



Okta

- [概要 \(1 ページ\)](#)
- [はじめに \(1 ページ\)](#)

概要

ここでは、Okta SAML アプリケーションを作成し、Security Cloud Sign On と統合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 Okta ダッシュボードにサインインできる必要があります。
- エンタープライズ設定ウィザードの [ステップ 1: エンタープライズの作成](#) と [ステップ 2: 電子メールアドレスの申請と検証](#) が完了している必要があります。

ステップ 1 Okta 管理コンソールにサインインして、次の手順を実行します。

- [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。
- [アプリケーション統合の作成 (Create App Integration)] をクリックします。
- [SAML 2.0 (SAML 2.0)] を選択し、[次へ (Next)] をクリックします。
- [全般設定 (General Settings)] タブで、統合の名前 (例: **Security Cloud Sign On**) を入力し、必要に応じてロゴをアップロードします。
- [Next] をクリックします。
- [SAML の設定 (Configure SAML)] タブを選択します。
- [シングルサインオン URL (Single sign on URL)] フィールドに一時的な値 (例: **https://example.com/sso**) を入力します。これは後で Security Cloud Sign On の実際の ACS URL に置き換えます。

- h) [オーディエンスURI (Audience URI)] フィールドに一時的な値 (例 : **https://example.com/audience**) を入力します。これは後で Security Cloud Sign On の実際のオーディエンス ID URI に置き換えます。
- i) [名前IDの形式 (Name ID Format)] で [指定なし (Unspecified)] または [EmailAddress (EmailAddress)] を選択します。
- j) [アプリケーションユーザー名 (Application username)] で [Oktaユーザー名 (Okta username)] を選択します。
- k) [属性ステートメント (オプション) (Attribute Statements (optional))] セクションで、次の属性マッピングを追加します。

[名前 (Name)] (SAML アサーション)	[値 (Value)] (Okta プロファイル)
email	user.email
firstName	user.firstName
lastName	user.email

図 1: 属性を追加する例

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="firstName"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.firstName"/> ▼	
<input type="text" value="lastName"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.lastName"/> ▼	✕
<input type="text" value="email"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.email"/> ▼	✕

- l) [Next] をクリックします。
- m) Okta にフィードバックを送信し、[完了 (Finish)] をクリックします。
- n) ユーザーのグループに [アプリケーションを割り当て](#) ます。
- o) [サインオン (Sign On)] タブを選択します。
- p) 下にスクロールして、[SAMLセットアップ手順を表示 (View SAML Setup Instructions)] をクリックします。

SAML Signing Certificates

[Generate new certificate](#)

Type	Created	Expires	Status	Actions
SHA-1	Today	Feb 2033	Inactive ⚠	Actions ▼
SHA-2	Today	Mar 2033	Active	Actions ▼

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

- q) 開いたページで [IDプロバイダーのシングルサインオンURL (Identity Provider Single Sign-On URL)] と [IDプロバイダー発行元 (Identity Provider Issuer)] をコピーし、X.509 証明書をダウンロードします。次に、エンタープライズ設定ウィザードで Security Cloud Sign On との SAML アプリケーションの統合を開始します。

ステップ 2 新しいブラウザタブでエンタープライズ設定ウィザードを開きます。 **ステップ 3 : SAML メタデータの交換** の画面が表示されます。

- a) [IDプロバイダー名 (Identity Provider Name)] フィールドに IdP の名前 (例 : **Okta 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、Okta からコピーした [IDプロバイダーのシングルサインオンURL (Identity Provider Single Sign-On 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、Okta からコピーした [IDプロバイダー発行元 (Identity Provider 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、Okta 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)] 画面に進みます。
- g) 次の手順で使用するために、[シングルサインオンサービスURL (ACS URL) (Single Sign-On Service URL (ACS URL))] フィールドと [エンティティID (オーディエンスURI) (Entity ID (Audience URI))] フィールドの値をコピーして保存します。
- h) 次の手順で使用するために、SAML 署名証明書 (cisco-securex.pem) をダウンロードします。

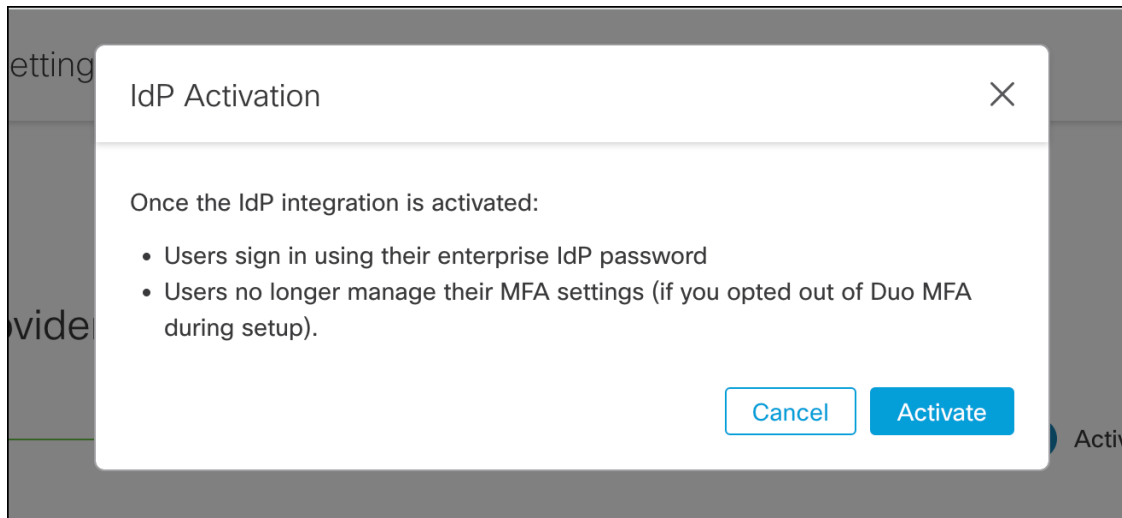
ステップ 3 Okta の SAML アプリケーション設定に戻ります。

- a) [全般 (General)] タブをクリックします。
- b) [SAML設定 (SAML Settings)] セクションで [編集 (Edit)] をクリックします。
- c) [次へ (Next)] をクリックします。
- d) [シングルサインオンURL (Single sign-on URL)] の値を、エンタープライズ設定ウィザードで提供された [シングルサインオンサービスURL (ACS URL) (Single Sign-On Service URL (ACS URL))] フィールドの値に置き換えます。
- e) [オーディエンスURI (SPエンティティID) (Audience URI (SP Entity ID))] の値を、エンタープライズ設定ウィザードで提供された [エンティティID (オーディエンスURI) (Entity ID (Audience URI))] フィールドの値に置き換えます。

- f) [詳細設定を表示 (Show Advanced Settings)] をクリックし、[署名証明書 (Signature Certificate)] フィールドを見つけます。
- g) [ファイルの参照 (Browse files)] をクリックし、前にダウンロードしたシスコの SAML 署名証明書を見つけます。
- h) [Next] をクリックします。
- i) [終了 (Finish)] をクリックして変更を保存します。

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 Okta SSO URL 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 Duo 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。



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。