

# Configuring EPM System 11.1.2.1 for SAML2-based Federation Services SSO

Scope.....	2
Prerequisites Tasks.....	2
Procedure .....	2
Step 1: Configure EPM's WebLogic domain for SP Federation Services .....	2
Step 2: Configuring a WebLogic domain to act as an Identity Provider. ....	5
Step 3: Deploy Diagnostics Web App to test SAML SSO .....	7
Step 4: Configure EPM Foundation Services for SAML SSO-based authentication...	14
Step 5: Configure and deploy the rest of EPM to this domain .....	15

## Scope

The documentation provided here assumes a sound understanding and knowledge of SAML-based Federation Services and WebLogic security administration; this document describes configuration steps required for a Service Provider (SP) initiated SSO for EPM System. The configuration steps do not include signed Assertions and make use of WebLogic's default certificates only. Before starting these procedures, confirm that the prerequisites for these tasks are completed. For more information on SAML and associated technologies, refer to <http://www.oasis-open.org/home/index.php>.

For details on the architecture and implementation of SAML in WebLogic, refer to [http://download.oracle.com/docs/cd/E12840\\_01/wls/docs103/secintro/archtect.html#wp1070945](http://download.oracle.com/docs/cd/E12840_01/wls/docs103/secintro/archtect.html#wp1070945).

## Prerequisites Tasks

1. Corporate Active Directory is configured for user authentication (<http://www.microsoft.com/windowsserver2003/technologies/security/kerberos/default.msp>).
2. A SAML based Identity Provider[IdP] like Active Directory Federation Services()
  - a. In the current configuration, a separate WebLogic Server domain is configured as an IdP as an example.
3. EPM System Foundation Services installed and configured (<http://support.microsoft.com/kb/295017>).
4. The host boxes running the IdP and SP configuration in Time Sync with a skew of not more than 5 minutes.

## Procedure

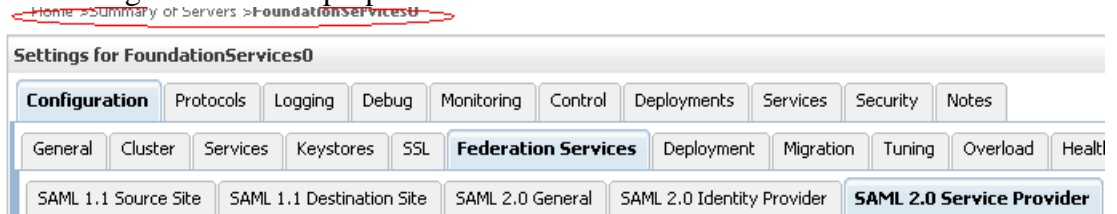
### ***Step 1: Configure EPM's WebLogic domain for SP Federation Services***

**Note:** Install all the products you wish to use but only deploy and configure EPM Foundation Services. This will create a WebLogic domain. The default domain name is [EPMSystem](#). The Hostname running EPM Foundation Services is represented as [HSSServer](#) and the default port as [HSSPort\[28080\]](#). The hostname running the front-ending OHS server for EPM is represented as [HypOHSServer](#) and the default port as [HypOHSPort\[19000\]](#). The WebLogic Admin Server running the IdP Services is represented as [IdPServer](#).

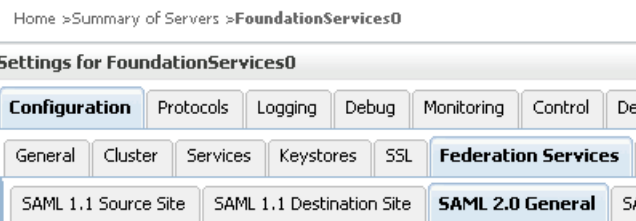
- Configure the EPMSystem domain to receive SAML assertions

- a. Create an LDAPAuthentication Provider for Active Directory - [http://download.oracle.com/docs/cd/E12839\\_01/web.1111/e13707/atn.htm#i1216261](http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/atn.htm#i1216261)
  - i. Create a user called ssouser in AD
- b. Create a SAML2 identity asserter - [http://download.oracle.com/docs/cd/E12839\\_01/web.1111/e13707/atn.htm#i1208059](http://download.oracle.com/docs/cd/E12839_01/web.1111/e13707/atn.htm#i1208059)
  - c. Note: Set the JAAS option to OPTIONAL for all of the Authenticators. Refer to [http://download.oracle.com/docs/cd/E12839\\_01/apirefs.1111/e13952/taskhelp/security/SetTheJAASControlFlag.html](http://download.oracle.com/docs/cd/E12839_01/apirefs.1111/e13952/taskhelp/security/SetTheJAASControlFlag.html) for more details
- Configure EPM Foundation Services as an SP

- a. On the WebLogic Server console, navigate to the Properties page of FoundationServices0 Server and click on SAML2 Service Provider tab and configure the below properties on the tab



- i. “Enabled” checkbox – Checked.
  - ii. “Default URL:” - Enter:  
http://<HSSServer>:<HSSPort>/interop/index.jsp
  - iii. Save the configuration and Activate Changes.
- b. On the WebLogic Server Console, navigate to the Properties page of the FoundationServices0 server and click on SAML 2.0 General.



- tab.
- c. Configure the following Properties on the tab.
  - i. “Contact Person Given Name:” – enter epm\_admin
  - ii. “Contact Person Type:” dropdown – Select “Administrative”
  - iii. “Published Site URL” – Enter:  
http://<HypOHSServer>:<HypOHSPort>/
  - iv. “Entity ID” – Enter”  
http://<HypOHSServer>:<HypOHSPort>/
  - v. Save the configuration and Activate Changes on the Change Center
- d. On the same “SAML 2.0 General Tab”, click on “Publish Metadata” button.

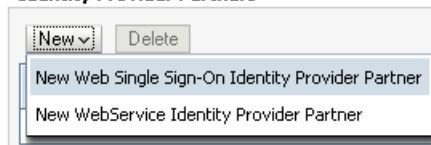
- i. Select a path on the HSSServer
    - ii. Enter a name for the SAML2 metadata file as -  
<HSSServer>-wls-sp-saml2-metadata.xml
    - iii. Click OK and verify that a non-zero size file is created
  - e. FTP the <HSSServer>-wls-sp-saml2-metadata.xml to the host running the <IdPServer>
- Navigate to SecurityRealms->myrealm->Providers and click on the SAML2 asserter created in Step 1.
  - a. Add a new Identity Provider Partner



On this page, you can add, delete, and view SAML 2.0

[Customize this table](#)

**Identity Provider Partners**



- b. Select the IdP metadata file. This is a file created on the <IdPServer> in a similar fashion as the <HSSServer>-wls-sp-saml2-metadata.xml and will be described in the IdP Configuration Section. Refer Step 2, bullet 2e.
  - c. Once the file is configured successfully, on the General tab of the new Identity Provider Partner as shown below,

## configure

Home > Summary of Servers > FoundationServices0 > Summary of Security Realms > myrealm > Providers > saml2-asserter > blr2230232-wls-idp

### settings for saml2-asserter

**General** | Site Info | Single Sign-On Signing Certificate | Transport Layer Client Certificate | Single Sign-On Service Endpoints | Art

Save

Configures a SAML 2.0 Web Single Sign-on Identity Provider Partner's General Properties

The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that a Topics.

#### Overview

**Name:** blr2230232-wls-idp

Enabled

**Description:**

#### Authentication Requests

**Identity Provider Name Mapper Class Name:**

**Issuer URI:** http://blr2230232.idc.oracle.com:7001

Virtual User

**Redirect URIs:**

/interop/\*

- i. “Enabled” checkbox – Enable
- ii. Rediret URLs – Enter “/interop/\*”
- iii. Save the changes.

## Step 2: Configuring a WebLogic domain to act as an Identity Provider.

**Note:** In case ADFS is the IdP, follow steps documented at

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=062f7382-a82f-4428-9bbd-a103b9f27654> instead of this Step. All other steps will remain the same.

- Create a user called souser in the WebLogic domain.
- Configure a SAML2 Identity Provider:
  - a. Navigate to the Credential Mappings tab

Home > Summary of Security Realms > myrealm > Providers

### settings for myrealm

Configuration | Users and Groups | Roles and Policies | Credential Mappings | **Providers** | Migration

Authentication | Password Validation | Authorization | Adjudication | Role Mapping | Auditing | **Credential Mapping**

- b. Create a new SAML2 Credential Mapper and restart the <IdPServer> instance:

**Create a New Credential Mapping Provider**

OK Cancel

---

**Create a new Credential Mapping Provider**

The following properties will be used to identify your new Credential Mapping Provider.  
\* Indicates required fields

---

The name of the Credential Mapping Provider.

\* Name:

---

This is the type of credential mapping provider you wish to create.

Type:  ▼

---

OK Cancel

- c. Navigate to the Servers->Admin Server -> Federation Services -> SAML Identity Provider and configure the following properties:

- i. "Enabled" Checkbox – checked.
- ii. "Preferred Binding" drop down – Select "POST"
- iii. Save changes

- d. Navigate to the "SAML2 General" tab and configure the following properties:

- i. Contact Person Given Name – Enter WebLogic administrator's user id.
- ii. Contact Person Type drop down box – Select "administrative".
- iii. Published Site URL : Enter  
http://<IdpServer>hostname:<weblogic admin Server port>/saml2. [ Note including saml2 is important]
- iv. Entity ID: - Enter  
http://<IdpServer>hostname:<weblogic admin Server port>.
- v. Save Changes.

- e. On the same tab, click on "Publish Meta Data" button.

- i. Choose a directory path and key in a file name as <IdPServer>-wls-idp-metadatav2.xml
- ii. FTP the xml metadata file onto the server running EPM Foundation Services for import.

- f. Navigate to the management Tab on the Credential Mapper:

Home >Summary of Servers >AdminServer >Summary of Security Realms >myrealm >Providers >hss-idp

---

**settings for hss-idp**

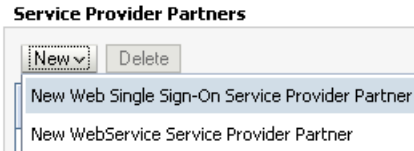
Configuration **Management** Migration

- g. Select New and create a new Service provider partner:



On this page, you can add, delete, and view SAML 2

▶ **Customize this table**



- h. Choose the Metadata XML <HSSServer>-wls-sp-saml2-metadata.xml file exported while configuring SP and click OK:



#### Partner Properties

Use this page to:

- Enter the name of your new Web Single Sign-on Service Provider partner
- Specify the name and location of the SAML 2.0 metadata file that you received from your new S

\* Indicates required fields

Please specify the name of the partner.

\* **Name:**

Please specify the name of the file containing the partner metadata document.

**Path:**

### ***Step 3: Deploy Diagnostics Web App to test SAML SSO***

EPM System has provided a Test Web Application that can be used to test that WebLogic is properly configured for SAML authentication.

1. This WAR is located under  
EPM\_ORACLE\_HOME/products/Foundation/AppServer/InstallableApps/common folder.
2. Launch the EPM domain WebLogic admin console to deploy the reference implementation SSODiag.war web application to the Foundation Services managed server.

## Login to WebLogic admin console and choose to install:

ORACLE WebLogic Server Administration Console

Home Log Out Preferences Record Help

Welcome, epm\_admin Connected to

Change Center

**View changes and restarts**

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

EPMSysSystem

- Environment
- Deployments**
- Services
- Security Realms
- Interoperability
- Diagnostics

Home > Summary of Deployments

Summary of Deployments

Control Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from this domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Customize this table

Deployments

Install Update Delete Start Stop

Showing 1 to 8 of 8 Previous

Name	State	Health	Type	Deployment Order
------	-------	--------	------	------------------

## Pick the SSODiag.war:

ORACLE WebLogic Server Administration Console

Home Log Out Preferences Record Help

Welcome, epm\_admin Connected to: E

Change Center

**View changes and restarts**

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

EPMSysSystem

- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

Home > Summary of Deployments

Messages

You must select an application before continuing.

Install Application Assistant

Back Next Finish Cancel

Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application directory or of the Path field.

Note: Only valid file paths are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application contains the required deployment descriptors.

Path: /home/arkkumar/SSODiag/SSODiag.war

Recently Used Paths: (none)

Current Location: dadvmh0362.us.oracle.com / home / arkkumar / SSODiag

- SSODiag.war**

Back Next Finish Cancel

## Choose install type as Application:

Install Application Assistant

Back Next Finish Cancel

Choose targeting style

Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.

Install this deployment as an application

The application and its components will be targeted to the same locations. This is the most common usage.

Install this deployment as a library

Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.

Back Next Finish Cancel

Deploy SSODiag.war application to the FoundationServices managed server:

Servers
<input type="checkbox"/> AdminServer

Clusters
<input type="checkbox"/> AnalyticProviderServices <ul style="list-style-type: none"><li><input type="radio"/> All servers in the cluster</li><li><input type="radio"/> Part of the cluster<ul style="list-style-type: none"><li><input type="checkbox"/> AnalyticProviderServices0</li></ul></li></ul>
<input type="checkbox"/> EssbaseAdminServices <ul style="list-style-type: none"><li><input type="radio"/> All servers in the cluster</li><li><input type="radio"/> Part of the cluster<ul style="list-style-type: none"><li><input type="checkbox"/> EssbaseAdminServices0</li></ul></li></ul>
<input checked="" type="checkbox"/> FoundationServices <ul style="list-style-type: none"><li><input checked="" type="radio"/> All servers in the cluster</li><li><input type="radio"/> Part of the cluster<ul style="list-style-type: none"><li><input type="checkbox"/> FoundationServices0</li></ul></li></ul>
<input type="checkbox"/> Planning

Choose Custom Roles and Policies as the security model:

— Security —

What security model do you want to use with this application?

- DD Only: Use only roles and policies that are defined in the deployment descriptors.
- Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.
- Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.
- Advanced: Use a custom model that you have configured on the realm's configuration page.

— Source accessibility —

## Complete the deployment:

### Install Application Assistant

Back Next **Finish** Cancel

#### Review your choices and click Finish

Click Finish to complete the deployment. This may take a few moments to complete.

#### Additional configuration

In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?

Yes, take me to the deployment's configuration screen.

No, I will review the configuration later.

#### Summary

**Deployment:** /home/arkkumar/SSODiag/SSODiag.war

**Name:** SSODiag

**Staging mode:** Use the defaults defined by the chosen targets

**Security Model:** CustomRolesAndPolicies: Ignore all roles and policies in deployment descriptors. Create custom roles and policies later.

#### Target Summary

Components	Targets
SSODiag	FoundationServices

Back Next **Finish** Cancel

3. Configure OHS and add a forwarding request for SSODiag URL.
4. Add the following lines into the mod\_wl\_ohs.conf file located under the OHS config directory to forward request to WLS from OHS. Restart the server after making the changes.

```
<LocationMatch ^/SSODiag/>
    SetHandler weblogic-handler
    WebLogicCluster HSS Server name:HSS port
</LocationMatch>
<LocationMatch ^/saml2/>
    SetHandler weblogic-handler
    WebLogicCluster HSS Server name:HSS port
</LocationMatch>
```
5. Protect the URL by creating a policy in the WebLogic administration console for the URL `http://OHS_server_name:port/SSODiag/ssodiag`

Home Log Out Preferences Record Help

Home > Summary of Deployments > SSODiag > Roles > Policies

### Create a New Stand-Alone Web Application URL Pattern Scoped Policy

OK Cancel

**Create a New Policy URL Pattern**

The following property will be used to identify your new Policy URL pattern.

What would you like to name your new Policy URL pattern?

**URL Pattern:**

What Authorizer Provider would you like to select?

**Provider Name:**

OK Cancel

- a. Allow access to this URL to the user **ssouser** created in AD.

Home Log Out Preferences Record Help

Home > Summary of Deployments > SSODiag > Roles > Policies > Edit a Stand-Alone Web Application URL Pattern Scoped P

### Edit a Stand-Alone Web Application URL Pattern Scoped Policy

Back Next Finish Cancel

**Choose a Predicate**

Choose the predicate you wish to use as your new condition

The predicate list is a list of available predicates which can be used to make up a security policy condition

**Predicate List:**

Back Next Finish Cancel

Home > Summary of Deployments > SSODiag > Roles > Policies > Edit a Stand-Alone Web Application URL Pattern Scope

### Edit a Stand-Alone Web Application URL Pattern Scoped Policy

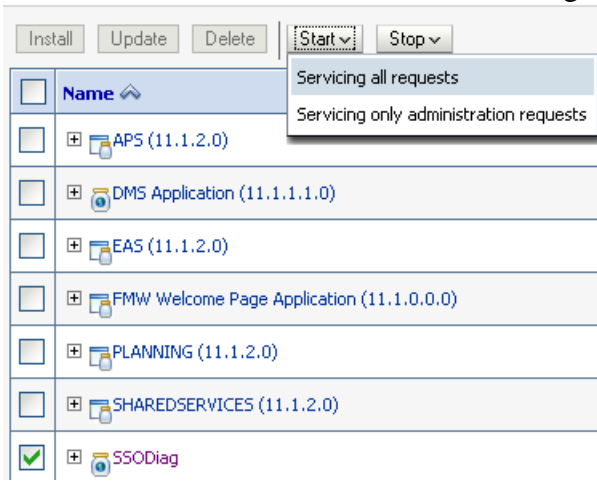
Back Next Finish Cancel

**Edit Arguments**

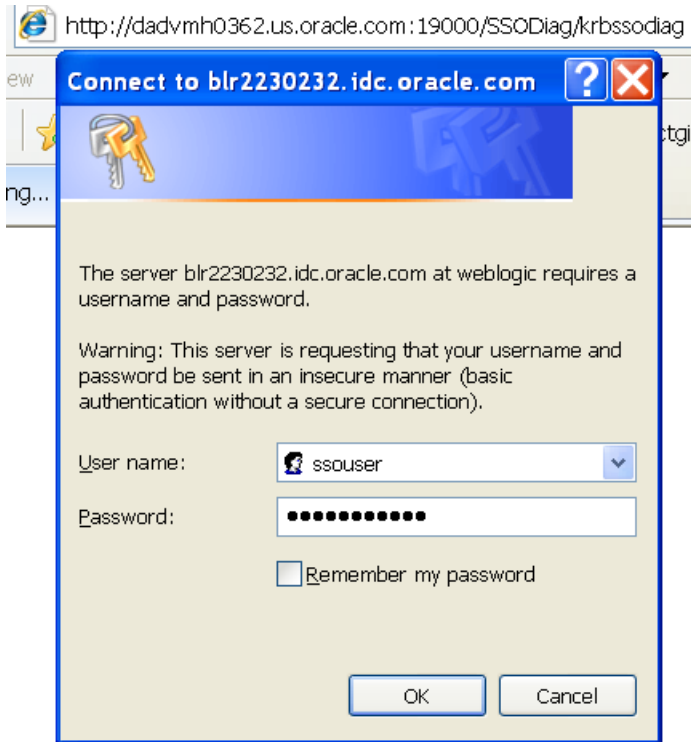
On this page you will fill in the arguments that pertain to the predicate you have chosen.

User Argument Description

6. Start the Foundation Services and SSODiag utility.



7. Login as a valid provisioned LDAP or Active directory user into the client machine configured for SAML authentication and access the page [http://OHS\\_server\\_name:port/SSODiag/krbssodiag](http://OHS_server_name:port/SSODiag/krbssodiag) from a browser
8. If the configuration is done correctly the following pages are shown.



9. Enter the password of ssouser created on the IdP side AD.

The screenshot shows a web browser window with the URL `http://dadvmh0362.us.oracle.com:19000/SSODiag/krbssodiag;jsessionid=TG5nNWOLjdLhhZwLp8shbTMnHQ`. The browser's address bar and menu bar are visible. The main content area displays the following text:

## Oracle Hyperion SSO diagnostic U

Retrieving User Principal name via getRemoteUser()...

**Success**

Authenticated Principal name retrieved...

**ssouser**

#### **Step 4: Configure EPM Foundation Services for SAML SSO-based authentication**

Once the Diagnostics Utility is run successfully, follow these steps.

**Note:** Before proceeding, the default Security model with which EPM is deployed is DD only. For the configuration described in the doc to work, change the Security model to CustomRolesAndPolicies in the `$ORACLE_HOME/user_projects/domains/EPMSysstem/config/config.xml` as

```
<name>SHAREDSERVICES#11.1.2.0</name>
<target>FoundationServices</target>
<module-type>ear</module-type>
<source-path>/scratch/arkkumar/Oracle/Middleware/EPMSysstem11F
.ear</source-path>
<security-dd-model>CustomRolesAndPolicies</security-dd-model>
<staging-mode>nostage</staging-mode>
</app-deployment>
```

1. Launch Shared Services and login as an administrator user.
2. Add an LDAP Directory or Active Directory as a User Directory and create the Federated user object – [ ssouser in our example ] in the directory.
3. Go to the Security Options tab for this Active Directory provider and enable Single Sign-On Configuration and choose the Get Remote User from HTTP Request as the SSO mechanism.

Provider Configuration **Security Options** Encryption Options

---

**Basic Configuration**

Token Timeout:  mins  
SAP Keystore Timeout:  secs  
SSO Compatibility:  ▼

Show Advanced Options

**Delegated User Management**

Enable Delegated User Management Mode:

**Single Sign-On Configuration**

Enable SSO:   
SSO Provider or Agent:  ▼  
SSO Mechanism:  ▼

**Custom Module**

Authentication Module:

Test configuration by logging into Shared Services and ensure it is properly configured.

### ***Step 5: Configure and deploy the rest of EPM to this domain***

Configure all EPM products using EPM System Configurator and deploy to the EPM domain.