Okta SAML SSO configureren voor SMA-eindgebruikersquarantaine

Inhoud

Inleiding

In dit document wordt beschreven hoe Okta kan worden geconfigureerd als de SAML 2.0-identiteitsprovider voor Cisco Secure Email SMA-quarantainetoegang voor eindgebruikers.

Voorwaarden

- Cisco Secure Email Security Management Appliance (SMA)
- Te gedenken gebeurtenis: SAML SSO voor End User Quarantine (EUQ)
- Identiteitsprovider: Okta (SAML 2.0)
- Van toepassing op: SMA-implementaties die EUQ-toegang bieden op virtuele of hardwareplatforms. Voorbeeldhostnamen en -poorten vervangen door waarden uit uw omgeving.
- Versiecontext: Deze procedure is van toepassing op SMA-releases die SAML voor EUQ ondersteunen. Controleer de beschikbare velden en menuopties in de geïnstalleerde versie.

Opmerking: Dit document richt zich op de SMA EUQ SAML-configuratie. ESA wordt alleen gebruikt voor het genereren van certificaten wanneer SMA geen zelf ondertekend certificaat kan genereren.

Vereisten

Voordat u begint, moet u controleren of u:

- Administratieve toegang tot de SMA-webinterface.
- Beheerdersrechten in Okta om SAML 2.0-toepassingen te maken en gebruikers of groepen toe te wijzen.
- Een certificaat en privésleutel voor de configuratie van de SMA-serviceprovider. Een zelf ondertekend certificaat is acceptabel voor testen.
- Een bereikbare SMA EUQ volledig gekwalificeerde domeinnaam (FQDN) en poort die eindgebruikers kunnen openen vanuit hun browsers.
- De waarden SMA SAML Assertion URL en SP Entity ID (van Systeembeheer > SAML nadat u het SP-item hebt gemaakt).
- Gebruikersaccounts in Okta die zijn toegewezen aan de Okta-toepassing.
- Directory-gesynchroniseerde gebruikers, als uw implementatie directory-integratie gebruikt.

Opmerking: Okta is een externe identiteitsprovider. In dit document wordt een voorbeeldconfiguratie weergegeven die door de klant kan worden geraadpleegd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

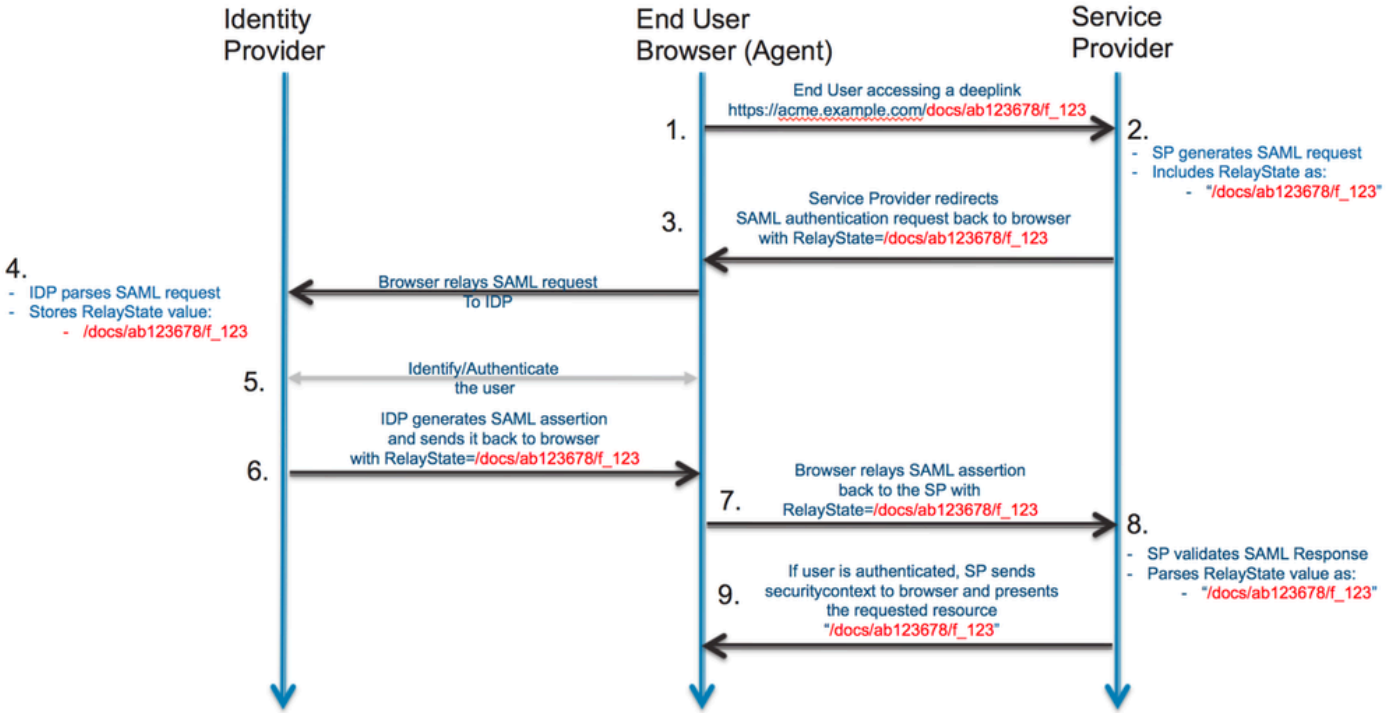
Achtergrondinformatie

Het doel is om single sign-on (SSO) te configureren voor het spam-quarantaineportaal, zodat gebruikers worden doorgestuurd naar Okta om te verifiëren, multifactor-authenticatie (MFA) te voltooien als deze is ingeschakeld in Okta en vervolgens terug te keren naar het SMA EUQ-portaal. Dit document is alleen van toepassing op SMA. Cisco Secure Email Gateway, voorheen Email Security Appliance (ESA), wordt alleen gebruikt voor het genereren van certificaten wanneer SMA geen zelf ondertekend certificaat kan genereren.

Probleem: gebruikers moeten zich authenticeren bij het SMA-spam-quarantaineportaal met Okta met behulp van SAML SSO en optionele MFA.

Oplossing: SMA configureren als serviceprovider, een SAML-toepassing configureren in Okta, de Okta IdP-instellingen importeren in SMA, gebruikers toewijzen in Okta en de toegang verifiëren.

SAML-stroom:



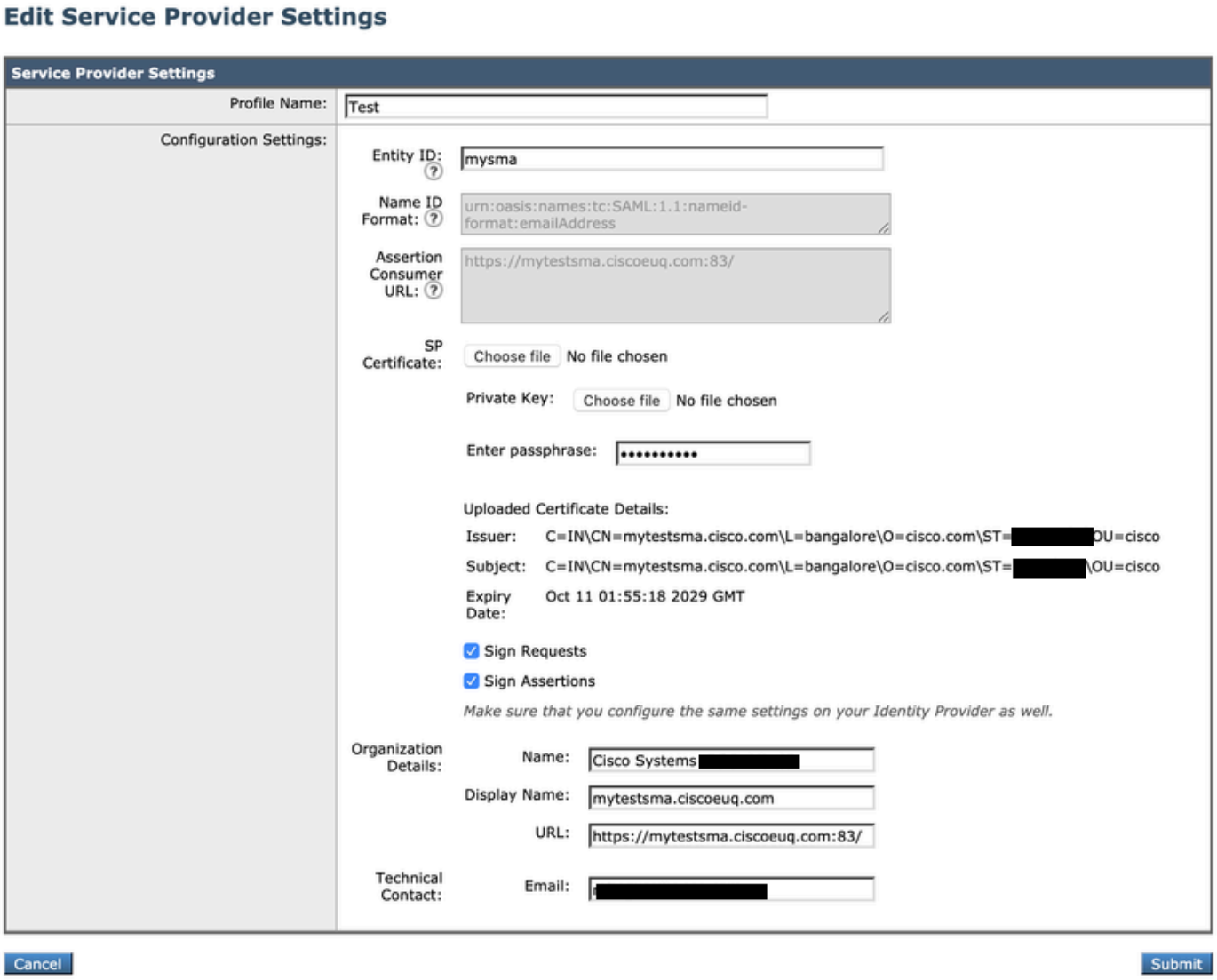
Configuratie

De Serviceverlener (SP) configureren op het SMA-toestel

Voer de volgende stappen uit om de SMA te configureren als een SAML-serviceprovider voor EUQ-toegang:

1. Meld u aan bij de SMA web interface.
2. Navigeer naar Systeembeheer > SAML.
3. Selecteer Serviceprovider toevoegen.
4. Voer in de Entiteit-ID van de Serviceverlener de Entiteit-ID in die u ook in Okta kunt configureren.
5. Controleer of het Name ID Format en de Assertion Consumer Service (ACS)-URL zijn ingevuld voor de EUQ-interface.
6. Upload in SP-certificaat een certificaat om SAML-verzoeken te ondertekenen.

Opmerking: SMA kan geen zelf ondertekend certificaat genereren. U kunt ook een certificaat op een ESA genereren en exporteren voor gebruik op de SMA.



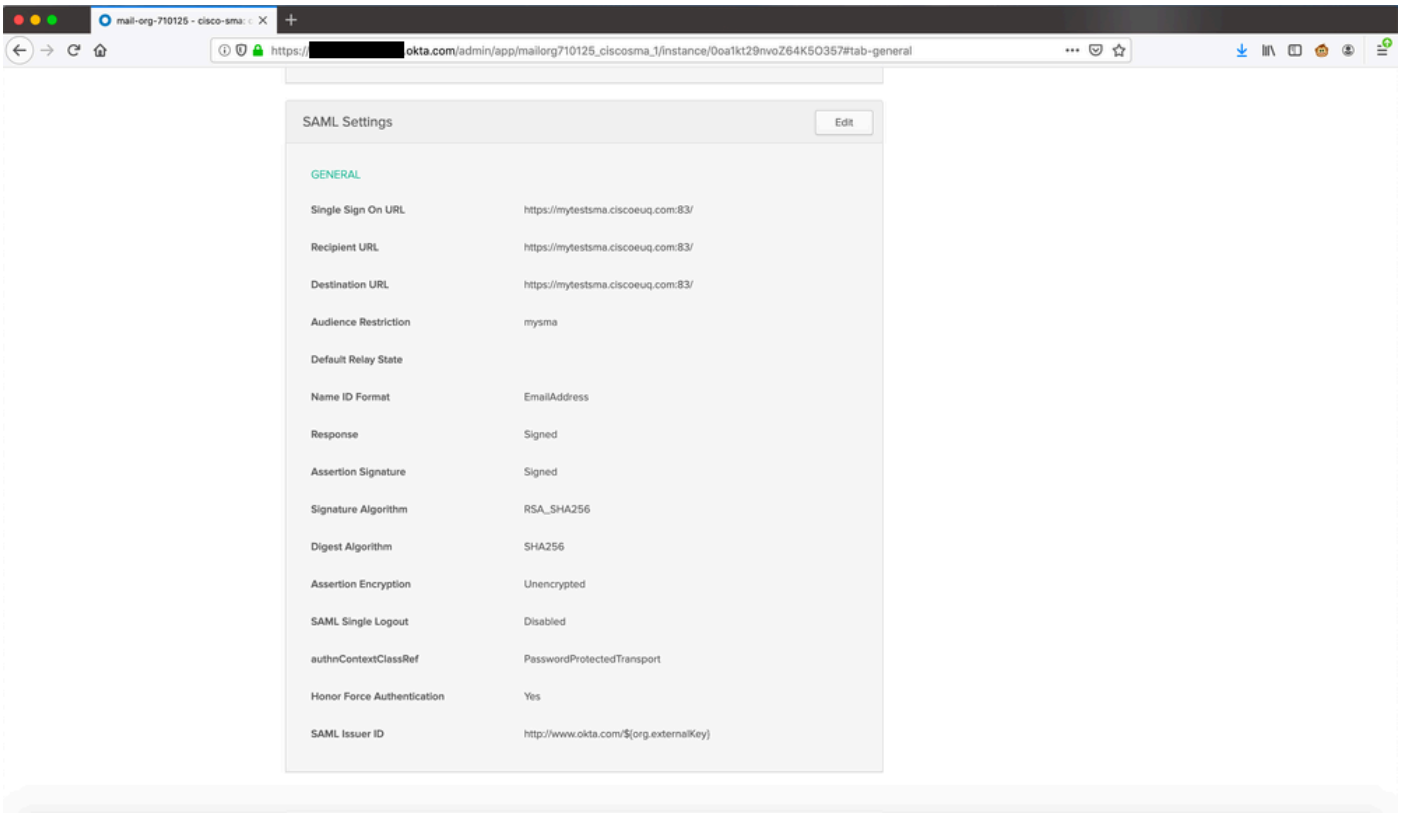
Instelling van serviceprovider in GUI

De SAML-toepassing configureren in Okta

Voer de volgende stappen uit om in Okta een SAML 2.0-toepassing voor SMA EUQ-toegang te maken:

1. Log in bij Okta als beheerder.
2. Navigeer naar Toepassingen > Toepassingen en selecteer vervolgens App-integratie maken.
3. Selecteer SAML 2.0 en selecteer Volgende.
4. Voer een app-naam in, bijvoorbeeld SMA EUQ, en selecteer Volgende.
5. Voer in de URL voor eenmalige aanmelding de SMA ACS-URL in vanuit de instellingen van de SMA-serviceprovider.
6. Voer in Publiek-URI (SP Entity ID) dezelfde entiteit-ID in die op de SMA is geconfigureerd.
7. Selecteer E-mailadres voor de bestandsindeling Naam-ID.
8. Selecteer voor de gebruikersnaam van de toepassing het juiste formaat voor de Okta-gebruikersnaam voor de implementatie.
9. Voltooi de wizard, open vervolgens de nieuwe toepassing en kopieer het IdP-metagegevens-

XML-bestand of de metagegevens URL.

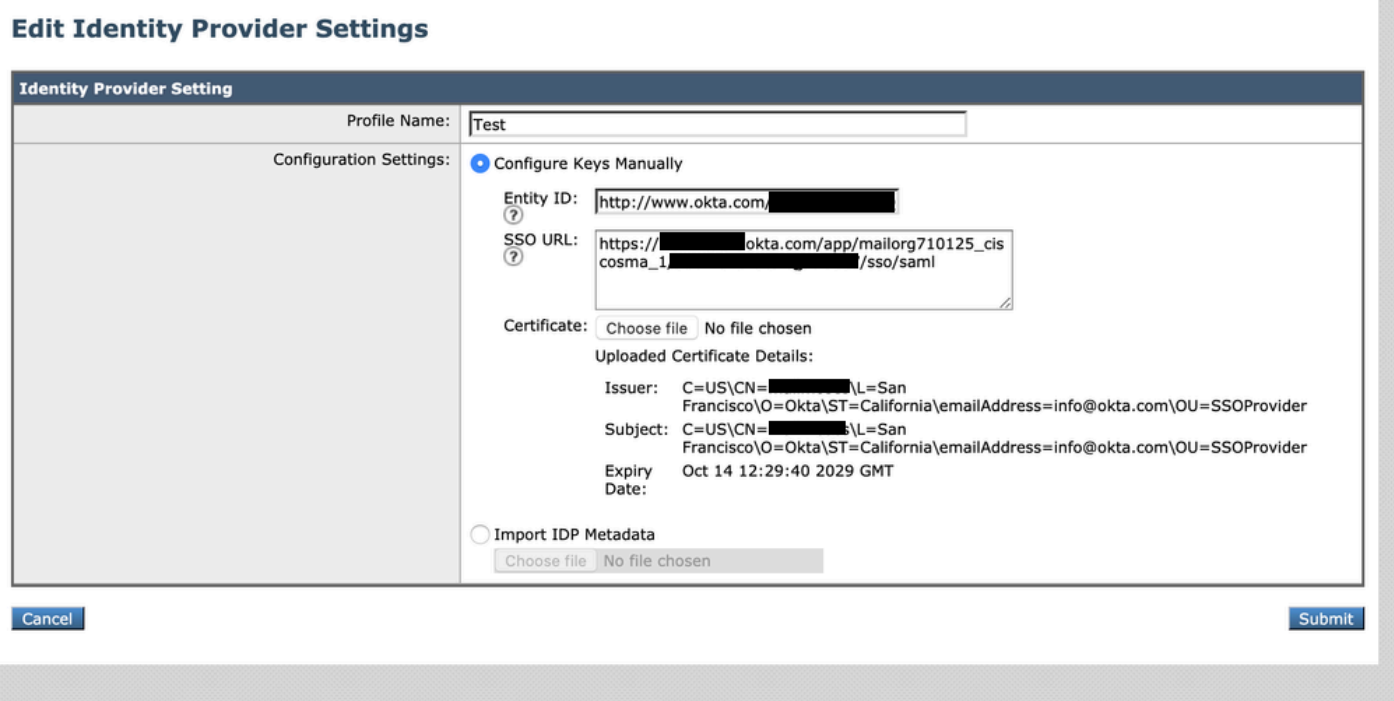


Okta Portal bekijken

De Identity Provider (IdP) configureren op het SMA-toestel

Voer de volgende stappen uit om Okta te configureren als de identiteitsprovider (IdP) op de SMA:

1. Meld u aan bij de SMA web interface.
2. Navigeer naar Systeembeheer > SAML.
3. Importeer onder Instellingen identiteitsleverancier de Okta IdP-metagegevens uit de vorige sectie of voer de waarden handmatig in.

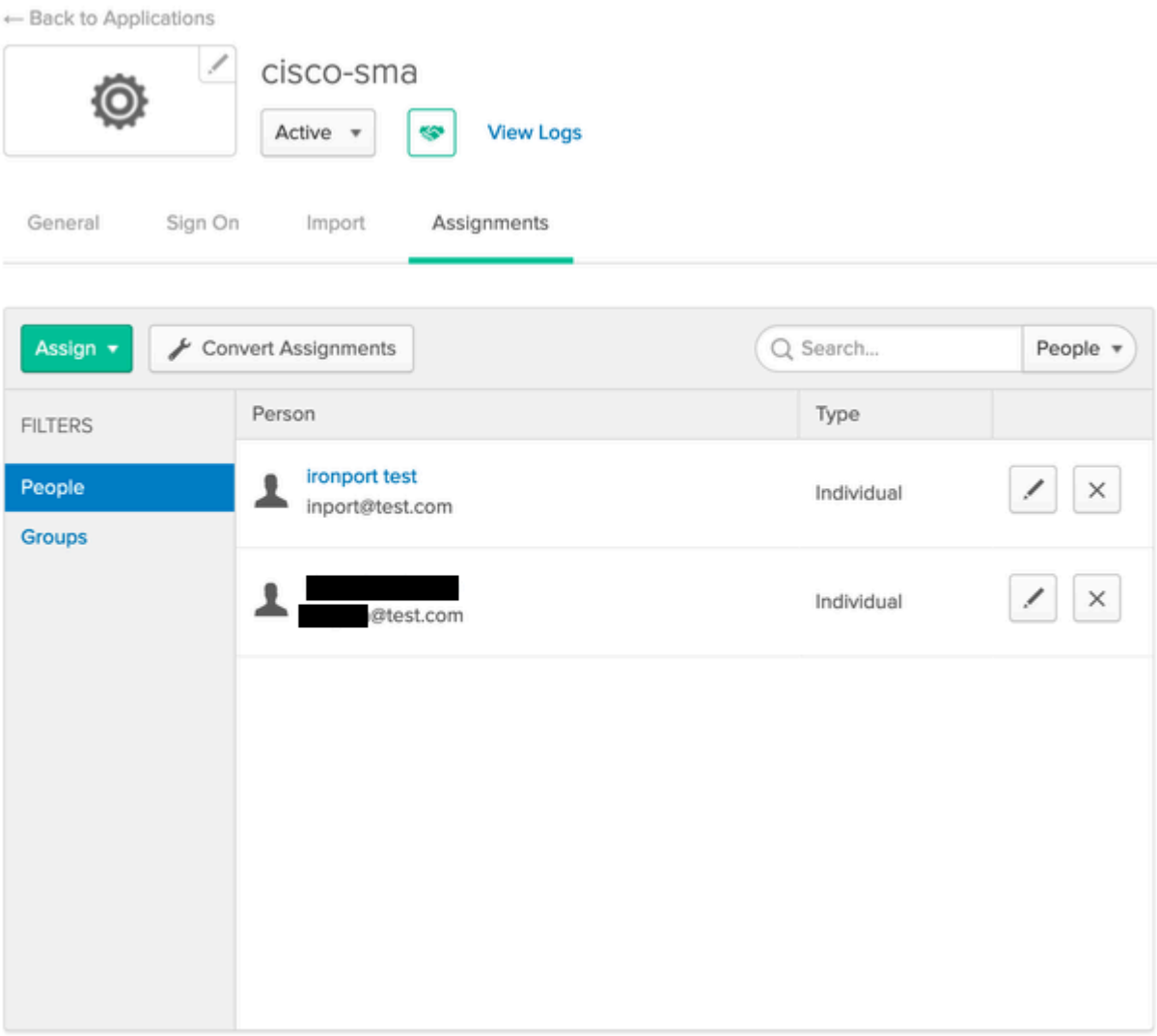


Instellingen voor IdP-profielen in SMA GUI

Gebruikers toewijzen aan de Okta-toepassing

Om gebruikers in staat te stellen zich via Okta te authenticeren bij SMA EUQ, wijzen gebruikers of groepen toe aan de Okta-toepassing:

1. Open in Okta de toepassing die u hebt gemaakt.
2. Navigeer naar Toewijzingen > Personen en selecteer Toewijzen.
3. Selecteer Toewijzen naast elke gebruiker en selecteer Gereed.



Gebruikers toewijzen in Okta Portal

Opmerking: U kunt gebruikers handmatig toewijzen, gebruikers synchroniseren vanuit Active Directory of een andere directoryintegratie gebruiken die Okta ondersteunt.

MFA configureren in Okta (optioneel)

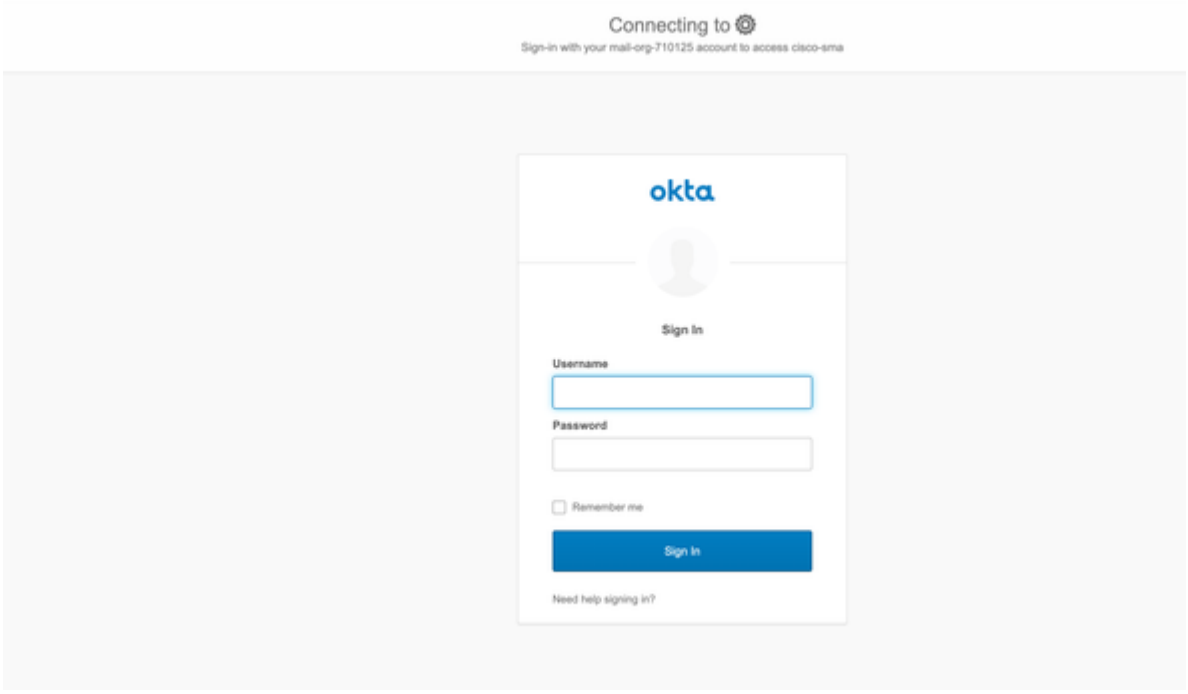
Als u multifactor-verificatie (MFA) voor EUQ-toegang wilt, configureert u het MFA-beleid in Okta voor de toepassing:

1. Navigeer in Okta Admin naar Beveiliging > Authenticatie.
2. Configureer de vereiste factoren, bijvoorbeeld Okta Verify, Google Authenticator of SMS, en pas het beleid toe op de SMA EUQ-toepassing.

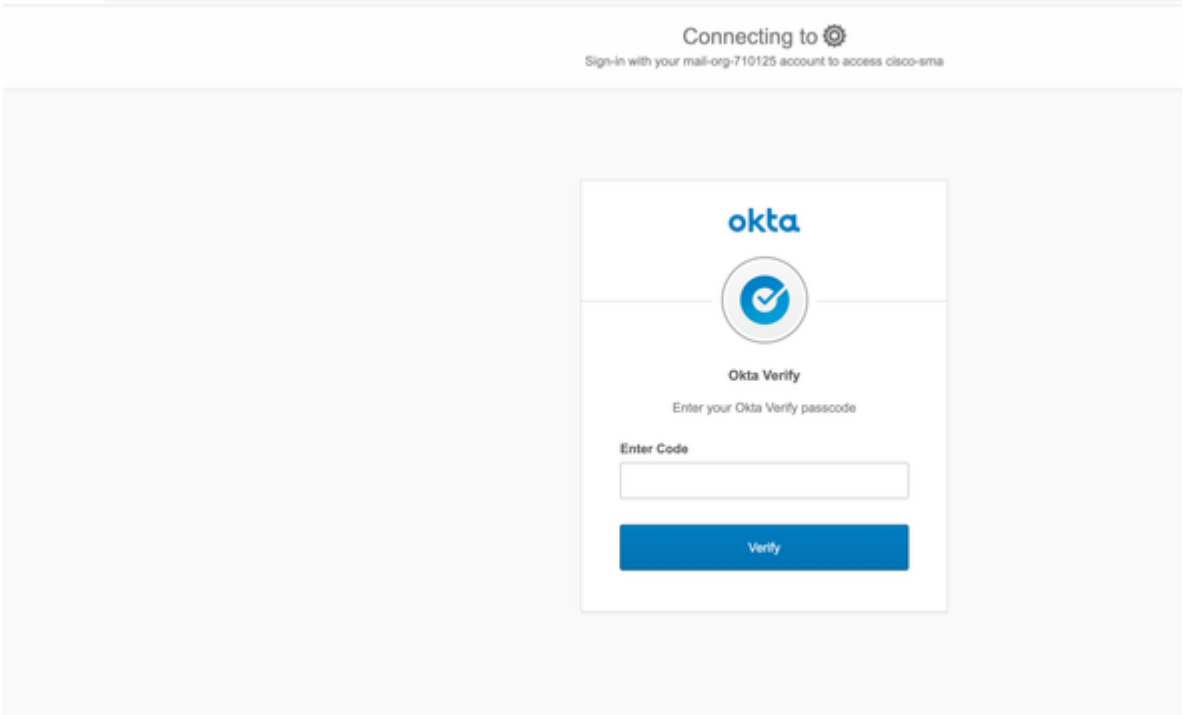
SAML-aanmelding verifiëren

Verwacht resultaat: Voer de volgende stappen uit om de configuratie te controleren:

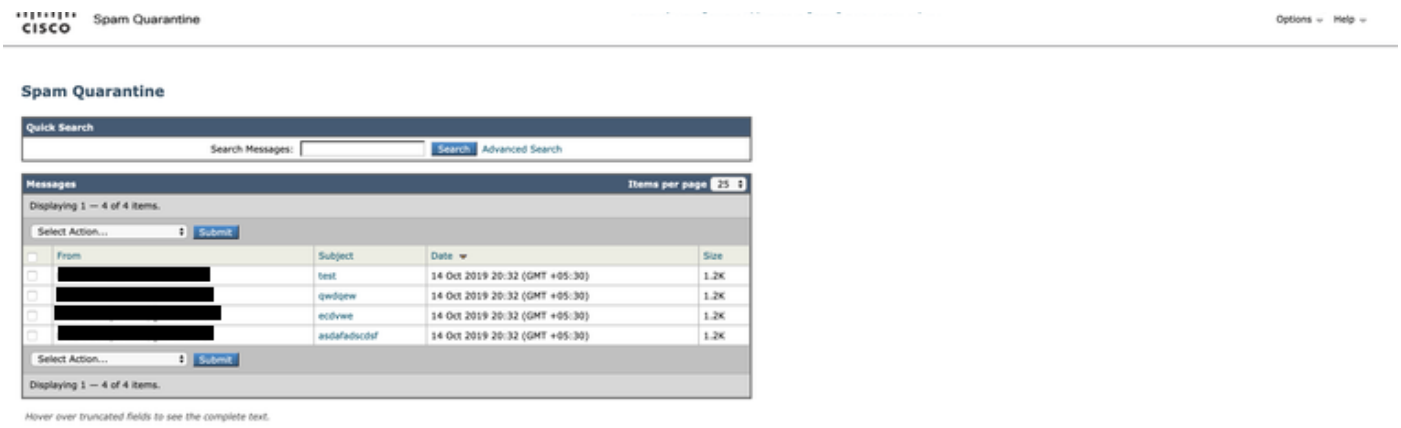
1. Blader naar uw SMA EUQ URL, bijvoorbeeld https://<sma-fqdn>:<port>/.
2. Bevestig dat de browser doorverwijst naar Okta voor verificatie.
3. Als MFB is ingeschakeld, voltooit u de MFB-uitdaging.
4. Bevestig dat u wordt teruggeleid naar het SMA-spam-quarantaineportaal en toegang hebt tot quarantainefuncties.



Inloggen met Okta



Code invoeren voor Okta Verify



Zicht op de Spam Quarantine na het inloggen met 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.