Adobe Sign

Enabling Single Sign-On with SAML Reference Guide
## Table of Contents

Introduction ............................................................................................................................................................. 3

Prerequisites ............................................................................................................................................................ 4

Enabling Single Sign On using SAML .................................................................................................................. 5

Working with SAML Settings ................................................................................................................................. 6
  SAML Mode Settings ........................................................................................................................................... 7
  Hostname ............................................................................................................................................................... 7
  User Creation Settings ......................................................................................................................................... 8
  Login Page Customization Settings .................................................................................................................... 8
  Identity Provider (IdP) Configuration .................................................................................................................. 10
  Adobe Sign SAML Service Provider (SP) Information ...................................................................................... 11
Introduction

The identity federation standard Security Assertion Markup Language (SAML) 2.0 enables the secure exchange of user authentication data between web applications and identity service providers.

When you use the SAML 2.0 protocol to enable single sign-on (SSO), security tokens containing assertions pass information about an end user (principal) between a SAML authority - an identity provider (IdP), and a SAML consumer - a service provider (SP). (See for more information about the SAML protocol.)

Adobe Sign, acting as the service provider (SP), supports single sign-on through SAML using external identity providers (IdPs) such as Okta, OneLogin, Oracle Federated Identity (OIF), and Microsoft Active Directory Federation Service. Adobe Sign is compatible with all external IdPs that support SAML 2.0.

More information on integrating with these identity providers (IdPs), can be found in the following guides:

- Enabling SAML Single Sign On for Microsoft Active Directory Federation Service Reference Guide
- Enabling SAML Single Sign On for Okta Reference Guide
- Enabling SAML Single Sign On for OneLogin Reference Guide
- Enabling SAML Single Sign-on with Oracle Identity Federation Reference Guide

You can also configure Adobe Sign for single sign-on (SSO) with other systems already used in your organization, for example Salesforce.com, or other providers that support SAML 2.0.

Adobe Sign uses federated authentication as opposed to delegated authentication. Federated authentication does not validate the user's actual password in Adobe Sign. Instead, Adobe Sign receives a SAML assertion in an HTTP POST request. Adobe Sign also supports encrypted assertions.

The SAML assertion has a limited validity period, contains a unique identifier, and is digitally signed. If the assertion is still within its validity period, has an identifier that has not been used before, and has a valid signature from a trusted identity provider, the user is granted access to Adobe Sign.

A summary of the Adobe Sign authentication specification is included in the table below:

<table>
<thead>
<tr>
<th>Specification (Standard Name)</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federation protocol</td>
<td>SAML 2.0</td>
</tr>
<tr>
<td>Federation profile</td>
<td>Browser Post</td>
</tr>
<tr>
<td>Federation unique identifier</td>
<td>Email Address</td>
</tr>
<tr>
<td>Relay State</td>
<td>Adobe Sign already has the logic to know where to point the User after they are authenticated so Relay State is not needed.</td>
</tr>
</tbody>
</table>
The following diagram shows how the request and response are processed.

Prerequisites

To enable SSO, your corporate network must support the SAML 2.0 protocol. If your corporate network does not support SAML, contact Adobe Sign Support at support@echosign.com to discuss other options to enable Single Sign On in your account.

Before beginning to set up SAML SSO, you must do the following:

- Establish a Domain Name. (For the examples in this guide, this will be rrassoc.com.)
- Enable SAML for your domain using a provider such as Microsoft Active Directory Federation, Okta, Onelogin, Oracle Identity Federation, or others. You may need to open an Adobe Sign support ticket to get your domain enabled from the backend.
- Create or verify that you have an administrator account with your IdP using an email address (For the examples in this guide, this email address will be susan@rrassoc.com.)
  - If you do not have an Okta account, you can create a free Okta Developer Edition organization using this link: https://www.okta.com/developer/signup/.
If you do not have a OneLogin account, you can create a free trials account using this link: https://www.onelogin.com/ and clicking the FREE TRIAL button in the upper right corner.

- (Optional) Add an additional email id for User Provisioning in both IdP and SP. This will allow you to add more users who can log into Adobe Sign with their SSO credentials.
- (Required) Verify that you have an admin user for Adobe Sign and an Admin user for the IdP.
  (Optional) Create or verify that you have an Adobe Sign administrator account that uses the same email address as the account for your IdP (For the examples in this guide, this email address will be susan@rrassoc.com.) This will make it easier for you to administer the accounts.
- In Adobe Sign, set your SAML Mode to "SAML Allowed". (See Working with the SAML Settings for more information.)

  **Note:** When setting up SAML SSO, we recommend that you set the SAML Mode to SAML Allowed until the entire setup process is complete and you've verified it is working correctly. Once verified, you can change the SAML Mode to SAML Mandatory.

### Enabling Single Sign On using SAML

At a high level, enabling SAML SSO between Adobe Sign (the SP) and your IdP involves the following high-level steps:

1. If required (by your IdP), set up your IdP using the Adobe Sign Service Provider (SP) Information.
2. Set up Adobe Sign using information from your IdP.
3. Verify that the SAML SSO has been properly set up.
Working with SAML Settings

To locate your Adobe Sign SAML Settings, log in as an account administrator or group administrator, then click Account. Under Account Settings, click SAML Settings.
To view the options for User Creation, Login Page Customization, Identity Provider (IdP) Configuration, and Adobe Sign Service Provider (SP) Information, scroll to the bottom of the SAML Settings page.

**SAML Mode Settings**

In Adobe Sign, there are three SAML Mode options and one additional option that works with the *SAML Mandatory* option.

- **SAML Disabled**—Enable this option that you are not using SAML for your account. When selected, none of the SAML Settings are accessible.
- **SAML Allowed**—Enable this option to allow all users, including account administrators, to use SAML SSO. Users can also continue using their Adobe Sign credentials as well.
- **SAML Mandatory**—Enable this option to enforce log in with SAML SSO for all users. If this option is selected, the “Allow Adobe Sign Administrators to log in using their Adobe Sign Credentials” option will be greyed out (disabled).

As noted above under Prerequisites, we recommend that you set the SAML Mode to **SAML Allowed** until you've verified your SAML SSO set up.

**Hostname**

The Hostname is your domain name. (See Prerequisites above.) When entered, your hostname becomes part of the Assertion Consumer URL, the Single Log Out (SLO) URL, and Single Sign-On (Login) URL.
User Creation Settings

Only the first of the two User Creation settings is directly connected with SAML Setup. The second setting pertains to all pending users, whether or not they are added as a result of authenticating through SAML.

- **Automatically add users authenticated through SAML**—If this option is enabled, users who are authenticated through your IdP are automatically added as pending users in Adobe Sign.

- **Automatically make pending users in my account active**—If the *Require signers in my account to log in to Adobe Sign before signing* setting, under *Signer Identity Verification* (Security Settings), is enabled, this setting should also be enabled. When a signature is requested from a new user, this user is created as a pending user in your account. If this option is not enabled, these users are prevented from signing agreements sent to them for signature.

Login Page Customization Settings

You can customize the sign on message that users see on the Adobe Sign **Sign In** page when SAML Single Sign On is enabled.

- **Single Sign On Login Message**—Optionally, enter a message to display above the SSO **Sign In** button on the Adobe Sign **Sign In** page. Below are examples of a custom SSO Login Message and the default SSO login message, in this case for Okta, and the default message.
Custom SSO Login Message

Email: susan@rrassoc.com
Password: *******

Sign In

I forgot my password

Please use Okta

Sign In

Default SSO Login Message

Email: susan@rrassoc.com
Password: *******

Sign In

I forgot my password

Sign in using your corporate credentials

Sign In
Identity Provider (IdP) Configuration

To set up most IdPs, except as noted for Okta, you must enter information from your IdP into the IdP configuration fields in Adobe Sign.

- **Entity ID/Issuer URL** — This value is provided by the IdP to uniquely identify your domain.
- **Logout URL/SLO Endpoint** — When someone logs out of Adobe Sign, this URL is called to log them out of the IdP as well.
- **Login URL/SSO Endpoint** — The URL that Adobe Sign will call to request a user login from the IdP. The IdP is responsible for authenticating and logging in the user.
- **IdP Certificate** — The authentication certificate issued by your IdP.
Adobe Sign SAML Service Provider (SP) Information

The SP information section displays the default information for Adobe Sign. Once you've entered and saved your host name and IdP Configuration information, the information in the SP information section is updated to include your hostname. (In our example, https://secure.echosign.com/public/samlConsume becomes https://globalcorp.na1.echosign.com/public/samlConsume.)

The SP Information provided is as follows:

- **Entity ID/SAML Audience** — A URL that describes the entity that is expected to receive the SAML message. In this case, it is the URL for Adobe Sign.
- **SP Certificate** — Some providers require a certificate to be used to identify the Service Provider. The link in this view points to the Adobe Sign Service Provider certificate.
- **Assertion Consumer URL** — This is the callback that the IdP will send to tell Adobe Sign to log in a user.
- **Single Log Out (SLO) URL** — The URL that users are redirected to when they log out.
- **Single Sign-On (Login) URL** — This is the URL that the IdP will send login requests to.