Auth0 社

概要

ここでは、Security Cloud Sign On と統合する Auth0 SAML アプリケーションを作成する方法について説明します。

はじめに

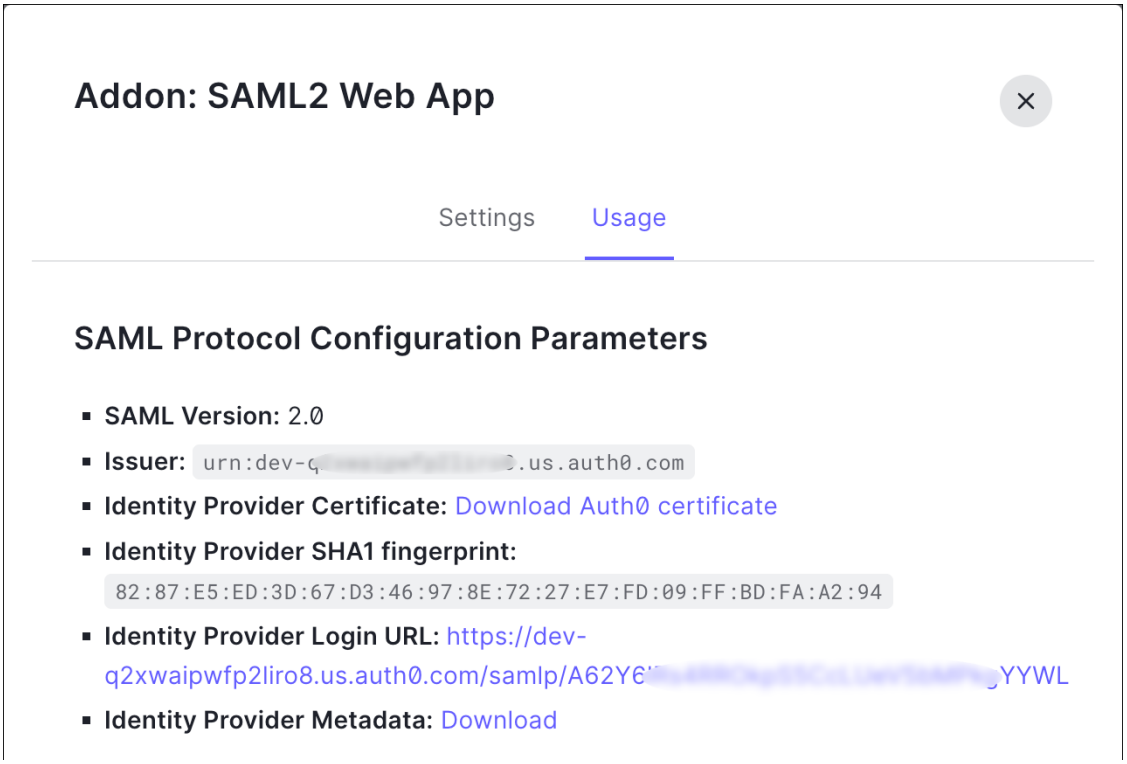
始める前に

- 管理者権限で Auth0 管理コンソールにサインインできる必要があります。
- ステップ 1：エンタープライズの作成 と ステップ 2：電子メールドメインの申請と検証 が完了している必要があります。

ステップ 1 Auth0 ダッシュボードにサインインし、次の手順を実行します。

a) [アプリケーション（Applications）] メニューから [アプリケーション（Applications）] を選択します。
b) [アプリケーションの作成（Create Application）] をクリックします。
c) [名前（Name）] フィールドに「**`Secure Cloud Sign On`**」または他の名前を入力します。
d) アプリケーションタイプとして [通常のWebアプリケーション（Regular Web Applications）] を選択し、[作成（Create）] をクリックします。
e) [アドオン（Addons）] タブをクリックします。
f) [SAML2 Web App（SAML2 Web App）] トグルをクリックしてアドオンを有効にします。

SAML2 Web App の構成ダイアログが開きます。



g) [発行元（Issuer）] フィールドと [IDプロバイダーログインURL（Identity Provider Login URL）] フィールドの値をコピーします。

h) [Auth0証明書のダウンロード（Download Auth0 certificate）] をクリックして ID プロバイダー証明書をダウンロードします。

ステップ 2 エンタープライズ設定ウィザードの [IDプロバイダーの統合（Integrate Identity Provider）] 画面を開き、次の手順を実行します。

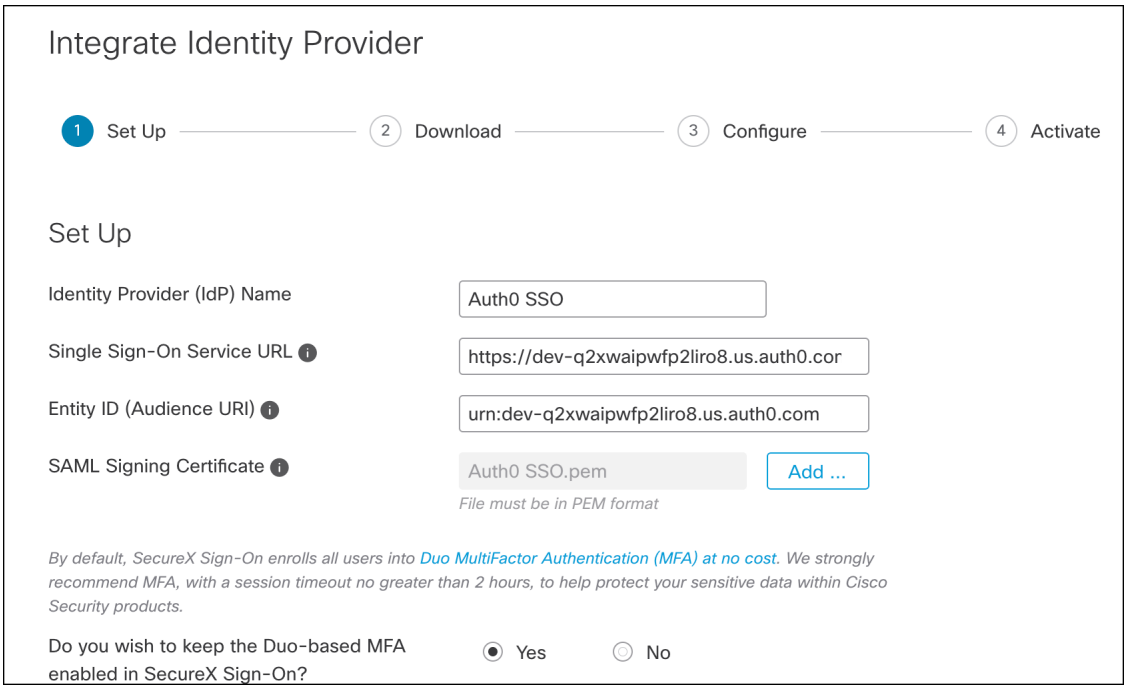
a) [IDプロバイダー名（Identity Provider Name）] フィールドに IdP の名前（例：**Auth0 SSO**）を入力します。

b) [シングルサインオンサービスURL（Single Sign On Service URL）] フィールドに、SAML アドオンダイアログからコピーした [IDプロバイダーログインURL（Identity Provider Login URL）] の値を入力します。

c) [エンティティID（Entity ID）] フィールドに、SAML アドオンダイアログからコピーした [発行元（Issuer）] フィールドの値を入力します。

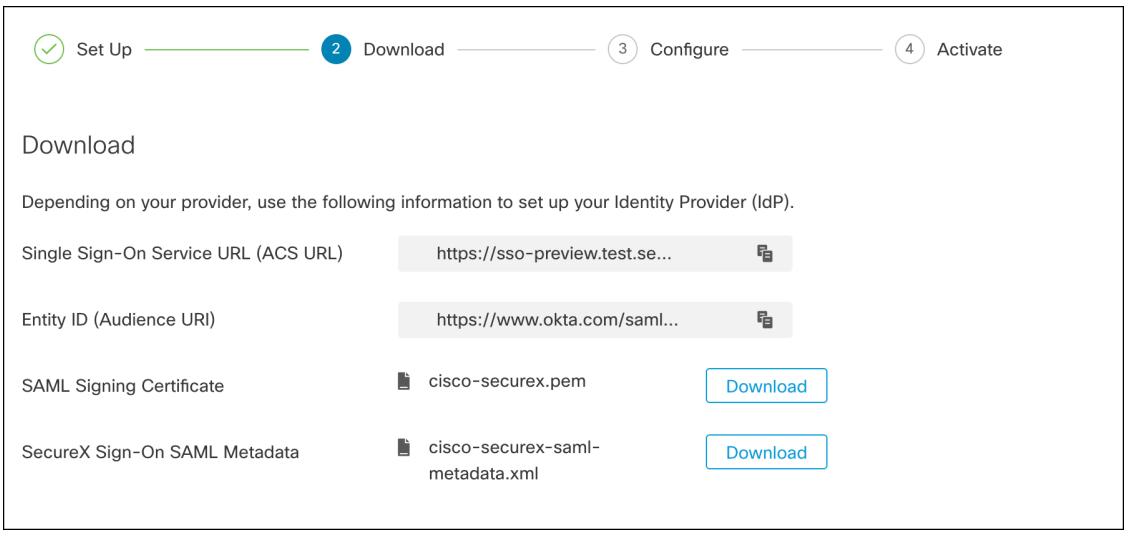
d) [ファイルの追加（Add File）] をクリックし、Auth0 からダウンロードした SAML 署名証明書を選択します。

e) 必要に応じて、Duo ベースの無料の MFA サービスからユーザーをオプトアウトします。



f) [次へ（Next）] をクリックして [ダウンロード（Download）] 設定ページに進みます。

g) 後で使用するために [シングルサインオンサービスURL（Single Sign-On Service URL）] と [エンティティID（Entity ID）] の値をコピーし、SAML 署名証明書（cisco-securex.pem）をダウンロードします。



h) [次へ（Next）] をクリックして [構成（Configure）] 画面に進みます。

ステップ 3 Auth0 コンソールのアドオン設定ダイアログに戻ります。

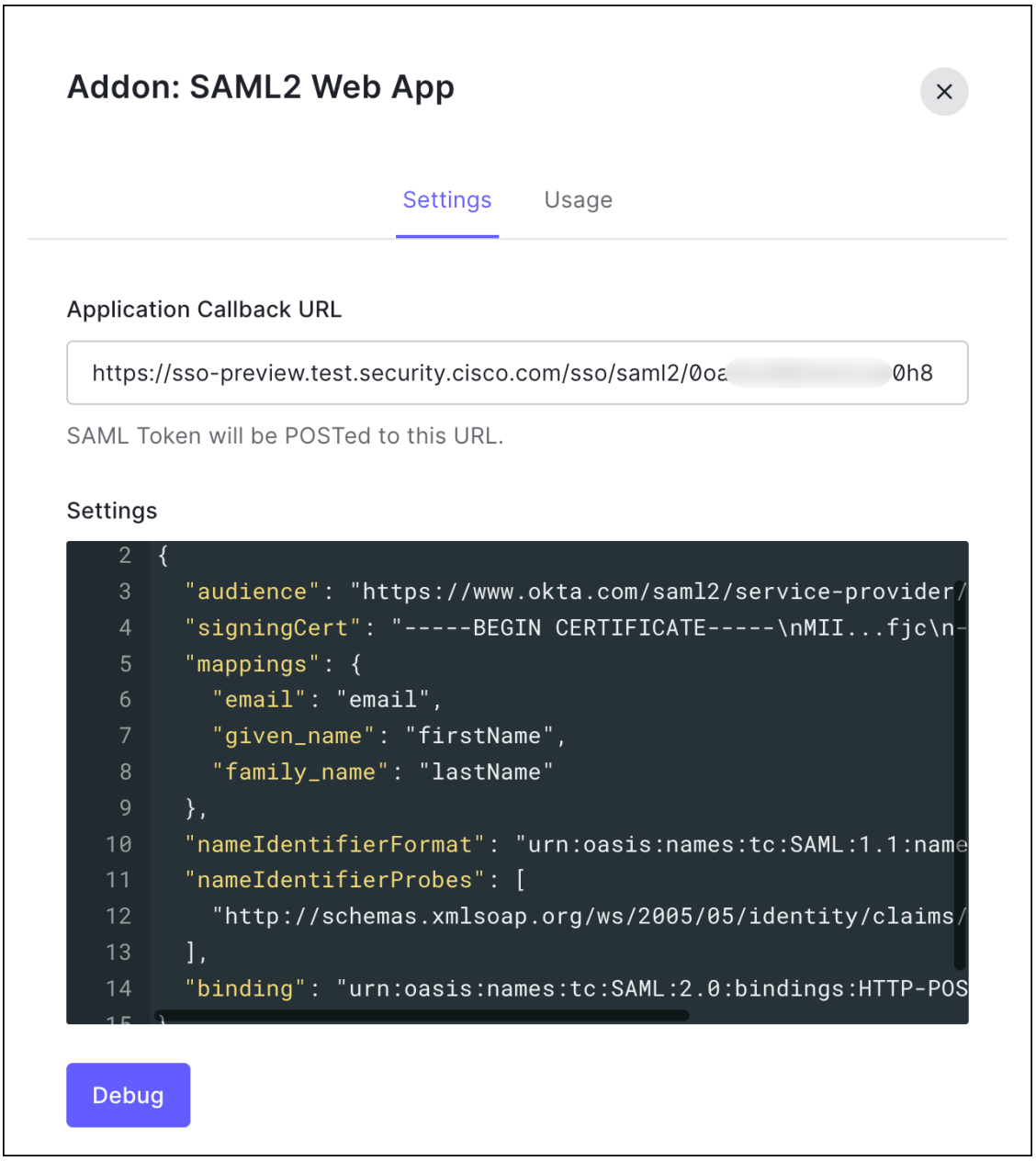
a) [設定（Settings）] タブをクリックします。

b) [アプリケーションコールバックURL（Application Callback URL）] フィールドに、エンタープライズ設定ウィザードからコピーした [シングルサインオンサービスURL（Single Sign-On Service URL）] の値を入力します。

c) 必要に応じて、[デバッグ（Debug）] をクリックしてサンプル SAML 応答の構造と内容を確認します（応答をデバッグするには、Auth0 ユーザーを SAML アプリケーションに割り当てる必要があります）。

d) [設定（Settings）] フィールドに次の JSON オブジェクトを入力します。<ENTITY_ID_URI> を、前にコピーした [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] の値に置き換え、<SIGNING_CERT> を、ダウンロードした SecureX Sign On 署名証明書（PEM ファイル）を 1 行の文字列に変換した内容に置き換えます。

```
{
  "audience": "https://www.okta.com/saml2/...",
  "signingCert": "-----BEGIN CERTIFICATE-----\n...-----END CERTIFICATE-----\n",
  "mappings": {
    "email": "email",
    "given_name": "firstName",
    "family_name": "lastName"
  },
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  ],
  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
}
```



e) ダイアログの下部にある [有効化（Enable）] をクリックして SAML アプリケーションを有効にします。

ステップ 4 エンタープライズ設定ウィザードの [構成（Configure）] 画面に戻ります。

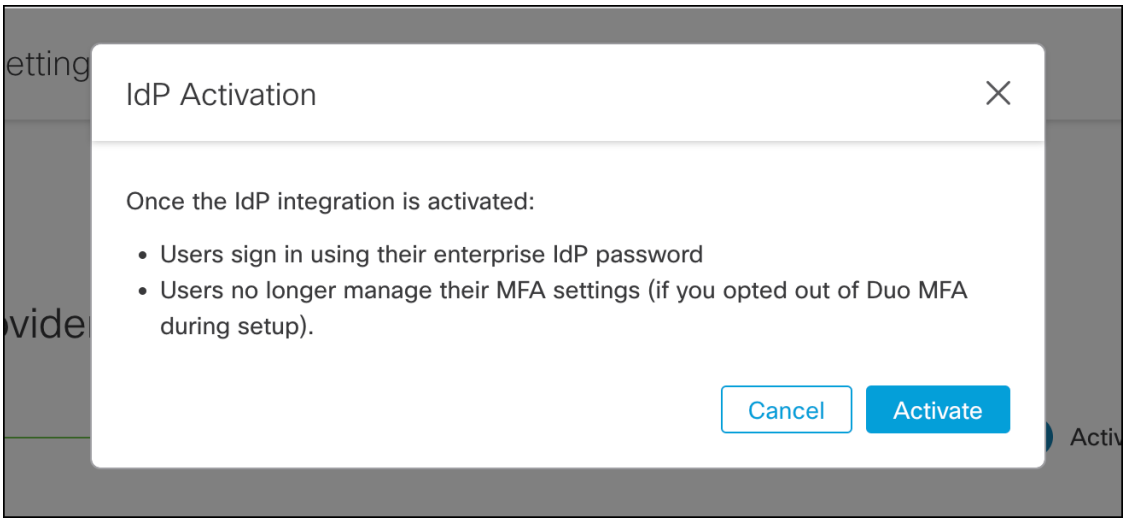
a) 表示された URL をコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。
ブラウザが Auth0 SSO ページにリダイレクトされます。

b) 申請したドメインと一致する電子メールアドレスで Auth0 にサインインします。
SecureX アプリケーションポータルに戻れば、テストは成功です。

c) 設定ウィザードで [次へ（Next）] をクリックして [アクティブ化（Activate）] 画面に進みます。

d) ユーザーの統合をアクティブ化するには、[IdPをアクティブ化（Activate my IdP）] をクリックします。

e) ダイアログで選択内容を確認します。


IdP Activation
Once the IdP integration is activated:
Users sign in using their enterprise IdP password
Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).
Cancel
Activate

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。