

# 使用Azure AD SAML SSO配置ISE 3.0發起人門戶

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[高級流程圖](#)

[設定](#)

[步驟1.在ISE上配置SAML身份提供者和發起人門戶](#)

[1.將Azure AD配置為外部SAML標識源](#)

[2.配置發起人門戶以使用Azure AD](#)

[3.匯出服務提供商資訊](#)

[步驟2.配置Azure AD IdP設定](#)

[1.建立Azure AD使用者](#)

[2.建立Azure AD組](#)

[3.將Azure AD使用者分配給組](#)

[4.建立Azure AD Enterprise應用程式](#)

[5.將組新增到應用程式](#)

[6.配置Azure AD Enterprise應用程式](#)

[7.配置Active Directory組屬性](#)

[8.下載Azure聯合後設資料XML檔案](#)

[步驟3.將後設資料從Azure Active Directory上載到ISE](#)

[步驟4.在ISE上配置SAML組](#)

[步驟5.在ISE上配置發起人組對映](#)

[驗證](#)

[疑難排解](#)

[常見問題](#)

[客戶端故障排除](#)

[ISE故障排除](#)

## 簡介

本文檔介紹如何使用思科身份服務引擎(ISE)3.0配置Azure Active Directory(AD)SAML伺服器，為發起人使用者提供單一登入(SSO)功能。

## 必要條件

### 需求

思科建議您瞭解以下主題：

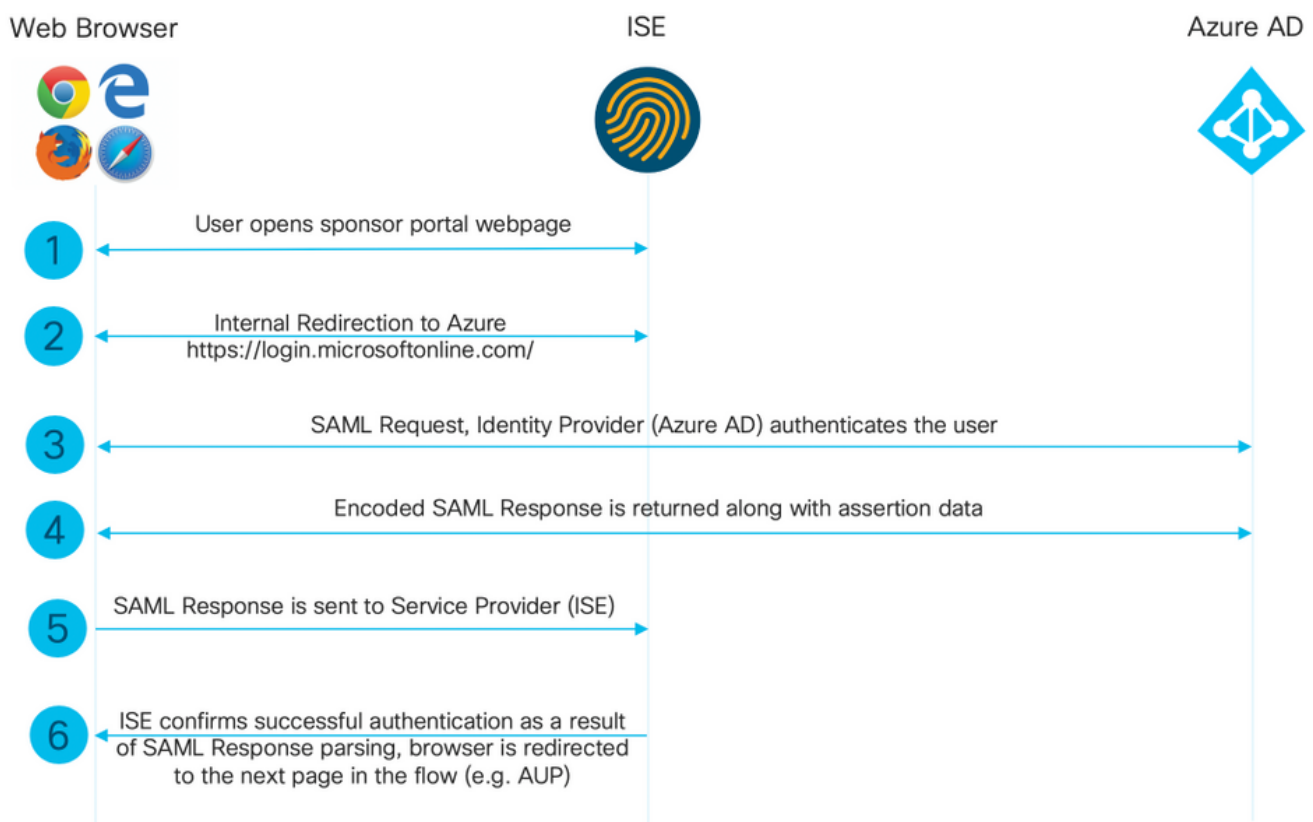
1. Cisco ISE 3.0
2. 有關SAML SSO部署的基本知識
3. Azure AD

## 採用元件

1. Cisco ISE 3.0
2. Azure AD

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 高級流程圖



## 設定



### 步驟1.在ISE上配置SAML身份提供者和發起人門戶

#### 1.將Azure AD配置為外部SAML標識源

在ISE上，導航到**Administration > Identity Management > External Identity Sources > SAML Id Providers**，然後點選**Add**按鈕。

輸入**Id Provider Name**，然後按一下**Submit**儲存它。**Id Provider Name**僅對ISE有效，如下圖所示。

## 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 &gt; New Identity Provider

## SAML Identity Provider

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

* Id Provider Name	Azure_SAML
Description	Azure Active Directory

## 2. 配置發起人門戶以使用Azure AD

導航至工作中心>訪客接入>門戶和元件>發起人門戶，然後選擇發起人門戶。在此示例中使用發起人門戶（預設）。

展開Portal Settings面板，然後在Identity source序列中選擇您的新SAML IdP。為發起人門戶配置完全限定域名(FQDN)。在本例中，它是sponsor30.example.com。按一下「Save」，如下圖所示。

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: \*

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 type="checkbox"/> Gigabit Ethernet 1 <input type="checkbox"/> Gigabit Ethernet 2 <input type="checkbox"/> Gigabit Ethernet 3 <input type="checkbox"/> Gigabit Ethernet 4 <input type="checkbox"/> Gigabit Ethernet 5	<input checked="" type="checkbox"/> Bond 0 <small>Uses Gigabit Ethernet 0 as primary, 1 as backup.</small> <input type="checkbox"/> Bond 1 <small>Uses Gigabit Ethernet 2 as primary, 3 as backup.</small> <input type="checkbox"/> Bond 2 <small>Uses Gigabit Ethernet 4 as primary, 5 as backup.</small>

Certificate group tag: \*

Configure certificates at:

[Work Centers > Guest Access > Administration > System Certificates](#)

Fully qualified domain names (FQDN) and host names:

Identity source sequence: \*

Configure authentication methods at:

[Work Centers > Guest Access > Identities > Identity Source Sequences](#)

[Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers](#)

### 3. 匯出服務提供商資訊

導航到管理>身份管理>外部身份源> SAML Id提供程式> [您的SAML提供程式]。

切換到Service Provider Info頁籤。然後按一下Export按鈕，如下圖所示。

[Identity Provider List](#) > Azure\_SAML

#### SAML Identity Provider

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

Service Provider Information

Load balancer (i)

Export Service Provider Info. (i)

**Export**

Includes the following portals:

Sponsor Portal (default)

下載並儲存該zip檔案。您可以在其中找到2個檔案。您需要稱為發起人門戶的XML檔案。

請記下來自SingleLogoutService Bindings的ResponseLocation、entityID值以及AssertionConsumerServiceBinding的Location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>
MIIFZjCCA06gAwIBAgIQX1oAvwAAAAChgVd9cEEW0zANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQOD
ExpTQU1MX01TRTMwLTF1ay5leGFtcGxlLmNvbTAeFw0yMDA5MTAxMDMyMzFaFw0yNTA5MDkxMDMy
MzFaMCUxIzAhBgNVBAMTG1NBTVUxfsVNFmZAtMwVrLmV4Yw1wbGUuY29tMIICiIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICGKCAgEAT+MixKfuZvg/oAWGES6zrUYL3H2JwvZw9yJs6sJ8/BpP6Sw027wh
FXnESXpqqmSVrVcQIrDdk318UYNn/+98PPkIi/4ftyFjZK9YdeverD6nrA2MeoLCzG1kWq/y4i
vvVcYuw344pySm65awVvro3q84x9esHqyLahExs9guiLJryD497XmNP4Z8eTHCctu777PuI1wLO4
QOYUs2sozXvR98D9Jok/+PjH3bjmVKapqAcNEFvk8Ez9x1sMBUgFwP4YdZzQB9IRVqQdIJGvqMyf
a6gn+KaddJnmIbXKFbrTaFiI2IvRs3qHJ0mMVfYRnYeMq19/PhzvSFtjRe32x/aQh23j9dCsVXmQ
ZmXpZyxxJ8p4RqyM0YgkfxnQXXtV9K0sRZPFn60+iszUw2hARRG/te0hTuVXpbonG2dT109JeeEe
S1E5uxenJvYkU7mMamvBjYQN6qVyyogf8F01HTSfd6TDsK3Qhmz0jg50PrBvvg5qE6OrxxNvqSVZ
ldhx/iHZA21yYSvdwizsZMCw0PjSwrRPx/h8103djeW0aL5R1AF1qTFHVHSNvigzh6FyjJkUJH66
JAYgPe0PKJFRgYzh5vWoJ41qvDqJlGk3c/zYi57MR1Bs0mkSvkOGbmjSsb+EehnYyLLB8FG3De2V
ZaXaH237gmoCNNmZHRn+GB0CAwEAAaOBkTCBjjAgBgNVHREETAXghVJU0UzMC0xZWsuZXhhbXBs
ZS5jb20wDAYDVROTBAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVR0OBByEFPt/6jpfyugxRolbjzWJ
858WfTP1MB0GA1UdJQQWMBQGCCsGAQUFBWMBBggrBgEFBQcDAjARBglghkgBhvhCAQEEBAMCBkAw
DQYJKoZIhvcNAQEMQADggIBABGyWZbLajm2LyLASg//4N6mL+xu/9IMdVvNWBQodF+j0WusW15a
VPSQU2t3Ckd/I1anvpK+cp77NMj09V9oWI3/ZnjZHGofAICHNlGCoEjmC1TvLau7ZzhCCII37DFA
yMKDrXLi3pR+ONLX1TivjPHTTzrKmlNHhkxkx/Js5Iuz+MyRKP8FNmWT0q4XGejyKzJWqrEu+bc1
idC1/gBNUcHGqmFeM82IGQ7jvOm1kBjLb4pTDbYk4fMIbJVh4V2Pgi++6MIfXAYEWL+LHjSGHCQT
PSM3+kpvlwHHpGWzQSmcJ4tXVXV95W0NC+LxQZLBPNUZorhuYCILXZxvXH1HGJJ0YKx91k9Ubd2
s5JaD+GN8jqm5XXAau7S4BawfvCo3boOiXnSvgtuH9YFiR2lp2n/2X0VVbdPHYZtqGieqBWebHr
4I1z18FXblYyMzpIkhtOOvkP5mAlR92VXBkvx2WPjtzQrvOtSXgvTCOKerYCBM/jnuwsztv7FVTV
JNdFwOsnaXC70YngZeujZyjPoUbfRKZI34VKZp4i05bZsG1bWE9Skdquv0PaQ8ecXTv8OCVBYUegl
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>
</md: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>
```

根據XML檔案：

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

## 步驟2.配置Azure AD IdP設定

### 1.建立Azure AD使用者

登入到Azure Active Directory管理中心儀表板並選擇你的AD，如下圖所示。

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

選擇Users，按一下New User，配置User name、Name和Initial Password。按一下「Create」，如下圖所示。

- 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. 建立 Azure AD 組

選擇組。按一下「New Group」，如下圖所示。

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](#)

將組型別保留為安全。設定群組名稱，如下圖所示。



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.將Azure AD使用者分配給組

按一下No members selected。選擇使用者並按一下Select。按一下Create以建立已為其分配「使用者」的組。

# 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

記下Group Object id，在此螢幕中，發起人組為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. 建立 Azure AD Enterprise 應用程式

在 AD 下，選擇 Enterprise Applications，然後按一下 New application，如下圖所示。

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.

選擇 Non-gallery 應用程式，如下圖所示。

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

輸入應用程式的名稱，然後按一下 Add。

## 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.將組新增到應用程式

選擇分配使用者和組。

## 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](#)

按一下Add user。

## ISE30 | Users and groups

Enterprise Application

+ Add user

Edit

Remove

Update Credentials

Columns

Got feedback?

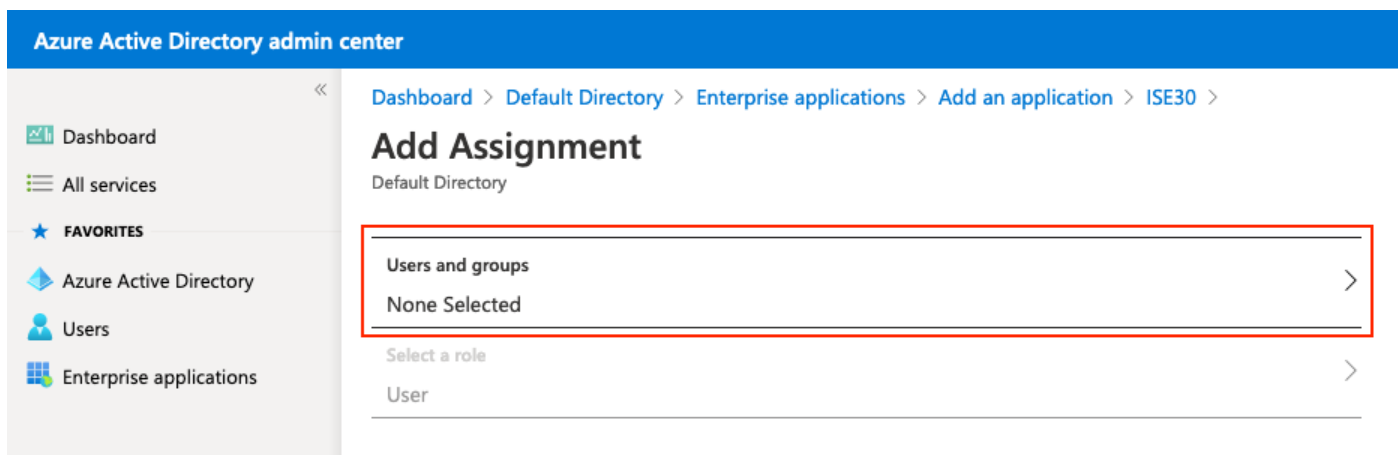
The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

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

Display Name

No application assignments found

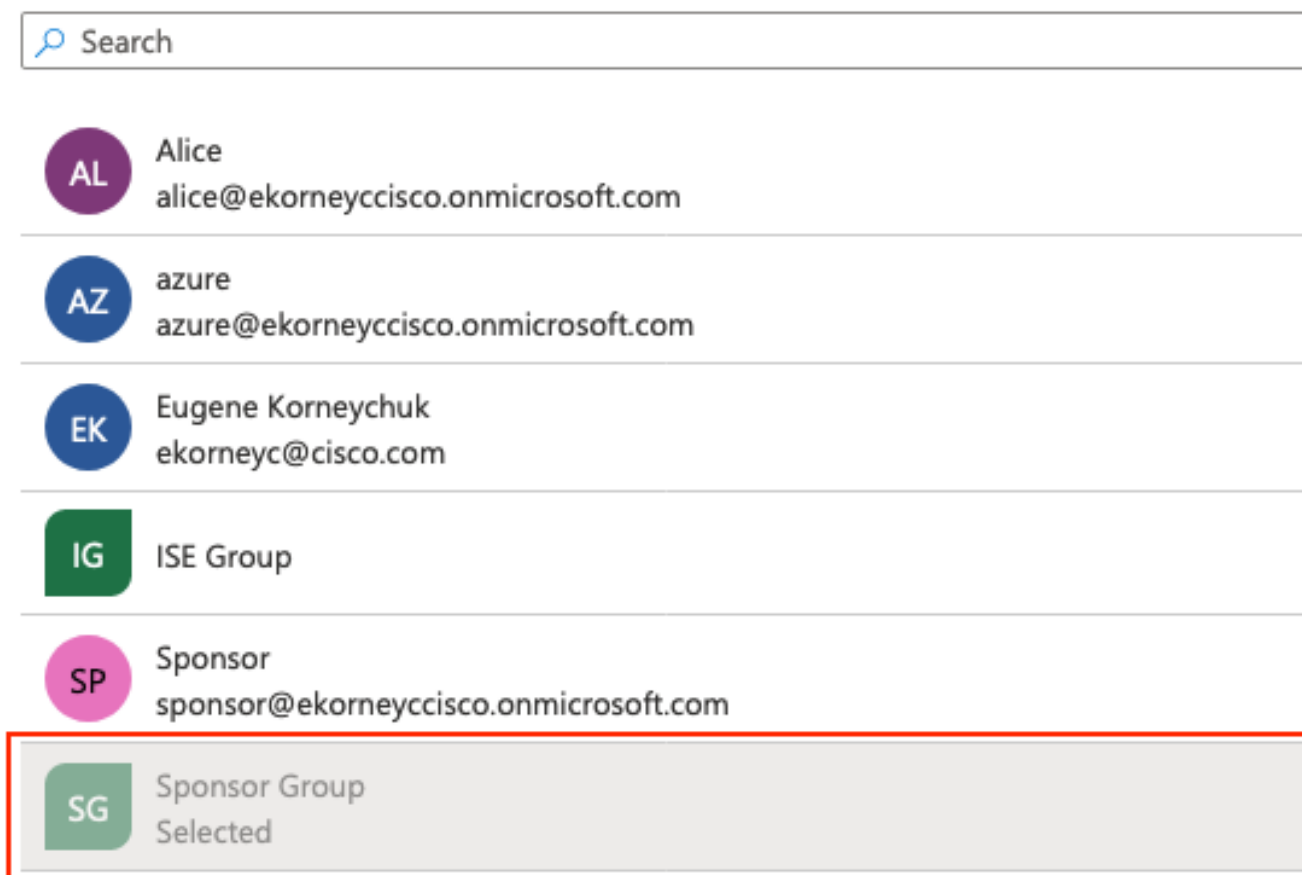
按一下Users and groups。



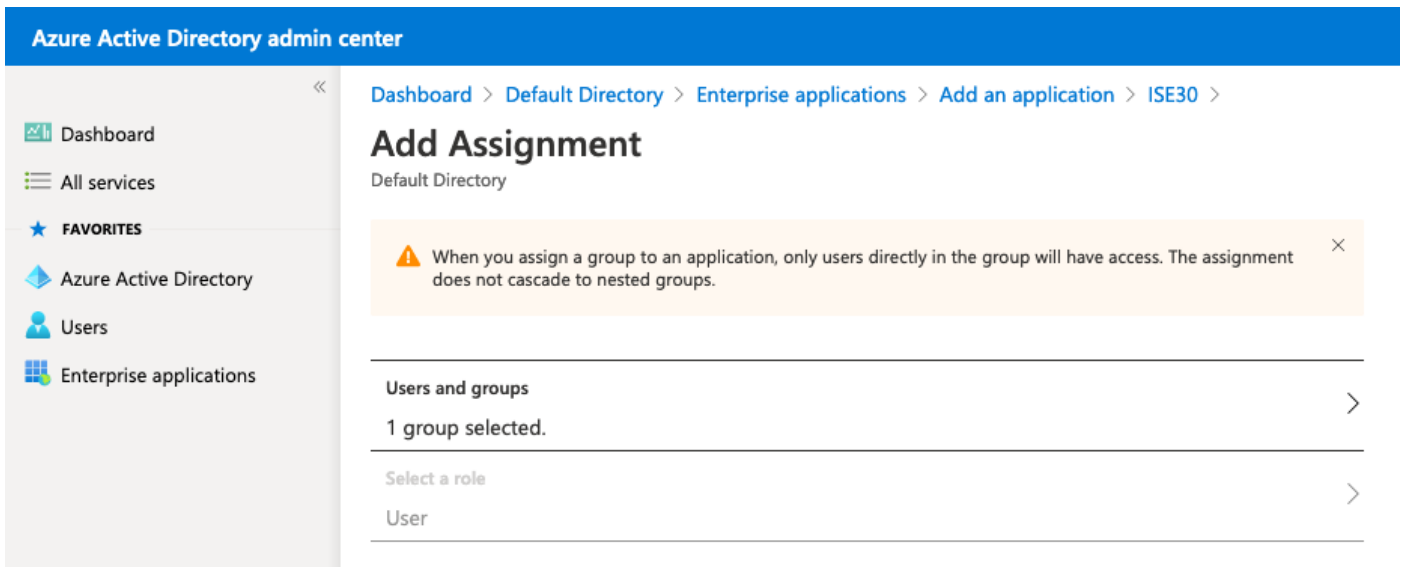
選擇先前配置的組，然後按一下**選擇**。

**附註：** 由您選擇應獲得訪問許可權的正確使用者或組。

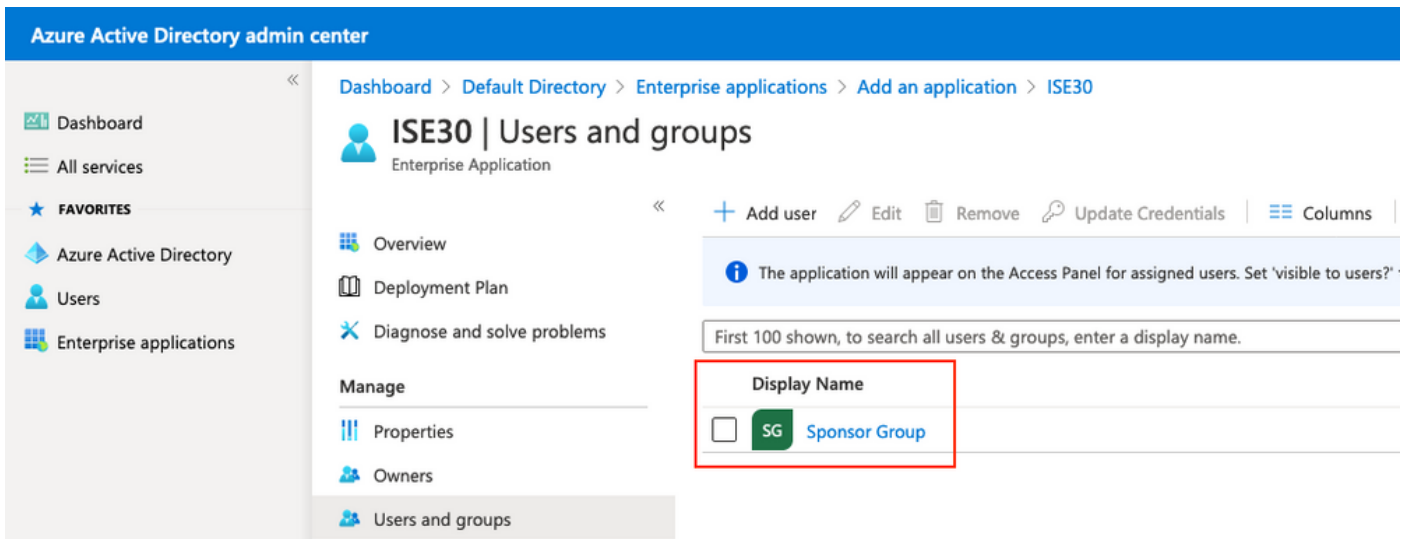
## Users and groups



選擇組後，按一下**Assign**，如下圖所示。



因此，應用程式的「用戶和組」選單應使用所選組進行填充。



## 6. 配置 Azure AD Enterprise 應用程式

導覽回您的應用程式，然後按一下 **Set up single sign-on**，如下圖所示。

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](#)

在下一個螢幕上選擇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.

按一下Basic SAML Configuration旁邊的Edit。

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)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- ### User Attributes & Claims

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

在步驟匯出服務提供商資訊中，使用XML檔案中的entityID值填充識別符號（實體ID）。使用AssertionConsumerService中的Locations值填充Reply URL(Assertion Consumer Service URL)。使用ResponseLocation 填充註銷Url值(來自SingleLogoutService)。按一下Save。

附註：回覆URL用作傳遞清單，允許某些URL在重定向到IdP頁面時用作源。



# 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 checked="" type="checkbox"/>	ⓘ	
<input type="text"/>			

## Sign on URL ⓘ

## Relay State ⓘ

## Logout Url ⓘ

## 7.配置Active Directory組屬性

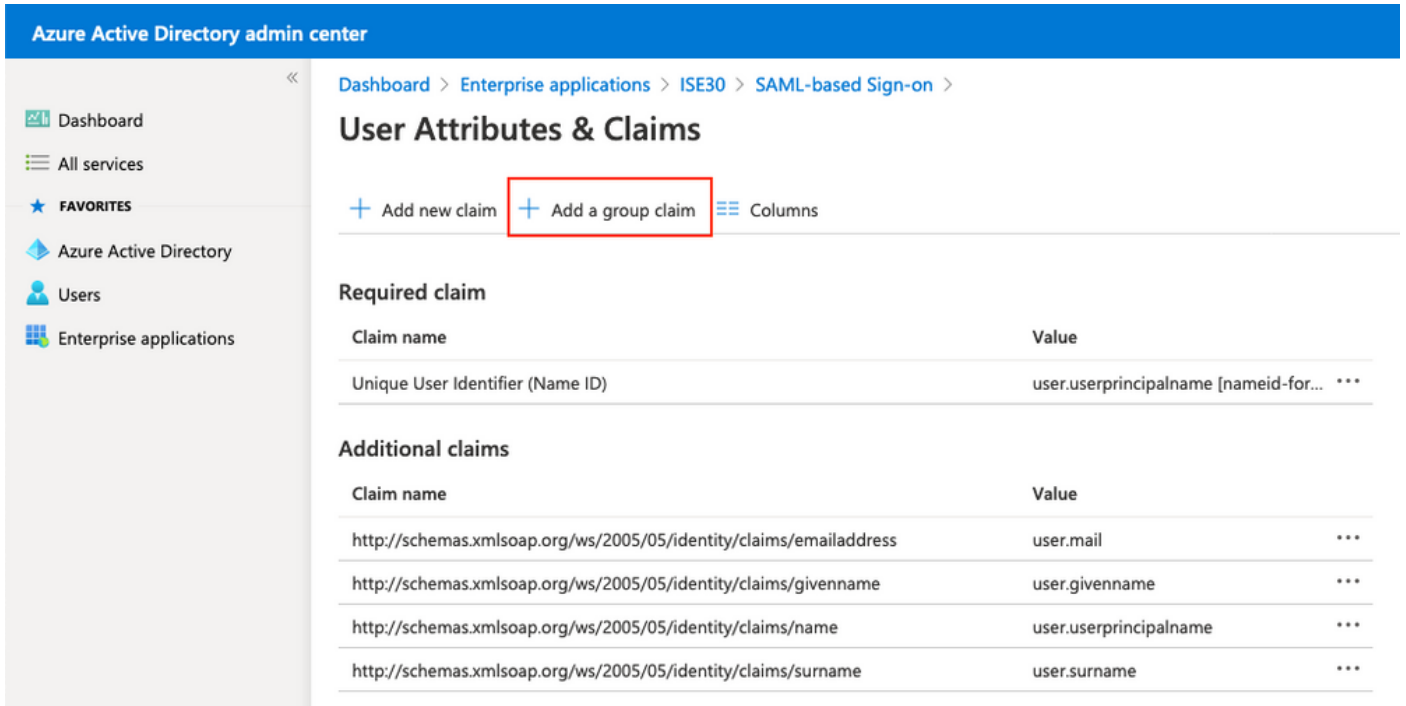
要返回先前配置的組屬性值，請按一下**使用者屬性和宣告**旁邊的**編輯**。

## User Attributes & Claims



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

按一下Add a group claim。



Azure Active Directory admin center

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

### User Attributes & Claims

+ Add new claim + Add a group claim Columns

**Required claim**

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

**Additional claims**

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

選擇Security groups，然後按一下Save。斷言中返回的Source屬性是組ID，它是之前獲取的組對象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

記下組的申請名稱。在本例中，它是  
<http://schemas.microsoft.com/ws/2008/06/identity/claims/groups>。

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area is titled 'User Attributes & Claims' and includes options to 'Add new claim', 'Add a group claim', and 'Columns'. Under 'Required claim', there is a table with one entry: 'Unique User Identifier (Name ID)' with value 'user.userprincipalname [nameid-for... \*\*\*]'. Under 'Additional claims', there is a table with five entries. The first entry is highlighted with a red box: 'http://schemas.microsoft.com/ws/2008/06/identity/claims/groups' with value 'user.groups [SecurityGroup] \*\*\*'. The other entries are: '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), and 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' (user.surname).

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***]
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. 下載 Azure 聯合後設資料 XML 檔案

在 SAML 簽名證書中按一下 **Download on Federation Metadata XML**。

## SAML Signing Certificate

 Edit

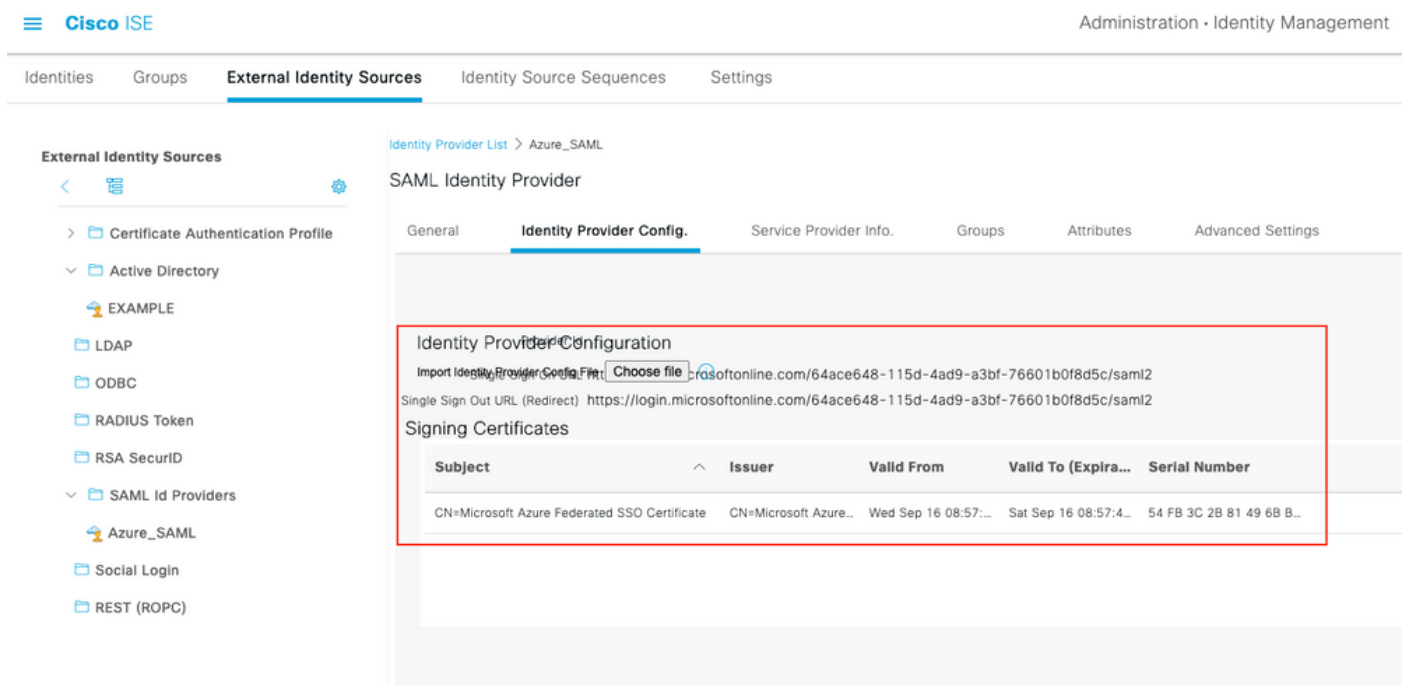
Status	Active
Thumbprint	9772DA460A43ACDA2AC5FBF09EE33ED7DAA7BAE2
Expiration	9/16/2023, 10:57:46 AM
Notification Email	ekorneyc@cisco.com
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/64ace648-115d ..."/>
Certificate (Base64)	<a href="#">Download</a>
Certificate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

### 步驟3.將後設資料從Azure Active Directory上載到ISE

導航到**管理>身份管理>外部身份源> SAML Id提供程式> [您的SAML提供程式]**。

切換到**Identity Provider Config**頁籤，然後按一下**Browse**按鈕。從下載Azure聯合後設資料XML步驟中選擇「**聯合後設資料XML檔案**」，然後按一下「**儲存**」。

**附註：** 身份提供程式配置的使用者介面問題應在[CSCvv74517](#)下解決。



The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is "Administration > Identity Management > External Identity Sources > Identity Source Sequences > Settings > SAML Identity Provider". The "Identity Provider Config." tab is selected. The "Import Identity Provider Configuration" section has a "Choose file" button highlighted with a red box. Below it, the "Signing Certificates" table is visible, with one certificate entry highlighted by a red box:

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...

### 步驟4.在ISE上配置SAML組

切換到頁籤**Groups**，並將**Claim name**的值從**Configure Active Directory Group attribute** 貼上到**Group Membership Attribute**中。

## External Identity Sources

- < 外部身份源
- > Certificate Authentication Profile
- > Active Directory
  - EXAMPLE
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers
  - Azure\_SAML
  - Social Login
  - REST (ROPC)

Identity Provider List &gt; 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

按一下「Add」。使用將Azure Active Directory使用者分配給組時捕獲的發起人組的組對象ID值填充Assertion中的Name。在ISE中配置具有有意義值的名稱，在這種情況下為Azure發起人組。按一下「OK」（確定）。按一下 儲存。

這會在Azure中的組與可在ISE上使用的組名稱之間建立對映。

### Add Group

\*Name in Assertion

\*Name in ISE  ⓘ

## 步驟5.在ISE上配置發起人組對映

導航到工作中心>訪客訪問>門戶和元件>發起人組，然後選擇要對映到Azure AD組的發起人組。在此示例中，使用了ALL\_ACCOUNTS（預設值）。

Guest Portals

Guest Types

**Sponsor Groups**

Sponsor Portals

## Sponsor Groups

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

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

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

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

**ALL\_ACCOUNTS (default)**

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

[More](#)

ALL\_ACCOUNTS (default)

**GROUP\_ACCOUNTS (default)**

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

[More](#)

GROUP\_ACCOUNTS (default)

**OWN\_ACCOUNTS (default)**

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

[More](#)

OWN\_ACCOUNTS (default)

按一下**成員**..... 並將**Azure\_SAML:Azure發起人組**新增到所選使用者組。這會將Azure中的發起人組對映到**ALL\_ACCOUNTS**發起人組。按一下**OK**。按一下**Save**。



# Select Sponsor Group Members

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

### Available User Groups

  
  
  
**Name** ^  
Employee  
GROUP\_ACCOUNTS (default)  
OWN\_ACCOUNTS (default)

### Selected User Groups

  
  
  
**Name** ^  
ALL\_ACCOUNTS (default)  
Azure\_SAML:Azure Sponsor Group

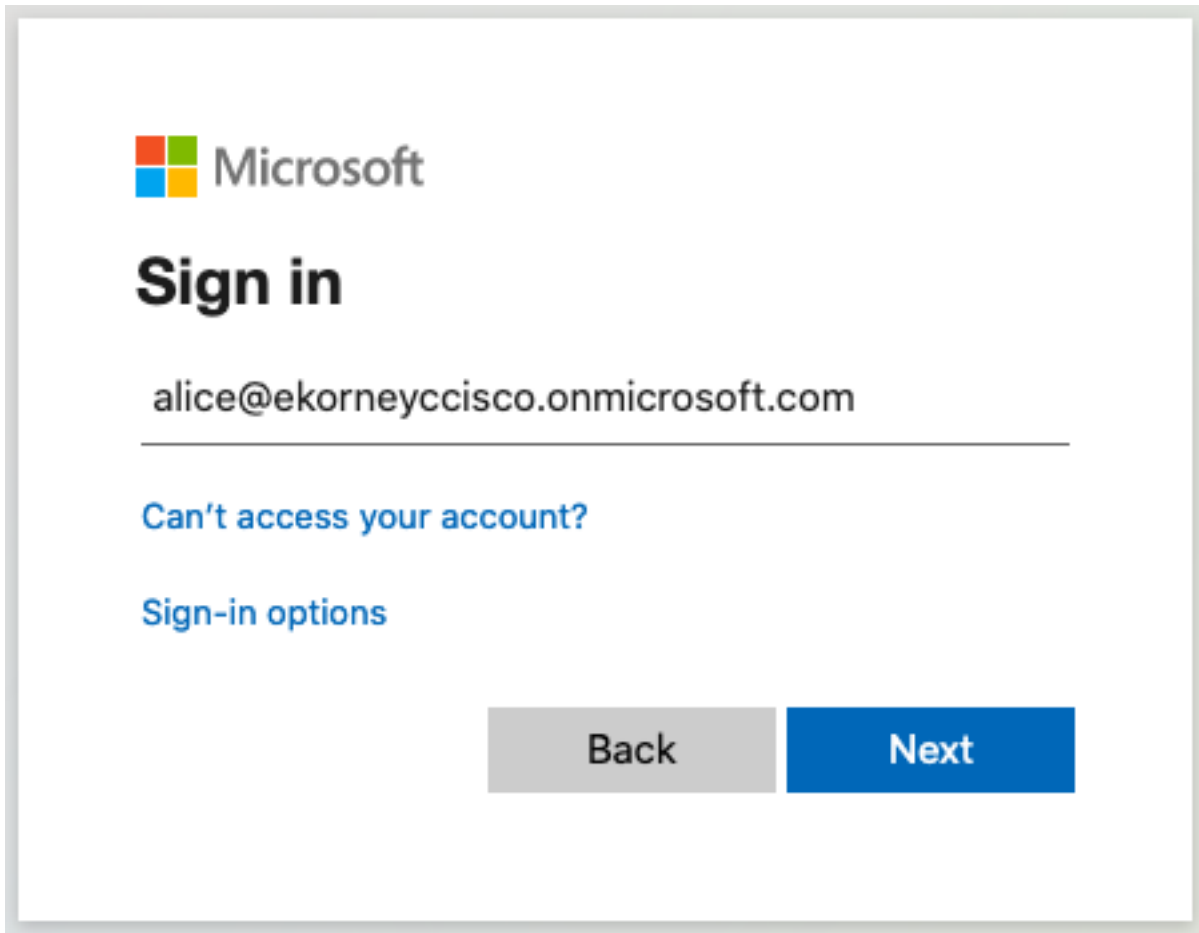
## 驗證

使用本節內容，確認您的組態是否正常運作。

**附註：** 首次登入時，新使用者將被強制更改使用者密碼。並接受AUP驗證步驟不包含它。驗證涵蓋這樣的情況：使用者不是第一次登入，並且發起人(alice)已經接受一次AUP。

現在，如果您開啟發起人門戶（例如，從測試URL），您將重定向到Azure進行登入，然後返回到發起人門戶。

1. 啟動發起人門戶，在門戶測試URL連結上使用其FQDN。ISE應將您重定向到Azure登入頁面。輸入**username** create earlier並按一下**Next**。

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 of the page 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. 輸入密碼，然後按一下**Sign In**。IdP登入螢幕會將使用者重定向到初始ISE的發起人門戶。





← alice@ekorneyccisco.onmicrosoft.com

## Enter password

.....|

[Forgot my password](#)

Sign in

### 3.接受AUP。

alice@ekorneyccisco.onmicrosoft.com ⓘ



#### Acceptable Use Policy

Please read the Acceptable Use Policy.

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

Accept

Decline

[Help](#)

### 4.此時，發起人使用者應具有對ALL\_ACCOUNTS發起人組許可權的門戶的完全訪問許可權。

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

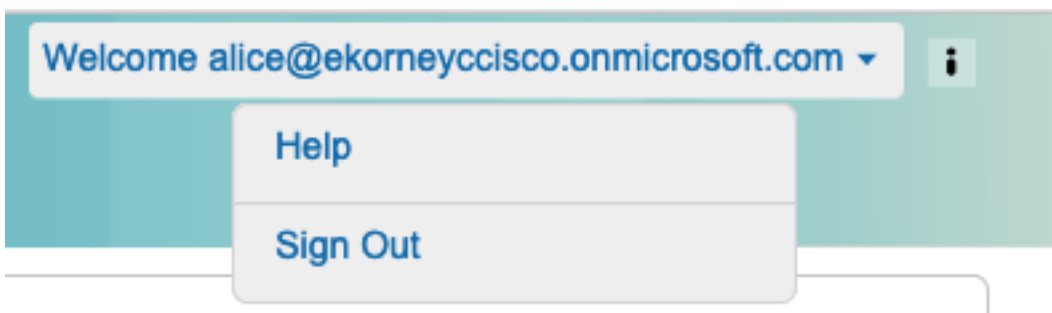
To Time \*

10:22

Create

[Help](#)

5.按一下「歡迎」下拉選單下的註銷。



6.使用者應成功註銷，然後再次重定向到登入螢幕。



## Pick an account



alice@ekorneyccisco.onmicrosoft.co  
m



Use another account

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

### 常見問題

瞭解在瀏覽器和Azure Active Directory之間處理SAML身份驗證至關重要。因此，您可以直接從身份提供程式(Azure)獲取與身份驗證相關的錯誤，其中ISE參與尚未啟動。

問題1.使用者輸入錯誤的密碼，未在ISE上處理使用者資料，該問題直接來自IdP(Azure)。若要修正：重置密碼或提供正確的密碼資料。



← 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. 使用者不屬於應該允許訪問SAML SSO的組，同樣在本例中，未在ISE上處理使用者資料，問題直接來自IdP(Azure)。若要修正：驗證Add group to the Application configuration步驟是否正確執行。



## 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未按預期工作，出現此錯誤 — 「SSO註銷失敗」。從您的SSO會話註銷時出現問題。請聯絡幫助台以獲得幫助。」當在SAML IdP上未正確配置註銷URL時，即可看到這種情況。在這種情況下，此URL使用的是「<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2>」，而應該是「<https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action>」才能修正：在 Azure IdP的註銷URL中輸入正確的URL。

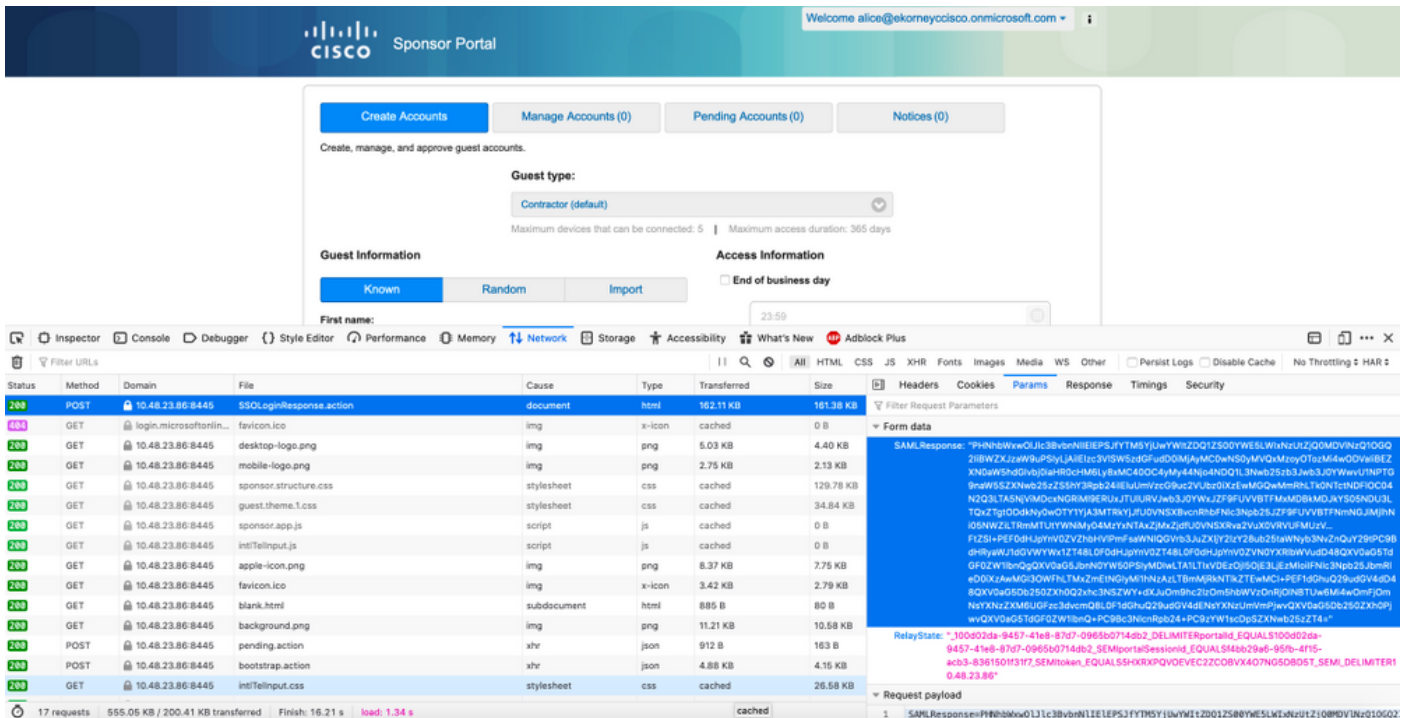
**Error**

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

[Help](#)

## 客戶端故障排除

若要驗證是否收到SAML負載，可以使用Web Developer Tools。如果使用Firefox，請導航到Tools > Web Developer > Network，然後使用Azure憑據登入到門戶。在Params頁籤中，可以看到加密的SAML響應：



## ISE故障排除

此處的元件的日誌級別應在ISE上更改。導航到操作>故障排除>調試嚮導>調試日誌配置。

元件名稱	日誌級別	日誌檔名
訪客接入	調試	guest.log
portal-web-action	調試	guest.log
opensaml	調試	ise-psc.log
saml	調試	ise-psc.log

正確流執行時調試的工作集(ise-psc.log):

## 1.使用者從發起人門戶重定向到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.從瀏覽器接收SAML響應。

```
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:ISE30-1ek LB:null request Server Name:sponsor30.example.com
2020-09-16 10:44:11,182 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][
cpm.saml.framework.impl.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.屬性 ( 斷言 ) 分析已啟動。

```
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.接收組屬性，值為f626733b-eb37-4cf2-b2a6-c2895fd5f4d3，簽名驗證。

```
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.將使用者組新增到身份驗證結果中，以便門戶可以使用它，通過SAML身份驗證。

```
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.註銷已觸發。SAML響應中接收到註銷

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:ISE30-1ek 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 successfully

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