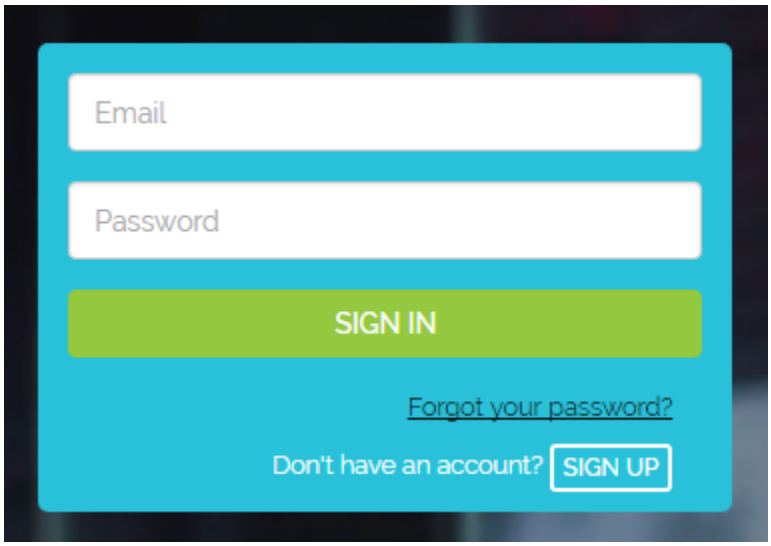
SAML 2.0 SSO Integration into Knowledge Anywhere LMS

Design Document

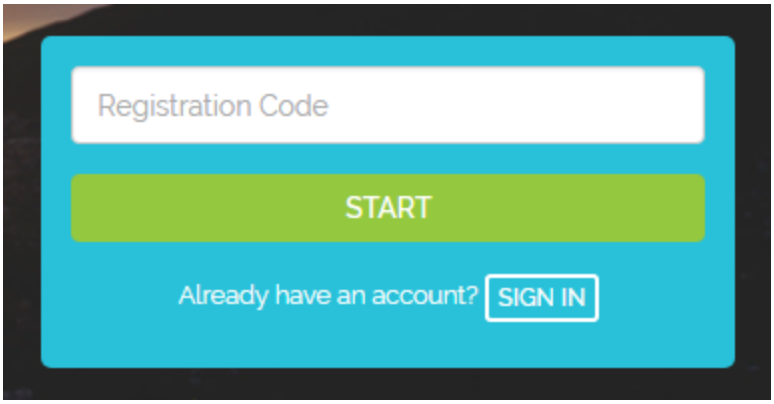
Last Updated: 11/20/17

Introduction

Knowledge Anywhere's Learning Management System (LMS) uses a login/password approach for users to sign in to the system. If a user does not have an account, they can create one with a valid registration code.



Sign In

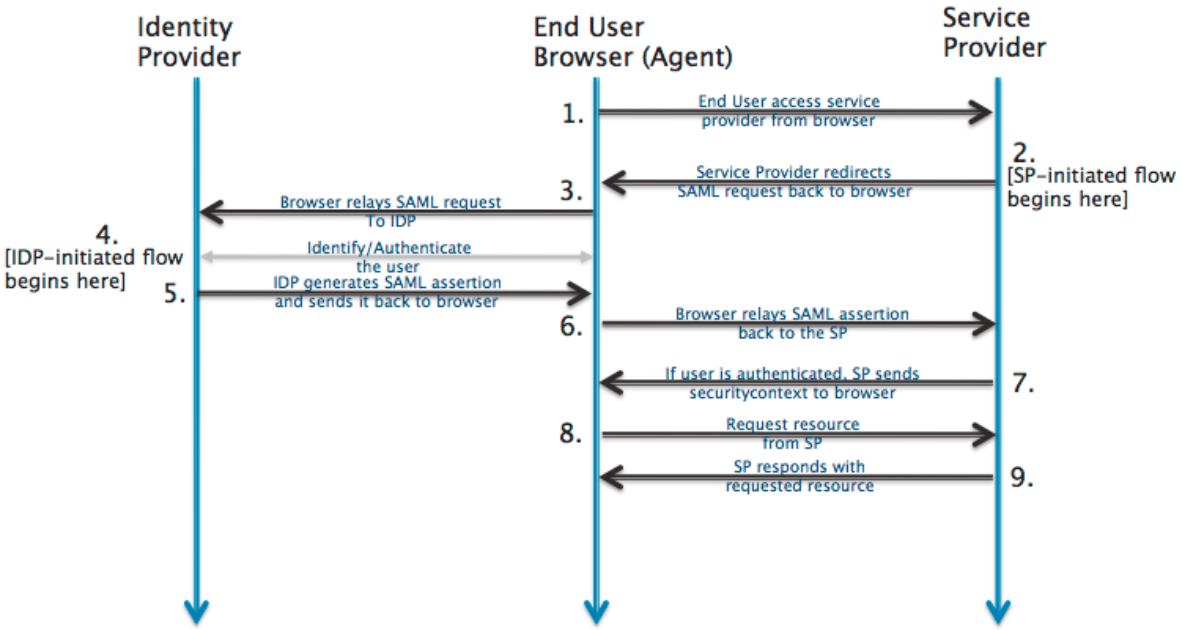


Sign Up

The login/password approach works in most scenarios, except for when a user needs to create another account that they need to manage. A simpler approach for enterprises that already have an authentication system is to leverage their existing authentication to provision users into the LMS.

SAML Flow

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between providers, in particular, between an Identity Provider (IDP) and a Service Provider (SP). The IDP and the SP do not talk directly but use the browser to broker the authentication flow. The diagram below illustrates this concept.



SAML Authentication Flow

When leveraging SAML for exchanging authentication and authorization data between systems, the LMS functions as the Service Provider (SP) and the Identity Provider (IDP) is provided by the organization.

To make the connection, we will use SAML 2.0 as the protocol for exchanging information between the two providers.

By default, the IDP and SP will use Http POST to redirect and transmit data between each other.

Flow Initiation

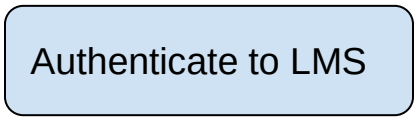
When a user initiates flow at the Identity Provider (IDP), the IDP redirects user to the primary Service Provider's (SP) URL after successful authentication.

When a user initiates flow at the Service Provider (SP), the SP will determine if the user has a valid session with the system. In case the session is invalid or expired, the SP will redirect user to IDP to authenticate. One of the use cases in this scenario is where user begins the flow at a URL somewhere inside the app. It would then make sense that when the user comes back to SP, they land at the same page instead of the SP's primary URL. This is accomplished using a parameter called RelayState. The LMS will set this value before redirecting the user to IDP, and when a user is returned back after successful authentication, it will take the user to that URL.

Sign Up vs. Sign in Flow

When a user uses SAML to authenticate into LMS, the sign in and sign up cases will follow a similar flow.

If the user does not have a valid session, we will show a single button to the user:



This will start the SP initiated flow. After the user has authenticated via the IDP, they will be redirected back to the SP. This will also be the URL that they will land on if they initiated the flow at IDP.

The IDP will pass back user authentication and profile data via SAML. The LMS will validate the digital signature associated with the IDP to make sure the data is sent by the proper IDP. Once that is confirmed, the LMS will read the profile information sent. The profile information will contain at the very least a field that uniquely identifies the user. We will call this SSOId and this can be the user's email address, guid or any other unique id. The profile data will also include other mandatory and optional fields like user's name, email address, etc.

Note: For each LMS instance, a set of mandatory fields will need to be configured. If these fields are not present as part of SAML data, then the request will result in an error. At the minimum, the LMS requires firstname, lastname and email address of the user.

The LMS will then determine if the user already exists in the system using SSOId. If it is a new user, LMS will use the profile data to set up their profile in the system. The user will then be sent to new user flow.

If the user already exists, the LMS will still use the profile data to update any changes to the user's profile. It will then login the user.

In both cases, the user will be issued an authentication token from the LMS, which will be valid for the life of the session. If the user was to come to the LMS directly with a valid authentication token, the user will be logged in without going through the SAML sign in flow.

Field Mapping

IDP may pass fields differently than what is expected by LMS. For example, the IDP may call the first name field first_name, while the LMS may call it firstName. This will be handled by LMS using field mapping. When configuring SAML, the admin will be able to set up field mapping, where they can designate first_name to map to firstName. This will ensure that the profile data is updated properly in the LMS.

As part of the field mapping, one of the fields that uniquely identifies the user will be designated as the SSOId.

IDP	SP/LMS
email_address	emailAddress (SSOId)
first_name	firstName
last_name	lastName
title	title

Sample Field Mapping

Change Password and Logout

Since the LMS is not the authentication authority, both Change Password and Logout will be handled by IDP.

For Change Password, the LMS will open the IDP provided change password URL in a new tab. This will not affect user's current session with the system. If a change password URL is not provided, the LMS will inform the user that the password needs to be changed on the IPD's end.

For Logout, the LMS will clear the user's current session and then redirect the user to the IDP provided logout URL.

Profile Editing

The profile fields that are sent by the IDP will not be editable in LMS. This is to avoid merging and conflicts in profile data. The user will be shown a message that these fields need to be updated on the IDP end.

Configuring SAML

For SAML to work properly, configuration is needed at both ends. The following information will need to be exchanged between IDP and SP:

1. **IDP Login URL:** This is the endpoint on the IDP where the SP will post authentication requests. This will be configured in the LMS.
2. **SP Login URL:** This is the primary URL for the LMS that will be provided to the IDP. The IDP on successful authentication will POST profile data back to this URL.
3. **Certificate:** The IDP will provide a public certificate that the LMS will store and use it to validate all SAML requests sent to it.
4. **SSOId:** This will be the name of the field used to uniquely identify the user in the system. This will be configured in the LMS. For SSOId, the system will default to: urn:oid:1.3.6.1.4.1.5923.1.1.1.10 (eduPersonTargetedID), but it can be changed to another SAML variable.
5. **Fields and Mapping:** List of fields that IDP will send as part of profile data and their mapping to internal fields within the LMS. The system will default to standard SAML 2.0 variables, but allow for modification:
    a. FirstName or GivenName: urn:oid:2.5.4.42
    b. LastName or Surname: urn:oid:2.5.4.4
    c. Email: urn:oid:0.9.2342.19200300.100.1.3
6. **Change password URL (optional):** The URL to open in case the user wants to change their password. This will be configured in the LMS.
7. **Logout URL (optional):** The URL to redirect to when a user logs out. This will be configured in the LMS.
8. Test accounts (optional): The IDP will provide one or more test accounts on their system, which can then be used to test the flow.

Backdoor for Admin Logins

The LMS will allow certain users to login directly using login/password. This will be needed for Knowledge Anywhere admins who may not have an account on the IDP side. There will be a special URL that they will be able to go to directly and login. Their accounts must exist with a valid login/password in the system beforehand, to be created via the LMS admin. This will ensure that we only allow select users to use this backdoor and it is not available for normal users.