

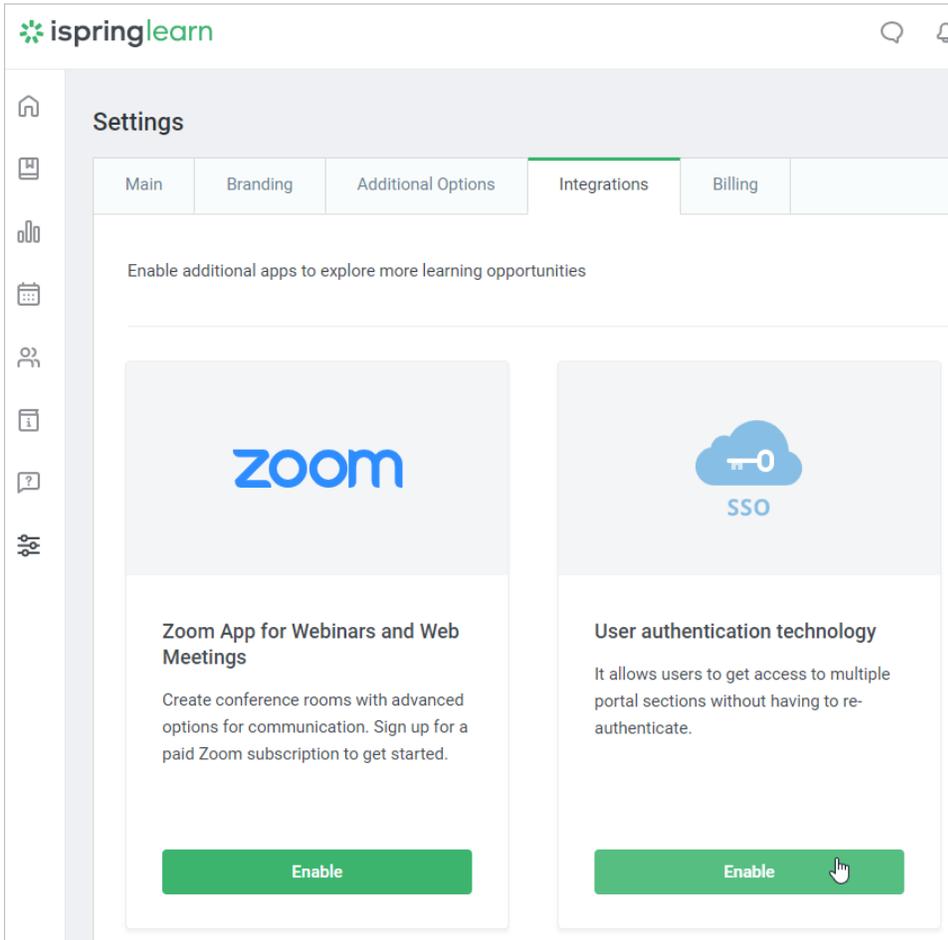
# SAML Authorization

iSpring Learn allows you to use [SAML](#) to enable single sign-on to the account.

 Authorization with SAML also works in the mobile application.

To set up SAML authentication in your account:

1. Go to the **Settings** section, then open the **Integrations** tab, and, in the **SSO** area, hit **Enable**.



The screenshot shows the iSpring Learn web interface. At the top left is the iSpring Learn logo. Below it is a navigation sidebar with icons for Home, Dashboard, Reports, Calendar, Users, Settings, Help, and Integrations. The main content area is titled "Settings" and has several tabs: Main, Branding, Additional Options, Integrations (which is selected), and Billing. Below the tabs, there is a heading "Enable additional apps to explore more learning opportunities". There are two cards displayed. The first card is for "Zoom App for Webinars and Web Meetings" and has an "Enable" button. The second card is for "User authentication technology" (SSO) and has an "Enable" button with a mouse cursor hovering over it.

- Fill out the form fields, adding the URL, and other details of your identity provider. The latter is the resource your users are supposed to use for the initial authorization on your corporate portal.

### Connection Settings

Issuer Url (IdP Entity ID):

Sign On Url:

Logout Url:

Certificate Fingerprint:

Redirect users to the SSO login page

Add a link on the side panel to return to the main site

Link title:

Main site Url:

<b>Issuer Url (IdP Entity ID)</b>	The URL that uniquely identifies the identity provider service. This value is equal to the <b>Issuer</b> element in the SAML request sent by the identity provider.
<b>Sign On Url</b>	Path to the server script which generates SAML identifier confirmation requests to handle authorization.
<b>Logout Url</b>	Path to the server script which generates SAML identifier confirmation requests to handle logout.
<b>Certificate Fingerprint</b>	A short version of <a href="#">the public key certificate</a> for verifying a digital signature. It is used to confirm signing requests issued by an identity provider. Learn more about certificate fingerprints <a href="#">here</a> .
<b>Redirect users to the SSO login page</b>	If this option is enabled, the iSpring login page will have the following URL: <a href="https://yourcompany.ispringlearn.com/sso/login">https://yourcompany.ispringlearn.com/sso/login</a> .
<b>Add a link on the side panel to return to the main site</b>	A link to a resource specified by the administrator will appear on the sidebar.
<b>Link title</b>	The title of the link that will appear on the sidebar.
<b>Main site Url</b>	The address of the link that will appear on the sidebar.

- If needed, [match fields](#) in iSpring Learn and your SSO service.

### Matching fields of iSpring Learn with the external SSO attributes

The data will be automatically synced when users sign in for any of the fields listed below.

Email	▼	email	🗑️
Last Name	▼	family_name	🗑️
First Name	▼	given_name	🗑️
Login	▼	preferred_username	🗑️
Login	▼	sub	🗑️

[+](#) Add a field

4. Click **Enable**.

← SSO integration settings

Use this page to manage SSO settings.

**Enable**

**Important:**

If you get a 400 error and a message about the request being composed incorrectly ("Cannot retrieve metadata for IdP 'https://myidp.com/oam/fed' because it isn't a valid IdP for this SP") after you enabled SAML in your iSpring Learn account, it means that the value set for the **Issuer Url (IdP Entity ID)** field is incorrect.

400

Wrong Request

Cannot retrieve metadata for IdP 'https://myidp.com/oam/fed' because it isn't a valid IdP for this SP.

← Go Back

To make the SAML authorization work properly in your account, copy the URL from the error text and paste it into the **Issuer Url (IdP Entity ID)** field.

### Connection Settings

Issuer Url (IdP Entity ID):

https://myidp.com/oam/fed

Sign On Url:

https://myidp.com/adfs/ls/idpinitiatedsignon.aspx

Logout Url:

https://myidp.com/adfs/ls/?wa=wsignout1.0

Certificate Fingerprint:

afe71c28ef740bc87425be13a2263d37971da1f6

## Setting Up SAML on the Server

We recommend that you should use [the SimpleSamlPhp library](#) to set up your identity provider server to enable authorization with SAML 2.0.

## Setting Up iSpring Learn

Configuration of your iSpring Learn account is completed by our employees. Just provide us with the following information:

1. Identity provider URL
2. SSL certificate (server.crt)
3. Secret key (server.pem)
4. certFingerprint for a quick verification

## Setting Up Identity Provider

To set up the identity provider, perform the following steps:

1. Enable support of SAML 2.0 and Shibboleth 1.3 in the **config/config.php** file.

```
'enable.saml20-idp' => true, 'enable.shib13-idp' => true,
```

2. Switch on the authorization module. Different authorization modules are located in the **modules** folder. Open the folder where the needed method is located and create an empty file called enabled in it.

3. Enable the authorization module in the config/authsources.php file.

**Important:** email is a required attribute.

```
$config = array( 'example-userpass' => array( 'exampleauth:UserPass', 'student:studentpass' => array( 'uid' => array('student'), 'email' => 'student@example.com', 'eduPersonAffiliation' => array('member', 'student'), ), 'employee:employeepass' => array( 'uid' => array('employee'), 'email' => 'employee@example.com', 'eduPersonAffiliation' => array('member', 'employee'), ), );
```

4. Configure the identity provider in the **saml20-idp-hosted** configuration file as in the example below.

```
'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri', 'authproc' => array( // Convert LDAP names to oids. 100 => array('class' => 'core:AttributeMap', 'name2oid'), ),
```

5. Add information about the identity provider into the **metadata/saml20-sp-remote.php** file.

```
$metadata['https://sp.example.org/simplesaml/module.php/saml/sp/metadata.php/default-sp'] = array( 'AssertionConsumerService' => 'https://sp.example.org/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp', 'SingleLogoutService' => 'https://sp.example.org/simplesaml/module.php/saml/sp/saml2-logout.php/default-sp', );
```

If you have enabled SAML in your iSpring Learn account and for some reasons can't login using single sign-on, type the following web address: [https://yourcompany.ispringlearn.com/login?no\\_sso](https://yourcompany.ispringlearn.com/login?no_sso).

Now you will sign in with the account, as usual, using your login and password.



### Useful links on SAML authorization:

[Configuring SAML 2.0 SSO with Microsoft Active Directory Federation Services](#)

[Setting Up SAML for G Suite](#)

[Configuring SAML with Azure AD](#)