#  OKTA INTEGRATION FOR AUTOMIC

There are 2 main steps to implement OKTA / SAML for Automic.

Currently, LDAP or AD authentication is enabled for Automic. No changes need to be made to these settings – they can be left as is.

## Step 1 – Server modifications

The following files are required for OKTA / SAML integration. Ensure they exist or are copied into the /u02/automic/v12/automationengine/bin/lib directory.

* orai18n.jar
* xdb6.jar
* xmlparserv2.jar

For Takeda, 2 of the 3 files are already in the ./lib directory. These are required to make sure that XML variables are processed correctly. So only the highlighted file needs to be copied.

Edit the /u02/automic/v12/tomcat/webapps/awi/config/configuration.properties file on the web server (s). Add in the following lines / parameters:

* sso.saml.enabled = true
	+ This enables single sign-on (SSO)

 

## Step 2 – Automic Client 0 Variable modifications

Use UC\_SYSTEM\_SETTINGS to enable SAML. No restart is needed for this change to take effect.

* SAML = Y

UC\_SAML\_SETTINGS already exists in client 0, but it is empty / unpopulated. This is what you use to configure SAML and link departments.

As soon as you add SAML = Y to UC\_SYSTEM\_SETTINGS then a \*SP (service provider) keyword is added to UC\_SAML\_SETTINGS. The \*SP key contains the metadata (xml) of the service provider of the AE and the URL of the AWI.

The value of this \*SP keyword will have 3 places where changes need to be made. These are indicated with "\*\_INSERT\_\*". However, you will only edit / update 2 of the instances initially.

* Location attribute for HTTP-POST
	+ Replace the value of the Location attribute with the URL that points to your AWI instance or load balancer
	+ Location ="<https://www.example.com/awi/>"
* Location attribute for HTTP-Artifact
	+ Replace the value of the Location attribute with the URL that points to your AWI instance or load balancer
	+ Location ="<https://www.example.com/awi/>"

Copy the entire content of \*SP value and send it to the OKTA team.

The OKTA team will send you back an XML file and the link to the XML file (referred to as the URI).

Update the 3rd location in the \*SP keyword with the URI.

* entityID
	+ Replace the value of the entityID attribute with the URI that points to the Service Provider. This is the link or URL to the metadata that the OKTA team generated.

Add in a new keyword into the UC\_SAML\_SETTINGS called CORP. Multiple domains can be added, but we only have 1 – CORP. This is the “Department” that is used for all the users on the system (i.e. LAURA/CORP).

Copy the contents of the metadata that the OKTA team sends – this will be in an XML file, to the value of the CORP keyword.

\*\*

The OKTA team will need to ensure that anyone who needs to login to the AE is in their OKTA “group”. At Takeda this is managed with an AD group.

Links to Documentation that have additional details:

<https://docs.automic.com/documentation/webhelp/english/ALL/components/DOCU/12.3/Automic%20Automation%20Guides/help.htm#AWA/Variables/UC_SAML_SETTINGS_SSO.htm?Highlight=SAML>

<https://docs.automic.com/documentation/webhelp/english/ALL/components/DOCU/12.3/Automic%20Automation%20Guides/help.htm#AWA/Variables/UC_SYSTEM_SETTINGS/UC_SYSTEM_SAML.htm?Highlight=SAML>

<https://docs.automic.com/documentation/webhelp/english/ALL/components/DOCU/12.3/Automic%20Automation%20Guides/help.htm#Installation_Common/SetUp_SAML_SSO.htm?Highlight=SAML>

<https://docs.automic.com/documentation/webhelp/english/ALL/components/DOCU/12.3/Automic%20Automation%20Guides/help.htm#Installation_Manual/AWI/AWI_config_configuration_properties.htm>