Okta IDP를 사용하여 CCX 및 Prem Contact Center 솔루션에 SSO 구성

목차

소개

이 문서에서는 다양한 Cisco On Prem Contact Center 솔루션에 대한 OKTA의 SSO(Single Sign On) 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Unified Contact Center Express, Cisco Unified UCCE(Contact Center Enterprise) 또는 PCCE(Packaged Contact Center Enterprise)
- 보안 어설션 마크업 언어
- 옥타

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- UCCX(Unified Contact Center Express) 15.0
- 옥타

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.

IDS/Cisco 측의 컨피그레이션

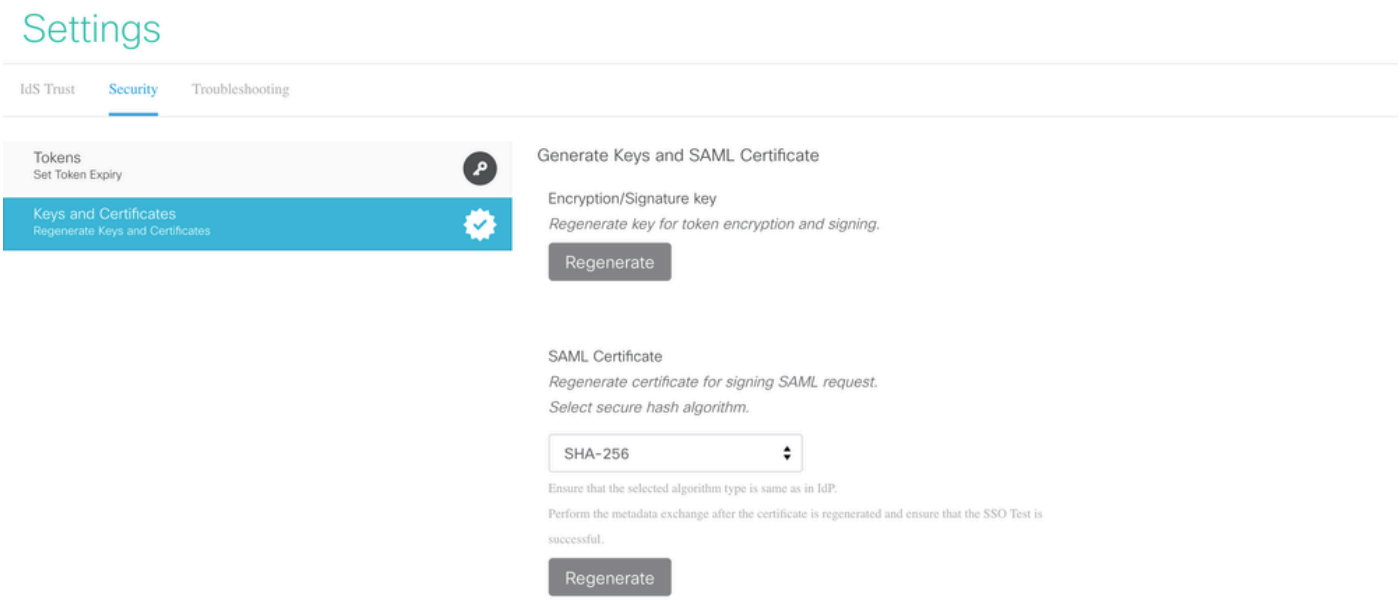
1. CLI에서 utils ids set_property IS_IdP_OKTA true 명령을 실행하고 IDS(Identity Service) 서비스를 다시 시작합니다.

2. HA(고가용성)인 경우 두 노드에서 모두 이 명령을 실행하고 IDS 서비스를 다시 시작합니다.

3. PUB 노드에서 UCCX Cisco IDS 관리 인터페이스 https:// <UCCX 서버 주소>:8553/idsadmin에 로그인합니다.

4. 설정 > 보안 > 키 및 인증서로 이동합니다.

5. SAML(Security Assertion Markup Language) 인증서를 다시 생성합니다.



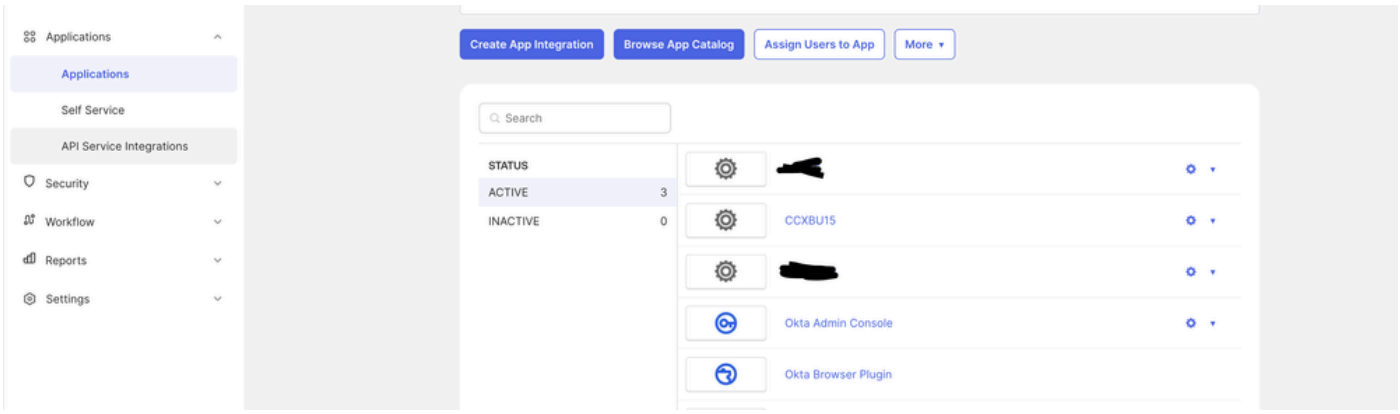
6. IDS Trust(IDS 트러스트) 탭에서 SAML SP 메타데이터 XML을 다운로드합니다.

7. SP(서비스 공급자) 메타데이터 XML을 열고 'AssertionConsumerService' 태그 내에 게시자 및 가입자 ID의 'Location' 특성 값을 기록합니다. SAML 메타데이터의 AssertionConsumerServiceURL에는 이제 PUB에 대한 쿼리 매개 변수 대신 metaAlias가 SAML 응답 URL의 일부로 포함됩니다.

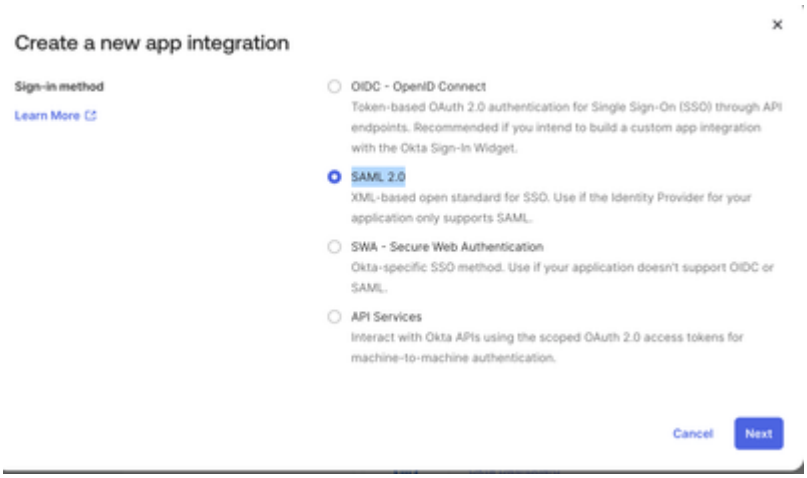
8. 가입자의 경우 쿼리 매개변수와 함께 표시되며 무시할 수 있습니다.

OKTA IDP 측의 컨피그레이션

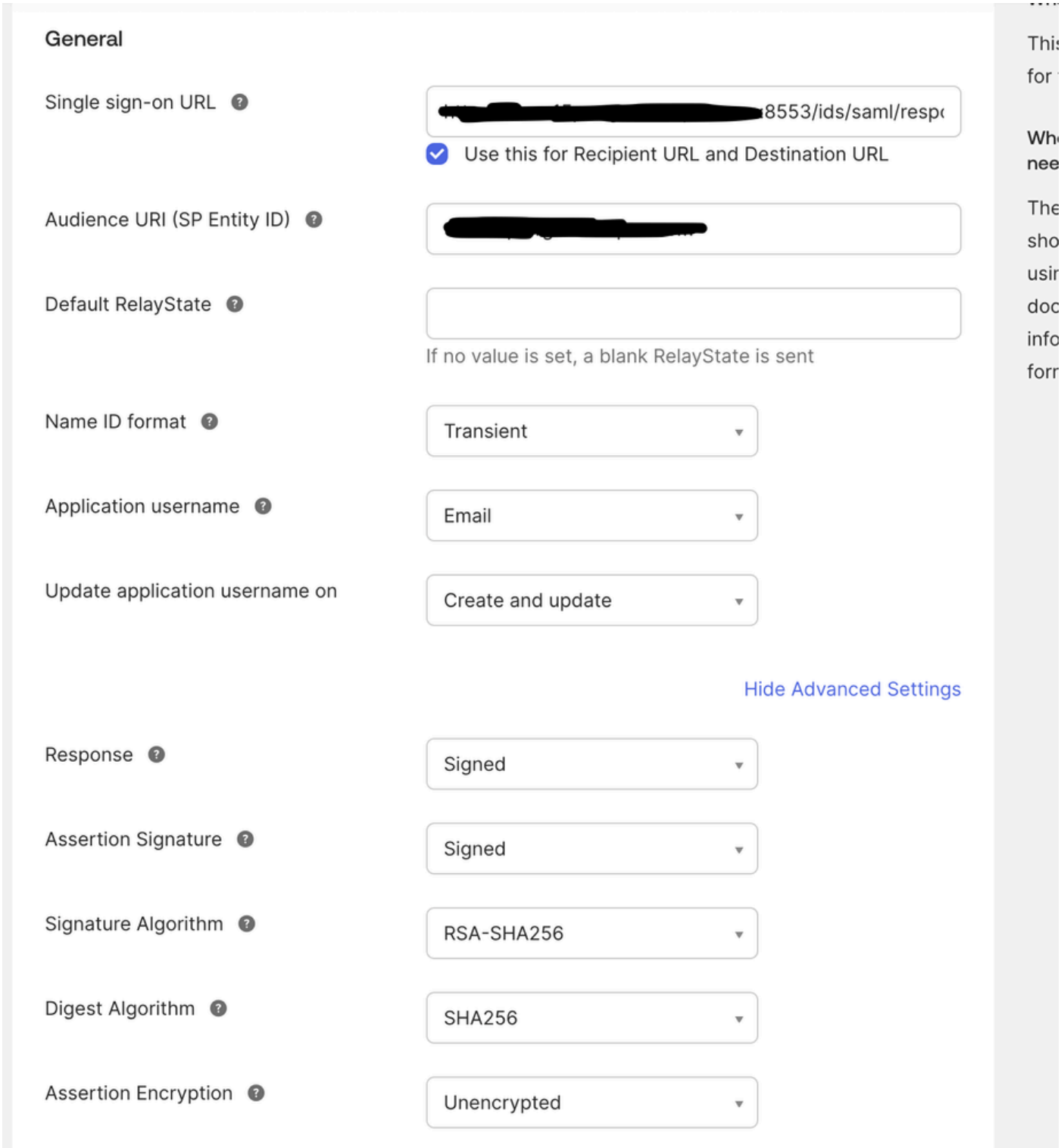
1. Applications(애플리케이션) 아래에서 Create App Integration(앱 통합 생성)을 클릭합니다.



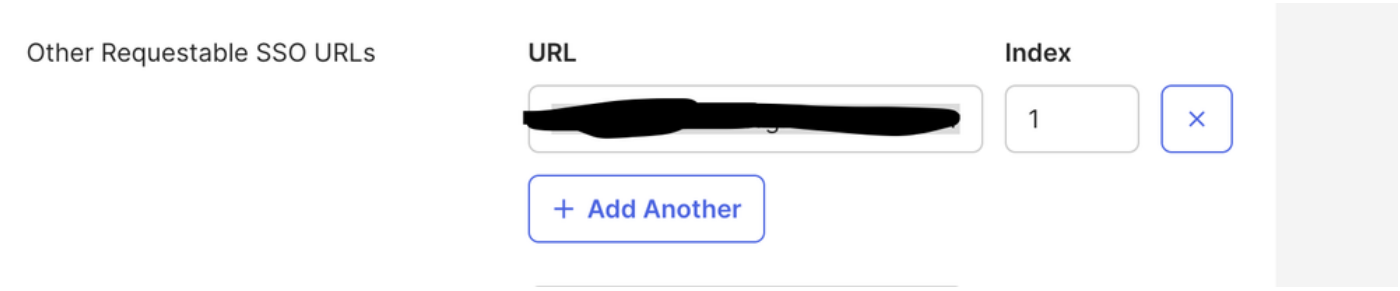
2. SAML2.0 옵션을 선택합니다.



3. SAML 설정 SSO URL에서 7단계에서 복사한 PUB의 SSO URL을 이 문서의 'IDS/Cisco 측 구성 '에 제공합니다. URI(Audience Uniform Resource Identifier)(SP Entity ID)의 ID 서비스 관리 설정에서 IDS trust 탭 아래에 SP 엔터티를 붙여넣습니다.



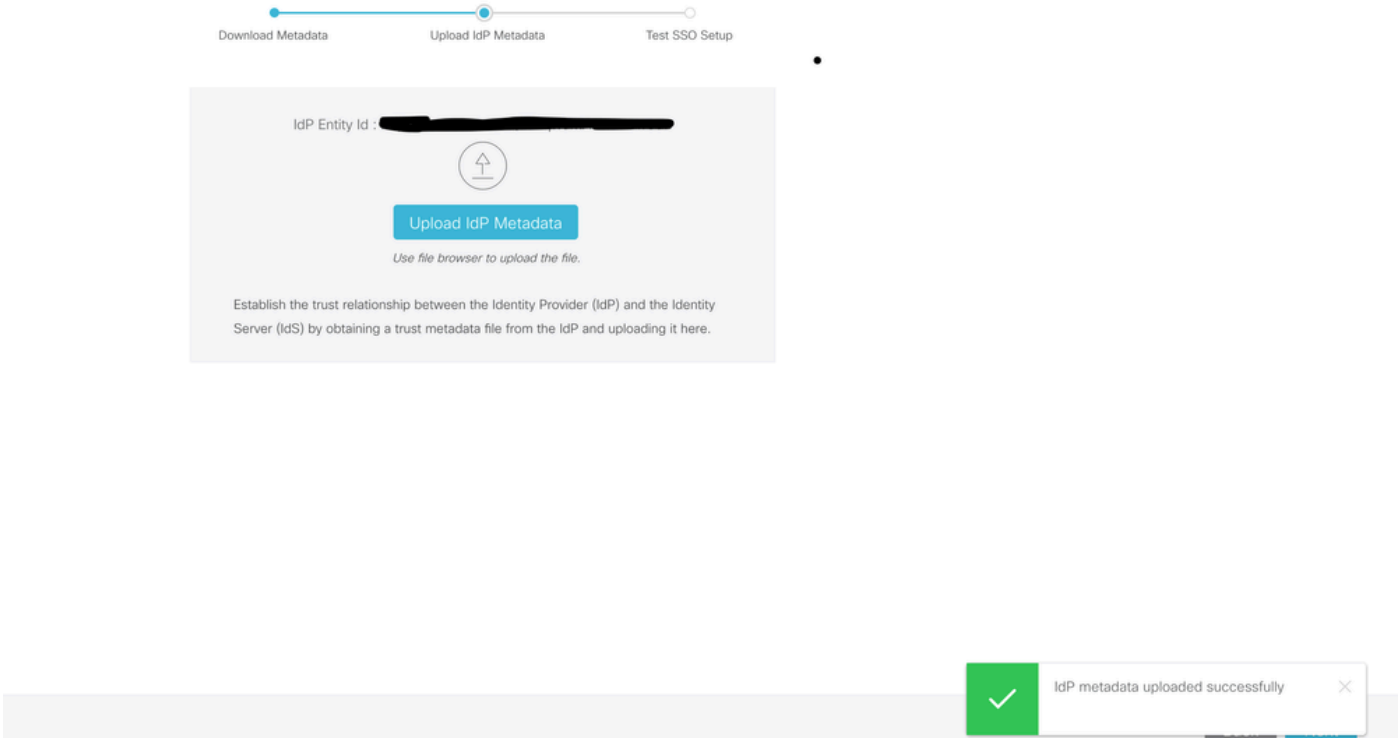
4. '기타 요청 가능한 SSO URL'에서 인덱스 값을 1로 하여 지정된 형식의 SUB https://<SUBFQDN>:8553/ids/saml/response/metaAlias/sp의 URL을 입력합니다.



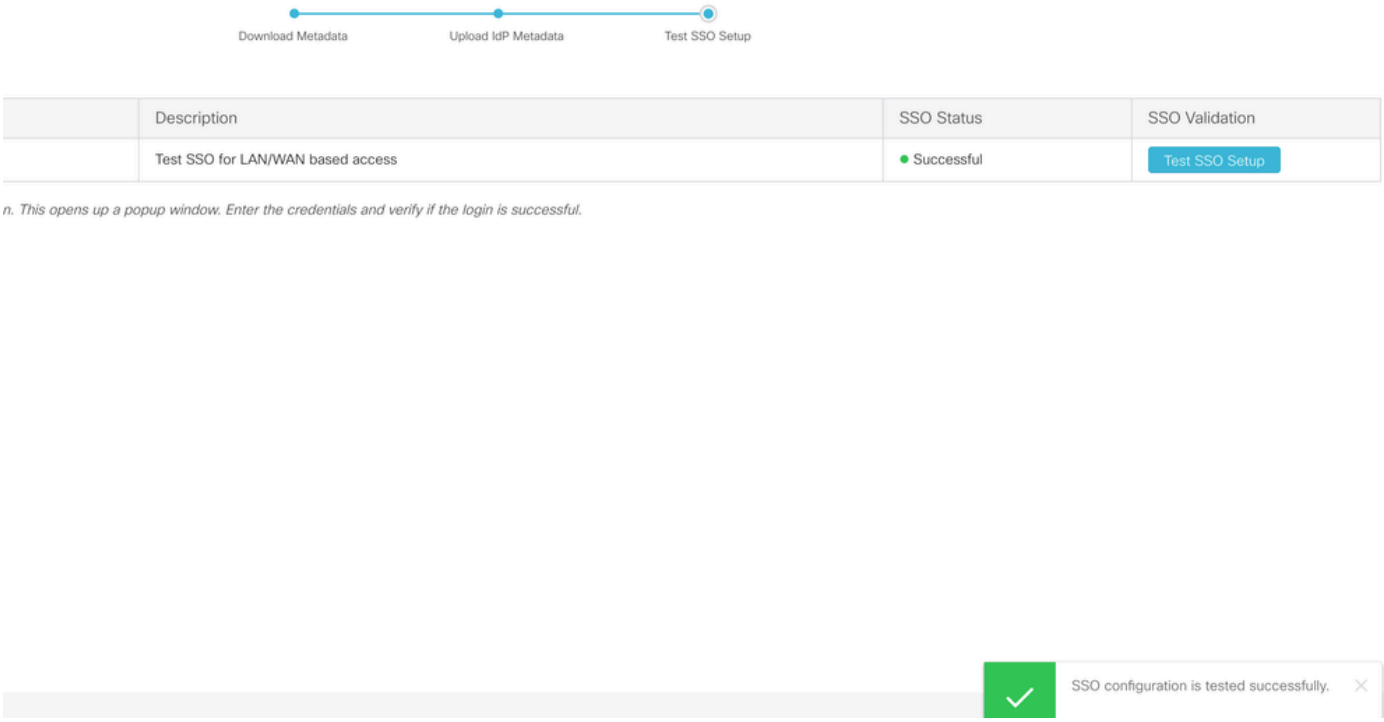
5. 다음 및 마침을 눌러 애플리케이션 구성을 완료합니다.

6. URL을 사용하여 로그인 탭에서 메타데이터를 복사하고 xml로 저장합니다.

7. 6단계의 메타데이터를 CCX 측의 Identity Service 관리 웹 페이지에 업로드합니다.

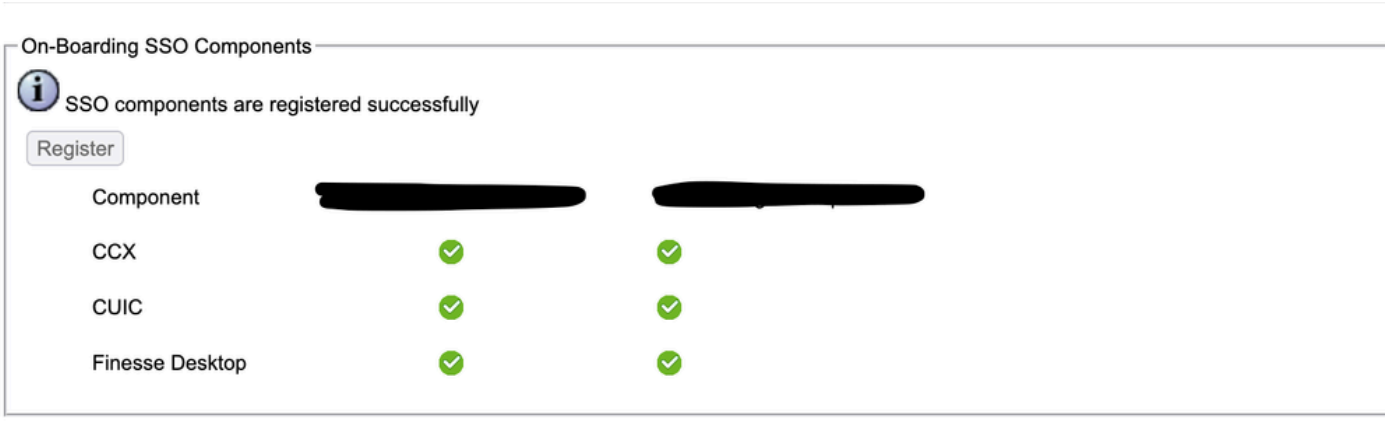


8. 테스트 SSO 설정을 실행하면 성공해야 합니다.



9. admin 사용자로 CCX의 admin 웹 페이지에 로그인하고 System > Single Sign On으로 이동합니다.

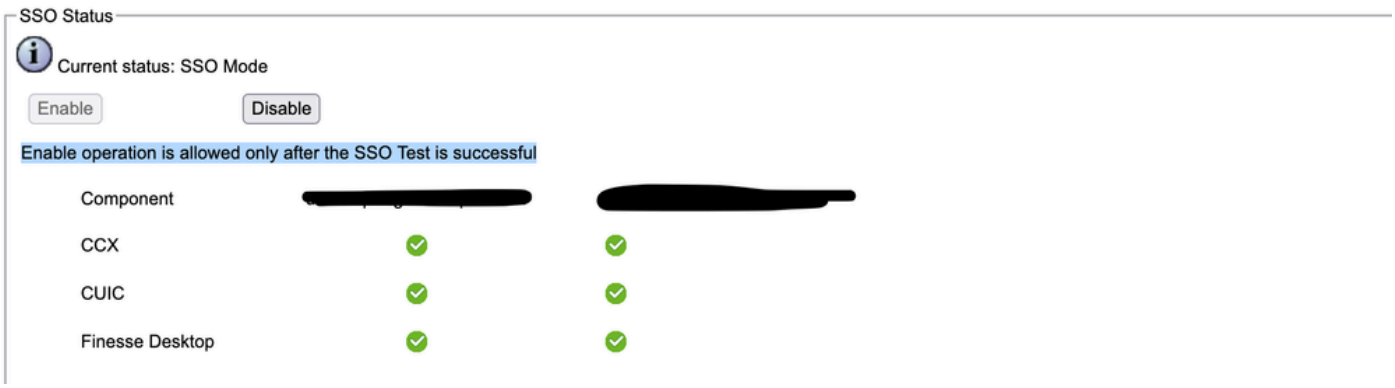
10. 등록 버튼을 눌러 구성품에 등록합니다.



11. Cisco Unified CCX 관리자에게 보고 기능 할당(관리자 기능 보기에서 할당) 및 CLI 명령 활용 cuic user make-admin CCX\<관리자 사용자 ID>을 실행하여 Cisco Unified Intelligence Center에서 관리자 권한을 제공합니다. SSO 테스트 작업에 대해 관리자 권한이 있는 구성된 사용자를 사용합니다.

12. SSO 테스트 작업을 실행합니다.

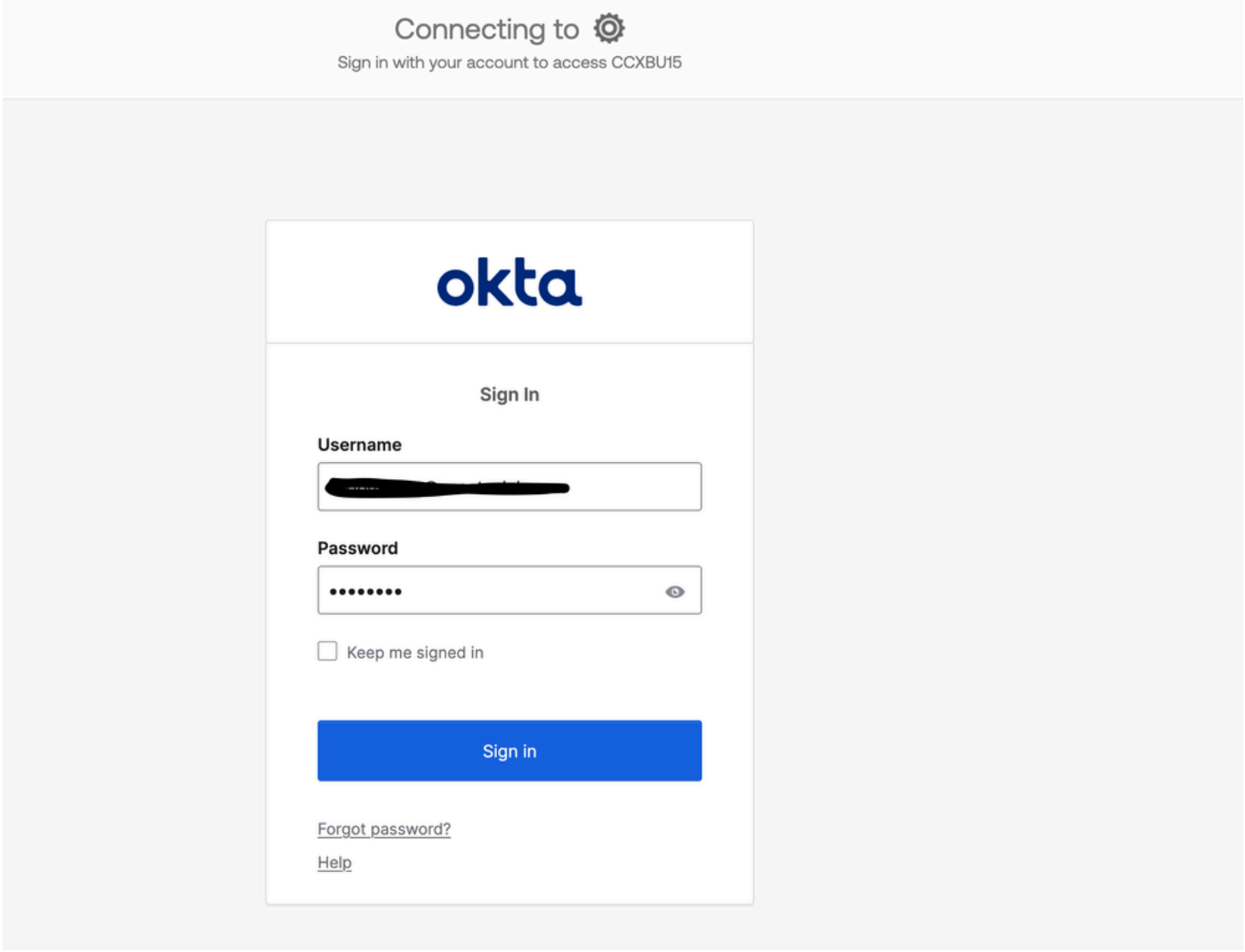
13. SSO 테스트가 성공하면 활성화 작업이 허용됩니다.



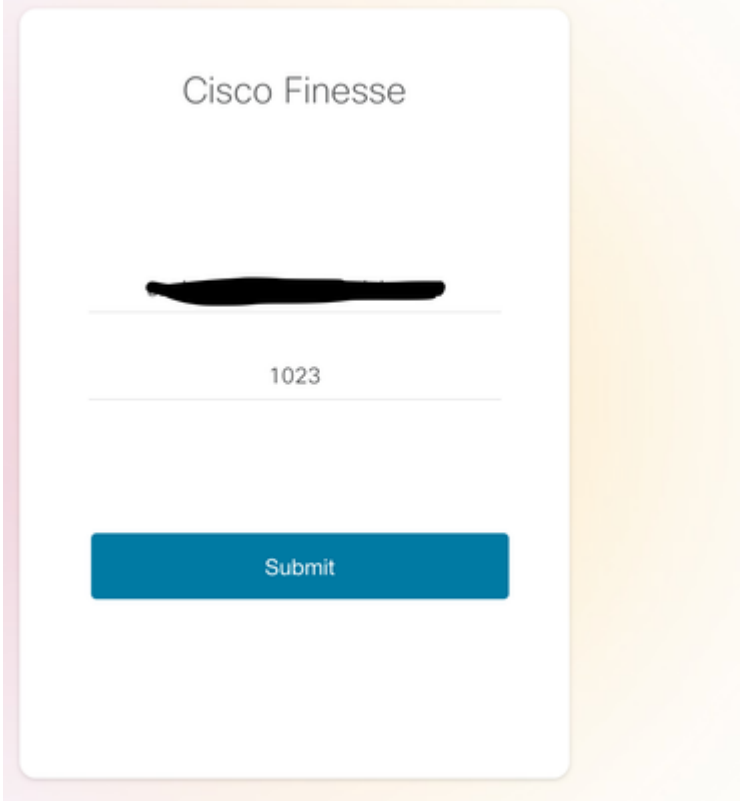
다음을 확인합니다.

CCX, Cisco CUIC(Unified Intelligence Center) 및 Finesse에서 상담원 및 관리자와의 로그인 작업을 확인합니다. 성공해야 합니다.

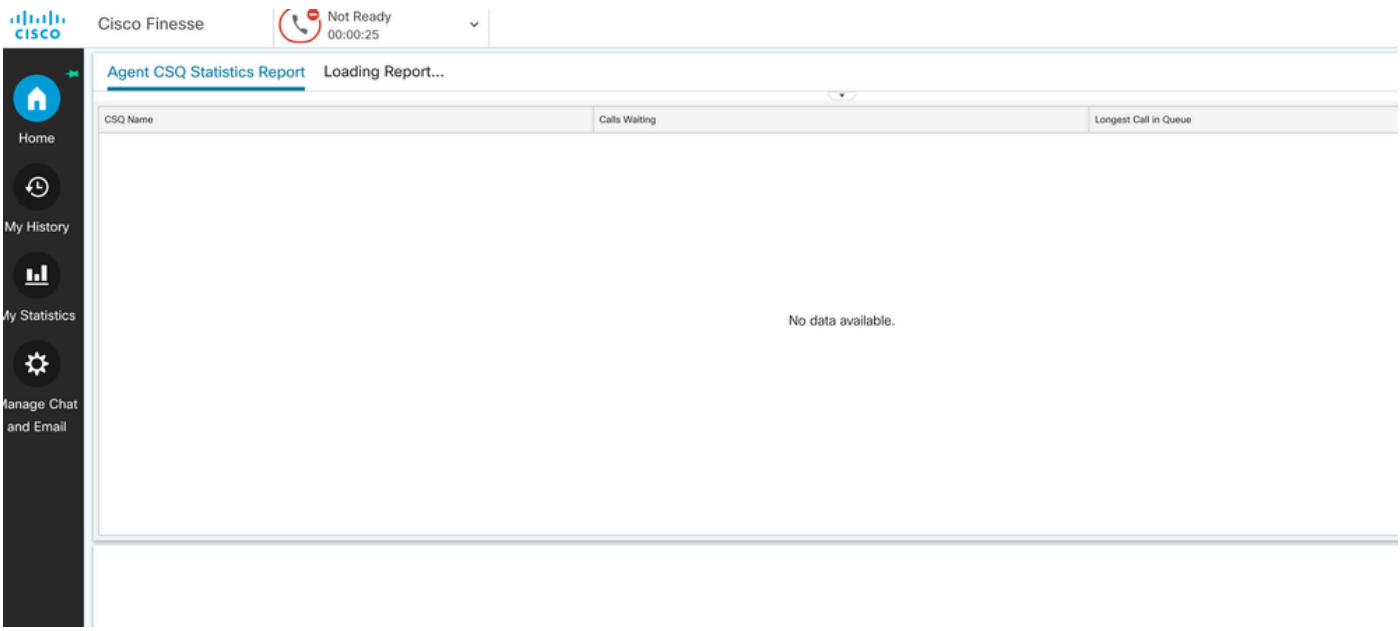
Finesse에서 에이전트를 로그인하면 OKTA 페이지로 리디렉션됩니다.



접속 정보를 입력한 후 finesse 로그인 페이지에서 내선 번호만 요청합니다.



이를 입력한 후에는 로그인에 성공해야 하며 모든 라이브 보고서가 올바르게 로드되어야 합니다.



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.