

Student Learning & Licensure

SAML SSO

Single Sign-on using SAML Protocol



Contents

Background and Prerequisite Steps



User Workflow



Student Learning & Licensure
Admin Configuration



FAQ



Background and Prerequisite Steps

- ▶ All Student Learning & Licensure accounts must be created prior to user login and it is highly recommended that the SSO_UID is supplied. The SSO_UID is based on the UID attribute.
- ▶ The university-specific URL can be referenced in the LMS, Portal, etc. and allow for seamless transition to Student Learning & Licensure.
- ▶ Student Learning & Licensure authentication is the only access. The removal of a user on the institution's side does not remove the user from Student Learning & Licensure.
- ▶ Student Learning & Licensure accounts are not created using the SAML integration.

User Workflow

- ▶ Click or visit redirect page for Student Learning & Licensure .
- ▶ If necessary, log in using University credentials.
- ▶ Access Student Learning & Licensure and arrive on "In Progress" page.

Authentication and Communication Workflow

- ▶ Student Learning & Licensure requests login page from IDP and includes callback information.
- ▶ IDP checks login status and if necessary, authenticates user.
- ▶ After login, IDP calls back with HTTP. Get request to Student Learning & Licensure including the token containing the User's ID.
- ▶ Student Learning & Licensure matches the UID to a known Student Learning & Licensure user.
- ▶ Upon successful match, user is logged in and shown the "In Progress" page in Student Learning & Licensure .

Student Learning & Licensure Admin Configuration

- ▶ Within the Top Level Admin account for your Student Learning & Licensure Organization, click on **Settings**.
- ▶ Click the **SSO Configuration tab**.
- ▶ Click **Edit** in the upper right corner of the SSO Configuration box.
- ▶ Select **SAML** as the strategy
- ▶ Enter in your **IdP URL**.
- ▶ Enter in the [Certificate Fingerprint](#).
- ▶ Enter in the **UID attribute**.
- ▶ Enter in the **SP URL** -
https://sl.watermarkinsights.com.
- ▶ Click **Save**.

The screenshot shows the 'Single Sign On' configuration page in the Watermark Student Learning & Licensure Admin interface. The page title is 'Single Sign On' and it includes a sub-header: 'Enter and complete protocol requirements to activate Single Sign On (SSO) for your users. All Watermark Student Learning & Licensure accounts must be created prior to user login.'

The configuration fields are as follows:

- Organization Login URL:** [Copy](#)
- Protocol:**
- IdP URL:**
URL of your SAML Server
- Certificate Fingerprint:**
The SHA1 fingerprint of the certificate. The certificate is provided by the identity provider.
- UID Attribute:**
The attribute that identifies the user. For example: EPPN, UID
- Service Provider URL:**
This URL is customized to represent the look and feel of your organization

At the bottom of the form, there is a link: 'Please refer to our SAML guide to learn more about the protocol, process and FAQs.' and two buttons: **ACTIVATE** and **CANCEL**.

The footer of the page contains: © 2022 Watermark Insights, LLC and its affiliates. All Rights Reserved. | [Privacy Policy](#) | [Accessibility Policy](#) | [Customer Support](#)

Generating the Certification Fingerprint

Generating the fingerprint on a local machine

- ▶ To generate the fingerprint, use the IdP X509 certificate file. This should be a .crt file.
- ▶ Copy the .crt file to a Linux-based machine (this works on a Mac) and run the following command from the command prompt.
- ▶ If the X509 certificate is called idp-signing.crt, it would look like this:

```
openssl x509 -noout -in idp-signing.crt -fingerprint
```

- ▶ The above command will generate the fingerprint.

Generating the fingerprint online

- ▶ The fingerprint can also be generated at this website: <https://www.samltool.com/fingerprint.php>
- ▶ Copy and paste the contents of the X509 file and the site will generate the fingerprint.