Adobe Sign

Enabling SAML Single Sign-On with OneLogin
Reference Guide
Overview

Adobe Sign can support Security Assertion Markup Language (SAML) single sign-on (SSO) using external identity providers (IdPs) such as OneLogin. This document describes the steps for configuring Adobe Sign for SAML SSO with OneLogin. This document also provides information on testing your SAML SSO configuration. Before proceeding, please see the Adobe Sign Single Sign On Using SAML Guide, which describes the SAML set up process and provides detailed information on the SAML Settings in Adobe Sign.

Configuring SAML SSO with OneLogin

1. Log in to OneLogin and Adobe Sign in different browsers or in different windows within the same browser.
   o In OneLogin, log in to your account with the same administrator credentials you use for your Adobe Sign Admin Account.

   ![OneLogin Login Screen](image1)

   o In Adobe Sign, log in to your account using the same admin account credentials you use for OneLogin. The passwords for these two logins do not have to be the same, but you must log in as the administrator for each account.

   ![Adobe Sign Login Screen](image2)
2. In OneLogin, click **Add Apps**.

3. Search for **Adobe Sign**.

4. Click the row for Adobe Sign.
5. In the *Add* page, under *Connectors* select **SAML 2.0 – user provisioning**, then click **Save** at the top.

7. In OneLogin, click the Configuration tab. In the Subdomain field, enter your Hostname from Adobe Sign, then click Save.
8. Click the SSO tab.

9. In the SSO tab, click **View Details** to display the *Standard Strength Certificate (2048-bit)* page.
10. In the Standard Strength Certificate page that displays, click the **Copy to Clipboard** button for the **X.509 Certificate** field to copy the certificate to the clipboard.

If the certificate successfully copies, the rollover text says “Copy to Clipboard” text updates to “Copied”.

11. In Adobe Sign, paste the copied certificate into the **IdP Certificate** field. Be sure to remove any returns that may have been copied. The cursor should be at the end of the last line as shown below.
12. In OneLogin, click the **Copy to Clipboard** button for the **Issuer URL**.

13. In Adobe Sign, paste the **Issuer URL** into the **Entity ID/Issuer URL** field.
14. In OneLogin, click the **Copy to Clipboard** button for the **SAML 2.0 Endpoint (HTTP)** URL.

15. In Adobe Sign, right click to paste the **SAML 2.0 Endpoint (HTTP)** URL in the **IdP Login URL** field.
16. In OneLogin, click the **Copy to Clipboard** button next to **SLO Endpoint (HTTP)**.

![Image showing OneLogin SAML 2.0 Endpoint URL]

**Note:** The OneLogin SAML 2.0 Endpoint URL is only a suggestion. You can actually specify any valid URL (e.g., Google).

17. In Adobe Sign, copy the **SLO Endpoint** value into the **Logout URL/SLO Endpoint** field.

![Image showing Adobe Sign Identity Provider (IdP) Configuration]

18. In Adobe Sign, click **Save**.

![Image showing Adobe Sign Save button]
19. In OneLogin, click the back arrow to return to the SSO page.

20. Click the Users tab to add users.

21. Click the row to add the user. The Save button is not activated until you click at least one user.

22. When done, click Save.
Testing Your OneLogin SAML SSO Configuration

There are two ways to test your OneLogin SAML Setup.

Log in to Adobe Sign through OneLogin

1. If logged in, log out of Adobe Sign.
2. Log in to OneLogin.
3. On the App Home page, click the Adobe Sign app.

You are automatically logged into Adobe Sign.
Log in to Adobe Sign using your URL

1. Enter your company login URL for Adobe Sign in the address line of your browser (such as myCompany.adobesign.com). The Adobe Sign Sign In page displays.

2. On the Sign In page, click the second Sign In button. If you've entered a custom Single Sign On Login Message that message displays above this button. If you have not entered a custom message, the default message displays.

3. You are logged into Adobe Sign.