

# SSO를 활성화하기 위해 PingFederate Identity Provider for Cisco Identity Service 설치 및 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

### [Install](#)

[시스템 요구 사항](#)

[운영 체제](#)

[Java 환경](#)

[최종 사용자를 위해 지원되는 브라우저](#)

[관리 콘솔용으로 지원되는 브라우저](#)

[데이터 저장소 통합](#)

[\(사용자 특성 조회\)](#)

[최소 하드웨어 요구 사항](#)

[최소 하드웨어 권장 사항](#)

### [Install](#)

[배포 ZIP 파일로 PingFederate 설치](#)

[배포 EXE 파일로 PingFederate 설치](#)

[처음으로 PingFederate 시작](#)

### [초기 설정 마법사](#)

[라이선스 계약 동의](#)

[PingOne 계정](#)

[라이선스](#)

[기본 정보](#)

[역할 활성화](#)

[ID 공급자 컨피그레이션](#)

[관리자 계정](#)

[확인](#)

[완료](#)

### [PingFederate 구성](#)

#### [서버 컨피그레이션](#)

[디지털 서명 및 XML\(Extensible Markup Language\) 암호 해독 키 및 인증서](#)

[데이터 저장소](#)

[암호 자격 증명 검증기](#)

[서버 설정](#)

#### [IdP\(Identity Provider\) 컨피그레이션](#)

[어댑터](#)

[SP 접속](#)

### [PingFederate 메타데이터 내보내기](#)

[메타데이터 내보내기](#)

---

[메타데이터 모드](#)

[연결 메타데이터](#)

[메타데이터 서명](#)

[내보내기 및 요약](#)

[샘플 메타데이터](#)

[문제 해결](#)

[SSO에 대한 추가 구성.](#)

---

## 소개

이 문서에서는 SSO(Single Sign On)를 사용하도록 설정하는 PingFederate Id Provider(IdP)의 컨피그레이션에 대해 설명합니다.

Cisco Id 구축 모델

제품	구축
UCCX	공동 거주자
PCCE	CUIC(Cisco Unified Intelligence Center) 및 LD(Live Data)와 공동 상주
UCCE	2k 구축을 위해 CUIC 및 LD와 공동 상주 4k 및 12k 구축을 위한 독립형

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco UCCX(Unified Contact Center Express) 릴리스 11.6 또는 Cisco Unified Contact Center Enterprise 릴리스 11.6 또는 PCCE(Packaged Contact Center Enterprise) 릴리스 11.6이 해당됩니다.
- Windows Server에 설치된 PingFederate

---

참고: 이 문서는 Cisco Id(Identify Service) 및 IdP(Identity Provider)와 관련된 구성을 참조합니다. 이 문서는 스크린샷과 예에서 UCCX를 참조하지만, Cisco Id Service(UCCX/UCCE/PCCE) 및 IdP와 관련된 구성은 유사합니다.

---

## 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

# Install

## 시스템 요구 사항

운영 체제	Java 환경	최종 사용자를 위해 지원되는 브라우저	관리 콘솔용으로 지원되는 브라우저	데이터 저장소 통합 (사용자 특성 조회)	초
<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2008 R2 SP(서비스 팩)</li> <li>• Microsoft Windows Server 2012 표준</li> <li>• Microsoft Windows Server 2012 R2 Datacenter</li> <li>• Oracle Enterprise Linux 6.5(Red Hat 호환 커널)</li> <li>• Oracle Solaris 10</li> <li>• Red Hat Enterprise Linux ES 6.6</li> <li>• Red Hat Enterprise Linux ES 7.0</li> </ul>	<ul style="list-style-type: none"> <li>• Oracle Java SE Runtime Environment(서버 JRE) 7 업데이트 79(64비트)</li> <li>• Oracle Java SE Runtime Environment(서버 JRE) 8 업데이트 45(64비트)</li> </ul>	<ul style="list-style-type: none"> <li>• 크롬</li> <li>• 파이어폭스</li> <li>• Internet Explorer(버전 9 이상)</li> <li>• 사파리</li> </ul>	<ul style="list-style-type: none"> <li>• 크롬</li> <li>• 파이어폭스</li> <li>• Internet Explorer(버전 9 이상)</li> </ul>	<ul style="list-style-type: none"> <li>• Microsoft Active Directory(2008 R2 및 2012)</li> <li>• Oracle Directory Server Enterprise Edition 11g</li> <li>• Microsoft SQL(구조적 쿼리 언어) 서버(2012 및 2014)</li> <li>• Oracle 데이터베이스(10g 및 11g R2)</li> <li>• Oracle MySQL 5.6</li> </ul>	

<ul style="list-style-type: none"> <li>• SUSE Linux Enterprise 11 SP 3</li> </ul>					
---	--	--	--	--	--

## Install

배포 ZIP 파일의 압축을 풀거나 플랫폼별 설치 프로그램을 사용하여 PingFederate를 설치합니다.

- Ping Identity 라이선스 웹 페이지([www.pingidentity.com/support-and-downloads/licensing.cfm](http://www.pingidentity.com/support-and-downloads/licensing.cfm))를 통해 라이선스 키 [요청](#)
- 응용 프로그램을 설치하고 실행할 수 있는 적절한 권한으로 시스템에 로그인했는지 확인합니다
- 서버 JRE(Java Runtime Environment)가 설치되어 있고 환경 및 PATH 변수가 올바르게 설정되어 있는지 확인합니다

### 배포 ZIP 파일로 PingFederate 설치

배포 ZIP 파일을 설치 디렉토리로 추출합니다.

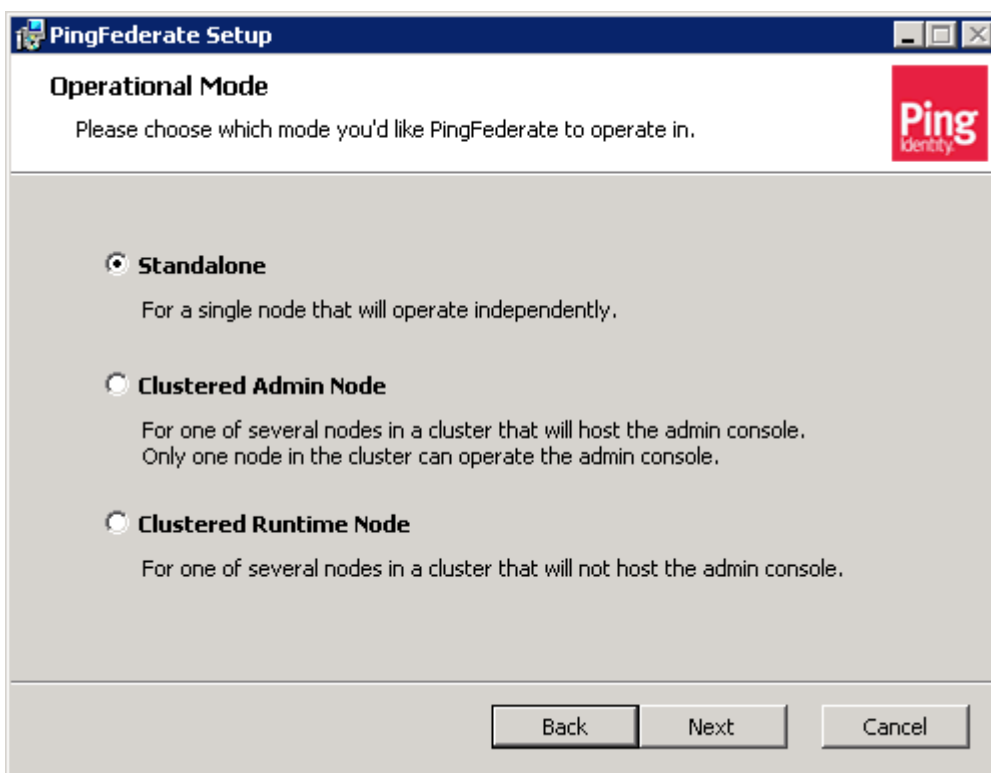
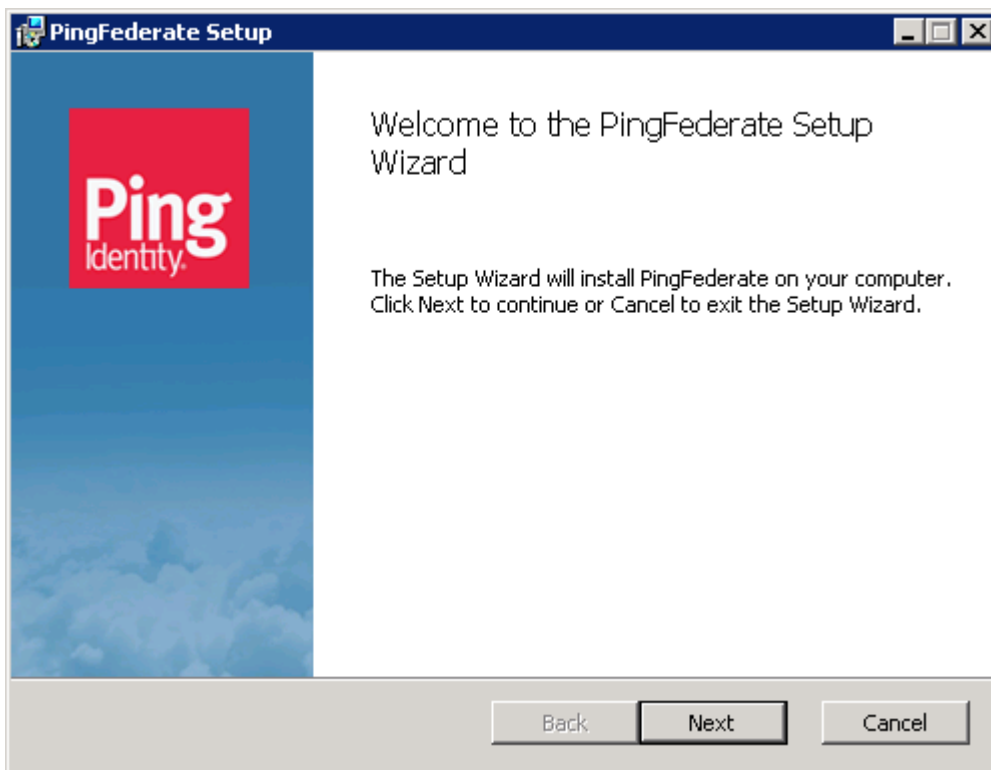
---

경고: 자동화된 업그레이드로 인해 발생할 수 있는 문제를 방지하려면 설치된 pingFederate 폴더의 이름을 변경하지 마십시오. 동일한 시스템에 PingFederate의 여러 인스턴스를 설치하는 경우(예: 특정 서버 클러스터링 시나리오), 각 인스턴스를 다른 위치에 설치하거나 상위 폴더의 이름을 변경하여 동일한 위치에 병렬 파일 구조를 설치합니다.

---

### 배포 EXE 파일로 PingFederate 설치


exe 파일을 두 번 클릭하고 설치 단계를 수행합니다



**PingFederate Setup**

### Administrative console and API

Enter the port for the admin console and API.




**Admin HTTPS port**

This is the port where PingFederate admin console and API will run.

**PingFederate Setup**

### Engine Settings

Enter the ports that PingFederate will use.

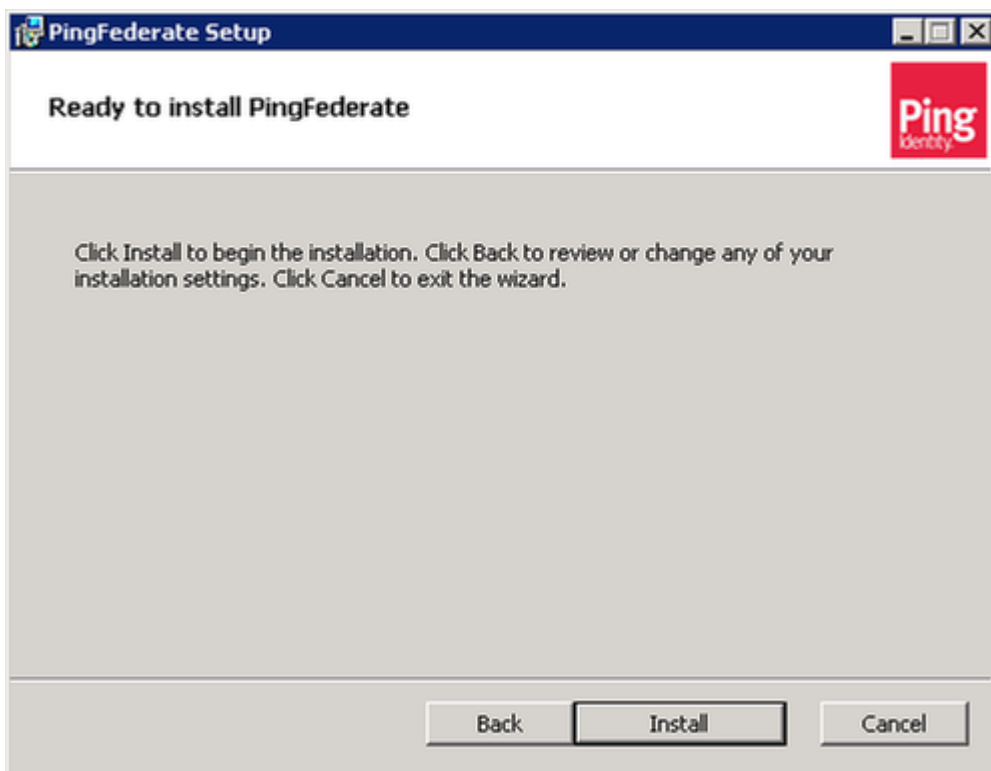
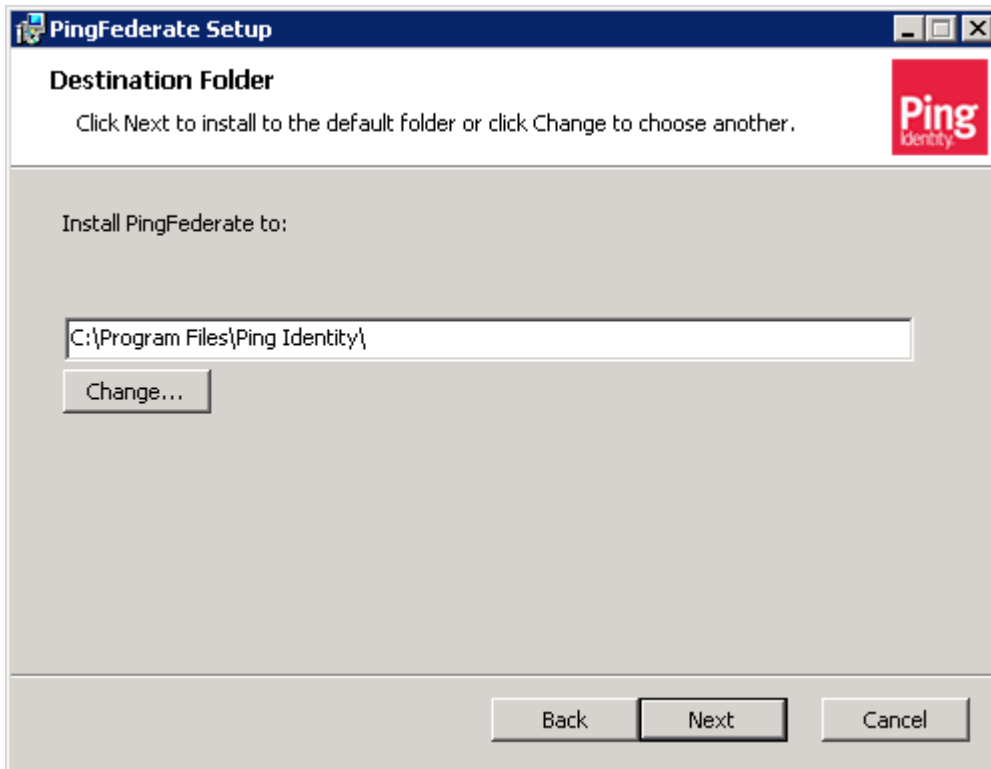


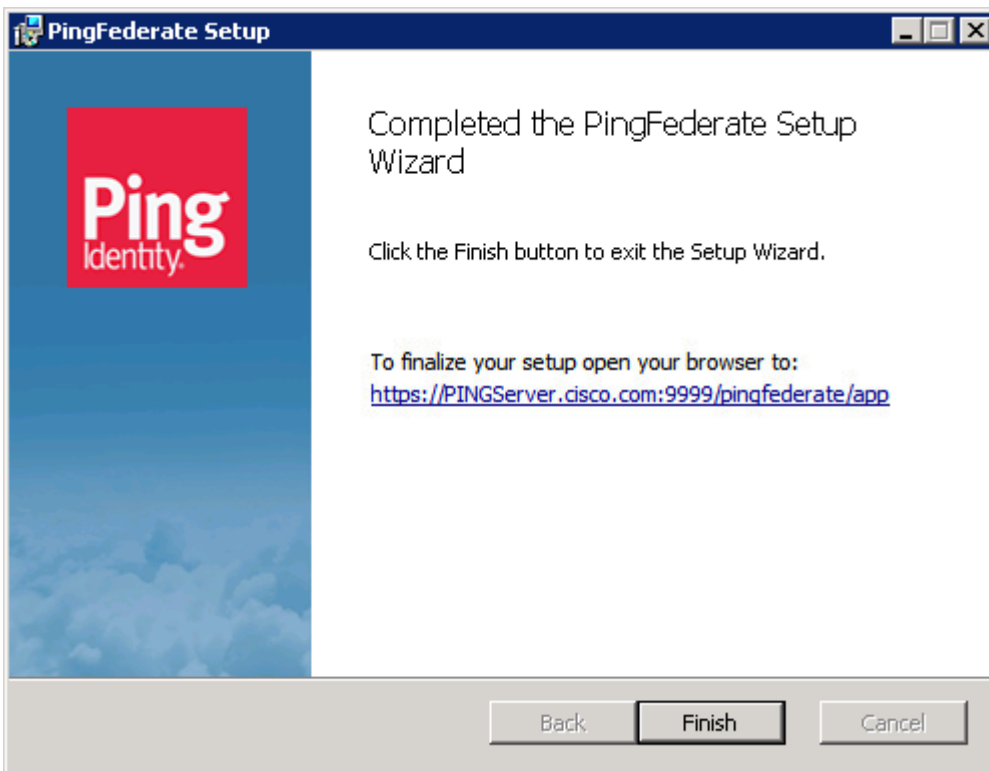
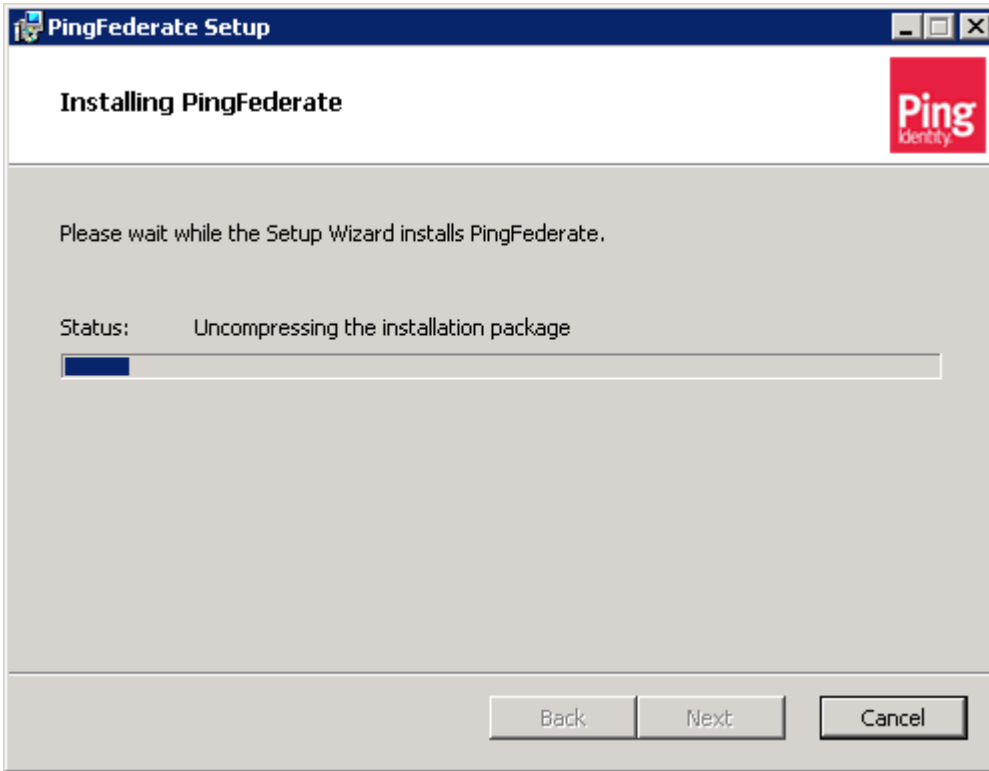
**HTTPS Port**

This is the port where PingFederate will listen for encrypted traffic.

**Secondary HTTPS Port**  Optional

If you need client X.509 certificate based authentication for end users or protocols, enable this port by specifying a value.





## 처음으로 PingFederate 시작

플랫폼별 설치 프로그램 중 하나로 PingFederate를 설치할 경우 PingFederate는 서비스로 실행되도록 구성되어 설치 프로세스가 끝나면 자동으로 시작됩니다.

배포 ZIP 파일로 PingFederate를 설치하는 경우 스크립트를 실행하여 수동으로 PingFederate를 시작합니다.

(Windows) <pf\_install>/pingfederate/bin/run.bat  
(Unix/Linux) <pf\_install>/pingfederate/bin/run.sh

스크립트가 완료될 때까지 대기 - 이 메시지가 시퀀스의 끝 근처에 나타나면 시작 프로세스가 완료됩니다.

PingFederate가 <X>s:<Y>ms에 시작되었습니다.

## 초기 설정 마법사

PingFederate 관리자의 사용자 인터페이스인 관리 콘솔은 마법사와 같은 제어 화면 시스템을 기반으로 합니다. PingFederate 관리 콘솔을 시작하고 초기 설정 마법사를 사용하여 ID 페더레이션 설정의 컨피그레이션을 완료합니다. 또한 PingFederate를 PingOne에 연결하여 강력한 온프레미스 및 클라우드 기반 하이브리드 솔루션을 구축할 수 있습니다.

관리 콘솔에 액세스하려면

브라우저를 시작하고 [---

참고: 포트 번호 9999는 기본적으로 설정됩니다. PingFederate 속성을 통해 변경할 수 있습니다.

---](https://<FQHN>:9999/pingfederate/app(<FQHN>은 PingFederate가 설치된 서버의 정규화된 호스트 이름)으로 이동합니다.</a></p></div><div data-bbox=)

라이선스 계약 동의

**Ping** PingFederate

License Agreement

For more information on commercial licensing or support, contact Ping Sales at [sales@pingidentity.com](mailto:sales@pingidentity.com) or call toll-free 877.898.2905 (+1303.468.2882 outside North America).

SOFTWARE LICENSE AGREEMENT

THIS CLICK-THROUGH AGREEMENT (THIS "AGREEMENT") IS BY AND BETWEEN PING IDENTITY CORPORATION ("PING IDENTITY") AND THE COMPANY OR ENTITY ON WHOSE BEHALF YOU ARE EXECUTING THIS AGREEMENT ("CUSTOMER"). You represent that you have the authority to bind Customer to the terms of this Agreement. By agreeing to the terms of this Agreement or by accessing, using or installing any part of the Products, Customer expressly agrees to and consents to be bound by all of the terms of this Agreement. If Customer does not agree to any of the terms of this Agreement, Customer is prohibited from downloading, installing, activating or using the Products. THE EFFECTIVE DATE OF THIS AGREEMENT IS THE DATE ON WHICH CUSTOMER ACCEPTS THESE TERMS BY CLICKING "ACCEPT" OR THE SIMILARLY LABELED BUTTON INDICATING ASSENT (THE "EFFECTIVE DATE").

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

**1. Definitions.**

"Administrator" is an individual who has been granted administrative permissions by Customer to the Service in order to set-up, modify and suspend the Service, each as applicable.

"Affiliate(s)" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"API" means an application programming interface.

"Customer Data" means all electronic data or information submitted by Customer to the Service. Customer Data also includes any data of an Identity Provider and its associated employees, consultants, contractors and agents transmitted through the Service in order to access Customer's services or applications.

"Documentation" means Ping Identity's then current on-line user's manuals made generally available by Ping Identity and provided to Customer along with the Software.

"Identity Provider" means an entity that desires single sign-on capabilities into a Service Provider's services or applications.

Accept

Copyright © 2003-2018  
Ping Identity Corporation  
All rights reserved.  
Version 10.2.2.0

PingOne 계정

Do you want to connect this identity provider with PingOne to enable cloud-based single sign-on?

### Yes, Connect to PingOne

To connect this PingFederate node to your PingOne account, enter your activation key below.

[Sign on to PingOne to get your activation key.](#)

ACTIVATION KEY

### No, Set Up PingFederate Without PingOne

PingFederate works with or without a PingOne connection. Continue the setup below to use PingFederate on its own.

Next

Next(다음)를 클릭합니다.

라이선스

Please upload a valid PingFederate license file.

License File

No file selected

Choose file

Previous

Next

pingidentity.com에서 개발 라이선스를 구매하거나 요청해야 합니다. 라이선스 파일을 업로드하고 Next(다음)를 클릭합니다.

기본 정보

Welcome to PingFederate. To set up your enterprise identity bridge, let's first confirm your Base URL and Entity ID.

BASE URL

https://pingserver.cisco.com:9031

ENTITY ID

pingserver

Previous Next

Copyright © 2003-2018  
Ping Identity Corporation  
All rights reserved  
Version 11.2.2.0

기본 URL 및 엔티티 ID를 설정하고 다음을 클릭합니다.

### 역할 활성화

Please select the roles you expect PingFederate to play.

ROLES

- IDENTITY PROVIDER
- SERVICE PROVIDER
- OAUTH AUTHORIZATION SERVER

Previous Next

Copyright © 2003-2018  
Ping Identity Corporation  
All rights reserved  
Version 11.2.2.0

ID 공급자를 선택하고 다음을 클릭합니다.

### ID 공급자 컨피그레이션

If you're connecting to Active Directory, start the quick connection process below. You can configure any other user store connections after the PingFederate setup is complete.

### Identity Provider Configuration

[Connect to Active Directory](#)

[Previous](#)

[Next](#)

Active Directory에 대한 연결은 나중에 수행할 수 있습니다. 다음을 클릭합니다.

### 관리자 계정

Please choose a username and password for your primary administrator. You can add other administrators to PingFederate after setup is complete.

USERNAME

PASSWORD

CONFIRM PASSWORD

[Previous](#)

[Next](#)

관리자의 암호를 설정하고 다음을 클릭합니다.

### 확인

Here is a summary of your PingFederate configuration:

BASE URL: https://pingserver.cisco.com:9031  
ENTITY ID: pingserver  
ENABLE ROLE: Identity Provider  
CREATE ACCOUNT: Administrator

Previous Next

확인하고 Next(다음)를 클릭합니다.

완료

Congratulations! You have successfully set up PingFederate.

What's Next?

**IDENTITY PROVIDER**

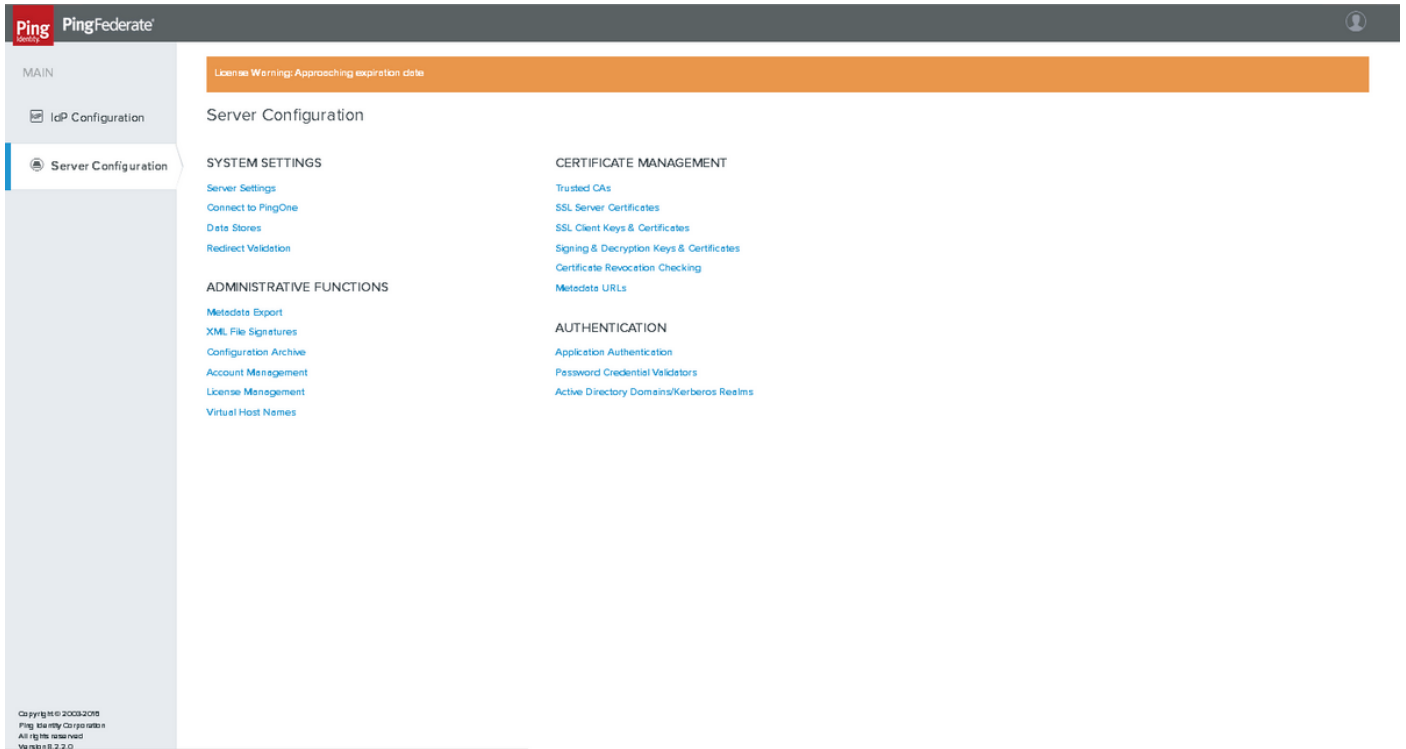
You can begin creating Service Provider connections to your target applications. Choose Create New under SP Connections to get started.

Done

Done(완료)을 클릭합니다

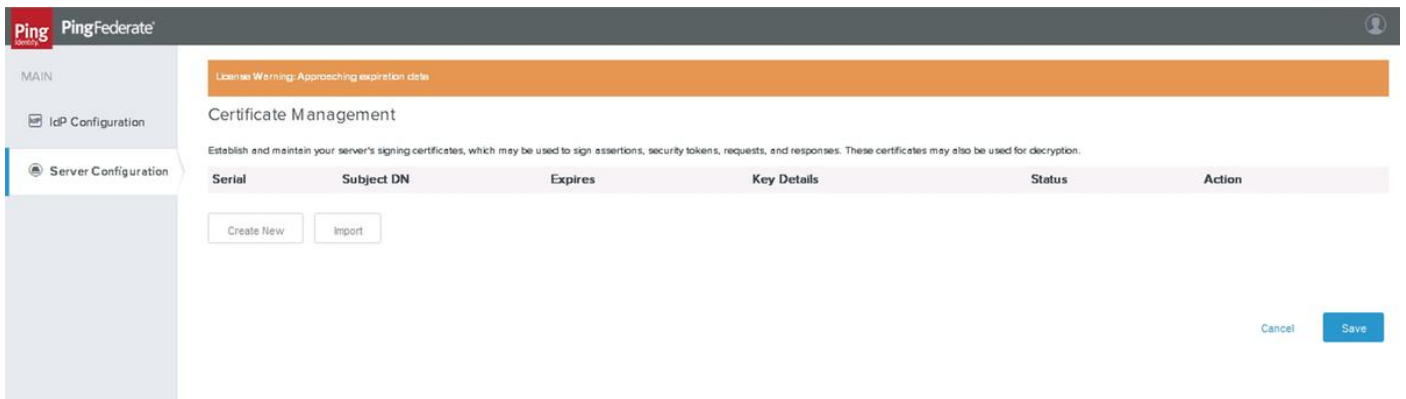
PingFederate 구성

# 서버 컨피그레이션



## 디지털 서명 및 XML(Extensible Markup Language) 암호 해독 키 및 인증서

Server Configuration(서버 컨피그레이션) > Certificate Management(인증서 관리) > Signing & XML Decryption Keys & Certificates(서명 및 XML 암호 해독 키 및 인증서)를 클릭합니다



Create New(새로 만들기)를 클릭합니다.

## 인증서 생성

License Warning: Approaching expiration date

### Certificate Management | Create Certificate

**Create Certificate** Summary

Create a new Certificate and Private Key.

COMMON NAME: SSO

ORGANIZATION: CISCO

ORGANIZATIONAL UNIT: CBABU

CITY: Bangalore

STATE: Karnataka

COUNTRY: IN

VALIDITY (DAYS): 365

KEY ALGORITHM: RSA

KEY SIZE (BITS): 2048

SIGNATURE ALGORITHM: RSA SHA256

Cancel Next

Copyright © 2008-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

Next(다음)를 클릭합니다.

인증서 내보내기

License Warning: Approaching expiration date

### Certificate Management | Export Certificate

**Export Certificate** Export & Summary

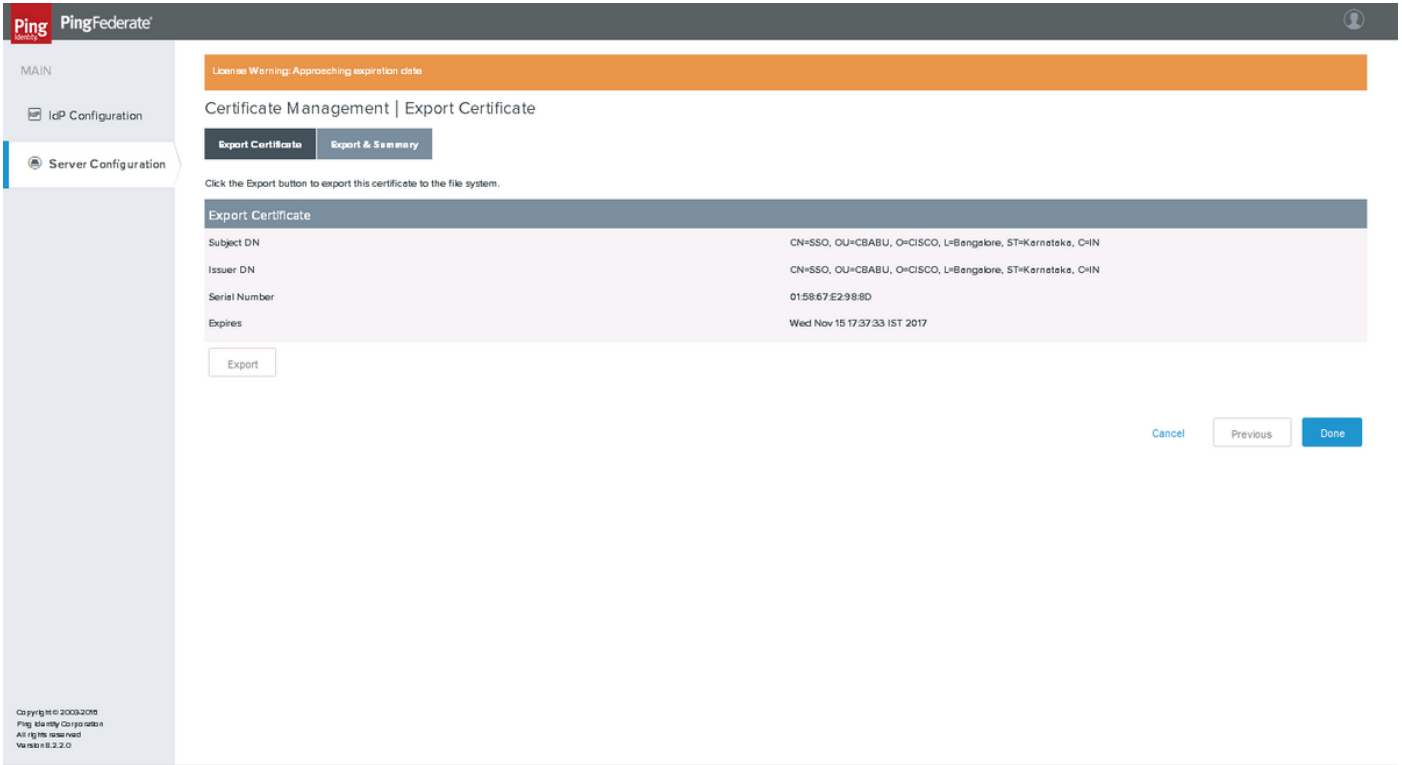
You have a choice of exporting the certificate and the key or just the certificate.

CERTIFICATE ONLY

CERTIFICATE AND PRIVATE KEY

Next

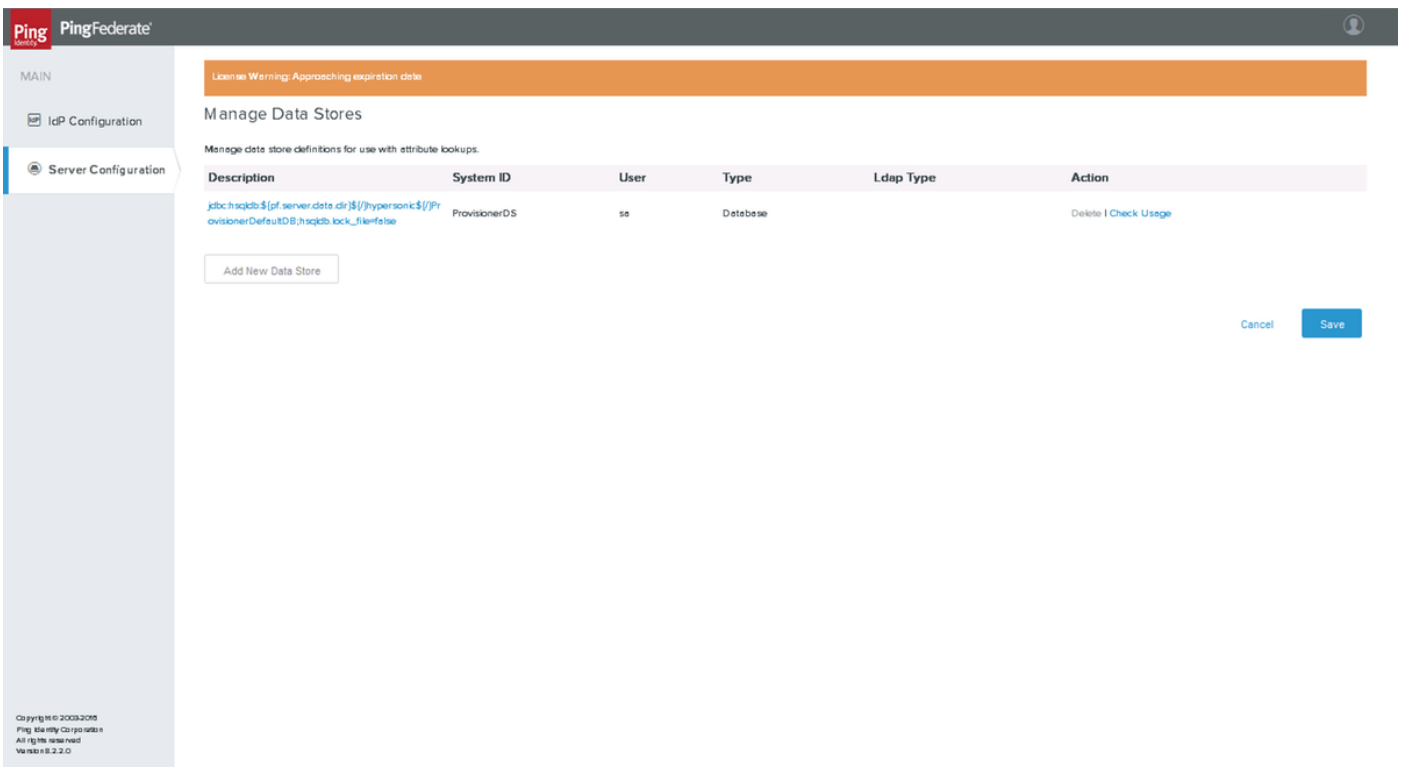
내보내기 및 요약



Export(내보내기)를 클릭합니다

데이터 저장소

Server Configuration(서버 컨피그레이션) > SYSTEM SETTINGS(시스템 설정) > Data Stores(데이터 저장소)를 클릭합니다



새 데이터 저장소 추가를 클릭합니다.

## LDAP 컨피그레이션

Copyright © 2003-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

License Warning: Approaching expiration date

### Manage Data Stores | Data Store

Data Store Type | LDAP Configuration | Summary

Please select a type of data store.

DATABASE

LDAP

CUSTOM

Cancel Next

LDAP를 선택하고 Next(다음)를 클릭합니다.

Copyright © 2003-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

License Warning: Approaching expiration date

### Manage Data Stores | Data Store

Data Store Type | LDAP Configuration | Summary

Please provide the details for configuring this LDAP connection.

HOSTNAME(S) 10.78.93.148:389

LDAP TYPE Active Directory

BIND ANONYMOUSLY

USER DN cn=Administrator,cn=u

PASSWORD .....

USE LDAPS

MASK VALUES IN LOG

Advanced

Cancel Previous Next

값을 입력하고 다음을 클릭합니다.

요약

License Warning: Approaching expiration date

Manage Data Stores | Data Store

Data Store Type | LDAP Configuration | Summary

Click a heading link to edit a configuration setting.

Data Store

**Data Store Type**

Type of Data Store: LDAP

**LDAP Configuration**

Hostname(s): 10.78.93.148:389

Username: cn=Administrator,cn=users,dc=cisco,dc=com

Cancel Previous Done Save

Copyright © 2008-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

확인 후 저장을 클릭합니다.

암호 자격 증명 검증기

Server Configuration(서버 컨피그레이션) > AUTHENTICATION(인증) > Password Credential Validators(비밀번호 자격 증명 검증기)를 클릭합니다

License Warning: Approaching expiration date

Manage Credential Validator Instances

Credential Validators are plug-ins used to verify username and password pairs in various contexts throughout the system. The actual application of a Validator instance must be configured in the appropriate context as needed (e.g., OAuth Resource Owner Credentials Mapping).

Instance Name	Instance Id	Type	Parent Name	Action
Create New Instance				

Cancel Save

Copyright © 2008-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

Create New Instance를 클릭합니다.

## 유형

The screenshot shows the 'Create Credential Validator Instance' page in the PingFederate console, specifically the 'Type' tab. The page title is 'Manage Credential Validator Instances | Create Credential Validator Instance'. Below the title are tabs for 'Type', 'Instance Configuration', 'Extended Contract', and 'Summary'. The main content area is titled 'Identify this Credential Validator Instance. The Validator types available are limited to the plug-in implementations currently installed on your server.' It contains several form fields: 'INSTANCE NAME' (LDAP Validator), 'INSTANCE ID' (LDAPValidator), 'TYPE' (LDAP Username Password Credential Validator), and 'PARENT INSTANCE' (None). A 'Cancel' button and a 'Next' button are located at the bottom right. A license warning banner is visible at the top.

LDAP 사용자 이름 비밀번호 자격 증명 검증기를 TYPE으로 선택합니다. Next(다음)를 클릭합니다.

## 인스턴스 컨피그레이션

The screenshot shows the 'Instance Configuration' tab of the 'Create Credential Validator Instance' page. The page title is 'Manage Credential Validator Instances | Create Credential Validator Instance'. Below the title are tabs for 'Type', 'Instance Configuration', 'Extended Contract', and 'Summary'. The main content area is titled 'Complete the configuration necessary for this Password Credential Validator to check username/password pairs. This configuration was designed into, and is specific to, the selected Credential Validator plug-in. This password credential validator provides a means of verifying credentials stored in a directory server via the LDAP protocol. Additional user attributes from the directory can also be returned by this PCV by adding the desired attribute names to the Extended Contract.' It contains several form fields: 'AUTHENTICATION ERROR OVERRIDES' (A table of LDAP authentication error codes and customized matching expressions that will match the error code to an LDAP error message. These entries override the default individual mappings of messages to codes. Use the localization features to customize the error messages displayed to end users.), 'MATCH EXPRESSION' (The expression matched against the LDAP error message returned by the server), 'LDAP DATASTORE' (1078.93.148.389), 'SEARCH BASE' (CN=Users,DC=disco,DC=com), 'SEARCH FILTER' (sAMAccountName=\${username}), 'SCOPE OF SEARCH' (One Level, Subtree), and 'CASE-SENSITIVE MATCHING' (checked). A 'Manage Data Stores' button is located at the bottom left. 'Cancel', 'Previous', and 'Next' buttons are located at the bottom right. A license warning banner is visible at the top.

LDAP Datastore(LDAP 데이터 저장소)를 선택하고 Search Base(검색 기준), Search Filter(검색 필터) 및 Scope of Search(검색 범위)를 입력합니다. Next(다음)를 클릭합니다.

## 연장 계약

The screenshot shows the 'Extend the Contract' step of the 'Create Credential Validator Instance' wizard. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the page title is 'Manage Credential Validator Instances | Create Credential Validator Instance'. There are four tabs: 'Type', 'Instance Configuration', 'Extended Contract', and 'Summary', with 'Extended Contract' being the active tab. A message states: 'You can extend the attribute contract of this Password Credential Validator instance.' Under 'Core Contract', there are input fields for 'DN', 'givenName', 'mail', and 'username'. Below this is the 'Extend the Contract' section with an 'Add' button. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Next(다음)를 클릭합니다.

## 요약

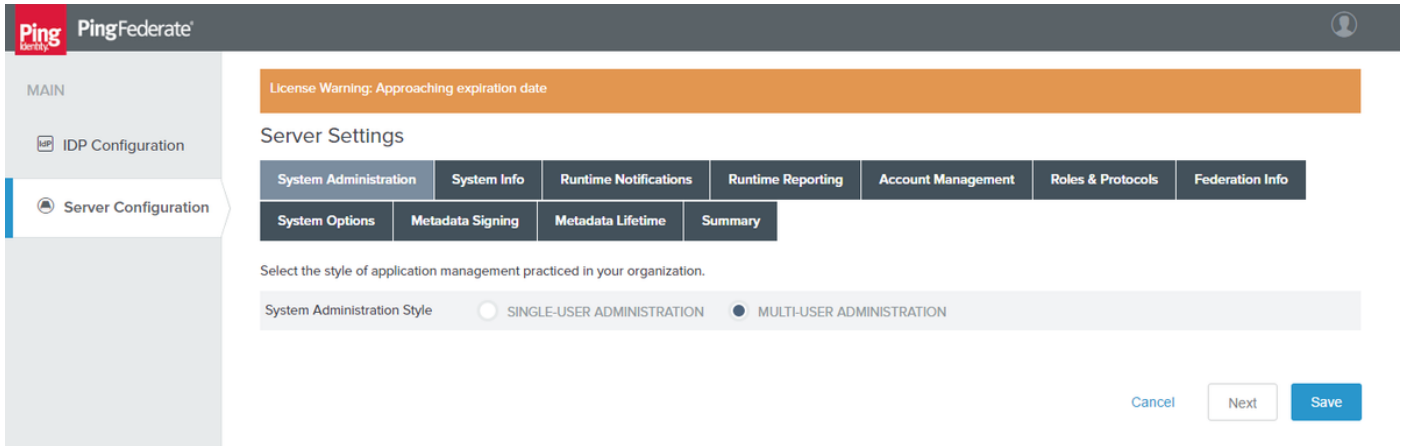
The screenshot shows the 'Summary' step of the 'Create Credential Validator Instance' wizard. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the page title is 'Manage Credential Validator Instances | Create Credential Validator Instance'. There are four tabs: 'Type', 'Instance Configuration', 'Extended Contract', and 'Summary', with 'Summary' being the active tab. A message states: 'Password Credential Validator configuration summary.' Below this is the 'Create Credential Validator Instance' section. Under 'Type', there are fields for 'Instance Name' (LDAP Validator), 'Instance Id' (LDAPValidator), 'Type' (LDAP Username Password Credential Validator), 'Class Name' (org.sourceid.sem120.domain.LDAPUsernamePasswordCredentialValidator), and 'Parent Instance Name' (None). Under 'Instance Configuration', there are fields for 'LDAP Dtestore' (10.78.93.148:389), 'Search Base' (CN=Users,DC=cisco,DC=com), 'Search Filter' (sAMAccountName=\${username}), 'Scope of Search' (Subtree), and 'Case-Sensitive Matching' (true). Under 'Extended Contract', there are fields for 'Attribute' (mail, givenName, DN, username). At the bottom right, there are 'Cancel', 'Previous', and 'Done' buttons.

설정을 확인하고 Done(완료)을 클릭합니다.

## 서버 설정

### 시스템 관리

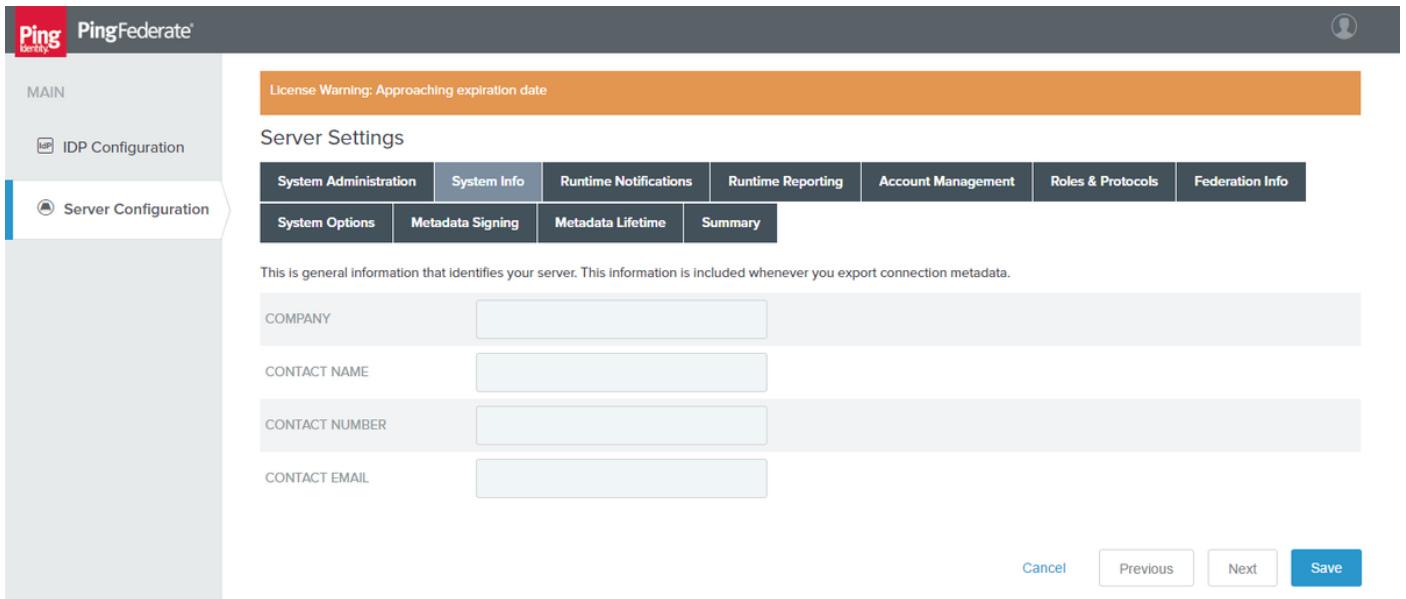
Server Configuration(서버 컨피그레이션) > SYSTEM SETTINGS(시스템 설정)> Server Settings(서버 설정)를 클릭합니다



The screenshot shows the PingFederate interface. At the top, there is a 'License Warning: Approaching expiration date' banner. Below it, the 'Server Settings' section is active, with a sub-tab 'System Administration' selected. Under this tab, 'System Options' is chosen. The main content area contains the text: 'Select the style of application management practiced in your organization.' Below this, there are two radio buttons: 'System Administration Style' with 'SINGLE-USER ADMINISTRATION' (unselected) and 'MULTI-USER ADMINISTRATION' (selected). At the bottom right, there are three buttons: 'Cancel', 'Next', and 'Save'.

Next(다음)를 클릭합니다.

### 시스템 정보



The screenshot shows the PingFederate interface. At the top, there is a 'License Warning: Approaching expiration date' banner. Below it, the 'Server Settings' section is active, with a sub-tab 'System Info' selected. Under this tab, 'System Options' is chosen. The main content area contains the text: 'This is general information that identifies your server. This information is included whenever you export connection metadata.' Below this, there are four input fields: 'COMPANY', 'CONTACT NAME', 'CONTACT NUMBER', and 'CONTACT EMAIL'. At the bottom right, there are four buttons: 'Cancel', 'Previous', 'Next', and 'Save'.

Next(다음)를 클릭합니다.

### 런타임 알림

Ping Federate

License Warning: Approaching expiration date

Server Settings

System Administration | System Info | Runtime Notifications | Runtime Reporting | Account Management | Roles & Protocols | Federation Info

System Options | Metadata Signing | Metadata Lifetime | Summary

Select which server events result in notifications sent via email.

NOTIFICATION FOR SERVER LICENSING EVENTS

NOTIFICATION FOR CERTIFICATE EVENTS

NOTIFICATION FOR SAML METADATA UPDATE EVENTS

Cancel Previous Next Save

Next(다음)를 클릭합니다.

런타임 보고

Ping Federate

License Warning: Approaching expiration date

Server Settings

System Administration | System Info | Runtime Notifications | Runtime Reporting | Account Management | Roles & Protocols | Federation Info

System Options | Metadata Signing | Metadata Lifetime | Summary

If your organization uses SNMP to monitor infrastructure, you can integrate this server with your existing network-management console.

RESPOND TO GET REQUESTS

GENERATE TRAPS

Cancel Previous Next Save

Next(다음)를 클릭합니다.

계정 관리

Ping Federate

License Warning: Approaching expiration date

Server Settings

System Administration | System Info | Runtime Notifications | Runtime Reporting | Account Management | Roles & Protocols | Federation Info

System Options | Metadata Signing | Metadata Lifetime | Summary

Manage administrative-console or API users and their role assignments.

Username		User Admin	Admin	Crypto Admin	Action
Administrator	<input type="radio"/> AUDITOR <input checked="" type="radio"/> ADMIN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Deactivate   Change Password

Create User

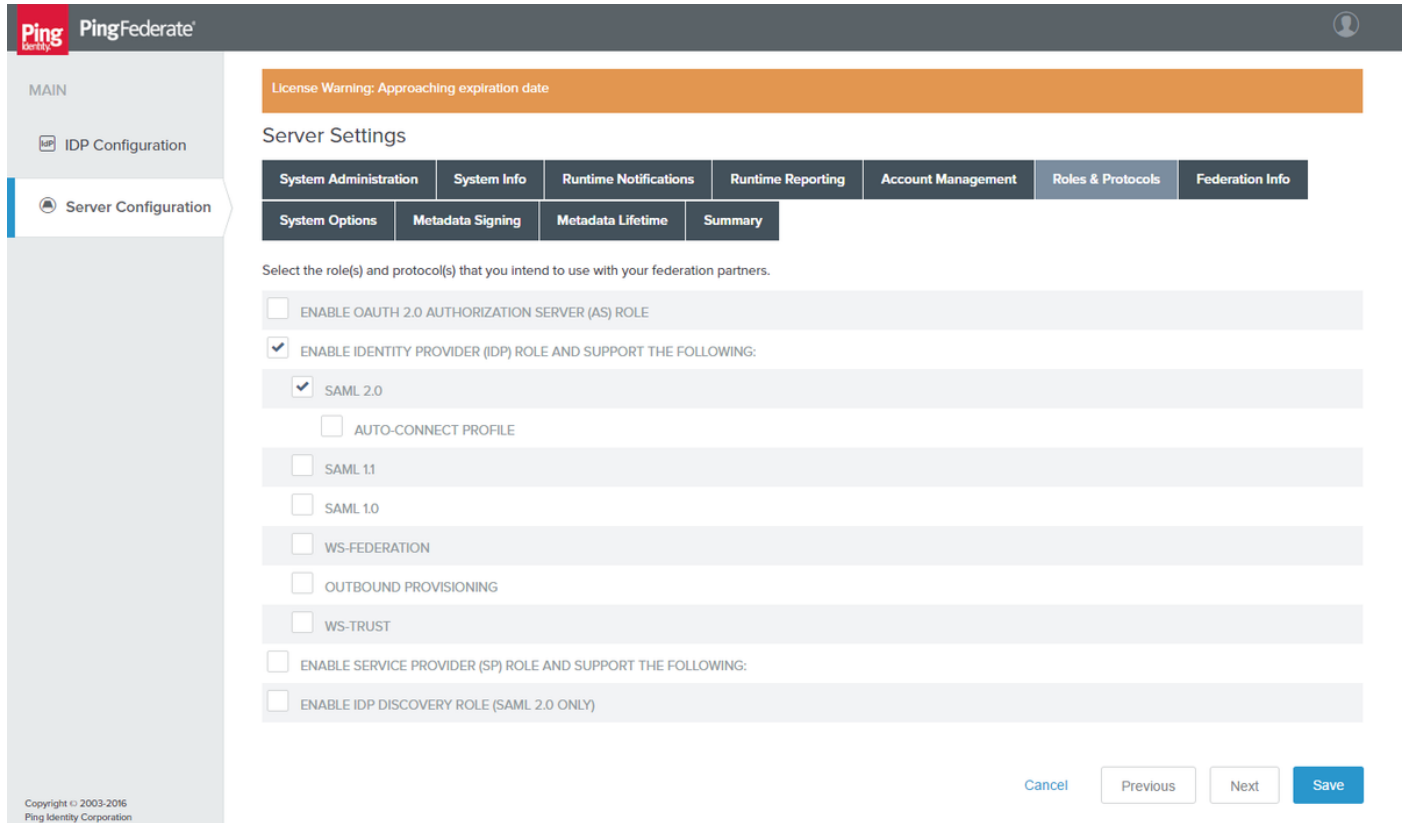
NOTIFY USER OF PASSWORD CHANGE

Cancel Previous Next Save

Next(다음)를 클릭합니다.

참고: 이 섹션에서는 사용자를 추가하거나 사용자의 비밀번호를 변경할 수 있습니다.

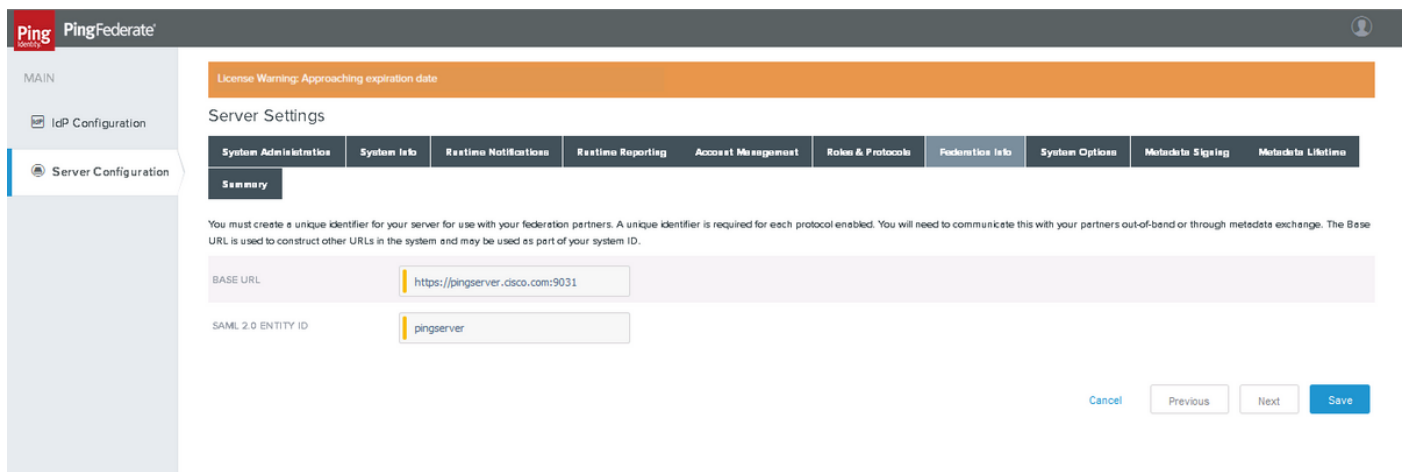
## 역할 및 프로토콜



The screenshot shows the PingFederate administration console. The left sidebar has 'Server Configuration' selected. The main content area is titled 'Server Settings' and has several tabs: 'System Administration', 'System Info', 'Runtime Notifications', 'Runtime Reporting', 'Account Management', 'Roles & Protocols', and 'Federation Info'. The 'Roles & Protocols' tab is active. Below the tabs, there is a warning banner: 'License Warning: Approaching expiration date'. The main content area contains the following text: 'Select the role(s) and protocol(s) that you intend to use with your federation partners.' Below this text are several checkboxes for roles and protocols. The 'ENABLE IDENTITY PROVIDER (IDP) ROLE AND SUPPORT THE FOLLOWING:' section is checked, and 'SAML 2.0' is selected. Other options include 'ENABLE OAUTH 2.0 AUTHORIZATION SERVER (AS) ROLE', 'AUTO-CONNECT PROFILE', 'SAML 1.1', 'SAML 1.0', 'WS-FEDERATION', 'OUTBOUND PROVISIONING', 'WS-TRUST', 'ENABLE SERVICE PROVIDER (SP) ROLE AND SUPPORT THE FOLLOWING:', and 'ENABLE IDP DISCOVERY ROLE (SAML 2.0 ONLY)'. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save'.

적절한 Role/s 및 Protocol/s를 선택합니다. Next(다음)를 클릭합니다.

## 페더레이션 정보



The screenshot shows the PingFederate administration console. The left sidebar has 'Server Configuration' selected. The main content area is titled 'Server Settings' and has several tabs: 'System Administration', 'System Info', 'Runtime Notifications', 'Runtime Reporting', 'Account Management', 'Roles & Protocols', 'Federation Info', 'System Options', 'Metadata Signing', and 'Metadata Lifetime'. The 'Federation Info' tab is active. Below the tabs, there is a warning banner: 'License Warning: Approaching expiration date'. The main content area contains the following text: 'You must create a unique identifier for your server for use with your federation partners. A unique identifier is required for each protocol enabled. You will need to communicate this with your partners out-of-band or through metadata exchange. The Base URL is used to construct other URLs in the system and may be used as part of your system ID.' Below this text are two input fields: 'BASE URL' with the value 'https://pingserver.cisco.com:9031' and 'SAML 2.0 ENTITY ID' with the value 'pingserver'. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save'.

Next(다음)를 클릭합니다.

## 시스템 옵션

License Warning: Approaching expiration date

### Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info
- System Options**
- Metadata Signing
- Metadata Lifetime
- Summary

Configure global server options. Please click Help for more information.

DISABLE AUTOMATIC CONNECTION VALIDATION

DATA-STORE VALIDATION INTERVAL (SECS)

#### Incoming Proxy Settings

HTTP HEADER FOR CLIENT IP ADDRESSES  Use Last Value

HTTP HEADER FOR HOSTNAME  Use Last Value

CLIENT CERTIFICATE HEADER NAME

CLIENT CERTIFICATE CHAIN HEADER NAME

INCOMING PROXY TERMINATES HTTPS CONNECTIONS

Cancel Previous Next Save

Next(다음)를 클릭합니다.

메타데이터 서명

License Warning: Approaching expiration date

### Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info
- System Options
- Metadata Signing**
- Metadata Lifetime
- Summary

Select a certificate for signing the metadata which will be published. If no certificate is selected, the published metadata will not be signed.

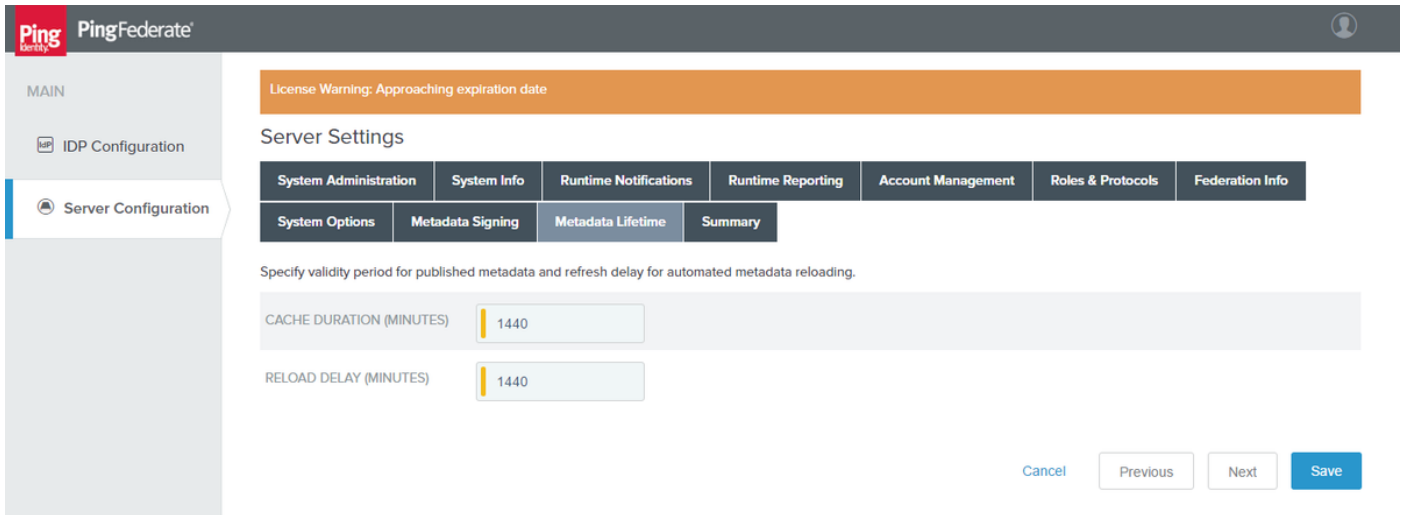
SIGNING CERTIFICATE

SIGNING ALGORITHM

Cancel Previous Next Save

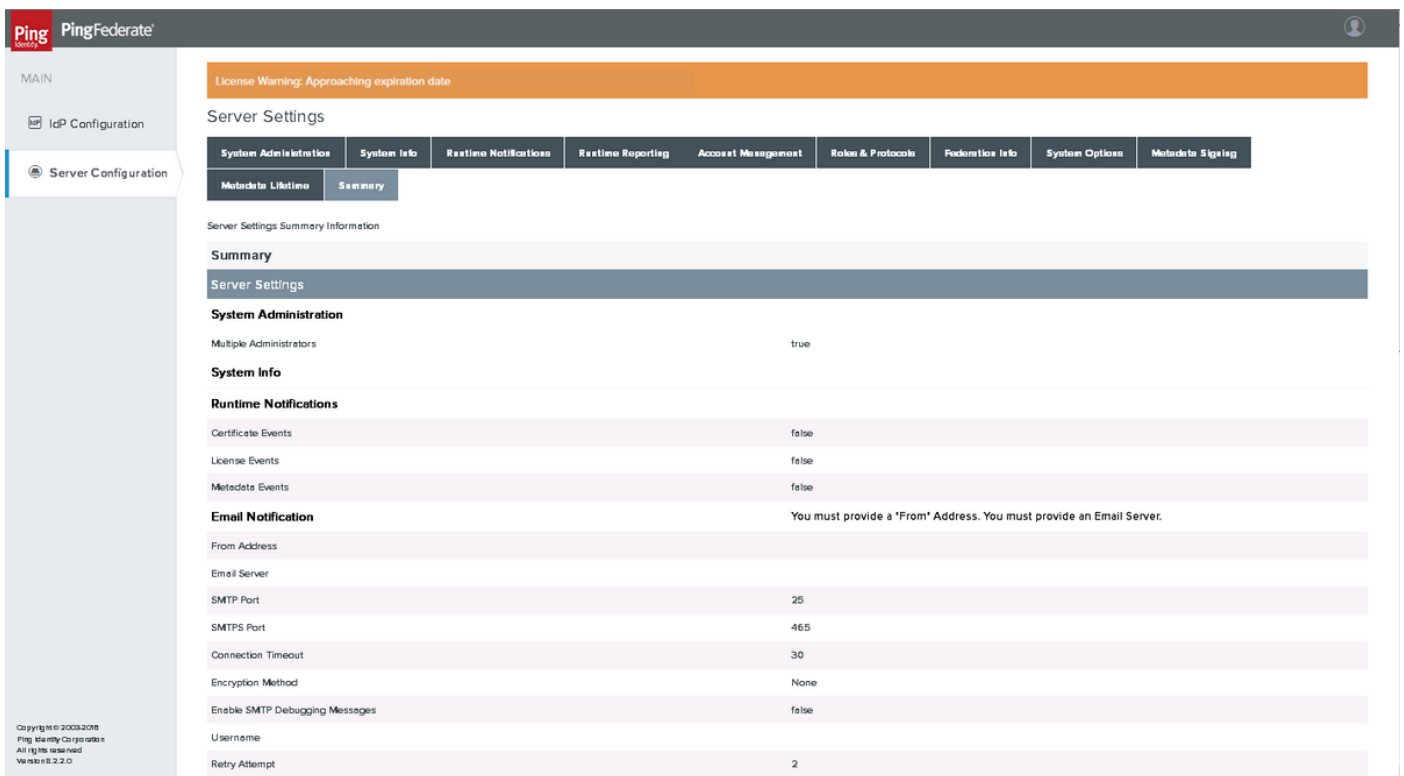
인증서 컨피그레이션의 일부로 앞에서 생성한 서명 인증서 및 서명 알고리즘을 선택합니다.  
Next(다음)를 클릭합니다.

메타데이터 수명



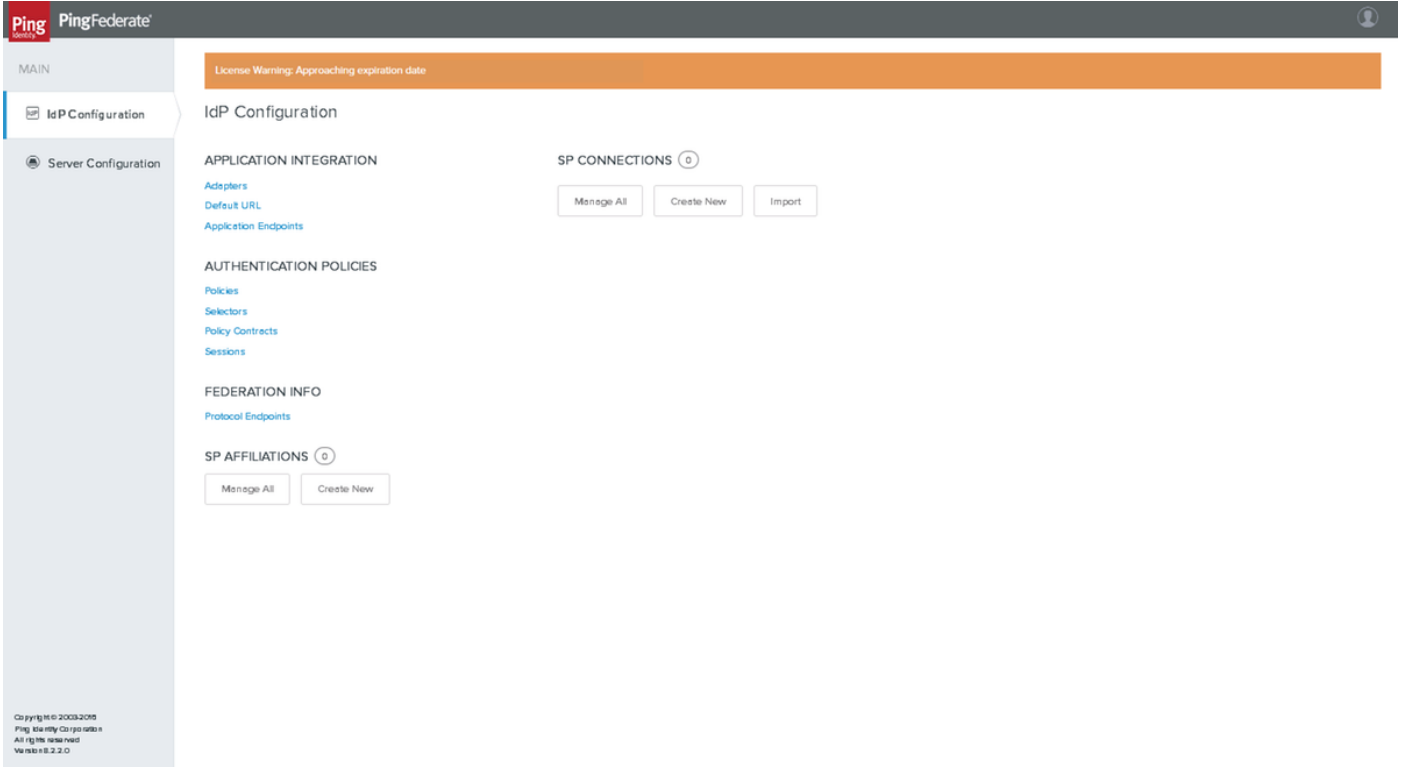
Next(다음)를 클릭합니다.

요약



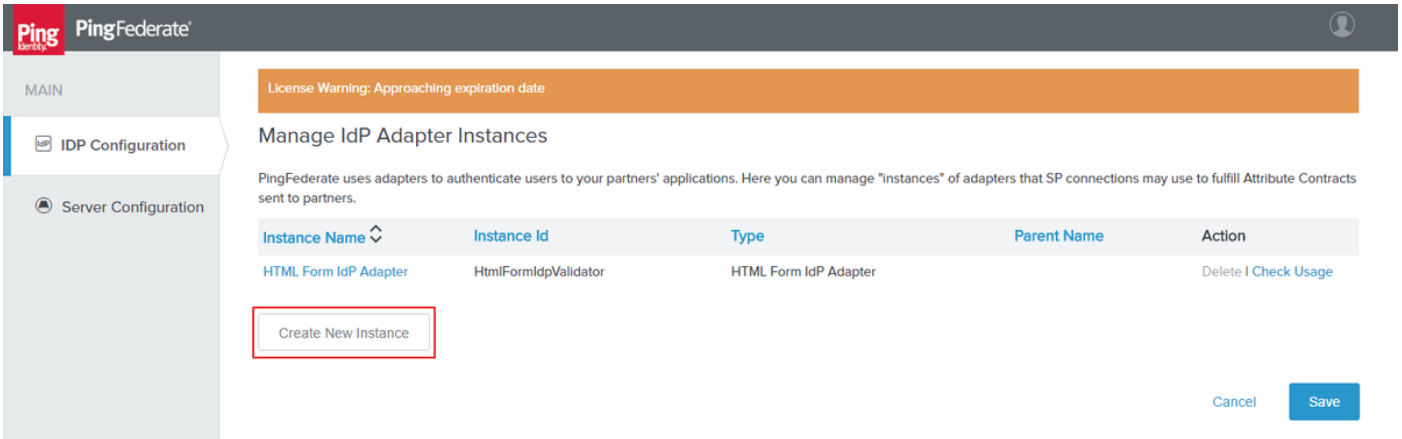
설정을 확인하고 저장을 클릭합니다.

IdP(Identity Provider) 컨피그레이션



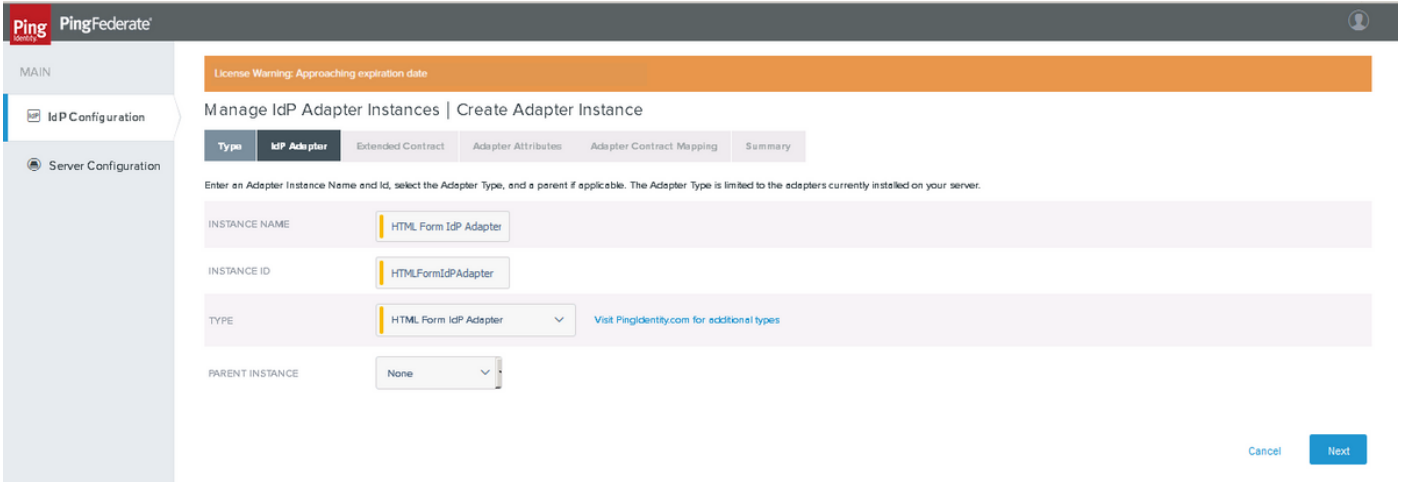
## 어댑터

IdP Configuration(IdP 컨피그레이션) > APPLICATION INTEGRATION(APPLICATION 통합) > Adapters(어댑터)를 클릭합니다



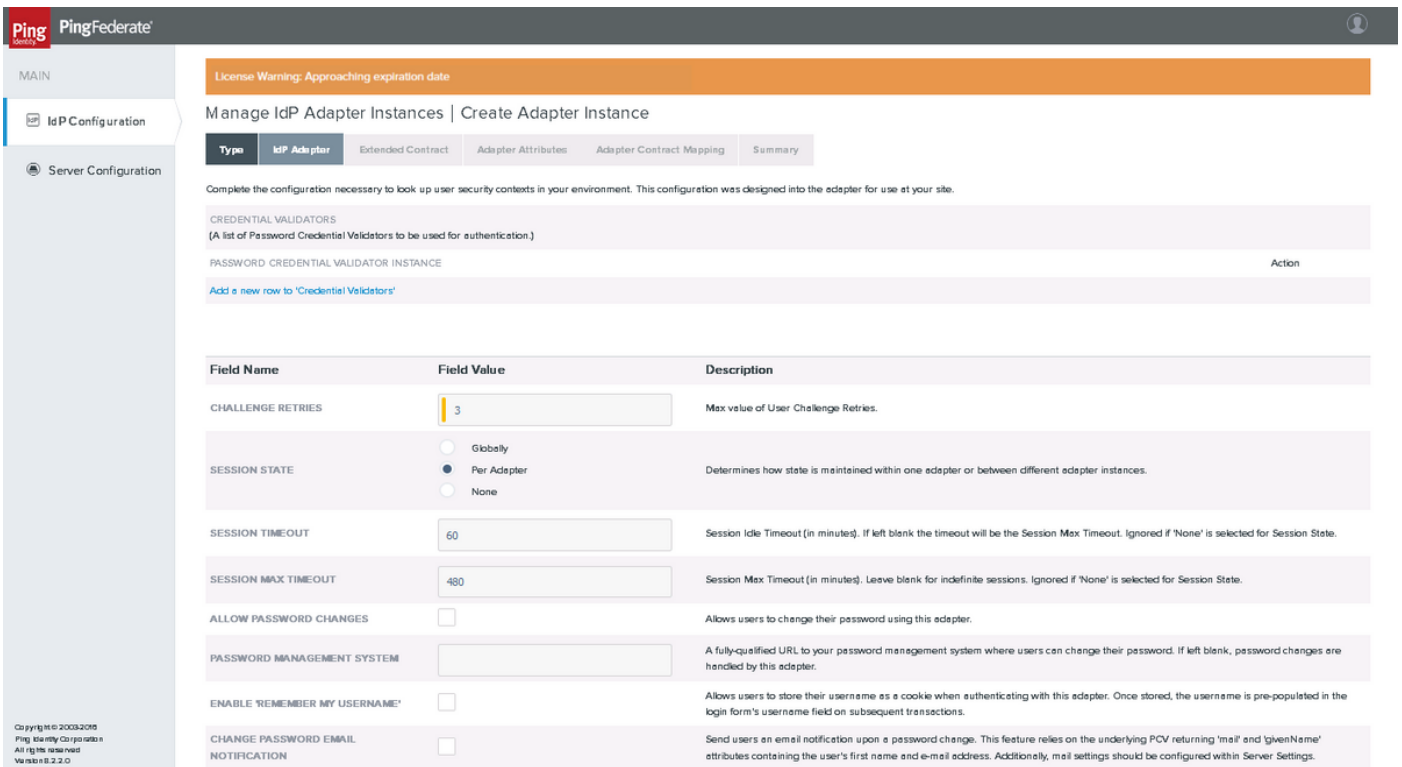
Create New Instance를 클릭합니다.

## 유형



HTML 양식 IDP 어댑터를 선택합니다. Next(다음)를 클릭합니다.

IdP 어댑터



Add a new row to 'Credential Validators'를 클릭하고 앞서 PASSWORD CREDENTIAL VALIDATOR INSTANCE로 만든 LDAP Validator를 선택한 후 Update를 클릭합니다. Next를 클릭합니다.

연장 계약

Ping Federate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance

Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract may be used to fulfill the Attribute Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

**Core Contract**

username

**Extend the Contract**      **Action**

email	<a href="#">Edit</a>   <a href="#">Delete</a>
firstname	<a href="#">Edit</a>   <a href="#">Delete</a>
lastname	<a href="#">Edit</a>   <a href="#">Delete</a>
uid	<a href="#">Edit</a>   <a href="#">Delete</a>
updatetimestamp	<a href="#">Edit</a>   <a href="#">Delete</a>
user_principal	<a href="#">Edit</a>   <a href="#">Delete</a>

[Cancel](#) [Previous](#) [Next](#) [Done](#)

표시된 대로 계약을 추가합니다. Next(다음)를 클릭합니다.

### 어댑터 특성

Ping Federate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance

Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
firstname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
lastname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
uid	<input checked="" type="checkbox"/>	<input type="checkbox"/>
updatetimestamp	<input checked="" type="checkbox"/>	<input type="checkbox"/>
user_principal	<input checked="" type="checkbox"/>	<input type="checkbox"/>
username	<input checked="" type="checkbox"/>	<input type="checkbox"/>

MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES

[Cancel](#) [Previous](#) [Next](#) [Done](#)

Next(다음)를 클릭합니다.

### 어댑터 계약 매핑

The screenshot shows the 'Configure Adapter Contract' step in the PingFederate interface. The breadcrumb trail is 'Manage IdP Adapter Instances | Create Adapter Instance'. The current step is 'Adapter Contract Mapping', with other steps being 'Type', 'IdP Adapter', 'Extended Contract', 'Adapter Attributes', and 'Summary'. A red box highlights the 'Configure Adapter Contract' button. Below the breadcrumb, there is a text block explaining that an Adapter Contract can be used to fulfill the Attribute Contract. At the bottom right, there are navigation buttons: 'Cancel', 'Previous', 'Next', and 'Done'.

Configure Adapter Contract(어댑터 계약 구성)를 클릭합니다.

특성 소스 및 사용자 조회

The screenshot shows the 'Adapter Contract Mapping' step in the PingFederate interface. The breadcrumb trail is 'Manage IdP Adapter Instances | Create Adapter Instance | Adapter Contract Mapping'. The current step is 'Adapter Contract Mapping', with other steps being 'Attribute Sources & User Lookup', 'Adapter Contract Fulfillment', 'Issuance Criteria', and 'Summary'. Below the breadcrumb, there is a text block explaining that you can choose to fulfill the Adapter Contract with the adapter's default values or use values plus additional attributes from local data stores. A table lists the attribute sources:

Description	Type	Action
LdapQA	LDAP	Delete

Below the table is an 'Add Attribute Source' button. At the bottom right, there are navigation buttons: 'Cancel', 'Next', and 'Done'.

특성 소스를 추가하고 이전에 생성한 LDAP 저장소를 선택합니다. Next(다음)를 클릭합니다.

어댑터 계약 이행

PingFederate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance | Adapter Contract Mapping

Attribute Sources & User Lookup | Adapter Contract Fulfillment | Issuance Criteria | Summary

Fulfill your Adapter Contract with values from the authentication adapter or with dynamic text values.

Contract	Source	Value	Actions
email	LDAP (LdapQA)	mail	None available
firstname	LDAP (LdapQA)	givenName	None available
lastname	LDAP (LdapQA)	sn	None available
uid	LDAP (LdapQA)	sAMAccountName	None available
updateTimestamp	LDAP (LdapQA)	whenChanged	None available
user_principal	LDAP (LdapQA)	userPrincipalName	None available
username	LDAP (LdapQA)	sAMAccountName	None available

Cancel Previous Next Done

특성을 매핑합니다. Next(다음)를 클릭합니다.

발급 기준

PingFederate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance | Adapter Contract Mapping

Attribute Sources & User Lookup | Adapter Contract Fulfillment | Issuance Criteria | Summary

PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization.

Source	Attribute Name	Condition	Value	Error Result	Action
- SELECT -	- SELECT -	- SELECT -			Add

Cancel Previous Next Done

Next(다음)를 클릭합니다.

요약

The screenshot shows the 'IdP Configuration' page in PingFederate. The left sidebar has 'MAIN', 'IdP Configuration', and 'Server Configuration'. The main content area is divided into several sections:

- Data Store:** 10.78.93.148:389
- LDAP Directory Search:**
  - Base DN: cn=users,dc=cisco,dc=com
  - Search scope: SUBTREE\_SCOPE
  - Attribute: Subject DN
  - Attribute: givenName
  - Attribute: mail
  - Attribute: sAMAccountName
  - Attribute: sn
  - Attribute: userPrincipalName
  - Attribute: whenChanged
- LDAP Filter:** Filter: sAMAccountName=\${username}
- Adapter Contract Fulfillment:**
  - uid: sAMAccountName (LDAP)
  - firstname: givenName (LDAP)
  - updateTimestamp: whenChanged (LDAP)
  - user\_principal: userPrincipalName (LDAP)
  - email: mail (LDAP)
  - lastname: sn (LDAP)
  - username: sAMAccountName (LDAP)
- Issuance Criteria:** Criterion: (None)

At the bottom right, there are 'Cancel', 'Previous', and 'Done' buttons. A copyright notice is visible in the bottom left corner.

설정을 확인하고 Done(완료)을 클릭합니다.

SP 접속

새 SP 접속 생성

연결 유형

The screenshot shows the 'SP Connection' page in PingFederate. The left sidebar has 'MAIN', 'IdP Configuration', and 'Server Configuration'. The main content area has a 'License Warning: Approaching expiration date' banner at the top. Below it, the 'SP Connection' title is followed by tabs: 'Connection Type', 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. The 'Connection Type' tab is active, showing a selection screen with the text: 'Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.'

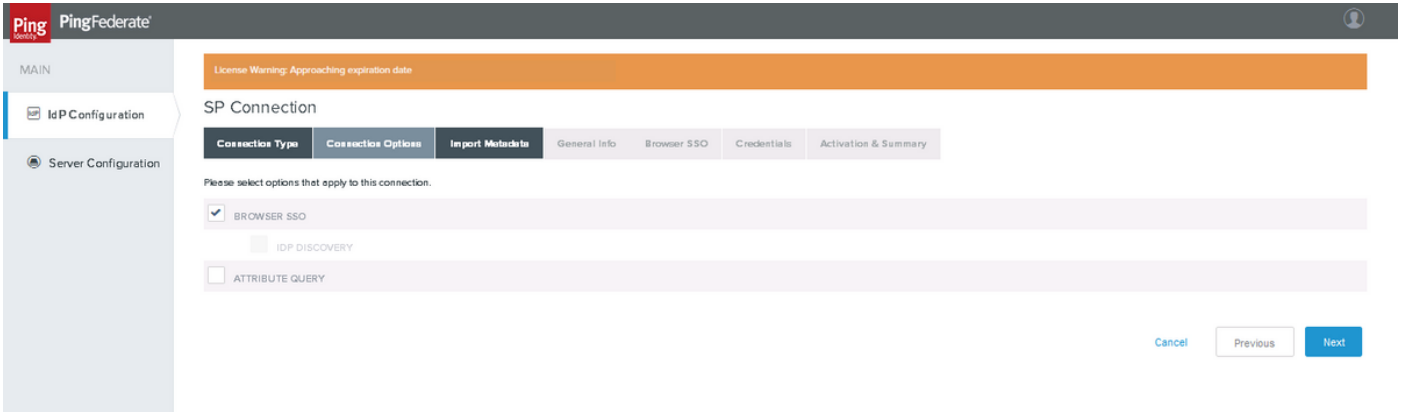
The 'CONNECTION TEMPLATE' section shows:

- BROWSER SSO PROFILES: No Template, PROTOCOL: SAML 2.0
- WS-TRUST STS
- OUTBOUND PROVISIONING

At the bottom right, there are 'Cancel' and 'Next' buttons.

Next(다음)를 클릭합니다.

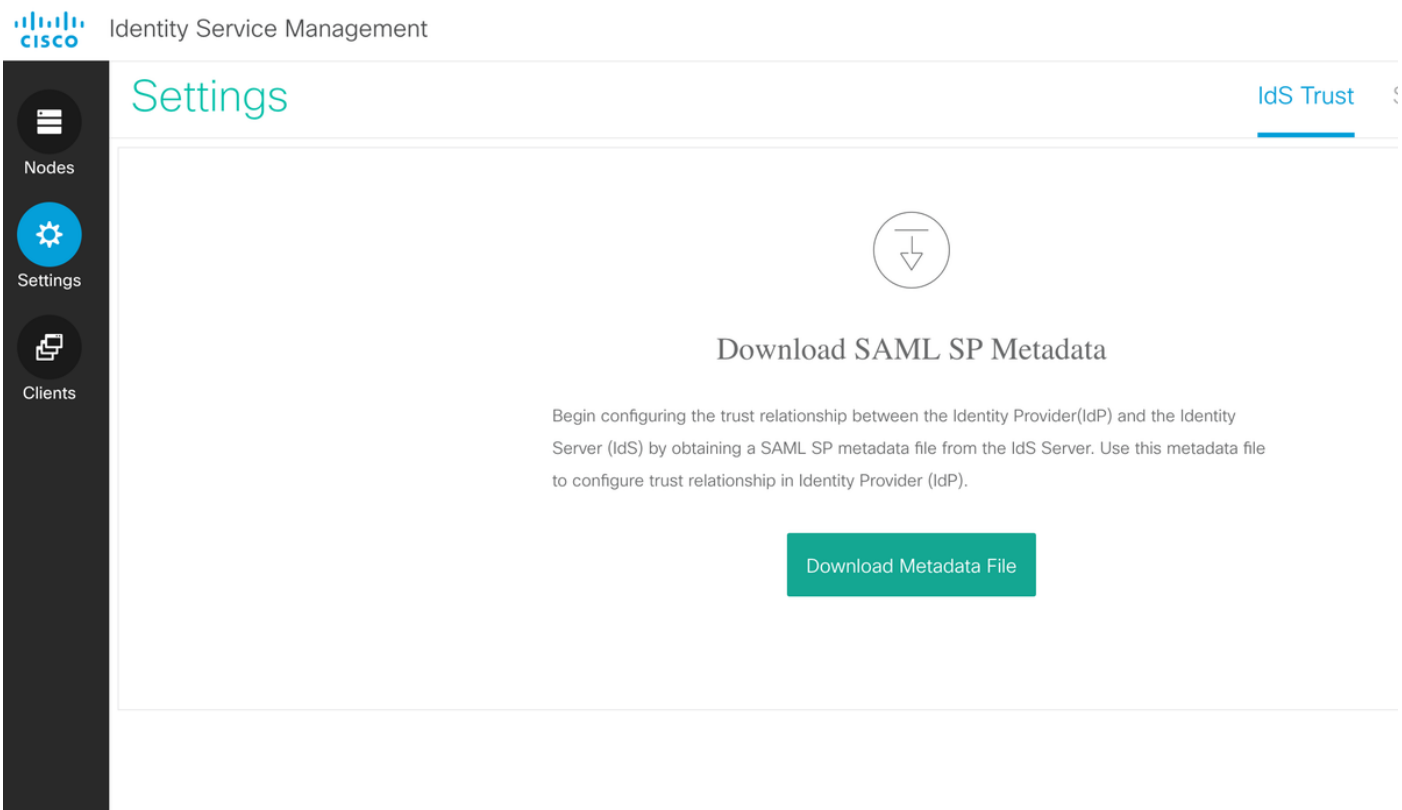
연결 옵션



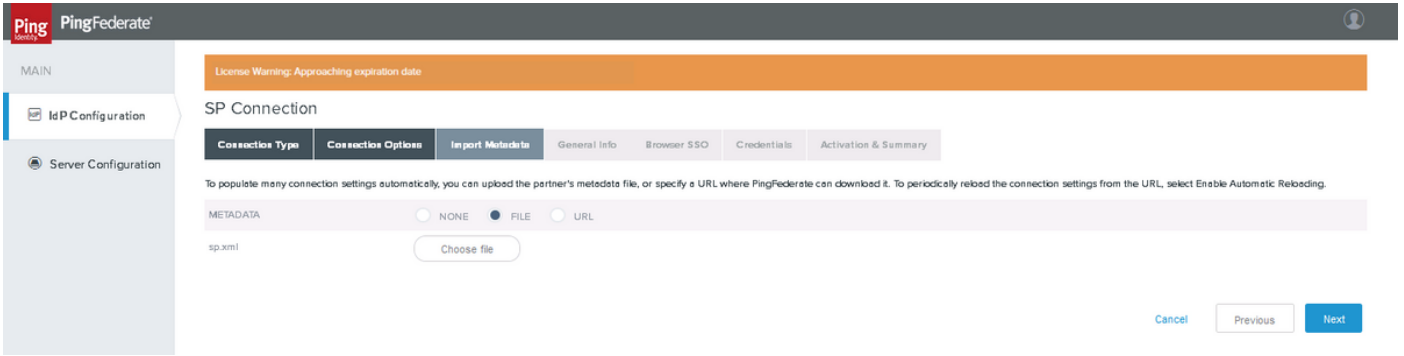
Next(다음)를 클릭합니다.

메타데이터 가져오기

Cisco Identity Service Admin(Cisco Identity Service 관리) > Settings(설정) > IdS Trust(IdS 트러스트) > Download Metadata(메타데이터 다운로드)에서 서비스 공급자의 메타데이터 xml 파일 다운로드

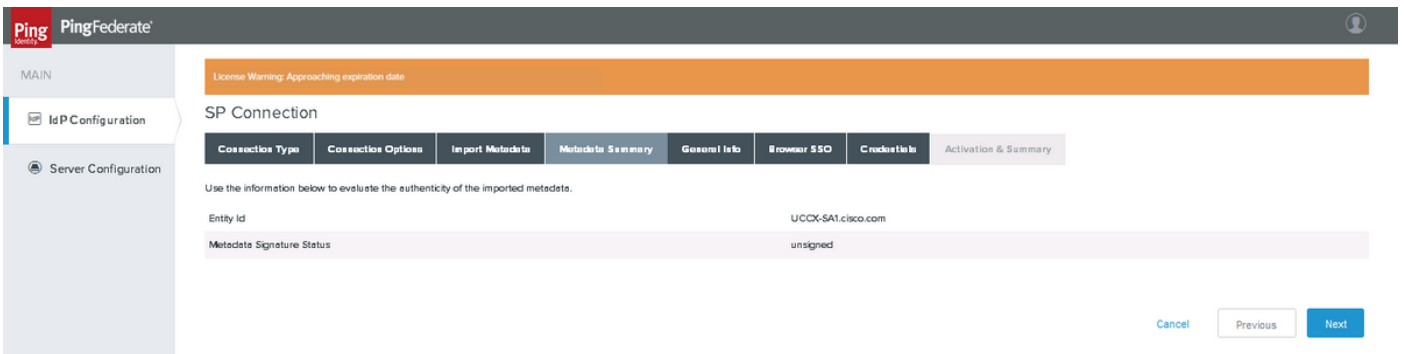


서비스 공급자의 메타데이터 xml 파일을 PingFederate에 업로드합니다.



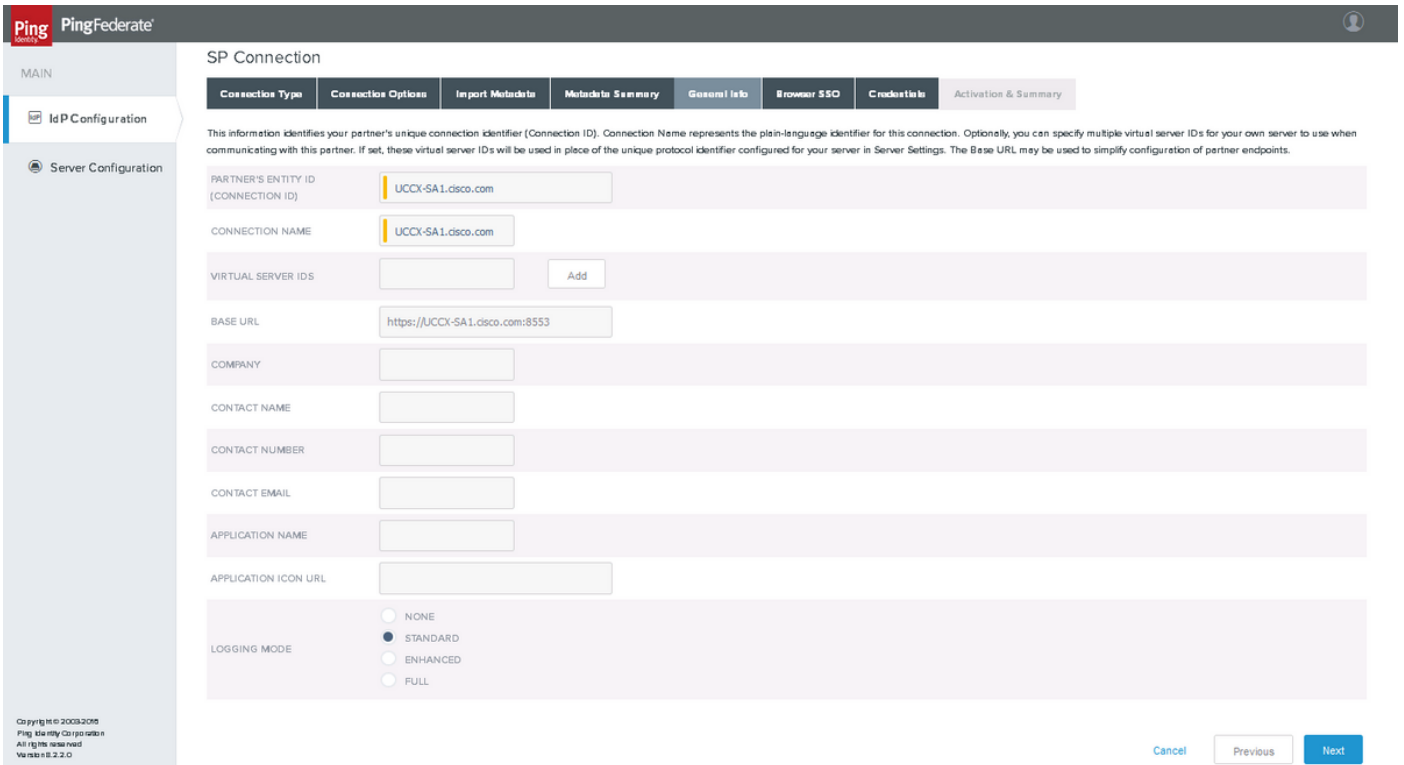
다운로드한 xml 파일을 선택하고 다음을 클릭합니다.

메타데이터 요약



Next(다음)를 클릭합니다.

general info



Next(다음)를 클릭합니다.

## 브라우저 SSO

The screenshot shows the PingFederate interface for configuring an SP Connection. The 'Browser SSO' tab is active. A 'Configure Browser SSO' button is located in the 'BROWSER SSO CONFIGURATION' section. Navigation buttons 'Cancel', 'Save Draft', 'Previous', and 'Next' are at the bottom right.

브라우저 SSO 구성을 클릭합니다

SAML(Security Assertion Markup Language) 프로파일

The screenshot shows the 'SAML Profiles' tab selected. Under 'Single Sign-On (SSO) Profiles', 'IDP-INITIATED SSO' and 'SP-INITIATED SSO' are checked. Under 'Single Logout (SLO) Profiles', both 'IDP-INITIATED SLO' and 'SP-INITIATED SLO' are unchecked. The 'Next' button is highlighted.

Next(다음)를 클릭합니다.

참고: SLO(Single Logout)는 11.6의 Cisco Id(Identity Service)에서 지원되지 않으며 선택되지 않습니다.

어설션 수명

The screenshot shows the 'Assertion Lifetime' tab selected. The 'MINUTES BEFORE' and 'MINUTES AFTER' input fields are both set to the value '5'. The 'Save' button is highlighted.

Next(다음)를 클릭합니다.

어설션 생성

License Warning: Approaching expiration date

### SP Connection | Browser SSO

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

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

#### Assertion Configuration

IDENTITY MAPPING	Standard
ATTRIBUTE CONTRACT	SAML_SUBJECT, email, firstname, lastname, uid, updateTimestamp
ADAPTER INSTANCES	1
AUTHENTICATION POLICY MAPPINGS	0

**Configure Assertion Creation**

Cancel Previous Next Done Save

Configure Assertion Creation(어설션 생성 구성)을 클릭합니다

ID 매핑

License Warning: Approaching expiration date

### SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

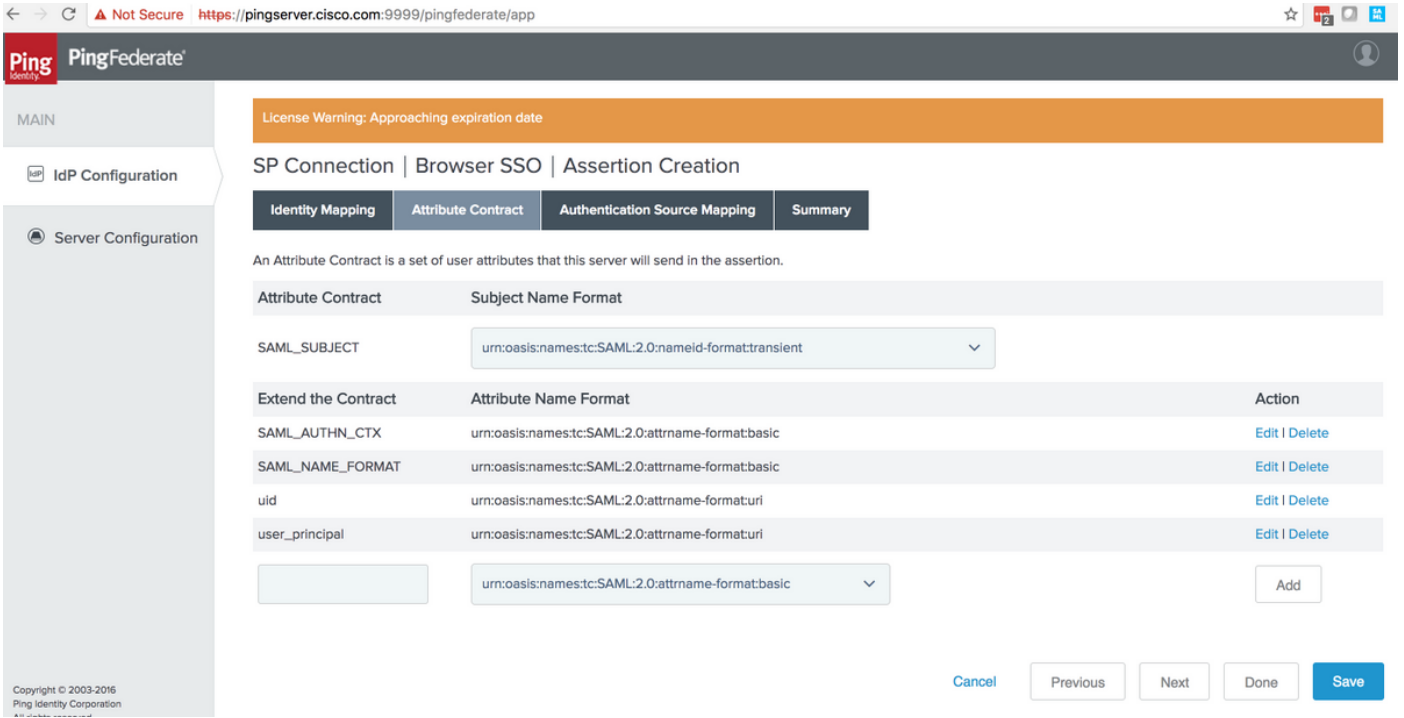
Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Select the type of name identifier that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.

- STANDARD:** Send the SP a known attribute value as the name identifier. The SP will often use account mapping to identify the user locally.
  - INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM.
- PSEUDONYM:** Send the SP a unique, opaque name identifier that preserves user privacy. The identifier cannot be traced back to the user's identity at this IdP and may be used by the SP to make a persistent association between the user and a specific local account. The SP will often use account linking to identify the user locally.
- TRANSIENT:** Send the SP an opaque, temporary value as the name identifier.
  - INCLUDE ATTRIBUTES IN ADDITION TO THE TRANSIENT IDENTIFIER.

Cancel Next Done Save

Next(다음)를 클릭합니다.

속성 계약



경고: 이러한 특성은 Cisco Identity Service(Id)와 PingFederate의 상호 운용성을 위해 반드시 필요합니다.

속성 계약	목적
SAML_제목	PingFederate 검색 필터에서 매핑된 값이 충족되는지 확인하는 데 사용됩니다.
SAML_AUTHN_CTX	'PasswordProtectedTransport' 인증 내용을 나타내기 위해 SAML 응답에 사용됩니다.
SAML_이름_형식	SAML 2.0 임시 이름 ID 형식을 나타내기 위해 SAML 응답에 사용됩니다.
uid	Cisco Id에서 인증된 사용자를 식별하는 데 사용
사용자_계정	Cisco Id에서 인증된 사용자의 전체 이름(예: id + 도메인)을 식별하는 데 사용됩니다.

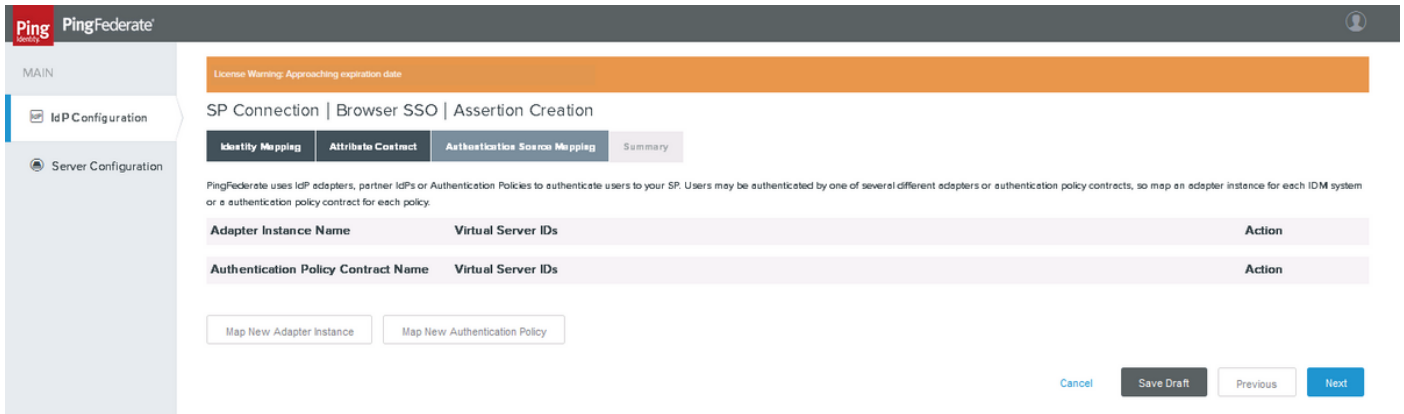
관리자는 이 디렉토리에 있는 custom-name-formats.xml 구성 파일을 통해 이름 형식 대안을 사용자 정의할 수 있습니다.

<pf\_install>/pingfederate/server/default/data/config-store.

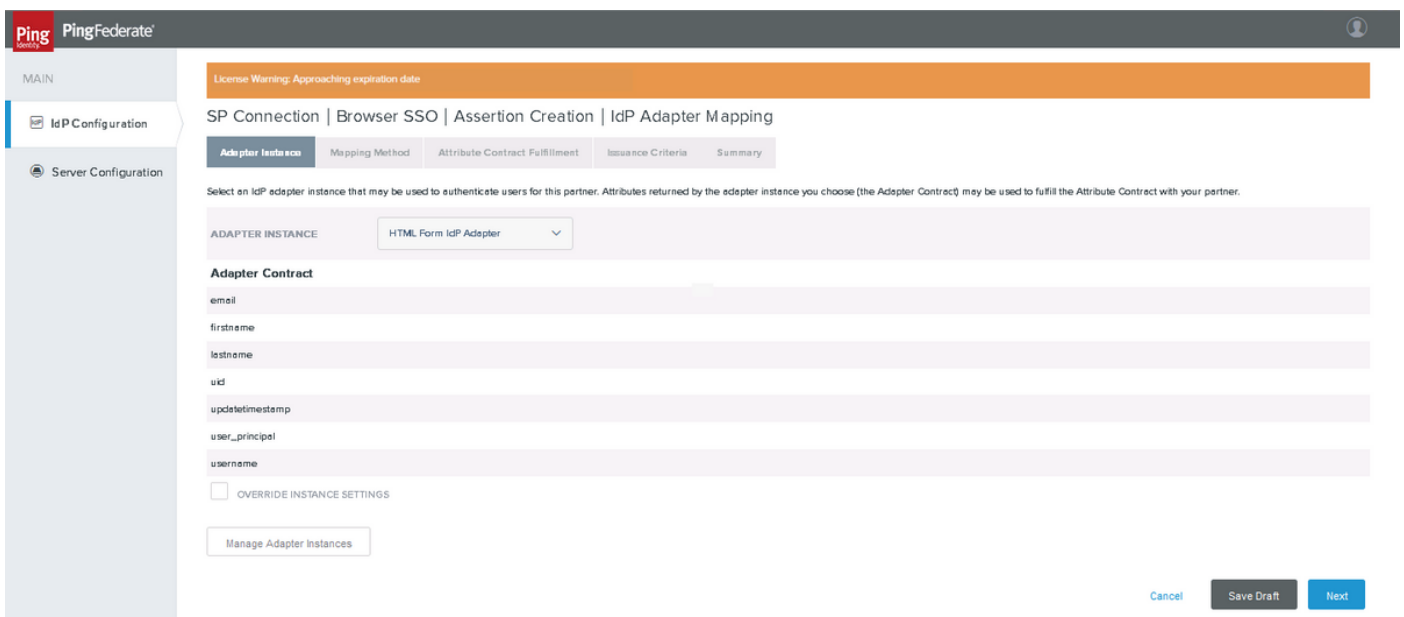
임시 SSO를 이름 식별자로 사용하려면 saml2-subject-name-formats 섹션에 xml 항목을 추가합니다. <con:item name="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">urn:oasis:names:tc:SAML:2.0:nameid-format:transient</con:item>

Next(다음)를 클릭합니다.

인증 소스 매핑

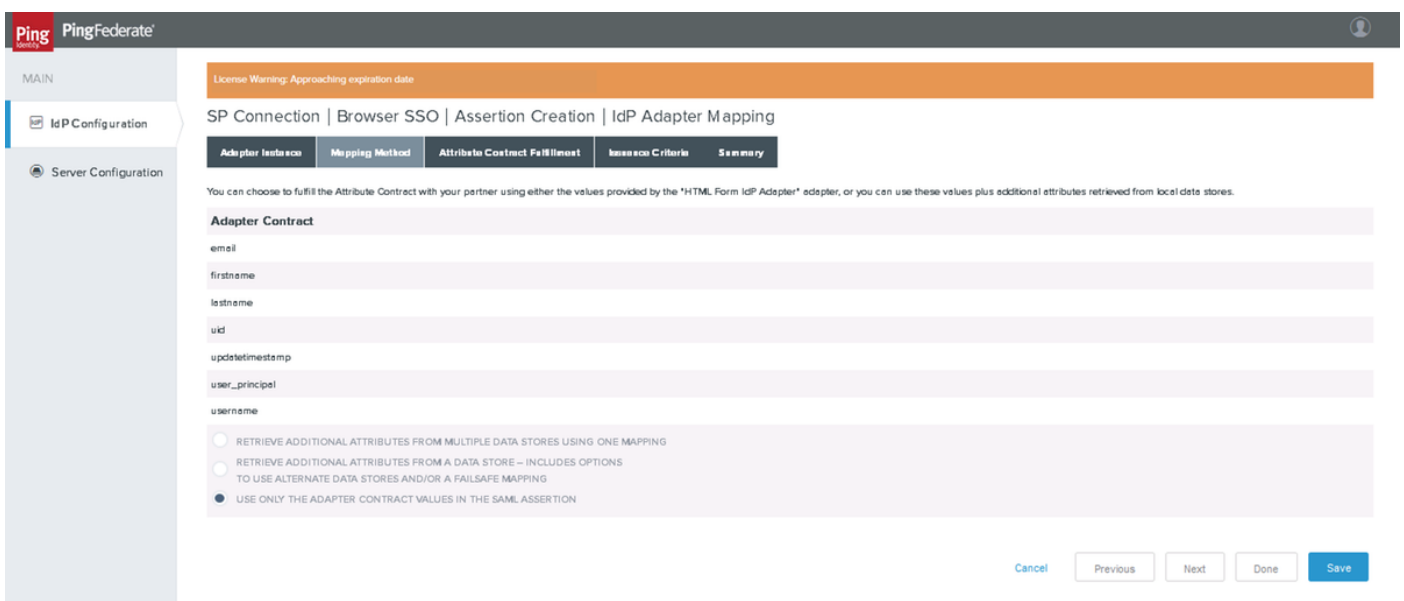


Map New Adapter Instance(새 어댑터 인스턴스 매핑)를 클릭합니다



이전에 만든 HTML 양식 IdP 어댑터를 매핑합니다. Next(다음)를 클릭합니다.

매핑 방법



Next(다음)를 클릭합니다.

계약 이행 속성

License Warning: Approaching expiration date

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

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | Issuance Criteria | Summary

Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

Attribute Contract	Source	Value	Actions
SAML_AUTHN_CTX	Text	urn:oasis:names:tc:SAI	None available
SAML_NAME_FORMAT	Text	urn:oasis:names:tc:SAI	None available
SAML_SUBJECT	Adapter	username	None available
uid	Adapter	uid	None available
user_principal	Adapter	user_principal	None available

Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

Cancel Previous Next Done Save

값이 로 설정되어 있는지 확인합니다.

속성 계약	소스	가치
SAML_제목	어댑터	사용자 이름 매우 중요 참고 사항: 이 설정에 사용된 값은 LDAP 필터 설정에 사용된 값과 일치해야 합니다(섹션#3.1.3.2. 인스턴스 구성). 참고: 'username'은 사용된 필터에 sAMAccountName=\${username}이(가) 있으므로 여기에 사용됩니다.
SAML_AUTHN_CTX	텍스트	urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport
SAML_이름_형식	텍스트	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
uid	어댑터	uid
사용자_계정	어댑터	사용자_계정

속성 계약	소스	가치
	터	

Next(다음)를 클릭합니다.

발급 기준

License Warning: Approaching expiration date

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

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | Issuance Criteria | Summary

PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization.

Source	Attribute Name	Condition	Value	Error Result	Action
- SELECT -	- SELECT -	- SELECT -			Add

Cancel Previous Next Done Save

요약

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

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | Issuance Criteria | Summary

Click a heading link to edit a configuration setting.

**Adapter Instance**

Selected adapter: HTML Form IdP Adapter 1

**Mapping Method**

Adapter: HTML Form IdP Adapter

Mapping Method: Use only the Adapter Contract values in the mapping

**Attribute Contract Fulfillment**

uid: uid (Adapter)

SAML\_AUTHN\_CTX: urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport (Text)

user\_principal: user\_principal (Adapter)

SAML\_SUBJECT: username (Adapter)

SAML\_NAME\_FORMAT: urn:oasis:names:tc:SAML:2.0:nameid-format:transient (Text)

**Issuance Criteria**

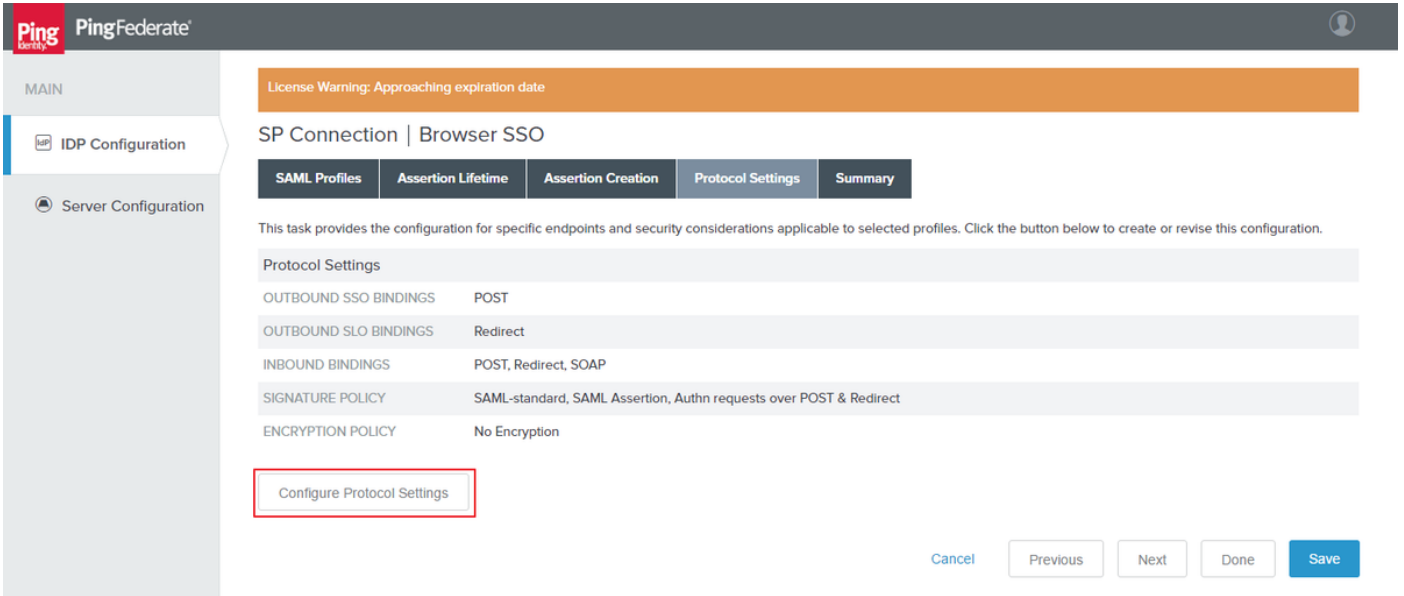
Criterion: (None)

Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

Cancel Previous Done Save

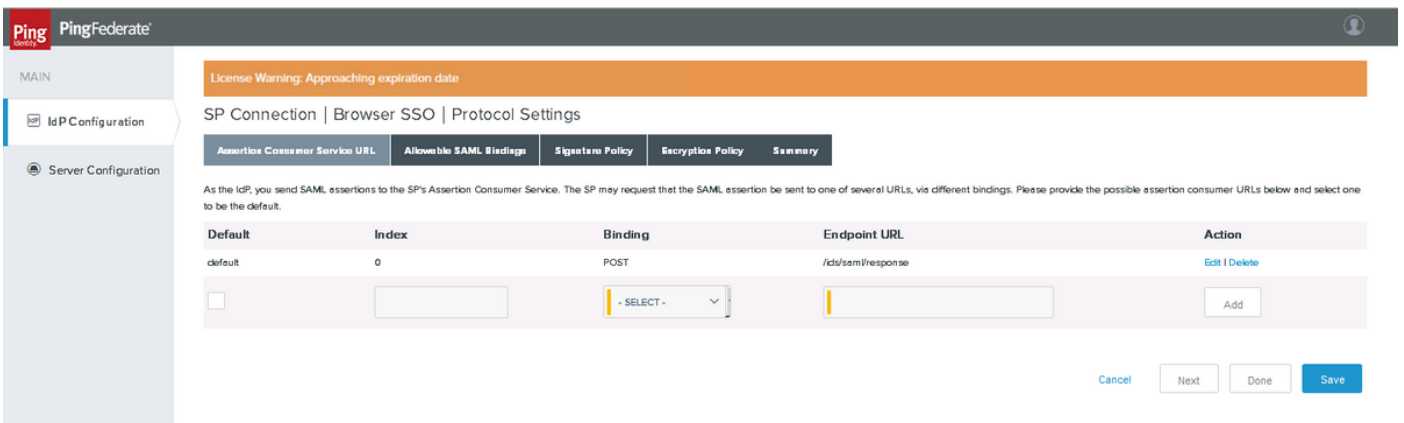
설정을 확인하고 Done(완료)을 클릭합니다.

프로토콜 설정



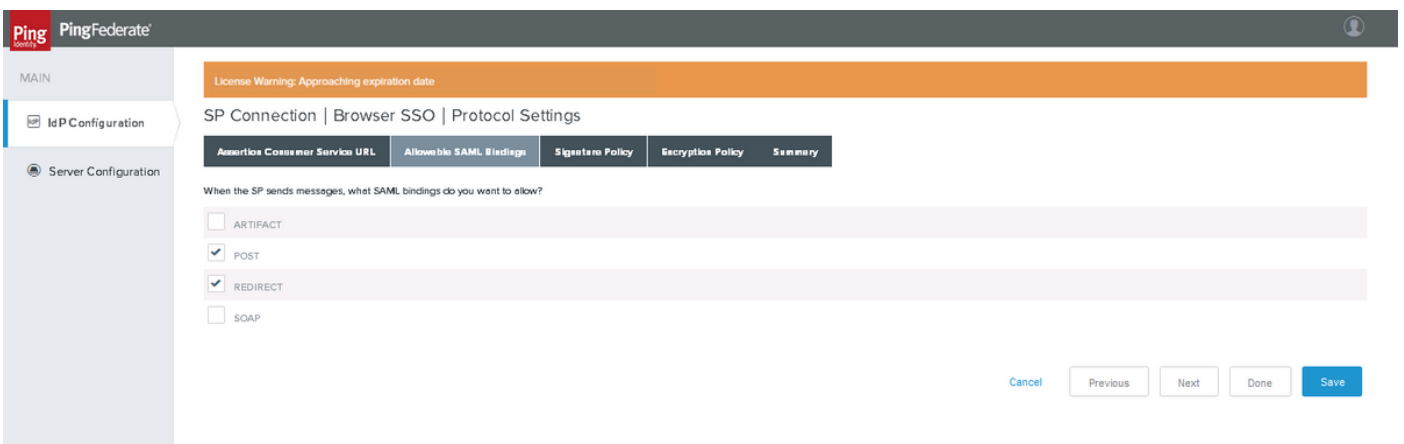
Configure Protocol Settings를 클릭합니다

어설션 소비자 서비스 URL



POST 바인딩 SSO 끝점을 추가합니다. Next(다음)를 클릭합니다.

허용 가능한 SAML 바인딩



Next(다음)를 클릭합니다.

## 서명 정책

The screenshot shows the 'Protocol Settings' page for 'Signatures Policy' in PingFederate. The page title is 'SP Connection | Browser SSO | Protocol Settings'. There are five tabs: 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signatures Policy', 'Encryption Policy', and 'Summary'. The 'Signatures Policy' tab is active. Below the tabs, there is a text block: 'Additional guarantees of authenticity may be agreed upon between you and your partner. For SP-initiated SSO, you can choose to require signed authentication requests sent via the POST or redirect bindings. You can also choose to sign assertions sent to this partner, regardless of the binding used.' There are two radio button options: 'REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIRECT BINDINGS' (which is selected) and 'ALWAYS SIGN THE SAML ASSERTION'. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

참고: Cisco Id는 SAML 메시지에 '서명됨'을 보증하므로 'ALWAYS SIGN THE SAML ASSERTION'을 선택하지 않습니다. 이는 PingFederate가 'SAML assertion' 또는 'SAML response' 중 하나만 서명할 수 있기 때문입니다.

Next(다음)를 클릭합니다.

## 암호화 정책

The screenshot shows the 'Protocol Settings' page for 'Encryption Policy' in PingFederate. The page title is 'SP Connection | Browser SSO | Protocol Settings'. There are five tabs: 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signatures Policy', 'Encryption Policy', and 'Summary'. The 'Encryption Policy' tab is active. Below the tabs, there is a text block: 'Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.' There are three radio button options: 'NONE' (which is selected), 'THE ENTIRE ASSERTION', and 'ONE OR MORE ATTRIBUTES'. Below these, there are four checkboxes: 'SAML\_SUBJECT', 'SAML\_NAME\_FORMAT', 'UID', and 'USER\_PRINCIPAL'. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

참고: Cisco Id는 암호화된 SAML 흐름을 지원하지 않으므로 '암호화 정책' 설정에 대해 '없음'을 선택합니다.

Next(다음)를 클릭합니다.

## 요약

License Warning: Approaching expiration date

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | Allowable SAML Bindings | Signature Policy | Encryption Policy | **Summary**

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

**Protocol Settings**

**Assertion Consumer Service URL**

Endpoint URL: /ids/saml/response (POST)

**Allowable SAML Bindings**

Artifact	false
POST	true
Redirect	true
SOAP	false

**Signature Policy**

Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false

**Encryption Policy**

Status	Inactive
--------	----------

Cancel Previous **Done** Save

설정을 확인하고 Done(완료)을 클릭합니다.

자격 증명

License Warning: Approaching expiration date

SP Connection

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

For each credential shown here, configure the necessary settings.

**Credential Requirement**

DIGITAL SIGNATURE	CN=SSO
-------------------	--------

**SIGNATURE VERIFICATION SETTINGS** Unanchored Certificate (Primary CN=UCCX-SA1.cisco.com, Secondary Not Configured)

Configure Credentials

Cancel Previous Next **Save**

Configure Credentials(자격 증명 구성)를 클릭합니다.

디지털 서명 설정

License Warning: Approaching expiration date

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/certificate to use from the list below.

SIGNING CERTIFICATE: 02:1E:14:B4 (cn=pingserver.cisco.com) ▼

INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

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

SIGNING ALGORITHM: RSA SHA1 ▼

Manage Certificates

Cancel Next Done Save

SIGNING CERTIFICATE CREATED EARLY(이전에 생성된 서명 인증서)를 선택합니다. 그렇지 않은 경우 Manage Certificates를 클릭하여 인증서를 생성할 수 있습니다.

참고: Cisco Id는 SAML 응답 서명에 대해 RSA SHA256을 지원하지 않으므로 'RSA SHA1'이 사용됩니다.

Next(다음)를 클릭합니다.

서명 확인 설정

License Warning: Approaching expiration date

SP Connection | Credentials

Back-Channel Authentication | Digital Signature Settings | Signature Verification Settings | Summary

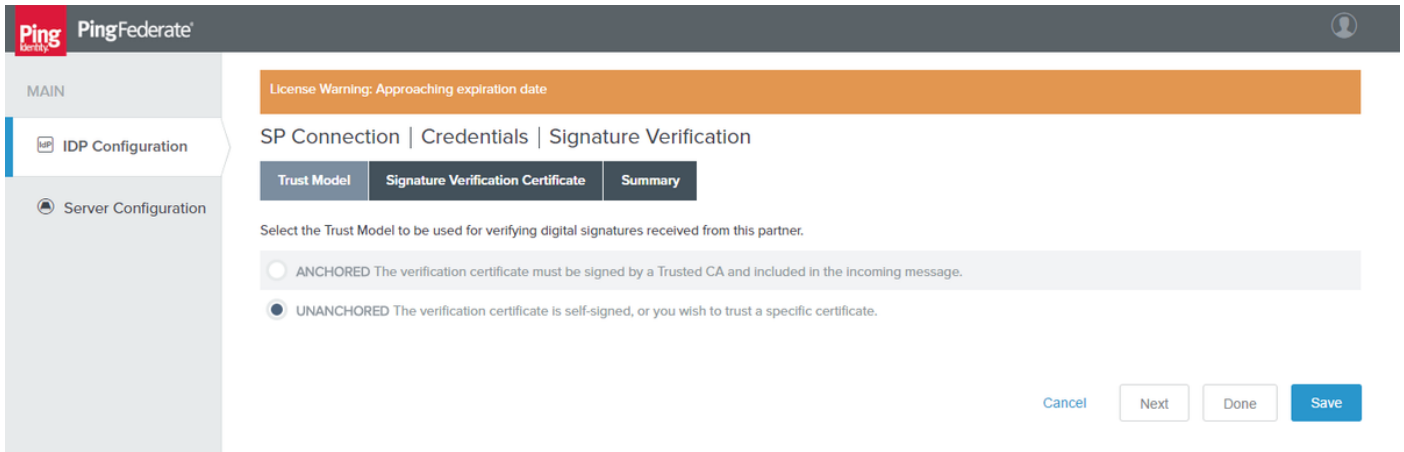
Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.

Manage Signature Verification Settings

Cancel Previous Next Done Save

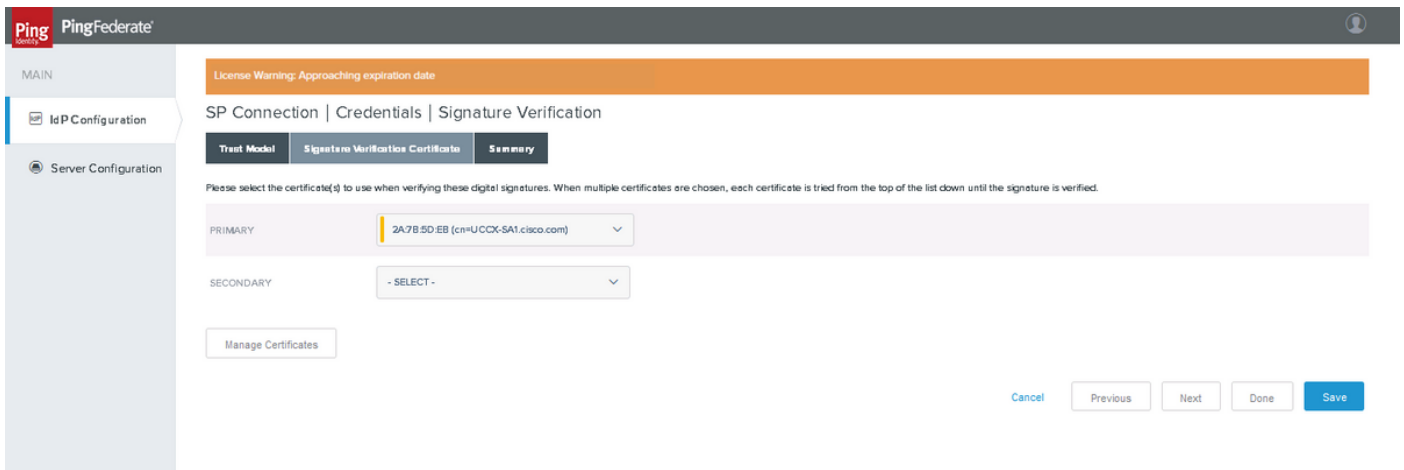
Manage Signature Verification Settings(서명 확인 설정 관리)를 클릭합니다.

신뢰 모델

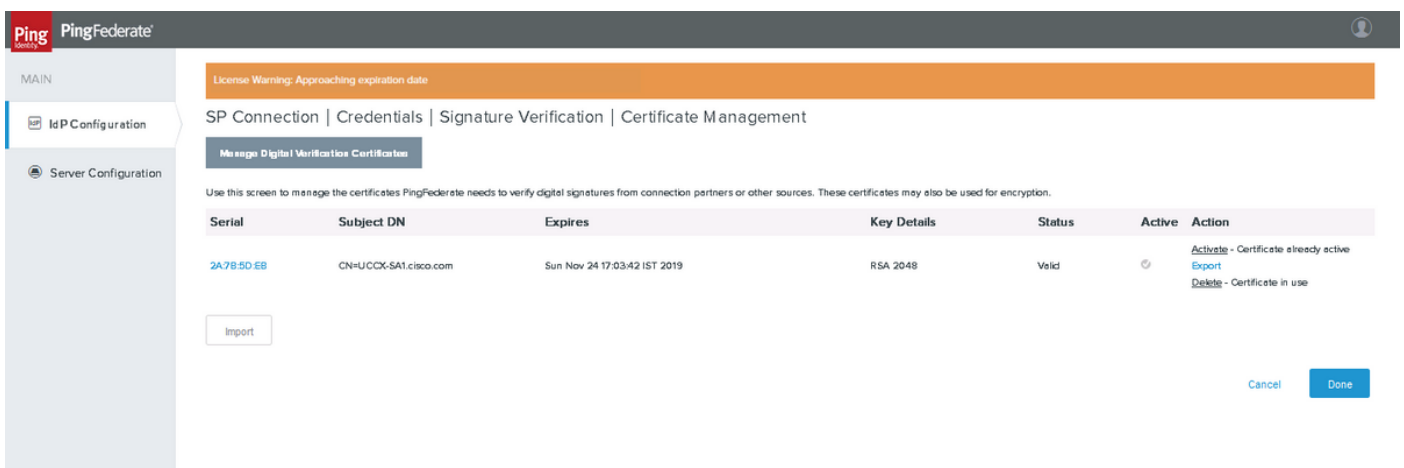


Next(다음)를 클릭합니다.

서명 확인 인증서

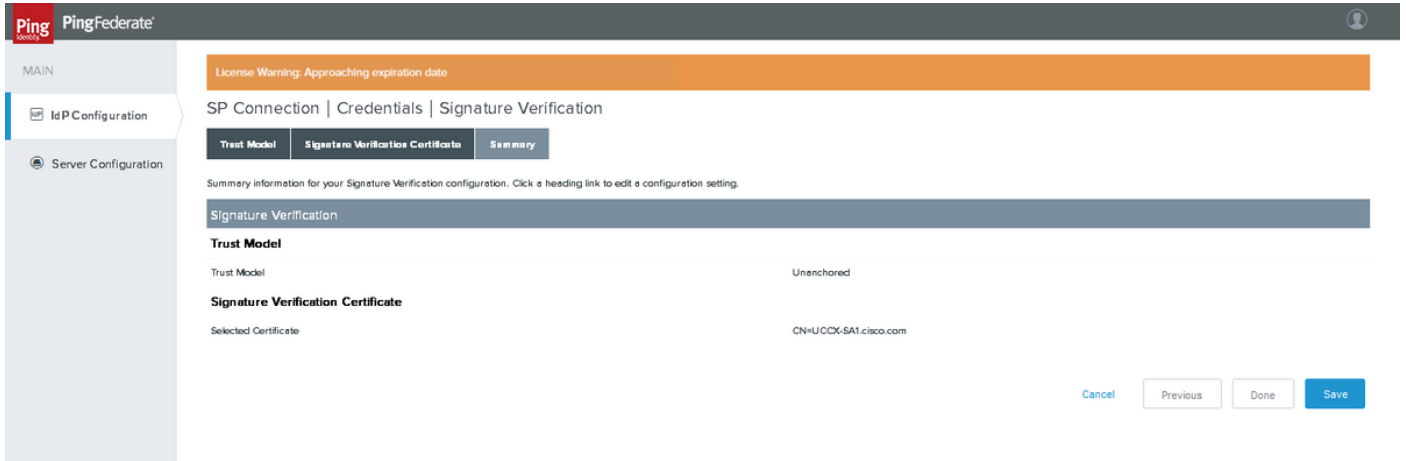


SP에서 인증서를 가져오려면 Manage Certificates를 클릭합니다.



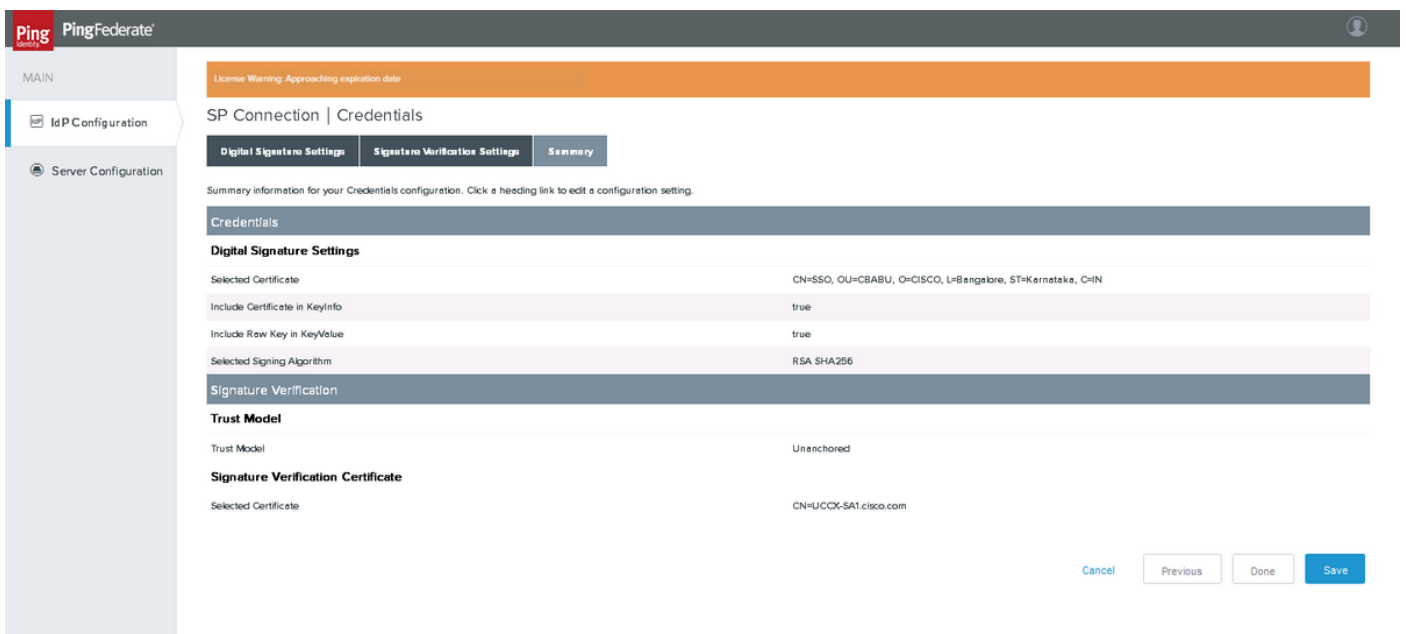
인증서를 가져오려면 Import(가져오기)를 클릭합니다.

요약



Done(완료)을 클릭합니다

요약



요약을 확인하고 Done(완료)을 클릭합니다

활성화 및 요약

MAIN

IdP IdP Configuration

Server Configuration

Copyright © 2003-2016 Ping Identity Corporation

## 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	<input checked="" type="radio"/> ACTIVE <input type="radio"/> INACTIVE
SSO Application Endpoint	https://pingserver.cisco.com:9031/idp/startSSO.ping?PartnerSpId=UCCX-SA1.cisco.com

### Summary

#### SP Connection

#### Connection Type

Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

#### Connection Options

Browser SSO	true
IdP Discovery	false
Attribute Query	false

MAIN

IdP IdP Configuration

Server Configuration

Copyright © 2003-2016 Ping Identity Corporation All rights reserved Version 8.2.2.0

### General Info

Partner's Entity ID (Connection ID)	UCCX-SA1.cisco.com
Base URL	https://UCCX-SA1.cisco.com:8553

### Browser SSO

#### SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	false

#### Assertion Lifetime

Valid Minutes Before	5
Valid Minutes After	5

### Assertion Creation

#### Identity Mapping

Enable Transient Identifier	true
Include additional attributes	false

#### Authentication Source Mapping

Adapter instance name	HTML Form IdP Adapter 1
-----------------------	-------------------------

#### Adapter Instance

Selected adapter	HTML Form IdP Adapter 1
------------------	-------------------------

MAIN

IdP IdP Configuration

Server Configuration

Copyright © 2003-2016

**Mapping Method**

Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping

**Attribute Contract Fulfillment**

**Issuance Criteria**

Criterion	(None)
-----------	--------

**Protocol Settings**

**Assertion Consumer Service URL**

Endpoint	URL: /ids/saml/response (POST)
----------	--------------------------------

**Allowable SAML Bindings**

Artifact	false
POST	true
Redirect	true
SOAP	false

**Signature Policy**

Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false

**Encryption Policy**

Status	Inactive
--------	----------

**Credentials**

**Digital Signature Settings**

Selected Certificate	CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	true
Selected Signing Algorithm	RSA SHA1

**Signature Verification**

**Trust Model**

Trust Model	Unanchored
-------------	------------

**Signature Verification Certificate**

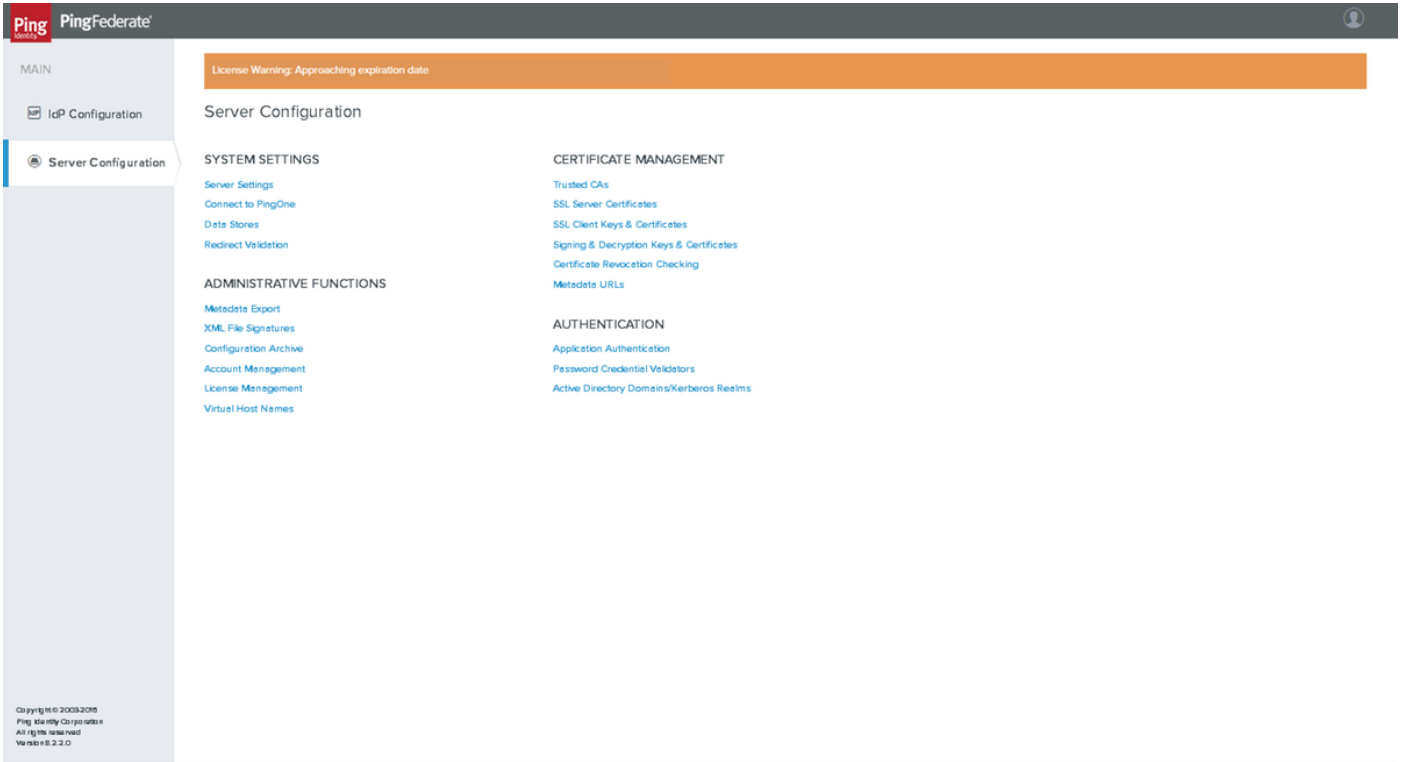
Selected Certificate	CN=UCCX-SA1.cisco.com
----------------------	-----------------------

Cancel Previous Save

요약을 확인하고 저장을 클릭합니다.

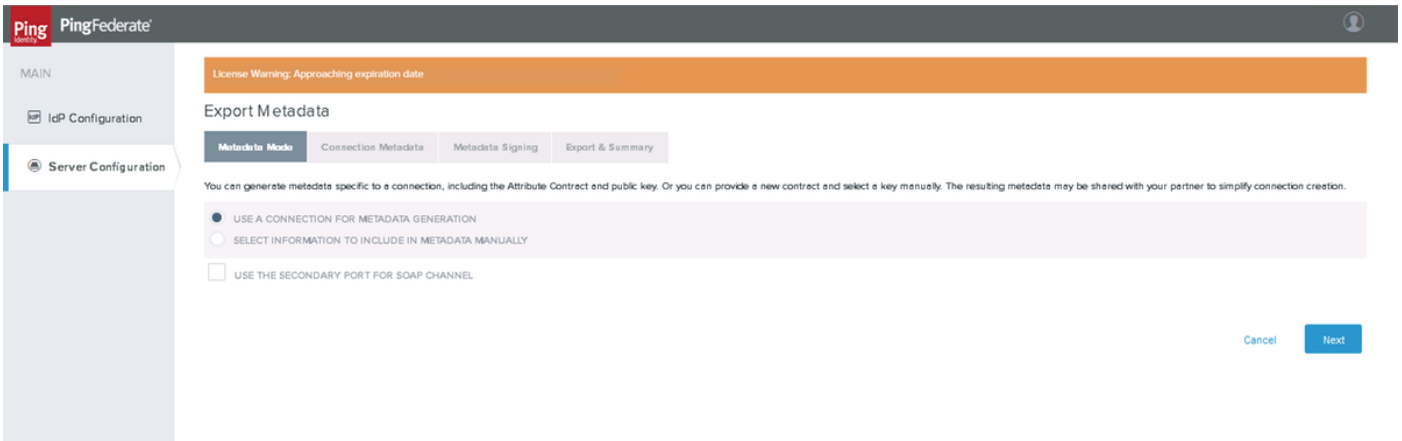
## PingFederate 메타데이터 내보내기

### 메타데이터 내보내기



## 메타데이터 모드

Server Configuration(서버 컨피그레이션) > ADMINISTRATIVE FUNCTIONS(관리 기능) > Metadata Export(메타데이터 내보내기)를 클릭합니다



Next(다음)를 클릭합니다.

## 연결 메타데이터

## Export Metadata

Metadata Mode | **Connection Metadata** | Metadata Signing | Export & Summary

Select a connection that contains the Attribute Contract and Digital Signature Key you wish to include in the metadata.

UCCX-SA1.cisco.com

**Attribute Contract**

SAML\_AUTHN\_CTX

SAML\_NAME\_FORMAT

uid

user\_principal

**DIGITAL SIGNATURE KEY**  
CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN

**XML ENCRYPTION KEY**  
No XML key available for this connection

Cancel Previous **Next**

생성한 SP 접속을 선택하고 Next(다음)를 클릭합니다.

## 메타데이터 서명

PingFederate

License Warning: Approaching expiration date

**Export Metadata**

Metadata Mode | **Connection Metadata** | Metadata Signing | Export & Summary

From this list of certificates, choose which one to use for signing the selected file.

SIGNING CERTIFICATE: 01584CA89AF6 (cn=SSO)

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

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

SIGNING ALGORITHM: RSA SHA256

Manage Certificates

Cancel Previous **Next**

생성한 메타데이터 인증서 및 서명 알고리즘을 RSA SHA256으로 선택합니다. 다음을 누릅니다.

## 내보내기 및 요약

**Export Metadata**

Click the Export button to export this metadata to the file system.

Metadata Mode	Connection Metadata	Metadata Signing	Export & Summary
Metadata mode		Use connection	
Use the secondary port for SOAP channel		false	
<b>Connection Metadata</b>			
Selected connection		UCCX-SA1.cisco.com	
Attribute		uid	
Attribute		SAML_AUTHN_CTX	
Attribute		user_principal	
Attribute		SAML_NAME_FORMAT	
Digital Signature Key		CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN	
<b>Metadata Signing</b>			
Signing Certificate		CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN	
Include Certificate in KeyInfo		true	
Include Raw Key in KeyValue		true	
Selected Signing Algorithm		RSA SHA256	

Export

Export(내보내기)를 클릭하고 로컬 시스템에 파일을 저장합니다.

- 다운로드한 메타데이터 XML 파일을 편집하여 'md' 네임스페이스 항목을 제거하고 저장합니다
- 그런 다음 저장된 메타데이터 파일을 idsadmin 페이지의 Id에 업로드하여 IDP 트러스트를 설정합니다

### 샘플 메타데이터

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<md:Metadata xmlns:md="urn:mace:org:pingfederate:1.0:md" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:mace:org:pingfederate:1.0:md md-metadata.xsd">
  <md:MetadataItem md:Name="SAML2-Assertion" md:Type="SAML2-Assertion" md:Value="<SAMLAssertion xmlns='urn:oasis:names:tc:SAML:2.0:assertion'>
    <Header>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-1 />
      <ID urn:oasis:names:tc:SAML:2.0:id-1 />
    </Header>
    <Subject>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-2 />
      <ID urn:oasis:names:tc:SAML:2.0:id-2 />
      <NameID urn:oasis:names:tc:SAML:2.0:nameid-format:emailAddress />
      <Principal urn:oasis:names:tc:SAML:2.0:principal-name:uid />
    </Subject>
    <Conditions>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-3 />
      <ID urn:oasis:names:tc:SAML:2.0:id-3 />
      <NotBefore>2016-01-01T00:00:00.000Z</NotBefore>
      <NotOnOrAfter>2016-01-01T00:00:00.000Z</NotOnOrAfter>
    </Conditions>
    <AuthnContext>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-4 />
      <ID urn:oasis:names:tc:SAML:2.0:id-4 />
      <AuthnContextClassRef urn:mace:org:pingfederate:1.0:authn-context-class-ref:uid />
    </AuthnContext>
    <Signature xmlns='http://www.w3.org/2000_09#sig-block'>
      <KeyInfo>
        <X509Data>
          <X509Certificate>
            <X509Certificate />
          </X509Certificate>
        </X509Data>
      </KeyInfo>
      <SignatureValue />
    </Signature>
  </SAMLAssertion>
  </md:MetadataItem>
  <md:MetadataItem md:Name="SAML2-Response" md:Type="SAML2-Response" md:Value="<SAMLResponse xmlns='urn:oasis:names:tc:SAML:2.0:protocol'>
    <Header>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-1 />
      <ID urn:oasis:names:tc:SAML:2.0:id-1 />
    </Header>
    <Status>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-2 />
      <ID urn:oasis:names:tc:SAML:2.0:id-2 />
      <StatusCode value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </Status>
    <AssertionConsumerServiceIndex>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-3 />
      <ID urn:oasis:names:tc:SAML:2.0:id-3 />
      <Index>1</Index>
    </AssertionConsumerServiceIndex>
    <AssertionConsumerServiceURL>
      <BaseID urn:oasis:names:tc:SAML:2.0:base-id-4 />
      <ID urn:oasis:names:tc:SAML:2.0:id-4 />
      <URL>https://pingfederate.cisco.com:9021/saml2 />
    </AssertionConsumerServiceURL>
    <Signature xmlns='http://www.w3.org/2000_09#sig-block'>
      <KeyInfo>
        <X509Data>
          <X509Certificate>
            <X509Certificate />
          </X509Certificate>
        </X509Data>
      </KeyInfo>
      <SignatureValue />
    </Signature>
  </SAMLResponse>
  </md:MetadataItem>
</md:Metadata>
```

### 문제 해결

문제	가능한 원인		
Id 관리 페이지에서 PingFederate 메타데이터 업로드가 실패함	<table border="1"> <tr> <td>텍스트 파일 편집기</td> <td>메타데이터 XML 파일에 'md' 네임스페이스 항목이 없는지 확인하십시오.</td> </tr> </table>	텍스트 파일 편집기	메타데이터 XML 파일에 'md' 네임스페이스 항목이 없는지 확인하십시오.
텍스트 파일 편집기	메타데이터 XML 파일에 'md' 네임스페이스 항목이 없는지 확인하십시오.		

문제	틀	가능한 원인
SAML 흐름 실패	SAML 트래이서	'StatusCode'가 'Success'를 나타내는지 확인(예: <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />  <ul style="list-style-type: none"> <li>그렇지 않은 경우 'Requester' 또는 'Responder'를 나타내는지 확인합니다. <ul style="list-style-type: none"> <li>'요청자'는 SAML 요청에 문제가 있음을 의미합니다(예: Cisco Id가 요청을 제대로 전송하지 않음). /opt/cisco/ids/log/ 폴더 아래의 Cisco IdS 로그를 확인하십시오.</li> <li>'Responder'는 IdP 문제를 의미하므로 PingFederate 로그를 확인하십시오.</li> </ul> </li> </ul>
SAML 흐름 실패	SAML 트래이서	<saml:AuthnContextClassRef> 요소를 확인합니다. 해당 값은 urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport여야 합니다.  값이 urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified로 설정된 경우 - SAML_AUTHN_CTXcontract가 제대로 구성되고 매핑되었는지 확인합니다.
SAML 흐름 실패	SAML 트래이서	<saml:AttributeStatement> 요소를 확인합니다. 요소가 있어야 하며 'uid' 및 'user_principal'에 해당하는 자식 요소를 포함해야 합니다.  찾을 수 없는 경우 'Assertion Creation'(어설션 생성) 설정과 'Contract Fulfillment'(계약 이행) 설정을 확인하여 계약 특성이 올바르게 정의되었는지 확인합니다.
SAML 흐름 실패	SAML 트래이서	Cisco Id 또는 PingFederate 로그에서 'Invalid Signature' 메시지를 확인합니다.  확인된 경우 Id 및 PingFederate 전체에서 메타데이터 트러스트를 다시 설정합니다.
SAML 흐름 실패	SAML 트래이서	시간 조건을 확인하십시오. Cisco Id가 SAML 응답을 받은 시간은 <saml:Conditions NotBefore="2016-12-18T07:24:10.191Z" NotOnOrAfter="2016-12-18T07:34:10.191">에 명시된 시간 사이여야 합니다.

## SSO에 대한 추가 구성:

이 문서에서는 SSO가 Cisco Identity Service와 통합되도록 IdP 측면에서 구성하는 방법을 설명합니다. 자세한 내용은 개별 제품 컨피그레이션 가이드를 참조하십시오.

- [UCCX](#)

- [UCCE](#)
- [PCCE](#)

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.