Konfigurieren von Okta SAML SSO für die SMA-Endbenutzerquarantäne

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Okta als SAML 2.0-Identitätsanbieter für den Quarantänezugriff für Cisco Secure Email SMA-Endbenutzer konfiguriert wird.

Voraussetzungen

- Produkt: Cisco Secure Email Security Management Appliance (SMA)
- Funktion: SAML SSO für Endbenutzerquarantäne (EUQ)
- Identitätsanbieter: Okta (SAML 2.0)
- Gilt für: SMA-Bereitstellungen, die EUQ-Zugriff auf virtuellen oder Hardwareplattformen ermöglichen. Ersetzen Sie Beispielhostnamen und -ports durch Werte aus Ihrer Umgebung.
- Versionskontext: Dieses Verfahren gilt für SMA-Versionen, die SAML für EUQ unterstützen. Überprüfen Sie die verfügbaren Felder und Menüoptionen in der installierten Version.

Anmerkung: Dieses Dokument behandelt die SMA EUQ SAML-Konfiguration. Auf die ESA wird nur für die Zertifikatgenerierung verwiesen, wenn SMA kein selbstsigniertes Zertifikat generieren kann.

Anforderungen

Bevor Sie beginnen, sollten Sie sich vergewissern, dass Folgendes zutrifft:

- Administrator-Zugriff auf die SMA-Webschnittstelle
- Administratorberechtigungen in Okta zum Erstellen von SAML 2.0-Anwendungen und zum Zuweisen von Benutzern oder Gruppen.
- Ein Zertifikat und ein privater Schlüssel für die Konfiguration des SMA-Dienstanbieters. Ein selbstsigniertes Zertifikat ist zum Testen zulässig.
- Ein erreichbarer vollqualifizierter SMA EUQ-Domänenname (Fully Qualified Domain Name, FQDN) und -Port, auf den Endbenutzer über ihre Browser zugreifen können.
- Die SMA SAML Assertion URL- und SP Entity ID-Werte (aus Systemverwaltung > SAML, nachdem Sie den SP-Eintrag erstellt haben).
- Benutzerkonten in Okta, die der Okta-Anwendung zugewiesen sind.
- Verzeichnissynchronisierte Benutzer, wenn in der Bereitstellung die Verzeichnisintegration verwendet wird.

Anmerkung: Okta ist ein Drittanbieter von Identitätslösungen. Dieses Dokument enthält eine Beispielkonfiguration für Kundenreferenzen.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

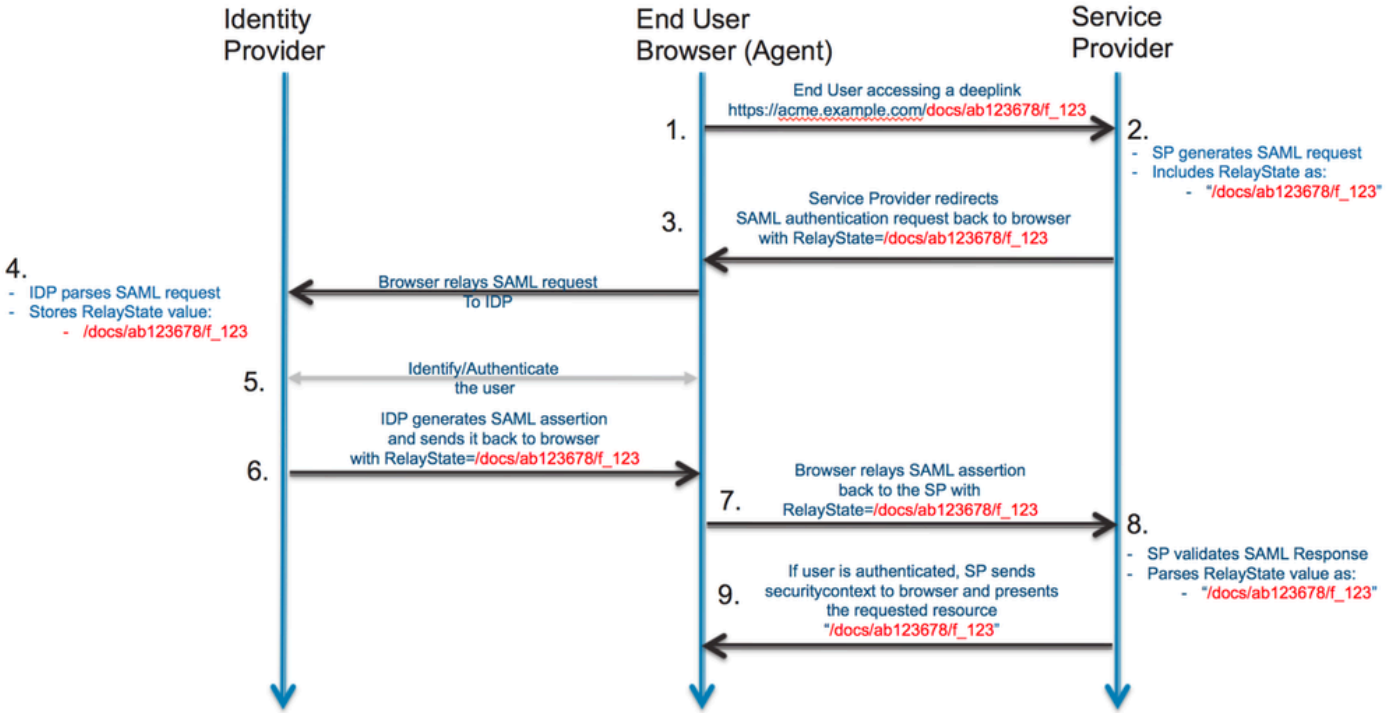
Hintergrundinformationen

Das Ziel ist es, die einmalige Anmeldung (Single Sign-on, SSO) für das Spam-Quarantäne-Portal so zu konfigurieren, dass Benutzer zur Authentifizierung an Okta umgeleitet werden, vollständige Multifaktor-Authentifizierung (MFA), wenn sie in Okta aktiviert ist, und dann zum SMA EUQ-Portal zurückzukehren. Dieses Dokument gilt nur für SMA. Auf Cisco Secure Email Gateway, ehemals Email Security Appliance (ESA), wird nur für die Zertifikatgenerierung verwiesen, wenn SMA kein selbstsigniertes Zertifikat generieren kann.

Problem: Benutzer müssen sich mit SAML SSO und optional MFA beim SMA Spam Quarantine Portal mit Okta authentifizieren.

Auflösung: Konfigurieren Sie SMA als Service Provider, konfigurieren Sie eine SAML-Anwendung in Okta, importieren Sie die Okta-IdP-Einstellungen in SMA, weisen Sie Benutzer in Okta zu, und überprüfen Sie den Zugriff.

SAML-Fluss:



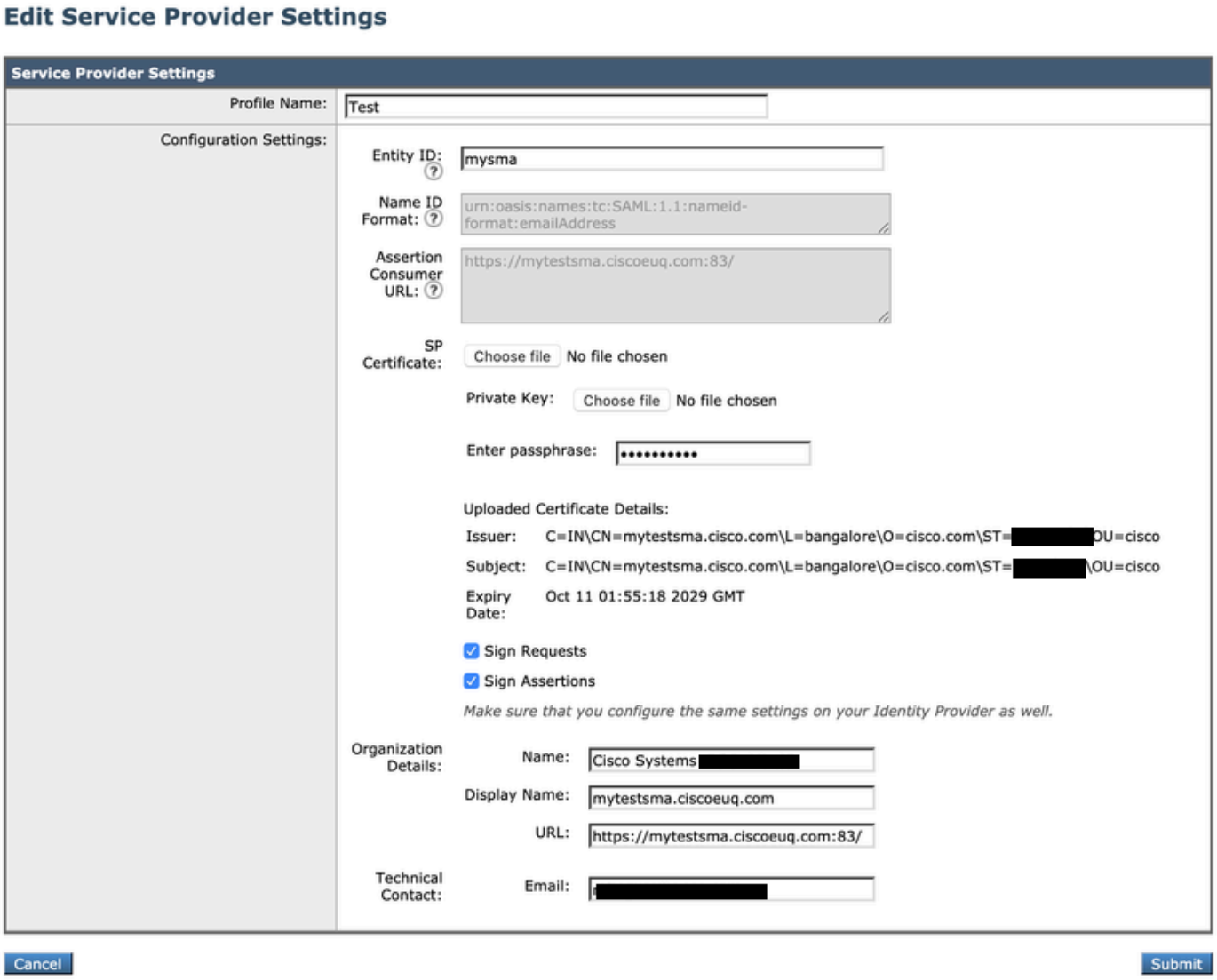
Konfiguration

Konfigurieren des Service Providers (SP) auf der SMA-Appliance

Führen Sie die folgenden Schritte aus, um die SMA als SAML-Dienstanbieter für den EUQ-Zugriff zu konfigurieren:

1. Melden Sie sich bei der SMA-Webschnittstelle an.
2. Navigieren Sie zu Systemverwaltung > SAML.
3. Wählen Sie Dienstanbieter hinzufügen aus.
4. Geben Sie in Service Provider Entity ID (Element-ID des Dienstanbieters) die Element-ID ein, die Sie auch in Okta konfigurieren können.
5. Überprüfen Sie, ob das Name ID-Format und die ACS-URL (Assertion Consumer Service) für die EUQ-Schnittstelle eingetragen sind.
6. Laden Sie im SP-Zertifikat ein Zertifikat hoch, um SAML-Anforderungen zu signieren.

Anmerkung: SMA kann kein selbstsigniertes Zertifikat generieren. Sie können auch ein Zertifikat auf einer ESA generieren und zur Verwendung auf der SMA exportieren.



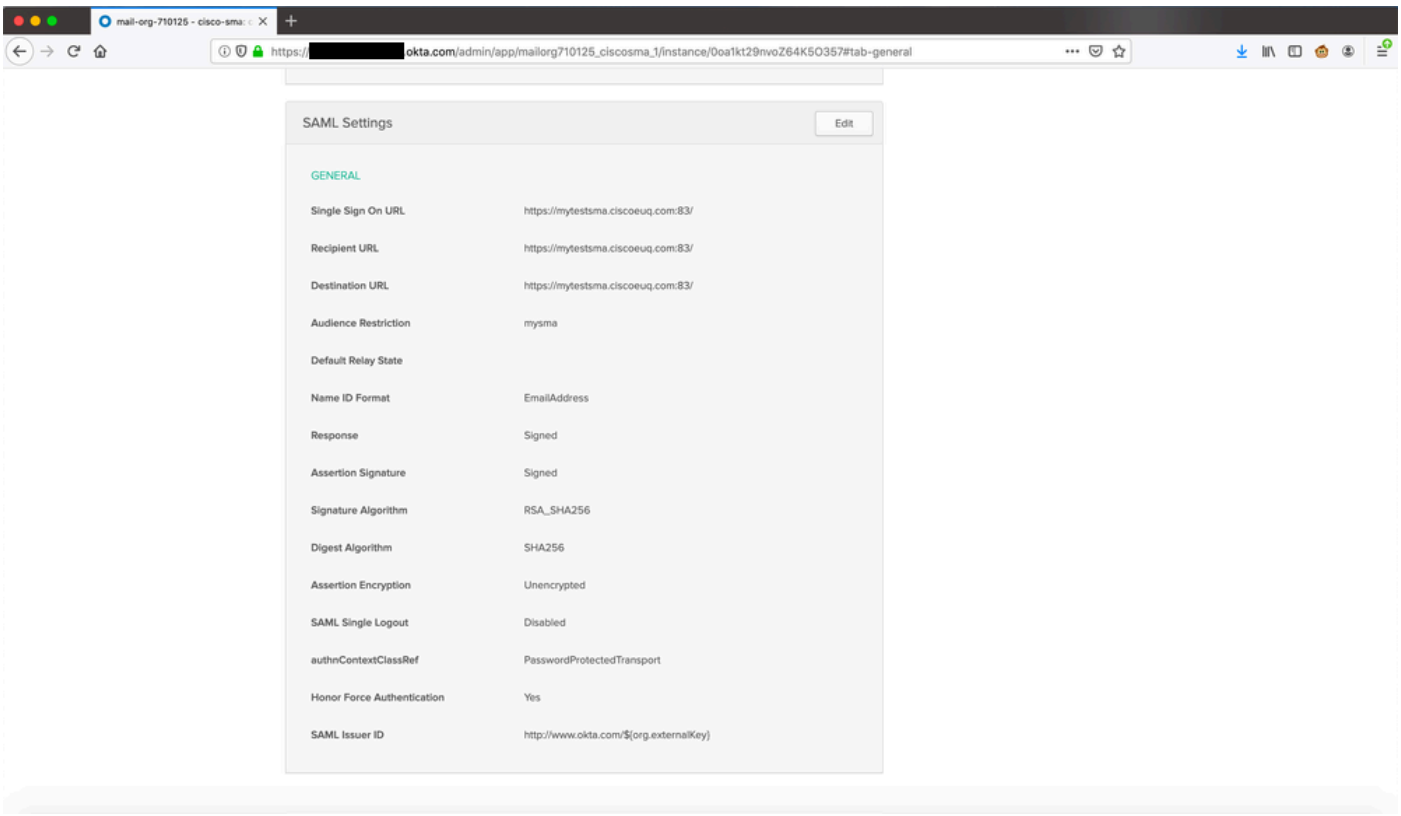
Einstellung des Service Providers in der GUI

Konfigurieren der SAML-Anwendung in Okta

Führen Sie die folgenden Schritte aus, um eine SAML 2.0-Anwendung in Okta für den SMA EUQ-Zugriff zu erstellen:

1. Melden Sie sich als Administrator bei Okta an.
2. Navigieren Sie zu Anwendungen > Anwendungen, und wählen Sie dann Anwendungsintegration erstellen aus.
3. Wählen Sie SAML 2.0 und dann Weiter aus.
4. Geben Sie einen Anwendungsnamen ein, z. B. SMA EUQ, und wählen Sie dann Weiter aus.
5. Geben Sie unter Single Sign-on URL (URL für einmalige Anmeldung) die SMA ACS-URL aus den Einstellungen des SMA Service Providers ein.
6. Geben Sie in Audience URI (SP Entity ID) dieselbe Entity-ID ein, die auf der SMA konfiguriert wurde.
7. Wählen Sie als Format der Namens-ID die Option EmailAddress aus.
8. Wählen Sie als Anwendungsbenutzernamen das für Ihre Bereitstellung geeignete Format für den Okta-Benutzernamen aus.

9. Schließen Sie den Assistenten ab, öffnen Sie dann die neue Anwendung und kopieren Sie die IdP-Metadaten-XML-Datei oder die Metadaten-URL. (nur in englischer Sprache verfügbar).

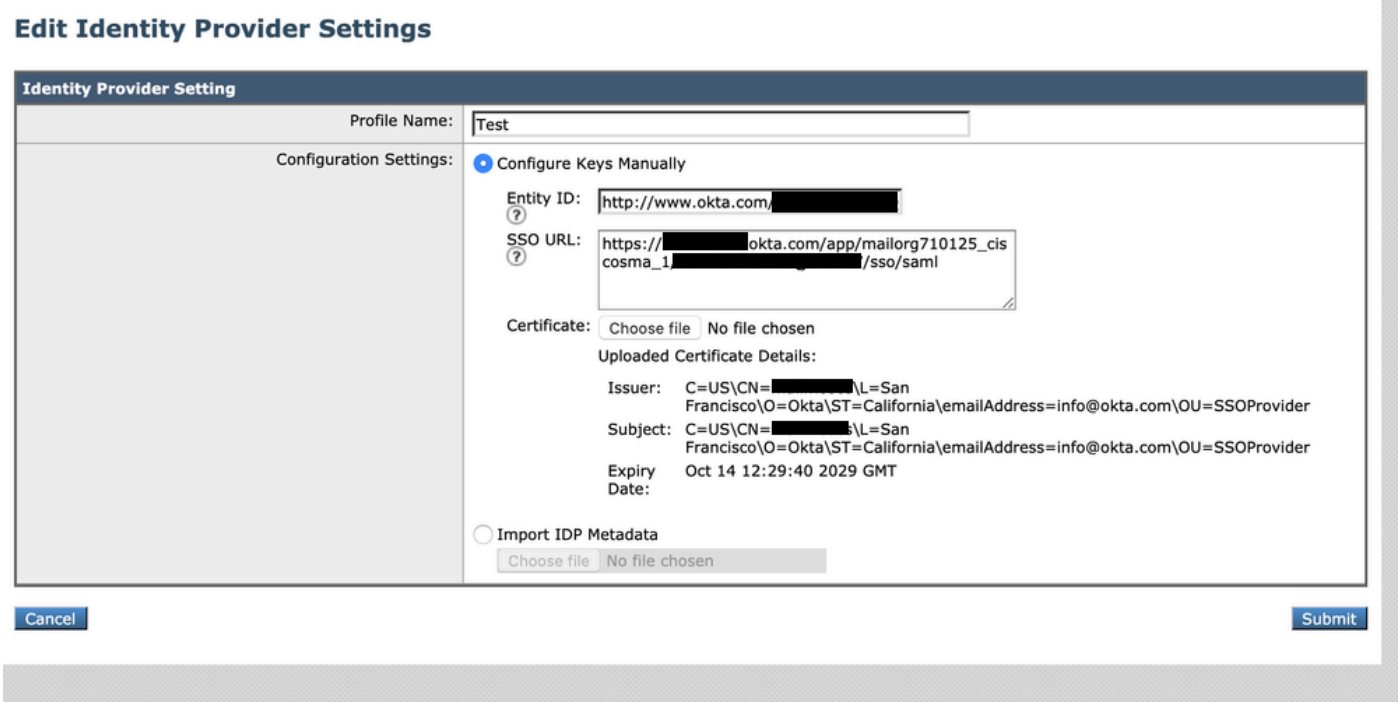


Okta-Portal anzeigen

Konfigurieren des Identitätsanbieters (IdP) auf der SMA-Appliance

Führen Sie die folgenden Schritte aus, um Okta als Identitätsanbieter (IdP) auf der SMA zu konfigurieren:

1. Melden Sie sich bei der SMA-Webschnittstelle an.
2. Navigieren Sie zu Systemverwaltung > SAML.
3. Importieren Sie unter Identity Provider Settings die Okta IdP-Metadaten aus dem vorherigen Abschnitt, oder geben Sie die Werte manuell ein.

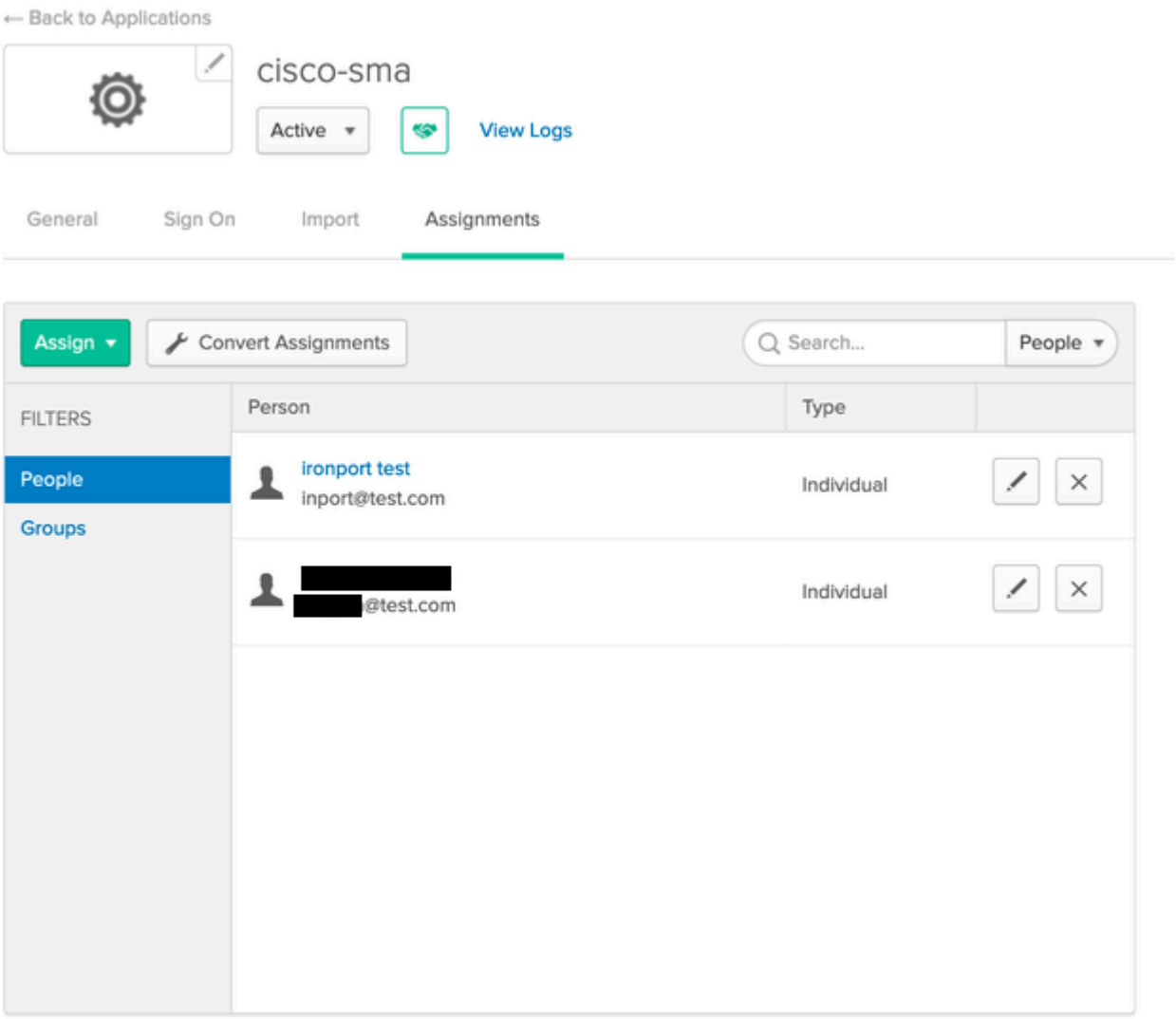


Einstellungen für IDp-Profile in der SMA-GUI

Zuweisen von Benutzern zur Okta-Anwendung

Um Benutzern die Authentifizierung bei SMA EUQ über Okta zu ermöglichen, weisen Sie der Okta-Anwendung Benutzer oder Gruppen zu:

1. Öffnen Sie in Okta die Anwendung, die Sie erstellt haben.
2. Navigieren Sie zu Aufgaben > Personen, und wählen Sie dann Zuweisen.
3. Wählen Sie Zuweisen neben jedem Benutzer aus, und wählen Sie dann Fertig.



Zuweisen von Benutzern im Okta-Portal

Anmerkung: Sie können Benutzer manuell zuweisen, Benutzer von Active Directory synchronisieren oder eine andere Verzeichnisintegration verwenden, die Okta unterstützt.

Konfigurieren von MFA in Okta (optional)

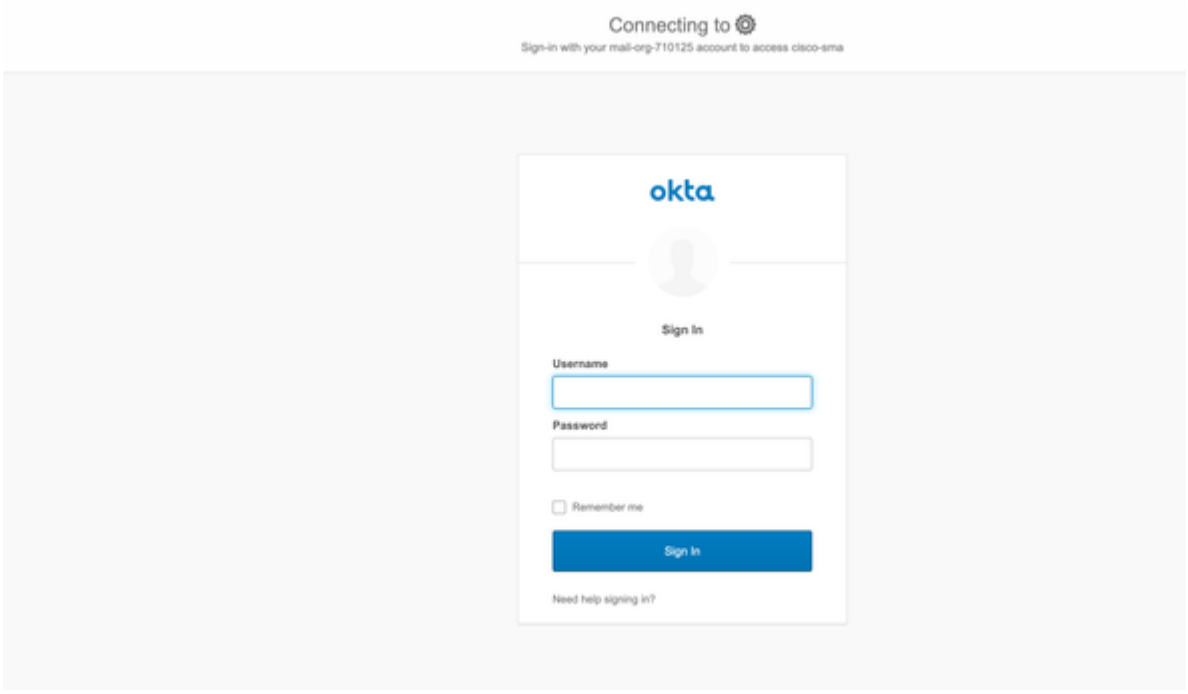
Wenn Sie Multifaktor-Authentifizierung (MFA) für den EUQ-Zugriff wünschen, konfigurieren Sie die MFA-Richtlinien in Okta für die Anwendung:

1. Navigieren Sie in Okta Admin zu Sicherheit > Authentifizierung.
2. Konfigurieren Sie die erforderlichen Faktoren, z. B. Okta Verify, Google Authenticator oder SMS, und wenden Sie die Richtlinie auf die SMA EUQ-Anwendung an.

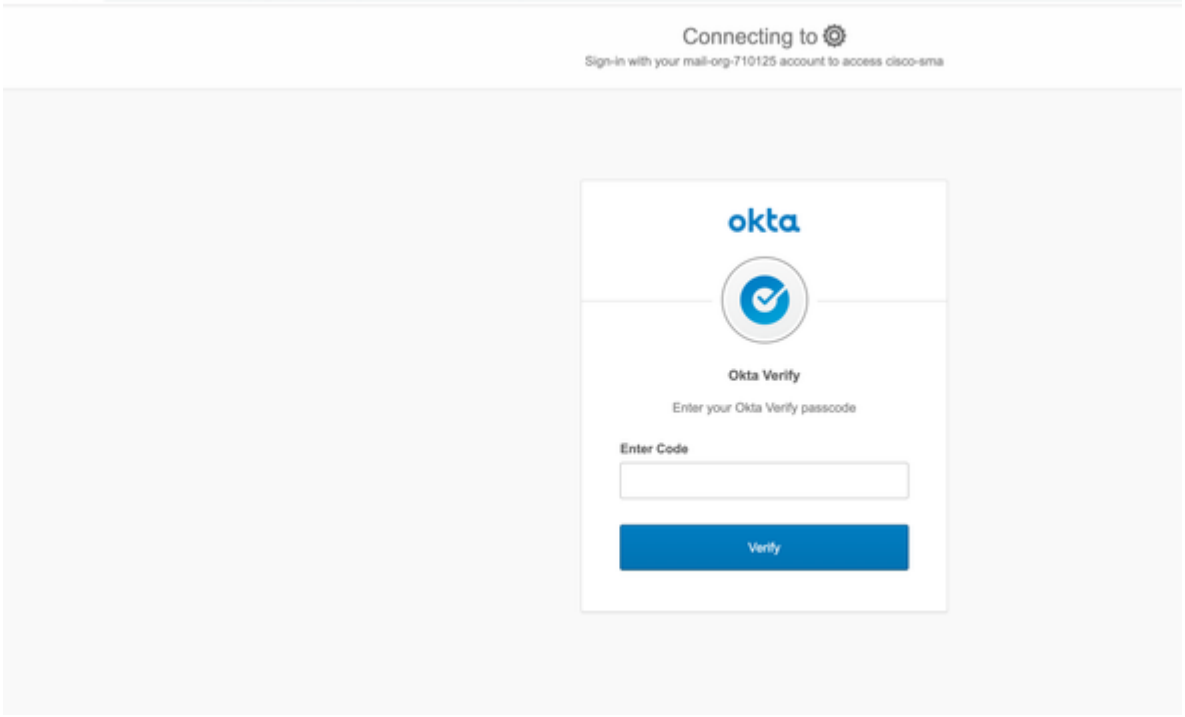
SAML-Anmeldung überprüfen

Erwartetes Ergebnis: Gehen Sie wie folgt vor, um die Konfiguration zu überprüfen:

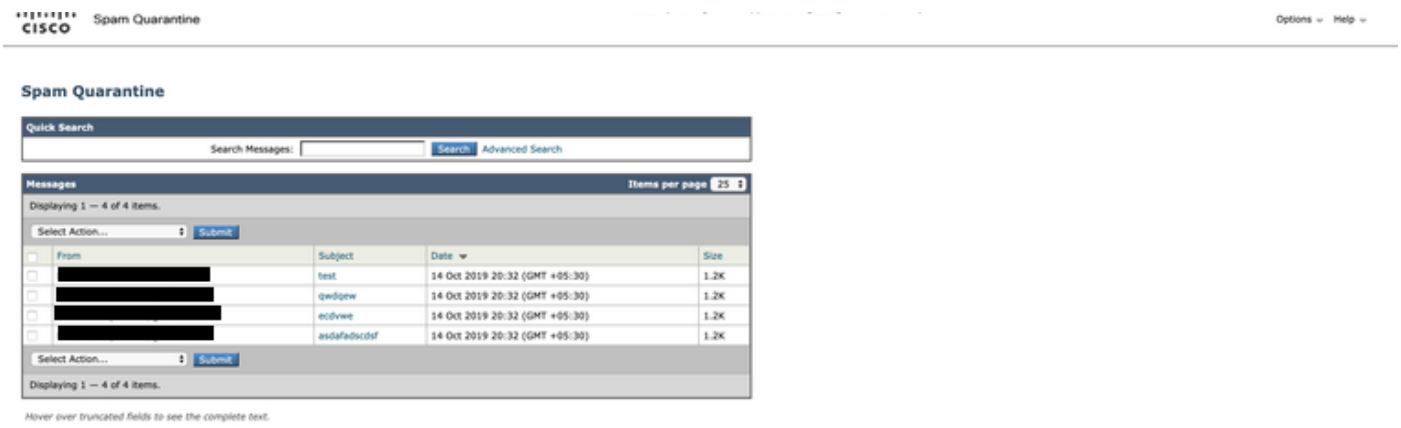
1. Navigieren Sie zu Ihrer SMA EUQ-URL, z. B. https://<sma-fqdn>:<port>/.
2. Bestätigen Sie, dass der Browser zur Authentifizierung auf Okta umleitet.
3. Wenn MFA aktiviert ist, führen Sie die MFA-Herausforderung aus.
4. Bestätigen Sie, dass Sie zurück zum SMA-Spam-Quarantäne-Portal weitergeleitet werden und auf Quarantäne-Funktionen zugreifen können.



Anmeldung mit Okta



Code für Okta-Überprüfung eingeben



Ansicht der Spam-Quarantäne nach Anmeldung bei Okta

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.