Oracle Fusion Applications Post-Installation Guide

11*g* Release 7 (11.1.7)

Part Number E22380-08

July 2013

Oracle® Fusion Applications Post-Installation Guide

Part Number E22380-08

Authors: P. S. G. V. Sekhar, Nancy Schwab

Contributors: Asra Alim, Tina Brand, Iqtidar Hussain, Essan Ni Jirman, Barbara Snyder, Vijay Tiwary, Kathryn Wohnoutka

Contents

1 Overview

2 Common

3 Customer Relationship Management

4 Financials

5 Fusion Accounting Hub

6 Human Capital Management

Preface

This Preface introduces the guides, online help, and other information sources available to help you more effectively use Oracle Fusion Applications.

Oracle Fusion Applications Help

You can access Oracle Fusion Applications Help for the current page, section, activity, or task by clicking the help icon. The following figure depicts the help icon.

?

You can add custom help files to replace or supplement the provided content. Each release update includes new help content to ensure you have access to the latest information. Patching does not affect your custom help content.

Oracle Fusion Applications Guides

Oracle Fusion Applications guides are a structured collection of the help topics, examples, and FAQs from the help system packaged for easy download and offline reference, and sequenced to facilitate learning. You can access the guides from the **Guides** menu in the global area at the top of Oracle Fusion Applications Help pages.

Guides are designed for specific audiences:

- **User Guides** address the tasks in one or more business processes. They are intended for users who perform these tasks, and managers looking for an overview of the business processes. They are organized by the business process activities and tasks.
- **Implementation Guides** address the tasks required to set up an offering, or selected features of an offering. They are intended for implementors. They are organized to follow the task list sequence of the offerings, as displayed within the Setup and Maintenance work area provided by Oracle Fusion Functional Setup Manager.
- **Concept Guides** explain the key concepts and decisions for a specific area of functionality. They are intended for decision makers, such as chief financial officers, financial analysts, and implementation consultants. They are organized by the logical flow of features and functions.
- **Security Reference Manuals** describe the predefined data that is included in the security reference implementation for one offering. They are

intended for implementors, security administrators, and auditors. They are organized by role.

These guides cover specific business processes and offerings. Common areas are addressed in the guides listed in the following table.

Guide	Intended Audience	Purpose
Common User Guide	All users	Explains tasks performed by most users.
Common Implementation Guide	Implementors	Explains tasks within the Define Common Applications Configuration task list, which is included in all offerings.
Functional Setup Manager User Guide	Implementors	Explains how to use Oracle Fusion Functional Setup Manager to plan, manage, and track your implementation projects, migrate setup data, and validate implementations.
Technical Guides	System administrators, application developers, and technical members of implementation teams	Explain how to install, patch, administer, and customize Oracle Fusion Applications. **Note** Limited content applicable to Oracle Cloud implementations.

For guides that are not available from the Guides menu, go to Oracle Technology Network at http://www.oracle.com/technetwork/indexes/documentation.

Other Information Sources

My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.

Oracle Enterprise Repository for Oracle Fusion Applications

Oracle Enterprise Repository for Oracle Fusion Applications provides details on service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production, and changes.

In Oracle Fusion Applications, you can use Oracle Enterprise Repository at http://fusionappsoer.oracle.com for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

Note
The content of Oracle Enterprise Repository reflects the latest release of Oracle Fusion Applications.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww_grp@oracle.com. You can use the **Send Feedback to Oracle** link in the footer of Oracle Fusion Applications Help.

1

Overview

Post-Installation: Overview

After Oracle Fusion Applications is installed, you need to provision the new application environment before getting started. You must have administrative privileges to perform several configuration and setup tasks that are necessary before using the environment. For more information on provisioning a new applications environment, see the Oracle Fusion Applications Installation Guide.

To prepare the Oracle Fusion applications for functional implementation, you must perform several configuration tasks of which some are common for all Oracle Fusion applications or multiple product families, and some are specific to the individual product families or products. The configuration tasks could either be mandatory or optional, depending on the requirement.

Note

Most of these tasks are not applicable to Oracle Cloud implementations.

Post-Provisioning Tasks for Individual Product Offerings

After successfully provisioning the Oracle Fusion Applications installation, configure the installed components to suit your business and functional requirements. For more information on configuring the installed components, see the Oracle Fusion Applications and Oracle Fusion Middleware product documentation, or the specific documentation for the installed component. For example, for more information about the changes to the Oracle Access Management policies that were installed during provisioning, see the Oracle Access Management documentation set.

2

Common

Verifying Installation

Verifying Installation Using Diagnostic Scripts: Procedures

After provisioning is complete, run the Oracle WebLogic Scripting Tool (WLST) diagnostic scripts to verify configurations.

Available WLST Diagnostic Scripts

This table lists what diagnostic scripts are available and what they do. You can find these diagnostic scripts at <ATGPF_ORACLE_HOME>/atgpf/bin/.

Diagnostic Scripts	Description
Application User Session (`applsessionDiagnostics.py`)	This script checks the setup and configuration definitions of Application User Session. Specifically, it checks the Session Filters and Filter-Mappings definitions and sequential order of the Filter-Mappings definitions in the application Web configuration. These are defined within the web.xml file of respective application .war file archived inside the application .ear file. This script also validates application user session runtime data for a user in any Oracle Fusion application. For example, if a user is having problems with the application user session even after confirming that all the application user session configurations are correct, then it might be the case that runtime data for that session for the user is not created properly in the database. This script can detect such type of issues. This script prompts for a session cookie and if a cookie is entered, it performs runtime data validations for the user session. If no cookie is entered, the script ignores this particular validation. To obtain the session cookie value: 1. Run the Application User Session Configuration diagnostic test to ensure if the ApplSession configuration values for your Oracle Fusion application are correct. 2. Use a valid user name and password to sign in to your Oracle Fusion Application. 3. Follow the instructions for your browser to display the list of cookies in the browser. 4. In the cookies listed for your domain site (domain site is the host in the URL after the first two periods, for example if the URL were http//apps.us.oracle.com, the domain would be oracle.com), select the cookie named `ORA_FND_SESSION_<database SID>` (<database SID> is your database session ID). 5. Check the Content field, displayed in the format `pillar_name:session_cookie_value:timestamp`. The value that you need to enter for the Application User Session Cookie parameter is the value held by `<session_cookie_value>`. If you cannot find the cookie `ORA_FND_SESSION_<database SID>` in the list of cookies, it means that ApplSession has not created for your application. Run `applsessionDiagnostics.py`, but press Enter when prompted to enter a value for the session cookie. This action will validate configuration for the application user session.
Attachments (`attachmentsDiagnostics.py`)	The script checks web.xml and verifies the configuration in the Content Server.

Data Security (`datasecurityDiagnostics.py`)	This script checks the setup and configuration definitions of data security. Specifically, it performs the following checks: • Validates JaasSecurityContext configuration defined in the adf-config.xml file, which is archived into the application .ear file. • Validates SessionGUID configuration defined in the weblogic-application.xml file, which is archived into the application .ear file. For the `datasecurityDiagnostics.py` to work properly, you must run the `applsessionDiagnostics.py` script first to ensure that Application User Session is configured properly.
Flexfields (`flexDiagnostics.py`)	This script checks the setup and configuration definitions of flexfields. Specifically, it performs the following: • Lists the Metadata Services (MDS) metadata namespaces configuration defined in the adf-config.xml file. • Lists the MDS session definition configuration defined in the adf-config.xml file. • Lists the MDS customization classes configuration defined in the adf-config.xml file. It also checks if at least one MDS customization class is registered in the adf-config.xml file. • Lists the MDS metadata store usage configuration defined in the adf-config.xml file. • Checks whether the MDS datasource defined in the adf-config.xml file exists in the domain. If the datasource exists, it checks whether it is enabled and running. • Checks whether the MDS metadata store repository defined in the adf-config.xml file exists in Oracle WebLogic Server domain. If the MDS metadata store repository exists in the domain, it checks whether the MDS metadata store partition defined in the adf-config.xml file exists in the repository. Validates that the flexfields servlet context listener is defined in the web.xml file.
Topology and taxonomy (`taxonomyDiagnostics.py`)	This script checks the setup and configuration definitions of topology and taxonomy. Specifically, it checks that the topology and taxonomy Java management extensions Managed Beans (MBeans) are correctly configured in Oracle WebLogic Server, and checks whether setup definitions of runtime MBeans attributes are defined in the topology-mbean.xml file.

UI shell integration and preferences (UIComponentsDiagnosticsCheck.py, PrefDiagnosticsCheck.py)	These scripts are used for diagnosing the configuration issues pertaining to UI Shell integration and preference settings. The UIComponentsDiagnosticsCheck.py script is used to diagnose the following: • Diagnose an Application which is already deployed on the server • Diagnose a .ear file which is locally available in file system • Diagnose a list of .war files in the .ear file The PrefDiagnosticsCheck.py script is used to check if Oracle Internet Directory is configured, and accordingly generates the output in the log file named PrefDiagnosticsCheck.log

Running WLST Diagnostic Scripts

To run the diagnostic scripts, perform the following on the Administration Server:

1. Open the setDomainEnv.sh file and set `-Dweblogic.jdbc.remoteEnabled` property to `true`.

   The setDomainEnv.sh file is located in the following directories:

   - (UNIX) DOMAIN_HOME/bin
   - (Windows) DOMAIN_HOME\bin

2. Start the Administration Server by using the following script from the fusionapps Middleware directory:

   - (UNIX) `DOMAIN_HOME/bin/startWebLogic.sh`
   - (Windows) `DOMAIN_HOME\bin\startWebLogic.cmd`

Note

For specific instructions about starting the WebLogic Administration Server, refer to the guide Oracle Fusion Middleware Managing Server Startup and Shutdown for Oracle WebLogic Server.

3. Start Oracle WebLogic Scripting Tool (WLST) console by using the following command:

Note

Before running the command, change to the directory where the scripts are stored.

- (UNIX) `ATG ORACLE_HOME/common/bin/wlst.sh`

- (Windows) `ATG ORACLE_HOME\common\bin\wlst.cmd`

4. At the `wls` offline prompt, enter the following command: `>wls:/offline> execfile ('script_name.py')`.
5. When prompted, enter the Oracle WebLogic Server user name and password, which is the same as the Oracle Fusion Middleware administrative user name and password entered during installation. Also, enter the `host` name and `port` to Administration Server for the Oracle WebLogic Server.

   The following table lists these values as an example:

Details	Sample Value
Enter directory path to store the output file	`/home/user`
Enter WebLogic server user name	`FAadmin`
Enter WebLogic server password	`Password`
Enter WebLogic server URL	t3://localhost:7001

6. For each application, enter the application name for which you want to run the diagnostics. Enter the application name along with its version, for example, `HomePageApp#V2.0`.
7. WLST generates a report of the diagnostic validation failures in the directory path you specified. View the output report file in the path displayed in the WLST output, such as the following.

```
Applsession Diagnostics Overall Status: Failure. See the output file at /
home/user/ApplsessionDiagResults.out for more information.
```

Configuring Oracle Metadata Services

Generating Optimized Query Plans for Oracle Metadata Services Queries: Procedures

After Oracle Fusion Applications is deployed and provisioned, you should ensure optimized query plans for Oracle Metadata Services (MDS) queries are generated so that performance does not decline until the next automatic statistics collection window. For each MDS schema, execute the following statements in SQL*Plus as a privileged database user, for example SYS.

1. Regather the statistics by executing the following:

```
execute dbms_stats.gather_schema_stats(
ownname =>'<schemaOwner>',
estimate_percent =>dbms_stats.auto_sample_size,
method_opt =>'for all columns size auto',
cascade => true);
```

Note

Replace <schemaOwner> with the name of the schema, for example FUSION_MDS. Also, place the entire command in a single line at the time of execution.

2. If performance does not improve after collecting statistics, then flush the shared pool to clear the execution plan for the database and generate a new query plan, using the following command:

```
alter system flush shared_pool;
alter system flush buffer_cache;
```

Note

Perform this action only when the system is not being actively used as it may affect the performance of production systems.

Installing Additional Languages

Installing Additional Languages: Highlights

Oracle Fusion Applications are released with American English as the default language. However, there is built-in support available for installing additional languages based on locale preferences. To install additional languages, you must apply the appropriate language pack using the Oracle Fusion Applications Language Pack Installer.

Note

This task is not applicable to Oracle Cloud implementations.

For administering the Oracle Fusion Applications environment, refer to the Oracle Fusion Applications Administrator's Guide.

For information on using the patching framework tools to update and maintain your Oracle Fusion Applications software between major releases, see the Oracle Fusion Applications Patching Guide.

Adding and Maintaining Languages

- You can add and maintain languages in Oracle Fusion Applications using the patching framework. When you apply patches to Oracle Fusion Applications, you can also apply associated translated patches.

  See: Introduction to Oracle Fusion Applications Languages

Setting Up Search

Setting Up Search for Oracle Fusion Applications: Highlights

Oracle Fusion Applications Search provides the search framework to manage enterprise-wide searches. Each product family within Oracle Fusion Applications such as Oracle Fusion Customer Relationship Management, Oracle Fusion Human Capital Management, and Oracle Fusion Supply Chain Management has its own set of seeded searchable objects that are packaged into its corresponding search application. For example, the seeded searchable objects for Oracle Fusion Customer Relationship Management such as leads, opportunities, and contacts are packaged in the Oracle Fusion Customer Relationship Management search application. To support the lifecycle management of searchable objects for a particular product family, you must provision your Oracle Fusion Applications environment.

Note

This task is not applicable to Oracle Cloud implementations.

Oracle Fusion Applications Environment

- Provisioning the Oracle Fusion Applications environment is mandatory before you can manage the searchable objects of any product family. Refer to the Oracle Fusion Applications Installation Guide.

  See: Provisioning a New Applications Environment

Oracle Enterprise Crawl and Search Framework

- Oracle Fusion Applications Search leverages the Oracle Enterprise Crawl and Search Framework to enable search on transactional business objects. Therefore, validating the environment for Enterprise Crawl and Search Framework involves the recommended checks for establishing Oracle Fusion Applications Search. Refer to the Oracle Fusion Applications Administrator's Guide.

  See: Validating the Environment for ECSF

- Managing search involves making seeded searchable objects available for search, maintaining search categories, and so on. Refer to Oracle Fusion Applications Administrator's Guide.

  See: Administering Search

- To make the Fusion Applications search components appear on the user interface, you need to enable the relevant profile option. Refer to Oracle Fusion Applications Administrator's Guide.

  See: Enable the Oracle Fusion Applications Search UI

Configuring Help Search: Highlights

You can include Help in the list of search categories for the search in the global area of Oracle Fusion Applications. This search is of type Oracle Fusion Applications Search, and administering this search involves tasks in Oracle Enterprise Crawl and Search Framework.

Note

This task is not applicable to Oracle Cloud implementations.

The search in Oracle Fusion Applications Help and the navigators, for example Search by Business Process, are based on other search functionality and do not require configuration.

Oracle Enterprise Crawl and Search Framework administration is described fully in the Oracle Fusion Applications Administrator's Guide. As you read content from that guide, keep in mind that Oracle Fusion Applications Search is not used only for Oracle Fusion Applications Help; therefore, the content is not specific to help.

Searchable Objects

- Deploy and activate the TopicSearchPVO searchable object, associate it with the Help category and deploy the category, and deploy and start index schedules. Each crawl picks up customizations and patches for help, so the frequency depends on how often you add, manage, or patch help.

  See: Making Seeded Searchable Objects Available for Search

- Do not modify the TopicSearchPVO searchable object itself.

  See: Modifying the Display Name of Deployed Searchable Objects

  See: Modifying the Title Body Keyword and Action Title of Searchable Objects

Configuring External Search Categories for Oracle Business Intelligence and Oracle WebCenter Portal: Procedures

To perform global search within Oracle Business Intelligence (BI) and Oracle WebCenter Portal, you must create the appropriate external search categories in Oracle Fusion Applications. For general instructions on making external search categories available for search, see the Oracle Fusion Applications Administrator's Guide.

However, before you proceed with the configuration of external search categories for Oracle Business Intelligence and Oracle WebCenter Portal, you must manually create the Business Intelligence data source. Refer to the section Configuring for Full-Text Catalog Search in the Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition.

You can perform the search-related configuration tasks using Oracle Enterprise Crawl and Search Framework. To configure external search categories for Oracle Business Intelligence and Oracle WebCenter Portal, follow these instructions.

1. Sign in to Oracle Enterprise Manager Fusion Applications Control.
2. From the navigation pane, open **Farm** - **Enterprise Crawl and Search Framework** folder.
3. Select the application engine instance SES 11.2.1. It contains the searchable objects that you want to manage to open the Enterprise Crawl and Search Framework Configuration Settings page.
4. From the Search Engine Types table, click Oracle Fusion Application Search engine SES 11.2.1 to open the Search Engine Instance administration page.
5. On the External Search Categories tab, click **Import**.
6. In the Available Categories column, select the check box of the external search categories you want to import, and click **Move** to shuttle your selection to the Selected Categories column.
   - To import BI, select bi_search
   - To import Oracle WebCenter Portal, select Collaboration
7. Click **OK** to import the selected external search categories.
8. Associate the Application ID with the imported external categories:
   - To associate with BI, in the Application ID column corresponding to the external search category you imported (bi_search), enter BI.
   - To associate with Oracle WebCenter Portal, in the Application ID column corresponding to the external search category you imported (Collaboration), enter WC.
9. Click **Save External Search Category** to save the selected record.
10. Associate the Application ID with the Search Service component:

a. From the navigation pane on the left side, select **Enterprise Crawl and Search Framework** folder. The Enterprise Crawl and Search Framework Settings page appears.

b. From the context menu of **Enterprise Crawl and Search Framework**, select **Home**.

c. Select the first active service component and note down the search engine instance that is associated with the active service component.

d. In the `ECSF_QUERY_SERVICE_APP_IDS` field, enter the Application ID in comma separated string format:

- To configure external search category for Business Intelligence, enter BI
- To configure external search category for Oracle WebCenter Portal, enter WC

11. Save the changes.
12. Restart the Search application from the WebLogic Server Console.

Making a Search Application Highly Available: Procedures

Each installation of Oracle Fusion Applications can provision one or more offerings such as Customer Relationship Management (CRM), Human Capital Management (HCM), and so on. Each offering has its own search application such as CRM Search Application, HCM Search Application and so on. However, the application architecture restricts running only one search application at a time and only that search application is registered as the identity plug-in end point of Oracle Secure Enterprise Search (SES). The identity plug-in end point of Oracle SES is a critical part of Oracle Fusion Search and is used in authenticating all users using the search functionality. Therefore, to mitigate the risk of any down time, it is necessary to identify and make the registered search application highly available by adding more managed WebLogic servers to the cluster.

Depending on the provisioned offerings, the actual search application registered as the identity plug-in endpoint varies. The following instructions help you identify the search application and add more managed WebLogic servers to the existing cluster.

1. Sign in to the Oracle SES Administration page.
2. On the Global Settings tab, click **Identity Management Setup**. Review the protocol identified by the HTTP end point for authentication and the current search application indicated by one of the following values for User ID:

   - User ID = `FUSION_APPS_CRM_ECSF_SEARCH_APPID`: indicates CRM Search Application is used
   - User ID = `FUSION_APPS_FSCM_ECSF_SEARCH_APPID`: indicates FSCM Search Application is used

- User ID = `FUSION_APPS_HCM_ECSF_SEARCH_APPID`: indicates HCM Search Application is used

3. Identify the search application and add more managed servers to the cluster. For detailed instructions, see the Oracle Fusion Applications High Availability Guide.

Setting Up Help

Setting Up Privacy Statement: Procedures

The Privacy Statement link under the Help menu on Oracle Fusion Applications Home page is provided so that customers can link it to a preferred URL to display the privacy content. By default, the link is grayed out. As an administrator, you can change the configuration settings to activate the link and point it to the desired URL page. When clicked, the page opens in a new browser window.

To set up the privacy statement:

1. Sign in to Oracle Fusion Applications.
2. From the menu bar, select **Administration** - **Setup and Maintenance** . The Setup and Maintenance work area appears.
3. Search for the **Manage Administrator Profile Values** task and open the task page. The Manage Administrator Profile Values page appears.
4. Search for the **PRIVACY_PAGE** profile option.
5. In the Profile Values region, check for the default profile value that is set to the **Site** profile level. If it does not exist, create a new profile value and from the **Profile Level** list, select **Site**.
6. In the **Profile Value** field, enter the URL of the web page that needs to be displayed when users click the **Privacy Statement** link.
7. Click **Save**.

Configuring Oracle User Productivity Kit In-Application Support: Procedures

Users may need to access and take advantage of the Oracle User Productivity Kit (UPK) content while working with Oracle Fusion Applications. To make the Oracle UPK content available for users, you need to enable and configure the UPK link under the Help menu of Oracle Fusion Applications, using the Oracle UPK In-Application Support functionality.

To perform this task, you must have the role of a System Administrator and have relevant privileges on the environment where you want to enable and configure the UPK link.

Configuring the Oracle UPK In-Application Support involves the following activities:

1. Registering Oracle UPK as an Enterprise Application.
2. Deploying the Oracle UPK package on a HTTP server.

Registering Oracle UPK as an Enterprise Application

Your System Administrator must have security access to use Oracle Fusion Functional Setup Manager to complete the steps that follow.

To complete the configuration:

1. On the Oracle Fusion Applications Home page, select **Navigator** - **Tools** - **Setup and Maintenance** to access the Setup and Maintenance work area.
2. In the Setup and Maintenance work area, in the Tasks list, click **Topology Registration** - **Register Enterprise Applications** .
3. In the Register Enterprise Applications work area, do one of the following:
   - To modify an existing configuration, click the Name link of the registered application.

     For example: Oracle User Productivity Kit
   - To register Oracle UPK as a new application in Oracle Fusion, click **Add (+)**, if this is a new configuration.
4. In the Add Enterprise Application work area, in the Basic Information section, do the following:

   a. In the Enterprise Environment drop-down list, select your environment.

   For example: Oracle

   b. In the Enterprise Application drop-down list, select your enterprise application.

   For example: Oracle User Productivity Kit

   c. In the Name field, enter the name of the enterprise application that you are registering.

   For example: Oracle User Productivity Kit
5. In the Server Details section, do the following:

   a. In the Server Protocol drop-down list, select the appropriate protocol for the server that you plan to use to launch UPK content.

   The UPK Player supports both HTTP and HTTPS.

   b. In the External Server Host field, enter the full DNS name of the server host.

   For example: content.mycompany.com

c. In the External Server Port field, enter the appropriate port for either HTTP or HTTPS. It could be either the default value 80/443 or customer configured port location.

Note

The Context Root name is the name of the virtual directory used in the URL that launches your UPK content.

d. Click **Save and Close** when you are done.

6. Click **Regenerate Domain Connections**.
7. Sign out of Oracle Fusion Applications and sign in again.
8. Click the Help menu on the Oracle Fusion Applications Home page to verify if the Oracle User Productivity Kit is now available as a menu item.

Deploying the Oracle UPK Player Package

Deploy your Player Package to any server that uses HTTP or HTTPS protocols.

The content root directory must be configured to the location of your UPK player on the web server.

For example: http(s)://<server>:<port>/<directory>

Test access to the content.

If the Oracle UPK Player launches with all topics, you are ready to configure Oracle Fusion Applications for In-Application Support.

Setting Up Notifications

Configuring Workflow E-Mail Notifications: Procedures

Oracle User Messaging Service is a component of Oracle SOA Suite, which enables you to receive notifications sent from SOA applications.

Applications in the following product families receive approval notifications and complete approvals and rejections of requests through e-mail:

- Oracle Fusion Customer Relationship Management
- Oracle Fusion Financials
- Oracle Fusion Human Capital Management
- Oracle Fusion Supply Chain Management
- Oracle Fusion Procurement
- Oracle Fusion Project Portfolio Management

Note

Before you proceed, ensure that an e-mail server exists. If you intend to use the bulk e-mail feature of Customer Relationship Management, you need to set up the e-mail to handle bulk e-mail. To configure an e-mail server, see detailed instructions in the Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher.

Configuring E-Mail Notification Using SOA Suite

You must configure Oracle SOA Suite as follows to enable e-mail notification:

1. For existing users, associate the users with their e-mail addresses in the domain.

   For new users:

   a. Add user profile in the domain.

   b. Create e-mail account in the e-mail server for the added user.

   c. Associate the user profile with the respective e-mail address.

   For more information on using the administration console to manage the users, groups, and roles, see the Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server.

2. Configure e-mail driver properties.

Note

To enable the workflow participants to receive and forward notifications, configure Oracle User Messaging Service by setting the appropriate driver instances with Oracle Enterprise Manager Fusion Applications Control.

a. In the navigation pane, expand **farm** - **User Messaging Service** - **usermessagingdriver-email** .

b. Go to **User Messaging Email Driver** - **Email Driver Properties** . The Email Driver Properties page displays.

c. In the **Driver-Specific Configuration**, modify the **Outgoing** and **Incoming** properties as provided below.

- Modify `OutgoingMailServer`, `OutgoingMailServerPort`, `OutgoingDefaultFromAddr`, `OutgoingUsername`, and `OutgoingPassword`.
- Modify `IncomingMailServer`, `IncomingMailServerPort`, `IncomingMailIDs`, `IncomingUserIDs`, `IncomingUserPasswords`, and `receivefolder`.
- Select the **ImapAuthPlainDisable** checkbox.

d. Click **Apply** to save the changes.

Note

To configure e-mail driver properties for other **usermessagingdriver-email** services under **farm** - **User Messaging Service** , repeat all the above steps (2a to 2d).

For more information on e-mail custom properties, see the Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite.

3. Configure workflow notification properties.

Set the notification properties properly to enable workflow e-mail notifications. To select the notification mode with Oracle Enterprise Manager Fusion Applications Control:

a. In the navigation pane, expand **farm - SOA** .

b. Go to **SOA Infrastructure** - **SOA Administration** - **Workflow Notification Properties** . The Workflow Notification Properties page displays.

c. From the **Notification Mode** list, choose **All**.

d. In the **Notification Service** section, specify the notification channel values. These properties are used to notify the users of any changes to the state of a task. Workflow notifications can use three types of addresses:

   - From Address: For sending notifications.
   - Actionable Address: For receiving actionable responses. The Actionable Address is the account in which task action-related e-mails are received and processed by human workflow.
   - Reply To Address: For receiving reply notifications.

e. Click **Apply** to save the changes.

Note

To configure workflow notification properties for other SOA servers, repeat all the above steps (3a to 3e).

For more information on user messaging server and configuring human workflow notification properties, refer to section Configuring Oracle User Messaging Service in the Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite.

4. Assign the actionable e-mail account name.

   To specify the actionable e-mail account name with Oracle Enterprise Manager Fusion Applications Control:

a. In the navigation pane, expand **farm - SOA** .

b. Go to **SOA Infrastructure** - **SOA Administration** - **Workflow Task Service Properties** . The Workflow Task Service Properties page displays.

c. In the **Actionable Email Account** field, enter the incoming actionable e-mail account to use. The default account name is `Default`, which is the account configured in step 3, Configure workflow notification properties. If a different account name is specified in the **Actionable Email Account** field, then create and configure that account.

For more information on configuring human workflow notification properties, see the Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite.

Important

Repeat steps 2, 3, and 4 to configure e-mail notification separately for each product family such as CRM, HCM, and so on.

5. Restart Oracle WebLogic Server

   To restart the Oracle WebLogic Server Managed Servers for the domains in the product families:

   a. Stop the Managed Servers by using one of the following scripts from the fusionapps Middleware home directory. In these scripts, `managed_server_name` specifies the name of the Managed Server and `admin_url` specifies the listen address and port number of the domain's administration server. The listen address is the host name, IP address, or domain name server (DNS) name. When prompted, enter your user name and password.

Platform	Script
Windows	`FA_MW_HOME\user_projects \domains\domain_name\bin \stopManagedWebLogic.cmd managed_server_name admin_url`
UNIX	`FA_MW_HOME/user_projects/ domains/domain_name/bin/ stopManagedWebLogic.sh managed_server_name admin_url`

   b. Start the Oracle WebLogic Server Managed Servers for the product families using one of the following scripts from the fusionapps Middleware directory. In these scripts, `managed_server_name` specifies the name of the Managed Server and `admin_url` specifies the listen address (host name, IP address, or DNS name) and port number of the domain's administration server. When prompted, enter your user name and password.

Platform	Script
Windows	`FA_MW_HOME\user_projects \domains\domain_name\bin \startManagedWebLogic.cmd managed_server_name admin_url`
UNIX	`FA_MW_HOME/user_projects/ domains/domain_name/bin/ startManagedWebLogic.sh managed_server_name admin_url`

   For more information about performing administrative activities, refer to the Oracle Fusion Applications Administrator's Guide.

6. Add the host name and address of the e-mail server to the /etc/hosts file on the server hosting the SOA managed servers where the drivers are running.

Configuring Oracle Business Intelligence

Configuring Oracle Business Intelligence Components: Highlights

The Oracle Business Intelligence applications suite consists of two products: the Oracle Transactional Business Intelligence application and Oracle Business Intelligence Applications. To use these components effectively, you must configure them after their installation.

Note

Only the task relevant to Oracle Transactional Business Intelligence is applicable to Oracle Cloud implementations.

Configuring Oracle Transactional Business Intelligence

After you install Oracle Fusion Transactional Business Intelligence, configure it to obtain real-time analysis of your organization's day-to-day operational data.

- For information on setting up accounting segment, modeling Essbase cubes, and setting up Descriptive Flexfields see the Oracle Fusion Transactional Business Intelligence Administrator's Guide.

Installing and Configuring Oracle Business Intelligence Applications

- Oracle Business Intelligence Administration Tool is a part of the Oracle Business Intelligence Client Tools and is packaged along with the Oracle Business Intelligence Applications. It enables you to manage the metadata repository and is required for certain steps in the Oracle Business Intelligence Applications setup process. Refer to the Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence.

  See: Installing and Uninstalling Oracle Business Intelligence Client Tools

- Oracle Business Intelligence Applications consists of pre-built metadata, dashboards, analyses, and ETL tools that provide insight into your organization's historical data. The Oracle Business Intelligence Applications software binaries are installed during Oracle Fusion Applications installation and provisioning in the Oracle Home for Business Intelligence. You must set up the Oracle Business Intelligence Applications components before using them. For details, refer to the Oracle Fusion Middleware Installation and Configuration Guide for Oracle Business Intelligence Applications.

  See: Setting Up Oracle Business Intelligence Applications

About Oracle Business Intelligence Enterprise Edition

- Oracle Business Intelligence Enterprise Edition provides the underlying platform for the real-time and historical reporting applications. Oracle Business Intelligence Enterprise Edition provides direct access to guides, context-sensitive help, and libraries for conceptual and procedural information for understanding and using Oracle Business Intelligence Enterprise Edition. Refer to the Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition (Oracle Fusion Applications Edition).

See: Where Can I Get Help or More Information?

Enabling Language Selection for Oracle Business Intelligence Enterprise Edition: Procedures

Users must be able to select a preferred language when using the single sign on page to log on to Oracle Business Intelligence (BI) Enterprise Edition.

To enable language selection via Oracle Access Manager, configure the following:

- Oracle BI Enterprise Edition
- Oracle Enterprise Manager

Configuring Oracle BI Enterprise Edition

Configure Oracle BI Enterprise Edition to support the libraries provided by Oracle Fusion Middleware Extensions for Applications.

1. Install Oracle BI Enterprise Edition using the BIEE shiphome from the BISHIPHOME label.

Note

BISHIPHOME should be the label picked up in the FMWTOOLS label that is used to setup the ATGPF environment.

2. Install the ATGPF shiphome.
3. Install Oracle WebCenter using the WebCenter shiphome:
   a. Download the /fmwtools/soa/shiphome/wc.zip and /fmwtools/shiphome/atgpf.zip files from the FMWTOOLS label.

   b. Extract the contents of wc.zip and atgpf.zip to a local folder, for example sh_folder.

   c. Run the WebCenter installer using the command `sh_folder/wc/Disk1/runInstaller -jreLoc $JAVA_HOME`.

   d. Follow the wizard to install WebCenter to $MW_HOME, where Oracle Business Intelligence Enterprise Edition is installed and deselect the ECM Server configure check box.

   e. Run the ATGPF installer using the command `sh_folder/atgpf/Disk1/runInstaller -jreLoc $JAVA_HOME`, and install ATGPF to $MW_HOME, where Oracle Business Intelligence Enterprise Edition is installed.
4. Extend the Business Intelligence domain:
   a. Shut down the Business Intelligence domain (both administration and managed servers).

   b. Run the configurator using the command `$MW_HOME/oracle_common/common/bin/config.sh`.

   c. Select the existing domain (BI domain) that you need to extend and from the list of templates, select **Oracle Application Core (Webapp)**.

d. In the configuration information field, enter the JDBC data sources.

Note

Ensure that you enter the same application database details, which exist in the ATGPF environment.

e. In the Custom Services Deployment field , select Target JDBC/ ApplicationDBDS to bi_cluster, and complete the process of extending the domain.

f. To start the Business Intelligence domain, start the administration server followed by the managed server.

5. Configure the Oracle Business Intelligence Publisher authentication schema:

   a. Log on to Oracle Enterprise Manager and from the menu, select **Business Intelligence** - **CoreApplication** - **Security** .

   b. Enable Single Sign On and select Oracle Access Manager plus Fusion Applications.

   c. Save the changes.

   d. Restart the Oracle Business Intelligence Publisher service.

6. Configure Single Sign On.

7. Restart the Oracle Business Intelligence domain in Oracle Fusion Applications mode.

8. Shut down the Business Intelligence domain and start it.

9. Start WebLogic servers using the command line interface:

   - To start the administration server, use:

```
cd $Domain_Home/bin

./startWeblogic.sh
```

   - To start the managed server, use:

```
cd $Domain_Home/bin
./startManagedWeblogic.sh bi_server1
```

Configuring Oracle Enterprise Manager

To configure Oracle Enterprise Manager:

1. Log on to Oracle Enterprise Manager.

2. From the menu, select **Business Intelligence** - **CoreApplication** - **Security** .

3. Enable Single Sign On and select Oracle Access Manager plus Fusion Applications.

4. Save the changes.

5. Restart the Business Intelligence components.

Setting Up Segregation of Duties

Setting Up Segregation of Duties for Role Provisioning: Procedures

When a role assignment is requested through Oracle Identity Management, it needs to check with the Application Access Controls Governor to see if there are any segregation of duties (SOD) violations. If Application Access Controls Governor reports any SOD violations, depending on the violation or access issues, Oracle Identity Manager needs to send the request for an approval to specific roles, automatically approve the request, or reject the request.

For more information about role provisioning and segregation of duties and the integration between Oracle Identity Management and Application Access Controls Governor, see the Oracle Fusion Applications Security Guide.

Setting Up SOD

To set up SOD, complete the following procedures.

1. Ensure that the following configuration requirements are met:
   - Set up an Application Access Controls Governor server
   - Set up the Oracle Fusion connector
   - Define a data source
   - Update the Application Access Controls Governor server details in Identity Manager

   For more information on setting up these as part of the Oracle Application Access Controls Governor, see the Oracle Governance, Risk and Compliance Installation Guide.

Important

Perform all the setup tasks only from the Identity Manager domain.

2. To manually switch from Oracle Identity Management to Lightweight Directory Access Protocol (LDAP) as the source of user roles for Service-Oriented Architecture (SOA) server deployed with Identity Manager, perform the following configuration steps.

   This step is applicable only to the environments set up with Oracle Identity Management and Oracle Access Management integration, and LDAP synchronization of users and roles enabled in Oracle Identity Manager.

   a. Sign in to the Enterprise Manager Console as a Weblogic_Administrator user.

   b. Access the Weblogic Domain in which Identity Manager is configured.

   c. Open **Security - Realms** .

d. On the Providers tab of the security realm settings page, open **OIDAuthenticator**.

e. In the provider specific parameters for `OIDAuthenticator`, update the Oracle Virtual Directory port with the Oracle Internet Directory port by changing the value of the port from Oracle Virtual Directory port to Oracle Internet Directory port.

f. On the Providers tab of the security realm settings page, create a new authentication provider with the name OIMSignatureAuthenticationProvider and the type OIMSignatureAuthenticationProvider.

g. Configure `OIMSignatureAuthenticationProvider` with the following parameters:

- DBDriver: oracle.jdbc.OracleDrive
- DBUrl: jdbc:oracle:thin:@<db_hostname>:<db_port>:<db_sid>.

  For example, jdbc:oracle:thin:@localhost:5521:iam4.
- PKIKeystore Provider: sun.security.rsa.SunRsaSign
- Symmetric Key Keystore Provider: com.sun.crypto.provider.SunJCE
- DBUser: the Identity Manager database schema user name
- DBPassword: the Identity Manager database schema user password

Note

These parameters as same as in `OIMAuthenticationProvider`.

h. Delete the existing `OIMSignatureAuthenticator`.

i. Reorder authentication providers into the following sequence:

1. OAMIDAsserter
2. OIMSignatureAuthenticationProvider
3. OIMAuthenticationProvider
4. OIDAuthenticator
5. DefaultAuthenticator
6. DefaultIdentityAsserter
7. IDMDomainAgent

j. Disable the **Weblogic** user profile in Identity Manager.

Note

You need to disable this user profile to avoid the authentication errors at Identity Manager Authenticator level, as Identity Manager Authenticator is now placed ahead of the Default Authenticator in authentication provider ordering. However, you cannot disable the user profile from Identity Manager

Administration page. Instead, run the following SQL scripts on the OIM database.

- `update usr set usr_status='Disabled' where usr_login='WEBLOGIC';`
- `update usr set usr_disabled=1 where usr_login='WEBLOGIC';`

---

k. Create the **Weblogic** user profile in LDAP and add it to the **Administrators** role. If the **Administrators** role does not exist in LDAP, create it first and then add the **Weblogic** user profile to it.

   You can create a user in LDAP by creating an LDAP Data Interchange Format (LDIF) file and using the **ldapadd** command.

l. In the jps-config.xml file, locate the element group `<jpsContext name="default">`.

m. Under `<jpsContext name="default">`, locate the identity store element `<serviceInstanceRef ref="idstore.oim"/>`, replace its value with `idstore.ldap` and save the file.

n. Restart all servers in the domain, including the admin server.

3. Administer role memberships using the Delegated Administration tasks in Oracle Identity Manager. To apply SOD checks on these administrative actions, configure the following Identity Manager system properties.

   - Set `XL.RM_REQUEST_ENABLED` to `TRUE`
   - Set `XL.RM_ROLE_ASSIGN_TEMPLATE` to `ASSIGN ROLES WITH CALLBACK POLICY`

   For more information about managing system properties of Identity Manager and its request-based role grants, see the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

Turning Off SOD Checks

To turn off the SOD checks, perform the following.

1. Sign in as an Administrator into the Enterprise Manager application that administers the Oracle Identity Manager server.
2. Navigate to the system MBean browser for the Identity Manager server.
3. Locate `OAACGConfig MBean` option.
4. Set the property `SODEnabled` to `False` and save.
5. Sign in to the Identity Manager's advanced console and set the system property `XL.RM_REQUEST_ENABLED` to `False`.
6. Restart the Identity Manager server.

Note

To turn on the SOD checks, set the properties `SODEnabled` and `XL.RM_REQUEST_ENABLED` to `True`.

Modifying the Segregation of Duties Routing Policies for Approving Role Provisioning: Procedures

When an access control necessitates an approval, the predefined routing rules determine the approver for a role provisioning request. These rules are defined in the `OAACGRoleAssignSODCheck` composite because of Approval Management Extensions (AMX) functionality such as Supervisory List.

The following rules are used to route the request to the suitable role.

- If the requested role assignment is of Chief Financial Officer, SOD remediation task is assigned to the IT Security Manager role.
- If SOD violation occurs because of a policy where the SOD control perspective is **Business Process** - **Information Technology Management** and the control priority is 1, SOD remediation task is assigned to the Application Administrator role.
- If SOD violation occurs for any other reason (Catch All rule), SOD remediation task is assigned to the Controller role.

If you need to modify these routing rules, you can do it in two ways:

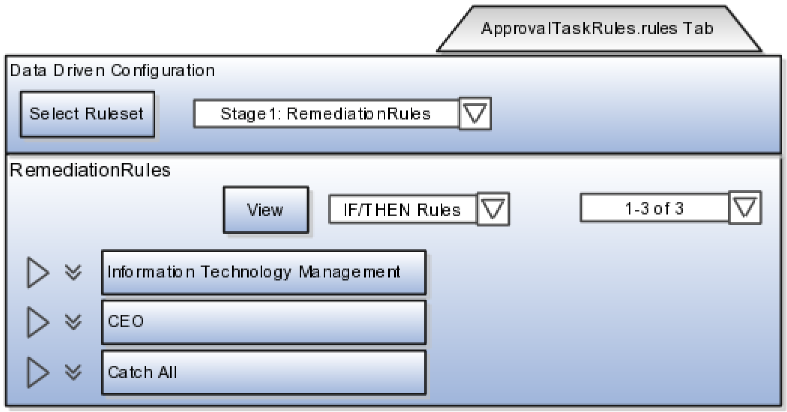
- Using Oracle SOA Composer
- Using JDeveloper

Modifying Rules Using Oracle SOA Composer

Use the Oracle SOA Composer associated with the SOA server used by Oracle Identity Management, and change the `RemediationRules` ruleset associated with `OAACGRoleAssignSODCheck` composite. For instance, you may want to shift the task assignment in the Catch All rule from the Controller role to a different role.

1. Sign in to the Oracle SOA Composer.
2. Click **Open** - **Open Task** .
3. Select **OAACGRoleAssignSODCheck** and click **Open**.
4. On the ApprovalTaskRules.rules tab, click **Edit**.
5. Expand Catch All and in the **THEN** statement, replace `GL_CONTROLLER_JOB` with the new role.
6. Save the changes.

The figure shows the ApprovalTaskRules.rules tab in Oracle SOA Composer.



For more information about using Oracle SOA Composer to add rules, see the Oracle Fusion Middleware User's Guide for Oracle Business Rules.

Modifying Rules Using JDeveloper

You can directly make the modifications to the configuration file available within OAACGRoleAssignSODCheck.zip.

Note

To perform this task, you must have the administrative privileges or the role of an Administrator.

---

1. Go to OIM_HOME/server/workflows/composites/ and extract the contents of OAACGRoleAssignSODCheck.zip to a directory.
2. Open the application in JDeveloper. You can see the routing rules in the ruleset `RemeditationRules` of the `ApprovalTaskRules.rules` file, where the following SOD related information is available for configuring the rules as part of the task payload element `oaacgResponse`.
   - hasIssues: Acceptable values are:
     - TRUE: Authorization issues exist but can be remedied
     - FALSE: No authorization issues
     - REJECT: Authorization issues exist but cannot be remedied; request has to be rejected
   - dimensions: List of dimensions and tags that are defined on the controls related to the authorization issues
   - requestedRoles: List of roles that are requested as part of this request
   - existingRoles: List of existing role memberships for the user
   - authIssues: List of Oracle Governance, Risk and Compliance Controls Incident IDs and the following additional details. This information is subsequently required to notify the approval decision.
     - ctrlPriority: Priority of the Oracle Applications Access Control Governor control that resulted in the authorization issue
     - ctrlName: Name of the SOD policy
     - userName: User profile to which the authorization issue belongs
     - roleName: Role associated with the authorization issue
     - sodStatus: Approval status of the request indicating whether the request is approved by Governance, Risk and Compliance Controls, or approved with conditions, or rejected
     - issuePath: Information about the entity on which the SOD policy is defined

After the rule modifications, update the following values in the OAACGRoleAssignSODCheck_cfgplan.xml configuration plan file.

Value	Description
`@oimT3URL`	The OIM server t3 URL
`@oimServerHost`	The OIM server host name
`@oimServerPort`	The OIM server port number

Thereafter, deploy the modified composite with this updated configuration plan file.

Troubleshooting Segregation of Duties for Role Provisioning: Procedures

The following scenarios may require troubleshooting measures to ensure successful completion of segregation of duties (SOD) checks and approval of role provisioning requests.

Failure of Role Assignment Request

The role assignment request fails and the request gets the Request Failed status. To troubleshoot this, do the following:

1. Sign in to the Identity Management domain in Enterprise Manager.
2. On the home page, under (Service Oriented Architecture), click **OAACGRoleAssignSODCheck** composite.
3. Under Recent Instances, click the latest instance and look for any error message or description of failure of request.
4. Check if the Application Access Controls Governor server information provided in Oracle Identity Manager is correct.
5. On the left pane, click IDM domain and from the context menu select System Mbean Browser.
6. Under Application Defined Mbeans, navigate to `oracle.iam` and select the OIM server and Application OIM.
7. Expand **XML Config - Config - XMLConfig.OAACGConfig** and select OAACGCOnfig.
8. Ensure that the attribute values used in Host, Port, DataSourceName, Service URL, and UserName are correct. To modify any incorrect information, on the Operations tab, click `updateOAACGConfigInformation` method, and provide the following parameters.

Parameter	Description
host	Application Access Controls Governor host name or IP address
port	Application Access Control Governor port
username	Admin username
password	Admin password

serviceURL	Application Access Control Governor service URL **Note** Ensure that there is a forward slash at the end of the URL. The URL must be in the format /grcc/services/GrccService/.
DatasourceName	Data source name of the Oracle Fusion connector that is configured in Application Access Control Governor

9. After saving the modifications, restart the Identity Management server.

Task Details Missing

If you do not find the task details of the assigned task, perform the following checks to troubleshoot.

1. Ensure that the taskflow is deployed on the SOA server.
   - Sign in to the Weblogic console.
   - On the left side, under the menu, click Deployments.
   - Ensure that TaskDetails application is deployed to SOA server and its state is Active.
2. Ensure that the predefined Admin user in Oracle Identity Management (OIM) is available in the Oracle Credential Store Framework (CSF), do the following:
   - Sign in to Identity Management domain in Enterprise Manager.
   - On the left pane, click Identity Management domain and from the context menu, select **Security** - **Credentials** .
   - Expand OIM and check for the key entry `sysadmin`.
   - Select the entry and click Edit to view the details.
   - Ensure that the user name is set to `xelsysadm`.

Note

If these steps do not help, refer to the generic troubleshooting tips associated with Oracle Identity Manager.

For generic information about troubleshooting OIM, see the Oracle Fusion Applications Administrator's Guide.

Configuring Oracle Data Integrator Studio

Configuring Oracle Data Integrator Studio for External Authentication: Explained

Configuring Oracle Data Integrator Studio for external authentication is necessary to prevent any unauthorized access. The access credentials are stored in a configuration file. To make the external configuration work, the jps configuration file (jps-config.xml) must be configured and placed in the prescribed directory where the application is installed.

Prerequisites

To be able to configure Oracle Data Integrator Studio, ensure that the following selections were made in the Oracle Data Integrator installation wizard:

- Developer Installation options on the Select Installation Type page:
  - **ODI Studio (with local agent)**
  - **ODI SDK**
- Skip Repository Configuration on the Repository Configuration page

Note

You must install Oracle Data Integrator Studio in a separate Oracle home other than Oracle Fusion Middleware Oracle homes and Oracle Fusion Applications Oracle home.

For more information on installing Oracle Data Integrator, see the Oracle Fusion Middleware Installation Guide for Oracle Data Integrator.

Configuration for ESS

In the <ODI_HOME>/oracledi/client/odi/bin directory, access the file odi.conf and update the parameter `AddVMOption -Doracle.odi.studio.ess=true`. This enables ESS configuration properties to be visible in Topology.

Configuration of jps-config.xml File

To configure external authentication for Oracle Data Integrator Studio, you need to configure the jps-config.xml file for Oracle Fusion Applications and place it in the appropriate directory on the computer where Oracle Fusion Applications is installed. The jps-config-jse.xml file is already provisioned for Oracle Fusion Applications, and is available in the <APPLTOP>/instance/domains/<server_name>/<domain name>/config/fmwconfig directory. The recommendation is to directly point to this file by providing complete path of the jps-config-jse.xml as the value for the parameter `AddVMOption -Doracle.security.jps.config=`, within the Oracle Data Integrator configuration file for Studio (odi.conf) in <ODI_HOME>/oracledi/client/odi/bin directory. Alternatively, copy the provisioned jps-config-jse.xml file along with the /bootstrap directory to the <ODI_HOME>/oracledi/client/odi/bin directory and rename the jps-config-jse.xml file to jps-config.xml. You may also need to copy any additional file that is referenced in the jps-config-jse.xml file for example, system-jazn-data.xml and default-keystore.jks.

Adding Additional Users as Oracle Data Integrator Supervisors

The Oracle Fusion Applications super user is the default supervisor for Oracle Data Integrator. However, it is recommended not to use that role for performing the administrative tasks within Oracle Data Integrator. Therefore, create additional users with supervisory access rights to Oracle Data Integrator.

Perform the following tasks while signed in as Oracle Fusion Applications super user.

1. In Lightweight Directory Access Protocol (LDAP), create a user without provisioning it with any role.
2. Sign in to Oracle Data Integrator Studio using Oracle Fusion Application super user, and create the same user that you created in LDAP.
3. In the Supervisor Access Privileges section, select the Supervisor check box to assign the role of Supervisor to that user.
4. In the **Retrieve GUID** field, reconcile the Globally Unique Identifier (GUID) for the user.

   The new user has a supervisory role in Oracle Data Integrator. The user can perform all functions of an Oracle Fusion Applications super user.

Installing Print Server

Installing Print Servers: Highlights

You must install print servers for external applications as part the implementation activity in Oracle Fusion Applications.

Note

This task is not applicable to Oracle Cloud implementations.

External Applications

Several external applications require specialized print servers. See the related product documentation for installing print servers for these applications.

- Oracle Business Intelligence Financial Reporting Studio and Financial Reporting Print Server.
- Primavera P6 Enterprise Project Portfolio Management.

- Informatica Identity Resolution. This product is associated with data quality as part of Oracle Fusion Trading Community Data Quality.

Configuring Presence Servers

Configuring Presence Servers: Explained

If you have an on-premise installation of Oracle Fusion Applications, you can optionally use Microsoft Office Communication Server (OCS) 2007 or Microsoft Live Communication Server (LCS) as the presence server. The setup involves creating external application connections, and instant messaging and presence connections, to OCS or LCS for each Oracle Fusion application.

Note

You also need to set up prerequisites for OCS or LCS. For more information on instant messaging and presence server prerequisites, see the Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal.

This table lists the Java EE applications that you can configure with OCS or LCS.

Product Family or Product	Java EE Application Name
Oracle Fusion Application Customer Relationship Management	• ContractManagementApp • CrmCommonApp • CrmPerformanceApp • CustomerApp • MarketingApp • OrderCaptureApp • SalesApp
Oracle Fusion Applications Human Capital Management	• HcmBenefitsApp • HcmCompensationApp • HcmCoreApp • HcmCoreSetupApp • HcmPayrollApp • HcmTalentApp
Oracle Fusion Applications Projects	ProjectFinancialsApp
Oracle Fusion Application Toolkit	HomePageApp

For each application, you execute the following commands against the appropriate domain:

- createExtAppConnection
- addExtAppField
- createIMPConnection

Important

Replace placeholder values enclosed within brackets (< >) with real values, for the appName, url, poolName, userDomain, and server fields.

- For the appName field, enter the Java EE application name, for example HcmBenefitsApp.
- The userDomain field is required only for the OCS connection and refers to the user domain associated with the OCS installation.
- For the server field, enter the managed server name on which the Java EE application is deployed. This field is optional if there is only one managed server for the application.

createExtAppConnection

Execute this command:

```
createExtAppConnection(appName='<JavaEEApp>', name='IMP_EXT_APP',
displayName='Presence Server Login Credentials')
```

The appName field is environment specific and requires you to enter a value.

addExtAppField

Execute this command:

```
addExtAppField(appName='<JavaEEApp>', name='IMP_EXT_APP',
fieldName='Account', fieldValue='', displayToUser=1)
```

The appName field is environment specific and requires you to enter a value.

createIMPConnection

If Oracle Fusion Applications is deployed in a high availability configuration, there may be multiple managed servers targeted for each Java EE application. You must run the createIMPConnection command for each application on each server, and specify the server in the server field.

If you are using the LCS adapter, then execute this command:

```
createIMPConnection(appName='<JavaEEApp>', name='presence',
adapter='LCS', url='<http://host:port/contextPath>',
appId='IMP_EXT_APP', poolName='<poolNameHere>', timeout=60, default=1,
server='<managedServerName>')
```

If you are using the OCS adapter, then execute this command:

```
createIMPConnection(appName='<JavaEEApp>', name='presence',
adapter='OCS2007', url='<http://host:port/contextPath>',
appId='IMP_EXT_APP', userDomain='<example.com>',
poolName='<poolNameHere>', timeout=60, default=1,
server='<managedServerName>')
```

These fields are environment specific and require you to enter a value:

- appName
- adapter (**OCS2007** or **LCS**)
- url
- poolName
- default (**1** or **0**)

Note

The connection will not be used unless this field is set to 1. If you use 0, then you essentially disable the connection.

- server

Setting Up a Secondary Oracle HTTP Server

Installing and Configuring a Secondary Oracle HTTP Server: Procedures

A secondary Oracle HTTP server needs to be added to the Oracle Fusion Application environment to effectively handle the load and improve the application performance.

Before you proceed with the installation of the secondary HTTP server, you need to ensure that the following prerequisites are met.

- Availability of a free slot to install the secondary HTTP server.

Note

Usually, the secondary HTTP server is installed on the same slot as the primary HTTP server. In such cases, the webgate used by the primary HTTP server can be used by the secondary HTTP server. However, if the secondary HTTP server is not installed on the same slot as the primary HTTP server, the webgate used by the primary HTTP server is not accessible by the secondary HTTP server. In that case, a separate webgate needs to be installed for the secondary HTTP server.

- Set up a directory structure similar to the directory structure of the primary HTTP server. The directory structure of the primary HTTP server is as follows.

```
First OHS mw home: /slot/ems5905/appmgr/APPTOP/webtier_mwhome
First OHS OH: webtier
First OHS instance dir: /slot/ems5905/appmgr/APPTOP/instance/
CommonDomain_webtier/
First OHS component name: ohs1
First OHS bin dir: /slot/ems5905/appmgr/APPTOP/instance/
CommonDomain_webtier/bin
First OHS config dir: /slot/ems5905/appmgr/APPTOP/instance/
CommonDomain_webtier/config/OHS/ohs1/moduleconf
```

  On the same lines, you can define a directory structure for the secondary HTTP server as shown here:

```
Second OHS mw home: /slot/ems5905/appmgr/APPTOP/webtier_mwhome2
Second OHS OH: webtier2
Second OHS instance dir: /slot/ems5905/appmgr/APPTOP/instance/
CommonDomain_webtier2
Second OHS component name: ohs2
```

Installing the Secondary Oracle HTTP Server

Follow these steps to install the secondary Oracle HTTP server.

1. Log on to the computer where the secondary Oracle HTTP server needs to be installed.
2. In the command line interface, change directory to the installer location: /net/adcnas421/export/fainteg_repos/ FAINTEG_11.1.1.5.1_PLATFORMS_110812.0749/installers/webtier/Disk1
3. Enter the command `./runInstaller`. The Installation wizard appears, displaying the Specify Inventory Directory screen.
4. Click **OK**. The Inventory Location Confirmation dialog box appears.
5. Select the **Continue Installation with Local Inventory** check box and click **OK**.
6. On the Welcome screen, click **Next**.
7. Select **Install and Configure** and proceed to the next screen.
8. On the Prerequisites screen, verify if all the prerequisites are met and click **Next**.
9. On the Specify Installation Locations screen, provide details to create the **Oracle Home** and **Oracle Middleware Home** directories, and click **Next**. The Configure Components screen appears.
10. Select the **Oracle HTTP Server** check box and click **Next**. The Specify Component Details screen appears.
11. Provide the **Instance Home Location**, **Instance Name** , and **OHS Component Name** and click **Next**.
12. On the Configure Ports screen, select the **Auto Port Configuration** check box and click **Next**.
13. On the Specify Security Updates page, clear the check box **I wish to receive security update** and click **Next**. A confirmation dialog box with

the message **Do you wish to remain uninformed of critical security updates?** appears.

14. Click **Yes**.
15. On the Installation Summary page, review the information and click **Install**.
16. Click **Finish** after the installation is complete.

Installing the Webtier Patch

Before you proceed with the installation, ensure that you shut down the secondary Oracle HTTP server using the following commands in the given order:

1. `cd to /slot/ems5905/appmgr/APPTOP/instance/CommonDomain_webtier2/bin`
2. `./opmnctl stopall`

Follow these steps to install the Webtier patch.

1. In the command line interface, changed directory to the installer location: `/net/adcnas421/export/fainteg_repos/FAINTEG_11.1.1.5.1_PLATFORMS_110812.0749/installers/webtier_patchset/Disk1`
2. Enter the command `./runInstaller`. The Installation wizard appears.
3. On the Inventory page, specify **Local Inventory**. This location should be the same as the one used during the secondary Oracle HTTP server installation.
4. On the Welcome page, click Next.
5. Provide the same **Oracle Home** and **Oracle Middleware Home** directory names used for installing Oracle HTTP server, and click **Next**.
6. On the Security Updates page, click **Next**.
7. On the Installation Summary page, review the information and click **Install**.

Configuring the Secondary Oracle HTTP Server

Follow these steps to configure the secondary Oracle HTTP server.

1. In the command line interface, use the `diff` command to check differences between the httpd.conf file of the primary HTTP server and the httpd.conf file of the secondary HTTP server. Except the server name, everything else must be the same between the two servers.
2. Copy the webgate related configuration from the httpd.conf of the primary HTTP server to the httpd.conf of the secondary HTTP server.
3. Copy all the .conf files from the **config** - **moduleconf** directory of the primary HTTP server to the **config** - **moduleconf** of the secondary HTTP server.
4. Within the .conf files inside the moduleconf, replace the references to the hostname of the primary HTTP server with the hostname of the secondary HTTP server. The references should be changed as per the following directives:

a. Listen adcdai02.us.oracle.com:xxxxx

b. <VirtualHost adcdai02.us.oracle.com:xxxxx >

Caution

While making changes to the hostname, please do not make a global change because WebLogic servers in the same host as the primary HTTP server might be referred in context roots and that might get changed.

5. Preferably, shut down the primary HTTP server and then start the secondary HTTP server. Ensure that there are no problems with the startup. You can then try to access the BIG/IP URLs.
6. Sign into the custom provisioning tool and ensure that all the HTTP server custom provisioning is completed in both the HTTP servers.
7. Add the secondary HTTP server information to the Admin server and update the start/stop script at $HOME/scripts/efops/start(stop)_webtier_2nd.sh.

For more information about configuring the Oracle HTTP server, refer to the Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server. You can also refer to the section Scaling Out Oracle HTTP Server in the Oracle Fusion Applications Enterprise Deployment Guide.

Setting Up Oracle ADF Desktop Integration

Deploying Oracle ADF Desktop Integration Client: Procedures

Oracle Application Development Framework (Oracle ADF) Desktop Integration is part of Oracle ADF and enables desktop integration with Microsoft Excel workbooks. Users can manage large volumes of data from web applications using Excel, for example to create journals, load currency rates, or create expense entries. To enable the integration of Oracle ADF with Microsoft Excel workbook, you need to make the Oracle ADF Desktop Integration add-in available on each client where Microsoft Excel is installed.

Note

This task is not applicable to Oracle Cloud implementations.

As Oracle ADF Desktop Integration is an add-in to Microsoft Office products, ensure that all the system requirements are fulfilled. For more information, refer to http://www.oracle.com/technetwork/developer-tools/jdev/index-091111.html#Desktop_Clients.

Note

- Ensure that the version installed on the client is same as that installed on the server. For information on verifying whether your Oracle Fusion web application supports desktop integration or not, see the Oracle Fusion Middleware Desktop Integration Developer's Guide for Oracle Application Development Framework.
- The Oracle ADF Desktop Integration Client must be installed as the user and not as the administrator. However, Microsoft prerequisites for Oracle ADF Desktop Integration Client require administrator privileges. Therefore, you must provide administrator privileges to the user before you install the Oracle ADF Desktop Integration Client. Alternatively, you can install prerequisites as the administrator and Oracle ADF Desktop Integration Client as the regular user. For more information on prerequisites, see the Oracle Fusion Middleware Desktop Integration Developer's Guide for Oracle Application Development Framework.

To install the client version of the add-in, you must first deploy it at one of the following locations:

- Web server
- Shared network location

After these tasks are performed, you must inform users about the link they can use to download and install the client.

Deploying Oracle ADF Desktop Integration Client on a Web Server

You can deploy the Oracle ADF Desktop Integration Client on a web server that is accessible to the end users from their respective computers running on Microsoft Windows. Ensure that the web server is always up and running. Otherwise, the integration fails when end users access the desktop integrated workbook.

1. Create a folder in $APPLTOP/fusionapps/applications/desktop_installer.
2. From the /u01/APPLTOP/fusionapps/oracle_common/modules/oracle.adf.desktopintegration_11.1.1 location, copy the adfdi-excel-runtime-client-installer.zip file and place it on the local computer.
3. Extract the contents of the zip file to a folder and ensure that setup.exe is present among the contents.
4. Using Windows Command Prompt, navigate to the folder path where you extracted the zip file.
5. Modify the URL property of the setup.exe file to assign the final URL or full path to the installer, as shown here:setup.exe/url="https://<web server url>:<port number>/homePage/desktop_installer/<name of folder created in step 1>/adfdi-excel-runtime-client-installer"

Note

Replace the variables indicated within <> with actual values.

6. While remaining in the same folder location in Windows Command Prompt, verify the URL assigned to the setup.exe, as shown here:

```
setup.exe/url
```

   A dialog box appears displaying the full path.

7. In Windows Explorer, zip the same folder that contains the modified setup.exe and copy it to folder created in $APPLTOP/fusionapps/applications/desktop_installer.
8. Extract the contents of the zip file.
9. Bounce the Home Page of the managed server in Common Domain so that users can access the setup.exe directly using the following URL:https://<web server url>:<port number>/homePage/desktop_installer/<name of folder created in step 1>/adfdi-excel-runtime-client-installer/setup.exe
10. Uninstall any existing version of Oracle ADF Desktop Integration client from the end user computers.
11. Access the URL to install the Oracle ADF Desktop Integration client on the end user computers.

Tip

After you place the Oracle ADF Desktop Integration Client on the web server, it is recommended that you use the Manage Menu Customizations task in the Setup and Maintenance work area of Oracle Fusion Applications to establish a link to the web server and install the client on the end user computer.

1. Sign in to Oracle Fusion Applications.
2. From the menu bar, select **Administration** - **Setup and Maintenance** .
3. Navigate to the task Manage Menu Customizations. The Manage Menu Customizations page appears.
4. Select the Tools folder and on the menu select **Actions** - **Insert Item Child** . The Create Item Node dialog box appears.
5. Enter a name in the Label field. For example, Download Oracle ADF Desktop Integration Runtime client.
6. In the Destination field, enter the URL of the setup.exe as shown here:

   #{EndPointProvider.externalEndpointByModuleShortName['HomePage']}/desktop_installer/<new folder created under desktop_installer>/adfdi-excel-runtime-client-installer/setup.exe
7. Click **Save**. The custom navigator link for Oracle ADF Desktop Installer appears under **Navigator** - **Tools** menu of Oracle Fusion Applications.

   Users can use this link to download or directly run the setup.exe to install the Oracle ADF Desktop Integration Client on their computers.

For more information on customizing the navigator menu by using the Manage Menu Customizations task, refer to the Oracle Fusion Applications Extensibility Guide.

Important

Whenever a new version of the Oracle ADF Desktop Integration Client is available for upgrade, you need to consider the following to keep the client up-to-date:

- Repeat steps 2 to 8 to overwrite the existing installer content in the adfdi-excel-runtime-client-installer folder.
- Whenever a new version of the Oracle ADF Desktop Integration Client is available at the web server location, it automatically checks for any updates to Microsoft Excel and prompts the end users to download and upgrade. To make this happen without any disruption, you need to ensure that the associated web server hosting the Oracle ADF Desktop Integration Client is always up and running.
- If there is a change in the web server location or the web server URL or the port number, end users will need to uninstall the ADF Desktop Integration Client and reinstall it as the links responsible for communicating automatic upgrades would have been broken.
- At step 7, users may encounter "The Publisher is not verified" warning message when running the downloaded setup.exe directly in Internet Explorer. The warning is prompted because the digital signature on the setup.exe file has been invalidated when you modify the URL property. This invalid signature warning does not prevent users from installing the client successfully. To avoid this warning, you need to sign the setup.exe file again with a valid certificate after modifying the URL property.

Deploying Oracle ADF Desktop Integration Client on a Shared Network Location

You can deploy the Oracle ADF Desktop Integration Client on a shared network location that is accessible to the end users from their respective computers running on Microsoft Windows.

1. Identify a shared network location where you plan to host the Oracle ADF Desktop Integration Client.
2. From the /u01/APPLTOP/fusionapps/oracle_common/modules/oracle.adf.desktopintegration_11.1.1 location, copy the adfdi-excel-runtime-client-installer.zip file and place it in a folder at the shared location.
3. Extract the contents of the zip file to the same folder.
4. Uninstall any existing version of Oracle ADF Desktop Integration client from the end user computers.
5. From the end user computer, access the shared folder and run the setup.exe to install the Oracle ADF Desktop Integration client on that computer.

Important

Whenever a new version of the Oracle ADF Desktop Integration Client is available for upgrade, you need to consider the following to keep the client up-to-date:

- Overwrite the existing installer content in the shared folder on the network.
- Whenever a new version of the Oracle ADF Desktop Integration Client is available at the shared location on the network, Microsoft Excel automatically checks for any updates and prompts the end users to upgrade. To make this happen without any disruption, you need to ensure that the network connectivity is always up.
- If there is a change in the shared location, end users will need to uninstall the Oracle ADF Desktop Integration Client and reinstall it from its new location as the links responsible for communicating automatic upgrades would have been broken.

Health Checking and Troubleshooting

Setting Up Health Checking and Troubleshooting: Highlights

The infrastructure for health checking and troubleshooting Oracle Fusion applications is provided along with provisioning. However, before beginning any production activity on Oracle Fusion applications, perform the following configuration tasks.

Note

This task is not applicable to Oracle Cloud implementations.

Health Checking and Diagnostic Tasks

- Only after ensuring the completeness of the following configuration, you can perform health checking and troubleshooting for Oracle Fusion applications using log files, incidents, diagnostic tests and so on. Refer to the Oracle Fusion Applications Administrator's Guide.

  See: Managing Oracle Fusion Applications Log Files and Diagnostic Tests

  See: Troubleshooting Oracle Fusion Applications Using Incidents, Logs, QuickTrace, and Diagnostic Tests

Configuration Tasks

The configuration tasks are described in the Oracle Fusion Applications Administrator's Guide unless otherwise specified.

- Enable viewing of logs generated by C and PL/SQL.

See: Configuring Access to Logs for Oracle Enterprise Manager Fusion Applications Control

- Configure log file rotation.

  See: Managing Log File Size and Disk Space Usage

- Review default logging profile options and adjust values for your specific requirements.

  See: Using Profile Options to Configure Standard Log Settings

- Review and adjust your QuickTrace settings.

  See: Default System Settings for Incident Creation and QuickTrace

- Configure user access to diagnostic testing functionality.

  See: Controlling Access to Diagnostic Testing Functionality

- Configure a job role for future user access to troubleshooting options.

  See: Assisting Users in Gathering Data Using Troubleshooting Options

- To benefit from the health checking, patching recommendations, and configuration services offered by My Oracle Support, install and configure Oracle Configuration Manager. For more information, see Install Configuration Manager on My Oracle Support at https://support.oracle.com.

- To use the latest troubleshooting features, including a purpose built Oracle Fusion Applications module, provided by Remote Diagnostic Agent (RDA), install and configure RDA. For more information, see RDA Documentation on My Oracle Support at https://support.oracle.com.

3

Customer Relationship Management

Setting Up E-Mail Marketing

Installing the Bounce Handling Daemon: Procedures

The E-Mail Marketing Server is a combination of components designed to support high volume, personalized e-mail messages, and to track e-mail bounces and click-through responses. The bounce handling daemon (BHD) tracks e-mail messages that cannot be delivered, parses the returned e-mail messages, and records the cause of the e-mail bounce.

Installing and Configuring the Bounce Handling Daemon

The bounce handling daemon installation program is available on the Fusion Applications companion disk. Prior to installing the program, ensure you have provisioned the Marketing application, noting the SOA host and port, and determined the designated server to place the daemon. The designated server must have port 25 available.

Note

It is recommended that you place the bounce handling daemon in the DMZ. Optionally, you can place the bounce handling daemon behind an inbound mail transfer agent (MTA). The approach that you choose depends on the configuration of your network, DMZ, existing inbound mail transfer agent, and firewall.

Complete the following steps to install and configure the bounce handling daemon:

1. Using the companion disk, locate and run the installation program: `fusionbhd/Disk1/runInstaller`. Provide information when prompted, such as the JDK location, designated BHD server installation directory, and the http or https protocol, host and port for the Marketing SOA URL.

2. Navigate to the `WLS_HOME/config/fwmconfig` directory and copy the files and directory listed below to the `$HOME/bhd/fusionapps/crm/ewm/bhd/bin` directory.
   - jps-config-jse.xml
   - default-keystore.jks
   - bootstrap directory (including the cwallet.sso)

3. Update the root user permissions to allow read, write, and execute access to the jps-config-jse.xml and default-keystore.jks files and the bootstrap directory.
4. Update the root user permissions to allow read, write, and execute access to the BHD server installation directory, it's subdirectories and files. The top level BHD server installation directory is specified during the install process.
5. Grant read access to the fusionapps/crm/ewm/bhd/logs directory to nonroot users to provide availability to application log files.
6. Sign in as a root user and enter the following to start the BHD service for port 25:

Server Platform	Action
UNIX	Navigate to the fusionapps/crm/ewm/bhd directory and enter the following command: • `$ ./bin/bhd-onpremise-ctl.sh start`
MS Windows	Run the bhd.exe executable file.

For more information on provisioning, see the Oracle Fusion Applications Quick Installation Guide. For more information on configuring other aspects of the e-mail server for marketing, see the Oracle Fusion Applications Marketing Implementation Guide.

Setting Up SMS Marketing

Enabling SMS Marketing Capability: Procedures

To use the SMS marketing campaign capability within Oracle Fusion Customer Relationship Management, you need to enable it after installing Oracle Fusion Applications. Customers interested in SMS marketing campaigns will need to complete SMPP Driver configuration in the SOA suite component Oracle User Messaging Service.

An instance of the SMPP driver is already installed as part of the Oracle Fusion Applications installation and is a part of the Oracle User Messaging Service, but it does not point to any User Messaging Server. To configure the SMPP driver, you need to have an account with an SMPP driver gateway vendor. For configuration instructions and the list of verified/approved 3rd party SMPP driver gateway vendors, refer the Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite on My Oracle Support.

Important

Before proceeding with the enabling process, ensure that you have access rights to update and deploy applications on the WebLogic Administration Console and Oracle Enterprise Manager associated with the Customer Relationship Management domain.

1. Sign in to the WebLogic Administration Console associated with the Customer Relationship domain.
2. Under Deployments, you see the application **usermessagingdriver-smpp** in the **Installed** state.
3. Expand **usermessagingdriver-smpp** and navigate to Targets tab. The Current Targets column shows (None specified), indicating that no target is configured.
4. On the console, switch to the Lock and Edit mode, update the target to all servers in the CRM_SOACluster, and save the changes.
5. While remaining in the Lock and Edit mode for the console, navigate to Deployments, select the check box next to **usermessagingdriver-smpp** and click Update. The Update Application Assistant wizard appears.
6. For the **Deployment Plan Path** field, click **Change Path** and select the Fusion Applications specific deployment plan APPTOP/instance/applications/ums/crm/usermessagingdriver-smpp_FusionPlan.xml.
7. Proceed to the subsequent screen of the Update Application Assistant wizard and select **Release Configuration** to commit the changes made until this point. The state of the application **usermessagingdriver-smpp** changes to **Active**.
8. Sign out of WebLogic Administration Console.
9. Sign in to the Oracle Enterprise Manager associated with the Customer Relationship Management domain.
10. Expand **CRMDomain** - **User Messaging Service** , right-click the application **usermessagingdriver-smpp** and select **SMPP Driver Properties** from the context menu.
11. Configure the driver and apply the changes.
12. Restart the application **usermessagingdriver-smpp** to bring into effect the driver configuration changes.

You can now use the SMS Marketing capability of Oracle Fusion Customer Relationship Management.

Setting Up Implicit Personalization Behavior

Post-Deployment Steps for Implicit Personalization Behavior: Procedure

This topic covers the post-deployment activities required for Oracle Fusion CRM applications that support implicit personalization behavior.

Performing these activities fixes the inconsistent implicit personalization behavior between sessions in the following Oracle Fusion CRM applications:

- Oracle Fusion CRM Common
- Oracle Fusion Territory Management
- Oracle Fusion Customer Center
- Oracle Fusion Marketing

- Oracle Fusion Order Capture Common Components
- Oracle Fusion Sales

Post-Deployment Activities

Make the following changes to the adf-config.xml file as a post-deployment activity.

Note

These steps are applicable only for the Oracle Fusion CRM applications where implicit personalization behavior is supported.

1. Shutdown the domain where the application is deployed.
2. Search for adf-config.xml file. For example, for Sales application, this file is typically located at `Sales <deploy directory>/SalesApp/V2.0/app/SalesApp/adf/META-INF/adf-config.xml`
3. Back up adf-config.xml file.
4. Open adf-config.xml file in a text editor and comment out all occurrences of the tag `<adf-faces-config>` under the root node `<adf-config>. . .</adf-config>`. For example:

```
<!-- adf-faces-config xmlns="http://xmlns.oracle.com/adf/faces/
config">. . . </adf-faces-config -->
```

5. Add the following after the commented section.

```
<adf-faces-config xmlns="http://xmlns.oracle.com/adf/faces/config">

 <persistent-change-manager>
 <persistent-change-manager-
class>oracle.adf.view.rich.change.MDSDocumentChangeManager</persistent-
change-manager-class>

 </persistent-change-manager>

 <taglib-config>
 <taglib uri="http://xmlns.oracle.com/adf/pageeditor">
 <tag name="layoutCustomizable">
 <!-- Added to pass JAudit-->
 <attribute name="layout">
 <persist-changes>true</persist-changes>
 </attribute>
 </tag>
 </taglib>

 <taglib uri="http://xmlns.oracle.com/adf/faces/customizable">
 <tag name="showDetailFrame">
 <persist-operations>all</persist-operations>
 <!-- Added to pass JAudit-->
 <attribute name="disclosed">
 <persist-changes>true</persist-changes>
 </attribute>
 <attribute name="height">
 <persist-changes>true</persist-changes>
 </attribute>
 </tag>

 <!-- Added to pass JAudit-->
 <tag name="portlet">
 <attribute name="disclosed">
 <persist-changes>true</persist-changes>
 </attribute>
 <attribute name="height">
 <persist-changes>true</persist-changes>
 </attribute>
 </tag>
 </taglib>


 <taglib uri="http://xmlns.oracle.com/adf/faces/rich">
 <tag name="column">
 <persist-operations>all</persist-operations>
 <attribute name="displayIndex">
 <persist-changes>true</persist-changes>
 </attribute>
 <attribute name="visible">
 <persist-changes>true</persist-changes>
 </attribute>

 <attribute name="width">
 <persist-changes>true</persist-changes>
 </attribute>
 </tag>
 </taglib>
 </taglib-config>
</adf-faces-config>
```

6. Specifically for Customer Center application, and as an additional step, locate these lines under the `<mds:cust-config>` section:

```
<mds:match path="/oracle/apps/">
 <mds:customization-class
 name="oracle.apps.fnd.applcore.customization.ProductFamilyCC"/>
 <mds:customization-class
 name="oracle.apps.fnd.applcore.customization.SiteCC"/>
</mds:match>
```

   When you comment the lines, they appear as:

```
<!--mds:match path="/oracle/apps/">
 <mds:customization-class
 name="oracle.apps.fnd.applcore.customization.ProductFamilyCC"/>
 <mds:customization-class
 name="oracle.apps.fnd.applcore.customization.SiteCC"/>
</mds:match>
```

7. Save and close the file
8. Start up the domain that hosts the Oracle Fusion CRM application

Setting Up Web Services Security

Setting Up Web Services Security for On-Premises Implementation of Oracle Fusion CRM: Procedures

This topic covers configurations that you must perform to enable a CRM user call an external, secured Web service. You perform these configurations differently for each security scheme based on the details that a CRM user provides in a service request (SR).

Configuration Required for Security Schemes

This table covers the configurations you perform for each security scheme.

Security Scheme	Configuration Required
Secure Sockets Layer (SSL) Security	A CRM user typically includes the following information in the SR: • WSDL location that the CRM user is trying to access. • SSL error details that the CRM user is encountering. • SSL certificate that the CRM user obtained from the service provider. Perform the following steps to resolve SSL errors: 1. Import the SSL certificate into Oracle CRM trust store using either WebLogic Scripting Tool (WLST) or Fusion Middleware Control. For more information about importing a certificate, see "Importing a Certificate or Trusted Certificate into a Keystore Using WLST" or "Importing a Certificate or Trusted Certificate into a Keystore Using Fusion Middleware Control" section, as applicable, in Oracle Fusion Middleware Administrator's Guide on Oracle Technology Network, at http://www.oracle.com/technetwork/indexes/documentation/index.html. 2. Update the service request. When you update the SR, a notification is sent to the CRM user.

Message Protection Security	A CRM user typically includes the following information in the SR: - WSDL location that the CRM user is trying to access. - Error details that the CRM user is encountering. - The server encryption certificate and the issuer certificate that the CRM user obtained from the service provider. Perform the following steps to resolve message protection errors: 1. Locate the path to the Java Key Store (JKS). This is where the Oracle Fusion Application's keystore is located. To locate JKS: 1. Sign in to Oracle Enterprise Manager as an administrator. 2. In the navigation pane, locate your component instance. 3. Click on your component_name at the top. 4. Select **Security**, and then select **Security Provider Configuration.** 5. On the Security Provider Configuration page and under the Web Services Manager Authentication Providers heading, expand the **Keystore** region. 6. Note the **Path** of JKS. You specify this location when importing certificates. For more information on how to use Oracle Enterprise Manager Fusion Middleware Control to configure the Oracle Web Services Manager (WSM) keystore, see "Configuring the Oracle WSM Keystore" in the Oracle Fusion Middleware Security and Administrator's Guide for Web Services on Oracle Technology Network, at http://www.oracle.com/technetwork/indexes/documentation/index.html. 2. Import the server encryption certificate into Oracle CRM keystore using the **keytool** utility and specify an alias, for example serverenckey, for the server encryption certificate. You specify this alias in your response to the SR. For information on the keytool utility, see "Tools and Utilities for Creating Keystores and Loading Private Keys and Certificates" in Oracle Fusion Middleware Securing Oracle WebLogic Server guide on Oracle Technology Network, at http://www.oracle.com/technetwork/indexes/documentation/index.html. 3. Import the issuer certificate into Oracle CRM keystore using the **keytool** utility and specify any alias. 4. Provide the server encryption key alias, for example serverenckey, in your response to the SR. **Note** The CRM user enters the server encryption key alias in the **Outgoing Encryption Key** field. 5. Update the SR.

4

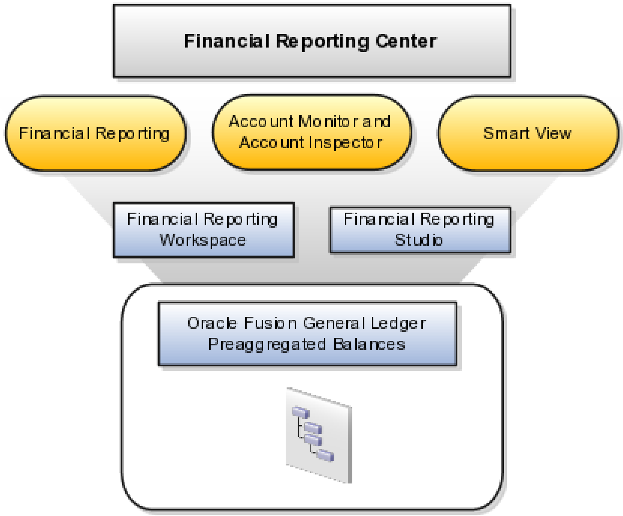
Financials

Setting Up Financial Reporting Center

Financial Reporting Center: How It Works

The Oracle Fusion Financial Reporting Center provides functionality for reporting on Oracle Fusion General Ledger balances. It provides secure, self-service access to reports that use real time account information.

You can design traditional financial report formats such as balance sheets, profit and loss statements, and cash flow reports. You can also design nontraditional formats for financial or analytic data that include text and graphics.


Financial Reporting Center
Financial Reporting
Account Monitor and Account Inspector
Smart View
Financial Reporting Workspace
Financial Reporting Studio
Oracle Fusion General Ledger Preaggregated Balances

Components

Financial Reporting Center is comprised of numerous components:

- **Financial Reporting:** Financial users and analysts access live reports and books or published snapshot reports and books from previously scheduled batches in a variety of formats. Other functionality includes:
  - Refreshing report data using runtime points of view or parameters
  - Drill through capability from parents to other parents
  - Drill down to detail balances, journal lines, and subledger transactions.
- **Oracle Hyperion Smart View:** Financial analysts view, import, manipulate, distribute, and share data from your Oracle Fusion General Ledger balances in Microsoft Excel.
- **Account Monitor and Account Inspector:** Financial analysts monitor and track key account balances in real time at every level of your dimensions and hierarchies. These tools provide multidimensional account analysis and drill down capability.
- **Workspace:** Reporting administrators create, open, save, and delete folders and store report objects, reports, and snapshot reports.
- **Oracle Hyperion Financial Reporting Studio:** Report authors use an object-oriented graphical report layout with report objects, such as text boxes, grids, images, and charts, to design reports.

Setting Up Your Financial Reporting Center: Critical Choices

Oracle Fusion Financial Reporting Center is a powerful tool for accessing, designing, and presenting financial reports and analytic data. The critical choices required to configure and install the components in Financial Reporting Center consist of:

- Configuring Financial Reporting Center
- Installing and configuring Financial Reporting Studio, performed by your end users.
- Installing Smart View, performed by your end user.
- Configuring Workspace Database Connection, performed by your administrator.
- Configuring Oracle Fusion Transactional BI Dimensions

Configuring Financial Reporting Center

You have access to the reports through the folder structure in the Financial Reporting Center and Workspace installed with Oracle Fusion Financial Applications. Your Oracle Fusion Business Intelligence (BI) administrator defines the folder structure in Workspace considering your company's security requirements for folders and reports, as well as report distribution requirements for financial reporting batches. Security can be set on folders and reports from Workspace. You are granted access to the folders and reports you want to view by your BI administrator.

Installing and Configuring Financial Reporting Studio

Oracle Hyperion Financial Reporting Studio is client-based software. If you access Oracle Fusion Applications from Oracle Cloud, you connect to the Financial Reporting Studio through a Windows Remote Desktop Connection.

Otherwise, report authors download the installation files for Financial Reporting Studio from Workspace by clicking **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting.** Once Workspace is launched, click **Tools > Install > Financial Reporting Studio**. After performing the prerequisites and completing the installation, launch the Financial Reporting Studio. Provide your user ID, password, and the Server URL. Derive the Server URL information by following the steps:

1. Open **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting** .
2. Edit the **Workspace URL** and remove workspace/index.jsp.
3. Following are two examples of Server URLs:
   - If the Workspace URL is https://fusionsystemtest-p-external-bi.us.oracle.com/workspace/index.jsp, the Server URL is https://fusionsystemtest-p-external-bi.us.oracle.com.
   - If the Workspace URL is https://fusionsystemtest-p-external-bi.us.oracle.com:10622/workspace/index.jsp, the Server URL is https://fusionsystemtest-p-external-bi.us.oracle.com:10622.
4. Copy the modified URL to the Server URL field.

Note

For end users installing the Oracle Fusion Financials Reporting Studio, the installer launches a separate console window that continues to run for a brief time after the installation completes the setup tasks. The process is normal, expected, and applies to Oracle Hyperion Reporting Studio installations in both the Oracle Fusion Applications and Enterprise Performance Manager modes.

Note

You must save a new report before attempting to preview it with Web Preview.

Prerequisites needed for installing the Financial Reporting Studio are:

1. Financial Reporting Studio Client Certifications that are found at: http://www.oracle.com/technetwork/middleware/bi-foundation/hyperion-supported-platforms-085957.html
2. Microsoft Office installed on your end-users computers.

Note

For more information, see:

- Oracle Enterprise Performance Management System Installation and Configuration Guide

- Oracle Hyperion Enterprise Performance Management System EPM System Standard Deployment Guide

Installing Smart View

Smart View is an Excel add-in that must be loaded to each client. To download the installation files from Workspace click the **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting**. Once the **Workspace** is launched, click on **Tools > Install > Smart View.** Alternatively, download Smart View from http://www.oracle.com/technetwork/middleware/epm/downloads/smart-view-1112x-1594693.html.

Note

Since Smart View is an add-in to Microsoft Office products, you can install Smart View only on a Windows operating system.

Once Smart View is installed, it must be configured to connect to Oracle Fusion Applications. This is done using the Smart View Shared Connections URL. You can derive the **Shared Connections URL** by following the steps below:

1. **Open Workspace for Financial Reporting** from the **Financial Reporting Center task panel**.
2. Edit the **Workspace URL**, for example, if the **Workspace URL** is https://fusionsystemtest-p-external-bi.us.oracle.com/workspace/index.jsp. Remove index.jsp and add SmartViewProviders at the end of the URL.

Note

This is another example for a Cloud based environment: If the Workspace URL is https://efops-rel5st4-cdrm-external-bi.us.oracle.com:10622/workspace/index.jsp, the Shared Connections URL is https://efops-rel5st4-cdrm-external-bi.us.oracle.com:10622/workspace/SmartViewProviders.

3. Copy the URL.
4. Launch Excel.
5. Navigate to the **Smart View** menu **> Options > Advanced**.
6. Paste the URL in the **Shared Connections URL** field.
7. Click on the **OK** button.

For more information on configuring Smart View client for users, see Oracle Hyperion Smart View for Office User's Guide for Oracle Hyperion Smart View.

To connect Oracle Fusion General Ledger Balances cubes in Smart View:

1. Open Smart View from your **Start menu > Programs > Microsoft Office > Microsoft Excel 2007.**
2. Go to the **Smart View** menu > **Open**, in the **Start** on the ribbon > click on **Smart View Panel** that appears in the drop down box under the ribbon. This launches a task pane.
3. Click on the **Shared Connections** button on the task pane.

4. Sign in with your user name and password.
5. Click on the **Select Server to proceed** drop down.

Note

If the Essbase Server is not there, then it has to be added. Use the following steps:

a. Click on the Add Essbase Server link on the bottom of the spreadsheet.
b. Specify the Essbase Server login and password.
c. Expand the Essbase sever and locate the cube under it.

6. Select **Oracle Essbase** from the list of shared connections.
7. Click the **Expand** to expand the list of cubes.
8. Expand your cube (name of your chart of accounts).
9. Click on **db.** A list of functions appears on the bottom of the panel.
10. Click the **Ad hoc analysis.**

Note

You need to perform these steps only once for a new server and database.

To set how the name and alias of the Essbase database appears:

1. Click on the **Options** on the ribbon > select the **Member Options** > select **Member Name Display.**
2. Set one of these three options:
   - **Distinct Member Name:** Only shows the full Essbase distinct path.
   - **Member Name and Alias**: Shows both the member name and the alias.
   - **Member Name Only:** Shows only the member name.

Note

The Smart Slice feature is not supported in Oracle Fusion General Ledger. For all other documentation, refer to the Oracle Hyperion Smart View for Office User's Guide for Oracle Hyperion Smart View.

Configuring Workspace Database Connections

Administrators need to create database connections from Workspace so users can access the cubes from Workspace and Financial Reporting Studio.

Note

Ledger setup has to be completed before the database connection can be created. Oracle Fusion General Ledger balances cubes are created as part of ledger setup. There is a separate cube for each combination of chart of accounts and accounting calendar. A database connection is needed for each cube.

Steps to define a database connection are:

1. Start at the **Navigator** by selecting **Financial Reporting Center.**
2. From the **Financial Reporting Center** task panel select **Open Workspace for Financial Reporting.**
3. From within **Workspace** select the **Navigator** menu > **BI Catalog.**
4. Select **Tools** menu **> Database Connection Manager.**
5. Select **New** button.
6. Enter a user friendly name for the **Database Connection Name.**
7. Enter Essbase as the **Type**, your server, user name, and password.
8. Select **Application** (cube) and **Database** from the list of values. Expand the **Application** name to see the related **Database**, for example, db.
9. Click the **OK** button twice to save your selections.
10. Click **Close** button in the **Database Connection Manager** window to save your connection.

For more information on configuring Essbase database connections in Workspace see: **Oracle Essbase Database Administrator's Guide for Oracle Essbase.**

Note

The database connection is available in both Workspace and Financial Reporting Studio. Optionally, it can be setup in Financial Reporting Studio when putting grids on a report. This should only be done by an administrator.

Configuring Oracle Fusion Transactional BI Dimensions

Within Oracle Fusion Transactional Business Intelligence (BI), Accounting Segment Dimensions such as Balancing segment or Cost Center segment are based on the Chart of Accounts configuration. These segments can be configured to be tree-enabled, which means that hierarchies are defined upon the segment values for rollup purposes. In such scenarios, you must filter by a specific hierarchy when performing ad-hoc queries against tree-based accounting segments. Incorrect results may occur if tree filters are not applied. To apply tree filters, create a filter condition on Tree Filter attributes in Accounting Segment Dimensions.

Note

For information on setting up General Ledger accounting segments, see the Oracle Fusion Transactional Business Intelligence Administrator's Guide.

Setting Up Oracle Document Capture and Oracle Forms Recognition

Installing Oracle Document Capture and Oracle Forms Recognition: Overview

Oracle Fusion Financials uses Oracle Document Capture to import payables invoice and expense receipt images from various sources including scanners, e-mail, and FTP sites. Oracle Fusion Payables also leverages Oracle Forms Recognition for intelligent data recognition for invoice entry.

Note

This task is not applicable to Oracle Cloud implementations.

If you plan to implement Oracle Fusion Expenses and use automated receipt image processing, then you must set up Document Capture and configure it for expenses. If you have licensed Oracle Fusion Automated Invoice Processing, then you must set up Forms Recognition in addition to Document Capture, and configure both for payables.

To set up Document Capture and Forms Recognition, perform these steps in the specified order:

1. Configure Document Capture and Forms Recognition network shares
2. Install and configure Document Capture and Forms Recognition on Windows desktop

Note

For details regarding users and privileges for the setup, refer to the installation guides of Oracle Document Capture and Oracle Forms Recognition.

Configuring the Oracle Imaging and Process Management Input Directory Network Share: Procedures

Oracle Document Capture and Oracle Forms Recognition save images to the Oracle Imaging and Process Management input directory for further processing. Since Document Capture and Forms Recognition are Windows-based products, you need to configure the input directory as a network shared directory so that Document Capture and Forms Recognition can save images to this location.

Note

This task is not applicable to Oracle Cloud implementations.

To install network sharing for Oracle Document Capture and Oracle Forms Recognition:

1. Verify the Oracle Imaging and Process Management input directory path

2. Configure the network share for the Imaging and Process Management input directory
3. Verify Oracle Imaging and Process Management Input Agent
4. Configure the Windows mapped network drive for the input directory

1. Verify the Oracle Imaging and Process Management Input Directory Path

To verify the input directory path:

1. Sign in to the Enterprise Manager on the Common Domain, as an Administrator.
2. Navigate to the Domain level.
3. Select **System MBean Browser**.
4. Open the oracle.imaging.config.bean.
5. Look for the **InputDirectories** value.
   - This is the Imaging and Process Management input directory where Imaging and Process Management will check for incoming scanned invoices.
   - The path will point to a directory on the server running Imaging and Process Management.
6. Open a terminal window for the server running Imaging and Process Management and check the path specified for the Input Directory.

   The path should be a symbolic link pointing to a folder on a storage server. Both the Imaging and Process Management server and the Windows server must have read/write access to the same folder on the storage server.

2. Configure the Network Share for the Imaging and Process Management Input Directory

Enable the Imaging and Process Management input directory to be accessed by Document Capture or Forms Recognition running on Windows:

- The storage server share should have Common Internet File System (CIFS) enabled for Windows compatible share names.
- The path to the Windows share name should be in Universal Naming Convention (UNC) format.

Note

If you have licensed Oracle Fusion Automated Invoice Processing, individual Oracle Document Capture workstations used for scanning invoices do not need access to the input directory.

The storage host must grant read/write access to the Imaging and Process Management Input Agent running on the Common Domain host and at least one Windows user with login access to the server running Oracle Document Capture and Oracle Forms Recognition.

---

3. Verify Oracle Imaging and Process Management Input Agent

To verify if the Oracle Imaging and Process Management Input Agent is operating correctly:

1. Log on to the Oracle Enterprise Manger for the Common Domain.
2. Navigate to the Imaging Server.
3. Restart the server.

   After the server restarts, check the input directory path referenced earlier. You should see a file named InputAgent.lock. If you do not see this file, verify that the image server is running and check the image server logs for errors. If you notice errors, check whether the Input Agent has the necessary permissions in the storage directory. The Input agent needs read/write file access to this directory.

   Additionally, verify that the Windows network drive is correctly mapped with permitted read/write access. You can do this by creating a folder or file from the Linux box where the IPM server is running. Oracle Forms Recognition is not compatible with NFS mounted shares on Windows. You must use create CIFS shares for Windows instead. The Windows user should be able to view it on the Windows network drive and should be able to open and modify it.

4. Configure the Windows Mapped Network Drive for the Input Directory

You must log on to the Windows desktop with a user ID that has explicit access to the input directory file share.

You need to map the drive on the Windows servers running Oracle Forms Recognition and Oracle Document Capture servers. The drive will not be mapped on individual user machines running Oracle Document Capture client for Invoicing.

1. Open Windows Explorer.
2. Right-click on the folder for the PC icon depicting a computer with same name as the PC.
3. Select **Map Network Drive**.
4. Select drive letter, for example **Y**.
5. Specify the path for the shared directory on the storage host, using the UNC format: \\<host name>\<name>.
6. Click **OK** and verify that the network share now appears in Windows Explorer as the drive letter you specified. If Windows Explorer is unable to create the mapped drive, the issue may be that CIFS is not enabled on the storage host.
7. Verify that Windows users have read/write access to the input directory and all its file contents.
8. Verify that the Input Agent directory includes the InputAgent.lock file (the input directory may be a sub-directory of the share). If you do not see the InputAgent.lock file, the following are possible explanations:

- The Imaging and Process Management (IPM) Server is not running and needs to be started.
- The IPM Server is running but the Input Agent does not have the appropriate access to the network share directory and cannot generate the InputAgent.lock file.
- IPM Server's configuration for Input Agent Directory does not point to the same network share as the mapped network drive, or it points to a sub-directory other than the one you are verifying.

Note

To verify that the Windows network drive is correctly mapped with permitted read/write access, create a folder or file from the Linux box where the IPM server is running and check if the Windows user is able to view the folder or file on the Windows network drive and is able to open and modify it.

Configuring the Oracle Forms Recognition Project Network Share: Procedures

The Oracle Forms Recognition project directory contains directories and files shared by Oracle Document Capture, Oracle Forms Recognition Designer, Oracle Forms Recognition Verifier, and Oracle Forms Recognition Runtime Service. In a typical installation scenario, these applications are not installed on the same computer. However, the project directory must be stored in a shared directory accessible to each application, regardless of where it is installed.

Note

This task is not applicable to Oracle Cloud implementations.

To configure the Oracle Forms Recognition project network share, do the following:

1. Configure the share for the Oracle Forms Recognition AP Project directory
2. Configure the Windows mapped network drive for the AP Project directory

1. Configure the Network Share for the Oracle Forms Recognition AP Project Directory

Ensure that the Oracle Forms Recognition project directory is accessible to the Oracle Document Capture or Oracle Forms Recognition applications running on Windows.

- The storage server share should be configured with Common Internet File System (CIFS) enabled for Windows compatible share names.

- The Windows share name must be in universal naming convention (UNC) format.
- The network share is meant for exclusive use by the Oracle Document Capture or Oracle Forms Recognition applications running on Windows.

Configure the storage host to share the Oracle Forms Recognition Project directory with the Oracle Document Capture and Oracle Forms Recognition users.

2. Configure the Windows Mapped Network Drive for the AP Project Directory

You must log on to the Windows desktop with a user ID that has explicit access to the Oracle Forms Recognition project file share.

Note

This mapping is done on the following:

- Windows servers running Oracle Forms Recognition and Oracle Document Capture servers for Expenses
- Servers running Oracle Forms Recognition Designer and Verifier
- Invoice scanning workstations running Oracle Document Capture

Perform the following steps to configure the Windows mapped network drive:

1. In Windows Explorer, identify the folder for the PC icon that displays the same name as that of the actual PC.
2. Right-click the folder for the PC icon depicting a computer with same name as the PC.
3. Right-click the folder and select **Map Network Drive**.
4. Select a drive letter, for example **X**.
5. Specify the path for the shared directory on the storage host, using the UNC format: \\<host name>\<share name>.
6. Click **OK** and verify that the network share now appears in Windows Explorer as the drive letter you specified. If Windows Explorer is unable to create the mapped drive, the issue may be that CIFS is not enabled on the storage host.

Installing and Configuring Oracle Document Capture and Oracle Forms Recognition on Windows - Part 1: Procedures

To configure Oracle Document Capture and Oracle Forms Recognition to run on Windows, perform the following tasks in the given order:

Note

These tasks are not applicable to Oracle Cloud implementations.

1. Install prerequisites
2. Run the setup utility
3. Install Oracle Document Capture
4. Configure Oracle Document Capture
5. Configure Oracle Document Capture Import Server for Importing Images from E-Mail
6. Install Oracle Forms Recognition for Payables
7. Configure Oracle Forms Recognition for Payables
8. Configure shared drive access for Oracle Forms Recognition Runtime Service Manager

Note

Ensure that you have configured the required network shares before performing these steps. Steps 4 to 7 (Configure Oracle Document Capture to Configure Oracle Forms Recognition for Payables) are required only if you have licensed Oracle Fusion Automated Invoice Processing.

For more information on performing post-installation tasks, see the Oracle Document Capture Installation Guide and the Oracle Forms Recognition Installation Guide.

1. Install Prerequisites

Before you proceed with the installation and configuration of Oracle Document Capture and Oracle Forms Recognition, you need to fulfill the following prerequisites:

1. Ensure that the empty Document Capture schema is created in the Oracle database with at least three user profiles: a read-only user profile for reporting, a read/write user profile for schema administration, and a read/write user profile for the Document Capture runtime connection. Document Capture tracks batches and stores audit information in the schema tables. The Document Capture runtime connection configuration includes read/write user profile credentials so that Document Capture can write data to the schema tables without requesting a separate login.

   For more information on configuring the Document Capture database, see the Oracle Document Capture Installation Guide.

2. Install and Configure Oracle database support for Open Database Connectivity (ODBC) and OLEDB. For more information, see Oracle Database Software Downloads on Oracle Technology Network at http://www.oracle.com/technetwork.
3. Ensure that Java Runtime Environment (JRE) 1.6 or higher is installed. For more information, see Java Downloads on Oracle Technology Network at http://www.oracle.com/technetwork.

4. To configure expenses, create the folder C:\ODC Projects\EXM\Import. You need to share this folder with read-write permissions enabled for incoming expense documents.
5. Download the Capture-FormsRec_FA.zip file from the Fusion Applications repository. The zip file is located at <repository_root>/ installers/Capture-FormsRec.

2. Run the Setup Utility

This program streamlines the installation and configuration of Oracle Document Capture and Oracle Forms Recognition.

1. Extract the contents of the Capture-FormsRec_FA.zip (downloaded earlier from the Fusion Applications repository) to a temporary folder and double-click Setup.exe to run the utility. The Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window appears.
2. In the **I/PM Input Agent Folder** field, enter a UNC path of the folder from which IPM uploads the documents. For example, \\<server_name> \<share_name>.
3. In the **Oracle Forms Recognition AP Project Folder** field, provide the root directory for the AP project. For example, <Drive Letter>:\OFR. If the specified directory does not exist at the mentioned location, the installer creates a directory with the same name.

You are now ready to install and configure Oracle Document Capture and Oracle Forms Recognition. The relevant instructions are provided in the subsequent sections.

3. Install Oracle Document Capture

You need to repeat the installation procedure on every machine that runs Oracle Document Capture.

Note

If an error occurs while installing Oracle Document Capture, verify if the computer's print spooler service is running (**Start** - **Settings** - **Control Panel** - **Administrative Tools** - **Services**). Scroll down until you see Print Spooler. If the status shows that it has not started, right-click the Print Spooler service and select Start. You can now retry installing Oracle Document Capture.

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Document Capture region, click **Install**. The Oracle Document Capture installer appears.
2. Proceed through the installation steps to complete the installation. Once the installation is complete, the Setup utility initiates an additional process to install a patch.
3. Proceed through the options to complete the patch installation. After it is complete, the **Configure** button in the Oracle Document Capture region is enabled.

4. Configure Oracle Document Capture

To configure Oracle Document Capture:

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Document Capture region, click **Configure**. The Oracle Document Capture Configuration Utility dialog box appears.
2. In the **Batch Folder** field, browse and select the folder where Oracle Document Capture batch files are stored.
3. In the **Commit Folder** field, browse and select the folder where Oracle Document Capture commits the captured files.

Note

If you are using Oracle Forms Recognition, leave this blank for now. After you install Oracle Forms Recognition, you will come back and set the folder path to <Drive Letter>:\OFR_Project\AP\Global\Import. If you are not installing Oracle Forms Recognition, set this to the Image Processing Management Input Directory.

4. Click **OK**. The Capture Batch Setup dialog box appears.

Note

The Capture Batch Setup dialog box appears only when configuring Oracle Document Capture for the first time.

5. On the Capture Batch Setup dialog box, enter the following details:
   a. In the **Enter Path to Network Batch Folder** field, specify the same folder path that you have provided in the **Batch Folder** field on the Oracle Document Capture Configuration Utility dialog box.

   b. In the **Enter Path to Network Commit Folder** field, specify the same folder path that you have provided in the **Commit Folder** field on the Oracle Document Capture Configuration Utility dialog box.

   c. In the Capture Database Setup area, select the **Other Database Platform** option and click **Configure**. The Configure Database Connection dialog box appears.

   d. Click **Configure DB Connection**. The Data Link Properties dialog box appears.
      1. On the **Provider** tab, select **Oracle Provider for OLE DB** and click **Next**.
      2. On the Connection tab, provide the following information:
         a. In the **Data Source** field, enter the name of the Oracle database.

         b. Select the **Use a specific user name and password** option and provide the **User name** and **Password** that have read and write access to the Capture schema.

         c. Select the **Allow saving password** option.

d. Click **Test Connection** to check for connectivity issue if any, and resolve it before you proceed with the configuration.

3. Click **OK**. The Data Link Properties dialog box closes.

e. On the Configure Database Connection dialog box, click **OK**. The Configure Database Connection dialog box closes.

f. On the Capture Batch Setup dialog box, click **Initialize DB** to populate the Capture schema in the Oracle database.

Note

- Initializing the database is required when you configure Oracle Document Capture for the first time.
- If you are configuring a standalone instance of Oracle Document Capture for testing, you can use the default Capture database (capture.mdb) that is installed with the product. On most systems, this database is located in the Oracle Document Capture installation directory. On Windows 2008 R2, the Capture database is installed in the system ALLUSERPROFILES\Oracle Document Capture folder. By default, ALLUSERSPROFILES is C:\ProgramData.

  To use the default capture.mdb, you need to create a data source based on Microsoft Jet OLE DB 4.0. The local Capture database is only used for testing. For production environments, you must create the Capture schema in the Oracle database.

A warning message appears indicating loss of existing data in the Capture schema if you proceed with the initialization.

1. Click **Yes**. The Security Model dialog box appears.
2. Select the option that is appropriate to the system environment and click **OK**. The Microsoft Windows Open dialog box appears.
3. Navigate to the Oracle Document Capture installation directory, search for the Capture_ORACLE.sql file, select it, and click **Open**. Oracle Document Capture runs the script of the Capture schema and creates the required tables in the Oracle database.

g. On the Capture Batch Setup dialog box, click OK. The Capture Batch Setup dialog box closes.

6. On the Oracle Document Capture Configuration Utility dialog box, click **OK**.

Note

If prompted for user credentials, enter the user name and password that have been used during the configuration process.

4.1 Configure Additional Routing Attributes for Manual Scanning

To configure additional routing attributes for manual scanning:

1. If you are installing the Automated Invoice Processing components for the first time you already have the latest cabinet files, so you can skip the unzip and import steps and proceed to Step 2. Otherwise, if you were already using Automated Invoice Processing, perform the following steps to import the latest cabinet files:

   a. Unzip the Capture-FormsRec_FA.zip package.

   b. Import the ApInvoiceOdcCabinet.zip and ApInvoiceOfrCabinet.zip files using the Document Capture Import Export utility.

2. Open Oracle Document Capture and select **Indexing** - **Manage Index Profiles** .
3. Select the Fields tab for index profiles **Fusion Payable Invoices With OFR** and **Fusion Payable Invoices Without OFR** and verify that they contain the following index fields: **Routing_Attribute_1** through **Routing_Attribute_5**, and **URN**.
4. Select **System** - **Manage Macros** .
5. Select the **Scan for ISIS** category.
6. Select the **OFR-Scan-ISIS-Macro** macro.
7. Click **Setup**.
8. (Optional) Review and modify the **Prompt User upon closing Review** option in the Index Documents area to meet your requirements.
9. Select the **Do not Commit Batch** option in the Commit Options area.
10. Click **OK**.
11. (Optional) If you are not planning to use all five attributes, or you decide to use a longer length for each of the remaining attributes, you can change the maximum length of the index field attributes:

    a. Select **Admin** - **File Cabinets** .

    b. Select either **Payables Invoice with OFR** or **Payables Invoices without OFR**, depending on which file cabinet you are using.

    c. Select the routing attribute that you want to edit.

    d. Click **Edit**.

    e. Update the **Max Length** field.

Note

- Do not modify the index field names, otherwise the predefined attribute configuration will not work as expected.

- The sum of the maximum lengths is limited to the number of characters allowed by Oracle Forms Recognition (233), minus the number of characters in the file path where the image files are imported, minus the TIF file extension including the period (4), minus the characters reserved for internal use (40), minus one separator character per attribute.

For example, if the image files are imported into the `C:\OFR\Import\` directory and if you are using all five attributes, you should not exceed 170 characters (233-14-4-40-5).

- The number of characters for an attribute value cannot exceed the **Max Length** for that attribute. If the attribute value character count exceeds the specified maximum length, Oracle Document Capture's scan and commit will error.

f. Click **OK**.

5. Configure Oracle Document Capture Import Server for Importing Images from E-Mail

To set up the Oracle Document Capture Import Server to import invoice images that are received through e-mail and to capture additional attributes for routing based on information in the e-mail subject, perform the following steps.

Configure additional routing attributes.

1. If you are installing the Automated Invoice Processing components for the first time, you already have the latest cabinet files, so you can skip the unzip and import steps and proceed to Step 2. Otherwise, if you were already using Automated Invoice Processing, perform the following steps to import the latest cabinet files:

   a. Unzip the Capture-FormsRec_FA.zip package.

   b. Import the ApInvoiceOdcCabinet.zip and ApInvoiceOfrCabinet.zip files using the Document Capture Import Export utility.

2. (Optional) Perform Step 11 in section "Configure Additional Routing Attributes for Manual Scanning" to change the maximum lengths of the index attribute fields.

Configure the Email Provider batch job.

1. Open the Oracle Document Capture Import Server.
2. Select **Setup** - **Batch Jobs** .
3. Expand the Email Provider folder.
4. Select the **AP Email Provider** batch job.
5. If you are not using Oracle Forms Recognition, perform the following steps, otherwise proceed to Step 6.

   a. Select the General tab.

   b. In the **File Cabinet** field, select **Payables Invoice without OFR**.

   c. In the **Server Macro** field, select <NONE>.

   d. Select the Processing tab.

   e. Uncheck the **Commit Batches** option.

6. Select the Image Output tab. The default resolution is set to **300 x 300**.

Important

Do not modify this setting.

7. Select the Email Provider Settings tab.
8. Select the Email Accounts subtab.
   a. In the **Email Protocol** field, select the e-mail protocol that is being used.
   b. In the **Email Server Name** field, specify the DNS name that the e-mail server uses.
   c. In the **Email Addresses to Process** field, enter the e-mail addresses that are designated to process scanned invoices.
9. Select the Email Filters subtab.
   a. Configure the settings in the **Process Emails containing specified text** area.

      Specify the e-mail text that the Oracle Document Capture Import Server must find to process an e-mail. If the designated e-mail account is responsible only for receiving scanned invoices, this section can be left blank.
   b. Configure the settings in the **Attachment Processing** area to process the invoice image attachments.
10. Select the Post-Processing subtab.
    a. In the Upon Successful Import area, select the action to take when the import process succeeds.

       The default setting is to delete the message from the e-mail account.
    b. In the Upon Failed Import area, select the action to take when the import process fails.

       The default setting is **Don't Delete Message**, which leaves the failed imported invoices in the e-mail account.
11. Click **Close**.

Schedule the Email Provider batch job.

1. Select **Server** - **Schedule** .
2. Click **Schedule New Event**.
3. In the **Event** field, select **Email Provider - AP Email Provider**.
4. In the Event Properties area, specify the intended frequency.

Note

The recommended frequency setting is **Every 1 Minute**.

5. Select **Server** - **Activate** to run the job.

Installing and Configuring Oracle Document Capture and Oracle Forms Recognition on Windows - Part 2: Procedures

To configure Oracle Document Capture and Oracle Forms Recognition to run on Windows, perform the following tasks in continuation of the tasks in Part 1.

Note

These tasks are not applicable to Oracle Cloud implementations.

6. Install Oracle Forms Recognition for Payables

You need to install Oracle Forms Recognition for Payables on two different servers, one server each for:

- The Runtime Service: The instance of Oracle Forms Recognition for the Runtime Service must be installed on a secure server accessible only to administrators. The Runtime Service normally runs without any user intervention. However, administrators need to access the Runtime Service to perform setup and configuration tasks.
- The Designer and Verifier: The instance of Oracle Forms Recognition for the Designer and Verifier needs to be installed on a server that is accessible to the users of the applications.

To install Oracle Forms Recognition, perform the following steps:

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Forms Recognition region, click **Install**. The Oracle Forms Recognition installer appears.

Note

While installing it on each server, ensure that you select the Complete install option.

2. Proceed through the installation steps to complete the installation. Once the installation is complete, the Setup utility initiates an additional process to install a patch, if any.
3. Proceed through the options to complete the patch installation. After it is complete, the **Configure** button in the Oracle Forms Recognition region is enabled.

For more information about installing Oracle Forms Recognition, see the Oracle Forms Recognition Installation Guide.

7. Configure Oracle Forms Recognition for Payables

To configure Oracle Forms Recognition for Payables, perform the following steps:

1. On the Oracle WebCenter Capture and Forms Recognition for Fusion Financials Setup window, in the Oracle Forms Recognition region, click **Configure**. The Oracle Forms Recognition Runtime Server Creation dialog box appears.

Note

The Oracle Forms Recognition Runtime Server Creation dialog box appears if you have installed Oracle Forms Recognition for the first time. If Oracle Forms Recognition is already available and was earlier configured, the Oracle Forms Recognition Runtime Server Creation dialog box is skipped and the Oracle Forms Recognition Configuration Utility dialog box appears. The instructions here are provided assuming that Oracle Forms Recognition is installed for the first time.

2. On the Oracle Forms Recognition Runtime Server Creation dialog box, select one of the options to create the Runtime Service:

   - **All (Import, OCR, Classification, Extraction, Export and Clean-up)** to create and configure a single instance of the Runtime Service that performs all Oracle Forms Recognition workflow operations. This is the default option and is normally reserved for use by demonstration systems.

   - **Custom** to customize the creation of the Runtime Service based on several parameters as described here:

Note

- For production environments, Oracle recommends that you create separate Runtime Service instances for each function using the Custom options as described below. If you need to increase system capacity, you need to add additional instances of OCR, Classification and Extraction Runtime Service.

- If you plan to create separate instances for each function, create all of them at this point. This dialog box is available only during first time installation. You cannot access it later to add Runtime Service instances. If you want to add instances later, you need to create each of them manually.

Sub-option	Functional Description
Import	Selecting this check box creates an import enabled instance of the Runtime Service.
OCR, Classification and Extraction	Selecting this check box creates an OCR, Classification and Extraction enabled instance of the Runtime Service.

Number of Instances	You can specify the number of OCR, Classification and Extraction enabled instances that you want to create. The default value is 1. An OCR, Classification and Extraction enabled instance is CPU intensive and therefore, if you need to balance higher invoice loads, you need to create additional instances. However, it is recommended that the number of such instances must not exceed the number of cores on the server. You can add additional instances using the SET file created by the Setup utility. The SET file name is FusionAP - OCE.set, which is located in the Bin folder of the Forms Recognition install folder, for example C:\Program Files\Oracle \Forms Recognition\Bin.
Export and Clean-up	Selecting this check box creates an Export and Clean-up enabled instance of the Runtime Service.

3. Click **OK**. The Oracle Forms Recognition Runtime Server Creation dialog box closes and the Oracle Forms Recognition Configuration Utility dialog box appears.
4. In the **AP Solution INI File** field, ensure that the path is set to the automatically installed INI file.
5. In Database Connections, ensure that at least one connection is selected. In absence of a Database Connection, click **Create** to create a database connection. Ensure that the selected database connection has read-only access to the Fusion schema.
6. From the **ODBC System DSN (32-bit)** list, select one of the predefined ODBC System DSN value. If the list is blank, create an ODBC System DSN using the ellipsis button next to the field. Ensure that the ODBC connection has read-only access to the Fusion schema.
7. Enter the **User ID** and **Password** associated with the selected ODBC System DSN.
8. Click Test Connections to ensure that the selected database connection is active and working.
9. In the PO Format field, enter the format of the purchase order.

Note

You can use **#** as a wildcard character to represent a single number and @ as a wildcard character to represent a single alphabet.

10. In the **Ignore Characters** field, specify the characters such as comma, hyphen, period that may appear as part of the purchase order but need to be ignored. The ignore characters are always associated with a PO format.

11. Click **Add**. The PO format is added to the **Defined Formats** list, while simultaneously storing the associated characters to be ignored when that PO format is in use.

For more information about installing Oracle Forms Recognition, see the Oracle Forms Recognition Installation Guide. For more information on PO Formats see the AP Solution Guide located at <Drive Letter>:\OFR_Projects\AP.

8. Configure Shared Drive Access for Oracle Forms Recognition Runtime Service Manager

The Oracle Forms Recognition runtime service manager processes invoice images and exports them to a shared network drive. By design, Windows services are not allowed to access mapped network drives. Therefore, to access a network share, a Windows service must be running as an authenticated Windows user and it must access the share by specifying a UNC style path (\\server_name\share_name).

You must therefore assign a Windows user profile to the Oracle Forms Recognition Runtime Service Manager. The specified user profile must have read/write access to the shared network drive.

1. On the server that hosts the Runtime Service, select **Start** - **Control Panel** - **Administrative Tools** .

2. Select **Services**.

3. Right-click **Oracle Forms Recognition Runtime Service Manager** and select **Properties**.

4. Select the Log On tab.

5. Select the **This account** radio button, and enter the user name and password of the user granted read/write access to the shared network folder.

6. Click **Apply** and then click **OK**.

Setting Up Tesseract

Setting Up Tesseract Optical Character Recognition Engine: Procedures

Tesseract is an open source optical character recognition engine that processes images and performs image-to-text conversion.

Note

This task is not applicable to Oracle Cloud implementations for Releases 5 and 6.

If you plan to implement the Oracle Fusion Expenses iPhone application and use automatic expense creation from receipt images, you must set up Tesseract.

Note

Expenses can use Tesseract only if it is installed on the Linux platform.

One or more instances of Expenses can access a single Tesseract installation. For example, a production instance and a test instance of Expenses can access a single Tesseract installation.

To set up Tessearct, perform the following steps:

1. Verify that the user who is installing Tesseract has root access. Use the following command and ensure that the response is `root`.

```
$whoami
```

2. Create the directory that will host the Tesseract executable. The Oracle Fusion Payables Java EE application must have access to this directory. Expenses services must have executable permission on this directory.

```
$mkdir exmocr
```

3. Create a shell script in the directory you created in step 2.

   a. Open a new shell script file using the file editor.

```
$vi installtesseract.sh
```

   b. Copy the following script into the file:

```
#!/bin/bash
downloadPackage()
{
 site=$1
 file=$2
 if [ -f ${file} ] ; then
 echo "Skipping $file download since it already exists."
 else
 echo "Dowloading $file from the internet"
 wget http://${site}.googlecode.com/files/$file
 if [ "$?" -ne "0" ] ; then
 echo "Downloading ${file} failed. Confirm whether you have network
 connectivity.";
 exit 1;
 fi
 fi
}

prepareQuestion() {
 if [ -e tesseract-ocr ] || [ -e leptonica-1.68 ] || [ -e
 tesseract-3.01 ] ; then
 echo "Previous versions of tesseract-ocr or leptonica-1.68 exists."
 echo "This installer will uninstall the current version and install the
 new version."
 echo -n "Do you wish to proceed? [Y/N]: "
 read wish
 if [ $wish = "Y" ] || [ $wish = "y" ] ; then
 rm -rf tesseract-3.01 leptonica-1.68 tesseract-ocr
 else
 echo "Exiting the install process per your request."
 exit 1;
 fi
 fi
}

untarAll () {
 tar xvf tesseract-3.01.tar.gz
 mv tesseract-3.01 tesseract-ocr
 tar xvf tesseract-ocr-3.01.eng.tar.gz
 tar xvf leptonica-1.68.tar.gz
}
downloadAll() {
 downloadPackage tesseract-ocr tesseract-3.01.tar.gz
 downloadPackage tesseract-ocr tesseract-ocr-3.01.eng.tar.gz
 downloadPackage leptonica leptonica-1.68.tar.gz
}

buildAll() {
 cd $EXM_OCR_PATH/leptonica-1.68
 ./configure
 make
 sudo make install

 cd $EXM_OCR_PATH/tesseract-ocr
 ./autogen.sh
 if ! [ -d m4 ] ; then
 mkdir m4;
 fi
 ./configure
 cat -v ccutil/strngs.h | sed -e 's/^M-oM-;M-?//g' > strngs.h.new
 mv strngs.h.new ccutil/strngs.h
 make
 #sudo make install
}

generateTesseractFiles() {

cat > $EXM_OCR_PATH/tesseract-ocr/tessdata/configs/validchars << EOF
tessedit_char_whitelist
 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz.:,!@#$
%&*()+=;'<>/-
EOF

cat > $EXM_OCR_PATH/tesseract << EOF
#!/bin/sh
basedir=\$(dirname \$0)
export TESSDATA_PREFIX=\${basedir}/tesseract-ocr/
\${basedir}/tesseract-ocr/api/tesseract \$* \${basedir}/tesseract-ocr/
tessdata/configs/validchars
EOF

chmod +x $EXM_OCR_PATH/tesseract

}
export EXM_OCR_PATH=`pwd`
echo $EXM_OCR_PATH
prepareQuestion
```

```
downloadAll
untarAll
buildAll
generateTesseractFiles
```

c. Save the file.

```
:wq
```

4. Verify that the following directories exist and the shell script can access these directories:

```
/usr/local

/usr/local/include

/usr/local/lib
```

   Tesseract temporarily copies several files into these directories during installation.

5. Verify that `wget` is present on the machine. The shell script uses `wget` to download the files from the internet.

```
$which wget
```

6. Execute the shell script with root access.

   - The shell script downloads, untars, and installs the following files:

```
./tesseract-ocr-3.01.eng.tar.gz
./tesseract-3.01.tar.gz
./leptonica-1.68.tar.gz
```

   - On installation, Tesseract creates the following directories:

```
./tesseract-ocr
./leptonica-1.68
```

   - The shell script also creates the following shell script that is invoked by the Expenses application:

```
./tesseract
```

Note

Do not modify this shell script.

7. Create the directory for storing the image files sent to Tesseract for processing the converted text files. The Tesseract executable must have read and write access to this directory.

   The image files and the corresponding text files are not deleted from this directory. Based on your storage policies, you can remove these files periodically.

8. Create the following environment variables and set them to their respective values:

- `FIN_EXM_OCR_PATH`: This directory hosts Tesseract. Enter the full path along with the executable name as the value.
- `FIN_EXM_OCR_OUTPUT_DIR`: This directory stores the images and the converted files. Enter the full path as the value.
- Modify the file and add the following entries at the end:
  - Change directory to `<domain name>/bin.`
  - Open the `setDomainEnv.sh` file in the file editor.

```
$vi setDomainEnv.sh
```

  - Add the following environment variables and set them to the correct directories:

```
FIN_EXM_OCR_EXEC_PATH=<Enter the full path of the directory where
 Tesseract is installed.>/tesseract

export FIN_EXM_OCR_EXEC_PATH

FIN_EXM_OCR_OUTPUT_DIR= <Enter the full path of the directory for storing
 image files.>

export FIN_EXM_OCR_OUTPUT_DIR
```

  - Save the `setDomainEnv.sh` file.

9. Stop and restart the Financials domain in Oracle Fusion Applications.

If you already have Tesseract installed for your use, you can set up additional instances of Expenses to access the same Tesseract installation. To configure Expenses with an existing Tesseract installation, perform the following steps:

1. Mount the directory of the Tesseract installation on the new instance of Expenses, so that the Payables Java EE application in the new instance can access the Tesseract executable.
2. Create the directory for storing the image files sent to Tesseract for processing and the converted text files. The Tesseract executable must have read and write access to this directory.
3. Create the following environment variables and set them to their respective values.

   Modify the file and add the following entries at the end:

   a. Change directory to <domain name>/bin.
   b. Open the setDomainEnv.sh file in the file editor.

```
$vi setDomainEnv.sh
```

   c. Add the following environment variables and set them to the correct directories:

```
FIN_EXM_OCR_EXEC_PATH=<Enter the full path of the directory where
 Tesseract is installed.>/tesseract
```

```
export FIN_EXM_OCR_EXEC_PATH

FIN_EXM_OCR_OUTPUT_DIR=<Enter the full path of the directory for storing
 image files.>

export FIN_EXM_OCR_OUTPUT_DIR
```

d. Stop and restart the Financials domain in Oracle Fusion Applications.

Setting Up Financial Transactions

Oracle Fusion Advanced Collections Dunning: Highlights

Oracle Fusion Advanced Collections Dunning feature utilizes Oracle Business Intelligence Publisher to distribute dunning letters to customers via e-mail, fax or print. To use this feature, you must configure Oracle Business Intelligence Publisher to connect to the deploying company's internal e-mail, or the print or fax servers.

Note

This task is not applicable to Oracle Cloud implementations.

Configuring Oracle Business Intelligence Publisher

- Configure Oracle Business Intelligence Publisher by adding an e-mail server. Refer to the Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher (Oracle Fusion Applications Edition).

  See: Adding an E-Mail Server

Enabling Encryption of Sensitive Payment Information: Procedures

Financial transactions contain sensitive information, which must be protected by a secure, encrypted mode. In Oracle Fusion Payments, you can enable the encryption process for various types of payment information. Before you can enable encryption for credit cards and external bank accounts, you must create a wallet file.

Note

This task is not applicable to Oracle Cloud implementations.

After installing Oracle Fusion Applications, you can secure sensitive information by using any one of the following methods:

- Automatically create a wallet file, automatically generate a master encryption key, and manually enable encryption.

- Manually create a wallet file, automatically generate a master encryption key, and manually enable encryption.
- Manually create a wallet file, manually generate a master encryption key, and manually enable encryption.
- Automatically create a wallet file, automatically generate a master encryption key, and manually enable encryption.

Automatically Create a Wallet File, Automatically Generate a Master Encryption Key, and Manually Enable Encryption

To automatically create a wallet file, automatically generate an encryption key, and manually enable encryption, perform the following steps:

1. Navigate to the Manage System Security Options page as follows: **Navigator link > Tools menu: Setup and Maintenance link > Overview page > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search button > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page.**
2. In the Manage System Security Options page, click the **Edit Master Encryption Key** button. The **Edit Master Encryption Key** dialog box appears.
3. In the **Edit Master Encryption Key** dialog box, select the **Application-generated** radio button.
4. Click the **Save and Close** button.
5. In the Manage System Security Options page, click the **Encrypt** button in either the Credit Card Data region or the Bank Account Data region or in both regions to enable encryption for sensitive financial data.

Manually Create a Wallet File, Automatically Generate a Master Encryption Key, and Manually Enable Encryption

To manually create a wallet file, automatically generate an encryption key, and manually enable encryption, perform the following steps:

1. Create an empty Oracle Wallet, ewallet.p12, using the Oracle Wallet Manager utility.
2. Navigate to the Manage System Security Options page as follows: **Navigator link > Tools menu: Setup and Maintenance link > Overview page > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search button > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page**.
3. In the Manage System Security Options page, click the **Edit Master Encryption Key** button. The **Edit Master Encryption Key** dialog box appears.
4. In the **Edit Master Encryption Key** dialog box, select the **Application-generated** radio button.
5. Click the **Save and Close** button.
6. In the Manage System Security Options page, click the **Encrypt** button in either the Credit Card Data region or the Bank Account Data region or in both regions to enable encryption for sensitive financial data.

Manually Create a Wallet File, Manually Generate a Master Encryption Key, and Manually Enable Encryption

To manually create a wallet file, manually generate an encryption key, and manually enable encryption, perform the following steps:

1. Create an empty Oracle Wallet, ewallet.p12, using the Oracle Wallet Manager utility.
2. Navigate to the Manage System Security Options page as follows: **Navigator link > Tools menu: Setup and Maintenance link > Overview page > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search button > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page**.
3. In the Manage System Security Options page, click the **Edit Master Encryption Key** button. The **Edit Master Encryption Key** dialog box appears.
4. Take one of the following actions:
   - In the **Edit Master Encryption Key** dialog box, select the **User-defined** radio button.

     In the **Key File Location** field, enter the path to the master encryption key, click the **Save and Close** button, and then click the **Done** button.
   - Generate a secure, custom key by copying a file containing the bits of the key to the same directory as the empty Oracle wallet, ewallet.p12

Note

After the wallet is created, ensure that you securely delete the file containing the key bits by using a utility that supports secure deletion.

5. In the Manage System Security Options page, click the **Encrypt** button in either the Credit Card Data region or the Bank Account Data region or in both regions to enable encryption for sensitive financial data.

Automatically Create a Wallet File, Automatically Generate a Master Encryption Key, and Manually Enable Encryption

To automatically create a wallet file, automatically generate an encryption key, and automatically enable encryption, perform the following steps:

1. Navigate to the Manage System Security Options page as follows: **Navigator link > Tools menu: Setup and Maintenance link > Overview page > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search button > Expand Define Payments Security folder > Manage System Security Options task: Go to Task icon > Manage System Security Options page**.
2. In the Manage System Security Options page, click the **Apply Quick Defaults** button. The **Apply Quick Defaults** dialog box appears.
3. In the **Apply Quick Defaults** dialog box, select all the check boxes: **Automatically create wallet file and encryption key**, **Encrypt credit card data**, and **Encrypt bank account data**.

4. Click the **Apply** button.

For more information on Payments security, see the chapter entitled Define Funds Capture and Payments Security in the Oracle Fusion Applications Financials Implementation Guide.

Configuring Communication Channel to a Payment System: Explained

To transmit or receive payment information to or from a payment system through a firewall, you must configure the communication channel used to communicate with the payment system by performing the following steps:

1. Configure and deploy a tunnel.
2. Set up SSL security to communicate with the payment system servlet.

Note

This task is not applicable to Oracle Cloud implementations.

1. Configure and Deploy a Tunnel

To communicate with a payment system through a firewall, you can use the Tunneling feature of Oracle Fusion Payments. The Tunneling feature is used to deliver data, such as a payment file or settlement batch, using two protocols, one of which encapsulates the other. Tunneling is also referred to as delegated transmission, since the initial transmission from Payments is a request to an external module (the transmission servlet) to deliver data using an independent transmission protocol. The name of the transmission protocol, its parameters, and the actual data to be delivered are encapsulated within the body of the tunneling transmission protocol.

The purpose of tunneling is to allow connectivity between Payments and external payment systems without compromising network security. Processor payment systems, for example, often require protocols, such as FTP or IP socket connectivity to receive payment files. Instead of creating breaches in your firewall to accommodate these connectivity requirements, you can instead deploy the Payments transmission servlet on a host outside your firewall and then tunnel or delegate requests to it from the Payments engine. The Payments transmission servlet does not use the applications database and can be completely isolated from the intranet of your deployment environment.

Tunneling Protocol

Payments uses a customized tunneling protocol called the Oracle Fusion Payments Tunneling Protocol. This protocol uses HTTP POST as its underlying transmission mechanism. HTTPS is also supported. When the tunneling protocol sends a request, it places an XML message header within the body of the request, which is meant to identify the tunneled or encapsulated protocol, as well as the parameters to use when invoking it, such as host name, user name, and password for FTP. The data to be delivered is sent after the XML message header is sent.

Important

Payments does not support the tunneling or encapsulation of a tunneling protocol.

As a supported transmission protocol, the tunneling protocol implements the `oracle.apps.financials.payments.sharedSetup.transmissions.publicModel.util.TunnelingFunction` interface. The following table presents the parameters and descriptions of the Payments tunneling protocol.

Parameter	Description
WEB_URL	The HTTP/HTTPS URL of the transmission servlet executing the protocol.
USERNAME/PASSWORD	The user name and password used to access the servlet if its URL is secured by HTTP authentication.

Transmission Servlet

Payments transmission servlet is the module which executes tunneled or delegated transmission requests sent from the Payments engine. The servlet receives the Payments HTTP XML delivery envelope requests and parses them into XML message header and transmission data components. The format of the XML message header is defined by an XML DTD file named DeliveryEnvelope.dtd. The message header specifies the transmission protocol, as well as the parameters to pass to the tunneled or encapsulated transmission protocol, using its Java class name and entry function name. The transmission servlet then dynamically loads the Java class implementing the tunneled protocol and initiates it by passing to it the transmission parameters parsed from the XML message header and the transmission data.

This behavior is identical to that of the Payments engine.
Any protocol can be tunneled, as long as it implements the `oracle.apps.financials.payments.sharedSetup.transmissions.publicModel.util.TransmitFunction` interface. Therefore, any custom-defined protocol can be tunneled or encapsulated to the servlet, provided the Java class which implements it is in the CLASSPATH of the servlet's application container. To deploy the servlet to a different host, such as the one in a DMZ network zone, you must copy FinPmtTransmitServlet.war to the transmission servlet's new servlet container. If you want the servlet to support any new transmission protocol that you develop, its Java code must be deployed to the transmission servlet's web application domain.

Configuring Tunneling

Tunneling is configured on the Create Transmission Configuration page. A tunneling transmission configuration is specified as any other transmission configuration, but the protocol is always Payments HTTP XML Delivery Envelope protocol. Once the tunneling protocol is configured, it can use or encapsulate any regular, non-tunneling transmission configuration by specifying a value from the Tunneling Configuration choice list on the Create Transmission Configuration page. Once that is done, ensure that you set up your payment system to support the tunneling protocol and that your corresponding funds capture process profiles and payment process profiles specify the tunneling configuration.

2. Set Up SSL Security to Communicate with the Payment System Servlet

When Payments communicates with the payment system servlets, the information exchanged may be sensitive information such as credit card numbers. If the communication is not secure, it poses a security risk.

The security risk is higher under the following circumstances:

- When Payments and the payment system servlets are installed on separate machines
- When Payments is deployed and operates outside your firewall

To set up a payment system servlet with a secured sockets layer, enable HTTPS on the middle-tier server where the servlet resides. If funds capture process profiles are not defined for the payment system, change the BASE URL parameter of the payment system to use the https: protocol. Otherwise, change the URLs on any transmission configurations set up to be used with that payment system to contain HTTPS.

Configuring Oracle B2B Inbound Flow to Receive Supplier Invoices in XML: Procedures

Oracle B2B Server is an Oracle SOA Suite component that manages interactions between deploying companies and trading partners such as suppliers. Oracle Fusion Payables supports an inbound Oracle B2B flow using Oracle B2B Server for receiving invoices from suppliers in XML format.

Note

This task is not applicable to Oracle Cloud implementations.

Trading partners can use this B2B feature to communicate electronically by sending documents in XML format. The B2B XML invoices use the same XML standard 171_Process_Invoice_002 (version 7.2.1) developed by the Open Applications Group (OAG). For more information on B2B XML Invoices, see the Oracle Fusion Applications Procurement, Payables, Payments, and Cash Guide.

Customers or deploying companies who want to receive and process invoices in XML format (complying to OAG standards) that are provided by the suppliers, need to perform the following post-installation configurations.

1. Host Company Configuration
2. Supplier Configuration

Note

These configurations are required only if customers or deploying companies want to use the B2B XML invoice feature.

1. Host Company Configuration

Perform the following steps to complete Host Company configuration.

1. Set up the Oracle B2B Server.
2. Set up Oracle Supplier Network for the Host Company

Note

This step is required only if customers use Oracle Supplier Network as the communication channel.

3. Set up B2B Site Code

1. To set up the Oracle B2B Server, do the following:

   a. Create a supplier trading partner.

Note

The Oracle B2B Server is preloaded with the supported OAG document schemas and sample trading partners such as **MyCompany** which is the host company trading partner, and **ApSampleTradingPartner** which is the supplier trading partner. However, you can create your own supplier trading partners as instructed here.

1. Sign in to the Oracle B2B Server.
2. On the left, click **Add** on the Partner toolbar. The Partner Name dialog box appears.
3. Enter the name of the trading partner and click **OK**. A confirmation message appears. The new supplier trading partner is listed in the Partner region.
4. On the Documents tab, click **Add** to add a document definition for the supplier trading partner. The Select Document Definition dialog box appears.
5. Select **OAG - 7.2.1 - PROCESS_INVOICE_002 - OAG_DEF** and click **Add**. The document definition is added to the supplier and is displayed under Documents.
6. For the document definition, clear the check box under **Receiver**.
7. In the Partner region, select the new supplier trading partner, and on the Agreement toolbar, click **Add** to add a new agreement between the host company and the new supplier trading partner.
8. Enter the name of the agreement.
9. On the process train, click the **Select Document Definition** train stop. The Select Document Definition dialog box appears.
10. Select the **PROCESS_INVOICE_002** document definition mapped to the supplier trading partner and click **OK**.
11. Under Agreement Parameters, ensure that the **Functional Ack** check box is clear, and click **Save**.
12. To validate the agreement, click **Validate**.
13. Click Deploy. An information message appears, indicating successful deployment of the agreement.

   b. Set up a listening channel.

Note

Oracle B2B Server supports multiple protocols for sending/receiving messages between trading partners. You can choose a protocol that is best suited for your company. Refer to the Oracle B2B Server documentation or online help to learn about each protocol and which parameters need to be set up. Listening channel can be set up at the global level (applicable to all trading partners) or at the trading partner level.

Do one of the following:

- To set up a global listening channel, click Administration and click the Listening Channel tab.
- To set up a trading partner listening channel, click Partners and click the Channels tab.
- No need to set up a listening channel if Oracle Supplier Network is used by the suppliers to send the B2B invoice payload.

Note

When Oracle Supplier Network is used, the only required setup to communicate with the supplier trading partner is to add a Generic Identifier on the B2B Server, using the Trading Partner Alias of the supplier as the value of the identifier. The Trading Partner Alias of suppliers is defined on the Trading Partners tab of the host company trading partner in the Oracle Supplier Network. The Generic Identifier entry is added to the Identifiers table on the Profile tab of the trading partner page.

Save the changes to complete the set up.

2. Set up Oracle Supplier Network for the Host Company if the supplier uses Oracle Supplier Network to send the B2B invoice payload. To complete the setup, perform the following:

   a. Sign into the Oracle Supplier Network using the registered account.

   b. Access **Messaging** - **Communication Parameters** and select **HTTPS URL Connection** as the Delivery Method.

   c. Click **Modify** to update the delivery method parameter values.

   d. Enter the URL of the B2B HTTP receiver. Consult your system administrator if you do not know the value.

   e. Enter the User ID and password for Oracle Supplier Network.

Note

You can specify different values for the Test and Production environments.

---

   f. Access **Messaging** - **Transaction Management** .

   g. Add the OAG **PROCESS_INVOICE_002** document from the list of available documents if it is not already added.

   h. From the Action drop down list, select **Receive**.

   i. From each Delivery Method drop down list (OSN Test Delivery Method and OSN Production Delivery Method), select **HTTPS URL Connection** and click **Submit**.

j. On the Trading Partners tab, in the Add Trading Partners region, click **Add** to add supplier trading partners. You can add all the supplier trading partners who send invoice payloads to the host company.

3. Set up the B2B Site Code.

   For each supplier site that is enabled for B2B communication, the host company assigns a B2B Site Code to the site and communicates it to the supplier. Supplier has to provide this B2B Site Code in the invoice payload in the `<PARTNER><PARTNRIDX>` element, with `<PARTNER><PARTNRTYPE> = Supplier` within the `<INVHEADER>` element. To assign a B2B Site Code to a supplier site, navigate to the Manage Suppliers UI in the Fusion application. Search for the supplier and then open the supplier site. Enter a value into the B2B Supplier Site Code. Click Save. This code needs to be communicated to the suppliers manually so that they can include it in their invoice payloads.

   To assign a B2B Site Code to a supplier site, do the following:

   a. In Oracle Fusion Applications, access **Suppliers** - **Manage Suppliers** .

   b. Search for the specific supplier and open the relevant supplier site.

   c. On the Edit Site tab, in the B2B Trading Partner Information region, enter the site code (the site code set by the host company in Oracle B2B Server) in the **B2B Supplier Site Code** field.

   d. Click **Save**.

   Communicate the same site code to the suppliers.

2. Supplier Configuration

The following configuration steps must be performed by suppliers if they are using Oracle Supplier Network to send the invoice payload.

1. Sign in to the Oracle Supplier Network using the registered account.
2. Access **Messaging** - **Communication Parameters** and select **HTTPS URL Connection** as the Delivery Method.
3. Click **Modify** to update the delivery method parameter values.
4. Enter the URL of the B2B HTTP receiver.
5. Enter the User ID and password for Oracle Supplier Network.

Note

You can specify different values for the Test and Production environments.

6. Access **Messaging** - **Transaction Management** .
7. Add the OAG **PROCESS_INVOICE_002** document from the list of available documents if it is not already added.
8. From the Action drop down list, select **Send**.
9. From each Delivery Method drop down list (OSN Test Delivery Method and OSN Production Delivery Method), select **HTTPS URL Connection** and click **Submit**.

10. On the Trading Partners tab, in the Add Trading Partners region, click **Add** to add host company trading partner.

Setting Up Oracle B2B to Send Receivables Transactions in XML: Procedures

Oracle B2B Server is an Oracle SOA Suite component that manages interactions between deploying companies and trading partners. Oracle Fusion Receivables supports an outbound Oracle B2B flow using Oracle B2B Server to send transactions to customer trading partners in XML format.

The setup of the Oracle B2B flow for Receivables makes use of these existing elements:

- XML Schema document guideline
- OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition
- Host trading partner MyCompany

To set up Oracle B2B to send Receivables transactions in XML:

- Configure the host and remote trading partners
- Configure agreements between the host and remote trading partners

Configuring Trading Partners

Configure your enterprise as the host trading partner, and all of your customers that receive XML documents as remote trading partners.

To configure trading partners:

1. Log in to the Oracle B2B Server.
2. Navigate to the Administration page.
3. Click the Document tab.
4. Load the OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition file.
5. Click the Types tab.
6. Add a new Internal Identifier with the name B2B Trading Partner Code.

   This name matches the field name on the customer account profile.
7. Navigate to the Partners page.
8. In the Partner regional area, select the default host partner MyCompany.
9. If necessary, update the default host partner name to reflect your enterprise.

10. Click the Documents tab.
11. Verify that the OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition is assigned to the host trading partner.
12. Ensure that the Sender option is enabled.
13. In the Partner regional area, click the Add icon.
14. Enter the name of a remote trading partner.
15. Select the **Internal Identifier Type** B2B Trading Partner Code that you previously created and enter the Value for the identifier.

    This is the value that you will enter in the **B2B Trading Partner Code** field on the customer account profile of this remote trading partner.
16. Click the Documents tab.
17. Click the Add icon to associate the OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF document definition with the remote trading partner.
18. Enable the Receiver option.
19. Click the Channel tab.
20. Define a channel for the remote trading partner.

    The channel determines how the XML transaction is delivered to the remote trading partner from B2B: directly; via the Oracle Supplier Network (OSN), or via a third party.

    If you are communicating using Oracle Supplier Network (OSN), select the Generic Identifier and enter the IP Address of the OSN machine.

    For more information about configuring a channel, refer to the Oracle Fusion Middleware User Guide.
21. Repeat steps 13 to 20 for each remote trading partner.

Configuring Agreements

A trading partner agreement defines the terms that enable two trading partners, the sender and the receiver, to exchange business documents. The agreement identifies the trading partners, trading partner identifiers, document definitions and channels.

An agreement consists of two trading partners, the host trading partner and one remote trading partner, and represents one type of business transaction between these partners. For example, if the host trading partner MyCompany and the remote trading partner ABC Solutions regularly exchange both purchase orders and invoices, then two separate agreements are needed for each document definition.

To configure agreements between the host and remote trading partners:

1. Log in to the Oracle B2B Server.
2. Navigate to the Partners page.
3. In the Agreement regional area, click the Add icon to open a new agreement for the host trading partner MyCompany.

4. Enter the agreement ID and Name.
5. Enter the agreement parameters.
6. Select the Document Definition OAG-7.2.1-PROCESS_INVOICE_002-OAG_DEF for this agreement.
7. Select the remote trading partner to include in this agreement.
8. Select the channel for the remote trading partner.
9. Add identifiers for the remote trading partner.
10. Click Save to save the agreement.
11. Click Validate to validate the agreement.
12. Click Deploy to deploy the agreement.

    Deployment is the process of activating an agreement from the design-time repository to the run-time repository.
13. Repeat steps 3 to 12 for each agreement between the host trading partner and this remote trading partner.

5

Fusion Accounting Hub

Integrating with Other Products

Integration with Oracle E-Business Suite and Oracle PeopleSoft: Overview

Oracle Fusion Applications provides a coexistence strategy that allows you to continue to use your Oracle E-Business Suite or Oracle PeopleSoft General Ledgers and subledgers while using Oracle Fusion Accounting Hub for financial reporting. Coexistence includes the ability to transfer balances from the Oracle E-Business Suite General Ledger and journal entries from Oracle PeopleSoft General Ledger to the Oracle Fusion Accounting Hub.

For more information on completing the post-installation setup for coexistence with Oracle E-Business Suite General Ledger see:

- **Configuring Oracle Golden Gate to Integrate the E-Business Suite Ledger with Fusion Accounting Hub** on My Oracle Support
- Oracle Fusion Accounting Hub Implementation Guide
- Oracle General Ledger Implementation Guide Release 12.2: See this guide for information on loading and transferring data from Oracle E-Business Suite to the Oracle Fusion Accounting Hub.

For more information on completing the post-installation setup for coexistence with Oracle PeopleSoft General Ledger, see:

- Oracle Fusion Accounting Hub Implementation Guide
- PeopleSoft General Ledger 9.1 Documentation Update: Integrating PeopleSoft General Ledger with Oracle Fusion Accounting Hub
- PeopleSoft General Ledger 9.1 Integration to Oracle Fusion Accounting Hub Implementation Guide

Note

The Oracle Data Integrator (ODI) component (extract file for manual import) is currently available via My Oracle Support only in note id: 1365971.1.

Register Applications Coexistence Instances

Register applications coexistence instances to indicate in Oracle Fusion General Ledger which Oracle E-Business Suite and Oracle PeopleSoft instances are integrated with the Oracle Fusion Accounting Hub. There is a user interface to this registration. For each E-Business Suite or PeopleSoft instance, provide a unique system identifier. This identifier must also be registered in the corresponding Oracle E-Business Suite or Oracle PeopleSoft instance.

You can specify a unique journal source per instance. For Oracle E-Business Suite, you can limit which instance and balancing segments may post to a particular Oracle Fusion General Ledger.

For Oracle E-Business Suite, determine the Function ID to move data from Oracle Fusion General Ledger to Oracle E-Business Suite General Ledger. You must include the Function ID at the end of the drill down URL that is provided during the registration of the Oracle E-Business Suite instance.

To find the Oracle E-Business Suite Function ID:

1. Login as a System Administrator and navigate to Function page
2. Query for the function name: GL_FUSION_EBS_DRILL
3. Go to the Help menu, click **Diagnostics** > **Examine**
4. Select the **FUNCTION_ID** field. The value box shows the value of the Function ID.

For Oracle E-Business Suite: The URL format for the non-dynamic portion needs to be in the following format: `http://<domain>:<port>/OAA_HTML/RF.jsp?function_id=<function_id>`.

In the above URL format, the domain, port, and function_id are for the Oracle E-Business Suite Instance.

For Oracle PeopleSoft: The URL format for the non-dynamic portion needs to be in the following format: `http://server/servlet_name/SiteName/PortalName/NodeName/c/PROCESS_JOURNALS.FUS_DRILLBACK_JRNL.GBL`

In the above URL format:

- http://server/: Scheme (http or https) and the web server name.
- servlet_name/: Name of the physical servlet that the web server invokes to handle the request.
- SiteName/: Site name specified during Oracle PeopleSoft Pure Internet Architecture setup.
- PortalName/: Name of the portal to use for this request.
- NodeName/: Name of the node that contains the content for this request.

Integration with Data Relationship Management: Overview

Oracle Fusion Applications provides integration between Oracle Fusion Accounting Hub and Oracle Hyperion Data Relationship Management. The integration is included with Oracle Fusion Accounting Hub, Oracle Hyperion Data Relationship Management to store corporate charts of accounts values and hierarchies, and then update this information to both Oracle Fusion Accounting Hub and the Oracle E-Business Suite General Ledger.

For more information on completing the post-installation setup for Data Relationship Management, see the Oracle Hyperion Data Relationship Management Oracle General Ledger Integration Guide Release 11.1.2.2 on My Oracle Support at https://support.oracle.com.

Integration with Hyperion Planning: Overview

For Oracle Cloud implementations, integrate with on-premise Oracle Hyperion Planning for advanced budgeting by loading actual balances from Oracle Fusion Accounting Hub to Oracle Hyperion Planning so you can use the actual data in the budgeting process. You can also load budget data from Oracle Hyperion Planning to Oracle Fusion Accounting Hub through the Budget Interface to perform budget variance reporting within Oracle Fusion Accounting Hub.

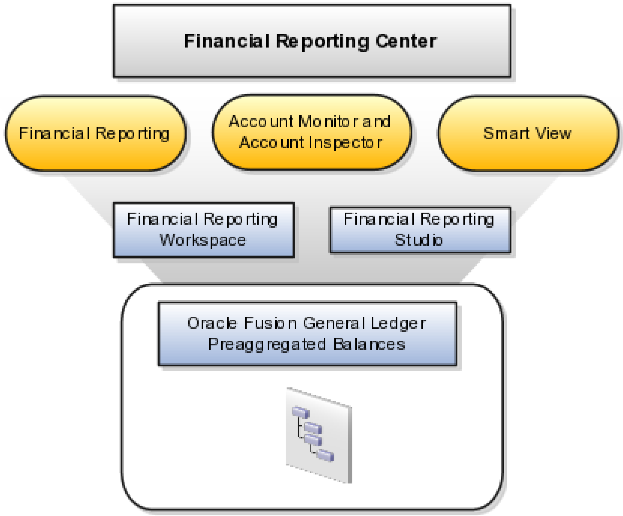
For other implementations, Oracle Fusion Applications provides integration between Oracle Fusion Accounting Hub and Oracle Hyperion Planning through Oracle Financial Data Quality Management ERP Integrator adapter. To complete the post-installation setup for the ERP Integrator adapter, see Oracle Hyperion Financial Data Quality Management ERP Integrator Adapter for Oracle Applications Administrator's Guide.

Setting Up Financial Reporting Center

Financial Reporting Center: How It Works

The Oracle Fusion Financial Reporting Center provides functionality for reporting on Oracle Fusion General Ledger balances. It provides secure, self-service access to reports that use real time account information.

You can design traditional financial report formats such as balance sheets, profit and loss statements, and cash flow reports. You can also design nontraditional formats for financial or analytic data that include text and graphics.


Financial Reporting Center
Financial Reporting
Account Monitor and Account Inspector
Smart View
Financial Reporting Workspace
Financial Reporting Studio
Oracle Fusion General Ledger Preaggregated Balances

Components

Financial Reporting Center is comprised of numerous components:

- **Financial Reporting:** Financial users and analysts access live reports and books or published snapshot reports and books from previously scheduled batches in a variety of formats. Other functionality includes:
  - Refreshing report data using runtime points of view or parameters
  - Drill through capability from parents to other parents
  - Drill down to detail balances, journal lines, and subledger transactions.
- **Oracle Hyperion Smart View:** Financial analysts view, import, manipulate, distribute, and share data from your Oracle Fusion General Ledger balances in Microsoft Excel.
- **Account Monitor and Account Inspector:** Financial analysts monitor and track key account balances in real time at every level of your dimensions and hierarchies. These tools provide multidimensional account analysis and drill down capability.
- **Workspace:** Reporting administrators create, open, save, and delete folders and store report objects, reports, and snapshot reports.
- **Oracle Hyperion Financial Reporting Studio:** Report authors use an object-oriented graphical report layout with report objects, such as text boxes, grids, images, and charts, to design reports.

Setting Up Your Financial Reporting Center: Critical Choices

Oracle Fusion Financial Reporting Center is a powerful tool for accessing, designing, and presenting financial reports and analytic data. The critical choices required to configure and install the components in Financial Reporting Center consist of:

- Configuring Financial Reporting Center
- Installing and configuring Financial Reporting Studio, performed by your end users.
- Installing Smart View, performed by your end user.
- Configuring Workspace Database Connection, performed by your administrator.
- Configuring Oracle Fusion Transactional BI Dimensions

Configuring Financial Reporting Center

You have access to the reports through the folder structure in the Financial Reporting Center and Workspace installed with Oracle Fusion Financial Applications. Your Oracle Fusion Business Intelligence (BI) administrator defines the folder structure in Workspace considering your company's security requirements for folders and reports, as well as report distribution requirements for financial reporting batches. Security can be set on folders and reports from Workspace. You are granted access to the folders and reports you want to view by your BI administrator.

Installing and Configuring Financial Reporting Studio

Oracle Hyperion Financial Reporting Studio is client-based software. If you access Oracle Fusion Applications from Oracle Cloud, you connect to the Financial Reporting Studio through a Windows Remote Desktop Connection.

Otherwise, report authors download the installation files for Financial Reporting Studio from Workspace by clicking **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting.** Once Workspace is launched, click **Tools > Install > Financial Reporting Studio**. After performing the prerequisites and completing the installation, launch the Financial Reporting Studio. Provide your user ID, password, and the Server URL. Derive the Server URL information by following the steps:

1. Open **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting** .
2. Edit the **Workspace URL** and remove workspace/index.jsp.
3. Following are two examples of Server URLs:
   - If the Workspace URL is https://fusionsystemtest-p-external-bi.us.oracle.com/workspace/index.jsp, the Server URL is https://fusionsystemtest-p-external-bi.us.oracle.com.
   - If the Workspace URL is https://fusionsystemtest-p-external-bi.us.oracle.com:10622/workspace/index.jsp, the Server URL is https://fusionsystemtest-p-external-bi.us.oracle.com:10622.
4. Copy the modified URL to the Server URL field.

Note

For end users installing the Oracle Fusion Financials Reporting Studio, the installer launches a separate console window that continues to run for a brief time after the installation completes the setup tasks. The process is normal, expected, and applies to Oracle Hyperion Reporting Studio installations in both the Oracle Fusion Applications and Enterprise Performance Manager modes.

Note

You must save a new report before attempting to preview it with Web Preview.

Prerequisites needed for installing the Financial Reporting Studio are:

1. Financial Reporting Studio Client Certifications that are found at: http://www.oracle.com/technetwork/middleware/bi-foundation/hyperion-supported-platforms-085957.html
2. Microsoft Office installed on your end-users computers.

Note

For more information, see:

- Oracle Enterprise Performance Management System Installation and Configuration Guide
- Oracle Hyperion Enterprise Performance Management System EPM System Standard Deployment Guide

Installing Smart View

Smart View is an Excel add-in that must be loaded to each client. To download the installation files from Workspace click the **Navigator > Financial Reporting Center > Open Workspace for Financial Reporting**. Once the **Workspace** is launched, click on **Tools > Install > Smart View.** Alternatively, download Smart View from http://www.oracle.com/technetwork/middleware/epm/downloads/smart-view-1112x-1594693.html.

Note

Since Smart View is an add-in to Microsoft Office products, you can install Smart View only on a Windows operating system.

Once Smart View is installed, it must be configured to connect to Oracle Fusion Applications. This is done using the Smart View Shared Connections URL. You can derive the **Shared Connections URL** by following the steps below:

1. **Open Workspace for Financial Reporting** from the **Financial Reporting Center task panel**.
2. Edit the **Workspace URL**, for example, if the **Workspace URL** is https://fusionsystemtest-p-external-bi.us.oracle.com/workspace/index.jsp. Remove index.jsp and add SmartViewProviders at the end of the URL.

Note

This is another example for a Cloud based environment: If the Workspace URL is https://efops-rel5st4-cdrm-external-bi.us.oracle.com:10622/workspace/index.jsp, the Shared Connections URL is https://efops-rel5st4-cdrm-external-bi.us.oracle.com:10622/workspace/SmartViewProviders.

3. Copy the URL.
4. Launch Excel.
5. Navigate to the **Smart View** menu **>** **Options** **>** **Advanced**.
6. Paste the URL in the **Shared Connections URL** field.
7. Click on the **OK** button.

For more information on configuring Smart View client for users, see Oracle Hyperion Smart View for Office User's Guide for Oracle Hyperion Smart View.

To connect Oracle Fusion General Ledger Balances cubes in Smart View:

1. Open Smart View from your **Start menu > Programs > Microsoft Office > Microsoft Excel 2007.**
2. Go to the **Smart View** menu **>** **Open**, in the **Start** on the ribbon > click on **Smart View Panel** that appears in the drop down box under the ribbon. This launches a task pane.
3. Click on the **Shared Connections** button on the task pane.
4. Sign in with your user name and password.
5. Click on the **Select Server to proceed** drop down.

Note

If the Essbase Server is not there, then it has to be added. Use the following steps:

a. Click on the Add Essbase Server link on the bottom of the spreadsheet.
b. Specify the Essbase Server login and password.
c. Expand the Essbase sever and locate the cube under it.

6. Select **Oracle Essbase** from the list of shared connections.
7. Click the **Expand** to expand the list of cubes.
8. Expand your cube (name of your chart of accounts).
9. Click on **db.** A list of functions appears on the bottom of the panel.
10. Click the **Ad hoc analysis.**

Note

You need to perform these steps only once for a new server and database.

To set how the name and alias of the Essbase database appears:

1. Click on the **Options** on the ribbon **>** select the **Member Options > ** select **Member Name Display.**
2. Set one of these three options:
   - **Distinct Member Name:** Only shows the full Essbase distinct path.
   - **Member Name and Alias**: Shows both the member name and the alias.
   - **Member Name Only:** Shows only the member name.

Note

The Smart Slice feature is not supported in Oracle Fusion General Ledger. For all other documentation, refer to the Oracle Hyperion Smart View for Office User's Guide for Oracle Hyperion Smart View.

Configuring Workspace Database Connections

Administrators need to create database connections from Workspace so users can access the cubes from Workspace and Financial Reporting Studio.

Note

Ledger setup has to be completed before the database connection can be created. Oracle Fusion General Ledger balances cubes are created as part of ledger setup. There is a separate cube for each combination of chart of accounts and accounting calendar. A database connection is needed for each cube.

Steps to define a database connection are:

1. Start at the **Navigator** by selecting **Financial Reporting Center.**
2. From the **Financial Reporting Center** task panel select **Open Workspace for Financial Reporting.**
3. From within **Workspace** select the **Navigator** menu > **BI Catalog.**
4. Select **Tools** menu **> Database Connection Manager.**
5. Select **New** button.
6. Enter a user friendly name for the **Database Connection Name.**
7. Enter Essbase as the **Type**, your server, user name, and password.
8. Select **Application** (cube) and **Database** from the list of values. Expand the **Application** name to see the related **Database**, for example, db.
9. Click the **OK** button twice to save your selections.
10. Click **Close** button in the **Database Connection Manager** window to save your connection.

For more information on configuring Essbase database connections in Workspace see: **Oracle Essbase Database Administrator's Guide for Oracle Essbase.**

Note

The database connection is available in both Workspace and Financial Reporting Studio. Optionally, it can be setup in Financial Reporting Studio when putting grids on a report. This should only be done by an administrator.

Configuring Oracle Fusion Transactional BI Dimensions

Within Oracle Fusion Transactional Business Intelligence (BI), Accounting Segment Dimensions such as Balancing segment or Cost Center segment are based on the Chart of Accounts configuration. These segments can be configured to be tree-enabled, which means that hierarchies are defined upon the segment values for rollup purposes. In such scenarios, you must filter by a specific hierarchy when performing ad-hoc queries against tree-based accounting segments. Incorrect results may occur if tree filters are not applied. To apply tree filters, create a filter condition on Tree Filter attributes in Accounting Segment Dimensions.

Note

For information on setting up General Ledger accounting segments, see the Oracle Fusion Transactional Business Intelligence Administrator's Guide.

6

Human Capital Management

Setting Up Oracle Fusion Human Capital Management Coexistence: Procedures

Oracle Fusion Human Capital Management (HCM) Coexistence functionality enables you to integrate your existing Oracle Human Resource applications with a hosted Oracle Fusion HCM implementation. As a result of the integration, you can use Oracle Fusion Workforce Compensation and Talent Management functionality alongside your existing setup.

Using Oracle Fusion HCM Coexistence, you can extract, transform, and transport files from PeopleSoft Enterprise or Oracle E-Business Suite and intelligently synchronize selected business object data between your source application and Oracle Fusion HCM applications. For more information, refer to HCM Coexistence: Explained.

Setting up an implementation of Oracle Fusion HCM for Coexistence with an existing application involves the following procedures.

1. Ensuring that tokens are correctly replaced during Oracle Enterprise Scheduler Service deployment
2. Setting up an FTP Server
3. Setting up FTP Accounts
4. Setting up SOA FTP Adapter
5. Setting up Oracle Data Integrator
6. Configuring the Oracle Web Services Manager for Interaction with the Source Application Web Services
7. Setting up the HCM Configuration for Coexistence Parameters

These procedures set up the connections in the Oracle Fusion environment to work with the source application. Therefore, you need to set up the connections in the source application as well. The instructions for configuring the source application are in the following documents, which are available on My Oracle Support (MOS):

- Integrating PeopleSoft HRMS 8.9 with Fusion Talent Management and Fusion Workforce Compensation (Document ID 1480967.1)
- Integrating PeopleSoft HRMS 9.0 with Fusion Talent Management and Fusion Workforce Compensation (Document ID 1480995.1)
- Integrating PeopleSoft HRMS 9.1 with Fusion Talent Management and Fusion Workforce Compensation (Document ID 1480996.1)
- HCM Coexistence - Integrating EBS HCM 11i and Fusion Talent Management and Workforce Compensation (Document ID 1460869.1
- HCM Coexistence - Integrating EBS HCM R12.1 and Fusion Talent Management and Workforce Compensation (Document ID 1460868.1

Prerequisites

Use Oracle Fusion Applications Provisioning to provision a new Oracle Fusion Applications environment. For information about using Oracle Fusion Applications Provisioning, see the Oracle Fusion Applications Installation Guide.

In addition to the components installed using Oracle Fusion Applications Provisioning, Oracle Fusion HCM Coexistence requires the following products to be installed.

- Adobe Reader
- Oracle Application Development Framework Desktop Integration (ADFDi)
- Microsoft Office 2007

For more details, see the topic Coexistence for HCM Offering: Overview.

1. Ensuring Correct Token Replacement During Oracle Enterprise Scheduler Service Deployment

Ensure that Oracle Fusion HCM invokes the following services defined in the Oracle Enterprise Scheduler Service connections.xml file for HcmEssApp.

- BulkLoadOdiInvoke - ODI Agent
- OdiAgentURLForHCM - ODI Agent via ODI-ESS bridge
- All entries with the prefix BulkLoad* - HCM product services

Ensure that the service URLs of the above entries are replaced correctly during deployment. Ensure that the Protocol, Host and Port tokens are assigned valid values for the application domain.

2. Setting Up an FTP Server

Oracle Fusion Applications Provisioning creates an FTP server and installs Oracle WebCenter. Ensure that the server is configured on port 20 and 21 and start the server.

3. Setting Up FTP Accounts

Create two user accounts with read and write access, a generic user account to configure the FTP adapter and a user specific account for Oracle Fusion Applications.

For example, create user accounts with directory structure and permissions as shown in the following table.

User/Usage	User Name (Operating System User)	Password	User Home Directory	Permissions	Comments
BPEL/SOA	`<bpel_username`	`<bpel_password`	/fusion	Read and write for current directory and child levels only	User account used with Oracle Fusion SOA FTP Adapter configuration.
Customer 1	`<customer1_use`	`<customer1-pswd>`	/fusion/E_<ENTERPRISE	Read and write for current directory and child levels only	The `<ENTERPRISE_ID>` corresponds to the Oracle Fusion Applications ID of Customer 1. The user account is used by the PeopleSoft Enterprise application interaction with the Oracle Fusion SOA/BPEL process.

4. Setting Up SOA FTP Adapter

Set up the following parameters of the SOA FTP adapter.

- Set the FTP server `hostname` in the FTP adapter connections properties file weblogic-ra.xml
- Set the FTP server operating system user name and password.

To set the FTP server `hostname` and set the FTP server operating system user name and password in the FTP adapter connections property file as follows.

1. Access FtpAdapter.rar available in the Oracle_SOA1 directory structure on Oracle Weblogic Server (WLS) HcmDomain server file system.
2. Extract and save the META-INF/weblogic-ra.xml file to a temporary location.
3. Update the META-INF/weblogic-ra.xml file with appropriate values for the following connection properties.

- <wls:jndi-name>eis/Ftp/FtpAdapter</wls:jndi-name>
- <wls:name>host</wls:name>

  <wls:value>ftpServerHostName</wls:value>
- <wls:name>username</wls:name>

  <wls:value>ftpUserName</wls:value>
- <wls:name>password</wls:name>

  <wls:value>ftpUserPswd</wls:value>

4. Create an additional copy of FtpAdapter.rar
5. Update FtpAdapter.rar with the updated META-INF/weblogic-ra.xml file.

   Run the following command.

```
zip -ur /<path>/Oracle_SOA1/soa/connectors/FtpAdapter.rar META-INF/
weblogic-ra.xml
```

6. Bounce the WLS HcmDomain.

5. Setting Up Oracle Data Integrator

To set up Oracle Data Integrator for HCM Coexistence, complete the following procedures.

- Create Oracle Data Integrator directories.
- Validate Oracle Data Integrator topology settings.
- Verify the configuration of the work repository.
- Verify database connections.
- Configure file technology connections.

Before performing the above steps, ensure that the following are set up.

- Oracle Data Integrator code is loaded using XML Import into a copy of the central template repository (id:500) using the FUSION_ODI schema.
- Topology entries are coming from the central template repository.
- Work repository (jdbc) is configured automatically to match the installation.
- Topology Java DataBase Connectivity (JDBC) entries for the database are configured automatically to match the installation.
- Installation uses the default FUSION and FUSION_ODI_STAGE schemas.
- Schemas FUSION and FUSION_ODI_STAGE are installed in the same database.

- The Oracle Data Integrator repository is in the same database as FUSION (schema: FUSION_ODI).
- Default context **Development** is used.
- Oracle Data Integrator console is available for configuration of the topology.

Create Oracle Data Integrator Directories

You need to manually create and specify the directories and files to which Oracle Data Integrator has read and write access.

- For each enterprise, create an enterprise folder in the work directory.
- For the operating system user of the Oracle Data Integrator agent, create or specify directories for the items listed in the following table for Oracle Data Integrator use. The users must have full read and write access to the directories.

Oracle Data Integrator Directory Name	Item Description	Example Value
FILE_ROOT_HCM	Oracle Data Integrator base work directory	/home/ODI_ROOT_DIRECTORY
FILE_OUTPUT_HCM	Oracle Data Integrator export work directory	/home/ODI_ROOT_DIRECTORY/export
N/a	Enterprise directory name, where `<eid>` is the numeric enterprise id	/home/ODI_ROOT_DIRECTORY/E_<eid>

Note

While creating the directory, ensure that the owner of the directory and the operating user of the Oracle Data Integrator agent are the same. The directory should be accessible from the Web logic domain that runs the Oracle Data Integrator agent and the SOA process.

Validate the Topology Settings

After you have created the directories, use either Oracle Data Integrator Studio or Oracle Data Integrator Repository Explorer to validate the Oracle Data Integrator topology settings.

Configure or validate the following.

- Work repository connection
- Oracle technology (database) connections
- File technology connections

Note

Use JDBC connection and credentials to validate and ensure that the connections refer to the correct database.

Verify the Configuration of the Work Repository

Use Oracle Data Integrator Studio to verify the work directories and repository configuration.

1. Go to **Topology** - **Repositories** - **Work Repositories** .
2. Double-click **FUSIONAPPS_WREP**.
3. Verify that the work repository (jdbc URL) points to your Oracle Fusion database.

Verify Database Connections

Verify that the JDBC data server URLs point to the Oracle Fusion Applications database.

1. Go to **Topology** - **Physical Architecture** - **Oracle** .
2. Double-click the **ORACLE_FUSION** data server
3. On the Definitions page, verify that the **Connection User** is FUSION_ODI_STAGE.
4. Enter the password.
5. In the **Instance/db link (Data Server)** field, enter the instance for the Oracle Fusion Applications database.

   Use the following format if the instance name is not registered with the Transparent Network Substrate (TNS) service: `<host>:<port>/<instance_name>`. If the instance name is registered with the TNS service, specify only the instance name.
6. Click **JDBC**.
7. Ensure that the URL in the **JDBC URL** field points to the Oracle Fusion Applications database.
8. Expand and open the child schema: **ORACLE_FUSION.FUSION**.
9. Ensure that the **Default** box is selected.
10. Verify that FUSION is entered as the value in the **Schema** field.
11. Verify that FUSION_ODI_STAGE is entered as the value in the **Work Schema** field.

Note

Perform the same steps for the ORACLE_WORK_HCM data server. However, ensure that the value of both the schema and the work schema is FUSION_ODI_STAGE.

Configure File Technology Connections

The ODI work directories that you defined now need to be configured in the topology so that ODI can make use of them.

Using ODI Studio, configure files in topology.

1. Go to **Topology** - **Physical Architecture** - **File** .
2. Double-click FILE_ROOT_HCM.
3. Verify that the value of **JDBC Driver** is com.sunopsis.jdbc.driver.file.FileDriver.
4. Verify that the value of **JDBC URL** is jdbc:snps:dbfile.
5. Expand and open the child physical schema.
6. For **Directory (Schema)** provide the directory path that you defined for FILE_ROOT_HCM.
7. Provide the same value for **Directory (Work Schema)**.
8. Ensure that the **Default** box is selected.

Use the same steps to configure FILE_OUTPUT_HCM using the directory path for FILE_OUTPUT_HCM instead of FILE_ROOT_HCM.

Enable SQL*Loader for Oracle Data Integrator

Oracle Fusion HCM Coexistence Oracle Data Integrator uses SQL*Loader to import file data. Use the SQL*Loader in Oracle Data Integrator from the Oracle Weblogic Server environment to perform the following steps.

1. Determine the directory where the Oracle client software is installed for your deployment. The default name is DBCLIENT and it is placed in the parent directory of <MW_HOME>. You could refer to this directory as DBCLIENT ORACLE_HOME.
2. Verify the existence of DBCLIENT ORACLE_HOME/bin/sqlldr.
3. Using the `cd` command, change the directory to <ODI ORACLE_HOME>/bin.
4. Use a text editor to create a script with the file name sqlldr containing the following.

```
#!/bin/sh
ORACLE_HOME=<DBCLIENT ORACLE_HOME>
export ORACLE_HOME
$ORACLE_HOME/bin/sqlldr $*
#
```

5. Make the script executable using the following command.

```
chmod +x sqlldr
```

6. Configuring the Oracle Web Services Manager for Interaction with the Source Application Web Services

Configure the Oracle Web Services Manager certificate key with the user credentials for a Simple Object Access Protocol (SOAP) interaction with the source application Web services.

The user credentials correspond to the source application user with entitlement to invoke the source application Web service.

1. Sign in to the Enterprise Manager Console as a Weblogic_Administrator user.
2. Access **HcmDomain** under the Weblogic Domain.
3. Open **Security** - **Credentials** .
4. Access and expand the key map oracle.wsm.security.
5. Click **Credential Key** to search for the key `FUSION_APPS_HCM_HR2HR_APPLOGIN-KEY`.
6. Click **Edit** to update the credentials.
7. Set the user name and password of the source application user.

7. Setting up the HCM Configuration for Coexistence Parameters

After you have created the FTP and Oracle Data Integrator directory paths, you need to set up the related parameters in Oracle Fusion HCM.

1. Sign into Oracle Fusion Applications.

Note

The Oracle Fusion Applications user must have the appropriate roles to set up and configure Oracle Fusion applications. At least, ensure that the user is assigned the **View All** data role for the **HCM Application Administrator** job role. For details on setting up implementation users, refer to the HCM Coexistence Implementation Guide.

---

2. Go to **Navigator** - **Tools** - **Setup and Maintenance** and perform the following tasks:

   a. Find and initiate the **Manage HCM Configuration for Coexistence** task to bring up the **Manage HCM Configuration for Coexistence** parameters page.

   b. Set up the following parameters.

Parameter	Description
On Demand FTP Root Directory	Mounted root directory of the server
ODI Context	The logical name for the group containing logical-to-physical mappings for connections in Oracle Data Integrator. The default value in Oracle Data Integrator is DEVELOPMENT. **Note** This value is case sensitive. Therefore, ensure that it is completely uppercase.
ODI User	The Oracle Data Integrator user name

ODI Password	The password associated with the Oracle Data Integrator user name
ODI Work Repository	The repository that contains the Oracle Data Integrator related code definitions. The default value in Oracle Data Integrator is `FUSIONAPPS_WREP`.
ODI Root Directory	The local directory where Oracle Data Integrator processes files and creates work and log files. It is the directory path defined for `FILE_ROOT_HCM`, when creating the Oracle Data Integrator directories.

You are now ready to implement Oracle Fusion Talent and Oracle Fusion Workforce Compensation using the Coexistence for HCM offering, available from the Setup and Maintenance work area of Oracle Fusion Applications.

7

Incentive Compensation

Integrating Oracle Fusion Incentive Compensation with Geo Map Server: Procedures

Oracle Fusion Incentive Compensation uses the functionality provided by the Geo Map server. Depending on the network connectivity where the application is installed and the available support for integration, you may have to modify the MapViewer and GeoMapViewer connections.

If you intend to use the map server provided by Oracle, you must connect to http://elocation.oracle.com.

Note

If the firewall on your network blocks HTTP connections, you cannot access the map server.

If you intend to use your preferred map server or any other map server that is available on premise or on another network, you must modify certain Application Development Framework (ADF) connection properties for MapViewer and GeoMapViewer.

1. Sign in to Oracle Enterprise Manager Fusion Applications Control.
2. In the left pane, navigate through **Oracle Fusion Incentive Compensation - Fusion Applications - IncentiveCompensationApp** and click the server for which you want to modify the ADF connection properties.
3. At the top of the page, from the **Fusion J2EE Application** context menu, select **ADF - Configure ADF Connections** .
4. On the ADF Connections Configuration page, go to the **URL Connections** section.
5. Select the **MapViewerURL** connection name and click **Edit**.

6. In the URL field, replace the default URL with the URL or location information of your preferred map server and click **OK**.

7. Repeat the steps to modify the URL for the **GeoMapViewer** connection name.

8

Project Portfolio Management

Configuring Oracle Fusion Project Portfolio Management Integration with Primavera P6 Enterprise Project Portfolio Management: Procedures

Use Oracle Fusion Project Integration Gateway to integrate Oracle Fusion Project Portfolio Management with Primavera P6 Enterprise Project Portfolio Management. The integration enables project accountants, project billing specialists, and executives to centrally perform project costing, billing, accounting, and executive reporting tasks in Oracle Fusion Project Portfolio Management while enabling each project manager to perform detailed project planning and scheduling in Primavera P6 Enterprise Project Portfolio Management.

Configuring Oracle Fusion Project Portfolio Management Integration With P6 Enterprise Project Portfolio Management

To configure Oracle Fusion Project Portfolio Management Integration with Primavera P6 Enterprise Project Portfolio Management, complete the following tasks:

1. Install Primavera P6 Enterprise Project Portfolio Management and configure Oracle Fusion Project Portfolio Management Bridge.

   For more information on installing Primavera P6 integration with Oracle Fusion Project Portfolio Management and working with Oracle Fusion Project Portfolio Management Bridge, see Primavera P6 EPPM Administrator's Guide for an Oracle Database.

2. Configure the Oracle Fusion Project Portfolio Management environment.

   a. Verify that `FUSION_APPS_PRJ_P6INT_ADMIN-KEY oracle.wsm.security` credential key is defined for the `ProjectsDomain` in Oracle Fusion Projects.

For the `FUSION_APPS_PRJ_P6INT_ADMIN-KEY` key, ensure that the user name and password match the user name and password of the P6 administration super user designated for use with the integration between Oracle Fusion Project Portfolio Management and Primavera P6 Enterprise Project Portfolio Management. For more information on managing the credential store and defining the credential keys, see the Oracle Fusion Middleware Application Security Guide.

b. Create a user named `FUSION_P6_PROJECT_INTEGRATION_USER`.

   For more information on using the administration console to manage users, groups, and roles, refer to the Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server.

c. Register the Primavera P6 Endpoint address details in Oracle Fusion Functional Setup Manager.

   1. Click Topology Registration > Register Enterprise Applications and add the following enterprise application:

      Enterprise Application: `PJGP6 Primavera Application`

      Name: `PJGP6_Primavera1`

   2. Enter the host and port server details where the P6 integration service is deployed:

      Server Protocol: `http`

      External Server host: `<host of the P6 integration service>`

      External Server port: `<port of the P6 integration service>`

9

Supply Chain Management

Installing Oracle Enterprise Data Quality for Product Data Oracle DataLens Server: Procedures

Oracle Enterprise Data Quality for Product Data is built on industry-leading DataLens Technology to standardize, match, enrich, classify, and correct product data from different sources and systems. For Oracle Fusion Product Hub to use Oracle Enterprise Data Quality for Product Data features, you must establish a connection between them.

For more information on installing and using Oracle Enterprise Data Quality for Product Data Oracle DataLens Server, see the Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Installation Guide. For more information on implementation, see Oracle Enterprise Data Quality for Product Data R12 PIM Connector Installation Guide.

Establishing Connection

After installation, use the Oracle Enterprise Manager to establish or modify the connection with the Oracle DataLens Server.

1. Log in to an Oracle Fusion Middleware farm using Oracle Enterprise Manager Fusion Applications Control.
2. Expand the Fusion Applications node under Oracle Fusion Supply Chain Management.
3. Right-click the application for which a connection will be established, for example, **ProductManagementApp**.
4. Select **ADF** - **Configure ADF Connections** from the menu.
5. On the ADF Connections Configuration page, set the connection type as `URL` and the connection name as `DSAServerURL`.
6. Click **Create Connection**. The added connection appears under URL Connections.

7. Under URL Connections, select **Edit** `DSAServerURL` and provide the **URL** for Oracle DataLens Server.

   For example, the SOA Common Properties Server URL with `/datalens` appended to the URL such as `http://fusionsystemtest-controlled-z-scm.us.oracle.com:80/datalens`.

8. Click **OK**.

9. Click **Apply**.

10. Set connections for **ProductManagementCommonApp** and **ScmEssApp** applications using step 3 to step 10.

    For the changes to take effect, restart the Product Management, SCM Common, and ESS servers from the Weblogic Admin Console.

For more information on establishing and modifying connection configurations, see the Oracle Fusion Middleware Administrator's Guide for Oracle Application Development Framework.

Glossary

BPEL

Business Process Execution Language; a standard language for defining how to send XML messages to remote services, manipulate XML data structures, receive XML messages asynchronously from remote services, manage events and exceptions, define parallel sequences of execution, and undo parts of processes when exceptions occur.

cube

A block of data that contains three or more dimensions. An Essbase database is a cube.

DMZ

Acronym for demilitarized zone. An isolated internal network used for servers that are accessed by external clients on the Internet, such as web servers, to provide a measure of security for internal networks behind the firewall.

e-mail bounce

An e-mail that is returned due to a temporary or permanent error condition.

financial reporting book

Comprised of reports and other documents such as text, PDF, PowerPoint, Excel and Word files. When run, the report data is dynamically retrieved from the database; the snapshot data remains static.

FTP

Acronym for File Transfer Protocol. A system for transferring computer files, generally by the Internet.

global area

The region across the top of the user interface. It provides access to features and tools that are relevant to any page you are on.

MTA

Acronym for mail transfer agent. A software program that transfers electronic mail messages from one computer to another.

offering

A comprehensive grouping of business functions, such as Sales or Product Management, that is delivered as a unit to support one or more business processes.

Oracle Fusion Applications Search

A special type of search based on technology that differs from that of most other searches in Oracle Fusion Applications. Oracle Fusion Applications Search is available in the global area and other places.

point of view

User selected dimensions that are not included in the grids at the row, column or page levels for a particular report. Only these dimensions can be overridden at run time, unless user also specifically defined Prompt for the dimensions on the grid.

SOA

Abbreviation for service-oriented architecture.

WSDL

Abbreviation for Web Services Description Language. It is an XML format that provides a model for describing Web services.