

PingFederate SAML SSO로 ISE 2.1 게스트 포털 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[플로우 개요](#)

[이 활용 사례의 예상 플로우](#)

[구성](#)

[1단계. 외부 SAML ID 공급자를 사용하도록 ISE 준비](#)

[2단계. 외부 ID 제공자를 사용하도록 게스트 포털 구성](#)

[3단계. PingFederate가 ISE 게스트 포털의 ID 제공자 역할을 하도록 구성](#)

[4단계. IdP 메타데이터를 ISE 외부 SAML IdP 공급자 프로필로 가져오기](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 게스트 포털 SAML(Security Assertion Markup Language)에 대해 Cisco ISE(Identity Services Engine) 버전 2.1 SSO(Single Sign On) 기능을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Identity Services Engine 게스트 서비스.
- SAML SSO에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 버전 2.1
- Ping Identity에서 PingFederate 8.1.3.0 서버를 SAML IdP(Identity Provider)로 사용

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.

플로우 개요

SAML은 보안 도메인 간에 인증 및 권한 부여 데이터를 교환하기 위한 XML 기반 표준입니다.

SAML 사양은 보안 주체(게스트 사용자), IDP(IDP)(IPing Federate 서버) 및 SP(서비스 공급자)(ISE)의 세 가지 역할을 정의합니다.

일반적인 SAML SSO 흐름에서 SP는 IdP에서 ID 어설션을 요청하고 가져옵니다. 이 결과에 따라 IdP에 ISE가 사용할 수 있는 구성 가능한 특성(즉, AD 객체와 연결된 그룹 및 이메일 주소)이 포함될 수 있으므로 ISE는 정책 결정을 수행할 수 있습니다.

이 활용 사례의 예상 플로우

1. WLC(Wireless LAN Controller) 또는 액세스 스위치는 일반적인 CWA(Central Web Authentication) 흐름에 맞게 구성됩니다.

팁: 기사 하단의 Related Information(관련 정보) 섹션에서 CWA 플로우의 컨피그레이션 예를 확인하십시오.

2. 클라이언트가 연결되고 세션이 ISE에 대해 인증됩니다. NAD(Network Access Device)는 ISE가 반환하는 AVP(redirect attributes value pair)를 적용합니다(url-redirect-acl 및 url-redirect).

3. 클라이언트가 브라우저를 열고 HTTP 또는 HTTPS 트래픽을 생성하며 ISE의 게스트 포털로 리디렉션됩니다.

4. 포털에서 클라이언트는 이전에 할당된 게스트 자격 증명을 입력할 수 있습니다(스폰서 생성). 새 게스트 계정을 셀프 프로비저닝하거나 AD 자격 증명을 사용하여 로그인합니다(직원 로그인). 그러면 SAML을 통해 Single Sign On 기능이 제공됩니다.

5. 사용자가 "Employee Login(직원 로그인)" 옵션을 선택하면 ISE는 IdP에 대해 이 클라이언트의 브라우저 세션에 연결된 활성 어설션이 있는지 확인합니다. 활성 세션이 없는 경우 IdP에서 사용자 로그인을 적용합니다. 이 단계에서 사용자에게 IdP 포털에 AD 자격 증명을 직접 입력하라는 프롬프트가 표시됩니다.

6. IdP는 LDAP를 통해 사용자를 인증하며 구성 가능한 시간 동안 활성 상태를 유지하는 새 Assertion을 생성합니다.

참고: Ping 페더레이트는 기본적으로 세션 시간 초과를 60분(초기 인증 후 60분 내에 ISE의 SSO 로그인 요청이 없는 경우 세션이 삭제됨) 및 세션 최대 시간 초과를 480분(IdP가 ISE로부터 이 사용자에게 대한 지속적인 SSO 로그인 요청을 받은 경우에도 세션이 8시간 내에 만료됨)으로 적용합니다.

Assertion 세션이 여전히 활성 상태인 경우 직원은 게스트 포털을 사용할 때 SSO를 경험하게 됩니다. 세션이 시간 초과되면 IdP에 의해 새 사용자 인증이 시행됩니다.

구성

이 섹션에서는 ISE를 Ping 페더레이트와 통합하는 컨피그레이션 단계 및 게스트 포털에 대해 브라우저 SSO를 활성화하는 방법에 대해 설명합니다.

참고: 게스트 사용자를 인증할 때 다양한 옵션과 가능성이 있지만 이 문서에서는 모든 조합에 대해 설명하지는 않습니다. 그러나 이 예에서는 구현하려는 정확한 컨피그레이션으로 예를 수정하는 방법을 이해하는 데 필요한 정보를 제공합니다.

1단계. 외부 SAML ID 공급자를 사용하도록 ISE 준비

1. Cisco ISE에서 Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > SAML Id Providers(SAML ID 공급자)를 선택합니다.
2. Add(추가)를 클릭합니다.
3. 일반 탭에서 ID 공급자 이름을 입력합니다. 저장을 클릭합니다. 이 섹션의 나머지 컨피그레이션은 이후 단계에서 IdP에서 가져와야 하는 메타데이터에 따라 달라집니다.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration > Identity Management > External Identity Sources > SAML Id Providers. The left sidebar shows a tree view of External Identity Sources, with 'SAML Id Providers' selected. The main content area is titled 'SAML Identity Provider' and shows the configuration for a provider named 'PingFederate'. The 'General' tab is active, showing the 'Id Provider Name' as 'PingFederate' and the 'Description' as 'SAML SSO IdP'.

2단계. 외부 ID 공급자를 사용하도록 게스트 포털 구성

1. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Configure(구성) > Guest Portals(게스트 포털)를 선택합니다.
2. 새 포털을 만들고 Self-Registered Guest Portal(셀프 등록 게스트 포털)을 선택합니다.

참고: 이 포털은 사용자가 경험하는 기본 포털이 아니라 세션 상태를 확인하기 위해 IdP와 상호 작용하는 하위 포털입니다. 이 포털을 SSOSubPortal이라고 합니다.

3. Portal Settings(포털 설정)를 확장하고 PingFederate for Authentication Method(인증 방법에 대해 PingFederate)를 선택합니다.

4. ID 소스 순서에서 이전에 정의된 외부 SAML IdP(PingFederate)를 선택합니다.

Portals Settings and Customization

Portal Name: * Description: [Portal test URL](#)

Authentication ⓘ
 method: * *Configure authentication methods at:*

5. Acceptable Use Policy(AUP)(사용 제한 정책(AUP) 및 Post-Login Banner Page Settings(로그인 후 배너 페이지 설정) 섹션을 확장하고 둘 다 비활성화합니다.

포털 흐름:



6. 변경사항을 저장합니다.

7. 게스트 포털로 돌아가 **셀프 등록 게스트 포털 옵션**으로 새 포털을 만듭니다.

참고: 이 포털은 클라이언트에 표시되는 기본 포털입니다. 기본 포털에서는 SSOSubportal을 ISE와 IdP 간의 인터페이스로 사용합니다. 이 포털을 PrimaryPortal이라고 합니다.

Portal Name: *	Description:
PrimaryPortal	Portal visible to the client during CWA flow.

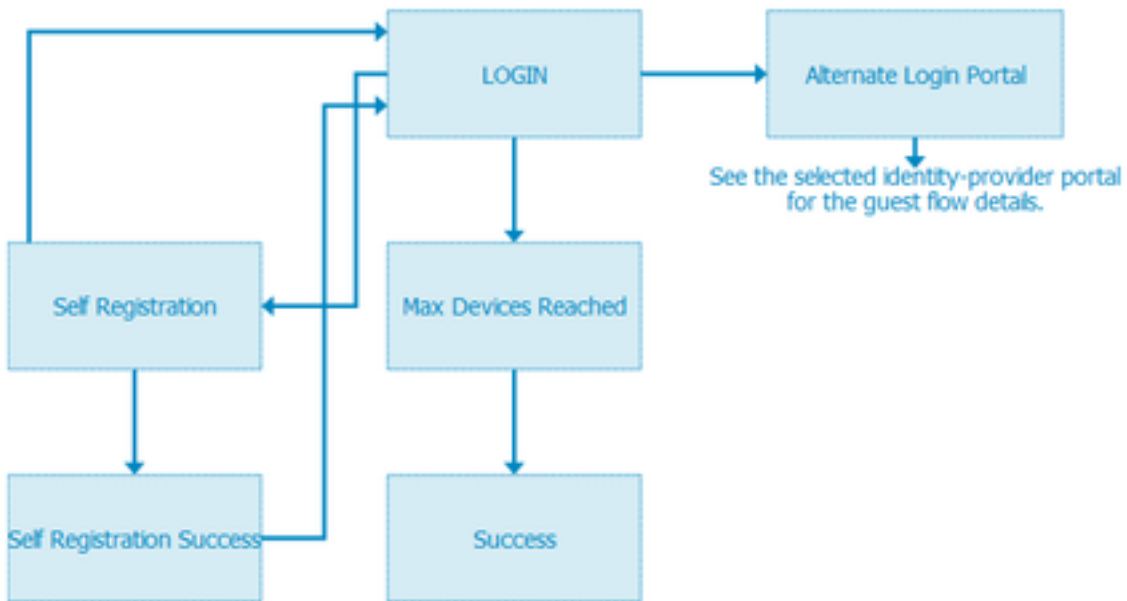
8. Login Page Settings(로그인 페이지 설정)를 확장하고 "Allow the following identity-provider guest portal to be used for login(다음 ID 제공자 게스트 포털을 로그인에 사용하도록 허용)"에서 이전에 생성한 SSOSubPortal을 선택합니다.

Allow the following identity-provider guest portal to be used for login ⓘ

9. Acceptable Use Policy AUP(사용 제한 정책 AUP) 및 Post-login Banner Page Settings(로그인 후 배너 페이지 설정)를 확장하고 선택을 취소합니다.

이때 포털 흐름은 다음과 같아야 합니다.

Guest Flow (Based on settings)



10. Portal Customization(포털 사용자 지정) > Pages(페이지) > Login(로그인)을 선택합니다. 이제 대체 로그인 옵션(아이콘, 텍스트 등)을 사용자 정의할 수 있는 옵션이 있어야 합니다.


Alternative login: (static text)

Alternative login access portal:

Use this text:

as link

as icon tooltip



참고: 오른쪽의 포털 미리 보기 아래에 추가 로그인 옵션이 표시됩니다.

You can also login with



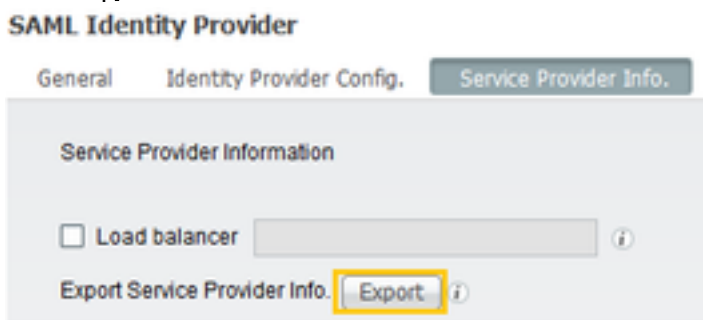
11. 저장을 클릭합니다.

이제 두 포털 모두 게스트 포털 목록 아래에 나타납니다.

PrimaryPortal Portal visible to the client during CWA flow. Used in 1 rules in the Authorization policy	Allow login using : SSOSubPortal
SSOSubPortal SubPortal that will connect to the SAML IdP Used by another portal for alternate login	Used as alternate login option by : PrimaryPortal

3단계. PingFederate가 ISE 게스트 포털의 ID 제공자 역할을 하도록 구성

1. ISE에서 Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > SAML Id Providers(SAML ID 제공자) > PingFederate를 선택하고 Service Provider Info(서비스 제공자 정보)를 클릭합니다.
2. Export Service Provider Info(서비스 공급자 정보 내보내기)에서 Export(내보내기)를 클릭합니다.



3. 생성된 zip 파일을 저장하고 압축 해제합니다. 여기에 포함된 XML 파일은 이후 단계에서 PingFederate에서 프로필을 만드는 데 사용됩니다.



참고: 이 문서에서는 이 시점부터 PingFederate 컨피그레이션을 다룹니다. 이 컨피그레이션은 스폰서 포털, MyDevices 및 BYOD 포털과 같은 여러 솔루션에서 동일합니다. (이러한 솔루션은 이 문서에서 다루지 않습니다.)

4. PingFederate 관리 포털(일반적으로 <https://ip:9999/pingfederate/app>)을 엽니다.
5. IdP Configuration(IdP 컨피그레이션) 탭 > SP Connections(SP 연결) 섹션에서 Create New(새로 만들기)를 선택합니다.

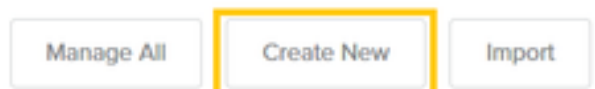
IdP Configuration

APPLICATION INTEGRATION

Adapters
 Default URL
 Application Endpoints

AUTHENTICATION POLICIES

SP CONNECTIONS



6. Connection Type(연결 유형)에서 Next(다음)를 클릭합니다.

SP Connection

Connection Type	Connection Options	Import Metadata
-----------------	--------------------	-----------------

Select the type of connection needed for this SP: Browser users/groups to an SP) or all.

CONNECTION TEMPLATE	No Template
<input checked="" type="checkbox"/> BROWSER SSO PROFILES	PROTOCOL SAML 2.0

7. [연결 옵션]에서 [다음]을 클릭합니다.

SP Connection

Connection Type	Connection Options
-----------------	--------------------

Please select options that apply to this connection.

<input checked="" type="checkbox"/> BROWSER SSO
<input type="checkbox"/> IDP DISCOVERY
<input type="checkbox"/> ATTRIBUTE QUERY

8. Import Metadata(메타데이터 가져오기)에서 File(파일) 라디오 버튼을 클릭하고 Choose file(파일 선택)을 클릭한 다음 ISE에서 이전에 내보낸 XML 파일을 선택합니다.

SP Connection

Connection Type	Connection Options	Import Metadata
-----------------	--------------------	-----------------

To populate many connection settings automatically, you can upload the metadata file. If you have the URL, select Enable Automatic Reloading.

METADATA	<input type="radio"/> NONE	<input checked="" type="radio"/> FILE
No file selected	<input type="button" value="Choose file"/>	

9. 메타데이터 요약 아래에서 다음 을 클릭합니다.

10. General Info(일반 정보) 페이지의 Connection Name(연결 이름)에 이름(예: ISEGuestWebAuth)을 입력하고 Next(다음)를 클릭합니다.

PARTNER'S ENTITY ID
(CONNECTION ID)

CONNECTION NAME

11. Browser SSO(브라우저 SSO)에서 **Configure Browser SSO(브라우저 SSO 구성)**를 클릭하고 **SAML Profiles(SAML 프로파일)**에서 옵션을 선택하고 **Next(다음)**를 클릭합니다.

SP Connection | Browser SSO

SAML Profiles | Assertion Lifetime | Assertion Creation | Protocol Settings | Summary

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the m information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
<input type="checkbox"/> IDP-INITIATED SSO	<input checked="" type="checkbox"/> IDP-INITIATED SLO
<input checked="" type="checkbox"/> SP-INITIATED SSO	<input checked="" type="checkbox"/> SP-INITIATED SLO

12. Assertion 수명에서 **Next(다음)**를 클릭합니다.

13. Assertion Creation(어설션 생성)에서 **Configure Assertion Creation(어설션 생성 구성)**을 클릭합니다.

14. Identity Mapping(ID 매핑)에서 **Standard(표준)**를 선택하고 **Next(다음)**를 클릭합니다.

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping

Identity mapping is the process in which users authenticated by the IdP are associated with local users. This process may affect the way that the SP will look up and associate the user to a specific local account.

STANDARD: Send the SP a known attribute value as the name identifier. The

15. 속성 계약 > 계약 확장에서 속성 **메일** 및 **memberOf**를 입력하고 **추가**를 클릭합니다. **Next(다음)**를 클릭합니다.

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Attribute Contract	Subject Name Format	
SAML_SUBJECT	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>	
Extend the Contract	Attribute Name Format	Action
mail	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
memberOf	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete

이 옵션의 컨피그레이션을 통해 ID 제공자는 Active Directory에서 제공한 MemberOf 및 이메일 특성을 ISE에 전달할 수 있습니다. ISE는 나중에 정책 결정 과정에서 조건으로 사용할 수 있습니다.

16. Authentication Source Mapping(인증 소스 매핑)에서 Map New Adapter Instance(새 어댑터 인스턴스 매핑)를 클릭합니다.

17. Adapter Instance(어댑터 인스턴스)에서 HTML Form Adapter(HTML 양식 어댑터)를 선택합니다. Next(다음)를 클릭합니다.

SP Connection | Browser SSO | Assertion Creation

Adapter Instance | Mapping Method | Attribute Contract Full

Select an IdP adapter instance that may be used to authenticate users for partner.

ADAPTER INSTANCE: HTML Form Adapter

Adapter Contract

- givenName
- mail
- memberOf
- objectGUID
- sn
- username
- userPrincipalName

OVERRIDE INSTANCE SETTINGS

18. 맵핑 방법에서 두 번째 옵션을 아래로 선택하고 다음을 누릅니다.

RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING

RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE -- INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING

USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

19. 속성 소스 및 사용자 조회에서 속성 소스 추가 상자를 클릭합니다.

20. Data Store(데이터 저장소) 아래에 설명을 입력하고 Active Data Store(활성 데이터 저장소)에서 LDAP 연결 인스턴스를 선택하고 디렉토리 서비스의 유형을 정의합니다. 구성된 데이터 저장소가 없는 경우 새 인스턴스를 추가하려면 데이터 저장소 관리를 클릭합니다.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Data Store	LDAP Directory Search	LDAP Filter	Attribute Contract Fulfillment	Summary
------------	-----------------------	-------------	--------------------------------	---------

This server uses local data stores to retrieve supplemental attributes to be sent in an assertion. Specify an Attribute Source

ATTRIBUTE SOURCE DESCRIPTION	[Redacted]et
ACTIVE DATA STORE	[Redacted]et
DATA STORE TYPE	LDAP

[Manage Data Stores](#)

21. LDAP Directory Search(LDAP 디렉토리 검색)에서 도메인에서 LDAP 사용자 조회를 위한 기본 DN을 정의하고 Next(다음)를 클릭합니다.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Data Store	LDAP Directory Search	LDAP Filter	Attribute Contract Fulfillment	Summary
------------	-----------------------	-------------	--------------------------------	---------

Please configure your directory search. This information, along with the attributes supplied in the contract, will be used

BASE DN	CN=Users,DC=[Redacted],DC=net
SEARCH SCOPE	Subtree

참고: 이 기능은 LDAP 사용자 조회 중에 기본 DN을 정의하므로 중요합니다. 기본 DN이 잘못 정의되면 LDAP 스키마에서 Object Not Found가 발생합니다.

22.LDAP 필터에서 sAMAccountName=\${username} 문자열을 추가하고 Next를 클릭합니다.

SP Connection | Browser SSO | Assertior

Data Store | **LDAP Directory Search** | LDAP Filter

Please enter a Filter for extracting data from your directory.

FILTER

23. 속성 계약 이행 아래에서 지정된 옵션을 선택하고 다음을 누릅니다.

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping | Attribute

Data Store | LDAP Directory Search | LDAP Filter | **Attribute Contract Fulfillment** | Summary

Fulfill your Attribute Contract with values from the authentication adapter, dynamic text values, or from a data store lookup.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	username
mail	Adapter	mail
memberOf	Adapter	memberOf

24. 요약 섹션에서 구성을 확인하고 완료를 클릭합니다.

25. 특성 소스 및 사용자 조회로 돌아가 다음을 클릭합니다는 방법.

26. Failsafe Attribute Source(장애 안전 특성 소스)에서 Next(다음)를 클릭합니다.

27. 속성 계약 이행 아래에서 이러한 옵션을 선택하고 다음을 누릅니다.

Attribute Contract	Source	Value
SAML_SUBJECT	Adapter	username
mail	Text	no email address
memberOf	Text	no group found

28. 요약 섹션에서 구성을 확인하고 완료를 클릭합니다.

29. 인증 소스 매핑으로 돌아가려면 다음 을 클릭합니다.

30. 요약 페이지에서 구성을 확인한 후 완료를 클릭합니다.

31. Assertion Creation(어설션 생성)으로 돌아간 후 **Next(다음)**를 클릭합니다.

32. Protocol Settings(**프로토콜 설정**)에서 **Configure Protocol Settings(프로토콜 설정 구성)**를 클릭합니다. 이 시점에서 이미 입력된 항목이 두 개여야 합니다. **Next(다음)**를 클릭합니다.

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL	Allowable SAML Bindings	Signature Policy	Encryption Policy	Summary
--------------------------------	-------------------------	------------------	-------------------	---------

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possibl

Default	Index	Binding	Endpoint URL
default	0	POST	https://14.36.157.210:8443/portal/SSOLoginResponse.action
	1	POST	https://orise21a.rtpaaa.net:8443/portal/SSOLoginResponse.action

33. SLO Service URLs(SLO 서비스 URL)에서 **Next(다음)**를 클릭합니다.

34. 허용되는 SAML 바인딩에서 ARTIFACT 및 SOAP 옵션의 선택을 취소하고 다음을 누릅니다.

Assertion Consumer Service URL	SLO Service URLs	Allowable SAML Bindings
--------------------------------	------------------	-------------------------

When the SP sends messages, what SAML bindings do you want to allow?

<input type="checkbox"/>	ARTIFACT
<input checked="" type="checkbox"/>	POST
<input checked="" type="checkbox"/>	REDIRECT
<input type="checkbox"/>	SOAP

35. Signature Policy(서명 정책)에서 **Next(다음)**를 클릭합니다.

36. Encryption Policy(암호화 정책)에서 **Next(다음)**를 클릭합니다.

37. 요약 페이지에서 구성을 검토하고 완료를 누릅니다.

38. Browser SSO(브라우저 SSO) > Protocol settings(프로토콜 설정)로 돌아가서 **Next(다음)**를 클릭하고 컨피그레이션을 검증한 후 **Done(완료)**을 클릭합니다.

39. 브라우저 SSO 탭이 나타납니다. **Next(다음)**를 클릭합니다.

SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials
-----------------	--------------------	--------------	--------------	-------------	-------------

This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources a configuration.

BROWSER SSO CONFIGURATION

Configure Browser SSO

40. **Credentials(자격 증명)**에서 **Configure Credentials(자격 증명 구성)**를 클릭하고 IdP와 ISE 통신 중에 사용할 서명 인증서를 선택하고 **Include the certificate in the signature(서명에 인증서 포함) 옵션을 선택합니다.** 그런 다음 **Next(다음)**를 클릭합니다.

SP Connection | Credentials

Digital Signature Settings	Signature Verification Settings	Summary
----------------------------	---------------------------------	---------

You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/c

SIGNING CERTIFICATE

INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.

SIGNING ALGORITHM

참고: 구성된 인증서가 없으면 **Manage Certificates(인증서 관리)**를 클릭하고 프롬프트에 따라 IdP를 ISE 통신에 서명하는 데 사용할 자체 서명 인증서를 생성합니다.

41. 요약 페이지에서 구성을 검증하고 완료를 클릭합니다.

42. **자격 증명** 탭으로 돌아가 다음을 클릭합니다는 것입니다.

43. **Activation & Summary(활성화 및 요약)**에서 **Connection Status ACTIVE(연결 상태 활성)**를 선택하고 나머지 컨피그레이션을 검증한 후 **Done(완료)**을 클릭합니다.

SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials	Activation & Summary
-----------------	--------------------	--------------	--------------	-------------	-------------	----------------------

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status ACTIVE INACTIVE

4단계. IdP 메타데이터를 ISE 외부 SAML IdP 공급자 프로필로 가져오기

1. PingFederate 관리 콘솔에서 **Server Configuration > Administrative Functions > Metadata Export**를 선택합니다. 서버가 여러 역할 (IdP 및 SP)에 대해 구성된 경우 **I am the Identity Provider(IdP) 옵션**을 선택합니다. **Next(다음)**를 클릭합니다.
2. 메타데이터 모드에서 **"메타데이터에 수동으로 포함할 정보 선택"**을 선택합니다. **Next(다음)**를 클릭합니다.

USE A CONNECTION FOR METADATA GENERATION

SELECT INFORMATION TO INCLUDE IN METADATA MANUALLY

USE THE SECONDARY PORT FOR SOAP CHANNEL

3. **프로토콜** 아래에서 다음을 클릭합니다.

4. **속성 계약**에서 다음을 클릭합니다.

5. **Signing Key(서명 키)** 아래에서 연결 프로파일에 이전에 구성된 인증서를 선택합니다. **Next(다음)**를 클릭합니다.

Export Metadata

Metadata Role	Metadata Mode	Protocol	Attribute Contract	Signing Key
---------------	---------------	----------	--------------------	-------------

The metadata may contain a public key that this system uses for digital signatures. If you wish to include

DIGITAL SIGNATURE KEYS/CERTS

01:55:31:36:ED:D8 (cn=████████.147.1) ▼

6. **Metadata Signing(메타데이터 서명)** 아래에서 서명 인증서를 선택하고 **Include this certificate's public key in the key info element(이 인증서의 공개 키를 key info 요소에 포함)**를 선택합니다. **Next(다음)**를 클릭합니다.

SIGNING CERTIFICATE ▼

INCLUDE THIS CERTIFICATE'S PUBLIC KEY CERTIFICATE IN THE <KEYINFO> ELEMENT.

SIGNING ALGORITHM ▼

7. **XML 암호화 인증서**에서 **Next(다음)**를 클릭합니다.

참고: 여기서 암호화를 적용하는 옵션은 네트워크 어드민에게 있습니다.

8. 요약 섹션에서 내보내기를 클릭합니다. 생성된 메타데이터 파일을 저장한 다음 완료를 누릅니다.

Export Metadata

Metadata Role	Metadata Mode	Protocol	Attribute Contract	Signing Key	Metadata Signing	XML Encryption Certificate	Export & Summary
Click the Export button to export this metadata to the file system.							
Export Metadata							
Metadata Role							
Metadata role	Identity Provider						
Metadata Mode							
Metadata mode	Select information manually						
Use the secondary port for SOAP channel	false						
Protocol							
Protocol	SAML 2.0						
Attribute Contract							
Attribute	None defined						
Signing Key							
Signing Key	CN=14.36.1471, OU=TAC, O=Cisco, L=RTP, C=US						
Metadata Signing							
Signing Certificate	CN=14.36.1471, OU=TAC, O=Cisco, L=RTP, C=US						
Include Certificate in KeyInfo	false						
Include Raw Key in KeyValue	false						
Selected Signing Algorithm	RSA SHA256						
XML Encryption Certificate							
Encryption Keys/Certs	NONE						
<input type="button" value="Export"/>							
<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input type="button" value="Done"/>							

9. ISE에서 Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > SAML Id Providers(SAML ID 제공자) > PingFederate를 선택합니다.

10. Identity Provider Config(ID 제공자 컨피그레이션) > Browse(찾아보기)를 클릭하고 PingFederate 메타데이터 내보내기 작업에서 저장된 메타데이터를 가져옵니다.

SAML Identity Provider

General

Identity Provider Config.

Service Provider I

Identity Provider Configuration

Import Identity Provider Config File

Browse...



Provider Id PingFederate

Single Sign On URL https://[redacted].147.1:9031

Single Sign Out URL (Post) https://[redacted].147.1:9031

Signing Certificates

Subject

CN=[redacted].147.1, OU=[redacted], O=Cisco, L=RTP, C=US

11. [그룹] 탭의 [그룹 구성원 속성] 아래에서 [구성원 추가]를 선택한 다음 [추가]를 클릭합니다

Assertion의 Name(이름) 아래에 memberOf 특성이 LDAP 인증에서 검색될 때 IdP가 반환해야 하는 Distinguished Name을 추가합니다. 이 경우 구성된 그룹은 TOR의 스폰서 그룹에 연결되며 이 그룹에 대한 DN은 다음과 같습니다.

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attributes

Advanced Settings

Groups

Group Membership Attribute

memberOf



+ Add / Edit / X Delete

Name in Assertion

Name in ISE

CN=TOR,DC=[redacted],DC=net

TOR

Save | Cancel

DN과 "Name in ISE(ISE의 이름)" 설명을 추가하고 나면 OK(확인)를 클릭합니다.

12. 속성 탭을 선택하고 추가를 누릅니다.

이 단계에서는 LDAP를 통한 Ping 쿼리를 기반으로 IdP에서 전달된 SAML 토큰에 포함된 "mail" 특성을 추가합니다. 이 특성에는 해당 객체에 대한 email 특성이 포함되어야 합니다.

참고: 11단계와 12단계에서는 ISE가 IdP 로그인 작업을 통해 AD 객체 Email 및 MemberOf 특성을 수신하는지 확인합니다.

다음을 확인합니다.

1. 포털 테스트 URL을 사용하거나 CWA 플로우를 따라 게스트 포털을 시작합니다. 사용자는 게스트 자격 증명을 입력하고, 자신의 계정을 만들고, 직원 로그인을 수행할 수 있습니다.

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)

You can also login with



2. **사원 로그인을 클릭합니다.** 활성 세션이 없으므로 사용자는 IdP 로그인 포털로 리디렉션됩니다.

Sign On

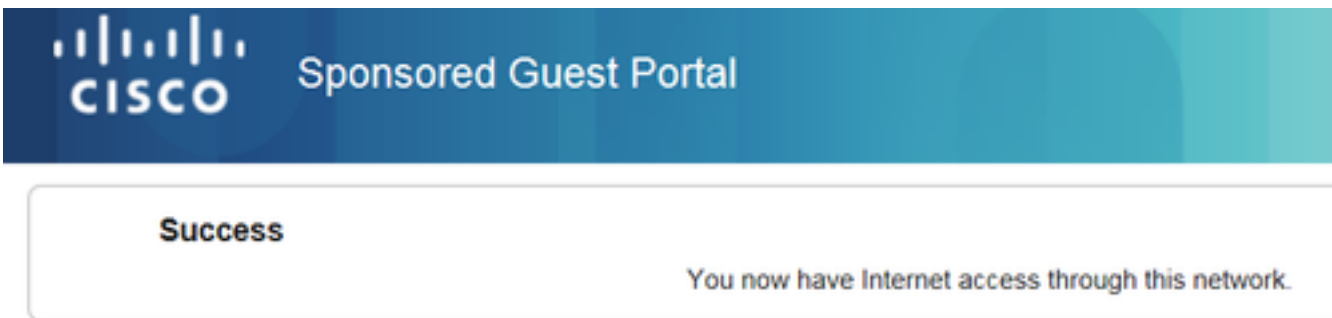
Please sign on and we'll send you right along.

USERNAME

PASSWORD

Sign On

- AD 자격 증명을 입력하고 **Sign On**을 클릭합니다.
- IdP 로그인 화면에서 사용자를 게스트 포털 성공 페이지로 리디렉션합니다.



- 이 시점에서 사용자가 게스트 포털로 돌아와 "**직원 로그인**"을 선택할 때마다 세션이 IdP에서 활성 상태인 한 네트워크에서 허용됩니다.

문제 해결

SAML ise-psc.log . Administration() > Logging() > **Debug log Configuration()** > **Select the node in question()** > **Set SAML component** to debug level(SAML) SAML().

CLI ISE **show logging application ise-psc.log tail SAML . Operations() > Troubleshoot() > Download Logs() > ISE > Debug Logs() > ise-psc.log** .

```
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://10.36.147.1:9031/idp/sso.saml2
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SPProviderId for PingFederate is: http://CiscoISE
/5b4c0780-2da2-11e6-a5e2-005056a15f11
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][
cpm.saml.framework.impl.SAMLFacadeImpl -::::- ResponseValidationContext:
    IdP URI: PingFederate
```

```
SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11
Assertion Consumer URL: https://10.36.157.210:8443/portal/SSOLoginResponse.action
Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8
b99-2ef6b76c1d4b_SEMI_DELIMITER10.36.157.210
Client Address: 10.0.25.62
Load Balancer: null
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::- Determine the signing certificate
2016-06-27 16:15:39,366 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::- Validate signature to SAML standard
with cert:CN=10.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352
2016-06-27 16:15:39,367 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::- Creating XMLSignature object
2016-06-27 16:15:39,367 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::- Validating signature with signature
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating response
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating assertion
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: validation succeeded for guest
IDPResponse
:
    IdP ID: PingFederate
    Subject: guest
    SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
    SAML Success:true
    SAML Status Message:null
    SAML email:guest@example
    SAML Exception:null
2016-06-27 16:15:39,368 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:guest
2016-06-27 16:15:39,375 DEBUG [http-bio-10.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Authenticate SAML User - result:PASSED
```

관련 정보

- [Cisco WLC 및 ISE 컨피그레이션을 통한 중앙 웹 인증 예](#)
- [스위치 및 ISE\(Identity Services Engine\) 컨피그레이션을 사용한 중앙 웹 인증 예.](#)
- [Cisco Identity Services Engine 릴리스 정보, 릴리스 2.1](#)
- [Cisco Identity Services Engine 관리자 가이드, 릴리스 2.1](#)

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.