onelogin

OneLogin for Adaptive Insights

www.onelogin.com | twitter.com/onelogin

OneLogin, Inc. | 150 Spear Street, Suite 1400, San Francisco, CA 94105

855.426.7227

Table of Contents

1. SIGN UP FOR ONELOGIN

OneLogin is the smart and simple way to eliminate passwords and automate user management for Adaptive Insights!

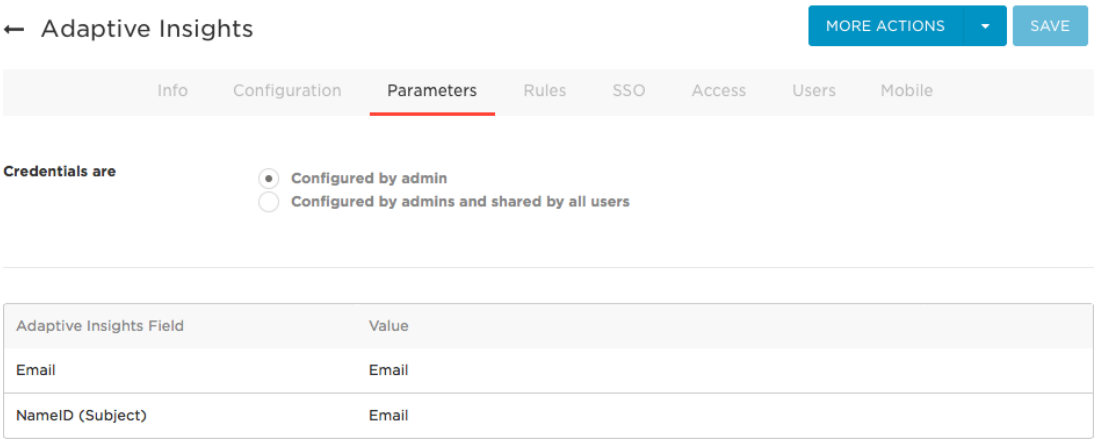
1.1 If you don't already have OneLogin, start by navigating to the OneLogin homepage and proceed to the OneLogin free trial at https://www.onelogin.com/signup At this point, you should be re-directed back into your account and have selected a password. Once you're within your OneLogin account, lets get started on setting up Adaptive Insights.

2. ADDING ADAPTIVE INSIGHTS TO ONELOGIN

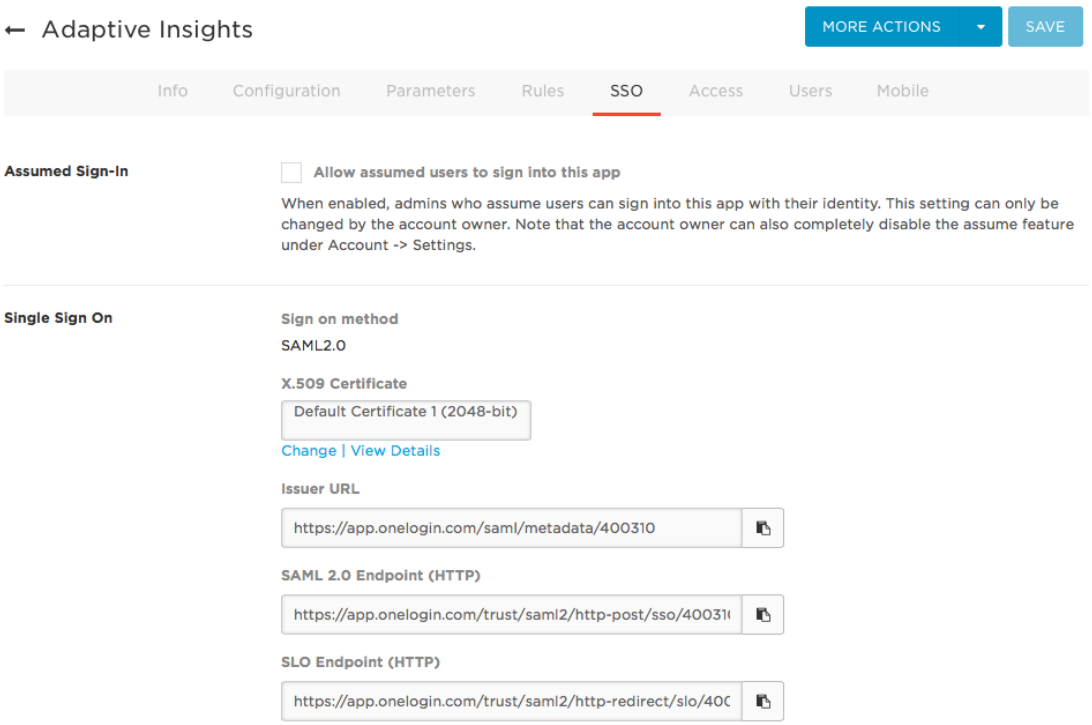
2.1 To add Adaptive Insights to your OneLogin account, start at your dashboard portal and proceed to **Apps** > **Add Apps** and search for 'Adaptive Insights'. There will be only one connector, so go ahead and select that and when you're in the configuration page, select **Save** to add Adaptive Insights to your OneLogin account.

3. SETTING UP SINGLE SIGN-ON

3.1 Immediately you will be brought to the Adaptive Insights **Info** tab. Proceed instead to the **Parameters** tab. Here ensure that **Credentials** are 'Configured by admin', and that both the **Email** and **NameID (Subject)** fields are set to 'Email'. Completed, your page should resemble the example below, so go ahead and select Save to confirm your settings.



3.2 Next, navigate over to the SSO page. Here you'll be copying down both the **Issuer URL** and the **SAML 2.0 Endpoint**. Then, proceed to 'View Details' under the associated X.509 Certificate to view that certificate's page. Select the **X.509 PEM** format, and then **Download** to acquire the certificate. The certificate and both URL's will be placed within the Adaptive Insights dashboard to confirm the SAML SSO connection.

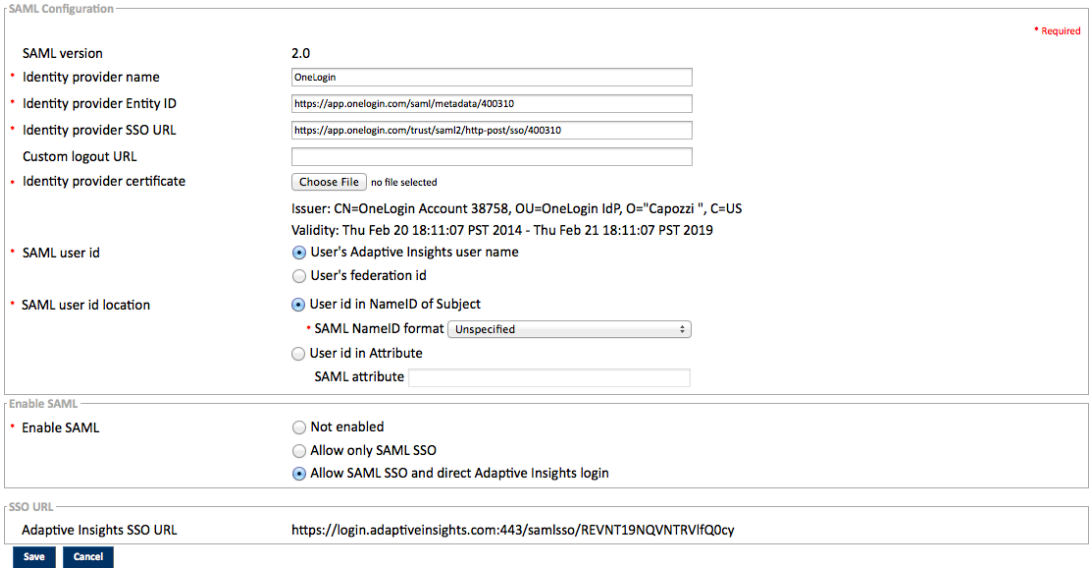


3.3 Now, move into your organization's Adaptive Insight account. Within the upper left configuration menu, navigate to **Admin** > **Manage SAML SSO Settings**, under **Users and Roles**.

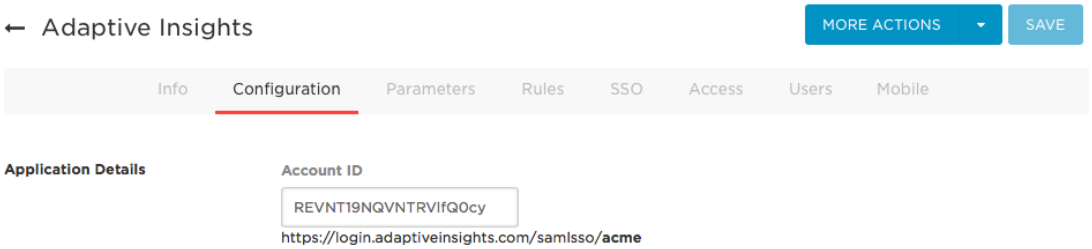
3.4 Begin by naming your SAML connection, and then upload the .PEM certificate by selecting **Choose File**. Under **Enable SAML**, select 'Allow SAML SSO and direct Adaptive Insights login', and then proceed to fill out the rest of the page with the information on the left. Finally, copy down the account ID *(samlsso/YOUR ACCOUNT ID)* from your **SSO URL** at the bottom of the page. When completed, your page will resemble the example below, so go ahead and select **Save** to confirm your settings.

Here's a quick list of the information you'll be needing within the SAML SSO section:

Identity provider Entity ID
OneLogin Issuer URL
Identity provider SSO URL
OneLogin HTTP Endpoint
SAML user id
User's Adaptive Insights user name
SAML user id location
SAML NameID format: unspecified



3.5 With the **Account ID** retrieved from Adaptive Insights, proceed back into OneLogin and proceed to **Apps** > **All Apps** > **Adaptive Insights**, and within the **Configuration** tab, place it within the **Account ID** field. When completed, your page will resemble the example below, so then go ahead and select **Save** to confirm your settings.



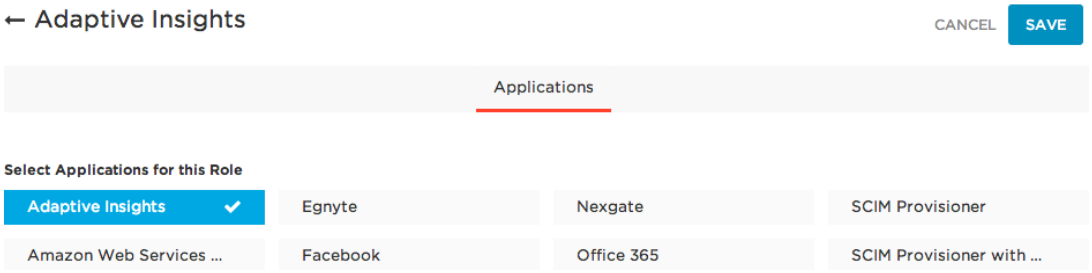
And with this, OneLogin should be successfully connected with Adaptive Insights through SAML!

4. MAPPING ADAPTIVE INSIGHTS TO USERS

With SAML successfully enabled and single sign-on properly configured, lets allocate Adaptive Insights to a group of users.

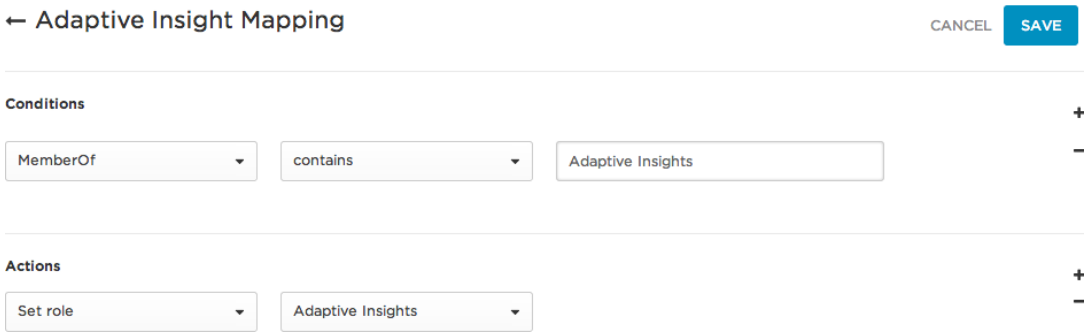
Roles are the key component of OneLogin that grant users access to an application. In many cases, Roles are linked to a security group in the corporate directory and members of that group are then granted access to apps in OneLogin.

4.1 Proceed to **Users** > **Roles** > ***New Role*** and give your role a name and associate it with Adaptive Insights. For simplicity I will use a Role named "Adaptive Insights" and the Security Group named "Adaptive Insights" in Active Directory.



4.2 Now with the Role established, lets generate a custom mapping that will assign the the Role of Adaptive Insights to everyone within the Group of Adaptive Insights. Proceed to **Users** > **Mappings** and, seeing as we have no mappings that includes Adaptive Insights, go ahead and select **New Mapping**.

4.3 In the **Custom Mapping** page, you can name a mapping and give it actions, and a condition to execute that action; here we're making a simple group for Adaptive Insights, a Role we've generated to give a group of users Adaptive Insights based on their active directory grouping. When you've created your mapping, select **Save** to proceed.



4.4 Note how when the **Condition** = Memberof > Contains > Adaptive Insights, **Perform these actions** = Set role > Adaptive Insights, it's saying that 'Anytime a user is a member of the group Adaptive Insights, set their role to 'Adaptive Insights'. Mappings are flexible, so tailor them to your personal user situations.

4.5 You can always check what users are going to be affected by your mapping by selecting **More Actions** > **Preview All Mapped Users** or **Preview All Mapped Users**.

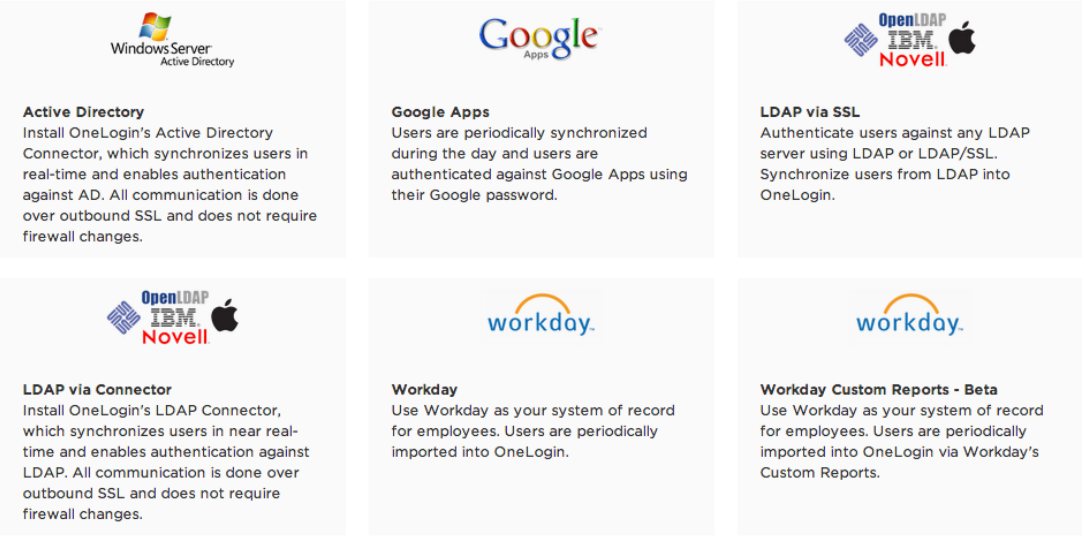
4.6 Once you're back in the Mappings page, select **Reapply All Mappings** to confirm and refresh the mapped entitlements to all users.

At this point, you and your users should have full access to Adaptive Insights and be able to log in to their accounts via single sign-on!

5. ADDING YOUR DIRECTORY

OneLogin easily integrates with all major user and corporate directories, and linking them to your accounts is incredibly easy.

5.1 Start by going to **Users** > **Directories** to select the directory you wish to integrate and then select it.



5.2 Each directory has its own workflow and such things are detailed elsewhere. Here are some links to helpful articles detailing how to configure your directory:

Active Directory:

https://onelogin.zendesk.com/hc/en-us/articles/202361690-Directory-Active-Directory

LDAP via Connector:

https://onelogin.zendesk.com/hc/en-us/articles/202361700-Directory-LDAP

Google Apps:

https://onelogin.zendesk.com/hc/en-us/articles/202361710-Directory-Google-Apps

Questions?

Send us an email at support@onelogin.com