

# Microsoft Entra ID SSO用のSNAマネージャの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定手順](#)

[Azureでエンタープライズアプリケーションを構成](#)

[SNAでのサービスプロバイダーXMLファイルの設定およびダウンロード](#)

[AzureでSSOを構成する](#)

[Enter IDでユーザを設定します。](#)

[SNAでのSSOの設定](#)

[トラブルシューティング](#)

---

## はじめに

このドキュメントでは、シングルサインオン(SSO)にMicrosoft Entra ID(MID)を使用するようにSecure Network Analytics(SNA)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Microsoft Azure
- Cisco Secure Network Analytics

### 使用するコンポーネント

- SNAマネージャv7.5.2
- MicrosoftエントリID

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

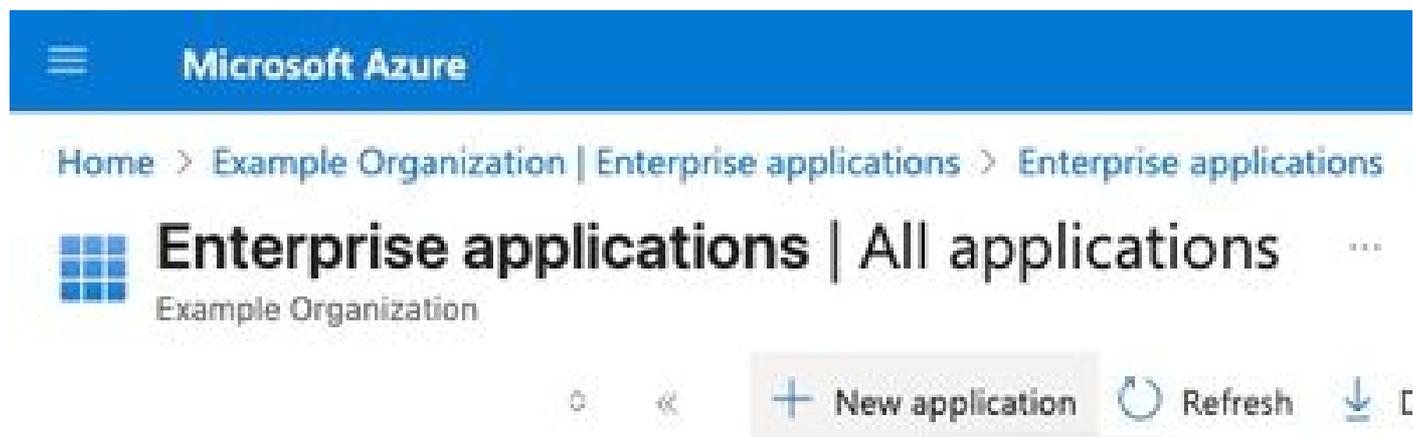
## 設定手順

## Azureでエンタープライズアプリケーションを構成

1. [Azureクラウドポータル](#)にログインします。
2. 検索ボックスでEntra IDサービスを検索し、Microsoft Entra IDを選択します。



3. 左側のペインでManageを展開し、Enterprise Applicationsを選択します。
4. New Applicationをクリックします。



5. ロードする新規ページで、「独自のアプリケーションの作成」を選択します。



[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. 「アプリケーションの名前は何ですか。」フィールドにアプリケーションの名前を入力します。
7. 「Integrate any other application you don't find in the gallery (Non-gallery)」ラジオ・ボタンを選択し、「Create」をクリックします。

# 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. 新しく構成されたアプリケーションダッシュボードで、[シングルサインオンのセットアップ]をクリックします。

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

Overview

- Deployment Plan
- Diagnose and solve problems
- > Manage
- > Security
- > Activity
- > Troubleshooting + Support

## Properties

**AE** Name ⓘ  
An Example SNA App Name

Application ID ⓘ

Object ID ⓘ

## 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. SAMLを選択します。

## 10. SAMLによるシングルサインオンの設定ページで、基本SAML設定の下の編集をクリックします。

### 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.

Identifier (Entity ID)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

## 11. Basic SAML Configurationペインで、Add Reply URL to <https://example.com/fedlet/fedletapplication>を設定し、[example.com](https://example.com)をSNA ManagerのFQDNに置き換えて、saveをクリックします。

# 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 Certificatesカードを見つけ、App Federation Metadata URLフィールド値を保存し、Federation Metadata XMLをダウンロードします。

**3** SAML Certificates

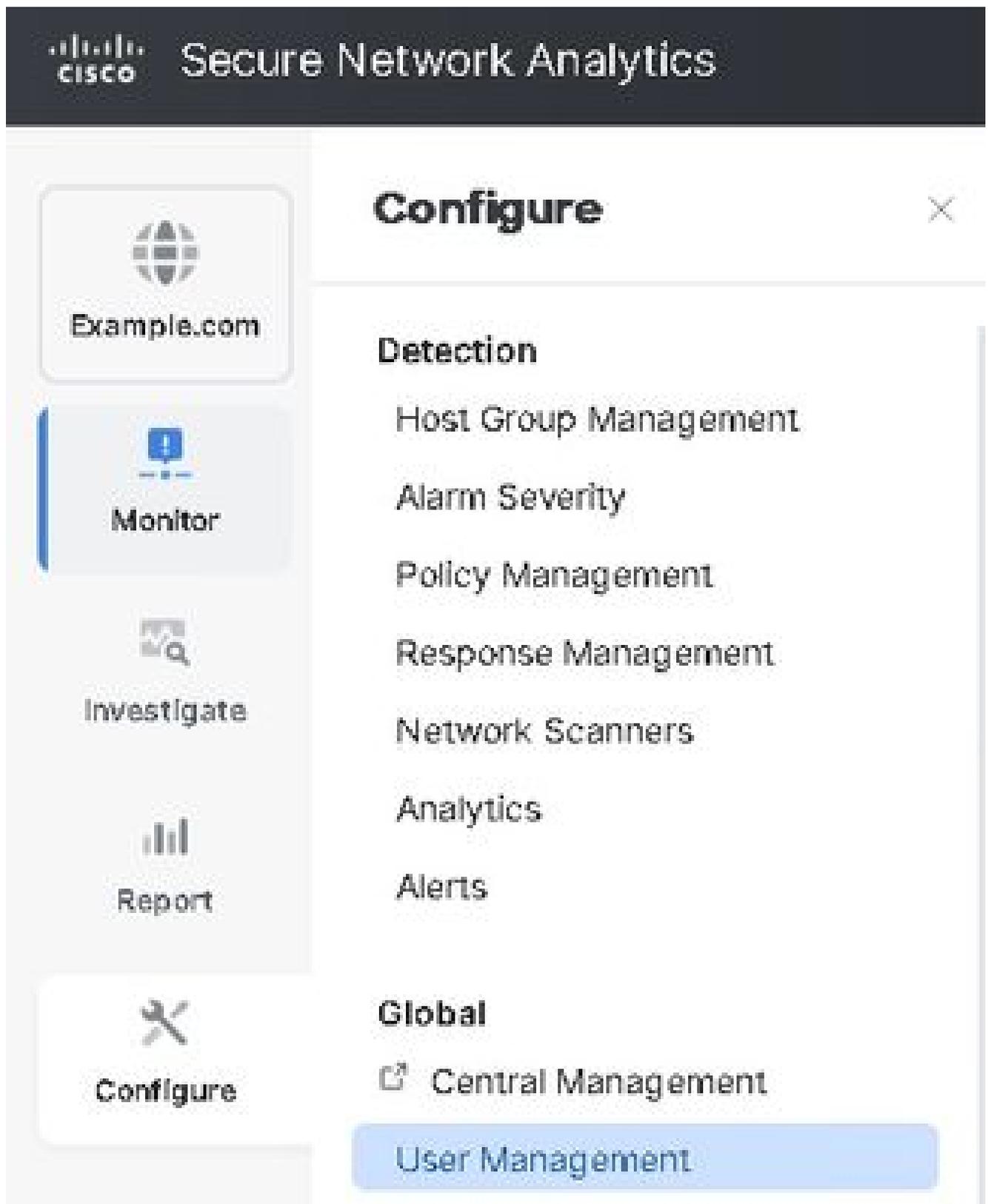
Token signing certificate		 Edit
Status	Active	
Thumbprint	123456789abcdefghijklmnop	
Expiration	6/3/2028, 8:39:10 AM	
Notification Email	someuser@example.com	
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/af42bac0-52aa- ..."/> 	
Certificate (Base64)	<a href="#">Download</a>	
Certificate (Raw)	<a href="#">Download</a>	
Federation Metadata XML	<a href="#">Download</a>	

---

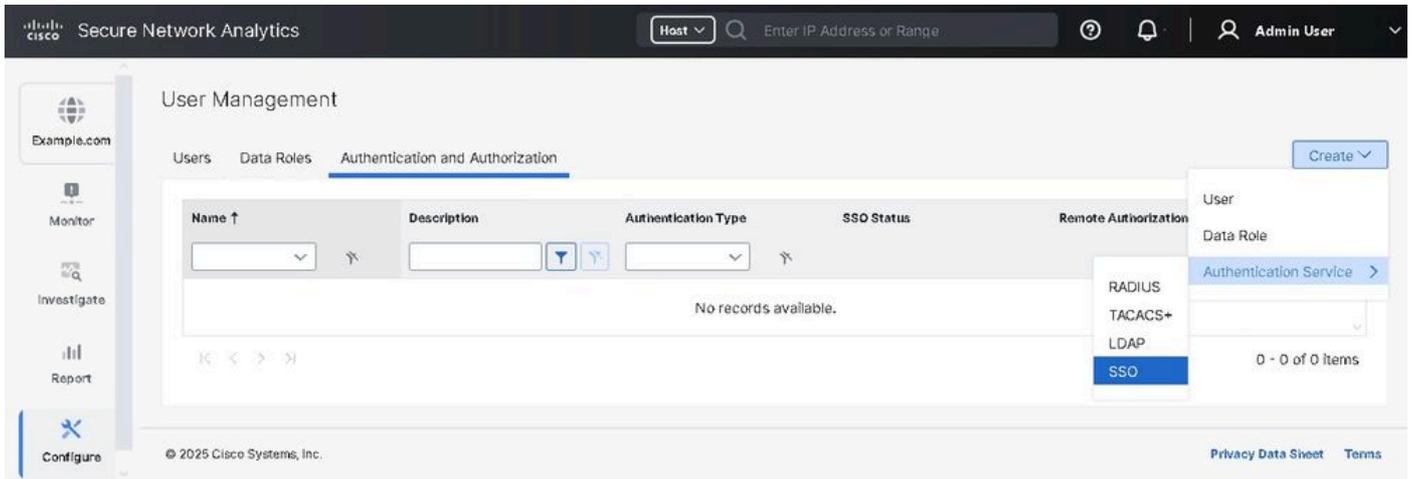
Verification certificates (optional)		 Edit
Required	No	
Active	0	
Expired	0	

SNAでのサービスプロバイダーXMLファイルの設定およびダウンロード

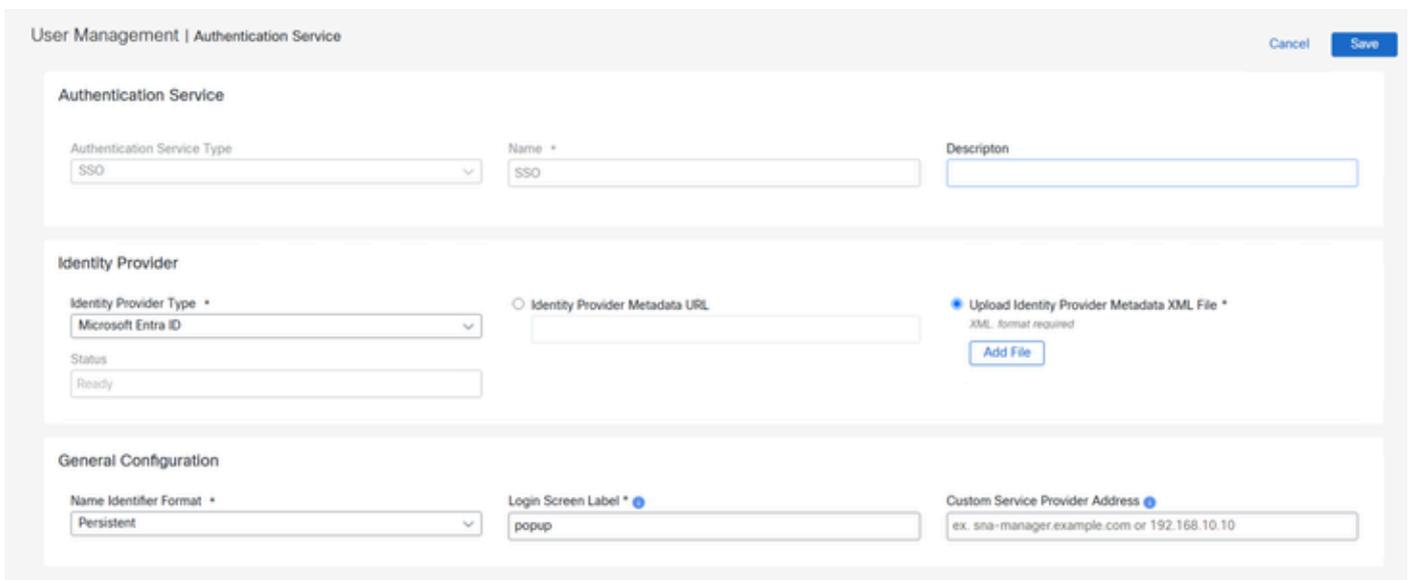
1. SNAマネージャUIにログインします。
2. Configure > Global > User Managementの順に選択します。

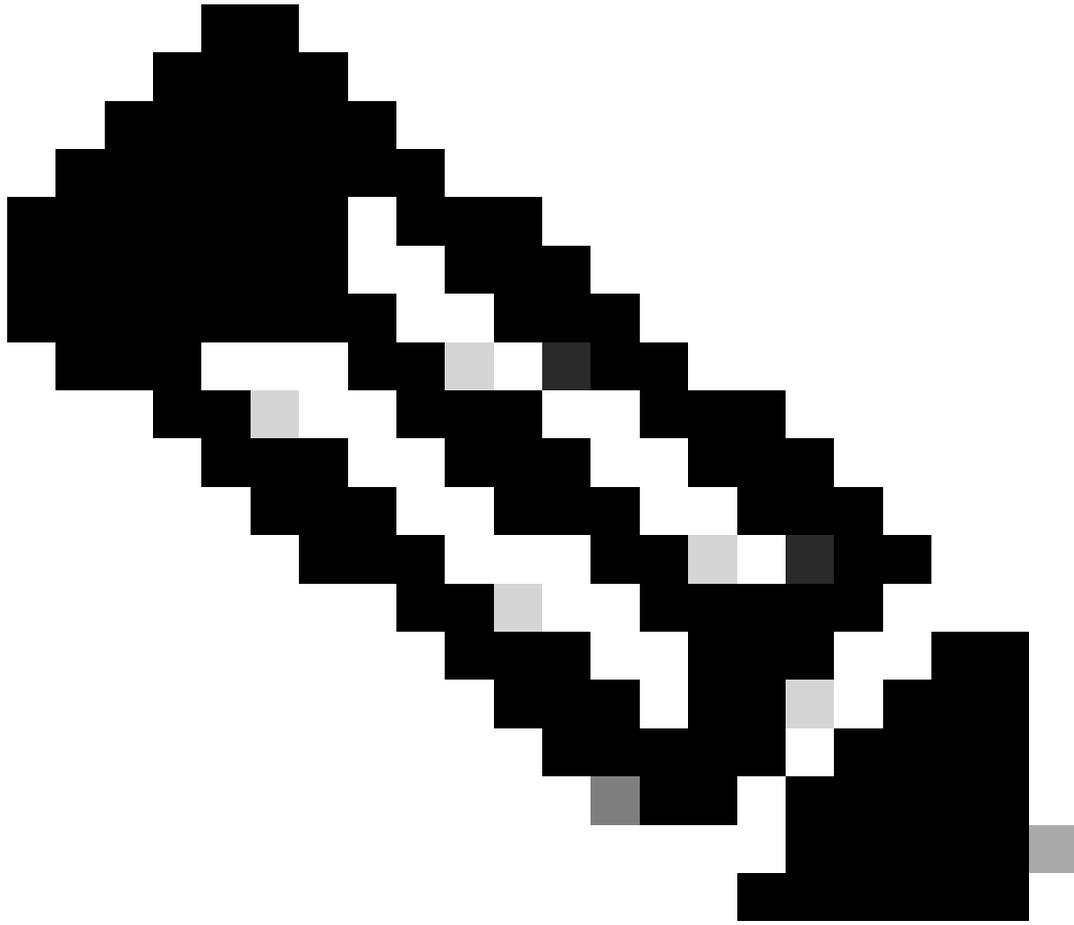


3. Authentication and Authorizationタブで、Create > Authentication Service > SSOの順にクリックします。



4. 「IDプロバイダのメタデータURL」または「IDプロバイダのメタデータXMLファイルのアップロード」に適切なラジオ・ボタンを選択します。

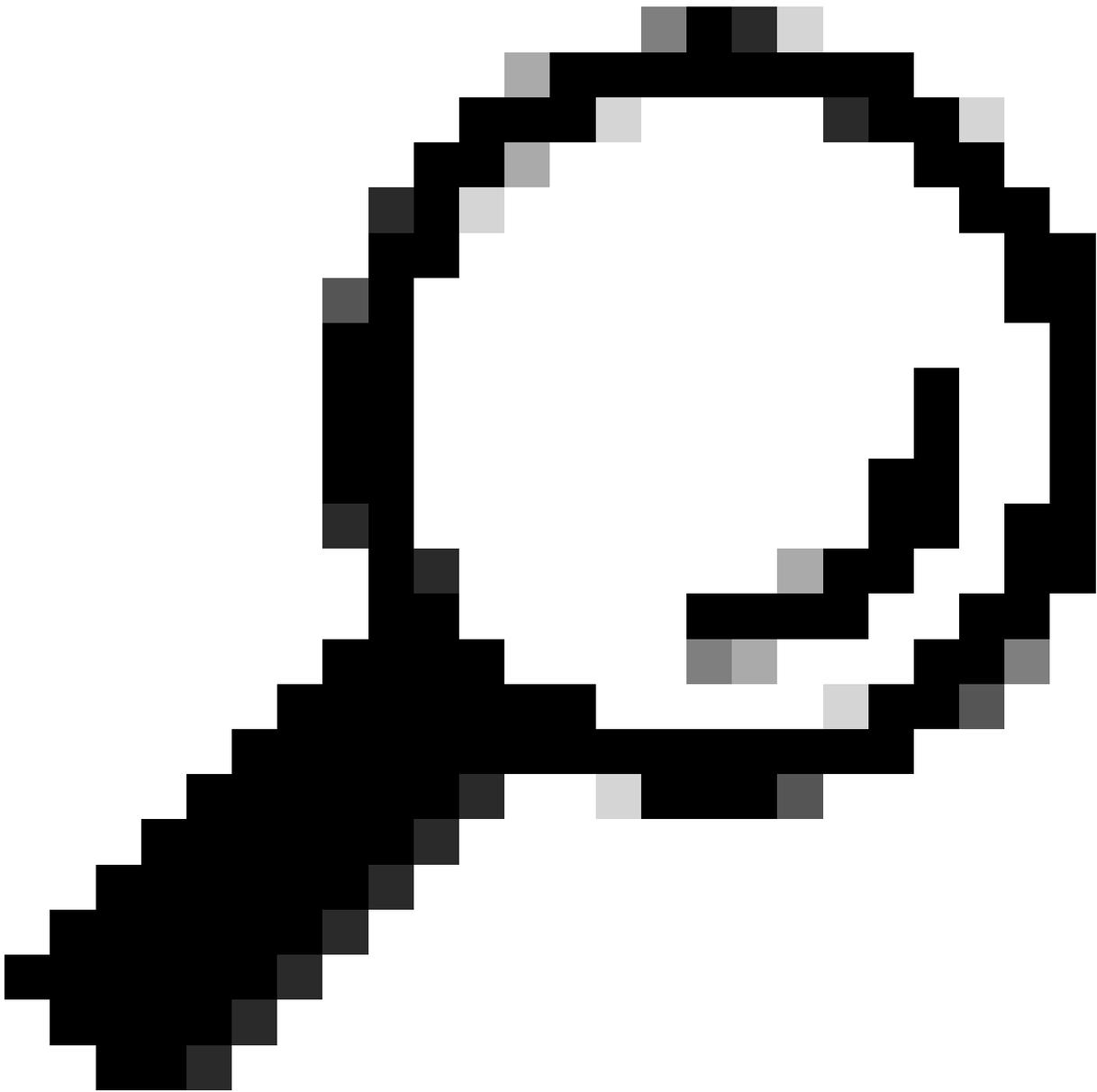




注：このデモでは、IDプロバイダーのメタデータXMLファイルのアップロードが選択されています。

---

5. IDプロバイダータイプフィールドをMicrosoft Entra IDに、名前識別子フォーマットを Persistentに設定し、ログイン画面ラベルを入力します。

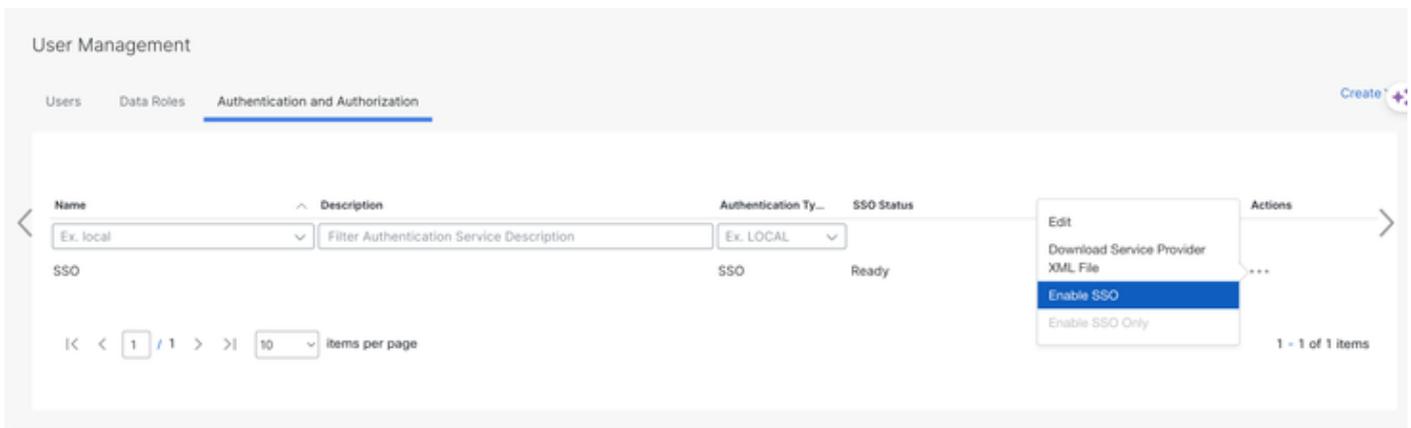


ヒント：設定済みのログイン画面ラベル（名前/テキスト）がSSOでのログインボタンの上に表示されます。このラベルを空のままにしないでください。

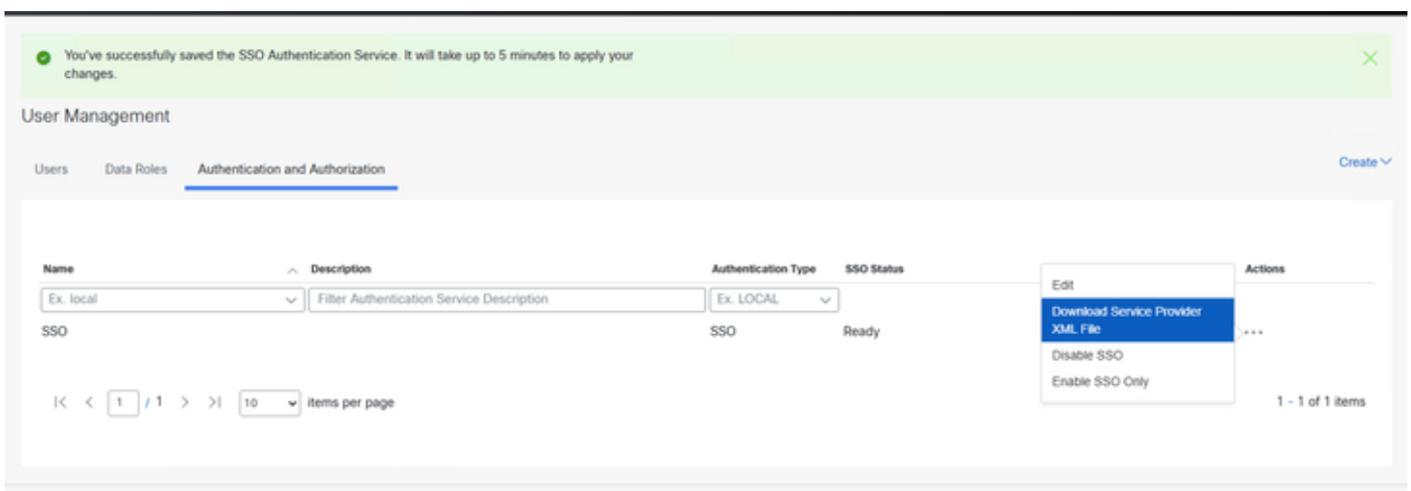
---

6. Saveをクリックすると、Authentication and Authorizationタブに戻ります。

7. ステータスがREADYになるまで待ち、アクションメニューからEnable SSOを選択します。



8. Authentication and Authorizationタブで、Actions列の3つのドットをクリックして、Download Service Provider XML Fileをクリックします。



## AzureでSSOを構成する

1. [Azureポータル](#)にログインします。
2. 検索バーから、Enterprise Application > Select configured Enterprise Application > Setup single sign onの順に選択します。
3. ページの上部にあるUpload metadata fileをクリックして、SNA Managerからダウンロードしたsp.xmlファイルをアップロードします。
4. 「基本的なSAML構成」画面が開き、さまざまな設定を正しい値に設定し、「保存」をクリックします。



Home > An Example SNA App Name

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

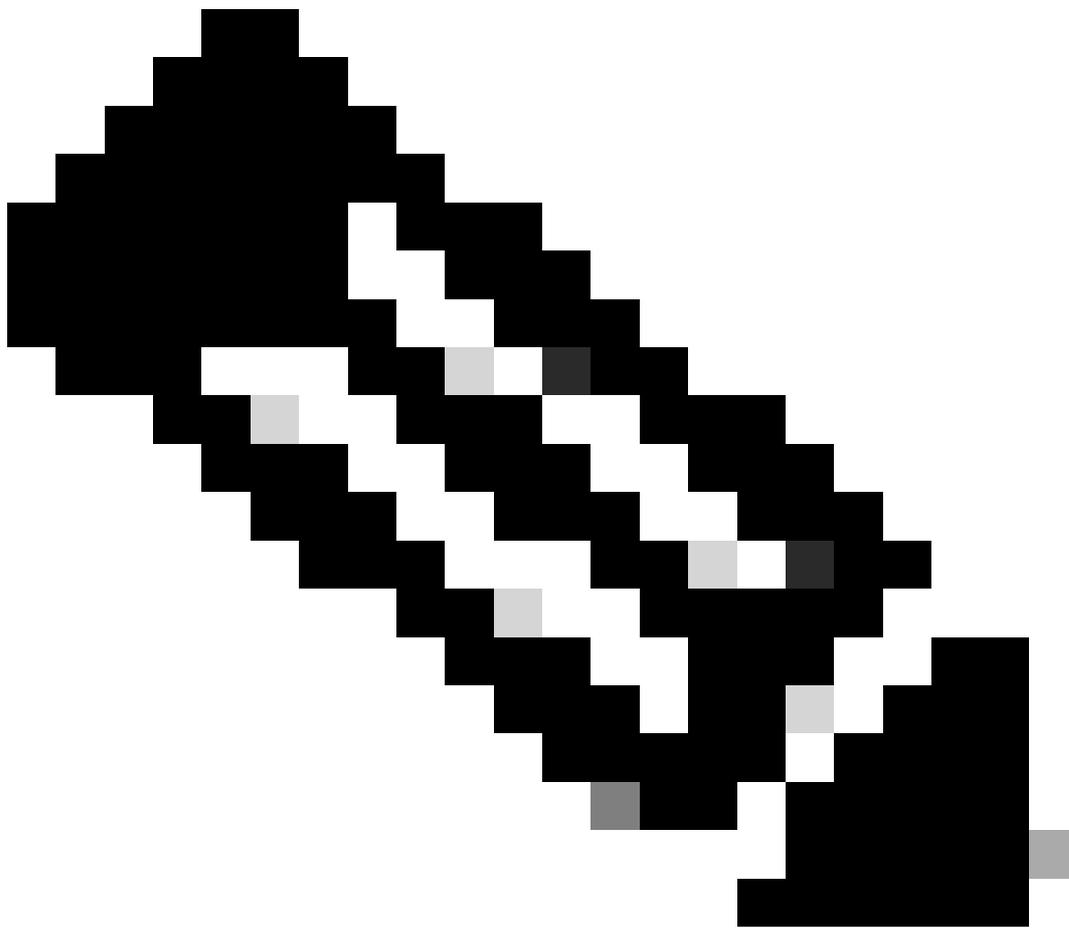
Enterprise Application



Upload metadata file



Change single sign-on



注:Entra IDの名前IDの形式が正しいことを確認してください。

5. 「Attributes & Claims」 セクションを探し、「Edit」をクリックします。

## 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

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

6. Claim Nameセクションにあるuser.userprincipalname値をクリックします。

[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. Manage Claim pageで、Choose name identifier formatを確認します。



# Manage claim ...

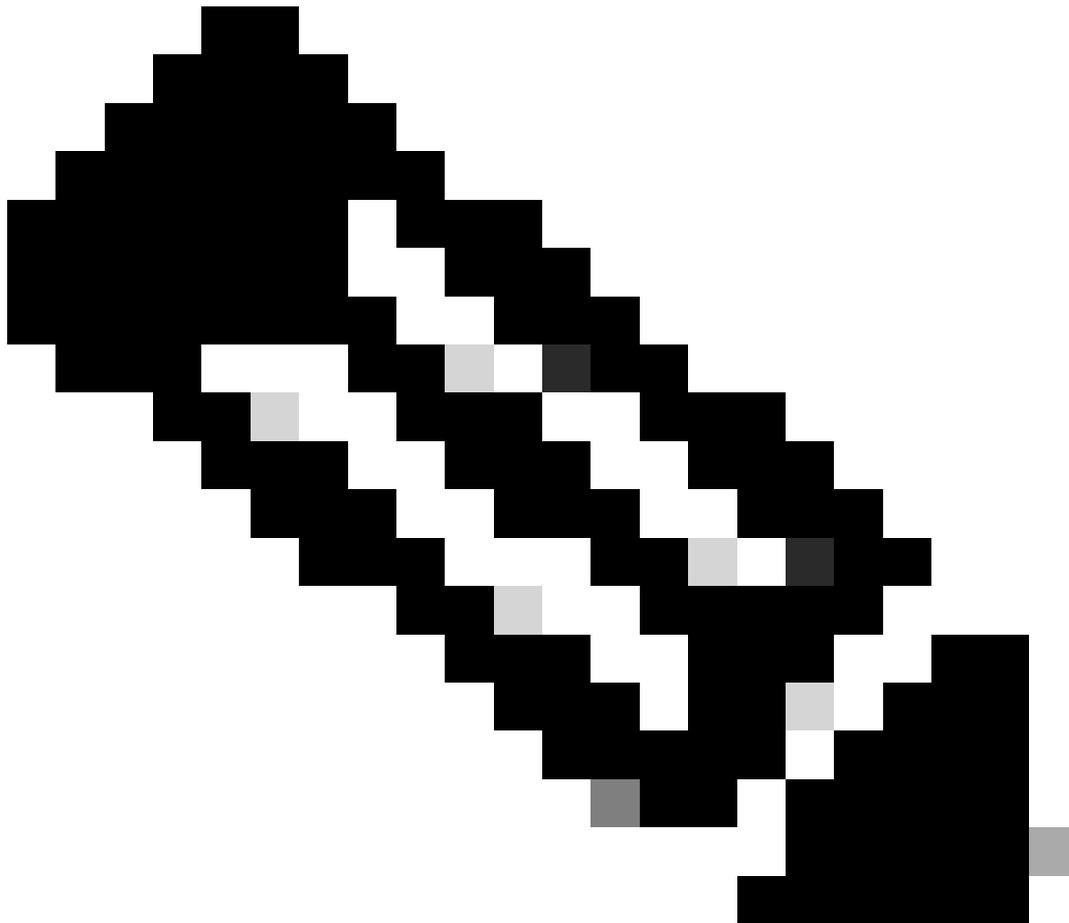
Save Discard changes | Got feedback?

Name

Namespace

^ Choose name identifier format

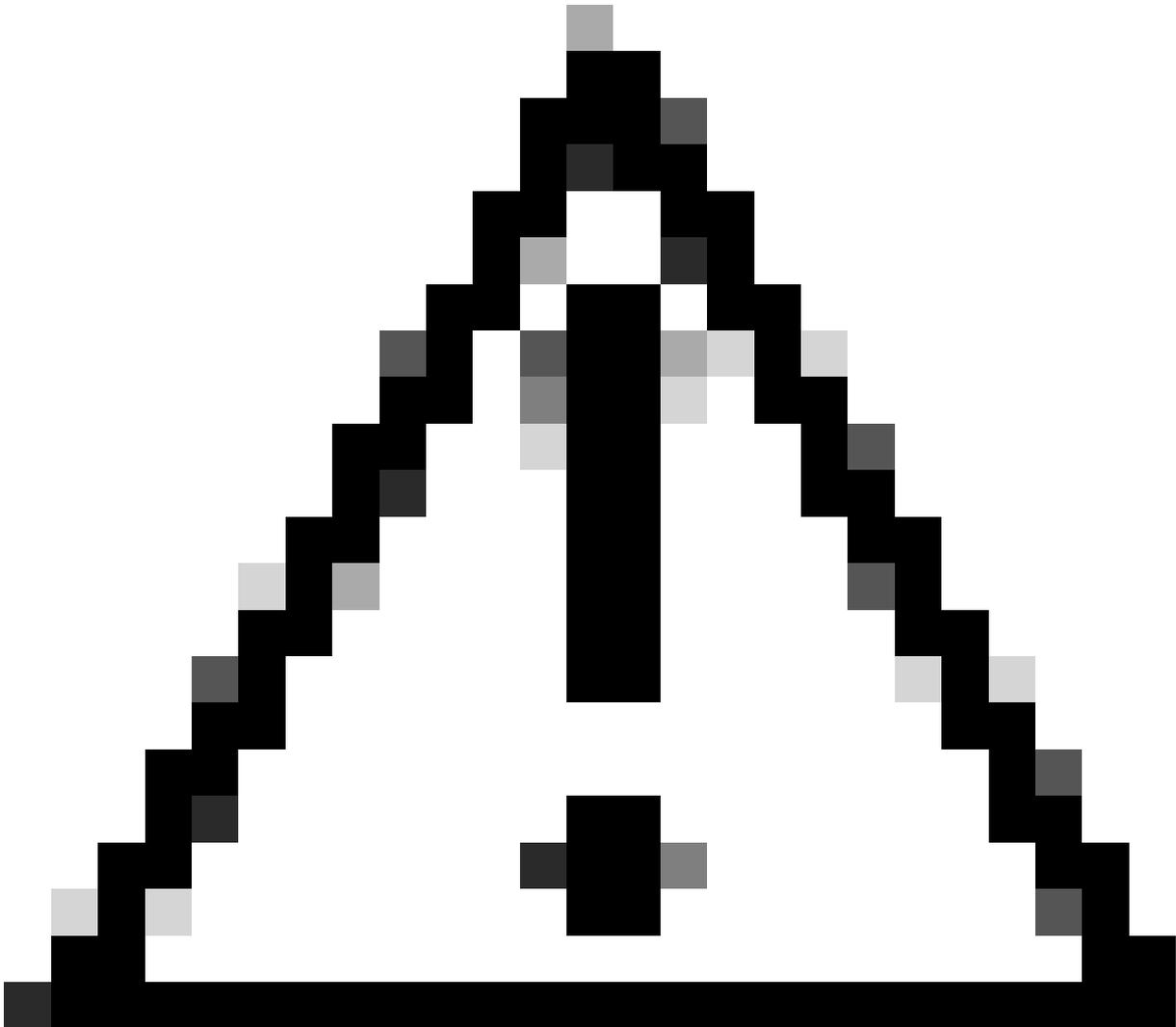
Name identifier format \*



---

注：名前ID形式フィールドが設定されていない場合は永続に設定され、ドロップダウンメニューから選択します。変更が行われた場合は、[保存]をクリックします。

---

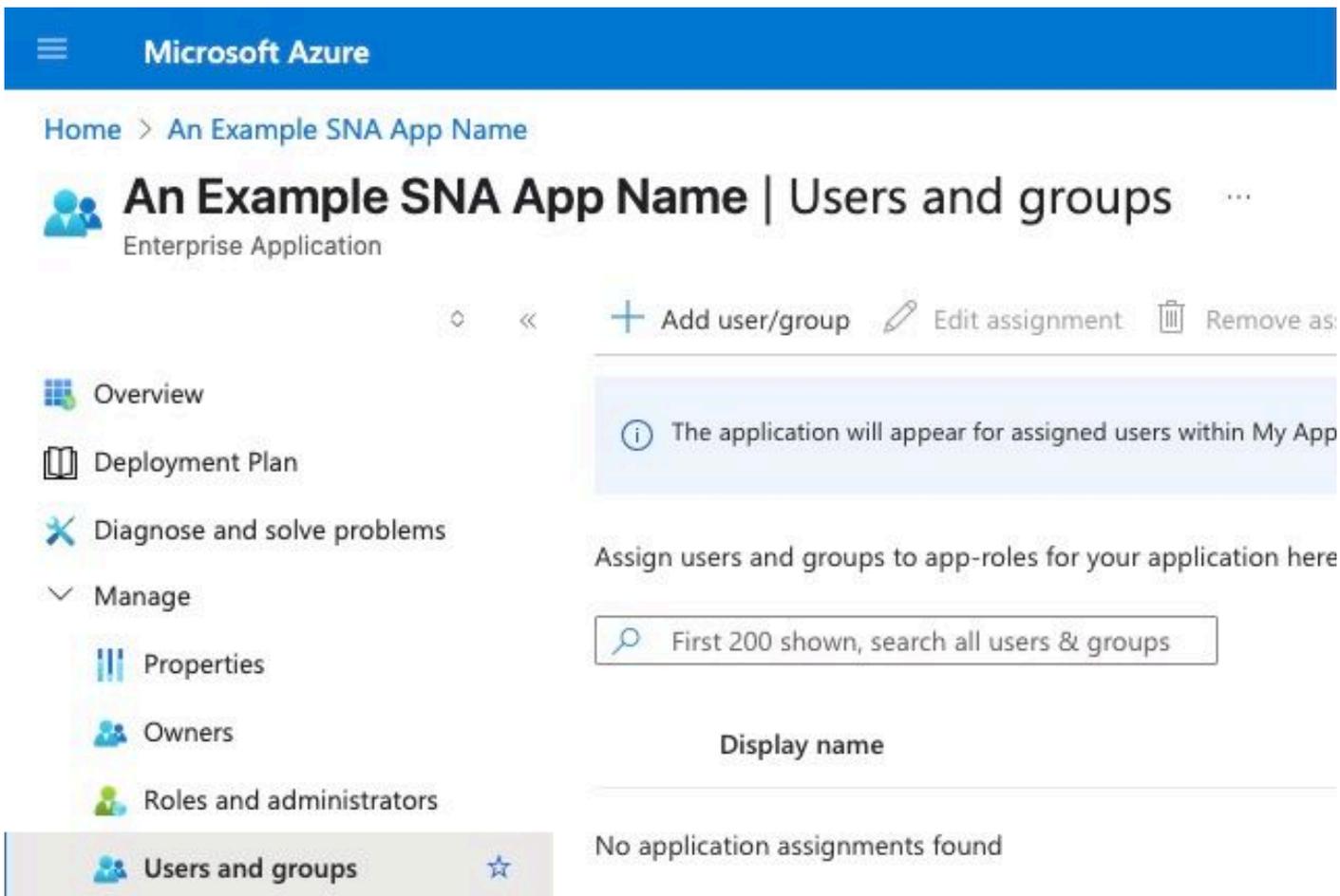


注意：問題が発生する最も一般的な場所です。SNAマネージャとMicrosoft Azureの設定が一致する必要があります。SNAでemailAddress形式を使用することを選択した場合は、この形式もEmail Addressである必要があります。

---

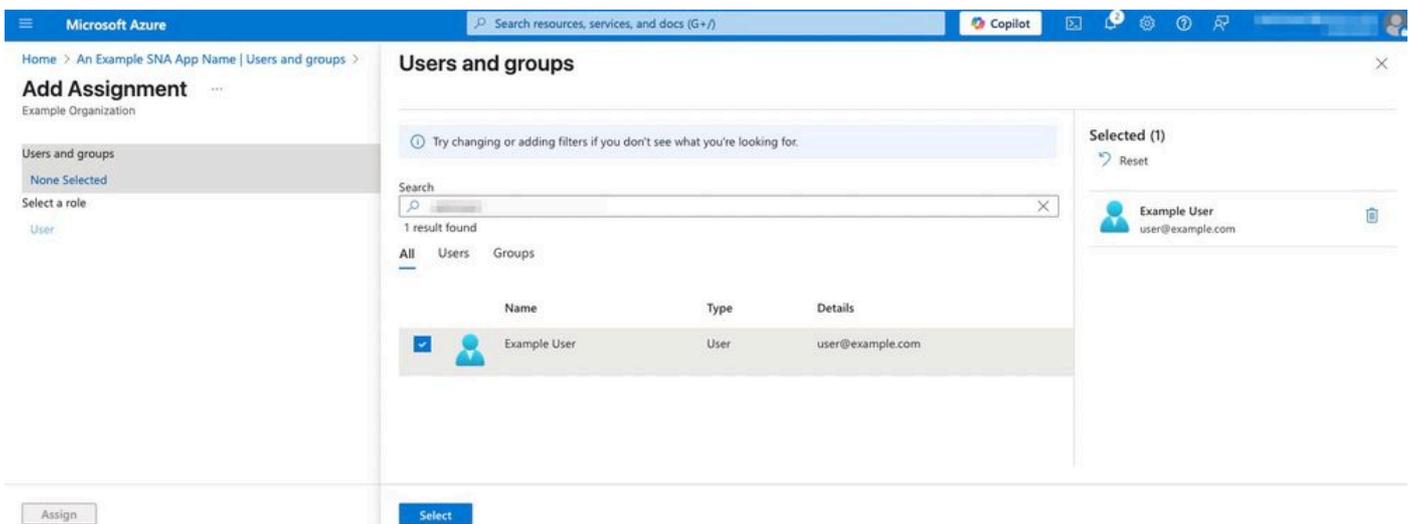
Enter IDでユーザを設定します。

1. [Azureポータル](#)にログインします。
2. 検索バーからEnterprise Application > Select configured Enterprise Application > 左側のUsers and Groupsを選択 > Add user/groupをクリックします。



3. 左側のペインでNone Selectedをクリックします。

4. 必要なユーザーを検索し、アプリケーションに追加します。

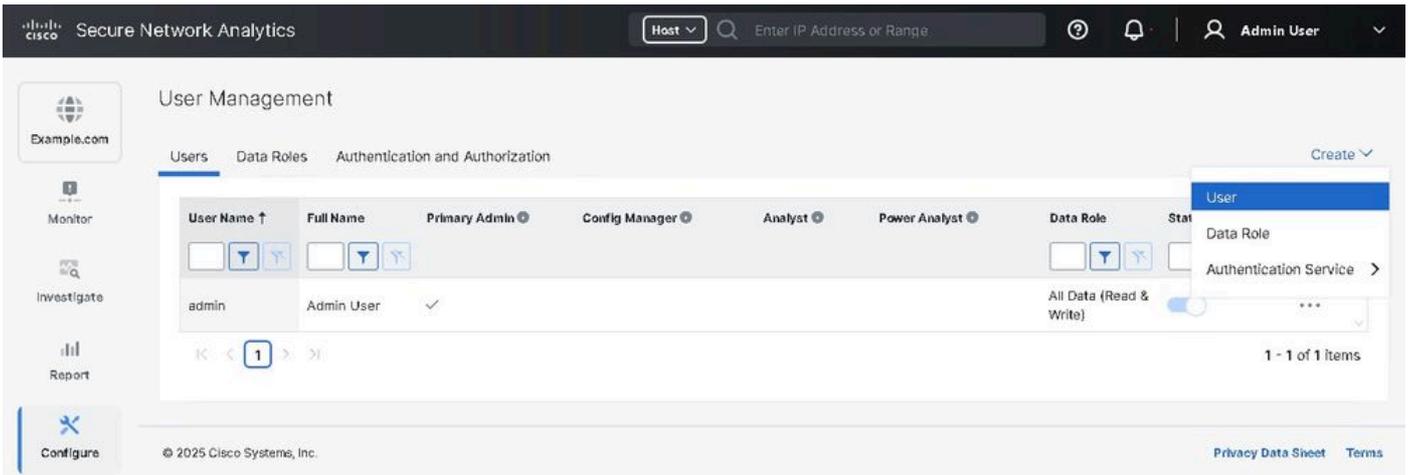


## SNAでのSSOの設定

1. SNAマネージャUIにログインします。

2. 「構成」>「グローバル」>「ユーザー管理」に移動します。

3. Create > Userの順にクリックします。



4. SSOとして選択した認証サービスに関連する詳細を指定してユーザを設定し、Saveをクリックします。

SNA-UIでのSAMLユーザの作成

## トラブルシューティング

ユーザがSNA Managerにログインできない場合は、SAMLトレーサを使用してさらに調査できます。

SNAマネージャの調査に関してさらにサポートが必要な場合は、TACケースを挙げることができます。

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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。