Configuración del flujo de inicio de sesión de administrador de ISE 3.1 mediante SSO de SAML con Azure AD

Contenido

Introducción

Este documento describe cómo configurar la integración SSO SAML de Cisco ISE 3.1 con un

proveedor de identidad externo como Azure Active Directory (AD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

1. Cisco ISE 3.1
2. implementaciones SSO de SAML
3. Azure AD

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

1. Cisco ISE 3.1
2. Azure AD

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.

Antecedentes

TÉRMINOS:

Proveedor de identidad (IdP):

la autoridad de Azure AD que comprueba y afirma la identidad de un usuario y los privilegios de acceso a un recurso solicitado (el proveedor de servicios).

Proveedor de servicios (SP):

el recurso o servicio alojado al que el usuario pretende acceder (ISE Application Server).

SAML

El Lenguaje de marcado de aserción de seguridad (SAML) es un estándar abierto que permite IdP para pasar credenciales de autorización al SP.

Las transacciones SAML utilizan el Lenguaje de marcado extensible (XML) para las comunicaciones estandarizadas entre el proveedor de identidad y los proveedores de servicios.

SAML es el link entre la autenticación de una identidad de usuario y la autorización para utilizar

un servicio.

Afirmación SAML

Una aserción SAML es el documento XML que el proveedor de identidad envía al proveedor de servicios que contiene la autorización de usuario.

Existen tres tipos diferentes de aserciones SAML: autenticación, atributo y decisión de autorización.

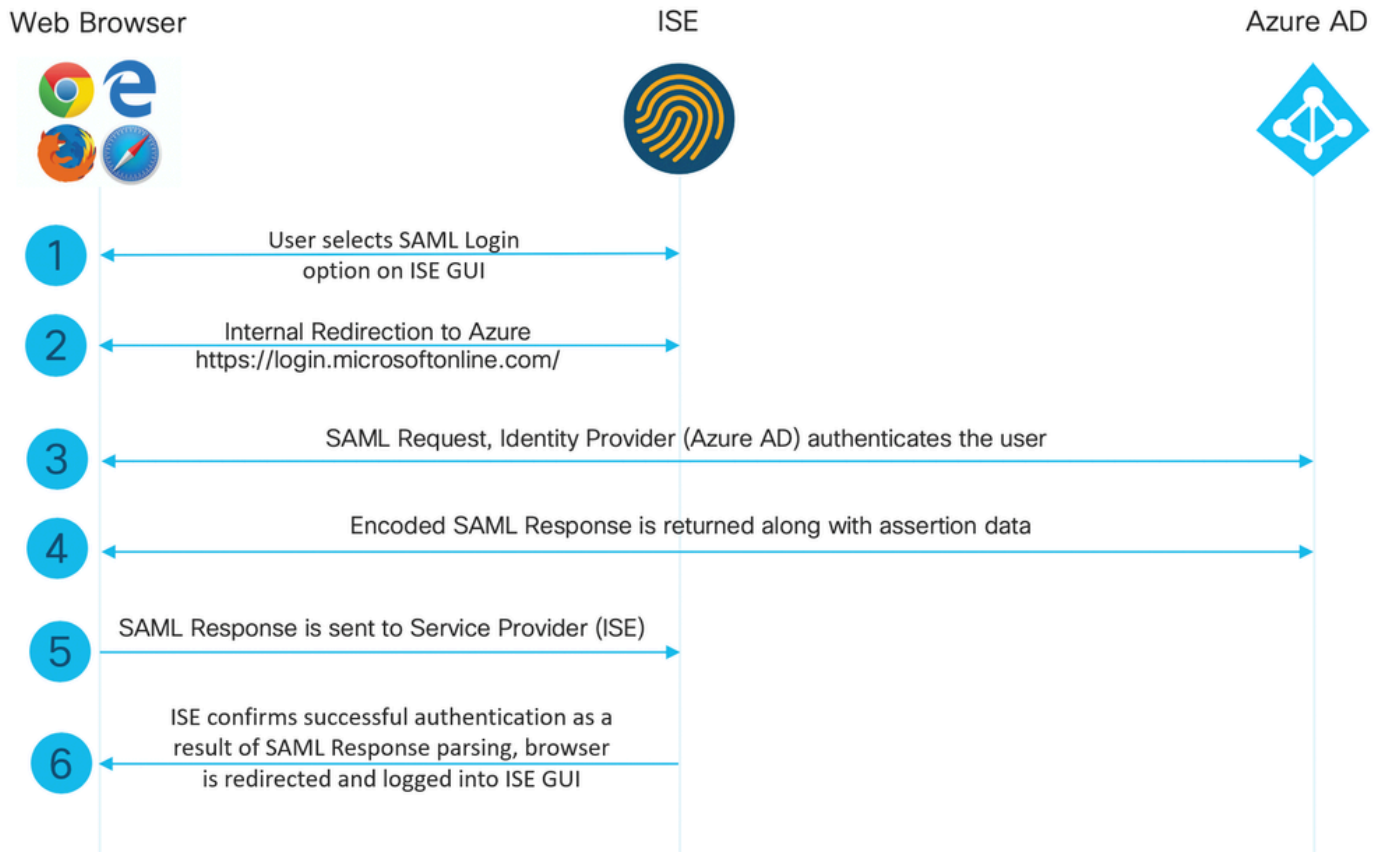
- Las aserciones de autenticación prueban la identificación del usuario y proporcionan la hora de inicio de sesión del usuario y el método de autenticación que utilizan (Kerberos, de dos factores, como ejemplos)
- La aserción de atribución pasa los atributos SAML, datos específicos que proporcionan información sobre el usuario, al proveedor de servicios.
- Una aserción de decisión de autorización declara si el usuario está autorizado a utilizar el servicio o si el proveedor de identidad ha denegado su solicitud debido a un error de contraseña o a la falta de derechos para el servicio.

Diagrama de flujo de alto nivel

SAML funciona pasando información sobre usuarios, inicios de sesión y atributos entre el proveedor de identidad, Azure AD, y el proveedor de servicios, ISE.

Cada usuario inicia sesión una vez en un inicio de sesión único (SSO) con el proveedor de identidad y, a continuación, el proveedor de Azure AD pasa los atributos SAML a ISE cuando el usuario intenta acceder a esos servicios.

ISE solicita autorización y autenticación de Azure AD, como se muestra en la imagen.



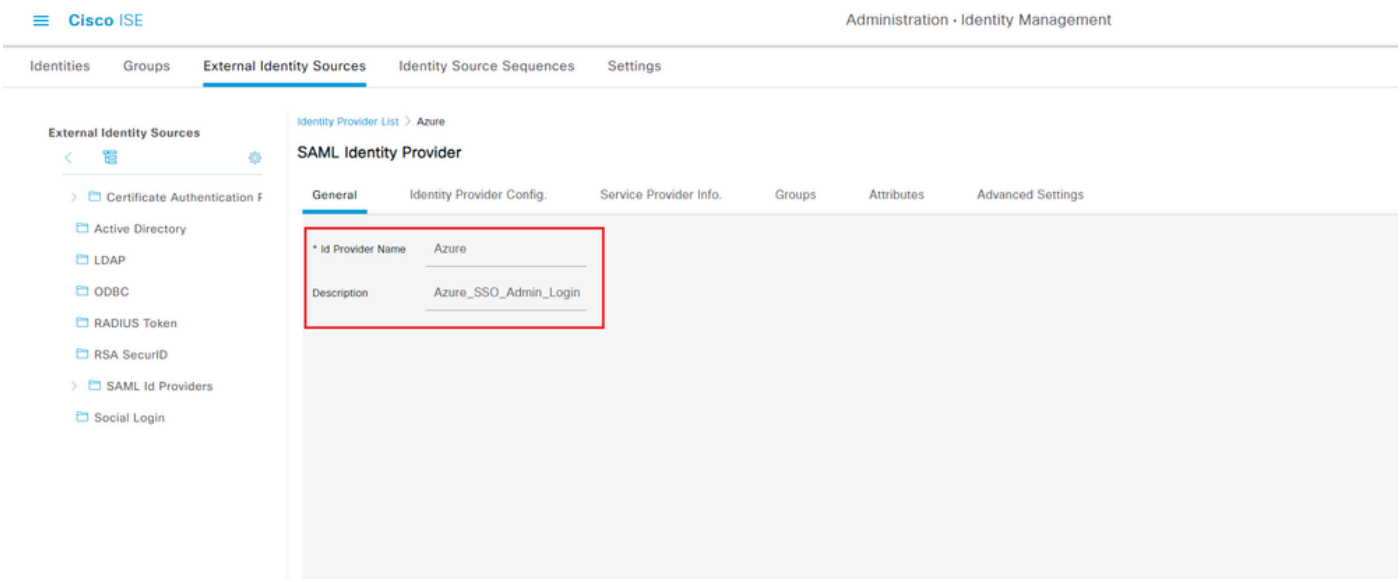
Configuración de la integración de SSO de SAML con Azure AD

Paso 1. Configuración del proveedor de identidad SAML en ISE

1. Configure Azure AD como origen de identidad SAML externo

En ISE, navegue hasta Administration > Identity Management > External Identity Sources > SAML Id Providers y haga clic en el botón Add.

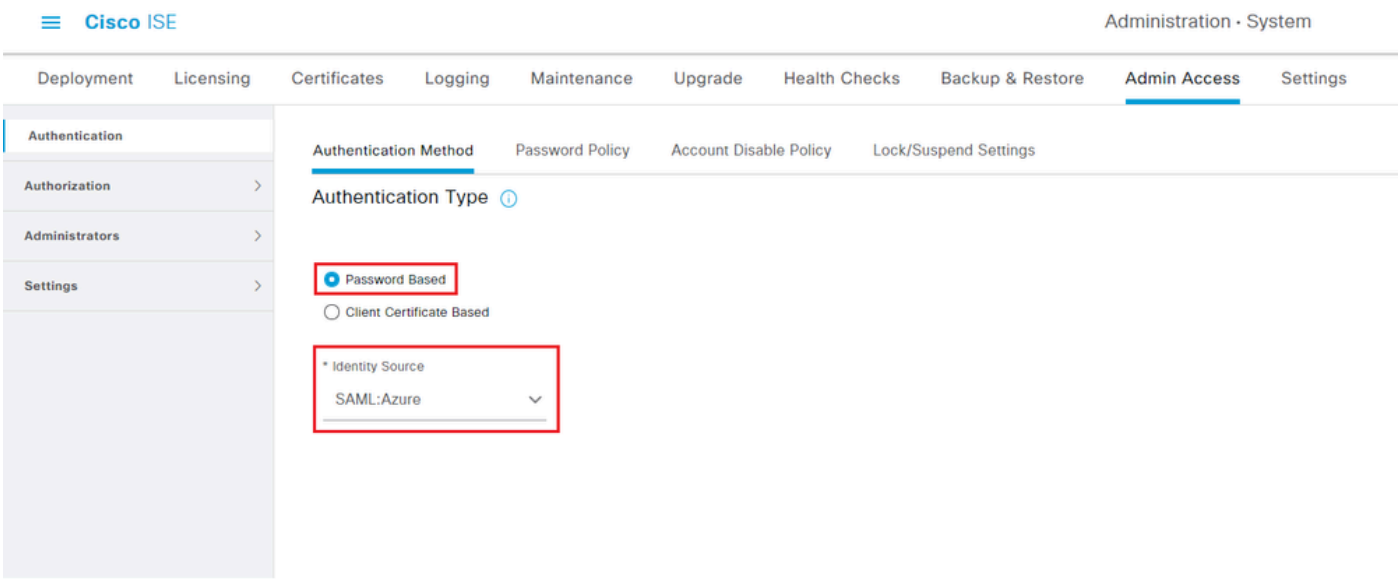
Ingrese el Nombre del Proveedor de Id y haga clic en Enviar para guardarlo. El nombre del proveedor de ID es significativo solo para ISE, como se muestra en la imagen.



2. Configurar el método de autenticación de ISE

Navegue hasta Administration >System > Admin Access > Authentication > Authentication Method y seleccione el botón de opción Password Based.

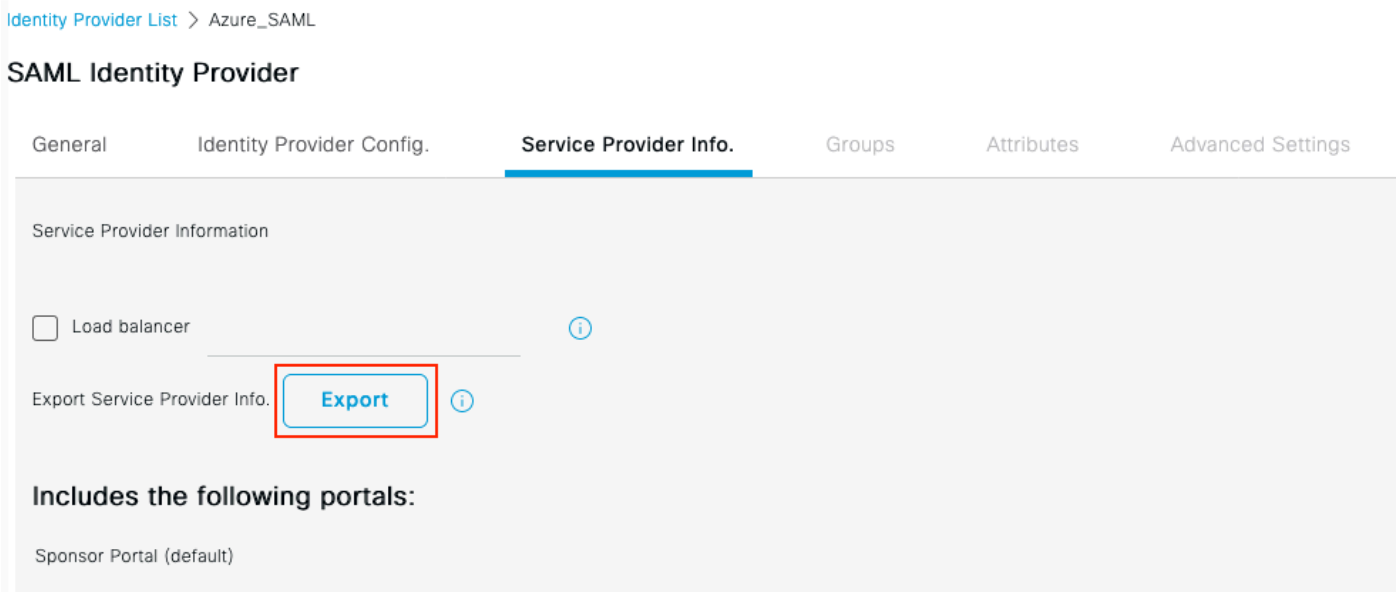
Seleccione el nombre de proveedor de ID necesario creado anteriormente en la lista desplegable Origen de identidad, como se muestra en la imagen.



3. Exportar información del proveedor de servicios

Vaya a Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider].

Cambie la pestaña a Service Provider Info. y haga clic en el botón Export como se muestra en la imagen.



Descargue el archivo .xml y guárdelo. Anote la URL de la ubicación y el valor de entityID.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasi
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSig
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amSlL6NAE8FY+tzANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQQDExpT
QU1MX2lzZTMtMS0xOS5ja3VtYXIyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTGlNBTUxfaXNlMy0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAvila4+SOuP3j037yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYdlDtE1LMEcGg1mCd56GfrDcJdXOcZJmiDzizyjGKDdPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzFO38ciQqlm0sqrVrrYZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFFlMzybvm1FYu
9h83gL4WJWMizETO6Vs/DOp6BSf2MPxKe79OR5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5ROgT7v3CDrdFtRoNYAT+YvO941KzFCSEOsshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNzlFuggaE8tC7uyuQZa2rcmTrXGWCl
sDU4uOvFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWIy+ctbBTO+EMO6Xj1aTI1bV8OmN/6LhiS8g7KpFz4RN+ag1iu6pgZ5O58Zot9gqkpFw
kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVR0RBBkwF4IVaXNlMy0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgLsMB0GA1UdDgQWBBRIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
2O6Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GWlvcgreC7R46qenaonXVrltRw11vVIdCf8JQFFMxya/rIC4mxVeooOj1Fl9d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4HOvdm6oF3uBteO/pdUtEi6fObqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gfHObE5luT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wk0BLZM
lgV8FTVQSnra9LwHP/PgeNAPUcRPXSwaKE4rvjvMcOaS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9yslIHmdqoH3EmOFOgnzRORvsMPbJxAoTFjfoITTMdQXNHhg+wlPOKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8EOv7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
```

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService index="0" Location="https://10.201.232.19:8443/portal/SSOLoginResponse.act
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLogin

</md:SPSSODescriptor>
</md:EntityDescriptor>
```

Atributos de interés del archivo XML:

entityID="http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2"

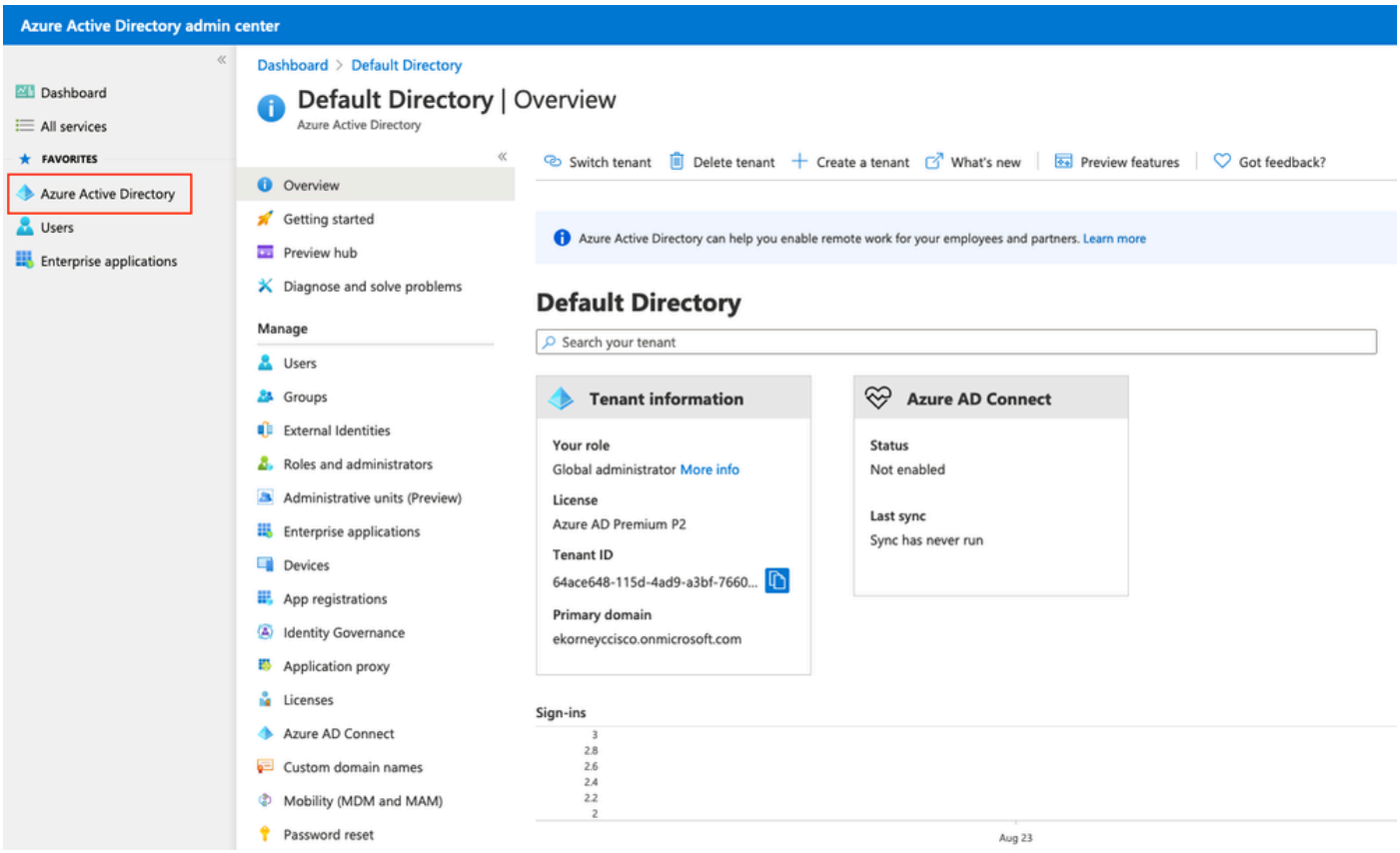
AssertionConsumerService Location="https://10.201.232.19:8443/portal/SSOLoginResponse.action"

AssertionConsumerService Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action"

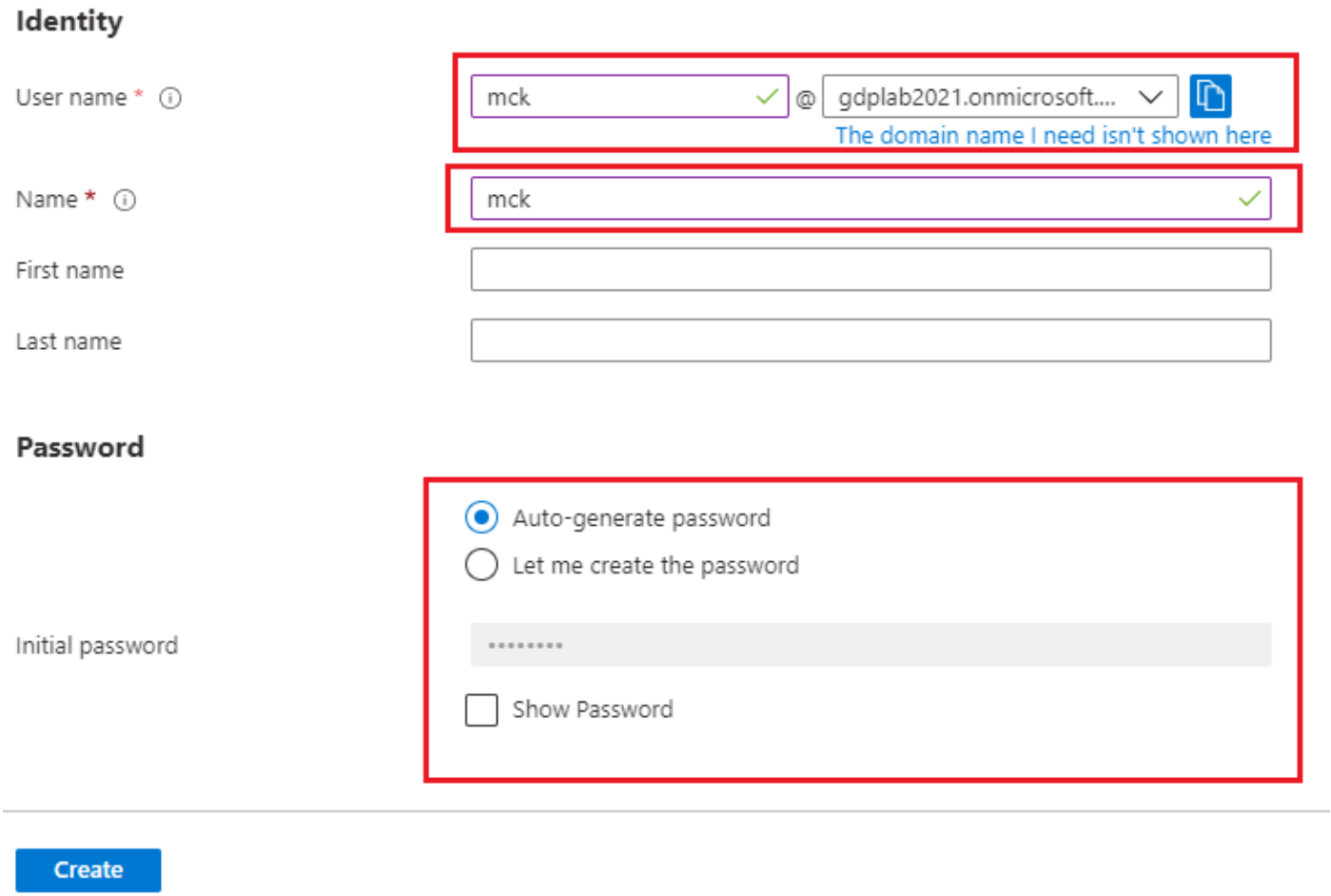
Paso 2. Configurar Azure AD IdP Settings

1. Crear un usuario de Azure AD

Inicie sesión en el panel del centro de administración de Azure Active Directory y seleccione su AD como se muestra en la imagen.

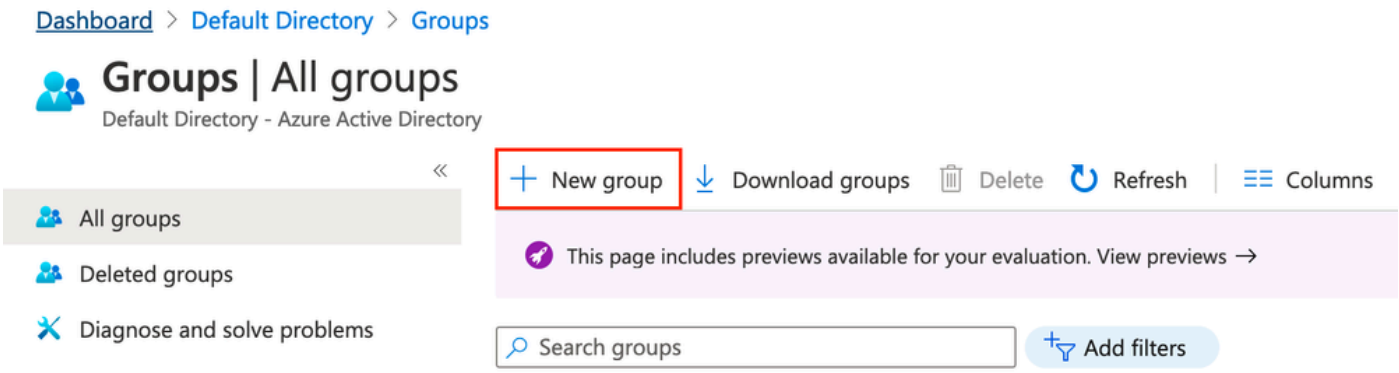


Seleccione Users, haga clic en New User, configure User name, Name y Initial Password según sea necesario. Haga clic en Create como se muestra en la imagen.

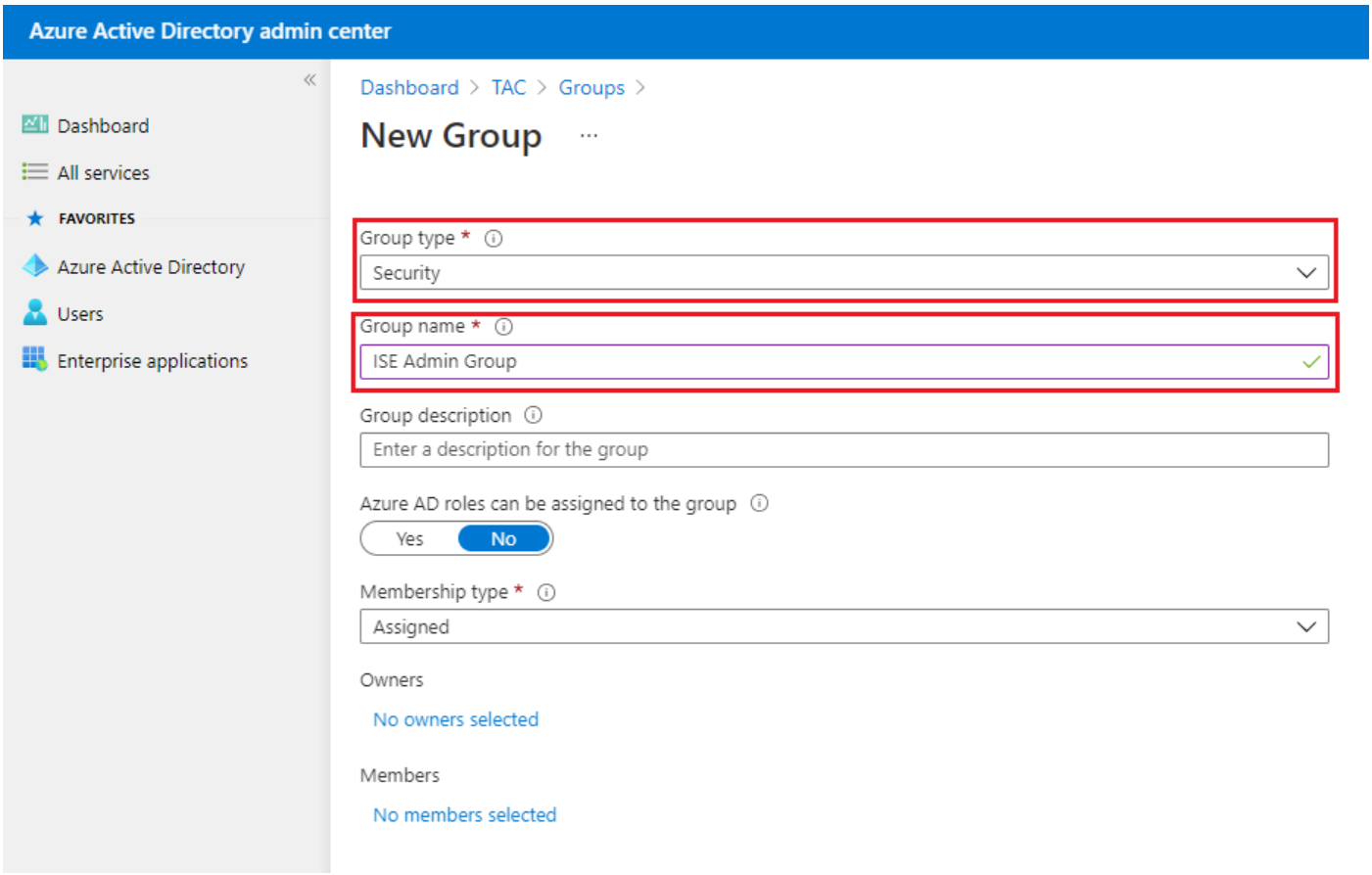


2. Crear un grupo de Azure AD

Seleccione Grupos. Haga clic en Nuevo grupo.

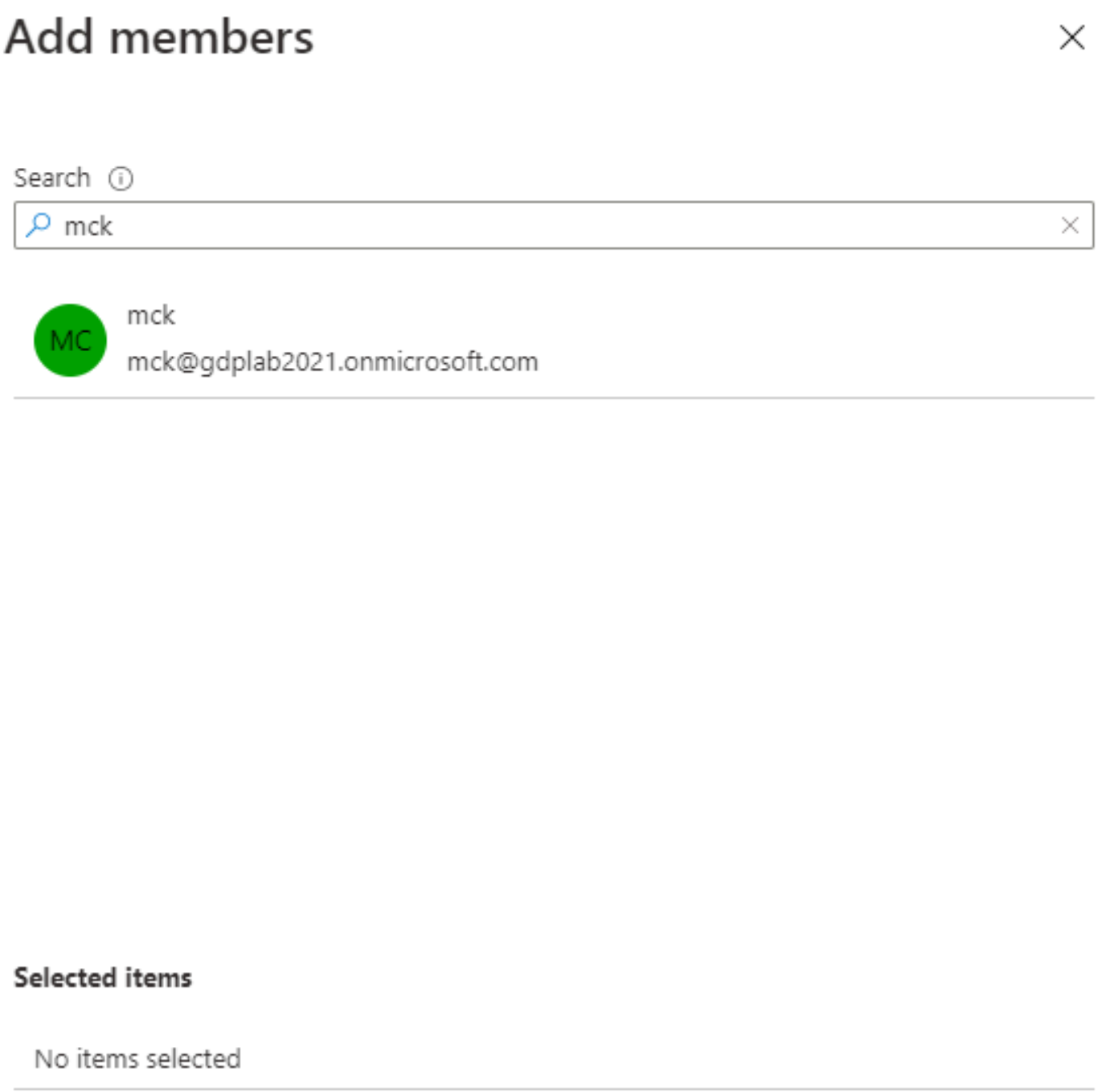


Mantener el tipo de grupo como Seguridad. Configure el nombre de grupo como se muestra en la imagen.

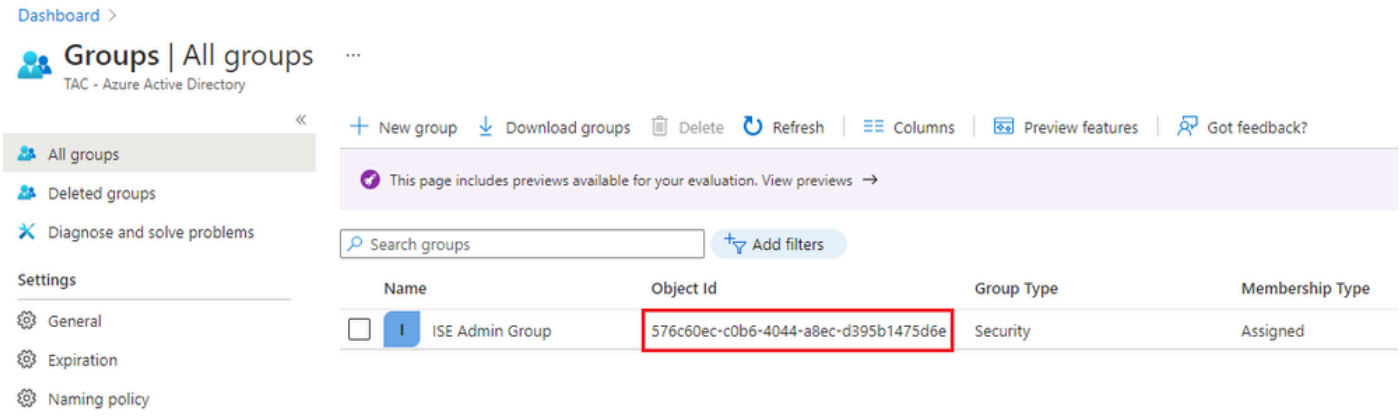


3. Asignar usuario de Azure AD al grupo

Haga clic en No hay miembros seleccionados. Elija el usuario y haga clic en Seleccionar. Haga clic en Crear para crear el grupo con un Usuario asignado a él.

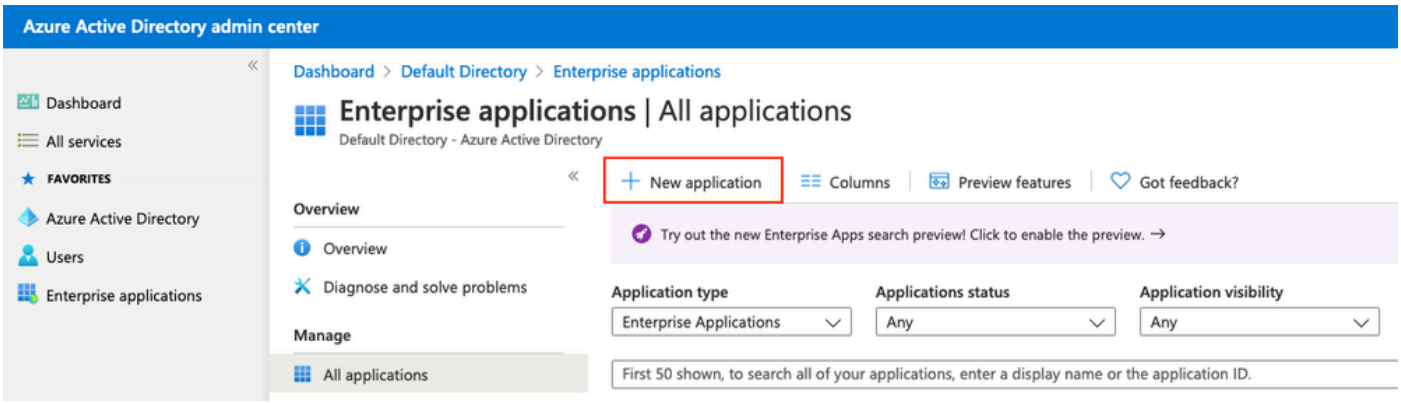


Tome nota de Group Object id, en esta pantalla, es 576c60ec-c0b6-4044-a8ec-d395b1475d6e para ISE Admin Group como se muestra en la imagen.

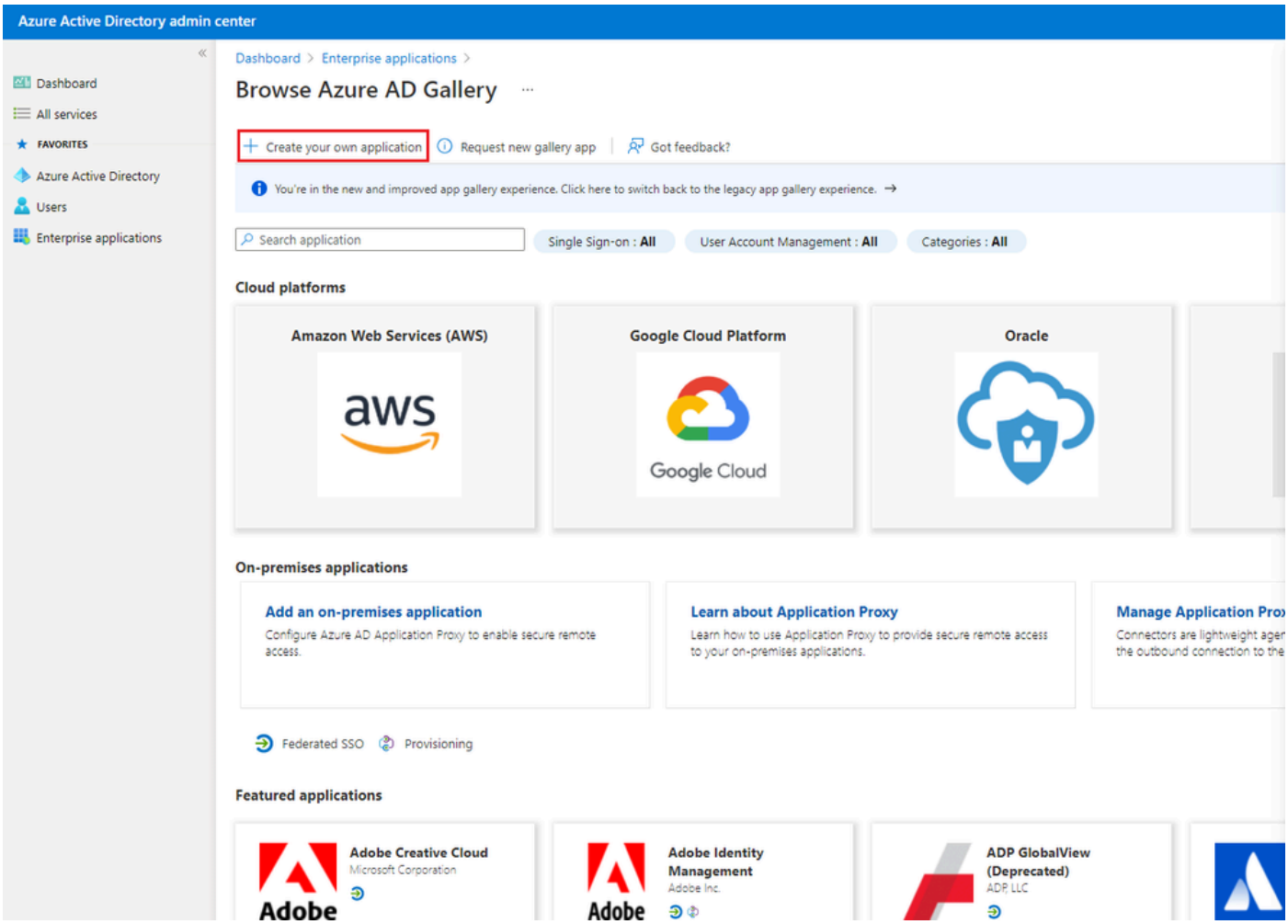


4. Crear una aplicación empresarial de Azure AD

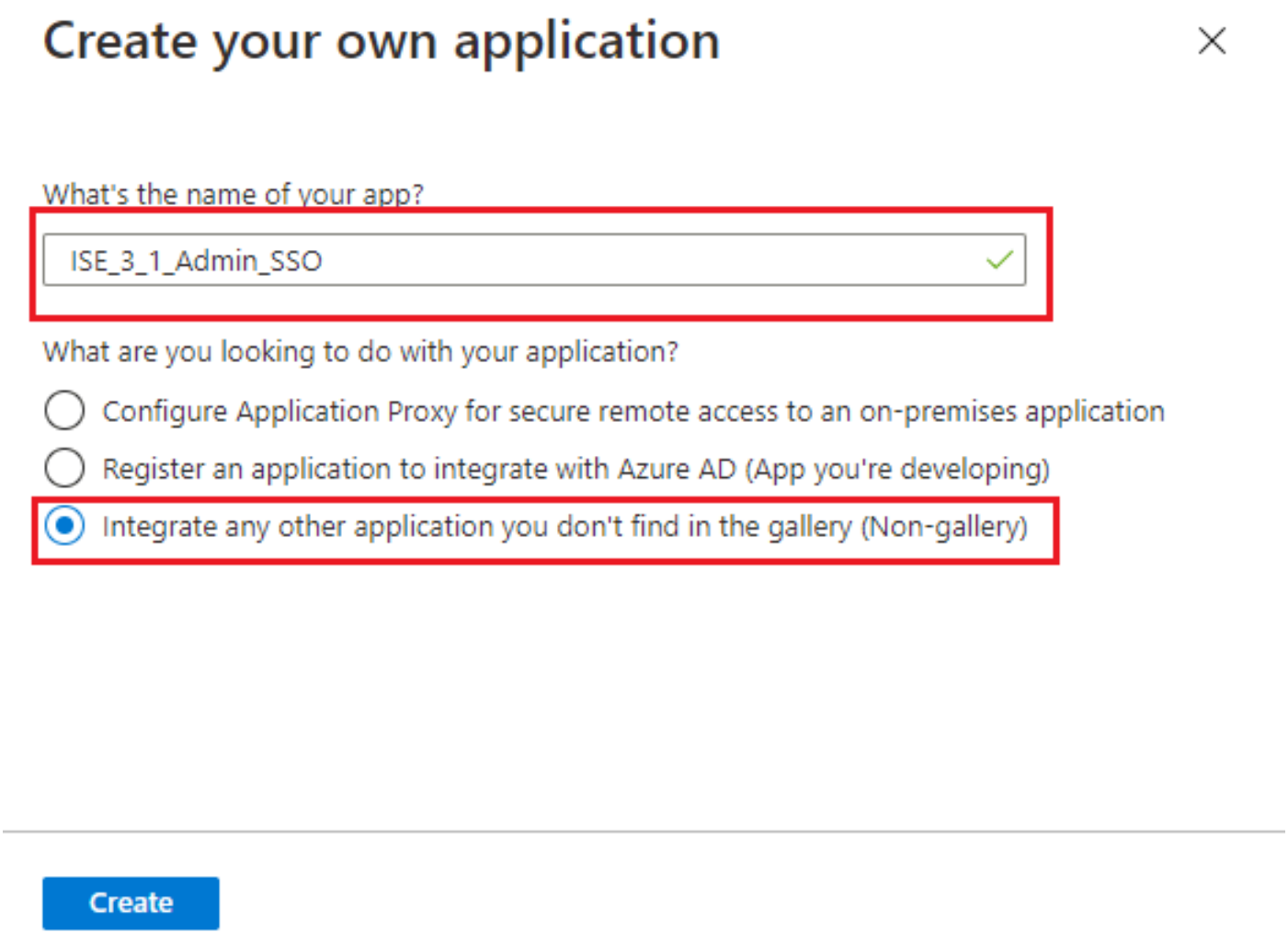
En AD, seleccione Aplicaciones empresariales y haga clic en Nueva aplicación.



Seleccione Crear su propia aplicación.

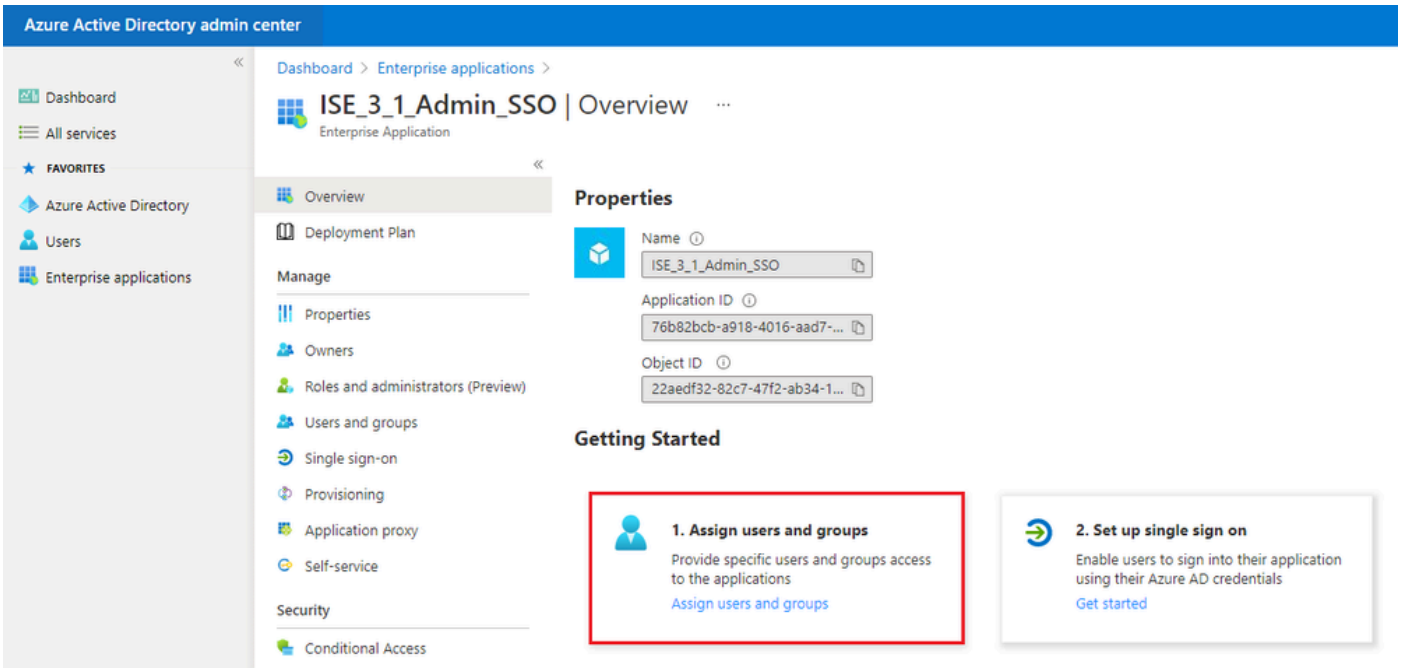


Ingrese el nombre de su aplicación y seleccione el botón de opción Integrar cualquier otra aplicación que no encuentre en la galería (No-galería) y haga clic en el botón Crear como se muestra en la imagen.

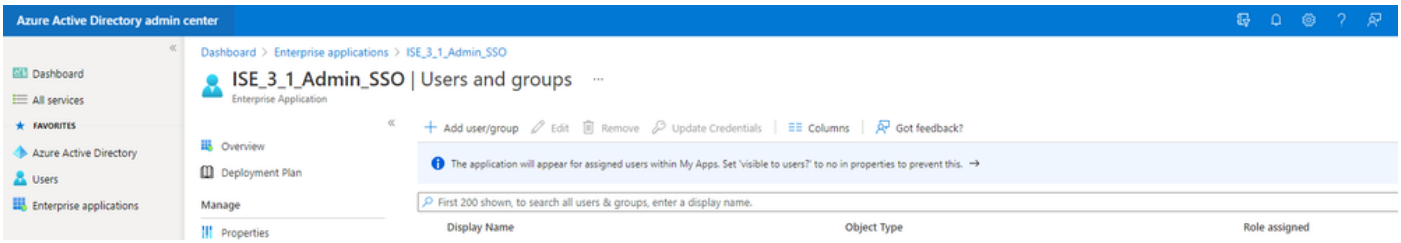


5. Agregar grupo a la aplicación

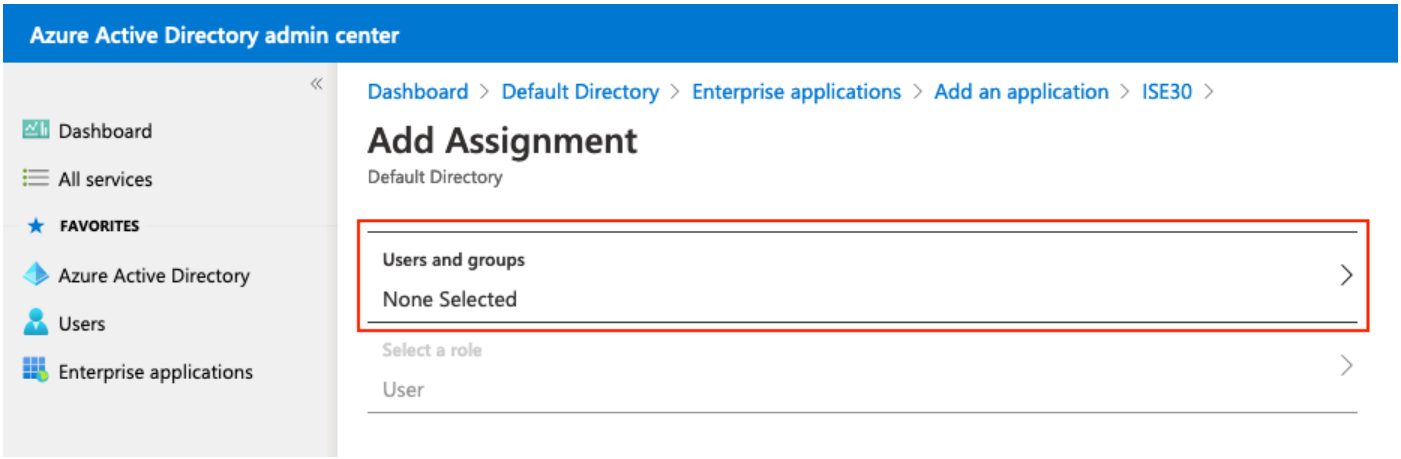
Seleccione Asignar usuarios y grupos.



Haga clic en Agregar usuario/grupo.



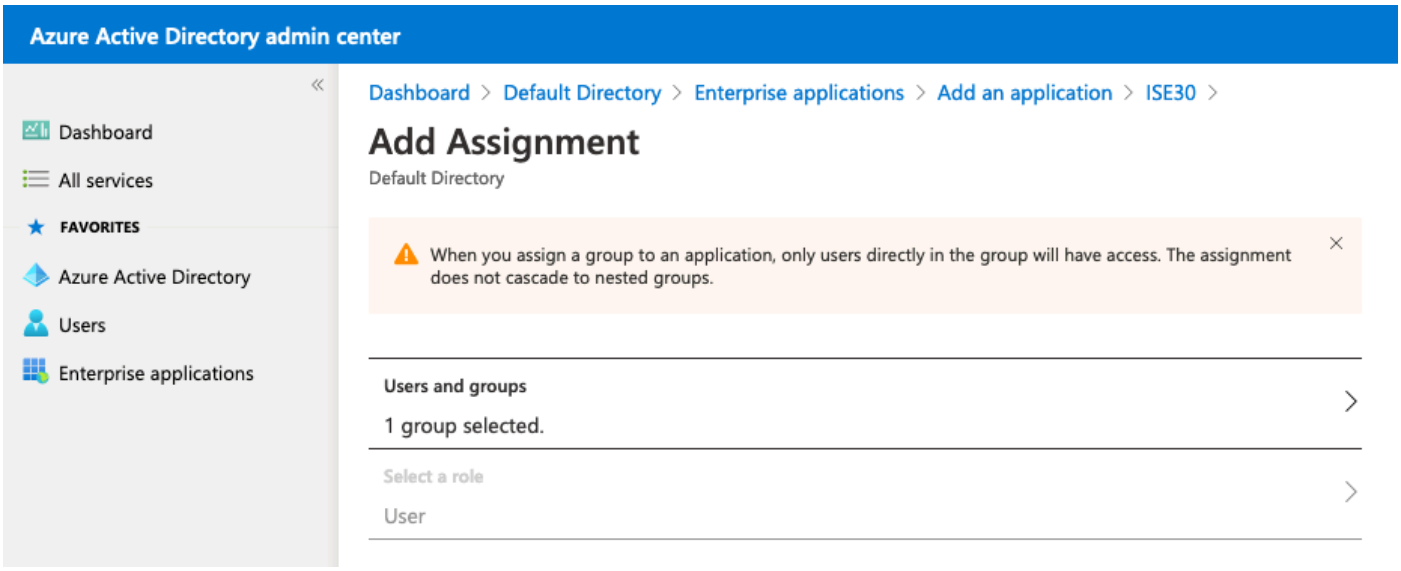
Haga clic en Usuarios y grupos.



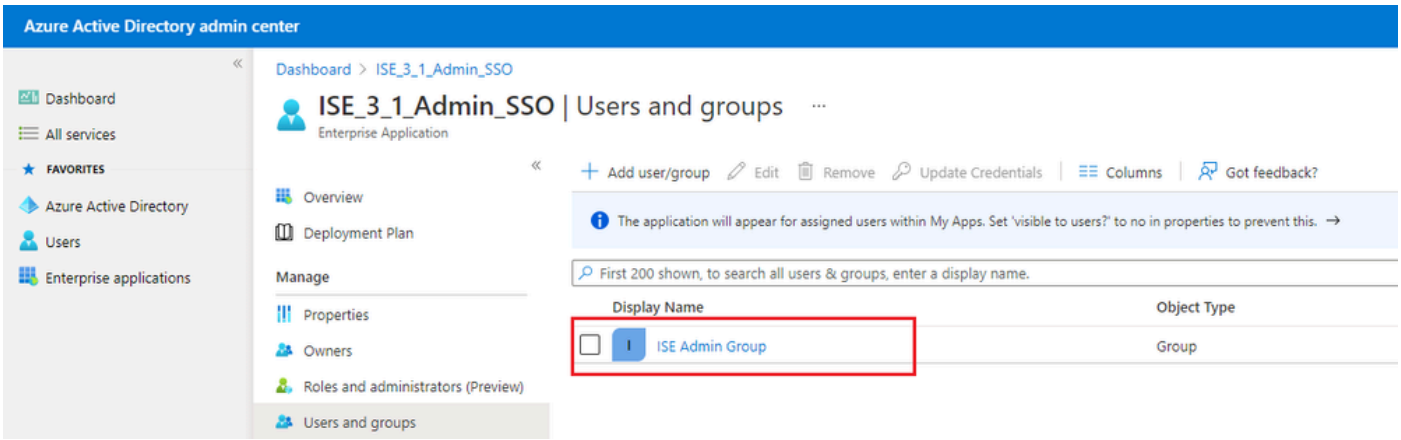
Elija el grupo configurado anteriormente y haga clic en Seleccionar.

Nota: seleccione el conjunto adecuado de usuarios o grupos que obtendrán acceso según lo previsto, ya que los usuarios y grupos mencionados aquí obtendrán acceso a ISE una vez finalizada la configuración.

Una vez seleccionado el grupo, haga clic en Asignar.

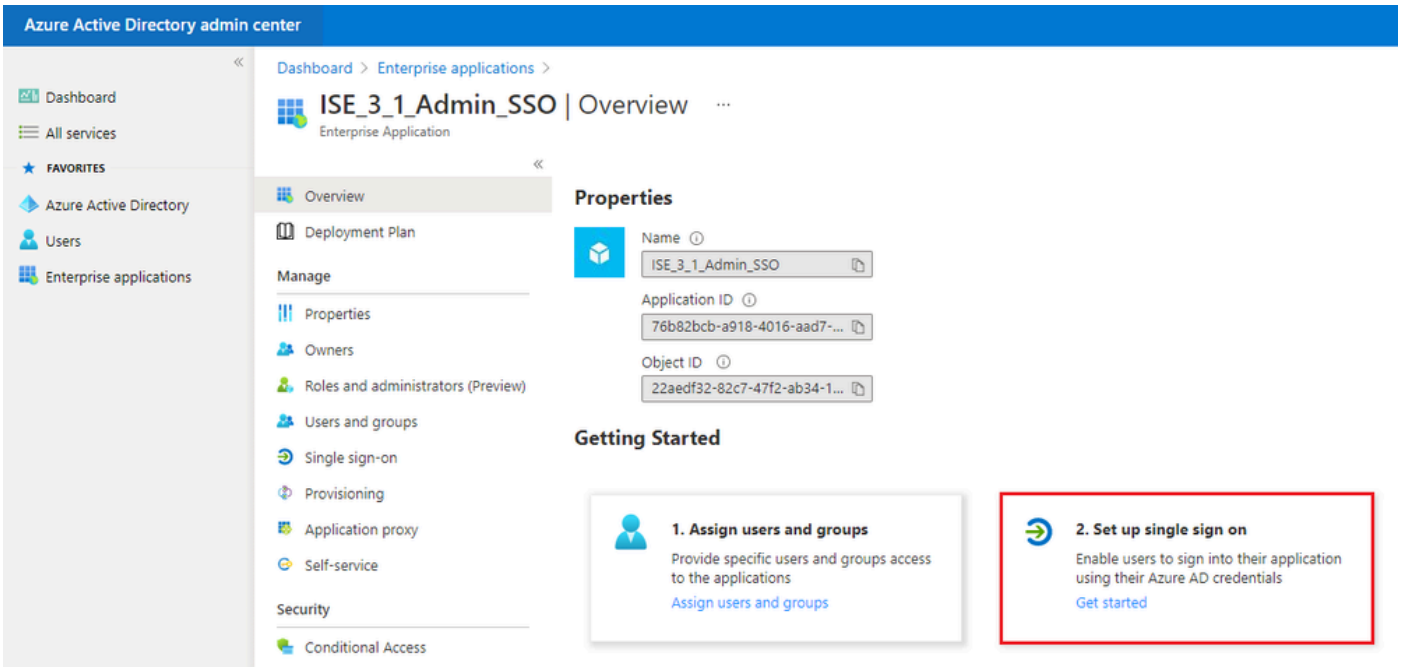


Como resultado, el menú Users and groups para la aplicación configurada se completa con el grupo seleccionado.

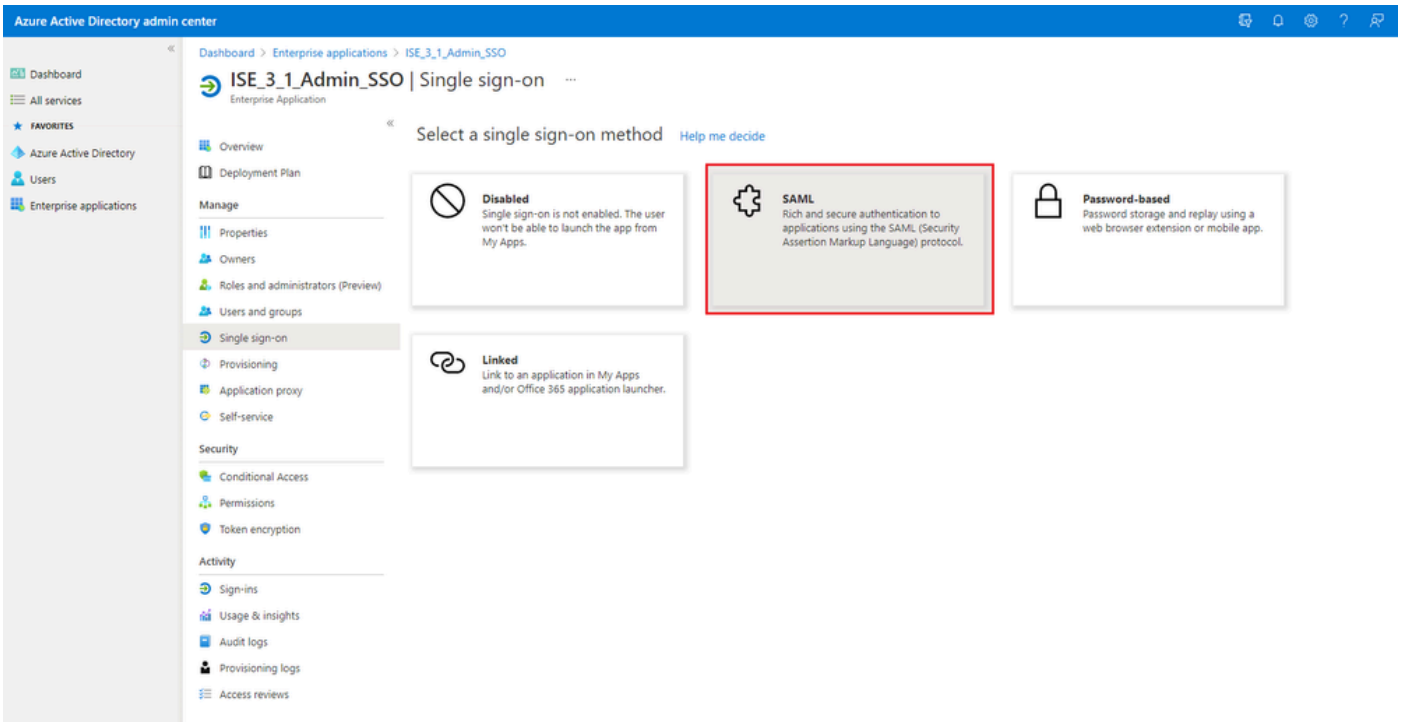


6. Configurar una aplicación empresarial de Azure AD

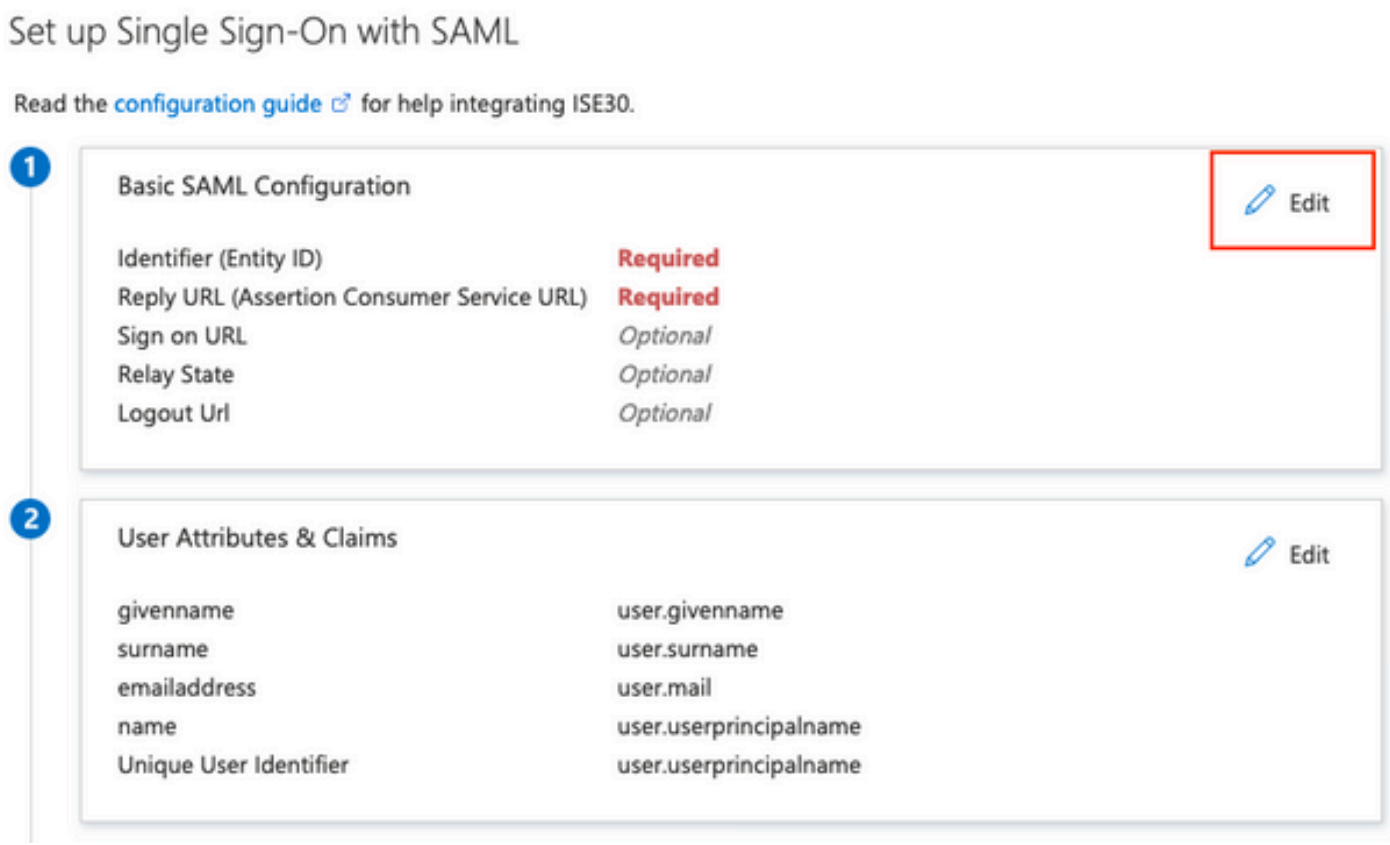
Vuelva a la aplicación y haga clic en Configurar inicio de sesión único.



Seleccione SAML en la siguiente pantalla.

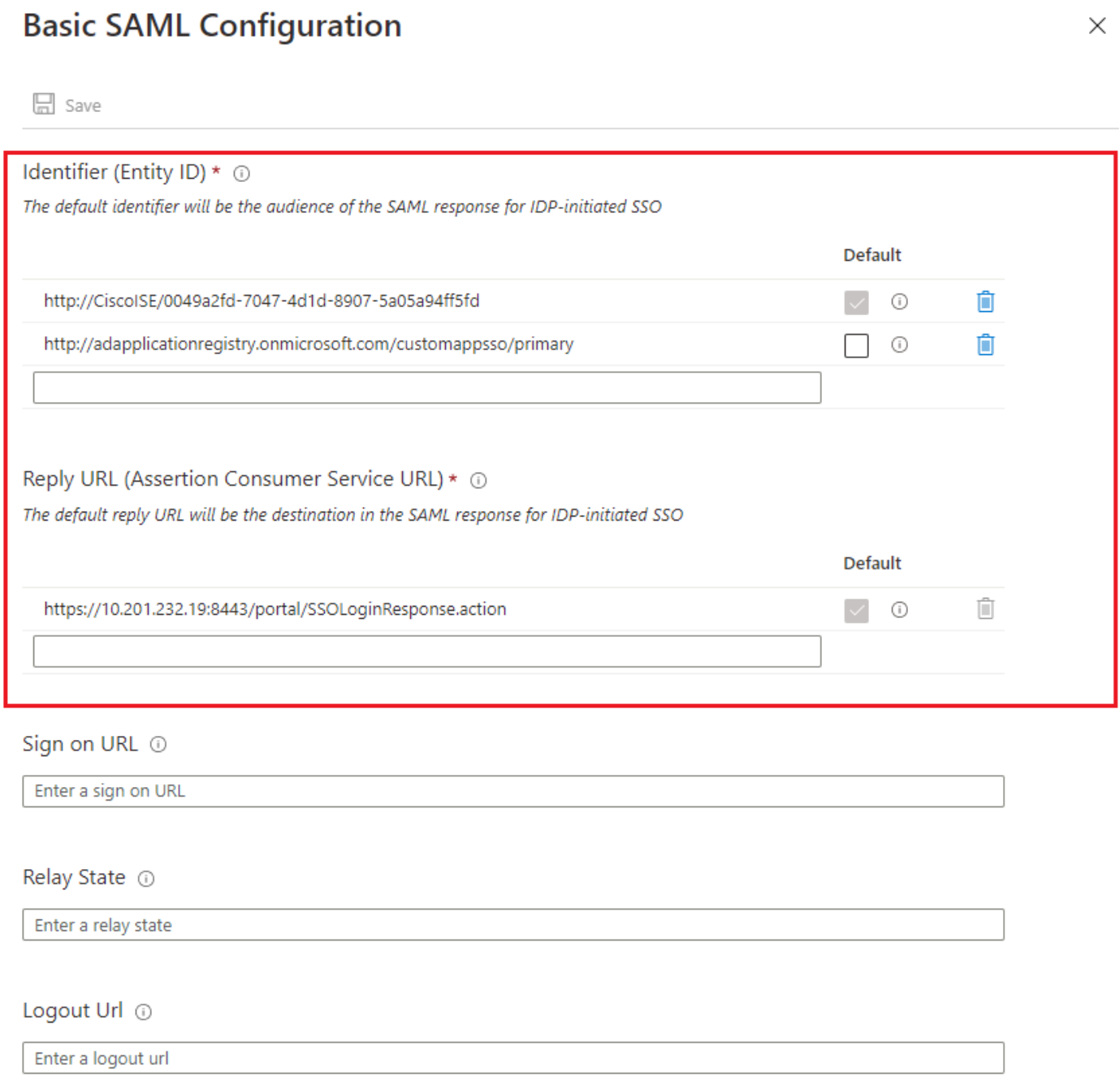


Haga clic en Edit junto a Basic SAML Configuration.



Rellene el identificador (Id. de entidad) con el valor de entityID del archivo XML del paso Exportar información del proveedor de servicios. Rellene URL de respuesta (URL de servicio de consumidor de aserción) con el valor de Ubicaciones de AssertionConsumerService. Click Save.

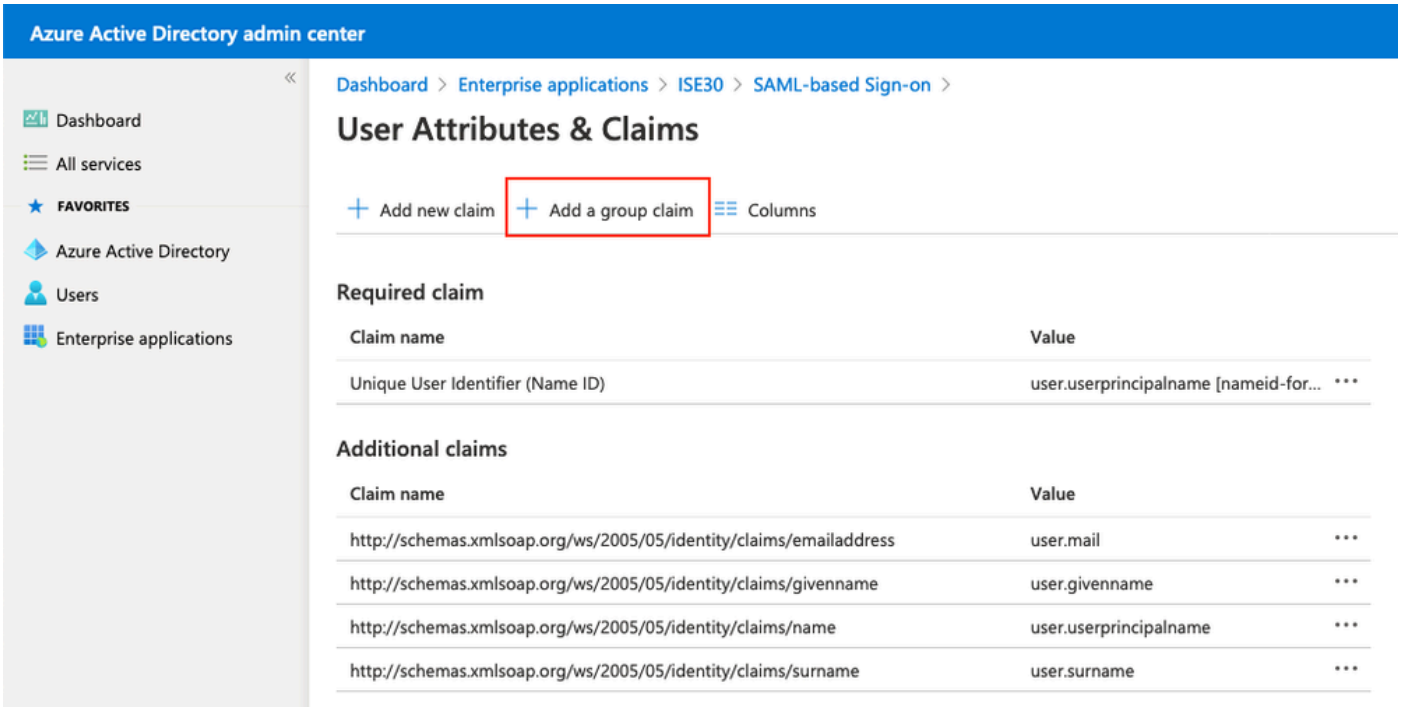
Nota: La URL de respuesta actúa como una lista de pasadas, lo que permite que ciertas URL actúen como fuente cuando se redireccionan a la página IdP.



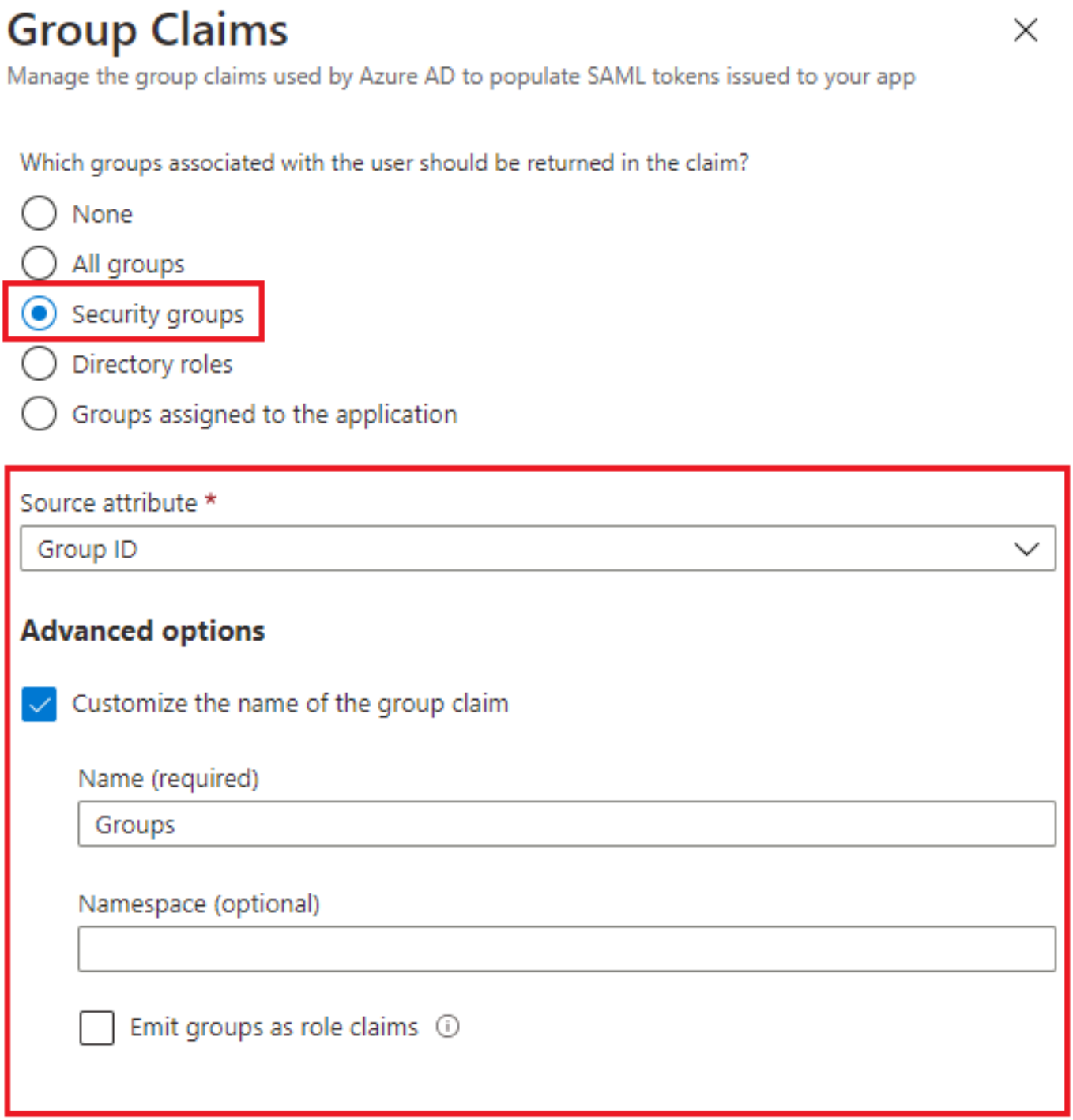
7. Configurar el atributo de grupo de Active Directory

Para devolver el valor de atributo de grupo configurado previamente, haga clic en Editar junto a Atributos de usuario y reclamaciones.

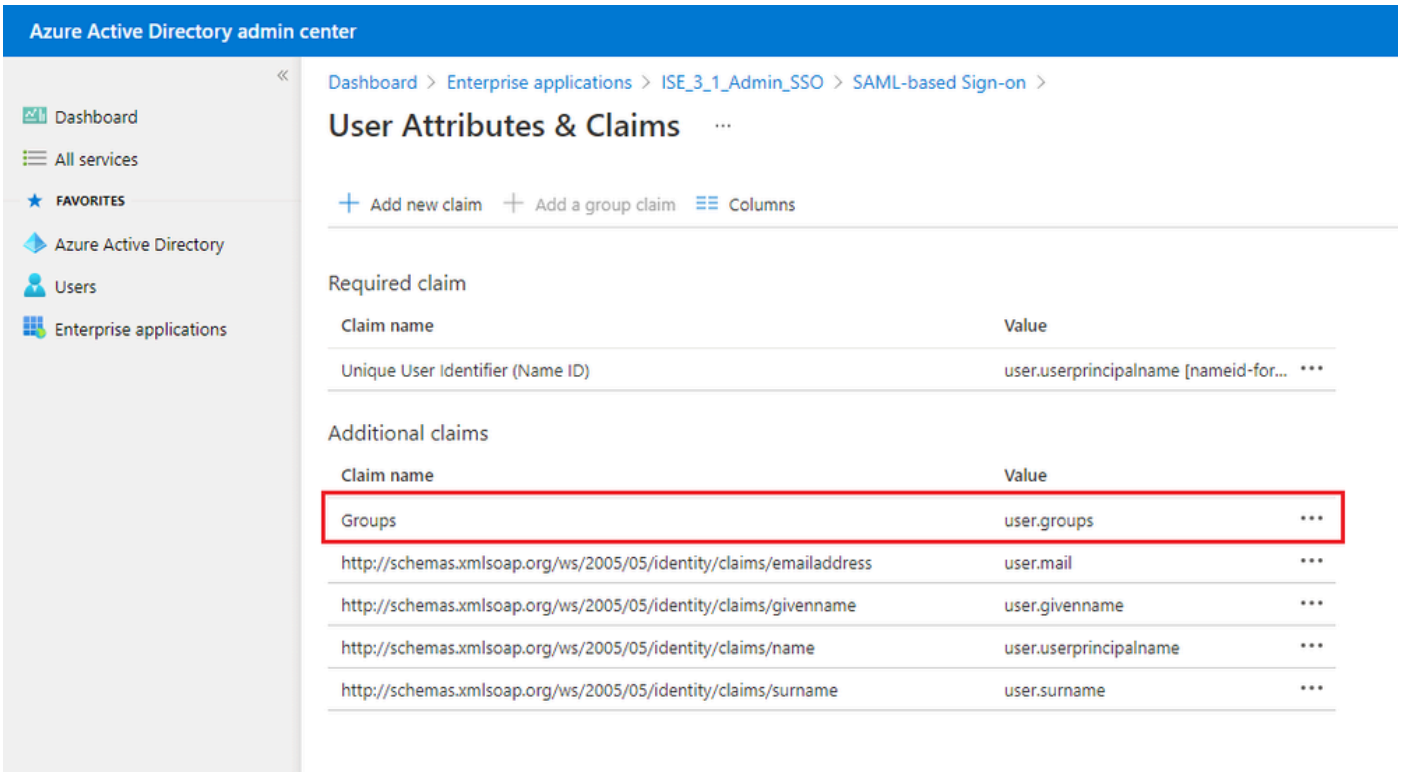
Haga clic en Agregar una reclamación de grupo.



Seleccione Security groups y haga clic en Save. Seleccione Group ID en el menú desplegable Source attribute. Active la casilla de verificación para personalizar el nombre de la notificación de grupo e introduzca el nombre Grupos.

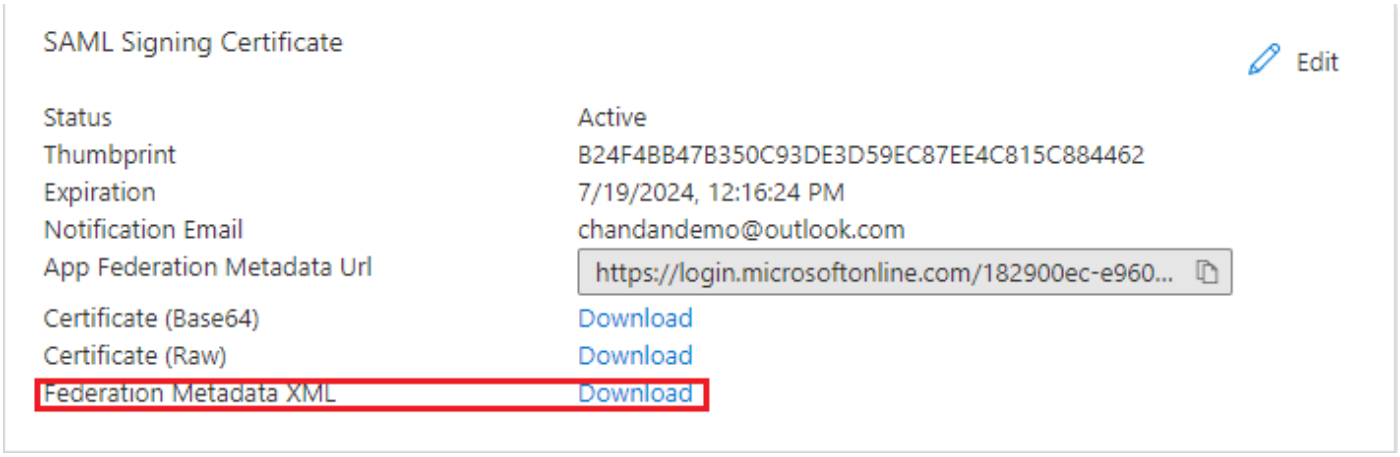


Anote el nombre de la reclamación del grupo. En este caso, se trata de Grupos.



8. Descargar el archivo XML de metadatos de Azure Federation

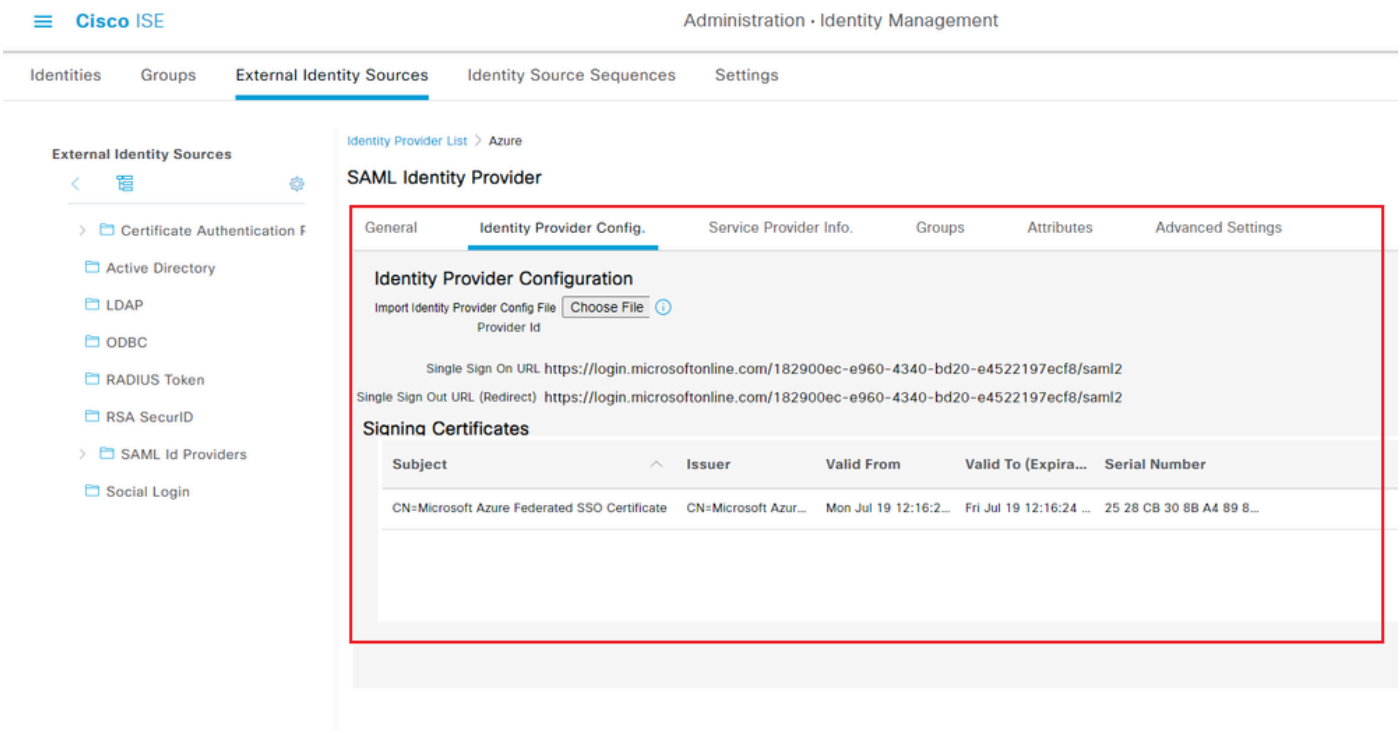
Haga clic en Descargar en XML de metadatos de federación en Certificado de firma SAML.



Paso 3. Cargar metadatos de Azure Active Directory en ISE

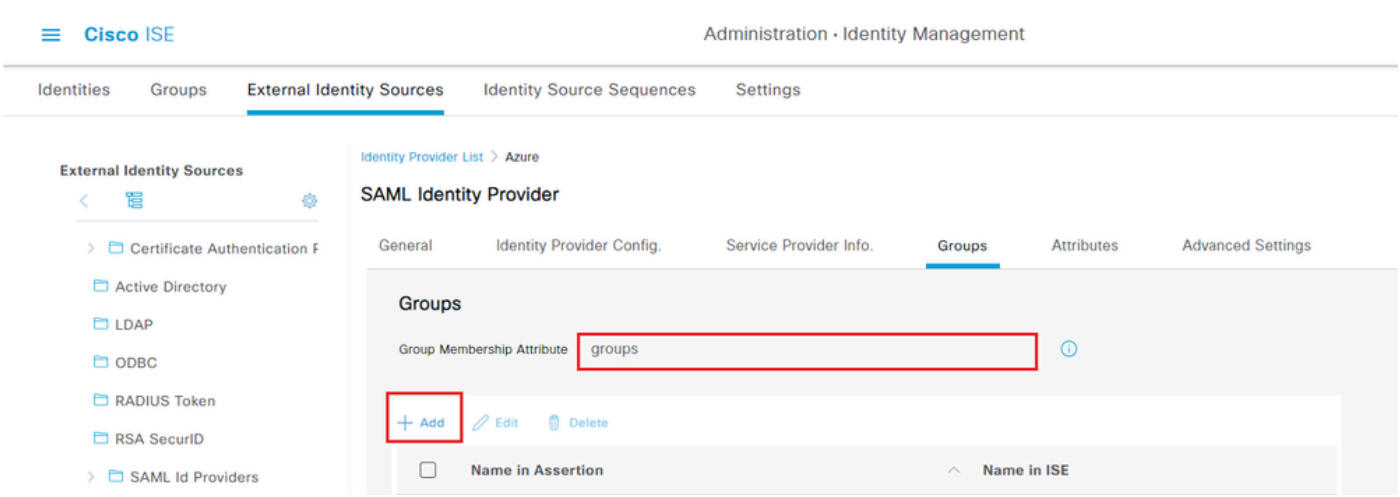
Vaya a Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider].

Cambie la ficha a Identity Provider Config. y haga clic en Browse. Seleccione el archivo Federation Metadata XML en el paso Download Azure Federation Metadata XML y haga clic en Save.



Paso 4. Configuración de grupos SAML en ISE

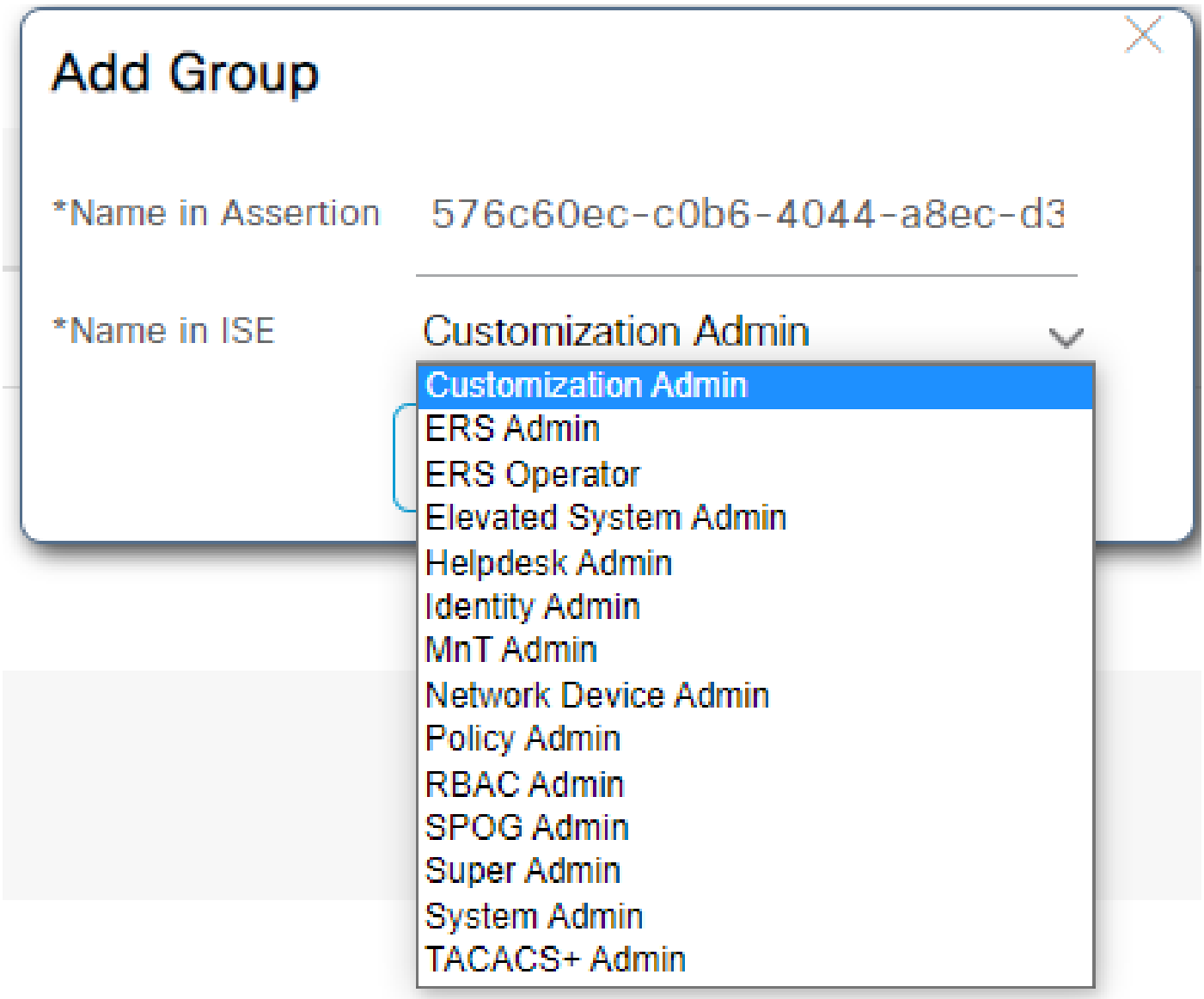
Cambie a la ficha Grupos y pegue el valor de Nombre de reclamación del atributo Configurar grupo de Active Directory en el atributo Pertenencia a grupo.



Haga clic en Agregar. Rellene Name en Assertion con el valor de Group Object id de ISE Admin Group capturado en Assign Azure Active Directory User to the Group.

Configure Name en ISE con el menú desplegable y seleccione el grupo adecuado en ISE. En este ejemplo, el grupo utilizado es Super Admin. Click OK. Click Save.

Esto crea una asignación entre el grupo en Azure y el nombre del grupo en ISE.

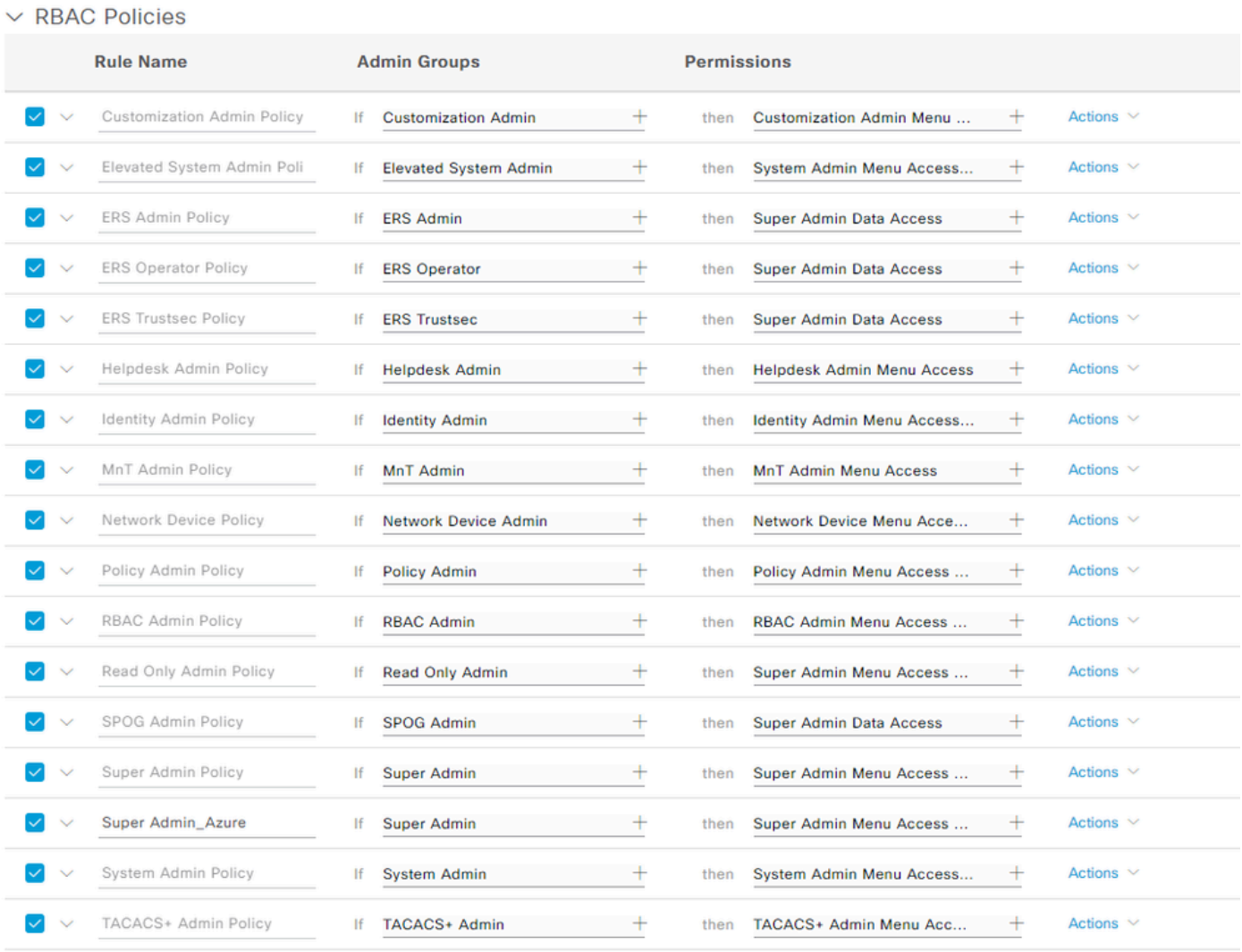


(Optativo) Paso 5. Configuración de políticas RBAC

A partir del paso anterior, hay muchos tipos diferentes de niveles de acceso de usuario que se pueden configurar en ISE.

Para editar las políticas de control de acceso basadas en roles (RBAC), vaya a Administration > System > Admin Access > Authorization > Permissions > RBAC Policies y configúrelas según sea necesario.

Esta imagen es una referencia a la configuración de ejemplo.



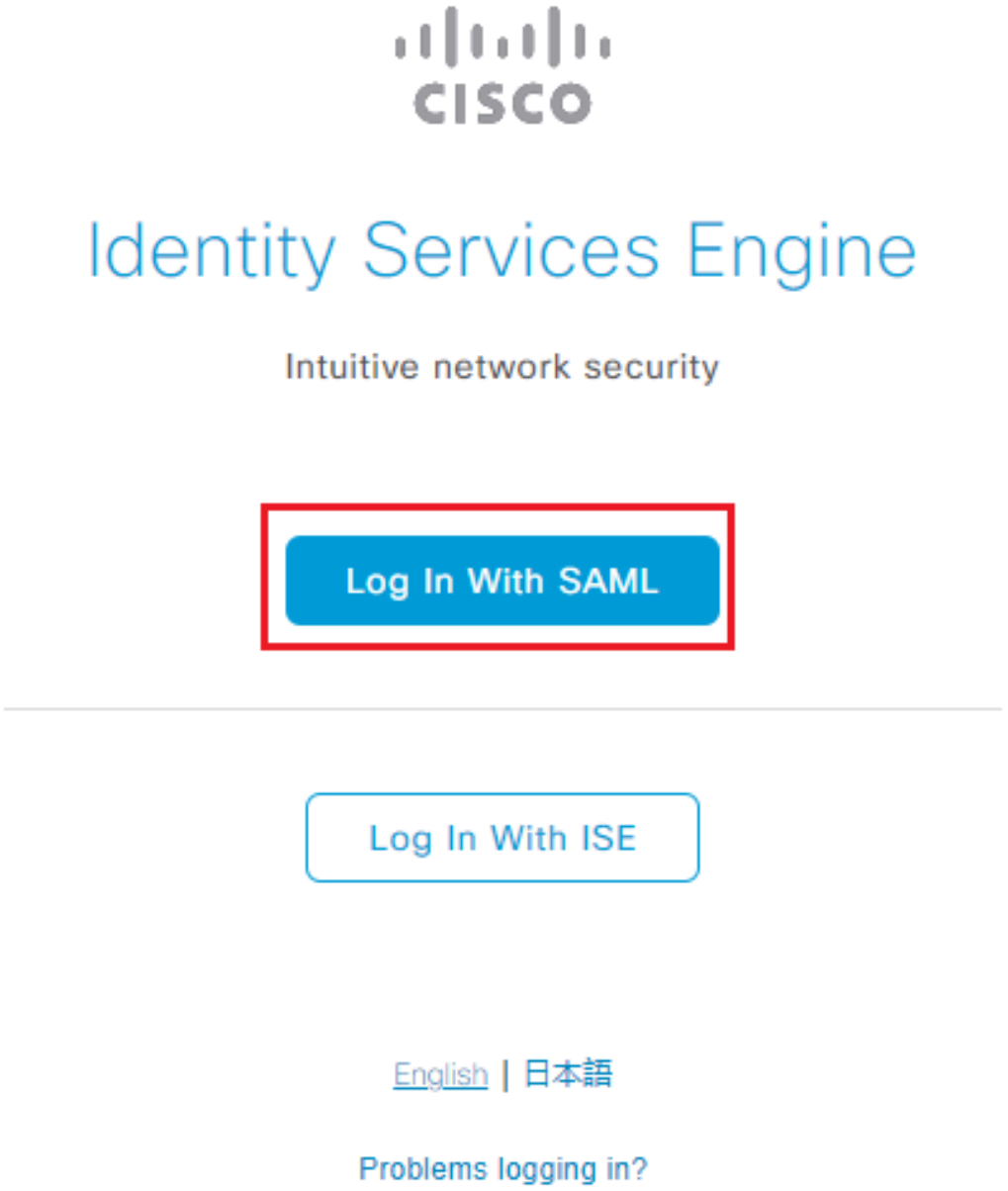
Verificación

Confirme que la configuración funciona correctamente.

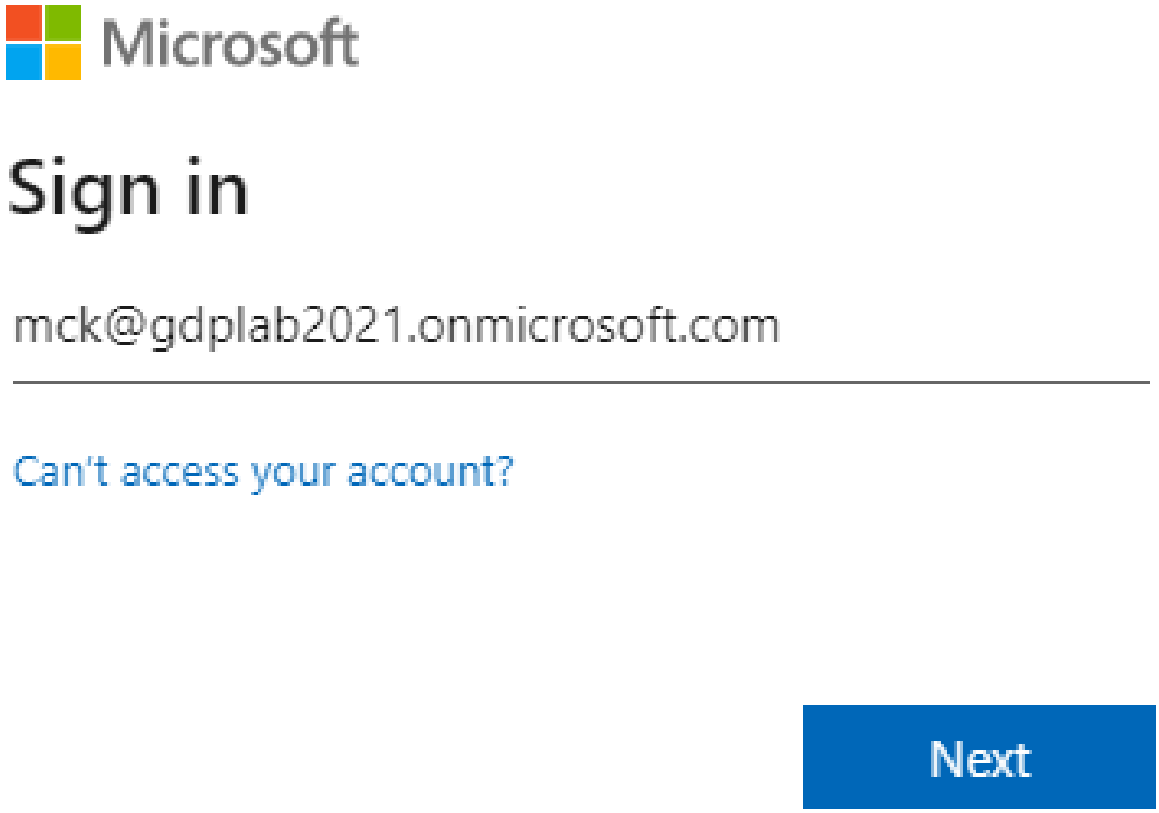
Nota: La prueba de inicio de sesión SSO de SAML de la funcionalidad de prueba de Azure no funciona. ISE debe iniciar la solicitud SAML para que el SSO SAML de Azure funcione correctamente.

Abra la pantalla de solicitud de inicio de sesión de la GUI de ISE. Se le presenta una nueva opción para Iniciar sesión con SAML.

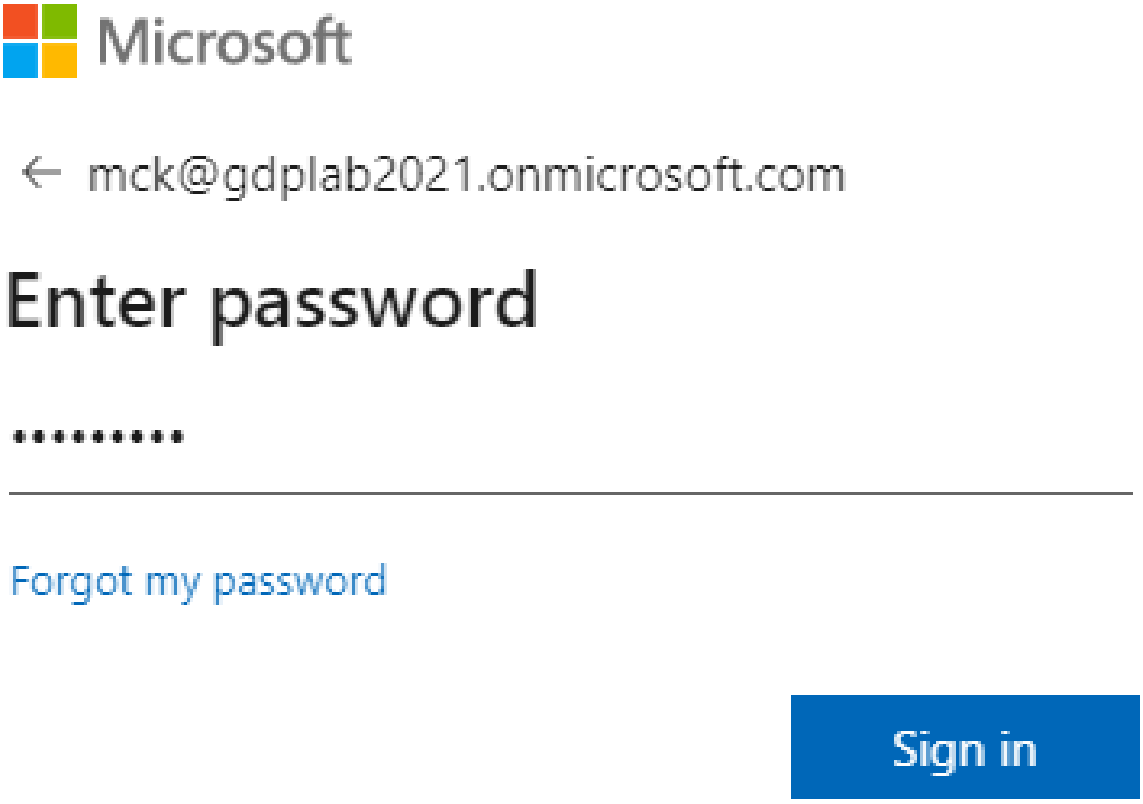
1. Acceda a la página de inicio de sesión de la GUI de ISE y haga clic en Iniciar sesión con SAML.



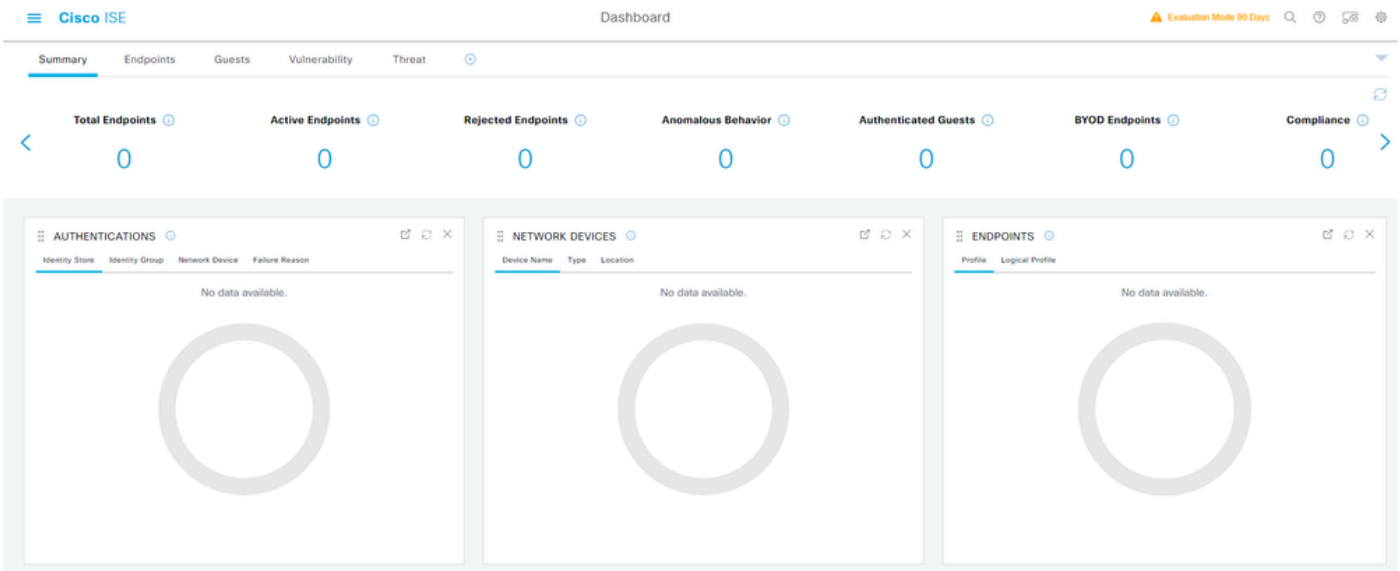
2. Se le redirigirá a la pantalla de inicio de sesión de Microsoft. Ingrese sus credenciales de nombre de usuario de una cuenta en un grupo asignado a ISE como se muestra aquí y haga clic en Siguiente como se muestra en la imagen.



3. Introduzca la contraseña del usuario y haga clic en Iniciar sesión.



4. Ahora se le redirigirá al panel de aplicación de ISE con los permisos adecuados configurados en función del grupo de ISE configurado anteriormente, como se muestra en la imagen.



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de

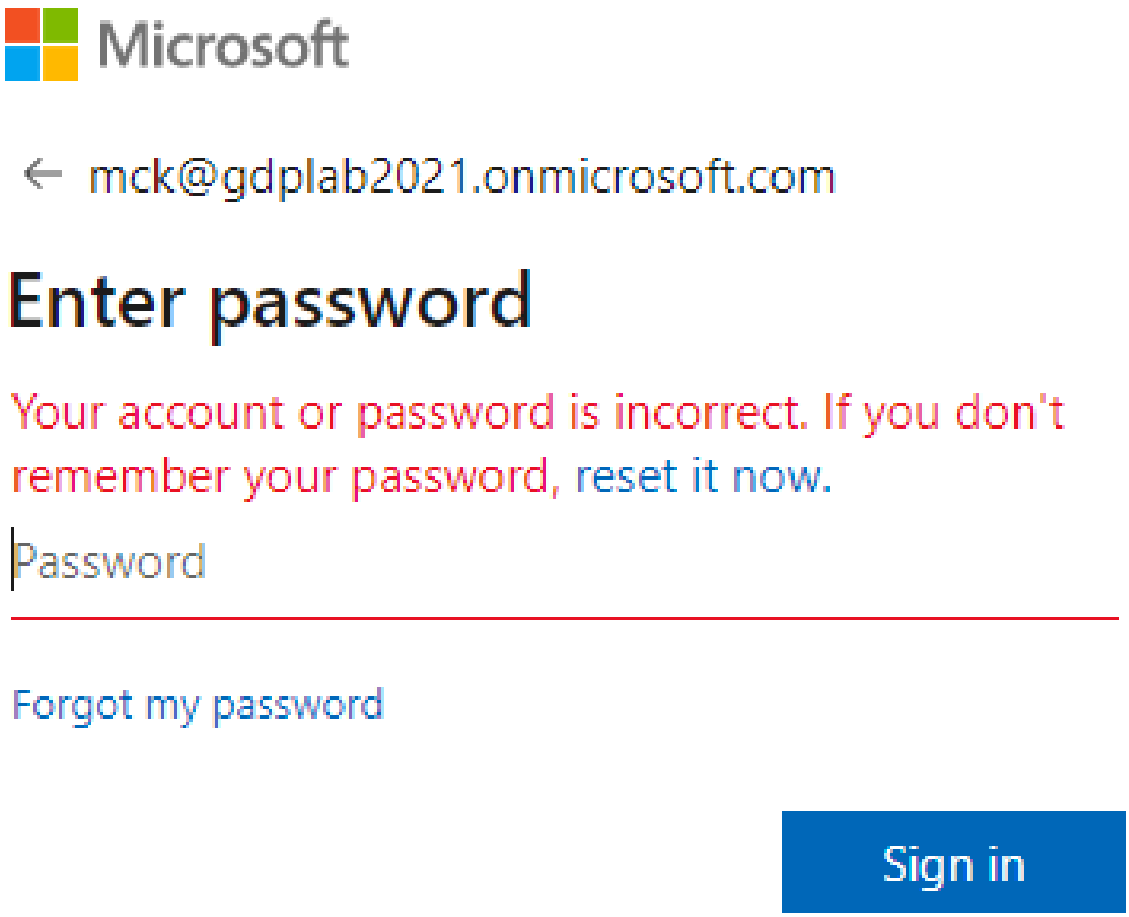
configuración.

Problemas comunes

Es fundamental comprender que la autenticación SAML se controla entre el explorador y Azure Active Directory. Por lo tanto, puede obtener errores relacionados con la autenticación directamente desde el proveedor de identidad (Azure), donde el compromiso con ISE aún no ha comenzado.

Problema 1. Aparece el error "Su cuenta o contraseña es incorrecta" después de introducir las credenciales. En este caso, ISE aún no ha recibido los datos del usuario y el proceso en este momento aún permanece con IdP (Azure).

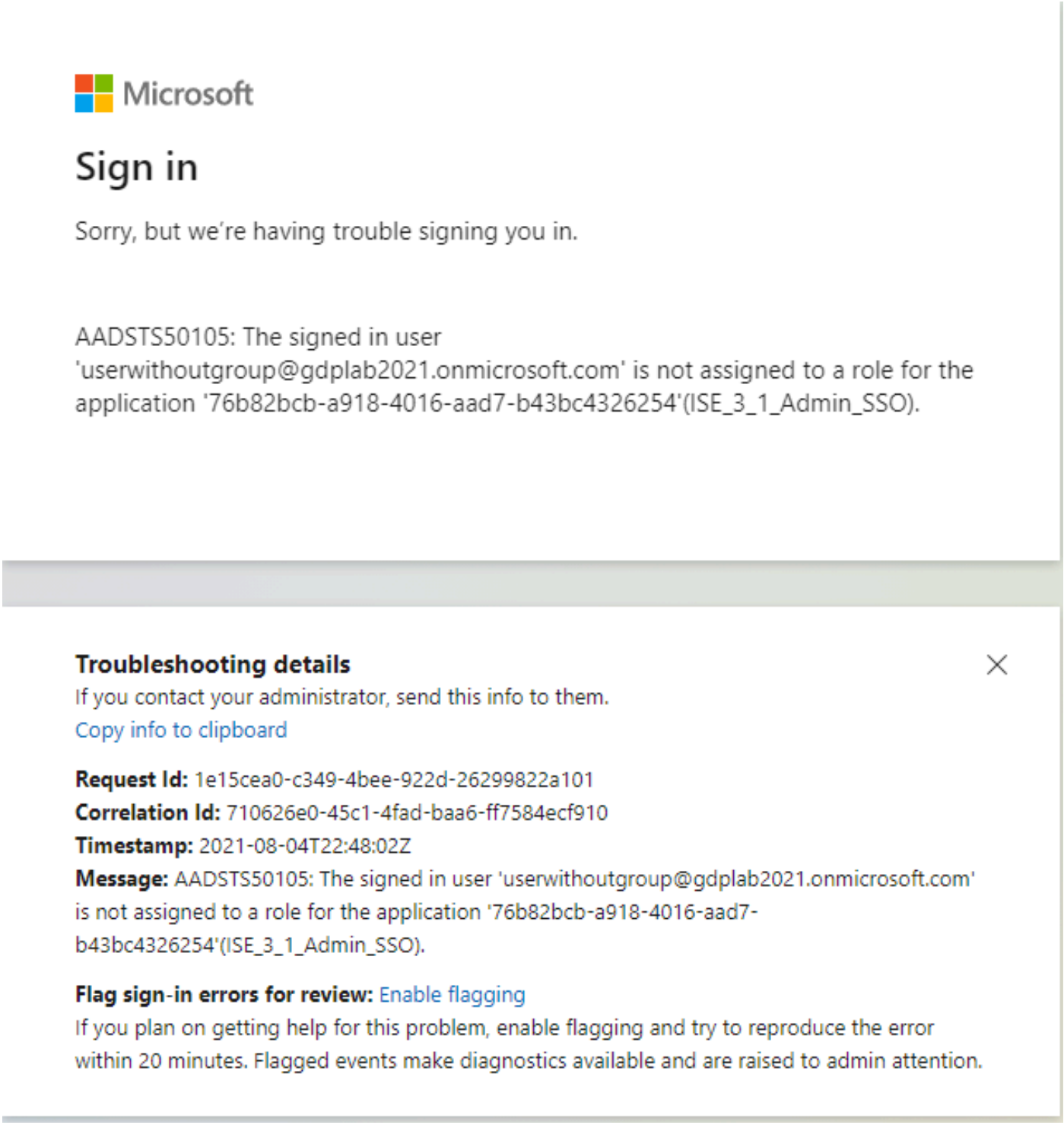
El motivo más probable es que la información de la cuenta sea incorrecta o que la contraseña no sea correcta. Para corregir: restablezca la contraseña o proporcione la contraseña correcta para esa cuenta como se muestra en la imagen.



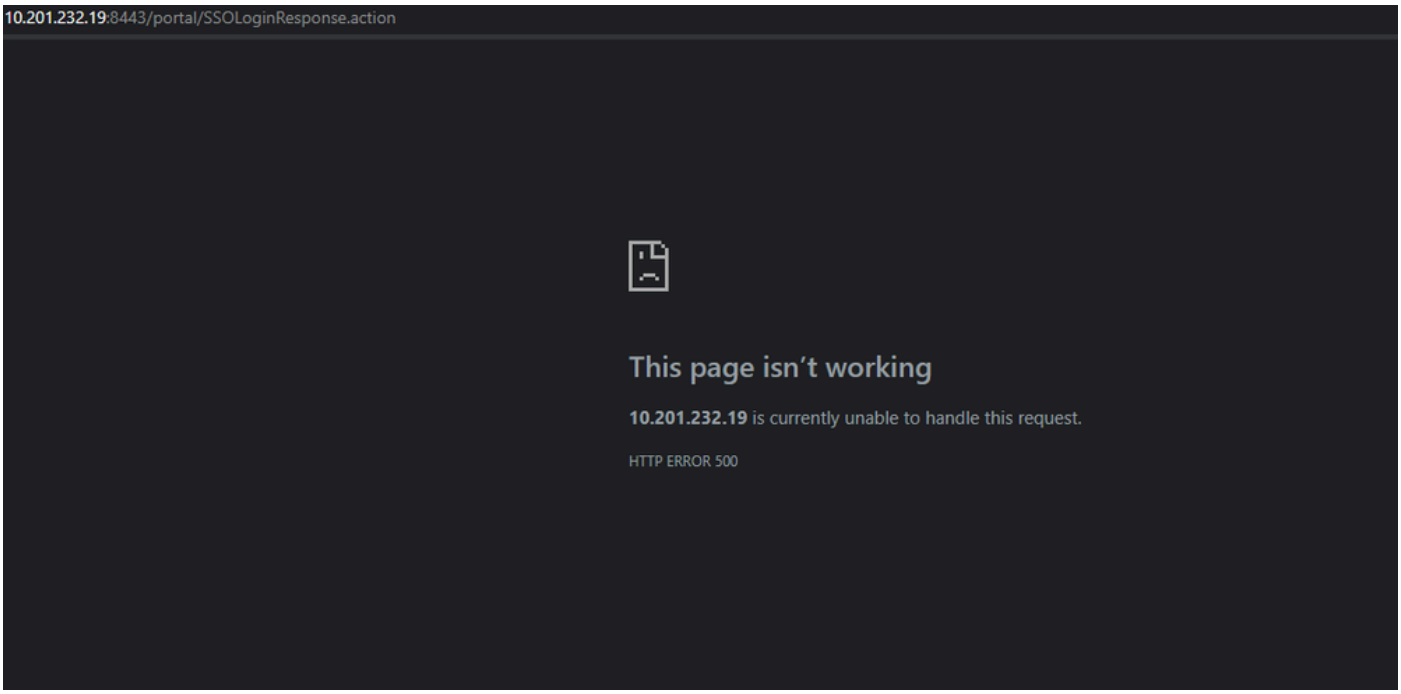
Problema 2. El usuario no es parte del grupo que se supone que tiene permiso para acceder a SSO SAML. Al igual que en el caso anterior, ISE aún no ha recibido los datos del usuario y, en

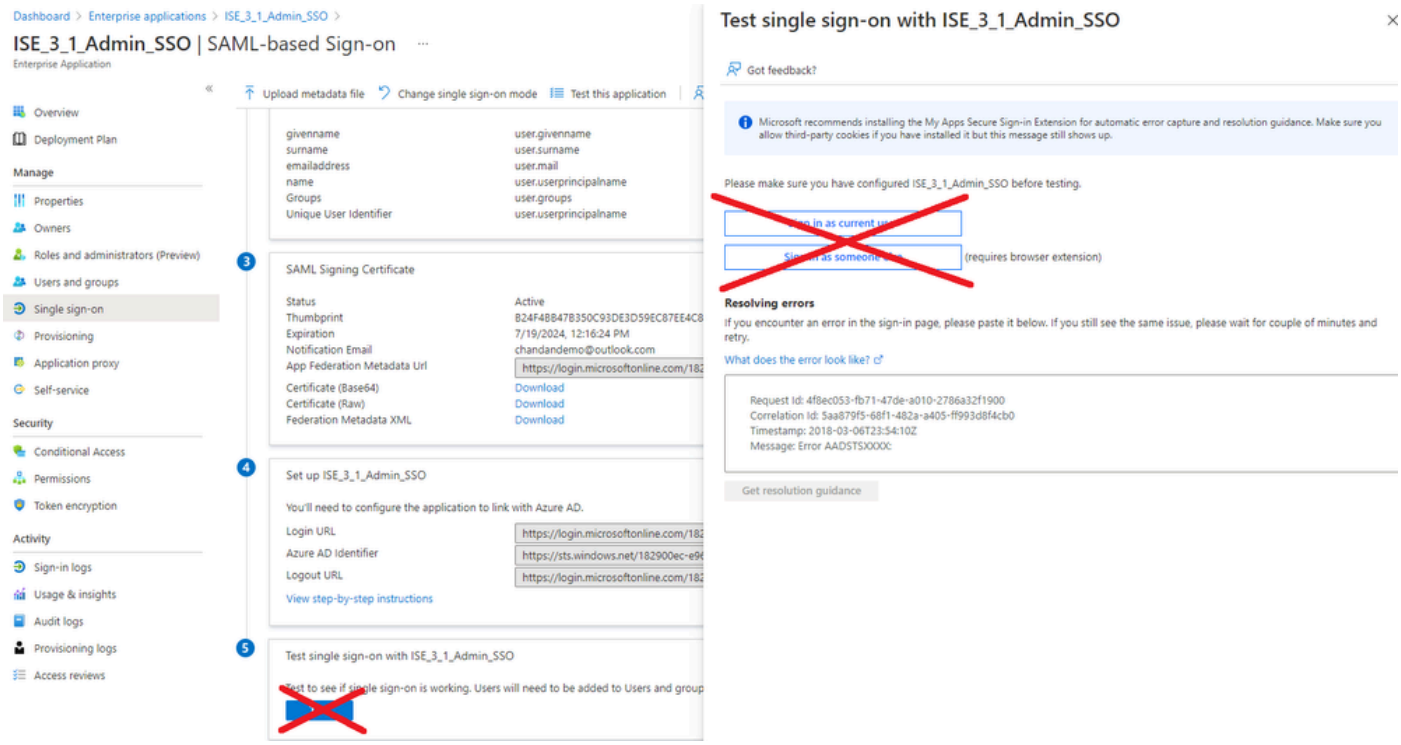
este momento, el proceso sigue en estado IdP (Azure).

Para corregir esto: verifique que el paso de configuración Agregar grupo a la aplicación se ejecute correctamente como se muestra en la imagen.



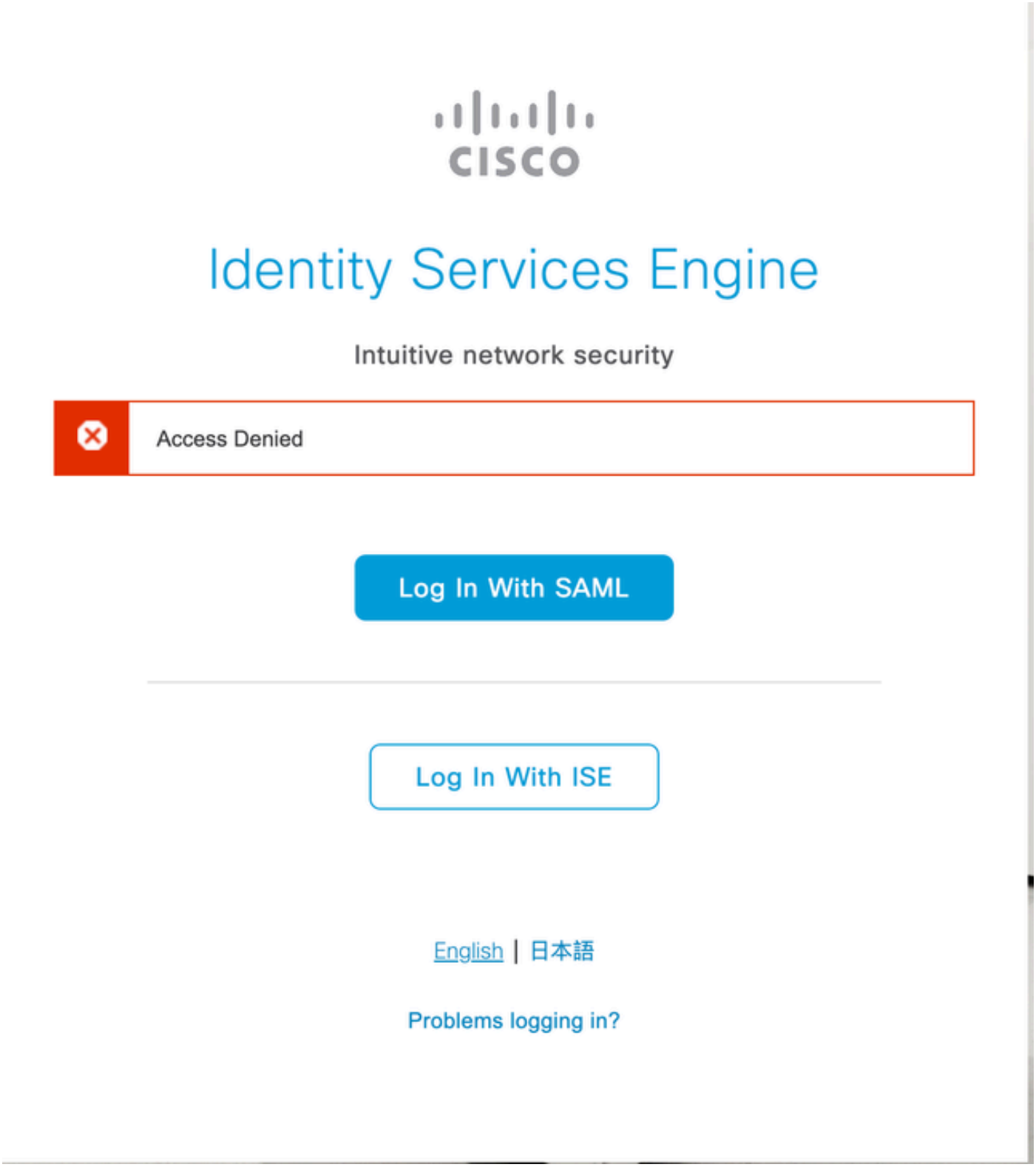
Problema 3. ISE Application Server no puede gestionar las solicitudes de inicio de sesión de SAML. Este problema ocurre cuando la solicitud SAML se inicia desde el proveedor de identidad, Azure, en lugar del proveedor de servicios, ISE. La prueba de inicio de sesión de SSO desde Azure AD no funciona, ya que ISE no admite solicitudes SAML iniciadas por el proveedor de identidad.





Problema 4. ISE muestra el error "Acceso denegado" después de un intento de inicio de sesión. Este error se produce cuando el nombre de notificación del grupo creado anteriormente en la aplicación empresarial de Azure no coincide en ISE.

Para solucionar esto: asegúrese de que el nombre de notificación de grupo en Azure e ISE en la pestaña Grupos de proveedores de identidad SAML sea el mismo. Consulte los pasos 2.7 y 4 en la sección Configuración de SSO SAML con Azure AD de este documento para obtener más detalles.



Troubleshooting de ISE

El nivel de registro de los componentes debe modificarse en ISE. Vaya a Operaciones > Solución de problemas > Asistente de depuración > Configuración del registro de depuración.

Nombre del componente	Nivel de registro	Nombre de archivo de registro

portal	DEPURAR	guest.log
opensmal	DEPURAR	ise-psc.log
pequeño	DEPURAR	ise-psc.log

Registros con inicio de sesión SAML y nombres de reclamación de grupo no coincidentes

Conjunto de depuraciones que muestran el escenario de resolución de problemas de discrepancia de nombres de notificaciones en el momento de la ejecución del flujo (ise-psc.log).

Nota: Esté atento a los elementos en negrita. Los registros se han acortado con fines de claridad.

1. El usuario es redirigido a la URL de IdP desde la página de administración de ISE.

<#root>

```
2021-07-29 13:48:20,709 INFO   [admin-http-pool46][] api.services.persistance.dao.DistributionDAO -::::
2021-07-29 13:48:20,712 INFO   [admin-http-pool46][] cpm.admin.infra.spring.ISEAdminControllerUtils -::
```

forwardStr for: https://10.201.232.19/admin/LoginAction.do

```
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

IDP URL: https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2

```
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

SAML request - spUrlToReturnTo:https://10.201.232.19:8443/portal/SSOLoginResponse.action

```
2021-07-29 13:48:20,844 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,851 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

2. La respuesta SAML se recibe desde el navegador.

<#root>

```
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

```
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI

-::::- Decoded SAML relay state of: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a

2021-07-29 13:48:27,177 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode

-::::- Decoded SAML message

2021-07-29 13:48:27,182 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.saml2.binding.dec
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -::::- Intended message destination endpoint: h
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de
```

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM

3. Se inicia el análisis de atributos (aserción).

<#root>

```
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM

```
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

[parseAttributes] Set on IdpResponse object - attribute<http://schemas.xmlsoap.org/ws/2005/05/identity/

```
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

4. El atributo de grupo se recibe con el valor 576c60ec-c0b6-4044-a8ec-d395b1475d6e,

validación de firmas.

```
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
        IdP URI: https://sts.windows.net/182900ec-e960-4340-bd20-e4522197ecf8/
        SP URI: http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd
        Assertion Consumer URL: https://10.201.232.19:8443/portal/SSOLoginResponse.action
        Request Id: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2fd-7047-4d1d-89
        Client Address: 10.24.226.171
        Load Balancer: null
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,358 INFO   [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImp
```

5. Validación de la autorización RBAC.

<#root>

```
************************Rbac Log Summary for user samlUser************************
2021-07-29 13:48:27,360 INFO   [admin-http-pool50][] com.cisco.ise.util.RBACUtil -::::- Populating cach

2021-07-29 13:48:27,368 ERROR  [admin-http-pool50][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::

java.lang.NullPointerException

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- In Login
```

```
2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- In Login

2021-07-29 13:48:27,369 ERROR  [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- Can't sav

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginActionResultHandler -::

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::
```

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).