

OKTA SSO configureren voor eindgebruiker spamquarantaine

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Achtergrondinformatie](#)

[Componenten](#)

[Configureren](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u OKTA SSO kunt configureren voor inloggen op de eindgebruiker in de spamquarantaine van de security applicatie.

Voorwaarden

- Beheerderstoegang tot Cisco Security Management-applicatie.
- Beheerder toegang tot OKTA.
- Zelfondertekende of CA-ondertekende (facultatieve) X.509 SSL-certificaten in PKCS #12- of PEM-formaat (geleverd door OKTA).

Achtergrondinformatie

Cisco Security Management-applicatie maakt SSO-aanmelding mogelijk voor eindgebruikers die de eindgebruiker spamquarantaine gebruiken en integreren met OKTA, een identiteitsbeheerder die verificatie- en autorisatieservices voor uw toepassingen biedt. De Cisco End User Spamquarantaine kan worden ingesteld als een toepassing die is aangesloten op OKTA voor verificatie en autorisatie en gebruikt SAML, een op XML gebaseerde open standaard dataformaat dat beheerders in staat stelt om naadloos toegang te krijgen tot een gedefinieerde set toepassingen na het teken in een van die toepassingen.

Voor meer informatie over SAML, raadpleegt u: [SAML General Information](#)

Componenten

- Cisco Security Management-applicatie cloudbehoudersaccount.
- OKTA-behoudersaccount.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een ontruimde (standaard) configuratie. Als het netwerk actief is, zorg er dan voor dat u de potentiële impact van een opdracht begrijpt.

Configureren

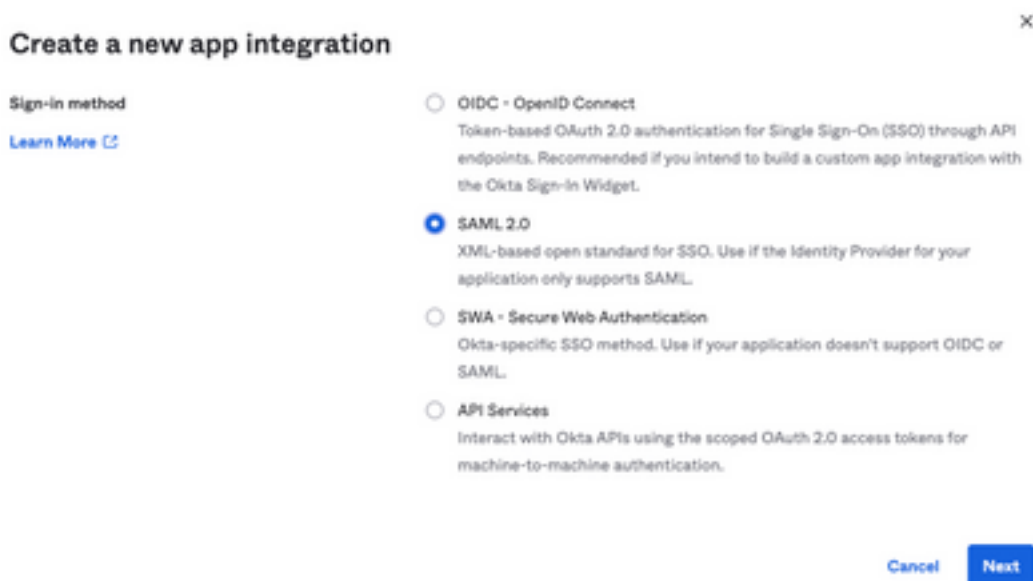
Onder Okta.

1. Navigeer naar het portaal Toepassingen en kies **Create App Integration**, zoals aangegeven op de afbeelding:

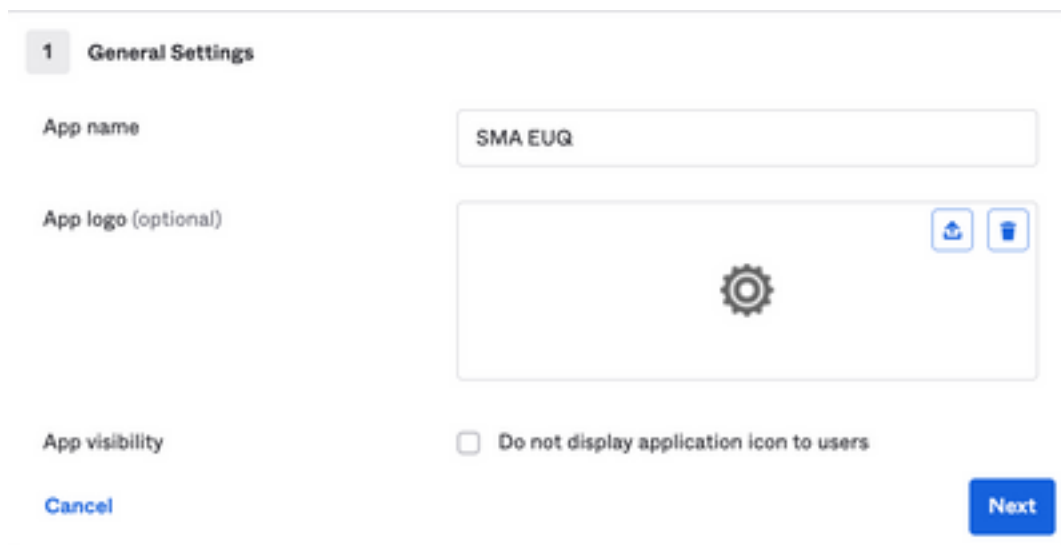
Applications



2. Kies **SAML 2.0** als het toepassingstype, zoals in de afbeelding:



3. Voer de naam van de app in **SMA EUQ** en kiezen **Next**, zoals aangegeven op de afbeelding:



4. Volgens de SAML settings Vul de gaten in, zoals in de afbeelding:


- Single sign on URL: Dit is de Assertion Consumer Service verkregen van de SMA EUQ-


interface.


- Audience URI (SP Entity ID): Dit is de Entity ID verkregen van de SMA EUQ Entity ID.
- Naam ID formaat: Bewaar het als Niet gespecificeerd.
- Toepassingsgebruikersnaam: E-mail die de gebruiker vraagt om zijn e-mailadres in te voeren in het verificatieproces.
- Gebruikersnaam voor toepassing bijwerken op: Aanmaken en bijwerken.


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](#)

Scroll naar beneden Group Attribute Statements (optional) , zoals aangegeven op de afbeelding:

Voer de volgende attribuutverklaring in:

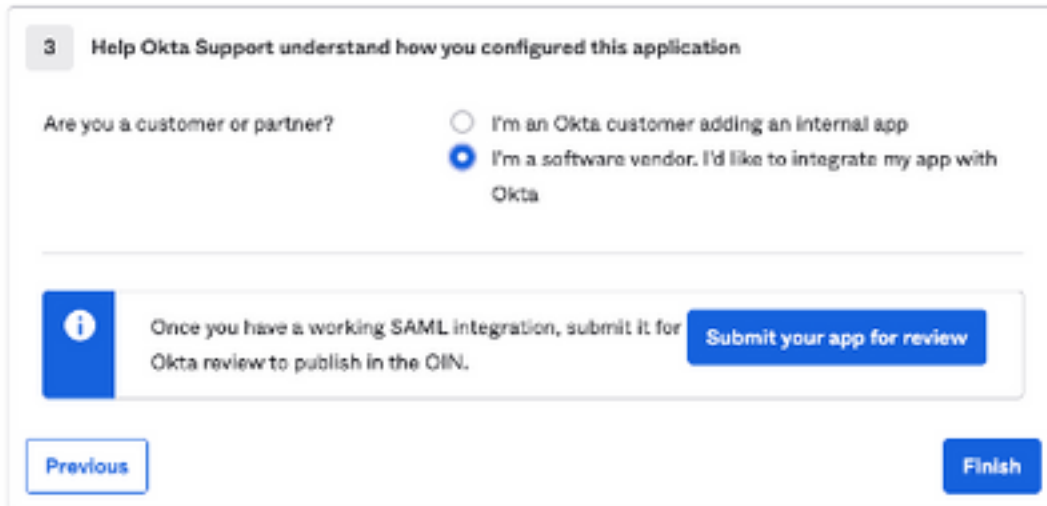
- Name: group
- Naamformaat: Unspecified
- filteren: Equals en OKTA

Group Attribute Statements (optional)

| Name | Name format (optional) | Filter |
|------------------------------------|--|---|
| <input type="text" value="group"/> | <input type="text" value="Unspecified"/> | <input type="text" value="Equals"/> <input type="text" value="OKTA"/> |

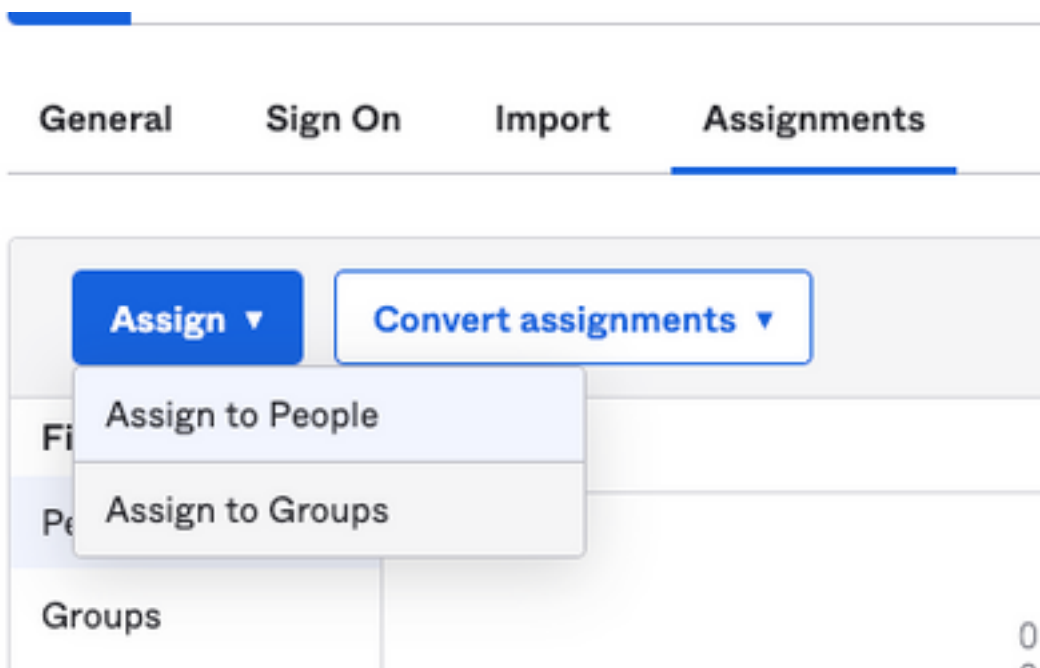
Kiezen Next .

5. Wanneer Help Okta to understand how you configured this application Geef ook de reden op die van toepassing is op de huidige omgeving, zoals aangegeven op de afbeelding:



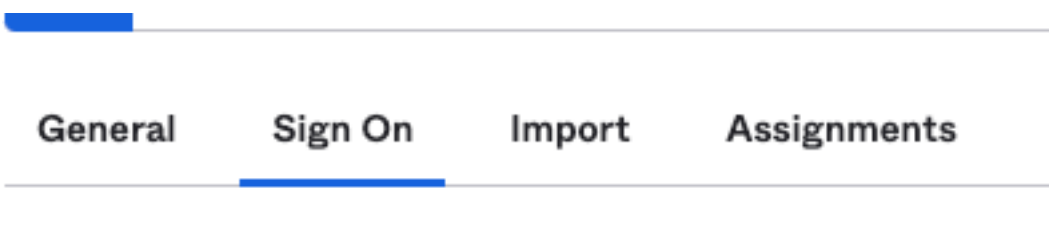
Kiezen Finish om verder te gaan naar de volgende stap.

6. Kies Assignments tabblad en selecteer vervolgens Assign > Assign to Groups, zoals aangegeven op de afbeelding:



7. Kies de OKTA-groep, de groep met de geautoriseerde gebruikers voor toegang tot de omgeving

8. Kies Sign On , zoals aangegeven op de afbeelding:



9. Blader naar beneden en kies de gewenste hoek View SAML setup instructions optie, zoals in de

afbeelding:

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. Sla deze informatie op in een kladblok. U moet deze in de Cisco Security Management Appliance SAML Configuration, zoals in het beeld:

- Identity Provider Single Sign-On URL
- uitgever van identiteitsbewijzen
- X.509-certificaat

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](#)

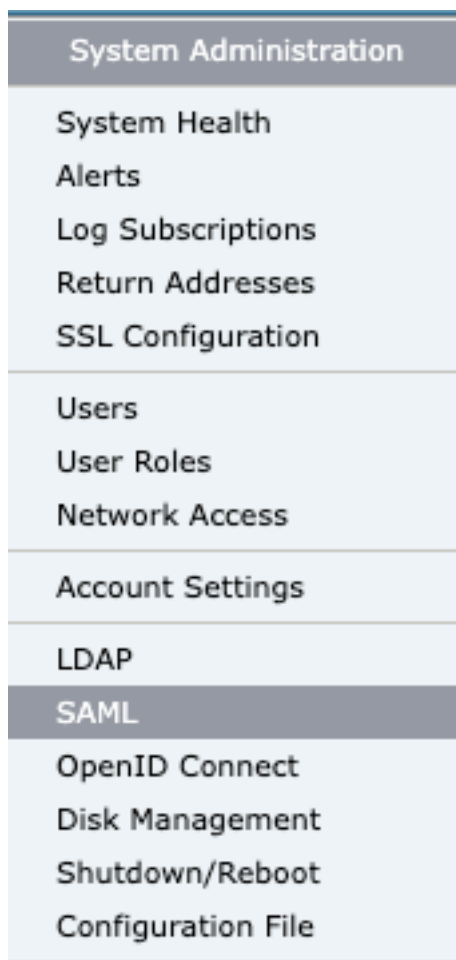
1. Zodra u de OKTA-configuratie hebt voltooid, kunt u terugkeren naar de Cisco Security Management-applicatie.

Onder Cisco Security Management-applicatie:

1. Log in op de Cisco Security Management-applicatie als cloudbeheerder, zoals in de afbeelding:



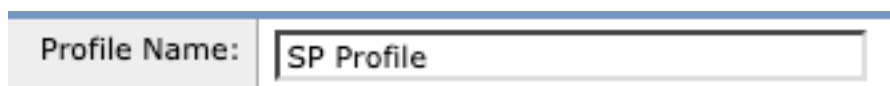
2. Op de System Administrationtabblad kiest u de SAML optie, zoals in de afbeelding:



3. Er wordt een nieuw venster geopend voor het configureren van SAML. Onder SAML for End-User Quarantine, klikken Add Service Provider , zoals aangegeven op de afbeelding:



4. Onder Profile Name Voer een profielnaam in voor het serviceproviderprofiel zoals in de afbeelding:



5. Voor Entity ID , voer een wereldwijd unieke naam voor de serviceprovider in (in dit geval uw apparaat). Het formaat van de dienstverlener Entity ID is doorgaans een URI, zoals in de afbeelding wordt getoond:




6. Voor Name ID Format , dit veld kan niet worden geconfigureerd. U hebt deze waarde nodig bij het configureren van de identiteitsprovider, zoals weergegeven in het afbeelding:

Name ID Format: 

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

7. Voor **Assertion Consumer URL**, voer de URL in waarnaar de identiteitsprovider de SAML-bewering verstuurt nadat de verificatie met succes is voltooid. In dit geval, is dit de URL naar uw spam quarantaine.

Assertion
Consumer URL: 

https://, 2-euq1.iphmx.com/

8. Voor **SP Certificate**, het certificaat en de sleutel te uploaden of het PKCS-#12 te uploaden. Nadat het is geüpload, klikt u op **Uploaded Certificate Details** displays, zoals weergegeven in het beeld:

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. Voor **Sign Requests and Sign Assertions** Vink beide aanvinkvakjes aan als u de SAML-verzoeken en -opmerkingen wilt ondertekenen. Als u deze opties selecteert, moet u ervoor zorgen dat u dezelfde instellingen op OKTA configureert, zoals in de afbeelding:

Sign Requests

Sign Assertions

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

10. Voor **Organization Details**, voer de gegevens van uw organisatie in, zoals te zien is op de afbeelding:

Organization
Details:

Name: EUQ SAML APP

Display Name: https:// -euq1.iphmx.com/

URL: https://, -euq1.iphmx.com/

Technical Contact:

Email: useradmin@domainhere.com

11. **Submit** en **Commit** wijzigingen voordat u verder gaat met configureren **Identity Provider Settings**.

12. Onder **SAML** klikt u op **Add Identity Provider**, zoals aangegeven op de afbeelding:

Add Identity Provider...

No Identity Provider Profiles have been defined.

13. Onder Profile Name: Voer een naam in voor het profiel van de identiteitsprovider, zoals getoond in de afbeelding:

Profile Name: iDP Profile

14. Selecteer Configure Keys Manually en Voer deze informatie in, zoals in de afbeelding:

- Identity ID: de Identity Provider Entity ID wordt gebruikt om de Identity Provider uniek te identificeren. Het wordt verkregen uit de instellingen van de OKTA in de voorgaande stappen.
- SSO URL: De URL waarnaar SP moet sturen SAML Auth aanvragen. Het wordt verkregen uit de instellingen van de OKTA in de voorgaande stappen.
- Certificaat: het certificaat dat wordt verstrekt door OKTA.

Configuration Settings: Configure Keys Manually

Entity ID:

SSO URL:

Certificate: Sin archivos seleccionados

Uploaded Certificate Details:

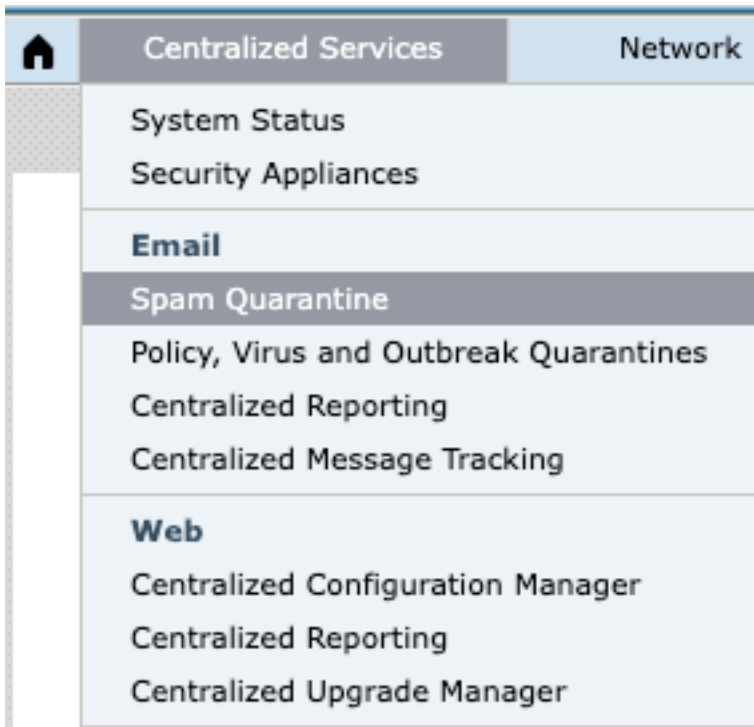
Issuer:

Subject:

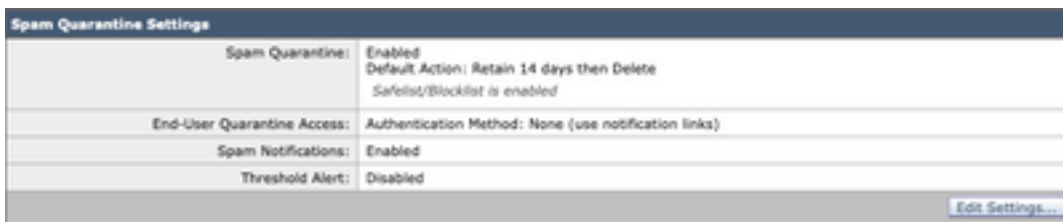
Expiry Date:

15. Submit en Commit de wijzigingen om verder te gaan met de activering van de SAML-aanmelding.

16. Onder Centralized Services > Email , klik op Spam Quarantine, zoals aangegeven op de afbeelding:



17. Onder Spam Quarantine -> Spam Quarantine Settings klikt u op Edit Settings , as shown in the image:



18. Scroll naar beneden End-User Quarantine Access > End-User Authentication , selecteer SAML 2.0 , zoals aangegeven op de afbeelding:



19. Submit en Commit wijzigingen om SAML-verificatie in te schakelen voor End User Spam Quarantine .

Verifiëren

1. Voer in een webbrowser de URL in van de spamquarantaine van de eindgebruiker van uw bedrijf, zoals in de afbeelding:



2. Er wordt een nieuw venster geopend om door te gaan met de OCTA-verificatie. Meld u aan met de **OKTA-referenties**, zoals in de afbeelding:



Sign In

Username

Keep me signed in

Next

Help

3. Als de verificatie succesvol is, gebruikt de End User Spam Quarantine Hiermee opent u de inhoud van de spamquarantaine voor de gebruiker die inlogt, zoals in de afbeelding:



Nu kan de eindgebruiker toegang krijgen tot de eindgebruiker spamquarantaine met OKTA-referenties. .

Gerelateerde informatie

[Cisco Secure Email and Web Manager-eindgebruikershandleidingen](#)

[Ondersteuning van OKTA](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.