Gui Bortolaso
Technical Implementation Consultant

4305 Hacienda Drive, Suite 300
Pleasanton, CA 94588 - USA
Mobile: +55 51 98175-0705
Skype: gui.bortolaso
Email: gui.bortolaso@gmail.com

To IT Support Department at ACME Co.

ACME SSO Implementation Document

1. About

This document describes the steps to setup Onelogin as Identity Provider (IdP) and Degreed as Service Provider (SP), also contains the credentials and metadata file for SSO Authentication setup.
Please, do not hesitate to contact in case of any issue as well to reach us to book a screen sharing session for technical support.

1.1 Glossary

- SP - Service Provider
- IdP - Identity Provider
- SAML - Security Assertion Markup Language
- SSO – Single Sign On

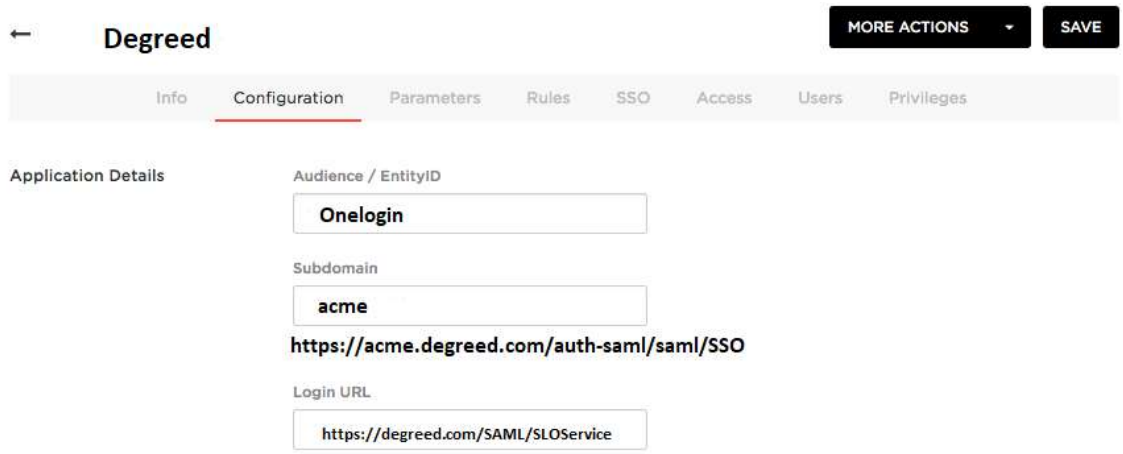
2. Providers and Metadata File

- Name of the Identity Provider (IdP) OneLogin
- Name of the Service Provider (SP) Degreed
- Service Provider metadata: Link to file

3. Configuring SAML for Degreed *(All the information and steps described in section 3 to 7 were adapted from OneLogin documentation for didactic purpose only, with no valid technical information)*

This topic describes how to configure OneLogin to provide SSO for **Degreed** using SAML.

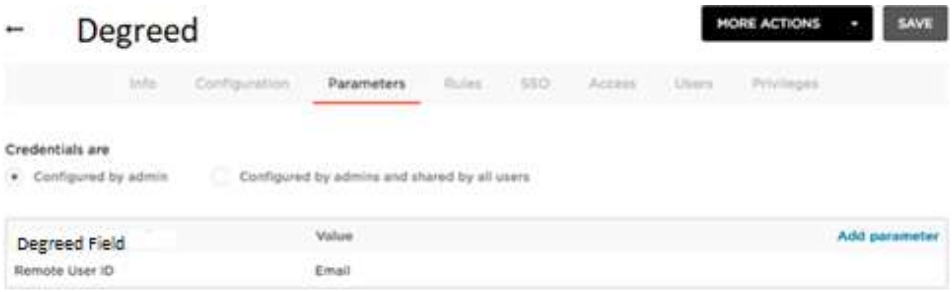
- Log into OneLogin as an admin and go to Apps > **Add Apps**.
- Search for and select the Degreed SAML connector Edit the Display Name, if necessary.
- Click Save to add the app to your Company Apps and display additional configuration tabs.
- Select the Configuration Tab.



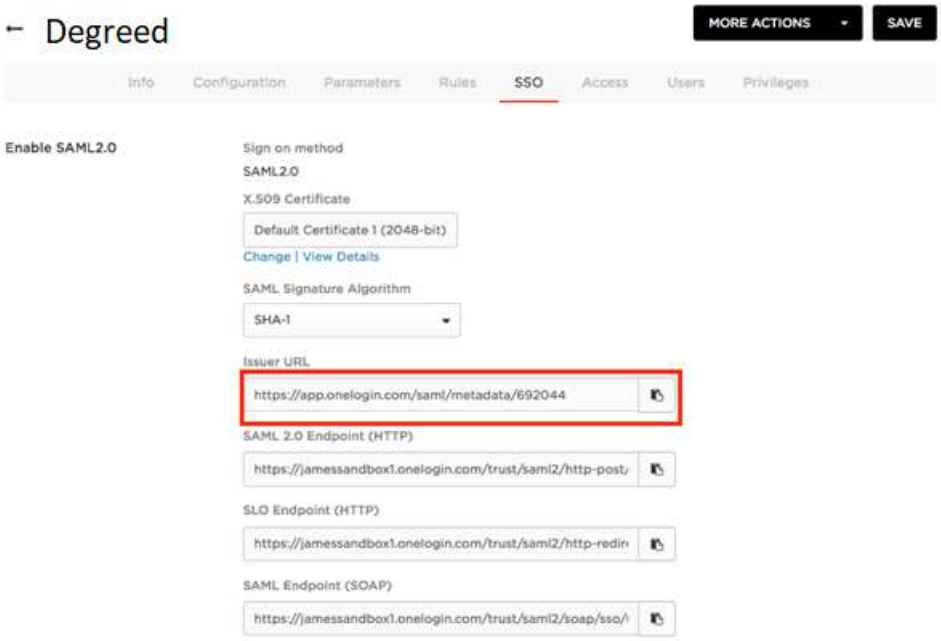
- Set the values below:

Audience / Entity ID	Enter "OneLogin"
subdomain	Subdomain of Degreed app e.g. https://**{subdomain}**. degreed.com/auth-saml/saml/SSO See figure above to obtain the value.
Login URL	Login URL listed in custom Degreed login page (hyperlink pointing to "Single Sign-On via OneLogin".

- Click Save.
- Select the Parameters Tab.
- Ensure that Credentials are Configured by admin and that the mappings are as follows:
  Remote User ID -> Email (or another username value currently in Degreed)



- Click Save.
- Go to the SSO tab to obtain the Issuer URL that you will need to setup your Degreed SSO settings. Copy this value and keep it for instructions further below under the "Configure Degreed" instructions below.



- On the OneLogin Access tab, assign the OneLogin roles that should have access to Degreed and provide any app security policy that you want to apply.
- You can also go to Users > All Users to add the app to individual user accounts.
- Click Save.

4. Configure Degreed - Activate the SAML Building Block

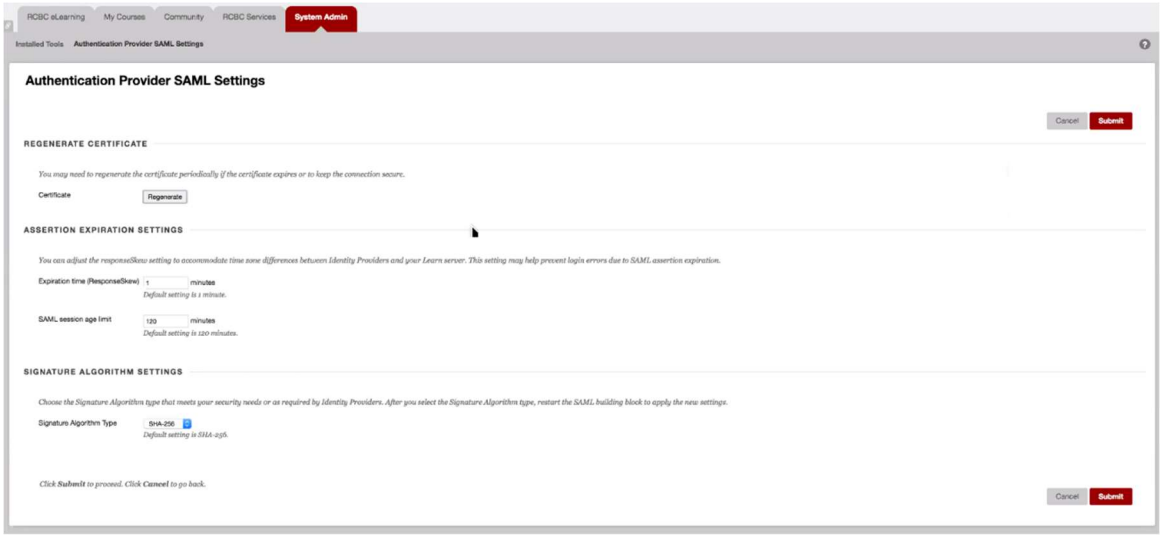
If you are using Degreed on a SaaS Deployment, you don't need to install the building block, as it is already present on your system. After you make the SAML 2.0 Building Block available, proceed to step 6.

1. Navigate to the Admin Panel.
2. Under Building Blocks, select Building Blocks.
3. Select Installed Tools, then select Upload Building Blocks.
4. If the SAML 2.0 Building Block is already installed, locate it in the list and set its status as available.
5. Select Browse to locate the Building Block package on your machine. When finished, select Submit.
6. Select Approve to make the Building Block available.
7. On the Admin Panel, under Building Blocks, select Authentication.
8. SAML now appears in the Create Provider list on the Authentication Provider page.

5. Configure settings

You can configure settings to troubleshoot issues or ensure the security of your SAML connection.

1. Navigate to the Admin Panel.
2. Under Building Blocks, select Building Blocks.
3. Select Installed Tools.
4. Locate Authentication Provider - SAML in the list. Open the menu and select Settings. You have the following options:

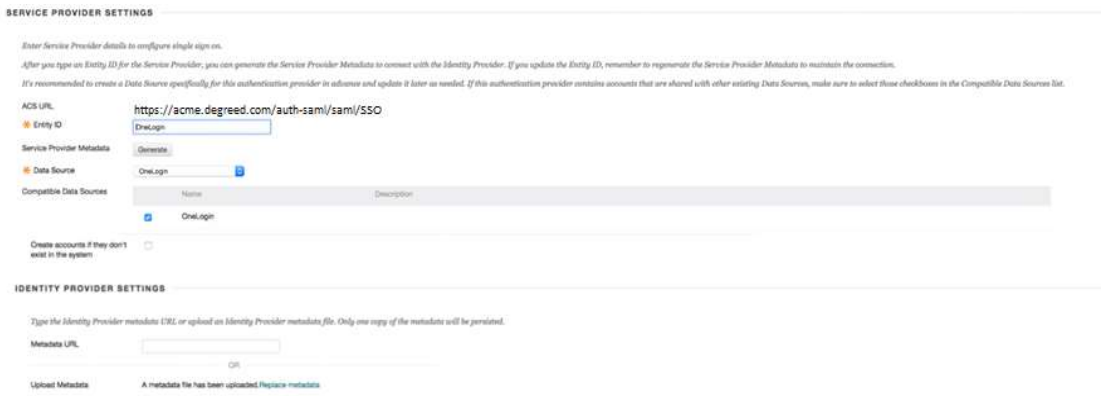


- Regenerate Certificate: Select Regenerate to regenerate the SAML certificate. You may need to regenerate a certificate to keep your connection secure, or if the certificate has expired.
- After you regenerate the certificate, you need to re-upload the Service Provider metadata to the Identity Provider. When you select Regenerate, the system prompts you to confirm this step.
- Assertion Expiration Settings: In this section, you can adjust the Expiration time (ResponseSkew) and the SAML session age limit. You may need to edit the ResponseSkew value if your Degreed server is in a different time zone than the Identity Provider's server. The time difference can cause SAML assertions to expire before users are properly authenticated. SAML sessions expire in the time length in SAML session age limit.
- Signature Algorithm Settings: Choose a signature algorithm type that meets your security needs or as required by Identity Providers. After you select the Signature Algorithm Type, restart the SAML building block to apply the new settings.
- Select Submit to save your changes.

6. Create and configure a SAML authentication provider

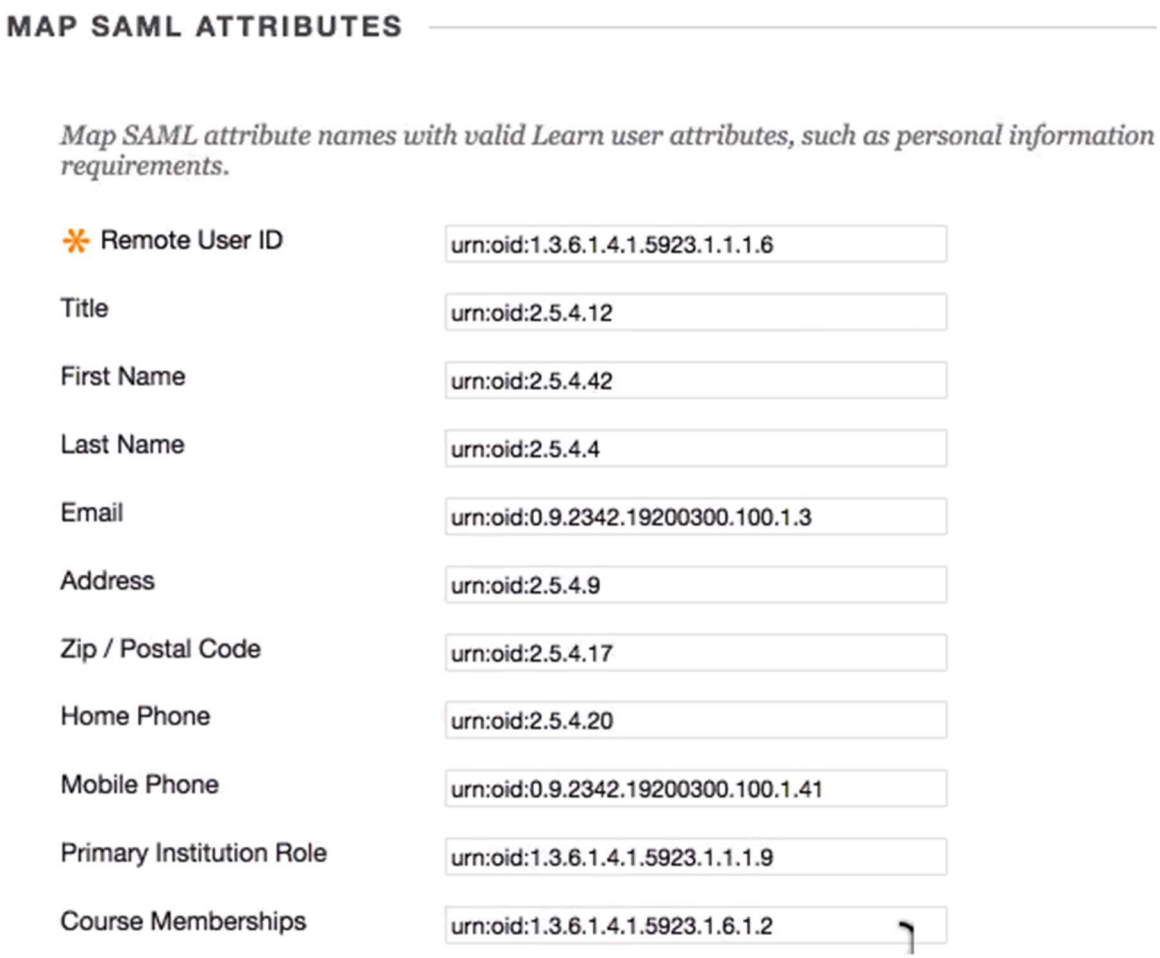
- Login to Degreed as an administrator and navigate to System Admin > Authentication.
- Select Create Provider > SAML.
- Enter the following settings:
- Name > Type OneLogin or anything you want.
- Authentication Provider > set as Active.

- User Lookup Method > Username
- Restrict by Hostname > Use this provider for any hostnames.
- Link Text > Type OneLogin login or anything you want.
- Select Save and Configure.
- In the ACS URL field value, grab the subdomain and apply it in the "subdomain" field in the Configuration Tab of the app connector in OneLogin.



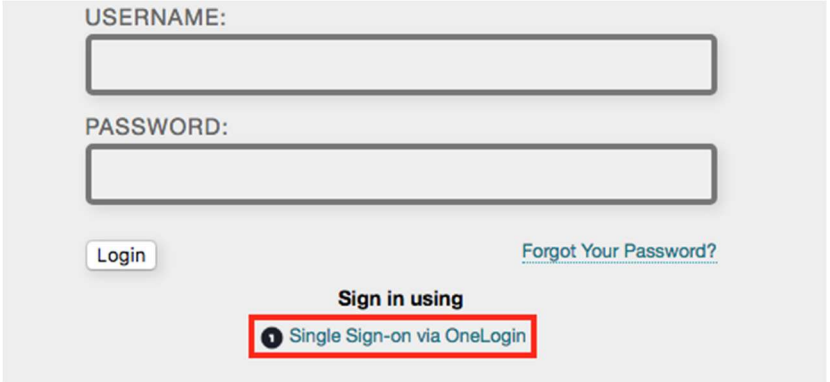
1. In the Entity ID field, enter "OneLogin".
2. It is recommended to create a new Data Source for this provider named SAML or OneLogin, otherwise use SYSTEM or whatever you choose.
3. Select the Enable JIT Provisioning checkbox to allow the system to automatically create an account when an unknown user attempts to login via this SAML authentication provider. If it is not selected, the user account will first need to be manually created in Degreed.
4. Select a Data Source for this authentication provider. The data source is the source of accounts that are provisioned by this authentication provider. The default value is Internal. It is recommended that you create a specific data source for use with a SAML authentication provider.
5. In the Compatible Data Sources list, be sure to select the data sources that this authentication provider should be compatible with.
6. Select SAML Identity Provider for the Identity Provider Type.
7. For the Identity Provider Metadata, use the Issuer URL from step 10 in the "Configure OneLogin" article above and launch that in a browser to download the XML file and use it to upload it to the Upload Metadata section by clicking Browse.
8. Note: in the XML file, you will need to update SingleLogoutService URL (typically line 36) to the value of your OneLogin portal, e.g. https://{yoursubdomain}.onelogin.com/client/apps

9. On the "SAML SAML Attributes section, leave the Remote User ID value selected, remove all others if you do not plan to send these values over. If you do, make sure to add these as custom parameters in OneLogin:



Apps>Company Apps>Degreed>Parameters Tab:

- To obtain the login URL to load into OneLogin, go to your custom Degreed site and copy the "Single Sign-on via OneLogin" hyperlink and past it in the Login URL.
-



7. Test the SAML Connection

Test the SAML connection.

- Ensure that you have user accounts in both OneLogin and Degreed that use the same value as the username.
- You can create a test user, or you can use your own account if you choose.
- Make sure you are logged out of Degreed.
- Log into OneLogin as an admin and give the test user access to the Degreed app in OneLogin.
- Log into OneLogin as the test user.
- Click the Degreed icon on your OneLogin dashboard.
- If you are able to access Degreed, then SAML works.