

# 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 ISE 3.0 to provide SSO capabilities for Sponsor users.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Services Engine (ISE) 3.0

- Basic knowledge about Security Assertion Markup Language (SAML) Single Sign-On (SSO) deployments
- Azure AD

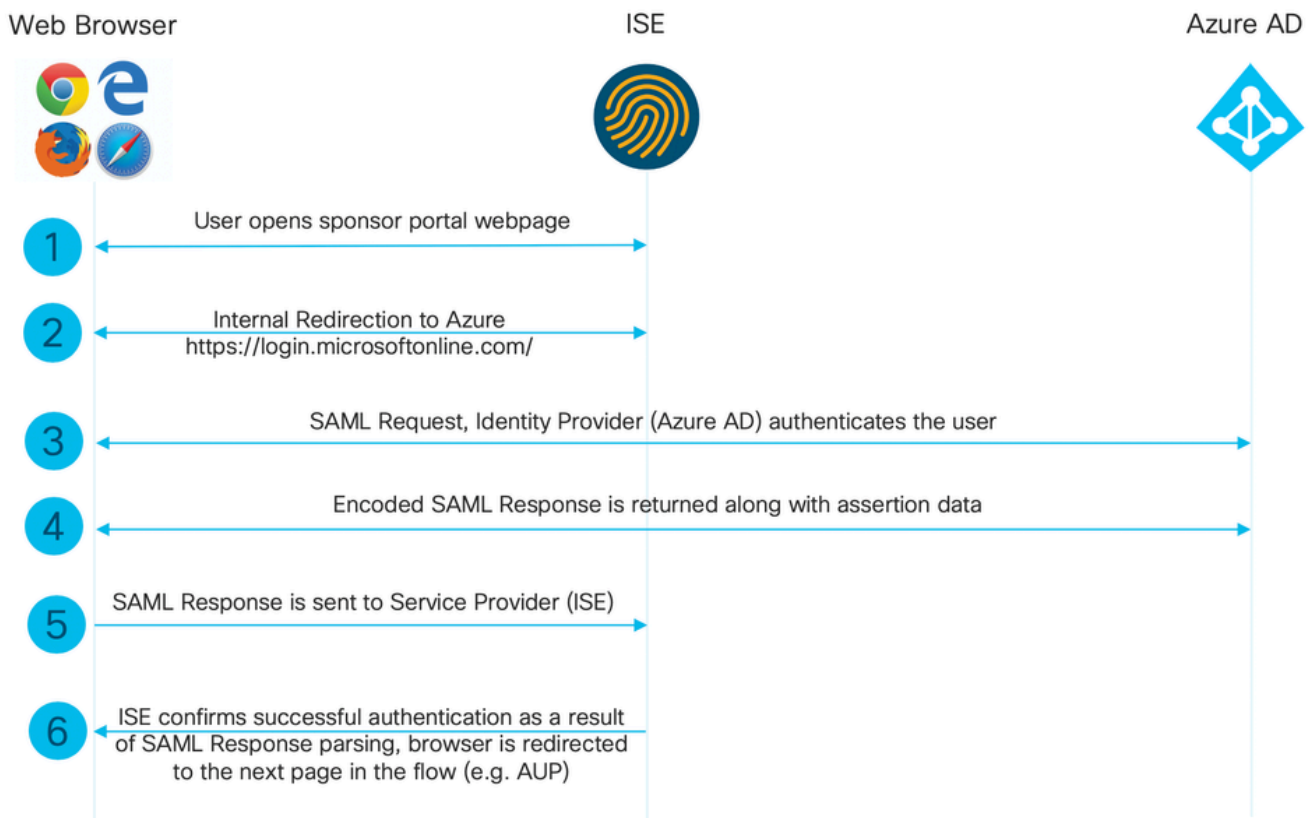
## Components Used

The information in this document is based on these hardware and software versions:

- Cisco ISE 3.0
- 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 &gt; 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 Identity Provider (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 **Save** as shown in the image:

Cisco ISE

Work Centers · Guest Access

OverviewIdentitiesIdentity GroupsExt Id SourcesAdministrationNetwork DevicesPortals & ComponentsManage AccountsPolicy ElementsPolicy Sets

Guest PortalsGuest TypesSponsor GroupsSponsor Portals

Portal Name: \*Sponsor Portal (default)Description: \*Default portal used by sponsors to create a session.  
Language File  
Portal test URL

Portal Behavior and Flow SettingsPortal Page Customization

Portal & Page Settings

▼ Portal Settings

HTTPS port: \*8445  
Allowed interfaces: \*

If bonding is not configured on a PSN, use:

☒ Gigabit Ethernet 0

☐ Gigabit Ethernet 1

☐ Gigabit Ethernet 2

☐ Gigabit Ethernet 3

☐ Gigabit Ethernet 4

☐ Gigabit Ethernet 5

If bonding is configured on a PSN, use:

☒ Bond 0  
Uses Gigabit Ethernet 0 as primary, 1 as backup.

☐ Bond 1  
Uses Gigabit Ethernet 2 as primary, 3 as backup.

☐ Bond 2  
Uses Gigabit Ethernet 4 as primary, 5 as backup.

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                                                                                                        |                           |                        |        |            |                   |
| <input type="checkbox"/> Load balancer <span style="float: right;">?</span>                                                         |                           |                        |        |            |                   |
| Export Service Provider Info. <span style="border: 2px solid red; padding: 2px;">Export</span> <span style="float: right;">?</span> |                           |                        |        |            |                   |
| 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
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration=
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFZjCCA06gAwIBAgIQX1oAvwAAAAChgVd9cEEW0zANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQD
ExpTQU1MX01TRTMwLTFlay5leGFtcGx1LmNvbTAeFw0yMDA5MTAxMDMyMzFaFw0yNTA5MDkxMDMy
MzFaMCUxIzAhBgNVBAMTG1NBtUXfSVNFMzAtMWVrLmV4YW1wbGUuY29tMIICiANBgkqhkiG9w0B
AQEFAAOCAg8AMIICGKCAgEAt+MixKfuZvg/oAWGES6zrUYL3H2JwvZw9yJs6sJ8/BpP6Sw027wh
FXnESXpqmmoSVrVEcQIRdDk3l8UYNn/+98PPKiI/4ftyFjZK9YdeverD6nrA2MeoLCzG1kWq/y4i
vvVcYuW344pySm65awVvro3q84x9esHqyLahExs9guiLJryD497XmNP4Z8eTHCctu777PuI1wL04
QOYUs2sozXvR98D9Jok/+PjH3bjmVKapqAcNEFvk8Ez9x1sMBUgFwP4YdZzQB9IRVkJdIJGvqMyf
a6gn+KaddJnmIbXKFbrTaFiI2IvRs3qHJ0mMVfYRnYeMq19/PhzvSFtjRe32x/aQh23j9dCsVXmQ
ZmXpZyxxJ8p4RqyM0YgkfxnQXXtV9K0sRZPFn60+iszUw2hARRG/tE0hTuVXpbonG2dT109JeeEe
S1E5uxenJvYkU7mMamvBjYQN6qVyyogf8F0lHTSfd6TDsK3Qhmz0jg50PrBvvg5qE60rxxNvqSVZ
1dhx/iHZAZ1yYSVdwizsZMCw0PjSwrRPx/h8l03djeW0aL5R1AF1qTFHVHNSvighz6FyjdkUJH66
JAygPeOPKJFRgYzh5vWoJ41qvDQj1Gk3c/zYi57MR1Bs0mkSvkOGbmjSsb+EehnYyLLB8FG3De2V
ZaXaHZ37gmoCNNmZHRn+GB0CAwEAAaOBkTCBjjAgBgNVHREETAXghVJU0UzMC0xZWsuZXhhbXBs
ZS5jb20wDAYDVROTBAAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVRO0BBYEFPT/6jpfyugxRo1bjzWJ
858WFTP1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjARBglghkgBhvhCAQEEBAMCBkAw
DQYJKoZIhvcNAQEMBQADggIBABGyWZbLajm2LyLASg//4N6mL+Xu/9IMdVvNWBQodF+j0WusW15a
VPSQU2t3Ckd/I1anvpK+cp77NMjo9V9oWI3/ZnjZHGofAICn1GCoEjmC1TvLau7ZzhCCII37DFA
yMKDrXLi3pR+ON1X1TivjpHTTzrKm1NHhkxkx/Js5Iuz+MyRKP8FnmWT0q4XGejyKzJWrqEu+bc1
idC1/gBNUCHgqmFeM82IGQ7jV0m1kBjLb4pTDbYk4fMIbJVh4V2Pgi++6MIfXAYEWL+LHjSGHCQT
PSM3+gvpv1wHHpGWzQSmcJ4tXVXV95W0NC+LxQZLBPNMUZorhuYCILXxvXH1HGJJ0YKx9lK9Ubd2
s5JaD+GN8jqm5XXAAu7S4BawfvCo3bo0iXnSvGcIuH9YFiR2lp2n/2X0VVbdPHYZtqGieqBWebHr
4I1z18FXb1YyMzpIkht00vkP5mA1R92VXBkvx2WPjtzQrv0tSXgvTCOKerYCBM/jnuwsztV7FVTV
JNdFwOsnXC70YngZeujZyJpUbfRkZI34VKZp4i05bZsG1bWE9Skdquv0PaQ8ecXTv80CVBYUeg1
vt0pde18h/9jImdLG8dF0rbADGHiieTcntSDdw3E7JFmS/oHw7FsA5GI8IxXfcOWUx/L0Dx3jTnd
Z1AXp4juysODIx9yDyM4yV0f
</ds:X509Certificate>
</ds:X509Data>
```

```

</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://
<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://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://

</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**="<https://ise30-3ek.example.com:8445/sponsorportal/SSOLoginResponse.action>"

## Step 2. Configure Azure AD IdP Settings

### 1. Create an Azure AD User

Log in to **Azure Active Directory Admin Center Dashboard** and select your **AD** as shown in the image:

Azure Active Directory admin center

Dashboard > Default Directory

## Default Directory | Overview

Azure Active Directory

Switch tenant | Delete tenant | Create a tenant | What's new | Preview features | Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

### Default Directory

Search your tenant

#### Tenant information

**Your role**  
Global administrator [More info](#)

**License**  
Azure AD Premium P2

**Tenant ID**  
64ace648-115d-4ad9-a3bf-7660...

**Primary domain**  
ekorneyccisco.onmicrosoft.com

#### Azure AD Connect

**Status**  
Not enabled

**Last sync**  
Sync has never run

#### Sign-ins

|     |
|-----|
| 3   |
| 2.8 |
| 2.6 |
| 2.4 |
| 2.2 |
| 2   |

Aug 23

Select **Users**, click **New User**, configure **User name**, **Name** and **Initial Password**. Click **Create** as shown in the image for this test user:

**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 **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 →

Search groups Add filters

All groups

Deleted groups

Diagnose and solve problems

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



Azure Active Directory admin center

Dashboard

All services

FAVORITES

Azure Active Directory

Users

Enterprise applications

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 **No members selected**. Choose the user and click **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 the Sponsor Group.

Dashboard > Default Directory > Groups

## 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 **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 **Add**.

Azure Active Directory admin center

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

## 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. Add Group to the Application

Select **Assign users and groups**.

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](#)

Click **Add user**.

Azure Active Directory admin center

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

### ISE30 | Users and groups

Enterprise Application

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

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 |

Manage

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

Click **Users and groups**.

Azure Active Directory admin center

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

## Add Assignment

Default Directory

Users and groups

None Selected

Select a role

User

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



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

# Users and groups



Search

AL

Alice  
alice@ekorneyccisco.onmicrosoft.com

AZ

azure  
azure@ekorneyccisco.onmicrosoft.com

EK

Eugene Korneychuk  
ekorneyc@cisco.com

IG

ISE Group

SP

Sponsor  
sponsor@ekorneyccisco.onmicrosoft.com

SG

Sponsor Group  
Selected

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

Azure Active Directory admin center

Dashboard

All services

FAVORITES

Azure Active Directory

Users

Enterprise applications

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

## Add Assignment

Default Directory

When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

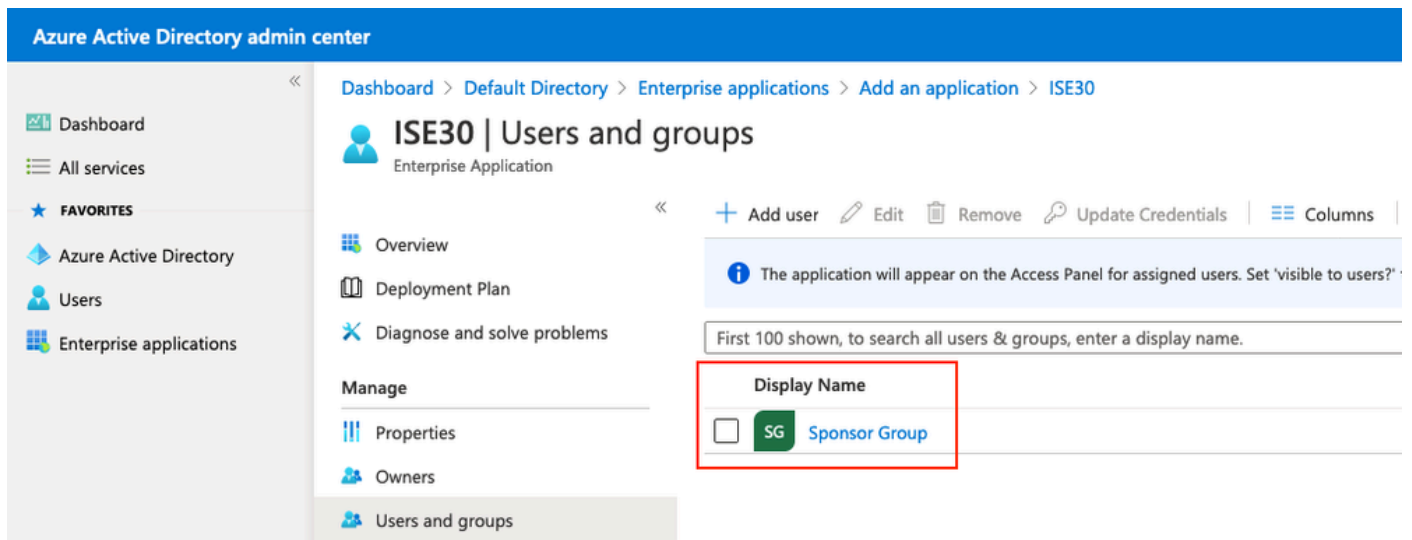
Users and groups

1 group selected.

Select a role

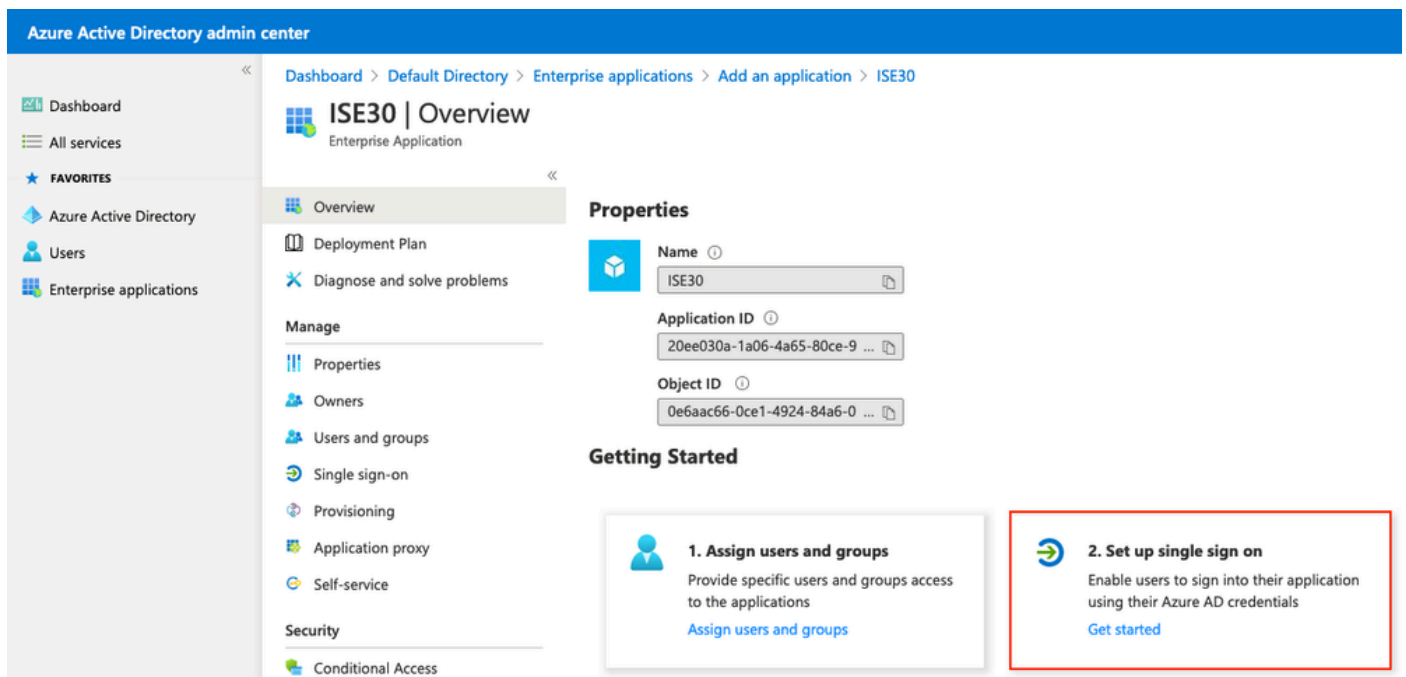
User

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



## 6. Configure an Azure AD Enterprise Application

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



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.

Manage

- Overview
- Deployment Plan
- Diagnose and solve problems
- Properties
- Owners
- Users and groups
- Single sign-on

Click **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** [Edit](#)

|                                            |                 |
|--------------------------------------------|-----------------|
| Identifier (Entity ID)                     | <b>Required</b> |
| Reply URL (Assertion Consumer Service URL) | <b>Required</b> |
| Sign on URL                                | Optional        |
| Relay State                                | Optional        |
| Logout Url                                 | Optional        |
- User Attributes & Claims** [Edit](#)

|                        |                        |
|------------------------|------------------------|
| givenname              | user.givenname         |
| surname                | user.surname           |
| emailaddress           | user.mail              |
| name                   | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |
- SAML Signing Certificate** [Edit](#)

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

Manage

- Overview
- Deployment Plan
- Diagnose and solve problems
- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs
- Provisioning logs (Preview)
- Access reviews

Troubleshooting + Support

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 the **Logout Url** value with **ResponseLocation** from **SingleLogoutService**. Click **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

|                                                                                   | 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 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 **Edit** next to the **User Attributes & Claims**.

## User Attributes & Claims

 Edit

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

Click **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 **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



Additionally provide the group name under the Advanced options

☒ Customize the name of the group claim

Name (required)

Sponsor Group



Namespace (optional)

- ☐ Emit groups as role claims ⓘ
- ☐ Apply regex replace to groups claim content
- ☐ Expose claim in JWT tokens in addition to SAML tokens

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

**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.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 **Download** against **Federation Metadata XML** in **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 | <a href="https://login.microsoftonline.com/64ace648-115d ...">https://login.microsoftonline.com/64ace648-115d ...</a> |
| Certificate (Base64)        | <a href="#">Download</a>                                                                                              |
| Certificate (Raw)           | <a href="#">Download</a>                                                                                              |
| Federation Metadata XML     | <a href="#">Download</a>                                                                                              |

## 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**, then 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 must be addressed under Cisco bug ID [CSCvv74517](#).

Cisco ISE

Administration • Identity Management

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

External Identity Sources

<Icon>Icon

Identity Provider List > Azure\_SAML

SAML Identity Provider

GeneralIdentity Provider Config.Service Provider Info.GroupsAttributesAdvanced Settings

Identity Provider Configuration

Import Identity Provider Configuration FileChoose file

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... |

## 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**.

Cisco ISE

Administration • Identity Management

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

External Identity Sources

<Icon>Icon

Identity Provider List > Azure\_SAML

SAML Identity Provider

GeneralIdentity Provider Config.Service Provider Info.GroupsAttributesAdvanced Settings

Groups

Group Membership Attributehttps://schemas.microsoft.com/ws/2008/06/identity/claims/groups

+ AddEditDelete

☐Name in Assertion

^Name in ISE

No data available

Click **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 **Save**.

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

×

# Add Group

\*Name in Assertion

eb37-4cf2-b2a6-c2895fd5f4d3

\*Name in ISE

Azure Sponsor Group

i

OK

Cancel

## 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:

Cisco ISE

Work Centers - Guest Access

OverviewIdentitiesIdentity GroupsExt Id SourcesAdministrationNetwork DevicesPortals & ComponentsManage AccountsPolicy ElementsPolicy SetsReportsCustom Portal Files

Guest PortalsGuest TypesSponsor GroupsSponsor 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) ⓘ

CreateEditDuplicateDelete

| Enabled                             | Name                                                                                                                                                                                                                                                                  | Member Groups            |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> | ALL_ACCOUNTS (default)<br>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<br><a href="#">More</a>                                                     | ALL_ACCOUNTS (default)   |
| <input checked="" type="checkbox"/> | GROUP_ACCOUNTS (default)<br>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<br><a href="#">More</a> | GROUP_ACCOUNTS (default) |
| <input checked="" type="checkbox"/> | OWN_ACCOUNTS (default)<br>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<br><a href="#">More</a>                              | OWN_ACCOUNTS (default)   |

Click **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 **OK**. Click **Save**.



# Select Sponsor Group Members

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

Available User Groups

Search

Name

^

Employee

GROUP\_ACCOUNTS (default)

OWN\_ACCOUNTS (default)

>

>>

<

<<

Selected User Groups

Search

Name

^

ALL\_ACCOUNTS (default)

Azure\_SAML:Azure Sponsor Group

OK

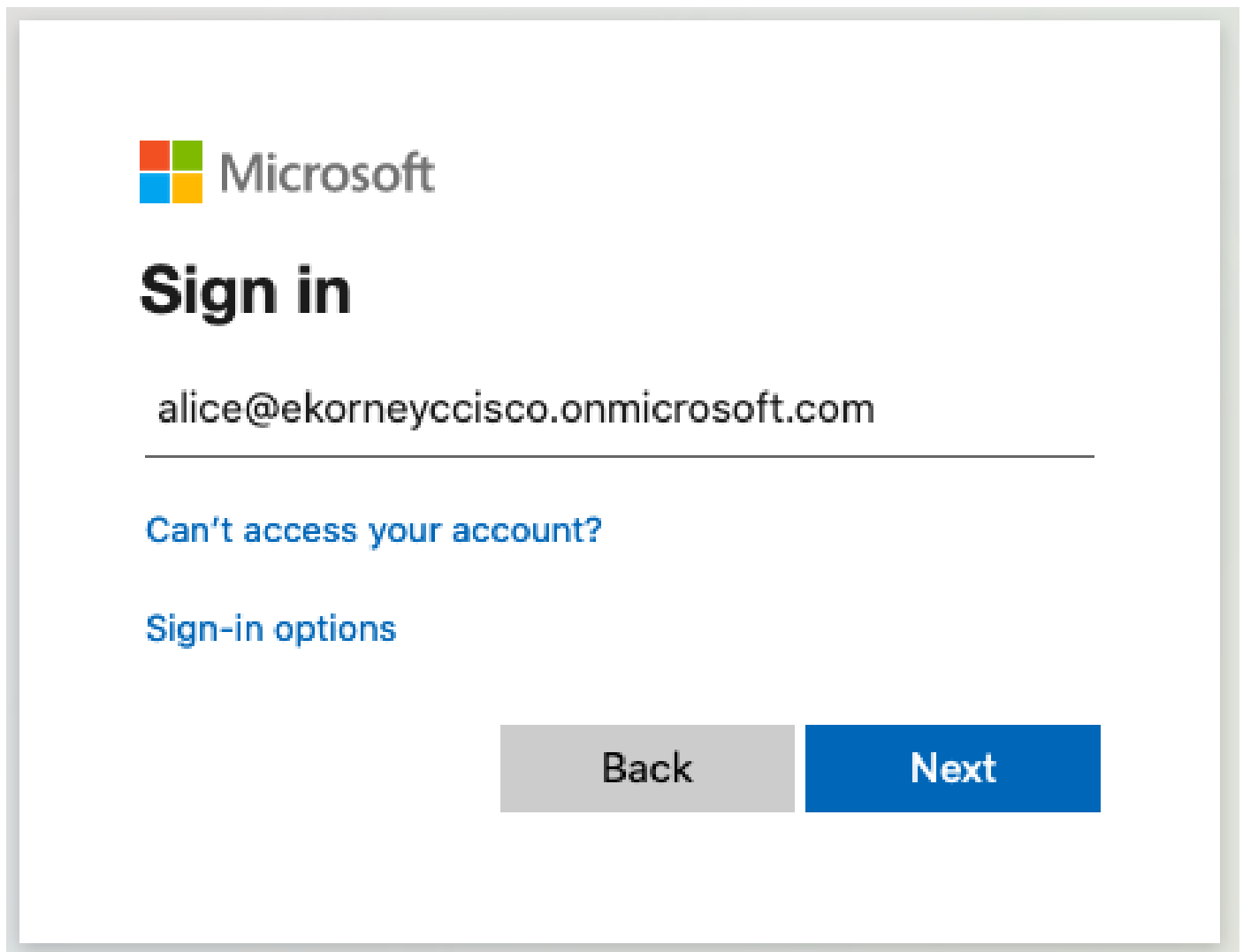
## Verify

Use this section to confirm that your configuration works properly.

 **Note:** The new user is forced to change user password upon the first login. And **Accept the AUP Verification steps** does 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 must redirect you to Azure Sign In page. Enter the **username** create earlier and click **Next**.

A screenshot of the Microsoft Sign in page. At the top left is the Microsoft logo. Below it, the word "Sign in" is displayed in a large, bold, black font. Underneath, the email address "alice@ekorneyccisco.onmicrosoft.com" is entered into a text field, which is underlined. Below the text field, there are two links: "Can't access your account?" and "Sign-in options", both in blue text. At the bottom right, there are two buttons: a grey "Back" button and a blue "Next" button.

 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 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 must 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

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

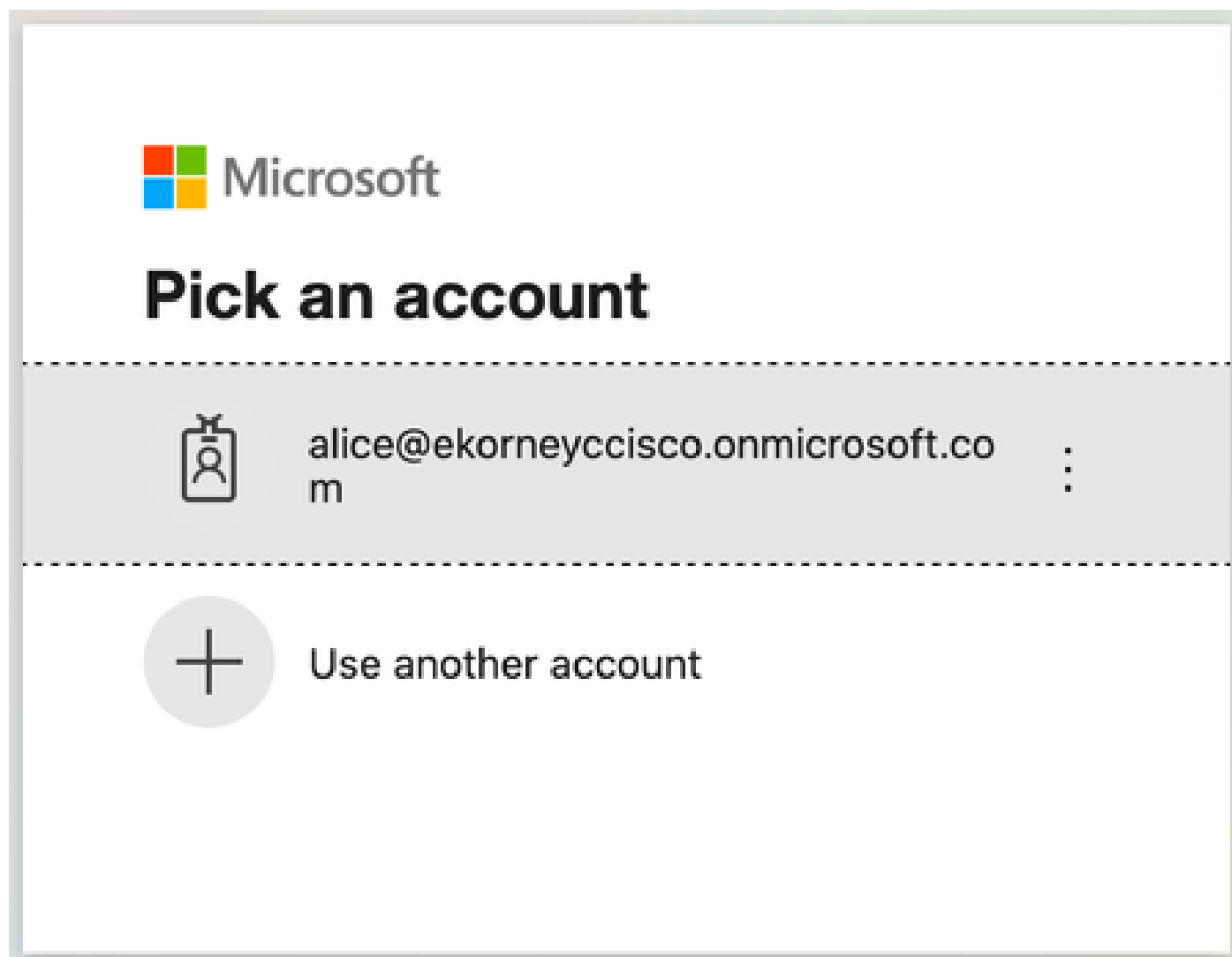
Welcome [alice@ekorneyccisco.onmicrosoft.com](#) ▼



Help

Sign Out

6. The user must be successfully logged out and redirected to the login screen again.



## 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).

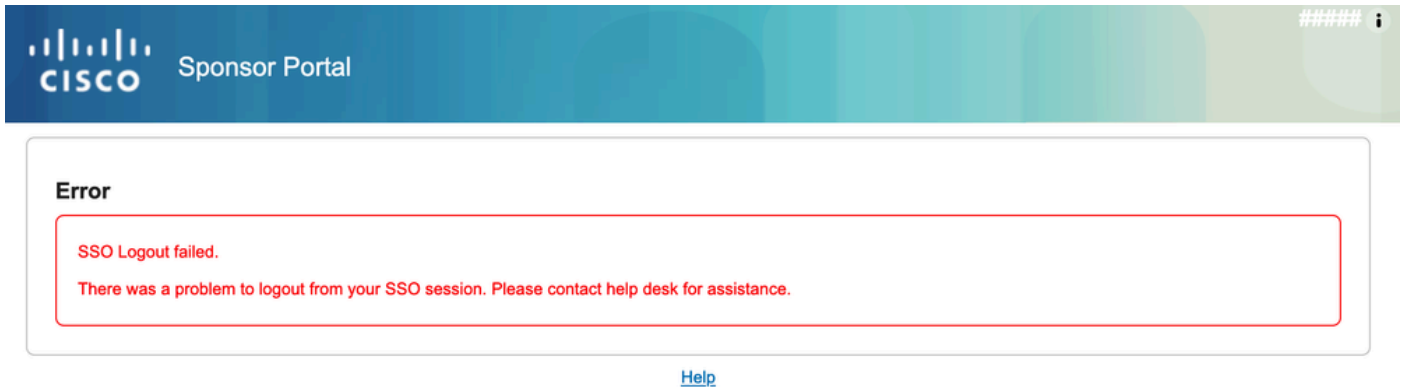
**Advanced diagnostics:** [Enable](#)

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. Sign Out does not work as expected and 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

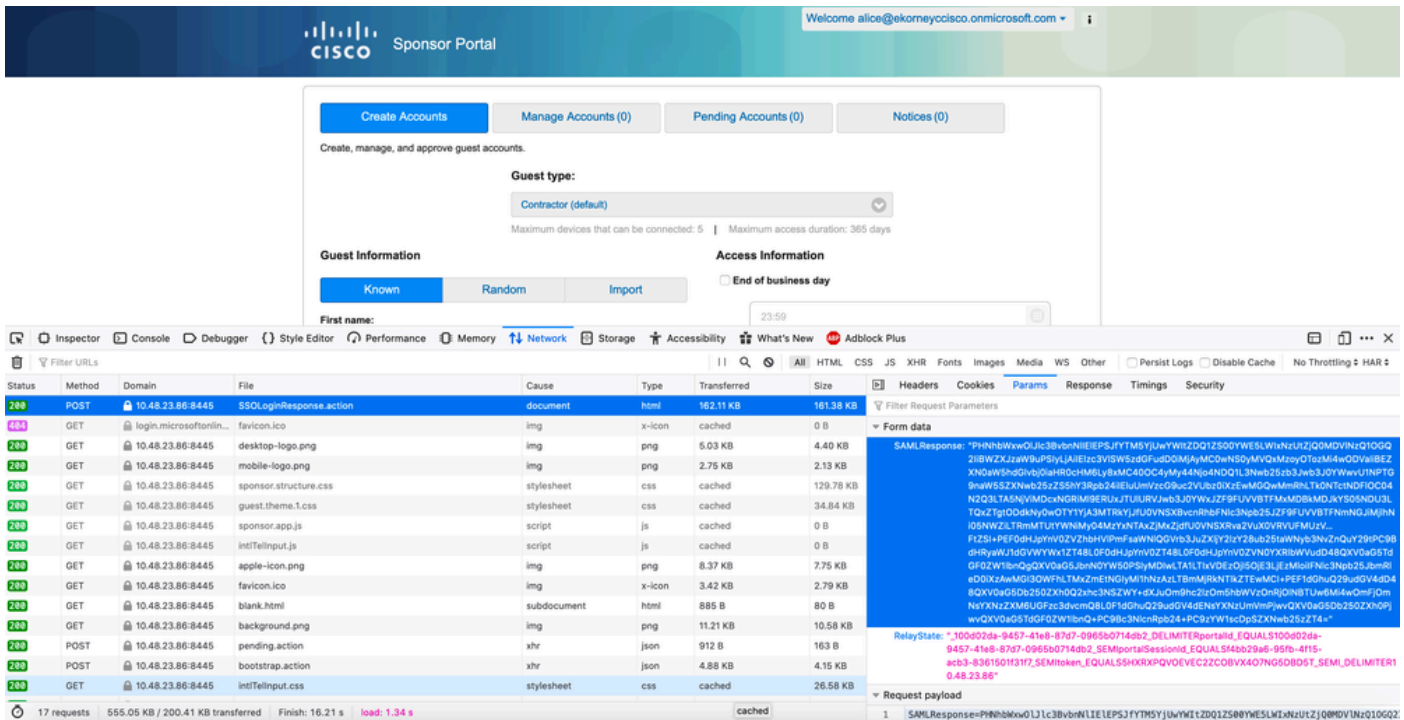
"<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2>" while it must be

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



## Client Troubleshooting

In order to verify that SAML payload is received, you can use Web Developer Tools. Navigate to **Tools > Web Developer > Network** if you make use of Firefox and log in with Azure credentials to the Portal. You can see the encrypted SAML response in Params Tab:



## ISE Troubleshooting

Log Level of the components here must be changed on **ISE**. Navigate to **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**.

| Component Name    | Log Level | Log Filename |
|-------------------|-----------|--------------|
| guestaccess       | DEBUG     | guest.log    |
| portal-web-action | DEBUG     | guest.log    |
| opensaml          | DEBUG     | ise-psc.log  |
| saml              | DEBUG     | ise-psc.log  |

Working set of Debugs at the time of correct flow execution (ise-psc.log):

1. The 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.SAMLFa
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
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.SAMLFa
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
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.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-8e40-e43d20c9f429_SEMI
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
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.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
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.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,126 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
:_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSes
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.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,129 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
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.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,133 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
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.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
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.SAMLFa
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
This node's host name:ISE30-1ek 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.SAMLFa
2020-09-16 10:44:11,184 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] org.opensaml.xml.parse.BasicPa
2020-09-16 10:44:11,187 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] org.opensaml.xml.parse.BasicPa
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.sam12.binding.decoding
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-8e40-e43d20c9f429_SEMI
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.sam12.binding.decoding
2020-09-16 10:44:11,191 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,193 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
```

```

2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.saml2.binding.decodin
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.saml2.binding.decodin
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.common.binding.decodi
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.common.binding.decodi
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.decodi
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.SAMLFa
SAML decoder's URIComparator - [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.decodi
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.SAMLFa

```

### 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.SAMLA
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.SAMLA
Attribute=<http://schemas.microsoft.com/identity/claims/tenantid> add value=<64ace648-115d-4ad9-a3bf-76
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLA
attribute<http://schemas.microsoft.com/identity/claims/tenantid> value=<64ace648-115d-4ad9-a3bf-76601b0
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLA
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.SAMLA
Attribute=<http://schemas.microsoft.com/identity/claims/objectidentifier> add value=<50ba7e39-e7fb-4cb1
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLA
attribute<http://schemas.microsoft.com/identity/claims/objectidentifier> value=<50ba7e39-e7fb-4cb1-8256
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLA
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.SAMLA
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.SAMLA
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.SAMLA
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.SAMLA
Attribute=<http://schemas.microsoft.com/ws/2008/06/identity/claims/groups> add value=<f626733b-eb37-4cf
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLA
<http://schemas.microsoft.com/ws/2008/06/identity/claims/groups> value=<f626733b-eb37-4cf2-b2a6-c2895fd
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLA
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.SAMLA
Attribute=<http://schemas.microsoft.com/identity/claims/identityprovider> add value=<https://sts.window
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLA
<http://schemas.microsoft.com/identity/claims/identityprovider> value=<https://sts.windows.net/64ace648

```



2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
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.SAMLAt  
Attribute=<http://schemas.microsoft.com/claims/authnmethodsreferences> add value=<http://schemas.micros  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
<http://schemas.microsoft.com/claims/authnmethodsreferences> value=<http://schemas.microsoft.com/ws/200  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
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.SAMLAt  
Attribute=<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> add value=<alice@ekorneyccisco.o  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
<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.SAMLFa  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.config.Identity  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
Attribute <http://schemas.microsoft.com/identity/claims/displayname> NOT configured in IdP dictionary, I  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
Attribute <http://schemas.microsoft.com/identity/claims/tenantid> NOT configured in IdP dictionary, NOT  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
Attribute <http://schemas.microsoft.com/identity/claims/identityprovider> NOT configured in IdP dictio  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
Attribute <http://schemas.microsoft.com/identity/claims/objectidentifier> NOT configured in IdP dictio  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
Attribute <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> NOT configured in IdP dictionary  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
Attribute <http://schemas.microsoft.com/claims/authnmethodsreferences> NOT configured in IdP dictionary  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLS  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAt  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
\_bd48c1a1-9477-4746-8e40-e43d20c9f429\_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess  
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.SAMLFa  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
\_bd48c1a1-9477-4746-8e40-e43d20c9f429\_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess  
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.SAMLFa  
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
\_bd48c1a1-9477-4746-8e40-e43d20c9f429\_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess  
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.SAMLFa  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa  
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.SAMLFa  
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.SAMLFa  
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-e43d2  
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.  
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.validators.

```

2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] org.opensaml.security.SAMLSign
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] org.opensaml.security.SAMLSign
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] org.opensaml.xml.signature.Sig
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] org.opensaml.xml.signature.Sig
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] org.opensaml.xml.signature.Sig
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] org.opensaml.xml.signature.Sig
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] org.opensaml.xml.signature.Sig
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.validators.
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress, sessionIndex=_4b798ec4-9aeb-40dc-8bed-6d
2020-09-16 10:44:11,292 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
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.SAMLFa
2020-09-16 10:44:11,306 INFO [RMI TCP Connection(346358)-127.0.0.1] [] api.services.server.role.RoleImpl
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cisco.cpm.saml.framework.SAMLS
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cisco.cpm.saml.framework.SAMLS

```

5. The 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.SAMLFa
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa

```

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.SAMLFa
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.Message
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.Message
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.Message
2020-09-16 10:44:53,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4] [] cpm.saml.framework.impl.SAMLFa

```

[illegible]