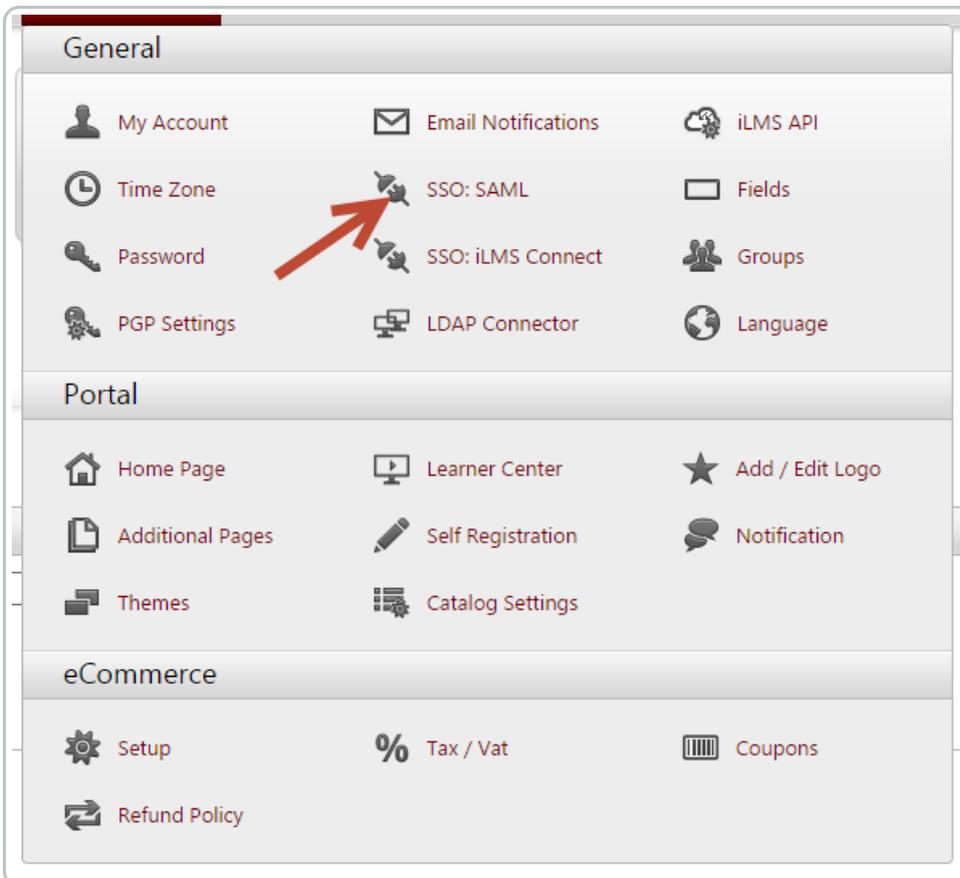


iLMS SSO: Single Sign-On Setup with SAML

Last Modified on 05/19/2020 6:38 am CDT

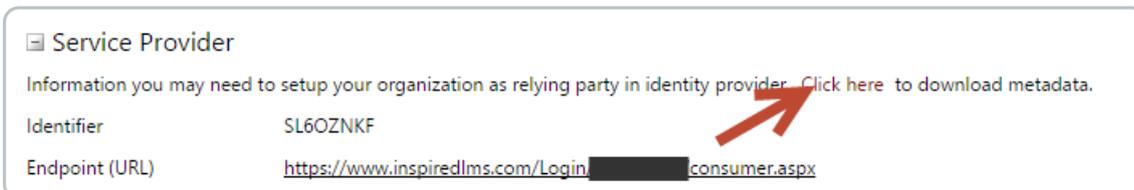
Overview of SAML Settings in iLMS

The SAML settings section in the iLMS will require information from your SAML configuration. The information needed in the iLMS configuration should be available from your SAML implementation as well. Hover over Settings in the administrator dashboard.



Download Metadata from iLMS

Click on SAML Expand the service provider section and click the click here download link to receive the metadata.



Service Provider

The automatically populated information in this section may be required by your identity provider to configure Single Sign-on.

Service Provider	
Information you may need to setup your organization as relying party in identity provider	
Identifier	iLMS91QI6F6D
Endpoint (URL)	https://www.inspiredlms.com/Login/[REDACTED]/consumer.aspx

Identity Provider - Issuer

In the Issuer section, enter the corresponding information from your identity provider to configure SSO.

or

Select "Import Metadata" to import the Metadata from the Identity-Provider you are using and the data will populate automatically.

Identity Provider

To setup SSO, please provide the information below related to identity provider.

Enter Information Manually
 Import Metadata

Issuer *

Sign-in page URL *

Verification Certificate No file chosen

This certificate file must contain the public key for iLMS to verify sign-in requests.

Additional Settings

Sign-out page URL Custom Login Page (<https://www.inspiredlms.com/mycompany>)

Change

Change Password URL

- **Sign-in page URL**
This will be used to redirect the user to login again if the iLMS doesn't receive a SAML token with the request.
- **Verification Certificate**
Allows your organization to upload the security certificate provided by your Identity provider.
Note: This must be in .cer format.
- **Sign-out page URL**
will close the Learner Center window upon logout and redirect the user to your organization's login page if specified, or redirect the user to any other specific URL.
- **Change Password URL**
will be associated with the Change Password link in User Profile page in the Learner Center.

User Identifier

Enter the primary identifier for your learners Email ID field. By default this is the NameID element, but optionally can be any other standard attribute element.

If your organization has set Employee ID as unique identifier in iLMS, this will display Employee ID in place of Email ID

Unique ID for iLMS can be changed here: [iLMS Fields and Unique Identifier](#)

User Identifier

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

Just-in-Time User Provisioning with SAML

Create Un-recognized User Account

Please map SAML Attributes to iLMS User Profile fields by entering the attribute name in respect to the user field. You can also select attribute from the drop down if you are using ADFS 2.0.

Mandatory

iLMS User Field	Default Value	Attribute
First Name *	<input type="text"/>	<input type="text"/>
Last Name *	<input type="text"/>	<input type="text"/>
Region *	Region 2	<input type="text"/>
Division *	Department Test	<input type="text"/>
Department *	Managers	<input type="text"/>

Optional

- The **Create Un-recognized User Account** checkbox will allow the system to create a user that is not registered in the iLMS at the time of Single Sign-on.
- SAML Attributes are then matched to the user profile fields. The first five are the default values for created or updated user profiles and must have matching attributes assigned from the IDP.
- A Default Value is added to any non-mandatory field that is left blank in the SAML token.
- Predefined ADFS 2.0 attributes are available from the drop down on the right for added convenience, but if the desired attribute name is not listed, you may type the correct input.
- Fields marked with an asterisk (*) are mandatory fields for registering a user and iLMS allows further profile fields to be defined. To add/remove fields see instructions here: [iLMS Fields and Unique Identifier](#)

Business Rules

SAML ?

Settings Business Rules

Create Un-recognized Regions, Divisions and Departments

Update User Profile During Sign-in

Update Blank Values for Non Mandatory Fields in User Profile

Send Error Notification Email

Recipients (To enter multiple email addresses, separate them by semicolon like one@email.com; two@email.com)

Save

- **Create Un-Recognized Regions, Divisions, and Departments**
If Checked, this will create new Regions, Divisions, and Departments that do not already exist at the time of Single Sign-on if listed in a user profile.
- **Update User Profile During Sign-In**
If enabled this will update data in the user profile upon each Sign-on.

- **Update Blank Values for Non Mandatory Fields**

This allows populated non-mandatory fields to be overwritten with blanks if the profile field(s) in the SAML token is blank upon Sign-On

- **Send Error Notification Email**

This allows your organization to specify an email address (usually a distro) that will receive error logs each time a user encounters an issue signing in to the iLMS via SSO. This log includes data sent in the SAML token along with the error message received by the user.

Note: a log will only be produced if the user gets far enough in the process that the request hits our system.

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](#)
