Upswing

Upswing Technical Guide for Partners – SSO, LDAP

The following steps are required to integrate Upswing with your LDAP server. Requested information is to be provided to your HERO.

LDAP Integration Instructions

1. Provide field names for the following properties
   a. **Username/User ID attribute** (ex: userPrincipalName, sAMAccountName, mail)
   b. **First name** (e.g., givenName, etc.)
   c. **Last name** (e.g., sn, etc.)
   d. **Email** (e.g., mail, email, etc.)
   e. **Unique ID** (e.g., employeeNumber, userPrincipalName, etc.)

2. Provide LDAP server connection information:
   a. **LDAP SSL server address**
   b. **LDAP SSL port**
   c. **LDAP service account credentials for Upswing** (username and password)

3. Provide user account base DN (e.g., DC=school,DC=local)

4. Provide user account filter string, e.g.,

(&(objectCategory=person)(objectClass=user)(|(sAMAccountName={0})(mail={0})))

5. Create a test account for Upswing's use and provide the username and password to Upswing
   ● This account must have each of the above attributes/fields from 1(a) above populated. *Note: fake values are accepted.*

6. Allow these IP addresses access through your firewall for the LDAP SSL port:
   ● Upswing Test Servers: 108.59.85.162
   ● Upswing Production Server: 104.154.51.38

Checklist

The checklist below is a great item to have at hand when confirming correct set-up of your LDAP connection with Upswing:
☐ Have you completed all the above listed steps?
☐ Do your users have all the required fields populated?

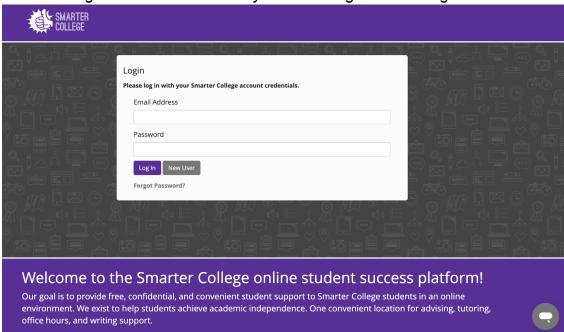### Personally Identifiable Information

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

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

Workflow

The following workflow is followed by users through LDAP integration:

For LDAP integrations, students and college faculty are able to access the Upswing system simply by logging in using their college credentials on the Upswing portal.

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).