Authentication Integration Worksheet

For any questions or assistance, please contact:
Authentication@CampusLabs.com
716-270-0000

campuslabs
Data Driven Innovation

08-20V4

Authentication Method

Please note that ALL campus community members will need to have access to your site. This includes students, faculty, and staff. Make sure that the information you provide will allow all of these users to access the site.

Campus Labs only supports ONE campus authentication method at a time.

Important Note

Campus Labs requires that the selected authentication method must return a unique, never-changing, and never-recycled Person Identifier for each user upon a successful sign in. Please refer to our documentation on *Choosing a Person Identifier* for guidance.

Review and Complete the Appropriate Sections Listed Below

- Contacts **(3)**
- Unique Identifier Selection Checklist **(3)**
- Authentication Method **(1)**
- Shibboleth/SAML **(5)**
- Steps to implement a Shibboleth/SAML authentication **(5)**
- Test Account Information **(7)**
- Central Authentication Service (CAS) **(10)**
- CAS URLs **(10)**
- Test Account Information **(10)**

Authentication Contacts (Required)

Primary Contact

Name

Title

Phone #

Email Address

Secondary Contact

Name

Title

Phone #

Email Address

Unique Identifier Checklist

The unique identifier is the value stored for each user by Campus Labs. Ideally, this identifier will be unique, immutable, and human-readable so that it will not change over time for each user. Please reach to us if you have any concerns regarding your institution's available identifiers meeting these criteria.

Required Parameters to Complete Setup

□ **Locally Unique:** Different than the rest of the identifiers in local authentication database

□ **Immutable:** Doesn't change throughout the lifetime of the user account

□ **Human Readable:** Intelligible for reporting and troubleshooting purposes (no ambiguous 32-digit GUIDS)

Recommended Parameters

Required When Possible

□ **Globally Unique:** Likely different than the rest of the identifiers in global database (e.g. user@school.edu)

□ **Independent of Role:** Formatting consistent across varied campus roles (doesn't change if role changes?)

□ **Appropriate for site admin use:** Easily accessible to populate and safe for viewing by site admins

Questions for Consideration

Required When Applicable

Does the site administrator have access to identifier outside of the application?

□ **Yes:** Good. They will need this to create and/or manage accounts

□ **No:** Please coordinate any required internal business processes to ensure they can obtain this information

Do identifiers have the potential to change for any of the following reasons?

□ We are planning to change our authentication method. More details and estimate of change timeline are described below.

□ Other

Please provide details about the potential change.

What identifier are users using for reporting, sorting, etc.?

What is the system of record for your identifiers?

Is your primary authentication system hosted in the cloud by a third-party vendor (e.g., Auth0, Okta, OneLogin, PingIdentity, etc.)? If so, please provide the name of the vendor and authentication product below.

If you have a Learning Management System (LMS; e.g., Blackboard, Canvas, D2L, etc.), is it connected to your institution's single sign-on (SSO) system?

□ **Yes**

Is the identifier users log into the SSO system with stored on their account in the LMS?

□ Yes

□ No

□ **No**

What identifier is used for users to log in to the LMS?

What do students type to log in to the LMS? What identifier does that login tie to? Is this the same for other campus services?

Shibboleth/SAML

Campus Labs supports native Shibboleth SP and SAML authentication and is a member of the InCommon Federation (http://www.incommon.org).

Steps to implement a Shibboleth/SAML authentication:

1. Contact our Authentication Support Specialist (authentication@campuslabs.com) and indicate that you'd like to setup Shibboleth authentication.
2. Answer the questions below so we can determine which configuration we will use.
3. We will work with you to get a site configured based on your answers to the questions.
4. Once provided, implement our metadata on your end and authorize the site we've created to connect to your authenticator.
5. Testing and troubleshooting

Are you a member of the InCommon Federation (http://www.incommon.org/participants/)?

□ Yes

What is your entity ID?

□ No

Are you running a local Shibboleth or other SAML-based (e.g., Microsoft ADFS, Gluu, SimpleSAMLphp, etc.) Identity Provider (IdP)?

□ Yes

Please provide the URL to your metadata or send your metadata to the authentication specialist.

□ No

Please provide information about your setup.

Service Provider Metadata and Supported Attributes

The service provider metadata will be provided upon receipt of the completed authentication worksheet.

Friendly Name	SAML2 Name
cardId	
cn	urn:oid:2.5.4.3
employeeNumber	urn:oid:2.16.840.1.113730.3.1.3
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
givenName	urn:oid:2.5.4.42
mail	urn:oid:0.9.2342.19200300.100.1.3
persistent-id	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
sn	urn:oid:2.5.4.4
uid	urn:oid:0.9.2342.19200300.100.1.1

Test Account Information

While a unique, permanent vendor account is not required, it can be helpful for assisting us with troubleshooting and authentication-related support issues. If we are not issued a test account, we will be required to contact your campus IT department for assistance.

User ID

Password: If you provide a test account username we will contact the individual(s) listed under the Authentication Contacts section above to receive the password.

Single Log Out & Shibboleth Authentication Considerations

What is Single Log Out?

Single Log Out (SLO) is the process of reversing a Single Sign On (SSO) authentication session. SSO is often preferred by campuses because it can reduce the number of times a user needs to provide credentials (username/password) to campus web applications throughout the day.

A Simple Analogy

Single Sign On (SSO) is like using your key fob to unlock all of your car doors at one time in order to keep them open at a tailgate party so that you can easily get in to grab additional items throughout the day. Single Log Out (SLO) is the action of locking your car with your key fob before heading to the game.

SSO is designed for convenience. SLO is designed for security. Sometimes these conflict. What if a neighbor accesses your car while you are not looking? What if you need to get back into your car several times after you locked the doors?

Ultimate security would have you unlock and re-lock your car each time you access it for items.

Ultimate convenience would not enable the ability to lock the car.

What is Shibboleth?

Shibboleth is a popular authentication protocol that many campuses (especially InCommon federation participants) use to apply security to web applications that are used by members of the campus community. Shibboleth is popular because it is highly secure and easy to configure for both the campus and third party platforms, like Campus Labs. However, there is one tradeoff for the security and simplicity of Shibboleth that can cause user experience issues in specific use circumstances that are important to understand.

Limitations of Shibboleth Single Log Out

The Shibboleth protocol **does not support** Single Log Out by design.

The best and only way to log out of an authenticated session is to completely close the web browser when finished using a web application, like Campus Labs, secured by Shibboleth.

Practical Implications of SLO Limitation

In scenarios where users are using their personal device and do not share their device with others this SLO limitation is not particularly invasive since the user will likely perceive that the Campus Labs application only requires seemingly periodic authentication, similar to Facebook or other web services that want to make it easy for users to quickly access content.

However, in scenarios where multiple users will use the same device and browser in rapid succession (taking turns filling out a survey, using the Location tracking kiosk screen, etc.), and where it is unlikely that the browser will be closed after each log out attempt, **users can unknowingly continue use of the application as a previous user who did not successfully log out.**

Remedies for the Shibboleth SLO Limitation

1. Users not sharing a device

If it is rare that multiple users will use a single device to participate in surveys or location tracking, then the simplest remedy is to **remind users to close the browser upon log out.** The Campus Labs platform offers a configuration option called a "Shibboleth log out URL" which allows a campus to define a URL that the system will direct the user to upon clicking the "Log out" button in the application. The content of the webpage is at the discretion of the campus but should contain a reminder to close the browser to complete the log out process.

It is important to note that the presence of a Shibboleth log out URL ***does not guarantee a successful log out* for each user, it is simply a mechanism to remind users to close their browser.*

2. Users sharing a device

If it is common for users to share a device, or the campus would like to use the location tracking features of the application then **a permanent change in authentication method** to one that supports SLO is needed. The Campus Labs platform supports the Central Authentication Services (CAS), Lightweight Directory Access Protocol (LDAP), and a proprietary authentication method based on Security Assertion Markup Language (SAML) that we call Generic Pass Through.

If you would like to employ either of these strategies please contact our support team by creating a help ticket.

Technical Summary of Issue

Adapted from The University of Texas at Austin
https://www.utexas.edu/its/help/shibboleth/2299

Campuses using a Shibboleth Identity Provider based on SAML 2.0 do not support single logout (SLO). SLO is the process of reversing the single sign on (SSO) process by destroying all sessions that are created while using SSO. For the context of this document, that would mean destroying the identity provider session and service provider sessions. Before explaining this in more detail, there are a couple of important terms to know.

This document will refer to a service provider (SP) which is the host of the service or application, in this case the Campus Labs platform that users are attempting to access and the identity provider (IdP) which hosts user authentication and user attributes at the campus to be consumed by the SP.

For example, the university controls idp.its.campus.edu which is the IdP used to allow users to authenticate using campus username/password credentials and gain access to an SP, like Campus Labs.

Understanding Shibboleth Single Sign-On Sessions

There are usually up to 3 sessions associated with Shibboleth IdP and SP integration: the IdP session, the SP session, and the optional web application session for the service the SP is providing. The following is the most common authentication flow for the creation of these sessions at a high level.

Whenever a user attempts to access an SP-protected application for the first time, they will not have an SP session or an application session and are redirected to the IdP to see if they have a valid IdP session. When they make it to the IdP, they also do not have an IdP session at this time and are prompted to provide credentials to authenticate.

Upon successful authentication, an IdP session is created and an associated IdP session cookie is placed in the user's browser. The user is redirected back to the SP where the IdP session is verified and an SP session is created and an SP session cookie is placed in the user's browser. Finally, the user is passed to the application itself where a web application session may also be created.

Upon returning to the application, the optional web application session is checked and then the SP session is checked. If either of these sessions are still valid, the user will not be redirected back to the IdP to re-authenticate. If neither of these sessions are valid, the user will be sent back to the IdP where the IdP session is checked using the IdP session cookie that was created upon initial authentication. If the user makes it back to the IdP with the IdP session cookie and the IdP session is still valid, the user will not get prompted to provide credentials. The IdP session will be refreshed and the user will be returned back to the SP and web application where new SP and web application sessions will be created.

If the user makes it back to the IdP without the IdP session cookie, or with an IdP session cookie but an invalid IdP session, the user will be asked to authenticate.

The Complications of Single Logout and User Expectations

When a user clicks on a logout button in an SP's application, they have a set of expectations. These expectations combined with technical roadblocks currently keep SLO from being implemented.

When the logout button is clicked, the user's web application session and SP session are ended, but the user is not logged out of the IdP. Therefore, if the user were to revisit the web application, they would be automatically re-authenticated because they still have a valid IdP session cookie.

In theory one might, instead of just destroying the web application session and SP session, have the SP tell the IdP to destroy its session as well. Unfortunately, the IdP does not know which SPs the user has sessions with, cannot inform those SPs to destroy the user's sessions, and cannot enforce that those SPs destroy the user's session on the SP and web application side. This creates a false sense of security for the user because they may believe that they have been logged out of all systems. It also means that the user could go from SP to SP and get varying experiences after logging out of one SP.

Central Authentication Service (CAS)

CAS URLs

The service provider consumer service URL will be provided upon receipt of the completed authentication worksheet.

Course Evaluations consumer service URL will be provided upon receipt of a completed worksheet

Please complete (if not relevant, please denote writing “N/A”):

CAS Login Page: This is the page the user gets redirected to from the login page. The user enters the CAS login credentials on this page.

CAS Logout URL: This is the URL that the user is redirected to when they log out.

	URL	**Parameters**
CAS Login URL		
CAS Logout URL		

Test Account Information

While a unique, permanent vendor account is not required, it can be helpful for assisting us with troubleshooting and authentication-related support issues. If we are not issued a test account, we will be required to contact your campus IT department for assistance.

User ID

Password: If you provide a testaccount username we will contact the individual(s) listed under the Authentication Contacts section above to receive the password.