Configuring Litmos

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

- 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 <u>https://myserver.Litmos.com</u>, then you must replace <your-organization> with myserver.
- 2. Log on to your Litmos account as an administrator.

And	Username
Level -	Password
Click here to login using your network credentials.	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**.

Dashboard	Courses
Profile	
Profile	
Theme	
Litmos Features	
Integrations	
Billing	

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:

	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.	
s ad	Below are a list of identity providers that support SAML authentication with Litmos::	Go
urse: F	http://www.okta.com http://www.onelogin.com http://www.centrify.com http://www.pingidentity.com http://azure.microsoft.com	og i
	Enable SAML	
	Origin URI:	
	https://	
GO ons i with	SAML x.509 Certificate: PA6WiHo8005LI 907G40b PRB54F0773ol 3botrel+il I9lo/fda5usH30Ld90XkV + g c U GED5 END CERTIFICATE	nd t and Sale
	https://caraaja.litmos.com/integration/samllogin	
	SAML Endpoint for ADFS integrations: https://chmnqn.litmos.com/integration/samllogin?adfs=1 Accepted Attributes: Email, FirstName, LastName	
Ba	Save changes Close	inin
nto Li	tmos from BambooHR. directly from ServiceNow Incidents. dire	ctly

- 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.

1		the second such that	ingental), ingen	Charlen and and		YTEU
B	and the second second	B1 8 19 19 11 11 12 1				NDk1
2			in the second	at a partie had a	a state	MDEx
1	Street and Links	C. Brief Hart	States and a state	and the second second		MRYW
Α	and the lot	-	a designed and a	and the second se	and the second second	aWR1
ji ma ma m	a second stand					Bgkq
k		ALC: NAME OF TAXABLE	A CONTRACTOR OF THE			7aff
С	1		Course of the		State of Street of Street	50yZ
a	General States of the	the local dates	Contraction of the local data	all states of the same states	States and the second strends	FF3k
+	discount of a	-		and discount of the same	a billion and a firm	H99Z
x	A CONTRACTOR OF			NAME OF TAXABLE PARTY.		hr8i

- 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.