Configuring Kintone

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

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

Login Name	
Password	
Having Trouble Logging In?	
Remember me	Login

3. On the home page, click **Administration**.



4. On the **Service Usage** page, in the left pane, scroll down to the **System Administration** section and under **Security**, click **Login**.

System Administration	
Customize	
Header	
Login Page	
Security	
Login	
Access Control	
Session Settings	

5. On the **Login Security** page, scroll down to the **SAML Authentication** section and select the **Enable SAML authentication** check box.

SAML Authentication	Enable SAML authentication

The section expands and displays additional fields.

6. In the expanded SAML Authentication section, specify the following information:

SAML Authentication	Enable SAML authentication
	Login URL 1
	https://www.com/saml/login
	Logout URL 2
	https://uni maga.com/cgi/tm/logout
	Certificate
	Current Certificate
	x509pem (Expiration Date: Aug. 30, 2018)
	Select a Certificate
	3 Browse (Maximum: 100 KB)
	📧 Download Service Provider Metadata 🛛 🕢

- i. **Login URL** type the login URL in https://<your organizationFQDN>/saml/login format.
- ii. **Logout URL** type a redirect URL to which you want users to be redirected after they log out from Kintone.
- iii. **Certificate** Upload the 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 marries, will be stationed	CARLO AND INCOME		and the post is a	YTE
Brid	and the second second		and the second states in the second	and south the second south		NDk
2			And in case of the local division in the loc	the Real Property lies and		MDE
1	alimente mais de mais	a second second second	and the local			MRY
A	Contract State		State and state	manifold a linea	A DECK OF THE OWNER.	BWR
it has seen in	a state of the local division of the	a la manage a partie	AND IN COLUMN			Bak
k -	-	a second states and				7af
C	1.00	a to the start of	the Party of the Party of the	and the second second	A DE LA LA LA LA	50v
a	Section 2.1	- Hardings in sec.	and the later of the second	times in the second		FFS
+			-		A DESCRIPTION OF THE OWNER OF THE	899
x	and the second second	A DESCRIPTION OF THE OWNER OF THE		THE IS NOT		hr8

- 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. To download the metadata in XML format, Click **Download Service Provider Metadata**.
- 7. Click Save.



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