Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Table of Contents

Disclaimer 1
Introduction 1
Prerequisites 2
  Install and configure the software 2
  Configure SSL for WebCenter Portal Domain 2
  Update webCenter.ear and Redeploy 2
  Configure the Identity Store in the WebCenter Portal Domain 4
Configure the Identity Provider 4
  Configure the Server Authentication Certificate in IIS 4
  Download ADFS SAML 2.0 Metadata 5
  Configure WebCenter Portal as Service Provider with ADFS 5
Configure WLS as the Service Provider 7
  Configure the SAML2.0 Identity Assertion Provider 7
  Configure SAML 2.0 Service Provider Services 9
  Configure SAML2.0 General Services 11
  Create and Configure Identity Provider Partners 13
Test SAML2.0 Based Federated SSO 16
Introduction

WebCenter Portal has been supporting SAML1.1-based SSO since Release 11.1.1.6.0. The purpose of this document is to describe the configuration steps for WebCenter Portal 11.1.1.8.0 or later to support SSO using SAML2.0.

For SAML authentication, there are two parties involved:

» **Identity Provider (IDP)**, which is responsible for authentication and generating SAML assertion.
» **Service Provider (SP)**, which is responsible for asserting the SAML assertion.

In SAML1.0 WebCenter Portal, was supported to use WebLogic Server (WLS) as both IDP and SP. For more information on SAML 1.0 support, see Configuring SAML-based Single Sign-On. Current SAML2.0 support in WebCenter Portal is not only to support the same topology of WLS as IDP and SP, but also to support other standard compliant SAML2.0 IDPs like ADFS, Ping Federate, OAM, and so on. This document is written with ADFS as SAML2.0 IDP and WLS as SP. ADFS steps can be replaced with the other SAML2.0 compliant IDP like OAM, WLS or Ping Federate to achieve similar outcome. For SSO validation in this paper, WebCenter Portal is used as Partner applications. WebCenter Portal is used as an example and can be substituted with any other Partner application with which SSO needs to be established. Figure1 describes the various roles in SAML based SSO:

![Figure 1 Roles in SAML based SSO](image)

In a typical use case for SAML based SSO, the user requests a resource from SP. In our case, SP will be a WLS server hosting WebCenter Portal. The user requests a protected page from WebCenter Portal, so WLS SP redirects the user to IDP, as IDP is ultimately responsible for authentication. Once IDP authenticates the user, it generates SAML2.0 assertion and redirects the user back to SP. SP has trust relationship with IDP through prior certificate exchange. Therefore, SP asserts the SAML2.0 assertion from IDP and creates the authenticated session for the user to allow access to the resource.
The following high-level steps configure SAML2.0-based SSO:

1. Prerequisites
2. Configure the Identity Provider
3. Configure WLS as the Service Provider

Prerequisites

Install and configure the software

The following are the software you need to install:

» ADFS 2.0 IDP running on Windows Server 2008 R2.
   If you are using different IDP, you can ignore this step. For more information, see Install and Configure Active Directory Federation Services (ADFS) 2.0.
» WebCenter Portal (WCP). For more information, see Installing the Oracle WebCenter Portal Software.

Configure SSL for WebCenter Portal Domain

In order to integrate with ADFS using the SAML 2.0 protocol, WebCenter Portal must be configured to use HTTPS/SSL as its endpoints. Failure to do so will result in ADFS not accepting the WCP SAML 2.0 Metadata when establishing Federation Trust. For more information for enabling SSL in WebCenter Portal, see SSL: An Introduction.

Update webCenter.ear and Redeploy

Installed webcenter.ear comes with cookie-path set with /webcenter. Due to limitation of WLS SAML2.0 mentioned in Configure SSL for WebCenter Portal Domain, cookie-path must be set at "/". This is required because WLS SP supports only "/" as cookie-path for SAML2.0.

To accomplish this,

1. Navigate to WebCenter Oracle home directory.
2. Unzip the webcenter.ear file ($WebCenter_Install_Dir/archives/applications)
3. Unzip the Spaces EAR file.
4. Open the weblogic.xml (/WEB-INF/weblogic.xml) in an XML editor and modify the cookie-path element under session-descriptor to the following value:
   `<cookie-path/></cookie-path>
5. To make use of assertions provided by IDP within WebCenter Portal, we need to change the authentication type of the WebCenter Portal to CLIENT-CERT. To do this, open the web.xml (/WEB-INF/web.xml) in an XML editor and modify login-config as follows:
   `<login-config>
      <auth-method>CLIENT-CERT</auth-method>
   </login-config>
6. After updating weblogic.xml and web.xml, zip the webcenter.ear again using the jar utility and redeploy it from the weblogic console.
7. After logging into the weblogic console, navigate to deployments and find WebCenter application deployment as shown in Figure 2.
Figure 2 WebCenter Application Deployment

8. Select WebCenter and click **Update**. The page is as shown in **Figure 3**.

Figure 3 Choose WebCenter Application Path

9. Select the Source path to update `webcenter.ear` and click **Finish** to redeploy `webcenter.ear`.
Configure the Identity Store in the WebCenter Portal Domain

An authenticator in WebCenter Portal must be configured to point to the same directory as the IDP; that is, ADFS users. Both IDP and SP should be configured to use a common LDAP. Otherwise, if IDP and SP are configured to use different LDAPs, then user attributes must be synchronized between IDP LDAP and SP LDAP. Also, different LDAPs mean that the same set of users must exist in both the systems, with each user having the same e-mail address, so that the e-mail address can be used as the common user attribute. For more information, see Configuring the Identity Store.

Configure the Identity Provider

For this white paper, we have used Active Directory Federation System (ADFS) as the Identity Provider (IP). ADFS is a software component developed by Microsoft to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and implements federated identity.

Skip this section, if the customer is using Ping Federate, OAM, Shiboleth or any other IDP. Use the product document of the IDP for installation and configuration and then move to SP Configuration section. In each IDP documents, there would be a section to configure SP where metadata file of SP is imported in IDP.

To Configure ADFS:

» Configure the server authentication certificate in IIS
» Configure ADFS as a standalone federation server
» Download ADFS SAML 2.0 Metadata
» Configure WebCenter Portal as Service Provider with ADFS

Configure the Server Authentication Certificate in IIS

To create a self-signed Secure Sockets Layer (SSL) certificate and bind it to the default web site using the IIS Manager console:

1. Open the Internet Information Services (IIS) Manager console.
2. From the Start menu, select All Programs, then Administrative Tools, then Internet Information Services (IIS) Manager.
3. In the console tree, click the root node that contains the name of the computer, and then in the details pane, double-click the Server Certificates icon from the IIS grouping.
4. In the Actions pane, click Create Self-Signed Certificate.
5. On the Specify Friendly Name page, type a descriptive name for the certificate, and click OK.
6. In the console tree, click Default Web Site.
7. In the Actions pane, click Bindings.
8. In the Site Bindings dialog box, click Add.
9. In the Add Site Binding dialog box, select http in the Type drop-down list, select the certificate of your machine in the SSL certificate drop-down list, click OK, and then Close.
10. Close the Internet Information Services (IIS) Manager console.
Configure ADFS as a Standalone Federation Server

1. Open the AD FS 2.0 Management console and select ADFS 2.0.
2. In the details pane, click the ADFS 2.0 Federation Server Configuration Wizard link to start the wizard.
3. On the Welcome page, click Create a new Federation Service, then click Next.
4. On the Select Stand-Alone or Farm Deployment page, click Stand-alone federation server, then click Next.
5. On the Specify the Federation Service Name page, verify that the certificate name created in Configure Server Authentication Certificate in IIS is selected, and then click Next.
6. On the Ready to Apply Settings page, review the settings, and then click Next.
7. On the configuration Results page, click Close. The ADFS Node appears on the left pane of the page, as shown in Figure 4.

Download ADFS SAML 2.0 Metadata

To download SAML 2.0 Metadata for ADFS:

1. Locate the xml file at the following URL: https://adfsHost:adfsPort/FederationMetadata/2007-06/FederationMetadata.xml. (Example: https://localhost/FederationMetadata/2007-06/FederationMetadata.xml)
2. Save this file locally as idp_metadata.xml to configure ADFS with WLS in the procedure WebCenter Portal as Service Provider Configuration.

If you are using any other product as IDP then review its product documentation to download the SAML2.0 metadata file of that IDP. This metadata file must be imported into WebCenter Portal's WLS, hence this step is mandatory.

Configure WebCenter Portal as Service Provider with ADFS

For now skip this section and complete Configure WLS as the Service Provider. Once metadata file for the SP is created in section Configure SAML2.0 General Services, come back here and complete this section.
Perform the following steps to add WebCenter Portal as the service provider in ADFS IDP:

1. Open the ADFS 2.0 Management console.
2. Right-click **Relying Party Trusts** and select **Add Relying Party Trust**.
3. In the Add Relying Party Trust wizard, click **Start**.
4. Select **Import data about the relying party from a file**, and point to the WLS SAML 2.0 metadata file (sp_metadata.xml).
   The step to generate this file is described in Configure SAML2.0 General Services.
5. Click Next and enter the **Display Name** for the new WCP SAML 2.0 Service Provider as **WCP SP**.
6. Click Next and select **Permit all users to access this relying party**.
7. Click Next, then Next again, then click Close.
   Leave the Open the Edit claims box checked.
8. Click Add rule when the Edit rule window opens.
   Configure ADFS to retrieve the user’s Login Name and Given Name from LDAP and include it as Name ID and Given Name SAML attribute.
9. Select **Send LDAP Attributes as Claims** in the Add Transform Claim Rule wizard.
10. Click Next and enter a name for claim rule as Name, select Active Directory from the Attribute store drop-down list, then select SAM-Account-Name for LDAP Attribute and Name ID as Outgoing Claim Type (Figure 5).

![Figure 5 Add Transform Rule Wizard - Configure LDAP Rule](image)

11. Click Finish.
12. Click Add rule and select the option **Send LDAP Attributes as Claims**.
13. Click Next and enter a name for the claim rule as Given Name.
14. Select Given Name for Incoming claim type, select Given Name for Outgoing claim type (Figure 6).
15. Click **Finish**.
16. Right-click the newly created Relying party, WCP SP, and select **Properties**.
17. Click the **Advanced** tab and select **SHA-1**, if WLS is not configured to work with SHA-256 and click **OK**.

**Configure WLS as the Service Provider**

In this section, each of the partner applications that participate in SSO needs to be configured as SP. In this white paper, we have described steps to configure WebCenter Portal as SP. Similar steps must be repeated for Discussion, WebCenter Content Server, and any other partner application.

Before you start, you will need the SAML 2.0 Identity Provider metadata file from the SAML Federation IDP. The metadata file should be in a standard format, compliant with the SAML 2.0 specification. Refer to the vendor documentation for information on how to obtain the SAML 2.0 IDP metadata from the Identity Provider. For ADFS, refer to Download ADFS SAML2.0 Metadata.

Instructions in this section are executed on the WebCenter Portal domain.

To configure the service provider (SP):

» **Configure the SAML 2.0 Identity Assertion Provider**
» **Configure SAML 2.0 Service Provider Services**
» **Configure SAML 2.0 General Services**
» **Create and Configure Identity Provider Partners**

**Configure the SAML2.0 Identity Assertion Provider**

1. Log in to Weblogic Admin console for the WebCenter Portal domain.
2. Select **Security Realms**, then **myrealm**, then **Providers**, then **Authentication**.
3. In the Authentication Providers page (Figure 7), click **New**, then select **SAML2IdentityAsserter**.
4. Enter the name for the SAML2IAsserter (or similar) and click **OK**.
   Note: There is no provider specific configuration required for this Asserter.
Figure 7: Create a New Authentication Provider

5. Click Activate Changes.

Figure 8: List of Authentication Providers
6. Restart the server.

For more information on Configuring Identity Assertion Providers, see Configuring Identity Assertion Providers.

If you are running in cluster, then select **Replicated Cache Enabled** property for the SAML2IAssertioner as shown in **Figure 9**.

![Figure 9 Configure SAML 2.0 Identity Assertion Provider for Cluster](image)

**Figure 9 Configure SAML 2.0 Identity Assertion Provider for Cluster**

**Configure SAML 2.0 Service Provider Services**

Select **Servers**, then **WC_Portal**, then Federation **Services**, then SAML 2.0 **Service Provider** and make the following changes (see **Figure10**):

- Select the **Enabled** check box.
- Select the **Always Sign Authentication Requests** check box.
- Select **Preferred Binding as POST** from the drop-down menu.
- Enter the **Default URL** as `https://WCP_HOST:WCP_SSL_PORT/webcenter`. 
Figure 10 Configure SAML 2.0 Service Provider Services
Configure SAML2.0 General Services

Configure the following in General SAML 2.0 services:

Select **Servers**, then **WC_Portal**, then **Federation Services**, then **SAML 2.0 General** and provide following property values *(Figure 11)*:

- Replicated Cache Enabled : Select or clear
  - Note: Enabling the replicated cache is required if you are configuring SAML 2.0 services on two or more WebLogic Server instances in a domain, such as in a cluster.
- Contact Person Given Name
- Contact Person Surname
- Contact Person Type
- Contact Person Company
- Contact Person Telephone Number
- Contact Person Email Address
- Organization Name
- Organization URL
- Published Site URL : https://<DestinationSiteDNSName>:<SSL_PORT>/saml2
- Entity ID : (Destination Domain name)
- Single Sign-on Signing Key Alias
- Single Sign-on Signing Key Pass Phrase
- Confirm Single Sign-on Signing Key Pass Phrase
This white paper was validated using demoidentity key store with demo certificates of WLS. A customer setup would have custom key store and proper signing certificate. Provide signing key information in this section (see Figure12).

Note: Demoidentity is used in the example and the password is DemoidentityPassPhrase.

---

**Figure 11 Configure General SAML2.0 General Services**

This page configures the general SAML 2.0 per server properties.

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicated Cache Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Person Given Name:</td>
</tr>
<tr>
<td>Contact Person Surname:</td>
</tr>
<tr>
<td>Contact Person Type:</td>
</tr>
<tr>
<td>Contact Person Company:</td>
</tr>
<tr>
<td>Contact Person Telephone Number:</td>
</tr>
<tr>
<td>Contact Person Email Address:</td>
</tr>
<tr>
<td>Organization Name:</td>
</tr>
<tr>
<td>Organization URL:</td>
</tr>
<tr>
<td>Published Site URL:</td>
</tr>
<tr>
<td>Entity ID:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bindings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient Check Enabled</td>
</tr>
</tbody>
</table>
Click **Save** to save the setting and click **Publish Metadata**. This downloads the SP metadata (`sp_metadata.xml`), which needs to be imported on IDP. This file should be used in section **Configure WebCenter Portal as Service Provider with ADFS**.

For more information, see [Configuring SAML 2.0 General Services](#).

### Create and Configure Identity Provider Partners

A SAML 2.0 IDP partner is an entity that generates SAML 2.0 assertions consumed by the Service Provider site. The configuration of IDP partners is available from the Administration Console, using the **Security Realms** > **RealmName** > **Providers** > **Authentication** > **SAML2IAsserterName** > **Management** page.

1. Select **Security Realms**, then myrealm, then Providers, then Authentication, then SAML2IAsserter, then Management, then New, then New **Web Single Sign-On Identity Provider Partner**.
2. In the Create SAML 2.0 Web Single Sign-on Identity Provider Partner page, enter Name as `SAML_SSO_IDP01` (see Figure 13).
3. Select ADFS generated `idp_metadata.xml`
4. Click **OK**.
If ADFS metadata import fails then the solution is to take out the WS-Trust metadata content, and the signature, and then most import processes will succeed. To remove the WS-Trust metadata content and the metadata signature:
5. Open `idp_metadata.xml` with an XML editor.
6. Delete the sections of the file shown in the following table.

<table>
<thead>
<tr>
<th>Description</th>
<th>Section starts with...</th>
<th>Section ends with...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata document signature</td>
<td><code>&lt;ds:Signature</code></td>
<td><code>&lt;/ds:Signature&gt;</code></td>
</tr>
<tr>
<td>WS-Trust &amp; WS-Federation application service metadata</td>
<td><code>&lt;RoleDescriptor xsi:type=&quot;fed:ApplicationServiceType&quot;</code></td>
<td><code>&lt;/RoleDescriptor&gt;</code></td>
</tr>
<tr>
<td>WS-Trust &amp; WS-Federation security token service metadata</td>
<td><code>&lt;RoleDescriptor xsi:type=&quot;fed:SecurityTokenServiceType&quot;</code></td>
<td><code>&lt;/RoleDescriptor&gt;</code></td>
</tr>
</tbody>
</table>

7. Auto-generated AD FS 2.0 metadata file includes information about performing both the IDP and SP roles. WLS doesn’t supports having both SAML 2.0 IDP and SP descriptors in the metadata file when trying to add an IDP on that basis. Delete the following section of the file:

<table>
<thead>
<tr>
<th>Description</th>
<th>Section starts with...</th>
<th>Section ends with...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0 SP metadata</td>
<td><code>&lt;SPSSODescriptor WantAssertionsSigned=&quot;true&quot;</code></td>
<td><code>&lt;/SPSSODescriptor&gt;</code></td>
</tr>
</tbody>
</table>

The first two elements of the resulting file should look like:

```
<EntityDescriptor ID="...">
  <IDPSSODescriptor WantAssertionsSigned="true"/>
```

8. Save the edited file and redo the import step.

After import is completed, click SAML_SSO_IDP01 and enter the following:

- **Name**: SAML_SSO_IDP01
- **Enabled**: Select the check box
- **Description**: SAML_SSO_IDP01
- **Redirect URIs**: `/webcenter/*`

This concludes the WCP SP Configuration. Similar configuration should be done for each of the partner applications that participate in SSO.

Now, go back and complete the section for **Configure WebCenter Portal as Service Provider with ADFS**.
Test SAML2.0 Based Federated SSO

At this point, WebCenter Domain is configured with SAML2.0 Service Provider and ADFS is configured as IDP.

To verify the federated SSO, do following:

» Wire the WebCenter Portal instance to same OID as ADFS or make sure that ADFS users exist in the OID wired to WebCenter Portal Server. For more information, see Configure the Identity Store in the WebCenter Portal Domain.

» Access the WebCenter Portal SSL URL (for example, https://WCP_HOST:WCP_PORT/webcenter). You will be redirected to ADFS which will throw a basic auth challenge. Provide your Windows credentials (credentials of ADFS credential store). If login is successful, the WebCenter Portal Home page appears.

If additional partner application is configured, then access the secured page of the partner application. It should directly take you to the secured page without prompting for login.
WebCenter Portal SAML2.0 Federated SSO
April 2016
Author: Nitin Shah
Contributing Author: Suresh Alagarswamy