

Azure AD SAML SSO로 ISE 3.0 스폰서 포털 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[고급 흐름도](#)

[구성](#)

[1단계. ISE에서 SAML ID 제공자 및 스폰서 포털을 구성합니다](#)

[1. Azure AD를 외부 SAML ID 원본으로 구성](#)

[2. Azure AD를 사용하도록 스폰서 포털 구성](#)

[3. 서비스 공급자 정보 내보내기](#)

[2단계. Azure AD IdP 설정 구성](#)

[1. Azure AD 사용자 만들기](#)

[2. Azure AD 그룹 만들기](#)

[3. 그룹에 Azure AD 사용자 할당](#)

[4. Azure AD Enterprise 응용 프로그램 만들기](#)

[5. 애플리케이션에 그룹 추가](#)

[6. Azure AD Enterprise 응용 프로그램 구성](#)

[7. Active Directory 그룹 특성 구성](#)

[8. Azure 페더레이션 메타데이터 XML 파일 다운로드](#)

[3단계. Azure Active Directory에서 ISE로 메타데이터 업로드](#)

[4단계. ISE에서 SAML 그룹 구성](#)

[5단계. ISE에서 스폰서 그룹 매핑 구성](#)

[다음은 확인합니다.](#)

[문제 해결](#)

[일반적인 문제](#)

[클라이언트 문제 해결](#)

[ISE 트러블슈팅](#)

소개

이 문서에서는 스폰서 사용자를 위해 SSO 기능을 제공하도록 ISE 3.0으로 Azure AD(Active Directory) SAML 서버를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE(Identity Services Engine) 3.0
- SAML(Security Assertion Markup Language) SSO(Single Sign-On) 구축에 대한 기본 지식
- Azure AD

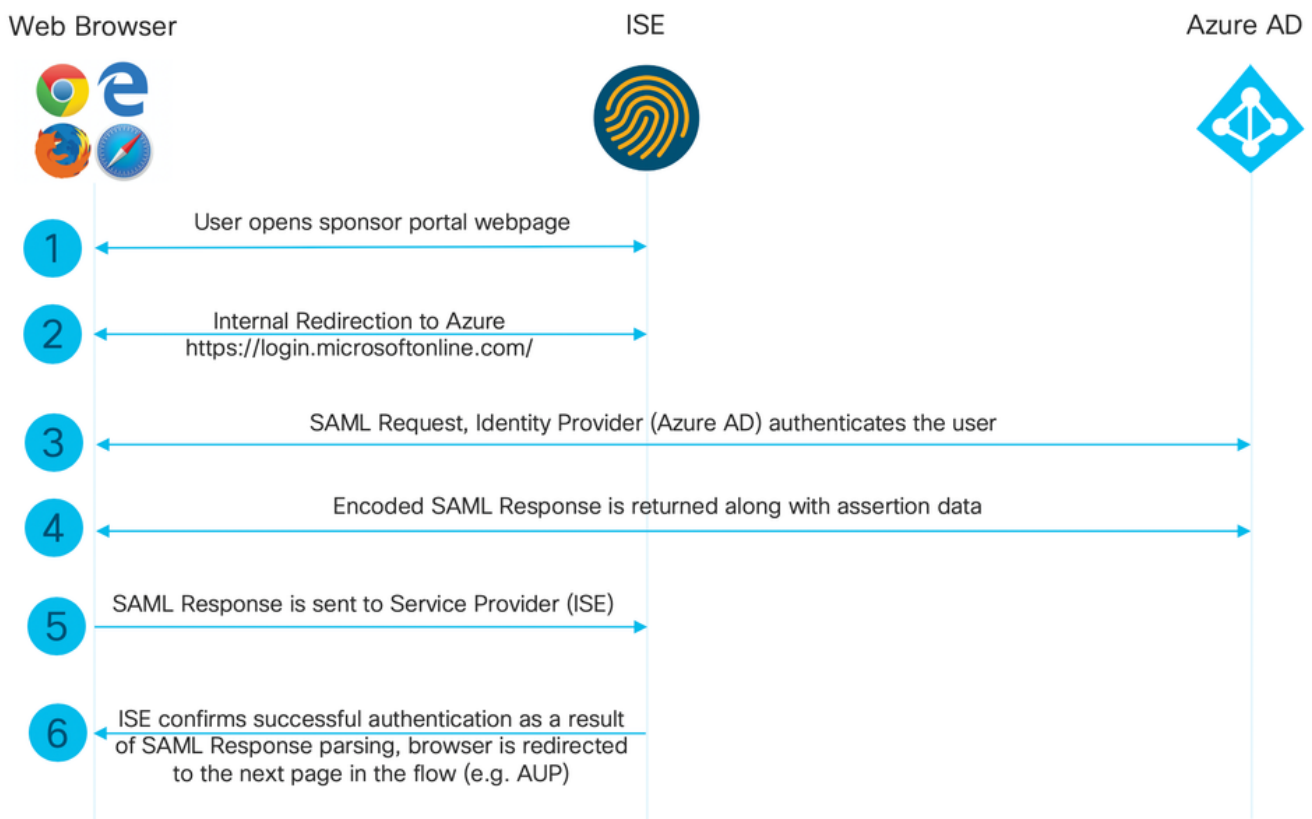
사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco ISE 3.0
- Azure AD

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

고급 흐름도



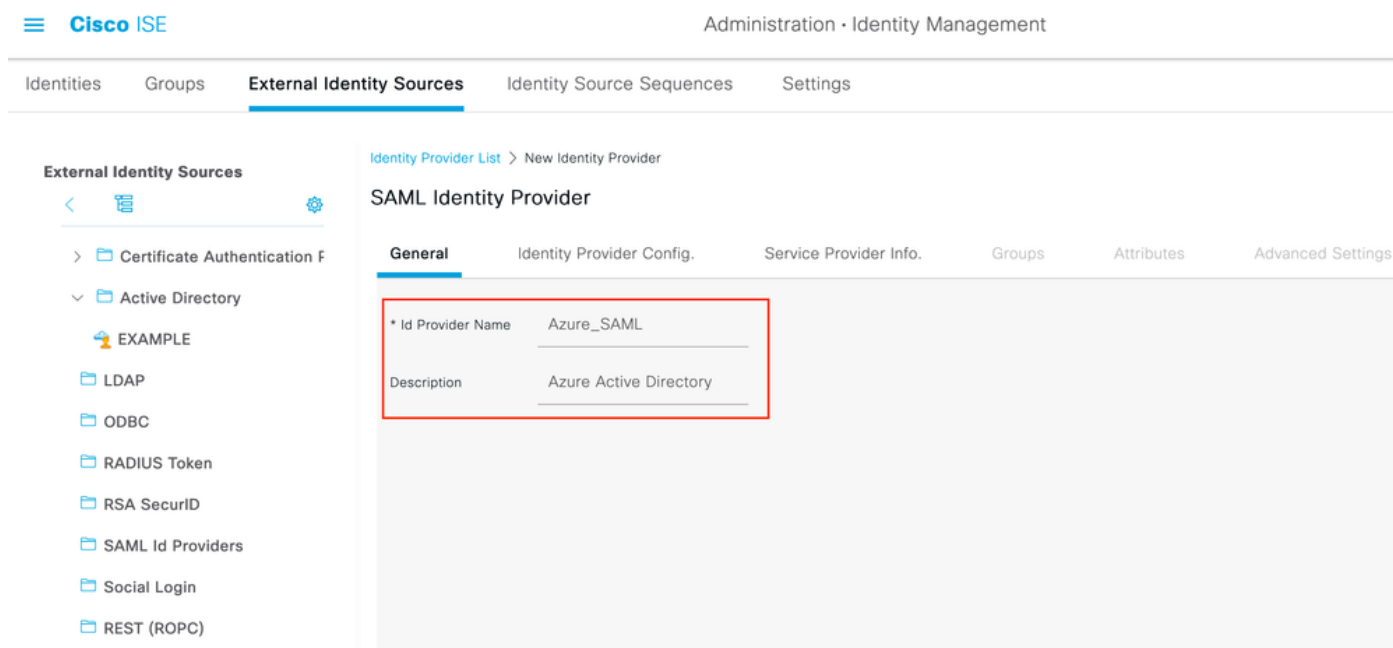
구성

1단계. ISE에서 SAML ID 제공자 및 스폰서 포털을 구성합니다

1. Azure AD를 외부 SAML ID 원본으로 구성

ISE에서 Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > SAML Id Providers(SAML ID 제공자)로 이동하고 Add(추가) 버튼을 클릭합니다.

ID 제공자 이름을 입력하고 Submit(제출)을 클릭하여 저장합니다. ID 제공자 이름은 이미지에 표시된 대로 ISE에서만 유효합니다.



2. Azure AD를 사용하도록 스폰서 포털 구성

Work Centers(작업 센터) > Guest Access(게스트 액세스) > Portals & Components(포털 및 구성 요소) > Sponsor Portals(스폰서 포털)로 이동하고 스폰서 포털을 선택합니다. 이 예에서는 스폰서 포털(기본값)이 사용됩니다.

Portal Settings(포털 설정) 패널을 확장하고 ID 소스 시퀀스에서 새 SAML IdP(Identity Provider)를 선택합니다. 스폰서 포털에 대한 FQDN(Fully Qualified Domain Name)을 구성합니다. 이 예에서는 sponsor30.example.com입니다. 이미지에 표시된 대로 저장을 클릭합니다.

Cisco ISE

Work Centers · Guest Access

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 create sessions

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:

☒ Gigabit Ethernet 0

☐ Gigabit Ethernet 1

☐ Gigabit Ethernet 2

☐ Gigabit Ethernet 3

☐ Gigabit Ethernet 4

☐ Gigabit Ethernet 5

If bonding is configured on a PSN, use:

☒ Bond 0

Uses Gigabit Ethernet 0 as primary, 1 as backup.

☐ Bond 1

Uses Gigabit Ethernet 2 as primary, 3 as backup.

☐ Bond 2

Uses Gigabit Ethernet 4 as primary, 5 as backup.

Certificate group tag:*

Default Portal Certificate Group

Configure certificates at:

Work Centers > Guest Access > Administration > System Certificates

Fully qualified domain names (FQDN) and host names:

sponsor30.example.com

Identity source sequence: *

Azure_SAML

Configure authentication methods at:

Work Centers > Guest Access > Identities > Identity Source Sequences

Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers

3. 서비스 공급자 정보 내보내기

Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > SAML Id Providers(SAML ID 제공자) > [Your SAML Provider](SAML 제공자)로 이동합니다.

서비스 공급자 정보 탭으로 전환합니다. 이미지에 표시된 대로 Export(내보내기) 버튼을 클릭합니다.

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 파일을 다운로드하고 저장합니다. 그 안에 2개의 파일이 있습니다. 스폰서 포털이라는 XML 파일이 필요합니다.

SingleLogoutService 바인딩의 ResponseLocation, entityID 값 및 AssertionConsumerService 바인딩의 Location 값을 기록합니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://CiscoISE/bd48c1a1
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration=
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFZjCCA06gAwIBAgIQX1oAvwAAAAChgVd9cEEW0zANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQD
ExpTQU1MX01TRTMwLTF1ay51eGFtcGx1LmNvbTAeFw0yMDA5MTAxMDMyMzFaFw0yNTA5MDkxMDMy
MzFaMCUxIzAhBgNVBAMTG1NBTUxsfSVNFMzAtMwVrLmV4YW1wbGUuY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICcGKCAgEAt+MixKfuZvg/oAWGES6zrUYL3H2JwvZw9yJs6sJ8/BpP6Sw027wh
FXnESXpqmmoSVrVEcQIrDdk318UYNn/+98PPkIi/4ftyFjZK9YdeverD6nrA2MeoLCzG1kWq/y4i
vvVcYuw344pySm65awVvro3q84x9esHqyLahExs9guiLJryD497XmNP4Z8eTHCctu777PuI1wL04
QOYUs2sozXvR98D9Jok/+PjH3bjmVKapqAcNEFvk8Ez9x1sMBUgFwP4YdZzQB9IRVkdIJGvqMyf
a6gn+KaddJnmIbXKFbrTaFi2IvRs3qHJ0mMVfYRnYeMq19/PhzvSFtjRe32x/aQh23j9dCsVXmQ
ZmXpZyxxJ8p4RqyM0YgkfxnQXXtV9K0sRZPFn60+iszUw2hARRG/tE0hTuVXpbonG2dT109JeeEe
S1E5uxenJvYkU7mMamvBjYQN6qVvyogf8F01HTSfd6TDsK3Qhmz0jg50PrBvvg5qE60rxxNvqSVZ
1dhx/iHZAZ1yYSVdwiZsZMCw0PjSwrRPx/h8103djeW0aL5R1AF1qTFHVHNSnvigzh6FyjdkUJH66
JAygPeOPKJFRgYzh5vWoJ41qvDqJlGk3c/zYi57MR1Bs0mkSvkOGbmjSsb+EehnYyLLB8FG3De2V
ZaXaHZ37gmoCNNmZHRn+GB0CAwEAA0BkTCBjjAgBgNVHREEGTAXghVJU0UzMC0xZWsuZXhhbXBs
ZS5jb20wDAYDVROTBABUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVRO0BBYEFPT/6jpfyugxRo1bjzWJ
858WFTP1MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjARBglghkgBhvhCAQEEBAMCBkAw
DQYJKoZIhvcNAQEMBQADggIBABGyWZbLajM2LyLASg//4N6mL+Xu/9IMdVvNBWQodF+j0WusW15a
VPSQU2t3Ckd/I1anvpK+cp77NMjo9V9oWI3/ZnjZHGofAIcHn1GCoEjmC1TvLau7ZzhCCII37DFA
yMKDrXLi3pR+ON1X1TivjHTTzrKm1NHhkxkx/Js5Iuz+MyRKP8FnmWT0q4XGejyKzJWrqEu+bc1
idC1/gBNUCHgqmFeM82IGQ7jV0m1kBjLb4pTDbYk4fMIbJVh4V2Pgi++6MIfXAYEwL+LHjSGHCQT
PSM3+kpv1wHHpGWzQSmcJ4tXVXV95W0NC+LxQZLBPNMUZorhuYCILXxvXH1HGJJ0YKx91k9Ubd2
s5Jad+GN8jqm5XXAAu7S4BawfvCo3bo0iXnSvvcIuH9YFiR21p2n/2X0VVbdPHYZtqGieqBWebHr
4I1z18FXb1YyMzpIkht00vkP5mA1R92VXBkvx2WPjtzQrv0tSXgvTCOKerYCBM/jnuwsztV7FVTV
JNdFwOsnXC70YngZeujZyJpUbfrKZI34VKZp4i05bZsG1bWE9Skdquv0PaQ8ecXTv80CVBYUeg1
vt0pde18h/9jImdLG8dF0rbADGHiieTcntSDdw3E7JFmS/oHw7FsA5GI8IxXfcOWUx/L0Dx3jTND
Z1AXp4juySODIx9yDyM4yV0f
</ds:X509Certificate>
```

```

</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://

</md:SPSSODescriptor>
</md:EntityDescriptor>

```

XML 파일에 따르면:

SingleLogoutService

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

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

AssertionConsumerService 위치

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

AssertionConsumerService 위치

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

AssertionConsumerService 위치

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

AssertionConsumerService 위치

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

AssertionConsumerService 위치 = "[https://ise30-](https://ise30-1ek.example.com:8445/sponsorportal/SSOLoginResponse.action)

[1ek.example.com:8445/sponsorportal/SSOLoginResponse.action](https://ise30-1ek.example.com:8445/sponsorportal/SSOLoginResponse.action)"

AssertionConsumerService 위치 = "[https://ise30-](https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action)

[2ek.example.com:8445/sponsorportal/SSOLoginResponse.action](https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action)"

AssertionConsumerService 위치 = "[https://ise30-](https://ise30-3ek.example.com:8445/sponsorportal/SSOLoginResponse.action)

[3ek.example.com:8445/sponsorportal/SSOLoginResponse.action](https://ise30-3ek.example.com:8445/sponsorportal/SSOLoginResponse.action)"

2단계. Azure AD IdP 설정 구성

1. Azure AD 사용자 만들기

Azure Active Directory Admin Center Dashboard에 로그인하고 이미지에 표시된 대로 AD를 선택합니다.

Azure Active Directory admin center

Dashboard > Default Directory

Default Directory | Overview

Azure Active Directory

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

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

Default Directory

Search your tenant

Tenant information

Your role
Global administrator [More info](#)

License
Azure AD Premium P2

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

Primary domain
ekorneyccisco.onmicrosoft.com

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

Sign-ins

3
2.8
2.6
2.4
2.2
2

Aug 23

Users(사용자)를 선택하고 New User(새 사용자)를 클릭한 다음 사용자 이름, 이름 및 초기 암호를 구성합니다. 이 테스트 사용자의 이미지에 표시된 대로 Create(생성)를 클릭합니다.

Azure Active Directory admin center

Dashboard > Users >

New user

Default Directory

Got feedback?

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

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

[Help me decide](#)

Identity

User name * ⓘ ✓ @ ✓

The domain name I need isn't shown here

Name * ⓘ ✓

First name

Last name

Password

☐ Auto-generate password

☒ Let me create the password

Initial password * ⓘ ✓

2. Azure AD 그룹 만들기

그룹을 선택합니다. 이미지에 표시된 대로 New Group(새 그룹)을 클릭합니다.

Dashboard > Default Directory > Groups

Groups | All groups

Default Directory - Azure Active Directory

+ New group ↓ Download groups 🗑 Delete ↻ Refresh ≡ Columns

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

🔍 Search groups + Add filters

All groups

Deleted groups

Diagnose and solve problems

그룹 유형을 보안으로 유지합니다. 이미지에 표시된 대로 그룹 이름을 구성합니다.

Azure Active Directory admin center

Dashboard

All services

FAVORITES

Azure Active Directory

Users

Enterprise applications

Dashboard > Default Directory > Groups >

New Group

Group type *

Security

Group name * ⓘ

Sponsor Group

Group description ⓘ

Enter a description for the group

Azure AD roles can be assigned to the group (Preview) ⓘ

Yes No

Membership type * ⓘ

Assigned

Owners

No owners selected

Members

No members selected

3. 그룹에 Azure AD 사용자 할당

선택한 멤버 없음을 클릭합니다. 사용자를 선택하고 선택을 클릭합니다. 사용자가 할당된 그룹을 만들려면 만들기를 클릭합니다.

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

Group Object id(그룹 개체 ID)를 기록해 둡니다. 이 화면에서 스폰서 그룹의 경우 ID는 f626733b-eb37-4cf2-b2a6-c2895fd5f4d3입니다.

Dashboard > Default Directory > Groups

Groups | All groups

Default Directory - Azure Active Directory

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

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

Search groups Add filters

Name	Object Id	Group Type	Membership Type
☐ IG ISE Group	eebf9cb9-91e2-4989-8c06-eef2cd3f69a3	Security	Assigned
☐ SG Sponsor Group	f626733b-eb37-4cf2-b2a6-c2895fd5f4d3	Security	Assigned

Settings

- General
- Expiration
- Naming policy

4. Azure AD Enterprise 응용 프로그램 만들기

AD 아래에서 Enterprise Applications를 선택하고 이미지에 표시된 대로 New application(새 애플리케이션)을 클릭합니다.

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.

이미지에 표시된 대로 비 갤러리 응용 프로그램을 선택합니다.

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

애플리케이션 이름을 입력하고 Add(추가)를 클릭합니다.

Azure Active Directory admin center

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

Add your own application

Name * ⓘ
ISE30 ✓

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports: ⓘ

- SAML-based single sign-on
[Learn more](#)
- Automatic User Provisioning with SCIM
[Learn more](#)
- Password-based single sign-on
[Learn more](#)

5. 애플리케이션에 그룹 추가

사용자 및 그룹 할당을 선택합니다.

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

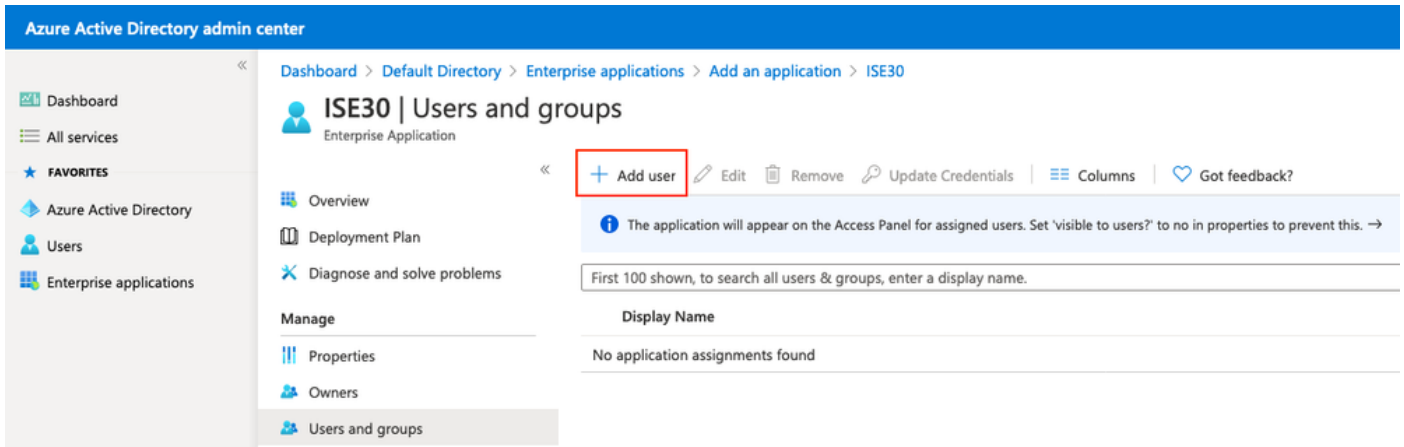
Application ID ⓘ
20ee030a-1a06-4a65-80ce-9 ...

Object ID ⓘ
0e6aac66-0ce1-4924-84a6-0 ...

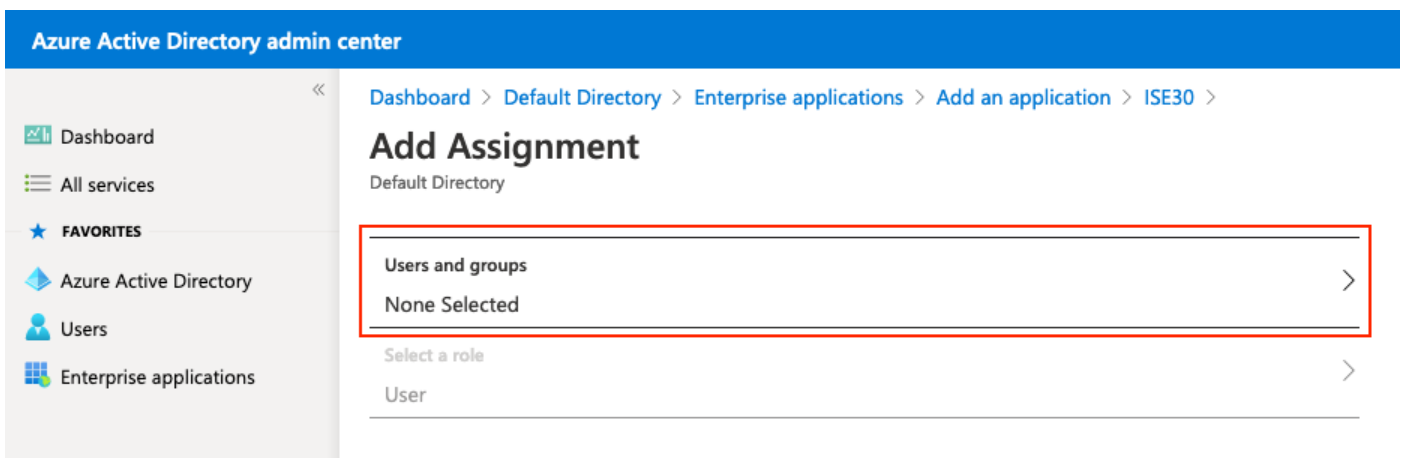
Getting Started

- 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](#)

Add user(사용자 추가)를 클릭합니다.



사용자 및 그룹을 클릭합니다.



이전에 구성한 그룹을 선택하고 선택을 클릭합니다.

 참고: 액세스 할 수 있는 사용자 또는 그룹의 적절 한 집합을 선택 하는 것은 귀하의 몫입니다.

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

그룹을 선택한 후 이미지에 표시된 대로 Assign(할당)을 클릭합니다.

Azure Active Directory admin center

Dashboard

All services

FAVORITES

Azure Active Directory

Users

Enterprise applications

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

Add Assignment

Default Directory

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

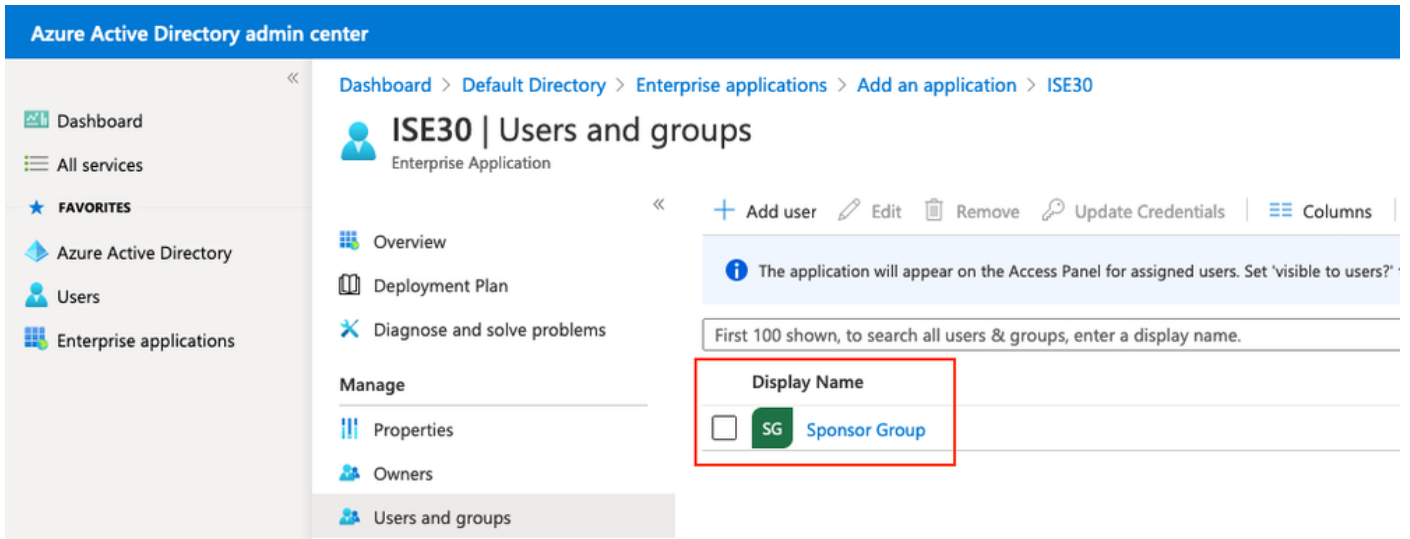
Users and groups

1 group selected.

Select a role

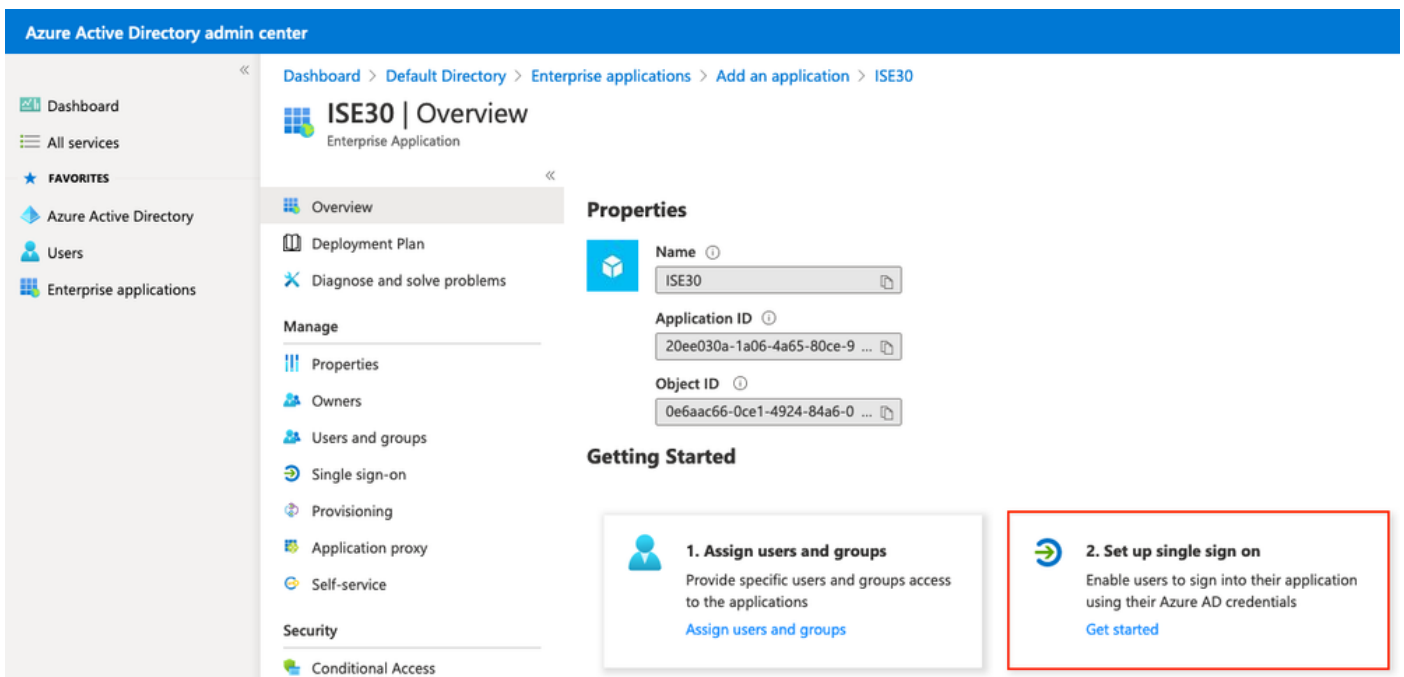
User

따라서 애플리케이션의 Users and groups 메뉴는 선택한 Group으로 채워져야 합니다.

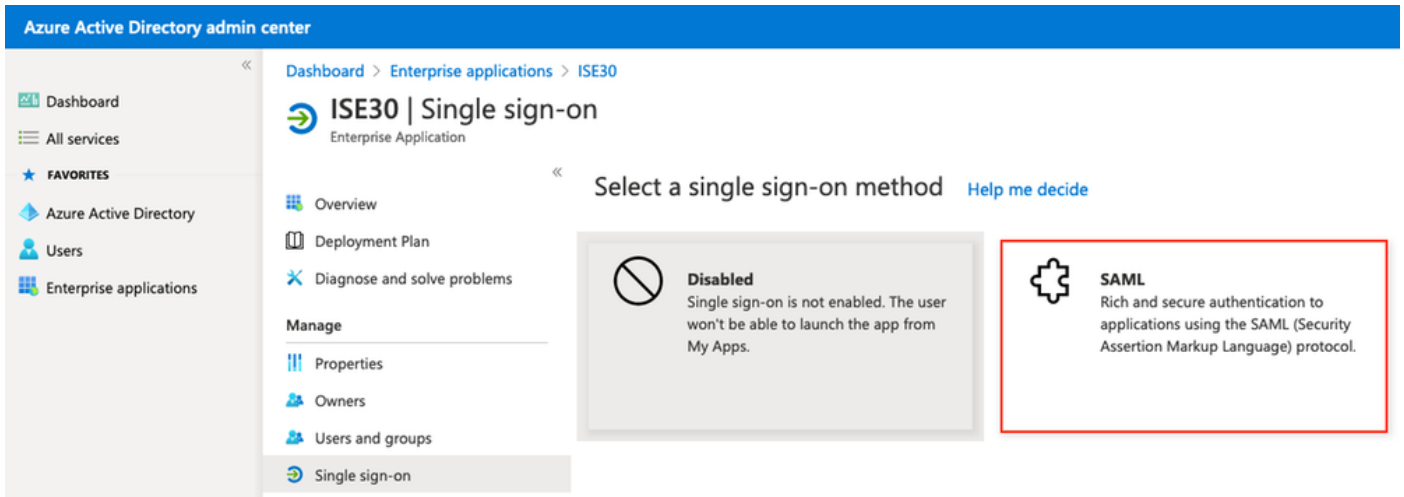


6. Azure AD Enterprise 응용 프로그램 구성

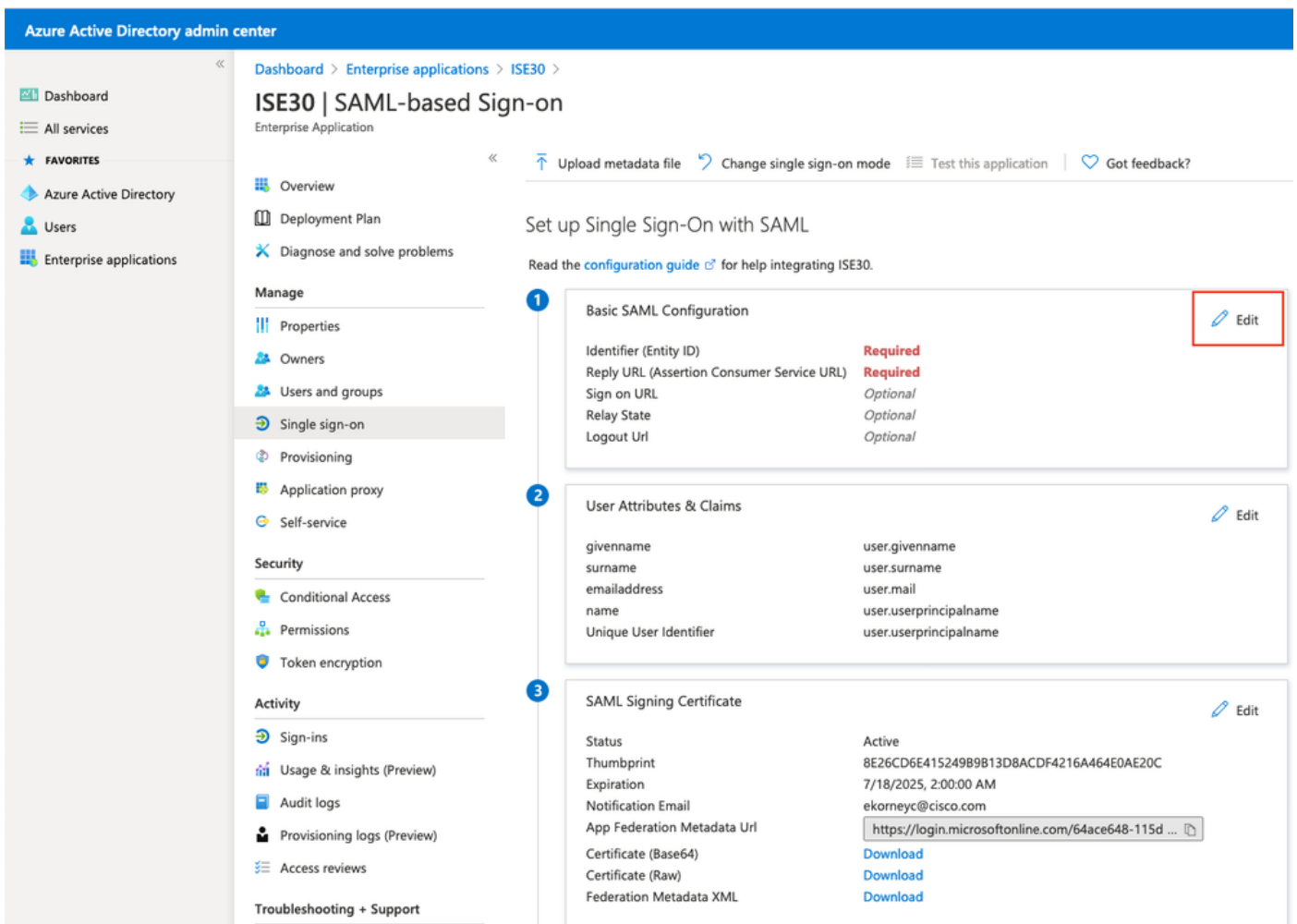
해당 애플리케이션으로 다시 이동한 다음 이미지에 표시된 대로 Set up single sign-on(단일 로그인 설정)을 클릭합니다.



다음 화면에서 SAML을 선택합니다.



Basic SAML Configuration 옆에 있는 Edit를 클릭합니다.



서비스 공급자 정보 내보내기 단계의 XML 파일에서 entityID 값으로 식별자(엔티티 ID)를 채웁니다. 응답 URL(Assertion Consumer Service URL)을 AssertionConsumerService의 Locations 값으로 채웁니다. SingleLogoutService의 ResponseLocation으로 로그아웃 Url 값을 채웁니다. 저장을 클릭합니다.

 참고: 회신 URL은 통과 목록 역할을 하며, 이를 통해 특정 URL이 IdP 페이지로 리디렉션될 때 소스 역할을 할 수 있습니다.

Basic SAML Configuration



Save

Identifier (Entity ID) * ⓘ

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

http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429	Default
	☒ ⓘ

Reply URL (Assertion Consumer Service URL) * ⓘ

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

	Default
https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action	☒ ⓘ
https://10.48.23.86:8445/sponsorportal/SSOLoginResponse.action	☐ ⓘ
https://10.48.26.63:8445/sponsorportal/SSOLoginResponse.action	☐ ⓘ
https://10.48.26.60:8445/sponsorportal/SSOLoginResponse.action	☐ ⓘ
https://ise30-1ek.example.com:8445/sponsorportal/SSOLoginResponse.action	☐ ⓘ
https://ise30-2ek.example.com:8445/sponsorportal/SSOLoginResponse.action	☐ ⓘ
https://ise30-3ek.example.com:8445/sponsorportal/SSOLoginResponse.action	☐ ⓘ

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

7. Active Directory 그룹 특성 구성

이전에 구성한 그룹 특성 값을 반환하려면 User Attributes & Claims(사용자 특성 및 클레임) 옆에 있는 Edit(수정)를 클릭합니다.

User Attributes & Claims



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

Add a group claim(그룹 클레임 추가)을 클릭합니다.

Azure Active Directory admin center

Dashboard

All services

FAVORITES

Azure Active Directory

Users

Enterprise applications

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 ***

Security groups(보안 그룹)를 선택하고 Save(저장)를 클릭합니다. 어설션에서 반환된 소스 특성은 앞서 캡처한 그룹 개체 ID인 그룹 ID입니다.

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



고급 옵션 아래에 그룹 이름을 추가로 제공합니다.

☒ Customize the name of the group claim

Name (required)

Sponsor Group



Namespace (optional)

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

그룹에 대한 클레임 이름을 기록해 둡니다. 이 경우에는 <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups>입니다.

Azure Active Directory admin center

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

User Attributes & Claims

+ Add new claim + Add a group claim Columns

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 페더레이션 메타데이터 XML 파일 다운로드

SAML 서명 인증서에서 페더레이션 메타데이터 XML에 대해 다운로드를 클릭합니다.

SAML Signing Certificate Edit

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

3단계. Azure Active Directory에서 ISE로 메타데이터 업로드

Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > SAML Id Providers(SAML ID 제공자) > [Your SAML Provider](SAML 제공자)로 이동합니다.

Identity Provider Config(ID 제공자 컨피그레이션) 탭으로 전환한 다음 Browse(찾아보기) 버튼을 클릭합니다. Azure Federation Metadata XML 다운로드 단계에서 페더레이션 메타데이터 XML 파일을 선택하고 저장을 클릭합니다.

 참고: ID 공급자 컨피그레이션의 UI 결함은 Cisco 버그 ID CSCv74517에서 [해결해야 합니다](#).

External Identity Sources

<

☰

⚙️

>

Certificate Authentication Profile

Active Directory

EXAMPLE

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Azure_SAML

Social Login

REST (ROPC)

Identity Provider List > Azure_SAML

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attributes

Advanced Settings

Identity Provider Configuration

Import Identity Provider Config File

Import Identity Provider Configuration File

Choose file

Import Identity Provider Configuration File

Choose file

Single Sign Out URL (Redirect)

https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2

Signing Certificates

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

4단계. ISE에서 SAML 그룹 구성

탭 그룹으로 전환하고 Active Directory 그룹 구성 특성에서 클레임 이름 값을 그룹 구성원 특성에 부여합니다.

External Identity Sources

<

>

Certificate Authentication Profile

>

Active Directory

>

EXAMPLE

>

LDAP

>

ODBC

>

RADIUS Token

>

RSA SecurID

>

SAML Id Providers

>

Azure_SAML

>

Social Login

>

REST (ROPC)

Identity Provider List > Azure_SAML

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attributes

Advanced Settings

Groups

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

+ Add

Edit

Delete

☐ Name in Assertion

Name in ISE

No data available

Add(추가)를 클릭합니다. 어설션에 있는 이름을 그룹에 Azure Active Directory 사용자 할당에서 캡처한 스폰서 그룹의 그룹 개체 ID 값으로 채웁니다. ISE에서 Azure Sponsor Group이라는 의미 있는 값을 사용하여 Name을 구성합니다. OK(확인)를 클릭합니다. 저장을 클릭합니다.

이렇게 하면 Azure의 그룹과 ISE에서 사용할 수 있는 그룹 이름 간의 매핑이 생성됩니다.

×

Add Group

*Name in Assertion

eb37-4cf2-b2a6-c2895fd5f4d3

*Name in ISE

Azure Sponsor Group

i

OK

Cancel

5단계. ISE에서 스폰서 그룹 매핑 구성

Work Centers(작업 센터) > Guest Access(게스트 액세스) > Portals & Components(포털 및 구성 요소) > Sponsor Groups(스폰서 그룹)로 이동하고 Azure AD Group(Azure AD 그룹)에 매핑하려는 스폰서 그룹을 선택합니다. 이 예에서는 ALL_ACCOUNTS(기본값)가 사용되었습니다.

☰ Cisco ISE

Work Centers - Guest Access

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

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) ⓘ

CreateEditDuplicateDelete

Enabled	Name	Member Groups
☒	ALL_ACCOUNTS (default)	ALL_ACCOUNTS (default)
☒	GROUP_ACCOUNTS (default)	GROUP_ACCOUNTS (default)
☒	OWN_ACCOUNTS (default)	OWN_ACCOUNTS (default)

멤버...를 클릭합니다. 을 누르고 Azure_SAML:Azure 스폰서 그룹을 선택한 사용자 그룹에 추가합니다. 이렇게 하면 Azure의 스폰서 그룹이 ALL_ACCOUNTS 스폰서 그룹에 매핑됩니다. OK(확인)를 클릭합니다. 저장을 클릭합니다.



Select Sponsor Group Members

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

Available User Groups

Search

Name ^
Employee
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Selected User Groups

Search

Name ^
ALL_ACCOUNTS (default)
Azure_SAML:Azure Sponsor Group

>

>>

<

<<

OK

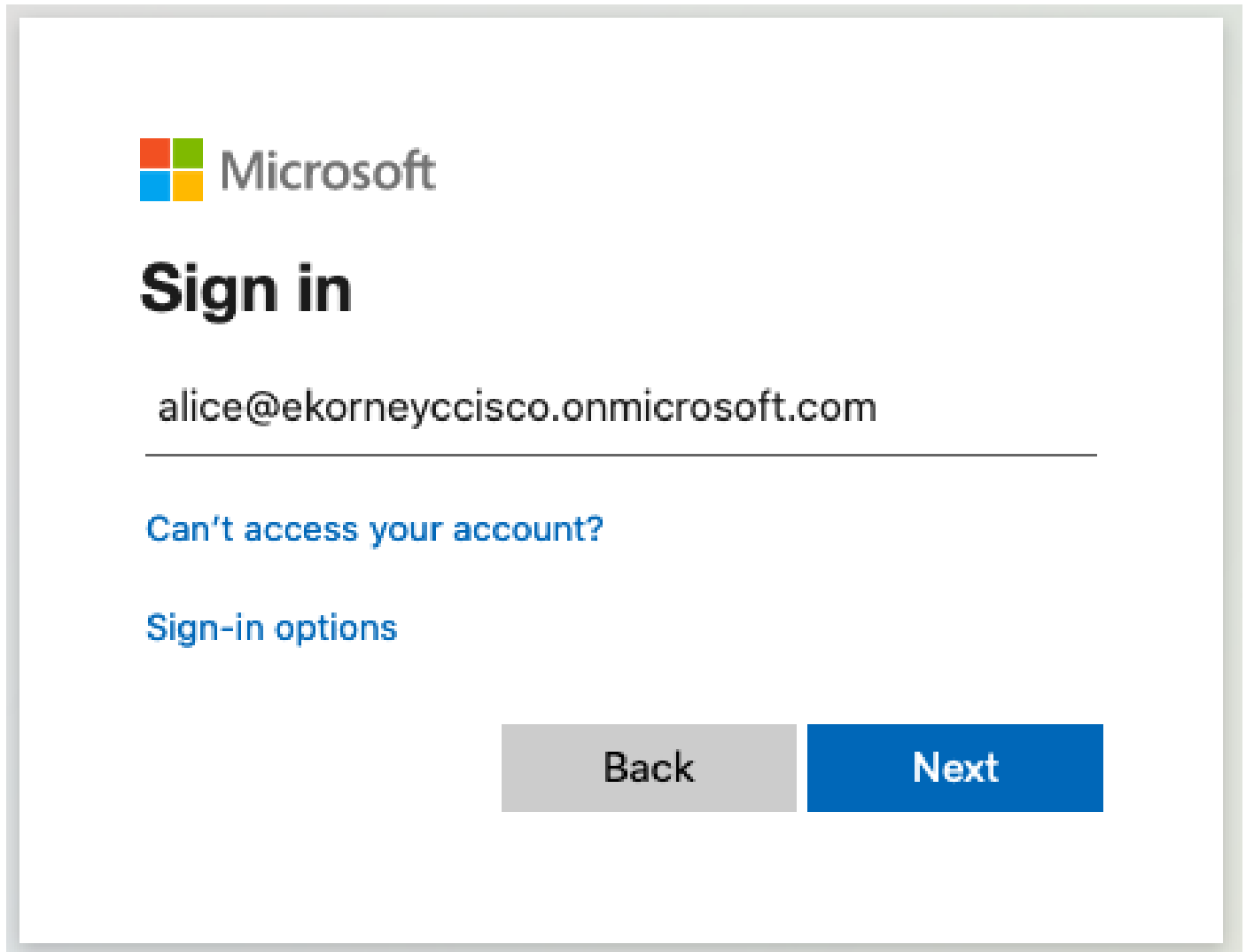
다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

 참고: 새 사용자는 첫 번째 로그인 시 사용자 비밀번호를 변경해야 합니다. 그리고 AUP 확인 절차에서는 이를 다루지 않습니다. 확인은 사용자가 처음으로 로그인하지 않고 스폰서 (alice)가 이미 AUP를 한 번 수락한 시나리오를 다룹니다.

이제 스폰서 포털을 열 경우(예: 테스트 URL에서) Azure로 리디렉션되어 로그인한 다음 스폰서 포털로 돌아갑니다.

1. 포털 테스트 URL 링크에서 해당 FQDN을 사용하여 스폰서 포털을 시작합니다. ISE는 사용자를 Azure 로그인 페이지로 리디렉션해야 합니다. 이전에 생성한 사용자 이름을 입력하고 Next(다음)를 클릭합니다.

A screenshot of the Microsoft Sign in page. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed in a large, bold, black font. Underneath "Sign in" is a text input field containing the email address "alice@ekorneyccisco.onmicrosoft.com". Below the input field is a horizontal line. Under the line, the text "Can't access your account?" is displayed in a blue, clickable font. Below that, the text "Sign-in options" is also displayed in a blue, clickable font. At the bottom right of the page are two buttons: a gray "Back" button and a blue "Next" button.

2. 비밀번호를 입력하고 로그인을 클릭합니다. IdP 로그인 화면은 사용자를 초기 ISE 스폰서 포털로 리디렉션합니다.



← [alice@ekorneyccisco.onmicrosoft.com](#)

Enter password

.....|

[Forgot my password](#)

Sign in

3. AUP를 수락합니다.



Sponsor Portal

[alice@ekorneyccisco.onmicrosoft.com](#) ⓘ

Acceptable Use Policy

Please read the Acceptable Use Policy.

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

Accept

Decline

[Help](#)

4. 이때 스폰서 사용자는 포털에 대한 ALL_ACCOUNTS 스폰서 그룹 권한을 가진 전체 액세스 권한을 가져야 합니다.



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. 시작 드롭다운 메뉴에서 로그아웃을 클릭합니다.

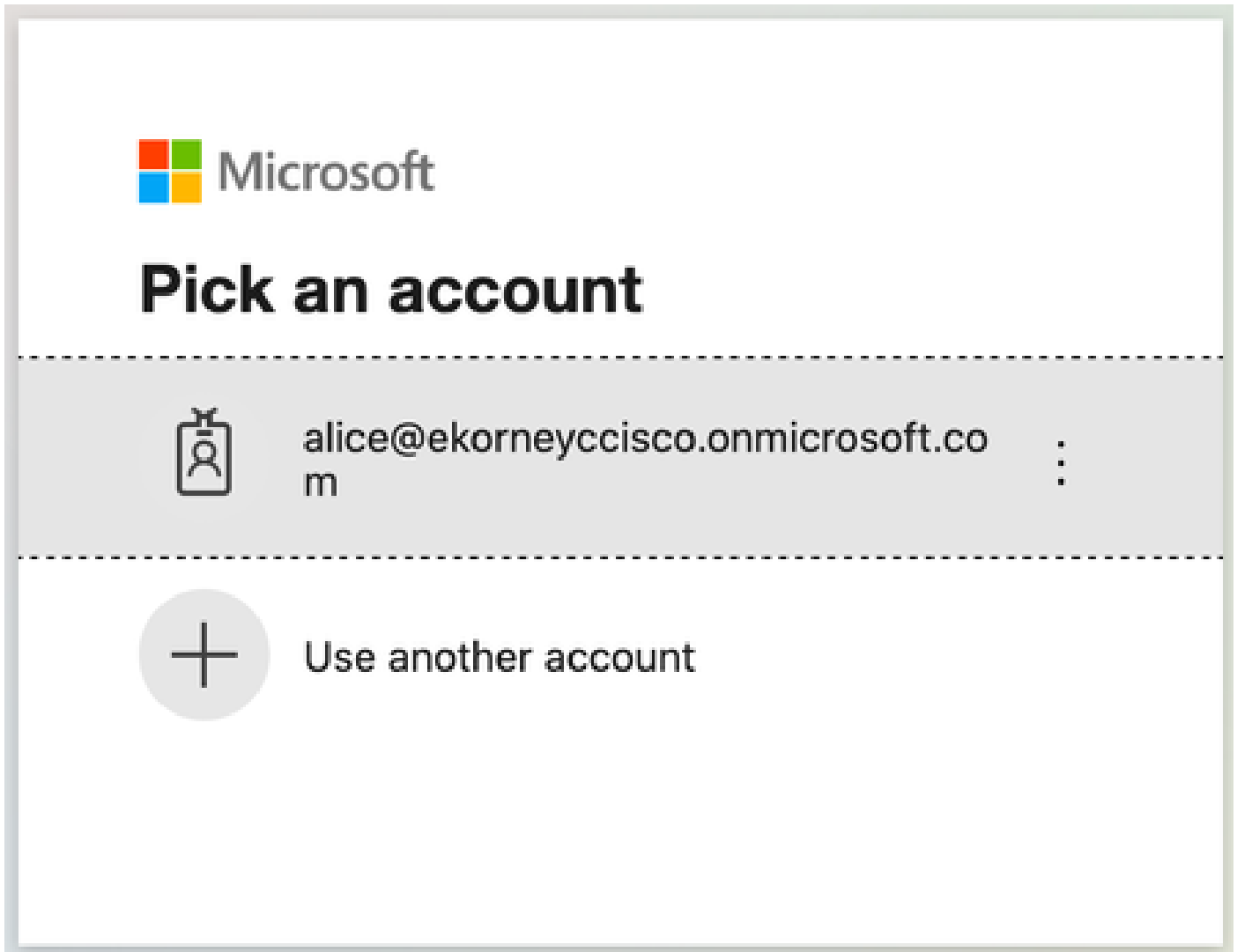
Welcome [alice@ekorneyccisco.onmicrosoft.com](#) ▾



Help

Sign Out

6. 사용자가 로그아웃하고 로그인 화면으로 다시 리디렉션되어야 합니다.



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

일반적인 문제

브라우저와 Azure Active Directory 간에 SAML 인증이 처리됨을 이해하는 것이 중요합니다. 따라서 ISE 참여가 아직 시작되지 않은 Azure(Identity Provider)에서 인증 관련 오류를 직접 가져올 수 있습니다.

문제 1. 사용자가 잘못된 암호를 입력했습니다. ISE에서 사용자 데이터를 처리하지 않았습니다. 문제가 IdP(Azure)에서 직접 발생합니다. 수정하려면 비밀번호를 재설정하거나 올바른 비밀번호 데이터를 제공합니다.



← `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

문제 2. 사용자가 SAML SSO에 액세스할 수 있도록 허용된 그룹에 속하지 않습니다. 이 경우에도 ISE에서 사용자 데이터를 처리하지 않았으므로 IdP(Azure)에서 직접 문제가 발생합니다. 수정하려면 Add group to the Application configuration(애플리케이션 구성에 그룹 추가) 단계가 올바르게 실행되었는지 확인합니다.



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. 로그아웃이 예상대로 작동하지 않으며 이 오류가 나타납니다. "SSO 로그아웃이 실패했습니다. SSO 세션에서 로그아웃하는 동안 문제가 발생했습니다. 도움이 필요하면 헬프 데스크에 문의하십시오." SAML IdP에서 로그아웃 URL이 올바르게 구성되지 않은 경우 확인할 수 있습니다. 이 경우 이 URL은 ["https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2"](https://sponsor30.example.com:8445/sponsorportal/SSOLogoutRequest.action?portal=100d02da-9457-41e8-87d7-0965b0714db2)이지만 ["https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action"](https://sponsor30.example.com:8445/sponsorportal/SSOLogoutResponse.action)이어야 합니다. 이 URL을 수정하려면 Azure IdP의 로그아웃 URL에 올바른 URL을 입력하십시오.

[Help](#)

클라이언트 문제 해결

SAML 페이로드가 수신되었는지 확인하려면 Web Developer Tools를 사용할 수 있습니다.

Firefox를 사용하고 포털에 Azure 자격 증명으로 로그인하는 경우 Tools(도구) > Web Developer(웹 개발자) > Network(네트워크)로 이동합니다. Params 탭에서 암호화된 SAML 응답을 확인할 수 있습니다.

Sponsor Portal

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

Access Information

☐ End of business day

Status	Method	Domain	File	Cause	Type	Transferred	Size		Headers	Cookies	Params	Response	Timings	Security
200	POST	10.48.23.86-8445	SSOLoginResponse.action	document	html	162.11 KB	161.38 KB							
404	GET	login.microsoftonline.com	favicon.ico	img	x-icon	cached	0 B							
200	GET	10.48.23.86-8445	desktop-logo.png	img	png	5.03 KB	4.40 KB							
200	GET	10.48.23.86-8445	mobile-logo.png	img	png	2.75 KB	2.13 KB							
200	GET	10.48.23.86-8445	sponsor.structure.css	stylesheet	css	cached	129.78 KB							
200	GET	10.48.23.86-8445	guest.theme.1.css	stylesheet	css	cached	34.84 KB							
200	GET	10.48.23.86-8445	sponsor.app.js	script	js	cached	0 B							
200	GET	10.48.23.86-8445	inteliTelnpJt.js	script	js	cached	0 B							
200	GET	10.48.23.86-8445	apple-icon.png	img	png	8.37 KB	7.75 KB							
200	GET	10.48.23.86-8445	favicon.ico	img	x-icon	3.42 KB	2.79 KB							
200	GET	10.48.23.86-8445	blank.html	subdocument	html	885 B	80 B							
200	GET	10.48.23.86-8445	background.png	img	png	11.21 KB	10.58 KB							
200	POST	10.48.23.86-8445	padding.action	xhr	json	912 B	163 B							
200	POST	10.48.23.86-8445	bootstrap.action	xhr	json	4.88 KB	4.15 KB							
200	GET	10.48.23.86-8445	inteliTelnpJt.css	stylesheet	css	cached	26.58 KB							

ISE 트러블슈팅

여기서 구성 요소의 로그 레벨은 ISE에서 변경해야 합니다. Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug Log Configuration(디버그 로그 컨피그레이션)으로 이동합니다.

구성 요소 이름	로그 레벨	로그 파일 이름
게스트 액세스	디버그	guest.log
포털 웹 작업	디버그	guest.log
opensaml	디버그	ise-psc.log

SAML	디버그	ise-psc.log
------	-----	-------------

올바른 플로우 실행 시 디버깅 작업 집합(ise-psc.log):

1. 사용자가 스폰서 포털에서 IdP URL로 리디렉션됩니다.

```

2020-09-16 10:43:59,207 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-8e40-e43d20c9f429_SEMI
2020-09-16 10:43:59,211 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-4][] cpm.saml.framework.impl.SAMLFa
https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action

```

2. 브라우저에서 SAML 응답을 수신합니다.

```

2020-09-16 10:44:11,122 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,126 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,126 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
:_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSes
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,126 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,129 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,129 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,133 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;token
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
token=OA6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,134 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
This node's host name:ISE30-1ek LB:null request Server Name:sponsor30.example.com
2020-09-16 10:44:11,182 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,184 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] org.opensaml.xml.parse.BasicPa
2020-09-16 10:44:11,187 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] org.opensaml.xml.parse.BasicPa
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.saml2.binding.decoding
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId_EQUALSbd48c1a1-9477-4746-8e40-e43d20c9f429_SEMI

```

```

2020-09-16 10:44:11,190 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.saml2.binding.decoder.Ba
2020-09-16 10:44:11,191 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,193 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
2020-09-16 10:44:11,195 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.xml.signature.impl.Si
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.saml2.binding.decoder.Ba
2020-09-16 10:44:11,197 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.saml2.binding.decoder.Ba
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.ws.message.decoder.Ba
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.common.binding.decoder.Ba
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.common.binding.decoder.Ba
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.decoder.Ba
https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
SAML decoder's URIComparator - [https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action]
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] opensaml.common.binding.decoder.Ba
SAML message intended destination endpoint matched recipient endpoint
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa

```

3. 특성(assertion) 구문 분석이 시작됩니다.

```

2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAT
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.SAMLAT
Attribute=<http://schemas.microsoft.com/identity/claims/tenantid> add value=<64ace648-115d-4ad9-a3bf-76601b0
2020-09-16 10:44:11,199 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAT
attribute<http://schemas.microsoft.com/identity/claims/tenantid> value=<64ace648-115d-4ad9-a3bf-76601b0
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAT
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.SAMLAT
Attribute=<http://schemas.microsoft.com/identity/claims/objectidentifier> add value=<50ba7e39-e7fb-4cb1-8256
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAT
attribute<http://schemas.microsoft.com/identity/claims/objectidentifier> value=<50ba7e39-e7fb-4cb1-8256
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAT
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.SAMLAT
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.SAMLAT
attribute<http://schemas.microsoft.com/identity/claims/displayname> value=<Alice>

```

4. 그룹 특성이 f626733b-eb37-4cf2-b2a6-c2895fd5f4d3 값으로 수신되며 서명 검증이 수행됩니다.

```

2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLAT
http://schemas.microsoft.com/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.SAMLAT
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.SAMLAT
<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.SAMLAT

```

```
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.SAMLat
Attribute=<http://schemas.microsoft.com/identity/claims/identityprovider> add value=<https://sts.window
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
<http://schemas.microsoft.com/identity/claims/identityprovider> value=<https://sts.windows.net/64ace648
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
http://schemas.microsoft.com/claims/authnmethodsreferences
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute=<http://schemas.microsoft.com/claims/authnmethodsreferences> add value=<http://schemas.microso
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
<http://schemas.microsoft.com/claims/authnmethodsreferences> value=<http://schemas.microsoft.com/ws/200
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute=<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> add value=<alice@ekorneyccisco.o
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> value=<alice@ekorneyccisco.onmicrosoft.com
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.cfg.Identity
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
2020-09-16 10:44:11,200 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute <http://schemas.microsoft.com/identity/claims/displayname> NOT configured in IdP dictionary, I
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute <http://schemas.microsoft.com/identity/claims/tenantid> NOT configured in IdP dictionary, NOT
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute <http://schemas.microsoft.com/identity/claims/identityprovider> NOT configured in IdP diction
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute <http://schemas.microsoft.com/identity/claims/objectidentifier> NOT configured in IdP diction
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> NOT configured in IdP dictionary
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
Attribute <http://schemas.microsoft.com/claims/authnmethodsreferences> NOT configured in IdP dictionary
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLS
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLat
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
_bd48c1a1-9477-4746-8e40-e43d20c9f429_DELIMITERportalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSess
token=0A6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
_token=0A6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
portalId=bd48c1a1-9477-4746-8e40-e43d20c9f429;portalSessionId=8fa19bf2-9fa6-4892-b082-5cdabfb5daa1;toke
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
_token=0A6CZJQD7X67TLYHE4Y3EM3EY097E2J;_DELIMITERSponsor30.example.com
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
IDP URL: https://login.microsoftonline.com/64ace648-115d-4ad9-a3bf-76601b0f8d5c/saml2
2020-09-16 10:44:11,201 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
2020-09-16 10:44:11,202 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8] [] cpm.saml.framework.impl.SAMLFa
IdP URI: https://sts.windows.net/64ace648-115d-4ad9-a3bf-76601b0f8d5c/
SP URI: http://CiscoISE/bd48c1a1-9477-4746-8e40-e43d20c9f429
Assertion Consumer URL: https://sponsor30.example.com:8445/sponsorportal/SSOLoginResponse.action
```


[illegible]

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.