고급 피싱 보호를 위한 OKTA SSO 외부 인증 구성

목차

소개

이 문서에서는 Cisco Advanced Phishing Protection에 로그인하기 위해 OKTA SSO 외부 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

Cisco Advanced Phishing Protection 포털에 대한 관리자 액세스 권한

Okta idP에 대한 관리자 액세스

PKCS #12 또는 PEM 형식의 자체 서명 또는 CA 서명(선택 사항) X.509 SSL 인증서

배경 정보

- Cisco Advanced Phishing Protection을 사용하면 SAML을 사용하는 관리자의 SSO 로그인을 활성화할 수 있습니다.
- OKTA는 애플리케이션에 인증 및 권한 부여 서비스를 제공하는 ID 관리자입니다.
- Cisco Advanced Phishing Protection은 인증 및 권한 부여를 위해 OKTA에 연결된 애플리케이션으로 설정할 수 있습니다.
- SAML은 XML 기반 개방형 표준 데이터 형식으로, 관리자가 정의된 애플리케이션 중 하나에 로그인한 후 해당 애플리케이션에 원활하게 액세스할 수 있습니다.
- SAML에 대해 자세히 알아보려면 다음 링크인 SAML General Information(SAML 일반 정보)에 액세스할 수 있습니다.

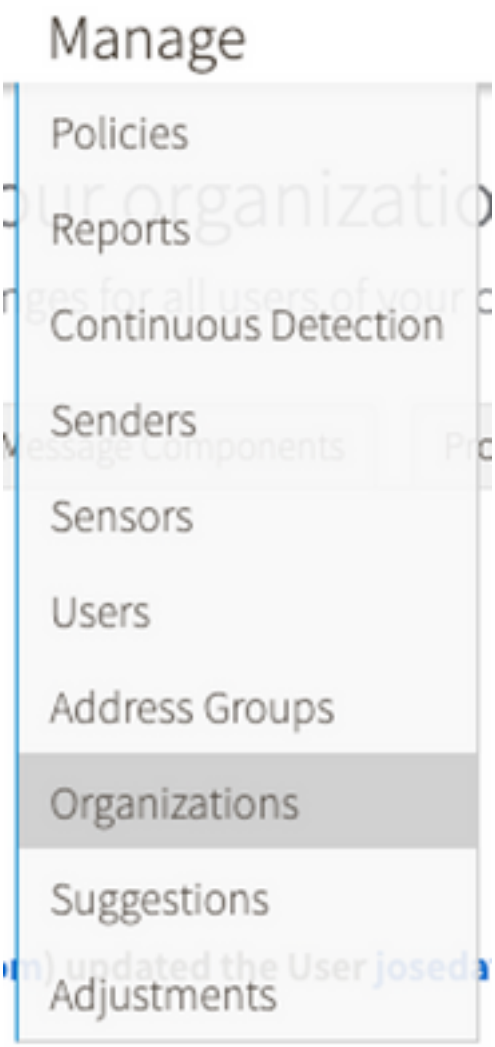
요구 사항

- Cisco Advanced Phishing Protection 포털
- OKTA 관리자 계정입니다.

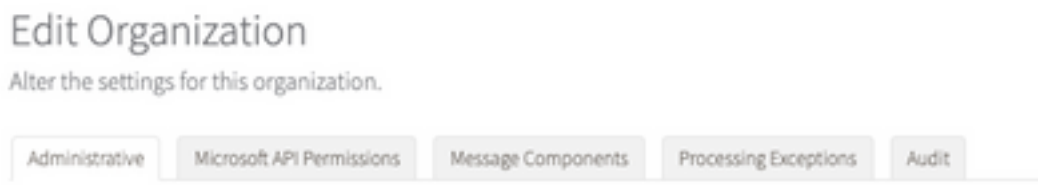
구성

Cisco Advanced Phishing Protection Portal에서

1. 이미지에 표시된 대로 조직 포털에 로그인한 다음 **관리 > 조직**을 선택합니다.



2. 이미지에 표시된 대로 **조직명** 조직 편집을 선택합니다.



3. 이미지**와** 같이 **Administrative**(관리) 탭에서 User Account Settings(**사용자 계정 설정**)로 아래로 스크롤하고 SSO(SSO)에서 **Enable(활성화)**을 선택합니다.

4. 다음 창에서는 OKTA SSO 컨피그레이션에 입력할 정보를 제공합니다. 다음 정보를 메모장에 붙여 넣고 OKTA 설정을 구성하는 데 사용합니다.

- 엔터티 ID: apcc.cisco.com

- 어설션 소비자 서비스: 이 데이터는 조직에 맞게 조정됩니다.

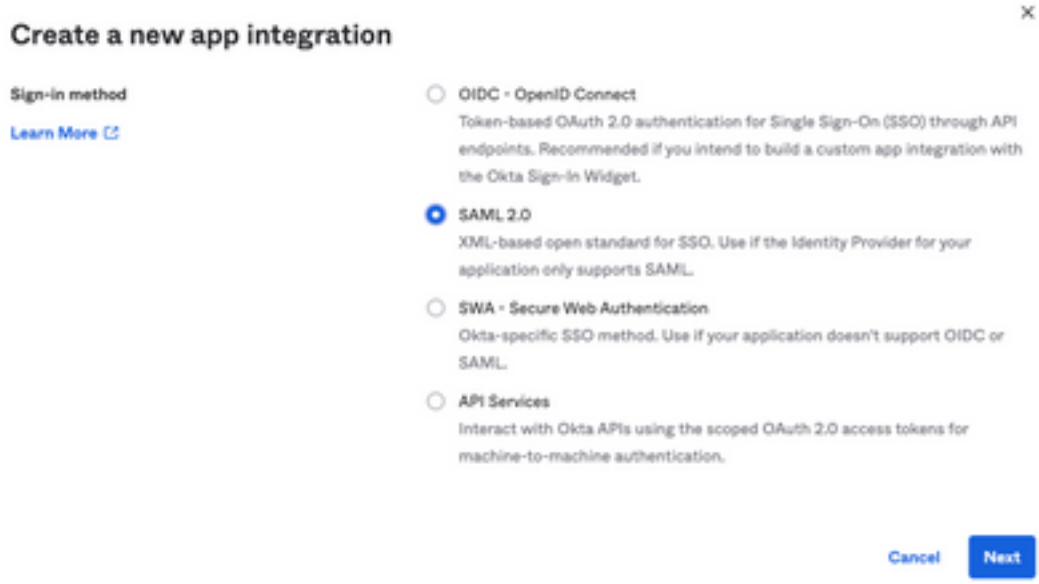
이미지에 표시된 이름**이 지정된** 전자 메일 주소를 로그인에 사용하려면 전자 메일을 선택합니다.

5. 다음 단계로 진행하기 전에 먼저 OKTA에서 애플리케이션을 설정해야 하므로 지금 Cisco Advanced Phishing Protection 구성을 최소화합니다.

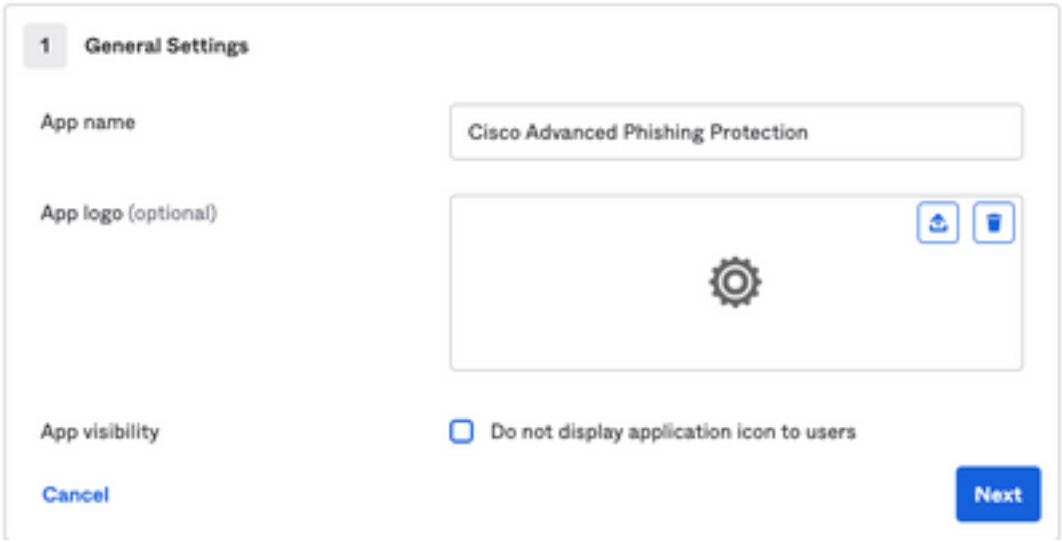
옥타 밑에

1. 이미지에 표시된 대로 Applications portal(애플리케이션 포털)로 이동하고 **Create App Integration(앱 통합 생성)**을 선택합니다.

2. 이미지에 표시된 대로 애플리케이션 유형으로 SAML **2.0**을 선택합니다.



3. 이미지에 표시된 대로 **Advanced Phishing Protection**이라는 앱 이름을 입력하고 다음을 **선택합니다**.



4. SAML 설정에서 이미지에 표시된 대로 간격을 채웁니다.

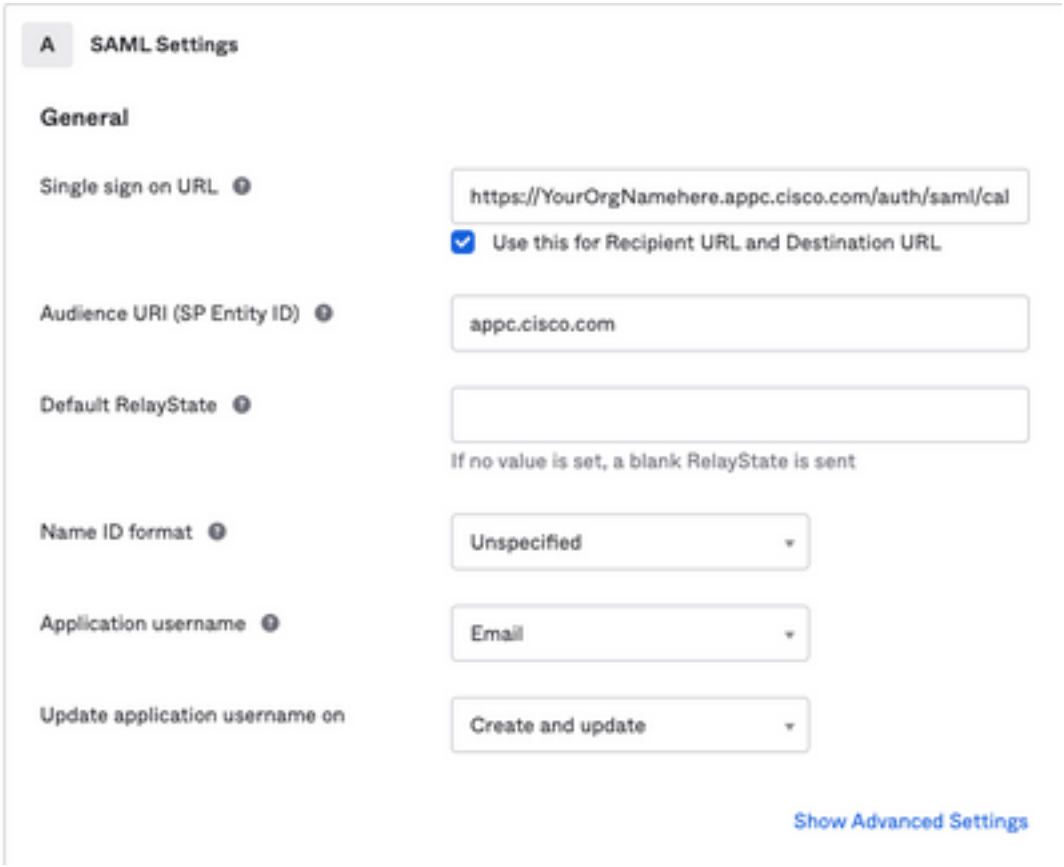
- 단일 로그인 URL: Cisco Advanced Phishing Protection에서 얻은 Assertion Consumer Service입니다.

- 수신자 URL: Cisco Advanced Phishing Protection에서 얻은 엔티티 ID입니다.

- 이름 ID 형식: 지정되지 않은 상태로 유지합니다.

- 애플리케이션 사용자 이름: 인증 프로세스에서 이메일 주소를 입력하라는 메시지를 표시하는 이메일

- 애플리케이션 사용자 이름 업데이트: 생성 및 업데이트



그림과 같이 아래로 스크롤하여 **Group Attribute Statements(선택 사항)**로 이동합니다.

다음 특성 명령문을 입력합니다.

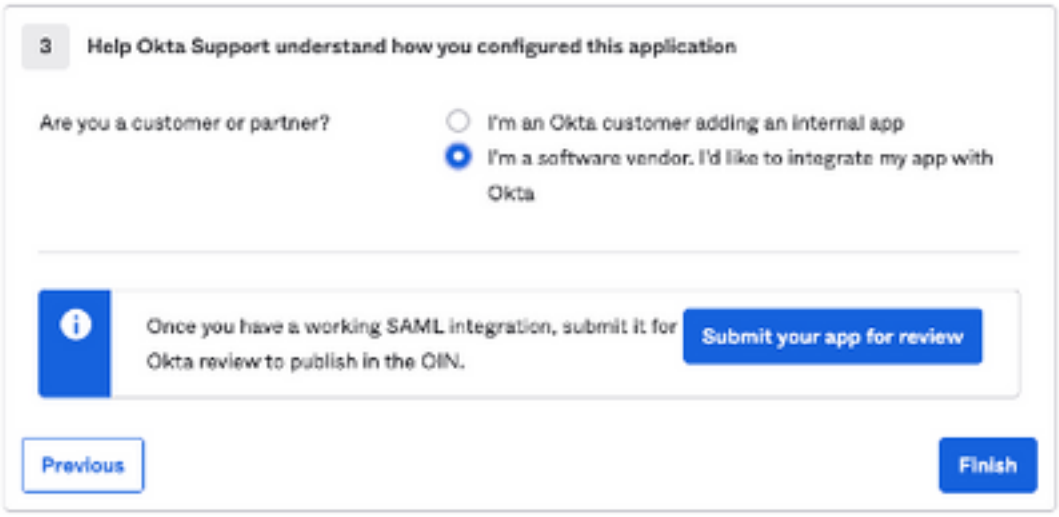
-이름: 그룹

- 이름 형식: 지정되지 않음.

- 필터: "Equals" 및 "OKTA"

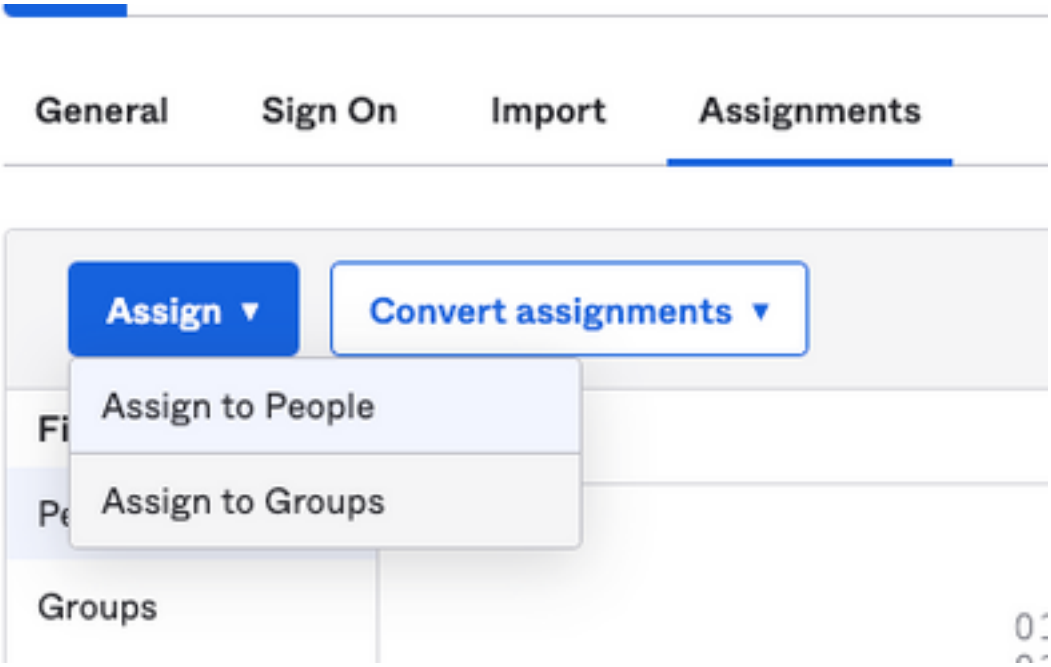
다음을 선택합니다.

5. Okta가 이 애플리케이션을 구성한 방법을 이해하도록 도와달라는 요청을 받았을 때, 이미지에 표시된 대로 현재 환경에 적용할 수 있는 이유를 입력하십시오.



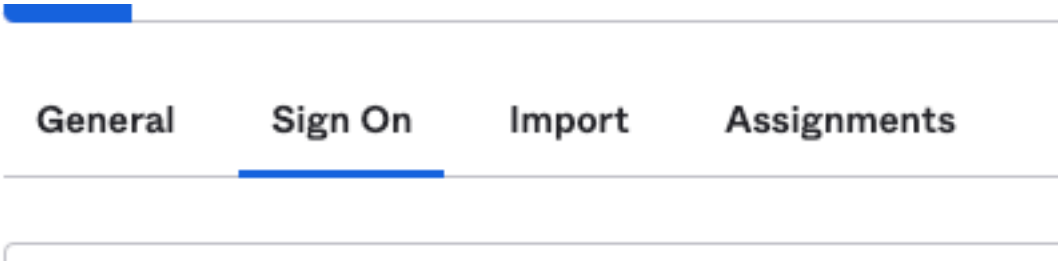
다음 **단계**로 진행하려면 Finish를 선택합니다.

6. 이미지와 같이 **지정** 탭을 선택한 다음 **지정 > 그룹에 지정**을 선택합니다.

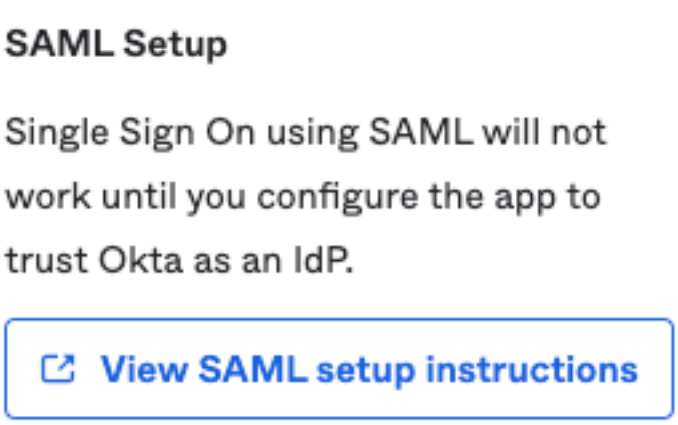


7. 환경에 액세스할 권한이 있는 사용자가 있는 그룹인 OKTA 그룹을 선택합니다

8. **이미지에** 표시된 대로 사인온을 선택합니다.



9. 아래로 스크롤하여 오른쪽 코너로 이동한 다음 이미지에 표시된 대로 **SAML 설정 지시사항** 보기 옵션을 입력합니다.

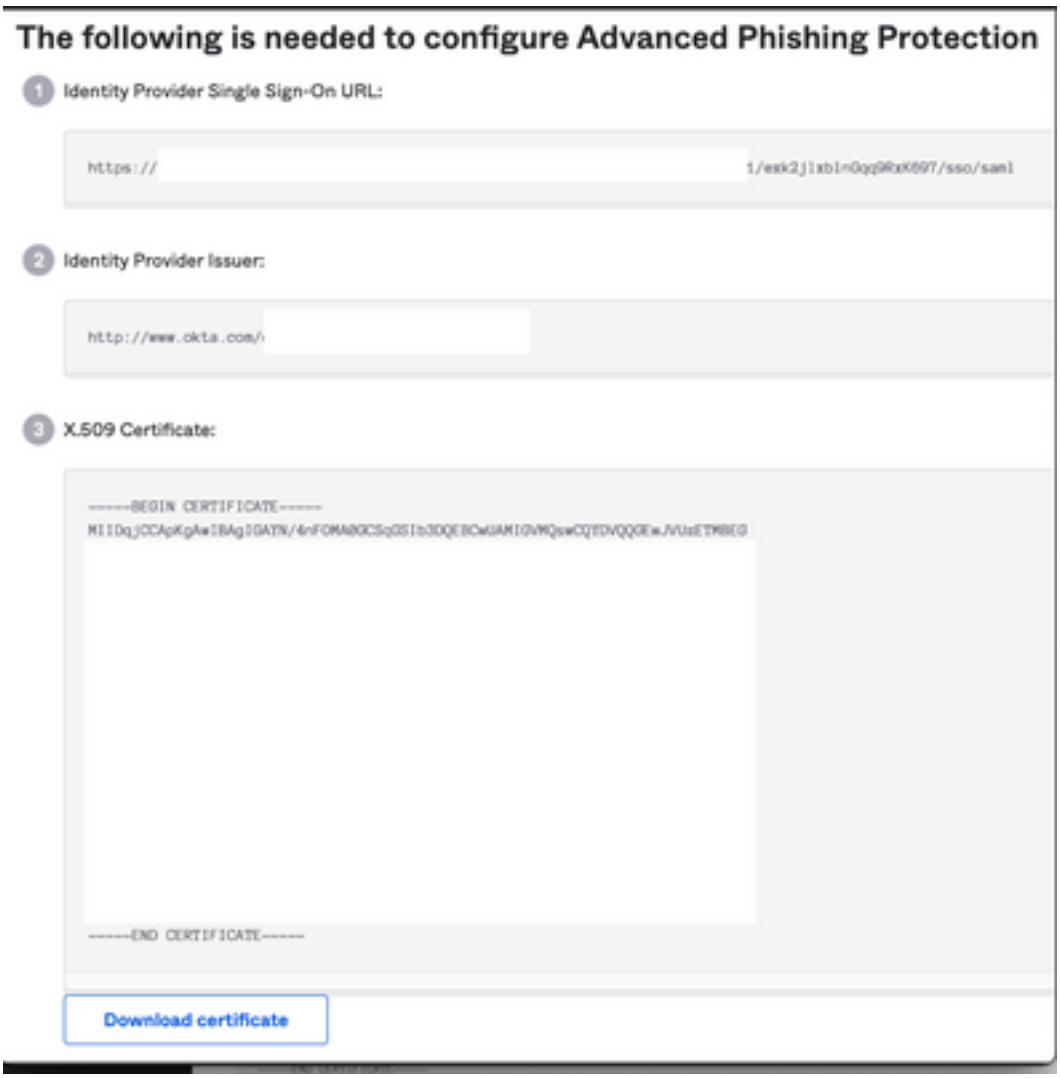


9. 이미지에 표시된 대로 Cisco Advanced Phishing Protection 포털에 입력하는 데 필요한 다음 정보를 메모장에 저장합니다.

- ID 공급자 단일 Sing-On URL

- 공급자 발행자 확인(Cisco Advanced Phishing Protection의 경우 필요하지 않지만 다른 애플리케이션의 경우 필수)

- X.509 인증서



10. OKTA 컨피그레이션을 완료하면 Cisco Advanced Phishing Protection으로 돌아갈 수 있습니다

Cisco Advanced Phishing Protection Portal에서

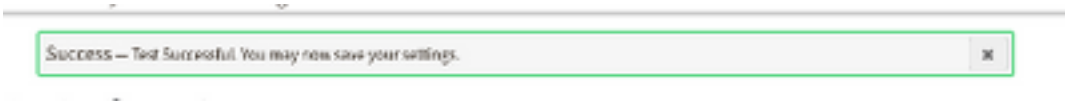
1. 이름 식별자 포맷으로 다음 정보를 입력합니다.

- SAML 2.0 엔드포인트(HTTP 리디렉션): Okta에서 제공하는 ID 공급자 Single Sign-On URL입니다.

- 공용 인증서: Okta에서 제공하는 X.509 인증서를 입력합니다.

2. **테스트 설정**을 선택하여 구성이 올바른지 확인합니다

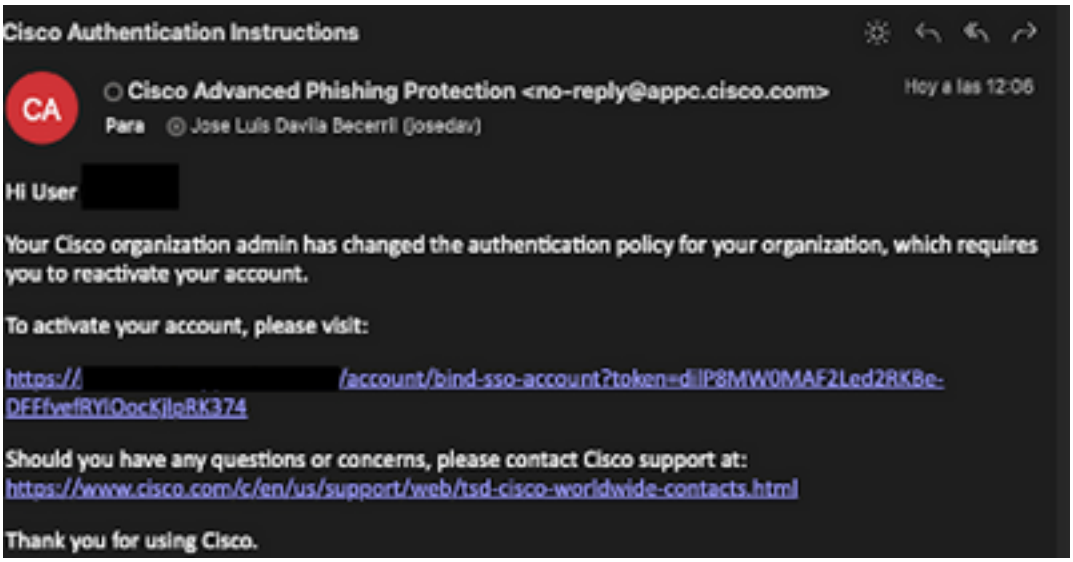
컨피그레이션에 오류가 없는 경우, 이미지에 표시된 대로 테스트 성공 항목이 표시되고 이제 설정을 저장할 수 있습니다.



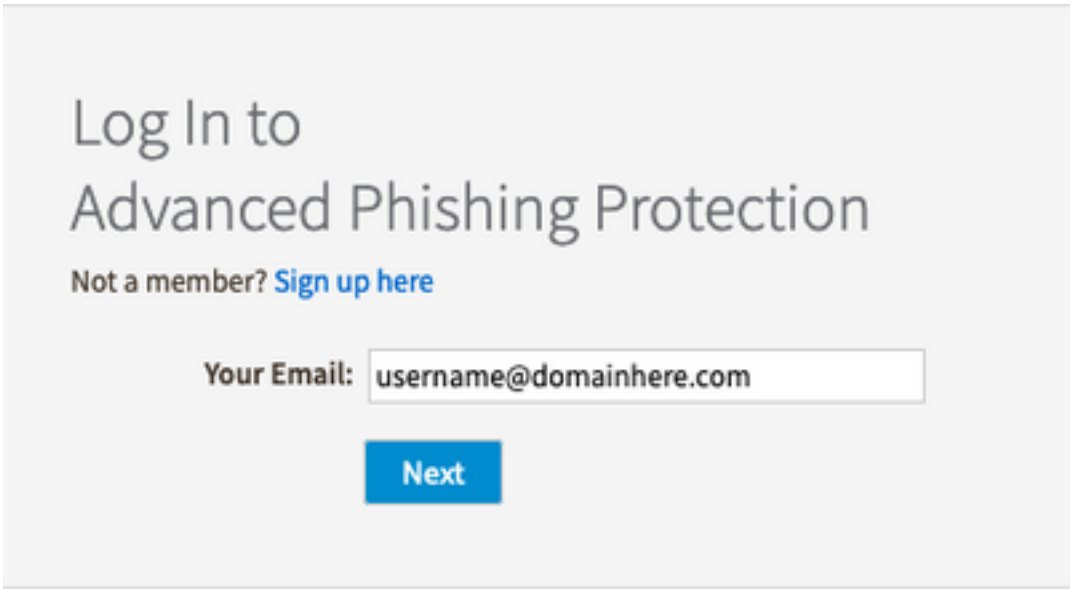
3. 설정 저장

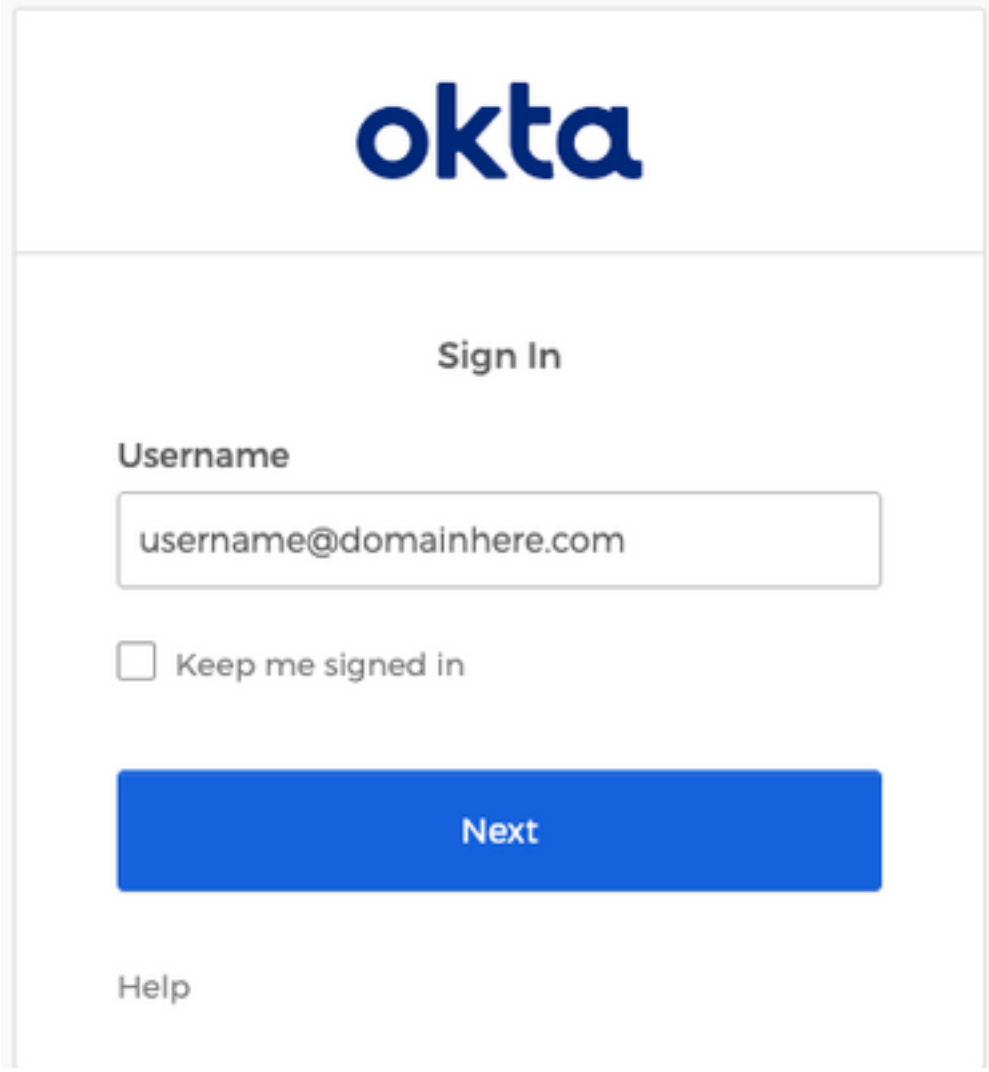
다음을 확인합니다.

1. SSO를 사용하지 않는 기존 관리자의 경우, 전자 메일을 통해 조직에 대한 인증 정책이 변경되었다는 알림을 받으며, 이미지에 표시된 것처럼 외부 링크를 사용하여 계정을 활성화하라는 메시지가 관리자에게 표시됩니다.

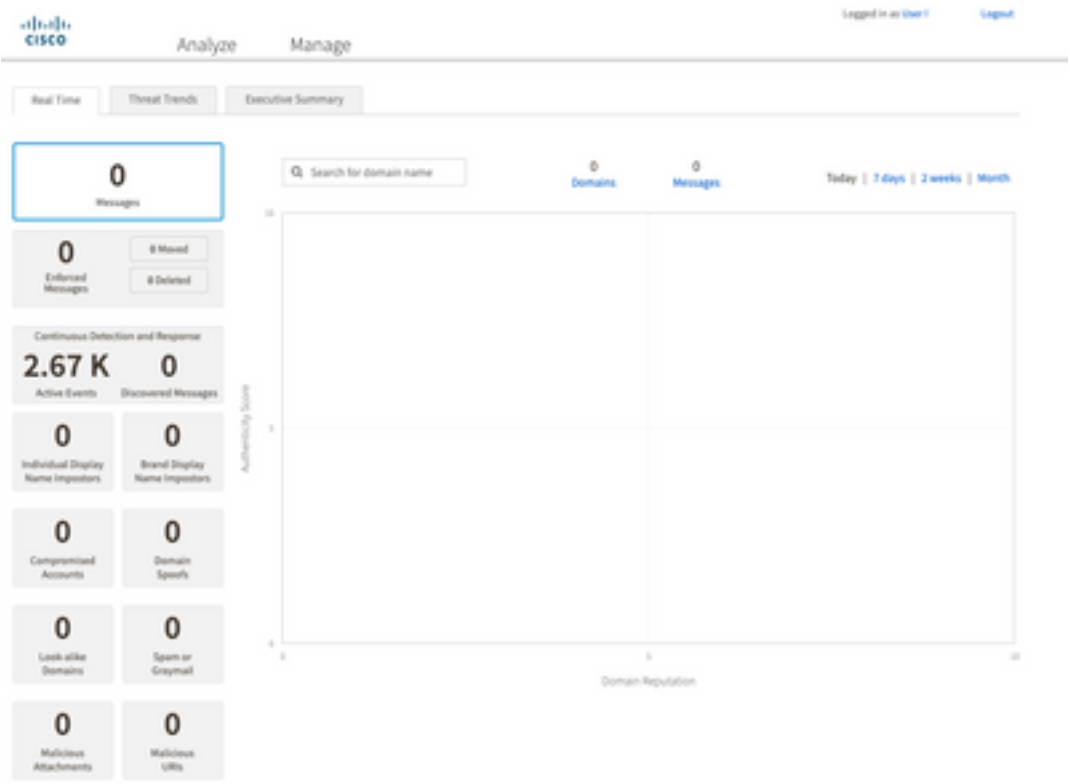


2. 계정이 활성화되면 이미지에 표시된 대로 이메일 주소를 입력한 다음 로그인을 위해 OKTA 로그인 웹 사이트로 리디렉션합니다.





3. OKTA 로그인 프로세스가 완료되면 그림과 같이 Cisco Advanced Phishing Protection 포털에 로그인합니다.



관련 정보

Cisco Advanced Phishing Protection - 제품 정보

Cisco Advanced Phishing Protection - 최종 사용자 가이드

OKTA 지원

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.