

使用Azure AD SAML SSO配置ISE 3.0保证人门户

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[高级流程图](#)

[配置](#)

[步骤1.在ISE上配置SAML身份提供程序和发起人门户](#)

[1.将Azure AD配置为外部SAML身份源](#)

[2.配置保证人门户以使用Azure AD](#)

[3.导出服务提供商信息](#)

[步骤2.配置Azure AD IdP设置](#)

[1.创建Azure AD用户](#)

[2.创建Azure AD组](#)

[3.将Azure AD用户分配给组](#)

[4.创建Azure AD企业应用程序](#)

[5.将组添加到应用程序](#)

[6.配置Azure AD企业应用程序](#)

[7.配置Active Directory组属性](#)

[8.下载Azure联合元数据XML文件](#)

[步骤3.将元数据从Azure Active Directory上传到ISE](#)

[步骤4.在ISE上配置SAML组](#)

[步骤5.在ISE上配置保证人组映射](#)

[验证](#)

[故障排除](#)

[常见问题](#)

[客户端故障排除](#)

[ISE故障排除](#)

简介

本文档介绍如何使用思科身份服务引擎(ISE)3.0配置Azure Active Directory(AD)SAML服务器，以为保证人用户提供单点登录(SSO)功能。

先决条件

要求

Cisco 建议您了解以下主题：

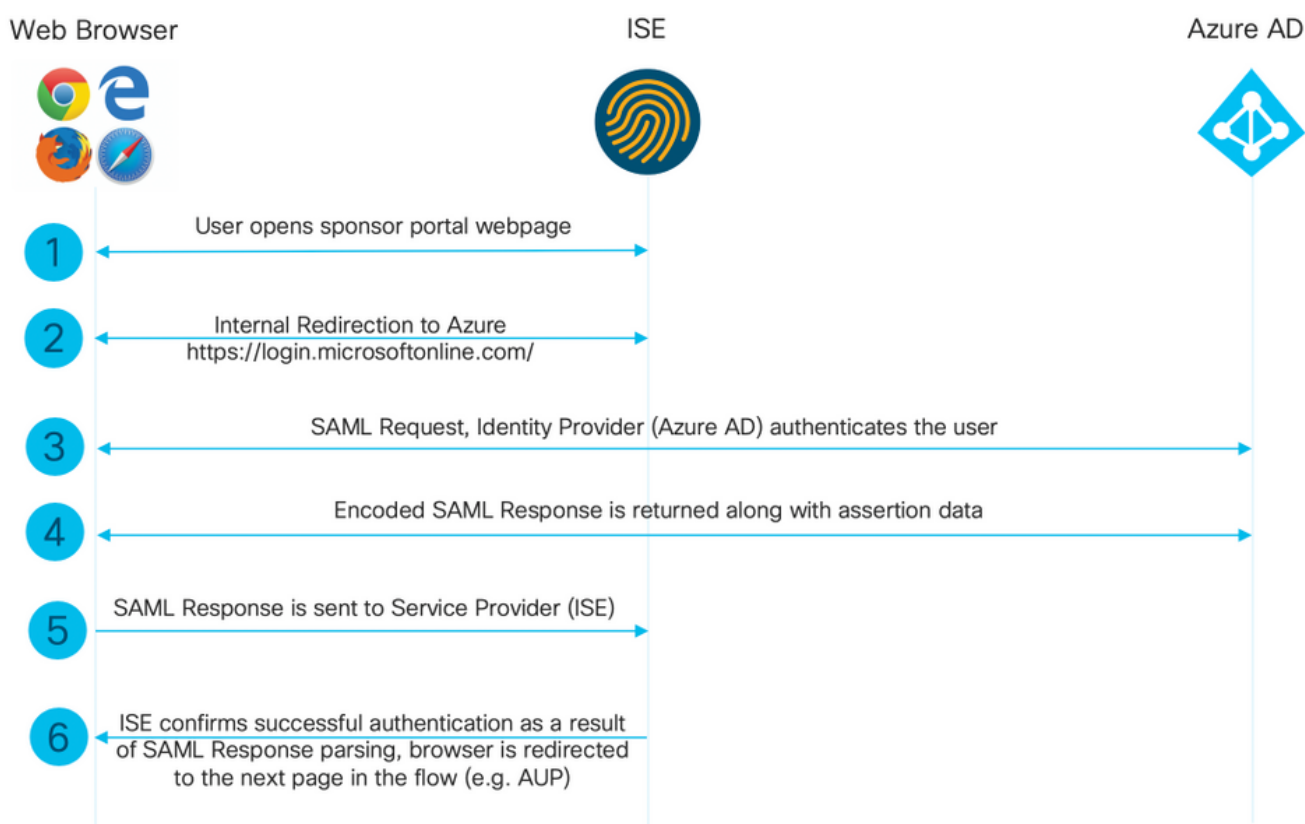
1. 思科ISE 3.0
2. 有关SAML SSO部署的基本知识
3. Azure AD

使用的组件

1. 思科ISE 3.0
2. Azure AD

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

高级流程图



配置



步骤1.在ISE上配置SAML身份提供程序和发起人门户

1.将Azure AD配置为外部SAML身份源

在ISE上，导航至Administration > Identity Management > External Identity Sources > SAML Id Providers，然后点击Add按钮。

输入ID提供程序名称并单击提交以保存它。ID Provider Name仅对ISE有效，如图所示。

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. 配置保证人门户以使用Azure AD

导航至工作中心>访客接入>门户和组件>发起人门户，然后选择您的发起人门户。在本示例中，使用保证人门户（默认）。

展开门户设置面板，并在身份源序列中选择新的SAML IdP。配置发起人门户的完全限定域名(FQDN)。在本例中，它为sponsor30.example.com。单击“Save（保存）”，如图所示。

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. 导出服务提供商信息

导航至**管理>身份管理>外部身份源> SAML ID Providers > [您的SAML提供程序]**。

切换到选项卡“**服务提供商信息**”。然后单击**Export**按钮，如图所示。

[Identity Provider List](#) > Azure_SAML

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)

下载压缩文件并保存。在其中，您可以找到2个文件。您需要名为“发起人门户”的XML文件。

记下SingleLogoutService Bindings、**实体ID值**和AssertionConsumerService Binding中的ResponseLocation值。

```
<?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>
MIIFZjCCA06gAwIBAgIQX1oAvwAAAAChgVd9cEEWozANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQOD
ExpTQU1MX01TRTMwLTFlay5leGFtcGxlLmNvbTAeFw0yMDA5MTAxMDMyMzFaFw0yNTA5MDkxMDMy
MzFaMCUxIzAhBgNVBAMTG1NBTVUxfSVNFmZAtMwVrLmV4Yw1wbGUuY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICGKCAgEAt+MixKfuZvg/oAWGES6zrUYL3H2JwvZw9yJs6sJ8/BpP6Sw027wh
FXnESXpqmmsSVrVcQIrDdk3l8UYNn/+98PPkIi/4ftyFjZK9YdeverD6nrA2MeoLCzGlkWq/y4i
vvVcYuw344pySm65awVvro3q84x9esHqyLahExs9guiLJryD497XmNP4Z8eTHCctu777PuI1wL04
QOYUs2sozXvR98D9Jok/+Pjh3bjmVKapqAcNEFvk8Ez9x1sMBUGFwP4YdZzQB9IRVkJdIJGvqMyf
a6gn+KaddJnmIbXKFbrTaFii2IvRs3qHJ0mMVfYRnYeMql9/PhzvSftjRe32x/aQh23j9dCsVXmQ
ZmXpZyxxJ8p4RqyM0YgkfxnQXXtV9K0sRZPFn60+iszUw2hARRG/te0hTuVXpbonG2dT109JeeEe
S1E5uxenJvYkU7mMamvBjYQN6qVyyogf8F0lHTSfd6TDsK3Qhmz0jg50PrBvvg5qE6OrxxNvqSVZ
ldhx/iHAZAlYYSvdwizsZMCw0PjSwrRPx/h8l03djeW0aL5R1AF1qTFHVHSNvigzh6FyjdkUJH66
JAYgPe0PKJFRgYzh5vWoJ41qvdQj1Gk3c/zYi57MR1Bs0mkSvkOGbmjSsb+EehnYyLLB8FG3De2V
ZaXaH37gmoCNNmZHRn+GB0CAwEAAaOBkTCBjjAgBgNVHREETAXghVJU0UzMC0xZWsuZXhhbXBs
ZS5jb20wDAYDVROTBABUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVR0OBBYEFPT/6jpfyugxRolbjzWJ
858WfTP1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjARBglghkgBhvhCAQEEBAMCBkAw
DQYJKoZIhvcNAQEMBQADggIBABGyWZbLaJm2LyLASg//4N6mL+xu/9IMdVvNWBQodF+j0WusW15a
VPSQU2t3Ckd/IlanvpK+cp77NMjo9V9oWi3/ZnjZHGofAicHnLGCoeJmC1TvLau7ZzhCCII37DFA
yMKDrXLi3pR+ONLX1TivjPHTTzrKmlNHhkxkx/Js5Iuz+MyRKP8FNmWT0q4XGejyKzJWqrEu+bc1
idC1/gBNUcHGqmFeM82IGQ7jvOm1kBjLb4pTDbYk4fMIbJVh4V2Pgi++6MIfXAYEWL+LHjSGHCQT
PSM3+kpvlwHHpGWzQSmcJ4tXVXV95W0NC+LxQZLBPNUMUZorhuYCILXZxvXH1HGJJ0YKx91k9Ubd2
s5JaD+GN8jqm5XXAau7S4Bawfvc03boOiXnSvgtIuH9YFIR2lp2n/2X0VVbdPHYZtqGieqWWebHr
4I1z18FXblYyMzpIkhtOOvkP5mAlR92VXBkvx2WPjtzQrvOtSXgvTCOKerYCBM/jnuwsztv7FVTV
JNdFwOsncX70YngZeuJzyjPoUbfRkZI34VKZp4i05bZsGlbWE9Skdquv0PaQ8ecXTv8OCVBYUegl
vt0pdel8h/9jImdLG8dF0rbADGHieTcntSDdw3E7Jfms/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:SPSSODescriptor>
</EntityDescriptor>
```

```
<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>
```

根据XML文件：

SingleLogoutService

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

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

AssertionConsumerService位置

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

AssertionConsumerService位置

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

AssertionConsumerService位置

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

AssertionConsumerService位置

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

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

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

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

步骤2.配置Azure AD IdP设置

1.创建Azure AD用户

登录Azure Active Directory管理中心控制面板并选择AD，如图所示。

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... [Copy](#)

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

选择用户，单击新用户，配置用户名、名称和初始密码。单击“创建”，如图所示。

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. 创建Azure AD组

选择组。单击“新建组”，如图所示。

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](#)

将组类型保留为安全。配置组名，如图所示。

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.将Azure AD用户分配给组

单击“No members selected (未选择成员)”。选择用户并单击“选择”。单击Create以创建分配了User的组。

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

记下组对象ID，在此屏幕中，发起人组的ID为f626733b-eb37-4cf2-b2a6-c2895fd5f4d3。

Groups | All groups

Default Directory - Azure Active Directory

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

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

Search groups Add filters

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

4. 创建Azure AD企业应用程序

在AD下，选择“企业应用程序”，然后单击“新建应用程序”，如图所示。

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.

选择图像中所示的“非库”应用程序。

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**

输入应用程序的名称，然后单击“添加”。

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

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.将组添加到应用程序

选择分配用户和组。

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 ⓘ

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](#)

单击“添加用户”。

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?

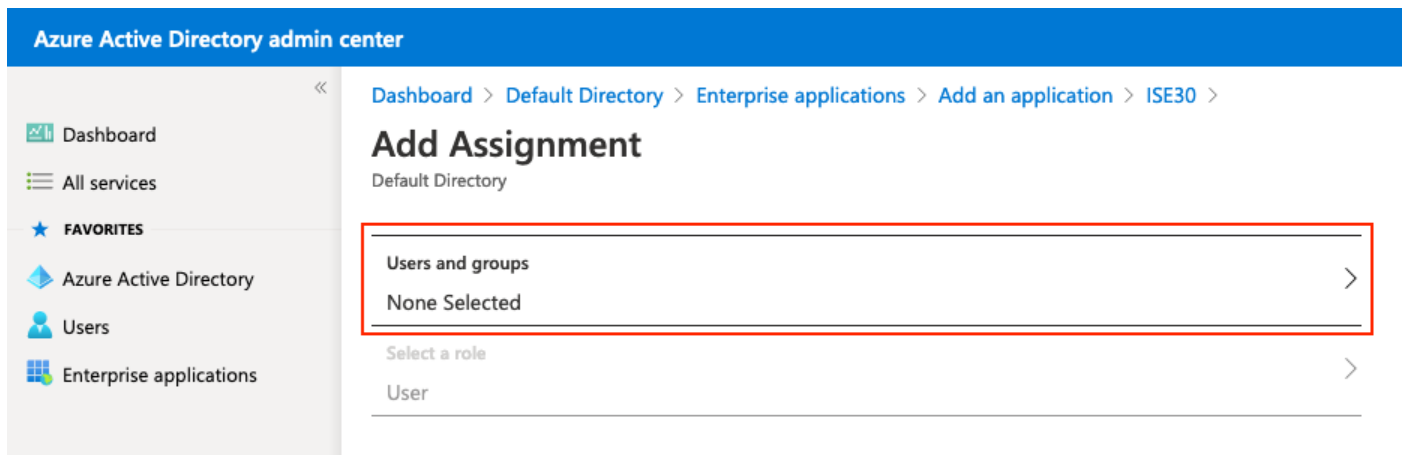
i The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

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

Display Name

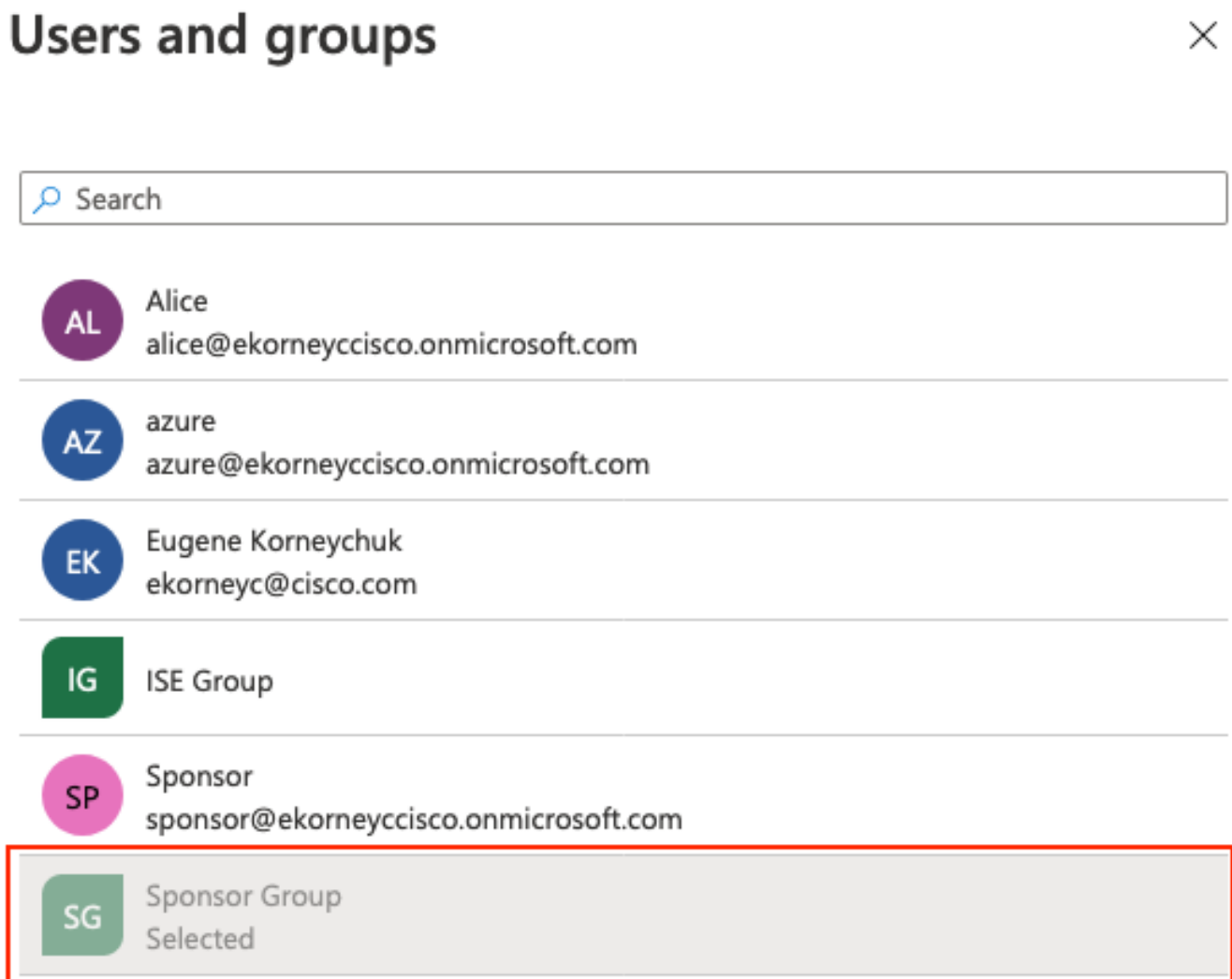
No application assignments found

单击“用户和组”。

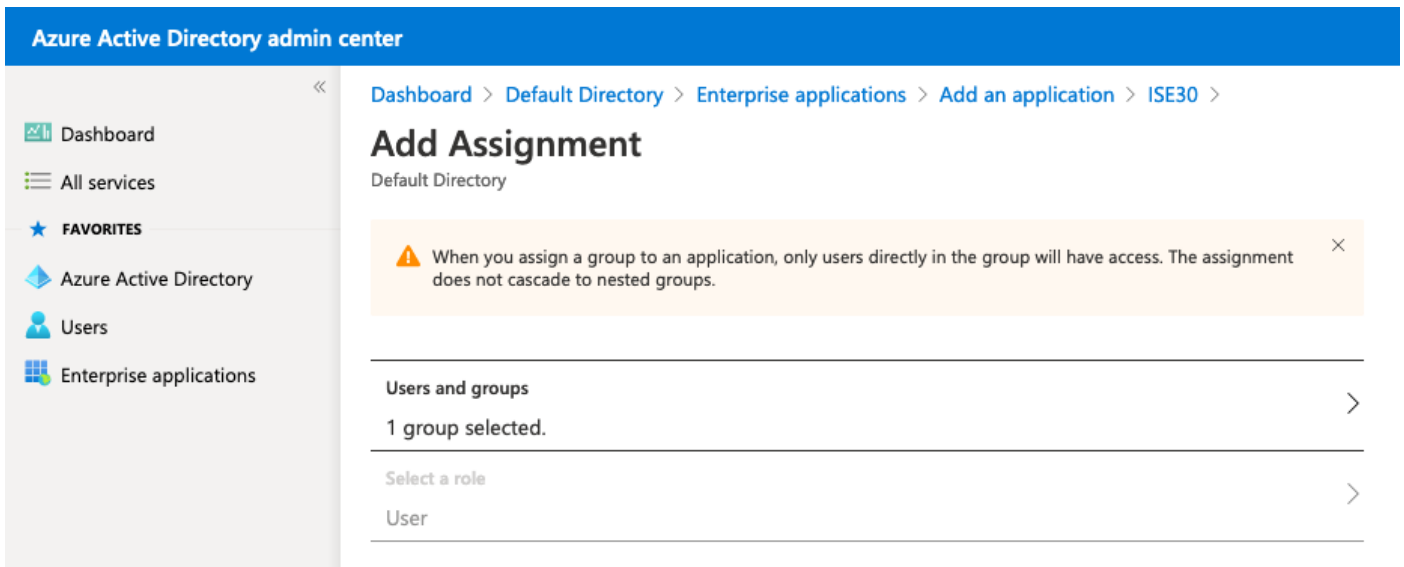


选择之前配置的组，然后单击“选择”。

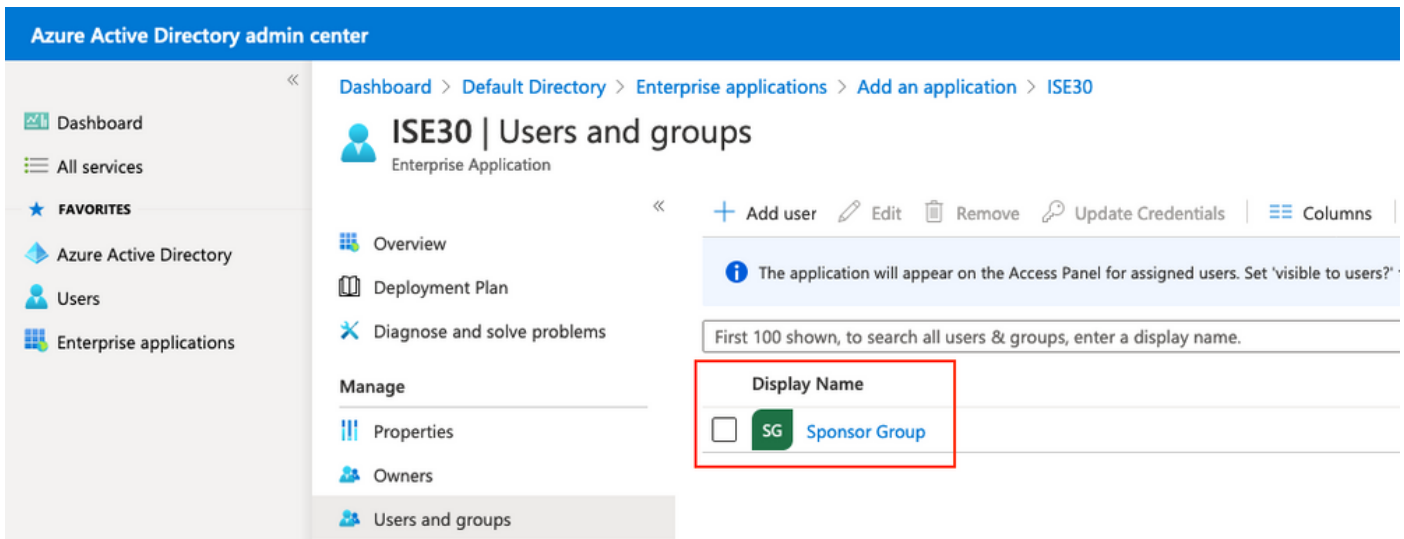
注意： 由您选择应该获得访问权限的一组用户或组。



选择组后，单击“分配”，如图所示。



因此，应用程序的“用户和组”菜单应填入选定的组。



6. 配置Azure AD企业应用程序

导航回您的应用程序，然后单击“设置单点登录”，如图所示。

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](#)

在下一屏幕上选择SAML。

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.

单击“Basic SAML Configuration(基本SAML配置)”旁边的“Edit (编辑)”。

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE30 >

ISE30 | SAML-based Sign-on

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
- Permissions
- Token encryption

Activity

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

Troubleshooting + Support

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

使用XML文件中的entityID值填充标识符(实体ID)，该值来自第导出服务提供商信息。使用AssertionConsumerService中的位置值填充回复URL(Assertion Consumer Service)。使用SingleLogoutService中的ResponseLocation填充注销URL值。单击“Save(保存)”。

注意： 回复URL充当通过列表，允许某些URL在重定向到IdP页面时充当源。

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 ⓘ

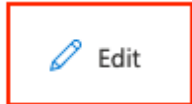
Logout Url ⓘ

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

7.配置Active Directory组属性

要返回之前配置的组属性值，请点击“用户属性和声明”旁边的“编辑”。

User Attributes & Claims



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

单击“Add a group claim (添加组声明)”。

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 ***

选择“安全组”并单击“保存”。断言中返回的源属性是组ID，它是之前捕获的组对象ID。

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



记录组的领款申请名称。在本例中，它为 <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. 下载Azure联合元数据XML文件

单击“Download abord 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: [https://login.microsoftonline.com/64ace648-115d ...](https://login.microsoftonline.com/64ace648-115d...)

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)



步骤3. 将元数据从Azure Active Directory上传到ISE

导航至管理>身份管理>外部身份源> SAML ID Providers > [您的SAML提供程序]。

切换到选项卡Identity Provider Config., 然后单击“浏览”按钮。从第步“下载Azure联合元数据XML”中选择“联合元数据XML”，然后单击“保存”。

注意：应在CSCv74517下解决身份提供程序配置的UI故障。

External Identity Sources

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

Identity Provider List > Azure_SAML

SAML Identity Provider

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

Identity Provider Configuration

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



Signing Certificates

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

步骤4.在ISE上配置SAML组

切换到选项卡Groups，并将Configure Active Directory Group属性中的Claim name值粘贴到Group Membership Attribute中。

External Identity Sources

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

Identity Provider List > Azure_SAML

SAML Identity Provider

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

Groups

Group Membership Attribute <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups> ⓘ

 Name in Assertion Name in ISE

No data available

单击“Add”。使用在将Azure Active Directory用户分配到组中捕获的保证人组的组对象ID值填充断言中的名称。在ISE中配置名称(在本例中为Azure保证人组)具有意义值Click OK. 点击 保存。

这将在Azure中的组和可在ISE上使用的组名之间创建映射。

Add Group

*Name in Assertion eb37-4cf2-b2a6-c2895fd5f4d3

*Name in ISE Azure Sponsor Group

OK Cancel

步骤5.在ISE上配置保证人组映射

导航至工作中心>访客访问>门户和组件>发起人组，然后选择要映射到Azure AD组的发起人组。在本示例中，使用ALL_ACCOUNTS（默认）。

Enabled	Name	Member Groups
<input checked="" type="checkbox"/>	ALL_ACCOUNTS (default)	ALL_ACCOUNTS (default)
<input checked="" type="checkbox"/>	GROUP_ACCOUNTS (default)	GROUP_ACCOUNTS (default)
<input checked="" type="checkbox"/>	OWN_ACCOUNTS (default)	OWN_ACCOUNTS (default)

单击成员..... 并将Azure_SAML:Azure保证人组添加到所选用户组。这会将Azure中的保证人组映射到ALL_ACCOUNTS保证人组。单击“OK(确定)”。单击“Save(保存)”。



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

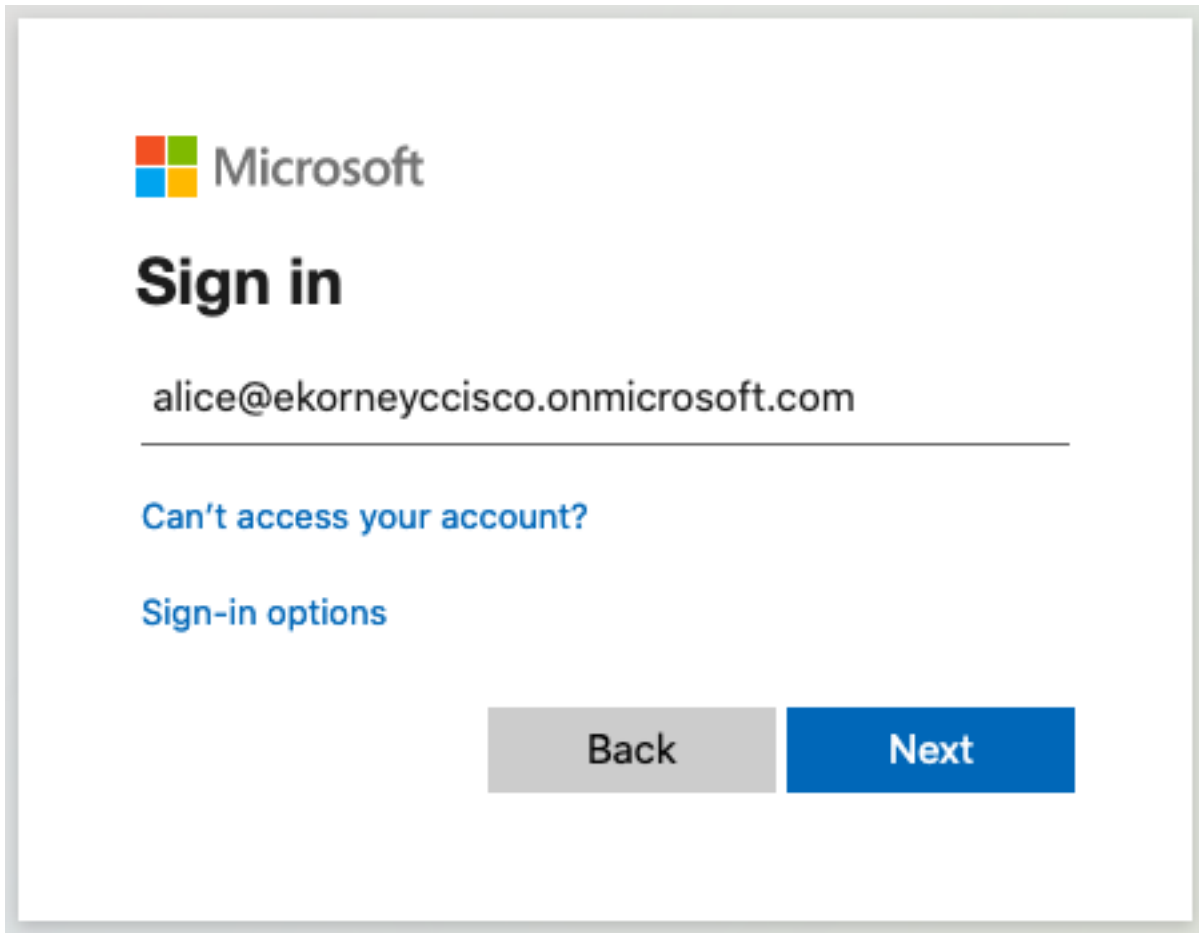
验证

使用本部分可确认配置能否正常运行。

注意：新用户首次登录时必须更改用户密码。接受AUP验证步骤，但不覆盖它。验证涵盖以下场景：用户不是首次登录，且发起人(alice)已接受一次AUP。

现在，如果您打开发起人门户（例如，从测试URL），您将重定向到Azure以登录，然后返回发起人门户。

1.在门户测试URL链接上启动具有其FQDN的发起人门户。ISE应将您重定向到Azure登录页面。输入用户名，以前创建并单击“下一步”。

A screenshot of the Microsoft sign-in page. At the top left is the Microsoft logo. Below it is the text "Sign in". A text input field contains the email address "alice@ekorneyccisco.onmicrosoft.com". Below the input field is a horizontal line. Underneath the line are two links: "Can't access your account?" and "Sign-in options". 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.输入密码，然后单击“登录”。IdP登录屏幕将用户重定向到初始ISE的发起人门户。



← alice@ekorneyccisco.onmicrosoft.com

Enter password

.....|

[Forgot my password](#)

Sign in

3.接受AUP。



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.此时，保证人用户应具有ALL_ACCOUNTS保证人组权限，对门户具有完全访问权限。

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

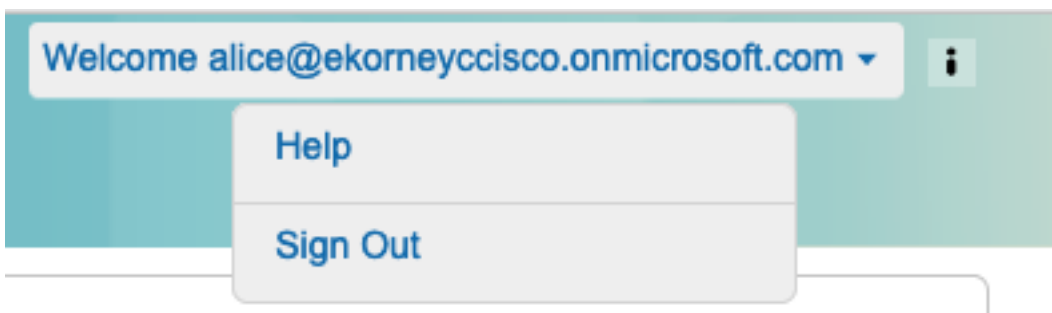
To Time *

10:22

Create

[Help](#)

5.单击“欢迎”下拉菜单下的“注销”。



6.用户应成功注销并重定向到登录屏幕。



Pick an account



alice@ekorneyccisco.onmicrosoft.co
m



Use another account

故障排除

本部分提供的信息可用于对配置进行故障排除。

常见问题

了解SAML身份验证是在浏览器和Azure Active Directory之间处理的，这一点至关重要。因此，您可以直接从ISE参与尚未启动的身份提供程序(Azure)获取与身份验证相关的错误。

问题1。用户输入了错误的密码，未在ISE上处理用户数据，问题直接来自IdP(Azure)。要修复：重置密码或提供正确的密码数据。



← 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

问题2。用户不属于应允许访问SAML SSO的组，在这种情况下，ISE上未完成用户数据处理，问题直接来自IdP(Azure)。要修复：验证是否正确执行了向应用程序添加组配置步骤。



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不按预期工作，出现此错误 — “SSO注销失败。从SSO会话注销时出现问题。请联系帮助台寻求帮助。” 在SAML IdP上未正确配置注销URL时，可以看到此消息。在这种情况下，此URL使用

“<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2>”，而它应使用

“<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action>”以修复：在Azure IdP的注销URL中输入正确的URL。

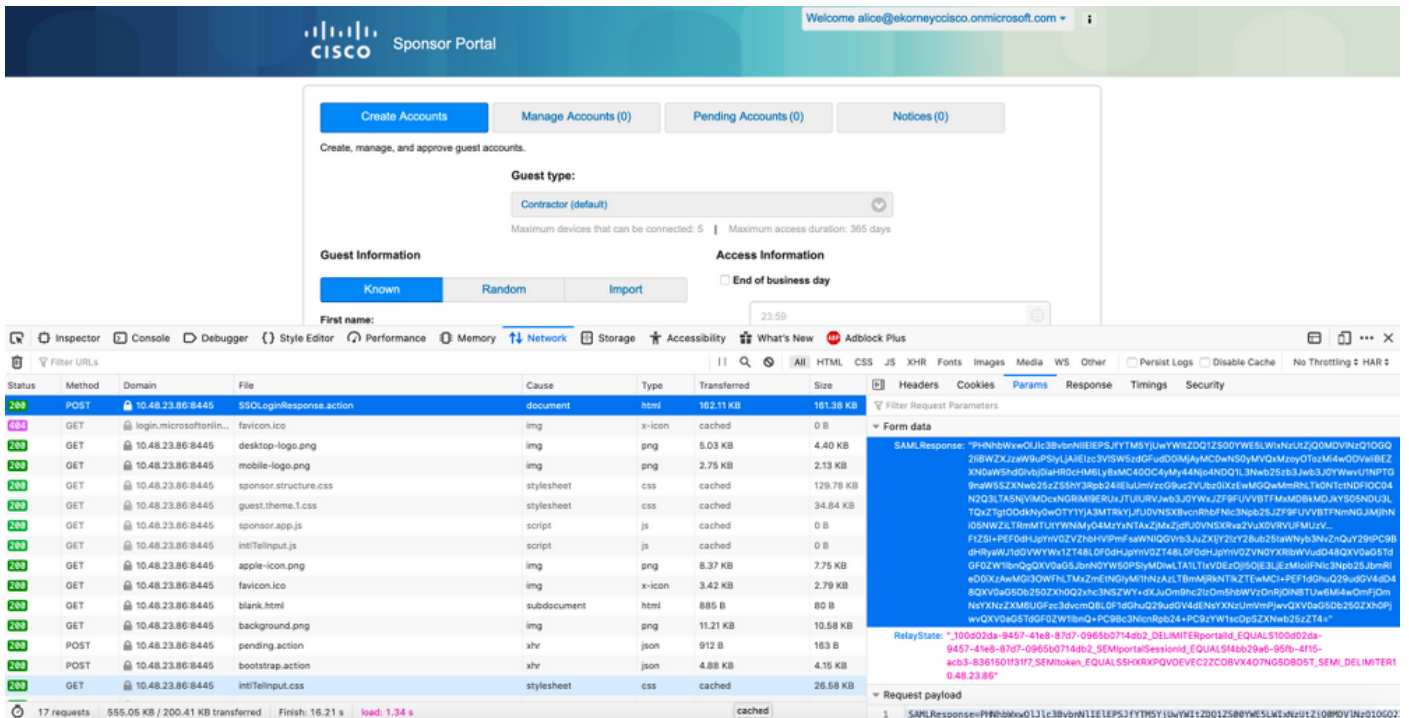
Error

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

[Help](#)

客户端故障排除

要验证是否收到SAML负载，可以使用Web Developer Tools。如果您使用Firefox并使用Azure凭据登录到门户，请导航到“工具”>“Web开发人员”>“网络”。您可以在“参数”选项卡中看到加密的SAML响应：



ISE故障排除

ISE上应更改此处组件的日志级别。导航至操作>故障排除>调试向导>调试日志配置。

组件名称	日志级别	日志文件名
访客访问	调试	guest.log
门户Web操作	调试	guest.log
opensaml	调试	ise-psc.log
saml	调试	ise-psc.log

正确执行流时的调试工作集(ise-psc.log):

1.用户从发起人门户重定向到IdP URL。

```
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.从浏览器收到SAML响应。

```
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.属性 (断言) 分析已启动。

```
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.收到组属性值为f626733b-eb37-4cf2-b2a6-c2895fd5f4d3 , 签名验证。

```
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
```



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

```
cpm.saml.framework.impl.SAMLAttributesParser -::::- [SAMLAttributesParser:readDict]: read Dict
attribute=<ExternalGroups>
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/displayname> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [cacheGroupAttr] Adding to cache
ExternalGroup values=<f626733b-eb37-4cf2-b2a6-c2895fd5f4d3>
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/tenantid> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/identityprovider> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/identity/claims/objectidentifier> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes]
Attribute <http://schemas.microsoft.com/claims/authnmethodsreferences> NOT configured in IdP
dictionary, NOT caching
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cisco.cpm.saml.framework.SAMLSessionDataCache -::::- [storeAttributesSessionData]
idStore=<Azure_SAML> userName=alice@ekorneyccisco.onmicrosoft.com>
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [SAMLAttributesParser:getEmail] The email
attribute not configured on IdP
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response: email attribute value:
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal ID:bd48c1a1-9477-4746-
8e40-e43d20c9f429
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal Session info:
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1;token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-
e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML flow initiator PSN's Host name
is:sponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isLoadBalancerConfigured() - LB NOT
```

```
configured for: Azure_SAML
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM.
IDP URL: https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SPProviderId for Azure_SAML is:
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- ResponseValidationContext:
IdP URI: https://sts.windows.net/64ace648-115d-4ad9-a3bf-76601b0f8d5c/
SP URI: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
Assertion Consumer URL: https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action
Request Id: _bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-
8e40-e43d20c9f429_SEMIportalSessionId_EQUALS8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1_SEMItoken_EQUALSOA6CZJQD7X67TLYHE4Y3EM3EY097E2J_SEMI_DELIMITERSponsor30.example.com
Client Address: 10.61.170.160
Load Balancer: null
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.SAMLSignatureValidator -::::- no signature in response
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Validating signature of assertion
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.BaseSignatureValidator -::::- Determine the signing certificate
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.BaseSignatureValidator -::::- Validate signature to SAML standard
with cert:CN=Microsoft Azure Federated SSO Certificate
serial:112959638548824708724869525057157788132
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
org.opensaml.security.SAMLSignatureProfileValidator -::::- Saw Enveloped signature transform
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
org.opensaml.security.SAMLSignatureProfileValidator -::::- Saw Exclusive C14N signature
transform
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.BaseSignatureValidator -::::- Validate signature againsta signing
certificate
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
org.opensaml.xml.signature.SignatureValidator -::::- Attempting to validate signature using key
from supplied credential
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
org.opensaml.xml.signature.SignatureValidator -::::- Creating XMLSignature object
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
org.opensaml.xml.signature.SignatureValidator -::::- Validating signature with signature
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
org.opensaml.xml.signature.SignatureValidator -::::- Validation credential key algorithm 'RSA',
key instance class 'sun.security.rsa.RSAPublicKeyImpl'
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
org.opensaml.xml.signature.SignatureValidator -::::- Signature validated with key from supplied
credential
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Assertion signature validated
succesfully
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating response
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating assertion
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.AssertionValidator -::::- Assertion issuer succesfully validated
2020-09-16 10:44:11,204 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.validators.AssertionValidator -::::- Authentication statements 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 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 -:::- 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.用户组被添加到身份验证结果中，以便Portal可以使用，SAML身份验证通过。

```
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.已触发注销。在SAML响应中收到LogOut

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

```
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
SAMLUtils::isOracle() - checking whether IDP URL indicates that its OAM. IDP URL:
https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:- getLogoutMethod
- method:REDIRECT_METHOD_LOGOUT
2020-09-16 10:44:51,462 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
getSignLogoutRequest - null
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
```

```
buildLogoutRequest - loginInfo:SAMLLoginInfo: name=alice@ekorneyccisco.onmicrosoft.com,
format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress, sessionIndex=_4b798ec4-9aeb-40dc-
8bed-6dd2fdd46800, time diff=26329
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
SAMLUtills::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:-
SAMLUtills::isOracle() - checking whether IDP URL indicates that its OAM. IDP URL:
https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:- SPPProviderId
for Azure_SAML is: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - spProviderId:http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][]
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - logoutURL:https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-
76601b0f8d5c/saml2
2020-09-16 10:44:53,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML HTTPRequest - Portal ID:bd48c1a1-9477-4746-
8e40-e43d20c9f429
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML flow initiator PSN's Host name
is:sponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Is redirect required:
InitiatorPSN:sponsor30.example.com This node's host name:ISE30-lek LB:null request Server
Name:sponsor30.example.com
2020-09-16 10:44:53,248 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- This node is the initiator (sponsor30.example.com)
this node host name is:sponsor30.example.com
2020-09-16 10:44:53,249 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,249 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML HTTPRequest - Portal Session info:8fa19bf2-
9fa6-4892-b082-5cdabfb5daa1
2020-09-16 10:44:53,250 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
org.opensaml.xml.parse.BasicParserPool -:::- Setting DocumentBuilderFactory attribute
'http://javax.xml.XMLConstants/feature/secure-processing'
2020-09-16 10:44:53,251 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
org.opensaml.xml.parse.BasicParserPool -:::- Setting DocumentBuilderFactory attribute
'http://apache.org/xml/features/disallow-doctype-decl'
2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
opensaml.ws.message.decoder.BaseMessageDecoder -:::- Beginning to decode message from inbound
transport of type: org.opensaml.ws.transport.http.HttpServletRequestAdapter
2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
opensaml.saml2.binding.decoding.HTTPRedirectDeflateDecoder -:::- Decoded RelayState: _bd48c1a1-
9477-4746-8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-
5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
opensaml.saml2.binding.decoding.HTTPRedirectDeflateDecoder -:::- Base64 decoding and inflating
SAML message
2020-09-16 10:44:53,253 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
opensaml.ws.message.decoder.BaseMessageDecoder -:::- Parsing message stream into DOM document
2020-09-16 10:44:53,256 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
```

```
opensaml.ws.message.decoder.BaseMessageDecoder -:::- Unmarshalling message DOM
2020-09-16 10:44:53,256 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
opensaml.ws.message.decoder.BaseMessageDecoder -:::- Message 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:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_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:bd48c1a1-9477-4746-
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:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_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-b082-5cdabfb5daa1
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:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_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 -:::- SPProviderId for Azure_SAML is:
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:53,258 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- ResponseValidationContext:
IdP URI: https://sts.windows.net/64ace648-115d-4ad9-a3bf-76601b0f8d5c/
SP URI: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
```

Assertion Consumer URL:
https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action
Request Id: _bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
Client Address: 10.61.170.160
Load Balancer: null
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- LogoutResponse signature validated
succesfully
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- This is LogoutResponse (only
REDIRECT is supported) no signature is on assertion, continue
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating response
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating assertion
2020-09-16 10:44:53,259 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: validation succeeded for null