

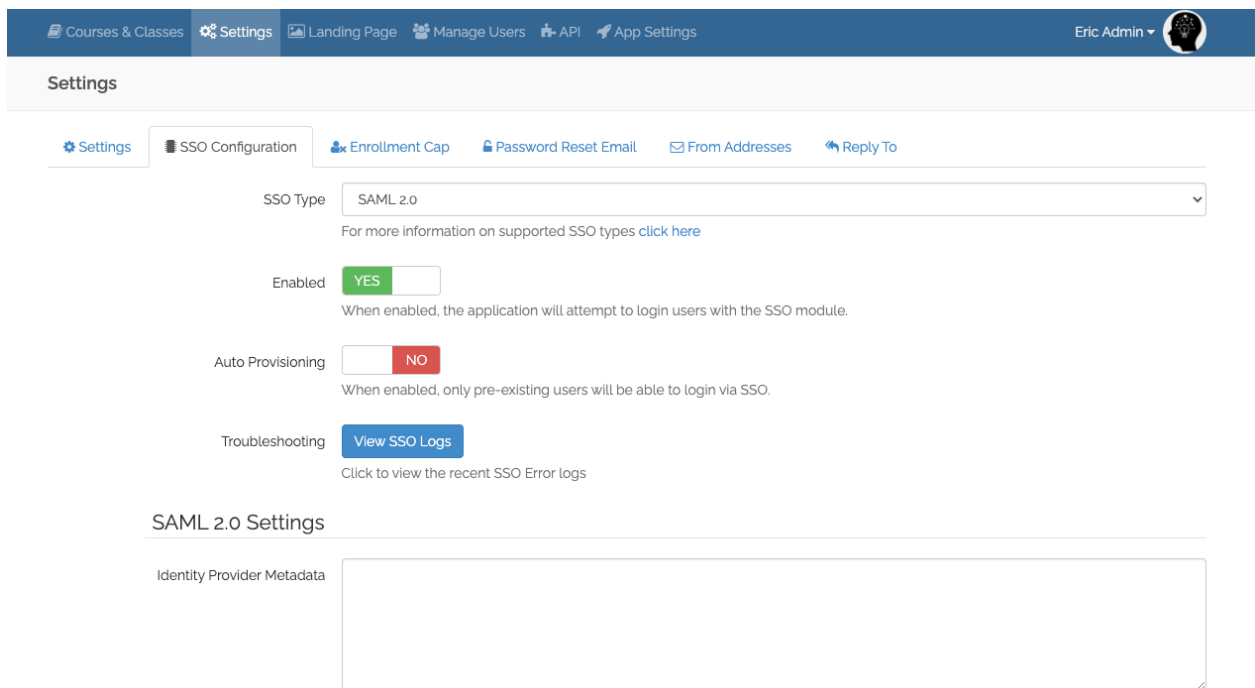
Integrating with Intrepid Learn via SSO

This document will cover how to integrate Intrepid Learn via Single Sign On. Intrepid Learn supports integrating with Identity Providers (IdPs) which support SAML 2.0 or OpenID Connect 1.0. The configuration using each protocol will be described below.

SAML 2.0 Protocol

To start configuring Intrepid Learn to use your SAML 2.0 IdP, start by logging into the existing Intrepid Site using the login page. Then navigate to the Admin Panel, and click “Settings” on the top bar, then click the SSO Configuration tab.

Under SSO Type change to “SAML 2.0” if not already selected. You will be presented with a configuration screen similar to below:



The screenshot shows the Admin Panel interface. At the top, there is a navigation bar with links for Courses & Classes, Settings, Landing Page, Manage Users, API, and App Settings. The user is logged in as Eric Admin. Below the navigation bar, the Settings page is displayed with several tabs: Settings, SSO Configuration (selected), Enrollment Cap, Password Reset Email, From Addresses, and Reply To. The SSO Configuration section includes a dropdown menu for SSO Type set to SAML 2.0, with a link for more information. There are three toggle switches: Enabled (set to YES), Auto Provisioning (set to NO), and Troubleshooting (with a View SSO Logs button). Below this is the SAML 2.0 Settings section, which contains a large text area for Identity Provider Metadata.

Now, you can start configuring based on your SAML 2.0 IdP settings. First, paste in the XML for the Identity Provider Metadata. This must be a valid XML file with no other extraneous text strings.

Next, review the SAML Request settings. Normally, these settings can be left as default, but some IdPs require these settings to be changed. For instance, you may need “Sign Authn” to be true if your IdP requires Authn Requests to be signed.

Finally, proceed to the SAML Attribute Map. This is where you can map the data in the SAML assertion coming from your IdP to Intrepid Learn. To review, at the end of the SAML authentication process (using an SP Initiated login flow), the IdP will send an XML document called a SAML Assertion to Intrepid Learn. The SAML Assertion will consist of information about the user being authenticated. It often contains a NameID identifying the user's persistent name, and other information about the user, such as First and Last name.

Intrepid Learn requires a unique attribute for the user called the "username". The username attribute should never change. Also required is a user's first and last name and email. Optionally, your IdP can send a user photo and what is called an "External Id" (see Appendix) if needed. User Photos can be in the form a URL, or a Base64 encoded string embedded in the Assertion. If using Base64 Encoded Photos make sure the IdP is using "POST" binding, or else URL size limitations may cause issues.

To determine how to fill out the Attribute Map, first configure your IdP using the Service Provider (SP) Metadata. This can be downloaded by clicking "Download" in the SAML Settings screen.

Now, using a new browser window with no cookies (InPrivate, Incognito etc.), attempt to login to the Intrepid Learn site using the Intrepid Domain Name as the URL. This will generate an error on the Intrepid Learn site, because the Attribute Map is not yet configured. However, if we copy the error code from the error page which appears, we can now use that to find the error in the log.

Click "View SSO Logs" then paste in the error from the error page. When you find the error, click "View More". This will show the raw SAML Assertion XML document. You can use this to determine your Attribute Names to use in the Attribute mapping.

SSO Logs

Searching for c7c824e76cb9481fa47d4bd5d3ed2c7d

✖ Clear

January 12, 2021 1:01 PM

Id: c7c824e76cb9481fa47d4bd5d3ed2c7d

Message: No username could be determined by SAML Assertion, please check Attribute Map.

[View Less](#)

```

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oas
  <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-e
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/
    <ds:Reference URI="#_be8aaa2e728a46fa235e7e46db830942d157bbeb7e"><ds:Transforms><ds:
  <ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICFzCCAAYACCQDFqMEP0GzLBTANBgkqhkiG9w0BA
    <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-e
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/
      <ds:Reference URI="#_6144c9248d69d598a640687e0accdd4db5e5330556"><ds:Transforms><ds:
    <ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICFzCCAAYACCQDFqMEP0GzLBTANBgkqhkiG9w0BA
    
```

For example, here is an example SAML Assertion:

```

<?xml version="1.0" encoding="UTF-8"?> <samlp:Response
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_be8aaa2e728a46fa235e7e46db830942d157bbeb7e" Version="2.0" IssueInstant="2021-01-
12T21:01:39Z" Destination="http://sso.example.com/mlp/saml/acs"
InResponseTo="id5480bc33-67da-465c-8bc7-cdd53bb07696">
<saml:Issuer>http://simplesaml.docker.intrepidagle.com/simplesaml/saml2/idp/metadata.
php</saml:Issuer> <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo> <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" /> <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" /> <ds:Reference URI="#_be8aaa2e728a46fa235e7e46db830942d157bbeb7e">
<ds:Transforms> <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" /> <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms> <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/> <ds:DigestValue> </ds:DigestValue> </ds:Reference> </ds:SignedInfo>
<ds:SignatureValue> </ds:SignatureValue> <ds:KeyInfo> <ds:X509Data>
<ds:X509Certificate></ds:X509Certificate> </ds:X509Data> </ds:KeyInfo> </ds:Signature>
<samlp:Status> <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status> <saml:Assertion xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
ID="_6144c9248d69d598a640687e0accdd4db5e5330556" Version="2.0" IssueInstant="2021-01-
12T21:01:39Z">
<saml:Issuer>http://idp.example.com/saml2/idp/metadata.php</saml:Issuer> <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:SignedInfo>
  
```

```

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#_6144c9248d69d598a640687e0accdd4db5e5330556"> <ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /> </ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
<ds:DigestValue> </ds:DigestValue> </ds:Reference> </ds:SignedInfo>
<ds:SignatureValue> </ds:SignatureValue> <ds:KeyInfo> <ds:X509Data>
<ds:X509Certificate> </ds:X509Certificate> </ds:X509Data> </ds:KeyInfo>
</ds:Signature> <saml:Subject> <saml:NameID
SPNameQualifier="http://sso.example.com/mlp/saml"
Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">_1c5cb58911af063e29034fc077e49288d4ec1d5ed0</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2021-01-12T21:06:39Z"
Recipient="http://sso.example.com/mlp/saml/acs" InResponseTo="id5480bc33-67da-465c-
8bc7-cdd53bb07696" /> </saml:SubjectConfirmation> </saml:Subject> <saml:Conditions
NotBefore="2021-01-12T21:01:09Z" NotOnOrAfter="2021-01-12T21:06:39Z">
<saml:AudienceRestriction>
<saml:Audience>http://sso.example.com/mlp/saml</saml:Audience>
</saml:AudienceRestriction> </saml:Conditions> <saml:AuthnStatement
AuthnInstant="2021-01-12T21:01:39Z" SessionNotOnOrAfter="2021-01-13T05:01:39Z"
SessionIndex="_08aa7a3fb3a5f687dd26bde24b4bcd9a969569fc0d"> <saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:Authn
ContextClassRef> </saml:AuthnContext> </saml:AuthnStatement> <saml:AttributeStatement>
<saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"> <saml:AttributeValue xsi:type="xs:string">98576</saml:AttributeValue>
</saml:Attribute> <saml:Attribute Name="externalId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue
xsi:type="xs:string">e98537</saml:AttributeValue> </saml:Attribute> <saml:Attribute
Name="givenName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue xsi:type="xs:string">Bob</saml:AttributeValue> </saml:Attribute>
<saml:Attribute Name="surName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"> <saml:AttributeValue xsi:type="xs:string">Grant</saml:AttributeValue>
</saml:Attribute> <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue
xsi:type="xs:string">bobgrant@example.com</saml:AttributeValue> </saml:Attribute>
<saml:Attribute Name="role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"> <saml:AttributeValue
xsi:type="xs:string">employee</saml:AttributeValue> </saml:Attribute>
</saml:AttributeStatement> </saml:Assertion> </saml:Response>

```

You can see in this assertion a number of XML attribute nodes with the qualifier of “<saml:Attribute>” the “Name=” attribute of these nodes are the names of the SAML Attributes and should be used in the SAML Attribute map. For instance, in this example the SAML Attribute with name “uid” is the username. The attribute with name “surName” is the last name and so on. If a NameID is included in your assertion that can be linked to the username field by turning the “Use NameID” toggle to ON.

OpenID Connect 1.0

Integrating with an IdP that supports [OpenID Connect](#) is usually a simple process. First, register a new Application with your IdP in order to generate a Client ID and Client Secret. The Application Reply URL to register with the new Application is in the Settings for the Open ID.

After registering the Application URL and generating a Client ID and Secret, enter those values along with the Issuer hostname of your IdP. This hostname will be used during OpenID Autodiscover requests. Autodiscover requests allow the Intrepid Learn application to obtain the correct endpoint URLs on your IdP for the Token, Authorization and User Info calls.

In a typical scenario, this configuration is all that is needed for an Open ID Connect 1.0 integration. Attribute Map does not need to be filled in in this case.

If your IdP does not fully support Open ID Connect an Attribute Map can be used, and Autodiscover can be turned off in favor of entering the Token, Authorization and User Info endpoints manually. This is an advanced use case however, with some limitations, talk to Technical Support if more information is needed.

Using Multiple Identity Providers

If more than one Identity Provider needs to be used for an Intrepid site, select the “Multiple Identity Providers” option. This is useful if you want to include learners who might login using different Identity Providers. Upon login, they will be presented with a page where they will select which Login Method (i.e. IdP) to use.

Configuration of Multiple Identity Providers is slightly different in that Admins will need to add each IdP separately by clicking “Add a new IdP”. An accordion will appear for each IdP that is added, each accordion can be expanded to configure the IdP specific settings.

Configure Multiple Identity Providers

Title

Title for Multiple IdP Selection page

Note that there are a few additional fields for each IdP and on the main page that control what learners will see on the initial login page where they can select which IdP to use. The first field is the “Title”, this is the overall title for this page.

Additionally, under each IdP there is a Title, Image and Help Text field.

SAML 2.0 Settings

Title

Name of SAML Integration for descriptive purposes (optional)

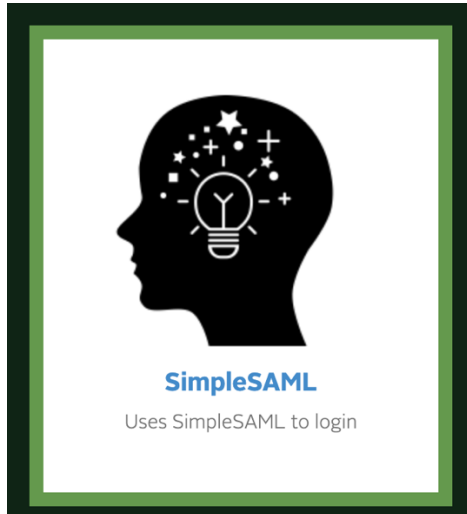
Image



Help Text

Explanation text shown to users on selection page for this IdP

These fields are what the users will see on the “Select Authentication” page when they need to login. Here’s an example of what the fields might look like on this page:



Learners can then click on this login method if it applies to them. The Multiple IdP option typically works best with two or three IdPs. Otherwise it can often be confusing for learners which option to pick upon login.

Appendix

Username vs External Ids

Normally the **Username** is the permanent attribute identifying the user, ideally it should never be changed. This is often an Employee ID or UID. Optionally, in cases where Auto Provisioning is turned ON and the users doing the Auto Provisioning would not be aware of a permanent attribute, an attribute like Email Address can be used in cooperation with the **External Id**. The **External Id** is an additional permanent attribute that can be used for identifying the user. In the case where Auto Provisioning must be used with a changeable attribute like Email Address, assign the **Username** attribute to an IdP attribute the users would know (i.e. email) and assign this Attribute to a permanent attribute like Employee ID