SAML Configurations

SAML Service Provider Configuration

The following properties need to be set to configure the Service Provider (the Yellowfin SAML Bridge). There are inline comments with the properties file that give more information about each option.

Consider the following scenario:

- You access Yellowfin via *http://yellowfin:8080/*.
- You have a SAML Bridge being installed in the ***Yellowfin/appserver/webapps/samlbridge*** folder.
- The name of your AD FS is **adfs.local**.

Here is how you will configure the Service Provider settings based on this scenario.

Property	Description
onelogin.saml2.sp.entityid	The entityId of the SAML Bridge SP. This will be the metadata URL for the SAML Bridge. The URL is of the form: **<scheme>://<host>:<port>/<context>/metadata.jsp**. The metadata.jsp file is located in the 'samlbridge' folder. This can be used to register the SAML Bridge SP in AD FS. For instance, http://yellowfin:8080/samlbridge/metadata.jsp *Note: Ensure that this URL is accessible from AD FS.*
onelogin.saml2.sp.assertion_consumer_service.url	This is the URL that handles a successful authentication. Yellowfin does it via **samlbridge/acs.jsp**. For instance, http:// yellowfin:8080/samlbridge/acs.jsp *Note: The SP entityid must be registered with the AD FS to allow user access to this service. For information on how to register, click here.*
onelogin.saml2.sp.single_logout_service.url	This is the URL that handles logging off. The **samlbridge/sls.jsp** file is used for this purpose. For instance, http:// yellowfin:8080/samlbridge/sls.jsp
onelogin.saml2.sp.x509cert	This is the text representation of a security certificate. A self-signed certificate can be generated with: **openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out sp.crt -keyout sp.pem** The text representation of the **sp.crt** from the above command is required for this option.
onelogin.saml2.sp.privatekey	This is the text representation of the certificate's private key. This is the text representation of the **sp.pem** file that was created by the self-signed certificate process above.
onelogin.saml2.sp.nameidformat	This is required by the OneLogin SAML; it should correspond to the Name ID format of the AD FS. Can be one of: NAMEID_EMAIL_ADDRESS = 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress'; NAMEID_X509_SUBJECT_NAME = 'urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName'; NAMEID_WINDOWS_DOMAIN_QUALIFIED_NAME = 'urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName'; NAMEID_UNSPECIFIED = 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified'; NAMEID_KERBEROS = 'urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos'; NAMEID_ENTITY = 'urn:oasis:names:tc:SAML:2.0:nameid-format:entity'; NAMEID_TRANSIENT = 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient'; NAMEID_PERSISTENT = 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent'; NAMEID_ENCRYPTED = 'urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted'; *Note: Any changes made to the **onelogin.saml.properties** file will require the Yellowfin SAML Bridge to be restarted for new settings to take effect.*

SAML Identity Provider (IDP) Configuration

The Yellowfin SAML Bridge uses the OneLogin Java API to interface with SAML Identity Providers (IDP). The **WEB-INF/classes/onelogin.saml.properties** file is also used to set up configuration of the SAML IDP.

Each SAML Identity Provider will require different options to be filled out in the properties file. Below is a list of what the AD FS requires.

Property	AD FS requirement
onelogin.saml2.idp.entityid	https://adfs.local/adfs/ls/IdpInitiatedSignon.aspx?loginToRp=Yellowfin ***Note.*** *You can find more details in the 'SSO service (IdpInitiatedSignOnPage)' chapter of this guide.*
onelogin.saml2.idp. single_sign_on_service.url	https://adfs.local/adfs/ls/IdpInitiatedSignon.aspx?loginToRp=Yellowfin ***Note.*** *Still filled in, however, maybe not required.*
onelogin.saml2.idp. single_logout_service.url	https://adfs.local/adfs/ls?wa=wsignout1.0
onelogin.saml2.idp.x509cert	This is required to sign SAML requests before sending them to AD FS. You can find more details in the AD FS Public Key chapter of this guide. ***Note.*** *There may be issues with key size. See Troubleshooting – Illegal Key Size chapter.*

*Note: Any changes made to the **onelogin.saml.properties** file will require the Yellowfin SAML Bridge to be restarted for the new settings to take effect.*

Previous topic: SAML bridge overview
Next topic: AD FS configuration