Okta Identity Provider가 있는 컨택 센터 SSO

목차

소개

이 문서에서는 Okta 클라우드 기반 SSO(Single Sign On)에 대한 Id(Identity Service) 및 IdP(Identity Provider)의 컨피그레이션에 대해 설명합니다.

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

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco Unified Contact Center Express, Cisco Unified UCCE(Contact Center Enterprise) 또는 PCCE(Packaged Contact Center Enterprise)
- SAML(Security Assertion Markup Language) 2.0
- 옥타

사용되는 구성 요소

- UCCE 11.6
- 옥타

참고: 이 문서에서는 스크린샷과 예에서 UCCE를 참조하지만 컨피그레이션은 Cisco Identity Service(UCCX/UCCE/PCCE) 및 IdP와 관련하여 유사합니다.

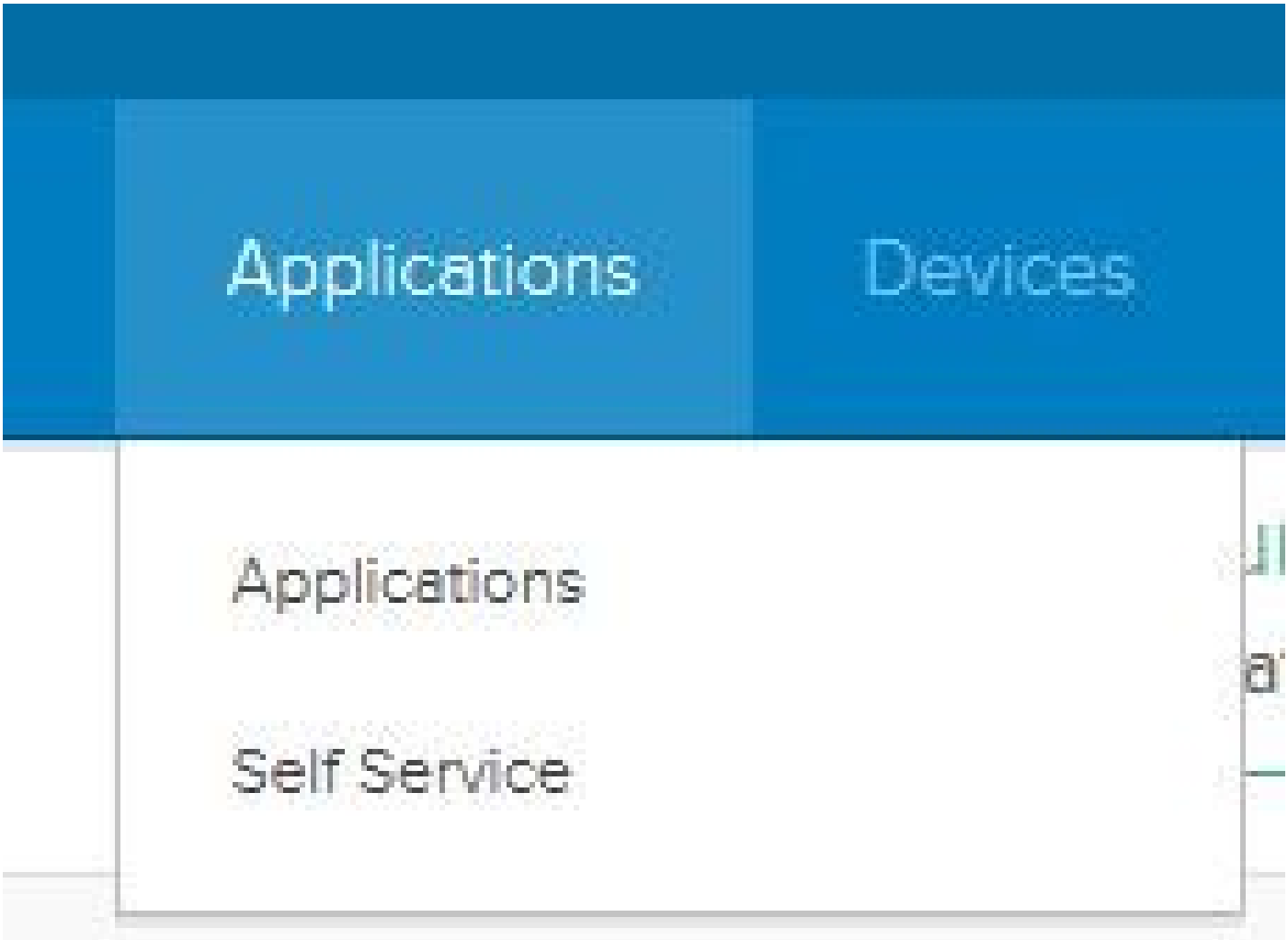
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Okta를 ID 서비스 공급자로 구성

1단계. Id(Identity Service) 웹 페이지에 로그인하고 Settings(설정)로 이동하여 Download Metadata File(메타데이터 파일 다운로드)을 클릭하여 메타데이터 파일을 다운로드합니다.

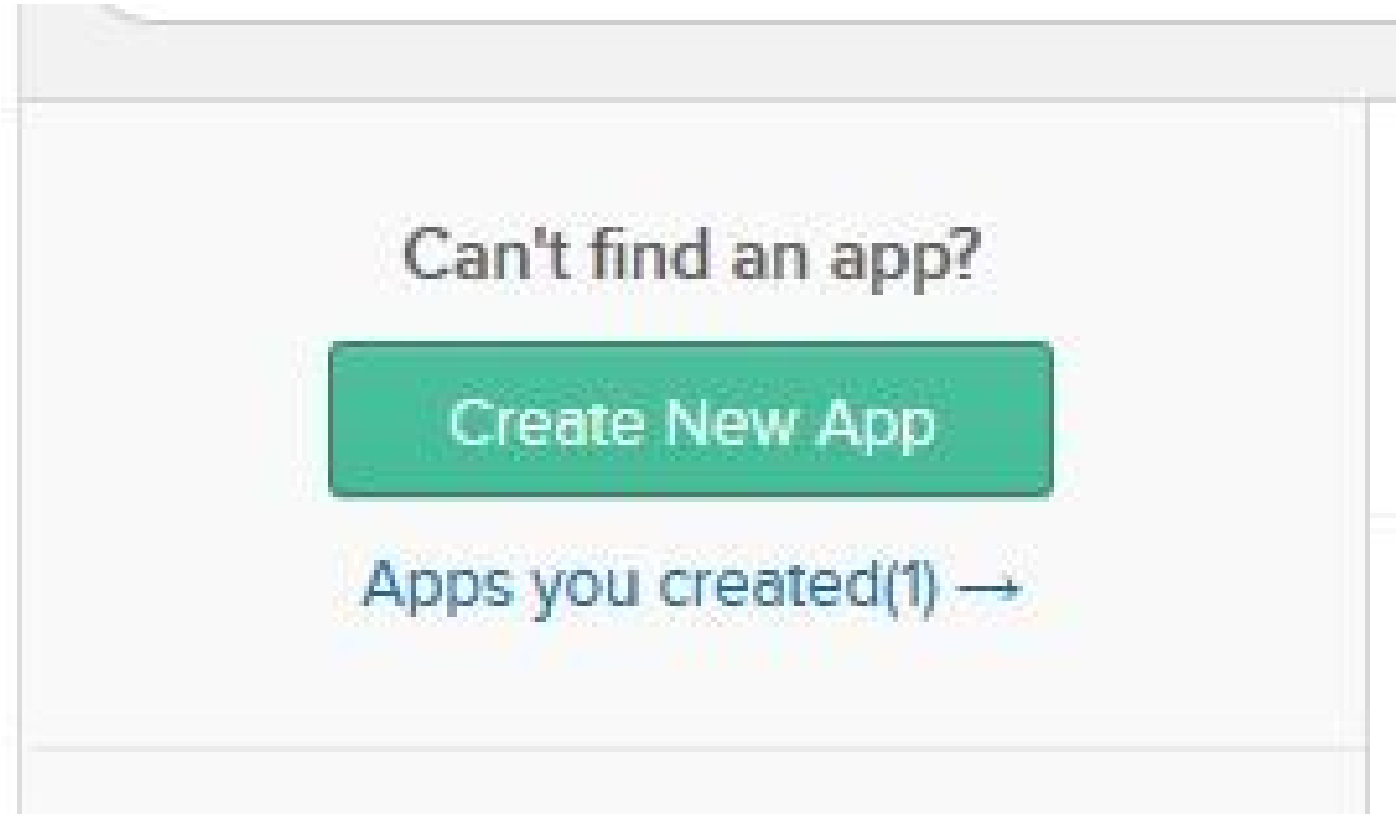
2단계. Okta 서버에 로그인하고 Admin(관리) 탭을 선택합니다.

3단계. Okta 대시보드에서 Applications(애플리케이션) > Applications(애플리케이션)를 선택합니다.

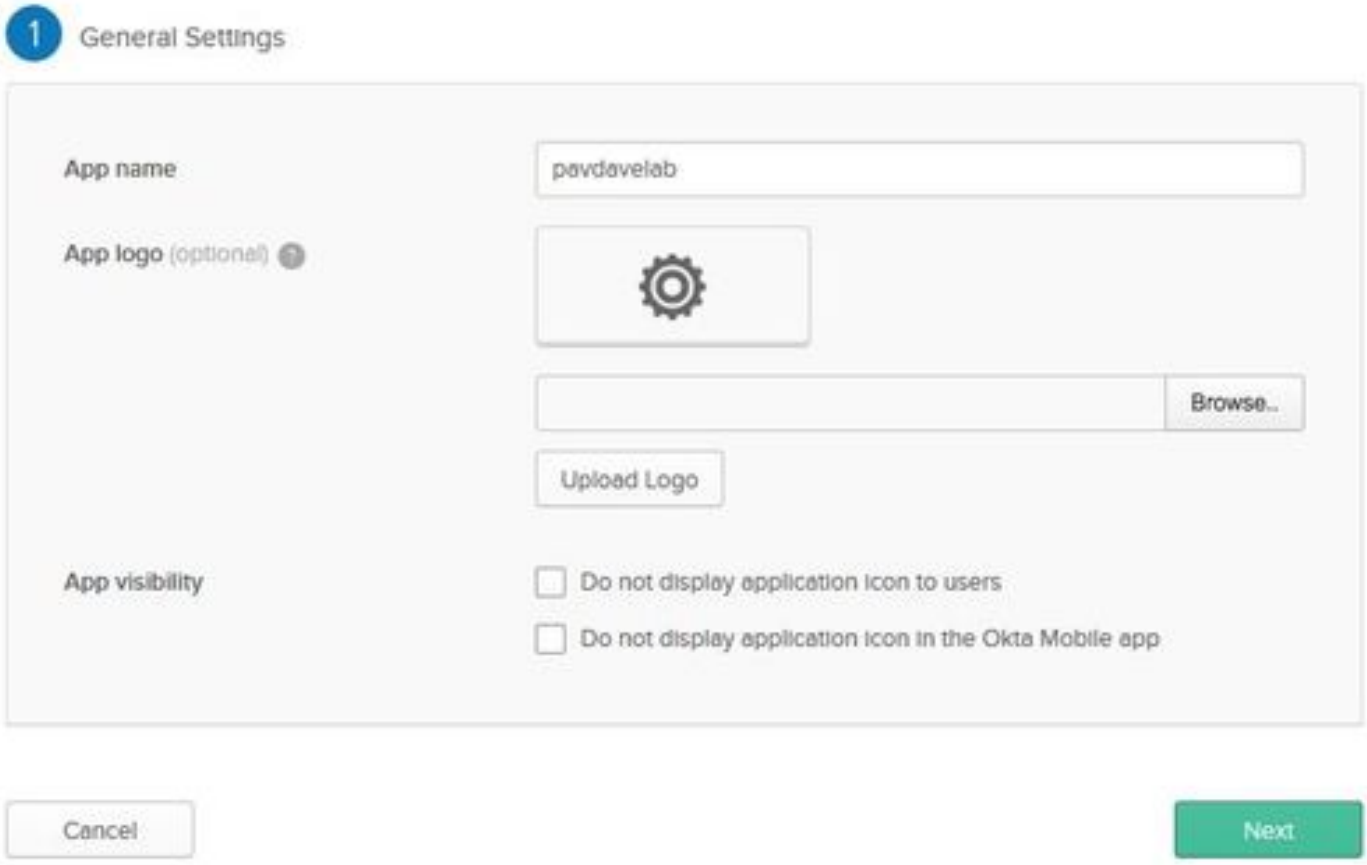


4단계. 마법사를 사용하여 새 사용자 지정 응용 프로그램을 만들려면 [새 응용 프로그램 만들기]를 클릭합니다.

5단계. Create a New Application Integration(새 애플리케이션 통합 생성) 창의 Platform(플랫폼)에 대해 드롭다운 목록에서 Web(웹)을 선택하고 Sign on(로그온) 방법으로 SAML 2.0을 선택한 다음 create(생성)를 선택합니다.



6단계. 앱 이름을 입력하고 다음을 클릭합니다.



7단계. SAML 통합에서 SAML 생성 페이지에 상세내역을 입력합니다.

- 단일 로그인 URL - 메타데이터 파일에서 AssertionConsumerService의 인덱스 0으로 지정된 URL을 입력합니다.

<#root>

<AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="

https://cuicpub-ids.pavdave.xyz:8553/ids/saml/response

" index="0" isDefault="true"/>

- Use this for Recipient URL and Destination URL(수신자 URL 및 대상 URL에 이 옵션 사용) - 수신자 및 대상 URL 일치를 활성화하려면 이 옵션을 선택합니다.
- 이 앱에서 다른 SSO URL을 요청할 수 있도록 허용 - 배포에 여러 ID 노드가 있고 ID 게시자 이외의 다른 SSO URL에서 요청을 허용하려면 이 옵션을 선택합니다.
  - Requestable SSO URLs(요청 가능한 SSO URL) - 이 필드는 위 확인란을 선택한 경우에만 나타납니다. 다른 노드에 대한 SSO URL을 입력할 수 있습니다. HTTP-POST 바인딩을 사용하는 모든 ACS(AssertionConsumerService) 주소를 검색하여 메타데이터 파일에서 ACS URL을 찾을 수 있습니다. 이 필드에 대한 세부 정보를 추가합니다. 여러 URL을 추가하려면 Add Another(다른 URL 추가) 버튼을 클릭합니다.
- 대상 그룹 URI(SP Entity ID) - 메타데이터 파일에서 entityID 주소를 입력합니다.
  <#root>

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

cuicpub-ids.pavdave.xyz

">

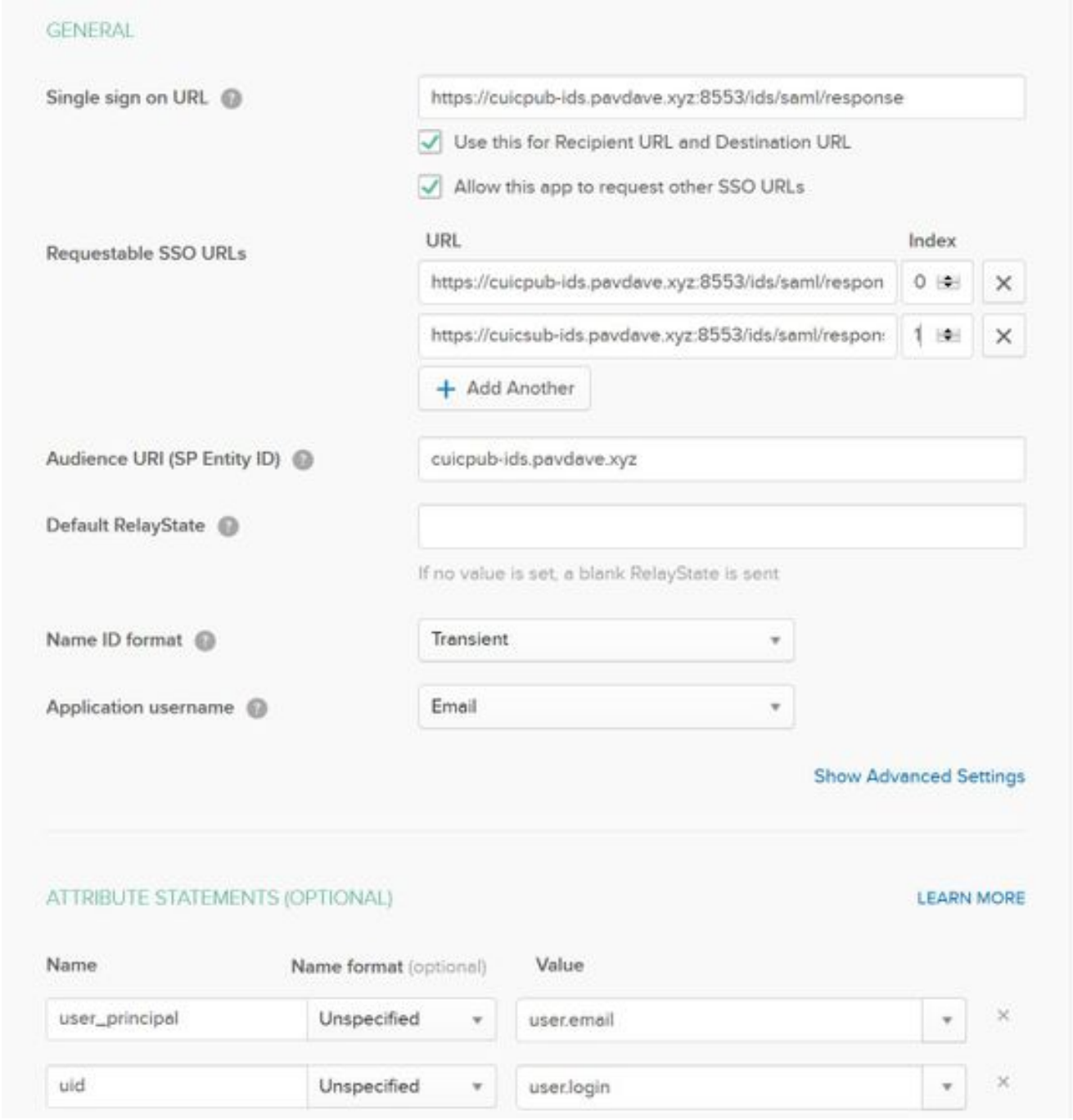
- Default RelayState(기본 릴레이 상태) - 이 필드를 비워 둡니다.
- Name ID Format(이름 ID 형식) - 드롭다운 목록에서 Transient(일시적)을 선택합니다.
- 애플리케이션 사용자 이름 - Unified CCE Administration(Unified CCE 관리) > Manage(관리) > Agents(에이전트)에서 구성한 사용자 이름과 일치하는 사용자 이름 형식을 선택합니다. 

참고: 이 스크린샷은 UCCE/PCCE에만 해당됩니다.

8단계. 필요한 특성 명령문을 추가합니다.

- uid - 애플리케이션에 전송된 청구에서 인증된 사용자를 식별합니다.
- user_principal - Cisco Identity Service로 전송된 어설션에서 사용자의 인증 영역을 식별합니다

.



9단계. 다음을 선택합니다.

10단계. "I'm a software vendor. 앱을 Okta에 통합하고 싶습니다."라고 말하고 Finish(마침)를 클릭합니다.

11단계. Sign On(로그온) 탭에서 ID 공급자 메타데이터를 다운로드합니다.

12단계. 다운로드한 메타데이터 파일을 열고 NameIDFormat의 두 행을 다음과 같이 변경하여 저장합니다.

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
```

ID 서비스 구성

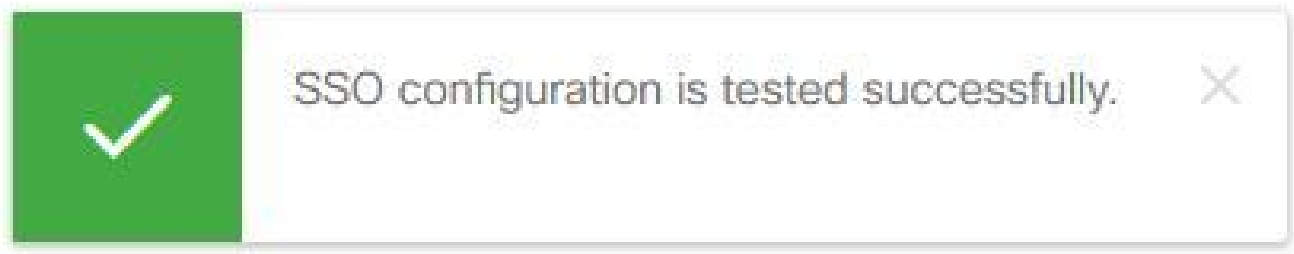
1단계. Identity Service 서버로 이동합니다.

2단계. Settings(설정)를 클릭합니다.

3단계. 다음을 클릭합니다.

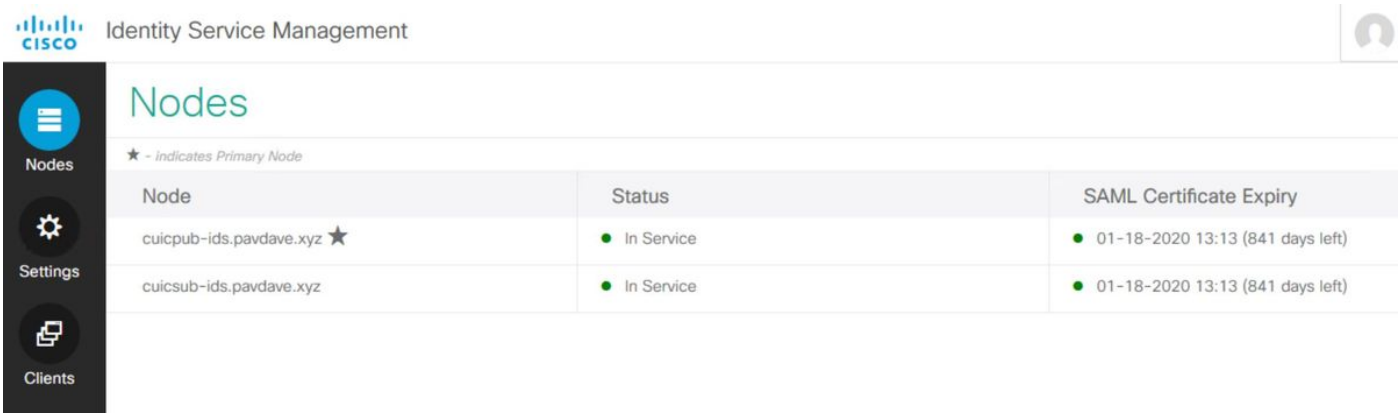
4단계. Okta에서 다운로드한 메타데이터 파일을 업로드하고 Next(다음)를 클릭합니다.

5단계. Test SSO Setup(SSO 설정 테스트)을 클릭합니다. 새 창에서 Okta에 대한 인증을 위한 로그인 프롬프트가 표시됩니다. 로그인에 성공하면 화면 오른쪽 하단에 SSO Configuration(SSO 컨피그레이션)이 성공적으로 테스트되었다는 확인 표시가 나타납니다.



참고: Okta에 대해 이미 인증된 경우 다시 로그인하라는 메시지가 표시되지 않지만 Id가 자격 증명을 확인하는 동안 간단한 팝업이 표시됩니다.

이 시점에서 ID 서비스 및 ID 제공자의 컨피그레이션이 완료되었으며 서비스 중인 노드가 표시되어야 합니다.



Single Sign-On 추가 컨피그레이션

ID 서비스 및 ID 제공자가 구성된 후 다음 단계는 UCCE 또는 UCCX용 단일 로그인을 설정하는 것입니다.

- UCCE/PCCE
- UCCX

추가 읽기

- UCCE/PCCE 단일 로그인
- UCCX Single Sign-On
- CUCM(Cisco Unified Communications Manager) - Okta Identity Provider Configuration

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.