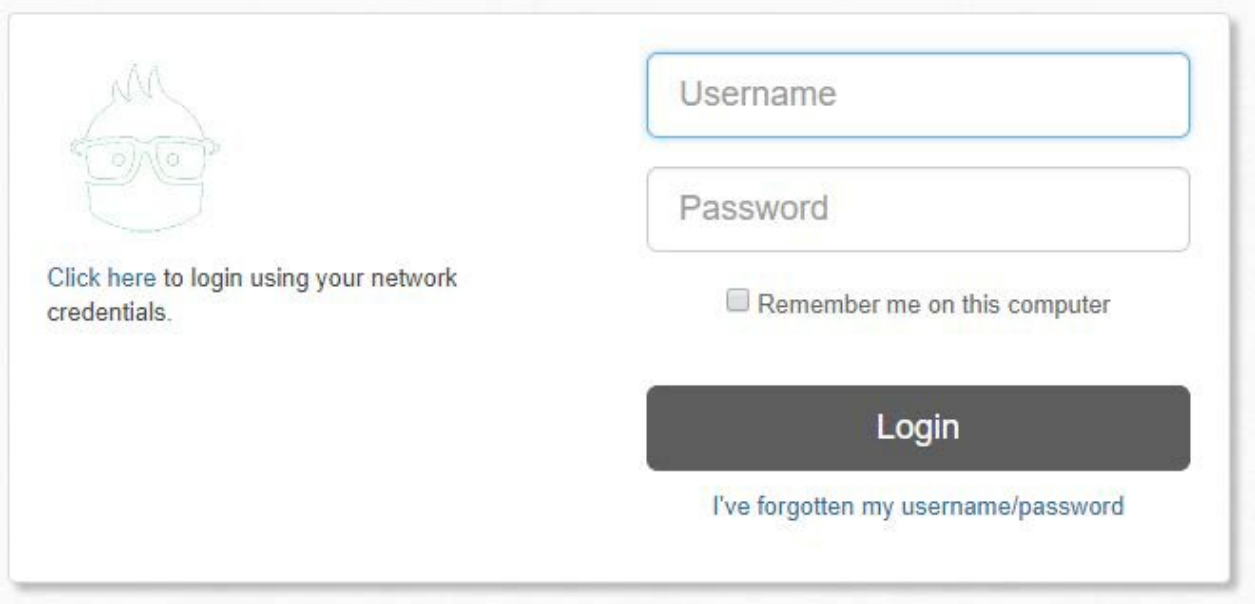
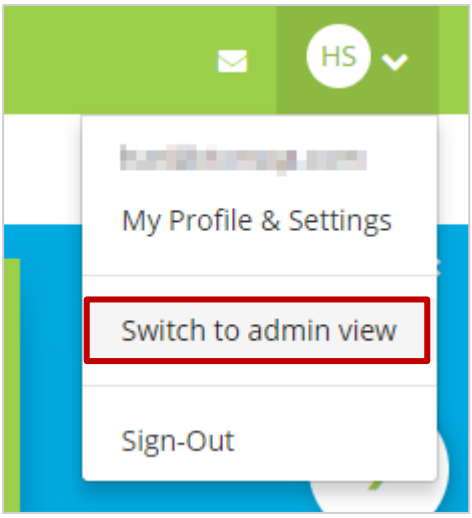
# Configuring Litmos

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

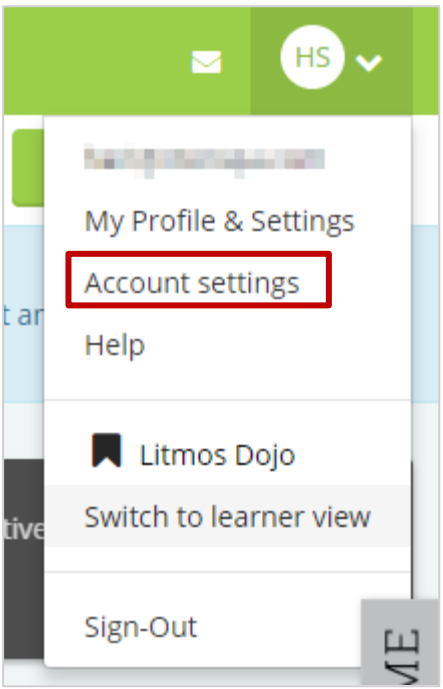
1. In a browser, type https://<your-organization>.Litmos.com/ and press enter.
   **Note**: For example, if the URL you use to access pager duty is https://myserver.Litmos.com, then you must replace <your-organization> with myserver.
2. Log on to your Litmos account as an administrator.



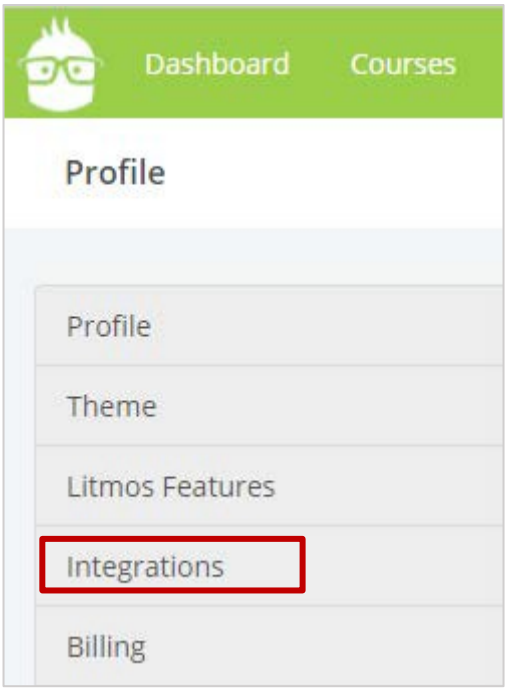
3. On the home page, in the upper right corner, click the profile arrow and click **Switch to admin view**.



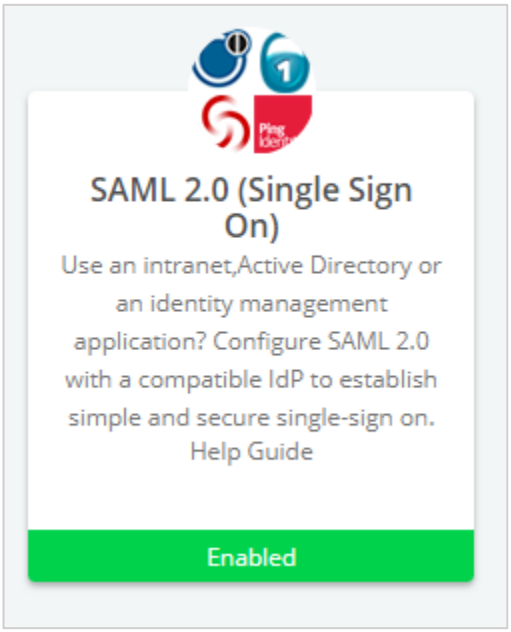

4. After enabling the admin view, in the upper right corner, click the profile arrow and click **Account Settings**.



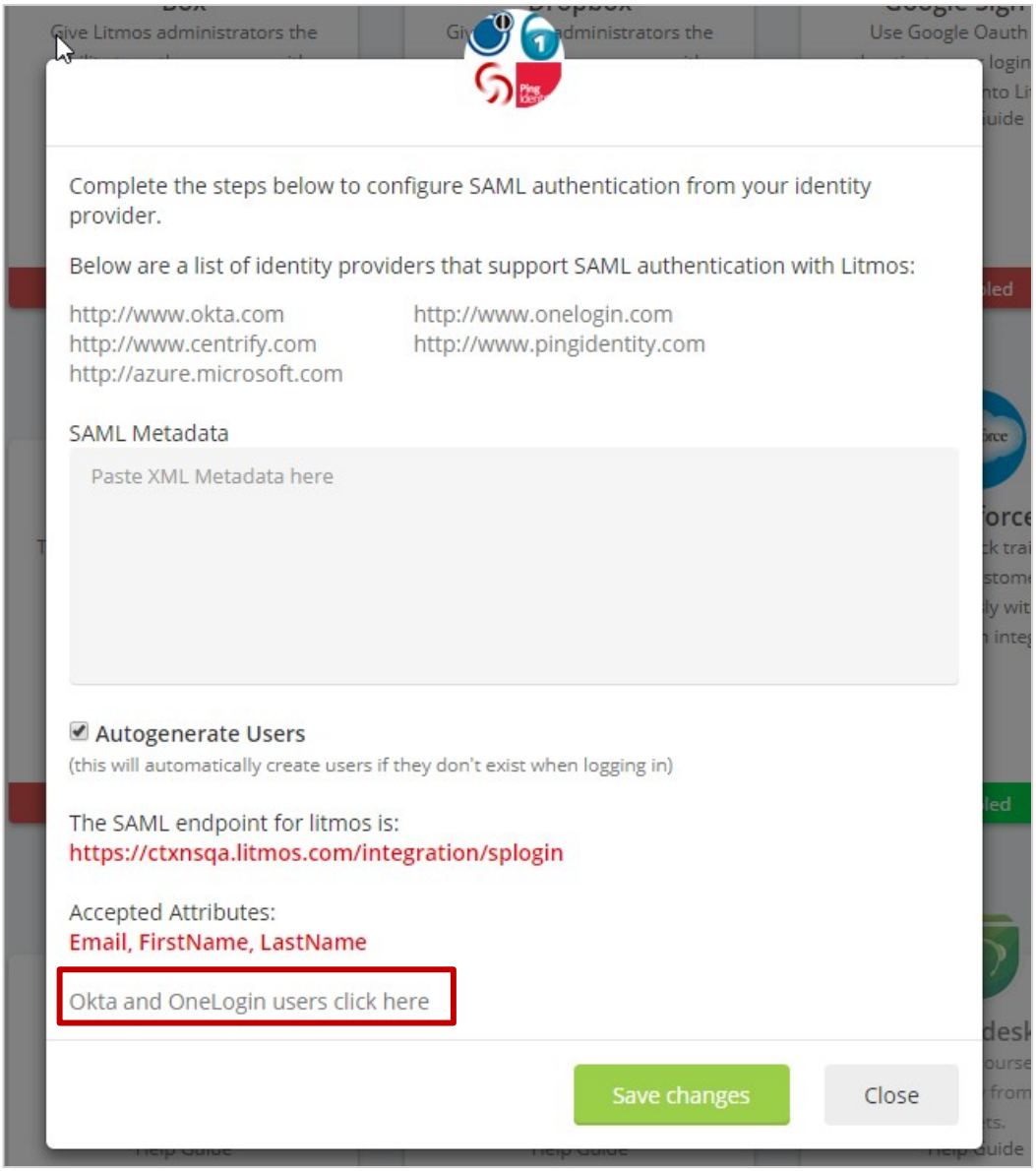
5. On the **Profile** page, click **Integrations**.



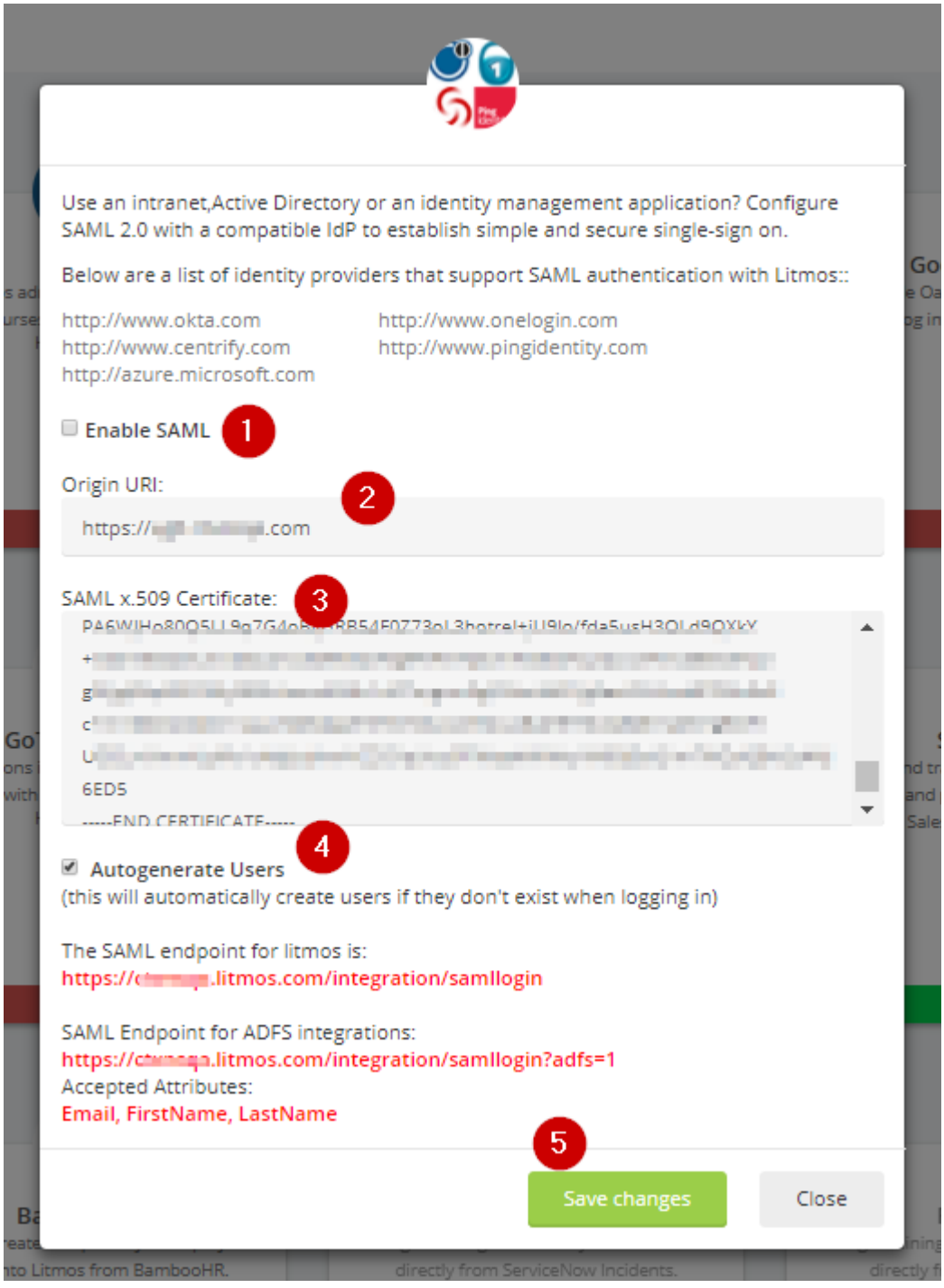

6. On the Litmos Integrations page, click **SAML 2.0 (Single Sign On)**.



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



8. Specify the following information for the required fields:




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.

To obtain your IdP X.509 certificate, follow the steps below:

i. Remotely access your NetScaler instance using PuTTY.
ii. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.
iii. Type cat <certificate-name> and press Enter.


iv. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----
v. Paste the text in a text editor and save the file in an appropriate format such as <your organization name>.pem

iv. **Autogenerate Users** – select the check box to allow account creation of non-SAML users.
v. Click **Save Changes**.

You have completed the required configuration for the service provider which is in this case –Litmos.