



Ping ID

- [概要 \(1 ページ\)](#)
- [使用する前に \(1 ページ\)](#)

概要

ここでは、Ping Identity で 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。

使用する前に

始める前に

- 管理者権限で Ping Identity 管理コンソールにサインインする必要があります。
- 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 Ping Identity コンソールで次の手順を実行します。

- a) [接続 (Connections)] > [アプリケーション (Applications)] に移動します。
- b) [+] ボタンをクリックして [アプリケーションの追加 (Add Application)] ダイアログを開きます。
- c) [アプリケーション名 (Application 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) 必要に応じて、説明を追加し、アイコンをアップロードします。
- e) [アプリケーションの種類 (Application Type)] で [SAMLアプリケーション (SAML application)] を選択し、[構成 (Configure)] をクリックします。
- f) [SAML設定 (SAML Configuration)] ダイアログで、SAML メタデータを手動で入力するオプションを選択し、[ACS URL (ACS URL)] と [エンティティID (Entity ID)] に一時的な URL を入力します。これらは後で実際の URL に置き換えます。

Add Application

SAML Configuration

Provide Application Metadata

Import Metadata
 Import From URL
 Manually Enter

ACS URLs *

https://www.example.com/acs

[+ Add](#)

Entity ID *

https://www.example.com/id

- g) [保存 (Save)] をクリックします。
- h) [設定 (Configuration)] タブをクリックします。
- i) [署名証明書のダウンロード (Download Signing Certificate)] をクリックします。
- j) 次の手順で使用するために、[発行元ID (Issuer ID)] プロパティと [シングルサインオンサービス (Single Signon Service)] プロパティの値をコピーします。
- k) [属性のマッピング (Attribute Mappings)] タブをクリックします。
- l) [編集 (Edit)] (鉛筆アイコン) をクリックします。
- m) 必須の [saml_subject (saml_subject)] 属性について、[電子メールアドレス (Email Address)] を選択します。
- n) [+追加 (+Add)] をクリックし、SAML 属性と PingOne ユーザー ID 属性の次のマッピングを追加し、それぞれのマッピングで [必須 (Required)] オプションを有効にします。

属性	[PingOne マッピング (PingOne Mappings)]
firstName	電子メールアドレス (Email Address)
lastName	名
email	Family Name

[属性マッピング (Attribute Mapping)] パネルは次のようになります。

Attributes	PingOne Mappings	Required
saml_subject	Email Address	<input checked="" type="checkbox"/>
email	Email Address	<input checked="" type="checkbox"/>
firstName	Given Name	<input checked="" type="checkbox"/>
lastName	Family Name	<input checked="" type="checkbox"/>

- o) [保存 (Save)] をクリックしてマッピングを保存します。

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](#)) が表示されます。

- [IDプロバイダー (IdP) 名 (Identity Provider (IdP) Name)] フィールドに統合の名前 (例 : **Ping 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、Ping SAML アプリケーションからコピーした [発行元ID (Issuer ID)] の値を入力します。
- [追加... (Add...)] をクリックし、前にダウンロードした Ping 署名証明書を選択します。
- 必要に応じて、無料の Duo 多要素認証からユーザーをオプトアウトします。

Integrate Identity Provider

1 Set Up
 2 Download
 3 Configure
 4 Activate

Set Up

Identity Provider (IdP) Name

Single Sign-On Service URL ⓘ

Entity ID (Audience URI) ⓘ

SAML Signing Certificate ⓘ

File must be in PEM format

By default, SecureX Sign-On enrolls all users into [Duo MultiFactor Authentication \(MFA\)](#) at no cost. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.

Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On? Yes No

If your organization has integrated MFA at your IdP, you may wish to disable MFA at the SecureX Sign-On level.

- e) [次へ (Next)] をクリックして [ダウンロード (Download)] 画面に進みます。
- f) [ダウンロード (Download)] 画面で、[シングルサインオンサービスURL (ACS URL) (Single Sign-On Service URL (ACS URL))] プロパティと [エンティティID (オーディエンスURI) (Entity ID (Audience URI))] プロパティの値をコピーし、[ダウンロード (Download)] をクリックして署名証明書をダウンロードします。

ステップ 3 Ping Identity コンソールに戻り、次の手順を実行します。

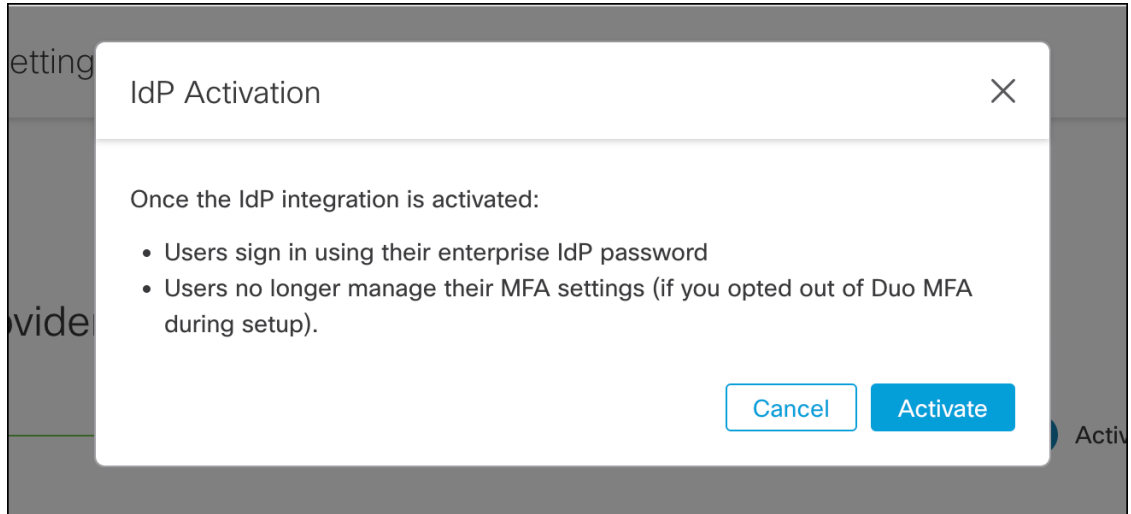
- a) [構成 (Configuration)] タブで、編集 (鉛筆) アイコンをクリックします。
- b) [ACS URL (ACS URLs)] フィールドで、一時的な URL を前の手順でコピーした [シングルサインオンサービスURL (ACS URL) (Single Sign-On Service URL (ACS URL))] に置き換えます。
- c) [エンティティID (Entity ID)] フィールドで、一時的な URL を前の手順でコピーした [エンティティID (オーディエンスURI) (Entity ID (Audience URI))] に置き換えます。
- d) [検証証明書 (Verification Certificate)] フィールドで、[インポート (Import)] オプションを選択し、[ファイルの選択 (Choose File)] をクリックします。
- e) 前の手順でダウンロードした Security Cloud Sign On 署名証明書を選択します。
- f) [保存 (Save)] をクリックします。
- g) アプリケーション設定パネルの上部にあるトグルをクリックして、アプリケーションへのユーザーアクセスを有効にします。

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 Ping Identity 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 Ping Identity 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。