Single Sign-On with Salsify

Last Modified on 03/19/2018 10:42 pm EDT

With single sign-on (SSO) in Salsify, users can login using their existing corporate credentials for login.

With single sign-on, you'll:

- Provide a better user experience for your users. They'll only need to remember their existing corporate password.
- Easily stay aligned with your internal security requirements. For example, terminated users are immediately prevented from logging into Salsify and your corporate password rules are used.

Salsify supports any *SSO* with any *SAML 2.0 Identity Provider* and includes certified integrations for *OneLogin*, *PingIdentity*, and *Okta*.

How to Configure Single Sign-On

Configuring Salsify for single sign-on requires two aspects. Salsify must configure your Salsify organization for single sign-on and you will configure your *Identity Provider* to work with Salsify. Once your Salsify organization is configured for single sign-on, users will enter their email address into Salsify and then will be prompted to login with their existing corporate login.

Users need to be manually invited to Salsify within the Salsify application. Learn how here.

Salsify requires an email address as the username (which is also used to send application notifications to), but the Salsify username does not need to match the username used to authenticate to your *Identity Provider*.

Salsify needs either the fingerprint of the *Identity Provider's* certificate (preferred) or the *Identity Provider's* certificate.

The identity provider should be configured to either send back a name attribute with the user's full name or firstName and lastName attributes with authentication response to maintain an updated user profile name.

Click the links below to review setup details by provider:

- SSO with AD FS 2.0
- SSO with OneLogin
- SSO with PingIdentity
- SSO with Okta
- SSO with Google Apps
- SSO with other SAML 2.0 Identity Providers
- SSO with Azure

Configuring SSO with OneLogin

1. Within *OneLogin*, click *Apps* > Add *Apps* and search for Salsify.

2. Accept the default display name and logo and click *Save*.
3. Click SSO in the newly created Salsify application and send Salsify the values of the following fields:
    - The value of the *SAML 2.0 Endpoint* (HTTP) field. This is the *Identity Provider* URL where authentication requests should be sent.

    - The fingerprint. Find the *SHA* fingerprint by clicking *View Details* in the X.509 *Certificate* section.

4. Once Salsify has configured your Salsify account with the *OneLogin Identity Provider*, you'll be provided with necessary values to complete the configuration.
5. On the *Configuration* tab, for Salsify ID, enter the ID provided to you by Salsify. Save the configuration.

6. On the *Parameters* tab, click *Full Name* to configure user attributes sent as the user's name in Salsify.

7. Fill in the appropriate mapping and save. This example uses a macro to concatenate first name and last name.

8. Save the configuration and continue with the regular *OneLogin* flow. Click the *Users* tab to choose which users you want to enable for the application.

Configuring SSO with PingIdentity

1. Reach out to customer support to request your Salsify organization to be configured with SSO. Include the following:
    - The *IdentityProvider SSO URL*
    - The *Certificate Fingerprint*
2. In *PingIdentity*, click *Applications* > *Application Catalog* and search for Salsify.

3. Click *Download Certificate* from the *PingIdentity* Salsify application screen.
4. To get the remaining information needed to set up your account, reach out to Salsify support and send:
    - *Target URL*
    - *Certificate Fingerprint*
5. Salsify will respond to your request and provide you with the remaining information needed to configure your account.
6. Use the *ACS URL* provided to you by Salsify to fill out the relevant application details, and click *Done*.

Configuring SSO with Okta

1. Reach out to Salsify support to request your Salsify organization to be configured with SSO. Include the following:
    - The *IDP SSO URL*
    - *IDP SHA1 Certificate Fingerprint*
2. Salsify will respond to your request and provide you with an *IDP ID*.
3. In *Okta*, click *Applications* > *Add Application*.
4. Search for Salsify and click *Add*.

5. In General Settings:
    - For *IDP ID*, enter the value provided to you by Salsify.
    - Set the *Application Visibility* as desired.
    - Click *Next*.
    - Assign the users that should be able to access Salsify.
    - Verify the email address of the users is assigned as the user name.
    - Click *Done*.

Configuring SSO with Google Apps

You must be signed in as a super administrator with Google to complete the process.

Step 1: Get Google identity provider (IdP) information

1. From the Admin console dashboard, go to *Security* > *Set up single sign-on (SSO)*.
   Note: To see *Security*, you might have to click *More controls* at the bottom.
2. In the *Set up single sign-on (SSO)* section:
   - Copy and save the *SSO URL*.
   - Copy and save the *Entity ID*.
   - *Download the Certificate*.

Step 2: Send idP information to Salsify

Click Contact Us above to request that SSO be enabled for your account. Include the following identity provider (IdP) information copied in Step 1:

- SSO URL
- Entity ID
- Attach the certificate you downloaded in Step 1 as a text file attachment to the email.

We will process your request and provide you with a Callback URL.

Step 3: Set up Google as a SAML identity provider

1. From the Admin console dashboard, go to *Apps* > *SAML Apps*.
   Note: To see Apps on the dashboard, you might have to click *More controls* at the bottom.
2. Click the plus (+) icon at bottom right.
3. Locate and click *Salsify* in the application list.
4. Click *Next*.
   The *Basic information* window shows the *Application name* and *Description* seen by users.
5. Click *Next*.
6. On the *Service Provider Details* page, replace the *ACS URL* with the Callback URL you got from Salsify.
7. Click *Finish*.

Step 4: Enable the Salsify App

1. From the Admin console dashboard, go to *Apps* > *SAML Apps*.
2. Select *Salsify*.
3. At the top of the gray box, click the *More* icon and choose:
   - *On for everyone* to turn on the service for all users (click again to confirm).
   - *Off* to turn off the service for all users (click again to confirm).
   - *On for some organizations* to change the setting only for some users.
4. Ensure that your Salsify user account email IDs match those in your Google domain.

Step 5: Verify that SSO is Working

1. Close all browser windows.
2. Open https://app.salsify.com/users/sign_in and attempt to sign in. You should be automatically redirected to the Google

sign-in page.
3. Enter your sign-in credentials.
4. After your sign-in credentials are authenticated, you are automatically redirected back to Salsify.

Configuring SSO with other SAML 2.0 Identity Providers

Salsify will configure your Salsify organization for single sign-on. To complete this step, please contact Salsify support and include the following information:

- The *Identity Provider URL* that authentication requests should be sent to. (Required)
- The fingerprint of the *Identity Provider*'s certificate (Required)
- The algorithm used to compute the fingerprint of the *Identity Provider*'s certificate. The default supported by Salsify is *SHA1*. See the XML Signature Spec for supported digest algorithms.

Your metadata file can be sent to provide this information.

Then configure your *Identity Provider* to recognize Salsify using the following information:

- *Application URL* - This is customer specific and will be provided to you after Salsify completes the first step above.
- *Entity ID/Audience* - salsify.com
- *Assertion Consumer Service (ACS) URL* - This is customer specific and will be provided to you after Salsify completes the first step above.
- *Name ID Format* - urn:oasis:names:tc:SAML:1.1:named-format:emailAddress Salsify identifies users by email address.
- *Requested Attributes* - This is a mapping from the *Identity Provider*'s user attributes to the attributes requested by Salsify. We expect a name which will be the user's full name.

Configuring SSO with Azure

1. Navigate to the appropriate *Active Directory*.
2. Click *Enterprise Applications* in the sidebar.
3. Click *New Application*.
4. Select *Non-Gallery Application*.
5. Name your application Salsify and click Add at the bottom.
6. On the application landing page, click Properties under the Manage header.
7. Find the User Access URL and copy it. You will need to send this to Salsify.
8. Navigate to the Single Sign On section under the Manage header.
9. Select SAML-based Sign On.
10. Scroll down to the SAML Signing Certificate section and click on the Certificate (base64) link. This is your SAML Signature

and must be sent to Salsify before configuration can continue.

11. Reach out to Salsify support to request your Salsify organization to be configured with SSO. Include the following:
    - The User Access URL
    - SAML Signature
12. Salsify will respond to your request and provide you with a Callback URL.
13. Once Salsify has replied with the Callback URL, go back to the Single Sign On configuration page.
    - In the Identifier field, type salsify.com.
    - In the Reply URL field, input your Callback URL provided by Salsify.

14. In the User Attributes section, set the User Identifier to user.mail, as Salsify uses the email address to authenticate.

15. Save your configuration. Reach out to Salsify support and request to have Single Sign On enabled.