Single Sign-On Integration

## Summary and Introduction

The purpose of this document is to define the YourCause standard for Single Sign-On (SSO) integration and to capture relevant client configuration data.

**The first section** outlines the YourCause standard.

**The second section** includes a configuration checklist, which captures details regarding the SSO configuration from the client.

Please read the first section carefully, then fill out all applicable sections in the configuration checklist below.

# Single Sign-On Configuration Specifications

# Introduction

This document is intended to describe the YourCause SSO services for web integration, as well as how to implement SAML integration.

# Overview

The YourCause application, which uses SAML 2.0, is configured to perform an HTTP Redirect or HTTP Post to the client SSO login page for authentication. If the client SSO application page recognizes that the user already has an active SSO session, it can redirect the user to the YourCause SSO Assertion URL with a signed SAML 2.0 token.

Once the user is verified, the user is logged into the YourCause application. If the user is not found or if the user’s account is not active, an error message is displayed to the user containing information on how to contact YourCause support.

# Supported SSO Providers

YourCause can support any SAML 2.0 compatible SSO Provider. Some common providers are:

## Okta

1. Microsoft Azure/ADFS
2. Ping Identity/Ping Federate
3. One Login
4. Salesforce
5. IBM
6. Google

# Supported SSO Types

YourCause can support two types of SAML 2.0 configurations: SP-initiated or IDP-initiated. YourCause prefers SP-I since it works better with deep links received via messages generated from the YourCause platform or emails.

In these integrations, the YourCause application is the Service Provider (SP) and will look for user identity from the Client (IDP) federation services.

1. **IDP-Initiated**

In this scenario, the user clicks on a link on the internal client portal. That link is configured to send a SAML token to YourCause containing the identity of the user.

## **SP-Initiated (preferred)**

In this scenario, the user comes to the YourCause application first via a direct YourCause URL (for example: https://<*ClientName*>.yourcause.com). At this point, if the user is not already logged in, the YourCause application will send a signed AuthnRequest and will expect a signed SAML Response in return.

\* This setup will typically support IDP in the background as well.

# Supported SSO Types cont.

1. **OIDC**

OpenID Connect lets developers authenticate their users across websites and apps without having to own and manage password files.

1. **Auto Provisioning**

Just in Time Provisioning is available for clients. The YourCause application only requires four attributes, but recommends additional attributes be mapped to optimize user experience (such as Zip or Postal Code).

# Environments

YourCause supports two environments for SSO connectivity: UAT and Production. The UAT environment will continue to exist after Production is set up for future use and testing.

The YourCause application will include “uat” as part of the URL for those URLs specific to the UAT environment (for example: https://<ClientName>.yourcauseuat.com).

# Metadata

1. **Outbound**: YourCause will provide metadata files for both the UAT and Production environments.

\*Any future changes will be communicated with new metadata files.

2. **Inbound**: YourCause can accept metadata files to set up both environments.

\* For IDP-initiated configurations, we will also need the IDP link for redirection.

\*Any future changes will need to be communicated with new metadata files.

# Encryption

Encryption is supported for the SAML Attribute in the SAML Response. YourCause will provide an encryption certificate as part of the metadata file.

# SAML Requirements

1. The SAML token should contain a signed response or signed assertion. YourCause supports SHA1 and SHA256 for signing certificates.
2. The signing certificate should be the same as what is shared with YourCause.

\* Any changes to the signing certificate will need to be coordinated with YourCause before the certificate changes or expires to avoid SSO downtime.

# Attributes Required in SAML

The only attribute required in the SAML token is the subject NameID, which contains an attribute shared in the HR data file provided to YourCause. Once verified, the YourCause application will compare the NameID to the value from the SSOID Column on the HR file.

All other attributes are optional and are not used unless Auto Provisioning (Just in Time) is selected. See checklist for details.

# Auto-Provisioning

CSRconnect and GrantsConnect are able to support SAML auto-provisioning of accounts using data supplied in claims. The available attributes are listed below in the mapping table. This method replaces an HR file and is not able to be used in tandem with an HR file.

Please note that auto-provisioning does NOT support the following functionality:

* Deactivation of user accounts upon termination (must be controlled by client)
* Segmentation
* Payroll
* Historical data imports
* Complex match program filtering (simple filtering may be available but must be reviewed by the Implementation team)

# Configuration Checklist

**Client Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. HR column name used as NAMEID field: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. SSO Type / Basic Login (check all that apply)
   * IDP-initiated SSO
     + UAT IDP link : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     + Prod IDP link: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   * SP-initiated SSO
     + Is response encrypted:  Yes  No
   * OIDC
   * Auto-Provisioning
     + Enter value that will be mapped to employee First Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     + Enter value that will be mapped to employee Last Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     + Enter value that will be mapped to employee External Employee ID:
     + \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     + Enter value that will be mapped to email address:
     + \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Basic authentication login
   * + SSOID Value for Basic Authentication\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     + Temporary Password Formula \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     + Employee types using basic authentication:

* Employees
* Retirees
* Contractors
* Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Is metadata XML file available?
   * Yes - Please send metadata files for UAT and Prod to your Implementation Manager
   * No
     + SSO links (if IDP: same as link above; if SP: link for SSO service)
       - UAT: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
       - Production: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     1. Certificate Files (please attach here or to an email with this document)
        + UAT: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
        + Production: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
        + Date of Certificate Expiration: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Attributes Available for mapping via Auto Provisioning

|  |  |  |
| --- | --- | --- |
| FirstName | First name of employee. | Mapping Value |
| LastName | Last name of employee. |  |
| Email | If you do not have email addresses for all employees, YourCause has a preferred email capture. Please discuss this with your Implementation Manager. |  |
| EmployeeID | Employee ID of employee. Must be unique and non-changing, even upon rehire. |  |
| Date of Birth | Employee date of birth |  |
| Salary | Salary of employee. Only used for the optional percent salary feature in payroll giving. |  |
| Region | Region of employee. Ex: North America, Asia. Used for reporting. |  |
| ManagerEmployeeID | Manager's employee ID. Used for reporting. |  |
| PayCurrencyCode | Three-digit Currency Code |  |
| PayPeriods | Numerical value of number of annual pay periods for an employee. Default is 24. (Ex: 12, 24, 26, 52) Required if Payroll feature is used. |  |
| PayrollCenter | Payroll center for employee. Used for reporting. |  |
| PayrollID | Payroll ID for employee. This value must be sent if the payroll ID required for payroll files differs from the employee ID. |  |
| ZipCode | Employee work zip code. This will be used as the primary zip code in the system. If another zip code should be considered as the primary zip, it must be mapped to this field. Used to calculate search radius in Volunteering. |  |
| Country | Employee country code. 2-digit ISO code is required. (Ex: US instead of United States or USA). If no value is sent, will be defaulted to US for all users. |  |
| WorkAddress1 | Employee work address line 1. |  |
| WorkAddress2 | Employee work address line 2. |  |
| WorkCity | Employee work city. Used to calculate search radius in Volunteering. |  |
| WorkState | Employee work state. Can be two-digit code or full name. Used to calculate search radius in Volunteering. |  |
| MailStop | Employee mail stop. Used for reporting. |  |
| HomeAddress | Employee home address line 1. Used for reporting. |  |
| HomeAddress2 | Employee home address line 2. Used for reporting. |  |
| HomeCity | Employee home city. Used for reporting. |  |
| HomeState | Employee home state. Used for reporting. |  |
| HomeZipCode | Employee home zip code. Used for reporting. |  |
| HomeCountryCode | Employee home country code. 2-digit ISO code is required. (Ex: US instead of United States or USA). Used for reporting. |  |
| HireDate | Employee hire date. Used for reporting. |  |
| Division | Employee division. Used for reporting. |  |
| Market | Employee market. Used for reporting. |  |
| BusinessUnit | Employee business unit. Used for reporting. |  |
| JobCode | Employee job code. Used for reporting. |  |
| ShiftCode | Employee shift code. Used for reporting. |  |
| EmployeeType | Employee employee type. Used for reporting. |  |
| EmployeeSubTypeCode | Employee employee sub type code. Used for reporting. |  |
| EmployeeStatus | Employee employee status. Used for reporting. |  |
| SubCompanyCode | Employee sub company code. Used for reporting. |  |
| SiteCode | Employee site code. Used for reporting. |  |
| FullTimeTemp | Employee full time temp. Used for reporting. |  |
| PayrollType | Employee payroll type. Used for reporting. |  |
| PayrollFilter | This is used to segment payroll. Consult with your Implementation Manager or Account Manager to determine the values for this column. Each payroll file that is sent will require a separate value for this field.  (Ex: US employees only should have payroll, so they should have a US value here. Or if Company 1 and Company 2 are handled by separate payroll teams, we'll need the value for Company 1 or Company 2 in this field.) NOTE: If using this field, it will be mapped to Custom1. |  |
| MatchType | Used to filter users to different match caps, such as 1= $5,000 2= $7,000 or 1= match eligble, 0= not match eligible |  |
| CustomSegment | This is used to filter employee populations into unique experiences in the platform. Consult your Implementation Manager to determine if this feature is needed. |  |