

Configure ISE 3.0 Sponsor Portal with Azure AD SAML SSO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[High-Level Flow Diagram](#)

[Configure](#)

[Step 1. Configure SAML Identity Provider and Sponsor Portal on ISE](#)

[1. Configure Azure AD as External SAML Identity Source](#)

[2. Configure Sponsor Portal to use Azure AD](#)

[3. Export Service Provider Information](#)

[Step 2. Configure Azure AD IdP Settings](#)

[1. Create an Azure AD User](#)

[2. Create an Azure AD Group](#)

[3. Assign Azure AD User to the Group](#)

[4. Create an Azure AD Enterprise Application](#)

[5. Add Group to the Application](#)

[6. Configure an Azure AD Enterprise Application](#)

[7. Configure Active Directory Group Attribute](#)

[8. Download Azure Federation Metadata XML File](#)

[Step 3. Upload MetaData from Azure Active Directory to ISE](#)

[Step 4. Configure SAML Groups on ISE](#)

[Step 5. Configure Sponsor Group Mapping on ISE](#)

[Verify](#)

[Troubleshoot](#)

[Common Issues](#)

[Client Troubleshooting](#)

[ISE Troubleshooting](#)

Introduction

This document describes how to configure an Azure Active Directory (AD) SAML server with Cisco Identity Services Engine (ISE) 3.0 to provide Single Sign-On (SSO) capabilities for Sponsor users.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

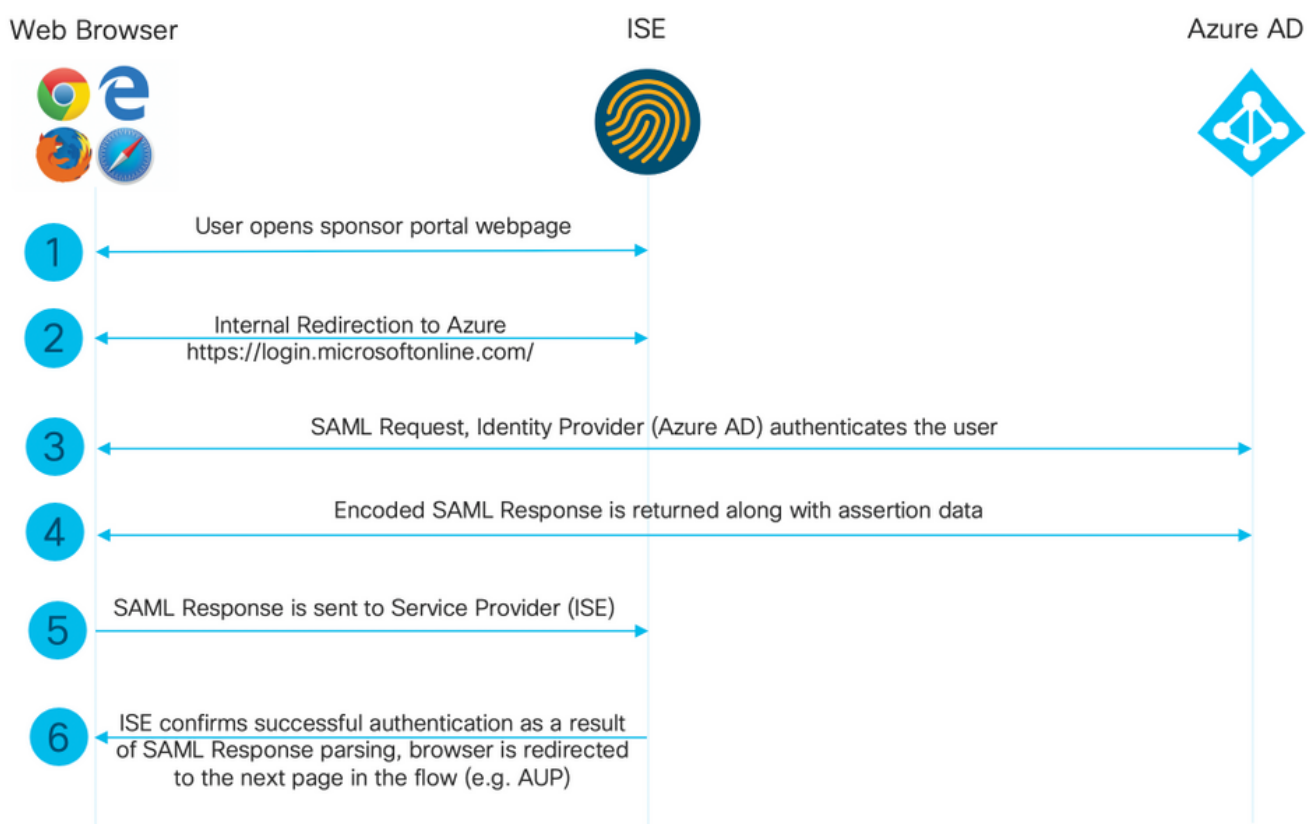
1. Cisco ISE 3.0
2. Basic knowledge about SAML SSO deployments
3. Azure AD

Components Used

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. If your network is live, ensure that you understand the potential impact of any command.

High-Level Flow Diagram



Configure



Step 1. Configure SAML Identity Provider and Sponsor Portal on ISE

1. Configure Azure AD as External SAML Identity Source

On ISE, navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers** and click the **Add** button.

Enter the **Id Provider Name** and click **Submit** in order to save it. The **Id Provider Name** is significant only for ISE as shown in the image.

External Identity Sources

- <  
- > Certificate Authentication F
- Active Directory
 - EXAMPLE
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST (ROPC)

Identity Provider List > New Identity Provider

SAML Identity Provider

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

* Id Provider Name	Azure_SAML
Description	Azure Active Directory

2. Configure Sponsor Portal to use Azure AD

Navigate to **Work Centers > Guest Access > Portals & Components > Sponsor Portals** and select your Sponsor Portal. In this example **Sponsor Portal (default)** is used.

Expand **Portal Settings** panel and select your new SAML IdP in the **Identity source sequence**. Configure the **Fully Qualified Domain Name (FQDN)** for the sponsor portal. In this example it is **sponsor30.example.com**. Click on **Save** as shown in the image.

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. Export Service Provider Information

Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]**.

Switch to tab **Service Provider Info**. and click the **Export** button as shown in the image.

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)

Download the zip file and save it. In it, you can find 2 files. You need the XML file called as your Sponsor Portal.

Make a note of **ResponseLocation** from **SingleLogoutService** Bindings, **entityID** value, and **Location** values from **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>
MIIFZjCCA06gAwIBAgIQXl0aVwAAAAChgVd9cEEW0zANBkgqhkiG9w0BAQwFADAlMSMwIQYDVQQD
ExpTQUlMX01lTRTMwLTFlay5leGFtcGxlLmNvbTAeFw0yMDA5MTAxMDMyMzFaFw0yNTA5MDkxMDMy
MzFaMCUxIzAhBgNVBAMTGlNBTUxfSVNFMzAtMWVrLmV4YW1wbGUuY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCGKCAgEAt+MixKfuZvg/oAWGEs6zrUYL3H2JwvZw9yJs6sJ8/BpP6Sw027wh
FXnESXpqqmnoSVrVcEQIrDdk3l8UYNn/+98PPkIi/4ftyFjZK9YdeverD6nrA2MeoLCzGlkWg/y4i
vvVcYuW344pySm65awVvro3q84x9esHqyLahExs9guiLJryD497XmNP4Z8eTHCctu777PuI1wL04
QOYUs2sozXvR98D9Jok/+PjH3bjmVKapqAcNEFvk8Ez9x1sMBUgFwP4YdZzQB9IRVkJdIJGvqMyf
a6gn+KaddJnmIbXKFbrTaFii2IvRs3qHJ0mMVfYRnYeMql9/PhzvSftjRe32x/aQh23j9dCsVXmQ
ZmXpZyxxJ8p4RqyM0YgkfxnQXXtV9K0sRZPFn60+iszUw2hARRG/te0hTuVXpbonG2dT109JeeEe
S1E5uxenJvYkU7mMamvBjYQN6qVvyogf8F0lHTSfd6TDsK3Qhmz0jg50PrBvvg5qE6OrxxNvqSVZ
ldhx/iHZAZlyYSVdwizsZMCw0PjSwrRPx/h8l03djeW0aL5R1AF1qTFHVHNSNvigzh6FyjdkUJH66
JAYgPe0PKJFRgYzh5vWoJ41qvDjLgk3c/zYi57MR1Bs0mkSvkOGbmjSsb+EehnYyLLB8FG3De2V
ZaXaHZ37gmoCNNmZHrn+GB0CAwEAAaOBkTCBjjAgBgNVHREEGTAXghVJU0UzMC0xZWsuZXhhbXBs
ZS5jb20wDAYDVDR0TBAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVDR0OBByEFPT/6jpfyugxRolbjzWJ
858wfTP1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjARBglghkgBhvhCAQEEBAMCBkAw
DQYJKoZIhvcNAQEMBQADggIBABGyWZbLaJm2LyLASg//4N6mL+Xu/9IMdVvNWBQodF+j0WusW15a
VPSQU2t3Ckd/I1anvpK+cp77NMjo9V9oWi3/ZnjZHGofAIChnLGCoeJmC1TvLau7ZzhCCII37DFA
yMKDrXLi3Pr+ONlXlTivjPHTTzrKmlNHhkxkx/Js5Iuz+MyRKP8FNmWT0q4XGejyKzJWrqEu+bc1
idC1/gBNuCHgqmFem82IGQ7jVomlkBjLb4pTDbYk4fMIbJVh4V2Pgi++6MIfXAYEWL+LHjSGHCQT
PSM3+kpvlwHHpGWzQSmcJ4tXVXV95W0NC+LxQZLBPNUMZorhuYCILXZxvXH1HGJJ0YKx91k9Ubd2
s5JaD+GN8jqm5XXAau7S4BawfvCo3bo0iXnSvGcIuh9YFiR2lp2n/2X0VVbdPHYZtqGieqBWebHr
4I1z18FXblYyMzpIkht00vkP5mAlR92VXBkvx2WPjtzQrvOtSXgvTCOKerYCBM/jnuwsztV7FVTV
JNdFwOsncXC70YngZeujZyJpUbfRKZI34VKZp4i05bZsG1bWE9Skdquv0PaQ8ecXTv80CVBYUeg1
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>
```

According to the XML file:

SingleLogoutService

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

entityID="<http://CiscoISE/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>"

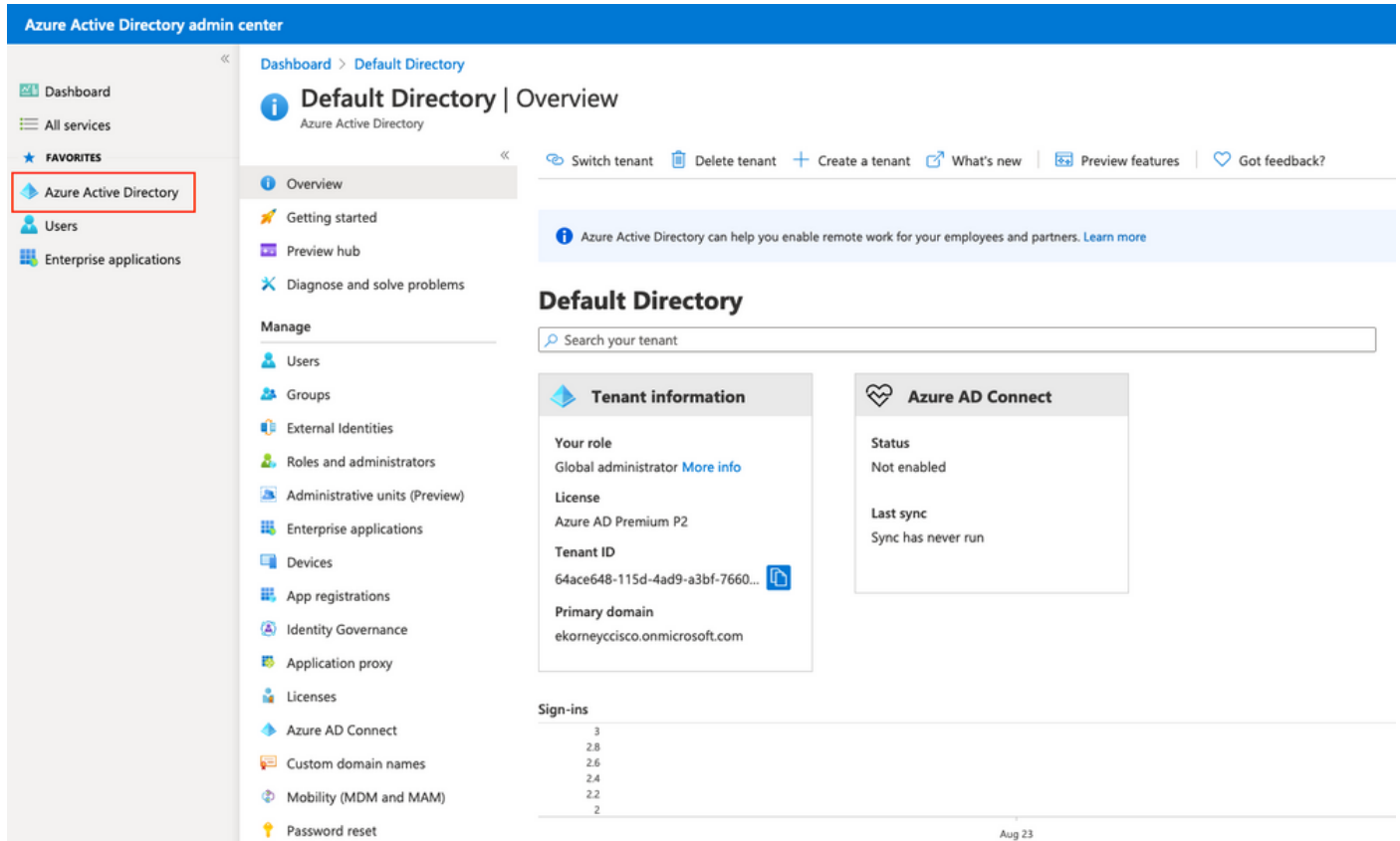
AssertionConsumerService Location="<https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action>"

AssertionConsumerService Location="

Step 2. Configure Azure AD IdP Settings

1. Create an Azure AD User

Login to Azure Active Directory Admin Center Dashboard and select your AD as shown in the image.



Select **Users**, click on **New User**, configure **User name**, **Name** and **Initial Password**. Click on **Create** as shown in the image.

Azure Active Directory admin center

Dashboard > Users >

New user

Default Directory

Got feedback?

Create user

Create a new user in your organization. This user will have a user name like `alice@ekorneyccisco.onmicrosoft.com`.
[I want to create users in bulk](#)

Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

User name * @ [The domain name I need isn't shown here](#)

Name *

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password *

2. Create an Azure AD Group

Select **Groups**. Click on **New Group** as shown in the image.

Dashboard > Default Directory > Groups

Groups | All groups

Default Directory - Azure Active Directory

[+ New group](#) [Download groups](#) [Delete](#) [Refresh](#) [Columns](#)

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

[Add filters](#)

Keep Group type as **Security**. Configure **Group name** as shown in the image.

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. Assign Azure AD User to the Group

Click on **No members selected**. Choose the user and click on **Select**. Click **Create** in order to create the group with a User assigned to it.

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

Make a note of **Group Object id**, in this screen, it is **f626733b-eb37-4cf2-b2a6-c2895fd5f4d3** for **Sponsor Group**.

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

Settings

- General
- Expiration
- Naming policy

4. Create an Azure AD Enterprise Application

Under AD, select **Enterprise Applications** and click on **New application** as shown in the image.

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.

Select the **Non-gallery application** as shown in the image.

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

Enter the name of your application and click on **Add**.

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Add your own application

Name * ⓘ

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. Add Group to the Application

Select **Assign users and groups**.

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

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 ⓘ

Application ID ⓘ

Object ID ⓘ

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](#)

Click on **Add user**.

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

ISE30 | Users and groups

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
- Properties
- Owners
- Users and groups

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

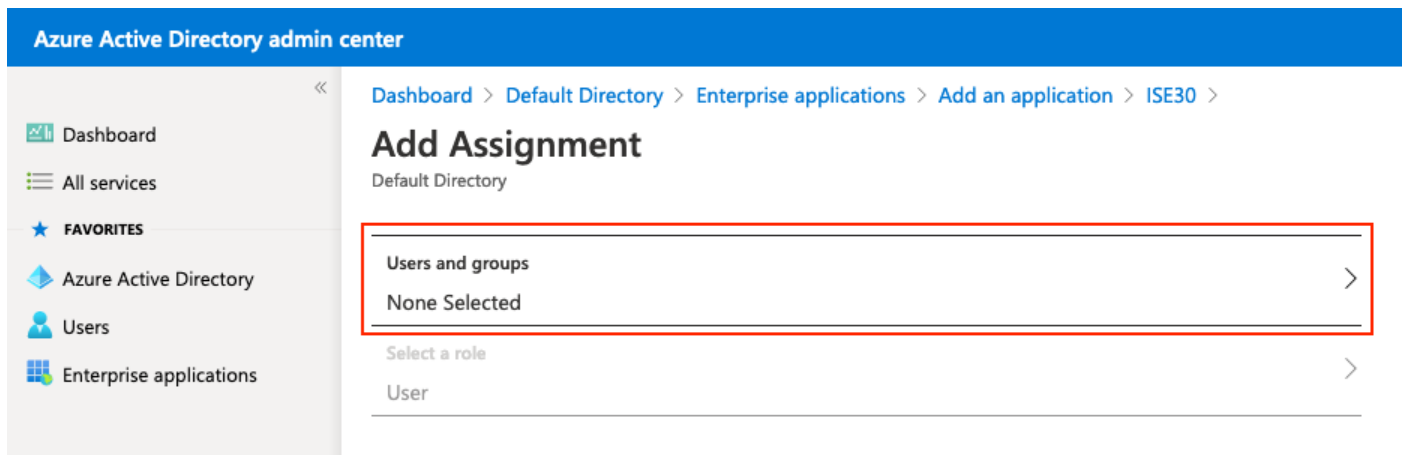
i The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

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

Display Name

No application assignments found

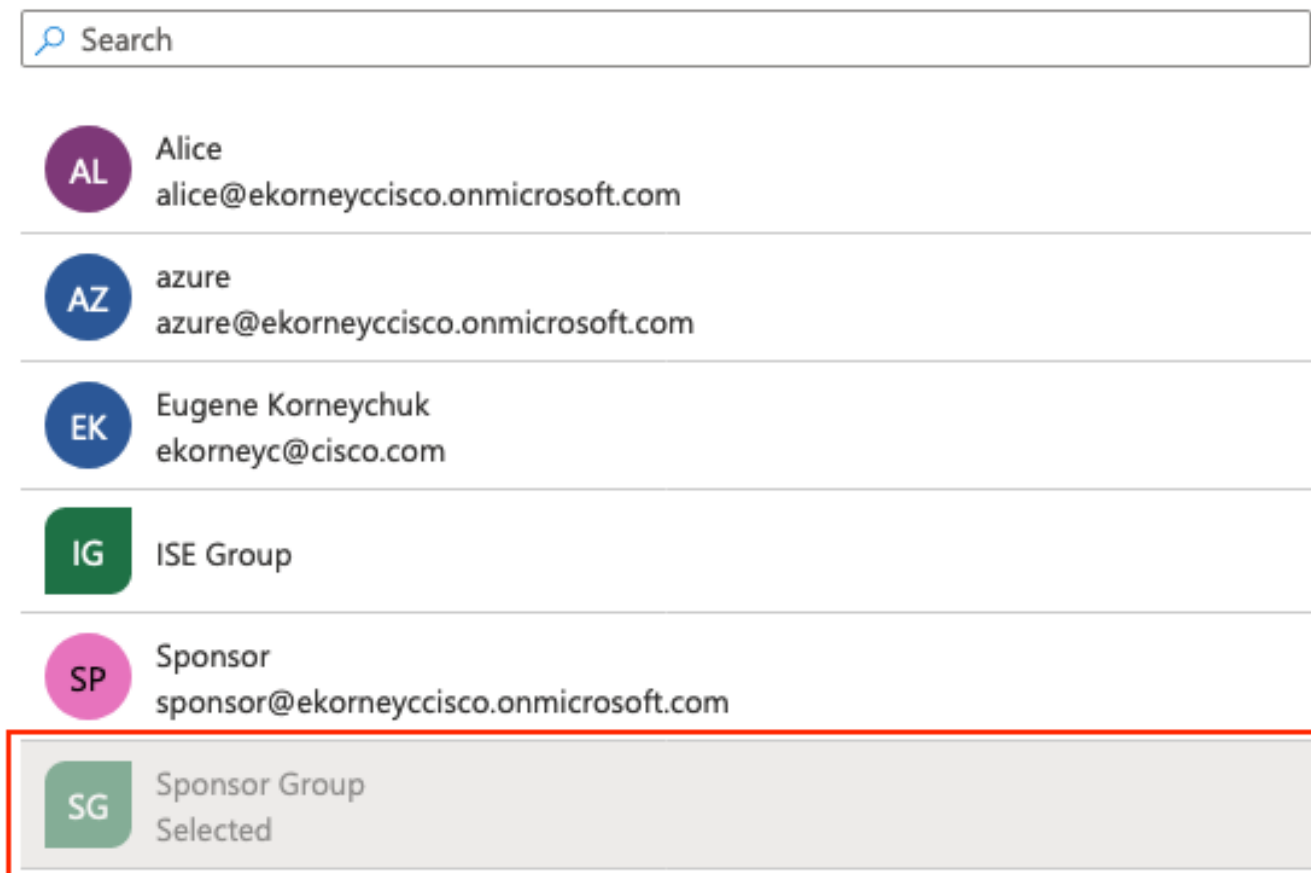
Click on **Users and groups**.



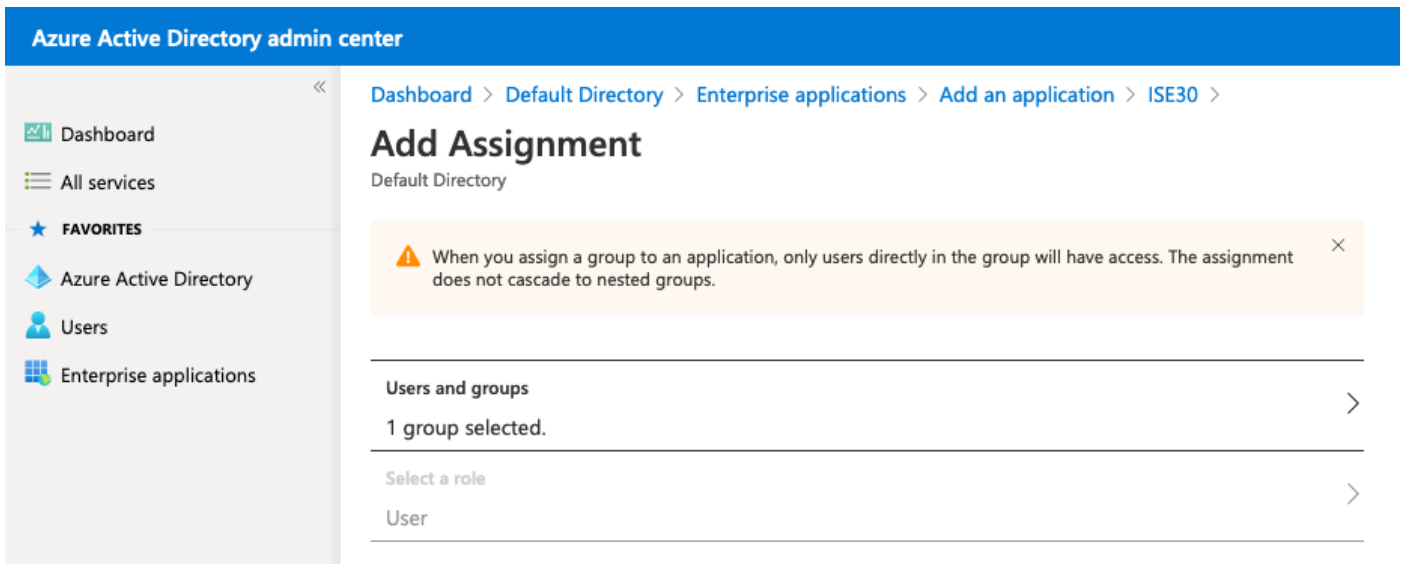
Choose the Group configured previously and click on **Select**.

Note: It is up to you to select the right set of users or groups which should get access.

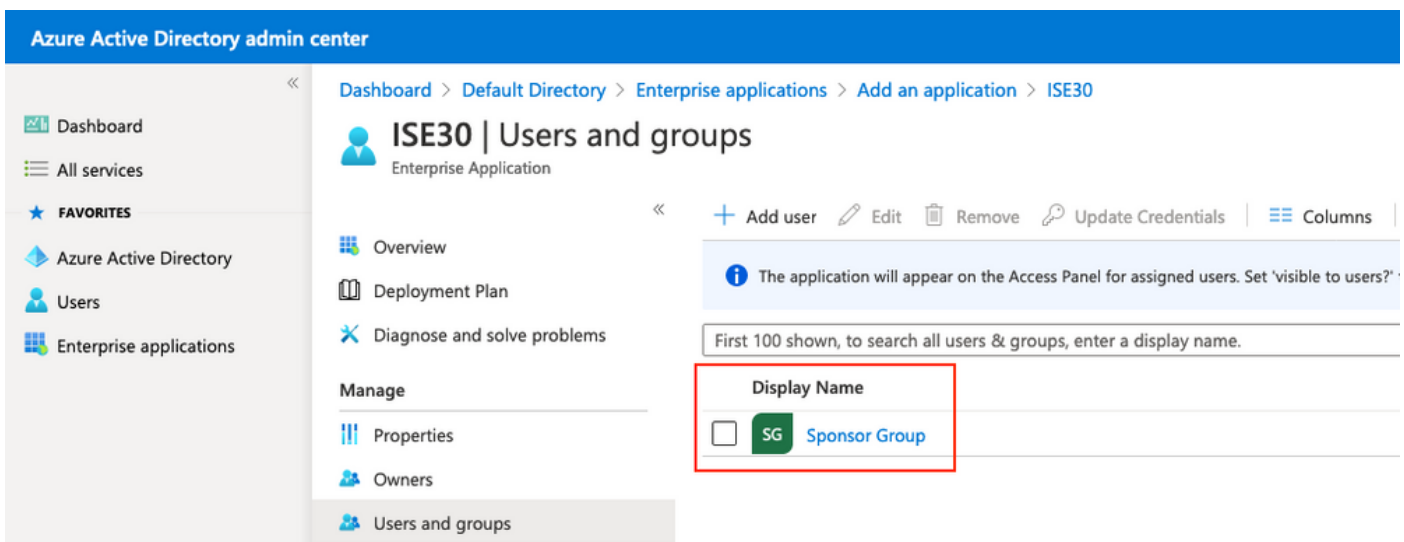
Users and groups



Once the Group is selected, click on **Assign** as shown in the image.



As a result, the **Users and groups** Menu for your application should be populated with the selected Group.



6. Configure an Azure AD Enterprise Application

Navigate back to your Application and click on **Set up single sign-on** as shown in the image.

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](#)

Select **SAML** on the next screen.


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.

Click on **Edit** next to **Basic SAML Configuration**.

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

Populate Identifier (Entity ID) with the value of **entityID** from the XML file from step **Export Service Provider Information**. Populate **Reply URL (Assertion Consumer Service URL)** with the value of **Locations** from **AssertionConsumerService**. Populate **Logout Url** value with **ResponseLocation** from **SingleLogoutService**. Click on **Save**.

Note: Reply URL acts as a pass list, which allows certain URLs to act as a source when redirected to the IdP page.

Basic SAML Configuration



Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

<input type="text" value="http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429"/>	<input checked="" type="checkbox"/> Default	
<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 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. Configure Active Directory Group Attribute

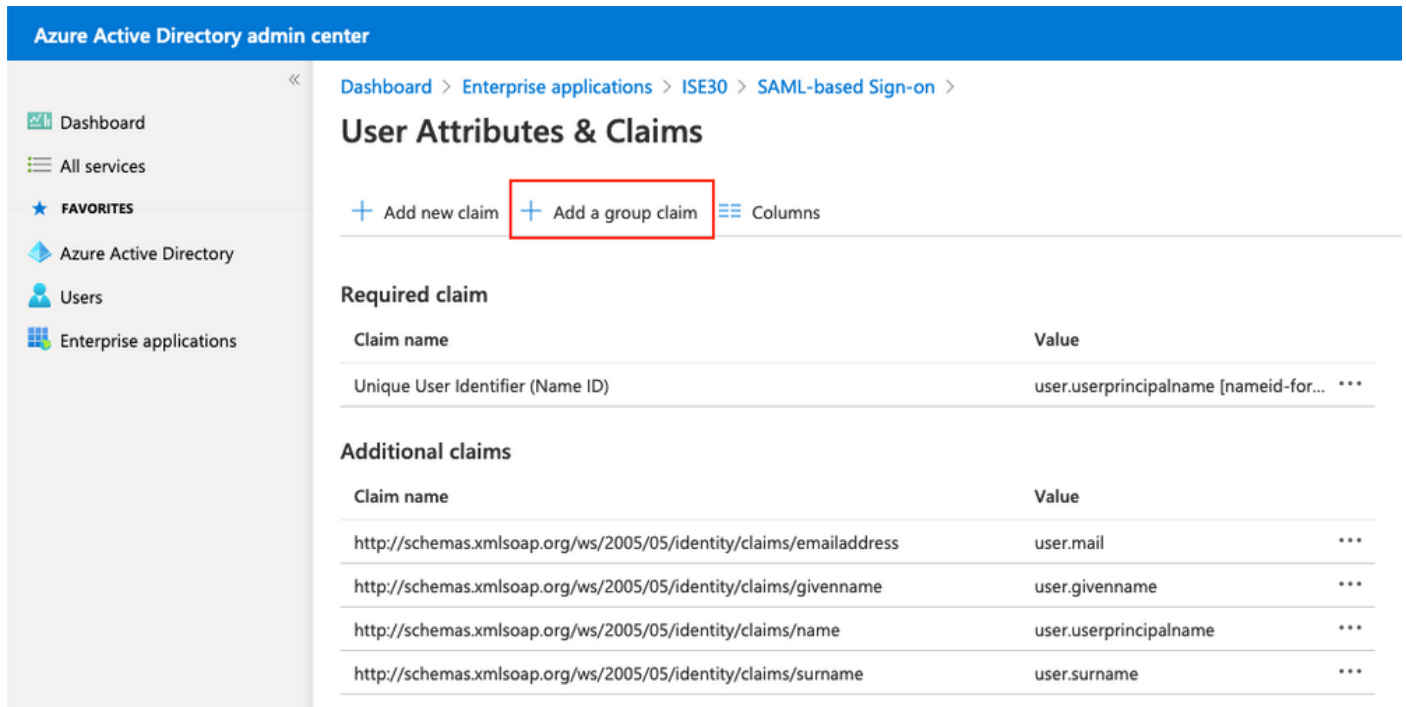
In order to return group attribute value configured previously, click on **Edit** next to the **User Attributes & Claims**.

User Attributes & Claims



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

Click on **Add a group claim**.



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 ***

Select **Security groups** and click on **Save**. **Source attribute** returned in assertion is a **group ID**, which is a **Group Object id** captured earlier.

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

Make a note of **Claim name** for the group. In this case, it is <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups>.

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area is titled 'User Attributes & Claims' and includes options to 'Add new claim', 'Add a group claim', and 'Columns'. It displays two tables: 'Required claim' and 'Additional claims'. The 'Additional claims' table has a red box highlighting the first row.

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

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. Download Azure Federation Metadata XML File

Click on **Download** against **Federation Metadata XML** in **SAML Signing Certificate**.

SAML Signing Certificate

 Edit

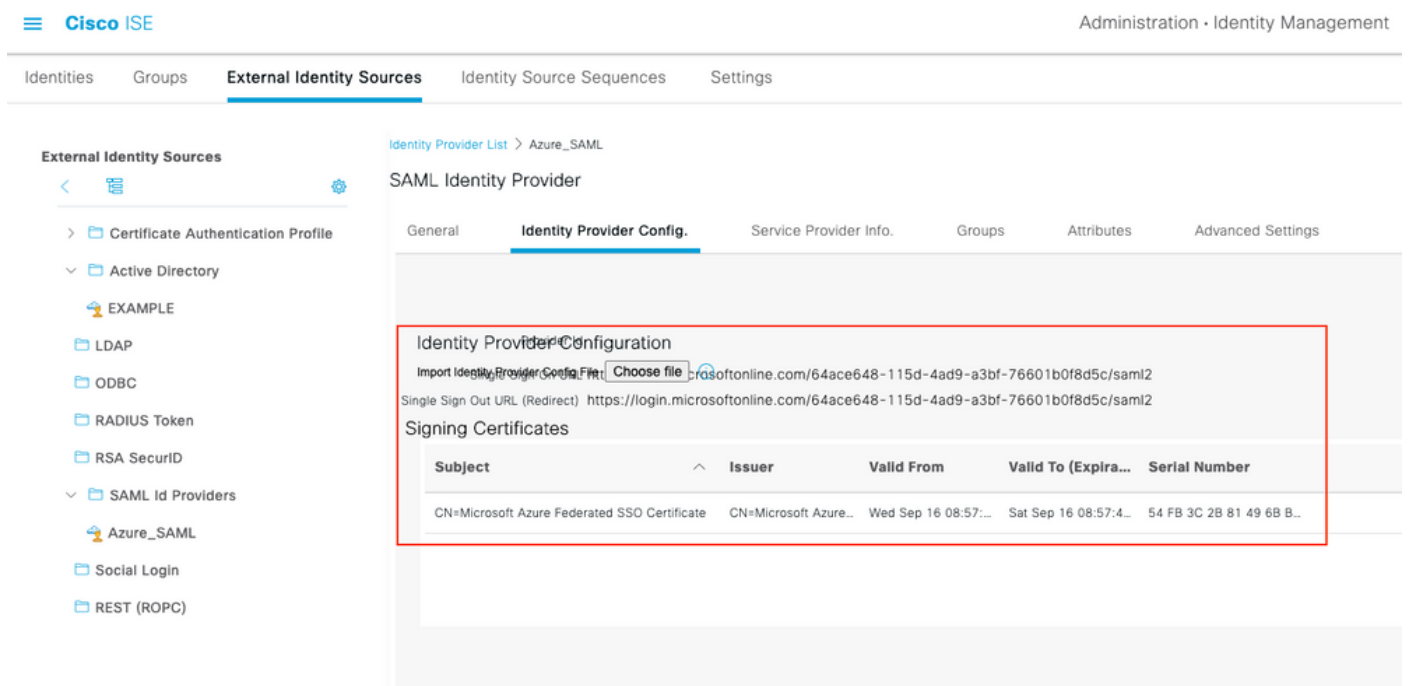
Status	Active
Thumbprint	9772DA460A43ACDA2AC5FBF09EE33ED7DAA7BAE2
Expiration	9/16/2023, 10:57:46 AM
Notification Email	ekorneyc@cisco.com
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/64ace648-115d ..."/>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Step 3. Upload MetaData from Azure Active Directory to ISE

Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]**.

Switch to tab **Identity Provider Config.** and click the **Browse** button. Select Federation Metadata XML file from step **Download Azure Federation Metadata XML** and click **Save**.

Note: UI glitch with Identity Provider Configuration should be addressed under [CSCvv74517](#).

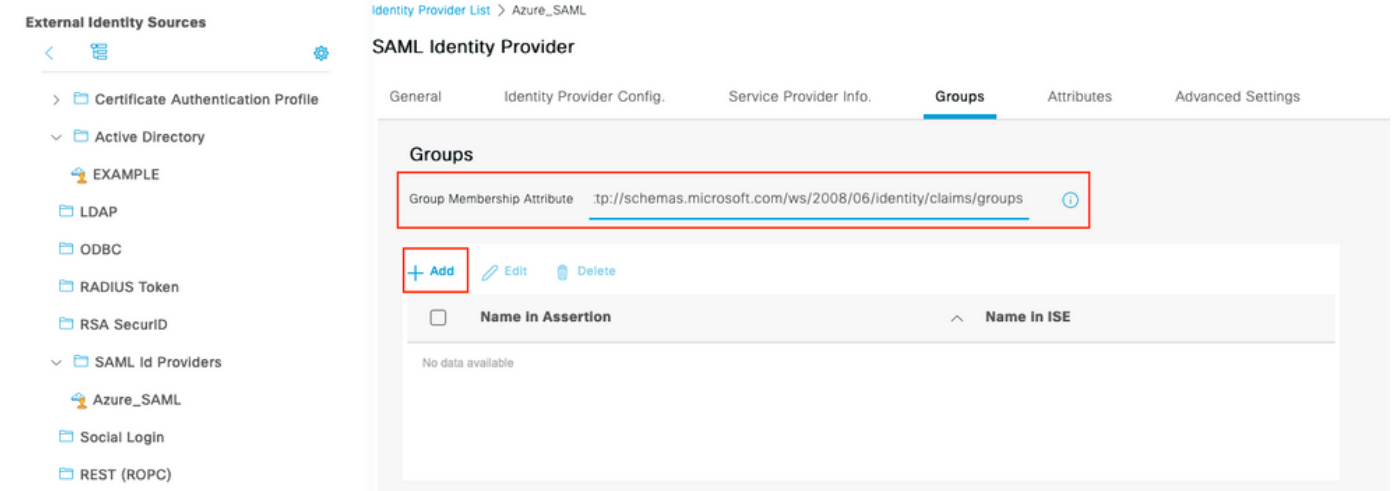


The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > Identity Management > External Identity Sources > SAML Identity Provider List > Azure_SAML. The main content area is titled 'SAML Identity Provider' and has tabs for General, Identity Provider Config. (selected), Service Provider Info., Groups, Attributes, and Advanced Settings. The 'Identity Provider Config.' tab is active, showing the 'Import Identity Provider Configuration File' button with a 'Choose file' dropdown. Below this, the 'Single Sign Out URL (Redirect)' is set to 'https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2'. The 'Signing Certificates' section contains a table with one entry:

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 6B B...

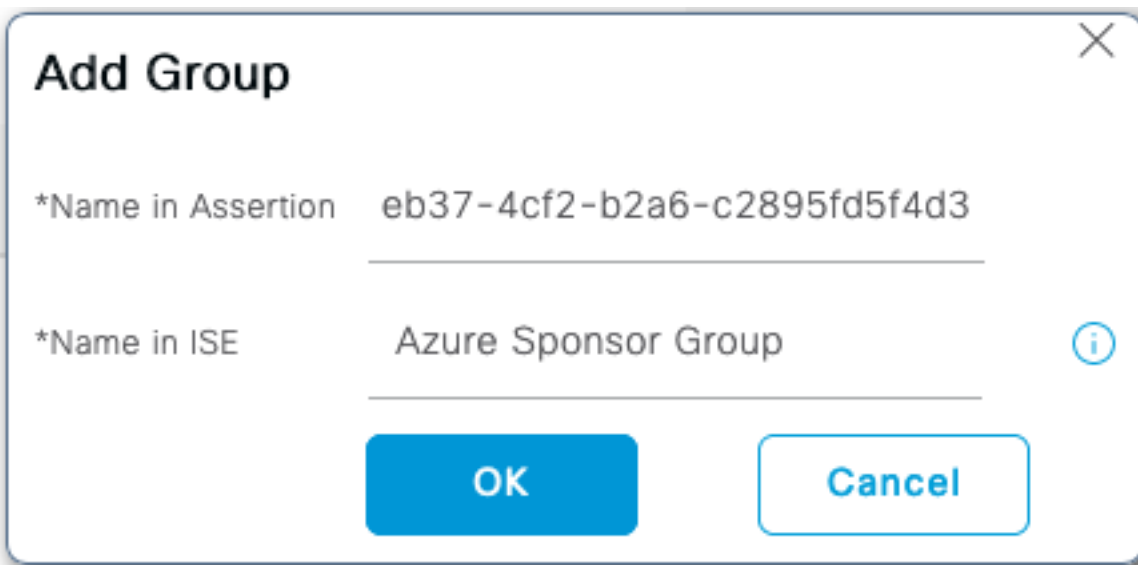
Step 4. Configure SAML Groups on ISE

Switch to tab **Groups** and paste the value of **Claim name** from **Configure Active Directory Group attribute** into **Group Membership Attribute**.



Click on **Add**. Populate **Name in Assertion** with the value of **Group Object id** of **Sponsor Group** captured in **Assign Azure Active Directory User to the Group**. Configure **Name in ISE** with the meaningful value in this case it is **Azure Sponsor Group**. Click **OK**. Click on **Save**.

This creates a mapping between Group in Azure and Group name which can be used on ISE.



Step 5. Configure Sponsor Group Mapping on ISE

Navigate to **Work Centers > Guest Access > Portals & Components > Sponsor Groups** and select **Sponsor Group** you would like to map to the **Azure AD Group**. In this example, ALL_ACCOUNTS (default) was used.

- 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
<input checked="" type="checkbox"/>	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)
<input checked="" type="checkbox"/>	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)
<input checked="" type="checkbox"/>	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)

Click on **Members...** and add **Azure_SAML:Azure Sponsor Group** to **Selected User Groups**. This maps the **Sponsor Group** in Azure to **ALL_ACCOUNTS** Sponsor Group. Click on **OK**. Click on **Save**.



Select Sponsor Group Members

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

Available User Groups

Name ^

Employee

GROUP_ACCOUNTS (default)

OWN_ACCOUNTS (default)

Selected User Groups

Name ^

ALL_ACCOUNTS (default)

Azure_SAML:Azure Sponsor Group

Verify

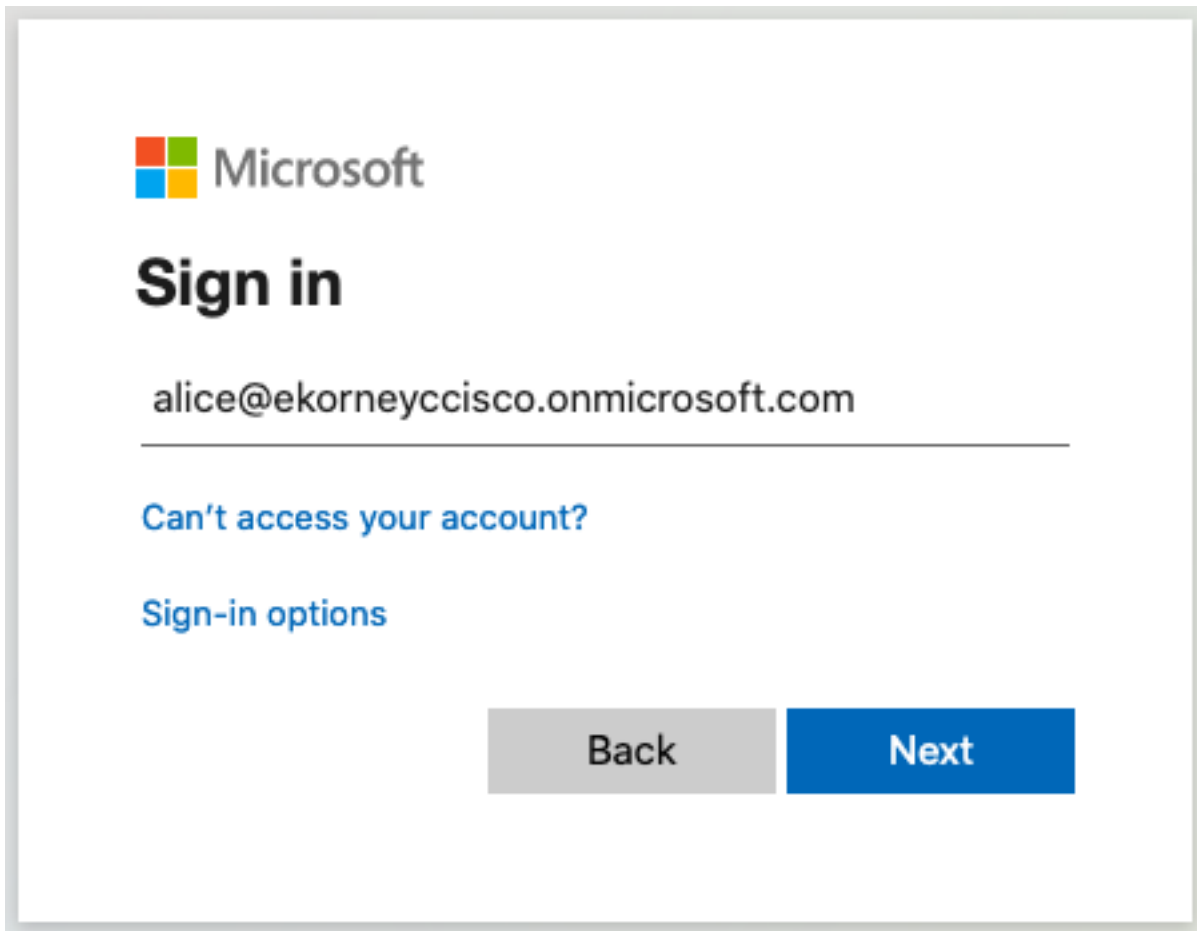
Use this section to confirm that your configuration works properly.

Note: New user is forced to change user password upon the first login. And accept the AUP Verification steps do not cover it. Verification covers the scenario, where users log in not for the first time, and AUP was already accepted once by the Sponsor (alice).

Now if you open the Sponsor Portal (from Test URL, for example) you are redirected to Azure to

sign in and then back to the Sponsor Portal.

1. Launch the Sponsor Portal with its FQDN on the Portal Test URL link. ISE should redirect you to Azure Sign In page. Enter the **username** create earlier and click **Next**.



Microsoft

Sign in

alice@ekorneyccisco.onmicrosoft.com

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

[Sign-in options](#)

[Back](#) [Next](#)

2. Enter the **password** and click **Sign In**. IdP login screen redirects the user to the initial ISE's Sponsor Portal.



← alice@ekorneyccisco.onmicrosoft.com

Enter password

.....|

[Forgot my password](#)

Sign in

3. Accept the AUP.



Sponsor Portal

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. At this point, the Sponsor User should have full access to the portal with **ALL_ACCOUNTS** Sponsor Group permissions.

[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



Duration:* Days (Maximum:365)

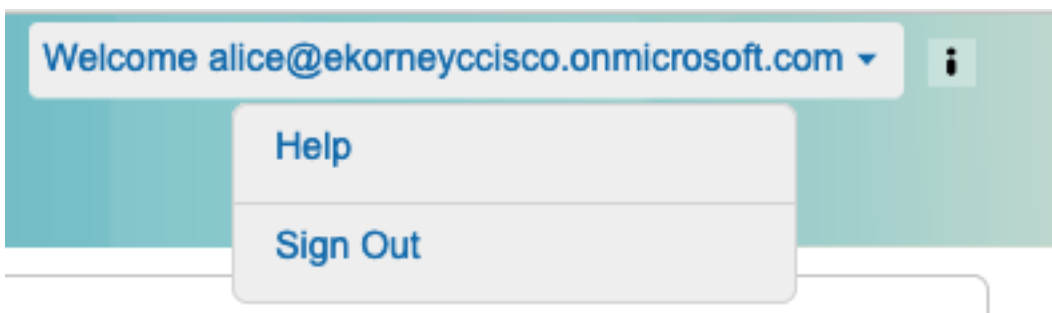
From Date (yyyy-mm-dd) *  From Time * 

To Date (yyyy-mm-dd) *  To Time * 

[Create](#)

[Help](#)

5. Click on **Sign Out** under the Welcome drop-down menu.



6. User should be successfully logged out and redirected to the login screen again.



Pick an account



alice@ekorneyccisco.onmicrosoft.co
m



Use another account

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Common Issues

It is vital to understand that SAML authentication is handled between the browser and the Azure Active Directory. Hence, you can get authentication-related errors directly from the Identity Provider (Azure) where ISE engagement has not started yet.

Issue 1. The user enters the wrong password, no processing of user data was done on ISE, the issue is coming directly from IdP (Azure). In order to fix: Reset the password or provide the right password data.



← 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

Issue 2. The user is not part of the group which supposed to be allowed to access SAML SSO, again in this case no processing of user data was done on ISE, issue comes directly from IdP (Azure). In order to fix: Verify that the **Add group to the Application** configuration step is correctly executed.



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. Sing Out does not work as expected, this error is seen - "SSO Logout failed. There was a problem to logout from your SSO session. Please contact help desk for assistance." It can be seen when Sign Out URL is not correctly configured on SAML IdP. In that case, this URL was used

"<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2>" while it should be

"<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action>" In order to fix: enter correct URL in Logout URL in Azure IdP.

1. User is redirected to IdP URL from Sponsor portal.

```
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 -::::- SPProviderId 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. SAML response is received from the browser.

```
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. Attribute (assertion) parsing is started.

```
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. Group attribute is received with the value of **f626733b-eb37-4cf2-b2a6-c2895fd5f4d3**, signing validation.

```
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 -::::- SAMLUtills::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 -::::- SAMLUtills::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 -::::- SAMLUtills::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 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 -:::- 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. User group is added to authentication results so it can be used by Portal, SAML authentication is passed.

```

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. Sign Out is triggered. LogOut URL is received in SAML

Response; <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:-
buildLgoutRequest - 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:-
buildLgoutRequest - 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:-
buildLgoutRequest - 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 successfully 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 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 -:::- SPPProviderId for Azure_SAML is:
http://CiscoISE/bd48clal-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