Getting Started with Single Sign-On

I. Introduction

Your institution is considering or has already purchased Collaboratory® from Treetop Commons, LLC. One benefit provided to member institutions is Single Sign-On Integration (SSO), an access control method that eliminates the need for creating and managing a separate account in Collaboratory. This document provides Information Technology administrators with the procedures necessary to implement the SSO process for your institution's network.

What is Collaboratory®?

Collaboratory® connects and enhances campus-wide information about and support for community engagement relationships, resources, activities, and outcomes. Faculty, staff and invited students can document and display their engagement and public service activities in a web-based, centralized hub, whether providing direct services at a nonprofit organization, teaching professionals and residents of a community, or conducting research collaboratively with community partners.

II. SSO/SAML Overview

The Benefits of Single Sign-On (SSO)

Users benefit from a simple and unified access method across multiple or disparate networks. This means interoperability, automation, and the seamless use of an SSO policy to reduce the burden of multiple account authentication processes. With SSO, only the existing credentials of an institution will be necessary for users while eliminating the need for creating and managing a separate Collaboratory account.

In order to offer SSO within your institution, Collaboratory embraces **Security Assertion Markup Language (SAML 2.0). SAML** is an XML-based format for exchanging authorization data between systems. It's widely adopted in private enterprises worldwide and considered the first choice for managing SSO authentication, due to its flexible configuration, multiple platform support, and ability to interoperate with widely used core protocols and authentication methods.

Regardless of SAML's rapid adoption, every system is different. There is always customization involved depending on the architecture, protocol, and mechanisms used by your institution. Our team is dedicated to working within your parameters, laying the groundwork for a seamless SSO implementation. For this process, we've setup two SAML components: a SAML-based registration and a SAML-based login.

You can learn more about SAML by viewing the official Security Assertion Markup Language website. This provides a complete overview of SAML's requirements, specifications, and deployment profile.

III. Next Steps for Implementation

Before implementing SSO, we require information about your organization's current system. This consists of two steps:

1. Complete the SSO Initial Assessment Help which you can access here.

   In *IV: SSO Initial Assessment Help*, we'll walk you through this questionnaire and clarify what's required.

2. Email develop@cecollaboratory.com with information specified in *V: SAML2 Identity Provider Setup*.

To assist in the information collection process, we've included two additional sections:

VI: Collaboratory SSO Flowchart - Provides a graphical representation of the SSO authentication process for previously established and newly linked accounts.

VII: Reference - Includes helpful definitions, links, and metadata for the SSO/SAML2 implementation.

IV. SSO Initial Assessment Help

This section provides an overview of each question asked within the SSO Initial Assessment Questionnaire. As you enter data into the online form, please use this document as a reference. It will help frame any relevant information required and help expedite your SSO implementation.

Basic Information

Q.1: Enter the name of your institution.

Q.2-Q.4: Provide us with the contact information for your IT Manager or SSO Project Team Leader.

System Information

Q.5: Provide the IdP (Identity Provider) solution currently in use by your institution.

Q.6: Help us determine if your system is capable of federation with external systems. This information is typically provided by your software partner or vendor.

Q.7: List all supported federations, solutions, protocols used by your institution. Please include all current versions as well as future versions, upgrades, or platform changes planned within the next 90 days. In order for TreeTop to implement SAML, we will need to understand protocol information such as authentication context, attributes, and bindings. Collaboratory supports a variety of solutions for the SAML protocol such as **LDAP, Shibboleth, ADFS, and PingFederate.**

Q.8: Help us identify your preferred protocol. We understand that our clients use different technologies. We have designed Collaboratory to pass an array of attributes during the authentication process.

Q.9: Provide us with all necessary account information used during the federation process. By default, Collaboratory receives basic account information such as *first name*, *last name*, and *email and* can be customized to accommodate additional data when necessary such as *date of birth*, *gender*, and *ethnicity*. An API is required to dissociate federated logons. This is typically provided by your current software partner or vendor. Regardless, our team will be on hand to understand and plan API specifics with you.

Q.10: Inform us of the steps your institution requires us to complete to become an official service provider.

Q.11: We require a test environment used as a staging area for dummy accounts that will simulate and verify authentication flow. We can work with simple test accounts or full production environments.

Additional Information

Q.12: Briefly explain the primary security concerns shared within your institution. Security is always an important component to us, especially the authentication process. At TreeTop Commons, we take all security concerns seriously and will adhere to any institutional standards required during the entire project cycle.

Q.13: Provide us with any internal support documentation that can help us work more effectively to implement SSO or that will clarify any potential incompatibilities.

Q.14: Include example data fields or headers that we can use for reference, especially within the test environment.

Q.15-Q.16: To help streamline the SSO implementation process, please define your role, as well as that of participating team members, along with their contact information.

Q.17: Help us define your preferred timeline for rolling out Collaboratory at your institution.

*When complete, please select **Submit questionnaire** at the end of the online form and proceed to* **IV: SAML2 Identity Provider Setup**

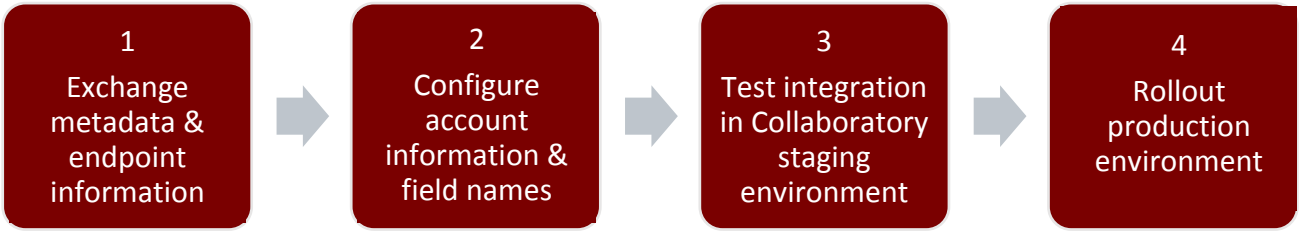
V. SAML2 Identity Provider Setup

Now that you've completed the SSO Initial Assessment Questionnaire, the next step is to send an email to us at develop@cecollaboratory.com to begin our four step process for your SAML2 setup and configuration.

For the implementation of SSO, we assume that your institution will already have an Identity Provider (IdP) and that users have an existing account (Principal Identity) with that specific IdP.

SAML2 SSO Timeline Synopsis

In order to set your institution up as a SAML2 Identity Provider, our team will perform the following:



1. **Exchange metadata and endpoint information with your team.**

   Send an email to develop@cecollaboratory.com providing us with:

   - The IdP metadata, certificate or fingerprint information
   - Single logon endpoint credentials
   - Entity ID
   - Please inform us if messages are digitally signed

2. **Configure the account information & field names you're able to provide.**

   When a user authenticates with IdP, a federated identity must be created in the Collaboratory system. This entails a process within Collaboratory that establishes the account using the Principle Identity provided by the IdP.

   While Collaboratory's SSO requires several basic attributes from the assertion within the authentication response, additional attributes can be used to establish a more detailed user profile.

The table titled **Attribute Table** on the next page identifies and defines the expected attributes, mapping them to two common Identity Providers for your reference.

Attribute Table

Attribute	Required	Shibboleth	PingFederate
uuid	FALSE	eduPersonTargetedID	<varies>
email	TRUE	eduPersonPrincipalName, mail	email
firstname	TRUE	givenName	firstname
lastname	TRUE	sn	lastname
over13	TRUE	<n/a>	over13
affiliation	FALSE	eduPersonAffiliation	<n/a>
birthdate	FALSE	<n/a>	birthdate

Note: *The requirement on the* **birthdate** *and* **over13** *attributes are mutually exclusive. If* **birthdate** *is provided, then the* **over13** *attribute does not need to be provided, and vice-versa.*

Continue to next page

Below is an example set of acceptable attributes:

```
 <saml:AttributeStatement xmlns:xs="http://www.w3.org/2001/XMLSchema">!
 <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
 basic" Name="over13">!
 <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
 xsi:type="xs:string">Y</saml:AttributeValue>!
 </saml:Attribute>!
 <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
 basic" Name="email">!
 <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
 xsi:type="xs:string">user@institution.edu</saml:AttributeValue>!
 </saml:Attribute>!
 <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
 basic" Name="lastname">!
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
 xsi:type="xs:string">Smith</saml:AttributeValue>!
 </saml:Attribute>!
 <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
 basic" Name="firstname">!
 <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
 xsi:type="xs:string">John</saml:AttributeValue>!
 </saml:Attribute>!
 </saml:AttributeStatement>!
```

3. Deploy and test integration in Collaboratory staging environment.

A. Test SP-initiated logins and account claiming.

B. Test IdP-initiated logins and account claiming.

We will communicate with your team during this phase to ascertain what's necessary and/or available for using as a test environment and credentials within your institution. A security analysis and deployment schedule will also be discussed, helping us understand when we can begin.

4. Rollout our production environment.

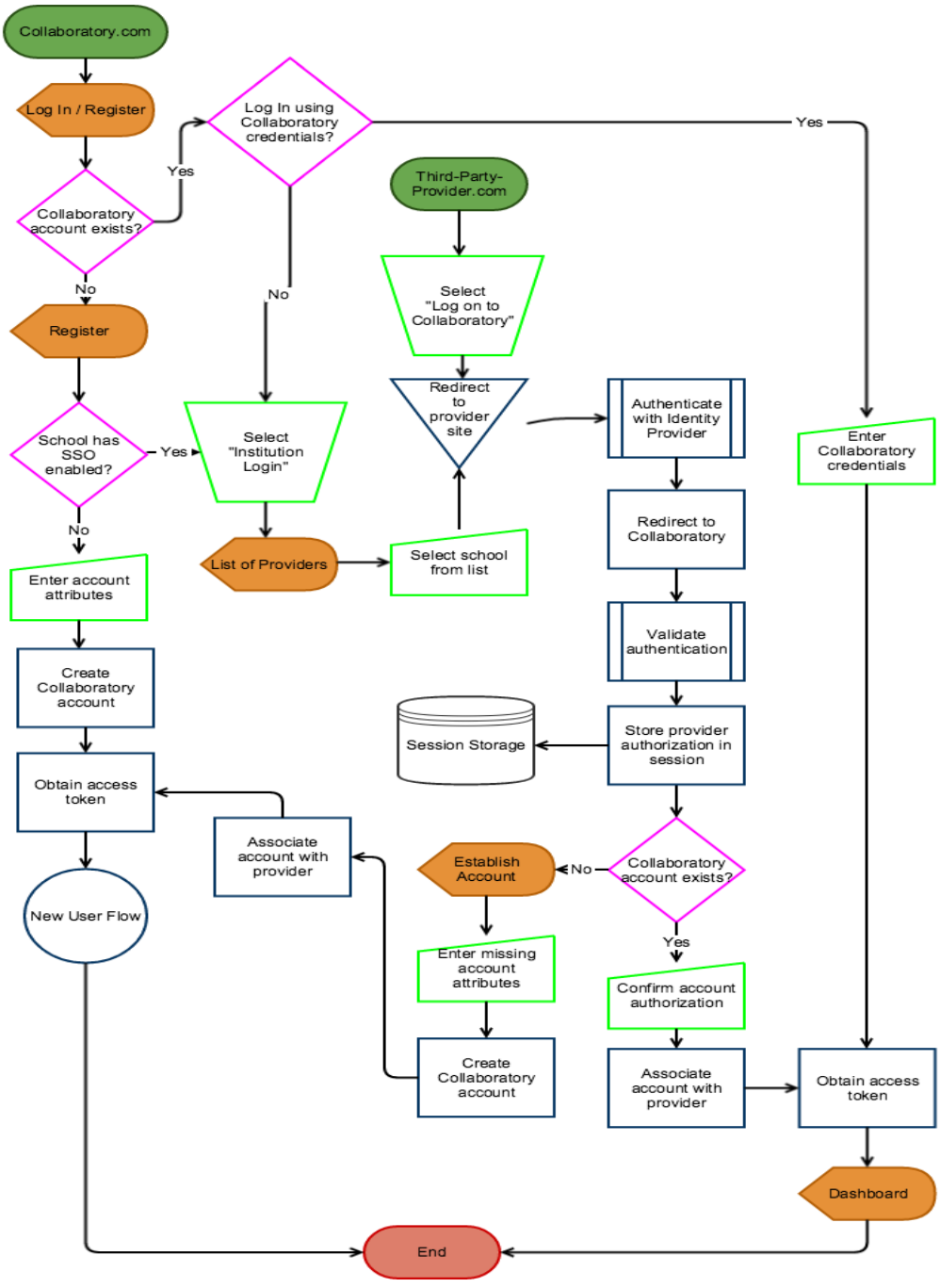
We will configure your Identity Provider (IdP) with your portal.

SSO Implementation Complete!

Once everything has been provided to us, we'll get started with the implementation. Upon completion, we'll inform your portal administrator. The portal administrator can then invite users to log-in to Collaboratory with your institution's credentials.

VI. Collaboratory SSO Flow Chart

Provides graphic illustration of the SSO authentication process for both existing and newly linked accounts.



VII. Reference

This section details important definitions you should become familiar with, along with links to help configure your Identity Provider.

SSO Primary Definitions

These definitions lay the groundwork for understanding Collaboratory's SSO implementation.

Single Sign-On (SSO) - A process enabling a user to log in once and gain access to related systems without being prompted to log in again at each of them.

Security Assertion Markup Language (SAML) - XML-based data format for exchanging authentication and authorization data between systems.

Identity Provider (IdP) - This is a module that creates, maintains, and manages identity information. IdP will also provide authentication to their service providers within a federation.

Service Provider (SP) - System entity providing services to users or other system entities.

Federation - An association composed of any number of service providers and identity providers.

System Entity - An active element of the system with a distinct set of functionality.

Identity - An entity described by attributes and unique data objects.

Principal - A system entity whose identity can be authenticated.

Principal Identity - A representation of a principal's identity as a unique data object (i.e., *User Account*).

Metadata

1. Our staging environment metadata can be found here.
2. Our production environment metadata can be found here.

Links

Links to help you in the configuration of popular identity providers.

SAML: http://saml2int.org/profile/current

LDAP: http://msdn.microsoft.com/en-us/library/aa367008%28v=vs.85%29.aspx

PingFederate: https://www.pingidentity.com/en/products/pingfederate.html

Shibboleth: http://shibboleth.net/

ADFS: http://technet.microsoft.com/en-us/library/cc736690%28v=WS.10%29.aspx

collaboratory
Track • Report • Connect • Plan

Revision History

11.4.2015	Document approved for circulation.

TREETOP
COMMONS