Microsoft Entra ID SSO用のSNAマネージャの設定

内容

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

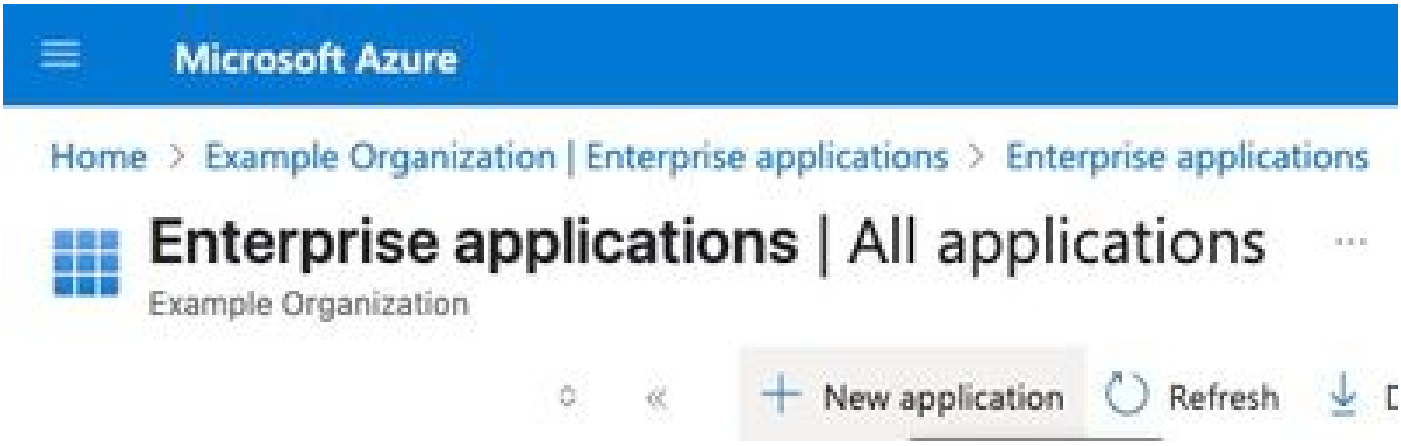
Azureでエンタープライズアプリケーションを構成

1. Azureクラウドポータルにログインします。

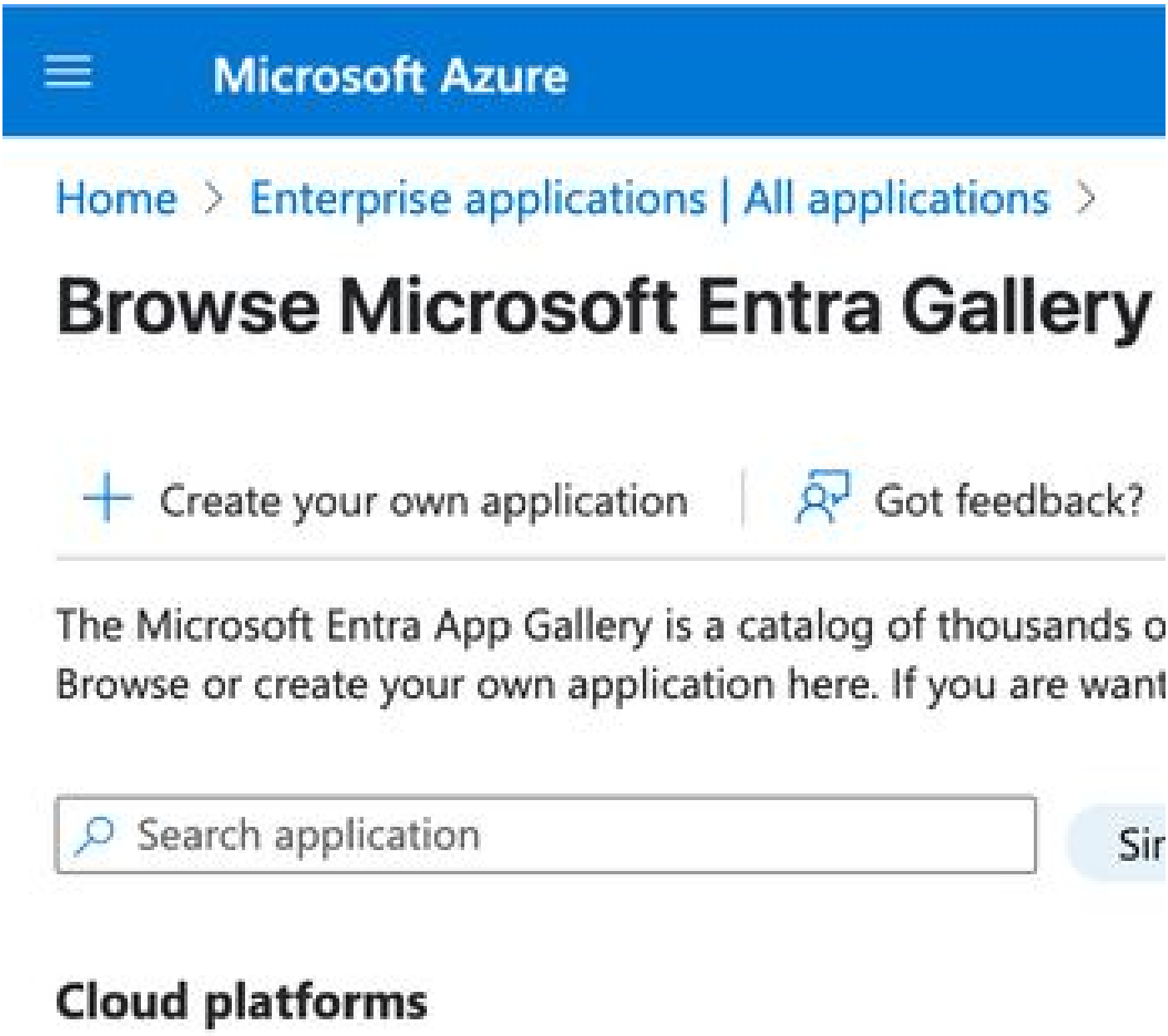
2. 検索ボックスでEntra IDサービスを検索し、Microsoft Entra IDを選択します。

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。



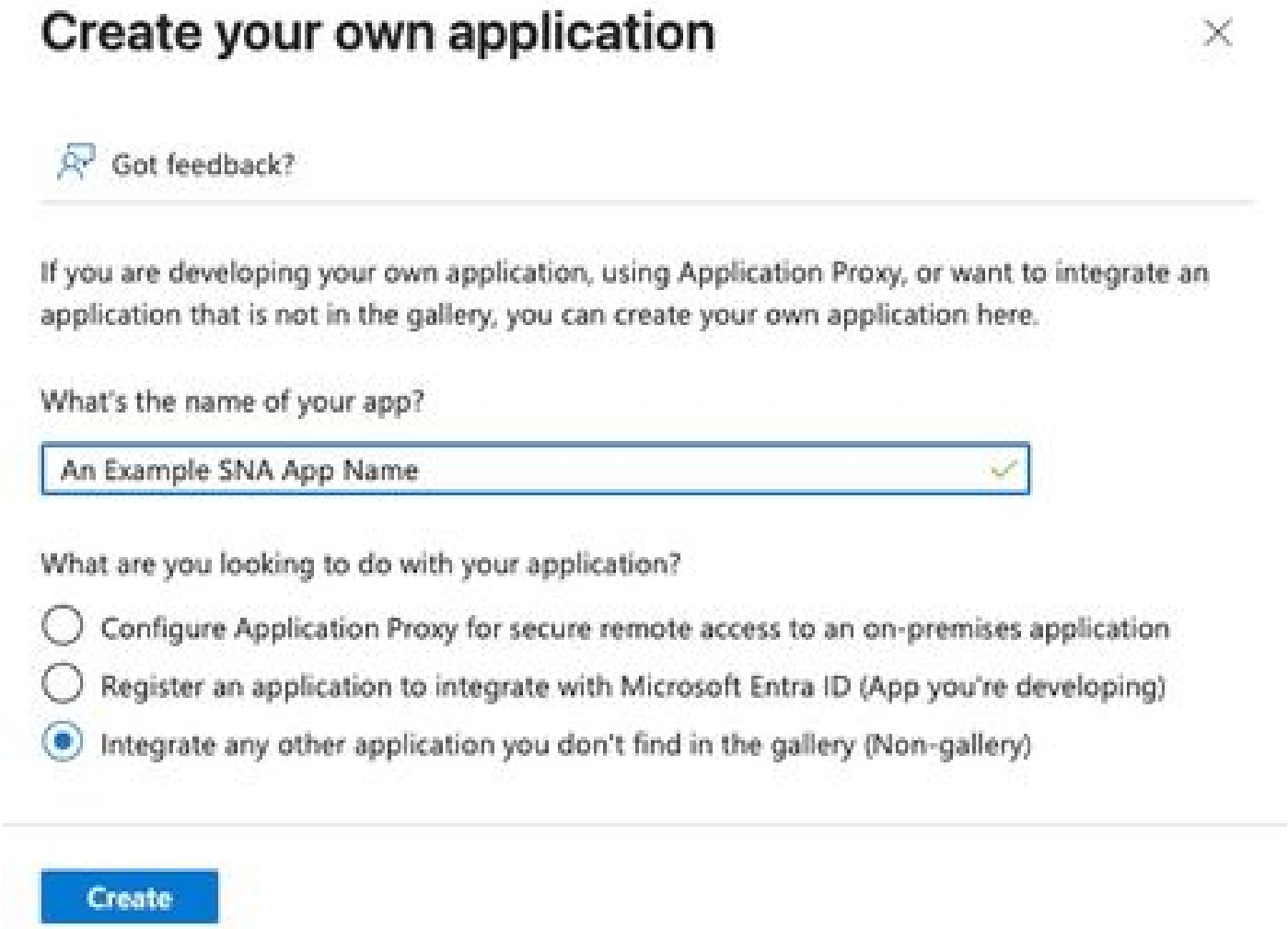
5. ロードする新規ページで、「独自のアプリケーションの作成」を選択します。



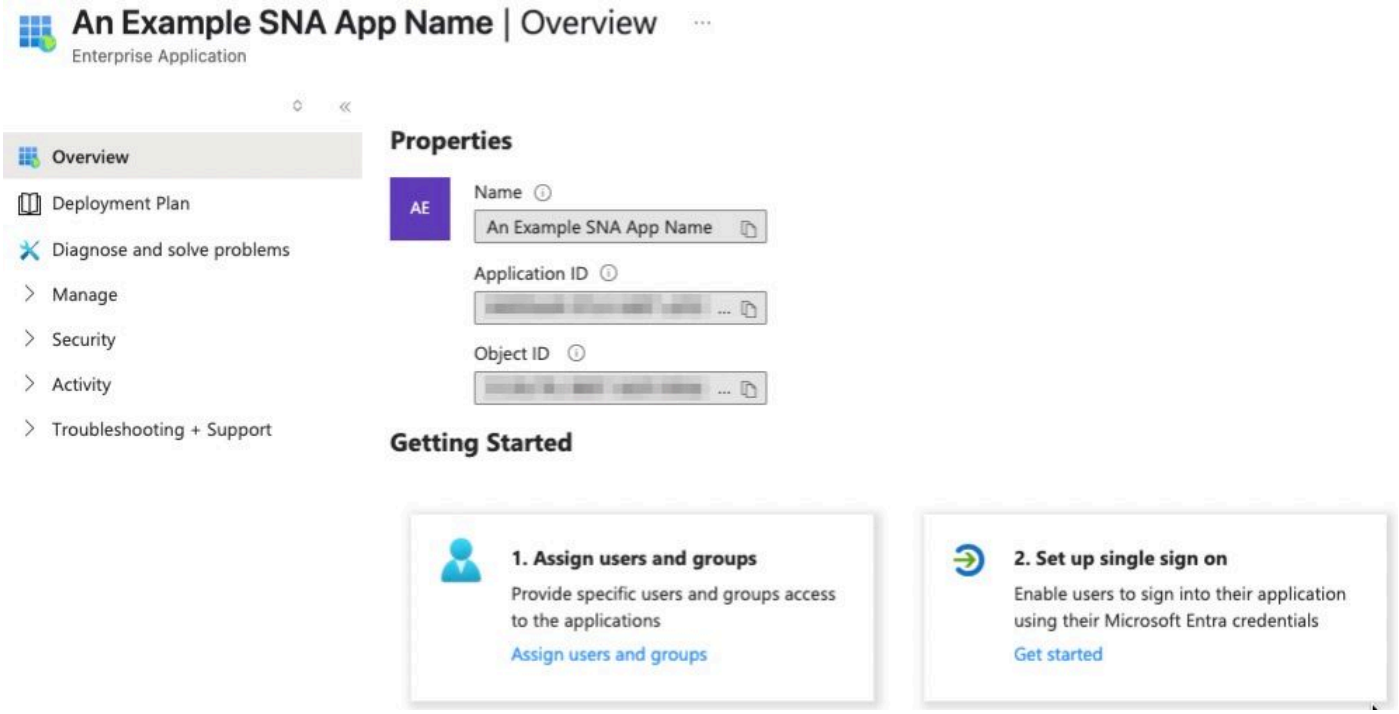
Azure-UI

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。

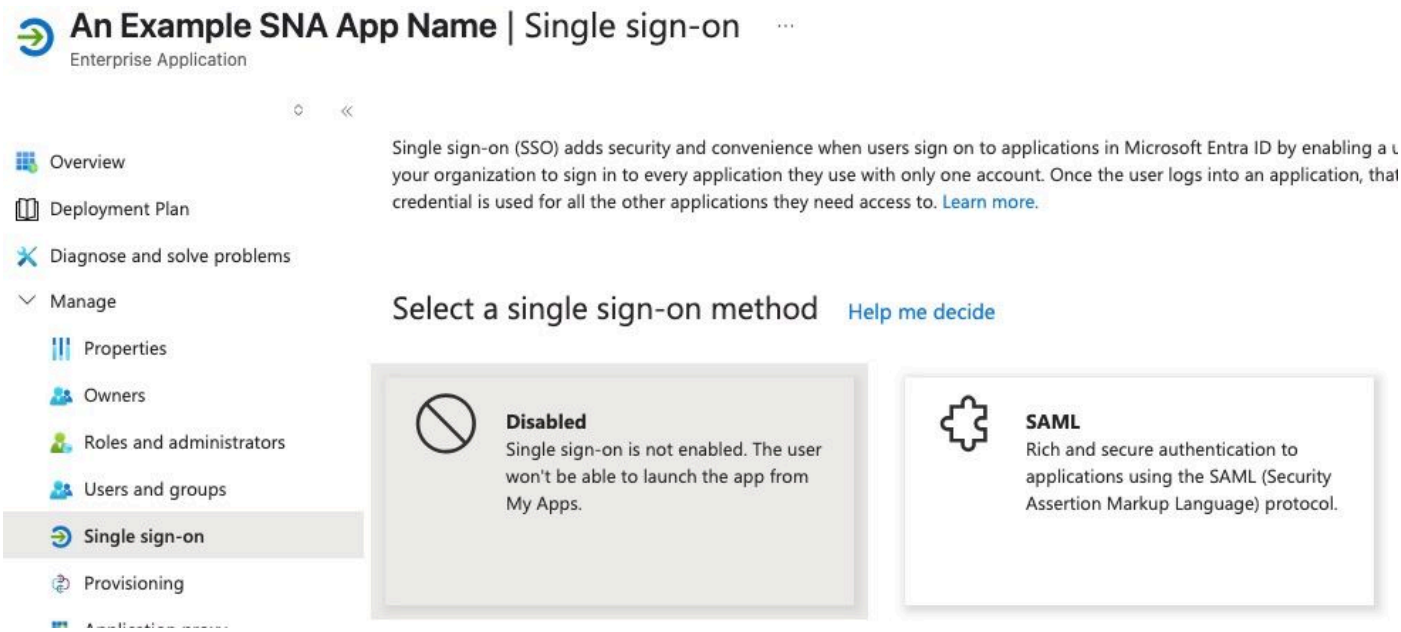
7. 「Integrate any other application you don't find in the gallery (Non-gallery)」ラジオ・ボタンを選択し、「Create」をクリックします。



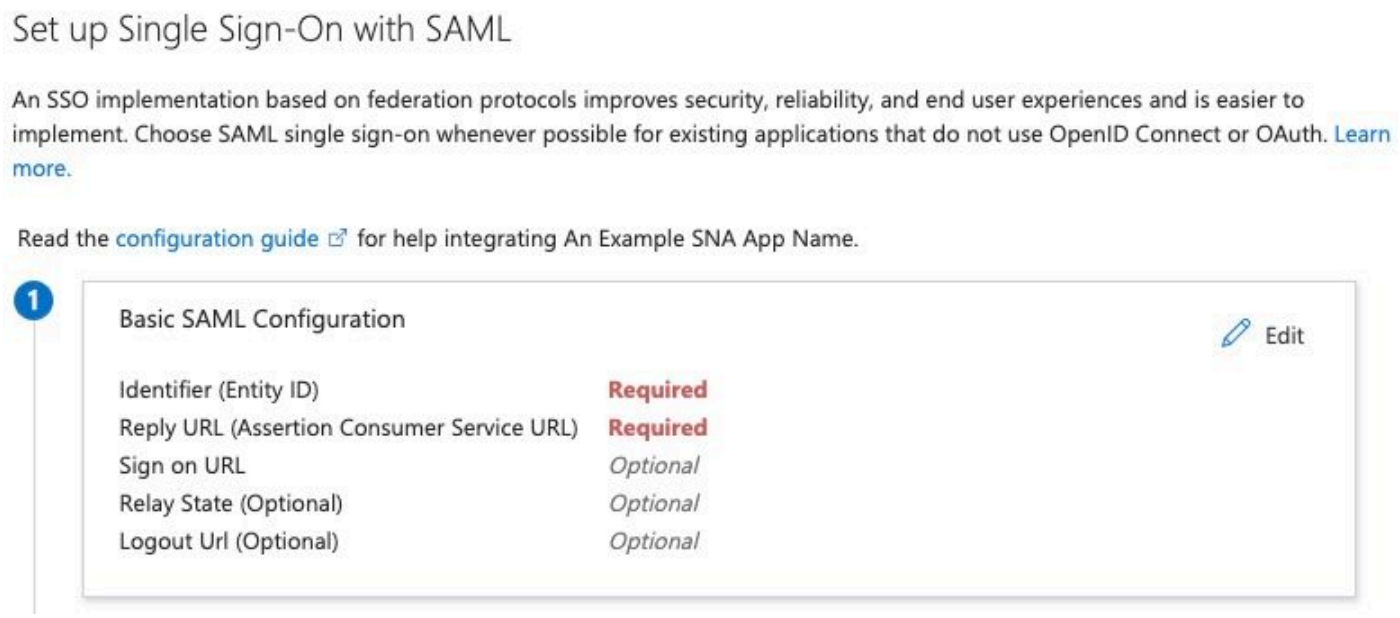
8. 新しく構成されたアプリケーションダッシュボードで、[シングルサインオンのセットアップ]をクリックします。



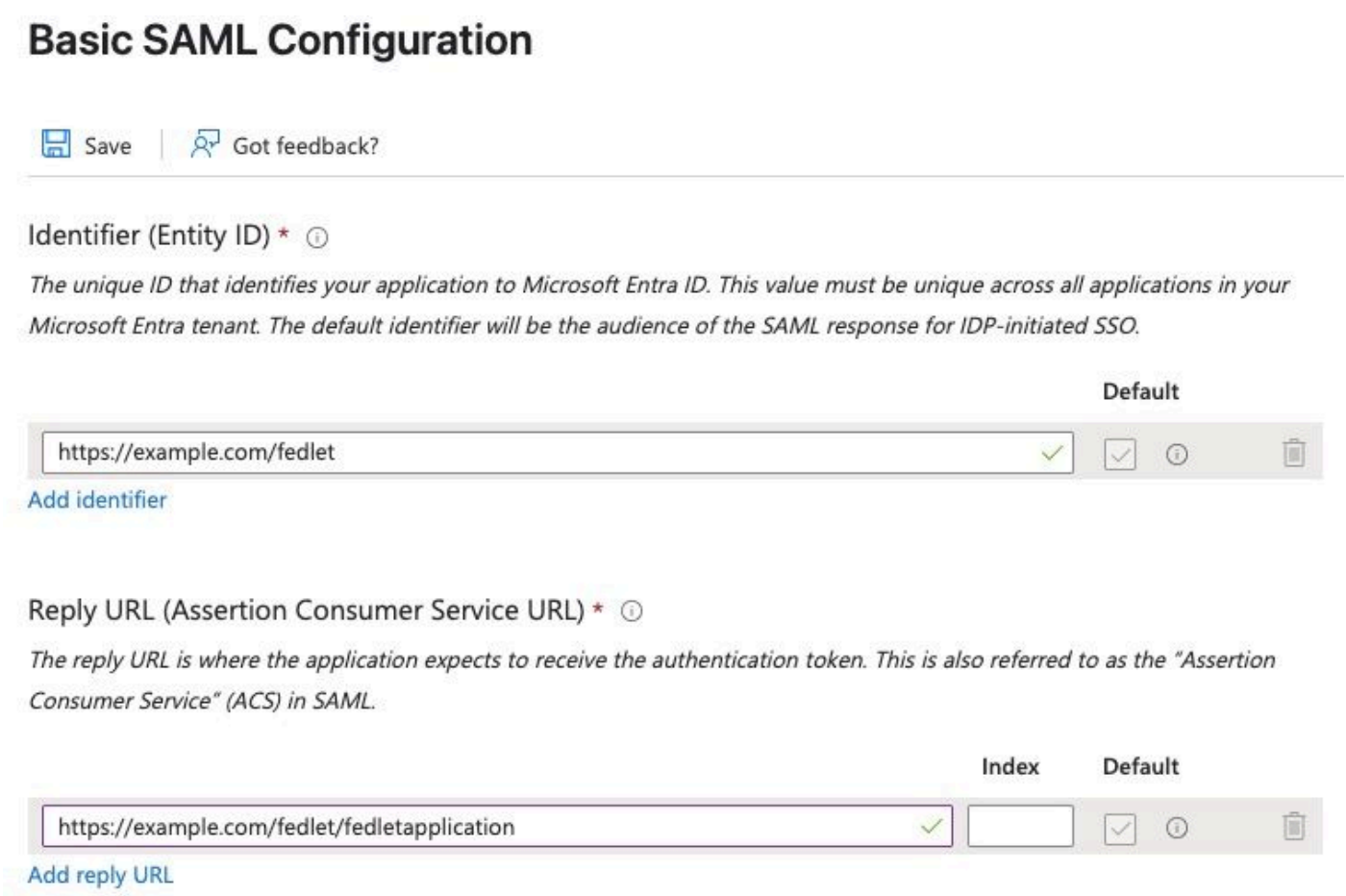
9. SAMLを選択します。



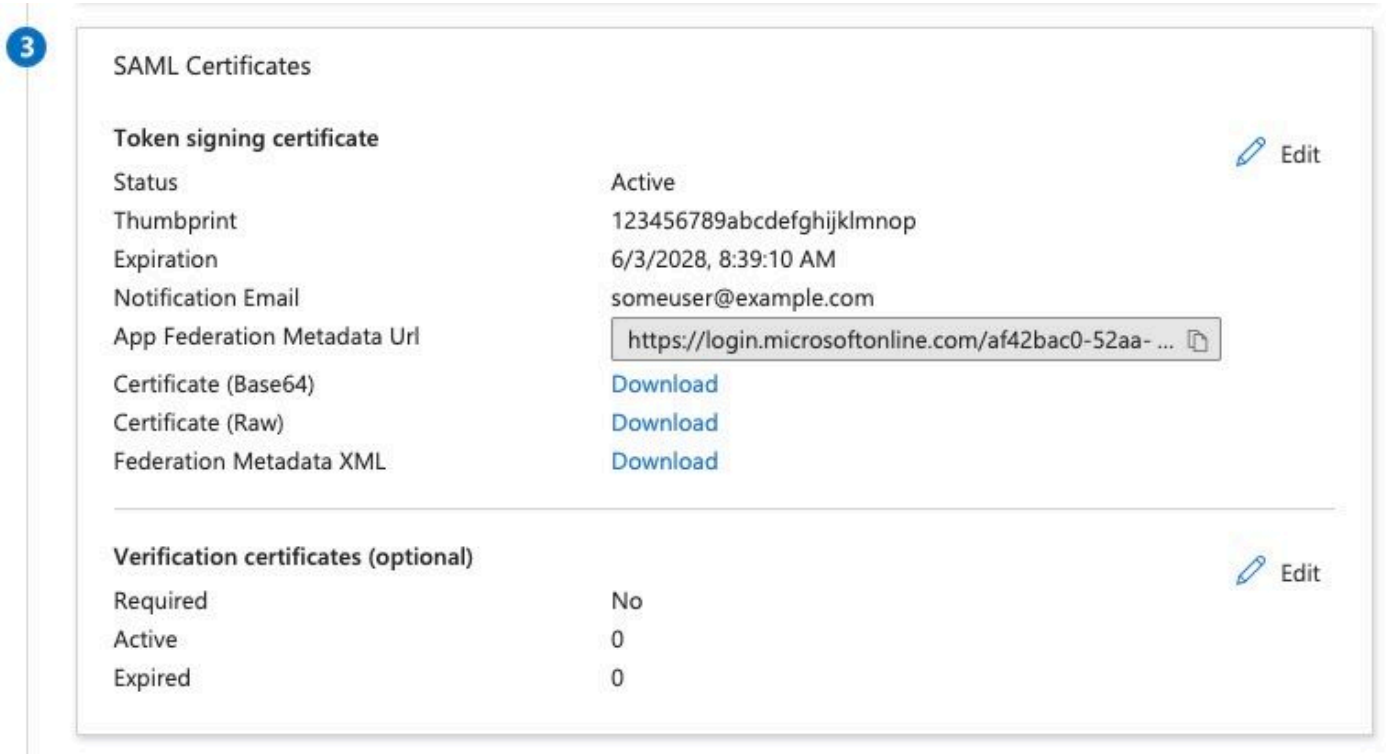
10. SAMLによるシングルサインオンの設定ページで、基本SAML設定の下の編集をクリックします。



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

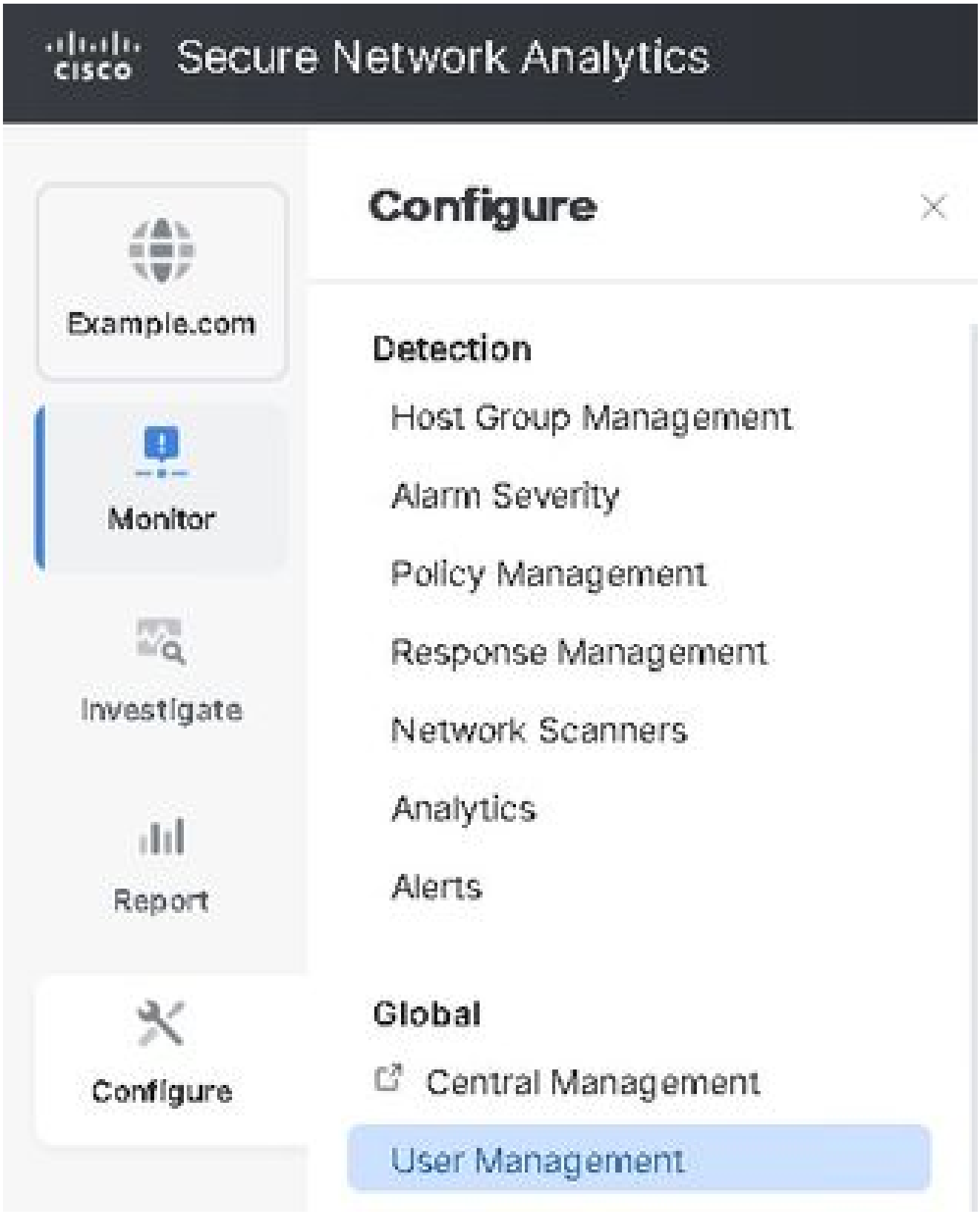


12. SAML Certificatesカードを見つけ、App Federation Metadata URLフィールド値を保存し、Federation Metadata XMLをダウンロードします。

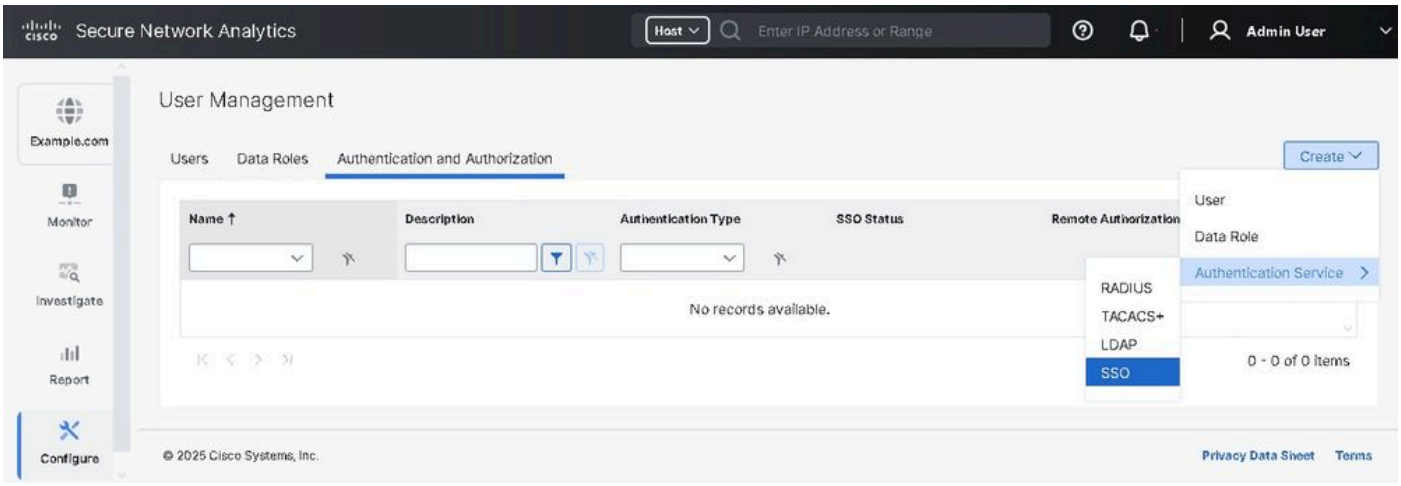


SNAでのサービスプロバイダーXMLファイルの設定およびダウンロード

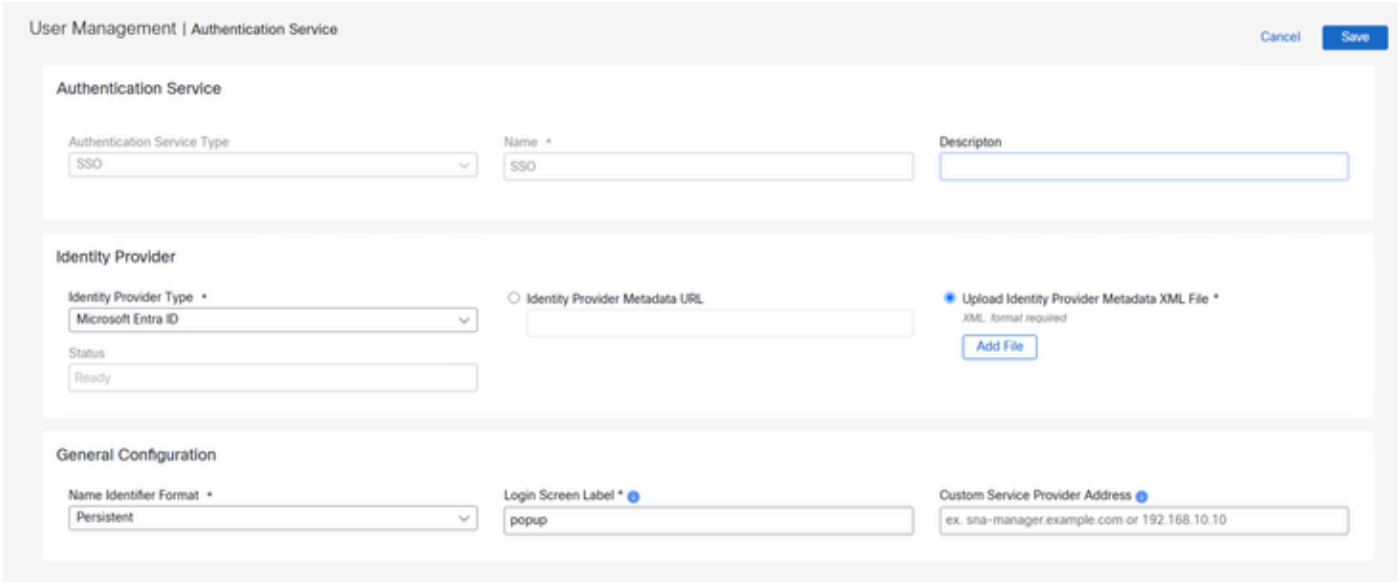
1. SNAマネージャUIにログインします。
2. Configure > Global > User Managementの順に選択します。

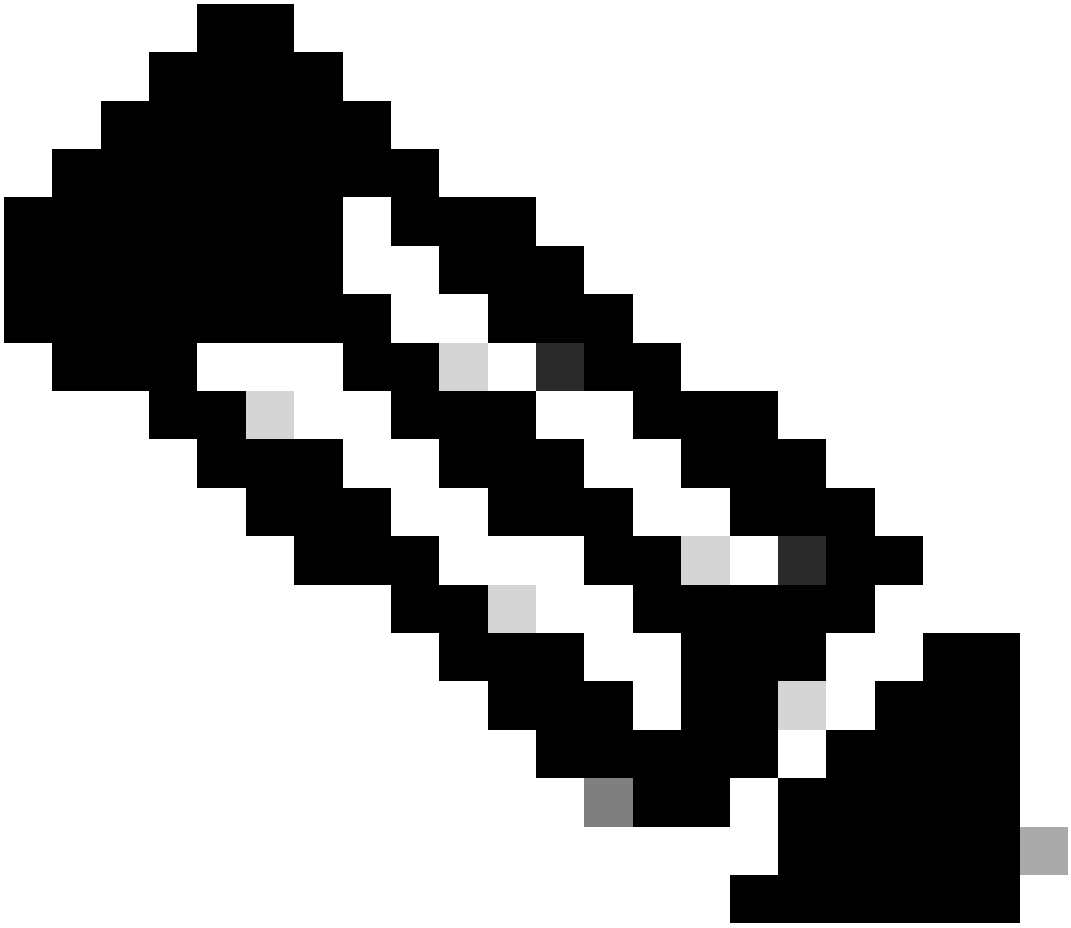


3. Authentication and Authorizationタブで、Create > Authentication Service > SSOの順にクリックします。



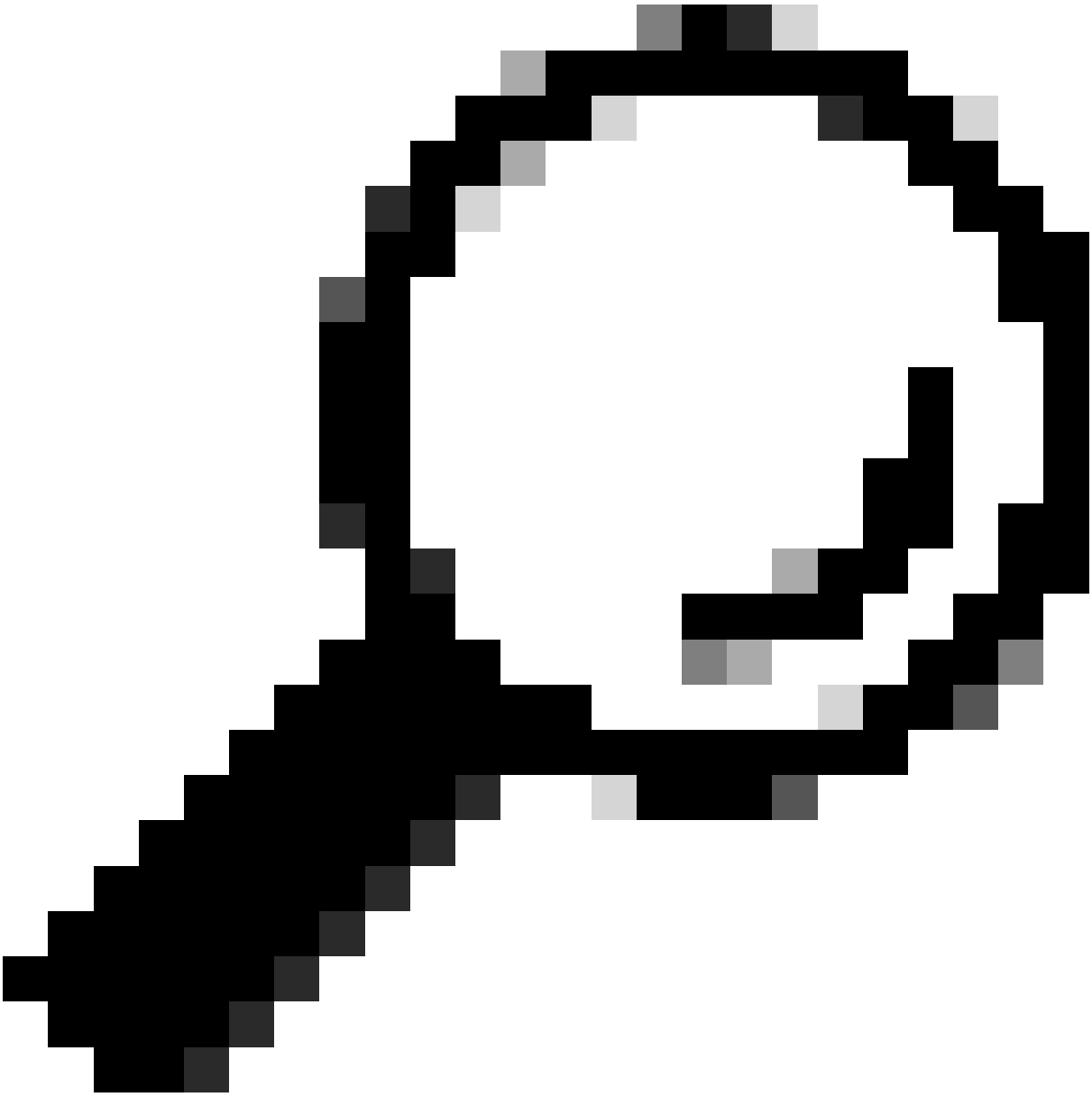
4. 「IDプロバイダのメタデータURL」または「IDプロバイダのメタデータXMLファイルのアップロード」に適切なラジオ・ボタンを選択します。





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。

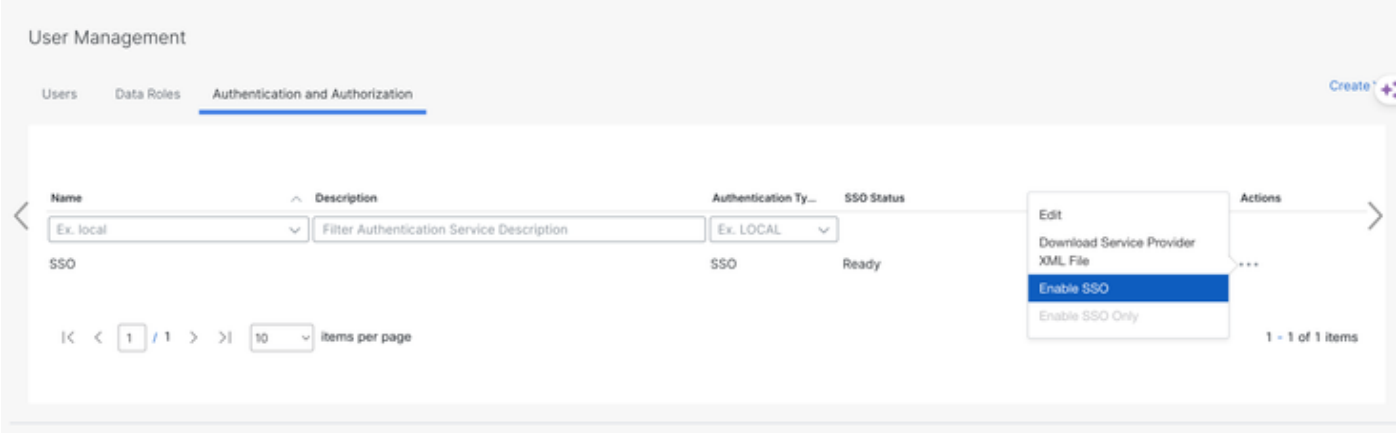
5. IDプロバイダータイプフィールドをMicrosoft Entra IDに、名前識別子フォーマットをPersistentに設定し、ログイン画面ラベルを入力します。



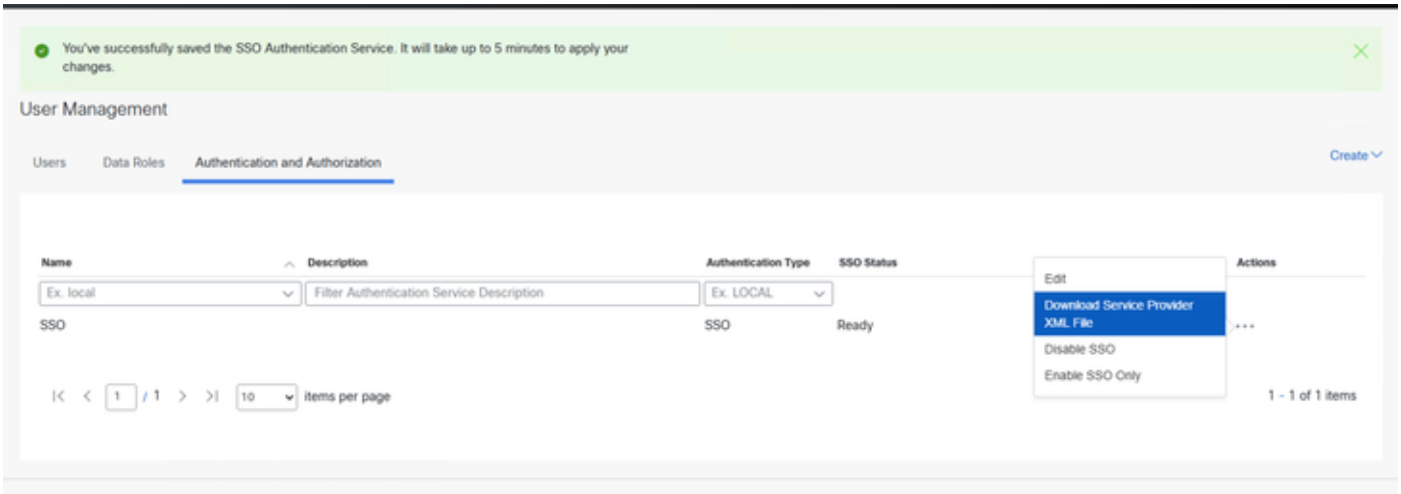
ヒント：設定済みのログイン画面ラベル（名前/テキスト）がSSOでのログインボタンの上に表示されます。このラベルを空のままにしないでください。

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。



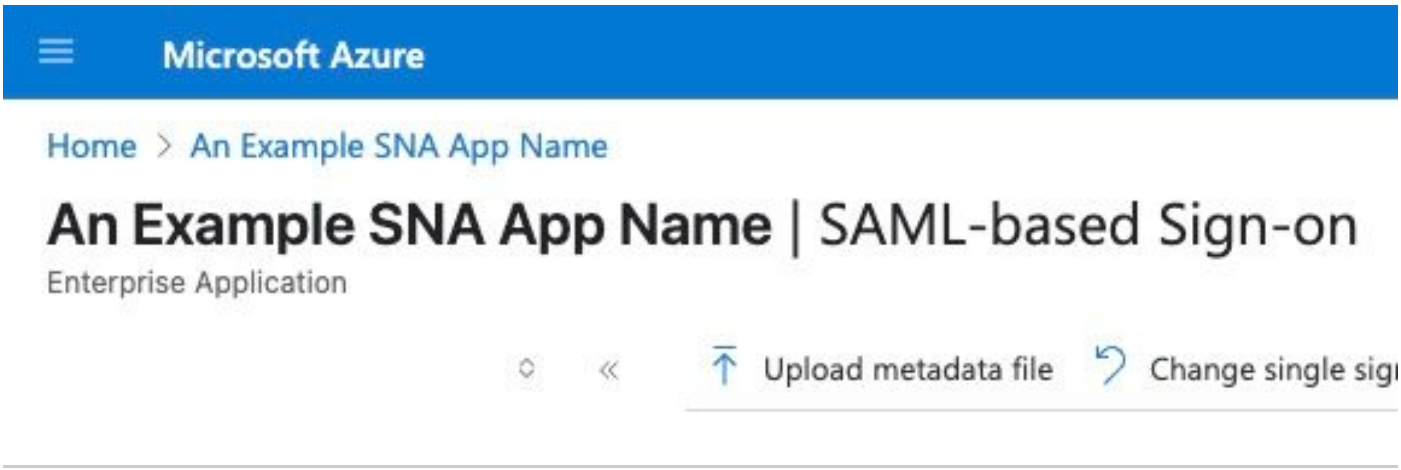
AzureでSSOを構成する

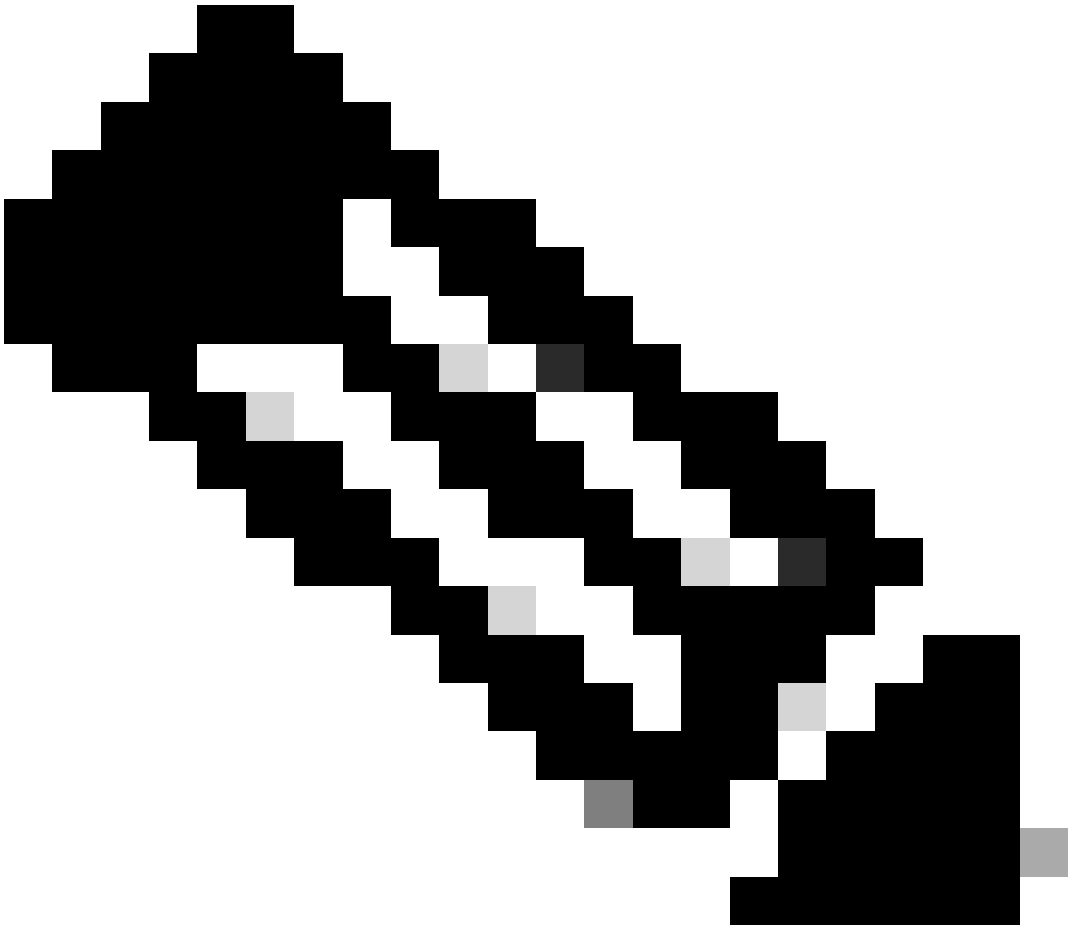
1. Azureポータルにログインします。

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。

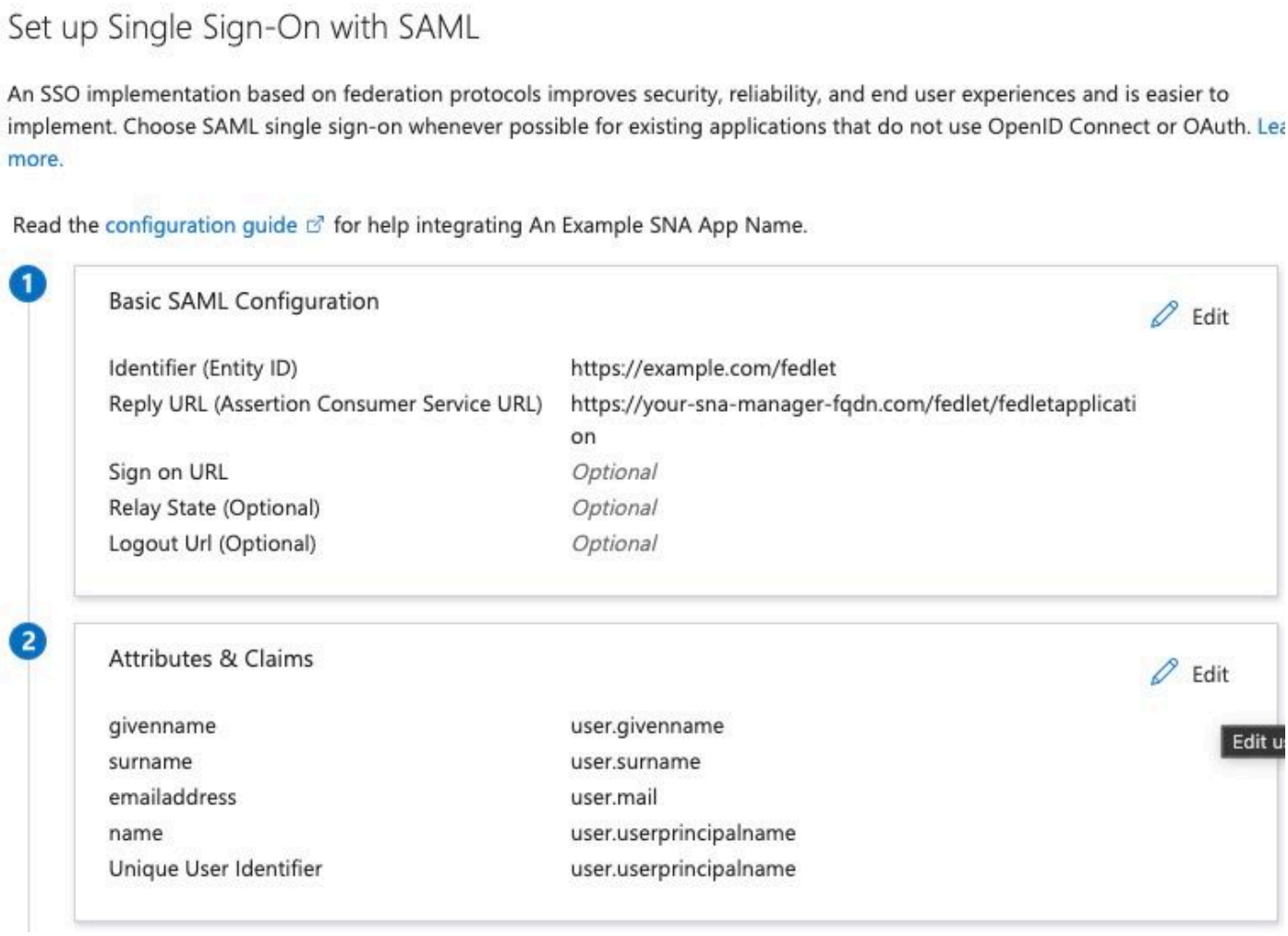
4. 「基本的なSAML構成」画面が開き、さまざまな設定を正しい値に設定し、 「保存」をクリックします。





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。



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

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

Microsoft Azure

Search

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

Manage claim ...

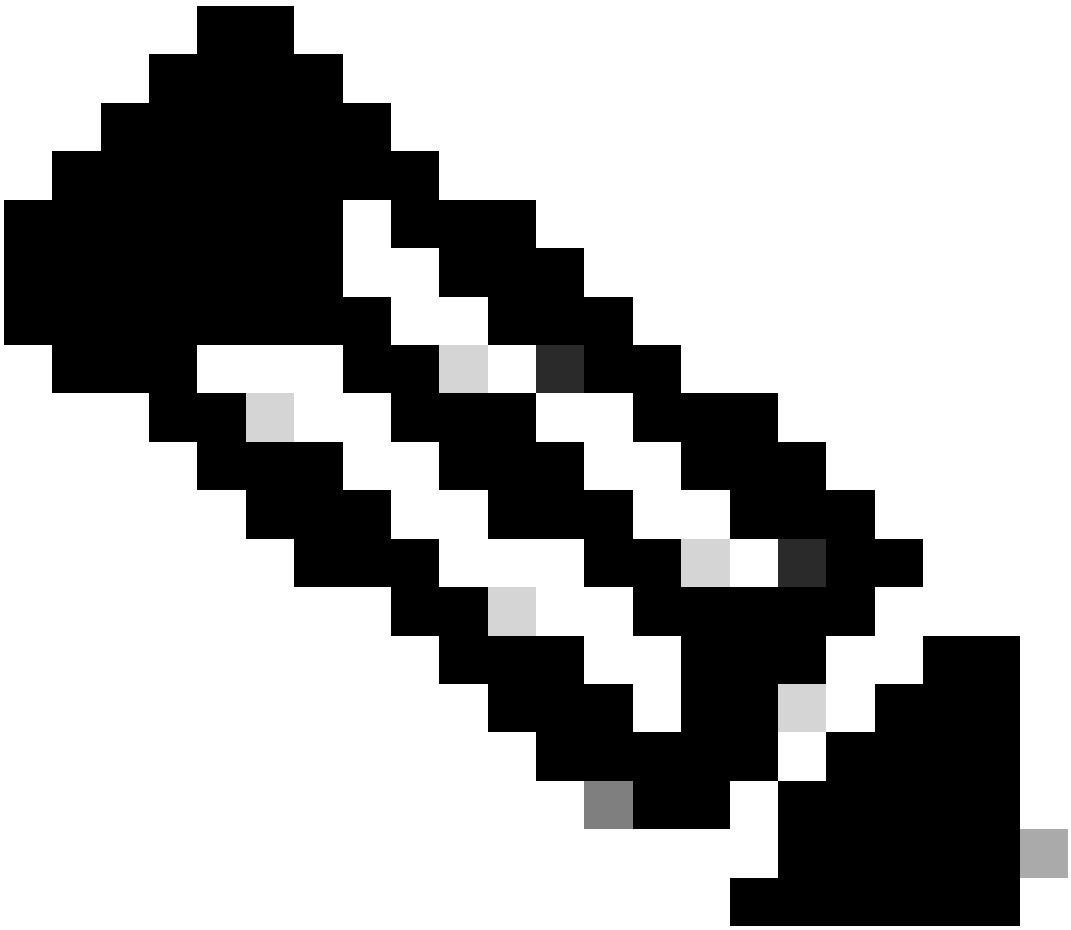
Save | Discard changes | Got feedback?

Name: nameidentifier

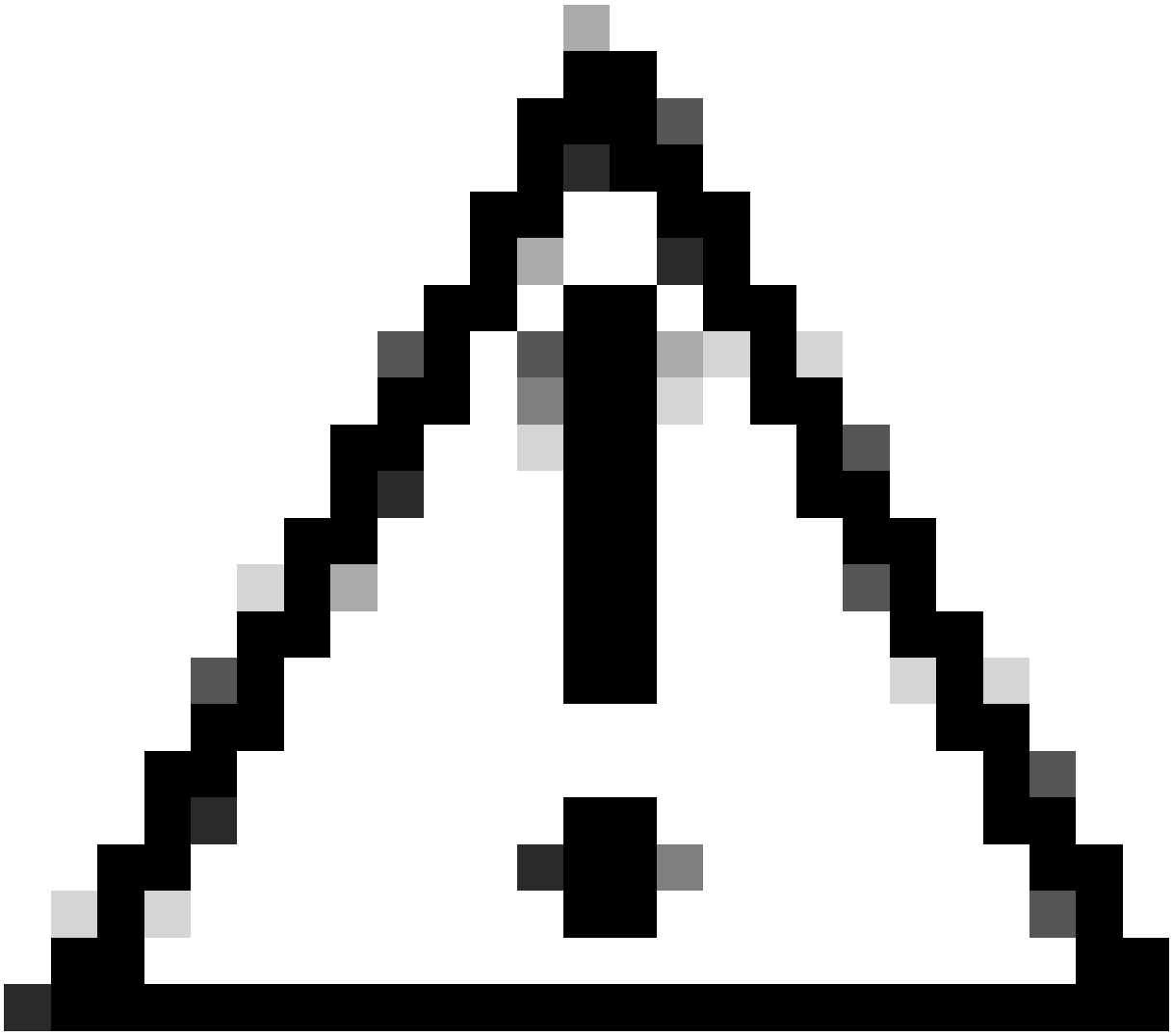
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Persistent



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。

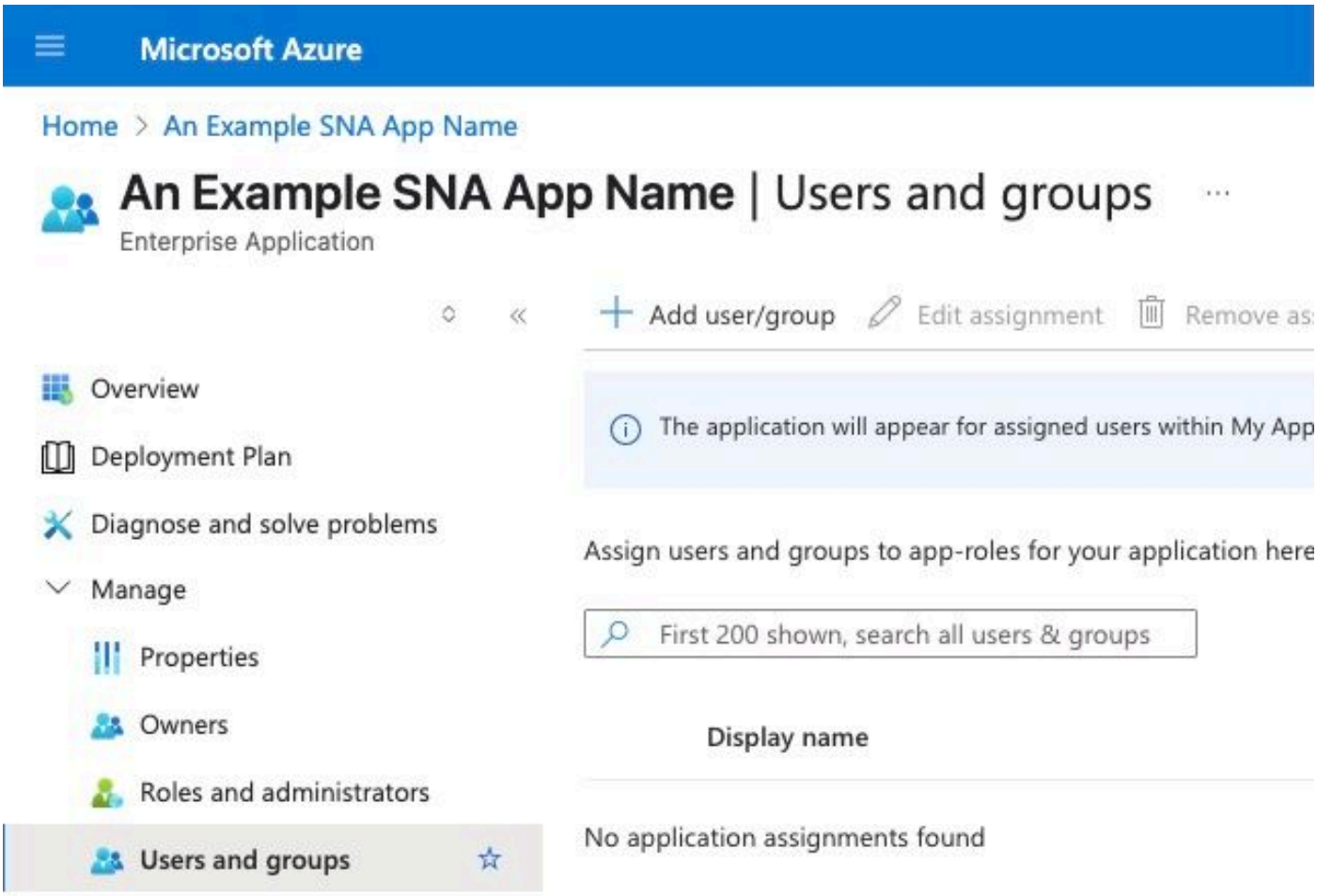


注意：問題が発生する最も一般的な場所です。SNAマネージャとMicrosoft Azureの設定が一致する必要があります。SNAでemailAddress形式を使用することを選択した場合は、この形式もEmail Addressである必要があります。

Enter IDでユーザを設定します。

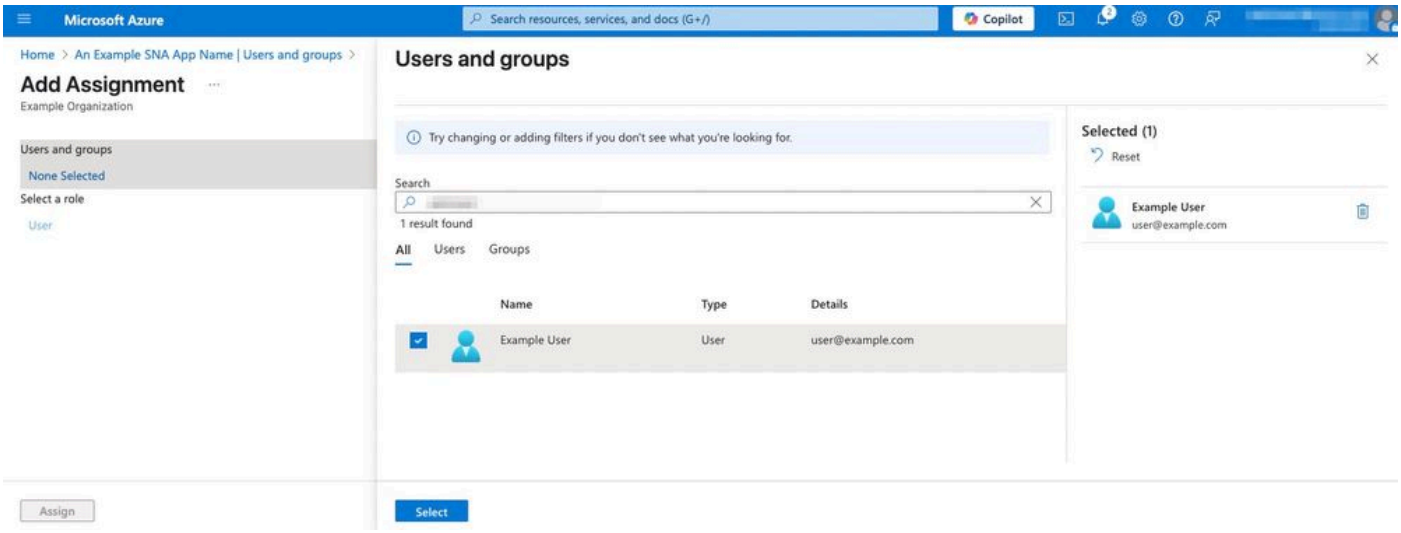
1. Azureポータルにログインします。

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。

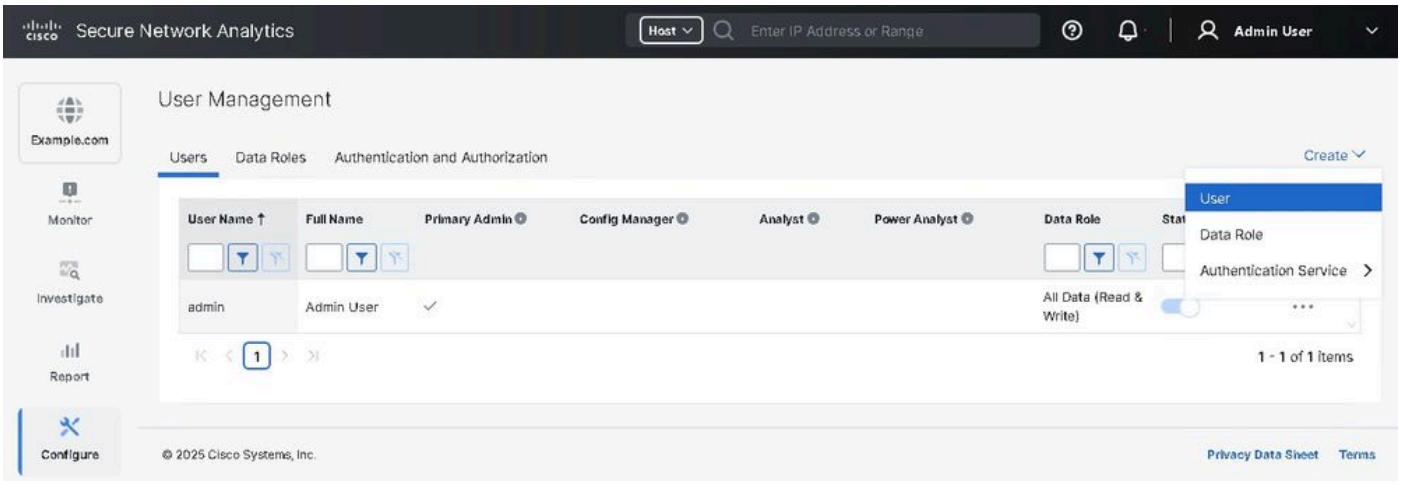


SNAでのSSOの設定

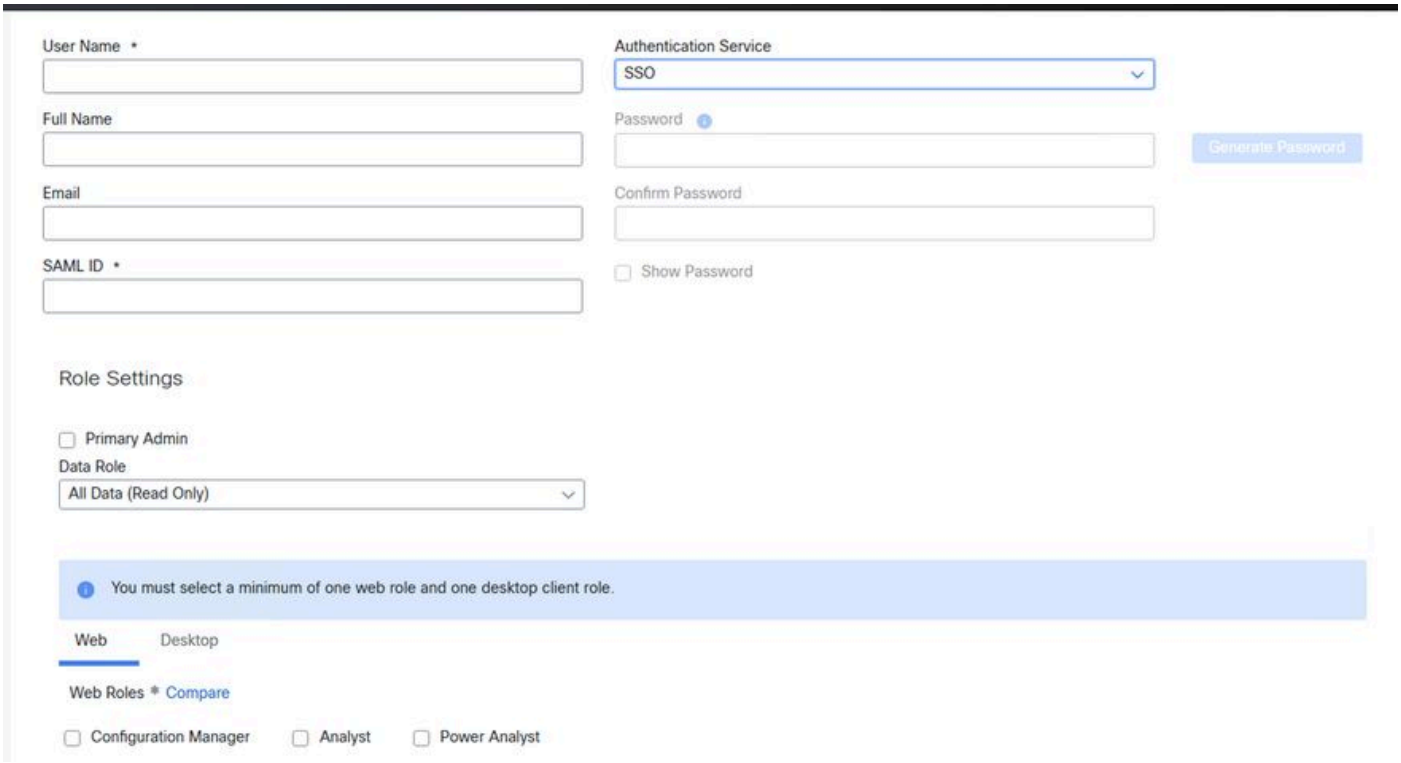
1. SNAマネージャUIにログインします。

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

トラブルシュート

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。