

Azure AD SAML SSOによるISE 3.0スポンサーポータルの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[概要フロー図](#)

[設定](#)

[ステップ1: ISEでのSAML IDプロバイダーとスポンサーポータルの設定](#)

[1. Azure ADを外部SAML IDソースとして構成します](#)

[2. Azure ADを使用するようにスポンサーポータルを構成します](#)

[3. サービスプロバイダー情報のエクスポート](#)

[ステップ2: Azure AD IdPの設定](#)

[1. Azure ADユーザーの作成](#)

[2. Azure ADグループの作成](#)

[3. Azure ADユーザーをグループに割り当てる](#)

[4. Azure ADエンタープライズアプリケーションの作成](#)

[5. アプリケーションへのグループの追加](#)

[6. Azure ADエンタープライズアプリケーションの構成](#)

[7. Active Directoryグループ属性の設定](#)

[8. Azure FederationメタデータXMLファイルのダウンロード](#)

[ステップ3: Azure Active DirectoryからISEへのメタデータのアップロード](#)

[ステップ4: ISEでのSAMLグループの設定](#)

[ステップ5: ISEでのスポンサーグループマッピングの設定](#)

[確認](#)

[トラブルシューティング](#)

[一般的な問題](#)

[クライアントのトラブルシューティング](#)

[ISEのトラブルシューティング](#)

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)3.0を使用してAzure Active Directory(AD)SAMLサーバを設定し、スポンサーユーザーにシングルサインオン(SSO)機能を提供する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

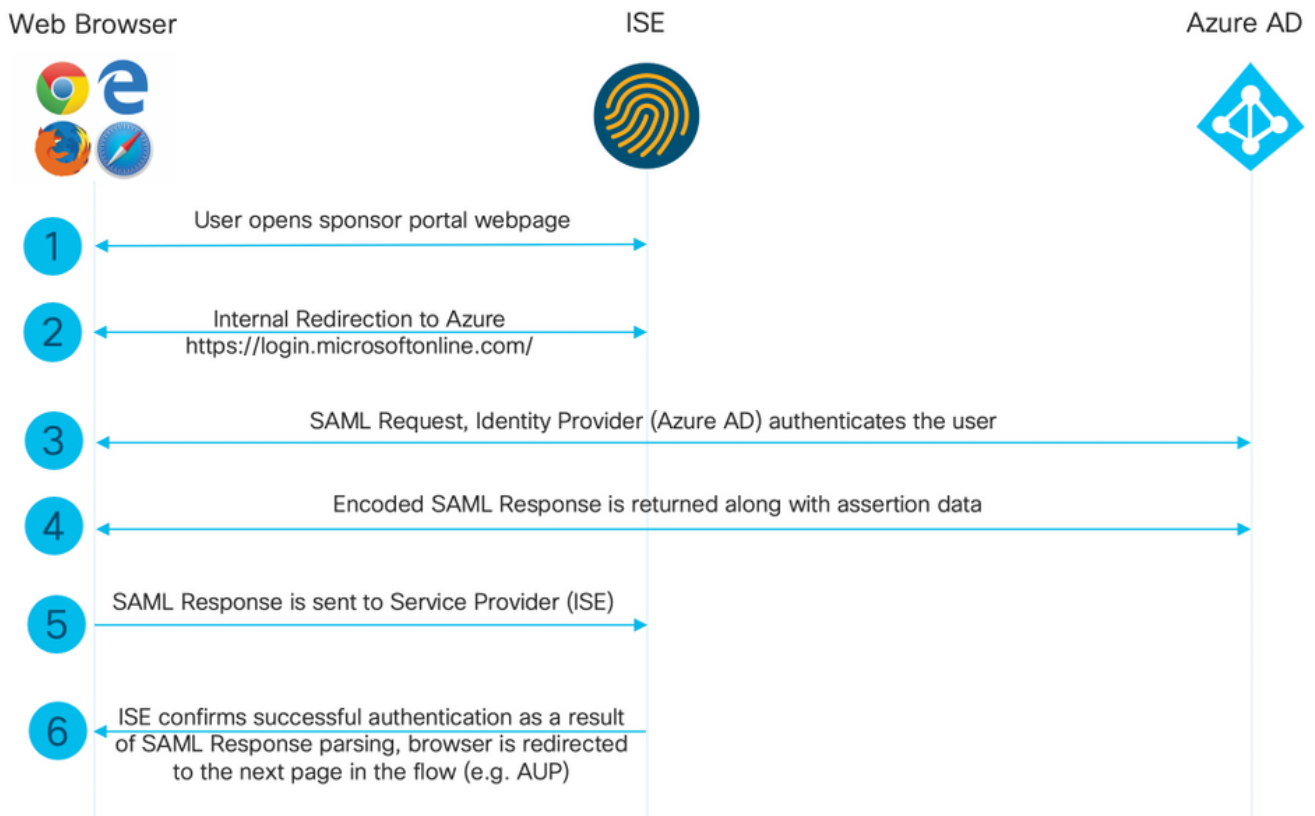
1. Cisco ISE 3.0
2. SAML SSOの導入に関する基礎知識
3. Azure AD

使用するコンポーネント

1. Cisco ISE 3.0
2. Azure AD

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要フロー図



設定

ステップ1: ISEでのSAML IDプロバイダーとスポンサーポータルの設定

1. Azure ADを外部SAML IDソースとして構成します

ISEで、[Administration] > [Identity Management] > [External Identity Sources] > [SAML Id Providers]に移動し、[Add]ボタンをクリックします。

[ID Provider Name]を入力し、[Submit]をクリックして保存します。IDプロバイダ名は、図に示す

ようにISEでのみ重要です。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · Identity Management'. Below it, a breadcrumb trail shows 'Identities > Groups > External Identity Sources > Identity Source Sequences > Settings'. The main content area is titled 'External Identity Sources' and contains a list of provider types: Certificate Authentication F, Active Directory, EXAMPLE, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, Social Login, and REST (ROPC). The 'SAML Id Providers' section is expanded, showing a 'New Identity Provider' form. The form has tabs for 'General', 'Identity Provider Config.', 'Service Provider Info.', 'Groups', 'Attributes', and 'Advanced Settings'. The 'General' tab is active, and a red box highlights the 'Id Provider Name' field (containing 'Azure_SAML') and the 'Description' field (containing 'Azure Active Directory').

2. Azure ADを使用するようにスポンサーポータルを構成します

[Work Centers] > [Guest Access] > [Portals & Components] > [Sponsor Portals]に移動し、スポンサーポータルを選択します。この例では、スポンサーポータル (デフォルト) が使用されています。

[Portal Settings]パネルを展開し、[Identity source sequence]で新しいSAML IdPを選択します。スポンサーポータルの完全修飾ドメイン名(FQDN)を構成します。この例では、sponsor30.example.comです。図に示すように、[Save]をクリックします。

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. サービスプロバイダー情報のエクスポート

[Administration] > [Identity Management] > [External Identity Sources] > [SAML Id Providers] > [Your SAML Provider]に移動します。

[サービスプロバイダ情報]タブに切り替え。図に示すように、[Export]ボタンをクリックします。

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)

zipファイルをダウンロードして保存します。その中には2つのファイルがあります。スポンサーポータルと呼ばれるXMLファイルが必要です。

SingleLogoutService BindingsからのResponseLocation、entityID値、およびAssertionConsumerServiceBindingからのLocation値を書き留めます。

```
<?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>
MIIFZjCCA06gAwIBAgIQX1oAvwAAAAChgVd9cEEW0zANBqkqhkiG9w0BAQwFADAlMSMwIQYDVQQL
ExpTQU1MX01TRTMwLTFlay5leGFtcGxlLmNvbTAeFw0yMDA5MTAxMDMyMzFaFw0yNTA5MDkxMDMy
MzFaMCUxIzAhBgNVBAMTGlNBTUxfSVNFMzAtMWVrLmV4YW1wbGUuY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCGKCAgEAT+MixKfuZvg/oAWG6zrUYL3H2JwvZw9yJs6sJ8/BpP6Sw027wh
FXnESXpqqmnoSVrVcEQIrDdk3l8UYNn/+98PPkIi/4ftyFjZK9YdeverD6nrA2MeoLCzG1kWq/y4i
vvVcYuW344pySm65awVvro3q84x9esHqyLahExs9guiLJryD497XmNP4Z8eTHCctu777PuI1wL04
QOYUs2sozXvR98D9Jok/+PjH3bjmVKapqAcNEFvk8Ez9x1sMBUgFwP4YdZzQB9IRVkJdIJGvqMyf
a6gn+KaddJnmIbXKFbrTaFii2IvRs3qHJ0mMVfYRnYeMql9/PhzvSftjRe32x/aQh23j9dCsVXmQ
ZmXpZyxxJ8p4RqyM0YgkfxnQXXtV9K0sRZPFn60+iszUw2hARRG/te0hTuVXpbonG2dT109JeeEe
S1E5uxenJvYkU7mMamvBjYQN6qVvyogf8F0lHTSfd6TDsK3QhmzOjg50PrBvvg5qE6OrxxNvqSVZ
ldhx/iHZAZ1yYSVdwizsZMCw0PjSwrRPx/h8l03djeW0aL5R1AF1qTFHVHNSNvigzh6FyjdkUJH66
JAYgPe0PKJFRgYzh5vWoJ41qvDj1Gk3c/zYi57MR1Bs0mkSvkOGbmjSsb+EehnYyLLB8FG3De2V
ZaXaHZ37gmoCNNmZHrn+GB0CAwEAAaOBkTCBjjAgBgNVHREEGTAXghVJU0UzMC0xZWsuZXhhbXBs
ZS5jb20wDAYDVDR0TBAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVDR0OBByEFPT/6jpfyugxRolbjzWJ
858wfTP1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjARBglghkgBhvhCAQEEBAMCBkAw
DQYJKoZIhvcNAQEMBQADggIBABGyWZbLajm2LyLASg//4N6mL+xu/9IMdVvNWBQodF+j0WusW15a
VPSQU2t3Ckd/I1anvpK+cp77NMjo9V9oWi3/ZnjZHGofAIcHn1GCoEjmc1TvLau7ZzhCCII37DFA
yMKDrXLi3pR+ONlX1TivjPHTTzrKm1NHhkkxkx/Js5Iuz+MyRKP8FNmWT0q4XGejyKzJWrqEu+bc1
idC1/gBNUCHgqmFem82IGQ7jVom1kBjLb4pTDbYk4fMIbJVh4V2Pgi++6MIfXAYEwL+LHjSGHCQT
PSM3+kpv1wHHpGWzQSmcJ4tXVXV95W0NC+LxQZLBPNUZorhuYCILXZxvXH1HGJJ0YKx91k9Ubd2
s5JaD+GN8jqm5XXAau7S4BawfvCo3bo0iXnSvGcIuh9YFiR2lp2n/2X0VVbdPHYZtqGieqBWebHr
4I1z18FXblYyMzpIkht00vkP5mAlR92VXBkvx2WPjtzQrvOtSXgvTCOKerYCBM/jnuwsztv7FVTV
JNdFwOsncX70YngZeujZyjPoUbfRKZI34VKZp4i05bZsG1bWE9Skdquv0PaQ8ecXTv8OCVBYUeg1
vt0pde18h/9jImdLG8dF0rbADGHiieTcntSDdw3E7JfMS/oHw7FsA5GI8IxXfcOWUx/L0Dx3jTND
ZlAXp4juySODIx9yDyM4yV0f
</ds:X509Certificate>
</ds:X509Data>
```

```
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=bd48c1
a1-9477-4746-8e40-e43d20c9f429"
ResponseLocation="https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action"/>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action" index="0"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://10.48.23.86:8445/sponsorportal/SSOLoginResponse.action" index="1"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://10.48.26.63:8445/sponsorportal/SSOLoginResponse.action" index="2"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://10.48.26.60:8445/sponsorportal/SSOLoginResponse.action" index="3"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://ise30-1ek.example.com:8445/sponsorportal/SSOLoginResponse.action" index="4"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action" index="5"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://ise30-3ek.example.com:8445/sponsorportal/SSOLoginResponse.action" index="6"/>
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

XMLファイルに従って、次の操作を行います。

SingleLogoutService

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

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

AssertionConsumerService

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

AssertionConsumerService

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

AssertionConsumerService

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

AssertionConsumerService

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

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

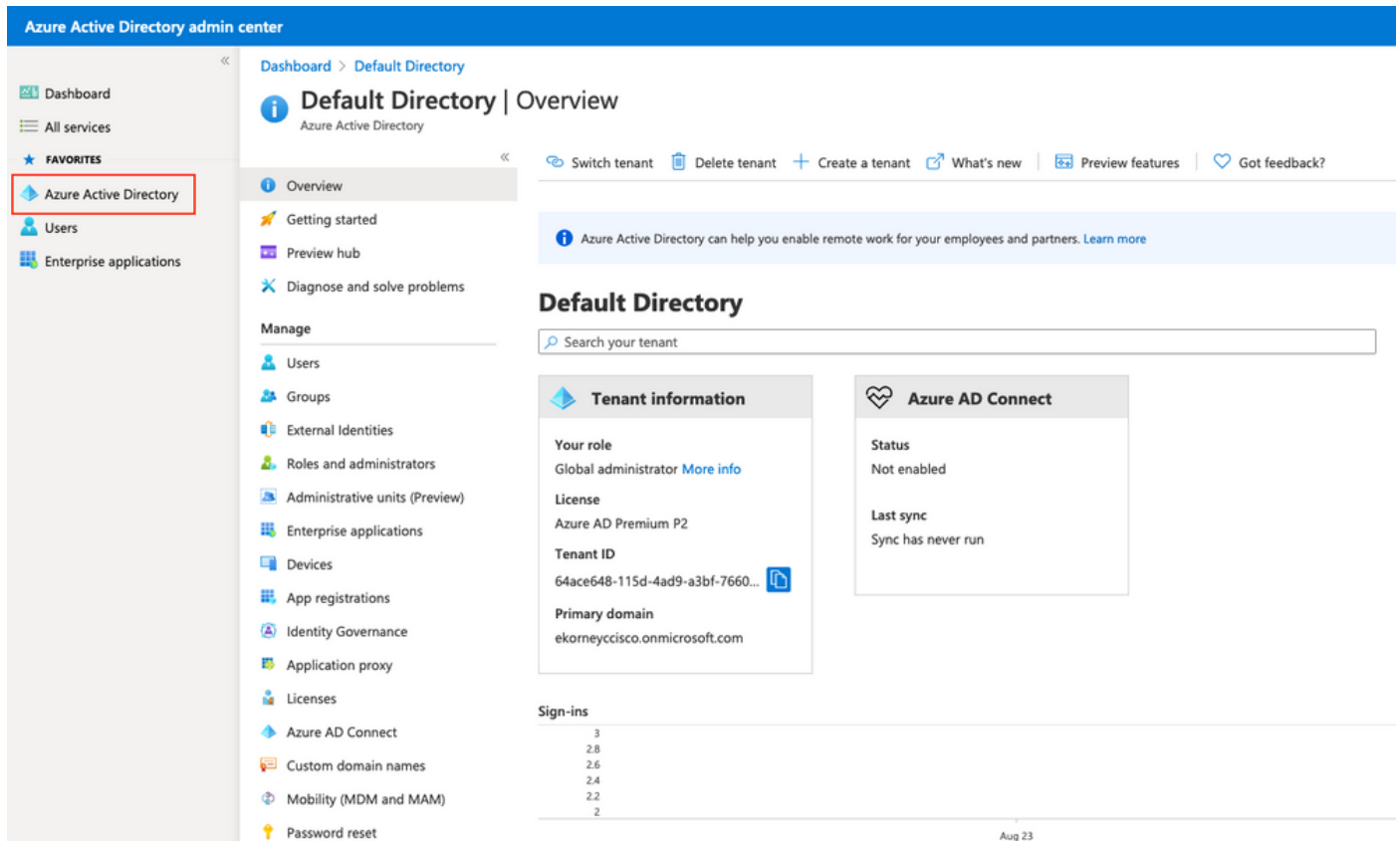
AssertionConsumerService Location="<https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action>"

AssertionConsumerService Location="

ステップ2: Azure AD IdPの設定

1. Azure ADユーザーの作成

Azure Active Directory Admin Center Dashboardにログインし、図に示すようにADを選択します
o



[Users]を選択し、[New User]をクリックし、[User name]、[Name]、および[Initial Password]を設定します。図に示すように[作成]をクリックします。

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

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. Azure ADグループの作成

グループを選択します。図に示すように[New Group]をクリックします。

Dashboard > Default Directory > Groups

Groups | All groups

Default Directory - Azure Active Directory

- All groups
- Deleted groups
- Diagnose and solve problems

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

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

[Add filters](#)

グループタイプを[セキュリティ]のままにしてください。図に示すようにグループ名を設定します

。

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. Azure ADユーザーをグループに割り当てる

[メンバーが選択されていません]をクリックします。ユーザーを選択し、「選択」をクリックします。[Create]をクリックし、ユーザが割り当てられたグループを作成します。

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

この画面では、スポンサーグループのグループオブジェクトidをメモします。

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. Azure ADエンタープライズアプリケーションの作成

図に示すように、[AD]の下で[Enterprise Applications]を選択し、[New application]をクリックします。

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
Applications status
Application visibility

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

図に示すようにギャラリー以外のアプリケーションを選択します。

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

アプリケーションの名前を入力し、「追加」をクリックします。

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.アプリケーションへのグループの追加

[ユーザーとグループの割り当て]を選択します。

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](#)

[Add user]をクリックします。

ISE30 | Users and groups

Enterprise Application

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

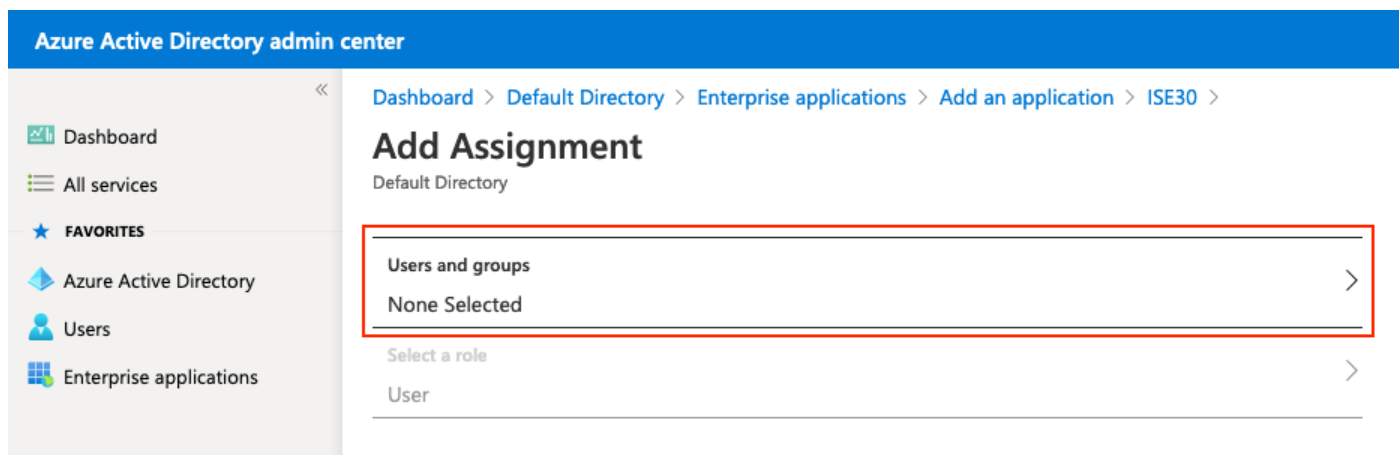
The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

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

Display Name

No application assignments found

[ユーザーとグループ]をクリックします。



Azure Active Directory admin center

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

Add Assignment

Default Directory

Users and groups >

None Selected

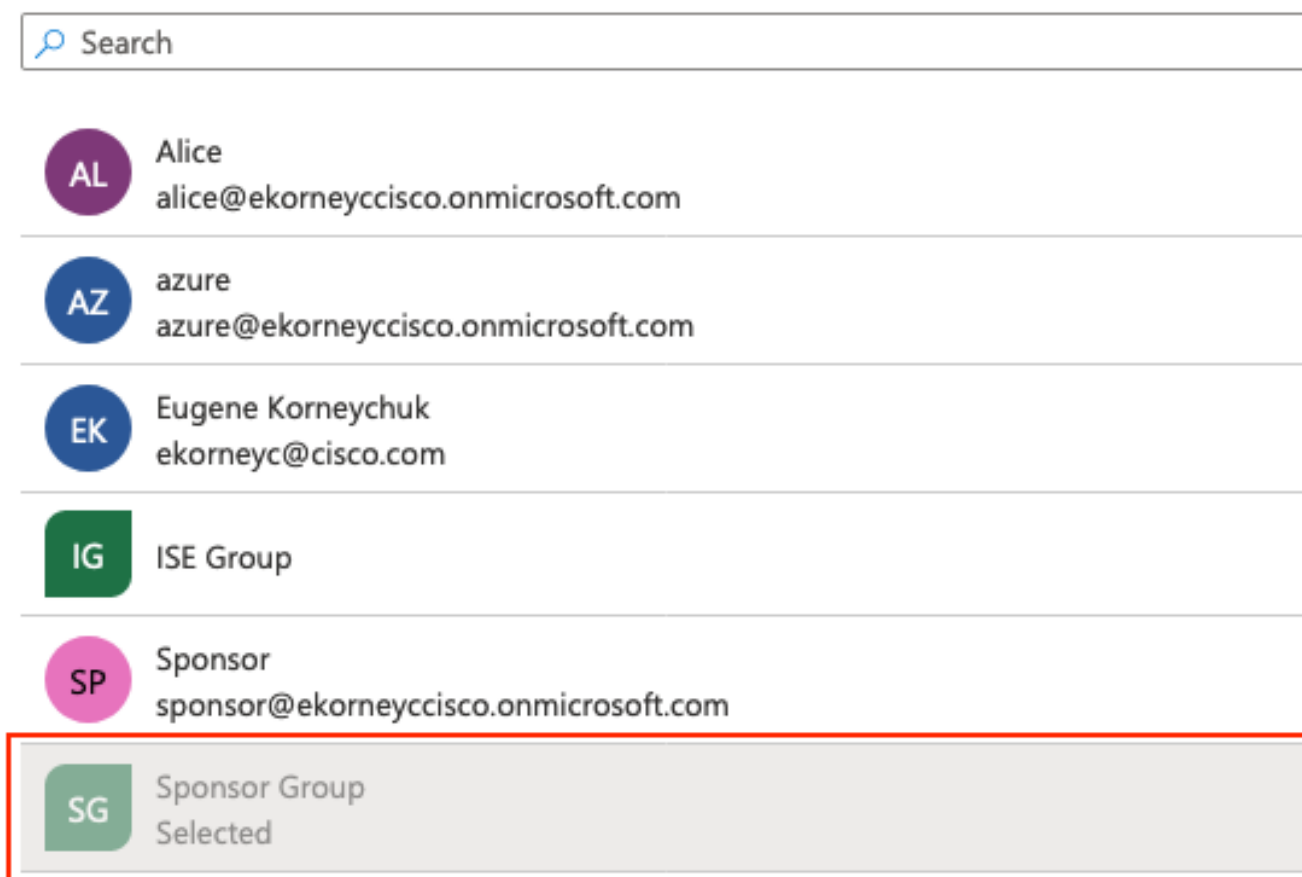
Select a role >

User

以前に設定したグループを選択し、[Select]をクリックします。

注：アクセス権を取得するユーザまたはグループの適切なセットを選択する必要があります。

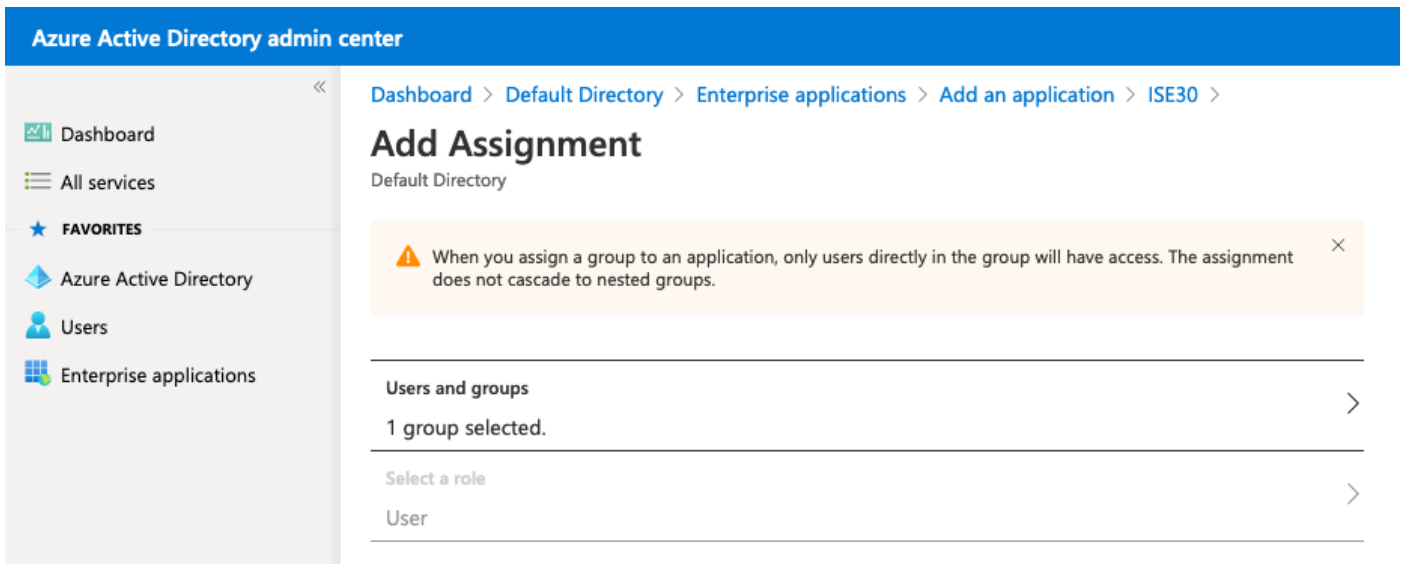
Users and groups



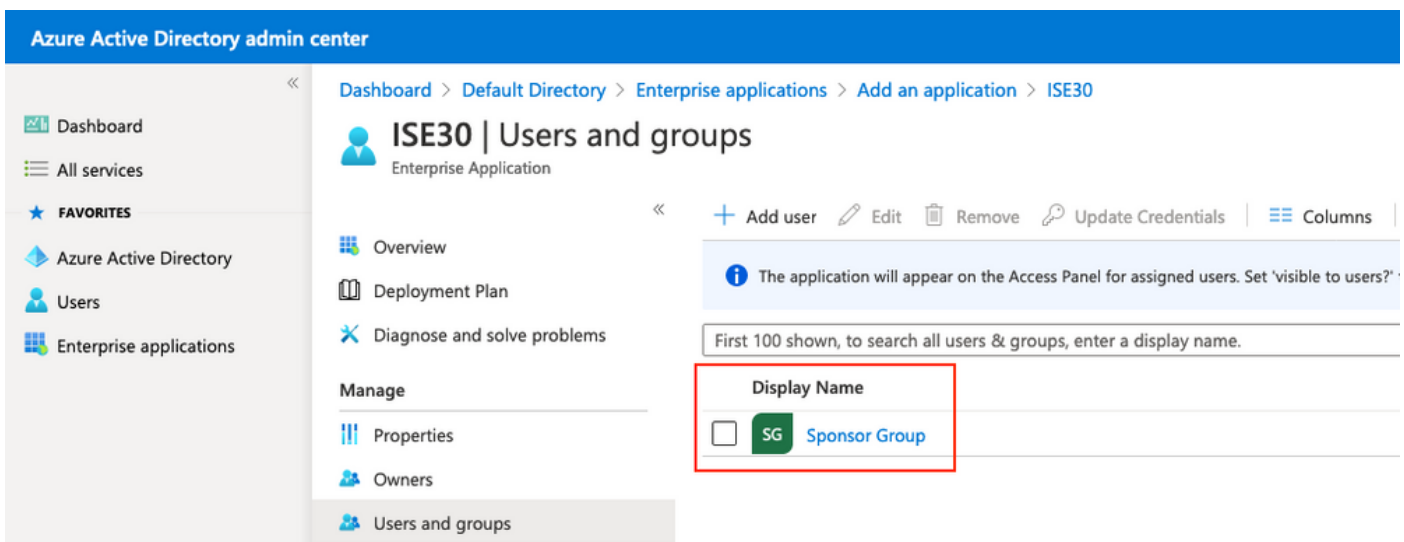
Search

- 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

グループを選択したら、図に示すように[割り当て]をクリックします。



その結果、アプリケーションの[ユーザーとグループ]メニューに、選択したグループが表示されま
す。



6. Azure ADエンタープライズアプリケーションの構成

アプリケーションに戻り、図に示すように[Set up single sign-on]をクリックします。

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](#)

次の画面で[SAML]を選択します。

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.

[Basic SAML Configuration]の横の[Edit]をクリックします。

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE30 >

ISE30 | SAML-based Sign-on

Enterprise Application

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

Set up Single Sign-On with SAML

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

- #### Basic SAML Configuration

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

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

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

ID (エンティティID) に、ステップ **Export Service Provider Information** のXMLファイルの **entityID** の値を入力します。AssertionConsumerServiceからのLocationsの値を返信URL (アサーションコンシューマサービスURL) に入力します。SingleLogoutServiceからLogout Urlの値にResponseLocationを入力します。[Save] をクリックします。

注：返信URLはパスリストとして機能し、特定のURLがIdPページにリダイレクトされたときにソースとして機能します。

Basic SAML Configuration



Save

Identifier (Entity ID) * ⓘ

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

Default

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

Reply URL (Assertion Consumer Service URL) * ⓘ

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

Default

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

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

7. Active Directoryグループ属性の設定

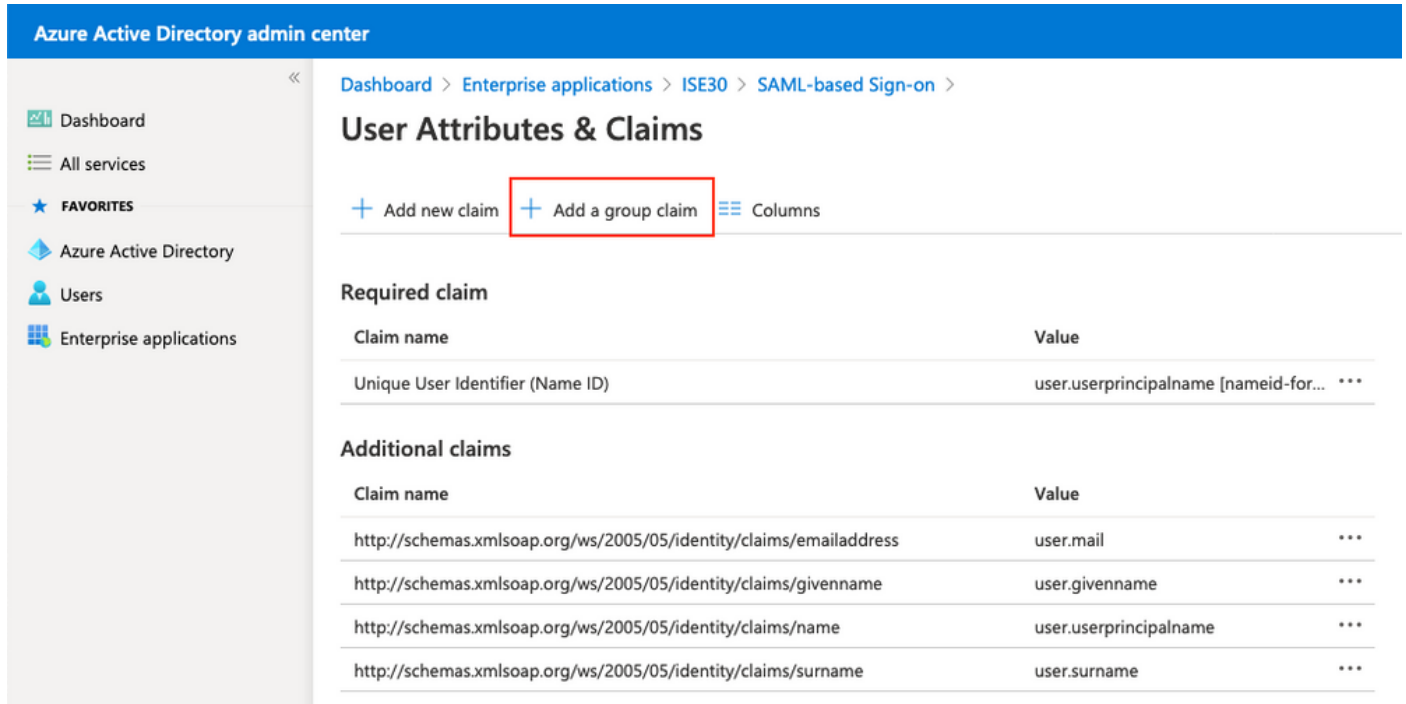
以前に設定したグループ属性値を返すには、[User Attributes & Claims]の横にある[Edit]をクリックします。

User Attributes & Claims



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

[Add a group claim]をクリックします。



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 ***

[セキュリティグループ]を選択し、[Save]をクリックします。assertionで返されるソース属性はグループIDで、以前にキャプチャしたグループオブジェクトIDです。

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

グループの要求名を書き留めます。この場合、これは <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups> です。

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. Azure FederationメタデータXMLファイルのダウンロード

SAML署名証明書の[Federation Metadata XML]に対して[Download]をクリックします。

SAML Signing Certificate

 Edit

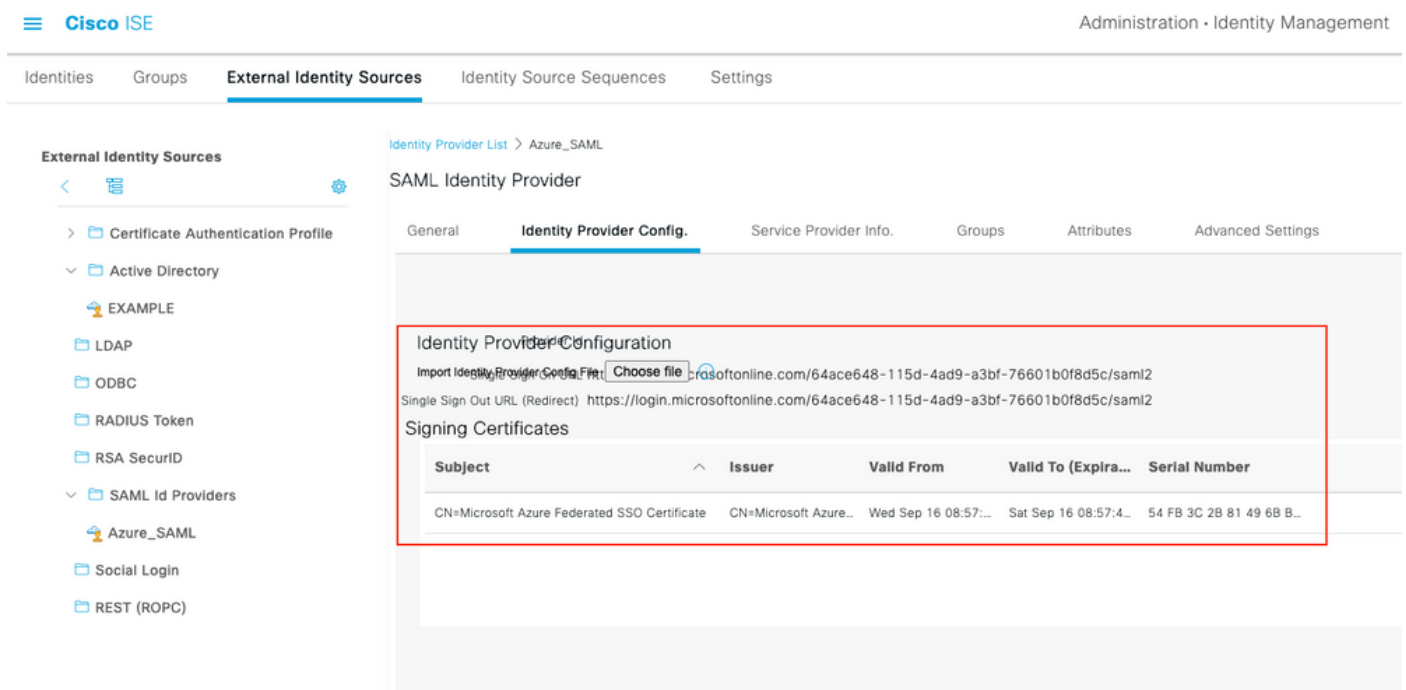
Status	Active
Thumbprint	9772DA460A43ACDA2AC5FBF09EE33ED7DAA7BAE2
Expiration	9/16/2023, 10:57:46 AM
Notification Email	ekorneyc@cisco.com
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/64ace648-115d ..."/>
Certificate (Base64)	Download
Certificate (Raw)	Download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

ステップ3: Azure Active DirectoryからISEへのメタデータのアップロード

[Administration] > [Identity Management] > [External Identity Sources] > [SAML Id Providers] > [Your SAML Provider]に移動します。

[IDプロバイダーの設定]タブに切り替え、[参照]ボタンをクリックします。手順「Azure Federation Metadata XMLのダウンロード」から「Federation Metadata XML file」を選択し、「Save」をクリックします。

注：IDプロバイダーの設定に関するUIエラーは、[CSCvv74517](#)で対処する必要があります。



The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > Identity Management > External Identity Sources > Identity Source Sequences > Settings. The left sidebar shows the 'External Identity Sources' tree with 'SAML Id Providers' expanded to 'Azure_SAML'. The main content area shows the 'SAML Identity Provider' configuration for 'Azure_SAML'. The 'Identity Provider Config.' tab is active, showing the 'Import Identity Provider Configuration File' button and the 'Signing Certificates' table. The table contains one certificate entry with the following details:

Subject	Issuer	Valid From	Valid To (Expira...	Serial Number
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azure...	Wed Sep 16 08:57:...	Sat Sep 16 08:57:4...	54 FB 3C 2B 81 49 6B B...

ステップ4: ISEでのSAMLグループの設定

[Groups]タブに切り替え、[Configure Active Directory Group]属性の[Claim name]の値を[Group Membership Attribute]に貼り付けます。

External Identity Sources

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

Identity Provider List > Azure_SAML

SAML Identity Provider

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

Groups

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

Name in Assertion

Name in ISE

No data available

[Add] をクリックします。アサーションの名前には、[Azure Active Directory Userをグループに割り当て]でキャプチャされたスポンサーグループのグループオブジェクトIDの値を入力してください。ISEで名前を設定し、この場合はAzure Sponsor Groupです。[OK] をクリックします。クリック保存

これにより、AzureのグループとISEで使用できるグループ名間のマッピングが作成されます。

Add Group

*Name in Assertion

*Name in ISE ⓘ

ステップ5: ISEでのスポンサーグループマッピングの設定

[Work Centers] > [Guest Access] > [Portals & Components] > [Sponsor Groups]に移動し、Azure ADグループにマップする[Sponsor Group]を選択します。この例では、ALL_ACCOUNTS (デフォルト) が使用されています。

Guest Portals

Guest Types

Sponsor Groups

Sponsor Portals

Sponsor Groups

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

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

Create Edit Duplicate Delete

Enabled	Name	Member Groups
<input checked="" type="checkbox"/>	ALL_ACCOUNTS (default) Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group. More	ALL_ACCOUNTS (default)
<input checked="" type="checkbox"/>	GROUP_ACCOUNTS (default) Sponsors assigned to this group can manage just the guest accounts created by sponsors from the same sponsor group. By default, users in the GROUP_ACCOUNTS user identity group are members of this sponsor group. More	GROUP_ACCOUNTS (default)
<input checked="" type="checkbox"/>	OWN_ACCOUNTS (default) Sponsors assigned to this group can manage only the guest accounts that they have created. By default, users in the OWN_ACCOUNTS user identity group are members of this sponsor group. More	OWN_ACCOUNTS (default)

メンバーをクリック... Azure_SAML:Azure Sponsor Groupを[Selected User Groups]に追加します。これにより、AzureのスポンサーグループがALL_ACCOUNTSスポンサーグループにマップされます。[OK]をクリックします。[Save] をクリックします。



Select Sponsor Group Members

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

Available User Groups

Selected User Groups

Name	
Employee	
GROUP_ACCOUNTS (default)	
OWN_ACCOUNTS (default)	

ALL_ACCOUNTS (default)
Azure_SAML:Azure Sponsor Group

確認

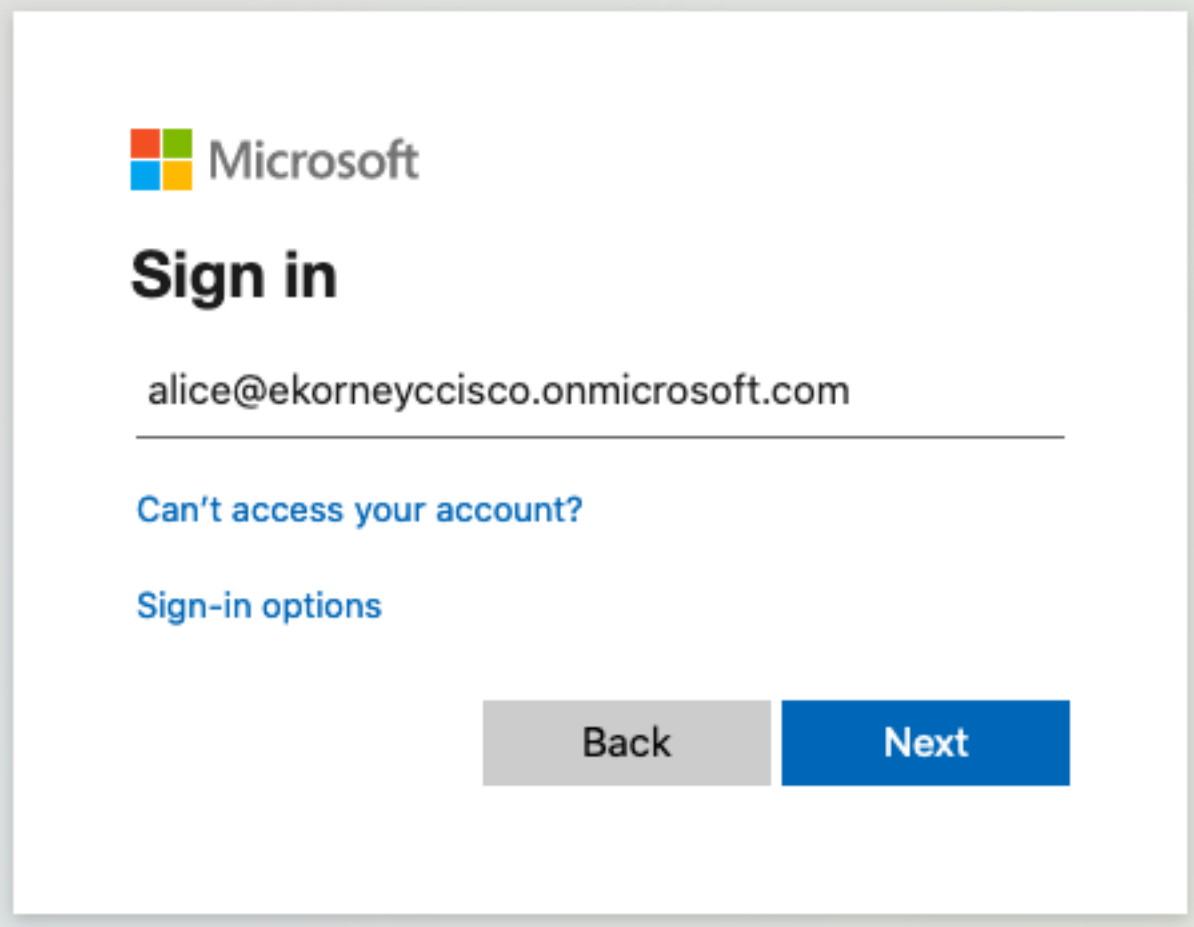
ここでは、設定が正常に機能しているかどうかを確認します。

注：新規ユーザは、最初のログイン時にユーザパスワードの変更を強制されます。AUPの検証手順は対象外です。検証では、ユーザが初めてログインせず、AUPがスポンサー（アリス）によって一度承認されたシナリオがカバーされます。

スポンサーポータルを開くと（たとえば、テストURLから）、Azureにリダイレクトされてサイ

ンインし、スポンサーポータルに戻ります。

1. [Portal Test URL]リンクで、FQDNを使用してスポンサーポータルを起動します。ISEから[Azure Sign In]ページにリダイレクトされます。以前に作成した**ユーザ名**を入力し、[Next]をクリックします。



Microsoft

Sign in

alice@ekorneyccisco.onmicrosoft.com

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

[Sign-in options](#)

Back Next

2.パスワードを入力し、「サインイン」をクリックします。IdPログイン画面は、ユーザを初期ISEのスポンサーポータルにリダイレクトします。



← alice@ekorneyccisco.onmicrosoft.com

Enter password

.....|

[Forgot my password](#)

Sign in

3. AUPを受け入れます。



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.この時点で、スポンサーユーザーはALL_ACCOUNTS Sponsorグループ権限を持つポータルに完全にアクセスできる必要があります。

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

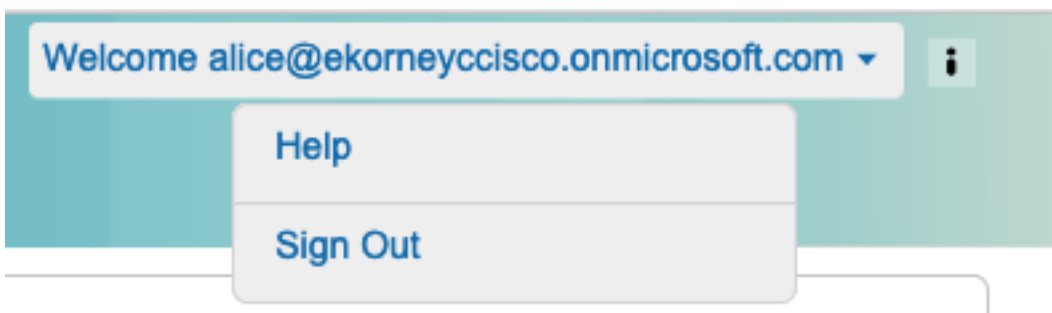
To Time *

10:22

Create

[Help](#)

5. [ようこそ]ドロップダウンメニューの下にある[サインアウト]をクリックします。



6. ユーザは正常にログアウトし、再度ログイン画面にリダイレクトされます。



Pick an account



alice@ekorneyccisco.onmicrosoft.co
m



Use another account

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

一般的な問題

ブラウザとAzure Active Directoryの間でSAML認証が処理されることを理解することが重要です。したがって、ISEエンゲージメントがまだ開始されていないアイデンティティプロバイダー (Azure) から認証関連のエラーを直接取得できます。

問題1：ユーザが誤ったパスワードを入力したため、ISEでユーザデータの処理が行われず、問題はIdP(Azure)から直接発生しています。修正するには、次の手順を実行します。パスワードをリセットするか、正しいパスワードデータを入力します。



← 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

問題2：ユーザはSAML SSOへのアクセスを許可されるグループに属していません。この場合も、ISEでユーザデータの処理が行われず、問題はIdP(Azure)から直接発生します。修正するには、次の手順を実行します。Add group to the **Application** configurationステップが正しく実行されていることを確認します。



Sign in

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

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

Troubleshooting details ×

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

[Copy info to clipboard](#)

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

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

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

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

Advanced diagnostics: [Enable](#)

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

3. Sing Out does not work as expected, this error - "SSO Logout failed.SSOセッションからログアウトするときに問題が発生しました。ヘルプデスクにお問い合わせください。" SAML IdPでサインアウトURLが正しく設定されていない場合に表示されます。この場合、このURLは「<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2>」で、「<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action>」を修正するために使用されます。Azure IdPの[Logout URL]に正しいURLを入力します。

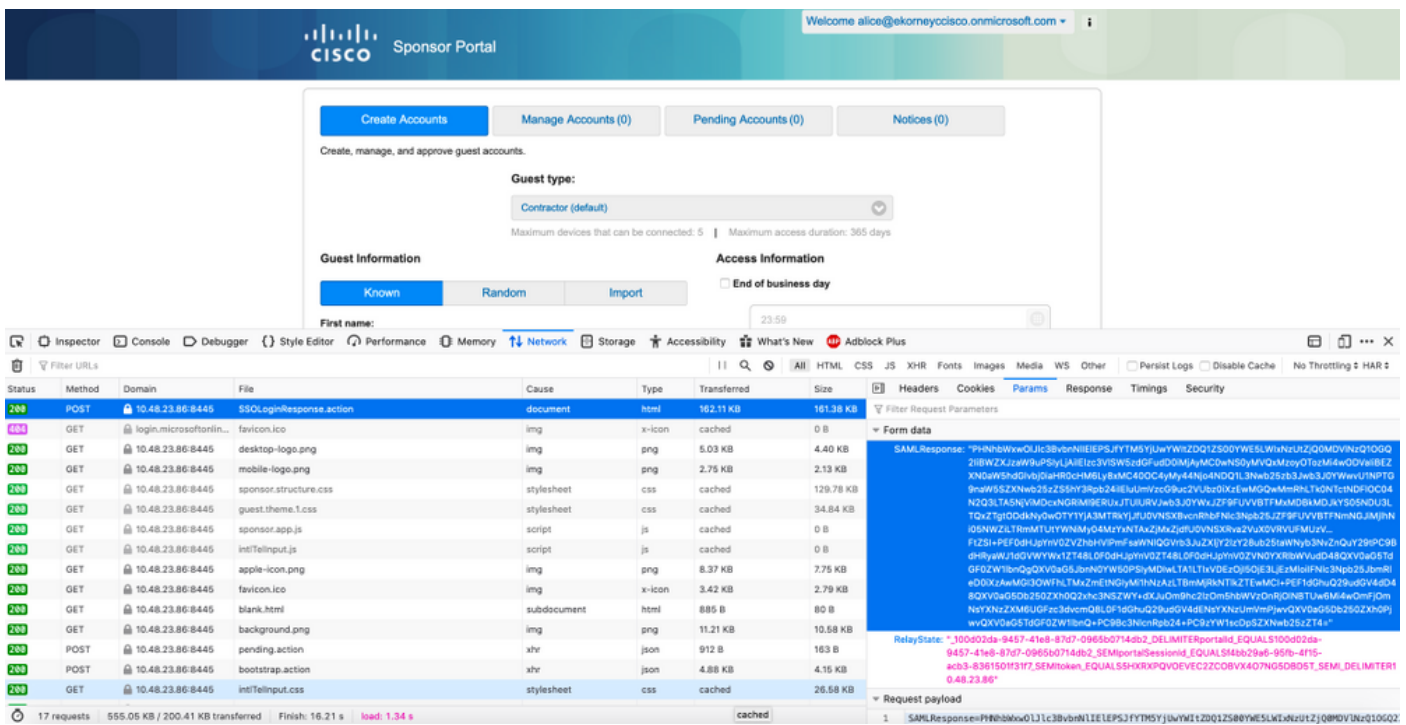
Error

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

[Help](#)

クライアントのトラブルシューティング

SAMLペイロードが受信されたことを確認するには、Web Developer Toolsを使用できます。Firefoxを使用し、Azureの資格情報を使用してポータルにログインする場合は、[ツール] > [Web開発者] > [ネットワーク]に移動します。暗号化されたSAML応答は、[Params]タブで確認できます。



ISEのトラブルシューティング

ここで使用するコンポーネントのログレベルは、ISEで変更する必要があります。[Operations] > [Troubleshoot] > [Debug Wizard] > [Debug Log Configuration]に移動します。

コンポーネント名	ログレベル	ログファイル名
ゲストアクセス	デバッグ	guest.log
portal-web-action	デバッグ	guest.log
opensaml	デバッグ	ise-psc.log
saml	デバッグ	ise-psc.log

正しいフロー実行時の一連のデバッグ(ise-psc.log):

1.ユーザはスポンサーポータルからIdP URLにリダイレクトされます。

```
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.ブラウザからSAML応答を受信します。

```
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 (アサーション) 解析が開始されます。

```
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.グループ属性は、f626733b-eb37-4cf2-b2a6-c2895fd5f4d3の値で受け取られます。

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

5.ユーザグループは認証結果に追加されるため、ポータルで使用でき、SAML認証が渡されます。

```
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.サインアウトがトリガーされます。ログアウトURLは、SAML応答
(<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action>)で受信します。**

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

```
getSignLogoutRequest - null
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - loginInfo:SAMLLoginInfo: name=alice@ekorneyccisco.onmicrosoft.com,
format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress, sessionIndex=_4b798ec4-9aeb-40dc-
8bed-6dd2fdd46800, time diff=26329
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
SAMLUtils::isLoadBalancerConfigured() - LB NOT configured for: Azure_SAML
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:-
SAMLUtils::isOracle() - checking whether IDP URL indicates that its OAM. IDP URL:
https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.SAMLFacadeImpl -:::alice@ekorneyccisco.onmicrosoft.com:- SPPProviderId
for Azure_SAML is: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - spProviderId:http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:51,463 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.MessageComposer -:::alice@ekorneyccisco.onmicrosoft.com:-
buildLogoutRequest - logoutURL:https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-
76601b0f8d5c/saml2
2020-09-16 10:44:53,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML HTTPRequest - Portal ID:bd48c1a1-9477-4746-
8e40-e43d20c9f429
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML response - Relay State:_bd48c1a1-9477-4746-
8e40-e43d20c9f429_DELIMITER8fa19bf2-9fa6-4892-b082-5cdabfb5daa1_DELIMITERsponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML flow initiator PSN's Host name
is:sponsor30.example.com
2020-09-16 10:44:53,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- Is redirect required:
InitiatorPSN:sponsor30.example.com This node's host name:ISE30-1ek 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
```