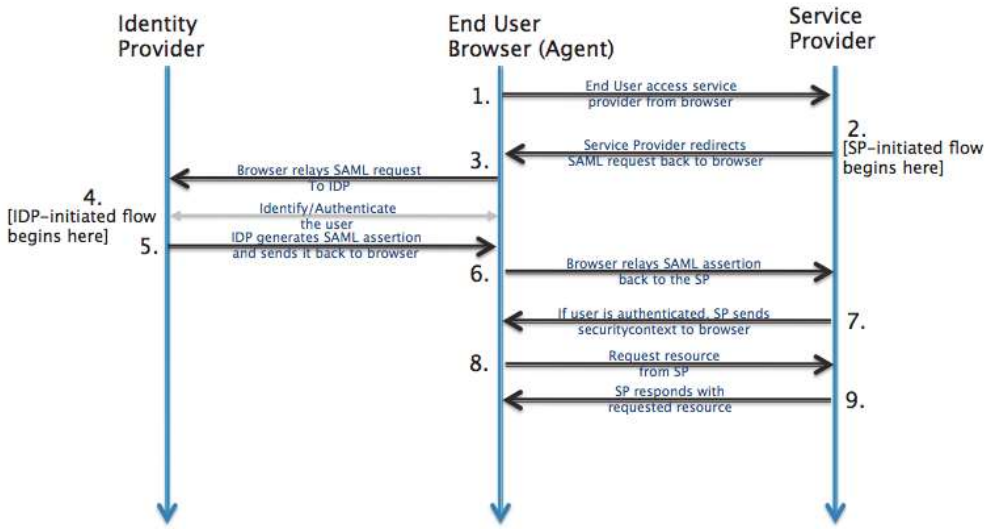
# Registering in WSO2 Identity Server IdP

## SAML: Overview

[1] SAML is mostly used as a web-based authentication mechanism as it relies on the browser being used as an agent that brokers the authentication flow. At high-level, the authentication flow of SAML looks like this:




| | | |
|---|---|---|
| Identity Provider | WSO2 Identity Server | The 3rd-party entity that takes care of the user's authentication; There are multiple such entities with SAML protocol support, such as OpenSSO, SSOCircle.com, OneLogin.com, Salesforce.com…<br>For this example, we'll be using a local install of WSO2 Identity Server |
| End-user browser agent | Pentaho User | User that accesses BA-server via browser |
| Service Provider | BA-server | Pentaho BA Server |

[1] http://developer.okta.com/docs/guides/saml_guidance.html

# Registering in WSO2 Identity Server's Resident Identification Provider (IdP)

## Prerequisites

1. **Have your chosen Service Provider ( i.e. Ba-Server ) metadata xml file at hand**

   **Developer/QA only**: if none is created yet, you can leverage on the already existing SP metadata file for Pentaho BA-Server. For this:
   a. Next to this document, you should have a "`resources`" folder
   b. Download "pentaho-sp.xml" and rename it to something more identifiable with wso2 ( e.g. "pentaho-wso2-sp.xml" );
   c. If the pentaho-sp.xml file contains an encryption KeyDescriptor (`<md:KeyDescriptor use="encryption">`) then comment that section of the metadata out. This document does not cover setting up encryption.

## Installing the WSO2 Identity Server

1. Go to https://wso2.com/identity-and-access-management/
2. Download the Identity Server for your desired platform
3. Run the installer
4. Start the server.
5. Visit https://localhost:9443/carbon/admin/login.jsp
6. Login with the default administrator credentials of admin/admin

## Registering a Service Provider in WSO2 Identity Server

1. Login to WSO2 as an administrative user
2. On the left menu, click on "Add" underneath the "Service Providers" section
3. Select "Manual Configuration"
   a. Under "Basic Information", please follow the table below to fill the fields, if a field is not mention leave it empty

| Field Name | Field value |
|---|---|
| Connected App Name | pentaho |
| Description | |

   b. Click the "Register"
   c. Once registration finishes, expand "Inbound Authentication Configuration"
   d. Expand "SAML2 Web SSO Configuration"
   e. Click the "Configure" link

4. On the “Register New Service Provider” page, select the “Metadata File Configuration” option.
    a. Under “Upload Service Provider Metadata File”, Click the “Choose File” button
    b. Select the pentaho-sp.xml SP Metadata XML file saved earlier and press “Upload”
    c. The screen will redirect to the newly added Service Provider, and the “Application Certificate” should now be filled out.
5. Click on the “Edit” option for the newly added issuer underneath “SAML2 Web SSO Configuration”
    a. Under “Edit Service Provider”, please verify the options match the table below.

| **Field Name** | **Field value** |
|---|---|
| Issuer | pentaho |
| Assertion Consumer URLs | http://{sp server ip:port or name}/pentaho/saml/SSO (e.g., http://localhost:8080/) |
| Default Assertion Consumer URL | http://{sp server ip:port or name}/pentaho/saml/SSO |
| NameID format | urn:osasis:names:tc:SAML:1.1:nameid-format-unspecified |
| Certificate Alias | wso2carbon is the default, and good for development. However, this certificate is distributed with every copy of WSO2, so it is for demonstration purposes only |
| Enable Response Signing | Checkbox: checked |
| Enable Signature Validation in Authentication Requests Logout Requests | Checkbox: checked |
| Enable Assertion Encryption | Checkbox: unchecked |
| Enable Single Logout | Checkbox: checked |
| SLO Response URL | http://{sp server ip:port or name}/pentaho/saml/SingleLogout |
| SLO Request URL | http://{sp server ip:port or name}/pentaho/saml/SingleLogout |
| Enable Attribute Profile | Checkbox: unchecked |
| Enable Audience Restriction | Checkbox: unchecked |
| Enable Recipient Validation | Checkbox: unchecked |
| Enable IdP Initiated SSO | Checkbox: unchecked |

    b. Click “Update” to save the changes

## Creating Users in the Resident Identity/User Store

WSO2 can be configured to federate user identities from other "User Stores." However, to keep things simple, this section only covers setting up "Users" in the local User Store.

1. On the left hand menu, click "Add" under "Users and Roles"
2. On the "Add Users and Roles" page, click "Add New User"
3. Enter a "Username", "Password", and the password again under "Confirm Password"
4. Click "Next >"
5. Select the "Application/pentaho" under "Users of Role"
6. Click "Finish"
7. Continue to add as many additional users as desired

## Getting WSO2 metadata xml file

1. From the left menu, select "Resident" underneath "Identity Providers"
2. Expand "Inbound Authentication Configuration"
3. Expand "SAML2 Web SSO Configuration"
4. Enter a desired "Identity Provider Entity ID"
    a. This document will use a value of "wso2". This value will be used as the **saml.idp.url** property later on in the document.
5. Scroll to the bottom of the page and press "Update"
6. Once the update completes and the page refreshes, expand to the same options again
7. Click the "Download SAML Metadata" button
8. Save the downloaded file, which contains the WSO2 metadata xml.

## Setting pentaho-solutions/system/karaf/etc/pentaho.saml.cfg properties

1. Edit pentaho-solutions/system/karaf/etc/pentaho.saml.cfg
2. Locate property **saml.idp.metadata.filesystem**
    a. Set the path to the WSO2 metadata xml file you downloaded in previous steps
3. Locate property **saml.idp.url**
    a. Open your WSO2 metadata xml file with a text editor of your choice
    b. Locate the "entityID" attribute
        i. The example above should have produced a value of "wso2"
        ii. Copy-paste that value into the saml.idp.url property

## Recap

We have:

1. Installed a WSO2 Identity Server

2. Added a Service Provider called “pentaho”, uploaded the our SP public key, passed the endpoint for it ( `http://localhost:8080/pentaho/saml/SSO` ) and have configured it to work with SAML 2.0

3. Created local User accounts in the Resident User Store of WSO2

4. Configured the Identity Provider to respond to AuthN and SingleLogout requests

5. Got the idp and sp metadata xml files

6. Configured the WSO2 Resident Identity Provider’s Entity ID to use from the “entityID” value

# Q&A

## Q1 | Do I need a certificate to sign the authentication requests?

Yes.

For this sample, we are using a certificate provided by spring-security-saml, stored in a .jks ( keystore file ).

It's already bundled in the saml-authentication-provider sample ( jar:/security/keystore.jks ).

You can get the original here: https://github.com/spring-projects/spring-security-saml/blob/1.0.1.RELEASE/core/src/test/resources/org/springframework/security/saml/key/keystore.jks

This certificate is used by some IdP's, such as SSOCircle.com and okta.developer.com.

If you plan to connect to some other IdPs, then you must ensure you update the keystore file to include the certificate provided by that Identification Provider.