

Configurar o Fluxo de Logon de Administração da GUI do ISE 3.1 via Integração do SSO do SAML com o Azure AD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Provedor de identidade \(IdP\)](#)

[Provedor de serviços \(SP\)](#)

[SAML](#)

[Asserção SAML](#)

[Diagrama de fluxo de alto nível](#)

[Configurar a Integração de SSO SAML com o Azure AD](#)

[Etapa 1. Configurar o provedor de identidade SAML no ISE](#)

[1. Configurar o Azure AD como Fonte de Identidade SAML Externa](#)

[2. Configurar o método de autenticação do ISE](#)

[3. Exportar informações do provedor de serviços](#)

[Etapa 2. Definir Configurações do Azure AD IdP](#)

[1. Criar um Usuário do Azure AD](#)

[2. Criar um Grupo do Azure AD](#)

[3. Atribuir Usuário do Azure AD ao Grupo](#)

[4. Criar um Aplicativo Empresarial do Azure AD](#)

[5. Adicionar Grupo ao Aplicativo](#)

[6. Configurar um Aplicativo Empresarial do Azure AD](#)

[7. Configurar Atributo de Grupo do Ative Directory](#)

[8. Baixar Arquivo XML de Metadados de Federação do Azure](#)

[Etapa 3. Carregar Metadados do Azure Ative Directory para ISE](#)

[Etapa 4. Configurar grupos SAML no ISE](#)

[\(Opcional\) Etapa 5. Configurar Políticas RBAC](#)

[Verificar](#)

[Troubleshooting](#)

[Problemas comuns](#)

[Solução de problemas do ISE](#)

[Logs com Login SAML e Nomes de Declaração de Grupo Incompatíveis](#)

Introdução

Este documento descreve como configurar a Integração do Cisco ISE 3.1 SAML SSO com um Provedor de Identidade Externo, como o Azure Active Directory (AD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

1. Cisco ISE 3.1
2. AD do Azure

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Provedor de identidade (IdP)

É a autoridade do Azure AD neste caso, que verifica e declara uma identidade de usuário e privilégios de acesso a um recurso solicitado (o "Provedor de Serviços").

Provedor de serviços (SP)

O recurso ou serviço hospedado que o usuário pretende acessar, o Servidor de Aplicativos ISE, neste caso.

SAML

A SAML (Security Assertion Markup Language) é um padrão aberto que permite que o IdP passe credenciais de autorização para o SP.

As transações SAML usam Extensible Markup Language (XML) para comunicações padronizadas entre o provedor de identidade e os provedores de serviços.

O SAML é o link entre a autenticação de uma identidade de usuário e a autorização para usar um serviço.

Asserção SAML

Uma Asserção SAML é o documento XML que o provedor de identidade envia ao provedor de serviços que contém a autorização do usuário.

Existem três tipos diferentes de Asserções SAML - autenticação, atributo e decisão de autorização.

- As asserções de autenticação comprovam a identificação do usuário e fornecem a hora em que o usuário efetuou login e o método de autenticação usado (Kerberos, dois fatores, como exemplos)
- A asserção de atribuição passa os atributos SAML, pedaços específicos de dados que fornecem informações sobre o usuário, para o provedor de serviços.
- Uma asserção de decisão de autorização declara se o usuário está autorizado a usar o serviço ou se o provedor de identidade negou sua solicitação devido a uma falha de senha ou à falta de direitos ao

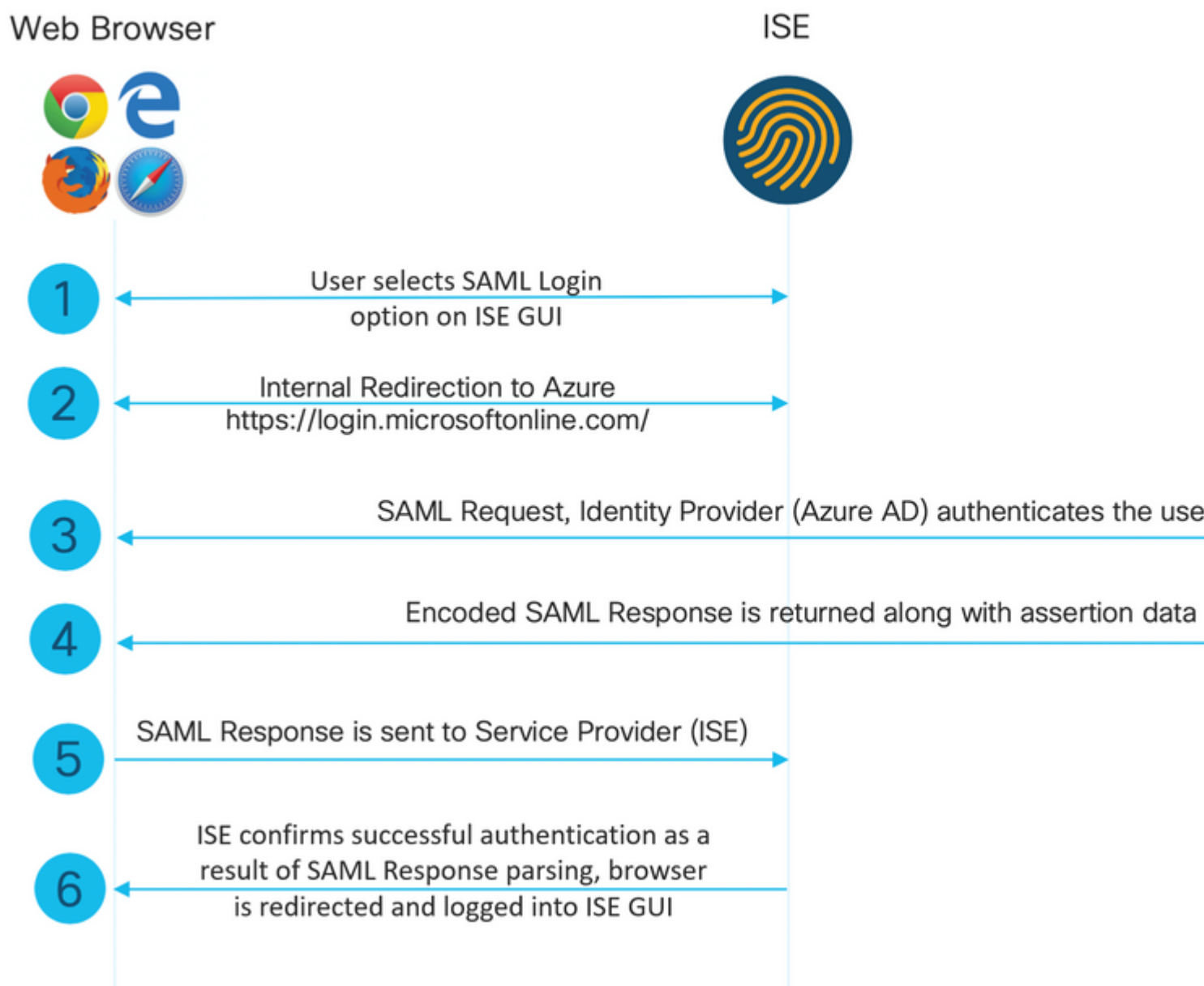
serviço.

Diagrama de fluxo de alto nível

O SAML funciona passando informações sobre usuários, logons e atributos entre o provedor de identidade, o Azure AD e o provedor de serviços, ISE.

Cada usuário faz logon uma vez em um Logon Único (SSO) com o provedor de identidade, o provedor do Azure AD passa os atributos SAML para o ISE quando o usuário tenta acessar esses serviços.

O ISE solicita autorização e autenticação do Azure AD como mostrado na imagem.



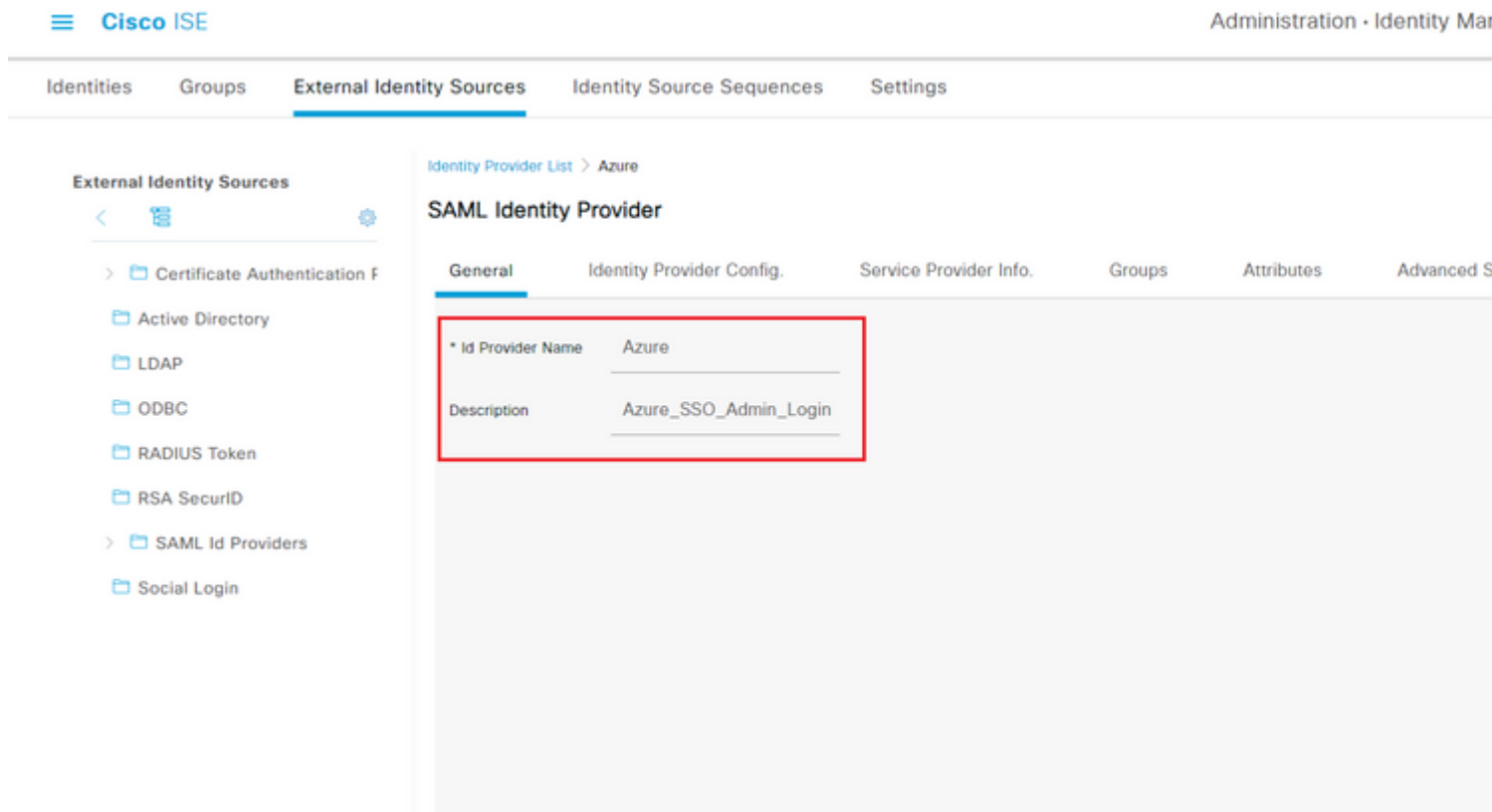
Configurar a Integração de SSO SAML com o Azure AD

Etapa 1. Configurar o provedor de identidade SAML no ISE

1. Configurar o Azure AD como Fonte de Identidade SAML Externa

No ISE, navegue para **Administração > Gerenciamento de identidades > Fontes de identidade externas > Provedores de ID SAML** e clique no botão Adicionar.

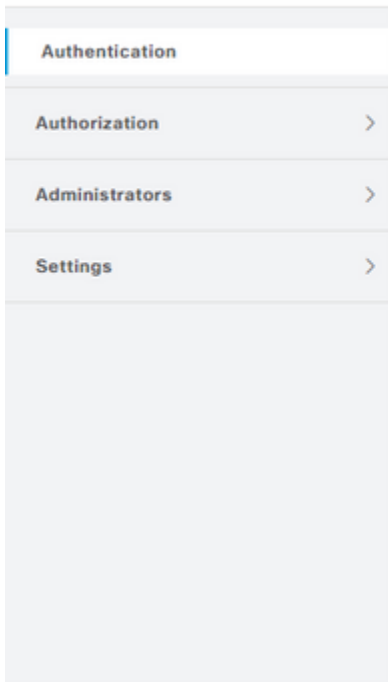
Insira o **Nome do provedor de IDs** e clique em **Enviar** para salvá-lo. O **Nome do provedor de ID** é significativo apenas para o ISE, como mostrado na imagem.



2. Configurar o método de autenticação do ISE

Navegue até **Administração > Sistema > Acesso de administrador > Autenticação > Método de autenticação** e selecione o botão de opção **Baseado em senha**.

Selecione o Nome do provedor de ID necessário criado anteriormente na lista suspensa **Origem da identidade** como mostrado na imagem.



Authentication Type ⓘ

Password Based

Client Certificate Based

* Identity Source

SAML:Azure



3. Exportar informações do provedor de serviços

Navegue até **Administração > Gerenciamento de identidades > Fontes de identidade externas > Provedores de Id SAML > [Seu Provedor SAML]**.

Altere a guia para **Informações do provedor de serviços** e clique no botão **Exportar** como mostrado na imagem.

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attribute

Service Provider Information

 Load balancer (i)Export Service Provider Info. (i)[Export](#)

Includes the following portals:

Sponsor Portal (default)

Faça o download do arquivo **.xml** e salve-o. Anote o valor de **Location URL** e **entityID**.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" >
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT
QU1MX21zZTMtMS0xOjUyOTIyLWVhbnR1bWVudD0wMDA1MjUyOTIyLWVhbnR1bWVudD0w
MCUxIzAhBgNVBAMTG1NBTUxfaXN1My0xLWVhbnR1bWVudD0wMDA1MjUyOTIyLWVhbnR1
AA0CAg8AMIICCgKCAgEAvila4+S0uP3j037yCOXnHAZADupfqcwcp1JQnFvhVfnDd0ixGRt8iaQ
1zdKhpwF/BsJeSznXyaPVxvFcmMFHbmyt46gQ/jjQEyt7YhyohG0t1op01qDgwt0nWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDzizyJGKdDpf+1VM5JHCo6UNLFIIfyPmGvcCXnt
NVqsYvxSzF038ciQq1m0sqvrrYzuIUAXDWUNUg9pSGzH0fKsSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83g4L4WJWmizET06Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0ssshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/lavr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBT0+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9vT4E0zwNGo7pQI8CAwEAAAN9MHswIAAYDVR0RBbkwF4IVaXN1My0xLWVhbnR1bWVudD0w
MAwGA1UdEQUFMAMBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwXqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHg0T2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GwlvccgreC7R46qenaonXVr1tRw11vVIdcf8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUtEi6f0bqr0wCyd9Tj7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gFH0bE5luT4EYVuuHwMNGbZqqqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmdh9g2mppbBw0cxzoUxDm+HReSe+0JhRCyIJC0vUpdNmYC8cfAZuiV/e3wk0BLZM
lgV8FTVQSNra9LwHP/PgeNAPUCRPXSwake4rvjvMc0aS/iYdwZhziJ8zBdIBanMv5mGu1nvTET9K
EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTFjfoITTMdQXNHhg+w1POKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKWER/q1GgaVvh3X/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.action">
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action">

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

Atributos de interesse do arquivo XML:

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

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

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

Etapa 2. Definir Configurações do Azure AD IdP

1. Criar um Usuário do Azure AD

Faça login no painel do centro de administração do Azure Active Directory e selecione seu **AD** como mostrado na imagem.

Azure Active Directory admin center

Dashboard > Default Directory

Default Directory | Overview

Azure Active Directory

Switch tenant Delete tenant Create a tenant What's new

Azure Active Directory can help you enable remote work for your employees and pa

Default Directory

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

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

Sign-ins

3
2.8
2.6
2.4
2.2
2

Aug 23

Selecione **Users**, clique em **New User**, configure **User name**, **Name** e **Initial Password** conforme necessário. Clique em **Criar** como mostrado na imagem.

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. Criar um Grupo do Azure AD

Selecione **Grupos**. Clique em **Novo grupo**.

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



Groups | All groups

Default Directory - Azure Active Directory

<<

+ New group



Download groups



Delete



All groups



Deleted groups



Diagnose and solve problems



This page includes previews available for your evaluation



Search groups

Mantenha o tipo Grupo como **Segurança**. Configure o **nome do grupo** como mostrado na imagem.

Navigation sidebar with items: Dashboard, All services, FAVORITES, Azure Active Directory, Users, Enterprise applications.

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. Atribuir Usuário do Azure AD ao Grupo

Clique em **Nenhum membro selecionado**. Escolha o usuário e clique em **Selecionar**. Clique em **Criar** para criar o grupo com um Usuário atribuído a ele.

Add members



Search ⓘ



mck
mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

Anote o **ID de objeto do grupo**, nesta tela, ele é **576c60ec-c0b6-4044-a8ec-d395b1475d6e** para o **grupo ISE Admin** como mostrado na imagem.

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 | Previews

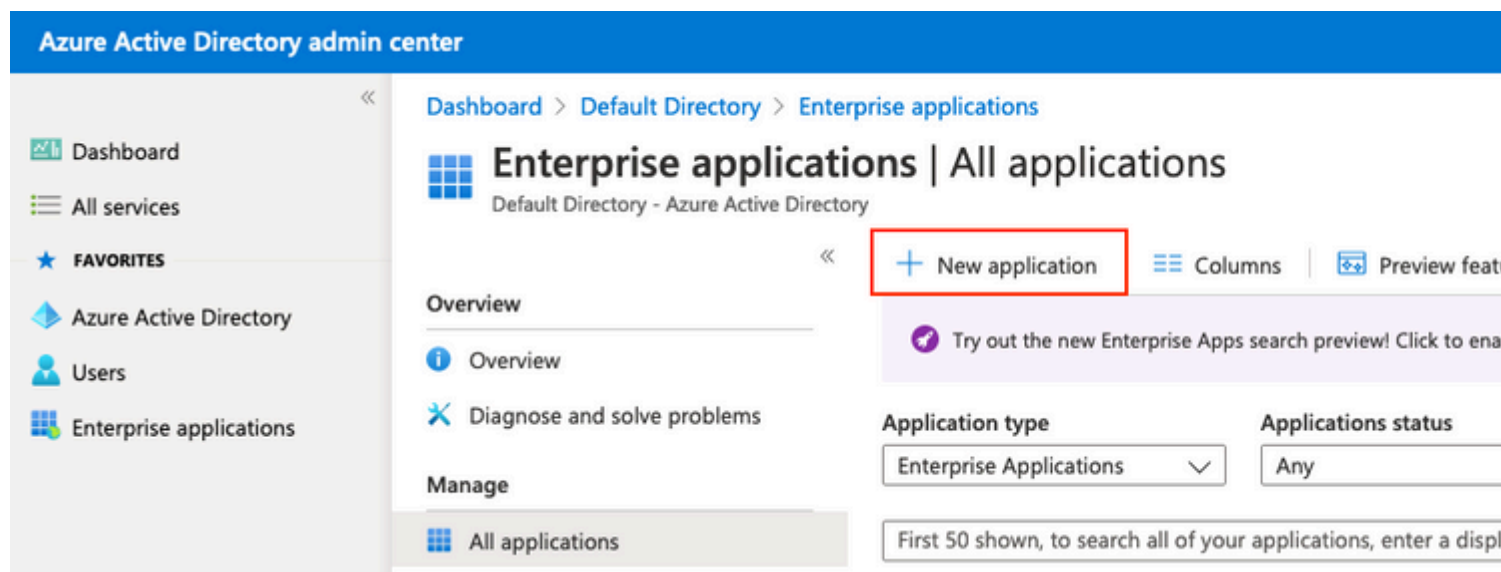
This page includes previews available for your evaluation. View previews →

Search groups | Add filters

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

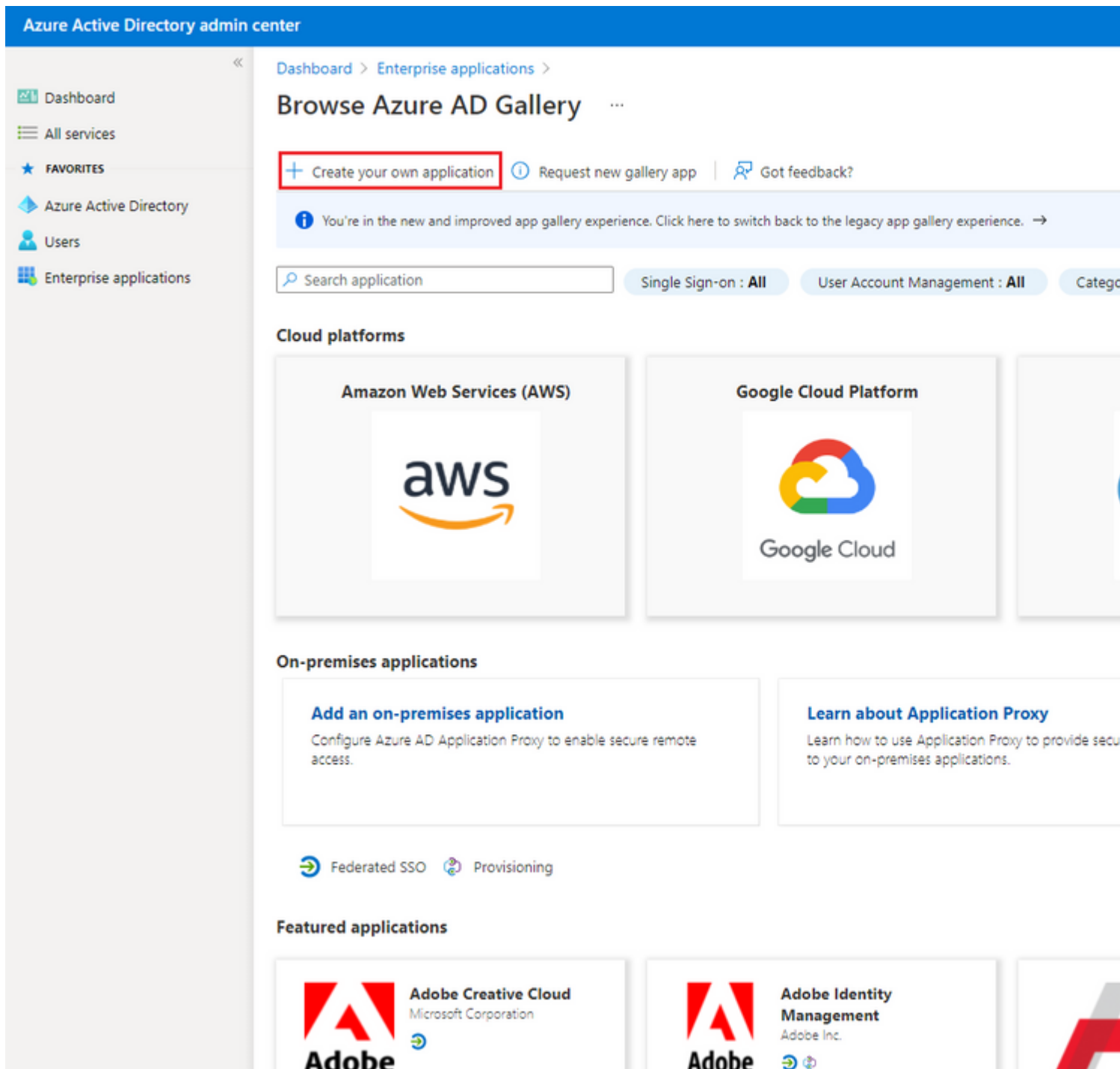
4. Criar um Aplicativo Empresarial do Azure AD

Em AD, selecione **Enterprise Applications** e clique em **New application**.



The screenshot displays the Azure Active Directory admin center interface. The top navigation bar is blue and contains the text "Azure Active Directory admin center". Below this, the breadcrumb trail reads "Dashboard > Default Directory > Enterprise applications". The main heading is "Enterprise applications | All applications" with the subtitle "Default Directory - Azure Active Directory". On the left sidebar, under "FAVORITES", "Enterprise applications" is selected. The main content area features a "New application" button with a plus sign, which is highlighted with a red rectangular box. To the right of this button are "Columns" and "Preview features" options. Below the button, there is a purple banner with a checkmark icon and the text "Try out the new Enterprise Apps search preview! Click to enable". Further down, there are two dropdown menus: "Application type" set to "Enterprise Applications" and "Applications status" set to "Any". At the bottom, a text box indicates "First 50 shown, to search all of your applications, enter a display name".

Selecione **Criar seu próprio aplicativo**.



Insira o nome do seu aplicativo e selecione o botão de opção **Integrar qualquer outro aplicativo que não esteja na galeria (Não galeria)** e clique no botão **Criar** conforme mostrado na imagem.

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. Adicionar Grupo ao Aplicativo

Selecione **Atribuir usuários e grupos**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview

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](#)

Clique em **Adicionar usuário/grupo**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO

ISE_3_1_Admin_SSO | Users and groups

Enterprise Application

+ Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
--------------	-------------

Clique em **Usuários e grupos**.

Add Assignment

Default Directory

Users and groups

None Selected

Select a role

User

Escolha o grupo configurado anteriormente e clique em **Selecionar**.

Note: Selecione o conjunto certo de usuários ou grupos que obtêm acesso conforme pretendido, à medida que os usuários e grupos mencionados aqui obtêm acesso ao ISE após a conclusão da configuração.

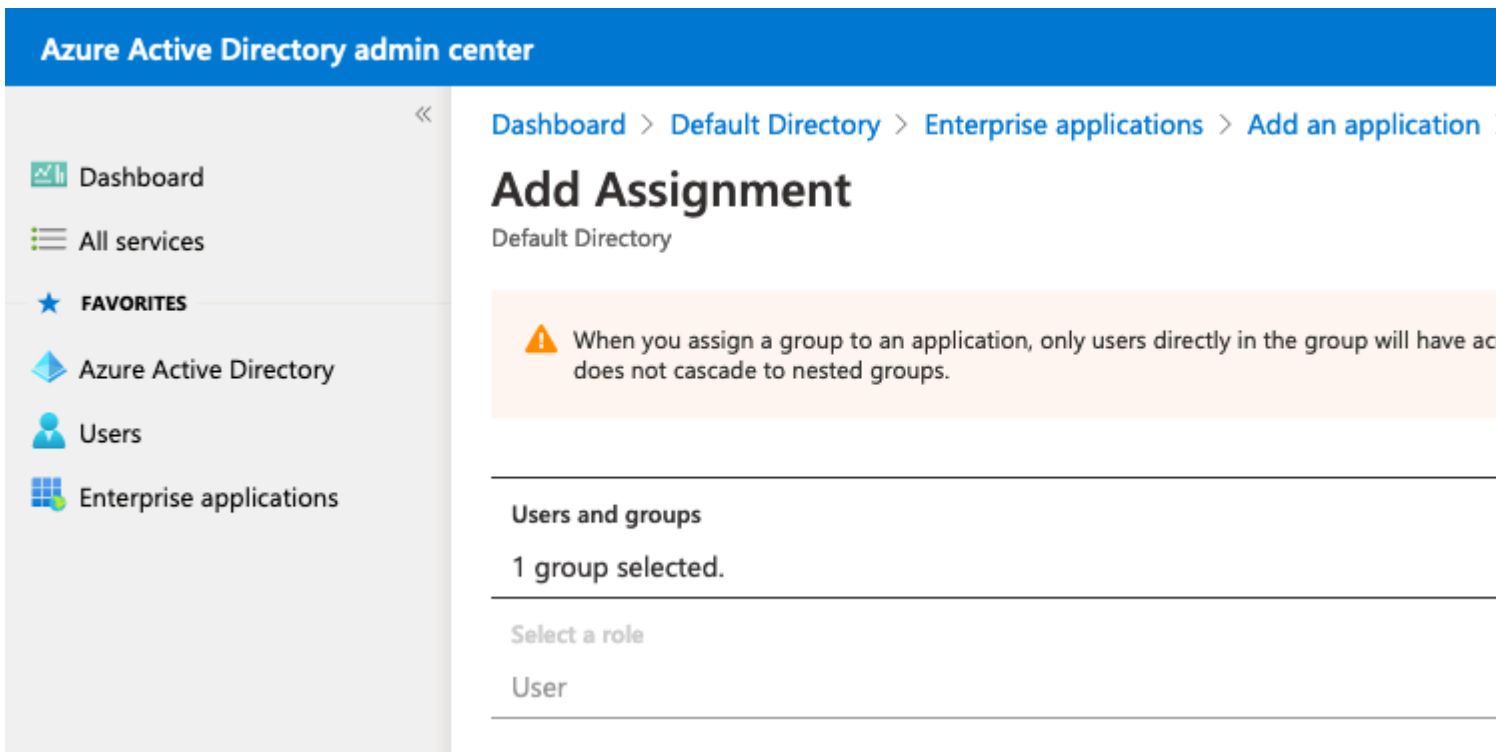
Users and groups

Search

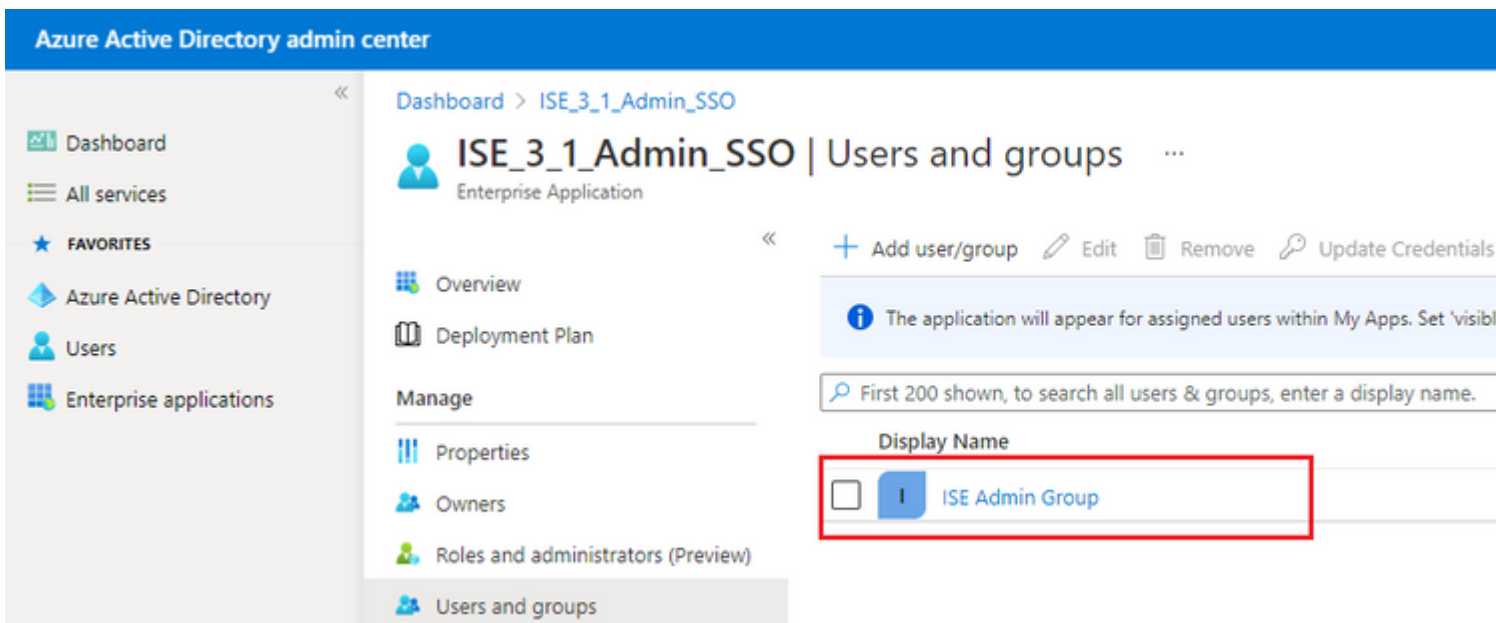
I ISE Admin Group

MC mck
mck@gdplab2021.onmicrosoft.com

Quando o grupo estiver selecionado, clique em **Atribuir**.



Como resultado, o menu **Users and groups** do aplicativo configurado é preenchido com o grupo selecionado.

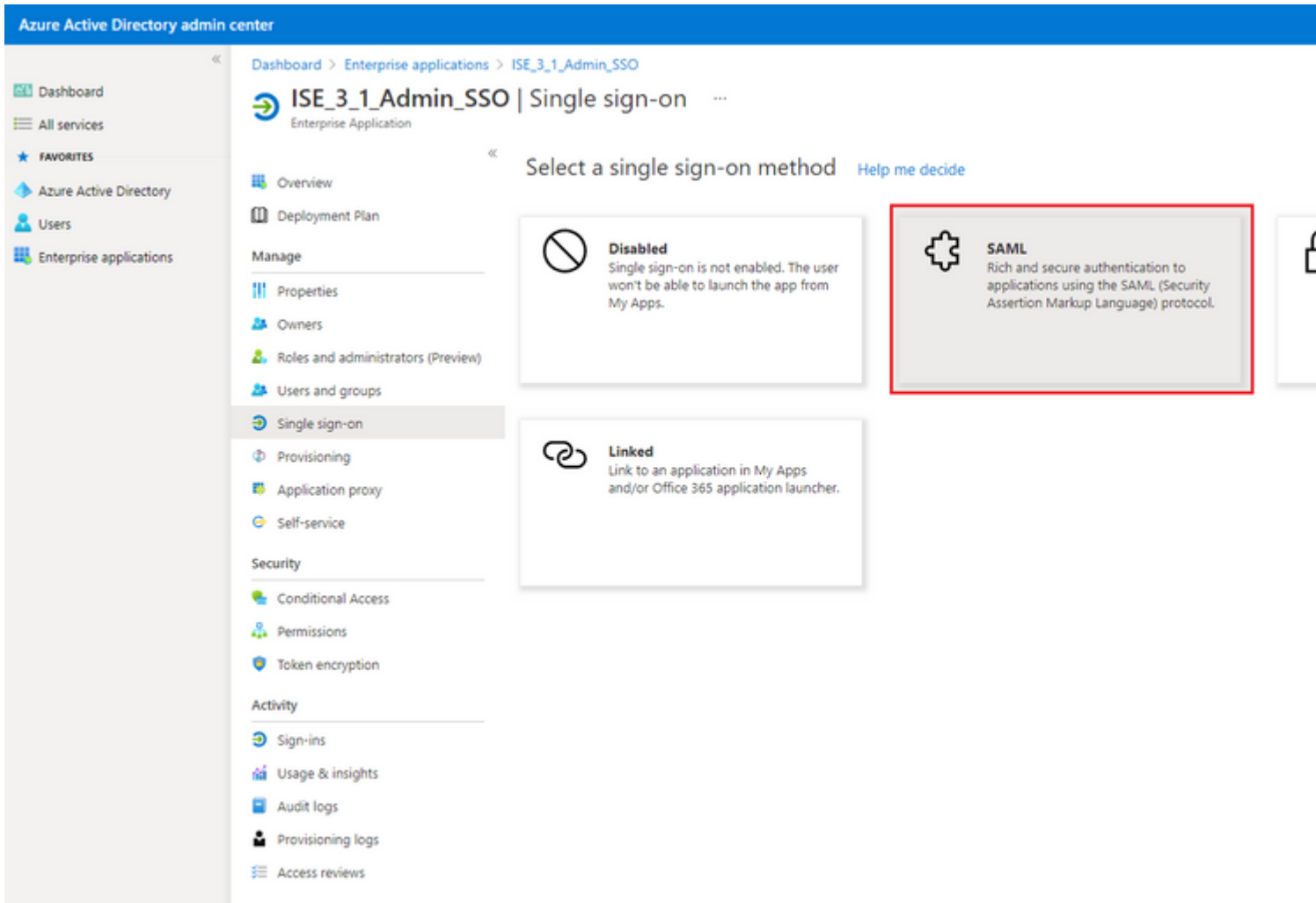


6. Configurar um Aplicativo Empresarial do Azure AD

Navegue de volta para seu Aplicativo e clique em **Configurar login único**.

The screenshot displays the Azure Active Directory admin center interface. The top navigation bar shows the breadcrumb path: Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview. The left-hand navigation pane includes sections for Dashboard, All services, FAVORITES, and a list of services: Azure Active Directory, Users, and Enterprise applications. The main content area is divided into three sections: Overview, Manage, and Security. The Overview section is active and shows the application name and ID. The Manage section lists various management tasks such as Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, and Self-service. The Security section includes Conditional Access. On the right, the Properties section displays the application's Name, Application ID, and Object ID. Below this, the Getting Started section provides a step-by-step guide, with the first step being '1. Assign users and groups', which includes a description and a link to 'Assign users and groups'.

Selecione **SAML** na próxima tela.



Clique em **Editar** ao lado de **Configuração SAML básica**.

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	

Preencha o identificador (ID da entidade) com o valor de **entityID** do arquivo XML da etapa **Export Service Provider Information**. Preencha URL de resposta (URL do serviço de consumidor de

assertão) com o valor de **Locations** de **AssertionConsumerService**. Click Save.

Note: A URL de resposta atua como uma lista de passagem, que permite que determinadas URLs atuem como uma origem quando redirecionadas para a 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://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd> ⓘ 

<http://adapplicationregistry.onmicrosoft.com/customappsso/primary> ⓘ 

Reply URL (Assertion Consumer Service URL) * ⓘ

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> ⓘ 

Sign on URL ⓘ

Enter a sign on URL

Relay State ⓘ

Enter a relay state

Logout Url ⓘ

Enter a logout url

7. Configurar Atributo de Grupo do Active Directory

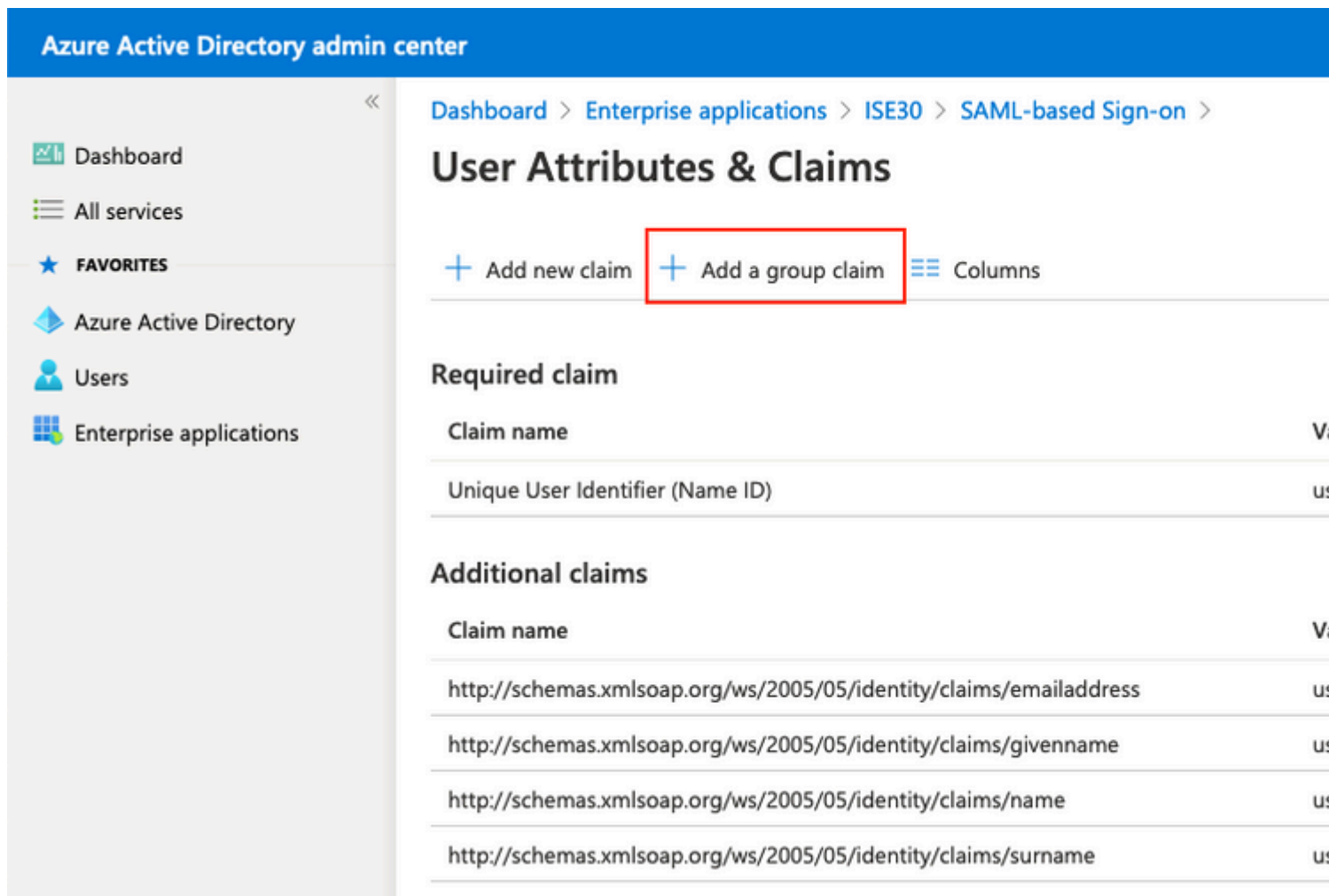
Para retornar o valor de atributo de grupo configurado anteriormente, clique em **Editar** ao lado de **Atributos e declarações do usuário**.

User Attributes & Claims



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

Clique em **Adicionar uma declaração de grupo**.

A screenshot of the Azure Active Directory admin center interface. The top navigation bar is blue with the text "Azure Active Directory admin center". The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area shows the breadcrumb "Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on > User Attributes & Claims". Below the breadcrumb, there are two buttons: "+ Add new claim" and "+ Add a group claim", with the latter being highlighted by a red box. To the right of these buttons is a "Columns" button. Below the buttons, there are two sections: "Required claim" and "Additional claims". The "Required claim" section has a table with one row: "Unique User Identifier (Name ID)". The "Additional claims" section has a table with four rows, each with a "Claim name" and a value: "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name", and "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname".

Selecione **Grupos de segurança** e clique em **Salvar**. Selecione **ID do grupo** no menu suspenso **Atributo de origem**. Marque a caixa de seleção para personalizar o nome da declaração de grupo e insira o nome **Groups**.

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 o **nome da reivindicação** do grupo. Nesse caso, são **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.o


Additional claims

Claim name	Value
Groups	user.g
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.m
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.g
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.r
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.s

8. Baixar Arquivo XML de Metadados de Federação do Azure

Clique em **Download** no **XML de Metadados de Federação** em **Certificado de Assinatura 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	<input type="text" value="https://login.microsoftonline.com/182900ec-e960..."/> 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Etapa 3. Carregar Metadados do Azure Active Directory para ISE

Navegue até **Administração > Gerenciamento de identidades > Fontes de identidade externas > Provedores de Id SAML > [Seu Provedor SAML]**.

Altere a guia para **Config. do provedor de identidade** e clique em **Procurar**. Selecione o arquivo **XML de Metadados de Federação** na etapa **Baixar XML de Metadados de Federação do Azure** e clique em **Salvar**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration · Identity Management'. The main navigation menu has 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' section is expanded, showing various authentication methods like Certificate Authentication, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The 'SAML Identity Provider' configuration page for 'Azure' is displayed, with the 'Identity Provider Config.' tab selected. This tab contains the 'Identity Provider Configuration' section with fields for 'Import Identity Provider Config File' (with a 'Choose File' button), 'Provider Id', 'Single Sign On URL', and 'Single Sign Out URL (Redirect)'. Below this is the 'Signing Certificates' section, which contains a table with the following data:

Subject	Issuer	Valid From	Valid To (Ex
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azur...	Mon Jul 19 12:16:2...	Fri Jul 19 12:

Etapa 4. Configurar grupos SAML no ISE

Altere para a guia **Grupos** e cole o valor de **Nome da reivindicação de Configurar atributo de grupo do Active Directory** em **Atributo de associação de 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**

Groups

Group Membership Attribute groups

+ Add Edit Delete Name in Assertion ^ Name in

Clique em **Add**. Preencha **Nome em Asserção** com o valor de **ID do Objeto de Grupo do Grupo de Administração do ISE** capturado em **Atribuir Usuário do Ative Directory do Azure ao Grupo**.

Configure **Name no ISE** com a lista suspensa e selecione o grupo apropriado no ISE. Neste exemplo, o grupo usado é o **Super Admin**. Click **OK**. Click **Save**.

Isso cria um mapeamento entre Grupo no Azure e Nome do grupo no ISE.

Add Group

*Name in Assertion 576c60ec-c0b6-4044-a8ec-d3

*Name in ISE Customization Admin

- Customization Admin
- ERS Admin
- ERS Operator
- Elevated System Admin
- Helpdesk Admin
- Identity Admin
- MnT Admin
- Network Device Admin
- Policy Admin
- RBAC Admin
- SPOG Admin
- Super Admin
- System Admin
- TACACS+ Admin

(Opcional) Etapa 5. Configurar Políticas RBAC

A partir da etapa anterior, há muitos tipos diferentes de níveis de acesso de usuários que podem ser configurados no ISE.

Para editar as RBAC (Role Based Access Control Policies, Políticas de controle de acesso baseado em

funções), navegue até **Administration > System > Admin Access > Authorization > Permissions > RBAC Policies** e configure conforme necessário.

Esta imagem é uma referência à configuração de exemplo.

∨ RBAC Policies

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

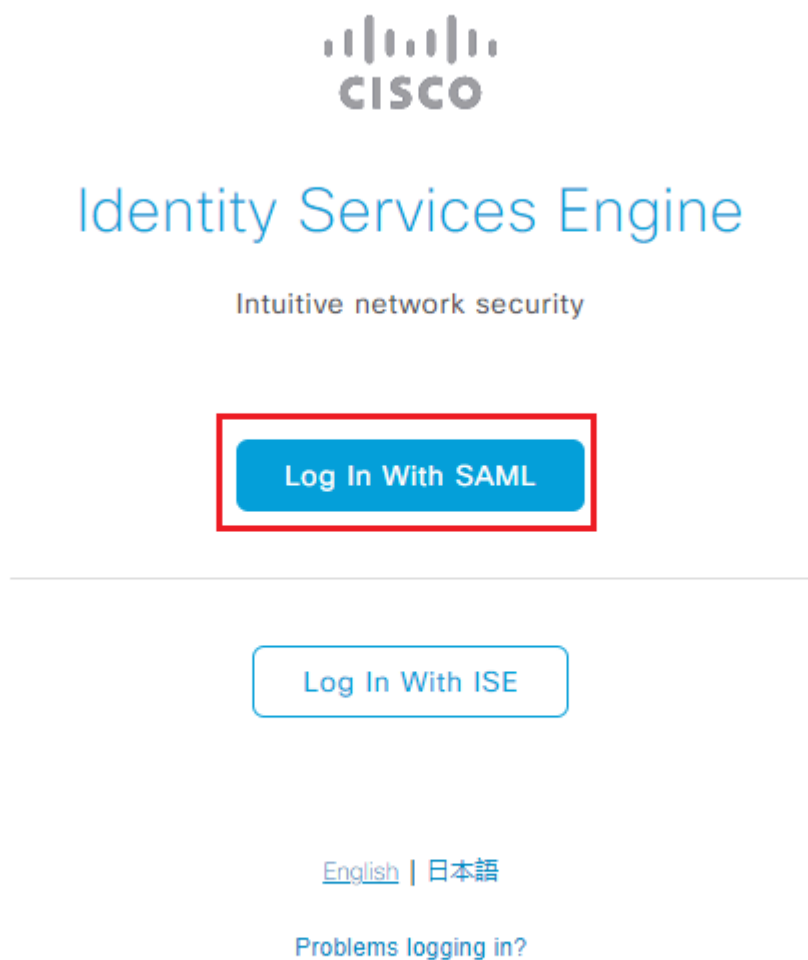
Verificar

Confirme se a configuração está funcionando corretamente.

Note: O teste de Logon do SAML SSO da funcionalidade de teste do Azure não funciona. A solicitação SAML deve ser iniciada pelo ISE para que o SSO SAML do Azure funcione corretamente.

Abra a tela do prompt de login da GUI do ISE. Você verá uma nova opção para **Fazer login com SAML**.

1. Acesse a página de Login da GUI do ISE e clique em **Login com SAML**.



2. Você será redirecionado para a tela de logon da Microsoft. Insira suas credenciais de **nome de usuário** de uma conta em um grupo mapeado para o ISE como mostrado aqui e clique em **Avançar** como mostrado na imagem.



Sign in

mck@gdplab2021.onmicrosoft.com

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

Next

3. Insira sua **Senha** para o usuário e clique em **Entrar**.



← mck@gdplab2021.onmicrosoft.com

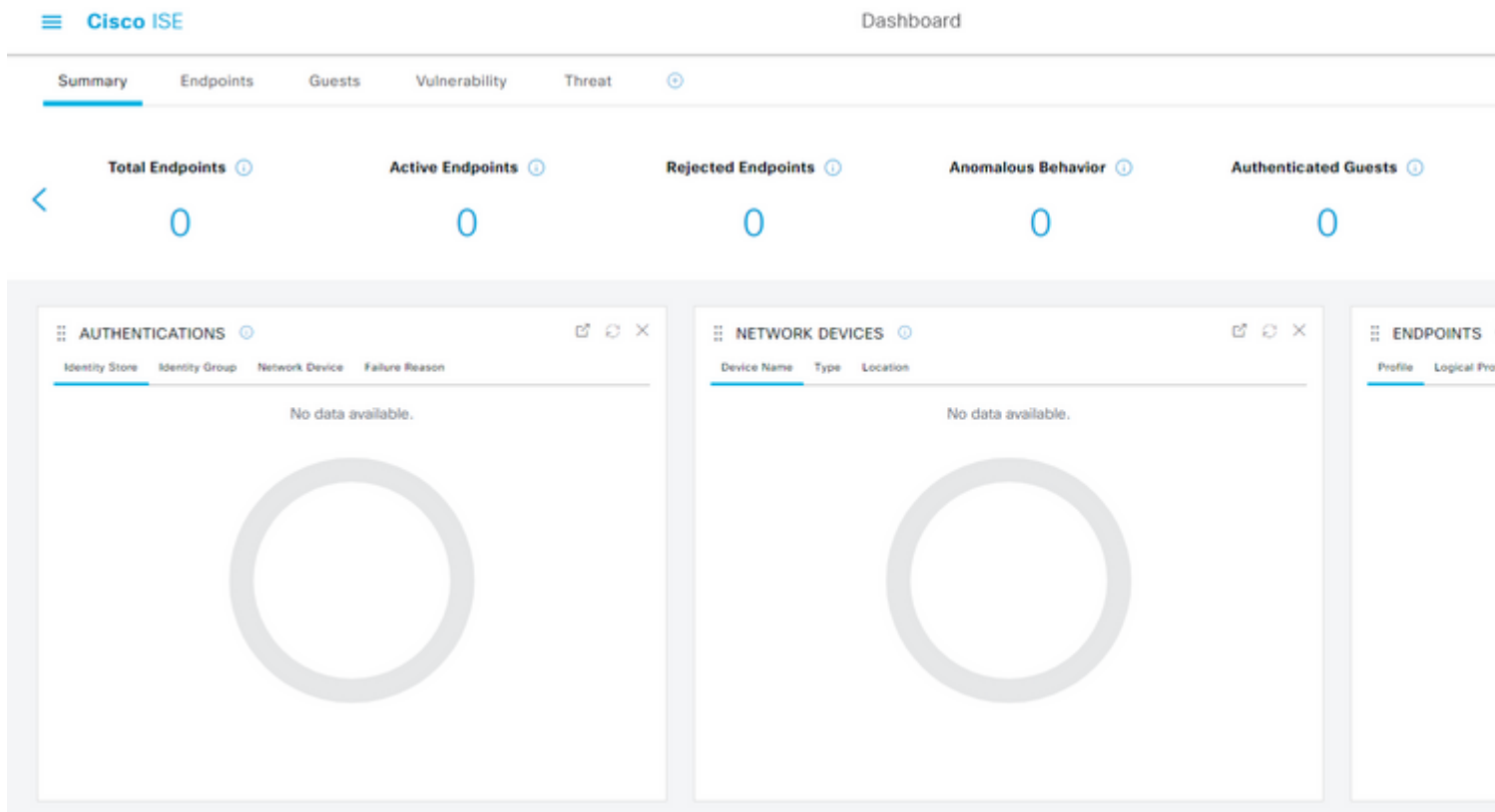
Enter password

.....

[Forgot my password](#)

Sign in

4. Agora você será redirecionado para o painel de controle do aplicativo ISE com as permissões apropriadas configuradas com base no grupo do ISE configurado anteriormente conforme mostrado na imagem.



Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Problemas comuns

É vital entender que a autenticação SAML é tratada entre o navegador e o Ative Directory do Azure. Portanto, você pode obter erros relacionados à autenticação diretamente do Provedor de Identidade (Azure) onde o compromisso do ISE ainda não foi iniciado.

Problema 1. O erro "Sua conta ou senha está incorreta" é visto depois que você insere as credenciais. Aqui, os dados do usuário ainda não são recebidos pelo ISE e o processo neste ponto ainda permanece com o IdP (Azure).

O motivo mais provável é que as informações da conta estão incorretas ou a senha não está correta. Para corrigir: redefina a senha ou forneça a senha correta para essa conta, como mostrado na imagem.



← 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. O usuário não faz parte do grupo que deve ter permissão para acessar o SAML SSO. Semelhante ao caso anterior, os dados do usuário ainda não são recebidos pelo ISE e o processo neste ponto ainda permanece com o IdP (Azure).

Para corrigir isso: verifique se a etapa de configuração **Add group to the Application** é executada corretamente como mostrado na imagem.



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. O Servidor de Aplicativos ISE não pode tratar solicitações de logon SAML. Esse problema ocorre quando a solicitação SAML é iniciada do Provedor de Identidade, Azure, em vez do Provedor de Serviço, ISE. Testar o Logon SSO do Azure AD não funciona, pois o ISE não oferece suporte a solicitações SAML iniciadas pelo Provedor de Identidade.



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	824F4BB47B350C93DE3D59EC87EE4C8
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182
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/182
Azure AD Identifier	https://sts.windows.net/182900ec-e96
Logout URL	https://login.microsoftonline.com/182

[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 to allow third-party cookies if you have installed it but this message

Please make sure you have configured ISE_3_1_Admin_SSO before

(requires browser)

Resolving errors

If you encounter an error in the sign-in page, please paste it below and retry.

What does the error look like?

Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: Saa879f5-68f1-482a-a405-ff993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX

[Get resolution guidance](#)

Problema 4. O ISE exibe o erro "Acesso negado" após uma tentativa de login. Este erro ocorre quando o nome da declaração do grupo criado anteriormente no Aplicativo Azure Enterprise não corresponde no ISE.

Para corrigir isso: verifique se o nome da declaração de grupo no Azure e no ISE na guia Grupos de Provedores de Identidade SAML são iguais. Consulte as etapas 2.7 e 4 na seção **Configurar SAML SSO com o Azure AD** deste documento para obter mais detalhes.



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

Solução de problemas do ISE

O nível de log dos componentes aqui deve ser alterado no ISE. Navegue até **Operações > Solução de problemas > Assistente de depuração > Configuração do log de depuração.**

Nome do componente	Nível de log	Nome do arquivo de log
portal	DEBUG	guest.log

opensaml	DEBUG	ise-psc.log
saml	DEBUG	ise-psc.log

Logs com Login SAML e Nomes de Declaração de Grupo Incompatíveis

Conjunto de depurações que exhibe o cenário de solução de problemas de incompatibilidade de nome de declaração no momento da execução do fluxo (ise-psc.log).

Observação: fique de olho nos itens em **negrito>**. Os registros foram reduzidos para fins de clareza.

1. O usuário é redirecionado para a URL do IdP na página de administração do 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.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7] [] cpm.saml.framework.impl.SAML
```

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

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

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

2. A resposta SAML é recebida do navegador.

<#root>

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

-:::- Decoded SAML relay state of: [_0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2](#)

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

-:::- Decoded SAML message


```

2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
IdP URI: https://sts.windows.net/182900ec-e960-4340-bd20-e4522197ecf8/
SP URI: http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd
Assertion Consumer URL: https://10.201.232.19:8443/portal/SSOloginResponse.action
Request Id: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2fd-7047-4d1d-8907-5a05a94ff5fd
Client Address: 10.24.226.171
Load Balancer: null
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAMLSignature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAMLSignature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,358 INFO [admin-http-pool150][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl

```

5. Validação da autorização RBAC.

<#root>

```

*****Rbac Log Summary for user samlUser*****
2021-07-29 13:48:27,360 INFO [admin-http-pool150][] com.cisco.ise.util.RBACUtil -:::- Populating cache
2021-07-29 13:48:27,368 ERROR [admin-http-pool150][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::-
java.lang.NullPointerException
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 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 save
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-pool50][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.