# Requirements:

# SAML IDP metadata file

Reference: <https://www.samltool.com/idp_metadata.php>

Required fields for a metadata file:

1. entityID :- A unique identifier provided my idp to ensure request is received from the correct endpoint. MUST be unique for different teams
2. X509Certificate :- Certificate used to sign the SAML Request
3. SLO Bindings
	1. SingleLogoutService -> HTTP Redirect:
	2. SingleSignOnService -> HTTP Redirect & HTTP Post
		1. Note if your SAML IDP only supports post HTTP Redirect should be commented
	3. The following will contain urls for HTTP Redirect and HTTP Post when a request occurs for Redirect or POST by automic to SAML IDP
	4. E.g: 

# SAML Service configured on Automic: -

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

\*SP file Please update the following details to carter for your specific environment 

entityID – (https\http)://<AWALAB\_URL>/SAML2

WantAssertionsSigned = Boolean (true|false) – note if your SAML is not signed set the parameter to false



AssertionConsumerService: (https\http)://<AWALAB\_URL>

Note: Your SAML NameIDFormat should contain the username or one of the following option is valid

The Automation Engine maps the AE Username with the value of one of the following attributes of the SAML response:

* **subject-id**

**Format:** urn:oasis:names:tc:SAML:2.0:attrname-format:uri

When this attribute is defined, the unique ID that precedes the *@* character is mapped with the AE Username.

* **NameID**

**Format:** urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

The value that is defined here is mapped with the AE Username when no value is defined for **subject-id**. Which part of the value is used to map with the AE Username depends on how the value is defined:

* + **@ character:** If the value contains this character, the part that precedes it is used for mapping
	+ **\ character:** If the value contains this character, the part that follows it is used for mapping
	+ If neither of the characters is used, the complete value is mapped with the AE Username.
* **aename**

**Format:** urn:oasis:names:tc:SAML:2.0:attrname-format:uri)

Use this attribute if you cannot use neither **subject-id** nor **NameID** with your Identity Provider.

**Note:** If this value is defined, it is mapped with the AE Username by default.

# SAML User must be created

The user must be created with Roles assigned in Automic.

SAML is only used for Authentication not Authorization. Authorization is a task assigned to the Admin user of the database

# A Valid SAML Response

