Configurer SNA Manager pour Microsoft Entra ID SSO

Table des matières

Introduction

Ce document décrit comment configurer Secure Network Analytics (SNA) pour utiliser Microsoft Entra ID for Single Sign On (SSO).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Microsoft Azure
- Analyses réseau sécurisées

Composants utilisés

- SNA Manager v7.5.2
- ID d'entrée Microsoft

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration Steps

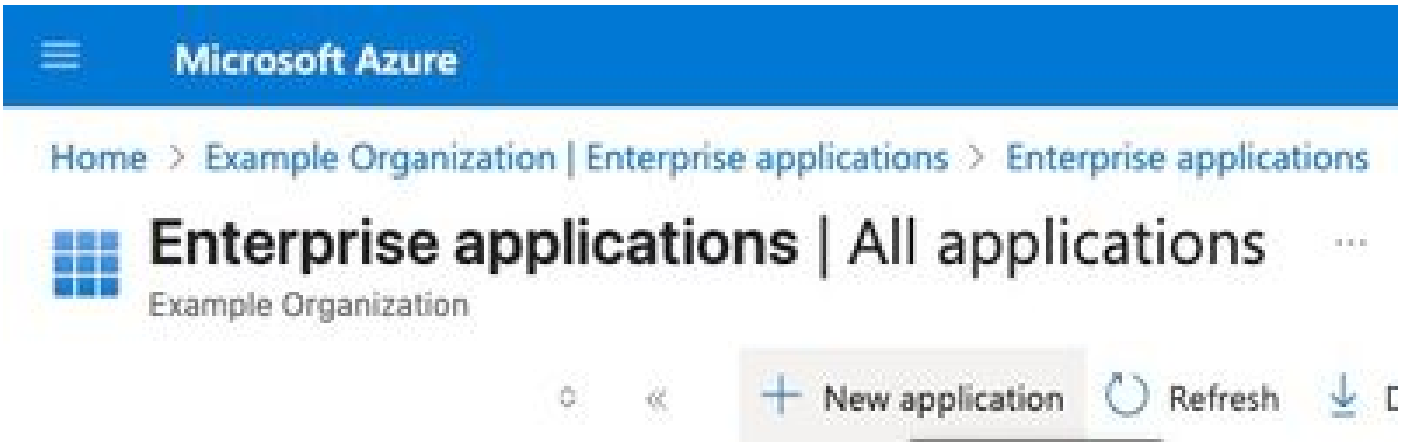
Configurer l'application d'entreprise dans Azure

1. Connectez-vous au portail cloud Azure.

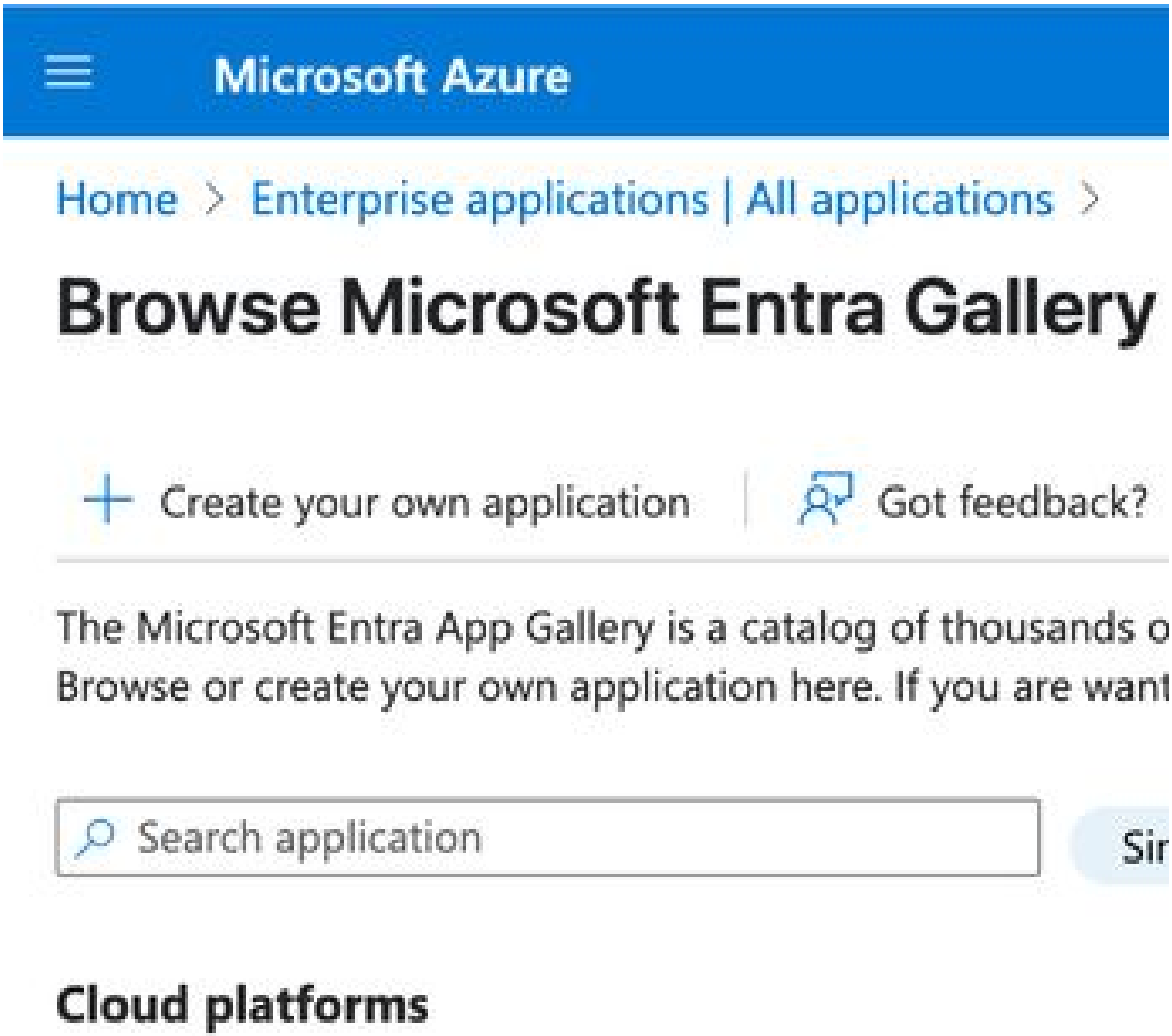
2. Recherchez le service Entra ID dans la zone de recherche et sélectionnez Microsoft Entra ID.

3. Dans le volet de gauche, développez Gérer et sélectionnez Applications d'entreprise.

4. Cliquez sur Nouvelle application.



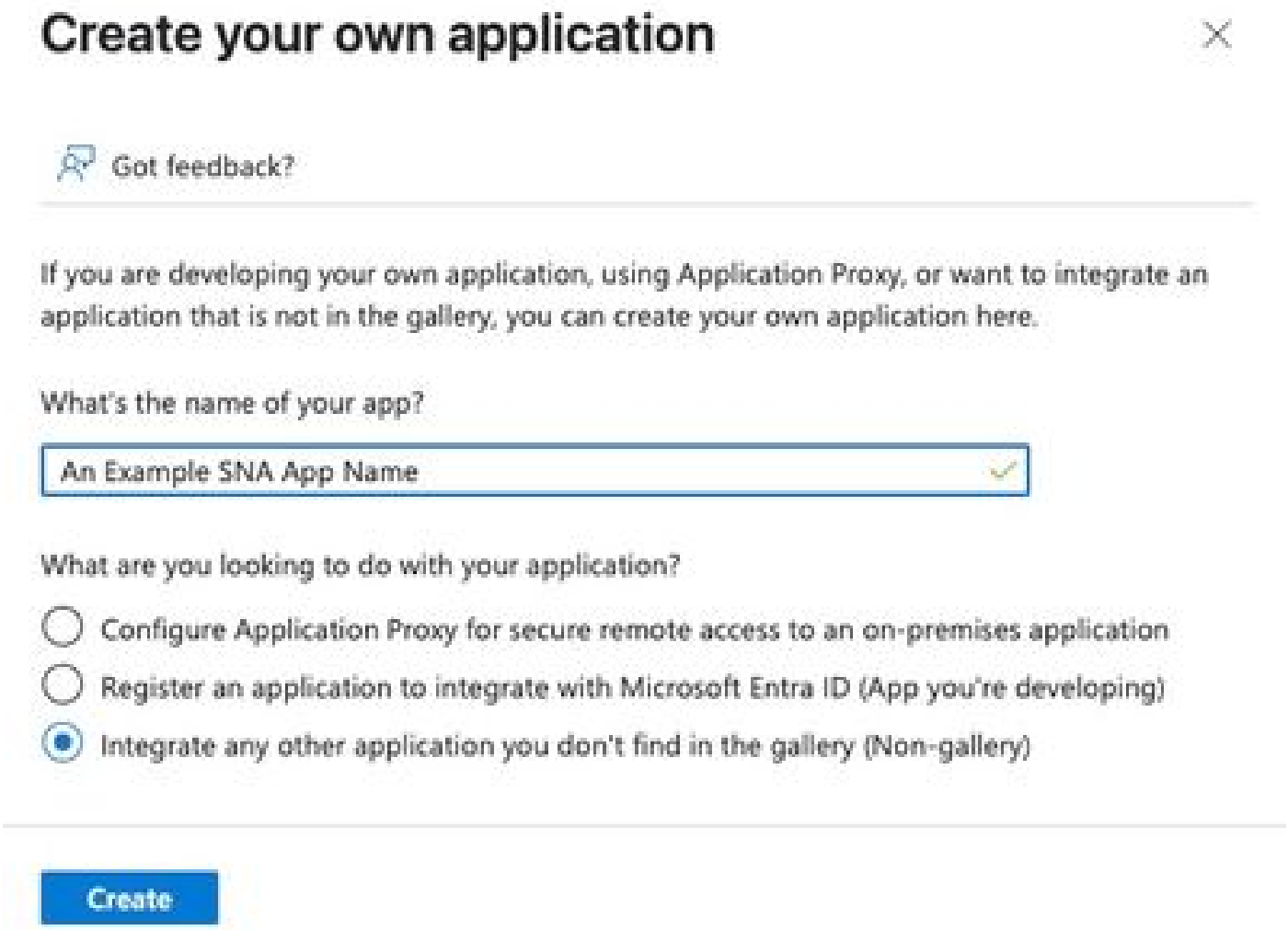
5. Sélectionnez Créer votre propre application sur la nouvelle page qui se charge.



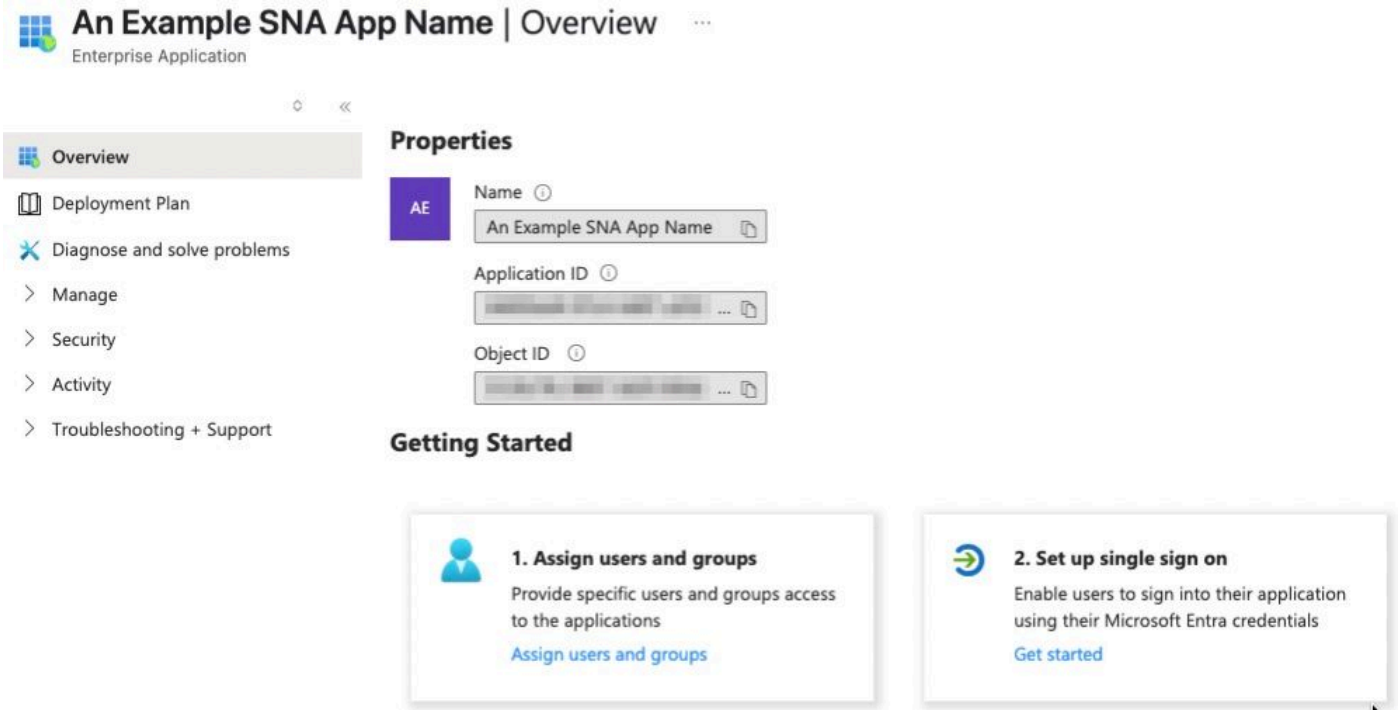
Azure-UI

6. Entrez un nom pour l'application dans Quel est le nom de votre application ? champ.

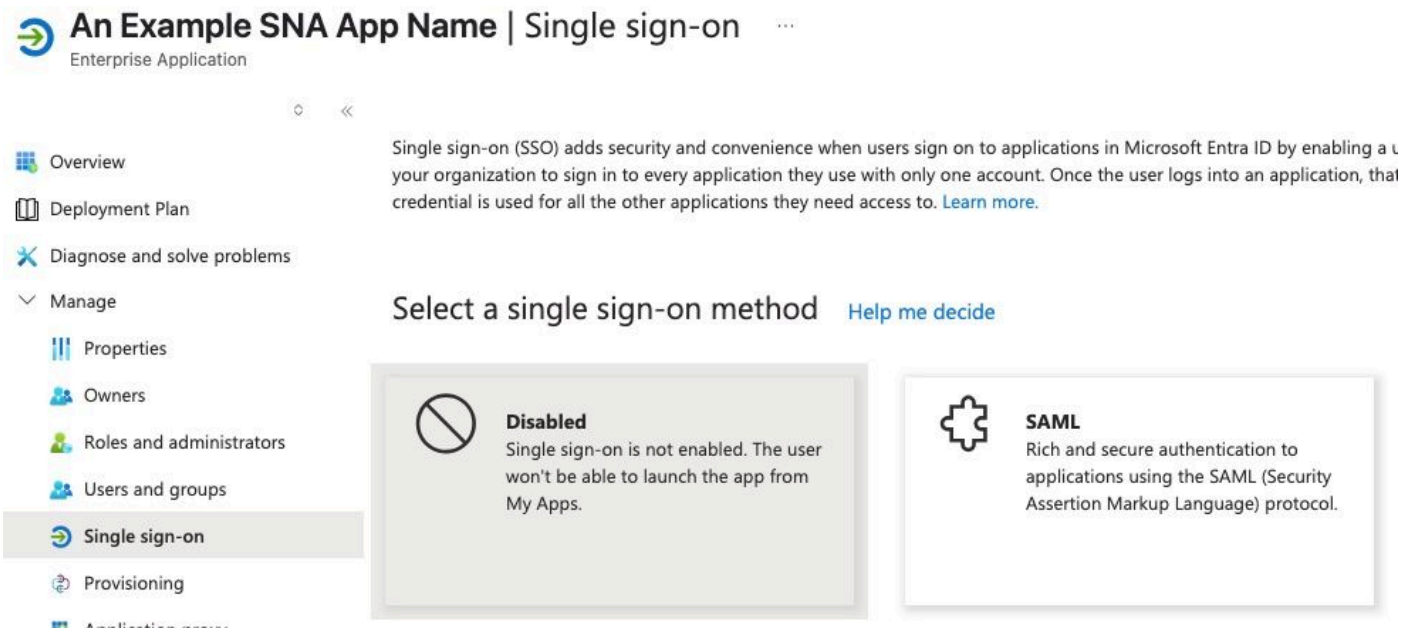
7. Sélectionnez la case d'option Intégrer toute autre application que vous ne trouvez pas dans la galerie (hors galerie) et cliquez sur Créer.



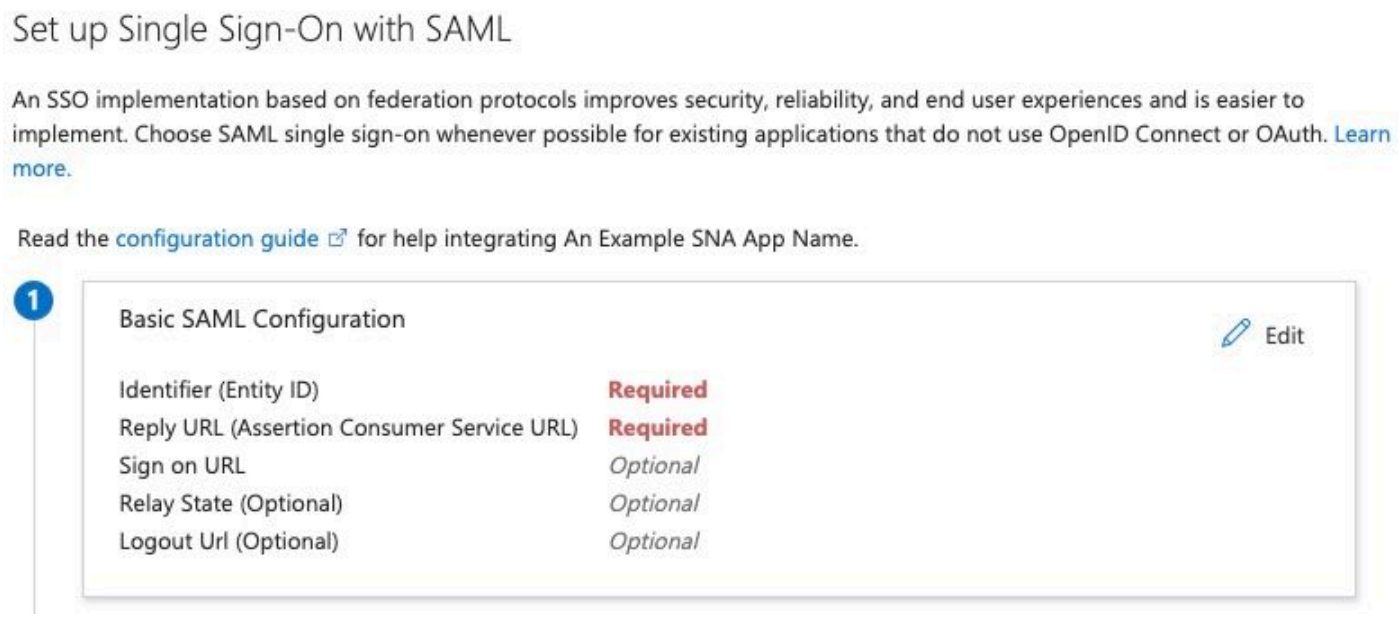
8. Sur le tableau de bord de l'application nouvellement configuré, cliquez sur Configurer l'authentification unique.



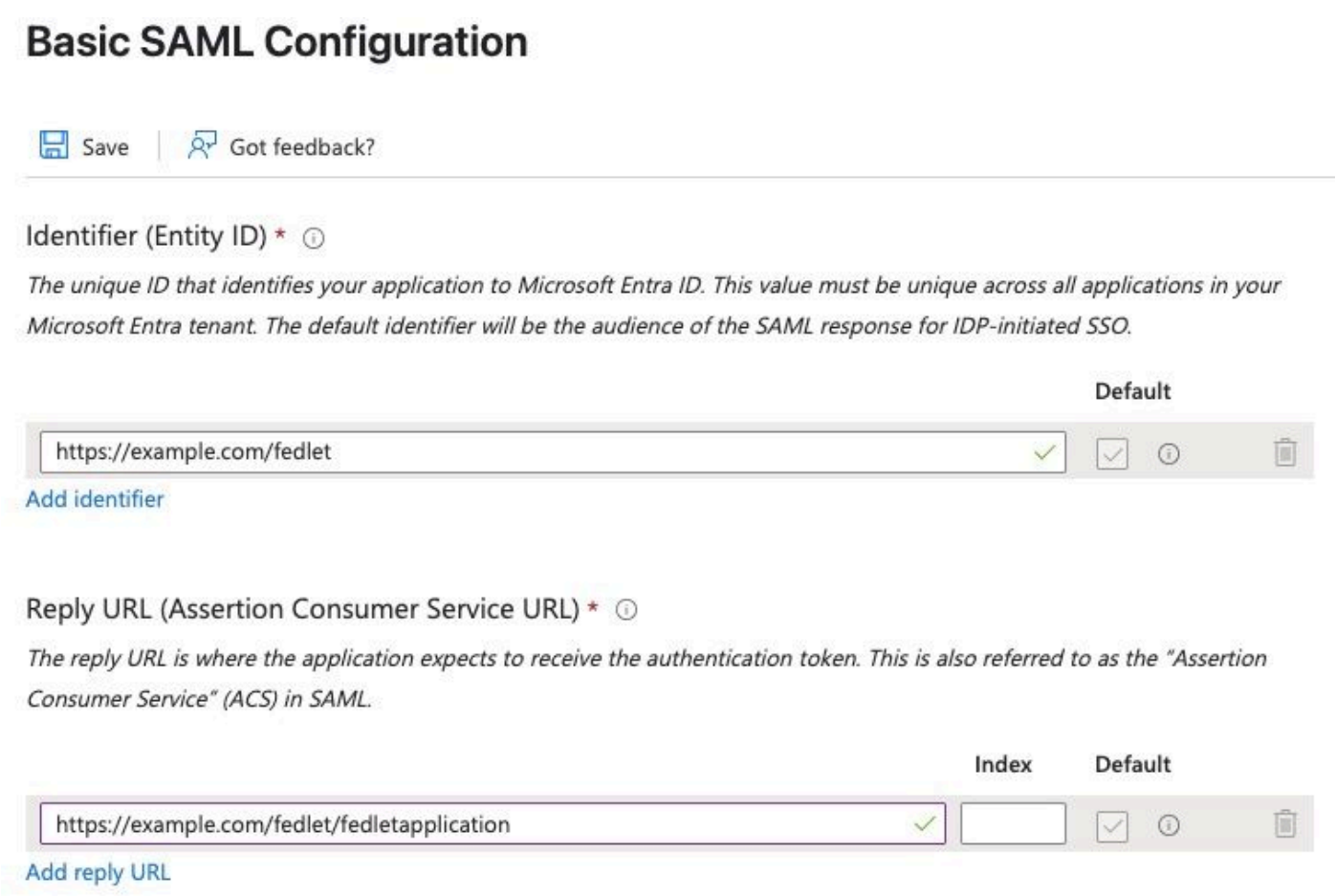
9. Sélectionnez SAML.



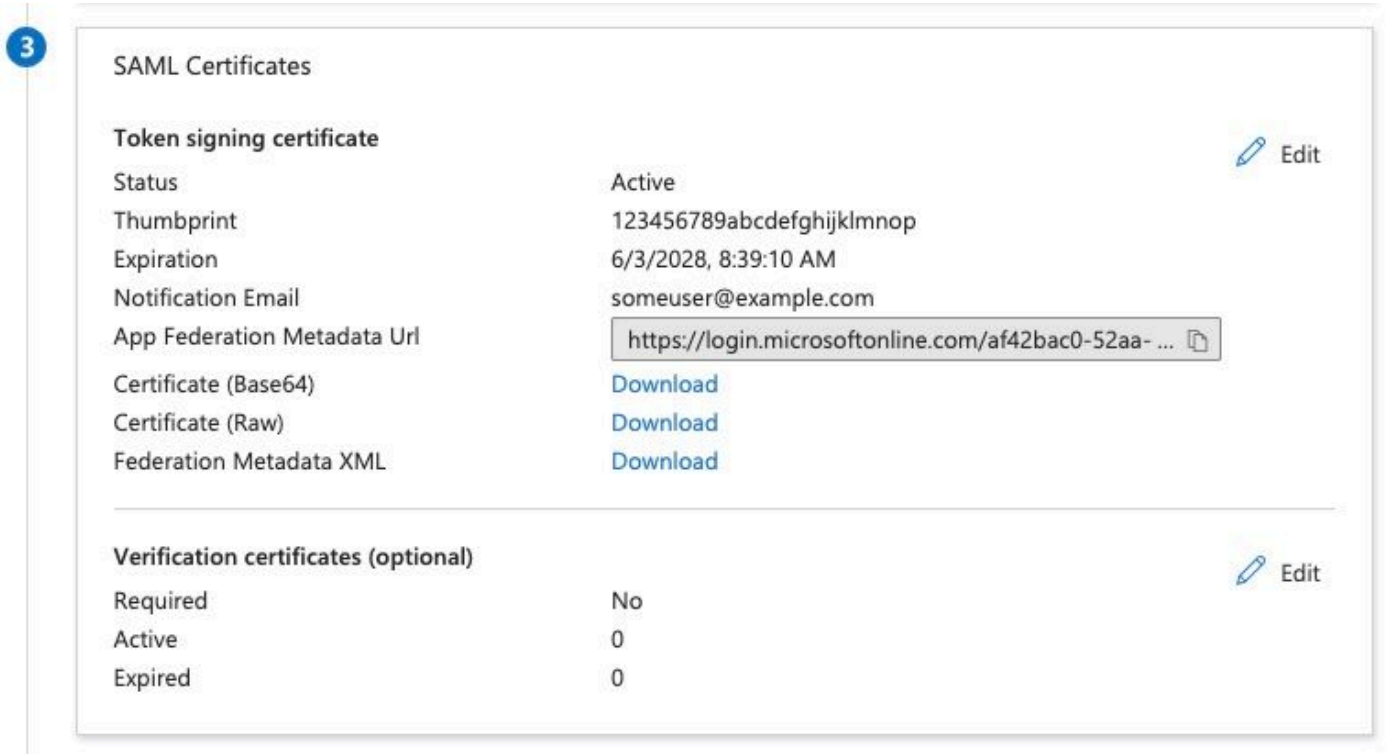
10. Sur la page Configurer l'authentification unique avec SAML, cliquez sur Modifier sous Configuration SAML de base.



11. Dans le volet Configuration SAML de base, configurez Add Reply URL to https://example.com/fedlet/fedletapplication en remplaçant example.com par FQDN de SNA Manager et cliquez sur save.



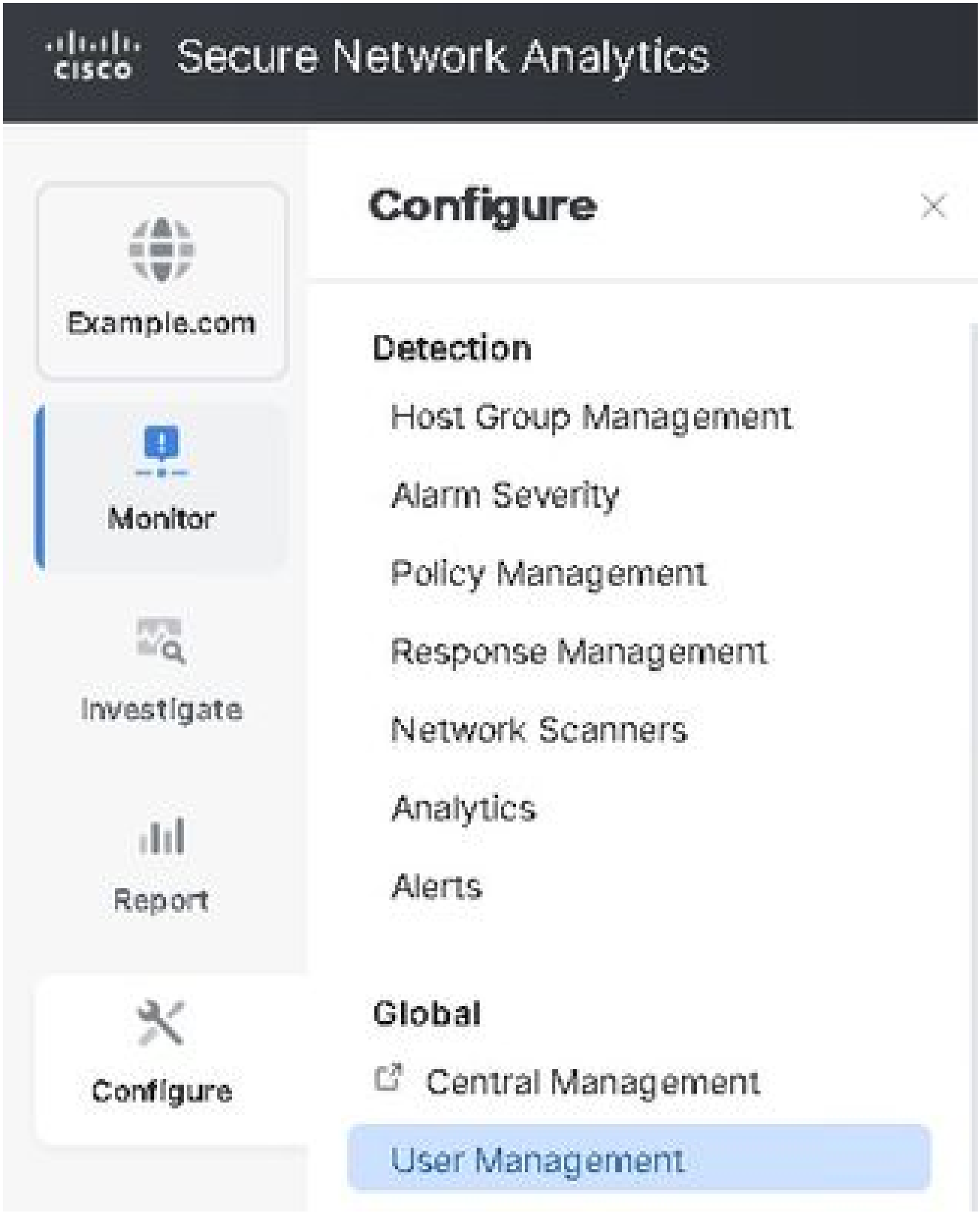
12. Localisez la carte Certificats SAML et enregistrez la valeur du champ URL des métadonnées de fédération d'application et téléchargez le fichier XML des métadonnées de fédération.



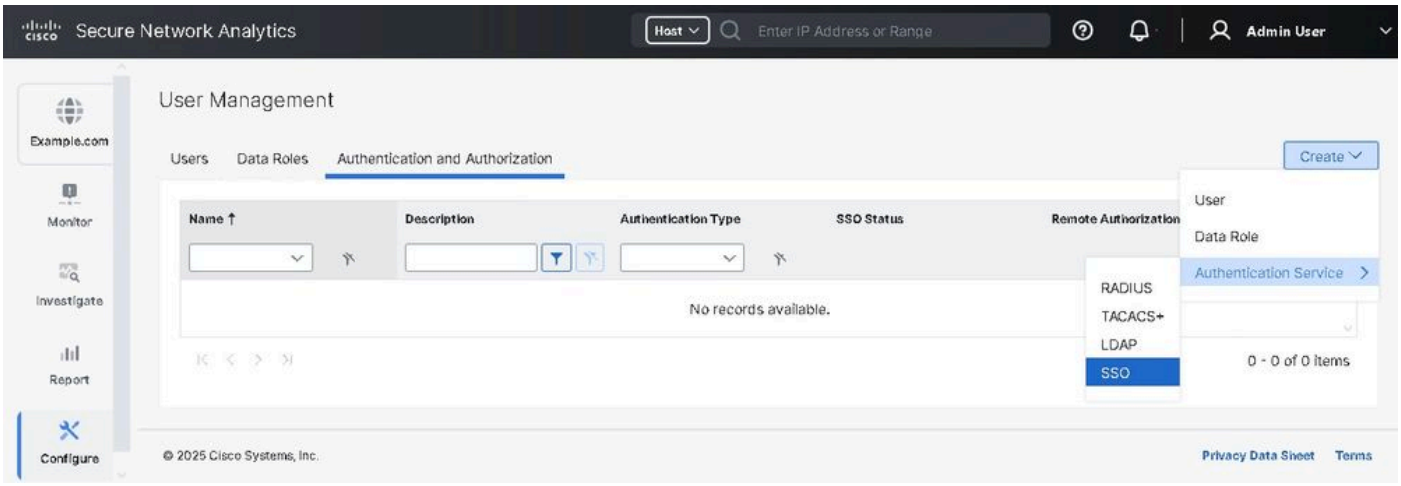
Configuration et téléchargement du fichier XML du fournisseur de services dans

SNA

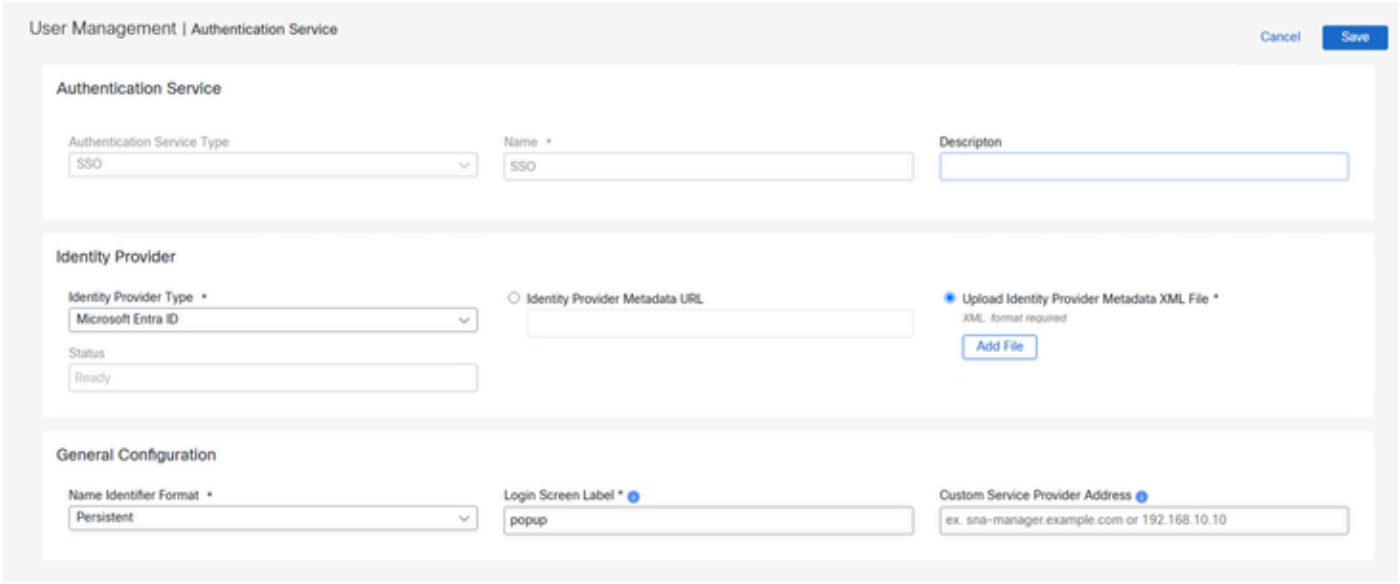
1. Connectez-vous à l'interface utilisateur SNA Manager.
2. Naviguez jusqu'à Configure > Global > User Management.

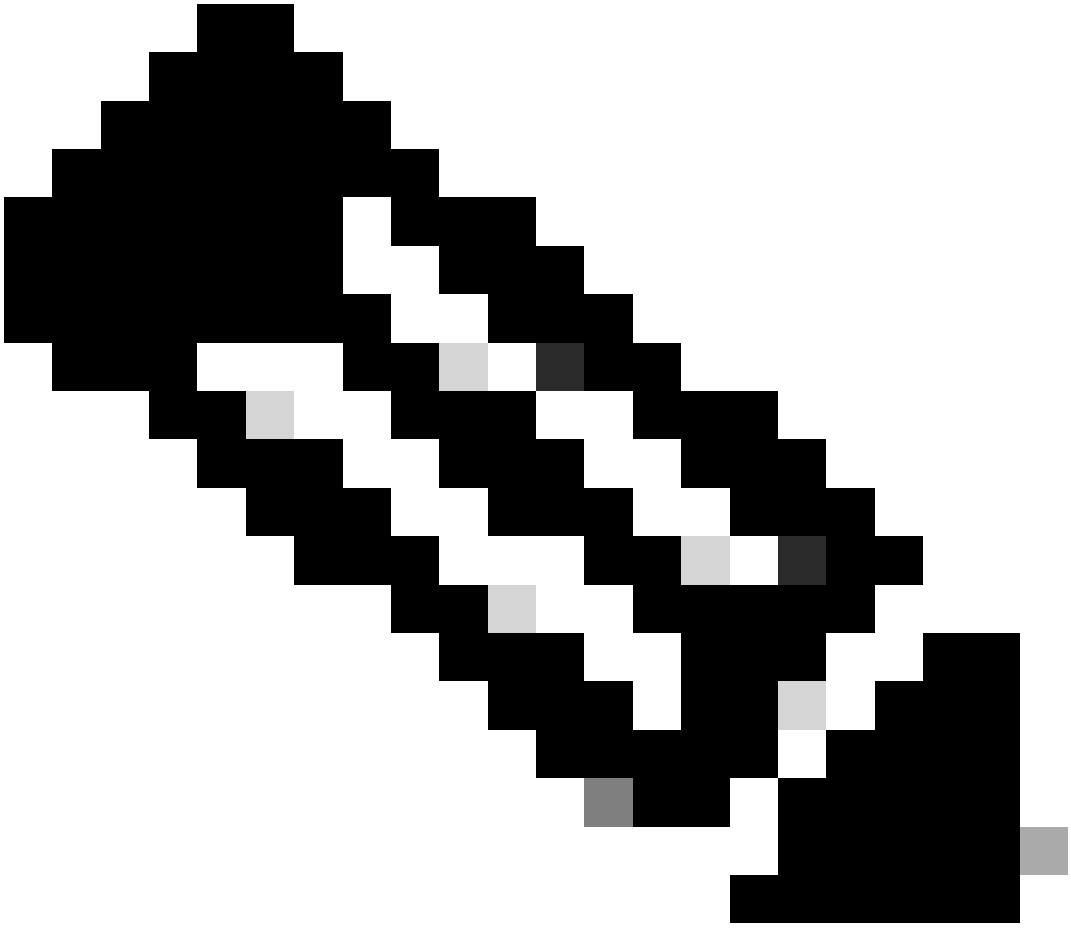


3. Sous l'onglet Authentication and Authorization, cliquez sur Create > Authentication Service > SSO.



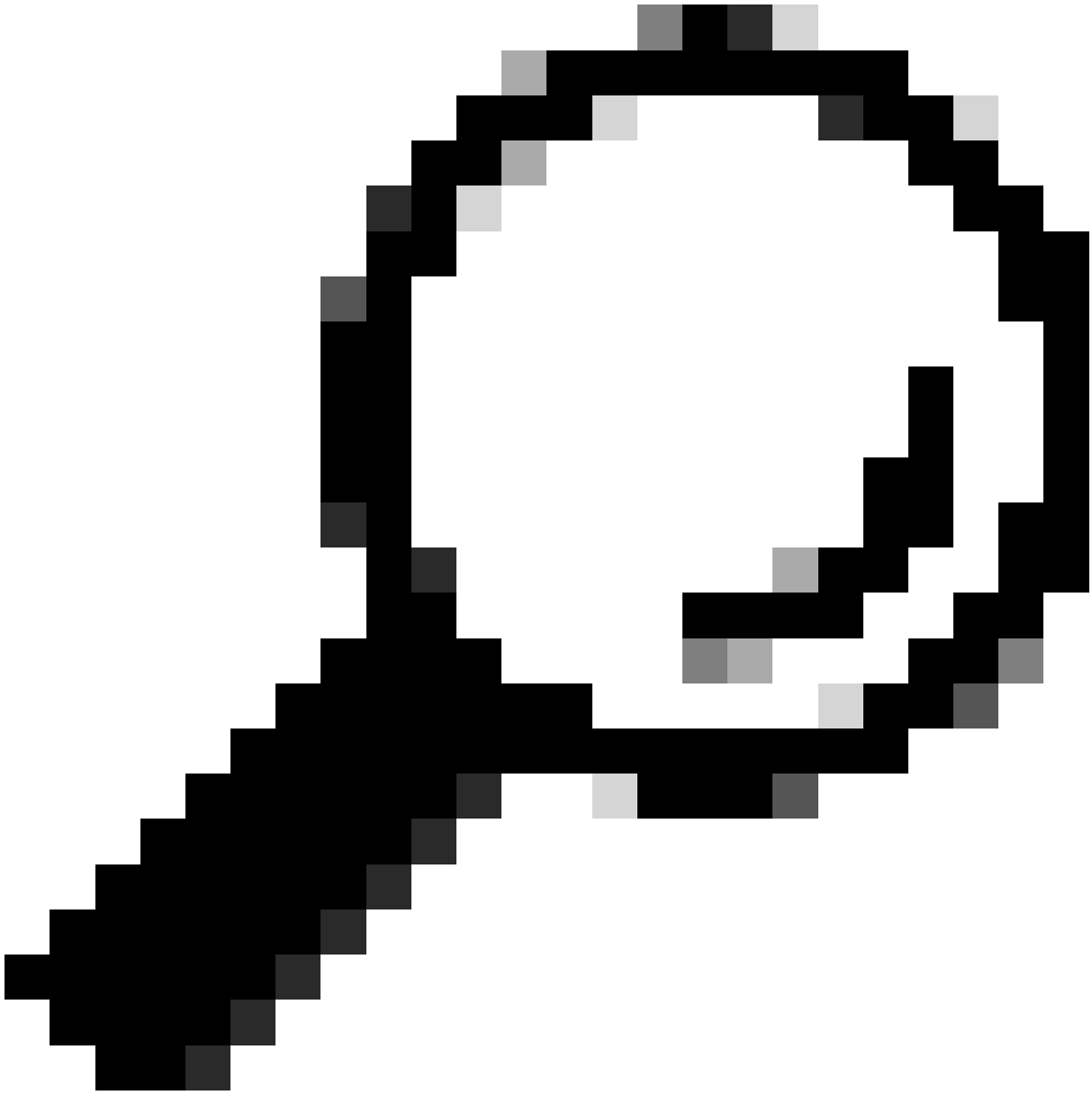
4. Sélectionnez la case d'option appropriée pour l'URL de métadonnées du fournisseur d'identité ou Télécharger le fichier XML de métadonnées du fournisseur d'identité.





Remarque : Dans cette démonstration, l'option Télécharger le fichier XML de métadonnées du fournisseur d'identités est sélectionnée.

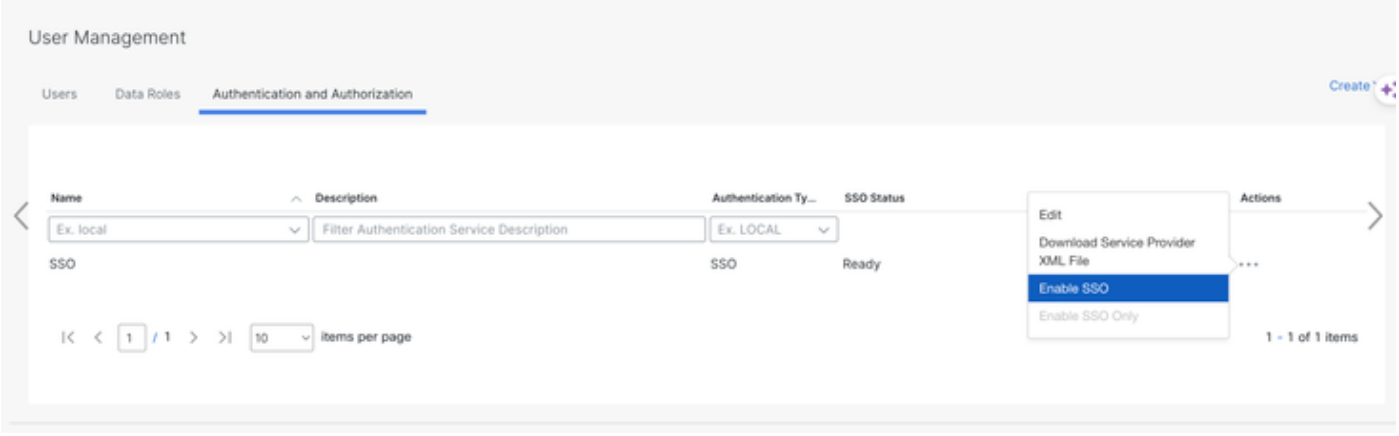
5. Configurez le champ Type de fournisseur d'identité sur Microsoft Entra ID, le format d'identificateur de nom sur Persistent, tapez une étiquette d'écran de connexion.



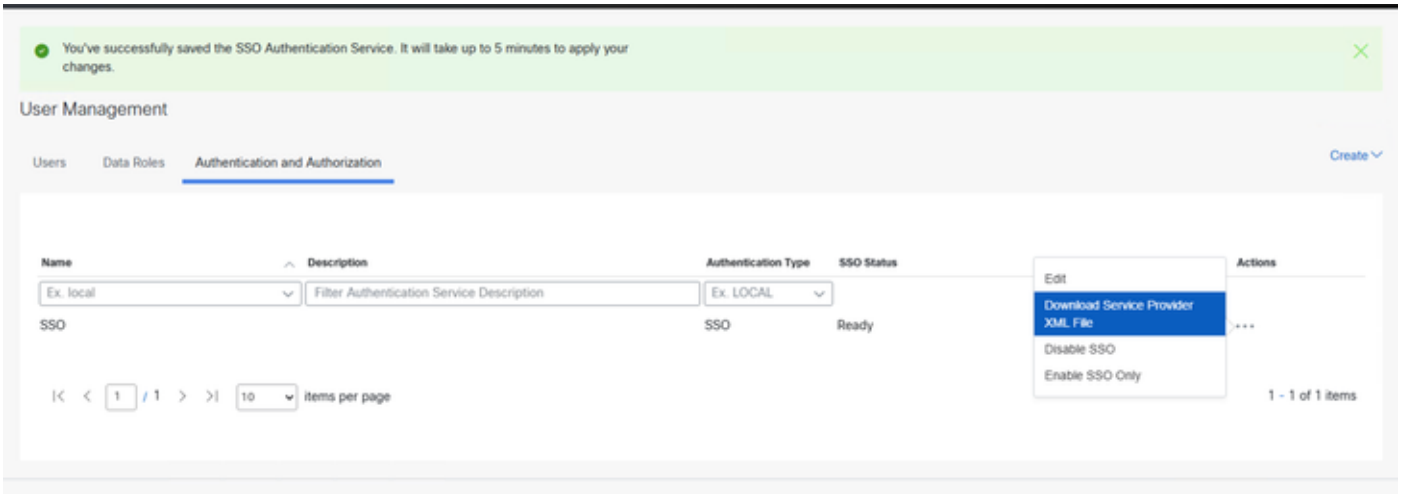
Conseil : Le libellé de l'écran de connexion configuré (nom/texte) apparaît au-dessus du bouton Connexion avec SSO et ne doit pas rester vide.

6. Cliquez sur Enregistrer pour revenir à l'onglet Authentification et autorisation.

7. Attendez que le statut soit READY et sélectionnez Enable SSO dans le menu d'action.



8. Sous l'onglet Authentification et autorisation, cliquez sur les trois points dans la colonne Actions et cliquez sur Télécharger le fichier XML du fournisseur de services.



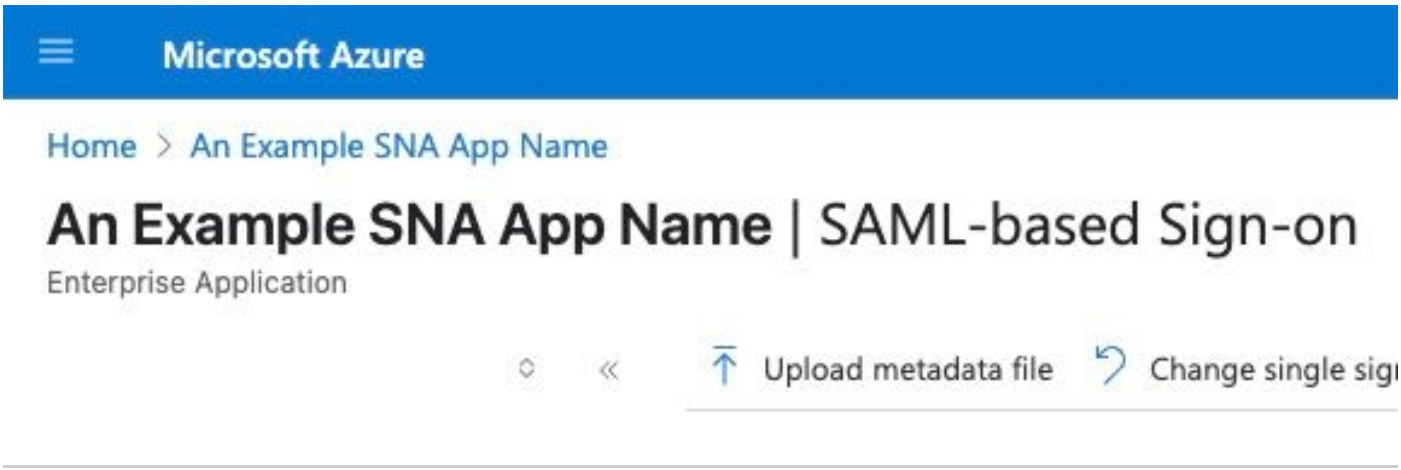
Configurer SSO dans Azure

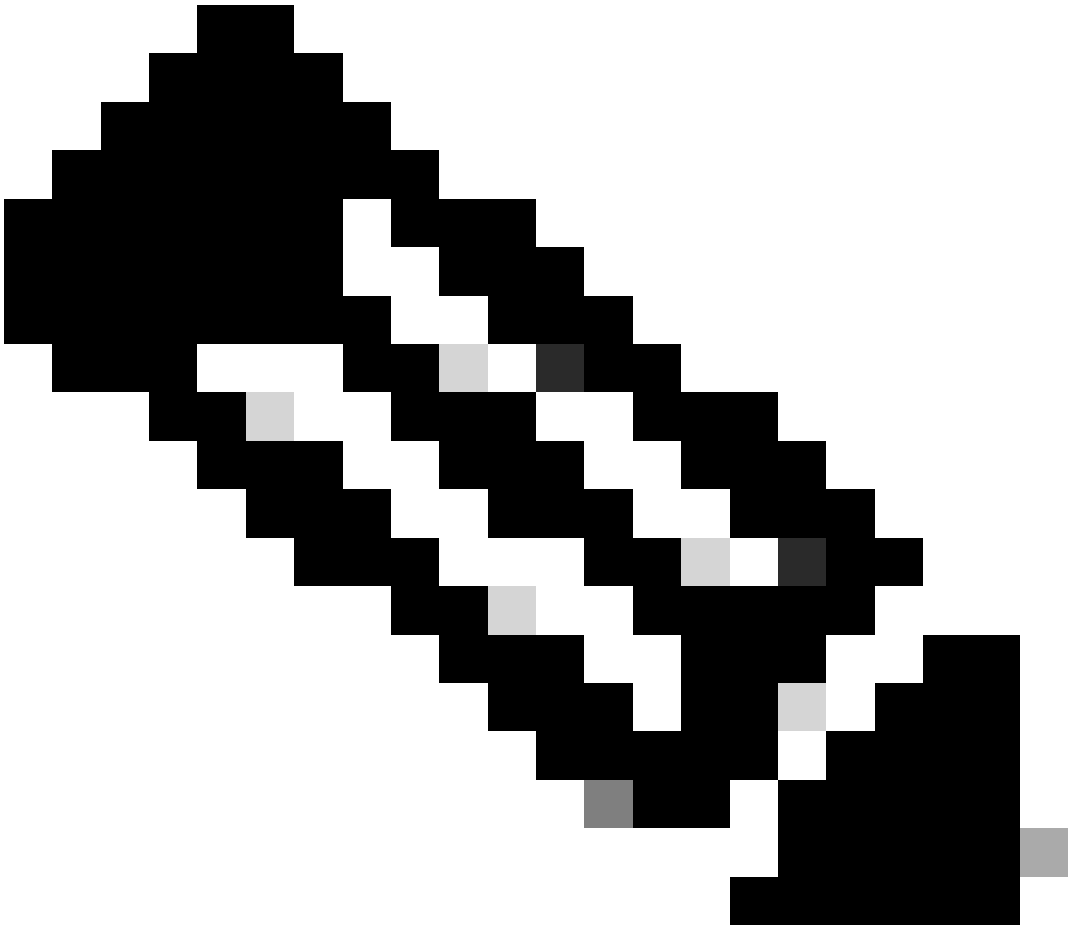
1. Connectez-vous au portail Azure.

2. Dans la barre de recherche, accédez à Application d'entreprise > Sélectionner l'application d'entreprise configurée > Cliquez sur Configurer l'authentification unique.

3. Cliquez sur Upload metadata file en haut de la page et téléchargez le fichier sp.xml téléchargé depuis SNA Manager.

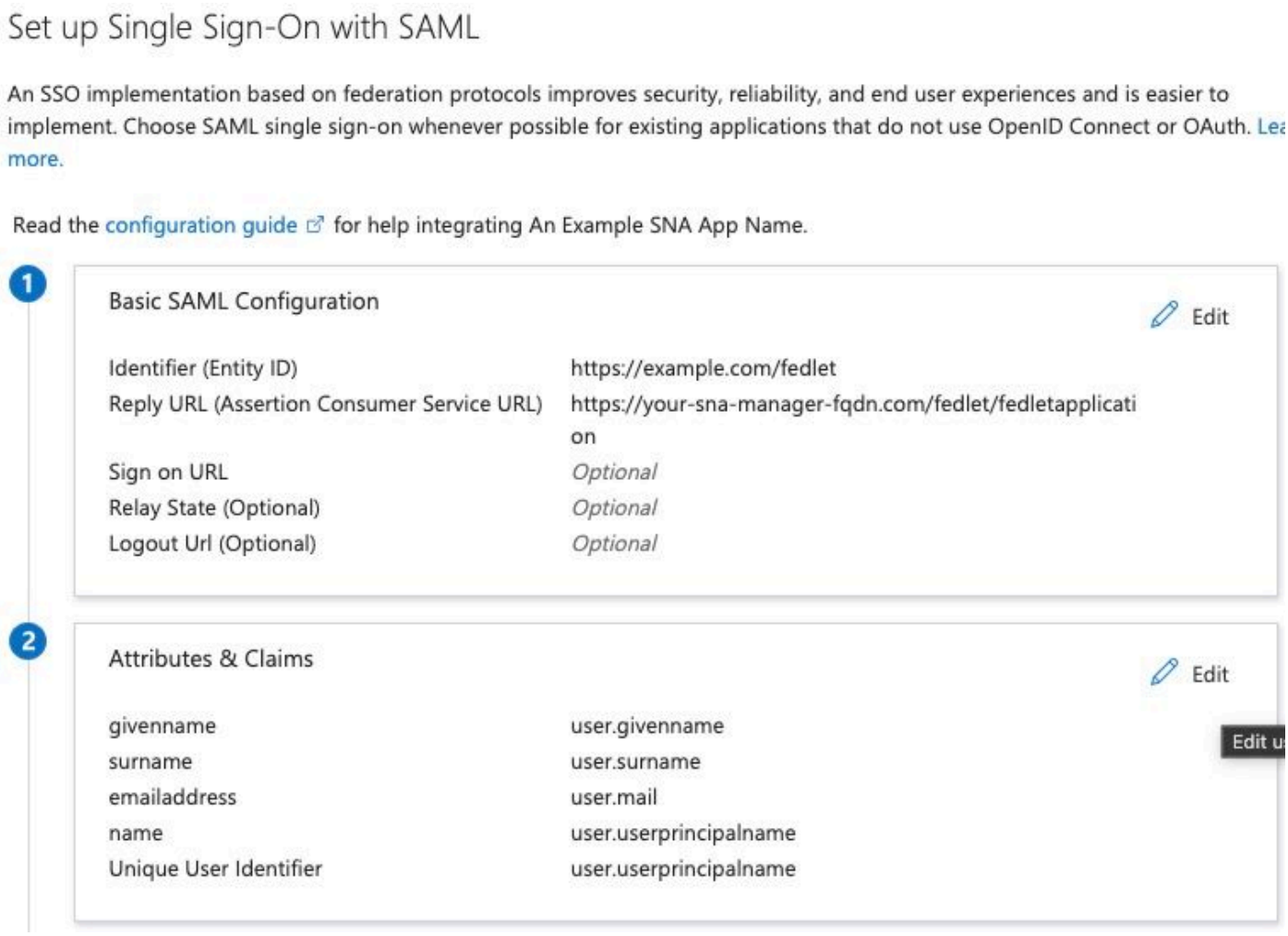
4. Il ouvre l'écran "Configuration SAML de base" et définit divers paramètres pour corriger les valeurs, Cliquez sur Enregistrer.





Remarque : Assurez-vous que le format d'ID de nom dans ID supplémentaire est correct.

5. Localisez la section Attributs et revendications et cliquez sur Modifier.



6. Cliquez sur la valeur user.userprincipalname sous la section Nom de la demande.

7. Sur la page Gérer la demande, vérifiez Choisir le format d'identificateur de nom.

Microsoft Azure

Search

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

Manage claim ...

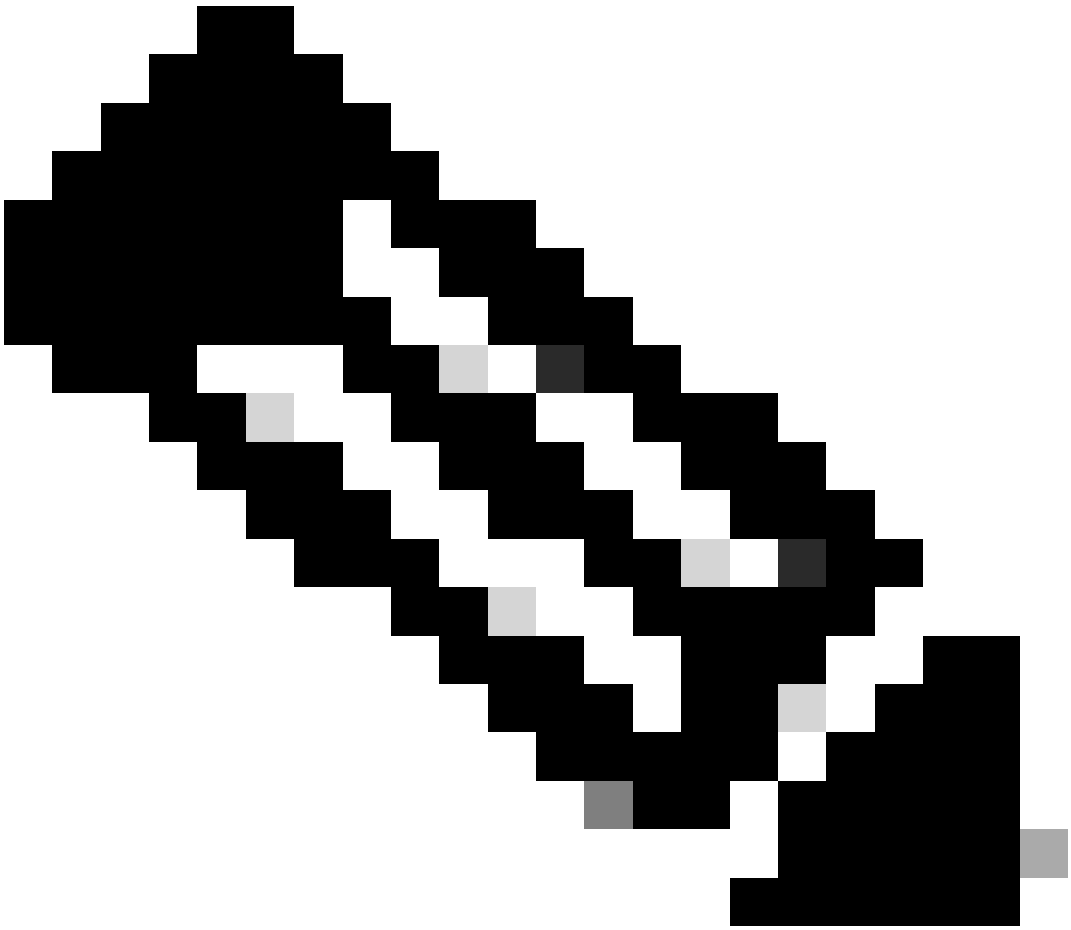
Save | Discard changes | Got feedback?

Name: nameidentifier

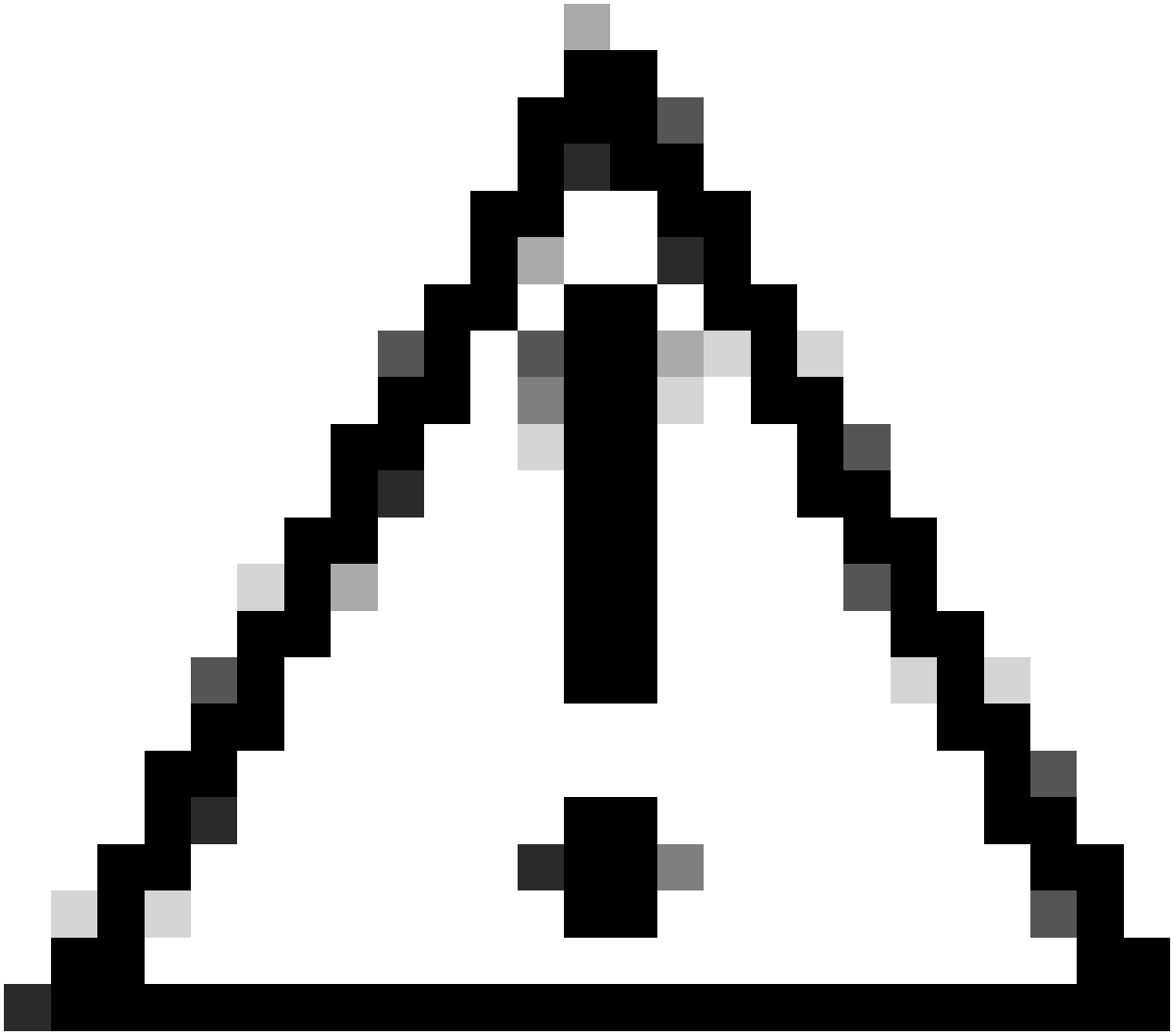
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Persistent



Remarque : Le champ de format d'identificateur de nom est défini sur Persistant si ce n'est pas le cas, sélectionnez-le dans le menu déroulant. Cliquez sur Enregistrer si des modifications ont été apportées.

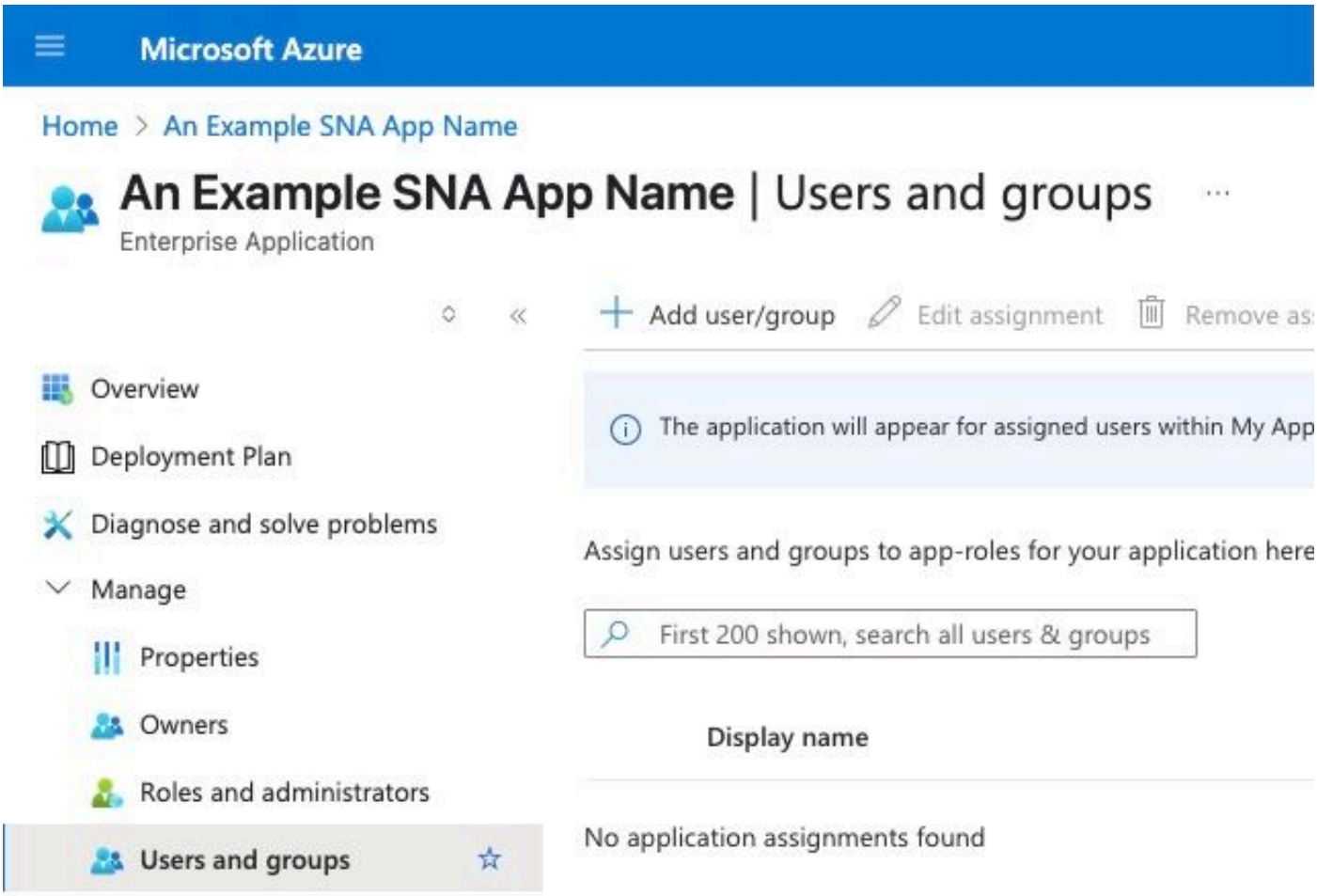


Mise en garde : C'est l'endroit le plus courant pour rencontrer des problèmes. Les paramètres de SNA Manager et de Microsoft Azure doivent correspondre. si vous avez choisi d'utiliser le format « adresse e-mail » dans l'architecture SNA, le format doit également être « adresse e-mail ».

Configurer les utilisateurs avec l'ID d'entrée.

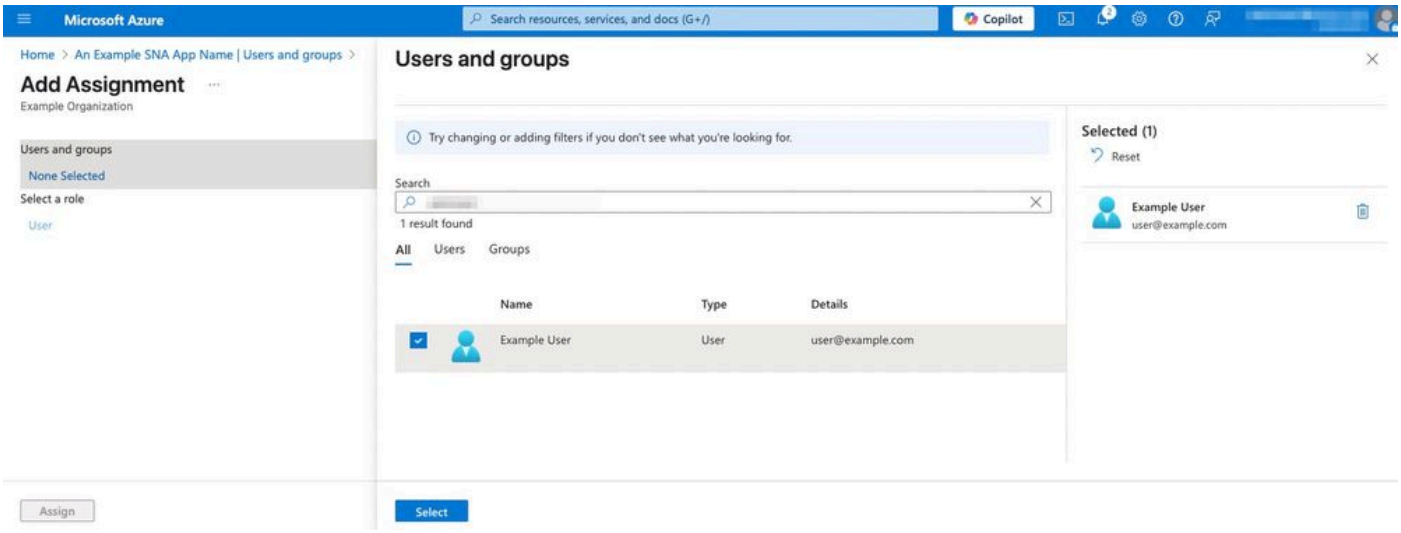
1. Connectez-vous au portail Azure.

2. Dans la barre de recherche, accédez à Application d'entreprise > Sélectionner l'application d'entreprise configurée > sélectionnez Utilisateurs et groupes sur la gauche > cliquez sur Ajouter un utilisateur/groupe.



3. Dans le volet de gauche, cliquez sur Aucun sélectionné.

4. Recherchez et ajoutez l'utilisateur requis à l'application.

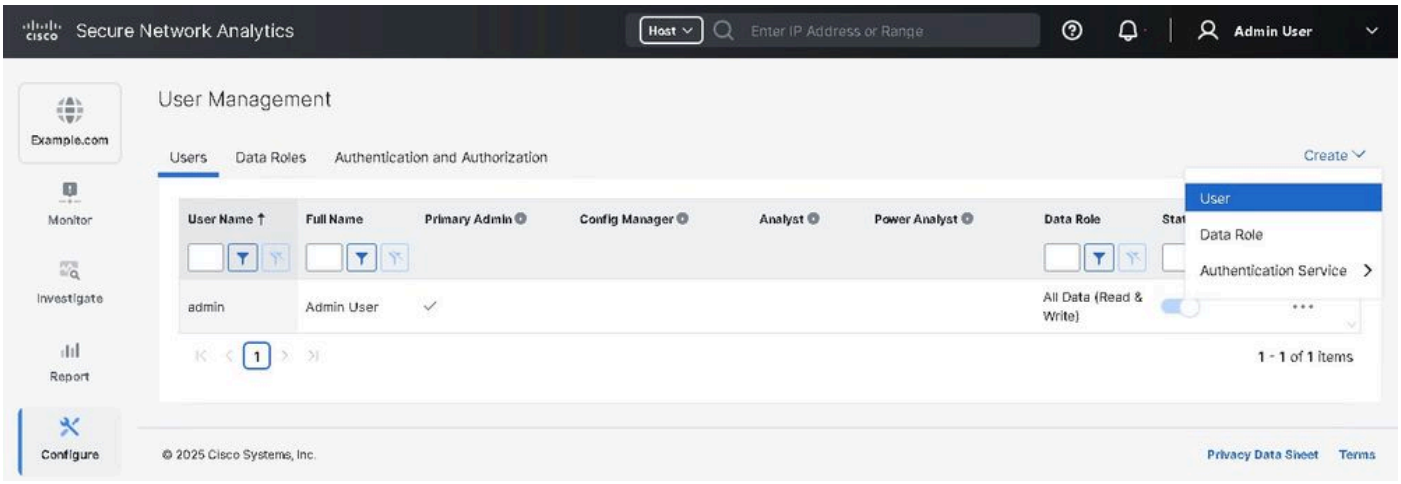


Configurer SSO dans SNA

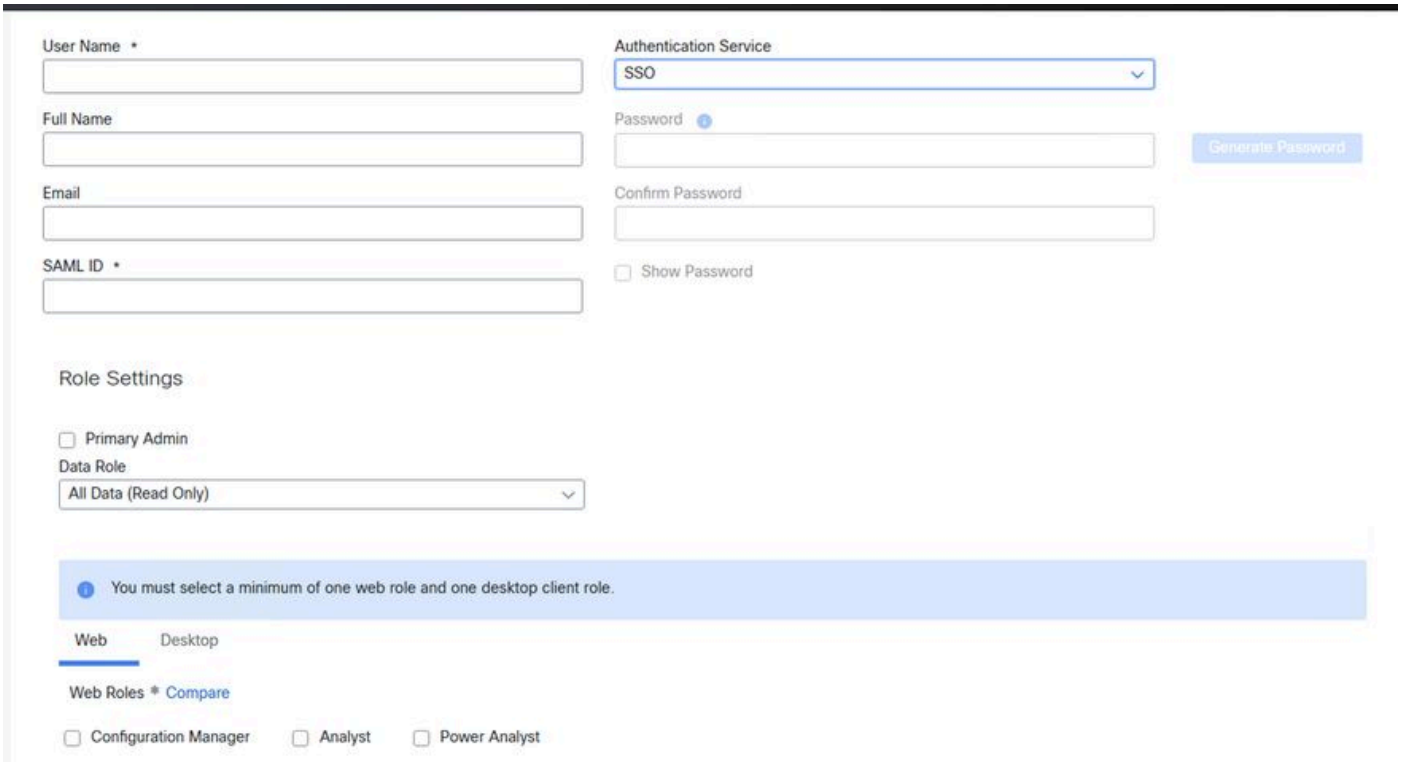
1. Connectez-vous à l'interface utilisateur de SNA Manager.

2. Accédez à Configure > Global > User Management.

3. Cliquez sur Créer > Utilisateur.



4. Configurez l'utilisateur en fournissant les détails associés au service d'authentification sélectionné comme SSO et cliquez sur Enregistrer.



Création SAML-User dans SNA-UI

Dépannage

Si les utilisateurs ne parviennent pas à se connecter à SNA Manager, un traceur SAML peut être utilisé pour approfondir les recherches.

Si une assistance supplémentaire est nécessaire pour enquêter sur le SNA Manager, un dossier TAC peut être généré.

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.