



Duo

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

概要

ここでは、Duo SAML アプリケーションを作成し、それを 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

- 所有者ロールを持つ Duo 管理者である必要があります。
- Duo の [Duo管理 (Duo Admin)] > [シングルサインオン (Single Sign-On)] > [設定済み認証ソース (Configured Authentication Sources)] で、少なくとも 1 つの認証ソースがすでに設定されている必要があります。
- 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 Duo Admin Panel にサインインします。

- a) 左側のメニューから [アプリケーション (Applications)] をクリックし、[アプリケーションの保護 (Protect an Application)] をクリックします。
- b) [汎用SAMLサービスプロバイダー (Generic SAML Service Provider)] を探します。
- c) [保護タイプ (Protection Type)] が [DuoがホストするSSOによる2FA (2FA with SSO hosted by Duo)] の [汎用サービスプロバイダー (Generic Service Provider)] アプリケーションの横にある [保護 (Protect)] をクリックします。汎用 SAML サービスプロバイダーの構成ページが開きます。
- d) [メタデータ (Metadata)] セクションを選択します。
- e) [エンティティID (Entity ID)] の値をコピーし、後で使用するために保存します。

- f) [シングルサインオンURL (Single Sign-On URL)] の値をコピーし、後で使用するために保存します。
- g) [ダウンロード (Downloads)] セクションで [証明書のダウンロード (Download certificate)] をクリックします。
- h) [SAML応答 (SAML Response)] セクションで次の手順を実行します。
- [NameID形式 (NameID format)] で [urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified (urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified)] または [urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress (urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress)] を選択します。
 - [NameID属性 (NameID attribute)] で [<Email Address> (<Email Address>)] を選択します。
 - [属性のマッピング (Map Attributes)] セクションで、Duo IdP ユーザー属性から SAML 応答属性への次のマッピングを入力します。

[IdP属性 (IdP Attribute)]	[SAML応答属性 (SAML Response Attribute)]
<Email Address>	email
<First Name>	firstName
<Last Name>	lastName

Map attributes	IdP Attribute	SAML Response Attribute
	<input type="text" value="x <Email Address>"/>	<input type="text" value="email"/> <input type="button" value="−"/>
	<input type="text" value="x <First Name>"/>	<input type="text" value="firstName"/> <input type="button" value="−"/>
	<input type="text" value="x <Last Name>"/>	<input type="text" value="lastName"/> <input type="button" value="−"/> <input style="color: green;" type="button" value="+"/>

- i) [設定 (Settings)] セクションで、[名前 (Name)] フィールドに「**Secure Cloud Sign On**」または他の値を入力します。

Duo の SAML 設定のブラウザウィンドウは開いたままにします。

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。[IDプロバイダーの統合 (Integrate Identity Provider)] 画面の [セットアップ (Set Up)] ステップ ([ステップ 3 : SAML メタデータの交換](#) を参照) が表示されます。

- [IDプロバイダー名 (Identity Provider Name)] フィールドに IdP の名前 (例 : **Duo SSO**) を入力します。
- [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、Duo からコピーした [シングルサインオンURL (Single Sign-On URL)] の値を入力します。
- [エンティティID (Entity ID)] フィールドに、Duo からコピーした [エンティティID (Entity ID)] 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、Duo 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) 後で使用するために、[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) SAML 署名証明書 (cisco-securex.pem) をダウンロードします。

Download

Depending on your provider, use the following information to set up your Identity Provider (IdP).

Single Sign-On Service URL (ACS URL)	https://sso-preview.test.se...	
Entity ID (Audience URI)	https://www.okta.com/saml...	
SAML Signing Certificate	cisco-securex.pem	Download
SecureX Sign-On SAML Metadata	cisco-securex-saml-metadata.xml	Download

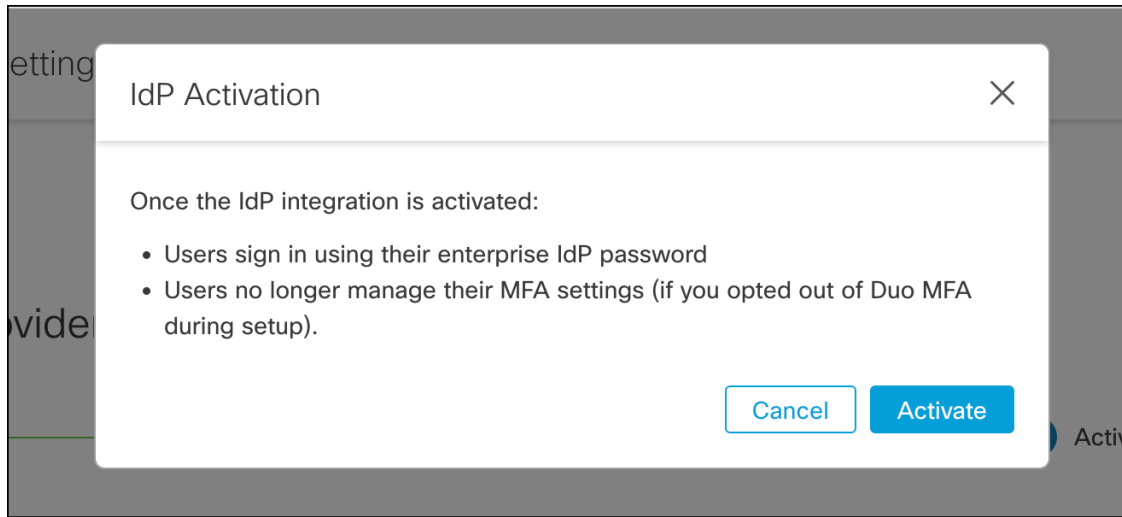
- i) [次へ (Next)] をクリックして [構成 (Configure)] 画面に進みます。

ステップ 3 Duo の SAML アプリケーション設定に戻り、次の手順を実行します。

- a) [サービスプロバイダー (Service Provider)] セクションの [エンティティ ID (Entity ID)] フィールドに、前の手順で設定ウィザードによって提供された [エンティティ ID (オーディエンス URI) (Entity ID (Audience URI))] フィールドの値を入力します。
- b) [Assertion Consumer Service (ACS) URL (Assertion Consumer Service (ACS) URL)] に、前の手順で設定ウィザードによって提供された [シングルサインオンサービス URL (ACS URL) (Single Sign-On Service URL (ACS URL))] フィールドの値を入力します。
- c) 設定ページの下部で [保存 (Save)] をクリックします。

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 Duo 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。