Student Learning & Licensure SAML SSO

Single Sign-on using SAML Protocol

watermark

Contents

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

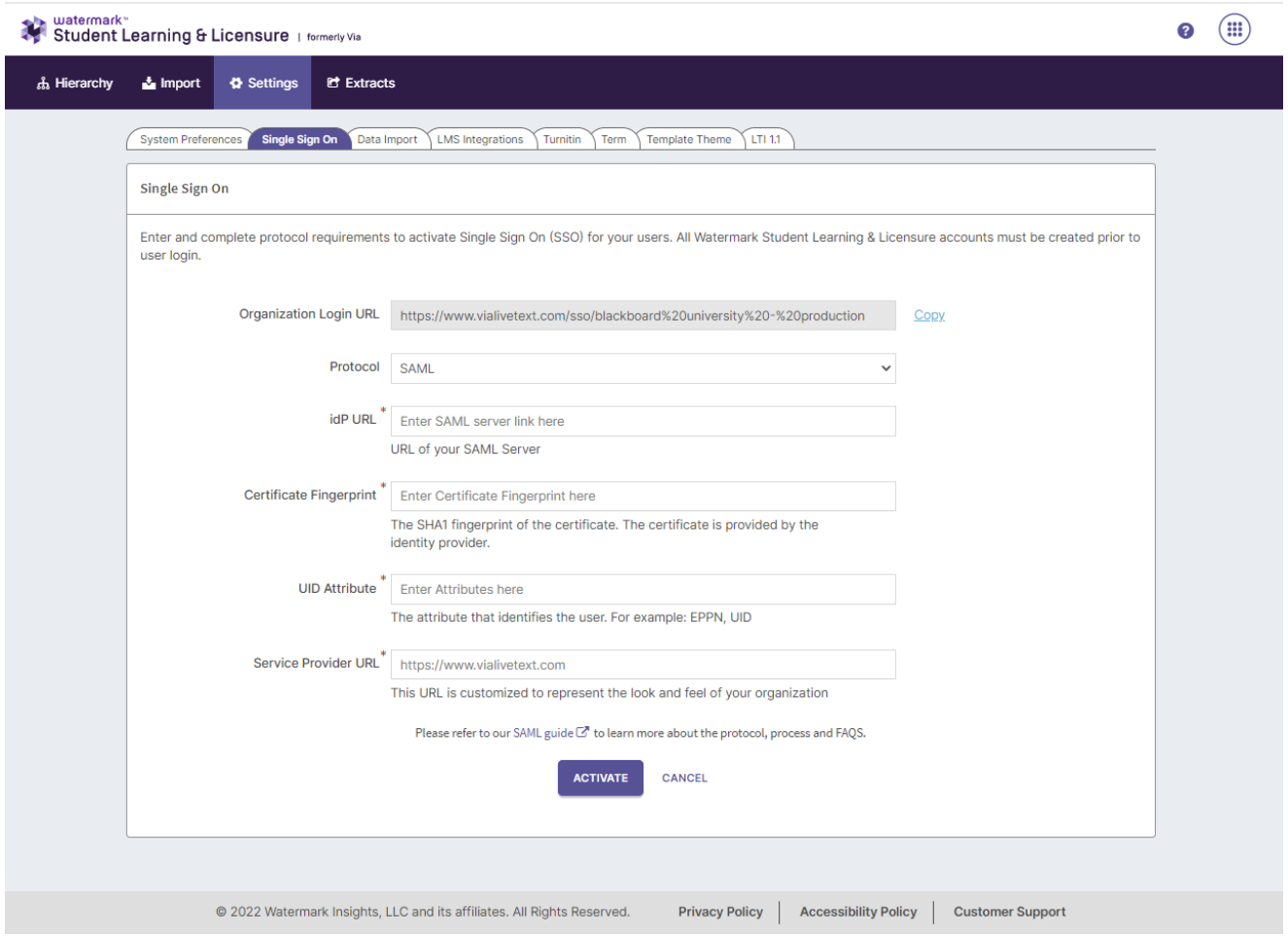
- Click or visit redirect page for Student Learning & Licensure .
- If necessary, log in using University credentials.
- Access Student Learning & Licensure and arrive on “In Progress” page.

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://sll.watermarkinsights.com**.
- Click **Save**.



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.