Konfigurieren von OKTA SSO für die Spam-Quarantäne für Endbenutzer

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie OKTA SSO für die Anmeldung bei der Endbenutzer-Spam-Quarantäne der Sicherheitsverwaltungs-Appliance konfiguriert wird.

Voraussetzungen

- Administratorzugriff auf die Cisco Security Management Appliance
- Administratorzugriff auf OKTA.
- Selbstsignierte oder CA-signierte (optional) X.509 SSL-Zertifikate im PKCS #12- oder PEM-Format (von OKTA bereitgestellt).

Hintergrundinformationen

Die Cisco Security Management Appliance ermöglicht die SSO-Anmeldung für Endbenutzer, die die Spam-Quarantäne für Endbenutzer verwenden, und lässt sich in OKTA integrieren, einen Identitätsmanager, der Authentifizierungs- und Autorisierungsdienste für Ihre Anwendungen bereitstellt. Die Cisco Endbenutzer-Spam-Quarantäne kann als Anwendung festgelegt werden, die zur Authentifizierung und Autorisierung mit OKTA verbunden ist. Sie verwendet SAML, ein XML-basiertes, offenes Standarddatenformat, das es Administratoren ermöglicht, nach der Anmeldung bei einer dieser Anwendungen nahtlos auf einen definierten Satz von Anwendungen zuzugreifen.

Weitere Informationen zu SAML finden Sie unter: Allgemeine Informationen zu SAML

Komponenten

- Cloud-Administratorkonto der Cisco Security Management Appliance
- OKTA-Administratorkonto.

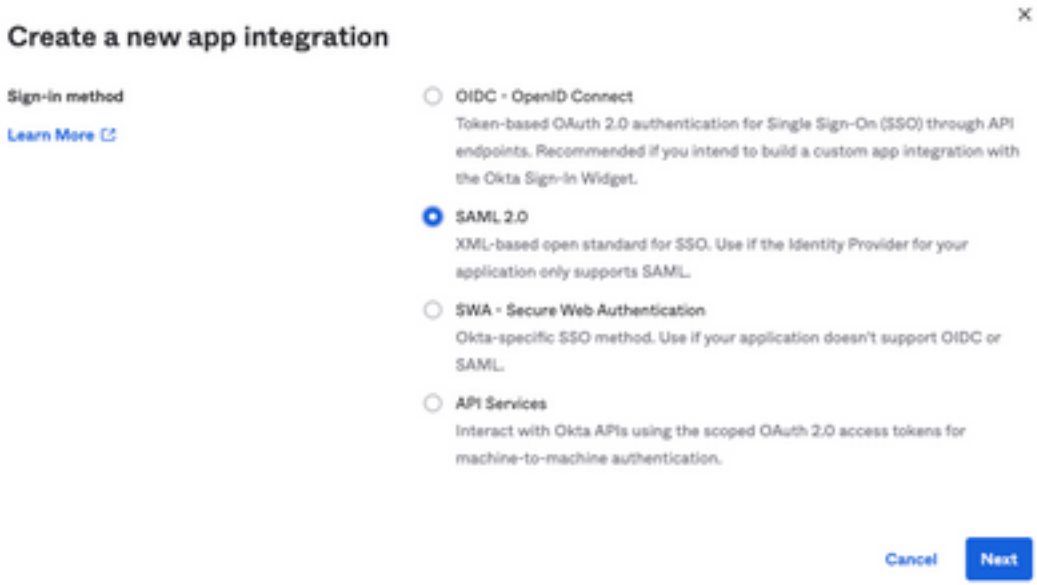
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn das Netzwerk aktiv ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

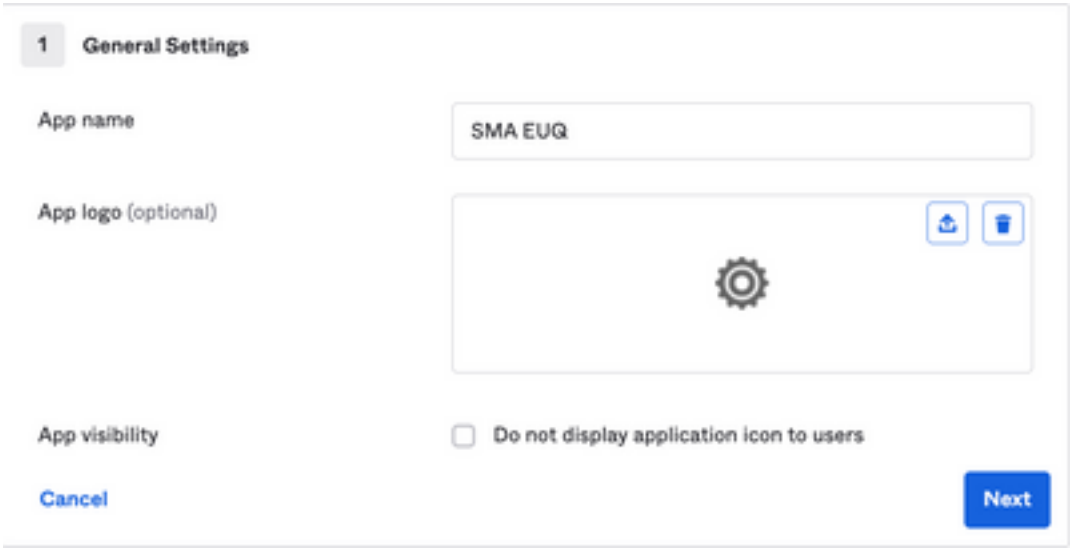
Unter Okta.

1. Navigieren Sie zum Anwendungsportal, und wählen Sie Create App Integration , wie in der Abbildung dargestellt:

2. Wählen SAML 2.0 als Anwendungstyp, wie in der Abbildung dargestellt:



3. Geben Sie den App-Namen ein. SMA EUQ und wählen Next, wie in der Abbildung dargestellt:



4. Unter dem SAML settings, füllen Sie die Lücken aus, wie in der Abbildung dargestellt:

- URL für einmalige Anmeldung: Dies ist der Assertion Consumer Service, der über die SMA

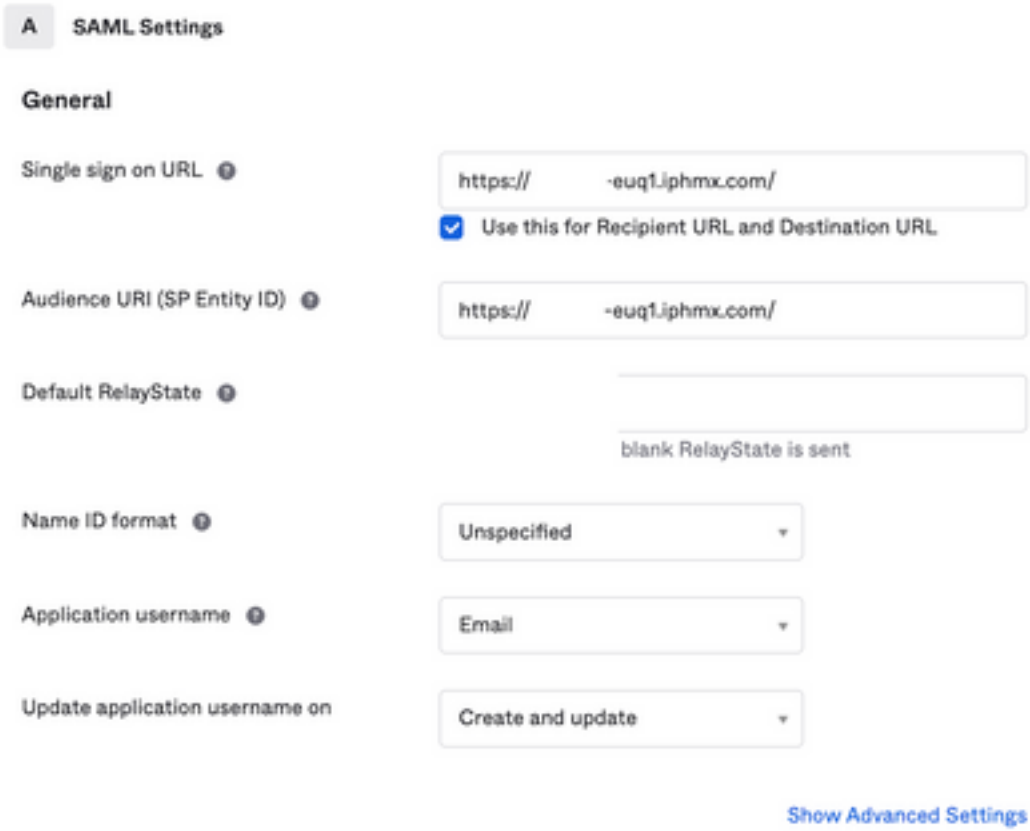
EUQ-Schnittstelle bereitgestellt wird.

- Zielgruppen-URI (SP Entity ID): Dies ist die aus der SMA EUQ Entity ID erhaltene Entity ID.

- Format der Namens-ID: Beibehalten des Namens "Nicht angegeben".

- Application username (Anwendungsbenutzername): Eine E-Mail, die den Benutzer auffordert, seine E-Mail-Adresse bei der Authentifizierung einzugeben.

- Aktualisieren Sie den Benutzernamen der Anwendung auf: Erstellen und Aktualisieren.



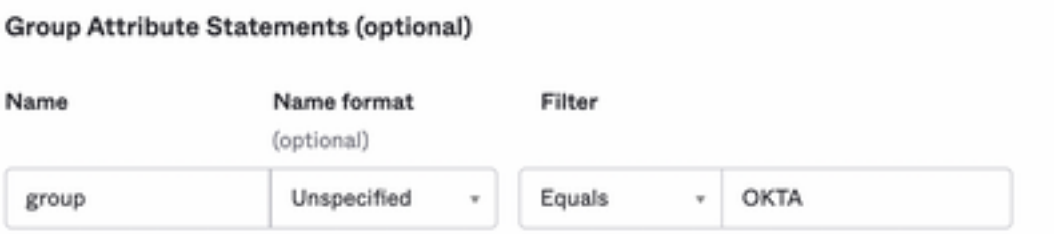
Blättern Sie nach unten zu Group Attibute Statements (optional) , wie in der Abbildung dargestellt:

Geben Sie die nächste Attributanweisung ein:

-Name: group

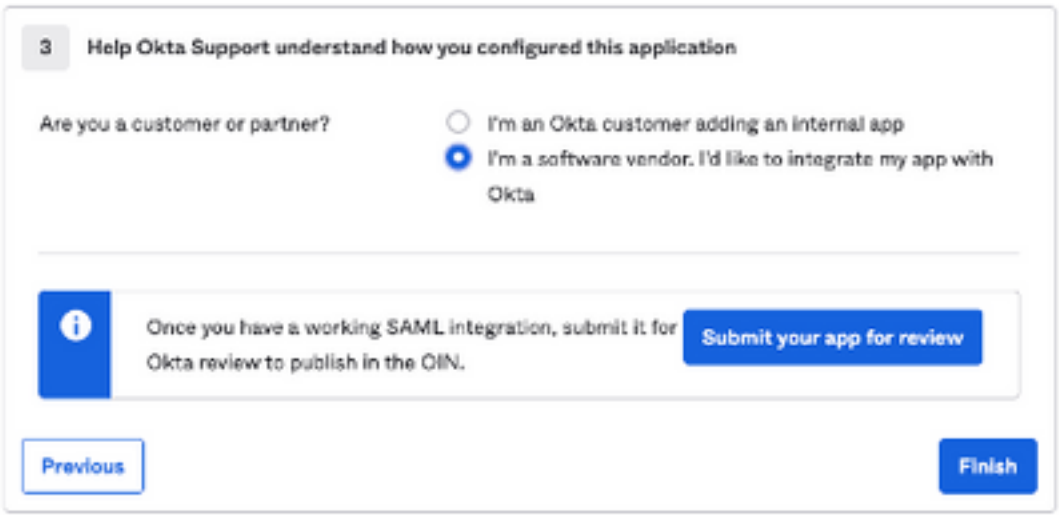
- Namensformat: Unspecified

- Filter: Equals und OKTA



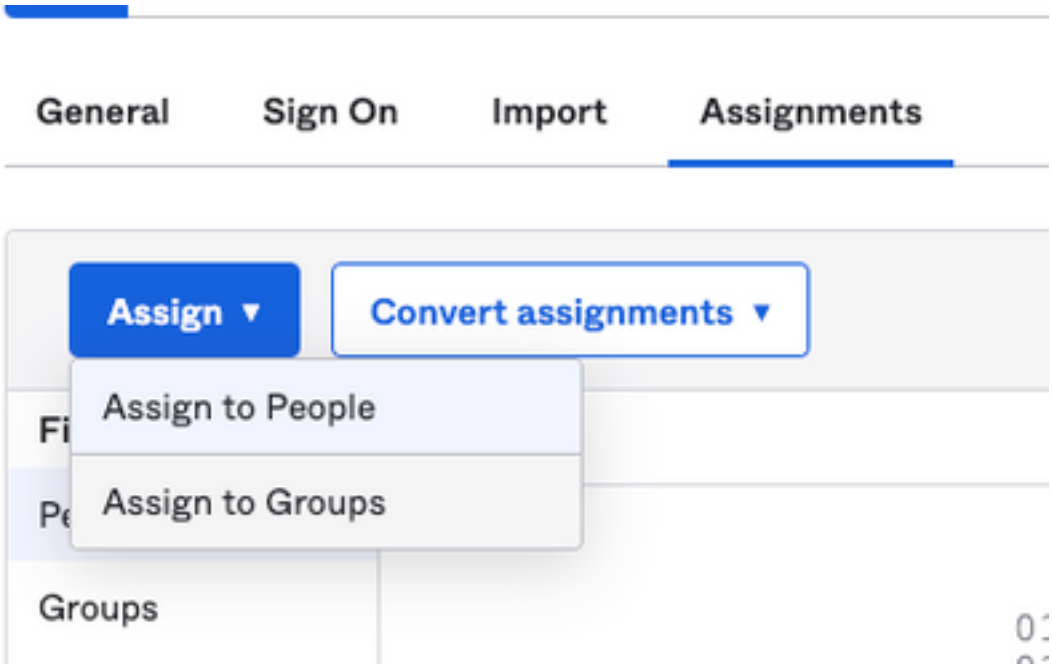
Auswählen Next .

5. Wenn Sie aufgefordert werden, Help Okta to understand how you configured this application, geben Sie bitte den zutreffenden Grund für die aktuelle Umgebung ein, wie in der Abbildung dargestellt:



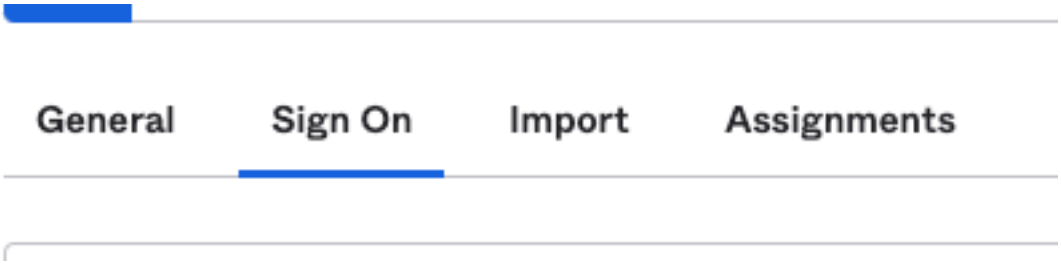
Auswählen Finish um mit dem nächsten Schritt fortzufahren.

6. Wählen Sie Assignments und anschließend Assign > Assign to Groups, wie in der Abbildung dargestellt:



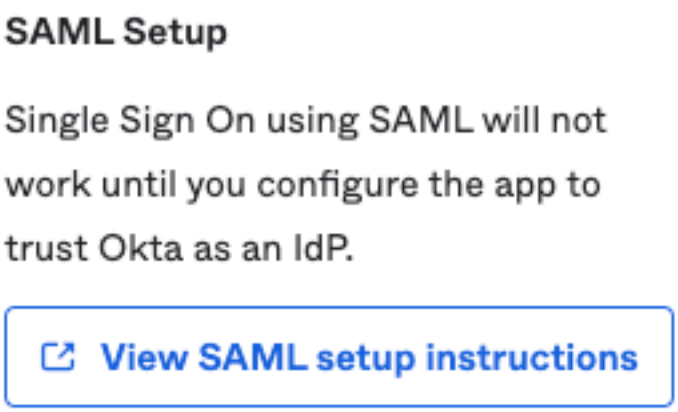
7. Wählen Sie die OKTA-Gruppe, d. h. die Gruppe mit den autorisierten Benutzern, um auf die Umgebung zuzugreifen.

8. Wählen Sign On , wie in der Abbildung dargestellt:



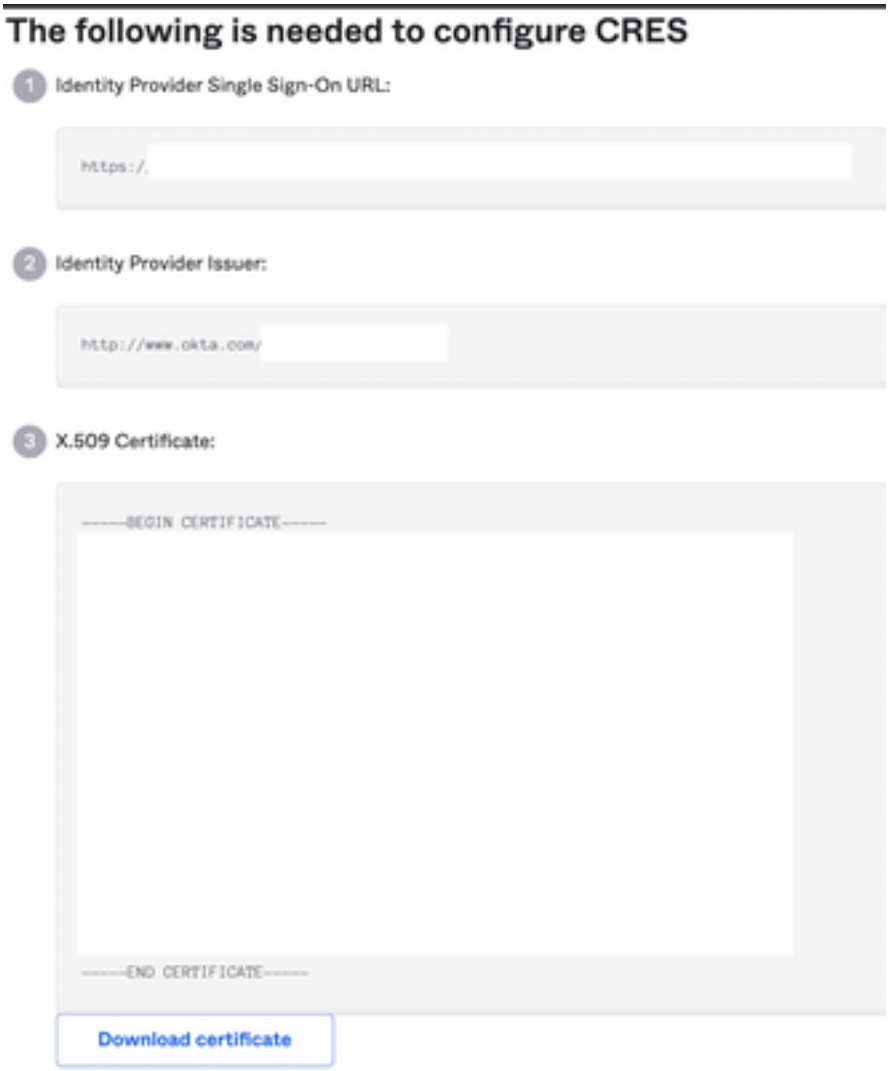
9. Scrollen Sie nach unten und zur rechten Ecke, wählen Sie View SAML setup instructions Option, wie

im Bild gezeigt:



10. Speichern Sie diese Informationen auf einem Notizblock, ist es notwendig, in die Cisco Security Management Appliance SAML-Konfiguration, wie im Bild gezeigt:

- URL für einmalige Anmeldung des Identitätsanbieters
- Aussteller des Identitätsanbieters
- X.509-Zertifikat

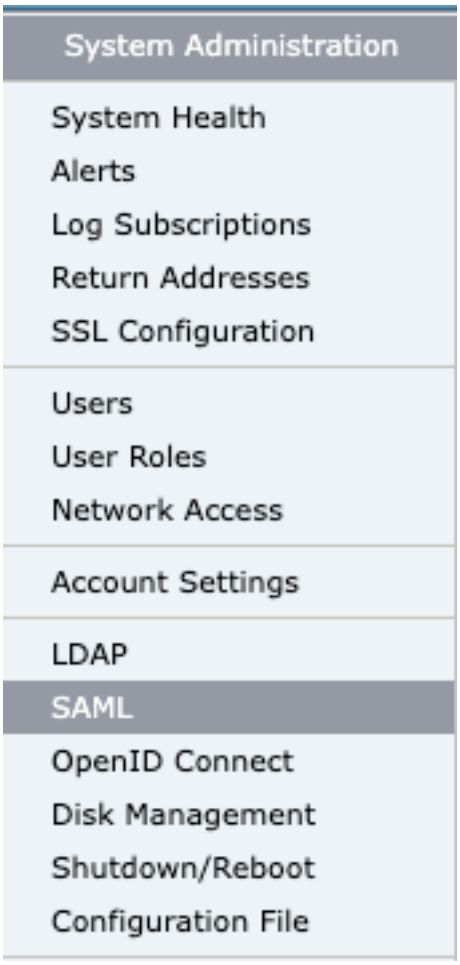


11. Nachdem Sie die OKTA-Konfiguration abgeschlossen haben, können Sie zur Cisco Security Management Appliance zurückkehren.

Unter Cisco Security Management Appliance:

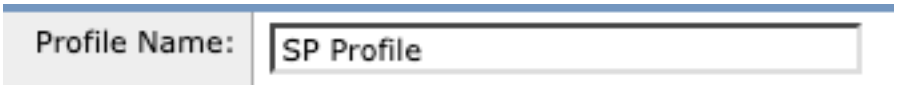
1. Melden Sie sich als Cloud-Administrator bei der Cisco Security Management Appliance an, wie in der Abbildung dargestellt:

2. Auf dem System AdministrationWählen Sie die SAML Option, wie im Bild gezeigt:



3. Ein neues Fenster wird geöffnet, um SAML zu konfigurieren. Unter SAML for End-User Quarantine, Klicken Sie auf Add Service Provider , wie in der Abbildung dargestellt:

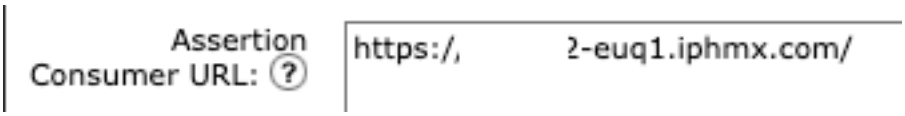
4. Unter Profile Name , geben Sie einen Profilnamen für das Service Provider-Profil ein, wie in der Abbildung dargestellt:



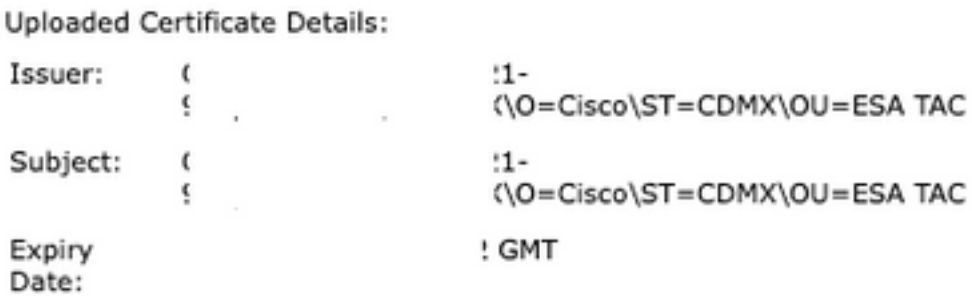
5. Für Entity ID einen global eindeutigen Namen für den Service Provider (in diesem Fall Ihre Appliance) ein. Das Format der Dienstanbieter-Element-ID ist in der Regel ein URI, wie in der Abbildung dargestellt:

6. Für **Name ID Format** , kann dieses Feld nicht konfiguriert werden. Sie benötigen diesen Wert für die Konfiguration des Identitätsanbieters, wie im Bild gezeigt:

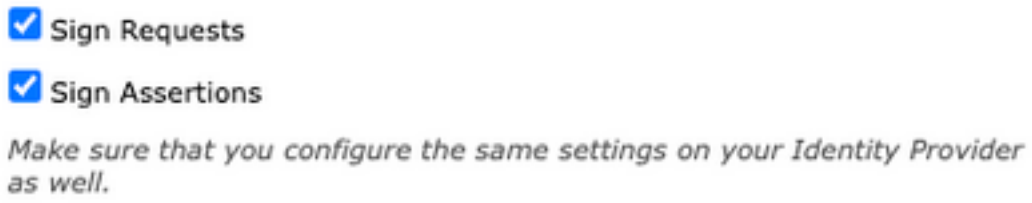
7. Für **Assertion Consumer URL**, geben Sie die URL ein, an die der Identitätsanbieter die SAML-Assertion sendet, nachdem die Authentifizierung erfolgreich abgeschlossen wurde. In diesem Fall ist dies die URL zu Ihrer Spam-Quarantäne.



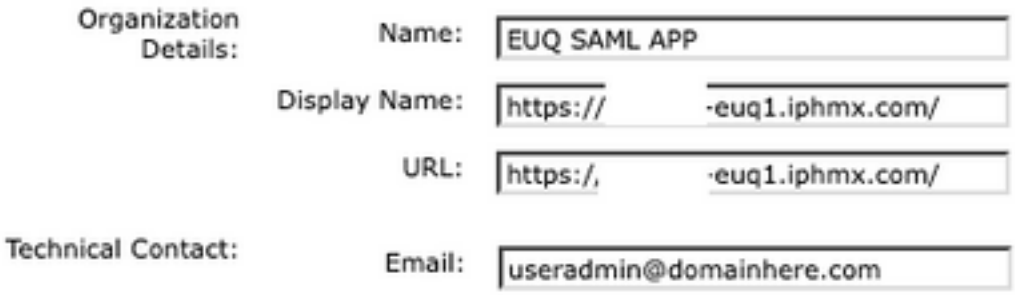
8. Für SP Certificate , das Zertifikat und den Schlüssel hochladen oder die Datei PKCS #12 hochladen. Nach dem Hochladen zeigt der Uploaded Certificate Details wird angezeigt, wie im Bild gezeigt:



9. Für Sign Requests and Sign Assertions , aktivieren Sie beide Kontrollkästchen, wenn Sie die SAML-Anfragen und -Assertionen signieren möchten. Wenn Sie diese Optionen aktivieren, stellen Sie sicher, dass Sie die gleichen Einstellungen für OKTA konfigurieren, wie im Bild gezeigt:

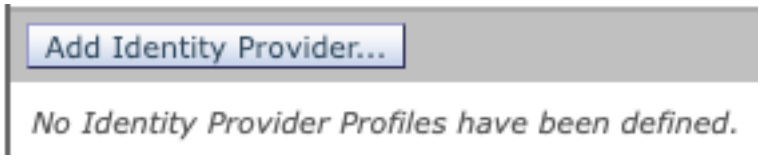


10. Für Organization Details, geben Sie die Details Ihrer Organisation ein, wie im Bild zu sehen:



11. Submit und Commit vor der Konfiguration Identity Provider Settings .

12. Unter SAML ,Klicken Sie auf Add Identity Provider, wie in der Abbildung dargestellt:



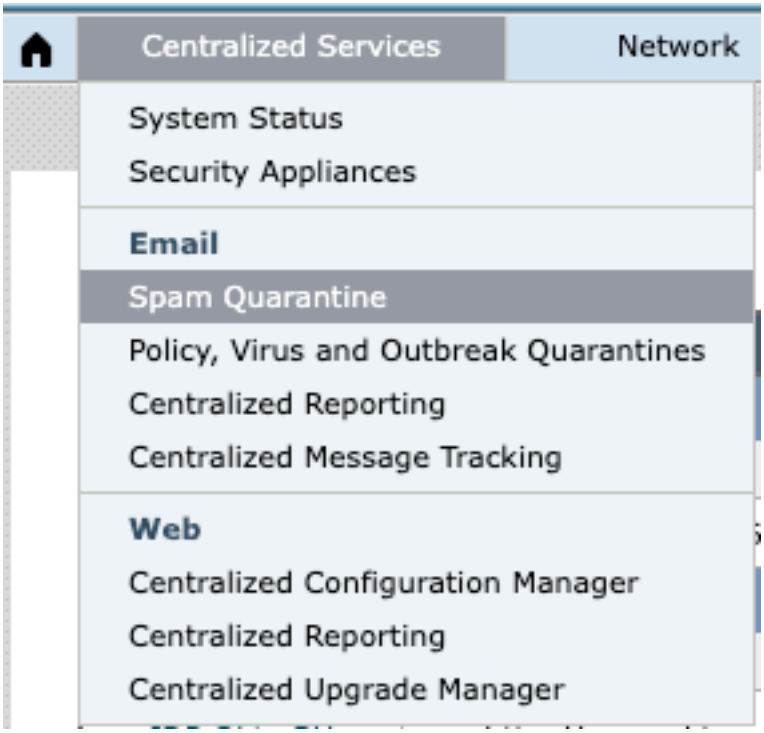
13. Unter Profile Name: Geben Sie einen Namen für das Identity Provider-Profil ein, wie im Bild dargestellt:

14. Wählen Sie Configure Keys Manually und geben Sie die folgenden Informationen ein:

- Element-ID: Die Element-ID des Identitätsanbieters wird zur eindeutigen Identifizierung des Identitätsanbieters verwendet. Sie wird aus den OKTA-Einstellungen in den vorherigen Schritten abgeleitet.
- SSO-URL: Die URL, an die SP SAML-Auth-Anfragen senden soll. Sie wird aus den OKTA-Einstellungen in den vorherigen Schritten abgeleitet.
- Zertifikat: Das Zertifikat, das von OKTA bereitgestellt wird.

15. Submit und Commit die Änderungen zur SAML-Anmeldeaktivierung.

16. Unter Centralized Services > Email , klicken Sie auf Spam Quarantine, wie in der Abbildung dargestellt:



17. Unter Spam Quarantine -> Spam Quarantine Settings ,Klicken Sie auf Edit Settings , as shown in the image:

18. Blättern Sie nach unten zu End-User Quarantine Access > End-User Authentication , wählen SAML 2.0 , wie in der Abbildung dargestellt:

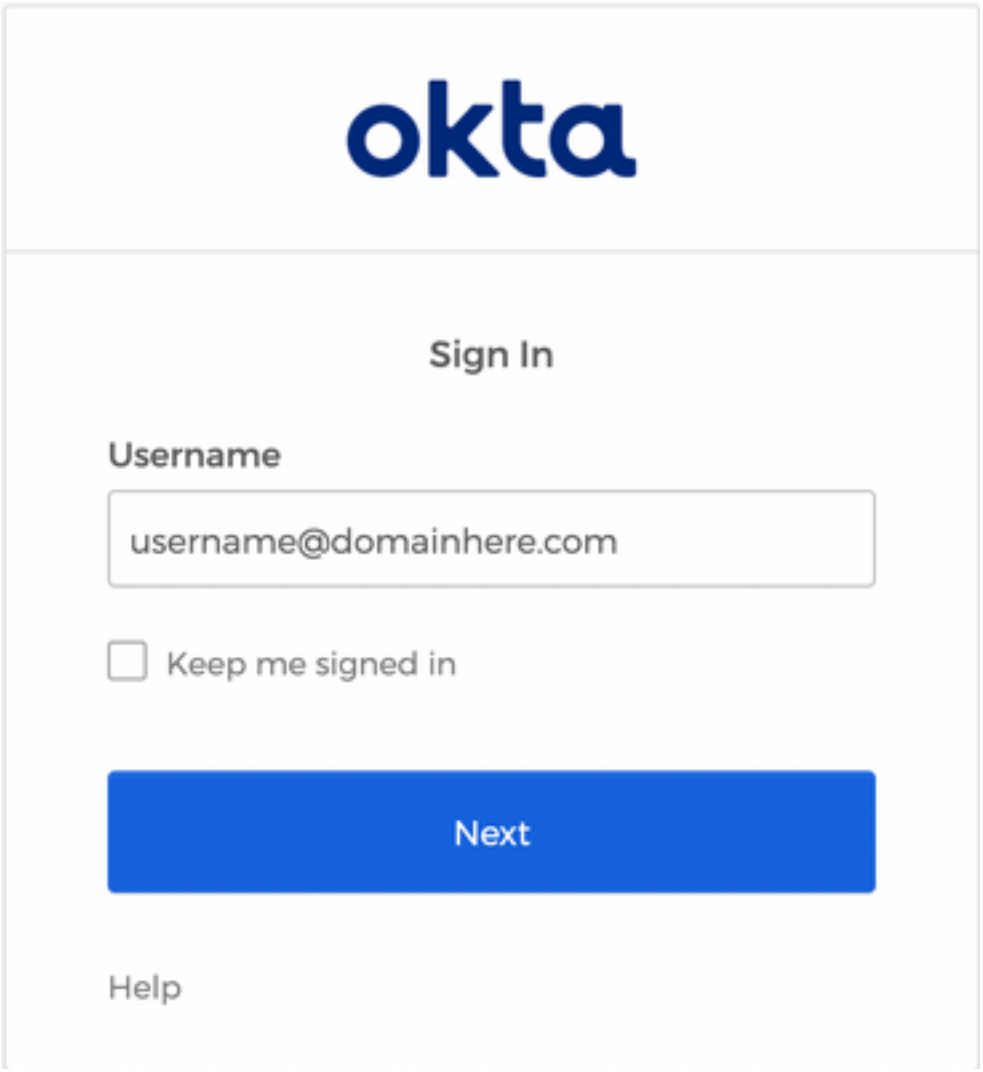
19. Submit und Commit Änderungen zur Aktivierung der SAML-Authentifizierung für **End User Spam Quarantine** .

Überprüfung

1. Geben Sie in einem beliebigen Webbrowser die URL der Spam-Quarantäne für Endbenutzer Ihres Unternehmens ein, wie im Bild gezeigt:

2. Es wird ein neues Fenster geöffnet, in dem Sie mit der OKTA-Authentifizierung fortfahren

können. Melden Sie sich mit den **OKTA-Anmeldeinformationen an**, wie im Bild gezeigt:



3. Wenn die Authentifizierung erfolgreich ist, End User Spam Quarantine öffnet den Inhalt der Spam-Quarantäne für den Benutzer, der sich anmeldet, wie in der Abbildung dargestellt:

Der Endbenutzer kann jetzt mit den OKTA-Anmeldeinformationen auf die Spam-Quarantäne für Endbenutzer zugreifen. .

Zugehörige Informationen

Cisco Secure Email und Web Manager - Benutzerhandbücher

OKTA-Unterstützung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.