Configure SNA Manager for Microsoft Entra ID SSO

Contents

Introduction

This document describes how to configure Secure Network Analytics (SNA) to use Microsoft Entra ID for Single Sign On (SSO.)

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Microsoft Azure
- Secure Network Analytics

Components Used

- SNA Manager v7.5.2
- Microsoft Entra ID

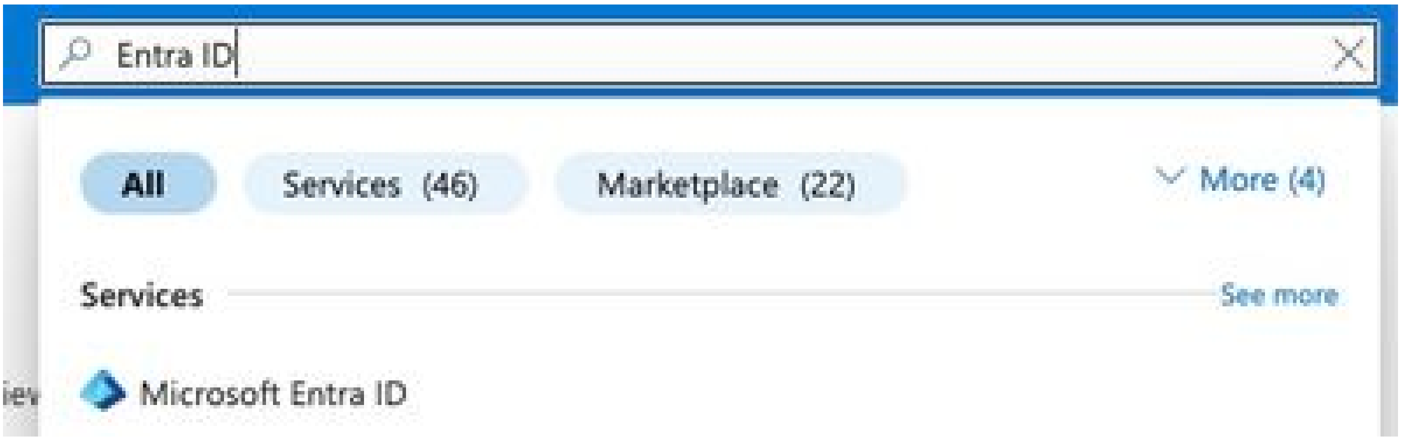
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration Steps

Configure Enterprise Application in Azure

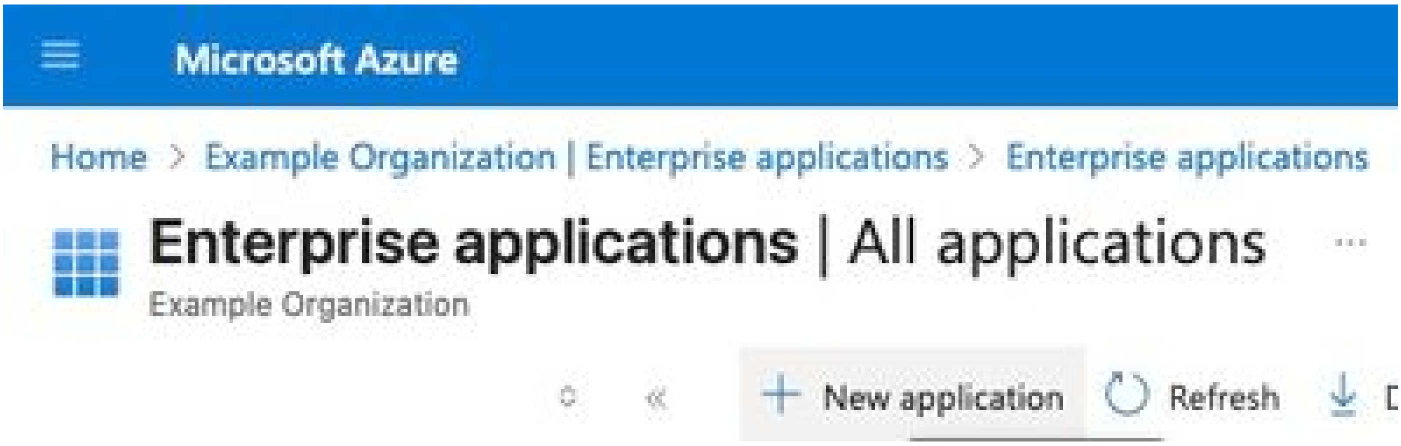
1. Log in to **Azure cloud portal**.

2. Search **Entra ID** service in the search box and select **Microsoft Entra ID**.

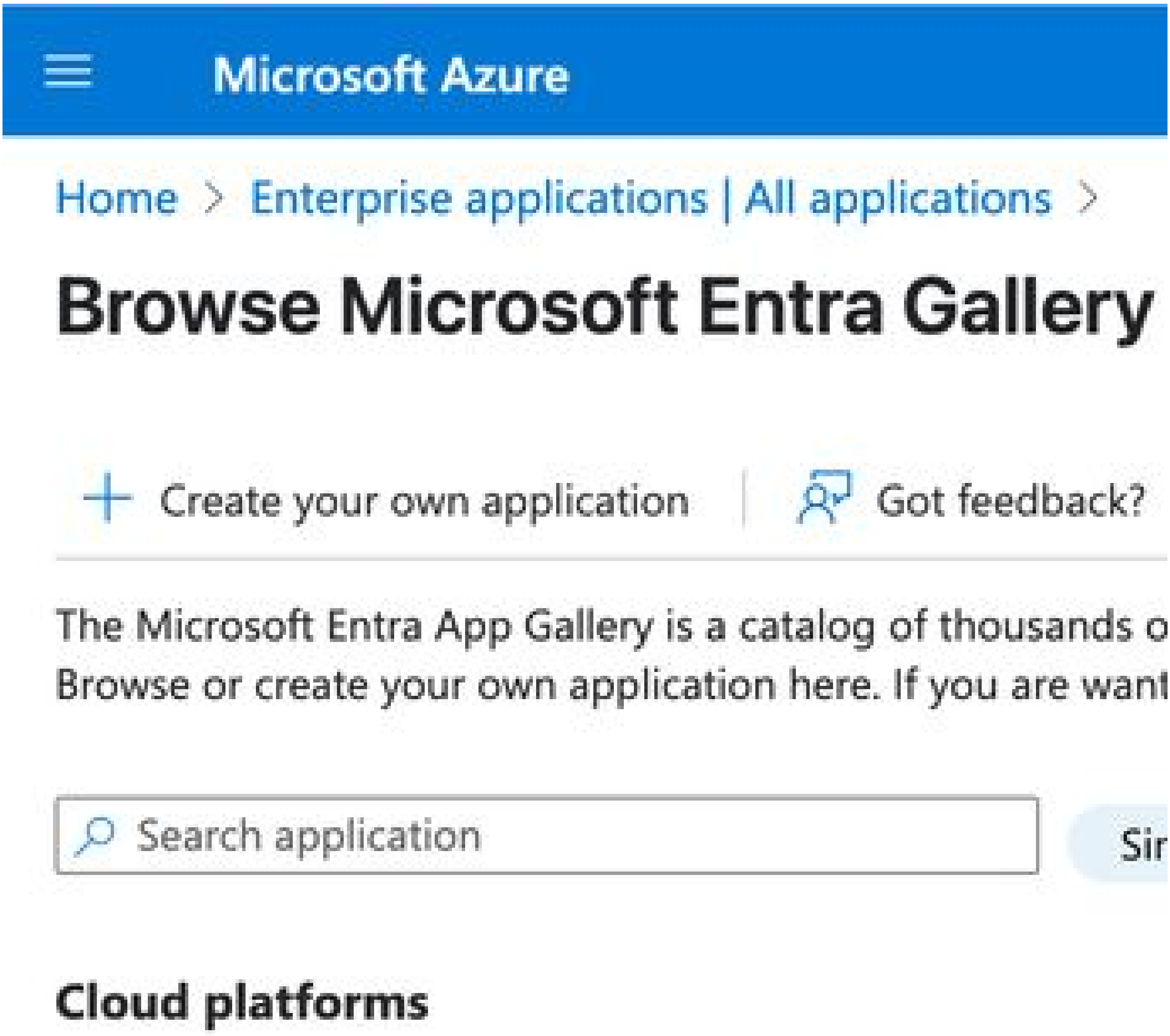


3. In the left pane expand **Manage** and select **Enterprise Applications.**

4. Click **New Application**.


Microsoft Azure
Home > Example Organization | Enterprise applications > Enterprise applications
Enterprise applications | All applications
Example Organization
New application
Refresh

5. Select **Create Your Own Application** on the new page that loads.


Microsoft Azure
Home > Enterprise applications | All applications >
Create your own application
Got feedback?
Search application
Sir

Browse Microsoft Entra Gallery

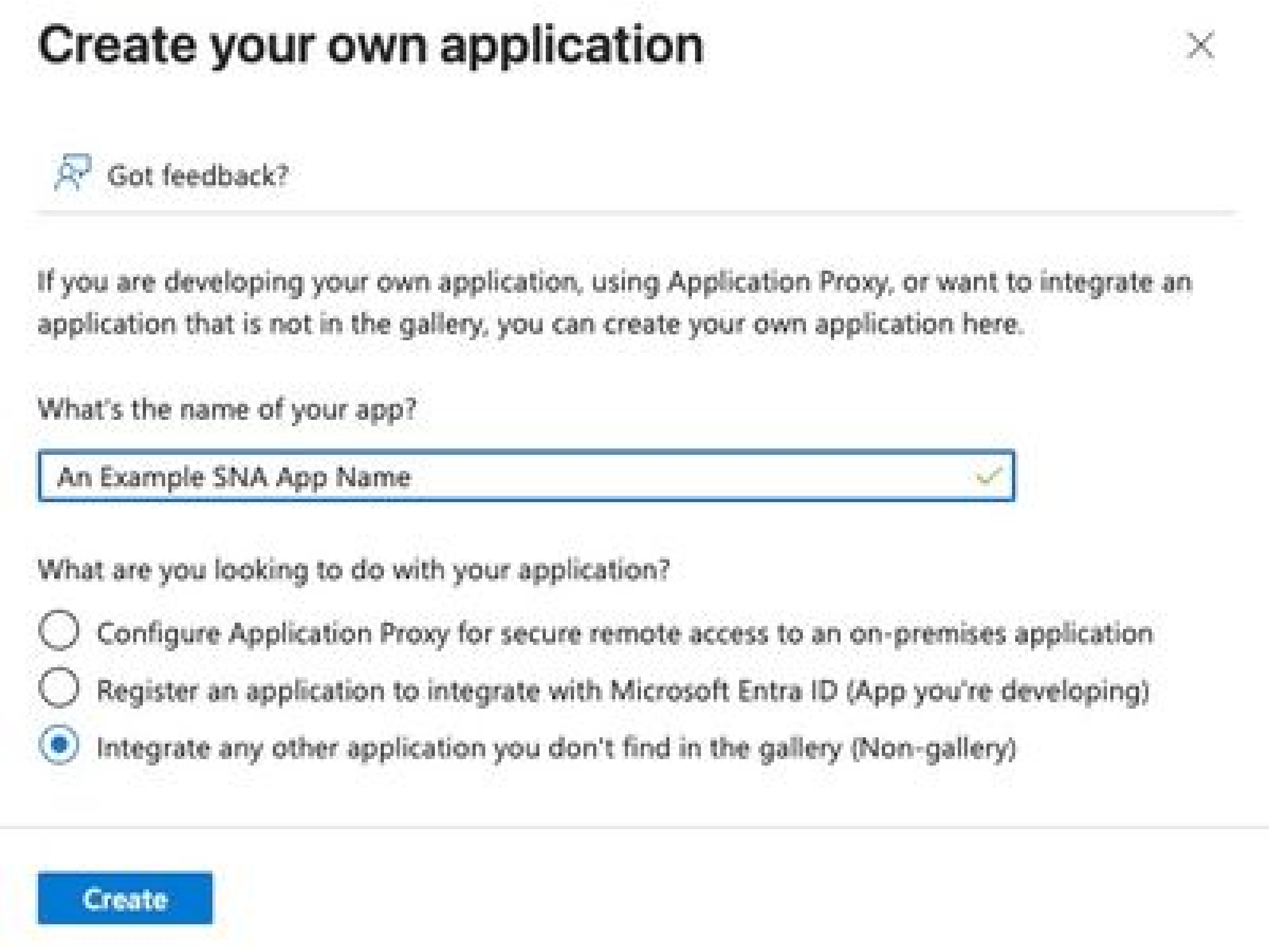
The Microsoft Entra App Gallery is a catalog of thousands o
Browse or create your own application here. If you are want

Cloud platforms

Azure-UI

6. Provide a name to application in **What's the name of your app?** field.

7. Select the radio button **Integrate any other application you don't find in the gallery (Non-gallery)** and click **Create**.



Create your own application

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 ✓

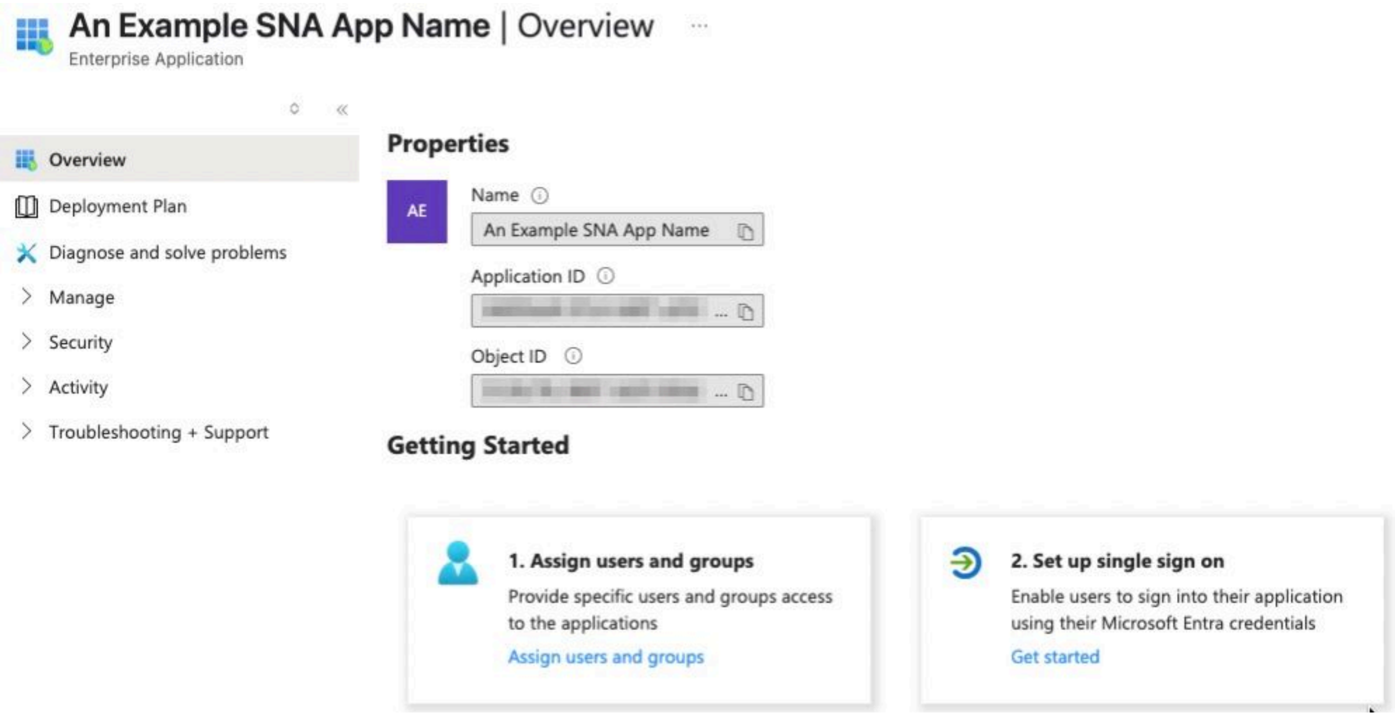
What are you looking to do with your application?

○ 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)

8. On newly configured application dashboard click **Set up single sign on**.



An Example SNA App Name | Overview

Enterprise Application

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

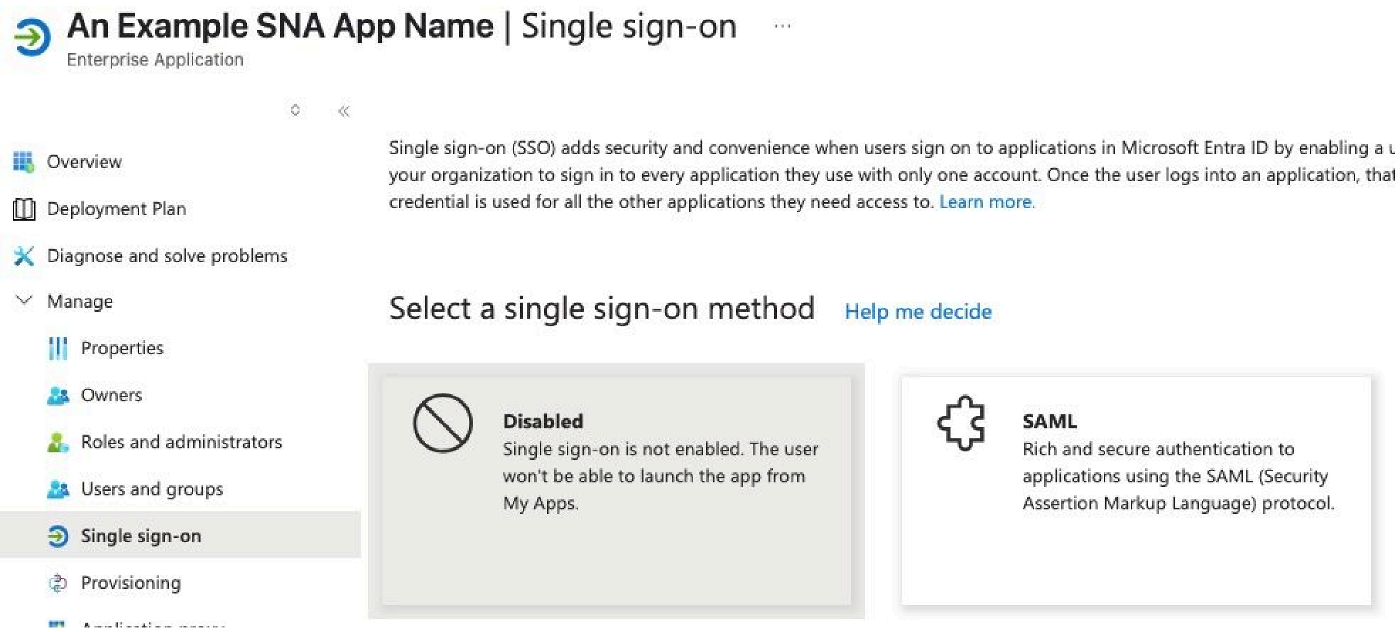
Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

Get started

9. Select **SAML**.



An Example SNA App Name | Single sign-on ...

Enterprise Application

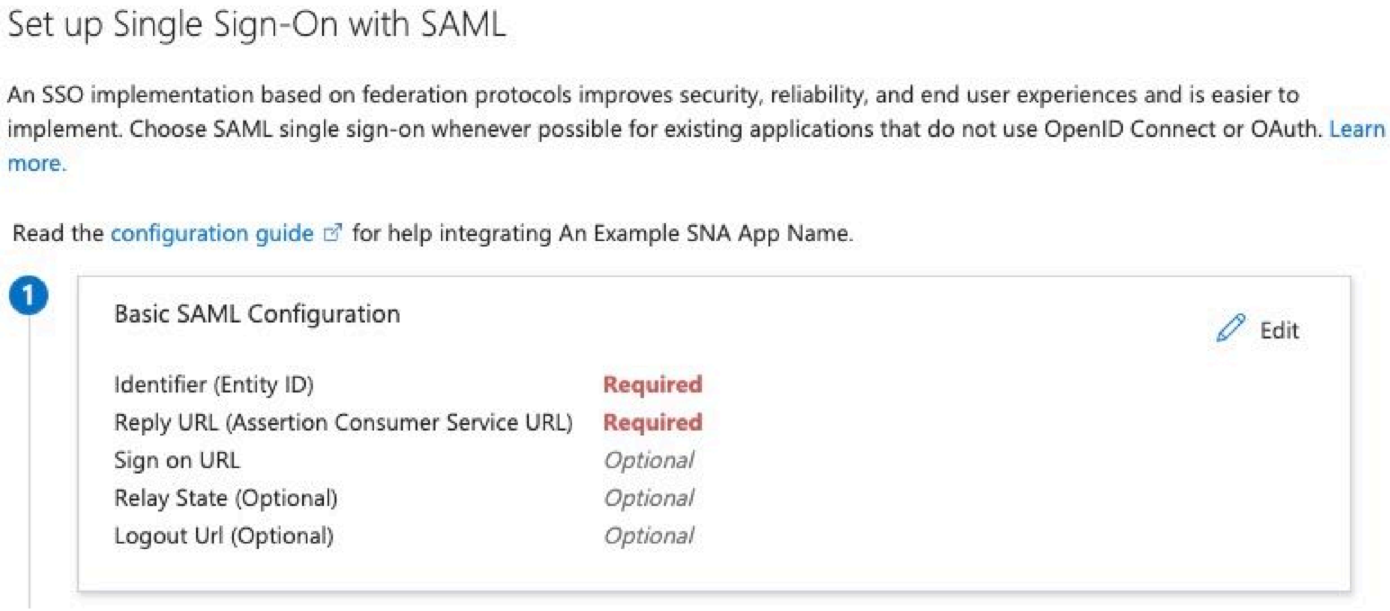
Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a u your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

10. On the Set up Single Sign-On with SAML page click **Edit** under Basic SAML Configuration.



Set up Single Sign-On with SAML

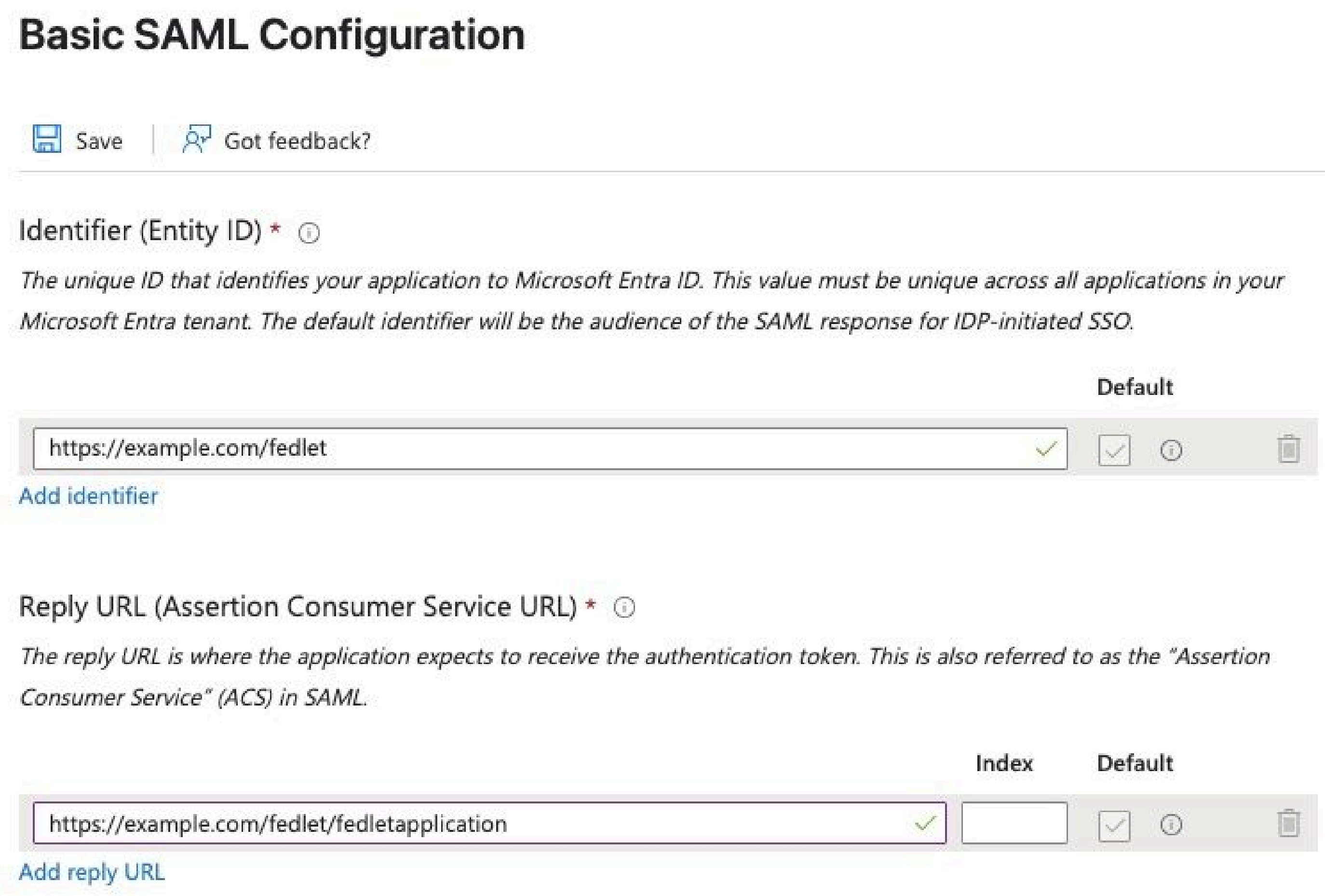
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating An Example SNA App Name.

1 Basic SAML Configuration Edit

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

11. Under **Basic SAML Configuration** pane configure **Add Reply URL** to https://example.com/fedlet/fedletapplication replacing example.com with FQDN of SNA Manager and click **save**.



Basic SAML Configuration

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

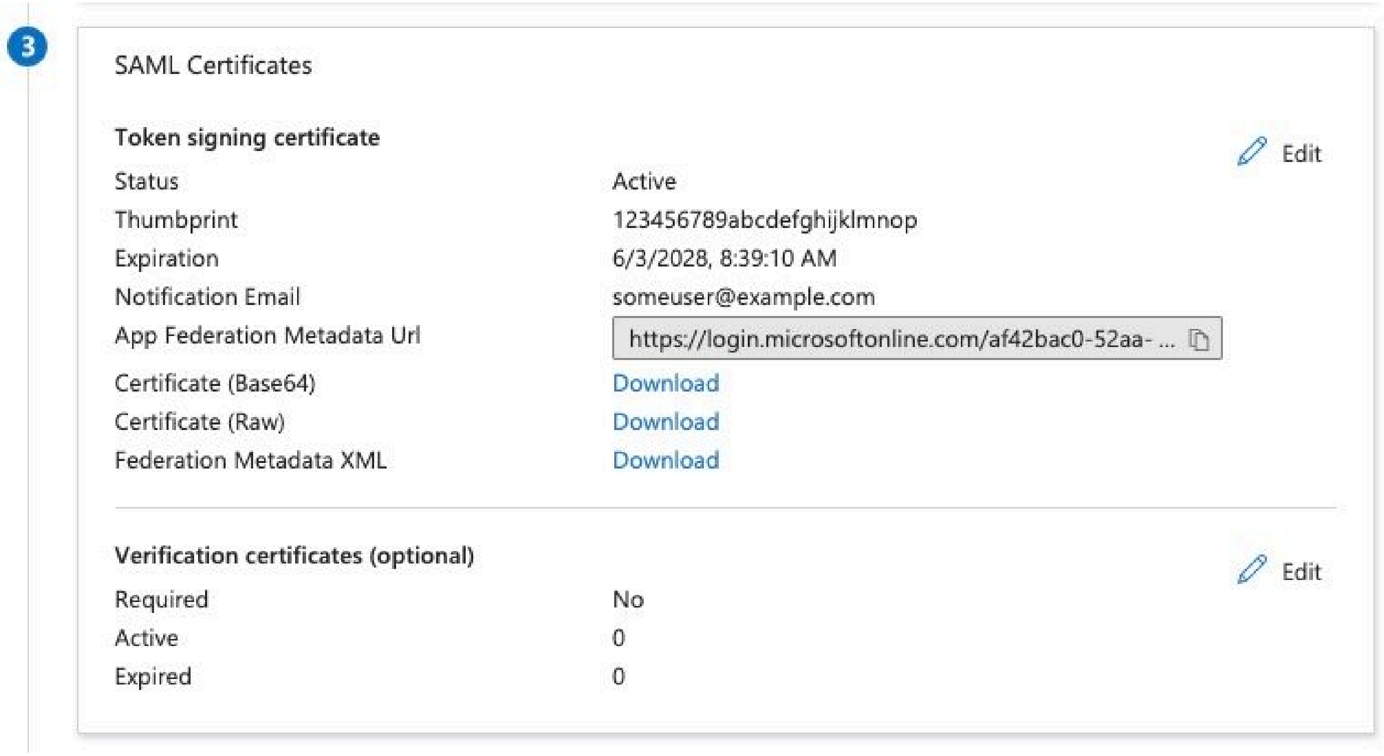
Reply URL (Assertion Consumer Service URL) *

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

12. Locate the **SAML Certificates** card and save the **App Federation Metadata URL** field value and download the **Federation Metadata XML**.



SAML Certificates

Token signing certificate

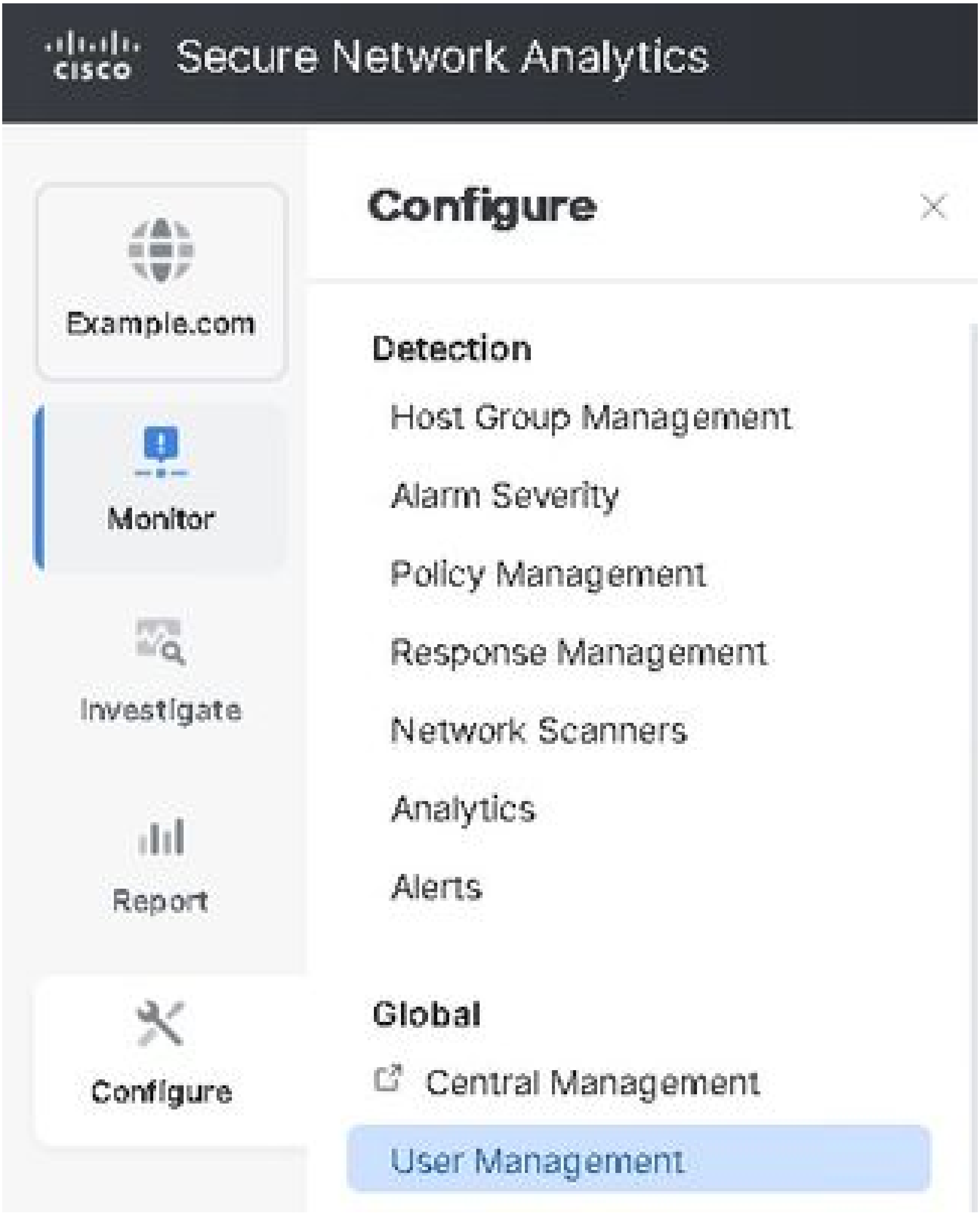
Status	Active
Thumbprint	123456789abcdefghijklmnop
Expiration	6/3/2028, 8:39:10 AM
Notification Email	someuser@example.com
App Federation Metadata Url	https://login.microsoftonline.com/af42bac0-52aa- ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

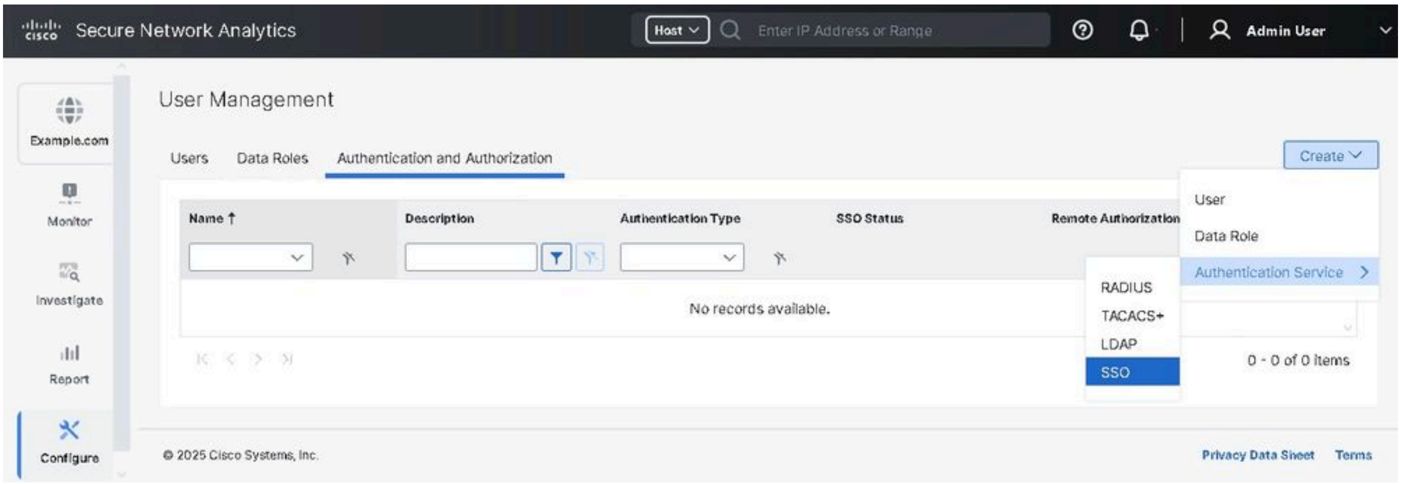
Required	No
Active	0
Expired	0

Configure and Download Service Provider XML File in SNA

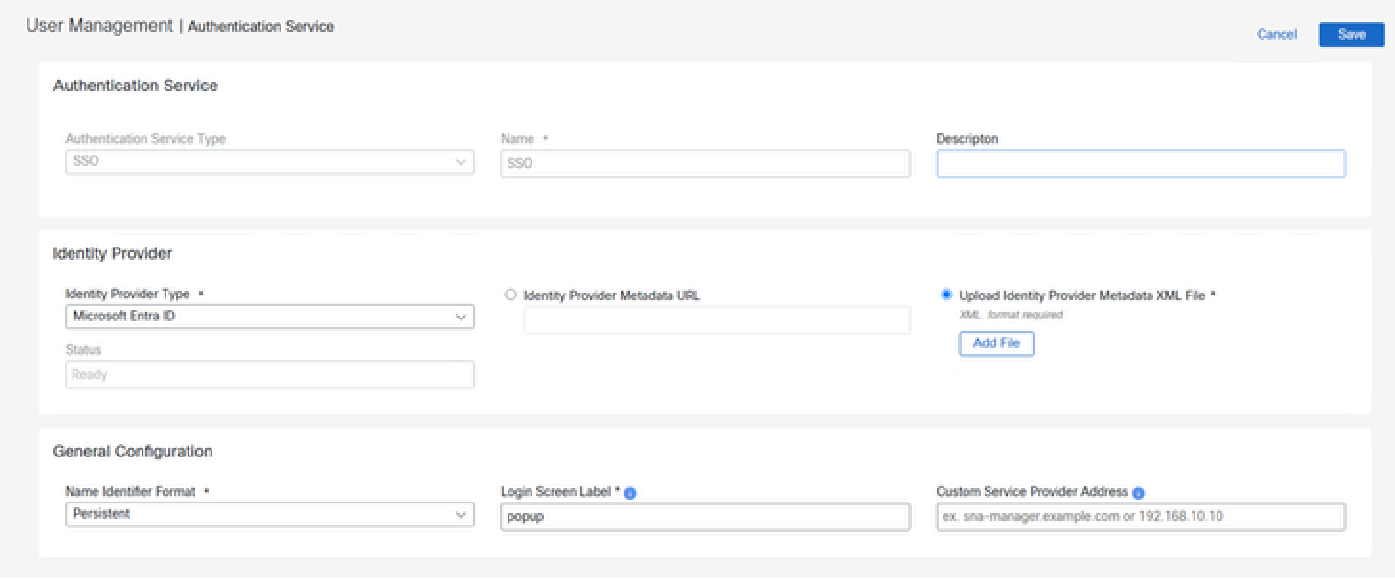
1. Log in to the **SNA Manager UI**.
2. Navigate to **Configure > Global > User Management**.



3. Under **Authentication and Authorization** tab click **Create > Authentication Service > SSO**.



4. Select the appropriate radio button for **Identity Provider Metadata URL** or **Upload Identity Provider Metadata XML File**.



Authentication Service

Authentication Service Type: SSO

Name *: SSO

Descripton:

Identity Provider

Identity Provider Type *: Microsoft Entra ID

Status: Ready

○ Identity Provider Metadata URL

● Upload Identity Provider Metadata XML File *

XML format required

General Configuration

Name Identifier Format *: Persistent

Login Screen Label *: popup

Custom Service Provider Address: ex. sna-manager.example.com or 192.168.10.10

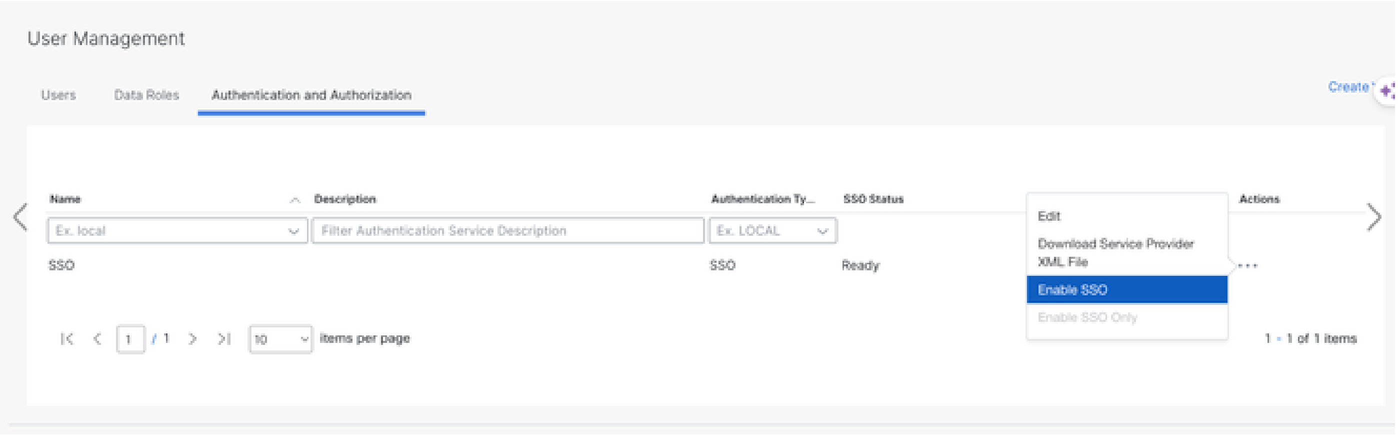
Note: In this demo Upload Identity Provider Metadata XML File is selected.

5. Configure **Identity Provider Type field** to **Microsoft Entra ID**, **Name Identifier Format** to **Persistent**, Type a **Login Screen Label**.

Tip: Configured Login Screen label (name/text) shows above the Login In with SSO button and should not be left empty.

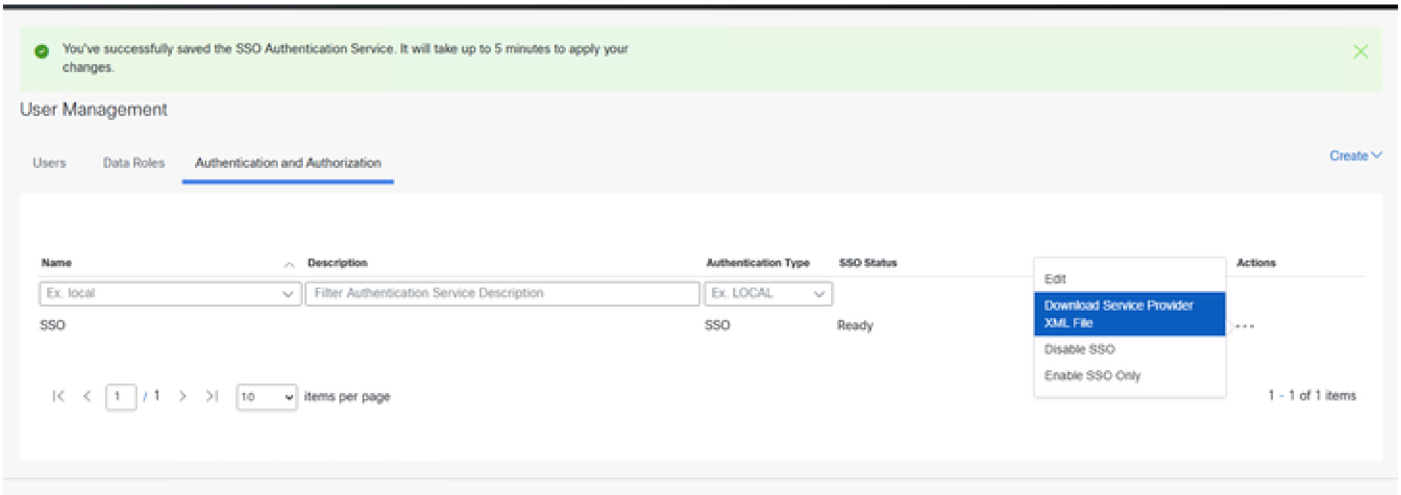
6. Click **Save** which returns you back to Authentication and Authorization tab.

7. Wait for the status to be **READY** and select **Enable SSO** from the action menu.



Name	Description	Authentication Ty...	SSO Status	Actions
Ex. local	Filter Authentication Service Description	Ex. LOCAL		
SSO		SSO	Ready	...

8. Under **Authentication and Authorization** tab click on **the three dots** in the **Actions** column and click **Download Service Provider XML File**.


You've successfully saved the SSO Authentication Service. It will take up to 5 minutes to apply your changes.

Name	Description	Authentication Type	SSO Status	Actions
Ex. local	Filter Authentication Service Description	Ex. LOCAL		
SSO		SSO	Ready	...

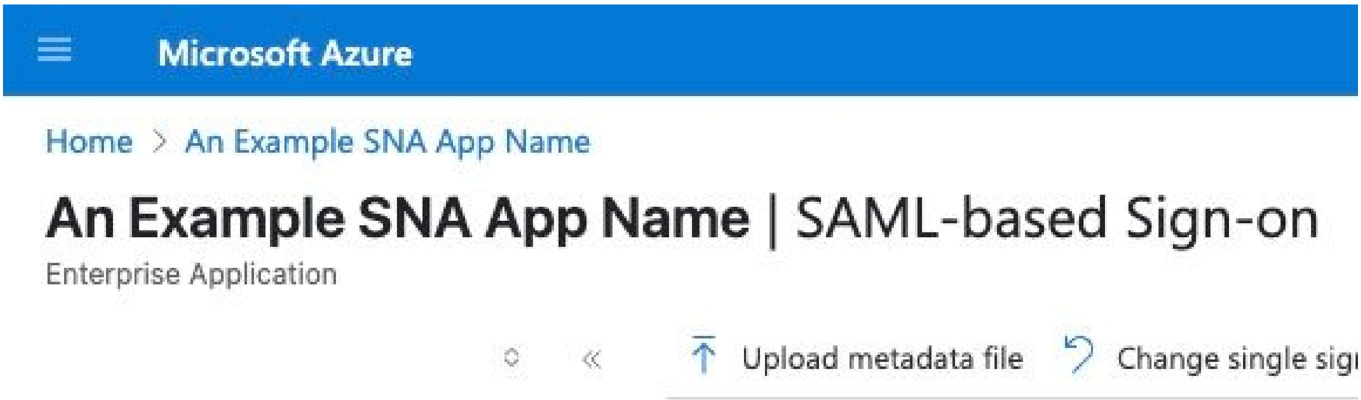
Configure SSO in Azure

1. Log in to [Azure portal]().

2. From the search bar navigate to **Enterprise Application > Select configured Enterprise Application > Click setup single sign on**.

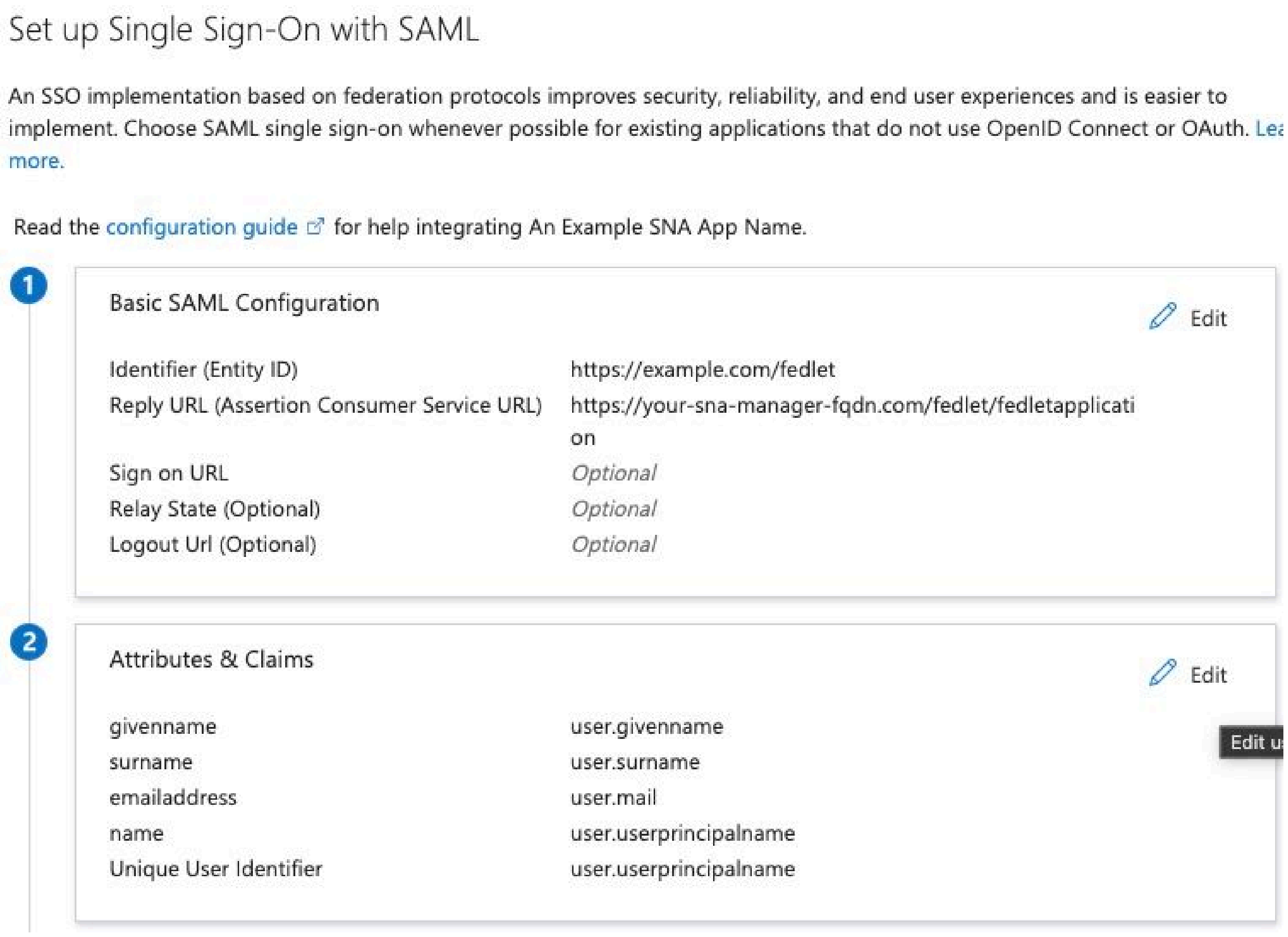
3. Click **Upload metadata file** at the top of the page and upload the sp.xml file downloaded from SNA Manager.

4. It opens "Basic SAML Configuration" screen and set various settings to correct values, Click **Save.**


Microsoft Azure
Home > An Example SNA App Name
An Example SNA App Name | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sig

Note: Ensure the Name ID Format in Entra ID is correct.

5. Locate **Attributes & Claims** section and click **Edit**.



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. Lea more.

Read the configuration guide for help integrating An Example SNA App Name.

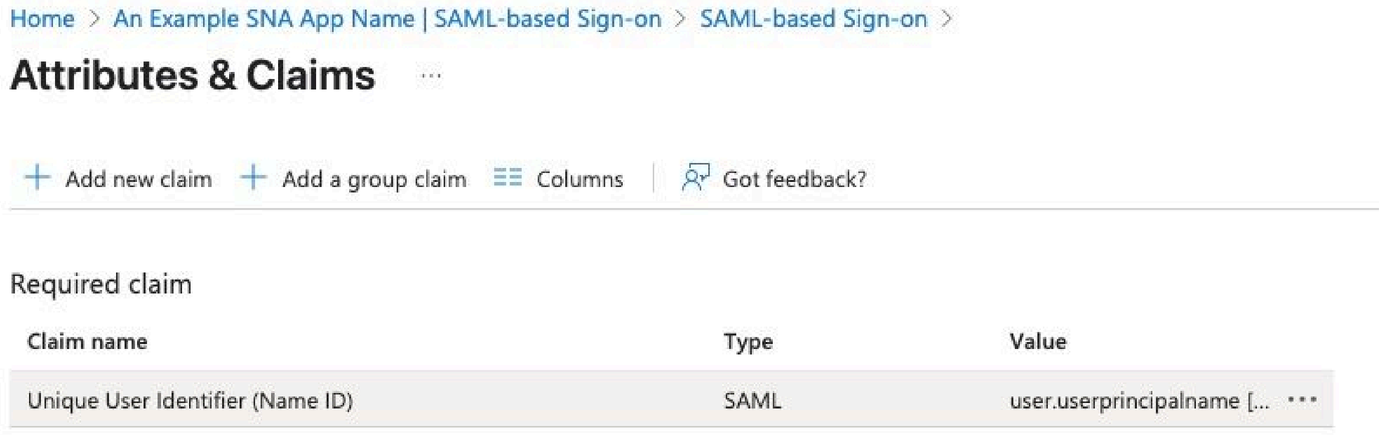
1 Basic SAML Configuration — Edit

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. Click **user.userprincipalname** value under **Claim Name** section.



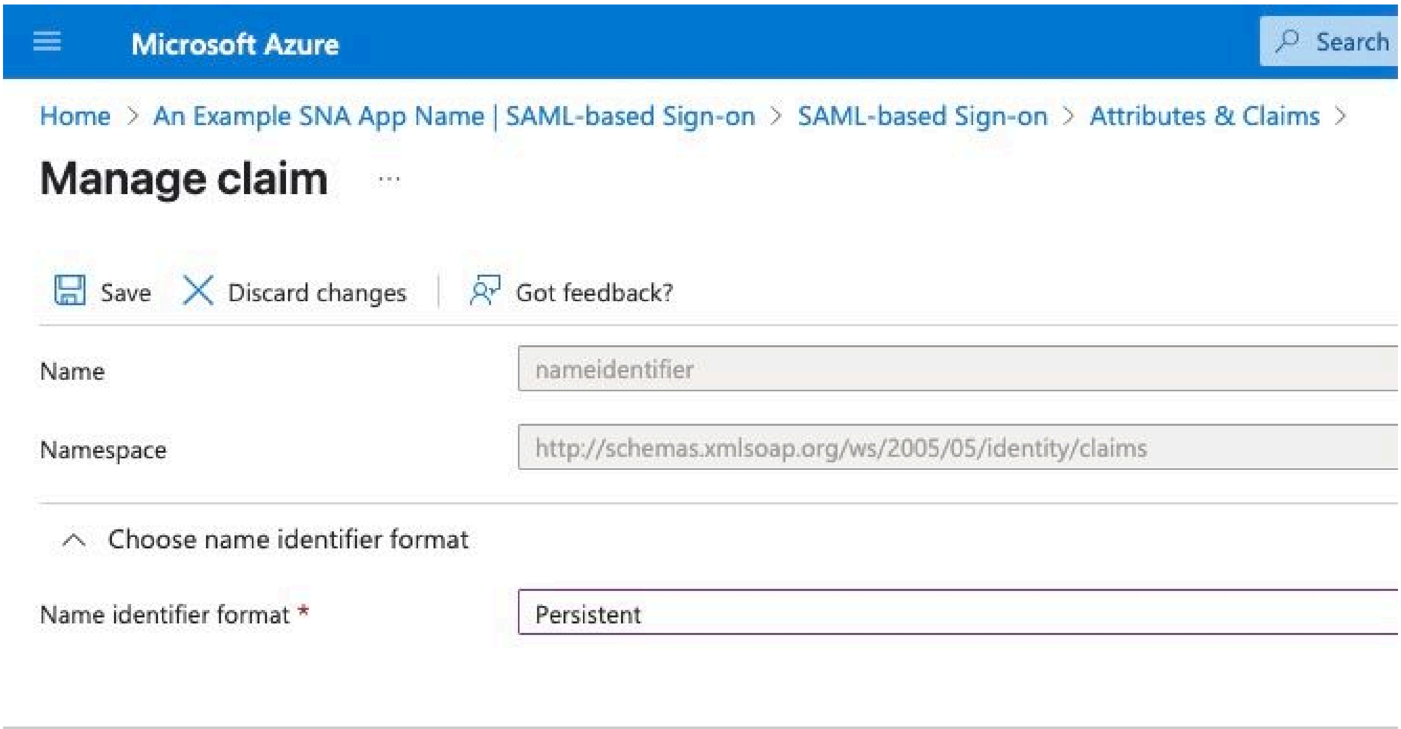
Home > An Example SNA App Name | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims ...

Required claim

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

7. Under **Manage Claim page** Verify **Choose name identifier format**.



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

Manage claim ...

Name: nameidentifier

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

Choose name identifier format

Name identifier format *: Persistent

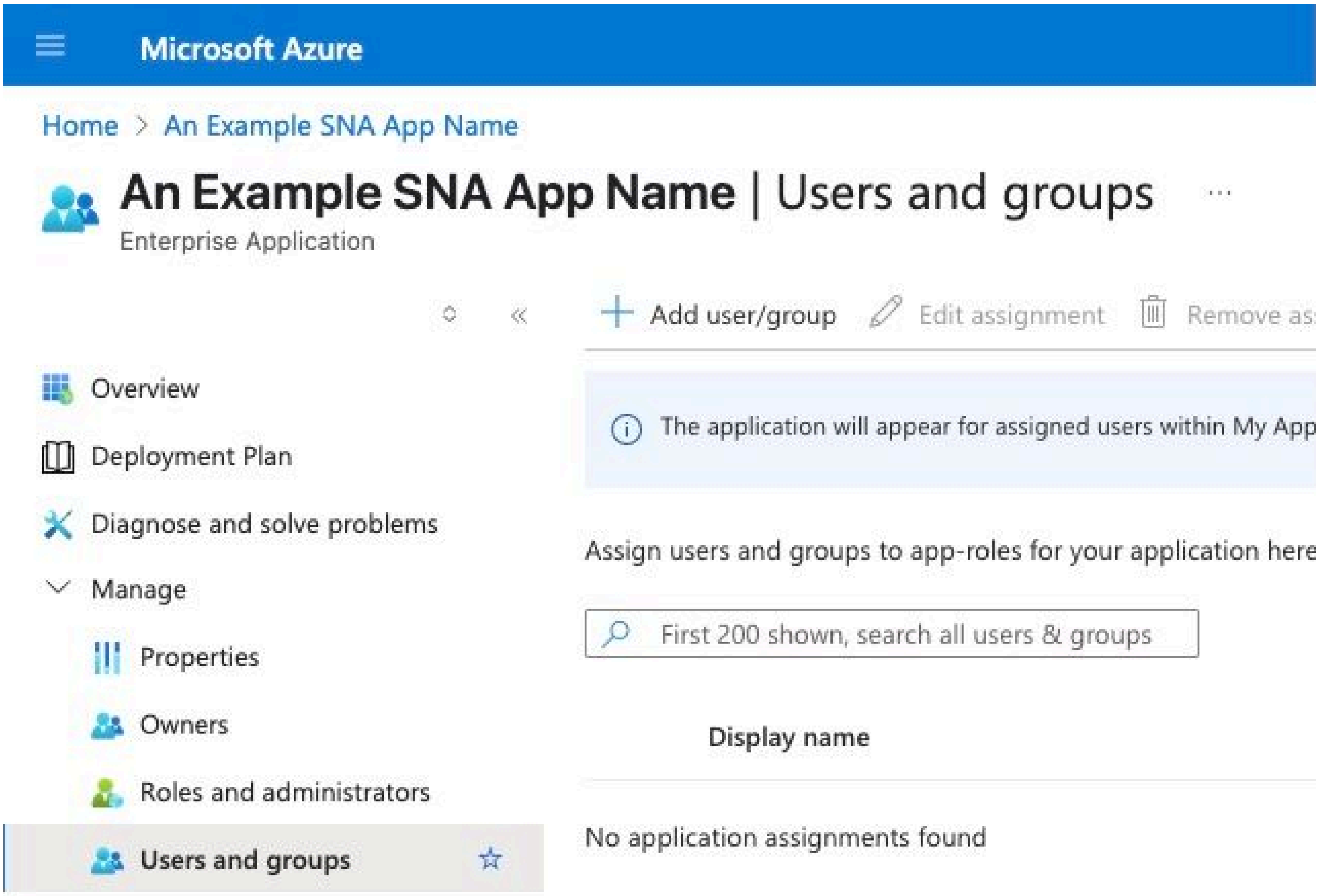
Note: Name identifier format field is set to Persistent if not then select it from the drop down menu. Click save if changes were made.

Caution: This is the most common place to encounter issues. The settings on the SNA Manager and Microsoft Azure must match. if you opted to use the "emailAddress" format in SNA, the format here must also be "Email Address.

Setup Users in Entra ID.

1. Log in to **Azure portal**.

2. From the search bar navigate to the **Enterprise Application > Select configured Enterprise Application > select Users and Groups on the left > click Add user/group.**


Microsoft Azure

Home > An Example SNA App Name

An Example SNA App Name | Users and groups ...

Enterprise Application

The application will appear for assigned users within My App

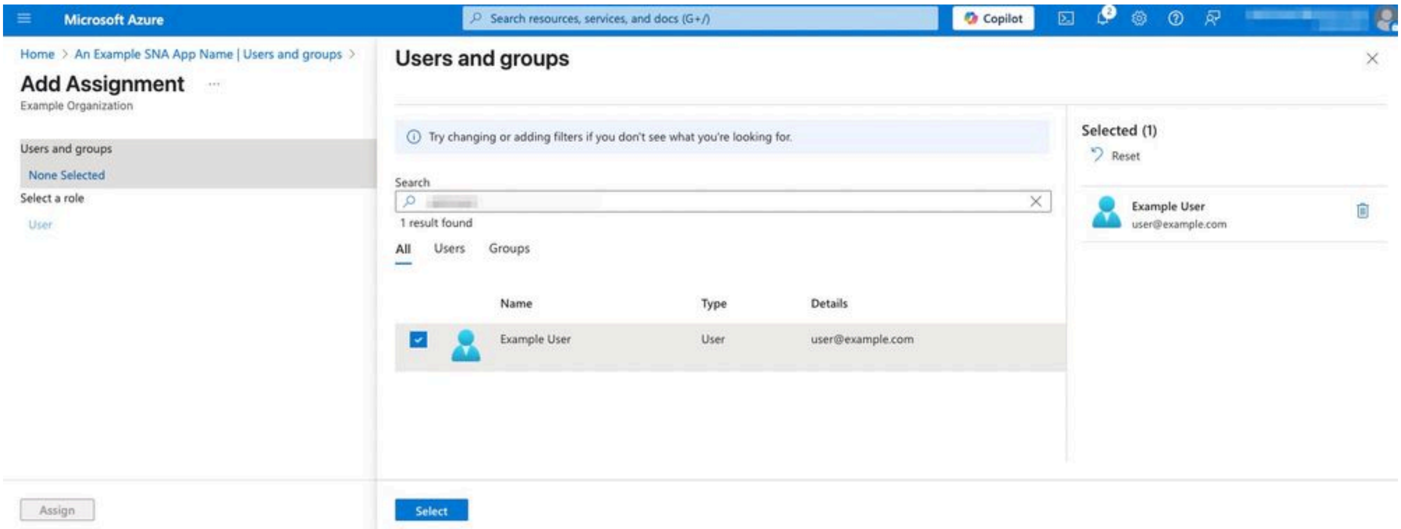
Assign users and groups to app-roles for your application here

First 200 shown, search all users & groups

Display name
No application assignments found

3. In the left pane click **None Selected.**

4. Search and add required user to the application.


Microsoft Azure

Search resources, services, and docs (G+/)

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

Add Assignment ...

Example Organization

Users and groups

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

Search

[redacted]

1 result found

All Users Groups

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

Selected (1)

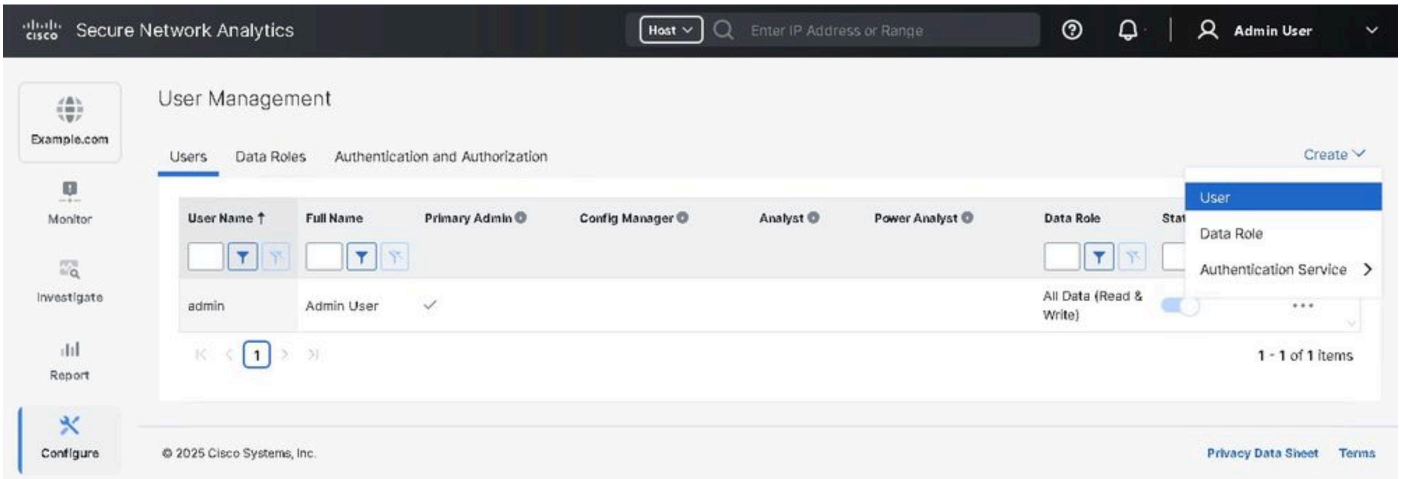
Example User
user@example.com

Configure SSO in SNA

1. Log in to the **SNA Manager UI**.

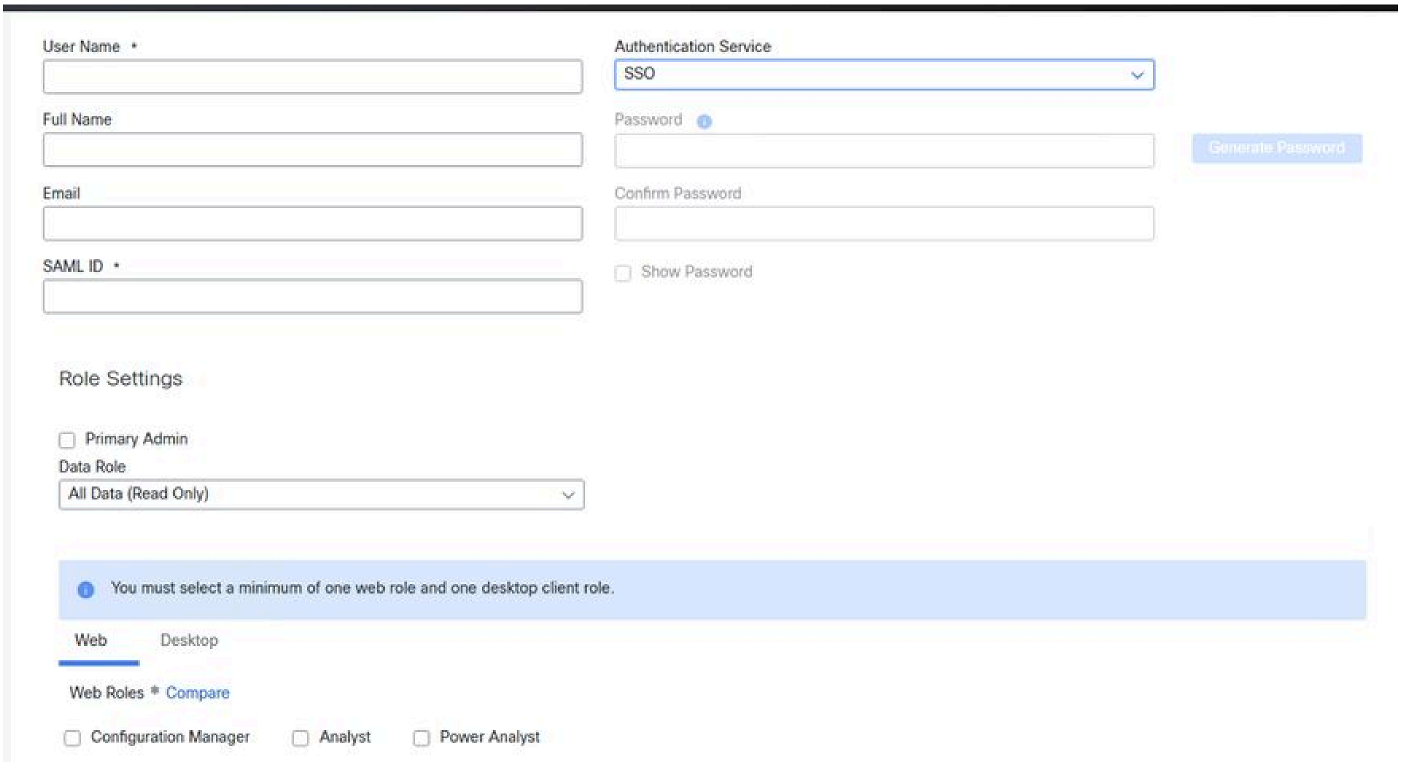
2. Navigate to **Configure > Global > User Management.**

3. Click **Create > User**.



User Name	Full Name	Primary Admin	Config Manager	Analyst	Power Analyst	Data Role	Stat
admin	Admin User	✓				All Data (Read & Write)	

4. Configure user by providing associated details with **Authentication service selected** as **SSO** and click **Save**.



Authentication Service: SSO

Data Role: All Data (Read Only)

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

SAML-User creation in SNA-UI

Troubleshoot

If users are unable to login to the SNA Manager, a SAML tracer can be used to investigate further.

If further assistance is needed investigating the SNA Manager a TAC Case can be raised.

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