Single Sign-On Generic Setup Steps

Last Modified on 08/25/2020 8:40 am CDT

General Setup Steps

Not Specific to a Particular IDP

Though each Identity-provider (IDP) may vary, there are certain steps in the SSO setup process that remain the same across all platforms.

• Exchange of Metadata

iLMS Metadata can be downloaded from the Service Provider Section of our tool.

🖃 Service Provide	r
Information you may need to setup your organization as relying party in identity provider. Click here to download metad	
Identifier	
Endpoint (URL)	https://www.inspiredlms.com/saml/consumer.aspx?on=mycompany

Your IDPs (Identity provider) Metadata can be uploaded under the Identity provider section as well.

Identity Provider			
To setup SSO, please provide the information below related to identity provider.			
Enter Information Manually	Import Metadata		
Select Metadata File	Choose File No file chosen		

This will create trust between the two parties.

• Mapping of Values

The iLMS needs to know what values to expect from your system, and to which field in iLMS that value correlates.

The most important value to map is the identifier.

User Identifier	
Email ID *	Email ID is the NameID element of Subject node.
	C Attribute element.

This will be based on the attribute name under which the value is passed, the most common of which is Name ID.

By default Email Address is used as the identifier and is set as Name ID.

If this differs for your system you are able to change the setting in the identifier section in iLMS.

• Provisioning (Optional)

If you are planning to provision with SAML as well there is a Create unrecognized Accounts option, and the rest of the Mandatory values (seen in iLMS) will need to be mapped across as well on both the IDP and iLMS side.

If you have Active Directory, we do recommend using LDAP provisioning in tandem with SAML to provision as this method is better at housekeeping. SAML can create accounts, but cannot inactivate them.

Learn More about Setting up LDAP Here: iLMS LDAP Connector: About the Connector and Setup

• After the setup

The SSO connection can be tested with either our SP-initiated link (Found in the Service Provider Section of iLMS SSO: SAML Settings)

It looks like this: https://www.inspiredlms.com/saml/consumer.aspx?on=mycompany or you can utilize the IDP-initiated link from your provider.

Note: If SSO is implemented. We recommend updating the access URL in the email communications sent to users with the SSO URL.

Editing Email Templates

If using LDAP to sync users from Active Directory the URL can be replaced easily, simply make the change shown below

Post-Setup:

Recommended Step if using LDAP Active Directory Sync for Provisioning Users

For the most seamless integration it is recommended to provision users with our LDAP connector's active directory sync and authenticate users with SSO: SAML.

Learn more about LDAP Active Directory Sync here: iLMS LDAP Connector: About the Connector and Setup

If using these systems in tandem it is important to ensure that users created during the AD sync will be given the correct URL for accessing iLMS in all email notifications.

Once Single SignOn has been enabled for your organization you have the ability to select which Login URL learners will receive once provisioned by the LDAP connector.

To view this setting, navigate to the Settings Tab and select "LDAP Connector".



Navigate to the Settings Sub-Tab.

From there select "SAML Enpoint URL" and click **Save.**

LDAP Connector 🥹		
Setup Settings		
For LDAP users, select the login URL that will replace "[AUTO DETECT LOGIN INFORMATION]" system variable in emails.		
Portal URL (<u>https://www.inspiredIms.com/</u>)		
SAML Endpoint URL (<u>https://www.inspiredlms.com/Login/ /consumer.aspx</u>)		
Save		

This, enables the use of "SAML Endpoint URL" in place of traditional login portal in iLMS Email Notifications for users provisioned via the LDAP connector.