

Configurazione di SNA Manager per Microsoft Entra ID SSO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura di configurazione](#)

[Configura applicazione enterprise in Azure](#)

[Configurazione e download del file XML del provider di servizi in SNA](#)

[Configura SSO in Azure](#)

[Impostare gli utenti in Entra ID.](#)

[Configura SSO in SNA](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare Secure Network Analytics (SNA) per l'utilizzo di Microsoft Entra ID per Single Sign-On (SSO).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Microsoft Azure
- Secure Network Analytics

Componenti usati

- SNA Manager v7.5.2
- ID Entra Microsoft

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

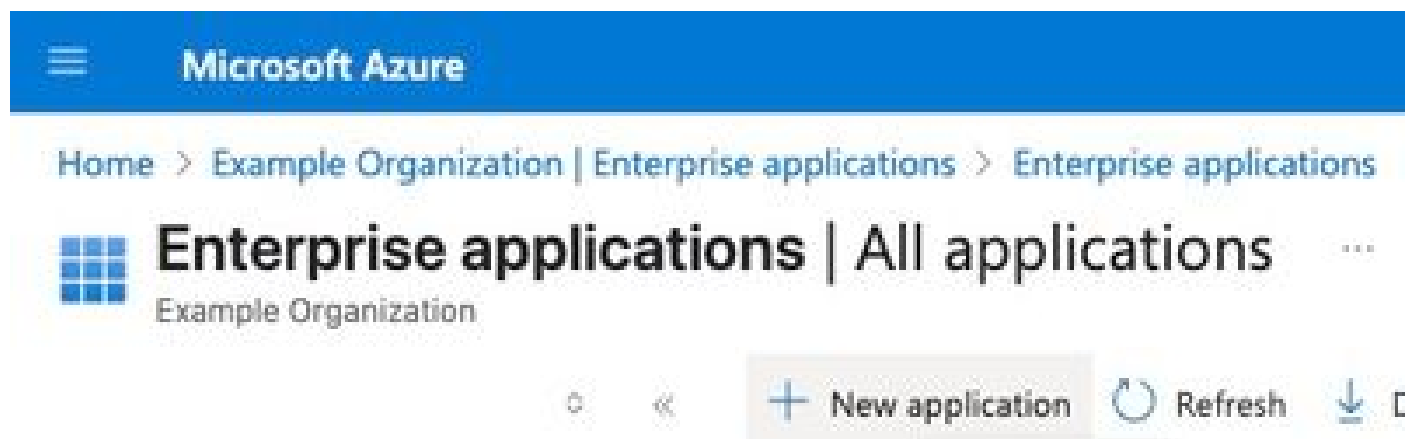
Procedura di configurazione

Configura applicazione enterprise in Azure

1. Accedere al [portale cloud di Azure](#).
2. Cercare il servizio Entra ID nella casella di ricerca e selezionare Microsoft Entra ID.



3. Nel riquadro di sinistra espandere Gestisci e selezionare Applicazioni enterprise.
4. Fare clic su Nuova applicazione.



5. Selezionare Crea applicazione personalizzata nella nuova pagina che viene caricata.



[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. Fornire un nome all'applicazione in Qual è il nome dell'applicazione? campo.
7. Selezionare il pulsante di opzione Integra qualsiasi altra applicazione non presente nella raccolta (Non-Gallery) e fare clic su Crea.

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. Nel dashboard dell'applicazione appena configurato, fare clic su Imposta Single Sign-On.



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 ⓘ

[Redacted Application ID] ...

Object ID ⓘ

[Redacted 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. Selezionare SAML.

The screenshot shows the 'Single sign-on' configuration page in the Microsoft Entra ID portal. The left sidebar contains a navigation menu with options: 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 is titled 'Select a single sign-on method' with a 'Help me decide' link. It features two cards: a 'Disabled' card with a red circle and slash icon, stating 'Single sign-on is not enabled. The user won't be able to launch the app from My Apps.', and a 'SAML' card with a puzzle piece icon, describing it as 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

10. Nella pagina Configurazione Single Sign-On con SAML fare clic su Modifica in Configurazione SAML di 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' pane, which is the first step in the configuration process. It includes an 'Edit' link in the top right corner. The configuration details are as follows:

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

11. In Basic SAML Configuration pane configurare Add Reply URL in <https://example.com/fedlet/fedletapplication> sostituendo example.com con FQDN di SNA Manager e fare clic su 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. Individuare la scheda Certificati SAML e salvare il valore del campo URL metadati federazione app e scaricare il file XML metadati federazione.

3

SAML Certificates

Token signing certificate

Edit

Status

Active

Thumbprint

123456789abcdefghijklmnop

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

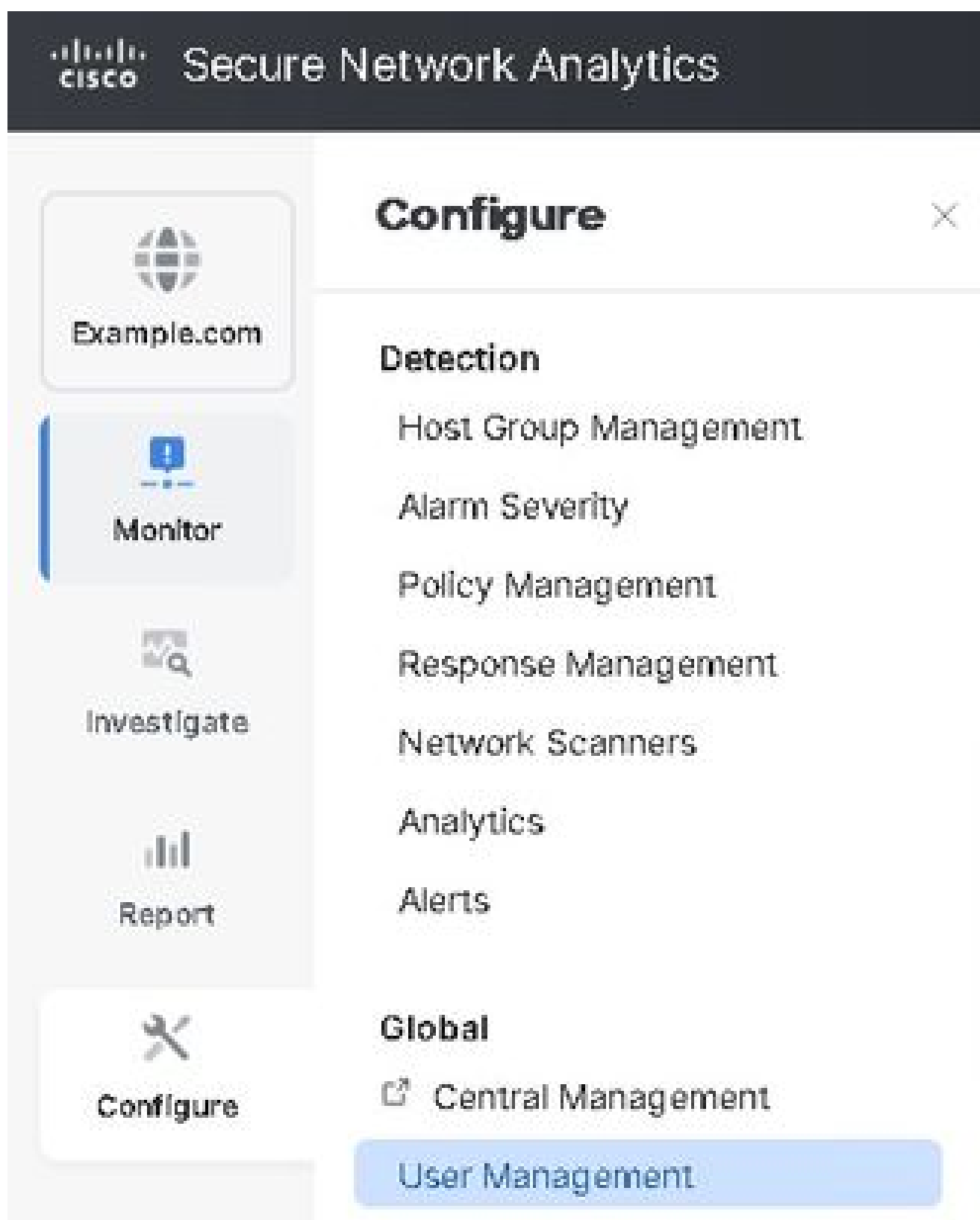
0

Expired

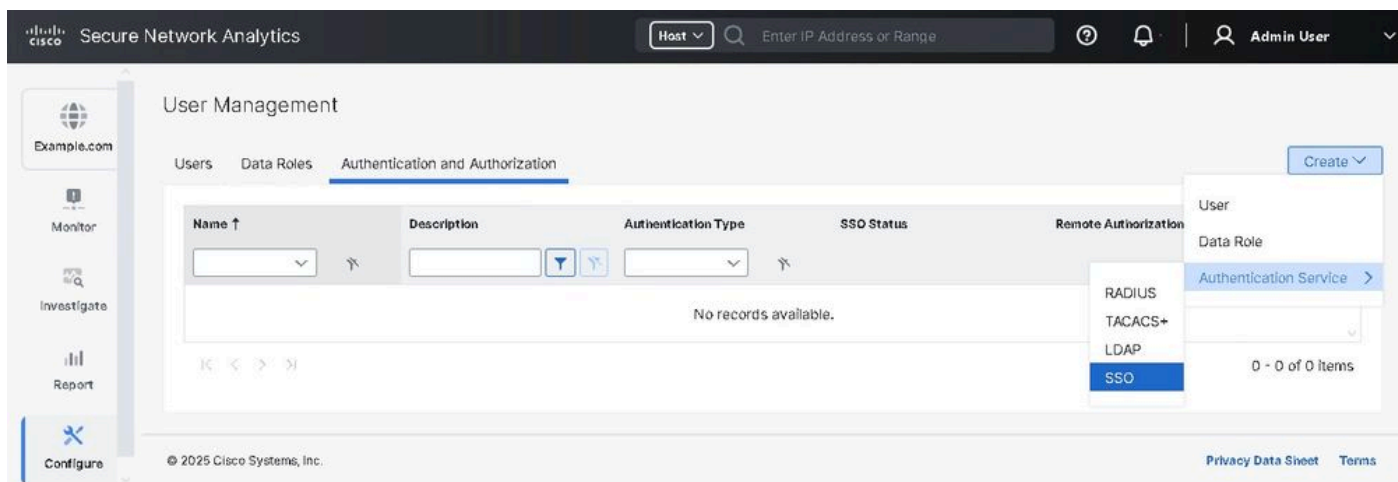
0

Configurazione e download del file XML del provider di servizi in SNA

1. Accedere all'interfaccia utente di SNA Manager.
2. Passare a Configura > Globale > Gestione utente.

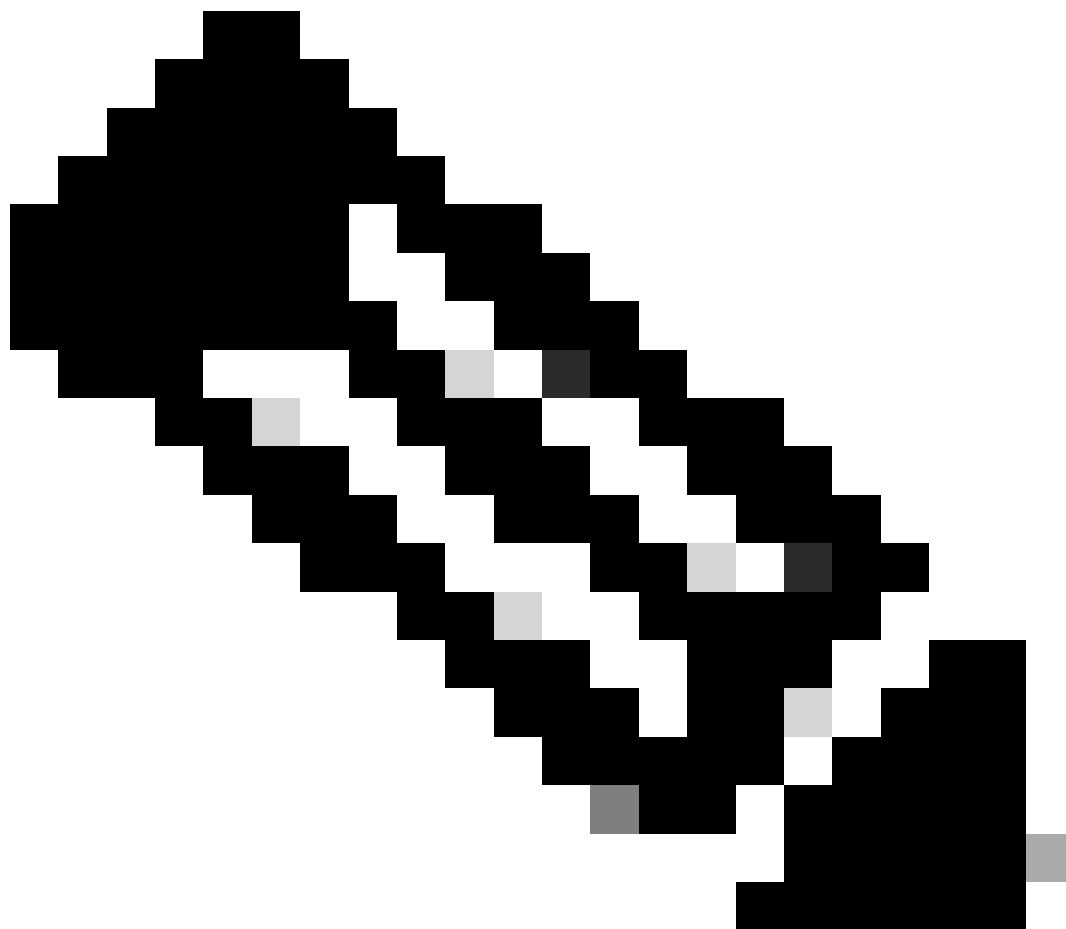


3. In scheda Autenticazione e autorizzazione fare clic su Crea > Servizio di autenticazione > SSO.



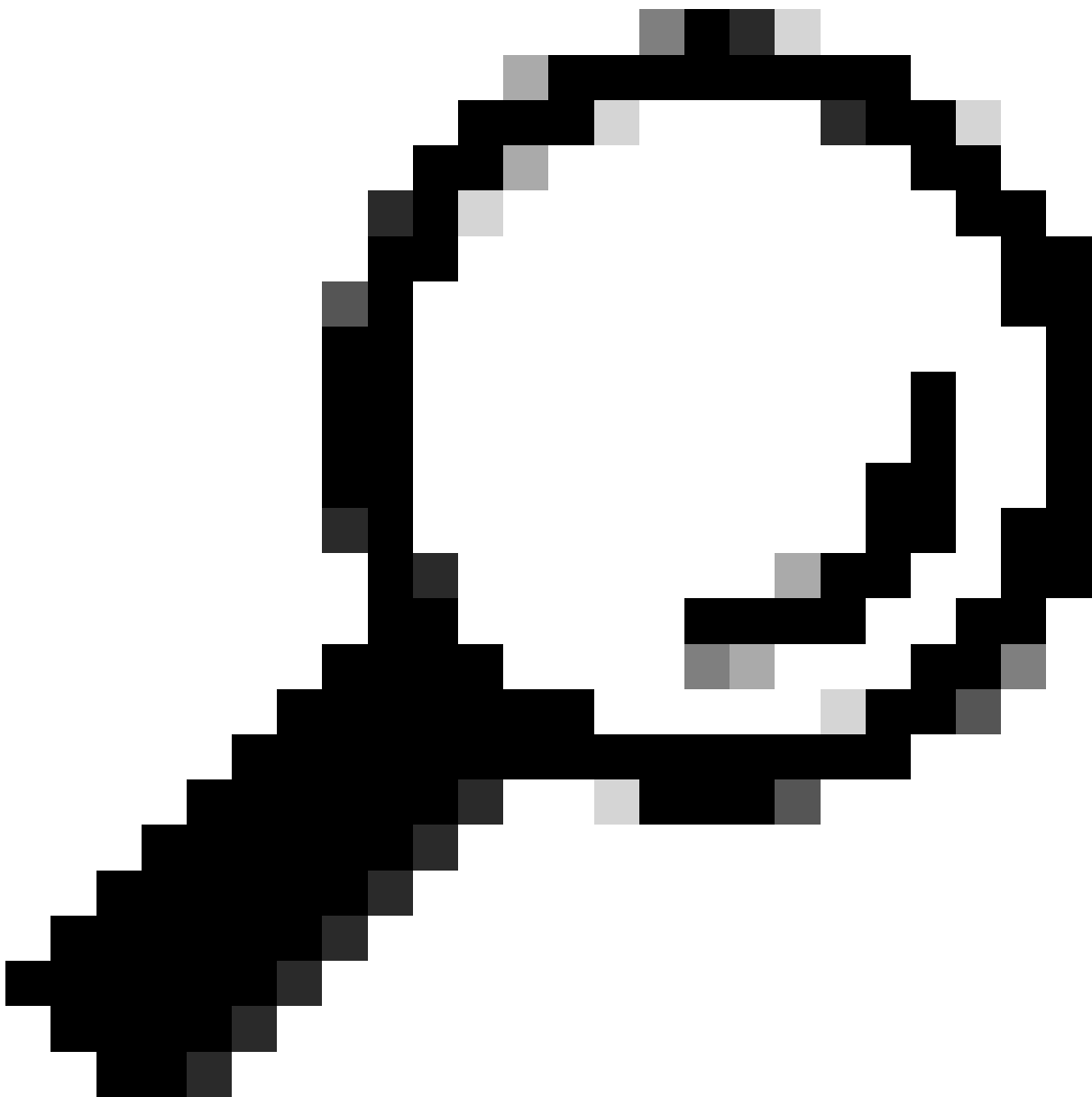
4. Selezionare il pulsante di opzione appropriato per URL metadati provider di identità o Carica file XML metadati provider di identità.

The screenshot shows the 'User Management | Authentication Service' configuration page. The 'Authentication Service' section has 'Authentication Service Type' set to 'SSO', 'Name' set to 'SSO', and 'Description' empty. The 'Identity Provider' section has 'Identity Provider Type' set to 'Microsoft Entra ID', 'Status' set to 'Ready', and 'Identity Provider Metadata URL' selected. The 'General Configuration' section has 'Name Identifier Format' set to 'Persistent', 'Login Screen Label' set to 'popup', and 'Custom Service Provider Address' set to 'ex. sna-manager.example.com or 192.168.10.10'.



Nota: In questa demo è selezionata l'opzione Carica file XML metadati del provider di identità.

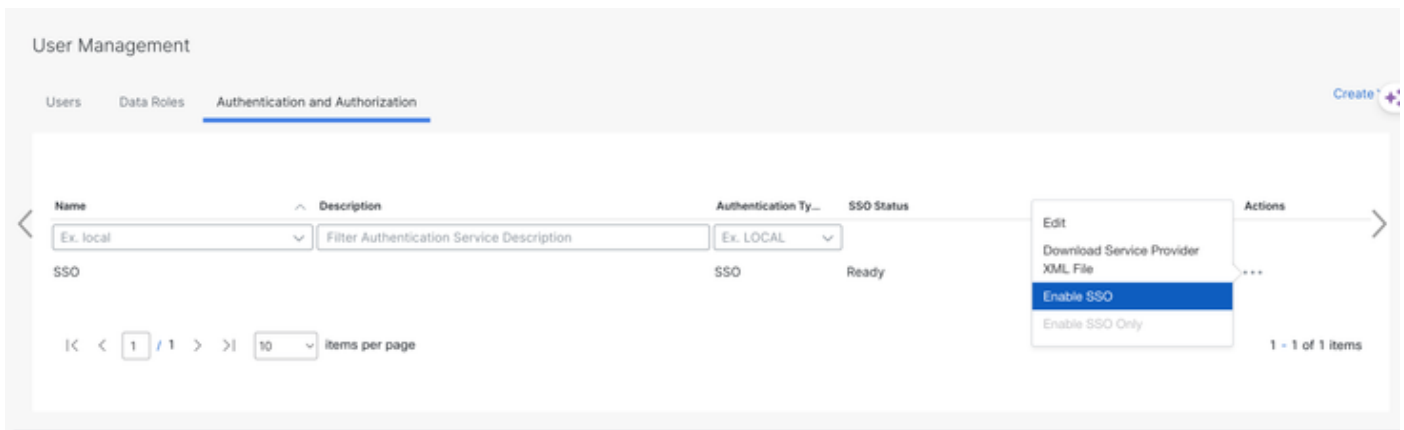
5. Configurare il campo Tipo di provider di identità su Microsoft Entra ID, Formato identificatore nome su Permanente, Digitare un'etichetta per la schermata di accesso.



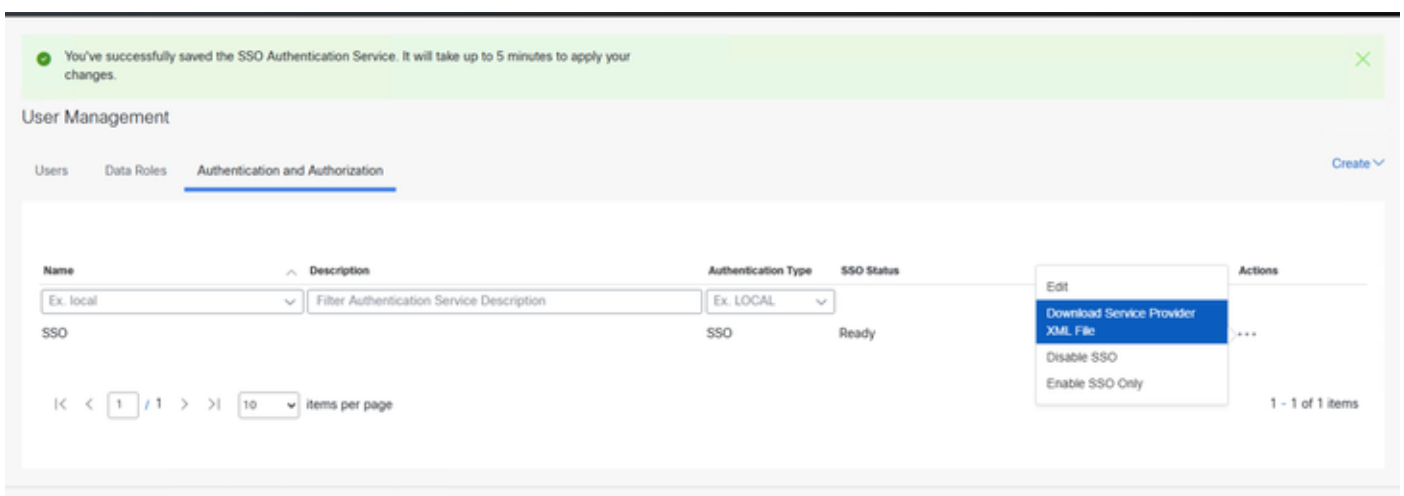
Suggerimento: L'etichetta della schermata di accesso configurata (nome/testo) viene visualizzata sopra il pulsante Accesso con SSO e non deve essere lasciata vuota.

6. Fare clic su Salva per tornare alla scheda Autenticazione e autorizzazione.

7. Attendere che lo stato sia READY e selezionare Abilita SSO dal menu Azione.



8. In Autenticazione e autorizzazione scheda fare clic sui tre punti nella colonna Azioni e fare clic su Scarica il file XML del provider di servizi.



Configura SSO in Azure

1. Accedere al [portale di Azure](#).
2. Dalla barra di ricerca passare a Applicazione enterprise > Seleziona applicazione enterprise configurata > Fare clic su Imposta Single Sign-On.
3. Fare clic su Upload metadata file nella parte superiore della pagina e caricare il file sp.xml scaricato da SNA Manager.
4. Viene visualizzata la schermata "Basic SAML Configuration" (Configurazione SAML di base) e si impostano varie impostazioni per correggere i valori. Fare clic su Save (Salva).



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

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

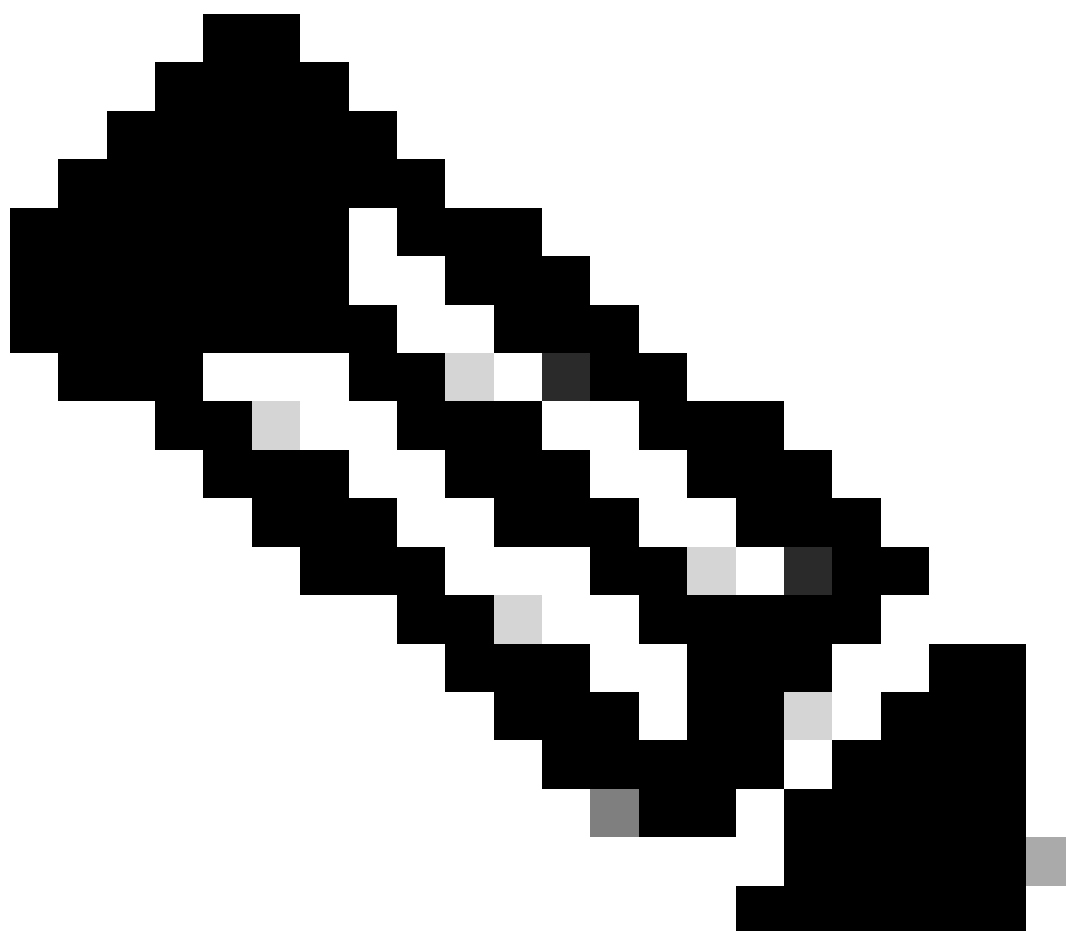
Enterprise Application



Upload metadata file



Change single sign-on



Nota: Assicurarsi che il formato ID del nome in Entra ID sia corretto.

5. Individuare la sezione Attributi e richieste di rimborso e fare clic su Modifica.

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. Fare clic sul valore user.userprincipalname nella sezione Nome attestazione.

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. In Gestisci risarcimento pagina Verifica Scegli formato identificativo nome.



Manage claim ...



Save



Discard changes



Got feedback?

Name

nameidentifier

Namespace

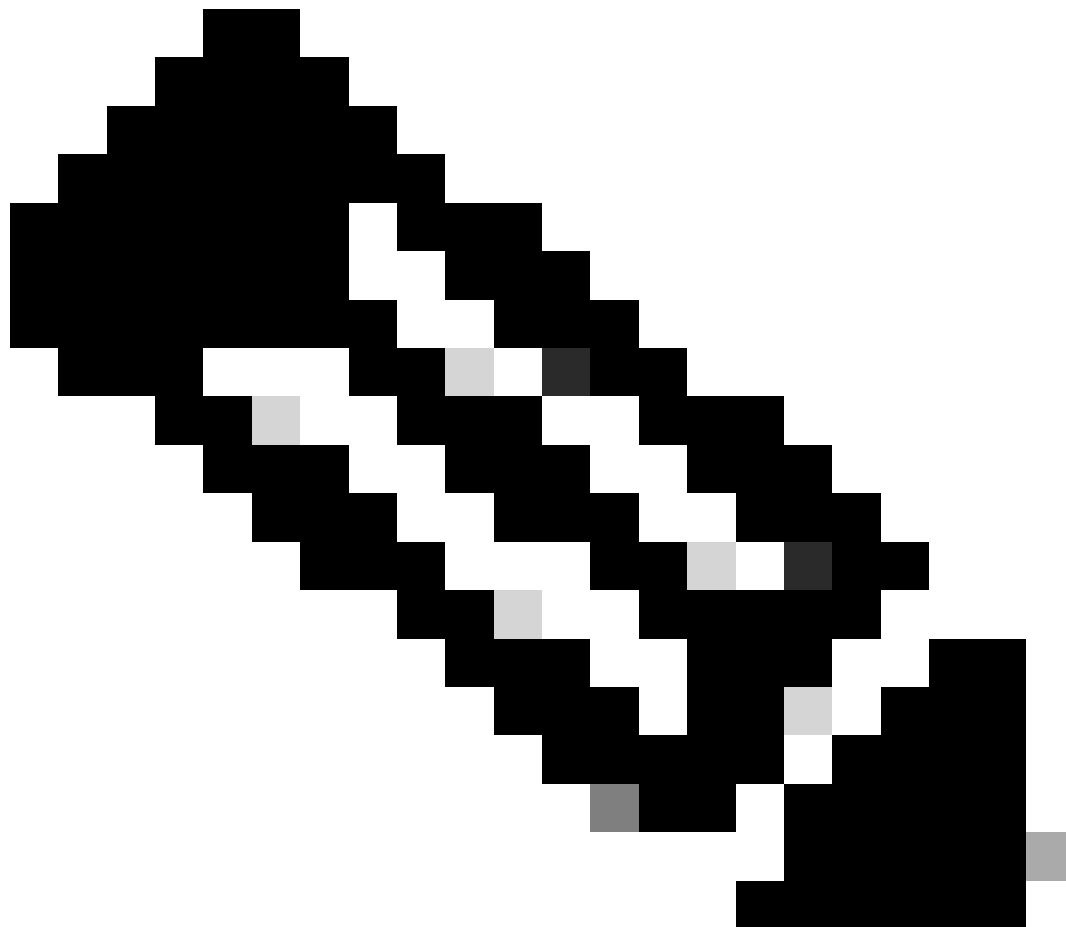
http://schemas.xmlsoap.org/ws/2005/05/identity/claims



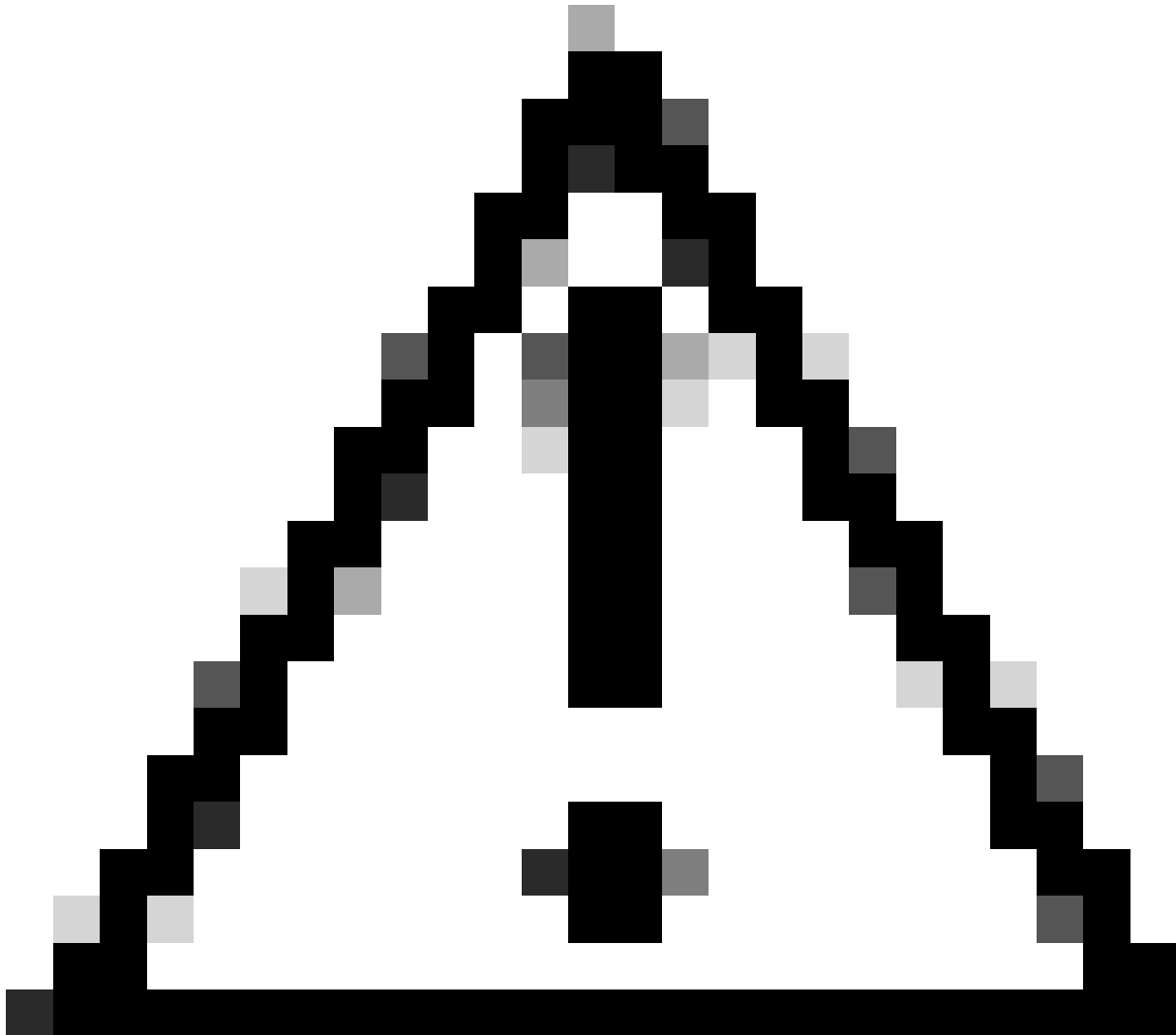
Choose name identifier format

Name identifier format *

Persistent



Nota: Il campo Formato identificatore nome è impostato su Persistente se non è selezionato dal menu a discesa. Fare clic su Salva se sono state apportate modifiche.



Attenzione: Si tratta del luogo più comune in cui si verificano problemi. Le impostazioni in Gestione SNA e Microsoft Azure devono corrispondere. se si è scelto di utilizzare il formato "indirizzo e-mail" in SNA, il formato deve essere "indirizzo e-mail".

Impostare gli utenti in Entra ID.

1. Accedere al [portale di Azure](#).
2. Dalla barra di ricerca passare a Applicazione enterprise > Seleziona applicazione enterprise configurata > seleziona utenti e gruppi a sinistra > fare clic su Aggiungi utente/gruppo.

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. Nel riquadro sinistro fare clic su Nessuna selezione.

4. Cercare e aggiungere l'utente richiesto all'applicazione.

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

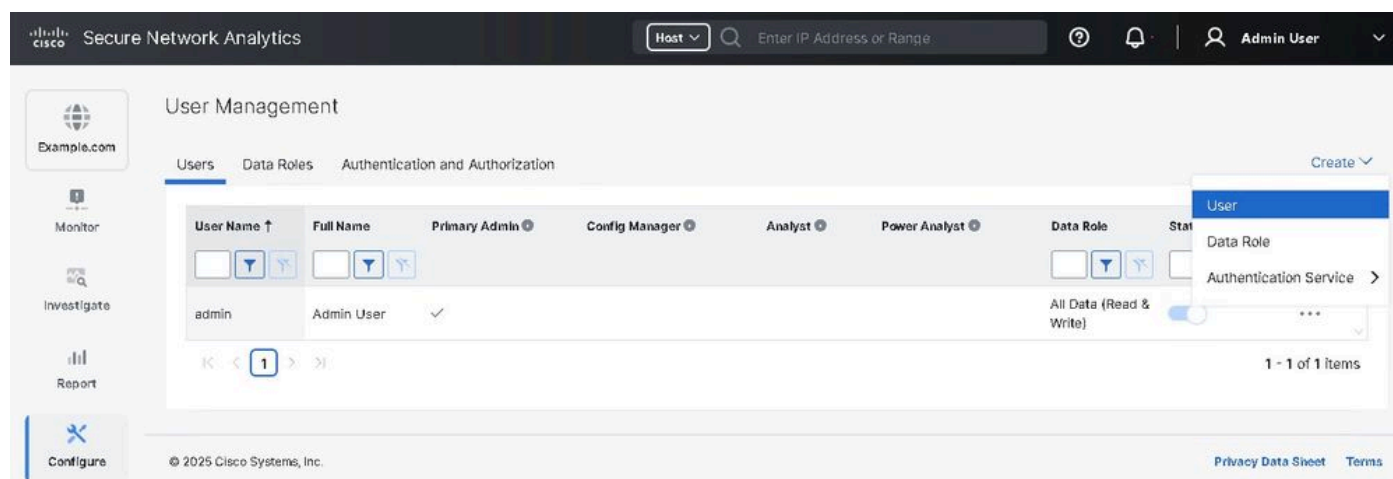
Assign Select

Configura SSO in SNA

1. Accedere all'interfaccia utente di SNA Manager.

2. Passare a Configura > Globale > Gestione utente.

3. Fare clic su Crea > Utente.



4. Configurare l'utente fornendo i dettagli associati con il servizio di autenticazione selezionato come SSO e fare clic su Salva.

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

Creazione utente SAML in SNA-UI

Risoluzione dei problemi

Se gli utenti non sono in grado di accedere a SNA Manager, è possibile usare un tracer SAML per ulteriori informazioni.

Se è necessaria ulteriore assistenza nelle indagini sul gestore SNA, è possibile segnalare un caso TAC.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).