## **Configuring Mango**

Username	
helige beinge dels	
Password	
Login	Forgot Password?

1. Login to MangoApps as an Admin user.



 From the top right corner move cursor on your account name > List will appear, Click on Manage Domain.



3. Admin window will open > From the left panel select SSO.

Single Sign-On (SSO) > SAML	
Active Directory/LDAP SAML 0AUTH 2.0 Cust	m SSO

4. Single Sign-On window will open > Click on SAML.

General Setting:			
1 🗸 Allow SAML based federated logir	1 1		
2 🗸 Auto User Provisioning 👔			
Servers:			Add New Server
Server 1 (Other SAML Providers)			~
Provider	Other SAML Providers v i 3		
Provider Name *	UG_VPN_Mangoapp	i 4	
Login Page Auto Re-direct	✓ ī 5		
Read from meta data url (Optional)		Read	
	If your IDP provides a meta data url, MangoApps can directly read the xml and aut fields below.	p populate the	
Issuer URL/EntityID (HTTPS) *	https://mangoapps.com	6	
	This is the URL from where all SAML requests have to be issued in order to be trusted by MangoApps. Your Identity Provider should give you this URL. SAML requests from other URLs will be not be trusted and hence ignored.		

Assertion Consumer Service	https://mangoapps.com/saml/consume	7	
URL (HTTPS)	Default Assertion Consumer Service (ACS) URL is https://ctxnsqa.mangoapps.com/saml/consume.		
SAML 2.0 Endpoint/SSO URL (HTTPS) *	https://ug1com/saml/login	8	
	This is the URL that MangoApps will invoke to re-direct users to your identity provider.		
Remote Logout URL (HTTPS) *	https://ug1 .com/cgi/logout	9	
	This is the URL that MangoApps will redirect your users to after they log out.		
Authentication Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTran 10		
	SAML authentication context classes your idp supports, recomended values are "urr:coasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport" (Default) and "urr.federation:authentication:windows" for more information please visit https://msdn.microsoft.com/en-us/library/hh599318.aspx		
User Identifier	Email	11	
	The field name that uniquely identifies the user in the configured SSO SAML provider.		
x509 Certificate *	BEGIN CERTIFICATE	12	
	REPORT PROPERTY AND A REPORT OF A REPORT O		
	REACTIVE CONTRACT CONTRACTOR OF CONTRACT OF CONTRACTOR OF CONTRACT OF CONTRACTOR OF CONTRACT OF CONTRACT.		
	the first of the second state of the second state of the second state		
	The y500 certificate for authenticating your Identity Provider Obtain this from your		
	SAMI identity provider		

## 5. **F**ill the template with appropriate values

Field Name	Values
Allow SAML based federated login	Should be <b>checked</b>
Auto User Provisioning	Should be <b>checked</b>
Provider	Other SAML Provider
Provider Name	As mentioned in IdP
Login Page Auto Re-direct	Should be <b>checked</b>
Issuer URL/EntityID(HTTPS)	https:// <customer_domain>.mangoapps.com</customer_domain>
	https:// <customer_domain>.mangoapps.com/saml/</customer_domain>
Assertion Consumer Service URL(HTTPS)	<u>consume</u>
SAML 2.0 Endpoint/SSO URL(HTTPS)	https://ug1. <customer_domain>.com/saml/login</customer_domain>
Remote Logout URL(HTTPS)	https://ug1. <customer_domain>.com/cgi/logout</customer_domain>
	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordPr
Authentication Method	otectedTransport (Default)
User Identifier	Email
x509 Certificate	Paste IdP certificate

## 6. Click on Save Settings.