SAML Authentication in Jedox

As of version 2018.4, Jedox offers native support for SAML 2.0. SAML (Security Assertion Markup Language) is an XML-based, open-standard data format for
exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider. SAML simplifies the login process by enabling users to access many services with a single sign-on, which is accomplished through metadata passed between the service provider (Jedox software) and the identity provider (external entity or party).

In Jedox, SAML is mainly used for 3rd-party authentication, as for Cloud connections. Authentication may be server-side (In-Memory DB, Jedox Web) and client-side (Excel Add-in).

Activating SAML in Jedox

1) Define CFG_AUTH_SSO as 'saml' in *<Install_path>\Jedox Suite\httpd\app\etc**config.php*** (Windows) or *<Install_path>/htdocs/app/etc/**config.php*** (Linux).

```
define('CFG_AUTH_SSO',saml);
```

2) Restart the Jedox httpd service or process.

3) Retrieve the metadata XML (which formally describes your

Jedox environment as a service provider) from
*<your_web_instance>/be/**saml.php*** file
(e.g. http://localhost/be/saml.php).

4) Add Jedox as a service provider in your corresponding identity provider with the XML or via the identity ID received in the previous step.

5) Add the following lines to *<Install_path>\olap\data**palo.ini*** (Windows) or *<Install_path>/Data/**palo.ini*** (Linux):

`saml-idp-metadata` (path to metadata XML URL for identity provider)
`saml-authorization` (to enable SVS processing of SAML users)
`saml-use-logout` (to support SAML logout)
`worker "<install_path>\svs\SupervisionServer.exe" workerlogin information`

An example that designates the identity provider as Azure:
`saml-idp-metadata "https://login.microsoftonline.com/1506ab1d-5566-43z5-b5b567f22e31f41/federationmetadata/2018-12/federationmetadata.xml"`
An example that designates the identity provider as Salesforce: `saml-idp-metadata`

```
"https://patwilly-dev-ed.my.salesforce.com/.wel
l-known/samlidp.xml"
```

6) Define the functions OnSAMLUserAuthenticate or OnSAMLUserAuthorize in a supervision script. In the file ***sep.inc.php***, events can be defined or you can reference added scripts with instructions on how the Supervision Server should react to the different events. In the file ***sep.inc.default.php***, basic responses are given to all possible events, including SAML events.

For example, the following script assigns the logged user through the SAML authorization event to the Admin group:

```
public function OnSAMLUserAuthorize(&$username,
array $attributes, array& $groups) { // bool
sep_log("<< User SAML authorize, username
$username >>");
$groups = array("admin");
return true;
}
```

7) Restart the Jedox Services.

The steps above outline basic SAML configuration. Other configuration options are possible; see the table below for more palo.ini keys.

SAML configuration options

Key name	Argument	Description	Default value
saml-authentication		Enables SAML authentication mode.	
saml-authorization		Enables SAML authorization mode	
saml-encrypt-login		Enables encrypting of SAML login requests	
saml-encrypt-logout		Enables encrypting of SAML logout requests	
saml-idp-metadata	<url>	Metadata XML URL for identity provider If metadata is distributed as a file, or server is restricted from accessing the internet, use file://<filepath>	empty string
saml-nameidpolicy	<NameID policy>	SAML NameID policy	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
saml-sign-login		Enables signing the SAML login requests	
saml-sign-logout		Enables signing the SAML logout requests	
saml-signature-algorithm	<algorithm type>	Algorithm used for SAML signatures	http://www.w3.org/2000/09/xmldsig#rsa-sha1
saml-use-logout		Enables SAML identity provider logout **Note:** to enable single logout, you must also define CFG_AUTH_SLO as true in config.php. See section on logout handling below.	

For more information on palo.ini options, see Configuring palo.ini for the In-Memory Database Server.

Authentication mode

In authentication mode, user, user groups, and group-role mappings have to be defined on the Jedox In-Memory DB server. Neither group assignment nor the creation of users will be done automatically.

To activate, add `saml-authentication` to the palo.ini.

Authorization mode

This option eliminates the need to define the user, groups, and group-role mappings on the In-Memory DB server. In this mode, only group-role mappings must be defined directly on the Jedox In-Memory DB server. Users are created automatically and need not be created manually in Jedox.

To activate, add `saml-authorization` to the palo.ini.

Logout handling

Enabling SAML Logout means that during logout, you will be logged out of both Jedox and the identity provider. The next time you login to Jedox, you will have to authenticate in the identity provider again.
Note: SAML logout may not be supported by the identity provider.

To enable single logout, set CFG_AUTH_SLO in config.php to true.
Note: you must also define saml-use-logout in palo.ini.