Cisco Identity Service(Id)용 OpenAM IdP(Identity Provider)를 설치하고 구성하여 SSO를 활성화합니다

목차

소개

이 문서에서는 SSO(Single Sign On)를 활성화하기 위한 OpenAM IdP(Identity Provider)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.

참고: 이 문서에서는 Cisco Id(Identity Service) 및 IdP(Identity Provider)와 관련된 컨피그레이션을 참조합니다. 이 문서에서는 스크린샷과 예에서 UCCX를 참조하지만, Cisco ID 서비스(UCCX/UCCE/PCCE) 및 IdP와 관련하여 컨피그레이션이 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

참고: 이 문서에서는 OpenAM 릴리스 10.0.1을 SSO 자격 증명의 일부로 참조합니다

시스템 요구 사항

운영 체제	Java 환경	웹 애플리케이션 컨테이너 요구 사항	지원되는 브라우저	데이터 저장소 요구 사항	최소 하드웨어 요구 사항

• Microsoft Windows Server 2003, 2008 R2 • Linux 2.6, 3.0 • Oracle Solaris 10	OpenAM 릴리스 10.0.1에는 Java Development Kit 1.6, 1.6.0_10 이상이 필요합니다. ForgeRock에서는 보안 수정 사항으로 인해 버전 1.6.0_27 이상을 사용할 것을 권장합니다. ForgeRock은 주로 Oracle Java SE JDK를 사용하여 이 OpenAM 릴리스를 테스트했습니다. OpenAM Java SDK는 Java Development Kit 1.5 또는 1.6을 지원합니다.	• Apache Tomcat 6.0.x, 7.0.x • 글래스피시 v2 • JBoss Enterprise Application Platform 4.x, 5.x • JBoss Application Server 7.x • 제 7 부두 • Oracle WebLogic Server 11g • Oracle WebLogic Server 12c 루트가 아닌 사용자로 실행하는 경우 웹 애플리케이션 컨테이너는 자체 홈 디렉토리에 쓸 수 있어야 합니다. 여기서 OpenAM은 컨피그레이션 파일을 저장합니다.	• Chrome and Chromium 16 이상 • Firefox 3.6 이상 • Internet Explorer(버전 7 이상) • Safari 5 이상	• 포지락 오픈DJ • Microsoft Active Directory • IBM Tivoli 디렉토리 서버 • OpenDS • Oracle Directory Server Enterprise 버전	• OpenAM용 1GB 무료 RAM 필요한 소프트웨어의 조합에 지원되는 모든 하드웨어에 OpenAM을 구축할 수 있습니다.

Install

OpenAM 소프트웨어 받기

- https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%201서 OpenAM 10.0.1 릴리스 다운로드
- OpenAM 핵심 서비스의 각 릴리스에 대해 전체 패키지를 .zip 아카이브로, OpenAM .war 파일만 .zip 아카이브로, 관리 도구만 .zip 아카이브로 다운로드할 수 있습니다
- 전체 패키지의 아카이브의 압축을 풀면 README, 라이센스 파일 세트 및 디렉토리가 포함된 opensso 디렉토리가 제공됩니다

전제 조건

설치 전에 OpenAM 핵심 서비스에 필요한 사전 요구 사항 소프트웨어가 있는지 확인합니다.

- Java 6 런타임 환경
- 웹 애플리케이션 컨테이너로 Apache Tomcat 설치
- OpenAM 코어 서비스에는 최소 1GB의 JVM(Java Virtual Memory) 힙 크기와 256MB의 영구 생성 크기가 필요합니다. tomcat 애플리케이션 서버 --Xmx1024m -XX:MaxPermSize=256m 시작 전에 카탈리나 파일에서 JAVA_OPTS를 설정할 때 JVM 옵션을 적용합니다

예제 집합 JAVA_OPTS=%JAVA_OPTS% -Xmx1024m -XX:MaxPermSize=256m -Xms512m

- Microsoft Active Directory를 사용자 수가 적은 데이터 저장소로 설치합니다.

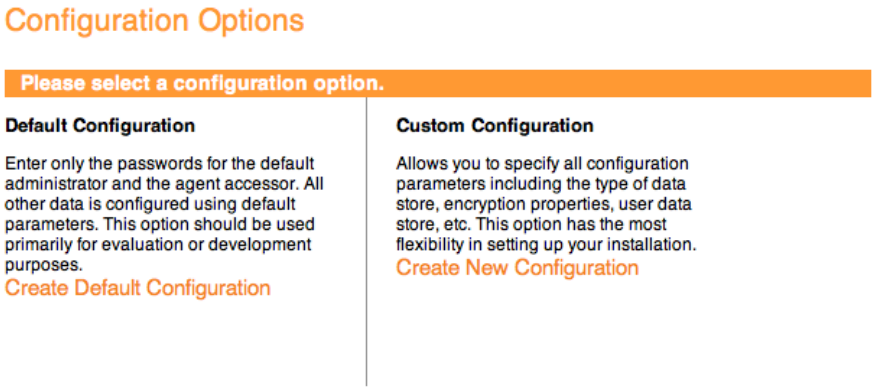
OpenAM 웹 응용 프로그램 설치

deployable-war/opensso.war 파일에는 opensso 디렉토리 아래의 모든 OpenAM 서버 구성 요소 및 샘플이 포함되어 있습니다.

Tomcat 컨테이너에 OpenAM 구축

opensso.war 파일을 tomcat 웹 애플리케이션이 저장된 디렉토리에 복사합니다. opensso.war 파일의 이름을 openam.war로 변경합니다. tomcat 서비스를 재시작합니다.

브라우저의 초기 컨피그레이션 화면(http://<FQHN>:8080/openam)을 확인합니다.



OpenAM 서비스 실행

Openam은 tomcat 서버에서 호스팅되는 간단한 웹 애플리케이션입니다. 따라서 tomcat 서버를 실행하기만 하면 OpenAM 웹 서비스에 액세스할 수 있습니다.

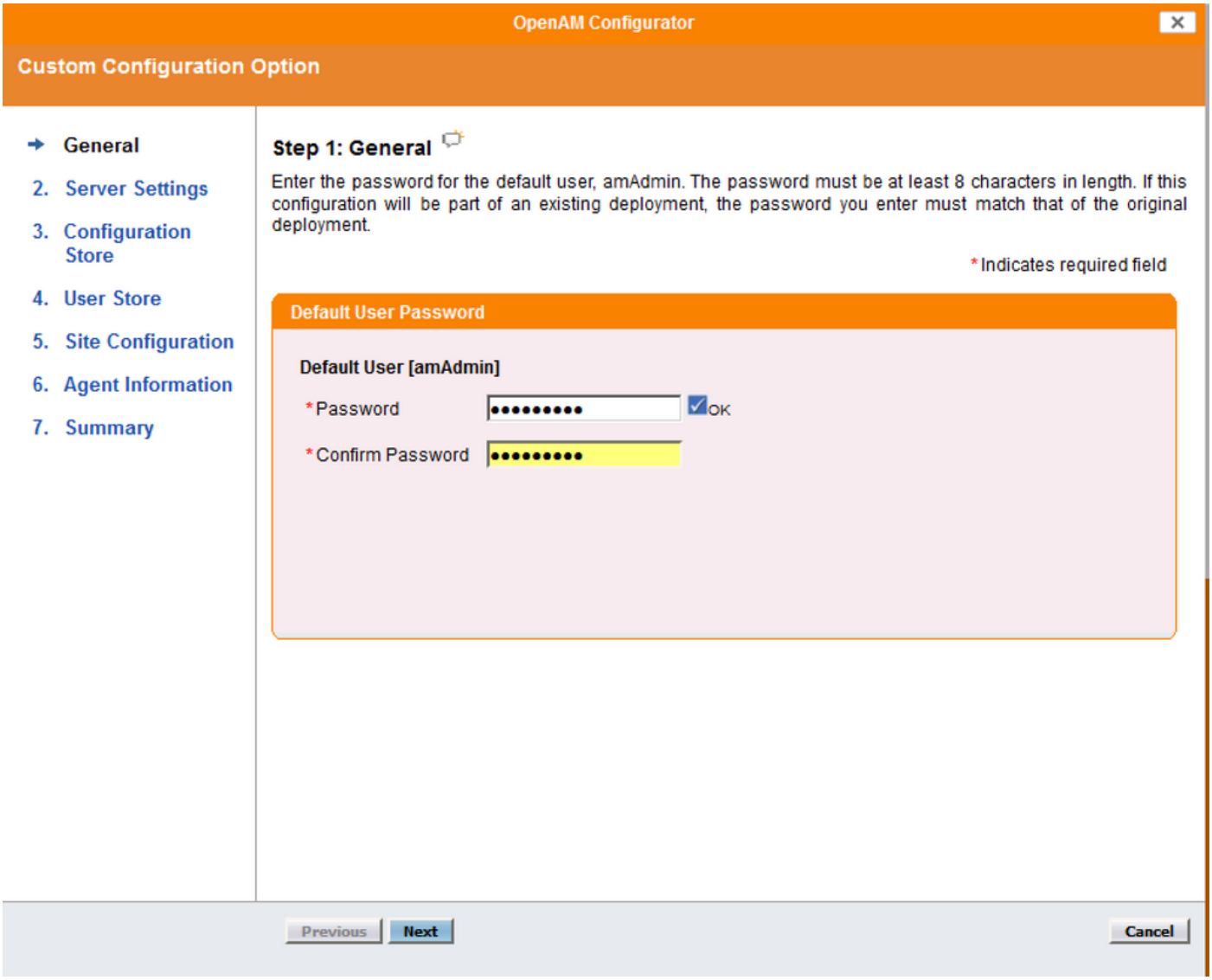
구성

OpenAM Configurator

OpenAM 사용자 지정 컨피그레이션 프로세스에서는 많은 공통 컨피그레이션 옵션을 쉽게 설정할 수 있으므로 컨피그레이션 전에 더 많은 노력을 기울여 나중에 필요한 컨피그레이션 단계를 저장합니다.

일반 설정

Create New Configuration(새 컨피그레이션 생성) 옵션을 클릭하고 기본 관리자 계정(amAdmin)의 비밀번호를 선택합니다. 비밀번호는 8자 이상이어야 합니다.

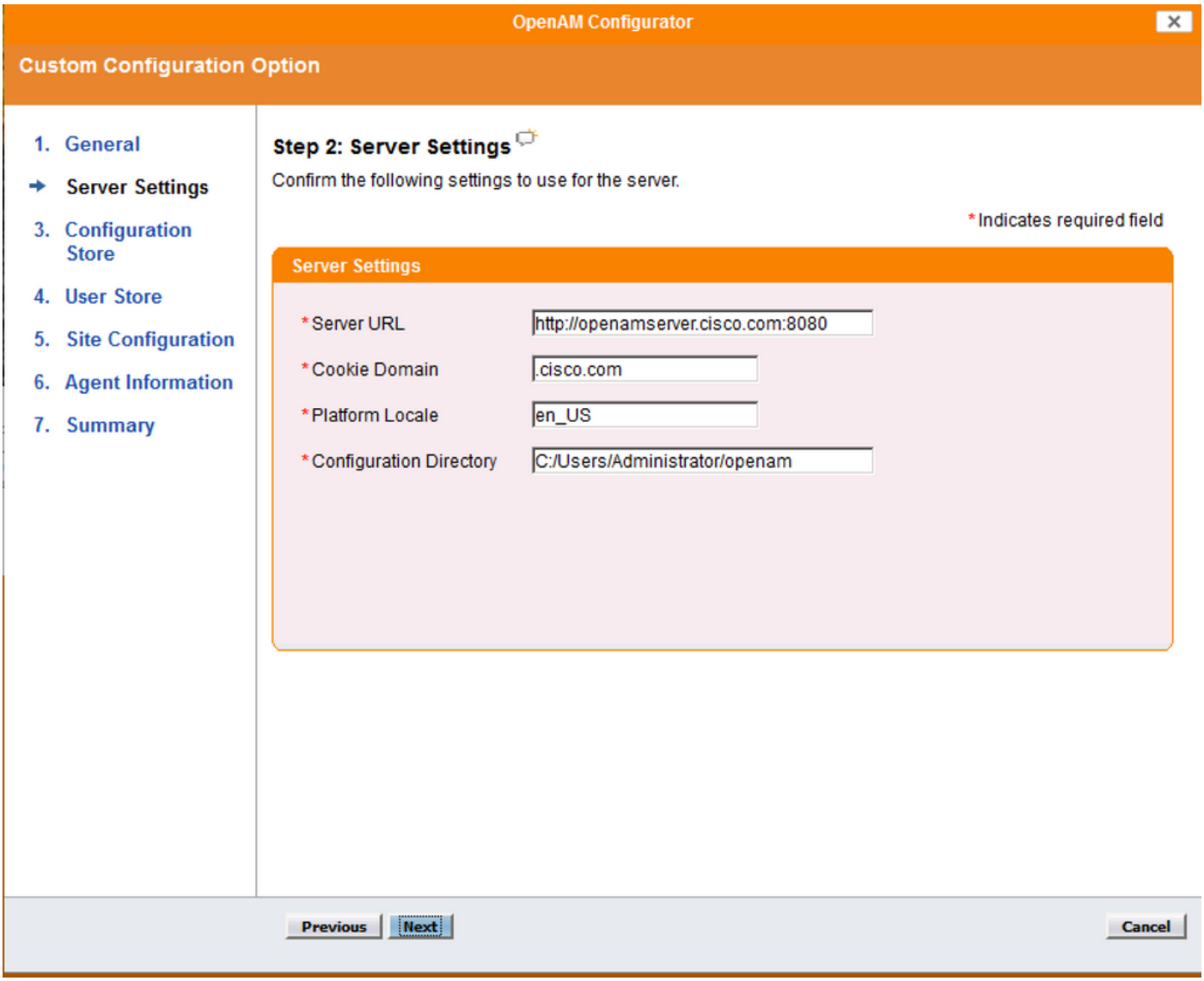


유효한 비밀번호를 두 번 입력하면 다음 버튼이 나타나며 컨피그레이션을 진행할 수 있습니다.

서버 설정

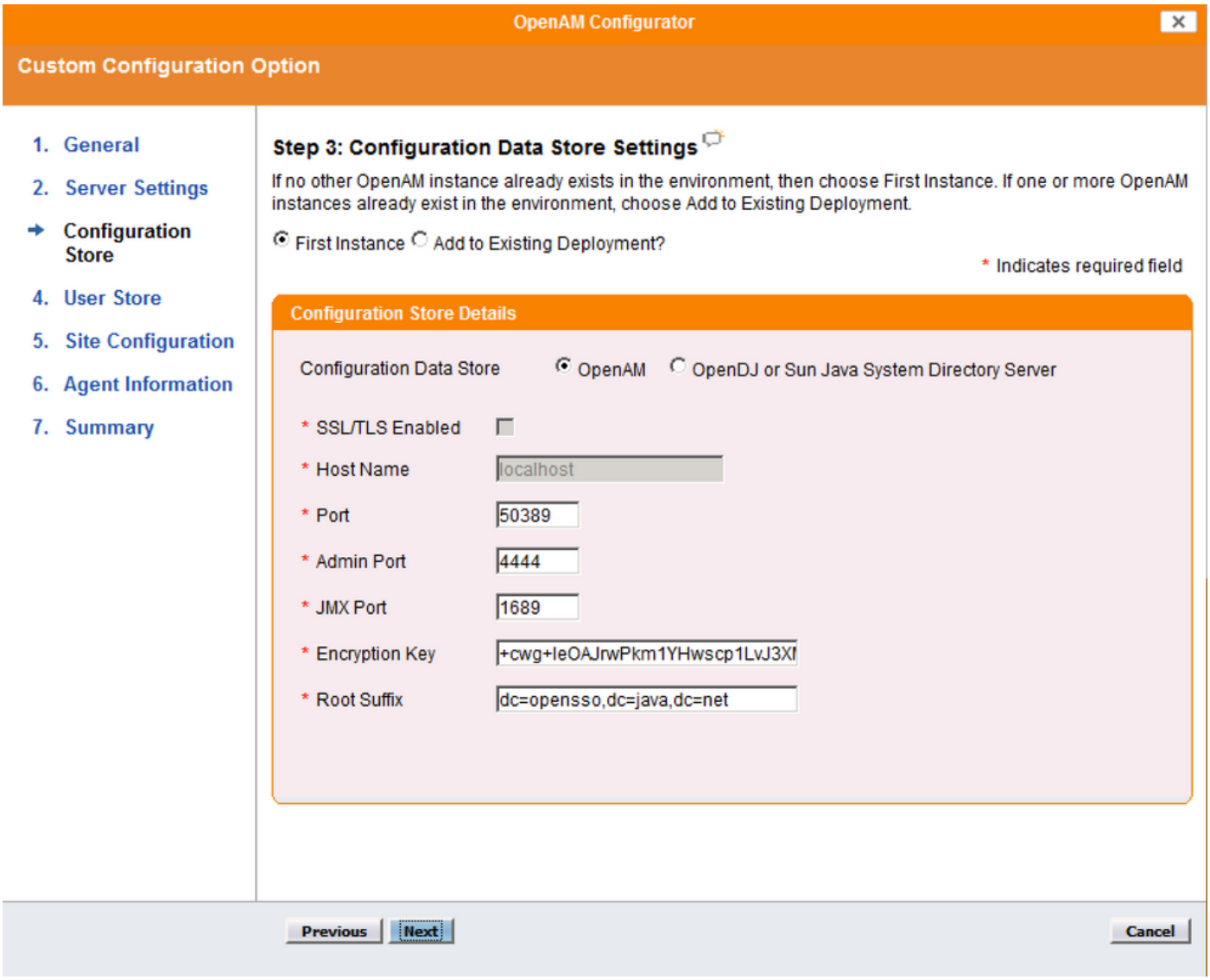
기본적으로 서버 URL은 서버의 정규화된 도메인 이름입니다.

참고: Apache Tomcat을 실행하는 사용자가 Configuration 디렉터리에 대한 쓰기 액세스 권한을 갖는 것이 중요합니다. 따라서 ~/openam/config가 이 목적에 적합합니다. 지원되는 플랫폼 로케일은 en_US(영어), de(독일어), es(스페인어), fr(프랑스어), ja(일본어), zh_CN(중국어 간체) 또는 zh_TW(중국어 번체)입니다.



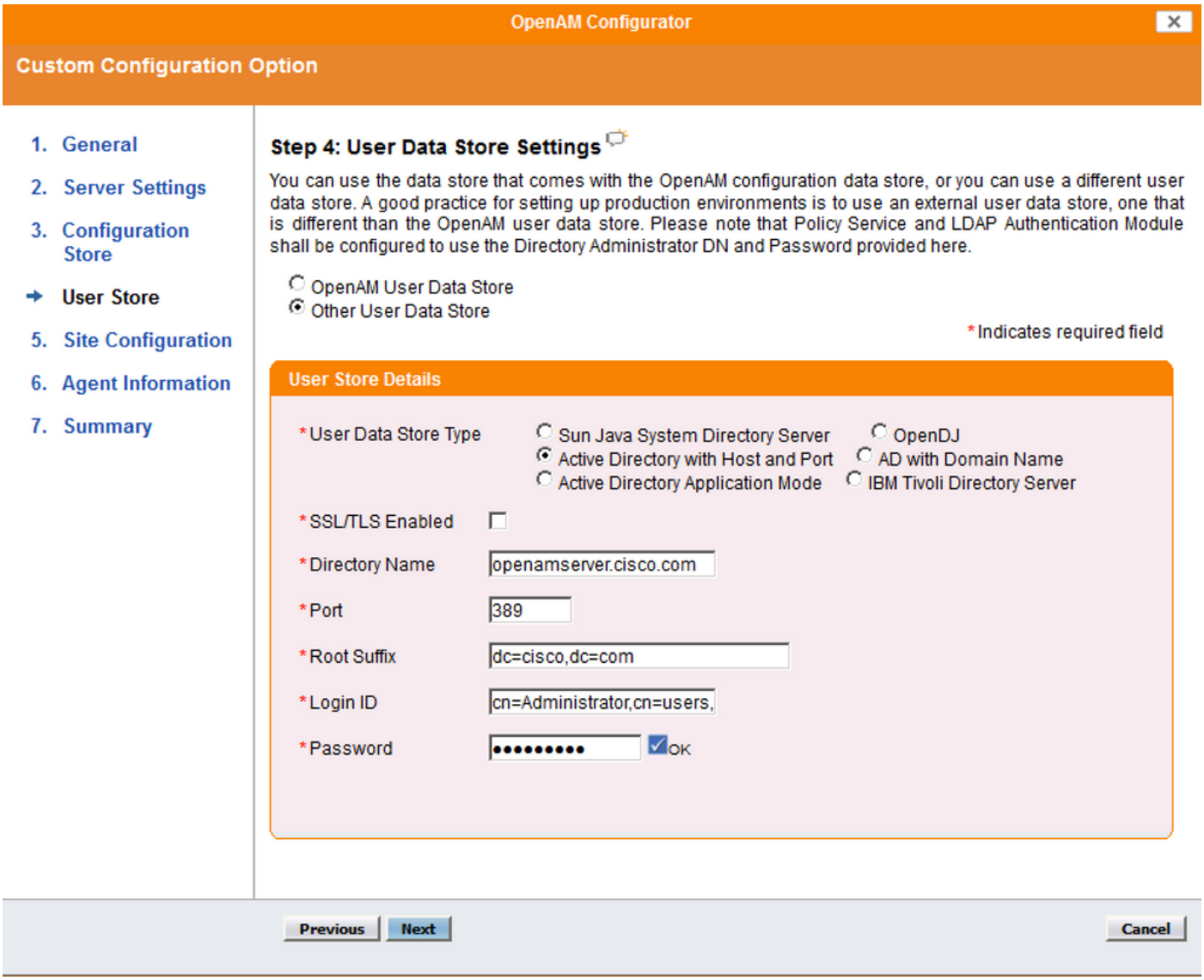
구성 데이터 저장소 설정

단일 서버 컨피그레이션의 경우 이러한 설정을 변경할 필요가 없습니다.



사용자 데이터 저장소 설정

사용자 데이터 저장소 설정은 OpenAM을 Microsoft Active Directory 데이터 저장소에 연결합니다.

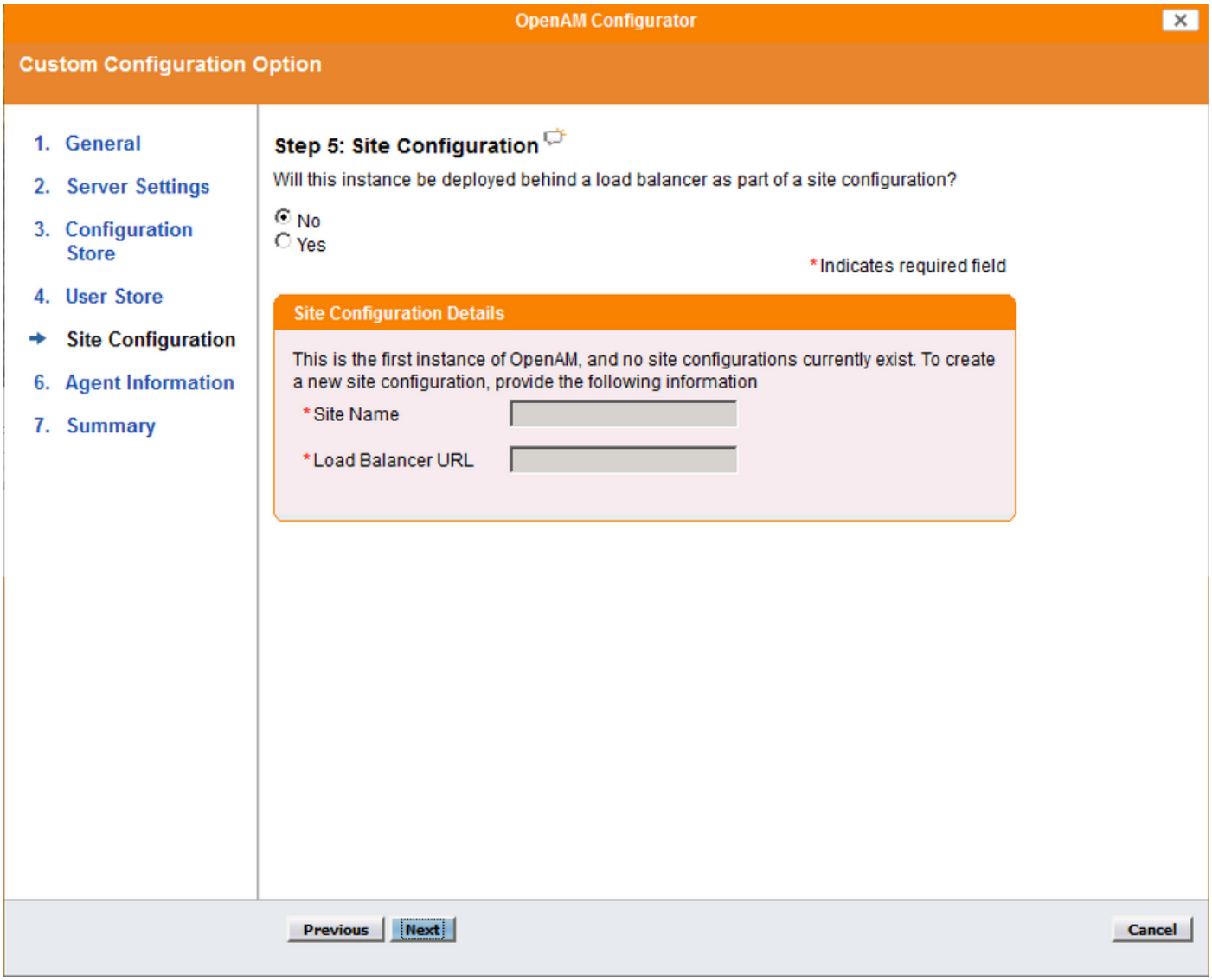


- 사용자 데이터 저장소 유형: 호스트 및 포트가 있는 Active Directory
- SSL/TLS 사용: 사용 안 함
- 디렉터리 이름: <AD 서버의 도메인 이름>
- 포트: 389
- 루트 접미사: dc=cisco,dc=com
- 로그인 ID: cn=<AD 사용자 이름>,cn=users,dc=cisco,dc=com
- 암호: <AD 사용자 암호>

참고: Configurator는 모든 설정이 올바르게 지정되고 Active Directory 인스턴스에 성공적으로 연결될 때까지 계속할 수 있는 옵션을 제공하지 않습니다.

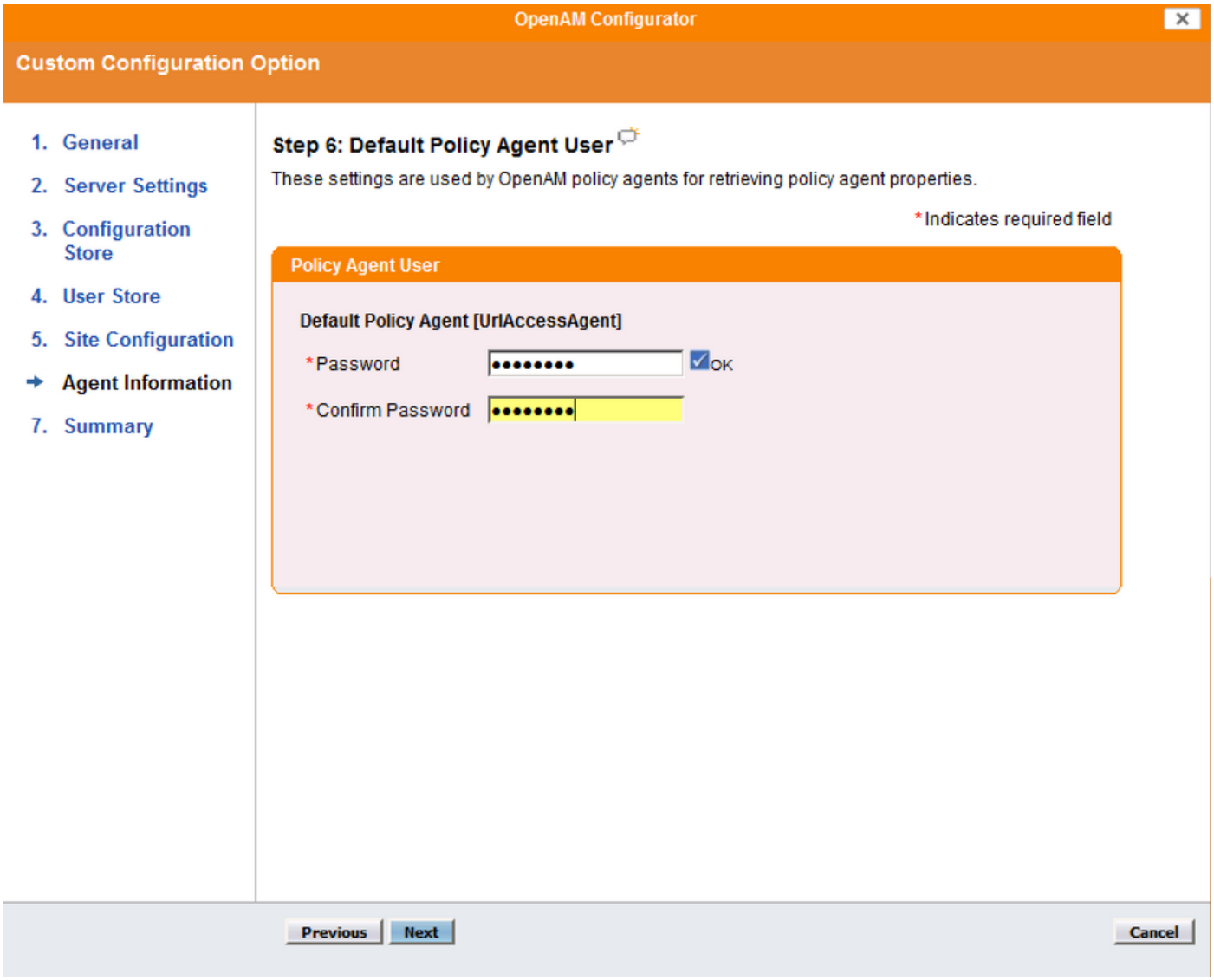
사이트 컨피그레이션

Site Configuration(사이트 컨피그레이션) 화면에서는 여러 OpenAM 서버에서 로드 밸런싱이 이루어지는 사이트의 일부로 OpenAM을 설정할 수 있습니다. 첫 번째 OpenAM 설치의 경우 기본값을 수락합니다.



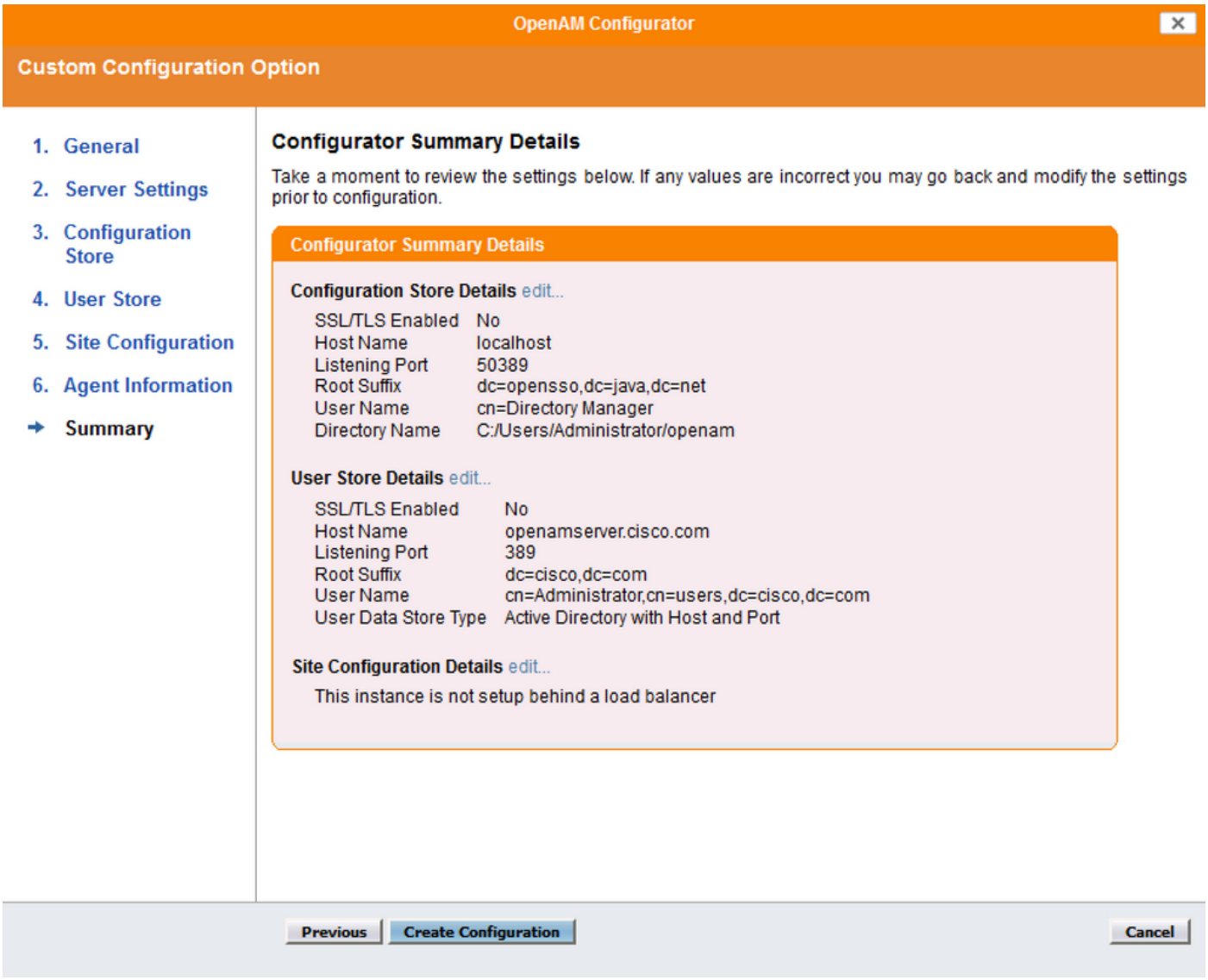
상담원 정보

Agent Information(에이전트 정보) 화면에서 정책 에이전트가 OpenAM에 연결하는 데 사용할 8자 이상의 비밀번호를 제공합니다.



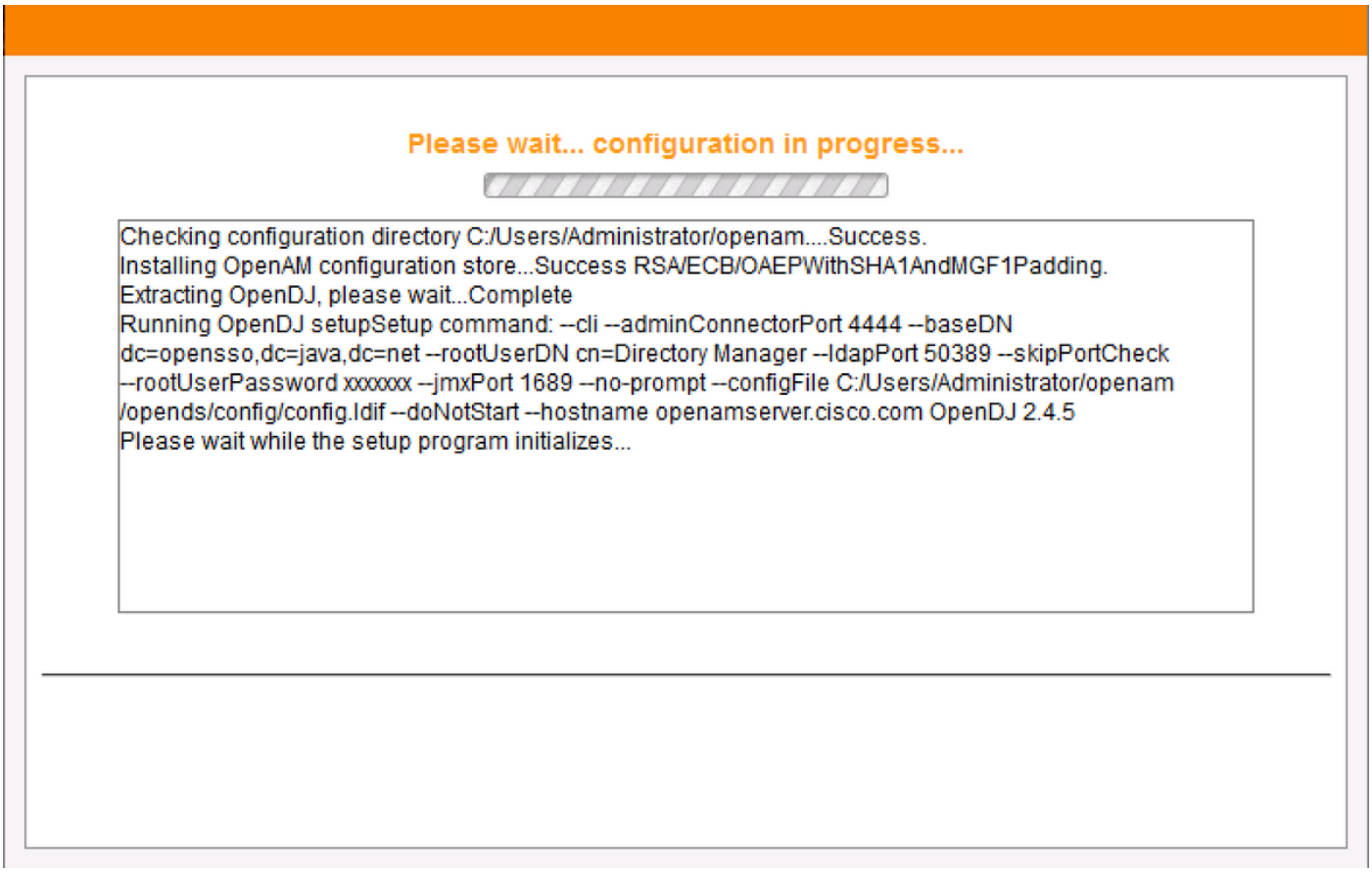
요약

정보를 검토하고 Create Configuration(컨피그레이션 생성)을 클릭합니다

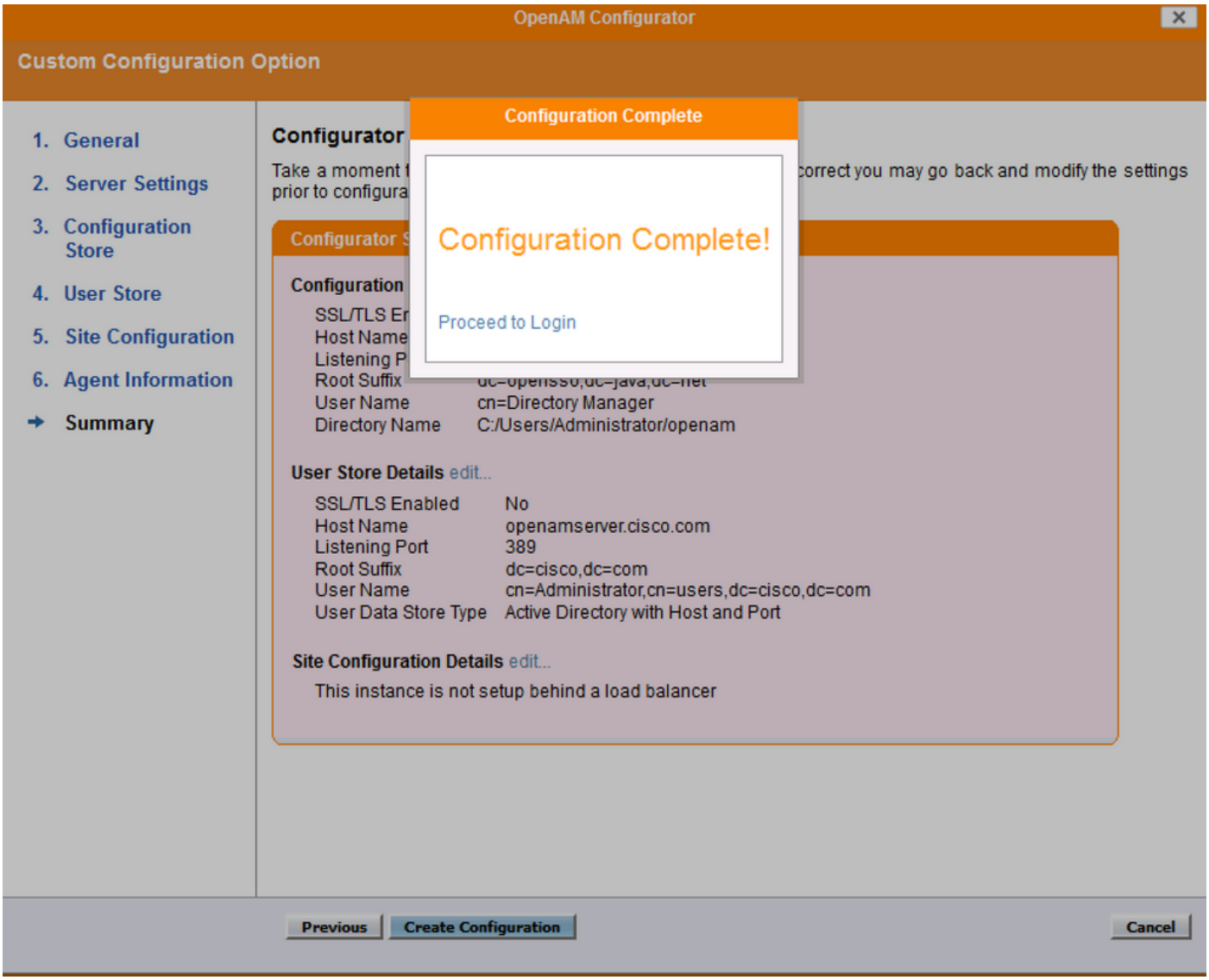


구성 진행률

Configuration Progress(컨피그레이션 진행) 화면에 설치 진행률이 표시됩니다. 이 화면의 모든 출력 및 오류가 파일에 기록됩니다. ~/openam/config/install.log.

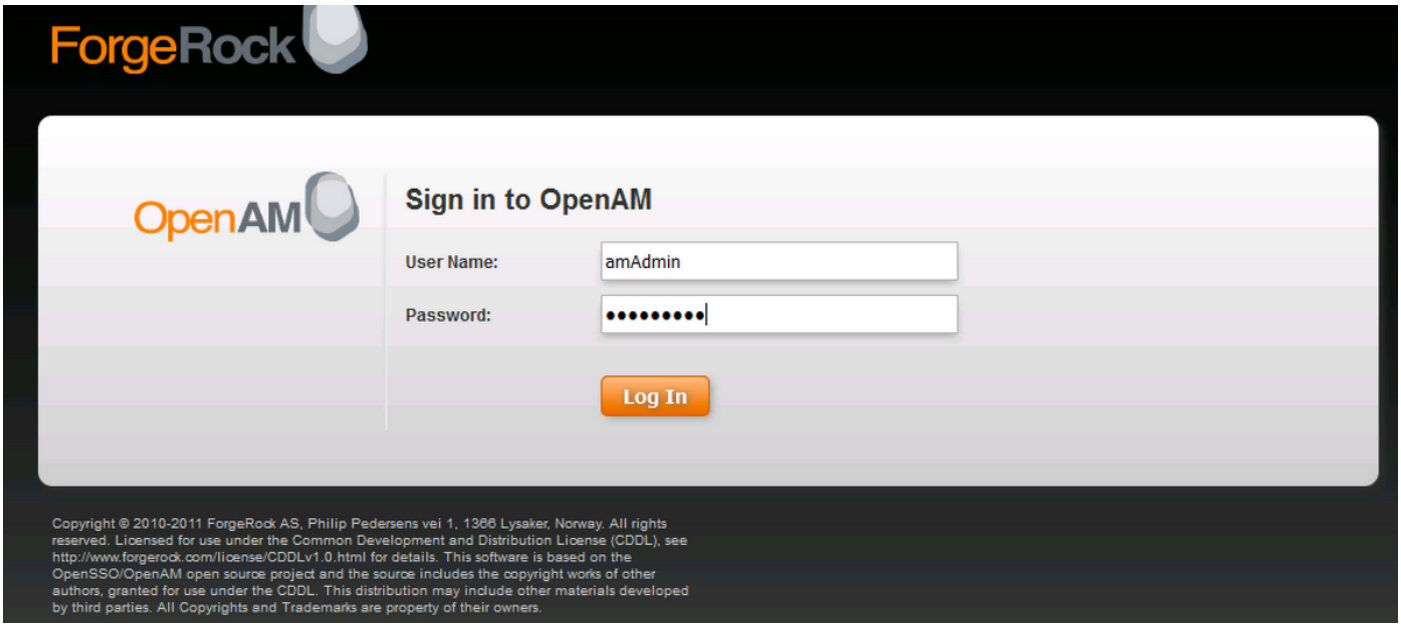

Please wait... configuration in progress...
Checking configuration directory C:/Users/Administrator/openam....Success.
Installing OpenAM configuration store...Success RSA/ECB/OAEPWithSHA1AndMGF1Padding.
Extracting OpenDJ, please wait...Complete
Running OpenDJ setupSetup command: --cli --adminConnectorPort 4444 --baseDN
dc=opensso,dc=java,dc=net --rootUserDN cn=Directory Manager --ldapPort 50389 --skipPortCheck
--rootUserPassword xxxxxxx --jmxPort 1689 --no-prompt --configFile C:/Users/Administrator/openam
/opends/config/config.ldif --doNotStart --hostname openamserver.cisco.com OpenDJ 2.4.5
Please wait while the setup program initializes...

구성 완료



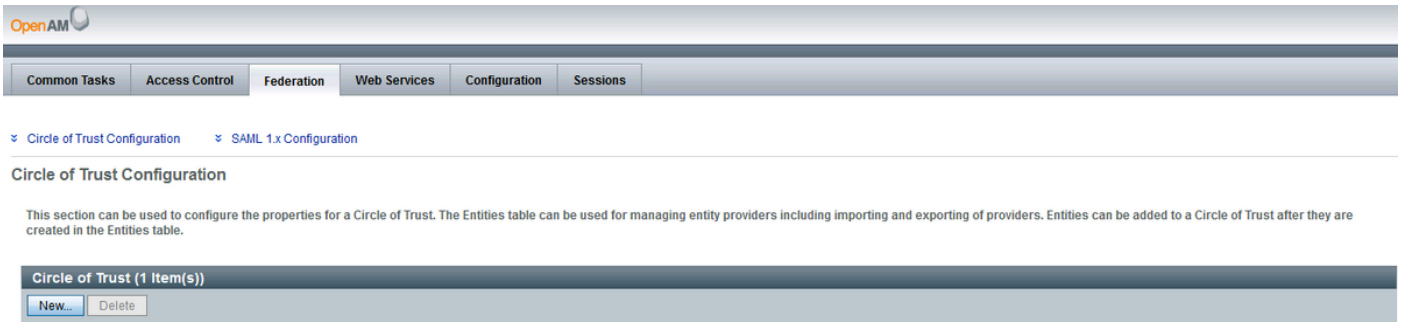
OpenAM을 IdP로 구성

- Proceed to Login or Access through URL http://<FQDN of OpenAM>:8080/openam을 클릭한 다음 OpenAM 관리자로 로그인합니다.
- OpenSSO Enterprise에 처음 액세스하는 경우 Configurator로 이동하여 OpenSSO Enterprise 초기 구성을 수행합니다
- 기본 구성 선택
- OpenAMserver에 대한 비밀번호를 구성해야 합니다
- 비밀번호 구성 및 OpemAM 서버 UI 로그인

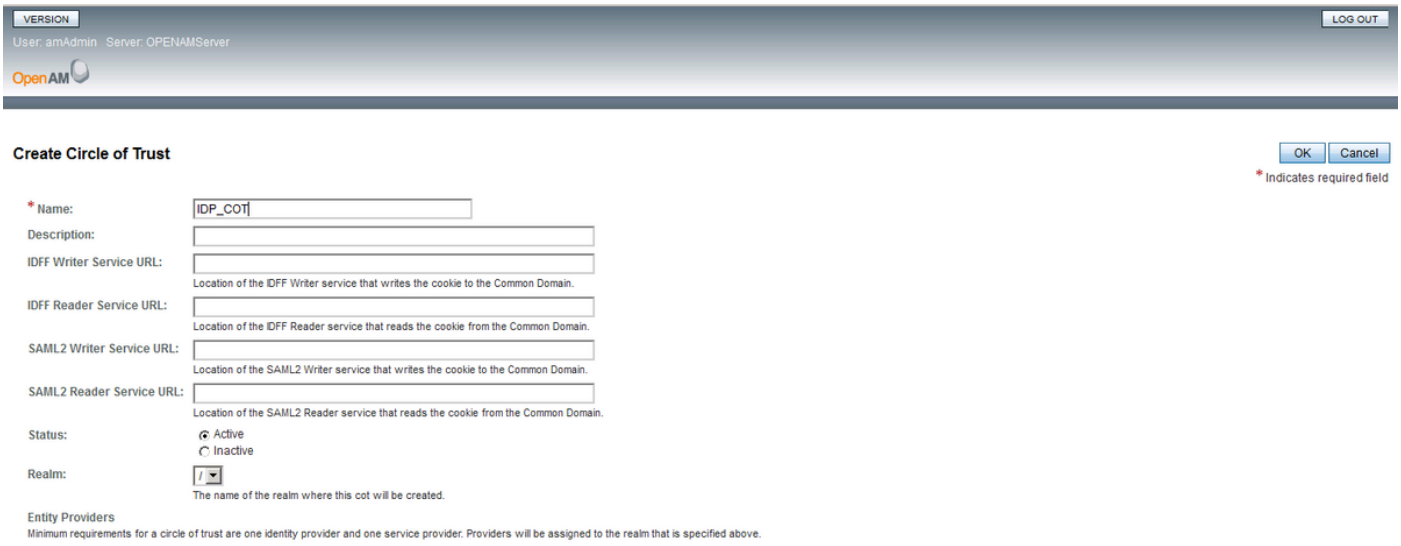


Circle of Trust 구성

Federation(페더레이션) 탭으로 이동하고 Circle of Trust(신뢰 범위) 섹션에서 New(새로 만들기) 버튼을 클릭합니다.



IdP Circle of trust의 고유한 이름을 사용하여 신뢰 원을 만들고 OK를 클릭합니다

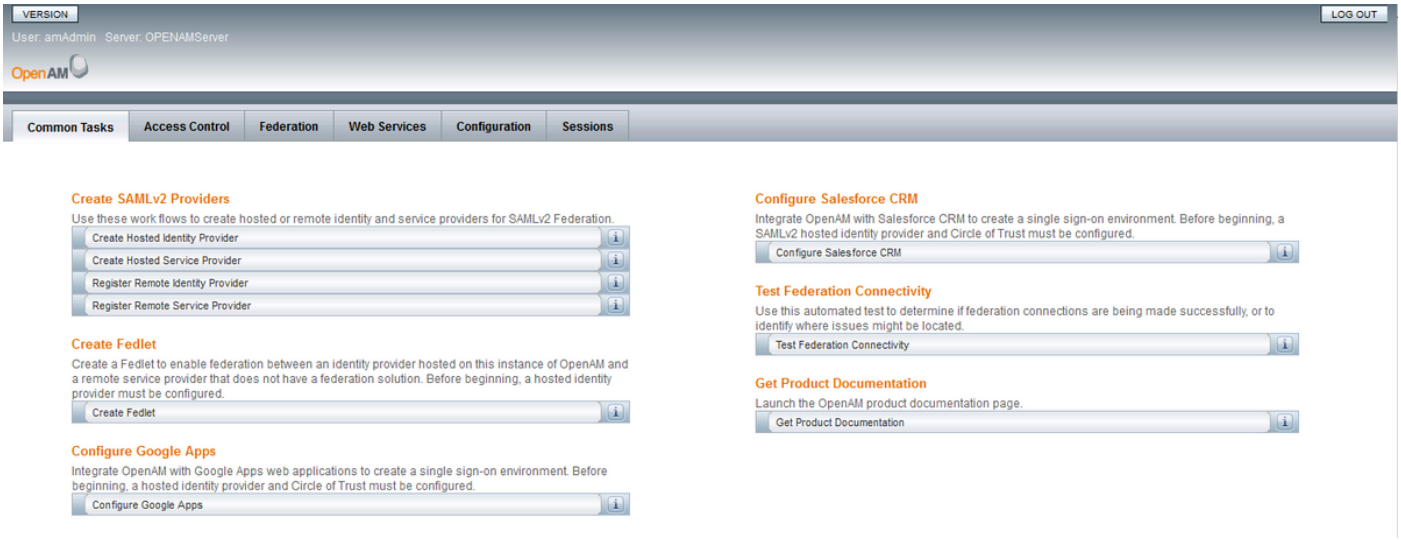


참고: SAML SSO가 작동하려면 서비스 공급자와 IdP가 동일한 CoT(Circle of Trust)에 있어야

합니다.

호스팅 ID 공급자 생성

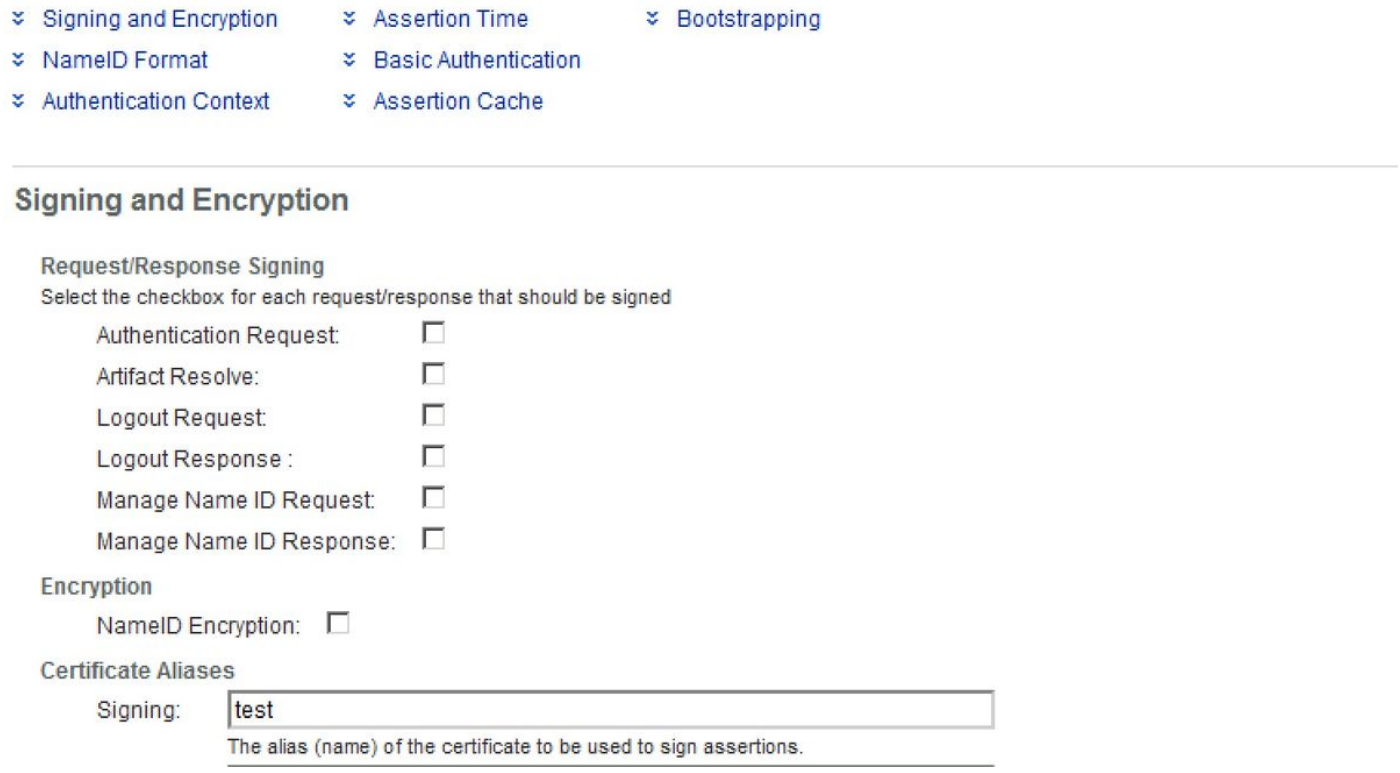
Common Tasks(공통 작업) 탭으로 이동하고 Create hosted Identity Provider(호스팅된 ID 제공자 생성)를 클릭하여 호스팅된 IdP를 생성합니다(구성된 기본값을 그대로 두고 설정을 저장하십시오).



이전에 만든 신뢰 범위가 나열됩니다

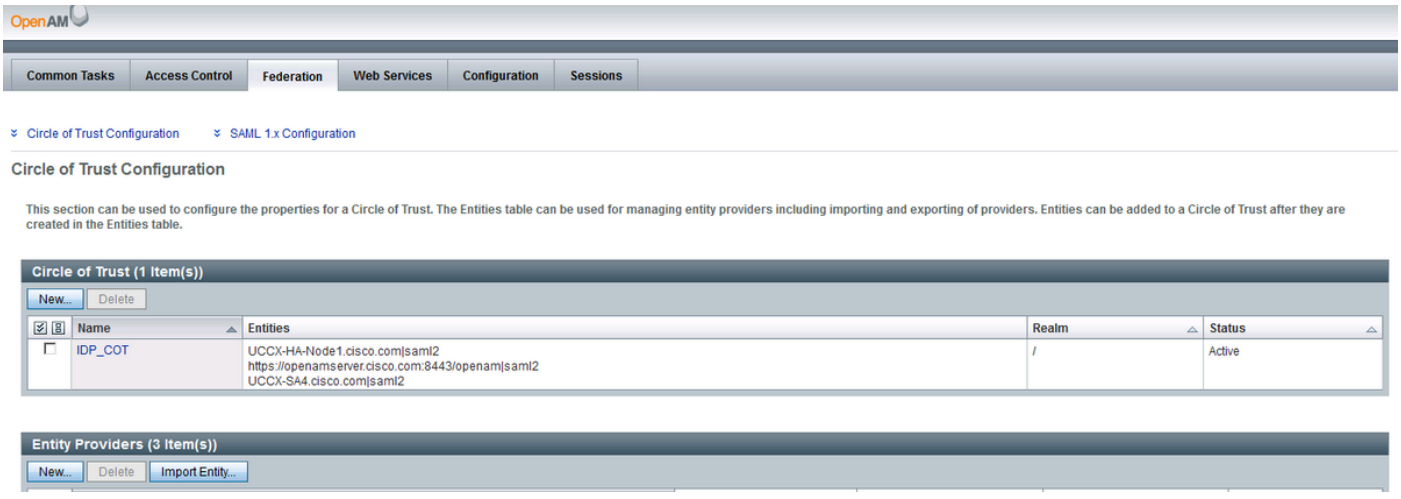
서명 키 구성

Federation(페더레이션) 탭으로 이동하고 Entity Providers(엔터티 공급자) 섹션에서 추가된 호스팅된 ID 공급자를 클릭합니다. Assertion Content(어설션 콘텐츠) 섹션으로 이동하고 Certificate Aliases(인증서 별칭) 섹션에서 Signing(서명) 필드 값을 test(테스트)로 구성합니다. SAML 어설션에 서명하는 데 사용되는 인증서입니다.

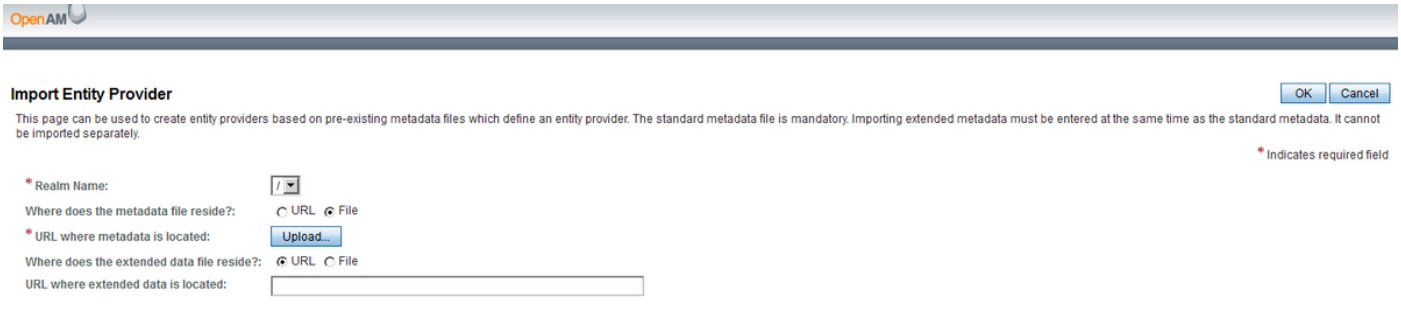


서비스 공급자 엔터티 가져오기

Federation Tab(페더레이션 탭)으로 이동하고 Entity Providers(엔티티 제공자) 섹션에서 Import Entity...(엔티티 가져오기..) 버튼을 클릭합니다.

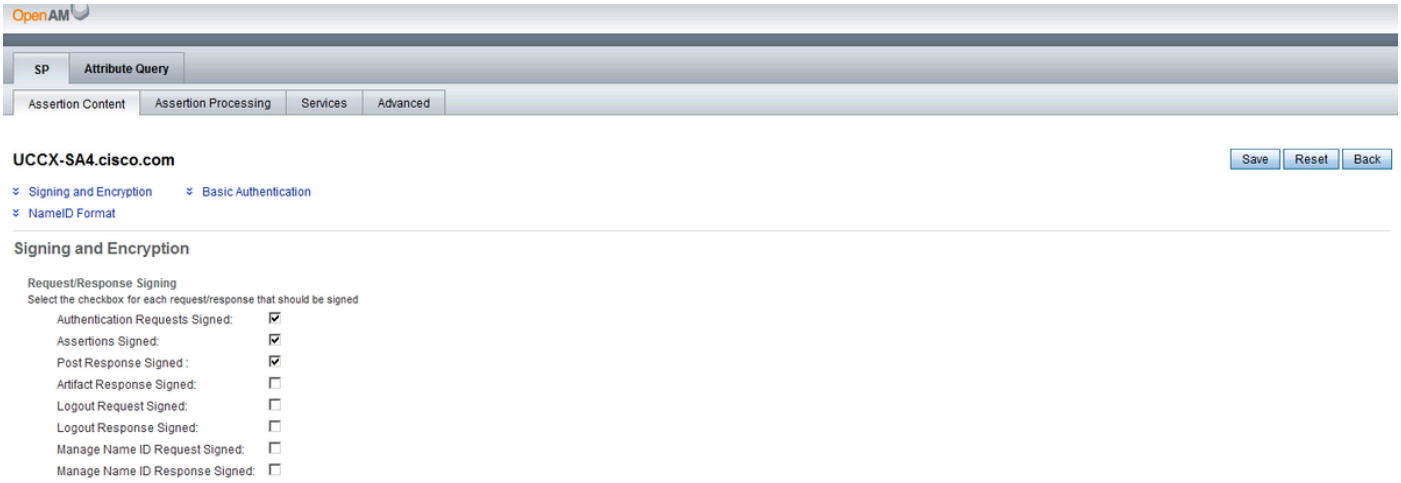


서비스 공급자의 엔터티 파일(sp.xml)을 업로드하고 페이지를 저장합니다.



요청/응답 서명

가져온 엔터티를 클릭하고 Request/Response(요청/응답)에 대해 서명을 활성화합니다.



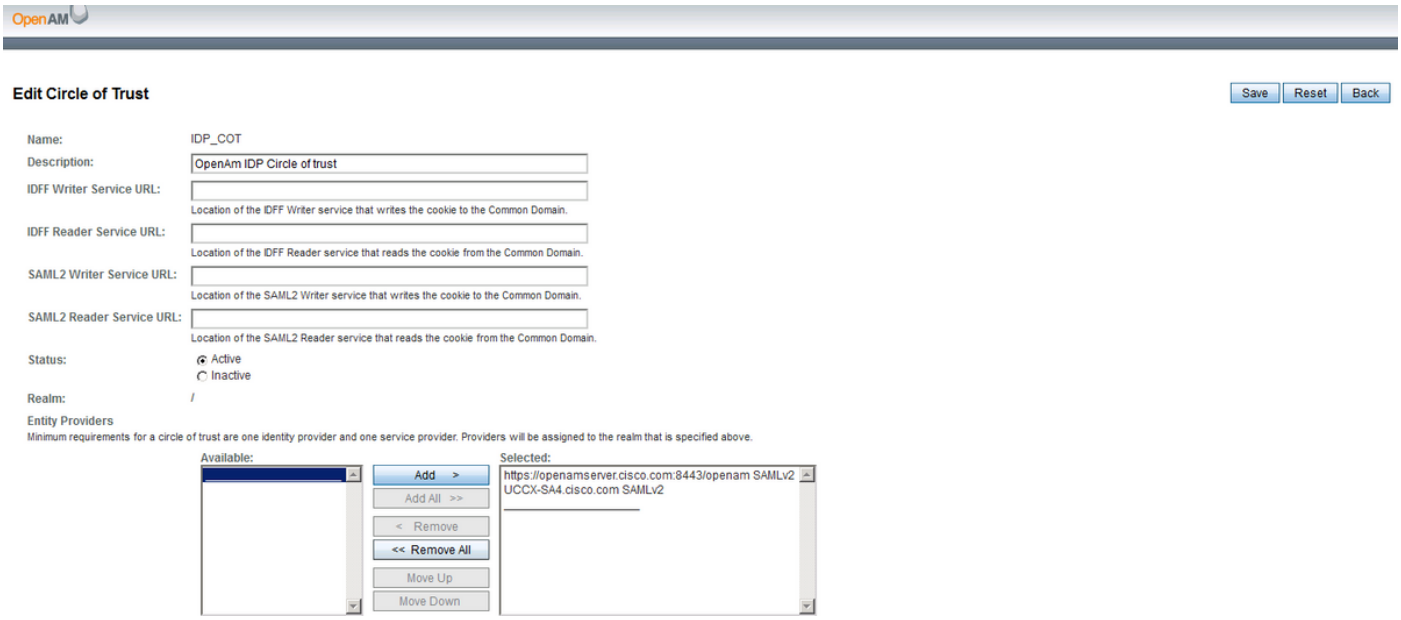
속성 매핑

Assertion Processing(어설션 처리)으로 이동하여 Directory(디렉토리) 및 OpenAM 설정에 따라 uid 및 user_principal에 대한 매핑 속성을 추가합니다. Save(저장)를 클릭합니다.

참고: SP(서비스 공급자)가 인증된 사용자의 ID를 식별하므로 uid 및 user_principal 특성은 모두 필수입니다. 또한 sAMAccountName 및 userPrincipalName 특성이 Active Directory 사용자 속성의 특성 편집기에도 매핑되어 있는지 확인합니다.

Circle of Trust 편집

Federation(페더레이션) 탭으로 이동하여 Circle of Trust added(추가된 신뢰 범위)를 클릭하고 IdP(OpenAm 서버) 및 서비스 공급자 엔티티를 Entity Providers(엔티티 공급자) 섹션의 Available(사용 가능) 섹션에서 Selected(선택한) 섹션으로 이동했는지 확인합니다. 이렇게 하면 IdP와 서비스 공급자가 동일한 Circle of Trust에 지정됩니다.



OpenAM IdP 메타데이터 다운로드

http://<FQDN of OpenAM>:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://<FQDN of OpenAM>:8080/openam&realm= URL로 OpenAM 서버의 IdPmetadatafile을 다운로드할 수 있습니다.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://openamserver.cisco.com:8443/openam">
    <IDPSSODescriptor WantAuthnRequestsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        MIICcTCCAdqgAwIBAgIEWEe4zDANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJJTjESMBAGA1UE
                        CBMJa2FybmF0YWthMRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMx
                        DTALBgNVBAsTBGNjYnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wHhcNMTYxMjA3
                        MDcyMjUyWhcNMTgxMjA3MDcyMjUyWjB9MQswCQYDVQQGEwJJTjESMBAGA1UECBMJa2FybmF0YWth
```

샘플 OpenAM 메타데이터 XML

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://openamserver.cisco.com:8443/openam">
    <IDPSSODescriptor WantAuthnRequestsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        MIICcTCCAdqgAwIBAgIEWEe4zDANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJJTjESMBAGA1UE
                        CBMJa2FybmF0YWthMRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMx
                        DTALBgNVBAsTBGNjYnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wHhcNMTYxMjA3
                        MDcyMjUyWhcNMTgxMjA3MDcyMjUyWjB9MQswCQYDVQQGEwJJTjESMBAGA1UECBMJa2FybmF0YWth
                        MRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMxDTALBgNVBAsTBGNj
                        YnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
                        MIGJAoGBAKvhLKeu0mA1+V2YdfyuiFKQWXdM6EOc/1fmig94cGdNXxvW13KxzjUF2Vv4r364rTFi
                        73eIduF6e1/M481ECYed24LxKpgcSFMijaBdQl7AeQgyzPnWQCJODf85OguGVQhZUUt0RKKYP/d0
                        bgvarRrwXGIvoURJ+8Wy+zLV0T7nAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAM7MNSup7MOHYCLFl
                        i7hK89EMUIxmeywvAjEa8STH7Ba5d0Z1+R/bnXTS/9/pBETi5knuKd+Q59Pl9je2W7l36vFHoF1Q
                        jLlAGnPJOVEmOtimcGZGCj3m7ThlqnOlICyjnrXcLvQ10m75yfimFeeHdFPGbuzTsXjkIKjmhMF9
                        +cc=
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>
        <ArtifactResolutionService index="0"
            isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/ArtifactResolver/metaAlias/idp1" />
        <SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloRedirect/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPSloRedirect/metaAlias/idp1" />
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloPOST/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPSloPOST/metaAlias/idp1" />
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloSoap/metaAlias/idp1" />
        <ManageNameIDService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniRedirect/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPMniRedirect/metaAlias/idp1" />
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniPOST/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPMniPOST/metaAlias/idp1" />
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniSoap/metaAlias/idp1" />
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
        </NameIDFormat>
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/SSORedirect/metaAlias/idp1" />
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/SSOPOST/metaAlias/idp1" />
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/SSOSoap/metaAlias/idp1" />
        <NameIDMappingService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/NIMSoap/metaAlias/idp1" />
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/AIDReqSoap/IDPRole/metaAlias/idp1" />
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI"
            Location="https://openamserver.cisco.com:8443/openam/AIDReqUri/IDPRole/metaAlias/idp1" />
    </IDPSSODescriptor>
</EntityDescriptor>
```

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.