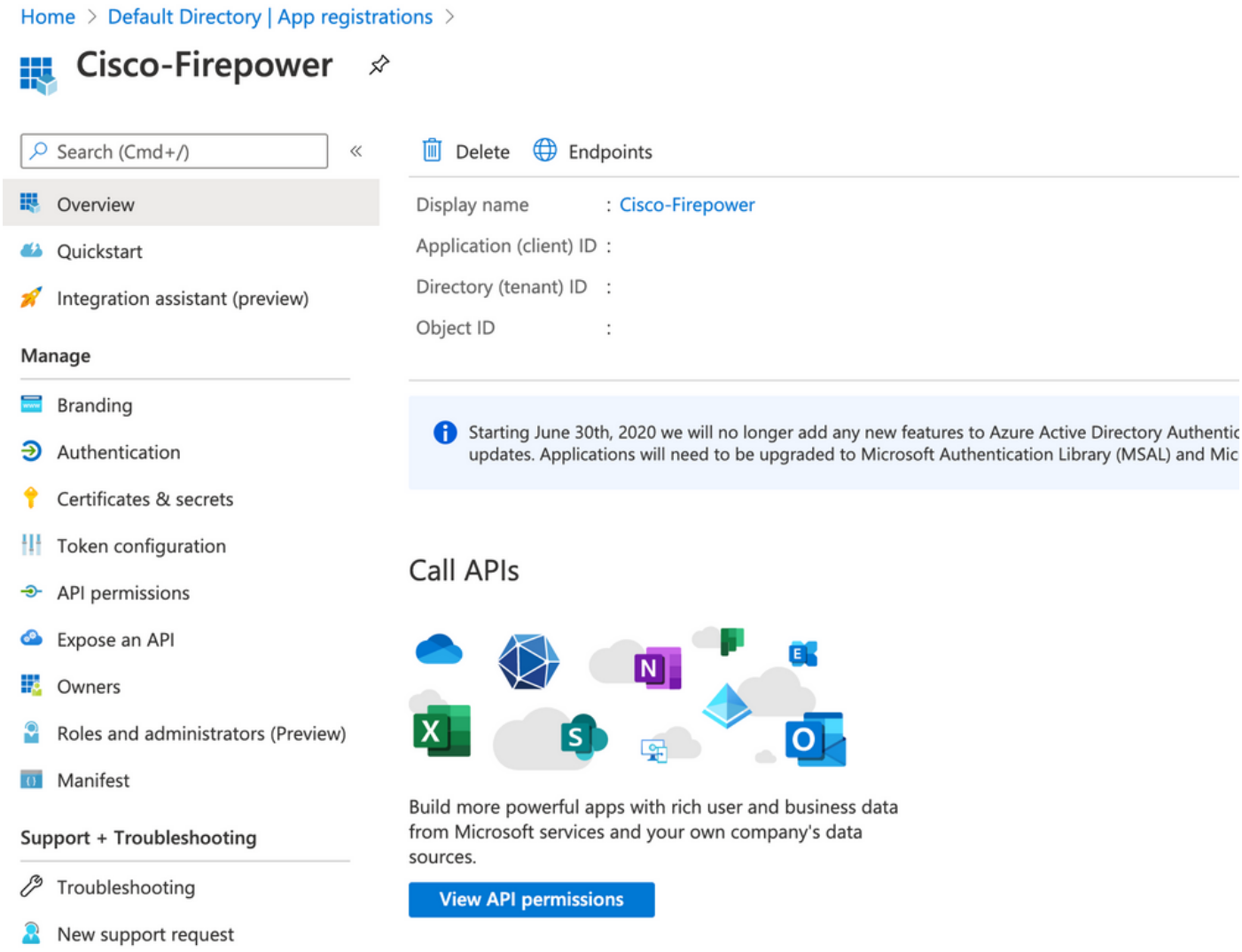

3단계. 컨피그레이션을 확인하고 이 이미지에 표시된 대로 **저장**을 클릭합니다.



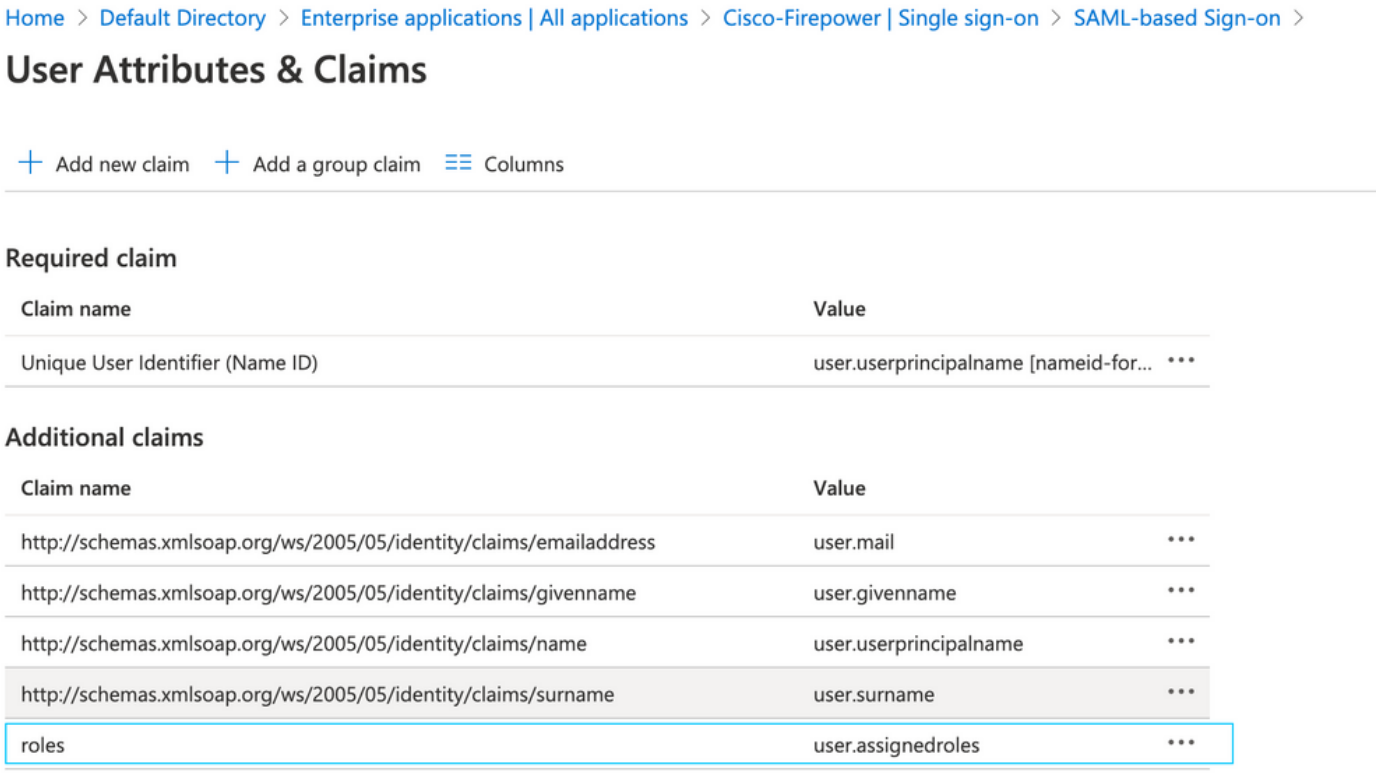

## 고급 구성 - RBAC with Azure

다양한 역할 유형을 사용하여 FMC의 역할에 매핑하려면 Azure의 응용 프로그램 매니페스트를 편집하여 역할에 값을 할당해야 합니다.기본적으로 역할은 Null 값을 가집니다.

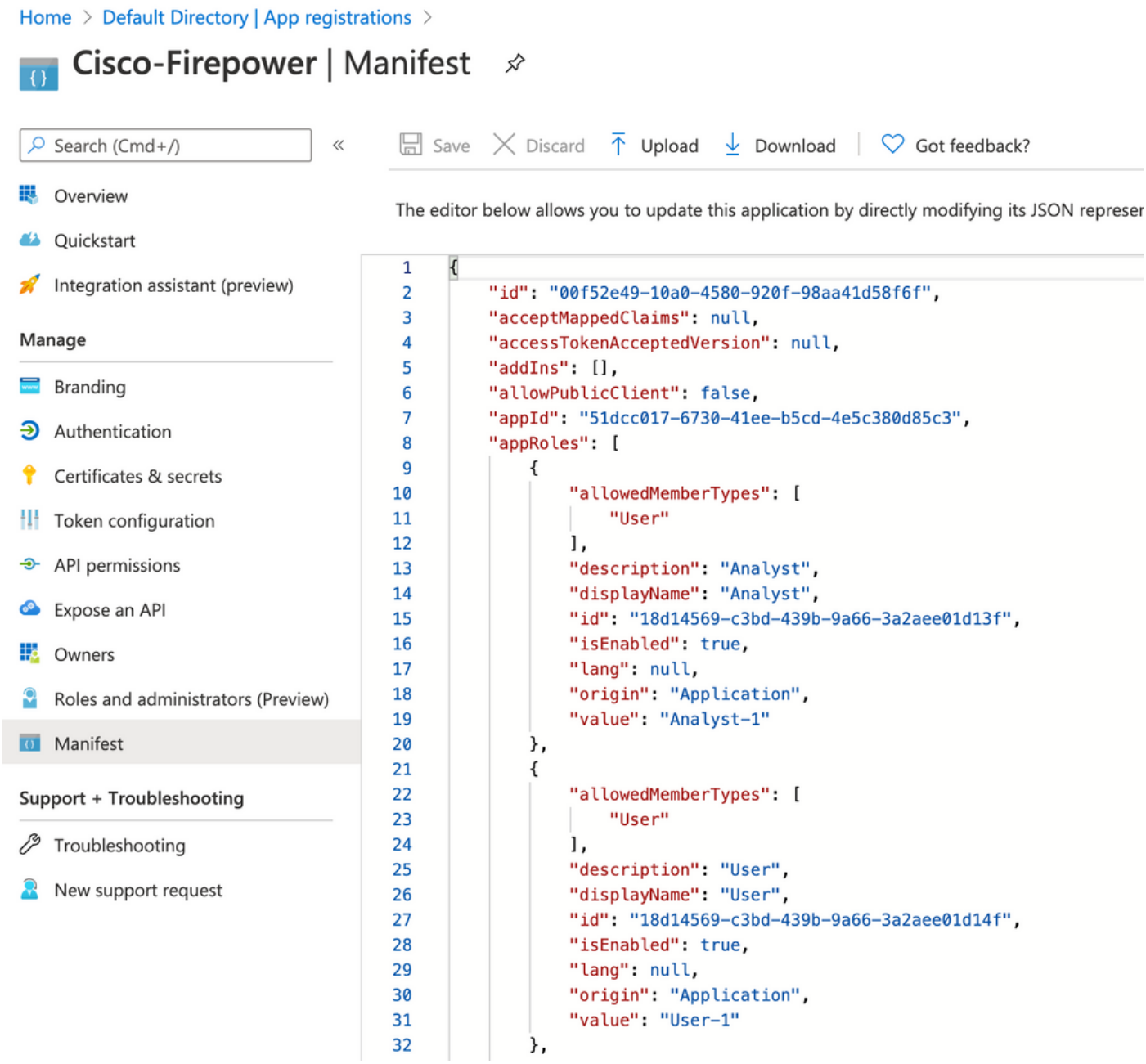
1단계. 생성된 **애플리케이션**으로 이동하고 **Single Sign-on**을 클릭합니다.



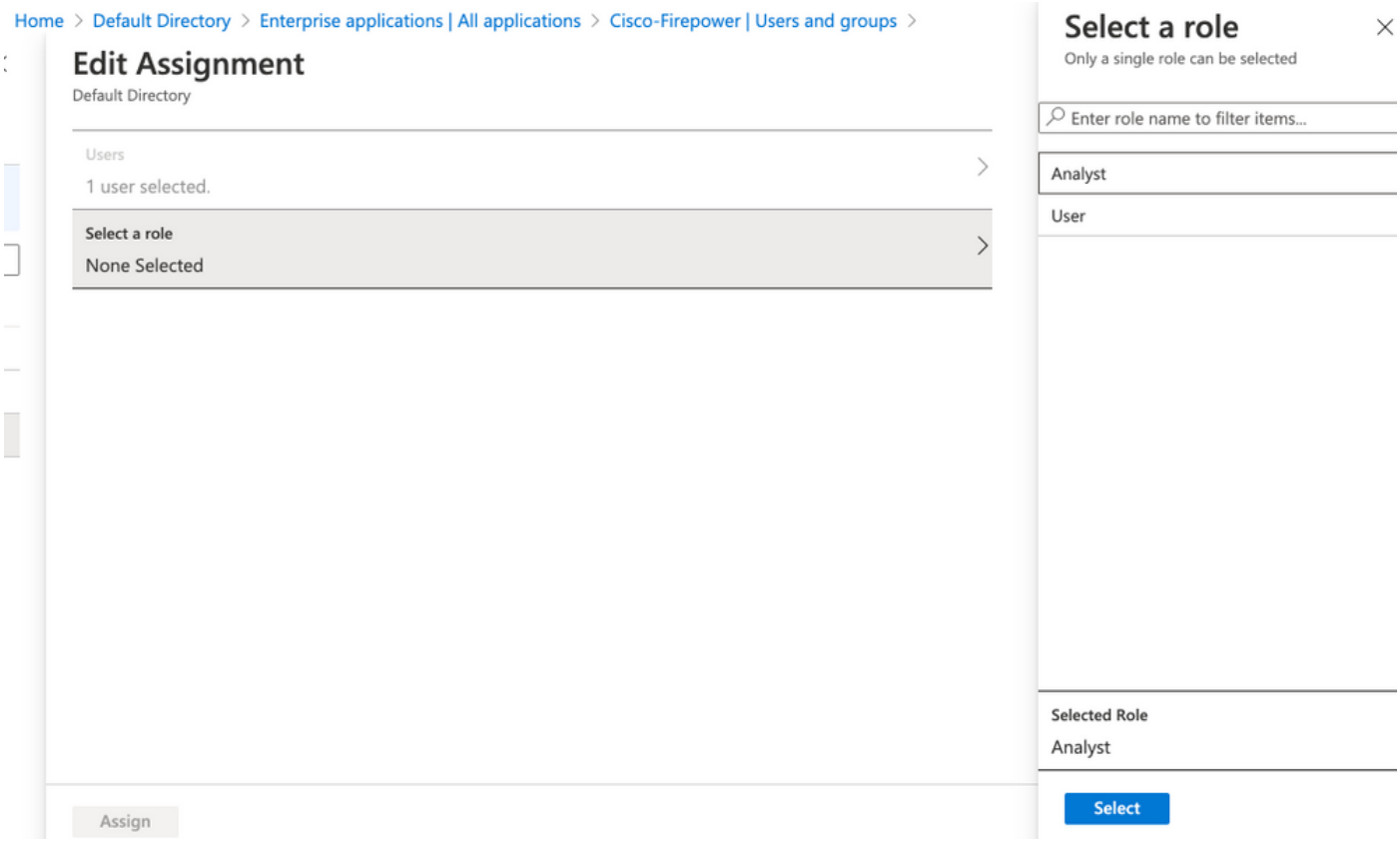

2단계. 사용자 속성 및 클레임을 편집합니다.이름으로 새 클레임 추가:**roles**를 선택하고 값을 user.assignedroles로 **선택합니다**.



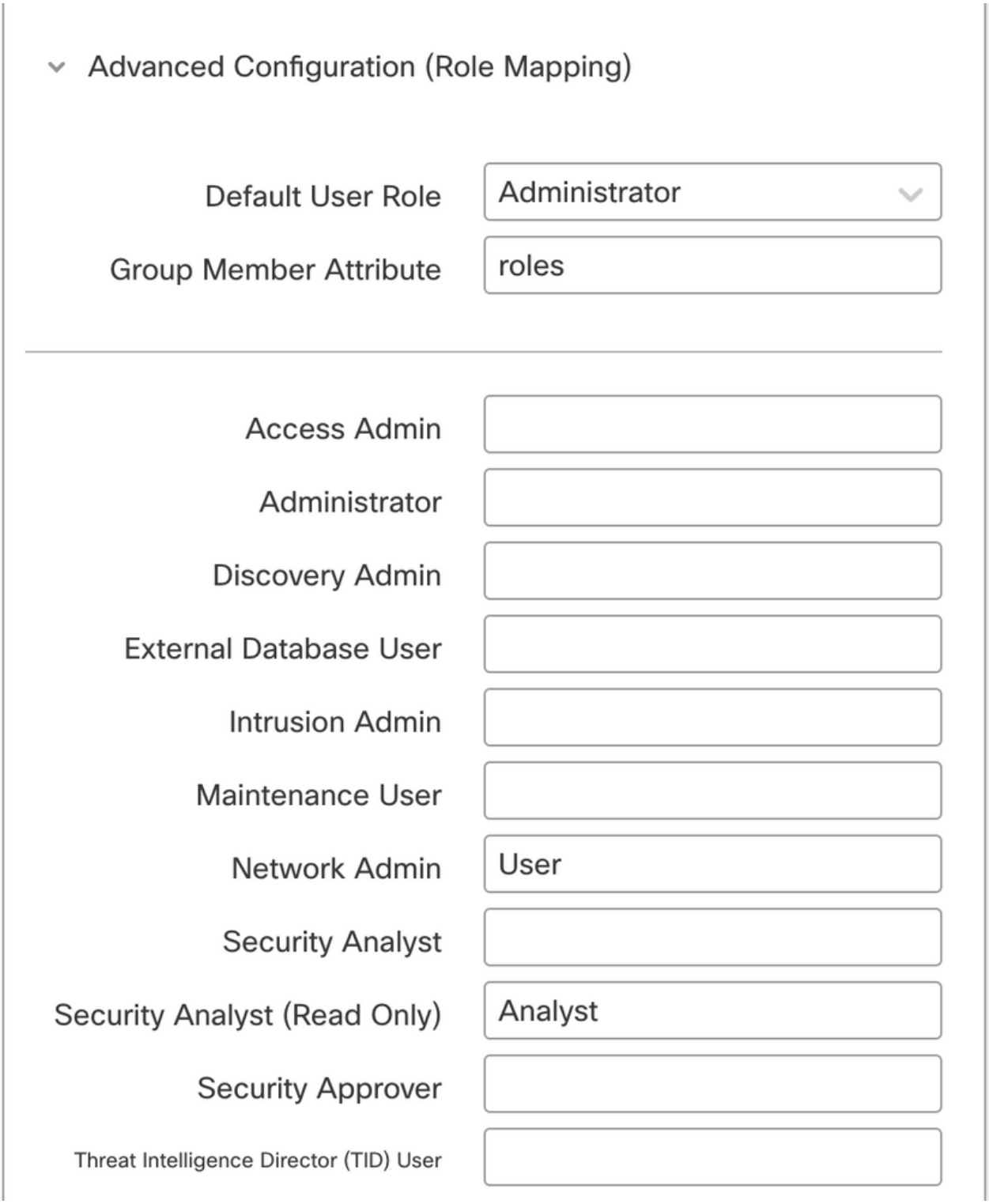

3단계. **<Application-Name> > 매니페스트로 이동합니다**. 매니페스트를 편집합니다.파일은 JSON 형식이며 기본 사용자를 복사할 수 있습니다.예를 들어, 여기서 두 개의 역할을 만듭니다.사용자 및 분석가.




4단계. **<Application-Name> > 사용자 및 그룹으로 이동합니다**.이 이미지에 표시된 대로 사용자를 편집하고 새로 만든 역할을 할당합니다.



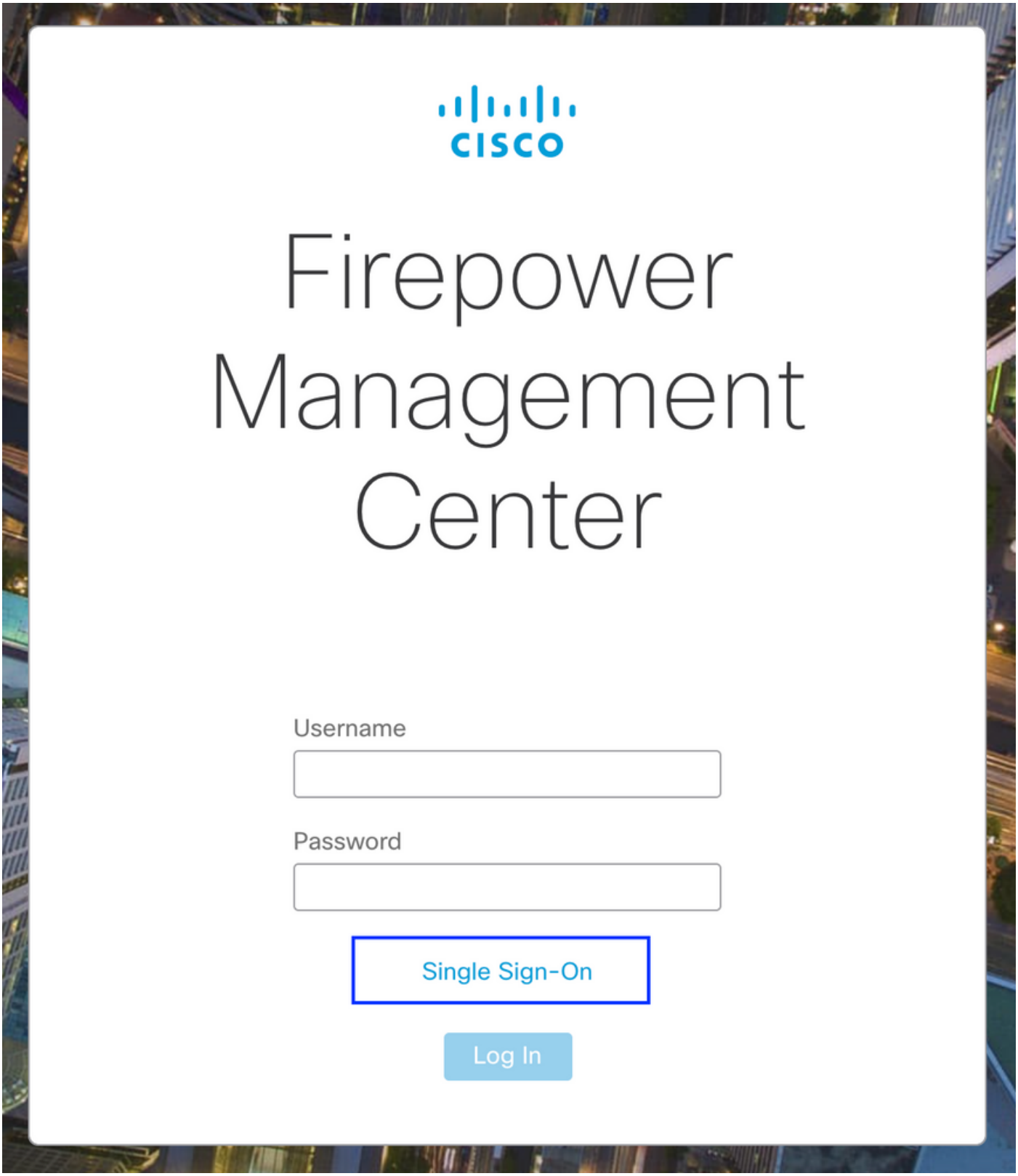

4단계. FMC에 로그인하고 SSO에서 고급 컨피그레이션을 편집합니다.의 경우 그룹 구성원 특성 :a응용 프로그램 **매니페스트에서** 제공한 표시 이름을 역할에 할당합니다.




그런 다음 지정된 역할에 로그인할 수 있어야 합니다.

## 다음을 확인합니다.

1단계. 브라우저에서 FMC URL로 이동합니다. https://<FMC URL>.이 이미지에 표시된 대로 **Single Sign-On**을 클릭합니다.




Microsoft 로그인 페이지로 리디렉션되고 로그인에 성공하면 FMC 기본 페이지가 반환됩니다.

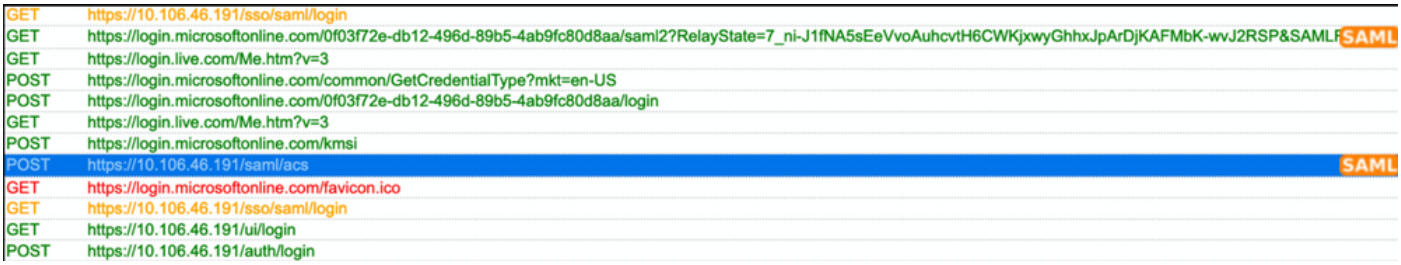
2단계. FMC에서 **System(시스템) > Users(사용자)**로 이동하여 데이터베이스에 추가된 SSO 사용자를 확인합니다.

| | | |
|---|---|---|
| test1@shbharticisco.onmicrosoft.com | Security Analyst | External (SSO) |
| test2guy@shbharticisco.onmicrosoft.com | Administrator | External (SSO) |

## 문제 해결

SAML 인증을 확인하고 이 워크플로가 성공적인 권한 부여를 위해 수행하는 워크플로인지 확인합니다(이 이미지는 실습 환경임).

## 브라우저 SAML 로그




## FMC SAML 로그

FMC의 SAML 로그(/var/log/auth-daemon.log)을 확인합니다.