Upswing

Upswing Technical Guide for Partners – SSO, SAML

The following steps are required to integrate Upswing with your SAML Identity Provider. Requested information is to be provided to your HERO.

SAML Integration Instructions

1. Exchange SAML metadata
    a. Provide the following information in your metadata:
        i. EntityDescriptor information
            1. entityID
        ii. IDPSSODescriptor information:
            a. SingleSignOnService
                - Upswing supports either Redirect or POST bindings
            b. SingleLogoutService
                - Upswing requires a SingleLogoutService, we support either Redirect or POST bindings
                - This may be the same Location as the SingleSignOnService
            c. KeyDescriptor for public signing key
        iii. Claims: Upswing requires equivalent claims for the following user directory information
            d. **First name** (e.g., givenName, firstName etc.)
            e. **Last name** (e.g., sn, lastName, etc.)
            f. **Email** (e.g. mail, email, etc.)
            g. **Unique ID** (e.g. employeeNumber, userPrincipalName, email, etc.)
                - A unique identifier, most commonly a student/employee ID number, or if none is provided, email address may be used.
    b. Upswing will send corresponding Service Provider SAML Metadata within <XML metadata generation SLA> business days.

2. Create a test account for Upswing's use and provide the username and password to Upswing.
    - This account must have all of the directory information from 1(a)(ii) above populated. *Note: fake values are accepted.*
    - This is currently required for Upswing to verify that the SSO integration is configured correctly prior to launch

*If you are using ADFS, an additional step is needed to enable Upswing's self-signed certificate. The following two commands will need to be run using PowerShell on the ADFS server:

```
Set-ADFSRelyingPartyTrust –TargetName "Upswing" –EncryptionCertificateRevocationCheck "None"
Set-ADFSRelyingPartyTrust –TargetName "Upswing" –SigningCertificateRevocationCheck "None"
```

These commands disable ADFS from checking the revocation status of Upswing's self-signed certificates. If these revocation checks are not disabled, a "SAML Responder Error" will occur preventing logins.

*If you are using Okta, an additional step is needed to enable Upswing's self-signed certificate. You will need to enable advanced settings in Okta and provide the certificate file. Single Logout (SLO) should also be enabled. This certificate can be found in the Onboarding Kit.

SAML Checklist

The checklist below is a great item to have at hand when confirming correct set-up of your SAML connection with Upswing:

- ☐ Have you completed all the above listed steps?
- ☐ Is your reply URL correct?
- ☐ Are you sending all of the attributes?
- ☐ Are the attributes sending correctly?
- ☐ If you are seeing an error, is your firewall preventing the connection?
- ☐ Have the students at your institution been granted access to the Upswing application via your SAML system?

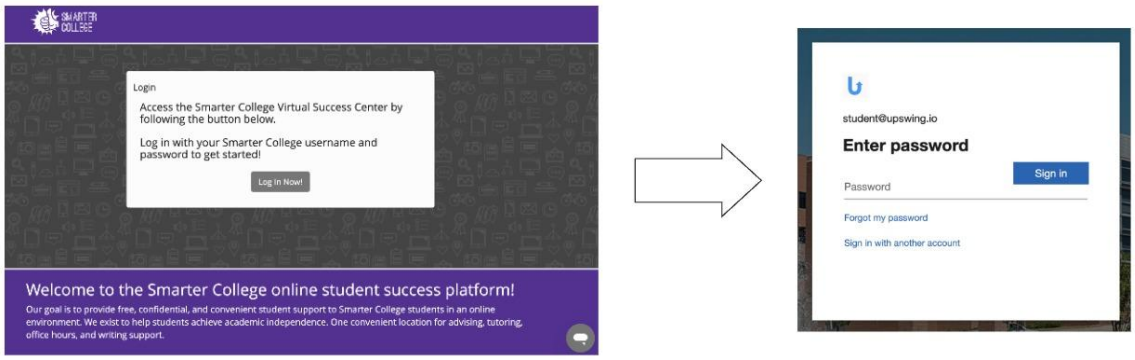
Personally Identifiable Information (PII)

The following directory information is stored by Upswing through SAML integration:

- User Email
- User First Name
- User Last Name
- School User ID

Workflow

The following workflow is followed by users through SAML integration:



Upswing will create a login page for your school. This page will have a button that will redirect to the school's SAML login form. Once the student completes the form with their credentials, they will be redirected to Upswing and be shown their home dashboard.

Service Level Agreements (SLAs)

Service level agreements define shared expectations between Upswing and our partners. For the SSO integration, partners can expect that:

- If all metadata and test credentials are received, Upswing will set up and validate the SSO integration within 15 business days.

Exceptions

- If the data is not received by the agreed-upon date, the request will be reprioritized and Upswing may not meet the above SLAs.

- Upswing's data validation process checks for missing information and patterns in the data provided. It is not possible for Upswing to fully validate the data or the configuration until the SSO implementation process is complete. If the data is found to be invalid during the implementation process and Upswing is unable to successfully get assistance and/or new data from your team, then the data submission cycle may need to be restarted.

- If valid test credentials (username and password) are not provided, you may experience longer implementation times. Without test credentials, it will also be difficult for Upswing to help troubleshoot any log-in issues after implementation.

Change Management Expectations

Once the Upswing platform is integrated with your single sign-on infrastructure, Upswing must be included in your change management plan for your SSO solution. For instance, if changes are made to the Unique ID format or any required SAML metadata, it is your responsibility to communicate these changes to your HERO **ahead of the changes taking place** so that the update can be coordinated with Upswing. Not doing so is likely to result in an interruption of service.

Uptime SLAs cannot be guaranteed if the platform is unavailable due to a change in your single sign-on configuration without having priorly informed and coordinated with Upswing's team. Please keep in mind that changes to SSO integrations cannot be made on short notice. To avoid any interruptions in service for your students, please inform Upswing of any changes that will occur with your SSO integrations at least 3 weeks in advance.

Data Retention Standards

Upswing adheres to data retention standards in accordance with the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).