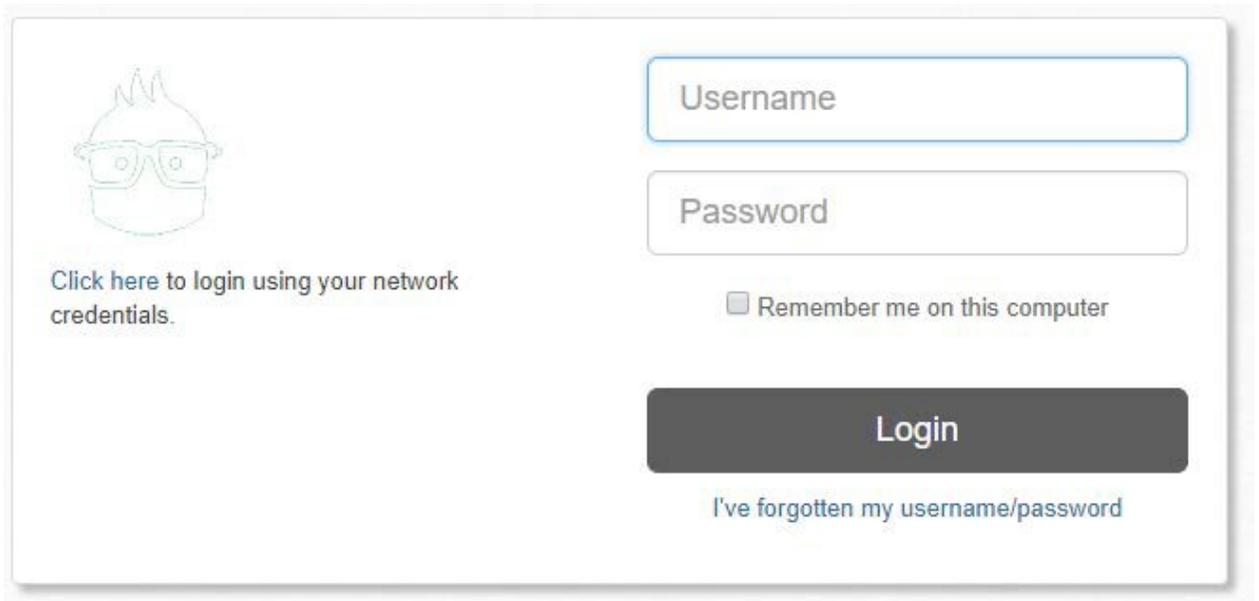


Configuring Litmos

Users can securely log on to Litmos using their enterprise credentials. To configure Litmos for SSO through SAML, follow the steps below:

1. In a browser, type <https://<your-organization>.Litmos.com/> and press enter.
Note: For example, if the URL you use to access pager duty is <https://myserver.Litmos.com>, then you must replace <your-organization> with myserver.
2. Log on to your Litmos account as an administrator.



Click [here](#) to login using your network credentials.

Username

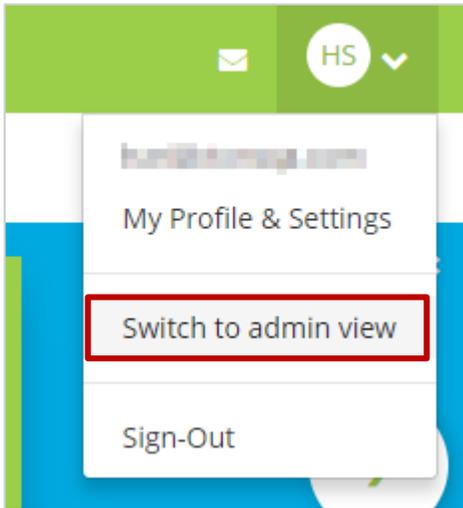
Password

Remember me on this computer

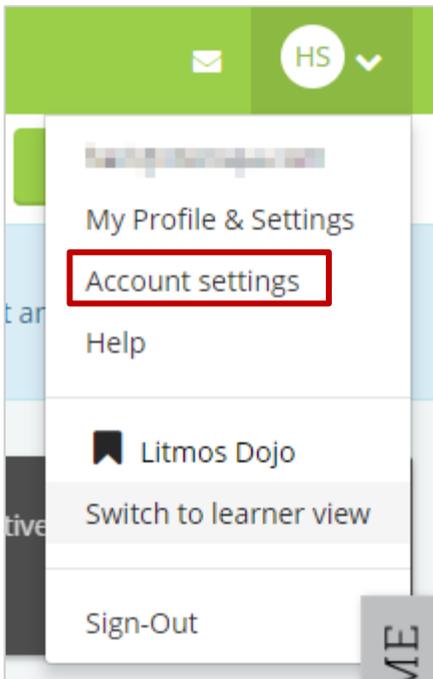
Login

[I've forgotten my username/password](#)

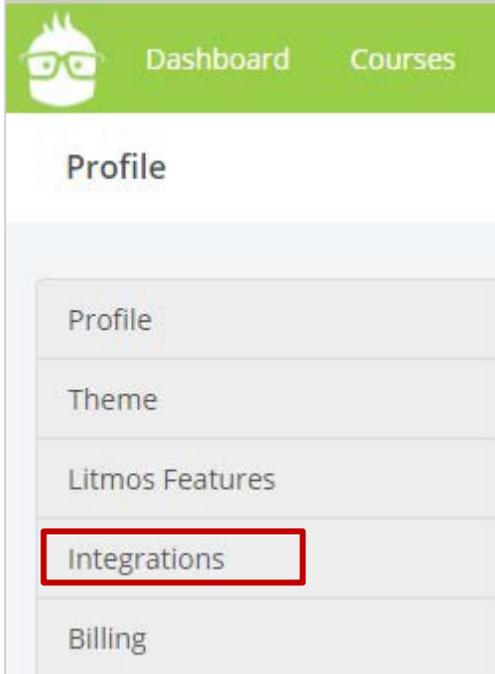
3. On the home page, in the upper right corner, click the profile arrow and click **Switch to admin view**.



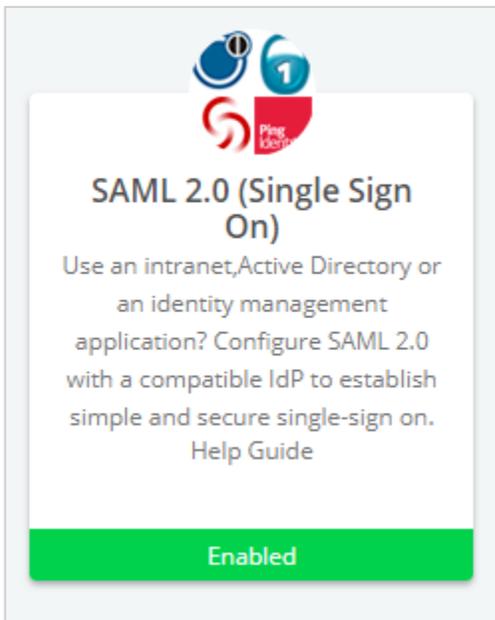
4. After enabling the admin view, in the upper right corner, click the profile arrow and click **Account Settings**.



5. On the **Profile** page, click **Integrations**.



6. On the Litmos Integrations page, click **SAML 2.0 (Single Sign On)**.



7. Click the **Okta and OneLogin users click here** link.

Complete the steps below to configure SAML authentication from your identity provider.

Below are a list of identity providers that support SAML authentication with Litmos:

http://www.okta.com	http://www.onelogin.com
http://www.centify.com	http://www.pingidentity.com
http://azure.microsoft.com	

SAML Metadata

Paste XML Metadata here

Autogenerate Users
(this will automatically create users if they don't exist when logging in)

The SAML endpoint for litmos is:
<https://ctxnsqa.litmos.com/integration/splogin>

Accepted Attributes:
Email, FirstName, LastName

[Okta and OneLogin users click here](#)

Save changes Close

8. Specify the following information for the required fields:

Use an intranet, Active Directory or an identity management application? Configure SAML 2.0 with a compatible IdP to establish simple and secure single-sign on.

Below are a list of identity providers that support SAML authentication with Litmos::

http://www.okta.com http://www.onelogin.com
http://www.centrify.com http://www.pingidentity.com
http://azure.microsoft.com

Enable SAML **1**

Origin URI: **2**
https://...l.com

SAML x.509 Certificate: **3**
PA6WlHq80Q5Ll9q7G4n...R54F0Z73oL3hotrel+ilU9lo/fda5usH3Qld9OXy
+
E
C
U
6ED5
-----END CERTIFICATE-----

Autogenerate Users **4**
(this will automatically create users if they don't exist when logging in)

The SAML endpoint for litmos is:
<https://...litmos.com/integration/samllogin>

SAML Endpoint for ADFS integrations:
<https://...litmos.com/integration/samllogin?adfs=1>

Accepted Attributes:
Email, FirstName, LastName

5
Save changes Close

- i. **Enable SAML**– select the check box.
- ii. **Origin URI** –type your NetScaler FQDN.
- iii. **SAML x.509 Certificate** – This is IdP signing certificate
Click **Browse** to browse to the folder where you saved the IdP provided certificate and upload it.

