

Configurar o SNA Manager para a ID do Microsoft Entra SSO

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Configurar Aplicativo Empresarial no Azure](#)

[Configurar e fazer download do arquivo XML do provedor de serviços no SNA](#)

[Configurar SSO no Azure](#)

[Configurar usuários na ID do Entra.](#)

[Configurar SSO em SNA](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar o Secure Network Analytics (SNA) para usar o Microsoft Entra ID para Single Sign On (SSO).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Microsoft Azure
- Análise de rede segura

Componentes Utilizados

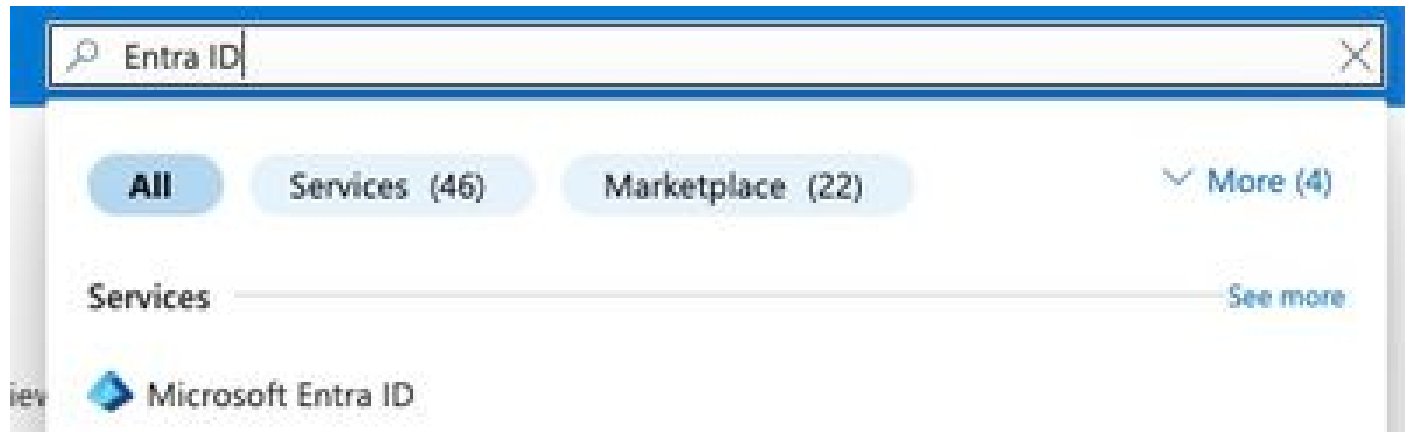
- SNA Manager v7.5.2
- ID do Microsoft Entra

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

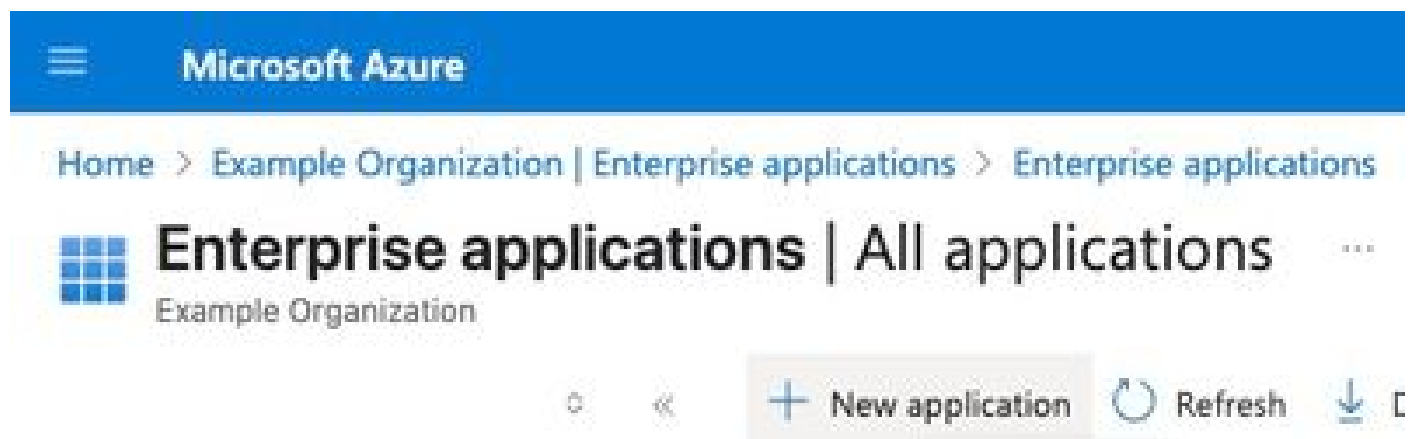
Configuration Steps

Configurar Aplicativo Empresarial no Azure

1. Faça login no [portal de nuvem do Azure](#).
2. Pesquise o serviço Entra ID na caixa de pesquisa e selecione Microsoft Entra ID.



3. No painel esquerdo, expanda Gerenciar e selecione Aplicativos corporativos.
4. Clique em Novo Aplicativo.



5. Selecione Criar Seu Próprio Aplicativo na nova página que é carregada.



[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

UI do Azure

6. Forneça um nome para o aplicativo em Qual é o nome do seu aplicativo? campo.
7. Selecione o botão de opção Integrar qualquer outro aplicativo que não esteja na galeria (Não-galeria) e clique em Criar.

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. No painel de instrumentos do aplicativo recém-configurado, clique em Configurar login 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. Selecione 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. Na página Configurar Single Sign-On com SAML, clique em Editar em Configuração SAML Básica.

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. No painel Configuração SAML básica, configure Adicionar URL de resposta para `https://example.com/fedlet/fedletapplication` substituindo `example.com` por FQDN do Gerenciador SNA e clique em 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



[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



[Add reply URL](#)

12. Localize o cartão Certificados SAML e salve o valor do campo URL de Metadados de Federação de Aplicativos e baixe o XML de Metadados de Federação.

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

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

Verification certificates (optional)

Edit

Required

No

Active

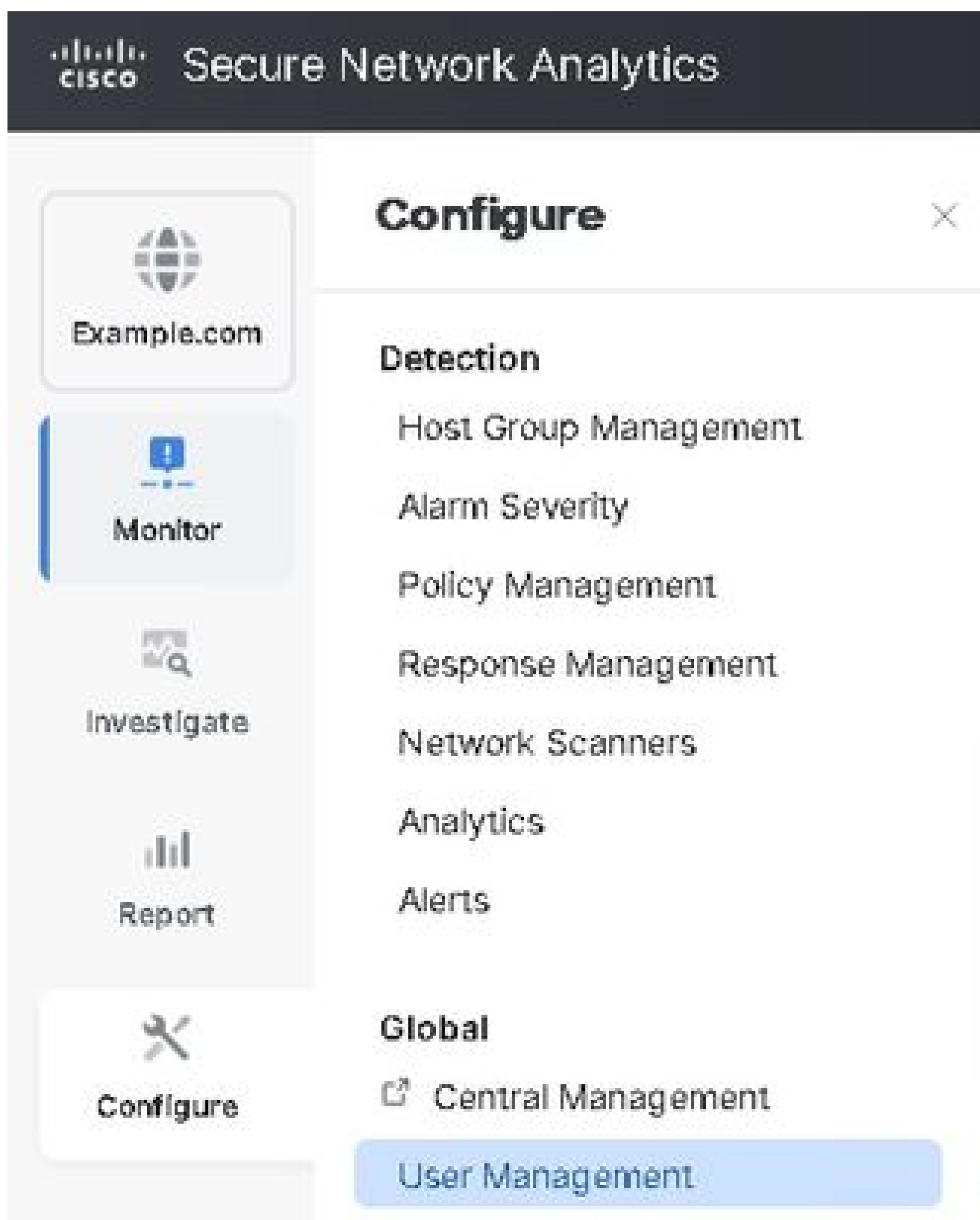
0

Expired

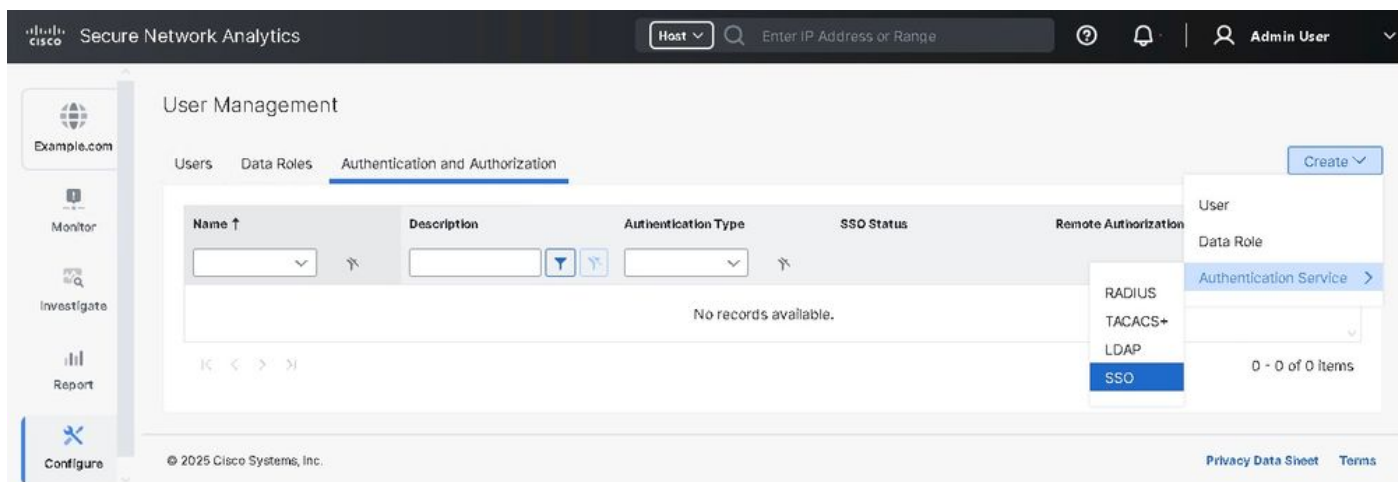
0

Configurar e fazer download do arquivo XML do provedor de serviços no SNA

1. Faça login na interface do usuário do SNA Manager.
2. Navegue até Configure > Global > User Management.



3. Na guia Authentication and Authorization, clique em Create > Authentication Service > SSO.



4. Selecione o botão de opção apropriado para URL de Metadados do Provedor de Identidade ou Carregar Arquivo XML de Metadados do Provedor de Identidade.

User Management | Authentication Service Cancel Save

Authentication Service

Authentication Service Type: SSO Name: SSO Description:

Identity Provider

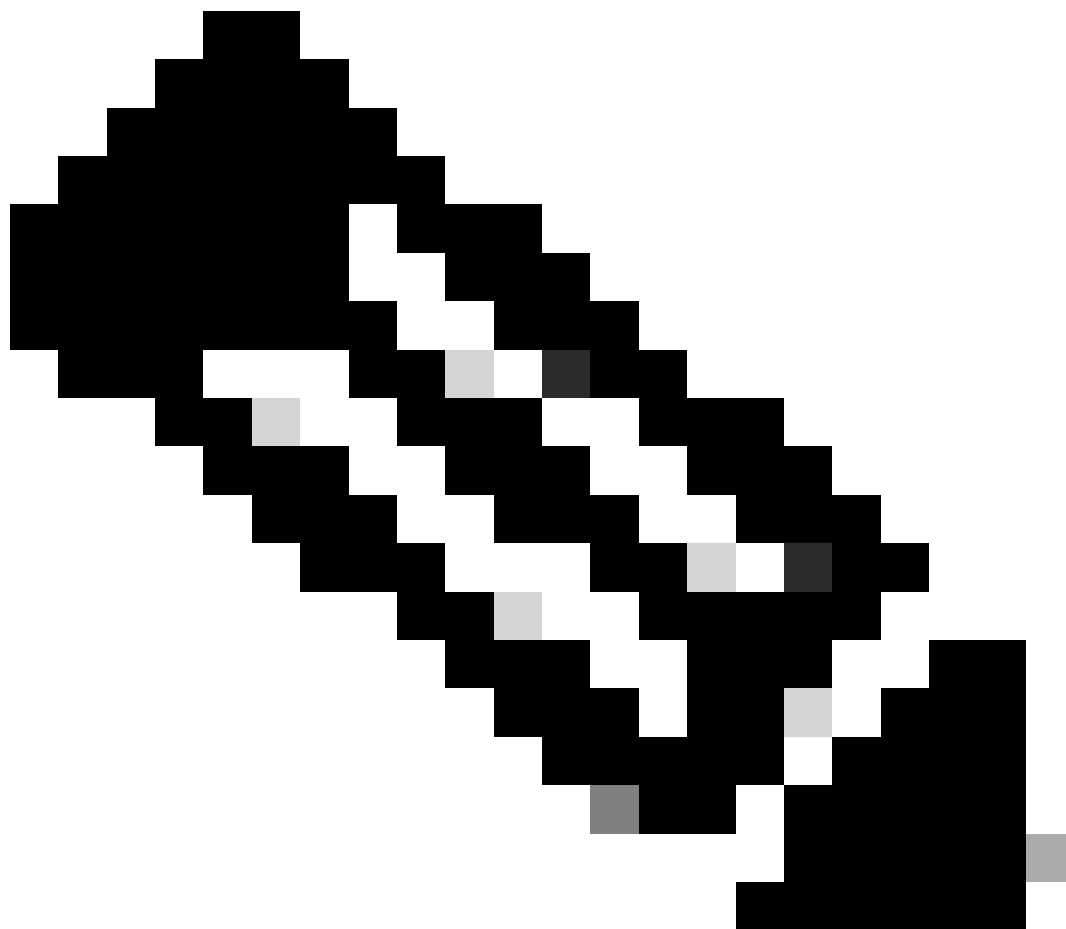
Identity Provider Type: Microsoft Entra ID

Status: Ready

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

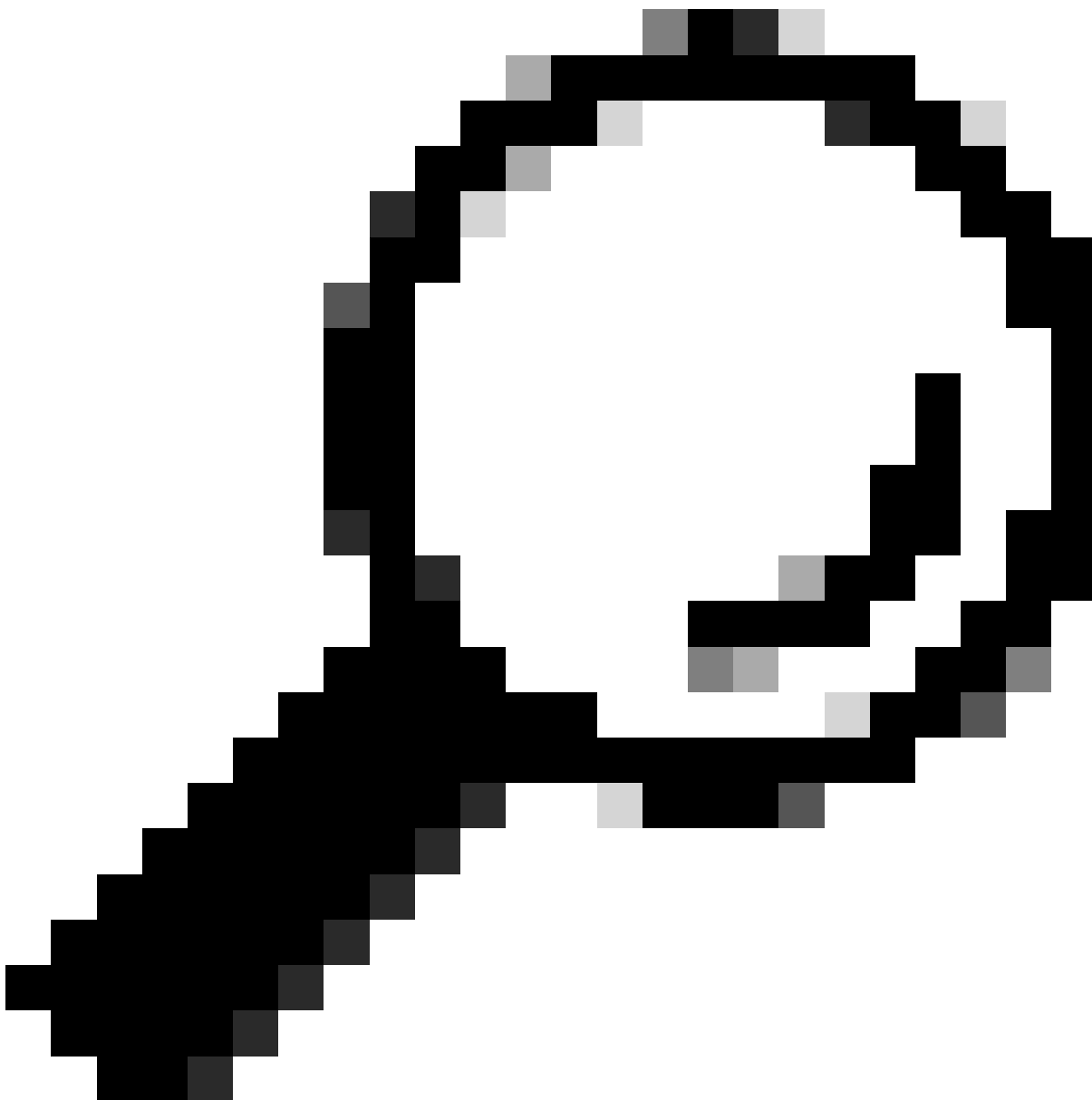
General Configuration

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



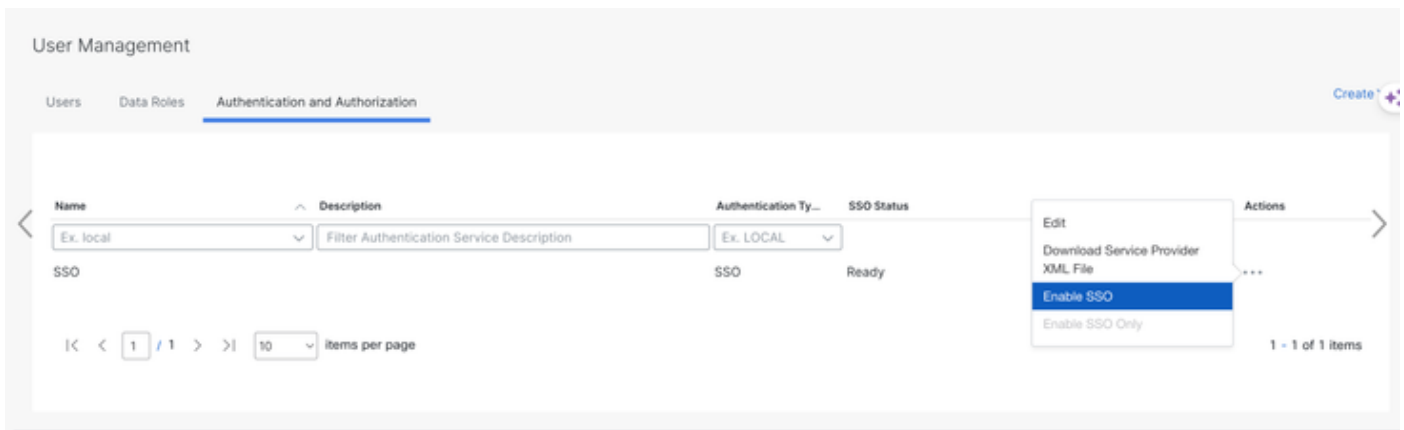
Note: Nesta demonstração, a opção Carregar arquivo XML de metadados do provedor de identidade está selecionada.

5. Configure o campo Tipo de Provedor de Identidade para ID do Microsoft Entra, Formato do Identificador de Nome para Persistente, Digite um Rótulo da Tela de Login.

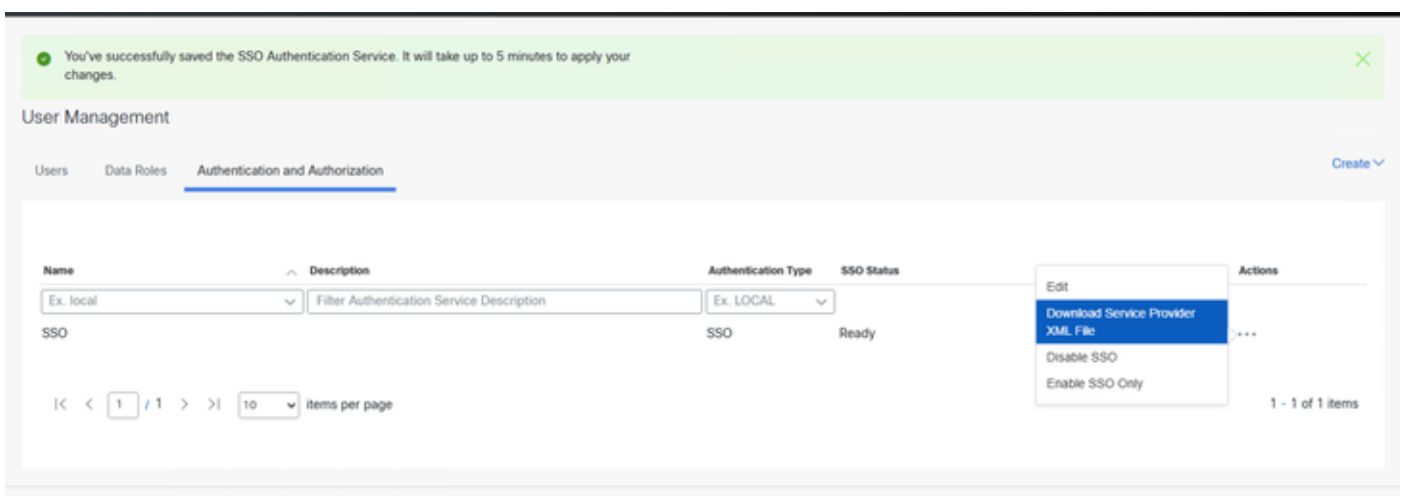


Tip: O rótulo da tela de logon configurado (nome/texto) é mostrado acima do botão Logon com SSO e não deve ser deixado em branco.

-
6. Clique em Salvar, que o levará de volta à guia Autenticação e Autorização.
 7. Aguarde até que o status seja READY e selecione Enable SSO no menu de ações.



8. Na guia Autenticação e autorização, clique nos três pontos da coluna Ações e clique em Download do arquivo XML do provedor de serviços.



Configurar SSO no Azure

1. Faça login no [portal do Azure](#).
2. Na barra de pesquisa, navegue até Aplicativo Empresarial > Selecionar Aplicativo Empresarial configurado > Clique em configurar login único.
3. Clique em Upload do arquivo de metadados na parte superior da página e carregue o arquivo sp.xml baixado do SNA Manager.
4. Ele abre a tela "Configuração SAML básica" e define várias configurações para corrigir valores, Clique em Salvar.



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

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

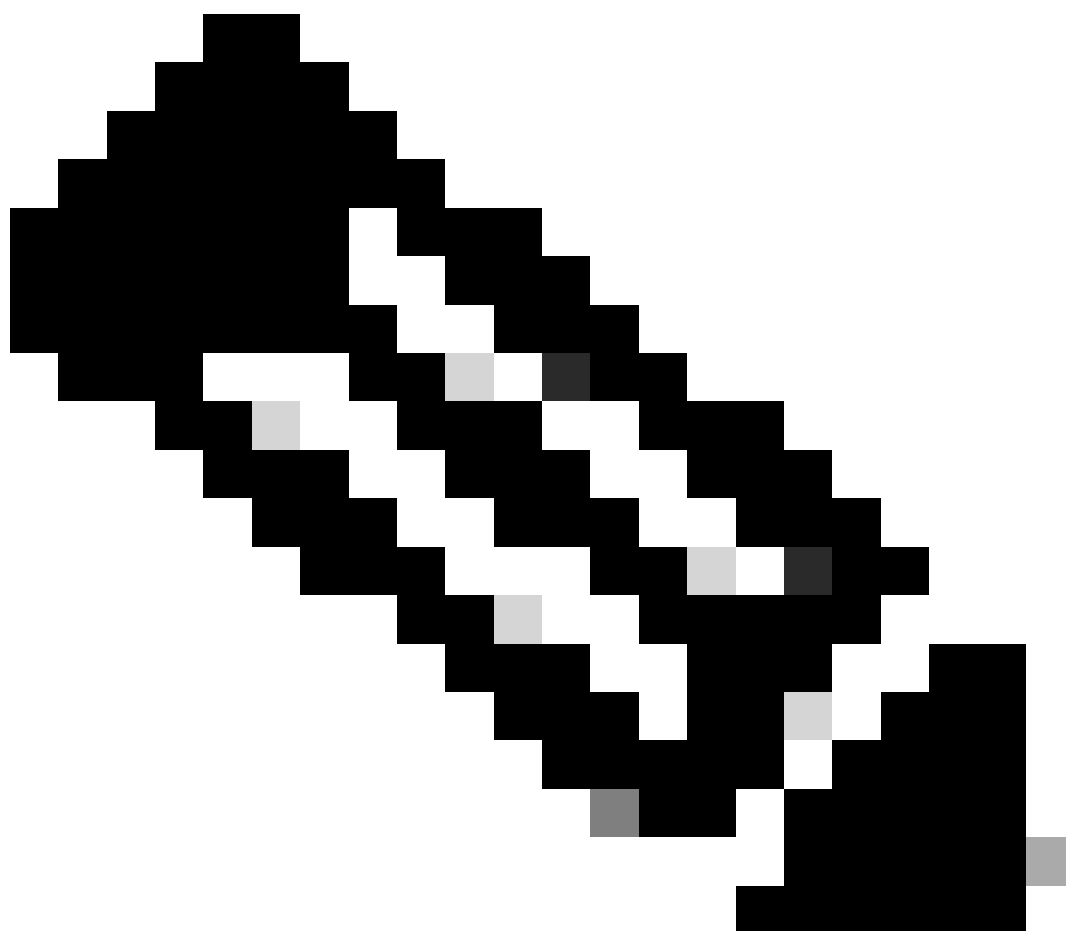
Enterprise Application



Upload metadata file



Change single sign-on



Note: Verifique se o Formato de ID do Nome no Entra ID está correto.

5. Localize a seção Atributos e Reivindicações e clique em 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/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. Clique no valor user.userprincipalname na seção Nome da reivindicação.

[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. Na página Gerenciar reivindicação, verifique o formato do identificador de nome.



Manage claim ...



Save



Discard changes



Got feedback?

Name

nameidentifier

Namespace

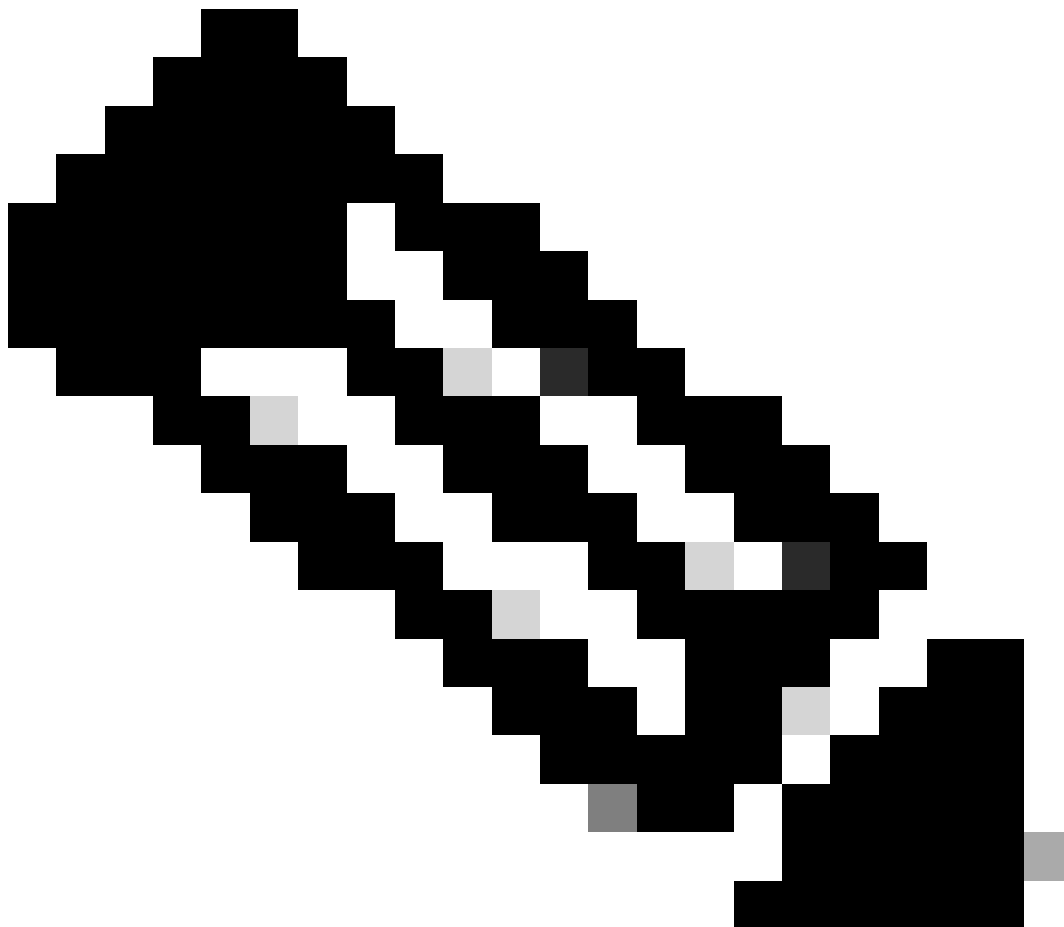
http://schemas.xmlsoap.org/ws/2005/05/identity/claims



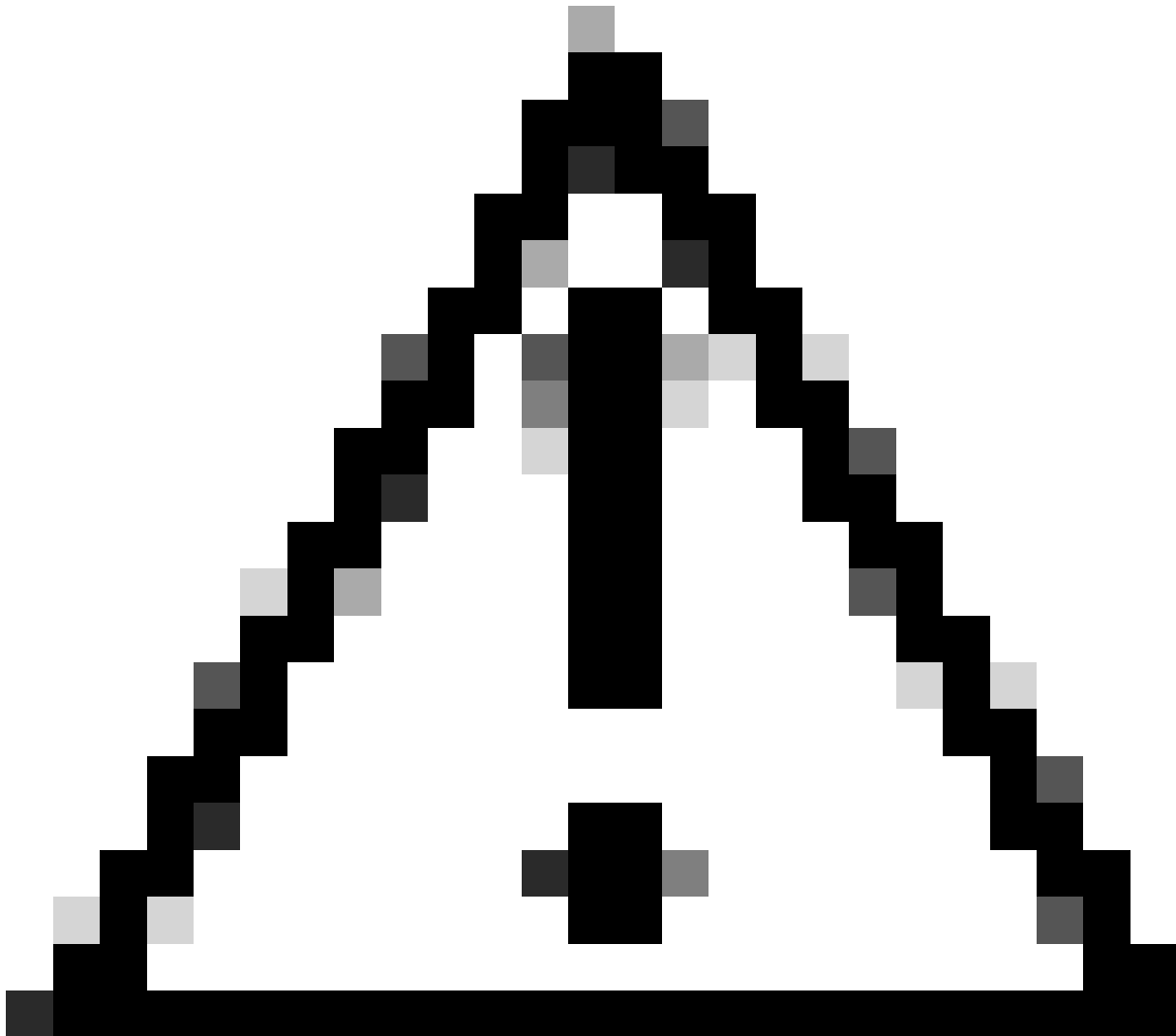
Choose name identifier format

Name identifier format *

Persistent



Note: O campo de formato do identificador de nome é definido como Persistente, caso contrário, selecione-o no menu suspenso. Clique em salvar se as alterações tiverem sido feitas.



Caution: Esse é o local mais comum para encontrar problemas. As configurações no Gerenciador SNA e no Microsoft Azure devem ser correspondentes. se você optou por usar o formato "emailAddress" em SNA, o formato aqui também deve ser "Email Address".

Configurar usuários na ID do Entra.

1. Faça login no [portal do Azure](#).
2. Na barra de pesquisa, navegue até Aplicativo Empresarial > Selecionar Aplicativo Empresarial configurado > selecione Usuários e Grupos à esquerda > clique em Adicionar usuário/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. No painel esquerdo, clique em Nenhum Selecionado.

4. Pesquise e adicione o usuário necessário ao aplicativo.

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

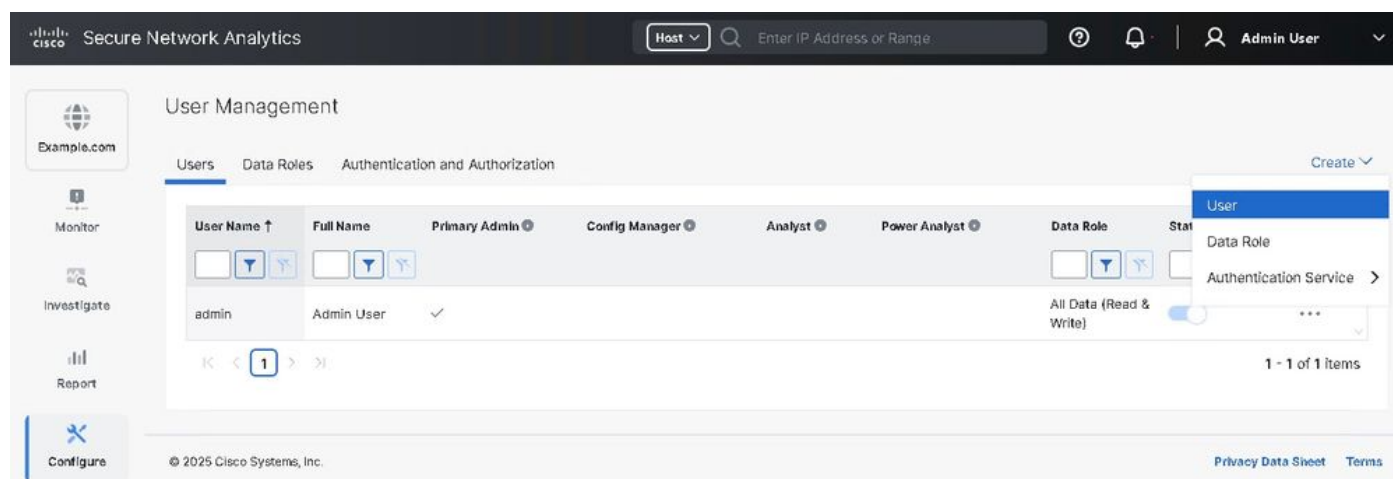
Assign Select

Configurar SSO em SNA

1. Faça login na interface do usuário do SNA Manager.

2. Navegue até Configure > Global > User Management.

3. Clique em Criar > Usuário.



4. Configure o usuário fornecendo detalhes associados ao serviço de Autenticação selecionado como SSO e clique em Salvar.

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

Criação de SAML-User em SNA-UI

Troubleshooting

Se os usuários não conseguirem fazer login no SNA Manager, um rastreador SAML pode ser usado para investigar mais.

Se for necessária assistência adicional na investigação do SNA Manager, um caso de TAC poderá ser levantado.

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.