Web Single Sign-On with SAML 2.0

This tutorial demonstrates the usage of SAML 2.0 in different Web SSO Scenarios. We will use Oracle Weblogic Server 12.1.3 as the technical platform.

1 Contents

Web Single Sign-On with SAML 2.0 ................................................................. 1
1 Contents ........................................................................................................... 1
2 Introduction ...................................................................................................... 2
3 The Web SSO Tutorial .................................................................................... 2
3.1 Tutorial Files ................................................................................................ 2
3.2 Documentation Links .................................................................................... 3
3.3 Installation of Java ........................................................................................ 4
3.4 Installation of Weblogic Server 12.1.3 .......................................................... 6
3.5 Example Overview ....................................................................................... 8
3.6 Creating Domains and Deploying Applications .......................................... 13
3.7 Configuring SAML ....................................................................................... 14
3.7.1 create SAML 2.0 Credential Mapper Provider ...................................... 15
3.7.2 configure SAML 2.0 General Settings ..................................................... 16
3.7.3 configure SAML 2.0 Identity Provider ..................................................... 18
3.7.4 export adminA_metadata.xml ................................................................. 19
3.7.5 create SAML 2.0 Identity Assertion Provider ........................................ 20
3.7.6 configure SAML 2.0 General Settings ..................................................... 21
3.7.7 configure SAML 2.0 Service Provider ..................................................... 22
3.7.8 export adminB_metadata.xml ................................................................. 23
3.7.9 create Partner-Idp-adminA ..................................................................... 24
3.7.10 import adminA_metadata.xml ............................................................... 25
3.7.11 configure Partner-Idp-adminB .............................................................. 26
3.7.12 create Partner-SP-adminB ................................................................. 27
3.7.13 Import adminB_metadata.xml .............................................................. 28
3.7.14 configure Partner-SP-adminB .............................................................. 29
3.8 Testing the example ................................................................................... 30
3.8.1 Testing via URL to IdP ........................................................................... 31
3.8.2 Testing via URL to SP ............................................................................ 32
3.9 Setting Debug Flags for the Example ......................................................... 33
3.10 Configuring IdP initiated flow with POST Binding ..................................... 33
3.10.1 Configure an additional end user URL ............................................... 34
3.10.2 Configure the POST Binding POST Form ............................................ 34
2 Introduction

While SAML is already widely used in the industry, the configuration within Weblogic Server is complex and in most companies not part of the regular routine. We want to have look at a simple SAML example that was published in an article by Vikrant Sawant in 2007. [http://www.oracle.com/au/products/database/sso-with-saml-099684.html](http://www.oracle.com/au/products/database/sso-with-saml-099684.html) This former example demonstrates a Web SSO scenario using SAML 1.1 in Weblogic Server 9.2. We want to upgrade this example, using SAML 2.0 in Weblogic Server 12.1.3.

This is a tutorial in which we will walk through all the necessary steps to setup and run the SAML 2.0 example. This includes the installation and configuration of weblogic server, creation of two weblogic server domains, installation of the test applications and configuration of the identity provider and service provider domains. To provide a comprehensive overview, the separate tutorial steps are summarized in mind map diagrams. The tutorial comprises a Service Provider initiated flow and an Identity Provider initiated flow, which both will be demonstrated during the testing steps.

As an addition, the tutorial demonstrates the usage of the weblogic feature “virtual user”.

The tutorial was developed and tested on a windows 7 machine. A zip package containing all necessary files is provided at the tutorial website. This also includes a text file with a set of windows commands to help setting up the domains and user configurations. We expect the tutorial to run also on Linux or any other platform supported by weblogic server, although this was not tested.

3 The Web SSO Tutorial

3.1 Tutorial Files

The following files are located at the website [www.andreaswittmann.de](http://www.andreaswittmann.de):

[www.andreaswittmann.de/weblogic-corner/saml2_sso/SAML2_Web_SSO_Tutorial.pdf](http://www.andreaswittmann.de/weblogic-corner/saml2_sso/SAML2_Web_SSO_Tutorial.pdf)
[www.andreaswittmann.de/weblogic-corner/saml2_sso/SAML_SSO.zip](http://www.andreaswittmann.de/weblogic-corner/saml2_sso/SAML_SSO.zip)

The zip archive contains the following files:
3.2 Documentation Links

We summarize some documentations links in the following table.

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0, ein Tutorium – Teil 1:</td>
<td>kain_keller_JS_05_0_Annotated.pdf (Article in)</td>
</tr>
</tbody>
</table>

Figure 1. Contents of the archive SAML_SSO.zip
3.3 Installation of Java

We install the latest Java 7 JDK from the download link
We run the installer.
3.4 Installation of Weblogic Server 12.1.3

Reviewing the certification matrix in Excel from this link:

Figure 3. Certification Matrix showing the certified release for Windows 7, 64 bits.

From the OTN we download the zip distribution and the supplement zip from this download link:
We follow the instruction of the Readme.

First we unzip the distribution to a location which will become the new middleware home for this installation.

The windows file explorer fails to unzip 2 files from the package because filenames are too long.

We use the jar tool to unzip instead and it works fine.

Running the installation:

Running the installation of the supplement package:

Error Message:
There are conflicts with Windows 64 bit versions.

Solutions: We supply username and password on the command line, thus mask.com is not called.

We ignore the ACL Settings, instead we start a command shell as administrator.

To start the example server:

```
D:\10Oracle\06WLS12\wls12130\run_samples.cmd  weblogic welcome1
```

It will be available at [http://192.168.56.1:7001/index.jsp](http://192.168.56.1:7001/index.jsp)

Ok.

### 3.5 Example Overview

In this tutorial we want to demonstrate two message flows which stem directly from the “OASIS SAML Technical Overview” document. The first case is the “SP-Initiated SSO with Redirect and POST Binding”. We copy the relevant image from the document and overlay it with the servers and components which will form this example.
The Service Provider will be realized by the WLS server adminB, the saml2AP Identity Assertion Provider together with the Federation Services provide the Assertion Consumer Service. The resource, which is accessed, is provided by the services.jsp. The Identity Provider will be configured as adminA. Here we use a SAML 2.0 Credential Mapping Provider together with the Federation Services to provide the Single Sign-On Service. The Login module will be provided by the login.jsp.

With a very similar picture, we present the IdP-Initiated SSO case.
Figure 6. OASIS Message Flow picture with overlaid tutorial components for IdP-Initiated Message Flow.

The components are the same as in the previous picture; however the message flow is different. The page that offers the remote resource in step 3 is provided by admin/auth.jsp. The POST form for step 4 and 5 is provided by saml2_post_form.jsp.

We will build up two WLS domains, each consisting only of a single Admin Server. We will configure the Federation Services between these domains as depicted in the following overview.
Figure 7. Domain configuration for this example with Federation Services.

We use adminB and adminA in domainB and domainA respectively. adminB will host appB which represents the service provided by the SAML Service Provider. adminA will host appA, which contains a login page and a service selection page. The security realms are also shown, together with the relevant users, groups and security providers.

The following diagram proposes a configuration sequence and depicts configuration details.
Web Single Sign-On with SAML 2.0

Figure 8. Proposed configuration sequence for the example.
The numbers in the circles propose a configuration sequence which is not mandatory but recommended to complete this task efficiently. The configuration steps are explained in more detail in the Chapter 3.6 and the section numbers map to this sequence.

The activities of the whole tutorial are split into four parts. We depict a summary in the following mind map.

![Mind map summarizing the parts of this tutorial.](image)

### 3.6 Creating Domains and Deploying Applications

In this step we configure two domains and deploy the sample application. The commands to setup the domains are contained in the file `$(EXAMPLE_HOME)/SAML_SSO/SAML_SSO.TXT`. We provide an overview mind map of the configuration steps.
We deploy appA and appB using the admin console. We create the users and groups using the
wlst commands in the file SAML_SSO.TXT.

<table>
<thead>
<tr>
<th>Application Folder</th>
<th>${EXAMPLE_HOME}\SAML_SSO\SAML_SSO.TXT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>domainA</td>
<td><a href="http://localhost:7001/console">http://localhost:7001/console</a></td>
</tr>
<tr>
<td>appA</td>
<td><a href="http://localhost:7001/appA">http://localhost:7001/appA</a></td>
</tr>
<tr>
<td>User/password</td>
<td>ssouser/welcome1</td>
</tr>
<tr>
<td>domainB</td>
<td><a href="http://localhost:7003/console">http://localhost:7003/console</a></td>
</tr>
<tr>
<td>appB</td>
<td><a href="http://localhost:7003/appB">http://localhost:7003/appB</a></td>
</tr>
<tr>
<td>appB</td>
<td><a href="http://localhost:7003/appB/admin/services.jsp">http://localhost:7003/appB/admin/services.jsp</a></td>
</tr>
</tbody>
</table>

### 3.7 Configuring SAML

In following steps we want to configure this SAML example. Since it is easy to get lost
during the manual configuration process, we provide an overview mind map.
Web Single Sign-On with SAML 2.0

Figure 11. Mind Map Overview of the SAML Configuration Process.
The configuration begins in domainA, which will be configured as Identity Provider. We need to configure a Credential Mapping Provider in the security realm. In the server settings of adminA we need to configure the “Federation Services”. In order to conclude the configuration of domainA we need to import the metadata file of the Service Provider which will be produced during the SAML configuration in domainB. Therefore we continue with the configuration of domainB. After that, we change back to domainA and complete the configuration here.
The individual steps from the mind map are explained in detail in the following sub sections.

3.7.1 create SAML 2.0 Credential Mapper Provider

We start with the IdP in domain.
We enable the SSL Port. We use the Demo Certificates
Configure a new credential mapping provider.
(Security Realms->myrealm->Providers->new->SAML 2.0 Credential Mapping Provider)

Figure 12. Creating a new SAML 2.0 Credential Mapping Provider for domain.
We configure the newly created provider.

For signing we use the DemoIdentity/DemoIdentityPassPhrase.
### Provider specific configuration of the SAML Credential Mapper.

We need to restart the Admin Server.

#### 3.7.2 configure SAML 2.0 General Settings

Now we create the SAML Metadata or the server specific SAML 2 profile.
### Figure 14. SAML 2.0 configuration of general per server settings.
configure SAML 2.0 Identity Provider

Now we change to the “SAML 2.0 Identity Provider” tab and configure the IdP. Settings of this tab will also go into the xml file containing the metadata.

We need to choose the preferred binding “Redirect”. Otherwise the Artifact Binding will be chosen from WLS.

The preferred binding will be used by the SP in domainB when sending the authentication request to the IdP (Step 2 of the SP-Initiated Flow). This information is transferred to domainB, when the metadata file is exchanged, i.e. when the metadata_adminA.xml is imported to the “Partner-IdP-adminA”.

Figure 15. SAML 2.0 configuration of general per server settings. (Part 2)
### Figure 16. IdP configuration.

**3.7.4 export adminA_metadata.xml**

We change back to the “SAML 2.0 General” tab and publish the Metadata to the XML file:

D:\10Oracle\06WLS12\domains\domainA\admin_metadata.xml
3.7.5 create SAML 2.0 Identity Assertion Provider

We create a new SAML2 Authentication Provider in the security realm “myrealm”.
Figure 18. Creating a SAML 2.0 Authentication Provider in domainB.

We restart the server.

3.7.6 configure SAML 2.0 General Settings

We configure the server specific SAML2.0 General settings.
For signing we use the DemoIdentity/DemoIdentityPassPhrase.

3.7.7 configure SAML 2.0 Service Provider

We change the „SAML 2.0 Service Provider“ Page of adminB. We choose “POST” as preferred Binding. This will influence how the SingleSignOn Service in domainA, or more specific the “Partner-SP-adminB” in the “SAML 2.0 Credential Mapping Provider”, communicates the SAML Assertion to the Service Provider.

There are two options. If we choose POST, the Assertion will be place into an HTML Form and send via POST to the Assertion Consumer Service (samlAP) of domainB. If we don’t choose anything or choose “Artifact” the IdP will sent a signed artifact via HTTP redirect.

These values will be comunicated to the domainA during import of the “adminB_metadata.xml” file.
3.7.8 export adminB_metadata.xml

We change back to the “SAML 2.0 General” Tab and publish the metadata to the file: D:\10Oracle\06WLS12\domains\domainB\adminB_metadata.xml.
3.7.9 create Partner-Idp-adminA

Now we create a new SSO Identity Provider Partner in the security realm of domainB.
This

3.7.10 \texttt{import adminA\_metadata.xml}

We import the metadata file from domainA, which is the IdP Partner.
3.7.11 configure Partner-IdP-adminB

And we enable the newly created Partner site and add redirect URIs for Service Provider initiated SSO.
Redirect URIs:
/appB/admin/services.jsp
/appB

Figure 23. Creating the IdP Partner for the Service Provider domainB.
This concludes the configuration in domainB.

3.7.12 create Partner-SP-adminB

We change to the Admin Server of domain to the “SAML 2.0 Credential Mapping Provider”. We want to create a Service Provider partner.
3.7.13 Import adminB_metadata.xml

We import the metadata file from domainB.
Figure 26. Importing the metadata from domainB.

3.7.14 configure Partner-SP-adminB

And we enable domainB as SAML partner service provider.
That’s all for the basic configuration of this SAML example.

3.8 Testing the example

We want to test the example via two URLs as indicated in the following mind map.

Figure 27. Enable the Service Provider Partner Configuration from the Metadata import.

Figure 28. Testing SP initiated SSO
3.8.1 Testing via URL to IdP

First we go to appA and get redirected to the login page. We provide the credentials.

We are logged in. Next we choose a service on appB.

We get redirected to appB and are already logged in.
While this looks like an IdP initiated flow, it is actually a SP initiated flow, however starting on the IdP. If we analyze the log files, we will discover that there is no SAML Assertion attached to the HTTP Request for appB. Instead the Assertion Consumer Service from domainB intercepts the call, builds a SAML AuthnRequest, sends it to domainA and receives the SAML Assertion in turn. It verifies the SAML Assertion and forwards to the appB Service page.

3.8.2 Testing via URL to SP

Now we want to go to the appB directly with an unauthenticated request.
In Firefox we delete the history and all cookies first.

Figure 32. Calling the Service on appB directly.
We are challenged with a Login dialog from adminA.

![Login Dialog from adminA](image)

After providing user and password we are redirected to the service page of appB and are already logged in.

![Service page of appB in the SP initiated flow.](image)

Further configuration is needed to specify the login.jsp as login page instead of the standard Authentication Dialog box. We leave this exercise to the interested readers.

### 3.9 Setting Debug Flags for the Example

For debugging we set the these Properties in the files:

- `D:\10Oracle\06WLS12\domains\domainB\bin\setDomainEnv.cmd`
- `D:\10Oracle\06WLS12\domains\domainA\bin\setDomainEnv.cmd`

```bash
```

We also want to see milliseconds in the logfiles.

- Navigate to Domain->Logging->Advanced and set
- Date Format Pattern = yyyy-MM-dd 'HH:mm:ss.S

We do this for both domains and both servers.

### 3.10 Configuring IdP initiated flow with POST Binding

This Blog explains how to configure the IdP initiated flow.

[http://fusionsecurity.blogspot.de/2012/06/before-i-forget-it-howto-saml-20-idp.html](http://fusionsecurity.blogspot.de/2012/06/before-i-forget-it-howto-saml-20-idp.html)

Here are the steps to configure this within this example:
3.10.1 Configure an additional end user URL.

In appA/admin/auth.jsp we add an additional URL that points to IdP and uses the target Service URL in the parameter.
It is of the form:
http://<idp-server>:<port>/saml2/idp/sso/initiator?SPName=<SP-Partner-Name>&RequestURL=<target-application-url>

In our case we use:

3.10.2 Configure the POST Binding POST Form

Within appA we need a jsp that contains a POST form, which posts the SAML Assertion to the Service Provider.
We include sam2_post_form.jsp in appA and redeploy App.
The post form is contained in the file /appA/saml2_post_form.jsp:

```html
<!DOCTYPE HTML PUBLIC "//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head></head>
<body onLoad="document.forms[0].submit();">
<FORM METHOD="POST" ACTION="http://localhost:7003/saml2/sp/acs/post">
<INPUT TYPE="HIDDEN" NAME="RelayState" VALUE="<%=relayState%>"/>
<INPUT TYPE="HIDDEN" NAME="SAMLResponse" VALUE="<%=samlResponse%>">
</FORM>
</body>
</html>
```

In the IdP-Partner configuration we specify the post form. We use the /appA/saml2_post_form.jsp
For testing, we login at appA with ssouser01 and choose the link for the POST Binding.
Choose the IdP initiated flow from appA.

We are directly transferred to the service page of domainB. This time the request is processed by the “Assertion Consumer Service” of domainB. It contains the SAML Assertion, as the following excerpt from the adminB.log demonstrates.
The user is contained in the NameID element and the group is contained in the AttributeStatement element.

This concludes the IdP initiated POST Binding example.

### 3.11 Configuring Virtual User:


We can use virtual users at the SP side, if we need users that are authenticated at the IdP but do not exist in the security realm of domainB. These foreign users are created as virtual users by an extra SAML Authenticator, i.e. this Authenticator populates the subject with principals from the SAML assertion (user and groups).

We need to configure an extra SAML Authenticator in domainA.

![Figure 37. Configuring a SAMLAuthenticator to use virtual users.](image.png)

We can test this with the user ssouser02 which is present in domainA but not in domainB.
3.12 Setting the Binding Sequence

The SAML Bindings which is chosen by the Federation Services is determined by the sequence as the Bindings appear in the Metadata file. We configure this in step 3. configure SAML 2.0 Identity Provider explained in Chapter 3.6.3 and in step 7. configure SAML 2.0 Service Provider as explained in Chapter 3.6.7. just before exporting the metadata files. In the Admin Server Console we can prefer a binding and set a default. This is visible in the resulting metadata files as shown below.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="saml2CMP"
   WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" />
</md:EntityDescriptor>
```

Here the artifact binding will be chose as the preferred binding for the SingleSignOnServices. In adminB metadata.xml the format is more explicit, containing an index number and a default flag.
Here the HTTP-POST Binding will be chosen for the AssertionConsumerService. If we want to change this behavior for a Partner-SP or Partner-IdP, we can modify the xml files directly and re-import the modified metadata files. Alternatively we could change the settings in the configurations of the Identity Provider and Service Provider (step 3 and step 7). But then we have to export and import the files again, just changing the settings will have no effect.

3.13 SAML 2.0 Examples in Blog Posts.

The following is a list of some blogs that demonstrate different aspects of SAML configuration in WLS.

SAML 2.0 Example from Biemond, based on earlier blog post, using ssl demo certs and saml metadata file.

Steps to configure SAML 2 on Weblogic Server 10.3.0, using pointbase for the rdbms security realm.
https://blogbypuneeth.wordpress.com/2011/01/15/steps-to-configure-saml-2-on-weblogic-server-10-3-0/

Configure WSO2 Identity Server SAML2 IDP with Oracle Weblogic as Service Provider Example of integration between WSO2 and WLS
http://tanyamadurapperuma.blogspot.de/2013/09/configure-wso2-identity-server-saml2.html

3.14 Conclusion

This tutorial comprises a comprehensive description of a web single-sign-on scenario using SAML 2.0 in weblogic server. It demonstrates all steps necessary to install, configure and run a demo application. The whole tutorial is split into four parts. In the first part we walked through the installation of weblogic server on a windows machine and the creation of two domains. We also installed the sample applications in this part. In part two we looked at the SAML configuration in weblogic server, using the Administration Console. We introduced a recommended configuration sequence which comprises 14 steps and was illustrated by
diagrams and mind maps. While this sequence is not mandatory, it structures the manual configuration process in an efficient manner and can serve as a template for configuring real world SAML scenarios.

In the third part we demonstrated two test cases for the service provider initiated flow scenario. In the fourth part we extended the example to include an identity provider initiated flow scenario and demonstrated an advanced weblogic feature called virtual user. The tutorial concludes with some configuration and debugging tips and a brief overview of other blog post covering similar subjects.