

# Oracle® PeopleSoft Adapter for Oracle Imaging and Process Management

Application Extension Framework Installation Guide

10.1.3.5

August 2010

---

This guide describes how to install the PeopleSoft Adapter for Oracle Imaging and Process Management. It includes the following main sections:

- ["Prerequisites"](#) on page 1
- ["Creating Database Users"](#) on page 2
- ["Installing AXF"](#) on page 3
- ["Configuring the PeopleSoft Adapter"](#) on page 8
- ["Securing AXF"](#) on page 12
- ["Configuring AXF for a Clustered Environment"](#) on page 14
- ["Configuring and Viewing Log Files"](#) on page 14
- ["Completing Additional Imaging Solution Configuration"](#) on page 16
- ["Uninstalling AXF"](#) on page 16
- ["Uninstalling AXF from PeopleSoft"](#) on page 16
- ["Troubleshooting"](#) on page 17

## 1 Prerequisites

The following software is required and must be installed prior to installing Oracle Application Extension Framework (AXF):

### **Application Server / Database (Windows or Linux)**

AXF requires Application Server 10gR3 Standard Edition or Application Server 10gR3 Enterprise Edition, backed by Oracle Database 10g. These administrative tasks may require assistance from your DBA or IT team.

---

---

**Notes:**

- Oracle Database 10g XE is not recommended for AXF production environments.
  - Oracle Database 10g must be properly installed, configured, and patched to the correct version for use by your Application Server.
  - After running the `irca` scripts and completing the installation, verify that basic J2EE functionality is working correctly. Follow the instructions for the Loopback Adapter configuration (contained in the Application Server Installation Documentation) if necessary.
  - Note the Application Server address, administration usernames and passwords, and instance name.
- 
- 

**Oracle I/PM and Oracle I/PM Web 10g**

You will need a fully functioning Oracle Imaging and Process Management (Oracle I/PM) and Oracle I/PM Web Server 10g in order to utilize the full functionality of AXF.

**PeopleSoft Release 8.9**

A fully functioning Oracle PeopleSoft system.

- PeopleTools 8.49.12 (includes Application Designer)
- If Single Sign-On is desired, then an Oracle Identity Management (OIM) / OID Server is necessary. Also, see "[Oracle Internet Directory and Single Sign-On \(OPTIONAL\)](#)" on page 13.

**BPEL Release 10.1.3.4 with MLR 7**

You will need a BPEL server instance. This instance is used in verifying the installation, as described in "[HelloBpel Solution](#)" on page 8.

## 2 Creating Database Users

AXF uses both a PeopleSoft and an AXF database to store configuration data for the integration. Each database requires a user that is configured with the appropriate access permissions. The database user requirements for each database are described in their respective sections:

- [AXF Configuration Database User](#)
- [AXF PeopleSoft Database Configuration](#)

## 2.1 AXF Configuration Database User

The AXF infrastructure and installed solutions require a database user with the appropriate privileges for installation. The system will not function without a database for the configuration store. It is highly recommended that a new user be created to store this data and that a system or default account is not used. This prevents AXF tables mixing with tables that belong to other applications. Consult with your DBA to ensure that a secure user configuration is used both before and after installation and that the configuration meets your organization's database security requirements.

The AXF configuration database user must have the following privileges in order to properly install AXF. The AXF user's access privileges can be reduced after completing the installation.

- Tablespace privileges for default or target tablespace
- Non-zero quota in default tablespace
- Connect role
- Create index
- Create table
- Create sequence
- Create session
- Create synonym
- Insert table
- Select table
- Select sequence
- Update table

## 2.2 AXF PeopleSoft Database Configuration

All necessary tables are created when importing a project. For information in importing a project, see "[Importing the PeopleSoft Project](#)" on page 9.

## 3 Installing AXF

An AXF install script is provided for both Windows and Unix-based platforms and is located in the `/install` directory of the AXF installation package. The install script automatically performs configuration and deployment of the AXF `.ear` and creates the required tables for AXF solutions. Sample data is not inserted as part of this install; this is performed manually during an AXF Template Installation.

---

---

**Note:** The Automated AXF Installation Script does not configure PeopleSoft. This is configured in a later step.

---

---

The Installer performs the following tasks:

- Creates Application Server database tables to support AXF
- Creates a data source for connecting to Application Server
- Creates a data source for connecting to PeopleSoft

- Configures properties of the AXF EAR based on `installer.properties`
- Deploys the configured `.ear` to the specified Application Server

### 3.1 Run the Automated AXF Installation Script

To run the AXF installation script:

1. Start your AXF configuration database.
2. Copy the installation package to your Application Server middle tier and then unzip the package. This location is referred to as `AXF_INSTALL_DIR` throughout this documentation.
3. Modify the values in `AXF_INSTALL_DIR/install/installer.properties` to match your environment configuration. Folder paths in the `installer.properties` must be entered with Unix folder delimiters (`/`) even when running on Windows.

Modify the following values:

Property	Description
<code>oracle.home</code>	Application Server Oracle Home ( <code>ORACLE_HOME</code> )
<code>j2ee.home</code>	Application Server J2EE (OC4J) Home ( <code>J2EE_HOME</code> )
<code>java.home</code>	Java JDK/JRE Home ( <code>JAVA_HOME</code> ) - NOTE: <code>JAVA_HOME</code> variable must be set in the environment for ANT to work properly
<code>oc4j.admin.user</code>	OC4J Administrative User
<code>oc4j.admin.password</code>	OC4J Administrative User password
<code>oc4j.deploy.uri</code>	OPMN URI for <code>.ear</code> deployment - verify that your container name ( <code>oc4j_soa</code> , <code>home</code> , etc.) is correct
<code>db.axf.user</code>	AXF configuration database user being used to install AXF. The user must have appropriate permissions as detailed in the section " <a href="#">AXF Configuration Database User</a> " on page 3. It is highly recommended that a new user be created to store installation data and that a system or default account is not used. This prevents AXF tables mixing with tables that belong to other applications.
<code>db.axf.password</code>	AXF configuration database user password
<code>db.axf.connection</code>	JDBC connection string for SOA database

---

**WARNING:** Passwords used in installation are stored in cleartext in the `installer.properties` file and are echoed to `install.out` when the installer is run. Ensure that these files are handled properly and that files are removed or secured immediately following installation.

---

4. From the `AXF_INSTALL_DIR/dbscripts` directory, modify the `CreateAxfData.sql` script to match your environment. Modify the following values:
  - `ERROR_URL`: Modify the machine name and port to match your Application Server installation.
  - `webSecurityCheckUrl`: Modify the machine name and port to match your Application Server installation.
5. (Linux/Unix Only) If your Application Server is installed in a Linux or Unix environment, the files `AXF_INSTALL_DIR/install/install.sh` and `AXF_INSTALL_DIR/install/ant/bin/ant` must be granted execute permissions. While the procedure varies from environment to environment, this can generally be accomplished by issuing the following command:
 

```
chmod u+x install.sh ./ant/bin/ant
```
6. Execute `AXF_INSTALL_DIR/install/install.sh` (Linux/Unix) or `AXF_INSTALL_DIR/install/install.bat` (Windows) to begin the automated installation.

---

**Note:** If the following error is displayed during installation, it is a non-fatal error and can be ignored:

```
Unable to locate tools.jar \ Expected to find it in /usr/java/jre1.5.0_06/lib/tools.jar
```

---

7. When the installation completes, use the `install.out` file to verify that the application deployment was successful.
8. Destroy or obfuscate the `install.out` file according to the security policies of your organization.

## 3.2 Enabling Oracle I/PM Web Services

Follow the steps below to enable certain Oracle I/PM web services that the AXF solution uses to update Oracle I/PM indexes.

1. Locate the `WebSupportServer.exe.config` file. By default, this file resides in the following directory:

```
C:\Program Files\Stellent\WSS
```

2. Within the `<appsettings>` section, add the following lines:

```
<add key="WebSupportServer.TypeAlias.-RetrieveIndexFieldsByDocID" value=
Stellent.IBPM.Web.WebSupportServerObjects.DocumentActions.
RetrieveIndexFieldsByDocID, IBPMWebSupportServerComponents" />
```

```
<add key="WebSupportServer.TypeAlias.-ModifyDocumentIndex" value=
"Stellent.IBPM.Web.WebSupportServerObjects.DocumentActions.ModifyDocumentIndex,
IBPMWebSupportServerComponents" />
```

## 3.3 Enable TrustedIP Mode

In order to secure the AXF integration with the Oracle I/PM Web Server, users must enable Web Trust Config on the Oracle I/PM Web Server:

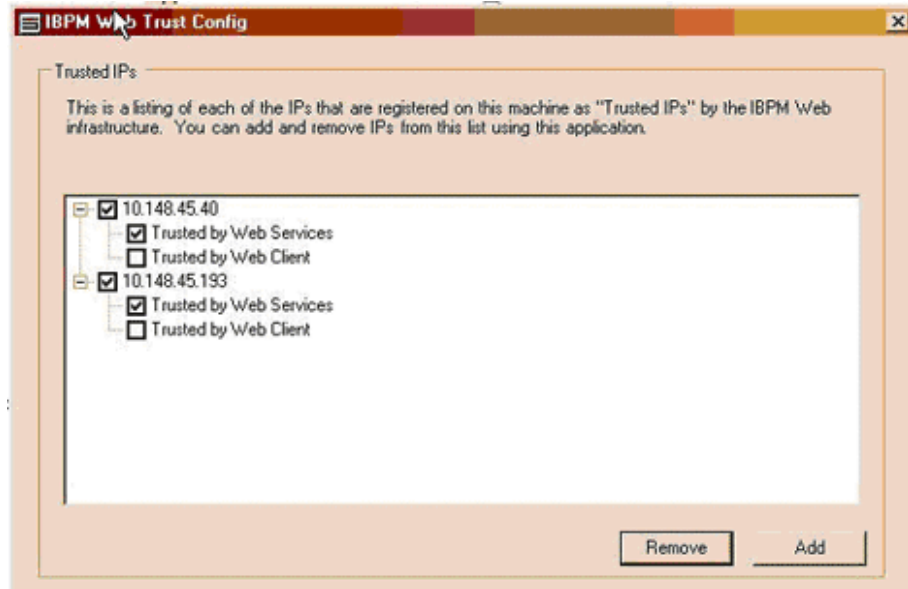
1. On the Oracle I/PM Web Server, locate and execute `IBPMWebTrustConfig.exe`, normally installed to `C:\Program Files\Oracle\IBPM`.
2. Click **Add**, and provide the IP Address for your Application Server.

---

**Note:** Verify during entry that the IP address provided does not contain spaces.

---

3. Select the `Trusted by Web Services` field.



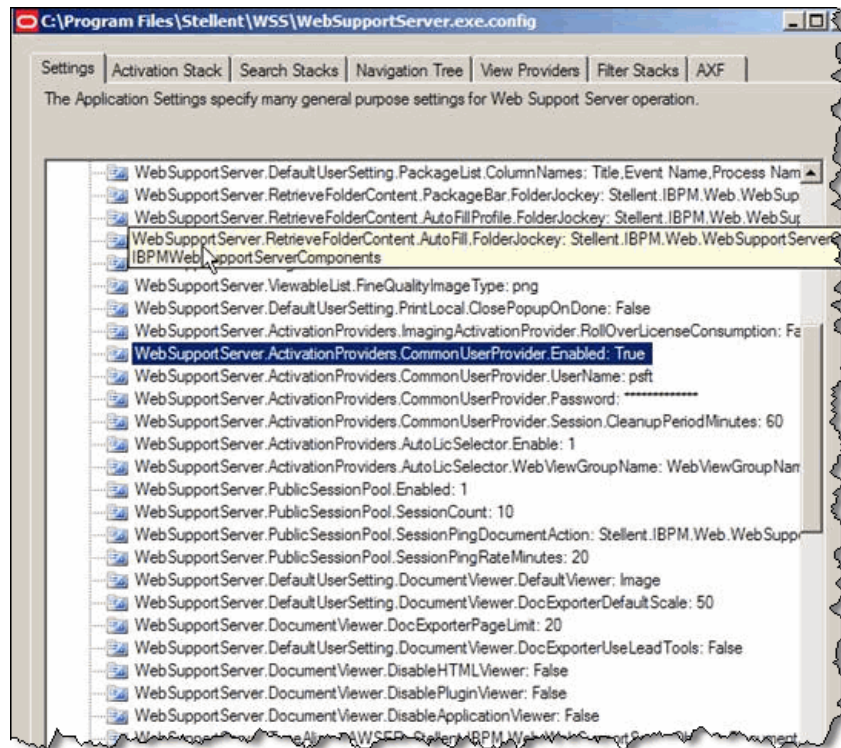
4. Click **OK** to complete the Web Trust Configuration.

### 3.4 Verify Common User Settings

Follow these steps to verify that the common user is set correctly. If it is not set correctly, no images will be displayed.

1. Open the `WSSConfigEditor.exe` application.
2. On the AXF tab, enter a valid IPM user that has permission to update image indexes.

3. On the Settings tab, ensure that the *CommonUserProvider.Enabled* setting is set to True.



4. Verify that the *CommonUserProvider.UserName* and *CommonUserProvider.Password* settings refer to a user that has view privileges.

### 3.5 Verify the Installation

Two simple solutions called HelloWorld and HelloBpel are included with AXF to verify that the AXF infrastructure is properly installed. HelloWorld is a solution which simply returns a Hello string. The HelloBpel solution includes a sample BPEL process to exercise the BPEL integration.

#### 3.5.1 HelloWorld Solution

To enable the HelloWorld solution:

1. Run the `insertHelloCommand.sql` script from the `AXF_INSTALL_DIR/drivers/HelloWorld/dbscripts` folder. It should be run as the AXF database user.
2. Access the driver page of the AXF Web application using the following URL:  
`http://host:port/axf-web/faces/Driver.jspx`
3. Enter the following values:
  - Solution Namespace: HelloWorld
  - Command Namespace: Hi
  - User Name: jcooper

#### 4. Click **Execute Command**.

An AXF response should display with a populated Conversation ID. If the response is returned, the AXF infrastructure is functioning correctly and commands can be added and executed.

### 3.5.2 HelloBpel Solution

The HelloBpel solution includes a BPEL Process and a SQL script to set up the HelloBpel SolutionNamespace for use by that process. The BPEL Process and database script can be found in the installation package under *AXF\_INSTALL\_DIR/drivers/HelloBpel*.

To enable the HelloBpel solution:

1. Edit and run the HelloBPEL SQL script (*AXF\_INSTALL\_DIR/drivers/HelloBpel/dbscripts/insertHelloWorldBpelData.sql*), replacing `localhost` with your Application Server host name and modifying all password entries as required for your environment. Ensure that the BPEL connection uses a valid external host name in the section which inserts a `providerUrl` into the `AXF_SYSTEM_PARAMETERS` table.
2. Open the BPEL project `HelloWorldBPELProcess.jpr` with JDeveloper 10.1.3.4 and deploy it to your BPEL server. If you are uncertain how to do this, consult the JDeveloper documentation for assistance with this task.
3. Access the driver page of the AXF Web application using the following URL:  
`http://host:port/axf-web/faces/Driver.jspx`
4. Enter the following values:
  - Solution Namespace: `HelloBpel`
  - Command Namespace: `OPEN_TASKLIST`
  - User Name: `jcooper`
5. Click **Execute Command**.

A response should be displayed in the response window.
6. Click **Execute Response**, and log in when prompted.

The AXF Task List should be displayed. If there are no tasks in the TaskList, open the BPEL Console and create a new instance of `HelloWorldBPELProcess` and refresh your Task List.

## 4 Configuring the PeopleSoft Adapter

Follow these main steps to configure the PeopleSoft adapter:

- ["Importing the PeopleSoft Project"](#) on page 9
- ["Configuring Integration Broker to Communicate with AXF"](#) on page 9
- ["Adding the AXF\\_ROLE to PeopleSoft"](#) on page 11
- ["Assigning Users the AXF\\_ROLE"](#) on page 11
- ["Setting User Locales"](#) on page 12
- ["Enabling AXF Components on PeopleSoft Pages"](#) on page 12



For more information about configuring AXF components on PeopleSoft pages, see the *Oracle PeopleSoft Adapter for Oracle Imaging and Process Management Application Extension Framework Configuration Guide*.

## 4.1 Importing the PeopleSoft Project

Follow these steps to import the PeopleSoft project:

1. If using Oracle DB, create a tablespace called **AXF** in the database containing the PeopleSoft schemas.
2. Start the PeopleSoft Application Designer in two-tier mode.
3. From the menu, select **Tools**, then **Copy Project**, then **From File**. The Copy From File screen is displayed.
4. Locate the **AXF\_INSTALL/psft** directory, found in the AXF file you previously unzipped in "[Run the Automated AXF Installation Script](#)" on page 4.
5. Select **psft**, the parent directory of the **AXF\_PS\_INTEGRATION** folder. The **AXF\_PS\_INTEGRATION** directory contains the project XML files, but you must select its parent directory to access them from the PeopleSoft Applications Designer. The project is displayed in the lower pane of the screen.
6. Click **Select**, select all definition types, and click **Copy**. The project files begin copying.
7. After all files have copied, select **Build**, then **Project** from the menu. The Build screen is displayed.
8. Select the **Create Tables** and **Execute SQL Now** options, and click **Build**. You can monitor the build status as the files are imported into PeopleSoft.
9. Once done, check the **PSBUILD.LOG** to verify that the project imported successfully.
10. If the log file shows *tablespace 'AXF' does not exist* errors, manually create a tablespace called **AXF** in the same database you logged into when starting the People Application Designer, then return to step 6 to rebuild the project.

## 4.2 Configuring Integration Broker to Communicate with AXF

Importing the **AXF\_PS\_INTEGRATION** project into PeopleSoft also imports the Integration Broker connection information. These components contain information needed to connect from PeopleSoft to the AXF Server. This section describes how to access this information in the PeopleSoft web client and edit it to point to the AXF Server.

Complete the steps in the sections listed below to configure communication between the Integration Broker and AXF:

- "[Configuring Communication With a 10g AXF Server](#)" on page 10
- "[Encrypting the Gateway Password](#)" on page 10
- "[Setting Up the Service Operation Routings](#)" on page 10
- "[Validating Domain Status](#)" on page 11

---

---

**Note:** A PeopleSoft local integration gateway must be set up for PeopleSoft external communications. See the PeopleSoft Enterprise documentation for information about setting up gateways. You can then proceed with configuring the PeopleSoft service operation to communicate with a 10g server.

---

---

#### 4.2.1 Configuring Communication With a 10g AXF Server

1. In PeopleSoft Server, open **PeopleTools**, then **Integration Broker**, then **Integration Setup**. The Integration setup menu expands to show the available options.
2. Click **Nodes**.
3. On the Find an Existing Value tab, select **Node Name**, enter AXF in the Node Name field, and click **Search**.
4. From the search results, click the **AXF\_SOLUTION\_MEDIATOR\_10G** link.
5. Click the Connectors tab.
6. Set the Host property name to the AXF Server name or IP address.
7. Set the URL property name to the following URL:  

```
http://AXF_Server name or IP address:port_  
number/imaging-bai-axf/AxfSolutionMediator
```
8. Click **Save**.
9. Click **Ping Node** to verify that the node is configured properly.
  - If configured properly, the word *Success* is displayed in the message text area of the Ping NodeResults page. Proceed to ["Setting Up the Service Operation Routings"](#) on page 10 and ["Validating Domain Status"](#) on page 11.
  - If *Success* is not displayed, return to the Node Configuration page to reenter values until you can ping the node successfully.

#### 4.2.2 Encrypting the Gateway Password

If *Success* is not displayed after pinging the node, you may need to encrypt the `secureFileKeystorePasswd` value under Gateway Properties, as described in the following steps.

1. In PeopleSoft Server, open **PeopleTools**, then **Integration Broker**, then **Configuration**, then **Gateways**.
2. Search for and open the LOCAL gateway, then click the **Gateway Setup Properties** link.
3. Sign on to access the `integrationGateway.properties` file.
4. Click the **Advanced Properties Page** link.
5. Use the Password Encryption Utility on the Gateway Properties page to encrypt the `secureFileKeystorePasswd` value.
6. In the Gateway Properties screen, paste the encrypted password after `secureFileKeystorePasswd=` and click **OK**.

#### 4.2.3 Setting Up the Service Operation Routings

1. From the Integration Setup Menu, select **Service Operations**.

2. On the Find Service Operation tab, enter AXF in the Service Operation field and click **Search**. A single results listing is returned.
3. Click the **AXF\_EXECUTE** link.
4. Click the Routings tab.
5. Verify that the AXF\_SM\_ROUTING\_10G routing definition's status is Active. If it is not, choose the Selected field, click the **Activate Selected Routings** button, and ensure that all other routing definition are set to Inactive.
6. Click the Save button.

#### 4.2.4 Validating Domain Status

Once you have configured the Integration Broker to communicate with AXF, follow these steps to verify its status.

1. Navigate to the Service Operation Monitor page by selecting **PeopleTools**, then **Integration Broker**, and then **Service Operations Monitor**. The Service Operations Monitor page is displayed.
2. Click **Domain Status** under the **Administration** section. The Domain Status page is displayed.
3. Verify that the domain status is listed as **Active** next to the PeopleSoft Server. If not, select **Active** from the Domain Status menu and click **Update**.

### 4.3 Adding the AXF\_ROLE to PeopleSoft

To ensure that appropriate PeopleSoft users have access to AXF functionality, follow these steps to add the AXF\_ROLE and permissions to PeopleSoft.

1. In PeopleSoft Server, open **PeopleTools**, then **Security**, then **Permissions & Roles**. The Permissions & Roles menu expands to show available options.
2. Click **Roles**. The Roles page is displayed.
3. Click the **Add New Value** tab.
4. Enter AXF\_ROLE in the Role Name field and click **Add**. The Role Name field is cleared and the AXF\_ROLE is added. You may need to enter a description and click **Save**.
5. Click **Roles**. Click the **Find an Existing Value** tab and find AXF\_ROLE from the list of available roles. Click AXF\_ROLE, and its details are displayed.
6. Click the **Permission Lists** tab, enter AXF\_PERMS in the Permission List field, and click **Save**.

### 4.4 Assigning Users the AXF\_ROLE

After creating the AXF\_ROLE in PeopleSoft, follow these steps to assign the role to all users that require access to AXF functionality.

---

---

**Note:** For AXF calls to be processed correctly from PeopleSoft, all users needing access to AXF functionality must be assigned the AXF\_ROLE in PeopleSoft.

---

---

1. In PeopleSoft Server, open **PeopleTools**, then **Security**, then **User Profiles**. The User Profiles menu expands to show available options.
2. Click **User Profiles**. The User Profiles page is displayed.
3. In the search field, select criteria to identify the user to find, and click **Search**. A listing of users is displayed.
4. Click the user to which to assign the role. A detailed page of user information is displayed.
5. Click the **Roles** tab. A listing of roles assigned to the user is displayed.
6. Click the + (plus) sign to add a blank field, and enter AXF\_ROLE in the blank field. To search for the role, click the magnifying glass icon.
7. Click **Save**. The user can now access AXF functionality on PeopleSoft pages.

## 4.5 Setting User Locales

To prevent issues with different locales when invoking AXF, PeopleSoft users should set the same values for their user locale preference and their browser locale.

## 4.6 Enabling AXF Components on PeopleSoft Pages

You configure AXF components on PeopleSoft pages using the PeopleSoft Application Designer and the AXF tables in PeopleSoft. For overview information and PeopleSoft table descriptions and examples, see the *Oracle PeopleSoft Adapter for Oracle Imaging and Process Management Application Extension Framework Configuration Guide*.

Follow these steps to enable an AXF component on a PeopleSoft page.

1. Open the AXF\_PS\_Integration Project in PeopleSoft Application Designer.
2. Open a PeopleSoft page to enable. For example, open VCHR\_HDR\_QV2.
3. Select an AXF component (user interface item or system event) and drag it onto the PeopleSoft page.
4. Save the page.
5. Configure the following PeopleSoft AXF tables to associate a command with the newly added user interface item or system event:
  - PS\_AXF\_CONFIG table
  - PS\_AXF\_COMMANDS table
  - PS\_AXF\_COMMAND\_PARAMS table

## 5 Securing AXF

The default AXF security setup uses the authentication and authorization services provided by OC4J. However, AXF can also be configured to use Oracle Internet Directory and Single Sign-On. For more information on OC4J security, refer to the *OC4J Security Guide*.

## 5.1 File-Based Security (DEFAULT)

The default AXF security setup uses the file-based security provider included with OC4J. It defines a logical role called `Users` and restricts AXF access to this role. To grant users access to AXF, they must be added to the `Users` role. A different logical role can be created/configured if so desired. For more information on managing the file-based security provider, including adding users to a role, see the section describing the file-based security provider in the *OC4J Security Guide*.

## 5.2 Oracle Internet Directory and Single Sign-On (OPTIONAL)

AXF can also be configured to use Oracle Internet Directory (OID) and Oracle Single Sign-On (OSSO). These services must be installed and configured if they are not currently part of your environment. For more information, see the section describing Oracle Identity Management in the *OC4J Security Guide*.

To secure AXF using OID and OSSO:

1. Verify that Oracle Identity Manager is installed and that the appropriate groups and users that require access to AXF are set up on OID. It may be convenient to define a group (for example, `APUsers`) and add the OID users and groups that require access to AXF to this new group.
2. Verify that the Application Server on which the AXF framework runs is a registered OSSO partner with OID.
3. Modify `mod_osso.conf`, found at `ORACLE_SOA_HOME/Apache/Apache/conf`, by inserting the following within the `<IfModule mod_osso.c>` element:

```
<Location /axf-web>
    require valid-user
    AuthType Basic
</Location>
```

4. Modify `orion-application.xml`, found inside the `/META-INF` subdirectory of the `ImagingBaiAxf` EAR file, to map the appropriate OID users and groups to the `users` logical group. For example, if there is an `APUsers` group that needs access to the AXF, insert the following node within the `<orion-application>` element:

```
<!-- Map OID groups and users to the Users logical group -->
<security-role-mapping name="users">
    <group name="APUsers" />
</security-role-mapping>
```

---

---

**Note:** This file must be modified before deploying the AXF EAR.

---

---

5. Restart the Application Server and verify that the AXF functionality works correctly within the OSSO configuration.
6. Modify `web.xml` file located at

```
<Oracle AS>\<J2EEHome>\<Instance>\applications\ImagingBaiAxf\
imaging-bai-axf-web\WEB-INF\web.xml
```

in the following ways:

- Modify `realm-name`.

- Ensure that `role-name` matches `security-role-mapping` name specified in `orion-application.xml` (see step 4).
- Based on the customer's environment, change `auth-method` and `form-login-page`, if needed.

A portion of the `web.xml` file is shown below:

```
<login-config>
  <auth-method>FORM</auth-method>
  <realm-name>jazn.com</realm-name>
  <form-login-config>
    <form-login-page>/login.jsp</form-login-page>
    <form-error-page>/loginError.jsp</form-error-page>
  </form-login-config>
</login-config>

<security-role>
  <description>Any Public User</description>
  <role-name>users</role-name>
</security-role>
```

## 6 Configuring AXF for a Clustered Environment

Perform the following steps for each server in the cluster.

1. Deploy the AXF EAR file on each Application Server instance.
2. Add the following entry to `start-parameters` in the `opmn.xml` file where AXF is installed (for example, `$INSTANCE_HOME/opmn/conf/opmn.xml`).
 

```
-Doracle.ias.jcache=true
```
3. Edit `$INSTANCE_HOME/javacache/admin/javacache.xml` to include the lines shown below, making sure to specify valid logging and persistence location nodes and physical IP addresses and ports. Note that this section must be EXACTLY the same for all instances in the cluster. You can specify any open port as the port.

```
<communication>
  <isDistributed>true</isDistributed>
  <discoverer ip="apphost1_ip_address" discovery-port="apphost1_discovery_
port"/>
  <discoverer ip="apphost2_ip_address" discovery-port="apphost2_discovery_
port"/>
</communication>
```

4. Restart OPMN on each server (not just the instance, because this is an OPMN level setting).

## 7 Configuring and Viewing Log Files

When troubleshooting, you may want to examine the following AXF-related logs:

- AXF logs (see "[Configuring AXF logging](#)" on page 15)
- Oracle I/PM WSS logs
- PeopleSoft logs (see "[Configuring PeopleSoft Logging](#)" on page 16)
- BPEL log files

## 7.1 Configuring AXF logging

Use the AXF logs to isolate issues in solution configuration. By default, AXF logging automatically occurs as part of Application Server logging. Follow these steps to configure separate AXF logging.

1. Add a log handler to the Application Server configuration.

```
$J2EE_HOME/config/j2ee-logging.xml
<log_handler name='axf-handler'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='path' value='%ORACLE_HOME%/j2ee/%OPMN_PROC_TYPE%/log/axf' />
<property name='maxFileSize' value='3485760' />
<property name='maxLogSize' value='3485760' />
<property name='encoding' value='UTF-8' />
<property name='supplementalAttributes' value='J2EE_APP.name,J2EE_
MODULE.name,WEBSERVICE.name,WEBSERVICE_PORT.name' />
</log_handler>
```

2. Add a logger and set the level from the Log Levels (ODL Message Types) listed in [Table 1](#). You can set the logging level in the XML file or via Enterprise Manager.

```
$J2EE_HOME/config/j2ee-logging.xml
<logger name='oracle.imaging' level='NOTIFICATION:1' useParentHandlers='false'>
<handler name='axf-handler' />
</logger>
<logger name='oracle.imaging.axf' level='NOTIFICATION:1'
useParentHandlers='false'>
<handler name='axf-handler' />
</logger>
```

**Table 1 Available Log Levels**

Log Type	Description	Log Level (ODL Message Type)
NULL	The logger inherits the log level set for its parent.	n/a
SEVERE	Log system errors requiring attention from the system administrator.	ERROR:1
WARNING	Log actions or conditions discovered that should be reviewed and may require action before an error occurs.	WARNING:1
INFO	Log normal actions or events. This could be a user operation, such as login completed, or an automatic operation, such as a log file rotation.	NOTIFICATION:1
CONFIG	Log configuration-related messages or problems.	NOTIFICATION:16
FINE	Log trace or debug messages used for debugging or performance monitoring. Typically contains detailed event data.	TRACE:1
FINER	Log fairly detailed trace or debug messages.	TRACE:16
FINEST	Log highly detailed trace or debug messages.	TRACE:32

3. Restart oc4j if it is running. The logger will be displayed in Enterprise Manager. You can change the logging level at runtime.

## 7.2 Configuring PeopleSoft Logging

The AXF PeopleSoft adapter uses standard apache log4j logging. Logging can be activated and managed through the log4j.properties file. This file is located in the <PeopleSoft Installation Directory>/class directory. Set the following options:

```
# A1 is set to be a ConsoleAppender which outputs to System.out.
log4j.appender.A1=org.apache.log4j.DailyRollingFileAppender
log4j.appender.A1.File=./LOGS/PS_AXF.log

# A1 uses PatternLayout.
log4j.appender.A1.layout=org.apache.log4j.PatternLayout
log4j.appender.A1.DatePattern=.yyyy-MM-dd
log4j.appender.A1.layout.ConversionPattern=%d{DATE} [%t] %-5p %c %x - %m%n

log4j.category.com.oracle.axf=DEBUG, A1
```

At a minimum, define an appender with a valid file location, and the level of messages to report (see above). Valid levels include the following in order of decreasing detail, where DEBUG displays all messages and detail:

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

---

---

**Note:** For detailed information about log4j, see the log4j documentation.

---

---

## 8 Completing Additional Imaging Solution Configuration

After completing installation as described in this guide, one of the following steps is required for implementation:

- Configure the AXF tables and PeopleSoft AXF tables, as described in the *Oracle PeopleSoft Adapter for Oracle Imaging and Process Management Application Extension Framework Configuration Guide*.
- Apply a solution template. To obtain a solution template, contact your systems integrator, Oracle Consulting, or Oracle Support.

## 9 Uninstalling AXF

To uninstall AXF from SOA, run `uninstall.sh` (Linux/UNIX) or `uninstall.bat` (Windows) and check `uninstall.out` to verify that the EAR was successfully undeployed and the database tables were successfully removed.

## 10 Uninstalling AXF from PeopleSoft

No resources are being used if no AXF solutions are implemented, so there is no harm in leaving AXF objects in the system. If no AXF solutions are implemented, you can remove all AXF objects using Application Designer.



# 11 Troubleshooting

If you are experiencing a problem returning to the Task List after completing the final task in Auto-Task mode, you may be encountering a timeout issue on the Application Server.

From Enterprise Manager, select the **Administration** on the Transaction Manager page for the container in which AXF is running. Increase the timeout value until the issue is resolved.

---

Oracle PeopleSoft Adapter for Oracle Imaging and Process Management Application Extension Framework Installation Guide, 10.1.3.5

Copyright © 2008, 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

