Configuración de SNA Manager para Microsoft Entra ID SSO

Contenido

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

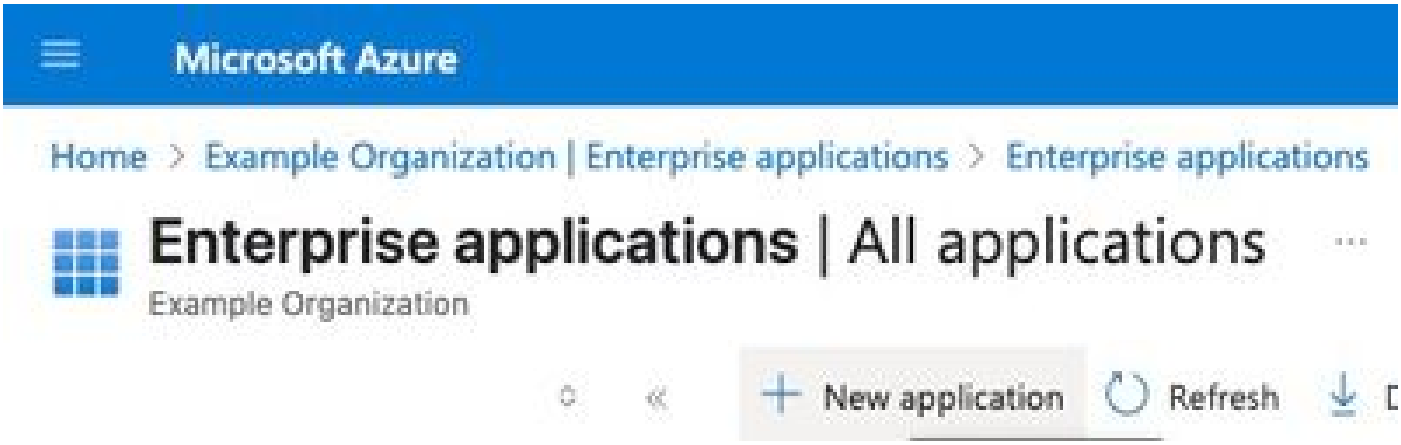
Configurar aplicación empresarial en Azure

1. Inicie sesión en el [portal de nube de Azure](#).

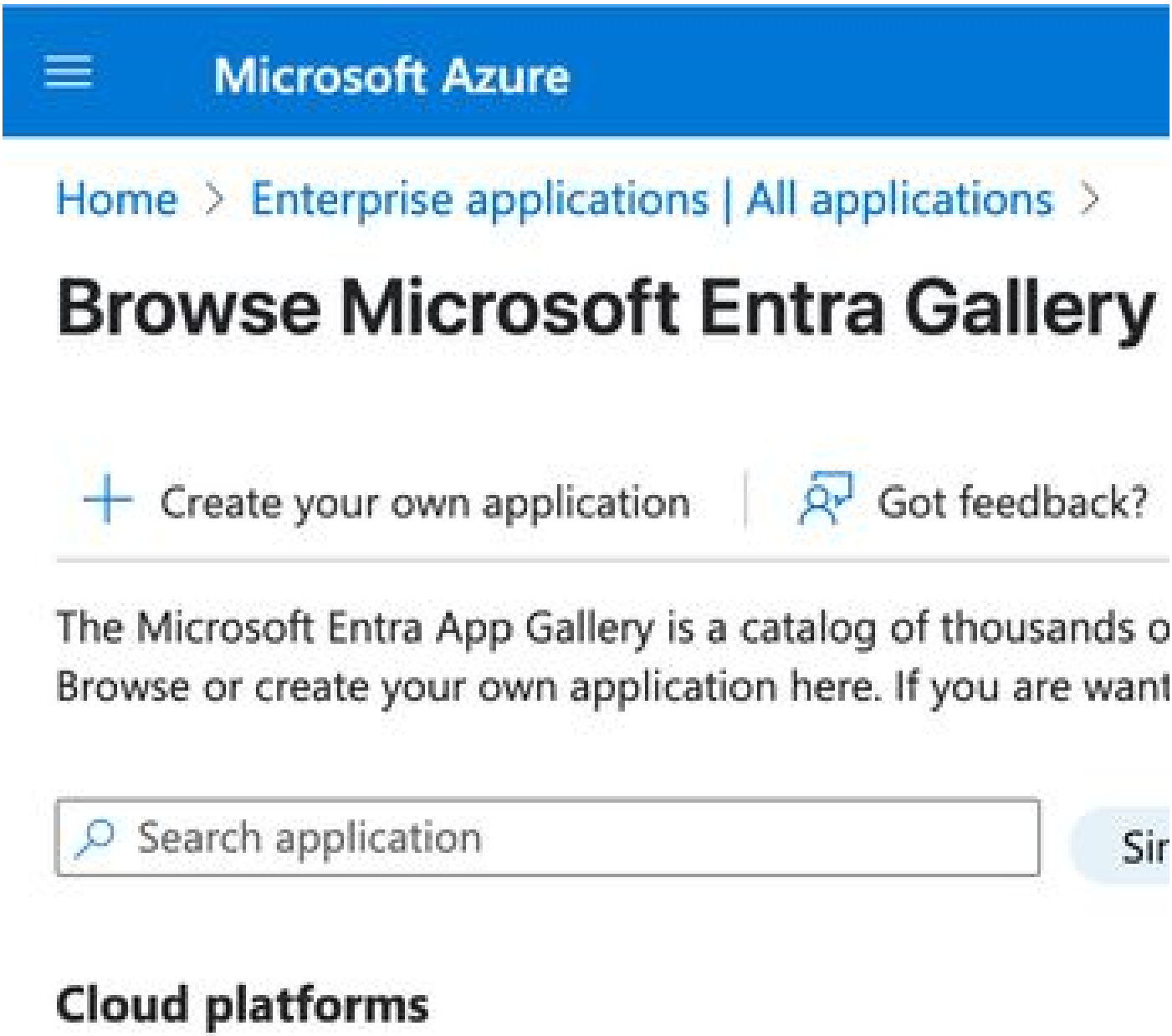
2. Busque el servicio Entra ID en el cuadro de búsqueda y seleccione Microsoft Entra ID.

3. En el panel izquierdo, expanda Administrar y seleccione Aplicaciones de empresa.

4. Haga clic en Nueva aplicación.



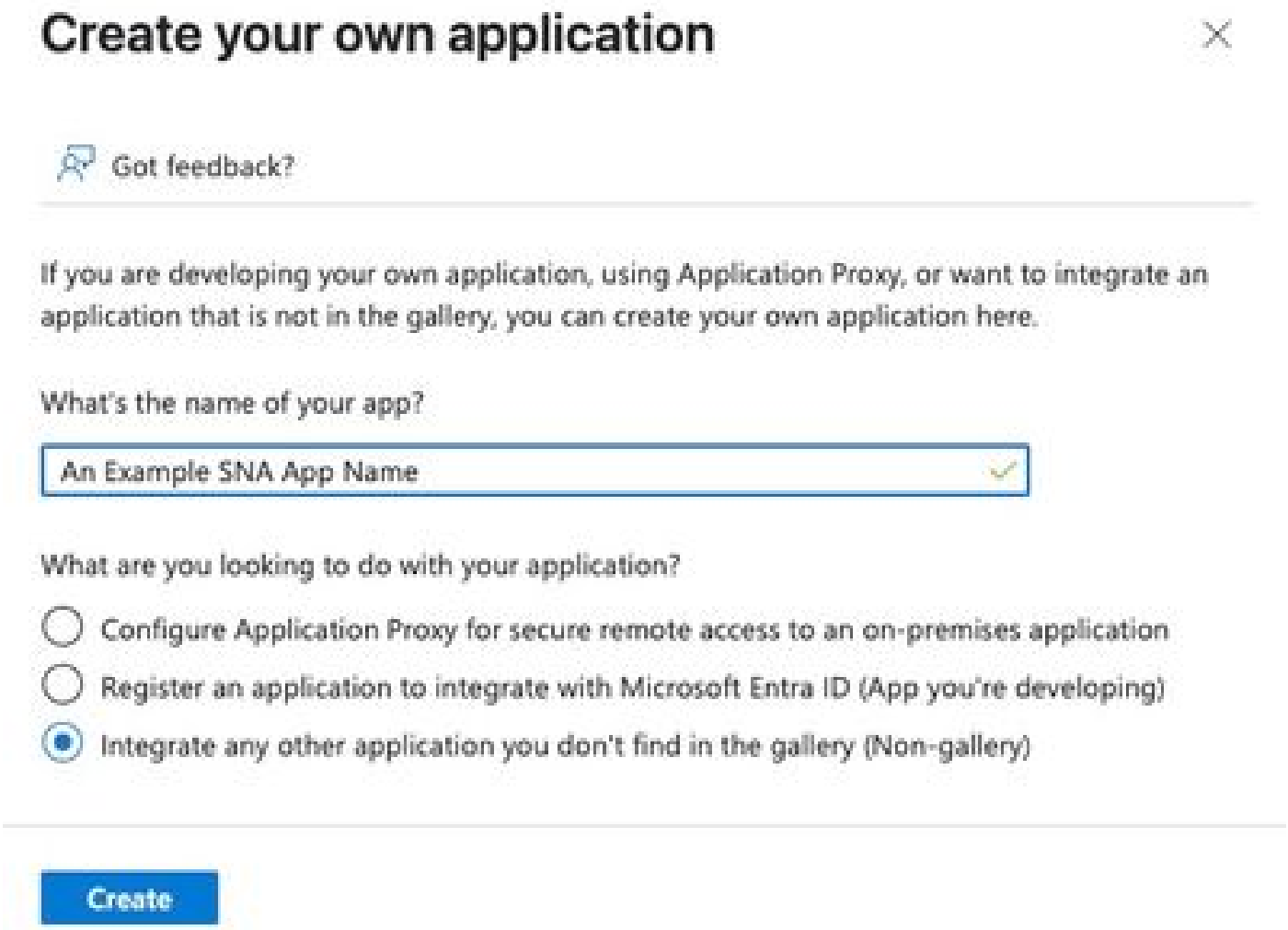
5. Seleccione Crear su propia aplicación en la nueva página que se carga.



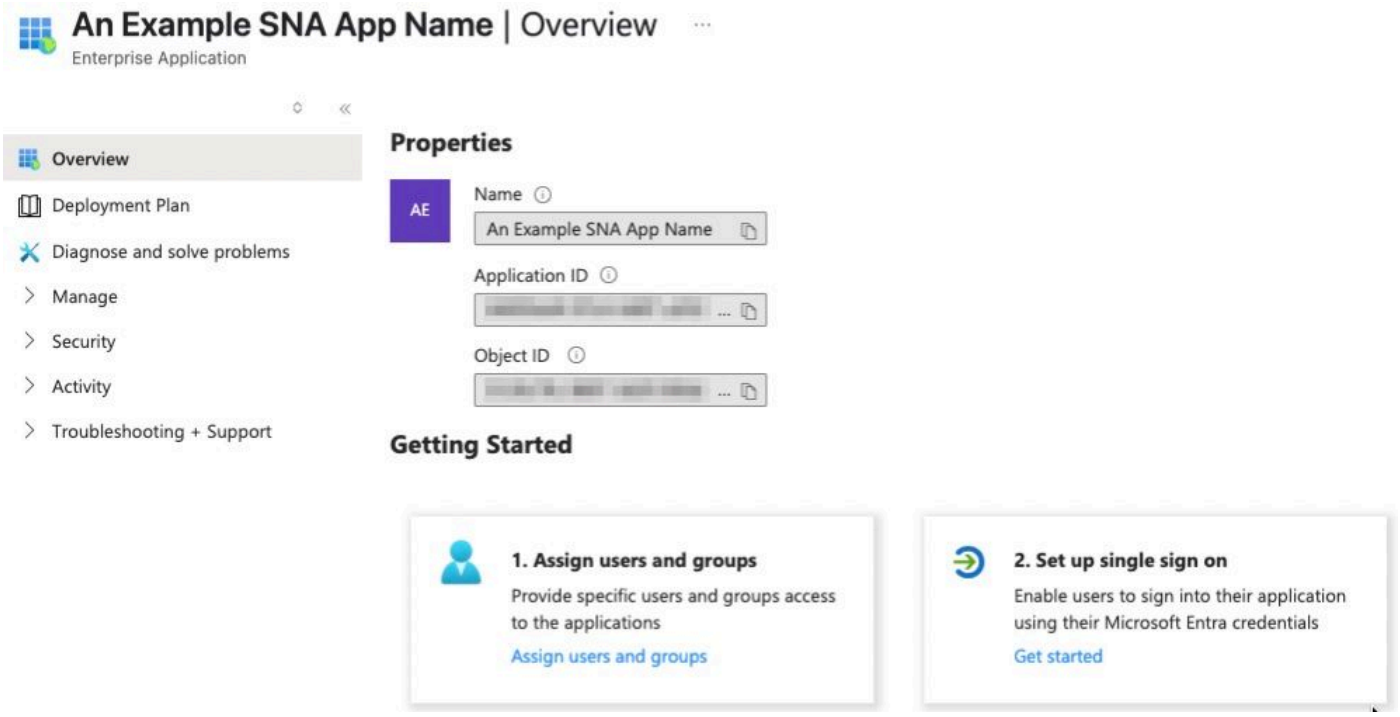
Azure-UI

6. Proporcione un nombre a la aplicación en ¿Cuál es el nombre de su aplicación? campo.

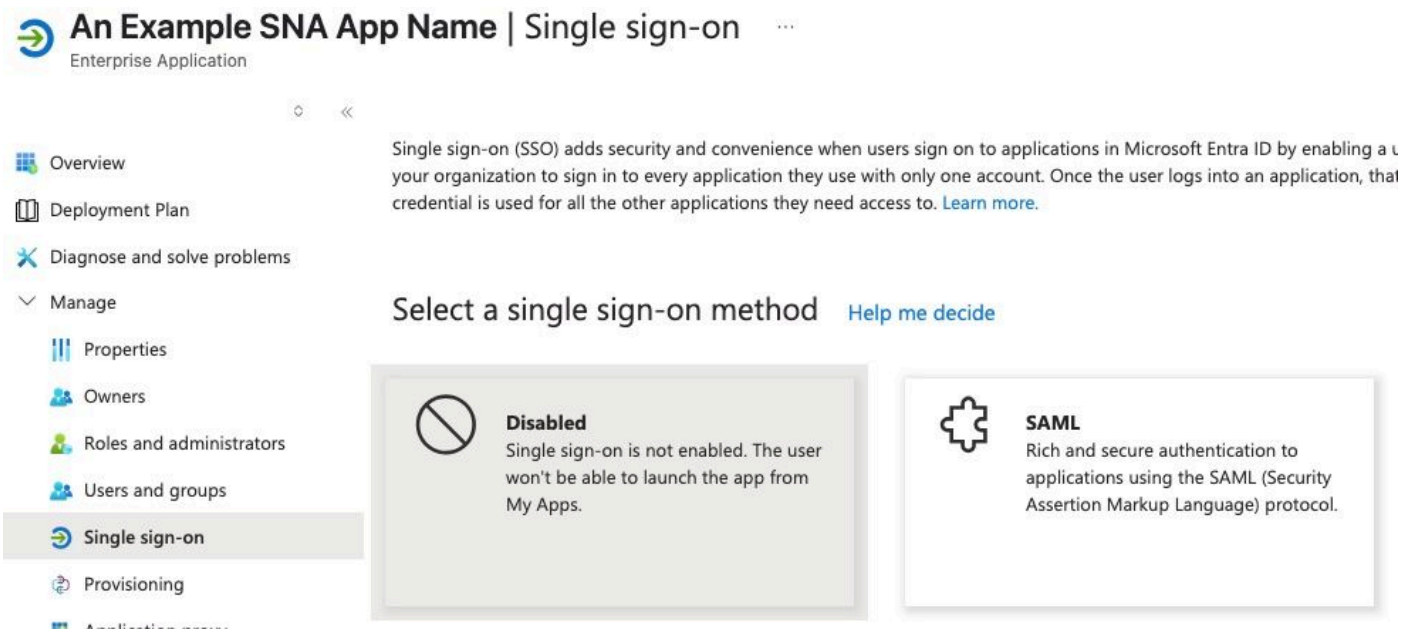
7. Seleccione el botón de opción Integrar cualquier otra aplicación que no encuentre en la galería (No galería) y haga clic en Crear.



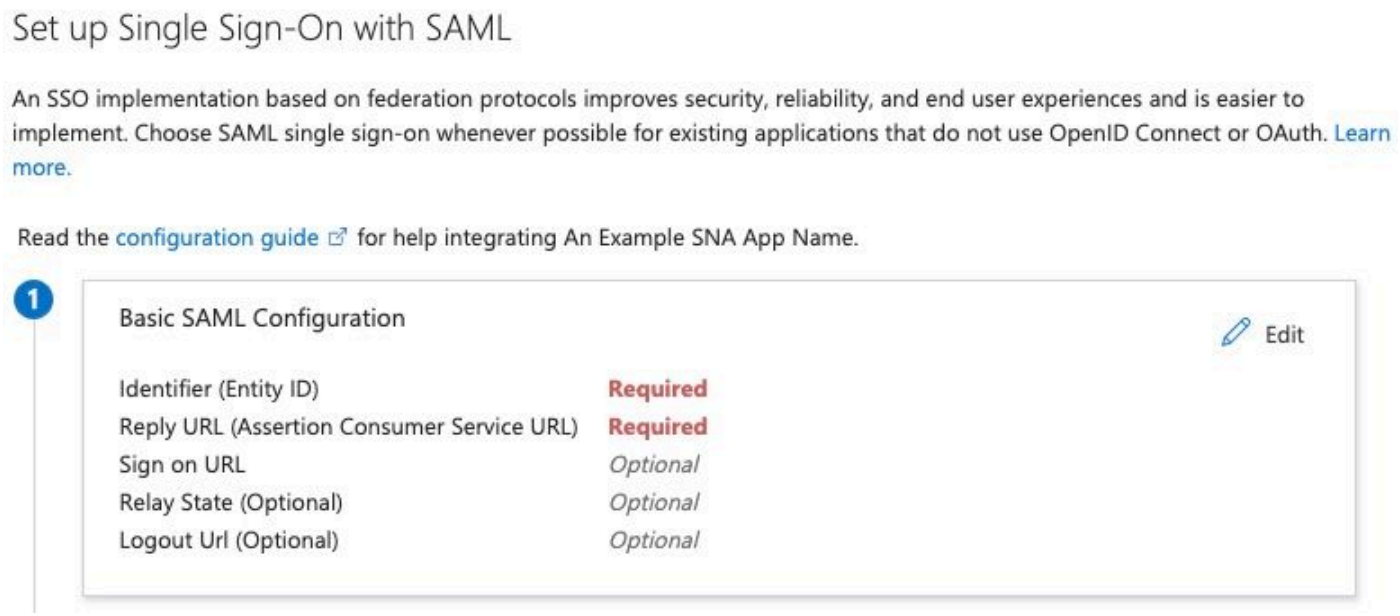
8. En el panel de aplicaciones recién configurado, haga clic en Configurar inicio de sesión único.



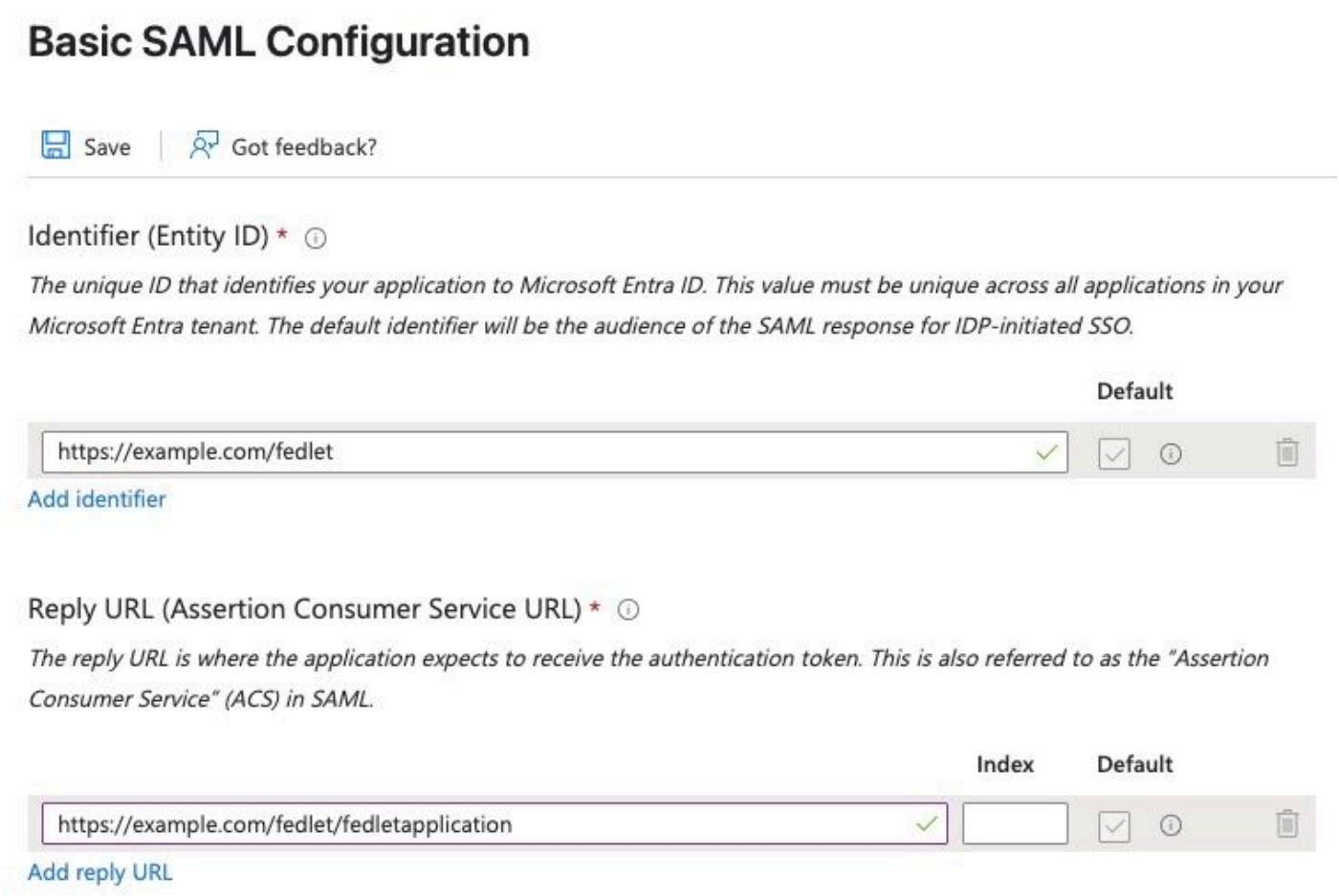
9. Seleccione SAML.



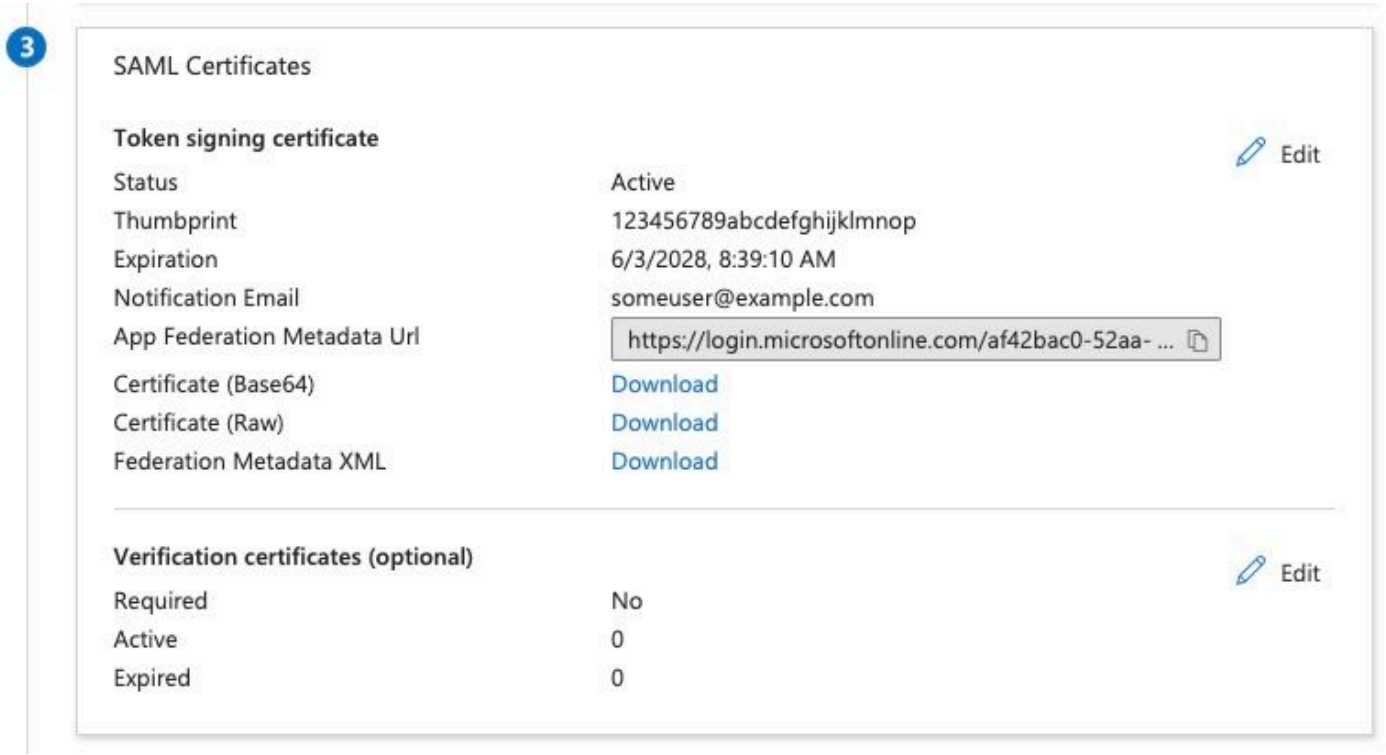
10. En la página Configurar el inicio de sesión único con SAML, haga clic en Editar en Configuración básica de SAML.



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.

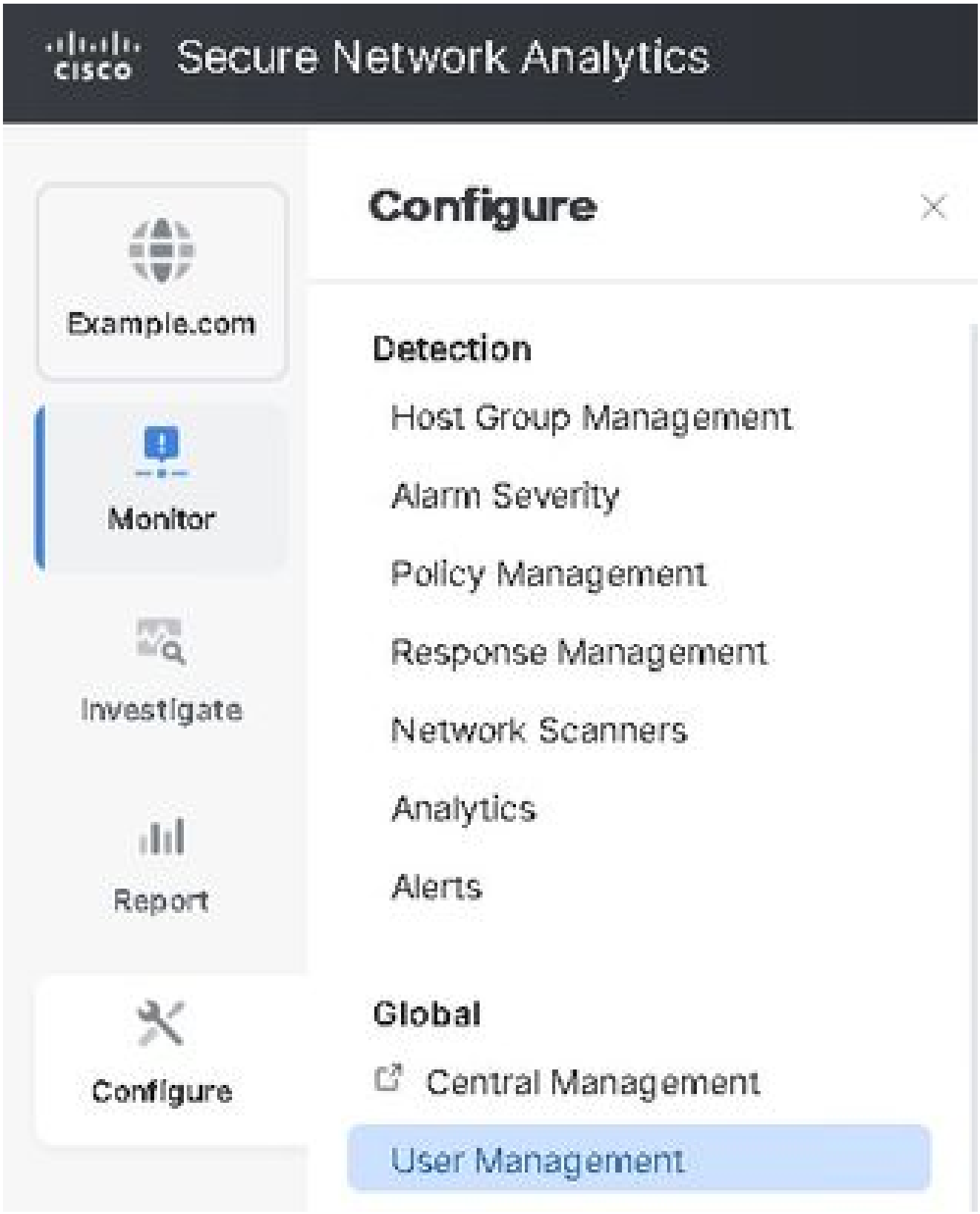


12. Localice la tarjeta de certificados SAML y guarde el valor del campo URL de metadatos de federación de aplicaciones y descargue el XML de metadatos de federación.

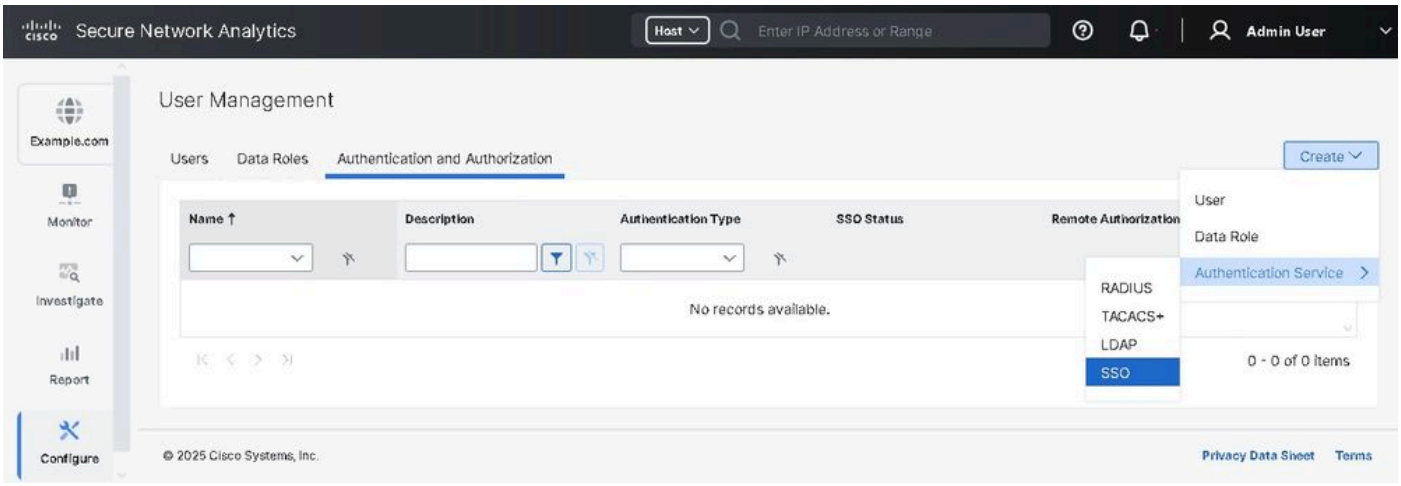


Configuración y descarga del archivo XML del proveedor de servicios en SNA

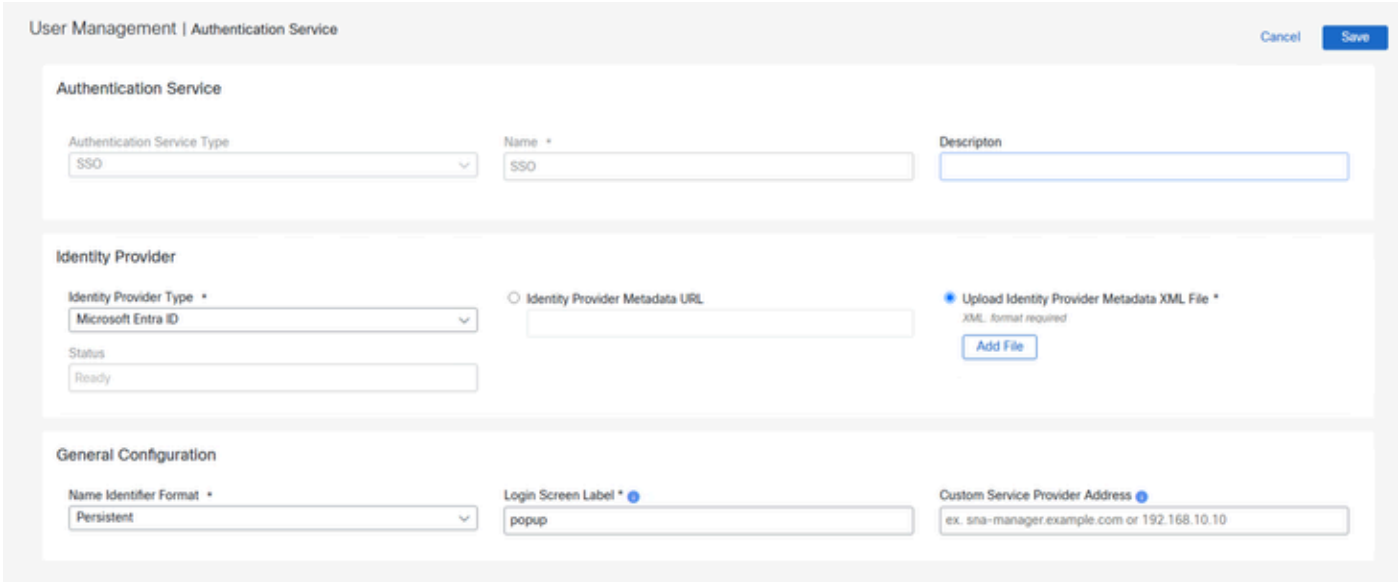
1. Inicie sesión en la interfaz de usuario del administrador SNA.
2. Vaya a Configure > Global > User Management.

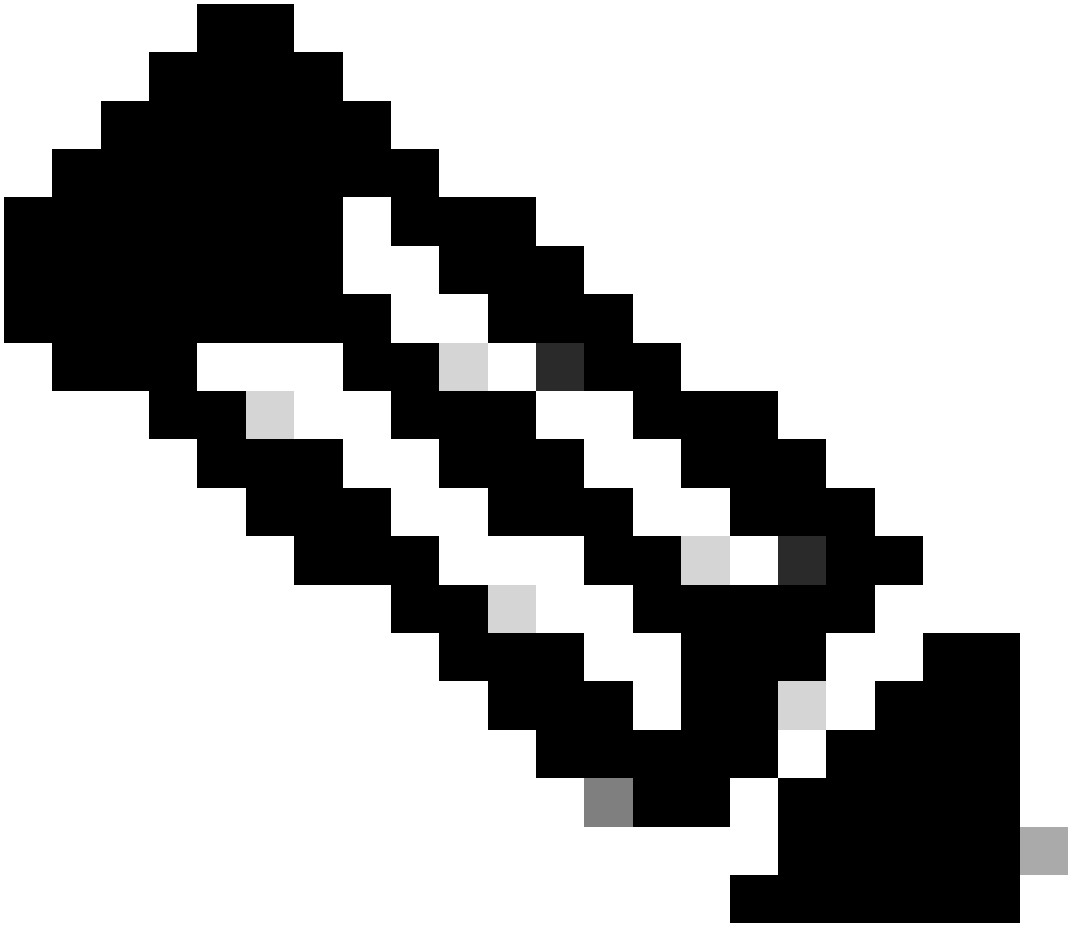


3. En la pestaña Authentication and Authorization, haga clic en Create > Authentication Service > SSO.



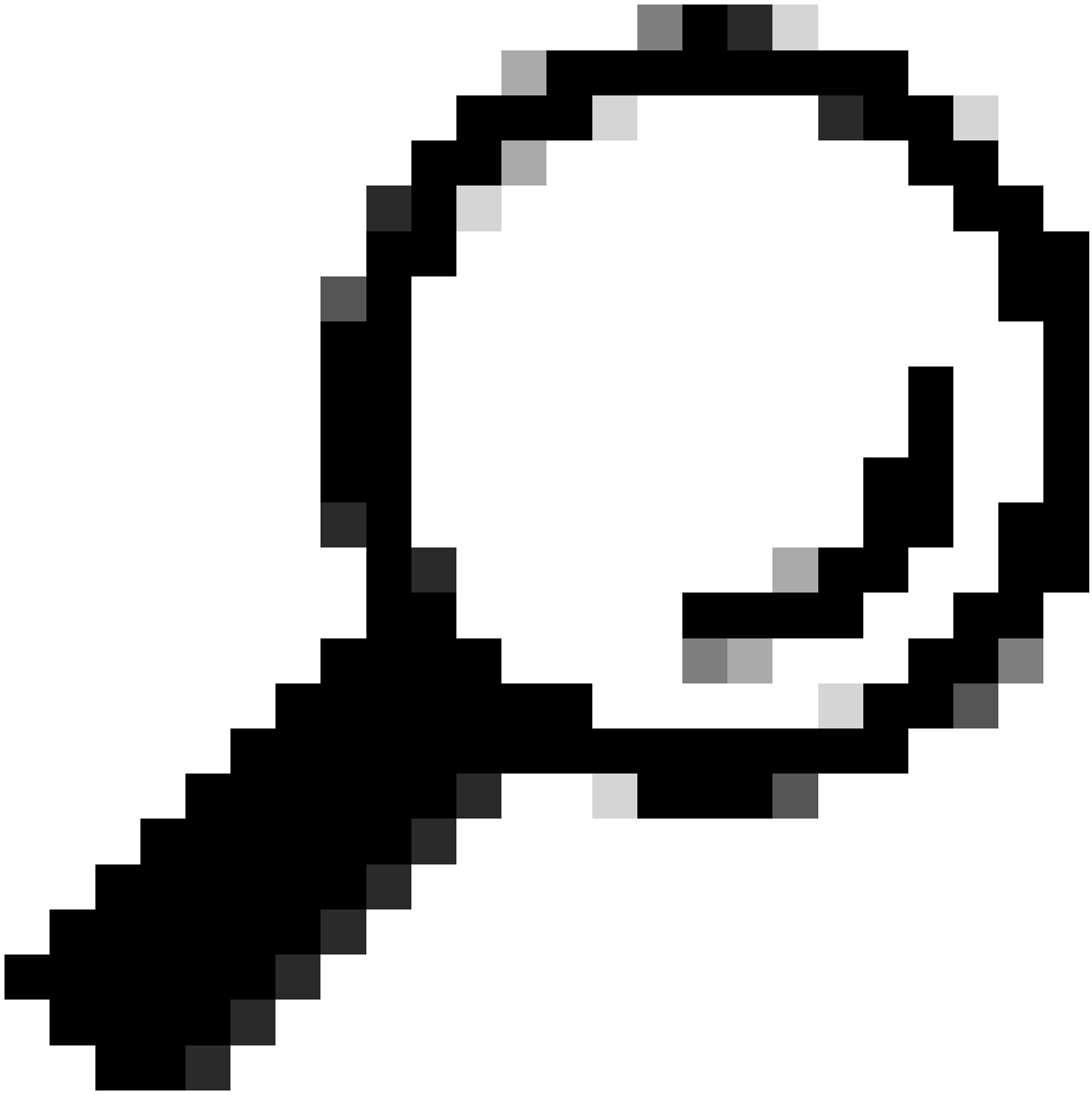
4. Seleccione el botón de opción correspondiente a URL de metadatos del proveedor de identidad o Cargar archivo XML de metadatos del proveedor de identidad.





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

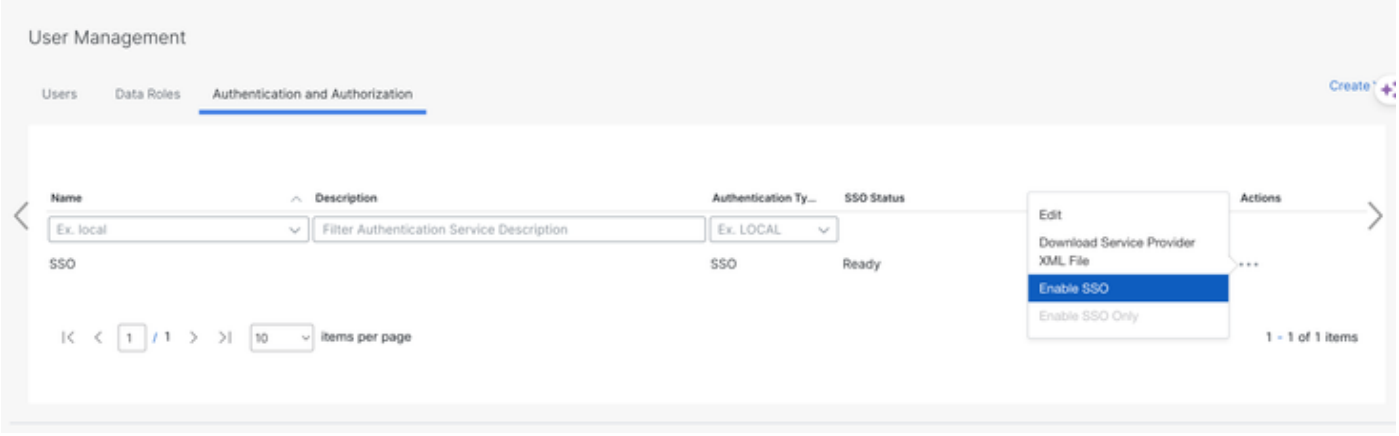
5. Configure el campo Tipo de proveedor de identidad a Microsoft Entry ID, Name Identifier Format a Persistent, Escriba una etiqueta de pantalla de inicio de sesión.



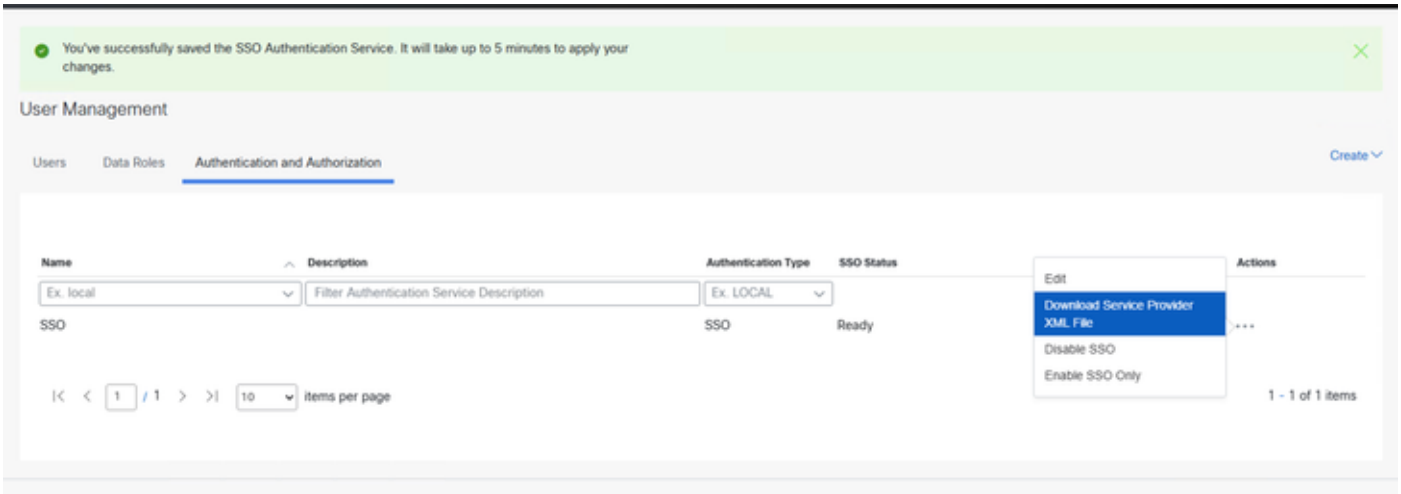
Consejo: La etiqueta de la pantalla de inicio de sesión configurada (nombre/texto) se muestra encima del botón Iniciar sesión con SSO y no debe dejarse vacía.

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.



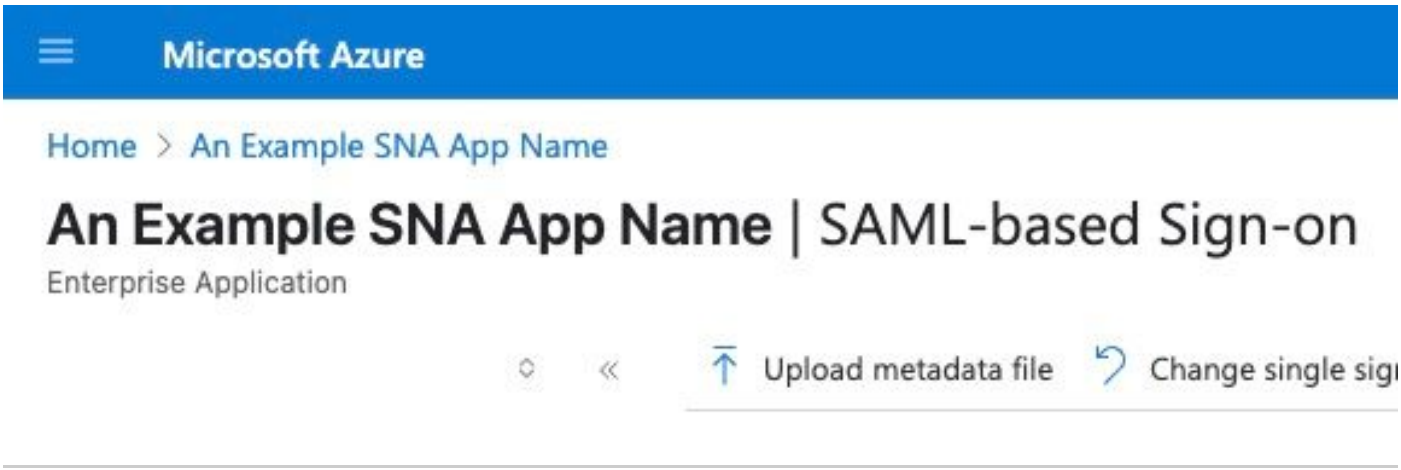
Configurar SSO en Azure

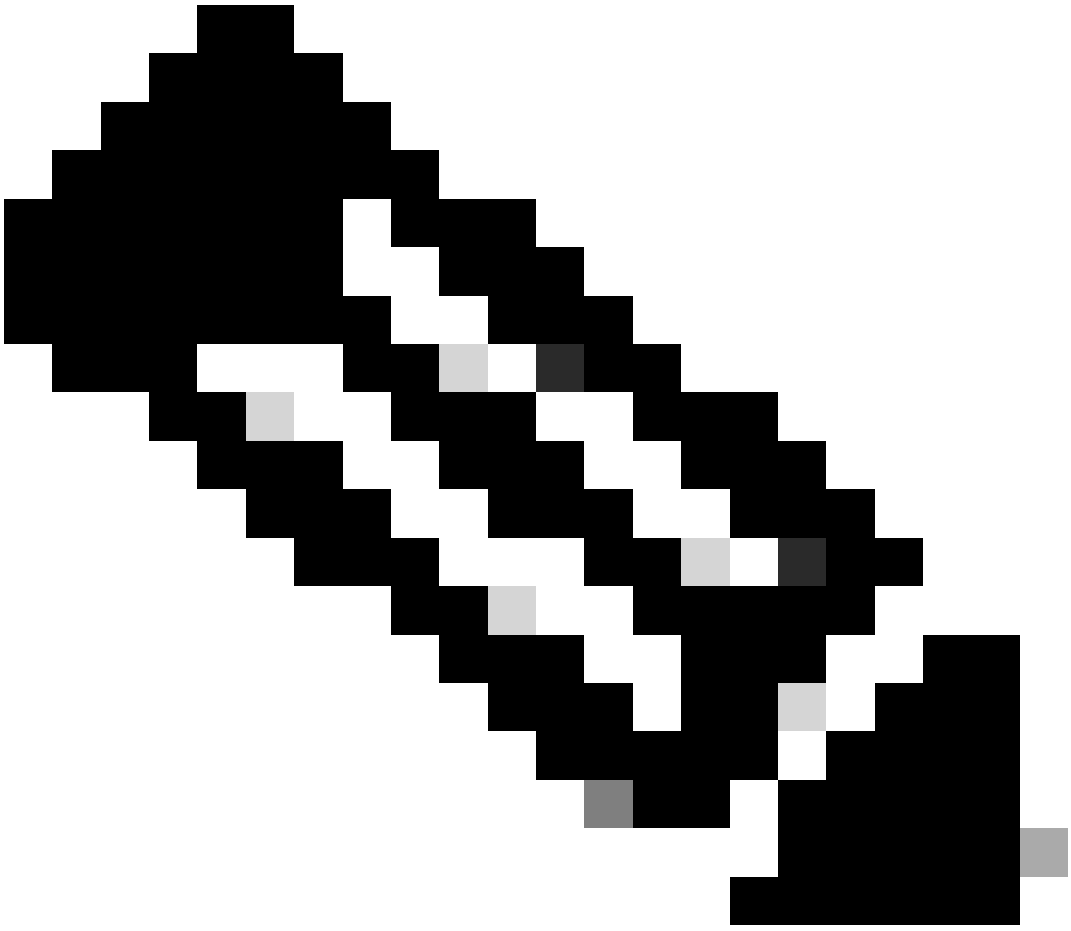
1. Inicie sesión en el portal de Azure.

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.

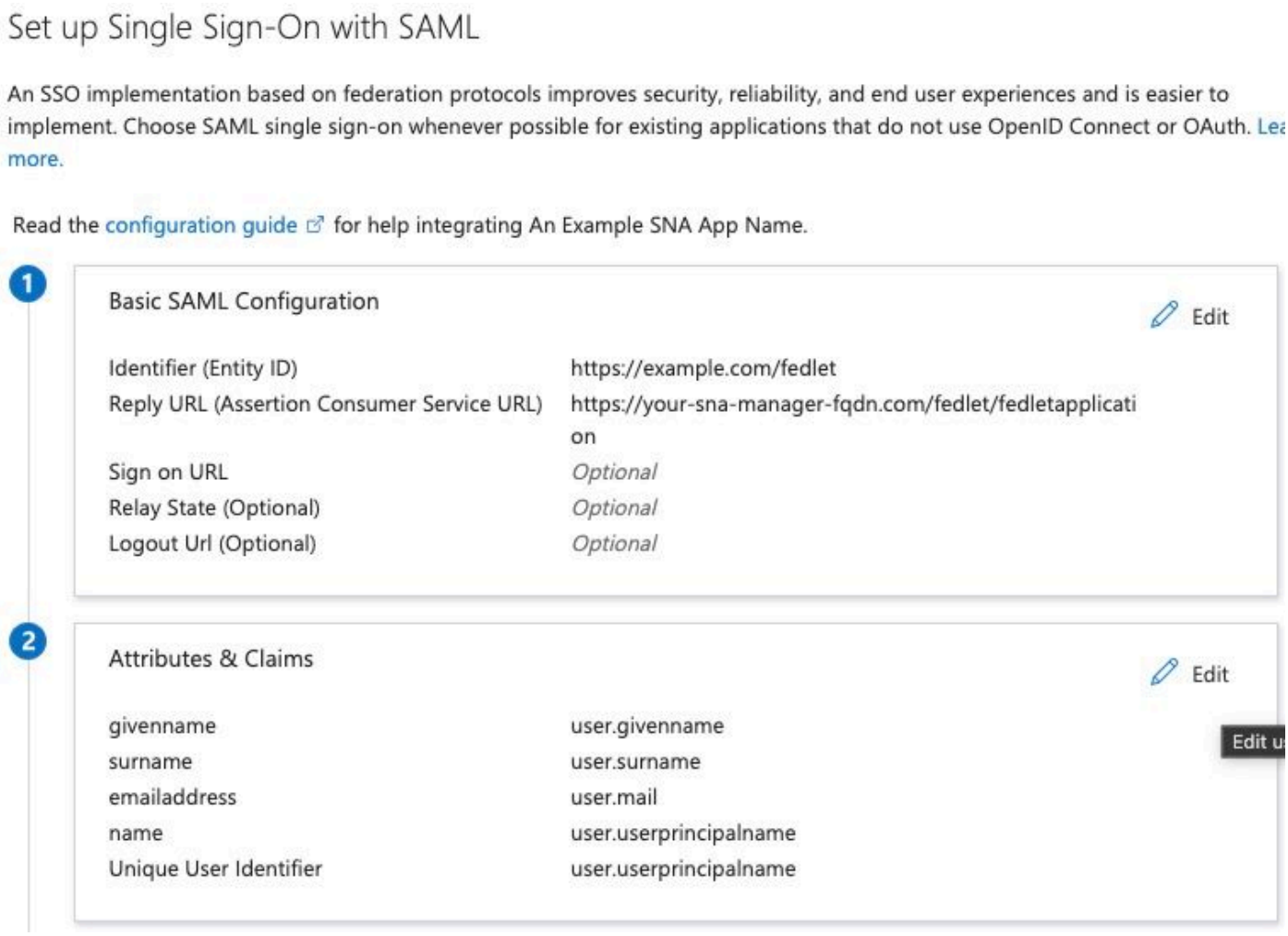
4. Se abre la pantalla "Basic SAML Configuration" y establece varios ajustes para corregir los valores, haga clic en Guardar.





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.



6. Haga clic en el valor user.userprincipalname en la sección Nombre de reclamación.

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

Microsoft Azure

Search

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

Manage claim ...

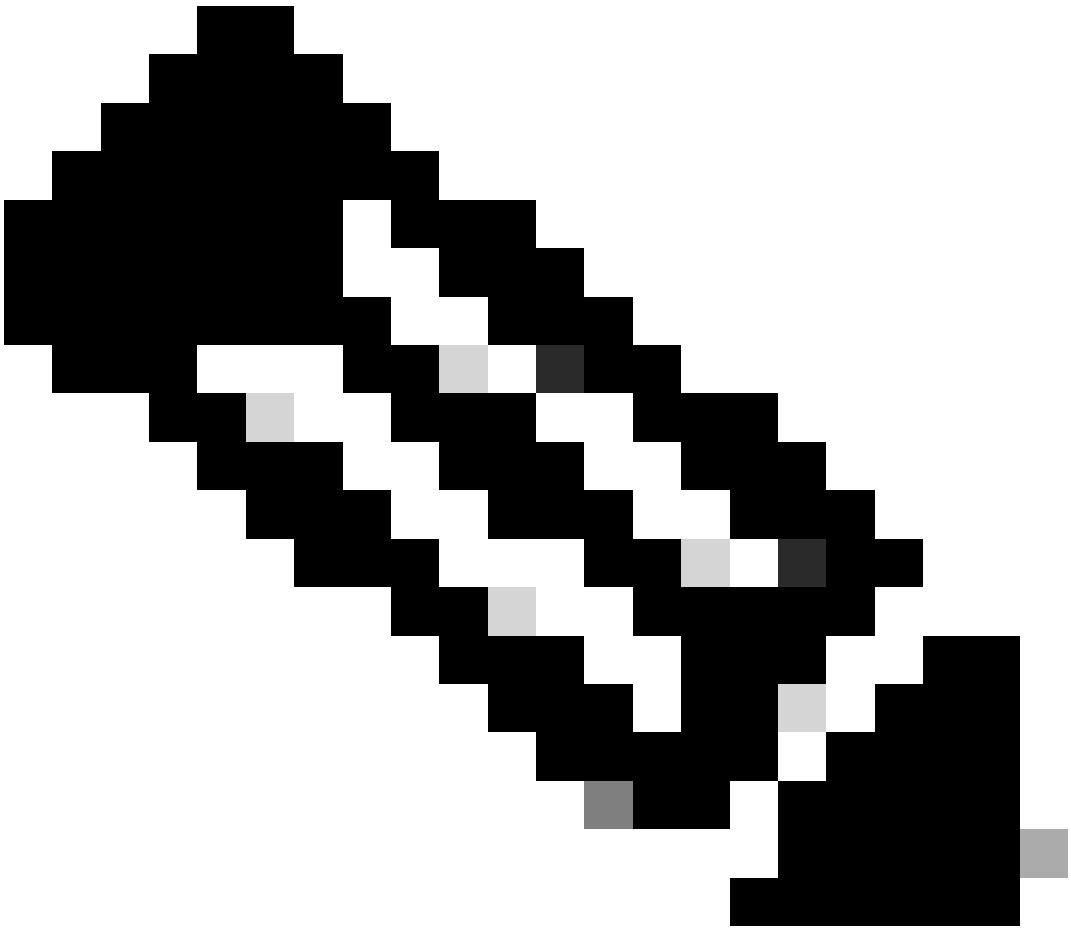
Save | Discard changes | Got feedback?

Name: nameidentifier

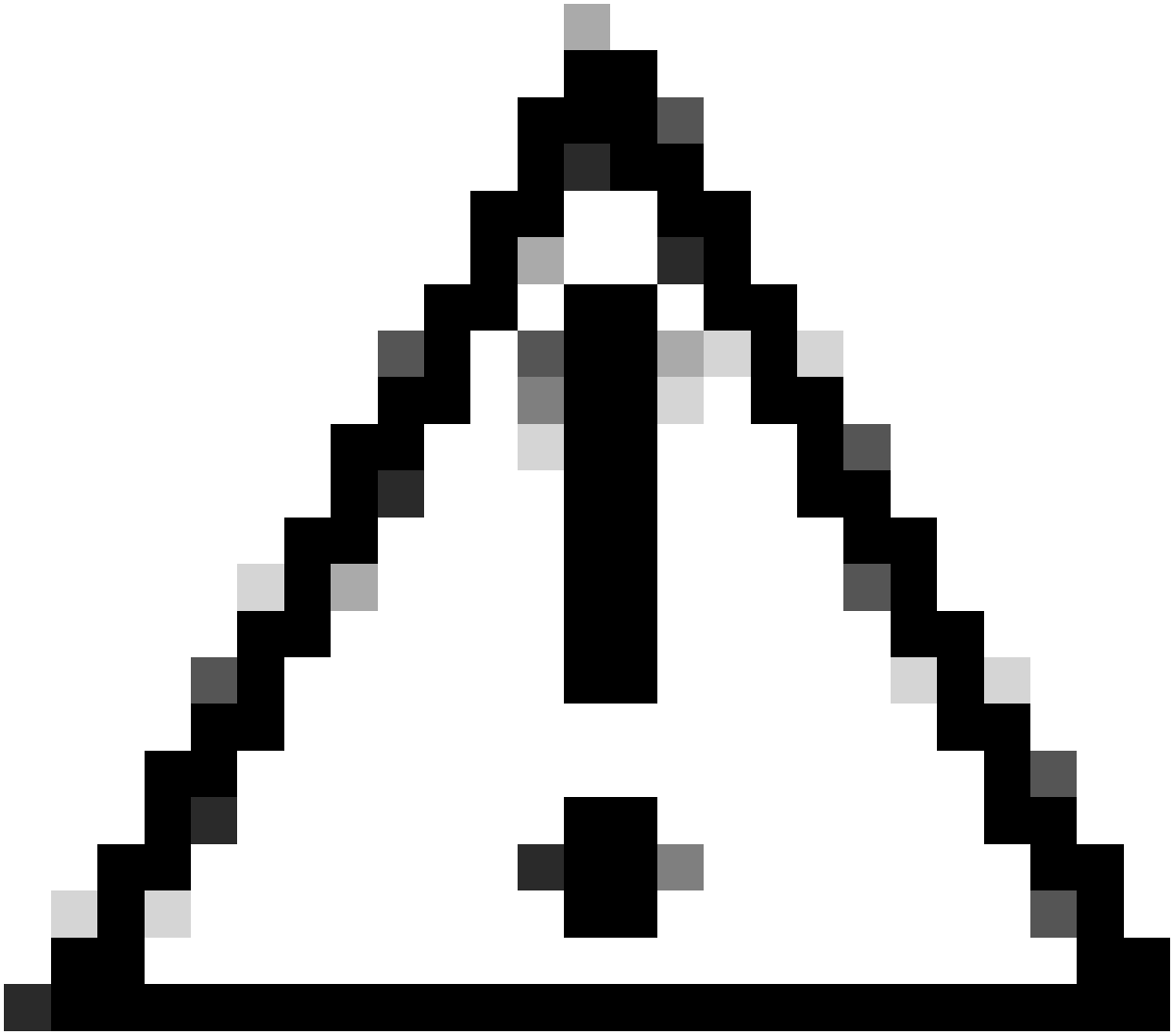
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Persistent



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.

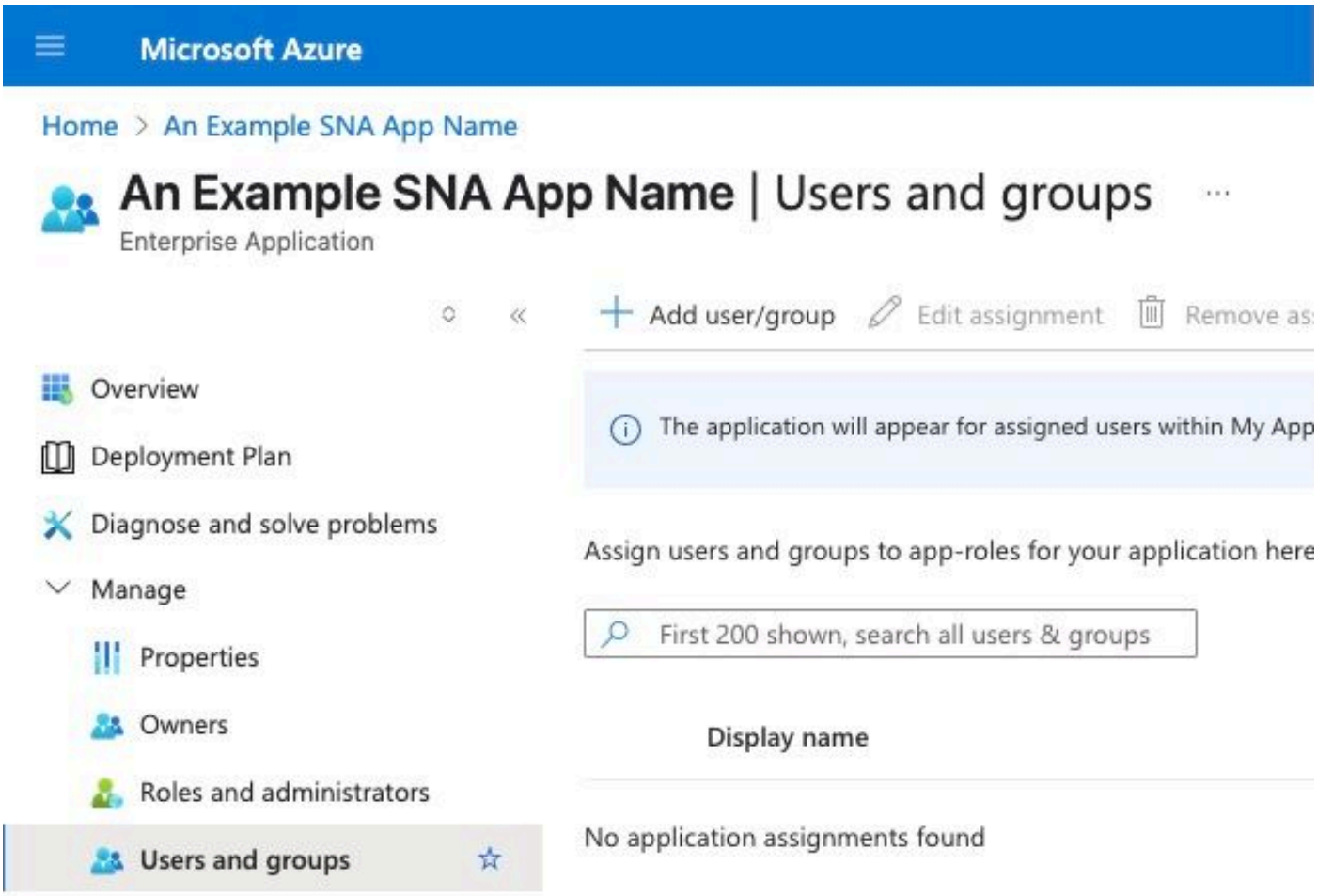


Precaución: Este es el lugar más común para encontrar problemas. La configuración del Administrador SNA y Microsoft Azure debe coincidir. si ha optado por utilizar el formato "emailAddress" en SNA, el formato aquí también debe ser "Email Address".

Configuración de usuarios en ID de entrada.

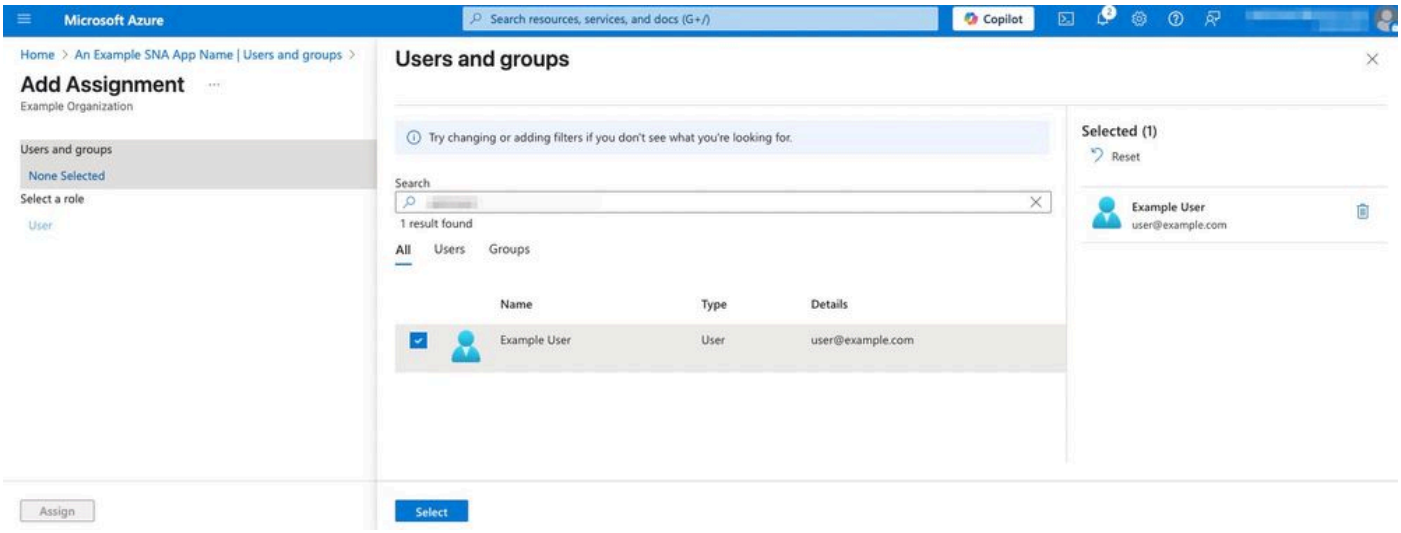
1. Inicie sesión en el portal de Azure.

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.



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

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

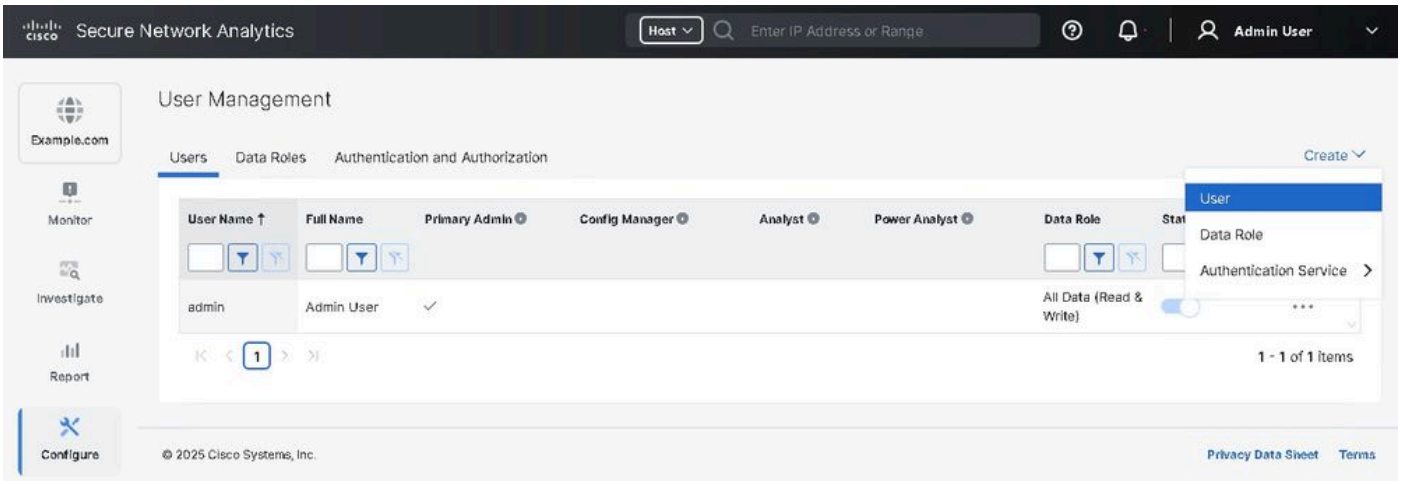


Configuración de SSO en SNA

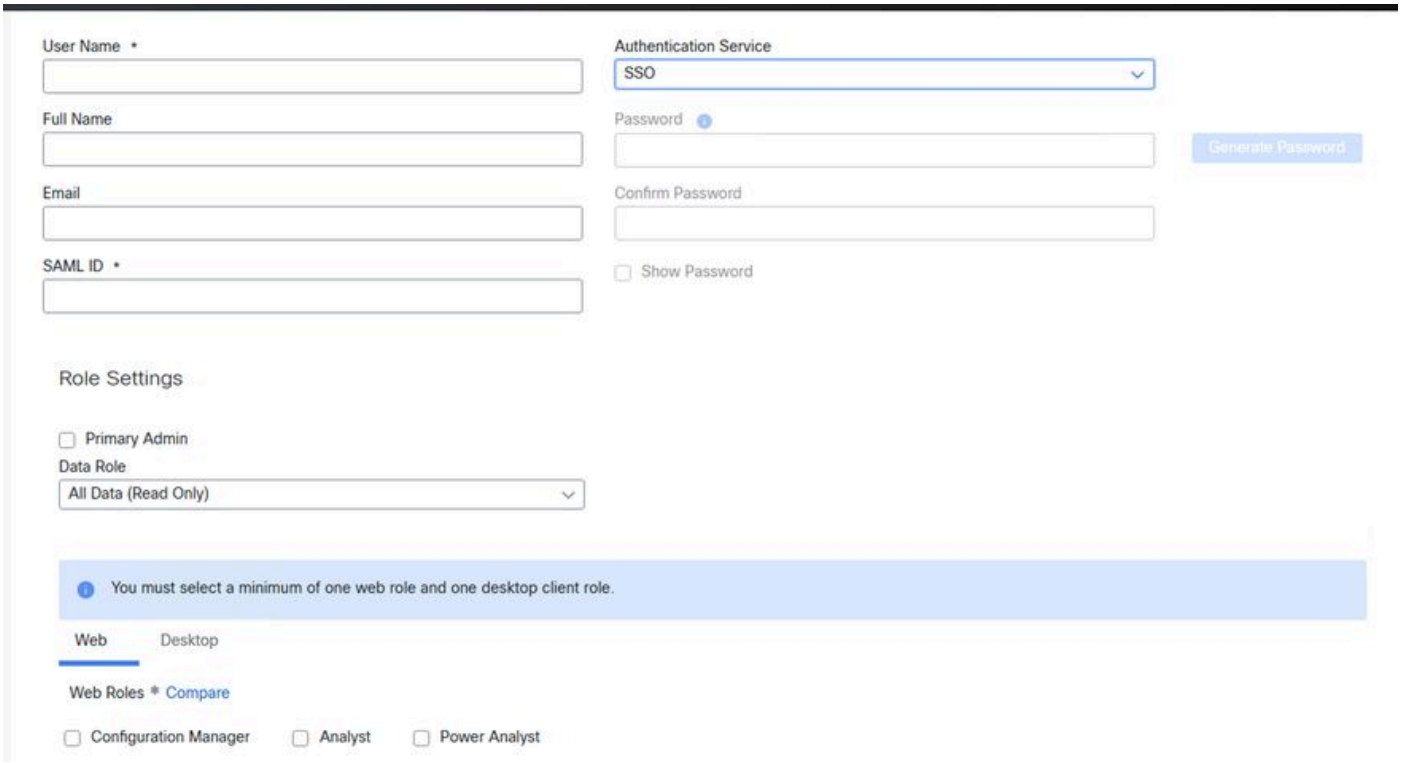
1. Inicie sesión en la interfaz de usuario del administrador SNA.

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).