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

목차

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)	최
• Microsoft Windows Server 2008 R2 SP(서비스 팩) • Microsoft Windows Server 2012 표준 • Microsoft Windows Server 2012 R2 Datacenter • Oracle Enterprise Linux 6.5(Red Hat 호환 커널) • Oracle Solaris 10 • Red Hat Enterprise Linux ES 6.6 • Red Hat Enterprise Linux ES 7.0	• Oracle Java SE Runtime Environment(서버 JRE) 7 업데이트 79(64비트) • Oracle Java SE Runtime Environment(서버 JRE) 8 업데이트 45(64비트)	• 크롬 • 파이어폭스 • Internet Explorer(버전 9 이상) • 사파리	• 크롬 • 파이어폭스 • Internet Explorer(버전 9 이상)	• Microsoft Active Directory(2008 R2 및 2012) • Oracle Directory Server Enterprise Edition 11g • Microsoft SQL(구조적 쿼리 언어) 서버(2012 및 2014) • Oracle 데이터베이스(10g 및 11g R2) • Oracle MySQL 5.6	

• SUSE Linux Enterprise 11 SP 3					

Install

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

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

배포 ZIP 파일로 PingFederate 설치

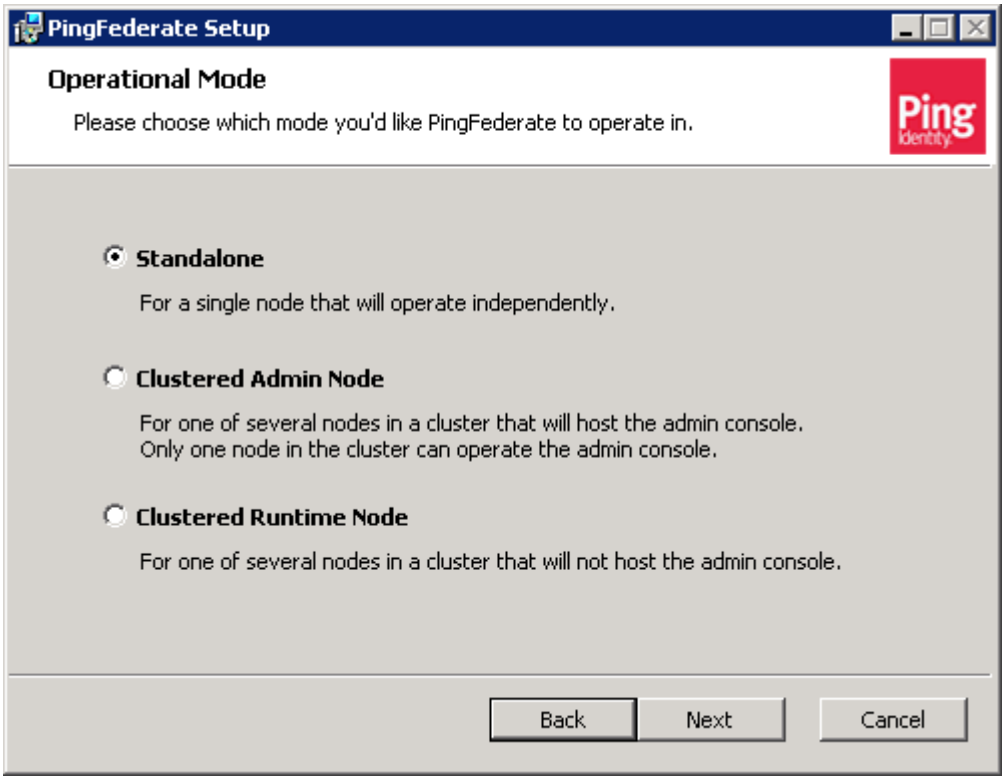
배포 ZIP 파일을 설치 디렉토리로 추출합니다.

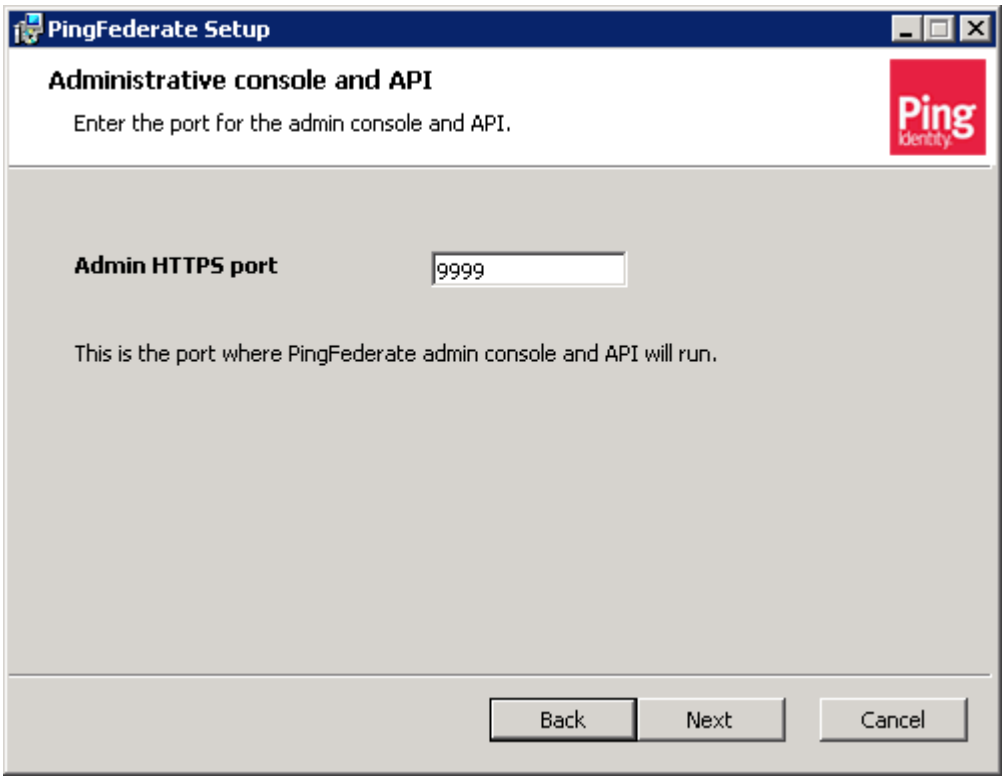
경고: 자동화된 업그레이드로 인해 발생할 수 있는 문제를 방지하려면 설치된 pingFederate 폴더의 이름을 변경하지 마십시오. 동일한 시스템에 PingFederate의 여러 인스턴스를 설치하는 경우(예: 특정 서버 클러스터링 시나리오), 각 인스턴스를 다른 위치에 설치하거나 상위 폴더의 이름을 변경하여 동일한 위치에 병렬 파일 구조를 설치합니다.

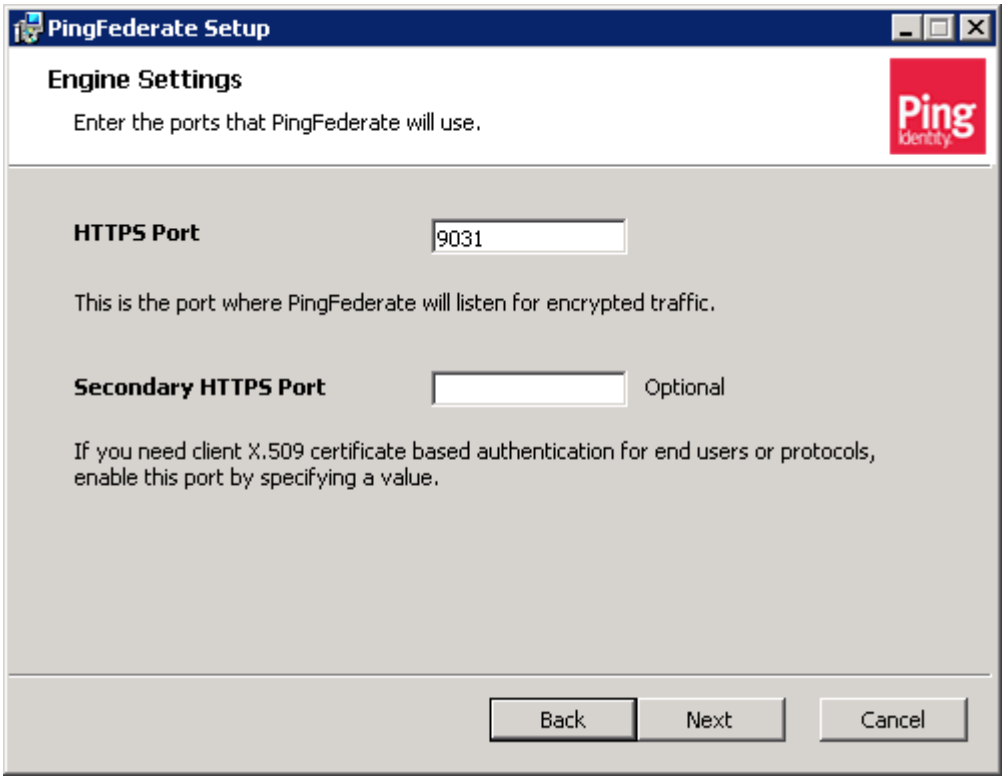
배포 EXE 파일로 PingFederate 설치

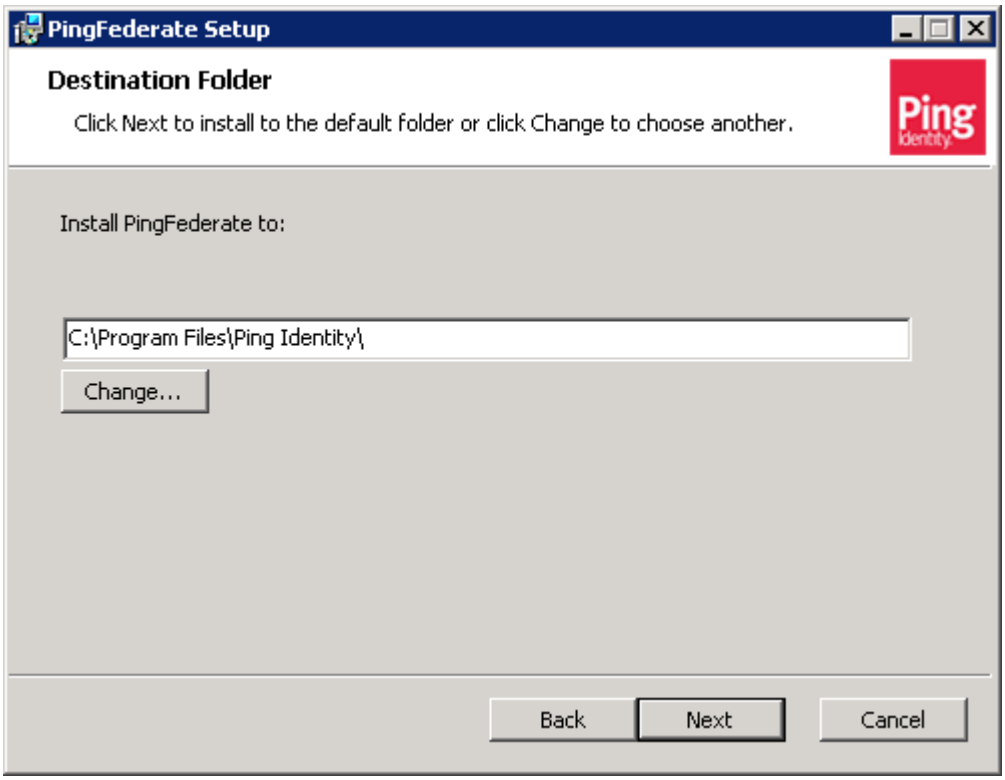
exe 파일을 두 번 클릭하고 설치 단계를 수행합니다

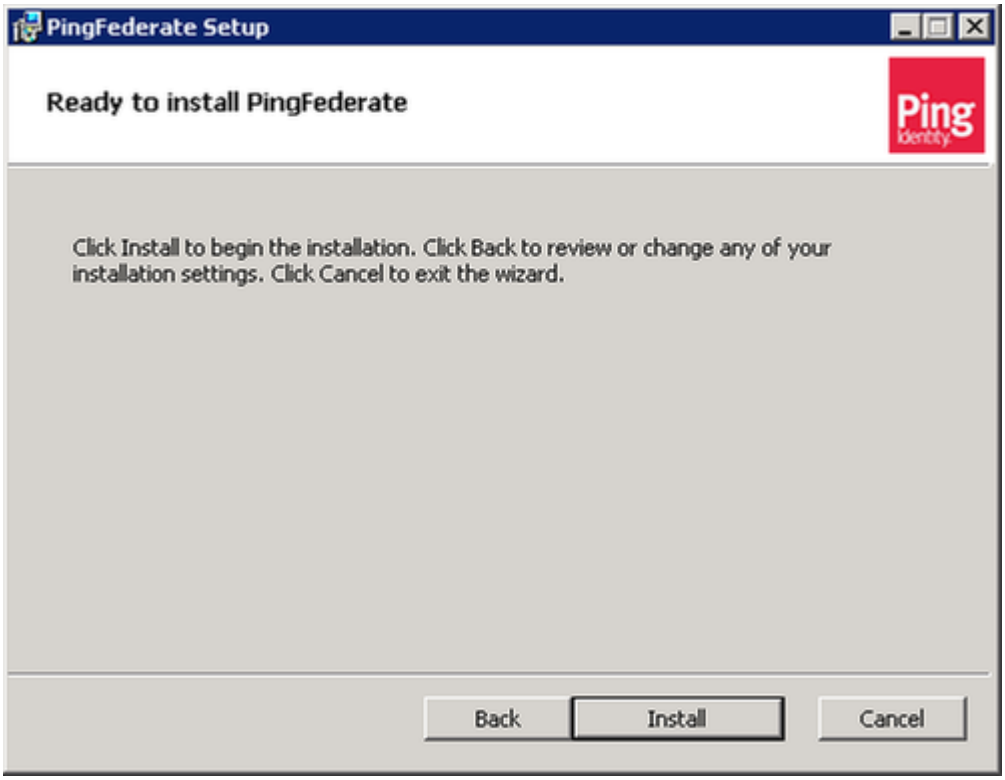

PingFederate Setup
Welcome to the PingFederate Setup Wizard
The Setup Wizard will install PingFederate on your computer.
Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

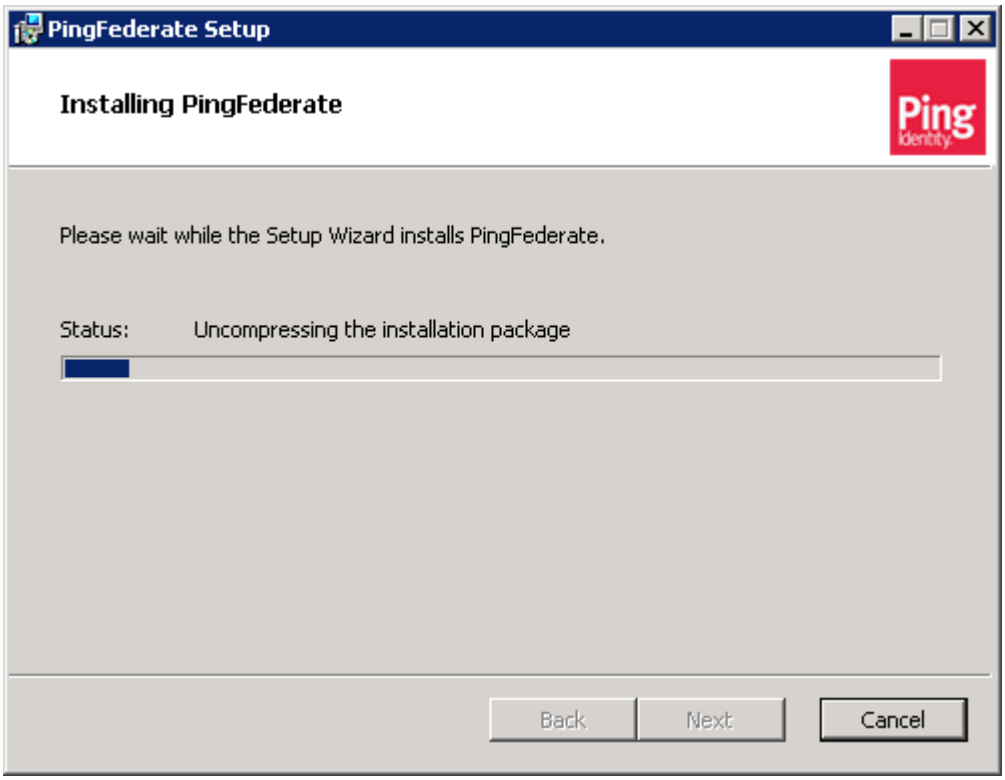

PingFederate Setup
Operational Mode
Please choose which mode you'd like PingFederate to operate in.
Standalone
For a single node that will operate independently.
Clustered Admin Node
For one of several nodes in a cluster that will host the admin console.
Only one node in the cluster can operate the admin console.
Clustered Runtime Node
For one of several nodes in a cluster that will not host the admin console.
Back
Next
Cancel

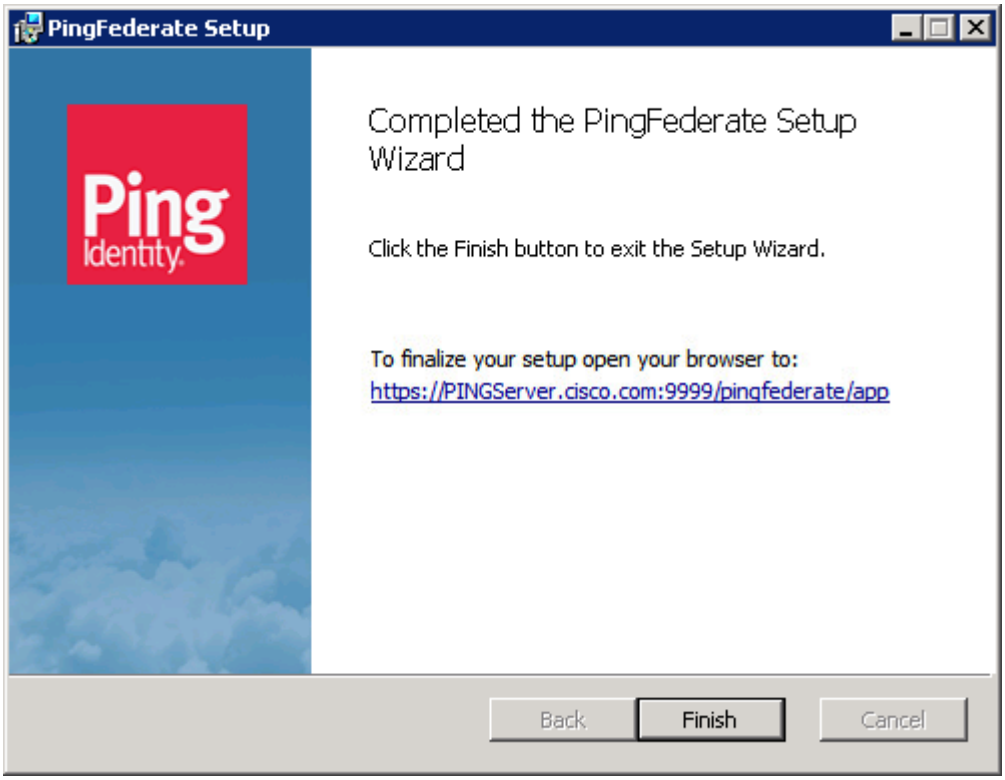

PingFederate Setup
Administrative console and API
Enter the port for the admin console and API.
Ping identity
Admin HTTPS port
9999
This is the port where PingFederate admin console and API will run.
Back
Next
Cancel


PingFederate Setup
Engine Settings
Enter the ports that PingFederate will use.
Ping identity
HTTPS Port
9031
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.
Back
Next
Cancel


PingFederate Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Ping identity
Install PingFederate to:
C:\Program Files\Ping Identity\
Change...
Back
Next
Cancel


PingFederate Setup
Ready to install PingFederate
Ping identity
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel





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

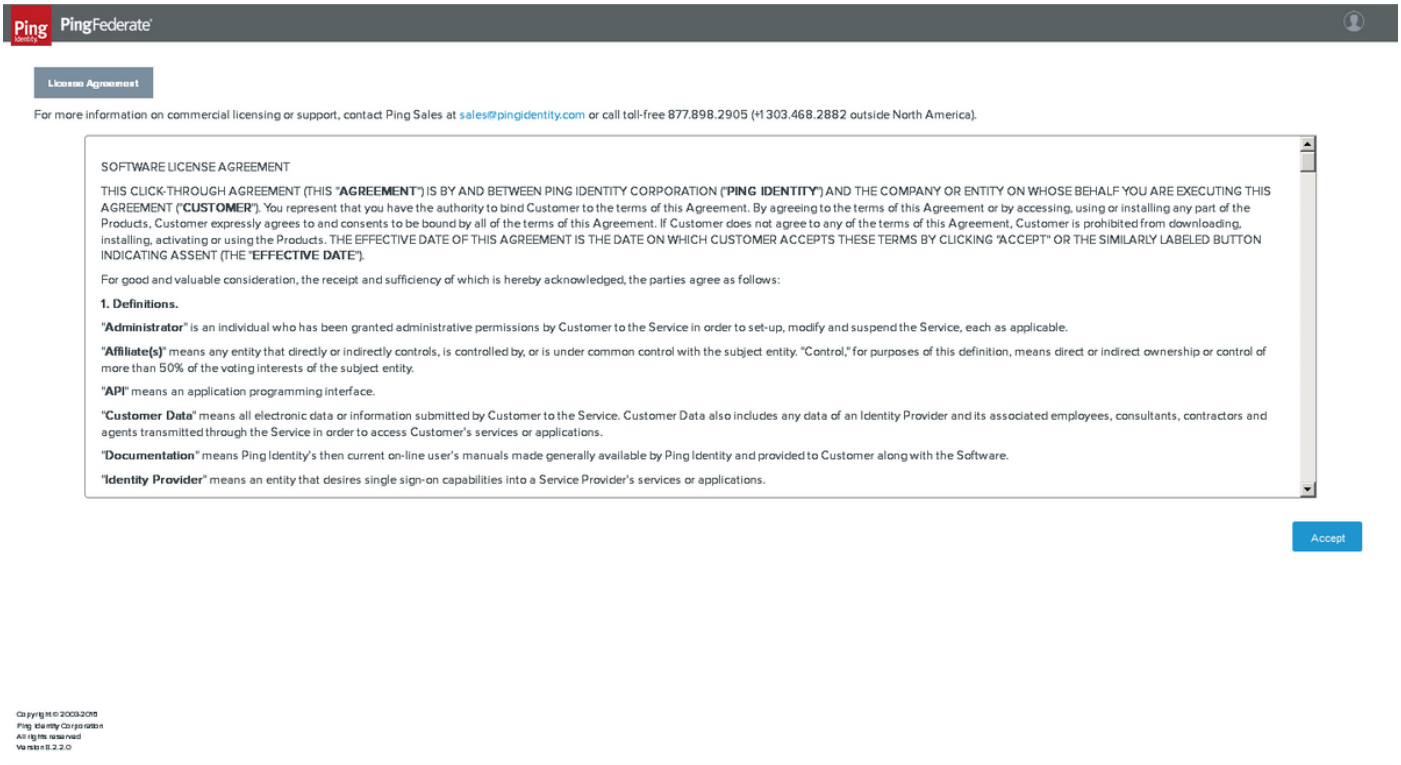
PingFederate 관리자의 사용자 인터페이스인 관리 콘솔은 마법사와 같은 제어 화면 시스템을 기반으로 합니다. PingFederate 관리 콘솔을 시작하고 초기 설정 마법사를 사용하여 ID 페더레이션 설정의 컨피그레이션을 완료합니다. 또한 PingFederate를 PingOne에 연결하여 강력한 온프레미스 및 클라우드 기반 하이브리드 솔루션을 구축할 수 있습니다.

관리 콘솔에 액세스하려면

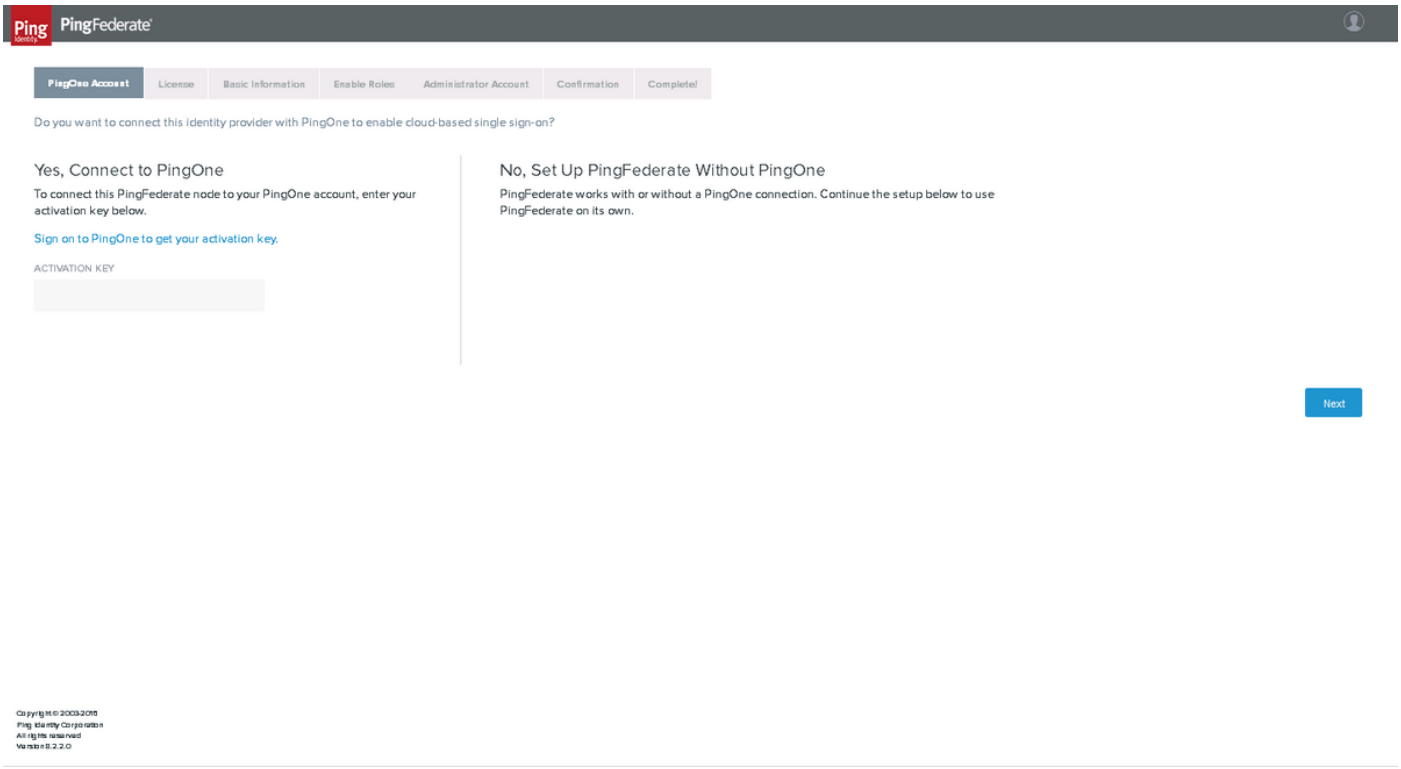
브라우저를 시작하고 https:// <FQHN>:9999/pingfederate/app(<FQHN>은 PingFederate가 설치된 서버의 정규화된 호스트 이름)으로 이동합니다.

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

라이센스 계약 동의



PingOne 계정

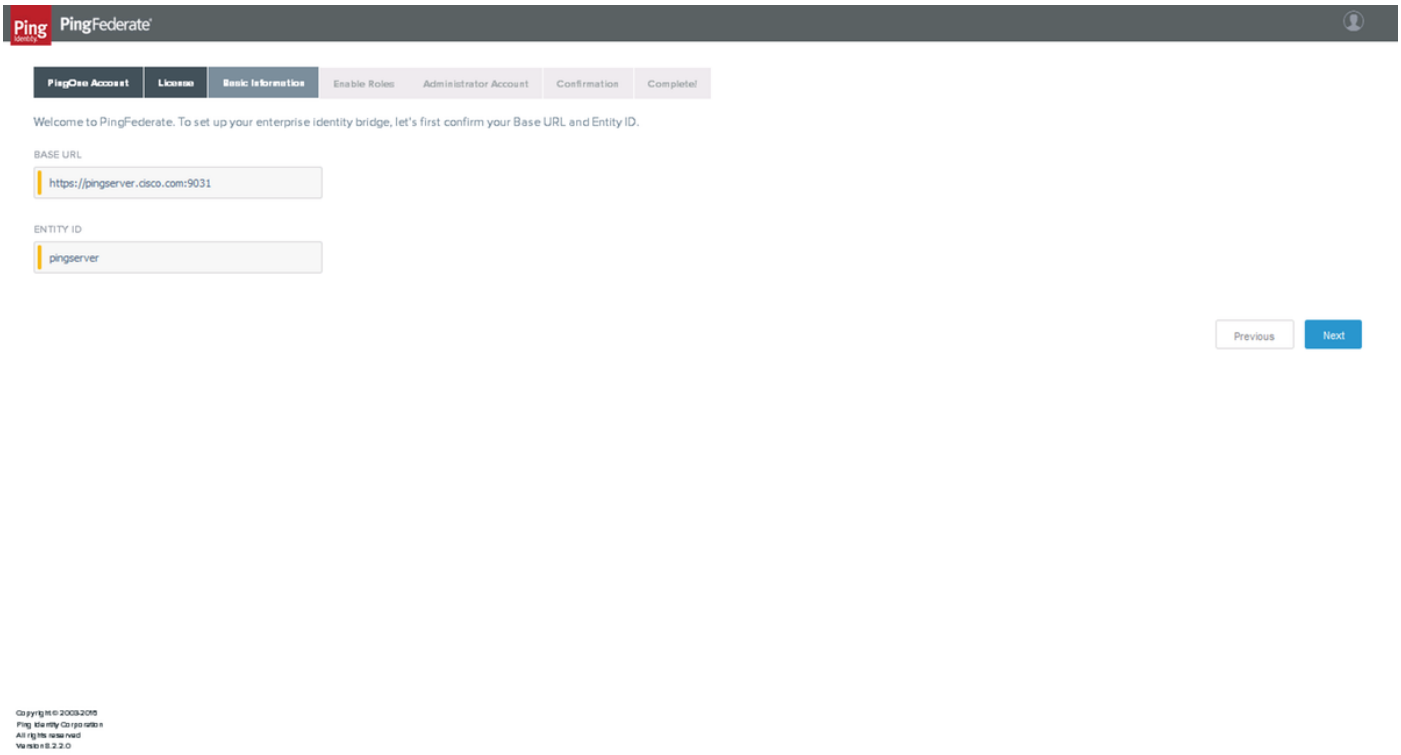


Next(다음)를 클릭합니다.

라이선스

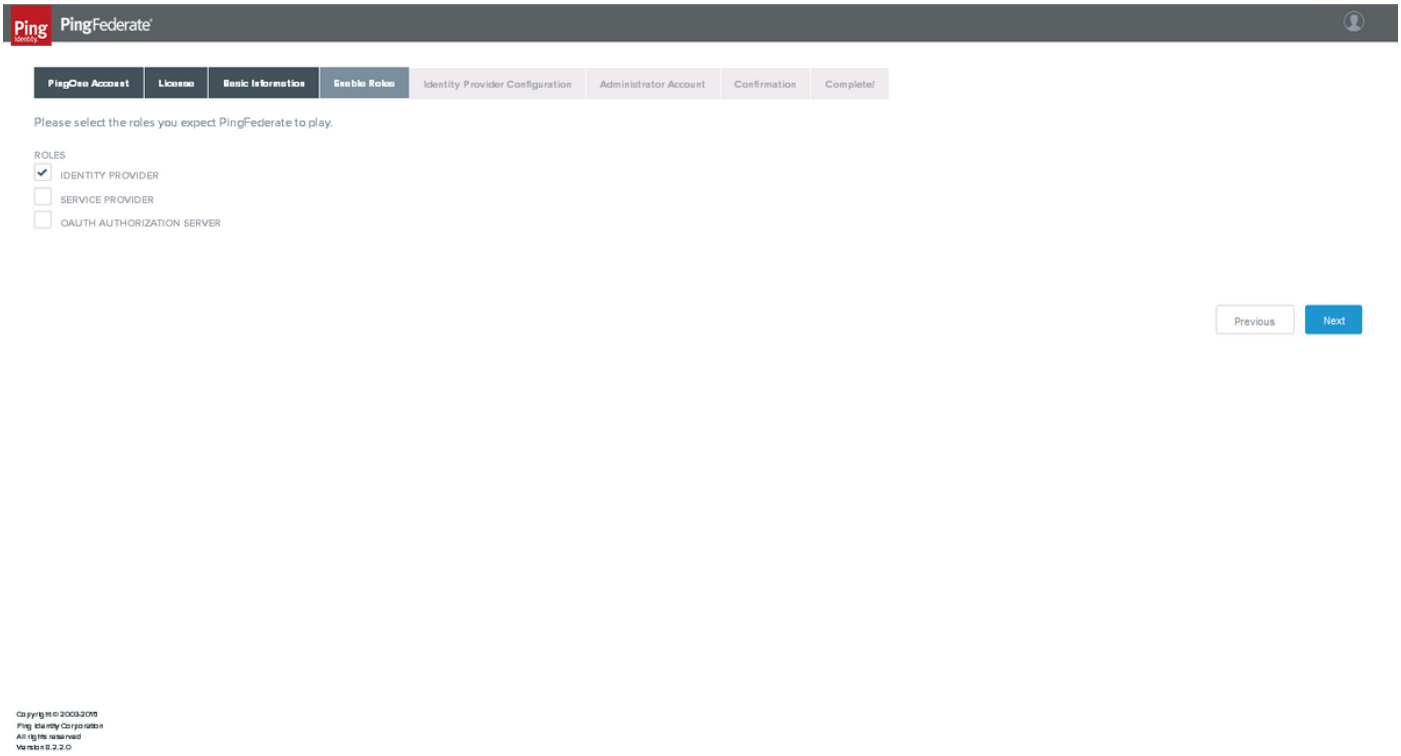
pingidentity.com에서 개발 라이센스를 구매하거나 요청해야 합니다. 라이센스 파일을 업로드하고 Next(다음)를 클릭합니다.

기본 정보



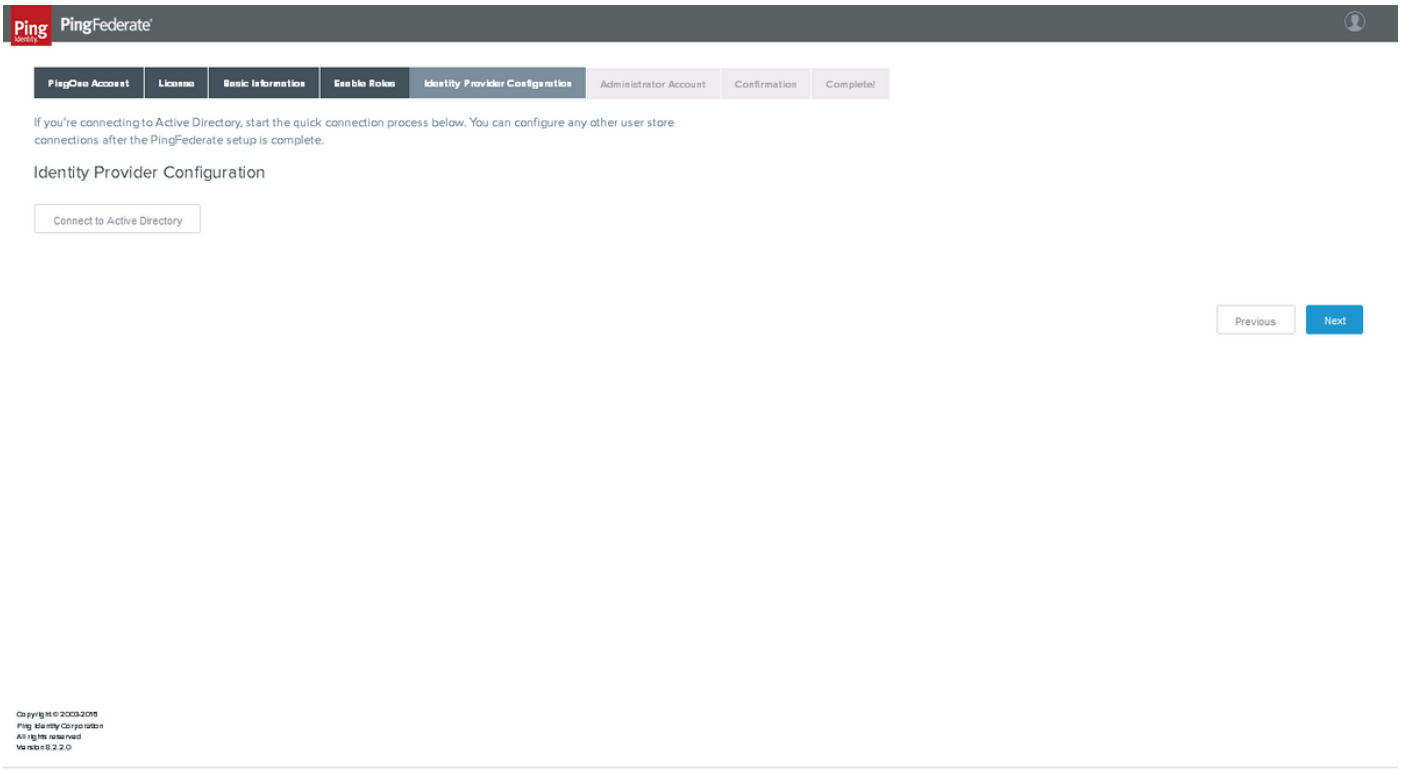
기본 URL 및 엔티티 ID를 설정하고 다음을 클릭합니다.

역할 활성화



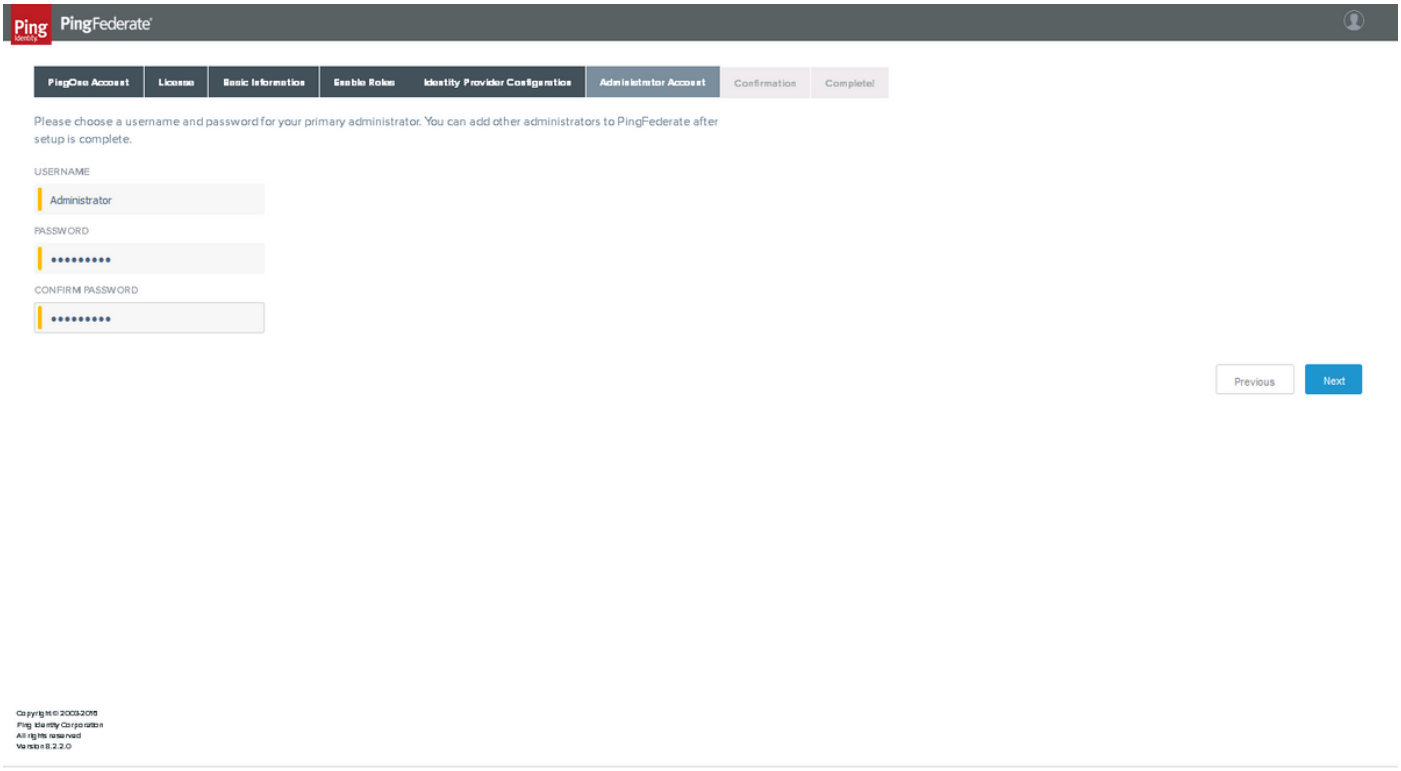
ID 공급자를 선택하고 다음을 클릭합니다.

ID 공급자 컨피그레이션



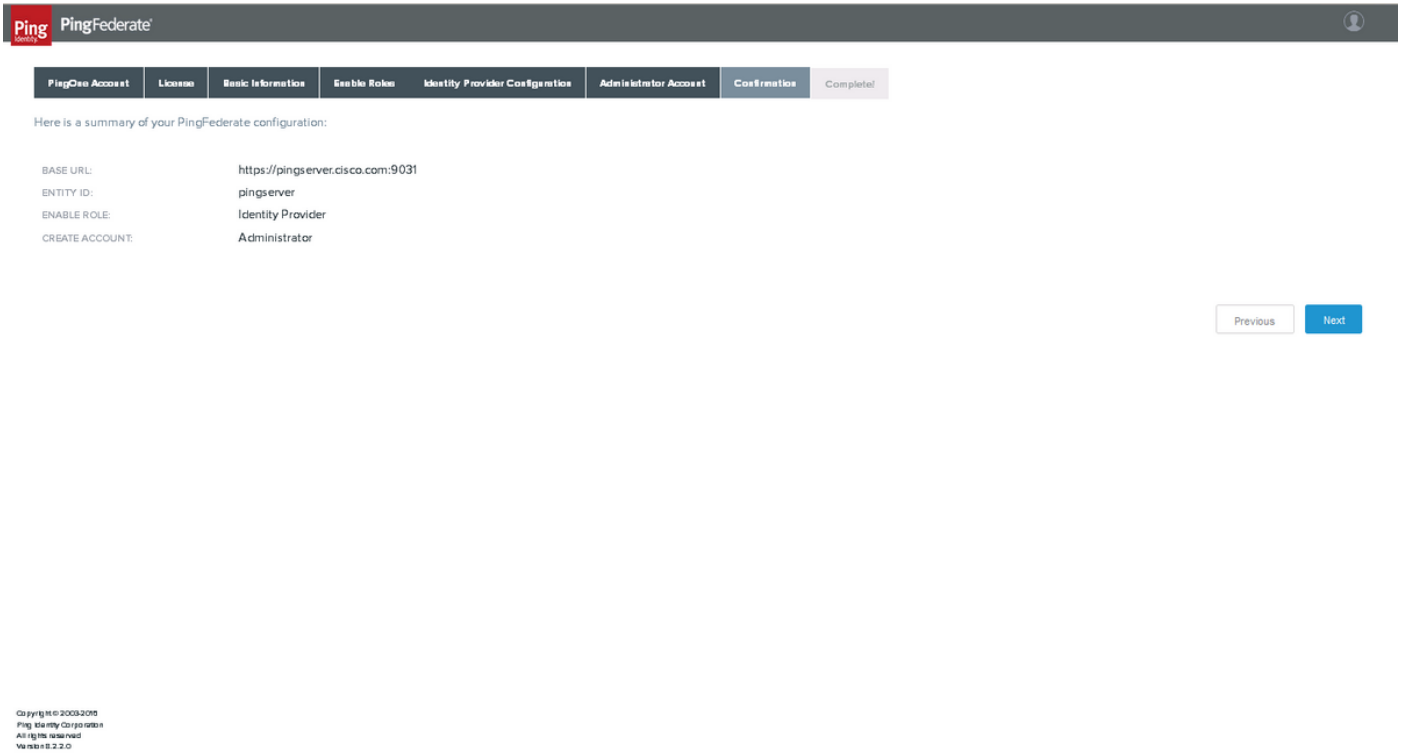
Active Directory에 대한 연결은 나중에 수행할 수 있습니다. 다음 을 클릭합니다.

관리자 계정



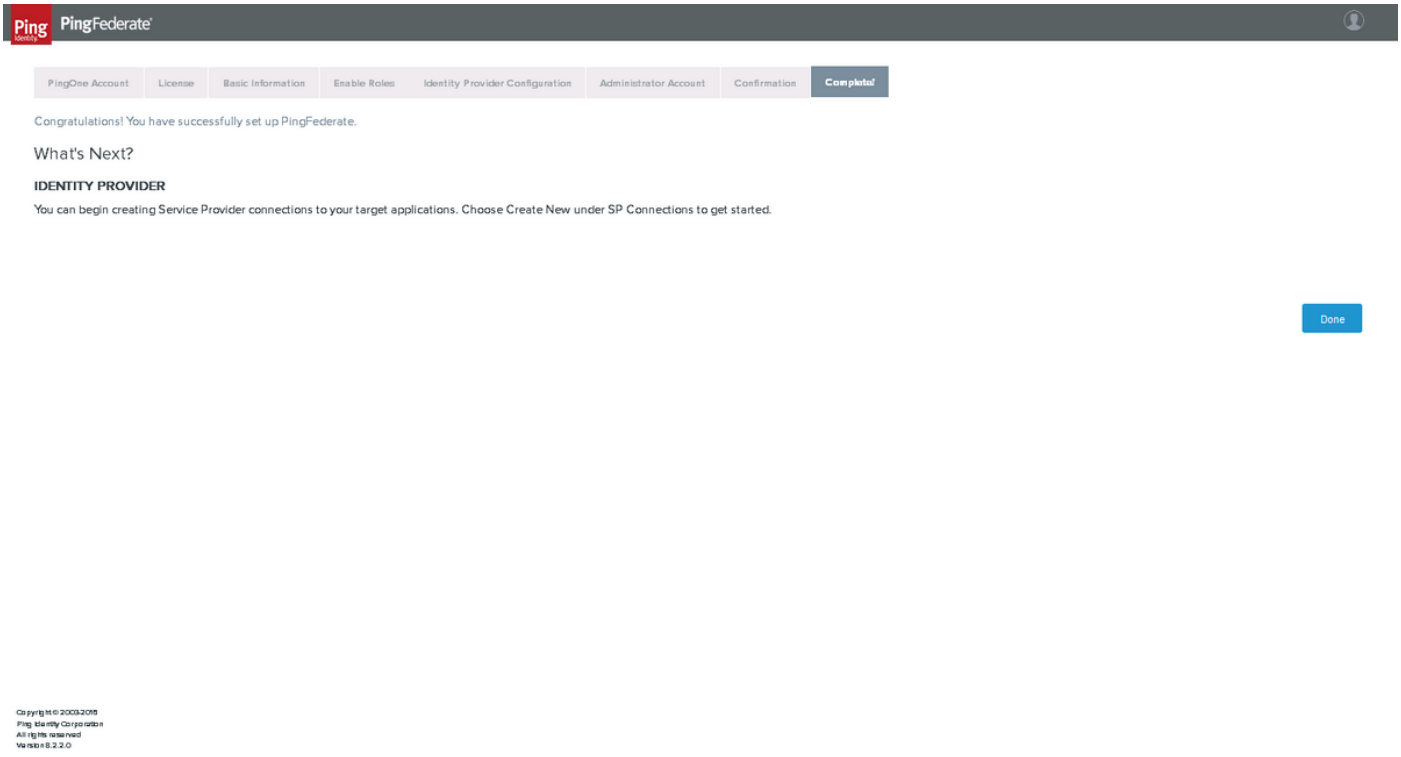
관리자의 암호를 설정하고 다음을 클릭합니다.

확인



확인하고 Next(다음)를 클릭합니다.

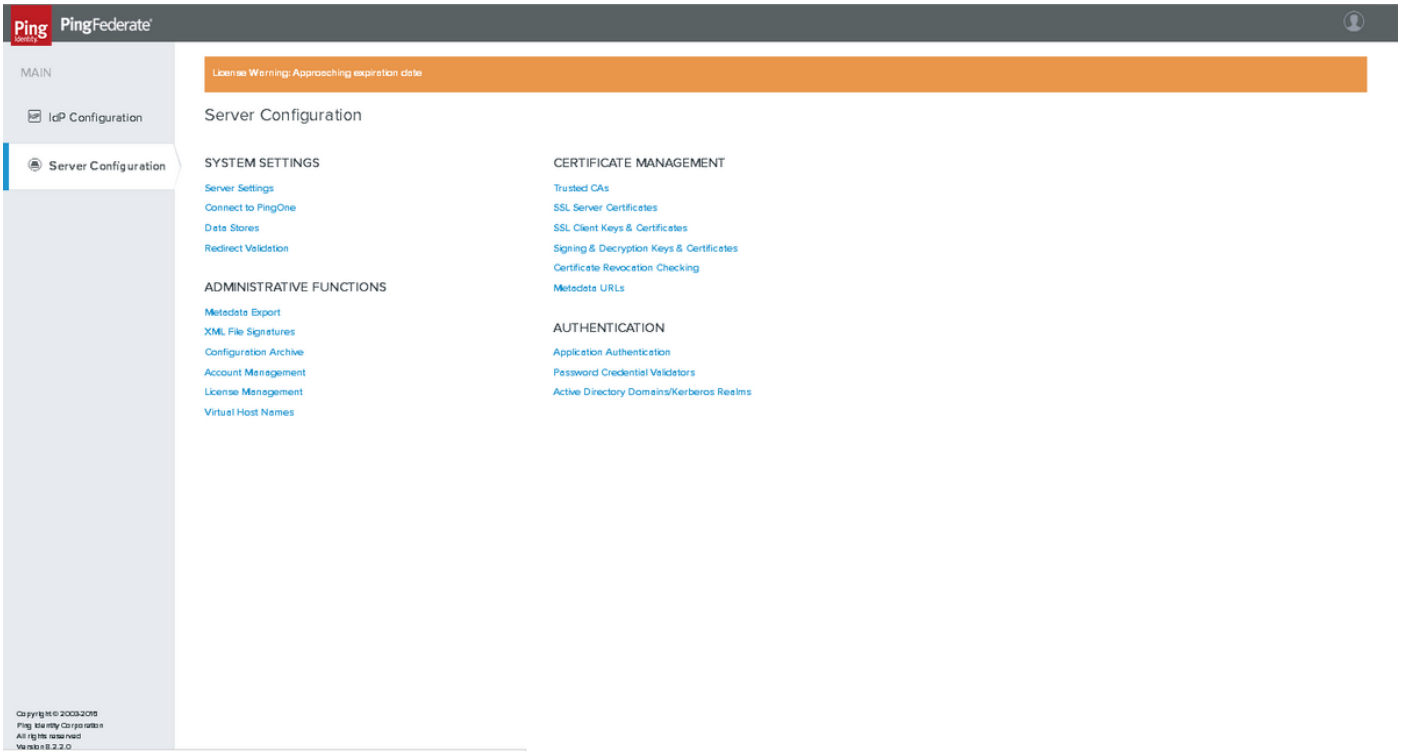
완료



Done(완료)을 클릭합니다

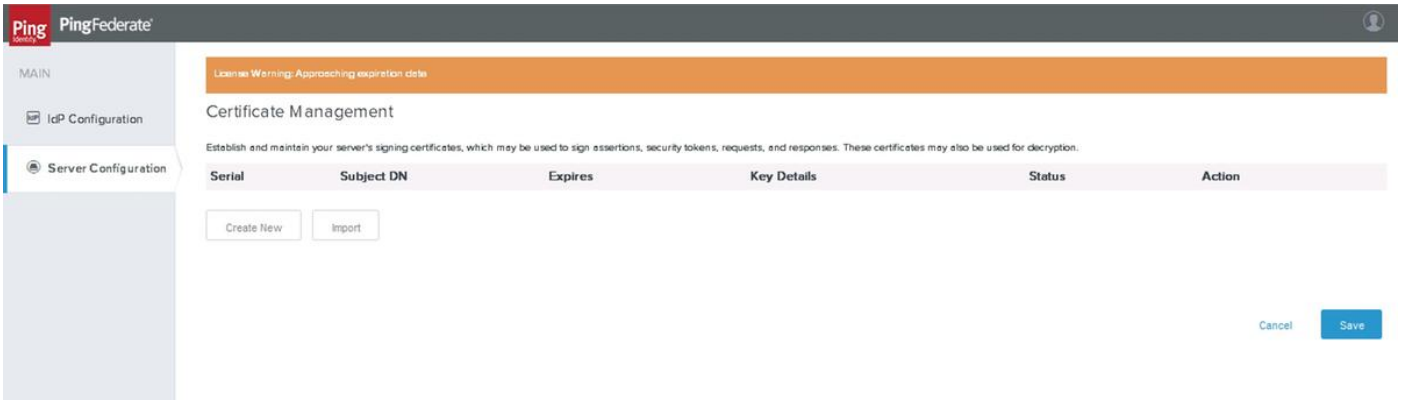
PingFederate 구성

서버 컨피그레이션



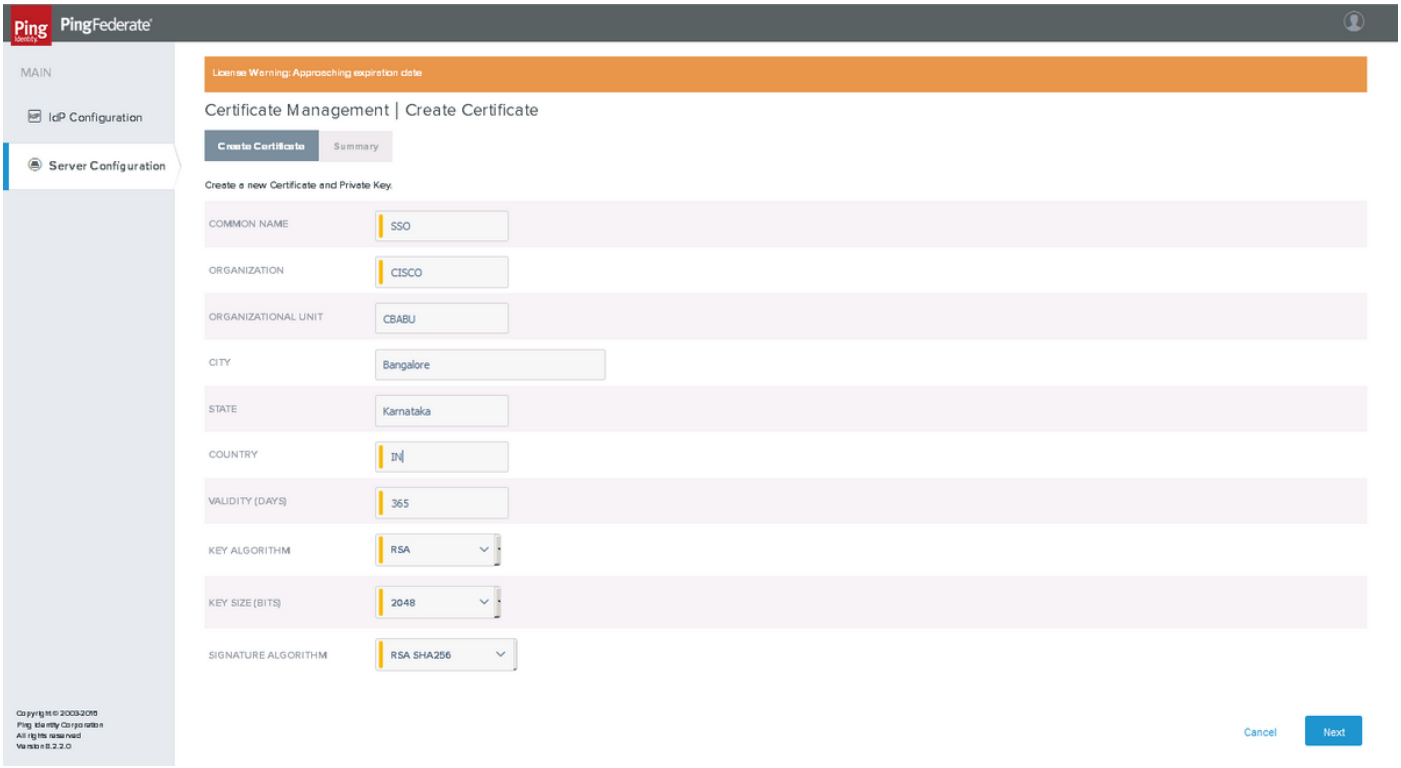
디지털 서명 및 XML(Extensible Markup Language) 암호 해독 키 및 인증서

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



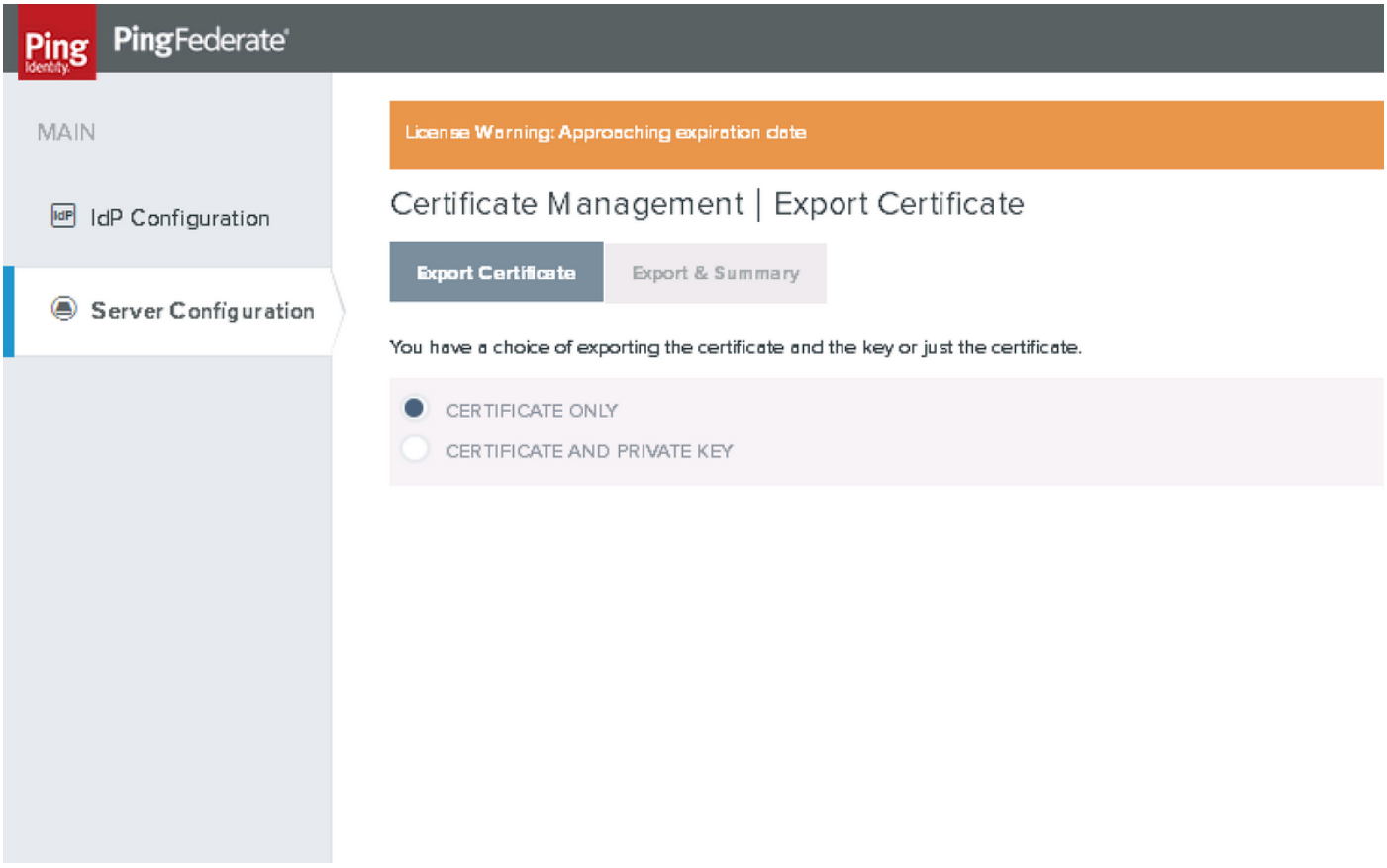
Create New(새로 만들기)를 클릭합니다.

인증서 생성

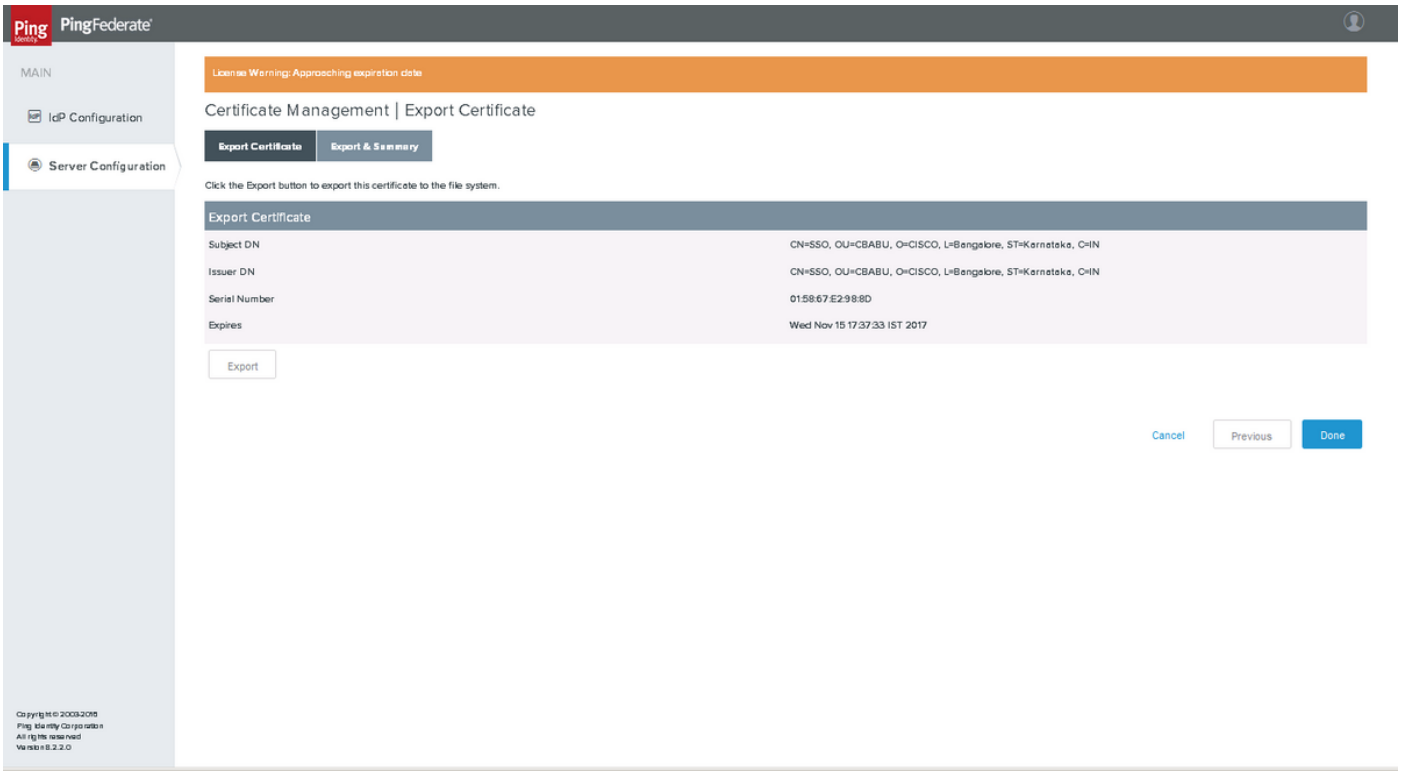


Next(다음)를 클릭합니다.

인증서 내보내기



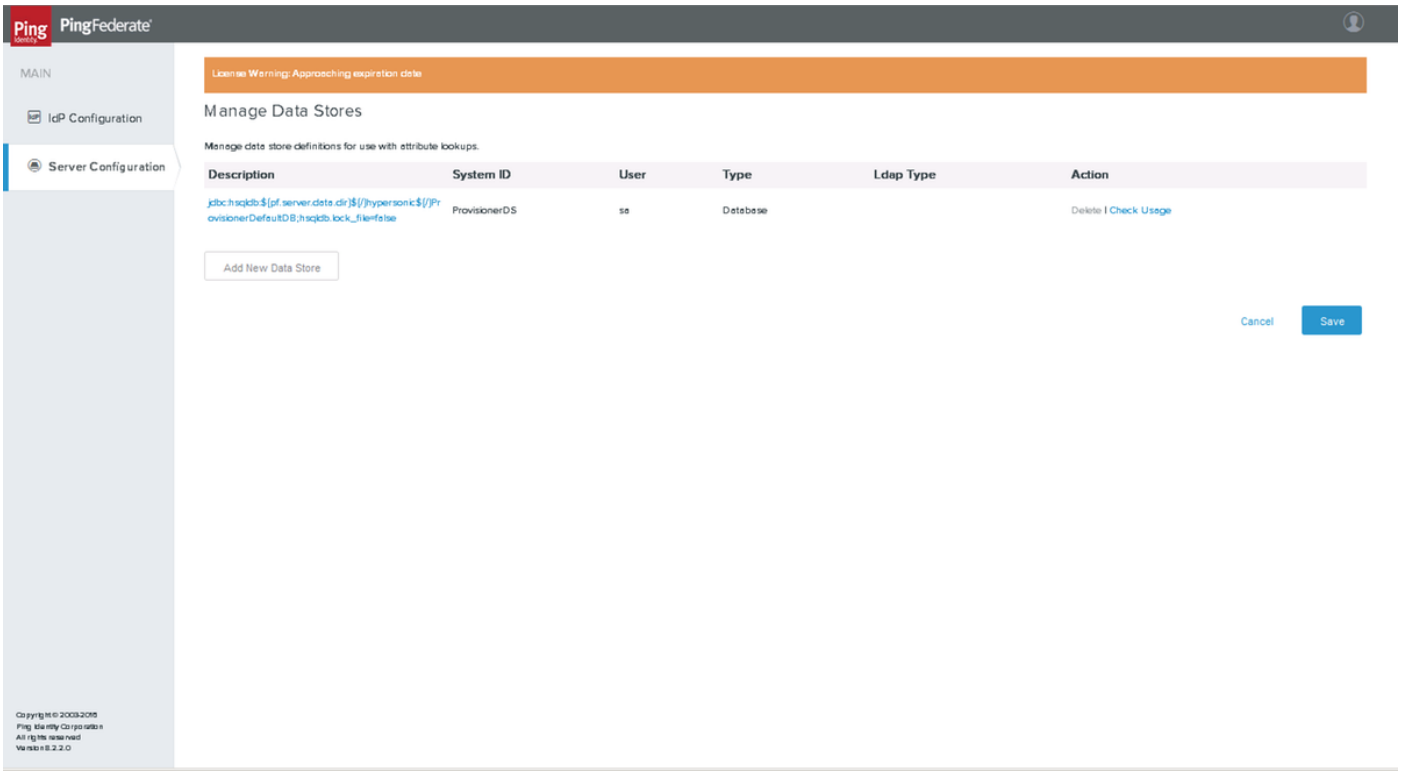
내보내기 및 요약



Export(내보내기)를 클릭합니다

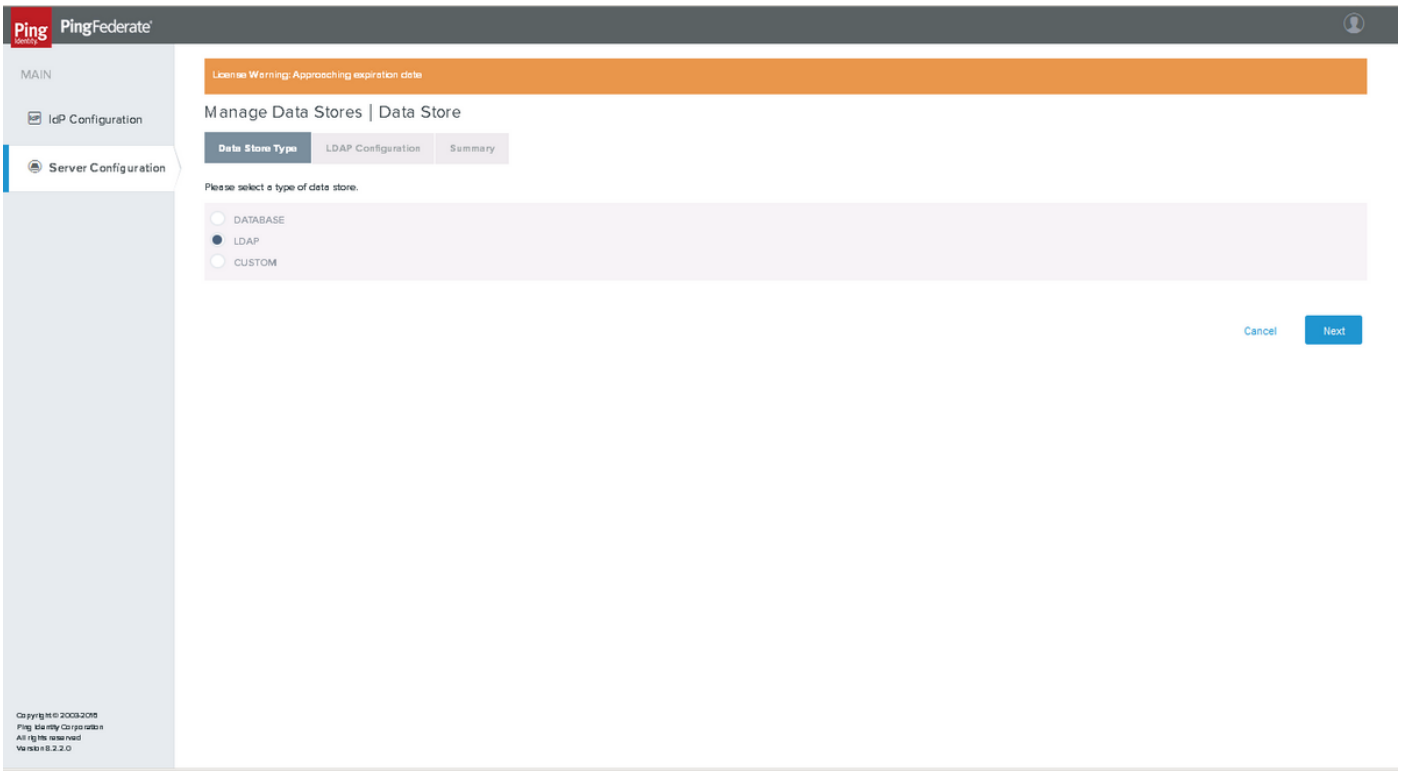
데이터 저장소

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

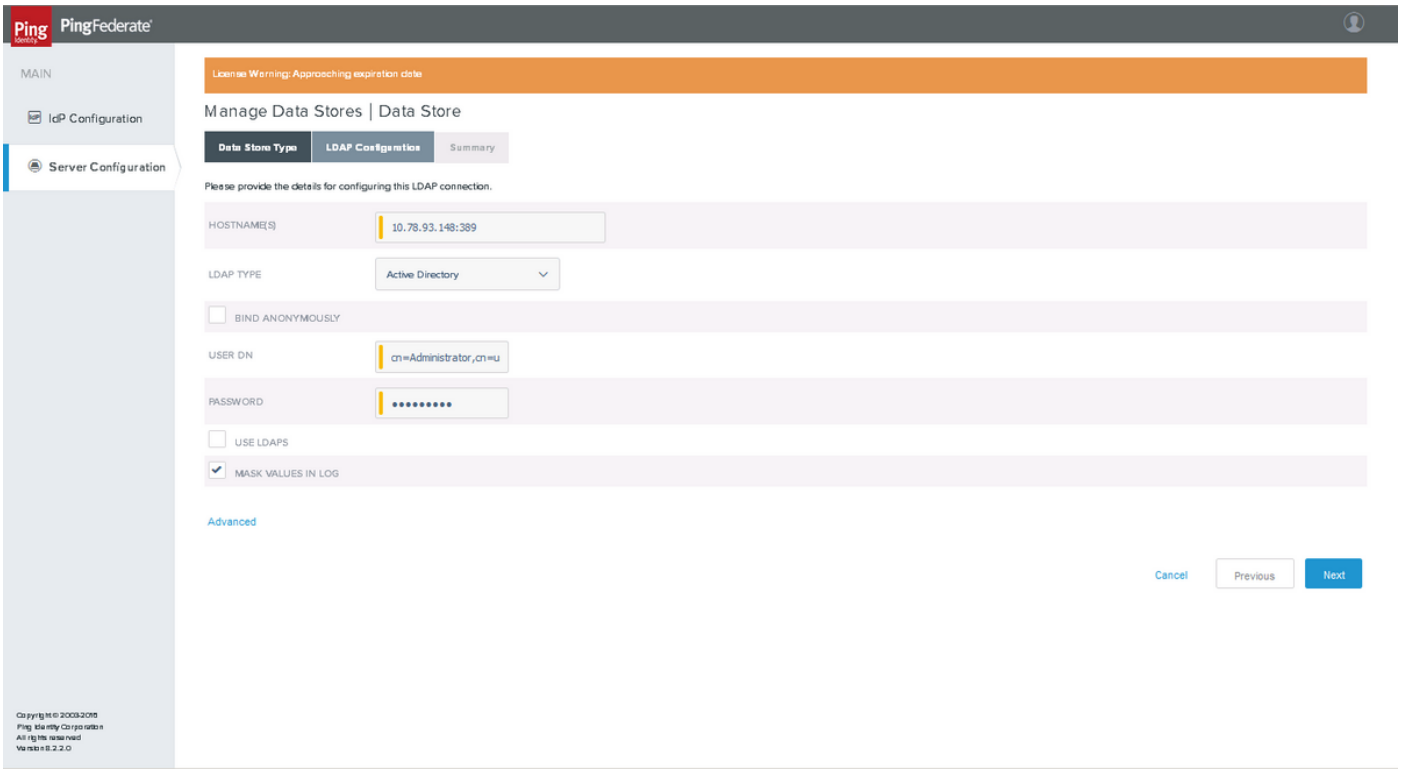


새 데이터 저장소 추가를 클릭합니다.

LDAP 컨피그레이션

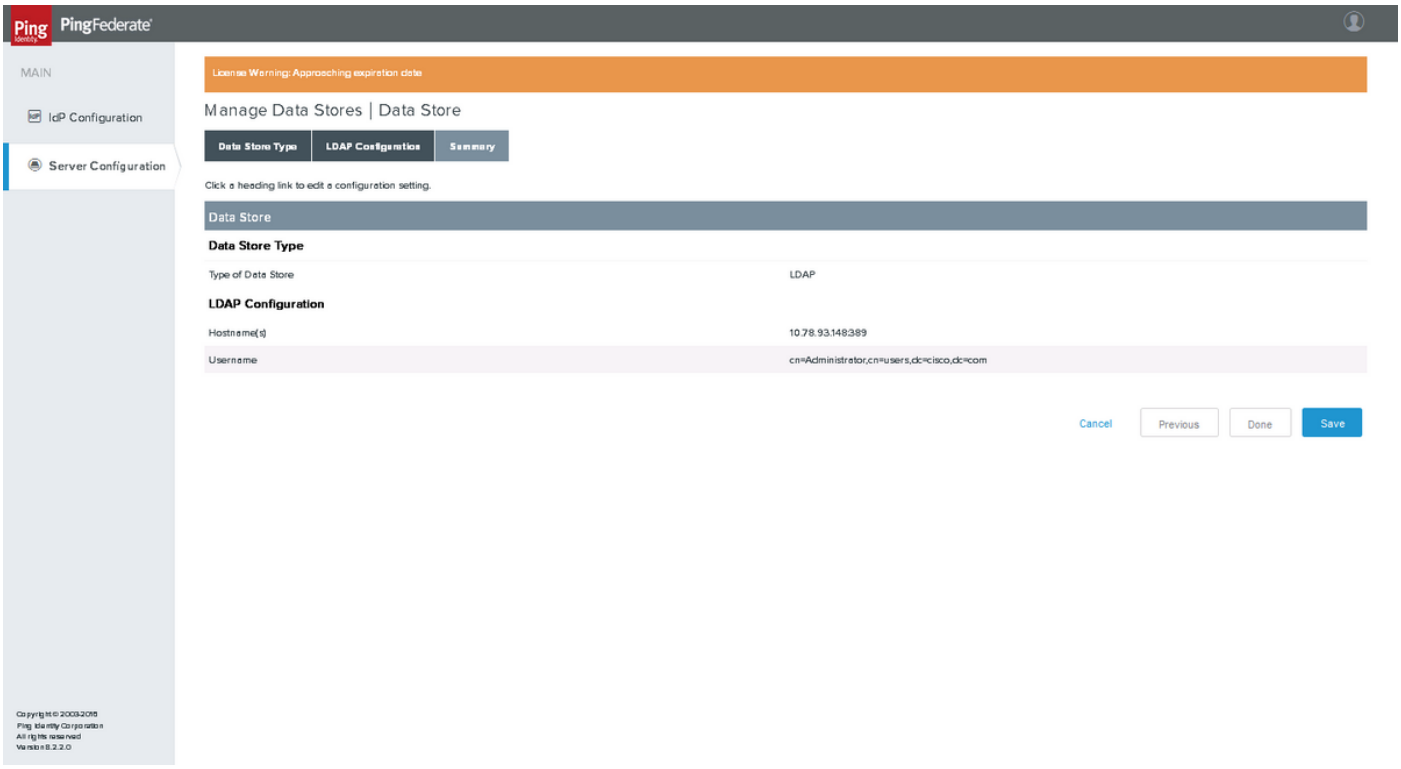


LDAP를 선택하고 Next(다음)를 클릭합니다.



값을 입력하고 다음을 클릭합니다.

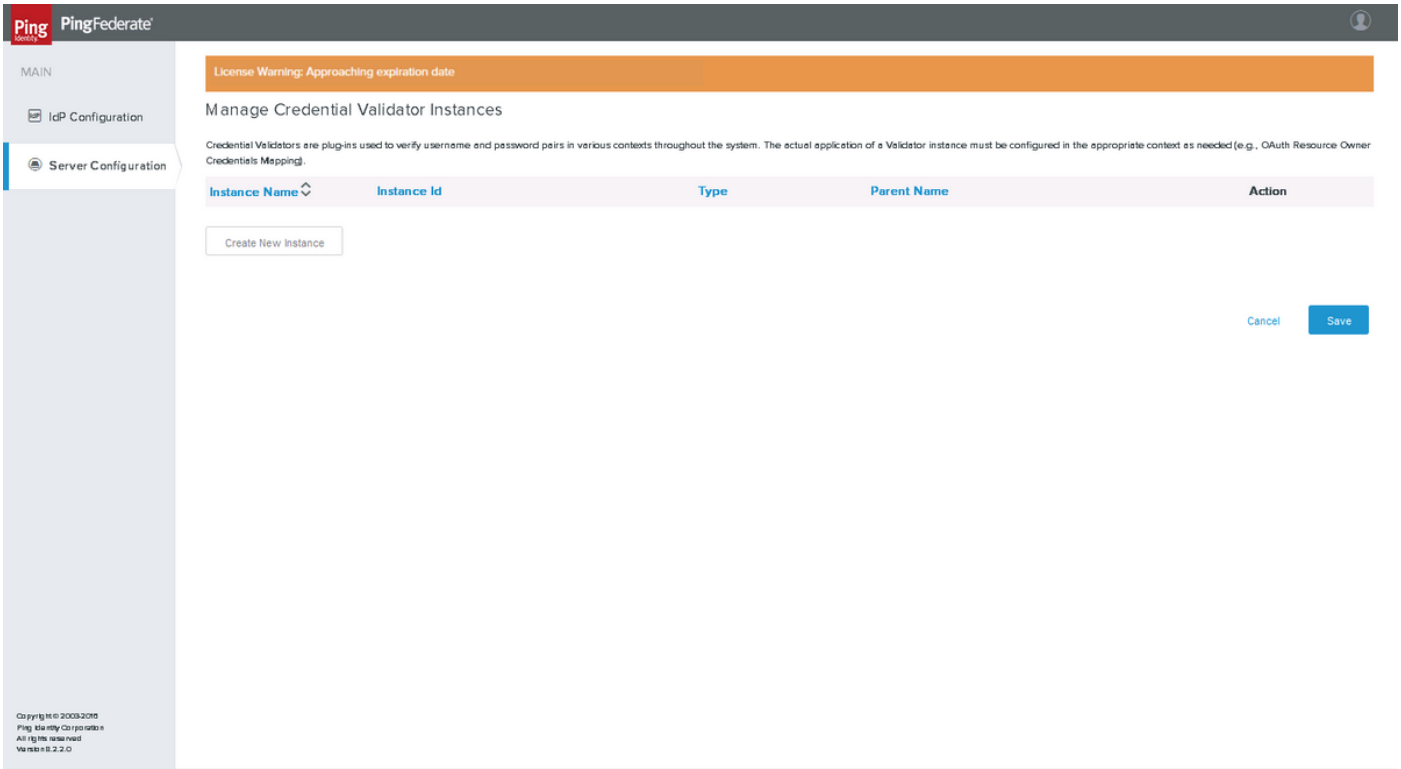
요약



확인 후 저장을 클릭합니다.

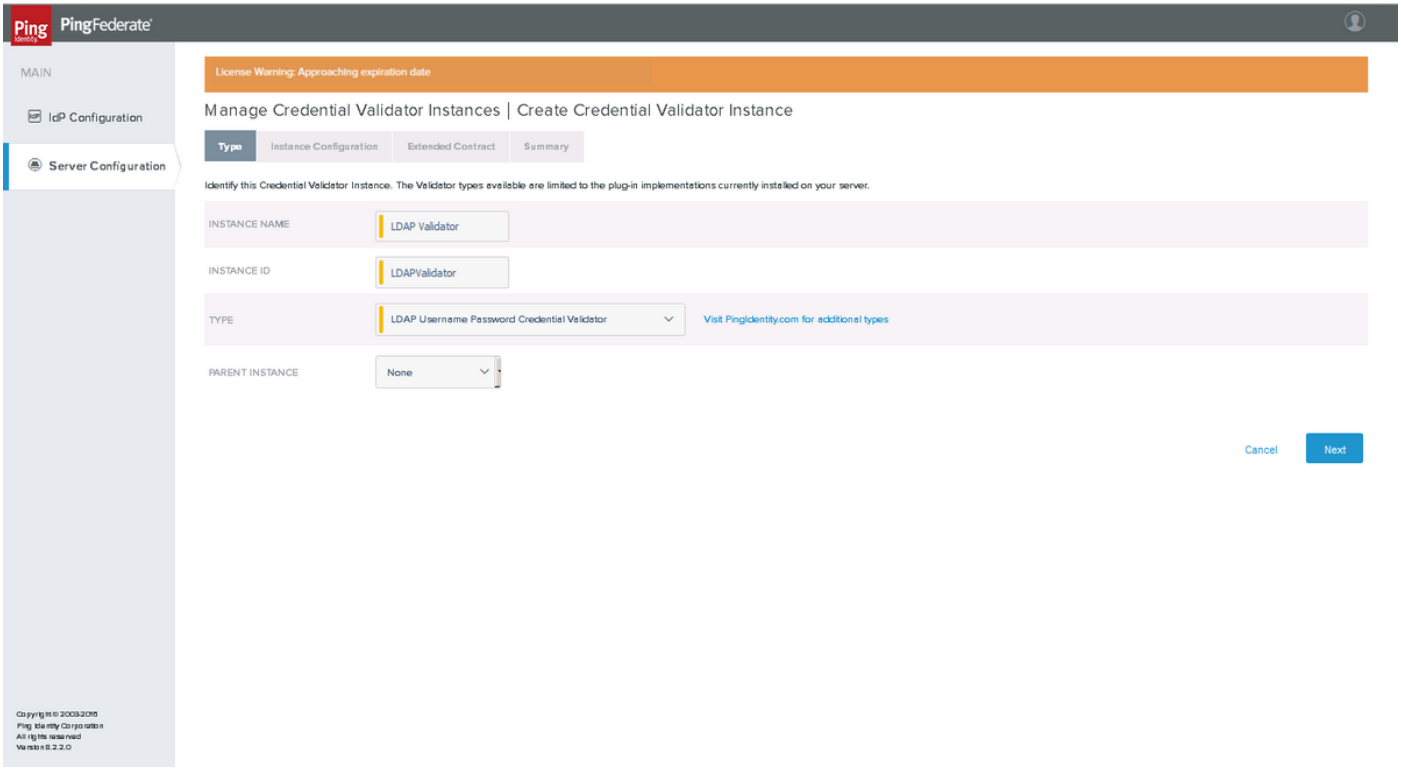
암호 자격 증명 검증기

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



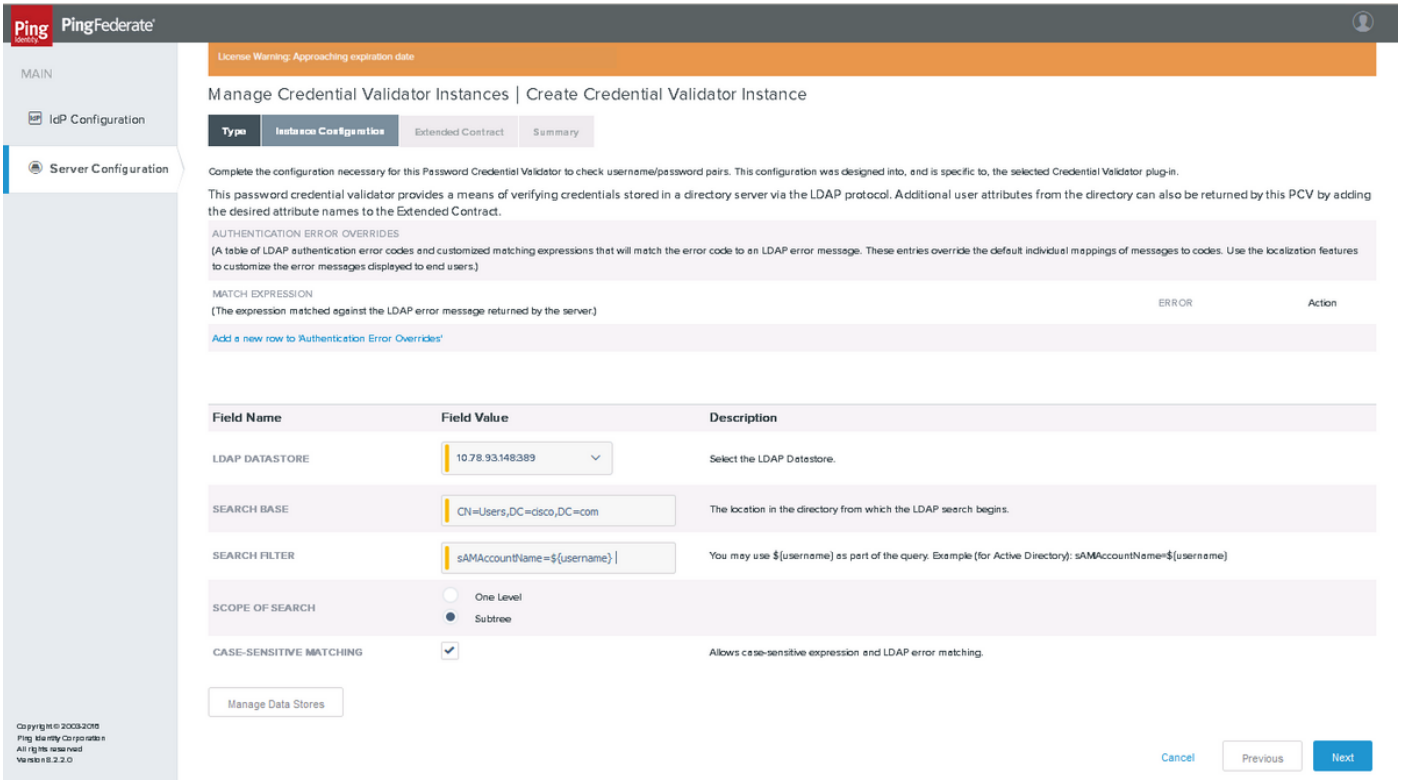
Create New Instance를 클릭합니다.

유형



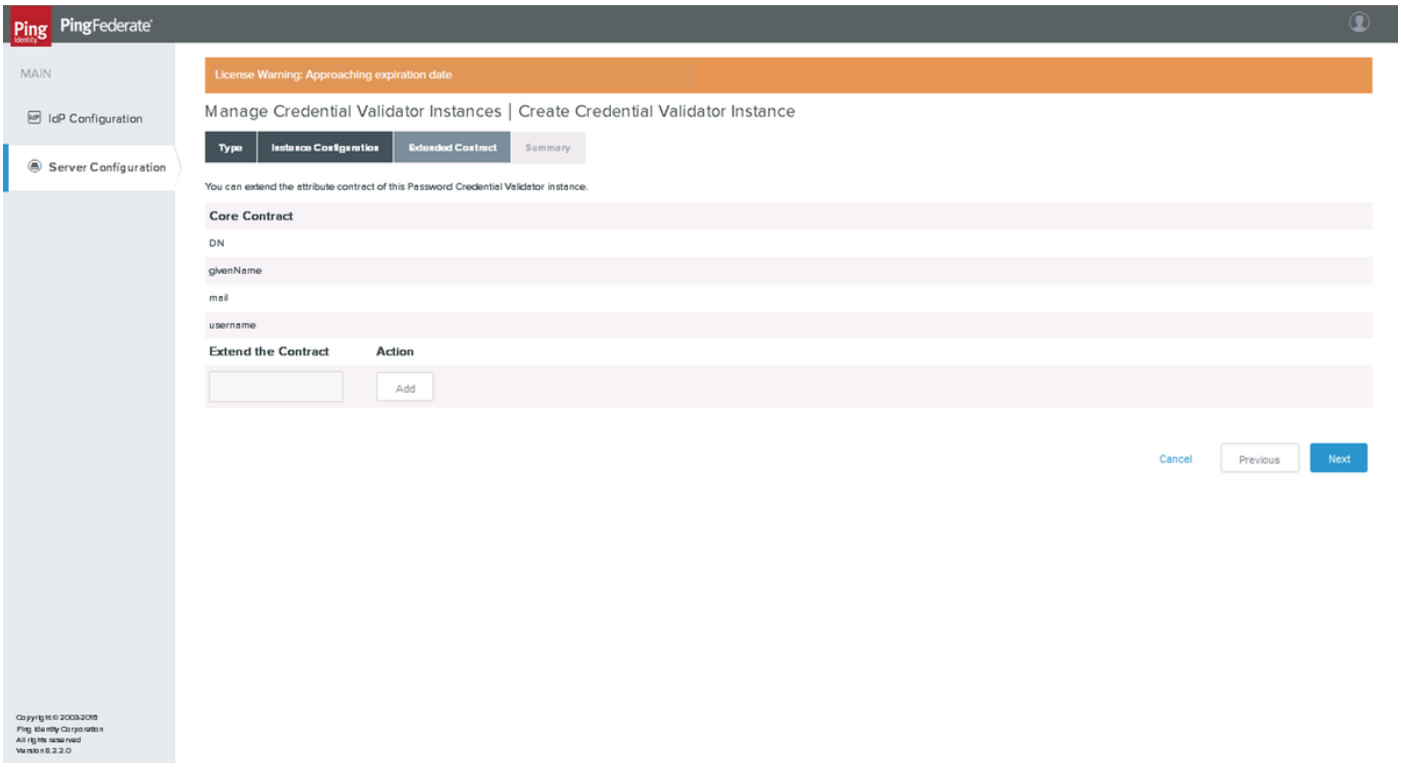
LDAP 사용자 이름 비밀번호 자격 증명 검증기를 TYPE으로 선택합니다. Next(다음)를 클릭합니다.

인스턴스 컨피그레이션



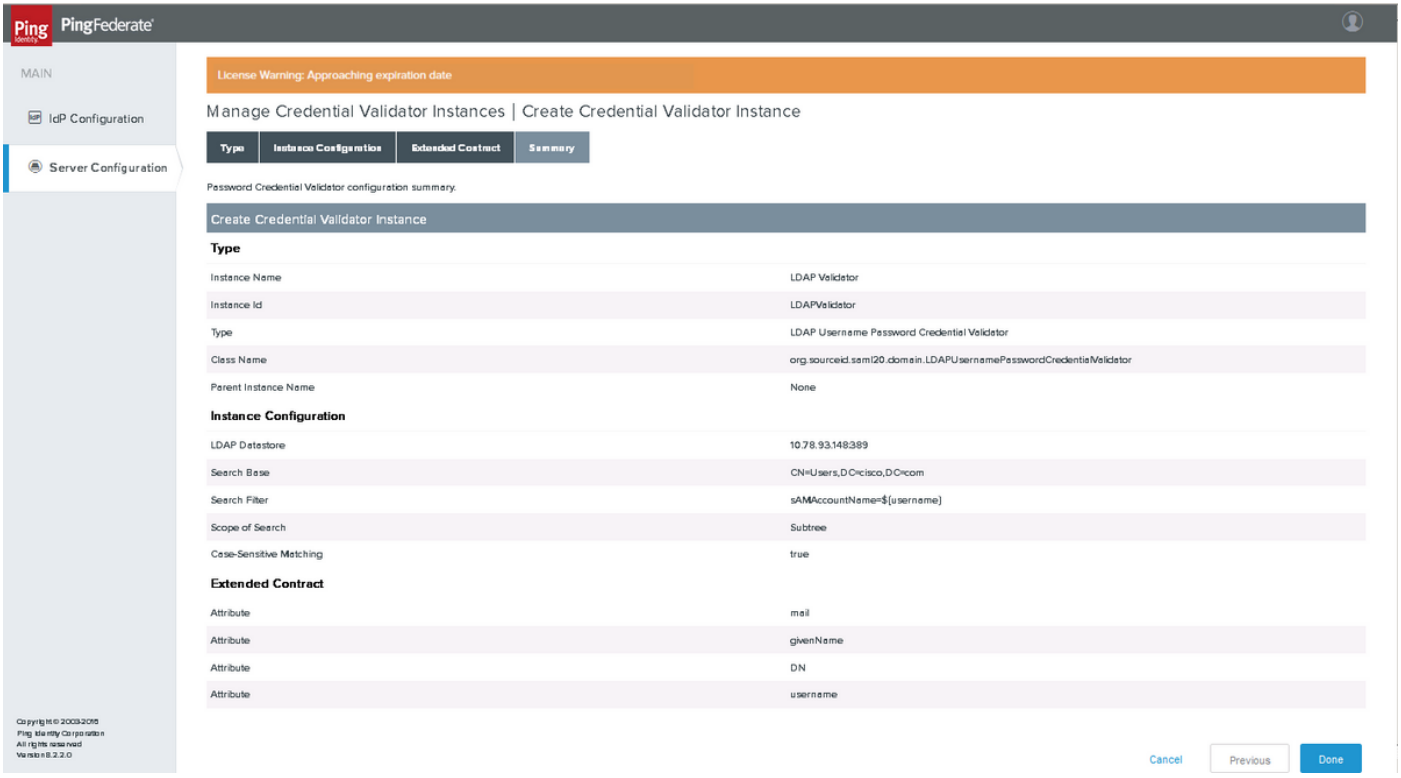
LDAP Datastore(LDAP 데이터 저장소)를 선택하고 Search Base(검색 기준), Search Filter(검색 필터) 및 Scope of Search(검색 범위)를 입력합니다. Next(다음)를 클릭합니다.

연장 계약



Next(다음)를 클릭합니다.

요약

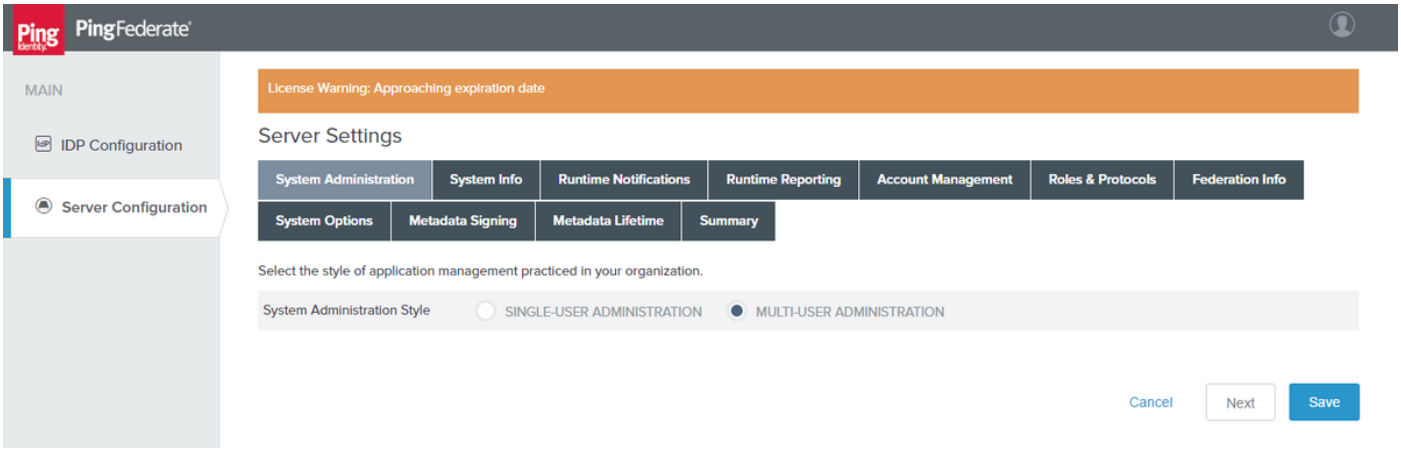


설정을 확인하고 Done(완료)을 클릭합니다.

서버 설정

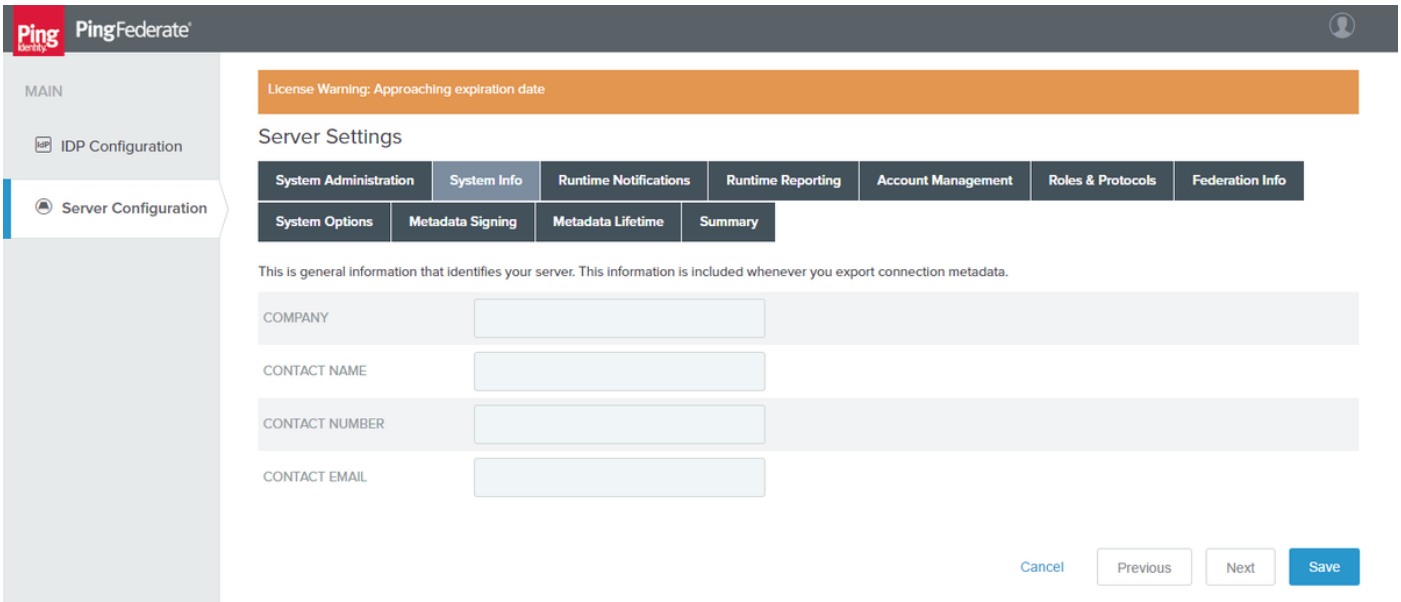
시스템 관리

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



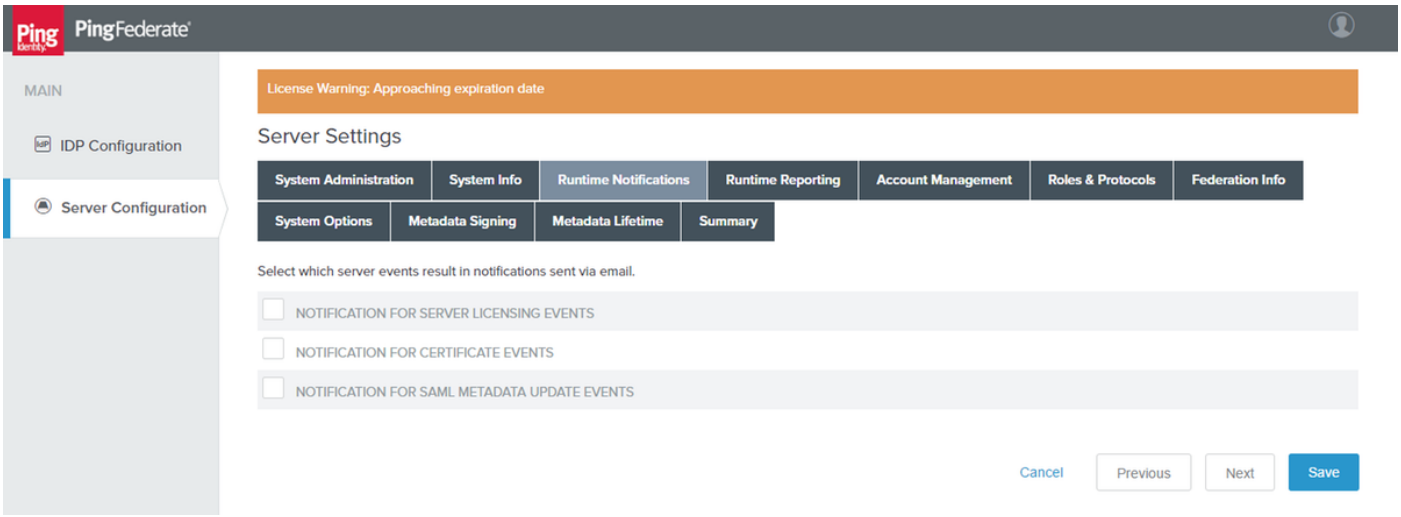
Next(다음)를 클릭합니다.

시스템 정보



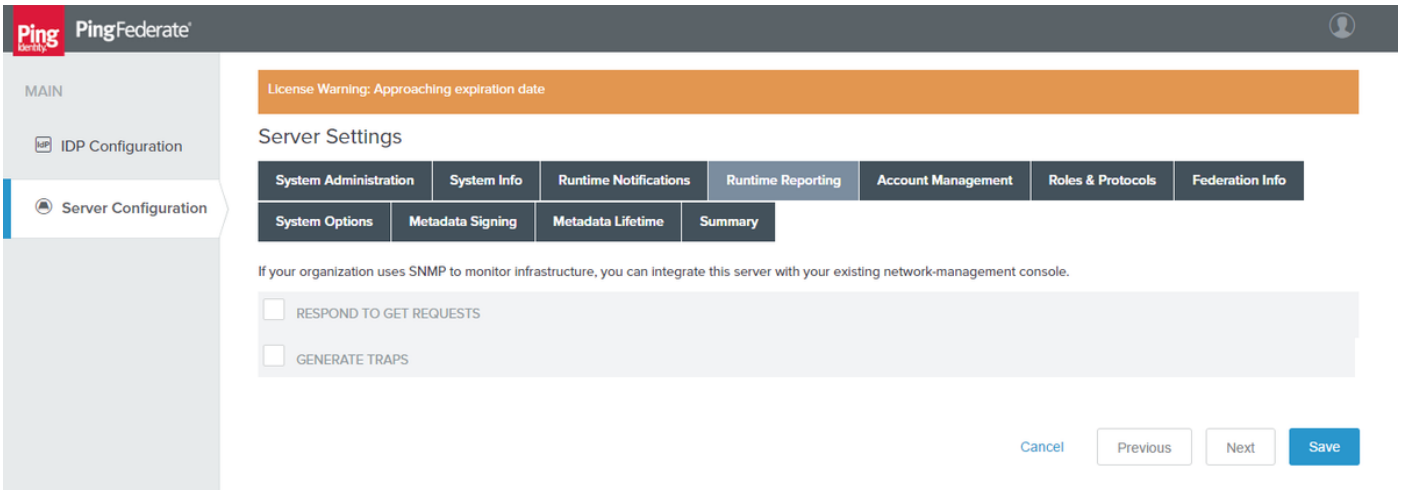
Next(다음)를 클릭합니다.

런타임 알림



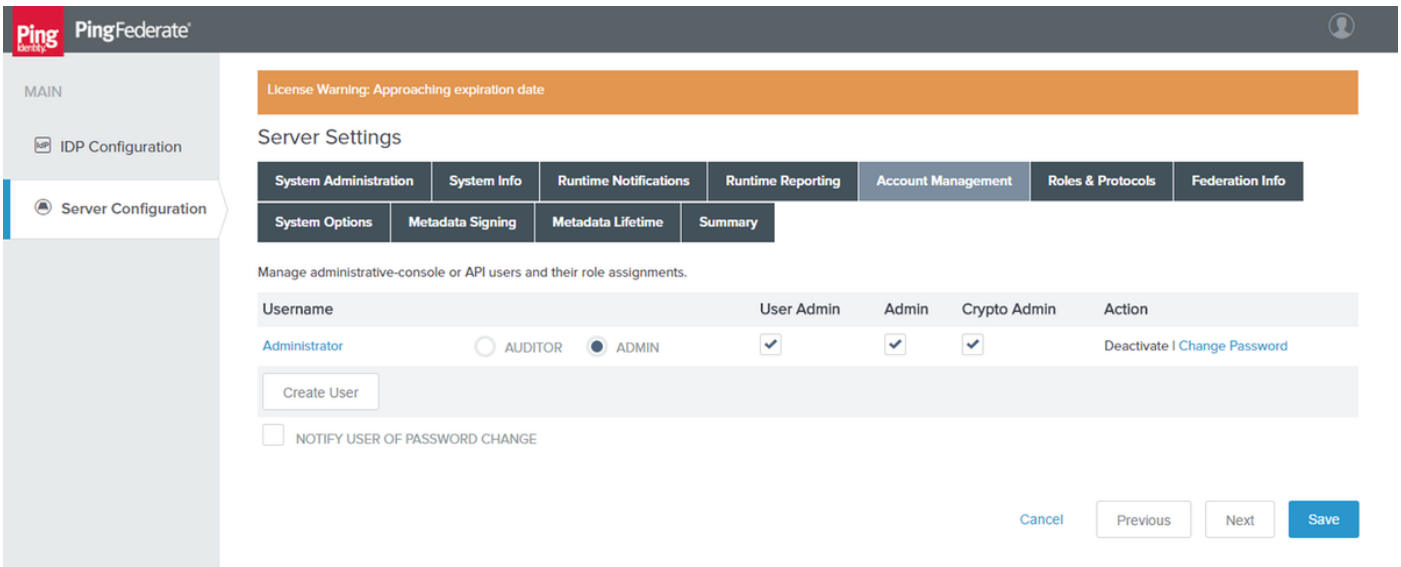
Next(다음)를 클릭합니다.

런타임 보고



Next(다음)를 클릭합니다.

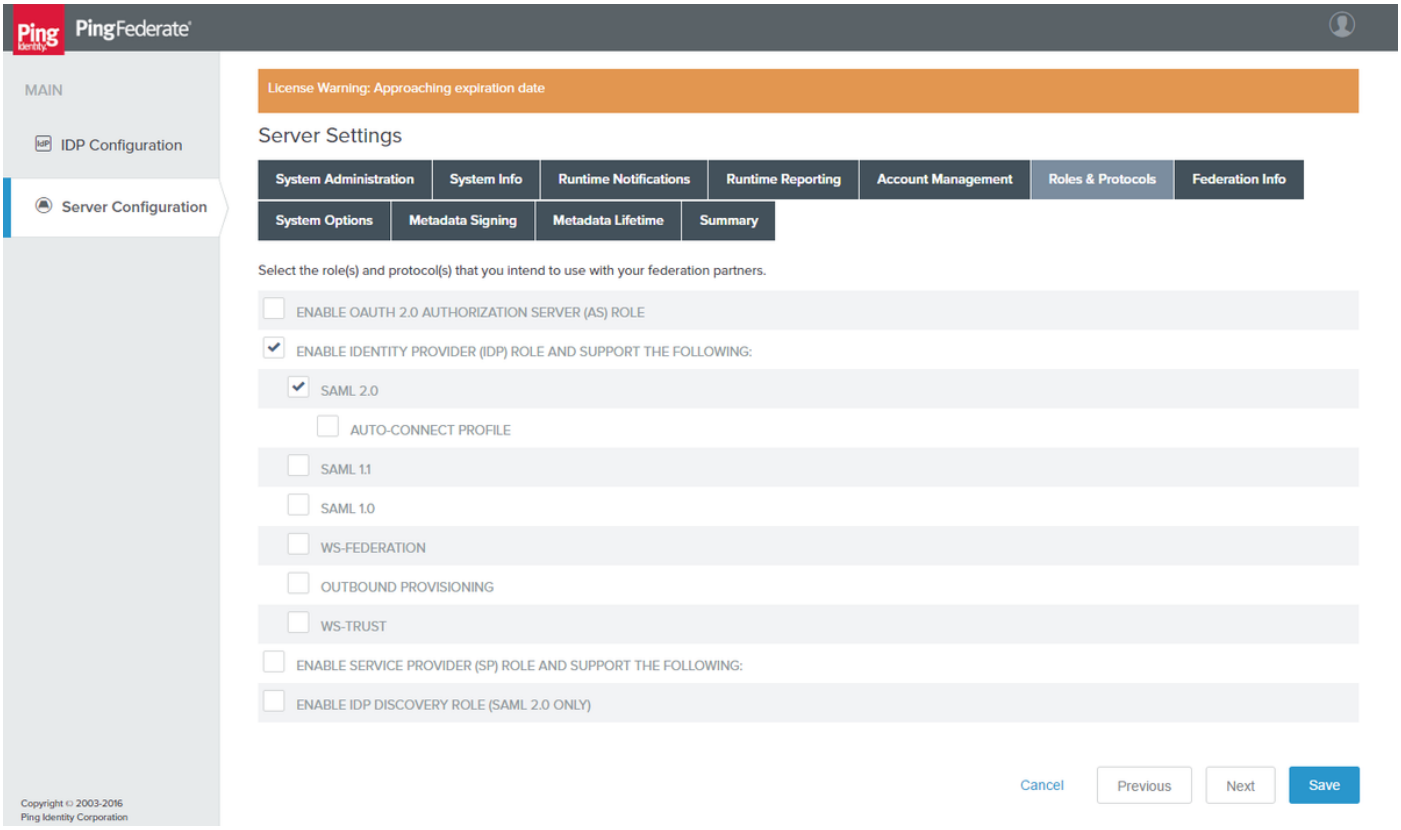
계정 관리



Next(다음)를 클릭합니다.

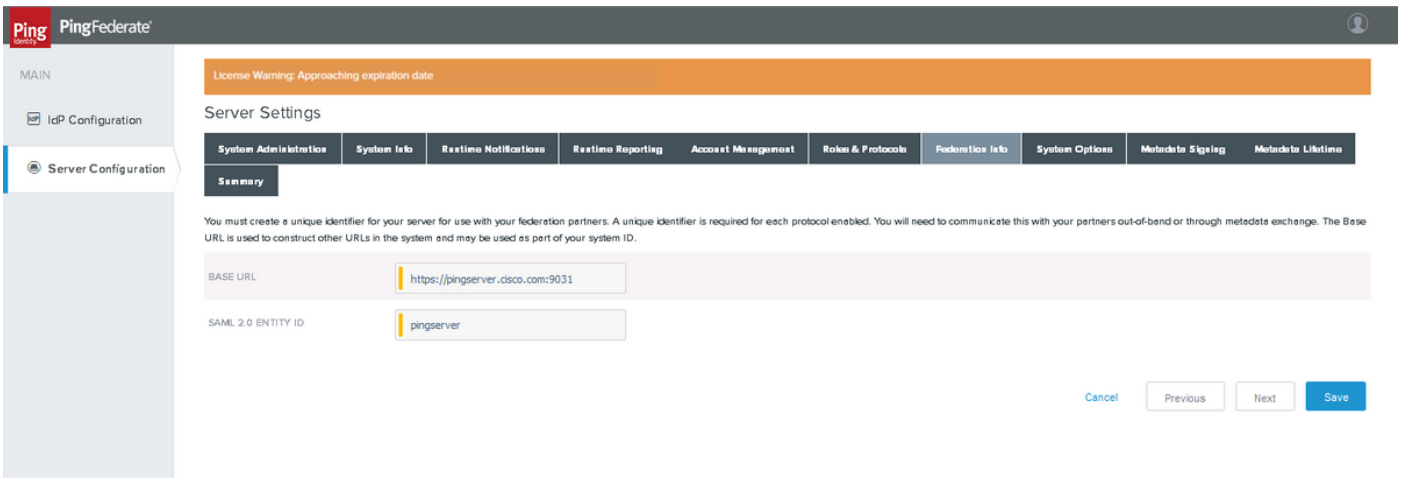
참고: 이 섹션에서는 사용자를 추가하거나 사용자의 비밀번호를 변경할 수 있습니다.

역할 및 프로토콜



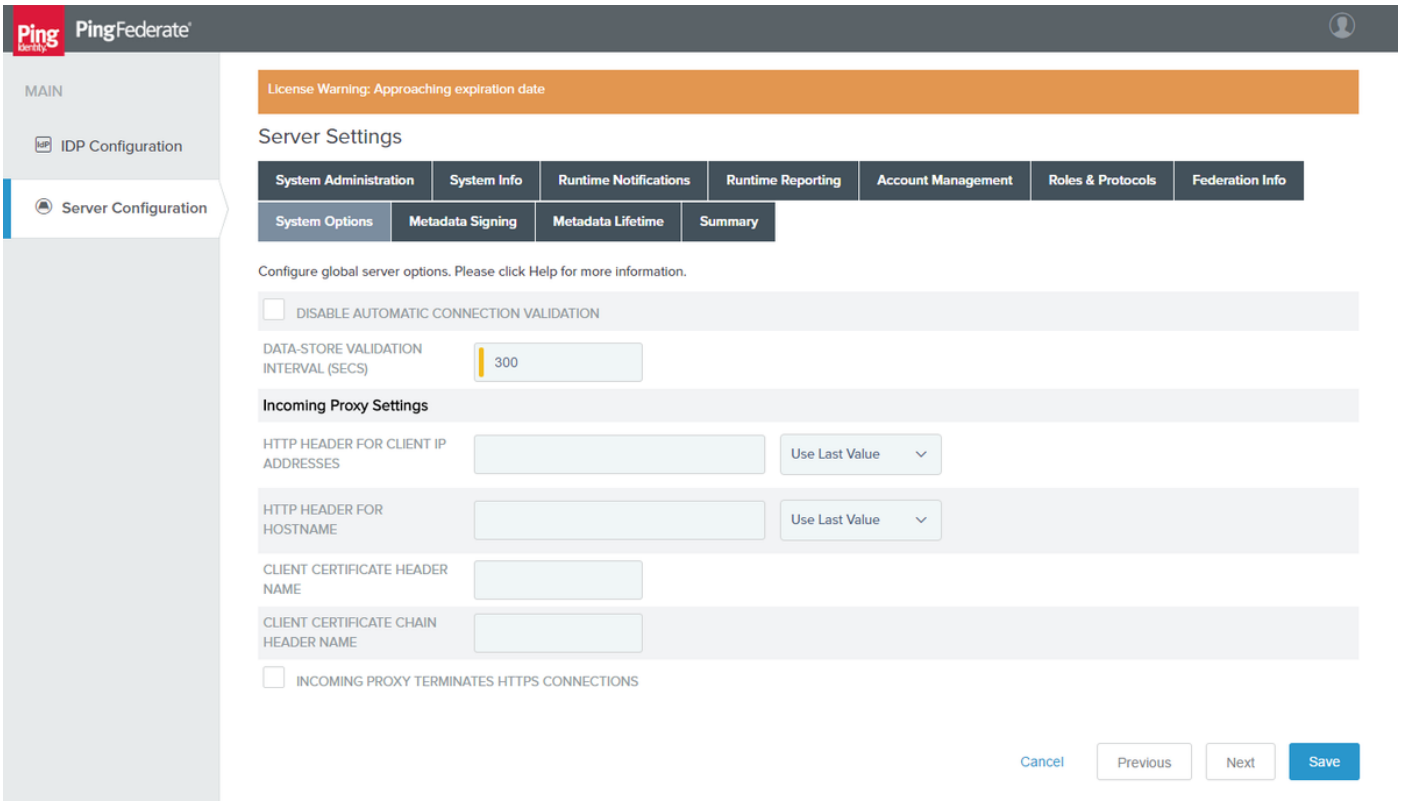
적절한 Role/s 및 Protocol/s를 선택합니다. Next(다음)를 클릭합니다.

페더레이션 정보



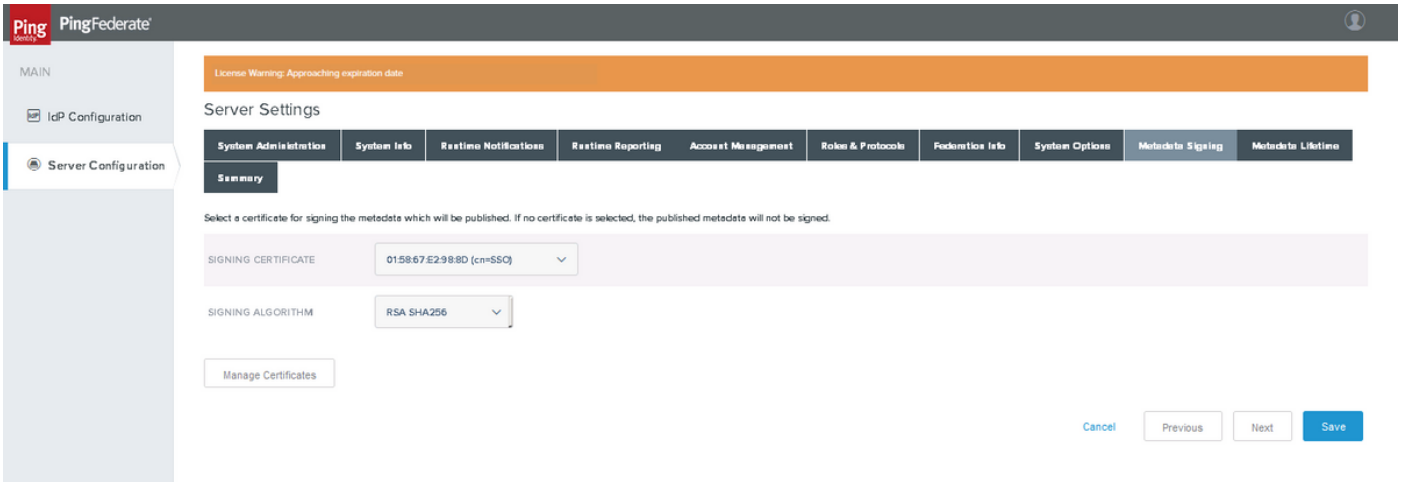
Next(다음)를 클릭합니다.

시스템 옵션



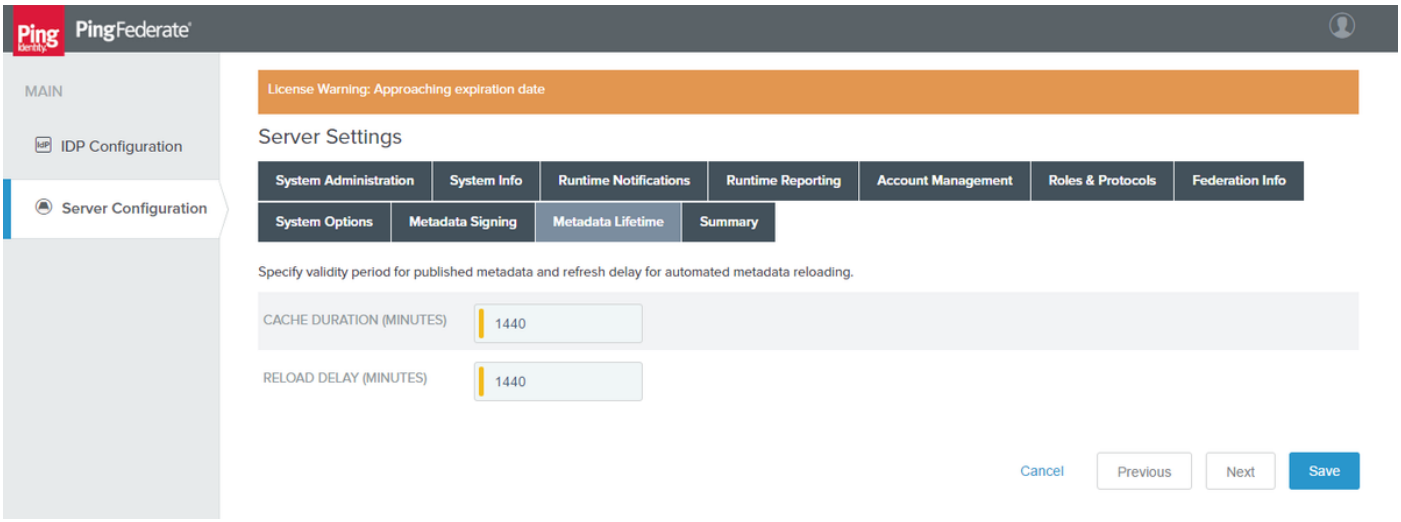
Next(다음)를 클릭합니다.

메타데이터 서명



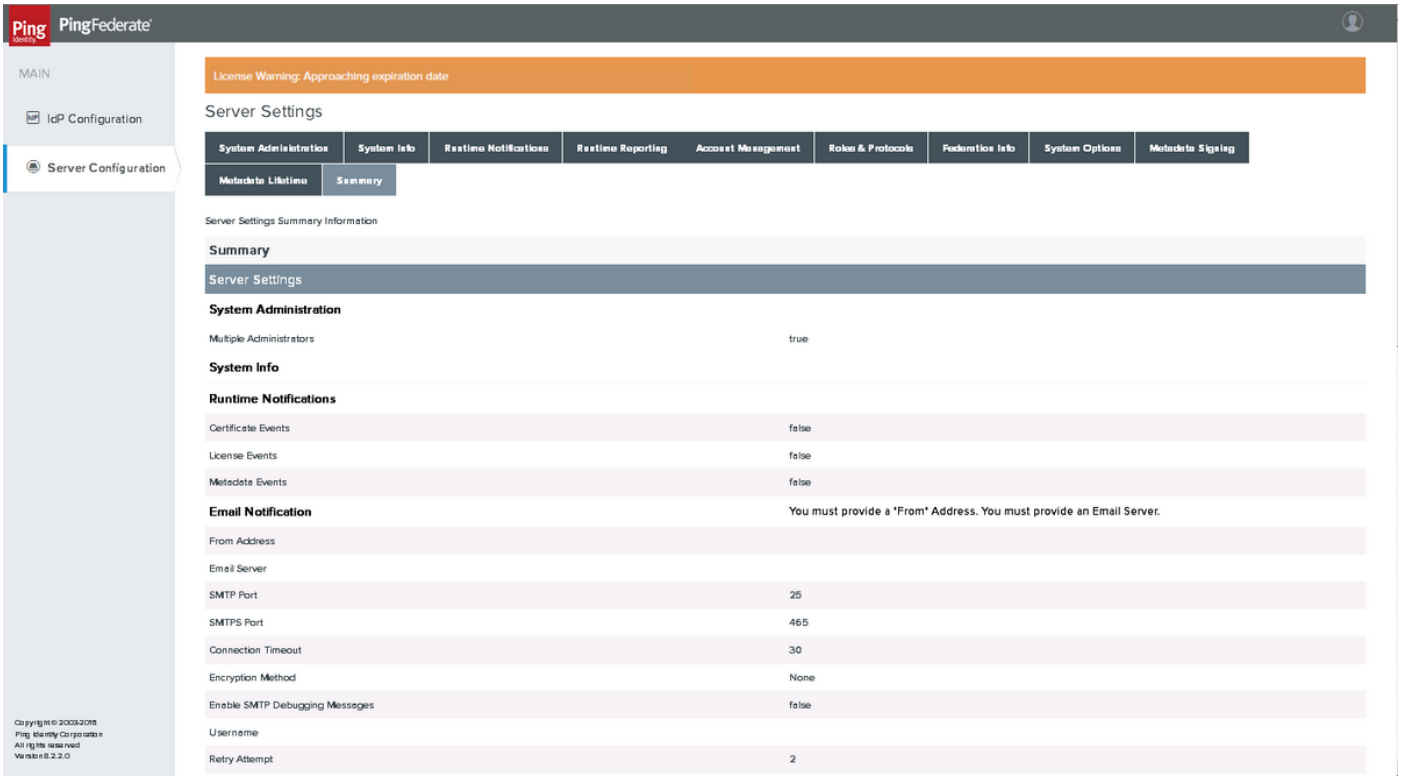
인증서 컨피그레이션의 일부로 앞에서 생성한 서명 인증서 및 서명 알고리즘을 선택합니다. Next(다음)를 클릭합니다.

메타데이터 수명



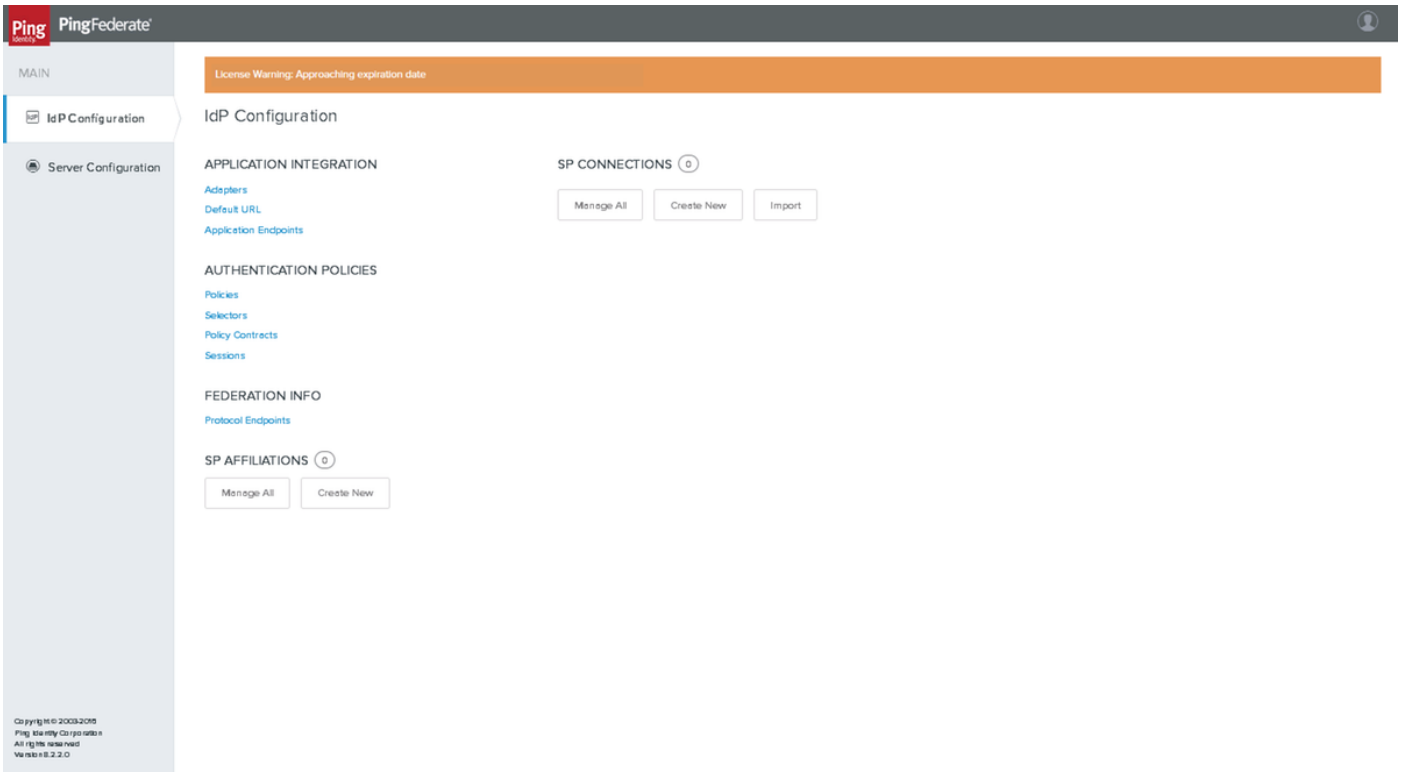
Next(다음)를 클릭합니다.

요약



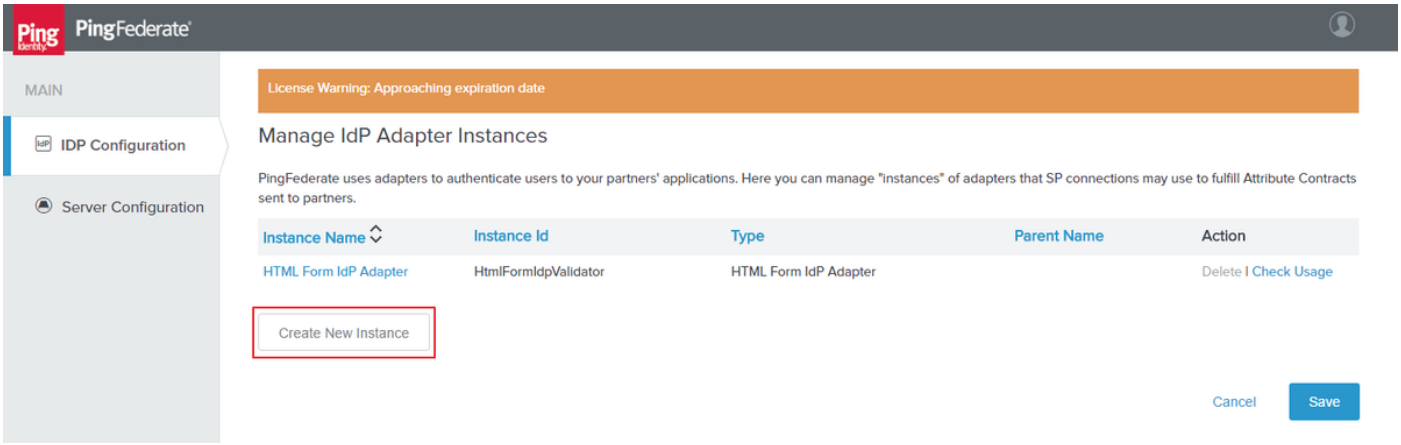
설정을 확인하고 저장을 클릭합니다.

IdP(Identity Provider) 컨피그레이션



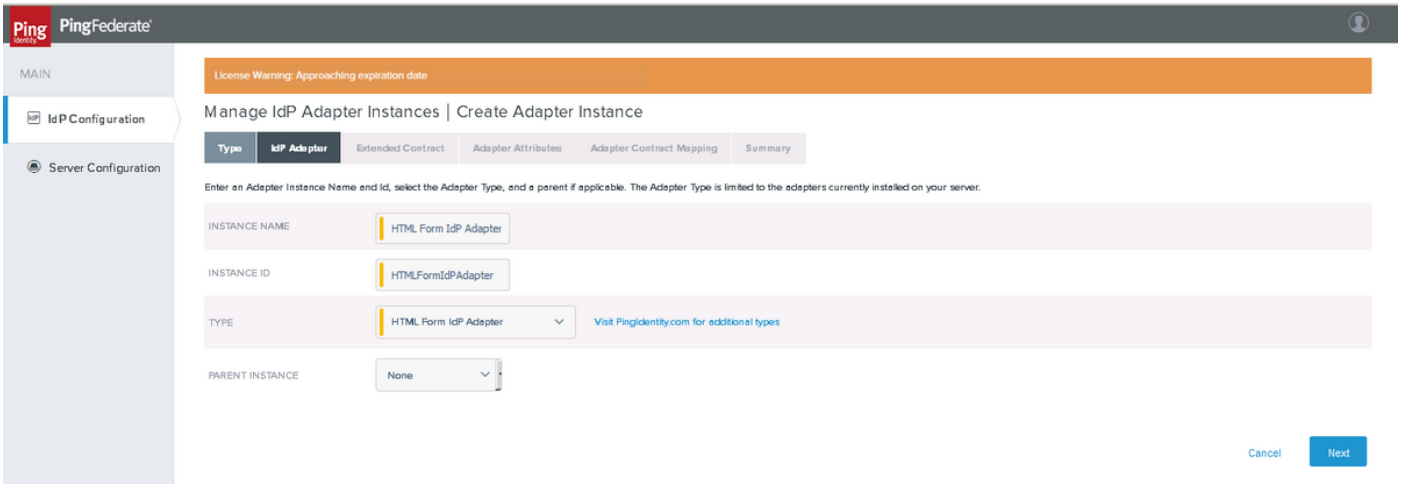
어댑터

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



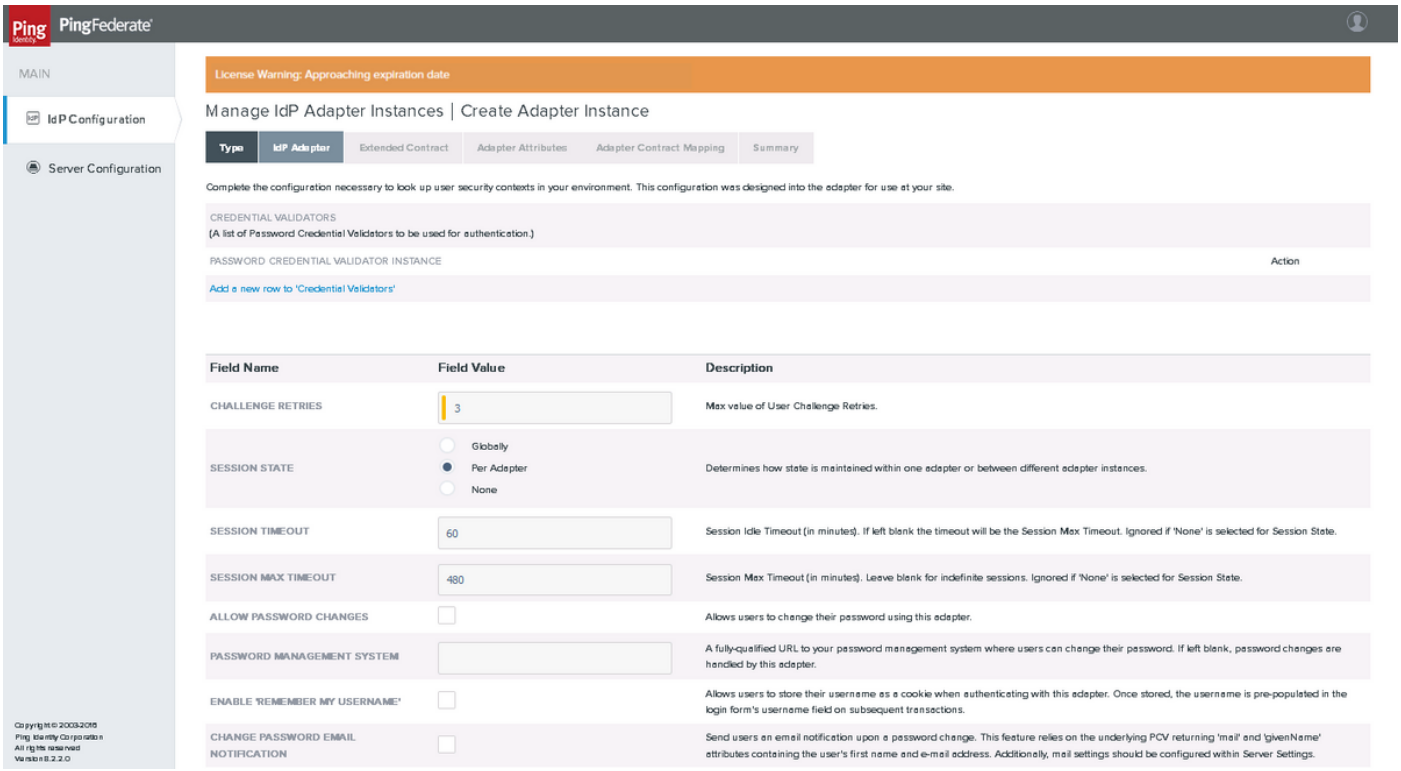
Create New Instance를 클릭합니다.

유형



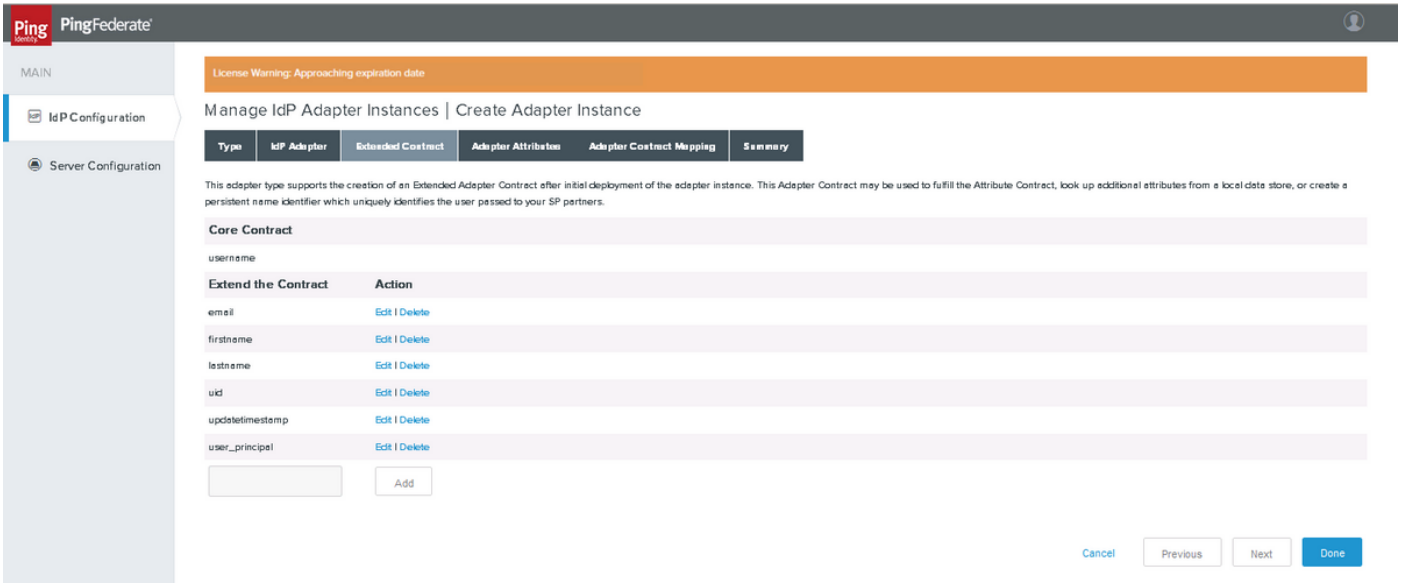
HTML 양식 IDP 어댑터를 선택합니다. Next(다음)를 클릭합니다.

IdP 어댑터



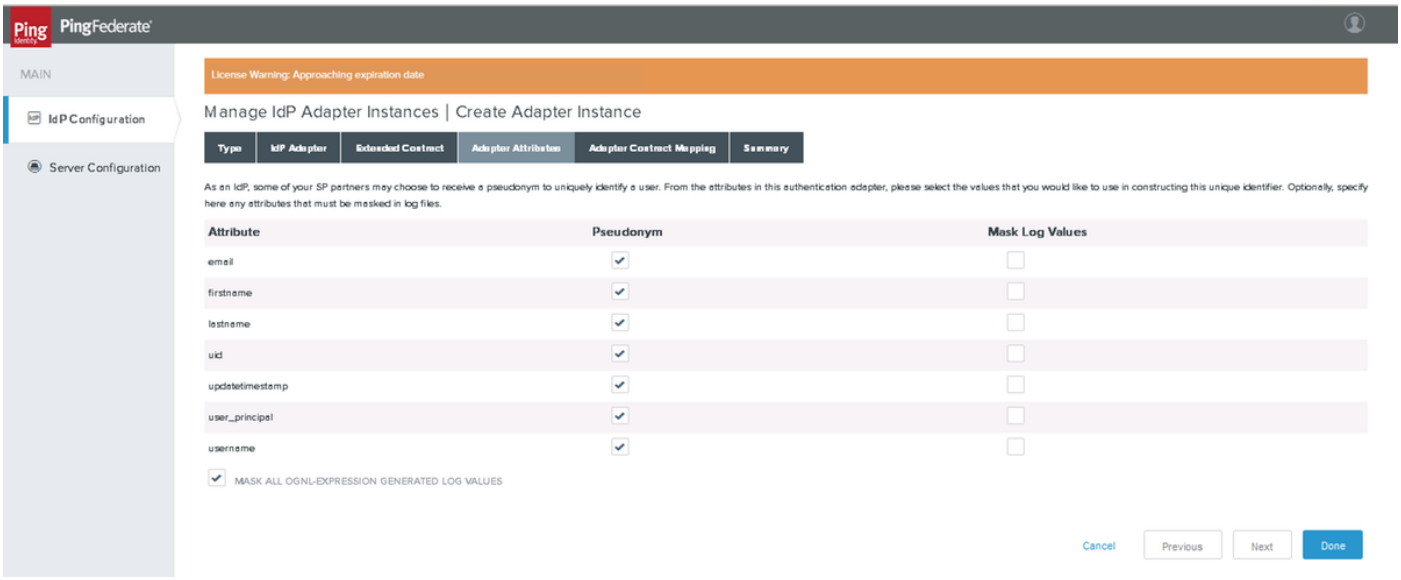
Add a new row to 'Credential Validators'를 클릭하고 앞서 PASSWORD CREDENTIAL VALIDATOR INSTANCE로 만든 LDAP Validator를 선택한 후 Update를 클릭합니다. Next를 클릭합니다.

연장 계약



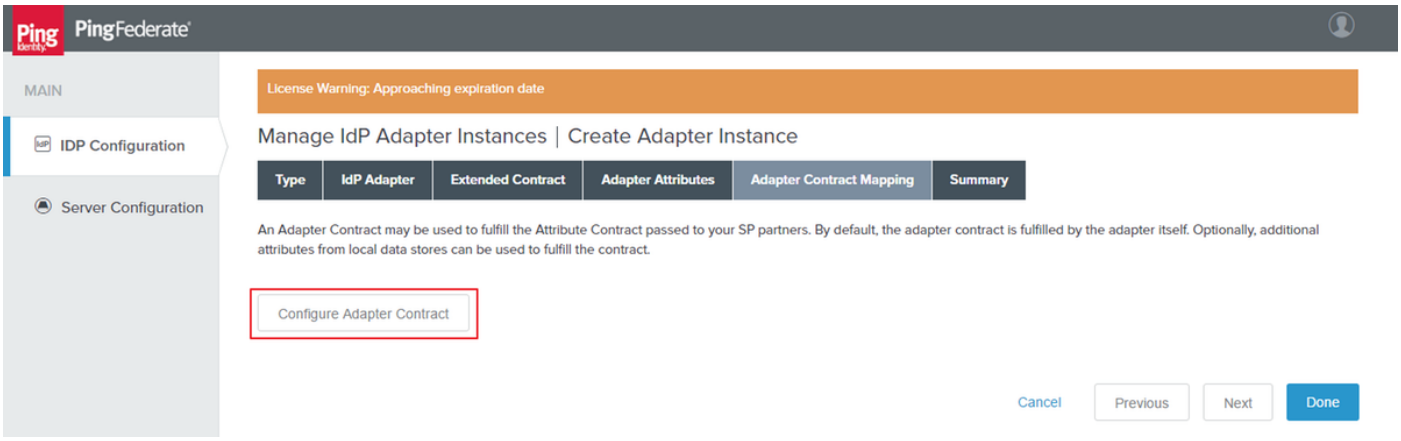
표시된 대로 계약을 추가합니다. Next(다음)를 클릭합니다.

어댑터 특성



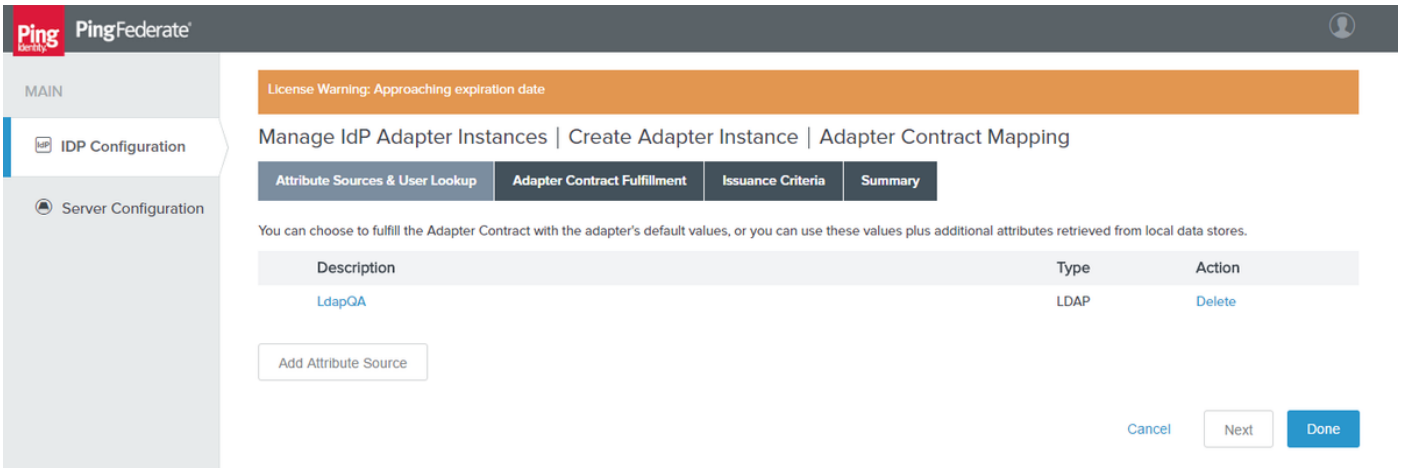
Next(다음)를 클릭합니다.

어댑터 계약 매핑



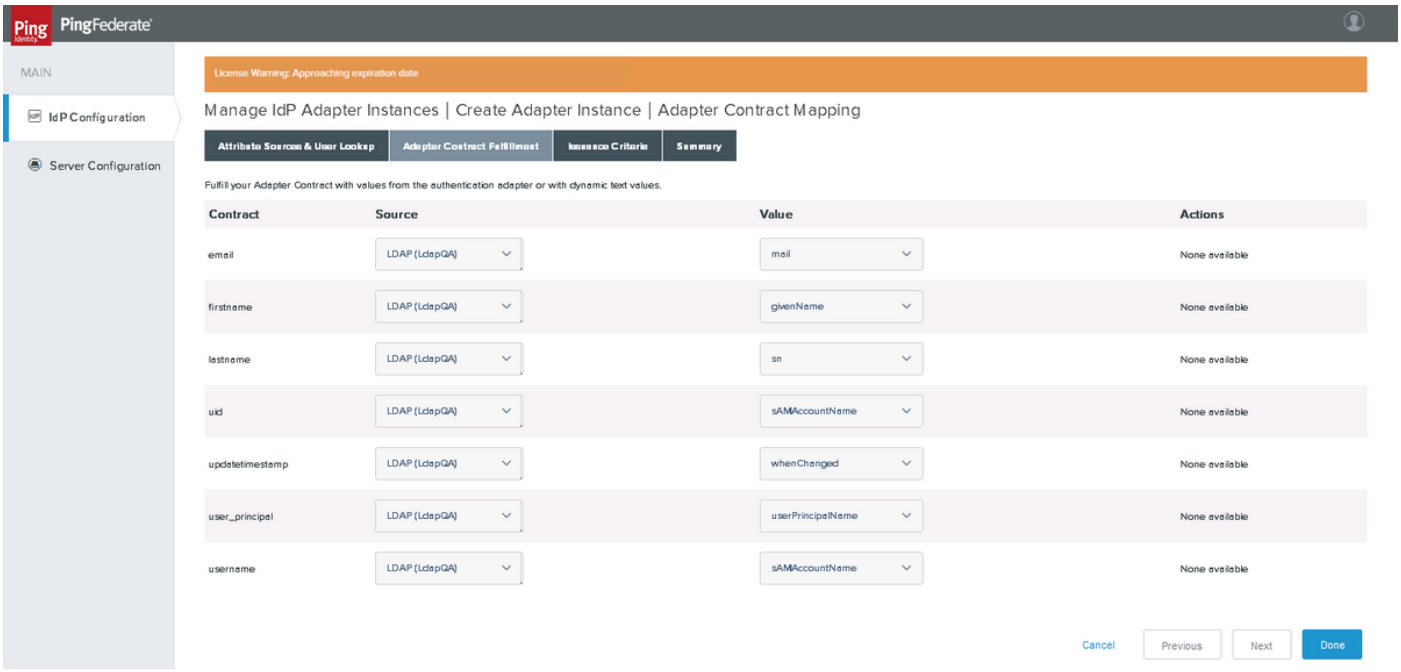
Configure Adapter Contract(어댑터 계약 구성)를 클릭합니다.

특성 소스 및 사용자 조회



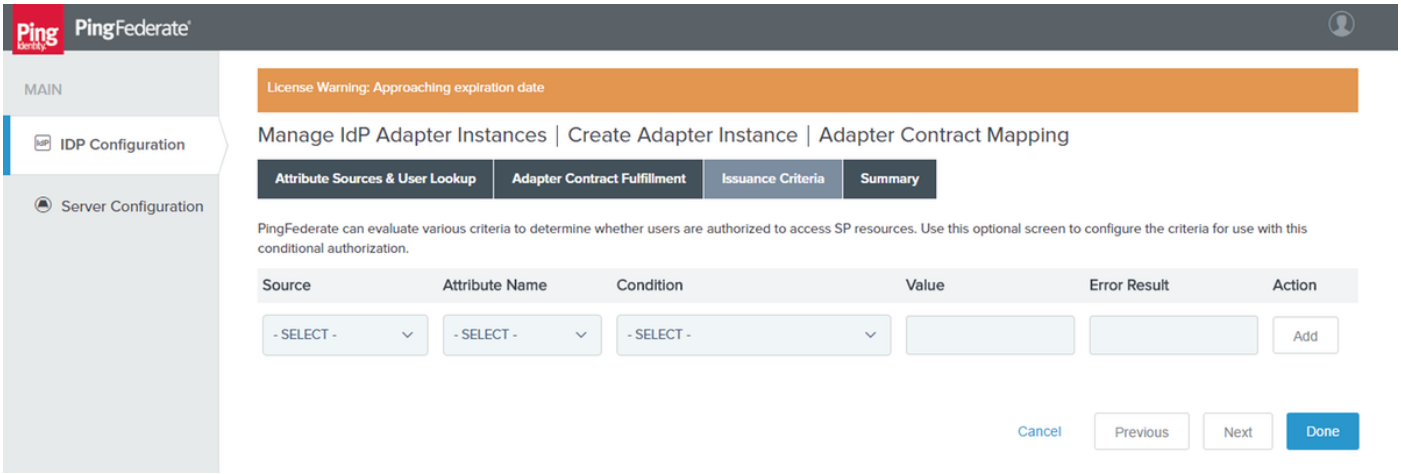
특성 소스를 추가하고 이전에 생성한 LDAP 저장소를 선택합니다. Next(다음)를 클릭합니다.

어댑터 계약 이행



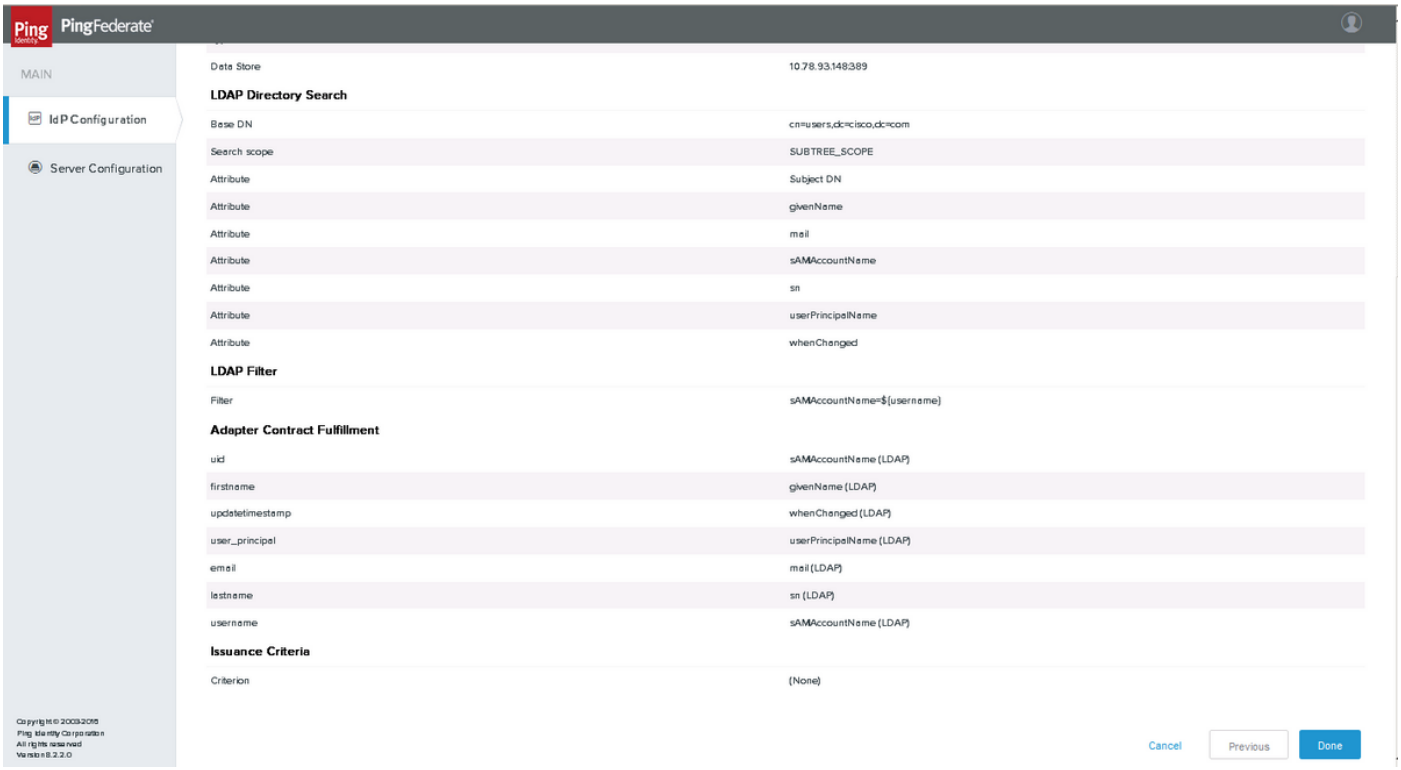
특성을 매핑합니다. Next(다음)를 클릭합니다.

발급 기준



Next(다음)를 클릭합니다.

요약

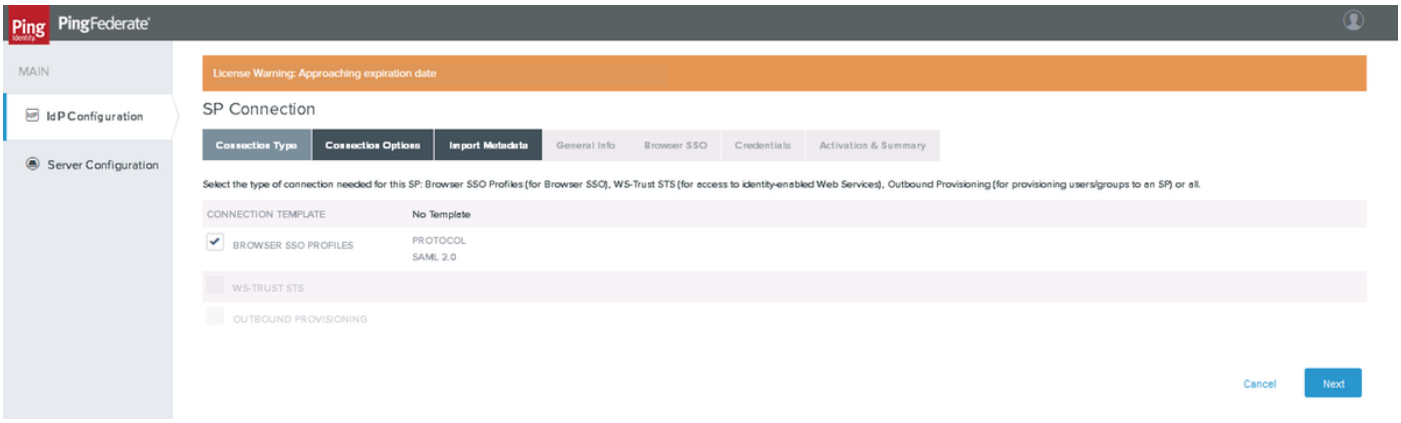


설정을 확인하고 Done(완료)을 클릭합니다.

SP 접속

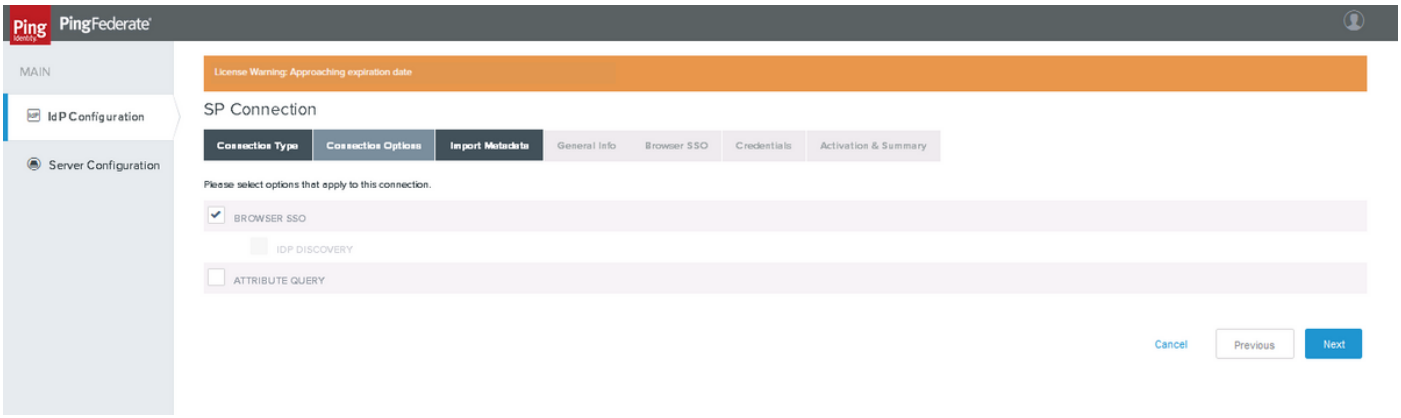
새 SP 접속 생성

연결 유형



Next(다음)를 클릭합니다.

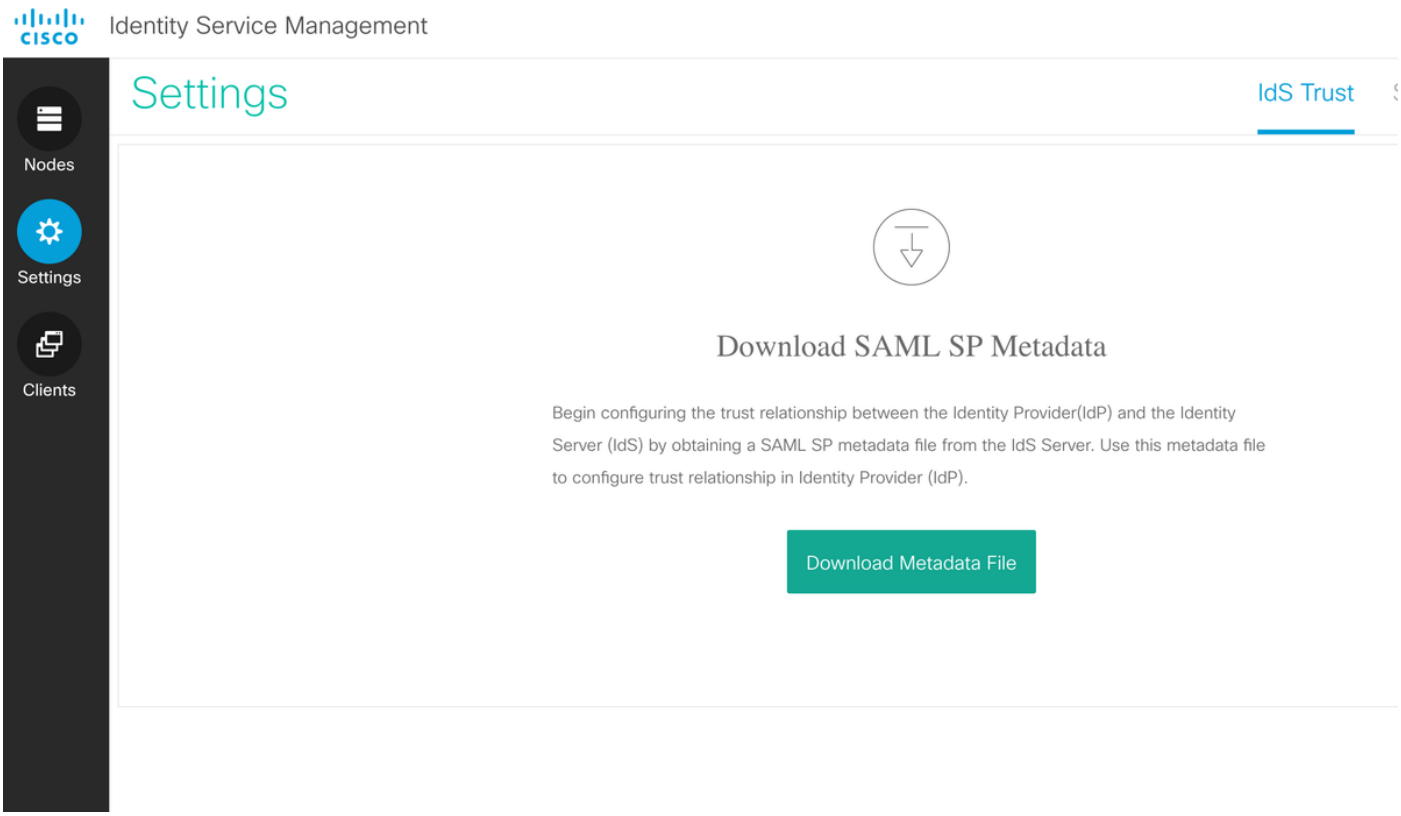
연결 옵션



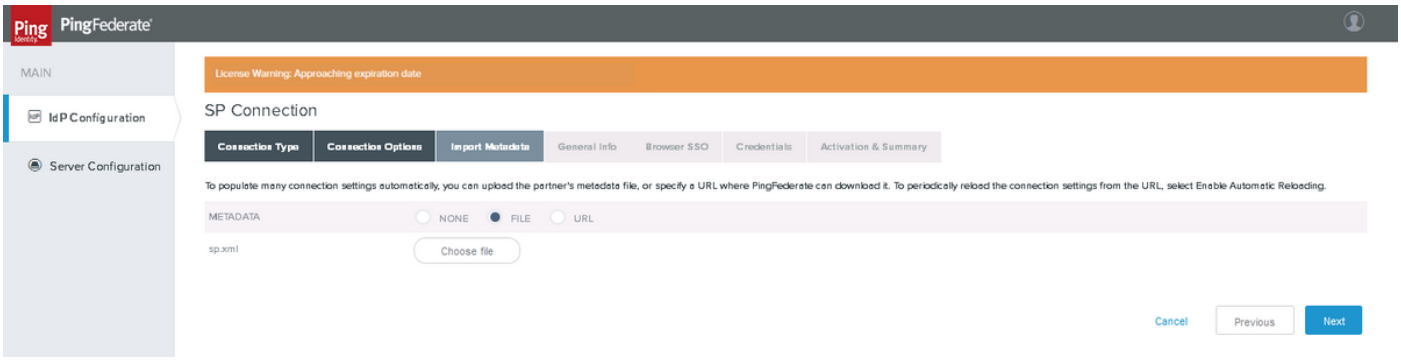
Next(다음)를 클릭합니다.

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

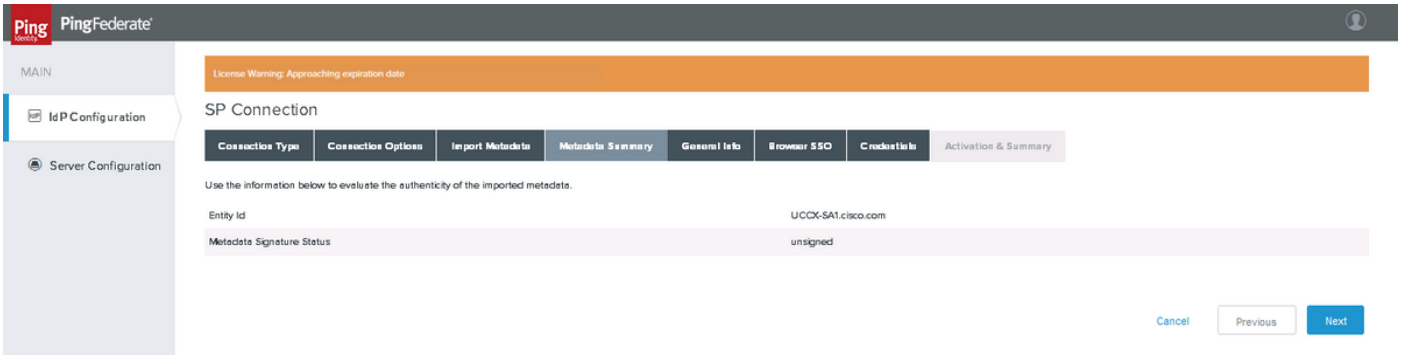


서비스 공급자의 메타데이터 xml 파일을 PingFederate에 업로드합니다.



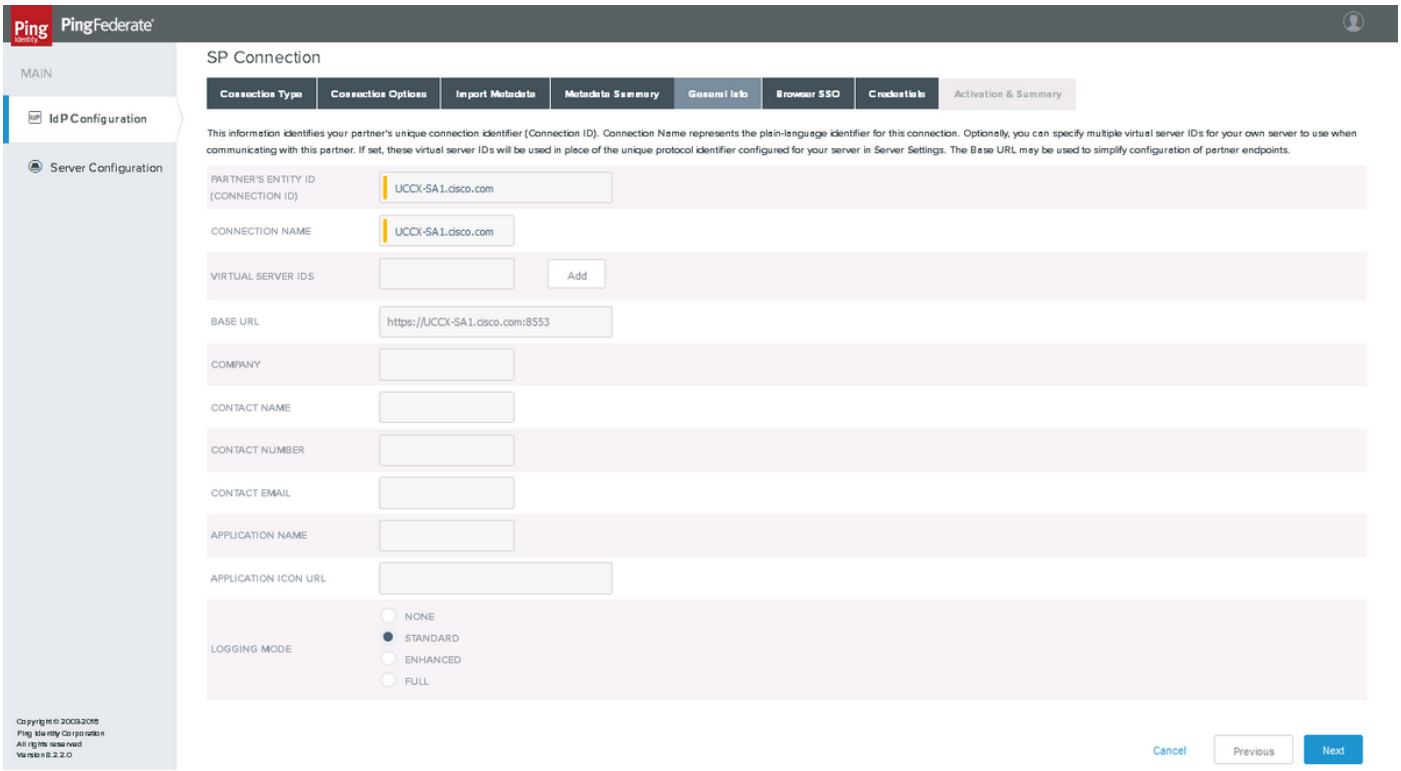
다운로드한 xml 파일을 선택하고 다음을 클릭합니다.

메타데이터 요약



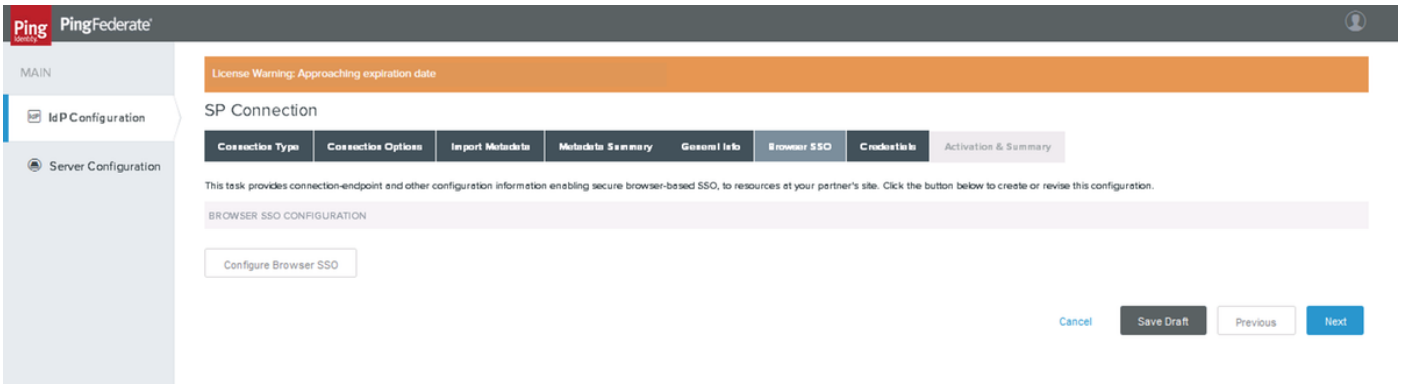
Next(다음)를 클릭합니다.

general info



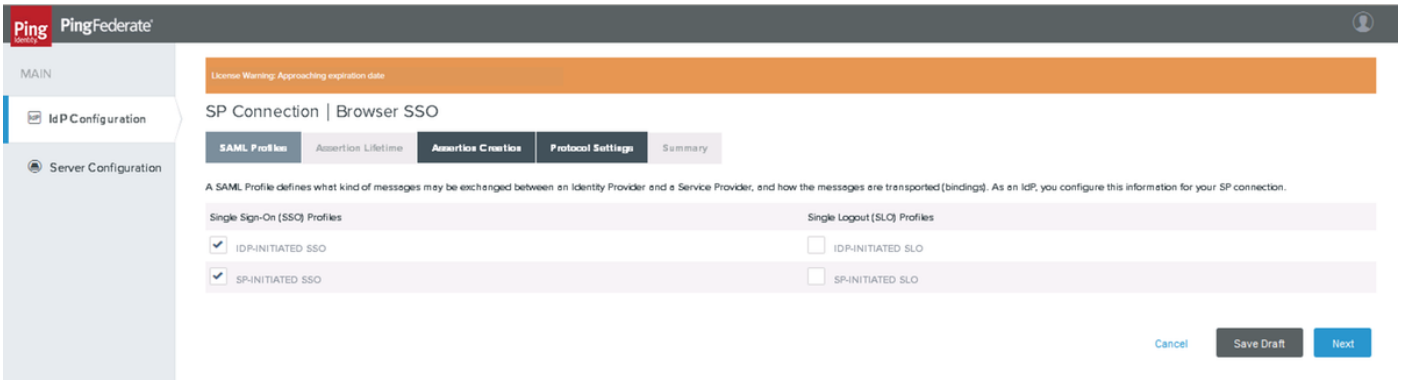
Next(다음)를 클릭합니다.

브라우저 SSO



브라우저 SSO 구성을 클릭합니다

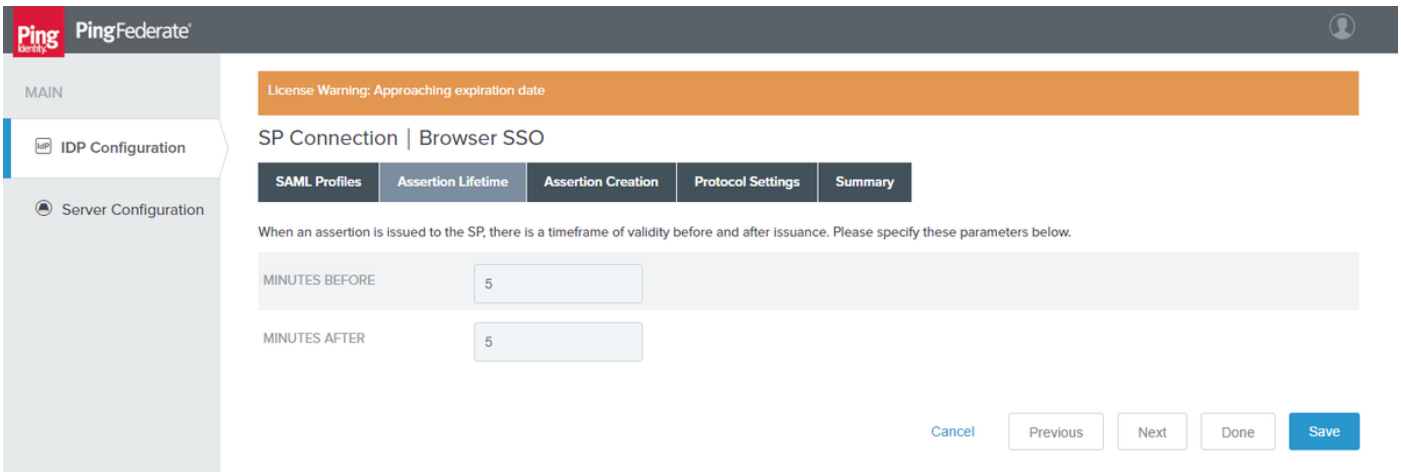
SAML(Security Assertion Markup Language) 프로파일



Next(다음)를 클릭합니다.

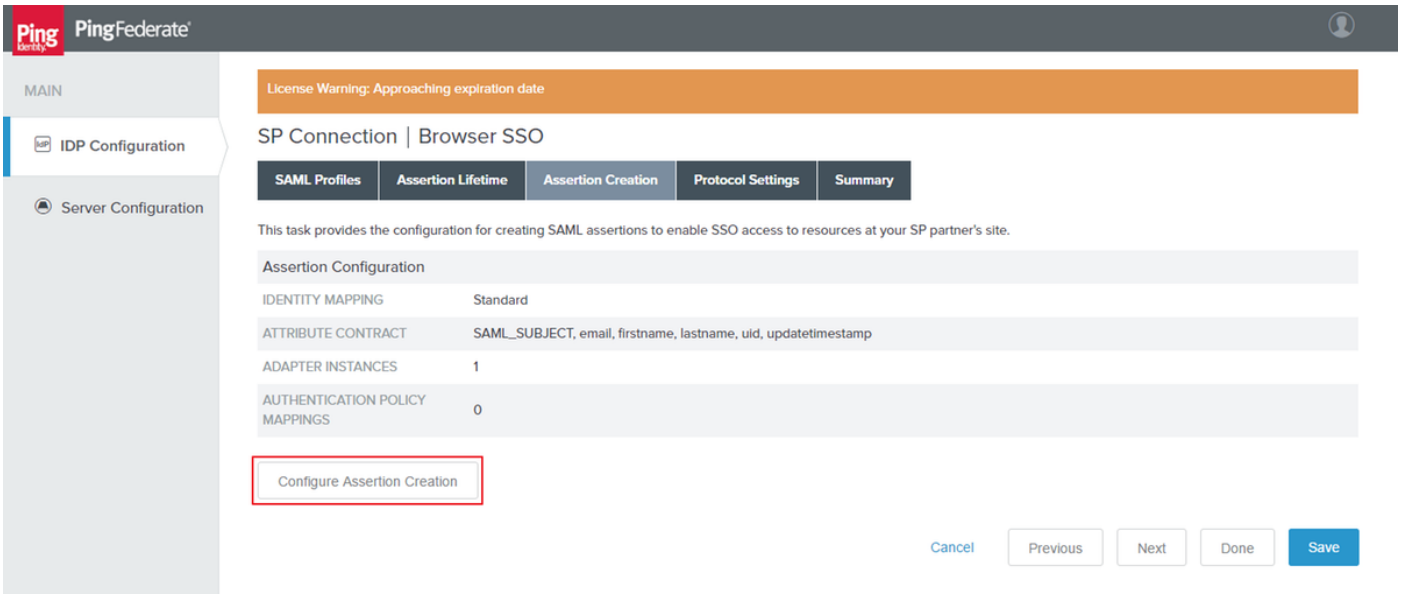
참고: SLO(Single Logout)는 11.6의 Cisco Id(Identity Service)에서 지원되지 않으며 선택되지 않습니다.

어설션 수명



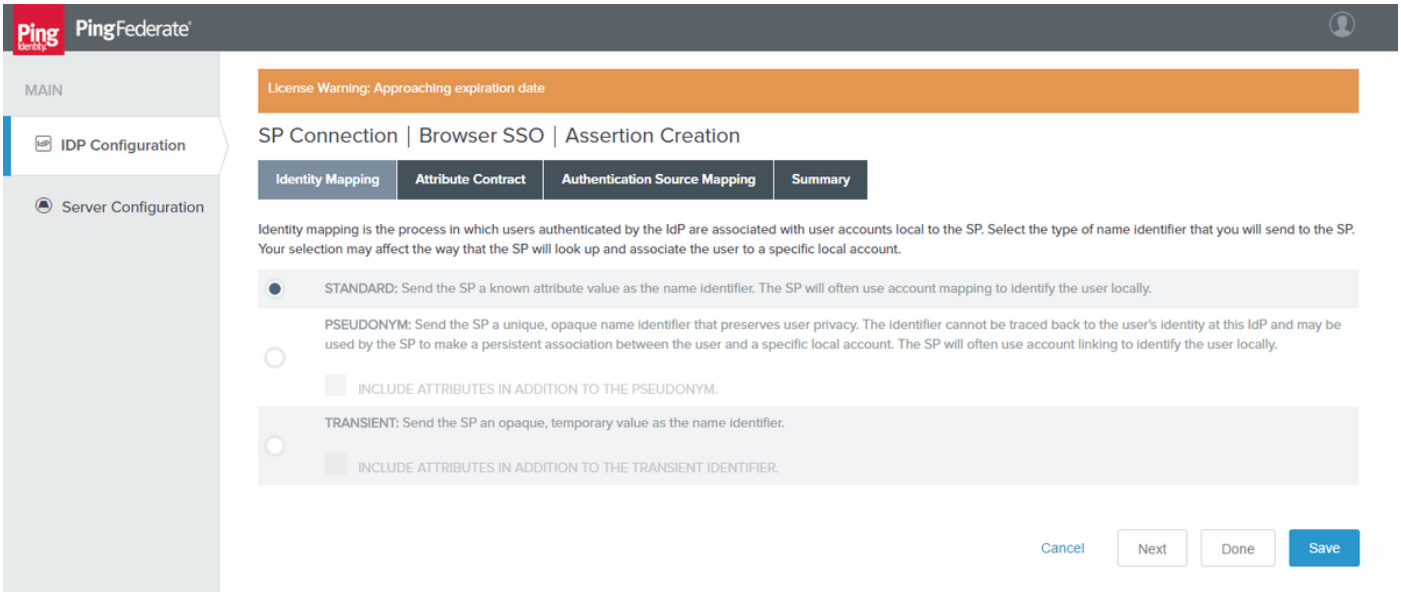
Next(다음)를 클릭합니다.

어설션 생성



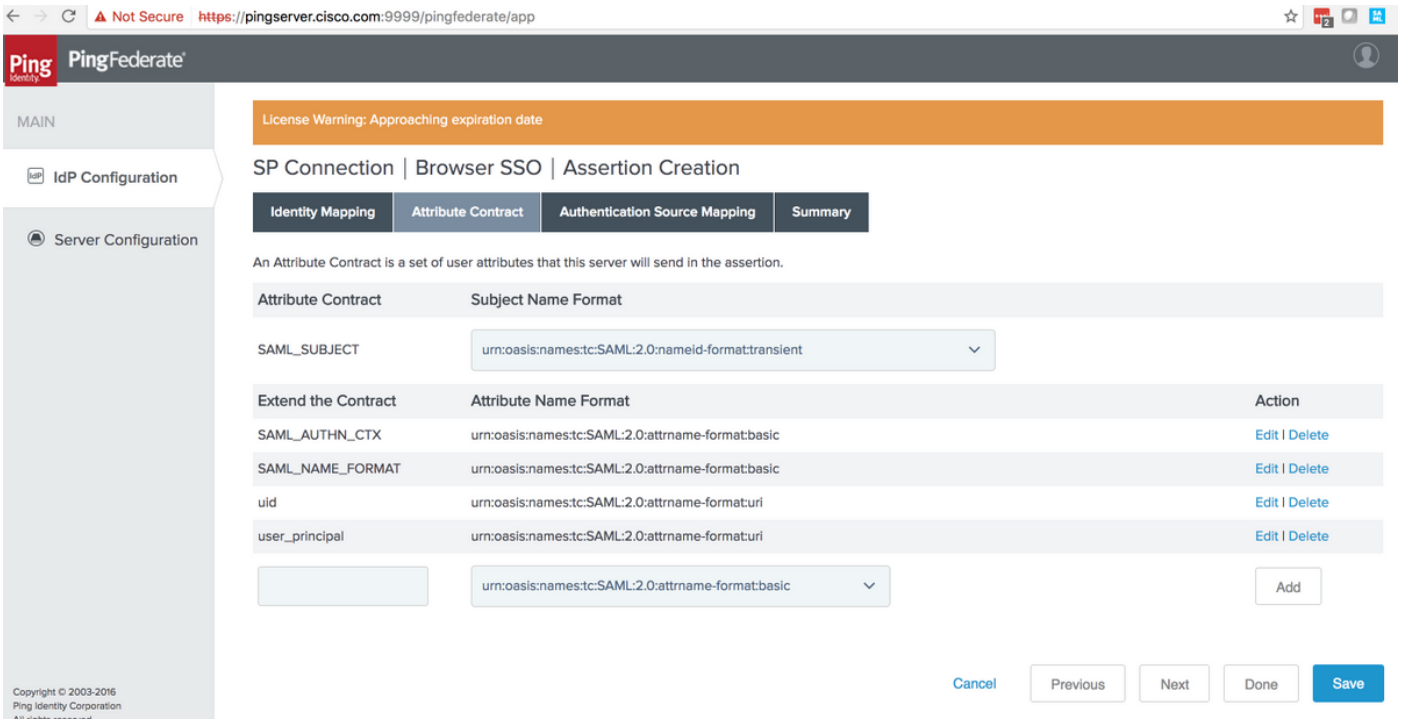
Configure Assertion Creation(어설션 생성 구성)을 클릭합니다

ID 매핑



Next(다음)를 클릭합니다.

속성 계약



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

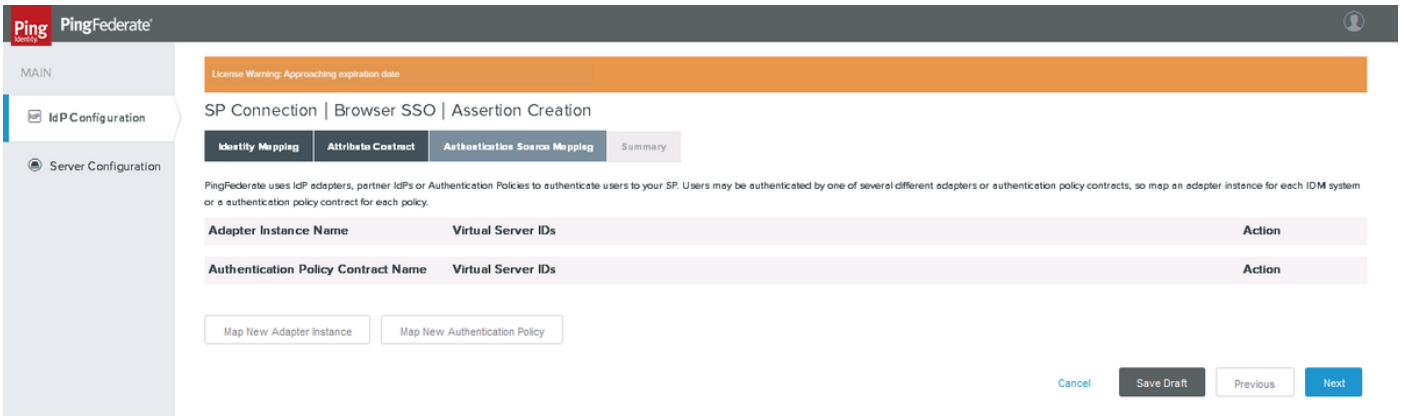
속성 계약	목적
SAML_제목	PingFederate 검색 필터에서 매핑된 값이 충족되는지 확인하는 데 사용됩니다.
SAML_AUTHN_CTX	'PasswordProtectedTransport' 인증 내용을 나타내기 위해 SAML 응답에 사용됩니다.
SAML_이름_형식	SAML 2.0 임시 이름 ID 형식을 나타내기 위해 SAML 응답에 사용됩니다.
uid	Cisco Id에서 인증된 사용자를 식별하는 데 사용
사용자_계정	Cisco Id에서 인증된 사용자의 전체 이름(예: id + 도메인)을 식별하는 데 사용됩니다.

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.

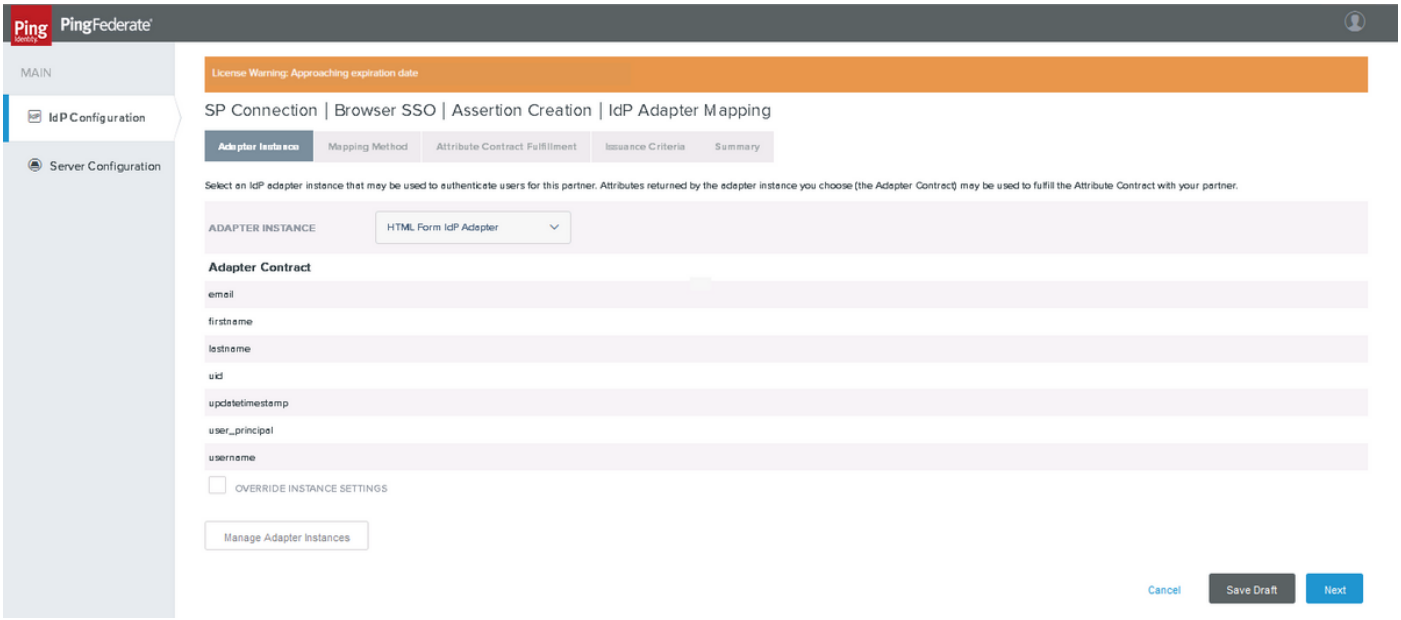
임시 SSO를 이름 식별자로 사용하려면 saml2-subject-name-formats 섹션에 xml 항목을 추가합니다. <con:item name="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">urn:oasis:names:tc:SAML:2.0:nameid-format:transient</con:item>

Next(다음)를 클릭합니다.

인증 소스 매핑

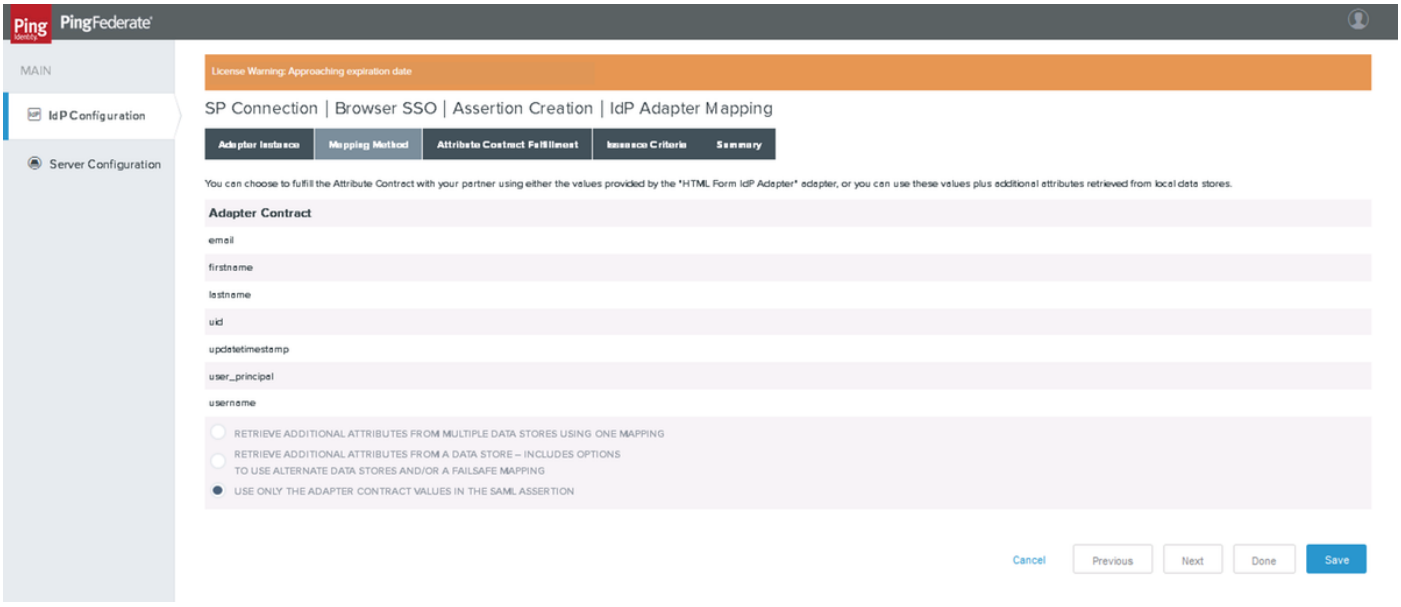


Map New Adapter Instance(새 어댑터 인스턴스 매핑)를 클릭합니다



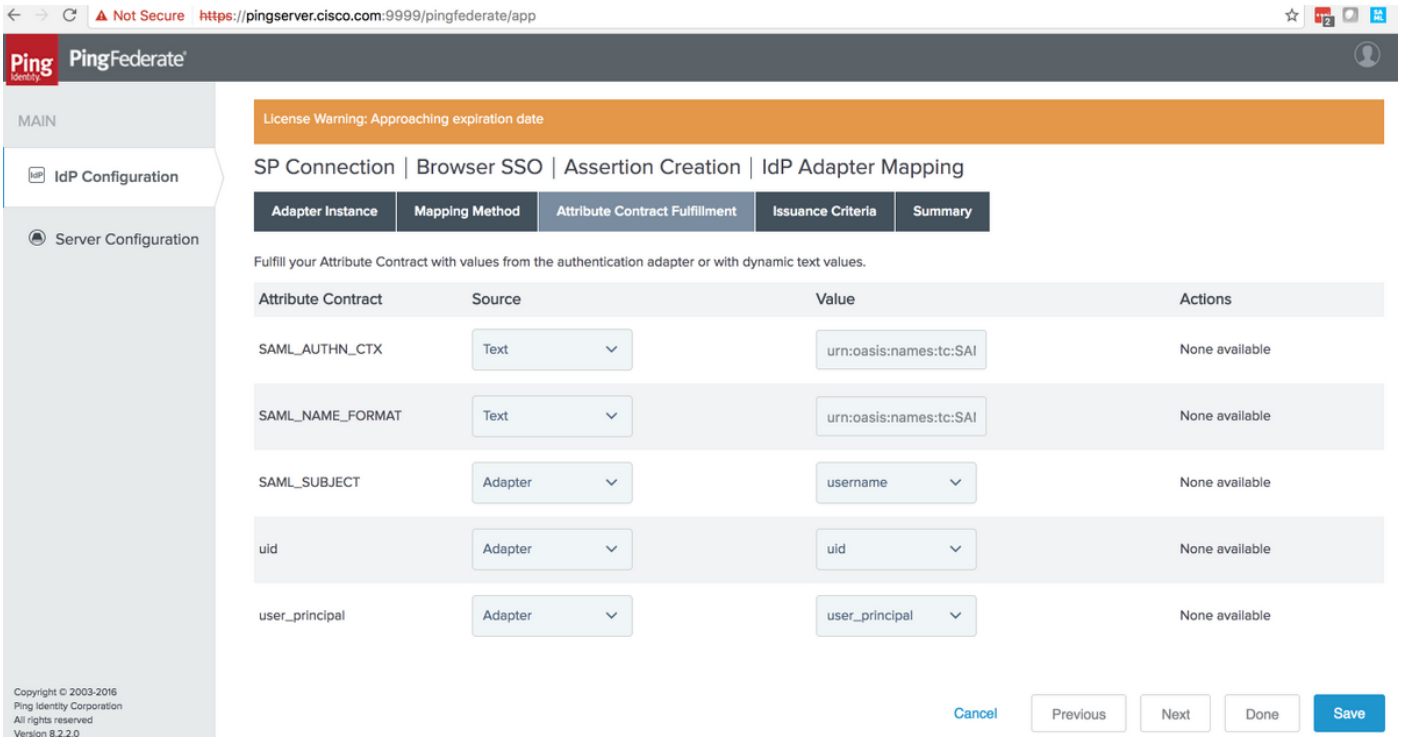
이전에 만든 HTML 양식 IdP 어댑터를 매핑합니다. Next(다음)를 클릭합니다.

매핑 방법



Next(다음)를 클릭합니다.

계약 이행 속성



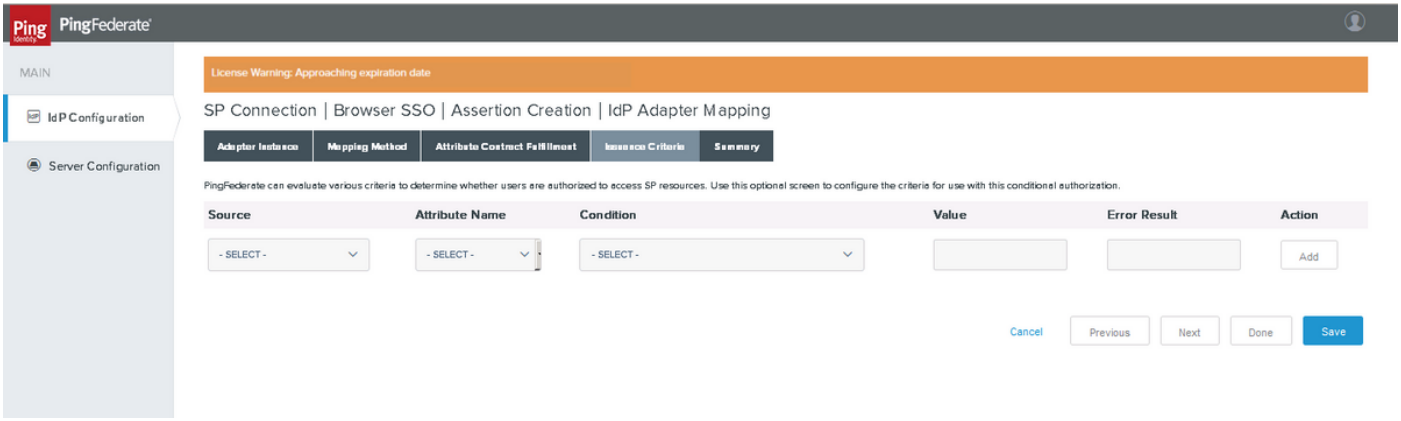
값이 로 설정되어 있는지 확인합니다.

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	어댑	사용자_계정

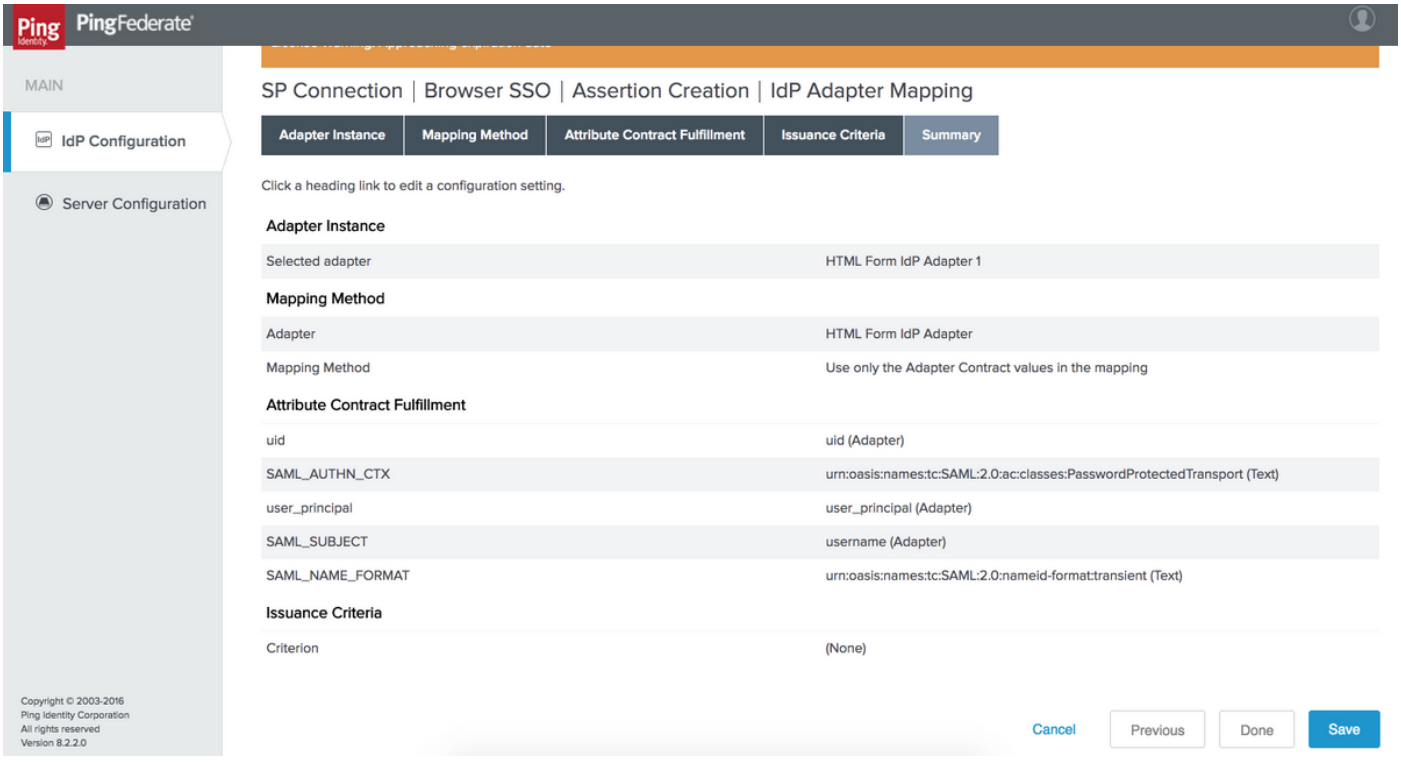
속성 계약	소스	가치

Next(다음)를 클릭합니다.

발급 기준

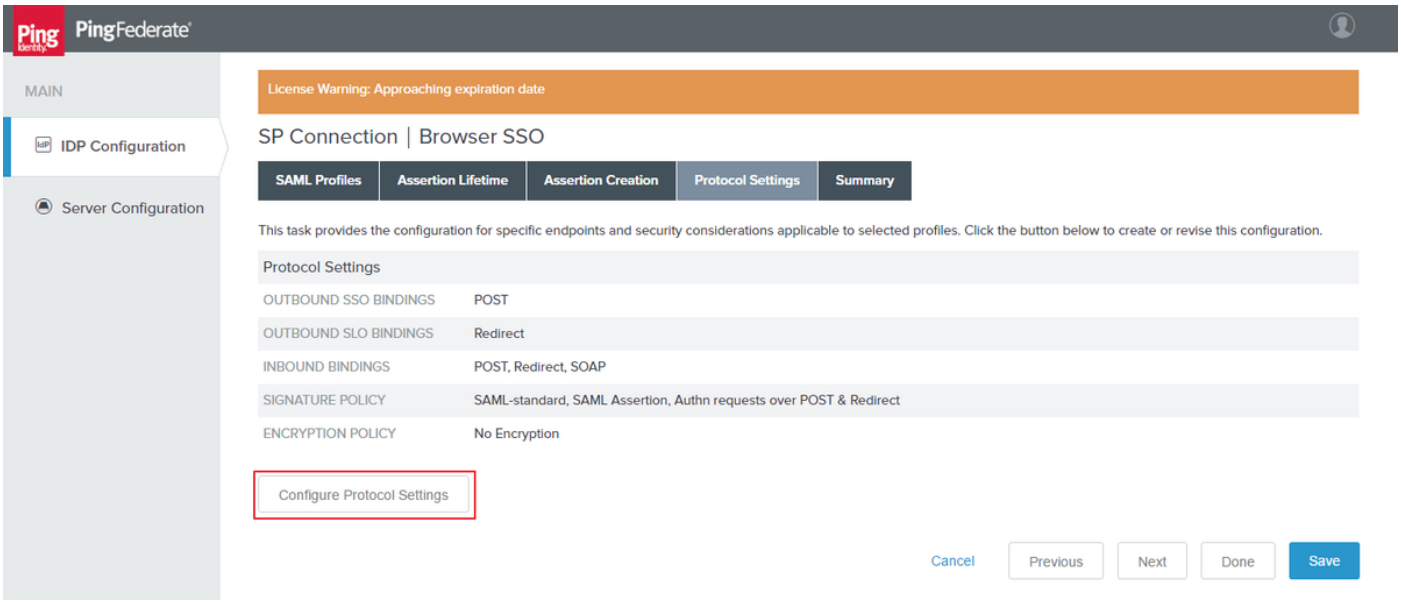


요약



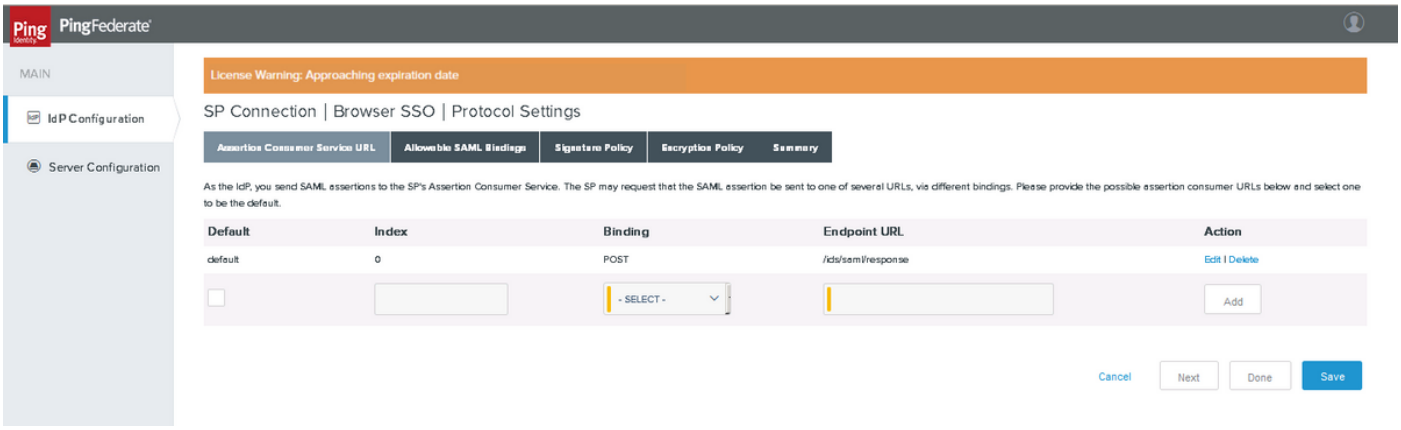
설정을 확인하고 Done(완료)을 클릭합니다.

프로토콜 설정



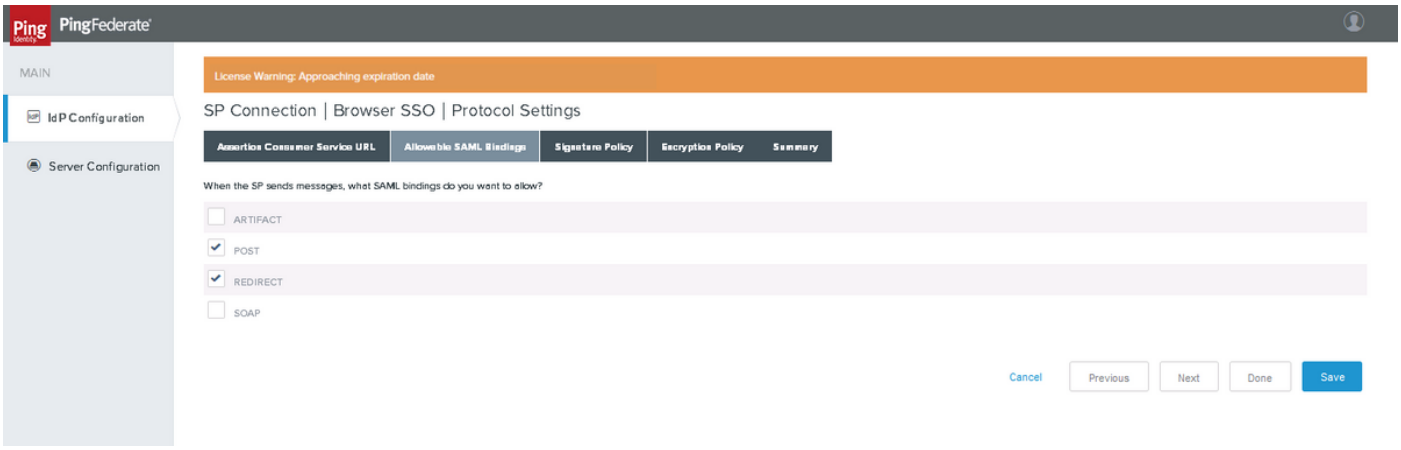
Configure Protocol Settings를 클릭합니다

어설션 소비자 서비스 URL



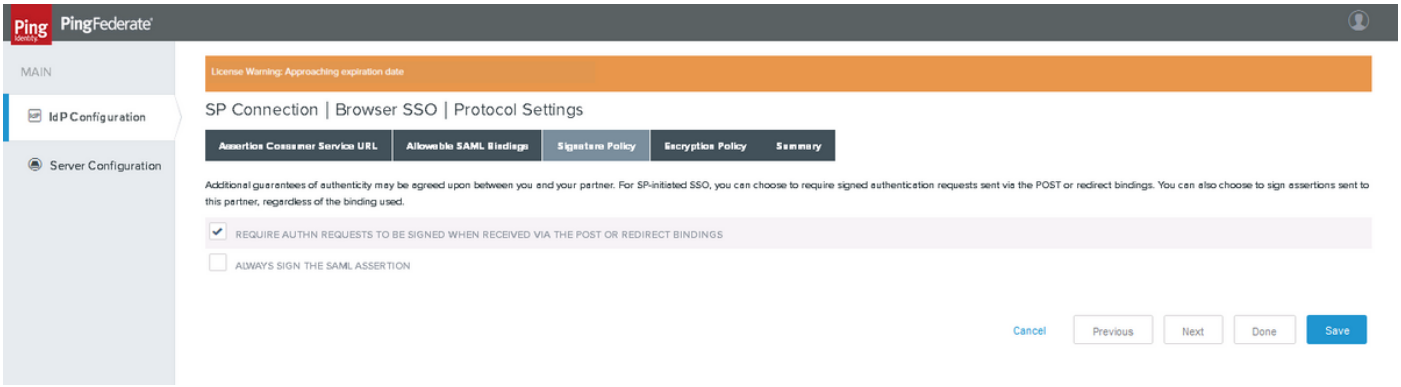
POST 바인딩 SSO 끝점을 추가합니다. Next(다음)를 클릭합니다.

허용 가능한 SAML 바인딩



Next(다음)를 클릭합니다.

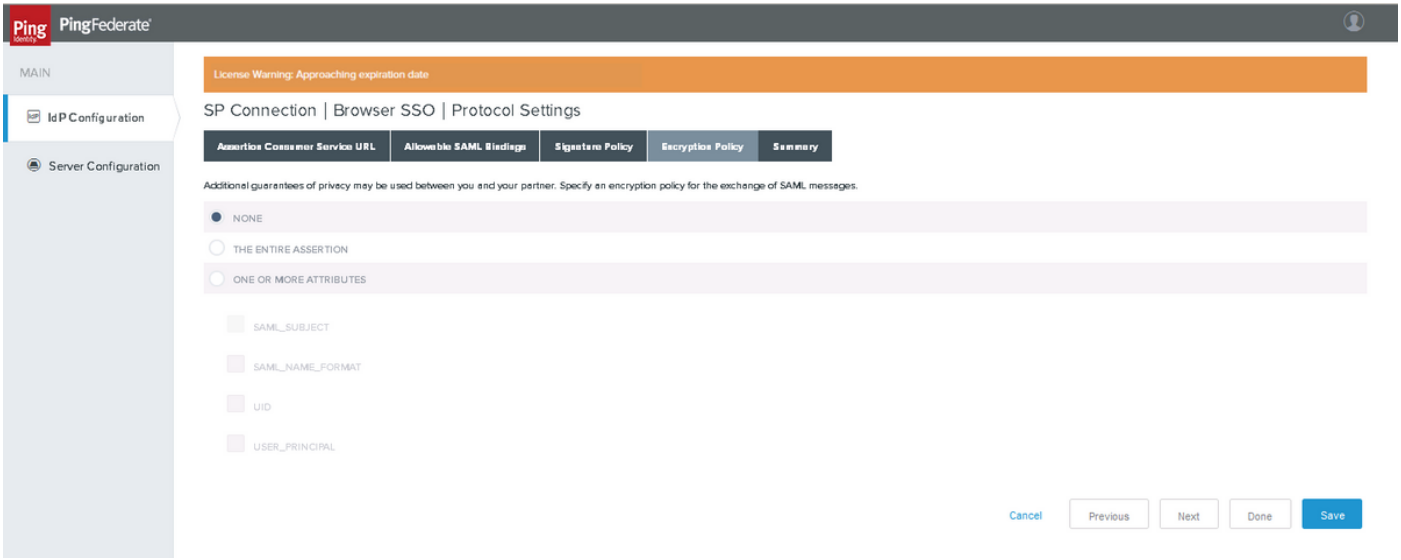
서명 정책



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.

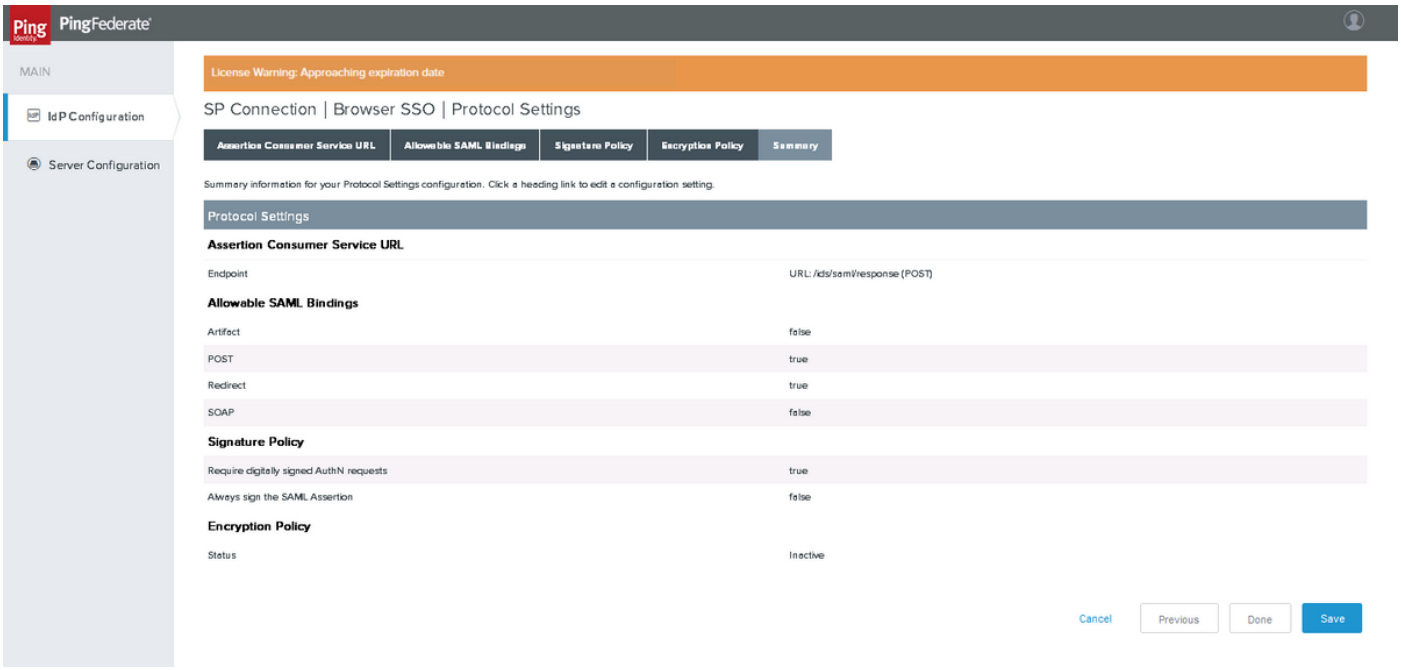
암호화 정책



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

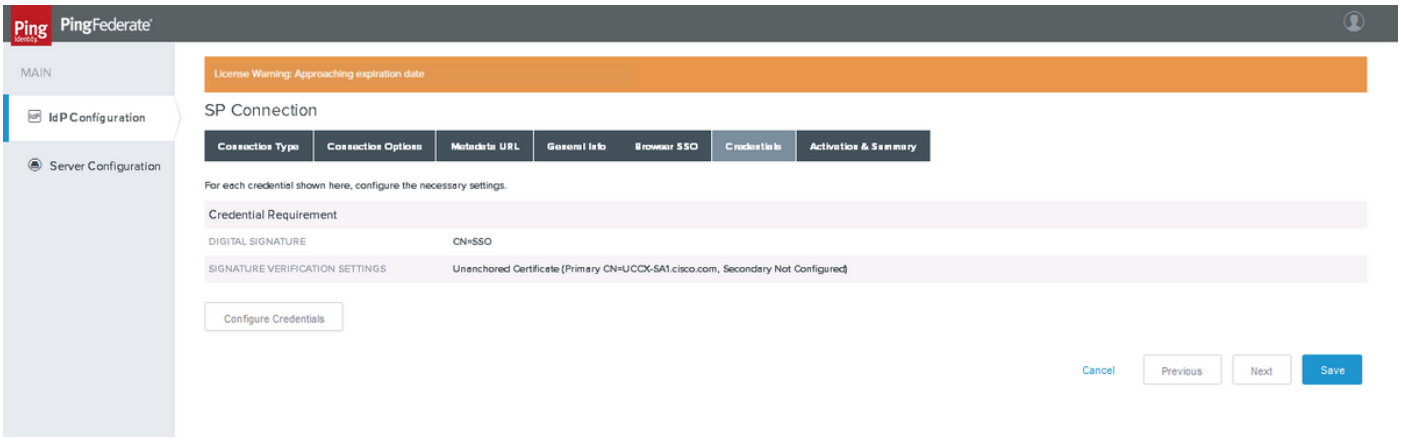
Next(다음)를 클릭합니다.

요약



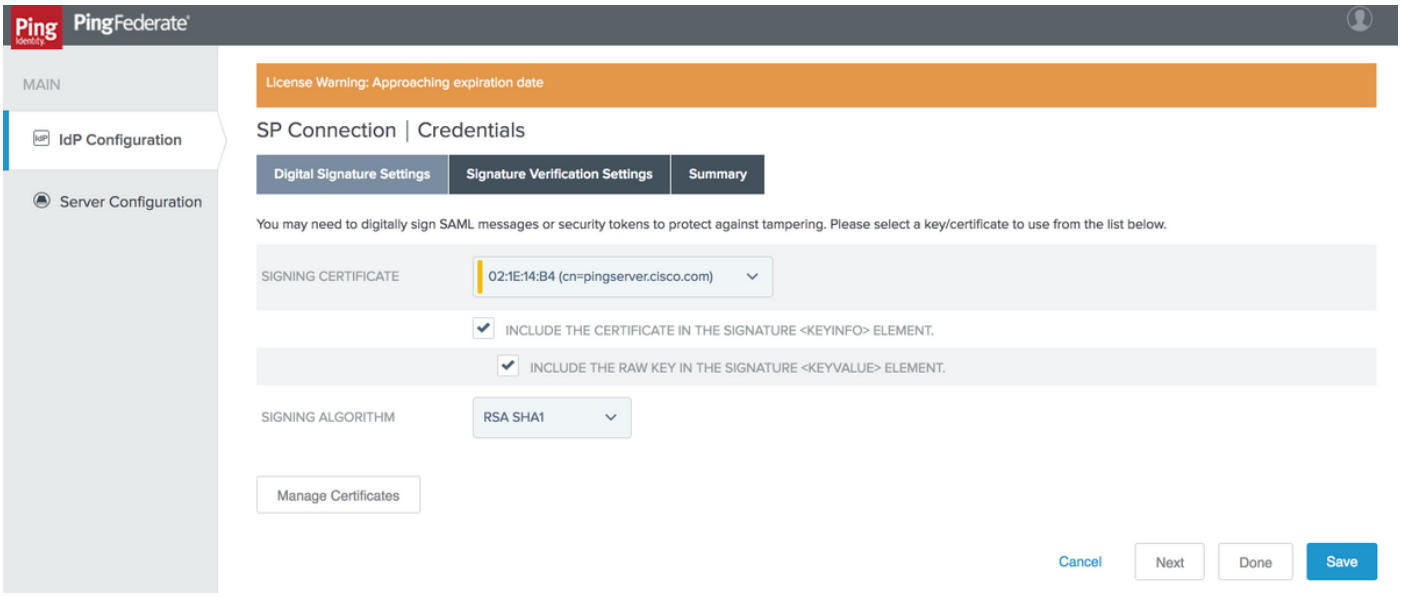
설정을 확인하고 Done(완료)을 클릭합니다.

자격 증명



Configure Credentials(자격 증명 구성)를 클릭합니다.

디지털 서명 설정

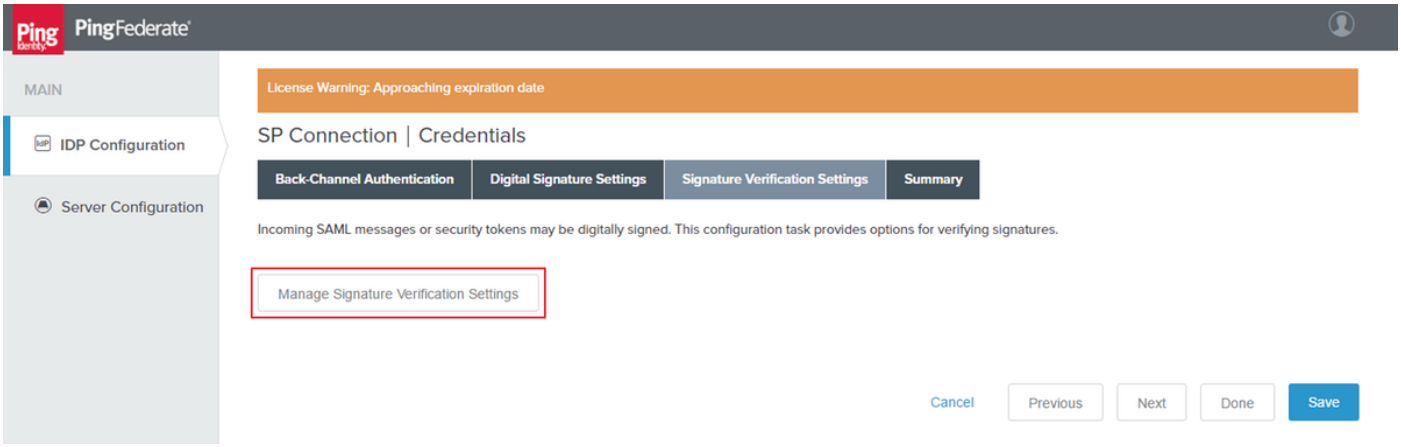


SIGNING CERTIFICATE CREATED EARLY(이전에 생성된 서명 인증서)를 선택합니다. 그렇지 않은 경우 Manage Certificates를 클릭하여 인증서를 생성할 수 있습니다.

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

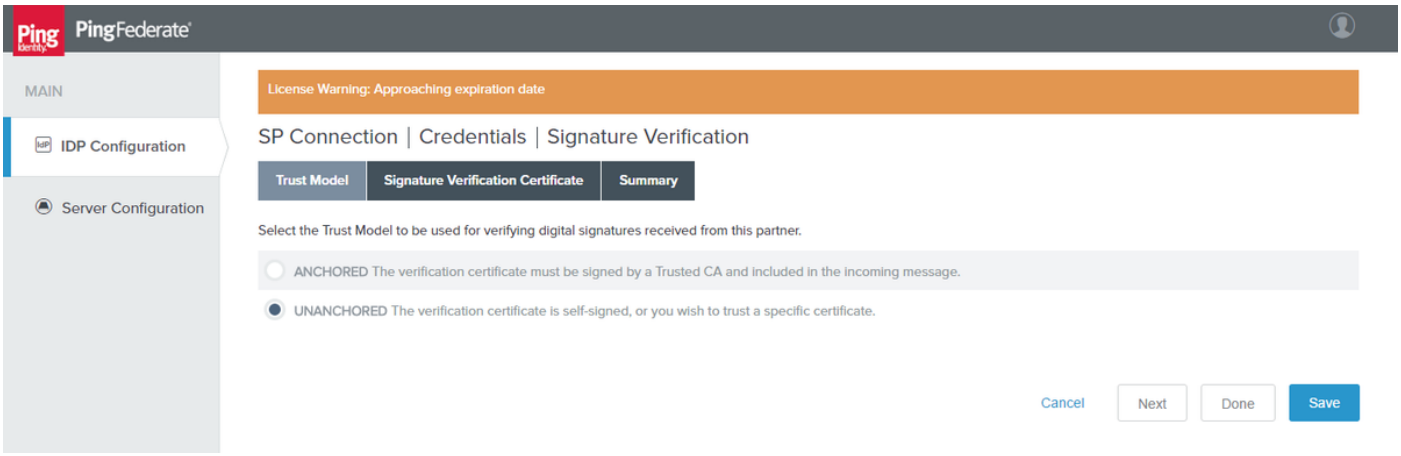
Next(다음)를 클릭합니다.

서명 확인 설정



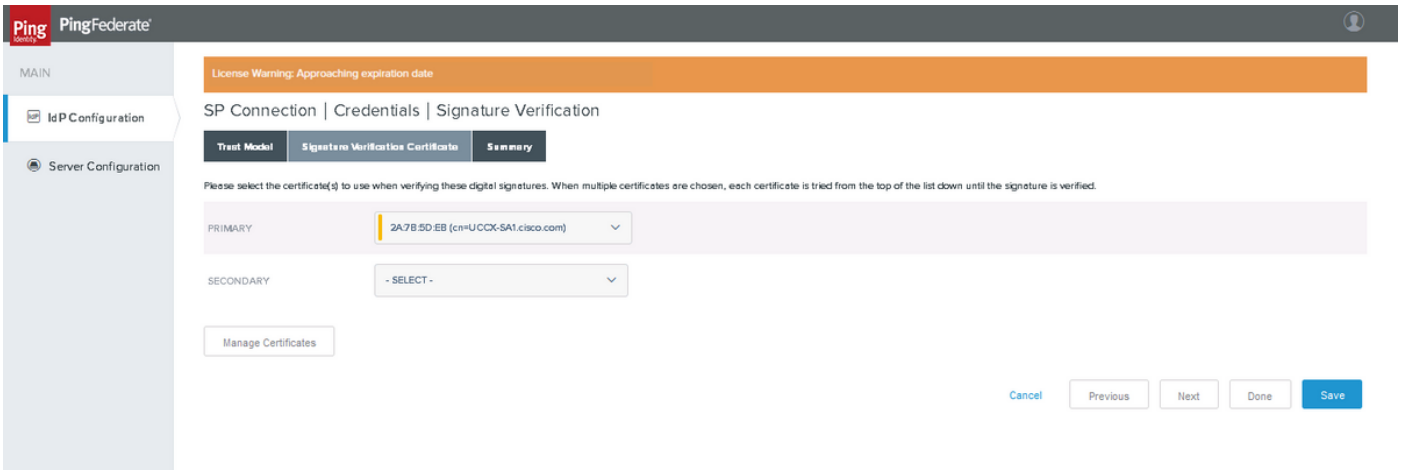
Manage Signature Verification Settings(서명 확인 설정 관리)를 클릭합니다.

신뢰 모델

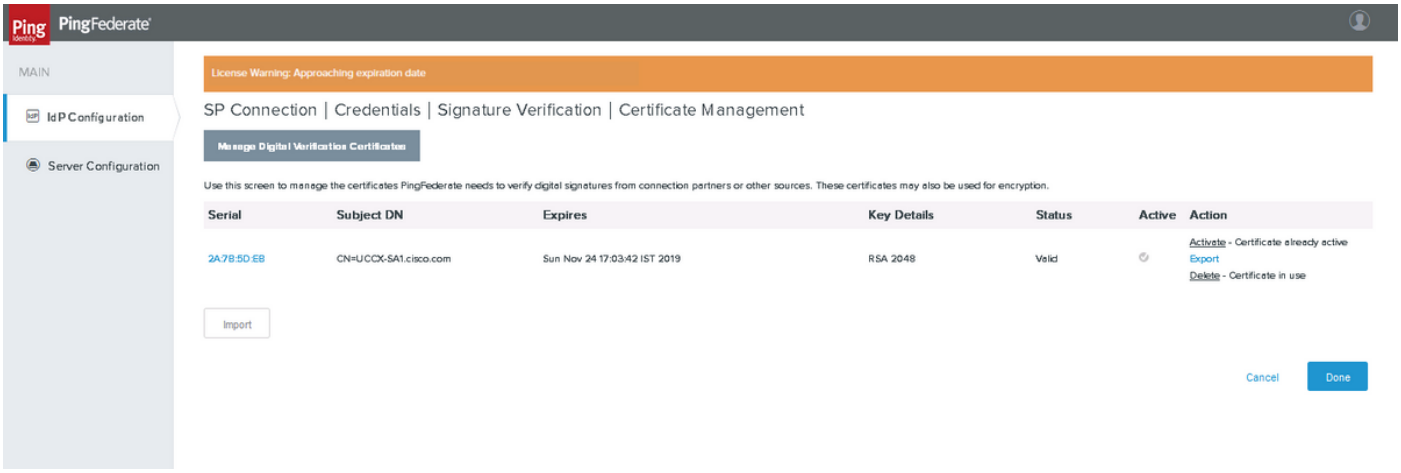


Next(다음)를 클릭합니다.

서명 확인 인증서

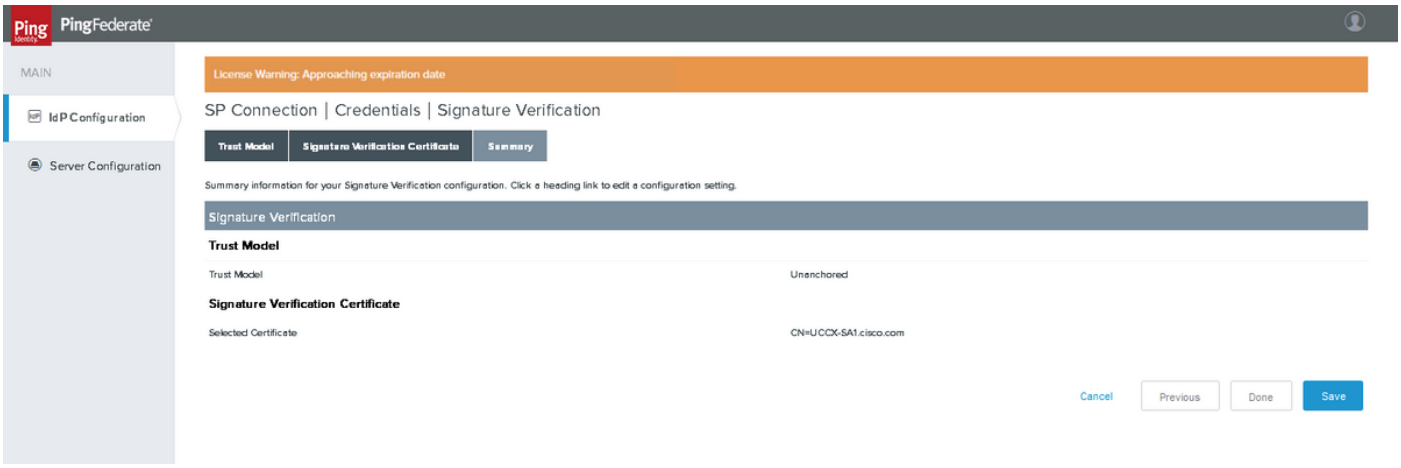


SP에서 인증서를 가져오려면 Manage Certificates를 클릭합니다.



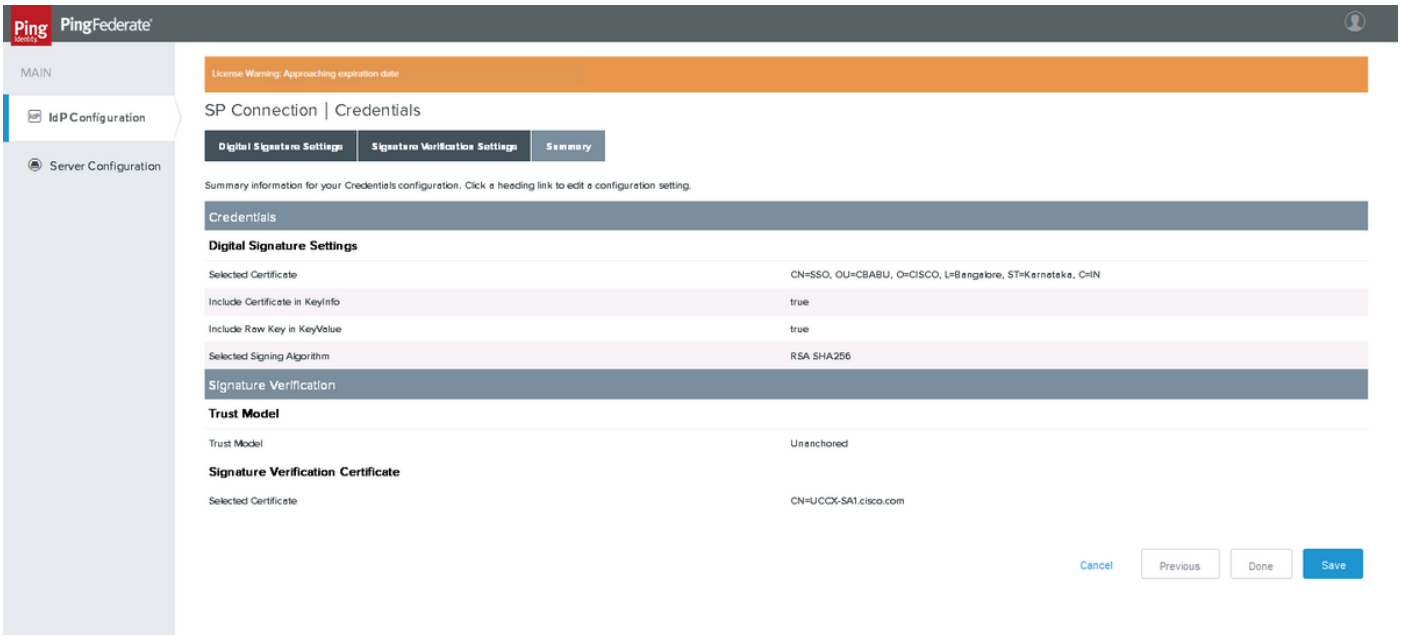
인증서를 가져오려면 Import(가져오기)를 클릭합니다.

요약



Done(완료)을 클릭합니다

요약



요약을 확인하고 Done(완료)을 클릭합니다

활성화 및 요약

PingFederate

MAIN

IdP Configuration

Server Configuration

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
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

PingFederate

MAIN

IdP Configuration

Server Configuration

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

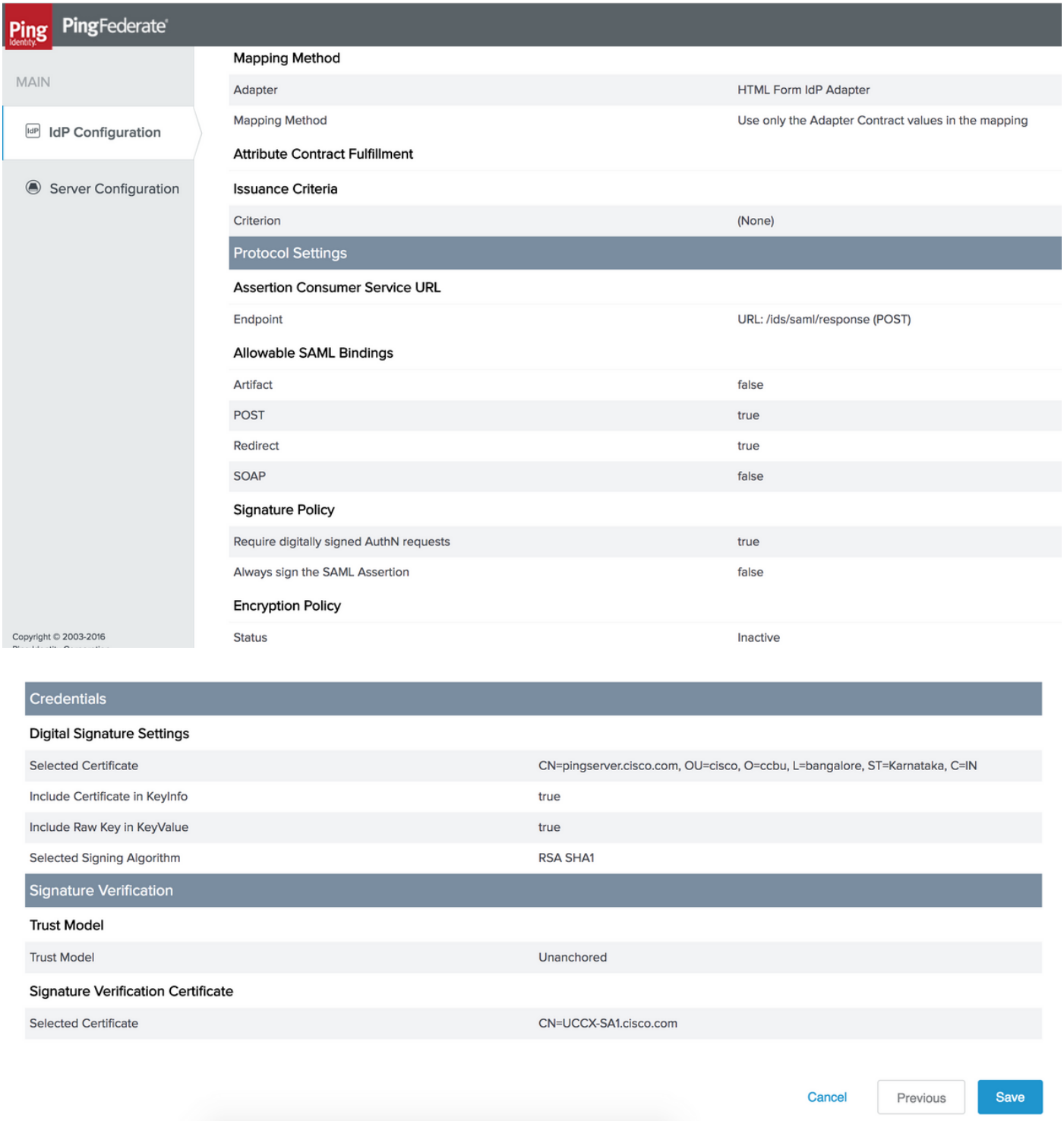
Enable Transient Identifier	true
Include additional attributes	false

Authentication Source Mapping

Adapter instance name	HTML Form IdP Adapter 1

Adapter Instance

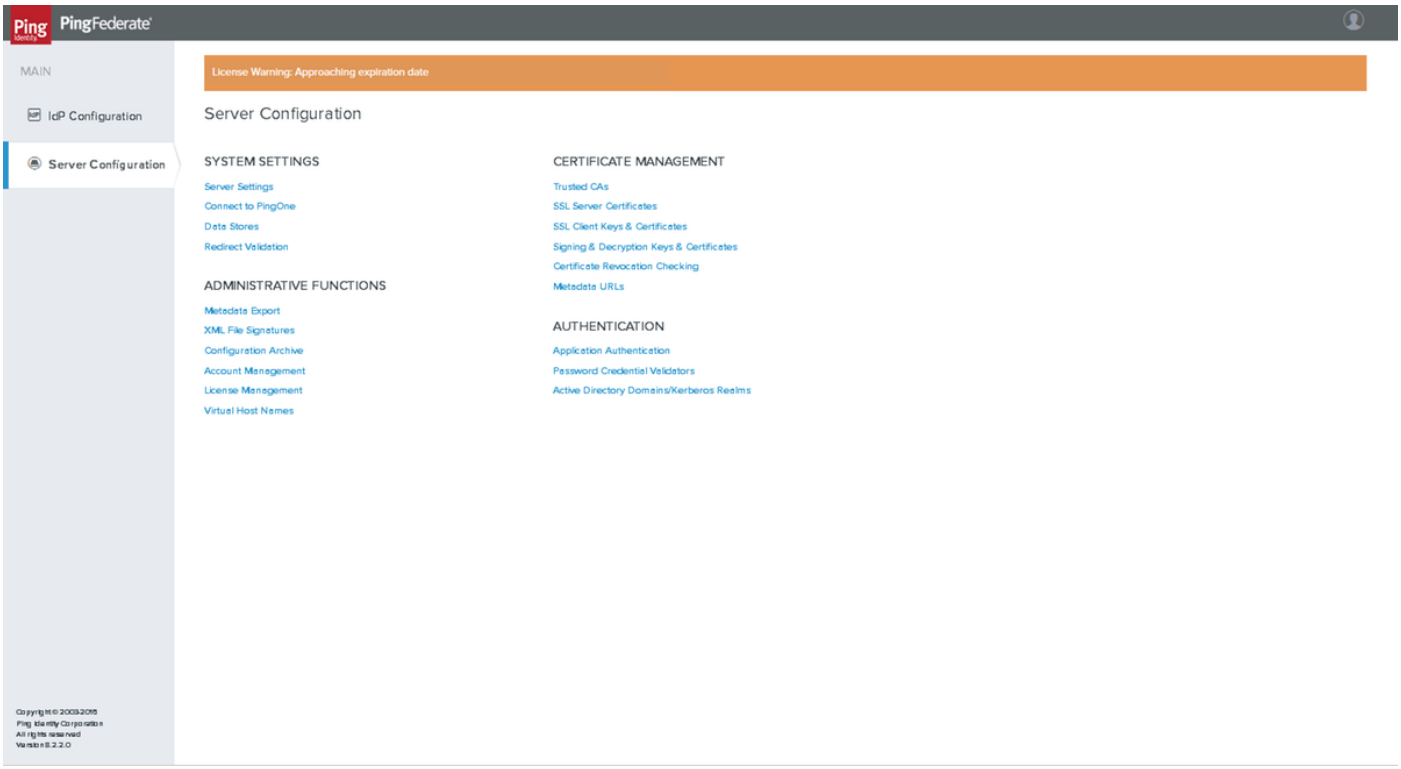
Selected adapter	HTML Form IdP Adapter 1



요약을 확인하고 저장을 클릭합니다.

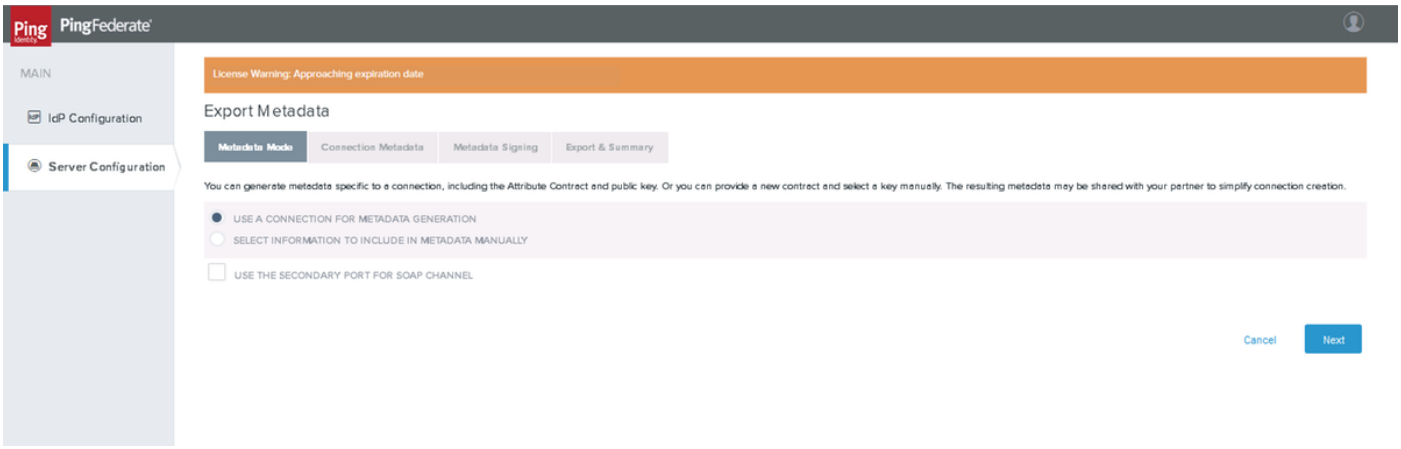
PingFederate 메타데이터 내보내기

메타데이터 내보내기



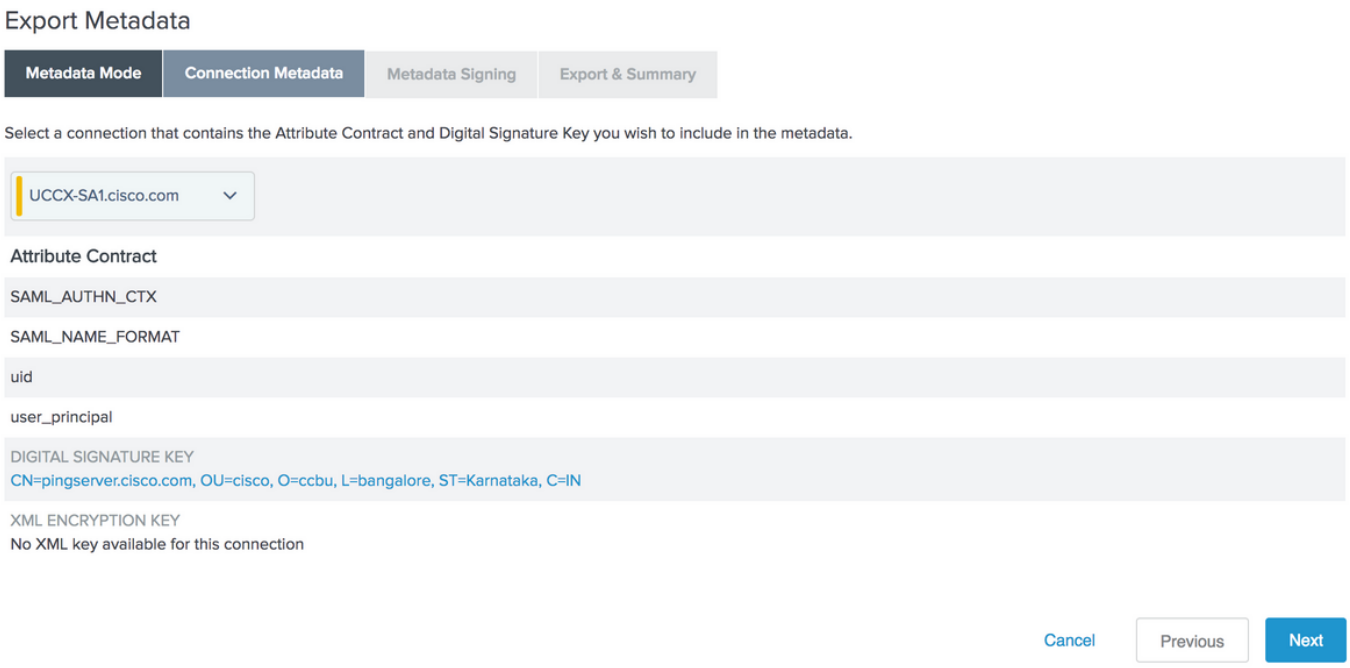
메타데이터 모드

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



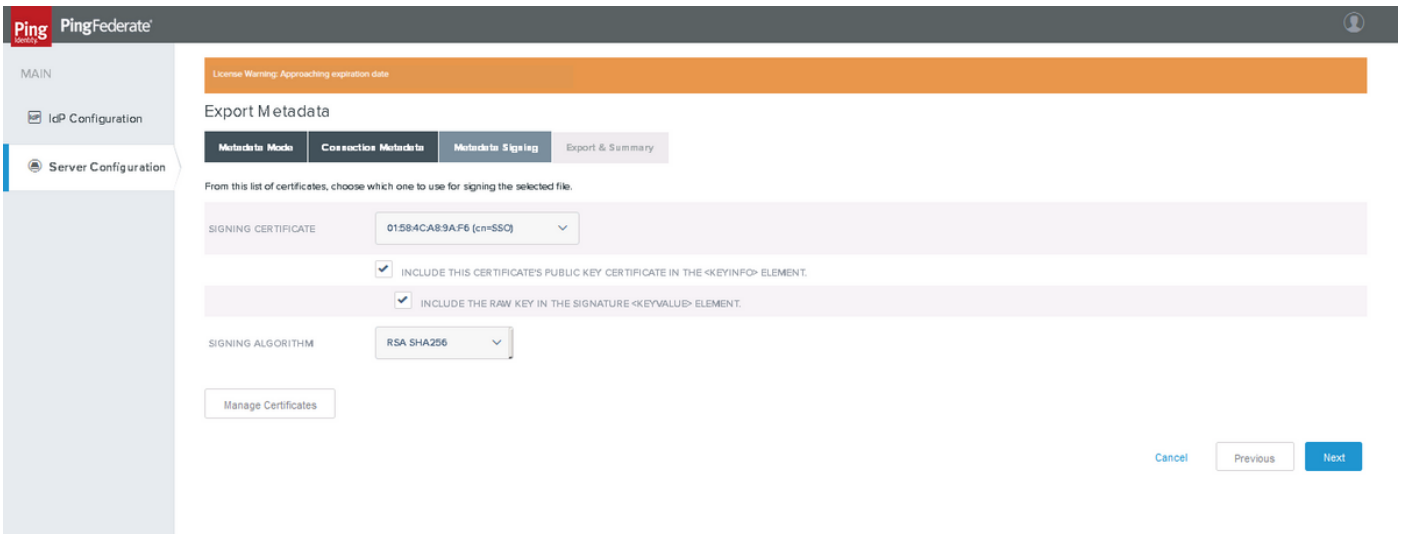
Next(다음)를 클릭합니다.

연결 메타데이터



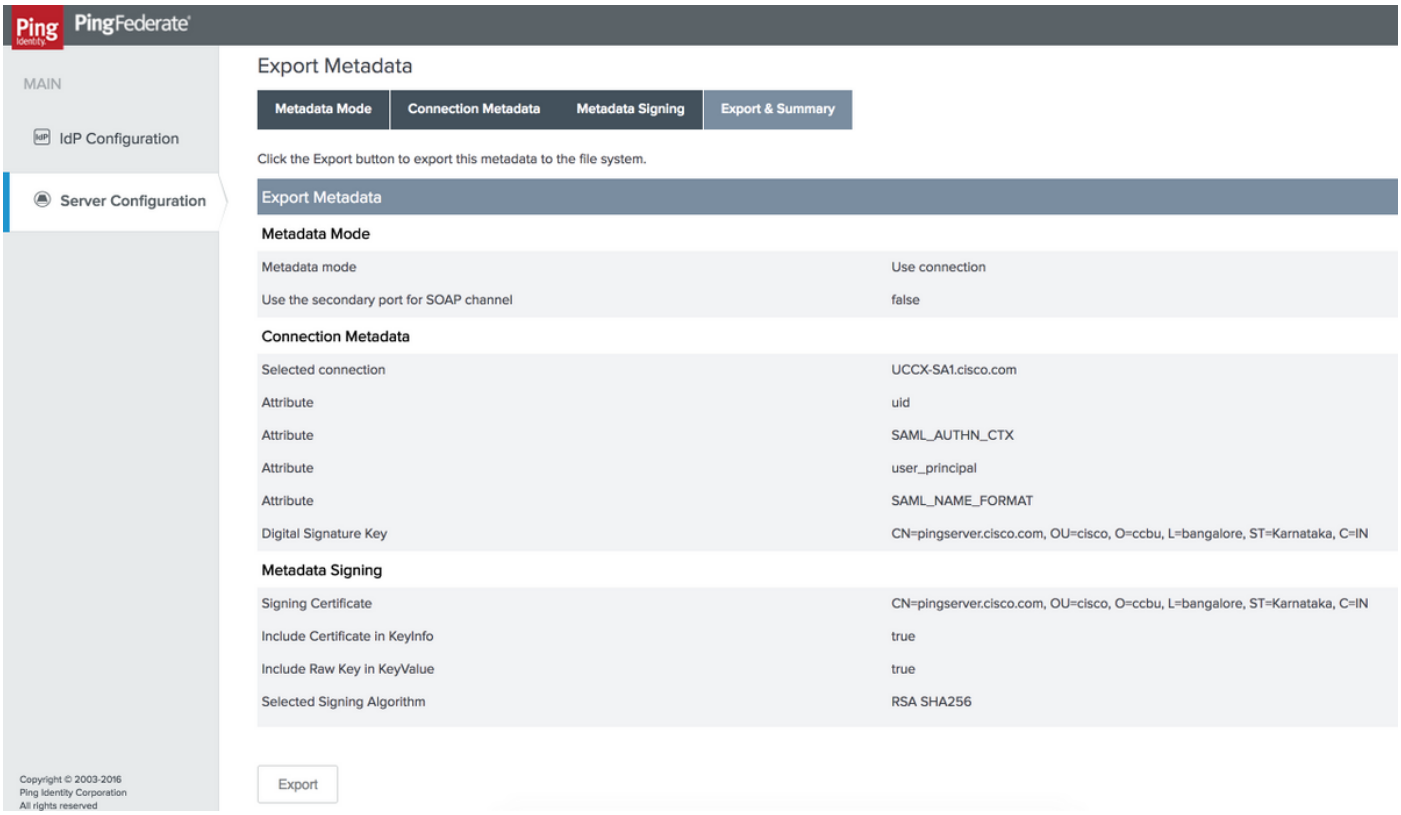
생성한 SP 접속을 선택하고 Next(다음)를 클릭합니다.

메타데이터 서명



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

내보내기 및 요약



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

문제 해결

문제	툴	가능한 원인
Id 관리 페이지에서 PingFederate 메타데이터 업로드가 실패함	텍스트 파일 편집기	메타데이터 XML 파일에 'md' 네임스페이스 항목이 없는지 확인하십시오.

문제	툴	가능한 원인
SAML 흐름 실패	SAML 트레이서	'StatusCode'가 'Success'를 나타내는지 확인(예: <samlp :StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /> • 그렇지 않은 경우 'Requester' 또는 'Responder'를 나타내는지 확인합니다. ◦ '요청자'는 SAML 요청에 문제가 있음을 의미합니다(예: Cisco Id가 요청을 제대로 전송하지 않음). /opt/cisco/ids/log/ 폴더 아래의 Cisco IdS 로그를 확인하십시오. ◦ 'Responder'는 IdP 문제를 의미하므로 PingFederate 로그를 확인하십시오.
SAML 흐름 실패	SAML 트레이서	<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 트레이서	<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 트레이서	Cisco Id 또는 PingFederate 로그에서 'Invalid Signature' 메시지를 확인합니다. 확인된 경우 Id 및 PingFederate 전체에서 메타데이터 트러스트를 다시 설정합니다.
SAML 흐름 실패	SAML 트레이서	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.