

# SAML과 Duo SSO 및 Windows AD의 통합을 사용하여 ISE 3.1 GUI 관리 로그 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

#### [배경 정보](#)

[IdP\(ID 공급자\)](#)

[서비스 공급자\(SP\)](#)

[SAML](#)

[SAML 어설션](#)

#### [고급 흐름도](#)

#### [SAML SSO와 Duo SSO의 통합 구성](#)

##### [1단계. ISE에서 SAML IdP 구성](#)

[Duo SSO를 외부 SAML ID 소스로 구성](#)

[Duo 관리 포털에서 SAML 메타데이터 XML 파일 가져오기](#)

[ISE 인증 방법 구성](#)

[관리자 그룹 생성](#)

[관리 그룹에 대한 RBAC 정책 생성](#)

[그룹 구성원 추가](#)

[SP 정보 내보내기](#)

##### [2단계. ISE에 대한 Duo SSO 구성](#)

##### [3단계. Cisco ISE와 Duo SSO를 일반 SP로 통합](#)

#### [다음을 확인합니다.](#)

[Duo SSO와의 통합 테스트](#)

#### [문제 해결](#)

---

## 소개

이 문서에서는 Cisco Duo SSO와 같은 외부 ID 제공자와 Cisco ISE 3.1 SAML SSO 통합을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE(Identity Services Engine) 3.1

- SAML(Security Assertion Markup Language) SSO(Single Sign-On) 배포(SAML 1.1)에 대한 기본 지식
- Cisco DUO SSO에 대한 지식
- Windows Active Directory에 대한 지식

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 3.1
- Cisco Duo SSO
- Windows Active Directory

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 Duo SSO는 사용자 ID를 확인하고 요청된 리소스('서비스 공급자')에 대한 액세스 권한을 어설션합니다.

Duo SSO는 IdP의 역할을 하며, SAML 1.1 또는 SAML 2.0 IdP(예: Microsoft Azure)가 있는 기존 온-프레미스 AD(Active Directory)를 사용하여 사용자를 인증하고 서비스 공급자 응용 프로그램에 대한 액세스를 허용하기 전에 2단계 인증을 요청합니다.

Duo SSO로 보호하도록 애플리케이션을 구성할 때 Duo SSO의 특성을 애플리케이션에 보내야 합니다. Active Directory는 추가 설정 없이 작동하지만 SAML(2.0) IdP를 인증 소스로 사용한 경우 올바른 SAML 특성을 전송하도록 구성했는지 확인합니다.

### 서비스 공급자(SP)

사용자가 액세스하려는 호스팅된 리소스 또는 서비스. 이 경우 Cisco ISE 애플리케이션 서버.

## SAML

SAML은 SP에 권한 부여 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 사용자의 ID 인증과 권한 부여 간의 링크입니다.

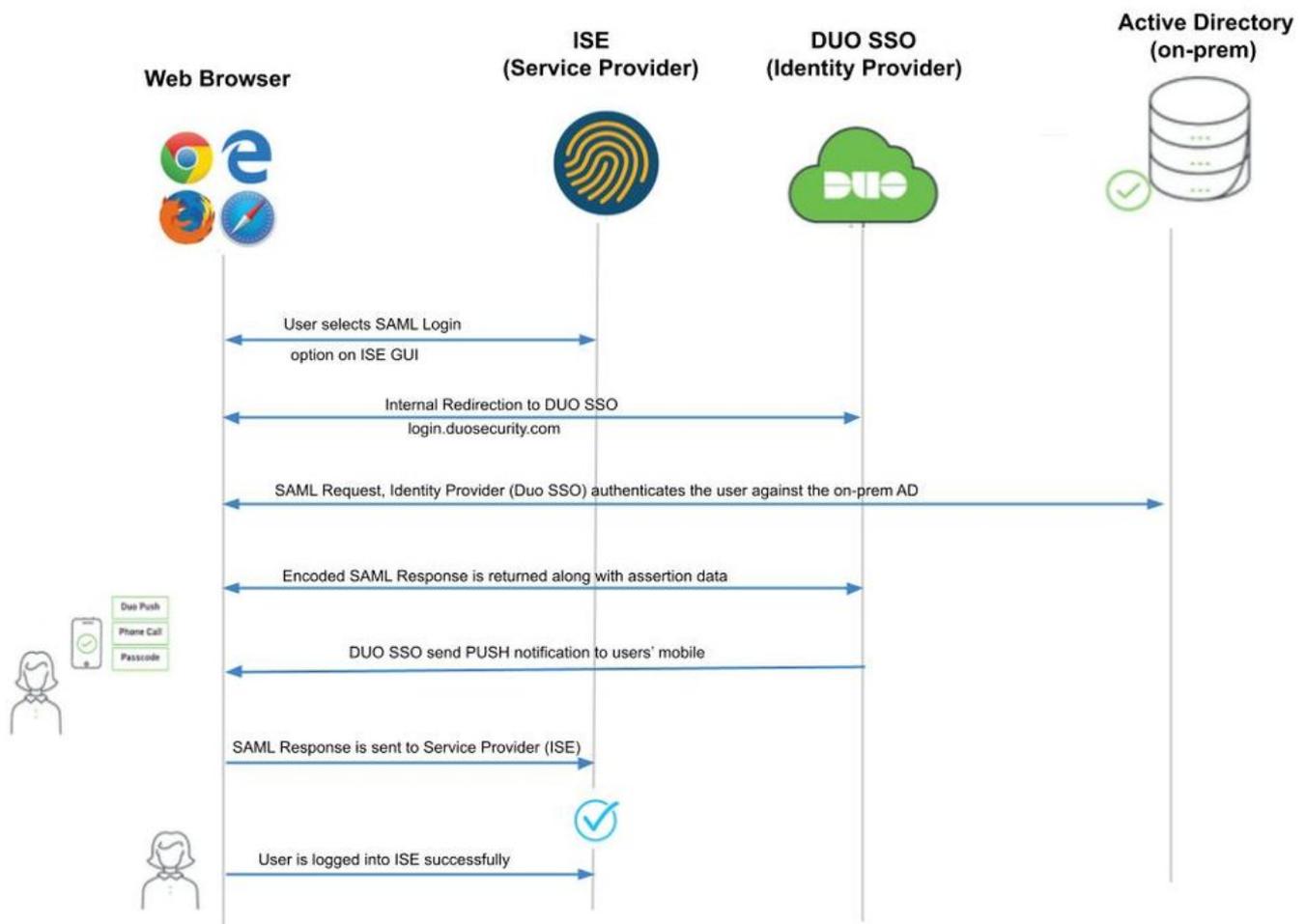
### SAML 어설션

SAML Assertion은 IdP가 사용자 권한 부여가 포함된 서비스 공급자에게 보내는 XML 문서입니다.

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

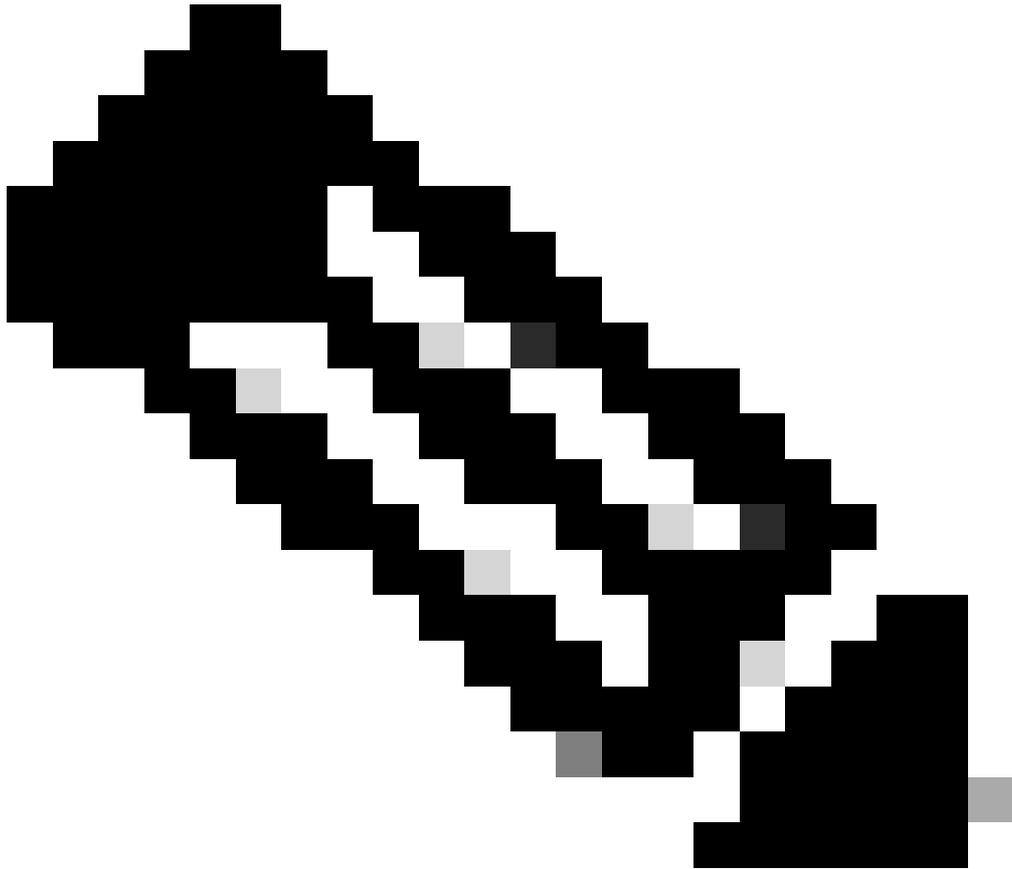
- 인증 어설션은 사용자의 ID를 증명하며 사용자가 로그인한 시간과 사용자가 사용한 인증 방법 (예: Kerberos, 2단계 등)을 제공합니다.
- 특성 어설션은 사용자에게 대한 정보를 제공하는 특정 데이터 조각인 SAML 특성을 SP에 전달합니다.
- 권한 부여 결정 어설션은 사용자가 서비스를 사용할 수 있도록 권한이 부여되었는지 또는 비밀번호 오류 또는 서비스에 대한 권한 부족으로 인해 IdP가 요청을 거부했는지 여부를 선언합니다.

## 고급 흐름도



흐름:

1. 사용자는 Login Via SAML 옵션을 사용하여 ISE에 로그인합니다.
2. ISE(SAML SP)는 사용자의 브라우저를 SAML 요청 메시지와 함께 Duo SSO로 리디렉션합니다.



참고: 분산 환경에서는 Invalid Certificate(유효하지 않은 인증서) 오류를 가져오고 3단계를 수행할 수 있습니다. 이제 작업을 수행할 수 있습니다. 따라서 분산 환경의 경우 2단계에서는 다음과 같은 점에서 약간 다릅니다.

문제: ISE는 일시적으로 PSN 노드 중 하나의 포털로 리디렉션합니다(포트 8443).

해결 방법: ISE가 관리 GUI 인증서와 동일한 인증서를 제공하는지 확인하려면 신뢰하는 시스템 인증서가 모든 PSN 노드에서 포털을 사용하는 데에도 유효한지 확인하십시오.

- 
3. 사용자가 기본 AD 자격 증명으로 로그인합니다.
  4. Duo SSO는 이를 AD로 전달하여 Duo SSO에 응답을 반환합니다.
  5. Duo SSO를 사용하려면 사용자가 모바일에서 PUSH를 전송하여 2단계 인증을 완료해야 합니다.
  6. 사용자가 Duo 2단계 인증을 완료합니다.
  7. Duo SSO는 응답 메시지와 함께 사용자의 브라우저를 SAML SP로 리디렉션합니다.
  8. 이제 사용자가 ISE에 로그인할 수 있습니다.

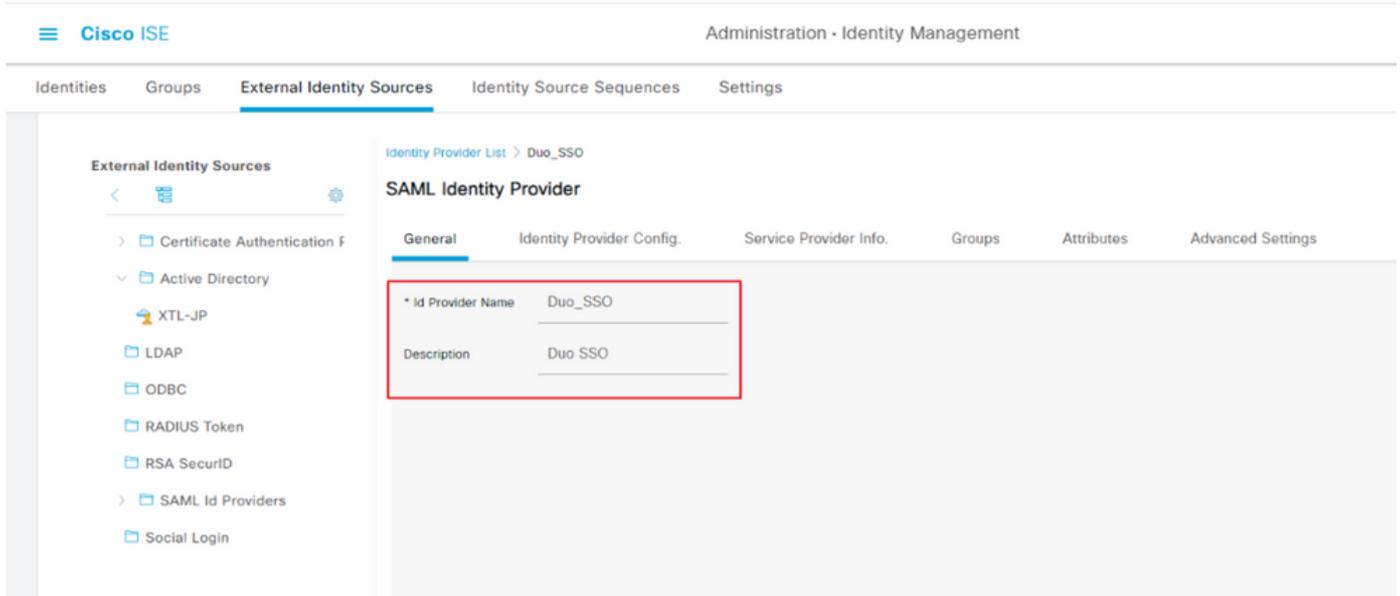
## SAML SSO와 Duo SSO의 통합 구성

## 1단계. ISE에서 SAML IdP 구성

### Duo SSO를 외부 SAML ID 소스로 구성

ISE에서 **로 이동** 하고 Administration > Identity Management > External Identity Sources > SAML Id Providers Add(추가) 버튼을 클릭합니다.

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

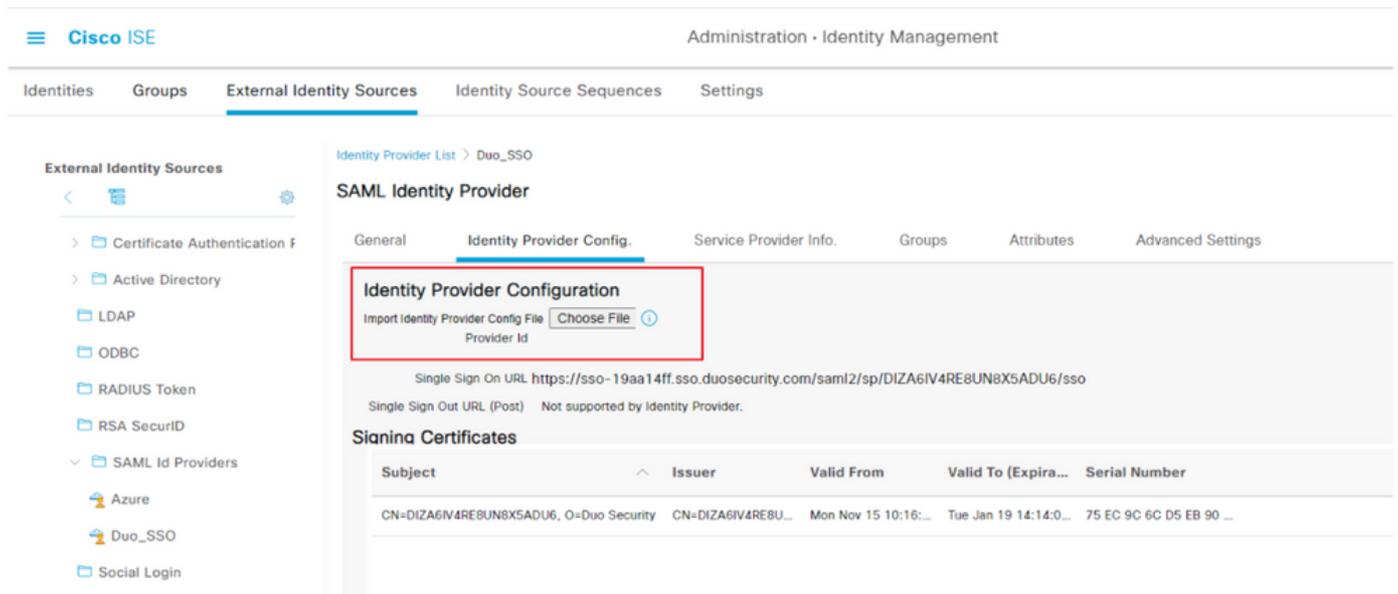


### Duo 관리 포털에서 SAML 메타데이터 XML 파일 가져오기

ISE에서 Administration > Identity Management > External Identity Sources > SAML Id Providers. > Choose the SAML IdP you created(생성한 SAML IdP 선택)로 이동하고 를 클릭한 Identity Provider Configuration 다음 Choose **File(파일 선택)** 버튼을 클릭합니다.

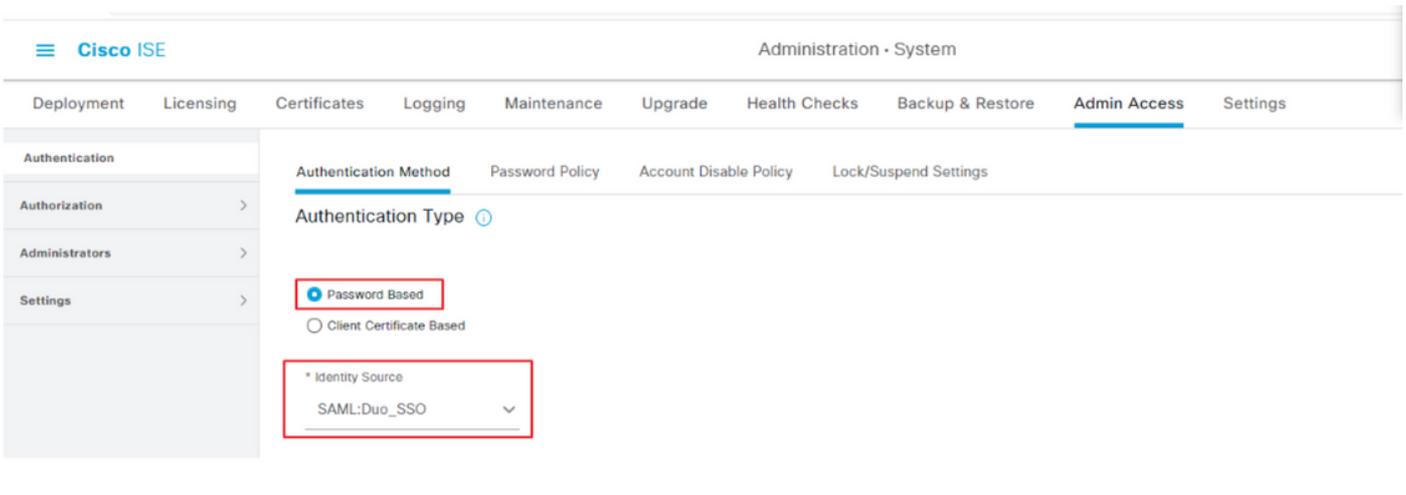
Duo Admin 포털에서 내보낸 **SSO IDP 메타데이터 XML** 파일을 선택하고 Open(열기)을 클릭하여 저장합니다. (이 단계는 이 문서의 Duo 섹션에서도 언급됩니다.)

SSO URL 및 서명 인증서는 다음과 같습니다.



### ISE 인증 방법 구성

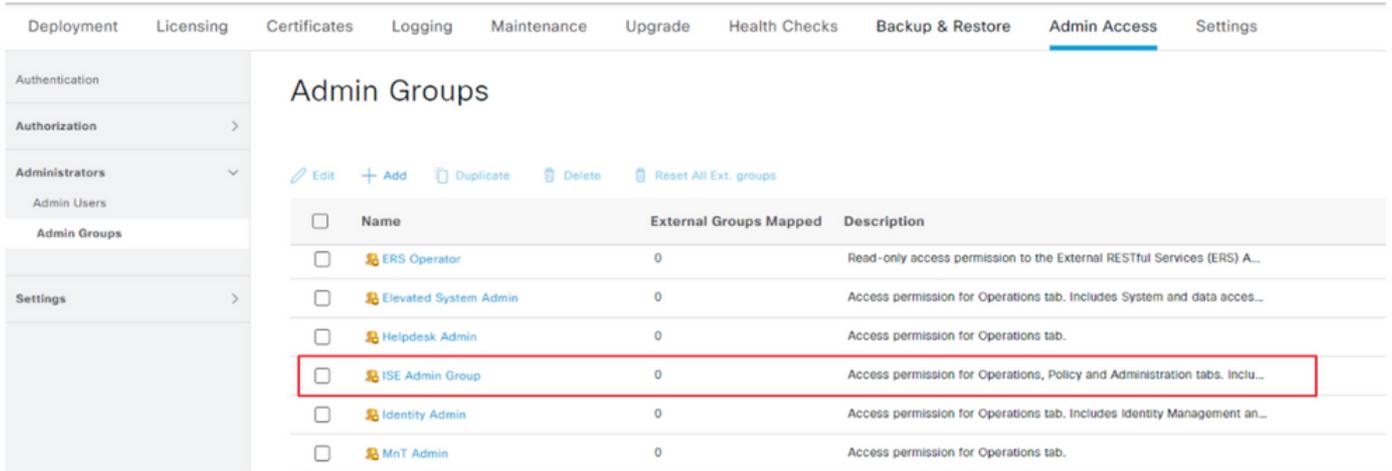
Password-Based(비밀번호 기반) 라디오 버튼으로 이동하여 Administration > System > Admin Access > Authentication > Authentication Method 선택합니다. 이미지에 표시된 대로 Identity Source(ID 소스) 드롭다운 목록에서 이전에 생성한 필수 IdP 이름을 선택합니다.



### 관리자 그룹 생성

로 Administration > System > Admin Access > Authentication > Administrators > Admin Group 이동하여 Super Admin(수퍼 관리자)을 클릭한 다음 Duplicate(복제) 버튼을 클릭합니다. 관리자 그룹 이름을 입력하고 Submit(제출) 버튼을 클릭합니다.

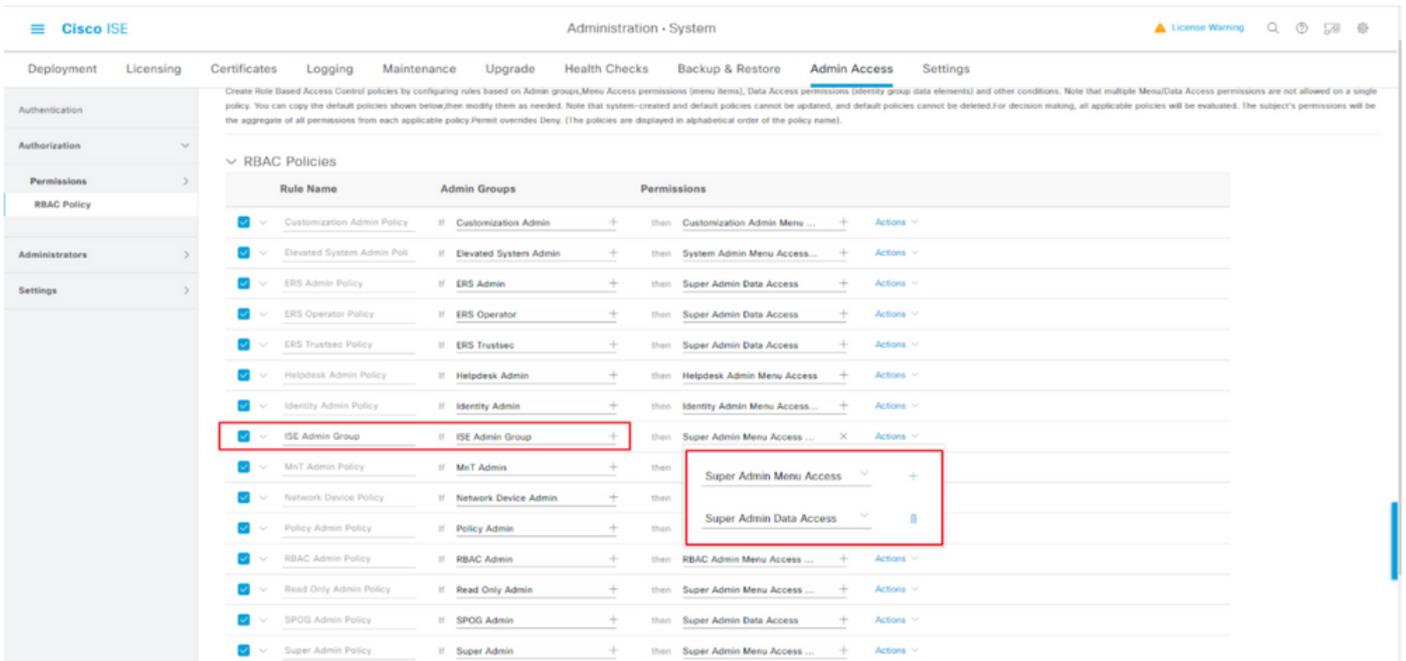
관리자 그룹에 수퍼 관리자 권한을 제공합니다.



관리 그룹에 대한 RBAC 정책 생성

로 Administration > System > Admin Access > Authorization > RBAC Policy 이동하여 슈퍼 관리자 정책에 해당하는 작업을 선택합니다. 를 Duplicate > Add the Name field > Save 클릭합니다.

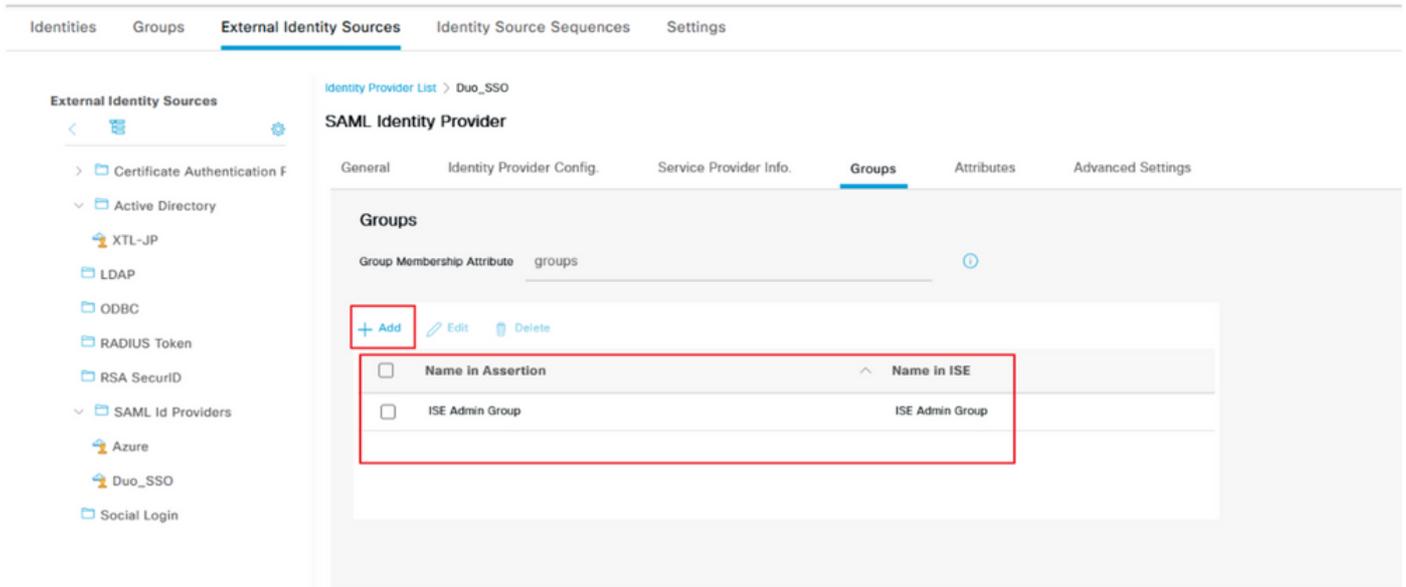
액세스 권한은 슈퍼 관리자 정책과 동일합니다.



그룹 구성원 추가

ISE에서 로 이동하고 Administration > Identity Management > External Identity Sources > SAML Id Providers 생성한 SAML IdP를 선택합니다. Groups(그룹)를 클릭한 다음 Add(추가) 버튼을 클릭합니다.

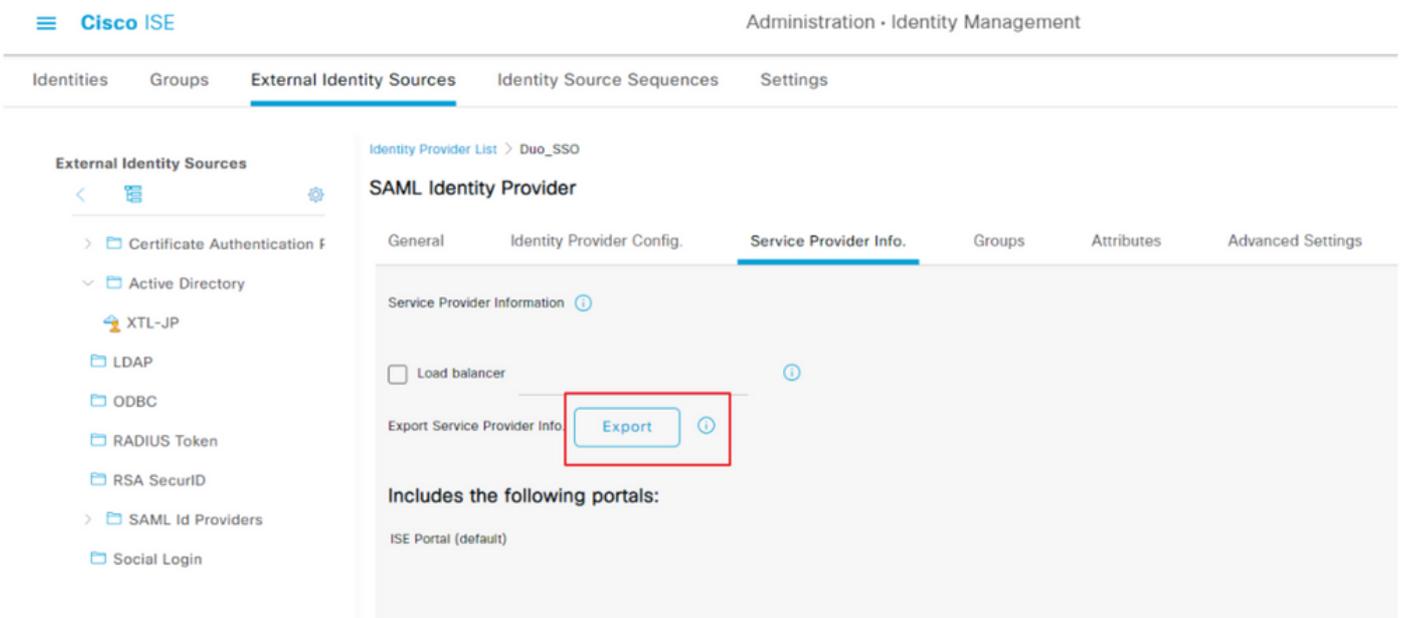
어설션에 이름(ISE 관리자 그룹의 이름)을 추가하고 드롭다운에서 생성된 RBAC(Role-Based Access Control) 그룹을 선택하고(4단계) Open(열기)을 클릭하여 저장합니다. SSO URL 및 서명 인증서는 자동으로 채워집니다.



SP 정보 내보내기

로 Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) 이동합니다.

탭을 SP 정보로 전환하고 이미지에 표시된 대로 **Export**(내보내기) 버튼을 클릭합니다.



파일을 .xml 다운로드하여 저장합니다. Duo SSO 포털에서 이러한 세부 AssertionConsumerService 사항이 필요하므로 위치 URL 및 **entityID** 값을 기록해 둡니다.

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metaData
```

다음은 Duo Generic SAML Integration에서 구성해야 하는 메타 파일에서 수집한 관련 세부 정보/속성입니다

entityID = <http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d>.

AssertionConsumerService 위치 = <https://10.x.x.x:8443/portal/SSOLoginResponse.action> 여기서 10.x.x.x는 XML 파일(위치)에 있는 ISE IP입니다.

AssertionConsumerService 위치 = <https://isenodename.com:8443/portal/SSOLoginResponse.action> 여기서isenodename 는 XML 파일(위치)에 있는 실제 ISE FQDN 이름입니다.

2단계. ISE에 대한 Duo SSO 구성

AD가 있는 Duo SSO를 인증 소스로 구성하려면 이 [KB](#)를 선택합니다.

### Configured Authentication Sources

[+ Add source](#)

| Name                             | Type             | Status  | Authentication Proxies               |
|----------------------------------|------------------|---------|--------------------------------------|
| <a href="#">Active Directory</a> | Active Directory | Enabled | <a href="#">Authentication Proxy</a> |

사용자 지정 [도메인](#)에서 SSO를 활성화하려면 이 KB를 선택합니다.

## Single Sign-On

**1 Custom Subdomain**  
Your users will see the custom subdomain when they authenticate to a Single Sign-On protected application. A familiar URL will help your users know that the site belongs to your organization. The subdomain will be home to Duo Central, if you choose to enable it. Duo Central allows your users to access your organization's sites and applications in one central place.

[Create a custom subdomain](#)

## Customize your SSO subdomain

Tailor the single sign-on experience to match your company's brand and help your users recognize phishing attempts. Your users will see this custom subdomain during authentication.

Custom subdomain  .login.duosecurity.com

Subdomain must contain only letters, numbers, or hyphens (-). Subdomain may not begin or end with a hyphen (-) and must be less than 63 characters in length.

[Save and continue](#) [Complete later](#)

3단계. Cisco ISE와 Duo SSO를 일반 SP로 통합

Cisco ISE를 Duo SSO와 일반 SP로 통합하려면 이 [KB](#)의 1단계와 2단계를 선택합니다.

일반 SP에 대한 Duo Admin(듀오 관리) 패널에서 Cisco ISE SP 세부 정보를 구성합니다.

| 이름                                  | 설명  |
|-------------------------------------|---|
| 엔티티 ID                              | <a href="http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d">http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d</a> |
| ACS(Assertion Consumer Service) URL | <a href="https://10.x.x.x:8443/portal/SSOLoginResponse.action">https://10.x.x.x:8443/portal/SSOLoginResponse.action</a> |

## Service Provider

Entity ID \*

<http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d>

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL \*

<https://10.52.14.44:8443/portal/SSOLoginResponse.action>

Cisco ISE에 대한 SAML 응답을 구성 합니다.

| 이름        | 설명  |
|-----------|---|
| 이름 ID 형식  | urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified |
| NameID 특성 | 사용자 이름  |

## SAML Response

NameID format \*

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

The format that specifies how the NameID is sent to the service provider.

NameID attribute \*

× <Username>

NameID is a SAML attribute that identifies the user. Enter in an IdP attribute or select one of Duo's preconfigured attributes that automatically chooses the NameID attribute based on the IdP. There are five preconfigured attributes: <Email Address>, <Username>, <First Name>, <Last Name> and <Display Name>.

Duo Admin(듀오 관리) 패널에서 Cisco Admin Group(Cisco 관리 그룹)이라는 그룹을 생성하고 이 그룹에 ISE 사용자를 추가하거나 Windows AD에서 그룹을 생성하고 디렉토리 동기화 기능을 사용하여 Duo Admin(듀오 관리) 패널에 동기화합니다.

Cisco ISE에 대한 역할 특성을 구성 합니다.

| 이름    | 설명        |
|-------|-----------|
| 속성 이름 | 그룹        |
| SP 역할 | ISE 관리 그룹 |
| 듀오 그룹 | ISE 관리 그룹 |

**Role attributes** Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional. [Learn more about Duo groups.](#)

**Attribute name**

The name of the attribute which will carry the mapped roles.

**Service Provider's Role**      **Duo groups**

      (+)

Settings(설정) 섹션의 Name(이름) 탭에서 이 통합에 적합한 이름을 제공합니다.

## Settings

**Type**      Generic Service Provider - Single Sign-On

**Name**     

Duo Push users will see this when approving transactions.

컨피그레이션을 저장하려면 Save(저장) 버튼을 클릭하고 자세한 내용은 이 [KB](#)를 참조하십시오.

SAML 메타데이터를 다운로드하려면 Download XML(XML 다운로드)을 클릭합니다.

## Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

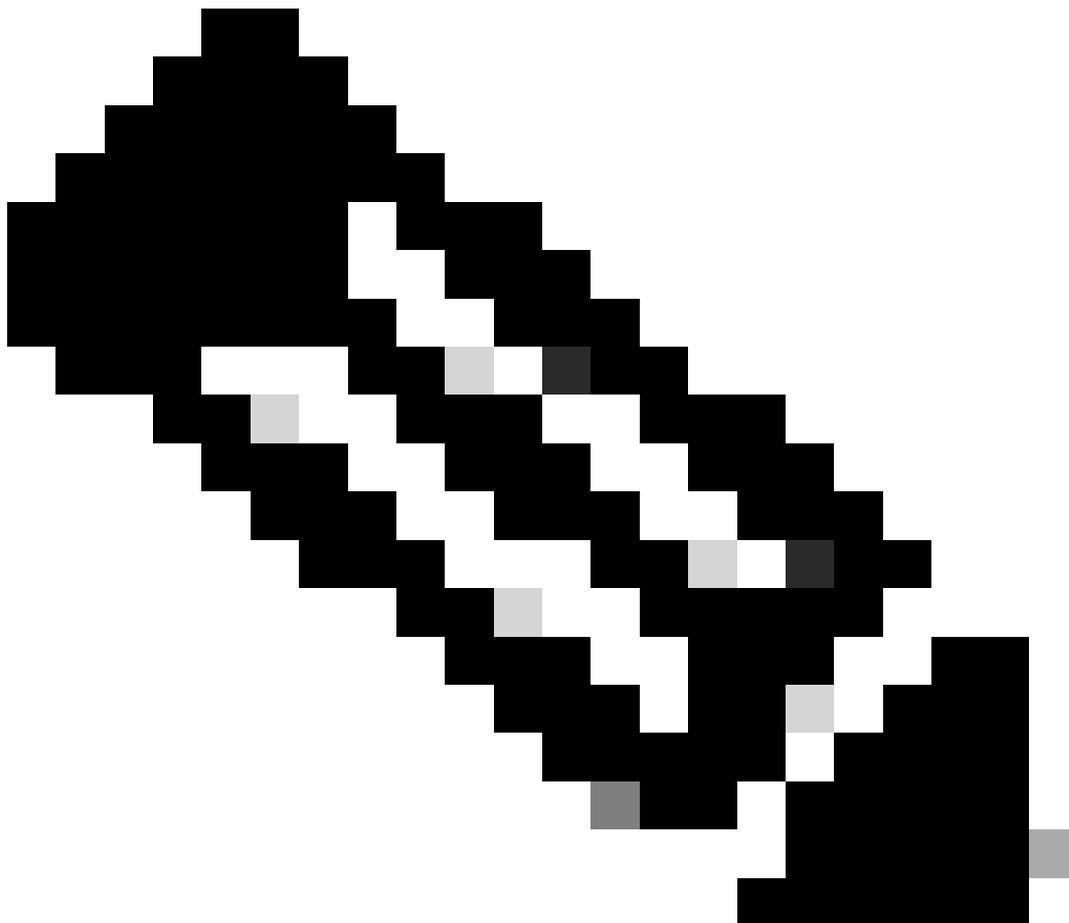
SAML Metadata

[Download XML](#)

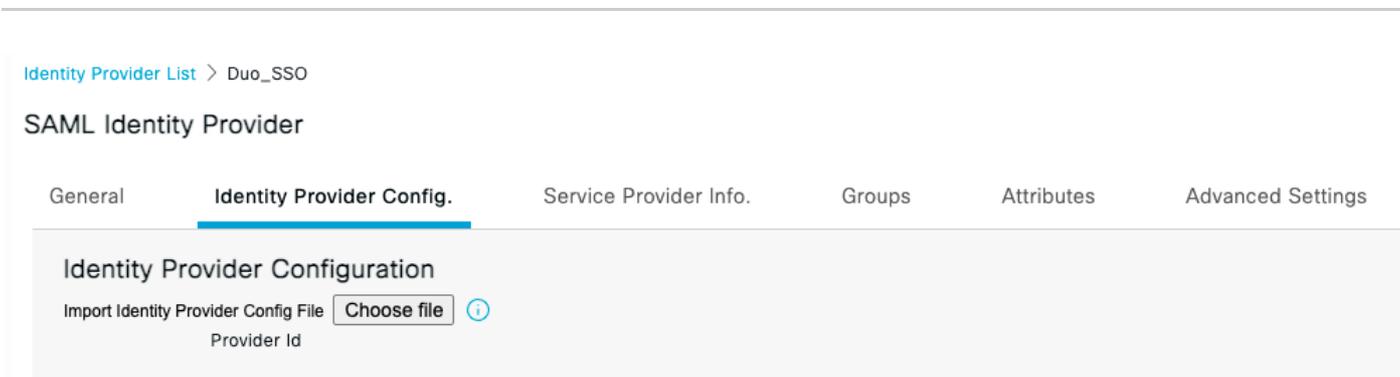
Duo Admin Panel에서 Cisco ISE로 SAML MetaData 다운로드를 업로드합니다 Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo\_SSO.

탭을 ID 공급자 구성으로 전환하고 파일 선택 단추를 클릭합니다.

8단계에서 다운로드한 메타데이터 XML 파일을 선택하고 저장을 누릅니다.



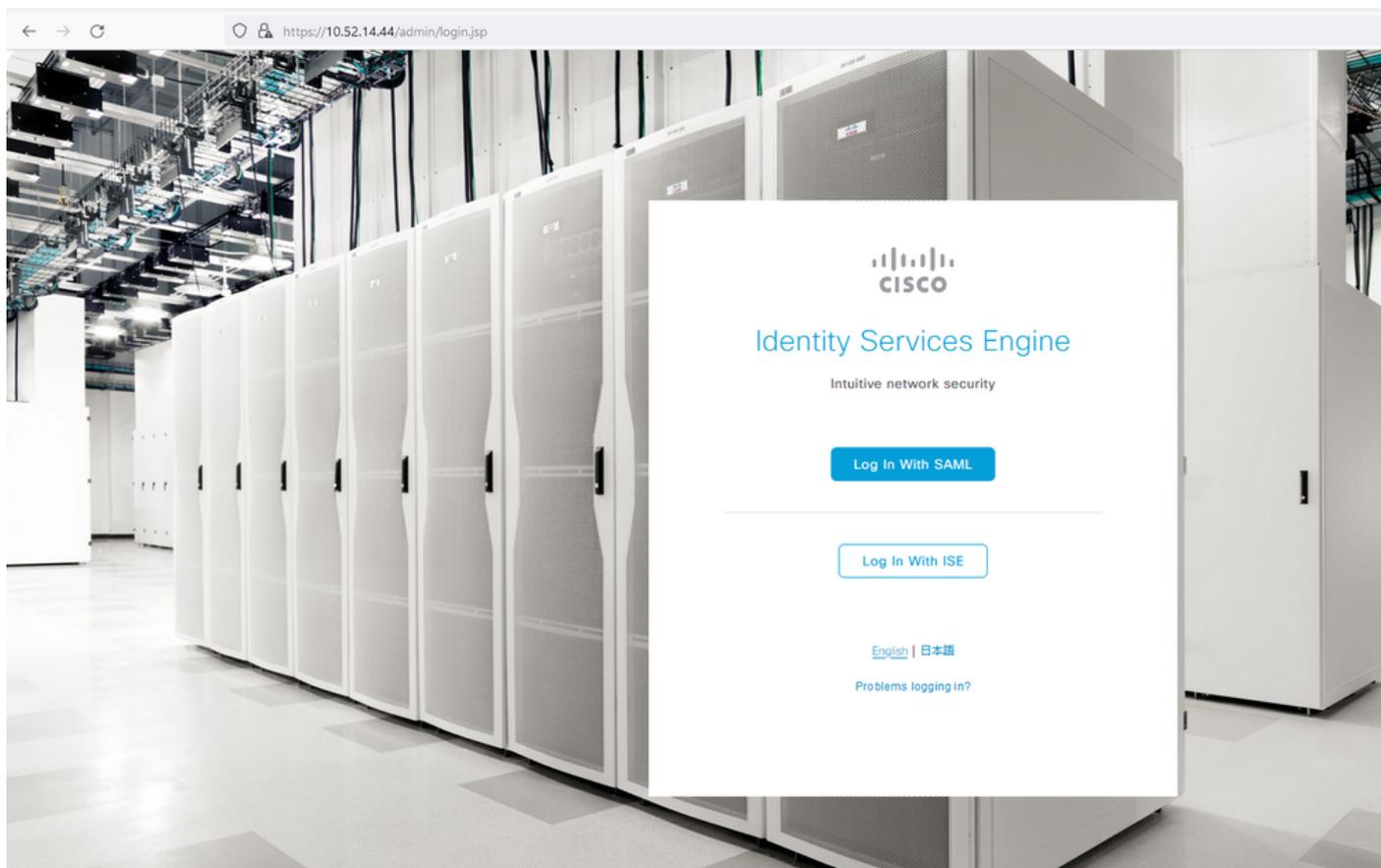
**참고:** 이 단계는 여기에서 Configure SAML SSO Integration with Duo SSO(SAML SSO와 듀오 SSO 통합 구성), 2단계 섹션에 설명되어 있습니다. Duo 관리 포털에서 SAML 메타데이터 XML 파일을 가져옵니다.



다음을 확인합니다.

Duo SSO와의 통합 테스트

1. Cisco ISE Admin Panel(Cisco ISE 관리 패널)에 로그인하고 Log In With SAML(SAML로 로그인)을 클릭합니다.

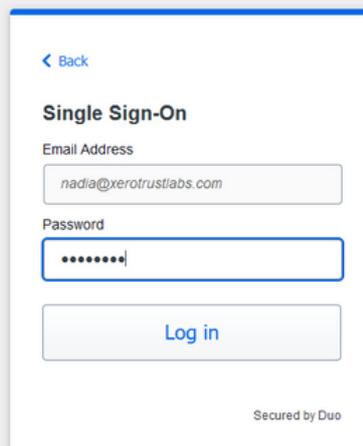


2. SSO 페이지로 리디렉션되고 이메일 주소를 입력하고 Next(다음)를 클릭합니다.



The image shows a web browser window displaying a Cisco Single Sign-On page. At the top left is the Cisco logo. Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below the input field is a button labeled "Next". At the bottom right of the form, it says "Secured by Duo".

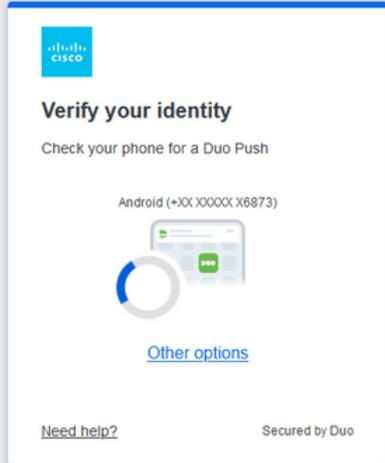
3. 비밀번호를 입력하고 로그인을 클릭합니다.



The image shows a web browser window displaying a Cisco Single Sign-On page. At the top left is a blue arrow pointing left with the text "Back". Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below that is a label "Password" followed by a password input field with masked characters "\*\*\*\*\*". Below the password field is a button labeled "Log in". At the bottom right of the form, it says "Secured by Duo".

4. 모바일 장치에 Duo Push 프롬프트가 표시됩니다.

Duo needs your help  
[Take a quick 6-question survey](#) to help us improve this experience.



The image shows a white rectangular box with a blue border, representing a Duo authentication prompt. At the top left is the Cisco Duo logo. The main heading is "Verify your identity" in bold. Below it, the text says "Check your phone for a Duo Push". A phone number is displayed: "Android (+XX XXXXX X6873)". In the center, there is a graphic of a smartphone with a green push notification icon and a circular progress indicator. Below the phone number is a blue link "Other options". At the bottom left, there is a link "Need help?". At the bottom right, it says "Secured by Duo".

5. 프롬프트를 수락하면 창이 나타나고 자동으로 ISE Admin(ISE 관리) 페이지로 리디렉션됩니다.

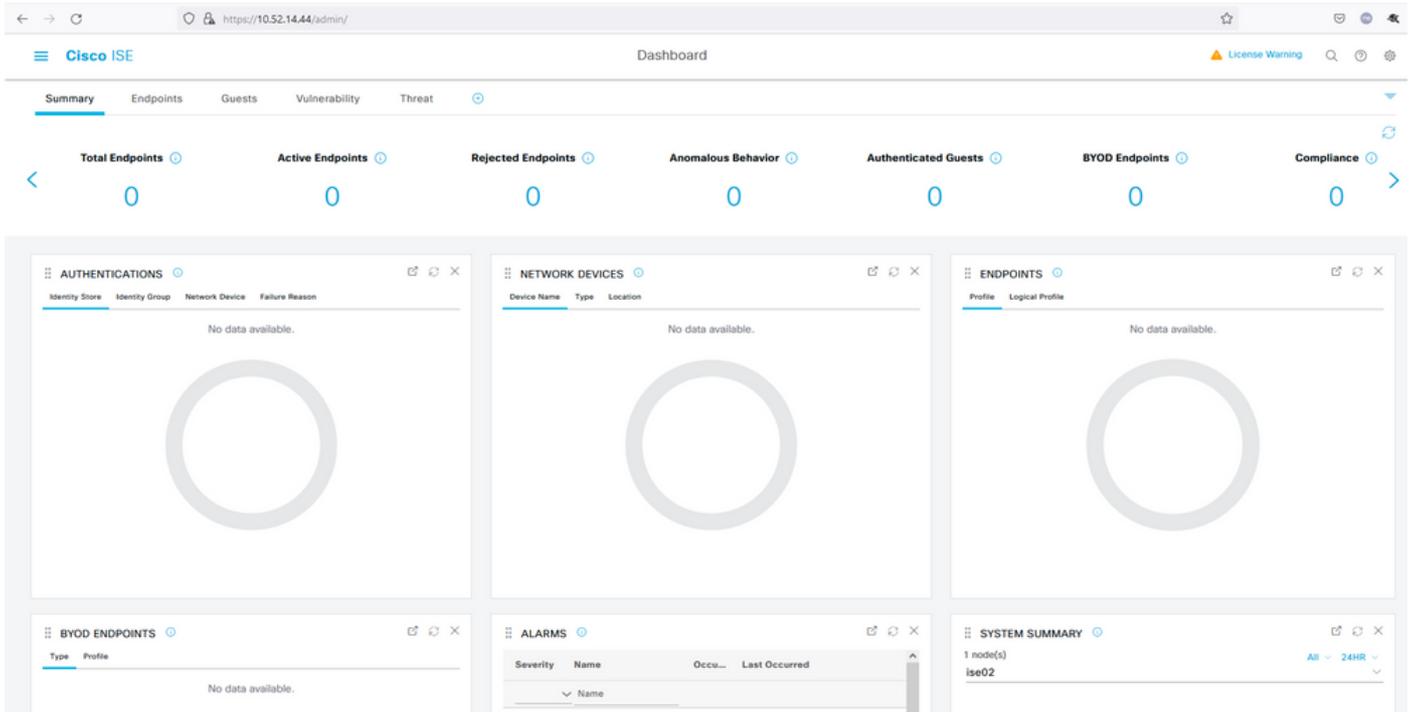


# Success!

Logging you in...



Secured by Duo



## 문제 해결

- Mozilla FF용 SAML 트레이서 확장 프로그램(<https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>)을 다운로드합니다.
- 패킷을 SSOLoginResponse.action 스크롤합니다. SAML 탭에서 Duo SAML에서 보낸 여러 특성(NameID, Recipient(AssertionConsumerService 위치 URL) 및 Audience(EntityID)가 표시됩니다.

```

GET https://zerotrustlabs.login.duosecurity.com/pw/ASOOZM6KCLX6T19QVNA3/ssp_callback?aid=643b5067d1f249f5bf6d744a7603ef83&req-trace-group=dfac3f2db
GET https://zerotrustlabs.login.duosecurity.com/favicon.ico
POST https://10.10.10.10:8443/portal/SSOLoginResponse.action SAML
GET https://10.10.10.10:8443/portal/css/images/favicon.ico
POST https://10.10.10.10:8443/admin/LoginAction.do
GET https://10.10.10.10:8443/admin/
GET https://10.10.10.10:8443/admin/ng/css/vendor/bootstrap/css/bootstrap-dialog.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/fuelux/css/fuelux.min.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/jstree/css/style.min.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/select2/select2.min.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/combobox.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/textboxsubmitter.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/expressionbuilder.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/saveprogressindicator.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/table/treetable.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/table/pagetable.css
GET https://10.10.10.10:8443/admin/pages/utills/css/common_icons.css
GET https://10.10.10.10:8443/admin/pages/utills/css/common_styles.css

```

HTTP Parameters SAML Summary

<ds:X509Data>

```

<ds:X509Certificate>MIIDTCCAFAwIBAgIUCbf+LB1BLJMeF6GV0B1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMGMGA1UECgwMRHRVIFN1Y3VyaXR5MR0wGwYDVQDD
BRESTZPODg2UkxETUJZMzExSFBjMjAeFw0yMTExMjYwMjQNTFAwFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMDER1byBTZW51cm10eTEdMBsGA1UEAwwURk2Tzg4N1JMRE
1CWTMxMuhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NoQzIhQZzu9H8vU/HSKLSH3058SMukj5FnoVV50PGTuoFN4u90tSiFULjC8eQnUs
BR1PYQ5jt0V23qVnvoGyqsuHAs8nbKwvzPShzNF59p03pXkoGPuB+Du2IrrvV0opSv4vbrgKV+H/bvMqyhIA6ywfHNZedG7pbwrYBtVPDXUpnLQvtL2
/Vd9230XuXHF+k32hagRgTLub5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49
/w+r5fz7xp66muRc0IBg3xjWnnFnyujy7v5ifn1KFUFQu+86A5GbuUWCyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB
/wQFMAMBAF8wDQYJKoZIhvcNAQELBQADggEBAH+Kitcw0KtDxXBvZ5S+25a+50F4Tqd/pHh56i19d2kDxInSUVsy
/Yy1FXAWge3WBke4b3JR7znD6000sZTYbF9w7H4svU2gxzdk0znXJNj2e4C5fDivnj/TawZakp2MbTaxfV2VTL0K0kV/1jM6PL61PbKGFwNmh+SjW/VseS+71C701eI
/U095XLbAu2iIny9zfv0hKNV72L8fgYgrjhpdxH8Y1SxPbVWZMwzytbwZFUogD30XrPq16aXZvJyOH5Vs0H90wQ8qQ48hI4F4J3DyRPNH1PzQTYM38kjymEkE0DJPcaGy9v
EMinHUkdwpiETB52Cmtwg+DzAw1jpc=</ds:X509Certificate>
</ds:X509Data>
<ds:KeyInfo>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">nadia</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2021-12-02T04:48:56Z"
Recipient="https://10.10.10.10:8443/portal/SSOLoginResponse.action"
InResponseTo="_7fdfc239-631e-439c-a3ab-f5e56429779d_SEMIportalSessionId_EQUALS859ee9c3-60e4-4482-9426-
b3904d4d6226_SEMItoken_EQUALS1RS257BC24SGVHZW76GMVEZNR0YCCCL_SEMI_DELIMITER10."/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2021-12-02T04:43:26Z"
NotOnOrAfter="2021-12-02T04:48:56Z"
>
<saml:AudienceRestriction>
<saml:Audience>http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2021-12-02T04:43:56Z"
SessionIndex="DUO_8dfe494ab8d617884446cb8f2259bb4a56492ef"
>
</saml:AuthnStatement>
</saml:AuthnContext>

```

1846 requests received (490 hidden)

- ISE의 라이브 로그:

Steps

5231 Guest Authentication Passed

| Overview             |                                  |
|----------------------|----------------------------------|
| Event                | 5231 Guest Authentication Passed |
| Username             | nadia                            |
| Endpoint Id          |                                  |
| Endpoint Profile     |                                  |
| Authorization Result |                                  |

| Authentication Details        |                                  |
|-------------------------------|----------------------------------|
| Source Timestamp              | 2021-11-28 15:36:03.59           |
| Received Timestamp            | 2021-11-28 15:36:03.59           |
| Policy Server                 | ise02                            |
| Event                         | 5231 Guest Authentication Passed |
| Username                      | nadia                            |
| User Type                     | NON_GUEST                        |
| Authentication Identity Store | Duo_SSO                          |
| Identity Group                | Any                              |
| Authentication Method         | PAP_ASCII                        |
| Authentication Protocol       | PAP_ASCII                        |

| Other Attributes |                         |
|------------------|-------------------------|
| ConfigVersionId  | 79                      |
| IpAddress        | 10.65.48.163            |
| PortalName       | ISE Portal (default)    |
| PsnHostName      | ise02.xerotrustlabs.com |
| GuestUserName    | nadia                   |

- ISE의 관리 로그인 로그: 사용자 이름: samUser.

- Export Summary
- My Reports
- Reports
- Audit
  - Adaptive Network Control
  - Administrator Logins
  - Change Configuration Audit
  - Cisco Support Diagnostics
  - Data Purging Audit
  - Endpoint Purge Activities
  - Internal Administrator Sum...
  - Policy OpenAPI Operations
  - Operations Audit
  - psGrid Administrator Audit
  - Secure Communications A...
  - TrustSec Audit
  - User Change Password Au...
- Device Administration
- Diagnostics
- Endpoints and Users
- Guest
- Threat Control NAC
- TrustSec
- Scheduled Reports

### Administrator Logins

From 2021-11-28 00:00:00 To 2021-11-28 18:38:10

Reports reported in last 7 days

Add to My Reports Export To Schedule

| Logged At               | Administrator | IP Address   | Server | Event                                  | Event Details                           |
|-------------------------|---------------|--------------|--------|--|---|
| Today                   | Administrator |              | Server |  |   |
| 2021-11-28 18:38:08.199 |               | 10.65.48.163 | 16402  | Administrator authentication succeeded | Administrator authentication successful |

Rows/Page 1 1 Total Rows

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.