Configurar o SNA Manager para a ID do Microsoft Entra SSO

Contents

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

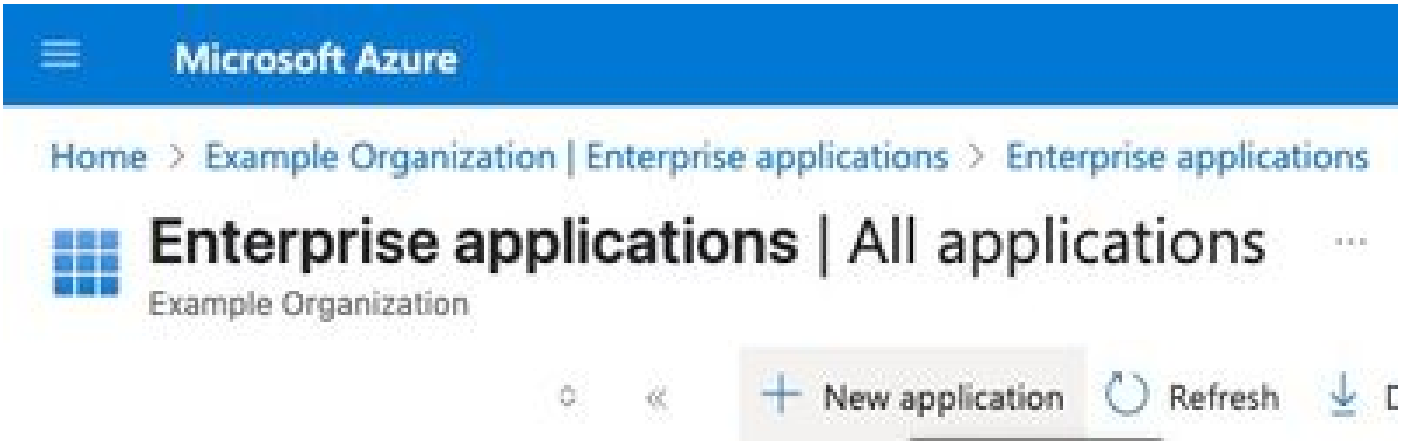
Configurar Aplicativo Empresarial no Azure

1. Faça logon no portal de nuvem do Azure.

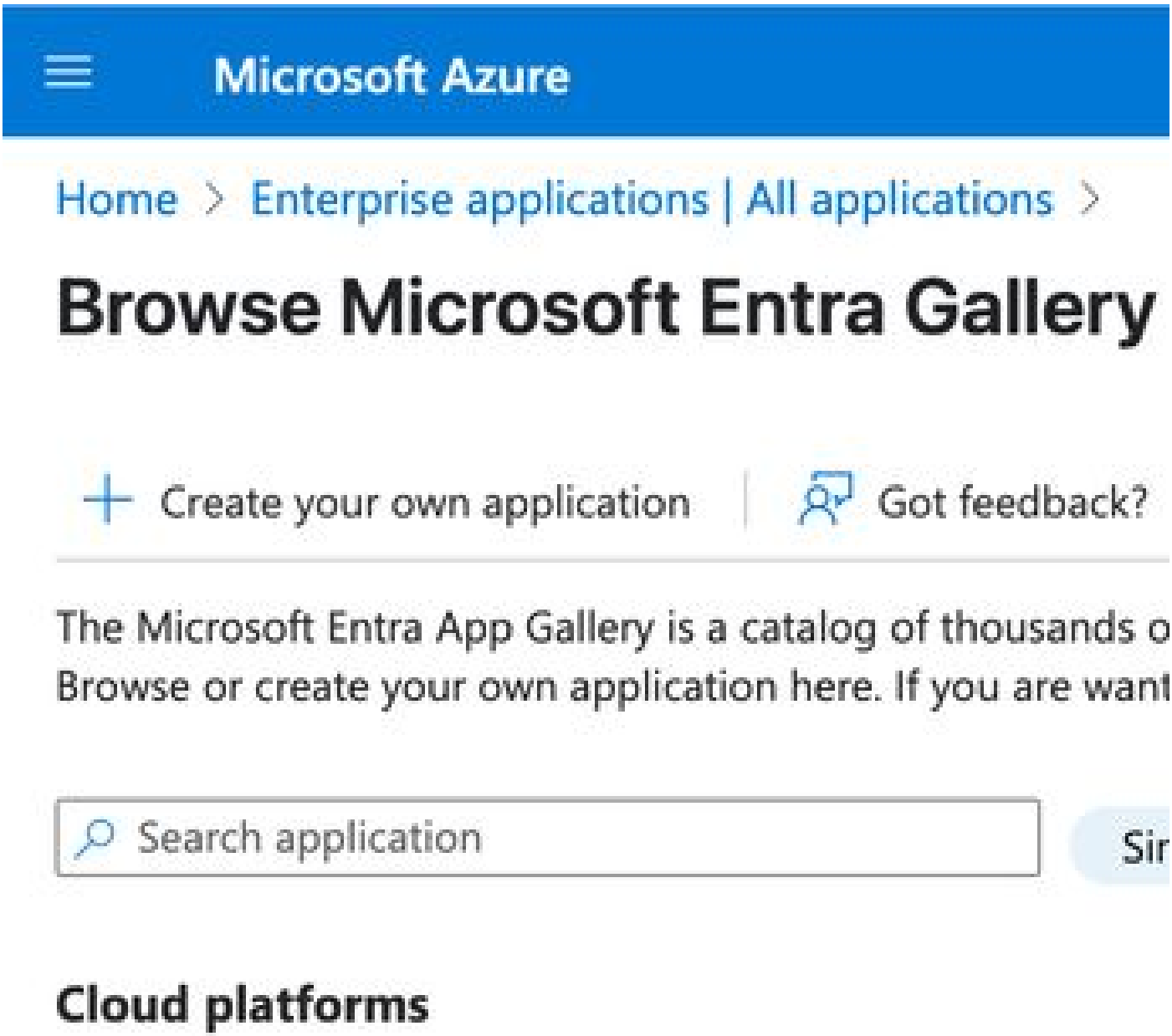
2. Pesquise o serviço Entra ID na caixa de pesquisa e selecione Microsoft Entra ID.

3. No painel esquerdo, expanda Gerenciar e selecione Aplicativos corporativos.

4. Clique em Novo Aplicativo.



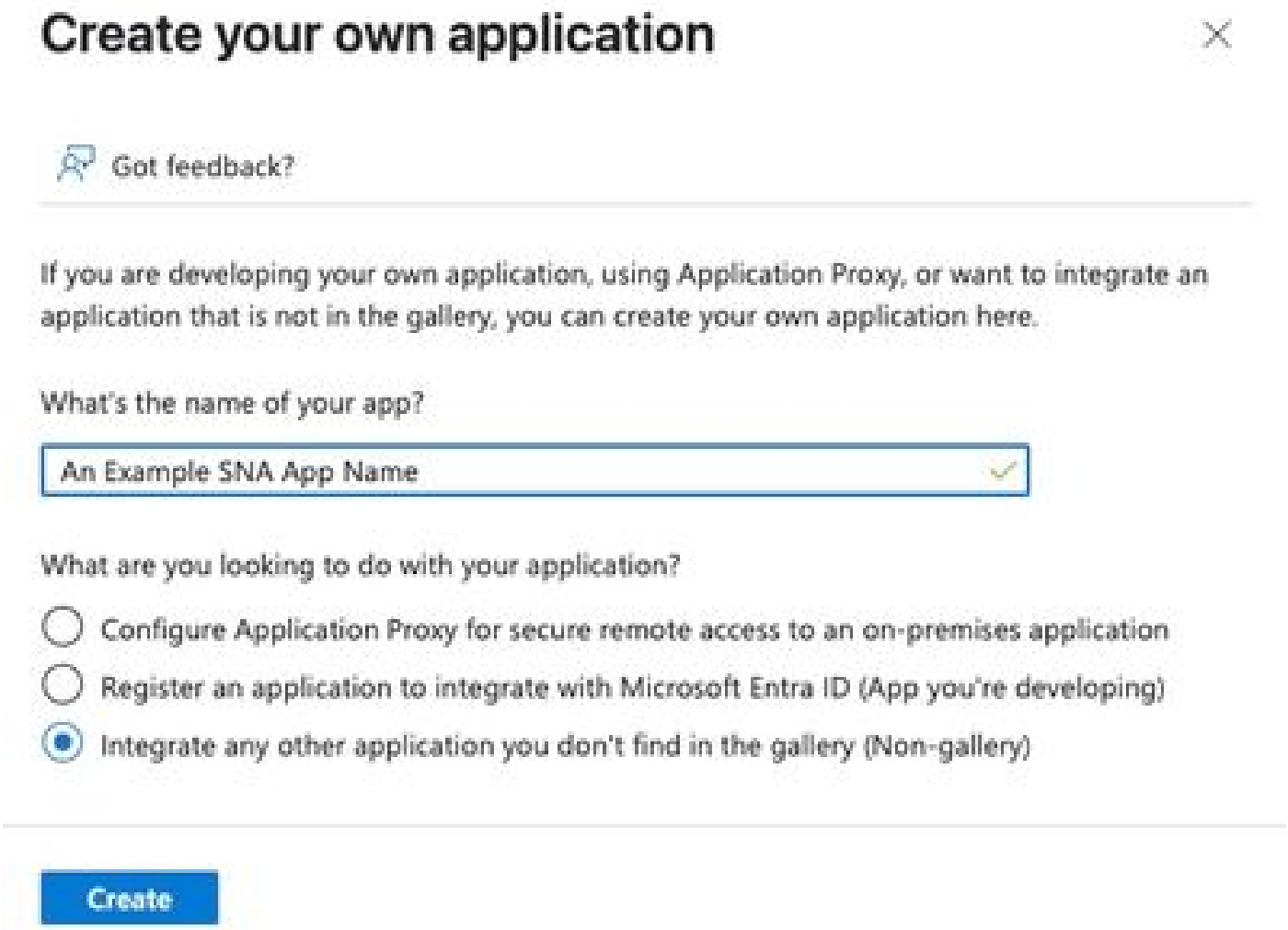
5. Selecione Criar Seu Próprio Aplicativo na nova página que é carregada.



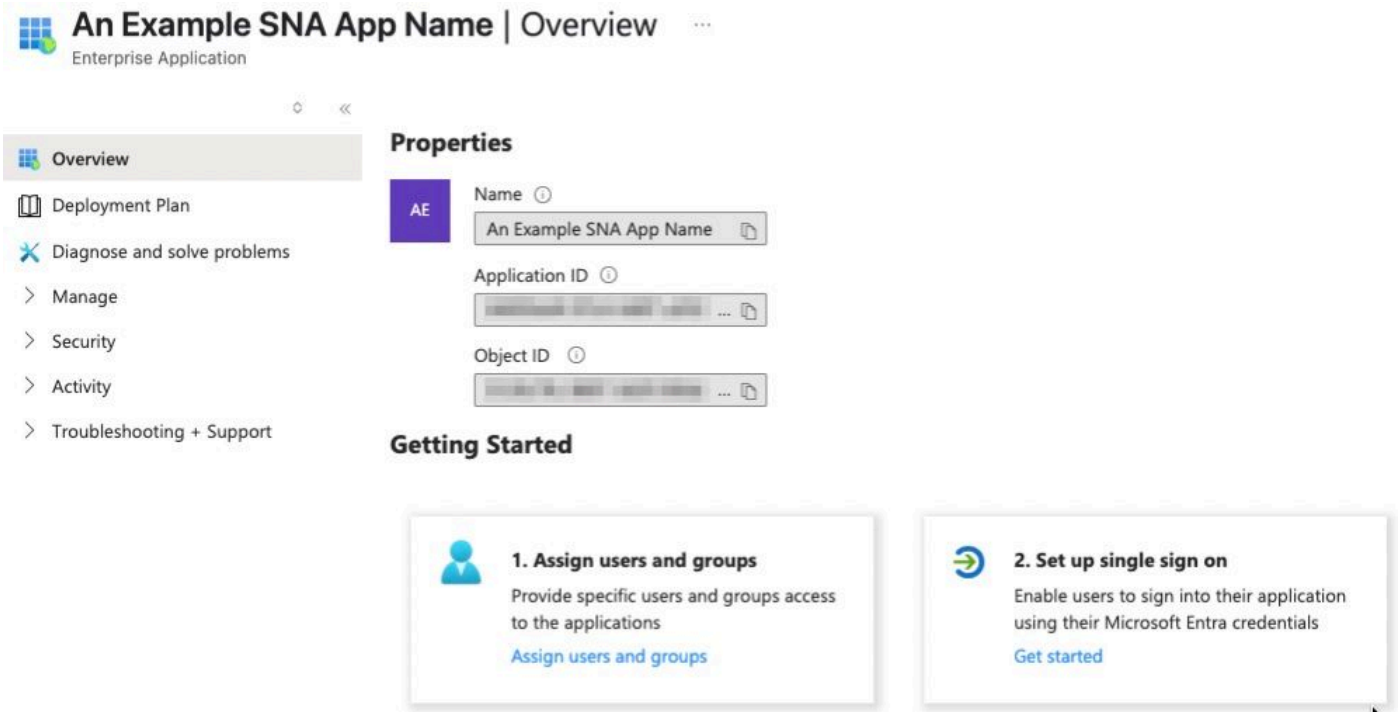
UI do Azure

6. Forneça um nome para o aplicativo em Qual é o nome do seu aplicativo? campo.

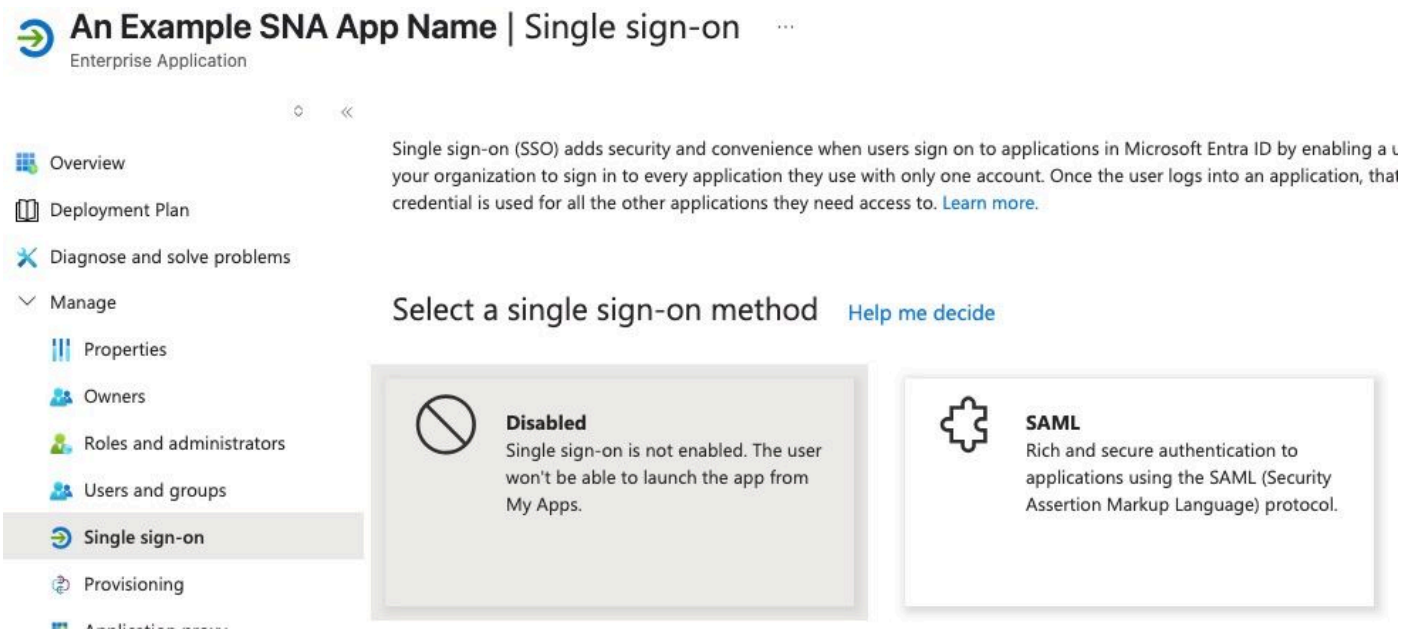
7. Selecione o botão de opção Integrar qualquer outro aplicativo que não esteja na galeria (Não-galeria) e clique em Criar.



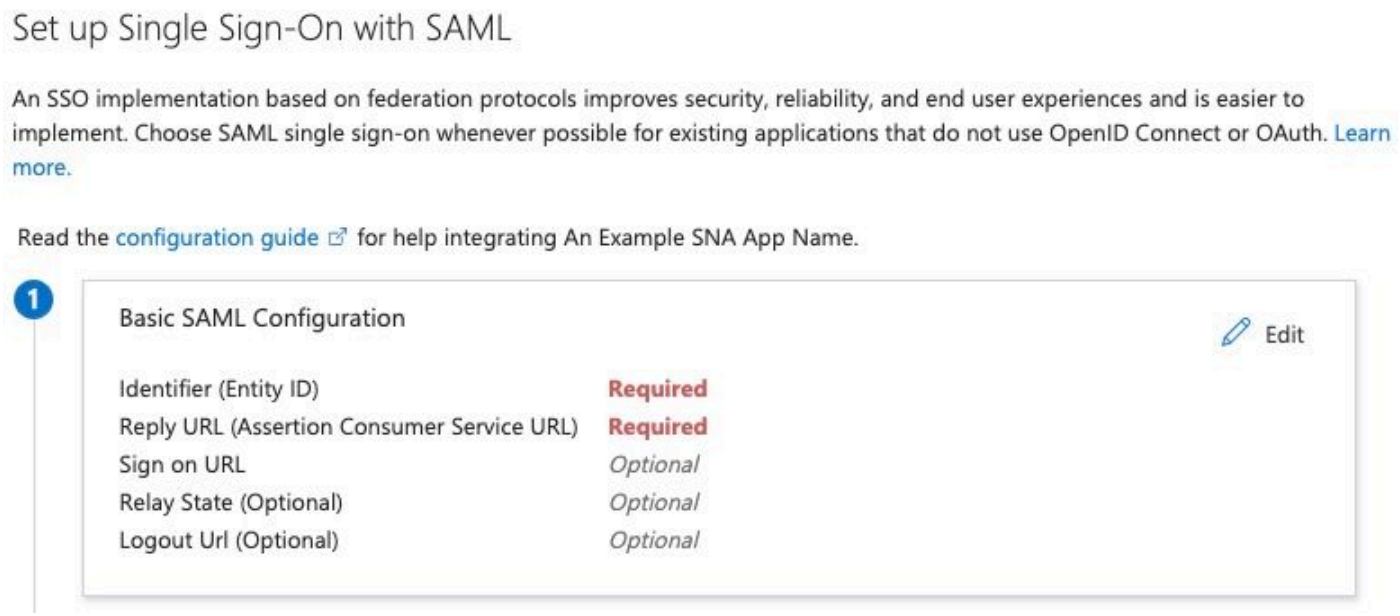
8. No painel de instrumentos do aplicativo recém-configurado, clique em Configurar logon único.



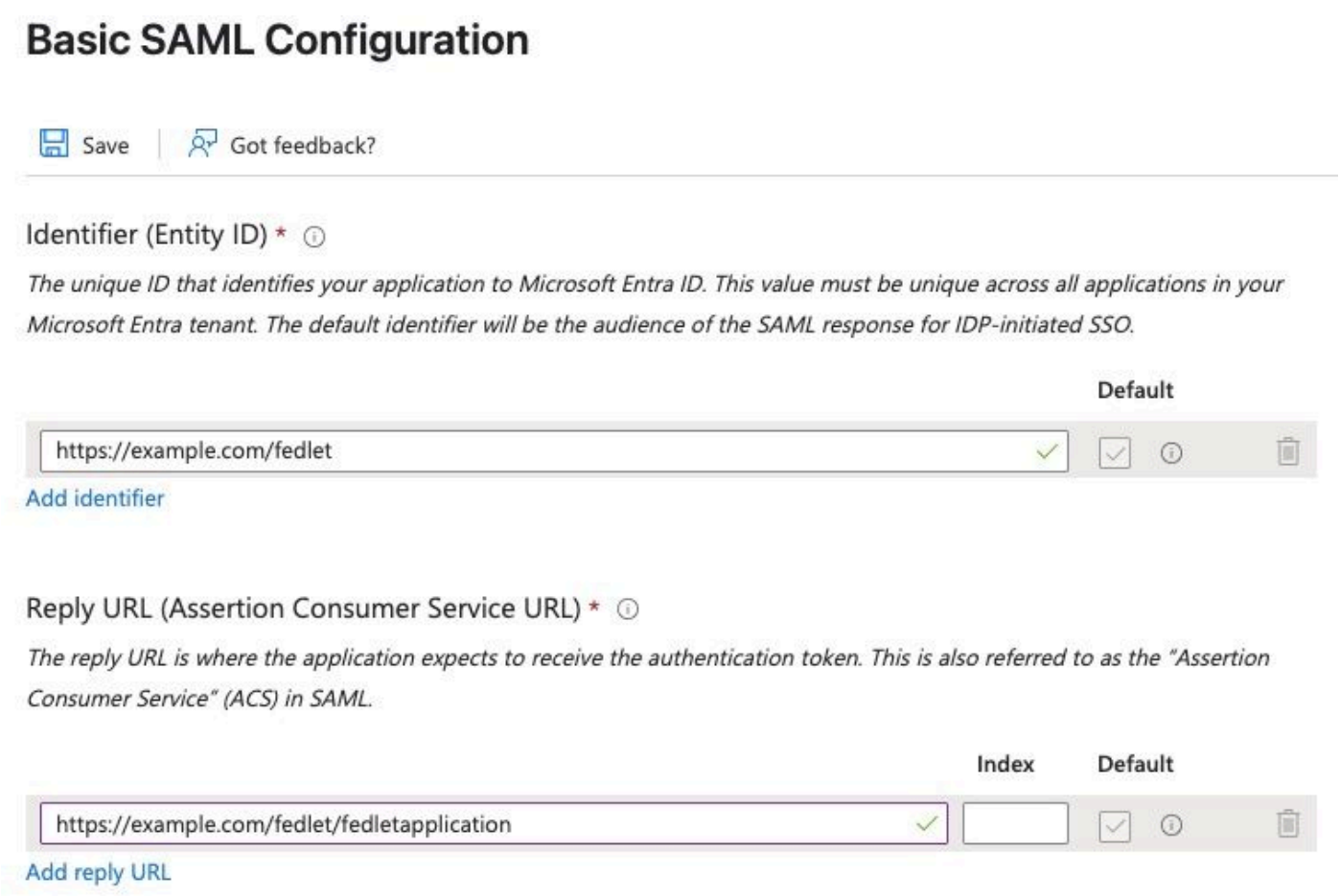
9. Selecione SAML.



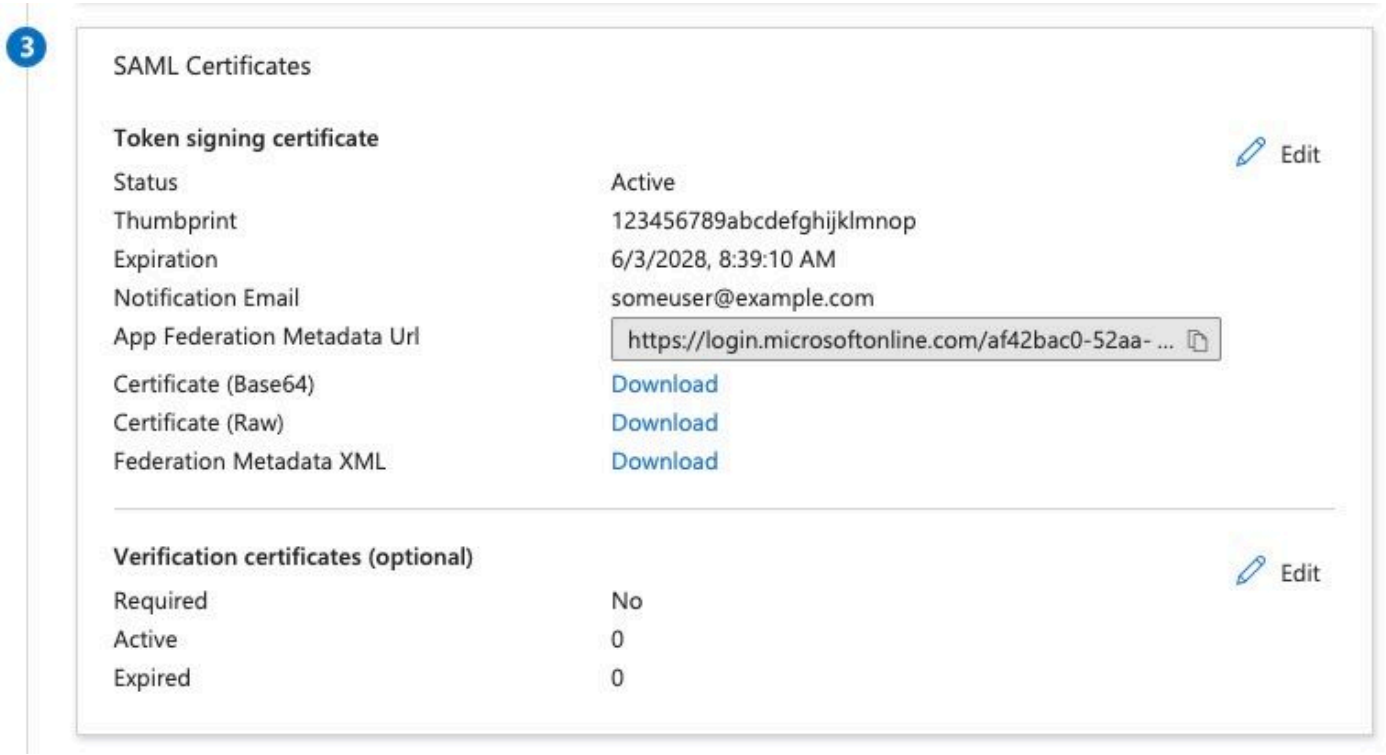
10. Na página Configurar Single Sign-On com SAML, clique em Editar em Configuração SAML Básica.



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.

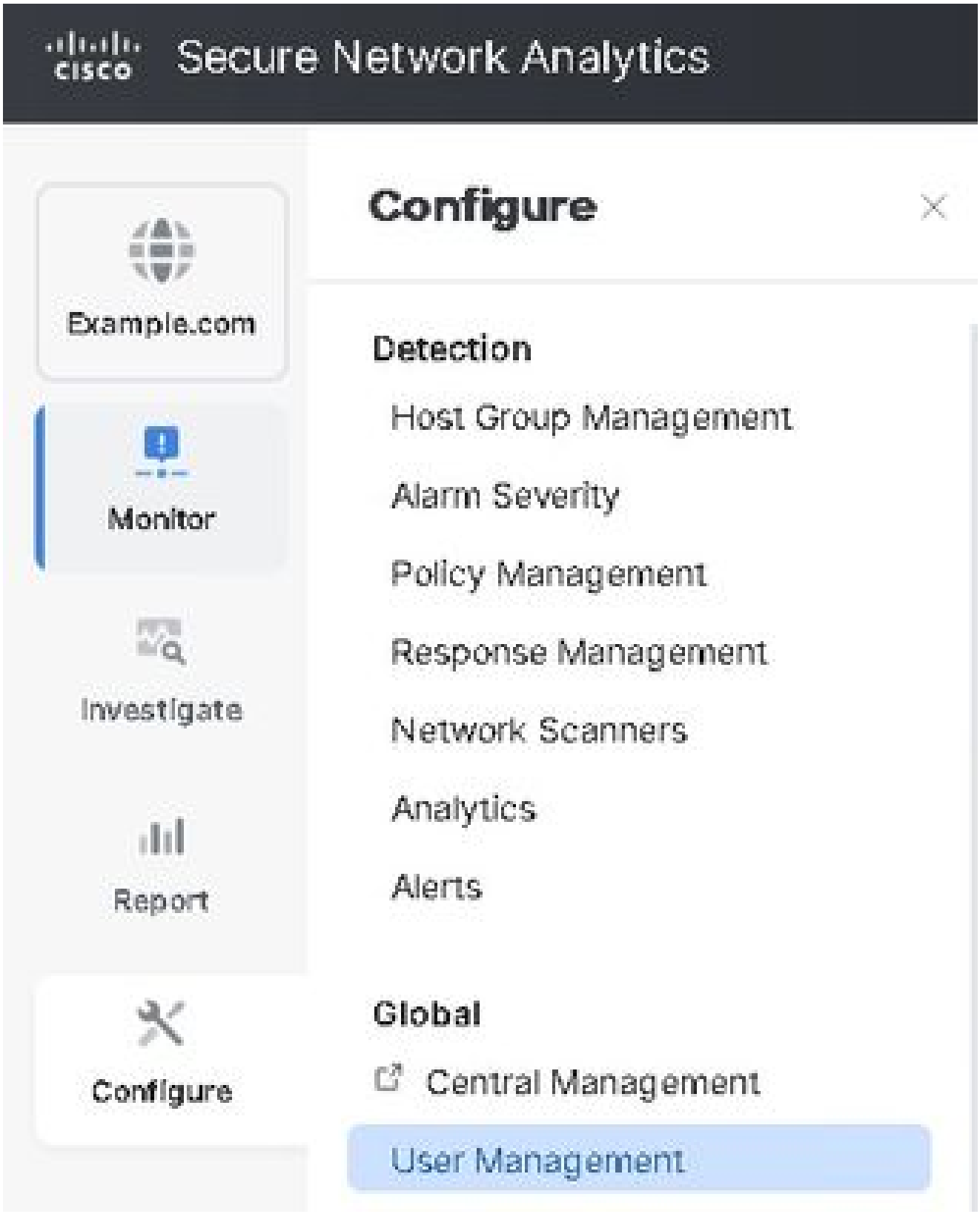


12. Localize o cartão Certificados SAML e salve o valor do campo URL de Metadados de Federação de Aplicativos e baixe o XML de Metadados de Federação.

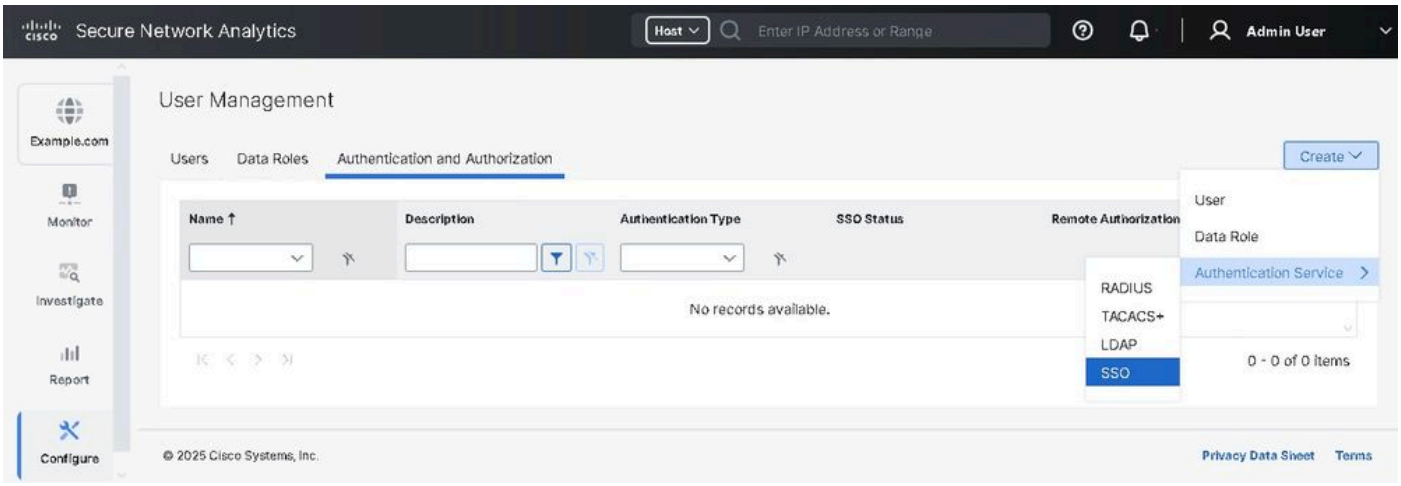


Configurar e fazer download do arquivo XML do provedor de serviços no SNA

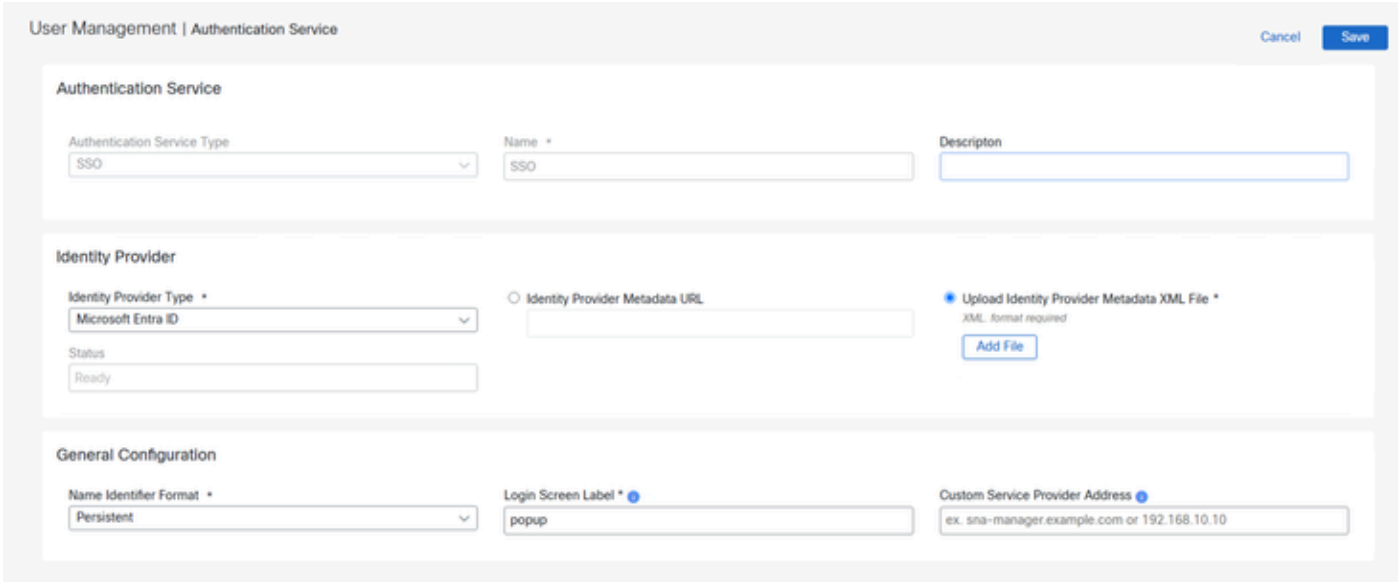
1. Faça login na interface do usuário do SNA Manager.
2. Navegue até Configure > Global > User Management.

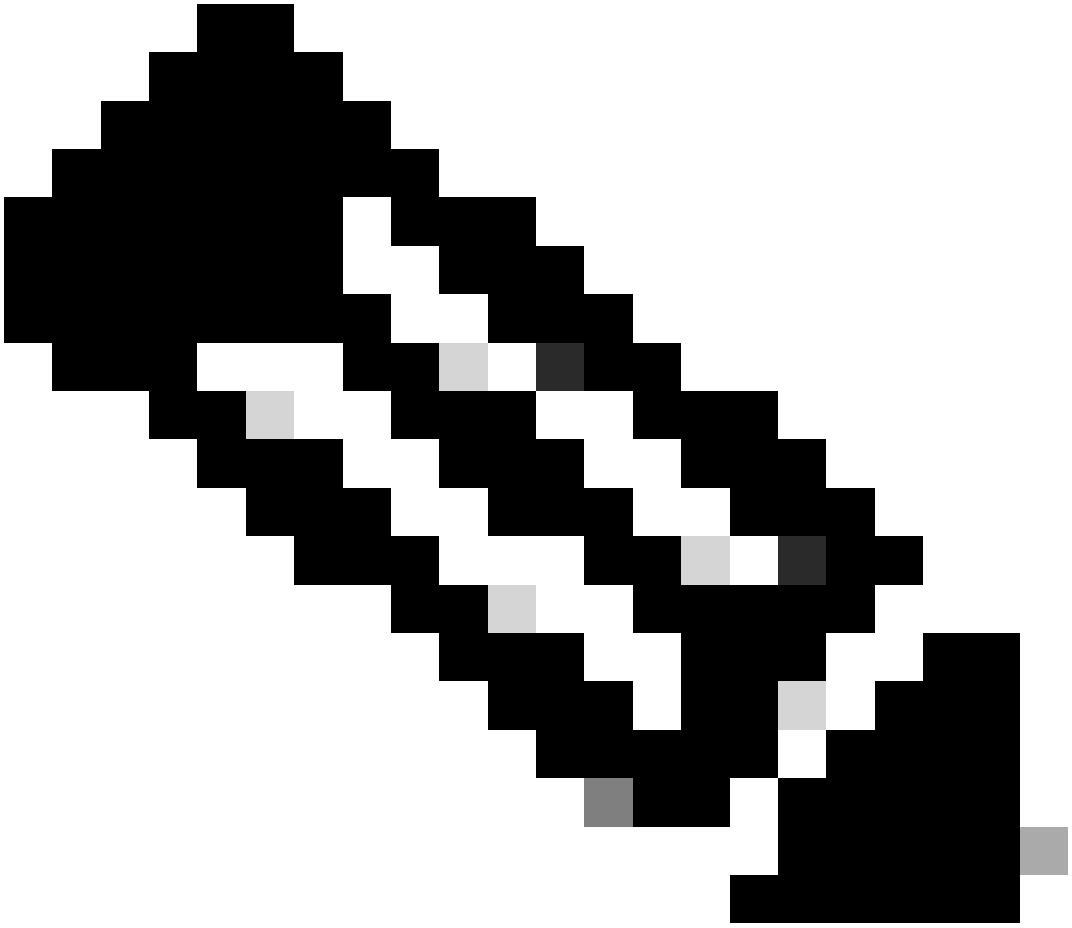


3. Na guia Authentication and Authorization, clique em Create > Authentication Service > SSO.



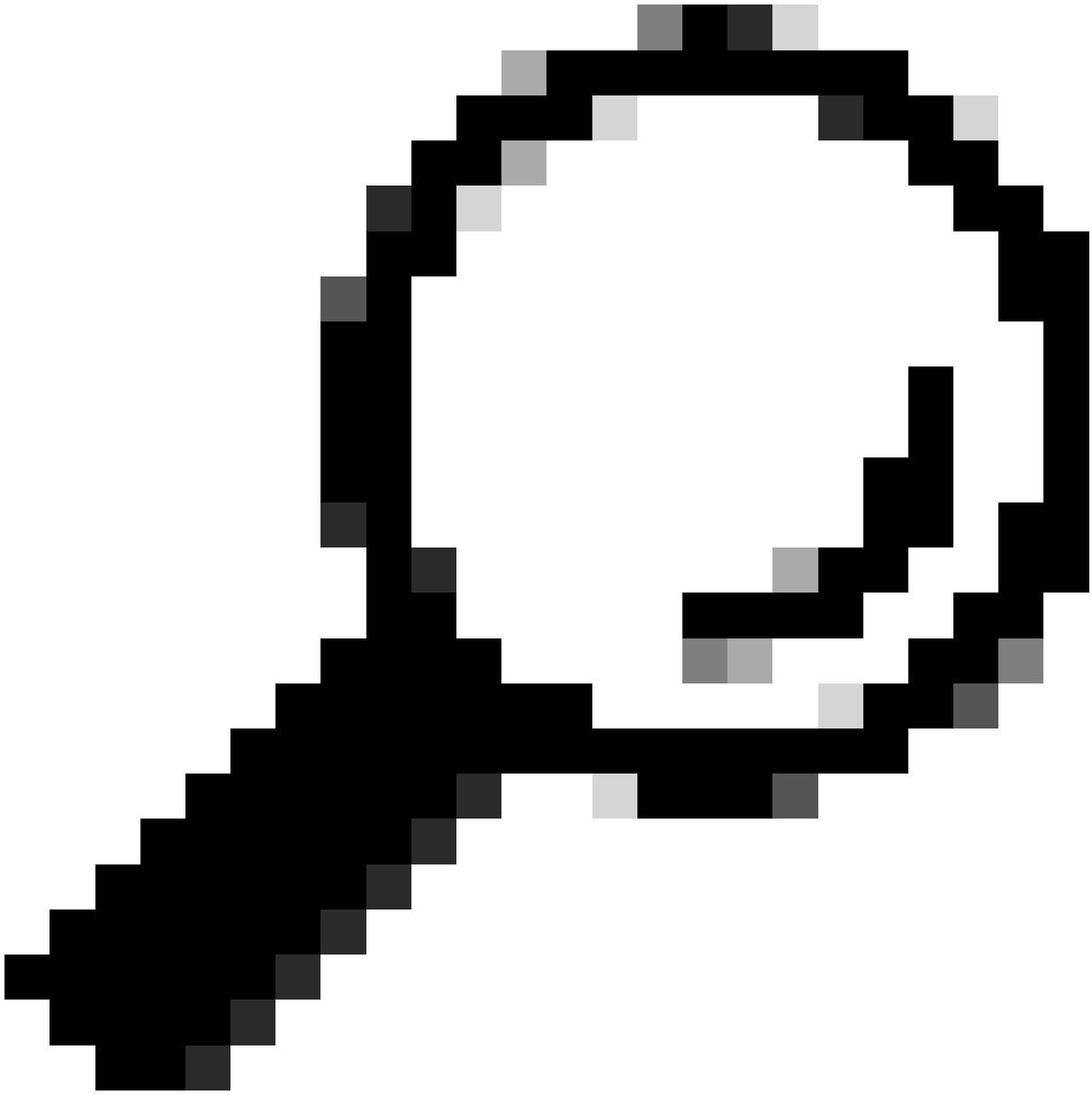
4. Selecione o botão de opção apropriado para URL de Metadados do Provedor de Identidade ou Carregar Arquivo XML de Metadados do Provedor de Identidade.





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

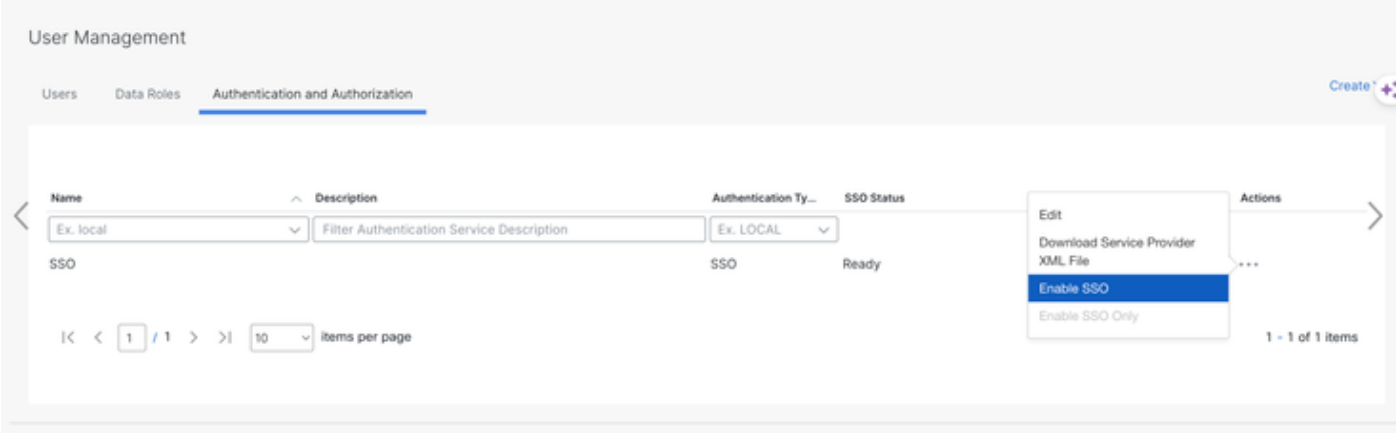
5. Configure o campo Tipo de Provedor de Identidade para ID do Microsoft Entra, Formato do Identificador de Nome para Persistente, Digite um Rótulo da Tela de Login.



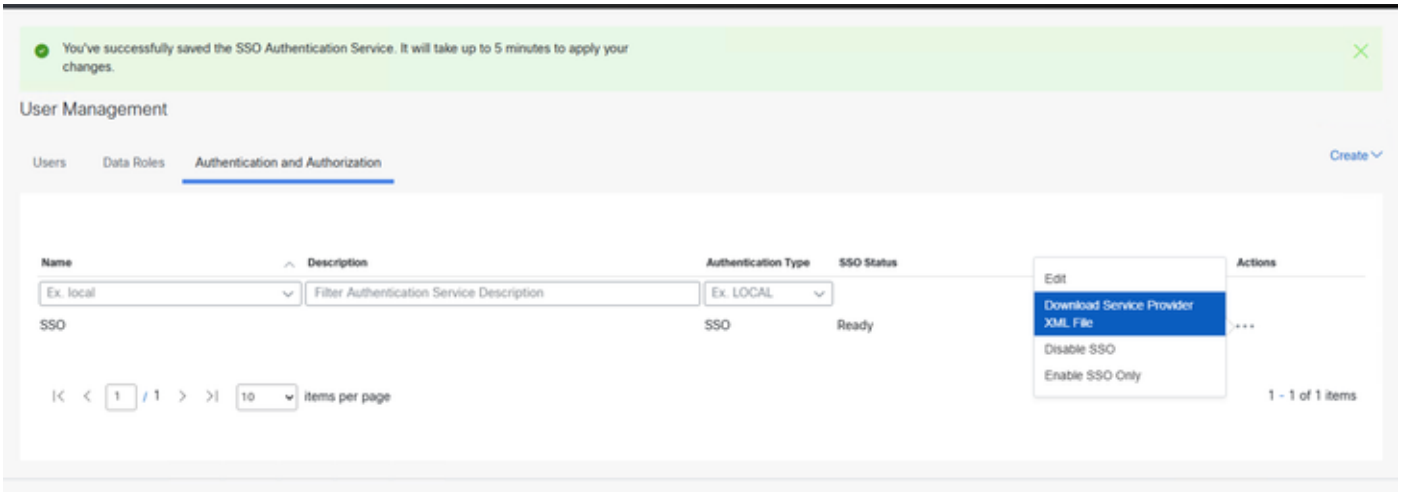
Tip: O rótulo da tela de logon configurado (nome/texto) é mostrado acima do botão Logon com SSO e não deve ser deixado em branco.

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.



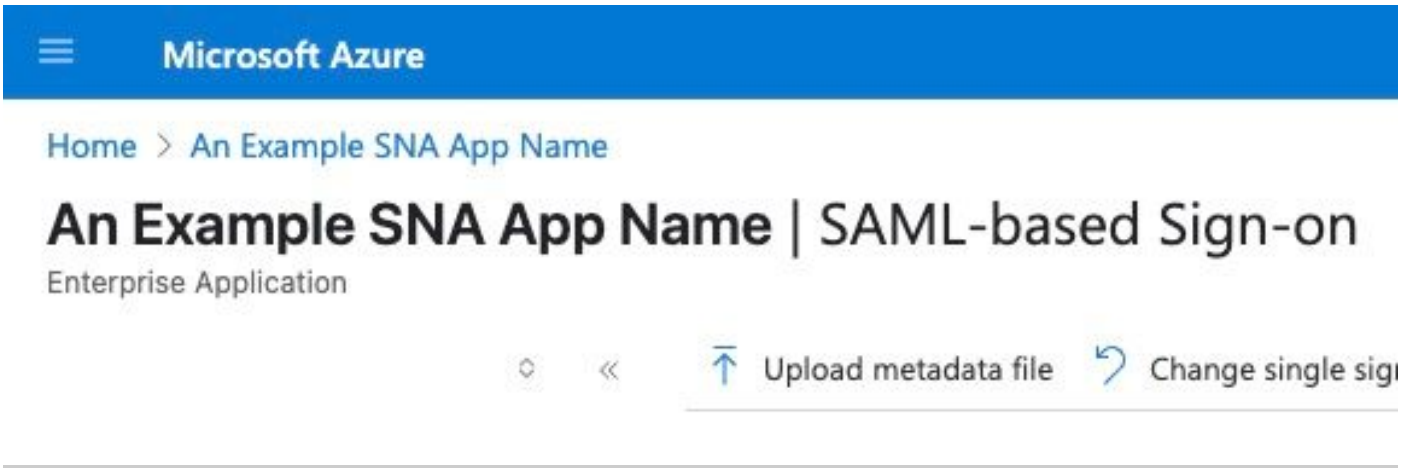
Configurar SSO no Azure

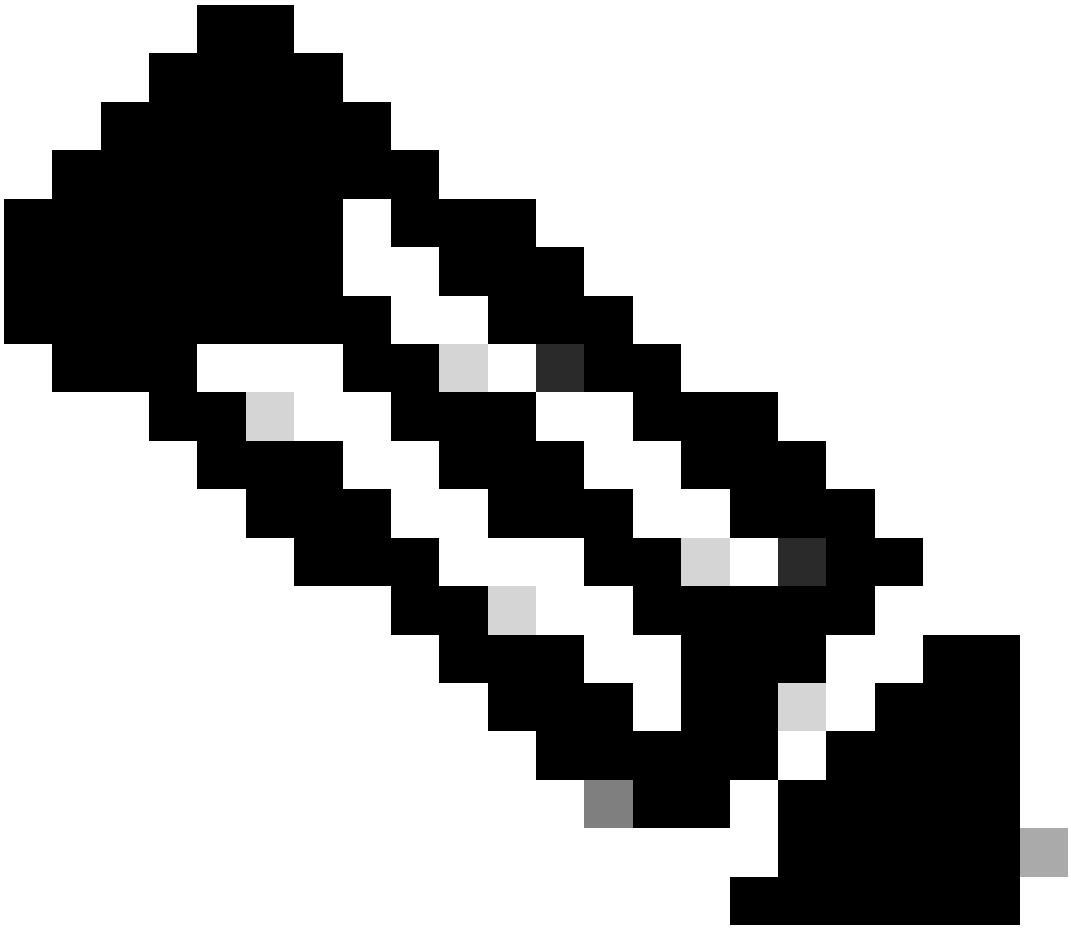
1. Faça logon no portal do Azure.

2. Na barra de pesquisa, navegue até Aplicativo Empresarial > Selecionar Aplicativo Empresarial configurado > Clique em configurar logon único.

3. Clique em Upload do arquivo de metadados na parte superior da página e carregue o arquivo sp.xml baixado do SNA Manager.

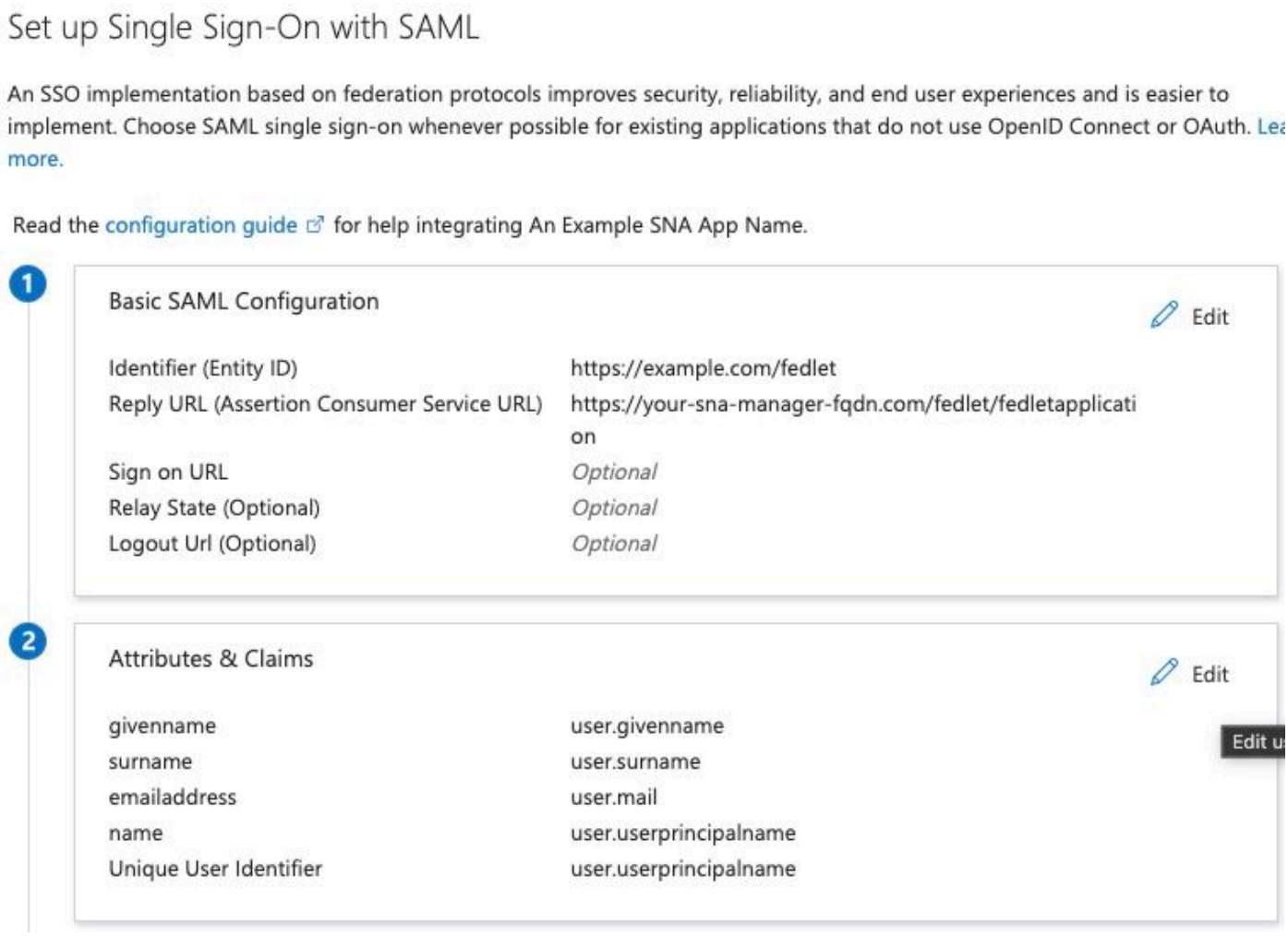
4. Ele abre a tela "Configuração SAML básica" e define várias configurações para corrigir valores, Clique em Salvar.





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.



6. Clique no valor user.userprincipalname na seção Nome da reivindicação.

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

Microsoft Azure

Search

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

Manage claim ...

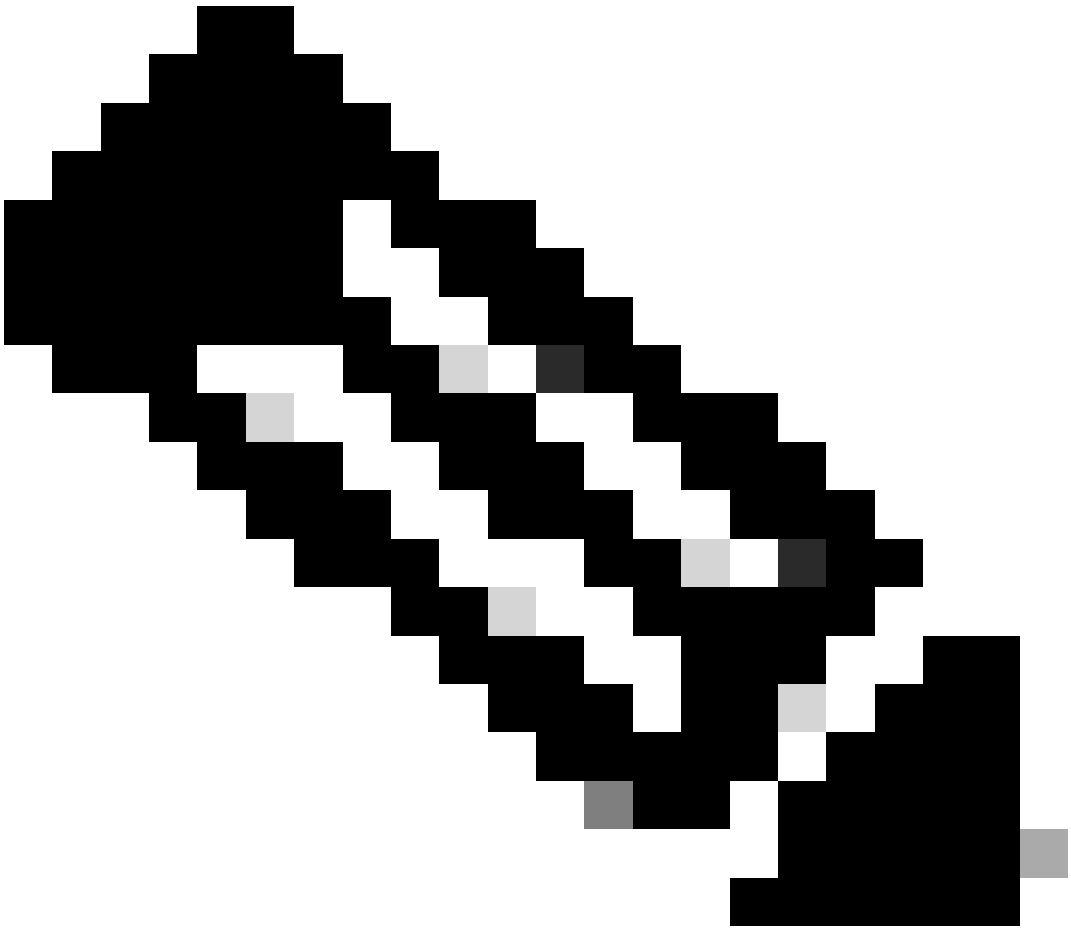
Save | Discard changes | Got feedback?

Name: nameidentifier

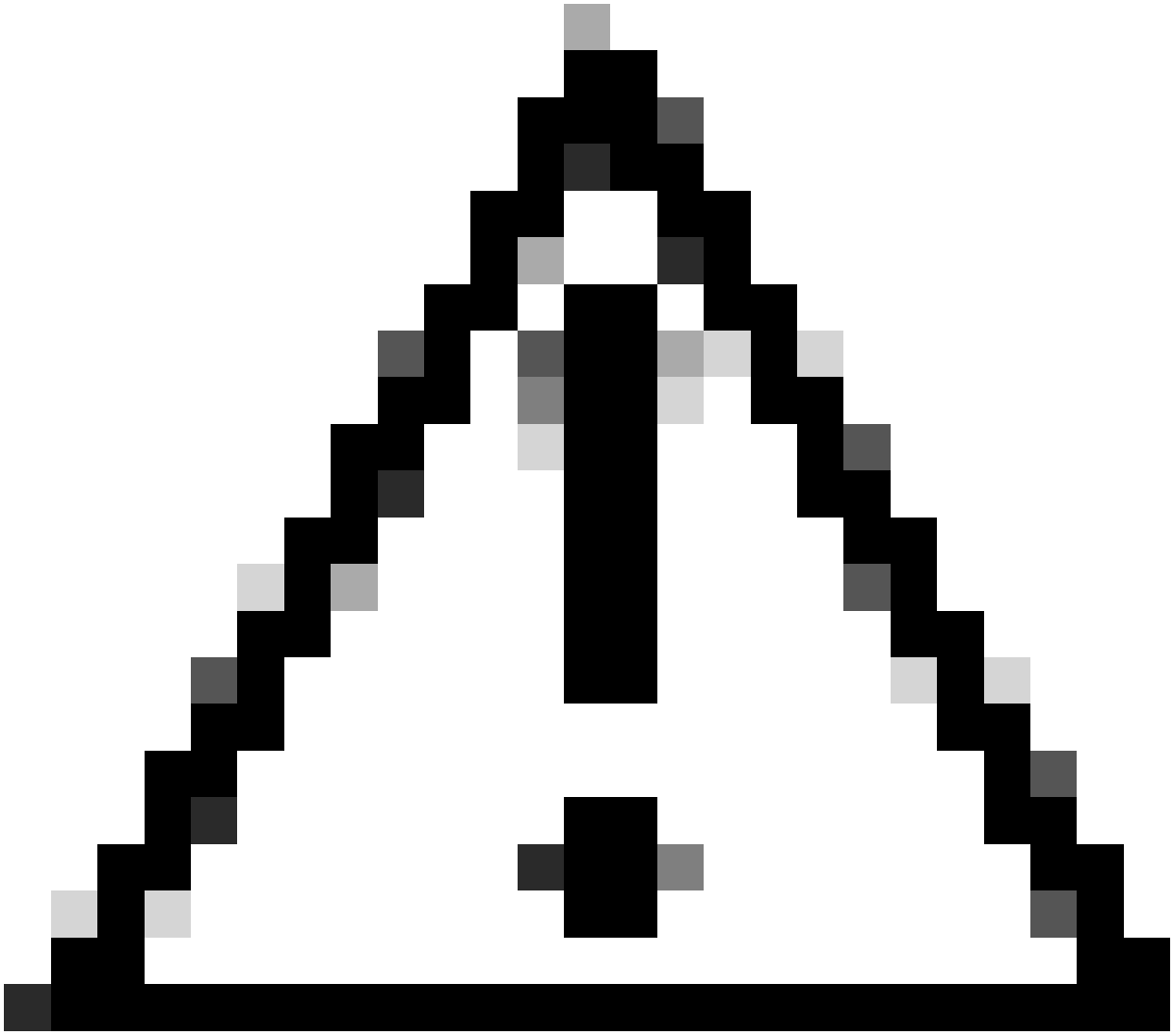
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

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.

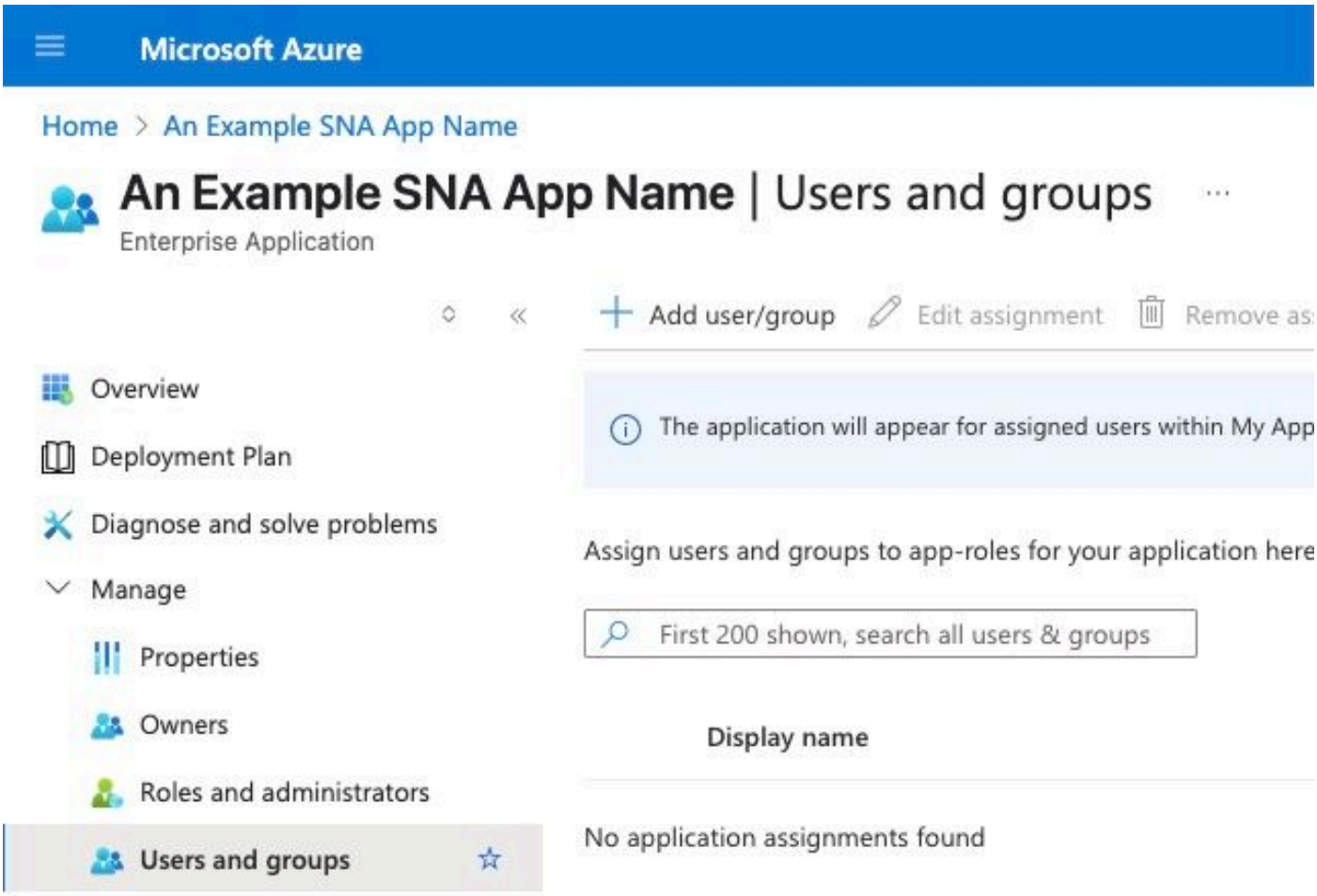


Caution: Esse é o local mais comum para encontrar problemas. As configurações no Gerenciador SNA e no Microsoft Azure devem ser correspondentes. se você optou por usar o formato "emailAddress" em SNA, o formato aqui também deve ser "Email Address".

Configurar usuários na ID do Entra.

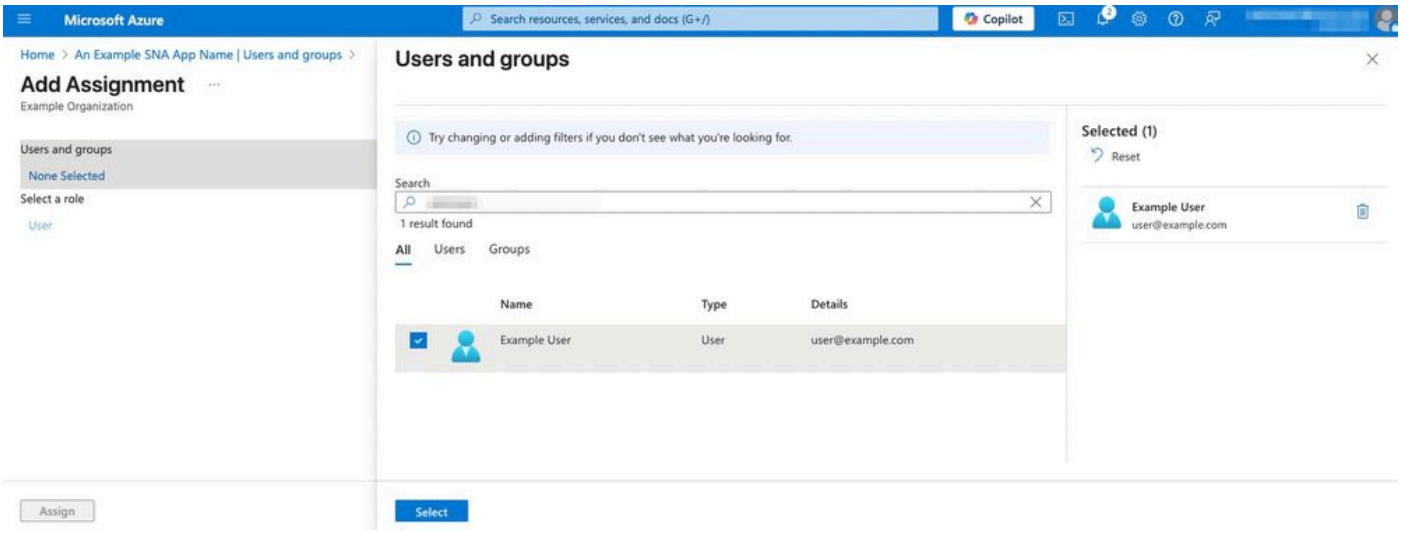
1. Faça logon no portal do Azure.

2. Na barra de pesquisa, navegue até Aplicativo Empresarial > Selecionar Aplicativo Empresarial configurado > selecione Usuários e Grupos à esquerda > clique em Adicionar usuário/grupo.



3. No painel esquerdo, clique em Nenhum Selecionado.

4. Pesquise e adicione o usuário necessário ao aplicativo.

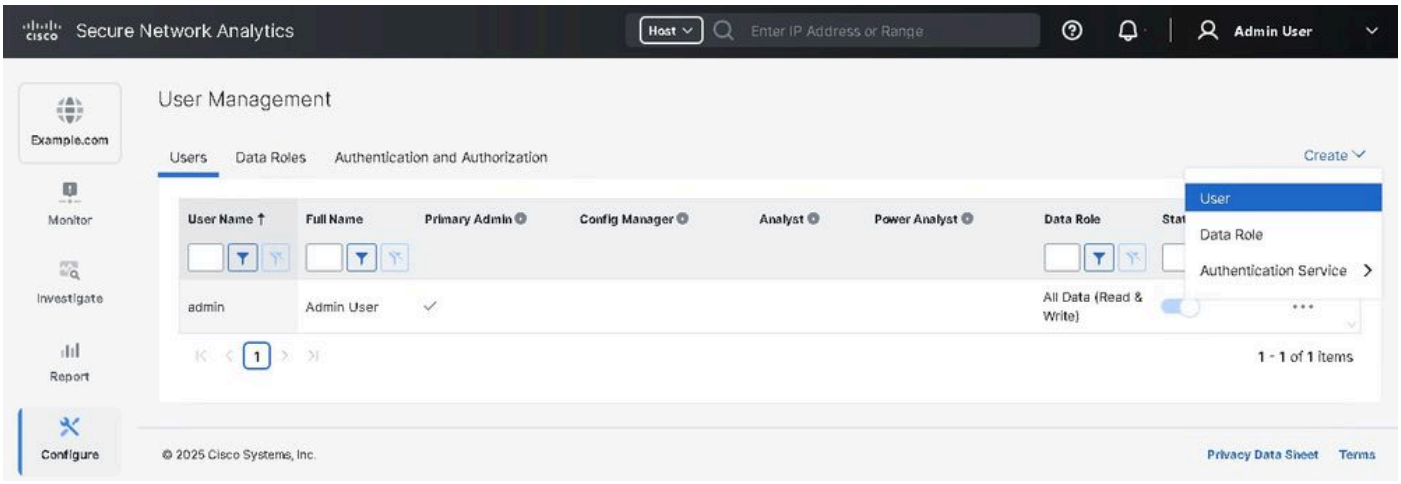


Configurar SSO em SNA

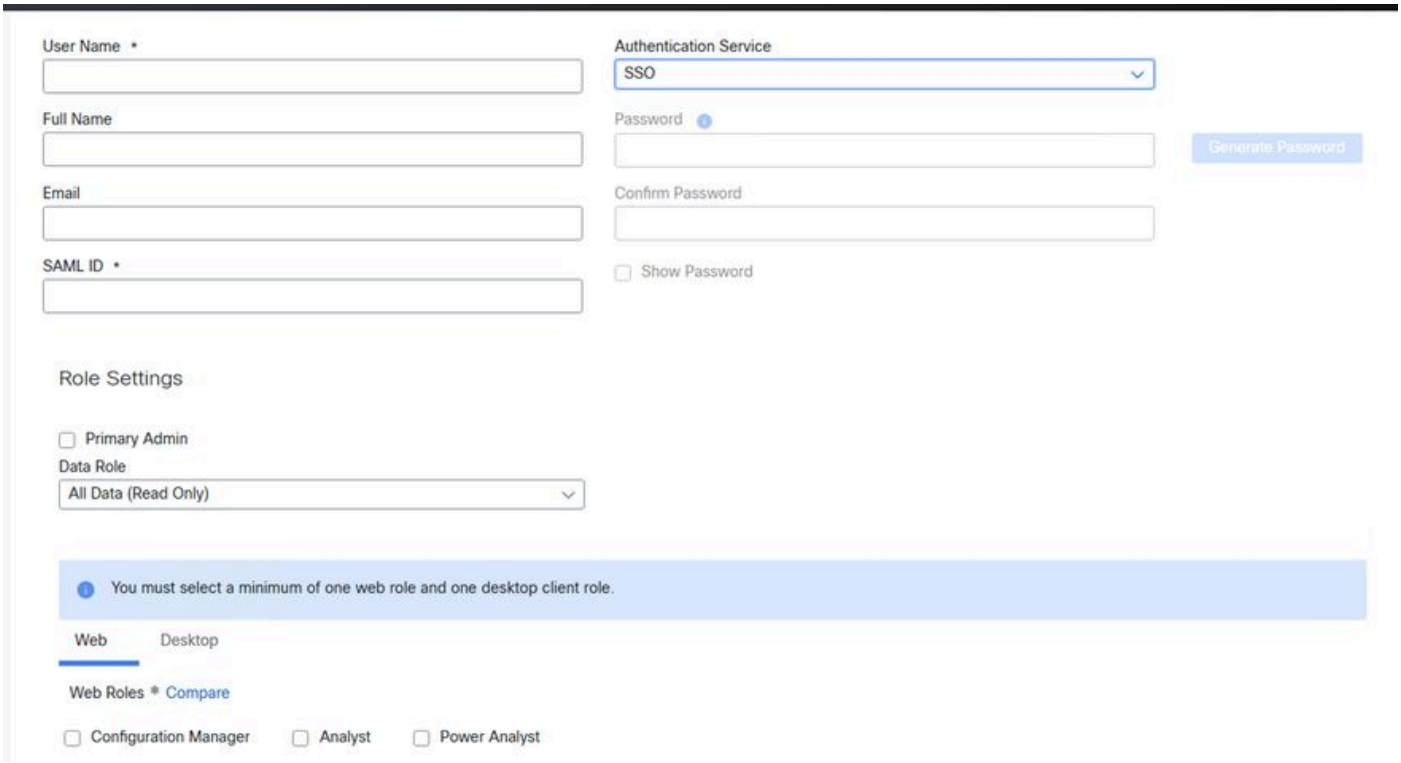
1. Faça login na interface do usuário do SNA Manager.

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.



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.