

최종 사용자 스팸 격리에 대한 OKTA SSO 구성

목차

[소개](#)

[사전 요구 사항](#)

[배경 정보](#)

[구성 요소](#)

[구성](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 Security Management Appliance의 최종 사용자 스팸 격리에 로그인하기 위해 OKTA SSO를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- Cisco Security Management Appliance에 대한 관리자 액세스.
- OKTA에 대한 관리자 액세스.
- PKCS #12 또는 PEM 형식의 자체 서명 또는 CA 서명(선택 사항) X.509 SSL 인증서(OKTA에 서 제공)

배경 정보

Cisco Security Management Appliance는 최종 사용자 스팸 격리를 사용하는 최종 사용자를 위해 SSO 로그인을 활성화하고 애플리케이션에 인증 및 권한 부여 서비스를 제공하는 ID 관리자인 OKTA와 통합합니다. Cisco End User Spam Quarantine은 인증 및 권한 부여를 위해 OKTA에 연결되는 애플리케이션으로 설정할 수 있으며, 관리자가 정의된 애플리케이션에 로그인한 후 해당 애플리케이션에 원활하게 액세스할 수 있도록 하는 XML 기반 개방형 표준 데이터 형식인 SAML을 사용합니다.

SAML에 대한 자세한 내용은 SAML [일반](#) 정보를 [참조하십시오](#).

구성 요소

- Cisco Security Management Appliance 클라우드 관리자 어카운트
- 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

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

2. 선택 SAML 2.0 애플리케이션 유형으로, 그림과 같이,

Create a new app integration ✕

Sign-in method

[Learn More](#)

OIDC - OpenID Connect

Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

SAML 2.0

XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

SWA - Secure Web Authentication

Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

API Services

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

3. 앱 이름을 입력합니다 SMA EUQ 선택 Next, 이미지에 표시된 대로

1 General Settings

App name

SMA EUQ

App logo (optional)



App visibility

Do not display application icon to users

Cancel

Next

4. 아래 SAML settings에서 그림과 같이 간격을 채웁니다.

- SSO(Single Sign On) URL: SMA EUQ 인터페이스에서 얻은 Assertion 소비자 서비스입니다.

- 대상 그룹 URI(SP 엔티티 ID): SMA EUQ 엔티티 ID에서 가져온 엔티티 ID입니다.


- 이름 ID 형식: 지정되지 않은 상태로 유지합니다.


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


- 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 
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 적용할 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

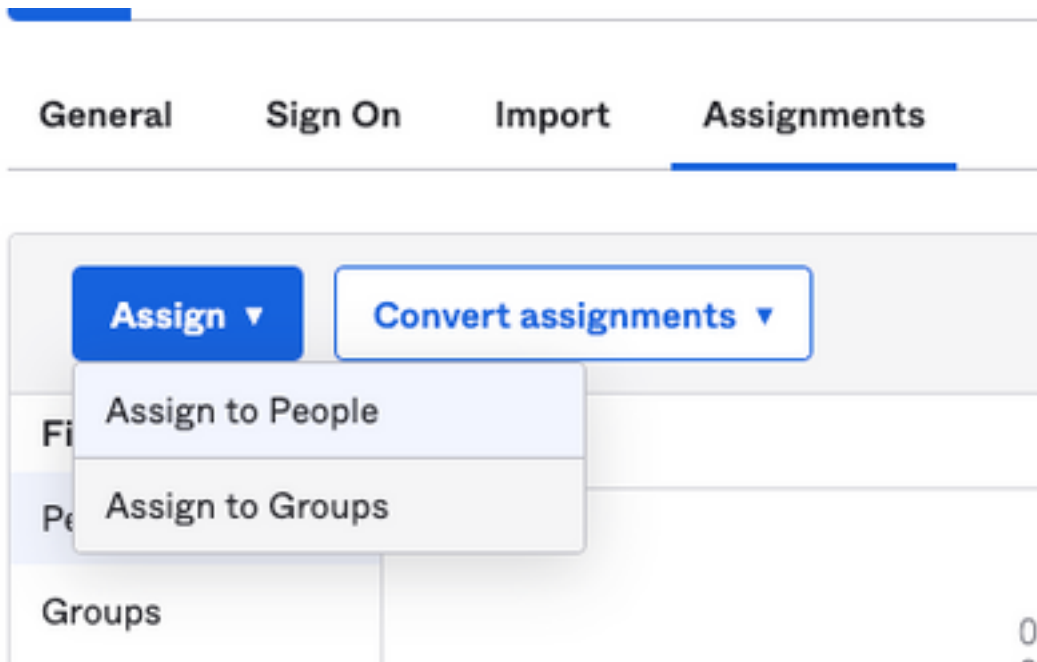
I'm a software vendor. I'd like to integrate my app with Okta

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

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

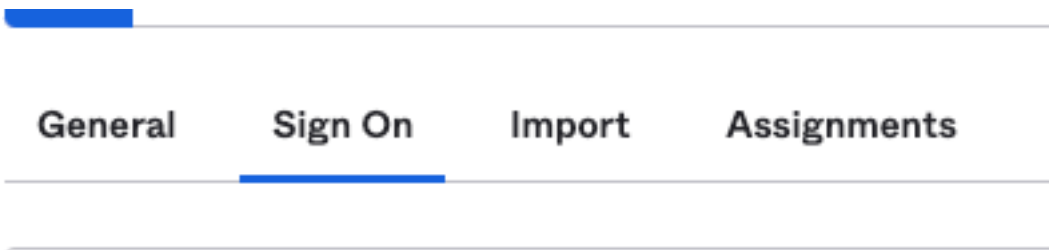
선택 Finish 을 눌러 다음 단계로 진행합니다.

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. 이 정보를 메모장에 저장합니다. Cisco Security Management Appliance 이미지에 표시된 대로 SAML 컨피그레이션:

- 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-----

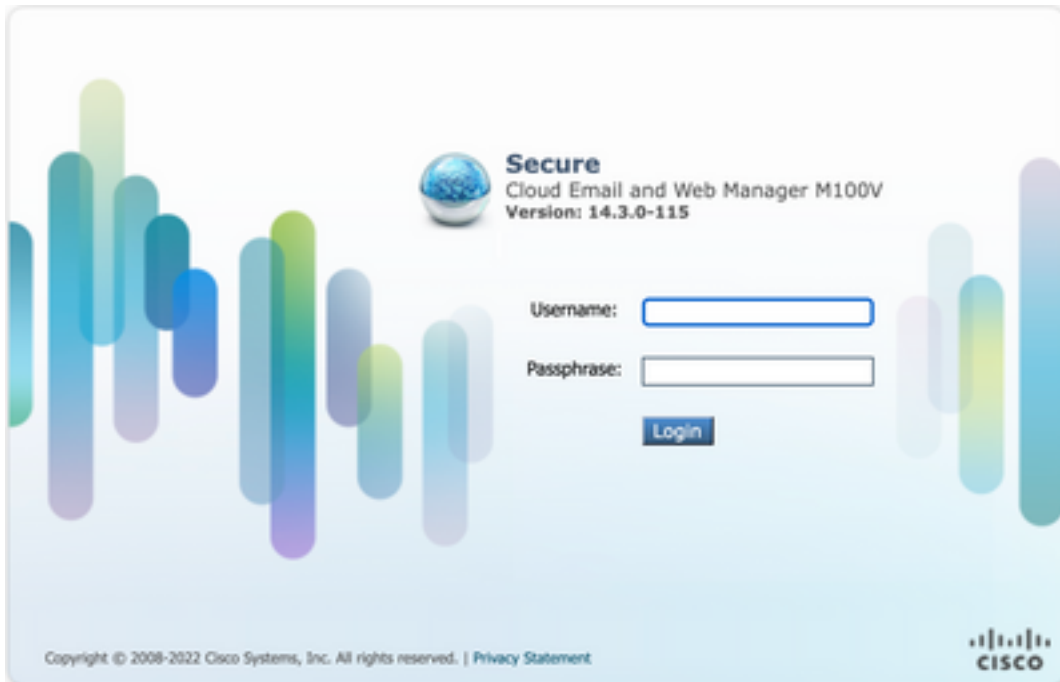
-----END CERTIFICATE-----

[Download certificate](#)

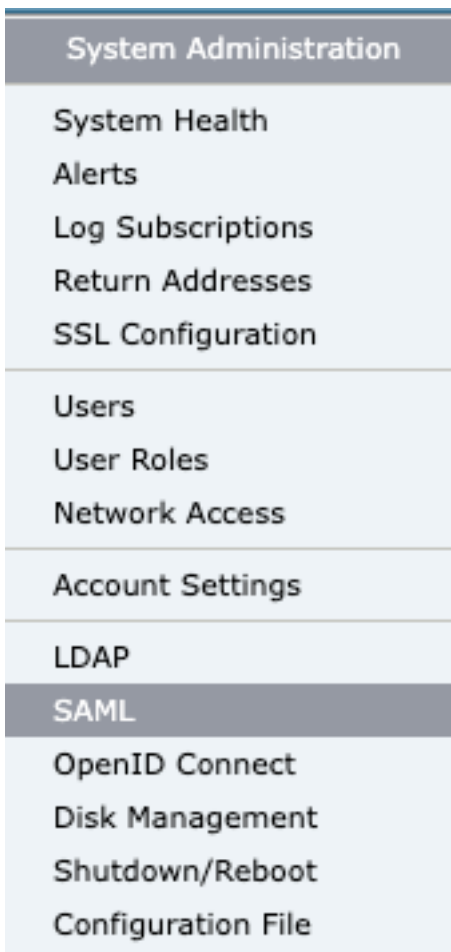
11. OKTA 컨피그레이션을 완료하면 Cisco Security Management Appliance로 돌아갈 수 있습니다.

Cisco Security Management Appliance에서

1. 그림과 같이 Cisco Security Management Appliance에 클라우드 관리자로 로그인합니다.



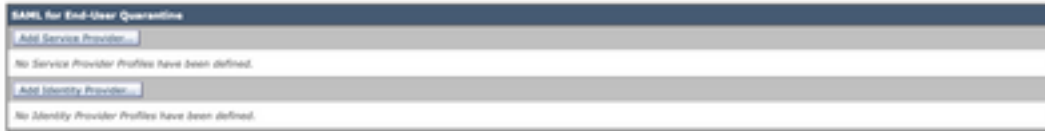
2. System Administration 탭에서 SAML 옵션(그림에 나와 있음):



3. SAML을 구성할 수 있는 새 창이 열립니다. 아래 SAML for End-User Quarantine, 클릭 Add Service Provider ,

이미지에 표시된 대로

SAML



4. 아래 Profile Name 그림과 같이 서비스 공급자 프로파일의 프로파일 이름을 입력합니다.

Profile Name:

5. Entity ID 에서 서비스 공급자(이 경우 어플라이언스)의 전역적으로 고유한 이름을 입력합니다. 서비스 공급자 엔티티 ID의 형식은 일반적으로 URI이며, 그림에 나와 있습니다.

Entity ID:

6. 대상 Name ID Format 이 필드는 구성할 수 없습니다. 이미지에 표시된 대로 ID 제공자를 구성할 때 이 값이 필요합니다.

Name ID Format:

7. 용 Assertion Consumer URL인증이 성공적으로 완료된 후 ID 제공자가 SAML 어설션을 전송하는 URL을 입력합니다. 이 경우 스팸 격리의 URL입니다.

Assertion Consumer URL:

8. SP Certificate , 인증서 및 키를 업로드하거나 PKCS #12 파일을 업로드합니다. 업로드된 후에는 Uploaded Certificate Details 다음과 같이 표시됩니다.

Uploaded Certificate Details:

Issuer: (:1-
{ \O=Cisco\ST=CDMX\OU=ESA TAC

Subject: (:1-
{ \O=Cisco\ST=CDMX\OU=ESA TAC

Expiry Date: ! GMT

9. 대상 Sign Requests and Sign Assertions SAML 요청 및 어설션에 서명하려면 두 확인란을 모두 선택합니다. 이러한 옵션 확인을 선택하는 경우 이미지에 표시된 대로 OKTA에서 동일한 설정을 구성해야 합니다.

- Sign Requests
- Sign Assertions

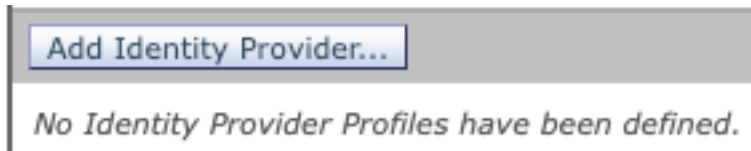
Make sure that you configure the same settings on your Identity Provider as well.

10. **용** Organization Details, 이미지에 표시된 대로 조직의 세부 정보를 입력합니다.

Organization Details:	Name:	<input type="text" value="EUQ SAML APP"/>
	Display Name:	<input type="text" value="https://-euq1.iphmx.com/"/>
	URL:	<input type="text" value="https://-euq1.iphmx.com/"/>
Technical Contact:	Email:	<input type="text" value="useradmin@domainhere.com"/>

11. Submit 및 Commit 구성을 진행하기 전에 변경 사항 Identity Provider Settings .

12. 아래 SAML , 클릭 Add Identity Provider, 이미지에 표시된 대로



13. 아래 Profile Name: 이미지에 표시된 대로 ID 제공자 프로파일의 이름을 입력합니다.

Profile Name:	<input type="text" value="iDP Profile"/>
---------------	--

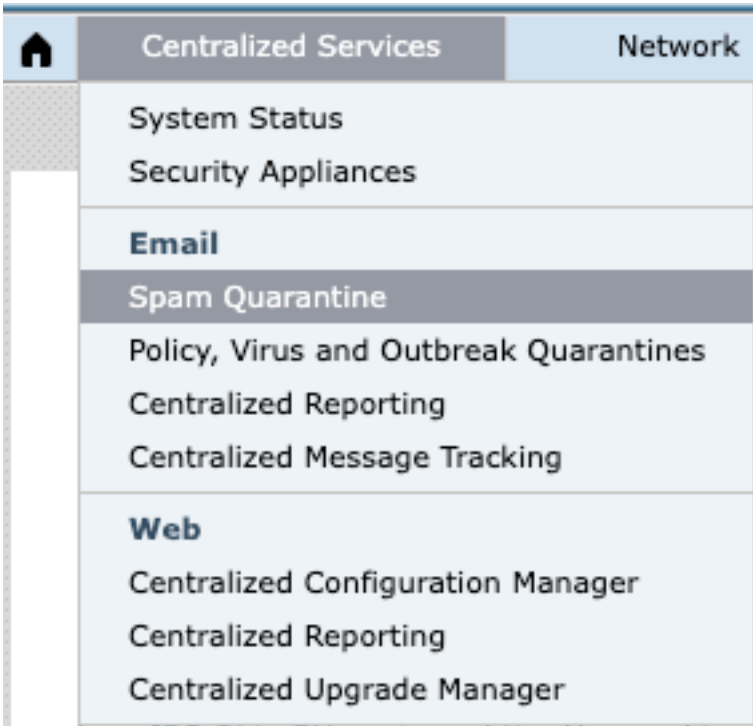
14. 선택 Configure Keys Manually 이미지에 표시된 대로 다음 정보를 입력합니다.

- 엔티티 ID: ID 제공자 엔티티 ID는 ID 제공자를 고유하게 식별하는 데 사용됩니다. 이전 단계의 OKTA 설정에서 가져옵니다.
- SSO URL: SP에서 SAML 인증 요청을 보내야 하는 URL입니다. 이전 단계의 OKTA 설정에서 가져옵니다.
- Certificate(인증서): OKTA에서 제공하는 인증서입니다.

The image shows the "Configure Keys Manually" configuration settings form. The "Entity ID" field contains "http://www.okta.com". The "SSO URL" field contains "https://67465". The "Certificate" field has a "Seleccionar archivo" button and the text "Sin archivos seleccionados". Below the certificate field, there are fields for "Uploaded Certificate Details": "Issuer:", "Subject:", and "Expiry Date:".

15. Submit 및 Commit saml 로그인 활성화로 진행하기 위한 변경 사항.

16. 아래 Centralized Services > Email , 클릭 Spam Quarantine, 이미지에 표시된 대로



17. 아래 Spam Quarantine -> Spam Quarantine Settings , 클릭 Edit Settings , as shown in the image:



18. 아래로 스크롤하여 End-User Quarantine Access > End-User Authentication , 선택 SAML 2.0 , 이미지에 표시된 대로



19 . Submit 및 Commit 에 대한 SAML 인증을 활성화하기 위한 변경 사항 End User Spam Quarantine .

다음을 확인합니다.

1. 이미지에 표시된 대로 웹 브라우저에서 회사의 최종 사용자 스팸 쿼런틴 URL을 입력합니다.



2. OKTA 인증을 진행하기 위한 새 창이 열립니다. 그림과 같이 OKTA 자격 증명으로 로그인합니다.



Sign In

Username

Keep me signed in

Next

Help

3. 인증에 성공하면 End User Spam Quarantine 이미지에 표시된 대로 로그인한 사용자의 스팸 쿼런틴 내용을 엽니다.



이제 최종 사용자는 OKTA 자격 증명으로 최종 사용자 스팸 격리에 액세스할 수 있습니다. .

관련 정보

[Cisco Secure Email and Web Manager 최종 사용자 설명서](#)

[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.