

Configuración de SNA Manager para Microsoft Entra ID SSO

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Configurar aplicación empresarial en Azure](#)

[Configuración y descarga del archivo XML del proveedor de servicios en SNA](#)

[Configurar SSO en Azure](#)

[Configuración de usuarios en ID de entrada.](#)

[Configuración de SSO en SNA](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Secure Network Analytics (SNA) para utilizar Microsoft Entra ID para el inicio de sesión único (SSO).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Microsoft Azure
- Secure Network Analytics

Componentes Utilizados

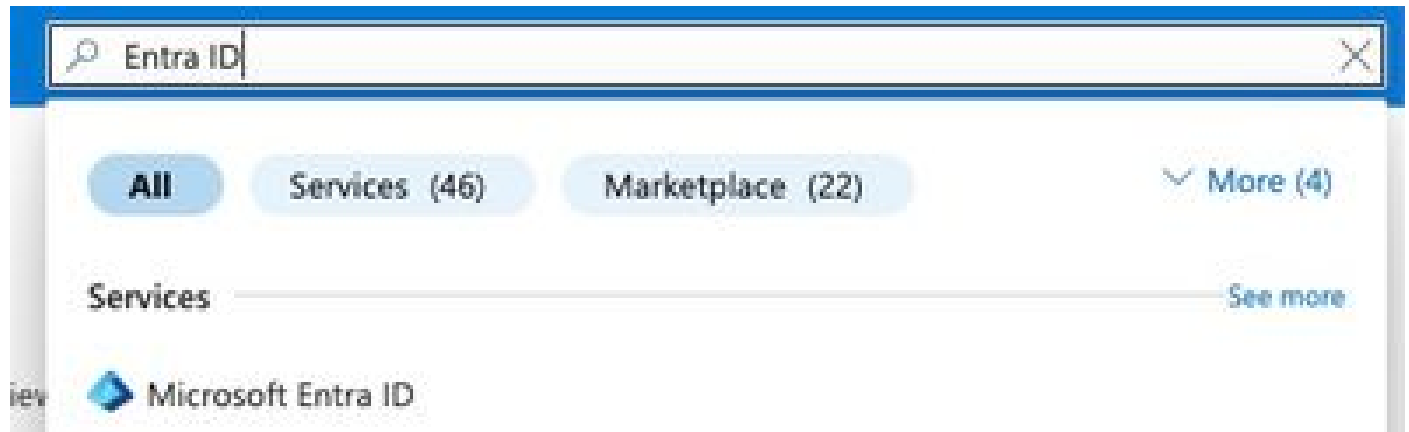
- Administrador SNA v7.5.2
- ID de Microsoft Entra

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

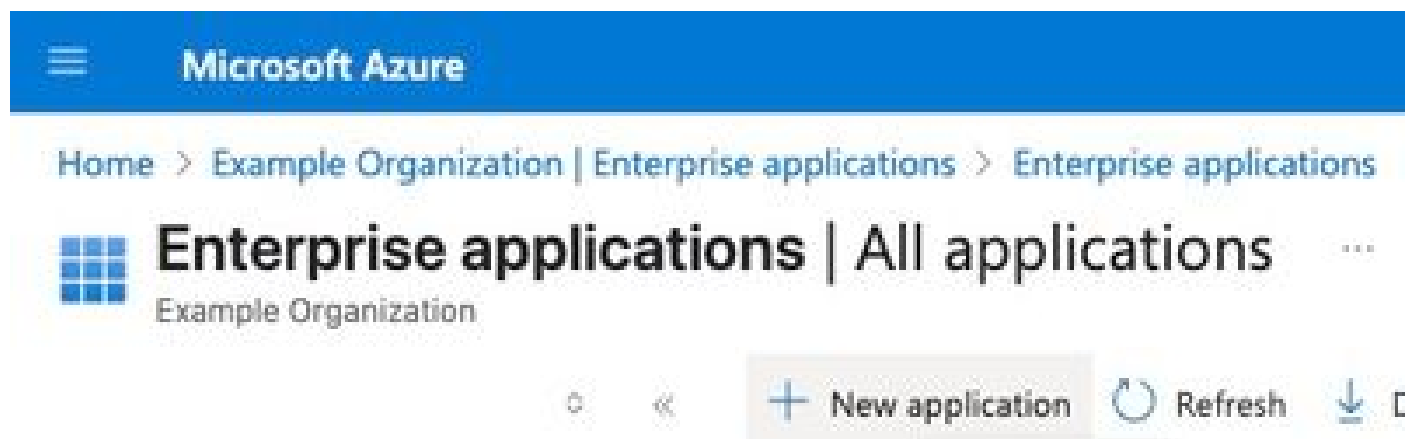
Configuration Steps

Configurar aplicación empresarial en Azure

1. Inicie sesión en el [portal de nube de Azure](#).
2. Busque el servicio Entra ID en el cuadro de búsqueda y seleccione Microsoft Entra ID.



3. En el panel izquierdo, expanda Administrar y seleccione Aplicaciones de empresa.
4. Haga clic en Nueva aplicación.



5. Seleccione Crear su propia aplicación en la nueva página que se carga.



[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

- Proporcione un nombre a la aplicación en ¿Cuál es el nombre de su aplicación? campo.
- Seleccione el botón de opción Integrar cualquier otra aplicación que no encuentre en la galería (No galería) y haga clic en Crear.

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. En el panel de aplicaciones recién configurado, haga clic en Configurar inicio de sesión único.



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. Selección SAML.

An Example SNA App Name | Single sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user's 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. En la página Configurar el inicio de sesión único con SAML, haga clic en Editar en Configuración básica de SAML.

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	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

11. En el panel Configuración básica de SAML, configure Agregar URL de respuesta en <https://example.com/fedlet/fedletapplication> reemplazando example.com con FQDN del Administrador SNA y haga clic en guardar.

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. Localice la tarjeta de certificados SAML y guarde el valor del campo URL de metadatos de federación de aplicaciones y descargue el XML de metadatos de federación.

3

SAML Certificates

Token signing certificate

Edit

Status

Active

Thumbprint

123456789abcdefghijklmnopqrstuvwxyz

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

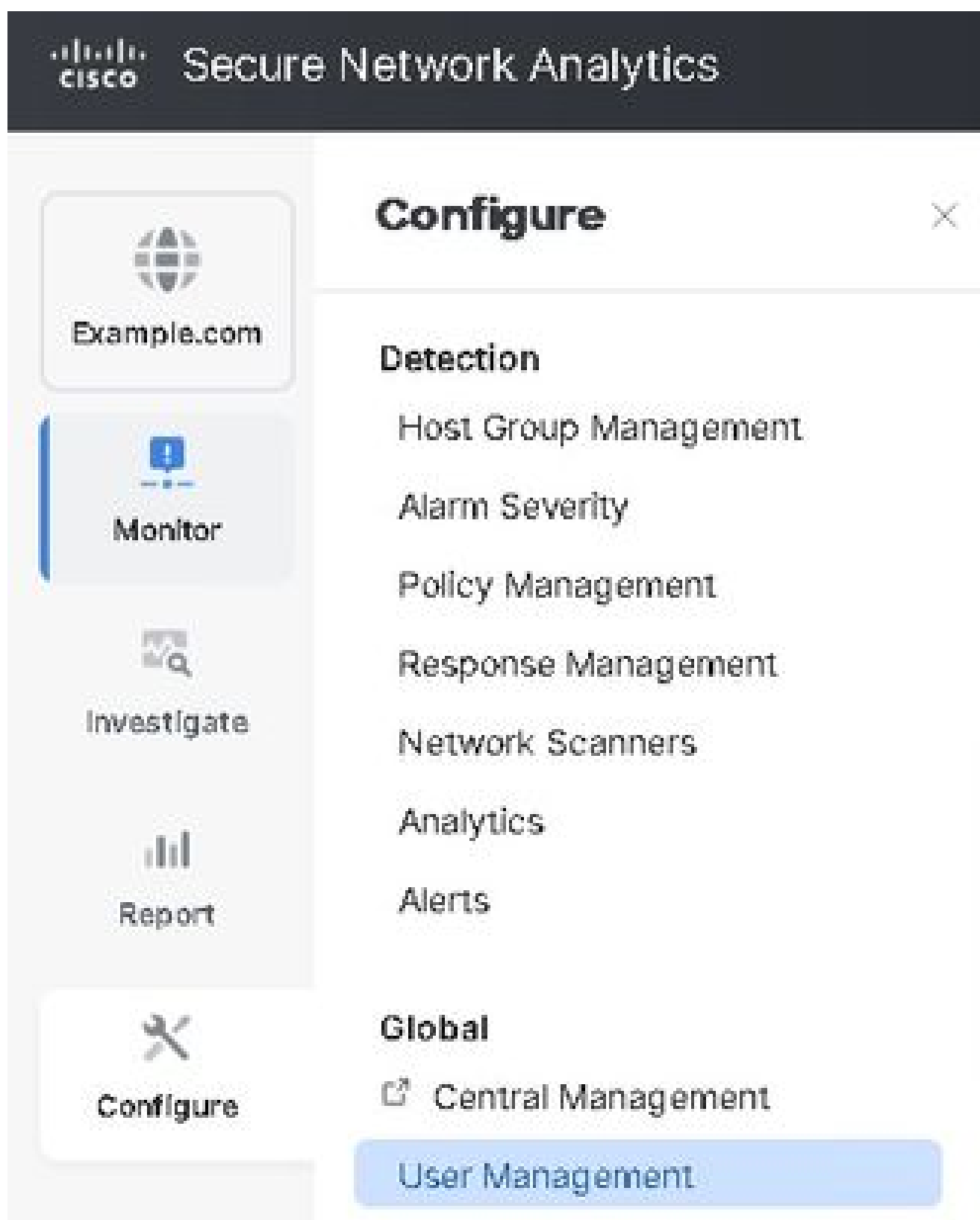
0

Expired

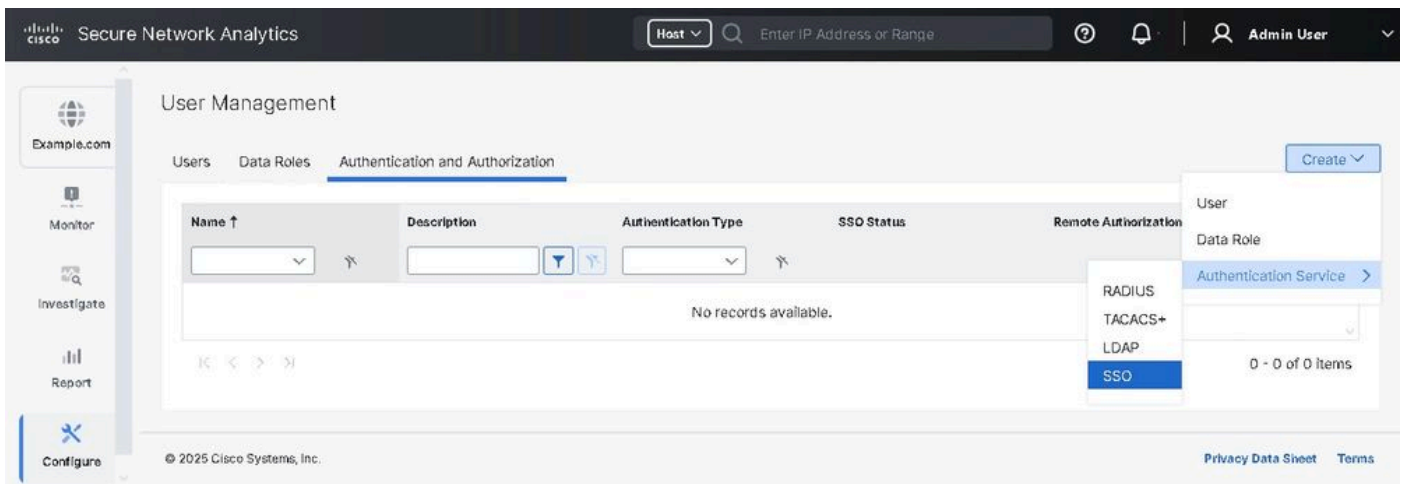
0

Configuración y descarga del archivo XML del proveedor de servicios en SNA

1. Inicie sesión en la interfaz de usuario del administrador SNA.
2. Vaya a Configure > Global > User Management.



3. En la pestaña Authentication and Authorization, haga clic en Create > Authentication Service > SSO.



4. Seleccione el botón de opción correspondiente a URL de metadatos del proveedor de identidad o Cargar archivo XML de metadatos del proveedor de identidad.

User Management | Authentication Service Cancel Save

Authentication Service

Authentication Service Type: SSO Name: SSO Description:

Identity Provider

Identity Provider Type: Microsoft Entra ID

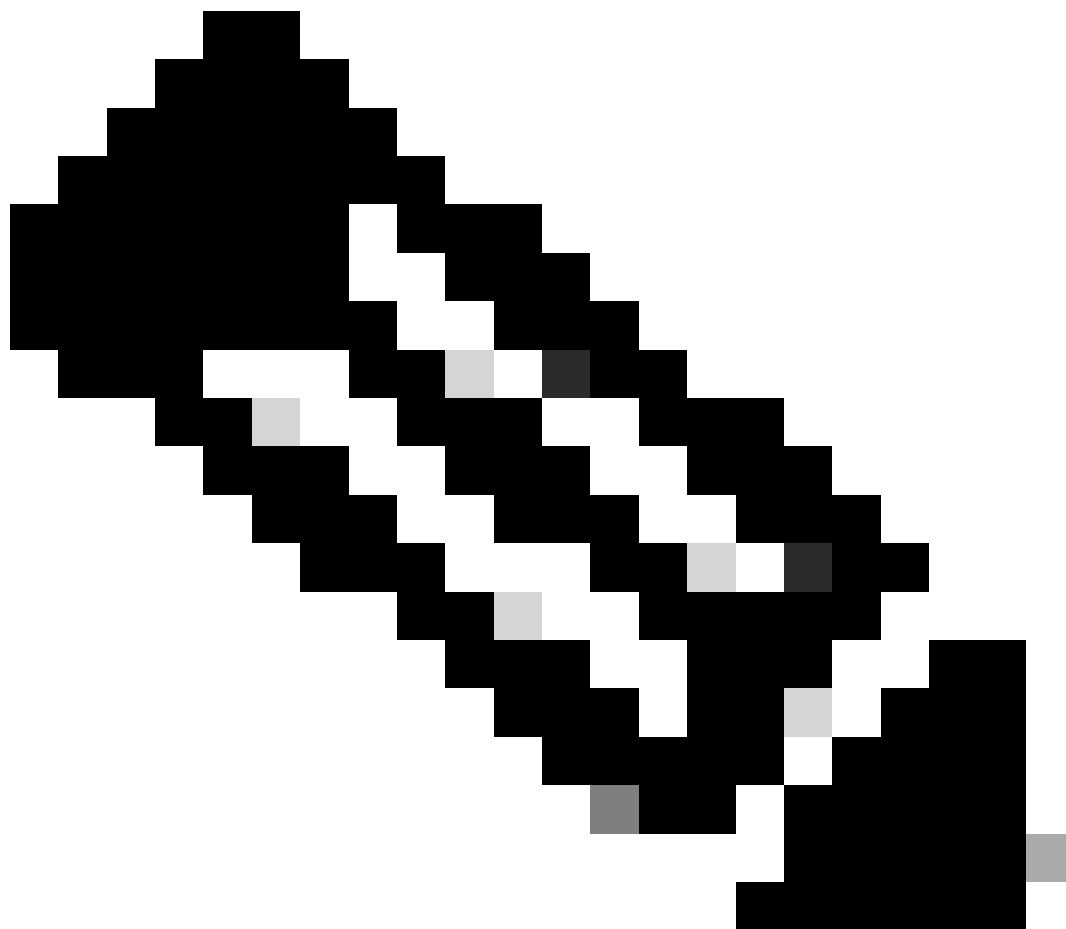
Status: Ready

☐ Identity Provider Metadata URL

☒ Upload Identity Provider Metadata XML File *
XML format required Add File

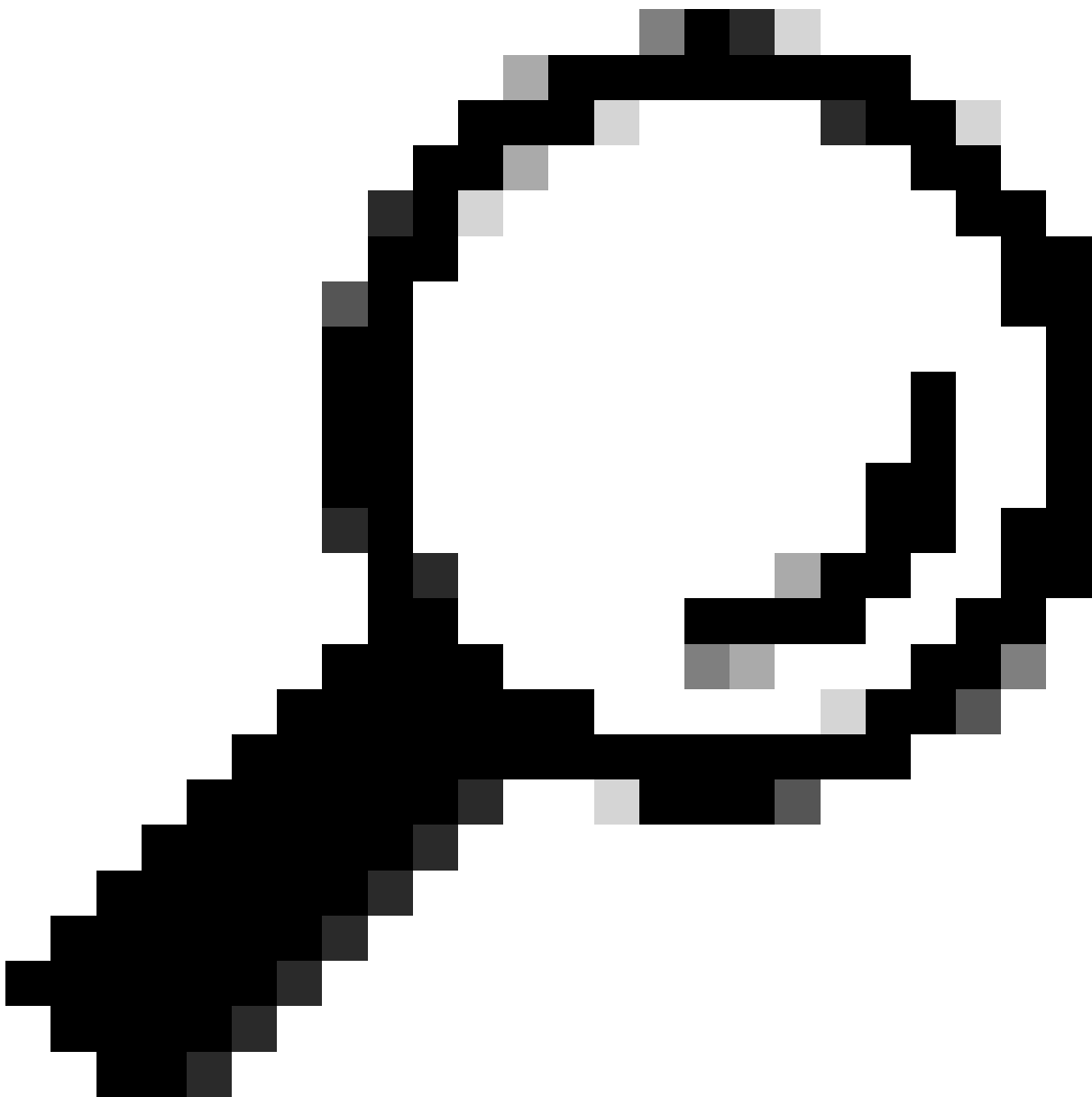
General Configuration

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



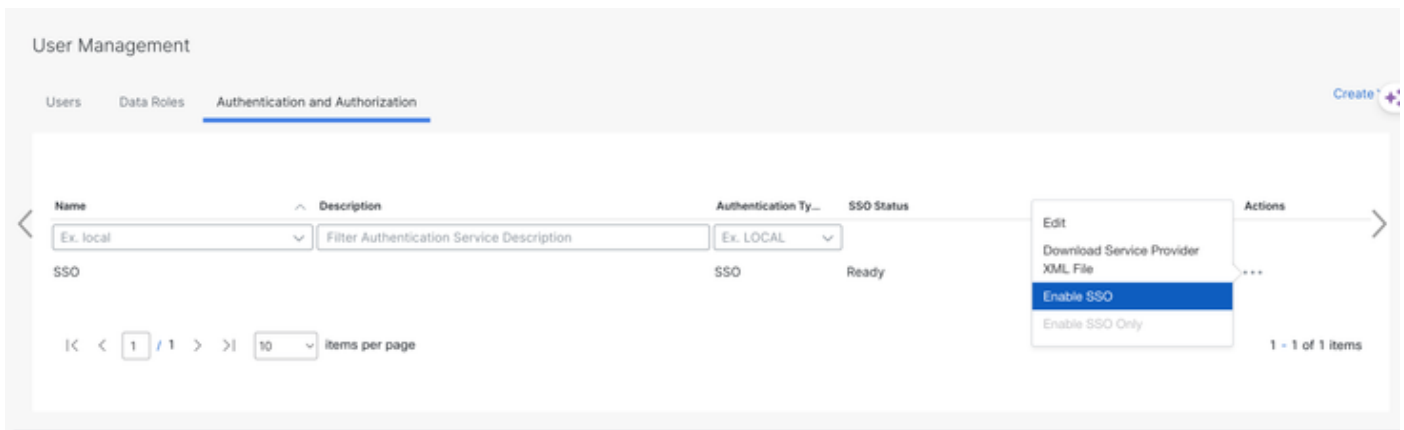
Nota: En esta demostración se ha seleccionado Cargar archivo XML de metadatos del proveedor de identidad.

5. Configure el campo Tipo de proveedor de identidad a Microsoft Entry ID, Name Identifier Format a Persistent, Escriba una etiqueta de pantalla de inicio de sesión.

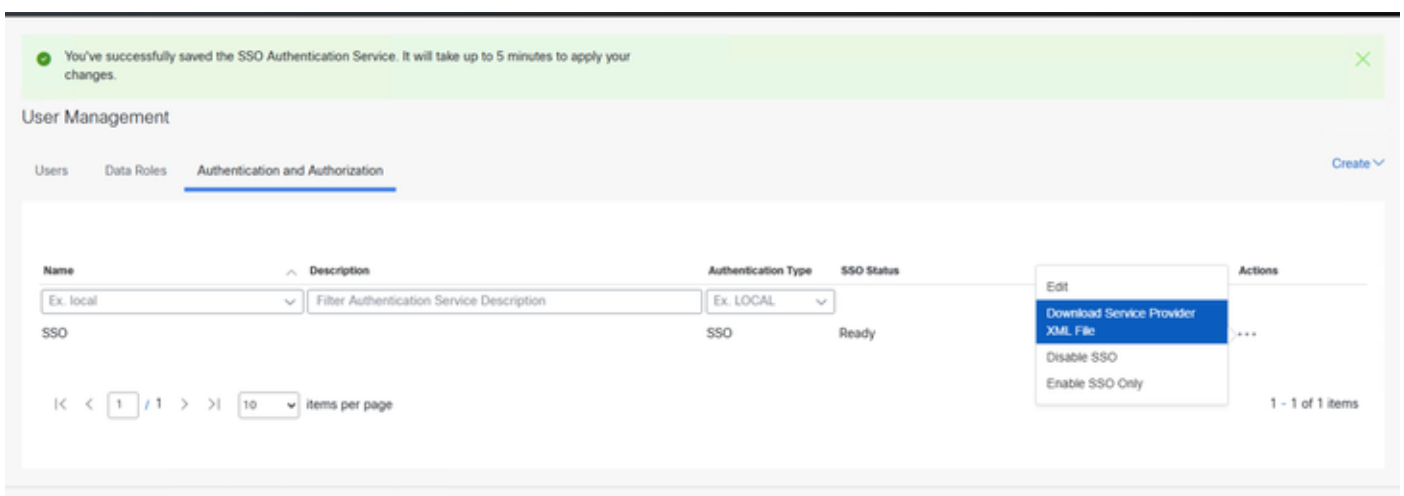


Consejo: La etiqueta de la pantalla de inicio de sesión configurada (nombre/texto) se muestra encima del botón Iniciar sesión con SSO y no debe dejarse vacía.

-
6. Haga clic en Guardar para volver a la pestaña Autenticación y Autorización.
 7. Espere a que el estado sea READY y seleccione Enable SSO en el menú de acción.



8. En la pestaña Authentication and Authorization, haga clic en los tres puntos de la columna Actions y haga clic en Download Service Provider XML File.



Configurar SSO en Azure

1. Inicie sesión en el [portal de Azure](#).
2. En la barra de búsqueda, acceda a Aplicación de Empresa > Seleccionar aplicación de empresa configurada > Hacer clic en configurar inicio de sesión único.
3. Haga clic en Cargar archivo de metadatos en la parte superior de la página y cargue el archivo sp.xml descargado desde el Administrador SNA.
4. Se abre la pantalla "Basic SAML Configuration" y establece varios ajustes para corregir los valores, haga clic en Guardar.



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

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

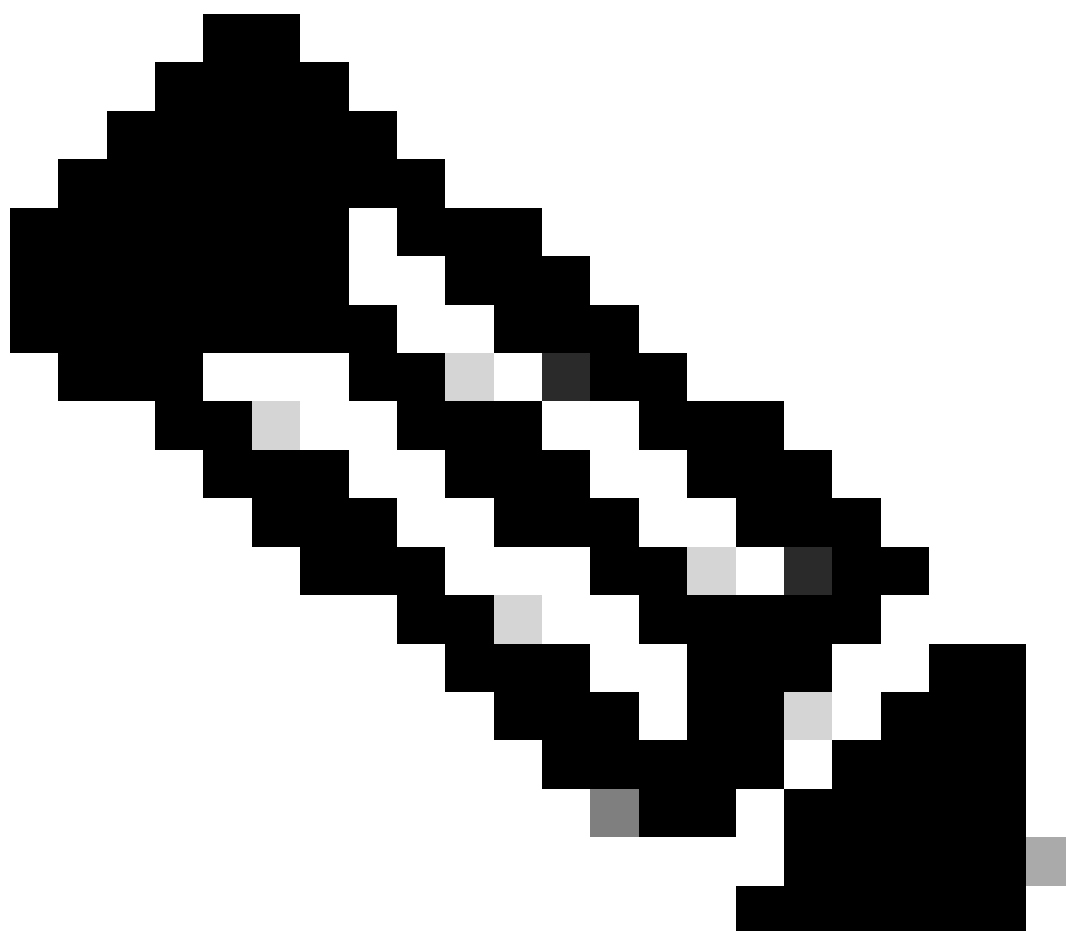
Enterprise Application



Upload metadata file



Change single sign-on



Nota: Asegúrese de que el formato de ID de nombre en ID de entrada es correcto.

5. Localice la sección Atributos y reclamaciones y haga clic en Editar.

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/fedletapplicati on
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. Haga clic en el valor user.userprincipalname en la sección Nombre de reclamación.

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. En la página Gestionar reclamación, compruebe Elija el formato de identificador de nombre.



Manage claim ...



Save



Discard changes



Got feedback?

Name

nameidentifier

Namespace

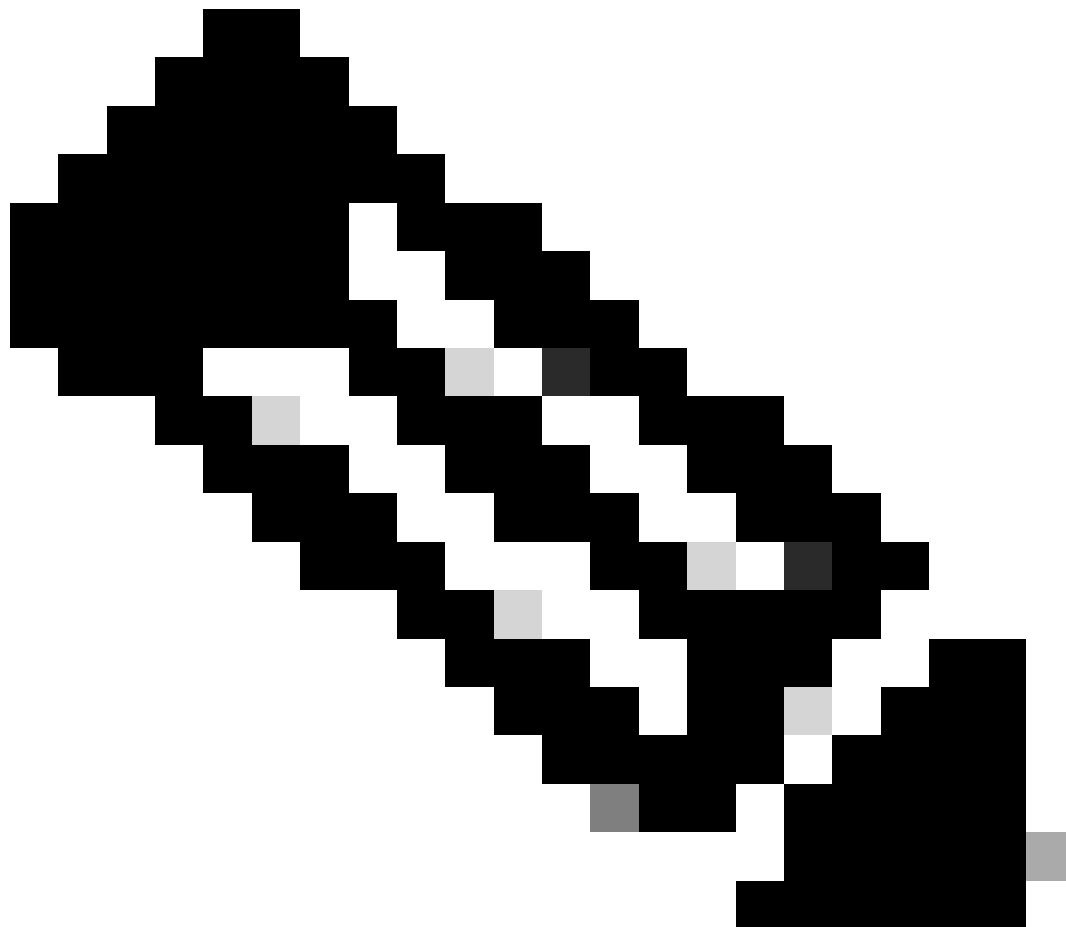
http://schemas.xmlsoap.org/ws/2005/05/identity/claims



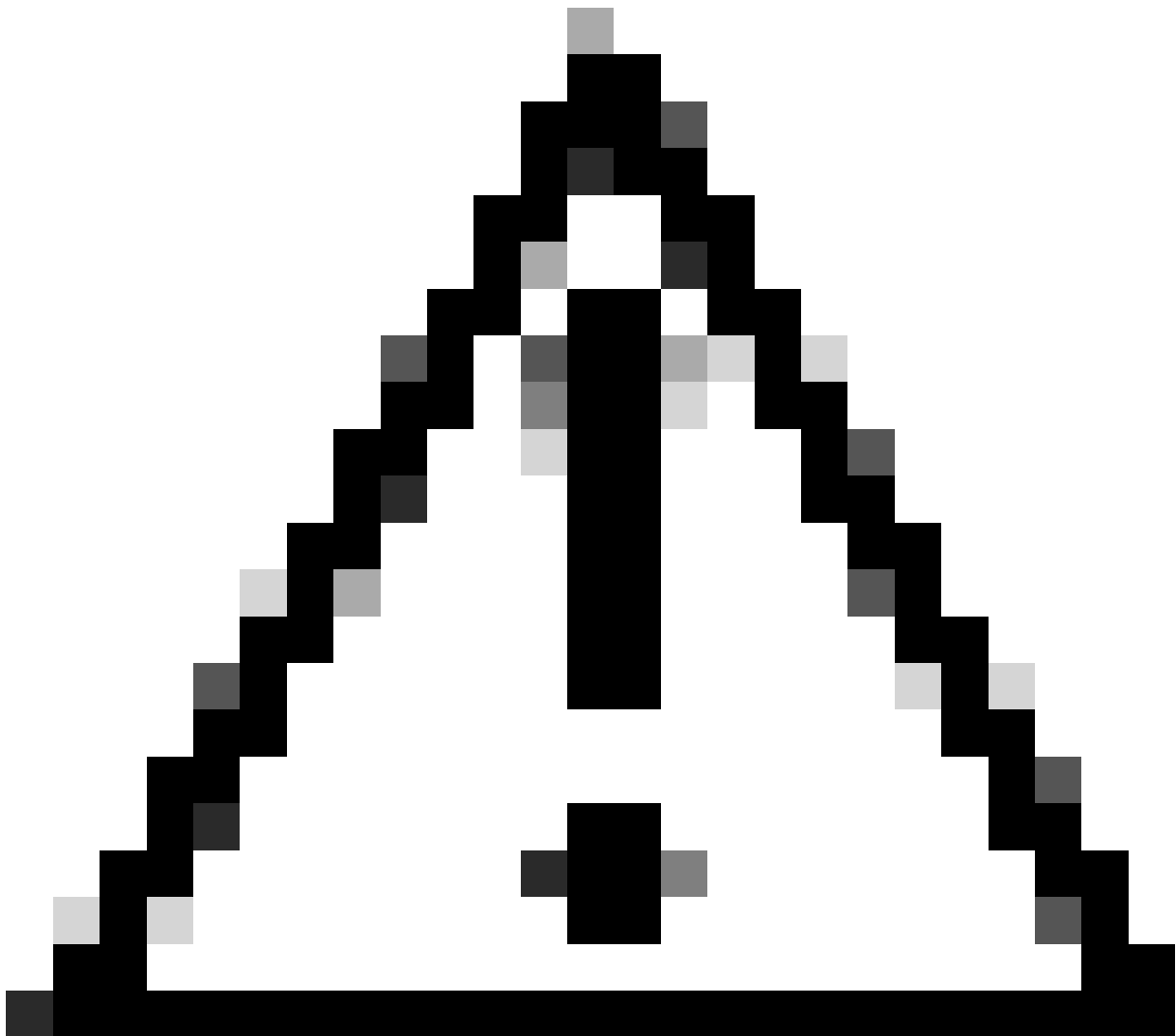
Choose name identifier format

Name identifier format *

Persistent



Nota: El campo de formato del identificador de nombre se establece en Persistente si no es así, selecciónelo en el menú desplegable. Haga clic en Guardar si se han realizado cambios.



Precaución: Este es el lugar más común para encontrar problemas. La configuración del Administrador SNA y Microsoft Azure debe coincidir. si ha optado por utilizar el formato "emailAddress" en SNA, el formato aquí también debe ser "Email Address".

Configuración de usuarios en ID de entrada.

1. Inicie sesión en el [portal de Azure](#).
2. En la barra de búsqueda, acceda a Aplicación de empresa > Seleccionar aplicación de empresa configurada > Seleccionar usuarios y grupos, a la izquierda > y haga clic en Agregar usuario/grupo.

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. En el panel izquierdo, haga clic en Ninguno seleccionado.

4. Busque y agregue el usuario necesario a la aplicación.

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

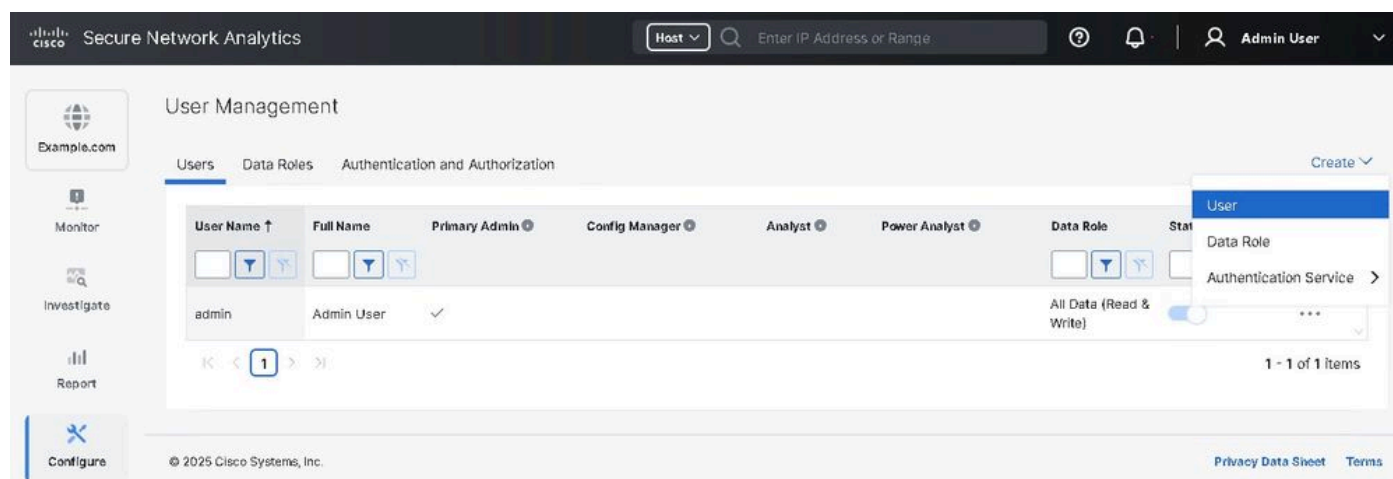
Assign Select

Configuración de SSO en SNA

1. Inicie sesión en la interfaz de usuario del administrador SNA.

2. Vaya a Configurar > Global > Administración de usuarios.

3. Haga clic en Crear > Usuario.



4. Configure el usuario proporcionando los detalles asociados con el servicio de autenticación seleccionado como SSO y haga clic en Guardar.

Creación de usuario de SAML en SNA-UI

Troubleshoot

Si los usuarios no pueden iniciar sesión en el Administrador SNA, se puede utilizar un rastreador SAML para investigar más a fondo.

Si se necesita más ayuda para investigar al administrador SNA, se puede plantear un caso TAC.

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).