# 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** Términos 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 Paso 2. Configuración de Azure AD IdP Settings Paso 3. Cargar metadatos de Azure Active Directory a ISE Paso 4. Configuración de grupos SAML en ISE (Opcional) 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): 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 el idP para pasar las credenciales de autorización al SP.

Las transacciones SAML utilizan 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.

Las solicitudes de autorización y autenticación de ISE de Azure AD se muestran 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.

| ≡ Cisco ISE  |   |                               | Administration - Identity Management |
|--|---|-------------------------------|--------------------------------------|
| Identities Groups External Ide   | ntity Sources Identity Source Sequences   | Settings                      |                                      |
| External Identity Sources < <il> <li>Certificate Authentication F</li> </il>   | Identity Provider List > Azure<br>SAML Identity Provider<br>General Identity Provider Config. 5 | Service Provider Info. Groups | Attributes Advanced Settings         |
| <ul> <li>Active Directory</li> <li>LDAP</li> <li>ODBC</li> <li>RADIUS Token</li> <li>RSA SecurID</li> <li>SAML Id Providers</li> <li>Social Login</li> </ul> | * Id Provéder Name Azure<br>Description Azure_SSO_Admin_Login                                   |                               |                                      |

2. Configure el método de autenticación 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.

| ≡ Cisco        | SE        |                            |            |                 |              |                   |                  | Administration · S | ystem    |
|----------------|-----------|----------------------------|------------|-----------------|--------------|-------------------|------------------|--------------------|----------|
| Deployment     | Licensing | Certificates               | Logging    | Maintenance     | Upgrade      | Health Checks     | Backup & Restore | Admin Access       | Settings |
| Authentication |           | Authenticatio              | on Method  | Password Policy | Account Disa | ble Policy Lock/S | Suspend Settings |                    |          |
| Authorization  | >         | Authentica                 | tion Type  | 0               |              |                   |                  |                    |          |
| Administrators | >         |                            |            |                 |              |                   |                  |                    |          |
| Settings       | >         | Password     Client Cer    | Based      |                 |              |                   |                  |                    |          |
|                |           | * Identity Sou<br>SAML:Azu | rce<br>ire | ~               |              |                   |                  |                    |          |

3. Información del proveedor de servicios de exportación:

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

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

| lde | entity Provider List > | Azure_SAML                |                        |        |            |                   |
|-----|------------------------|---------------------------|------------------------|--------|------------|-------------------|
| S   | AML Identity F         | Provider                  |                        |        |            |                   |
|     | General                | Identity Provider Config. | Service Provider Info. | Groups | Attributes | Advanced Settings |
|     | Service Provider Info  | ormation                  |                        |        |            |                   |
|     | Load balancer          |                           | (i)                    |        |            |                   |
|     | Export Service Provi   | ider Info. Export (i)     |                        |        |            |                   |
|     | Includes the           | following portals:        |                        |        |            |                   |
|     | Sponsor Portal (def    | ault)                     |                        |        |            |                   |
|     |                        |                           |                        |        |            |                   |

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> MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT QU1MX21zZTMtMS0x0S5ja3VtYXIyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa MCUxIzAhBqNVBAMTG1NBTUxfaXN1My0xLTE5LmNrdW1hcjIuY29tMIICIjANBqkqhkiG9w0BAQEF AAOCAg8AMIICCgKCAgEAvila4+S0uP3j037yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ 1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1op01qDGwtOnWZGQ+ccvqXSL Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDzizyjGKDdPf+1VM5JHCo6UNLF1IFyPmGvcCXnt NVqsYvxSzF038ciQq1m0sqrVrrYZuIUAXDWUNUg9pSGzH0FkSsZRPxrQh+3N5DEFF1Mzybvm1FYu 9h83gL4WJWMizET06Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ nGGkH5ROgT7v3CDrdFtRoNYAT+Yv0941KzFCSE0sshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/ wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1 sDU4u0vFpFvrcC/lavr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ ef+WFC9dWIy+ctbBT0+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVR0RBBkwF4IVaXN1My0xLTE5LmNrdW1hcjIuY29t MAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgLsMB0GA1UdDgQWBBRIkY2z/9H9PpwSn0PGARCj5iaZ oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL 206Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn CGchSHqDt3bQ7g+GW1vcgreC7R46qenaonXVr1tRw11vVIdCf8JQFFMxya/rIC4mxVeoo0j1F19d rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUtEi6f0bqr0wCyWd9Tjq7KXfd2ITW hMxaFsv8wWcVu0MDPkP9xUwwt6gfH0bE51uT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31 nf/341cuRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wk0BLZM lgV8FTVQSnra9LwHP/PgeNAPUcRPXSwaKE4rvjvMc0aS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTFjfoITTMdQXNHhg+w1P0KXS2GCZ29vAM52d8ZCq UrzOVxNHKWKwER/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: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/SS0LoginResponse.act
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SS0Login
</md:SPSS0Descriptor>
```

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

Atributos de interés del archivo XML:

- entityID="<u>http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2</u>"
- AssertionConsumerService Location="<u>https://10.201.232.19:8443/portal/SSOLoginResponse.action</u>"
- AssertionConsumerService Location="<u>https://ise3-1-</u> <u>19.onmicrosoft.com:8443/portal/SSOLoginResponse.action</u>"

#### Paso 2. Configuración de 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.

| Azure Active Directory admin center |  |   |   |                          |  |
|-------------------------------------|--|---|---|--------------------------|--|
| Azure Active Directory admin        | center  Dashboard > Default Directory  Default Directory  Coverview  Getting started  Preview hub  Diagnose and solve problems  Manage  Users  Groups  External Identities   | Overview  Switch tenant  Delete tenant  Creat  Azure Active Directory can help you enable remu  Default Directory  Search your tenant  Tenant information   | te a tenant <sup>2</sup> What's new <b>E</b> Preview<br>ote work for your employees and partners. Learn m | features V Got feedback? |  |
|                                     | <ul> <li>Users</li> <li>Groups</li> <li>External Identities</li> <li>Roles and administrators</li> <li>Administrative units (Preview)</li> <li>Enterprise applications</li> <li>Devices</li> <li>App registrations</li> <li>Identity Governance</li> <li>Application proxy</li> <li>Licenses</li> <li>Azure AD Connect</li> <li>Custom domain names</li> </ul> | Search your tenant  Tenant information  Your role Global administrator More info License Azure AD Premium P2 Tenant ID 64ace648-115d-4ad9-a3bf-7660 Primary domain ekorneyccisco.onmicrosoft.com  Sign-ins  3 28 26 | Xure AD Connect  Status Not enabled  Last sync Sync has never run   |                          |  |
|                                     | <ul> <li>Mobility (MDM and MAM)</li> <li>Password reset</li> </ul>   | 22<br>2   | Aug 23  |                          |  |

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         |   |
| Initial password | Auto-generate password     Let me create the password     Show Password |

Create

2. Crear un grupo de Azure AD:

Seleccione Grupos. Haga clic en Nuevo grupo.

| Dashboard > Default Directory > Groups                            | 5  |
|---|--|
| Groups   All groups<br>Default Directory - Azure Active Directory |  |
| *   | + New group ↓ Download groups 🔟 Delete 💍 Refresh 🛛 🗉 Columns                                   |
| All groups  |  |
| 🐣 Deleted groups  | ${rak olimits}$ This page includes previews available for your evaluation. View previews $	o$ |
| 🗙 Diagnose and solve problems                                     |  |

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

| Azure Active Directory admin | Azure Active Directory admin center           |  |  |  |  |
|------------------------------|---|--|--|--|--|
| «                            | Dashboard > TAC > Groups >                    |  |  |  |  |
| 📶 Dashboard                  | New Group                                     |  |  |  |  |
| E All services               | ·   |  |  |  |  |
| ★ FAVORITES                  | Group type * ①                                |  |  |  |  |
| 🚸 Azure Active Directory     | Security V                                    |  |  |  |  |
| 🚨 Users                      | Group name * ①                                |  |  |  |  |
| Enterprise applications      | ISE Admin Group                               |  |  |  |  |
|                              | Group description ①                           |  |  |  |  |
|                              | Enter a description for the group             |  |  |  |  |
|                              | Azure AD roles can be assigned to the group ① |  |  |  |  |
|                              | Yes No  |  |  |  |  |
|                              | Membership type * 🛈                           |  |  |  |  |
|                              | Assigned V                                    |  |  |  |  |
|                              | 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 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.

 $\times$ 

 $\times$ 

#### Dashboard >

| Groups   All groups           |   |                                      |                           |                 |
|-------------------------------|---|--------------------------------------|---------------------------|-----------------|
| *                             | + New group 🞍 Download groups   | 🗊 Delete 👌 Refresh 🕴 🗮 Columns       | 💀 Preview features 🛛 🔗 Go | t feedback?     |
| All groups                    |   |                                      |                           |                 |
| Deleted groups                | 🕜 This page includes previews available for your evaluation. View previews $ ightarrow$ |                                      |                           |                 |
| × Diagnose and solve problems | ✓ Search groups   | + <sub>▼</sub> Add filters           |                           |                 |
| Settings                      | Name  | Object Id                            | Group Type                | Membership Type |
| l General                     | ISE Admin Group   | 576c60ec-c0b6-4044-a8ec-d395b1475d6e | Security                  | Assigned        |
| Expiration                    |   |                                      |                           |                 |
| Naming policy                 |   |                                      |                           |                 |

4. Cree una aplicación de Azure AD Enterprise:

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

| Azure Active Directory admin | Azure Active Directory admin center                   |  |  |                        |  |  |
|------------------------------|---|--|--|------------------------|--|--|
| «                            | Control A Default Directory > Enterprise applications |  |  |                        |  |  |
| Z Dashboard                  | Enterprise applicati                                  | ons   All applications                     |  |                        |  |  |
| E All services               | Default Directory - Azure Active Director             | Default Directory - Azure Active Directory |  |                        |  |  |
| * FAVORITES                  | »   | + New application                          | umns 🛛 🐼 Preview features 🛛 🛇                | Got feedback?          |  |  |
| Azure Active Directory       | Overview  |  |  |                        |  |  |
| 🔒 Users                      | <ol> <li>Overview</li> </ol>                          | Iry out the new Enterprise App             | os search preview! Click to enable the previ | ew. →                  |  |  |
| Enterprise applications      | 🗙 Diagnose and solve problems                         | Application type                           | Applications status                          | Application visibility |  |  |
|                              | Manage  | Enterprise Applications $\checkmark$       | Any 🗸  | Any 🗸                  |  |  |
|                              | All applications                                      | First 50 shown, to search all of you       | ur 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?



Create

#### 5. Agregue el grupo a la aplicación:

Seleccione Asignar usuarios y grupos.



Haga clic en Agregar usuario/grupo.

| Azure Active Directory admin | zure Active Directory admin center 문 이 🐵 ? 🔊  |  |      |        |          |  | R |
|------------------------------|---|--|------|--------|----------|--|---|
| **                           | Control Destroyer A con |  |      |        |          |  |   |
| 🔠 Dashboard                  | ISE 3 1 Admin SSO   | Users and groups   |      |        |          |  |   |
| I All services               | Enterprise Application  |  |      |        |          |  |   |
| * FAVORITES                  | ~   | 🕂 Add user/group 🖉 Edit 📋 Remove 🖉 Update Credentials 📔 🎫 Columns 📗 🛜 Got feedback                                       | k?   |        |          |  |   |
| Azure Active Directory       | U Overview  | 0  |      |        |          |  |   |
| 🚨 Users                      | Deployment Plan   | The application will appear for assigned users within My Apps. Set Visible to users C to no in properties to prevent the | 5. → |        |          |  |   |
| Enterprise applications      | Manage  | age  |      |        |          |  |   |
|                              | Properties  | Display Name Object Type   |      | Role a | assigned |  |   |

#### Haga clic en Usuarios y grupos.

| Azure Active Directory admin center |   |  |  |  |
|-------------------------------------|---|--|--|--|
| ≪<br>■ Dashboard<br>■ All services  | Dashboard > Default Directory > Enterprise applications > Add an application > ISE30 > Add Assignment Default Directory |  |  |  |
| Azure Active Directory     Users    | Users and groups > None Selected  |  |  |  |
| Enterprise applications             | Select a role ><br>User   |  |  |  |

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 que se haya completado la configuración.

# Users and groups

| 🔎 Sear | rch                                   |
|--------|---------------------------------------|
| I      | ISE Admin Group                       |
| МС     | mck<br>mck@gdplab2021.onmicrosoft.com |

Una vez seleccionado el grupo, haga clic en Asignar.

| Azure Active Directory admin o | enter   |   |
|--------------------------------|---|---|
| **                             | Dashboard $>$ Default Directory $>$ Enterprise applications $>$ Add an application $>$ ISE30 $>$  |   |
| 📶 Dashboard                    | Add Assignment  |   |
| E All services                 | Default Directory   |   |
| ★ FAVORITES                    |   | × |
| Azure Active Directory         | When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups. |   |
| L Users                        |   |   |
| Enterprise applications        | Users and groups  | > |
|                                | 1 group selected.   |   |
|                                | Select a role   | > |
|                                | User  |   |

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

| Azure Active Directory admin center  |   |  |   |  |  |  |
|--|---|--|---|--|--|--|
| ≪<br>■ Dashboard<br>■ All services   | Dashboard > ISE_3_1_Admin_SSO<br>ISE_3_1_Admin_SSO<br>Enterprise Application      | Users and groups   |   |  |  |  |
| FAVORITES     Azure Active Directory     Users     Enterprise applications | Overview     Deployment Plan     Manage   | <ul> <li>+ Add user/group  Edit  Remove  </li> <li>Characterization will appear for assigned users with</li> <li>P First 200 shown, to search all users &amp; groups, ent</li> </ul> | Update Credentials   ≡≡ Columns   R Got feedback?<br>in My Apps. Set 'visible to users?' to no in properties to prevent this. →<br>er a display name. |  |  |  |
|  | Properties     Owners     Roles and administrators (Preview)     Users and groups | Display Name   | Object Type<br>Group  |  |  |  |

6. Configure una aplicación de Azure AD Enterprise:

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

| Azure Active Directory admin c       | enter  |   |  |
|--------------------------------------|--|---|--|
| ≪<br>☑ Dashboard<br>ⅲ All services   | Dashboard > Enterprise applications > ISE_3_1_Admin_SSO Enterprise Application   | )   Overview  |  |
| FAVORITES     Azure Active Directory | «<br>W Overview  | Properties  |  |
| Lusers                               | Manage   | Name ()<br>ISE_3_1_Admin_SSO ()   |  |
|                                      | Properties Owners  | Application ID ①<br>76b82bcb-a918-4016-aad7 D<br>Object ID ①                                    |  |
|                                      | <ul> <li>Roles and administrators (Preview)</li> <li>Users and groups</li> </ul> | 22aedf32-82c7-47f2-ab34-1 D   |  |
|                                      | <ul> <li>Single sign-on</li> <li>Provisioning</li> </ul>                         |   |  |
|                                      | <ul> <li>Application proxy</li> <li>Self-service</li> </ul>                      | 1. Assign users and groups     Provide specific users and groups access     to the applications | <ul> <li>2. Set up single sign on</li> <li>Enable users to sign into their application<br/>using their Azure AD credentials</li> </ul> |
|                                      | Security   | Assign users and groups   | Get started  |

Seleccione SAML en la siguiente pantalla.

| Azure Active Directory admin   | center   |   |  | ଟ୍ରେ (କ୍ର ୧ <i>ନ</i>  |
|--|--|---|--|---|
| Azure Active Directory admin<br>Comparison of the second sec | Center  Dashboard > Enterprise applications >  ISE_3_1_Admin_SSO Enterprise Application  (  ISE_3_1_Admin_SSO Enterprise Application  ( ISE_3_1_Admin_SSO ( Deployment Plan  Manage  II Properties  Content of the oppose ( Provisioning  Continional Access Contini | ISE_3_1.Admin_SSO<br>Single sign-on<br>Select a single sign-on method<br>Disabled<br>Single sign-on is not enabled. The user<br>wont be able to launch the app from<br>My Apps.<br>Linked<br>Link to an application in My Apps<br>and/or Office 365 application launcher. | Relp me decide<br>SAML<br>Rich and secure authentication to<br>applications using the SAML (Security<br>Assertion Markup Language) protocol. | Password-based<br>Password storage and replay using a<br>web browser extension or mobile app. |
|  | Activity<br>Sign-ins<br>di Usage & insights<br>Audit logs<br>Provisioning logs<br>E Access reviews   |   |  |   |

Haga clic en Edit junto a Basic SAML Configuration.

#### Set up Single Sign-On with SAML

Read the configuration guide C for help integrating ISE30.

| Basic SAML Configuration                   |                        | 🖉 Ed |
|--|------------------------|------|
| Identifier (Entity ID)                     | Required               |      |
| Reply URL (Assertion Consumer Service URL) | Required               |      |
| Sign on URL                                | Optional               |      |
| Relay State                                | Optional               |      |
| Logout Url                                 | Optional               |      |
| User Attributes & Claims                   |                        | 0 Ed |
| givenname                                  | user.givenname         |      |
| surname                                    | user.surname           |      |
| emailaddress                               | user.mail              |      |
| 0.2000                                     | user.userprincipalname |      |
| name                                       |                        |      |

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. Haga clic en Guardar.

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

### **Basic SAML Configuration**

🗄 Save

| Identifier (Entity ID) * 💿   |                       |                  |
|--|-----------------------|------------------|
| The default identifier will be the audience of the SAML response for IDP-initiated SSO   |                       |                  |
|  | Default               |                  |
| http://circols5/004000fd-7047_4d14_0007_5005004ff5fd                                     |                       | r <del>a</del> t |
| http://Ciscolse/0049a2id=7047=4d1d=6907=5a05a94ii5id                                     | U                     |                  |
| http://adapplicationregistry.onmicrosoft.com/customappsso/primary                        | i                     | ١                |
|  |                       |                  |
|  |                       |                  |
| Reply URL (Assertion Consumer Service URL) * ①   |                       |                  |
| The default reply URL will be the destination in the SAML response for IDP-initiated SSO |                       |                  |
|  |                       |                  |
|  | Default               |                  |
| https://10.201.232.19:8443/portal/SSOLoginResponse.action                                | <ul> <li>O</li> </ul> | Û                |
|  |                       |                  |
|  |                       |                  |
| Sign on LIRL   |                       |                  |
|  |                       |                  |
| Enter a sign on URL  |                       |                  |
|  |                       |                  |
| Relay State 🕕  |                       |                  |
| Enter a relay state  |                       |                  |
|  |                       |                  |
|  |                       |                  |
| Logout Url 🛈   |                       |                  |
| Enter a logout url   |                       |                  |
|  |                       |                  |

#### 7. Configure 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.

#### 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 o   | enter  |  |              |
|--|--|--|--------------|
| <ul> <li>         Mashboard     </li> <li>All services</li> <li>         FAVORITES     </li> </ul> | Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on > User Attributes & Claims + Add new claim + Add a group claim == Columns   |  |              |
| <ul> <li>Azure Active Directory</li> <li>Users</li> <li>Enterprise applications</li> </ul>         | Required claim<br>Claim name<br>Unique User Identifier (Name ID)   | Value<br>user.userprincipalname [nameid-for                                    | •••          |
|  | Additional claims         Claim name         http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname         http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name         http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name         http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name         http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | Value<br>user.mail<br>user.givenname<br>user.userprincipalname<br>user.surname | ····<br>···· |

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 | aroups | associated | with  | the | user  | should | be | returned | in | the   | claim?  |
|-------|--------|------------|-------|-----|-------|--------|----|----------|----|-------|---------|
| 11110 | groups | associated | 11111 |     | 0.501 | Should | 20 | reconneo |    | CLUC- | CIGHTIN |

| O None   |
|--|
| All groups   |
| <ul> <li>Security groups</li> </ul>                    |
| O 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)                                   |
|  |

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 > |                                    |   |  |  |  |
| 🖾 Dashboard                  | User Attributes & Claims   |                                    |   |  |  |  |
| E All services               |  |                                    |   |  |  |  |
| * FAVORITES                  | + Add new claim + Add a group claim ≡≡ Columns                                 |                                    |   |  |  |  |
| 🚸 Azure Active Directory     |  |                                    |   |  |  |  |
| 🚨 Users                      | Required claim   |                                    |   |  |  |  |
| Enterprise applications      | Claim name   | Value                              |   |  |  |  |
|                              | Unique User Identifier (Name ID)   | user.userprincipalname [nameid-for |   |  |  |  |
|                              | Additional claims  |                                    |   |  |  |  |
|                              | 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 la Federación de Azure:

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

| SAML Signing Certificate    |   | 0 | 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 | 1 |      |
| Certificate (Base64)        | Download  |   |      |
| Certificate (Raw)           | Download  |   |      |
| Federation Metadata XML     | Download  |   |      |
|                             |   |   |      |

#### Paso 3. Cargar metadatos de Azure Active Directory a 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.

| ■ Cisco ISE  |  | Administration • Identity Ma  | nagement   |   |
|--|--|---|--|---|
| Identities Groups External Ide   | ntity Sources Identity Source Sequences  | s Settings  |  |   |
| External Identity Sources       <     Image: Constraint of the second sec | Identity Provider List > Azure       SAML Identity Provider       General     Identity Provider Config.  | Service Provider Info.  | Groups Attributes                                  | Advanced Settings                       |
| <ul> <li>Active Directory</li> <li>LDAP</li> <li>ODBC</li> <li>RADIUS Token</li> <li>RSA SecurID</li> </ul>  | Identity Provider Configuration<br>Import Identity Provider Config File Choose File<br>Provider Id<br>Single Sign On URL https://login.micros<br>Single Sign Out URL (Redirect) https://login.micros<br>Signing Certificates | softonline.com/182900ec-e960-43<br>softonline.com/182900ec-e960-43          | 40-bd20-e4522197ecf8/sa<br>40-bd20-e4522197ecf8/sa | ml2<br>ml2                              |
| <ul> <li>SAML Id Providers</li> <li>Social Login</li> </ul>  | Subject  CN=Microsoft Azure Federated SSO Certificate  | Issuer         Valid From           CN=Microsoft Azur         Mon Jul 19 12 | Valid To (Expira                                   | Serial Number<br>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.

| ■ Cisco ISE                     | /  | Administration - Identity Mana | agement         |                   |
|---------------------------------|--|--------------------------------|-----------------|-------------------|
| Identities Groups External Iden | tity Sources Identity Source Sequences                   | Settings                       |                 |                   |
| External Identity Sources       | Identity Provider List > Azure<br>SAML Identity Provider | Semine Dravider Info           | auna Attributea | Advanted Continue |
| Certificate Authentication F    | General Identity Provider Config.                        | Service Provider Into. Gr      | oups Attributes | Advanced Settings |
| Active Directory                | Groups   |                                |                 |                   |
| LDAP                            | Group Membership Ambuda Groups                           |                                |                 |                   |
| C ODBC                          | Group Membership Adhibite                                |                                |                 |                   |
| C RADIUS Token                  |  |                                |                 |                   |
| E RSA SecurID                   | + Add Zedit Delete                                       |                                |                 |                   |
| > 🛅 SAML Id Providers           | Name in Assertion  |                                | Name in ISE     |                   |

Haga clic en Add (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.

| Add Group          |  | $\times$ |
|--------------------|--|----------|
| *Name in Assertion | 576c60ec-c0b6-4044-a8ec-d3   |          |
| *Name in ISE       | Customization Admin  |          |
|                    | Customization Admin<br>ERS Admin<br>ERS Operator<br>Elevated System Admin<br>Helpdesk Admin<br>Identity Admin<br>MnT Admin |          |
|                    | Network Device Admin<br>Policy Admin<br>RBAC Admin<br>SPOG Admin<br>Super Admin<br>System Admin<br>TACACS+ Admin           |          |

(Opcional) 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                  | A  | dmin Groups             | Permis | ssions                     |   |                |
|------------|----------------------------|----|-------------------------|--------|----------------------------|---|----------------|
| <b>~</b>   | Customization Admin Policy | lf | Customization Admin +   | then   | Customization Admin Menu   | + | Actions ~      |
| <b>~</b> ~ | Elevated System Admin Poli | lf | Elevated System Admin + | then   | System Admin Menu Access   | + | Actions ~      |
| <b>~</b> ~ | ERS Admin Policy           | lf | ERS Admin +             | then   | Super Admin Data Access    | + | Actions $\sim$ |
| <b>~</b> ~ | ERS Operator Policy        | lf | ERS Operator +          | then   | Super Admin Data Access    | + | Actions $\sim$ |
| <b>~</b> ~ | ERS Trustsec Policy        | lf | ERS Trustsec +          | then   | Super Admin Data Access    | + | Actions $\sim$ |
| <b>~</b> ~ | Helpdesk Admin Policy      | lf | Helpdesk Admin +        | then   | Helpdesk Admin Menu Access | + | Actions $\sim$ |
| <b>~</b> ~ | Identity Admin Policy      | lf | Identity Admin +        | then   | Identity Admin Menu Access | + | Actions $\sim$ |
| <b>~</b> ~ | MnT Admin Policy           | lf | MnT Admin +             | then   | MnT Admin Menu Access      | + | Actions $\sim$ |
| <b>~</b> ~ | Network Device Policy      | lf | Network Device Admin +  | then   | Network Device Menu Acce   | + | Actions $\sim$ |
| <b>~</b> ~ | Policy Admin Policy        | lf | Policy Admin +          | then   | Policy Admin Menu Access   | + | Actions $\sim$ |
| <b>~</b> ~ | RBAC Admin Policy          | lf | RBAC Admin +            | then   | RBAC Admin Menu Access     | + | Actions $\sim$ |
| <b>~</b> ~ | Read Only Admin Policy     | lf | Read Only Admin +       | then   | Super Admin Menu Access    | + | Actions $\sim$ |
| <b>~</b> ~ | SPOG Admin Policy          | lf | SPOG Admin +            | then   | Super Admin Data Access    | + | Actions ~      |
| <b>~</b> ~ | Super Admin Policy         | lf | Super Admin +           | then   | Super Admin Menu Access    | + | Actions ~      |
| <b>~</b> ~ | Super Admin_Azure          | lf | Super Admin +           | then   | Super Admin Menu Access    | + | Actions $\sim$ |
| <b>~</b> ~ | System Admin Policy        | lf | System Admin +          | then   | System Admin Menu Access   | + | Actions $\sim$ |
| <b>~</b> ~ | TACACS+ Admin Policy       | lf | TACACS+ Admin +         | then   | TACACS+ Admin Menu Acc     | + | Actions ~      |

## Verificación

Confirme que la configuración funciona correctamente.

Nota: La prueba de inicio de sesión de 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.

# cisco

# 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

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.

Sign in

| ≡ Cisc   | o ISE                                   |                        | Das                  | hboard                   |                     | Levaluation Mode 9  | Days Q 💮 💭 💮 |
|----------|---|------------------------|----------------------|--------------------------|---------------------|---|--------------|
| Summary  | Endpoints Guest                         | s Vulnerability Threat | ⊙                    |                          |                     |   | •            |
| Tota     | al Endpoints 🕕                          | Active Endpoints 🕕     | Rejected Endpoints 🕕 | Anomalous Behavior ()    | Authenticated Guest | s 🕢 BYOD Endpoints 🕠  | Compliance ① |
|          | 0                                       | 0                      | 0                    | 0                        | 0                   | 0   | 0            |
| # AUTHEN | Loberty Group Remove Device     No data | e o<br>Fabre Reson     | X ENETWORK DEVICES   | on<br>No data available. | S O X               | ENDPOINTS Outer to the second | 0 0 ×        |

## 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. Con el fin de fijar: 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 forma parte del grupo al que se supone que se le debe permitir el acceso 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).

Solución: 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-aad7b43bc4326254'(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.



10.201.232.19:8443/portal/SSOLoginResponse.action

#### This page isn't working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500



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.

Solución: asegúrese de que el nombre de notificación de grupo en Azure e ISE en la ficha 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.

# ılıılıı cısco

# **Identity Services Engine**

Intuitive network security

| <b>8</b> A | ccess Denied |                    |  |
|------------|--------------|--------------------|--|
|            |              | Log In With SAML   |  |
|            |              | Log In With ISE    |  |
|            |              | <u>English</u> 日本語 |  |

#### 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>

2021-07-2913:48:20,709INFO[admin-http-pool46][]api.services.persistance.dao.DistributionDAO-:::2021-07-2913:48:20,712INFO[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

```
2021-07-2913:48:20,839DEBUG[https-jsse-nio-10.201.232.19-8443-exec-7][]cpm.saml.framework.impl.SAM2021-07-2913:48:20,839DEBUG[https-jsse-nio-10.201.232.19-8443-exec-7][]cpm.saml.framework.impl.SAM2021-07-2913:48:20,839DEBUG[https-jsse-nio-10.201.232.19-8443-exec-7][]cpm.saml.framework.impl.SAM2021-07-2913:48:20,839DEBUG[https-jsse-nio-10.201.232.19-8443-exec-7][]cpm.saml.framework.impl.SAM2021-07-2913:48:20,839DEBUG[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.SA -::::- 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][] opensam].ws.message.decode 2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensam].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 [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.sam].framework.imp].SA 2021-07-29 13:48:27,183 DEBUG 2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensam].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.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.sam].framework.imp].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<<u>http://schemas.xmlsoap.org/ws/2005/05/identity</u>
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,

| 2021-07-29 | 13:48:27,185           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
|------------|------------------------|-----------------|--|
| 2021-07-29 | 13:48:27,185           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,185           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,185           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,185           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,185           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,186           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| Idf        | P URI: <u>https:</u> / | //sts.wi        | ndows.net/182900ec-e960-4340-bd20-e4522197ecf8/                          |
| SP         | URI: <u>http://</u>    | <u>CiscoISE</u> | <u>/0049a2fd-7047-4d1d-8907-5a05a94ff5fd</u>                             |
| Ass        | sertion Consur         | mer URL:        | <pre>https://10.201.232.19:8443/portal/SSOLoginResponse.action</pre>     |
| Red        | quest Id: _004         | 49a2fd-7        | 047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2fd-7047-4d1d-89 |
| C1-        | ient Address:          | 10.24.2         | 26.171   |
| Loa        | ad Balancer: n         | 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.opensam].xm].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.SA |
| 2021-07-29 | 13:48:27,188           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,189           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,189           | DEBUG           | [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA |
| 2021-07-29 | 13:48:27,358           | INFO            | [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImp |
|            |                        |                 |  |

5. Validación de la autorización RBAC.

#### <#root>

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 save

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).