SMA 최종 사용자 격리를 위한 Okta SAML SSO 구성

목차

소개

이 문서에서는 Okta를 Cisco Secure Email SMA 최종 사용자 격리 액세스를 위한 SAML 2.0 ID 공급자로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- 제품: Cisco Secure SMA(Email Security Management Appliance)
- 기능: EUQ(End User Quarantine)용 SAML SSO
- ID 공급자: 옥타(SAML 2.0)
- 적용 대상: 가상 또는 하드웨어 플랫폼에서 EUQ 액세스를 제공하는 SMA 구축. 예제 호스트 이름 및 포트를 해당 환경의 값으로 대체합니다.
- 버전 컨텍스트: 이 절차는 EUQ용 SAML을 지원하는 SMA 릴리스에 적용됩니다. 설치된 버전에서 사용 가능한 필드 및 메뉴 옵션을 확인합니다.

참고: 이 문서에서는 SMA EUQ SAML 컨피그레이션에 대해 중점적으로 설명합니다. SMA에서 자체 서명 인증서를 생성할 수 없는 경우 ESA는 인증서 생성에만 참조됩니다.

요구 사항

시작하기 전에 다음 사항이 있는지 확인합니다.

- SMA 웹 인터페이스에 대한 관리 액세스.
- SAML 2.0 응용 프로그램을 만들고 사용자 또는 그룹을 할당하기 위한 Okta의 관리 권한
- SMA 서비스 공급자 컨피그레이션을 위한 인증서 및 개인 키. 자체 서명 인증서는 테스트에 사용할 수 있습니다.
- 최종 사용자가 브라우저에서 액세스할 수 있는 연결 가능한 SMA EUQ FQDN(정규화된 도메인 이름) 및 포트.
- SMA SAML Assertion URL 및 SP Entity ID 값(SP 항목을 생성한 후 System Administration > SAML에서).
- Okta 응용 프로그램에 할당된 Okta의 사용자 계정입니다.
- 구축에서 디렉토리 통합을 사용하는 경우 디렉토리 동기화된 사용자.

참고: Okta는 서드파티 ID 공급자입니다. 이 문서에서는 고객 참조를 위한 샘플 컨피그레이션을 제공합니다.

사용되는 구성 요소

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.

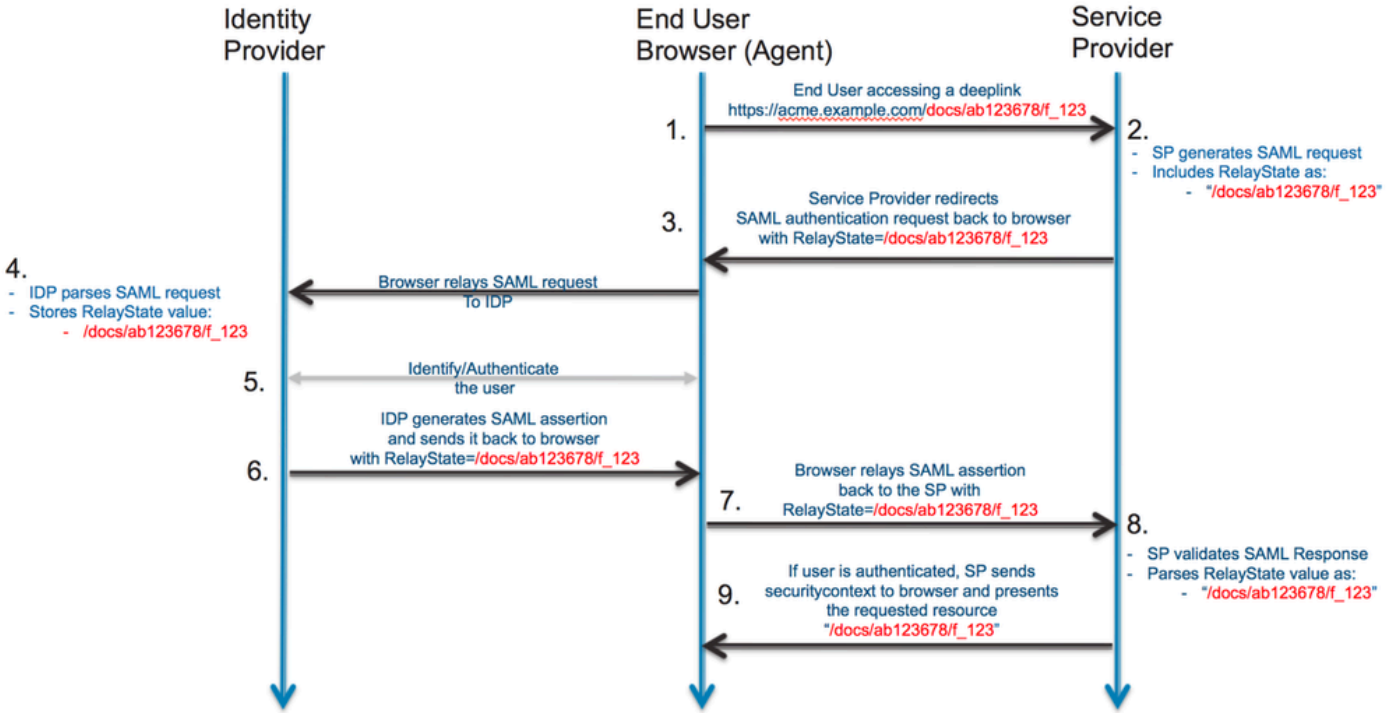
배경 정보

스팸 격리 포털에 대한 SSO(Single Sign-On)를 구성하여 사용자가 Okta로 리디렉션되어 인증하고, Okta에서 MFA(multifactor authentication)가 활성화된 경우 이를 완료한 다음 SMA EUQ 포털로 돌아가도록 하는 것이 목표입니다. 이 문서는 SMA에만 적용됩니다. Cisco Secure Email Gateway, 이전의 ESA(Email Security Appliance)는 SMA에서 자체 서명 인증서를 생성할 수 없는 경우 인증서 생성에만 참조됩니다.

문제/장애: 사용자는 SAML SSO 및 선택적 MFA를 사용하여 OCTA로 SMA 스팸 격리 포털에 인증해야 합니다.

해결 방법: SMA를 서비스 공급자로 구성하고, Okta에서 SAML 애플리케이션을 구성하고, Okta IdP 설정을 SMA로 가져오고, Okta에서 사용자를 할당하고, 액세스를 확인합니다.

SAML 흐름:



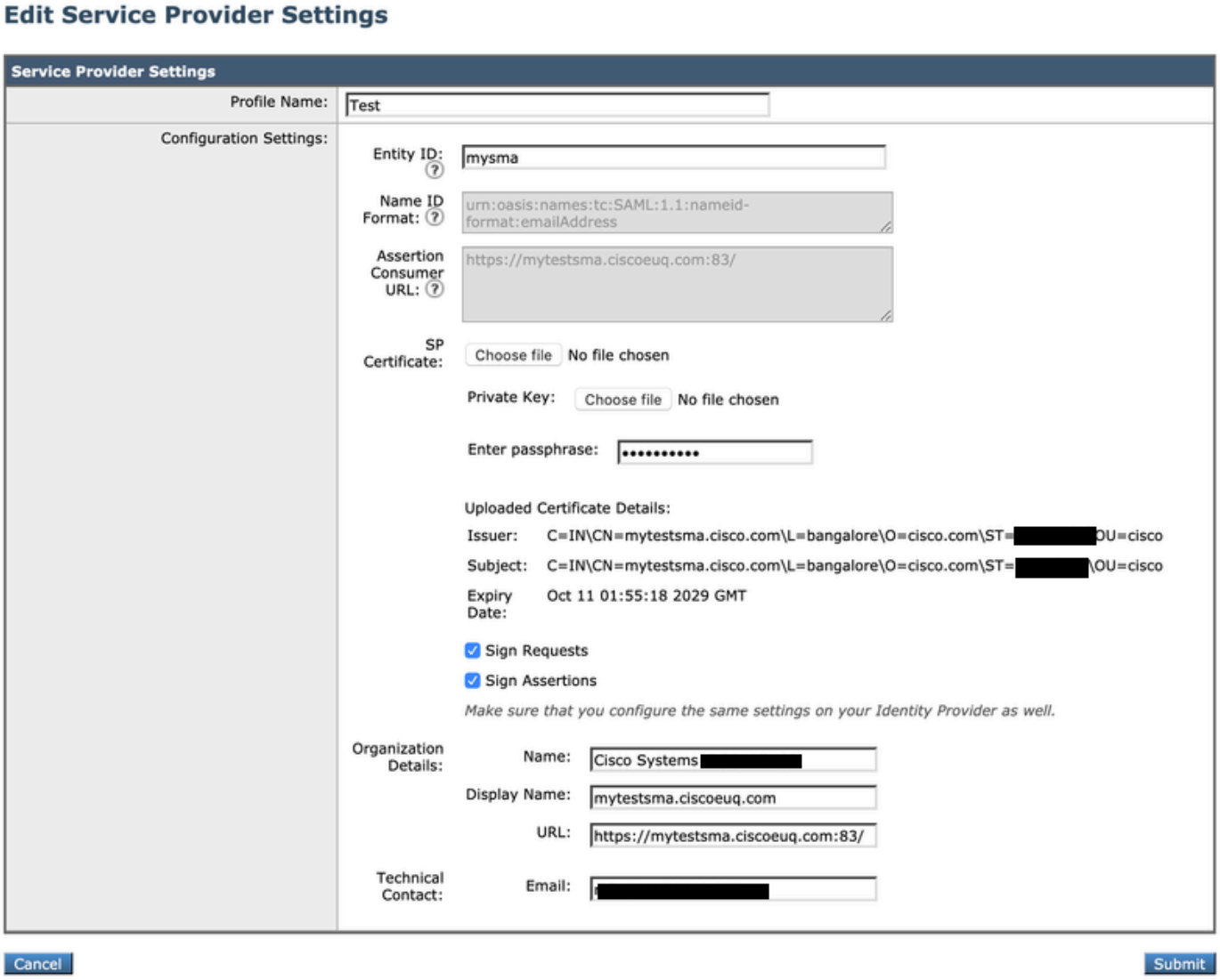
설정

SMA 어플라이언스에서 SP(서비스 공급자) 구성

EUQ 액세스를 위한 SAML 서비스 공급자로 SMA를 구성하는 절차는 다음과 같습니다.

1. SMA 웹 인터페이스에 로그인합니다.
2. System Administration(시스템 관리) > SAML로 이동합니다.
3. Add Service Provider를 선택합니다.
4. Service Provider Entity ID(서비스 공급자 엔티티 ID)에서 Okta(okta)에서도 구성할 수 있는 엔티티 ID를 입력합니다.
5. EUQ 인터페이스에 대해 이름 ID 형식 및 Assertion ACS(Consumer Service) URL이 채워졌는지 확인합니다.
6. SP Certificate(SP 인증서)에서 SAML 요청에 서명할 인증서를 업로드합니다.

참고: SMA에서 자체 서명 인증서를 생성할 수 없습니다. ESA에서 인증서를 생성하고 SMA에서 사용하도록 내보낼 수도 있습니다.

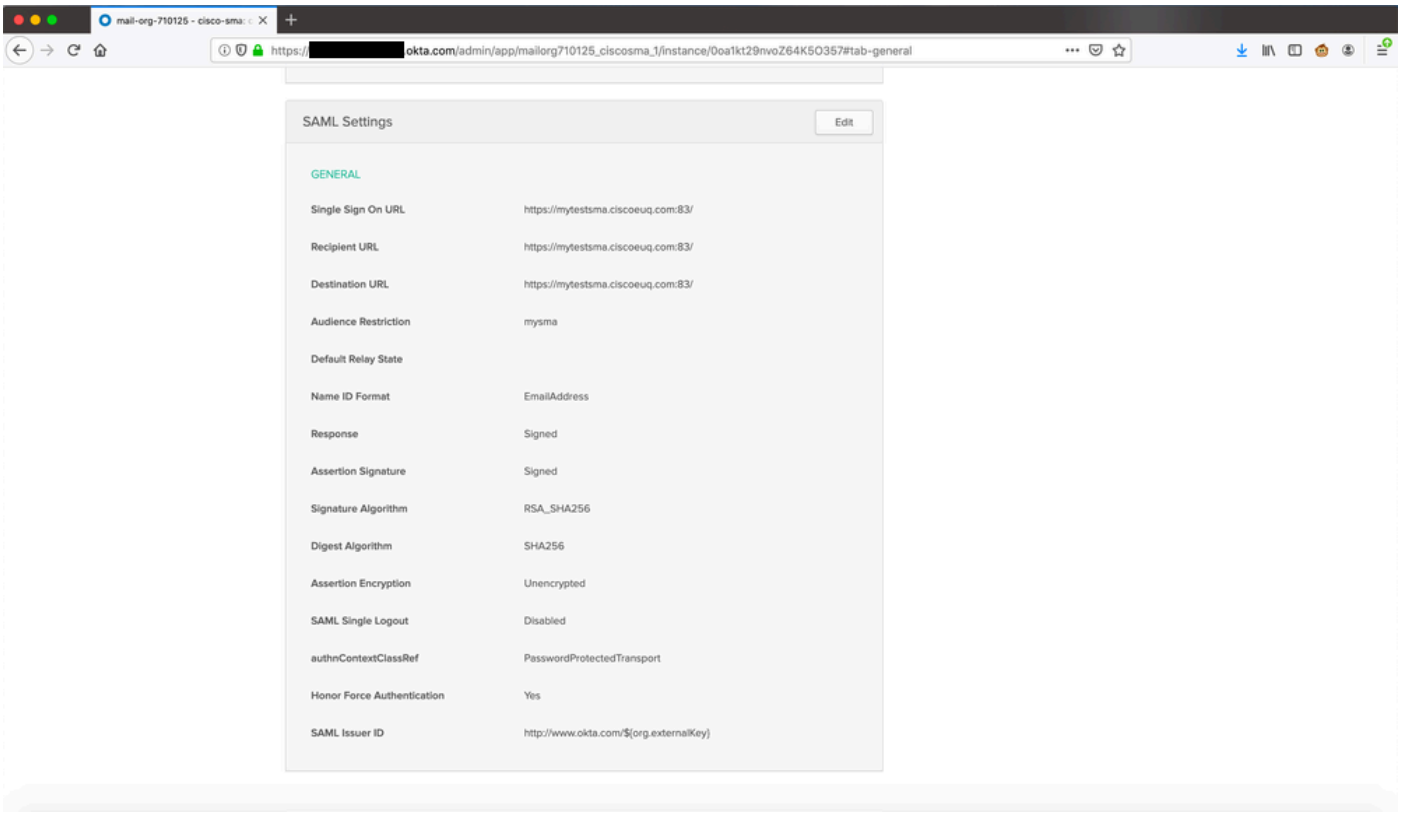


GUI의 서비스 공급자 설정

Okta에서 SAML 애플리케이션 구성

SMA EUQ 액세스를 위해 Okta에서 SAML 2.0 애플리케이션을 만드는 절차는 다음과 같습니다.

1. Okta에 관리자로 로그인합니다.
2. Applications(애플리케이션) > Applications(애플리케이션)로 이동한 다음 Create App Integration(애플리케이션 통합 생성)을 선택합니다.
3. SAML 2.0을 선택하고 다음을 선택합니다.
4. SMA EUQ와 같은 앱 이름을 입력한 다음, Next(다음)를 선택합니다.
5. Single sign-on URL의 SMA 서비스 공급자 설정에서 SMA ACS URL을 입력합니다.
6. Audience URI(SP Entity ID)에 SMA에 구성된 동일한 엔터티 ID를 입력합니다.
7. 이름 ID 형식으로 EmailAddress를 선택합니다.
8. 애플리케이션 사용자 이름에서 구축에 적합한 Okta 사용자 이름 형식을 선택합니다.
9. 마법사를 완료한 다음 새 응용 프로그램을 열고 IdP 메타데이터 XML 파일 또는 메타데이터 URL을 복사하십시오!를

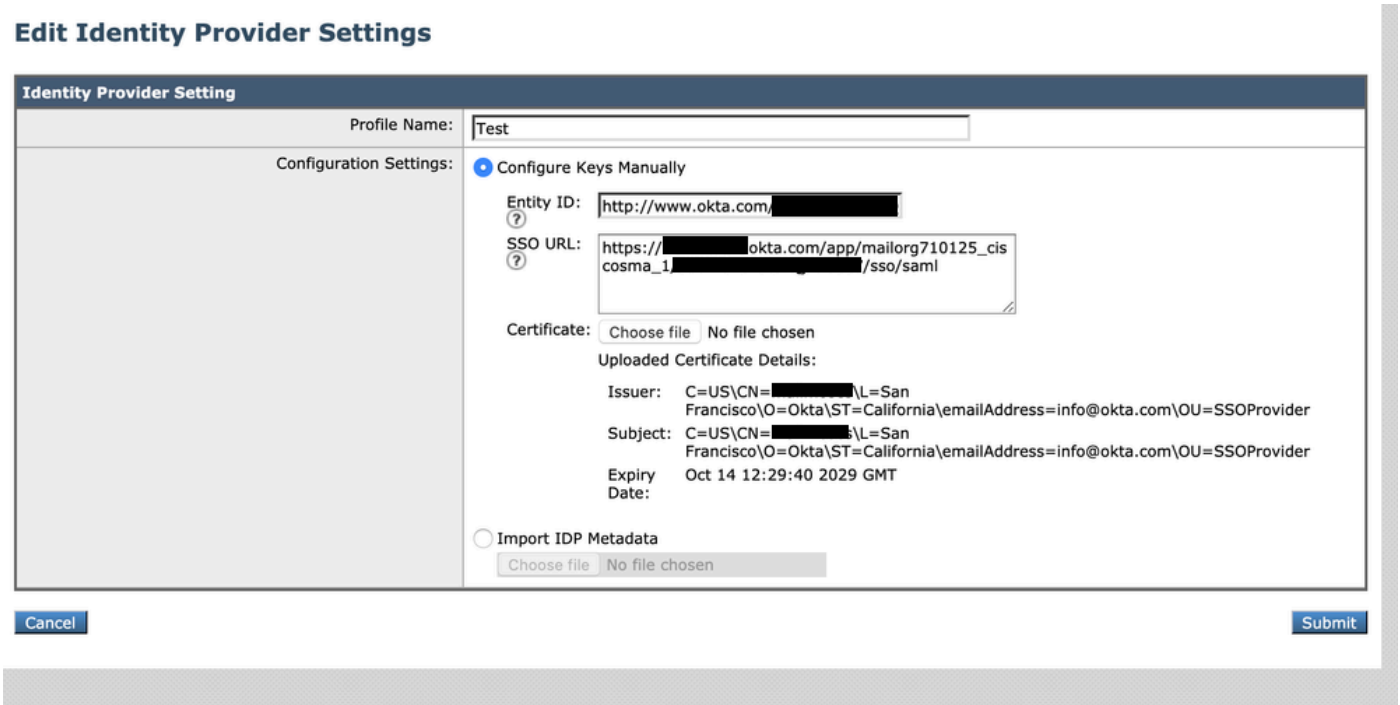


Okta 포털 보기

SMA 어플라이언스에 IdP(Identity Provider) 구성

SMA에서 Okta를 IdP(ID 제공자)로 구성하는 절차는 다음과 같습니다.

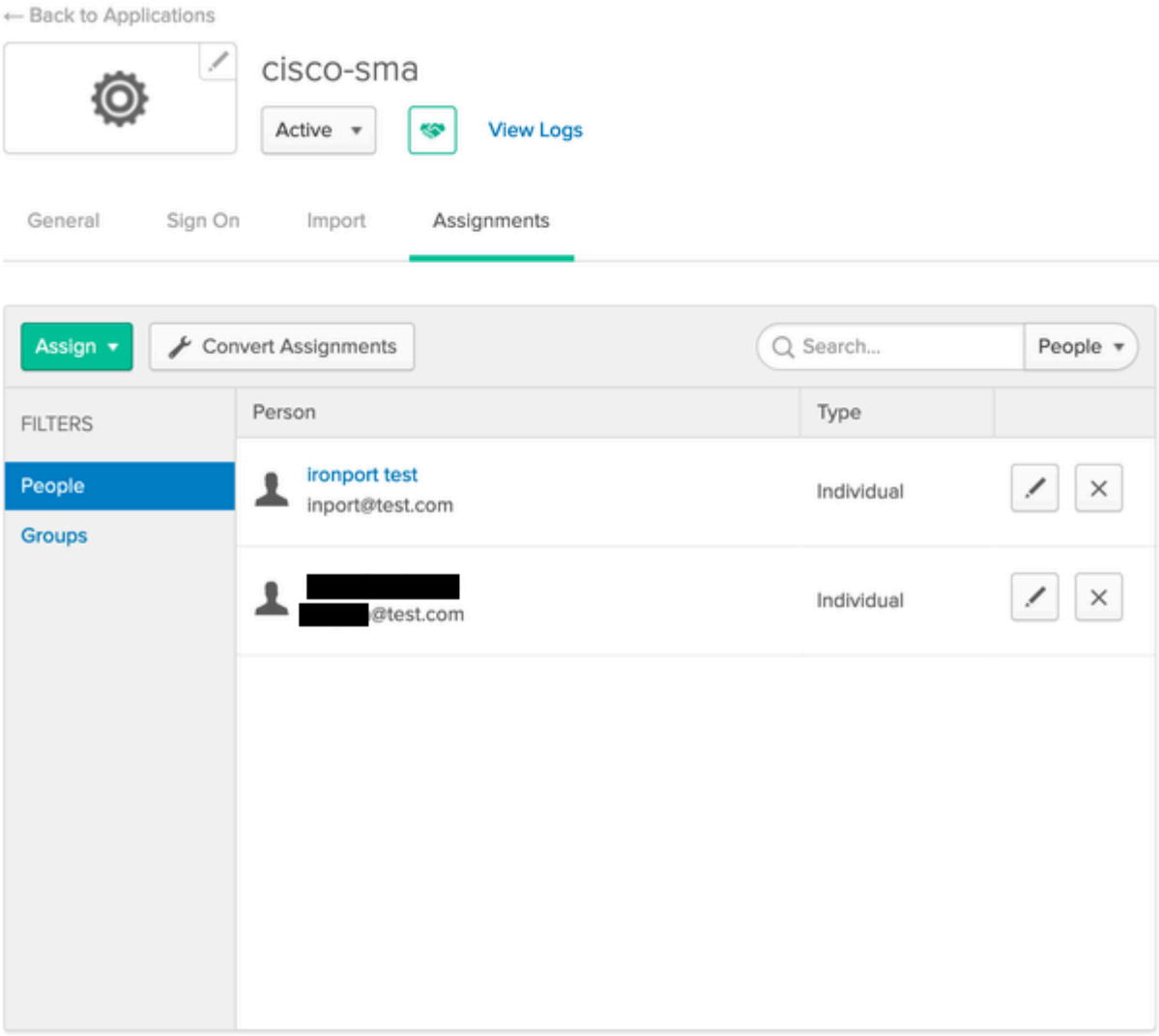
1. SMA 웹 인터페이스에 로그인합니다.
2. System Administration(시스템 관리) > SAML로 이동합니다.
3. Identity Provider Settings(ID 제공자 설정)에서 이전 섹션에서 Okta IdP 메타데이터를 가져오거나 값을 수동으로 입력합니다.



Okta 애플리케이션에 사용자 할당

사용자가 Okta를 통해 SMA EUQ에 인증하도록 허용하려면 Okta 애플리케이션에 사용자 또는 그룹을 할당합니다.

1. 옥타에서 생성한 애플리케이션을 엽니다.
2. 발령 > 인력으로 이동한 다음, 발령을 선택합니다.
3. 각 사용자 옆에서 Assign(할당)을 선택한 다음 Done(완료)을 선택합니다.



Okta 포털에서 사용자 할당

참고: 사용자를 수동으로 할당하거나, Active Directory에서 사용자를 동기화하거나, Okta가 지원하는 다른 디렉토리 통합을 사용할 수 있습니다.

옥타에서 MFA 구성(선택 사항)

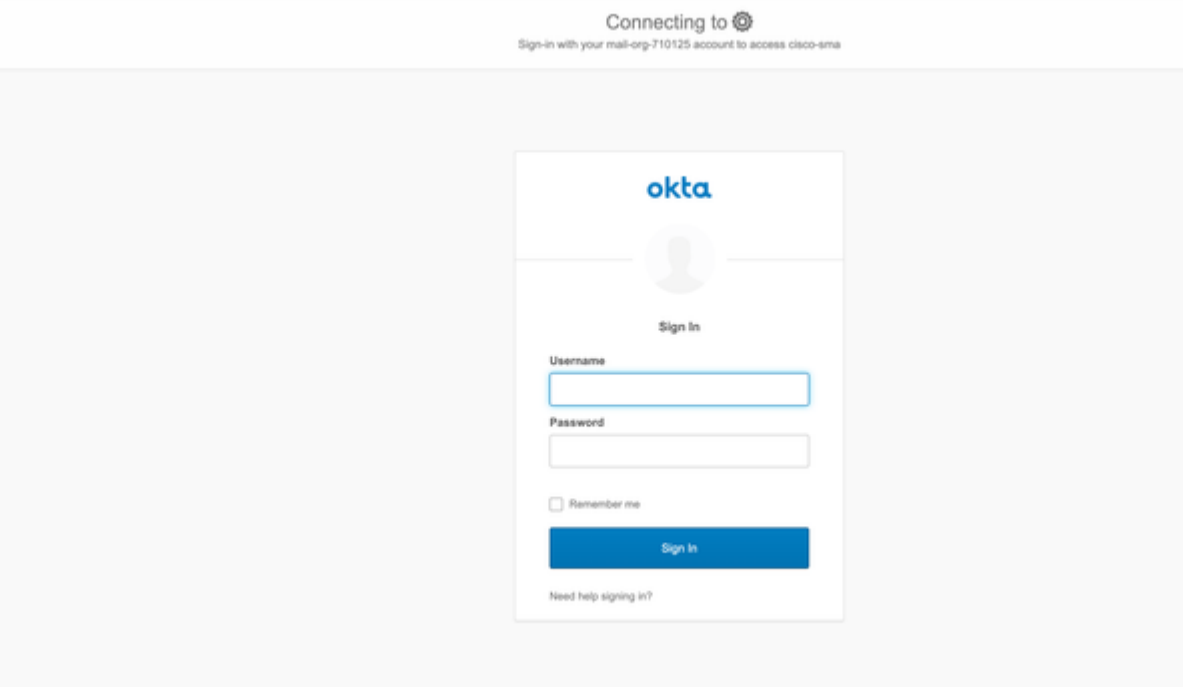
EUQ 액세스에 MFA(multifactor authentication)를 사용하려면 애플리케이션에 대해 Okta에서 MFA 정책을 구성합니다.

1. Okta Admin에서 Security > Authentication으로 이동합니다.
2. Okta Verify, Google Authenticator, SMS와 같은 필수 요소를 구성하고 SMA EUQ 애플리케이션에 정책을 적용합니다.

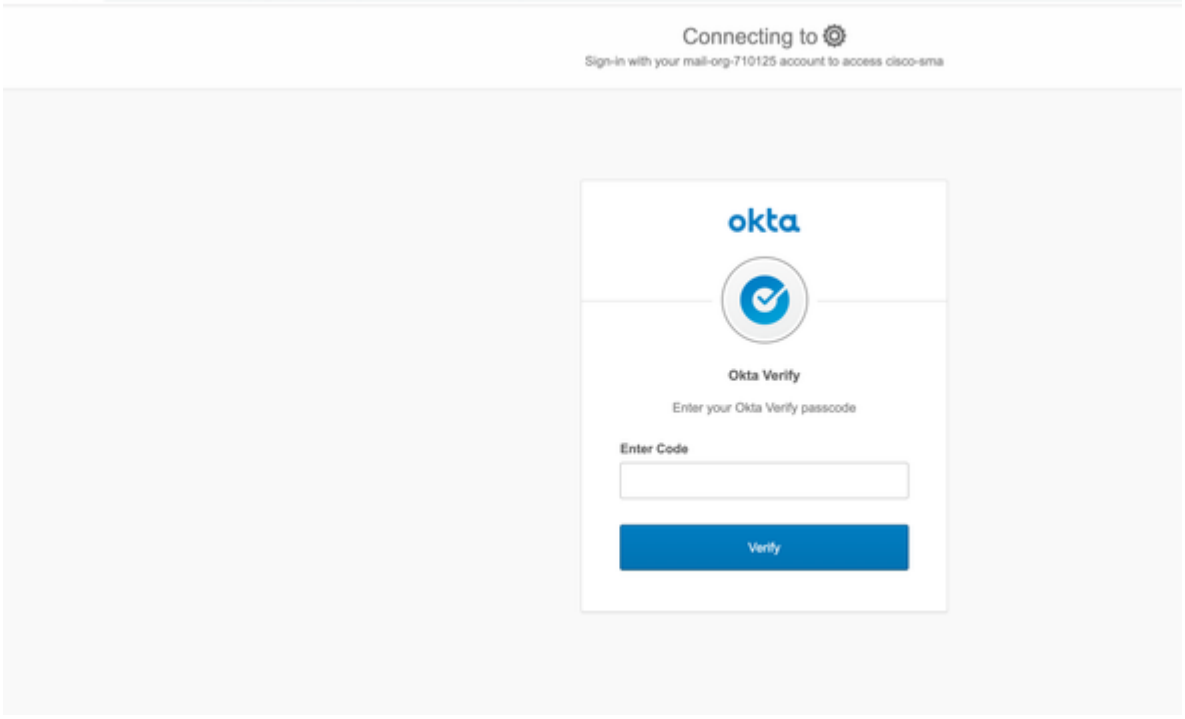
SAML 로그인 확인

예상 결과: 컨피그레이션을 확인하는 절차는 다음과 같습니다.

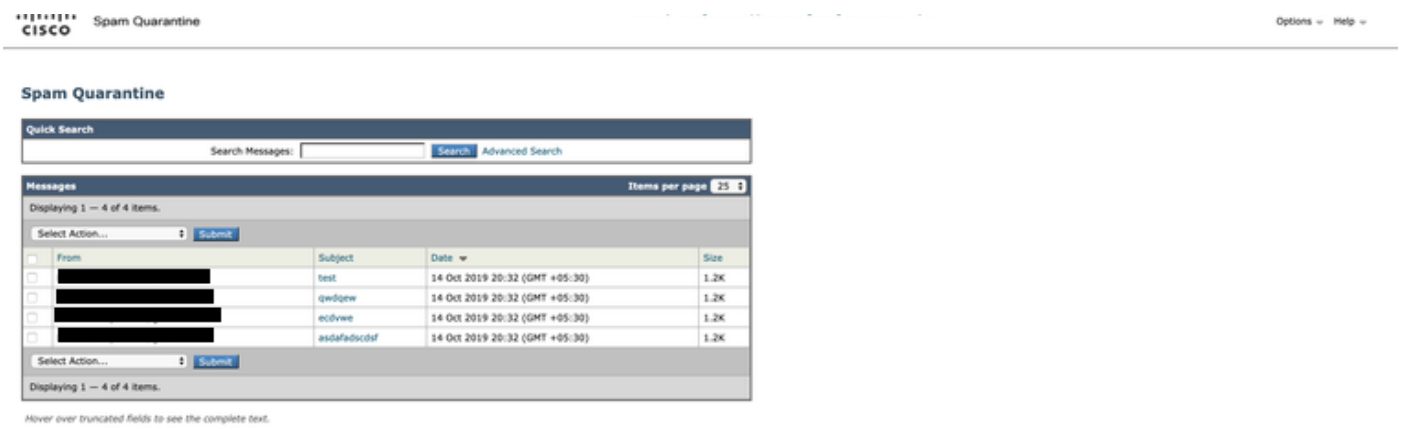
1. SMA EUQ URL(예: https://<sma-fqdn>:<port>/)을 찾습니다.
2. 브라우저에서 인증을 위해 Okta로 리디렉션하는지 확인합니다.
3. MFA가 활성화된 경우 MFA 챌린지를 완료합니다.
4. SMA 스팸 격리 포털로 다시 리디렉션되고 격리 기능에 액세스할 수 있는지 확인합니다.



Okta를 사용하여 로그인



Okta Verify 코드 입력



Okta로 로그인한 후 스팸 쿼런틴 보기

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.