Yellowfin SAML Bridge Integration with AAD

The Yellowfin SAML Bridge is a Java web application that is used for interfacing between a SAML Identity Provider and Yellowfin. This way users can use the same credentials that they use for other applications at their organisation. The Yellowfin SAML Bridge in this case is a SAML Service Provider (SP). The SAML Bridge uses Yellowfin’s web services to SSO the user into Yellowfin. Azure AD in this case is the SAML Identity Provider (IdP).

A **Non-gallery Enterprise Application** needs to be created by an Azure AD Global Admin & Single-Sign-On configured as per the mappings in the table below:

SAML Bridge OneLogin Element	**AAD Single Sign-on Mapping**	**Section**	**Value**
onelogin.saml2.sp.entityid	Identifier (Entity ID)	Basic SAML	https://<YF_FQDN>:8443/samlbridge/metadata.jsp
onelogin.saml2.sp.assertion_consumer_service.url	Reply URL (Assertion Consumer Service URL)		https:// <YF_FQDN>:8443/samlbridge/acs.jsp
onelogin.saml2.organization.url	Sign on URL		https:// <YF_FQDN>:8443/samlbridge/dologin.jsp
N/A	Relay State		Leave Blank
SAMLBridgeWebXML FirstNameAttribute -> http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Givenname	User Attributes & Claims	user.givenname
SAMLBridgeWebXML LastNameAttribute -> http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Surname		user.surname
SAMLBridgeWebXML FullNameAttribute -> http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Name		user.userprincipalname
SAMLBridgeWebXML EmailAttribute -> http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Emailaddress		user.userprincipalname

SAMLBridgeWebXML UsernameAttribute -> http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Unique User Identifier		user.userprincipalname
N/A	Status	SAML Signing Certificate	Active
N/A	Thumbprint		Auto-generated with the creation of the Non-gallery Enterprise Application
N/A	Expiration		Auto-generated with the creation of the Non-gallery Enterprise Application
N/A	Notification Email		Email address of the person who creates the Non-gallery Enterprise Application
N/A	App Federation Metadata Url		Auto-generated with the creation of the Non-gallery Enterprise Application
onelogin.saml2.idp.single_sign_on_service.url	Login URL	Set up <Name_of_your_Enterprise_app>	https://login.microsoftonline.com/<AzureTenantId>/saml2
onelogin.saml2.idp.entityid	Azure AD Identifier		https://sts.windows.net/<AzureTenantId>/
onelogin.saml2.idp.single_logout_service.url	Logout URL		https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

SAML Bridge OneLogin SAML Properties File: Other Settings

onelogin.saml2.strict = **true** #Set this True For Prod Environment

onelogin.saml2.debug = **false** #Set this False for Prod Environment, unless investigating an issue

onelogin.saml2.sp.single_logout_service.url = **https:// <YF_FQDN>:8443/samlbridge/sls.jsp**

onelogin.saml2.sp.nameidformat = **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**

onelogin.saml2.sp.x509cert = **<LEAVE BLANK AS SETTING IN TOMCAT ./conf/server.xml file>**

onelogin.saml2.sp.privatekey = **<LEAVE BLANK AS SETTING IN TOMCAT ./conf/server.xml file>**

onelogin.saml2.idp.single_logout_service.response.url = **<LEAVE BLANK>**

onelogin.saml2.idp.x509cert =**<Enter Cert here obtained from Azure AD SSO Page – Remember, this needs to be 'All on one line'>**

onelogin.saml2.security.requested_authncontext = **urn:oasis:names:tc:SAML:2.0:ac:classes:Password** #Change to be this, instead of what the default settings are in the template example file

onelogin.saml2.organization.name = **<ENTER ORGANISATION NAME>**

onelogin.saml2.organization.displayname = **<ENTER ORGANISATION DISPLAY NAME>**

onelogin.saml2.organization.url = **https:// <YF_FQDN>:8443/samlbridge/dologin.jsp**

onelogin.saml2.contacts.technical.given_name = **<CONTACT FIRSTNAME + LASTNAME>**

onelogin.saml2.contacts.technical.email_address = **<CONTACT EMAIL ADDRESS >**

onelogin.saml2.contacts.support.given_name = **<CONTACT FIRSTNAME + LASTNAME>**

onelogin.saml2.contacts.support.email_address = **<CONTACT EMAIL ADDRESS >**

Configuration Database Update

NOTE: SSO via Azure AD continued to fail until this code was applied (My DB = SQLServerAzure)

```
BEGIN
   IF NOT EXISTS (SELECT * FROM dbo.Configuration WHERE
dbo.Configuration.ConfigCode = 'SIMPLE_AUTHENTICATION')
   BEGIN
       INSERT INTO dbo.Configuration (IPORG,CONFIGTYPECODE, CONFIGCODE,
CONFIGDATA)
       VALUES ('1','SYSTEM', 'SIMPLE_AUTHENTICATION', 'TRUE')
   END
END
```

SAML Bridge web.xml config changes (i.e. ./ appserver/webapps/samlbridge/WEB-INF/web.xml)

```
…
    <param-name>YellowfinWebserviceURL</param-name>
    <param-value>https://<YF_FQDN>:8443</param-value>
…
    <param-name>YellowfinWebserviceUser</param-name>
    <param-value>admin@yellowfin.com.au</param-value>
…
    <param-name>YellowfinWebservicePassword</param-name>
    <param-value><Update as appropriate></param-value>
…
    <param-name>EmailAttribute</param-name>
    <param-value>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</param-value>
…
    <param-name>FirstNameAttribute</param-name>
    <param-value>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</param-value>
  </init-param>
  <init-param>
    <param-name>LastNameAttribute</param-name>
    <param-value>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</param-value>
  </init-param>
  <init-param>
    <param-name>FullNameAttribute</param-name>
    <param-value>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</param-value>
  </init-param>
  <init-param>
    <param-name>UsernameAttribute</param-name>
    <param-value>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</param-value>
  </init-param>
  <init-param>
    <param-name>YellowfinRole</param-name>
    <param-value>Consumer &amp; Collaborator</param-value> #Choose an appropriate ‘default’ role
  </init-param>
  <init-param>
    <param-name>AutoProvision</param-name>
    <param-value>true</param-value>
  </init-param>
   <load-on-startup>1</load-on-startup>
 </servlet>
```