



Google



Important **Enterprise Manager has been discontinued.** You can now use [Security Cloud Control](#) to manage your identity provider integrations. See the [Identity provider integration guide](#) for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

- [Overview, on page 1](#)
- [Getting Started, on page 1](#)

Overview

This guide explains how to create and integrate a Google Workplace SAML application and integrate it with Security Cloud Sign On.


Getting Started

Before you begin

- You must have a Google Workspace account with super administrator privileges.
- You need to have completed [Step 1: Create an enterprise](#) and [Step 2: Claim and verify your email domain](#) of the enterprise settings wizard.

Step 1

Sign in to your [Google Admin console](#) using an account with super administrator privileges.

- a) In the Admin console, go to Menu  > **Apps** > **Web and mobile apps**.
- b) Click **Add App** > **Add custom SAML app**.
- c) On the **App Details** page:
 - Enter **Secure Cloud Sign On** or other value for the application name.
 - Optionally, upload an icon to associate with the application.

- d) Click **Continue**.
- e) Copy the **SSO URL** and **Entity ID** and download the **Certificate**.

Step 2

In a new browser tab, open the Enterprise settings wizard. You should be on [Step 3: Exchange SAML metadata](#).

- a) Enter **Google SSO** or other value for **Identity Provider (IdP) Name**.
- b) In the **Single Sign-On Service URL** field enter the "SSO URL" you copied from the Google admin console.
- c) In the **Entity ID (Audience URI)** field enter the "Entity ID" you copied from the Google admin console.
- d) Click **Add File...** and select the certificate you downloaded from the Google admin console.
- e) If desired, opt out of free [Duo Multi-Factor Authentication](#) for your users.
- f) Click **Next**.
- g) Copy the **Single Sign-On Service URL (ACS URL)** and **Entity ID (Audience URI)** and download the **SAML Signing Certificate**.

Step 3

Return to the Google admin console.

- a) Click **Continue** on the **Add custom SAML app** page.
- b) In the **ACS URL** field enter the "Single Sign-On Service URL (ACS URL)" you previously copied from the enterprise settings wizard.
- c) For **Name ID** format select either `UNSPECIFIED` or `EMAIL`.
- d) For Name ID select **Basic Information > Primary email**.
- e) Click **Continue**.
- f) On the **Attributes mapping** page, add the following attribute mappings:

Google Directory attributes	App attributes
First name	firstName
Last name	lastName
Primary email	email

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

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

Step 4

Return to the Enterprise settings wizard's **Configure** screen.

- a) Copy the displayed URL and open it in a private (incognito) browser window.

- The browser is redirected to your Google SSO URL.
- Sign in to Google with an email address that matches your [claimed domain](#). The test is successful if you land back in the SecureX Application Portal.
 - Click **Next** in the settings wizard to advance to the **Activate** screen.
 - To activate the integration for your users, click **Activate my IdP**.
 - Confirm your decision in the dialog.

