

Configurer SNA Manager pour Microsoft Entra ID SSO

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration Steps](#)

[Configurer l'application d'entreprise dans Azure](#)

[Configuration et téléchargement du fichier XML du fournisseur de services dans SNA](#)

[Configurer SSO dans Azure](#)

[Configurer les utilisateurs avec l'ID d'entrée.](#)

[Configurer SSO dans SNA](#)

[Dépannage](#)

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

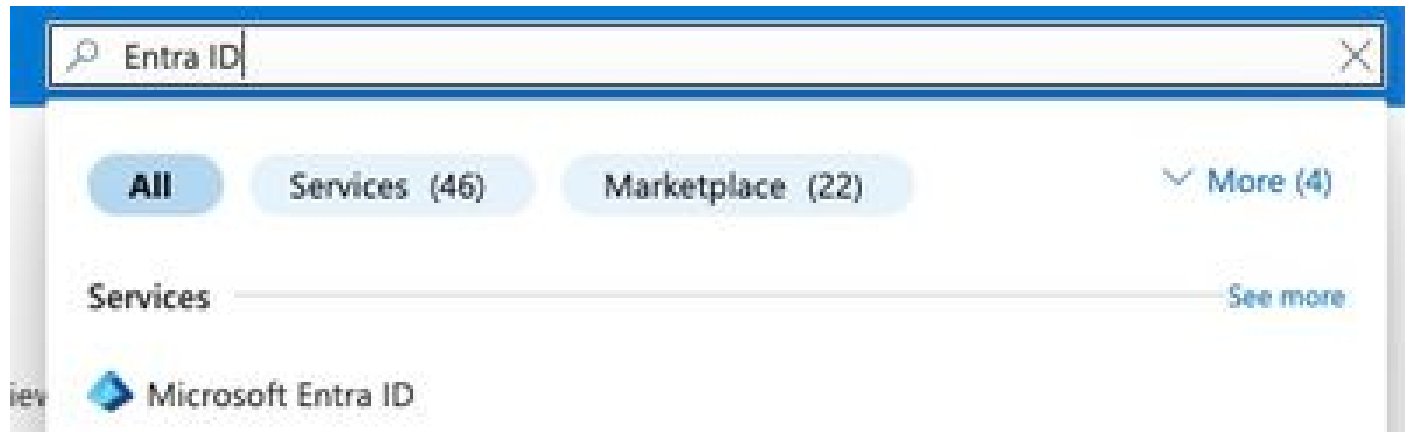
- SNA Manager v7.5.2
- ID d'entrée Microsoft

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.

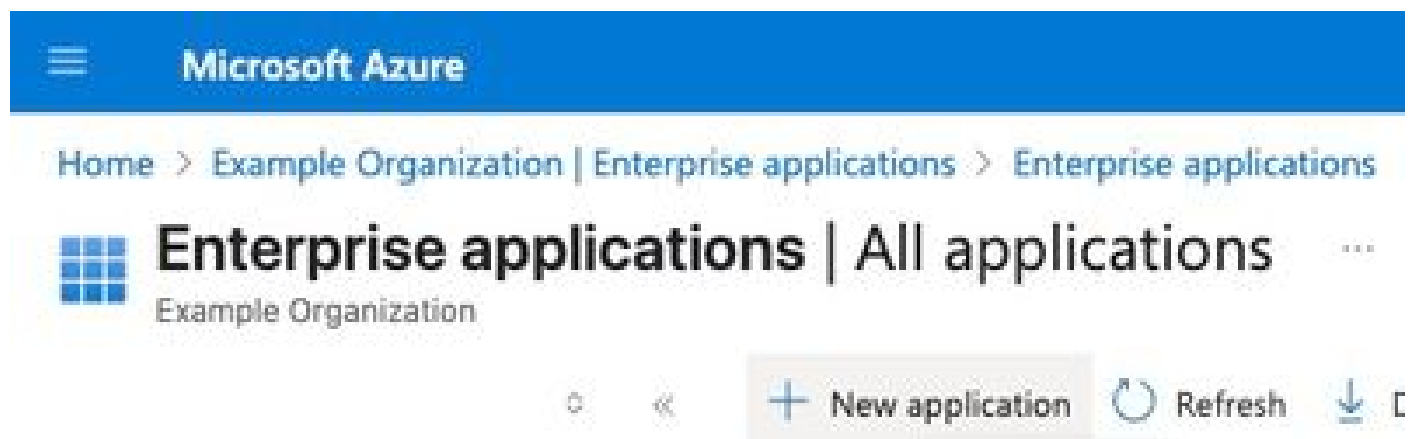
Configuration Steps

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.



[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. 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.

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



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 ⓘ

[Application ID]

Object 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. Sélectionnez SAML.

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), Provisioning, and Authentication. The main content area has a heading 'Select a single sign-on method' with a 'Help me decide' link. Below this, there are two cards: 'Disabled' (with a crossed-out circle icon) and 'SAML' (with a plus icon). The 'Disabled' card states: 'Single sign-on is not enabled. The user won't be able to launch the app from My Apps.' The 'SAML' card states: 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

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

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. Below is a table of configuration options:

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

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.

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

https://example.com/fedlet



[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

https://example.com/fedlet/fedletapplication



[Add reply URL](#)

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.

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

https://login.microsoftonline.com/af42bac0-52aa- ...

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

Verification certificates (optional)

Edit

Required

No

Active

0

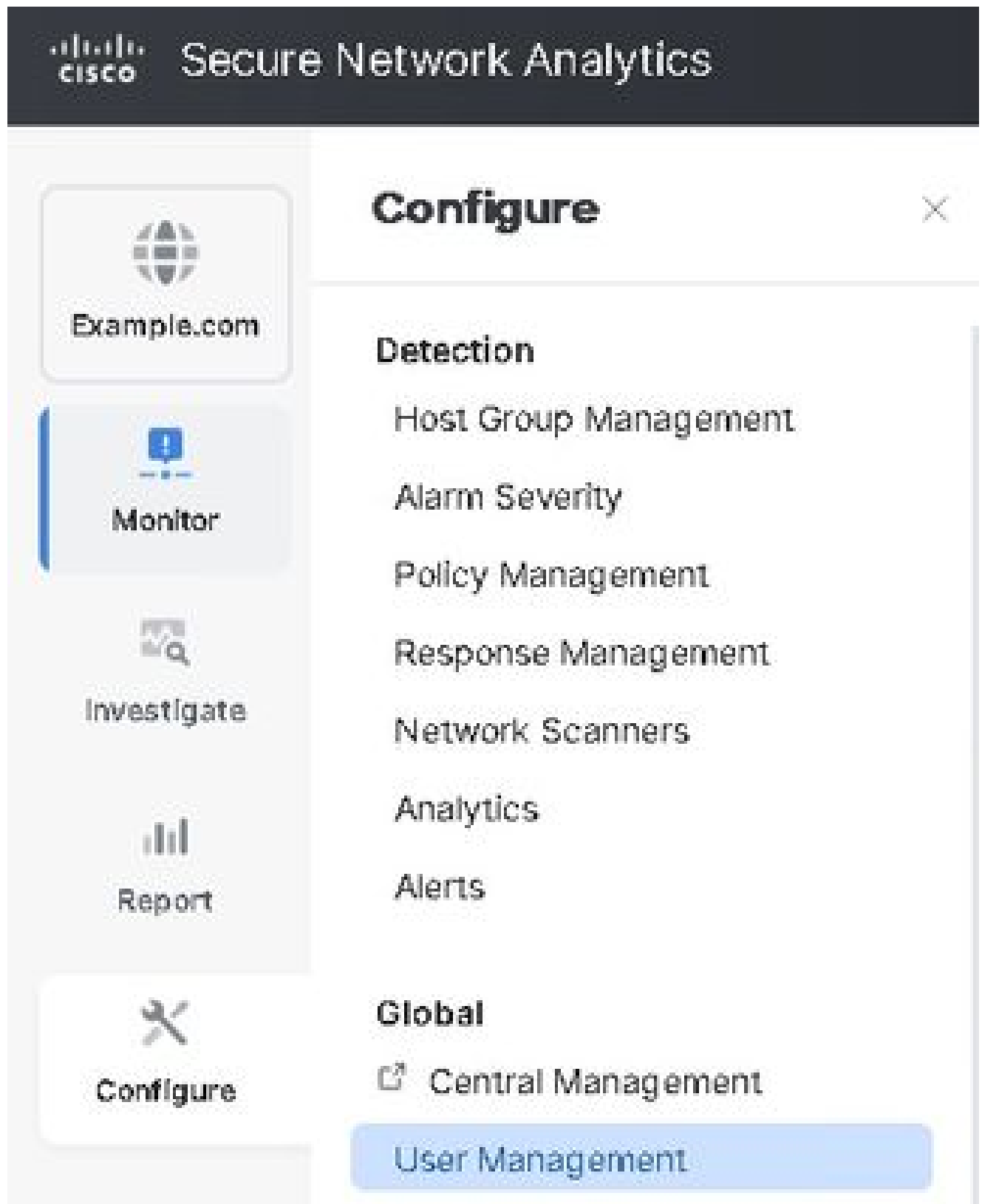
Expired

0

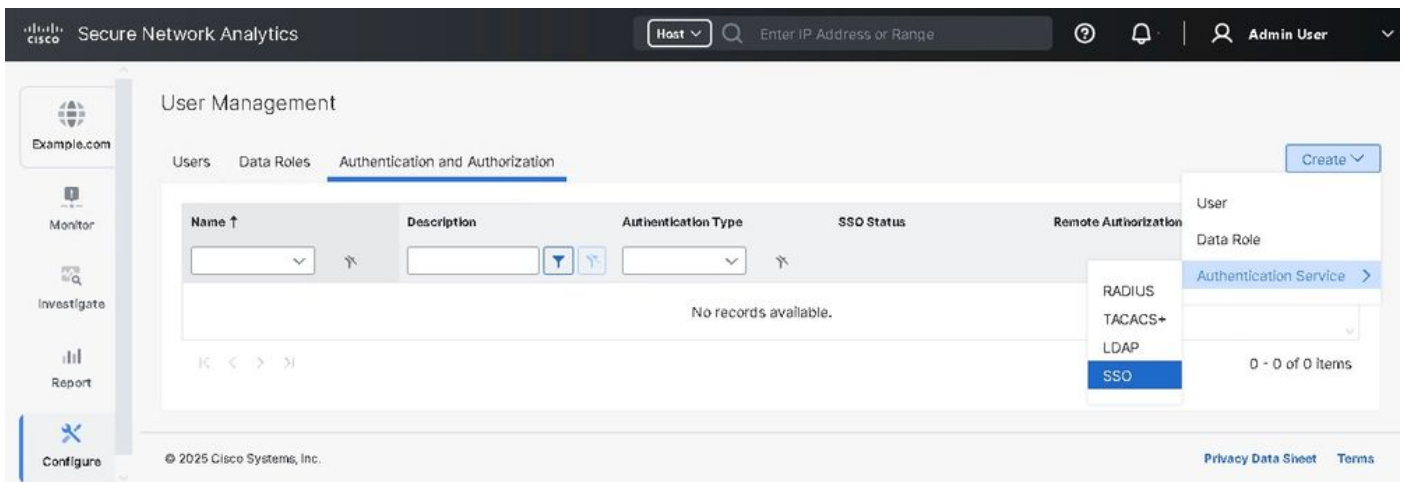
Configuration et téléchargement du fichier XML du fournisseur de services dans

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.

User Management | Authentication Service

Cancel Save

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

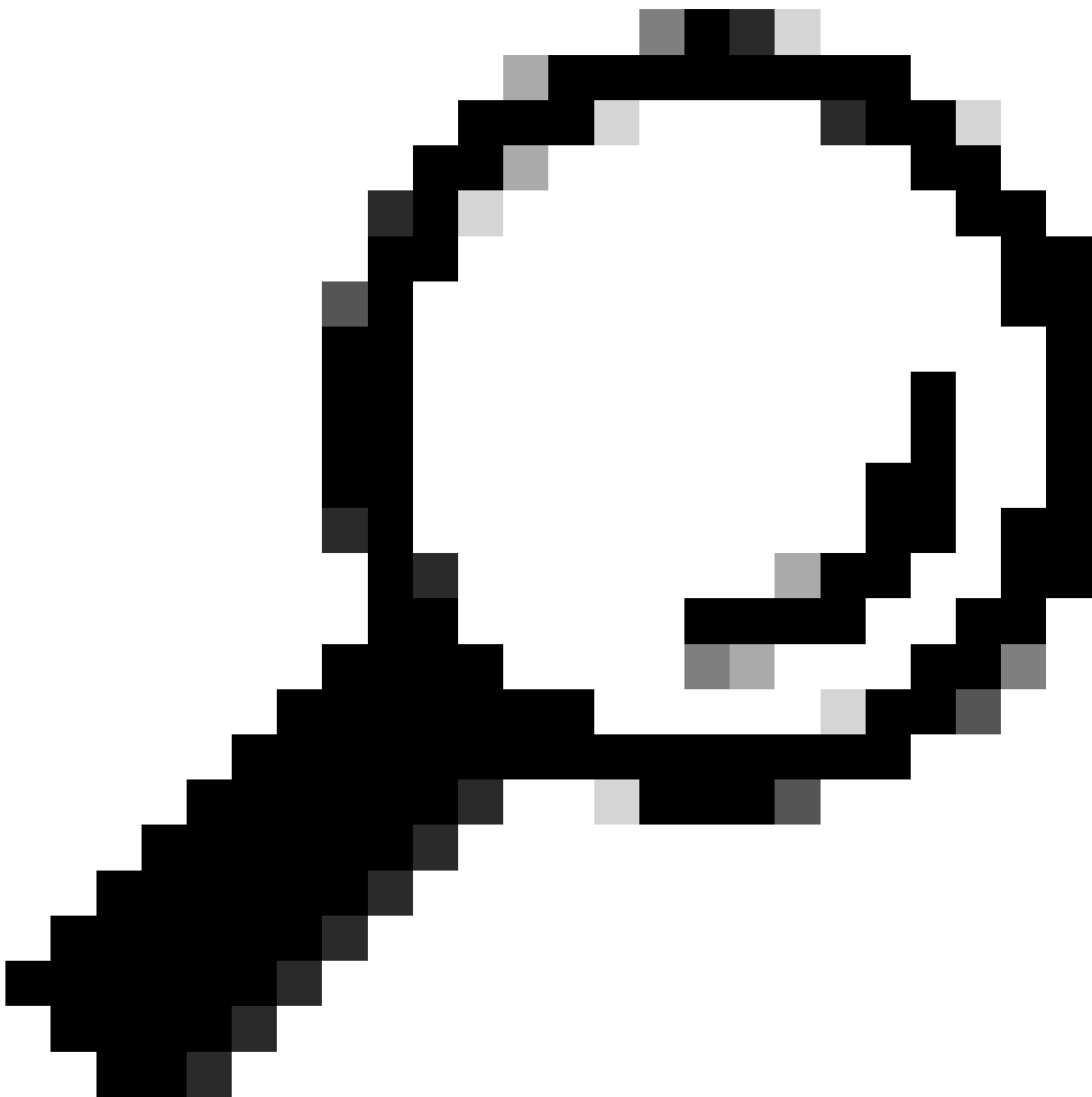
General Configuration

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



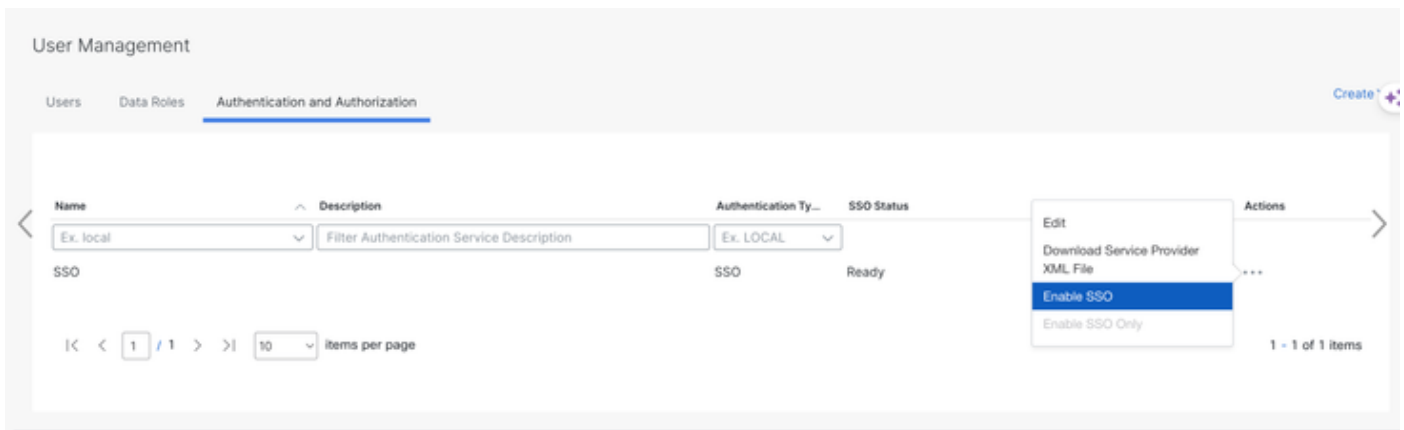
Remarque : Dans cette démonstration, l'option Télécharger le fichier XML de métadonnées du fournisseur d'identités est sélectionnée.

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.

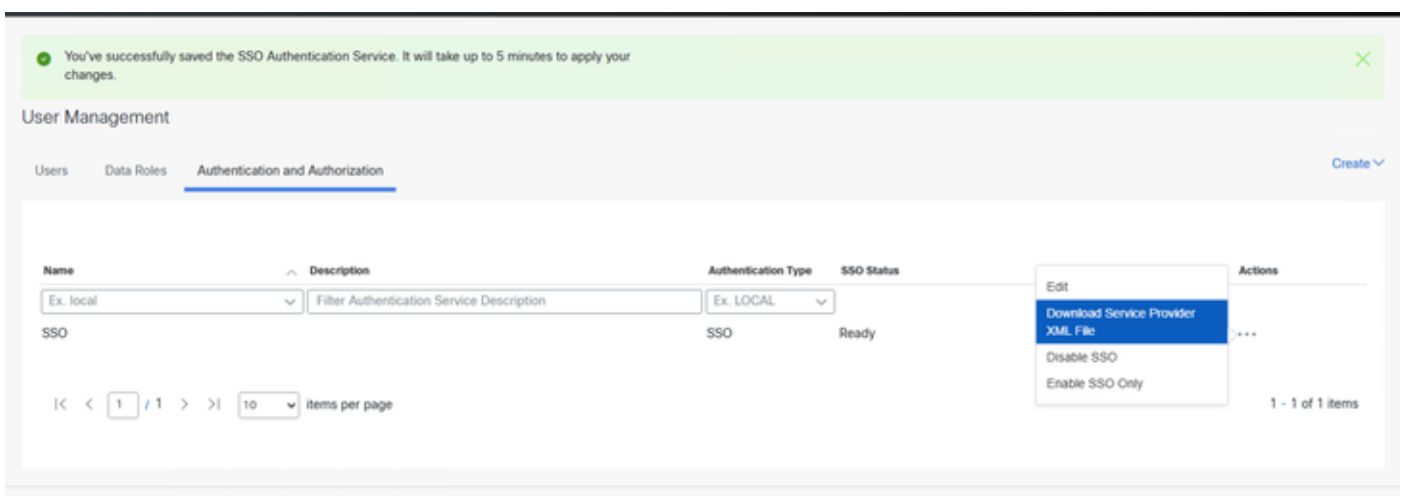


Conseil : Le libellé de l'écran de connexion configuré (nom/texte) apparaît au-dessus du bouton Connexion avec SSO et ne doit pas rester vide.

-
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.



[Home](#) > [An Example SNA App Name](#)

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

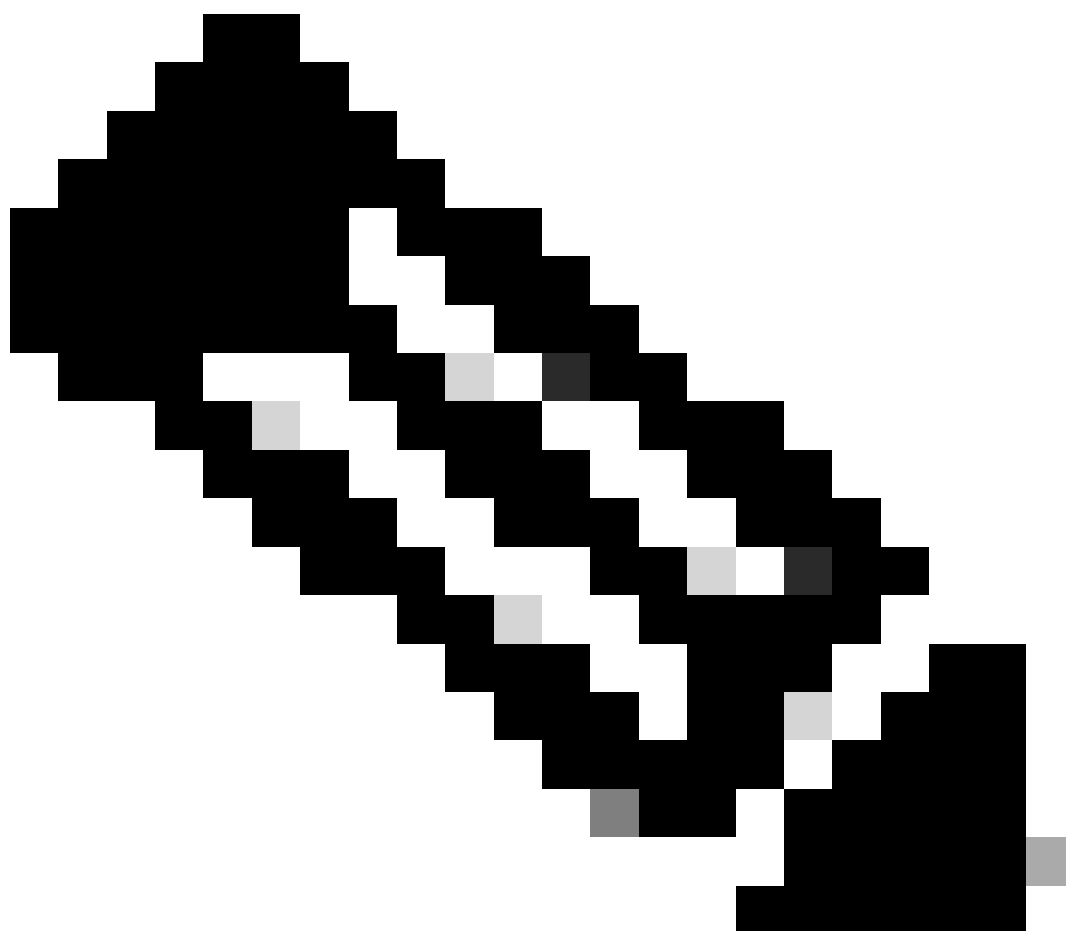
Enterprise Application



Upload metadata file



Change single sign-on



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.

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

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



Manage claim ...



Save



Discard changes



Got feedback?

Name

nameidentifier

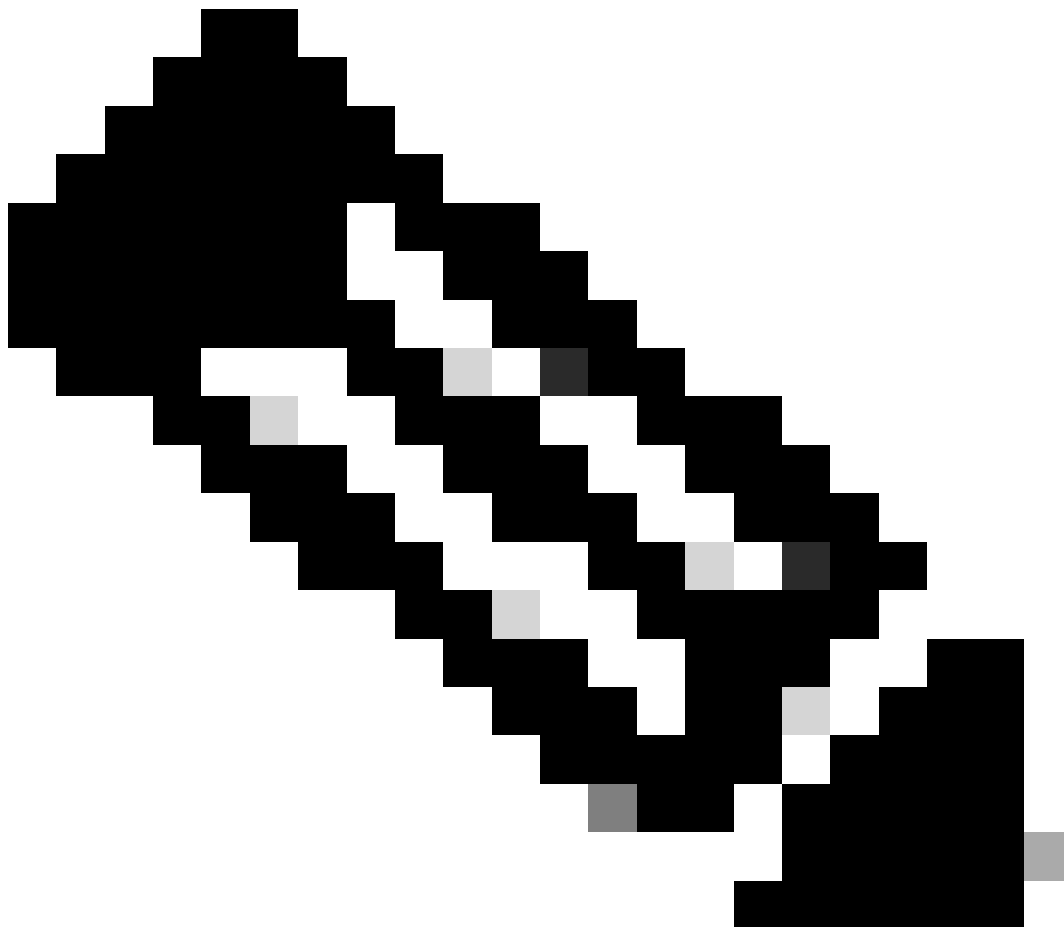
Namespace

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

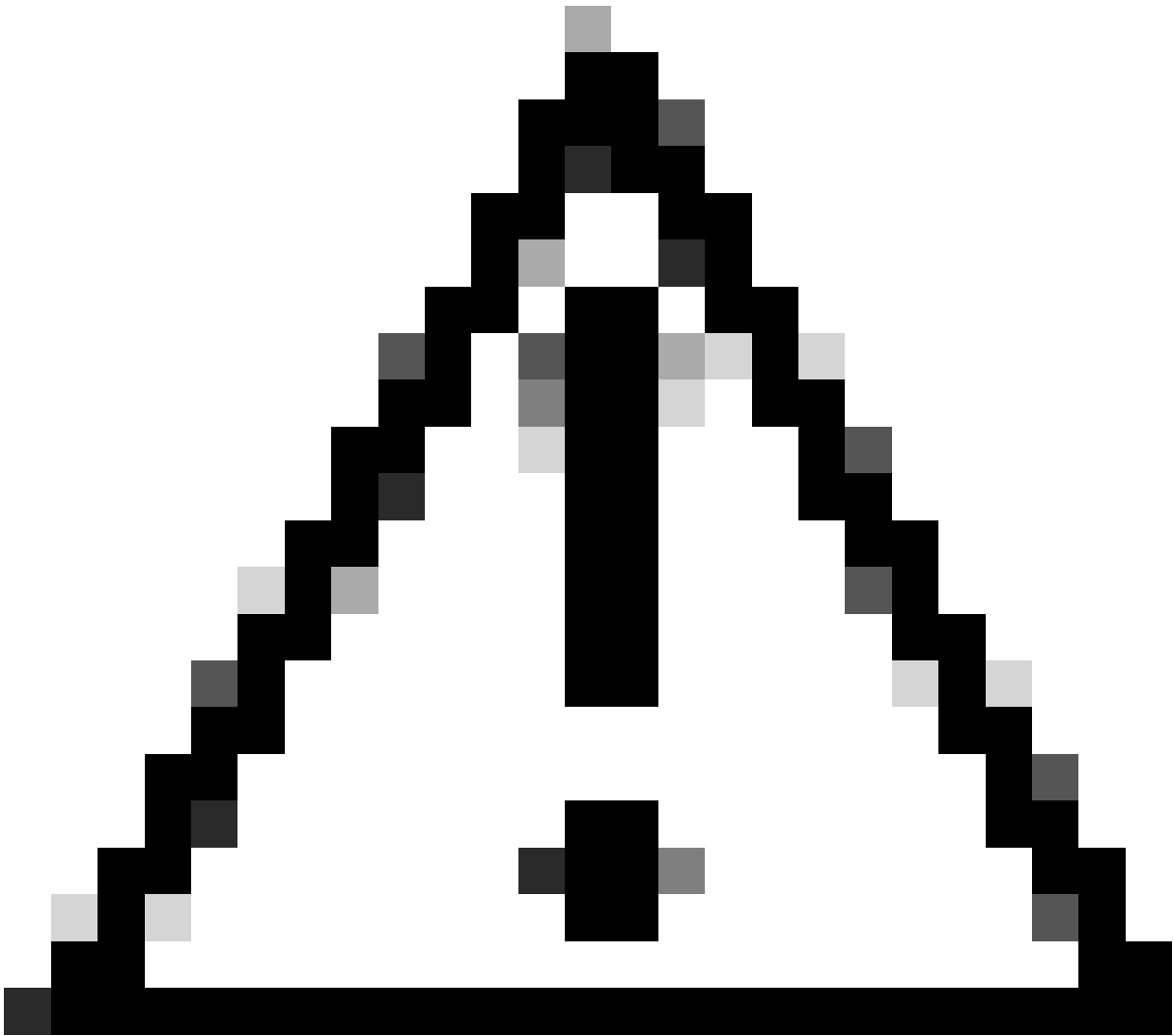
Choose name identifier format

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.

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

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

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

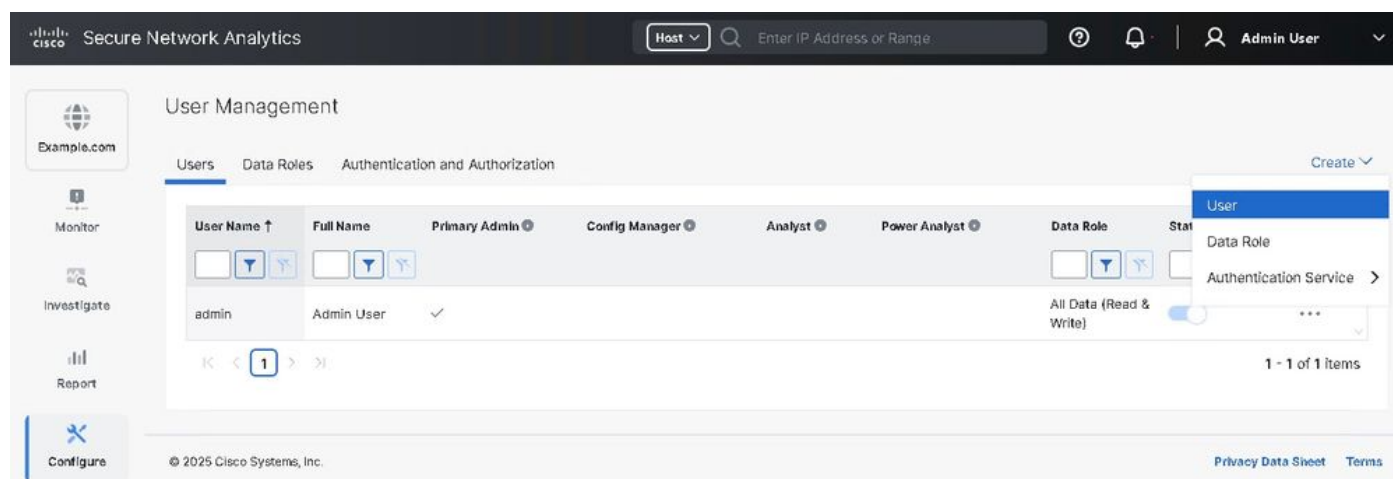
Assign Select

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.

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

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.