エンドユーザのスパム隔離のためのOKTA SSOの設定

内容

概要

このドキュメントでは、セキュリティ管理アプライアンス(SMA)のエンドユーザのスパム隔離にログインするためのOKTA SSOの設定方法について説明します。

前提条件

- Ciscoセキュリティ管理アプライアンスへの管理者アクセス。
- OKTAへの管理者アクセス。
- 自己署名またはCA署名（オプション）PKCS #12またはPEM形式のX.509 SSL証明書（OKTAから提供）。

背景説明

Ciscoセキュリティ管理アプライアンスは、エンドユーザのスパム検疫を使用するエンドユーザに対してSSOログインを可能にし、アプリケーションに認証および許可サービスを提供するアイデンティティマネージャであるOKTAと統合します。Cisco End User Spam Quarantineは、OKTAに接続して認証と許可を行うアプリケーションとして設定できます。また、SAMLを使用します。SAMLは、XMLベースのオープンスタンダードデータ形式で、管理者がアプリケーションのいずれかにサインインした後、定義された一連のアプリケーションにシームレスにアクセスできるようにします。

SAMLの詳細については、「SAMLの一般情報」を参照してください。

コンポーネント

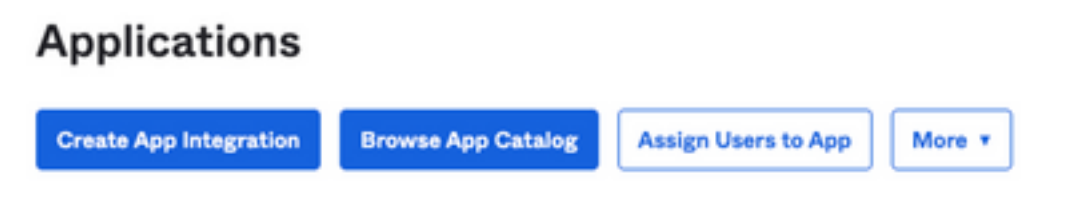
- Ciscoセキュリティ管理アプライアンス(SMA)クラウド管理者アカウント。
- OKTA管理者アカウント。

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ました。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（デフォルト）設定で開始されています。ネットワークが稼働中の場合は、コマンドによる潜在的な影響を十分に理解しておく必要があります。

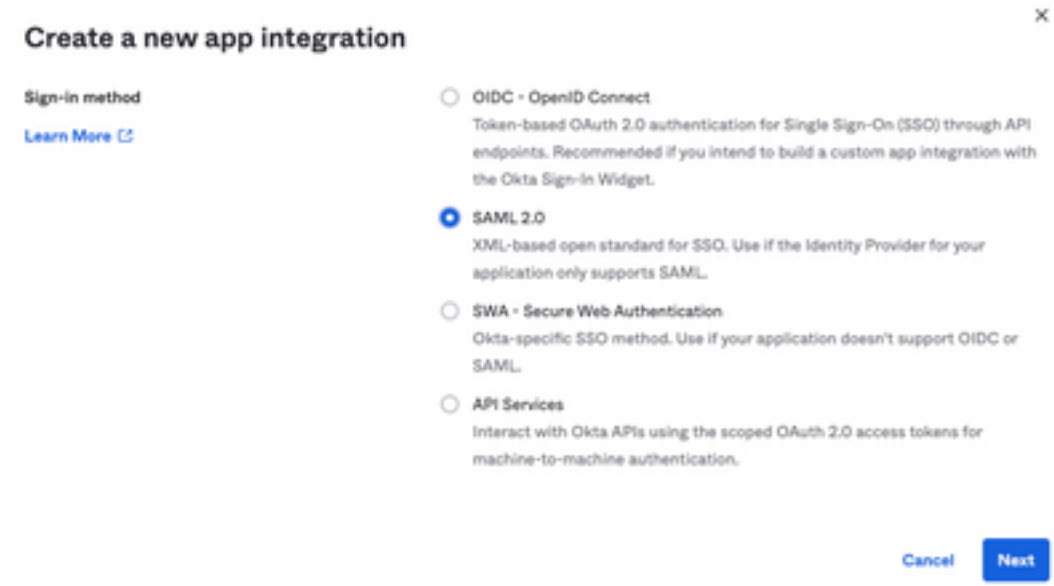
設定

オクタの下で。

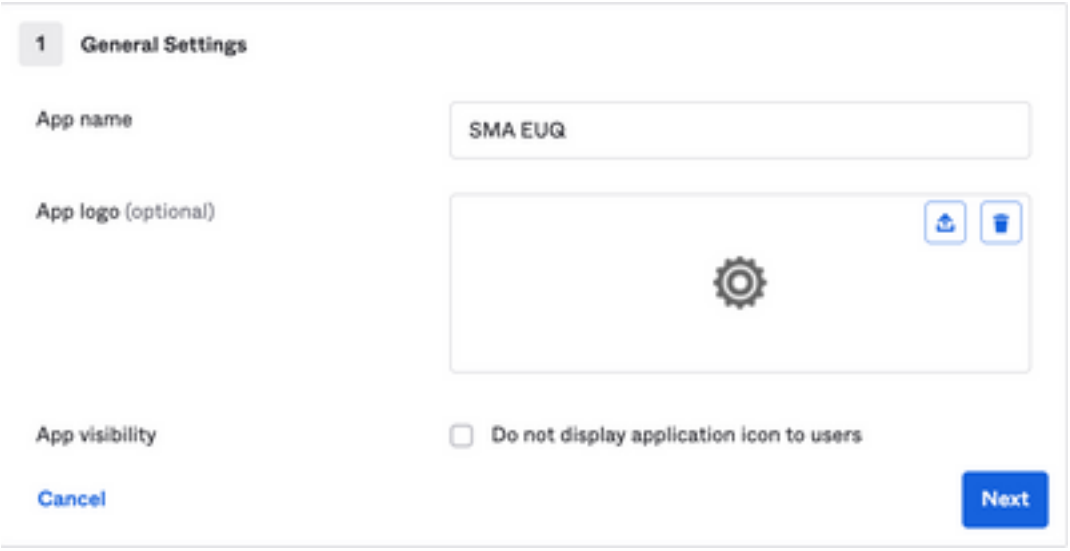
1. [Applications]ポータルに移動し、 Create App Integration （ 図を参照 ）。



2.選択 SAML 2.0 をアプリケーションタイプとして使用します（ 図を参照 ）。



3.アプリ名を入力します SMA EUQ を選択し、 Next（ 図を参照 ）。



4. SAML settingsをクリックして、図に示すようにギャップを埋めます。

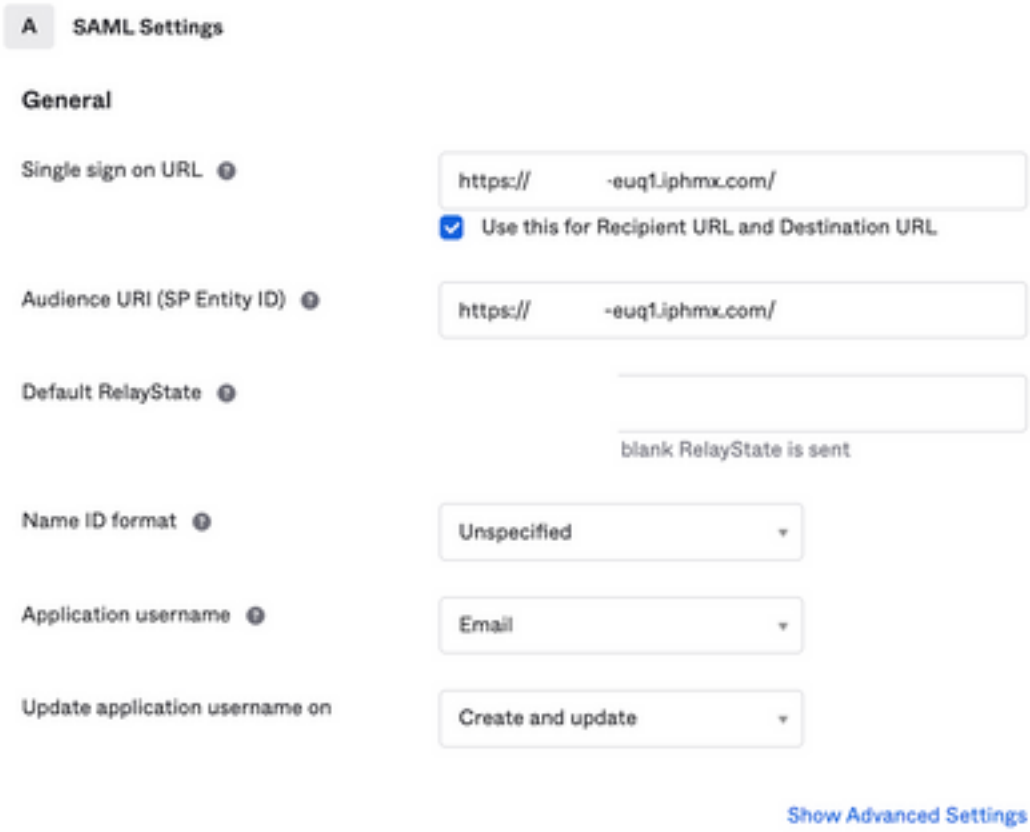
– シングルサインオンURL：これはSMA EUQインターフェイスから取得したアサーションコンシューマサービスです。

- Audience URI (SP Entity ID)：これはSMA EUQエンティティIDから取得したエンティティIDです。

– 名前IDの形式：未指定のままにしておきます。

– アプリケーションユーザ名：認証プロセスでユーザに電子メールアドレスの入力を求める電子メール。

– アプリケーションのユーザー名の更新：作成および更新。



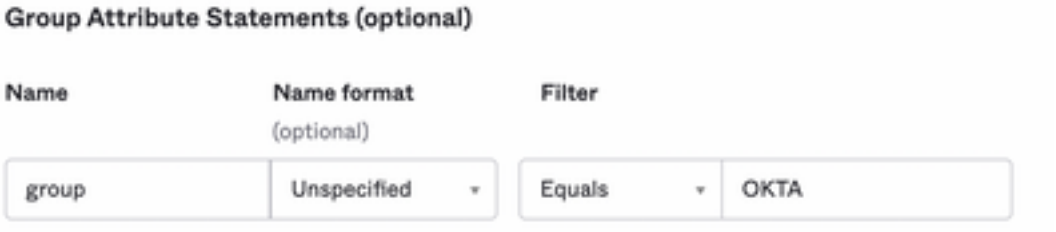
下にスクロールして Group Attibute Statements (optional) （図を参照）。

次の属性文を入力します。

-Name： group

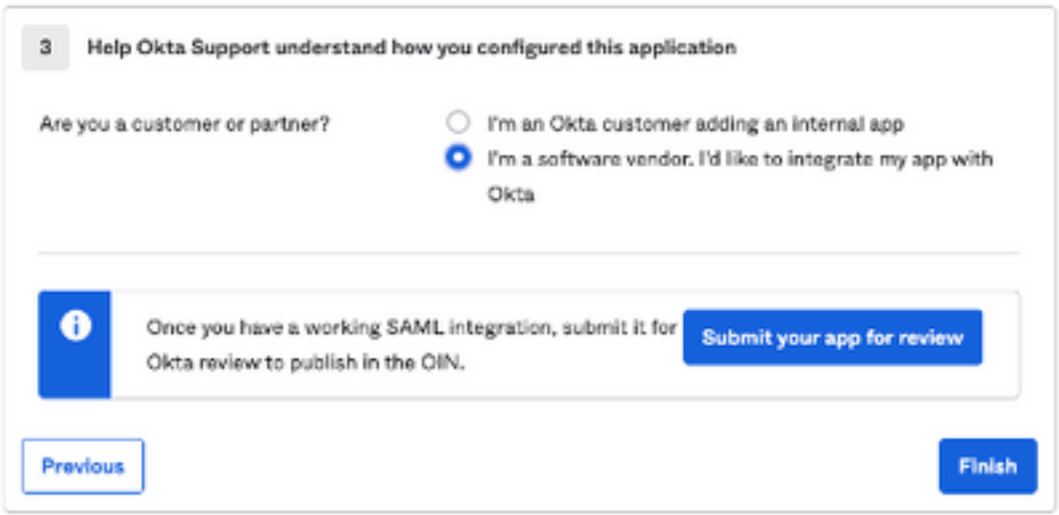
– 名前の形式： Unspecified

-フィルタ: Equals と OKTA



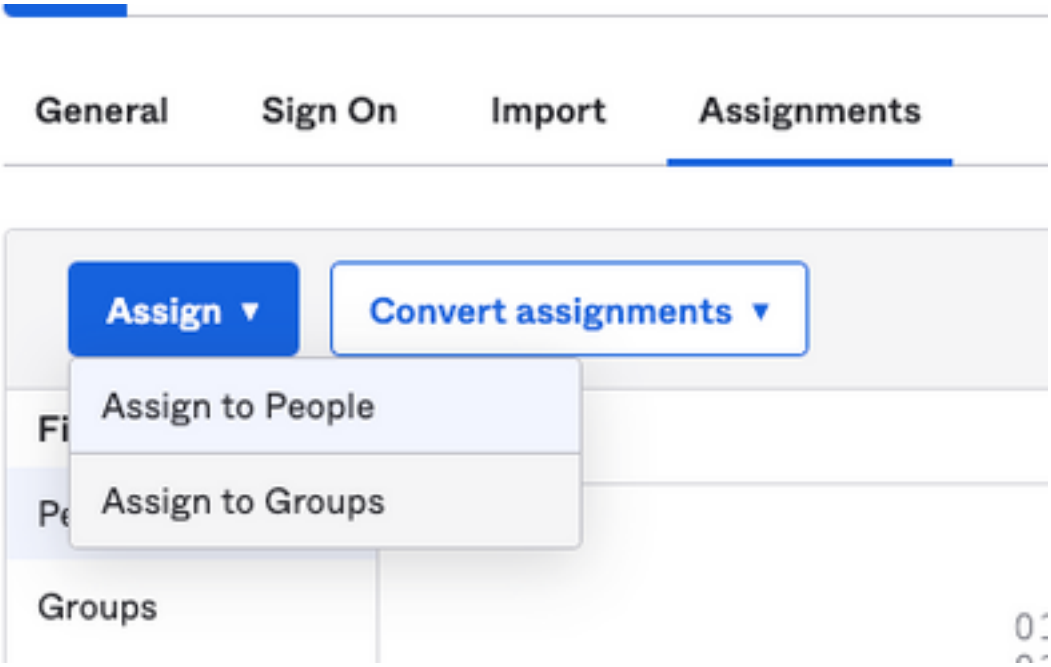
選択 Next .

5.依頼された場合 Help Okta to understand how you configured this applicationを選択した場合は、次の図に示すように、現在の環境に該当する理由を入力してください。



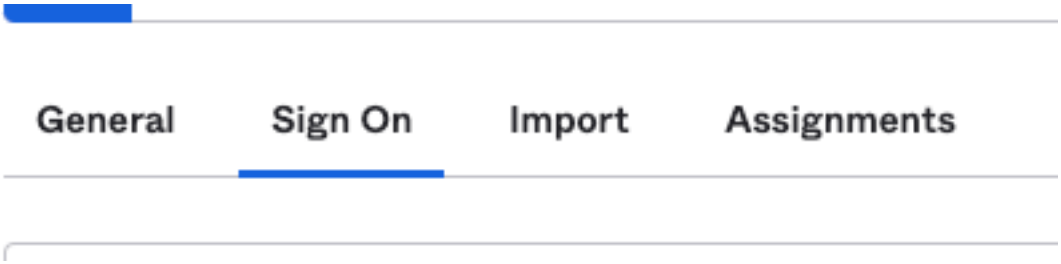
選択 Finish 次のステップに進みます。

6.選択 Assignments タブをクリックし、 Assign > Assign to Groups（ 図を参照 ）。



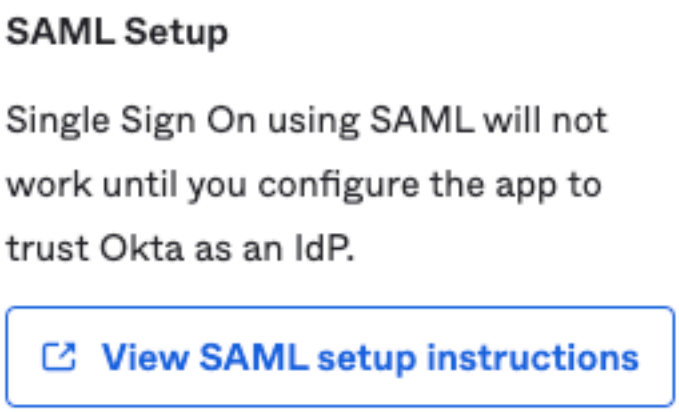
7. OKTAグループを選択します。このグループは、環境にアクセスする権限を持つユーザのグループです

8.選択 Sign On （ 図を参照 ）。



9.下にスクロールして右隅に移動し、 View SAML setup instructions オプションを選択します（ 図を参照

）。

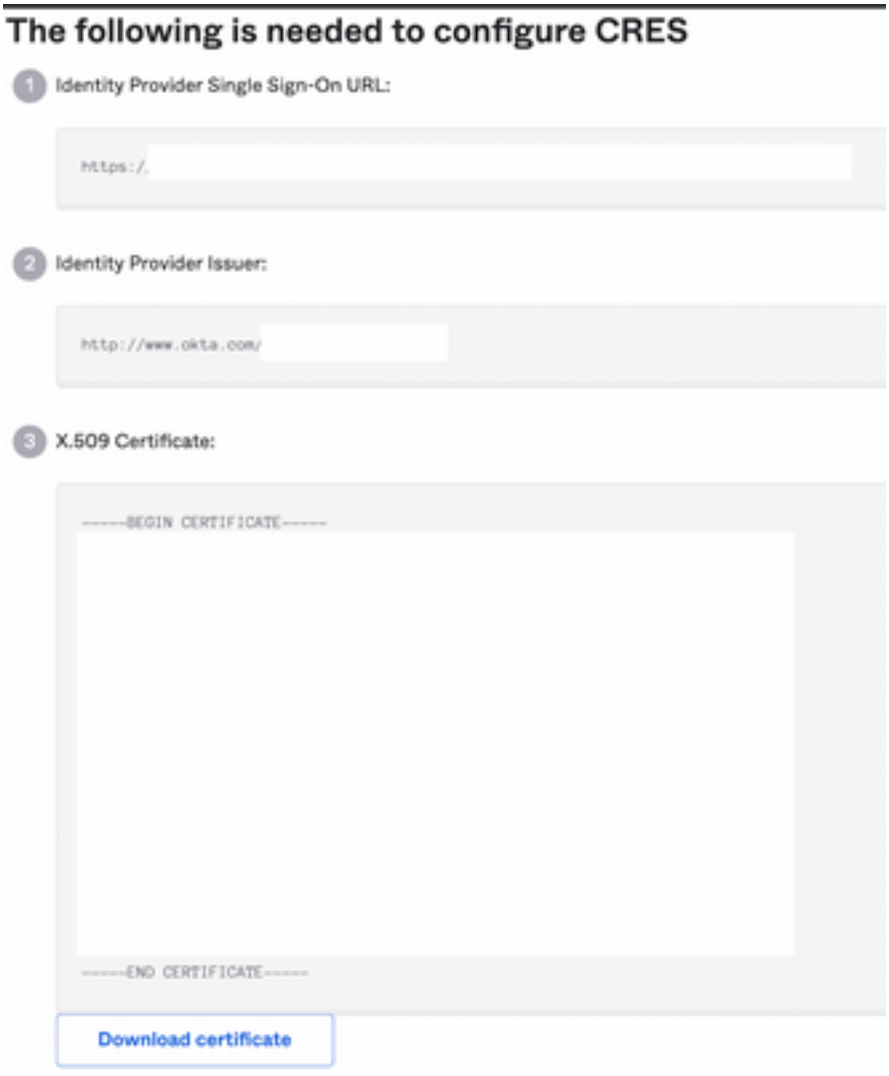


10.この情報をメモ帳に保存します。 Cisco Security Management Appliance 図に示すSAML設定：

– アイデンティティプロバイダーのシングルサインオンURL

– アイデンティティプロバイダー発行者

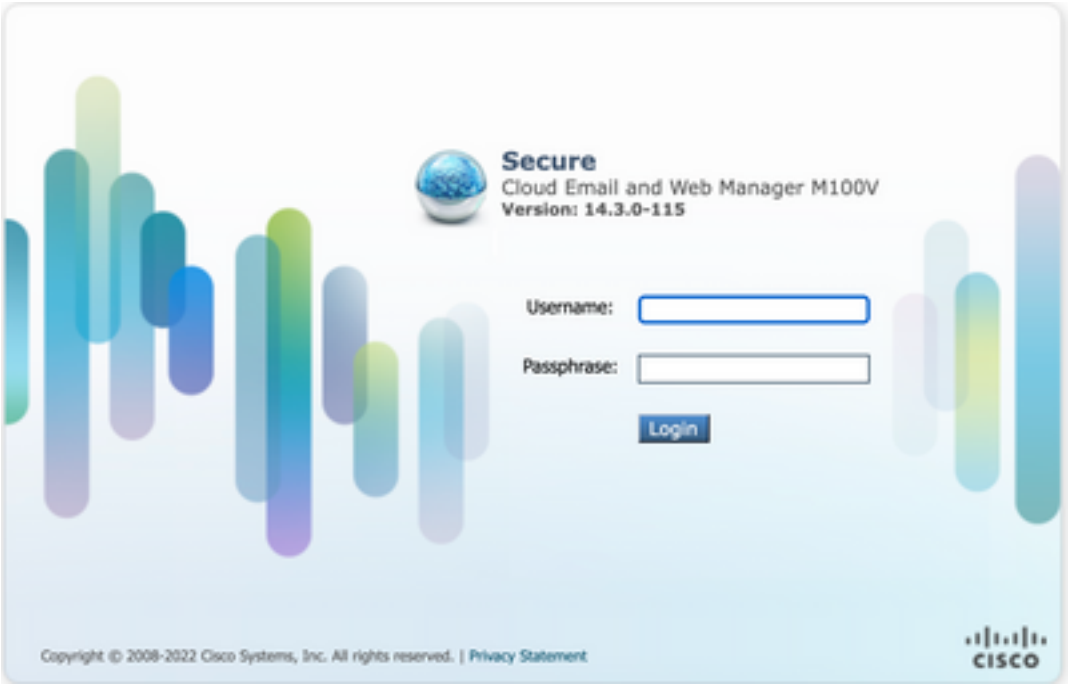
- X.509証明書



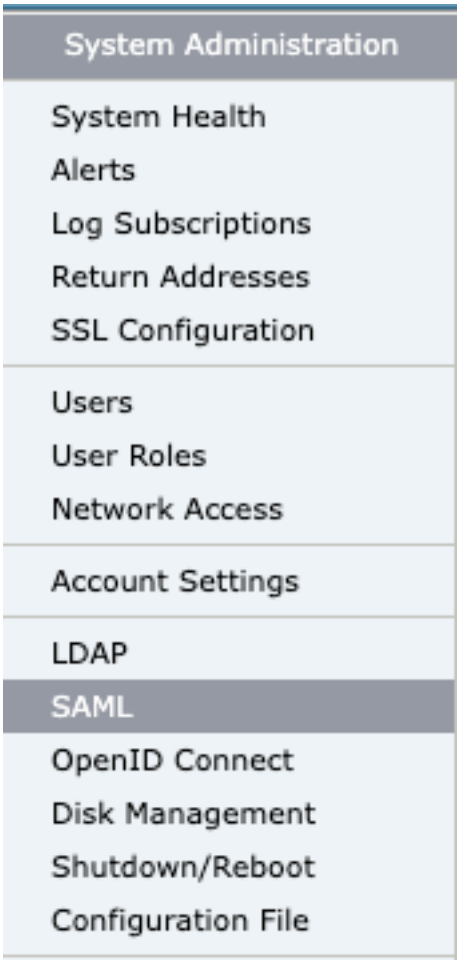
11. OKTAの設定が完了したら、Ciscoセキュリティ管理アプライアンスに戻ることができます。

Cisco Security Management Applianceで次の手順を実行します。

1.図に示すように、Cisco Security Management Applianceにクラウド管理者として**ログイン**します。

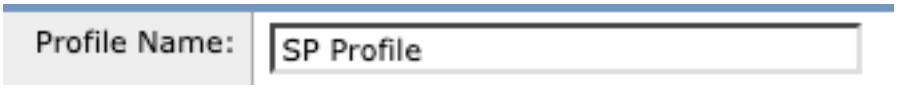


2. System Administrationタブを選択し、 SAML オプションを選択します（図を参照）。



3. SAMLを設定するための新しいウィンドウが開きます。通常の SAML for End-User Quarantine, クリック Add Service Provider （ 図を参照 ）。

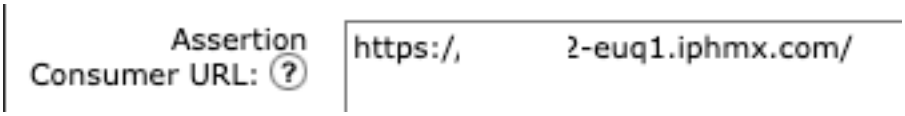
4.以下 Profile Name 次の図に示すように、サービスプロバイダープロファイルのプロファイル名を入力します。



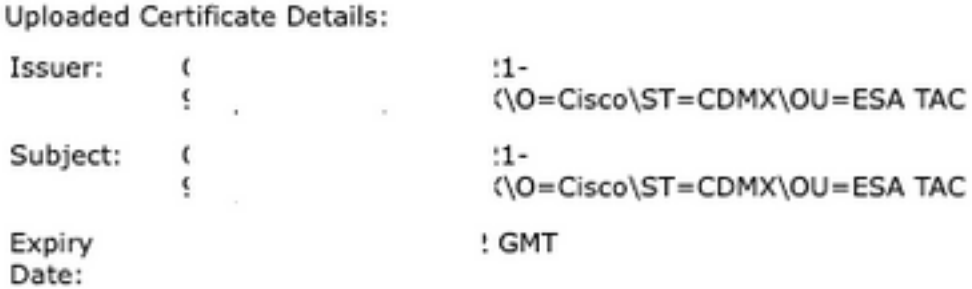
5.対象 Entity ID 、サービスプロバイダー（この場合はアプライアンス）のグローバルに一意な名前を入力します。図に示すように、サービスプロバイダーのエンティティIDの形式は通常URIです。

6.対象 **Name ID Format** このフィールドは設定できません。この値は、図に示すようにアイデンティティプロバイダを設定するときに必要です。

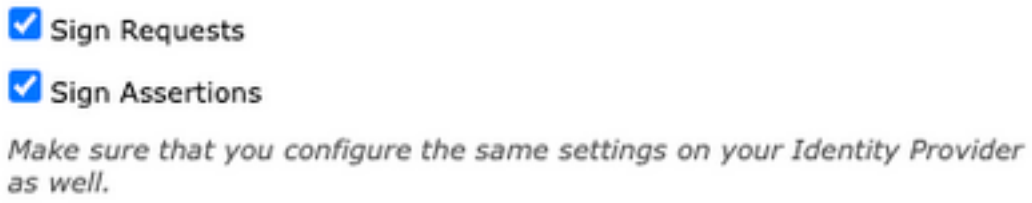
7.対象 **Assertion Consumer URL**認証が正常に完了した後、アイデンティティプロバイダーがSAMLアサーションを送信するURLを入力します。この場合、これはスパム検疫へのURLです。



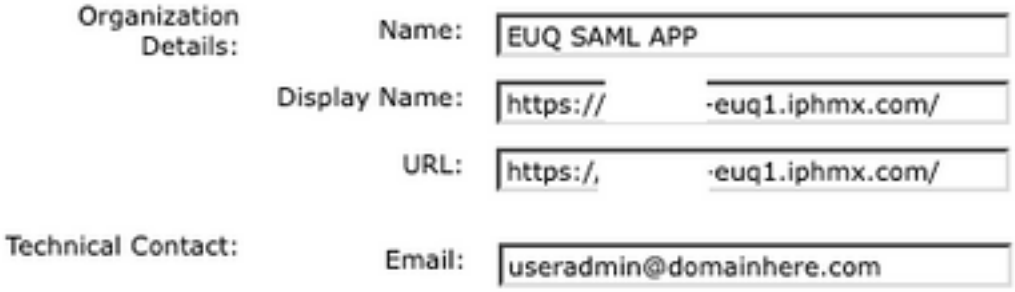
8.対象 SP Certificate 証明書とキーをアップロードするか、PKCS #12ファイルをアップロードします。アップロード後、 Uploaded Certificate Details 次の図のように表示されます。



9.対象 Sign Requests and Sign Assertions SAML要求とアサーションに署名する場合は、両方のチェックボックスをオンにします。[check these options]を選択した場合は、図に示すように、OKTAで同じ設定を構成していることを確認します。

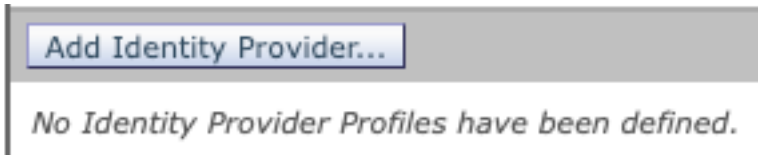


10.対象 Organization Detailsをクリックし、次の図に示すように、組織の詳細を入力します。



11．Submit と Commit 設定に進む前の変更 Identity Provider Settings．

12.下 SAML をクリックし、 Add Identity Provider（ 図を参照 ）。



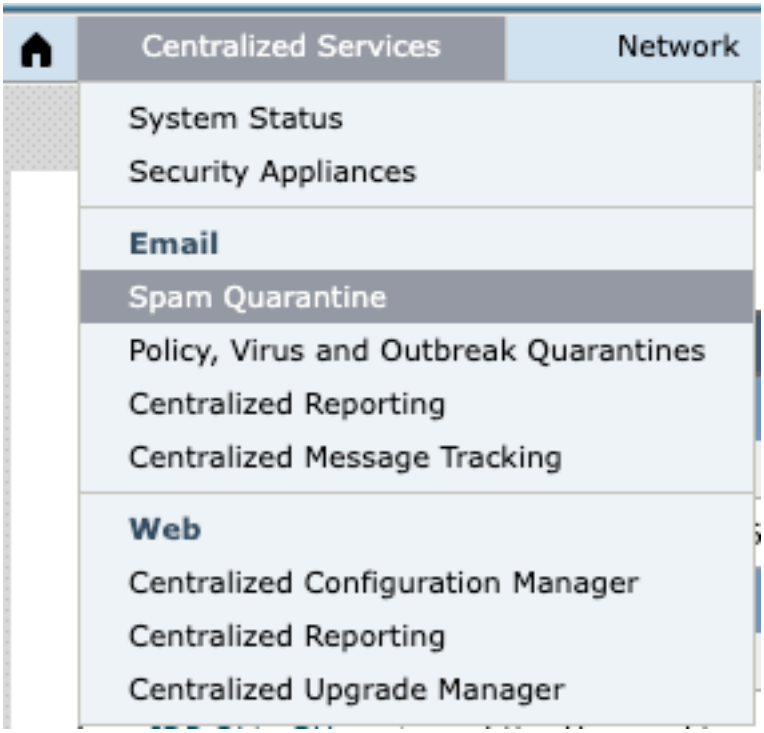
13未満 Profile Name: 次の図に示すように、アイデンティティプロバイダープロファイルの名前を入力します。

14.選択 Configure Keys Manually 次の図に示すように、次の情報を入力します。

- [エンティティID(Entity ID)]:アイデンティティプロバイダーを一意に識別するために、アイデンティティプロバイダーのエンティティIDが使用されます。これは、前の手順のOKTA設定から取得されます。
- [SSO URL]:SPがSAML認証要求を送信するURL。これは、前の手順のOKTA設定から取得されます。
- [証明書(Certificate)]:OKTAによって提供される証明書。

15 . Submit と Commit saml口グインアクティベーションに進むための変更。

16未満 Centralized Services > Email をクリックし、 Spam Quarantine (図を参照) 。



17アンダー Spam Quarantine -> Spam Quarantine Settings をクリックし、 Edit Settings , as shown in the image:

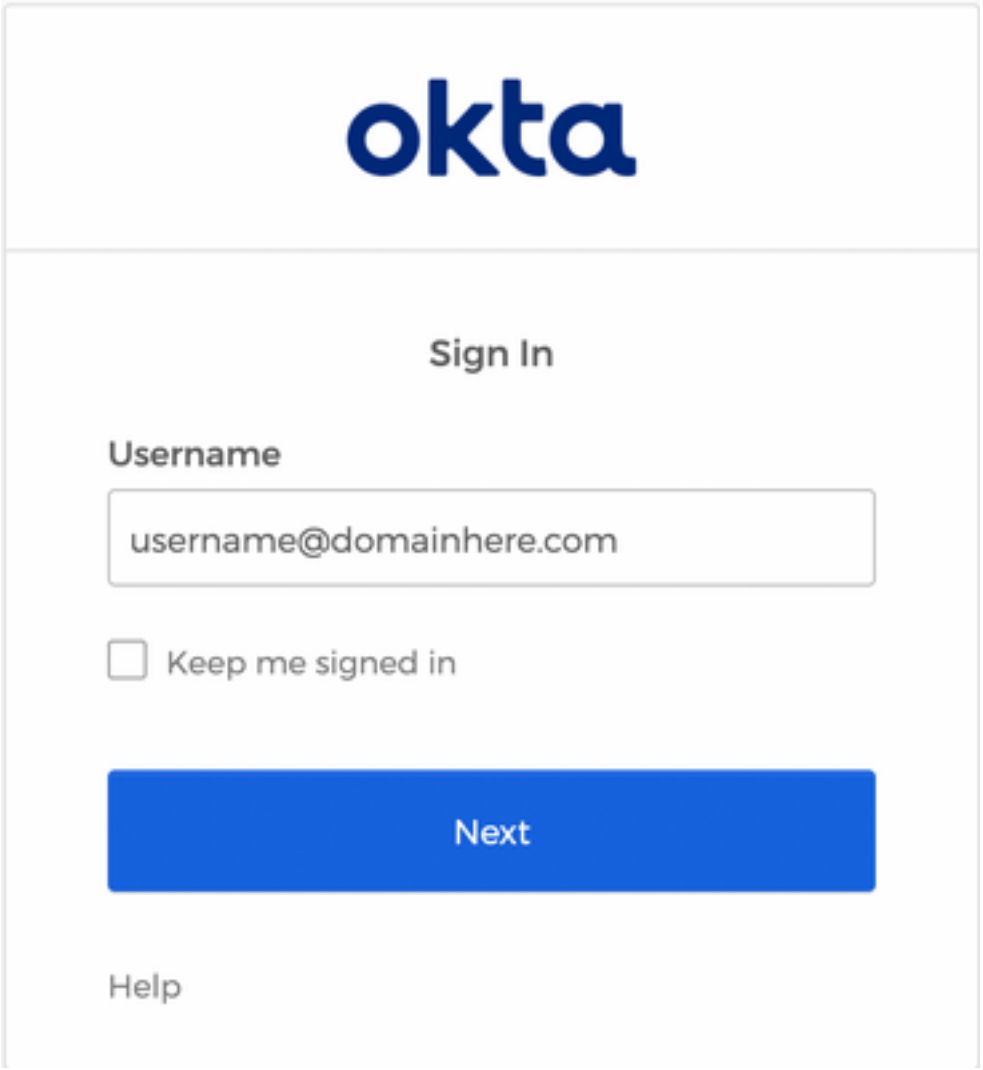
18.スクロールダウンして End-User Quarantine Access > End-User Authentication 、選択 SAML 2.0 (図を参照) 。

19 . Submit と Commit のSAML認証を有効にするための変更 **End User Spam Quarantine** .

確認

1.次の図に示すように、任意のWebブラウザで、会社のエンドユーザスパム検疫のURLを入力します。

2.新しいウィンドウが開き、OKTA認証に進みます。次の図に示すように、**OKTAクレデンシャル**でサインインします。



3.認証が成功した場合、 End User Spam Quarantine 次の図に示すように、ログインしたユーザのスパム検疫の内容を開きます。

これで、エンドユーザはOKTAクレデンシャルを使用してエンドユーザのスパム隔離にアクセスできます。.

関連情報

Cisco Secure Email and Web Managerエンドユーザガイド

OKTAサポート

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。