



Google



重要 **Enterprise Manager** は廃止されました。[Security Cloud Control](#) を使用して ID プロバイダーの統合を管理できるようになりました。詳細については、[ID プロバイダー統合ガイド](#)を参照してください。

既存の ID プロバイダー統合データはすべて、[Security Cloud Control](#) を介して使用できます。

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

概要


ここでは、Google Workplace 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

- スーパー管理者権限を持つ Google Workspace アカウントが必要です。
- 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 スーパー管理者権限を持つアカウントを使用して [Google 管理コンソール](#) にサインインします。

- a) 管理コンソールで、メニュー  > [アプリ (Apps)] > [ウェブアプリとモバイルアプリ (Web and mobile apps)] に移動します。
- b) [アプリを追加 (Add App)] > [カスタム SAML アプリの追加 (Add custom SAML app)] をクリックします。

- c) [アプリの詳細 (App Details)] で以下を行います。
 - アプリケーション名に「**Secure Cloud Sign On**」または他の値を入力します。
 - 必要に応じて、アプリケーションに関連付けるアイコンをアップロードします。
- d) [続行 (Continue)] をクリックします。
- e) [SSOのURL (SSO URL)] と [エンティティID (Entity ID)] をコピーし、証明書をダウンロードします。

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 (IdP) 名 (Identity Provider (IdP) Name)] に「**Google SSO**」または他の値を入力します。
- 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、Google 管理コンソールからコピーした [SSOのURL (SSO URL)] を入力します。
- c) [エンティティID (オーディエンスURI) (Entity ID (Audience URI))] フィールドに、Google 管理コンソールからコピーした [エンティティID (Entity ID)] を入力します。
- d) [ファイルの追加 (Add File)] をクリックし、Google 管理コンソールからダウンロードした証明書を選択します。
- e) 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。
- f) [次へ (Next)] をクリックします。
- g) [シングルサインオンサービスURL (ACS URL) (Single Sign-On Service URL (ACS URL))] と [エンティティID (オーディエンスURI) (Entity ID (Audience URI))] をコピーし、SAML 署名証明書をダウンロードします。

ステップ 3 Google 管理コンソールに戻ります。

- a) [カスタムSAMLアプリの追加 (Add custom SAML app)] ページで [続行 (Continue)] をクリックします。
- b) [ACSのURL (ACS URL)] フィールドに、エンタープライズ設定ウィザードから前にコピーした [シングルサインオンサービスURL (ACS URL) (Single Sign-On Service URL (ACS URL))] を入力します。
- c) [名前IDの形式 (Name ID format)] で [UNSPECIFIED (UNSPECIFIED)] または [EMAIL (EMAIL)] を選択します。
- d) [名前ID (Name ID)] で [Basic Information > Primary email (Basic Information > Primary email)] を選択します。
- e) [続行 (Continue)] をクリックします。
- f) [属性のマッピング (Attributes mapping)] ページで次の属性マッピングを追加します。

[Googleディレクトリの属性 (Google Directory attributes)]	[アプリの属性 (App attributes)]
名 (First name)	firstName
姓 (Last name)	lastName
Primary email	email

Google Directory attributes		App attributes
Basic Information > First name	→	firstName
Basic Information > Last name	→	lastName
Basic Information > Primary email	→	email

ADD MAPPING

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。

- 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 Google SSO URL にリダイレクトされます。
- 申請したドメインと一致する電子メールアドレスで Google 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。
- 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。
- 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。
- 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。