



Connecting to Lt with SAML 2.0

[Introduction](#)

[Getting Lt SP Details](#)

[Service Provider Options](#)

[Setting up your IDP](#)

[Example setup with Microsoft Azure AD](#)

[Enforcing SSO](#)



Introduction

Single Sign On (SSO) using SAML 2.0 allows your staff and students to log in to Lt without accepting an email invitation or creating a password. This means your students can get straight into Lt without them having to do any setup or remember any extra passwords.

User accounts do need to be first created in Lt, this can be done using [SCIM](#) or through the email invite workflow.

Getting Lt SP Details

You will first need to gather some SAML details from your Lt Instance.

1. As Instance Administrator, log into your Lt instance at ltlogin.com
2. Select **Instance Administration**
3. Select **SAML 2.0 Settings**

Here you will find your Service Provider details Service Provider Metadata (XML) URL and X509 certificate.

SAML 2.0 Settings
✕

Security Assertion Markup Language (SAML 2.0)

Configure your Identity Provider (IdP)

Add and configure your IdP

Configure

[SAML 2.0 Setup Guide](#)

SP Settings

These settings are necessary to establish Lt, the Service Provider (SP), as trusted by your Identity Provider (IdP)

SP EntityId

https://[redacted]/saml2

SP Assertion URL

https://[redacted]/saml2-ssso/

SP Logout URL

https://[redacted]/saml2/slo

SP X509 Certificate

-----BEGIN CERTIFICATE-----

- **SP EntityId** - The entity Id your IDP will use to identify Lt.
- **SP Assertion URL** - Where authentication assertions from your IDP should be sent.
- **SP Logout URL** - Where Logout requests from your IDP should be sent to enforce logging out of all services.
- **SP X509 Certificate** - The security certificate that may be used to sign requests from Lt (depending on the configuration options below).
- **SP Metadata URL** - After configuring Lt for your IDP, the Metadata XML can be retrieved from this URL. This can be used to setup some IDPs.

Service Provider Options

When you select **Edit Configuration** you will be presented with options for setting up Lt as a Service Provider.

- **User identified by** - When a user is directed to Lt from your IDP, whether to match user in Lt by their email address or an external ID provided using SCIM.
- **Entity Id** - The Entity Id of your IDP.
- **Service URL (Redirect only)** - The login service URL of your IDP that users will be directed to to login.
- **X509 Certificate** - The X509 Certificate of your IDP.

Advanced Settings

- **Use AuthNContext unspecified** - Whether an authentication request from Lt should specify minimum authentication of Password. Some IDP will not accept this to be specified and must be unspecified.
- **Sign AuthnRequest** - Whether an authentication request from Lt should be signed with the provided X509 certificate. Some IDP do not support signing of authentication requests.
- **Use attribute to identify user (instead of Nameld)** - By default, when a user is directed to Lt from your IDP, Lt uses the Nameld of the login request to identify the user. You can change to using a different attribute passed by your IDP.
 - **Attribute Name** - The unique attribute passed by your IDP that can be used to identify an individual user.
- **Logout Service URL (Redirect only)** - The logout service URL of your IDP, which is used during Idp initiated Single Log Out
- **Email domain requiring SSO** - You can require all users from a particular email domain to login using SSO. The normal login flow using email address and password will be disabled. More information is [provided below](#).
- **Response Signing** - Whether the SAML Response and/or Assertion should be signed.

Setting up your IdP

If your IdP uses SP XMLs for setup you can acquire your XML from the SP Metadata URL. You can alter this XML by selecting **Edit Configuration** and changing some of the displayed fields. Otherwise, use the SP details provided in the admin UI to set up your IdP. An example is shown below.



You can also use the following icons for creating link buttons from your IdP:


<https://staticfiles.kuracloud.com/lti/lit-logo-50px.png>

<https://staticfiles.kuracloud.com/lti/lit-logo-128px.png>


Example setup with Microsoft Azure AD

To set up SAML with MS Azure AD you will need to select or create an enterprise application within Azure AD that you will use.

1. Within the application select **Single Sign-on**
2. Select **SAML** as the single sign-on method
3. Edit the **Basic SAML Configuration**
 - a. Add the **SP Entity ID** from your Lt details as an **Identifier**
 - b. Add the **SP Assertion URL** from your Lt details as the **Reply URL**
 - c. (Optional) Add the **SP Logout URL** from your Lt details as the **Logout URL**
4. Edit the **Attributes & Claims** to suit your institutions data
 - By default the **Unique User Identifier (Name ID)** will be an email address in *nameid-format:emailAddress*, you can use a different identifier if it has been established as an **External ID** using [SCIM](#)
5. Edit the **SAML Certificates**
 - a. Set the **Signing Option** to *Sign SAML response and assertion*
 - b. Ensure the **Signing Algorithm** is *SHA-256*
6. Download your **Certificate (Base 64)**
7. Record the **Set up [enterprise application]** details to enter into Lt


Basic SAML Configuration  Edit


Identifier (Entity ID)	https:// [region] .kuracloud.com/i/XXXXXXX /saml2
Reply URL (Assertion Consumer Service URL)	https:// [region] .kuracloud.com/i/XXXXXXX /saml2-ss/o/acs
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	https:// [region] .kuracloud.com/i/XXXXXXX /saml2/slo


Attributes & Claims  Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Certificates

Token signing certificate  Edit




Status	Active
Thumbprint	
Expiration	11/23/2025, 2:47:09 PM
Notification Email	@ .onmicrosoft.com
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/"/> .. 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) (Preview)  Edit

Required	No
Active	0
Expired	0

Set up LT Dev 2

You'll need to configure the application to link with Azure AD.

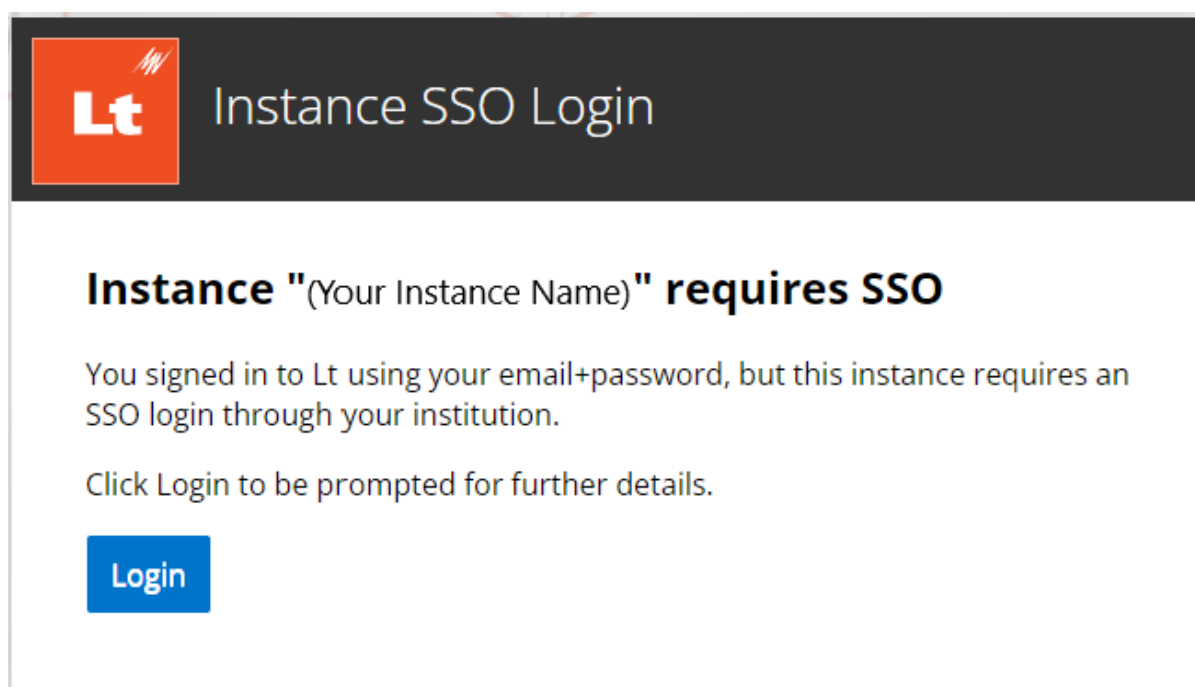
Login URL	<input type="text" value="https://login.microsoftonline.com/"/> ... 
Azure AD Identifier	<input type="text" value="https://sts.windows.net/"/> ... 
Logout URL	<input type="text" value="https://login.microsoftonline.com/"/> ... 

8. Return to the Lt **SAML 2.0 Settings**
9. Select **Configure**
10. Enter the details from Microsoft Azure
 - a. Set **User Identified By** to *Email address* or *SCIM externalId* as appropriate
 - b. The **Azure AD Identifier** as the **Entity Id**
 - c. The **Login URL** as the **Service URL (Redirect only)**
 - d. Open the **Certificate (Base 64)** in a text editor and copy the contents into the **X509 Certificate**

Enforcing SSO

Logging in using email and password can be disabled for your instance for all users using a particular email domain. This allows you to control how your users login and enforce using SSO. This is limited to one email domain so you can restrict the access of your students and staff while allowing for guest users and emergency access.

Users that attempt to login with an email and password will be blocked and instead directed to login using your IDP via the Service URL entered when setting up SAML.



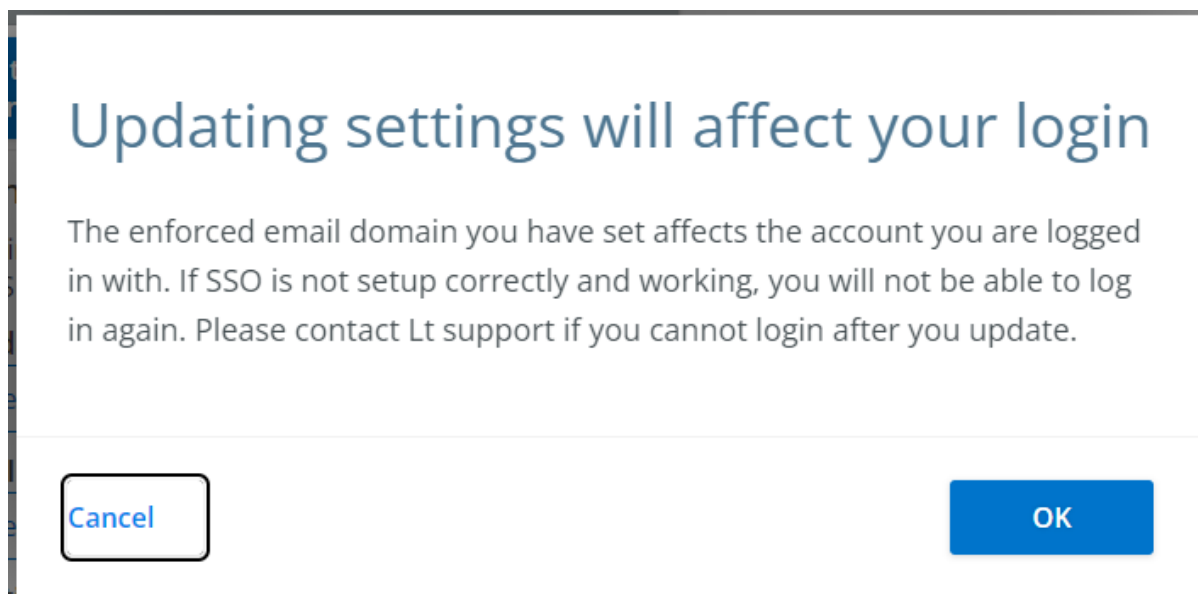
The screenshot shows a dark header bar with the Lt logo on the left and the text "Instance SSO Login" on the right. Below the header, the main content area has a white background. It features a bold heading: "Instance "(Your Instance Name)" requires SSO". Underneath, a paragraph explains: "You signed in to Lt using your email+password, but this instance requires an SSO login through your institution." Below this is a line of text: "Click Login to be prompted for further details." At the bottom of this section is a blue button with the word "Login" in white text.

This message will be displayed to users that attempt to login without using SSO. Clicking the Login button will redirect the user to your IDP.

To enable SSO enforcement for a domain:

1. Login as an instance administrator, preferably using SSO to login.
2. Select **Instance Administration**.
3. Select **SAML 2.0 Settings**.
4. Select **Edit Configuration**.
5. Select **Advanced Settings**.
6. Fill in the **Email domain requiring SSO** with the email domain you want to restrict. Usually this will be your institution's email domain. You do not need to include the "@".
Example: gmail.com
7. Select **OK**.

Warning: Enforcing SSO will also affect administrators including yourself. If your logged in account is covered by the domain restriction, you will see a confirmation dialog before the change is applied. Please make sure that you have tested your SSO setup before enabling enforcement.



Enforcement is based on the email domain that the user was originally invited with. Users that have later changed their email address to a different domain will still be restricted based on the domain they were originally registered with.