

CRES에 대한 OKTA SSO 외부 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[배경 정보](#)

[요구 사항](#)

[구성](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Secure Email Encryption Service(Registered Envelope)에 로그인하기 위해 OKTA SSO 외부 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

Cisco Secure Email Encryption Service(Registered Envelope)에 대한 관리자 액세스

OKTA에 대한 관리자 액세스.

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

배경 정보

- Cisco Secure Email Encryption Service(Registered Envelope)는 SAML을 사용하는 최종 사용자를 위해 SSO 로그인을 활성화합니다.
- OKTA는 애플리케이션에 인증 및 권한 부여 서비스를 제공하는 ID 관리자입니다.
- Cisco Secure Email Encryption Service(Registered Envelope)는 인증 및 권한 부여를 위해 OKTA에 연결된 애플리케이션으로 설정할 수 있습니다.
- SAML은 XML 기반의 개방형 표준 데이터 형식으로, 관리자가 정의된 애플리케이션 중 하나에 로그인한 후 해당 애플리케이션에 원활하게 액세스할 수 있습니다.
- SAML에 대한 자세한 내용은 SAML [일반](#) 정보를 [참조하십시오](#).

요구 사항

- Cisco Secure Email Encryption Service(Registered Envelope) 관리자 계정
- OKTA 관리자 계정.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 장치는 초기화된(기본) 구성으로 시작되었습니다. 네트워크가 활성 상태인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

옥타 밑에.

1. 애플리케이션 포털로 이동하여 Create App Integration, 이미지에 표시된 대로

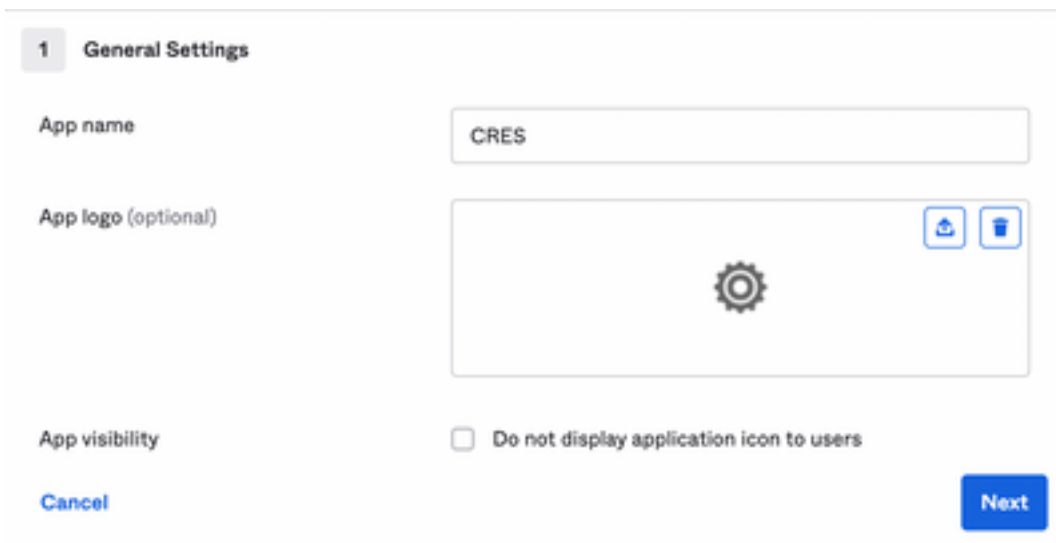
Applications



2. 선택 SAML 2.0 애플리케이션 유형으로, 그림과 같이,



3. 앱 이름을 입력합니다 CRES 및 선택 Next, 이미지에 표시된 대로



4. 아래 SAML settings에서 그림과 같이 간격을 채웁니다.

- SSO(Single Sign On) URL: Cisco Secure Email Encryption Service에서 얻은 Assertion Consumer Service입니다.

- 대상 그룹 URI(SP Entity ID): Cisco Secure Email Encryption Service에서 얻은 그룹 ID입니다.
- 이름 ID 형식: 지정되지 않은 상태로 유지합니다.
- 애플리케이션 사용자 이름: Email - 인증 프로세스에서 사용자에게 이메일 주소를 입력하라는 메시지를 표시합니다.
- 애플리케이션 사용자 이름 업데이트 켜기: Create and Update.

A SAML Settings

General

Single sign on URL ⓘ
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ
If no value is set, a blank RelayState is sent

Name ID format ⓘ

Application username ⓘ

Update application username on

[Show Advanced Settings](#)

아래로 스크롤하여 Group Attribute Statements (optional), 이미지에 표시된 대로 다음 특성 명령문을 입력합니다.

- 이름: group
- 이름 형식: Unspecified
- 필터: Equals 및 OKTA

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
group	Unspecified	Equals OKTA

선택 Next .

5. 요청 시 Help Okta to understand how you configured this application, 이미지에 표시된 대로 현재 환경에 적용

할 수 있는 이유를 입력하십시오.

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

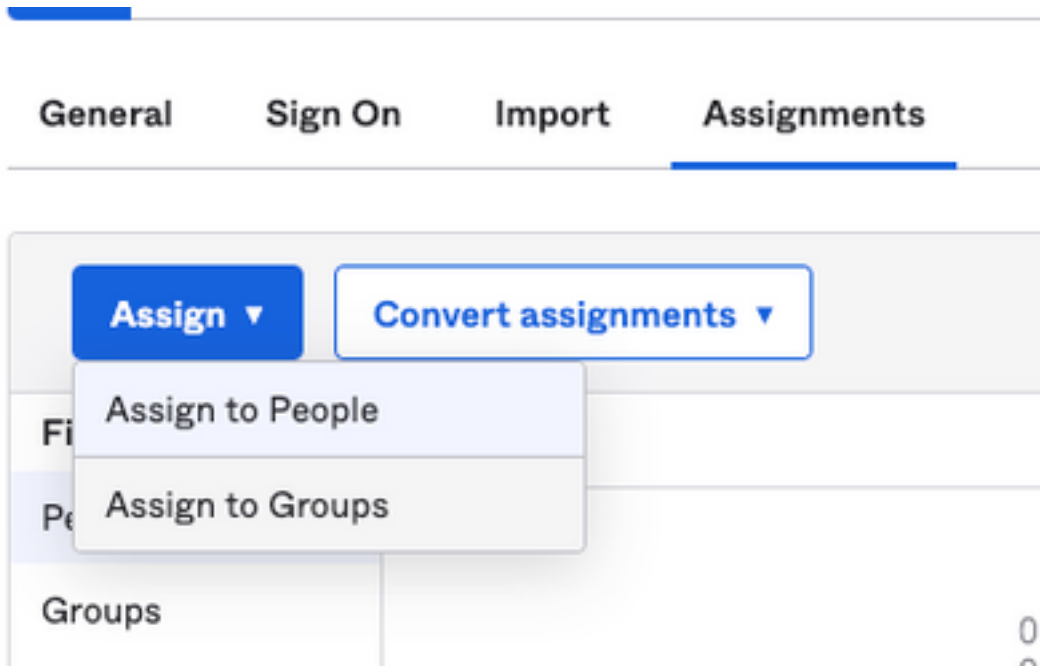
I'm a software vendor. I'd like to integrate my app with Okta

Once you have a working SAML integration, submit it for Okta review to publish in the OIN. [Submit your app for review](#)

[Previous](#) [Finish](#)

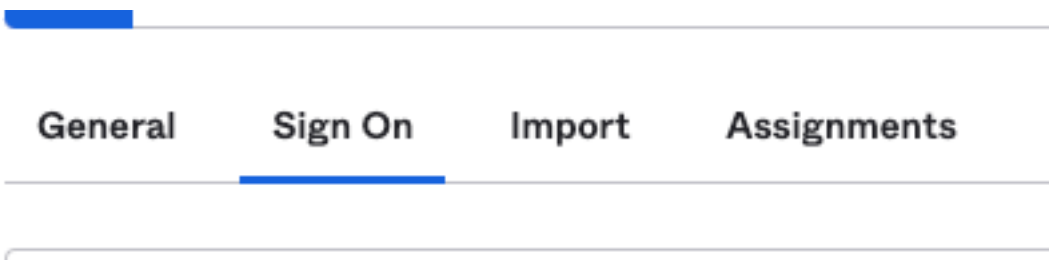
선택 Finish 을 눌러 다음 단계로 진행합니다.

6. 선택 Assignments 탭을 클릭한 다음 Assign > Assign to Groups, 이미지에 표시된 대로



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

8. 선택 Sign On, 이미지에 표시된 대로



9. 아래로 스크롤하여 오른쪽 코너로 이동한 다음 View SAML setup instructions 옵션(그림에 나와 있음):

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

10. 다음 정보를 메모장에 저장합니다. Cisco Secure Email Encryption Service 이미지에 표시된 포털:

- ID 공급자 Single Sign-On URL
- ID 공급자 발급자
- X.509 인증서

The following is needed to configure CRES

1 Identity Provider Single Sign-On URL:

https://

2 Identity Provider Issuer:

http://www.okta.com/

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----


-----END CERTIFICATE-----

[Download certificate](#)

11. OKTA 컨피그레이션을 완료하면 Cisco Secure Email Encryption Service로 돌아갈 수 있습니다

Cisco Secure Email Encryption Service(Registered Envelope) 아래에 있는:

1. 조직 포털에 관리자로 로그인합니다. 링크는 CRES [Administration Portal](#)로, 그림에 나와 있습니다.



Administration Console Log In

Welcome, please log in:

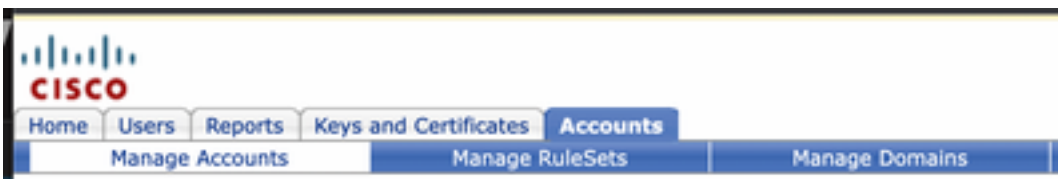
Username

Password

Remember me on this computer.

[Forgot password?](#)

2. Accounts 탭에서 Manage Accounts 탭, 이미지에 표시된 대로



3. 계정 번호를 클릭하고 Details 탭, 이미지에 표시된 대로



4. 아래로 스크롤하여 Authentication Method 및 선택 SAML 2.0, 이미지에 표시된 대로

Authentication Method

5. SSO Alternate Email Attribute을 누르고 다음 그림과 같이 비워 둡니다.

SSO Alternate Email Attribute Name

6. SSO Service Provider Entity ID*, 입력 사항 <https://res.cisco.com/> , 이미지에 표시된 대로

SSO Service Provider
Entity ID*

7. SSO Customer Service URL*, 을 입력합니다. Identity Provider Single Sign-On URL 이미지에 표시된 대로 Okta에서 제공합니다.

SSO Customer Service
URL*

8. 의 경우 SSO Logout URL 을 누르고 다음 그림과 같이 비워 둡니다.

SSO Logout URL

9. SSO Identity Provider Verification Certificate, OKTA에서 제공한 X.509 인증서를 업로드합니다.

10. 선택 **save** 이미지에 표시된 대로 설정을 저장하려면 다음을 수행합니다.

Save

Back to Accounts List

11. 선택 **Activate SAML** 이미지에 표시된 대로 SAML 인증 프로세스를 시작하고 SSO 인증을 적용하려면

**Activate
SAML**

Save

**Back to
Accounts List**

12. SAML ID 제공자와의 인증에 성공한 후 SAML 인증이 활성화됨을 알리는 새 창이 열립니다. 선택 **Continue**, 이미지에 표시된 대로

SAML authentication will be active after a successful authentication with the SAML Identity Provider.
Please click continue to authenticate.

Continue

13. OKTA 자격 증명으로 인증할 수 있는 새 창이 열립니다. 다음을 입력합니다. Username 및 선택 **Next**, 이미지에 표시된 대로



Sign In

Username

Keep me signed in

Next

Help

14. 인증 프로세스가 성공하면 SAML Authentication Successful 이 표시됩니다. 선택 Continue 이미지에 표시된 대로 이 창을 닫으려면 다음을 수행합니다.

SAML Authentication Successful.

Please click continue to close.

Continue

15. SSO Enable Date 은 이미지에 표시된 대로 SAML 인증이 성공한 날짜 및 시간으로 설정됩니다.

Authentication Method	SAML 2.0 ▾
SSO Enable Date	10/18/2022 15:21:07 CDT
SSO Email Name ID Format	transient
SSO Alternate Email Attribute Name	<input type="text"/>
SSO Service Provider Entity ID*	<input type="text" value="https://res.cisco.com/"/>
SSO Customer Service URL*	<input type="text" value="https://"/> <input type="text" value="t.okta.com/app/"/>
SSO Logout URL	<input type="text"/>
SSO Service Provider Verification Certificate	Download
SSO Binding	HTTP-Redirect, HTTP-POST
SSO Assertion Consumer URL	https://res.cisco.com/websafe/ssourl
Current Certificate	

SAML 컨피그레이션이 완료되었습니다. 현재 CRES 조직에 속한 사용자는 이메일 주소를 입력할 때 OKTA 자격 증명을 사용하도록 리디렉션됩니다.

다음을 확인합니다.


1. [Secure Email Encryption Service Portal로 이동합니다.](#) 그림과 같이 CRES에 등록된 이메일 주소를 입력합니다.

Secure Email Encryption Service

Username*

Log In

OR

 Sign in with Google

2. 새 창이 열리고 그림과 같이 OKTA 자격 증명으로 OKTA 인증 로그인을 진행합니다.



Sign In

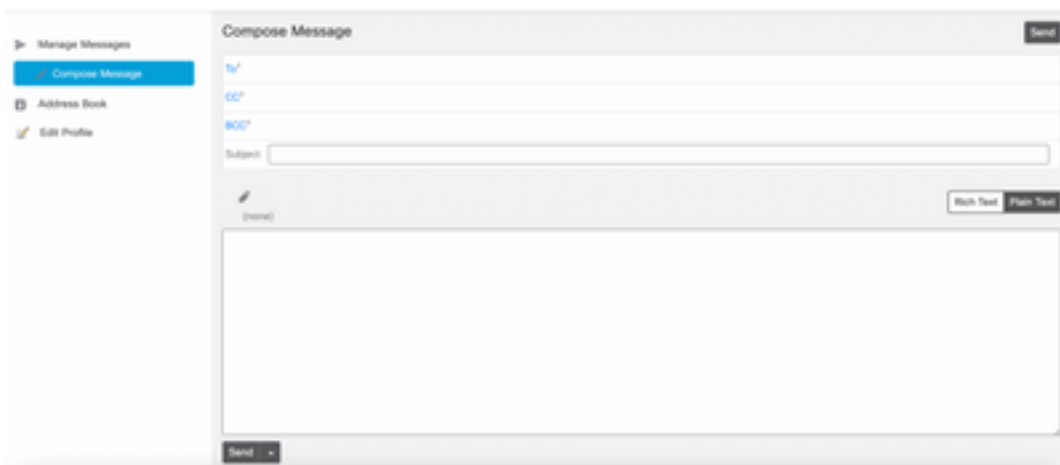
Username

Keep me signed in

Next

Help

3. 인증에 성공하면 Secure Email Encryption Service가 Compose Message 창(그림에 나와 있음):



이제 최종 사용자는 Secure Email Encryption Service 포털에 액세스하여 보안 이메일을 작성하거나 OKTA 자격 증명으로 새 봉투를 열 수 있습니다.

관련 정보

[Cisco Secure Email Encryption Service 6.2 계정 관리자 설명서](#)

[Cisco Secure Gateway 최종 사용자 가이드](#)

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.