

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Proveedor de identidad \(IdP\):](#)

[Proveedor de servicios \(SP\):](#)

[SAML](#)

[Afirmación SAML](#)

[Diagrama de flujo de alto nivel](#)

[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](#)
- [2. Configurar el método de autenticación de ISE](#)
- [3. Exportar información del proveedor de servicios](#)

[Paso 2. Configurar Azure AD IdP Settings](#)

- [1. Crear un usuario de Azure AD](#)
- [2. Crear un grupo de Azure AD](#)
- [3. Asignar usuario de Azure AD al grupo](#)
- [4. Crear una aplicación empresarial de Azure AD](#)
- [5. Agregar grupo a la aplicación](#)
- [6. Configurar una aplicación empresarial de Azure AD](#)
- [7. Configurar el atributo de grupo de Active Directory](#)
- [8. Descargar el archivo XML de metadatos de Azure Federation](#)

[Paso 3. Cargar metadatos de Azure Active Directory en ISE](#)

[Paso 4. Configuración de grupos SAML en ISE](#)

[\(Optativo\) Paso 5. Configuración de políticas RBAC](#)

[Verificación](#)

[Troubleshoot](#)

[Problemas comunes](#)

[Troubleshooting de ISE](#)

[Registros con inicio de sesión SAML y nombres de reclamación de grupo no coincidentes](#)

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.

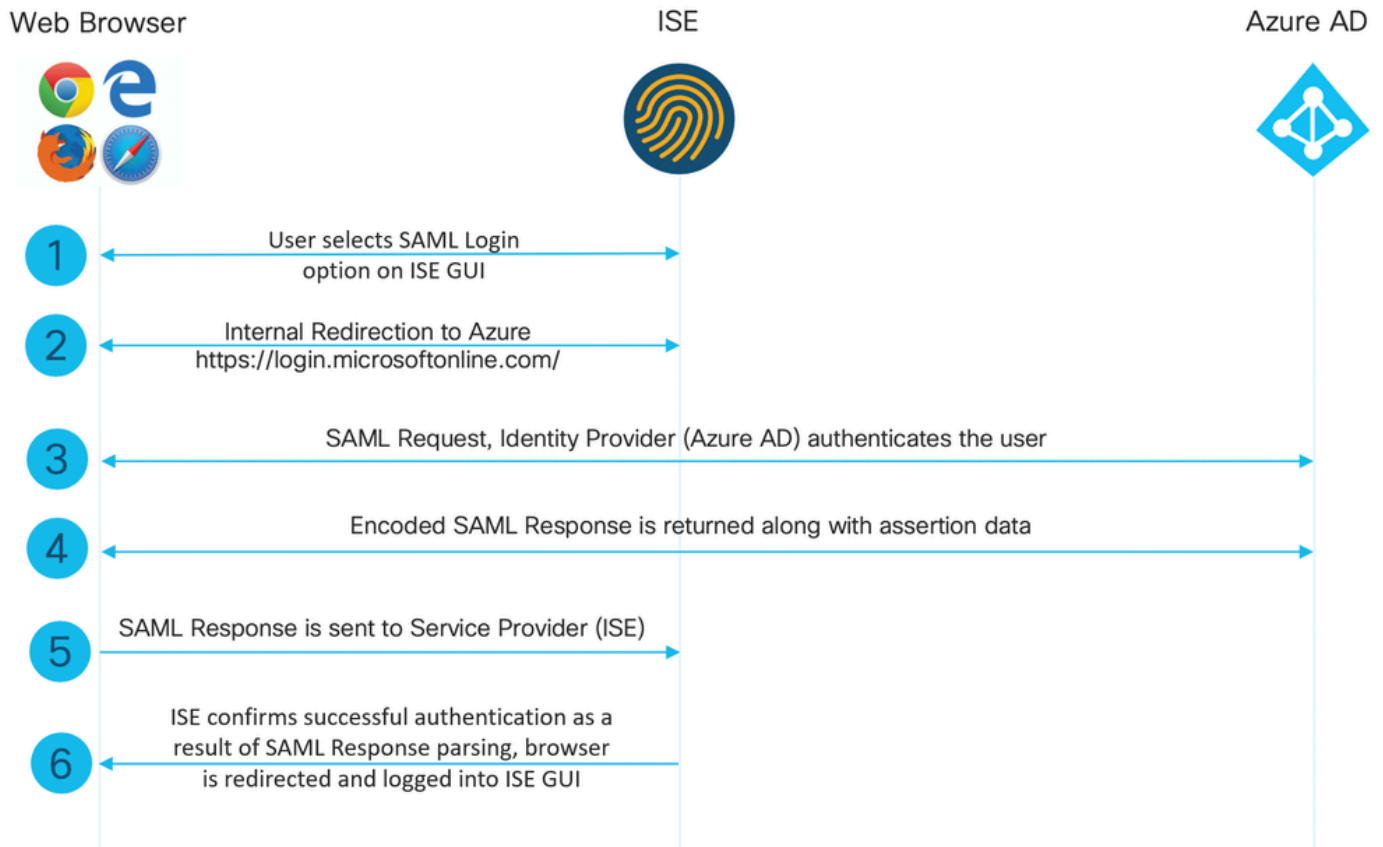
- Las aserciones de autenticación prueban la identificación del usuario y proporcionan la hora de inicio de sesión del usuario y el método de autenticación que utilizan (Kerberos, de dos factores, como ejemplos)
- La aserción de atribución pasa los atributos SAML, datos específicos que proporcionan información 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.

External Identity Sources

- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers
- Social Login

Identity Provider List > Azure

SAML Identity Provider

General Identity Provider Config. Service Provider Info. Groups Attributes Advanced Settings

* Id Provider Name	Azure
Description	Azure_SSO_Admin_Login

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.

Authentication

Authorization >

Administrators >

Settings >

Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings

Authentication Type ⓘ

- Password Based
- Client Certificate Based

* Identity Source

SAML:Azure

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.

SAML Identity Provider

General Identity Provider Config. **Service Provider Info.** Groups Attributes Advanced Settings

Service Provider Information

Load balancer ⓘ

Export Service Provider Info. **Export** ⓘ

Includes the following portals:

Sponsor Portal (default)

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:oasis:
<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>
MIIFTjCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT
QU1MX2lZTMTMS0xOS5ja3VtYXlyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTG1NBtUxfaXN1My0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCGKCAgEAvila4+S0uP3j037yCOXnHAzADupfqcgcwcp1JQnFhxvfnDd0ixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohG0t1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDziyzyGKdDpf+1VM5JHCo6UNLF1IFyPmGvcCXnt
NVqsYvxSzF038ciQq1m0sqrVrryZuIUAXDWUNUg9pSGzH0FkSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83g4L4WJMiZET06Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0sshkGSjgVn31XQ5vgDH1PvqNaYs/PWicvmI/
wYKSTn9/hn7JM1DqOR1PGEKvjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/1avr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBTO+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9v4E0zwnGo7pQI8CAwEAAAN9MhswIAYDVR0RBbkwF4IVaXN1My0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHUEFjAUBggrBgEFBQCDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwqxvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9Fshn
CGchSHqDt3bQ7g+Gw1vcgreC7R46qenaonXVr1tRw11vVIcF8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUteif0bqroWcyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwvt6gfH0bE51uT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmdh9g2mppbBw0cxzoUxDm+HReSe+0JhRCyIJc0vUpdNmYC8cFAZuiv/e3wk0BLZM
TgV8FTVQSnra9LwHP/PgeNAPUcRPXSwake4rvjvMc0aS/iYdwZhziJ8zBdIBanMv5mGu1nvTEt9K
EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTfjfoITTMdQXNHhg+w1POKXS2GCZ29vAM52d8ZCq
Urz0VxNHKWKwER/q1GgaWvh3X/G+z1shUQDRjCbdLcZi1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/nchcoxFY759LA+m7Brp7FFPiGCrPW8E0v7bUMSDmmg/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://CiscoSE/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.

The screenshot displays the Azure Active Directory admin center interface. The left sidebar shows the navigation menu with 'Azure Active Directory' highlighted in a red box. The main content area shows the 'Default Directory | Overview' page. The page includes a search bar for the tenant, a 'Tenant information' card showing the user's role as 'Global administrator', the license as 'Azure AD Premium P2', the tenant ID, and the primary domain 'ekorneyccisco.onmicrosoft.com'. There is also an 'Azure AD Connect' card showing the status as 'Not enabled' and 'Last sync' as 'Sync has never run'. At the bottom, there is a 'Sign-ins' table with the following data:

Sign-ins
3
2.8
2.6
2.4
2.2
2

The date 'Aug 23' is visible in the bottom right corner of the interface.

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.

Identity

User name * ⓘ

mck ✓

@

gdplab2021.onmicrosoft... ▾



The domain name I need isn't shown here

Name * ⓘ

mck ✓

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password

.....

Show Password

Create

2. Crear un grupo de Azure AD

Seleccione Grupos. Haga clic en Nuevo grupo.

[Dashboard](#) > [Default Directory](#) > [Groups](#)



Groups | All groups

Default Directory - Azure Active Directory

<<

+ New group



Download groups



Delete



Refresh



Columns

All groups

Deleted groups

Diagnose and solve problems



This page includes previews available for your evaluation. [View previews](#) →

Search groups

Add filters

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

Dashboard > TAC > Groups >

New Group

Group type * ⓘ
Security

Group name * ⓘ
ISE Admin Group

Group description ⓘ
Enter a description for the group

Azure AD roles can be assigned to the group ⓘ
Yes No

Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

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.

Add members



Search ⓘ



mck
mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

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.

Dashboard >

Groups | All groups

TAC - Azure Active Directory

- All groups
 - Deleted groups
 - Diagnose and solve problems
- Settings
- General
 - Expiration
 - Naming policy

+ New group | Download groups | Delete | Refresh | Columns | Preview features | Got feedback?

This page includes previews available for your evaluation. View previews →

Search groups | Add filters

Name	Object Id	Group Type	Membership Type
<input type="checkbox"/> I ISE Admin Group	576c60ec-c0b6-4044-a8ec-d395b1475d6e	Security	Assigned

4. Crear una aplicación empresarial de Azure AD

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

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications

Enterprise applications | All applications

Default Directory - Azure Active Directory

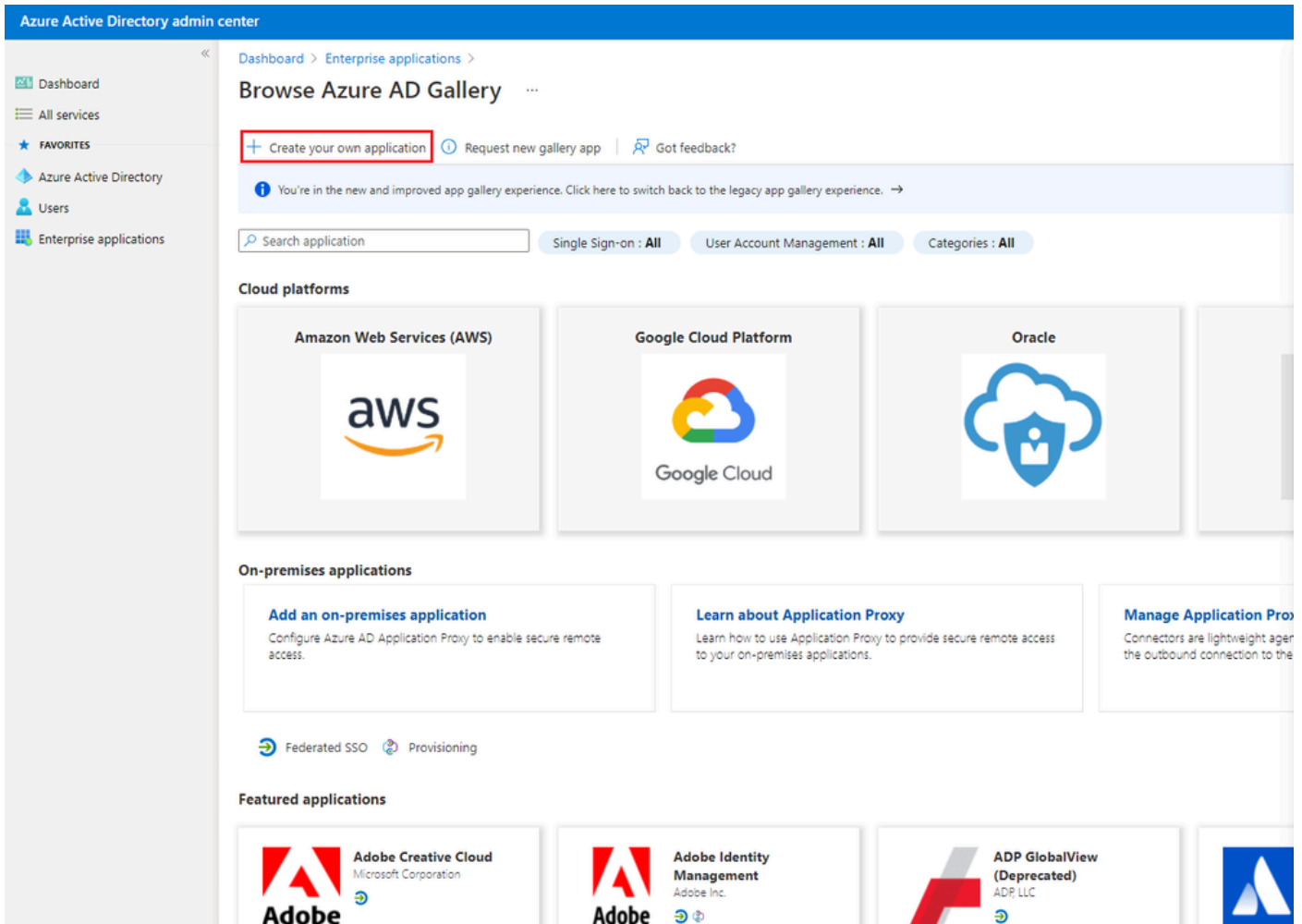
+ New application | Columns | Preview features | Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type: Enterprise Applications | Applications status: Any | Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

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.

Create your own application



What's the name of your app?

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 Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Create

5. Agregar grupo a la aplicación

Seleccione Asignar usuarios y grupos.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Properties

Name: ISE_3_1_Admin_SSO

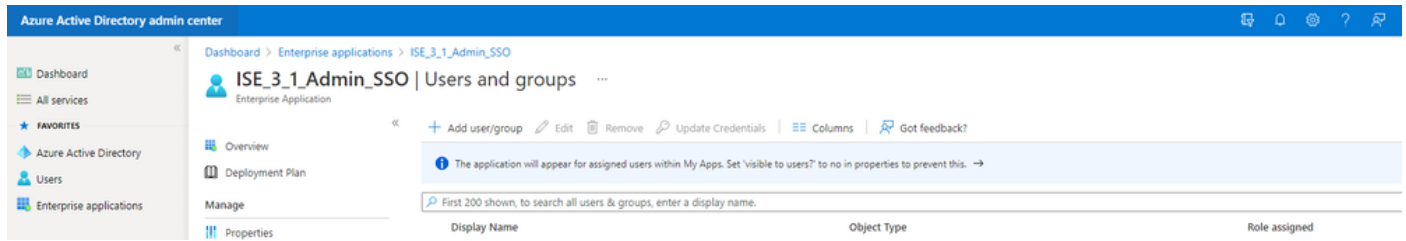
Application ID: 76b82bcb-a918-4016-aad7-...

Object ID: 22aedf32-82c7-47f2-ab34-1...

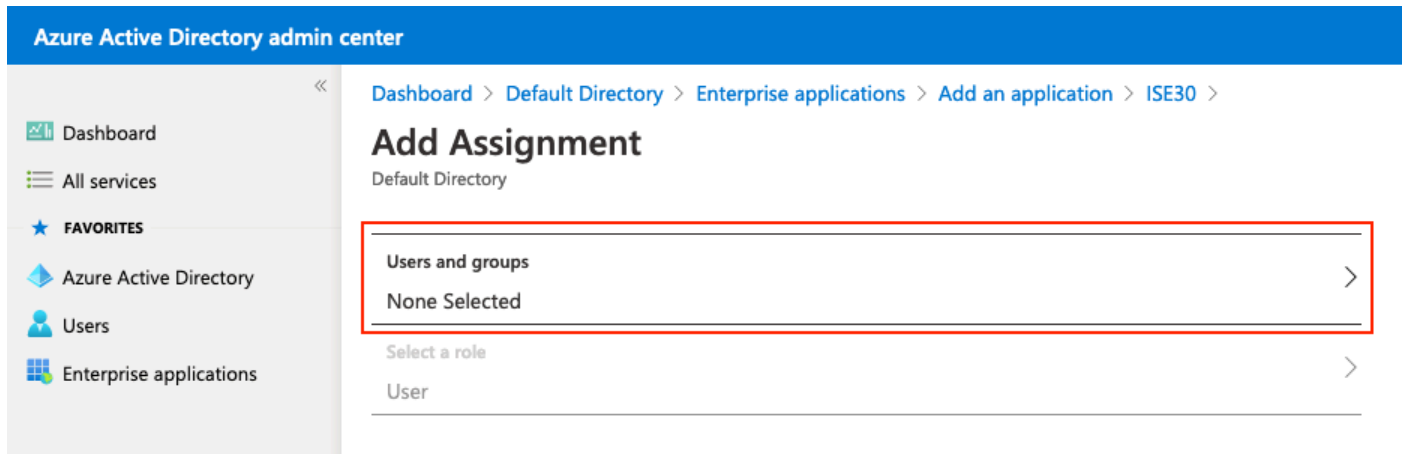
Getting Started

- 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 Azure AD credentials
[Get started](#)


Haga clic en Agregar usuario/grupo.



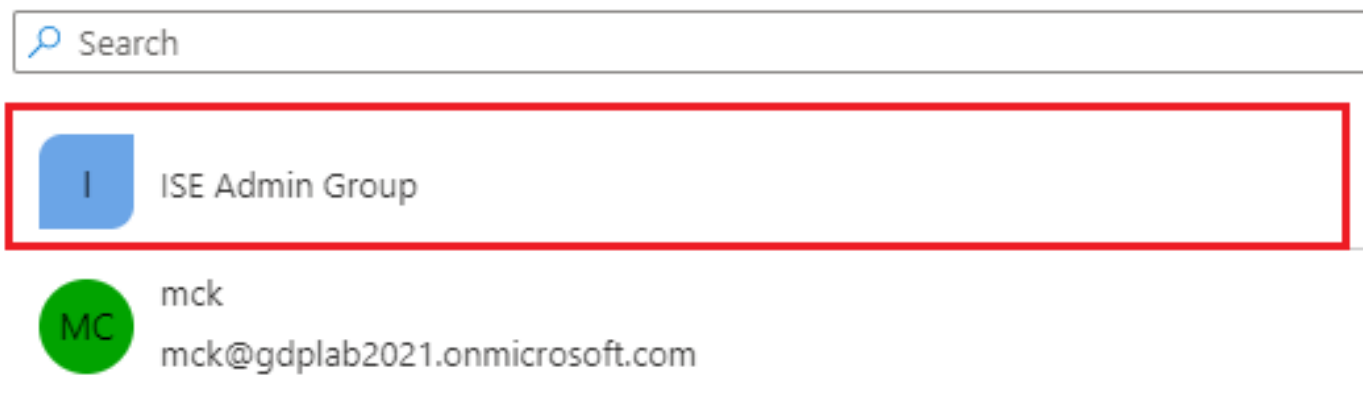
Haga clic en Usuarios y grupos.



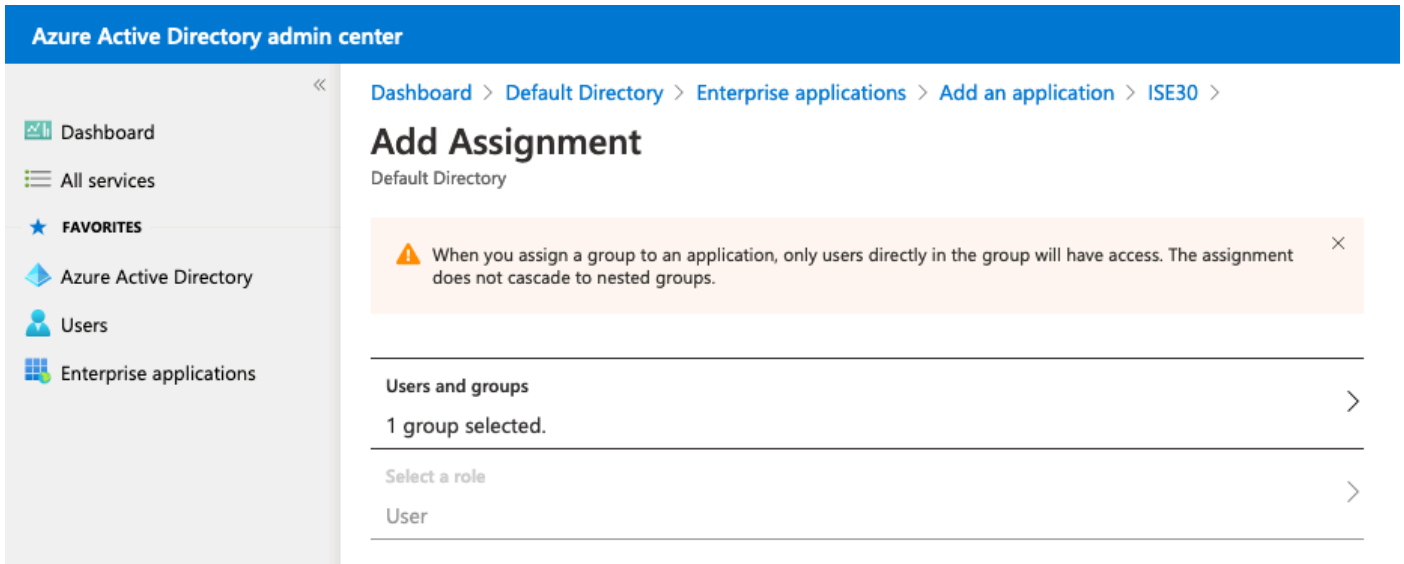
Elija el grupo configurado anteriormente y haga clic en Seleccionar.

 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.

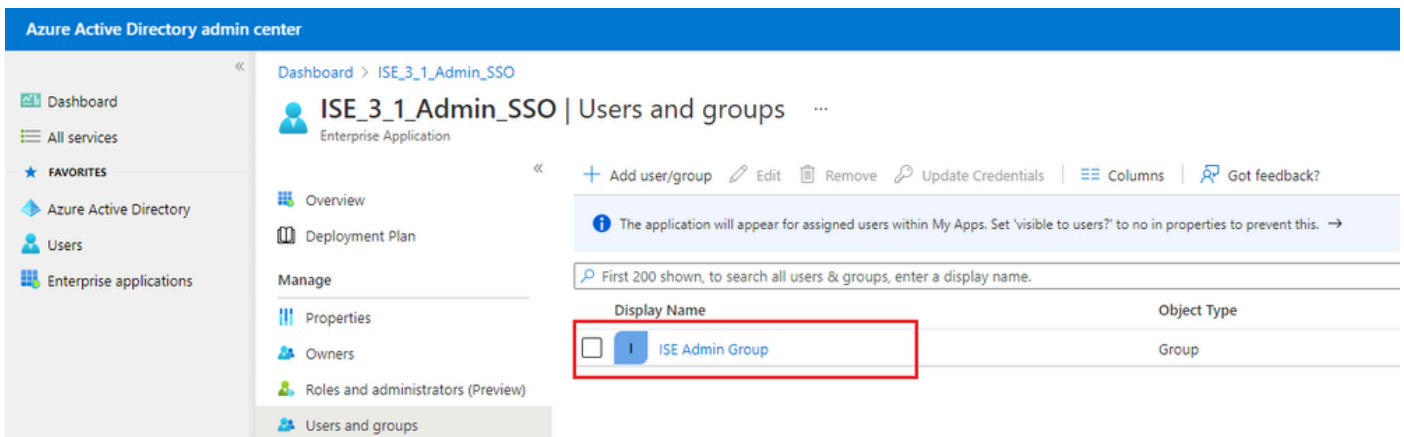
Users and groups



Una vez seleccionado el grupo, haga clic en Asignar.

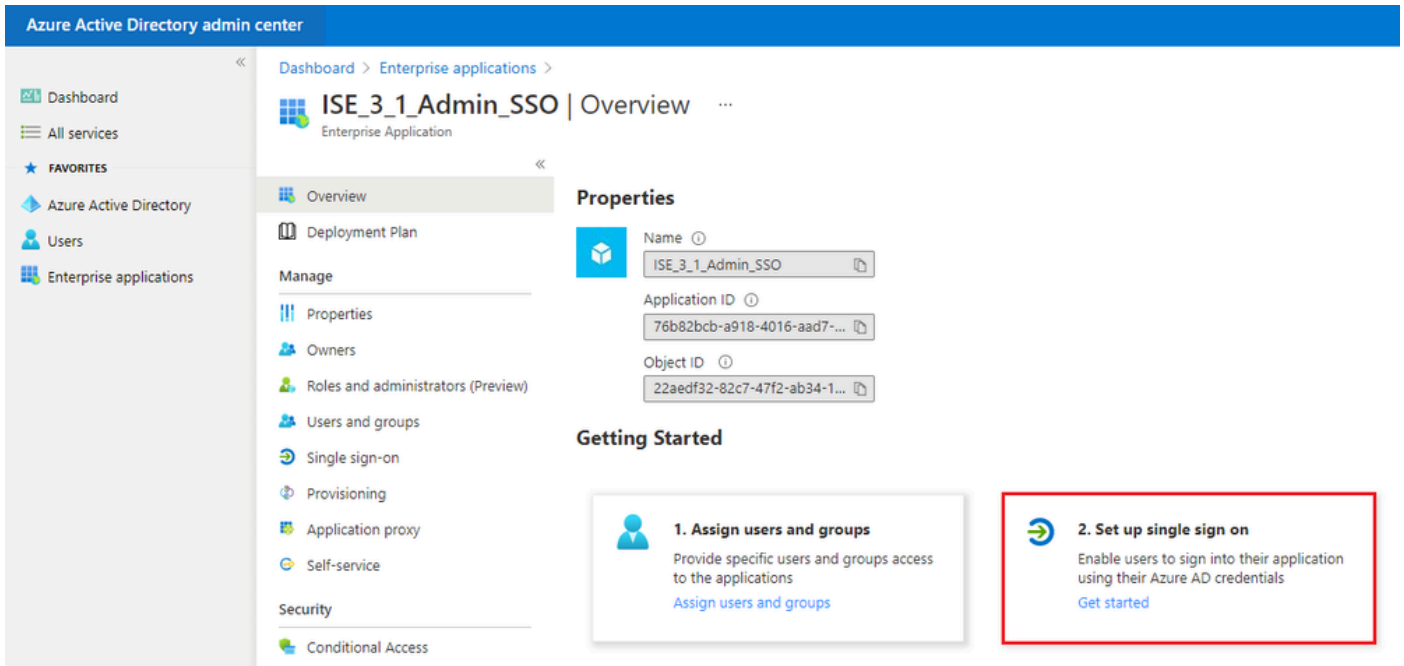


Como resultado, el menú Users and groups para la aplicación configurada se completa con el grupo seleccionado.

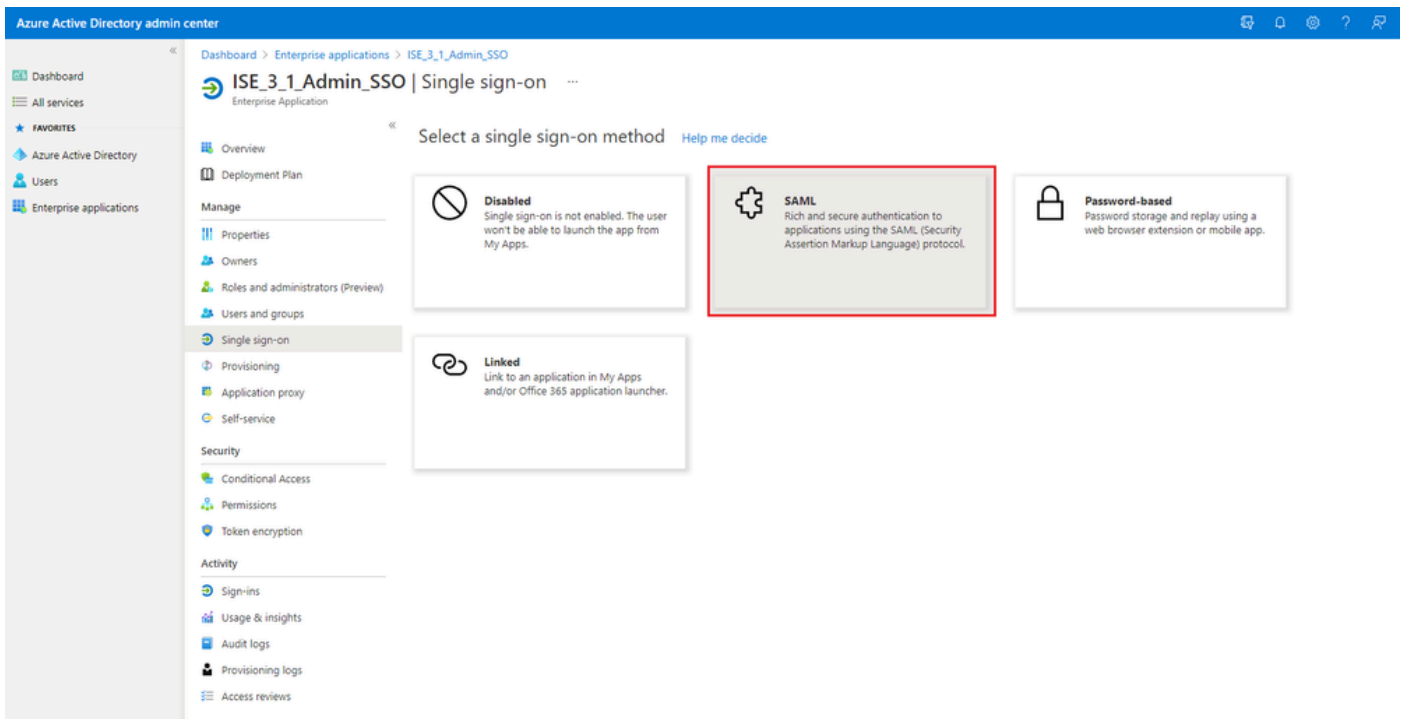


6. Configurar una aplicación empresarial de Azure AD

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.

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating ISE30.

1


Basic SAML Configuration

 Edit

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


2

User Attributes & Claims

 Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

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.

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname



Haga clic en Agregar una reclamación de grupo.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

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.

Group Claims



Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- None
- All groups
- Security groups
- Directory roles
- Groups assigned to the application

Source attribute *

Group ID



Advanced options

- Customize the name of the group claim

Name (required)

Groups

Namespace (optional)

- Emit groups as role claims ⓘ

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

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***

Additional claims

Claim name	Value
Groups	user.groups ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

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.

SAML Signing Certificate Edit

Status: Active

Thumbprint: B24F4BB47B350C93DE3D59EC87EE4C815C884462

Expiration: 7/19/2024, 12:16:24 PM

Notification Email: chandandemo@outlook.com

App Federation Metadata Url: <https://login.microsoftonline.com/182900ec-e960...>

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)



Federation Metadata XML: [Download](#)

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.

External Identity Sources

- <  
- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers
- Social Login

Identity Provider List > Azure

SAML Identity Provider

General Identity Provider Config. Service Provider Info. Groups Attributes Advanced Settings

Identity Provider Configuration

Import Identity Provider Config File ⓘ

Provider Id

Single Sign On URL <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>

Single Sign Out URL (Redirect) <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>



Signia Certificates

Subject	Issuer	Valid From	Valid To (Expira...	Serial Number
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azur...	Mon Jul 19 12:16:2...	Fri Jul 19 12:16:24 ...	25 28 CB 30 8B A4 89 8...

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.

External Identity Sources

- <  
- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers

Identity Provider List > Azure

SAML Identity Provider

General Identity Provider Config. Service Provider Info. **Groups** Attributes Advanced Settings

Groups

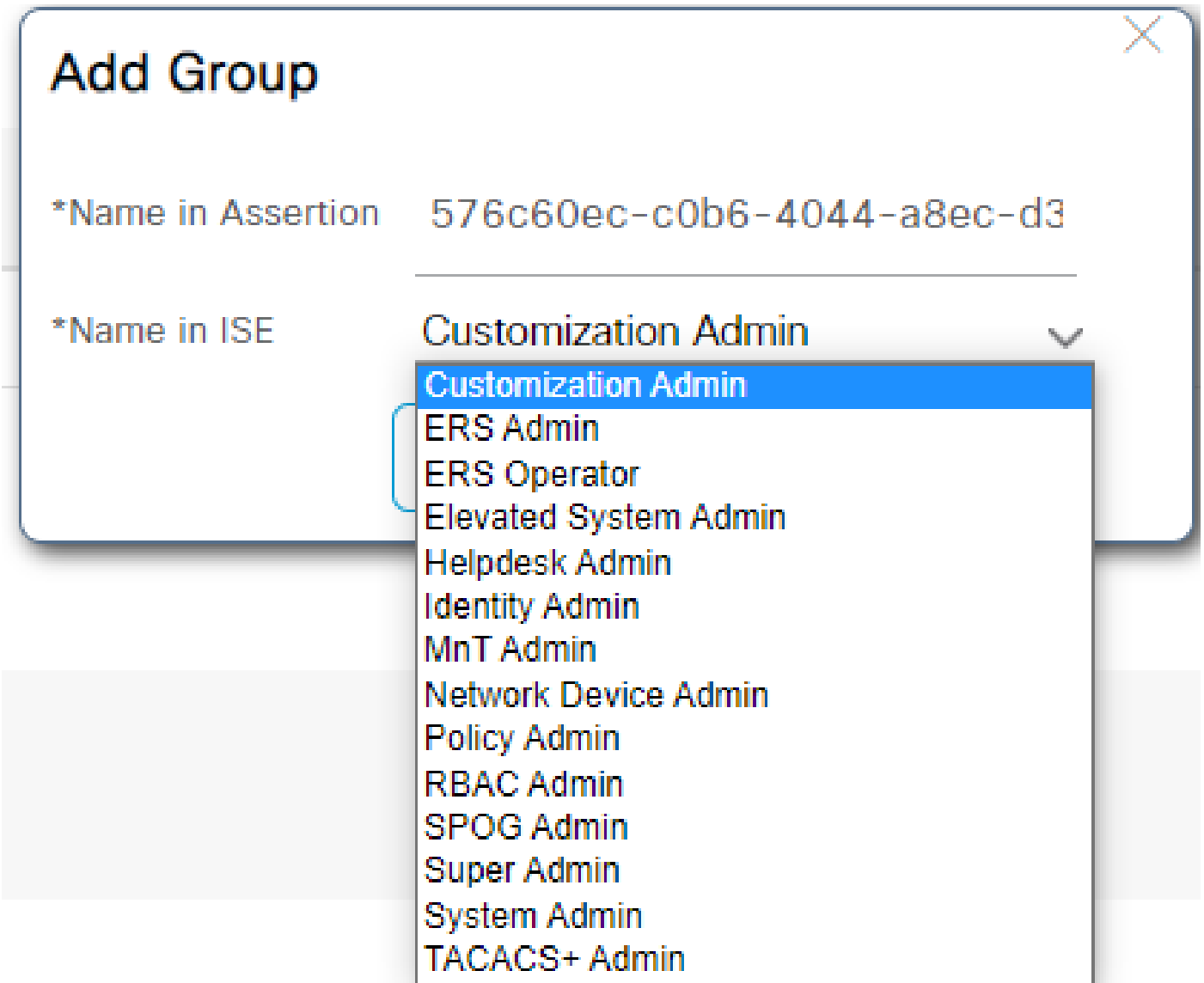
Group Membership Attribute ⓘ

Name in Assertion ^ Name in ISE

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.

▼ RBAC Policies

Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin	then Customization Admin Menu ...
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin	then System Admin Menu Access...
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	then Super Admin Data Access
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	then Super Admin Data Access
<input checked="" type="checkbox"/> ERS Trustsec Policy	If ERS Trustsec	then Super Admin Data Access
<input checked="" type="checkbox"/> Helpdesk Admin Policy	If Helpdesk Admin	then Helpdesk Admin Menu Access
<input checked="" type="checkbox"/> Identity Admin Policy	If Identity Admin	then Identity Admin Menu Access...
<input checked="" type="checkbox"/> MnT Admin Policy	If MnT Admin	then MnT Admin Menu Access
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin	then Network Device Menu Acce...
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin	then Policy Admin Menu Access ...
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin	then RBAC Admin Menu Access ...
<input checked="" type="checkbox"/> Read Only Admin Policy	If Read Only Admin	then Super Admin Menu Access ...
<input checked="" type="checkbox"/> SPOG Admin Policy	If SPOG Admin	then Super Admin Data Access
<input checked="" type="checkbox"/> Super Admin Policy	If Super Admin	then Super Admin Menu Access ...
<input checked="" type="checkbox"/> Super Admin_Azure	If Super Admin	then Super Admin Menu Access ...
<input checked="" type="checkbox"/> System Admin Policy	If System Admin	then System Admin Menu Access...
<input checked="" type="checkbox"/> TACACS+ Admin Policy	If TACACS+ Admin	then TACACS+ Admin Menu Acc...

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.



Identity Services Engine

Intuitive network security

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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.



Sign in

mck@gdplab2021.onmicrosoft.com

[Can't access your account?](#)

Next

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



← mck@gdplab2021.onmicrosoft.com

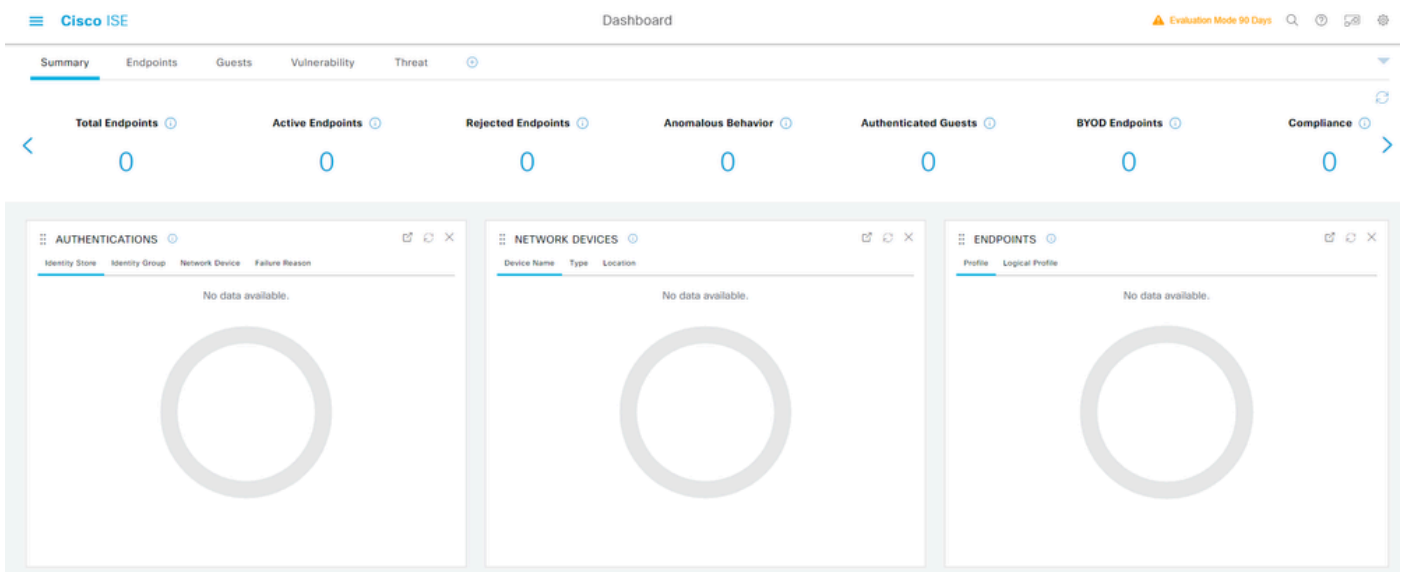
Enter password

••••••••••

[Forgot my password](#)

Sign in

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.



← mck@gdplab2021.onmicrosoft.com

Enter password

Your account or password is incorrect. If you don't remember your password, reset it now.

Password

[Forgot my password](#)

Sign in

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.



Sign in

Sorry, but we're having trouble signing you in.

AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Troubleshooting details ✕

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Request Id: 1e15cea0-c349-4bee-922d-26299822a101

Correlation Id: 710626e0-45c1-4fad-baa6-ff7584ecf910

Timestamp: 2021-08-04T22:48:02Z

Message: AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Flag sign-in errors for review: [Enable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

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.



This page isn't working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500

ISE_3_1_Admin_SSO | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators (Preview)
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews

Upload metadata file | Change single sign-on mode | Test this application

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Groups	user.groups
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	824F48B478350C93DE3D59EC87EE4C8
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182900ec-e99d-4423-b017-080020331378/...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up ISE_3_1_Admin_SSO

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/182900ec-e99d-4423-b017-080020331378/...
Azure AD Identifier	https://sts.windows.net/182900ec-e99d-4423-b017-080020331378/
Logout URL	https://login.microsoftonline.com/182900ec-e99d-4423-b017-080020331378/...

[View step-by-step instructions](#)

5 Test single sign-on with ISE_3_1_Admin_SSO

Test to see if single sign-on is working. Users will need to be added to Users and group

Test single sign-on with ISE_3_1_Admin_SSO

Got feedback?

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up.

Please make sure you have configured ISE_3_1_Admin_SSO before testing.

~~Sign in as current user~~
~~Sign in as someone else~~ (requires browser extension)

Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

What does the error look like?

Request id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation id: Saa879f5-68f1-482a-a405-f993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXXX

[Get resolution guidance](#)

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.



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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 acertado 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.persistence.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.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7] [] cpm.sam].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.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7] [] cpm.sam].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.sam].framework.impl.SAM
2021-07-29 13:48:20,851 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7] [] cpm.sam].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.sam].framework.impl.SAM
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
```


2021-07-29 13:48:27,369 INFO [admin-http-pool150][] cpm.admin.infra.action.LoginAction -::::- In Login

2021-07-29 13:48:27,369 ERROR [admin-http-pool150][] cpm.admin.infra.action.LoginAction -::::- Can't sav

2021-07-29 13:48:27,369 INFO [admin-http-pool150][] cpm.admin.infra.action.LoginActionResultHandler -::

2021-07-29 13:48:27,369 INFO [admin-http-pool150][] 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).