

SAML SSO와 Azure AD의 통합을 통해 ISE 3.1 ISE GUI 관리 로그의 흐름 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[IdP\(ID 공급자\)](#)

[서비스 공급자\(SP\)](#)

[SAML](#)

[SAML 어설션](#)

[고급 흐름도](#)

[Azure AD와 SAML SSO 통합 구성](#)

[1단계. ISE에서 SAML ID 제공자 구성](#)

- [1. Azure AD를 외부 SAML ID 원본으로 구성](#)
- [2. ISE 인증 방법 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](#)

[\(선택 사항\) 5단계. RBAC 정책 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일반적인 문제](#)

[ISE 트러블슈팅](#)

[SAML 로그인 및 일치하지 않는 그룹 클레임 이름이 있는 로그](#)

소개

이 문서에서는 Azure AD(Active Directory)와 같은 외부 ID 공급자와 Cisco ISE 3.1 SAML SSO 통합을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

1. Cisco ISE 3.1
2. SAML SSO 구축
3. Azure AD

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

1. Cisco ISE 3.1
2. 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.

배경 정보

IdP(ID 공급자)

이 경우 Azure AD는 사용자 ID를 확인하고 요청한 리소스("서비스 공급자")에 대한 액세스 권한을 어설션합니다.

서비스 공급자(SP)

사용자가 액세스하려는 호스팅된 리소스 또는 서비스이며, 이 경우 ISE 애플리케이션 서버입니다.

SAML

SAML(Security Assertion Markup Language)은 SP에 인증 자격 증명을 전달하기 위해 IdP를 허용하는 개방형 표준입니다.

SAML 트랜잭션은 ID 공급자와 서비스 공급자 간의 표준화된 통신에 XML(Extensible Markup Language)을 사용합니다.

SAML은 서비스를 사용하기 위해 사용자 ID의 인증과 권한 부여 간의 링크입니다.

SAML 어설션

SAML Assertion은 ID 제공자가 사용자 권한 부여가 포함된 서비스 제공자에게 전송하는 XML 문서입니다.

SAML 어설션에는 인증, 특성 및 권한 부여 결정이라는 세 가지 유형이 있습니다.

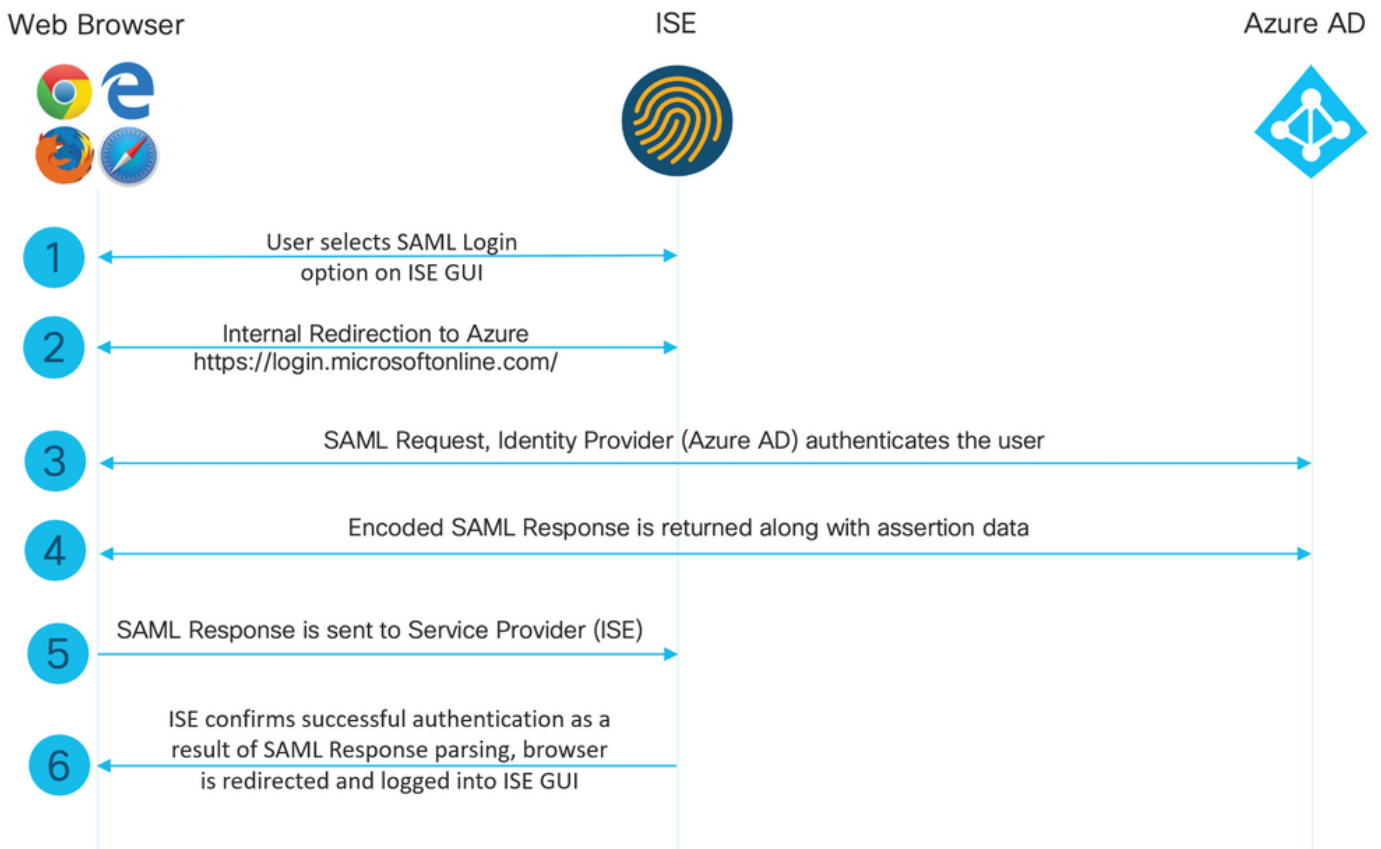
- 인증 어설션은 사용자의 ID를 증명하며 사용자가 로그인한 시간 및 어떤 인증 방법을 사용했는지 제공합니다(예: Kerberos, 2단계)
- 특성 어설션은 사용자에 대한 정보를 제공하는 특정 데이터 조각인 SAML 특성을 서비스 공급자에게 전달합니다.
- 권한 부여 결정 어설션은 사용자가 서비스를 사용할 권한이 있는지 또는 비밀번호 오류 또는 서비스에 대한 권한 부족으로 인해 ID 제공자가 요청을 거부했는지 여부를 선언합니다.

고급 흐름도

SAML은 ID 공급자, Azure AD 및 서비스 공급자, ISE 간에 사용자, 로그인 및 특성에 대한 정보를 전달하여 작동합니다.

각 사용자가 ID 공급자를 사용하여 SSO(Single Sign-On)에 한 번 로그인하면 Azure AD 공급자는 사용자가 해당 서비스에 액세스하려고 시도할 때 SAML 특성을 ISE에 전달합니다.

ISE는 이미지에 표시된 대로 Azure AD에서 권한 부여 및 인증을 요청합니다.



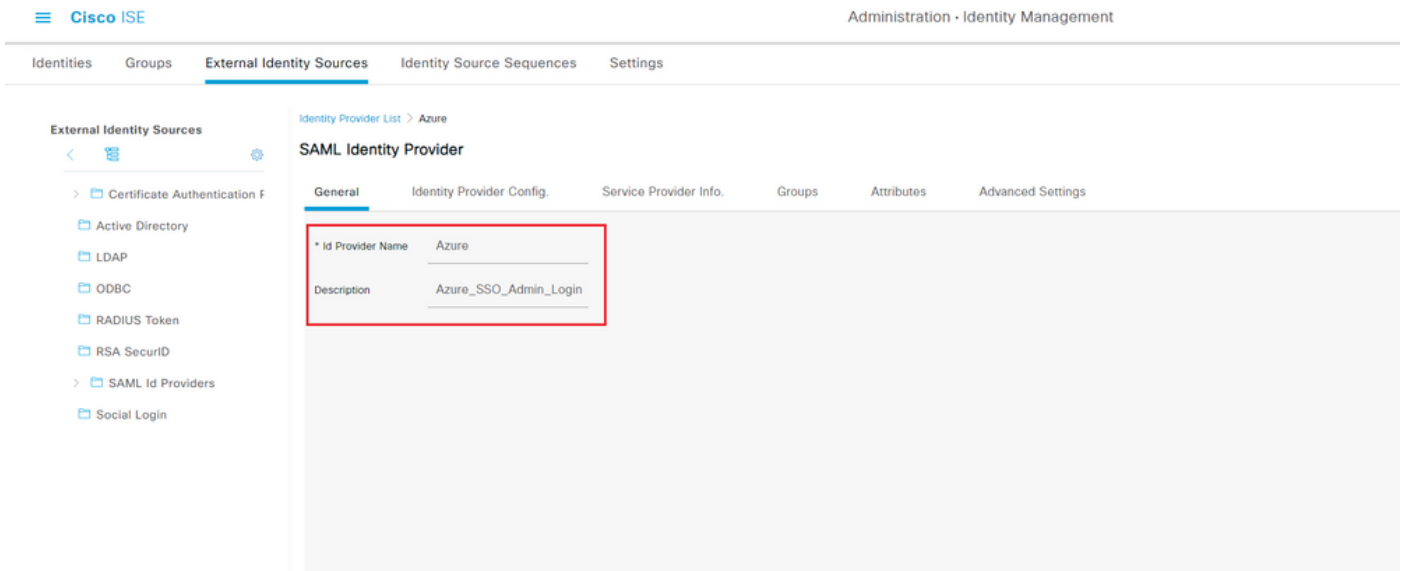
Azure AD와 SAML SSO 통합 구성

1단계. ISE에서 SAML ID 제공자 구성

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.

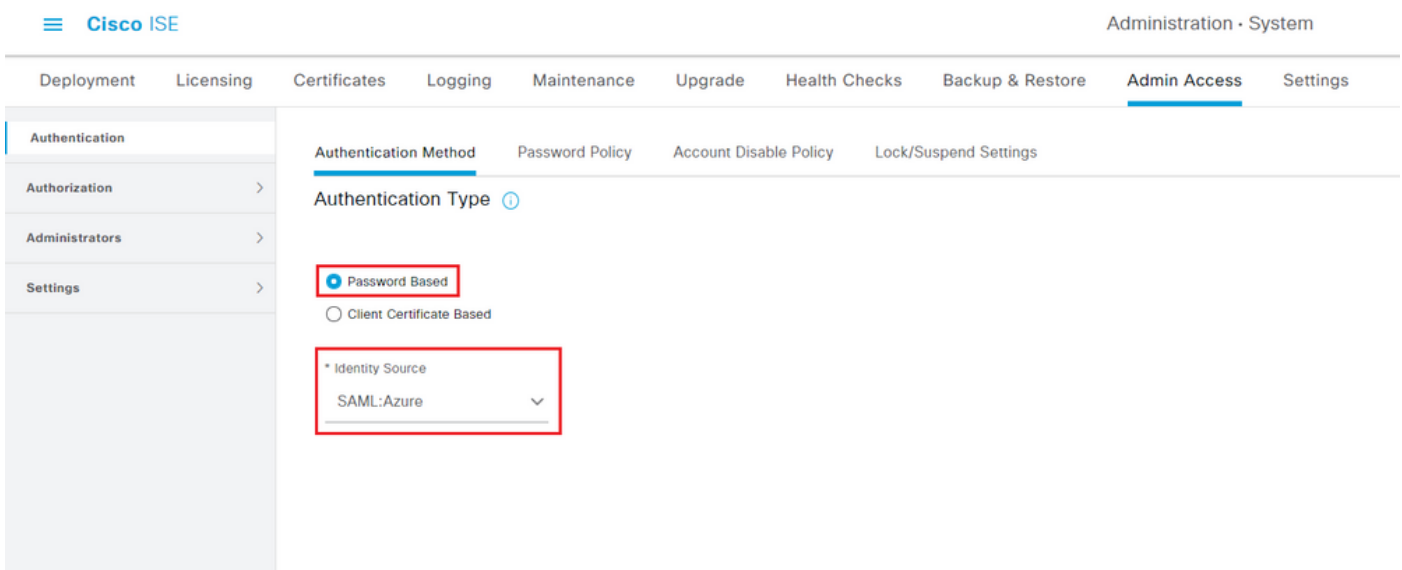
ID 제공자 이름을 입력하고 Submit(제출)을 클릭하여 저장합니다. ID 제공자 이름은 이미지에 표시된 대로 ISE에서만 유효합니다.



2. ISE 인증 방법 구성

Administration(관리) > System(시스템) > Admin Access(관리자 액세스) > Authentication(인증) > Authentication Method(인증 방법)로 이동하고 Password Based(비밀번호 기반) 라디오 버튼을 선택합니다.

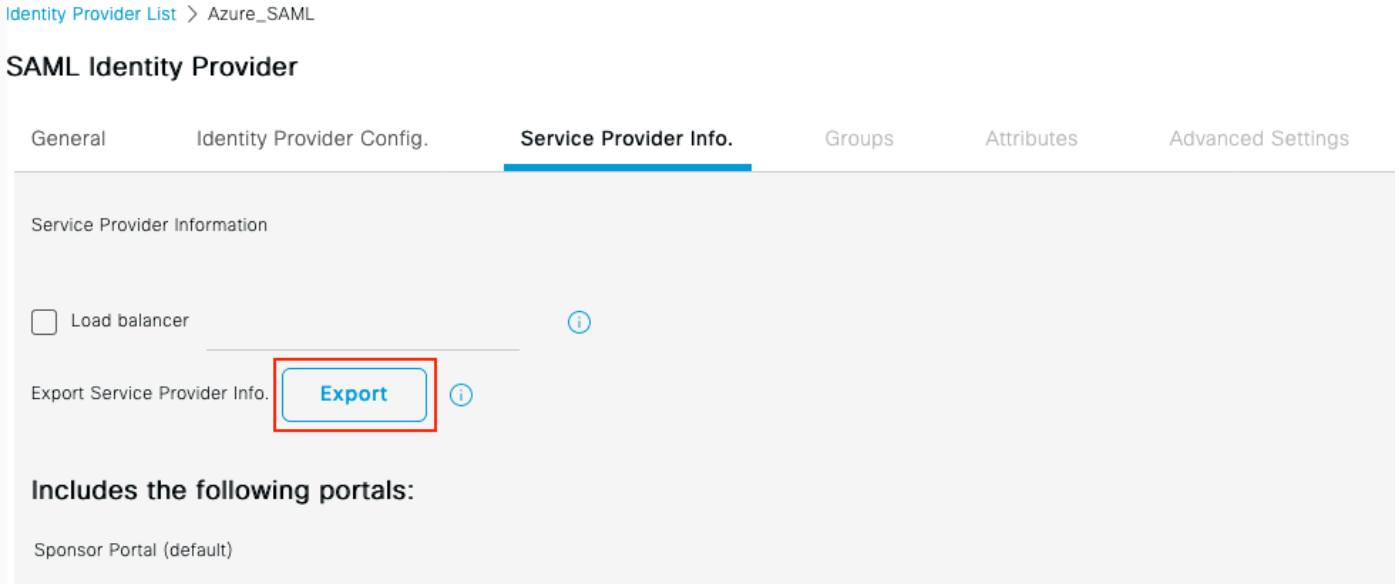
이미지에 표시된 대로 Identity Source(ID 소스) 드롭다운 목록에서 앞서 생성한 필수 ID 제공자 이름을 선택합니다.



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.

탭을 서비스 공급자 정보로 전환하고 이미지에 표시된 대로 내보내기 버튼을 클릭합니다.



.xml 파일을 다운로드하고 저장합니다. 위치 URL 및 entityID 값을 기록해 둡니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmlsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDEExpT
QU1MX21zZTMtMS0xOS5ja3VtYXJyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTG1NBtUxfaXN1My0xLkTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICGKCAgEAavila4+S0uP3j037yCOXnHAzADupfqcgwcp1JQnFxfhVfnDd0ixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohG0t1op01qDGwtOnwZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDziyZjGKDDPf+1VM5JHCo6UNLFIIFyPmGvcCXnt
NVqsYvxSzF038ciQq1m0sqrVrrYzuIUAXDWUNUg9pSGzH0FkSsZRPxRqh+3N5DEFF1Mzybvm1FYu
9h83gl4WJWmizETO6Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0sshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBTO+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+agi6pgZ5058Zot9gqkpfw
kVS9vT4EOzwNGo7pQI8CAwEAaA9MHswIAyDVRORBBkWF4IVaXN1My0xLkTE5LmNrdW1hcjIuY29t
MAWGA1UdEwQFMAMBAF8wCwYDVR0PBAQDAgLSMBOGA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBAQDAggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwqxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZFhgOT2UTgZpRF9F5Hn
CGchSHqDt3bQ7g+Gw1vcgreC7R46qenaonXVr1tRw11vVIDcF8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQwkuLp8zPJUuqfa4H0vdm6of3uBte0/pdUteif0bqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUuwtt6gfH0bE51uT4EYVuuHiwMNGbZqqqb+a4uSkX/EfiDVoLSL6KI31
nf/341vRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cFAZuiv/e3wk0BLZM
1gV8FTVQSnra9LwHP/PgeNAPUCRPXswaKE4rvjvMc0aS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9ys1IHmdqoh3Em0FOgnzR0RvsMPbJxAoTFjfoITTMdQXNHhg+w1POKXS2GCZ29vAM52d8ZCq
```

```
Urz0VxNHKWKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8E0v7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<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 index="0" Location="https://10.201.232.19:8443/portal/SSOLoginResponse.action">
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action">
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

XML 파일의 관련 특성:

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

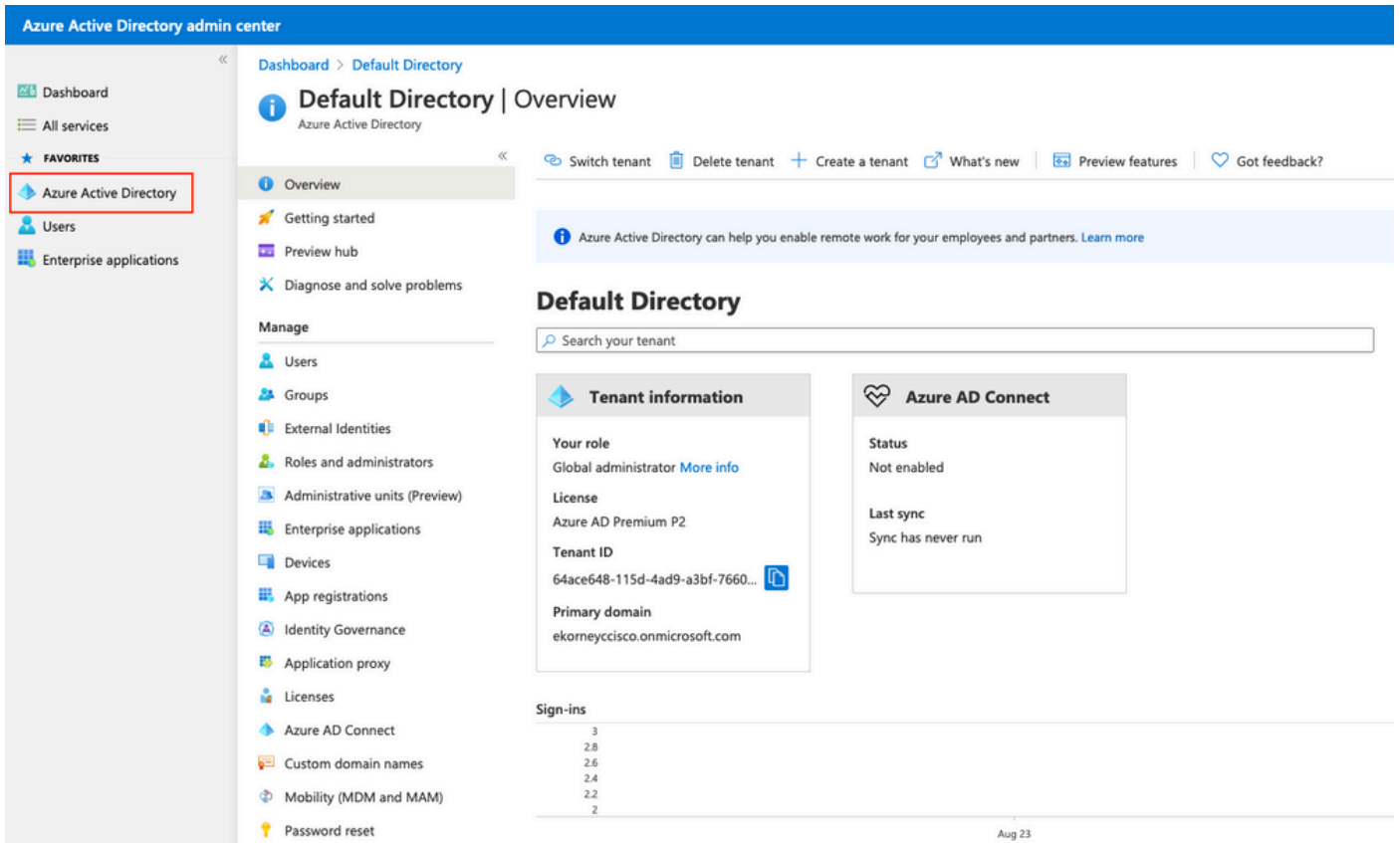
AssertionConsumerService 위치="<https://10.201.232.19:8443/portal/SSOLoginResponse.action>"

AssertionConsumerService 위치="<https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action>"

2단계. Azure AD IdP 설정 구성

1. Azure AD 사용자 만들기

Azure Active Directory 관리 센터 대시보드에 로그인하고 이미지에 표시된 대로 AD를 선택합니다.



사용자를 선택하고 새 사용자를 클릭한 다음 필요에 따라 사용자 이름, 이름 및 초기 암호를 구성합니다. 이미지에 표시된 대로 Create(생성)를 클릭합니다.

Identity

User name * ⓘ

mck ✓ @ gdplab2021.onmicrosoft....
 The domain name I need isn't shown here

Name * ⓘ

mck ✓

First name

Last name

Password

Initial password

Auto-generate password
 Let me create the password

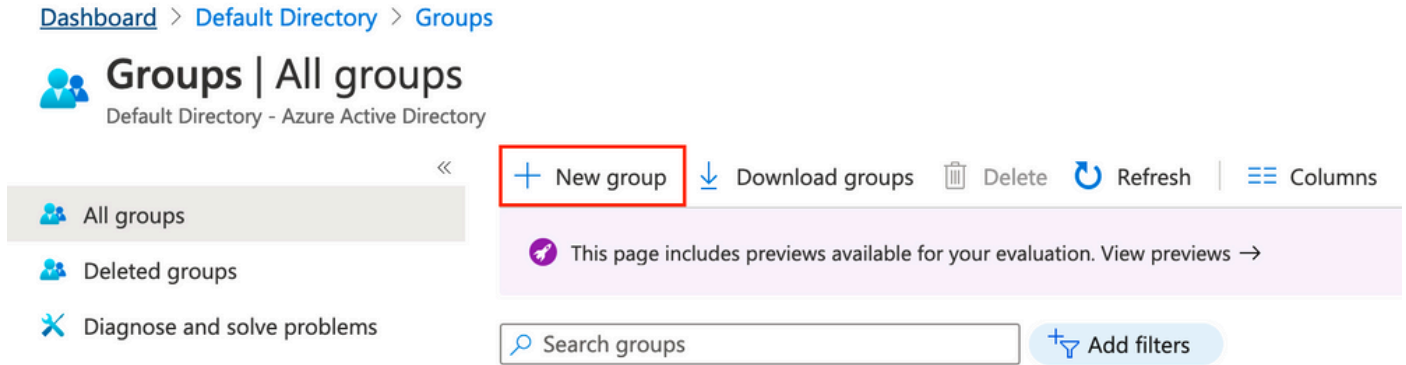
.....

Show Password

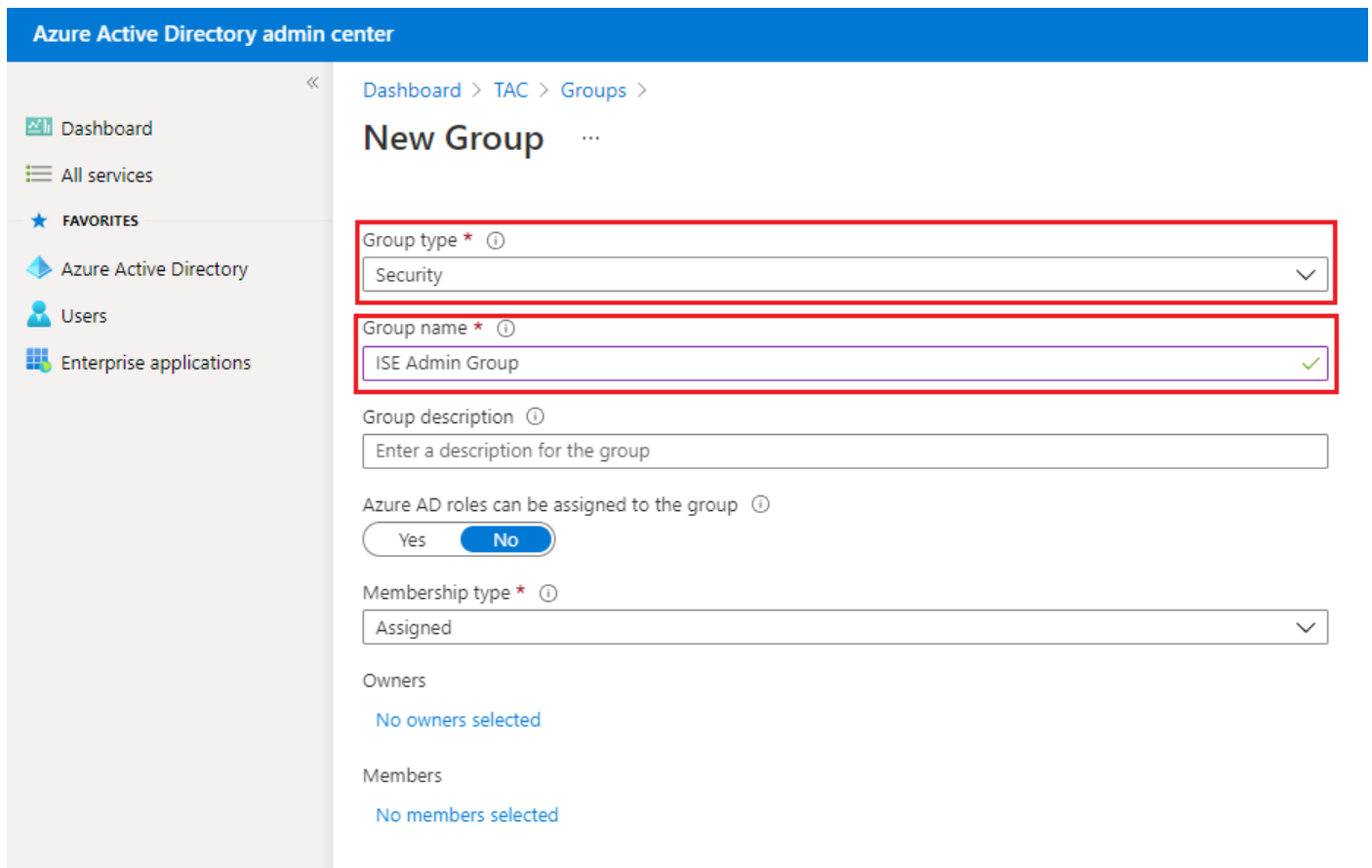
Create

2. Azure AD 그룹 만들기

그룹을 선택합니다. New Group(새 그룹)을 클릭합니다.



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



3. 그룹에 Azure AD 사용자 할당

No members selected(선택한 멤버 없음)를 클릭합니다. 사용자를 선택하고 선택을 클릭합니다. 사용자가 할당된 그룹을 만들려면 만들기를 클릭합니다.

Add members



Search ⓘ



mck
mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

이 화면에서는 그룹 객체 ID를 기록해 둡니다. 이 ID는 이미지에 표시된 ISE 관리자 그룹의 경우 576c60ec-c0b6-4044-a8ec-d395b1475d6e입니다.

Dashboard >

Groups | All groups

TAC - Azure Active Directory

- All groups
- Deleted groups
- Diagnose and solve problems
- Settings
 - General
 - Expiration
 - Naming policy

+ 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"/>	ISE Admin Group	576c60ec-c0b6-4044-a8ec-d395b1475d6e	Security	Assigned

4. Azure AD Enterprise 응용 프로그램 만들기

AD에서 Enterprise Applications를 선택하고 New application을 클릭합니다.

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications

Enterprise applications | All applications

Default Directory - Azure Active Directory

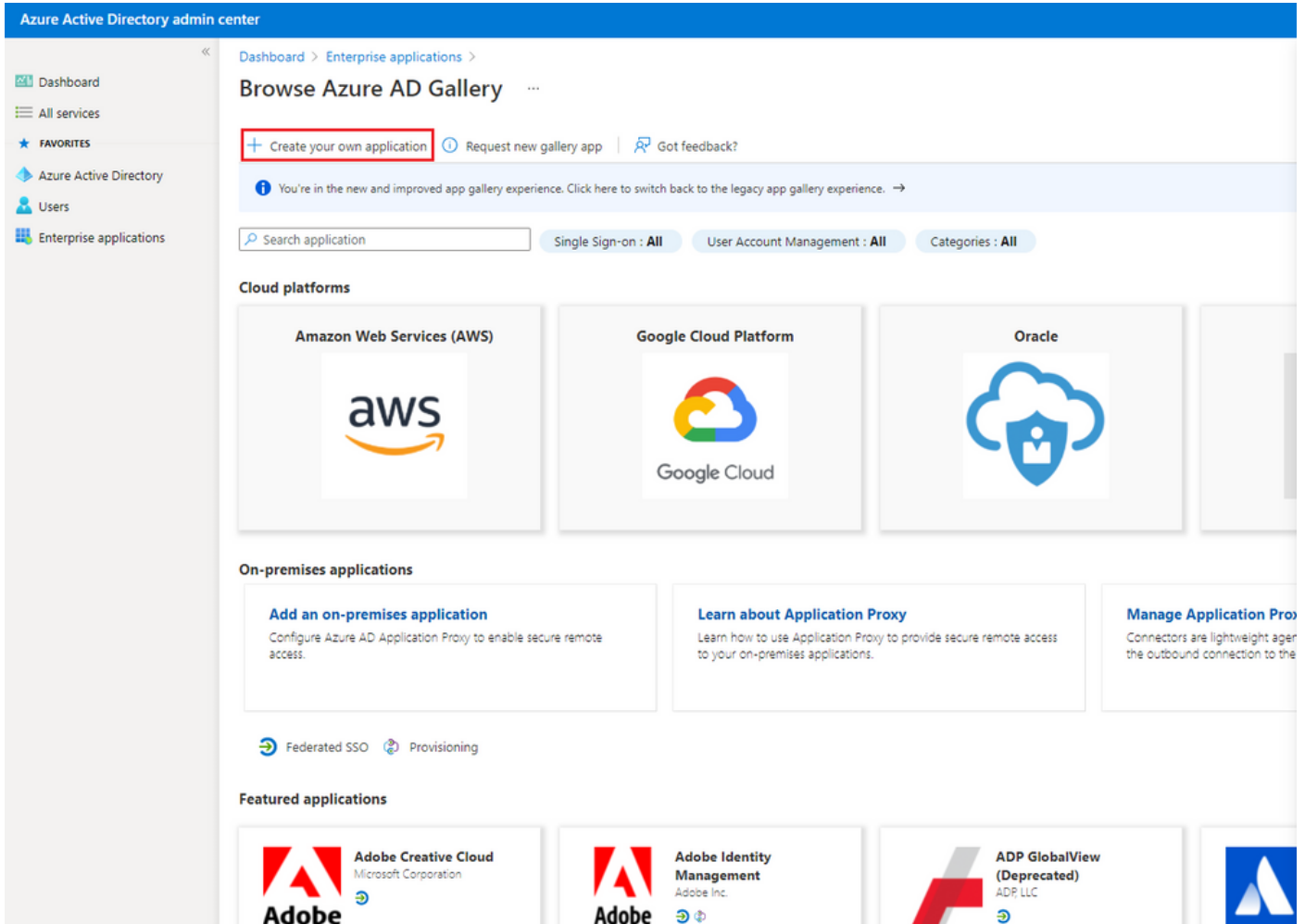
+ New application | Columns | Preview features | Got feedback?

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.

Create your own application을 선택합니다.



응용 프로그램의 이름을 입력하고 갤러리(비갤러리)에서 찾지 못한 다른 응용 프로그램 통합 라디오 버튼을 선택하고 이미지에 표시된 것처럼 만들기 버튼을 클릭합니다.

Create your own application



What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

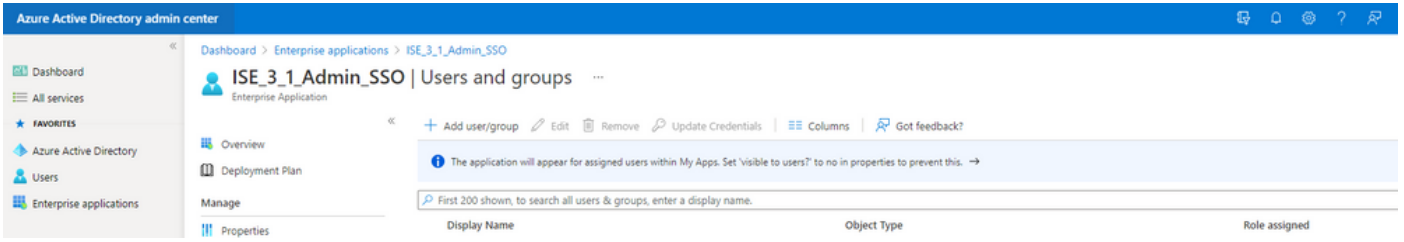
Create

5. 애플리케이션에 그룹 추가

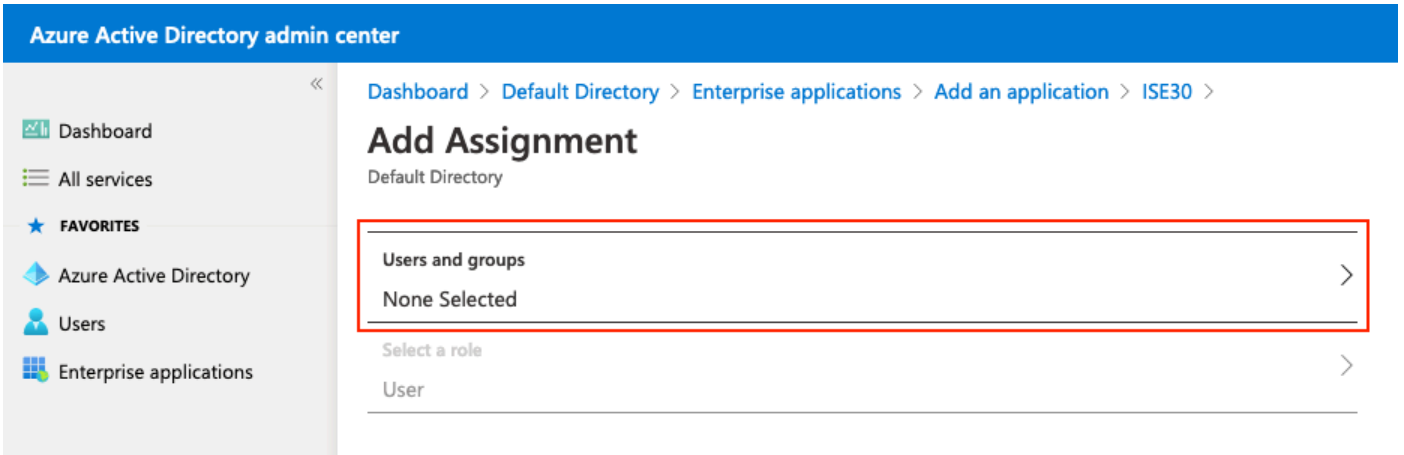
사용자 및 그룹 할당을 선택합니다.

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 'ISE_3_1_Admin_SSO | Overview' and includes a 'Manage' section with options like Overview, Deployment Plan, Properties, Owners, Roles and administrators (Preview), Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, and Security. The 'Properties' section displays the application name 'ISE_3_1_Admin_SSO', Application ID '76b82bcb-a918-4016-aad7-...', and Object ID '22aedf32-82c7-47f2-ab34-1...'. The 'Getting Started' section contains two steps: '1. Assign users and groups' (highlighted with a red box) and '2. Set up single sign on'. Step 1 includes the instruction 'Provide specific users and groups access to the applications' and a link 'Assign users and groups'. Step 2 includes the instruction 'Enable users to sign into their application using their Azure AD credentials' and a link 'Get started'.


Add user/group(사용자/그룹 추가)을 클릭합니다.



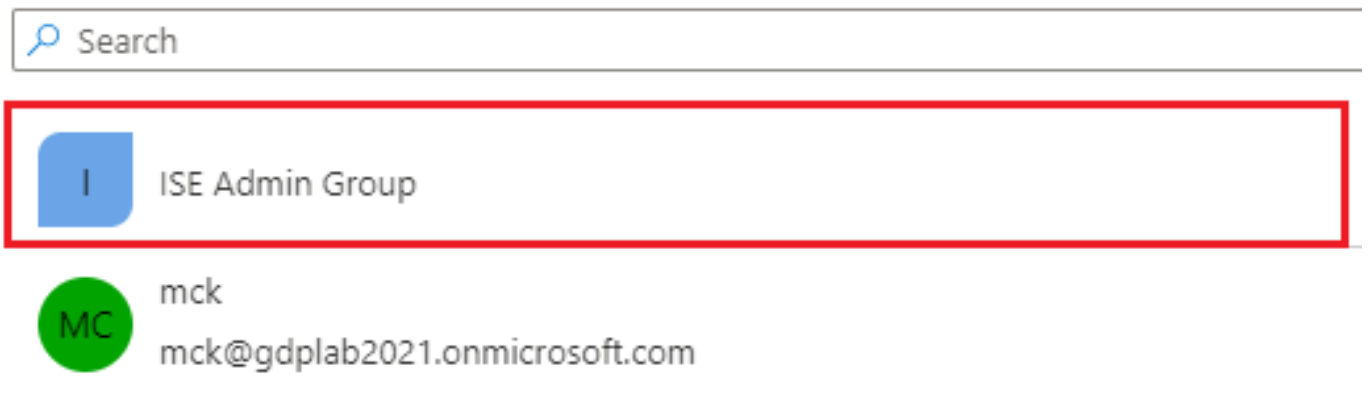
사용자 및 그룹을 클릭합니다.



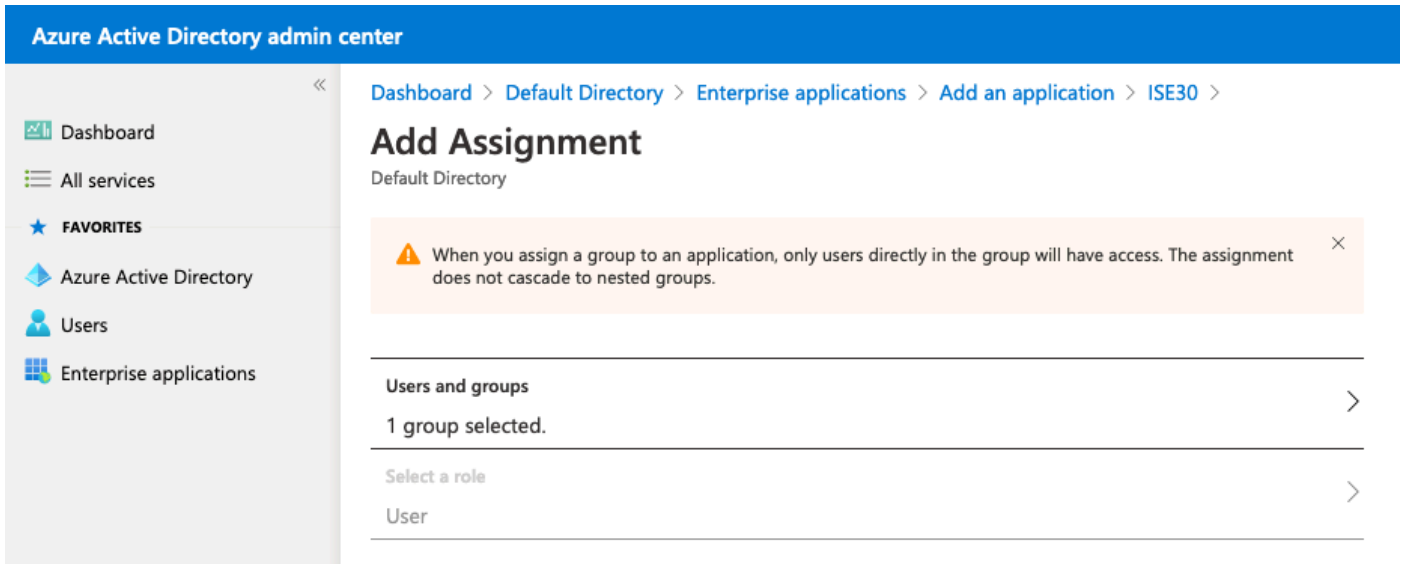
이전에 구성한 그룹을 선택하고 선택을 클릭합니다.

 참고: 설정이 완료되면 여기에 언급된 사용자 및 그룹이 ISE에 액세스할 수 있는 것처럼 원하는 대로 액세스할 수 있는 올바른 사용자 또는 그룹 집합을 선택합니다.

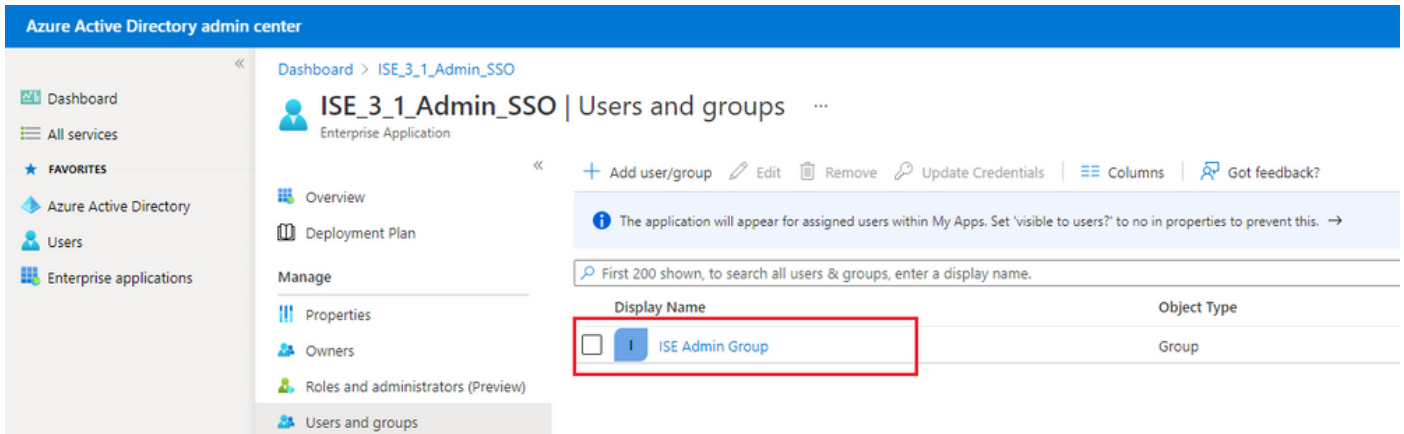
Users and groups



Group(그룹)을 선택한 후 Assign(할당)을 클릭합니다.

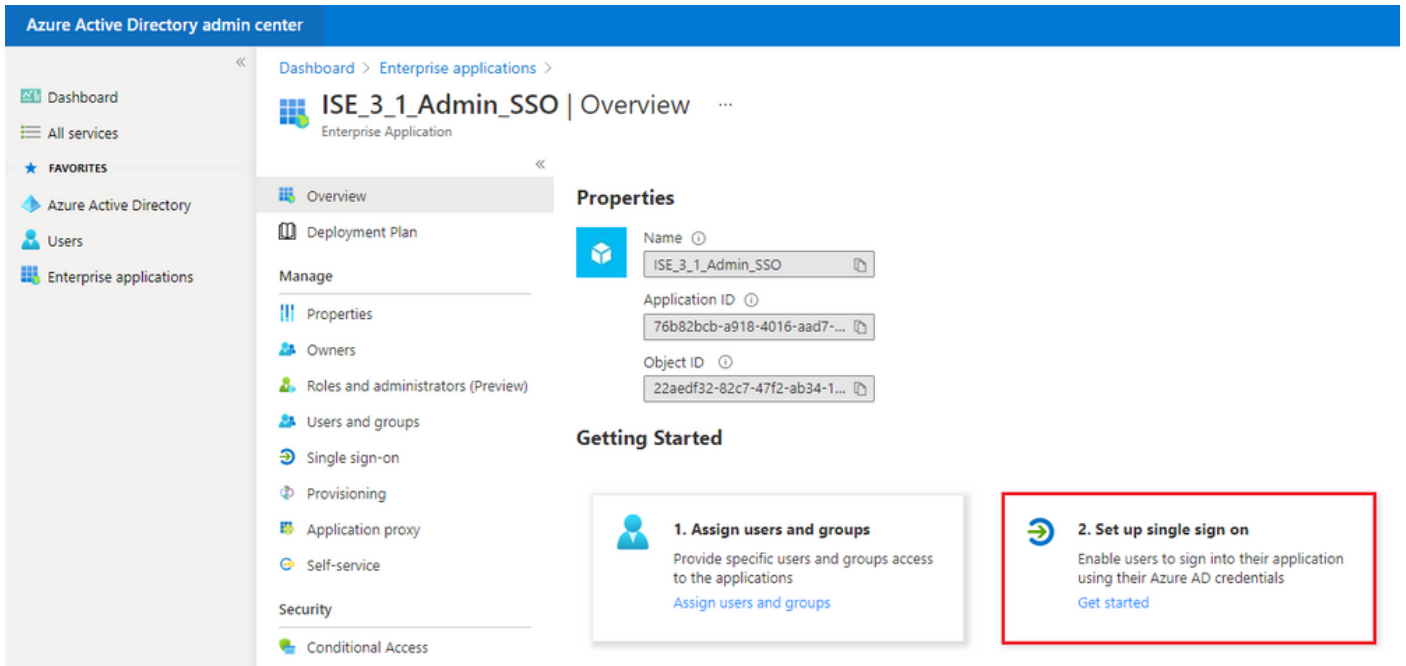


따라서 구성된 애플리케이션의 Users and groups Menu(사용자 및 그룹 메뉴)가 선택된 Group(그룹)으로 채워집니다.

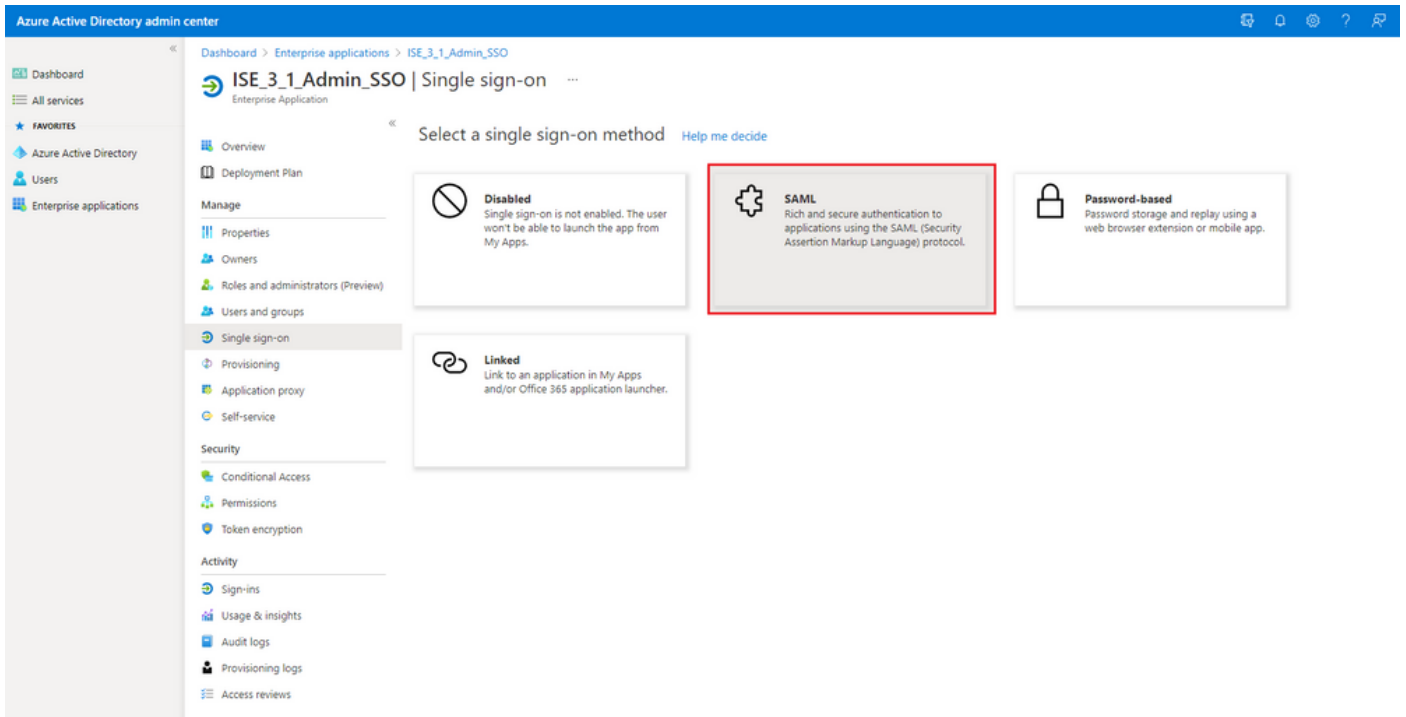


6. Azure AD Enterprise 응용 프로그램 구성

애플리케이션으로 다시 이동하고 Set up single sign on을 클릭합니다.



다음 화면에서 SAML을 선택합니다.




Basic SAML Configuration 옆에 있는 Edit를 클릭합니다.

Set up Single Sign-On with SAML

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

1


Basic SAML Configuration

 Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>


2

User Attributes & Claims

 Edit

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

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. 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

Default

<input checked="" type="checkbox"/> <input type="text" value="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd"/>	<input checked="" type="checkbox"/> ⓘ
<input type="checkbox"/> <input type="text" value="http://adapplicationregistry.onmicrosoft.com/customappsso/primary"/>	<input 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 checked="" type="checkbox"/> <input type="text" value="https://10.201.232.19:8443/portal/SSOLoginResponse.action"/>	<input checked="" type="checkbox"/> ⓘ
<input type="text"/>	

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 > 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. Source attribute 드롭다운 메뉴에서 Group ID를 선택합니다. 확인란을 선택하여 그룹 청구의 이름을 사용자 지정하고 Groups(그룹)라는 이름을 입력합니다.

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

Advanced options

Customize the name of the group claim

Name (required)

Groups

Namespace (optional)

Emit groups as role claims ⓘ

그룹의 클레임 이름을 기록합니다. 이 경우에는 그룹입니다.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO > 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
Groups	user.groups ***
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: B24F48B47B350C93DE3D59EC87EE4C815C884462

Expiration: 7/19/2024, 12:16:24 PM

Notification Email: chandandemo@outlook.com

App Federation Metadata Url: <https://login.microsoftonline.com/182900ec-e960...>

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.

탭을 Identity Provider Config로 전환하고 Browse(찾아보기)를 클릭합니다. Azure Federation Metadata XML 다운로드 단계에서 페더레이션 메타데이터 XML 파일을 선택하고 저장을 클릭합니다.

External Identity Sources

- <  
- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers
- Social Login

Identity Provider List > Azure

SAML Identity Provider

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

Identity Provider Configuration

Import Identity Provider Config File ⓘ

Provider Id

Single Sign On URL <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>

Single Sign Out URL (Redirect) <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>



Sianina Certificates

Subject	Issuer	Valid From	Valid To (Expira...	Serial Number
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azur...	Mon Jul 19 12:16:2...	Fri Jul 19 12:16:24 ...	25 28 CB 30 8B A4 89 8...

4단계. ISE에서 SAML 그룹 구성

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

External Identity Sources

- <  
- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers

Identity Provider List > Azure

SAML Identity Provider

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

Groups

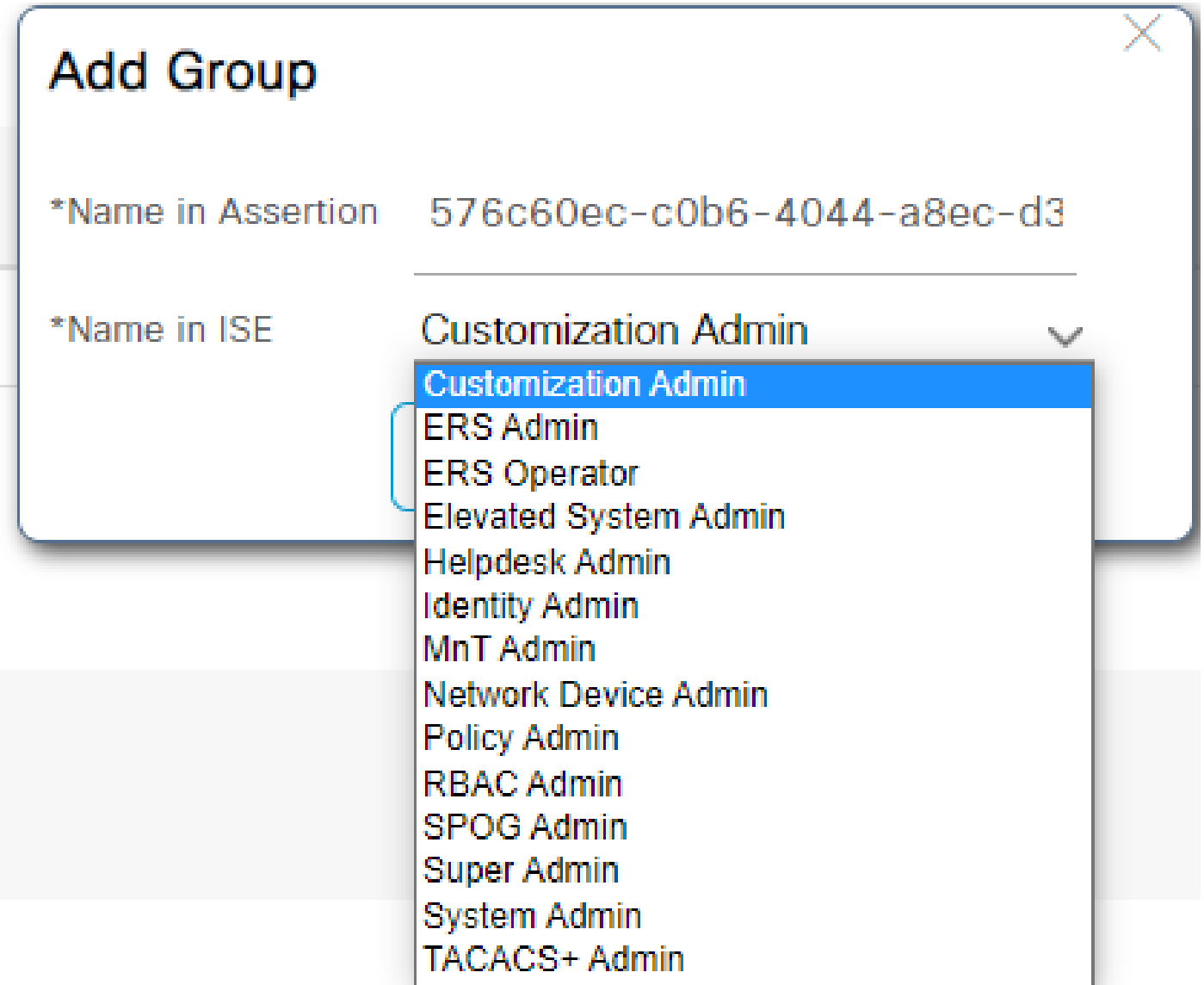
Group Membership Attribute ⓘ

Name in Assertion ^ Name in ISE

Add를 클릭합니다. Assertion에 Name(이름)을 Assertion to the Group(그룹에 Azure Active Directory 사용자 할당)에서 캡처한 ISE 관리자 그룹의 그룹 개체 ID 값으로 채웁니다.

드롭다운으로 ISE의 Name(이름)을 구성하고 ISE에서 적절한 그룹을 선택합니다. 이 예에서 사용된 그룹은 슈퍼 관리자(Super Admin)입니다. OK(확인)를 클릭합니다. 저장을 클릭합니다.

이렇게 하면 Azure의 그룹과 ISE의 그룹 이름 간에 매핑이 생성됩니다.



(선택 사항) 5단계. RBAC 정책 구성

이전 단계에서 ISE에서 구성할 수 있는 다양한 유형의 사용자 액세스 레벨이 있습니다.

RBAC(Role Based Access Control Policies)를 편집하려면 Administration(관리) > System(시스템) > Admin Access(관리자 액세스) > Authorization(권한 부여) > Permissions(권한) > RBAC Policies(RBAC 정책)로 이동하고 필요에 따라 구성합니다.


이 이미지는 샘플 컨피그레이션에 대한 참조입니다.

▼ RBAC Policies

Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin	then Customization Admin Menu ...
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin	then System Admin Menu Access...
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	then Super Admin Data Access
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	then Super Admin Data Access
<input checked="" type="checkbox"/> ERS Trustsec Policy	If ERS Trustsec	then Super Admin Data Access
<input checked="" type="checkbox"/> Helpdesk Admin Policy	If Helpdesk Admin	then Helpdesk Admin Menu Access
<input checked="" type="checkbox"/> Identity Admin Policy	If Identity Admin	then Identity Admin Menu Access...
<input checked="" type="checkbox"/> MnT Admin Policy	If MnT Admin	then MnT Admin Menu Access
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin	then Network Device Menu Acce...
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin	then Policy Admin Menu Access ...
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin	then RBAC Admin Menu Access ...
<input checked="" type="checkbox"/> Read Only Admin Policy	If Read Only Admin	then Super Admin Menu Access ...
<input checked="" type="checkbox"/> SPOG Admin Policy	If SPOG Admin	then Super Admin Data Access
<input checked="" type="checkbox"/> Super Admin Policy	If Super Admin	then Super Admin Menu Access ...
<input checked="" type="checkbox"/> Super Admin_Azure	If Super Admin	then Super Admin Menu Access ...
<input checked="" type="checkbox"/> System Admin Policy	If System Admin	then System Admin Menu Access...
<input checked="" type="checkbox"/> TACACS+ Admin Policy	If TACACS+ Admin	then TACACS+ Admin Menu Acc...

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인합니다.

 참고: Azure 테스트 기능의 SAML SSO 로그인 테스트가 작동하지 않습니다. Azure SAML SSO가 제대로 작동하려면 ISE에서 SAML 요청을 시작해야 합니다.

ISE GUI 로그인 프롬프트 화면을 엽니다. SAML을 사용하여 로그인하는 새로운 옵션이 표시됩니다

1. ISE GUI 로그인 페이지에 액세스하고 SAML로 로그인을 클릭합니다.



Identity Services Engine

Intuitive network security

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

2. Microsoft 로그인 화면으로 이동됩니다. 여기에 표시된 대로 ISE에 매핑된 그룹의 계정에 대한 사용자 이름 자격 증명을 입력하고 이미지에 표시된 대로 Next(다음)를 클릭합니다.



Sign in

mck@gdplab2021.onmicrosoft.com

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

Next

3. 사용자의 비밀번호를 입력하고 로그인을 클릭합니다.



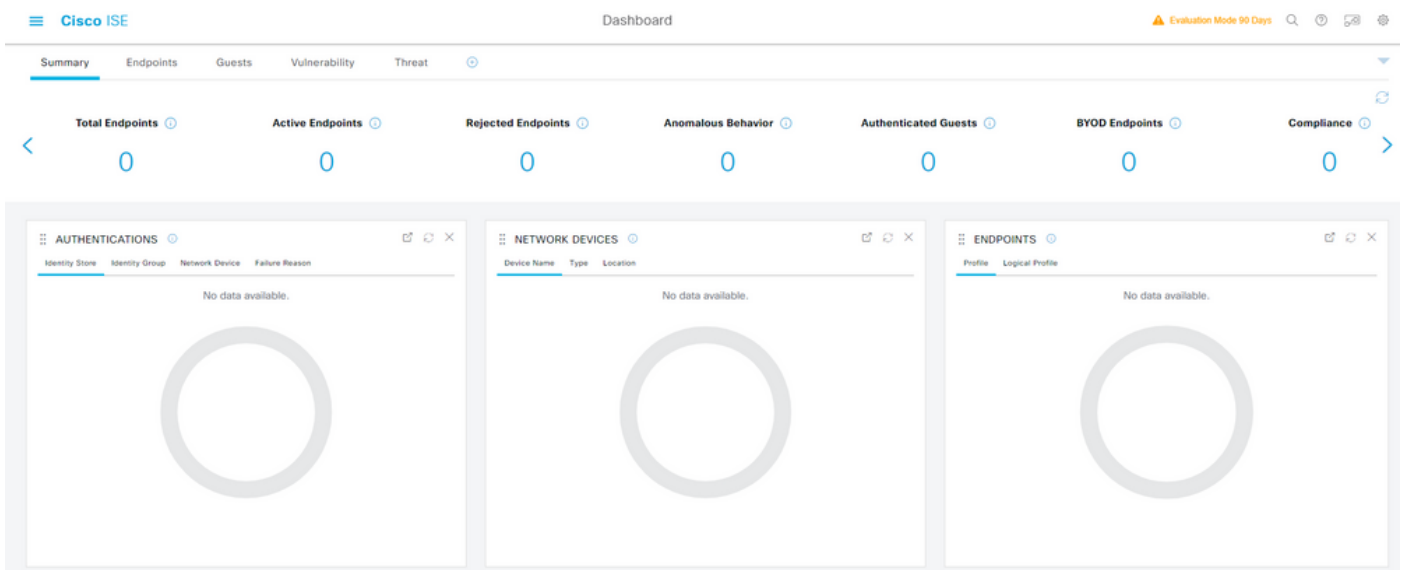
← mck@gdplab2021.onmicrosoft.com

Enter password

[Forgot my password](#)

Sign in

4. 이제 이미지에 표시된 대로 이전에 구성된 ISE 그룹을 기반으로 구성된 적절한 권한을 사용하여 ISE 애플리케이션 대시보드로 리디렉션됩니다.



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. 자격 증명을 입력한 후 "계정 또는 암호가 잘못되었습니다" 오류가 나타납니다. 여기서 사용자 데이터는 아직 ISE에서 수신되지 않으며 이 시점의 프로세스는 여전히 IdP(Azure)를 유지합니다.

계정 정보가 잘못되었거나 암호가 정확하지 않은 경우가 가장 많은 이유입니다. 수정하려면: 이미지에 표시된 대로 비밀번호를 재설정하거나 해당 계정에 올바른 비밀번호를 입력합니다.



← mck@gdplab2021.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. 이전 사례와 마찬가지로 사용자 데이터는 아직 ISE에서 수신되지 않으며 이 시점의 프로세스는 여전히 IdP(Azure)로 유지됩니다.

이 문제를 해결하려면 이미지에 표시된 대로 Add group to the Application configuration(애플리케이션 컨피그레이션에 그룹 추가) 단계가 올바르게 실행되었는지 확인합니다.



Sign in

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

AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Troubleshooting details ✕

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

[Copy info to clipboard](#)

Request Id: 1e15cea0-c349-4bee-922d-26299822a101

Correlation Id: 710626e0-45c1-4fad-baa6-ff7584ecf910

Timestamp: 2021-08-04T22:48:02Z

Message: AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Flag sign-in errors for review: [Enable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

3호 ISE 애플리케이션 서버가 SAML 로그인 요청을 처리할 수 없습니다. 이 문제는 SAML 요청이 서비스 공급자 ISE 대신 ID 공급자 Azure에서 시작될 때 발생합니다. ISE가 ID 공급자가 시작한 SAML 요청을 지원하지 않으므로 Azure AD에서 SSO 로그인 테스트가 작동하지 않습니다.



This page isn't working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO >

ISE_3_1_Admin_SSO | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

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

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

3 SAML Signing Certificate

Status	Active
Thumbprint	824F48B478350C93DE3D59EC87EE4C8
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182900ec-e99e-4403-8100-000000000000
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up ISE_3_1_Admin_SSO

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/182900ec-e99e-4403-8100-000000000000
Azure AD Identifier	https://sts.windows.net/182900ec-e99e-4403-8100-000000000000/
Logout URL	https://login.microsoftonline.com/182900ec-e99e-4403-8100-000000000000

[View step-by-step instructions](#)

5 Test single sign-on with ISE_3_1_Admin_SSO

Test to see if single sign-on is working. Users will need to be added to Users and group

Test single sign-on with ISE_3_1_Admin_SSO

Got feedback?

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up.

Please make sure you have configured ISE_3_1_Admin_SSO before testing.

~~Sign in as current user~~

~~Sign in as someone else~~ (requires browser extension)

Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

What does the error look like?

Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: Saa879f5-68f1-482a-a405-f993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX

[Get resolution guidance](#)

4호 ISE는 로그인 시도 후 "액세스 거부" 오류를 표시합니다. 이 오류는 Azure 엔터프라이즈 응용 프로그램에서 이전에 만든 그룹의 클레임 이름이 ISE에서 일치하지 않을 때 발생합니다.

이 문제를 해결하려면: Azure 및 ISE의 SAML ID 공급자 그룹 탭 아래에 있는 그룹 클레임 이름이 동일한지 확인합니다. 자세한 내용은 이 문서의 Azure AD로 SAML SSO 구성 섹션에서 2.7단계 및 4단계를 참조하십시오.



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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
----------	-------	----------

포털	디버그	guest.log
opensaml	디버그	ise-psc.log
SAML	디버그	ise-psc.log

SAML 로그인 및 일치하지 않는 그룹 클레임 이름이 있는 로그

플로우 실행 시 클레임 이름 불일치 문제 해결 시나리오를 표시하는 디버그 집합(ise-psc.log).



참고: 굵게 표시된 항목을 확인하십시오. 명확성을 위해 로그를 줄였습니다.

1. 사용자가 ISE 관리 페이지에서 IdP URL로 리디렉션됩니다.

<#root>

```
2021-07-29 13:48:20,709 INFO [admin-http-pool46][] api.services.persistence.dao.DistributionDAO -:::
2021-07-29 13:48:20,712 INFO [admin-http-pool46][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::
```

forwardStr for: <https://10.201.232.19/admin/LoginAction.do>

```
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
```

IDP URL: <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>

```
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
```

SAML request - spUrlToReturnTo: <https://10.201.232.19:8443/portal/SSOLoginResponse.action>

```
2021-07-29 13:48:20,844 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:20,851 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.sam].framework.impl.SAM
```

2. 브라우저에서 SAML 응답을 수신합니다.

<#root>

```
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.sam].framework.impl.SAM
```


2021-07-29 13:48:27,369 ERROR [admin-http-pool50][] cpm.admin.infra.action.LoginAction -:::- Can't save

2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.action.LoginActionResultHandler -:::

2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::

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.