CONTENTS IN BRIEF

About Financial Close Management Manual Configuration ........................................... 2
Deploying Notification .EAR Files to the SOA Server ..................................................... 3
Creating Business Events Data Sources on the Financial Close Management Managed
Server ............................................................................................................................ 4
Targeting the Financial Close Management Datasource to the SOA Managed Server ...... 5
Configuring the SOA Managed Server ........................................................................... 5
Installing and Configuring EPMIdentityAsserter ............................................................ 9
Configuring the Keystore for Oracle Web Services Manager ........................................... 12
Raising the Maximum Capacity in the Connection Pool .................................................. 13
Modifying the XA Transaction Timeout ......................................................................... 14
Specifying the Language for E-Mail Notifications .......................................................... 14
About Financial Close Management Manual Configuration


Caution! You must perform these tasks before you can start and run Financial Close Management.

The following table describes Financial Close Management manual configuration tasks. The tasks are described in detail in the sections that follow.

For the procedures that follow, note that if you selected Production Mode when you created the WebLogic domain, to make changes in the WebLogic Admin Server Console you must first click Lock & Edit in the Change Center. After you make the changes, click Activate Changes in the Change Center.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy the notification .EAR files to the SOA Server.</td>
<td>“Deploying Notification .EAR Files to the SOA Server” on page 3</td>
</tr>
<tr>
<td>Create Business Events datasources on the Financial Close Management Managed Server.</td>
<td>“Creating Business Events Data Sources on the Financial Close Management Managed Server” on page 4</td>
</tr>
<tr>
<td>Target the Financial Close Management datasource to the SOA managed server.</td>
<td>“Targeting the Financial Close Management Datasource to the SOA Managed Server” on page 5</td>
</tr>
<tr>
<td>Configure the SOA managed server.</td>
<td>“Configuring the SOA Managed Server” on page 5</td>
</tr>
<tr>
<td>Install and configure EPMIdentityAssertioner.</td>
<td>“Installing and Configuring EPMIdentityAssertioner” on page 9</td>
</tr>
<tr>
<td>Configure the keystore for Oracle Web Services Manager.</td>
<td>“Configuring the Keystore for Oracle Web Services Manager” on page 12</td>
</tr>
<tr>
<td>Raise the maximum capacity in the connection pool.</td>
<td>“Raising the Maximum Capacity in the Connection Pool” on page 13</td>
</tr>
<tr>
<td>Modify the XA transaction timeout.</td>
<td>“Modifying the XA Transaction Timeout” on page 14</td>
</tr>
<tr>
<td>To receive e-mail notifications in a language different from the default language specified on the SOA server, perform additional steps.</td>
<td>“Specifying the Language for E-Mail Notifications” on page 14</td>
</tr>
</tbody>
</table>
Deploying Notification .EAR Files to the SOA Server

Perform this procedure to enable the SOA Server to communicate with the Financial Close Management Server, which is required for sending notification messages.

1. To deploy the notification .ear files:
   1. Log in to the WebLogic Admin Server Console from the machine on which Financial Close Management is installed: http://WebLogic_Admin_Host:WebLogic_Admin_Port/console.
   2. Go to the Deployment page, and then click Install.
   3. Select a notification .ear file from the Browse dialog box, and then click Next.
      - There are three notification .ear files:
        - FCCAlertNotification.ear
        - FCCNotification.ear
        - FCCTaskNotification.ear
   4. Select Install this deployment as an application, and then click Next.
   5. Select the target to SOA Managed Server (the default name is soa_server1) and then click Next.
      - The notification ear files should not be targeted to any other managed servers besides soa_server1.
   6. Under Security, leave the default selection. Under Source Accessibility, select Copy this application onto every target for me, and then click Next.
   7. Click Finish.
   8. Repeat these steps for the other two notification .ear files.

Tip: To make sure the notification .ear files are deployed properly, log in to the Admin Server Console (http://WebLogic_Admin_Host:WebLogic_Admin_Port/console), and click Deployments in the left pane. In the right pane, verify that the three notification applications (FCCAlertNotification, FCCTaskNotification, FCCNotification), are deployed and are in an Active state. If they are not in an Active state, click the check box beside the FCCXXXXNotification file name, select Start, and then select Servicing all requests.
Creating Business Events Data Sources on the Financial Close Management Managed Server

Perform this procedure to enable Financial Close Management to communicate with the SOA Server.

Caution! Be very careful to use the exact JNDI name. Do not get confused by the similar data source name that already exists and is targeted to the SOA server.

1. To add the EDNLocalTxSource data source:
   1. Log in to the WebLogic Admin Server console if you are not already logged in.
   2. Select Services, then JDBC, then DataSources, and then New, enter the following information, and then click Next.
      - Name - EDNLocalTxSource
      - JNDI Name - jdbc/EDNLocalTxSource
      - Database Type - Oracle
      - Database Driver - Oracle’s Driver (Thin) for Service Connections
   3. Clear the Supports Global Transactions box and then click Next.
   4. Enter the database details and then click Next.
      Provide the database details of the soa-infra schema that is used for SOA Server.
      Make sure to provide details for the soa-infra schema and not the financialClose_datasource schema.
   5. Click Test Configuration, and after the database connection is tested and verified, click Next.
   6. Select FinancialClose Managed Server (under Clusters, All Servers in the Cluster) as the target, and then click Finish.

2. To add the EDNSource data source:
   1. Log in to the WebLogic Admin Console, if you are not already logged in.
   2. Select Services, then JDBC, then DataSources, and then New, enter the following information, and then click Next.
      - Name - EDNSource
      - JNDI Name - jdbc/EDNSource
      - Database Type - Oracle
      - Database Driver - Oracle’s Driver (Thin XA) for Service Connections
   3. Click Next on the Transaction Options page.
   4. On the JDBC Datasource Properties panel, enter the database details and then click Next.
Provide the database details of the soa-infra schema that is used for Oracle SOA Suite Server.

5. Click Test Configuration, and after the database connection is tested and verified, click Next.

6. Select FinancialClose Managed Server (under Clusters, All Servers in the Cluster) as the target, and then click Finish.

Targeting the Financial Close Management Datasource to the SOA Managed Server

This procedure is required to access Financial Close Management data from the SOA Server, such as the notification messages that are stored in the Financial Close Management database.

➢ To target the jdbc/financialclose_datasource in SOA Server:

1. Log in to the WebLogic Admin Server console if you are not already logged in.
2. Go to DataSources, and then click jdbc/financialclose_datasource.
3. Click the Targets tab and then select the SOA Managed Server from the Target list.
4. Click Save.

Configuring the SOA Managed Server

Subtopics

- Setting the Listener Address on the SOA Server
- Connecting Oracle Internet Directory (OID), Microsoft Active Directory (MSAD), or SunOne to the SOA Server
- Configuring the E-mail Driver

Setting the Listener Address on the SOA Server

When you are configuring a new SOA Server, make sure you configure the listener address properly so that Financial Close Management can identify the SOA Server location by querying the admin server repository.

➢ To set the listener address on the SOA Server:

1. Log in to the WebLogic Admin Server console if you are not already logged in.
2. Set Listen address to the hostname of the SOA Server in two places:
   - Select Environment, then Servers, and then soa_server1.
   - Select Environment, then Machines, then LocalMachine, and then Node Manager.
Connecting Oracle Internet Directory (OID), Microsoft Active Directory (MSAD), or SunOne to the SOA Server

This procedure is required to configure the SOA Server to communicate with an external provider, such as OID, MSAD, or SunOne. Oracle’s Hyperion® Shared Services must also be configured to work with this external provider. Follow the sections specific to your provider.

**Note:** Financial Close Management does not support Shared Services Native Directory. See the Oracle Hyperion Enterprise Performance Management System User and Role Security Guide for more information.

To connect OID, MSAD, or SunOne to the SOA Server:

1. Log in to the WebLogic Admin Server console if you are not already logged in.
2. Click Security Realms on the left, click myrealm, and then click the Providers tab.
3. Click Add, enter the following details, and then click OK.
   - **For OID:**
     - Name - OID
     - Type - OracleInternetDirectoryAuthenticator
   - **For MSAD:**
     - Name - MSAD
     - Type - ActiveDirectoryAuthenticator
   - **For SunOne:**
     - Name - SunOne
     - Type - IPlanetAuthenticator

You can ignore the prompt to restart the server; you will be restarting at the end of this procedure.

4. Click the provider you just added, click the Provider Specific tab, enter the following details for your provider, and then click OK.
   - Host
   - Port
   - Principal
   - Credential
   - User Base DB
   - Group Base DB
   - User from Name Filter (MSAD only)
   - UserName Attribute (MSAD only)
You can leave the rest of the default values unchanged.

5 Click **Reorder** to move **OID, MSAD, or SunOne** so that it is second in the list of providers (after **DefaultAuthenticator** and before **EPMIdentityAsserter**).

6 Click **OID, MSAD, or SunOne** and for **Control Flag**, select **SUFFICIENT**.

7 Stop WebLogic server.

8 Make a backup copy of **domain_name/config/fmwconfig/jps-config.xml**.

9 Open **domain_name/config/fmwconfig/jps-config.xml** in a text editor, and to the **<serviceInstances>** tag, add the following **<serviceInstance>** definition:

For OID (replace the italicized values with OID information):

```xml
<serviceInstance provider="idstore.ldap.provider" name="idstore.OID">
    <property value="yourSubscriberName" name="subscriber.name"/>
    <property value="OID" name="idstore.type"/>
    <property value="username:password" name="cleartext.ldap.credentials"/>
    <property value="ldap://hostname:port" name="ldap.url"/>
    <property value="uid" name="username.attr"/>
    <extendedProperty>
        <name>user.search.bases</name>
        <values>
            <value>User Base DN</value>
        </values>
    </extendedProperty>
    <extendedProperty>
        <name>group.search.bases</name>
        <values>
            <value>Group Base DN</value>
        </values>
    </extendedProperty>
</serviceInstance>
```

For MSAD (replace the italicized values with MSAD information):

```xml
<serviceInstance provider="idstore.ldap.provider" name="idstore.AD">
    <property value="yourSubscriberName" name="subscriber.name"/>
    <property value="ACTIVE_DIRECTORY" name="idstore.type"/>
    <property value="username:password" name="cleartext.ldap.credentials"/>
    <property value="ldap://hostname:port" name="ldap.url"/>
    <property value="cn" name="username.attr"/>
    <extendedProperty>
        <name>user.search.bases</name>
        <values>
            <value>User Base DN</value>
        </values>
    </extendedProperty>
    <extendedProperty>
        <name>group.search.bases</name>
        <values>
            <value>Group Base DN</value>
        </values>
    </extendedProperty>
</serviceInstance>
```

For SunOne (replace the italicized values with SunOne information):
<serviceInstance provider="idstore.ldap.provider" name="idstore.SUNONE">
<property value="yourSubscriberName" name="subscriber.name"/>
<property value="IPLANET" name="idstore.type"/>
<property value="username:password" name="cleartext.ldap.credentials"/>
<property value="ldap://hostname:port" name="ldap.url"/>
<property value="uid" name="username.attr"/>
</serviceInstance>

Note that you must provide your password for cleartext.ldap.credentials.

10 Refer to the newly defined serviceInstance in the default jpsContext as shown in the following example:

For OID:

<jpsContext name="default">
  <serviceInstanceRef ref="credstore" />
  <serviceInstanceRef ref="keystore" />
  <serviceInstanceRef ref="policystore.xml" />
  <serviceInstanceRef ref="audit" />
  <serviceInstanceRef ref="idstore.OID" />
</jpsContext>

For MSAD:

<jpsContext name="default">
  <serviceInstanceRef ref="credstore" />
  <serviceInstanceRef ref="keystore" />
  <serviceInstanceRef ref="policystore.xml" />
  <serviceInstanceRef ref="audit" />
  <serviceInstanceRef ref="idstore.AD" />
</jpsContext>

For SunOne:

<jpsContext name="default">
  <serviceInstanceRef ref="credstore" />
  <serviceInstanceRef ref="keystore" />
  <serviceInstanceRef ref="policystore.xml" />
  <serviceInstanceRef ref="audit" />
  <serviceInstanceRef ref="idstore.SUNONE" />
</jpsContext>

11 Restart WebLogic Server.

Manual Configuration
Configuring the E-mail Driver

To configure the e-mail driver:

1. Go to Oracle Enterprise Manager for the SOA server: http://WebLogic_Admin_Host:WebLogic_Admin_Port/em and log in as user weblogic.

2. Expand the User Messaging Service folder, right-click usermessagingdriver-email(soa_server1), and select Email Driver Properties.

3. Specify the following properties, and then click Apply.
   - OutgoingMailServer - enter the mail server name, for example: myMailServer.myCompany.com
   - OutgoingMailServerPort - specify the port for the mail server.
   - OutgoingMailServerSecurity - SSL is recommended.
   - OutgoingUserName - specify a valid e-mail address.
   - OutgoingPassword - Type of Password - select Clear Text.
   - OutgoingPassword - Password - specify the password for the OutgoingUserName you specified.

4. In the left panel, expand the SOA folder, right-click soa-infra (soa-server1), click SOA Administration, and then select Workflow Notification Properties.

5. Specify the following properties, and then click Apply.
   - Notification Mode - select ALL or EMAIL.
   - Email: From Address - specify a valid e-mail address.

6. Restart the SOA Server.

7. Go to Oracle Enterprise Manager to test the human workflow notification settings:
   a. Expand the SOA folder, right-click soa-infra (soa_server1), select Service Engines, then Human Workflow, select the Notification Management tab, and then click Send Test Notification.
   b. Enter a valid SentTo e-mail address, select EMAIL as the channel, enter a test message, and then click Send.
   c. Verify that you received the e-mail message.

Installing and Configuring EPMIdentityAssertioner

Subtopics

- Adding EPMIdentityAssertioner to the Security Providers
- Creating and Configuring a Security Role in WebLogic Server

Financial Close Management uses Oracle WebLogic Server Container Security. To provide support for container security, you must install and configure the Custom WebLogic Identity
Asserter (EPMIdentityAsserter) in the Oracle WebLogic Server domain for Oracle Hyperion
Enterprise Performance Management System.

Adding EPMIdentityAsserter to the Security Providers

Note: In a distributed environment, perform steps 2 - 4 on each machine in the EPM System deployment.

To install and configure EPMIdentityAsserter:

1. Stop all managed servers (all the Web applications you deployed, including Oracle's Hyperion®
   Foundation Services, Financial Close Management, and any other managed servers in the domain).

2. Make a backup copy of setDomainEnv.cmd, which is in the WebLogic domain folder
domain_home/bin. In a distributed environment, perform this step on each machine in the EPM
   System deployment.

3. Edit setDomainEnv.cmd to include the following entries. In a distributed environment, perform this
   step on each machine in the EPM System deployment.
   a. Add the following entries after the LONG_DOMAIN_HOME environment variable. Insert a
      blank line between the existing path and the new content. Update the locations to
      point to the appropriate path on your machine:
      
      set EPM_ORACLE_HOME=C:\Oracle\Middleware\EPMSystem11R1
      set EPM_ORACLE_INSTANCE=C:\Oracle\Middleware\user_projects\epmsystem1

      For example:
      
      set LONG_DOMAIN_HOME=C:\Oracle\Middleware\EPMSystem11R1\.\user_projects\domains
      \soa_domain
      @insert new line here
      set EPM_ORACLE_HOME=C:\Oracle\Middleware\EPMSystem11R1

      set EPM_ORACLE_INSTANCE=C:\Oracle\Middleware\user_projects\epmsystem1

      Tip: Make sure you insert a blank line before and after the text you add. Make sure there
      are no trailing spaces at the end of each line you add. Also include a blank line
      between the entries for EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE.

   b. Add epm.jar to the POST_CLASSPATH. Add the following line after the last instance
      that sets POST_CLASSPATH:
      
      set POST_CLASSPATH=%POST_CLASSPATH%;%EPM_ORACLE_HOME%/common\jlib\11.1.2.0\epm.jar

      For example:
      
      if NOT "%EXT_POST_CLASSPATH%"=="" ( 
      if NOT "%POST_CLASSPATH%"=="" ( 
          set POST_CLASSPATH=%POST_CLASSPATH%;%EXT_POST_CLASSPATH%
      ) else ( 
          set POST_CLASSPATH=%EXT_POST_CLASSPATH%
      )

Manual Configuration
c. Save and close the file.

4 Copy EPMIdentityAsserter.jar from EPM_ORACLE_HOME/common/SharedServices/11.1.2.0/lib to MIDDLEWARE_HOME/wl_server10.3/server/lib/mbeantypes. In a distributed environment, perform this step on each machine in the Oracle Hyperion Enterprise Performance Management System deployment.

5 Restart WebLogic Admin Server. Do not start any of the managed servers.

6 Log in to the WebLogic Admin Console (http://WebLogic_Admin_Host:WebLogic_Admin_Port/console) using WebLogic admin credentials.

7 In the Domain Structure portlet, click Security Realms.

8 From the available realms, click the realm name with Default Realm status true.

   Tip: Click the realm name, not the check box.

9 Click the Providers tab to list all configured Authentication/Assertion providers.

10 Click New under Authentication Providers.

11 Select EPMIdentityAsserter from the list of supported Authentication/Assertion providers, then in the Create a New Authentication Provider panel, specify a name for the provider, such as EPMIdentityAsserter, and then click OK. EPMIdentityAsserter is now listed in the list of configured providers.

12 Reorder the list so that the providers are in the following order:

   - DefaultAuthenticator
   - MSAD, OID, or SunOne, depending on which provider you are using
   - EPMIdentityAsserter

   For example, to make EPMIdentityAsserter third in the Provider list, click Reorder, select EPMIdentityAsserter from the list of available providers, click the Up arrow until EPMIdentityAsserter is third from the top of the available providers list, and then click OK.

13 Click DefaultAuthenticator, and for Control Flag, select SUFFICIENT.

14 Stop WebLogic Admin Server.

15 Start WebLogic Admin Server.
Creating and Configuring a Security Role in WebLogic Server

To create and configure the security role in WebLogic Server:

1. Log in to the WebLogic Admin Console (http://WebLogic_Admin_Host:WebLogic_Admin_Port/console) using WebLogic admin credentials.
2. In the Domain Structure portlet, click Security Realms.
3. From the Available Realms list, select the realm name with Default Realm status True.
4. Click the Role and Policies tab.
5. From the Available Role list, expand Global Roles, click Roles, and then click New.
6. Specify the name valid_users for the role, and then click OK.
    The new role valid_users appears in list of Global Roles.
7. Click the valid_users role name, and on the Edit Global Role panel, click Add Conditions.
8. From the Predicate List, select Allow access to everyone, click Finish, and then click Save.

Tip: After you click Save, go back to make sure that the Allow access to everyone condition was set correctly.

Configuring the Keystore for Oracle Web Services Manager

You must set up the Keystore for message protection and configure the Credential Store Provider.

The Financial Close Management client and the Oracle Hyperion Financial Management, Fusion Edition Web service use the following policies:

- wss11_saml_token_with_message_protection_client_policy
- wss11_saml_token_with_message_protection_service_policy

To configure Oracle Web Services security:

1. Set up the items required by the policies noted above. For more information, see http://fmwdocs.us.oracle.com/doclibs/fmw/E10285_01/web.1111/b32511/setup_config.htm#BABJHIBI.
2. In particular, refer to the section “SAML Message Protection Use Case.”

2. Start each managed server in the following order:
   - WebLogic Admin Server
   - Oracle's Hyperion® Shared Services
   - Oracle HTTP Server
   - In any order:


- Oracle SOA managed server
- Financial Close Management Web application - must be started last

## Raising the Maximum Capacity in the Connection Pool

Fine tune the data source to size the connection pool.

To raise the maximum capacity in the connection pool:

1. In the WebLogic Admin Console ([http://WebLogic_Admin_Host:WebLogic_Admin_Port/console](http://WebLogic_Admin_Host:WebLogic_Admin_Port/console)), select Services, then JDBC, and then Datasources.

2. Select your data source, then Connection Pool, and then Maximum Capacity.

3. Edit settings to increase capacity as follows:

   - EDNSource—150
   - EDNLocalTxSource—150
   - financialclose_datasource—150

If resource errors specific to these data sources are logged, increase their capacity:

- EDNDataSource
- EDNLocalTxDataSource
- mds-owsm
- mds-soa
- EPMSystemRegistry
- OraSDPMDatasource
- SOADatasource
- SOALocalTxDataSource

**Note:** You can increase the capacity for each data source by a different amount, depending on the needs for your installation.
If the Oracle Hyperion Financial Close Management log includes this error message:

    java.sql.SQLException: Could not retrieve datasource via JNDI url 'jdbc/data source' weblogic.jdbc.extensions.PoolDisabledSQLException: weblogic.common.resourcepool.ResourceDisabledException: Pool data source is Suspended, cannot allocate resources to applications...', then you have exceeded the maximum connections allowed in the connection pool for the specified data source, and you need to increase the capacity of the connection pool.

### Modifying the XA Transaction Timeout

You must modify the data source transaction timeout.

**To modify the XA transaction timeout:**

1. **In the WebLogic Administration Console** (http://WebLogic_Admin_Host:WebLogic_Admin_Port/console), select Services, then JDBC, then Datasources, then SOADatasource, and then Transaction.

2. Specify the following:
   - Select Set XA Transaction Timeout.
   - Set XA Transaction Timeout to 0.

### Specifying the Language for E-Mail Notifications

To receive e-mail notifications in a language different from the default language specified on the SOA server, specify the user's language preference in the identity store.

For example, with an LDAP-based identity store:

1. Connect to the identity store.
2. Navigate to the user entry.
3. Add or set the preferredLanguage attribute.
COPYRIGHT NOTICE

Financial Close Management Manual Configuration, 11.1.2
Copyright © 2010, Oracle and/or its affiliates. All rights reserved.
Authors: EPM Information Development Team

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.