SMAエンドユーザ隔離のためのOkta SAML SSOの設定

内容

はじめに

このドキュメントでは、Cisco Secure Email SMAエンドユーザ隔離アクセス用のSAML 2.0 IDプロバイダーとしてOktaを設定する方法について説明します。

前提条件

- 製品：Cisco Secure Email Security Management Appliance(SMA)
- 機能：エンドユーザ隔離(EUQ)用のSAML SSO
- アイデンティティプロバイダー：Okta(SAML 2.0)
- 対象：仮想プラットフォームまたはハードウェアプラットフォームでEUQアクセスを提供するSMA展開。ホスト名とポートの例を、実際の環境の値に置き換えてください。
- バージョンコンテキスト：この手順は、EUQのSAMLをサポートするSMAリリースに適用されます。インストールされているバージョンで使用可能なフィールドとメニューオプションを確認します。

注：このドキュメントでは、SMA EUQ SAML設定を中心に説明します。ESAは、SMAが自己署名証明書を生成できない場合にのみ、証明書生成のために参照されます。

要件

作業を開始する前に、次の点を確認してください。

- SMA Webインターフェイスへの管理アクセス。
- SAML 2.0アプリケーションを作成し、ユーザまたはグループを割り当てるOktaの管理者権限。
- SMAサービスプロバイダー設定の証明書および秘密キー。自己署名証明書は、テストに使用できます。
- 到達可能なSMA EUQの完全修飾ドメイン名(FQDN)と、エンドユーザがブラウザからアクセスできるポート。
- SMA SAMLアサーションURLおよびSPエンティティIDの値(SPエントリの作成後にSystem Administration > SAMLから取得)。
- Oktaアプリケーションに割り当てられているOktaのユーザーアカウント。
- ディレクトリ統合を使用している場合は、ディレクトリ同期ユーザー。

注：Oktaはサードパーティのアイデンティティプロバイダーです。このドキュメントでは、カスタマーリファレンスの設定例を紹介します。

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

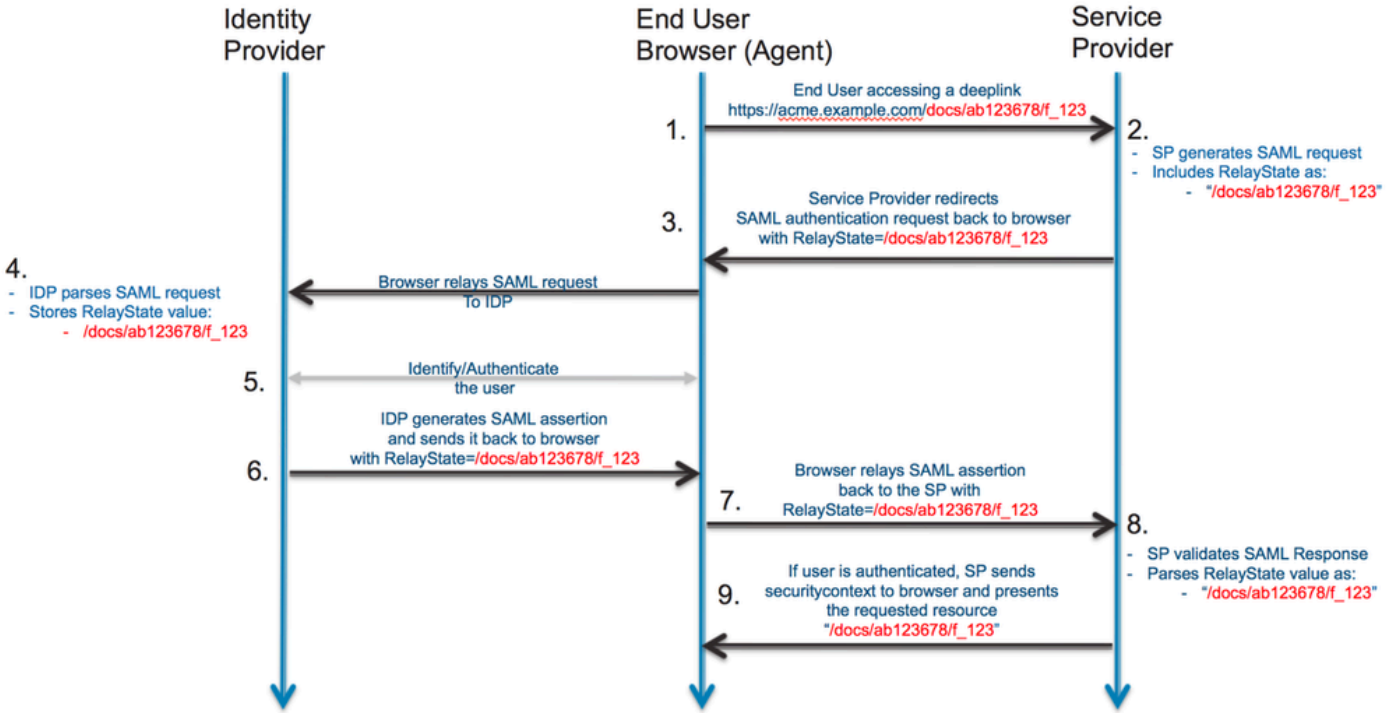
バックグラウンド情報

目標は、ユーザが認証のためにOktaにリダイレクトされ、Oktaでマルチファクタ認証(MFA)が有効になっている場合にそれを完了して、SMA EUQポータルに戻るように、スパム検疫ポータルのシングルサインオン(SSO)を設定することです。このドキュメントは、SMAにのみ適用されます。Cisco Secure Email Gateway(以前のEmail Security Appliance(ESA))は、SMAが自己署名証明書を生成できない場合にのみ証明書の生成で参照されます。

問題：ユーザはSAML SSOとオプションのMFAを使用して、OktaでSMAスパム検疫ポータルに認証する必要があります。

解決策：SMAをサービスプロバイダーとして設定し、OktaでSAMLアプリケーションを設定し、Okta IdP設定をSMAにインポートし、Oktaでユーザを割り当て、アクセスを確認します。

SAMLフロー：



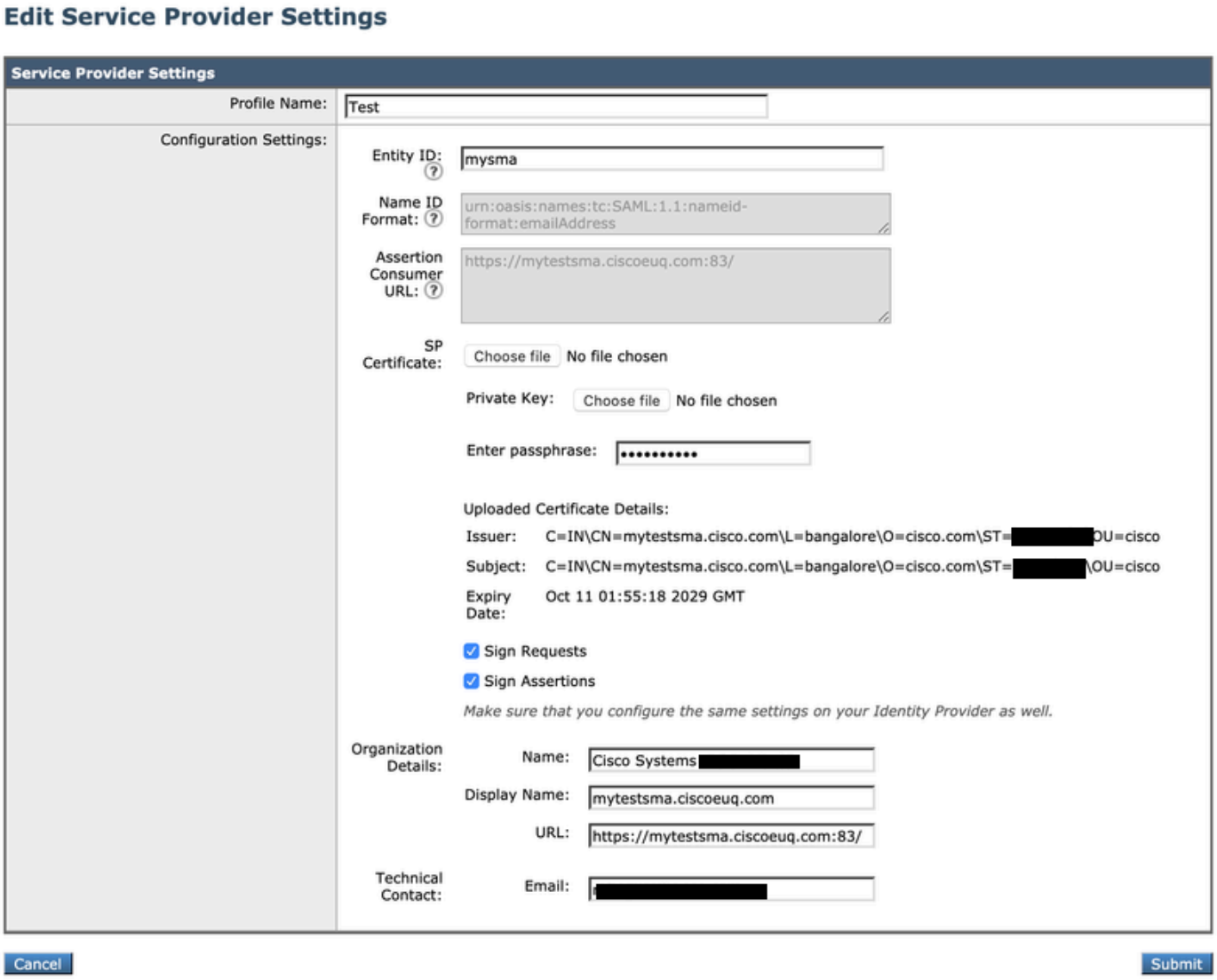
コンフィギュレーション

SMAアプライアンスでのサービスプロバイダー(SP)の設定

EUQアクセス用のSAMLサービスプロバイダーとしてSMAを設定するには、次の手順を実行します。

1. SMA Webインターフェイスにログインします。
2. System Administration > SAMLの順に移動します。
3. Add Service Providerを選択します。
4. 「サービスプロバイダーエンティティID」に、Oktaでも設定できるエンティティIDを入力します。
5. Name ID FormatとAssertion Consumer Service(ACS)URLがEUQインターフェイスに対して入力されていることを確認します。
6. SP Certificateで、証明書をアップロードしてSAML要求に署名します。

注:SMAは自己署名証明書を生成できません。ESAで証明書を生成し、SMAで使用するためにエクスポートすることもできます。



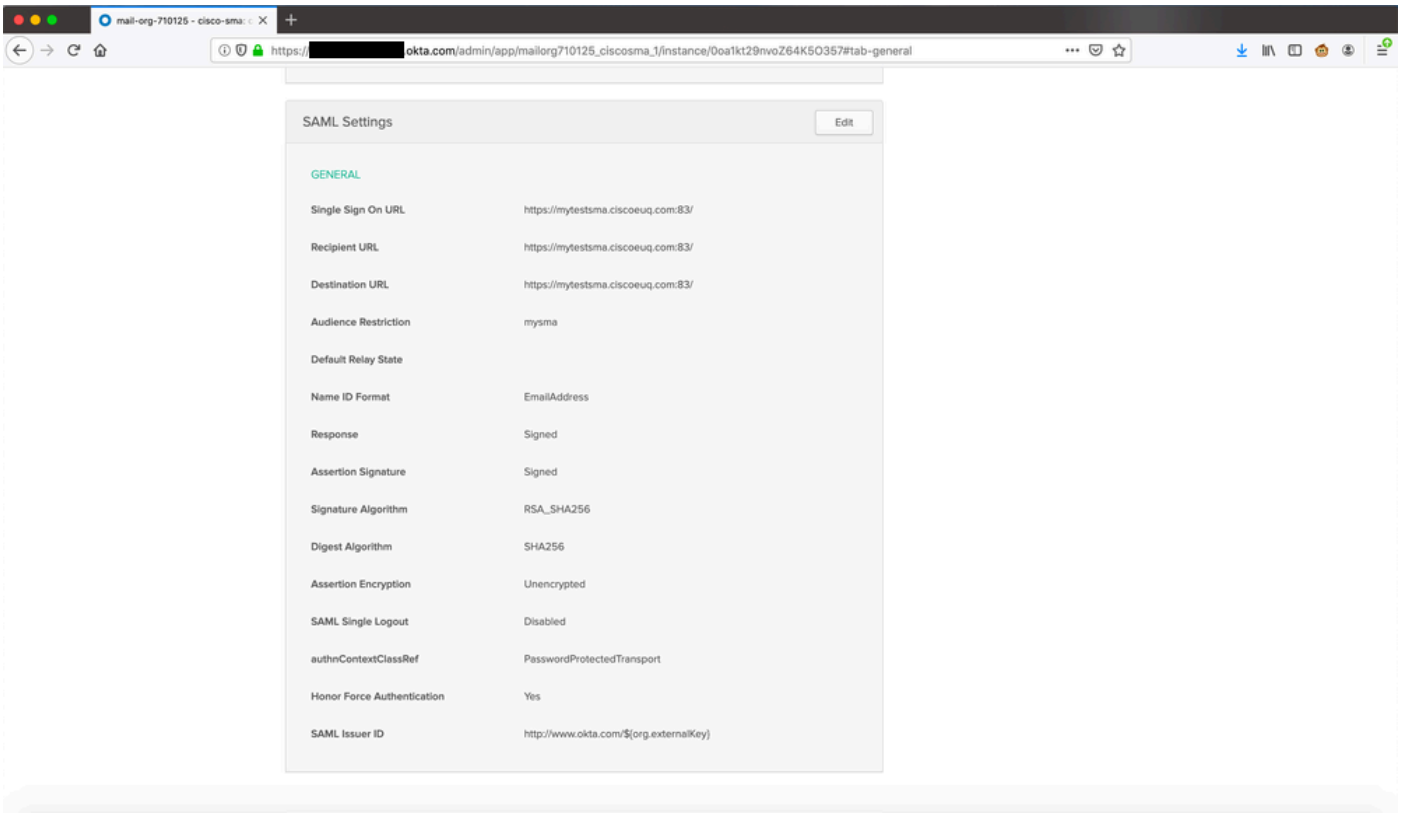
GUIでのサービスプロバイダーの設定

OktaでのSAMLアプリケーションの設定

SMA EUQアクセス用のSAML 2.0アプリケーションをOktaに作成するには、次の手順を実行します。

1. Oktaに管理者としてログインします。
2. Applications > Applicationsの順に移動し、Create App Integrationを選択します。
3. SAML 2.0を選択し、Nextを選択します。
4. アプリケーション名(例：SMA EUQ)を入力し、Nextを選択します。
5. 「シングルサインオンURL」で、SMAサービスプロバイダーの設定からSMA ACS URLを入力します。
6. [対象ユーザーURI（SPエンティティID）]で、SMAで構成されているのと同じエンティティIDを入力します。
7. Name ID formatには、EmailAddressを選択します。
8. アプリケーションユーザ名には、使用する環境に適したOktaユーザ名の形式を選択します。
9. ウィザードを完了してから、新しいアプリケーションを開き、IdPメタデータXMLファイル

またはメタデータURLをコピーします。

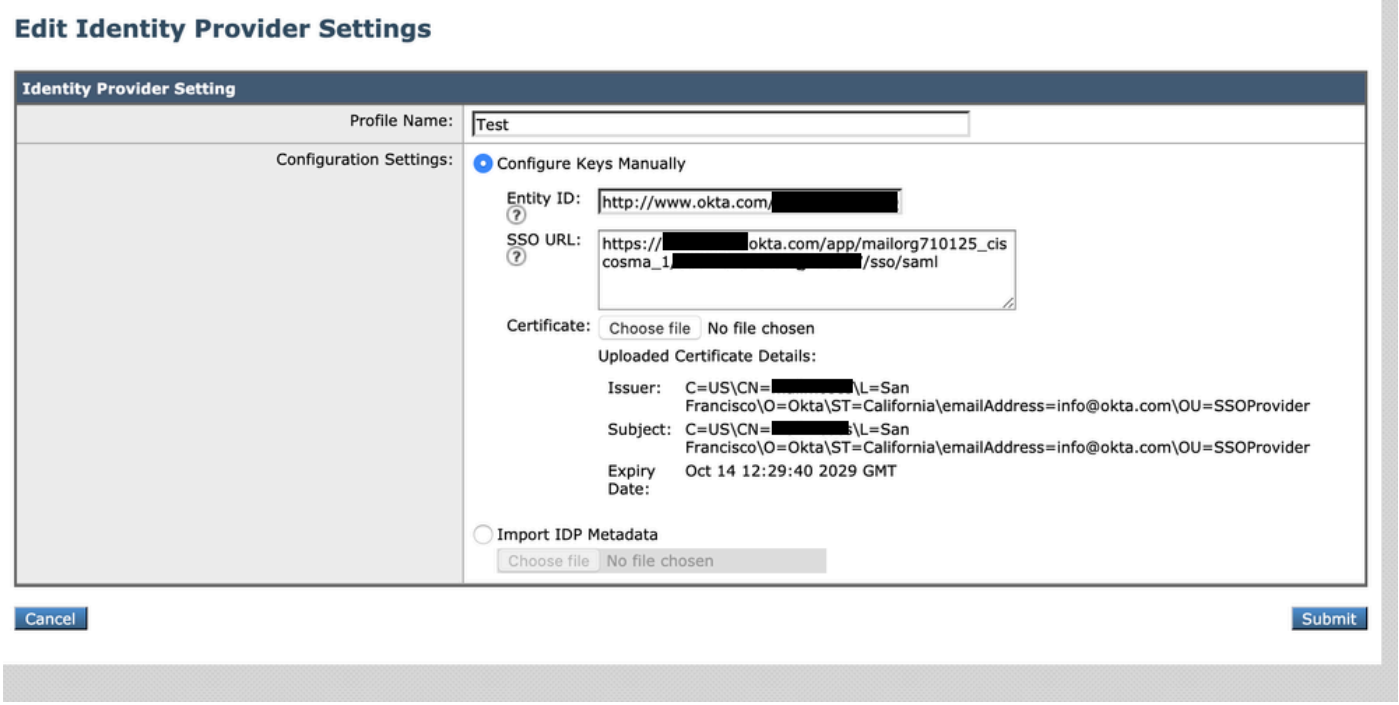


Oktaポータルの表示

SMAアプライアンスでのアイデンティティプロバイダー(IdP)の設定

SMAでIDプロバイダー(IdP)としてOktaを設定するには、次の手順を実行します。

1. SMA Webインターフェイスにログインします。
2. System Administration > SAMLの順に移動します。
3. Identity Provider Settingsで、前のセクションのOkta IdPメタデータをインポートするか、値を手動で入力します。

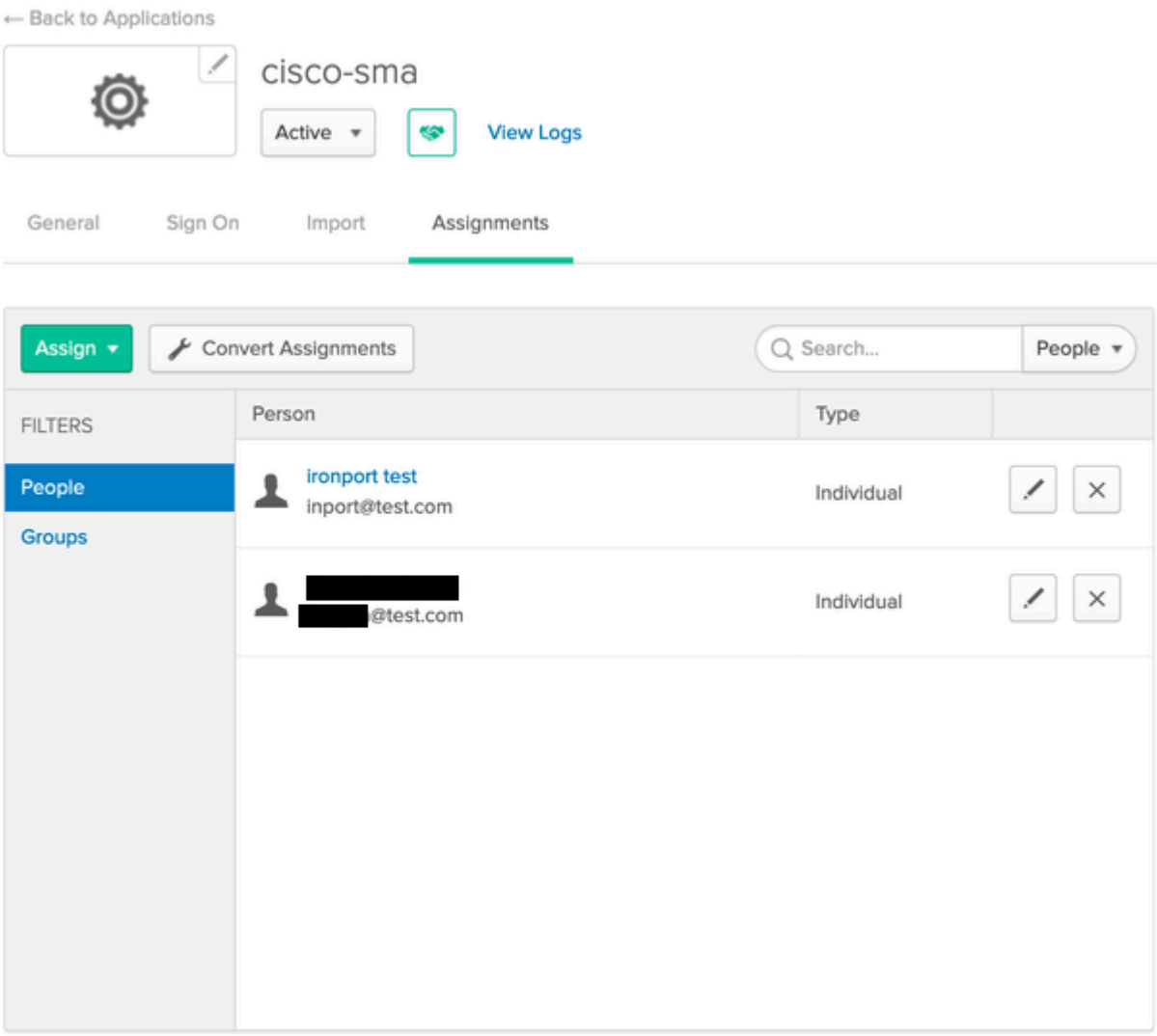


SMA GUIでのIdPプロファイルの設定

Oktaアプリケーションへのユーザの割り当て

ユーザがOktaを介してSMA EUQで認証できるようにするには、Oktaアプリケーションにユーザまたはグループを割り当てます。

1. Oktaで、作成したアプリケーションを開きます。
2. Assignments > Peopleの順に移動し、Assignを選択します。
3. 各ユーザの横にあるAssignを選択し、Doneを選択します。



Oktaポータルでのユーザの割り当て

注：ユーザーを手動で割り当てたり、Active Directoryからユーザーを同期したり、Oktaがサポートする別のディレクトリ統合を使用したりできます。

OktaでのMFAの設定（オプション）

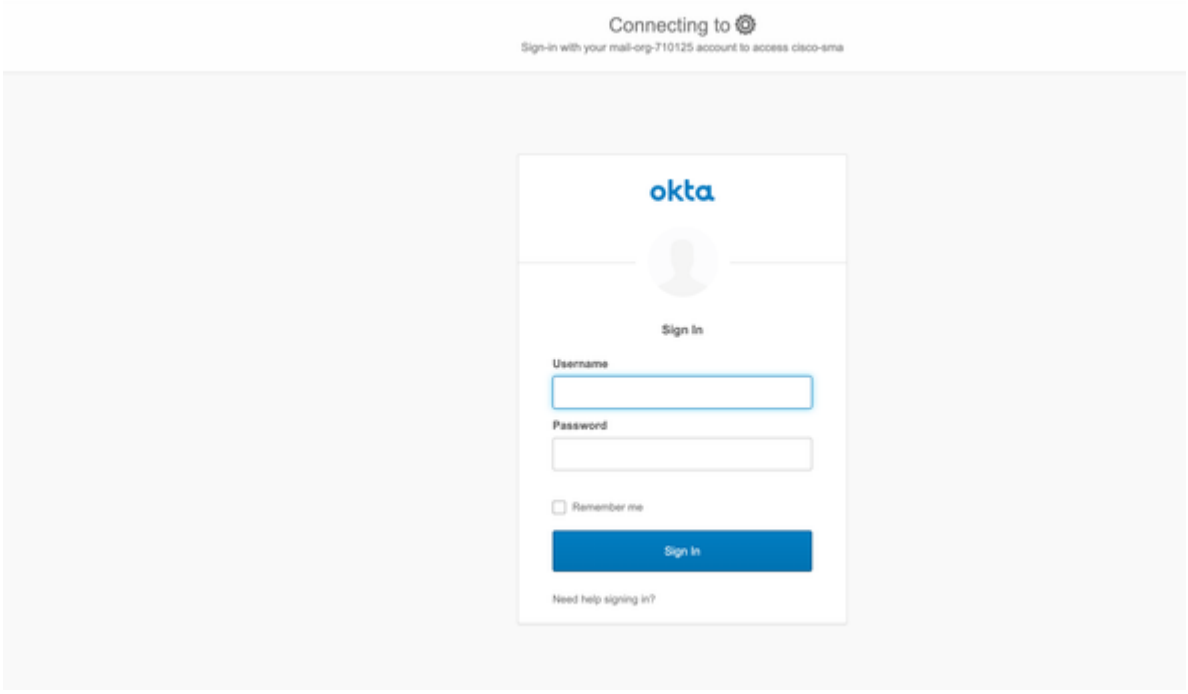
EUQアクセス用の多要素認証(MFA)が必要な場合は、Oktaでアプリケーション用にMFAポリシーを設定します。

1. Okta Adminで、Security > Authenticationに移動します。
2. 必要な要因（Okta Verify、Google Authenticator、SMSなど）を設定し、ポリシーをSMA EUQアプリケーションに適用します。

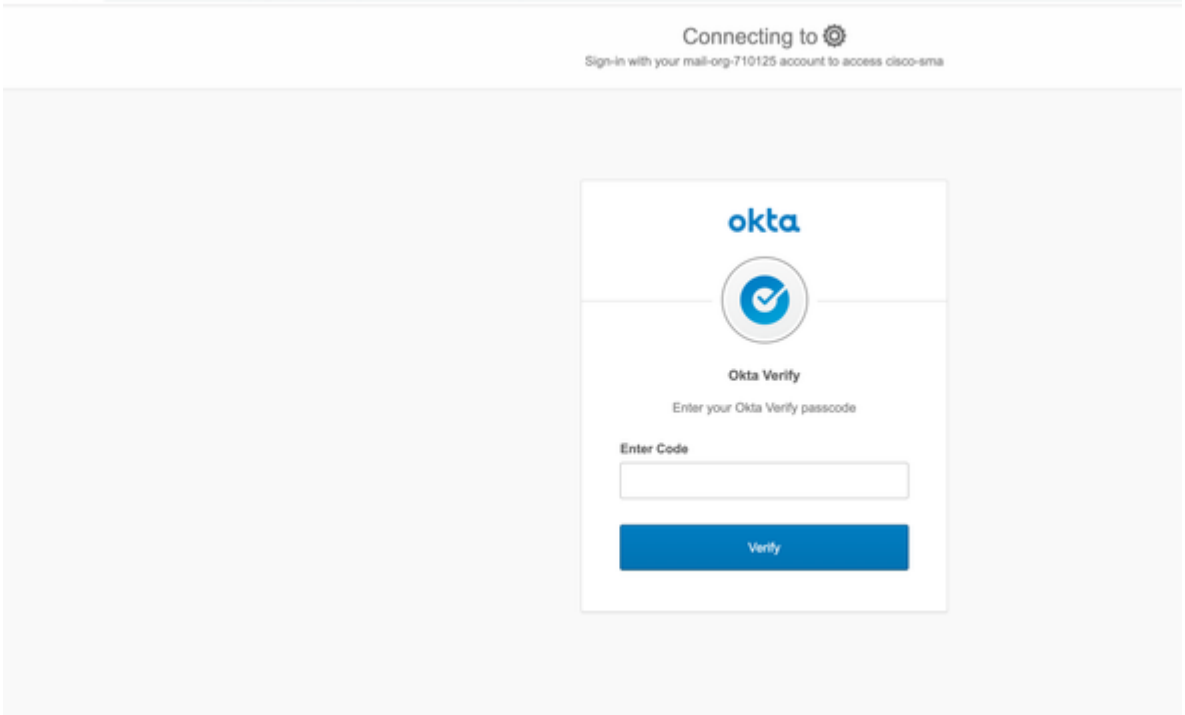
SAMLログインの確認

予想される結果：設定を確認するには、次の手順を実行します。

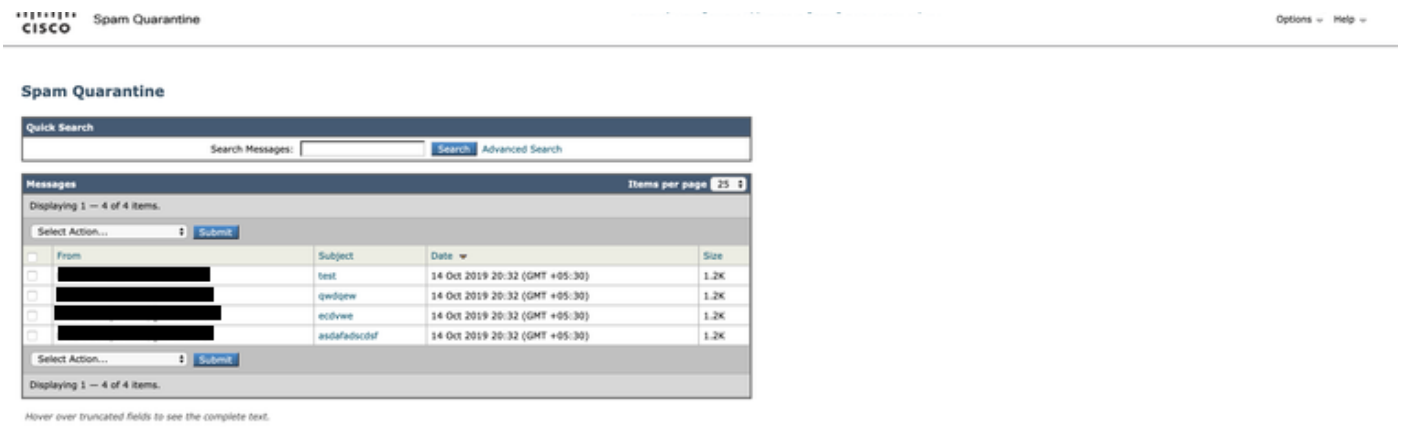
1. SMA EUQ URL(https://<sma-fqdn>:<port>/など)を参照します。
2. ブラウザが認証のためにOktaにリダイレクトされることを確認します。
3. MFAが有効になっている場合は、MFA challengeを実行します。
4. SMAスパム検疫ポータルにリダイレクトされ、検疫機能にアクセスできることを確認します。



Oktaを使用したログイン



Okta検証のコードを入力



Oktaでログインした後のスパム隔離の表示

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。