

Configurar o Portal do Patrocinador do ISE 3.0 com o Azure AD SAML SSO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de fluxo de alto nível](#)

[Configurar](#)

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

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

[2. Configurar o Portal do Patrocinador para usar o Azure AD](#)

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

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

[1. Criar um Usuário do Azure AD](#)

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

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

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

[5. Adicionar grupo ao aplicativo](#)

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

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

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

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

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

[Etapa 5. Configurar o mapeamento de grupo de patrocinadores no ISE](#)

[Verificar](#)

[Troubleshoot](#)

[Problemas comuns](#)

[Solução de problemas do cliente](#)

[Troubleshooting do ISE](#)

Introduction

Este documento descreve como configurar um servidor SAML do Azure Active Directory (AD) com o Cisco Identity Services Engine (ISE) 3.0 para fornecer recursos de Logon Único (SSO) para usuários Patrocinadores.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

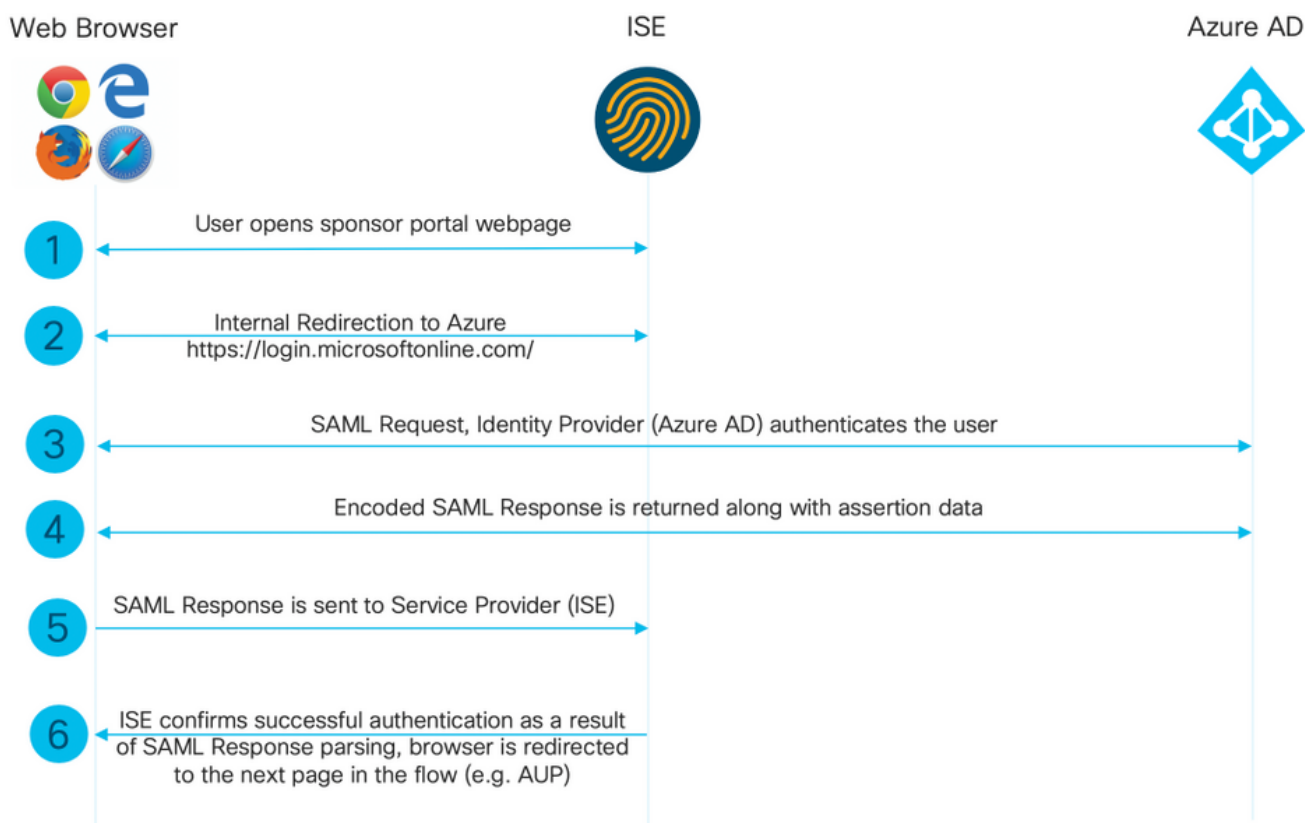
1. Cisco ISE 3.0
2. Conhecimento básico sobre implantações de SSO SAML
3. Azure AD

Componentes Utilizados

1. Cisco ISE 3.0
2. Azure AD

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de fluxo de alto nível



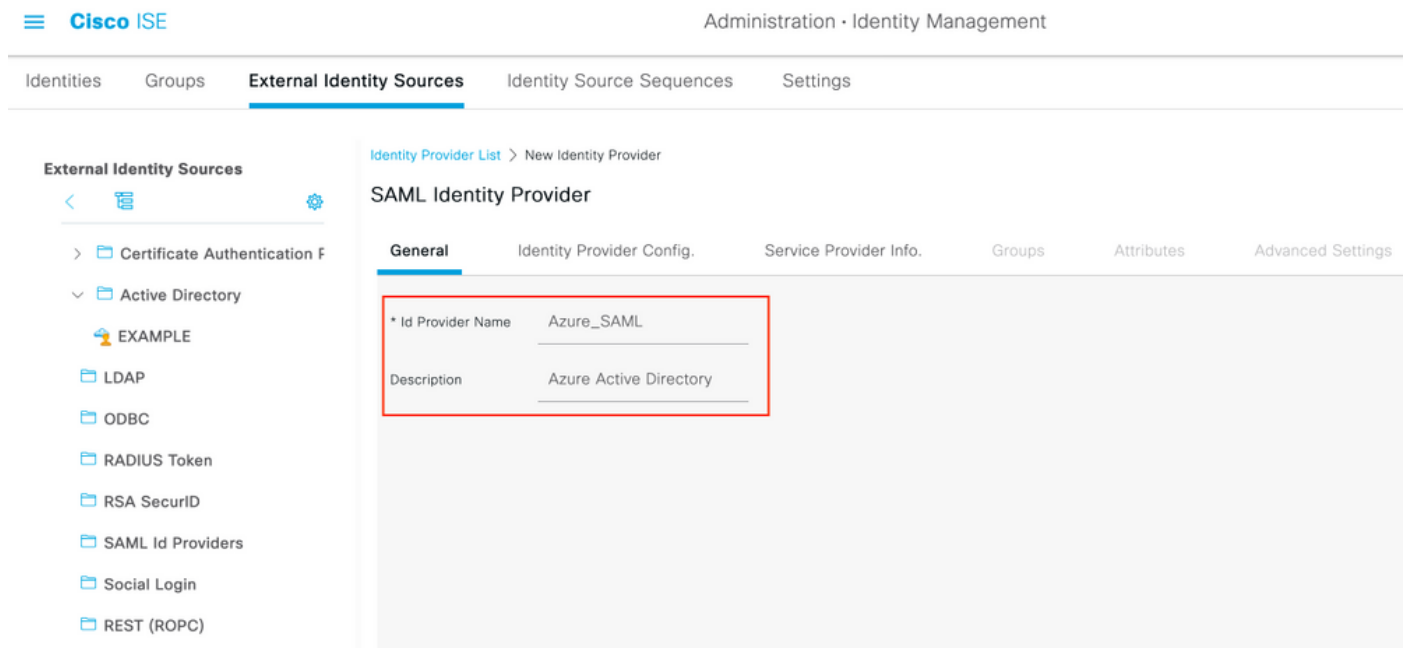
Configurar

Etapa 1. Configurar o provedor de identidade e o portal do patrocinador do SAML no ISE

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

No ISE, navegue para **Administration > Identity Management > External Identity Sources > SAML Id Providers** e clique no botão **Add**.

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



2. Configurar o Portal do Patrocinador para usar o Azure AD

Navegue até **Centros de trabalho > Acesso de convidados > Portais e componentes > Portais de patrocinadores** e selecione seu Portal de patrocinadores. Neste exemplo, o **Portal do Patrocinador (padrão)** é usado.

Expanda o painel **Configurações do portal** e selecione seu novo IDP SAML na **sequência de origem da identidade**. Configure o **Nome de domínio totalmente qualificado (FQDN)** para o portal do patrocinador. Neste exemplo, é **esponsor30.example.com**. Clique em **Salvar** como mostrado na imagem.

Overview Identities Identity Groups Ext Id Sources Administration Network Devices **Portals & Components** Manage Accounts Policy Elements Policy Sets

Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals

Portal Name: * **Sponsor Portal (default)** Description: * **Default portal used by sponsors to crei**

Language File
[Portal test URL](#)

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port: * **8445**

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding is not configured on a PSN, use:	If bonding is configured on a PSN, use:
<input checked="" type="checkbox"/> Gigabit Ethernet 0	<input checked="" type="checkbox"/> Bond 0 Uses Gigabit Ethernet 0 as primary , 1 as backup .
<input type="checkbox"/> Gigabit Ethernet 1	<input type="checkbox"/> Bond 1 Uses Gigabit Ethernet 2 as primary , 3 as backup .
<input type="checkbox"/> Gigabit Ethernet 2	<input type="checkbox"/> Bond 2 Uses Gigabit Ethernet 4 as primary , 5 as backup .
<input type="checkbox"/> Gigabit Ethernet 3	
<input type="checkbox"/> Gigabit Ethernet 4	
<input type="checkbox"/> Gigabit Ethernet 5	

Certificate group tag: * **Default Portal Certificate Group**

Configure certificates at:
[Work Centers > Guest Access > Administration > System Certificates](#)

Fully qualified domain names (FQDN) and host names: **sponsor30.example.com**

Identity source sequence: * **Azure_SAML**

Configure authentication methods at:
[Work Centers > Guest Access > Identities > Identity Source Sequences](#)
[Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers](#)

3. Exportar informações do provedor de serviços

Navegue até **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]**.

Mude para a guia **Informações do provedor de serviços**, e clique no botão **Exportar** conforme mostrado na imagem.

SAML Identity Provider

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

Service Provider Information

Load balancer ?

Export Service Provider Info. **Export** ?

Includes the following portals:

Sponsor Portal (default)

Baixe o arquivo zip e salve-o. Nele, você pode encontrar 2 arquivos. Você precisa do arquivo XML chamado de Portal do Patrocinador.

Anote o Location da Resposta de Ligações de **SingleLogoutService**, o valor de **EntityID** e os valores de **Location** de **AssertionConsumerService Binding**.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429">
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFZjCCA06gAwIBAgIQX1oAvwAAAAChgVd9cEEWozANBqkqhkiG9w0BAQwFADAlMSMwIQYDVQQD
ExpTQUlMX01TRTMwLTFlay5leGFtcGxlLmNvbTAeFw0yMDA5MTAxMDMyMzFaFw0yNTA5MDkxMDMy
MzFaMCUxIzAhBgNVBAMTGlNBTUxfSVNFMzAtMWVrLmV4YW1wbGUuY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCGKCAgEAt+MixKfuZvg/oAWGEs6zrUYL3H2JwvZw9yJs6sJ8/BpP6Sw027wh
FXnESXpqqmnoSVrVcQIrDdk3l8UYNn/+98PPkIi/4ftyFjZK9YdeverD6nrA2MeoLCzGlkWg/y4i
vvVcYuW344pySm65awVvro3q84x9esHqyLahExs9guiLJryD497XmNP4Z8eTHCctu777PuI1wL04
QOYUs2sozXvR98D9Jok/+PjH3bjmVKapqAcNEFvk8Ez9x1sMBUgFwP4YdZzQB9IRVkJdIJGvqMyf
a6gn+KaddJnmIbXKFbrTaFii2IvRs3qHJ0mMVfYRnYeMql9/PhzvSftjRe32x/aQh23j9dCsVXmQ
ZmXpZyxxJ8p4RqyM0YgkfxnQXXtV9K0sRZPFn60+iszUw2hARRG/te0hTuVXpbonG2dT109JeeEe
S1E5uxenJvYkU7mMamvBjYQN6qVvyogf8F0lHTSfd6TDsK3Qhmz0jg50PrBvvg5qE6OrxxNvqSVZ
ldhx/iHZAZlyYSVdwizsZMCw0PjSwrRPx/h8l03djeW0aL5R1AF1qTFHVHSNvigzh6FyjdkUJH66
JAygPe0PKJFRgYzh5vWoJ4lqvDqjlGk3c/zYi57MR1Bs0mkSvkOGbmjSsb+EehnYyLLB8FG3De2V
ZaXaHZ37gmoCNNmZHrn+GB0CAwEAAoBkTCBjjAgBgNVHREEGTAXghVJU0UzMC0xZWsuZXhhbXBs
ZS5jb20wDAYDVDR0TBAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVR0OBBYEFPT/6jpfyugxRolbjzWJ
858wfTP1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjARBglghkgBhvhCAQEEBAMCBkAw
DQYJKoZIhvcNAQEMBQADggIBABGyWZbLaJm2LyLASg//4N6mL+xu/9IMdVvNWBQodF+j0WusW15a
VPSQU2t3Ckd/IlanvpK+cp77NMjo9V9oWi3/ZnjZHGofAicHnLGCoeJmC1TvLau7ZzhCCII37DFA
yMKDrXLi3pR+ONlXlTivjPHTTzrKmlNHhkxkx/Js5Iuz+MyRKP8FNmWT0q4XGejyKzJWrqEu+bc1
idC1/gBNUCHgqmFem82IGQ7jVomlkBjLb4pTDbYk4fMIbJVh4V2Pgi++6MIfXAYEWL+LHjSGHCQT
PSM3+kpvlwHHpGWzQSmcJ4tXVXV95W0NC+LxQZLBPNUMZorhuYCILXZxvXH1HGJJ0YKx91k9Ubd2
s5JaD+GN8jqm5XXAAu7S4BawfvCo3bo0iXnSvGcIuh9YFiR2lp2n/2X0VVbdPHYZtqGieqBWebHr
4I1z18FXblYyMzpIkht00vkP5mAlR92VXBkvx2WPjtzQrvOtSXgvTCOKerYCBM/jnuwsztV7FVTV
JNdFwOsncXC70YngZeujZyJpUbfRKZI34VKZp4i05bZsGlbWE9Skdquv0PaQ8ecXTv8OCVBYUeg1
vt0pde18h/9jImdLG8dF0rbADGHiieTcntSDdw3E7JFmS/oHw7FsA5GI8IxXfcOWUx/L0Dx3jTND
ZlAXp4juySODIx9yDyM4yV0f
</ds:X509Certificate>
</ds:X509Data>
```

```
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=bd48c1
a1-9477-4746-8e40-e43d20c9f429"
ResponseLocation="https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action"/>
<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 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action" index="0"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://10.48.23.86:8445/sponsorportal/SSOLoginResponse.action" index="1"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://10.48.26.63:8445/sponsorportal/SSOLoginResponse.action" index="2"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://10.48.26.60:8445/sponsorportal/SSOLoginResponse.action" index="3"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://ise30-1ek.example.com:8445/sponsorportal/SSOLoginResponse.action" index="4"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action" index="5"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://ise30-3ek.example.com:8445/sponsorportal/SSOLoginResponse.action" index="6"/>
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

De acordo com o arquivo XML:

SingleLogoutService

ResponseLocation="<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action>"

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

AssertionConsumerService

Location="<https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action>"

AssertionConsumerService

Location="<https://10.48.23.86:8445/sponsorportal/SSOLoginResponse.action>"

AssertionConsumerService

Location="<https://10.48.23.63:8445/sponsorportal/SSOLoginResponse.action>"

AssertionConsumerService

Location="<https://10.48.26.60:8445/sponsorportal/SSOLoginResponse.action>"

AssertionConsumerService Location="<https://ise30-1ek.example.com:8445/sponsorportal/SSOLoginResponse.action>"

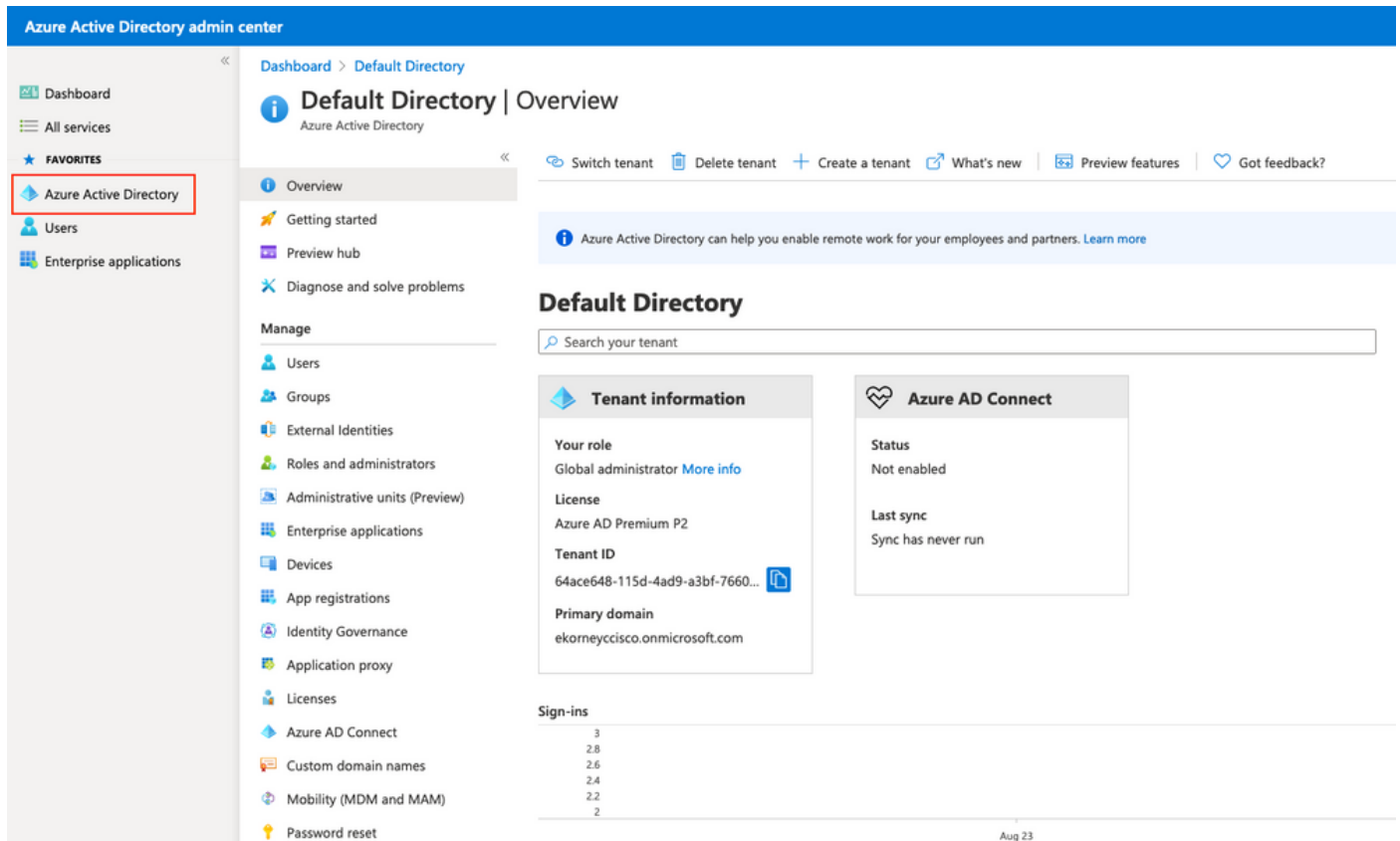
AssertionConsumerService Location="<https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action>"

AssertionConsumerService Location="

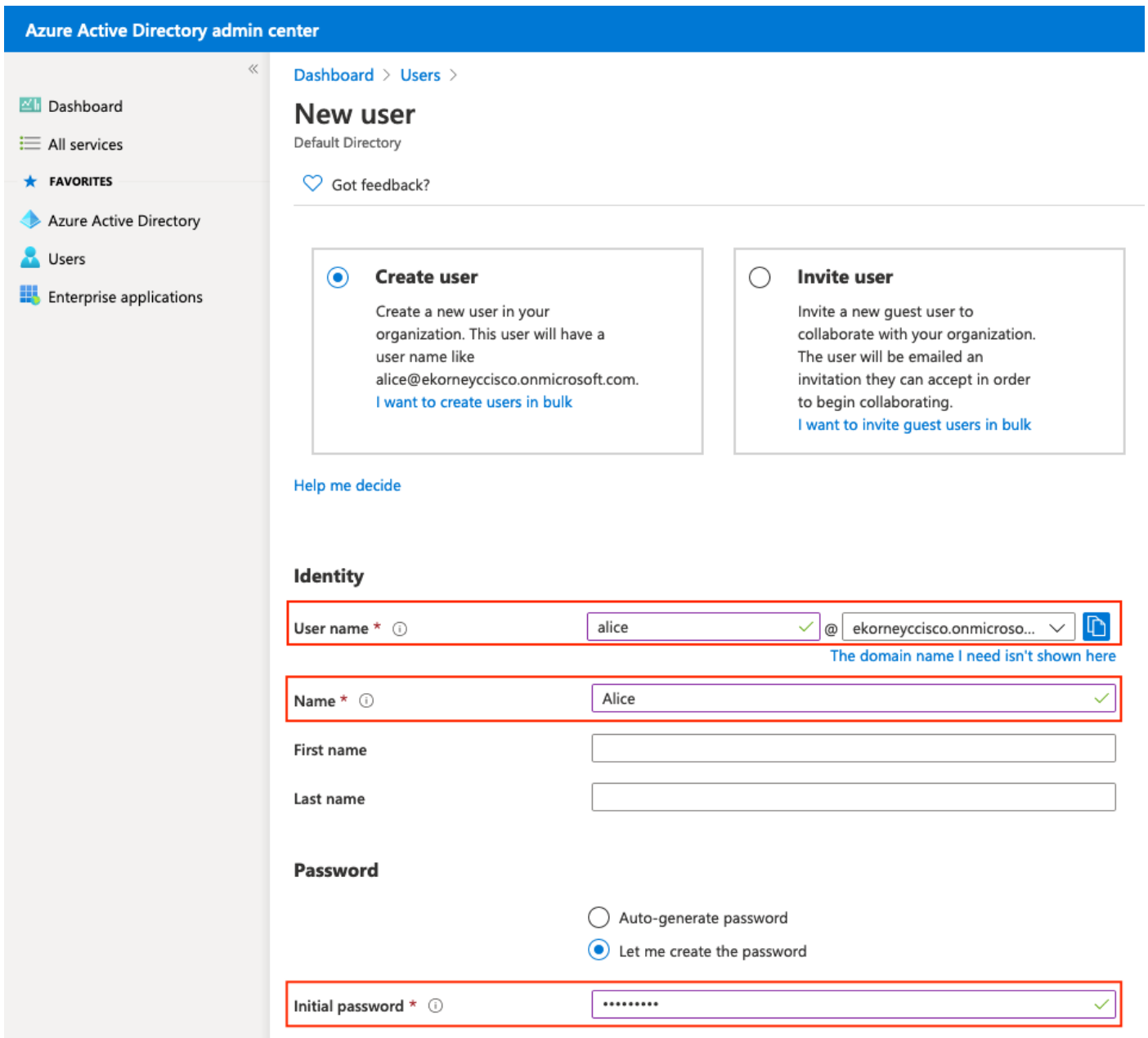
Etapa 2. Definir as Configurações do IdP do Azure AD

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.

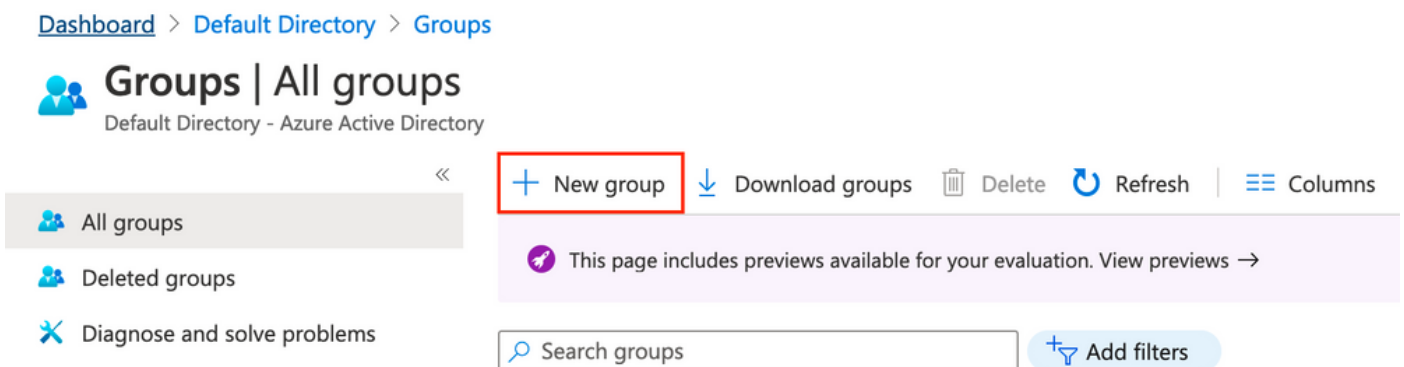


Selecione **Users**, clique em **New User**, configure **User name**, **Name** e **Initial Password**. Clique em **Criar** como mostrado na imagem.



2. Criar um Grupo AD do Azure

Selecione **Grupos**. Clique em **Novo grupo** conforme mostrado na imagem.



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

Dashboard > Default Directory > Groups >

New Group

Group type *
Security

Group name * ⓘ
Sponsor Group

Group description ⓘ
Enter a description for the group

Azure AD roles can be assigned to the group (Preview) ⓘ
 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 ⓘ



AAD Terms Of Use
d52792f4-ba38-424d-8140-ada5b883f293



Alice
alice@ekorneyccisco.onmicrosoft.com
Selected



azure
azure@ekorneyccisco.onmicrosoft.com



Azure AD Identity Governance - Directory Management
ec245c98-4a90-40c2-955a-88b727d97151



Azure AD Identity Governance - Dynamics 365 Management
c495cfdc-814f-46a1-89f0-657921c9fbe0



Azure AD Identity Governance Insights
58c746b0-a0b0-4647-a8f6-12dde5981638



Azure AD Identity Protection
fc68d9e5-1f76-45ef-99aa-214805418498



Azure AD Notification
fc03f97a-9db0-4627-a216-ec98ce54e018



Azure ESTS Service
00000001-0000-0000-c000-000000000000

Selected items



Alice
alice@ekorneyccisco.onmicrosoft.com

Remove

Anote a ID do objeto de grupo, nesta tela, ela é f626733b-eb37-4cf2-b2a6-c2895fd5f4d3 para o grupo de patrocinadores.

Groups | All groups

Default Directory - Azure Active Directory

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

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

Search groups Add filters

Name	Object Id	Group Type	Membership Type
<input type="checkbox"/> IG ISE Group	eebf9cb9-91e2-4989-8c06-eef2cd3f69a3	Security	Assigned
<input type="checkbox"/> SG Sponsor Group	f626733b-eb37-4cf2-b2a6-c2895fd5f4d3	Security	Assigned

4. Criar um Aplicativo Azure AD Enterprise

Em AD, selecione **Enterprise Applications** e clique em **New application** conforme mostrado na imagem.

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications

Enterprise applications | All applications

Default Directory - Azure Active Directory

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

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

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

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

Selecione o aplicativo **Não é galeria** como mostrado na imagem.

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications >

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access.
- Non-gallery application**
Integrate any other application that you don't find in the gallery

Digite o nome do aplicativo e clique em **Adicionar**.

Add your own application

Name * ⓘ

ISE30

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports: ⓘ

SAML-based single sign-on

[Learn more](#)

Automatic User Provisioning with SCIM

[Learn more](#)

Password-based single sign-on

[Learn more](#)

5. Adicionar grupo ao aplicativo

Selecione **Atribuir usuários e grupos**.

ISE30 | Overview

Enterprise Application

Overview

- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Security
- Conditional Access

Properties

- Name ⓘ
ISE30
- Application ID ⓘ
20ee030a-1a06-4a65-80ce-9 ...
- Object ID ⓘ
0e6aac66-0ce1-4924-84a6-0 ...

Getting Started



1. Assign users and groups

Provide specific users and groups access to the applications
[Assign users and groups](#)



2. Set up single sign on

Enable users to sign into their application using their Azure AD credentials
[Get started](#)

Clique em **Adicionar usuário**.

ISE30 | Users and groups

Enterprise Application

[+ Add user](#) [Edit](#) [Remove](#) [Update Credentials](#) | [Columns](#) | [Got feedback?](#)

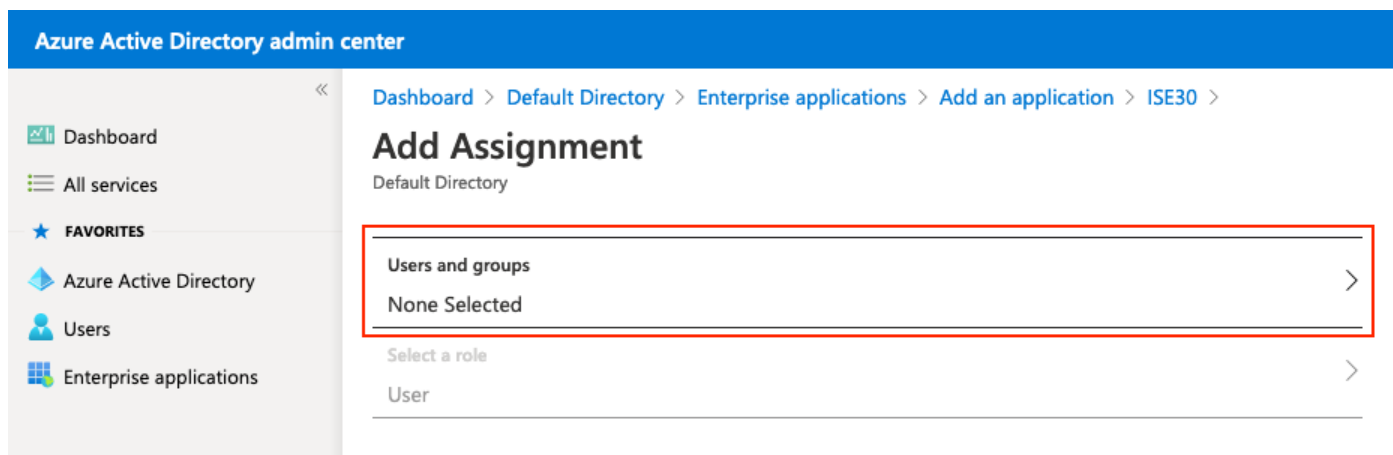
i The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

Display Name

No application assignments found

Clique em **Usuários e grupos**.



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

Note: Cabe a você selecionar o conjunto certo de usuários ou grupos que devem obter acesso.

Users and groups



Search



Alice
alice@ekorneyccisco.onmicrosoft.com



azure
azure@ekorneyccisco.onmicrosoft.com



Eugene Korneychuk
ekorneyc@cisco.com



ISE Group

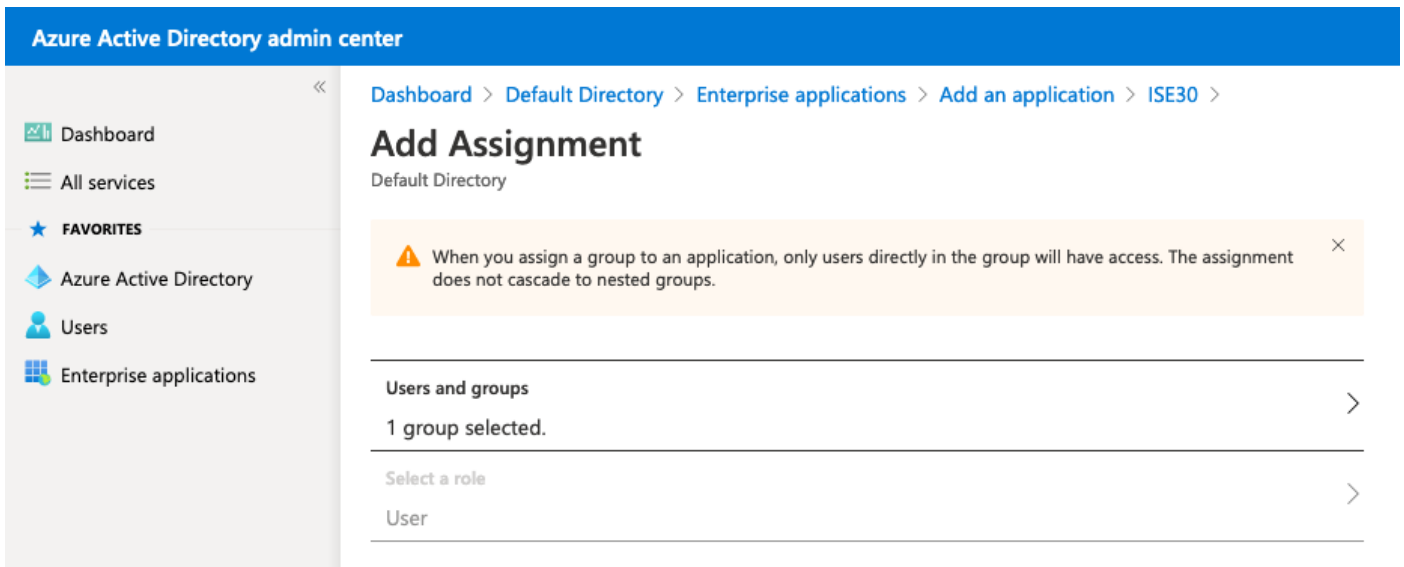


Sponsor
sponsor@ekorneyccisco.onmicrosoft.com

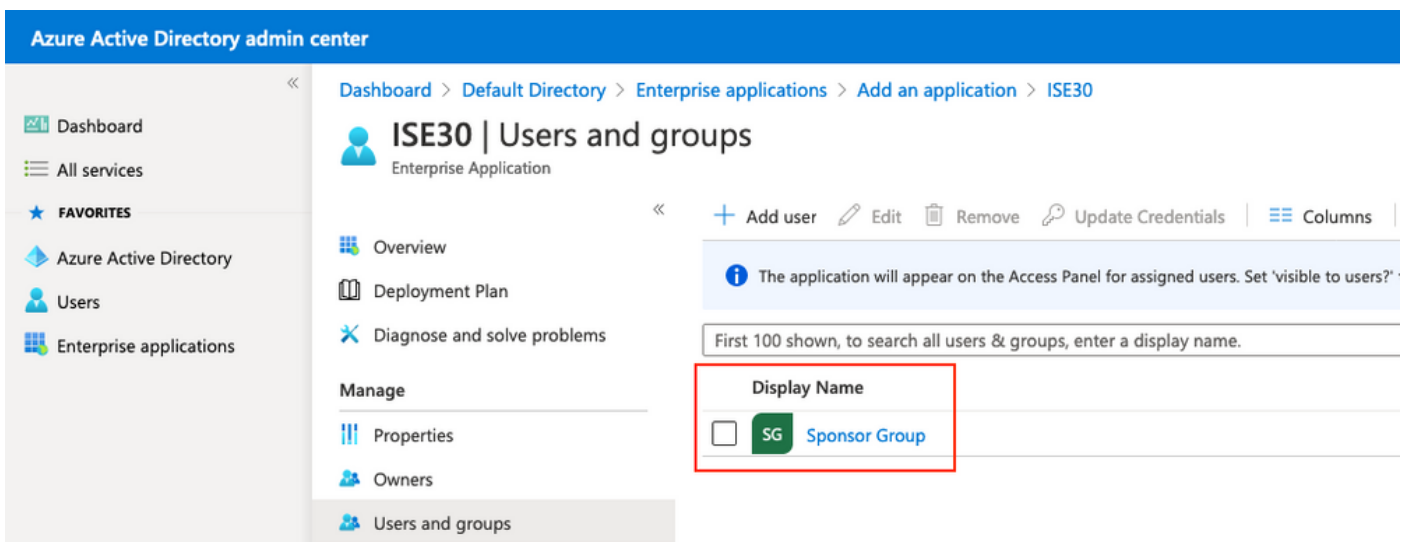


Sponsor Group
Selected

Quando o grupo for selecionado, clique em **Atribuir** conforme mostrado na imagem.



Como resultado, o menu **Usuários e grupos** de seu aplicativo deve ser preenchido com o grupo selecionado.



6. Configurar um Aplicativo Azure AD Enterprise

Volte para o Aplicativo e clique em **Configurar login único** conforme mostrado na imagem.

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications > Add an application > ISE30

ISE30 | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access

Properties

Name ⓘ
ISE30

Application ID ⓘ
20ee030a-1a06-4a65-80ce-9 ...

Object ID ⓘ
0e6aac66-0ce1-4924-84a6-0 ...

Getting Started

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)

Selecione **SAML** na próxima tela.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE30

ISE30 | Single sign-on

Enterprise Application

Select a single sign-on method [Help me decide](#)

- Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

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

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE30 >

ISE30 | SAML-based Sign-on

Enterprise Application

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

Set up Single Sign-On with SAML

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

- ### Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- ### User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- ### SAML Signing Certificate

Status	Active
Thumbprint	8E26CD6E415249B9B13D8ACDF4216A464E0AE20C
Expiration	7/18/2025, 2:00:00 AM
Notification Email	ekorneyc@cisco.com
App Federation Metadata Url	https://login.microsoftonline.com/64ace648-115d ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Preencha o Identificador (ID da entidade) com o valor de ID da entidade do arquivo XML da etapa Exportar informações do provedor de serviços. Preencha a URL de resposta (URL de serviço do consumidor de asserção) com o valor de Locais do AssertionConsumerService. Preencha o valor de Url de Logoff com ResponseLocation do SingleLogoutService. Clique em Salvar.

Note: A URL de resposta atua como uma lista de aprovação, o que permite que determinados URLs atuem como origem quando redirecionados 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

<input type="text" value="http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429"/>	<input checked="" type="checkbox"/>	ⓘ	
<input type="text"/>			

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

<input type="text" value="https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action"/>	<input checked="" type="checkbox"/>	ⓘ	
<input type="text" value="https://10.48.23.86:8445/sponsorportal/SSOLoginResponse.action"/>	<input type="checkbox"/>	ⓘ	
<input type="text" value="https://10.48.26.63:8445/sponsorportal/SSOLoginResponse.action"/>	<input type="checkbox"/>	ⓘ	
<input type="text" value="https://10.48.26.60:8445/sponsorportal/SSOLoginResponse.action"/>	<input type="checkbox"/>	ⓘ	
<input type="text" value="https://ise30-1ek.example.com:8445/sponsorportal/SSOLoginResponse.action"/>	<input type="checkbox"/>	ⓘ	
<input type="text" value="https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action"/>	<input type="checkbox"/>	ⓘ	
<input type="text" value="https://ise30-3ek.example.com:8445/sponsorportal/SSOLoginResponse.action"/>	<input checked="" type="checkbox"/>	ⓘ	
<input type="text"/>			

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

<input type="text" value="https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action"/>	<input checked="" type="checkbox"/>
--	-------------------------------------

7. Configurar Atributo de Grupo do Ative Directory

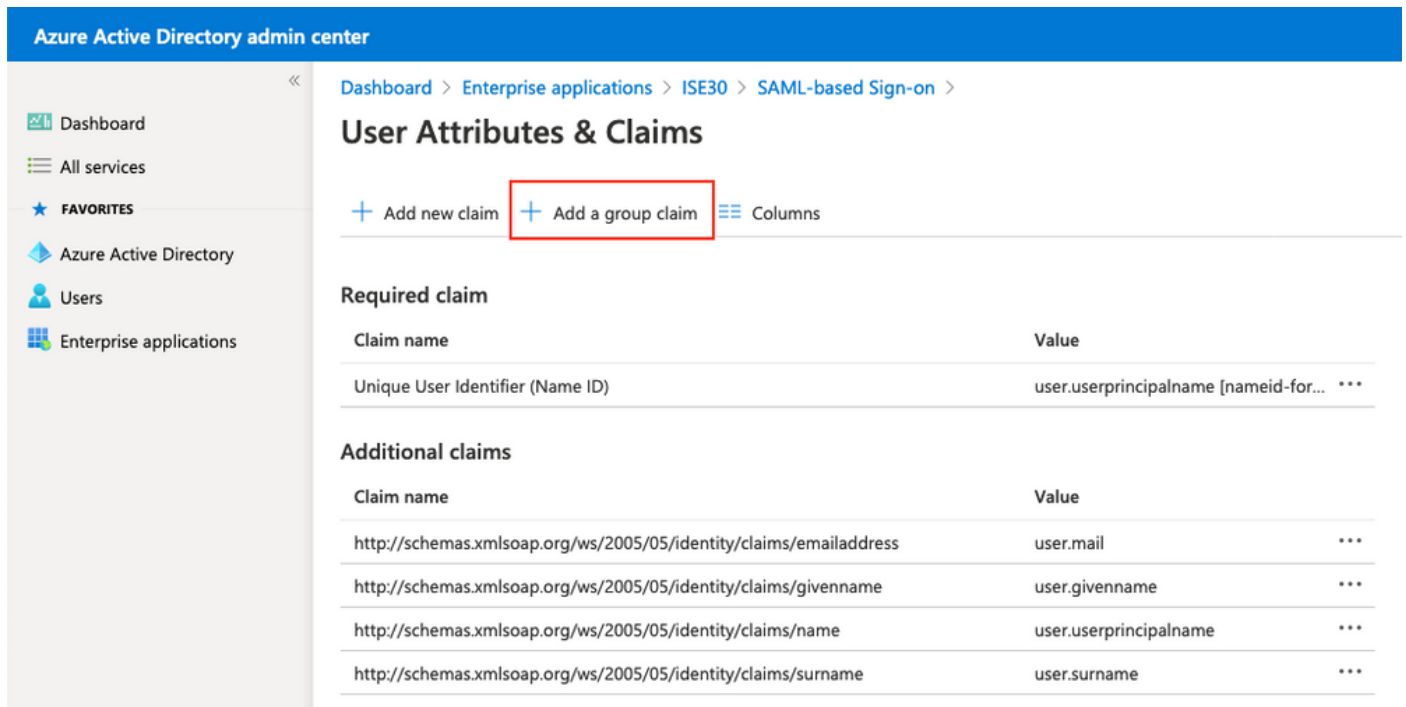
Para retornar o valor do atributo do grupo configurado anteriormente, clique em **Editar** ao lado de **Atributos e reivindicações do usuário**.

User Attributes & Claims



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

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



Azure Active Directory admin center

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

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

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

Additional claims

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

Selecione **Grupos de segurança** e clique em **Salvar**. O atributo de origem retornado na asserção é um **ID de grupo**, que é um **ID de objeto de grupo** capturado anteriormente.

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

Anote o nome da Reivindicação para o grupo. Nesse caso, é o <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups>.

The screenshot shows the Azure Active Directory admin center interface. The breadcrumb navigation is: Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on > User Attributes & Claims. The page title is "User Attributes & Claims". There are three buttons: "+ Add new claim", "+ Add a group claim", and "Columns".

Required claim

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

Additional claims

Claim name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups [SecurityGroup] ***
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. Baixar Arquivo XML de Metadados de Federação do Azure

Clique em **Download** em **XML de metadados de federação em SAML Signing Certificate**.

SAML Signing Certificate

 Edit

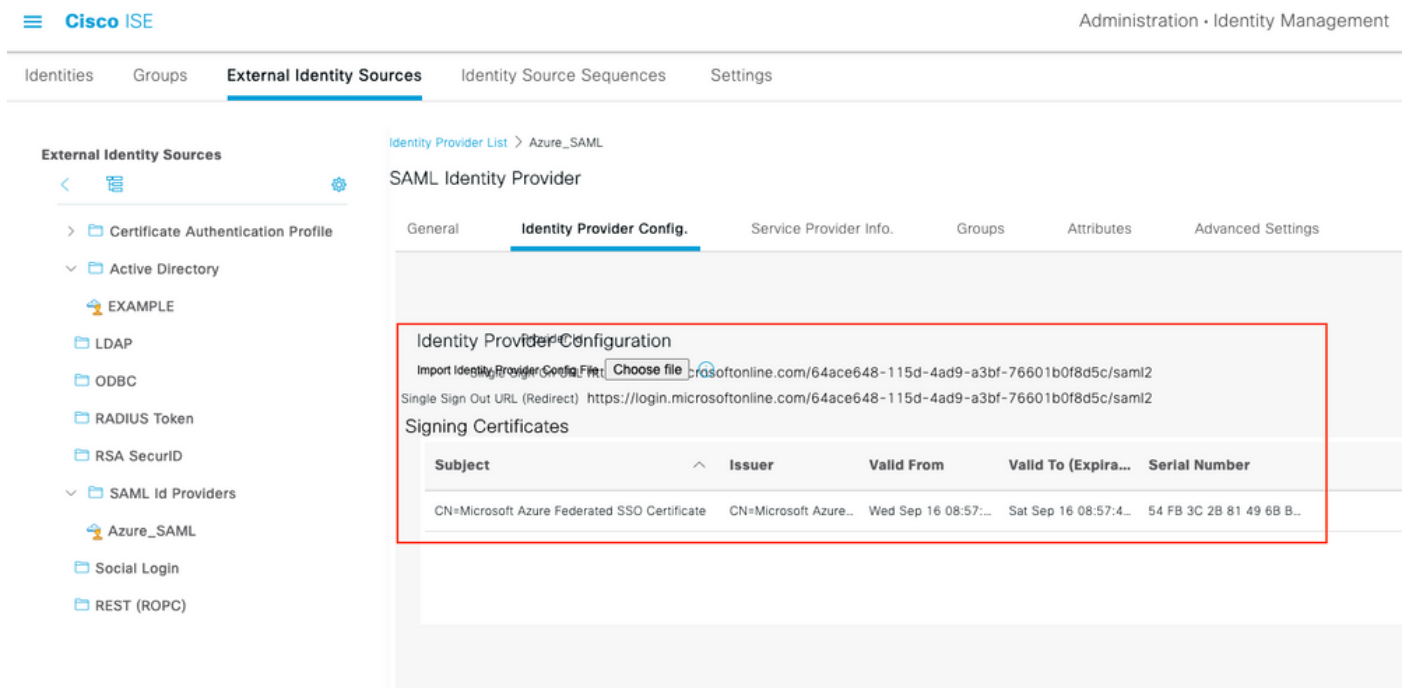
Status	Active
Thumbprint	9772DA460A43ACDA2AC5F09EE33ED7DAA7BAE2
Expiration	9/16/2023, 10:57:46 AM
Notification Email	ekorneyc@cisco.com
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/64ace648-115d ..."/>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Etapa 3. Carregar Metadados do Azure Active Directory para o ISE

Navegue até **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]**.

Mude para a guia **Config. provedor de identidade**, e clique no botão **Procurar**. Selecione o ficheiro XML de Metadados de Federação na etapa **Transferir XML de Metadados de Federação do Azure** e clique em **Guardar**.

Note: A falha da interface do usuário com a configuração do provedor de identidade deve ser tratada em [CSCvv74517](#).



The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is **Administration > Identity Management > External Identity Sources > SAML Id Providers > Azure_SAML**. The main content area is titled **SAML Identity Provider** and has several tabs: **General**, **Identity Provider Config.** (selected), **Service Provider Info.**, **Groups**, **Attributes**, and **Advanced Settings**. The **Identity Provider Config.** tab is highlighted with a red box. It contains the following information:

- Import Identity Provider Configuration:** `https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2`
- Single Sign Out URL (Redirect):** `https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2`
- Signing Certificates:**

Subject	Issuer	Valid From	Valid To (Expira...	Serial Number
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azure...	Wed Sep 16 08:57:...	Sat Sep 16 08:57:4...	54 FB 3C 2B 81 49 68 B...

Etapa 4. Configurar grupos SAML no ISE

Mude para a guia **Grupos** e cole o valor do **Nome da reivindicação do atributo Configurar Grupo do Active Directory** no **Atributo de Associação do Grupo**.

External Identity Sources

- < External Identity Sources
- > Certificate Authentication Profile
- > Active Directory
 - EXAMPLE
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers
 - Azure_SAML
 - Social Login
 - REST (ROPC)

Identity Provider List > Azure_SAML

SAML Identity Provider

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

Groups

Group Membership Attribute [Ip://schemas.microsoft.com/ws/2008/06/identity/claims/groups](http://schemas.microsoft.com/ws/2008/06/identity/claims/groups)[+ Add](#) [Edit](#) [Delete](#)

Name in Assertion

Name in ISE

No data available

Clique em **Adicionar**. Preencha o **Nome na Asserção** com o valor da **ID do Objeto do Grupo Patrocinador** capturado em **Atribuir Usuário do Azure Active Directory ao Grupo**. Configure o **Nome no ISE** com o valor significativo nesse caso, é o **Grupo de Patrocinadores do Azure**. Click **OK**. Clique em **Save**.

Isso cria um mapeamento entre o Grupo no Azure e o nome do Grupo que pode ser usado no ISE.

Add Group

*Name in Assertion

*Name in ISE

Etapa 5. Configurar o mapeamento de grupo de patrocinadores no ISE

Navegue até **Centros de Trabalho > Acesso de Convidado > Portais e Componentes > Grupos de Patrocinadores** e selecione **Grupo de Patrocinadores** que deseja mapear para o **Grupo AD do Azure**. Neste exemplo, ALL_ACCOUNTS (padrão) foi usado.

Guest Portals

Guest Types

Sponsor Groups

Sponsor Portals

Sponsor Groups

You can edit and customize the default sponsor groups and create additional ones.

A sponsor is assigned the permissions from **all** matching sponsor groups (multiple matches are permitted) ⓘ

[Create](#) [Edit](#) [Duplicate](#) [Delete](#)

Enabled	Name	Member Groups
---------	------	---------------

**ALL_ACCOUNTS (default)**

Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group

[More](#)

ALL_ACCOUNTS (default)

**GROUP_ACCOUNTS (default)**

Sponsors assigned to this group can manage just the guest accounts created by sponsors from the same sponsor group. By default, users in the GROUP_ACCOUNTS user identity group are members of this sponsor group

[More](#)

GROUP_ACCOUNTS (default)

**OWN_ACCOUNTS (default)**

Sponsors assigned to this group can manage only the guest accounts that they have created. By default, users in the OWN_ACCOUNTS user identity group are members of this sponsor group

[More](#)

OWN_ACCOUNTS (default)

Clique em **Membros...** e adicione **Azure_SAML:Azure Sponsor Group** a **Seleted User Groups**. Isso mapeia o **Grupo de Patrocinadores** no Azure para o Grupo de Patrocinadores **ALL_ACCOUNTS**. Clique em **OK**. Clique em **Salvar**.



Select Sponsor Group Members

Select the user groups who will be members of this Sponsor Group

Available User Groups

Selected User Groups

Name ^

Employee

GROUP_ACCOUNTS (default)

OWN_ACCOUNTS (default)

Name ^

ALL_ACCOUNTS (default)

Azure_SAML:Azure Sponsor Group

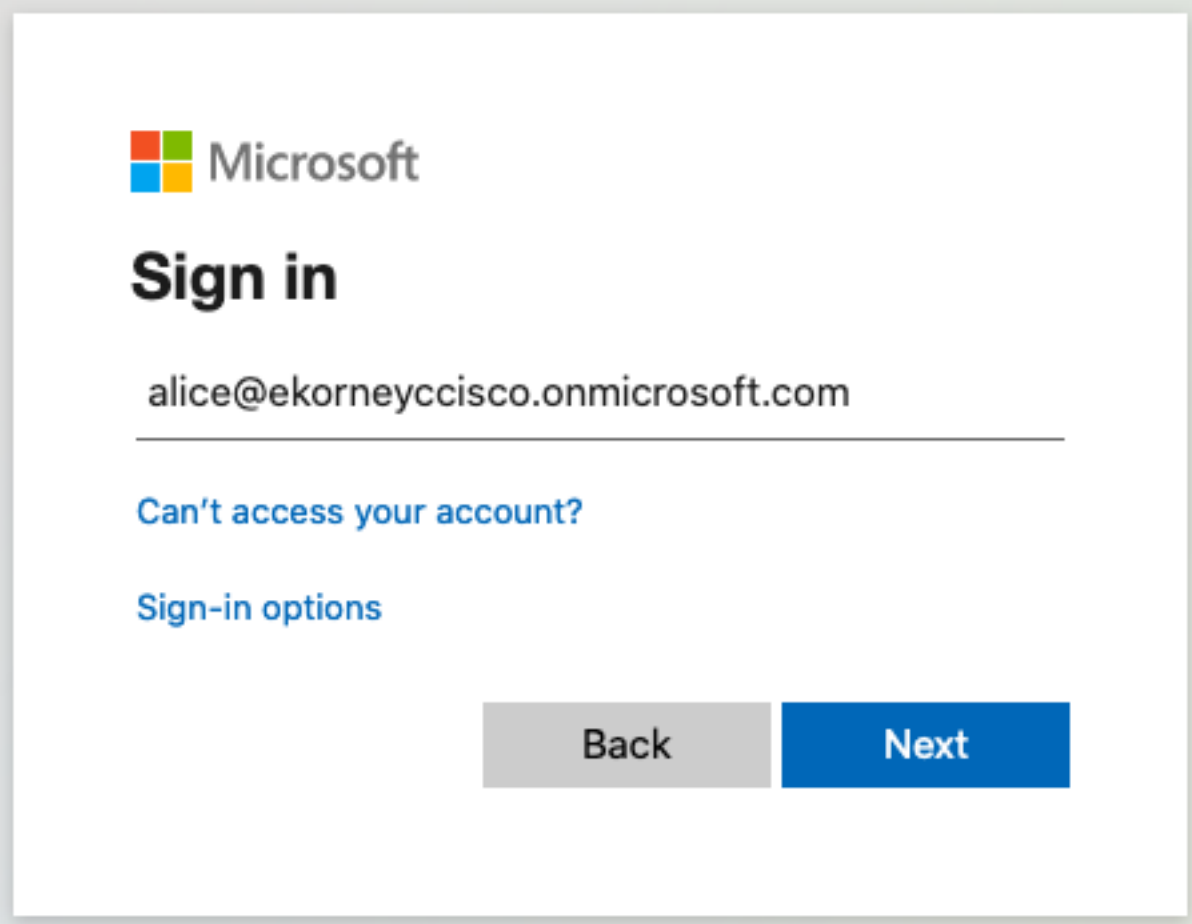
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Note: O novo usuário é forçado a alterar a senha do usuário no primeiro login. E aceite que as etapas de verificação AUP não cobrem isso. A verificação abrange o cenário, em que os usuários fazem login não pela primeira vez, e a AUP já foi aceita uma vez pelo Patrocinador (alice).

Agora, se você abrir o Portal do Patrocinador (na URL do teste, por exemplo), será redirecionado para o Azure para entrar e, em seguida, voltar para o Portal do Patrocinador.

1. Inicie o Portal do Patrocinador com seu FQDN no link do URL do Teste do Portal. O ISE deve redirecioná-lo para a página de entrada do Azure. Insira o **nome de usuário** criado anteriormente e clique em **Avançar**.



Microsoft

Sign in

alice@ekorneyccisco.onmicrosoft.com

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

[Sign-in options](#)

Back Next

2. Digite a **senha** e clique em **Entrar**. A tela de login do IdP redireciona o usuário para o Portal do Patrocinador do ISE inicial.



← alice@ekorneyccisco.onmicrosoft.com

Enter password

.....|

[Forgot my password](#)

Sign in

3. Aceite o AUP.

alice@ekorneyccisco.onmicrosoft.com ⓘ



Acceptable Use Policy

Please read the Acceptable Use Policy.

You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline

[Help](#)

4. Neste ponto, o usuário do patrocinador deve ter acesso total ao portal com permissões de grupo de patrocinadores **ALL_ACCOUNTS**.

Create Accounts

Manage Accounts (0)

Pending Accounts (0)

Notices (0)

Create, manage, and approve guest accounts.

Guest type:

Contractor (default)

Maximum devices that can be connected: 5 | Maximum access duration: 365 days

Guest Information

Known

Random

Import

First name:

Last name:

Email address:

Mobile number:

Company:

Person being visited (email):

Reason for visit:

Group tag:

Language:

English - English

Access Information

End of business day

23:59

Duration:*

90

Days (Maximum:365)

From Date (yyyy-mm-dd) *

2020-09-16

From Time *

11:22

To Date (yyyy-mm-dd) *

2020-12-15

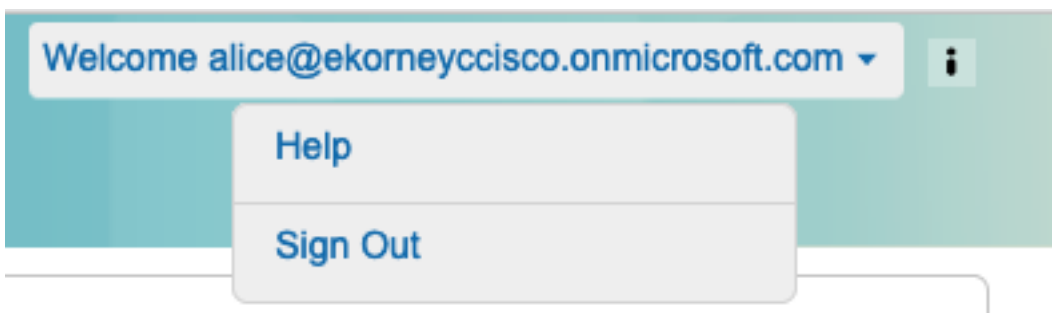
To Time *

10:22

Create

[Help](#)

5. Clique em **Sair** no menu suspenso Welcome (Bem-vindo).



6. O usuário deve ser desconectado com êxito e redirecionado para a tela de login novamente.



Pick an account



alice@ekorneyccisco.onmicrosoft.co
m



Use another account

Troubleshoot

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 Azure Active Directory. Assim, você pode obter erros relacionados à autenticação diretamente do provedor de identidade (Azure), onde o comprometimento do ISE ainda não foi iniciado.

Problema 1. O usuário digita a senha errada, nenhum processamento de dados do usuário foi feito no ISE, o problema vem diretamente do IdP (Azure). Para corrigir: Redefina a senha ou forneça os dados de senha corretos.



← alice@ekorneyccisco.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 deveria ter permissão para acessar SAML SSO, novamente nesse caso, nenhum processamento de dados do usuário foi feito no ISE, o problema vem diretamente do IdP (Azure). Para corrigir: Verifique se o **grupo Add (Adicionar)** à etapa de configuração **do aplicativo** foi executado corretamente.



Sign in

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

AADSTS50105: The signed in user 'azure@ekorneyccisco.onmicrosoft.com' is not assigned to a role for the application '92ecf9db-766a-42bf-af42-617e95d44675'(ISE).

Troubleshooting details ×

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

[Copy info to clipboard](#)

Request Id: e128020b-a4b1-4a5e-9ea8-2c7007b1fe00

Correlation Id: 09a3bce1-8dc9-464d-ab97-85e2bf1f0a33

Timestamp: 2020-05-21T13:03:07Z

Message: AADSTS50105: The signed in user 'azure@ekorneyccisco.onmicrosoft.com' is not assigned to a role for the application '92ecf9db-766a-42bf-af42-617e95d44675'(ISE).

Advanced diagnostics: [Enable](#)

If you plan on getting support for an issue, turn this on and try to reproduce the error. This will collect additional information that will help troubleshoot the issue.

3. O Sing Out não funciona como esperado, esse erro é visto - "Falha no Logout SSO. Ocorreu um problema ao encerrar a sessão SSO. Entre em contato com o help desk para obter assistência." Ele pode ser visto quando a URL de logoff não está configurada corretamente no IdP de SAML. Nesse caso, este URL foi usado como ["https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2"](https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2) enquanto deveria ser ["https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action"](https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action) Para corrigir: digite a URL correta na URL de Logoff no IdP do Azure.

Error

SSO Logout failed.
 There was a problem to logout from your SSO session. Please contact help desk for assistance.

[Help](#)

Solução de problemas do cliente

Para verificar se o payload SAML é recebido, você pode usar as ferramentas de desenvolvedor da Web. Navegue até **Ferramentas > Web Developer > Rede** se você fizer uso do Firefox e efetuar login com credenciais do Azure no Portal. Você pode ver a resposta SAML criptografada na guia **Params**:

The screenshot shows the Cisco Sponsor Portal interface with the Firefox Developer Tools Network tab open. The page content includes buttons for 'Create Accounts', 'Manage Accounts (0)', 'Pending Accounts (0)', and 'Notices (0)'. Below these are sections for 'Guest type' (Contractor), 'Guest Information' (Known, Random, Import), and 'Access Information' (End of business day). The Network tab shows a list of requests, with the SAML response selected. The Params pane displays the SAML response payload, which is a complex XML structure containing various attributes and elements.

Troubleshooting do ISE

O nível de log dos componentes aqui deve ser alterado no ISE. Navegue até **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**.

Nome do componente	Nível de log	Nome do arquivo de log
acesso de convidado	DEBUG	guest.log
portal-web-ação	DEBUG	guest.log
opensamol	DEBUG	ise-psc.log
amostra	DEBUG	ise-psc.log

Conjunto de depurações em funcionamento no momento da execução correta do fluxo (ise-

psc.log):

1. O usuário é redirecionado para a URL do IdP no portal do patrocinador.

```
2020-09-16 10:43:59,207 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isLoadBalancerConfigured() - LB NOT
configured for: Azure_SAML
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL:
https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SPPProviderId for Azure_SAML is:
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isLoadBalancerConfigured() - LB NOT
configured for: Azure_SAML
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request - providerId (as should be found in
IdP configuration):
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request - returnToId (relay state):
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-8e40-
e43d20c9f429_SEMIportalSessionId_EQUALS8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1_SEMItoken_EQUALSOA6CZJQD7X67TLYHE4Y3EM3EY097E2J_SEMI_DELIMITERSponsor30.example.com
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request - spUrlToReturnTo:
https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action
```

2. A resposta SAML é recebida do navegador.

```
2020-09-16 10:44:11,122 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,126 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1;token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;
2020-09-16 10:44:11,126 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State
:_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,126 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1;token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;
2020-09-16 10:44:11,129 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,129 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1;token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;
```

2020-09-16 10:44:11,133 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1;token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML flow initiator PSN's Host name
is:sponsor30.example.com
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- Is redirect required:
InitiatorPSN:sponsor30.example.com
This node's host name:ISE30-lek LB:null request Server Name:sponsor30.example.com
2020-09-16 10:44:11,182 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- This node is the initiator (sponsor30.example.com)
this node host name is:sponsor30.example.com
2020-09-16 10:44:11,184 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
org.opensaml.xml.parse.BasicParserPool -::::- Setting DocumentBuilderFactory attribute
'http://javax.xml.XMLConstants/feature/secure-processing'
2020-09-16 10:44:11,187 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
org.opensaml.xml.parse.BasicParserPool -::::- Setting DocumentBuilderFactory attribute
'http://apache.org/xml/features/disallow-doctype-decl'
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Beginning to decode message from inbound
transport of type: org.opensaml.ws.transport.http.HttpServletRequestAdapter
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.saml2.binding.decoding.HTTPPostDecoder -::::- Decoded SAML relay state of:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-8e40-
e43d20c9f429_SEMIportalSessionId_EQUALS8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1_SEMItoken_EQUALSOA6CZJQD7X67TLYHE4Y3EM3EY097E2J_SEMI_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.saml2.binding.decoding.HTTPPostDecoder -::::- Getting Base64 encoded message from
request
2020-09-16 10:44:11,191 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Parsing message stream into DOM document
2020-09-16 10:44:11,193 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Unmarshalling message DOM
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.xml.signature.impl.SignatureUnmarshaller -::::- Starting to unmarshall Apache XML-
Security-based SignatureImpl element
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.xml.signature.impl.SignatureUnmarshaller -::::- Constructing Apache XMLSignature object
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.xml.signature.impl.SignatureUnmarshaller -::::- Adding canonicalization and signing
algorithms, and HMAC output length to Signature
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.xml.signature.impl.SignatureUnmarshaller -::::- Adding KeyInfo to Signature
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Message succesfully unmarshalled
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.saml2.binding.decoding.HTTPPostDecoder -::::- Decoded SAML message
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.saml2.binding.decoding.BaseSAML2MessageDecoder -::::- Extracting ID, issuer and issue
instant from status response
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- No security policy resolver attached to


```
this message context, no security policy evaluation attempted
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
opensaml.ws.message.decoder.BaseMessageDecoder -:::- Successfully decoded message.
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::- Checking SAML message intended
destination endpoint against receiver endpoint
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::- Intended message destination
endpoint:
https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::- Actual message receiver endpoint:
https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::-
SAML decoder's URIComparator -
[https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action] vs.
[https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action]
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::-
SAML message intended destination endpoint matched recipient endpoint
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
```

3. A análise de atributo (asserção) foi iniciada.

```
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Found attribute name :
http://schemas.microsoft.com/identity/claims/tenantid
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Delimiter not configured,
Attribute=<http://schemas.microsoft.com/identity/claims/tenantid> add value=<64ace648-115d-4ad9-a3bf-76601b0f8d5c>
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Set on IdpResponse object
-
attribute<http://schemas.microsoft.com/identity/claims/tenantid> value=<64ace648-115d-4ad9-a3bf-76601b0f8d5c>
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Found attribute name :
http://schemas.microsoft.com/identity/claims/objectidentifier
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Delimiter not configured,
Attribute=<http://schemas.microsoft.com/identity/claims/objectidentifier> add value=<50ba7e39-e7fb-4cb1-8256-0537e8a09146>
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Set on IdpResponse object
-
attribute<http://schemas.microsoft.com/identity/claims/objectidentifier> value=<50ba7e39-e7fb-4cb1-8256-0537e8a09146>
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Found attribute name :
http://schemas.microsoft.com/identity/claims/displayname
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Delimiter not configured,
Attribute=<http://schemas.microsoft.com/identity/claims/displayname> add value=<Alice>
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Set on IdpResponse object
-
attribute<http://schemas.microsoft.com/identity/claims/displayname> value=<Alice>
```

4. O atributo de grupo é recebido com o valor de f626733b-eb37-4cf2-b2a6-c2895fd5f4d3,

validação de assinatura.

```
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<http://schemas.microsoft.com/ws/2008/06/identity/claims/groups> add value=<f626733b-  
eb37-4cf2-b2a6-c2895fd5f4d3>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Set on IdpResponse object  
- attribute  
<http://schemas.microsoft.com/ws/2008/06/identity/claims/groups> value=<f626733b-eb37-4cf2-b2a6-  
c2895fd5f4d3>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
http://schemas.microsoft.com/identity/claims/identityprovider  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<http://schemas.microsoft.com/identity/claims/identityprovider> add  
value=<https://sts.windows.net/64ace648-115d-4ad9-a3bf-76601b0f8d5c/>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Set on IdpResponse object  
- attribute  
<http://schemas.microsoft.com/identity/claims/identityprovider>  
value=<https://sts.windows.net/64ace648-115d-4ad9-a3bf-76601b0f8d5c/>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
http://schemas.microsoft.com/claims/authnmethodsreferences  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<http://schemas.microsoft.com/claims/authnmethodsreferences> add  
value=<http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Set on IdpResponse object  
- attribute  
<http://schemas.microsoft.com/claims/authnmethodsreferences>  
value=<http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> add  
value=<alice@ekorneyccisco.onmicrosoft.com>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Set on IdpResponse object  
- attribute  
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>  
value=<alice@ekorneyccisco.onmicrosoft.com>  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::getUserNameFromAssertion:  
IdentityAttribute is set to Subject Name  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::getUserNameFromAssertion: username  
value from Subject is=[alice@ekorneyccisco.onmicrosoft.com]  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::getUserNameFromAssertion: username set  
to=[alice@ekorneyccisco.onmicrosoft.com]  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response: Found value for 'username'  
attribute assertion: alice@ekorneyccisco.onmicrosoft.com
```

2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [SAMLAttributesParser:readDict]
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.cfg.IdentityProviderMgr -::::- getDict: Azure_SAML
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [SAMLAttributesParser:readDict]: read Dict
attribute=<ExternalGroups>
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/displayname> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [cacheGroupAttr] Adding to cache
ExternalGroup values=<f626733b-eb37-4cf2-b2a6-c2895fd5f4d3>
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/tenantid> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/identityprovider> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/objectidentifier> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/claims/authnmethodsreferences> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cisco.cpm.saml.framework.SAMLSessionDataCache -::::- [storeAttributesSessionData]
idStore=<Azure_SAML> userName=alice@ekorneyccisco.onmicrosoft.com>
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLAttributesParser -::::- [SAMLAttributesParser:getEmail] The email
attribute not configured on IdP
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response: email attribute value:
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal ID:bd48c1a1-9477-4746-
8e40-e43d20c9f429
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1;token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com

```
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML flow initiator PSN's Host name  
is:sponsor30.example.com  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isLoadBalancerConfigured() - LB NOT  
configured for: Azure_SAML  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isOracle() - checking whether IDP URL  
indicates that its OAM.  
IDP URL: https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SPProviderId for Azure_SAML is:  
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- ResponseValidationContext:  
IdP URI: https://sts.windows.net/64ace648-115d-4ad9-a3bf-76601b0f8d5c/  
SP URI: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429  
Assertion Consumer URL: https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action  
Request Id: _bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-  
8e40-e43d20c9f429_SEMIportalSessionId_EQUALS8fa19bf2-9fa6-4892-b082-  
5cdabfb5daa1_SEMItoken_EQUALSOA6CZJQD7X67TLYHE4Y3EM3EY097E2J_SEMI_DELIMITERSponsor30.example.com  
Client Address: 10.61.170.160  
Load Balancer: null  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.SAMLSignatureValidator -::::- no signature in response  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Validating signature of assertion  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.BaseSignatureValidator -::::- Determine the signing certificate  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.BaseSignatureValidator -::::- Validate signature to SAML standard  
with cert:CN=Microsoft Azure Federated SSO Certificate  
serial:112959638548824708724869525057157788132  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
org.opensaml.security.SAMLSignatureProfileValidator -::::- Saw Enveloped signature transform  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
org.opensaml.security.SAMLSignatureProfileValidator -::::- Saw Exclusive C14N signature  
transform  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.BaseSignatureValidator -::::- Validate signature againsta signing  
certificate  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
org.opensaml.xml.signature.SignatureValidator -::::- Attempting to validate signature using key  
from supplied credential  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
org.opensaml.xml.signature.SignatureValidator -::::- Creating XMLSignature object  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
org.opensaml.xml.signature.SignatureValidator -::::- Validating signature with signature  
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
org.opensaml.xml.signature.SignatureValidator -::::- Validation credential key algorithm 'RSA',  
key instance class 'sun.security.rsa.RSAPublicKeyImpl'  
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
org.opensaml.xml.signature.SignatureValidator -::::- Signature validated with key from supplied  
credential  
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Assertion signature validated  
succesfully  
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating response  
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating assertion  
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][  
cpm.saml.framework.validators.AssertionValidator -::::- Assertion issuer succesfully validated
```

```
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.AssertionValidator -:::- Authentication statements successfully
validated
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.AssertionValidator -:::- Subject successfully validated
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.AssertionValidator -:::- Conditions successfully validated
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: validation succeeded for
alice@ekorneyccisco.onmicrosoft.com
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: found signature on the assertion
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Retrieve [CN=Microsoft Azure Federated SSO
Certificate] as signing certificates
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: loginInfo:SAMLLoginInfo:
name=alice@ekorneyccisco.onmicrosoft.com,
format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress, sessionIndex=_4b798ec4-9aeb-40dc-
8bed-6dd2fdd46800, time diff=26329
2020-09-16 10:44:11,292 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: Azure_SAML
Subject: alice@ekorneyccisco.onmicrosoft.com
SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
SAML Success:true
SAML Status Message:null
SAML email:
SAML Exception:nullUserRole : SPONSOR
2020-09-16 10:44:11,292 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:alice@ekorneyccisco.onmicrosoft.com
2020-09-16 10:44:11,306 INFO [RMI TCP Connection(346358)-127.0.0.1][]
api.services.server.role.RoleImpl -:::- Fetched Role Information based on RoleID: 6dd3b090-
8bff-11e6-996c-525400b48521
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cisco.cpm.saml.framework.SAMLSessionDataCache -:::- [SAMLSessionDataCache:getGroupsOnSession]
idStore=<Azure_SAML> userName=<alice@ekorneyccisco.onmicrosoft.com>
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cisco.cpm.saml.framework.SAMLSessionDataCache -:::- [getAttributeOnSession]
idStore=<Azure_SAML> userName=<alice@ekorneyccisco.onmicrosoft.com>
attributeName=<Azure_SAML.ExternalGroups>
```

5. O grupo de usuários é adicionado aos resultados da autenticação para que possa ser usado pelo Portal, a autenticação SAML é passada.

```
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- AuthenticatePortalUser - added user groups from
SAML response to AuthenticationResult, all retrieved groups:[f626733b-eb37-4cf2-b2a6-
c2895fd5f4d3]
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Authenticate SAML User - result:PASSED
```

6. Sair é acionado. O URL de Logout é recebido na Resposta SAML;

<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action>.

```
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
SAMLUtils::isOracle() - checking whether IDP URL indicates that its OAM. IDP URL:
https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:- getLogoutMethod
```

```
- method:REDIRECT_METHOD_LOGOUT
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
getSignLogoutRequest - null
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - loginInfo:SAMLLoginInfo: name=alice@ekorneyccisco.onmicrosoft.com,
format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress, sessionIndex=_4b798ec4-9aeb-40dc-
8bed-6dd2fdd46800, time diff=26329
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
SAMLUtils::isLoadBalancerConfigured() - LB NOT configured for: Azure_SAML
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
SAMLUtils::isOracle() - checking whether IDP URL indicates that its OAM. IDP URL:
https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:- SPPProviderId
for Azure_SAML is: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - spProviderId:http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - logoutURL:https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-
76601b0f8d5c/saml2
2020-09-16 10:44:53,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML HTTPRequest - Portal ID:bd48c1a1-9477-4746-
8e40-e43d20c9f429
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML flow initiator PSN's Host name
is:sponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Is redirect required:
InitiatorPSN:sponsor30.example.com This node's host name:ISE30-lek LB:null request Server
Name:sponsor30.example.com
2020-09-16 10:44:53,248 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- This node is the initiator (sponsor30.example.com)
this node host name is:sponsor30.example.com
2020-09-16 10:44:53,249 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,249 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML HTTPRequest - Portal Session info:8fa19bf2-
9fa6-4892-b082-5cdabfb5daa1
2020-09-16 10:44:53,250 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
org.opensaml.xml.parse.BasicParserPool -:::- Setting DocumentBuilderFactory attribute
'http://javax.xml.XMLConstants/feature/secure-processing'
2020-09-16 10:44:53,251 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
org.opensaml.xml.parse.BasicParserPool -:::- Setting DocumentBuilderFactory attribute
'http://apache.org/xml/features/disallow-doctype-decl'
2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
opensaml.ws.message.decoder.BaseMessageDecoder -:::- Beginning to decode message from inbound
transport of type: org.opensaml.ws.transport.http.HttpServletRequestAdapter
2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
opensaml.saml2.binding.decoding.HTTPRedirectDeflateDecoder -:::- Decoded RelayState: _bd48c1a1-
9477-4746-8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1_DELIMITERsponsor30.example.com
```

2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.saml2.binding.decoding.HTTPRedirectDeflateDecoder -::::- Base64 decoding and inflating
SAML message
2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Parsing message stream into DOM document
2020-09-16 10:44:53,256 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Unmarshalling message DOM
2020-09-16 10:44:53,256 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Message succesfully unmarshalled
2020-09-16 10:44:53,256 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.saml2.binding.decoding.HTTPRedirectDeflateDecoder -::::- Decoded SAML message
2020-09-16 10:44:53,256 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.saml2.binding.decoding.BaseSAML2MessageDecoder -::::- Extracting ID, issuer and issue
instant from status response
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- No security policy resolver attached to
this message context, no security policy evaluation attempted
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.ws.message.decoder.BaseMessageDecoder -::::- Successfully decoded message.
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -::::- Checking SAML message intended
destination endpoint against receiver endpoint
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -::::- Intended message destination
endpoint: https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -::::- Actual message receiver endpoint:
https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML decoder's URIComparator -
[https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action] vs.
[https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action]
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -::::- SAML message intended destination
endpoint matched recipient endpoint
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:_bd48clal-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daal_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal ID:bd48clal-9477-4746-
8e40-e43d20c9f429
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:_bd48clal-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daal_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:8fa19bf2-
9fa6-4892-b082-5cdabfb5daal
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:_bd48clal-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daal_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:8fa19bf2-
9fa6-4892-b082-5cdabfb5daal
2020-09-16 10:44:53,257 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML flow initiator PSN's Host name
is:sponsor30.example.com
2020-09-16 10:44:53,258 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isLoadBalancerConfigured() - LB NOT
configured for: Azure_SAML
2020-09-16 10:44:53,258 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-
76601b0f8d5c/saml2
2020-09-16 10:44:53,258 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][

```
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SPProviderId for Azure_SAML is:
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:53,258 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- ResponseValidationContext:
IdP URI: https://sts.windows.net/64ace648-115d-4ad9-a3bf-76601b0f8d5c/
SP URI: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
Assertion Consumer URL:
https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action
Request Id: _bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1_DELIMITERSponsor30.example.com
Client Address: 10.61.170.160
Load Balancer: null
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- LogoutResponse signature validated
succesfully
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- This is LogoutResponse (only
REDIRECT is supported) no signature is on assertion, continue
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating response
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating assertion
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: validation succeeded for null
```