

Microsoft Entra ID SSO용 SNA 관리자 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[컨피그레이션 단계](#)

[Azure에서 엔터프라이즈 응용 프로그램 구성](#)

[SNA에서 서비스 공급자 XML 파일 구성 및 다운로드](#)

[Azure에서 SSO 구성](#)

[Entra ID에서 사용자를 설정합니다.](#)

[SNA에서 SSO 구성](#)

[문제 해결](#)

소개

이 문서에서는 SSO(Single Sign On)에 Microsoft Entra ID를 사용하도록 SNA(Secure Network Analytics)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Microsoft Azure
- 보안 네트워크 분석

사용되는 구성 요소

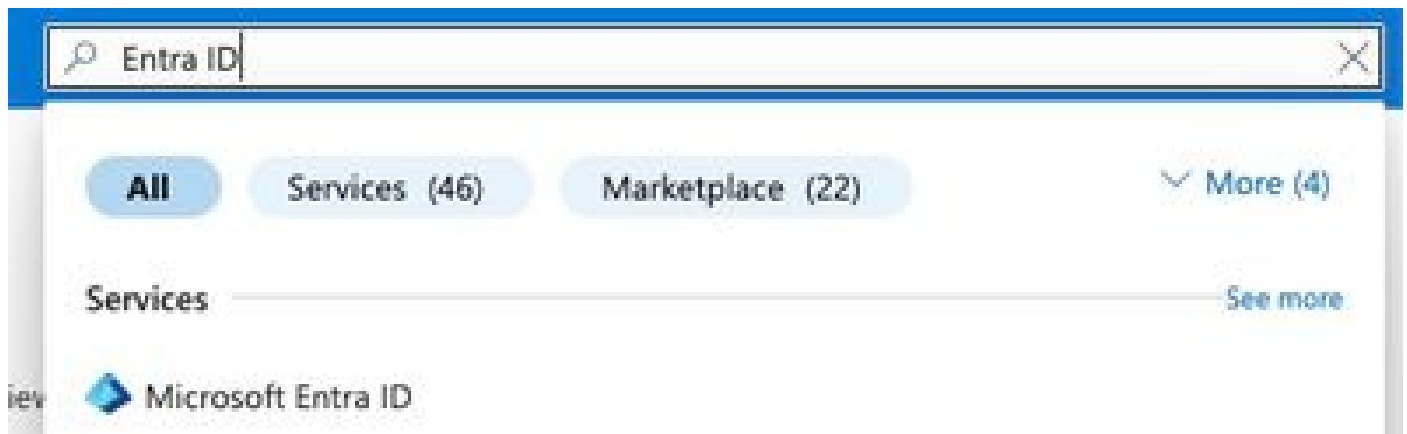
- SNA Manager v7.5.2
- Microsoft Entra ID

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.

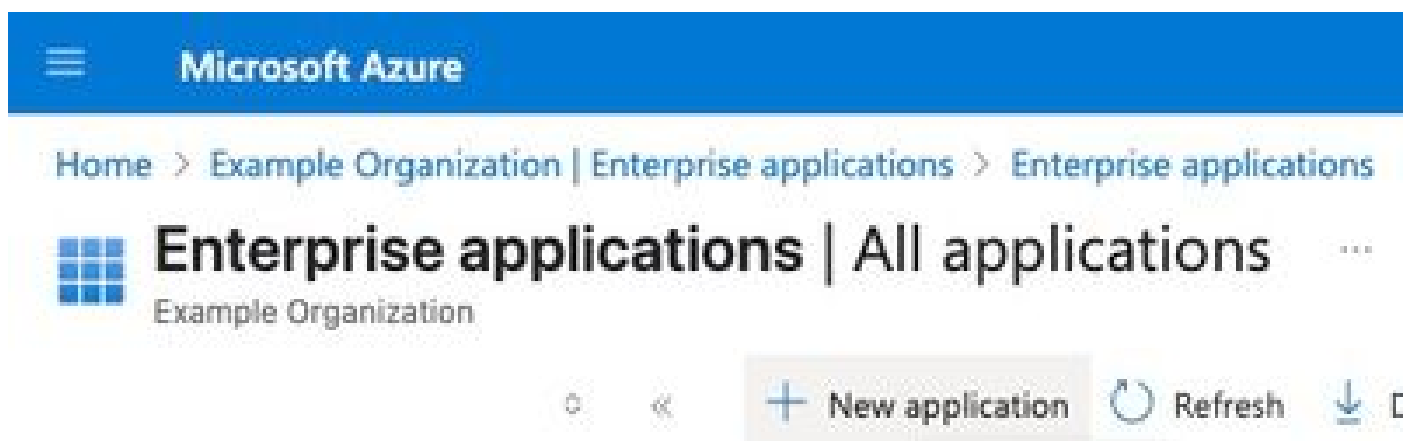
컨피그레이션 단계

Azure에서 엔터프라이즈 응용 프로그램 구성

1. [Azure 클라우드](#) 포털에 [로그인](#)합니다.
2. 검색 상자에서 Entra ID 서비스를 검색하고 Microsoft Entra ID를 선택합니다.



3. 왼쪽 창에서 Manage(관리)를 확장하고 Enterprise Applications(엔터프라이즈 애플리케이션)를 선택합니다.
4. 신규 애플리케이션을 클릭합니다.



5. 로드되는 새 페이지에서 사용자 고유의 응용 프로그램 생성을 선택합니다.



[Home](#) > [Enterprise applications](#) | [All applications](#) >

Browse Microsoft Entra Gallery



Create your own application



Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of applications. Browse or create your own application here. If you are want



Sir

Cloud platforms

Azure-UI

6. 앱의 이름을 입력하세요. 필드.

7. 라디오 버튼 갤러리(비갤러리)에서 찾을 수 없는 다른 모든 응용 프로그램 통합을 선택하고 생성을 클릭합니다.

Create your own application



Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

An Example SNA App Name



What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

8. 새로 구성된 애플리케이션 대시보드에서 Set up single sign on을 클릭합니다.

An Example SNA App Name | Overview ...
Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Security

Activity

Troubleshooting + Support

Properties

Name ⓘ
An Example SNA App Name

Application ID ⓘ
[Redacted] ...

Object ID ⓘ
[Redacted] ...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
[Get started](#)

9. SAML을 선택합니다.

The screenshot shows the 'Single sign-on' configuration page in the Microsoft Entra ID portal. The left sidebar contains navigation links: Overview, Deployment Plan, Diagnose and solve problems, Manage (expanded), Properties, Owners, Roles and administrators, Users and groups, Single sign-on (selected), and Provisioning. The main content area is titled 'Select a single sign-on method' with a 'Help me decide' link. It features two cards: 'Disabled' (with a crossed-out circle icon) stating 'Single sign-on is not enabled. The user won't be able to launch the app from My Apps.' and 'SAML' (with a puzzle piece icon) describing it as 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

10. [SAML을 사용하여 Single Sign-On 설정] 페이지의 [기본 SAML 구성]에서 [편집]을 클릭합니다.

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating An Example SNA App Name.

The screenshot shows the 'Basic SAML Configuration' section, indicated by a blue circle with the number '1'. It includes an 'Edit' link with a pencil icon. The configuration details are as follows:

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

11. Basic SAML Configuration(기본 SAML 컨피그레이션) 창에서 Add Reply URL to <https://example.com/fedlet/fedletapplication>(에 최신 URL 추가)를 구성하고 example.com을 SNA Manager의 FQDN으로 바꾸고 save(저장)를 클릭합니다.

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



[Add identifier](#)

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



[Add reply URL](#)

12. SAML 인증서 카드를 찾아 App Federation Metadata URL 필드 값을 저장하고 Federation Metadata XML을 다운로드합니다.

3

SAML Certificates

Token signing certificate



Edit

Status

Active

Thumbprint

123456789abcdefghijklmnp

Expiration

6/3/2028, 8:39:10 AM

Notification Email

someuser@example.com

App Federation Metadata Url



Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

Verification certificates (optional)



Edit

Required

No

Active

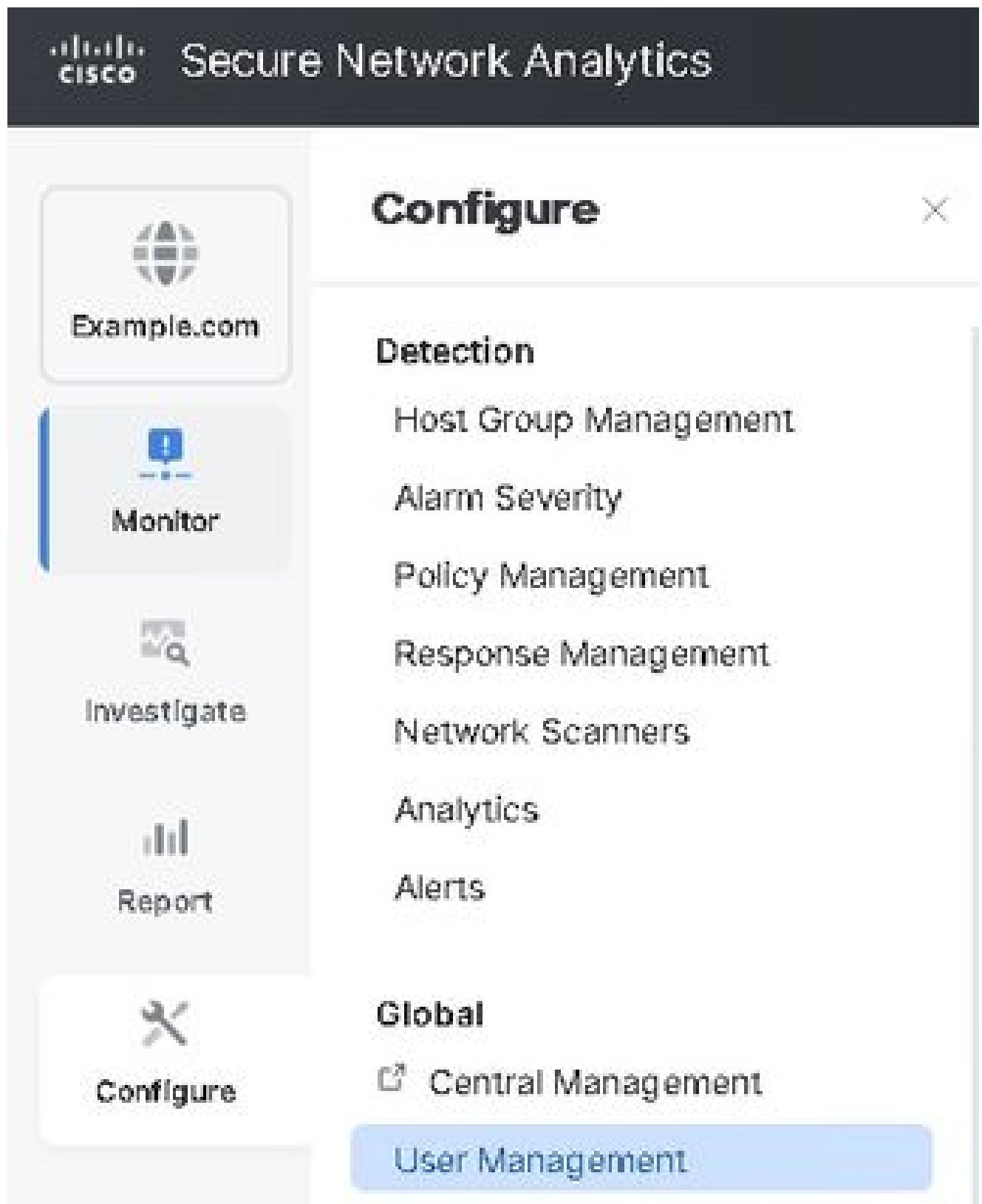
0

Expired

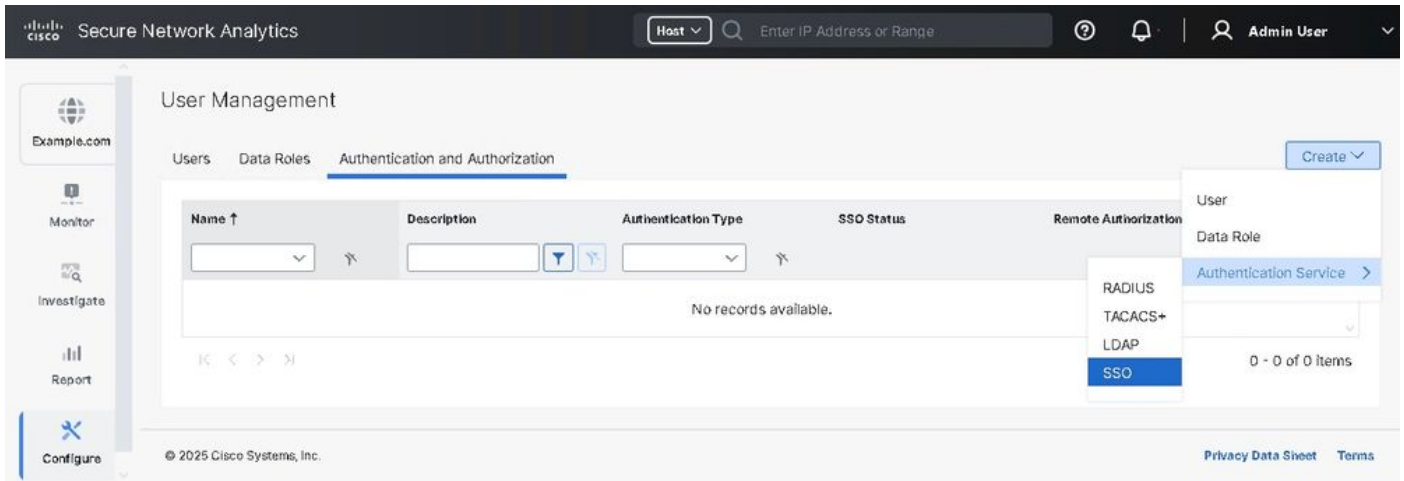
0

SNA에서 서비스 공급자 XML 파일 구성 및 다운로드

1. SNA Manager UI에 로그인합니다.
2. Configure(구성) > Global(전역) > User Management(사용자 관리)로 이동합니다.



3. Authentication and Authorization(인증 및 권한 부여) 탭에서 Create(생성) > Authentication Service(인증 서비스) > SSO를 클릭합니다.



4. ID 제공자 메타데이터 URL 또는 ID 제공자 메타데이터 XML 파일 업로드에 적합한 라디오 버튼을 선택합니다.

The screenshot shows the Cisco Secure Network Analytics User Management | Authentication Service configuration page. The page is divided into three sections: Authentication Service, Identity Provider, and General Configuration.

Authentication Service

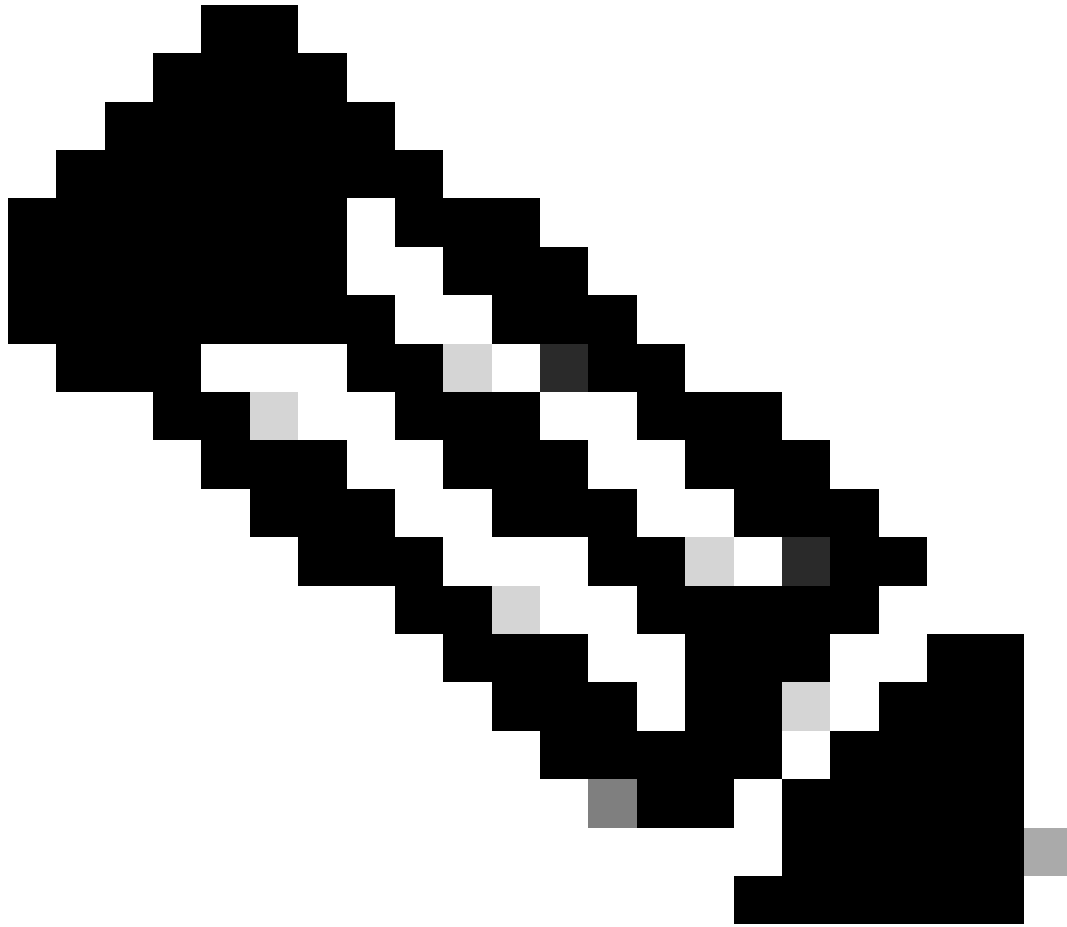
- Authentication Service Type: SSO
- Name: SSO
- Description:

Identity Provider

- Identity Provider Type: Microsoft Entra ID
- Status: Ready
- Identity Provider Metadata URL:
- Upload Identity Provider Metadata XML File: XML format required. Add File

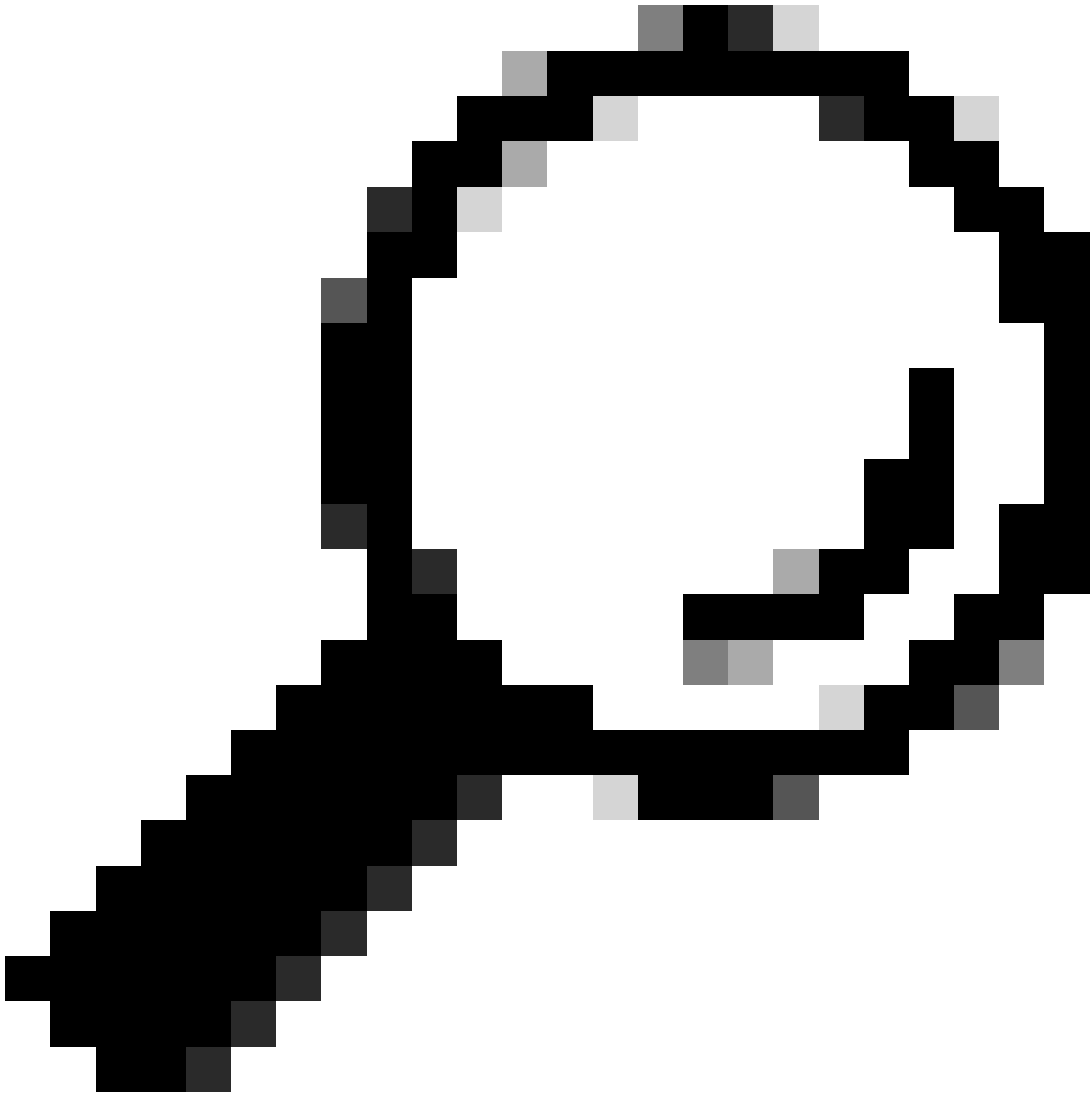
General Configuration

- Name Identifier Format: Persistent
- Login Screen Label: popup
- Custom Service Provider Address: ex. sna-manager.example.com or 192.168.10.10



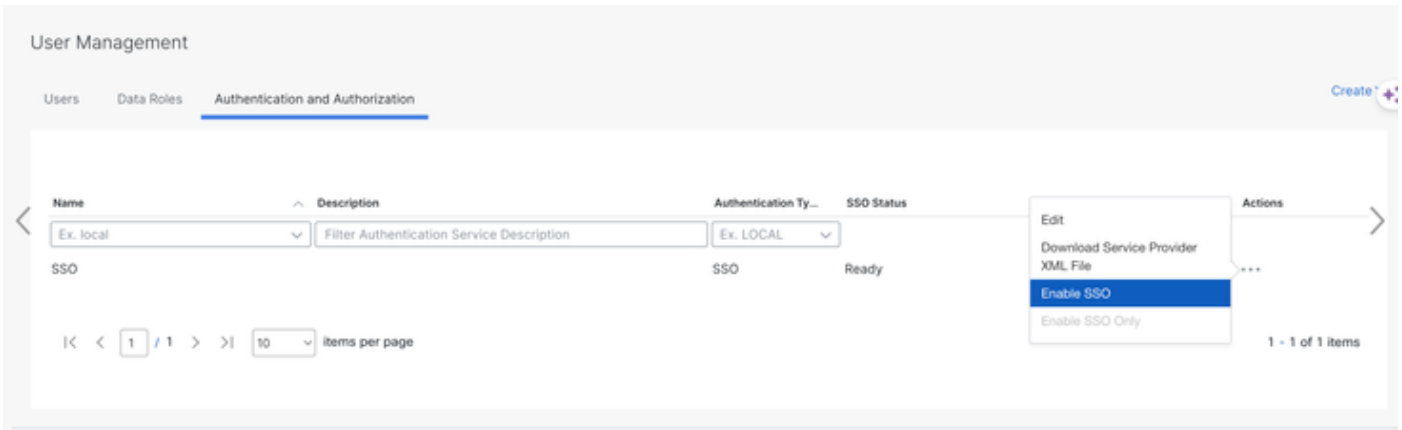
참고: 이 데모에서는 Upload Identity Provider Metadata XML File(ID 제공자 메타데이터 XML 파일 업로드)을 선택합니다.

5. Microsoft Entra ID로 ID 공급자 유형 필드, 영구으로 이름 식별자 형식, 로그인 화면 레이블을 구성합니다.

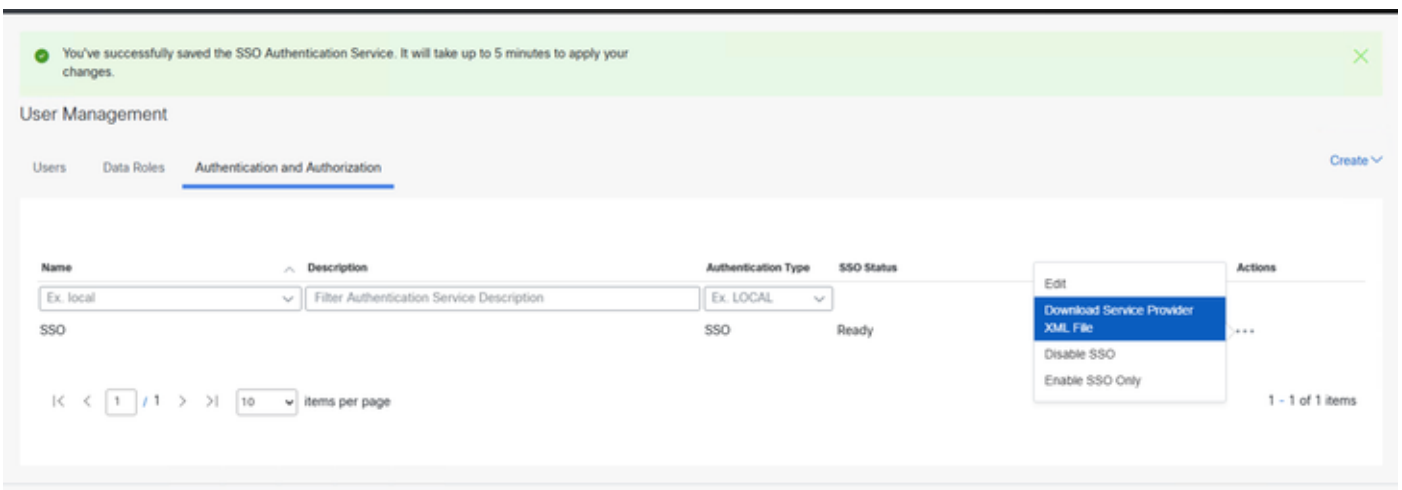


팁: 구성된 로그인 화면 레이블(이름/텍스트)은 SSO로 로그인 버튼 위에 표시되며 비워둘 수 없습니다.

-
6. 저장을 눌러 인증 및 권한 부여 탭으로 돌아갑니다.
 7. 상태가 READY(준비)가 될 때까지 기다린 후 조치 메뉴에서 SSO 활성화를 선택합니다.



8. Authentication and Authorization(인증 및 권한 부여) 탭 아래의 Actions(작업) 열에서 세 개의 점을 클릭하고 Download Service Provider XML File(서비스 공급자 XML 파일 다운로드)을 클릭합니다.



Azure에서 SSO 구성

1. [Azure](#) 포털에 [로그인합니다](#).
2. 검색 표시줄에서 Enterprise Application > 구성된 Enterprise Application 선택 > Setup Single Sign On으로 이동합니다.
3. 페이지 상단에서 메타데이터 파일 업로드를 클릭하고 SNA Manager에서 다운로드한 sp.xml 파일을 업로드합니다.
4. "기본 SAML 구성" 화면을 열고 다양한 설정을 통해 값을 수정하고 저장을 클릭합니다.



Home > An Example SNA App Name

An Example SNA App Name | SAML-based Sign-on

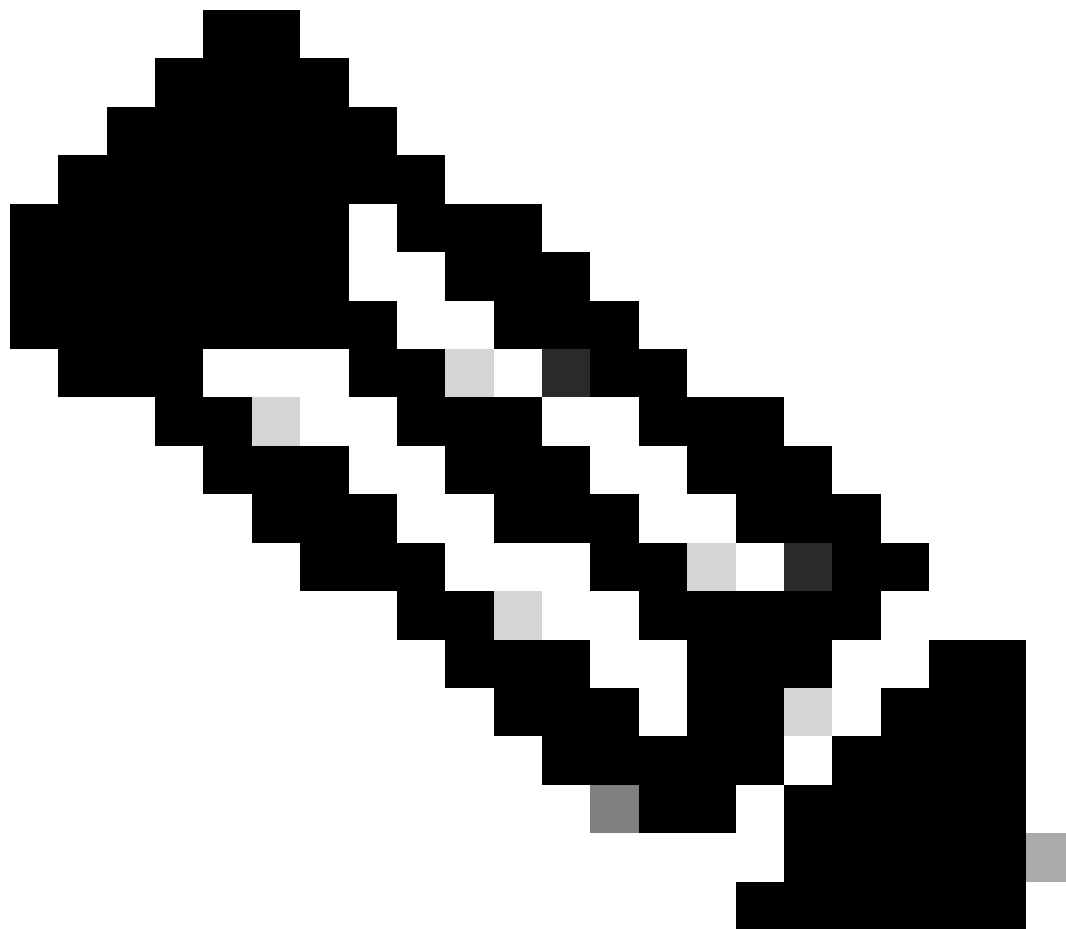
Enterprise Application



Upload metadata file



Change single sign-on



참고: Entra ID의 Name ID Format(이름 ID 형식)이 올바른지 확인합니다.

5. 속성 및 클레임 섹션을 찾은 후 편집을 클릭합니다.

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating An Example SNA App Name.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://example.com/fedlet
Reply URL (Assertion Consumer Service URL)	https://your-sna-manager-fqdn.com/fedlet/fedletapplication
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2

Attributes & Claims

Edit

Edit u

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

6. 청구명 섹션에서 user.userprincipalname value를 클릭합니다.

Home > An Example SNA App Name | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ...

7. 청구 관리 페이지에서 이름 식별자 형식을 선택합니다.



Manage claim ...



Save



Discard changes



Got feedback?

Name

nameidentifier

Namespace

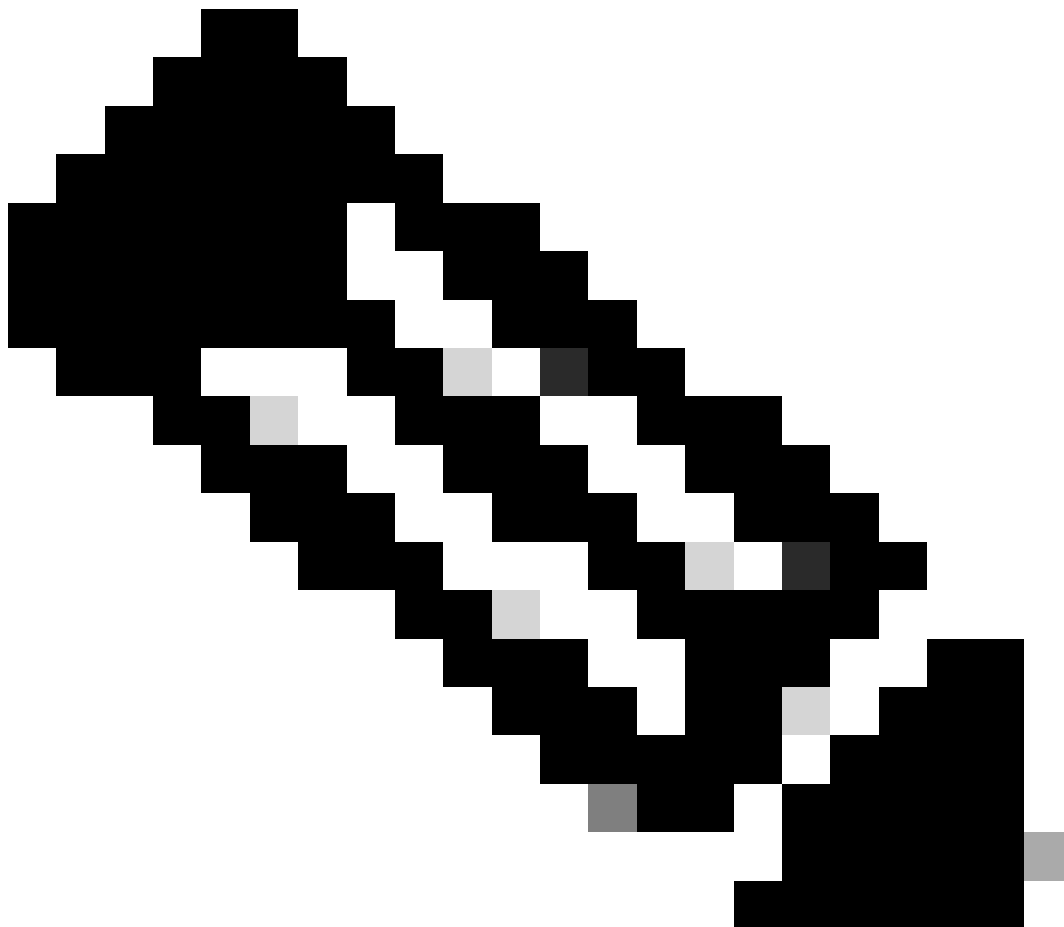
http://schemas.xmlsoap.org/ws/2005/05/identity/claims



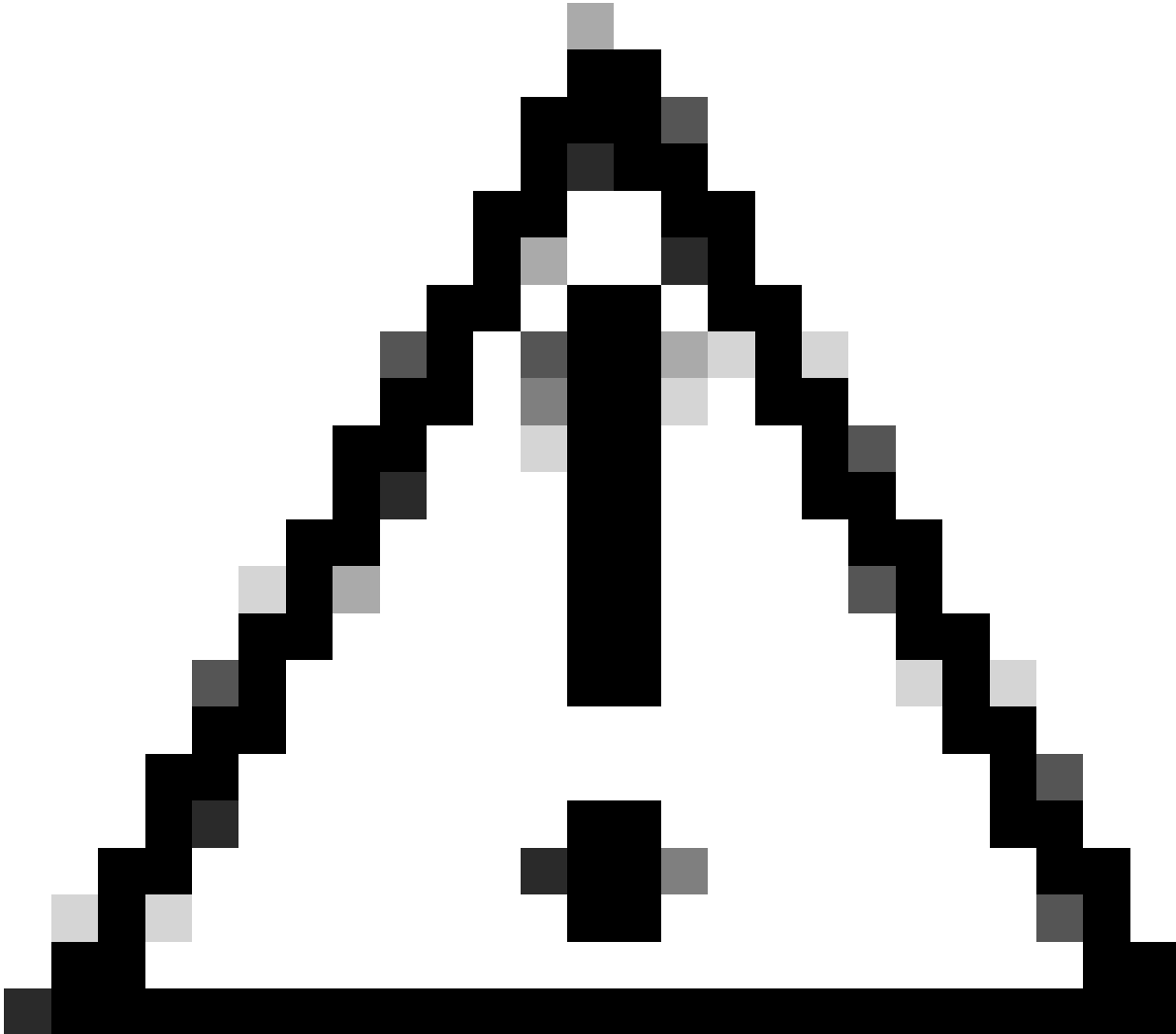
Choose name identifier format

Name identifier format *

Persistent



참고: 이름 식별자 형식 필드가 지속적(그렇지 않은 경우)으로 설정된 경우 드롭다운 메뉴에서 선택합니다. 변경 사항이 있는 경우 저장을 클릭합니다.



주의: 이 곳에서 가장 자주 문제를 접하게 됩니다. SNA 관리자 및 Microsoft Azure의 설정이 일치해야 합니다. SNA에서 "emailAddress" 형식을 사용하기로 선택한 경우,여기의 형식도 "Email Address"여야 합니다.

Entra ID에서 사용자를 설정합니다.

1. [Azure](#) 포털에 [로그인합니다](#).
2. 검색 표시줄에서 Enterprise Application > 구성된 Enterprise Application 선택 > 왼쪽의 사용자 및 그룹 선택 > 사용자/그룹 추가를 누릅니다.

Microsoft Azure

Home > An Example SNA App Name

An Example SNA App Name | Users and groups

Enterprise Application

+

 Add user/group
 Edit assignment
 Remove as:

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

The application will appear for assigned users within My App

Assign users and groups to app-roles for your application here

First 200 shown, search all users & groups

Display name

No application assignments found

3. 왼쪽 창에서 None Selected(선택 안 함)를 클릭합니다.

4. 필요한 사용자를 검색하여 애플리케이션에 추가합니다.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > An Example SNA App Name | Users and groups >

Add Assignment

Example Organization

Users and groups

None Selected

Select a role

User

Users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

1 result found

All Users Groups

	Name	Type	Details
☒	Example User	User	user@example.com

Selected (1)

Reset

Example User

user@example.com

Assign

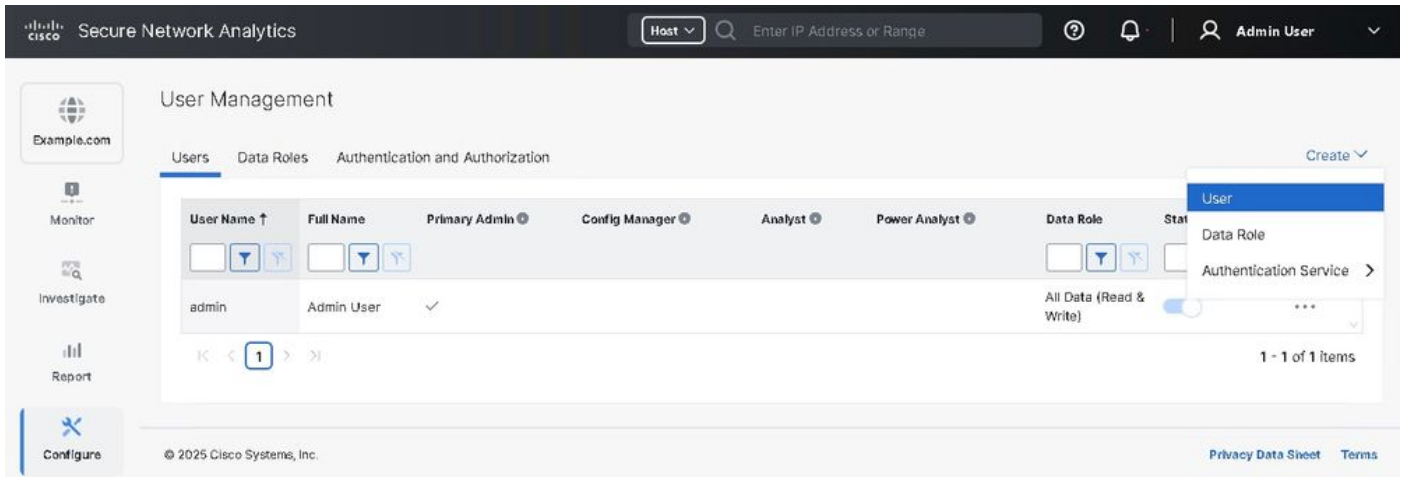
Select

SNA에서 SSO 구성

1. SNA Manager UI에 로그인합니다.

2. 구성 > 글로벌 > 사용자 관리로 이동합니다.

3. 생성 > 사용자를 클릭합니다.



4. SSO로 선택한 인증 서비스에 관련 세부 정보를 제공하여 사용자를 구성하고 저장을 클릭합니다.

User Name *

Full Name

Email

SAML ID *

Authentication Service

SSO

Password

Generate Password

Confirm Password

Show Password

Role Settings

Primary Admin

Data Role

All Data (Read Only)

You must select a minimum of one web role and one desktop client role.

Web Desktop

Web Roles * Compare

Configuration Manager Analyst Power Analyst

SNA-UI에서 SAML-사용자 생성

문제 해결

사용자가 SNA Manager에 로그인할 수 없는 경우 SAML 추적기를 사용하여 더 자세히 조사할 수 있습니다.

SNA Manager를 조사하는 데 추가 지원이 필요한 경우 TAC 케이스를 제기할 수 있습니다.

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

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.